IP8800/S3660 ソフトウェアマニュアル

コンフィグレーションガイド Vol.1

Ver. 12.2 対応

IP88S38-S010-D0

■ 対象製品

このマニュアルは IP8800/S3660 を対象に記載しています。また，ソフトウェア OS-L3M Ver. 12.2 の機能について記載しています。

■ 輸出時の注意

本製品を輸出される場合には，外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ，必要な手続きをお取りください。なお，不明な場合は，弊社担当営業にお問い合わせください。

■ 商標一覧

AMD は，米国 Advanced Micro Device, Inc.の米国および他の国々における登録商標です。
Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，富士フイルムビジネスイノベーション株式会社の登録商標です。
GSRP は，アラクサラネットワークス株式会社の登録商標です。
Internet Explorer は，米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。
IPX は，Novell,Inc.の商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
OpenSSL は，米国およびその他の国における米国 OpenSSL Software Foundation の登録商標です。
Python は，Python Software Foundation の登録商標です。
RSA および RC4 は，米国およびその他の国における米国 EMC Corporation の登録商標です。
sFlow は，米国およびその他の国における米国 InMon Corp. の登録商標です。
ssh は，SSH Communications Security,Inc.の登録商標です。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
イーサネットは，富士フイルムビジネスイノベーション株式会社の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■ マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■ ご注意

このマニュアルの内容については，改良のため，予告なく変更する場合があります。

■ 発行

２０２４年　１０月 （第１４版） ＩＰ８８Ｓ３８-Ｓ０１０－Ｄ０

■ 著作権

変更内容

【Ver. 12.2 対応版】

表　変更内容

章・節・項・タイトル	追加・変更内容
3.12.2　経路エントリ数と最大隣接ルータ数の関係	• IPv4 モードでの OSPF の最大経路エントリ数を変更しました。
3.13.1　IPv4 マルチキャスト	• 1 ネットワーク（VPN）当たりランデブーポイントに設定できる延べグループ数の最大数を変更しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 12.1 対応 Rev.11 版】

表　変更内容

項目	追加・変更内容
収容回線数	• IP8800/S3660-16S4XW および IP8800/S3660-24S8XW の SFP ポートに，SFP-T の記述を追加しました。
IPv4 マルチキャスト	• IPv4 マルチキャストの収容条件を拡張しました。
ポートの種類とサポート機能	• SFP ポートに，SFP-T の記述を追加しました。

【Ver. 12.1 対応 Rev.10 版】

表　変更内容

項目	追加・変更内容
IGMP snooping/MLD snooping	• IGMP snooping の収容条件に記述を追加しました。
VRRP	• VRRP の収容条件に記述を追加しました。
IPv4 マルチキャスト	• IPv4 マルチキャストの収容条件を拡張しました。
マルチホームでの使用	• 本項を追加しました。

【Ver. 12.1 対応 Rev.9 版】

表　変更内容

項目	追加・変更内容
ハードウェア構成	• PS-A06R および FAN-04R の記述を追加しました。
受信側フィルタエントリ数	• 受信側フロー検出モードに custom を追加しました。
受信側 QoS エントリ数	• 受信側フロー検出モードに custom を追加しました。
受信側ポリシーベースミラーリングエントリ数	• 受信側フロー検出モードに custom を追加しました。
custom 指定時のエントリ分配	• 本項を追加しました。
DHCP snooping	• 受信側フロー検出モードに custom を追加しました。

項目	追加・変更内容
ポリシーベースルーティング（IPv4）	• ポリシーベースルーティングの使用条件となる受信側フロー検出モードに custom を追加しました。
サポート機能	• IPv6 DHCP リレーについて, スタックでのサポート状況を変更しました。
メンバスイッチの通信切り替え	• スタックでの短時間通信切り替えサポート状況に IPv6 DHCP リレーを追加しました。
ポートの種類とサポート機能	• 100GBASE-CWDM4 および 100GBASE-4WDM-40 の記述を追加しました。
100GBASE-R	• 100GBASE-CWDM4 および 100GBASE-4WDM-40 の記述を追加しました。

【Ver. 12.1 対応 Rev.8 版】

表　変更内容

項目	追加・変更内容
本装置のモデル	• IP8800/S3660-24X4QW について記述を追加しました。
収容回線数	• IP8800/S3660-24X4QW について記述を追加しました。
ソフトウェア	• IP8800/S3660-24X4QW について記述を追加しました。
VLAN	• IP8800/S3660-24X4QW について記述を追加しました。
フィルタ・QoS・ポリシーベースミラーリング	• フロー検出モード layer3-mirror-1-out, layer3-mirror-2-out の記述を削除しました。 •「送信側ポリシーベースミラーリングエントリ数」の記述を削除しました。
スタックポートとスタックリンク	• IP8800/S3660-24X4QW について記述を追加しました。
SNMP 概説	• SNMPv3 の認証プロトコルとプライバシープロトコルについて記述を追加しました。
Sync-E	• IP8800/S3660-24X4QW について記述を追加しました。

【Ver. 12.1 対応 Rev.7 版】

表　変更内容

項目	追加・変更内容
SSH(Secure Shell)	• SSHv2 のサポート仕様を変更しました。

【Ver. 12.1 対応 Rev.6 版】

表　変更内容

項目	追加・変更内容
本装置のモデル	• IP8800/S3660-16S4XW および IP8800/S3660-24S8XW について記述を追加しました。
収容回線数	• IP8800/S3660-16S4XW および IP8800/S3660-24S8XW について記述を追加しました。

項目	追加・変更内容
ソフトウェア	• ポート数拡張のオプションライセンスについて記述を追加しました。
VLAN	• IP8800/S3660-16S4XW および IP8800/S3660-24S8XW について記述を追加しました。 • VLAN ごとの MAC アドレスの装置当たりの数を訂正しました。
IPv4 マルチキャスト	• 1 ネットワーク（VPN）当たりランデブーポイントに設定できる延べグループ数の最大数を変更しました。 • 1 ネットワーク（VPN）当たりのランデブーポイント候補数の記述を追加しました。
サポート機能	• sFlow 統計について，スタックでのサポート状況を変更しました。
スタックポートとスタックリンク	• IP8800/S3660-16S4XW および IP8800/S3660-24S8XW について記述を追加しました。
ポートの種類とサポート機能	• SFP ポートおよび SFP+ポートについて記述を追加しました。
10GBASE-R	• 10GBASE-BR について記述を追加しました。
サポート仕様	• リンクアグリゲーションの準拠規格を IEEE802.1AX に変更しました。

【Ver. 12.1 対応 Rev.5 版】

表　変更内容

項目	追加・変更内容
LLDP/OADP	• 「(1) LLDP」に次の記述を追加しました。 Port And Protocol VLAN ID TLV で送信できる VLAN 数 VLAN Name TLV で送信できる VLAN 数
PTP	• 本項を追加しました。
UDP ブロードキャストリレー	• 本項を追加しました。
サポート機能	• IGMP snooping について，スタックでのサポート状況を変更しました。 • PTP の記述を追加しました。 • UDP ブロードキャストリレーの記述を追加しました。
メンバスイッチの通信切り替え	• LACP について，スタックでの短時間切り替えサポートの記述を変更しました。
スタックでの IGMP snooping の設定	• 本項を追加しました。

【Ver. 12.1 対応 Rev.4 版】

表　変更内容

項目	追加・変更内容
本装置のモデル	• IP8800/S3660-24T4X について記述を追加しました。
収容回線数	• IP8800/S3660-24T4X について記述を追加しました。
ハードウェア構成	• 電源固定式モデルについて記述を追加しました。

項目	追加・変更内容
ソフトウェア	• オプションライセンス OP-ULTG の記述に IP8800/S3660-24T4X を追加しました。 • オプションライセンス OP-SYNC の記述を追加しました。
VLAN	• IP8800/S3660-24T4X について記述を追加しました。
フィルタ・QoS・ポリシーベースミラーリング	• 受信側フロー検出モード追加に伴って受信側フィルタエントリ数の収容条件を追加しました。 • 受信側フロー検出モード追加に伴って受信側 QoS エントリ数の収容条件を追加しました。 • 受信側フロー検出モード追加に伴って受信側ポリシーベースミラーリングエントリ数の収容条件を追加しました。
LLDP/OADP	• LLDP 隣接装置情報の最大収容数を変更しました。
サポート機能	• LLDP について，スタックでのサポート状況を変更しました。
電源固定式モデルでの電源の重度障害判定の設定	• 本項を追加しました。
Sync-E	• 本項を追加しました。
Sync-E の設定	• 本項を追加しました。
Sync-E の確認	• 本項を追加しました。
VXLAN のパケット長	• 本項を追加しました。

【Ver. 12.1 対応 Rev.3 版】

表　変更内容

項目	追加・変更内容
VXLAN	• VXLAN の収容条件に記述を追加しました。
アップリンク・リダンダント	• アップリンクポート数を変更しました。
サポート機能	• アップリンク・リダンダントについて，スタックでのサポート状況を変更しました。
スタックポートとスタックリンク	• 100GBASE-CR4 についての記述を追加しました。
スタックの注意事項	•「(11) スタックリンクを接続できるポートの組み合わせについて」を追加しました。
ポートの種類とサポート機能	• 100GBASE-SR4 の記述を追加しました。
100GBASE-R	• 100GBASE-SR4 の記述を追加しました。
MAC アドレス学習の移動検出	• MAC アドレス学習移動監視機能のサポートに伴って記述を追加しました。
MAC アドレス学習移動監視機能	• 本項を追加しました。
MAC アドレス学習移動監視機能の設定	• 本項を追加しました。
概要	•「(4) UDLD フォワーディング機能」を追加しました。

項目	追加・変更内容
L2 プロトコルフレーム透過機能の注意事項	•「(2) UDLD フォワーディング機能」を追加しました。
L2 プロトコルフレーム透過機能の設定	•「(4) UDLD フォワーディング機能の設定」を追加しました。
カプセル化およびデカプセル化時の優先度引き継ぎ	• L2 プロトコルフレーム透過機能使用時の記述を追加しました。

【Ver. 12.1 対応 Rev.2 版】

表　変更内容

項目	追加・変更内容
SSH	• 本節を追加しました。
リンクアグリゲーションの転送動作	• リンクアグリゲーションの転送動作の記述を変更しました。
SSH(SecureShell)	• 本章を追加しました。
高機能スクリプト	• 本章を追加しました。
ポートの種類とサポート機能	• 100GBASE-CR4 のサポートに伴って記述を追加しました。
100GBASE-R	• 100GBASE-CR4 の記述を追加しました。
フレーム送信時のポート振り分け	• スタック構成時のポート振り分けの記述を変更しました。

【Ver. 12.1 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
本装置のモデル	• IP8800/S3660-48X4QW の記述を追加しました。
収容回線数	• IP8800/S3660-48X4QW の記述を追加しました。
VLAN	• IP8800/S3660-48X4QW の記述を追加しました。
VXLAN	• VTEP 数の最大数を変更しました。
ポートの種類とサポート機能	• SFP+/SFP 共用ポートの記述に SFP-T の記述を追加しました。
10BASE-T/100BASE-TX/1000BASE-T/10GBASE-T	• SFP+/SFP 共用ポートで SFP-T を使用した場合の接続仕様を追加しました。
MAC アドレス学習抑止	•「(2) VNI 単位の MAC アドレス学習抑止」を追加しました。
MAC アドレステーブルのクリア	• MAC アドレス学習抑止のコンフィグレーションの設定の説明に，VXLAN 機能有効時の記述を追加しました。
概要	•「(3) LLDP フォワーディング機能」を追加しました。
L2 プロトコルフレーム透過機能の設定	•「(3) LLDP フォワーディング機能の設定」を追加しました。
VXLAN カプセル化	• 本項を追加しました。
MAC アドレステーブル	•「(3) MAC アドレステーブルの学習抑止」を追加しました。
カプセル化およびデカプセル化時の優先度引き継ぎ	• 本項を追加しました。

【Ver. 12.1 対応版】

表　変更内容

項目	追加・変更内容
VLAN	• MAC VLAN の登録 MAC アドレス数の記述を変更しました。
VXLAN	• サブインタフェース数について記述を追加しました。
フレーム送信時のポート振り分け	• 振り分けに使用する情報にイーサタイプを追加しました。
MAC アドレス学習抑止	• 本項を追加しました。
注意事項	•「(2) MAC アドレス学習の抑止について」を追加しました。
MAC アドレス学習抑止の設定	• 本項を追加しました。
VLAN マッピングの設定	•「(2) VTEP と VNI の設定」に，VLAN マッピングで収容条件を拡張するモードを使用する場合の記述を追加しました。

はじめに

■ 対象製品およびソフトウェアバージョン

このマニュアルは IP8800/S3660 を対象に記載しています。また，ソフトウェア OS-L3M Ver. 12.2 の機能について記載しています。ソフトウェア機能は，ソフトウェアライセンスおよびオプションライセンスによってサポートする機能について記載します。

操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。

なお，このマニュアルでは特に断らないかぎり，SL-L3A および SL-L3L のソフトウェアライセンスに共通の機能について記載します。共通でない機能については以下のマークで示します。

【SL-L3A】：

ソフトウェアライセンス SL-L3A についての記述です。

■ このマニュアルの訂正について

このマニュアルに記載の内容は，ソフトウェアと共に提供する「リリースノート」および「マニュアル訂正資料」で訂正する場合があります。

■ 対象読者

本装置を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。

また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■ このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。

https://jpn.nec.com/ip88n/

■ マニュアルの読書手順

本装置の導入，セットアップ，日常運用までの作業フローに従って，それぞれの場合に参照するマニュアルを次に示します。

●装置の開梱から，初期導入時の基本的な設定を知りたい

クイックスタートガイド
(IP88S36-Q002)

●ハードウェアの設備条件，取扱方法を調べる

ハードウェア取扱説明書
(IP88S36-H002)

トランシーバ
ハードウェア取扱説明書
(IP88-COM-H001)

●ソフトウェアの機能，
コンフィグレーションの設定，
運用コマンドについての確認を知りたい

コンフィグレーションガイド
Vol.1
(IP88S38-S010)

Vol.2
(IP88S38-S011)

Vol.3
(IP88S38-S012)

●コンフィグレーションコマンドの
入力シンタックス，パラメータ詳細
について知りたい

コンフィグレーション
コマンドレファレンス
Vol.1 (IP88S38-S013)

Vol.2
(IP88S38-S014)

●運用コマンドの入力シンタックス，
パラメータ詳細について知りたい

運用コマンドレファレンス
Vol.1
(IP88S38-S015)

Vol.2
(IP88S38-S016)

●メッセージとログについて調べる

メッセージ・ログレファレンス
(IP88S38-S017)

●MIBについて調べる

MIBレファレンス
(IP88S38-S018)

●トラブル発生時の対処方法について
知りたい

トラブルシューティングガイド
(IP88S36-T002)

■ このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second　　*bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DNSSL	Domain Name System Search List
DR	Designated Router
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECDHE	Elliptic Curve Diffie-Hellman key exchange, Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GCM	Galois/Counter Mode
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol

IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second *ppsと表記する場合もあります。
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PMTU	Path Maximum Transmission Unit
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PTP	Precision Time Protocol
QoS	Quality of Service
QSFP+	Quad Small Form factor Pluggable Plus
QSFP28	28Gbps Quad Small Form factor Pluggable
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
RDNSS	Recursive Domain Name System Server
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol

RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSA	Rivest, Shamir, Adleman
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
Sync-E	Synchronous Ethernet
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLS	Transport Layer Security
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VLAN	Virtual LAN
VNI	VXLAN Network Identifier
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
VTEP	VXLAN Tunnel End Point
VXLAN	Virtual eXtensible Local Area Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web

■ KB（キロバイト）などの単位表記について

1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト），1TB（テラバイト）はそれぞれ 1024 バイト，1024^2 バイト，1024^3 バイト，1024^4 バイトです。

目次

第 1 編　本装置の概要と収容条件

第 2 編　運用管理

1 本装置の概要

この章では，本装置の特長について説明します。

1.1　本装置の概要

企業内のネットワークは，IP 電話，インターネット接続，基幹業務などに使われ，PC は一人に 1 台が配布されるなど企業内の通信トラフィックは増大し続ける一方です。

また, ネットワークに流れるデータは企業の利益を左右するミッションクリティカルな重要データが流れています。ミッションクリティカルな市場は，ISP やネットワーク事業者が中心でしたが，今後は企業や公共の構内網に拡大されていく傾向にあります。

本装置は，ミッションクリティカルの分野に適用可能な製品にすることで，信頼性・可用性・拡張性の高い情報ネットワーク基盤を柔軟に構築するスイッチ製品です。

製品コンセプト

本装置は，「ギャランティード・ネットワーク」を実現するために開発してきた基幹ルータの高信頼・高機能をコンパクトに凝縮した，コアから拠点接続まで幅広いシーンに最適なギガビットレイヤ 3 スイッチです。

本装置は次の機能を実現します。

- 大規模ネットワークで使用される OSPF，BGP4 などのルーティングプロトコルや，先進の IPv6，マルチキャストなどを装備し，多様で柔軟なネットワークを実現
- さまざまなネットワーク冗長機能をサポートし，高信頼・高可用なネットワークを実現
- 複数の装置を接続して論理的に 1 台の装置として動作させるスタック機能によって，一元管理，冗長化，拡張性を実現
- リンクアグリゲーションや 10Gbit/s，40Gbit/s，100Gbit/s ポートを用意し，トラフィック増大に対して余裕を持ったネットワークを実現
- 企業内で扱われるさまざまなトラフィック（基幹業務データ，VoIP 電話データ，テレビ会議，ストリーミング配信，CAD データなど）を QoS 技術などで保護するギャランティ型ネットワークを実現
- 高機能フィルタ，ユーザ認証などのセキュリティ機能で安全なネットワークを実現
- フルワイヤレートでのパケットフォワーディングを実現
- 複数のサービスネットワークを一つの物理ネットワーク内に仮想的に収容し，統合化することによって，ネットワークの構築・運用コストを削減するネットワーク・パーティションを実現

1.2　本装置の特長

(1)　高速で多様な VLAN 機能をサポート

●レイヤ 2 の VLAN 機能

- ポート VLAN，プロトコル VLAN，MAC VLAN 機能を実装
- 用途に応じた VLAN 構築が可能

●スパニングツリープロトコル

- スパニングツリー（IEEE 802.1D），高速スパニングツリー（IEEE 802.1w），PVST+，マルチプルスパニングツリー（IEEE 802.1s）を実装

●VLAN トンネリングによる L2-VPN の実現

(2)　強固なセキュリティ機能

●認証・検疫ソリューション

- レイヤ 2 認証機能（IEEE802.1X，Web 認証，MAC 認証）によって，エッジの物理構成の自由度を保ちつつ，PC1 台 1 台を認証し，VLAN に加入させることが可能
- 認証サーバと検疫サーバとの組み合わせによって，検疫チェックをパスした PC だけを業務 VLAN に自動接続する検疫ソリューションを構築可能

●高性能できめ細かなパケットフィルタが可能

- ハードウェアによる高性能なフィルタ処理
- L2/L3/L4 ヘッダの一部指定が可能

●RADIUS／TACACS+による装置へのログイン・パスワード認証およびユーザごとに実行可能コマンドの制限を設定可能

●不正な DHCP サーバ／固定 IP アドレス端末の排除が可能

- DHCP snooping によって，不正な DHCP サーバや固定 IP アドレス端末の排除が可能

(3)　ハードウェアによる強力な QoS で通信品質を保証

- ハードウェアによる高性能な QoS 処理
- きめ細かなパラメータ（L2/L3/L4 ヘッダ）指定で，高い精度の QoS 制御が可能
- 多様な QoS 制御機能
  L2-QoS（IEEE 802.1p，帯域制御，優先制御，廃棄制御など），IP-QoS（Diff-Serv，帯域制御，優先制御，廃棄制御など）
- 音声・データ統合ネットワークでさまざまなシェーパ機能
  VoIP パケットを優先し，クリアな音声を提供可能。

(4)　10G/40G/100G イーサネット対応

●10G／40G／100G イーサネット対応

- 構内ネットワークで IP8800/S8600,IP8800/S8300,IP8800/S4600 シリーズと組み合わせると，ハイパフォーマンスな 10G／40G／100G ネットワークを実現。
- 10G イーサネットのトランシーバとして 1G と 10G のイーサネットに対応可能な SFP+を採用。

- 40G イーサネットのトランシーバとして QSFP+を採用。
- 100G イーサネットのトランシーバとして 100G のイーサネットに対応可能な QSFP28 を採用（IP8800/S3660-48XT4QW，IP8800/S3660-24X4QW，IP8800/S3660-48X4QW）。
- ダイレクトアタッチケーブルのサポートによって低価格な接続ソリューションを提供。
- 10G サーバの収容に最適な 10GBASE-T（UTP）環境を提供（IP8800/S3660-48XT4QW）。

(5)　フォールト・トレラント・スイッチを実現するスタック機能

●拡張性が高いフォールト・トレラント・スイッチ

- 複数の装置で構成することで，一部の障害でも通信の継続が可能
- 装置の追加によって，利用できるポート数を拡張可能

●スタックポートの帯域に依存しないトラフィック中継

- 複数のメンバスイッチにポートを収容しているリンクアグリゲーションが転送先となる場合，受信した回線を収容するメンバスイッチのリンクアグリゲーションポートから転送が可能

●無停止ソフトウェアアップデート

- ネットワークの通信を中断することなく，マスタスイッチ，バックアップスイッチを切り替えながら，ソフトウェアのアップデートが可能

●管理の一元化によるコスト低減

- 複数の装置を 1 台の装置として運用することで，管理の一元化が可能

(6)　実績あるルーティング機能

●安定した高機能ルーティング

- 広域イーサネットサービスや IP-VPN サービスを利用した拠点間接続に，OSPF 機能や BGP 機能を使用した信頼性の高いルーティングと，マルチパスを使った負荷分散を実現
- ルーティングソフトウェアには，実績ある弊社上位機種と同等のものを実装

●IPv6 マルチキャスト対応

- IPv4 と IPv6 で同一ピーク性能の実現
- 10 ギガビット・イーサネットでフルワイヤレートの IPv6 ルーティングを実現
- 豊富な IPv6 ルーティングプロトコル（スタティック，RIPng，OSPFv3，BGP4+，PIM-SM，PM-SSM，MLD）によって，多様で柔軟な IPv6 ネットワークを実現可能
- IPv4/IPv6 デュアルスタック，IPv6-only 環境に対応したネットワーク管理（SNMP over IPv6）など充実した機能

●充実した IPv4 ルーティングプロトコル

- 実績ある豊富な IPv4 ルーティングプロトコルをサポート
  （スタティック，RIP，OSPF，BGP4，PIM-SM/SSM，IGMP）

●ポリシーベースルーティング

- 中継先の経路状態に合わせて最適な経路を選択できるポリシーベースルーティングをサポート

(7)　ネットワーク・パーティション対応

●ネットワークの水平統合・垂直統合によるコスト低減

- 論理的に分割された複数のスイッチを一つのスイッチ内に仮想的に収容する VRF 機能によって，従来物理的に分かれていた複数のネットワークを一つの物理ネットワーク内に統合
- センターにレイヤ 3 装置を集約, 各オフィスや拠点にはレイヤ 2 装置を配置することで, ネットワーク設計や運用管理の容易なネットワークを実現

(8)　ミッションクリティカル対応のネットワークを実現する高信頼性

●高い装置品質

- 厳選した部品と厳しい設計・検査基準による装置の高い信頼性
- キャリア／ISP で実績あるソフトウェアを継承した安定したルーティング処理

●電源冗長による単体装置としての高信頼化

●多様な冗長ネットワーク構築

- 高速な経路切り替え

  高速スパニングツリープロトコル（IEEE 802.1w，IEEE 802.1s），GSRP※1，Autonomous Extensible Ring Protocol※2（以降，Ring Protocol と呼びます。），リンクアグリゲーション（IEEE802.1AX），ホットスタンバイ（VRRP），スタティック／VRRP ポーリング※3 など
- ロードバランス

  OSPF イコールコストマルチパスによる IP レベルの均等トラフィック分散

注※1

GSRP（Gigabit Switch Redundancy Protocol）。詳細については,「コンフィグレーションガイド Vol.2」「13　GSRP の解説」を参照してください。

注※2

Ring Protocol の詳細については,「28　Ring Protocol の解説」を参照してください。

注※3

指定経路上の可達性をポーリングによって確認し，動的に VRRP やスタティックルーティングと連動して経路を切り替えるための監視機能。

(9)　柔軟な仮想ネットワークの VXLAN 機能をサポート

- 柔軟でスケーラブルな VXLAN ファブリックを，データセンター内で構築可能。
- データセンター間の L2 接続を延伸し，既設ネットワークを活用した BCP/DR（Business Continuity Plan/Disaster Recovery）対策を実現。

(10)　高速な冗長切り替えによって高信頼・高可用なシステムを実現

- Ring Protocol によって，50 ミリ秒以下の高速切り替えが可能。
- 独自のマルチコア CPU 最適化技術によって，高速な冗長切り替えを実現。

(11)　優れたネットワーク管理，保守・運用

- IPv4/v6 デュアルスタックや IPv6 環境に対応したネットワーク管理（SNMP over IPv6）など充実した機能

- 基本的な MIB-II に加え，IPv6 MIB，RMON などの豊富な MIB をサポート
- ミラーポート機能によって，トラフィックを監視，解析することが可能（受信側と送信側ポートの両方可能）
- テナント単位でトラフィックを監視するポリシーベースミラーリングに対応
- sFlow や sFlow-MIB によるトラフィック特性の分析が可能
- オンライン保守
  コンフィグレーションの変更などで部分リブートによる通信が継続可能。
- SD メモリカード採用
  - コンフィグレーションのバックアップや障害情報採取が容易に実行可能。
  - 保守作業の簡略化が可能。
- 全イーサネットポート，コンソールポート，マネージメントポート，メモリカードスロットを前面に配置
- イーサネット網の保守管理機能の CFM（Connectivity Fault Management）をサポート

(12)　省電力対応

●アーキテクチャ設計，部品選択の段階で低消費電力を志向。導入後の TCO（Total Cost of Ownership）の削減に寄与

2 装置構成

この章では，本装置の各モデル構成要素など，各装置本体について説明します。

2.1　本装置のモデル

本装置はボックス型イーサネットスイッチです。

最大ポート数ごとの対応モデルを次の表に示します。

表 2-1　最大ポート数ごとの対応モデル

最大ポート数による分類	対応モデル	
	電源固定式モデル	電源交換式モデル
10BASE-T/100BASE-TX/1000BASE-T　24 ポート 1000BASE-X　4 ポート 10GBASE-R　4 ポート 40GBASE-R　2 ポート（スタック専用）	IP8800/S3660-24T4X	IP8800/ S3660-24T4XW
10BASE-T/100BASE-TX/1000BASE-T　48 ポート 1000BASE-X　4 ポート 10GBASE-R　4 ポート 40GBASE-R　2 ポート（スタック専用）	－	IP8800/ S3660-48T4XW
10BASE-T/100BASE-TX/1000BASE-T　36 ポート 1000BASE-X　24 ポート 10GBASE-R　8 ポート 40GBASE-R　2 ポート（スタック専用）	－	IP8800/ S3660-16S4XW IP8800/ S3660-24S8XW
100BASE-TX/1000BASE-T/10GBASE-T　44 ポート 1000BASE-X　4 ポート 10GBASE-R　4 ポート 40GBASE-R　4 ポート 100GBASE-R　4 ポート	－	IP8800/ S3660-48XT4QW
10BASE-T/100BASE-TX/1000BASE-T　48 ポート 1000BASE-X　48 ポート 10GBASE-R　48 ポート 40GBASE-R　4 ポート 100GBASE-R　4 ポート	－	IP8800/ S3660-24X4QW IP8800/ S3660-48X4QW

（凡例）－：該当なし

2.2　収容回線数

各モデルの最大収容可能回線数を次に示します。

(1)　IP8800/S3660-24T4X, IP8800/S3660-24T4XW, および IP8800/S3660-48T4XW

IP8800/S3660-24T4X，IP8800/S3660-24T4XW，および IP8800/S3660-48T4XW には，次に示す種類のポートがあります。

- 10BASE-T/100BASE-TX/1000BASE-T ポート
- SFP+/SFP 共用ポート

  SFP+使用時は 10GBASE-R で，SFP 使用時は 1000BASE-X で使用できるポートです。なお，10GBASE-R は，アップリンク 10G に対応するソフトウェアライセンスまたはオプションライセンス使用時に利用できます。
- QSFP+ポート（スタック専用）

  QSFP+を使用する 40GBASE-R のポートで，スタックポートとしてだけ使用できます。以降，このポートをスタック専用ポートと呼びます。

ポートの種類と収容回線数を次の表に示します。

表 2–2　最大収容可能回線数（IP8800/S3660-24T4X，IP8800/S3660-24T4XW，および IP8800/S3660-48T4XW）

ポートの種類	IP8800/S3660-24T4X IP8800/ S3660-24T4XW	IP8800/ S3660-48T4XW
10BASE-T/100BASE-TX/1000BASE-T ポート	24	48
SFP+/SFP 共用ポート	4※	4※
QSFP+ポート（スタック専用）	2	2

注※

SFP+/SFP 共用ポートで SFP+を使用するには，オプションライセンス（アップリンク 10G）が必要です。

(2)　IP8800/S3660-16S4XW および IP8800/S3660-24S8XW

IP8800/S3660-16S4XW および IP8800/S3660-24S8XW には，次に示す種類のポートがあります。

- 10BASE-T/100BASE-TX/1000BASE-T ポート
- SFP ポート

  1000BASE-X で使用できるポートです。また，10BASE-T/100BASE-TX/1000BASE-T 用 SFP もサポートしていて，10BASE-T/100BASE-TX/1000BASE-T としても使用できるポートです。
- SFP+ポート

  10GBASE-R で使用できるポートです。
- QSFP+ポート（スタック専用）

  QSFP+を使用する 40GBASE-R のポートで，スタックポートとしてだけ使用できます。

ポートの種類と収容回線数を次の表に示します。

表 2-3　最大収容可能回線数（IP8800/S3660-16S4XW および IP8800/S3660-24S8XW）

ポートの種類	IP8800/S3660-16S4XW IP8800/S3660-24S8XW
10BASE-T/100BASE-TX/1000BASE-T ポート	12
SFP ポート	24※
SFP+ポート	8※
QSFP+ポート（スタック専用）	2

注※

IP8800/S3660-16S4XW の場合，オプションライセンス（ポート数拡張）が必要です。該当するオプションライセンスが設定されていない場合に使用できる SFP ポートおよび SFP+ポートは次のとおりです。

・SFP ポート：ポート 1～16 の 16 ポート

・SFP+ポート：ポート 37～40 の 4 ポート

(3)　IP8800/S3660-48XT4QW

IP8800/S3660-48XT4QW には，次に示す種類のポートがあります。

- 100BASE-TX/1000BASE-T/10GBASE-T ポート
- SFP+/SFP 共用ポート

  SFP+使用時は 10GBASE-R で，SFP 使用時は 1000BASE-X で使用できるポートです。
- QSFP28/QSFP+共用ポート

  QSFP28 使用時は 100GBASE-R で，QSFP+使用時は 40GBASE-R で使用できるポートです。スタックポートとしても使用できます。100GBASE-R 使用時，使用する回線数に応じて一部の 100BASE-TX/1000BASE-T/10GBASE-T ポートは無効になります。

ポートの種類と収容回線数を次の表に示します。

表 2-4　最大収容可能回線数（IP8800/S3660-48XT4QW）

ポートの種類	IP8800/S3660-48XT4QW
100BASE-TX/1000BASE-T/10GBASE-T ポート	44
SFP+/SFP 共用ポート	4
QSFP28/QSFP+共用ポート	4

QSFP28/QSFP+共用ポートを 100GBASE-R で使用する回線数と，その場合に使用できる 100BASE-TX/1000BASE-T/10GBASE-T ポート数の対応を次の表に示します。

表 2-5　100GBASE-R 使用回線数と 100BASE-TX/1000BASE-T/10GBASE-T ポート数の対応

QSFP28/QSFP+共用ポート		100BASE-TX/1000BASE-T/10GBASE-T ポート
100GBASE-R 回線数	40GBASE-R 回線数	
0	4	44
1	3	42
2	2	36／40

QSFP28/QSFP+共用ポート		100BASE-TX/1000BASE-T/10GBASE-T ポート
100GBASE-R 回線数	40GBASE-R 回線数	
3	1	34
4	0	28

なお，100GBASE-R で使用するポート番号をコンフィグレーションコマンド system interface hundredgigabitethernet で設定すると，100BASE-TX/1000BASE-T/10GBASE-T ポートのうち，いくつかのポートは無効になります。詳細は，「14.5　100GBASE-R の設定と 100BASE-TX/1000BASE-T/10GBASE-T ポートの排他変更」を参照してください。

(4)　IP8800/S3660-24X4QW および IP8800/S3660-48X4QW

IP8800/S3660-24X4QW および IP8800/S3660-48X4QW には，次に示す種類のポートがあります。

- SFP+/SFP 共用ポート

  SFP+使用時は 10GBASE-R で，SFP 使用時は 1000BASE-X で使用できるポートです。また，10BASE-T/100BASE-TX/1000BASE-T 用 SFP もサポートしており，10BASE-T/100BASE-TX/1000BASE-T としても使用できるポートです。
- QSFP28/QSFP+共用ポート

  QSFP28 使用時は 100GBASE-R で，QSFP+使用時は 40GBASE-R で使用できるポートです。スタックポートとしても使用できます。

ポートの種類と収容回線数を次の表に示します。

表 2-6　最大収容可能回線数（IP8800/S3660-24X4QW および IP8800/S3660-48X4QW）

ポートの種類	IP8800/S3660-24X4QW IP8800/S3660-48X4QW
SFP+/SFP 共用ポート	48※
QSFP28/QSFP+共用ポート	4

注※

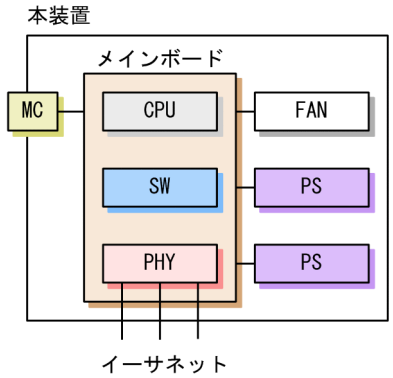
IP8800/S3660-24X4QW の場合，オプションライセンス（ポート数拡張）が必要です。該当するオプションライセンスが設定されていない場合に使用できる SFP+/SFP 共用ポートは，ポート 1～24 の 24 ポートです。

2.3　ハードウェア構成

本装置には，電源固定式モデルおよび電源交換式モデルがあります。電源固定式モデルは，PS が 2 台内蔵されており電源の冗長構成ができます。電源交換式モデルは，PS-A06/PS-A06R/PS-D06 を 2 台搭載することで電源の冗長構成ができます。

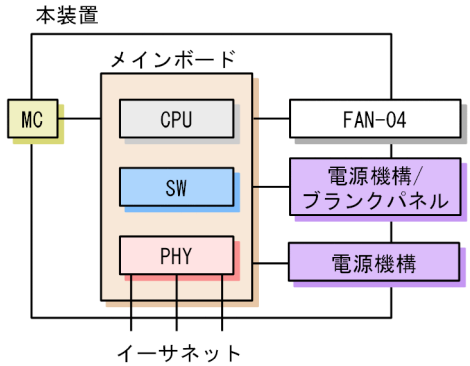
ハードウェアの構成を次の図に示します。

図 2-1　ハードウェアの構成（電源固定式モデル）



（凡例）MC：Memory Card
SW：SWitch processor
PHY：Physical Interface
PS：Power Supply

図 2-2　ハードウェアの構成（電源交換式モデル）



（凡例） MC：Memory Card
SW：SWitch processor
PHY：Physical Interface

(1)　装置筐体

装置筐体には，メインボード，電源，ファンが含まれています。電源固定式モデルは電源およびファンが内蔵されているタイプです。電源交換式モデルは電源およびファンを含む電源機構を搭載するタイプであり，電源機構およびファンユニットを取り外しできます。

(2)　メインボード

メインボードは CPU 部，SW 部，PHY 部から構成されます。

- CPU（Central Processing Unit）
  CPU を実装し，装置全体の管理，SW 部/PHY 部の制御，各種プロトコル処理をソフトウェアで行います。
  ソフトウェアは CPU 部に実装される装置内メモリに格納されます。
- MC（Memory Card）
  MC スロットです。MC を使用して，コンフィグレーションのバックアップ，およびダンプ情報の採取ができます。
- SW（Switch processor）
  L2 フレーム，L3（IPv4/IPv6）パケットのスイッチングを行います。SW 部はハードウェアによる MAC アドレス学習/エージング，リンクアグリゲーション，ルーティングテーブル検索，フィルタ/QoS テーブル検索，自宛/自発パケットの DMA 転送を行います。これによって IP フォワーディングを実現します。
- PHY（Physical Interface）
  各種メディア対応のインタフェース部です。

(3)　PS（Power Supply）

PS は電源固定式モデルに内蔵され，外部供給電源から本装置内で使用する直流電源を生成します。

また，PS は 2 台内蔵されており，電源冗長を構成できます。これによって，本装置の運用中に PS が故障しても装置を停止させることなく運用できます。冗長構成で運用する場合は，「14.1.5　電源固定式モデルでの電源の重度障害判定の設定」を参照してください。

なお，PS には電源スイッチ（ブレーカ）がありません。電源ケーブルを接続／抜去（取り付け／取り外し）することで，電源が ON／OFF の状態となります。

(4)　PS-A06/PS-A06R/PS-D06

PS-A06/PS-A06R※/PS-D06 は電源交換式モデルに搭載し，外部供給電源から本装置内で使用する直流電源を生成する電源機構です。電源機構は装置に最大 2 台搭載でき，冗長構成時には装置を停止することなく交換できます。電源機構を 1 台で運用する場合には，空きスロットにブランクパネルを搭載します。

また，電源機構は内部を冷却するための FAN を装備します。

なお，電源機構には電源スイッチ（ブレーカ）がありません。電源ケーブルを接続／抜去（取り付け／取り外し）することで電源が ON／OFF の状態となります。

注※　IP8800/S3660-48XT4QW では，PS-A06R は未サポートです。

(5)　FAN

FAN は電源固定式モデルに内蔵され，装置内部を冷却するファンです。

(6)　FAN-04/FAN-04R

FAN-04/FAN-04R※は電源交換式モデルに搭載し，装置内部を冷却するファンユニットです。ファンユニットはファンスロットに 1 台搭載します。ファンユニットは運用中に装置を停止することなく交換できます。

注※　IP8800/S3660-48XT4QW では，FAN-04R は未サポートです。

2.4　実装メモリ量

実装メモリ量および内蔵フラッシュメモリ量を次の表に示します。本装置では実装メモリおよび内蔵フラッシュメモリの増設はできません。

表 2-7　実装メモリ量と内蔵フラッシュメモリ量

項目	全モデル共通
実装メモリ量	4GB
内蔵フラッシュメモリ量	1GB

2.5　ソフトウェア

本装置は，L3 ライト機能および L3 アドバンス機能を主としたソフトウェアライセンスをサポートします。また，ソフトウェアライセンスにオプションライセンスを追加すると，スタック機能や高速な回線を使用できます。

L3 ライト機能および L3 アドバンス機能の内容と，本装置でサポートしているソフトウェアライセンスを次に示します。

表 2-8　L3 ライト機能および L3 アドバンス機能の内容

機能名	内容
L3 ライト機能	VLAN，スパニングツリー，RIP，マルチキャスト，SNMP，LLDP，Ring Protocol など，L3 スイッチとしての基本的な機能をサポート
L3 アドバンス機能	L3 ライト機能に加え，OSPF，BGP，VRF，ポリシーベースルーティング，VXLAN，および高速 Ring 切替（50 ミリ秒未満）をサポート

表 2-9　本装置のソフトウェアライセンス一覧

ソフトウェアライセンス略称	内容
SL-L3A-001	L3 アドバンス機能，スタック機能，アップリンク 10G
SL-L3A-002	L3 アドバンス機能，スタック機能
SL-L3A-003	L3 アドバンス機能，アップリンク 10G
SL-L3A-004	L3 アドバンス機能
SL-L3L-001	L3 ライト機能，スタック機能，アップリンク 10G
SL-L3L-002	L3 ライト機能，スタック機能
SL-L3L-003	L3 ライト機能，アップリンク 10G
SL-L3L-004	L3 ライト機能

本装置でサポートしているオプションライセンスを次の表に示します。

表 2-10　本装置のオプションライセンス一覧

オプションライセンス略称	内容
OP-ADV	L3 アドバンス機能 L3 ライト機能が動作している装置に本ライセンスを設定すると，L3 アドバンス機能が使用できます。
OP-STK	スタック機能
OP-ULTG	アップリンク 10G 次の装置に本ライセンスを設定すると，SFP+/SFP 共用ポートを 10Gbit/s（SFP+）で使用できます。 • IP8800/S3660-24T4X • IP8800/S3660-24T4XW • IP8800/S3660-48T4XW

オプションライセンス略称	内容
OP-SYNC	Sync-E 次の装置に本ライセンスを設定すると，Sync-E が使用できます。 • IP8800/S3660-24X4QW • IP8800/S3660-48X4QW
OP-PORT	ポート数拡張 次の装置に本ライセンスを設定すると，使用できるポートが拡張されます。 • IP8800/S3660-16S4XW SFP ポートのポート 17～24 および SFP+ポートのポート 41～44 が使用できます。 • IP8800/S3660-24X4QW SFP+/SFP 共用ポートのポート 25～48 が使用できます。

3 収容条件

この章では，収容条件について説明します。

3.1　テーブルエントリ数

本装置では，装置の適用形態に合わせ，モードの選択によってテーブルエントリ数の配分パターンを変更できます。モードには，IPv4 モード，IPv4/IPv6 モード，IPv6 ユニキャスト優先モード，および L2 優先モードの 4 種類があり，コンフィグレーションコマンド swrt_table_resource で設定します。

この節では，モードごとのテーブルエントリ数について説明します。

なお，マルチパス経路のエントリ数については，「コンフィグレーションガイド Vol.3」「表 8-5　マルチパス仕様」を参照してください。

モードごとの，装置当たりのテーブルエントリの最大数（最大装置エントリ数）を次の表に示します。

表 3-1　最大装置エントリ数

項目		最大装置エントリ数			
		IPv4 モード	IPv4/IPv6 モード	IPv6 ユニキャスト優先モード	L2 優先モード
IPv4	ユニキャスト経路	16285	8093	1023	8093
	マルチキャスト経路	8191	2048	128	1024
	ARP※1	30720※2	15360※2	7680※2	10240
IPv6	ユニキャスト経路	－	3007※3	6542※4	3007※3
	マルチキャスト経路	－	1024	1024	128
	NDP※1	－	15360※2	23040※2	1536
L2	MAC アドレステーブル	81920※5			212992※5

（凡例）－：該当なし

注※1

エクストラネット使用時に他 VRF からインポートされた直結経路で通信が発生すると，該当する通信で使用する ARP エントリおよび NDP エントリがインポート先の VRF にも生成されます。インポート先の VRF に生成された ARP エントリおよび NDP エントリは，通常の ARP エントリおよび NDP エントリと同様に 1 エントリ分のリソースを消費します。【SL-L3A】

注※2

VXLAN 機能有効時は収容条件が変わります。詳細は「表 3-2　最大ダイナミックエントリ数および最大スタティックエントリ数」～「表 3-4　最大ダイナミックエントリ数および最大スタティックエントリ数」を参照してください。

注※3

プレフィックス長が 64 以下のユニキャスト経路は 1983 まで登録できます。

注※4

プレフィックス長が 64 以下のユニキャスト経路は 5518 まで登録できます。

注※5

ハードウェアの制限によって，収容条件の最大数まで登録できないことがあります。

モードごとの，ダイナミックエントリとスタティックエントリの最大数（最大ダイナミックエントリ数および最大スタティックエントリ数）を次に示します。ダイナミックエントリとスタティックエントリの合計値が，最大装置エントリ数を超えないようにしてください。

3.1.1　IPv4 モード

IPv4 モードを使用する場合の最大ダイナミックエントリ数および最大スタティックエントリ数を次の表に示します。なお，括弧内の値は VXLAN 機能有効時の収容条件です。

表 3-2　最大ダイナミックエントリ数および最大スタティックエントリ数

分類	項目	最大装置エントリ数	最大ダイナミックエントリ数		最大スタティックエントリ数
			スタンドアロン時	スタック時	
IPv4	ユニキャスト経路エントリ	16285	16285	16285	2048
	マルチキャスト経路エントリ	8191	8191	8191	－
	ARP	30720 （14336）	30720 （14336）	13000	4096

（凡例）－：未サポート

3.1.2　IPv4/IPv6 モード

IPv4/IPv6 モードを使用する場合の最大ダイナミックエントリ数および最大スタティックエントリ数を次の表に示します。なお，括弧内の値は VXLAN 機能有効時の収容条件です。

表 3-3　最大ダイナミックエントリ数および最大スタティックエントリ数

分類	項目	最大装置エントリ数	最大ダイナミックエントリ数		最大スタティックエントリ数
			スタンドアロン時	スタック時	
IPv4	ユニキャスト経路エントリ	8093	8093	8093	2048※
	マルチキャスト経路エントリ	2048	2048	2048	－
	ARP	15360 （7168）	15360 （7168）	7000	4096
IPv6	ユニキャスト経路エントリ	3007	3007	3007	2048※
	マルチキャスト経路エントリ	1024	1024	－	－
	NDP	15360 （7168）	15360 （7168）	7000	128

（凡例）－：未サポート

注※

IPv4 と IPv6 の合計は 2048 以内としてください。

3.1.3　IPv6 ユニキャスト優先モード

IPv6 ユニキャスト優先モードを使用する場合の最大ダイナミックエントリ数および最大スタティックエントリ数を次の表に示します。なお，括弧内の値は VXLAN 機能有効時の収容条件です。

表 3-4　最大ダイナミックエントリ数および最大スタティックエントリ数

分類	項目	最大装置エントリ数	最大ダイナミックエントリ数		最大スタティックエントリ数
			スタンドアロン時	スタック時	
IPv4	ユニキャスト経路エントリ	1023	1023	1023	1023※
	マルチキャスト経路エントリ	128	128	128	－
	ARP	7680 (3564)	7680 (3564)	3000	128
IPv6	ユニキャスト経路エントリ	6542	6542	6542	2048※
	マルチキャスト経路エントリ	1024	1024	－	－
	NDP	23040 (10752)	23040 (10752)	9000	128

（凡例）－：未サポート

注※

IPv4 と IPv6 の合計は 2048 以内としてください。

3.1.4　L2 優先モード

L2 優先モードを使用する場合の最大ダイナミックエントリ数および最大スタティックエントリ数を次の表に示します。

表 3-5　最大ダイナミックエントリ数および最大スタティックエントリ数

分類	項目	最大装置エントリ数	最大ダイナミックエントリ数		最大スタティックエントリ数
			スタンドアロン時	スタック時	
IPv4	ユニキャスト経路エントリ	8093	8093	8093	2048※
	マルチキャスト経路エントリ	1024	1024	1024	－
	ARP	10240	10240	10240	4096
IPv6	ユニキャスト経路エントリ	3007	3007	3007	2048※
	マルチキャスト経路エントリ	128	128	－	－
	NDP	1536	1536	1536	128

（凡例）－：未サポート

注※
　IPv4 と IPv6 の合計は 2048 以内としてください。

3.2　リモートアクセス

本装置へのリモートアクセスでの収容条件を示します。

(1)　リモートログインできるユーザ数

telnet や ssh によって本装置へリモートログインできるユーザの最大数は，コンフィグレーションコマンド line vty で設定する，ログインできるユーザ数です。なお，line vty コマンドで設定できるログインできるユーザ数は，最大で 16 です。

(2)　本装置へのユーザ公開鍵の登録

SSH によって本装置へ接続するユーザが公開鍵認証を使用する場合は，ユーザ名と，該当ユーザのユーザ公開鍵を登録してください。公開鍵認証を使用する場合に登録できるユーザ数およびユーザ公開鍵数を次の表に示します。

表 3-6　登録できるユーザ数およびユーザ公開鍵数

項目	最大数
登録できる公開鍵認証ユーザ数	20 ユーザ／装置
登録できるユーザ公開鍵数	10 個／ユーザ

3.3　リンクアグリゲーション

コンフィグレーションによって設定できるリンクアグリゲーションの収容条件を次の表に示します。

表 3-7　リンクアグリゲーションの収容条件

モデル	チャネルグループ当たりの 最大ポート数	装置当たりの 最大チャネルグループ
全モデル共通	8	48（スタンドアロン時）
		96（スタック時）

3.4　レイヤ 2 スイッチ

3.4.1　MAC アドレステーブル

L2 スイッチ機能では，接続されたホストの MAC アドレスをダイナミックに学習して MAC アドレステーブルへ登録します。また，スタティックに MAC アドレステーブルへ登録することもできます。

MAC アドレステーブルに登録できる MAC アドレスのエントリの最大数を次の表に示します。

表 3-8　MAC アドレステーブルに登録できる MAC アドレスのエントリ数

テーブルエントリ数の配分パターン	装置当たり	
	最大エントリ数	スタティックエントリ数
IPv4 モード IPv4/IPv6 モード IPv6 ユニキャスト優先モード	81920※	2048
L2 優先モード	212992※	

注※

ハードウェアの制限によって，収容条件の最大数まで登録できないことがあります。

MAC アドレスが収容条件を超えた場合，学習済みエントリがエージングされるまで新たな MAC アドレス学習は行われません。したがって，未学習の MAC アドレス宛てのパケットは該当する VLAN ドメイン内でフラッディングされます。

また，本装置では，MAC アドレステーブルのエントリの数をコンフィグレーションによって変更することはできません。

3.4.2　VLAN

コンフィグレーションによって設定できる VLAN の数を次の表に示します。

表 3-9　VLAN のサポート数

モデル	ポート当たり VLAN	装置当たり VLAN	ポートごと VLAN 数の装置での合計	
			スタンドアロン時	スタック時
IP8800/S3660-24T4X	4094※1	4094※1	28672	10000
IP8800/S3660-24T4XW			28672	10000
IP8800/S3660-48T4XW			53248	10000
IP8800/S3660-16S4XW			32768※2	10000
IP8800/S3660-24S8XW			45056	10000
IP8800/S3660-48XT4QW			53248	10000
IP8800/S3660-24X4QW			28672※3	10000

モデル	ポート当たり VLAN	装置当たり VLAN	ポートごと VLAN 数の装置での合計	
			スタンドアロン時	スタック時
IP8800/S3660-48X4QW			53248	10000

注※1
　スタック構成時に設定できる VLAN の数は 4093 です。

注※2
　オプションライセンス（ポート数拡張）を設定した場合，収容数は IP8800/S3660-24S8XW と同じになります。

注※3
　オプションライセンス（ポート数拡張）を設定した場合，収容数は IP8800/S3660-48X4QW と同じになります。

なお，推奨する VLAN 数は 1024 以下です。スタックを構成する場合，推奨する VLAN 数は 1024 をスタックの構成台数で割った数以下（2 台構成のときは 512 以下）です。

ポートごと VLAN 数の装置での合計は，ポートに設定している VLAN の数を，装置の全ポートで合計した値です。例えば，24 ポートの装置で，ポート 1 からポート 10 では設定している VLAN 数が 2000，ポート 11 からポート 24 では設定している VLAN 数が 1 の場合，ポートごと VLAN 数の装置での合計は 20014 となります。なお，チャネルグループに所属するポートでも，チャネルグループでまとめるのではなく，ポートに設定している VLAN の数で計算されます。ポートごと VLAN 数の装置での合計が収容条件を超えた場合，CPU の利用率が高くなり，コンフィグレーションコマンドや運用コマンドのレスポンスが遅くなったり，実行できなくなったりすることがあります。スタックを構成する場合でも，ポートごと VLAN 数の装置での合計は，構成台数に関係なくスタック全体で装置単体のサポート数と同じになります。

(1)　プロトコル VLAN

プロトコル VLAN では，イーサネットフレーム内の Ethernet-Type，LLC SAP，および SNAP type フィールドの値を基にプロトコルの識別を行います。コンフィグレーションによって設定できるプロトコル VLAN の収容条件を次の表に示します。

表 3-10　プロトコル VLAN のプロトコルの種類数

モデル	ポート当たり	装置当たり
全モデル共通	16	16

表 3-11　プロトコル VLAN 数

モデル	ポート当たり	装置当たり
全モデル共通	100※	100

注※　トランクポートに設定できるプロトコル VLAN 数。プロトコルポートに設定できるプロトコル VLAN 数は 16 です。

(2)　MAC VLAN

MAC VLAN の収容条件を次の表に示します。

表 3-12　MAC VLAN の登録 MAC アドレス数

モデル	コンフィグレーションによる最大登録 MAC アドレス数	L2 認証機能による最大登録 MAC アドレス数	同時登録最大 MAC アドレス数
IP8800/S3660-24T4X	1024	1024	2048
IP8800/S3660-24T4XW			
IP8800/S3660-48T4XW			
IP8800/S3660-16S4XW			
IP8800/S3660-24S8XW			
IP8800/S3660-48XT4QW	1024	1024	1024
IP8800/S3660-24X4QW			
IP8800/S3660-48X4QW			

なお，コンフィグレーションコマンド mac-based-vlan static-only が設定された場合は，次の表に示す収容条件となります。

表 3-13　mac-based-vlan static-only 設定時の登録 MAC アドレス数

モデル	コンフィグレーションによる最大登録 MAC アドレス数	L2 認証機能による最大登録 MAC アドレス数
全モデル共通	1024	0

(3)　VLAN トンネリング

コンフィグレーションによって設定できる VLAN トンネリングの数を次の表に示します。

表 3-14　VLAN トンネリングの数

モデル	装置当たり
全モデル共通	4094※

注※　スタック構成時に設定できる VLAN トンネリングの数は 4093 です。

(4)　Tag 変換

コンフィグレーションによって設定できる Tag 変換情報エントリ数を次の表に示します。Tag 変換をチャネルグループに設定した場合は，チャネルグループに所属するポートごとにエントリを消費します。

表 3-15　Tag 変換情報エントリ数

モデル	装置当たり
全モデル共通	768

(5)　VLAN ごとの MAC アドレス

コンフィグレーションによって VLAN インタフェースに設定する MAC アドレス（レイヤ 3 通信で使用する VLAN ごとの MAC アドレス）の装置当たりの数を次の表に示します。

表 3-16　VLAN インタフェースの MAC アドレス数

モデル	装置当たり
全モデル共通	128

3.4.3　VXLAN【SL-L3A】

VXLAN の収容条件を次の表に示します。

表 3-17　VXLAN の収容条件

項目	最大数
VTEP 数	255／装置
VNI 数※1	6000／装置
サブインタフェース数※2	8191／装置
VNI マッピングエントリ数※3	8192／装置
トンネルインタフェース数（宛先）	256／装置
トンネルインタフェース数（送信元）	1／VTEP
VXLAN Network ポートがリンクアグリゲーション構成時の Nexthop 数※4	160／装置

注※1

VTEP に所属する VNI 数の総和です。

注※2

VNI マッピング方式がサブインタフェースマッピングの場合，サブインタフェースごとに 1 と数えます。

VNI マッピング方式が VLAN マッピングで，コンフィグレーションコマンド vxlan vlan-mapping mode extended を設定しない場合は，VXLAN を使用する VLAN を設定したポート数の合計をサブインタフェース数として数えます。コンフィグレーションコマンド vxlan vlan-mapping mode extended を設定した場合は，サブインタフェース数に数えません。

注※3

VLAN マッピングで VNI を割り当てた VLAN に所属するポート数と，サブインタフェースマッピングで VNI を割り当てたサブインタフェース数の総和です。

注※4

VXLAN Network ポートをリンクアグリゲーション構成としているチャネルグループに対する Nexthop 数の総和です。チャネルグループでマルチパス経路を構成している場合は，その経路数の掛け算でエントリが消費されます。

3.4.4　スパニングツリー

スパニングツリーの収容条件を種類ごとに次の表に示します。

なお，スパニングツリーの VLAN ポート数は，スパニングツリーが動作する VLAN に所属するポート数の延べ数です。チャネルグループの場合，チャネルグループ当たりの物理ポート数を数えます。ただし，次の VLAN やポートは，VLAN ポート数に含めません。

- コンフィグレーションコマンド state で suspend パラメータが設定されている VLAN
- VLAN トンネリングを設定しているポート
- BPDU ガード機能を設定しているが，BPDU フィルタ機能を設定していないポート

- PortFast 機能と BPDU フィルタ機能を設定しているアクセスポート

表 3-18　PVST+の収容条件

モデル	Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数※1
全モデル共通	共存なし	250	256※2
	共存あり	128	200※2

注※1

スパニングツリー対象となる各 VLAN に設定するポート数の合計（VLAN 数とポート数の積）。

例えば，100 個の VLAN を設定し，それぞれの VLAN に 2 回線が所属している場合，ポート数は 100×2 ＝ 200 となります。

VLAN トンネリングとの併用時，アクセスポートはポート数に含みません。

注※2

PortFast 機能を設定したポート数は含めません。

表 3-19　シングルスパニングツリーの収容条件

モデル	Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数※1	VLAN ポート数※1 (PVST+併用時※2)
全モデル共通	共存なし	1024※3	5000	1000
	共存あり	1024※3	4000	800

注※1

スパニングツリー対象となる各 VLAN に設定するポート数の合計（VLAN 数とポート数の積）。

例えば，100 個の VLAN を設定し，それぞれの VLAN に 2 回線が所属している場合，ポート数は 100×2 ＝ 200 となります。

VLAN トンネリングとの併用時，アクセスポートはポート数に含みません。

注※2

PVST+の対象ポート含み合計の最大値が 1000 となります。

注※3

PVST+同時動作時は PVST+対象 VLAN 数を引いた値となります。

表 3-20　マルチプルスパニングツリーの収容条件

モデル	Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数※1	MST インスタンス数	MST インスタンスごとの対象 VLAN 数※2
全モデル共通	共存なし	1024	5000	16	50
	共存あり	1024	4000	16	50

注※1

スパニングツリー対象となる各 VLAN に設定するポート数の合計（VLAN 数とポート数の積）。

例えば，100 個の VLAN を設定し，それぞれの VLAN に 2 回線が所属している場合，ポート数は 100×2 ＝ 200 となります。

VLAN トンネリングとの併用時，アクセスポートはポート数に含みません。

注※2

MST インスタンス 0 は除きます。MST インスタンス 0 の対象 VLAN 数は 1024 となります。なお，運用中は運用コマンド show spanning-tree port-count で対象 VLAN 数と VLAN ポート数を確認できます。

3.4.5　Ring Protocol

(1)　Ring Protocol

Ring Protocol の収容条件を次の表に示します。

表 3-21　Ring Protocol の収容条件

項目	リング当たり	装置当たり
リング数	－	24※1
VLAN マッピング数	－	128
VLAN グループ数	2	48※2
VLAN グループの VLAN 数	1023※3※4	1023※3※4
リングポート数※5	2	48※2

（凡例）－：該当なし

注※1

Ring Protocol とスパニングツリーの併用，Ring Protocol と GSRP の併用，または多重障害監視機能を使用する場合は，8 となります。

注※2

Ring Protocol とスパニングツリーの併用，Ring Protocol と GSRP の併用，または多重障害監視機能を使用する場合は，16 となります。

注※3

装置として推奨する VLAN の最大数です。

リング当たりに制御 VLAN 用として VLAN を一つ消費するため，VLAN グループに使用できる VLAN の最大数は 1023 となります。ただし，リング数が増加するに従い，VLAN グループに使用できる VLAN の最大数は減少します。

注※4

多重障害監視機能は，多重障害監視 VLAN 用としてリング当たり VLAN を一つ消費するため，VLAN グループに使用できる VLAN の最大数は減少します。

注※5

チャネルグループの場合は，チャネルグループ単位で 1 ポートと数えます。

(2)　仮想リンク

仮想リンクの収容条件を次の表に示します。

表 3-22　仮想リンクの収容条件

項目	最大数
装置当たりの仮想リンク ID 数	1
仮想リンク当たりの VLAN 数	1
拠点当たりのリングノード数	2
ネットワーク全体での仮想リンクの拠点数	250

(3)　多重障害監視機能

多重障害監視機能の収容条件を次の表に示します。

表 3-23　多重障害監視機能の収容条件

項目	最大数
装置当たりの多重障害監視可能リング数	4
リング当たりの多重障害監視 VLAN 数	1
装置当たりの多重障害監視 VLAN 数	4

3.4.6　IGMP snooping/MLD snooping

IGMP snooping の収容条件を次の表に示します。

表 3-24　IGMP snooping の収容条件

項目	最大数
設定 VLAN 数	64
VLAN ポート数※1	512
登録エントリ数※2※3	1024
IP アドレス数×ポート数※4	1024

注※1

IGMP snooping が動作するポート数（IGMP snooping を設定した VLAN に収容されるポートの総和）です。例えば，各々 10 ポート収容している 16 個の VLAN で IGMP snooping を動作させる場合，IGMP snooping 動作ポート数は 160 となります。

注※2

登録エントリ数の最大数には，ルーティングプロトコルなどで使用する制御パケットのマルチキャストアドレスも含みます。該当するエントリは，制御パケットに対するグループ参加要求を受信した場合に登録します。VLAN 内で複数のルーティングプロトコルを同時に使用する場合，該当するプロトコルの制御パケットが使用するマルチキャストアドレス分だけエントリを使用します。

注※3

IPv4 マルチキャストまたは IPv6 マルチキャストと同時に使用しない場合は，各 VLAN で学習したマルチキャスト MAC アドレスの総和です。IPv4 マルチキャストまたは IPv6 マルチキャストと同時に使用する場合は，各 VLAN で学習したマルチキャスト IP アドレスの総和です。

注※4

VLAN インタフェースに設定された IP アドレス数×VLAN に収容されるポート数の総和です。例えば，16 個の VLAN にセカンダリアドレス 1 個（IP アドレス計 2 個）を設定して，各 VLAN が 10 ポート収容している場合，ポート数は 320 となります。

MLD snooping の収容条件を次の表に示します。

表 3-25　MLD snooping の収容条件

項目	最大数
設定 VLAN 数	32

項目	最大数
VLAN ポート数※1	512
登録エントリ数※2※3	500

注※1

MLD snooping が動作するポート数（MLD snooping を設定した VLAN に収容されるポートの総和）です。例えば，各々 10 ポート収容している 16 個の VLAN で MLD snooping を動作させる場合，MLD snooping 動作ポート数は 160 となります。

注※2

登録エントリ数の最大数には，ルーティングプロトコルなどで使用する制御パケットのマルチキャストアドレスも含みます。該当するエントリは, 制御パケットに対するグループ参加要求を受信した場合に登録します。VLAN 内で複数のルーティングプロトコルを同時に使用する場合，該当するプロトコルの制御パケットが使用するマルチキャストアドレス分だけエントリを使用します。

注※3

IPv6 マルチキャストと同時に使用しない場合は，各 VLAN で学習したマルチキャスト MAC アドレスの総和です。IPv6 マルチキャストと同時に使用する場合は，各 VLAN で学習したマルチキャスト IP アドレスの総和です。

3.5　フィルタ・QoS・ポリシーベースミラーリング

フィルタ・QoS・ポリシーベースミラーリングの検出条件はコンフィグレーション（access-list，qos-flow-list）で設定します。ここでは，設定したリストを装置内部で使用する形式（エントリ）に変換したエントリ数の上限をフィルタ・QoS・ポリシーベースミラーリングの収容条件として示します。

フィルタ・QoS・ポリシーベースミラーリングの検出条件によるリソース配分を決定するために，フィルタ，QoS，およびポリシーベースミラーリングの共通モードであるフロー検出モードを選択します。フロー検出モードは，受信側および送信側について，それぞれ対応する次のコンフィグレーションコマンドで設定します。選択するモードによって，エントリ数の上限値を決定する条件が異なります。

- コンフィグレーションコマンド flow detection mode：受信側フロー検出モードの設定
- コンフィグレーションコマンド flow detection out mode：送信側フロー検出モードの設定

受信側はフィルタ，QoS，およびポリシーベースミラーリングを，送信側はフィルタをサポートしています。なお，受信側のエントリ数については「3.5.1　受信側フィルタエントリ数」，「3.5.2　受信側 QoS エントリ数」，または「3.5.3　受信側ポリシーベースミラーリングエントリ数」を，送信側のエントリ数については「3.5.5　送信側フィルタエントリ数」を参照してください。

3.5.1　受信側フィルタエントリ数

受信側フロー検出モードごとの，装置当たりに設定できる受信側フィルタ最大エントリ数を次の表に示します。

表 3-26　受信側フィルタ最大エントリ数

受信側フロー検出モード	受信側フィルタ最大エントリ数※1※2		
	MAC 条件	IPv4 条件	IPv6 条件
layer3-1	2048×n	2048×n	−
layer3-2	−	4096×n	−
layer3-6	−	2048×n	1024×n
layer3-dhcp-1	−	1024	−
layer3-mirror-1	1024×n	2048×n	−
layer3-mirror-2	−	4096×n	−
layer3-mirror-3	−	1024×n	512×n
layer3-mirror-4	−	1024×n	512×n
layer3-mirror-5	−	1024×n	1024×n
layer3-suppress-1	1024×n	2048×n	−
layer3-suppress-2	−	1024×n	1024×n
layer3-suppress-dhcp-1	−	1024	−
layer3-suppress-mirror-1	1024×n	1024×n	−
layer3-suppress-mirror-2	−	1024×n	1024×n

受信側フロー検出モード	受信側フィルタ最大エントリ数※1※2		
	MAC 条件	IPv4 条件	IPv6 条件
custom	0～6144×n※3	0～6144×n※3	0～3072×n※3

（凡例）－：該当なし　n：メンバスイッチの台数

注※1

フィルタエントリ追加時，該当イーサネットインタフェースまたは VLAN インタフェースに対してフロー未検出時に動作するエントリ（廃棄動作）を自動的に付与します。このため，フィルタ最大エントリ数のすべてを使用できません。フィルタエントリの数え方の例を次に示します。

（例 1）

エントリ条件：イーサネットインタフェース 1/0/1 に 1 エントリ設定

エントリ数　：設定エントリ(1)とイーサネットインタフェース 1/0/1 の廃棄エントリ(1)の合計 2 エントリを使用する

残エントリ数：受信側フィルタ最大エントリ数－エントリ数

（例 2）

エントリ条件：イーサネットインタフェース 1/0/1 に 2 エントリ，VLAN10 のインタフェースに 3 エントリ設定

エントリ数　：設定エントリ(5)とイーサネットインタフェース 1/0/1 の廃棄エントリ(1)および VLAN10 のインタフェースの廃棄エントリ(1)の合計 7 エントリを使用する

残エントリ数：受信側フィルタ最大エントリ数－エントリ数

注※2

スタック構成時はメンバスイッチの台数に応じて収容条件が増加します。ただし，VLAN インタフェースの収容条件は変わりません。

また，スタンドアロン時は n が 1 となります。

注※3

受信側フィルタの最大エントリ数は，エントリブロックに機能を指定しなかった場合の 0 エントリから，すべてのエントリブロックに同じフロー検出条件（MAC 条件，IPv4 条件，IPv6 条件）の受信側フィルタを指定した場合の最大エントリ数までとなります。

3.5.2　受信側 QoS エントリ数

受信側フロー検出モードごとの，装置当たりに設定できる受信側 QoS 最大エントリ数を次の表に示します。

表 3-27　受信側 QoS 最大エントリ数

受信側フロー検出モード	受信側 QoS 最大エントリ数※1		
	MAC 条件	IPv4 条件	IPv6 条件
layer3-1	512×n	512×n	－
layer3-2	－	1024×n	－
layer3-6	－	512×n	512×n
layer3-dhcp-1	－	512	－
layer3-mirror-1	512×n	512×n	－
layer3-mirror-2	－	768×n	－
layer3-mirror-3	－	512×n	512×n

受信側フロー検出モード	受信側 QoS 最大エントリ数※1		
	MAC 条件	IPv4 条件	IPv6 条件
layer3-mirror-4	－	512×n	512×n
layer3-mirror-5	－	512×n	－
layer3-suppress-1	512×n	512×n	－
layer3-suppress-2	－	512×n	512×n
layer3-suppress-dhcp-1	－	512	－
layer3-suppress-mirror-1	512×n	512×n	－
layer3-suppress-mirror-2	－	－	－
custom	0～3072×n※2	0～3072×n※2	0～3072×n※2

（凡例）－：該当なし　n：メンバスイッチの台数

注※1

スタック構成時はメンバスイッチの台数に応じて収容条件が増加します。ただし，VLAN インタフェースの収容条件は変わりません。

また，スタンドアロン時は n が 1 となります。

注※2

受信側 QoS の最大エントリ数は，エントリブロックに機能を指定しなかった場合の 0 エントリから，すべてのエントリブロックに同じフロー検出条件（MAC 条件，IPv4 条件，IPv6 条件）の受信側 QoS を指定した場合の最大エントリ数までとなります。

3.5.3　受信側ポリシーベースミラーリングエントリ数

受信側フロー検出モードごとの，装置当たりに設定できる受信側ポリシーベースミラーリング最大エントリ数を次の表に示します。

表 3-28　受信側ポリシーベースミラーリング最大エントリ数

受信側フロー検出モード	受信側ポリシーベースミラーリング最大エントリ数※1		
	MAC 条件	IPv4 条件	IPv6 条件
layer3-1	－	－	－
layer3-2	－	－	－
layer3-6	－	－	－
layer3-dhcp-1	－	－	－
layer3-mirror-1	512×n	512×n	－
layer3-mirror-2	－	512×n	－
layer3-mirror-3	512×n	512×n	－
layer3-mirror-4	－	－	512×n
layer3-mirror-5	512×n	512×n	512×n

受信側フロー検出モード	受信側ポリシーベースミラーリング最大エントリ数※1		
	MAC 条件	IPv4 条件	IPv6 条件
layer3-suppress-1	－	－	－
layer3-suppress-2	－	－	－
layer3-suppress-dhcp-1	－	－	－
layer3-suppress-mirror-1	512×n	512×n	－
layer3-suppress-mirror-2	－	512×n	512×n
custom	0～6144×n※2	0～6144×n※2	0～3072×n※2

（凡例）－：該当なし　n：メンバスイッチの台数

注※1

スタック構成時はメンバスイッチの台数に応じて収容条件が増加します。ただし，VLAN インタフェースの収容条件は変わりません。

また，スタンドアロン時は n が 1 となります。

注※2

受信側ポリシーベースミラーリングの最大エントリ数は，エントリブロックに機能を指定しなかった場合の 0 エントリから，すべてのエントリブロックに同じフロー検出条件（MAC 条件，IPv4 条件，IPv6 条件）の受信側ポリシーベースミラーリングを指定した場合の最大エントリ数までとなります。

3.5.4　custom 指定時のエントリ分配

受信側フロー検出モード custom は，ハードウェアテーブルのエントリブロック単位で次に示す機能を選択できるフロー検出モードです。

- フィルタ
- QoS
- ポリシーベースミラーリング
- DHCP snooping の端末フィルタ

エントリブロックには 8 個（1 番～8 番）のエリアがあり，エントリブロックに割り当てる機能ごとに，使用できるエントリ数が決まります。複数のエントリブロックに同じ機能を割り当てる場合，連続した番号のエントリブロックだけを選択できます。その場合，該当エントリブロックで使用できるエントリ数の総和が，その機能の収容条件となります。

エントリブロックに割り当てられる受信側フロー検出の機能と，各機能を割り当てた場合に使用できるエントリ数を次の表に示します。

表 3-29　受信側フロー検出の機能とエントリブロックごとのエントリ数

機能	受信側フロー検出条件（コンフィグレーション指定値）	エントリブロック番号							
		1	2	3	4	5※1	6※1	7	8
フィルタ	MAC 条件（mac-filter）	1024	1024	1024	1024	512	512	512	512
	IPv4 条件	1024	1024	1024	1024	512	512	512	512

機能	受信側フロー検出条件（コンフィグレーション指定値）	エントリブロック番号							
		1	2	3	4	5※1	6※1	7	8
	（ip-filter）								
	IPv6 条件※2（ipv6-filter）	1024		1024		512		512	
QoS	MAC 条件（mac-qos）	512	512	512	512	256	256	256	256
	IPv4 条件（ip-qos）	512	512	512	512	256	256	256	256
	IPv6 条件※2（ipv6-qos）	1024		1024		512		512	
ポリシーベースミラーリング	MAC 条件（mac-pbm）	1024	1024	1024	1024	512	512	512	512
	IPv4 条件（ip-pbm）	1024	1024	1024	1024	512	512	512	512
	IPv6 条件※2（ipv6-pbm）	1024		1024		512		512	
DHCP snooping	端末フィルタ※3（dhcp-filter）	1024	1024	1024	1024	512	512	512	512

注※1

IP 未設定 VLAN 抑止モードを併用した場合，エントリブロック 5 番および 6 番には機能を割り当てられません。IP 未設定 VLAN 抑止モードについては，「コンフィグレーションガイド Vol.2」「1.1.3　受信側フロー検出モード」を参照してください。

注※2

IPv6 条件のフィルタ，QoS，およびポリシーベースミラーリングは，一つの機能で二つのエントリブロックを使用します。

注※3

DHCP snooping の端末フィルタは，割り当てたエントリブロックのエントリ数の総和－2 が収容条件となります。また，バインディングデータベースの最大エントリ数を超えて割り当てたエントリブロックのエントリは，未使用エントリとなります。

3.5.5　送信側フィルタエントリ数

送信側フロー検出モードごとの，装置当たりに設定できる送信側フィルタ最大エントリ数を次の表に示します。

表 3-30　送信側フィルタ最大エントリ数

送信側フロー検出モード	送信側フィルタ最大エントリ数※1※2		
	MAC 条件	IPv4 条件	IPv6 条件
layer3-1-out	－	1024×n	－

送信側フロー検出モード	送信側フィルタ最大エントリ数※1※2		
	MAC 条件	IPv4 条件	IPv6 条件
layer3-2-out	256×n	256×n	256×n

（凡例）－：該当なし　n：メンバスイッチの台数

注※1

フィルタエントリ追加時，該当イーサネットインタフェースまたは VLAN インタフェースに対してフロー未検出時に動作するエントリ（廃棄動作）を自動的に付与します。このため，フィルタ最大エントリ数のすべてを使用できません。フィルタエントリの数え方の例を次に示します。

（例 1）

エントリ条件：イーサネットインタフェース 1/0/1 に 1 エントリ設定

エントリ数　：設定エントリ(1)とイーサネットインタフェース 1/0/1 の廃棄エントリ(1)の合計 2 エントリを使用する

残エントリ数：送信側フィルタ最大エントリ数－エントリ数

（例 2）

エントリ条件：イーサネットインタフェース 1/0/1 に 2 エントリ，VLAN10 のインタフェースに 3 エントリ設定

エントリ数　：設定エントリ(5)とイーサネットインタフェース 1/0/1 の廃棄エントリ(1)および VLAN10 のインタフェースの廃棄エントリ(1)の合計 7 エントリを使用する

残エントリ数：送信側フィルタ最大エントリ数－エントリ数

注※2

スタック構成時はメンバスイッチの台数に応じて収容条件が増加します。ただし，VLAN インタフェースの収容条件は変わりません。

また，スタンドアロン時は n が 1 となります。

3.5.6　TCP/UDP ポート番号検出パターン数

フィルタ・QoS のフロー検出条件での TCP/UDP ポート番号検出パターンの収容条件を次の表に示します。TCP/UDP ポート番号検出パターンは，フロー検出条件のポート番号指定で使用されるハードウェアリソースです。

表 3-31　TCP/UDP ポート番号検出パターン収容条件

モデル	装置当たりの最大数
全モデル共通	32※1×n※2

（凡例）n：メンバスイッチの台数

注※1

VXLAN PMTU 機能を有効にすると，ハードウェアリソースを一つ消費します。

注※2

スタック構成時はメンバスイッチの台数に応じて収容条件が増加します。

次の表に示すフロー検出条件の指定で，TCP/UDP ポート番号検出パターンを使用します。なお，アクセスリスト（access-list）および QoS フローリスト（qos-flow-list）の作成だけでは TCP/UDP ポート番号検出パターンを使用しません。作成したアクセスリストおよび QoS フローリストを次に示すコンフィグレーションでインタフェースに適用したときに TCP/UDP ポート番号検出パターンを使用します。

- ip access-group
- ipv6 traffic-filter

- ip qos-flow-group
- ipv6 qos-flow-group

表 3-32　TCP/UDP ポート番号検出パターンを使用するフロー検出条件パラメータ

フロー検出条件のパラメータ	指定方法	受信側フロー検出モード	送信側フロー検出モード
		全モード共通	全モード共通
送信元ポート番号	単一指定(eq)	−	−
	範囲指定(range)	○	指定不可
宛先ポート番号	単一指定(eq)	−	−
	範囲指定(range)	○	指定不可

(凡例)
○：TCP/UDP ポート番号検出パターンを使用する
−：TCP/UDP ポート番号検出パターンを使用しない

本装置では，TCP/UDP ポート番号検出パターンを共有して使用します。

1. フィルタと QoS での共有については，複数のフィルタエントリと複数の QoS エントリでは共有します。
2. フロー検出条件の TCP と UDP で共有します。
3. フロー検出条件の送信元ポート番号と宛先ポート番号では共有しません。
4. フロー検出条件の IPv4 条件と IPv6 条件で共有します。

TCP/UDP ポート番号検出パターンを使用する例を次の表に示します。

表 3-33　TCP/UDP ポート番号検出パターンの使用例

パターンの使用例※	使用するパターン数	運用コマンド show system での表示 (Resources(Used/Max)の Used の値)
フィルタエントリで • 送信元ポート番号の範囲指定(10～30) フィルタエントリで • 送信元ポート番号の範囲指定(10～40)	二つのエントリでは指定している送信元ポート番号の範囲が異なるため， • 送信元ポート番号の範囲指定(10～30) • 送信元ポート番号の範囲指定(10～40) の 2 パターンを使用します。	2
フィルタエントリで • 送信元ポート番号の指定なし • 宛先ポート番号の範囲指定(10～20) フィルタエントリで • 送信元ポート番号の指定なし • 宛先ポート番号の範囲指定(10～20) QoS エントリで • 送信元ポート番号の指定なし	上記 1.の共有する場合の例です。 三つのエントリがありますが，どれも宛先ポート番号の範囲指定(10～20)で同じ範囲を指定しているのでパターンを共有します。 • 宛先ポート番号の範囲指定(10～20) の 1 パターンを使用します。	1

パターンの使用例※	使用するパターン数	運用コマンド show system での表示 (Resources(Used/Max)の Used の値)
• 宛先ポート番号の範囲指定(10～20)		
QoS エントリで • TCP を指定 • 送信元ポート番号の範囲指定(10～20) • 宛先ポート番号の指定なし QoS エントリで • UDP を指定 • 送信元ポート番号の範囲指定(10～20) • 宛先ポート番号の指定なし	上記 2.の共有する場合の例です。 二つのエントリがありますが，どちらも送信元ポート番号の範囲指定(10～20)で同じ値を指定しているのでパターンを共有します。 • 送信元ポート番号の範囲指定(10～20) の 1 パターンを使用します。	1
QoS エントリで • 送信元ポート番号の範囲指定(10～20) • 宛先ポート番号の範囲指定(10～20)	上記 3.の共有しない場合の例です。 指定した範囲が同じでも送信元と宛先ではパターンを共有しません。 • 送信元ポート番号の範囲指定(10～20) • 宛先ポート番号の範囲指定(10～20) の 2 パターンを使用します。	2
QoS エントリで • IPv4 条件で送信元ポート番号の範囲指定(10～20) QoS エントリで • IPv6 条件で送信元ポート番号の範囲指定(10～20)	上記 4.の共有する場合の例です。 二つのエントリがありますが，どちらも送信元ポート番号の範囲指定(10～20)で同じ範囲を指定しているのでパターンを共有します。 • 送信元ポート番号の範囲指定(10～20) の 1 パターンを使用します。	1

注※　（）内は単一指定したときの値，または範囲指定したときの範囲です。

3.6　レイヤ 2 認証

3.6.1　IEEE802.1X

IEEE802.1X の収容条件を次に示します。

本装置の IEEE802.1X では，三つの認証モードをサポートしています。

- ポート単位認証
- VLAN 単位認証（静的）
- VLAN 単位認証（動的）

VLAN 単位認証を使用する場合に，IEEE802.1X を設定できる装置当たりの総ポート数を次の表に示します。

表 3-34　IEEE802.1X を設定できる装置当たりの総ポート数

モデル	IEEE802.1X を設定できる装置当たりの総ポート数※
全モデル共通	1024

注※

IEEE802.1X を設定できる装置当たりの総ポート数とは，VLAN 単位認証を設定した VLAN での VLAN ポート数の総和の最大値です。VLAN 内にチャネルグループが含まれている場合は，チャネルグループを構成する物理ポート数に関係なく，チャネルグループを 1 ポートとして計算します。また，1 ポートに VLAN が Tag で多重化されている場合も個別に数えます。例えば，一つのポートに Tag で多重化された 10 個の VLAN が設定されていた場合，その 10 個の VLAN で VLAN 単位認証を動作させると，総ポート数は 10 ポートになります。

各認証モードでの単位当たりの最大認証端末数を次の表に示します。

表 3-35　各認証モード単位当たりの最大認証端末数

モデル	認証モード		
	ポート単位認証	VLAN 単位認証（静的）	VLAN 単位認証（動的）
全モデル共通	64/ポート	256/VLAN	1024※/装置

注※

IEEE802.1X（VLAN 単位認証（動的））および Web 認証（ダイナミック VLAN モード）を同時に動作した場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

本装置の最大認証端末数を次の表に示します。

表 3-36　本装置の最大認証端末数

モデル	3 モード合計での最大認証端末数
全モデル共通	1024※/装置

注※

IEEE802.1X（ポート単位認証および VLAN 単位認証（静的）），Web 認証（固定 VLAN モード）および MAC 認証を同時に動作させた場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

3.6.2　Web 認証

Web 認証の収容条件を次の表に示します。

表 3-37　Web 認証の装置当たりの収容条件

項目		最大数
最大認証数	固定 VLAN モード	1024※1
	ダイナミック VLAN モード	1024※2
	レガシーモード	1024※3
内蔵 Web 認証 DB 登録ユーザ数		300※4
認証画面入れ替えで指定できるファイルの合計サイズ		1024KB
認証画面入れ替えで指定できるファイル数		100
認証前端末用に設定できる IPv4 アクセスリスト数		1
認証前端末用 IPv4 アクセスリストに指定できるフィルタ条件数		20

注※1

Web 認証（固定 VLAN モード），IEEE802.1X（ポート単位認証および VLAN 単位認証（静的））および MAC 認証（固定 VLAN モード）を同時に動作させた場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

注※2

Web 認証（ダイナミック VLAN モード），MAC 認証（ダイナミック VLAN モード）および IEEE802.1X（VLAN 単位認証（動的））を同時に動作した場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

注※3

Web 認証（レガシーモード）および IEEE802.1X（VLAN 単位認証（動的））を同時に動作した場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

注※4

内蔵 Web 認証 DB に登録したユーザ ID を複数の端末で使用すると，最大認証端末数まで端末を認証できます。ただし，認証対象となるユーザ ID の数が内蔵 Web 認証 DB の最大登録数より多い場合は，RADIUS サーバを用いた RADIUS 認証方式を使用してください。

3.6.3　MAC 認証

MAC 認証の収容条件を次の表に示します。

表 3-38　MAC 認証の装置当たりの収容条件

項目		最大数
最大認証数	固定 VLAN モード	1024※1
	ダイナミック VLAN モード	1024※2
内蔵 MAC 認証 DB 登録ユーザ数		1024

注※1

MAC 認証（固定 VLAN モード），IEEE802.1X（ポート単位認証および VLAN 単位認証（静的））および Web 認証（固定 VLAN モード）を同時に動作させた場合は，それぞれの認証端末数の合計で 1024 までとなります。

注※2

MAC 認証（ダイナミック VLAN モード），Web 認証（ダイナミック VLAN モード）および IEEE802.1X（VLAN 単位認証（動的））を同時に動作した場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

3.7　DHCP snooping

DHCP snooping の収容条件を次の表に示します。

表 3-39　DHCP snooping の最大エントリ数

受信側フロー検出モード	バインディングデータベースエントリ数※1		端末フィルタエントリ数※2
	ダイナミック／スタティックの合計	スタティック	
layer3-dhcp-1， layer3-suppress-dhcp-1	3070	256	3070
custom	3070	256	0～3070※3
上記以外	3070	256	0

注※1

untrust ポート配下の端末当たり 1 エントリを消費します。

注※2

バインディングデータベースエントリ配下のポート当たり 1 エントリを消費します。

チャネルグループの場合，チャネルグループ当たりのポート数を数えます。

注※3

エントリブロックに DHCP snooping の端末フィルタを指定しなかった場合の 0 エントリから，エントリブロックにバインディングデータベースの最大エントリ数分の DHCP snooping の端末フィルタを指定した場合の 3070 エントリまでとなります。

表 3-40　DHCP snooping の最大 VLAN 数

モデル	最大 VLAN 数
全モデル共通	1024

3.8　冗長化構成による高信頼化

3.8.1　GSRP

GSRP の収容条件を次の表に示します。

表 3-41　GSRP 収容条件

モデル	VLAN グループ最大数	VLAN グループ当たりの VLAN 最大数
全モデル共通	64	1024

なお，レイヤ 3 冗長切替機能を使用する場合には，VLAN グループに所属している VLAN に設定するポート数の合計の最大数が 5000 となります。チャネルグループの場合は，チャネルグループ単位で 1VLAN ポートと数えます。

3.8.2　VRRP

VRRP に関する収容条件を次の表に示します。

表 3-42　VRRP 収容条件

モデル	仮想ルータ最大数		障害監視インタフェースと VRRP ポーリング最大数	
	インタフェース当たり	装置当たり	仮想ルータ当たり	装置当たり
全モデル共通	255※1	255※1	16※2	255※2

注※1　IPv4/IPv6 の仮想ルータの合計数です。

注※2　障害監視インタフェースと VRRP ポーリングの合計数です。

表 3-43　VRRP 収容条件（グループ切替機能使用時）

モデル	仮想ルータ最大数		最大グループ数	1 グループ当たりの最大フォロー仮想ルータ数	障害監視インタフェースと VRRP ポーリング最大数	
	インタフェース当たり	装置当たり			仮想ルータ当たり	装置当たり
全モデル共通	255※1	1023※1	255	1022	16※2	255※2

注※1

IPv4/IPv6 の仮想ルータの合計数は 255 までです。ただし，グループ切替機能を利用し，フォロー仮想ルータを作成することで，最大 1023 の仮想ルータが動作できます。

注※2

障害監視インタフェースと VRRP ポーリングの合計数です。

3.8.3　アップリンク・リダンダント

アップリンク・リダンダントに関する収容条件を次の表に示します。

表 3-44　アップリンク・リダンダント収容条件

モデル	アップリンクポート数	アップリンクポート当たりの 収容インタフェース数
全モデル共通	50※	2

注※　チャネルグループの場合は，チャネルグループ単位で 1 ポートと数えます。

表 3-45　MAC アドレスアップデート機能の収容条件

モデル	最大送信 MAC アドレスエントリ数
全モデル共通	3000

3.9　ネットワーク監視機能

3.9.1　L2 ループ検知

L2 ループ検知の L2 ループ検知フレーム送信レートを次の表に示します。

表 3-46　L2 ループ検知フレーム送信レート

モデル	L2 ループ検知フレームの送信レート（装置当たり）※1	
	スパニングツリー，GSRP，Ring Protocol のどれかを使用している場合	スパニングツリー，GSRP，Ring Protocol のどれも使用していない場合
全モデル共通	30pps（推奨値）※2	200pps（最大値）※3

- L2 ループ検知フレーム送信レート算出式
  L2 ループ検知フレーム送信対象の VLAN ポート数÷L2 ループ検知フレームの送信レート（pps）≦送信間隔（秒）
  なお，チャネルグループの場合，VLAN ポート数はチャネルグループ単位で 1 ポートと数えます。

注※1

送信レートは上記の条件式に従って，自動的に 200pps 以内で変動します。

注※2

スパニングツリー，GSRP，Ring Protocol のどれかを使用している場合は，30pps 以下に設定してください。30pps より大きい場合，スパニングツリー，GSRP，Ring Protocol の正常動作を保証できません。

注※3

200pps を超えるフレームは送信しません。送信できなかったフレームに該当するポートや VLAN ではループ障害を検知できなくなります。必ず 200pps 以下に設定してください。

3.10　ネットワークの管理

3.10.1　IEEE802.3ah/UDLD

スタックポートを除く全物理ポートでの運用を可能にします。1 ポート 1 対地を原則とするため，同一ポートから複数装置の情報を受信する場合（禁止構成）でも，保持する情報は 1 装置分だけです。IEEE802.3ah/UDLD の収容条件を次の表に示します。

表 3-47　最大リンク監視情報数

モデル	最大リンク監視情報数
全モデル共通	スタックポートを除く装置の最大物理ポート数

3.10.2　CFM

CFM の収容条件を次の表に示します。

表 3-48　CFM の収容条件

モデル	ドメイン数	MA 数	MEP 数	MIP 数	CFM ポート総数※1※2	リモート MEP 総数※2※3
全モデル共通	8／装置	32／装置	32／装置	32／装置	256／装置	2016／装置

注※1

CFM ポート総数とは，MA のプライマリ VLAN のうち，CFM のフレームを送信する VLAN ポートの総数です。

Down MEP だけの MA の場合

Down MEP の VLAN ポートの総数

Up MEP を含む MA の場合

プライマリ VLAN の全 VLAN ポートの総数

なお，CFM ポート総数は運用コマンド show cfm summary で確認できます。

注※2

CFM ポート総数およびリモート MEP 総数は，CCM 送信間隔がデフォルト値のときの収容条件です。CCM 送信間隔を変更すると，CFM ポート総数およびリモート MEP 総数の収容条件が変わります。CCM 送信間隔による CFM ポート総数およびリモート MEP 総数の収容条件を次の表に示します。

表 3-49　CCM 送信間隔による収容条件

モデル	CCM 送信間隔	CFM ポート総数	リモート MEP 総数
全モデル共通	1 分以上	256／装置	2016／装置
	10 秒	128／装置	2016／装置
	1 秒	50／装置	200／装置

注※3

リモート MEP 総数とは，自装置以外の MEP の総数です。MEP からの CCM 受信性能に影響します。
リモート MEP 総数は運用コマンド show cfm remote-mep で確認できます。

表 3-50　CFM の物理ポートおよびチャネルグループの収容条件

モデル	MEP・MIP を設定可能な物理ポートおよびチャネルグループの総数※
全モデル共通	8／装置

注※

MEP・MIP は同一ポートに対して複数設定できます。チャネルグループの場合は，チャネルグループ単位で 1 ポートと数えます。

表 3-51　CFM のデータベース収容条件

モデル	MEP CCM データベース エントリ数	MIP CCM データベース エントリ数	Linktrace データベース エントリ数※
全モデル共通	63／MEP	2048／装置	1024／装置

注※

1 ルート当たり 256 装置の情報を保持する場合は，最大で 4 ルート分を保持します（1024÷256 装置＝ 4 ルート）。

3.10.3　LLDP/OADP

(1)　LLDP

LLDP の収容条件を次の表に示します。

表 3-52　LLDP の収容条件

項目		最大収容数
LLDP 隣接装置情報	IEEE 802.1AB Draft 6	104
	IEEE Std 802.1AB-2009	104
Port And Protocol VLAN ID TLV で送信できる VLAN 数		100※
VLAN Name TLV で送信できる VLAN 数		100※

注※

Port And Protocol VLAN ID TLV と VLAN Name TLV で合わせて 100 個となります。また，値の小さい順に 100 個となります。

(2)　OADP

OADP の収容条件を次の表に示します。

表 3-53　OADP の収容条件

項目	最大収容数
OADP 隣接装置情報	100※

注※

チャネルグループの場合は，チャネルグループ単位で 1 と数えます。

3.10.4　PTP

PTP の収容条件を次の表に示します。

表 3-54　PTP の収容条件

項目	装置当たりの数
PTP を使用できる VLAN 数	1
PTP インタフェース数	52

3.11　IPv4・IPv6 パケット中継

本装置では VLAN に対して IP アドレスを設定します。ここでは，IP アドレスを設定できる VLAN インタフェースの最大数，設定できる IP アドレスの最大数，通信できる相手装置の最大数などについて説明します。また，DHCP リレー/DHCP サーバの収容条件についても説明します。

3.11.1　IP アドレスを設定できるインタフェース数

本装置でサポートする最大インタフェース数を次の表に示します。ここで示す値は，IPv4 と IPv6 との合計の値です。なお，IPv4 と IPv6 を同一のインタフェースに設定することも，個別に設定することもできます。

表 3-55　最大インタフェース数

モデル	インタフェース数（装置当たり）
全モデル共通	1024

3.11.2　マルチホームの最大サブネット数

LAN のマルチホーム接続では一つのインタフェースに対して，複数の IPv4 アドレス，または IPv6 アドレスを設定します。

(1)　IPv4 の場合

IPv4 でのマルチホームの最大サブネット数を次の表に示します。

表 3-56　マルチホームの最大サブネット数（IPv4 の場合）

モデル	マルチホーム サブネット数 （インタフェース当たり）
全モデル共通	256

(2)　IPv6 の場合

IPv6 でのマルチホームの最大サブネット数を次の表に示します。なお，ここで示す値にはリンクローカルアドレスを含みます。一つのインタフェースには必ず一つのリンクローカルアドレスが設定されます。このため，すべてのインタフェースで IPv6 グローバルアドレスだけを設定した場合，実際に装置に設定される IPv6 アドレス数は，表の数値に自動生成される IPv6 リンクローカルアドレス数 1 を加算した 8 になります。

表 3-57　マルチホームの最大サブネット数（IPv6 の場合）

モデル	マルチホーム サブネット数 （インタフェース当たり）
全モデル共通	7

3.11.3　IP アドレス最大設定数

(1)　IPv4 アドレス

装置当たりのコンフィグレーションで設定できる IPv4 アドレスの最大数を次の表に示します。なお，この表で示す値は，通信用インタフェースに設定できる IPv4 アドレス数です。

表 3-58　コンフィグレーションで装置に設定できる IPv4 アドレス最大数

モデル	IPv4 アドレス数（装置当たり）
全モデル共通	1024※

注※　IPv6 ユニキャスト優先モードの場合，最大数は 128 になります。

(2)　IPv6 アドレス

コンフィグレーションで設定できる装置当たりの IPv6 アドレスの最大数を次の表に示します。なお，ここで示す値は通信用のインタフェースに設定する IPv6 アドレスの数です。また，IPv6 リンクローカルアドレスの数も含みます。一つのインタフェースには必ず一つの IPv6 リンクローカルアドレスが設定されます。このため，すべてのインタフェースに IPv6 グローバルアドレスを設定した場合，インタフェースには自動で IPv6 リンクローカルアドレスが付与され，実際に装置に設定される IPv6 アドレスの数は「表 3-60　コンフィグレーションで装置に設定できる IPv6 アドレス数と，装置に設定される IPv6 アドレス数の関係」に示す値となります。

表 3-59　コンフィグレーションで装置に設定できる IPv6 アドレス最大数

モデル	IPv6 アドレス数（装置当たり）
全モデル共通	128

表 3-60　コンフィグレーションで装置に設定できる IPv6 アドレス数と，装置に設定される IPv6 アドレス数の関係

コンフィグレーションで設定する IPv6 アドレスの数		コンフィグレーションで設定する IPv6 アドレスの合計数	自動で設定する IPv6 リンクローカルアドレスの数	装置に設定される IPv6 アドレス数
IPv6 リンクローカルアドレス	IPv6 グローバルアドレス			
128(128×1)	0	128	0	128
0	128(128×1)	128	128	256

注　（）内数字の意味：

（A×B）　A：インタフェース数　B：各インタフェースに設定するアドレス数

3.11.4　最大相手装置数

本装置が接続する LAN を介して通信できる最大相手装置数を示します。この場合の相手装置はルータに限らず，端末も含みます。

(1)　ARP エントリ数

IPv4 の場合，LAN では ARP によって，送信しようとするパケットの宛先アドレスに対応するハードウェアアドレスを決定します。したがって，これらのメディアでは ARP エントリ数によって最大相手装置数が

決まります。本装置でサポートするARPエントリの最大数については，「3.1　テーブルエントリ数」を参照してください。

(2)　NDPエントリ数

IPv6の場合，LANではNDPでのアドレス解決によって，送信しようとするパケットの宛先アドレスに対応するハードウェアアドレスを決定します。したがって，NDPエントリ数によって最大相手装置数が決まります。本装置でサポートするNDPエントリの最大数については，「3.1　テーブルエントリ数」を参照してください。

(3)　RAの最大相手端末数

RAではルータから通知されるIPv6アドレス情報を基に端末でアドレスを生成します。本装置での最大相手端末数を次の表に示します。

表3-61　RAの最大相手端末数

モデル	RAの最大相手端末数	
	インタフェース当たり	装置当たり
全モデル共通	128	128

3.11.5　ポリシーベースルーティング（IPv4）【SL-L3A】

(1)　ポリシーベースルーティングの収容条件

ポリシーベースルーティングでは，フィルタのフロー検出を使用して，ポリシーベースルーティングの対象にするフローを検出します。なお，ポリシーベースルーティングは受信側フロー検出モードがlayer3-6，layer3-mirror-3，layer3-mirror-4，layer3-mirror-5，layer3-suppress-2，layer3-suppress-mirror-2，またはcustomの場合に使用できます。

装置当たりのポリシーベースルーティンググループのエントリ数を次の表に示します。

表3-62　装置当たりのポリシーベースルーティンググループのエントリ数

項目	IPv4ポリシーベースルーティンググループ
アクセスリストエントリ数	「表3-26　受信側フィルタ最大エントリ数」を参照※1
ポリシーベースルーティングリスト数	256※2
ポリシーベースルーティングリスト情報内に設定できる経路数	8
ポリシーベースルーティングのトラッキング機能と連携できる経路数	1024※3

注※1

エントリ数の算出方法は，「3.5　フィルタ・QoS・ポリシーベースミラーリング」と同じです。

注※2

1ポリシーベースルーティングリスト情報を1リストとして登録します。このため，複数のアクセスリストで同一のポリシーベースルーティングリスト情報を設定した場合，使用するリスト数は1リストと計算します。

注※3

1 トラック ID を 1 エントリとして登録します。このため，複数の経路で同一のトラック ID を設定した場合，使用するエントリ数は 1 エントリと計算します。

(2)　トラッキング機能の収容条件

ポリシーベースルーティングのトラッキング機能の収容条件を次の表に示します。

表 3-63　トラッキング機能の収容条件

項目	収容条件
トラックの数	1024
ポーリング監視トラックの数※	1024

注※　コンフィグレーションコマンド type icmp を設定したトラックの数です。

3.11.6　DHCP/BOOTP リレー

DHCP/BOOTP リレーで設定できるインタフェース数およびリレー先アドレス数を次の表に示します。

表 3-64　DHCP/BOOTP リレーの最大数

項目	最大数
DHCP/BOOTP リレーインタフェース数	1023
DHCP/BOOTP リレー先アドレス数 （グローバルネットワーク，VRF 当たり）	16
VRF 使用時の装置当たりの DHCP/BOOTP リレー先アドレス数	256

3.11.7　IPv6 DHCP リレー

IPv6 DHCP リレーの収容条件を次の表に示します。

表 3-65　IPv6 DHCP リレーの最大数

項目	装置当たりの最大数
配布プレフィックス数※	1024
インタフェース数	127

注※

クライアントを直接収容した場合に IPv6 DHCP サーバによって配布される PD プレフィックス数です。ほかのリレー経由のパケットや PD プレフィックス以外の情報は，この条件に関係なく中継できます。

3.11.8　DHCP サーバ

DHCP サーバで設定できるインタフェース数および配布可能 IP アドレス数などを次の表に示します。

表 3-66　DHCP サーバの最大数

項目	装置当たりの最大数
DHCP サーバインタフェース数	1024
DHCP サーバ管理サブネット数	1024
配布可能 IP アドレス数※1	2000
配布可能固定 IP アドレス数	160
配布除外 IP アドレス範囲数※2	4096

注※1　配布可能固定 IP アドレス数を含みます。

注※2　サブネット当たり 1024 までです。

3.11.9　IPv6 DHCP サーバ

IPv6 DHCP サーバで設定できるインタフェース数および配布可能 IPv6 プレフィックス数などを次の表に示します。

表 3-67　IPv6 DHCP サーバの最大数

項目	装置当たりの最大数
インタフェース数	128
最大配布可能 Prefix 数	1024

3.11.10　UDP ブロードキャストリレー

UDP ブロードキャストリレーで設定できるインタフェース数，転送先アドレス数，および転送対象とするパケットの宛先ポート番号の数を次の表に示します。

表 3-68　UDP ブロードキャストリレーの最大数

項目	最大数
インタフェース数	1024
転送先アドレス数 （インタフェース当たり）	16
転送対象とするパケットの宛先ポート番号の数 （インタフェース当たり）	16

3.12　IPv4・IPv6 ルーティングプロトコル

3.12.1　最大隣接ルータ数

最大隣接ルータ数を次の表に示します。

表 3-69　最大隣接ルータ数

ルーティングプロトコル	最大隣接ルータ数	
	ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
スタティックルーティング（IPv4，IPv6 の合計）	1024※	128※
RIP	50	25
RIPng	50	25
OSPF	200	25
OSPFv3	50	25
BGP4	250	25
BGP4+	50	25
RIP，OSPF，BGP4，RIPng，OSPFv3，BGP4+の合計	250	25

注※

動的監視機能を使用する隣接ルータは，ポーリング間隔によって数が制限されます。詳細は，次の表を参照してください。

表 3-70　スタティックの動的監視機能を使用できる最大隣接ルータ数

ポーリング周期	動的監視機能を使用できる最大隣接ルータ数
1 秒	60
2 秒	120
3 秒	180
5 秒	300
10 秒	600
20 秒	1024

最大隣接ルータ数の定義を次の表に示します。

表 3-71　最大隣接ルータ数の定義

ルーティングプロトコル	定義
スタティック	ネクストホップ・アドレスの数

ルーティング プロトコル	定義
ルーティング	
RIP	RIP が動作するネットワーク上の RIP ルータ数
RIPng	RIPng が動作するネットワーク上の RIPng ルータ数
OSPF	OSPF が動作する各インタフェースにおける下記の総計 1. 該当インタフェースが指定ルータまたはバックアップ指定ルータになる場合 該当インタフェースと接続されるほかの OSPF ルータの数 2. 該当インタフェースが指定ルータまたはバックアップ指定ルータにならない場合 該当インタフェースと接続される指定ルータおよびバックアップ指定ルータの数 上記は，運用コマンド show ip ospf neighbor で表示される隣接ルータの状態(State)が”Full”となる隣接ルータの数と同じ意味となります。
OSPFv3	OSPFv3 が動作する各インタフェースにおける下記の総計 1. 該当インタフェースが指定ルータまたはバックアップ指定ルータになる場合 該当インタフェースと接続されるほかの OSPFv3 ルータの数 2. 該当インタフェースが指定ルータまたはバックアップ指定ルータにならない場合 該当インタフェースと接続される指定ルータおよびバックアップ指定ルータの数 上記は，運用コマンド show ipv6 ospf neighbor で表示される隣接ルータの状態(State)が”Full”となる隣接ルータの数と同じ意味となります。
BGP4	BGP4 ピア数
BGP4+	BGP4+ピア数

3.12.2　経路エントリ数と最大隣接ルータ数の関係

最大経路エントリ数と最大隣接ルータ数の関係について，IPv4 モードの場合，IPv4/IPv6 モードの場合，IPv6 ユニキャスト優先モードの場合，および L2 優先モードの場合を次の表に示します。

表 3-72　経路エントリ数と最大隣接ルータ数の関係(RIP，OSPF，BGP4)（IPv4 モード）

ルーティング プロトコル	最大経路エントリ数※1	最大隣接ルータ数※2	
		ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
RIP	1000	50	25
OSPF※3※4	1200	200	50
	12000	20	5
BGP4	16285 (65140※5)	250	25

注※1　最大経路エントリ数は代替経路を含みます。

注※2　各ルーティングプロトコル（RIP，OSPF，BGP4）を併用して使用する場合の最大隣接ルータ数は，各々 1/n (n：使用ルーティングプロトコル数）となります。

注※3　OSPF の最大経路エントリ数は LSA 数を意味します。

注※4　VRF で OSPF を使用している場合，各 VRF で保持している LSA 数×各 VRF の隣接ルータ数の総計が 24 万を超えないようにしてください。

注※5　非アクティブ経路を含みます。

表 3-73　経路エントリ数と最大隣接ルータ数の関係(RIP/RIPng，OSPF/OSPFv3，BGP4/BGP4+) (IPv4/IPv6 モード)

ルーティングプロトコル	最大経路エントリ数※1	最大隣接ルータ数※2	
		ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
RIP	1000	50	25
RIPng	1000	50	25
OSPF※3※4	1000	200	50
	2000	100	25
	8000	25	6
OSPFv3※3※5	1000	50	25
	2000	25	13
BGP4	8093 (32372※6)	250	25
BGP4+	3007 (12028※6)	50	25

注※1　最大経路エントリ数は代替経路を含みます。

注※2　各ルーティングプロトコル（RIP，RIPng，OSPF，OSPFv3，BGP4，BGP4+）を併用して使用する場合の最大隣接ルータ数は，各々 1/n（n：使用ルーティングプロトコル数）となります。

注※3　OSPF/OSPFv3 の最大経路エントリ数は LSA 数を意味します。

注※4　VRF で OSPF を使用している場合，各 VRF で保持している LSA 数×各 VRF の隣接ルータ数の総計が 20 万を超えないようにしてください。

注※5　VRF で OSPFv3 を使用している場合，各 VRF で保持している LSA 数×各 VRF の隣接ルータ数の総計が 5 万を超えないようにしてください。

注※6　非アクティブ経路を含みます。

表 3-74　経路エントリ数と最大隣接ルータ数の関係(RIP/RIPng，OSPF/OSPFv3，BGP4/BGP4+) (IPv6 ユニキャスト優先モード)

ルーティングプロトコル	最大経路エントリ数※1	最大隣接ルータ数※2	
		ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
RIP	1000	50	25
RIPng	1000	50	25
OSPF※3※4	1000	200	25
OSPFv3※3※5	1000	50	25
	5000	10	5

ルーティングプロトコル	最大経路エントリ数※1	最大隣接ルータ数※2	
		ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
BGP4	1023 (4092※6)	250	25
BGP4+	6542 (26168※6)	50	25

注※1　最大経路エントリ数は代替経路を含みます。

注※2　各ルーティングプロトコル（RIP，RIPng，OSPF，OSPFv3，BGP4，BGP4+）を併用して使用する場合の最大隣接ルータ数は，各々 1/n（n：使用ルーティングプロトコル数）となります。

注※3　OSPF/OSPFv3 の最大経路エントリ数は LSA 数を意味します。

注※4　VRF で OSPF を使用している場合，各 VRF で保持している LSA 数×各 VRF の隣接ルータ数の総計が 20 万を超えないようにしてください。

注※5　VRF で OSPFv3 を使用している場合，各 VRF で保持している LSA 数×各 VRF の隣接ルータ数の総計が 5 万を超えないようにしてください。

注※6　非アクティブ経路を含みます。

表 3-75　経路エントリ数と最大隣接ルータ数の関係(RIP/RIPng，OSPF/OSPFv3，BGP4/BGP4+)（L2 優先モード）

ルーティングプロトコル	最大経路エントリ数※1	最大隣接ルータ数※2	
		ポリシーベースルーティングのトラッキング機能を使用しない	ポリシーベースルーティングのトラッキング機能を使用する
RIP	1000	50	25
RIPng	1000	50	25
OSPF※3※4	1000	200	25
	2000	100	25
	8000	25	6
OSPFv3※3※5	1000	50	25
	2000	25	13
BGP4	8093 (32372※6)	250	25
BGP4+	3007 (12028※6)	50	25

注※1　最大経路エントリ数は代替経路を含みます。

注※2　各ルーティングプロトコル（RIP，RIPng，OSPF，OSPFv3，BGP4，BGP4+）を併用して使用する場合の最大隣接ルータ数は，各々 1/n（n：使用ルーティングプロトコル数）となります。

注※3　OSPF/OSPFv3 の最大経路エントリ数は LSA 数を意味します。

注※4　VRF で OSPF を使用している場合，各 VRF で保持している LSA 数×各 VRF の隣接ルータ数の総計が 20 万を超えないようにしてください。

注※5　VRF で OSPFv3 を使用している場合，各 VRF で保持している LSA 数×各 VRF の隣接ルータ数の総計が 5 万を超えないようにしてください。

注※6　非アクティブ経路を含みます。

3.12.3　本装置で設定できるコンフィグレーションの最大数

ルーティングプロトコルについて，設定できるコンフィグレーションの最大数を次の表に示します。

なお, この表で示す値はコンフィグレーションで設定できる最大数です。運用する際は本章にある収容条件をすべて満たすようにしてください。

表 3-76　コンフィグレーションの最大設定数

分類	コンフィグレーションコマンド	最大数の定義	最大設定数
IPv4 スタティック	ip route	設定行数	12288
IPv6 スタティック	ipv6 route	設定行数	2048
IPv4 集約経路	ip summary-address	設定行数	1024
IPv6 集約経路	ipv6 summary-address	設定行数	1024
RIP	network	設定行数	128
	ip rip authentication key	設定行数	512
	address-family ipv4	設定行数	31
RIPng	ipv6 rip enable	設定行数	128
	ipv6 router rip	設定行数	32
OSPF	area range	設定行数	1024
	area virtual-link	authentication-key，message-digest-key パラメータを設定した行数の総計	512
	ip ospf authentication-key ip ospf message-digest-key	各設定行数の総計	512
	network	設定行数	256
	router ospf	設定行数	256
	インタフェースに設定する OSPF コマンド passive-interface	設定したインタフェース数 (ループバックインタフェースを含む)	288
OSPFv3	area range	設定行数	1024
	ipv6 router ospf	設定行数	256
	インタフェースに設定する OSPFv3 コマンド passive-interface	設定したインタフェース数 (ループバックインタフェースを含む)	288
BGP4	network	設定行数	1024
	address-family ipv4	設定行数	31

分類	コンフィグレーションコマンド	最大数の定義	最大設定数
BGP4+	network	設定行数	1024
	address-family ipv6	設定行数	32
経路フィルタ	distribute-list in（RIP） distribute-list out（RIP） redistribute（RIP）	各設定行数の総計	500
	distribute-list in（OSPF） distribute-list out（OSPF） redistribute（OSPF）	各設定行数の総計	500
	distribute-list in（BGP4） distribute-list out（BGP4） redistribute（BGP4）	各設定行数の総計	500
	distribute-list in（RIPng） distribute-list out（RIPng） redistribute（RIPng）	各設定行数の総計	500
	distribute-list in（OSPFv3） distribute-list out（OSPFv3） redistribute（OSPFv3）	各設定行数の総計	500
	distribute-list in（BGP4+） distribute-list out（BGP4+） redistribute（BGP4+）	各設定行数の総計	500
	ip as-path access-list	設定<Id>の種類数	200
		設定行数	1024
	ip community-list	設定<Id>の種類数	100
		standard 指定の設定行数	100
		expanded 指定の設定行数	100
	ip prefix-list	設定<Id>の種類数	1024
		設定行数	4096
	ipv6 prefix-list	設定<Id>の種類数	1024
		設定行数	4096
	neighbor in（BGP4） neighbor out（BGP4）	<IPv4-Address>の設定行数の総計	500
		<Peer-Group>の設定行数の総計	500
	neighbor in（BGP4+） neighbor out（BGP4+）	<IPv6-Address>の設定行数の総計	500
		<Peer-Group>の設定行数の総計	500
	route-map	設定<Id>の種類数	256
		設定<Id>と<Seq>の組み合わせ種類数	4096

分類	コンフィグレーションコマンド	最大数の定義	最大設定数
	match as-path	各設定行で指定したパラメータの総計	2048
	match community	各設定行で指定したパラメータの総計	2048
	match interface	各設定行で指定したパラメータの総計	2048
	match ip address match ipv6 address	各設定行で指定したパラメータの総計	2048
	match ip route-source match ipv6 route-source	各設定行で指定したパラメータの総計	2048
	match origin	設定行数	2048
	match protocol	各設定行で指定したパラメータの総計	2048
	match route-type	設定行数	2048
	match tag	各設定行で指定したパラメータの総計	2048
	match vrf	各設定行で指定したパラメータの総計	1024
	set as-path prepend count set distance set local-preference set metric set metric-type set origin set tag	どれか一つが設定された route-map の，<Id>と<Seq>の組み合わせ種類数	2048
	set community	各設定行で指定したパラメータの総計	2048
	set community-delete	各設定行で指定したパラメータの総計	2048

3.13　IPv4・IPv6 マルチキャストルーティングプロトコル

3.13.1　IPv4 マルチキャスト

IPv4 マルチキャストを設定できるインタフェース数およびルーティングテーブルのエントリ数を次の表に示します。本装置は IPv4 マルチキャストルーティングプロトコルとして PIM-SM または PIM-SSM をサポートします。PIM-SM と PIM-SSM は同時に動作できます。

複数の VRF で IPv4 マルチキャストを使用する場合，グローバルネットワークとすべての VRF の合計を本収容条件内に収めてください。

表 3-77　IPv4 マルチキャストの最大数

項　目	最大数
PIM-SM/SSM マルチキャストインタフェース数※1※2	511／装置
IGMP 動作インタフェース数※2	511／装置
マルチキャスト送信元の数	128／グループ
PIM-SM/SSM マルチキャスト経路情報のエントリ((S,G)エントリ，(*,G)エントリ，およびネガティブキャッシュ)数※3 S：送信元 IP アドレス G：グループアドレス	8191／装置
IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連携動作させる設定数(ソース，グループのペア数)※4	1024／装置
IGMPv3 で 1Report につき処理できる record 情報※5	256record／メッセージ 256 ソース／record
IGMP 加入グループ数※6	1024／装置
マルチキャストルータ隣接数	64／装置
ランデブーポイント数	2／グループ
1 装置当たりランデブーポイントで設定できるグループ数	128／装置
1 ネットワーク（VPN）当たりランデブーポイントに設定できる延べグループ数	2048／ネットワーク（VPN） 2048／装置※7
1 ネットワーク（VPN）当たりのランデブーポイント候補数	1024／ネットワーク（VPN） 1024／装置※7
1 ネットワーク（VPN）当たりの BSR 候補数	16／ネットワーク（VPN） 32／装置※7
静的加入グループ数※8	256／装置
静的ランデブーポイント（RP）ルータアドレス数	16／装置
インタフェース当たりの IGMP 加入グループ数※6	1024／インタフェース

項　目	最大数
IGMP グループ当たりのソース数	128／グループ
マルチキャストを設定できる VRF 数	32／装置※9
エクストラネットのマルチキャストフィルタ数※10	64／装置
エクストラネットで使用する route-map 数	32／装置 32／VRF
PIM-SM VRF Gateway 動作マルチキャストアドレス数※11	32／装置 32／VRF

注※1

PIM-SM/PIM-SSM として他ルータと隣接するインタフェース数。

注※2

インタフェースに PIM-SM/SSM を使用した場合，該当するインタフェースで IGMP も自動的に動作するため，それぞれのインタフェース数を一つずつ消費します。

注※3

上限はテーブルエントリ数の配分パターンによって異なります。詳細は「3.1　テーブルエントリ数」を参照してください。ただし，次の条件を同時に満たす環境で PIM-SM を使用する場合，最大エントリ数が 128 以上のモードを選択していても，最大エントリ数は 128 になります。

- ストリーミングのような転送量の多いマルチキャスト通信
- 本装置が first hop router またはランデブーポイント

また，エントリの入出力ポート数にも上限があるため，入出力ポート数によっても設定できるエントリ数が変わります。

1 エントリ内の入出力ポート数は，入出力インタフェースで同一のポートを使用している場合は 1 で数えます。例えば，入力インタフェースでポート 1/0/1 および 1/0/2，出力インタフェース 1 でポート 1/0/2，1/0/3 および 1/0/4，出力インタフェース 2 でポート 1/0/3，1/0/4 および 1/0/5 を使用している場合，該当するエントリの入出力ポート数は 5 となります。

入出力ポート数が「表 3-78　IGMP/MLD 動作インタフェース数に対するマルチキャスト入出力ポート数」に示す値までエントリを設定できます。エントリ間で入出力インタフェースの重複が多い場合は，「表 3-78　IGMP/MLD 動作インタフェース数に対するマルチキャスト入出力ポート数」に示す値より多くのエントリを設定できることがあります。

なお，入出力ポート数は IPv4 と IPv6 を同時動作させた場合，IPv4 と IPv6 のエントリの合計となります。

注※4

マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-79　使用インタフェース数に対する IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定可能数」および「表 3-80　加入グループ数に対する IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。加入グループ数は，動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合，加入グループ数は一つではなく，加入したインタフェースの数になります。

注※5

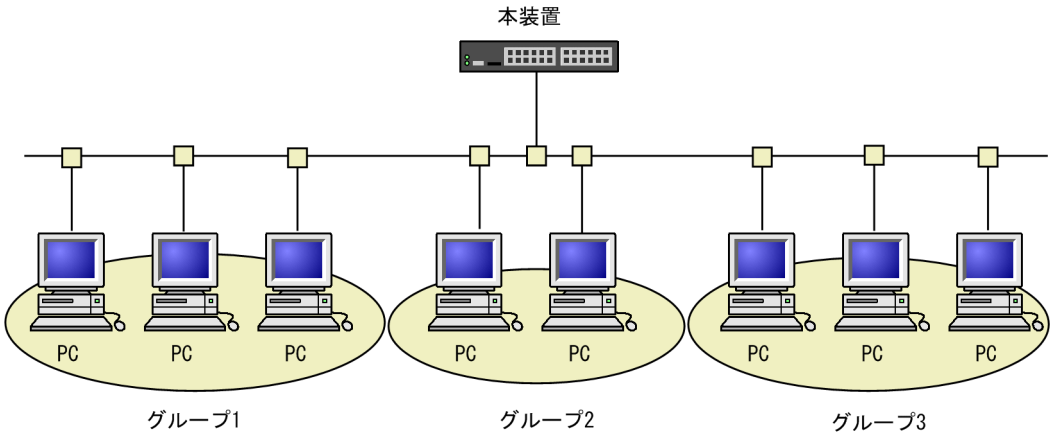
一つの Report メッセージで処理できるソース数は延べ 256 ソースまでです。ソース情報のない record も 1 ソースとして数えます。

IGMPv3（EXCLUDE モード）で PIM-SSM を連携動作させる設定をした場合，その設定に一致した EXCLUDE record で定義されているソース数を数えます。また，受信した Report メッセージ内に EXCLUDE record が複数存在し，IGMPv3（EXCLUDE モード）で PIM-SSM を連携動作させる設定で追加したソース数が延べ 256 を超えた場合，以降のそのメッセージ内の EXCLUDE record で，連携動作の対象となる EXCLUDE record についてマルチキャスト中継情報は作成しません。

注※6

本装置に直接接続しているグループの数を示します。IGMPv3 使用時に送信元を指定する場合のグループ数は，送信元とグループの組み合わせの数となります。「図 3-1　マルチキャストグループ数の例」の例では 3 です。インタフェース当たりの加入可能グループ数については，「表 3-81　IPv4 でのインタフェース当たりの加入可能グループ数」を参照してください。

図 3-1　マルチキャストグループ数の例



注※7

本装置のグローバルネットワークとすべての VRF に接続するネットワーク（VPN）上の総数です。

注※8

静的加入グループ数とは，各マルチキャストインタフェースで静的加入するグループアドレスの総数です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合，静的加入グループ数は一つではなく，静的加入設定したインタフェースの数になります。一つのインタフェースに設定できる静的加入グループ数は 256 までです。

注※9

グローバルでマルチキャストを設定している場合，31 になります。

注※10

すべての route-map で指定した access-list 内のアドレスの延べ数です。

注※11

エクストラネットで指定した route-map を使用します。route-map に指定した access-list 内で，ホストアドレス（32 ビットマスク）として指定したマルチキャストアドレスが対象となります。

装置当たりの上限は，すべての VRF で指定した PIM-SM VRF ゲートウェイのグループアドレスの延べ数です。

また，静的加入グループ数で指定したグループアドレス数との合計になります。

表 3-78　IGMP/MLD 動作インタフェース数に対するマルチキャスト入出力ポート数

IGMP/MLD 動作インタフェース数	エントリ単位の入出力ポート数を全エントリ分合算したポート数
64 以下	24575

IGMP/MLD 動作インタフェース数	エントリ単位の入出力ポート数を全エントリ分合算したポート数
65～128	12287
129～192	8191
193～256	6143
257～320	4915
321～384	4095
385～448	3510
449～512	3071
513～576	2730
577～638	2457

表 3-79　使用インタフェース数に対する IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定可能数

使用インタフェース数	IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定可能数
15	1024
31	512
63	256
127	128
255	64
511	32

表 3-80　加入グループ数に対する IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定可能数

加入グループ（延べ数）	IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定数
32	1024
64	512
128	256
256	128
512	64
1024	32
2048	16
4096	8
8128	4

表 3-81　IPv4 でのインタフェース当たりの加入可能グループ数

使用インタフェース数	インタフェース当たりの加入可能グループ数
7	1024
15	512
31	256
63	128
127	64
255	32
511	16

3.13.2　IPv6 マルチキャスト

IPv6 マルチキャストを設定できるインタフェース数およびルーティングテーブルのエントリ数を次の表に示します。本装置は IPv6 マルチキャストルーティングプロトコルとして PIM-SM および PIM-SSM をサポートしています。PIM-SM と PIM-SSM は同時に動作できます。

複数の VRF で IPv6 マルチキャストを使用する場合，グローバルネットワークとすべての VRF の合計を本収容条件内に収めてください。

表 3-82　IPv6 マルチキャストエントリ最大数

項　目	最大数
PIM-SM/SSM マルチキャストインタフェース数※1	63／装置
MLD 動作インタフェース数	127／装置
マルチキャスト送信元の数	128／グループ
PIM-SM/SSM マルチキャスト経路情報のエントリ((S,G)エントリ，(*,G)エントリ，およびネガティブキャッシュ)数※2 S：送信元 IP アドレス G：グループアドレス	1024／装置
MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM を連携動作させる設定数※3	256／装置
MLDv2 で 1Report に対し処理できる record 情報※4	32record／メッセージ 32 ソース／record
MLD 加入グループ数※5	256／装置
マルチキャストルータ隣接数	64／装置
ランデブーポイント数	1／グループ
1 装置当たりランデブーポイントで設定できるグループ数	128／装置
1 ネットワーク（VPN）当たりランデブーポイントに設定できる延べグループ数	128／ネットワーク（VPN） 128／装置※6

項　目	最大数
1 ネットワーク（VPN）当たりの BSR 候補数	16／ネットワーク（VPN） 32／装置※6
静的加入グループ数※7	256／装置
静的ランデブーポイント（RP）ルータアドレス数	16／装置
インタフェース当たりの MLD 加入グループ数※5	256／インタフェース
MLD グループ当たりのソース数	256／グループ
遠隔のマルチキャストサーバアドレスを直接接続サーバとして扱う設定数	256／装置 128／インタフェース
マルチキャストを設定できる VRF 数	32／装置※8
エクストラネットのマルチキャストフィルタ数※9	64／装置
エクストラネットで使用する route-map 数	32／装置 32／VRF
PIM-SM VRF Gateway 動作マルチキャストアドレス数※10	32／装置 32／VRF

注※1

PIM-SM/PIM-SSM として他ルータと隣接するインタフェース数。

注※2

上限はテーブルエントリ数の配分パターンによって異なります。詳細は「3.1　テーブルエントリ数」を参照してください。ただし，次の条件を同時に満たす環境で PIM-SM を使用する場合，最大エントリ数が 128 以上のモードを選択していても，最大エントリ数は 128 になります。

- ストリーミングのような転送量の多いマルチキャスト通信
- 本装置が first hop router またはランデブーポイント

また，エントリの入出力ポート数にも上限があるため，入出力ポート数によっても設定できるエントリ数が変わります。

1 エントリ内の入出力ポート数は，入出力インタフェースで同一のポートを使用している場合は 1 で数えます。例えば，入力インタフェースでポート 1/0/1 および 1/0/2，出力インタフェース 1 でポート 1/0/2，1/0/3 および 1/0/4，出力インタフェース 2 でポート 1/0/3，1/0/4 および 1/0/5 を使用している場合，該当するエントリの入出力ポート数は 5 となります。

入出力ポート数が「表 3-78　IGMP/MLD 動作インタフェース数に対するマルチキャスト入出力ポート数」に示す値までエントリを設定できます。エントリ間で入出力インタフェースの重複が多い場合は，「表 3-78　IGMP/MLD 動作インタフェース数に対するマルチキャスト入出力ポート数」に示す値より多くのエントリを設定できることがあります。

なお，入出力ポート数は IPv4 と IPv6 を同時動作させた場合，IPv4 と IPv6 のエントリの合計となります。

注※3

マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 3-83　使用インタフェース数に対する MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM を連動させる設定可能数」および「表 3-84　加入グループ数に対する MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。加入グループ数は，動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合，加入グループ数は一つではなく，加入したインタフェースの数になります。

注※4

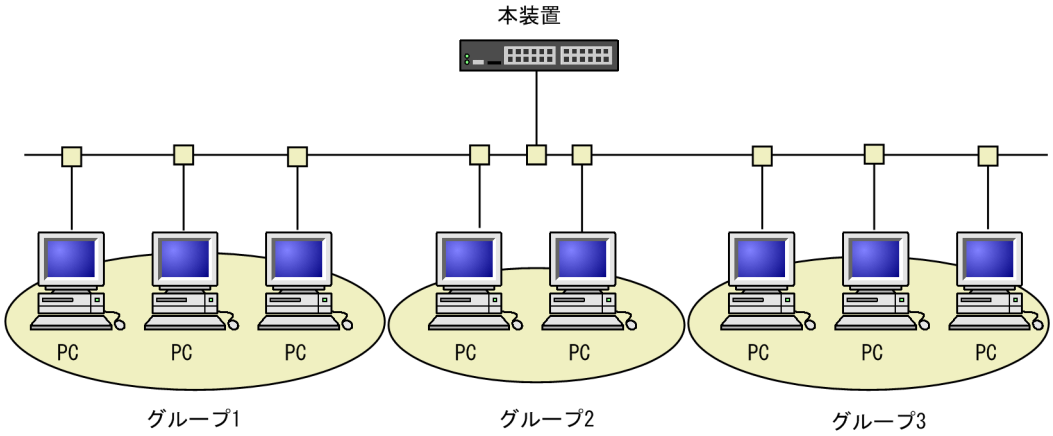
一つの Report メッセージで処理できるソース数は延べ 1024 ソースまでです。ソース情報のない record も 1 ソースとして数えます。

MLDv2（EXCLUDE モード）で PIM-SSM を連携動作させる設定をした場合，その設定に一致した EXCLUDE record で定義されているソース数を数えます。また，受信した Report メッセージ内に EXCLUDE record が複数存在し，MLDv2（EXCLUDE モード）で PIM-SSM を連携動作させる設定で追加したソース数が延べ 1024 を超えた場合，以降のそのメッセージ内の EXCLUDE record で，連携動作の対象となる EXCLUDE record についてマルチキャスト中継情報は作成しません。

注※5

本装置に直接接続しているグループの数を示します。MLDv2 使用時に送信元を指定する場合のグループ数は，送信元とグループの組み合わせの数となります。「図 3-2　マルチキャストグループ数の例」の例では 3 です。インタフェース当たりの加入可能グループ数については，「表 3-85　IPv6 でのインタフェース当たりの加入可能グループ数」を参照してください。

図 3-2　マルチキャストグループ数の例



注※6

本装置のグローバルネットワークとすべての VRF に接続するネットワーク（VPN）上の総数です。

注※7

静的加入グループ数とは，各マルチキャストインタフェースで静的加入するグループアドレスの総数です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合，静的加入グループ数は一つではなく，静的加入設定したインタフェースの数になります。一つのインタフェースに設定できる静的加入グループ数は 256 までです。

注※8

グローバルでマルチキャストを設定している場合，31 になります。

注※9

すべての route-map で指定した access-list 内のアドレスの延べ数です。

注※10

エクストラネットで指定した route-map を使用します。route-map に指定した access-list 内で，ホストアドレス（128 ビットマスク）として指定したマルチキャストアドレスが対象となります。

装置当たりの上限は，すべての VRF で指定した PIM-SM VRF ゲートウェイのグループアドレスの延べ数です。

また，静的加入グループ数で指定したグループアドレス数との合計になります。

表 3-83　使用インタフェース数に対する MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM を連動させる設定可能数

使用インタフェース数	MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM を連動させる設定可能数
31	256
63	128
127	64

表 3-84　加入グループ数に対する MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM を連動させる設定可能数

加入グループ（延べ数）	MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM を連動させる設定数
64	256
128	128
256	64
512	32
1024	16
2048	8
4096	4
8128	2

表 3-85　IPv6 でのインタフェース当たりの加入可能グループ数

使用インタフェース数	インタフェース当たりの加入可能グループ数
31	256
63	128
127	64

3.14　BFD

BFD セッションの収容条件を次の表に示します。

表 3-86　BFD セッションの収容条件

項目	装置当たりの数
BFD セッション数	50

3.15　VRF【SL-L3A】

設定できる VRF 数を次の表に示します。VRF 設定可能数にグローバルネットワークは含みません。

表 3-87　設定できる VRF 数

項目	装置当たりの数
VRF 設定可能数	255

4 装置へのログイン

この章では，装置の起動と停止，およびログイン・ログアウト，運用管理の概要，運用端末とその接続形態について説明します。

4.1　運用端末による管理

本装置の運用にはコンソールまたはリモート運用端末が必要です。コンソールは RS232C に接続する端末，リモート運用端末は IP ネットワーク経由で接続する端末です。また，本装置は IP ネットワーク経由で SNMP マネージャによるネットワーク管理にも対応しています。コンソールやリモート運用端末など本装置の運用管理を行う端末を運用端末と呼びます。

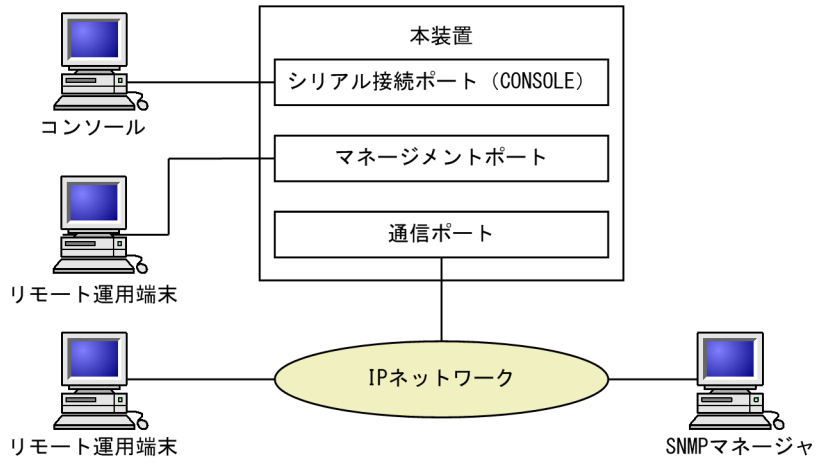
4.1.1　運用端末の接続形態

コンソールは本装置のシリアル接続ポート（CONSOLE）に接続します。また，リモート運用端末は次に示す接続形態がとれます。

- マネージメントポートに接続する形態
- 通信ポートが接続する IP ネットワークから接続する形態

運用端末の接続形態を次の図に示します。

図 4-1　運用端末の接続形態



(1)　シリアル接続ポート（CONSOLE）

シリアル接続ポート（CONSOLE）にコンソールを接続します。コンフィグレーションを設定していなくても本ポートを経由してログインできるため，初期導入時には本ポートからログインして，初期設定ができます。

(2)　マネージメントポート

マネージメントポートを経由して，遠隔のリモート運用端末からの本装置に対するログインや SNMP マネージャによるネットワーク管理ができます。このポートを経由して telnet，ssh，ftp などによって本装置へログインするためには，本装置のコンフィグレーションで IP アドレスおよびリモートアクセスの設定をする必要があります。

(3)　通信用ポート

マネージメントポートと同様の運用ができます。

4.1.2　運用端末

コンソールとリモート運用端末の運用管理での適用範囲の違いを次の表に示します。

表 4-1　コンソールとリモート運用端末の運用管理での適用範囲の違い

運用機能	コンソール	リモート運用端末
遠隔からのログイン	不可	可
本装置から運用端末へのログイン	不可	可
アクセス制御	なし	あり
コマンド入力	可	可
ファイル転送方式	zmodem 手順	ftp
IP 通信	不可	IPv4 および IPv6
SNMP マネージャ接続	不可	可
コンフィグレーション設定	不要	必要

(1)　コンソール

コンソールは RS232C に接続する端末で，一般的な通信端末，通信ソフトウェアが使用できます。コンソールが本装置と通信できるように，次の標準 VT-100 設定値（本装置のデフォルト設定値）が通信ソフトウェアに設定されていることを確認してください。

- 通信速度：9600bit/s
- データ長：8 ビット
- パリティビット：なし
- ストップビット：1 ビット
- フローコントロール：なし

なお，通信速度を 9600bit/s 以外（1200／2400／4800／19200bit/s）で設定して使用したい場合は，コンフィグレーションコマンド speed で本装置側の通信速度設定を変更してください。ただし，実際に設定が反映されるのはコンソールからいったんログアウトしたあとになります。

図 4-2　コンソールの通信速度の設定例

```
(config)# line console 0
(config-line)# speed 19200
```

スタック構成で運用している装置にコンソールからログインする場合，シリアル接続しているメンバスイッチにログインします。マスタスイッチとシリアル接続しているときはマスタスイッチに，バックアップスイッチとシリアル接続しているときはバックアップスイッチにログインします。

注意

コンソールを使用する場合は次の点に注意してください。

- 本装置ではコンソール端末からログインする際に，自動的に VT-100 の制御文字を使用して画面サイズを取得・設定します。VT-100 に対応していないコンソール端末では，不正な文字列が表示されたり，最初の CLI プロンプトがずれて表示されたりして，画面サイズが取得・設定できません。

また，ログインと同時にキー入力した場合，VT-100 の制御文字の表示結果が正常に取得できないため同様の現象となりますのでご注意ください。この場合は，再度ログインし直してください。

- 通信速度の設定が反映されるのは，ログアウトしたあとになります。コンソールからいったんログアウトしたあとで，使用している通信端末や通信ソフトウェアの通信速度の設定を変更してください。変更するまでは文字列が不正な表示になります（「login」プロンプトなど）。
- 通信速度を 9600bit/s 以外に設定して運用している場合，装置を起動（再起動）するとコンフィグレーションが装置に反映されるまでの間，不正な文字列が表示されます。

(2)　リモート運用端末

本装置に IP ネットワーク経由で接続してコマンド操作を行う端末が，リモート運用端末です。telnet プロトコルまたは ssh プロトコルのクライアント機能がある端末はリモート運用端末として使用できます。

注意

本装置の telnet サーバは，改行コードとして[CR]を認識します。一部のクライアント端末では，改行コードとして[CR]および[LF]を送信します。これらの端末から接続した場合，空行が表示されたり，(y/n）確認時にキー入力ができなかったりするなどの現象がおこります。このような場合は，各クライアント端末の設定を確認してください。

4.1.3　運用管理機能の概要

本装置はセットアップ作業が終了し，装置の電源 ON で運用に入ります。本装置と接続した運用端末では，運用コマンドやコンフィグレーションコマンドを実行し，装置の状態を調べたり，接続ネットワークの変更に伴うコンフィグレーションの変更を実施したりできます。本装置で実施する運用管理の種類を次の表に示します。

表 4-2　運用管理の種類

運用機能	概要
コマンド入力機能	コマンドラインによる入力を受け付けます。
ログイン制御機能	不正アクセス防止，パスワードチェックを行います。
コンフィグレーション編集機能	運用のためのコンフィグレーションを設定します。設定された情報はすぐ運用に反映されます。
ネットワークコマンド機能	リモート操作コマンドなどをサポートします。
ログ・統計情報	過去に発生した障害情報および回線使用率などの統計情報を表示します。
LED および障害部位の表示	LED によって本装置の状態を表示します。
MIB 情報収集	SNMP マネージャによるネットワーク管理を行います。
装置保守機能	装置を保守するための状態表示，装置とネットワークの障害を切り分けるための回線診断などのコマンドを持ちます。
MC 保守機能	MC のフォーマットなどを行います。

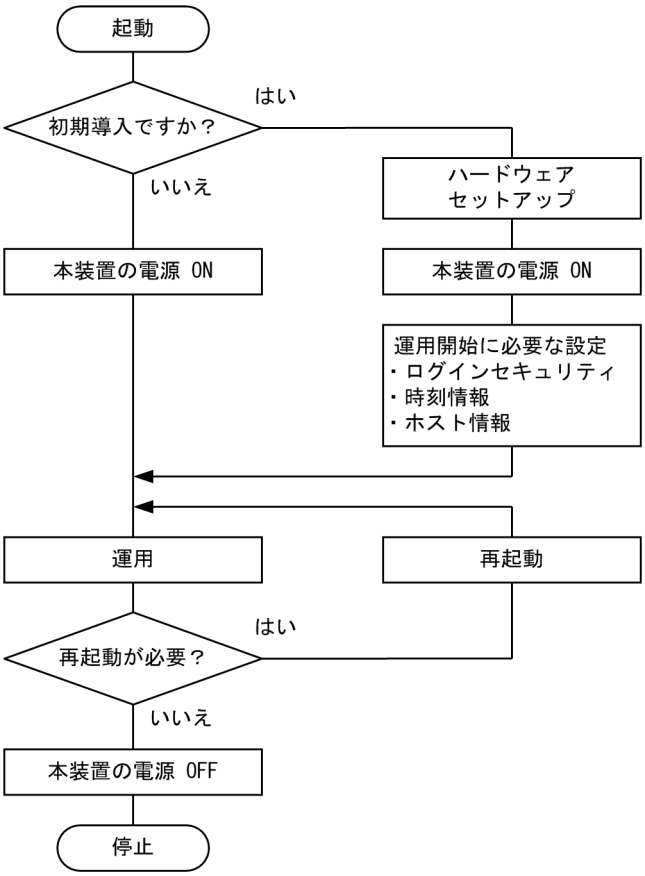
4.2　装置起動

この節では，装置の起動と停止について説明します。

4.2.1　起動から停止までの概略

本装置の起動から停止までの概略フローを次の図に示します。ハードウェアセットアップの内容については「ハードウェア取扱説明書」を参照してください。

図 4-3　起動から停止までの概略フロー



4.2.2　装置の起動

本装置の起動，再起動の方法を次の表に示します。

表 4-3　起動，再起動の方法

起動の種類	内容	操作方法
電源 ON による起動	本装置の電源 OFF からの立ち上げです。	電源機構に電源ケーブルを取り付けることで電源を ON にします。
リセットによる再起動	障害発生などにより，本装置をリセットしたい場合に行います。	本体のリセットスイッチを押します。

起動の種類	内容	操作方法
コマンドによる再起動	障害発生などにより，本装置をリセットしたい場合に行います。	reload コマンドを実行します。
デフォルト リスタート	パスワードを忘れてログインできない場合や，コマンド承認の設定ミスなどでコンソールからコマンドが実行できなくなった場合に行います。 パスワードによるログイン認証，装置管理者モードへの変更（enable コマンド）時の認証，およびコマンド承認を行いませんのでデフォルトリスタートによる起動を行う場合は十分に注意してください。なお，アカウント，コンフィグレーションはデフォルトリスタート前のものが使用されます。 また，ログインユーザ名を忘れると，デフォルトリスタートで起動してもログインできないので注意してください。 デフォルトリスタート中に設定したパスワードは，装置再起動後に有効になります。	本体のリセットスイッチを５秒以上押します。

本装置を起動，再起動したときに STATUS ランプが赤点灯となった場合は，「トラブルシューティングガイド」を参照してください。また，LED ランプ表示内容の詳細は，「ハードウェア取扱説明書」を参照してください。

本装置は，ソフトウェアイメージを k.img という名称で書き込んだ MC をスロットに挿入して起動した場合，MC から起動します。MC から装置を起動した場合，アカウント，コンフィグレーションは工場出荷時の初期状態となり，設定しても保存することはできません。通常運用時は MC から起動しないでください。

4.2.3　装置の停止

本装置の電源を OFF にする場合は，アクセス中のファイルが壊れるおそれがあるので，本装置にログインしているユーザがいない状態で行ってください。運用コマンド reload stop で装置を停止させたあとに電源を OFF にすることを推奨します。本装置に搭載されているすべての電源機構から電源ケーブルを取り外すことで，電源を OFF にできます。

4.3　ログイン・ログアウト

この節では，ログインとログアウトについて説明します。

(1)　ログイン

装置が起動すると, ログイン画面を表示します。この画面でユーザ名とパスワードを入力してください。正しく認証された場合は，コマンドプロンプトを表示します。また，認証に失敗した場合は”Login incorrect”のメッセージを表示し，ログインできません。ログイン画面を次の図に示します。

なお，初期導入時には，ユーザ名 operator でパスワードなしでログインができます。

図 4-4　ログイン画面

```
login: operator
Password:                                                              …1
No password is set. Please set password!                               …2

Copyright (c) 20XX ALAXALA Networks Corporation. All rights reserved.

>                                                                      …3
```

1. パスワードが設定されていない場合は改行だけでログインができます。
   また，パスワードの入力文字は表示しません。
2. 本装置に設定したパスワード未設定のログインユーザ（operator も含む）でログインした場合に表示されます。
3. コマンドプロンプトを表示します。

(2)　ログアウト

CLI での操作を終了してログアウトしたい場合は logout コマンドまたは exit コマンドを実行してください。ログアウト画面を次の図に示します。

図 4-5　ログアウト画面

```
> logout
login:
```

(3)　自動ログアウト

一定時間（デフォルト：60 分）内にキーの入力がなかった場合，自動的にログアウトします。なお，自動ログアウト時間はコンフィグレーションコマンド username，または運用コマンド set exec-timeout で変更できます。

5 コマンド操作

この章では，本装置でのコマンドの指定方法について説明します。

5.1　コマンド入力モード

5.1.1　運用コマンド一覧

コマンド入力モードの切り換えおよびユーティリティに関する運用コマンド一覧を次の表に示します。

表 5-1　運用コマンド一覧

コマンド名	説明
enable	コマンド入力モードを一般ユーザモードから装置管理者モードに変更します。
disable	コマンド入力モードを装置管理者モードから一般ユーザモードに変更します。
quit	現在のコマンド入力モードを終了します。
exit	現在のコマンド入力モードを終了します。
logout	装置からログアウトします。
configure (configure terminal)	コマンド入力モードを装置管理者モードからコンフィグレーションコマンドモードに変更して，コンフィグレーションの編集を開始します。
diff※	指定した二つのファイル同士を比較し，相違点を表示します。
grep※	指定したファイルを検索して，指定したパターンを含む行を出力します。
more※	指定したファイルの内容を一画面分だけ表示します。
less※	指定したファイルの内容を一画面分だけ表示します。
tail※	指定したファイルの指定された位置以降を出力します。
hexdump※	ヘキサダンプを表示します。

注※
「運用コマンドレファレンス Vol.1」「10　ユーティリティ」を参照してください。

5.1.2　コマンド入力モード

本装置でコンフィグレーションの変更を実施したり，または装置の状態を参照したりする場合，適切なコマンド入力モードに遷移し，コンフィグレーションコマンドや運用コマンドを入力する必要があります。また，CLI プロンプトでコマンド入力モードを識別できます。

コマンド入力モードとプロンプトの対応を次の表に示します。

表 5-2　コマンド入力モードとプロンプトの対応

コマンド入力モード	実行可能なコマンド	プロンプト
一般ユーザモード	運用コマンド（configure，adduser コマンドなど，一部のコマンドは装置管理者モードでだけ実行可能です。）	>
装置管理者モード		#
コンフィグレーションコマンドモード	コンフィグレーションコマンド※	(config)#

注※

コンフィグレーションの編集中に運用コマンドを実行したい場合，quit コマンドや exit コマンドによってコマンド入力モードを装置管理者モードに切り替えなくても，運用コマンドの先頭に「$」を付けた形式で入力することで実行できます。

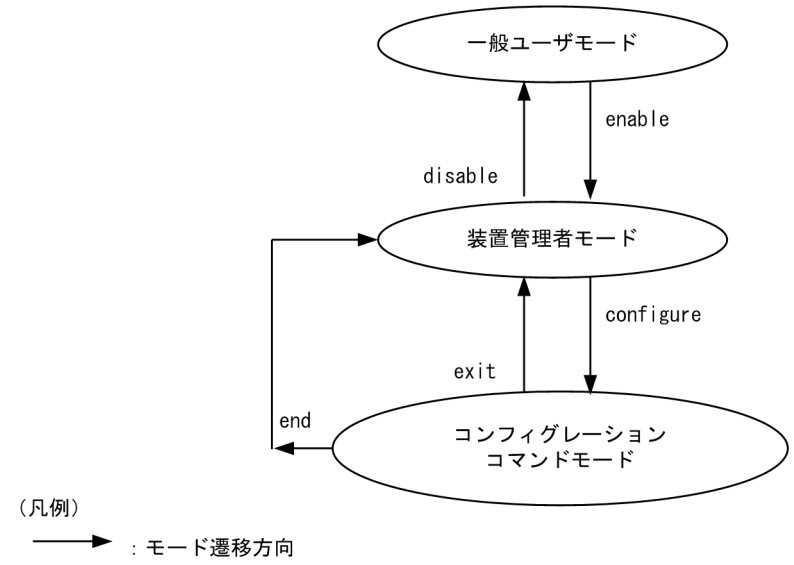
＜例＞

コンフィグレーションコマンドモードで運用コマンド show ip arp を実行する場合

```
(config)# $show ip arp
```

モード遷移の概要を次の図に示します。

図 5-1　モード遷移の概要



また，CLI プロンプトとして，次に示す場合でも，その状態を意味する文字がプロンプトの先頭に表示されます。

1. コンフィグレーションコマンド hostname でホスト名称を設定している場合，ホスト名称の先頭から 20 文字目までがプロンプトに反映されます。
2. ランニングコンフィグレーションを編集し，その内容をスタートアップコンフィグレーションに保存していない場合，プロンプトの先頭に「！」が付きます。

1.～2.のプロンプト表示例を次の図に示します。

図 5-2　プロンプト表示例

```
> enable
# configure
(config)# hostname "OFFICE1"
!OFFICE1(config)# save
OFFICE1(config)# quit
OFFICE1# quit
OFFICE1>
```

5.2 CLI での操作

5.2.1 補完機能

コマンドライン上で［Tab］を入力することで，コマンド入力時のコマンド名称やファイル名の入力を少なくすることができ，コマンド入力が簡単になります。補完機能を使用したコマンド入力の簡略化を次の図に示します。

図 5-3 補完機能を使用したコマンド入力の簡略化

```
(config)# in[Tab]
(config)# interface
```

［Tab］押下で使用できるパラメータやファイル名の一覧が表示されます。

```
(config)# interface [Tab]
gigabitethernet     port-channel        tengigabitethernet
loopback            range               vlan
(config)# interface
```

5.2.2 ヘルプ機能

コマンドライン上で［?］を入力することで，指定できるコマンドまたはパラメータを検索できます。また，コマンドやパラメータの意味を知ることができます。次の図に［?］入力時の表示例を示します。

図 5-4 ［?］入力時の表示例

```
> show vlan ?
  <vlan id list>        1 to 4094 ex. "5", "10-20" or "30,40"
  channel-group-number  Display the VLAN information specified by
                        channel-group-number
  detail                Display the detailed VLAN information
  list                  Display the list of VLAN information
  mac-vlan              Display the MAC VLAN information
  port                  Display the VLAN information specified by port number
  summary               Display the summary of VLAN information
  <cr>
> show vlan
```

なお，パラメータの入力途中でスペース文字を入れないで［?］を入力した場合は，補完機能が実行されます。また，コマンドパラメータで?文字を使用する場合は，［Ctrl］＋［V］を入力後，［?］を入力してください。

5.2.3 入力エラー位置指摘機能

コマンドまたはパラメータを不正に入力した際，エラー位置を「 ^ 」で指摘し，次行にエラーメッセージ（「運用コマンドレファレンス Vol.1」「入力エラー位置指摘で表示するメッセージ」を参照）を表示します。［Tab］入力時と［?］入力時も同様となります。

「 ^ 」の指摘個所とエラーメッセージの説明によって，コマンドまたはパラメータを見直して再度入力してください。入力エラー位置指摘の表示例を「図 5-5 スペルミスをしたときの表示例」および「図 5-6 パラメータ入力途中の表示例」に示します。

図 5-5 スペルミスをしたときの表示例

```
(config)# interface gigabitehternet 1/0/1
interface gigabitehternet 1/0/1
                  ^
% illegal parameter at '^' marker
(config)# interface gigabitehternet 1/0/1
```

図 5-6　パラメータ入力途中の表示例

```
(config)# interface gigabitethernet 1/0/1
(config-if)# speed
speed
      ^
% Incomplete command at '^' marker
(config-if)#
```

5.2.4　コマンド短縮実行

コマンドまたはパラメータを短縮して入力し，入力された文字が一意のコマンドまたはパラメータとして認識できる場合，コマンドを実行します。短縮入力のコマンド実行例を次の図に示します。

図 5-7　短縮入力のコマンド実行例（show ip arp の短縮入力）

```
> sh ip ar
Date 20XX/11/15 19:37:02 UTC
Total: 1 entries
 IP Address       Linklayer Address  Netif             Expire     Type
 192.168.0.1      0012.e2d0.e9f5     VLAN0010          3h44m57s   arpa
>
```

なお，「表 6-1　コンフィグレーションコマンド一覧」にあるコンフィグレーションの編集および操作に関するコマンドは，コンフィグレーションモードの第一階層以外で短縮実行できません。

また，*を含むパラメータを指定した場合は，それ以降のパラメータについて短縮実行できません。

5.2.5　ヒストリ機能

ヒストリ機能を使用すると，過去に入力したコマンドを簡単な操作で再実行したり，過去に入力したコマンドの一部を変更して再実行したりできます。ヒストリ機能を使用した例を次の図に示します。

図 5-8　ヒストリ機能を使用したコマンド入力の簡略化

```
> ping 192.168.0.1 numeric count 1                          …1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.329 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 1.329/1.329/1.329 ms
>                                                           …2
> ping 192.168.0.1 numeric count 1                          …3
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.225 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 1.225/1.225/1.225 ms
>                                                           …4
> ping 192.168.0.2 numeric count 1                          …5
PING 192.168.0.2 (192.168.0.2): 56 data bytes

--- 192.168.0.2 PING Statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
>
```

1. 192.168.0.1 に対して ping コマンドを実行します。
2. [↑] キーを入力することで前に入力したコマンドを呼び出せます。
   この例の場合，[↑] キーを 1 回押すと「ping 192.168.0.1 numeric count 1」が表示されるので，[Enter] キーの入力だけで同じコマンドを再度実行できます。
3. 192.168.0.1 に対して ping コマンドを実行します。

4. [↑] キーを入力することで前に入力したコマンドを呼び出し，[←] キーおよび [Backspace] キーを使ってコマンド文字列を編集できます。

   この例の場合，[↑] キーを 1 回押すと「ping 192.168.0.1 numeric count 1」が表示されるので，IP アドレスの「1」の部分を「2」に変更して [Enter] キーを入力しています。

5. 192.168.0.2 に対して ping コマンドを実行します。

ヒストリ機能に次の表に示す文字列を使用した場合，コマンド実行前に過去に実行したコマンド文字列に変換したあとにコマンドを実行します。なお，コンフィグレーションコマンドでは，コマンド文字列変換はサポートしていません。

表 5-3　ヒストリのコマンド文字列変換で使用できる文字一覧

項番	指定	説明
1	!!	直前に実行したコマンドへ変換して実行します。
2	!n	ヒストリ番号 n※のコマンドへ変換して実行します。
3	!-n	n 回前のコマンドへ変換して実行します。
4	!str	文字列 str で始まる過去に実行した最新のコマンドへ変換して実行します。
5	^str1^str2	直前に実行したコマンドの文字列 str1 を str2 に置換して実行します。

注※

運用コマンド show history で表示される配列番号のこと。

また，過去に実行したコマンドを呼び出して，コマンド文字列を編集したり，[Backspace] キーや [Ctrl] ＋ [C] キーで消去したりしたあと，再度コマンドを呼び出すと，該当コマンドのヒストリを編集したり消去したりできます。

注意

通信ソフトウェアによって方向キー（[↑]，[↓]，[←]，[→]）を入力してもコマンドが呼び出されない場合があります。その場合は，通信ソフトウェアのマニュアルなどで設定を確認してください。

5.2.6　パイプ機能

パイプ機能を利用することによって，コマンドの実行結果を別のコマンドに引き継ぐことができます。実行結果を引き継ぐコマンドに grep コマンドを使うことによって，コマンドの実行結果をよりわかりやすくすることができます。ただし，コマンドが実行できなかった場合などに表示される応答メッセージは，引き継ぎをしないで，そのタイミングで画面に表示されます。「図 5-9　show sessions コマンド実行結果」に show sessions コマンドの実行結果を，「図 5-10　show sessions コマンド実行結果を grep コマンドでフィルタリング」に show sessions コマンドの実行結果を grep コマンドでフィルタリングした結果を示します。

図 5-9　show sessions コマンド実行結果

```
> show sessions
Date 20XX/01/07 12:00:00 UTC
operator console  -----  0   Jan  6 14:16
operator ttyp0    -----  2   Jan  6 14:16 (192.168.3.7)
operator ttyp1    -----  3   Jan  6 14:16 (192.168.3.7)
operator ttyp2    admin  4   Jan  6 14:16 (192.168.3.7)
```

図 5-10　show sessions コマンド実行結果を grep コマンドでフィルタリング

```
> show sessions | grep admin
operator ttyp2    admin  4   Jan  6 14:16 (192.168.3.7)
>
```

5.2.7　リダイレクト

リダイレクト機能を利用することによって，コマンドの実行結果をファイルに出力できます。ただし，コマンドが実行できなかった場合などに表示される応答メッセージは，ファイルに出力しないで，そのタイミングで画面に表示されます。show ip interface コマンドの実行結果をファイルに出力する例を次の図に示します。

図 5-11　show ip interface コマンド実行結果をファイルに出力

```
> show ip interface > show_interface.log
>
```

5.2.8　ページング

コマンドの実行により出力される結果について，表示すべき情報が一画面にすべて表示しきれない場合は，ユーザのキー入力を契機に一画面ごとに区切って表示します。ただし，リダイレクトがあるときにはページングを行いません。なお，ページングはコンフィグレーションコマンド username，または運用コマンド set terminal pager でその機能を有効にしたり無効にしたりできます。

5.2.9　CLI 設定のカスタマイズ

自動ログアウト機能や CLI 機能の一部は，CLI 環境情報としてユーザごとに動作をカスタマイズできます。カスタマイズ可能な CLI 機能と CLI 環境情報を次の表に示します。

表 5-4　カスタマイズ可能な CLI 機能と CLI 環境情報

機能	カスタマイズ内容と初期導入時のデフォルト設定
自動ログアウト	自動ログアウトするまでの時間を設定できます。 初期導入時のデフォルト設定は，60 分です。
ページング	ページングするかどうかを設定できます。 初期導入時のデフォルト設定は，ページングをします。
ヘルプ機能	ヘルプメッセージで表示するコマンドの一覧を設定できます。 初期導入時のデフォルト設定は，運用コマンドのヘルプメッセージを表示する際に，入力可能なすべての運用コマンドの一覧を表示します。

これらの CLI 環境情報は，ユーザごとに，コンフィグレーションコマンド username，または次に示す運用コマンドで設定できます。

- set exec-timeout
- set terminal pager
- set terminal help

コンフィグレーションコマンド username による設定は，運用コマンドによる設定よりも優先されます。三つの CLI 環境情報のうち，どれか一つでもコンフィグレーションコマンドで設定した場合，その対象ユーザには，運用コマンドによる設定値は使用されません。コンフィグレーションコマンドの設定値または省略時の初期値で動作します。

運用コマンドによる設定は，コンフィグレーションコマンドによる設定がない場合に使用されます。コンフィグレーションコマンドで一つも CLI 環境情報を設定していないユーザは，運用コマンドによる設定値が使用されます。なお，運用コマンドによる設定では，設定状態を表示できないため，各機能の動作状態で確認してください。

運用コマンドによる設定内容は，コマンドが実行されたセッションでは実行直後から動作に反映されます。同一ユーザでも別セッションの場合は，次回ログイン時に反映されます。また，コンフィグレーションコマンドによる設定で動作している場合でも，一時的に実行された該当セッションでの動作を変更できます。

なお，運用コマンドによる設定の場合，adduser コマンドで no-flash パラメータを指定して追加したアカウントのユーザは，装置を再起動したときに，CLI 環境情報が初期導入時のデフォルト設定に戻ります。

5.3　CLI の注意事項

(1)　ログイン後に運用端末がダウンした場合

ログイン後に運用端末がダウンした場合，本装置内ではログインしたままの状態になっていることがあります。この場合，自動ログアウトを待つか，再度ログインし直して，ログインしたままの状態になっているユーザを運用コマンド killuser で削除してください。

(2)　CLI の特殊キー操作に関する注意事項

［Ctrl］＋［C］キー，［Ctrl］＋［Z］キー，［Ctrl］＋［\］キーのどれかを押した場合に，ごくまれにログアウトする場合があります。その場合は，再度ログインしてください。

6 コンフィグレーション

本装置には，ネットワークの運用環境に合わせて，構成および動作条件などのコンフィグレーションを設定しておく必要があります。この章では，コンフィグレーションを設定するのに必要なことについて説明します。

6.1　コンフィグレーション

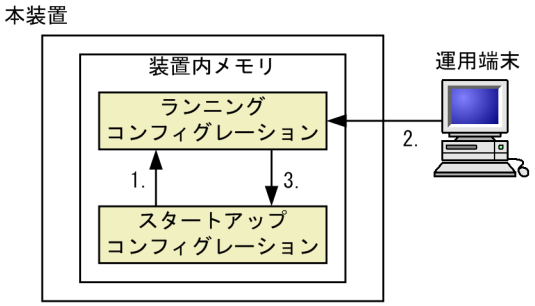
運用開始時または運用中，ネットワークの運用環境に合わせて，本装置に接続するネットワークの構成および動作条件などのコンフィグレーションを設定する必要があります。初期導入時，コンフィグレーションは設定されていません。

6.1.1　起動時のコンフィグレーション

本装置の電源を入れると，装置内メモリ上のスタートアップコンフィグレーションファイルが読み出され，設定されたコンフィグレーションに従って運用を開始します。運用に使用されているコンフィグレーションをランニングコンフィグレーションと呼びます。

なお，スタートアップコンフィグレーションは，直接編集できません。ランニングコンフィグレーションを編集したあとに save(write)コマンドを使用することで，スタートアップコンフィグレーションが更新されます。起動時，および運用中のコンフィグレーションの概要を次の図に示します。

図 6-1　起動時，および運用中のコンフィグレーションの概要



1. 本装置を起動すると，装置内メモリのスタートアップコンフィグレーションが読み出され，
   ランニングコンフィグレーションとしてロードされる。
   ランニングコンフィグレーションの内容で運用を開始する。
2. コンフィグレーションを変更した場合は，ランニングコンフィグレーションに反映される。
3. 変更されたランニングコンフィグレーションをスタートアップコンフィグレーションに
   保存する。

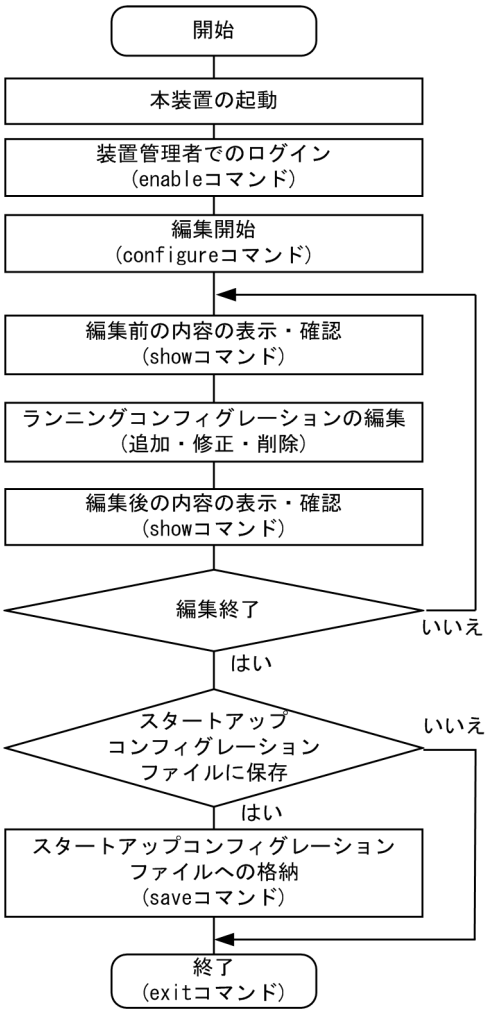
6.1.2　運用中のコンフィグレーション

運用中にコンフィグレーションを編集すると，編集した内容はランニングコンフィグレーションとしてすぐに運用に反映されます。save(write)コマンドを使用することで，ランニングコンフィグレーションが装置内メモリにあるスタートアップコンフィグレーションに保存されます。編集した内容を保存しないで装置を再起動すると，編集した内容が失われるので注意してください。

6.2　ランニングコンフィグレーションの編集概要

初期導入時やネットワーク構成を変更する場合は，ランニングコンフィグレーションを編集します。なお，初期導入時のランニングコンフィグレーションの編集はコンソールから行う必要があります。ランニングコンフィグレーションの編集の流れを次の図に示します。詳細については，「6.4　コンフィグレーションの編集方法」を参照してください。

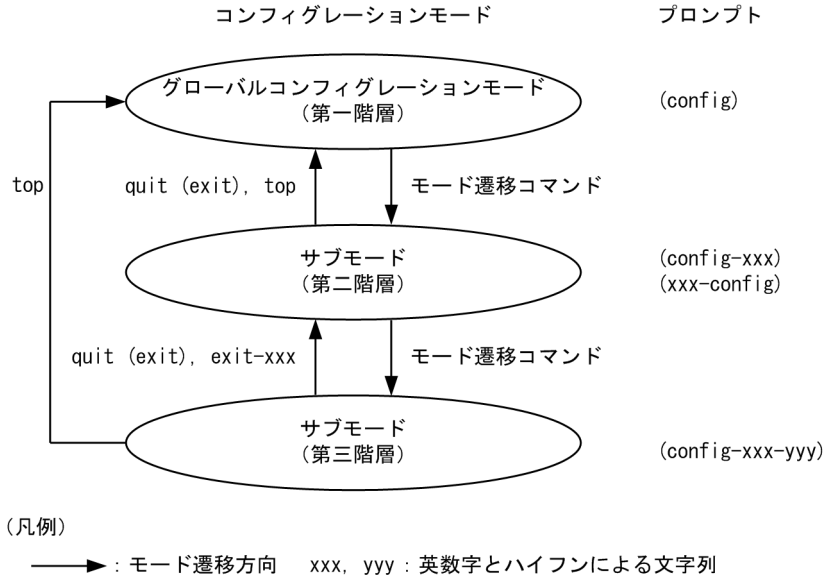
図 6-2　ランニングコンフィグレーションの編集の流れ



6.3　コンフィグレーションコマンド入力におけるモード遷移

コンフィグレーションは，実行可能なコンフィグレーションモードで編集します。第二階層のコンフィグレーションを編集する場合は，グローバルコンフィグレーションモードで第二階層のコンフィグレーションモードに移行するためのコマンドを実行してモードを移行した上で，コンフィグレーションコマンドを実行する必要があります。コンフィグレーションのモード遷移の概要を次の図に示します。

図 6-3　コンフィグレーションのモード遷移の概要



（凡例）

：モード遷移方向　xxx，yyy：英数字とハイフンによる文字列

6.4　コンフィグレーションの編集方法

6.4.1　コンフィグレーション・運用コマンド一覧

コンフィグレーションの編集および操作に関するコンフィグレーションコマンド一覧を次の表に示します。

表 6-1　コンフィグレーションコマンド一覧

コマンド名	説明
end	コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。
quit (exit)	モードを一つ戻ります。グローバルコンフィグレーションモードで編集中の場合は，コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。
save (write)	編集したコンフィグレーションをスタートアップコンフィグレーションに保存します。
show	編集中のコンフィグレーションを表示します。
status	編集中のコンフィグレーションの状態を表示します。
top	コンフィグレーションコマンドモードの第二階層以下からグローバルコンフィグレーションモード（第一階層）に戻ります。

コンフィグレーションの編集および操作に関する運用コマンド一覧を次の表に示します。

表 6-2　運用コマンド一覧

コマンド名	説明
show running-config	ランニングコンフィグレーションを表示します。
show startup-config	スタートアップコンフィグレーションを表示します。
copy	コンフィグレーションをコピーします。
erase configuration	ランニングコンフィグレーションの内容を初期導入時のものに戻します。
show file	ローカルまたはリモートサーバ上のファイルの内容と行数を表示します。
cd	現在のディレクトリ位置を移動します。
pwd	カレントディレクトリのパス名を表示します。
ls	ファイルおよびディレクトリを表示します。
dir	復元可能な形式で削除された本装置用のファイルの一覧を表示します。
cat	指定されたファイルの内容を表示します。
cp	ファイルをコピーします。
mkdir	新しいディレクトリを作成します。
mv	ファイルの移動およびファイル名の変更をします。
rm	指定したファイルを削除します。
rmdir	指定したディレクトリを削除します。

コマンド名	説明
delete	本装置用のファイルを復元可能な形式で削除します。
undelete	復元可能な形式で削除された本装置用のファイルを復元します。
squeeze	復元可能な形式で削除された本装置用の deleted ファイルを完全に消去します。
zmodem	本装置と RS232C で接続されているコンソールとの間でファイル転送をします。

6.4.2　configure（configure terminal）コマンド

コンフィグレーションを編集する場合は，enable コマンドを実行して装置管理者モードに移行してください。装置管理者モードで，configure コマンドまたは configure terminal コマンドを入力すると，プロンプトが「(config)#」になり，ランニングコンフィグレーションの編集が可能となります。ランニングコンフィグレーションの編集開始例を次の図に示します。

図 6-4　ランニングコンフィグレーションの編集開始例

```
> enable                  …1
# configure               …2
(config)#
```

1. enable コマンドで装置管理者モードに移行します。
2. ランニングコンフィグレーションの編集を開始します。

6.4.3　コンフィグレーションの表示・確認（show コマンド）

(1)　スタートアップコンフィグレーション，ランニングコンフィグレーションの表示・確認

装置管理者モードで運用コマンド show running-config／show startup-config を使用することで，ランニングコンフィグレーションおよびスタートアップコンフィグレーションを表示･確認できます。ランニングコンフィグレーションの表示例を次の図に示します。

図 6-5　ランニングコンフィグレーションの表示例

```
OFFICE01# show running-config                    …1
#default configuration file for XXXXXX-XX
!
hostname "OFFICE01"
switch 1 provision 3660-24t4xw
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01#
```

1. ランニングコンフィグレーションを表示します。

(2)　コンフィグレーションの表示・確認

コンフィグレーションモードで show コマンドを使用することで，編集前，編集後のコンフィグレーションを表示・確認できます。コンフィグレーションを表示した例を「図 6-6　コンフィグレーションの内容をすべて表示」～「図 6-9　インタフェースモードで指定のインタフェース情報を表示」に示します。

図 6-6　コンフィグレーションの内容をすべて表示

```
OFFICE01(config)# show                  …1
#default configuration file for XXXXXX-XX
!
hostname "OFFICE01"
switch 1 provision 3660-24t4xw
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01(config)#
```

1.パラメータを指定しない場合はランニングコンフィグレーションを表示します。

図 6-7　設定済みのすべてのインタフェース情報を表示

```
OFFICE01(config)# show interface gigabitethernet        …1
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 1/0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01(config)#
```

1.ランニングコンフィグレーションのうち，設定済みのすべてのインタフェースを表示します。

図 6-8　指定のインタフェース情報を表示

```
OFFICE01(config)# show interface gigabitethernet 1/0/1       …1
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
OFFICE01(config)#
```

1.ランニングコンフィグレーションのうち，インタフェース 1/0/1 を表示します。

図 6-9　インタフェースモードで指定のインタフェース情報を表示

```
OFFICE01(config)# interface gigabitethernet 1/0/1
OFFICE01(config-if)# show                                …1
interface gigabitethernet 1/0/1
  switchport mode access
  switchport access vlan 100
!
OFFICE01(config-if)#
```

1. ランニングコンフィグレーションのうち，インタフェース 1/0/1 を表示します。

6.4.4 コンフィグレーションの追加・変更・削除

(1) コンフィグレーションコマンドの入力

コンフィグレーションコマンドを使用して，コンフィグレーションを編集します。また，コンフィグレーションのコマンド単位での削除は，コンフィグレーションコマンドの先頭に「no」を指定することで実現できます。

ただし，機能の抑止を設定するコマンドでは，コンフィグレーションコマンドの先頭に「no」を指定して設定し，機能の抑止を解除する場合は「no」を外したコンフィグレーションコマンドを入力します。

コンフィグレーションの編集例を「図 6-10　コンフィグレーションの編集例」に，機能の抑止および解除の編集例を「図 6-11　機能の抑止および解除の編集例」に示します。

図 6-10　コンフィグレーションの編集例

```
(config)# vlan 100                                  …1
(config-vlan)# state active                         …2
(config-vlan)# exit
(config)# interface gigabitethernet 1/0/1           …3
(config-if)# switchport mode access                 …4
(config-if)# switchport access vlan 100             …5
(config-if)# exit
(config)#
(config)# vlan 100                                  …6
(config-vlan)# state suspend                        …7
(config-vlan)# exit
(config)#
(config)# interface gigabitethernet 1/0/1           …8
(config-if)# no switchport access vlan              …9
```

1. VLAN 100 をポート VLAN として設定します。
2. VLAN 100 を有効にします。
3. イーサネットインタフェース 1/0/1 にモードを遷移します。
4. ポート 1/0/1 にアクセスモードを設定します。
5. アクセス VLAN に 100 を設定します。
6. VLAN 100 にモードを遷移します。
7. VLAN 100 を有効から無効に変更します。
8. イーサネットインタフェース 1/0/1 にモードを遷移します。
9. 設定されているアクセス VLAN の VLAN ID 100 を削除します。

図 6-11　機能の抑止および解除の編集例

```
(config)# no ip domain lookup                       …1
(config)# ip domain name router.example.com         …2
(config)# ip name-server 192.168.0.1                …3
(config)# ip domain lookup                          …4
```

1. DNS リゾルバ機能を無効にします。
2. ドメイン名を router.example.com に設定します。
3. ネームサーバを 192.168.0.1 に設定します。
4. DNS リゾルバ機能を有効にします。

(2)　入力コマンドのチェック

コンフィグレーションコマンドを入力すると，入力されたコンフィグレーションに誤りがないかすぐにチェックされます。エラーがない場合は「図 6-12　正常入力時の出力」に示すようにプロンプトが表示されて，コマンドの入力待ちになります。ランニングコンフィグレーションの編集中の場合は，変更した内容がすぐに運用に使用されます。

エラーがある場合は「図 6-13　異常入力時のエラーメッセージ出力」に示すように，入力したコマンドの行の下にエラーの内容を示したエラーメッセージが表示されます。この場合，入力したコンフィグレーションは反映されないので，入力の誤りを正してから再度入力してください。

図 6-12　正常入力時の出力

```
(config)# interface gigabitethernet 1/0/1
(config-if)# description TokyoOsaka
(config-if)#
```

図 6-13　異常入力時のエラーメッセージ出力

```
(config)# interface tengigabitethernet 1/0/1
(config-if)# description
description
           ^
% Incomplete command at '^' marker
(config-if)#
```

6.4.5　コンフィグレーションの運用への反映

コンフィグレーションの変更は，コンフィグレーションコマンドの入力を契機に即時に運用に反映されます。ただし，BGP に関するフィルタ設定の変更内容を運用に反映する場合は，運用コマンド clear ip bgp を実行する必要があります。

運用コマンド clear ip bgp を使用すると，次に示すコマンドで変更した内容を運用に反映できます。

- access-list コマンド
- prefix-list コマンド
- route-map コマンド
- distribute-list in コマンド
- distribute-list out コマンド
- redistribute コマンド
- neighbor in コマンド
- neighbor out コマンド

コマンドの入力例を次の図に示します。

図 6-14　コマンド入力例

```
(config)# ip access-list standard 1  ..............................(1)
(config-std-nacl)# permit 10.0.0.0 0.255.255.255  .................(2)
(config-std-nacl)# permit 172.16.0.0 0.0.255.255  .................(3)
(config-std-nacl)# exit
(config)# ip prefix-list PEER-OUT seq 10 permit 172.16.1.0/24  ...(4)
(config)# route-map SET-COMM 10  ..................................(5)
(config-route-map)# match ip address prefix-list PEER-OUT  .......(6)
(config-route-map)# set community no-export  ......................(7)
(config-route-map)# exit
(config)# router bgp 65530
(config-router)# distribute-list 1 in  ............................(8)
(config-router)# redistribute static  .............................(9)
```

```
(config-router)# neighbor 192.168.1.1 remote-as 65531
(config-router)# neighbor 192.168.1.2 remote-as 65532
(config-router)# neighbor 192.168.1.2 send-community
(config-router)# neighbor 192.168.1.2 route-map SET-COMM out  ....(10)
(config-router)# exit
(config)# save
(config)# exit
# clear ip bgp * both                                              …1
```

1. (1)～(10)の変更内容が運用に使用されます。

6.4.6 コンフィグレーションのファイルへの保存（save コマンド）

save(write)コマンドを使用することで，編集したランニングコンフィグレーションをスタートアップコンフィグレーションファイルに保存できます。コンフィグレーションの保存例を次の図に示します。

図 6-15 コンフィグレーションの保存例

```
# configure                  …1
(config)#
        :
        :                    …2
        :
!(config)# save              …3
(config)#
```

1. ランニングコンフィグレーションの編集を開始します。
2. コンフィグレーションを変更します。
3. スタートアップコンフィグレーションファイルに保存します。

6.4.7 コンフィグレーションの編集終了（exit コマンド）

ランニングコンフィグレーションの編集を終了する場合は, グローバルコンフィグレーションモードで exit コマンドを実行します。コンフィグレーションを編集したあと，save コマンドで変更後の内容をスタートアップコンフィグレーションファイルへ保存していない場合は, exit コマンドを実行すると確認のメッセージが表示されます。スタートアップコンフィグレーションファイルに保存しないでコンフィグレーションコマンドモードを終了する場合は「y」を入力してください。「y」以外が入力されるとコンフィグレーションコマンドモードを終了できません。コンフィグレーションの編集終了例を「図 6-16 コンフィグレーションの編集終了例」と「図 6-17 変更内容を保存しない場合のコンフィグレーションの編集終了例」に示します。

図 6-16 コンフィグレーションの編集終了例

```
!(config)# save
(config)# exit             …1
```

1. 編集を終了します。

図 6-17 変更内容を保存しない場合のコンフィグレーションの編集終了例

```
# configure                                                          …1
(config)#
        :
        :                                                          …2
        :
!(config)# exit
Unsaved changes found! Do you exit "configure" without save ? (y/n): y …3
!#
```

1. コンフィグレーションの編集を開始します。
2. コンフィグレーションを変更します。

3. 確認メッセージが表示されます。

6.4.8　コンフィグレーションの編集時の注意事項

(1)　設定できるコンフィグレーションのコマンド数に関する注意事項

設定されたコンフィグレーションはメモリに保持されるため，設定できるコンフィグレーションのコマンド数はメモリ量によって決まります。設定するコンフィグレーションに比べてメモリ量が少なかったり，制限を超えるようなコンフィグレーションを編集したりした場合は，「Maximum number of entries are already defined (config memory shortage). <IP>」または「Maximum number of entries are already defined.<IP>」のメッセージが表示されます。このような場合，むだなコンフィグレーションが設定されていないか確認してください。

(2)　コンフィグレーションをコピー＆ペーストで入力する際の注意事項

コンフィグレーションをコピー＆ペーストで入力する場合，一行に入力できる文字数は 1000 文字，一度に入力できる文字数は 4000 文字未満（スペース，改行を含む）です。4000 文字以上を一度にペーストすると正しくコンフィグレーションを設定できない状態になるので注意してください。

4000 文字を超えるコンフィグレーションを設定する場合は，一行を 1000 文字，一度のペーストを 4000 文字未満で複数回にわけてコピー＆ペーストを行ってください。

6.5 コンフィグレーションの操作

この節では，コンフィグレーションのバックアップ，ファイル転送などの操作について説明します。

6.5.1 コンフィグレーションのバックアップ

運用コマンド copy を使用することで，コンフィグレーションをリモートサーバや本装置上にバックアップすることができます。ただし，本装置にバックアップ用のコンフィグレーションファイルを格納する場合，スタートアップコンフィグレーションファイルの格納ディレクトリ（/config）は指定できません。バックアップ用のコンフィグレーションファイルはログインユーザのホームディレクトリに作成してください。

バックアップできるコンフィグレーションは，スタートアップコンフィグレーションとランニングコンフィグレーションの 2 種類です。運用中にコンフィグレーションを変更し保存していない場合は，スタートアップコンフィグレーションをバックアップしても，バックアップしたコンフィグレーションファイルの内容は運用中のコンフィグレーションと異なります。それぞれのバックアップ例を次の図に示します。

図 6-18 スタートアップコンフィグレーションのバックアップ例

```
> enable
# copy startup-config ftp://staff@[2001:240:400::101]/backup.cnf
Configuration file copy to ftp://staff@[2001:240:400::101]/backup.cnf?
(y/n): y

Authentication for 2001:240:400::101.
User: staff
Password: xxx                                  …1
transferring…

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

図 6-19 ランニングコンフィグレーションのバックアップ例

```
> enable
# copy running-config ftp://staff@[2001:240:400::101]/backup.cnf
Configuration file copy to ftp://staff@[2001:240:400::101]/backup.cnf?
(y/n): y

Authentication for 2001:240:400::101.
User: staff
Password: xxx                                  …1
transferring…

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

6.5.2 バックアップコンフィグレーションファイルの本装置への反映

バックアップコンフィグレーションファイルをスタートアップコンフィグレーションまたはランニングコンフィグレーションに反映する場合は，運用コマンド copy を使用します。それぞれの反映例を次の図に示します。

図 6-20 スタートアップコンフィグレーションへの反映例

```
> enable
# copy ftp://staff@[2001:240:400::101]/backup.cnf startup-config
Configuration file copy to startup-config?
(y/n): y
```

```
Authentication for 2001:240:400::101.
User: staff
Password: xxx                                  …1
transferring…

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

図 6-21　ランニングコンフィグレーションへの反映例

```
> enable
# copy ftp://staff@[2001:240:400::101]/backup.cnf running-config
Configuration file copy to running-config?
(y/n): y

Authentication for 2001:240:400::101.
User: staff
Password: xxx                                  …1
transferring…

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

6.5.3　zmodem コマンドを使用したファイル転送

本装置と RS232C ケーブルで接続されているコンソールとの間でファイル転送をするときは zmodem コマンドを使用します。

(1)　バックアップコンフィグレーションファイルを本装置に転送する場合

バックアップコンフィグレーションファイルを格納するディレクトリ（/usr/home/operator）にバックアップコンフィグレーションファイルを転送後, 運用コマンド copy を使用してスタートアップコンフィグレーションにコピーします。zmodem コマンドを使用してバックアップコンフィグレーションファイルを本装置に転送する例を次の図に示します。

図 6-22　バックアップコンフィグレーションファイルの本装置へのファイル転送例 (zmodem コマンド)

```
> cd /usr/home/operator
> zmodem get backup.cnf                                    …1
**B000000027fed4
**B000000027fed4
> enable
# copy /usr/home/operator/backup.cnf startup-config       …2
Configuration file copy to startup-config ? (y/n): y       …3
#
```

1. バックアップコンフィグレーションファイルを転送します。転送後のファイル名は転送元で指定したファイル名と同じになります。
2. backup.cnf のバックアップコンフィグレーションファイルをスタートアップコンフィグレーションに使用します。
3. 入れ替えてよいかどうかの確認です。

(2)　バックアップコンフィグレーションファイルをコンソールに転送する場合

本装置に格納したバックアップコンフィグレーションファイルをコンソールに転送する例を次の図に示します。

図 6-23 バックアップコンフィグレーションファイルのコンソールへのファイル転送例

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf                    …1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> zmodem put backup.cnf                             …2
**000000000000
>
```

1. 運用しているコンフィグレーションファイルをバックアップコンフィグレーションファイルへコピーします。
2. バックアップコンフィグレーションファイルを転送します。

6.5.4 ftp コマンドを使用したファイル転送

リモート運用端末との間でファイル転送をするときは ftp コマンドを使用します。

(1) バックアップコンフィグレーションファイルを本装置に転送する場合

バックアップコンフィグレーションファイルを格納するディレクトリ（/usr/home/operator）にバックアップコンフィグレーションファイルを転送後, 運用コマンド copy を使用してスタートアップコンフィグレーションにコピーします。ftp コマンドを使用してバックアップコンフィグレーションファイルを本装置に転送する例を次の図に示します。

図 6-24 バックアップコンフィグレーションファイルの本装置へのファイル転送例（ftp コマンド）

```
> cd /usr/home/operator
> ftp 192.168.0.1
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Wed Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> get backup.cnf                                        …1
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
> enable
# copy /usr/home/operator/backup.cnf startup-config        …2
Configuration file copy to startup-config ? (y/n): y       …3
#
```

1. バックアップコンフィグレーションファイルを転送します。
2. backup.cnf のバックアップコンフィグレーションファイルをスタートアップコンフィグレーションに使用します。
3. 入れ替えてよいかどうかの確認です。

(2) バックアップコンフィグレーションファイルをリモート運用端末へ転送する場合

本装置に格納したバックアップコンフィグレーションファイルをリモート運用端末へ転送する例を次の図に示します。

図 6-25　バックアップコンフィグレーションファイルのリモート運用端末へのファイル転送例

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf                              …1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> ftp 192.168.0.1
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> put backup.cnf                                           …2
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
>
```

1. 運用しているコンフィグレーションファイルをバックアップコンフィグレーションファイルへコピーします。
2. バックアップコンフィグレーションファイルを転送します。

6.5.5　MC を使用したファイル転送

MC にファイル転送をするときは cp コマンドを使用します。

(1)　バックアップコンフィグレーションファイルを本装置に転送する場合

バックアップコンフィグレーションファイルを格納するディレクトリ（/usr/home/operator）にバックアップコンフィグレーションファイルを MC から転送後，運用コマンド copy を使用してスタートアップコンフィグレーションにコピーします。cp コマンドを使用してバックアップコンフィグレーションファイルを本装置に転送する例を次の図に示します。

図 6-26　バックアップコンフィグレーションファイルの MC から本装置へのファイル転送例（cp コマンド）

```
> cd /usr/home/operator
> cp mc-file backup.cnf backup.cnf                              …1
> enable
# copy /usr/home/operator/backup.cnf startup-config            …2
Configuration file copy to startup-config? (y/n): y            …3
#
```

1. バックアップコンフィグレーションファイルを MC から転送します。
2. backup.cnf のバックアップコンフィグレーションファイルを運用に使用します。
3. 入れ替えてよいかどうかの確認です。

(2)　バックアップコンフィグレーションファイルを MC に転送する場合

本装置に格納したバックアップコンフィグレーションファイルを MC に転送する例を次の図に示します。

図 6-27　バックアップコンフィグレーションファイルの MC へのファイル転送例

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf                              …1
```

```
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> cp backup.cnf mc-file backup.cnf                          …2
>
```

1. 運用しているコンフィグレーションファイルをバックアップコンフィグレーションファイルへコピーします。
2. バックアップコンフィグレーションファイルを MC へ転送します。

6.5.6 バックアップコンフィグレーションファイル反映時の注意事項

運用コマンド copy を使用して，バックアップコンフィグレーションファイルをランニングコンフィグレーションにコピーする場合，運用中のポートが再起動しますので，ネットワーク経由でログインしている場合は注意してください。

バックアップコンフィグレーションファイルの内容が本装置の構成と一致していない場合は，バックアップコンフィグレーションファイルの内容を変更してから運用コマンド copy を使用してください。本装置の構成と一致していないバックアップコンフィグレーションファイルに copy コマンドを実行すると，copy コマンドがエラー終了するか，copy コマンドが正常終了しても運用には正常に反映されないことがあります。その際は，バックアップコンフィグレーションファイルの内容を変更してから，再度 copy コマンドを実行してください。

7 スタックの解説

この章ではスタックについて解説します。

7.1　スタックの概要

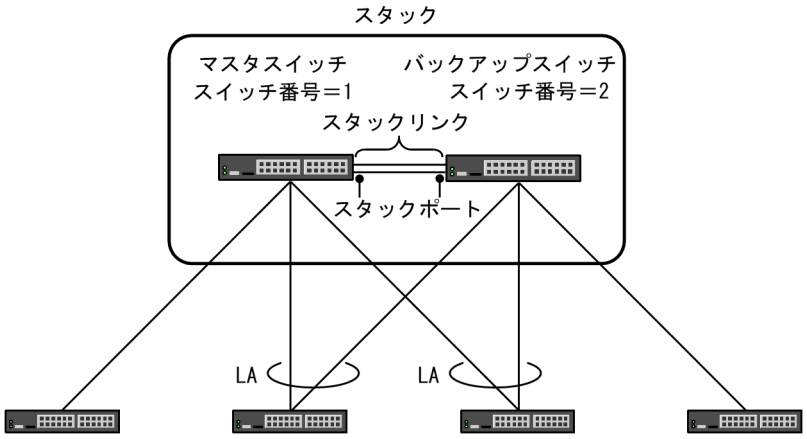
7.1.1　概要

スタックは，複数の装置を接続して論理的に 1 台の装置として動作させます。複数の装置を論理的な 1 台の装置として管理する機能を**スタック機能**と呼びます。スタックには，次に示す特長があります。

- 一元管理
  複数の装置を 1 台の装置として運用できます。
- 冗長性
  複数の装置で構成されるため，一部の障害でも通信を継続できます。
- 拡張性
  装置を追加することで，利用できるポート数を増やせます。

スタック機能が動作している装置をイーサネットインタフェースで接続すると，スタックを構成します。スタックの構成例を次の図に示します。

図 7-1　スタックの構成例



（凡例）LA：リンクアグリゲーション

スタックを構成するそれぞれの装置を**メンバスイッチ**と呼び，メンバスイッチを識別するための番号を**スイッチ番号**と呼びます。また，スタックを構成するメンバスイッチのうち一つを**マスタスイッチ**，一つを**バックアップスイッチ**と呼びます。このメンバスイッチ間を接続するポートを**スタックポート**，スタックポートで 2 台のメンバスイッチを接続する回線を**スタックリンク**と呼びます。

スタックは 1 台のメンバスイッチでも構成でき，最大で 2 台です。また，1 台のメンバスイッチに設定できるスタックポートは最大で 4 ポートです。

マスタスイッチはスタックを構成するメンバスイッチを制御します。バックアップスイッチはマスタスイッチに障害が発生した場合に，新しいマスタスイッチとして動作します。

7.1.2　スタックとスタンドアロン

スタック機能が動作していないスイッチ状態を**スタンドアロン**と呼びます。スタンドアロンの装置がスタックを構成することはなく，必ず 1 台で動作します。

本装置はスタック機能を動作させることで，スタックを構成します。スタック機能を動作させるには，コンフィグレーションコマンド stack enable を設定したあと，スタートアップコンフィグレーションに保存してから装置を再起動する必要があります。

また，スタック機能が動作している装置をスタンドアロンに戻すには，コンフィグレーションコマンド no stack enable で設定を削除したあと，スタートアップコンフィグレーションに保存してから装置を再起動する必要があります。

スタックでサポートしていない機能が必要な場合は，スタンドアロンで使用してください。

7.1.3　サポート機能

各機能のスタックでのサポート状況を次の表に示します。

表 7-1　スタックでのサポート状況

項目		サポート状況	備考
運用管理	コンソールからのログイン	○	なし
	リモート運用端末からのログイン	○	
	コンフィグレーションの操作と編集	○	
	ログインセキュリティと RADIUS/TACACS+	○	
	SSH	○	
	時刻の設定と NTP	○	
	ホスト名と DNS	○	
	省電力機能	△	コンフィグレーションコマンド shutdown によるポートの電力供給 OFF をサポートします。
	ログ出力機能	○	なし
	SNMP	△	RMON は未サポートです。また，一部の MIB は未サポートです。詳細は「MIB レファレンス」を参照してください。
	OAN（Open Autonomic Networking）	−	なし
	高機能スクリプト	○	
ネットワークインタフェース	イーサネット	△	回線テストは未サポートです。 Sync-E では，スタックポートを経由した外部クロック同期は未サポートです。

項目		サポート状況	備考
	リンクアグリゲーション	○	なし
レイヤ 2 スイッチ	MAC アドレス学習	○	なし
	VLAN	△	MAC VLAN は未サポートです。また，VLAN ID 4094 は使用できません。
	VLAN トンネリング	○	なし
	Tag 変換	○	
	ポート間中継遮断	○	
	レイヤ 2 中継遮断	○	
	VXLAN	○	
	スパニングツリー	△	Ring Protocol との併用はできません。
	Ring Protocol	△	スタック構成のノードを含むリングネットワークでは，次の機能は未サポートです。 • スパニングツリーとの併用 • GSRP との併用 • 仮想リンク また，スタック構成のノードは，次に示す設定ができません。 • 共有ノードの設定 • 一つのリング ID で，同一メンバスイッチに二つのリングポートを設定 • 複数のメンバスイッチにわたるリンクアグリゲーションを，リングポートに設定
	IGMP snooping	○	IPv4 マルチキャスト（PIM）併用時にサポートします。使用方法については「32.1.5　スタックでの IGMP snooping の設定」を参照してください。
	MLD snooping	−	なし
フィルタ・QoS	フロー検出モード	○	なし

項目		サポート状況	備考
	アクセスリスト	○	
	QoS	○	
レイヤ 2 認証	IEEE 802.1X	－	なし
	Web 認証	－	
	MAC 認証	－	
セキュリティ	DHCP snooping	－	なし
冗長化構成による高信頼化機能	GSRP	－	GSRP aware として動作できます。
	VRRP	－	なし
	アップリンク・リダンダント	△	次に示す設定はできません。 • プライマリポートとセカンダリポートを同一メンバスイッチに設定 • 複数のメンバスイッチにわたるリンクアグリゲーションを，プライマリポートまたはセカンダリポートに設定
ネットワーク監視機能	L2 ループ検知	○	なし
	ストームコントロール	○	
ネットワークの管理	ポートミラーリング	○	802.1Q Tag 付与機能を使用する場合，VLAN ID 4094 は使用できません。
	ポリシーベースミラーリング	○	なし
	sFlow 統計	○	
	IEEE802.3ah/UDLD	○	
	CFM	－	
	LLDP	○	
	OADP	－	
	PTP	－	
IPv4 パケット中継	IPv4・ARP・ICMP	○	なし
	ループバックインタフェース	○	
	Null インタフェース	○	
	ポリシーベースルーティング	○	

項目		サポート状況	備考
	DHCP リレー機能	○	
	DHCP サーバ機能	－	
	UDP ブロードキャストリレー	○	
IPv4 ルーティングプロトコル	ルーティングオプション	○	なし
	経路集約	○	
	スタティックルーティング	○	
	RIP	○	
	OSPF	○	
	BGP4	○	
	経路フィルタリング	○	
	IPv4 マルチキャスト	○	
IPv6 パケット中継	IPv6・NDP・ICMPv6	○	なし
	ループバックインタフェース	○	
	Null インタフェース	○	
	RA	○	
	IPv6 DHCP リレー	○	
	IPv6 DHCP サーバ機能	－	
IPv6 ルーティングプロトコル	ルーティングオプション	○	なし
	経路集約	○	
	スタティックルーティング	○	
	RIPng	○	
	OSPFv3	○	
	BGP4+	○	
	経路フィルタリング	○	
	IPv6 マルチキャスト	－	
ネットワーク経路監視機能	BFD	－	なし
ネットワークパーティション	VRF	○	なし

（凡例）○：サポート　△：一部サポート　－：未サポート

7.2　スタック構成

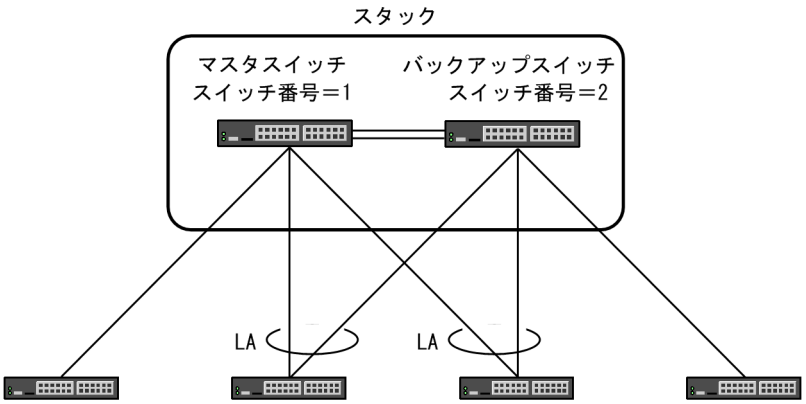
7.2.1　スタック構成

スタックを構成するメンバスイッチは最大で 2 台です。

(1)　メンバスイッチ 2 台でのスタック構成

メンバスイッチ 2 台でのスタック構成例を次の図に示します。

図 7-2　メンバスイッチ 2 台でのスタック構成例



（凡例）LA：リンクアグリゲーション

スタック構成ではマスタスイッチがほかのメンバスイッチを制御して，仮想的に 1 台の装置として動作します。

スタック構成時のリンクアグリゲーションは，スタックを構成するそれぞれのメンバスイッチに対して設定することをお勧めします。この設定によって，一つのメンバスイッチで障害が発生しても通信を継続できます。

また，スタックリンクに障害が発生し，メンバスイッチ間で通信できなくなると，スタックが分かれ，どちらもマスタスイッチになります。これによって，通信ができなくなるおそれがあります。この状態を避けるため，スタックリンクを 2 本以上設定して，冗長化しておくことをお勧めします。

(2)　メンバスイッチ 1 台でのスタック構成

1 台のメンバスイッチでもスタックを構成できます。

メンバスイッチ 2 台でスタックを構成する場合でも，まずメンバスイッチ 1 台のスタックを構成すれば，その後，それぞれのメンバスイッチのスタックポートを接続し，メンバスイッチ 2 台のスタックに移行できます。

また，最初からメンバスイッチ 1 台のスタックで運用すれば，運用中に通信を停止することなく，装置を追加して利用できるポート数を増やせます。

7.2.2　メンバスイッチのモデル

マスタスイッチとなるメンバスイッチでは，スタックを構成するメンバスイッチのモデルを設定する必要があります。なお，マスタスイッチとは異なる IP8800/S3660 モデルのメンバスイッチも設定できます。

自メンバスイッチのモデルは起動時に自動で設定されます。ほかのメンバスイッチのモデルはコンフィグレーションコマンド switch provision で設定します。

7.2.3 スタックを構成する条件

スタックを構成する場合は，メンバスイッチ間で次の条件をすべて満たすようにしてください。

- スイッチ番号が異なること
- ソフトウェアライセンス，およびオプションライセンスによって有効化された機能が一致すること（ただし，アップリンク 10G およびポート数拡張は除く）
- ソフトウェアバージョンが一致すること

なお，これらの条件を満たしていないと，マスタスイッチ以外のメンバスイッチが再起動を繰り返すことがあります。その後，そのメンバスイッチはデフォルト設定情報で起動します。

また，ソフトウェアバージョンが一致していなくても，コンフィグレーションが一致していればスタックを構成できます。ただし，その場合，コンフィグレーションを編集できません。

7.3　スタックの基本機能

7.3.1　スイッチ番号

スイッチ番号とは，スタックを構成するメンバスイッチを識別するための番号です。各メンバスイッチ固有の情報であり，スタックを構成しても引き継がれます。スイッチ番号には 1 または 2 が設定できます。

スイッチ番号は運用コマンド set switch で設定します。設定したあと，メンバスイッチを再起動すると有効になります。

なお，スタンドアロンの場合，スイッチ番号は 1 固定です。そのため，運用コマンド set switch で 1 以外の値を設定しても，スタック機能を有効にしなければ再起動後のスイッチ番号は 1 となります。

7.3.2　スタックポートとスタックリンク

スタックポートとは，スタックを構成するメンバスイッチ間を接続するポートであり，モデルによってポート種別が異なります。モデルごとのスタックポートのポート種別を次の表に示します。

表 7-2　各モデルのスタックポートとして使用できるポート種別

モデル	スタックポートのポート種別
IP8800/S3660-24T4X	QSFP+ポート※1
IP8800/S3660-24T4XW	
IP8800/S3660-48T4XW	
IP8800/S3660-16S4XW	
IP8800/S3660-24S8XW	
IP8800/S3660-48XT4QW	QSFP28/QSFP+共用ポート※2
IP8800/S3660-24X4QW	
IP8800/S3660-48X4QW	

注※1

スタックポートとしてだけ使用できるスタック専用ポートです。ネットワークを構成するためのイーサネットインタフェースとしては使用できません。そのため，QSFP+ポートはスタック機能が動作している場合だけ使用できます。

注※2

100 ギガビットインタフェースをスタックポートとして使用する場合，100GBASE-CR4 だけをサポートします。

スタックリンクとは，2 台のメンバスイッチのスタックポート間を接続した回線です。スタックリンクは回線で直接接続してください。2 台のメンバスイッチを接続するスタックポートの間に，ほかのネットワーク機器を接続しないでください。

メンバスイッチ 2 台のスタックではスタックリンクが必要です。スタックリンクは 2 本以上設定することをお勧めします。2 本以上のスタックリンクで冗長化すると，特定のスタックリンクで障害が発生しても，残りのスタックリンクで動作し続けます。

スタックリンクが 2 本以上の場合，スタックリンクでメンバスイッチ間の通信をロードバランスします。このとき，スタックリンク同士の通信性能が異なると，ロードバランスの結果パケットが廃棄されるおそれ

が高くなります。スタックリンクを 2 本以上設定する場合は，スタックポートに使用するダイレクトアタッチケーブルやトランシーバ種別（QSFP+/QSFP28）を同じにして回線速度を統一してください。

スタックリンクの接続仕様については，「ハードウェア取扱説明書」を参照してください。

スタックポートは，コンフィグレーションコマンド switchport mode の stack パラメータで設定します。

なお，スタックポートとして使用するイーサネットインタフェースでは，次に示すコンフィグレーションコマンドだけが設定できます。

- bandwidth
- description
- no snmp trap link-status
- shutdown

これら以外のコンフィグレーションコマンドは，コマンド省略時の動作になります。ただし，次に示すコンフィグレーションコマンドはコマンド省略時の動作にならないため注意してください。

- flowcontrol
  受信および送信動作どちらも off になります。
- link debounce
  リンクダウン検出時間はスタックポート固有の値となります。
- mtu
  MTU はスタック固有の値となります。コンフィグレーションコマンド system mtu の設定値に影響されません。

7.3.3　スイッチ状態

ここでは，スイッチ状態とスイッチ状態遷移後の変更処理について説明します。

(1)　スイッチ状態一覧

スイッチ状態一覧を次の表に示します。なお，英字略称はログまたはコマンドプロンプトで，スイッチ状態の識別のために使われます。

表 7-3　スイッチ状態一覧

スイッチ状態	英字略称	説明
初期状態	I	装置が起動したあと，スイッチ状態が次のどれかに決まるまでの状態。 • スタンドアロン • マスタ • バックアップ
スタンドアロン	S	スタックを構成しない装置の状態。
マスタ	M	スタックを構成していて，ほかのメンバスイッチを制御するメンバスイッチの状態。
バックアップ	B	スタックを構成していて，かつ，現在のマスタスイッチに障害が発生した場合マスタスイッチに切り替わるメンバスイッチの状態。

(2)　スイッチ状態遷移後の変更処理

スイッチ状態が遷移すると，メンバスイッチは遷移後のスイッチ状態で正しく動作するために次に示す処理をします。

- 初期化
- 切り替え

これらの処理を**変更処理**と呼びます。遷移前と遷移後のスイッチ状態によって，必要な変更処理が異なります。また，変更処理には時間が掛かります。

(a)　初期状態からマスタへ遷移した場合の変更処理

スイッチ状態が初期状態からマスタへ遷移すると，変更処理として，転送動作を始めるための初期化をします。初期化中のマスタスイッチは，スタックポートでメンバスイッチと接続しても，メンバスイッチをすぐに追加しません。初期化が完了してから，接続したメンバスイッチを追加します。

(b)　初期状態からバックアップへ遷移した場合の変更処理

スイッチ状態が初期状態からバックアップへ遷移すると，変更処理として，転送動作を始めるための初期化をします。初期化中のバックアップスイッチはマスタスイッチとの接続がなくなると再起動します。そのため，バックアップスイッチの初期化中に，マスタスイッチが停止または再起動すると，パケットの転送を継続できません。初期化が完了したバックアップスイッチは，マスタスイッチとの接続がなくなった時点で，マスタスイッチに切り替わります。したがって，初期化が完了したあとマスタスイッチとの接続がなくなっても，バックアップスイッチのポートがアップしていれば，パケットの転送を継続できます。

なお，初期化中のバックアップスイッチに対しては，マスタスイッチから運用コマンドを実行して情報を表示したり，操作したりできません。バックアップスイッチの初期化が完了してから，再度実行してください。

(c)　バックアップからマスタへ遷移した場合の変更処理

スイッチ状態がバックアップからマスタへ遷移すると，変更処理として，新しいマスタスイッチとして動作するための切り替えをします。切り替え中のマスタスイッチは，スタックポートでメンバスイッチと接続しても，メンバスイッチをすぐに追加しません。切り替えが完了してから，接続したメンバスイッチを追加します。

7.3.4　マスタスイッチの役割と選出

マスタスイッチは，スタック全体を制御するスイッチであり，スイッチ状態，マスタ選出優先度およびメンバスイッチの筐体 MAC アドレスの三つの要素に従って選出されます。

ここでは，マスタスイッチの役割とマスタスイッチの選出について説明します。

(1)　マスタスイッチの役割

マスタスイッチはスタックを構成するすべてのメンバスイッチとその機能を制御します。スタックを構成するすべてのメンバスイッチは，マスタスイッチのコンフィグレーションとマスタスイッチからの制御に従って動作します。

マスタスイッチはメンバスイッチの代表であり，リモート運用端末からスタックへログインすると，必ずマスタスイッチへログインします。

ログインしたマスタスイッチでは，次に示す操作ができます。

- コンフィグレーションの編集
- すべてのメンバスイッチのオペレーション
- すべてのメンバスイッチの運用メッセージ・運用ログの確認

(2) マスタスイッチの選出

マスタスイッチは次に示す基準で選出されます。

(a) すでにマスタスイッチがある場合

既存のマスタスイッチをそのままマスタスイッチに選びます。

すでに動作しているスタックに新しいメンバスイッチをスタックポートで接続して起動しても，既存のマスタスイッチがマスタ状態を継続します。これによって，スタックの転送機能を維持したまま新しいメンバスイッチを追加できます。

例外として，マスタスイッチのマスタ選出優先度が 1 であり，それ以外にマスタ選出優先度が 2 以上のメンバスイッチがある場合，マスタ選出優先度が 2 以上のメンバスイッチをマスタスイッチに選びます。

(b) マスタスイッチが 1 台もない場合

バックアップスイッチをマスタスイッチに選びます。

(c) マスタスイッチおよびバックアップスイッチが 1 台もない場合

マスタ選出優先度が最も大きいメンバスイッチをマスタスイッチに選びます。マスタ選出優先度も同じ場合は，筐体 MAC アドレスが最も小さいメンバスイッチをマスタスイッチに選びます。

(d) マスタスイッチが 2 台ある場合

マスタ選出優先度が最も大きいメンバスイッチをマスタスイッチに選びます。マスタ選出優先度も同じ場合は，筐体 MAC アドレスが最も小さいメンバスイッチをマスタスイッチに選びます。

(3) マスタスイッチ選出の例

マスタスイッチを選出する例を次に示します。

（例 1）メンバスイッチ 1 台のスタックにメンバスイッチを追加した

スタックで動作しているメンバスイッチが 1 台だけでマスタスイッチとして動作しているとき，別のメンバスイッチを起動した場合，元のマスタスイッチのマスタ状態は継続します。選出基準の(a)に該当します。

ただし，元のマスタスイッチのマスタ選出優先度が 1 であり，かつ追加したメンバスイッチのマスタ選出優先度が 2 以上の場合，追加したメンバスイッチがマスタスイッチに選ばれます。元のマスタスイッチは再起動し，スタックのマスタスイッチではないメンバスイッチとなります。

（例 2）2 台のメンバスイッチを同時に起動した

スタックポートで接続済みの 2 台のメンバスイッチを同時に起動した場合，マスタ選出優先度，筐体 MAC アドレスの順に比較され，マスタスイッチが選ばれます。選出基準の(c)に該当します。

（例 3）マスタスイッチとマスタスイッチを接続した

1 台のメンバスイッチでスタックを構成している二つのスタックを接続した場合，マスタ選出優先度，筐体 MAC アドレスの順に比較され，マスタスイッチが選ばれます。選出基準の(d)に該当します。

マスタスイッチに選ばれなかったメンバスイッチは再起動し，マスタスイッチに選ばれたメンバスイッチのスタックに加わります。

(4)　2 台構成のスタックでマスタスイッチの選出を固定する方法

2 台構成のスタックのすべてのメンバスイッチを起動するときに，選んだメンバスイッチをマスタスイッチにするには，次に示す二つの方法があります。

- マスタスイッチにする予定のメンバスイッチのマスタ選出優先度に 2 以上を設定し，マスタスイッチにしない予定のメンバスイッチのマスタ選出優先度に 1 を設定してください。
- マスタスイッチにする予定のメンバスイッチを先に起動してください。マスタスイッチとして起動し終わったあとに，マスタスイッチにしない予定のメンバスイッチを起動してください。

(5)　マスタ選出優先度

マスタ選出優先度とは，スタックを構成するメンバスイッチからマスタスイッチを選出するための優先度です。マスタ選出優先度として，1 から 31 までの値をコンフィグレーションコマンド switch priority で設定できます。

マスタ選出優先度が大きいメンバスイッチは，スタックを構成するすべてのメンバスイッチを同時に起動したときに，優先してマスタスイッチに選ばれます。しかし，すでにマスタスイッチが動作しているスタックにマスタ選出優先度が大きいメンバスイッチを追加して起動しても，既存のマスタスイッチのマスタ選出優先度が 1 以外であれば，既存のマスタスイッチがマスタ状態を継続します。

マスタ選出優先度 1 は特別な優先度です。メンバスイッチが 2 台動作していて，1 台のメンバスイッチのマスタ選出優先度が 1，もう 1 台のメンバスイッチのマスタ選出優先度が 2 以上であれば，必ずマスタ選出優先度が 2 以上のメンバスイッチをマスタスイッチに選びます。

例えば，1 台のマスタ選出優先度 1 のマスタスイッチで構成されたスタックに，マスタ選出優先度が 2 以上のメンバスイッチを追加して起動すると，追加したメンバスイッチがマスタスイッチに選ばれます。

なお，マスタスイッチを切り替えるときに，元のマスタスイッチ（マスタ選出優先度 1）と追加したメンバスイッチが共に再起動するため，通信が一時的に停止します。

マスタ選出優先度を 1 に設定したメンバスイッチは，次の場合を除いてマスタスイッチに選出されません。

- スタックを構成するメンバスイッチが 1 台しかない場合
- スタックを構成するすべてのメンバスイッチのマスタ選出優先度が 1 の場合

既存のスタックにメンバスイッチを追加するときは，追加するメンバスイッチのマスタ選出優先度を 1 に設定してください。これは，メンバスイッチを追加すると同時に既存のマスタスイッチが障害などで再起動した場合，追加したメンバスイッチがマスタスイッチになって，旧マスタスイッチのコンフィグレーションが追加したメンバスイッチのコンフィグレーションに置き換わることを防ぐためです。なお，スタックが構築されたあと，バックアップスイッチのマスタ選出優先度は，マスタスイッチで設定したマスタ選出優先度に変更されます。

7.3.5　スタックの装置 MAC アドレス

初めてスタックを構成したときマスタスイッチに選出されたメンバスイッチの筐体 MAC アドレスを，スタックの装置 MAC アドレスとして使用します。その後，マスタスイッチに障害が発生してバックアップスイッチが新しいマスタスイッチになっても，スタックの装置 MAC アドレスは変更しないでそのまま引き継ぎます。

なお，すべてのメンバスイッチが同時に再起動した場合は，新しくマスタスイッチに選出されたメンバスイッチの筐体 MAC アドレスがスタックの装置 MAC アドレスとなります。

7.4　スタックの運用管理

(1)　コンフィグレーション

(a)　メンバスイッチのコンフィグレーション

スタックでは，スタックを構成するすべてのメンバスイッチが同じコンフィグレーションで動作します。各メンバスイッチにはスタートアップコンフィグレーションとランニングコンフィグレーションがありますが，ランニングコンフィグレーションをすべてのメンバスイッチで同じ状態にしてスタックは動作します。

(b)　ランニングコンフィグレーションの編集

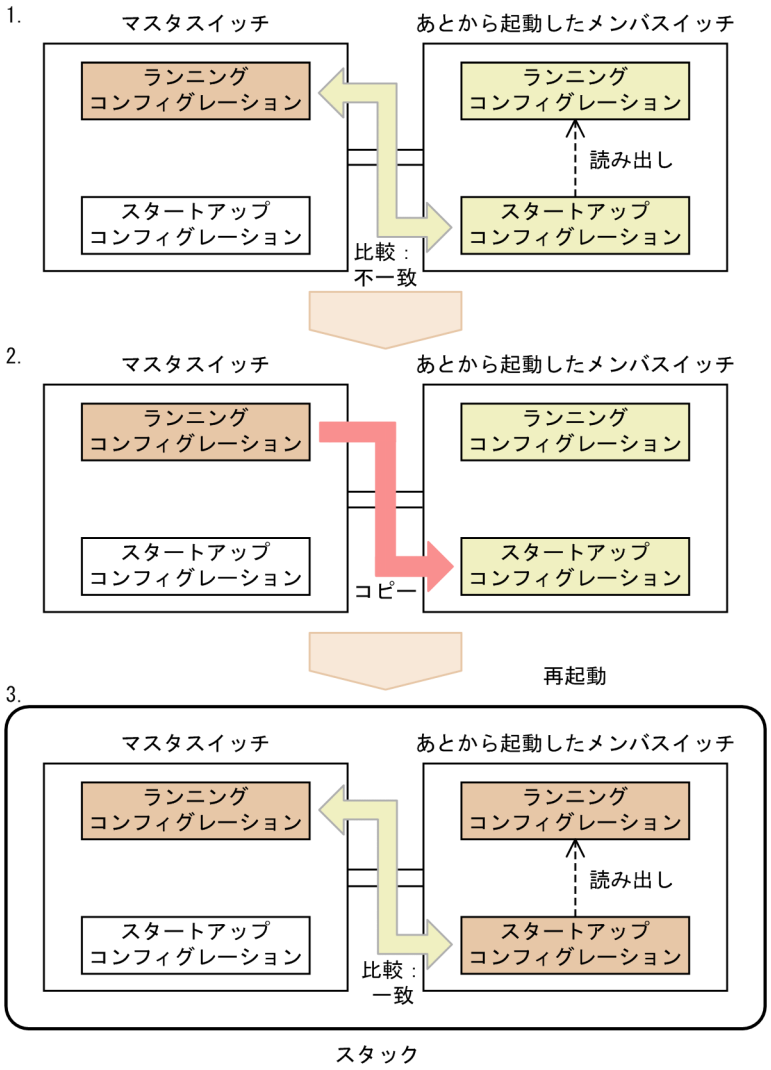
スタック構成時のランニングコンフィグレーションはマスタスイッチだけで編集できます。マスタスイッチ以外では，ランニングコンフィグレーションを編集できません。マスタスイッチで編集したランニングコンフィグレーションは，ほかのメンバスイッチのランニングコンフィグレーションと同期します。また，マスタスイッチで save コマンドを実行すると，すべてのメンバスイッチのランニングコンフィグレーションがそれぞれのスタートアップコンフィグレーションに保存されます。

(c)　あとから起動したメンバスイッチとの同期までの流れ

スタック運用中に，メンバスイッチがあとから起動したときは，マスタスイッチのランニングコンフィグレーションとあとから起動したメンバスイッチのスタートアップコンフィグレーションが同じかどうかを確認します。

- コンフィグレーションが同じ場合
  あとから起動したメンバスイッチはそのままスタックの一部となります。
- コンフィグレーションが異なる場合
  次の図に示すような手順でコンフィグレーションを一致させ，メンバスイッチをスタックの一部にします。

図 7-3　コンフィグレーションの一致まで流れ



1. マスタスイッチのランニングコンフィグレーションとあとから起動したメンバスイッチのスタートアップコンフィグレーションを比較すると不一致である。
2. メンバスイッチではマスタスイッチのランニングコンフィグレーションをスタートアップコンフィグレーションにコピーし，再起動する。
3. マスタスイッチのランニングコンフィグレーションと再起動したメンバスイッチのスタートアップコンフィグレーションが一致したため，メンバスイッチはマスタスイッチのランニングコンフィグレーションに同期したランニングコンフィグレーションで動作する。

(2)　運用コマンドの実行

スタックでは，マスタスイッチから運用コマンドを使用して，メンバスイッチの情報を表示したり，操作したりできます。スタック構成での運用コマンドの動作については，「運用コマンドレファレンス」の［スタック構成時の運用］を確認してください。また，運用コマンド remote command を使用しても，マスタスイッチから指定したメンバスイッチに対して運用コマンドを実行できます。

なお，remote command コマンドを実行するときは，次に示す点に注意してください。

- マスタスイッチ以外のメンバスイッチでは，ほかのメンバスイッチに対して運用コマンドを実行できません。
- remote command コマンドは，初期化が完了したメンバスイッチに対して実行できます。初期化中のメンバスイッチに対しては実行できません。その場合は，初期化が完了してから再度実行してください。
- remote command コマンドを含む運用コマンドを連続して実行する場合は，remote command コマンドが終了してプロンプトが表示されたあとに，次の運用コマンドを実行してください。remote command コマンドを含む運用コマンドをコピー＆ペーストで入力して実行した場合，remote command コマンドよりあとの運用コマンドが実行されないことがあります。その場合は実行されなかった運用コマンドを再度入力して実行してください。

(3) ユーザアカウント

スタックでは，マスタスイッチ以外のメンバスイッチのユーザアカウントはマスタスイッチのユーザアカウントに同期します。したがって，マスタスイッチ以外のメンバスイッチだけに存在するユーザアカウントは，スタックを構成するときに削除されます。なお，ホームディレクトリ配下のファイルは同期しません。

(4) メンバスイッチへのログイン

スタックでは，運用コマンド session を使用するか，またはコンソールを接続してそれぞれのメンバスイッチにログインできます。

どのメンバスイッチにログインしているかは，コマンドプロンプトで識別できます。例えば，コンフィグレーションコマンド hostname で OFFICE1 を設定していて，スイッチ番号 1 がマスタスイッチ，スイッチ番号 2 がバックアップスイッチの場合，コマンドプロンプトは次のようになります。

- マスタスイッチのコマンドプロンプト：`OFFICE1>`
- バックアップスイッチのコマンドプロンプト：`OFFICE1-02B>`

バックアップスイッチのコマンドプロンプトのハイフン“-”以降は，スイッチ番号（2 文字）とスイッチ状態（1 文字）を意味します。

なお，あとから起動したメンバスイッチにログインできるのは，マスタスイッチと起動したメンバスイッチの接続が完了してからです。あとから起動したメンバスイッチにログインできないときは，運用コマンド show switch でメンバスイッチの状態を確認するか，またはログイン用のコマンドプロンプトが表示されるまで待ってください。

リモート運用端末からログインする場合は，マスタスイッチにログインします。

運用コマンド session で接続しているときに一定時間キーの入力がない場合，自動ログアウトの対象となって，接続を終了して接続元のスイッチに戻ります。

(5) SSH サーバのホスト鍵ペア

マスタスイッチ以外のメンバスイッチの SSH サーバのホスト鍵ペアは，マスタスイッチの SSH サーバのホスト鍵ペアで同期します。また，マスタスイッチで運用コマンド set ssh hostkey や erase ssh hostkey を実行してホスト鍵ペアを生成および削除すると，マスタスイッチ以外のメンバスイッチのホスト鍵ペアもマスタスイッチと同じホスト鍵ペアが生成および削除されます。

(6)　メンバスイッチの時刻

マスタスイッチ以外のメンバスイッチの時刻は，マスタスイッチの時刻に同期します。ただし，時刻は秒単位で同期するため，メンバスイッチ間で誤差が発生することがあります。

マスタスイッチで運用コマンド set clock を実行すると，ほかのメンバスイッチの時刻は，最大で 1 分後に同期します。

(7)　ソフトウェアの管理

(a)　ソフトウェアのアップデート

ソフトウェアをアップデートするときは，1 台のメンバスイッチのアップデートが完了してそのポートがアップしたあと，もう 1 台をアップデートしてください。なお，バックアップスイッチ，マスタスイッチの順でアップデートすることをお勧めします。

運用コマンド show switch でアップデートの完了を確認してください。アップデートを実施したメンバスイッチの初期化が完了していれば，アップデートが完了しています。また，運用コマンド show port でポートがアップしていることを確認してください。

(b)　ソフトウェアライセンスおよびオプションライセンス

ソフトウェアライセンスおよびオプションライセンスを設定したあと再起動して適用するときは，バックアップスイッチ，マスタスイッチの順で再起動することをお勧めします。

なお，バックアップスイッチの再起動からマスタスイッチの再起動まで時間が掛かると，スタックを構成できないことがあります。

(8)　運用情報のバックアップ・リストア

バックアップ・リストアの対象には，メンバスイッチ個別のスタック情報ファイルと呼ぶ情報を含みます。

(9)　運用メッセージの画面出力とログ保存

メンバスイッチで発生したイベント情報は，運用メッセージとして，各メンバスイッチの運用端末に表示されるほか，運用ログとして各メンバスイッチに保存されます。

このうち，メッセージ種別 ERR および EVT の運用メッセージは，マスタスイッチにも通知されます。つまり，すべてのメンバスイッチの運用メッセージが，マスタスイッチの運用端末に表示されるほか，運用ログとしてマスタスイッチに保存されます。また，運用メッセージは syslog インタフェースを使用してネットワーク上のサーバへ出力できます。

なお，運用メッセージのフォーマットには，スイッチ番号とスイッチ状態が含まれます。これによって，イベントが発生したメンバスイッチやその状態を区別できます。

(10)　MIB と SNMP 通知

スタックでは，スタンドアロンと同様に SNMP の設定で MIB の取得や設定，SNMP 通知の送信ができます。

(11)　高機能スクリプト

(a)　スクリプトファイルのインストール

マスタスイッチで運用コマンド install script によってスクリプトファイルをインストールすると，マスタスイッチ以外のメンバスイッチにも自動的にインストールします。

インストールされているすべてのスクリプトファイルを同期したい場合は，運用コマンド install script に sync パラメータを指定してください。この場合，マスタスイッチ以外のメンバスイッチにインストールされているすべてのスクリプトファイルは，マスタスイッチのスクリプトファイルに同期します。なお，マスタスイッチ以外のメンバスイッチだけに存在するスクリプトファイルは削除されます。

(b)　スクリプトの起動

スクリプトの起動はマスタスイッチで実行できます。実行中にスイッチ状態が遷移したときのスクリプトの動作について，次の表に示します。

表 7-4　スイッチ状態遷移時のスクリプトの動作

スクリプト種別	マスタへ遷移	バックアップへ遷移
コマンドスクリプト	スクリプトは自動で実行されません。	実行中だったスクリプトは強制終了します。
常駐スクリプト	新しく常駐スクリプトを起動します。	
イベント起動スクリプト	マスタスイッチで新たにイベントを検出すると起動します。	

(c)　スクリプトファイルの同期

メンバスイッチを追加したり交換したりした場合は，スクリプトファイルを同期してください。同期するには，ソフトウェアバージョンを一致させたうえで，運用コマンド install scrip に sync パラメータを指定して実行してください。同期しないで運用すると，マスタスイッチが切り替わったときに，新しくマスタスイッチとなったメンバスイッチにインストールされていないスクリプトは起動しません。

なお，運用コマンド install script に diff パラメータを指定して実行すると，同期の要否について確認できます。

7.5　障害時と復旧時のスタック動作

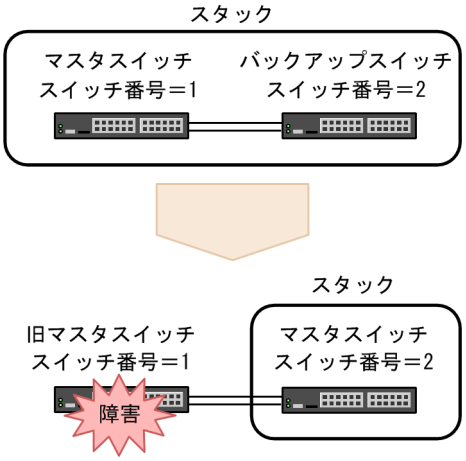
この節では，障害時と復旧時のスタック動作について説明します。

7.5.1　メンバスイッチの障害と復旧

(1)　マスタスイッチ障害時

マスタスイッチに障害が発生した場合の動作について次の図に示します。

図 7-4　マスタスイッチ障害時

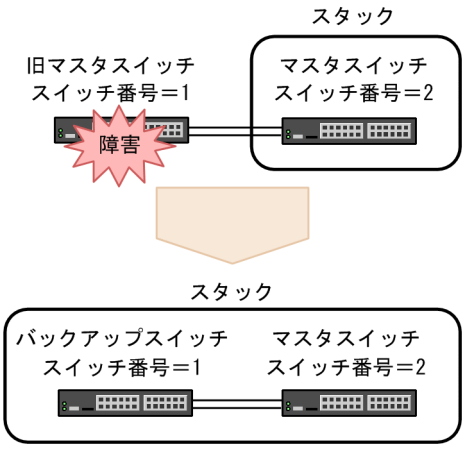


マスタスイッチに障害が発生して停止すると，バックアップスイッチが新しいマスタスイッチになって，マスタスイッチ 1 台のスタックで動作します。このとき，装置 MAC アドレスは変更しません。

(2)　旧マスタスイッチ復旧時

旧マスタスイッチが障害から復旧した場合の動作について次の図に示します。

図 7-5　旧マスタスイッチ復旧時

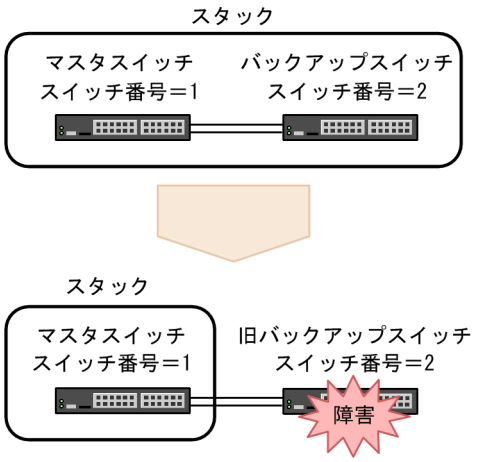


旧マスタスイッチが障害から復旧すると，このメンバスイッチはバックアップスイッチになって，メンバスイッチ 2 台のスタックで動作します。このとき，装置 MAC アドレスは変更しません。

(3)　バックアップスイッチ障害時

バックアップスイッチに障害が発生した場合の動作について次の図に示します。

図 7-6　バックアップスイッチ障害時

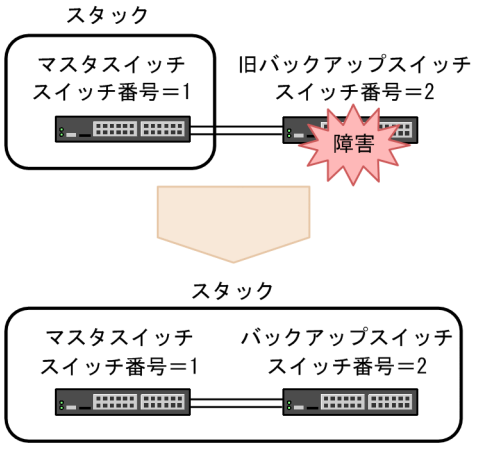


バックアップスイッチに障害が発生して停止すると，マスタスイッチ 1 台のスタックで動作します。このとき，装置 MAC アドレスは変更しません。

(4)　旧バックアップスイッチ復旧時

旧バックアップスイッチが障害から復旧した場合の動作について次の図に示します。

図 7-7　旧バックアップスイッチ復旧時



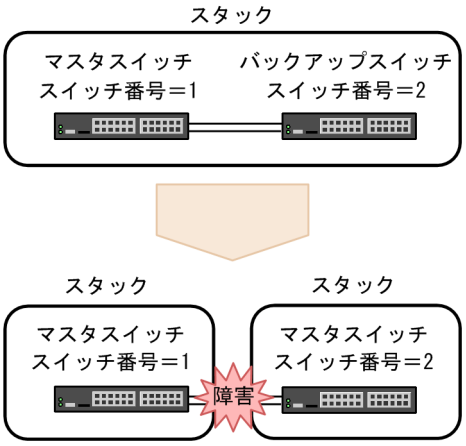
旧バックアップスイッチが障害から復旧すると，このメンバスイッチはバックアップスイッチになって，メンバスイッチ 2 台のスタックで動作します。このとき，装置 MAC アドレスは変更しません。

7.5.2　スタックリンクの障害と復旧

(1)　スタックリンク障害時

すべてのスタックリンクで障害が発生した場合の動作について次の図に示します。

図 7-8　スタックリンク障害時



すべてのスタックリンクで障害が発生すると，マスタスイッチとバックアップスイッチは互いに隣接するメンバスイッチを認識できなくなります。その結果，一つのスタックが二つのスタックに分かれて，マスタスイッチはマスタスイッチのまま，バックアップスイッチは新しくマスタスイッチに切り替わって動作します。

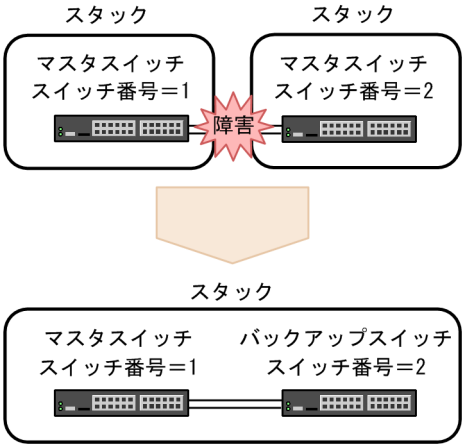
このとき，二つのスタックでは同じ IP アドレスおよび装置 MAC アドレスを使用するため，アドレスの重複によって正しく通信できなくなります。

なお，スタックリンクが 2 本以上あれば，特定のスタックリンクで障害が発生しても残りのスタックリンクで動作し続けられます。しかし，残りのスタックリンクで障害が発生すると，スタックが二つに分かれてしまうため，スタックリンクの 1 本で障害が発生した場合もすぐに復旧させてください。

(2)　スタックリンク復旧時

スタックリンクが障害から復旧した場合の動作について次の図に示します。

図 7-9　スタックリンク復旧時



スタックリンクが障害から復旧すると，二つのスタックに分かれていたメンバスイッチは互いに認識して，一つのスタックで動作します。

7.5.3　メンバスイッチの通信切り替え

スタックを構成すると，メンバスイッチの障害時や復旧時に短時間で通信を切り替えられます。短時間で通信を切り替える必要がある場合は，他装置との接続に複数のメンバスイッチにわたるリンクアグリゲーションの構成を組んだ上で，スタックでの短時間通信切り替えをサポートしている機能を使用してください。機能ごとのスタックでの短時間通信切り替えサポート状況を次の表に示します。

表 7-5　スタックでの短時間通信切り替えサポート状況

分類	機能	サポート
ネットワークインタフェース	イーサネット	○
リンクアグリゲーション	スタティック	○
	LACP※1	○
	スタンバイリンク　リンクダウンモード	×
	スタンバイリンク　非リンクダウンモード	○
レイヤ 2 中継	MAC アドレス学習	○
	ポート VLAN	○
	プロトコル VLAN	○
	Tag 変換	○
	VLAN トンネリング	○
	スパニングツリー	×※2
	Ring Protocol※3	○
	IGMP snooping	○
フィルタ・QoS	フィルタ	○
	QoS	○
冗長化構成による高信頼化機能	アップリンク・リダンダント※3	○
ネットワーク監視機能	L2 ループ検知	○
ネットワークの管理	IEEE802.3ah/UDLD	○
IPv4 パケット中継※4	IPv4・ARP	○
	ポリシーベースルーティング	○
	DHCP リレー	○
IPv4 ユニキャストルーティングプロトコル	スタティックルーティング	○
	RIP	×
	OSPF	○※5
	BGP4	○※5
IPv4 マルチキャストルーティングプロトコル	PIM-SM	○※6

分類	機能	サポート
	PIM-SSM	○※6
IPv6 パケット中継※4	IPv6・NDP	○
	IPv6 DHCP リレー	○
IPv6 ユニキャストルーティングプロトコル	スタティックルーティング	○
	RIPng	×
	OSPFv3	○※5
	BGP4+	○※5

（凡例）○：サポート　×：未サポート

注※1

次の表に示す条件を満たすと，マスタスイッチの切り替え時に LACP のチャネルグループをダウンしないで通信を継続できます。ただし，マスタスイッチが切り替わったときは，本装置の LACP 開始方法が active でも，対向装置から LACPDU を受信するまで LACPDU を送信しません。そのため，対向装置も LACP の短時間通信切り替えをサポートしている場合は，本装置と対向装置で同時にマスタスイッチの切り替えが発生すると，両装置で LACPDU 受信待ち状態となり，タイムアウトによってチャネルグループがダウンします。

また，離脱ポート制限機能は，対向装置から LACPDU を受信するまで動作しません。

表 7-6　通信を継続できる条件

項目	本装置	対向装置
複数のメンバスイッチにわたるリンクアグリゲーションの構成	必須	任意
LACPDU 送信間隔	long	long

注※2

マスタスイッチの切り替え時にトポロジー計算を最初からやり直します。トポロジー計算が完了するまでの間，スパニングツリーが動作している VLAN の通信が停止します。

注※3

複数のメンバスイッチにわたるリンクアグリゲーションの構成を組まなくても，短時間通信切り替えができます。

注※4

IPv4/IPv6 パケットのソフトウェア中継および本装置への IPv4/IPv6 通信は，短時間通信切り替えをサポートしていません。

注※5

グレースフル・リスタートを使用した場合です。

注※6

コンフィグレーションコマンド ip pim nonstop-forwarding を設定した場合です。

なお，通信の切り替え時間には，スタックに接続する回線のリンクダウン検出時間，およびリンクアップ検出時間が含まれます。

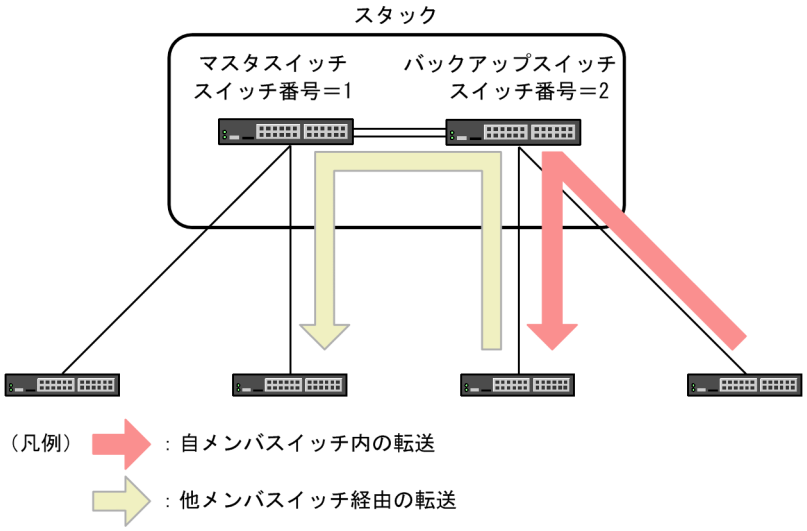
7.6　スタックの転送動作

7.6.1　物理ポートの転送動作

(1)　正常時の転送動作

受信したポートと転送先のポートが同じメンバスイッチの場合，そのメンバスイッチ内で転送します。受信したポートと転送先のポートが異なるメンバスイッチの場合，スタックリンクを経由して転送します。物理ポートで正常時の転送動作を次の図に示します。

図 7-10　正常時の転送動作（物理ポート）



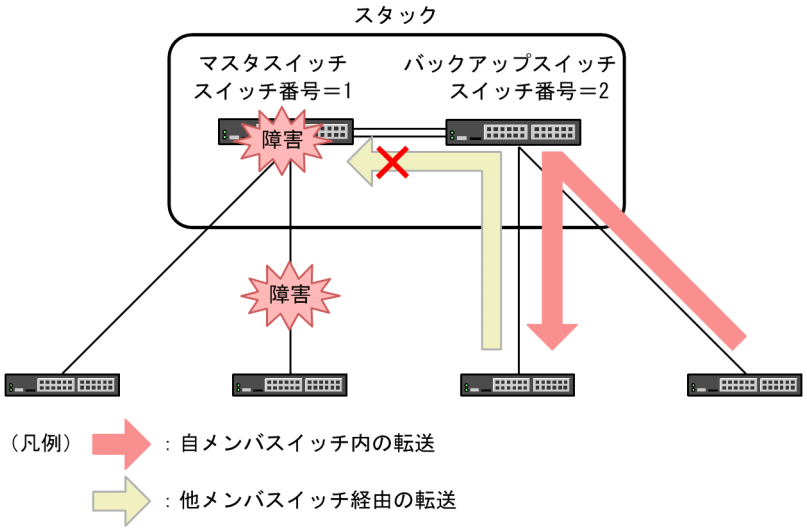
(2)　障害時の転送動作

この構成では経路を冗長化していません。そのため，受信したポートと転送先のポートが異なるメンバスイッチの場合，次のような状態になると転送を継続できません。

- ほかのメンバスイッチの転送先の経路に障害が発生した
- ほかのメンバスイッチに障害が発生した

物理ポートで障害時の転送動作を次の図に示します。

図 7-11　障害時の転送動作（物理ポート）



このような状態になっても転送を継続するために，スタックでリンクアグリゲーションを使用することをお勧めします。

7.6.2　リンクアグリゲーションの転送動作

複数のメンバスイッチと接続するリンクアグリゲーションが転送先となる場合，受信したメンバスイッチのポートへ優先して転送します。フレームを受信したメンバスイッチのポートに優先して振り分けることで，スタックリンクの帯域を有効に利用できます。また，スタックを構成するほかのメンバスイッチに障害が発生しても，通信に影響を受けなくなります。優先振り分けを有効に利用するために，スタックでリンクアグリゲーションを使用する場合は，複数のメンバスイッチにわたって設定することをお勧めします。

一方で，受信したメンバスイッチのポートを優先して転送すると，特定のメンバスイッチのポートにトラフィックが集中する場合があります。この場合は，コンフィグレーションコマンド system port-channel load-balance-all-port を設定することで，リンクアグリゲーションに属するすべてのメンバスイッチのポートを振り分け対象にできます。

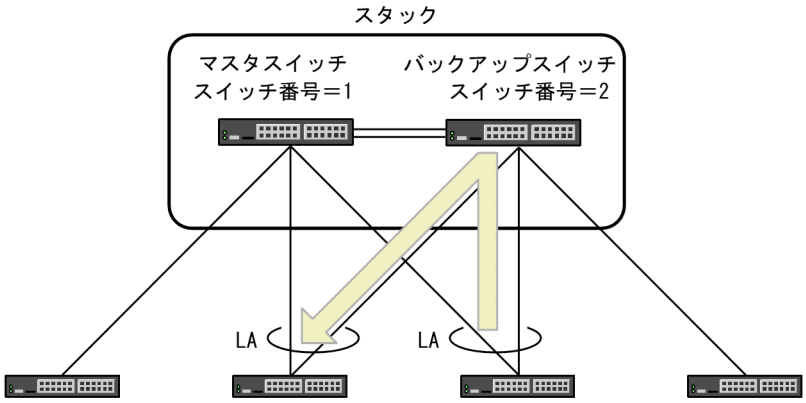
それぞれの転送動作で振り分け対象となるポートが複数存在する場合の転送ポートの選択については，「21.1.5　フレーム送信時のポート振り分け」を参照してください。

(1)　正常時の転送動作

(a)　受信したメンバスイッチのポートを優先する場合

複数のメンバスイッチと接続するリンクアグリゲーションが転送先となる場合，受信したメンバスイッチのポートへ優先して転送します。リンクアグリゲーションで受信したメンバスイッチのポートを優先する場合の正常時の転送動作を次の図に示します。

図 7-12　受信したメンバスイッチのポートを優先する場合の正常時の転送動作（リンクアグリゲーション）

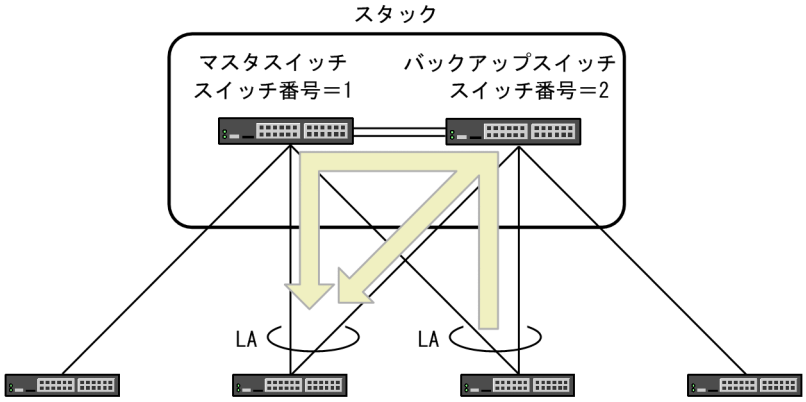


（凡例）LA：リンクアグリゲーション

(b)　すべてのメンバスイッチのポートを振り分け対象とする場合

複数のメンバスイッチと接続するリンクアグリゲーションが転送先となる場合，リンクアグリゲーションに属するすべてのメンバスイッチのポートから選択して転送します。リンクアグリゲーションですべてのメンバスイッチのポートを振り分け対象とする場合の正常時の転送動作を次の図に示します。

図 7-13　すべてのメンバスイッチのポートを振り分け対象とする場合の正常時の転送動作（リンクアグリゲーション）



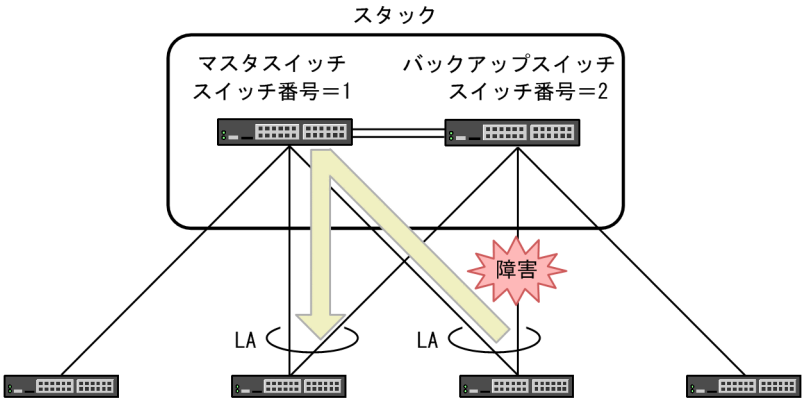
（凡例）LA：リンクアグリゲーション

バックアップスイッチのポートから直接転送する経路と，スタックリンクを経由してマスタスイッチのポートから転送する経路のうち，どちらかを選択して転送します。

(2)　転送元のポート障害時の転送動作

リンクアグリゲーションで転送元のポートが障害になって受信するメンバスイッチが変更された場合，受信したメンバスイッチのポートへ優先して転送します。リンクアグリゲーションで転送元のポート障害時の転送動作を次の図に示します。

図 7-14　転送元のポート障害時の転送動作（リンクアグリゲーション）



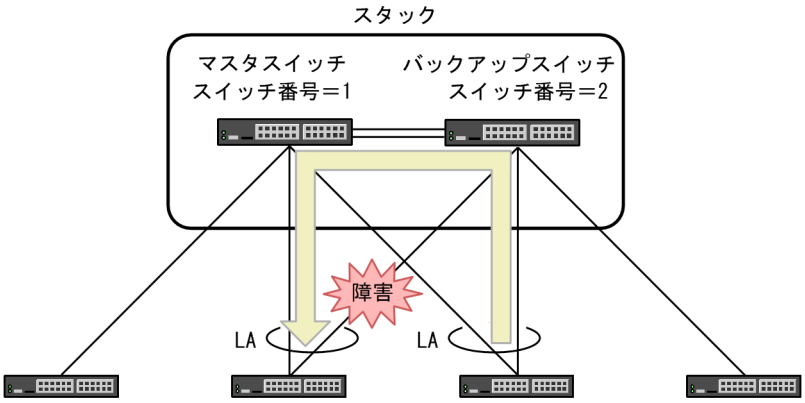
（凡例）LA：リンクアグリゲーション

すべてのメンバスイッチのポートを振り分け対象とする場合は，受信するメンバスイッチが変更されても正常時と同じ方法でポートを選択して転送します。

(3)　転送先のポート障害時の転送動作

リンクアグリゲーションで転送先のポートが障害になって受信したメンバスイッチに転送するポートがない場合，スタックリンクを経由してほかのメンバスイッチのポートへ転送します。リンクアグリゲーションで転送先のポート障害時の転送動作を次の図に示します。

図 7-15　転送先のポート障害時の転送動作（リンクアグリゲーション）



（凡例）LA：リンクアグリゲーション

すべてのメンバスイッチのポートを振り分け対象とする場合は，リンクアグリゲーションに属するすべてのメンバスイッチのポートから障害の発生していないポートを選択して転送します。

7.7　スタックの禁止構成と注意事項

7.7.1　スタックの禁止構成

(1)　メンバスイッチの台数

スタックを構成できるメンバスイッチの台数は 2 台までです。

3 台以上のメンバスイッチではスタックを構成できません。また，1 台のメンバスイッチに異なる 2 台のメンバスイッチをスタックポートで接続しないでください。

(2)　スタックリンク

スタックリンクは回線で直接接続してください。2 台のメンバスイッチを接続するスタックポートの間に，ほかのネットワーク機器を接続しないでください。スタックポートにレイヤ 2 スイッチ，ハブ，メディアコンバータなどのネットワーク機器を接続した場合，スタックの動作を保証できません。

7.7.2　スタックの注意事項

(1)　コンフィグレーションファイルの操作について

- 運用コマンド erase configuration は実行できません。
  初期導入時のコンフィグレーションに戻したい場合は，「8.1.7　スタンドアロンへの転用」の手順を実施したあと，erase configuration コマンドを実行してください。
- ランニングコンフィグレーションファイルをコピー先とする，運用コマンド copy は実行できません。
  ランニングコンフィグレーションファイルを変更する場合は，copy コマンドでスタートアップコンフィグレーションにコピーして，メンバスイッチを再起動してください。
- スタンドアロンで動作している場合，運用コマンド copy で，コンフィグレーションコマンド stack enable が設定されたコンフィグレーションファイルをランニングコンフィグレーションファイルへはコピーできません。
  コピーする場合は，「8.1.2　スタンドアロンからの構築」の手順を実施したあと，copy コマンドを実行してください。
- メンバスイッチ間でソフトウェアバージョンが一致しない場合，またはソフトウェアライセンスおよびオプションライセンスによって有効化された機能が一致しない場合，コンフィグレーションを編集できません。

(2)　装置または VLAN プログラムの再起動が必要なコンフィグレーションについて

スタックでは，変更した内容を反映するために装置または VLAN プログラムの再起動が必要なコンフィグレーションを編集した場合，すべてのメンバスイッチを再起動する必要があります。コンフィグレーションを編集して save コマンドでスタートアップコンフィグレーションに保存したあと，各メンバスイッチを再起動してください。再起動の手順については「8.2.6　スタックの再起動」を参照してください。

該当するのは次に示すコンフィグレーションコマンドです。

- ip route static maximum-paths
- ipv6 route static maximum-paths
- limit-queue-length

- maximum-paths
- swrt_table_resource
- system flowcontrol off
- system l2-table mode
- system interface hundredgigabitethernet enable
- system port-channel load-balance-all-port
- vxlan enable
- swrt_multicast_table

このうち，ip route static maximum-paths，ipv6 route static maximum-paths，および maximum-paths コマンドは，コンフィグレーションの編集後に警告レベルの運用メッセージが出力された場合だけ各メンバスイッチを再起動する必要があります。詳細は「コンフィグレーションガイド Vol.3」「8.4.2 ロードバランス仕様」を参照してください。

なお，すべてのメンバスイッチを再起動しないでコンフィグレーションを変更したメンバスイッチだけ再起動して運用すると，再起動したメンバスイッチにだけ新しいコンフィグレーションが適用されます。

例えば，次に示すコンフィグレーションコマンドでテーブルエントリについてのコンフィグレーションを変更した場合，コンフィグレーションを変更したメンバスイッチだけ再起動して運用すると，テーブルエントリについてメンバスイッチごとに異なる状態で動作します。

- ip route static maximum-paths
- ipv6 route static maximum-paths
- maximum-paths
- swrt_table_resource
- system l2-table mode

このとき，動作が保証されるテーブルエントリ数は，すべてのメンバスイッチの中で最小となる上限値までです。各メンバスイッチのテーブルエントリについて確認するには，運用コマンド show system を実行してください。

(3)　IPv4 マルチキャスト使用時のパケット転送について

スタックで IPv4 マルチキャストを使用すると，マルチキャスト中継エントリの変更時に，該当する中継エントリで中継対象となるパケットをレイヤ 2 転送しないで廃棄することがあります。また，マルチキャスト中継のネガティブキャッシュの変更時にも，該当するネガティブキャッシュでレイヤ 3 廃棄の対象となるパケットをレイヤ 2 転送しないで廃棄することがあります。

(4)　フローコントロールについて

スタックポートではフローコントロールは動作しません。

スタックでフローコントロールを使用して，あるメンバスイッチで受信バッファが枯渇しても，ほかのメンバスイッチではバッファが枯渇しないことがあります。そのため，あるメンバスイッチで送信パケットが滞留して受信バッファが枯渇しても，ほかのメンバスイッチからはポーズパケットが送信されません。

(5)　MAC アドレス学習について

スタックでは，各メンバスイッチが個別に MAC アドレスを学習します。あるメンバスイッチが MAC アドレスを学習してからほかのメンバスイッチへ MAC アドレス学習の結果が反映されるまで，最大 180 秒掛かります。MAC アドレス学習を安定して動作させるために，学習 MAC アドレスのエージングタイムをデフォルトの 300 秒より短くしないことをお勧めします。

なお，各メンバスイッチが個別に MAC アドレスを学習するため，次に示す二つの制限があります。

(a)　MAC アドレス学習の移動検出の制限

PC などの端末を，あるメンバスイッチのポートからほかのポートへ移動した場合，端末が移動した先のメンバスイッチが移動を検出して，各メンバスイッチの MAC アドレステーブルに，移動後に学習した MAC アドレスを反映します。しかし，端末の移動数や移動の頻度によって，次のような障害が発生します。

- 一度に多くの端末が移動すると，移動先を除いて，メンバスイッチの MAC アドレステーブルには，移動前のポートで学習した MAC アドレスが残ることがあります。この状態では移動前のポートにフレームを送信するため，正常に通信できないことがあります。
- MAC アドレステーブルの収容条件数近くまで MAC アドレスを学習している場合，多くの端末の移動が頻発すると，各メンバスイッチで学習した MAC アドレスが上記時間内にほかのメンバスイッチに反映されないことがあります。この場合，反映されていない MAC アドレスを宛先とするフレームがフラッディングされます。

このような場合は，各メンバスイッチで新たに学習した MAC アドレスが，ほかのメンバスイッチに反映されるまで待ってください。

(b)　ユニキャスト通信の制限

2 台の端末がそれぞれ別のメンバスイッチに接続している場合，この 2 台の端末間でユニキャスト通信をしても，どちらかの端末からのユニキャスト通信が VLAN 内にフラッディングされることがあります。その場合，次のどちらかの条件が満たされるまで，待ってください。

- フラッディングされたフレームの宛先である端末から，マルチキャストパケットまたはブロードキャストパケットが送信される
- 各メンバスイッチが学習した MAC アドレスがほかのメンバスイッチに反映される

(6)　スタックで使用していたメンバスイッチの転用について

スタックでは，初めてスタックを構成したときのマスタスイッチの筐体 MAC アドレスが装置 MAC アドレスとなります。その後，マスタスイッチに障害が発生しても装置 MAC アドレスは変更しません。

そのため，スタックで使用していたメンバスイッチをスタックから外してこの装置を該当するスタックと同じネットワークに接続するときは，あらかじめ，スタックの装置 MAC アドレスと外したメンバスイッチの筐体 MAC アドレスが異なることを確認してください。同じ場合には，該当するメンバスイッチをスタックから外したあとスタックを再起動することで，スタックの装置 MAC アドレスを変更してください。

なお，スタックの装置 MAC アドレスについては「7.3.5　スタックの装置 MAC アドレス」を，スタックの再起動については「8.2.6　スタックの再起動」を参照してください。

(7)　マスタスイッチを切り替える場合について

パケットの転送を継続したままマスタスイッチを切り替える場合は，次のどちらも満たしていることを確認してから切り替えてください。

- バックアップスイッチの初期化が完了している
- バックアップスイッチのポートがアップしている

バックアップスイッチの初期化中にマスタスイッチを切り替えると，初期化中のバックアップスイッチは再起動するためパケットの転送を継続できません。

バックアップスイッチの初期化が完了しているかどうか運用コマンド show switch で確認できます。また，ポートがアップしているかどうか運用コマンド show port で確認できます。

(8)　マスタ選出優先度 1 を使用する場合について

マスタ選出優先度 1 のメンバスイッチ 1 台で構成されたスタックに，マスタ選出優先度 2 以上のメンバスイッチ 1 台で構成されたスタックを接続した場合，マスタ選出優先度 2 以上のメンバスイッチがマスタスイッチに選ばれます。マスタ選出優先度 1 のメンバスイッチは再起動し，バックアップスイッチとしてスタックに加わります。マスタ選出優先度 2 以上のメンバスイッチは，再起動することなくマスタ状態を継続するため，スタックの転送機能は維持されます。

しかし，マスタ選出優先度 1 のメンバスイッチ 1 台で構成されたスタックに，マスタ選出優先度 2 以上のメンバスイッチを接続して起動した場合，マスタ選出優先度 2 以上のメンバスイッチは，マスタスイッチを検出するため，初期状態でマスタスイッチからのバックアップ遷移指示を待ちます。同時に，マスタ選出優先度 1 のメンバスイッチは，マスタ選出優先度 2 以上のメンバスイッチを検出するため，再起動します。バックアップ遷移指示を待っていたメンバスイッチは，マスタスイッチの不在を検出し，再起動します。この間，マスタ選出優先度 2 以上のメンバスイッチがマスタスイッチとして初期化を完了するまで，通信断となります。

このように，マスタ選出優先度 1 を使用すると，マスタスイッチを切り替えるときに，通信断の時間が長くなることがあります。

マスタ選出優先度 1 は，既存のスタックにメンバスイッチを追加する場合に，意図しないコンフィグレーションの置き換えを防ぐための，一時的な運用に使用してください。通常の運用で，マスタ選出優先度 1 を使用してマスタスイッチの選出を固定するような設定は，お勧めしません。スタック構築後は，マスタ選出優先度 2 以上を設定して運用することをお勧めします。

(9)　ストームコントロール使用時のメンバスイッチの起動時間について

スタックで，受信フレーム数の閾値を設定してストームコントロールを使用している場合，メンバスイッチを追加すると，ストームコントロールを使用しない場合と比べて，追加したメンバスイッチの起動完了までの時間が数分程度長くなります。なお，メンバスイッチの追加とは次のようなことを指します。

- メンバスイッチ 1 台で構成しているスタックに，ほかのメンバスイッチを追加する
- メンバスイッチ 2 台で構成しているスタックで，一方のメンバスイッチを再起動する
- メンバスイッチ 2 台で構成しているスタックで，ソフトウェアアップデートする

(10)　スタック構成時のマネージメントポートの扱いについて

マネージメントポートはマスタスイッチだけで動作し，バックアップスイッチのマネージメントポートは閉塞します。

バックアップスイッチからマスタスイッチに切り替わった装置では，マネージメントポートが動作するようになります。この場合，マネージメントポートの MAC アドレスが変更されるため，運用端末側のアドレス情報が更新されるまで通信できません。

(11)　スタックリンクを接続できるポートの組み合わせについて

スタックリンクは，接続できるポートおよび接続インタフェースの組み合わせに制限があります。サポートしていない組み合わせで使用した場合，動作を保証できません。

表 7-7　スタックリンクを接続できるポートの組み合わせ（40GBASE-R での接続）

接続インタフェース	マスタスイッチ	バックアップスイッチ		
	ポート種別 ポート番号	QSFP+ポート※1	QSFP28/QSFP+ 共用ポート※2 ポート 49～50	QSFP28/QSFP+ 共用ポート※2 ポート 51～52
40GBASE-SR4 40GBASE-LR4	QSFP+ポート※1	○	○	○
	QSFP28/QSFP+ 共用ポート※2 ポート 49～50	○	○	○
	QSFP28/QSFP+ 共用ポート※2 ポート 51～52	○	○	○
40GBASE-CR4	QSFP+ポート※1	○	○	×
	QSFP28/QSFP+ 共用ポート※2 ポート 49～50	○	○	×
	QSFP28/QSFP+ 共用ポート※2 ポート 51～52	×	×	○

（凡例）○：サポート　×：未サポート

注※1

IP8800/S3660-24T4X，IP8800/S3660-24T4XW，IP8800/S3660-48T4XW，IP8800/S3660-16S4XW，および IP8800/S3660-24S8XW

注※2

IP8800/S3660-48XT4QW，IP8800/S3660-24X4QW，および IP8800/S3660-48X4QW

表 7-8　スタックリンクを接続できるポートの組み合わせ（100GBASE-R での接続）

接続インタフェース	マスタスイッチ	バックアップスイッチ	
	ポート種別 ポート番号	QSFP28/QSFP+ 共用ポート※ ポート 49～50	QSFP28/QSFP+ 共用ポート※ ポート 51～52
100GBASE-SR4 100GBASE-CWDM4 100GBASE-LR4 100GBASE-4WDM-40	QSFP28/QSFP+共用ポート※ ポート 49～50	×	×
	QSFP28/QSFP+共用ポート※ ポート 51～52	×	×
100GBASE-CR4	QSFP28/QSFP+共用ポート※	○	×

接続インタフェース	マスタスイッチ	バックアップスイッチ	
	ポート種別 ポート番号	QSFP28/QSFP+ 共用ポート※ ポート 49～50	QSFP28/QSFP+ 共用ポート※ ポート 51～52
	ポート 49～50		
	QSFP28/QSFP+共用ポート※ ポート 51～52	×	○

（凡例）○：サポート　×：未サポート

注※　IP8800/S3660-48XT4QW，IP8800/S3660-24X4QW，および IP8800/S3660-48X4QW

8 スタックの設定と運用

この章ではスタックのオペレーションについて説明します。

8.1　スタックの設定

この節では，コンフィグレーションコマンドおよび運用コマンドを使用したスタックの構築と，スタンドアロンへの転用について説明します。

8.1.1　コンフィグレーション・運用コマンド一覧

スタックのコンフィグレーションコマンド一覧を次の表に示します。

表 8-1　コンフィグレーションコマンド一覧

コマンド名	説明
stack enable	スタック機能を有効にします。
switch priority	マスタ選出優先度を設定します。
switch provision	スタックを構成するメンバスイッチのモデルを設定します。
switchport mode※	スタックを構成するメンバスイッチ間を接続するポートを設定します。

注※
「コンフィグレーションコマンドレファレンス Vol.1」「18　VLAN」を参照してください。

スタックの設定に使用する運用コマンド一覧を次の表に示します。

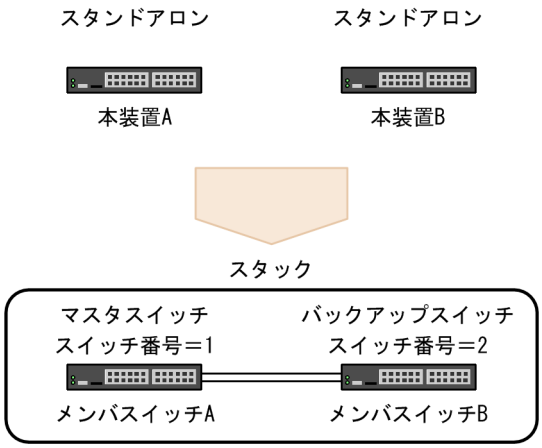
表 8-2　運用コマンド一覧（スタックの設定）

コマンド名	説明
set switch	メンバスイッチのスイッチ番号を設定します。

8.1.2　スタンドアロンからの構築

次の図に示すように，スタンドアロンの本装置 A および本装置 B からスタックを構築します。

図 8-1　スタンドアロンからの構築



スタンドアロンからスタックを構築する流れを次の表に示します。

表 8-3　スタンドアロンからスタックを構築する流れ

操作の流れとその内容	設定対象
(1)　本装置 A と本装置 B のライセンスとソフトウェアを確認 • ソフトウェアライセンスおよびオプションライセンスの確認 • ソフトウェアバージョンの確認	本装置 A (メンバスイッチ A) 本装置 B (メンバスイッチ B)
(2)　本装置 A をスイッチ番号 1 として 1 台スタックへ移行 • スタック機能の設定 • 装置の再起動	本装置 A (メンバスイッチ A)
(3)　メンバスイッチ A とメンバスイッチ B のコンフィグレーションの設定 • メンバスイッチ A のスタックポートの設定※ • メンバスイッチ A のマスタ選出優先度の設定 • メンバスイッチ B のモデルの設定 • メンバスイッチ B のスタックポートの設定※ • メンバスイッチ B のマスタ選出優先度の設定	本装置 A (メンバスイッチ A)
(4)　本装置 B をスイッチ番号 2 として 1 台スタックへ移行 • スイッチ番号の設定 • スタック機能の設定 • 装置の再起動	本装置 B (メンバスイッチ B)
(5)　メンバスイッチ A と接続するためのメンバスイッチ B のコンフィグレーションの設定 • スタックポートの設定※ • マスタ選出優先度の設定（1 に設定）	本装置 B (メンバスイッチ B)
(6)　メンバスイッチ A とメンバスイッチ B の 2 台スタックへ移行 • スタックポートの接続	－

(凡例) －：該当なし

注※

スタック専用ポートを実装するモデルでは，この操作は不要です。

スタック機能を設定してから装置を再起動すると，ランニングコンフィグレーションに対してスタックポートを設定したイーサネットインタフェース（スタック専用ポート）が反映された状態で装置が起動します。

(1)　本装置 A と本装置 B のライセンスとソフトウェアを確認

本装置 A と本装置 B のソフトウェアライセンスとオプションライセンス，およびソフトウェアのバージョンを確認します。

本装置 A と本装置 B とでソフトウェアライセンスおよびオプションライセンスによって有効化される機能が異なる場合は，ソフトウェアライセンスおよびオプションライセンスを設定し直して一致させてください。本装置 A と本装置 B とでソフトウェアのバージョンが異なる場合には，ソフトウェアのバージョンをアップデートして一致させてください。

[手順]

1.
```
> show license
Date 20XX/10/26 12:00:00 UTC
  Available: SL-L3L-004
```

```
       Serial Number        Licensed software
       1500-abcd-0009-0000  SL-L3L-004(AX-P3660-G8)
```

本装置 A でソフトウェアライセンスおよびオプションライセンスを確認します。

```
2. > show version software
   Date 20XX/10/26 12:01:00 UTC
   S/W: OS-L3M Ver. 12.0
```

本装置 A でソフトウェアのバージョンを確認します。

```
3. > show license
   Date 20XX/10/26 13:00:00 UTC
     Available: SL-L3L-004
       Serial Number        Licensed software
       1500-abcd-0009-0000  SL-L3L-004(AX-P3660-G8)
```

本装置 B でソフトウェアライセンスおよびオプションライセンスを確認します。手順 1 で確認した本装置 A のソフトウェアライセンスおよびオプションライセンスと同じであることを確認してください。

```
4. > show version software
   Date 20XX/10/26 13:01:00 UTC
   S/W: OS-L3M Ver. 12.0
```

本装置 B でソフトウェアのバージョンを確認します。手順 2 で確認した本装置 A のソフトウェアのバージョンと同じであることを確認してください。

(2) 本装置 A をスイッチ番号 1 として 1 台スタックへ移行

本装置 A で，スタック機能を有効にする設定をします。

[設定のポイント]

本装置をスタックで動作させるには，stack enable コマンドを設定します。stack enable コマンドの設定を有効にするには，本装置の再起動が必要です。そのため，運用を開始する前に設定してください。また，stack enable コマンドを設定すると，本装置を再起動するまですべてのコンフィグレーションが変更できません。

なお，stack enable コマンドを設定すると，同時に次のコンフィグレーションが自動で設定されます。

- no service ipv6 dhcp

このため，stack enable コマンドを設定する前に，IPv6 DHCP サーバ機能などスタックでサポートしていない機能を使用していないことを確認してください。

[コマンドによる設定]

1. **(config)# stack enable**

   After this command execute, please save configuration editing now in startup-config, and please reboot a device.

   Do you wish to continue ? (y/n):

   スタックで動作させる設定をします。コンフィグレーションの変更確認メッセージに対して y を入力します。

2. **(config)# save**

   (config)# exit

   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

3. **# reload**

   本装置を再起動します。再起動後，本装置は 1 台構成のスタックのメンバスイッチとして動作します。

(3)　メンバスイッチ A とメンバスイッチ B のコンフィグレーションの設定

メンバスイッチ A に，スタックを構成するすべてのメンバスイッチのコンフィグレーションを設定します。

[設定のポイント]

バックアップスイッチとなるメンバスイッチ B のコンフィグレーションは，マスタスイッチとなるメンバスイッチ A のコンフィグレーションに同期します。そのため，メンバスイッチ A では次のコンフィグレーションを設定する必要があります。

- メンバスイッチ A のスタックポート
- メンバスイッチ A のマスタ選出優先度
- メンバスイッチ B のモデル
- メンバスイッチ B のスタックポート
- メンバスイッチ B のマスタ選出優先度

メンバスイッチ B のモデルを設定すると，指定したモデルに対応するイーサネットインタフェースのコンフィグレーションが自動で作成されます。また，メンバスイッチ A がマスタスイッチになるように，メンバスイッチ A のマスタ選出優先度をメンバスイッチ B より大きい値に設定します。

[コマンドによる設定]

1. **(config)# interface hundredgigabitethernet 1/0/49**
   (config-if)# switchport mode stack
   (config-if)# exit
   (config)# interface hundredgigabitethernet 1/0/50
   (config-if)# switchport mode stack
   (config-if)# exit
   メンバスイッチ A（スイッチ番号 1）のイーサネットインタフェースにスタックポートを設定します。
2. **(config)# switch 1 priority 20**
   メンバスイッチ A（スイッチ番号 1）のマスタ選出優先度を 20 に設定します。
3. **(config)# switch 2 provision 3660-48xt4qw**
   メンバスイッチ B として予定している装置のモデルを設定します。ここでは，モデルを IP8800/S3660-48XT4QW で設定しています。
4. **(config)# interface hundredgigabitethernet 2/0/49**
   (config-if)# switchport mode stack
   (config-if)# exit
   (config)# interface hundredgigabitethernet 2/0/50
   (config-if)# switchport mode stack
   (config-if)# exit
   メンバスイッチ B（スイッチ番号 2）のイーサネットインタフェースにスタックポートを設定します。
5. **(config)# switch 2 priority 10**
   メンバスイッチ B（スイッチ番号 2）のマスタ選出優先度を 10 に設定します。
6. **(config)# save**
   (config)# exit
   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

(4) 本装置 B をスイッチ番号 2 として 1 台スタックへ移行

本装置 B のスイッチ番号を 2 にして，スタック機能を有効にする設定をします。

[設定のポイント]

本装置 B のスイッチ番号を 2 に設定します。その後，stack enable コマンドでスタックで動作させる設定をしてから本装置を再起動する必要があります。

[コマンドによる設定]

1. **# set switch 2**
   # configure
   スイッチ番号を 2 に設定します。
2. **(config)# stack enable**
   After this command execute, please save configuration editing now in startup-config, and please reboot a device.
   Do you wish to continue ? (y/n):
   スタックで動作させる設定をします。コンフィグレーションの変更確認メッセージに対して y を入力します。
3. **(config)# save**
   (config)# exit
   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。
4. **# reload**
   本装置を再起動します。再起動後，本装置は 1 台構成のスタックのメンバスイッチとして動作します。

(5) メンバスイッチ A と接続するためのメンバスイッチ B のコンフィグレーションの設定

メンバスイッチ B に，メンバスイッチ A と接続してスタックを構成するための最小限のコンフィグレーションを設定します。

[設定のポイント]

メンバスイッチ A と接続したときにメンバスイッチ A が障害などで再起動してもメンバスイッチ B がマスタスイッチとして動作しないように，メンバスイッチ B のマスタ選出優先度を 1 に設定します。

なお，ここで設定したコンフィグレーションは，マスタスイッチとなるメンバスイッチ A で設定したコンフィグレーションに置き換えられます。

[コマンドによる設定]

1. **(config)# interface hundredgigabitethernet 2/0/49**
   (config-if)# switchport mode stack
   (config-if)# exit
   (config)# interface hundredgigabitethernet 2/0/50
   (config-if)# switchport mode stack
   (config-if)# exit
   メンバスイッチ B（スイッチ番号 2）のイーサネットインタフェースにスタックポートを設定します。
2. **(config)# switch 2 priority 1**
   メンバスイッチ B（スイッチ番号 2）のマスタ選出優先度を 1 に設定します。

3. **(config)# save**

   (config)# exit

   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

(6)　メンバスイッチ A とメンバスイッチ B の 2 台スタックへ移行

それぞれ 1 台構成のスタックのメンバスイッチとして動作しているメンバスイッチ A とメンバスイッチ B のスタックポートを接続して，2 台構成のスタックに移行します。

メンバスイッチ B のマスタ選出優先度が 1 のため，メンバスイッチ A はマスタスイッチとして動作を継続して，メンバスイッチ B は自動で再起動します。

再起動後，メンバスイッチ A のコンフィグレーションに同期するためにメンバスイッチ B は自動で再起動します。その後，メンバスイッチ A がマスタスイッチ，メンバスイッチ B がバックアップスイッチとなるスタック構成で動作します。

[手順]

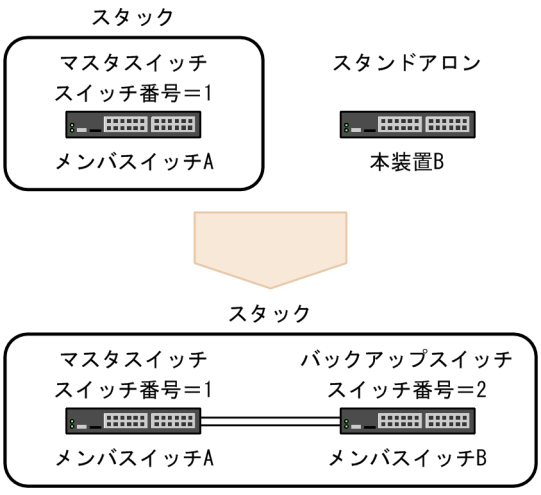
1. メンバスイッチ A とメンバスイッチ B のスタックポートを接続します。
2. **# show switch detail**

   運用コマンド show switch detail を実行して，メンバスイッチ A がマスタスイッチ，メンバスイッチ B がバックアップスイッチとなるスタックで動作していることを確認します。

8.1.3　メンバスイッチの追加

次の図に示すように，メンバスイッチ A が 1 台で構成しているスタックにスタンドアロンの本装置 B を追加します。

図 8-2　メンバスイッチの追加



メンバスイッチを追加する流れを次の表に示します。

表 8-4　メンバスイッチを追加する流れ

操作の流れとその内容	設定対象
(1)　メンバスイッチ A と本装置 B のライセンスとソフトウェアを確認	メンバスイッチ A

操作の流れとその内容	設定対象
• ソフトウェアライセンスおよびオプションライセンスの確認 • ソフトウェアバージョンの確認	本装置 B （メンバスイッチ B）
(2)　メンバスイッチ B のコンフィグレーションの設定 • メンバスイッチ B のモデルの設定 • メンバスイッチ B のスタックポートの設定※1 • メンバスイッチ B のマスタ選出優先度の設定	メンバスイッチ A
(3)　本装置 B をスイッチ番号 2 として 1 台スタックへ移行 • スイッチ番号の設定 • スタック機能の設定 • 装置の再起動	本装置 B （メンバスイッチ B）
(4)　メンバスイッチ A と接続するためのメンバスイッチ B のコンフィグレーションの設定 • スタックポートの設定※2 • マスタ選出優先度の設定（1 に設定）	本装置 B （メンバスイッチ B）
(5)　メンバスイッチ A とメンバスイッチ B の 2 台スタックへ移行 • スタックポートの接続	－

（凡例）－：該当なし

注※1

メンバスイッチ B がスタック専用ポートを実装するモデルの場合，スタック機能が動作している状態でメンバスイッチ B のモデルを設定すると，メンバスイッチ B のスタック専用ポートに対してスタックポートを設定したものとして，対応するイーサネットインタフェースのコンフィグレーションが自動で作成されます。そのため，この操作は不要です。

注※2

メンバスイッチ B がスタック専用ポートを実装するモデルの場合，この操作は不要です。

スタック機能を設定してから装置を再起動すると，ランニングコンフィグレーションに対してスタックポートを設定したイーサネットインタフェース（スタック専用ポート）が反映された状態で装置が起動します。

(1)　メンバスイッチ A と本装置 B のライセンスとソフトウェアを確認

動作しているメンバスイッチ A と，追加する本装置 B のソフトウェアライセンスとオプションライセンス，およびソフトウェアのバージョンを確認します。

メンバスイッチ A と本装置 B とでソフトウェアライセンスおよびオプションライセンスによって有効化される機能が異なる場合は，メンバスイッチ A に合わせて本装置 B のソフトウェアライセンスおよびオプションライセンスを設定し直してください。メンバスイッチ A と本装置 B とでソフトウェアのバージョンが異なる場合には，本装置 B のソフトウェアをメンバスイッチ A と同じソフトウェアのバージョンにアップデートして一致させてください。

[手順]

1.
```
> show license
Date 20XX/10/26 12:00:00 UTC
  Available: SL-L3L-004
    Serial Number        Licensed software
    1500-abcd-0009-0000  SL-L3L-004(AX-P3660-G8)
```
メンバスイッチ A でソフトウェアライセンスおよびオプションライセンスを確認します。

```
2. > show version software
   Date 20XX/10/26 12:01:00 UTC
   S/W: OS-L3M Ver. 12.0
```

メンバスイッチ A でソフトウェアのバージョンを確認します。

```
3. > show license
   Date 20XX/10/26 13:00:00 UTC
     Available: SL-L3L-004
       Serial Number        Licensed software
       1500-1234-0009-0000  SL-L3L-004(AX-P3660-G8)
```

本装置 B でソフトウェアライセンスおよびオプションライセンスを確認します。手順 1 で確認したメンバスイッチ A と同じであることを確認してください。

```
4. > show version software
   Date 20XX/10/26 13:01:00 UTC
   S/W: OS-L3M Ver. 12.0
```

本装置 B でソフトウェアのバージョンを確認します。手順 2 で確認したメンバスイッチ A のソフトウェアのバージョンと同じであることを確認してください。

(2)　メンバスイッチ B のコンフィグレーションの設定

メンバスイッチ A に，追加するメンバスイッチ B のコンフィグレーションを設定します。なお，メンバスイッチ A には，次に示すスタックポートおよびマスタ選出優先度のコンフィグレーションが設定されているものとします。

```
switch 1 priority 20
!
interface hundredgigabitethernet 1/0/49
  switchport mode stack
!
interface hundredgigabitethernet 1/0/50
  switchport mode stack
```

[設定のポイント]

バックアップスイッチとなるメンバスイッチ B のコンフィグレーションは，マスタスイッチとなるメンバスイッチ A のコンフィグレーションに同期します。そのため，メンバスイッチ A では次のコンフィグレーションを設定する必要があります。

- メンバスイッチ B のモデル
- メンバスイッチ B のスタックポート
- メンバスイッチ B のマスタ選出優先度

メンバスイッチ B のモデルを設定すると，指定したモデルに対応するイーサネットインタフェースのコンフィグレーションが自動で作成されます。また，メンバスイッチ B がバックアップスイッチになるように，メンバスイッチ B のマスタ選出優先度をメンバスイッチ A より小さい値に設定します。

[コマンドによる設定]

1. **(config)# switch 2 provision 3660-48xt4qw**

   メンバスイッチ B として予定している装置のモデルを設定します。ここでは，モデルを IP8800/S3660-48XT4QW で設定しています。

2. **(config)# interface hundredgigabitethernet 2/0/49**

   (config-if)# switchport mode stack

   (config-if)# exit

   (config)# interface hundredgigabitethernet 2/0/50

   (config-if)# switchport mode stack

   (config-if)# exit

メンバスイッチ B（スイッチ番号 2）のイーサネットインタフェースにスタックポートを設定します。

3. **(config)# switch 2 priority 10**
   メンバスイッチ B（スイッチ番号 2）のマスタ選出優先度を 10 に設定します。
4. **(config)# save**
   (config)# exit
   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

(3) 本装置 B をスイッチ番号 2 として 1 台スタックへ移行

本装置 B のスイッチ番号を 2 にして，スタック機能を有効にする設定をします。

[設定のポイント]

本装置 B のスイッチ番号を 2 に設定します。その後，stack enable コマンドでスタックで動作させる設定をしてから本装置を再起動する必要があります。そのため，運用を開始する前に設定してください。また，stack enable コマンドを設定すると，本装置を再起動するまですべてのコンフィグレーションが変更できません。

なお，stack enable コマンドを設定すると，同時に次のコンフィグレーションが自動で設定されます。

- no service ipv6 dhcp

[コマンドによる設定]

1. **# set switch 2**
   # configure
   スイッチ番号を 2 に設定します。
2. **(config)# stack enable**
   After this command execute, please save configuration editing now in startup-config, and please reboot a device.
   Do you wish to continue ? (y/n):
   スタックで動作させる設定をします。コンフィグレーションの変更確認メッセージに対して y を入力します。
3. **(config)# save**
   (config)# exit
   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。
4. **# reload**
   本装置を再起動します。再起動後，本装置は 1 台構成のスタックのメンバスイッチとして動作します。

(4) メンバスイッチ A と接続するためのメンバスイッチ B のコンフィグレーションの設定

メンバスイッチ B に，メンバスイッチ A と接続してスタックを構成するための最小限のコンフィグレーションを設定します。

[設定のポイント]

メンバスイッチ A と接続したときにメンバスイッチ A が障害などで再起動してもメンバスイッチ B がマスタスイッチとして動作しないように，メンバスイッチ B のマスタ選出優先度を 1 に設定します。

なお，ここで設定したコンフィグレーションは，マスタスイッチとなるメンバスイッチ A で設定したコンフィグレーションに置き換えられます。

[コマンドによる設定]

1. **(config)# interface hundredgigabitethernet 2/0/49**
   (config-if)# switchport mode stack
   (config-if)# exit
   (config)# interface hundredgigabitethernet 2/0/50
   (config-if)# switchport mode stack
   (config-if)# exit
   メンバスイッチ B（スイッチ番号 2）のイーサネットインタフェースにスタックポートを設定します。
2. **(config)# switch 2 priority 1**
   メンバスイッチ B（スイッチ番号 2）のマスタ選出優先度を 1 に設定します。
3. **(config)# save**
   (config)# exit
   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

(5)　メンバスイッチ A とメンバスイッチ B の 2 台スタックへ移行

それぞれ 1 台構成のスタックのメンバスイッチとして動作しているメンバスイッチ A とメンバスイッチ B のスタックポートを接続して，2 台構成のスタックに移行します。

メンバスイッチ B のマスタ選出優先度が 1 のため，メンバスイッチ A はマスタスイッチとして動作を継続して，メンバスイッチ B は自動で再起動します。

再起動後，メンバスイッチ A のコンフィグレーションに同期するためにメンバスイッチ B は自動で再起動します。その後，メンバスイッチ A がマスタスイッチ，メンバスイッチ B がバックアップスイッチとなるスタック構成で動作します。

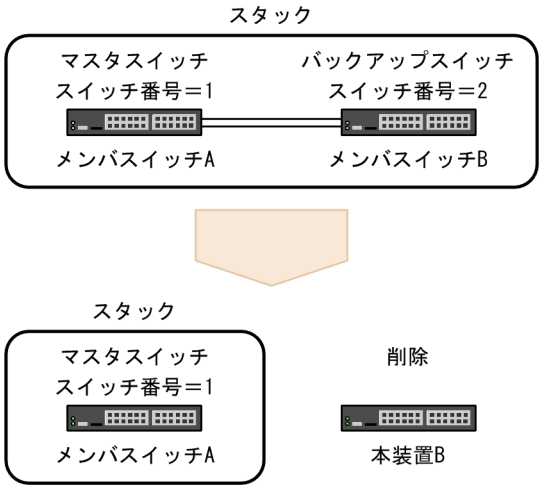
[手順]

1. メンバスイッチ A とメンバスイッチ B のスタックポートを接続します。
2. **# show switch detail**
   運用コマンド show switch detail を実行して，メンバスイッチ A がマスタスイッチ，メンバスイッチ B がバックアップスイッチとなるスタックで動作していることを確認します。

8.1.4　メンバスイッチの削除（バックアップスイッチ）

次の図に示すように，マスタスイッチとして動作するメンバスイッチ A とバックアップスイッチとして動作するメンバスイッチ B で構成するスタックから，メンバスイッチ B を削除します。

図 8-3　メンバスイッチの削除（バックアップスイッチ）



メンバスイッチ（バックアップスイッチ）を削除する流れを次の表に示します。

表 8-5　メンバスイッチ（バックアップスイッチ）を削除する流れ

操作の流れとその内容	設定対象
(1)　メンバスイッチ B の停止	本装置 B （メンバスイッチ B）
(2)　メンバスイッチ B のコンフィグレーションの削除 • モデルの削除 • マスタ選出優先度の削除	メンバスイッチ A

(1)　メンバスイッチ B の停止

メンバスイッチ B にログインして，メンバスイッチ B を停止します。

[手順]

1. **> reload stop**
   メンバスイッチ B を停止します。
   なお，マスタスイッチであるメンバスイッチ A からもメンバスイッチ B を停止できます。その場合は，メンバスイッチ A にログインして次のコマンドを実行してください。

   ```
   > reload switch 2 stop
   ```

2. 電源を OFF にして，スタック構成から外します。

(2)　メンバスイッチ B のコンフィグレーションの削除

マスタスイッチであるメンバスイッチ A から，削除したメンバスイッチ B のコンフィグレーションを削除します。

[設定のポイント]

メンバスイッチ A のコンフィグレーションからメンバスイッチ B のモデルを削除すると，対応するイーサネットインタフェースのコンフィグレーションも削除されます。

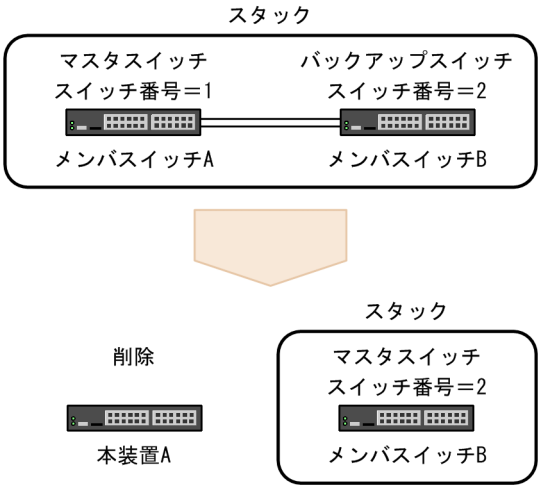
[コマンドによる設定]

1. **(config)# no switch 2 provision**
   スイッチ番号 2 のモデルを削除します。モデルを削除すると，指定したモデルに対応するイーサネットインタフェースのコンフィグレーションも削除されます。
2. **(config)# no switch 2 priority**
   スイッチ番号 2 のマスタ選出優先度を削除します。
3. **(config)# save**
   (config)# exit
   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

8.1.5　メンバスイッチの削除（マスタスイッチ）

次の図に示すように，マスタスイッチとして動作するメンバスイッチ A とバックアップスイッチとして動作するメンバスイッチ B で構成するスタックから，メンバスイッチ A を削除します。

図 8-4　メンバスイッチの削除（マスタスイッチ）



メンバスイッチ（マスタスイッチ）を削除する流れを次の表に示します。

表 8-6　メンバスイッチ（マスタスイッチ）を削除する流れ

操作の流れとその内容	設定対象
(1)　メンバスイッチ B の状態確認 • 初期化が完了していることの確認 • ポートがアップしていることの確認	メンバスイッチ B
(2)　メンバスイッチ A の停止	本装置 A （メンバスイッチ A）
(3)　メンバスイッチ A のコンフィグレーションの削除 • モデルの削除 • マスタ選出優先度の削除	メンバスイッチ B

(1)　メンバスイッチ B の状態確認

メンバスイッチ A にログインして，メンバスイッチ B の状態を確認します。

[手順]

1. **> show switch**
   メンバスイッチ B の初期化が完了していることを確認します。
2. **> show port**
   メンバスイッチ B のポートがアップしていることを確認します。

(2)　メンバスイッチ A の停止

メンバスイッチ A を停止します。

[手順]

1. **> reload stop**
   メンバスイッチ A を停止します。メンバスイッチ B はバックアップスイッチからマスタスイッチに遷移します。
2. 電源を OFF にして，スタック構成から外します。

(3)　メンバスイッチ A のコンフィグレーションの削除

マスタスイッチであるメンバスイッチ B から，削除したメンバスイッチ A のコンフィグレーションを削除します。

[設定のポイント]

メンバスイッチ B のコンフィグレーションからメンバスイッチ A のモデルを削除すると，対応するイーサネットインタフェースのコンフィグレーションも削除されます。

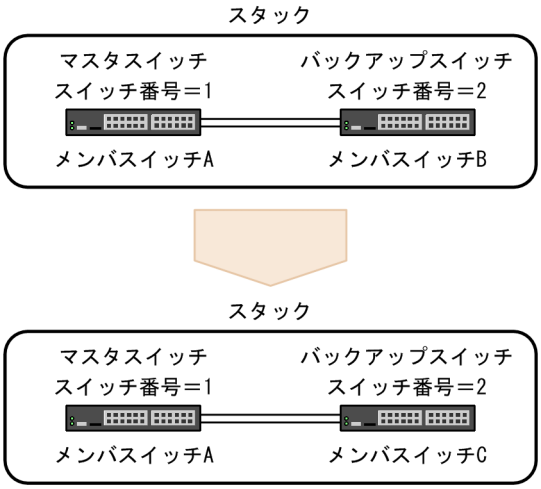
[コマンドによる設定]

1. **(config)# no switch 1 provision**
   スイッチ番号 1 のモデルを削除します。モデルを削除すると，指定したモデルに対応するイーサネットインタフェースのコンフィグレーションも削除されます。
2. **(config)# no switch 1 priority**
   スイッチ番号 1 のマスタ選出優先度を削除します。
3. **(config)# save**
   (config)# exit
   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

8.1.6　メンバスイッチの交換

次の図に示すように，マスタスイッチとして動作するメンバスイッチ A とバックアップスイッチとして動作するメンバスイッチ B で構成するスタックで，メンバスイッチ B をメンバスイッチ C に交換します。

図 8-5　メンバスイッチの交換



メンバスイッチを交換する流れを次の表に示します。

表 8-7　メンバスイッチを交換する流れ

操作の流れとその内容	設定対象
(1)　メンバスイッチ A と本装置 C のライセンスとソフトウェアを確認 • ソフトウェアライセンスおよびオプションライセンスの確認 • ソフトウェアバージョンの確認	メンバスイッチ A 本装置 C (メンバスイッチ C)
(2)　メンバスイッチ B の停止	メンバスイッチ B
(3)　本装置 C をスイッチ番号 2 として 1 台スタックへ移行 • スイッチ番号の設定 • スタック機能の設定 • 装置の再起動	本装置 C (メンバスイッチ C)
(4)　メンバスイッチ A と接続するためのメンバスイッチ C のコンフィグレーションの設定 • スタックポートの設定※ • マスタ選出優先度の設定（1 に設定）	本装置 C (メンバスイッチ C)
(5)　メンバスイッチ A とメンバスイッチ C の 2 台スタックへ移行 • スタックポートの接続	－

(凡例) －：該当なし

注※

メンバスイッチ C がスタック専用ポートを実装するモデルの場合，この操作は不要です。

スタック機能を設定してから装置を再起動すると，ランニングコンフィグレーションに対してスタックポートを設定したイーサネットインタフェース（スタック専用ポート）が反映された状態で装置が起動します。

(1)　メンバスイッチ A と本装置 C のライセンスとソフトウェアを確認

動作しているメンバスイッチ A と，交換する本装置 C のソフトウェアライセンスとオプションライセンス，およびソフトウェアのバージョンを確認します。

メンバスイッチ A と本装置 C とでソフトウェアライセンスおよびオプションライセンスによって有効化される機能が異なる場合は，メンバスイッチ A に合わせて本装置 C にソフトウェアライセンスおよびオプションライセンスを設定してください。メンバスイッチ A と本装置 C とでソフトウェアのバージョンが異なる場合には，本装置 C のソフトウェアをメンバスイッチ A と同じソフトウェアのバージョンにアップデートして一致させてください。

[手順]

1.
```
> show license
Switch 1 (Master)
-----------------
Date 20XX/10/26 12:00:00 UTC
  Available: SL-L3L-004
    Serial Number        Licensed software
    1500-abcd-0009-0000  SL-L3L-004(AX-P3660-G8)

Switch 2 (Backup)
-----------------
Date 20XX/10/26 12:00:00 UTC
  Available: SL-L3L-004
    Serial Number        Licensed software
    1500-1234-0009-0000  SL-L3L-004(AX-P3660-G8)
```
メンバスイッチ A でソフトウェアライセンスおよびオプションライセンスを確認します。

2.
```
> show version software
Switch 1 (Master)
-----------------
Date 20XX/10/26 12:01:00 UTC
S/W: OS-L3M Ver. 12.0

Switch 2 (Backup)
-----------------
Date 20XX/10/26 12:01:00 UTC
S/W: OS-L3M Ver. 12.0
```
メンバスイッチ A でソフトウェアのバージョンを確認します。

3.
```
> show license
Date 20XX/10/26 13:00:00 UTC
  Available: SL-L3L-004
    Serial Number        Licensed software
    1500-1234-0009-0000  SL-L3L-004(AX-P3660-G8)
```
本装置 C でソフトウェアライセンスおよびオプションライセンスを確認します。手順 1 で確認したメンバスイッチ A のソフトウェアライセンスおよびオプションライセンスと有効化される機能が同じであることを確認してください。

4.
```
> show version software
Date 20XX/10/26 13:01:00 UTC
S/W: OS-L3M Ver. 12.0
```
本装置 C でソフトウェアのバージョンを確認します。手順 2 で確認したメンバスイッチ A のソフトウェアのバージョンと同じであることを確認してください。

(2) メンバスイッチ B の停止

メンバスイッチ B にログインして，メンバスイッチ B を停止します。

[手順]

1. **02B> reload stop**

メンバスイッチ B を停止します。

なお，マスタスイッチであるメンバスイッチ A からもメンバスイッチ B を停止できます。その場合は，メンバスイッチ A にログインして次のコマンドを実行してください。

```
> reload switch 2 stop
```

2. 電源を OFF にして，スタック構成から外します。

(3)　本装置 C をスイッチ番号 2 として 1 台スタックへ移行

本装置 C のスイッチ番号を 2 にして，スタック機能を有効にする設定をします。

[設定のポイント]

本装置 C のスイッチ番号を 2 に設定します。その後，stack enable コマンドでスタックで動作させる設定をしてから本装置を再起動する必要があります。そのため，運用を開始する前に設定してください。また，stack enable コマンドを設定すると，本装置を再起動するまですべてのコンフィグレーションが変更できません。

なお，stack enable コマンドを設定すると，同時に次のコンフィグレーションが自動で設定されます。

- no service ipv6 dhcp

[コマンドによる設定]

1. **# set switch 2**

   # configure

   スイッチ番号を 2 に設定します。

2. **(config)# stack enable**

   After this command execute, please save configuration editing now in startup-config, and please reboot a device.

   Do you wish to continue ? (y/n):

   スタックで動作させる設定をします。コンフィグレーションの変更確認メッセージに対して y を入力します。

3. **(config)# save**

   (config)# exit

   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

4. **# reload**

   本装置を再起動します。再起動後，本装置は 1 台構成のスタックのメンバスイッチとして動作します。

(4)　メンバスイッチ A と接続するためのメンバスイッチ C のコンフィグレーションの設定

メンバスイッチ C に，メンバスイッチ A と接続してスタックを構成するための最小限のコンフィグレーションを設定します。

[設定のポイント]

メンバスイッチ A と接続したときにメンバスイッチ A が障害などで再起動してもメンバスイッチ C がマスタスイッチとして動作しないように，メンバスイッチ C のマスタ選出優先度を 1 に設定します。

なお，ここで設定したコンフィグレーションは，マスタスイッチとなるメンバスイッチ A で設定したコンフィグレーションに置き換えられます。

[コマンドによる設定]

1. **(config)# interface hundredgigabitethernet 2/0/49**

   (config-if)# switchport mode stack

   (config-if)# exit

(config)# interface hundredgigabitethernet 2/0/50

(config-if)# switchport mode stack

(config-if)# exit

メンバスイッチC（スイッチ番号2）のイーサネットインタフェースにスタックポートを設定します。

2. **(config)# switch 2 priority 1**

   メンバスイッチC（スイッチ番号2）のマスタ選出優先度を1に設定します。

3. **(config)# save**

   (config)# exit

   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

(5) メンバスイッチAとメンバスイッチCの2台スタックへ移行

それぞれ1台構成のスタックのメンバスイッチとして動作しているメンバスイッチAとメンバスイッチCのスタックポートを接続して，2台構成のスタックに移行します。

メンバスイッチCのマスタ選出優先度が1のため，メンバスイッチAはマスタスイッチとして動作を継続して，メンバスイッチCは自動で再起動します。

再起動後，メンバスイッチAのコンフィグレーションに同期するためにメンバスイッチCは自動で再起動します。その後，メンバスイッチAがマスタスイッチ，メンバスイッチCがバックアップスイッチとなるスタック構成で動作します。

[手順]

1. メンバスイッチAとメンバスイッチCのスタックポートを接続します。
2. **# show switch detail**

   運用コマンドshow switch detailを実行して，メンバスイッチAがマスタスイッチ，メンバスイッチCがバックアップスイッチとなるスタックで動作していることを確認します。

8.1.7 スタンドアロンへの転用

スイッチ番号1およびスイッチ番号2のメンバスイッチで構成されているスタックから，それぞれのメンバスイッチをスタンドアロンへ戻します。スイッチ番号1のスイッチとスイッチ番号2のスイッチでは設定手順が異なります。設定の前にネットワークから切り離して，1台構成のスタックにしておきます。

なお，2台構成のスタックでは次に示すコンフィグレーションが設定されていたものとします。

```
stack enable
switch 1 provision 3660-48xt4qw
switch 2 provision 3660-48xt4qw
switch 1 priority 20
switch 2 priority 10
!
   :
   :
interface gigabitethernet 1/0/1
  switchport mode access
!
   :
   :
interface gigabitethernet 1/0/24
  switchport mode access
!
interface tengigabitethernet 1/0/25
  switchport mode access
```

```
!
   :
   :
interface hundredgigabitethernet 1/0/52
  switchport mode stack
!
interface gigabitethernet 2/0/1
  switchport mode access
!
   :
   :
interface gigabitethernet 2/0/24
  switchport mode access
!
interface tengigabitethernet 2/0/25
  switchport mode access
!
   :
   :
interface hundredgigabitethernet 2/0/52
  switchport mode stack
!
```

(1)　スイッチ番号 1 のメンバスイッチのスタンドアロンへの転用

スイッチ番号 2 のメンバスイッチについてのコンフィグレーションと，スタック機能に関するコンフィグレーションを削除します。

なお，スタック専用ポートを実装するモデルでは，スタックポートのコンフィグレーションを削除できません。スタック機能を無効に設定して装置を再起動すると，ランニングコンフィグレーションからスタックポートが削除された状態で装置が起動します。

[設定のポイント]

スタック機能に関するコンフィグレーションを削除したあと，装置を再起動する必要があります。

[コマンドによる設定]

1. **(config)# interface hundredgigabitethernet 1/0/52**
   (config-if)# no switchport mode stack
   (config-if)# exit
   本メンバスイッチのスタックポートを削除します。
2. **(config)# no switch 2 provision**
   本メンバスイッチ以外のモデルを削除します。本メンバスイッチはスイッチ番号 1 なので，スイッチ番号 2 のモデルを削除します。
3. **(config)# no switch 1 priority**
   (config)# no switch 2 priority
   スイッチ番号 1 およびスイッチ番号 2 のマスタ選出優先度を削除します。
4. **(config)# no stack enable**
   スタック機能を無効にします。
5. **(config)# save**
   (config)# exit
   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。
6. **# reload**
   本装置を再起動します。

(2) スイッチ番号 2 のメンバスイッチのスタンドアロンへの転用

まず，スイッチ番号を 1 に変更します。次に，スイッチ番号 2 のメンバスイッチについてのコンフィグレーションと，スタック機能に関するコンフィグレーションを削除します。

[設定のポイント]

スイッチ番号を 1 に変更したら，まずメンバスイッチを再起動してください。

次に，スイッチ番号 2 のメンバスイッチについてのコンフィグレーションと，スタック機能に関するコンフィグレーションを削除したあと，もう一度装置を再起動する必要があります。

[コマンドによる設定]

1. **(config)# no switch 1 provision**

   (config)# save

   (config)# exit

   スイッチ番号 1 のモデルを削除します。コンフィグレーションを保存して，装置管理者モードに戻ります。

2. **# set switch 1**

   スイッチ番号に 1 を設定します。

3. **# reload**

   本メンバスイッチを再起動します。再起動後，本メンバスイッチはスイッチ番号 1 のマスタスイッチとして動作します。

4. **(config)# no switch 2 provision**

   本メンバスイッチ以外のモデルを削除します。本メンバスイッチはスイッチ番号 1 なので，スイッチ番号 2 のモデルを削除します。

5. **(config)# no switch 1 priority**

   (config)# no switch 2 priority

   スイッチ番号 1 およびスイッチ番号 2 のマスタ選出優先度を削除します。

6. **(config)# no stack enable**

   スタック機能を無効にします。

7. **(config)# save**

   (config)# exit

   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

8. **# reload**

   本装置を再起動します。

8.1.8 スタックリンクの追加

スタックリンク 1 本で構成されているスタックに対して，新たにスタックリンクを追加します。スタックリンクの追加前は次に示すコンフィグレーションが設定されていたものとします。

```
stack enable
switch 1 provision 3660-48xt4qw
switch 2 provision 3660-48xt4qw
   :
   :
interface hundredgigabitethernet 1/0/51
  switchport mode stack
```

```
!
interface hundredgigabitethernet 1/0/52
  switchport mode access
   :
   :
interface hundredgigabitethernet 2/0/51
  switchport mode stack
!
interface hundredgigabitethernet 2/0/52
  switchport mode access
!
```

(1)　追加するスタックポートにケーブルが接続されていないか確認

スタックポートとして追加するポートにケーブルが接続されていないか確認します。ケーブルが接続されている場合は，コンフィグレーションの設定前にケーブルを外してください。

(2)　スタックポートのコンフィグレーションの設定

追加するスタックポートのコンフィグレーションを設定します。スタック専用ポートを実装するモデルでは，スタック機能が動作している場合，スタック専用ポートに対してスタックポートが設定された状態になります。そのため，この操作は不要です。

[コマンドによる設定]

1. **(config)# interface hundredgigabitethernet 1/0/52**

   (config-if)# switchport mode stack

   (config-if)# exit

   (config)# interface hundredgigabitethernet 2/0/52

   (config-if)# switchport mode stack

   (config-if)# exit

   スイッチ番号 1 およびスイッチ番号 2 のイーサネットインタフェースにスタックポートを設定します。

2. **(config)# save**

   (config)# exit

   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

(3)　追加するスタックポート間の接続

スイッチ番号 1 およびスイッチ番号 2 の追加するスタックポートをケーブルで接続します。

8.1.9　スタックリンクの削除

スタックリンク 2 本で構成されているスタックから，スタックリンクを 1 本削除します。スタックリンクの削除前は次に示すコンフィグレーションが設定されていたものとします。

```
stack enable
switch 1 provision 3660-48xt4qw
switch 2 provision 3660-48xt4qw
   :
   :
interface hundredgigabitethernet 1/0/51
  switchport mode stack
!
interface hundredgigabitethernet 1/0/52
  switchport mode stack
   :
   :
```

```
interface hundredgigabitethernet 2/0/51
  switchport mode stack
!
interface hundredgigabitethernet 2/0/52
  switchport mode stack
!
```

(1) 削除するスタックポート間の切断

削除するスタックポートのケーブルを外します。ケーブルが外せない場合は,次に示すコンフィグレーションでスタックポートをシャットダウン状態にしてください。

[コマンドによる設定]

1. **(config)# interface hundredgigabitethernet 1/0/52**
   (config-if)# shutdown
   (config-if)# exit
   (config)# interface hundredgigabitethernet 2/0/52
   (config-if)# shutdown
   (config-if)# exit
   スイッチ番号 1 およびスイッチ番号 2 のスタックポートをシャットダウン状態にします。

(2) スタックポートのコンフィグレーションの削除

削除するスタックポートからコンフィグレーションを削除します。スタック専用ポートを実装するモデルでは，スタック機能が動作している場合，スタックポートを削除できません。

[コマンドによる設定]

1. **(config)# interface hundredgigabitethernet 1/0/52**
   (config-if)# no switchport mode stack
   (config-if)# exit
   (config)# interface hundredgigabitethernet 2/0/52
   (config-if)# no switchport mode stack
   (config-if)# exit
   スイッチ番号 1 およびスイッチ番号 2 のスタックポートを削除します。
2. **(config)# save**
   (config)# exit
   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

8.2　オペレーション

8.2.1　運用コマンド一覧

スタックの運用コマンド一覧を次の表に示します。

表 8-8　運用コマンド一覧

コマンド名	説明
show switch	スタックを構成するメンバスイッチの情報を表示します。
remote command	マスタスイッチから指定したメンバスイッチに対して，運用コマンドを実行します。
dump stack	スタック管理プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。
session	スタックを構成するほかのメンバスイッチに接続します。

8.2.2　スタックを構成するメンバスイッチの情報の確認

運用コマンド show switch で，スタックを構成するメンバスイッチの情報を確認できます。スイッチ番号は「No」に表示されます。スイッチ状態とスイッチ状態遷移後の変更処理は「Switch status」に表示されます。

図 8-6　show switch コマンドの実行結果

```
> show switch
Date 20XX/10/26 11:38:56 UTC
Stack status : Enable          Switch No : 1
System MAC Address : 0012.e220.5101
No  Switch status           Model         Machine ID      Priority  Ver
 1  Master                   3660-48xt4qw  0012.e220.5101  31        1
 2  Backup  (Initializing)  3660-48xt4qw  0012.e220.5102  11        1
>
```

運用コマンド show switch で detail パラメータを指定すると，メンバスイッチの詳細情報を確認できます。スタックポートの情報が「Port」と「Neighbor(Port)」に表示されます。

図 8-7　show switch detail コマンドの実行結果

```
> show switch detail
Date 20XX/10/26 11:38:56 UTC
Stack status : Enable          Switch No : 1
System MAC Address : 0012.e220.5101
No  Switch status           Model         Machine ID      Priority  Ver
 1  Master                   3660-48xt4qw  0012.e220.5101  31        1
 2  Backup  (Initializing)  3660-48xt4qw  0012.e220.5102  11        1
Port     Status           Neighbor(Port    Model         Machine ID)
1/0/49   Up(Forwarding)            2/0/49  3660-48xt4qw  0012.e220.5102
1/0/50   Up(Forwarding)            2/0/50  3660-48xt4qw  0012.e220.5102
2/0/49   Up(Forwarding)            1/0/49  3660-48xt4qw  0012.e220.5101
2/0/50   Up(Forwarding)            1/0/50  3660-48xt4qw  0012.e220.5101
>
```

なお，スイッチ状態とスイッチ番号は，装置の正面パネルでも確認できます。詳細は，「8.2.3　正面パネルでのスイッチ状態とスイッチ番号の表示」を参照してください。

8.2.3　正面パネルでのスイッチ状態とスイッチ番号の表示

装置前面の LED でスイッチ状態とスイッチ番号が確認できます。スイッチ状態は ST2 の点灯有無で確認できます。スイッチ番号（1～2）は，スイッチ番号に対応する LED（ID1～ID2）の点灯で確認できます。

表 8-9　スイッチ状態に対応する LED の状態

LED 名	スイッチ状態	LED 状態
ST2	初期状態	消灯
	マスタ	緑点灯
	バックアップ	消灯

8.2.4　マスタスイッチからメンバスイッチへの運用コマンドの実行

スイッチ番号 1 がマスタスイッチ，スイッチ番号 2 がバックアップスイッチの場合に，運用コマンド show logging でメンバスイッチのログを表示する例を次に示します。なお，先頭にはスイッチ番号とスイッチ状態が表示されます。

図 8-8　スイッチ番号 2 のメンバスイッチのログを表示

```
> show logging switch 2
Switch 2 (Backup)
-----------------
Wed Jun 22 15:30:00 UTC 20XX
System information
...
>
```

運用コマンド remote command を使用しても，マスタスイッチから指定したメンバスイッチに対して運用コマンドを実行できます。スイッチ番号 1 がマスタスイッチ，スイッチ番号 2 がバックアップスイッチの場合に，remote command コマンドと運用コマンド show clock でメンバスイッチの時刻を表示する例を次に示します。なお，先頭にはスイッチ番号とスイッチ状態が表示されます。

図 8-9　スイッチ番号 2 のメンバスイッチの時刻を表示

```
# remote command 2 show clock
Switch 2 (Backup)
-----------------
Wed Jun 22 15:30:00 UTC 20XX
#
```

図 8-10　すべてのメンバスイッチの時刻を表示

```
# remote command all show clock
Switch 1 (Master)
-----------------
Wed Jun 22 15:30:00 UTC 20XX


Switch 2 (Backup)
-----------------
Wed Jun 22 15:30:00 UTC 20XX
#
```

8.2.5　マスタスイッチとメンバスイッチ間の接続

運用コマンド session を使用して，異なるメンバスイッチに接続できます。スイッチ番号 1 がマスタスイッチ，スイッチ番号 2 がバックアップスイッチの場合に，バックアップスイッチにログインしたあと，マスタスイッチに接続してコンフィグレーションを編集する例を次に示します。

図 8-11　スイッチ番号 1 のマスタスイッチに接続してコンフィグレーションを編集

```
02B> session switch 1            …1
> enable                         …2
# configure                      …3
(config)#                        …4
```

1. バックアップスイッチから，スイッチ番号 1 を指定した session コマンドを実行して，マスタスイッチ（スイッチ番号 1）に接続します。
2. 接続したマスタスイッチで運用コマンド enable を実行して，装置管理者モードに遷移します。
3. コンフィグレーションコマンド configure を実行して，コンフィグレーションコマンドモードに遷移します。
4. 編集を開始します。

8.2.6　スタックの再起動

オプションライセンスを追加または削除した場合や，装置または VLAN プログラムの再起動が必要なコンフィグレーションを編集した場合は, 変更した内容を正しく反映するためにスタックを再起動する必要があります。

スタックを再起動するには, スタックを構成するすべてのメンバスイッチを再起動します。スタックを再起動する手順を次に示します。なお，最初のメンバスイッチを再起動してから 30 秒以内に，すべてのメンバスイッチを再起動してください。

1. マスタスイッチにログインします。
2. enable コマンドを実行して，装置管理者モードに移行します。
3. show switch コマンドを実行して，現在動作しているメンバスイッチを確認します。

   以降，次に示す実行結果が表示されたものとして説明します。ここでは，スイッチ番号 1 のマスタスイッチと，スイッチ番号 2 のメンバスイッチが動作していることが確認できます。

```
> show switch
Date 20XX/10/26 11:38:56 UTC
Stack status : Enable          Switch No : 1
System MAC Address : 0012.e220.5101
No  Switch status           Model         Machine ID      Priority  Ver
 1  Master                  3660-48xt4qw  0012.e220.5101  31        1
 2  Backup                  3660-48xt4qw  0012.e220.5102  11        1
>
```

4. マスタスイッチ以外のメンバスイッチを再起動します。

   再起動はマスタスイッチ以外のメンバスイッチから始めます。

   この例ではマスタスイッチ以外にスイッチ番号 2 のメンバスイッチがあるので，次のコマンドを実行します。

```
> reload switch 2 no-dump-image -f
```

5. 次のコマンドを実行して，マスタスイッチを再起動します。

   最初のメンバスイッチを再起動してからマスタスイッチを再起動するまで，30 秒以内に次のコマンドを実行します。

```
> reload no-dump-image -f
```

8.2.7　オプションライセンスの設定

スタックでオプションライセンスを追加または削除する手順を次に示します。

スタックを構成するメンバスイッチ間でオプションライセンスが一致していないと，スタックを構成できません。このため，オプションライセンスを追加または削除したあと再起動して適用するときは，バックアップスイッチを再起動してから 30 秒以内にマスタスイッチを再起動してください。

1. マスタスイッチにログインします。
2. enable コマンドを実行して，装置管理者モードに移行します。
3. set license コマンドまたは erase license コマンドの switch パラメータにバックアップスイッチのスイッチ番号を指定して，バックアップスイッチのオプションライセンスを追加または削除します。
4. マスタスイッチのオプションライセンスを追加または削除します。
5. オプションライセンスを反映させるため，スタックを構成するすべてのメンバスイッチを再起動します。

   再起動の手順については「8.2.6　スタックの再起動」を参照してください。

9 リモート運用端末から本装置へのログイン

この章では, リモート運用端末から本装置へのリモートアクセスについて説明します。

9.1　解説

9.1.1　マネージメントポート接続

マネージメントポートはリモート運用端末を接続するためのインタフェースを提供します。

(1)　マネージメントポートの機能仕様

マネージメントポートは 10BASE-T/100BASE-TX のツイストペアケーブル（UTP）を使用します。マネージメントポートの機能仕様を次の表に示します。

表 9-1　マネージメントポートの機能仕様

機能概要	仕様
インタフェース種別	10BASE-T，100BASE-TX
オートネゴシエーション	サポート
自動 MDI/MDIX 機能	サポート
フローコントロール	未サポート
ジャンボフレーム	未サポート
MAC および LLC 副階層制御フレーム	Ethernet V2 形式だけをサポート （802.3 形式，そのほかは未サポート）
対象プロトコル	IPv4，IPv6
フィルタリング	未サポート
QoS	未サポート
マルチキャスト	未サポート

マネージメントポートでは，IPv4 中継および IPv6 中継をするかどうかを，コンフィグレーションで選択できます。マネージメントポートに設定できない IPv4 機能および IPv6 機能の仕様を次の表に示します。

表 9-2　マネージメントポートでの IPv4／IPv6 機能仕様

機能概要	仕様
MTU	1500（固定）
サブネットブロードキャスト中継	未サポート
ICMP／ICMPv6 リダイレクト	送信
IPv4 ソースルーティング	中継機能が設定されている場合は中継
ProxyARP	未サポート
ローカル ProxyARP	未サポート
ARP 関連パラメータ	再送回数 1 回（固定） 再送間隔 2 秒（固定） 満了時間 14400 秒（固定）

機能概要	仕様
スタティック ARP／NDP	未サポート
VRRP（IPv4／IPv6）／GSRP	未サポート

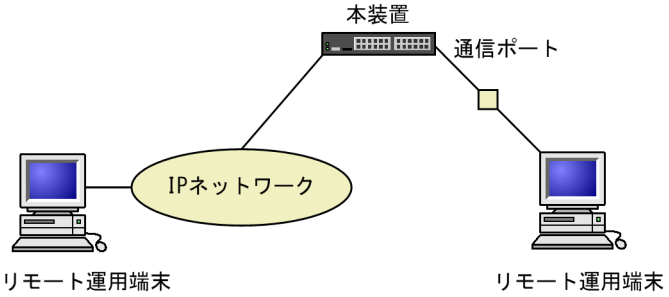
(2)　マネージメントポート使用時の注意事項

マネージメントポートは，リモート運用を主目的としたインタフェースです。マネージメントポートを経由した通信の性能については，制限が掛かります。

9.1.2　通信用ポート接続

通信用ポートを介して，リモート運用端末から本装置へログインするには，本装置で VLAN や IP アドレスなどの設定が必要です。ただし，初期導入時には，VLAN や IP アドレスなどの設定が行われていません。そのため，コンソールからログインして，コンフィグレーションを設定する必要があります。

図 9-1　リモート運用端末からの本装置へのログイン



9.2　コンフィグレーション

9.2.1　コンフィグレーションコマンド一覧

マネージメントポートのコンフィグレーションコマンド一覧を次の表に示します。

表 9-3　コンフィグレーションコマンド一覧

コマンド名	説明
description	補足説明を設定します。
duplex	マネージメントポートの duplex を設定します。
interface mgmt	マネージメントポートのコンフィグレーションを指定します。
ip routing	マネージメントポートでの IPv4 のレイヤ 3 中継可否を指定します。
ipv6 routing	マネージメントポートでの IPv6 のレイヤ 3 中継可否を指定します。
shutdown	マネージメントポートをシャットダウン状態にします。
speed	マネージメントポートの回線速度を設定します。
ip address※1	マネージメントポートの IPv4 アドレスを指定します。
ipv6 address※2	マネージメントポートの IPv6 アドレスを指定します。
ipv6 enable※2	マネージメントポートの IPv6 機能を有効にします。このコマンドによって，リンクローカルアドレスが自動生成されます。

注※1

「コンフィグレーションコマンドレファレンス Vol.2」「2　IPv4・ARP・ICMP」を参照してください。

注※2

「コンフィグレーションコマンドレファレンス Vol.2」「17　IPv6・NDP・ICMPv6」を参照してください。

運用端末の接続とリモート操作に関するコンフィグレーションコマンド一覧を次の表に示します。

表 9-4　コンフィグレーションコマンド一覧

コマンド名	説明
ftp-server	リモート運用端末から ftp プロトコルを使用したアクセスを許可します。
line console	コンソール（RS232C）のパラメータを設定します。
line vty	装置へのリモートアクセスを許可します。
speed	コンソール（RS232C）の通信速度を設定します。
transport input	リモート運用端末から各種プロトコルを使用したアクセスを規制します。

SSH の設定については，「11　SSH(Secure Shell)」を参照してください。

VLAN の設定，および IPv4/IPv6 インタフェースの設定に関するコンフィグレーションコマンドについては，「24　VLAN」，「コンフィグレーションガイド Vol.3」「2　IP・ARP・ICMP の設定と運用」，または「コンフィグレーションガイド Vol.3」「19　IPv6・NDP・ICMPv6 の設定と運用」を参照してください。

9.2.2　マネージメントポートの設定

(1)　マネージメントポートのシャットダウン

[設定のポイント]

マネージメントポートでは，複数のコマンドでコンフィグレーションを設定することがあります。そのとき，コンフィグレーションの設定が完了していない状態でマネージメントポートがリンクアップ状態になると期待した通信ができません。したがって，最初にマネージメントポートをシャットダウンしてから，コンフィグレーションを設定し，完了したあとにマネージメントポートのシャットダウンを解除することを推奨します。

[コマンドによる設定]

1. **(config)# interface mgmt 0**
   マネージメントポートのコンフィグレーションモードに移行します。
2. **(config-if)# shutdown**
   マネージメントポートをシャットダウンします。
3. **(config-if)# *******
   マネージメントポートに対するコンフィグレーションを設定します。
4. **(config-if)# no shutdown**
   マネージメントポートのシャットダウンを解除します。

[関連事項]

運用コマンド inactivate でマネージメントポートの運用を停止することもできます。ただし，inactivate コマンドで inactive 状態とした場合は，装置を再起動するとマネージメントポートが active 状態になります。マネージメントポートをシャットダウンした場合は，装置を再起動してもマネージメントポートは disable 状態のままです。マネージメントポートを active 状態にするにはコンフィグレーションで no shutdown を設定して，シャットダウンを解除する必要があります。

(2)　IPv4 アドレスの設定

[設定のポイント]

マネージメントポートに IPv4 アドレスを設定します。IPv4 アドレスを設定するには，インタフェースのコンフィグレーションモードに移行する必要があります。

[コマンドによる設定]

1. **(config)# interface mgmt 0**
   マネージメントポートのコンフィグレーションモードに移行します。
2. **(config-if)# ip address 192.168.1.1 255.255.255.0**
   マネージメントポートに IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

(3)　IPv6 アドレスの設定

[設定のポイント]

マネージメントポートに IPv6 アドレスを設定します。ipv6 enable コマンドを設定して，IPv6 機能を有効にする必要があります。ipv6 enable コマンドの設定がない場合，IPv6 設定は無効になります。

[コマンドによる設定]

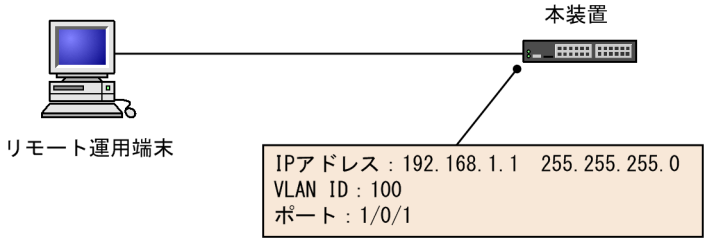
1. **(config)# interface mgmt 0**
   マネージメントポートのコンフィグレーションモードに移行します。
2. **(config-if)# ipv6 enable**
   マネージメントポートに IPv6 アドレス使用可を設定します。
3. **(config-if)# ipv6 address 2001:db8::1/64**
   マネージメントポートに IPv6 アドレス 2001:db8::1，プレフィックス長 64 を設定します。

9.2.3　本装置への IP アドレスの設定

[設定のポイント]

リモート運用端末から本装置へアクセスするためには，あらかじめ，接続するインタフェースに対して IP アドレスを設定しておく必要があります。

図 9-2　リモート運用端末との接続例



[コマンドによる設定]

1. **(config)# vlan 100**
   (config-vlan)# exit
   VLAN ID 100 のポート VLAN を作成し，VLAN 100 の VLAN コンフィグレーションモードに移行します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 100
   (config-if)# exit
   ポート 1/0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。ポート 1/0/1 を VLAN 100 のアクセスポートに設定します。
3. **(config)# interface vlan 100**
   (config-if)# ip address 192.168.1.1 255.255.255.0
   (config-if)# exit
   (config)#
   VLAN ID 100 のインタフェースコンフィグレーションモードに移行します。VLAN ID 100 に IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

9.2.4　telnet によるログインを許可する

[設定のポイント]

あらかじめ，IP アドレスを設定しておく必要があります。

リモート運用端末から本装置に telnet プロトコルによるリモートログインを許可するコンフィグレーションコマンド line vty を設定します。

このコンフィグレーションが設定されていない場合，コンソールからだけ本装置にログインできます。

[コマンドによる設定]

1. **(config)# line vty 0 2**

   (config-line)#

   リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。また，装置に同時にリモートログインできるユーザ数を最大 3 に設定します。

9.2.5　ftp によるログインを許可する

[設定のポイント]

あらかじめ，IP アドレスを設定しておく必要があります。

リモート運用端末から本装置に ftp プロトコルによるリモートアクセスを許可するコンフィグレーションコマンド ftp-server を設定します。

このコンフィグレーションを実施していない場合，ftp プロトコルを用いた本装置へのアクセスはできません。

[コマンドによる設定]

1. **(config)# ftp-server**

   リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可します。

9.2.6　VRF での telnet によるログインを許可する【SL-L3A】

(1)　グローバルネットワークを含む全 VRF から telnet によるログインを許可する場合

[設定のポイント]

全 VRF からのアクセスを許可するには，コンフィグレーションコマンド transport input の vrf all パラメータを設定します。この vrf all パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

[コマンドによる設定]

1. **(config)# line vty 0 2**

   (config-line)#

   リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。また，装置に同時にリモートログインできるユーザ数を最大 3 に設定します。

2. **(config-line)# transport input vrf all telnet**

   (config-line)#

   グローバルネットワークを含む全 VRF で，リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。

(2) 指定 VRF から telnet によるログインを許可する場合

[設定のポイント]

指定 VRF からのアクセスを許可するには，コンフィグレーションコマンド transport input の vrf パラメータで VRF ID を設定します。この vrf パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

[コマンドによる設定]

1. **(config)# line vty 0 2**
   (config-line)#
   リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。また，装置に同時にリモートログインできるユーザ数を最大 3 に設定します。
2. **(config-line)# transport input vrf 2 telnet**
   (config-line)#
   VRF 2 で，リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。なお，グローバルネットワークは含みません。

9.2.7 VRF での ftp によるログインを許可する【SL-L3A】

(1) グローバルネットワークを含む全 VRF から ftp によるログインを許可する場合

[設定のポイント]

全 VRF からのアクセスを許可するには，コンフィグレーションコマンド ftp-server の vrf all パラメータを設定します。この vrf all パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

[コマンドによる設定]

1. **(config)# ftp-server vrf all**
   グローバルネットワークを含む全 VRF で，リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可します。

(2) 指定 VRF から ftp によるログインを許可する場合

[設定のポイント]

指定 VRF からのアクセスを許可するには，コンフィグレーションコマンド ftp-server の vrf パラメータで VRF ID を設定します。この vrf パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

[コマンドによる設定]

1. **(config)# ftp-server vrf 2**
   VRF 2 で，リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可します。なお，グローバルネットワークは含みません。

9.3　オペレーション

9.3.1　運用コマンド一覧

運用端末の接続とリモート操作に関する運用コマンド一覧を次の表に示します。

表 9-5　運用コマンド一覧

コマンド名	説明
set exec-timeout	自動ログアウトが実行されるまでの時間を設定します。
set terminal help	ヘルプメッセージで表示するコマンドの一覧を設定します。
set terminal pager	ページングの実施／未実施を設定します。
show history	過去に実行した運用コマンドの履歴を表示します（コンフィグレーションコマンドの履歴は表示しません）。
telnet	指定された IP アドレスのリモート運用端末と仮想端末と接続します。
ftp	本装置と TCP/IP で接続されているリモート端末との間でファイル転送をします。
tftp	本装置と接続されているリモート端末との間で UDP でファイル転送をします。

SSH の設定については，「11　SSH(Secure Shell)」を参照してください。

VLAN の設定，および IPv4/IPv6 インタフェースの設定に関するコンフィグレーションコマンドについては，「24　VLAN」，「コンフィグレーションガイド Vol.3」「2　IP・ARP・ICMP の設定と運用」，または「コンフィグレーションガイド Vol.3」「19　IPv6・NDP・ICMPv6 の設定と運用」を参照してください。

9.3.2　リモート運用端末と本装置との通信の確認

本装置とリモート運用端末との通信は，運用コマンド ping や ping ipv6 などを用いて確認できます。詳細は，「コンフィグレーションガイド Vol.3」「2　IP・ARP・ICMP の設定と運用」，または「コンフィグレーションガイド Vol.3」「19　IPv6・NDP・ICMPv6 の設定と運用」を参照してください。

10 ログインセキュリティと RADIUS/TACACS+

この章では，本装置のログイン制御，ログインセキュリティ，アカウンティング，および RADIUS/TACACS+について説明します。

10.1　ログインセキュリティの設定

10.1.1　コンフィグレーション・運用コマンド一覧

ログインセキュリティに関するコンフィグレーションコマンド一覧を次の表に示します。

表 10-1　コンフィグレーションコマンド一覧

コマンド名	説明
aaa authentication enable	装置管理者モードへの変更（enable コマンド）時に使用する認証方式を指定します。
aaa authentication enable attribute-user-per-method	装置管理者モードへの変更（enable コマンド）時の認証に使用するユーザ名属性を変更します。
aaa authentication enable end-by-reject	装置管理者モードへの変更（enable コマンド）時の認証で，否認された場合に認証を終了します。
aaa authentication login	リモートログイン時に使用する認証方式を指定します。
aaa authentication login console	コンソール（RS232C）からのログイン時に aaa authentication login コマンドで指定した認証方式を使用します。
aaa authentication login end-by-reject	ログイン時の認証で，否認された場合に認証を終了します。
aaa authorization commands	RADIUS サーバまたは TACACS+サーバによるコマンド承認をする場合に指定します。
aaa authorization commands console	コンソール(RS232C)からのログインの場合に aaa authorization commands コマンドで指定したコマンド承認を行います。
banner	ユーザのログイン前およびログイン後に表示するメッセージを設定します。
commands exec	ローカル（コンフィグレーション）によるコマンド承認で使用するコマンドリストに，コマンド文字列を追加します。
ip access-group	本装置へリモートログインを許可または拒否するリモート運用端末の IPv4 アドレスを指定したアクセスリストを設定します。
ipv6 access-class	本装置へリモートログインを許可または拒否するリモート運用端末の IPv6 アドレスを指定したアクセスリストを設定します。
parser view	ローカル（コンフィグレーション）によるコマンド承認で使用するコマンドリストを生成します。
username	指定ユーザに，ローカル（コンフィグレーション）によるコマンド承認で使用するコマンドリストまたはコマンドクラスを設定します。

ログインセキュリティに関する運用コマンド一覧を次の表に示します。

表 10-2　運用コマンド一覧

コマンド名	説明
adduser	新規ログインユーザ用のアカウントを追加します。
rmuser	adduser コマンドで登録されているログインユーザのアカウントを削除します。

コマンド名	説明
password	ログインユーザのパスワードを変更します。
clear password	ログインユーザのパスワードを削除します。
show sessions	本装置にログインしているユーザを表示します。
show whoami	本装置にログインしているユーザの中で，このコマンドを実行したログインユーザだけを表示します。
killuser	ログイン中のユーザを強制的にログアウトさせます。

10.1.2　ログイン制御の概要

本装置にはローカルログイン（シリアル接続）と IPv4 および IPv6 ネットワーク経由のリモートログイン機能（telnet）があります。

本装置ではログイン時およびログイン中に次に示す制御を行っています。

1. ログイン時に不正アクセスを防止するため，ユーザ ID によるコマンドの使用範囲の制限やパスワードによるチェックを設けています。
2. 複数の運用端末から同時にログインできます。
3. 本装置にログインできるリモートユーザ数は最大 16 ユーザです。なお，コンフィグレーションコマンド line vty でログインできるユーザ数を制限できます。
4. 本装置にアクセスできる IPv4 および IPv6 アドレスをコンフィグレーションコマンド ip access-list standard，ipv6 access-list，access-list，ip access-group，ipv6 access-class で制限できます。
5. 本装置にアクセスできるプロトコル（telnet，ftp）をコンフィグレーションコマンド transport input や ftp-server で制限できます。
6. VRF で本装置にアクセスできる IPv4 および IPv6 アドレスをコンフィグレーションコマンド ip access-list standard，ipv6 access-list，access-list，ip access-group，ipv6 access-class で制限できます。【SL-L3A】
7. VRF で本装置にアクセスできるプロトコル（telnet，ftp）をコンフィグレーションコマンド transport input や ftp-server で制限できます。【SL-L3A】
8. コマンド実行結果はログインした端末だけに表示します。運用メッセージはログインしているすべての運用端末に表示されます。
9. 入力したコマンドとその応答メッセージおよび運用メッセージを運用ログとして収集します。運用ログは運用コマンド show logging で参照できます。
10. キー入力が最大 60 分間ない場合は自動的にログアウトします。
11. 運用コマンド killuser を使用してユーザを強制ログアウトできます。

10.1.3　ログインユーザの作成と削除

adduser コマンドを用いて本装置にログインできるユーザを作成してください。ログインユーザの作成例を次の図に示します。

図 10–1　ユーザ newuser を作成

```
> enable
# adduser newuser
User(empty password) add done. Please setting password.
```

```
Changing local password for newuser.
New password:********                                    … 1
Retype new password:********                             … 2
# quit
>
```

1. パスワードを入力します（実際には入力文字は表示されません）。
2. 確認のため再度パスワードを入力します（実際には入力文字は表示されません）。

また，使用しなくなったユーザは rmuser コマンドを用いて削除できます。

特に，初期導入時に設定されているログインユーザ”operator”を運用中のログインユーザとして使用しない場合，セキュリティの低下を防ぐため，新しいログインユーザを作成したあとに rmuser コマンドで削除することをお勧めします。また，コンフィグレーションコマンド aaa authentication login で，RADIUS/TACACS+を使用したログイン認証ができます。コンフィグレーションの設定例については，「10.3.2　RADIUS サーバによる認証の設定」および「10.3.3　TACACS+サーバによる認証の設定」を参照してください。

なお，作成したログインユーザ名は忘れないようにしてください。ログインユーザ名を忘れると，デフォルトリスタートで起動してもログインできないので注意してください。

10.1.4　装置管理者モード変更のパスワードの設定

コンフィグレーションコマンドを実行するためには enable コマンドで装置管理者モードに変更する必要があります。初期導入時に enable コマンドを実行した場合，パスワードは設定されていませんので認証なしで装置管理者モードに変更します。ただし，通常運用中にすべてのユーザがパスワード認証なしで装置管理者モードに変更できるのはセキュリティ上危険ですので，初期導入時にパスワードを設定しておいてください。パスワード設定の実行例を次の図に示します。

図 10-2　初期導入直後の装置管理者モード変更のパスワード設定

```
> enable
# password enable-mode
Changing local password for admin.
New password:
Retype new password:
#
```

また，コンフィグレーションコマンド aaa authentication enable で，RADIUS/TACACS+を使用した認証ができます。コンフィグレーションの設定例については，「10.3.2　RADIUS サーバによる認証の設定」および「10.3.3　TACACS+サーバによる認証の設定」を参照してください。

10.1.5　リモート運用端末からのログインの許可

コンフィグレーションコマンド line vty を設定することで，リモート運用端末から本装置へログインできるようになります。このコンフィグレーションが設定されていない場合，コンソールからだけ本装置にログインできます。リモート運用端末からのログインを許可する設定例を次の図に示します。

図 10-3　リモート運用端末からのログインを許可する設定例

```
(config)# line vty 0 2
(config-line)#
```

また，リモート運用端末から ftp プロトコルを用いて，本装置にアクセスする場合には，コンフィグレーションコマンド ftp-server を設定する必要があります。本設定を実施しない場合，ftp プロトコルを用いた本装置へのアクセスはできません。

図 10–4　ftp プロトコルによるアクセス許可の設定例

```
(config)# ftp-server
(config)#
```

10.1.6　同時にログインできるユーザ数の設定

コンフィグレーションコマンド line vty を設定することで，リモート運用端末から本装置へログインできるようになります。line vty コマンドの<num>パラメータで，リモートログインできるユーザ数が制限されます。なお，この設定にかかわらず，コンソールからは常にログインできます。2 人まで同時にログインを許可する設定例を次の図に示します。

図 10–5　同時にログインできるユーザ数の設定例

```
(config)# line vty 0 1
(config-line)#
```

同時ログインに関する動作概要を次に示します。

- 複数ユーザが同時にログインすると，ログインしているユーザ数が制限数以下でもログインできない場合があります。
- 同時にログインできるユーザ数を変更しても，すでにログインしているユーザのセッションが切れることはありません。

10.1.7　リモート運用端末からのログインを許可する IP アドレスの設定

リモート運用端末から本装置へのログインを許可する IP アドレスを設定することで，ログインを制限できます。なお，設定後はリモート運用端末から本装置へのログインの可否を確認してください。

[設定のポイント]

特定のリモート運用端末からだけ，本装置へのアクセスを許可する場合は，コンフィグレーションコマンド ip access-list standard，ipv6 access-list，access-list，ip access-group，ipv6 access-class であらかじめアクセスを許可する端末の IP アドレスを登録しておく必要があります。アクセスを許可する IPv4 アドレスとサブネットマスク，または IPv6 アドレスとプレフィックスは，合わせて最大 128 個の登録ができます。このコンフィグレーションを実施していない場合，すべてのリモート運用端末から本装置へのアクセスが可能となります。なお，アクセスを許可していない（コンフィグレーションで登録していない）端末からのアクセスがあった場合，すでにログインしているそのほかの端末には，アクセスがあったことを示す”Unknown host address <IP アドレス>”のメッセージが表示されます。アクセスを許可する IP アドレスを変更しても，すでにログインしているユーザのセッションは切れません。

[コマンドによる設定]（IPv4 の場合）

1. **(config)# ip access-list standard REMOTE**
   (config-std-nacl)# permit 192.168.0.0 0.0.0.255
   (config-std-nacl)# exit
   ネットワーク（192.168.0.0/24）からだけログインを許可するアクセスリスト情報 REMOTE を設定します。
2. **(config)# line vty 0 2**
   (config-line)# ip access-group REMOTE in
   (config-line)#

line モードに遷移し，アクセスリスト情報 REMOTE を適用し，ネットワーク（192.168.0.0/24）にあるリモート運用端末からだけログインを許可します。

［コマンドによる設定］（IPv6 の場合）

1. **(config)# ipv6 access-list REMOTE6**
   (config-ipv6-nacl)# permit ipv6 3ffe:501:811:ff01::/64 any
   (config-ipv6-nacl)# exit
   ネットワーク（3ffe:501:811:ff01::/64）からだけログインを許可するアクセスリスト情報 REMOTE6 を設定します。
2. **(config)# line vty 0 2**
   (config-line)# ipv6 access-class REMOTE6 in
   (config-line)#
   line モードに遷移し，アクセスリスト情報 REMOTE6 を適用し，ネットワーク（3ffe:501:811:ff01::/64）にあるリモート運用端末からだけログインを許可します。

10.1.8 ログインバナーの設定

コンフィグレーションコマンド banner でログインバナーの設定を行うと，console から，またはリモート運用端末の telnet や ftp クライアントなどから本装置に接続したとき，ログインする前やログインしたあとにメッセージを表示できます。

［設定のポイント］

リモート運用端末の telnet や ftp クライアントからネットワークを介して本装置の telnet や ftp サーバへ接続するとき，ログインする前に次のメッセージを表示させます。

```
##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
```

［コマンドによる設定］

1. **(config)# banner login plain-text**
   --- Press CTRL+D or only '.' line to end ---
   ##
   Warning!!! Warning!!! Warning!!!
   This is our system. You should not login.
   Please close connection.
   ##
   .
   ログイン前メッセージのスクリーンイメージを入力します。
   入力が終わったら，"."（ピリオド）だけの行（または CTRL+D）を入力します。
2. **(config)# show banner**
   banner login encode
   "IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjCldhcm5pbmchISEgV2F
   ybmluZyEhISBXYXJuaW5nISEhClRoaXMgaXMgb3VyIHN5c3RlbS4gWW91IHNob3VsZCBub3QgbG9
   naW4uClBsZWFzZSBjbG9zZSBjb25uZWN0aW9uLgojIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
   jIyMjIyMjIyMjIyMK"

入力されたメッセージは自動的にエンコードされて設定されます。

3. **(config)# show banner login plain-text**
   ##
   Warning!!! Warning!!! Warning!!!
   This is our system. You should not login.
   Please close connection.
   ##
   (config)#
   show の際に plain- text パラメータを指定すると，テキスト形式で確認できます。

設定が完了したら，リモート運用端末の telnet または ftp クライアントから本装置へ接続します。接続後，クライアントにメッセージが表示されます。

図 10-6　リモート運用端末から本装置へ接続した例（telnet で接続した場合）

```
> telnet 10.10.10.10
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^]'.

##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
login:
```

図 10-7　リモート運用端末から本装置へ接続した例（ftp で接続した場合）

```
> ftp 10.10.10.10
Connected to 10.10.10.10.
220-
##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
220 10.10.10.10 FTP server (NetBSD-ftpd) ready.
Name (10.10.10.10:staff):
```

10.1.9　VRF でのリモート運用端末からのログインの許可【SL-L3A】

コンフィグレーションコマンド line vty を設定することで，リモート運用端末から本装置にログインできるようになります。さらに，コンフィグレーションコマンド transport input の vrf パラメータを設定して，VRF からのアクセスを許可します。この vrf パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

グローバルネットワークを含む全 VRF で，リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可する設定例を次の図に示します。

図 10-8　グローバルネットワークを含む全 VRF でリモート運用端末からのログインを許可する設定例

```
(config)# line vty 0 2
(config-line)# transport input vrf all telnet
(config-line)#
```

指定 VRF で，リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可する設定例を次の図に示します。なお，グローバルネットワークは含みません。

図 10-9　VRF 2 でリモート運用端末からのログインを許可する設定例

```
(config)# line vty 0 2
(config-line)# transport input vrf 2 telnet
(config-line)#
```

また，リモート運用端末から ftp プロトコルを使用して本装置にアクセスする場合には，コンフィグレーションコマンド ftp-server を設定する必要があります。VRF からのアクセスを許可する場合は，vrf パラメータを設定します。この vrf パラメータが設定されていない場合，グローバルネットワークからのアクセスだけを許可します。

グローバルネットワークを含む全 VRF で，リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可する設定例を次の図に示します。

図 10-10　グローバルネットワークを含む全 VRF でリモート運用端末から ftp プロトコルによるアクセスを許可する設定例

```
(config)# ftp-server vrf all
(config)#
```

指定 VRF で，リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可する設定例を次の図に示します。なお，グローバルネットワークは含みません。

図 10-11　VRF 2 でリモート運用端末から ftp プロトコルによるアクセスを許可する設定例

```
(config)# ftp-server vrf 2
(config)#
```

10.1.10　VRF でのリモート運用端末からのログインを許可する IP アドレスの設定【SL-L3A】

リモート運用端末から本装置へのログインを許可する IP アドレスをアクセスリストに設定することで，ログインを制限できます。

アクセスリストは，グローバルネットワークや VRF に対して個別に設定しますが，同一のアクセスリストを，グローバルネットワークを含むすべての VRF に適用する設定もできます。また，これらを組み合わせて設定できますが，複数のアクセスリストを使用する場合は，最後のアクセスリストだけ暗黙の廃棄が適用されます。

なお，アクセス元の VRF に対してアクセスリストがどのように適用される（アクセスリストの適用範囲）かは，アクセス元とアクセスリストの設定個所との関係によって変わります。例として，グローバルネットワーク，VRF 10 および VRF 20 から本装置にアクセスする場合，アクセスリストが設定されている個所によって，どのアクセスリストが適用されるかを次の表に示します（括弧内が，どのアクセスリストが適用されるかを示しています）。

表 10-3　アクセスリストの適用範囲

アクセスリスト設定個所	アクセス元 VRF		
	グローバルネットワーク	VRF 10	VRF 20
• global	(global)	−	−
• global • VRF 10	(global)	(VRF 10)	−
• global • VRF 10	(global) ※ 適用後	(VRF 10) ※ 適用後	(VRF ALL)

アクセスリスト設定個所	アクセス元 VRF		
	グローバルネットワーク	VRF 10	VRF 20
• VRF ALL	（VRF ALL）	（VRF ALL）	

（凡例）

－：アクセスリストは適用されない。したがって，アクセス制限されない。

global：グローバルネットワーク

VRF 10：VRF 10

VRF ALL：グローバルネットワークを含む全 VRF

注※

個別に設定したアクセスリストは，VRF ALL に設定したアクセスリストよりも優先して適用されます。また，アクセスリストを複数使用しているため，個別に設定したアクセスリストの暗黙の廃棄は無視されます。そのため，個別に設定したアクセスリストに一致しない場合は，VRF ALL に設定したアクセスリストが適用されます。VRF ALL に設定したアクセスリストに一致しない場合は，暗黙の廃棄によって制限されます。

なお，設定後はリモート運用端末から本装置へのログインの可否を確認してください。

[設定のポイント]

特定のリモート運用端末からだけ本装置へのアクセスを許可する場合は，アクセスリストを使用します。コンフィグレーションコマンド ip access-list standard, ipv6 access-list, access-list, ip access-group，ipv6 access-class で，あらかじめアクセスを許可する端末の IP アドレスを登録しておく必要があります。アクセスを許可する IPv4 アドレスとサブネットマスク，または IPv6 アドレスとプレフィックスは, 合わせて最大 128 個の登録ができます。このコンフィグレーションを設定していない場合，すべてのリモート運用端末から本装置へのアクセスが可能となります。なお，アクセスを許可していない（コンフィグレーションで登録していない）端末からのアクセスがあった場合，すでにログインしているそのほかの端末には，アクセスがあったことを示す”Unknown host address <IP アドレス>”のメッセージが表示されます。

設定例を次に示します。まず，グローバルネットワークを含む全 VRF でのリモート運用端末からのログインを制限します。次に，グローバルネットワークと指定 VRF だけ個別にログインを許可します。これによって，特定のネットワークからだけログインを許可します。

[コマンドによる設定]

1. **(config)# ip access-list standard REMOTE_VRFALL**
   (config-std-nacl)# deny any
   (config-std-nacl)# exit
   グローバルネットワークを含む全 VRF で, ログインを制限するアクセスリスト REMOTE_VRFALL を設定します。
2. **(config)# ip access-list standard REMOTE_GLOBAL**
   (config-std-nacl)# permit 192.168.0.0 0.0.0.255
   (config-std-nacl)# exit
   グローバルネットワークで，ネットワーク（192.168.0.0/24）からだけログインを許可するアクセスリスト REMOTE_GLOBAL を設定します。
3. **(config)# ip access-list standard REMOTE_VRF10**
   (config-std-nacl)# permit 10.10.10.0 0.0.0.255
   (config-std-nacl)# exit

VRF 10 で，ネットワーク（10.10.10.0/24）からだけログインを許可するアクセスリスト REMOTE_VRF10 を設定します。

4. **(config)# line vty 0 2**

   (config-line)# ip access-group REMOTE_VRFALL vrf all in

   (config-line)# ip access-group REMOTE_GLOBAL in

   (config-line)# ip access-group REMOTE_VRF10 vrf 10 in

   (config-line)#

   line モードに遷移し，グローバルネットワークを含む全 VRF にアクセスリスト REMOTE_VRFALL を，グローバルネットワークにアクセスリスト REMOTE_GLOBAL を，VRF10 にアクセスリスト REMOTE_VRF10 を適用します。

   グローバルネットワークでは，ネットワーク（192.168.0.0/24）にあるリモート運用端末からだけログインを許可します。

   VRF10 では，ネットワーク（10.10.10.0/24）にあるリモート運用端末からだけログインを許可します。

   また，その他の VRF ではログインを制限します。

10.2　RADIUS/TACACS+の解説

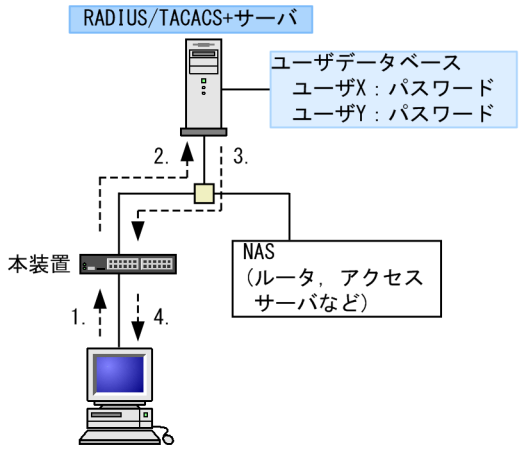
10.2.1　RADIUS/TACACS+の概要

RADIUS（Remote Authentication Dial In User Service），TACACS+（Terminal Access Controller Access Control System Plus）とは，NAS（Network Access Server）に対して認証，承認，およびアカウンティングを提供するプロトコルです。NAS は RADIUS/TACACS+のクライアントとして動作するリモートアクセスサーバ，ルータなどの装置のことです。NAS は構築されている RADIUS/TACACS+サーバに対してユーザ認証，コマンド承認，およびアカウンティングなどのサービスを要求します。RADIUS/TACACS+サーバはその要求に対して，サーバ上に構築された管理情報データベースに基づいて要求に対する応答を返します。本装置は NAS の機能をサポートします。

RADIUS/TACACS+を使用すると一つの RADIUS/TACACS+サーバだけで，複数 NAS でのユーザパスワードなどの認証情報や，コマンド承認情報やアカウンティング情報を一元管理できるようになります。本装置では，RADIUS/TACACS+サーバに対してユーザ認証，コマンド承認，およびアカウンティングを要求できます。

RADIUS/TACACS+認証の流れを次の図に示します。

図 10-12　RADIUS/TACACS+認証の流れ



1. リモート運用端末からユーザXが本装置にtelnetを実行する。
2. 本装置はコンフィグレーションで指定したRADIUS/TACACS+サーバに対して認証を要求する。
3. RADIUS/TACACS+サーバはユーザデータベースに基づいてユーザXを認証し，本装置にユーザXを認証したことを通知する。
4. 本装置はRADIUS/TACACS+認証に基づいて，ユーザXのリモート運用端末からのtelnet許可する。
5. 本装置はコンフィグレーションでコマンド承認を設定した場合，RADIUS/TACACS+サーバに設定してあるコマンドリストに従って，ユーザが投入する運用コマンドを許可／制限する。

10.2.2　RADIUS/TACACS+の適用機能および範囲

本装置では RADIUS/TACACS+を，運用端末からのログイン認証と装置管理者モードへの変更（enable コマンド）時の認証，コマンド承認，およびアカウンティングに使用します。また，RADIUS は IEEE802.1X および Web 認証の端末認証にも使用します。RADIUS/TACACS+機能のサポート範囲を次に示します。

(1)　RADIUS/TACACS+の適用範囲

RADIUS/TACACS+認証を適用できる操作を次に示します。

- 本装置への telnet（IPv4/IPv6）
- 本装置への ssh（IPv4/IPv6）
- 本装置への ftp（IPv4/IPv6）
- 本装置への sftp（IPv4/IPv6）
- 本装置への scp（IPv4/IPv6）
- コンソール（RS232C)からのログイン
- 装置管理者モードへの変更（enable コマンド）

RADIUS/TACACS+コマンド承認を適用できる操作を次に示します。

- 本装置への telnet（IPv4/IPv6）
- 本装置への ssh（IPv4/IPv6）
- コンソール（RS232C）からのログイン

RADIUS/TACACS+アカウンティングを適用できる操作を次に示します。

- 本装置への telnet（IPv4/IPv6）によるログイン・ログアウト
- 本装置への ssh（IPv4/IPv6）によるログイン・ログアウト
- 本装置への ftp（IPv4/IPv6）によるログイン・ログアウト
- 本装置への sftp（IPv4/IPv6）によるログイン・ログアウト
- 本装置への scp（IPv4/IPv6）によるログイン・ログアウト
- コンソール（RS232C）からのログイン・ログアウト
- CLI でのコマンド入力（TACACS+だけサポート）

(2)　RADIUS のサポート範囲

RADIUS サーバに対して，本装置がサポートする NAS 機能を次の表に示します。

表 10-4　RADIUS のサポート範囲

分類	内容
文書全体	NAS に関する記述だけを対象にします。
パケットタイプ	ログイン認証，装置管理者モードへの変更（enable コマンド）時の認証，コマンド承認で使用する次のタイプ • Access-Request (送信) • Access-Accept (受信) • Access-Reject (受信) アカウンティングで使用する次のタイプ • Accounting-Request (送信) • Accounting-Response (受信)

分類	内容
属性	ログイン認証と装置管理者モードへの変更（enable コマンド）時の認証で使用する次の属性 • User-Name • User-Password • Service-Type • NAS-IP-Address • NAS-IPv6-Address • NAS-Identifier • Reply-Message コマンド承認で使用する次の属性 • Class • Vendor-Specific(Vendor-ID=21839) アカウンティングで使用する次の属性 • User-Name • NAS-IP-Address • NAS-IPv6-Address • NAS-Port • NAS-Port-Type • Service-Type • Calling-Station-Id • Acct-Status-Type • Acct-Delay-Time • Acct-Session-Id • Acct-Authentic • Acct-Session-Time

(a)　使用する RADIUS 属性の内容

使用する RADIUS 属性の内容を次の表に示します。

RADIUS サーバを利用してコマンド承認する場合は，認証時に下の表に示すような Class や Vendor-Specific を返すようにあらかじめ RADIUS サーバを設定しておく必要があります。RADIUS サーバには，ベンダー固有属性を登録(dictionary ファイルなどに設定)してください。コマンド承認の属性詳細については「10.2.4　RADIUS/TACACS+/ローカルを使用したコマンド承認」を参照してください。

表 10-5　使用する RADIUS 属性の内容

属性名	属性値	パケットタイプ	内容
User-Name	1	Access-Request Accounting-Request	認証するユーザの名前。 ログイン認証の場合は，ログインユーザ名を送信します。 装置管理者モードへの変更（enable コマンド）時の認証の場合は，「表 10-10　設定するユーザ名属性」に従ってユーザ名を送信します。

属性名	属性値	パケットタイプ	内容
User-Password	2	Access-Request	認証ユーザのパスワード。送信時には暗号化されます。
Service-Type	6	Access-Request Accounting-Request	Login(値=1)。Administrative(値=6，ただしパケットタイプが Access-Request の場合だけ使用)。Access-Accept および Access-Reject に添付された場合は無視します。
NAS-IP-Address	4	Access-Request Accounting-Request	本装置の IP アドレス。ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は送信インタフェースの IP アドレスになります。
NAS-IPv6-Address	95	Access-Request Accounting-Request	本装置の IPv6 アドレス。ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は送信インタフェースの IPv6 アドレスになります。ただし，IPv6 リンクローカルアドレスで通信する場合は，ローカルアドレス設定の有無にかかわらず送信インタフェースの IPv6 リンクローカルアドレスになります。
NAS-Identifier	32	Access-Request Accounting-Request	本装置の装置名。装置名が設定されていない場合は添付されません。
Reply-Message	18	Access-Accept Access-Reject Accounting-Response	サーバからのメッセージ。添付されている場合は，運用ログとして出力されます。
Class	25	Access-Accept	ログインクラス。コマンド承認で適用します。
Vendor-Specific	26	Access-Accept	ログインリスト。コマンド承認で適用します。
NAS-Port	5	Accounting-Request	ユーザが接続されている NAS のポート番号を指します。本装置では，tty ポート番号を格納します。ただし，ftp の場合は 100 を格納します。
NAS-Port-Type	61	Accounting-Request	NAS に接続した方法を指します。本装置では，telnet/ftp は Virtual(5)，コンソールは Async(0)を格納します。
Calling-Station-Id	31	Accounting-Request	利用者の識別 ID を指します。本装置では，telnet/ftp はクライアントの IPv4/IPv6 アドレス，コンソールは“console”を格納します。
Acct-Status-Type	40	Accounting-Request	Accounting-Request がどのタイミングで送信されたかを指します。本装置では，ユーザのログイン時に Start(1)，ログアウト時に Stop(2)を格納します。
Acct-Delay-Time	41	Accounting-Request	送信する必要のあるイベント発生から Accounting-Request を送信するまでにかかった時間(秒)を格納します。
Acct-Session-Id	44	Accounting-Request	セッションを識別するための文字列を指します。本装置では，セッションのプロセス ID を格納します。

属性名	属性値	パケットタイプ	内容
Acct-Authentic	45	Accounting-Request	ユーザがどのように認証されたかを指します。本装置では，RADIUS(1)，Local(2)，Remote(3)の 3 種類を格納します。
Acct-Session-Time	46	Accounting-Request（Acct-Status-Type が Stop の場合だけ）	ユーザがサービスを利用した時間(秒)を指します。本装置では，ユーザがログイン後ログアウトするまでの時間(秒)を格納します。

- Access-Request パケット
  本装置が送信するパケットには，この表で示す以外の属性は添付しません。
- Access-Accept，Access-Reject，Accounting-Response パケット
  この表で示す以外の属性が添付されていた場合，本装置ではそれらの属性を無視します。

(3)　TACACS+のサポート範囲

TACACS+サーバに対して，本装置がサポートする NAS 機能を次の表に示します。

表 10-6　TACACS+のサポート範囲

分類		内容
パケットタイプ		ログイン認証と装置管理者モードへの変更（enable コマンド）時の認証で使用する次のタイプ • Authentication Start (送信) • Authentication Reply(受信) • Authentication Continue (送信) コマンド承認で使用する次のタイプ • Authorization Request (送信) • Authorization Response (受信) アカウンティングで使用する次のタイプ • Accounting Request (送信) • Accounting Reply (受信)
ログイン認証 装置管理者モードへの変更（enable コマンド）時の認証	属性	• User • Password • priv-lvl
コマンド承認	service	• taclogin
	属性	• class • allow-commands • deny-commands
アカウンティング	flag	• TAC_PLUS_ACCT_FLAG_START • TAC_PLUS_ACCT_FLAG_STOP
	属性	• task_id • start_time

分類		内容
		• stop_time • elapsed_time • timezone • service • priv-lvl • cmd

(a)　使用する TACACS+属性の内容

使用する TACACS+属性の内容を次の表に示します。

TACACS+サーバを利用してコマンド承認する場合は，認証時に class または allow-commands や deny-commands 属性とサービスを返すように TACACS+サーバ側で設定します。コマンド承認の属性詳細については「10.2.4　RADIUS/TACACS+/ローカルを使用したコマンド承認」に示します。

表 10-7　使用する TACACS+属性の内容

service	属性	説明
-	User	認証するユーザの名前。 ログイン認証の場合は，ログインユーザ名を送信します。 装置管理者モードへの変更（enable コマンド）時の認証の場合は，「表 10-10　設定するユーザ名属性」に従ってユーザ名を送信します。
	Password	認証ユーザのパスワード。送信時には暗号化されます。
	priv-lvl	認証するユーザの特権レベル。 ログイン認証の場合，1 を使用します。装置管理者モードへの変更（enable コマンド）時の認証の場合，15 を使用します。
taclogin	class	コマンドクラス
	allow-commands	許可コマンドリスト
	deny-commands	制限コマンドリスト

（凡例）－：該当なし

アカウンティング時に使用する TACACS+ flag を次の表に示します。

表 10-8　TACACS+アカウンティング flag 一覧

flag	内容
TAC_PLUS_ACCT_FLAG_START	アカウンティング START パケットを示します。ただし，aaa コンフィグレーションで送信契機に stop-only を指定している場合は，アカウンティング START パケットは送信しません。
TAC_PLUS_ACCT_FLAG_STOP	アカウンティング STOP パケットを示します。ただし，aaa コンフィグレーションで送信契機に stop-only を指定している場合は，このアカウンティング STOP パケットだけを送信します。

アカウンティング時に使用する TACACS+属性(Attribute-Value)の内容を次の表に示します。

表 10-9　TACACS+アカウンティング Attribute-Value 一覧

Attribute	Value
task_id	イベントごとに割り当てられる ID です。本装置ではアカウンティングイベントのプロセス ID を格納します。
start_time	イベントを開始した時刻です。本装置ではアカウンティングイベントが開始された時刻を格納します。この属性は次のイベントで格納されます。 • 送信契機 start-stop 指定時のログイン時，コマンド実行前 • 送信契機 stop-only 指定時のコマンド実行前
stop_time	イベントを終了した時刻です。本装置ではアカウンティングイベントが終了した時刻を格納します。この属性は次のイベントで格納されます。 • 送信契機 start-stop 指定時のログアウト時，コマンド実行後 • 送信契機 stop-only 指定時のログアウト時
elapsed_time	イベント開始からの経過時間(秒)です。本装置ではアカウンティングイベントの開始から終了までの時間(秒)を格納します。この属性は次のイベントで格納されます。 • 送信契機 start-stop 指定時のログアウト時，コマンド実行後 • 送信契機 stop-only 指定時のログアウト時
timezone	タイムゾーン文字列を格納します。
service	文字列“shell”を格納します。
priv-lvl	コマンドアカウンティング設定時に，入力されたコマンドが運用コマンドの場合は 1，コンフィグレーションコマンドの場合は 15 を格納します。
cmd	コマンドアカウンティング設定時に，入力されたコマンド文字列（最大 250 文字）を格納します。

10.2.3　RADIUS/TACACS+を使用した認証

RADIUS/TACACS+を使用した認証方法について説明します。

(1)　認証サービスの選択

ログイン認証および装置管理者モードへの変更（enable コマンド）時の認証に使用するサービスは複数指定できます。指定できるサービスは RADIUS，TACACS+および adduser/password コマンドによる本装置単体でのログインセキュリティ機能です。

これらの認証方式は単独でも同時でも指定できます。同時に指定された場合に先に指定された方式で認証に失敗したときの認証サービスの選択動作を，次に示す end-by-reject を設定するコンフィグレーションコマンドで変更できます。

ログイン認証の場合

　aaa authentication login end-by-reject

装置管理者モードへの変更（enable コマンド）時の認証の場合

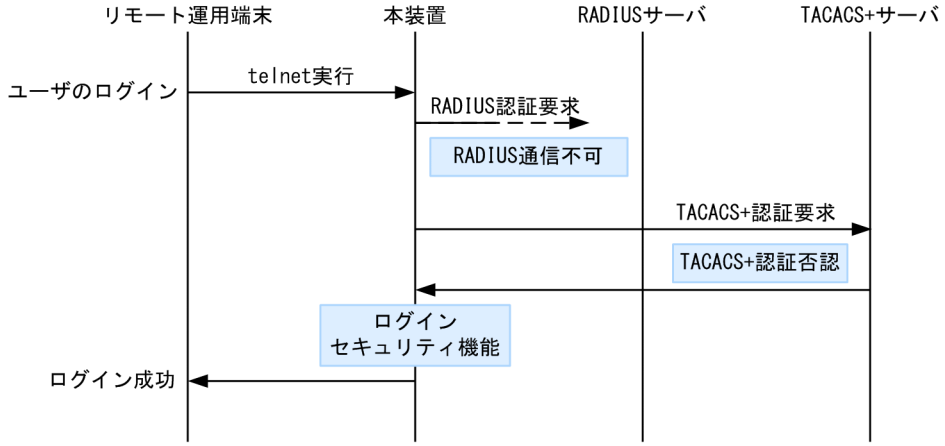
　aaa authentication enable end-by-reject

(a)　end-by-reject 未設定時

end-by-reject 未設定時の認証サービスの選択について説明します。end-by-reject 未設定時は，先に指定された方式で認証に失敗した場合に，その失敗の理由に関係なく，次に指定された方式で認証できます。

例として，コンフィグレーションで認証方式に RADIUS，TACACS+，単体でのログインセキュリティの順番で指定し，それぞれの認証結果が RADIUS サーバ通信不可，TACACS+サーバ認証否認，ログインセキュリティ機能認証成功となる場合の認証方式シーケンスを次の図に示します。

図 10-13　認証方式シーケンス（end-by-reject 未設定時）



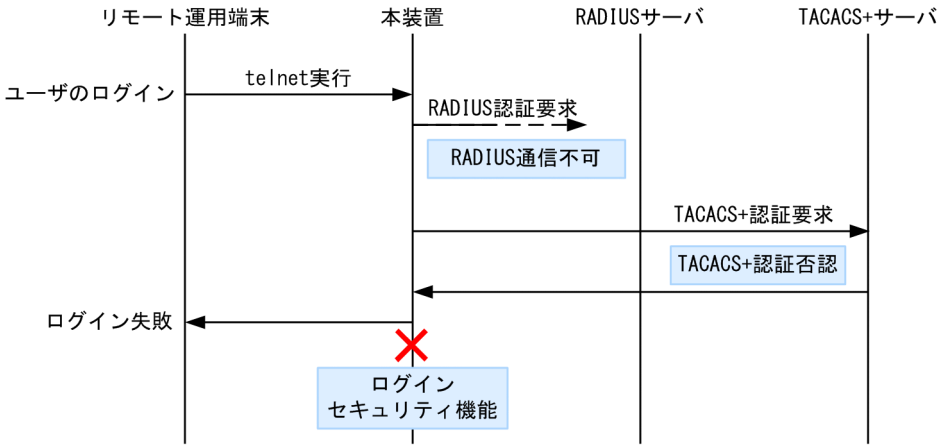
この図で端末からユーザが本装置に telnet を実行すると，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバとの通信不可によって RADIUS サーバでの認証に失敗すると，次に TACACS+サーバに対し本装置から TACACS+認証を要求します。TACACS+認証否認によって TACACS+サーバでの認証に失敗すると，次に本装置のログインセキュリティ機能での認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

(b)　end-by-reject 設定時

end-by-reject 設定時の認証サービスの選択について説明します。end-by-reject 設定時は，先に指定された方式で認証否認された場合に，次に指定された方式で認証を行いません。否認された時点で認証を終了し，一連の認証が失敗となります。通信不可などの異常によって認証が失敗した場合だけ，次に指定された方式で認証できます。

例として，コンフィグレーションで認証方式に RADIUS，TACACS+，単体でのログインセキュリティの順番で指定し，それぞれの認証結果が RADIUS サーバ通信不可，TACACS+サーバ認証否認となる場合の認証方式シーケンスを次の図に示します。

図 10-14　認証方式シーケンス（end-by-reject 設定時）



この図で端末からユーザが本装置に telnet を実行すると，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバとの通信不可によって RADIUS サーバでの認証に失敗すると，次に TACACS+サーバに対し本装置から TACACS+認証を要求します。TACACS+認証否認によって TACACS+サーバでの認証に失敗すると，この時点で一連の認証が失敗となり，認証を終了します。次に指定されている本装置のログインセキュリティ機能での認証を実行しません。その結果，ユーザは本装置へのログインに失敗します。

(2)　RADIUS/TACACS+サーバの選択

RADIUS サーバ，TACACS+サーバはそれぞれ最大四つまで指定できます。一つのサーバと通信できず，認証サービスが受けられない場合は，順次これらのサーバへの接続を試行します。

また，RADIUS サーバ，TACACS+サーバをホスト名で指定したときに，複数のアドレスが解決できた場合は，優先順序に従い，アドレスを一つだけ決定し，RADIUS サーバ，TACACS+サーバと通信します。

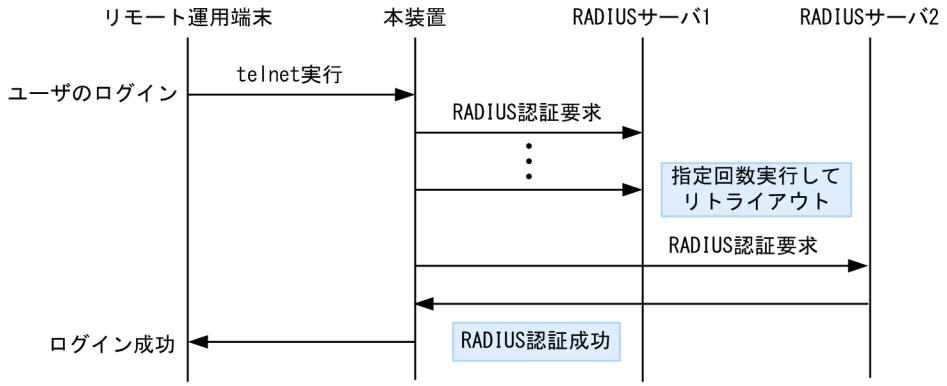
優先順序についての詳細は，「13　ホスト名と DNS　13.1　解説」を参照してください。

注意

DNS サーバを使用してホスト名を解決する場合，DNS サーバとの通信に時間が掛かることがあります。このため，RADIUS サーバ，TACACS+サーバは IP アドレスで指定することをお勧めします。

RADIUS/TACACS+サーバと通信不可を判断するタイムアウト時間を設定できます。デフォルト値は 5 秒です。また，各 RADIUS サーバでタイムアウトした場合は，再接続を試行します。この再試行回数も設定でき，デフォルト値は 3 回です。このため，ログイン方式として RADIUS が使用できないと判断するまでの最大時間は，タイムアウト時間×リトライ回数×RADIUS サーバ設定数になります。なお，各 TACACS+サーバでタイムアウトした場合は，再接続を試行しません。このため，ログイン方式として TACACS+が使用できないと判断するまでの最大時間は，タイムアウト時間×TACACS+サーバ設定数になります。RADIUS サーバ選択のシーケンスを次の図に示します。

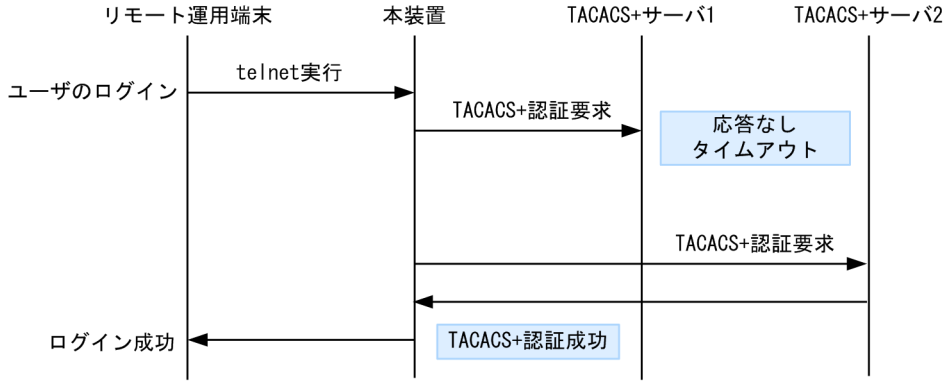
図 10-15　RADIUS サーバ選択のシーケンス



この図でリモート運用端末からユーザが本装置に telnet を実行すると，RADIUS サーバ 1 に対し本装置から RADIUS 認証を要求します。RADIUS サーバ 1 と通信できなかった場合は，続いて RADIUS サーバ 2 に対して RADIUS 認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

TACACS+サーバ選択のシーケンスを次の図に示します。

図 10-16　TACACS+サーバ選択のシーケンス



この図でリモート運用端末からユーザが本装置に telnet を実行すると，TACACS+サーバ 1 に対し本装置から TACACS+認証を要求します。TACACS+サーバ 1 と通信できなかった場合は，続いて TACACS+サーバ 2 に対して TACACS+認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

(3)　RADIUS/TACACS+サーバへの登録情報

(a)　ログイン認証を使用する場合

RADIUS/TACACS+サーバにユーザ名およびパスワードを登録します。RADIUS/TACACS+サーバへ登録するユーザ名には次に示す 2 種類があります。

- 本装置に adduser コマンドを使用して登録済みのユーザ名
  本装置に登録されたユーザ情報を使用してログイン処理を行います。
- 本装置に未登録のユーザ名
  次に示す共通のユーザ情報でログイン処理を行います。
  - ユーザ ID：remote_user
  - ホームディレクトリ：/usr/home/remote_user

本装置に未登録のユーザでログインした場合の注意点を示します。

- ファイルの管理

  ファイルを作成した場合，すべて remote_user 管理となって，別のユーザでも，作成したファイルの読み込みおよび書き込みができます。重要なファイルは ftp などで外部に保管するなど，ファイルの管理に注意してください。

(b)　装置管理者モードへの変更（enable コマンド）時の認証を使用する場合

装置管理者モードへの変更（enable コマンド）用に，次のユーザ情報を登録してください。

- ユーザ名

  本装置ではユーザ名属性として，次の表に示すユーザ名をサーバに送信します。送信するユーザ名はコンフィグレーションコマンドで変更できます。対応するユーザ名をサーバに登録してください。

  表 10-10　設定するユーザ名属性

コマンド名	ユーザ名	
	RADIUS 認証	TACACS+認証
設定なし	admin	admin
aaa authentication enable attribute-user-per-method	$enab15$	ログインユーザ名

- 特権レベル

  特権レベルは 15 で固定です。

ただし，サーバによっては，送信したユーザ名属性に関係なく特定のユーザ名（例えば$enab15$）を使用する場合や，特権レベルの登録が不要な場合などがあります。詳細は，使用するサーバのマニュアルを確認してください。

10.2.4　RADIUS/TACACS+/ローカルを使用したコマンド承認

RADIUS/TACACS+/ローカル（コンフィグレーション）を使用したコマンド承認方法について説明します。

(1)　コマンド承認の概要

RADIUS サーバ，TACACS+サーバ，またはローカルパスワードによる認証の上ログインしたユーザに対し，使用できる運用コマンドの種類を制限することができます。これをコマンド承認と呼びます。使用できる運用コマンドは，RADIUS サーバまたは TACACS+サーバから取得する，コマンドクラスおよびコマンドリスト，またはコンフィグレーションで設定したコマンドクラスおよびコマンドリストに従い制御を行います。また，制限した運用コマンドは，CLI の補完機能で補完候補として表示しません。なお，<option>や<Host Name>などの，<>で囲まれたパラメータ部分の値や文字列を含んだ運用コマンドを，許可するコマンドリストに指定した場合は，<>部分は補完候補として表示しません。

図 10-17　RADIUS/TACACS+サーバによるログイン認証，コマンド承認

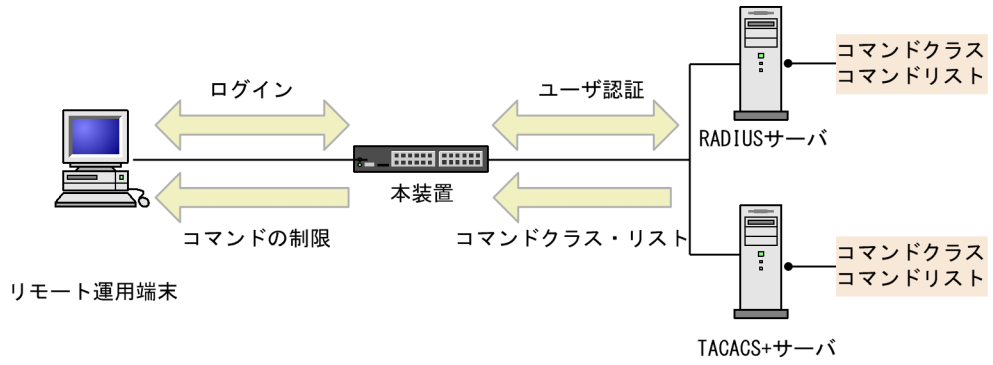
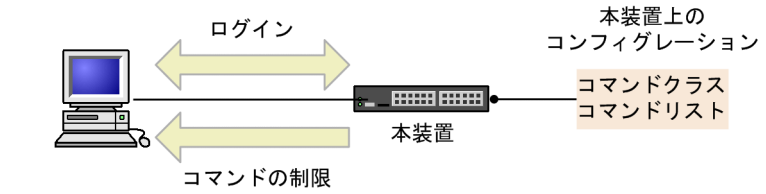


図 10-18　ローカルによるログイン認証，コマンド承認



本装置の aaa コンフィグレーションでコマンド承認を設定すると，RADIUS/TACACS+指定時は，ログイン認証と同時に，サーバからコマンドリストを取得します。ローカル指定時は，ログイン認証と同時に，コンフィグレーションで設定されたコマンドリストを使用します。本装置ではこれらのコマンドリストに従ってログイン後の運用コマンドを許可／制限します。

図 10-19　RADIUS/TACACS+サーバによるコマンド承認のシーケンス

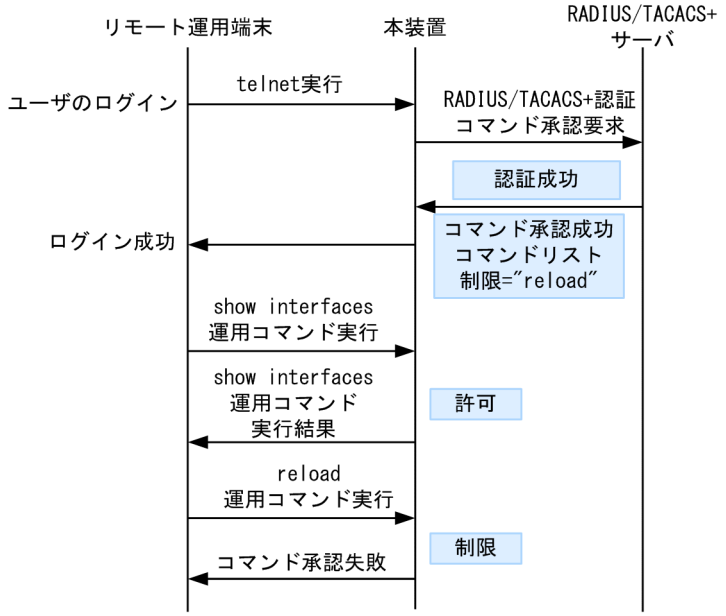
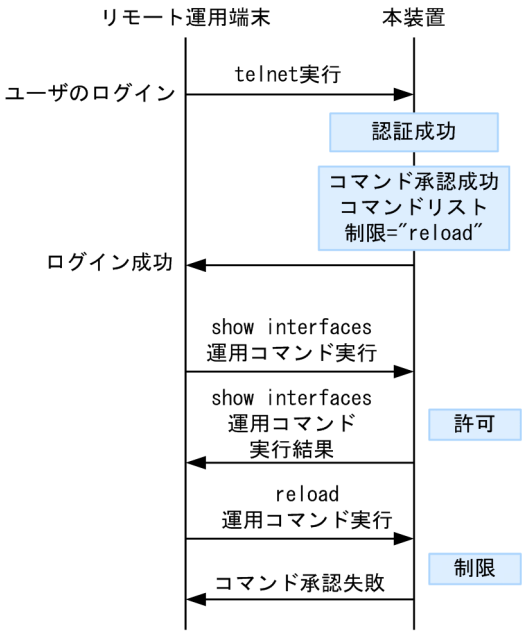


図 10-20　ローカルコマンド承認のシーケンス



「図 10-19　RADIUS/TACACS+サーバによるコマンド承認のシーケンス」で端末からユーザが本装置に telnet を実行すると，RADIUS/TACACS+サーバに対し本装置から認証，コマンド承認を要求します。認証成功時に RADIUS/TACACS+サーバからコマンドリストを取得し，ユーザは本装置にログインします。

「図 10-20　ローカルコマンド承認のシーケンス」で端末からユーザが本装置に telnet を実行すると，ローカル認証を行います。認証成功時にコンフィグレーションからコマンドリストを取得し，ユーザは本装置にログインします。

ログイン後，ユーザは本装置で運用コマンド show interfaces などを実行できますが，運用コマンド reload はコマンドリストによって制限されているために実行できません。

注意

RADIUS/TACACS+サーバのコマンドリストの設定を変更した場合またはコンフィグレーションのコマンドリストを変更した場合は，次回のログイン認証後から反映されます。

(2)　RADIUS/TACACS+/ローカルコマンド承認設定手順

RADIUS/TACACS+によるコマンド承認を使用するためには，次の手順で RADIUS/TACACS+サーバや本装置を設定します。

1. コマンド制限のポリシーを決める。

   各ユーザに対し，運用コマンドの中で，制限・許可するコマンドのポリシーを決めます。

2. コマンドリストを指定する。

   コマンドクラス以外に，許可／制限コマンドリストとして，許可コマンドと制限コマンドをそれぞれ指定できます。

3. RADIUS/TACACS+サーバを設定する。

   決定したコマンド制限ポリシーを基に，RADIUS または TACACS+のリモート認証サーバに，コマンド制限のための設定を行います。

4. 本装置のリモート認証を設定する。

本装置で RADIUS または TACACS+サーバのコンフィグレーション設定と aaa コンフィグレーション設定を行います。

5. コマンド承認の動作を確認する。
   RADIUS/TACACS+を使用したリモート運用端末から本装置へログインし，確認を行います。

ローカルコマンド承認を使用するためには，次の手順で本装置を設定します。

1. コマンド制限のポリシーを決める。
   各ユーザに対し，運用コマンドの中で，制限・許可するコマンドのポリシーを決めます。
2. コマンドリストを作成する。
   コマンドクラス以外に，コマンドリストとして許可コマンドと制限コマンドをそれぞれ指定できます。決定したコマンド制限ポリシーを基に，コマンドリストのコンフィグレーション設定を行います。
   なお，コマンドクラスだけを使用する場合は作成不要です。
3. ユーザにコマンドクラスまたはコマンドリストを割り当てる。
   各ユーザに対し，コマンドクラスまたはコマンドリストを割り当てる username コンフィグレーション設定を行います。
   その後に，aaa コンフィグレーション設定を行います。
4. コマンド承認の動作を確認する。
   本装置へローカル認証でログインし確認を行います。

(3)　コマンド制限のポリシー決定

各ユーザに対し，運用コマンドの中で，制限・許可するコマンドのポリシーを決めます。ここでは，各ユーザがログインしたときに，あるコマンド群は許可し，それ以外のコマンドは制限するなどを決めます。ポリシーは「(5)　RADIUS/TACACS+/ローカルコマンド承認の設定」で設定します。

コマンド制限・許可の対象となるのは，運用コマンドです。マニュアル未掲載のデバッグコマンド（ps コマンドなど）は対象外で，常に制限されます（許可が必要な場合は，次に説明するコマンドクラスで root を指定してコマンド無制限クラスとしてください）。なお，logout，exit，quit，disable，end，set terminal，show whoami，who am i コマンドに関しては常に許可されます。

本装置には，あらかじめ「コマンドクラス」として，以下のポリシーが定義されています。規定のコマンドクラスを選択することで，そのクラスの応じたコマンド制限を行うことができます。

表 10-11　コマンドクラス一覧

コマンドクラス	許可コマンド	制限コマンド
root 全コマンド無制限クラス	従来どおりすべてのコマンド（マニュアル未掲載のデバッグコマンドを含む）	なし
allcommand 運用コマンド無制限クラス	すべての運用コマンド"all"	なし（マニュアル未掲載のデバッグコマンドは不可）
noconfig コンフィグレーション変更制限クラス（コンフィグレーションコマンド指定も制限します）	制限以外の運用コマンド	"config, copy, erase configuration"
nomanage ユーザ管理コマンド制限クラス	制限以外の運用コマンド	"adduser, rmuser, clear password, password, killuser"

コマンドクラス	許可コマンド	制限コマンド
noenable 装置管理者モードコマンド制限クラス	制限以外の運用コマンド	"enable"

また，コマンドクラス以外に，許可コマンドリストと制限コマンドリストをそれぞれ指定することもできます。

(4)　コマンドリストの指定方法について

コマンドクラス以外に，許可／制限コマンドリストとして，許可コマンドと制限コマンドをそれぞれ指定できます。コマンドを指定する場合は，各コマンドリストに設定対象のコマンド文字列をスペースも意識して指定します。複数指定する場合はコンマ(,)で区切って並べます。なお，ローカルコマンド承認では，コマンド文字列をコンフィグレーションコマンド commands exec で一つずつ設定します。本装置では，その設定されたコマンド文字列をコンマ(,)で連結したものをコマンドリストとして使用します。

コマンドリストで指定されたコマンド文字列と，ユーザが入力したコマンドの先頭部分とが，合致するかどうかを判定します(前方一致)。なお，特別な文字列として，all を指定できます。all は運用コマンドすべてを意味します。

判定時に，許可コマンドリストと制限コマンドリストの両方に合致した場合は，合致したコマンド文字数が多い方の動作を採用します（ただし，all 指定は文字数を 1 とします)。その際，許可コマンドリストと制限コマンドリストに同じコマンド文字列が指定されていた場合は，許可として判定されます。

また，コマンドクラスと許可／制限コマンドリストを同時に指定した場合は，コマンドクラスごとに規定されているコマンドリスト（「表 10-11　コマンドクラス一覧」中の" "で囲まれているコマンドリストに対応）と許可／制限コマンドリストを合わせて判定を行います。なお，コマンドクラスに root を指定した場合，許可／制限コマンドクラスの設定は無効となり，マニュアル未掲載のデバッグコマンド（ps コマンドなど）を含むすべてのコマンドが実行できるようになります。

例 1～7 にある各コマンドリストを設定した場合，本装置でどのようなコマンドが許可／制限されるかを示します。

(例 1)

許可コマンドリストだけを設定した場合，設定されたコマンドだけが実行を許可されます。

表 10-12　コマンドリスト例 1

コマンドリスト	指定コマンド	判定
許可コマンドリスト="show ,ping" 制限コマンドリスト 設定なし	show ip arp	許可
	ping ipv6 ::1	許可
	reload	制限

(例 2)

許可コマンドリストと制限コマンドリストの両方に合致した場合は，合致したコマンド文字数が多い方の動作とします(ただし，all 指定は文字数 1 とします)。

表 10-13　コマンドリスト例 2

コマンドリスト	指定コマンド	判定
許可コマンドリスト="show ,ping ipv6"	show system	許可

コマンドリスト	指定コマンド	判定
制限コマンドリスト="show ip,ping"	show ipv6 neighbors	制限
	ping ipv6 ::1	許可
	ping 10.10.10.10	制限

(例 3)

許可コマンドリストと制限コマンドリストの両方を設定し，両方に合致しない場合は，許可として判定されます。

表 10-14　コマンドリスト例 3

コマンドリスト	指定コマンド	判定
許可コマンドリスト="show" 制限コマンドリスト="reload"	ping 10.10.10.10	許可
	reload	制限

(例 4)

許可コマンドリストと制限コマンドリストに同じコマンド文字列が指定されている場合は，許可として判定されます。

表 10-15　コマンドリスト例 4

コマンドリスト	指定コマンド	判定
許可コマンドリスト="show" 制限コマンドリスト="show,ping"	show system	許可
	ping ipv6 ::1	制限

(例 5)

コマンドリストをまったく設定しなかった場合は，logout などのコマンド以外はすべて制限されます。

表 10-16　コマンドリスト例 5

コマンドリスト	指定コマンド	判定
許可コマンドリスト 設定なし 制限コマンドリスト 設定なし	すべて	制限
	logout，exit，quit，disable，end，set terminal，show whoami，who am i	許可

(例 6)

クラスとして root を指定した場合は，従来どおりすべてのコマンドが実行可能となります。なお，コマンドクラスに root を指定した場合，許可／制限コマンドクラスの制限は無効となり，マニュアル未掲載のデバッグコマンド（ps コマンドなど）を含むすべてのコマンドが実行可能となります。

表 10-17　コマンドリスト例 6

コマンドリスト	指定コマンド	判定
コマンドクラス="root"	すべて（マニュアル未掲載のデバッグコマンドを含む）	許可

(例 7)

制限コマンドリストだけを設定した場合は，リストに合致しない運用コマンドはすべて許可となります。

表 10-18　コマンドリスト例 7

コマンドリスト	指定コマンド	判定
許可コマンドリスト 設定なし 制限コマンドリスト= "reload"	reload 以外の運用コマンドすべて	許可
	reload	制限

本マニュアルでは，例として次表のようなポリシーでコマンド制限を行います。

表 10-19　コマンド制限のポリシー例

ユーザ名	コマンドクラス	許可コマンド	制限コマンド
staff	allcommand	運用コマンドすべて	なし
guest	なし	制限以外の運用コマンドすべて許可	reload …※ inactivate …※ enable …※
test	なし	show ip …※ (show ipv6 …は制限)	許可以外，すべて制限

注※　…は任意のパラメータを意味します（show ip …は show ip arp など)。

(5)　RADIUS/TACACS+/ローカルコマンド承認の設定

「表 10-19　コマンド制限のポリシー例」で決定したコマンド制限ポリシーを基に，RADIUS または TACACS+のリモート認証サーバでは，通常のログイン認証の設定以外に，以下の属性値を使用したコマンド制限のための設定を行います。

なお，サーバ側でコマンド承認の設定を行っていない場合，ユーザが認証されログインできても logout，exit，quit，disable，end，set terminal，show whoami，who am i 以外のすべてのコマンドが制限され，コマンドを実行できなくなりますのでご注意ください。その場合は，コンソールからログインしてください。

また，コンフィグレーションコマンド aaa authorization commands console によってコンソールもコマンド承認の対象となっている場合は，デフォルトリスタート後，ログインしてください。

- RADIUS サーバを使用する場合

RADIUS サーバを利用してコマンド制限する場合は，認証時に以下のような属性を返すようにサーバで設定します。

表 10-20　RADIUS 設定属性一覧

属性	ベンダー固有属性	値
25 Class	－	クラス 次の文字列のどれか一つを指定します。 root，allcommand，noconfig，nomanage，noenable
26 Vendor-Specific Vendor-Id: 21839	ALAXALA-Allow-Commands Vendor type: 101	許可コマンドリスト 許可するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては"all"を指定します。

属性	ベンダー固有属性	値
		許可コマンドリストだけ設定した場合は, 許可コマンドリスト以外のコマンドはすべて制限となります。 (例：ALAXALA-Allow-Commands="show ,ping ,telnet ")
	ALAXALA-Deny-Commands Vendor type: 102	制限コマンドリスト 制限するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては"all"を指定します。 制限コマンドリストだけ設定した場合は, 制限コマンドリスト以外はすべて許可となります。 (例：ALAXALA-Deny-Commands="enable,reload, inactivate")

(凡例) －：該当なし

RADIUS サーバには，上記のベンダー固有属性を登録（dictionary ファイルなどに設定）してください。

図 10-21　RADIUS サーバでのベンダー固有属性の dictionary ファイル登録例

```
VENDOR          ALAXALA                     21839
ATTRIBUTE       ALAXALA-Allow-Commands      101       string  ALAXALA
ATTRIBUTE       ALAXALA-Deny-Commands       102       string  ALAXALA
```

「表 10-19　コマンド制限のポリシー例」で決定したポリシーを一般的な RADIUS サーバに設定する場合, 以下のような設定例になります。

図 10-22　RADIUS サーバ設定例

```
staff  Password = "******"
       Class = "allcommand"                                    … 1


guest  Password = "******"
       Alaxala-Deny-Commands = "enable,reload,inactivate"      … 2


test  Password = "******"
      Alaxala-Allow-Commands = "show ip "                      … 3
```

注 ******の部分には各ユーザのパスワードを設定します。

1. クラス"allcommand"で運用コマンドすべてを許可します。
2. enable，reload，および inactivate で始まるコマンドを制限します。
   allow-commands が指定されていないため，ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
   "show ip "の後ろに空白があるため，show ip arp などのコマンドは許可されますが，show ipv6 neighbors などのコマンドは許可されません。
   ほかのコマンドはすべて制限となります。

注意

- 本装置では Class エントリを複数受信した場合，1 個目の Class を認識し 2 個目以降の Class エントリは無効となります。

図 10-23　複数 Class エントリ設定例

```
Class = "noenable"                                                    … 1

Class = "allcommand"
```

1. 本装置では一つ目の noenable だけ有効となります。

- 本装置では Class エントリに複数のクラス名を記述した場合，1 個目のクラス名を認識し 2 個目以降のクラス名は無効となります。例えば，class="nomanage,noenable"と記述した場合，nomanage だけが有効になります。
- ALAXALA-Deny-Commands, ALAXALA-Allow-Commands のそれぞれにおいて，同一属性のエントリを複数受信した場合，一つの属性につきコンマ(,)と空白も含み 1024 文字までを認識し，1025 文字以降は受信しても無効となります。なお，下記の例のように同一属性を複数エントリ記述し，本装置で 2 個目以降のエントリを受信した場合にはエントリの先頭に自動的にコンマ(,)を設定します。

図 10-24　複数 Deny-Commands エントリ設定例

```
ALAXALA-Deny-Commands = "inactivate,reload"                           … 1

ALAXALA-Deny-Commands = "activate,test,............"                  … 1
```

1. 本装置では下線の部分を合計 1024 文字まで認識します。

　上記の Deny-Commands を受信した場合は，下記のように 2 個目のエントリの先頭である activate コマンドの前にコンマ(,)が自動的に設定されます。

```
Deny-Commands = "inactivate,reload,activate,test,........."
```

- TACACS+サーバを使用する場合

TACACS+サーバを使用してコマンド制限をする場合は，TACACS+サーバで承認の設定として以下のような属性－値のペアを設定します。

表 10-21　TACACS+設定属性一覧

service	属性	値
taclogin	class	コマンドクラス 次の文字列のどれかを指定 root，allcommand，noconfig，nomanage，noenable
	allow-commands	許可コマンドリスト 許可するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては"all"を指定します。 許可コマンドリストだけ設定した場合は，許可コマンドリスト以外のコマンドはすべて制限となります。 （例：allow-commands="show ,ping ,telnet "）
	deny-commands	制限コマンドリスト 制限するコマンドの前方一致文字列をコンマ(,)で区切って指定します。空白も区別します。 運用コマンドすべては"all"を指定します。制限コマンドリストだけ設定した場合は，制限コマンドリスト以外はすべて許可となります。 （例：deny-commands="enable,reload,inactivate"）

「表 10-19　コマンド制限のポリシー例」で決定したポリシーを一般的な TACACS+サーバに設定する場合，以下のような設定ファイルイメージになります。

図 10-25 TACACS+サーバの設定例

```
user=staff {
    login = cleartext "******"
    service = taclogin {                                    … 1
        class = "allcommand"
    }
}


user=guest {
    login = cleartext "******"
    service = taclogin {
        deny-commands = "enable,reload,inactivate"          … 2
    }
}


user=test {
    login = cleartext "******"
    service = taclogin {
        allow-commands = "show ip "                         … 3
    }
}
```

注 ******の部分には各ユーザのパスワードを設定します。

1. service 名は taclogin と設定します。
   クラス"allcommand"で運用コマンドすべてを許可します。
2. enable，reload，および inactivate で始まるコマンドを制限します。
   allow-commands が指定されていないため，ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
   "show ip "の後ろに空白があるため，show ip arp などのコマンドは許可されますが，show ipv6 neighbors などのコマンドは許可されません。
   ほかのコマンドはすべて制限となります。

注意

- 本装置では class エントリに複数のクラス名を記述した場合, 1 個目のクラス名を認識し 2 個目以降のクラス名は無効となります。例えば class="nomanage,noenable"と記述した場合，nomanage だけが有効になります。
- deny-commands，allow-commands のそれぞれにおいて，一つの属性につきコンマ(,)と空白も含み 1024 文字までを認識し，1025 文字以降は受信しても無効となります。

- **ローカルコマンド承認を使用する場合**

「表 10-19 コマンド制限のポリシー例」で決定したポリシーをローカルコマンド承認で設定する場合，次のようなコンフィグレーションの設定になります。

図 10-26 コンフィグレーションの設定例

```
username guest view guest_view
username staff view-class allcommand                        … 1
username test view test_view
!
parser view guest_view
  commands exec exclude all "enable"                        … 2
  commands exec exclude all "inactivate"                    … 2
  commands exec exclude all "reload"                        … 2
!
parser view test_view
  commands exec include all "show ip "                      … 3
!
```

```
aaa authentication login default local
aaa authorization commands default local
```

1. ユーザ"staff"に対し，クラス"allcommand"で運用コマンドすべてを許可します。
2. enable，inactivate，および reload で始まるコマンドを制限します。
   commands exec include が指定されていないため，ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
   "show ip "の後ろに空白があるため，show ip arp などのコマンドは許可されますが，show ipv6 neighbors などのコマンドは許可されません。
   ほかのコマンドはすべて制限となります。

(a) ログインしての確認

設定が完了した後，RADIUS/TACACS+/ローカルを使用したリモート運用端末から本装置へのログインを行います。ログイン後，show whoami コマンドでコマンドリストが設定されていること，コマンドを実行して制限・許可していることを確認してください。

図 10-27　staff がログイン後の確認例

```
> show whoami
Date 20XX/01/07 12:00:00 UTC
staff ttyp0    -----  2   Jan  6 14:17 (10.10.10.10)

Home-directory: /usr/home/staff
Authentication: TACACS+ (Server 192.168.10.1)
Class: allcommand
      Allow: "all"
      Deny : -----
Command-list: -----
>
> show clock
Wed Jan 7 12:00:10 UTC 20XX
> /bin/date
% Command not authorized.
>
```

図 10-28　guest がログイン後の確認例

```
>show whoami
Date 20XX/01/07 12:00:00 UTC
guest ttyp0    -----  2   Jan  6 14:17 (10.10.10.20)

Home-directory: /usr/home/guest
Authentication: RADIUS (Server 192.168.10.1)
Class: -----
Command-list:
      Allow: -----
      Deny : "enable,reload,inactivate"
>
> show clock
Wed Jan 7 12:00:10 UTC 20XX
> reload
% Command not authorized.
>
```

図 10-29　test がログイン後の確認例

```
>show whoami
Date 20XX/01/07 12:00:00 UTC
test ttyp0    -----  2   Jan  6 14:17 (10.10.10.30)

Home-directory: /usr/home/test
Authentication: LOCAL
Class: -----
Command-list:
      Allow: "show ip "
      Deny : -----
```

```
>
> show ip arp
***コマンド実行されます***
> show ipv6 neighbors
% Command not authorized.
>
```

10.2.5　RADIUS/TACACS+を使用したアカウンティング

RADIUS/TACACS+を使用したアカウンティング方法について説明します。

(1)　アカウンティングの指定

本装置の RADIUS/TACACS+コンフィグレーションと aaa accounting コンフィグレーションのアカウンティングを設定すると，運用端末から本装置へのログイン・ログアウト時に RADIUS または TACACS+サーバへアカウンティング情報を送信します。また，本装置へのコマンド入力時に TACACS+サーバへアカウンティング情報を送信します。

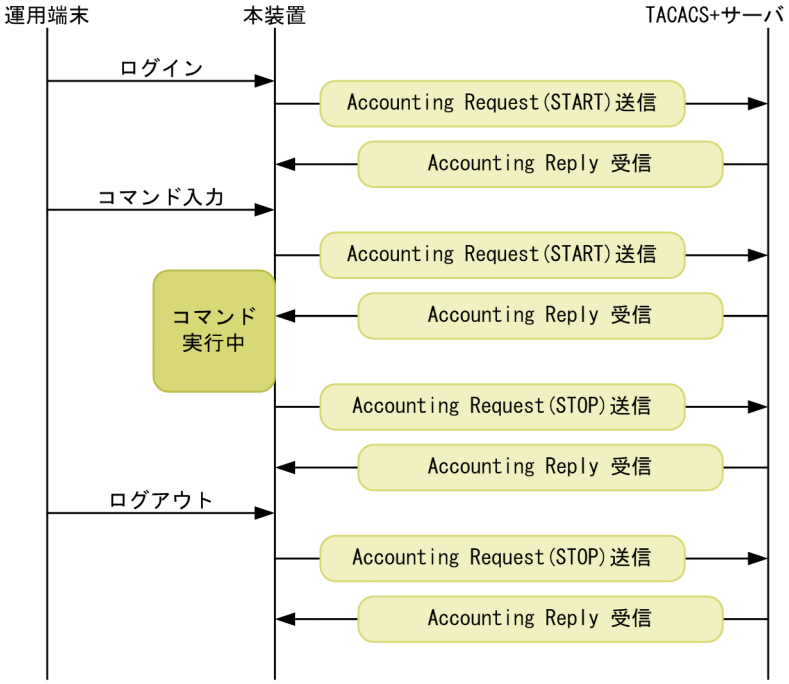
アカウンティングの設定は，ログインとログアウトのイベントを送信するログインアカウンティング指定と, コマンド入力のイベントを送信するコマンドアカウンティング指定があります。コマンドアカウンティングは TACACS+だけでサポートしています。

それぞれのアカウンティングに対して，アカウンティング START と STOP を両方送信するモード（start-stop）と STOP だけを送信するモード（stop-only）を選択できます。さらに，コマンドアカウンティングに対しては, 入力したコマンドをすべて送信するモードとコンフィグレーションだけを送信するモードを選択できます。また，設定された各 RADIUS/TACACS+サーバに対して，通常はどこかのサーバでアカウンティングが成功するまで順に送信しますが, 成功したかどうかにかかわらずすべてのサーバへ順に送信するモード（broadcast）も選択できます。

(2)　アカウンティングの流れ

ログインアカウンティングとコマンドアカウンティングの両方を START-STOP 送信モードで TACACS+サーバへ送信する設定をした場合のシーケンスを次の図に示します。

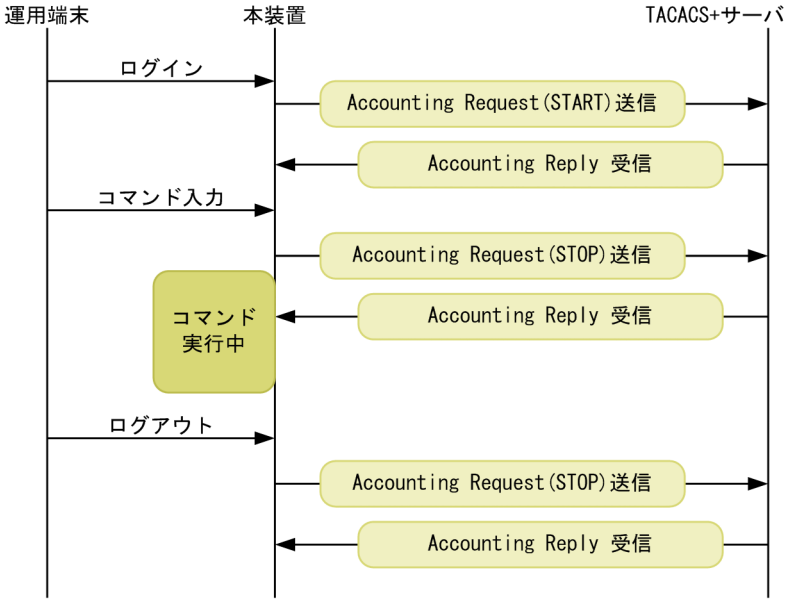
図 10-30　TACACS+アカウンティングのシーケンス（ログイン・コマンドアカウンティングの START-STOP 送信モード時）



この図で運用端末から本装置にログインが成功すると，本装置から TACACS+サーバに対しユーザ情報や時刻などのアカウンティング情報を送信します。また，コマンドの入力前後にも本装置から TACACS+サーバに対し入力したコマンド情報などのアカウンティング情報を送信します。最後に，ログアウト時には，ログインしていた時間などの情報を送信します。

ログインアカウンティングは START-STOP 送信モードのままで，コマンドアカウンティングだけを STOP-ONLY 送信モードして TACACS+サーバへ送信する設定をした場合のシーケンスを次の図に示します。

図 10-31　TACACS+アカウンティングのシーケンス（ログインアカウンティング START-STOP，コマンドアカウンティング STOP-ONLY 送信モード時）



「図 10-30　TACACS+アカウンティングのシーケンス（ログイン・コマンドアカウンティングの START-STOP 送信モード時）」の例と比べると，ログイン・ログアウトでのアカウンティング動作は同じですが，コマンドアカウンティングで STOP-ONLY を指定している場合，コマンドの入力前にだけ本装置から TACACS+サーバに対し入力したコマンド情報などのアカウンティング情報を送信します。

(3)　アカウンティングの注意事項

RADIUS/TACACS+コンフィグレーション，aaa accounting コンフィグレーションのアカウンティングの設定や interface loopback コンフィグレーションで IPv4 装置アドレスを変更した場合は，送受信途中や未送信のアカウンティングイベントと統計情報はクリアされ，新しい設定で動作します。

多数のユーザが，コマンドを連続して入力したり，ログイン・ログアウトを繰り返したりした場合，アカウンティングイベントが大量に発生するため，一部のイベントでアカウンティングできないことがあります。

アカウンティングイベントの大量な発生による本装置・サーバ・ネットワークへの負担を避けるためにも，コマンドアカウンティングは STOP-ONLY で設定することをお勧めします。また，正常に通信できない RADIUS/TACACS+サーバは指定しないでください。

運用コマンド clear accounting でアカウンティング統計情報をクリアする場合，clear accounting コマンドの入力時点で各サーバへの送受信途中のアカウンティングイベントがあるときは，そのイベントの送受信終了後に，各サーバへの送受信統計のカウントを開始します。

DNS サーバを使用してホスト名を解決する場合，DNS サーバとの通信に時間が掛かることがあります。このため，RADIUS サーバおよび TACACS+サーバは IP アドレスで指定することをお勧めします。

10.2.6　RADIUS/TACACS+との接続

(1)　RADIUS サーバとの接続

(a)　RADIUS サーバでの本装置の識別

RADIUS プロトコルでは NAS を識別するキーとして，要求パケットの発信元 IP アドレスを使用するよう規定されています。本装置では要求パケットの発信元 IP アドレスに次に示すアドレスを使用します。

- コンフィグレーションコマンド interface loopback 0 のローカルアドレスが設定されている場合は，ローカルアドレスを発信元 IP アドレスとして使用します。
- ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレスを使用します。

このため，ローカルアドレスが設定されている場合は，RADIUS サーバに本装置を登録するためにローカルアドレスで指定した IP アドレスを使用する必要があります。これによって，RADIUS サーバと通信するインタフェースが特定できない場合は，ローカルアドレスを設定することで RADIUS サーバを確実に識別できる本装置の情報を登録できるようになります。

(b)　RADIUS サーバのメッセージ

RADIUS サーバは応答に Reply-Message 属性を添付して要求元にメッセージを送付する場合があります。本装置では，RADIUS サーバからの Reply-Message 属性の内容を運用ログに出力します。RADIUS サーバとの認証に失敗する場合は，運用ログを参照してください。

(c)　RADIUS サーバのポート番号

RADIUS の認証サービスのポート番号は，RFC2865 で 1812 と規定されています。本装置では特に指定しないかぎり，RADIUS サーバへの要求に 1812 のポート番号を使用します。しかし，一部の RADIUS サーバで 1812 ではなく初期の実装時に使用されていた 1645 のポート番号を使用している場合があります。このときはコンフィグレーション radius-server host の auth-port パラメータで 1645 を指定してください。なお，auth-port パラメータでは 1～65535 の任意の値が指定できますので，RADIUS サーバが任意のポート番号で待ち受けできる場合にも対応できます。

(2)　TACACS+サーバとの接続

(a)　TACACS+サーバの設定

- 本装置と TACACS+サーバを接続する場合は，Service と属性名などに注意してください。TACACS+サーバの属性については，「10.2.4　RADIUS/TACACS+/ローカルを使用したコマンド承認」を参照してください。
- コンフィグレーションコマンド interface loopback 0 のローカルアドレスが設定されている場合は，ローカルアドレスを発信元 IP アドレスとして使用します。

10.3　RADIUS/TACACS+のコンフィグレーション

10.3.1　コンフィグレーションコマンド一覧

RADIUS/TACACS+，アカウンティングに関するコンフィグレーションコマンド一覧を次の表に示します。

表 10-22　コンフィグレーションコマンド一覧（RADIUS）

コマンド名	説明
radius-server host	認証，承認，アカウンティングに使用する RADIUS サーバを設定します。
radius-server key	認証，承認，アカウンティングに使用する RADIUS サーバ鍵を設定します。
radius-server retransmit	認証，承認，アカウンティングに使用する RADIUS サーバへの再送回数を設定します。
radius-server timeout	認証，承認，アカウンティングに使用する RADIUS サーバの応答タイムアウト値を設定します。

表 10-23　コンフィグレーションコマンド一覧（TACACS+）

コマンド名	説明
tacacs-server host	認証，承認，アカウンティングに使用する TACACS+サーバを設定します。
tacacs-server key	認証，承認，アカウンティングに使用する TACACS+サーバの共有秘密鍵を設定します。
tacacs-server timeout	認証，承認，アカウンティングに使用する TACACS+サーバの応答タイムアウト値を設定します。

表 10-24　コンフィグレーションコマンド一覧（アカウンティング）

コマンド名	説明
aaa accounting commands	コマンドアカウンティングを行うときに設定します。
aaa accounting exec	ログイン・ログアウトアカウンティングを行うときに設定します。

10.3.2　RADIUS サーバによる認証の設定

(1)　ログイン認証の設定例

[設定のポイント]

RADIUS サーバ，およびローカル認証を行う設定例を示します。RADIUS サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお，否認によって認証に失敗した場合には，その時点で一連の認証を終了し，ローカル認証を行いません。

あらかじめ，通常のリモートアクセスに必要な設定を行っておく必要があります。

[コマンドによる設定]

1. **(config)# aaa authentication login default group radius local**

ログイン時に使用する認証方式を RADIUS 認証，ローカル認証の順に設定します。

2. **(config)# aaa authentication login end-by-reject**
   RADIUS 認証で否認された場合には，その時点で一連の認証を終了し，ローカル認証を行わないように設定します。
3. **(config)# radius-server host 192.168.10.1 key "039fkllf84kxm3"**
   RADIUS 認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

(2)　装置管理者モードへの変更（enable コマンド）時の認証の設定例

[設定のポイント]

RADIUS サーバ，およびローカル認証を行う設定例を示します。RADIUS サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお，否認によって認証に失敗した場合には，その時点で一連の認証を終了し，ローカル認証を行いません。

また，RADIUS 認証時のユーザ名属性として$enab15$を送信するように設定します。

[コマンドによる設定]

1. **(config)# aaa authentication enable default group radius enable**
   装置管理者モードへの変更（enable コマンド）時に使用する認証方式を RADIUS 認証，ローカル認証の順に設定します。
2. **(config)# aaa authentication enable end-by-reject**
   RADIUS 認証で否認された場合には，その時点で一連の認証を終了し，ローカル認証を行わないように設定します。
3. **(config)# aaa authentication enable attribute-user-per-method**
   RADIUS 認証時のユーザ名属性として$enab15$を送信するように設定します。
4. **(config)# radius-server host 192.168.10.1 key "039fkllf84kxm3"**
   RADIUS 認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

10.3.3　TACACS+サーバによる認証の設定

(1)　ログイン認証の設定例

[設定のポイント]

TACACS+サーバおよびローカル認証を行う設定例を示します。TACACS+サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお，否認によって認証に失敗した場合には，その時点で一連の認証を終了し，ローカル認証を行いません。

あらかじめ，通常のリモートアクセスに必要な設定を行っておく必要があります。

[コマンドによる設定]

1. **(config)# aaa authentication login default group tacacs+ local**
   ログイン時に使用する認証方式を TACACS+認証，ローカル認証の順に設定します。
2. **(config)# aaa authentication login end-by-reject**
   TACACS+認証で否認された場合には，その時点で一連の認証を終了し，ローカル認証を行わないように設定します。
3. **(config)# tacacs-server host 192.168.10.1 key "4h8dlir9r-w2"**
   TACACS+認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

(2)　装置管理者モードへの変更（enable コマンド）時の認証の設定例

[設定のポイント]

TACACS+サーバおよびローカル認証を行う設定例を示します。TACACS+サーバとの通信不可などの異常によって認証に失敗した場合だけローカル認証を行うように設定します。なお，否認によって認証に失敗した場合には，その時点で一連の認証を終了し，ローカル認証を行いません。

また，TACACS+認証時のユーザ名属性としてログインユーザ名を送信するように設定します。

[コマンドによる設定]

1. **(config)# aaa authentication enable default group tacacs+ enable**
   装置管理者モードへの変更（enable コマンド）時に使用する認証方式を TACACS+認証，ローカル認証の順に設定します。
2. **(config)# aaa authentication enable end-by-reject**
   TACACS+認証で否認された場合には，その時点で一連の認証を終了し，ローカル認証を行わないように設定します。
3. **(config)# aaa authentication enable attribute-user-per-method**
   TACACS+認証時のユーザ名属性としてログインユーザ名を送信するように設定します。
4. **(config)# tacacs-server host 192.168.10.1 key "4h8dlir9r-w2"**
   TACACS+認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

10.3.4　RADIUS/TACACS+/ローカルによるコマンド承認の設定

(1)　RADIUS サーバによるコマンド承認の設定例

[設定のポイント]

RADIUS サーバによるコマンド承認を行う設定例を示します。

あらかじめ，RADIUS 認証を使用する設定を行ってください。

[コマンドによる設定]

1. **(config)# aaa authentication login default group radius local**
   (config)# radius-server host 192.168.10.1 key "RaD#001"
   あらかじめ，RADIUS サーバによる認証の設定を行います。
2. **(config)# aaa authorization commands default group radius**
   RADIUS サーバを使用して，コマンド承認を行います。

[注意事項]

本設定後にユーザが RADIUS 認証されてログインしたとき，RADIUS サーバ側でコマンド承認の設定がされていなかった場合は，コマンドがすべて制限されて実行できなくなります。設定ミスなどでコマンドの実行ができない場合は，コンソールからログインして修正してください。なお，コンフィグレーションコマンド aaa authorization commands console によってコンソールもコマンド承認の対象となっている場合は，デフォルトリスタート後，ログインして修正してください。

(2)　TACACS+サーバによるコマンド承認の設定例

[設定のポイント]

TACACS+サーバによるコマンド承認を行う設定例を示します。

あらかじめ，TACACS+認証を使用する設定を行ってください。

[コマンドによる設定]

1. **(config)# aaa authentication login default group tacacs+ local**
   (config)# tacacs-server host 192.168.10.1 key "TaC#001"
   あらかじめ，TACACS+サーバによる認証の設定を行います。
2. **(config)# aaa authorization commands default group tacacs+**
   TACACS+サーバを使用して，コマンド承認を行います。

[注意事項]

本設定後にユーザが TACACS+認証されてログインしたとき，TACACS+サーバ側でコマンド承認の設定がされていなかった場合は，コマンドがすべて制限されて実行できなくなります。設定ミスなどでコマンドの実行ができない場合は，コンソールからログインして修正してください。なお，コンフィグレーションコマンド aaa authorization commands console によってコンソールもコマンド承認の対象となっている場合は，デフォルトリスタート後，ログインして修正してください。

(3)　ローカルコマンド承認の設定例

[設定のポイント]

ローカルコマンド承認を行う設定例を示します。

あらかじめ，ユーザ名とそれに対応したコマンドクラス（username view-class）またはコマンドリスト（username view・parser view・commands exec）の設定を行ってください。

また，ローカルパスワード認証を使用する設定を行ってください。

[コマンドによる設定]

1. **(config)# parser view Local_001**
   (config-view)# commands exec include all "show"
   (config-view)# commands exec exclude all "reload"
   コマンドリストを使用する場合は，あらかじめコマンドリストの設定を行います。
   なお，コマンドクラスだけを使用する場合は，コマンドリストの設定は必要ありません。
2. **(config)# username user001 view Local_001**
   (config)# username user001 view-class noenable
   指定ユーザにコマンドクラスまたはコマンドリストの設定を行います。
   なお，コマンドクラスとコマンドリストを同時に設定することもできます。
3. **(config)# aaa authentication login default local**
   ローカルパスワードによる認証の設定を行います。
4. **(config)# aaa authorization commands default local**
   ローカル認証を使用して，コマンド承認を行います。

[注意事項]

ローカルコマンド承認を設定すると，ローカル認証でログインしたすべてのユーザに適用されますので，設定に漏れがないようご注意ください。

コマンドクラスまたはコマンドリストの設定がされていないユーザは，コマンドがすべて制限されて実行できなくなります。

設定ミスなどでコマンドの実行ができない場合は，コンソールからログインして修正してください。なお，コンフィグレーションコマンド aaa authorization commands console によってコンソールもコマンド承認の対象となっている場合は，デフォルトリスタート後，ログインして修正してください。

10.3.5　RADIUS/TACACS+によるログイン・ログアウトアカウンティングの設定

(1)　RADIUS サーバによるログイン・ログアウトアカウンティングの設定例

[設定のポイント]

RADIUS サーバによるログイン・ログアウトアカウンティングを行う設定例を示します。あらかじめ，アカウンティング送信先となる RADIUS サーバホスト側の設定を行ってください。

[コマンドによる設定]

1. **(config)# radius-server host 192.168.10.1 key "RaD#001"**
   あらかじめ，RADIUS サーバの設定を行います。
2. **(config)# aaa accounting exec default start-stop group radius**
   ログイン・ログアウトアカウンティングの設定を行います。

[注意事項]

radius-server コンフィグレーションの設定がされていない状態で aaa accounting exec を設定した場合，ユーザがログイン・ログアウトしたときに System accounting failed という運用ログが表示されます。使用する radius-server コンフィグレーションを設定してください。

(2)　TACACS+サーバによるログイン・ログアウトアカウンティングの設定例

[設定のポイント]

TACACS+サーバによるログイン・ログアウトアカウンティングを行う設定例を示します。あらかじめ，アカウンティング送信先となる TACACS+サーバホスト側の設定を行ってください。

[コマンドによる設定]

1. **(config)# tacacs-server host 192.168.10.1 key "TaC#001"**
   あらかじめ，TACACS+サーバの設定を行います。
2. **(config)# aaa accounting exec default start-stop group tacacs+**
   ログイン・ログアウトアカウンティングの設定を行います。

[注意事項]

tacacs-server コンフィグレーションの設定がされていない状態で aaa accounting exec を設定した場合，ユーザがログイン・ログアウトしたときに System accounting failed という運用ログが表示されます。使用する tacacs-server コンフィグレーションを設定してください。

10.3.6　TACACS+サーバによるコマンドアカウンティングの設定

(1)　TACACS+サーバによるコマンドアカウンティングの設定例

[設定のポイント]

TACACS+サーバによるコマンドアカウンティングを行う設定例を示します。

あらかじめ，アカウンティング送信先となる TACACS+サーバホスト側の設定を行ってください。

[コマンドによる設定]

1. **(config)# tacacs-server host 192.168.10.1 key "TaC#001"**
   TACACS+サーバの設定を行います。
2. **(config)# aaa accounting commands 0-15 default start-stop group tacacs+**
   コマンドアカウンティングを設定します。

[注意事項]

tacacs-server コンフィグレーションの設定がされていない状態で aaa accounting commands を設定した場合，ユーザがコマンドを入力したときに System accounting failed という運用ログが表示されます。使用する tacacs-server コンフィグレーションを設定してください。

11 SSH(Secure Shell)

この章では，SSH の解説と操作方法について説明します。

11.1　解説

11.1.1　概要

SSH は，クライアントからサーバへ，安全ではないネットワーク上で，セキュアに接続する機能です。

SSH を使用すると，クライアントとサーバは相互に認証し，通信内容を暗号化し，メッセージ認証によって通信内容が変更されていないことを確認します。このため，ネットワーク上の悪意ある第三者によるなりすまし，盗聴，改ざんから通信を保護できます。SSH を使用することで，telnet 接続の脅威（不正なりすましサーバへの誤接続，運用情報の流出，データの改ざんなど）から保護された，セキュアな運用管理を実現できます。telnet 接続による脅威および SSH 接続によるセキュアな運用管理を次の図に示します。

図 11-1　telnet 接続による脅威

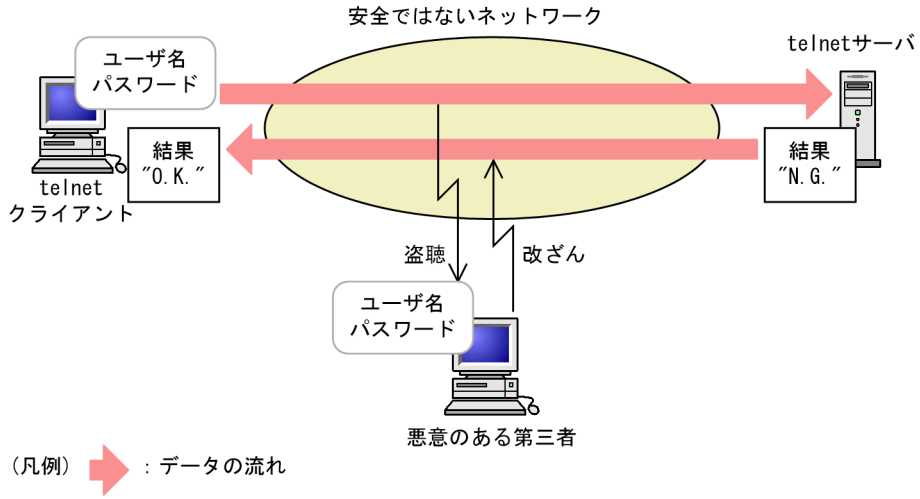
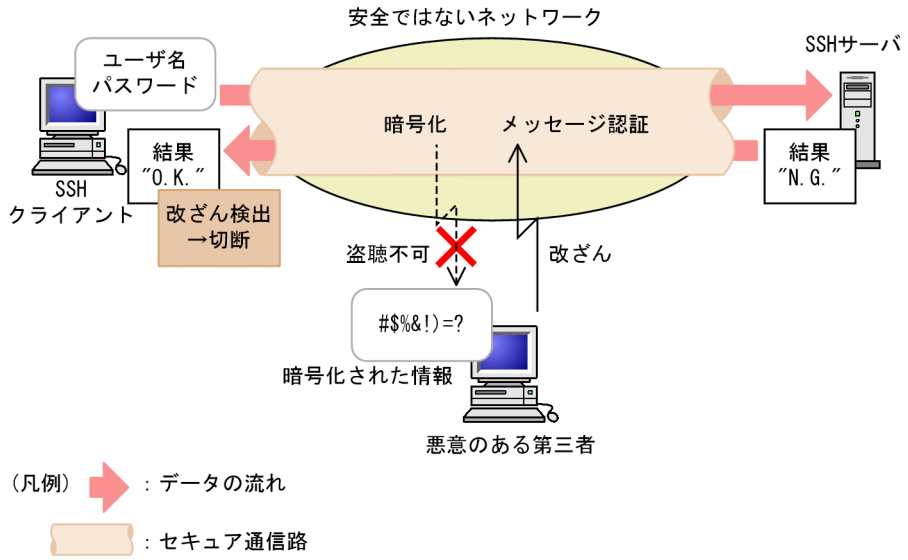


図 11-2　SSH 接続によるセキュアな運用管理



SSH サーバへ接続するユーザの認証方法として，telnet や FTP で使用されていたパスワード認証のほかに，より安全な公開鍵認証を使用できます。公開鍵認証を使用することで，パスワードが漏洩して他者に利用されることを防ぎます。

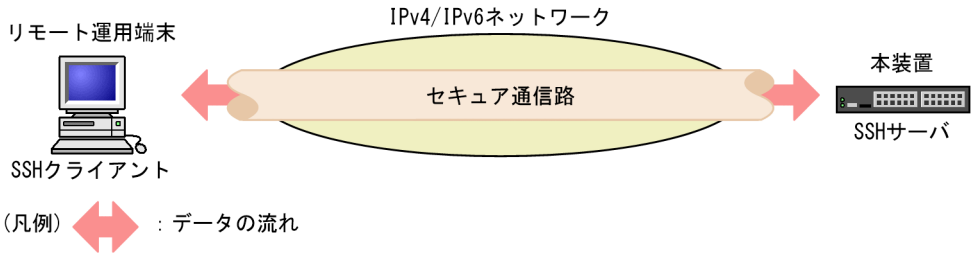
SSH には，バージョン 1（SSHv1）とバージョン 2（SSHv2）があります。本装置は SSHv1 と SSHv2 の両方をサポートしています。

しかし，できるだけ SSHv2 に限定して運用することを推奨します。理由は，SSHv2 は SSHv1 に比べてセキュリティが向上しているためです。SSHv2 では，メッセージ認証によって通信の改ざんを防ぎます。また，SSHv2 は SSHv1 よりも進歩した暗号技術を採用しています。

本装置の SSH 機能は，IPv4 ネットワークと IPv6 ネットワークのどちらでも使用できます。本装置は SSH サーバ機能と SSH クライアント機能の両方をサポートしています。

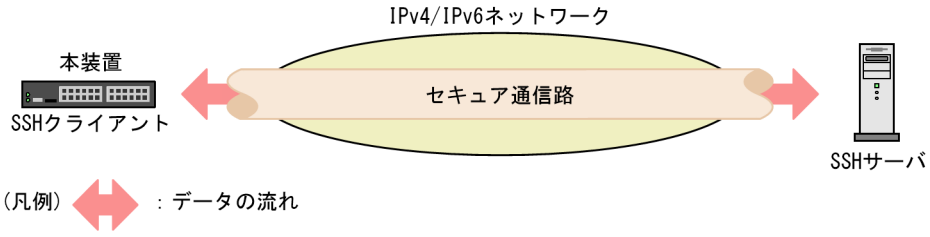
本装置の SSH サーバ機能によって，セキュア通信路上でリモート運用端末から本装置へのログインやファイル転送を実現できます。リモート運用端末から本装置への SSH の接続例を次の図に示します。

図 11-3　リモート運用端末から SSH クライアントを使用して本装置へ接続する例



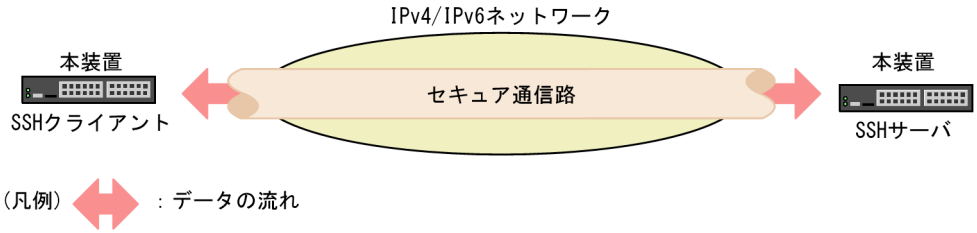
本装置の SSH クライアント機能によって，セキュア通信路を使用して本装置から SSH サーバへのログインやファイル転送を実現できます。本装置から SSH サーバへの接続例を次の図に示します。

図 11-4　本装置の SSH クライアントからリモートにある SSH サーバへ接続する例



また，本装置は SSH サーバと SSH クライアントの両方をサポートしているため，セキュア通信路を使用し，本装置から別の本装置へのログインやファイル転送を実現できます。本装置から別の本装置への接続例を次の図に示します。

図 11-5　本装置から別の本装置へ SSH を使用して接続する例



11.1.2 SSH の基本機能

(1) セキュアリモートログイン

SSH が提供するセキュア通信路をリモートログインに使用する機能です。セキュアリモートログインを使用すると，インターネット経由でも安全に，運用端末から SSH サーバへログインできます。また，通信内容を他者に見られないため，安全な運用管理を実現できます。

本装置の運用にセキュアリモートログインを使用することで, インターネット経由でも運用端末から本装置へ安全にログインし運用できます。

(2) セキュアコマンド実行

SSH が提供するセキュア通信路を使用して，サーバ上でコマンドを実行する機能です。ユーザ認証に公開鍵認証を使用した環境でセキュアコマンド実行を使用すると, リモート運用端末からログインやパスワード入力をしないで安全にコマンドを実行できます。

本装置の運用にセキュアコマンド実行を使用することで，ARP テーブルの確認や ping による疎通確認など，単純な，運用コマンドによる運用が容易になります。

なお，SSH クライアントからセキュアコマンド実行を使用して本装置上でコマンドを実行する場合，次に示す三つの注意点があります。

- SSH クライアント側で仮想端末を割り当てるように指定する必要があります。一般的な SSH クライアントの実装では，ssh コマンドの-t パラメータを指定することで仮想端末を割り当てます。本装置の運用コマンド ssh でも，-t パラメータによって仮想端末を割り当てます。
- 実行できるコマンドは，一般ユーザモードで実行できる運用コマンドだけです。装置管理者モードの運用コマンドや，コンフィグレーションコマンドは実行できません。
- 実行中にキー入力が必要な運用コマンドは実行できません。例えば，運用コマンド reload を実行すると，確認メッセージが出力されて(y/n)の入力を促されます。しかし，セキュアコマンド実行では，確認メッセージが出力されないで実行もされません。

  このようなコマンドについては，確認および入力が不要になるパラメータがある場合には，そのパラメータを指定することでセキュアコマンド実行ができます。

(3) セキュアコピー（SCP）

SSH が提供するセキュア通信路を使用して，コピー元ファイル名とコピー先ファイル名を指定し，クライアントとサーバ間でファイルを転送する機能です。コピー元にサーバ上のファイルを指定すると, サーバからクライアントへファイルをコピーします。コピー先にサーバ上のファイルを指定すると, クライアントからサーバへファイルをコピーします。

本装置の運用にセキュアコピーを使用することで, コンフィグレーションのバックアップなどを安全に実行できます。

(4) セキュア FTP（SFTP）

SSH が提供するセキュア通信路を使用して，FTP と同様の会話型インタフェースを使用し，クライアントとサーバ間でファイルを転送する機能です。ファイル転送のほかに, ファイル名を確認したりファイルを削除したりできます。

本装置の運用にセキュア FTP を使用することで，アップデート実施時のアップデートファイル取得などを安全に実行できます。

11.1.3　サポート機能

本装置がサポートするSSHサーバおよびSSHクライアントの役割，SSHプロトコルバージョン，SSH接続に使用できるプロトコルを次の表に示します。

表 11-1　SSHサーバ／クライアント・プロトコルバージョン・接続プロトコルサポート一覧

機能名		サポート有無
SSHサーバ		○
SSHクライアント		○
SSHプロトコルバージョン	バージョン1（SSHv1）	○
	バージョン2（SSHv2）	○
SSH接続に使用できるプロトコル	IPv4	○
	IPv6	○
	IPv4 VRF【SL-L3A】	○
	IPv6 VRF【SL-L3A】	○

（凡例）　○：サポート

SSHの基本機能とサポート状況を次の表に示します。

表 11-2　SSH基本機能サポート一覧

機能名	説明	サポート有無
セキュアリモートログイン	SSHを使用したリモートログイン	○
セキュアコマンド実行	SSHを使用したコマンド実行	○
セキュアコピー（SCP）	SSHを使用したファイルコピー	○
セキュアFTP（SFTP）	SSHを使用したファイル転送	SSHv1：× SSHv2：○
認証エージェント	認証エージェント機能	×
ポート転送	TCP転送機能	×
X11プロトコル自動転送	X11を自動転送する機能	×
データ圧縮	通信のデータを圧縮する機能	×

（凡例）　○：サポート　×：未サポート

SSHv1のセキュリティ機能の方式別サポート状況を次の表に示します。

表 11-3　SSHv1 セキュリティ機能の方式別サポート一覧

機能名	方式		サポート有無
ホスト認証	公開鍵認証	RSA	○
ユーザ認証	公開鍵認証	RSA	サーバ：○

機能名	方式		サポート有無
			クライアント：×
	パスワード認証		○
	RHOSTS 認証		×
	RHOSTS ＋ RSA 認証		×
暗号化	共通鍵暗号	3des-cbc，blowfish-cbc	○
	その他の方式		×

（凡例）　○：サポート　×：未サポート

SSHv2 のセキュリティ機能の方式別サポート状況を次の表に示します。

表 11-4　SSHv2 セキュリティ機能の方式別サポート一覧

機能名	方式		サポート有無
ホスト認証	公開鍵認証	ECDSA，RSA，DSA	○
	証明局証明書による公開鍵認証		×
	PGP 証明書による公開鍵認証		×
ユーザ認証	公開鍵認証	ECDSA，RSA，DSA	サーバ：○ クライアント：×
	証明局証明書による公開鍵認証		×
	PGP 証明書による公開鍵認証		×
	ホストベース認証		×
	パスワード認証		○
鍵交換	ecdh-sha2-nistp256，ecdh-sha2-nistp384，ecdh-sha2-nistp521，dh-group16-sha512，dh-group14-sha256，dh-group-ex-sha1，dh-group14-sha1，dh-group1-sha1		○
	その他の方式		×
共通鍵暗号	aes128-ctr，aes192-ctr，aes256-ctr，aes128-cbc，aes192-cbc，aes256-cbc，3des-cbc，blowfish，arcfour256，arcfour128，arcfour		○
	その他の方式		×
メッセージ認証コード	hmac-sha2-256，hmac-sha2-512，hmac-sha1，hmac-md5，hmac-sha1-96，hmac-md5-96		○
	その他の方式		×
認証付き暗号	aes128-gcm@openssh.com aes256-gcm@openssh.com		○
	その他の方式		×

（凡例）　○：サポート　×：未サポート

SSH サーバのログインセキュリティと RADIUS/TACACS+対応のサポート状況を次の表に示します。

表 11-5　SSH サーバのログインセキュリティ機能サポート一覧

機能名		サポート有無
同時にログインできるユーザ数の設定		○
リモート運用端末の IP アドレスによる制限		○
ログインメッセージ	ログイン前	SSHv1：× SSHv2：○
	ログイン後	○
RADIUS/TACACS+	認証	○
	コマンド承認	○
	アカウンティング	○

（凡例）　○：サポート　×：未サポート

11.1.4　SSH のセキュリティ機能

SSH には，セキュリティを確保するために暗号技術を使用する機能が五つあります。

1. ホスト認証
2. ユーザ認証
3. セッション鍵の共有
4. 暗号化
5. メッセージ認証（SSHv2 だけ）

以降，各機能について説明します。

(1)　ホスト認証

ホスト認証は，SSH クライアントが SSH サーバを認証する機能です。

各 SSH サーバは，それぞれ異なるホスト鍵ペアを保持しています。SSHv1 では，ホスト公開鍵を使用してクライアントからサーバへ公開鍵暗号で通信することによって，サーバを認証します。SSHv2 では，サーバがホスト秘密鍵でデジタル署名を作成し，クライアントがホスト公開鍵で署名を確認することによって，サーバを認証します。本装置がサポートするホスト鍵ペアの公開鍵アルゴリズムとサイズを次の表に示します。

表 11-6　本装置がサポートするホスト鍵ペアの公開鍵アルゴリズムとサイズ

SSH バージョン	公開鍵 アルゴリズム	鍵のサイズ	
		SSH サーバ	SSH クライアント
SSHv1	RSA	1024bit	1024bit～2048bit
SSHv2	ECDSA	521bit（nistp521）， 384bit（nistp384）， 256bit（nistp256）	521bit（nistp521）， 384bit（nistp384）， 256bit（nistp256）

SSH バージョン	公開鍵アルゴリズム	鍵のサイズ	
		SSH サーバ	SSH クライアント
	RSA	1024bit，2048bit，3072bit，4096bit	512bit～5120bit
	DSA	1024bit	512bit～1536bit

本装置の SSH サーバ機能では，デフォルトで SSHv1 用 RSA 1024bit と DSA 1024bit のホスト鍵ペアを生成します。デフォルト以外の鍵ペアを使用する場合や鍵ペアを生成し直す場合は，運用コマンド set ssh hostkey を使用してください。SSHv2 の不要なアルゴリズムの鍵ペアを削除する場合は，運用コマンド erase ssh hostkey を使用してください。なお，SSHv1 の RSA ホスト鍵ペアは削除できません。

SSH クライアントでは，過去に接続したサーバのホスト公開鍵を保持しています。SSH クライアントでは，SSH サーバへ初めて接続するときやサーバのホスト公開鍵が変更されたときに，公開鍵のフィンガープリント（ハッシュ値）を表示して，ユーザに正しい公開鍵かどうか確認を要求します。事前にユーザへ告知したサーバのホスト公開鍵のフィンガープリントと，ユーザが接続したときに表示されたフィンガープリントを比較することで，サーバのなりすましを防げます。

本装置の SSH サーバ機能のホスト公開鍵およびホスト公開鍵のフィンガープリントを確認するには，運用コマンド show ssh hostkey を使用してください。表示内容と表示形式を次の表に示します。

表 11-7　SSH サーバ機能のホスト公開鍵およびフィンガープリント表示形式

SSH バージョン	表示内容	表示形式
SSHv1	公開鍵	SSHv1 形式
	フィンガープリント	SECSH（MD5）形式（RFC4716）
	フィンガープリント	SHA256 形式
SSHv2	公開鍵	OpenSSH 形式
	フィンガープリント	SECSH（MD5）形式（RFC4716）
	フィンガープリント	SHA256 形式

本装置の SSH クライアント機能がサーバ初回接続時に表示する，フィンガープリントの表示形式を次の表に示します。

表 11-8　SSH クライアント機能の未知ホストフィンガープリント表示形式

SSH バージョン	表示内容	表示形式
SSHv1	フィンガープリント	SECSH（MD5）形式（RFC4716）
	フィンガープリント	SHA256 形式
SSHv2	フィンガープリント	SECSH（MD5）形式（RFC4716）
	フィンガープリント	SHA256 形式

(2)　ユーザ認証

ユーザ認証は，SSH サーバが SSH クライアントを認証する機能です。本装置では，ユーザ認証方式として次に示す二つの方式をサポートしています。

- 公開鍵認証
- パスワード認証

本装置の SSH サーバが使用するユーザ認証方式は，コンフィグレーションコマンド ip ssh authentication で設定できます。なお，本装置の SSH クライアントは，パスワード認証だけをサポートしています。

(a)　公開鍵認証

公開鍵アルゴリズムを使用してユーザを認証する機能です。各ユーザは，それぞれ鍵ペアを用意します。SSH サーバには，ユーザの公開鍵を設定しておきます。SSHv1 では，サーバから公開鍵暗号で通信することによってユーザを認証します。SSHv2 では，クライアントがユーザの秘密鍵でデジタル署名を作成し，サーバが署名を確認することでユーザを認証します。

本装置では，SSH サーバ機能だけが公開鍵認証をサポートして，SSH クライアント機能は公開鍵認証をサポートしません。本装置から別の本装置へ SSH で接続する場合，ユーザ認証方式に公開鍵認証を使用できない点に注意してください。

本装置の SSH サーバがユーザ認証でサポートする，公開鍵アルゴリズムと公開鍵のサイズを次の表に示します。

表 11-9　本装置の SSH サーバがサポートするユーザ公開鍵のアルゴリズムとサイズ

SSH バージョン	公開鍵アルゴリズム	ユーザ公開鍵のサイズ
SSHv1	RSA	512bit～2560bit
SSHv2	ECDSA	521bit（nistp521），384bit（nistp384），256bit（nistp256）
	RSA	512bit～5120bit
	DSA	512bit～1536bit

本装置の SSH サーバでは，ユーザ公開鍵の登録にコンフィグレーションコマンド ip ssh authkey を使用します。登録できる公開鍵の形式を次の表に示します。

表 11-10　登録できる公開鍵の形式

SSH バージョン	表示形式
SSHv1	SSHv1 形式の公開鍵ファイル
	SSHv1 形式の公開鍵を示す数字列
SSHv2	SECSH（RFC4716）形式の公開鍵ファイル
	OpenSSH 形式の公開鍵ファイル
	SECSH 形式または OpenSSH 形式の公開鍵を示す文字列

(b)　パスワード認証

SSH クライアントがユーザ名とパスワードを送信し，SSH サーバがサーバ内のユーザアカウント情報と照合するか，または RADIUS/TACACS+などによって認証サーバへユーザ名とパスワードが正しいかどうか問い合わせることで，ユーザ名とパスワードを確認します。SSH では，ユーザ認証情報は暗号化されるため，盗聴によってパスワードが漏洩する危険はありません。

本装置では，SSH サーバ機能および SSH クライアント機能のどちらもパスワード認証をサポートしています。ただし，本装置の SSH サーバでは，パスワードを設定していないユーザはパスワード認証ができません。本装置への SSH 接続のユーザ認証方式としてパスワード認証を使用する場合は，ユーザアカウントにパスワードを設定してください。

(3) セッション鍵の共有

セキュア通信路の暗号化やメッセージ認証に共通鍵として使用するセッション鍵を，サーバとクライアントで共有する機能です。SSHv1 では，クライアントがセッション鍵を作成し，ホスト認証時の RSA 公開鍵暗号によってクライアントからサーバへセッション鍵を送付します。SSHv2 では，鍵交換方式によってサーバとクライアントの両方に同じセッション鍵を生成します。

本装置では，SSHv2 サーバが使用する鍵交換方式を選択できます。鍵交換方式を選択するには，コンフィグレーションコマンド ip ssh key-exchange を使用してください。

(4) 暗号化

セキュア通信路を暗号化する機能です。暗号化には共通鍵暗号を使用しますが，SSHv2 では認証付き暗号も使用できます。

本装置では，コンフィグレーションコマンド ip ssh ciphers を設定することで，SSHv2 サーバの暗号化方式を制限できます。また，SSH クライアント機能の運用コマンドに-c パラメータを使用すると，SSH クライアント機能で使用する暗号化方式を指定できます。

(5) メッセージ認証

セキュア通信路のデータを認証する機能で，SSHv2 だけに存在します。メッセージ認証では，メッセージ認証コードを使用します。また，暗号化方式に認証付き暗号を使用した場合は，認証付き暗号でデータを認証します。

本装置では，コンフィグレーションコマンド ip ssh macs を設定することで，SSHv2 サーバのメッセージ認証コードを制限できます。また，SSHv2 クライアント機能の運用コマンドに-m パラメータを使用すると，SSHv2 クライアント機能が使用するメッセージ認証方式を指定できます。

11.1.5 SSH が使用する暗号技術

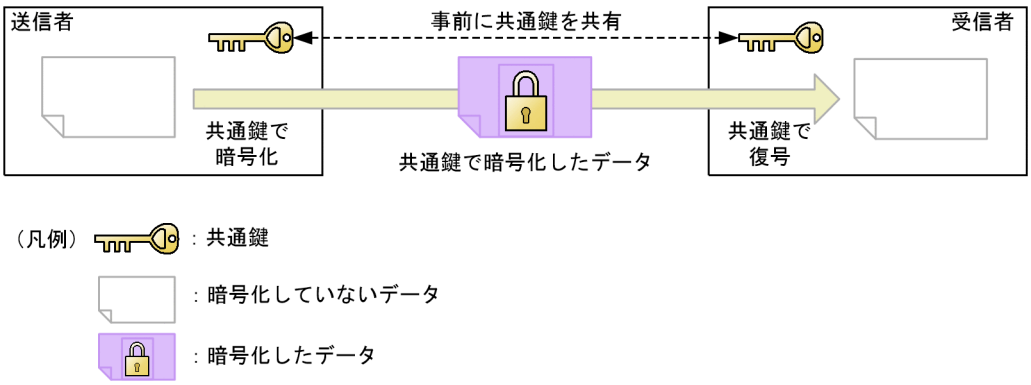
SSH では，次に示す暗号技術を使用して，セキュアな通信を実現します。

- 共通鍵暗号
- メッセージ認証コード
- 認証付き暗号
- 公開鍵アルゴリズム
- 鍵交換

(1) 共通鍵暗号

送信者と受信者で同じ鍵（共通鍵と呼ぶ）を使用します。共通鍵暗号は，送信者と受信者とで共通鍵を共有し，送信者はその鍵で暗号化し，受信者はその鍵で復号する技術です。共通鍵暗号による暗号化通信の例を次の図に示します。

図 11-6　共通鍵暗号による暗号化通信の例

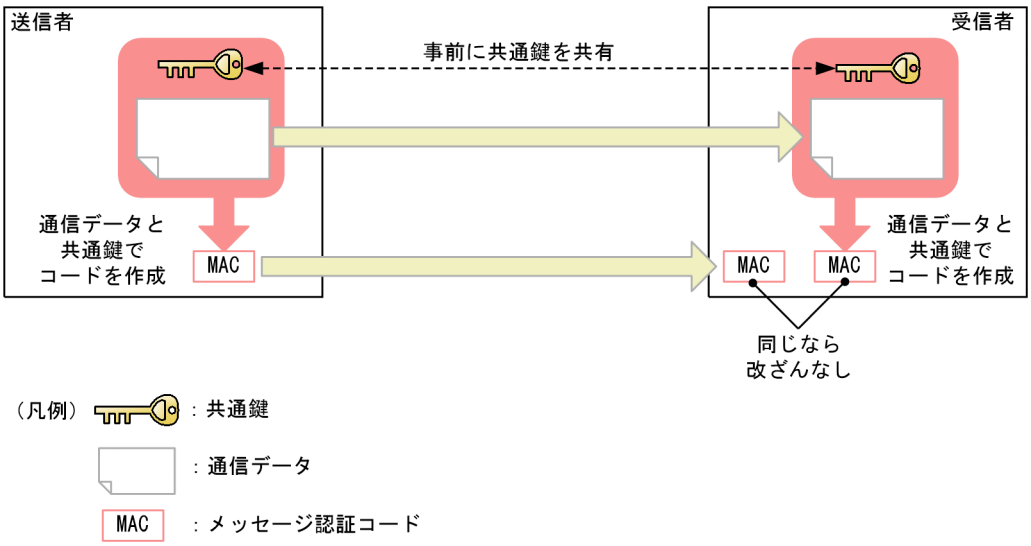


(2)　メッセージ認証コード

メッセージ認証コードは，共通鍵を使用して，送信者が送信した通信データが改ざんされていないことを確認する技術です。また，改ざんされていないことを確認するために使用する固定長のデータのことも，メッセージ認証コードと呼びます。

送信者は通信データと共通鍵を組み合わせてメッセージ認証コードを作成し，通信データと同時に送信します。受信者でも通信データと共通鍵を組み合わせてメッセージ認証コードを作成し，受信したメッセージ認証コードと比較します。比較した結果同じであれば，通信データが改ざんされてないことが確認できます。メッセージ認証コードによる改ざん確認の例を次の図に示します。

図 11-7　メッセージ認証コードによる改ざん確認の例



(3)　認証付き暗号

認証付き暗号は，共通鍵暗号とメッセージ認証コードを組み合わせた方式です。共通鍵を使用し，暗号とメッセージ認証を同時に実現します。

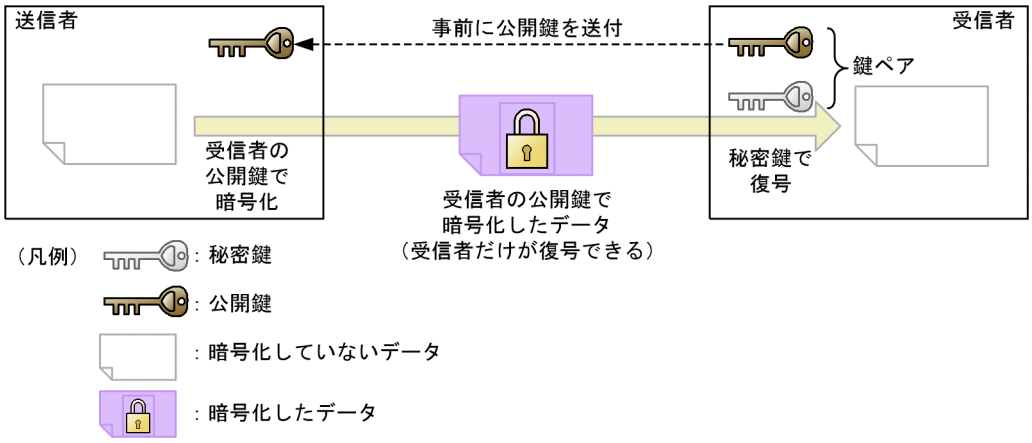
(4)　公開鍵アルゴリズム

公開鍵アルゴリズムは，二種類の鍵である公開鍵と秘密鍵を，ペアで使用するアルゴリズムです。ペアになる公開鍵と秘密鍵の組み合わせを鍵ペアと呼びます。

(a)　公開鍵暗号

公開鍵暗号は，公開鍵で暗号化し，秘密鍵で復号する暗号化技術です。受信者は鍵ペアを作成して，公開鍵だけを送信者へ送付します。送信者は，受信者の公開鍵でデータを暗号化して送信します。このように，秘密鍵を保持する受信者しか復号できない暗号化通信を実現します。公開鍵暗号による暗号化通信の例を次の図に示します。

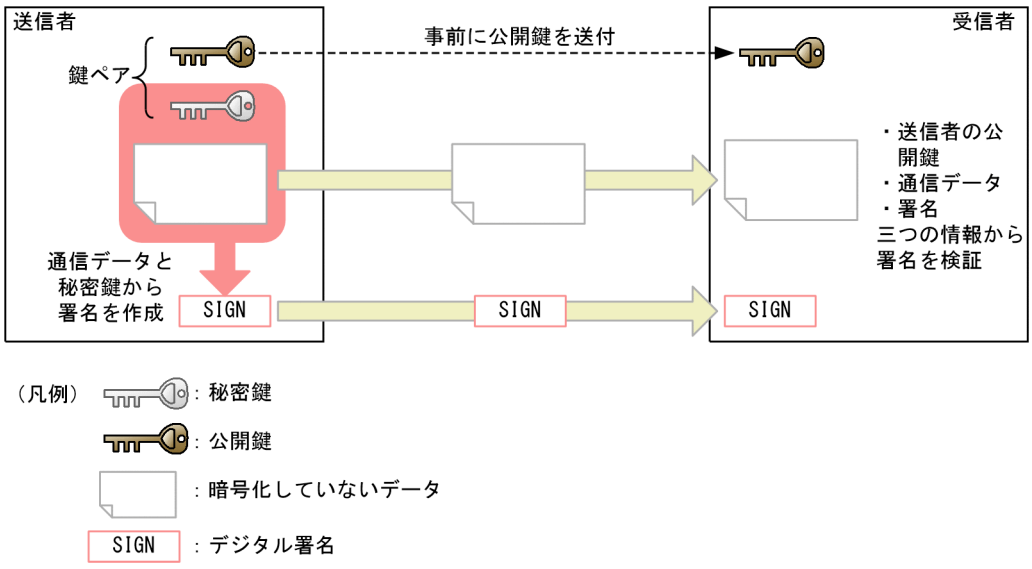
図 11-8　公開鍵暗号による暗号化通信の例



(b)　デジタル署名

デジタル署名は，通信データが改ざんされていないか，送信者が正しいかを確認する技術です。送信者は，あらかじめ公開鍵を受信者へ公開しておき，通信データと秘密鍵から署名を作成します。受信者は，通信データと署名と公開鍵から，署名が正しいことを確認します。署名が正しければ，通信データが改ざんされていないこと（通信データの認証），および送信者が秘密鍵の保有者であること（送信者の認証）が確認できます。デジタル署名の例を次の図に示します。

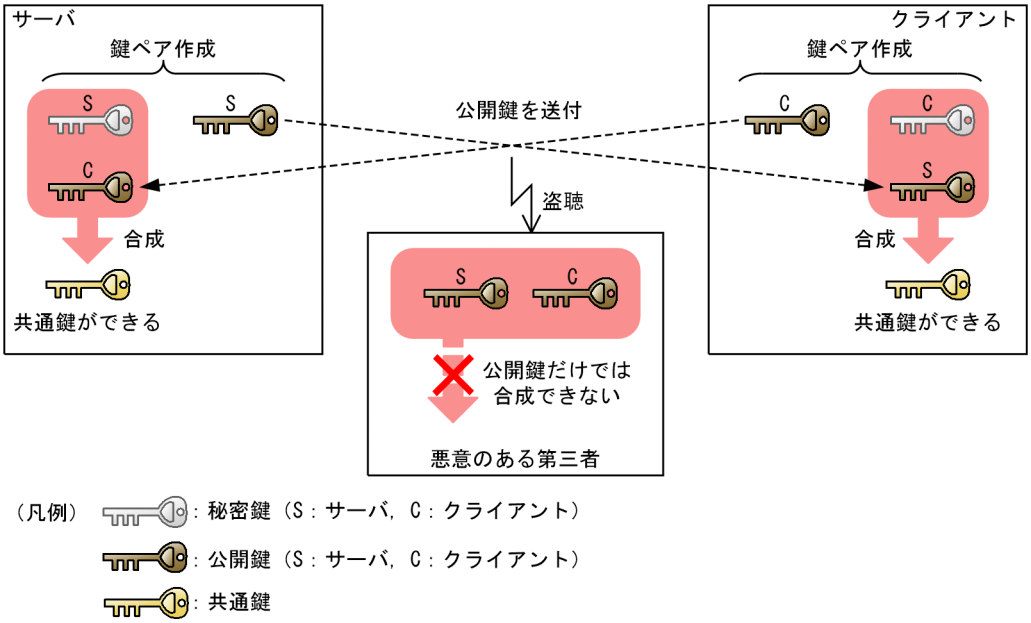
図 11-9　デジタル署名の例



(5)　鍵交換

鍵交換は，通信の両端が交換した情報を基に共通鍵を作成する方式です。サーバとクライアントは，それぞれ鍵ペアを生成し，互いに公開鍵を送付します。自装置の秘密鍵と対向装置の公開鍵を合成すると，サーバとクライアントで同じ共通鍵が生成されます。悪意ある第三者が盗聴してサーバとクライアントの公開鍵を入手しても，公開鍵だけでは共通鍵を作成できません。このため，サーバとクライアントの間で安全に共通鍵を共有できます。鍵交換の例を次の図に示します。

図 11-10　鍵交換の例



11.1.6　ログイン制御機能のサポート

(1)　リモート運用端末からのログインの許可および同時にログインできるユーザ数

本装置に対してセキュアリモートログインする場合やセキュアコマンド実行をする場合は，コンフィグレーションコマンド line vty を設定する必要があります。また，セキュアリモートログインとセキュアコマンド実行は，リモートログインのユーザ数としてカウントされ，ユーザ数の制限対象となります。

(2)　リモート運用端末の IP アドレスによる制限

リモート運用端末から本装置の SSH サーバへのアクセスは，リモート運用端末の IP アドレスによる制限対象となります。

(3)　ログインメッセージ表示

ログインバナーを設定すると，リモート運用端末から本装置へ SSH で接続した場合にも，ログイン前後にログインメッセージを表示します。

ログイン前のメッセージは，SSHv2 だけでサポートします。どの SSH 基本機能を利用する場合でも表示します。

ログイン後のメッセージは，SSHv1 と SSHv2 の両方でサポートします。なお，セキュアリモートログインの場合だけ表示し，セキュアコマンド実行，SCP，および SFTP の場合には表示しません。

11.1.7　RADIUS/TACACS+のサポート

本装置の SSH サーバは，RADIUS/TACACS+による認証，コマンド承認，およびアカウンティングをサポートしています。ただし，RADIUS/TACACS+によるログイン認証を使用できるのはパスワード認証だけです。詳細は，「10.2.2　RADIUS/TACACS+の適用機能および範囲」を参照してください。

11.1.8　SSH 使用時の注意事項

(1)　多国語 SSH クライアントの制限

日本語などの一部の多国語クライアントでは，ASCII 文字以外の文字（日本語など）でサーバへエラーメッセージを送付することがあります。

本装置の SSH サーバでログを表示する際，クライアントからのエラーメッセージを表示する部分では，送付された文字が ASCII 文字以外の場合に，ASCII 表示できる文字にエンコード変換されて表示します。

できるだけ，ASCII 文字でエラーメッセージを送付するクライアントを使用してください。

11.2　SSH サーバのコンフィグレーション

ここでは，SSH サーバ機能について説明します。なお，SSH クライアント機能はコンフィグレーションを設定する必要はありません。

11.2.1　コンフィグレーションコマンド一覧

SSH サーバのコンフィグレーションコマンド一覧を次の表に示します。

表 11-11　コンフィグレーションコマンド一覧

コマンド名	説明
ip ssh	SSH サーバを動作させます。
ip ssh authentication	SSH サーバのユーザ認証方式を制限します。
ip ssh authkey	SSH サーバで公開鍵認証に使用するユーザ公開鍵を登録します。
ip ssh ciphers	SSHv2 サーバで使用する暗号方式を制限します。
ip ssh key-exchange	SSHv2 サーバで使用する鍵交換方式を制限します。
ip ssh macs	SSHv2 サーバで使用するメッセージ認証コード方式を制限します。
ip ssh version	SSH サーバの SSH プロトコルバージョンを制限します。
transport input※1	リモート運用端末から本装置へのアクセスに使用できるプロトコルをを制限するために使用します。
ip access-group※2	リモート運用端末から本装置へのアクセスを，端末の IPv4 アドレスによって制限するために使用します。
ipv6 access-class※2	リモート運用端末から本装置へのアクセスを，端末の IPv6 アドレスによって制限するために使用します。

注※1

「コンフィグレーションコマンドレファレンス Vol.1」「2　運用端末接続」を参照してください。

注※2

「コンフィグレーションコマンドレファレンス Vol.1」「6　ログインセキュリティと RADIUS/TACACS+」を参照してください。

11.2.2　SSH サーバの基本設定（パスワード設定）

本装置の SSH サーバ機能を利用するために必要な設定を示します。ユーザ認証方式は，telnet と同じパスワード認証を使用します。

[設定のポイント]

SSH 接続に使用するユーザアカウントへのパスワードの設定例と，SSHv2 サーバを動作させる設定例を示します。セキュリティのため SSHv1 が不要な場合は，動作させる SSH のバージョンを SSHv2 に制限してください。

ログインユーザの作成時にパスワードを設定するように注意してください。パスワードを設定していないユーザは，SSH のパスワード認証でログインできないためです。ログインユーザの作成については，「10.1.3　ログインユーザの作成と削除」を参照してください。

SSH クライアントが本装置へ初めて接続するとき，SSH クライアントはホスト公開鍵のフィンガープリントを表示して正しいかどうか確認を要求します。本装置のホスト公開鍵とフィンガープリントの表示方法については，「11.3.2　ホスト公開鍵の確認」を参照してください。

[コマンドによる設定]

1. **# configure**
   (config)# ip ssh version 2
   SSH サーバが動作するバージョンを SSHv2 に制限します。
2. **(config)# ip ssh**
   SSH サーバの動作を開始させます。
3. **(config)# line vty 0 2**
   本装置へのリモートログインを許可します。この設定例では，ログインできるユーザ数を 3 に設定しています。

11.2.3　ユーザ認証に公開鍵認証を使用する設定

(1)　ユーザ公開鍵を転送する場合

クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録し，公開鍵認証をする設定例を示します。

[設定のポイント]

あらかじめ，クライアントでユーザ公開鍵ファイルを作成し，本装置へ転送しておいてください。ユーザ公開鍵の転送には ftp を使用できますが，よりセキュリティを確保できる SCP または SFTP を使用することをお勧めします。

ここでは SECSH 形式の SSHv2 DSA のユーザ公開鍵で説明していますが，SSHv2 RSA や ECDSA のユーザ公開鍵，OpenSSH 形式や SSHv1 形式のユーザ公開鍵も同様の方法で登録できます。

[コマンドによる設定]

1. **(config)# ip ssh authentication publickey**
   ユーザ認証方式として公開鍵認証だけを許可します。
2. **(config)# ip ssh authkey staff client-v2 load-key-file /usr/home/staff/id_dsa_1024_a.pub**
   ユーザ（staff）の SSHv2 のユーザ公開鍵を，あらかじめ転送したファイル（/usr/home/staff/id_dsa_1024_a.pub）から読み込みます。このとき，この鍵の名前（インデックス名）を client-v2 とします。コンフィグレーションには，ユーザ公開鍵の内容が設定されます。

[注意事項]

各ユーザのホームディレクトリ配下に，「.ssh」という名前のディレクトリを作成しないでください。さらに，「.ssh」ディレクトリ配下にファイルを転送，コピー，および生成しないでください。

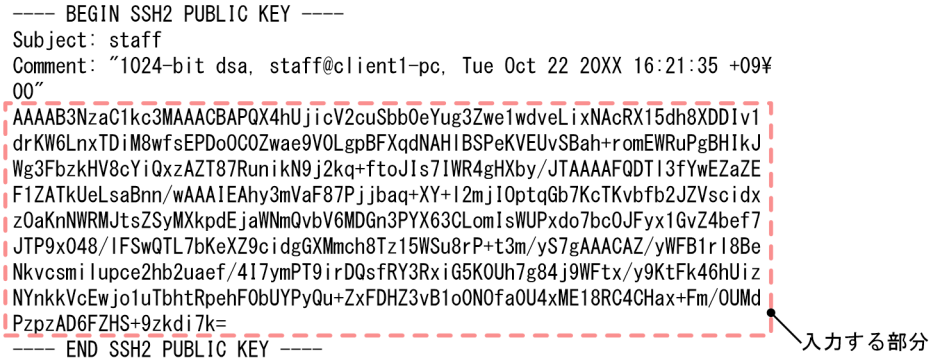
「.ssh」ディレクトリは，本装置の SSH サーバ機能が自動的に生成し，使用します。ユーザがファイルを置いた場合，削除されたり上書きされたりします。

(2)　SSHv2 ユーザ公開鍵（SECSH 形式）を直接入力する場合

公開鍵認証をするために, クライアントで作成したユーザ鍵ペアのうち, ユーザ公開鍵を本装置の SSH サーバへ登録します。

クライアントで，あらかじめ SECSH 形式のユーザ公開鍵を作成します。ip ssh authkey コマンドで SECSH 形式のユーザ公開鍵の内容を直接入力する場合は，ヘッダ（Comment:コメントなど），開始マーカ，終了マーカ，および改行コードを除いた，鍵の部分だけを入力してください。ユーザ公開鍵（SECSH 形式）の入力部分を次の図に示します。

図 11-11　SSHv2 ユーザ公開鍵（SECSH 形式）の入力部分



[設定のポイント]

この例では，ユーザ公開鍵ファイルの内容を ip ssh authkey コマンドで直接入力して，ユーザ公開鍵を登録します。

ここでは SECSH 形式の SSHv2 DSA のユーザ公開鍵で説明していますが，SSHv2 RSA や ECDSA のユーザ公開鍵も同様の方法で登録できます。

[コマンドによる設定]

1. **(config)# ip ssh authkey staff client-v2 "AAAAB3NzaC…S+9zkdi7k="**

   SSHv2 クライアントであらかじめ作成したユーザ（staff）のユーザ公開鍵（SECSH 形式）の内容を，途中で改行しないようにダブルクォート（"）で囲んで入力します。このとき，このユーザ公開鍵の名前（インデックス名）を client-v2 とします。

[注意事項]

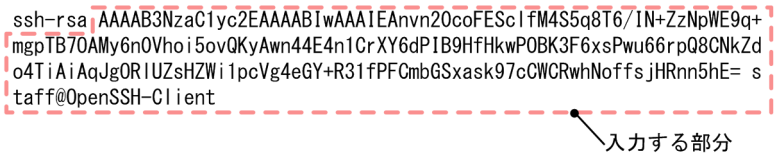
SECSH 形式のユーザ公開鍵には改行コードが含まれているため，すべての改行を取り除いて 1 行の形式にしてください。また，変換後のユーザ公開鍵の部分に空白を含めないでください。空白のあとは，コメントと見なされます。

(3)　SSHv2 ユーザ公開鍵（OpenSSH 鍵）を直接入力する場合

公開鍵認証をするために，クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録します。

クライアントで，あらかじめ OpenSSH 形式のユーザ公開鍵を作成します。ip ssh authkey コマンドで SECSH 形式のユーザ公開鍵の内容を直接入力する場合は，先頭にある「ssh-rsa」，「ecdsa-sha2-nistpXXX」，または「ssh-dss」を取り除いた部分を，改行コードを含めないでそのまま 1 行で入力してください。ユーザ公開鍵（OpenSSH 鍵）の入力部分を次の図に示します。

図 11-12　SSHv2 ユーザ公開鍵（OpenSSH 鍵）の入力部分



[設定のポイント]

この例では，ユーザ公開鍵ファイルの内容を ip ssh authkey コマンドで直接入力して，ユーザ公開鍵を登録します。

ここでは OpenSSH の SSHv2 RSA ユーザ公開鍵で説明していますが，SSHv2 DSA や ECDSA のユーザ公開鍵も同様の方法で登録できます。

[コマンドによる設定]

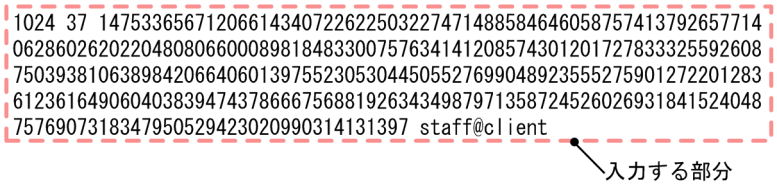
1. **(config)# ip ssh authkey staff client-O "AAAAB…n5hE= staff@OpenSSH-Client"**
   あらかじめ作成したユーザ（staff）の SSHv2 のユーザ公開鍵（OpenSSH 形式）を，途中で改行しないようにダブルクォート（"）で囲んで入力します。このとき，このユーザ公開鍵の名前（インデックス名）を client-O とします。

(4)　SSHv1 ユーザ公開鍵を直接入力する場合

公開鍵認証をするために，クライアントで作成したユーザ鍵ペアのうち，ユーザ公開鍵を本装置の SSH サーバへ登録します。

クライアントで，あらかじめ SSHv1 ユーザ公開鍵を作成します。ユーザ公開鍵の入力部分を次の図に示します。

図 11-13　SSHv1 ユーザ公開鍵の入力部分



[設定のポイント]

この例では，ユーザ公開鍵ファイルの内容を ip ssh authkey コマンドで直接入力して，ユーザ公開鍵を登録します。

[コマンドによる設定]

1. **(config)# ip ssh authkey staff client-v1 "1024 37 14753…31397 staff@client"**
   あらかじめ作成したユーザ（staff）の SSHv1 のユーザ公開鍵を，途中で改行しないようにダブルクォート（"）で囲んで入力します。このとき，このユーザ公開鍵の名前（インデックス名）を client-v1 とします。

11.2.4　SSHv2 サーバの暗号アルゴリズムの設定変更

SSHv2 のセキュリティ機能では，ホスト認証とユーザ認証のほかに，鍵交換，暗号化，メッセージ認証を使用します。本装置の SSHv2 サーバ機能では，鍵交換，暗号化，メッセージ認証についても，複数の種類のアルゴリズムをサポートしています。

[設定のポイント]

サポートしている複数のアルゴリズムのうちから，使用するアルゴリズムを設定します。

[コマンドによる設定]

1. **(config)# ip ssh key-exchange ecdh-sha2-nistp256 diffie-hellman-group14-sha256**

   SSHv2 サーバの鍵交換アルゴリズムとして，ecdh-sha2-nistp256 と diffie-hellman-group14-sha256 だけを使用するように設定します。

2. **(config)# ip ssh ciphers aes128-gcm@openssh.com aes128-ctr**

   SSHv2 サーバの暗号化アルゴリズムとして，認証付き暗号の aes128-gcm@openssh.com と，共通鍵暗号の aes128-ctr だけを使用するように設定します。

3. **(config)# ip ssh macs hmac-sha2-256 hmac-sha1**

   SSHv2 サーバのメッセージ認証コードアルゴリズムとして，hmac-sha2-256 と hmac-sha1 だけを使用するように設定します。

11.2.5　リモート運用端末からの SSH 接続を許可する IP アドレスの設定

リモート運用端末からのアクセスを許可する IPv4 アドレスおよび IPv6 アドレスを制限すると，SSH による接続も制限されます。アクセスを許可する IP アドレスの設定例については,「10.1.7　リモート運用端末からのログインを許可する IP アドレスの設定」および「10.1.10　VRF でのリモート運用端末からのログインを許可する IP アドレスの設定【SL-L3A】」を参照してください。

11.2.6　RADIUS/TACACS+機能と連携した SSH サーバの設定

RADIUS/TACACS+を設定すると，SSH サーバも RADIUS/TACACS+と連携して動作します。
RADIUS/TACACS+のコンフィグレーションについては，「10.3　RADIUS/TACACS+のコンフィグレーション」を参照してください。

11.2.7　VRF での SSH によるアクセスを許可する【SL-L3A】

[設定のポイント]

グローバルネットワークを含む全 VRF で，運用端末から本装置への SSH プロトコルによるリモートアクセスを許可する場合の SSH サーバの設定例を示します。

[コマンドによる設定]

1. **(config)# line vty 0 2**

   (config-line)# transport input vrf all ssh

   本装置にログインできるユーザ数を 3 に設定します。また，グローバルネットワークを含む全 VRF で，リモート運用端末から SSH プロトコルによるアクセスだけを許可します。

11.3 SSH サーバのオペレーション

11.3.1 運用コマンド一覧

SSH サーバ機能の運用コマンド一覧を次に示します。

表 11-12 運用コマンド一覧

コマンド名	説明
show ssh hostkey	ホスト公開鍵とフィンガープリントを表示します。
set ssh hostkey	ホスト鍵ペアを変更します。
erase ssh hostkey	SSH ホスト鍵ペアを削除します。
show ssh logging	SSH サーバのトレースログを表示します。
clear ssh logging	SSH サーバのトレースログを消去します。

11.3.2 ホスト公開鍵の確認

SSH クライアントが SSH サーバを確認できるように，各 SSH サーバは異なるホスト鍵ペアを保持しています。SSH クライアント側では，SSH サーバに初めて接続する場合や，ホスト公開鍵が変更された場合に，そのサーバのフィンガープリントを確認するようにメッセージが表示されます。このとき，あらかじめ接続先サーバのフィンガープリント（またはホスト公開鍵）を入手しておき，接続時に目視確認することでより安全に接続できます。

show ssh hostkey コマンドで，SSHv1/SSHv2 のホスト公開鍵およびそのフィンガープリントが確認できます。

図 11-14 ホスト公開鍵の表示

```
> show ssh hostkey
Date 20XX/01/20 12:00:00 UTC
******* SSHv1 Hostkey *******
1024 65537 14698797177375959661209963212352629087681324221885617869300690227975
2499641505633273
74294515778228277627736937005824220192838922145093952246943786354524785835232009819519418410439
05657066855796690911797058967562169284131198788610748307323233604943076115695684771646338245359
75566336906750637684297547763208749 1024-bit rsa1 hostkey

Fingerprint for key:
SHA256:gblxC3SCNJsZfjaV5BC6rcckTR+B/hYYTEcBEQO00m8
MD5:c9:d5:c0:4f:1b:2e:ff:b7:2e:9d:c3:66:ed:93:d3:4e

******* SSHv2 DSA Hostkey *******
ssh-dss AAAAB3NzaC1kc3MAAACBAJenC0V9Xr8ahylD8fqpiAIYGwpjoRqDosb9udd/bDkxicU5YAhwsKktXvh5lPI+GDL
0JVB5hHOVmVCH45PAcoAx+xrEvL2wjoghhLVzDbTfyCCtehxvfcsVxoJSBhGggtWTmllytogGvE3us2vCgEybau8qIpUy+B
iA7ONunIDpAAAAFQDz1v9c2U8Eh5xNCApzCFL2ez48gwAAAIAOeAgtPewuIHY1Q3z00SawBa2xWrLxly4WcFrzfAja9GIRp
/+s3iJLu/6UZ5nyMyjSF10KAZUzFSG+HteGE/pLB1c+r4B2okzZVH1R7tnst/LAoDg3fQObTF74+j7cGMIwgE0i1E8hciHq
9NmQ9RBe2uBxsej8crzXDTpljfP/gQAAAIB3IWnKpTSvI4Rs49ItzGY+SS5DfkSy+BKB1VFB1xoUr/DYFpT4Q4kA3RTuPFx
pjElEIIUP5/+WET/iJSBizyfpwM/lairBhWtSNyOcjeWLD9eYVhw1HqexjQLl8BvTFQtICWWvsviYgNGUGfwTH0RZ6B5HKK
O5IVs6bh2VVHoq2A== 1024-bit dsa hostkey
```

```
Fingerprint for key:
SHA256:EH9axeEZO+hj5qzBRqx4fgyncb/J5BN4DffD/my9tN8
MD5:21:b9:aa:78:66:df:02:67:01:48:86:88:cb:31:c4:da

******* SSHv2 RSA Hostkey *******
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDQ0re6puJtq2gqvyZwzWVqlJgxPuXo7EphTgysp4a
v+LaGYdiU2jYoQ66
Eo4759z4fZQ/yHtXJicaDMvIz3iNbBQTr01x4F/5m1oR5UJS7XHfhqc5pGNLKglEaIZo8dJkKOo72xI
1lHERY11ICobKshhW
HpGP95WmrRIdxBGUDZKBIk8iW0CeS5duMksrL9O0LMLf1+NXkELmJBT/npMkHiZHBPJcKn1kPRiq5X8
igO3THLKeYcPUzOP
OkUAUrIDT42s8oJG2FkwO6CIewQcGK9zkCcqKPyFyZahDI8OvwZ05o7VOQb3/sLNiFZfQlRqoGxpiGv
NZae76Hb6kS3+cOJ
+Yyu/Tbz5kKK0Bz70dxb+4DqClV7yYfquiTdues6hOO8+KAUttNf/w3PNSyjFUFyRxcEDENvxDDq11/
gA78VXWitre1ZMin
9ybsSEZGzIS7OzDd0I5/AosKcYNWGkLRrBdGFcB5mJ/9haTALMOWsyxbF3RjXMvcCWVUpxbGKuqs= 3
072-bit rsa host
key

Fingerprint for key:
SHA256:lnaICZdvjFnmZoRCum+XblmhEmcilZhq15w4W8R3vOg
MD5:81:48:0e:52:a6:7f:64:d8:29:57:e8:fb:4b:34:bb:a0

******* SSHv2 ECDSA Hostkey *******
ecdsa-sha2-nistp384 AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAABhBNLBG8R
hJwOBU8Z/e+c1wz6
qwZP+IHXM6iUINja2EMOi947VPI8/CA7ZK2INnUW7lXaqkeu6LihUN68wwz8Gisgx9sAPthB3VkNqBE
svKjxk2aSC1/neyg
mD5H/5Wo9Q6A== 384-bit ecdsa hostkey

Fingerprint for key:
SHA256:rnuan5fOrHpNP8IVbZgKNt+t+x/EVTxWKF3tF2CMRA0
MD5:69:5f:70:c3:a0:09:91:e8:70:12:fe:c5:52:21:fe:19

>
```

11.3.3 ホスト鍵ペアの変更

本装置ではホスト鍵ペアは初回の装置起動時に自動生成されるため，SSH サーバとして運用するに当たり，意図してホスト鍵ペアを生成する必要はありません。

本装置を別の用途へ転用する場合は，SSH のホスト鍵ペアを変更することをお勧めします。SSH のホスト鍵ペアを変更する場合は，set ssh hostkey コマンドを実行します。

また，SSHv2 のホスト鍵としてデフォルトの DSA 1024bit 以外のホスト鍵ペアを使用する場合にも，set ssh hostkey コマンドを実行します。デフォルトの DSA ホスト鍵ペアを使用しない場合には，erase ssh hostkey コマンドを実行して DSA ホスト鍵ペアを削除してください。

図 11-15 ホスト鍵ペア（SSHv1 RSA と SSHv2 DSA）の変更

```
> enable
# set ssh hostkey

WARNING!!
Would you wish to generate SSHv1 RSA and SSHv2 DSA hostkeys? (y/n): y
Generating public/private rsa1 key pair.
The key fingerprint is:
SHA256:nxeQpjv+aQOQXo6Wqg0Q9BklwosYJ7K3kkUCXgXwwBg
MD5:a6:7e:c8:3c:0a:d7:ae:e8:78:58:66:8e:9e:be:e8:3a

Generating public/private dsa key pair.
The key fingerprint is:
SHA256:O+GPxz5QtjOD8wCEK2HhhHDkjocEY3IEIeF+ltuwJU4
MD5:e8:f8:71:1b:31:ba:c0:21:ee:ce:88:0f:78:e4:d7:09

The hostkey generation is completed.
#
```

図 11-16 SSHv2 ECDSA ホスト鍵ペアの作成および SSHv2 DSA ホスト鍵ペアの削除

```
> enable
# set ssh hostkey ecdsa 521

WARNING!!
Would you wish to generate the SSHv2 ECDSA hostkey? (y/n): y
Generating public/private ecdsa key pair.
The key fingerprint is:
SHA256:jTz5rFJlA6oIrYrWKb6EueKvHcyCQXA1jYU1N+orgqg
MD5:0c:c1:c4:8a:38:b0:46:66:2e:ff:f2:44:3c:57:88:4e

The hostkey generation is completed.
# erase ssh hostkey dsa

WARNING!!
Would you wish to erase the SSHv2 DSA hostkey? (y/n): y

The hostkey was erased successfully.
#
```

11.4　SSH クライアントのオペレーション

11.4.1　運用コマンド一覧

SSH クライアント機能の運用コマンド一覧を次に示します。

表 11-13　運用コマンド一覧

コマンド名	説明
ssh	セキュアリモートログイン機能およびセキュアコマンド実行機能を提供します。
sftp	セキュア FTP によってファイルを転送します。
scp	セキュアコピーによってファイルを転送します。

11.4.2　セキュアリモートログイン

ssh コマンドで，SSH サーバへログインできます。ただし，本装置の SSH クライアント機能はパスワード認証だけをサポートしているため，SSH サーバ側でパスワード認証を有効にする必要があります。

ssh，scp，および sftp コマンドで SSH サーバと最初に接続する場合，接続したサーバが意図したサーバであることを確認するために，接続した SSH サーバのホスト公開鍵のフィンガープリントを表示します。事前に接続先サーバのフィンガープリントを入手し，コマンドが表示したフィンガープリントと比較確認することで，より安全に接続できます。

本装置から SSH サーバへ接続する例を次の図に示します。

図 11-17　本装置から SSH サーバへの接続例

```
> ssh -c aes128-ctr -m hmac-sha2-256 staff@192.168.1.1
…1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
DSA key fingerprint is SHA256:EH9axeEZO+hj5qzBRqx4fgyncb/J5BN4DffD/my9tN8.
DSA key fingerprint is MD5:21:b9:aa:78:66:df:02:67:01:48:86:88:cb:31:c4:da.
Are you sure you want to continue connecting (yes/no)? yes
…2
Warning: Permanently added '192.168.1.1' (DSA) to the list of known hosts.
staff@192.168.1.1's password: ******
…3
```

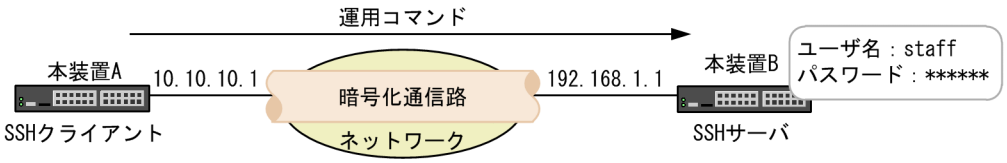
1. SSH サーバ 192.168.1.1 へ，ユーザ staff として接続します。その際，共通鍵暗号方式として aes128-ctr を，メッセージ認証コード方式として hmac-sha2-256 を使用します。
2. SSH サーバに最初に接続する場合は，クライアントユーザのホスト公開鍵データベースにホスト公開鍵が登録されていないため，登録の確認メッセージが表示されます。フィンガープリント（鍵の指紋）を確認し，接続しようとしている SSH サーバの正しいホスト公開鍵であることを確認してください。確認できたら，yes と入力することで，データベースに登録し接続を続けます。

   なお，一度ユーザのホスト公開鍵データベースにホスト公開鍵を登録すると，次回の接続時にはフィンガープリントの確認はありません。
3. staff のパスワードを入力してログインします。

11.4.3　セキュアコマンド実行

ssh コマンドにパラメータとしてコマンドを指定することで，SSH サーバ上で運用コマンドを実行できます。本装置 A から本装置 B 上でコマンドを実行する構成例を次の図に示します。

図 11-18　本装置 A から本装置 B 上でコマンドを実行する構成例



本装置 A から本装置 B 上で運用コマンドを実行する例を次の図に示します。本装置上で運用コマンドを実行するときには，強制的に仮想端末を割り当てるように，クライアント側でパラメータを指定する必要があります。一般的な SSH の実装では，ssh コマンドの-t パラメータを指定します。次の図に示す例でも，本装置 A の運用コマンド ssh に-t パラメータを指定します。

図 11-19　本装置 A から本装置 B 上で運用コマンドを実行する例

```
> ssh -t staff@192.168.1.1 ping 10.10.10.1
staff@192.168.1.1's password: ******
PING 10.10.10.1 (10.10.10.1): 56 data bytes
64 bytes from 10.10.10.1: icmp_seq=0 ttl=255 time=0.108 ms
64 bytes from 10.10.10.1: icmp_seq=1 ttl=255 time=0.113 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=255 time=0.116 ms
^C
--- 10.10.10.1 PING statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max = 0.108/0.114/0.118 ms
Connection to 192.168.1.1 closed.
>
```

11.4.4　セキュアコピー

scp コマンドによって，本装置と SSH サーバとの間でファイルを転送できます。ftp とは異なり通信路には SSH を利用しているため，ユーザ名，パスワード，およびファイルは暗号化されて送信され，外部に漏洩したり改ざんされたりしません。

本装置の scp コマンドによって，IPv4 で接続して SSH サーバへコンフィグレーションファイルを転送する例を次の図に示します。

図 11-20　IPv4 で接続してセキュアコピーで本装置からファイルを転送する例

```
> scp config.txt staff@192.168.1.1:/home/staff/config/
…1
staff@192.168.1.1's password: ******
…2
config.txt                                    100% 4062     4.0KB/s   00:00
…3
>
```

1. SSH サーバ 192.168.1.1 へユーザ staff として接続し，あらかじめホームディレクトリに保存したコンフィグレーションファイル config.txt を，/home/staff/config/配下へ転送します。
2. staff のパスワードを入力します（SSH サーバに 2 回目以降接続するときは，クライアントユーザのホスト公開鍵データベースにホスト公開鍵が登録されているため，ホスト公開鍵の確認メッセージは表示されません）。
3. ファイルが転送されます。

本装置の scp コマンドによって，IPv6 で接続して SSH サーバから本装置へコンフィグレーションファイルを転送する例を次の図に示します。

図 11-21　IPv6 で接続してセキュアコピーで本装置へファイルを転送する例

```
> scp staff@[2001:db8::1]:/home/staff/config/config.txt .
…1
```

```
staff@2001:db8::1's password: ******
…2
config.txt                                    100% 4062     4.0KB/s   00:00
…3
>
```

1. SSH サーバ 2001:db8::1 へユーザ staff として接続し，サーバの/home/staff/config/配下にあるコンフィグレーションファイル config.txt を，本装置のカレントディレクトリへ転送します。IPv6 アドレスは角括弧[ ]で囲んで入力します。
2. staff のパスワードを入力します。
3. ファイルが転送されます。

11.4.5　セキュア FTP

sftp コマンドによって，ftp と同様のインタフェースでファイルを転送できます。ftp とは異なり通信路には SSHv2 を利用しているため，ユーザ名，パスワード，およびファイルは暗号化されて送信され，外部に漏洩しません。

本装置の sftp コマンドによって，SSH サーバへ接続し，本装置のコンフィグレーションファイルを転送する例を次の図に示します。

図 11-22　セキュア FTP でファイルを転送する例

```
> sftp staff@2001:db8::1
…1
Connecting to 2001:db8::1...
staff@2001:db8::1's password:******
…2
sftp> cd /home/staff/
…3
sftp> mkdir config
…4
sftp> cd config
…5
sftp> put config.txt
…6
Uploading config.txt to /home/staff/config/config.txt
config.txt                                    100% 4062     4.0KB/s   00:00
sftp> quit
…7
>
```

1. sftp コマンドを使用して，SSH サーバ 2001:db8::1 へユーザ staff として接続します。
2. staff のパスワードを入力します（SSH サーバに 2 回目以降接続するときは，クライアントユーザのホスト公開鍵データベースにホスト公開鍵が登録されているため，ホスト公開鍵の確認メッセージは表示されません）。
3. /home/staff へディレクトリを移動します。
4. config ディレクトリを作成します。
5. /home/staff/config へディレクトリを移動します。
6. config.txt をサーバへ転送します。
7. サーバから切断します。

12 時刻の設定と NTP

この章では，時刻の設定と NTP について説明します。

12.1　時刻の設定と NTP 確認

時刻は，本装置の初期導入時に設定してください。時刻は，本装置のログ情報や各種ファイルの作成時刻などに付与される情報です。運用開始時には正確な時刻を本装置に設定してください。運用コマンド set clock で時刻を設定できます。

また，このほかに，NTP プロトコルを使用して，ネットワーク上の NTP サーバと時刻の同期を行えます。本装置は RFC1305 NTP バージョン 3 に準拠しています。なお，本装置は NTP モード 6 およびモード 7 のパケットには応答しません。

12.1.1　コンフィグレーションコマンド・運用コマンド一覧

時刻設定および NTP に関するコンフィグレーションコマンド一覧を次の表に示します。

表 12-1　コンフィグレーションコマンド一覧

コマンド名	説明
clock timezone	タイムゾーンを設定します。
ntp access-group	アクセスグループを作成し，IPv4 アドレスフィルタによって，NTP サービスへのアクセスを許可または制限できます。
ntp authenticate	NTP 認証機能を有効化します。
ntp authentication-key	認証鍵を設定します。
ntp broadcast	インタフェースごとにブロードキャストで NTP パケットを送信し，ほかの装置が本装置に同期化するように設定します。
ntp broadcast client	接続したサブネット上の装置からの NTP ブロードキャストメッセージを受け付けるための設定をします。
ntp broadcastdelay	NTP ブロードキャストサーバと本装置間で予測される遅延時間を指定します。
ntp master	ローカルタイムサーバの設定を指定します。
ntp peer	NTP サーバに，シンメトリック・アクティブ／パッシブモードを構成します。
ntp server	NTP サーバをクライアントモードに設定し，クライアントサーバモードを構成します。
ntp trusted-key	ほかの装置と同期化する場合に，セキュリティ目的の認証をするように鍵番号を設定します。

時刻設定および NTP に関する運用コマンド一覧を次の表に示します。

表 12-2　運用コマンド一覧

コマンド名	説明
set clock	日付，時刻を表示，設定します。
show clock	現在設定されている日付，時刻を表示します。
show ntp associations	接続されている NTP サーバの動作状態を表示します。
restart ntp	ローカル NTP サーバを再起動します。

12.1.2　システムクロックの設定

[設定のポイント]

日本時間として時刻を設定する場合は，あらかじめコンフィグレーションコマンド clock timezone でタイムゾーンに JST，UTC からのオフセットを+9 に設定する必要があります。

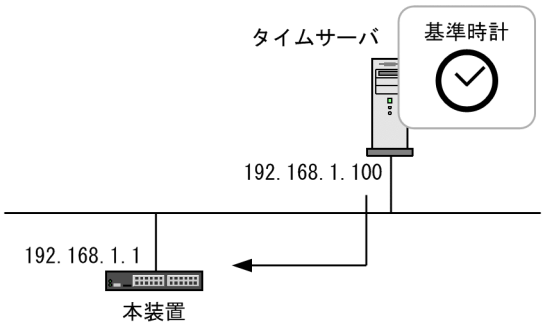
[コマンドによる設定]

1. **(config)# clock timezone JST +9**
   日本時間として，タイムゾーンに JST，UTC からのオフセットを+9 に設定します。
2. **(config)# save**
   (config)# exit
   保存し，コンフィグレーションモードから装置管理者モードに移行します。
3. **# set clock 0506221530**
   Wed Jun 22 15:30:00 2005 JST
   2005 年 6 月 22 日 15 時 30 分に時刻を設定します。

12.1.3　NTP によるタイムサーバと時刻同期の設定

NTP 機能を用いて，本装置の時刻をタイムサーバの時刻に同期させます。

図 12-1　NTP 構成図（タイムサーバへの時刻の同期）



[設定のポイント]

タイムサーバを複数設定した場合の本装置の同期先は，ntp server コマンドの prefer パラメータを指定されたタイムサーバが選択されます。また，prefer パラメータが指定されなかった場合は，タイムサーバの stratum 値が最も小さいタイムサーバが選択され，すべての stratum 値が同じ場合の同期先は任意となります。

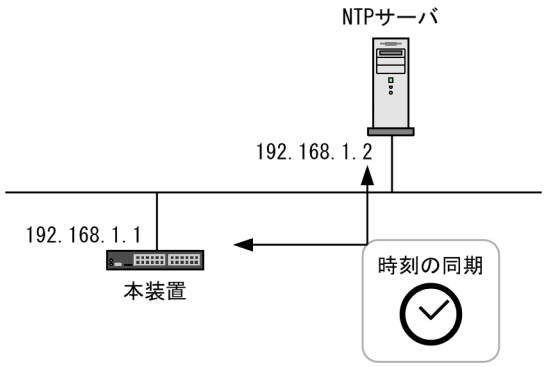
[コマンドによる設定]

1. **(config)# ntp server 192.168.1.100**
   IP アドレス 192.168.1.100 のタイムサーバに本装置を同期させます。

12.1.4　NTP サーバとの時刻同期の設定

NTP 機能を用いて，本装置の時刻と NTP サーバの時刻をお互いに調整しながら，同期させます。

図 12-2　NTP 構成図（NTP サーバとの時刻の同期）



[設定のポイント]

複数の NTP サーバと本装置を同期する場合には，ntp peer コマンドを用いて複数設定する必要があります。

NTP サーバを複数設定した場合の本装置の同期先は，ntp peer コマンドの prefer パラメータを指定された NTP サーバが選択されます。また，prefer パラメータが指定されなかった場合は，NTP サーバの stratum 値が最も小さい NTP サーバが選択され，すべての stratum 値が同じ場合の同期先は任意となります。

[コマンドによる設定]

1. **(config)# ntp peer 192.168.1.2**
   IP アドレス 192.168.1.2 の NTP サーバとの間を peer 関係として設定します。

12.1.5　NTP 認証の設定

[設定のポイント]

NTP 機能でほかの装置と時刻の同期を行う場合に，セキュリティ目的の認証を行います。

[コマンドによる設定]

1. **(config)# ntp authenticate**
   NTP 認証機能を有効化します。
2. **(config)# ntp authentication-key 1 md5 NtP#001**
   NTP 認証鍵として，鍵番号 1 に「NtP#001」を設定します。
3. **(config)# ntp trusted-key 1**
   NTP 認証に使用する鍵番号 1 を指定します。

12.1.6　VRF での NTP による時刻同期の設定【SL-L3A】

NTP 機能を用いて，VRF に存在する NTP サーバや NTP クライアントに対して時刻を同期させる設定をします。

[設定のポイント]

NTP 機能を用いて，本装置の時刻を任意の VRF に存在する NTP サーバに同期させます。また，本装置の時刻が NTP サーバに同期している場合，グローバルネットワークを含む全 VRF に存在する複数の NTP クライアントに本装置の時刻を配布できます。

同期の対象にする NTP サーバと NTP クライアントの VRF が異なる場合，NTP クライアントに対して，本装置の参照先ホストをローカルタイムサーバとして通知します。

[コマンドによる設定]

1. **(config)# ntp server vrf 10 192.168.1.100**
   VRF 10 に存在する IP アドレス 192.168.1.100 の NTP サーバに，本装置の時刻を同期させます。構成はクライアントサーバモードです。
2. **(config)# ntp peer vrf 10 192.168.1.100**
   VRF 10 に存在する IP アドレス 192.168.1.100 の NTP サーバと本装置の時刻を同期させます。構成はシンメトリック・アクティブ／パッシブモードです。
3. **(config)# ntp broadcast client**
   NTP ブロードキャストメッセージで本装置の時刻を同期させます。グローバルネットワークを含む全 VRF 上のサブネットを対象にして，NTP サーバからの NTP ブロードキャストメッセージを受信します。
4. **(config)# interface vlan 100**
   (config-if)# vrf forwarding 20
   (config-if)# ip address 192.168.10.1 255.255.255.0
   (config-if)# ntp broadcast
   VRF が指定されたインタフェースに対して NTP ブロードキャストの設定をします。本装置の時刻が NTP サーバに同期すると，VRF20，IPv4 アドレス 192.168.10.0，サブネット 255.255.255.0 のネットワークに NTP ブロードキャストパケットを送信します。

12.1.7　時刻変更に関する注意事項

- 本装置で収集している統計情報の CPU 使用率は，時刻が変更された時点で 0 にクリアされます。

12.1.8　時刻の確認

本装置に設定されている時刻情報は，運用コマンド show clock で確認できます。次の図に例を示します。

図 12-3　時刻の確認

```
> show clock
Wed Jun 22 15:30:00 20XX JST
>
```

また，NTP プロトコルを使用して，ネットワーク上の NTP サーバと時刻の同期を行っている場合，運用コマンド show ntp associations で動作状態を確認できます。次の図に例を示します。

図 12-4　NTP サーバの動作状態の確認

```
> show ntp associations
Date 20XX/01/23 12:00:00 UTC
  remote         refid      st t when poll reach   delay   offset    disp
==============================================================================
*timesvr    192.168.1.100    3 u    1   64  377     0.89   -2.827    0.27
>
```

13 ホスト名と DNS

この章では，ホスト名と DNS の解説と操作方法について説明します。

13.1　解説

本装置では, ネットワーク上の装置を識別するためにホスト名情報を設定できます。設定したホスト名情報は, 本装置のログ情報などのコンフィグレーションを設定するときにネットワーク上のほかの装置を指定する名称として使用できます。本装置で使用するホスト名情報は次に示す方法で設定できます。

- コンフィグレーションコマンド ip host／ipv6 host で個別に指定する方法
- DNS リゾルバ機能を使用してネットワーク上の DNS サーバに問い合わせる方法

コンフィグレーションコマンド ip host／ipv6 host を使用して設定する場合は，使用するホスト名ごとに IP アドレスとの対応を明示的に設定する必要があります。DNS リゾルバを使用する場合は，ネットワーク上の DNS サーバで管理されている名称を問い合わせて参照するため，本装置で参照するホスト名ごとに IP アドレスを設定する必要がなくなります。

コンフィグレーションコマンド ip host／ipv6 host と DNS リゾルバ機能の両方が設定されている場合, ip host／ipv6 host で設定されているホスト名が優先されます。コンフィグレーションコマンド ip host／ipv6 host または DNS リゾルバ機能を使用して，IPv4 と IPv6 で同一のホスト名を設定している場合，IPv4 が優先されます。

本装置の DNS リゾルバ機能は RFC1034 および RFC1035 に準拠しています。

13.2　コンフィグレーション

13.2.1　コンフィグレーションコマンド一覧

ホスト名・DNS に関するコンフィグレーションコマンド一覧を次の表に示します。

表 13-1　コンフィグレーションコマンド一覧

コマンド名	説明
ip domain lookup	DNS リゾルバ機能を無効化または有効化します。
ip domain name	DNS リゾルバで使用するドメイン名を設定します。
ip host	IPv4 アドレスに付与するホスト名情報を設定します。
ip name-server	DNS リゾルバが参照するネームサーバを設定します。
ipv6 host	IPv6 アドレスに付与するホスト名情報を設定します。

13.2.2　ホスト名の設定

(1)　IPv4 アドレスに付与するホスト名の設定

[設定のポイント]

IPv4 アドレスに付与するホスト名を設定します。

[コマンドによる設定]

1. **(config)# ip host WORKPC1 192.168.0.1**
   IPv4 アドレス 192.168.0.1 の装置にホスト名 WORKPC1 を設定します。

(2)　IPv6 アドレスに付与するホスト名の設定

[設定のポイント]

IPv6 アドレスに付与するホスト名を設定します。

[コマンドによる設定]

1. **(config)# ipv6 host WORKPC2 3ffe:501:811:ff45::87ff:fec0:3890**
   IPv6 アドレス 3ffe:501:811:ff45::87ff:fec0:3890 の装置にホスト名 WORKPC2 を設定します。

13.2.3　DNS の設定

(1)　DNS リゾルバの設定

[設定のポイント]

DNS リゾルバで使用するドメイン名および DNS リゾルバが参照するネームサーバを設定します。
DNS リゾルバ機能はデフォルトで有効なため，ネームサーバが設定された時点から機能します。

[コマンドによる設定]

1. **(config)# ip domain name router.example.com**

ドメイン名を router.example.com に設定します。

2. **(config)# ip name-server 192.168.0.1**
   ネームサーバを 192.168.0.1 に設定します。

(2) DNS リゾルバ機能の無効化

[設定のポイント]

DNS リゾルバ機能を無効にします。

[コマンドによる設定]

1. **(config)# no ip domain lookup**
   DNS リゾルバ機能を無効にします。

14 装置の管理

この章では，本装置を導入した際，および本装置を管理する上で必要な作業について説明します。

14.1　装置の状態確認，および運用形態に関する設定

14.1.1　コンフィグレーション・運用コマンド一覧

装置を管理する上で必要なコンフィグレーションコマンド，および運用コマンド一覧の一覧を次の表に示します。

表 14-1　コンフィグレーションコマンド一覧

コマンド名	説明
power redundancy-mode	電源を冗長構成で運用する際の異常を検知し，重度障害と判定します。
swrt_multicast_table	IPv4/IPv6 マルチキャストと IGMP/MLD snooping を同時に使用する場合に設定します。
swrt_table_resource	装置のルーティングのテーブルエントリ数の配分パターンを設定します。
system fan mode	ファンの運転モードを設定します。
system interface hundredgigabitethernet※1	指定したインタフェースを 100GBASE-R で動作可能にして，対応するインタフェースを無効にします。
system l2-table mode	レイヤ 2 ハードウェアテーブルの検索方式を設定します。
system recovery	no system recovery コマンドを設定すると，装置の障害が発生した際に，障害部位の復旧処理を行わないようにし，障害発生以降に障害部位を停止したままにします。
system temperature-warning-level	装置の入気温度が指定温度以上になった場合に運用メッセージを出力します。
switch provision※2	本装置のモデルを設定します。

注※1

100GBASE-R を使用する場合の設定と無効になるインタフェースについては，「14.5　100GBASE-R の設定と 100BASE-TX/1000BASE-T/10GBASE-T ポートの排他変更」を参照してください。

注※2

「コンフィグレーションコマンドレファレンス Vol.1」「4　スタック」を参照してください。

表 14-2　運用コマンド一覧（ソフトウェアバージョンと装置状態の確認）

コマンド名	説明
show version	本装置に組み込まれているソフトウェアや実装されているボードの情報を表示します。
show system	本装置の運用状態を表示します。
clear control-counter	障害による装置再起動回数および部分再起動回数を 0 クリアします。
show environment	筐体のファン，電源，温度の状態と累積稼働時間を表示します。
reload	装置を再起動します。
show tech-support	テクニカルサポートで必要となるハードウェアおよびソフトウェアの状態に関する情報を表示します。

コマンド名	説明
show tcpdump	本装置に対して送受信されるパケットをモニタします。

表 14-3　運用コマンド一覧（装置内メモリと MC の確認）

コマンド名	説明
show flash	装置内メモリの使用状態を表示します。
show mc	MC の形式と使用状態を表示します。
format mc	MC を本装置用のフォーマットで初期化します。

表 14-4　運用コマンド一覧（ログ情報の確認）

コマンド名	説明
show logging	本装置で収集しているログを表示します。
clear logging	本装置で収集しているログを消去します。
show logging console	set logging console コマンドで設定された内容を表示します。
set logging console	運用メッセージの画面表示をイベントレベル単位で制御します。

表 14-5　運用コマンド一覧（リソース情報とダンプ情報の確認）

コマンド名	説明
show cpu	CPU 使用率を表示します。
show processes	装置の現在実行中のプロセスの情報を表示します。
show memory	装置の現在使用中のメモリの情報を表示します。
df	ディスクの空き領域を表示します。
du	ディレクトリ内のファイル容量を表示します。
erase dumpfile	ダンプファイルを消去します。
show dumpfile	ダンプファイル格納ディレクトリに格納されているダンプファイルの一覧を表示します。

14.1.2　ソフトウェアバージョンの確認

運用コマンド show version で本装置に組み込まれているソフトウェアの情報を確認できます。次の図に例を示します。

図 14-1　ソフトウェア情報の確認

```
> show version software
Date 20XX/04/01 02:54:45 UTC
S/W: OS-L3M Ver. 12.0
>
```

14.1.3 装置の状態確認

運用コマンド show system で装置の動作状態や実装メモリ量などを確認できます。次の図に例を示します。

図 14-2 装置の状態確認

```
> show system
Date 20XX/01/16 17:53:12 UTC
System: AX3660S-48XT4QW, OS-L3M (SL-L3A-001) Ver. 12.1.D
Node : Name=
    Contact=
    Locate=
    Elapsed time : 00:45:03
    LED Brightness mode : normal
    Machine ID : 0012.e23e.b20f
    Power redundancy-mode : check is not executed
    Power slot 1 : active PS-M(AC)
        Fan  : active No = Fan1(1)  Speed = --------, Direction = F-to-R
        PS   : active
    Power slot 2 : notconnect
    Fan slot : active FAN-M
        Fan  : active No = Fan3(1) , Fan3(2) , Fan3(3) , Fan3(4)
               Speed = normal , Direction = F-to-R
        Lamp : ALM LED=light off
    Main board : active
        Boot : 20XX/01/16 17:08:19 , operation reboot
        Fatal restart : CPU 0 times ,  SW 0 times
        Lamp : Power LED=green , Status LED1=green
        Board : CPU=AMD GX-420 2000MHz , Memory=4,194,304KB(4096MB)
        Management port: active up
             100BASE-TX full(auto) 0012.e23e.b20f
        Temperature : normal(26degree)
        Flash :
                  user area   config area     dump area    area total
            used  238,599KB          99KB           0KB     238,698KB
            free  229,857KB     116,963KB     131,008KB     477,828KB
            total 468,456KB     117,062KB     131,008KB     716,526KB
        MC  : enabled
            Manufacture ID : 00000030
            24,077KB used
            971,008KB free
            995,085KB total
        System interface hundredgigabitethernet :
            disable (10G)  : 0/21-22,37-44
            enable  (100G) : 0/49,51-52
    Device resources
        Current selected swrt_table_resource : l3switch-2
        Current selected swrt_multicast_table : Off
        Current selected unicast multipath number: 4
        Current selected port-channel load-balance-all-port: Off
        IP routing entry :
            Unicast : current number=98 , max number=8093
            Multicast : current number=0 , max number=2048
            ARP : current number=2 , max number=15360
        IPv6 routing entry :
            Unicast : current number=34 , max number=3007
            Multicast : current number=0 , max number=1024
            NDP : current number=2 , max number=15360
        Multipath table entry : current number=0 , max number=512
        MAC-Address table entry : current number=1014 , max number=81920
        VXLAN Layer2 Nexthop entry : current number=0 , max number=0
        System Layer2 Table Mode : mode=0
        Flow detection mode : layer3-mirror-5
          Used resources for filter inbound(Used/Max)
                    MAC      IPv4      IPv6
                    n/a    0/1024    2/1024
          Used resources for QoS(Used/Max)
                    MAC      IPv4      IPv6
                    n/a    0/ 512       n/a
          Used resources for UPC(Used/Max)
                    MAC      IPv4      IPv6
```

```
                n/a    0/ 512       n/a
          Used resources for Mirror inbound(Used/Max)
                MAC      IPv4      IPv6
              2/ 512    3/ 512    0/ 512
          Used resources for TCP/UDP port detection pattern
            Resources(Used/Max):  1/32
              Destination Port   Used
                100-200        :       -/  -/mirror
        Flow detection out mode : layer3-2-out
          Used resources for filter outbound(Used/Max)
                MAC      IPv4      IPv6
              0/ 256    0/ 256    0/ 256
        Flow action change
            cos                : enable
            arp discard class  : enable
            arp reply cos      : enable
>
```

運用コマンド show environment でファン，電源，温度の状態，累積稼働時間を確認できます。ファンの運転モードはコンフィグレーションコマンド system fan mode で設定できます。次の図に例を示します。

図 14-3 装置の環境状態確認

```
> show environment
Date 20XX/12/10 10:00:00 UTC
Power slot 1 : PS-M(AC)
Power slot 2 : PS-M(AC)
Fan slot     : FAN-M

Fan environment
    Power slot 1 : Fan1(1) = active
                   Speed = --------
    Power slot 2 : Fan2(1) = active
                   Speed = --------
    Fan slot     : Fan3(1) = active
                   Fan3(2) = active
                   Fan3(3) = active
                   Fan3(4) = active
                   Speed = normal
    Fan mode     : 1 (silent)

Power environment
    Power slot 1 : active
    Power slot 2 : active

Temperature environment
    Main  :  30 degrees C
    Warning level : normal

Accumulated running time
    Main         :  total    : 365 days and 18 hours.
                    critical : 10 days and 8 hours.
    Power slot 1 :  total    : 365 days and 18 hours.
                    critical : 10 days and 8 hours.
    Power slot 2 :  total    : 365 days and 18 hours.
                    critical : 10 days and 8 hours.
    Fan slot     :  total    : 365 days and 18 hours.
                    critical : 10 days and 8 hours.
>
```

運用コマンド show environment の temperature-logging パラメータで温度履歴情報を確認できます。次の図に例を示します。

図 14-4 温度履歴情報の確認

```
> show environment temperature-logging
Date 20XX/12/10 20:00:00 UTC
Date         0:00  6:00 12:00 18:00
20XX/12/10      -     -  26.0  24.0
20XX/12/09   22.2  24.9  26.0  24.0
20XX/12/08   24.0  23.5  26.0  24.0
20XX/12/07   21.0     -  26.0  24.0
```

```
20XX/12/06   25.6     -  26.0  24.0
20XX/12/05   21.8  25.1  26.0  24.0
20XX/12/04   24.3  24.2  26.0
>
```

14.1.4　装置内メモリの確認

運用コマンド show flash で装置内メモリ上のファイルシステムの使用状況を確認できます。もし，使用量が合計容量の 95%を超える場合は，「トラブルシューティングガイド」を参照して対応してください。次の図に例を示します。

図 14–5　Flash 容量の確認

```
> show flash
Date 20XX/06/21 17:53:11 UTC
Flash :
          user area   config area     dump area    area total
    used  121,161kB        289kB          0kB     121,450kB
    free   14,619kB     75,117kB      65,390kB     155,126kB
    total 135,780kB     75,406kB      65,390kB     276,576kB
>
```

14.1.5　電源固定式モデルでの電源の重度障害判定の設定

電源固定式モデルでは，コンフィグレーションコマンド power redundancy-mode を設定することで，片方の電源だけに給電している場合や電源が停止する障害が発生した場合に，重度障害の発生と判定し，イベントレベル 8 の運用メッセージを表示して ST1 LED を赤点滅させます。

[設定のポイント]

両方の電源を使用する場合は，コンフィグレーションコマンド power redundancy-mode を設定してください。ただし，運用上，片方の電源だけを使用する場合は，重度障害の発生と誤判断するため，power redundancy-mode コマンドを設定しないでください。

[コマンドによる設定]

1. **(config)# power redundancy-mode redundancy-check**

   コンフィグレーションモードで，電源で異常を検知した場合に重度障害と判定するように設定します。

14.1.6　運用メッセージの出力抑止と確認

装置の状態が変化した場合，本装置は動作情報や障害情報などを運用メッセージとしてコンソールやリモート運用端末に表示します。例えば，回線が障害状態から回復した場合は回線が回復したメッセージを，回線が障害になって運用を停止した場合は回線が障害になったメッセージを表示します。運用メッセージの詳細は，「メッセージ・ログレファレンス」「1　運用メッセージ」を参照してください。

運用端末に出力される運用メッセージは，運用コマンド set logging console を使用することでイベントレベル単位で出力を抑止できます。また，その抑止内容については，運用コマンド show logging console で確認できます。イベントレベルが E5 以下の運用メッセージの運用端末への出力抑止の設定例を次に示します。

図 14–6　運用メッセージの出力抑止の設定例

```
> set logging console disable E5
> show logging console
  System message mode : E5
>
```

注意

多数の運用メッセージが連続して発生した際は，コンソールやリモート運用端末上には一部しか表示しませんので，運用コマンド show logging で確認してください。

14.1.7　運用ログ情報の確認

運用メッセージは運用端末に出力するほか，運用ログとして装置内に保存します。この情報で装置の運用状態や障害の発生を管理できます。

運用ログは装置運用中に発生した事象（イベント）を発生順に記録したログ情報で，運用メッセージと同様の内容が格納されます。運用ログとして格納する情報には次に示すものがあります。

- オペレータの操作および応答メッセージ
- 運用メッセージ

種別ログは装置内で発生した障害や警告についての運用ログ情報をメッセージ ID ごとに分類した上で，同事象が最初に発生した日時および最後に発生した日時と累積回数をまとめた情報です。

これらのログは装置内にテキスト形式で格納されており，運用コマンド show logging で確認できます。また，grep を使用してパターン文字列の指定を実施することで，特定のログ情報だけを表示することもできます。例えば，障害に関するログは show logging | grep EVT や show logging | grep ERR の実行でまとめて表示できます。障害に関するログの表示例を次の図に示します。

図 14–7　障害に関するログ表示

```
> show logging | grep EVT
     :
（途中省略）
     :
EVT 08/10 20:39:38 01S E3 SOFTWARE 00005002 1001:000000000000 Login operator
from LOGHOST1 (ttyp1).
EVT 08/10 20:41:43 01S E3 SOFTWARE 00005003 1001:000000000000 Logout operator
from LOGHOST1 (ttyp1).
     :
（以下省略）
     :
>
```

14.1.8　ルーティングテーブルのエントリ数の配分パターンの設定

本装置では，装置の適用形態に合わせ，ルーティングテーブルのエントリ数の配分パターンを変更することができます。配分パターンはコンフィグレーションコマンド swrt_table_resource のパラメータ l3switch-1，l3switch-2，l3switch-3，または l3switch-4 で指定します。l3switch-1 は IPv4 モード，l3switch-2 は IPv4/IPv6 モード，l3switch-3 は IPv6 ユニキャスト優先モード，l3switch-4 は L2 優先モードでエントリ数の配分パターンを設定できます。

なお，ルーティングテーブルのエントリ数については，「表 3–1　最大装置エントリ数」を参照してください。

初期状態は l3switch-1 で，IPv4 のルーティングにリソースを割り当てる IPv4 モードの配分パターンになっています。IPv6 のルーティングを併用する場合は，設定を変更してください。

なお，配分パターンとテーブルのエントリ数に関する情報は，運用コマンド show system で確認できます。

[設定のポイント]

本設定の変更を有効にするには，本装置の再起動が必要となるため，初期導入時に設定することをお勧めします。

[コマンドによる設定]

1. **(config)# swrt_table_resource l3switch-2**
   コンフィグレーションモードで，テーブルエントリ数の配分パターンを l3switch-2 に設定します。
2. **(config)# save**
   (config)# exit
   保存して，コンフィグレーションモードから装置管理者モードに移行します。
3. **# reload**
   本装置を再起動します。

14.1.9 IPv4/IPv6 マルチキャストと IGMP/MLD snooping 同時使用時の設定

本装置では，コンフィグレーションコマンド swrt_multicast_table を設定することで，IPv4/IPv6 マルチキャストと IGMP/MLD snooping を同時に使用できます。

なお，swrt_multicast_table の設定情報は，運用コマンド show system で確認できます。

[設定のポイント]

初期状態では swrt_multicast_table は設定されていません。swrt_multicast_table を設定したあと，有効にするには本装置の再起動が必要となるため，初期導入時に設定することをお勧めします。

[コマンドによる設定]

1. **(config)# swrt_multicast_table**
   コンフィグレーションモードで，swrt_multicast_table を設定します。
2. **(config)# save**
   (config)# exit
   保存して，コンフィグレーションモードから装置管理者モードに移行します。
3. **# reload**
   本装置を再起動します。

14.1.10 モデルに応じたコンフィグレーション

本装置には，装置のモデルを設定するコンフィグレーションコマンド switch provision があります。

自装置のモデルは自動で設定されます。変更および削除できません。

スタックで動作させる場合は，スタックを構成する前に自装置以外のメンバスイッチに対してモデルを設定しておく必要があります。

なお，switch provision の設定情報は，運用コマンド show running-config で確認できます。

図 14–8 switch provision の設定情報の確認

```
# show running-config
#default configuration file for AX3660S-48TX4QW
```

```
!
switch 1 provision 3660-48xt4qw
!
   :
   :
#
```

14.2　運用情報のバックアップ・リストア

装置障害または交換時の運用情報の復旧手順を示します。

次に示す「14.2.2　backup/restore コマンドを用いる手順」を実施してください。すべてを手作業で復旧することもできますが，取り扱う情報が複数にわたるため管理が複雑になり，また，完全に復旧できないため，お勧めしません。

14.2.1　運用コマンド一覧

バックアップ・リストアに使用する運用コマンド一覧を次の表に示します。

表 14-6　運用コマンド一覧

コマンド名	説明
backup	稼働中のソフトウェアおよび装置の情報を MC またはリモートの ftp サーバに保存します。
restore	MC およびリモートの ftp サーバに保存している装置情報を本装置に復旧します。

14.2.2　backup/restore コマンドを用いる手順

(1)　情報のバックアップ

装置が正常に稼働しているときに，backup コマンドを用いてバックアップを作成しておきます。backup コマンドは，装置の稼働に必要な次の情報を一つのファイルにまとめて，MC または外部の FTP サーバに保存します。

これらの情報に変更があった場合，backup コマンドによるバックアップの作成をお勧めします。

- ソフトウェアを稼働中のバージョンにアップデートするためのファイル
- ソフトウェアライセンスおよびオプションライセンス
- 電源運用モード
- スタートアップコンフィグレーション
- ユーザアカウント／パスワード
- SSH サーバのホスト鍵ペア
- 内蔵 Web 認証 DB
- Web 認証画面
- Web 認証のサーバ証明書・秘密鍵・中間 CA 証明書
- 内蔵 MAC 認証 DB
- IPv6 DHCP サーバの本装置 DUID
- スタック情報ファイル
- インストール済みのスクリプトファイル

backup コマンドでは次に示す情報は保存されないので注意してください。

- show logging コマンドで表示される運用ログ情報など

- 装置内に保存されているダンプファイルなどの障害情報
- ユーザアカウントごとに設けられるホームディレクトリにユーザが作成および保存したファイル

(2)　情報のリストア

backup コマンドで作成されたバックアップファイルから情報を復旧する場合，restore コマンドを使用します。

restore コマンドを実行すると，バックアップファイル内に保存されているソフトウェアアップデート用ファイルを使用して装置のソフトウェアをアップデートします。このアップデート作業後, 装置は自動的に再起動します。再起動後，復旧された環境になります。

なお，restore コマンドを実行するときは，次の点に注意してください。

- restore コマンドで情報を復旧する場合は，リストア対象の装置と同じモデル名称の装置で作成したバックアップファイルを使用してください。

  装置のモデル名称は，show version コマンドで表示される Model で確認してください。
- バックアップファイル作成時のソフトウェアバージョンが，リストア対象の装置に適していることを確認してください。
- 装置に設定されたユーザアカウントと，バックアップファイルに含まれるユーザアカウントが同じ（ユーザ名およびユーザの追加／削除順序が同じ）になるようにしてください。ユーザアカウントが異なる場合，リストア後にファイルが操作できなくなります。

14.3　障害時の復旧

本装置では運用中に障害が発生した場合は自動的に復旧処理を行います。障害部位に応じて復旧処理を局所化して行い，復旧処理による影響範囲を狭めることによって，正常運用部分が中断しないようにします。

14.3.1　障害部位と復旧内容

障害発生時，障害の内容によって復旧内容が異なります。障害部位と復旧内容を次の表に示します。

表 14-7　障害部位と復旧内容

障害部位	装置の対応	復旧内容	影響範囲
ポートで検出した障害	該当するポートの自動復旧を 6 回／1 時間行います。自動復旧の回数が 6 回のときに障害が発生すると停止します。※ただし，初回の障害発生から 1 時間以上運用すると，自動復旧の回数を初期化します。	該当するポートの再初期化を行います。	該当するポートを介する通信が中断されます。
メインボード障害（CPU）	自動復旧を 6 回まで行います。自動復旧の回数が 6 回のときに障害が発生すると停止します。ただし，復旧後 1 時間以上運用すると，自動復旧の回数を初期化します。	該当するメインボードの再初期化を行います。 6 回目の自動復旧の場合は，ランニングコンフィグレーションを初期化かつ VLAN の状態を disable に設定して起動します。	装置内の全ポートを介する通信が中断されます。
メインボード障害（SW）	自動復旧を 6 回／1 時間行います。自動復旧の回数が 6 回のときに障害が発生すると停止します。※ただし，初回の障害発生から 1 時間以上運用すると，自動復旧の回数を初期化します。	該当するスイッチングプロセッサの再初期化を行います。	装置内の全ポートを介する通信が中断されます。
電源障害（PS）	装置の運用に必要な電力が供給されなくなると停止します。なお，電源機構が冗長化されている場合は停止しません。	装置を停止します。なお，電源機構が冗長化されている場合は停止しません。	装置内全ポートを介する通信が中断されます。なお，電源機構が二重化されている場合は通信の中断はありません。
ファン障害	残りのファンを高速にします。	自動復旧はありません。電源機構またはファンユニットを交換して下さい。	ファンが高速回転しますが通信に影響はありません。

注※　コンフィグレーションコマンド no system recovery で復旧処理を行わない設定をしている場合には，自動復旧を行いません。

14.4　内蔵フラッシュメモリへ保存時の注意事項

本装置はソフトウェア，コンフィグレーション，ログ情報など，装置情報の保存先として，内蔵フラッシュメモリを使用しています。

内蔵フラッシュメモリはデバイスの一般的な特性上，書き換えられる回数に上限があります。その回数を超えて書き換えた場合，内蔵フラッシュメモリは故障するおそれがあります。

本装置の内蔵フラッシュメモリへの書き込み契機は，コンフィグレーションを保存したとき，および装置に対して一部の運用コマンドを実行したときです。これらの操作を 30 分周期で継続した場合，6 年程度で書き込み上限値に達することがあります。

(1)　コンフィグレーションコマンド

内蔵フラッシュメモリへの書き込み契機になる主なコンフィグレーションコマンドを，次に示します。

- save（write）
- ip dhcp snooping database url flash

(2)　運用コマンド

内蔵フラッシュメモリへの書き込み契機になる主な運用コマンドを，次の表に示します。

表 14-8　内蔵フラッシュメモリへの書き込み契機になる主な運用コマンド

分類	運用コマンド
運用端末とリモート操作	set terminal pager※，set exec-timeout※
コンフィグレーションとファイルの操作	copy，cp，rm，delete，undelete，squeeze，erase configuration
スタック	set switch，dump stack
ログインセキュリティと RADIUS/TACACS+	adduser，rmuser，password，clear password，dump protocols accounting
ソフトウェアバージョンと装置状態の確認	show tcpdump（writefile パラメータ指定時），restore
ソフトウェアの管理	ppupdate，set license，erase license
ログ	clear logging
VXLAN	dump protocols overlay
Web 認証	commit web-authentication，set web-authentication html-files，clear web-authentication html-files
MAC 認証	commit mac-authentication
ポリシーベースルーティング	dump policy，dump protocols track-object
DHCP サーバ機能	dump protocols dhcp
IPv4 マルチキャストルーティングプロトコル	dump protocols ipv4-multicast，erase protocol-dump ipv4-multicast

分類	運用コマンド
IPv4・IPv6 ルーティングプロトコル共通	dump protocols unicast，erase protocol-dump unicast
IPv6 DHCP リレー	dump protocols ipv6-dhcp relay
IPv6 DHCP サーバ機能	dump protocols ipv6-dhcp server
IPv6 マルチキャストルーティングプロトコル	dump protocols ipv6-multicast，erase protocol-dump ipv6-multicast
BFD	dump protocols bfd

注※　運用コマンド adduser で no-flash パラメータを指定したユーザアカウントは，対象外です。

14.5　100GBASE-R の設定と 100BASE-TX/1000BASE-T/10GBASE-T ポートの排他変更

この設定の対象は，IP8800/S3660-48XT4QW だけです。

QSFP28/QSFP+共用ポートであるポート 49～52 の工場出荷時（デフォルト）の設定は 40GBASE-R です。100GBASE-R の設定がなく，すべての 100BASE-TX/1000BASE-T/10GBASE-T ポートは有効です。

QSFP28/QSFP+共用ポートを 100GBASE-R で使用する場合，100BASE-TX/1000BASE-T/10GBASE-T ポートのポート 17～24 およびポート 37～44 の該当するポートが無効になります。100GBASE-R を使用するポート番号と無効になる 100BASE-TX/1000BASE-T/10GBASE-T ポートの対応を次の表に示します。

表 14–9　100GBASE-R を使用するポート番号と無効になる 100BASE-TX/1000BASE-T/10GBASE-T ポートの対応

100GBASE-R を使用するポート番号（QSFP28/QSFP+共用ポート）	無効になるポート番号（100BASE-TX/1000BASE-T/10GBASE-T ポート）
100GBASE-R の設定なし	なし
49 または 50 のどちらか一方	21，22
49 および 50 の両方	17，18，19，20，21，22，23，24
51 または 52 のどちらか一方	41，42
51 および 52 の両方	37，38，39，40，41，42，43，44

(1)　QSFP28/QSFP+共用ポートを 100GBASE-R で使用する設定

QSFP28/QSFP+共用ポートを 100GBASE-R に設定します。コンフィグレーションの設定後に装置を再起動すると，指定したポートは 100GBASE-R で動作できます。また，対応する 100BASE-TX/1000BASE-T/10GBASE-T ポートの interface tengigabitethernet およびその配下のコンフィグレーションは削除されます。

[設定のポイント]

この例では，QSFP28/QSFP+共用ポートのポート 50 を 100GBASE-R に設定していないという前提で，QSFP28/QSFP+共用ポートのポート 49 を 100GBASE-R に設定します。設定後，対応する 100BASE-TX/1000BASE-T/10GBASE-T ポートのポート 21～22 は無効になります。

[コマンドによる設定]

1. **(config)# system interface hundredgigabitethernet 1/0/49 enable**
   After this command execute, please save configuration editing now in startup-config, and please reboot a device.
   Do you wish to continue ? (y/n):
   ポート 49（QSFP28/QSFP+共用ポート）を 100GBASE-R に設定します。コンフィグレーションの変更確認メッセージに対して y を入力します。
2. **(config)# save**
   (config)# exit

コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。

3. **# reload**

本装置を再起動します。

再起動後，ポート 49 は 100GBASE-R で動作できます。また，100BASE-TX/1000BASE-T/10GBASE-T ポートのうち，ポート 21～22 の interface tengigabitethernet およびその配下のコンフィグレーションは削除されます。

[注意事項]

スタック構成で設定した場合は，スタックを構成するすべてのメンバスイッチを再起動してください。

15 ソフトウェアの管理

この章では，ソフトウェアの管理について説明します。

15.1　ソフトウェアアップデートの解説

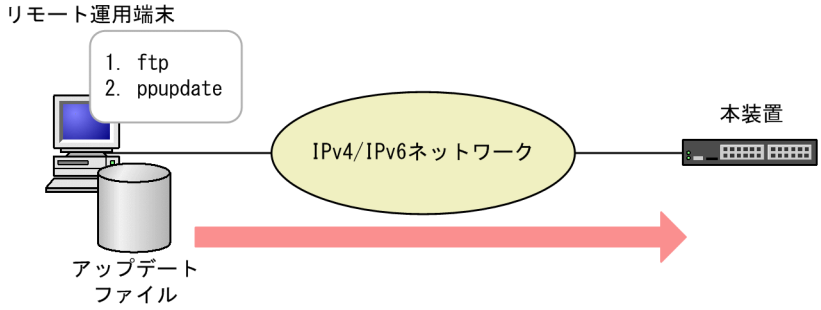
15.1.1　概要

ソフトウェアのアップデートとは，旧バージョンのソフトウェアから新バージョンのソフトウェアにバージョンアップすることを指します。ソフトウェアをアップデートするには，リモート運用端末や MC からアップデートファイルを本装置に転送し，運用コマンド ppupdate を実行します。アップデート時，装置管理のコンフィグレーションおよびユーザ情報（ユーザアカウント，パスワードなど）はそのまま引き継がれます。

(1)　リモート運用端末からのアップデート

PC などのリモート運用端末からアップデートする流れを次の図に示します。

図 15-1　リモート運用端末からアップデートする流れ

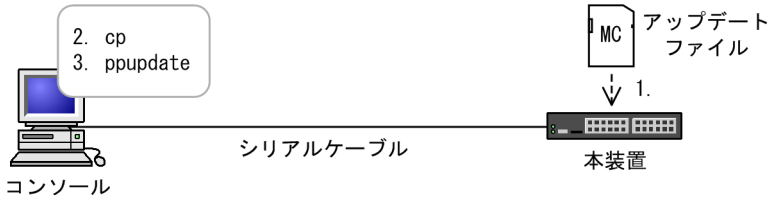


1. アップデートファイルを ftp でリモート運用端末から本装置に転送します。
2. 本装置にログイン後，アップデートコマンド（ppupdate）を実行します。

(2)　MC によるアップデート

MC を使用してアップデートする流れを次の図に示します。

図 15-2　MC を使用してアップデートする流れ

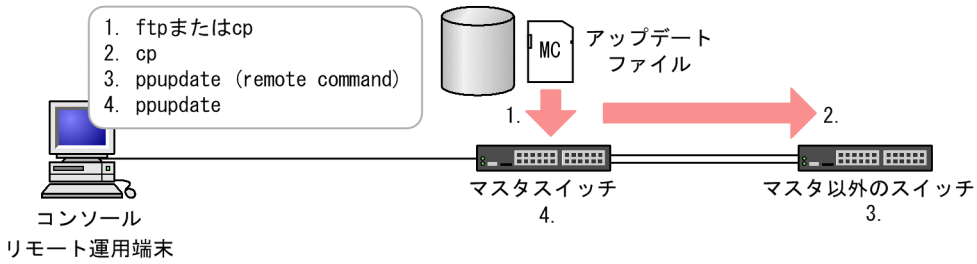


1. アップデートファイルが格納されている MC を本装置に挿入します。
2. アップデートファイルを MC から本装置にコピー（cp）します。
3. 本装置にログイン後，アップデートコマンド（ppupdate）を実行します。

(3)　スタック構成でのアップデート

スタック構成でアップデートする流れを次の図に示します。

図 15-3　スタック構成でアップデートする流れ



1. アップデートファイルを，ftp または MC でマスタスイッチに転送します。
2. マスタスイッチからマスタ以外のスイッチへ，アップデートファイルをコピー（cp）します。
3. マスタ以外のスイッチに対して，運用コマンド remote command を使用してアップデートコマンド（ppupdate）を実行します。
4. マスタスイッチに対して，アップデートコマンド（ppupdate）を実行します。

15.1.2　アップデートの準備

アップデート作業をする前に次の内容を確認してください。

(1)　アップデートに必要な条件

本装置へアップデートファイルを転送し，アップデートコマンドを実行するためには，いくつかの条件を満たす必要があります。アップデートに必要な条件を次の表に示します。

表 15-1　アップデートに必要な条件

操作	条件	対処方法
共通	内蔵フラッシュメモリに，アップデートファイルを転送できる未使用容量が確保されていること。※	容量不足のためアップデートファイルが転送できない場合は，「(2)　内蔵フラッシュメモリ容量を確保する方法」を参照して，必要な未使用容量を確保してください。
	運用コマンド enable で装置管理者モードへ変更するための権限があること。	アップデートコマンドを実行するには enable コマンドで装置管理者モードへ変更する必要があるため，装置管理者モードの権限を設定してください。
リモート運用端末からのアップデート	リモート運用端末から本装置に対して，IPv4 ネットワークまたは IPv6 ネットワーク経由で到達できる状態であること。	リモート運用端末を用意して，本装置と IP 通信ができるようネットワークに接続してください。
	リモート運用端末で ftp クライアントソフトウェアが動作し，本装置に対してファイルの書き込み（put）ができること。	ftp クライアントソフトウェアを用意して，リモート運用端末にインストールしてください。なお，Windows では，OS に付属している ftp を使用できます。
	リモート運用端末からの ftp プロトコルによるリモートアクセスを本装置で許可していること。	コンフィグレーションコマンド ftp-server を設定してください。また，config-line モード（line vty）でアクセスリストを指定している場合には，リモート運用端末からのアクセスを許可する設定としてください。
	リモート運用端末から本装置へログインできること。	リモート運用端末から telnet でログインする場合には，コンフィグレーションコマンド line vty で telnet プロトコ

操作	条件	対処方法
		ルによるリモートアクセスを許可する設定をしてください。
MC によるアップデート	コンソールから本装置へログインできること。	コンソールと本装置を接続してください。
		コンソールで通信ソフトウェアが使用できるようにしてください。

注※

運用コマンド show system で，内蔵フラッシュメモリのユーザ領域（user area）に，次に示す値以上の未使用容量（free）があることを確認してください。

アップデートファイルのサイズ＋ 10MB

(2)　内蔵フラッシュメモリ容量を確保する方法

内蔵フラッシュメモリ容量が不足している場合は，次に示す方法で未使用容量を確保してください。

- /usr/var/core/配下のファイルを運用コマンド rm で削除する。
- 運用コマンド erase protocol-dump を実行する。
- 運用コマンド squeeze を実行する。
- ユーザ領域に保存しているユーザファイルを削減する。

15.1.3　アップデートの注意事項

(1)　ファイル転送時の注意事項

アップデートファイルは，本装置上の/usr/var/update ディレクトリ配下に k.img というファイル名で転送してください。すでにファイルが存在している場合は，既存のファイルに上書きします。なお，ファイルのアクセス権によっては，ほかのユーザ※が作成した k.img ファイルに上書きできない場合があります。その場合は，いったん k.img ファイルを運用コマンド rm で削除してから転送してください。また，転送先およびファイル名を誤った場合は，誤ったファイルを削除してから再度転送してください。

注※　運用コマンド rmuser で削除済みのユーザが作成したファイルの場合，運用コマンド ls で詳細情報を表示したときに，ファイル所有者を数字で表示します。

(2)　MC からファイルをコピーするときの注意事項

- MC は，弊社製品を使用してください。
- 事前に PC などを使用して，アップデートファイルを MC に格納しておいてください。
- ファイル名 k.img のアップデートファイルを保存した MC を使用する場合，装置へファイルを転送後，MC を抜去するか，ファイル k.img を MC から削除してからアップデートコマンドを実行してください。k.img を保存した MC をスロットに挿入して装置を起動した場合，MC から起動するため，アカウント，コンフィグレーションは工場出荷時の初期状態となり，設定しても保存することはできません。

(3)　アップデートコマンド実行時の注意事項

- アップデートコマンドが異常終了した場合は，次のコマンドを実行して，ppupdate.exec ファイルの有無を確認してください。

```
ls /tmp/ppupdate.exec
```

該当するファイルが存在するときは，運用コマンド rm で対象ファイルを削除してください。

なお，スタック構成の場合は，マスタスイッチ以外は運用コマンド remote command を使用してファイルを確認したり削除したりしてください。

- アップデートコマンドは，複数のユーザで同時に実行できません。実行した場合，メッセージ「another user is executing now」を表示し，異常終了します。
- コンフィグレーションコマンドモードでは，アップデートコマンドを実行できません。
- k.img ファイルは削除しないでください。異常終了時にファイルを復旧できなくなります。
- アップデート実行中は，電源を OFF にしないでください。電源が OFF になった場合は，再起動後，最初からアップデートを再実行してください。
- 内蔵フラッシュメモリに保存されているコンフィグレーションは，アップデート後のバージョンにも内容が引き継がれます。保存されているコンフィグレーションの設定数が多い状態でアップデートすると，コンフィグレーションの引き継ぎに時間が掛かることがあります。

  なお，バージョンダウンする場合，未サポートになるコンフィグレーションはあらかじめ削除してください。未サポートのコンフィグレーションを削除しないでバージョンダウンを実行した場合，スタック構成では，メンバスイッチ間でコンフィグレーションが一致しないため，バージョンダウンしたメンバスイッチはスタックを構成できません。スタンドアロンの装置では，未サポートになるコンフィグレーションは削除して運用するため，意図しないネットワークを構築するおそれがあります。

15.2　アップデートのオペレーション

15.2.1　運用コマンド一覧

アップデートに関する運用コマンド一覧を次の表に示します。

表 15-2　運用コマンド一覧

コマンド名	説明
ppupdate	指定したソフトウェアにアップデートします。

15.2.2　アップデートファイルの準備

アップデートに使用するアップデートファイルを準備します。

1. コンフィグレーションをオンラインで編集したあと保存していない場合は，アップデートの前にコンフィグレーションコマンド save を実行して，コンフィグレーションを保存します。

   コンフィグレーションを保存しないと，アップデート終了後の再起動によって編集前のコンフィグレーションに戻ります。

2. show flash コマンドを実行します。

   内蔵フラッシュメモリのユーザ領域（user area）に，次に示す値以上の未使用容量（free）があることを確認してください。

   　アップデートファイルのサイズ－「/usr/var/update/k.img」のサイズ＋ 10MB

3. アップデートファイルを本装置に転送して，k.img という名前でディレクトリ（/usr/var/update）に置きます。

   ファイルの転送には，FTP を使用する方法と MC を使用する方法があります。FTP を使用する場合は，バイナリモードで転送してください。MC を使用してアップデートファイルを転送する例を次の図に示します。

   図 15-4　MC を使用したアップデートファイルの転送例

```
> ls mc-dir
Name              Size
k.img                 29603328
>
>cp mc-file k.img /usr/var/update/k.img
>
>ls -l /usr/var/update
total 28952
-rw-r--r--  1 operator  users  29603328 Nov  3 00:42 k.img
>
```

   下線の部分でファイルサイズを確認できます。

4. ls -l /usr/var/update コマンドを実行します。

   k.img のファイルサイズが，取得元のファイルサイズと等しいことを確認してください。確認が終了したら，「15.2.3　アップデートコマンドの実行」に進んでください。

15.2.3　アップデートコマンドの実行

ソフトウェアのバージョンを次の手順で旧バージョンから新バージョンにアップデートします。アップデートが完了すると，装置が自動で再起動します。再起動時には通信が一時的に中断されるため，注意してください。また，事前にアップデートファイルを本装置へ転送しておいてください。

1. enable コマンドを実行します。
   コマンドプロンプトが“#”に変更されます。
2. cd /usr/var/update コマンドを実行します。
3. ppupdate k.img コマンドを実行します。
   インストールされるソフトウェアのバージョンと，アップデート対象が表示されます。アップデートが完了すると，自動で装置が再起動します。
4. 再起動後，再度装置にログインします。
5. show version コマンドを実行して，アップデート後のバージョンで動作していることを確認します。

アップデートの実行例を次の図に示します。

図 15-5　アップデートの実行例

```
> enable
#
# cd /usr/var/update/
#
# ls -l
total 28952
-rw-r--r--  1 operator  users  29603328 Nov  3 00:42 k.img
#
# ppupdate k.img

Software update start

Broadcast Message from operator@
        (??) at 10:24 JST...

*********************************************
** UPDATE IS STARTED.                       **
*********************************************

Current version is 12.0
New version is 12.1
Automatic reboot process will be run after installation process.
Do you wish to continue? (y/n) y

100% |************************| 28909 KiB    1.72 MiB/s    00:00 ETA

Update done.

Broadcast Message from operator@
        (??) at 10:25 JST...

*********************************************
** UPDATE IS FINISHED SUCCESSFULLY.         **
*********************************************

#

         :

login: operator
Password:

Copyright (c) 20XX ALAXALA Networks Corporation. All rights reserved.


> show version software
Date 20XX/11/03 10:27:29 UTC
S/W: OS-L3M Ver. 12.1
>
```

15.2.4　スタック構成でのアップデートコマンドの実行

スタック構成の場合は，次の手順でアップデートします。

1. enable コマンドを実行します。
   コマンドプロンプトが“#”に変更されます。
2. cd /usr/var/update コマンドを実行します。
3. cp k.img switch <switch no.> /usr/var/update/k.img コマンドを実行して，アップデート対象スイッチにアップデートファイルをコピーします。
   <switch no.>には，転送先のスイッチ番号を指定してください。
4. マスタスイッチで remote command <switch no.> ppupdate /usr/var/update/k.img コマンドを実行して，マスタスイッチ以外のアップデート対象スイッチをアップデートします。
5. ppupdate k.img コマンドを実行して，マスタスイッチをアップデートします。
   アップデートが完了すると，自動で装置が再起動します。
6. 再起動後，再度装置にログインします。
7. show version コマンドを実行して，アップデート後のバージョンで動作していることを確認します。

15.3　ライセンスの解説

15.3.1　概要

本装置には，ソフトウェアライセンスとオプションライセンスの 2 種類のライセンスを設定できます。ソフトウェアライセンスとは，装置の基本的な機能を使用するために必要となるライセンスです。オプションライセンスとは，装置に含まれる付加機能を使用するために必要となるライセンスで，付加機能ごとに提供します。

15.3.2　ライセンスに関する注意事項

- ソフトウェアライセンスおよびオプションライセンスは，装置に対応したものを設定してください。
- ソフトウェアライセンスおよびオプションライセンスの設定情報は，装置に保存されます。
  装置の交換やソフトウェアの新規インストール時には，ライセンスの再設定が必要です。ソフトウェアのバージョンアップ時には，ライセンスの再設定は不要です。
- ソフトウェアライセンスおよびオプションライセンスを設定した場合，設定を反映するには装置を再起動する必要があります。
- ある機能のオプションライセンスが設定された状態で，別機能のオプションライセンスを追加で設定できます。
- ソフトウェアライセンスは，装置に一つだけ設定できます。
  あるソフトウェアライセンスが設定された状態で，別のソフトウェアライセンスを設定した場合，先に設定されていたソフトウェアライセンスは削除されます。

15.4　ライセンスのオペレーション

15.4.1　運用コマンド一覧

ライセンスに関する運用コマンド一覧を次の表に示します。

表 15-3　運用コマンド一覧

コマンド名	説明
set license	ソフトウェアライセンスまたはオプションライセンスを設定します。
show license	設定されているソフトウェアライセンスおよびオプションライセンスを表示します。
erase license	指定したオプションライセンスを削除します。

15.4.2　ライセンスの設定方法

ソフトウェアライセンスおよびオプションライセンスは，ライセンスキーを使用して次の手順で設定します。なお，ライセンスキーは「ソフトウェアライセンス使用許諾契約書兼ライセンスシート」または「オプションライセンス使用許諾契約書兼ライセンスシート」に記述されています。

1. enable コマンドを実行します。
2. show license コマンドを実行して，現在のライセンスの設定状況を確認します。
3. set license key-code <license key>コマンドを実行して，ライセンスを設定します。
   <license key>には，設定するライセンスキーを指定してください。
4. show license コマンドを実行して，設定したライセンスが表示されることを確認します。
   設定したライセンスキーの先頭 16 桁が表示されます。
5. reload -f no-dump-image コマンドを実行して，装置を再起動します。
   設定したライセンスキーは，装置が再起動したあとで有効になります。
6. 再起動後，再度装置にログインします。
7. show license コマンドを実行して，設定したライセンスが有効になっていることを確認します。

ライセンス設定の実行例を次の図に示します。

図 15-6　ライセンス設定の実行例

```
> enable
#
# show license
Date 20XX/11/03 10:35:39 UTC
  Available:SL-L3L-004
    Serial Number        Licensed software
    1500-abcd-0009-0000  SL-L3L-004(AX-P3660-G8)
#
# set license key-code 1600-1234-4000-0000-1234-5678-abcd-ef00
#
# show license
Date 20XX/11/03 10:36:07 UTC
  Available:SL-L3L-004
    Serial Number        Licensed software
    1500-abcd-0009-0000  SL-L3L-004(AX-P3660-G8)
    1600-1234-4000-0000  OP-STK(AX-P3660-F2)
#
# reload -f no-dump-image
#
```

```
         :

login: operator
Password:

Copyright (c) 20XX ALAXALA Networks Corporation. All rights reserved.


>
> show license
Date 20XX/11/03 00:27:05 UTC
  Available:SL-L3L-004 OP-STK
    Serial Number        Licensed software
    1500-abcd-0009-0000  SL-L3L-004(AX-P3660-G8)
    1600-1234-4000-0000  OP-STK(AX-P3660-F2)
>
```

15.4.3　オプションライセンスの削除方法

オプションライセンスは次の手順で削除します。

1. enable コマンドを実行します。
2. show license コマンドを実行して，現在のオプションライセンスの設定状況を確認します。
   削除するオプションライセンスのシリアル番号を確認してください。シリアル番号は 16 桁の英数字です。
3. erase license <serial no.>コマンドを実行して，オプションライセンスを削除します。
   <serial no.>には，削除するオプションライセンスのシリアル番号を指定してください。
4. 確認メッセージが表示されたら，“y”を入力します。
5. show license コマンドを実行して，指定したオプションライセンスが削除されていることを確認します。
6. reload -f no-dump-image コマンドを実行して，装置を再起動します。
   削除したライセンスキーは，装置が再起動したあとで無効になります。
7. 再起動後，再度装置にログインします。
8. show license コマンドを実行して，オプションライセンスが無効になっていることを確認します。

オプションライセンス削除の実行例を次の図に示します。

図 15-7　オプションライセンス削除の実行例

```
> enable
#
# show license
Date 20XX/11/03 00:27:53 UTC
  Available:SL-L3L-004 OP-STK
    Serial Number        Licensed software
    1500-abcd-0009-0000  SL-L3L-004(AX-P3660-G8)
    1600-1234-4000-0000  OP-STK(AX-P3660-F2)
#
# erase license 1600-1234-4000-0000
This serial number enable OP-STK
Erase OK? (y/n): y
#
# show license
Date 20XX/11/03 00:28:12 UTC
  Available:SL-L3L-004 OP-STK
    Serial Number        Licensed software
    1500-abcd-0009-0000  SL-L3L-004(AX-P3660-G8)
#
# reload -f no-dump-image
#
```

```
          :

login: operator
Password:

Copyright (c) 20XX ALAXALA Networks Corporation. All rights reserved.

>
> show license
Date 20XX/11/03 00:30:06 UTC
  Available:SL-L3L-004
    Serial Number        Licensed software
    1500-abcd-0009-0000  SL-L3L-004(AX-P3660-G8)
>
```

16 省電力機能

この章では，本装置の省電力機能について説明します。

16.1　省電力機能の解説

16.1.1　省電力機能の概要

ネットワークの使用量の増加に備え，収容ポートの帯域を増やしているケースでは，増やしたポート帯域分の電力も消費しています。本装置では，省電力機能によって，不要に消費される電力を抑えられます。

(1)　サポートする省電力機能

本装置では，省電力機能として次に示す機能をサポートします。これらの省電力機能を常時動作させることも，スケジューリングによって動作させる時間帯を限定することもできます。

- ポートの電力供給 OFF
- LED 輝度制御機能

16.1.2　省電力機能

(1)　ポートの電力供給 OFF

使用していないポートの電力供給を OFF にすると，消費電力を削減できます。次の方法でポートの電力供給を OFF にできます。

- コンフィグレーションコマンドでポートを shutdown 状態にする
- 運用コマンドでポートを inactive 状態にする

(2)　LED 輝度制御機能

本装置の LED の輝度を制御して，消費電力を削減できます。

本装置は，LED の輝度を固定的に省電力輝度または消灯に設定できます。さらに，本装置には LED の輝度を自動的に調整する機能があります。この機能を輝度自動調整機能といいます。

輝度自動調整機能を使用すると，次に示す契機が一定時間発生しないときに本装置の LED の輝度を落とし，さらに一定時間契機が発生しないと LED を消灯します。

- コンソールからのログイン
- MC の挿入または抜去
- イーサネットインタフェースのリンクアップとリンクダウン

ただし，コンソールからのログイン中は LED の輝度を変更しないで，ログアウトするまで LED は通常輝度となります。

LED 輝度制御を設定したときの LED の輝度を次の表に示します。

表 16-1　LED 輝度制御設定時の LED の輝度

LED	LED 輝度制御の設定		
	通常輝度	省電力輝度	消灯
ポート LED（点灯時）	通常輝度	省電力輝度	消灯

なお，ポート LED は，LED 輝度設定の有無とは関係なく，状態によっては消灯となります。

16.1.3　省電力機能のスケジューリング

時間帯を指定して省電力機能を実行する場合はスケジューリングをします。スケジューリングは，実行する省電力機能と実施したい時間帯を指定します。これらの指定によって，開始時刻になると，自動的に省電力機能が実行されます。また，すでに実行中の省電力機能をある時間帯だけ無効にするスケジューリングもできます。なお，省電力のスケジュールを設定している時間帯を**スケジュール時間帯**，スケジュールを設定していない時間帯を**通常時間帯**と呼びます。

(1)　スケジュールに指定できる省電力機能

スケジュールに指定できる省電力機能として，ポートの電力供給 OFF および LED 輝度制御機能があります。省電力機能は組み合わせて使用できます。

(2)　スケジュールの時刻指定方法

省電力で運用する時間帯をスケジュール時間帯として，開始と終了の時刻で指定します。時間帯の指定方法を次に示します。

- 日時で時間帯を指定して省電力にする
- 曜日と時刻で時間帯を指定して省電力にする
- 毎日の時間帯を指定して省電力にする
- 時間帯を指定して省電力スケジュールを無効にする

スケジューリングの際には，これらの指定方法を組み合わせて設定できるため，さまざまな時間帯で省電力機能を有効にしたり，無効にしたりできます。

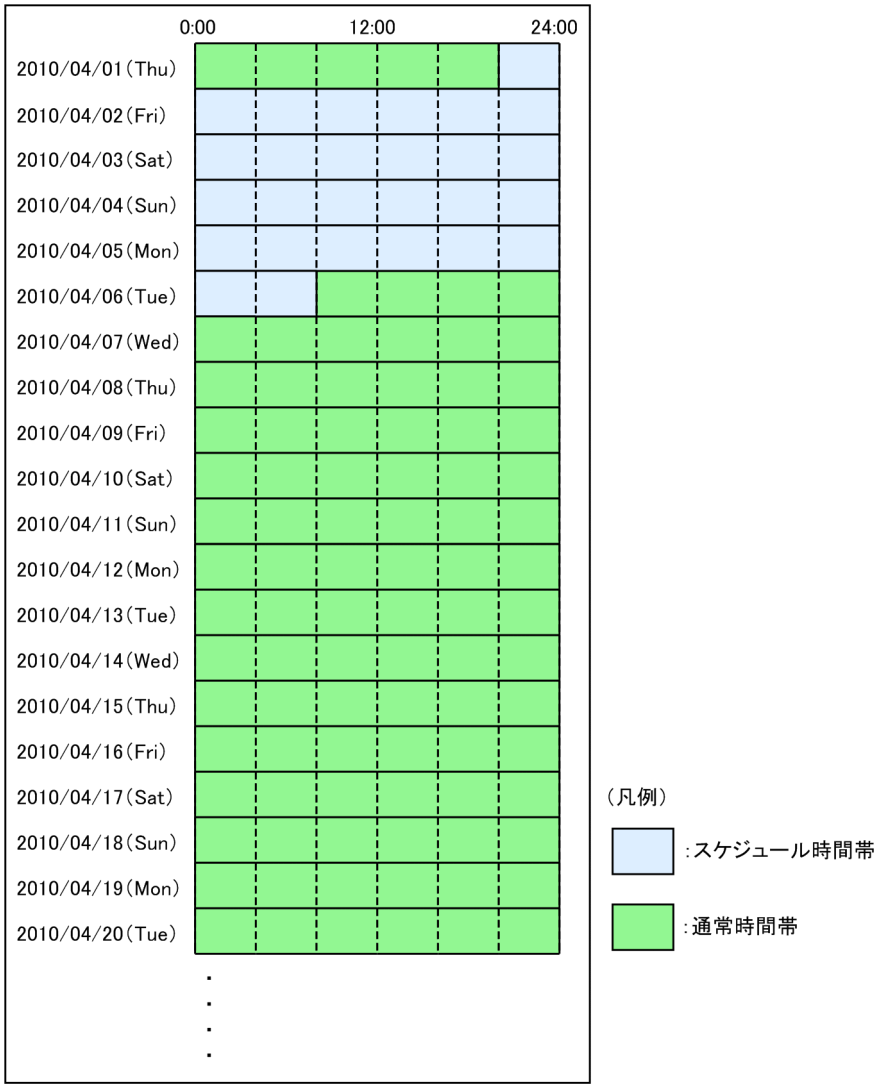
(a)　日時で時間帯を指定して省電力にする

省電力に設定したい，開始と終了の日付および時刻を指定します。

例：

2010 年 4 月 2 日から 5 日までは業務システムの稼働が低減します。稼働低減に合わせて，2010 年 4 月 1 日 20 時から 2010 年 4 月 6 日 8 時までを省電力にするスケジュールを指定します。動作スケジュールを次の図に示します。

図 16-1　省電力スケジュール（特定の日付）



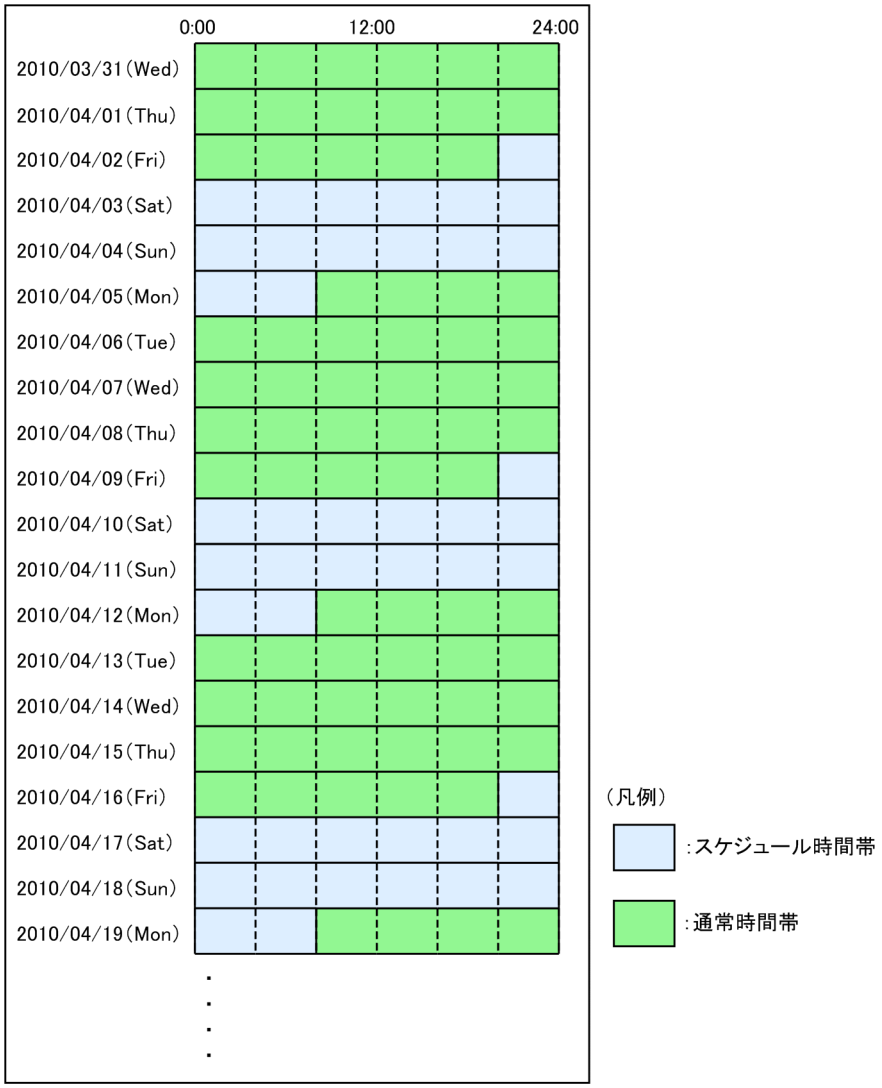
(b)　曜日と時刻で時間帯を指定して省電力にする

省電力に設定したい，開始と終了の曜日および時刻を指定します。

例：

毎週土曜日と日曜日は休日となっていて，その間は業務システムの稼働が低減します。稼働低減に合わせて，毎週金曜日 20 時から毎週月曜日 8 時までを省電力にするスケジュールを指定します。動作スケジュールを次の図に示します。

図 16-2　省電力スケジュール（特定の曜日）



(c)　毎日の時間帯を指定して省電力にする

省電力に設定したい，開始と終了の時刻を指定します。

例：

通常業務は毎日 8 時 30 分から 17 時までとなっているため，業務システムを 8 時から 20 時まで通常の電力で運用します。毎日 20 時から翌日の 8 時までを省電力にするスケジュールを指定します。動作スケジュールを次の図に示します。

図 16-3　省電力スケジュール（毎日）

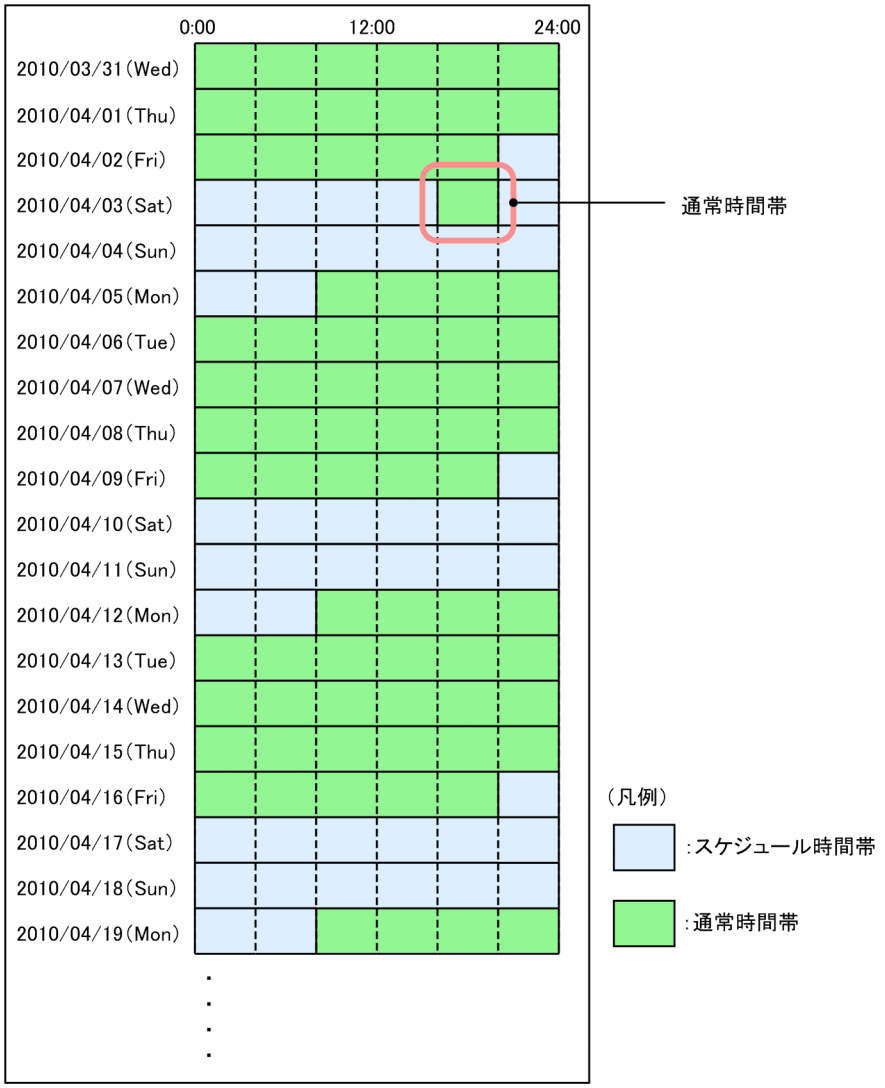
(d)　時間帯を指定して省電力スケジュールを無効にする

すでに省電力機能がスケジュールされている時間帯の，スケジュールの実行を無効にできます。実行を無効にしたい開始と終了の時刻を指定します。特定の日付，特定の曜日，および毎日の特定時間で無効にする時間帯を指定できます。

例：

毎週土曜日と日曜日は休日のため，毎週金曜日 20 時から毎週月曜日 8 時までを省電力にするスケジュールが指定してあります。ただし，業務システムのバッチ処理を行うために 2010 年 4 月 3 日 16 時から 20 時までを通常の電力で運用します。動作スケジュールを次の図に示します。

図 16-4　省電力スケジュール（無効設定）



16.1.4　省電力機能に関する注意事項

(1)　スケジューリングを使用した省電力機能に関する注意事項

- 通常時間帯とスケジュール時間帯で同じ省電力機能を使用する場合は，通常時間帯とスケジュール時間帯の両方にその設定をしてください。

  例

  通常時間帯でポートの電力供給を OFF にするために，コンフィグレーションコマンド shutdown を設定します。スケジュール時間帯でも該当ポートの電力供給を OFF にする場合は，コンフィグレーションコマンド schedule-power-control shutdown の設定対象に，shutdown を設定したポートも含める必要があります。

(2)　スケジュール時間帯の開始・終了時間の誤差に関する注意事項

スケジューリングではソフトウェアのタイマを使用しているため，CPU の負荷が高い場合などに，スケジュール時間帯の開始または終了が設定した時間とずれるおそれがあります。このずれは，通常 1 分を超えることはありません。また，スケジューリングによってポートの電力供給を OFF にしていた場合，スケ

ジュールが終了してから実際に通信できるまでネットワークの構成に応じた時間が必要です。省電力機能のスケジューリングでは余裕を持った時間を設定してください。

16.2　省電力機能のコンフィグレーション

16.2.1　コンフィグレーションコマンド一覧

省電力機能のコンフィグレーションコマンド一覧を次の表に示します。

表 16-2　コンフィグレーションコマンド一覧

コマンド名		説明
通常時間帯への設定コマンド	スケジュール時間帯への設定コマンド	
shutdown※	schedule-power-control shutdown	ポートへの電力供給を OFF に設定します。
system port-led	schedule-power-control port-led	LED の輝度を制御します。
system port-led trigger console		輝度自動調整の契機にコンソールからのログインを設定します。
system port-led trigger interface		輝度自動調整の契機にポートのリンクアップ／ダウンを設定します。
system port-led trigger mc		輝度自動調整の契機に MC の挿抜を設定します。
－	schedule-power-control time-range	省電力スケジュールの時間帯を指定します。

（凡例）－：該当なし

注※

「コンフィグレーションコマンドレファレンス Vol.1」「15　イーサネット」を参照してください。

16.2.2　コンフィグレーションコマンド設定例

(1)　スケジュールによる未使用ポートの電力供給 OFF

スケジュールによって未使用ポートの電力供給を OFF にする場合のコンフィグレーションコマンドの設定例を次に示します。

[設定のポイント]

未使用ポートの電力供給 OFF を設定して，消費電力を低減します。

[コマンドによる設定]

1. **(config)# schedule-power-control shutdown interface gigabitethernet 1/0/1-10**
   スケジュール時間帯に電力供給を OFF にするポートを指定します。
2. **(config)# schedule-power-control time-range 1 weekly start-time fri 2000 end-time mon 0800 action enable**
   毎週金曜日 20 時から毎週月曜日 8 時まで動作するスケジュールを指定します。
3. **(config)# schedule-power-control time-range 2 date start-time 100403 1600 end-time 100403 2000 action disable**

2010 年 4 月 3 日 16 時から 20 時までの時間帯は省電力スケジュールの実行を無効にする指定をします。

(2) LED の輝度制御機能

通常時間帯とスケジュール時間帯のどちらも LED の輝度自動調整をする場合のコンフィグレーションコマンドの設定例を次に示します。

[設定のポイント]

スケジュールを設定している場合，通常時間帯とスケジュール時間帯でそれぞれ LED の輝度制御機能を設定します。輝度自動調整の契機として，ポート 1/0/1-10 とコンソールからのログインを設定します。

[コマンドによる設定]

1. **(config)# system port-led enable**
   通常時間帯に LED の輝度自動調整を設定します。
2. **(config)# schedule-power-control port-led enable**
   スケジュール時間帯に LED の輝度自動調整を設定します。
3. **(config)# system port-led trigger interface gigabitethernet 1/0/1-10**
   LED の輝度自動調整の契機に，ポート 1/0/1-10 を設定します。
4. **(config)# system port-led trigger console**
   LED の輝度自動調整の契機にコンソールからのログインを設定します。

16.3　省電力機能のオペレーション

16.3.1　運用コマンド一覧

省電力機能の運用コマンド一覧を次の表に示します。

表 16-3　運用コマンド一覧

コマンド名	説明
show power-control schedule	省電力スケジュールの一覧を表示します。
show power	装置の最大消費電力情報を表示します。
clear power	装置の消費電力量情報をクリアします。
set power-control schedule	省電力スケジュールの適用または抑止を設定します。
inactivate※	ポートの電力供給を OFF に設定します。

注※

「運用コマンドレファレンス Vol.1」「21　イーサネット」を参照してください。

16.3.2　LED 動作状態の表示

LED 動作の設定状態は，運用コマンド show system の「LED Brightness mode」で確認できます。詳細は，「14.1.3　装置の状態確認」を参照してください。

図 16-5　LED 動作状態の確認

```
> show system
Date 20XX/01/16 17:53:12 UTC
System: AX3660S-24T4XW, OS-L3M (SL-L3A-001) Ver. 12.0
Node : Name=
    Contact=
    Locate=
    Elapsed time : 00:45:03
    LED Brightness mode : normal
                :
```

16.3.3　省電力機能の状態確認

(1)　省電力スケジュールの確認

運用コマンド show power-control schedule で，現在の省電力スケジュールの状態と，設定されている省電力スケジュールを確認できます。20XX 年 4 月 1 日以降に予定されているスケジュールを 5 件表示する例を次の図に示します。

図 16-6　省電力スケジュールの確認

```
> show power-control schedule XX0401 count 5
Date 20XX/04/01(Thu) 18:36:57 UTC
Current Schedule Status : Disable
Schedule Power Control Date:
  20XX/04/01(Thu) 20:00 UTC  -  20XX/04/02(Fri) 06:00 UTC
  20XX/04/02(Fri) 20:00 UTC  -  20XX/04/05(Mon) 06:00 UTC
  20XX/04/05(Mon) 20:00 UTC  -  20XX/04/06(Tue) 06:00 UTC
  20XX/04/06(Tue) 20:00 UTC  -  20XX/04/07(Wed) 06:00 UTC
  20XX/04/07(Wed) 20:00 UTC  -  20XX/04/08(Thu) 06:00 UTC
>
```

16.3.4 省電力スケジュールの適用または抑止

運用コマンド set power-control schedule で，スケジュール時間帯に省電力スケジュールの適用または抑止を設定できます。

図 16-7 省電力スケジュールの適用

```
> show power-control schedule XX1001 count 1
Date 20XX/10/01(Fri) 18:36:57 UTC
Current Schedule Status : Enable(force disabled)
Schedule Power Control Date:
  20XX/10/01(Fri) 18:36 UTC  -  20XX/10/02(Sat) 06:00 UTC
```

省電力スケジュールを確認します。状態が“Enable(force disabled)”となっているので，スケジュール時間帯でスケジュールが抑止されていることが確認できます。

```
> set power-control schedule enable
```

省電力スケジュールを適用します。

```
> show power-control schedule XX1001 count 1
Date 20XX/10/01(Fri) 18:37:20 UTC
Current Schedule Status : Enable
Schedule Power Control Date:
  20XX/10/01(Fri) 18:37 UTC  -  20XX/10/02(Sat) 06:00 UTC
```

省電力スケジュールを確認します。状態が“Enable”となっているので，スケジュール時間帯でスケジュールが適用されていることが確認できます。

17 ログ出力機能

この章では，本装置のログ出力機能について説明します。

17.1　解説

本装置では動作情報や障害情報などを運用メッセージとして通知します。同メッセージは運用端末に出力するほか，運用ログとして装置内に保存します。この情報で装置の運用状態や障害の発生を管理できます。

運用ログは装置運用中に発生した事象（イベント）を発生順に記録したログ情報で，運用メッセージと同様の内容が格納されます。運用ログとして格納する情報には次に示すものがあります。

- オペレータの操作および応答メッセージ
- 運用メッセージ

種別ログは装置内で発生した障害や警告についての運用ログ情報をメッセージ ID ごとに分類した上で，同事象が最初に発生した日時および最後に発生した日時と累積回数をまとめた情報です。

これらのログは装置内にテキスト形式で格納されています。装置管理者は，表示コマンドでこれらの情報を参照できます。

採取した本装置のログ情報は，syslog インタフェースを使用して syslog 機能を持つネットワーク上の他装置（UNIX ワークステーションなど）に送ることができます※1，※2，※3。また，同様に，ログ情報を E-Mail を使用してネットワーク上の他装置に送ることもできます。これらのログ出力機能を使用することで，多数の装置を管理する場合にログの一元管理ができるようになります。また，ログ情報を E-Mail で送信することもできます。

注※1

他装置からの syslog メッセージを受信する機能はサポートしていません。

注※2

本装置で生成した syslog メッセージでは，RFC3164 で定義されている HEADER 部の HOSTNAME 欄は未設定です。

注※3

スタック構成でメンバスイッチのスイッチ状態がバックアップからマスタへ遷移した直後は，一時的に syslog サーバへ IP パケットを送信できない状態になります。その場合，syslog サーバへのメッセージが syslog サーバに届かないため，ログ情報が記録されないことがあります。

スイッチ状態遷移時のログ情報は，運用コマンド show logging で確認してください。

17.2　コンフィグレーション

17.2.1　コンフィグレーションコマンド一覧

ログ出力機能に関するコンフィグレーションコマンド一覧を次の表に示します。

表 17-1　コンフィグレーションコマンド一覧（syslog 出力に関する設定）

コマンド名	説明
logging event-kind	syslog サーバに送信対象とするログ情報のメッセージ種別を設定します。
logging facility	ログ情報を syslog インタフェースで出力するためのファシリティを設定します。
logging host	ログ情報の出力先を設定します。
logging trap	syslog サーバに送信対象とするログ情報の重要度を設定します。

表 17-2　コンフィグレーションコマンド一覧（E-Mail 出力に関する設定）

コマンド名	説明
logging email	ログ情報を E-Mail で出力するための E-Mail アドレスを設定します。
logging email-event-kind	E-Mail で出力対象とするログ情報のメッセージ種別を設定します。
logging email-from	ログ情報を E-Mail で出力する E-Mail の送信元を設定します。
logging email-interval	ログ情報を E-Mail で出力するための送信間隔を設定します。
logging email-server	ログ情報を E-Mail で出力するため SMTP サーバの情報を設定します。

17.2.2　ログの syslog 出力の設定

[設定のポイント]

syslog 出力機能を使用して，採取したログ情報を syslog サーバに送信するための設定をします。

[コマンドによる設定]

1. **(config)# logging host LOG_HOST**

ログをホスト名 LOG_HOST 宛てに出力するように設定します。

17.2.3　ログの VRF への syslog 出力の設定【SL-L3A】

[設定のポイント]

syslog 出力機能を使用して，採取したログ情報を VRF に存在する syslog サーバに送信するための設定をします。

VRF を指定する場合には，ログ出力先を IPv4 アドレスまたは IPv6 アドレスで指定する必要があります。ホスト名で指定した場合は，VRF を指定できません。

[コマンドによる設定]

1. **(config)# logging host 128.1.1.2 vrf 2**

ログを IP アドレス 128.1.1.2，VRF ID 2 宛てに出力するように設定します。

17.2.4　ログの E-Mail 出力の設定

[設定のポイント]

E-Mail 送信機能を使用して，採取したログ情報をリモートホスト，PC などに送信するための設定をします。

[コマンドによる設定]

1. **(config)# logging email system@loghost**
   送信先のメールアドレスとして system@loghost を設定します。

18 SNMP

この章では本装置の SNMP エージェント機能についてサポート仕様を中心に説明します。

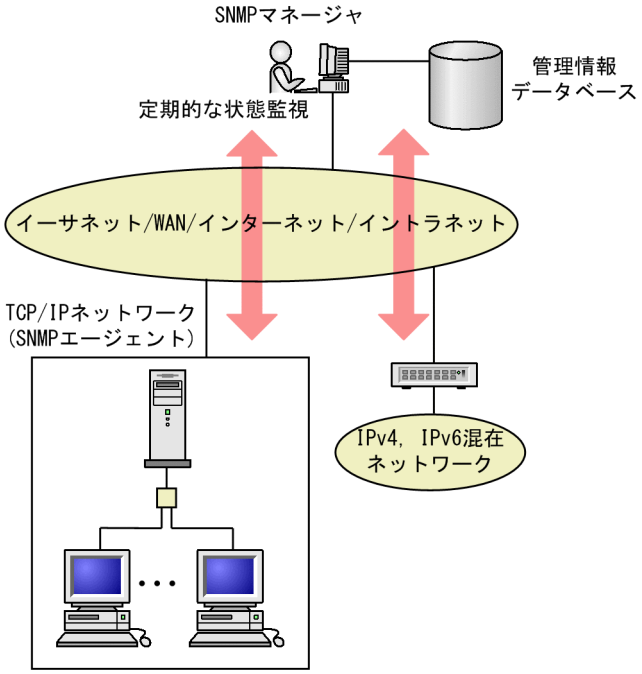
18.1　解説

18.1.1　SNMP 概説

(1)　ネットワーク管理

ネットワークシステムの稼働環境や性能を維持するためには，高度なネットワーク管理が必要です。SNMP（simple network management protocol）は業界標準のネットワーク管理プロトコルです。SNMP をサポートしているネットワーク機器で構成されたマルチベンダーネットワークを管理できます。管理情報を収集して管理するサーバを SNMP マネージャ，管理される側のネットワーク機器を SNMP エージェントといいます。ネットワーク管理の概要を次の図に示します。

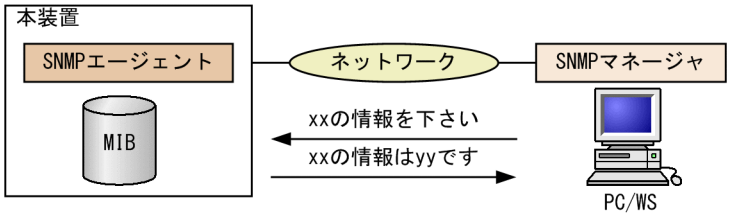
図 18-1　ネットワーク管理の概要



(2)　SNMP エージェント機能

本装置の SNMP エージェントは，ネットワーク上の装置内部に組み込まれたプログラムです。装置内の情報を SNMP マネージャに提供する機能があります。装置内にある各種情報を MIB（Management Information Base）と呼びます。SNMP マネージャは，装置の情報を取り出して編集・加工し，ネットワーク管理を行うための各種情報をネットワーク管理者に提供するソフトウェアです。MIB 取得の例を次の図に示します。

図 18-2　MIB 取得の例

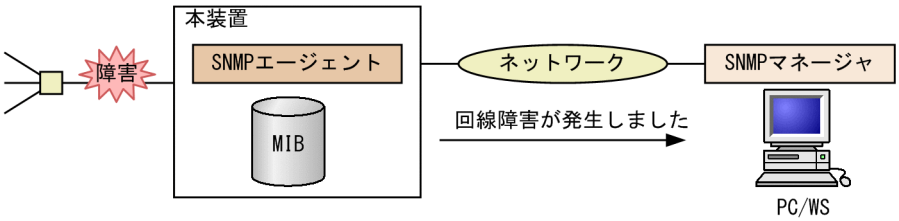


本装置の運用コマンドには MIB 情報を表示するための SNMP コマンドがあります。このコマンドは，自装置およびリモート装置の SNMP エージェントの MIB を表示します。

本装置では，SNMPv1（RFC1157），SNMPv2C（RFC1901），および SNMPv3（RFC3410）をサポートしています。SNMP マネージャを使用してネットワーク管理を行う場合は，SNMPv1，SNMPv2C，または SNMPv3 プロトコルで使用してください。なお，SNMPv1，SNMPv2C，SNMPv3 をそれぞれ同時に使用することもできます。

また，SNMP エージェントは**トラップ**（Trap）や**インフォーム**（Inform）と呼ばれるイベント通知（主に障害発生の情報など）機能があります。以降，トラップおよびインフォームを SNMP 通知と呼びます。SNMP マネージャは，SNMP 通知を受信することで定期的に装置の状態変化を監視しなくても変化を知ることができます。ただし，トラップは UDP を使用しているため，装置から SNMP マネージャに対するトラップの到達確認ができません。そのため，ネットワークの輻輳などによって，トラップがマネージャに到達しない場合があります。トラップの例を次の図に示します。

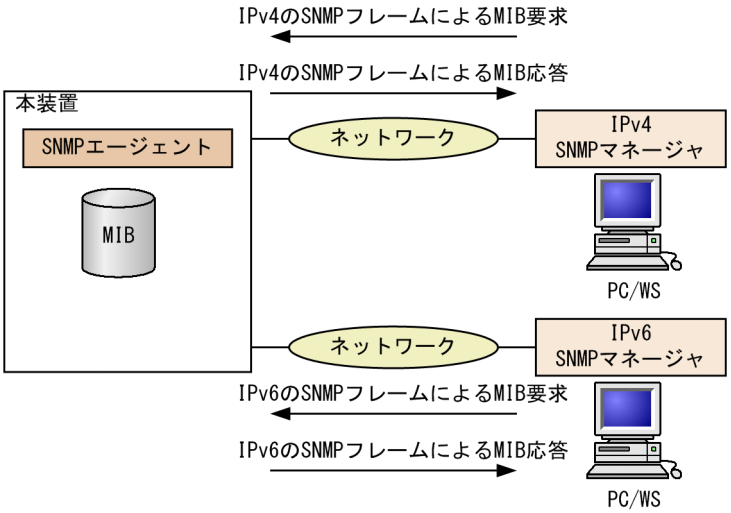
図 18-3　トラップの例



インフォームもトラップと同じ UDP によるイベント通知ですが，トラップとは異なって SNMP マネージャからの応答を要求します。そのため，応答の有無でインフォームの到達を確認できます。これによって，ネットワークの輻輳などに対してもインフォームの再送で対応できます。

本装置の SNMP プロトコルは IPv6 に対応しています。コンフィグレーションに設定した SNMP マネージャの IP アドレスによって，IPv4 または IPv6 アドレスが設定されている SNMP マネージャからの MIB 要求や，SNMP マネージャへの SNMP 通知の送信ができます。IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例を次の図に示します。

図 18-4　IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例



(3) SNMPv3

SNMPv3 は SNMPv2C までの全機能に加えて，管理セキュリティ機能が大幅に強化されています。ネットワーク上を流れる SNMP パケットを認証・暗号化することによって，SNMPv2C でのコミュニティ名と SNMP マネージャの IP アドレスの組み合わせによるセキュリティ機能では実現できなかった，盗聴，なりすまし，改ざん，再送などのネットワーク上の危険から SNMP パケットを守ることができます。

(a) SNMP エンティティ

SNMPv3 では，SNMP マネージャおよび SNMP エージェントを「SNMP エンティティ」と総称します。本装置の SNMPv3 は，SNMP エージェントに相当する SNMP エンティティをサポートしています。

(b) SNMP エンジン

SNMP エンジンは認証，および暗号化したメッセージ送受信と管理オブジェクトへのアクセス制御のためのサービスを提供します。SNMP エンティティとは 1 対 1 の関係です。SNMP エンジンは，同一管理ドメイン内でユニークな SNMP エンジン ID により識別されます。

(c) ユーザ認証と暗号化機能

SNMPv1，SNMPv2C でのコミュニティ名による認証に対して，SNMPv3 ではユーザ認証を行います。また，SNMPv1，SNMPv2C にはなかった暗号化機能も SNMPv3 でサポートされています。ユーザ認証と暗号化機能は，ユーザ単位に設定できます。

本装置では，ユーザ認証に使用する認証プロトコルとして次のプロトコルをサポートしています。

HMAC-MD5-96
: MD5 アルゴリズムを使用した認証プロトコルです。128 ビットのダイジェストのうち，先頭の 96 ビットを使用します。

HMAC-SHA-96
: SHA-1 アルゴリズムを使用した認証プロトコルです。160 ビットのダイジェストのうち，先頭の 96 ビットを使用します。

HMAC-SHA-256
: SHA-256 アルゴリズムを使用した認証プロトコルです。256 ビットのダイジェストのうち，先頭の 192 ビットを使用します。

HMAC-SHA-512
: SHA-512 アルゴリズムを使用した認証プロトコルです。512 ビットのダイジェストのうち，先頭の 384 ビットを使用します。

暗号化機能に使用するプライバシープロトコルとして次のプロトコルをサポートしています。

CBC-DES
: DES アルゴリズムと，暗号利用モード CBC を組み合わせて暗号化するプライバシープロトコルです。

CFB128-AES-128
: AES アルゴリズムと，暗号利用モード CFB を組み合わせて暗号化するプライバシープロトコルです。

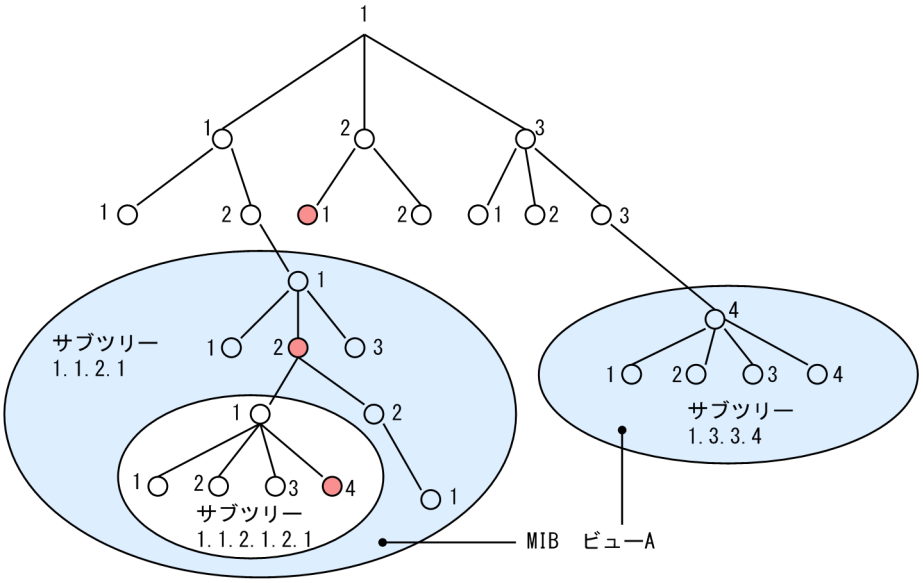
(d) MIB ビューによるアクセス制御

SNMPv3 では，ユーザ単位に，アクセスできる MIB オブジェクトの集合を設定できます。この MIB オブジェクトの集合を MIB ビューと呼びます。MIB ビューは，MIB のオブジェクト ID のツリーを表すビューサブツリーを集約することによって表現されます。集約する際には，ビューサブツリーごとに included

(MIB ビューに含む)，または excluded (MIB ビューから除外する) を選択できます。MIB ビューは，ユーザ単位に，Read ビュー，Write ビュー，Notify ビューとして設定できます。

次に，MIB ビューの例を示します。MIB ビューは，「図 18-5　MIB ビューの例」に示すような MIB ツリーの一部である MIB サブツリーをまとめて設定します。オブジェクト ID 1.1.2.1.2 は，サブツリー 1.1.2.1 に含まれるので，MIB ビュー A でアクセスできます。しかし，オブジェクト ID 1.2.1 は，どちらのサブツリーにも含まれないので，アクセスできません。また，オブジェクト ID 1.1.2.1.2.1.4 は，サブツリー 1.1.2.1.2.1 がビュー A から除外されているためアクセスできません。

図 18-5　MIB ビューの例



コンフィグレーションの内容

```
ViewA  1.1.2.1      included
       1.3.3.4      included
       1.1.2.1.2.1 excluded
```

18.1.2　MIB 概説

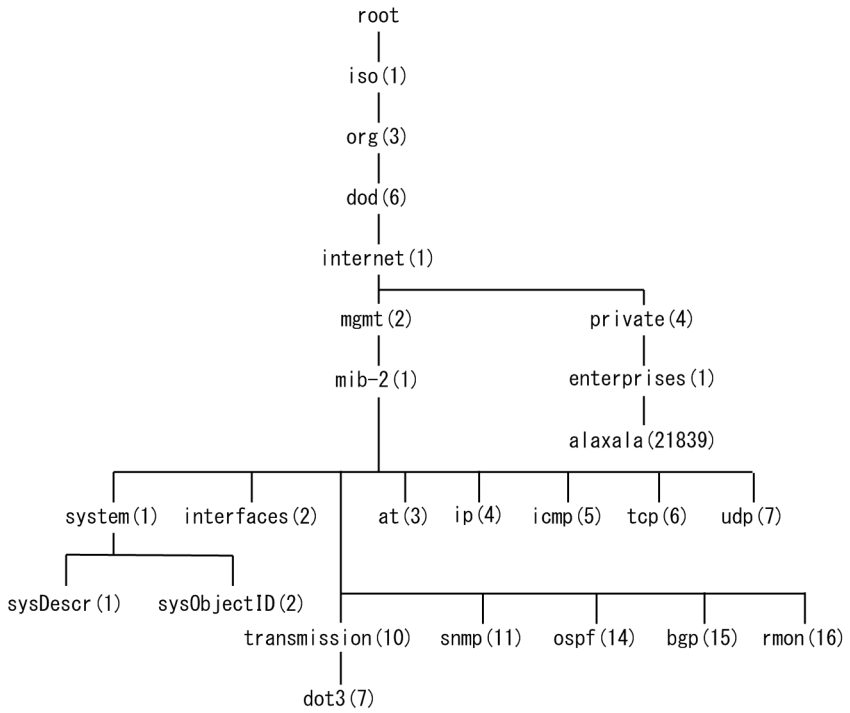
装置が管理し，SNMP マネージャに提供する MIB は，RFC で規定されたものと，装置の開発ベンダーが独自に用意する情報の 2 種類があります。

RFC で規定された MIB を**標準 MIB** と呼びます。標準 MIB は規格化されているため提供情報の内容の差はあまりありません。装置の開発ベンダーが独自に用意する MIB を**プライベート MIB** と呼び，装置によって内容が異なります。ただし，MIB のオペレーション（情報の採取・設定など）は，標準 MIB，プライベート MIB で共通です。オペレーションは，装置と目的の MIB 情報を指定するだけです。装置は IP アドレスで，MIB 情報はオブジェクト ID で指定します。

(1)　MIB 構造

MIB の構造はツリー構造になっています。MIB はツリー構造のため，各ノードを識別するために番号を付けて表す決まりになっています。root から各ノードの数字を順番にたどって番号を付けることで個々の MIB 情報を一意に識別できます。この番号列をオブジェクト ID と呼びます。オブジェクト ID は root から下位のオブジェクトグループ番号をドットで区切って表現します。例えば，sysDescr という MIB をオブジェクト ID で示すと 1.3.6.1.2.1.1.1 になります。MIB ツリーの構造例を次の図に示します。

図 18-6 MIB ツリーの構造例



(2) MIB オブジェクトの表し方

オブジェクト ID は数字と.（ドット）（例：1.3.6.1.2.1.1.1）で表現します。しかし，数字の羅列ではわかりにくいため，マネージャによっては，sysDescr というニーモニックで指定できるものもあります。ニーモニックで指定する場合，SNMP マネージャがどの MIB のニーモニックを使えるか確認してから使用してください。また，本装置の SNMP コマンドで使用できるニーモニックについては，snmp lookup コマンドを実行することで確認できます。

(3) インデックス

MIB を指定するときのオブジェクト ID を使用しますが，一つの MIB に一つの意味だけある場合と一つの MIB に複数の情報がある場合があります。MIB を特定するためにはインデックス（INDEX）を使用します。インデックスは，オブジェクト ID の後ろに数字を付加して表し，何番目の情報かなどを示すために使用します。

一つの MIB に一つの意味だけがある場合，MIB のオブジェクト ID に".0"を付加して表します。一つの MIB に複数の情報がある場合，MIB のオブジェクト ID の後ろに数字を付加して何番目の情報であるか表します。例えば，インタフェースのタイプを示す MIB に ifType（1.3.6.1.2.1.2.2.1.2）があります。本装置には複数のインタフェースがあります。特定のインタフェースのタイプを調べるには，"2 番目のインタフェースのタイプ"というように具体的に指定する必要があります。MIB で指定するときは，2 番目を示すインデックス.2 を MIB の最後に付加して ifType.2（1.3.6.1.2.1.2.2.1.2.2）と表します。

インデックスの表し方は，各 MIB によって異なります。RFC などの MIB の定義で，
INDEX{ xxxxx,yyyyy,zzzzzz }となっている MIB のエントリは，xxxxx と yyyyy と zzzzzz をインデックスに持ちます。それぞれの MIB について，どのようなインデックスを取るか確認して MIB のオペレーションを行ってください。

(4)　本装置のサポート MIB

本装置では，装置の状態，インタフェースの統計情報，装置の機器情報など，管理に必要な MIB を提供しています。なお，プライベート MIB の定義（ASN.1）ファイルは，ソフトウェアとともに提供します。

各 MIB の詳細については，「MIB レファレンス」を参照してください。

18.1.3　SNMPv1，SNMPv2C オペレーション

管理データ（MIB:management information base）の収集や設定を行うため，SNMP では次に示す 4 種類のオペレーションがあります。

- GetRequest　　：指定した MIB の情報を取り出します。
- GetNextRequest：指定した次の MIB の情報を取り出します。
- GetBulkRequest：GetNextRequest の拡張版です。
- SetRequest　　：指定した MIB に値を設定します。

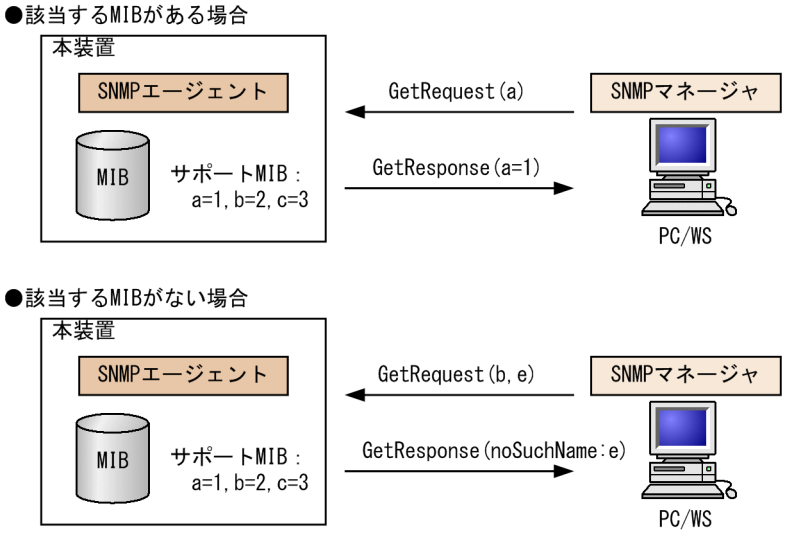
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

(1)　GetRequest オペレーション

GetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して MIB の情報を取り出すときに使用します。このオペレーションでは，一つまたは複数 MIB を指定できます。

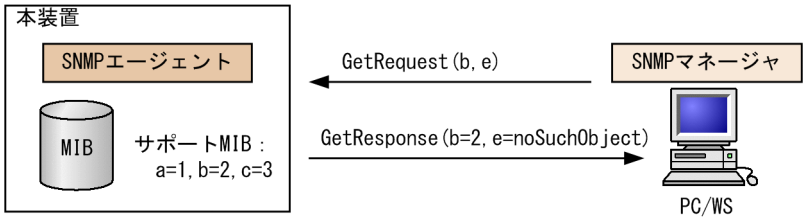
装置が該当する MIB を保持している場合，GetResponse オペレーションで MIB 情報を応答します。該当する MIB を保持していない場合は，GetResponse オペレーションで noSuchName を応答します。
GetRequest オペレーションを次の図に示します。

図 18-7　GetRequest オペレーション



SNMPv2C では，装置が該当する MIB を保持していない場合は，GetResponse オペレーションで MIB 値に noSuchObject を応答します。SNMPv2C の場合の GetRequest オペレーションを次の図に示します。

図 18-8　GetRequest オペレーション（SNMPv2C）

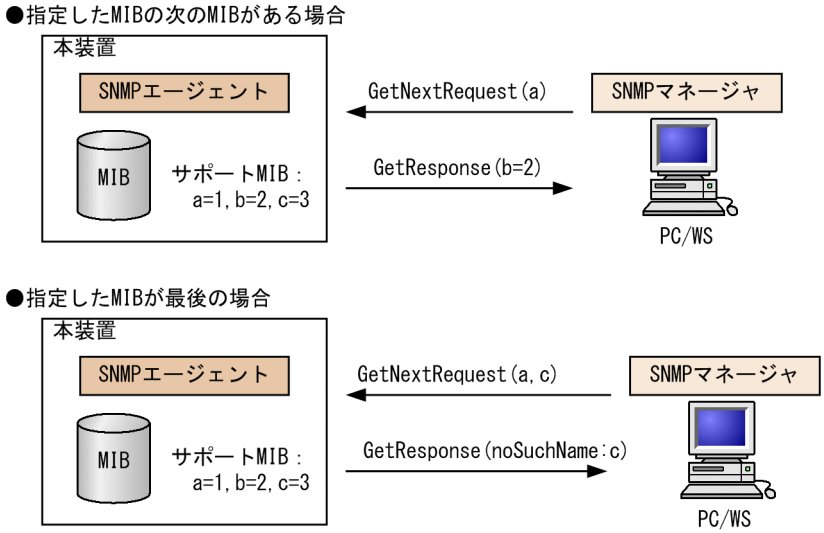


(2)　GetNextRequest オペレーション

GetNextRequest オペレーションは，GetRequest オペレーションに似たオペレーションです。GetRequest オペレーションは，指定した MIB の読み出しに使用しますが，GetNextRequest オペレーションは，指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

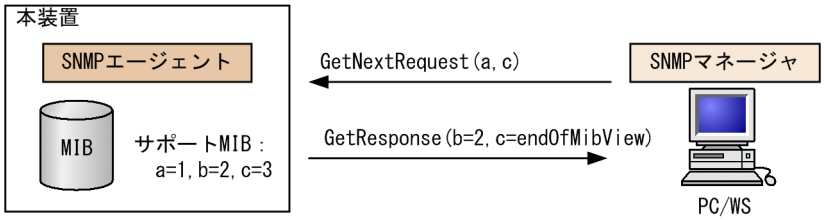
装置が指定した次の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合は，GetResponse で noSuchName を応答します。GetNextRequest オペレーションを次の図に示します。

図 18-9　GetNextRequest オペレーション



SNMPv2C の場合，指定した MIB が最後の場合は GetResponse で MIB 値に endOfMibView を応答します。SNMPv2C の場合の GetNextRequest オペレーションを次の図に示します。

図 18-10　GetNextRequest オペレーション（SNMPv2C）

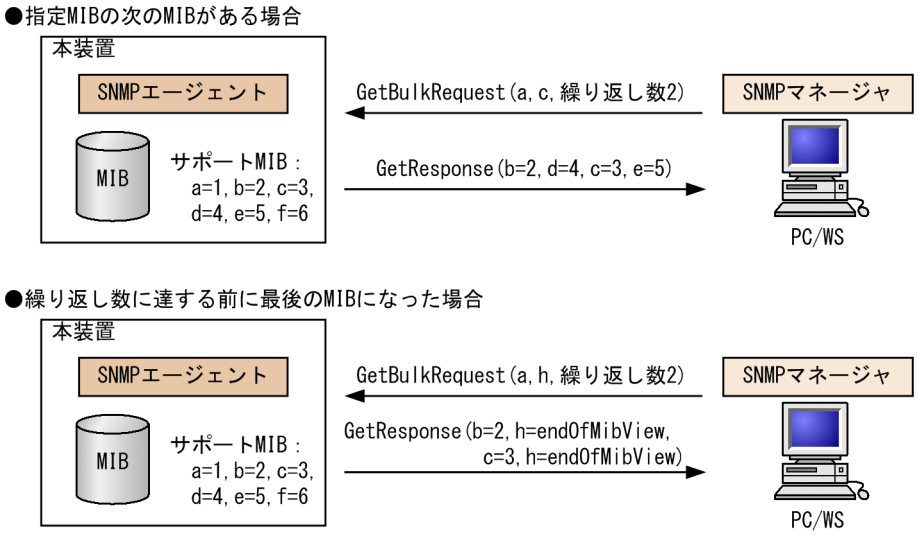


(3)　GetBulkRequest オペレーション

GetBulkRequest オペレーションは，GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも，一つまたは複数の MIB を指定できます。

装置が，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合，または繰り返し数に達する前に最後の MIB になった場合，GetResponse オペレーションで MIB 値に endOfMibView を応答します。GetBulkRequest オペレーションを次の図に示します。

図 18-11　GetBulkRequest オペレーション

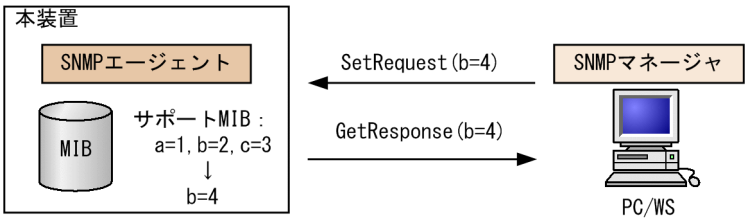


(4)　SetRequest オペレーション

SetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して行うオペレーションという点で GetRequest，GetNextRequest，GetBulkRequest オペレーションと似ていますが，値の設定方法が異なります。

SetRequest オペレーションでは，設定する値と MIB を指定します。値を設定すると，GetResponse オペレーションで MIB と設定値を応答します。SetRequest オペレーションを次の図に示します。

図 18-12　SetRequest オペレーション



(a)　MIB を設定できない場合の応答

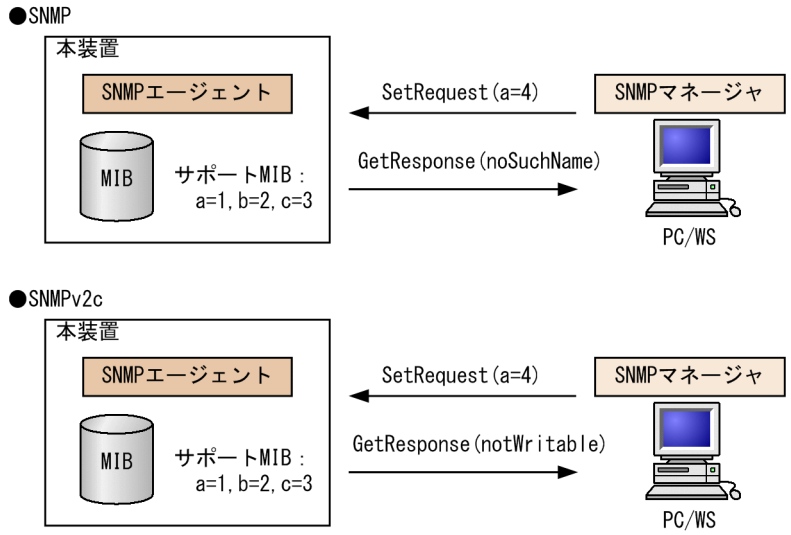
MIB を設定できないケースは，次に示す 3 とおりです。

- MIB が読み出し専用の場合（読み出し専用コミュニティに属するマネージャの場合も含む）

- 設定値が正しくない場合
- 装置の状態によって設定できない場合

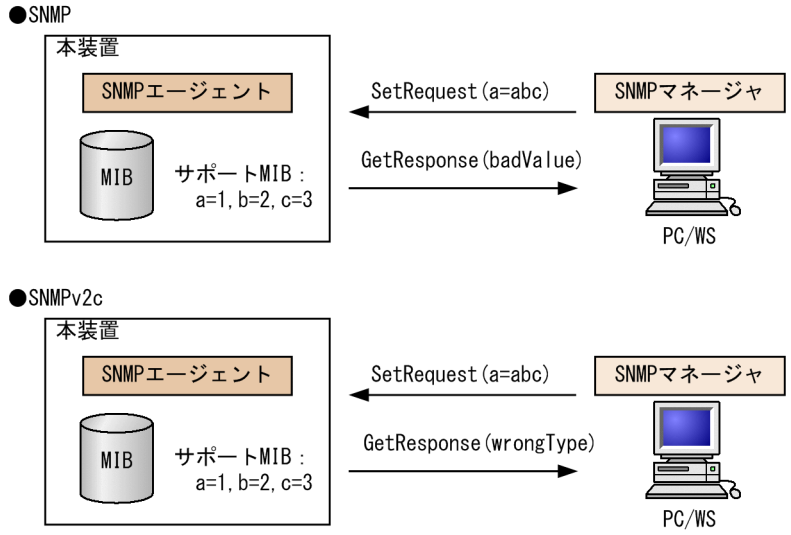
各ケースによって，応答が異なります。MIB が読み出し専用の場合，noSuchName の GetResponse 応答をします。SNMPv2C の場合，MIB が読み出し専用のときは notWritable の GetResponse 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 18-13　MIB 変数が読み出し専用の場合の SetRequest オペレーション



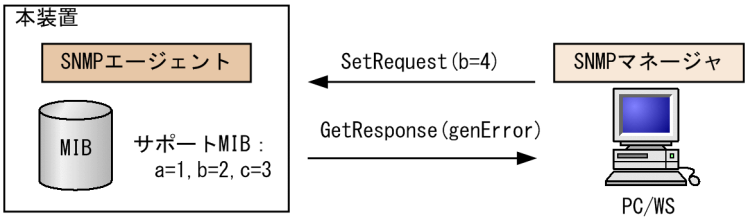
設定値のタイプが正しくない場合，badValue の GetResponse 応答をします。SNMPv2C の場合，設定値のタイプが正しくないときは wrongType の GetResponse 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 18-14　設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合，genError を応答します。例えば，装置内で値を設定しようとしたときに，装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

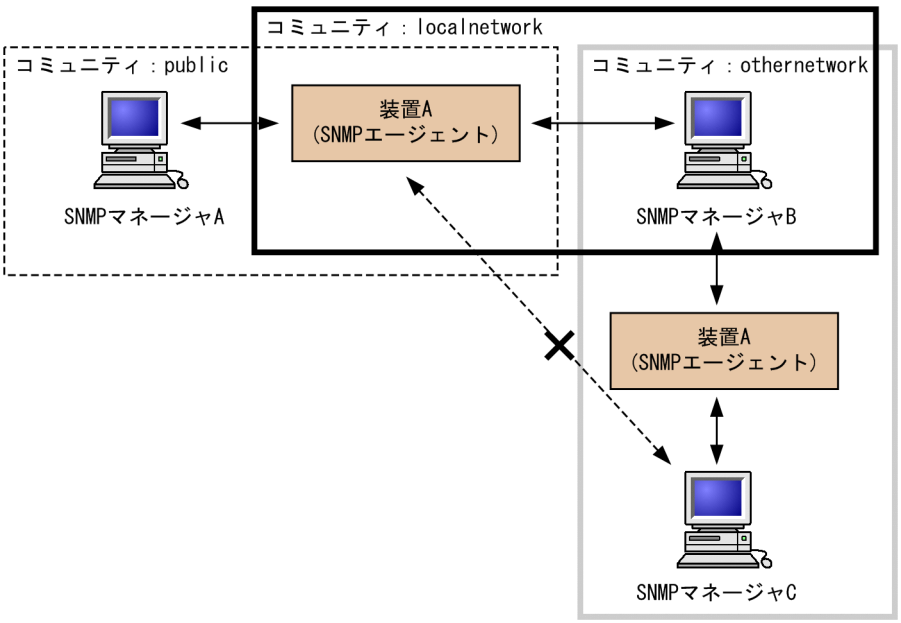
図 18-15　装置の状態によって設定できない場合の SetRequest オペレーション



(5)　コミュニティによるオペレーション制限

SNMPv1 および SNMPv2C では，オペレーションを実行する SNMP マネージャを限定するため，コミュニティという概念があります。コミュニティはオペレーションを実行する SNMP マネージャと SNMP エージェントを一つのグループとして割り当てる名称です。MIB に対してオペレーションする場合は，SNMP マネージャと SNMP エージェントは，同一のグループ（コミュニティ）に属する必要があります。コミュニティによるオペレーションを次の図に示します。

図 18-16　コミュニティによるオペレーション



装置 A はコミュニティ（public）およびコミュニティ（localnetwork）に属しています。コミュニティ（othernetwork）には属していません。この場合，装置 A はコミュニティ（public）およびコミュニティ（localnetwork）の SNMP マネージャ A，B から MIB のオペレーションを受け付けますが，コミュニティ（othernetwork）の SNMP マネージャ C からのオペレーションは受け付けません。

(6)　IP アドレスによるオペレーション制限

本装置では，セキュリティを考慮し，アクセスリストを使用することでコミュニティと SNMP マネージャの IP アドレスの組み合わせが合わないときは MIB のオペレーションを受け付けないようにできます。本装置で SNMPv1 および SNMPv2C を使用するときは，コミュニティをコンフィグレーションコマンドで登録する必要があります。なお，コミュニティは文字列で設定します。また，一般的にコミュニティ名称は，public を使用している場合が多いです。

(7) SNMP オペレーションのエラーステータスコード

オペレーションでエラーが発生した場合，SNMP エージェントはエラーステータスにエラーコードを設定し，何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した GetResponse オペレーションの応答を返します。オペレーションの結果が正常なら，エラーステータスにエラーなしのコードを設定し，MIB 情報内にオペレーションした MIB 情報を設定した GetResponse オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 18-1 エラーステータスコード

エラーステータス	コード	内容
noError	0	エラーはありません。
tooBig	1	データサイズが大きく PDU に値を設定できません。
noSuchName	2	指定 MIB がない，または書き込みできませんでした。
badValue	3	設定値が不正です。
readOnly	4	書き込みできませんでした(本装置では，応答することはありません)。
genError	5	その他のエラーが発生しました。
noAccess	6	アクセスできない MIB に対して set を行おうとしました。
wrongType	7	MIB で必要なタイプと異なるタイプが指定されました。
wrongLength	8	MIB で必要なデータ長と異なる長さが指定されました。
wrongEncoding	9	ASN.1 符号が不正でした。
wrongValue	10	MIB 値が不正でした。
noCreation	11	該当する MIB が存在しません。
inconsistentValue	12	現在何か理由があって値が設定できません。
resourceUnavailable	13	値の設定のためにリソースが必要ですが，リソースが利用できません。
commitFailed	14	値の更新に失敗しました。
undoFailed	15	値の更新に失敗したときに，更新された値を元に戻すのに失敗しました。
notWritable	17	セットできません。
inconsistentName	18	該当する MIB が存在しないため，現在は作成できません。

18.1.4 SNMPv3 オペレーション

管理データ（MIB:management information base）の収集や設定を行うため，SNMP では次に示す四種類のオペレーションがあります。

- GetRequest ：指定した MIB の情報を取り出します。
- GetNextRequest：指定した次の MIB の情報を取り出します。
- GetBulkRequest：GetNextRequest の拡張版です。
- SetRequest ：指定した MIB に値を設定します。

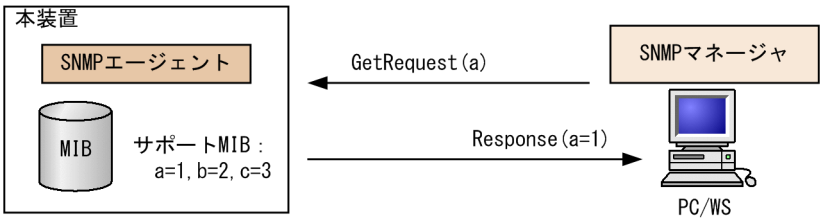
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

(1)　GetRequest オペレーション

GetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して MIB の情報を取り出すときに使用します。このオペレーションでは，一つまたは複数の MIB を指定できます。装置が該当する MIB を保持している場合，Response オペレーションで MIB 情報を応答します。

GetRequest オペレーションを次の図に示します。

図 18-17　GetRequest オペレーション

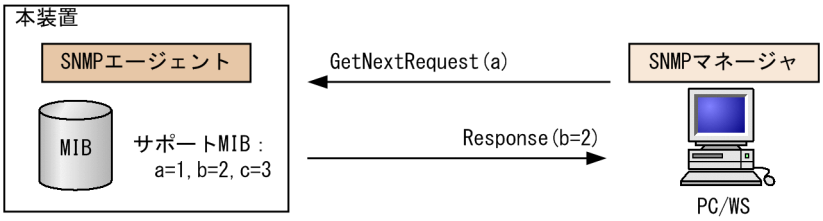


(2)　GetNextRequest オペレーション

GetNextRequest オペレーションは，GetRequest オペレーションに似たオペレーションです。GetRequest オペレーションが指定した MIB の読み出しに使用するのに対し，GetNextRequest オペレーションは指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

GetNextRequest オペレーションを次の図に示します。

図 18-18　GetNextRequest オペレーション

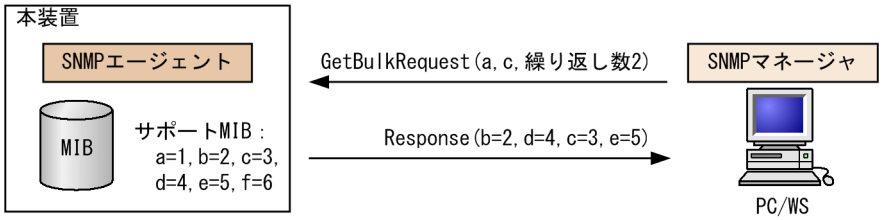


(3)　GetBulkRequest オペレーション

GetBulkRequest オペレーションは，GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも，一つまたは複数の MIB を指定できます。

GetBulkRequest オペレーションを次の図に示します。

図 18-19　GetBulkRequest オペレーション



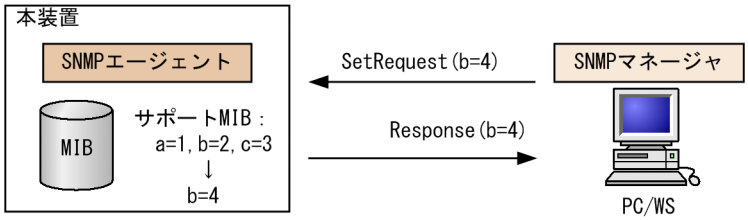
(4)　SetRequest オペレーション

SetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して行うオペレーションという点で GetRequest，GetNextRequest，GetBulkRequest オペレーションと似ていますが，値の設定方法が異なります。

SetRequest オペレーションでは，設定する値と MIB を指定します。値を設定すると，Response オペレーションで MIB と設定値を応答します。

SetRequest オペレーションを次の図に示します。

図 18-20　SetRequest オペレーション



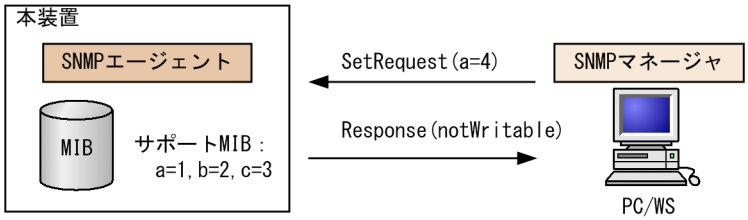
(a)　MIB を設定できない場合の応答

MIB を設定できないケースは，次に示す 3 とおりです。

- MIB が読み出し専用の場合
- 設定値が正しくない場合
- 装置の状態によって設定できない場合

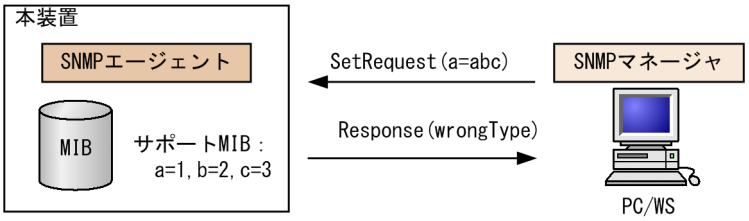
各ケースによって，応答が異なります。MIB が読み出し専用のときは notWritable の Response 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 18-21　MIB 変数が読み出し専用の場合の SetRequest オペレーション



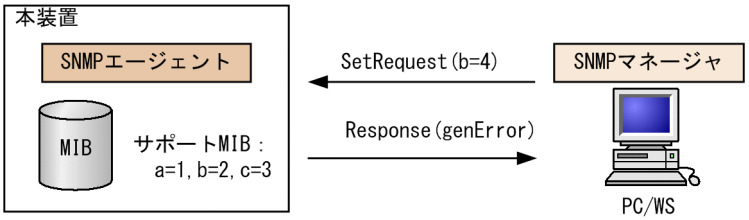
設定値のタイプが正しくないときは wrongType の Response 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 18-22　設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合，genError を応答します。例えば，装置内で値を設定しようとしたときに，装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

図 18-23　装置の状態によって設定できない場合の SetRequest オペレーション



(5)　SNMPv3 でのオペレーション制限

SNMPv1 および SNMPv2C ではコミュニティと SNMP マネージャの IP アドレスの組み合わせによって確認が行われるのに対し，SNMPv3 ではユーザ認証と MIB ビューによって MIB のオペレーションを制限します。本装置で SNMPv3 を使用するときは，SNMP セキュリティユーザ，MIB ビューおよびセキュリティグループをコンフィグレーションコマンドで登録する必要があります。また，トラップを送信するには，SNMP セキュリティユーザ，MIB ビュー，セキュリティグループ，およびトラップ送信 SNMP マネージャをコンフィグレーションコマンドで登録する必要があります。

(6)　SNMPv3 オペレーションのエラーステータスコード

オペレーションの結果エラーが発生した場合，SNMP エージェントはエラーステータスにエラーコードを設定し，何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した Response オペレーションの応答を返します。オペレーションの結果が正常であれば，エラーステータスにエラーなしのコードを設定し，MIB 情報内にオペレーションした MIB 情報を設定した Response オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 18-2　エラーステータスコード

エラーステータス	コード	内容
noError	0	エラーはありません。
tooBig	1	データサイズが大きく PDU に値を設定できません。
noSuchName	2	指定 MIB がない，または書き込みできませんでした。
badValue	3	設定値が不正です。
readOnly	4	書き込みできませんでした(本装置では，応答することはありません)。
genError	5	その他のエラーが発生しました。

エラーステータス	コード	内容
noAccess	6	アクセスできない MIB に対して set を行おうとしました。
wrongType	7	MIB で必要なタイプと異なるタイプが指定されました。
wrongLength	8	MIB で必要なデータ長と異なる長さが指定されました。
wrongEncoding	9	ASN.1 符号が不正でした。
wrongValue	10	MIB 値が不正でした。
noCreation	11	該当する MIB が存在しません。
inconsistentValue	12	現在何か理由があって値が設定できません。
resourceUnavailable	13	値の設定のためにリソースが必要ですが，リソースが利用できません。
commitFailed	14	値の更新に失敗しました。
undoFailed	15	値の更新に失敗したときに，更新された値を元に戻すのに失敗しました。
authorizationError	16	認証に失敗しました。
notWritable	17	セットできません。
inconsistentName	18	該当する MIB が存在しないため，現在は作成できません。

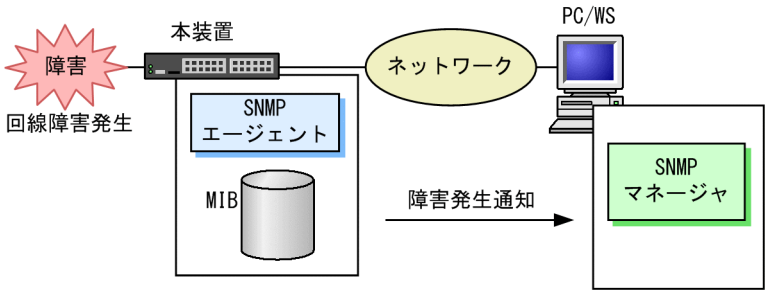
18.1.5　トラップ

(1)　トラップ概説

SNMP エージェントは**トラップ**（Trap）と呼ばれるイベント通知（主に障害発生の情報やログ情報など）機能があります。トラップは重要なイベントを SNMP エージェントから SNMP マネージャに非同期に通知する機能です。SNMP マネージャは，トラップを受信することで装置の状態変化を検知できます。この通知を基に，装置内の MIB を取得して，さらに詳細な情報を得ることができます。

なお，トラップは UDP を使用しているため，装置から SNMP マネージャに対するトラップの到達が確認できません。そのため，ネットワークの輻輳などによってトラップがマネージャに到達しない場合があります。トラップの例を次の図に示します。

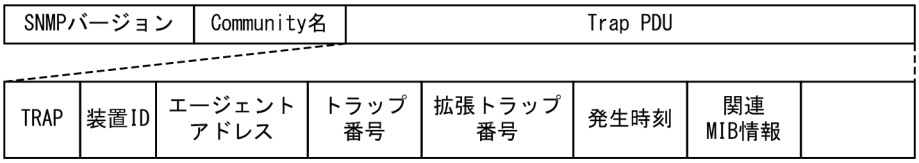
図 18-24　トラップの例



(2)　トラップフォーマット（SNMPv1）

トラップフレームには，どの IP アドレスの装置で，いつ，何が発生したかを示す情報を含みます。トラップフォーマット（SNMPv1）を次の図に示します。

図 18-25 トラップフォーマット（SNMPv1）

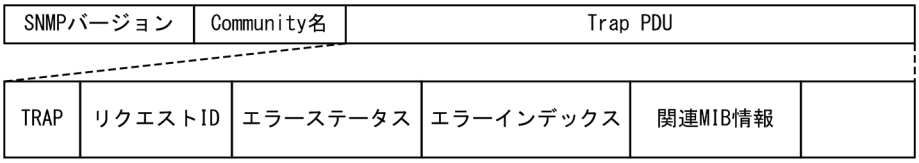


装置ID　：装置の識別ID（通常MIB-IIのsysObjectIDの値が設定される）
エージェントアドレス：トラップが発生した装置のIPアドレス
トラップ番号　：トラップの種別を示す識別番号
拡張トラップ番号　：トラップ番号の補足をするための番号
発生時刻　：トラップが発生した時間（装置が起動してからの経過時間）
関連MIB情報　：このトラップに関連するMIB情報

(3) トラップフォーマット（SNMPv2C，SNMPv3）

トラップフレームには，いつ，何が発生したかを示す情報を含みます。トラップフォーマット（SNMPv2C，SNMPv3）を次の図に示します。

図 18-26 トラップフォーマット（SNMPv2C，SNMPv3）



リクエストID　：メッセージ識別子。リクエストごとに異なる。
エラーステータス　：発生したエラーを示す値
エラーインデックス　：関連MIB情報でのエラー位置
関連MIB情報　：このトラップに関連するMIB情報

18.1.6 インフォーム

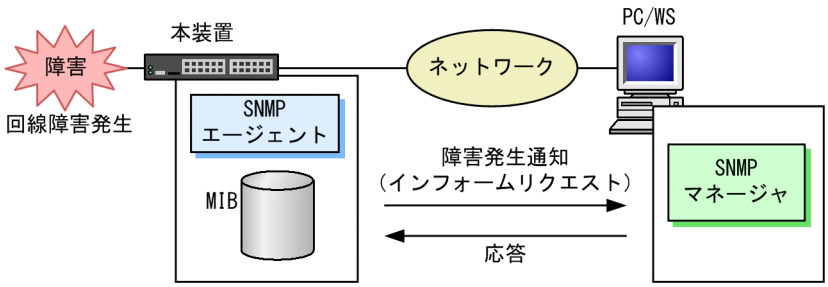
(1) インフォーム概説

SNMP エージェントは**インフォーム**（Inform）と呼ばれるイベント通知（主に障害発生の情報やログ情報など)機能があります。インフォームはインフォームリクエストを送信して，重要なイベントを SNMP エージェントから SNMP マネージャに通知する機能です。SNMP マネージャは，インフォームリクエストを受信することで装置の状態変化を検知できます。この通知を基に，装置内の MIB を取得して，さらに詳細な情報を得ることができます。

インフォームは SNMPv2C だけのサポートとなります。また，SNMP マネージャもインフォームに対応している必要があります。

なお，インフォームもトラップと同じ UDP によるイベント通知ですが，トラップとは異なって SNMP マネージャからの応答を要求します。そのため，応答の有無でインフォームリクエストの到達を確認できます。これによって，ネットワークの輻輳などに対してもインフォームリクエストの再送で対応できます。インフォームの例を次の図に示します。

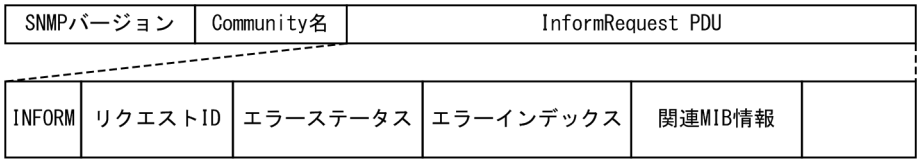
図 18-27　インフォームの例



(2)　インフォームリクエストフォーマット

インフォームリクエストフレームには，いつ，何が発生したかを示す情報を含みます。インフォームリクエストフォーマットを次の図に示します。

図 18-28　インフォームリクエストフォーマット



リクエストID　：メッセージ識別子。リクエストごとに異なる。
エラーステータス　：発生したエラーを示す値
エラーインデックス　：関連MIB情報でのエラー位置
関連MIB情報　：このインフォームリクエストに関連するMIB情報

18.1.7　RMON MIB

RMON（Remote Network Monitoring）とは，イーサネット統計情報を提供する機能，収集した統計情報の閾値チェックを行ってイベントを発生させる機能，パケットをキャプチャする機能などを持ちます。この RMON は RFC1757 で規定されています。

RMON MIB のうち，statistics，history，alarm，event の各グループについて概要を説明します。

(1)　statistics グループ

監視対象のサブネットワークについての，基本的な統計情報を収集します。例えば，サブネットワーク中の総パケット数，ブロードキャストパケットのような各種類ごとのパケット数，CRC エラー，コリジョンエラーなどのエラー数などです。statistics グループを使うと，サブネットワークのトラフィック状況や回線状態などの統計情報を取得できます。

(2)　history グループ

statistics グループで収集する情報とほぼ同じ統計情報をサンプリングし，来歴情報として保持できます。

history グループには historyControlTable という制御テーブルと，etherHistoryTable というデータテーブルがあります。historyControlTable はサンプリング間隔や来歴記録数の設定を行うための MIB です。

etherHistoryTable は，サンプリングした統計情報の来歴記録の MIB です。history グループは，一定期間の統計情報を装置内で保持しています。このため，SNMP マネージャなどが定期的にポーリングして統計情報を収集するのと比較して，ネットワークに負荷をかけることが少なく，連続した一定期間の統計情報を取得できます。

(3) alarm グループ

監視対象とする MIB のチェック間隔，閾値などを設定して，その MIB が閾値に達したときにログを記録したり，SNMP マネージャに SNMP 通知を送信したりすることを指定する MIB です。この alarm グループを使用するときは，event グループも設定する必要があります。

alarm グループによる MIB 監視には，MIB 値の差分（変動）と閾値を比較する **delta 方式**と，MIB 値と閾値を直接比較する **absolute 方式**があります。

delta 方式による閾値チェックでは，例えば，CPU 使用率の変動が 50%以上あったときに，ログを収集したり，SNMP マネージャに SNMP 通知を送信したりできます。absolute 方式による閾値チェックでは，例えば，CPU の使用率が 80%に達したときに，ログを収集したり，SNMP マネージャに SNMP 通知を送信したりできます。

本装置では，閾値をチェックするタイミングによる検出漏れをできるだけ防止するために，alarmInterval（MIB 値を監視する時間間隔（秒）を表す MIB）の間に複数回チェックします。alarmInterval ごとの閾値チェック回数を次の表に示します。

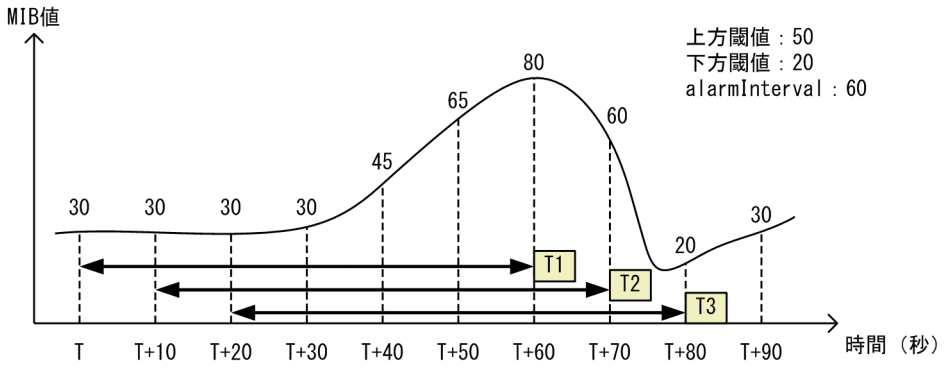
表 18-3 alarmInterval ごとの閾値チェック回数

alarmInterval（秒）	閾値チェック回数
1	1
2～5	2
6～10	3
11～20	4
21～50	5
51～100	6
101～200	7
201～400	8
401～800	9
801～1300	10
1301～2000	11
2001～4294967295	12

閾値のチェックは，およそ alarmInterval を閾値チェック回数で割った秒数ごとに行います。例えば，alarmInterval が 60（秒）の場合，閾値チェック回数は 6 回になるため，10 秒に 1 回のタイミングで閾値をチェックします。

上方閾値を 50，下方閾値を 20，alarmInterval を 60 として，CPU 使用率の MIB 値を delta 方式で監視した場合の例を次の図に示します。

図 18-29　delta 方式による MIB 監視例



T1

閾値と比較する値が 50（T+60（秒）の MIB 値 80－T（秒）の MIB 値 30）のため，上方閾値以上を検出

T2

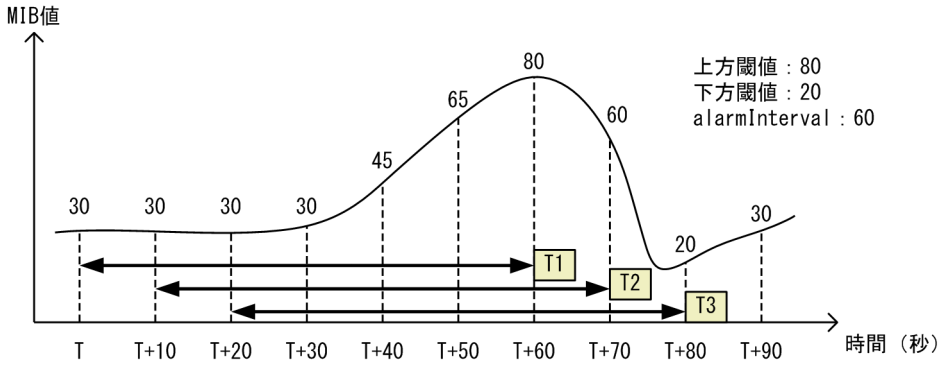
閾値と比較する値が 30（T+70（秒）の MIB 値 60－T+10（秒）の MIB 値 30）のため，閾値検出なし

T3

閾値と比較する値が-10（T+80（秒）の MIB 値 20－T+20（秒）の MIB 値 30）のため，下方閾値以下を検出

上方閾値を 80，下方閾値を 20，alarmInterval を 60 として，CPU 使用率の MIB 値を absolute 方式で監視した場合の例を次の図に示します。

図 18-30　absolute 方式による MIB 監視例



T1

閾値と比較する値が 80（T+60（秒）の MIB 値）のため，上方閾値以上を検出

T2

閾値と比較する値が 60（T+70（秒）の MIB 値）のため，閾値検出なし

T3

閾値と比較する値が 20（T+80（秒）の MIB 値）のため，下方閾値以下を検出

(4) event グループ

event グループには alarm グループで設定した MIB の閾値を超えたときの動作を指定する eventTable グループ MIB と閾値を超えたときにログを記録する logTable グループ MIB があります。

eventTable グループ MIB は，閾値に達したときにログを記録するのか，SNMP マネージャに SNMP 通知を送信するのか，またはその両方するか何もしないかを設定するための MIB です。

logTable グループ MIB は，eventTable グループ MIB でログの記録を指定したときに，装置内にログを記録します。装置内のログのエントリ数は決まっているので，エントリをオーバーした場合，新しいログ情報の追加によって，古いログ情報が消去されていきます。定期的に SNMP マネージャに記録を退避しないと，前のログが消されてしまう可能性がありますので注意してください。

18.1.8 SNMP マネージャとの接続時の注意事項

(1) MIB 情報収集周期のチューニング

SNMP マネージャは，ネットワーク上の新しい装置を検出したり，トラフィック状況を監視したりするため，SNMP エージェントサポート機器から定期的に MIB を取得します。この定期的な MIB 取得の間隔が短いと，ネットワーク機器やネットワークに負荷が掛かります。また，装置の状態や構成などによって，MIB 取得時にマネージャ側でタイムアウトが発生するおそれがあります。特に，次に示すケースでは応答タイムアウトの発生するおそれが高まります。

- 接続 SNMP マネージャ数が多い場合
  本装置に SNMP マネージャが多数接続され，MIB 情報の収集が集中した場合。
- SNMP イベントが同時に多数発生している場合
  本装置から大量に SNMP 通知が送信されるような状態のときに，MIB を取得した場合や，本装置から送信された SNMP 通知に基づいて，並行して MIB を取得した場合。

応答タイムアウトが頻発する場合は，SNMP マネージャのポーリング周期や応答監視タイマ値をチューニングしてください。代表的な SNMP マネージャのチューニングパラメータには，次の三つがあります。

- ポーリング周期
- 応答監視タイマ
- 応答監視タイムアウト時のリトライ回数

18.2 コンフィグレーション

18.2.1 コンフィグレーションコマンド一覧

SNMP/RMON に関するコンフィグレーションコマンド一覧を次の表に示します。

表 18-4 コンフィグレーションコマンド一覧

コマンド名	説明
hostname	本装置のホスト名称を設定します。本設定は RFC1213 の sysName に対応します。
rmon alarm	RMON（RFC1757)アラームグループの制御情報を設定します。
rmon collection history	RMON（RFC1757)イーサネットの統計来歴の制御情報を設定します。
rmon event	RMON（RFC1757)イベントグループの制御情報を設定します。
snmp-server community	SNMP コミュニティに対するアクセスリストを設定します。
snmp-server contact	本装置の連絡先などを設定します。本設定は RFC1213 の sysContact に対応します。
snmp-server engineID local	SNMP エンジン ID 情報を設定します。
snmp-server group	SNMP セキュリティグループ情報を設定します。
snmp-server host	SNMP 通知を送信する宛先のネットワーク管理装置（SNMP マネージャ）を登録します。
snmp-server informs	インフォームの再送条件を設定します。
snmp-server location	本装置を設置する場所の名称を設定します。本設定は RFC1213 の sysLocation に対応します。
snmp-server traps	SNMP 通知の送信契機を設定します。
snmp-server user	SNMP セキュリティユーザ情報を設定します。
snmp-server view	MIB ビュー情報を設定します。
snmp trap link-status	回線がリンクアップまたはダウンした場合に，SNMP 通知（linkUp または LinkDown）の送信を抑止します。

18.2.2 SNMPv1，SNMPv2C による MIB アクセス許可の設定

[設定のポイント]

SNMP マネージャから本装置の MIB へのアクセスを許可するための設定をします。

[コマンドによる設定]

1. **(config)# access-list 1 permit 10.1.1.1 0.0.0.0**

   IP アドレス 10.1.1.1 からのアクセスを許可するアクセスリストの設定を行います。

2. **(config)# snmp-server community "NETWORK" ro 1**

   SNMP マネージャのコミュニティに対する MIB アクセスモードおよび適用するアクセスリストを設定します。

- コミュニティ名：NETWORK
- アクセスリスト：1
- アクセスモード：read only

18.2.3 SNMPv3 による MIB アクセス許可の設定

[設定のポイント]

SNMPv3 で MIB にアクセスするために，アクセスを許可する MIB オブジェクトの集合を MIB ビューとして設定し，ユーザ認証と暗号化機能の情報を SNMP セキュリティユーザとして設定します。また，MIB ビューと SNMP セキュリティユーザを関連づけるために，SNMP セキュリティグループを設定します。

[コマンドによる設定]

1. **(config)# snmp-server view "READ_VIEW" 1.3.6.1 included**
   (config)# snmp-server view "READ_VIEW" 1.3.6.1.6.3 excluded
   (config)# snmp-server view "WRITE_VIEW" 1.3.6.1.2.1.1 included
   MIB ビューを設定します。
   - ビュー名 READ_VIEW に internet グループ MIB（サブツリー：1.3.6.1）を登録します。
   - ビュー名 READ_VIEW から snmpModules グループ MIB（サブツリー：1.3.6.1.6.3）を対象外にします。
   - ビュー名 WRITE_VIEW に system グループ MIB（サブツリー：1.3.6.1.2.1.1）を登録します。
2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"**
   SNMP セキュリティユーザを設定します。
   - SNMP セキュリティユーザ名：ADMIN
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - 認証プロトコル：HMAC-MD5
   - 認証パスワード：ABC*_1234
   - プライバシープロトコル：CBC-DES
   - プライバシーパスワード：XYZ/+6789
3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv read "READ_VIEW" write "WRITE_VIEW"**
   SNMP セキュリティグループを設定します。
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - セキュリティレベル：認証あり，暗号化あり
   - Read ビュー名：READ_VIEW
   - Write ビュー名：WRITE_VIEW

18.2.4 SNMPv1，SNMPv2C によるトラップ送信の設定

[設定のポイント]

トラップを送信する宛先の SNMP マネージャを登録します。

[コマンドによる設定]

1. **(config)# snmp-server host 10.1.1.1 traps "NETWORK" version 1 snmp**
   SNMP マネージャに標準トラップを送信する設定をします。
   - コミュニティ名：NETWORK
   - SNMP マネージャの IP アドレス：10.1.1.1
   - 送信するトラップ：coldStart，warmStart，linkDown，linkUp，authenticationFailure

18.2.5 SNMPv3 によるトラップ送信の設定

[設定のポイント]

MIB ビューと SNMP セキュリティユーザを設定の上，SNMP セキュリティグループを設定し，さらに SNMP トラップモードを設定します。

[コマンドによる設定]

1. **(config)# snmp-server view "ALL_TRAP_VIEW" * included**
   MIB ビューを設定します。
   - ビュー名 ALL_TRAP_VIEW に全サブツリーを登録します。
2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"**
   SNMP セキュリティユーザを設定します。
   - SNMP セキュリティユーザ名：ADMIN
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - 認証プロトコル：HMAC-MD5
   - 認証パスワード：ABC*_1234
   - プライバシープロトコル：CBC-DES
   - プライバシーパスワード：XYZ/+6789
3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv notify "ALL_TRAP_VIEW"**
   SNMP セキュリティグループを設定します。
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - セキュリティレベル：認証あり，暗号化あり
   - Notify ビュー名：ALL_TRAP_VIEW
4. **(config)# snmp-server host 10.1.1.1 traps "ADMIN" version 3 priv snmp**
   SNMPv3 によって SNMP マネージャに標準トラップを送信する設定をします。
   - SNMP マネージャの IP アドレス：10.1.1.1
   - SNMP セキュリティユーザ名：ADMIN
   - セキュリティレベル：認証あり，暗号化あり
   - 送信するトラップ：coldStart，warmStart，linkDown，linkUp，authenticationFailure

18.2.6　SNMPv2C によるインフォーム送信の設定

[設定のポイント]

インフォームを送信する宛先の SNMP マネージャを登録します。

[コマンドによる設定]

1. **(config)# snmp-server host 10.1.1.1 informs "NETWORK" version 2c snmp**

   SNMP マネージャに標準のインフォームを送信する設定をします。

   - コミュニティ名：NETWORK
   - SNMP マネージャの IP アドレス：10.1.1.1
   - 送信するインフォーム：coldStart，warmStart，linkDown，linkUp，authenticationFailure

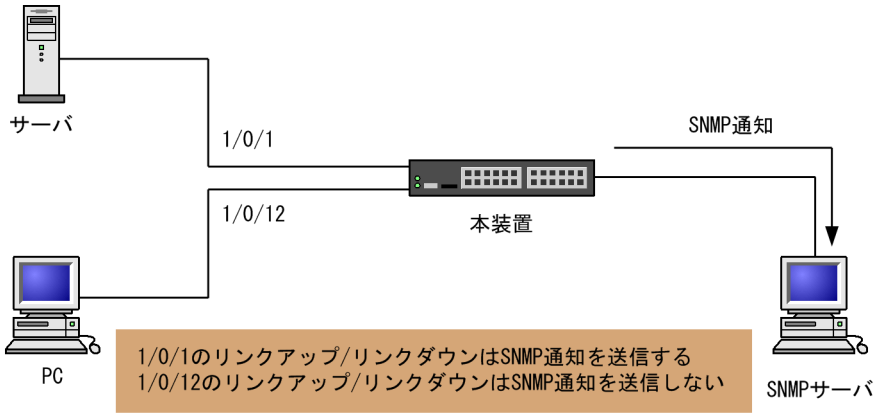
18.2.7　リンクトラップの抑止

本装置は，デフォルト動作としてイーサネットインタフェースがリンクアップまたはリンクダウンしたときに，SNMP 通知（linkUp または linkDown）を送信します。これをリンクトラップと呼びます。また，コンフィグレーションによって，イーサネットインタフェースごとに，リンクトラップの送信抑止を設定できます。例えば，サーバと接続する回線のように重要度の高い回線だけ SNMP 通知を送信し，そのほかの回線のリンクトラップの送信を抑止することで，本装置，ネットワーク，および SNMP マネージャの不要な処理を削減できます。

[設定のポイント]

リンクトラップの設定内容はネットワーク全体の運用方針に従って決定します。

図 18-31　リンクトラップの構成図



ここでは，ポート 1/0/1 については，SNMP 通知を送信するので，コンフィグレーションの設定は必要ありません。ポート 1/0/12 については，SNMP 通知を送信しないように設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/12**

   (config-if)# no snmp trap link-status

   リンクアップ／リンクダウン時に SNMP 通知を送信しません。

2. **(config-if)# exit**

18.2.8 RMON イーサネットヒストリグループの制御情報の設定

[設定のポイント]

RMON（RFC1757）イーサネットの統計来歴の制御情報を設定します。本コマンドでは最大 32 エントリの設定ができます。あらかじめ SNMP マネージャを登録しておく必要があります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/5**
   ギガビット・イーサネットインタフェース 1/0/5 のインタフェースモードに遷移します。
2. **(config-if)# rmon collection history controlEntry 33 owner "NET-MANAGER" buckets 10**
   統計来歴の制御情報の情報識別番号，設定者の識別情報，および統計情報を格納する来歴エントリ数を設定します。
   - 情報識別番号：33
   - 来歴情報の取得エントリ：10 エントリ
   - 設定者の識別情報：”NET-MANAGER”

18.2.9 RMON による特定 MIB 値の閾値チェック

[設定のポイント]

特定の MIB の値に対して定期的に閾値チェックを行い，閾値を超えたら SNMP マネージャにイベントを通知するように設定します。

イベント実行方法に trap を指定する場合は，あらかじめ SNMP トラップモードの設定が必要です。

[コマンドによる設定]

1. **(config)# rmon event 3 log trap public**
   アラームが発生したときに実行するイベントを設定します。
   - 情報識別番号：3
   - イベント実行方法：log，trap
   - SNMP 通知先コミュニティ名：public
2. **(config)# rmon alarm 12 "ifOutDiscards.3" 256111 delta rising-threshold 400000 rising-event-index 3 falling-threshold 100 falling-event-index 3 owner "NET-MANAGER"**
   RMON アラームグループの制御情報を次の条件で設定します。
   - RMON アラームグループの制御情報識別番号：12
   - 閾値チェックを行う MIB のオブジェクト識別子：ifOutDiscards.3
   - 閾値チェックを行う時間間隔：256111 秒
   - 閾値チェック方式：差分値チェック（delta）
   - 上方閾値の値：400000
   - 上方閾値を超えたときのイベント方法の識別番号：3
   - 下方閾値の値：100
   - 下方閾値を超えたときのイベント方法の識別番号：3

- コンフィグレーション設定者の識別情報：NET-MANAGER

18.2.10 SNMPv1, SNMPv2C による VRF からの MIB アクセス許可の設定【SL-L3A】

[設定のポイント]

VRF に存在する SNMP マネージャから本装置の MIB へのアクセスを許可するための設定をします。

[コマンドによる設定]

1. **(config)# access-list 2 permit 10.1.1.1 0.0.0.0**
   IP アドレス 10.1.1.1 からのアクセスを許可するアクセスリストを設定します。
2. **(config)# snmp-server community "NETWORK" ro 2 vrf 2**
   SNMP マネージャのコミュニティに対する MIB アクセスモードおよび適用するアクセスリストを設定します。
   - コミュニティ名：NETWORK
   - アクセスリスト：2
   - アクセスモード：read only
   - VRF ID：2

18.2.11 SNMPv3 による VRF からの MIB アクセス許可の設定【SL-L3A】

[設定のポイント]

SNMPv3 で MIB にアクセスするために，アクセスを許可する MIB オブジェクトの集合を MIB ビューとして設定し，ユーザ認証と暗号化機能の情報，およびアクセスを許可する VRF ID を SNMP セキュリティユーザとして設定します。また, MIB ビューと SNMP セキュリティユーザを関連づけるために, SNMP セキュリティグループを設定します。

[コマンドによる設定]

1. **(config)# snmp-server view "READ_VIEW" 1.3.6.1 included**
   (config)# snmp-server view "READ_VIEW" 1.3.6.1.6.3 excluded
   (config)# snmp-server view "WRITE_VIEW" 1.3.6.1.2.1.1 included
   MIB ビューを設定します。
   - ビュー名 READ_VIEW に internet グループ MIB（サブツリー：1.3.6.1）を登録します。
   - ビュー名 READ_VIEW から snmpModules グループ MIB（サブツリー：1.3.6.1.6.3）を対象外にします。
   - ビュー名 WRITE_VIEW に system グループ MIB（サブツリー：1.3.6.1.2.1.1）を登録します。
2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789" vrf 2**
   SNMP セキュリティユーザを設定します。
   - SNMP セキュリティユーザ名：ADMIN
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - 認証プロトコル：HMAC-MD5

- 認証パスワード：ABC*_1234
- プライバシープロトコル：CBC-DES
- プライバシーパスワード：XYZ/+6789
- VRF ID：2

3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv read "READ_VIEW" write "WRITE_VIEW"**
   SNMP セキュリティグループを設定します。
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - セキュリティレベル：認証あり，暗号化あり
   - Read ビュー名：READ_VIEW
   - Write ビュー名：WRITE_VIEW

18.2.12 SNMPv1，SNMPv2C による VRF へのトラップ送信の設定【SL-L3A】

[設定のポイント]

VRF に存在する SNMP マネージャに対して，トラップを送信する設定をします。

[コマンドによる設定]

1. **(config)# snmp-server host 10.1.1.1 vrf 2 traps "NETWORK" version 1 snmp**
   SNMP マネージャに標準トラップを送信する設定をします。
   - コミュニティ名：NETWORK
   - SNMP マネージャの IP アドレス：10.1.1.1
   - 送信するトラップ：coldStart，warmStart，linkDown，linkUp，authenticationFailure
   - VRF ID：2

18.2.13 SNMPv3 による VRF へのトラップ送信の設定【SL-L3A】

[設定のポイント]

MIB ビューと SNMP セキュリティユーザを設定の上，SNMP セキュリティグループを設定し，さらに SNMP トラップモードを設定します。SNMP セキュリティユーザで登録する VRF ID と SNMP トラップモードで設定する VRF ID は，同一である必要があります。

[コマンドによる設定]

1. **(config)# snmp-server view "ALL_TRAP_VIEW" * included**
   MIB ビューを設定します。
   - ビュー名 ALL_TRAP_VIEW に全サブツリーを登録します。
2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789" vrf 2**
   SNMP セキュリティユーザを設定します。
   - SNMP セキュリティユーザ名：ADMIN
   - SNMP セキュリティグループ名：ADMIN_GROUP

- 認証プロトコル：HMAC-MD5
- 認証パスワード：ABC*_1234
- プライバシープロトコル：CBC-DES
- プライバシーパスワード：XYZ/+6789
- VRF ID：2

3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv notify "ALL_TRAP_VIEW"**
   SNMP セキュリティグループを設定します。
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - セキュリティレベル：認証あり，暗号化あり
   - Notify ビュー名：ALL_TRAP_VIEW
4. **(config)# snmp-server host 10.1.1.1 vrf 2 traps "ADMIN" version 3 priv snmp**
   SNMPv3 によって SNMP マネージャに標準トラップを送信する設定をします。
   - SNMP マネージャの IP アドレス：10.1.1.1
   - SNMP セキュリティユーザ名：ADMIN
   - セキュリティレベル：認証あり，暗号化あり
   - 送信するトラップ：coldStart，warmStart，linkDown，linkUp，authenticationFailure
   - VRF ID：2

18.2.14 SNMPv2C による VRF へのインフォーム送信の設定【SL-L3A】

[設定のポイント]

VRF に存在する SNMP マネージャに対して，インフォームを送信する設定をします。

[コマンドによる設定]

1. **(config)# snmp-server host 10.1.1.1 vrf 2 informs "NETWORK" version 2c snmp**
   SNMP マネージャに標準のインフォームを送信する設定をします。
   - コミュニティ名：NETWORK
   - SNMP マネージャの IP アドレス：10.1.1.1
   - 送信するインフォーム：coldStart，warmStart，linkDown，linkUp，authenticationFailure
   - VRF ID：2

18.3 オペレーション

18.3.1 運用コマンド一覧

SNMP/RMON に関する運用コマンド一覧を次の表に示します。

表 18-5 運用コマンド一覧

コマンド名	説明
show snmp	SNMP 情報を表示します。
show snmp pending	送信を保留中のインフォームリクエストを表示します。
snmp lookup	サポート MIB オブジェクト名称およびオブジェクト ID を表示します。
snmp get	指定した MIB の値を表示します。
snmp getnext	指定した次の MIB の値を表示します。
snmp walk	指定した MIB ツリーを表示します。
snmp getif	interface グループの MIB 情報を表示します。
snmp getroute	ipRouteTable（IP ルーティングテーブル）を表示します。
snmp getarp	ipNetToMediaTable（IP アドレス変換テーブル）を表示します。
snmp getforward	ipForwardTable（IP フォワーディングテーブル）を表示します。
snmp rget	指定したリモート装置の MIB の値を表示します。
snmp rgetnext	指定したリモート装置の次の MIB の値を表示します。
snmp rwalk	指定したリモート装置の MIB ツリーを表示します。
snmp rgetroute	指定したリモート装置の ipRouteTable（IP ルーティングテーブル）を表示します。
snmp rgetarp	指定したリモート装置の ipNetToMediaTable（IP アドレス変換テーブル）を表示します。

18.3.2 SNMP マネージャとの通信の確認

本装置に SNMP エージェント機能を設定して SNMP プロトコルによるネットワーク管理を行う場合，次のことを確認してください。

- ネットワーク上の SNMP マネージャから本装置に対して MIB を取得できること
- 本装置からネットワーク上の SNMP マネージャへ SNMP 通知が送信されていること，さらに，インフォームの場合は応答を受信できること

show snmp コマンドで SNMP マネージャとの通信状態を確認できます。

図 18-32 show snmp コマンドの実行結果

```
> show snmp
Date 20XX/12/27 15:06:08 UTC
Contact: Suzuki@example.com
Location: ServerRoom
SNMP packets input   : 137    (get:417 set:2)
    Get-request PDUs    : 18
```

```
    Get-next PDUs       : 104
    Get-bulk PDUs       : 0
    Set-request PDUs    : 6
    Response PDUs       : 3    (with error 0)
    Error PDUs          : 7
        Bad SNMP version errors: 1
        Unknown community name : 5
        Illegal operation      : 1
        Encoding errors        : 0

SNMP packets output : 185
    Trap PDUs           : 4
    Inform-request PDUs : 53
    Response PDUs       : 128    (with error 4)
        No errors              : 124
        Too big errors         : 0
        No such name errors    : 3
        Bad values errors      : 1
        General errors         : 0
    Timeouts            : 49
    Drops               : 0

[TRAP]
    Host: 192.168.0.1, sent:1
    Host: 192.168.0.2, sent:3

[INFORM]
    Timeout(sec)       : 10
    Retry              : 5
    Pending informs    : 1/25 (current/max)
    Host: 192.168.0.3
        sent    :8          retries:26
        response:2          pending:1          failed:5          dropped:0
    Host: 192.168.0.4
        sent    :3          retries:15
        response:0          pending:0          failed:3          dropped:0
    Host: 2001:db8::10
        sent    :1          retries:0
        response:1          pending:0          failed:0          dropped:0
```

SNMP マネージャから MIB が取得できない場合は，「SNMP packets input」の項目で，「Error PDUs」の値が増加していないこと，および PDU を受信できていることを確認してください。「Error PDUs」の値が増加しているときは，コンフィグレーションの内容を確認してください。PDU を受信できていないときは，ネットワークの設定が正しいか，また，SNMP マネージャまでの経路上で障害が発生していないかを確認してください。

SNMP マネージャで SNMP 通知が受信できない場合は，「[TRAP]」と「[INFORM]」の項目で，SNMP マネージャの IP アドレスが「Host」として設定されていることを確認してください。設定されていないときは，コンフィグレーションコマンド snmp-server host を実行して，SNMP マネージャに関する情報を設定してください。

なお，これらの方法で解決できない場合は「トラブルシューティングガイド」を参照してください。また，本装置から取得できる MIB および SNMP 通知については「MIB レファレンス」を参照してください。

19 高機能スクリプト

この章では，高機能スクリプトの使用方法について説明します。

19.1　解説

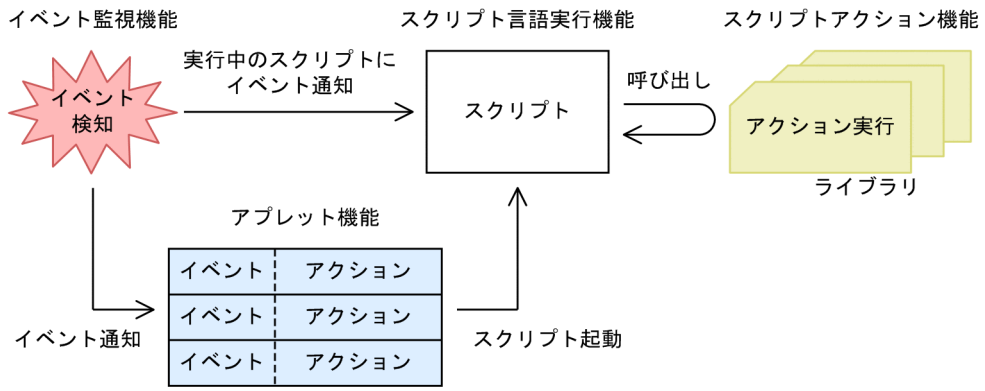
19.1.1　概要

高機能スクリプトとは，本装置のコンフィグレーションやオペレーションを，装置内でプログラミングできるようにする機能です。本機能は，次のような用途に適用できます。

- オペレーションの自動化
  例えば，運用メッセージの出力を契機として，コマンドを自動で実行できます。
- 運用機能のカスタマイズ
  例えば，ユーザが作成した運用メッセージを出力できます。

高機能スクリプトを構成する主要機能，およびそれぞれの関連性を次の図に示します。

図 19-1　高機能スクリプトを構成する主要機能



(1)　スクリプト言語実行機能

スクリプトは，本装置のコンフィグレーションやオペレーションの手順をプログラミングしたものです。スクリプト言語実行機能とは，作成したスクリプトを実行する機能です。

なお，本装置では，スクリプト言語に Python を使用します。Python は次に示す特徴を持つ言語です。

- 可読性が高い
  コードブロックをインデントでそろえるなど，記述方法を統一することで，高い可読性を持ちます。
- デバッグやプロトタイピングが容易
  Python で作成したスクリプトはインタプリタ方式で 1 行ずつ実行できるため，デバッグやプロトタイピングが容易です。
- ライブラリ提供機能の再利用が容易
  Python では，メール送信や本装置の管理機能など，よく使用する機能をまとめてライブラリという形で提供します。ライブラリで提供される機能は，スクリプトからライブラリを参照するだけで実行できます。これを利用することで，手軽にオペレーションをカスタマイズできます。

(2)　スクリプトアクション機能

スクリプトアクション機能とは，本装置へのコマンド実行などのアクションをスクリプトから実行する機能です。次に示すようなアクションがあります。

- Python 本体とともに配布される標準ライブラリを使用した，メール送信やファイルアクセスなど利便性の高い多数のアクション
- 本装置固有の拡張ライブラリを使用した，コマンド実行や運用メッセージ出力などのアクション
- ユーザが作成したライブラリを使用した，独自のアクション

このうち，本装置固有の拡張ライブラリで実行できるスクリプトアクションを次の表に示します。

表 19-1　本装置固有の拡張ライブラリのスクリプトアクション一覧

アクション	説明
コマンド実行	スクリプトで指定したコマンドを実行します。
運用メッセージ出力	指定した任意の文字列を運用メッセージとして出力します。

(3)　イベント監視機能

イベント監視機能とは，装置やネットワークの状態などを監視する機能です。監視対象の状態変化（イベント）を契機として，次に示すスクリプトやアプレットに通知します。通知先は，監視イベントの登録方法によって異なります。

- 実行中のスクリプトにイベントを通知
  監視イベントの登録と検出には，本装置が提供する拡張ライブラリを使用します。
- アプレットにイベントを通知
  監視イベントの登録には，アプレット機能が提供するコンフィグレーションを使用します。

監視イベントの一覧を次の表に示します。

表 19-2　監視イベントの一覧

監視イベント	説明
運用メッセージ監視	出力された運用メッセージを監視します。
タイマ監視	タイマを使用して，決められた時間を監視します。 タイマでは，次の 2 種類の形式で時間を指定できます。 • 時間間隔を指定（interval タイマ） • 時刻を指定（cron タイマ）

(4)　アプレット機能

アプレット機能とは，イベント監視機能と連携して，イベント発生を契機として事前に登録したアクションを実行する機能です。

監視イベントおよびアクションは，コンフィグレーションで登録します。なお，サポートしているアクションは，スクリプトファイルの起動（イベント起動スクリプト）だけです。

(5)　高機能スクリプトの使用方法

高機能スクリプトを使用する場合，まず本装置のコンフィグレーションやオペレーションをスクリプトとして作成します。このとき，スクリプトアクション機能，イベント監視機能，およびアプレット機能を自由に組み合わせて作成できます。

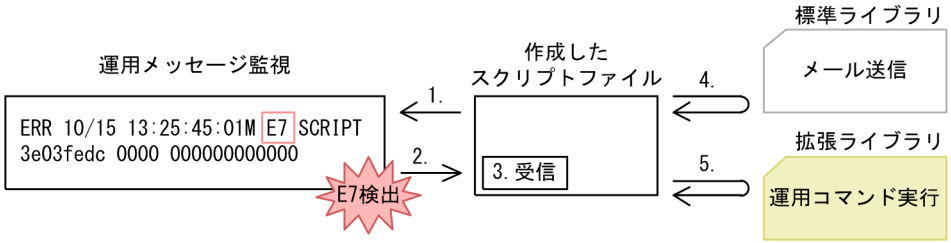
作成したスクリプトをスクリプト言語実行機能で実行すると，スクリプトに記載した各処理が実行されます。このように，高機能スクリプトを使用すると，本装置のコンフィグレーションやオペレーションをプログラミングして実行できるようになります。

19.1.2　高機能スクリプトの適用例

(1)　異常検出

スクリプトを使用して，異常（警告）検出時にオペレータへの通知と解析情報の自動収集をする例を次の図に示します。この図では運用メッセージを監視して，レベル E7 の運用メッセージ出力を検出したら，スクリプトからメール送信と運用コマンドを実行します。

図 19-2　運用メッセージ監視によるメール送信および運用コマンド実行

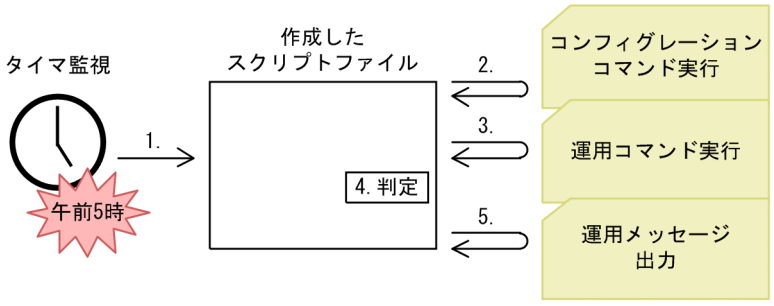


1. 運用メッセージ監視イベントを登録して，イベントの発生を待ちます。
2. レベル E7 の運用メッセージ出力を検出したら，イベントを通知します。
3. イベントを受信します。
4. イベントを受信したスクリプトは，Python の標準ライブラリを使用してオペレータにメールを送信します。
5. 関連する運用コマンドを実行して，事象発生時の解析情報を収集します。

(2)　定期的なコマンド実行

スクリプトを使用して，定期的にコマンドを実行する例を次の図に示します。この図ではタイマ監視をして，コンフィグレーションコマンドおよび運用コマンドを実行したあと，運用メッセージを出力します。

図 19-3　タイマ監視によるコマンド実行および運用メッセージ出力



事前に，午前 5 時に発生するタイマ監視イベントと，イベント発生時に起動するスクリプトファイルを，コンフィグレーションで登録しておきます。

1. 午前 5 時になるとイベントが発生して，スクリプトが起動します。
2. コンフィグレーションコマンドを実行します。

3. コンフィグレーションの反映結果が確認できる運用コマンドを実行します。

4. 3.の運用コマンドの出力結果を文字列解析して，正常性を確認します。

5. コンフィグレーションの反映結果を格納した運用メッセージを出力して，オペレータへ通知します。

19.1.3　高機能スクリプトの仕様

(1)　スクリプトの分類

スクリプトは起動方法によって次の 3 種類に分けられます。

表 19-3　起動方法によるスクリプト種別

スクリプト種別	説明
コマンドスクリプト	運用コマンド python を実行して，スクリプトを起動します。
常駐スクリプト	常駐プログラムとしてスクリプトを起動します。 運用コマンド install script でインストールしたファイルを，コンフィグレーションコマンド resident-script で指定することで起動します。
イベント起動スクリプト	監視イベントの検出を契機としてスクリプトを起動します。 運用コマンド install script でファイルをインストールしたあと，監視イベントと起動対象のファイルの関連づけをアプレット機能のコンフィグレーションコマンドで指定します。

(2)　スクリプトの標準入出力

スクリプトの標準入出力に対するサポートを次の表に示します。

表 19-4　スクリプトの標準入出力に対するサポート

スクリプト種別	標準入力	標準出力	標準エラー出力
コマンドスクリプト	○	○	○
常駐スクリプト	×	×	○※
イベント起動スクリプト	×	×	○※

（凡例）　○：サポートする　×：サポートしない

注※

運用コマンド dump script-user-program で確認できます。

(3)　スクリプト専用ユーザ

常駐スクリプトおよびイベント起動スクリプトは, スクリプト専用ユーザの権限で動作します。スクリプト専用ユーザについて次の表に示します。

表 19-5　スクリプト専用ユーザ

項目	ユーザ情報
ユーザ名	script
ホームディレクトリ	/opt/script

(4)　アクセス権限

本装置で実行するスクリプトでは，本装置上のディレクトリおよびファイルへアクセスできます。スクリプトでアクセスできるディレクトリおよびファイルの範囲を次の表に示します。

表 19-6　アクセスできるディレクトリおよびファイルの範囲

アクセス種別	説明
コマンドスクリプト	コマンドスクリプトを起動したユーザ権限に従います。
常駐スクリプト	スクリプト専用ユーザの権限に従います。
イベント起動スクリプト	

(5)　同時に実行できるスクリプト数

本装置では複数回スクリプトを起動させることで，同時に複数のスクリプトを実行できます。同時に実行できるスクリプト数を次の表に示します。

表 19-7　同時に実行できるスクリプト数

スクリプト種別	同時に実行できる上限数
コマンドスクリプト	4
常駐スクリプト	4
イベント起動スクリプト	4

19.1.4　スクリプト使用時の注意事項

(1)　使用する作業ディレクトリについて

頻繁にファイルへアクセスする場合は，RAM ディスク（メモリ）上にある次の作業ディレクトリを使用してください。

表 19-8　作業ディレクトリ

ディレクトリ名	容量
/opt/script※	16MB

注※

装置を再起動すると，配下のファイルは削除されます。

(2)　動作検証について

スクリプトを使用した運用に当たっては，実環境での使用を想定して，事前に CPU やメモリなど装置のリソースの利用状況に留意した動作検証をしてください。

(3)　運用コマンド show logging での表示について

スクリプトが実行するコマンドのログを運用コマンド show logging で非表示とした場合，ログを確認するときに運用上重要なコマンドのエラーを見逃すおそれがあります。そのため，次に示す対応を推奨します。

- 重要なコマンドを実行するときは一時的に表示対象とする。

- コマンドの実行結果がエラーになったときにメッセージを出力するスクリプトを作成する。

19.2　スクリプトの作成と実行

19.2.1　コンフィグレーション・運用コマンド一覧

高機能スクリプトのコンフィグレーションコマンド一覧を次の表に示します。

表 19-9　コンフィグレーションコマンド一覧

コマンド名	説明
aaa authorization commands script	スクリプトによるコマンド実行時のコマンド承認動作を設定します。
action	アプレット機能による監視イベント検出時のアクション（イベント起動スクリプト）を指定します。
disable	アプレット機能の動作を抑止します。
event manager applet	アプレット機能に関する動作情報を指定します。
event sysmsg	アプレット機能による運用メッセージ監視の監視条件を指定します。
event timer	アプレット機能によるタイマ監視の監視条件を指定します。
priority	アプレットの実行優先度を指定します。
resident-script	常駐スクリプトの起動情報を指定します。

高機能スクリプトの運用コマンド一覧を次の表に示します。

表 19-10　運用コマンド一覧

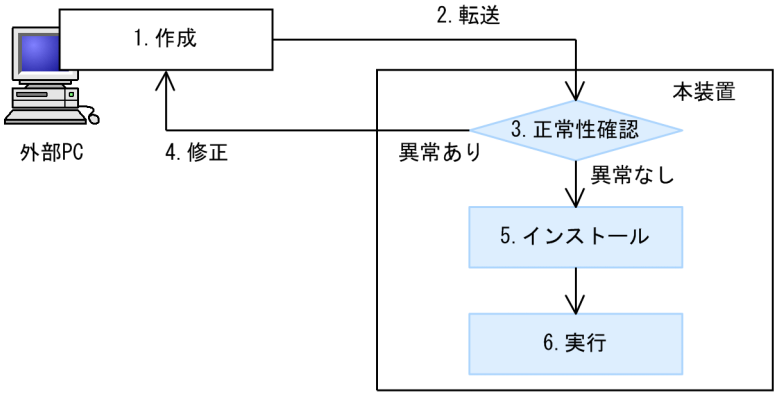
コマンド名	説明
python	Python を実行します。
stop python	起動中のスクリプトを停止します。
pyflakes	スクリプトファイルの文法チェックをします。
install script	作成したスクリプトファイルを本装置にインストールします。
uninstall script	本装置にインストールされているスクリプトファイルを削除します。
show script installed-file	本装置にインストールされているスクリプトファイルの情報を表示します。
show script running-state	スクリプトの起動情報を表示します。
show event manager history	監視イベントの発生履歴を表示します。
show event manager monitor	監視イベント情報を表示します。
clear event manager	イベント管理に関連する統計情報と発生履歴をクリアします。
restart script-manager	スクリプト管理プログラムを再起動します。 スクリプト管理プログラムは, コマンドスクリプトおよび常駐スクリプトの起動情報を管理します。
restart event-manager	イベント管理プログラムを再起動します。 イベント管理プログラムは, スクリプトから登録されたイベントを監視および検出します。

コマンド名	説明
dump script-user-program	常駐スクリプトおよびイベント起動スクリプトで出力される標準エラーを取得します。
dump script-manager	スクリプト管理プログラムで採取している制御情報をファイルへ出力します。
dump event-manager	イベント管理プログラムで採取している制御情報をファイルへ出力します。

19.2.2　スクリプトの実行の流れ

本装置でスクリプトを実行する流れについて次の図に示します。

図 19-4　スクリプト実行の流れ



1. 外部 PC でスクリプトを作成します。
2. 作成したスクリプトを，本装置に転送します。
3. 本装置内の機能を使用して，スクリプトの正常性を確認します。
4. スクリプトに異常がある場合，外部 PC でスクリプトを修正します。
5. スクリプトに異常がない場合，スクリプトを本装置にインストールします。
6. インストールしたスクリプトを実行します。

19.2.3　スクリプトファイルの作成

スクリプトファイルは，PC などの外部装置で作成してから，ftp などを使用して本装置に転送してください。作成および転送時の注意事項を次に示します。

- 文字コードは UTF-8（BOM なし）を使用してください。
- 本装置へ ftp で転送するときは，スクリプトファイルの形式に合わせたモードを使用してください。

  テキストのスクリプトファイル（拡張子が.py）の場合

  　アスキーモードで転送してください。

  コンパイル済みのスクリプトファイル（拡張子が.pyc または.pyo）の場合

  　バイナリモードで転送してください。

19.2.4　スクリプトファイルの正常性確認

作成したスクリプトファイルの正常性を確認する方法を次の表に示します。

表 19-11　スクリプトファイルの正常性を確認する方法

確認方法	説明
運用コマンド pyflakes	PyPI（Python ライブラリの公開サイト）に公開されている，「pyflakes（pyflakes3k）」と呼ばれる文法チェッカーを利用して確認します。
pdb モジュール	Python の標準ライブラリとして提供されているデバッガを利用して確認します。ブレークポイントの設定や，ステップ実行ができます。
運用コマンド dump script-user-program	常駐スクリプトで出力される標準エラーを取得して確認します。

(1)　運用コマンド pyflakes による確認

運用コマンド pyflakes を実行すると，指定したファイルに対して pyflakes（pyflakes3k）による文法チェックをします。pyflakes コマンドを使用して，sample.py ファイルの文法チェックをする例を次の図に示します。

図 19-5　pyflakes コマンドの実行例

```
> pyflakes sample.py
sample.py:4: invalid syntax
for cnt in range(10)
                    ^                                   …1
>
```

1. for 文の末尾に異常があることを示しています。

(2)　pdb モジュールを使用した確認

運用コマンド python で pdb モジュールを使用すると，指定したファイルをデバッグするためのデバッガコマンドが使用できます。pdb モジュールを使用して，sample.py ファイルの正常性を確認する例を次の図に示します。

図 19-6　pdb モジュールの使用例

```
# python -m pdb sample.py                               …1
> /usr/home/share/sample.py(1)<module>()
-> import os
(Pdb) b 4                                               …2
Breakpoint 1 at /usr/home/share/sample.py:4
(Pdb) r                                                 …3
> /usr/home/share/sample.py(4)<module>()
-> for cnt in range(10):
(Pdb) s                                                 …4
> /usr/home/share/sample.py(5)<module>()
-> if(cnt == 9):
(Pdb) cl                                                …5
Clear all breaks? y
Deleted breakpoint 1 at /usr/home/share/sample.py:4
(Pdb) r
--Return--
> /usr/home/share/sample.py(7)<module>()->None
-> sys.exit()
(Pdb) q                                                 …6
#
```

1. -m オプションで pdb モジュールを使用して，sample.py スクリプトを実行します。
2. デバッガコマンド b(reak)で，sample.py の 4 行目にブレークポイントを作成します。
3. デバッガコマンド r(un)で，スクリプトを実行します。

4. ブレークポイントで処理が停止したため，デバッガコマンド s(tep)でスクリプトをステップ実行します。
5. デバッガコマンド cl(ear)で，ブレークポイントを削除します。
6. デバッガコマンド q(uit)で，デバッガを終了します。

(3)　運用コマンド dump script-user-program による確認

運用コマンド dump script-user-program を実行すると，常駐スクリプトで出力される標準エラーを取得できます。ただし, 標準出力は取得できません。常駐スクリプトの標準エラー出力を確認する例を次の図に示します。

図 19–7　常駐スクリプトの標準エラー出力例

```
# dump script-user-program                              …1
# cd /usr/var/scriptManager                             …2
# gzip -d smd_script_user.gz                            …3
# cat smd_script_user                                   …4
[resident tag 1 info]
**** 20XX/03/19 17:52:36 UTC ****
Script start filename=/usr/var/script/script.file/sample1.py pid=128

**** 20XX/03/19 17:52:36 UTC ****
  File "/usr/var/script/script.file/sample1.py", line 1
    print a
          ^
SyntaxError: invalid syntax

**** 20XX/03/19 17:52:36 UTC ****
Script end filename=/usr/var/script/script.file/sample1.py pid=128
        :
        :
        :
#
```

1. 標準エラーをファイル（smd_script_user.gz）へ出力します。このファイルは，/usr/var/scriptManager/の配下に作成されます。
2. /usr/var/scriptManager/の配下に移動します。
3. smd_script_user.gz を解凍します。
4. 解凍したファイルを表示します。

19.2.5　スクリプトファイルのインストール

スクリプトファイルをインストールします。常駐スクリプトおよびイベント起動スクリプトは, インストールしたスクリプトファイルを起動します。また，インストールしたスクリプトファイルは，Python モジュールとしてインポートできます。

インストールできるスクリプトファイルには，次の条件があります。

- インストールできるスクリプトファイルの拡張子は，次のどれかです。
  - .py
  - .pyc
  - .pyo
- インストール済みのスクリプトファイルと，拡張子だけが異なるスクリプトファイルは，インストールできません。

スクリプトファイルのインストールでの上限値を次の表に示します。

表 19-12　スクリプトファイルのインストールでの上限値

項目	上限値
インストールできるファイル数	100
合計ファイルサイズ	4MB
1 ファイルのサイズ	512KB

スクリプトファイルのインストールには，運用コマンド install script を使用します。install script コマンドを使用して sample.py ファイルをインストールする例を次の図に示します。

図 19-8　スクリプトファイルのインストール

```
# install script sample.py                          …1
# show script installed-file                        …2
Date 20XX/01/15 20:32:35 UTC
Total: 1 files, 100 bytes

name: sample.py
size: 100 bytes
MD5: 12f58123c2b0f4286cf6d607656207c3
#
```

1. sample.py ファイルを本装置にインストールします。
2. 本装置にインストールされているスクリプトファイルを確認します。

19.2.6　スクリプトの起動

作成したスクリプトを，コマンドスクリプト，常駐スクリプト，またはイベント起動スクリプトとして起動します。

(1)　コマンドスクリプトの起動

スクリプトファイル名を指定して運用コマンド python を実行すると，コマンドスクリプトが起動します。

図 19-9　python コマンドの実行例（スクリプトの起動）

```
# python sample.py                                  …1
```

1. sample.py ファイルを起動します。

また，次の図に示すように，インストールしたスクリプトをモジュールとして起動できます。

図 19-10　python コマンドの実行例（モジュールの起動）

```
# install script sample.py                          …1
# python -m sample                                  …2
```

1. sample.py ファイルを本装置にインストールします。
2. sample.py ファイルをモジュールとして起動します。モジュールとして起動する場合は，拡張子を省略します。

(2)　常駐スクリプトの起動

常駐スクリプトを起動するには，次の二つの設定が必要です。

- 本装置へのスクリプトファイルのインストール
- スクリプトファイルの常駐スクリプト登録

両登録の完了を契機として，常駐スクリプトが起動します。常駐スクリプトの設定例を次の図に示します。

図 19-11　常駐スクリプトの設定例

```
# install script sample.py                          …1
# configure
(config)# resident-script 1 python sample.py        …2
(config)#
```

1. sample.py ファイルを本装置にインストールします。
2. sample.py ファイルを常駐スクリプトのスクリプト ID 1 に登録します。登録を契機として，sample.py が起動します。

(3)　イベント起動スクリプトの起動

イベント起動スクリプトを起動するには，次の三つの設定が必要です。

- 本装置へのスクリプトファイルのインストール
- 監視イベントの登録
- イベント検出時に起動するスクリプトファイル名の登録

これらの登録後，監視イベントの検出を契機として，イベント起動スクリプトが起動します。

監視イベントをタイマ監視とする場合の，イベント起動スクリプトの設定例を次の図に示します。

図 19-12　イベント起動スクリプトの設定例（タイマ監視）

```
# install script sample.py                          …1
# configure
(config)# event manager applet INTERVAL100s         …2
(config-applet)# event timer interval 100           …3
(config-applet)# action 1 python sample.py          …4
(config-applet)#
```

1. sample.py ファイルを本装置にインストールします。
2. アプレット名が INTERVAL100s のアプレットを作成して，アプレットのコンフィグレーションモードに移行します。
3. 100 秒周期でイベントを発生させる，タイマ監視を登録します。
4. sample.py ファイルをアクションのシーケンス番号 1 に登録します。登録を契機として，100 秒周期で sample.py が起動します。

監視イベントを運用メッセージ監視とする場合の，イベント起動スクリプトの設定例を次の図に示します。

図 19-13　イベント起動スクリプトの設定例（運用メッセージ監視）

```
# install script sample.py                          …1
# configure
(config)# event manager applet PORT_UP              …2
(config-applet)# event sysmsg message-id 25011001 …3
(config-applet)# action 1 python sample.py          …4
(config-applet)#
07/07 12:00:00 01S E4 PORT GigabitEthernet1/0/1 25011001 1350:000000000000 Port
 up.
                                                    …5
(config-applet)#
```

1. sample.py ファイルを本装置にインストールします。
2. アプレット名が PORT_UP のアプレットを作成して，アプレットのコンフィグレーションモードに移行します。

3. メッセージ識別子が 25011001 の運用メッセージ出力を監視する，運用メッセージ監視を登録します。
4. sample.py ファイルをアクションのシーケンス番号 1 に登録します。
5. 監視条件（メッセージ識別子 25011001）に該当する運用メッセージの出力を契機として，sample.py が起動します。

(4) 起動スクリプトの PID 確認

起動したスクリプトには，OS によって PID（Process ID）と呼ばれる識別子が割り当てられます。同じスクリプトを複数起動した場合でも，それぞれを区別するために異なる PID が割り当てられます。

各スクリプトに割り当てられた PID は，運用コマンド show script running-state で確認できます。複数の端末から同じスクリプトを起動した場合の PID 表示例を次の図に示します。

図 19–14 起動スクリプトの PID 確認

```
# show script running-state                          …1
Date 20XX/02/05 18:17:40 UTC

[operation command]                                  …2
  command line args: python sample.py
  PID: 2213
  start time: 20XX/02/05 18:17:24 UTC

  command line args: python sample.py
  PID: 1968
  start time: 20XX/02/05 18:17:26 UTC

[applet]                                             …3
  applet name: INTERVAL100s
  action sequence: 1
  command line args: python sample.py
  PID: 11700
  start time: 20XX/02/05 18:17:38 UTC

[resident]                                           …4
  script id: 1
  command line args: python sample.py
  state: Running
  PID: 1977
  start time: 20XX/02/05 18:17:29 UTC
#
```

1. 現在起動中のスクリプトを表示します。
2. コマンドスクリプトとして起動しているスクリプトが確認できます。
   この例では，PID が 2213 と 1968 のスクリプトが起動中であることを確認できます。
3. イベント起動スクリプトとして起動しているスクリプトが確認できます。
   この例では，PID が 11700 のスクリプトが起動中であることを確認できます。
4. 常駐スクリプトとして起動しているスクリプトが確認できます。
   この例では，PID が 1977 のスクリプトが起動中であることを確認できます。

19.3　本装置の Python サポート内容

本装置に実装する Python は，バージョン 3.2.3 です。オリジナルの Python 言語や標準ライブラリの仕様については，Python Software Foundation が公開しているドキュメントや一般書籍などを参照してください。この節では，本装置がサポートする内容について説明します。

19.3.1　標準 Python との差分および制限

本装置の Python サポート内容と，標準 Python との差分および制限を次に示します。

(1)　python コマンド

本装置の運用コマンド python のコマンドラインオプションについて，標準 Python 3.2.3 との差異を次に示します。

- -B オプションは未サポートです。
- -O(OO) オプションは未サポートです。
- -u オプションは未サポートです。
- スクリプトファイルの起動時に適用できるパラメータ数は，最大 32 です。
- スクリプトファイルの起動時に適用できる一つのパラメータの文字数は，最大 63 文字です。
- 指定できる総文字数は，空白文字を含めて最大 1000 文字です。
- スクリプトファイルの起動時に適用できるパラメータには，次の表に示す特殊文字を設定できません。

表 19-13　設定できない特殊文字

文字の名称	文字
ダブルクォート	"
シングルクォート	'
セミコロン	;
バックスラッシュ	¥
逆シングルクォート	`

(2)　__pycache__制限

本装置では，Python からスクリプトをインポートしても，ディレクトリ__pycache__を作成しません。

(3)　ポートの使用制限

Python を使用して特定のポートをバインドする場合は，IPv4 または IPv6 に関係なく，TCP，UDP のどちらもポート番号 49155～49166 を使用してください。

19.3.2　標準ライブラリ

標準ライブラリのサポート内容を次に示します。

(1)　サポートライブラリー覧

本装置が提供する Python の標準ライブラリー覧を次の表に示します。

表 19-14　標準ライブラリー覧

モジュール名				
__future__	_dummy_thread	_thread	abc	aifc
argparse	array	ast	asynchat	asyncore
atexit	audioop	base64	bdb	binascii
binhex	bisect	builtins	cProfile	calendar
cgi	cmath	cmd	code	codecs
collections	colorsys	compileall	concurrent	configparser
contextlib	copy	copyreg	csv	datetime
dbm	decimal	difflib	dis	distutils
doctest	dummy_threading	email	encodings	errno
fcntl	filecmp	fnmatch	fractions	ftplib
functools	gc	getopt	getpass	gettext
glob	hashlib	heapq	hmac	html
http	imaplib	imghdr	imp	importlib
inspect	io	itertools	json	keyword
lib2to3	linecache	locale	logging	macpath
mailbox	marshal	math	mimetypes	mmap
modulefinder	netrc	nntplib	numbers	operator
optparse	os	parser	pdb	pickle
pickletools	pipes	pkgutil	platform	plistlib
poplib	posixpath	pprint	profile	pstats
pty	pwd	py_compile	pyclbr	pydoc
queue	quopri	random	re	rlcompleter
runpy	sched	select	shelve	shlex
shutil	signal	site	smtpd	smtplib
sndhdr	socket	socketserver	stat	string
stringprep	struct	sunau	symtable	sys
sysconfig	tabnanny	tarfile	telnetlib	tempfile
test	textwrap	threading	time	timeit

モジュール名				
token	tokenize	trace	traceback	tty
types	unicodedata	unittest	urllib	uu
uuid	warnings	wave	weakref	webbrowser
wsgiref	xdrlib	xml	xmlrpc	zipfile
zipimport	zlib	-	-	-

（凡例）　-：該当なし

(2)　os モジュール制限

os モジュールが提供する一部の関数には，次に示す制限があります。

- os.kill 制限
  本装置では，Python の os.kill()および os.killpg()を使用して，スクリプト以外にシグナルを送信できません。
- os.fork 制限
  本装置では，Python の os.fork()および os.forkpty()によって，サブプロセスを作成できません。
- os.system 制限
  本装置では，Python の os.system()によるプログラムの実行について，動作を保証しません。プログラムを実行する場合は commandline モジュールを使用してください。

(3)　socketserver モジュール制限

socketserver モジュールが提供する次のクラスは，サポート対象外です。

- ForkingMixIn
- ForkingUDPServer
- ForkingTCPServer

(4)　http.server モジュール制限

http.server モジュールが提供する次のクラスは，サポート対象外です。

- CGIHTTPRequestHandler

(5)　ユーザ制限

標準ライブラリにはスーパーユーザでだけ実行できるライブラリがありますが，本装置ではスーパーユーザでの実行をサポートしません。

19.4　Python 拡張ライブラリの使用方法

本装置は実装する Python に加えて，本装置へのオペレーションを制御するための拡張ライブラリを提供します。この節では，拡張ライブラリの使用方法について説明します。提供するモジュールのメソッドや関数の詳細は，「運用コマンドレファレンス Vol.1」「20　Python 拡張ライブラリ」を参照してください。

19.4.1　指定コマンド実行の設定

ここでは，commandline モジュールを使用して，指定したコマンドを実行する方法を説明します。

commandline モジュールには，コンフィグレーションコマンドおよび運用コマンドをスクリプトから実行する CommandLine クラスがあります。CommandLine クラスのメソッド一覧を次の表に示します。

表 19-15　CommandLine クラスのメソッド一覧

メソッド名	説明
exec	引数に指定したコマンドを実行します。
exit	該当インスタンスによるコマンド実行を終了します。
set_default_timeout	該当インスタンスによるコマンド実行時のデフォルトタイムアウト時間を設定します。
set_default_logging	該当インスタンスから実行するコマンドのログを，運用コマンド show logging の表示対象とするかどうかのデフォルト値を設定します。

(1)　スクリプトファイルおよび実行結果の例

(a)　さまざまなコマンドを実行する例

さまざまなコマンドを実行するスクリプトファイルの例を次に示します。

図 19-15　スクリプトファイル（sample1.py）記載例

```
# sample1.py
# -*- coding: utf-8 -*-
import extlib.commandline                                              …1
obj = extlib.commandline.CommandLine()                                 …2

# デフォルトタイムアウトの指定
obj.set_default_timeout(180)                                           …3

# コマンドログのshow loggingデフォルト非表示指定
obj.set_default_logging(extlib.commandline.DISABLE)                    …4

# ユーザ応答なしコマンド（ls）
print("ls start")
dict_ret = obj.exec("ls")                                              …5
if dict_ret['result'] == extlib.commandline.OK:
    print(dict_ret['strings'])                                         …6
else:
    print("timeout.")

# ユーザ応答ありコマンド（file1，file2の削除）
print("rm start")
dict_ret = obj.exec("rm -i file1 file2", ("?","y"), ("?", "y"),
                    logging=extlib.commandline.ENABLE)                 …7
if dict_ret['result'] == extlib.commandline.OK:
    print(dict_ret['strings'])                                         …8
else:
    print("timeout.")

# コマンド応答タイムアウト時間指定（pingを3秒間実行）
```

```
print("ping start")
dict_ret = obj.exec("ping 192.0.2.1", 3)                                    …9
if dict_ret['result'] == extlib.commandline.TIMEOUT:
    print(dict_ret['strings'])                                              …10
obj.exit()                                                                  …11
```

1. モジュールをインポートします。
2. CommandLine クラスのインスタンスを生成します。
3. コマンド応答のデフォルトタイムアウト時間を指定します。
4. コマンドログのデフォルトの show logging 表示設定を非表示にします。
5. exec メソッドで，実行するコマンド（ユーザ応答なし）を指定します。
6. コマンドの実行結果を出力します。
7. exec メソッドで，実行するコマンド（ユーザ応答あり）とコマンドログの show logging 表示設定（表示する）を指定します。
8. コマンドの実行結果を出力します。
9. exec メソッドで，実行するコマンドとコマンド応答のタイムアウト時間を指定します。
10. コマンドの実行結果を出力します。
11. コマンド実行状態を終了します。

スクリプトファイル sample1.py の実行結果を次に示します。exec メソッドで指定した運用コマンド ls, rm，および ping が，正しく実行されています。

図 19-16　スクリプト（sample1.py）実行結果

```
# python sample1.py
ls start
file1 file2

rm start
remove 'file1'? remove 'file2'?
ping start
PING 192.0.2.1 (192.0.2.1): 56 data bytes
64 bytes from 192.0.2.1: icmp_seq=0 ttl=63 time=0.377 ms
64 bytes from 192.0.2.1: icmp_seq=1 ttl=63 time=0.545 ms
64 bytes from 192.0.2.1: icmp_seq=2 ttl=63 time=1.349 ms
64 bytes from 192.0.2.1: icmp_seq=3 ttl=63 time=0.578 ms

----192.0.2.1 PING Statistics----
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.377/0.858/1.385/0.445 ms

#
```

(b)　スクリプト実行中にエラーが発生する例

コマンド応答のタイムアウト時間に，不正な値を指定した例を次に示します。

図 19-17　スクリプトファイル（sample2.py）記載例

```
# sample2.py
# -*- coding: utf-8 -*-
import extlib.commandline                                                   …1
obj = extlib.commandline.CommandLine()                                      …2

# コマンド応答タイムアウト時間指定（時間に負数を指定）
print("ping start")
dict_ret = obj.exec("ping 192.0.2.1", -3)                                   …3
print(dict_ret['strings'])                                                  …4

obj.exit()                                                                  …5
```

1. モジュールをインポートします。
2. CommandLine クラスのインスタンスを生成します。
3. exec メソッドで，実行するコマンドとコマンド応答のタイムアウト時間（負数）を指定します。
4. コマンドの実行結果を出力します。
5. コマンド実行状態を終了します。

スクリプトファイル sample2.py の実行結果を次に示します。タイムアウト時間に指定した値が正しくないため，エラーになります。

図 19-18　スクリプト（sample2.py）実行結果

```
# python sample2.py
ping start
Traceback (most recent call last):
  File "sample2.py", line 7, in <module>
    dict_ret = obj.exec("ping 192.0.2.1", -3)
  File "/usr/local/lib/python3.2/site-packages/extlib/commandline.py", line 741
, in exec
    CNST.ERR_TIMER_INVALID))
ValueError: The timer value is invalid.
#
```

(c)　コマンド実行失敗の例外が発生する例

exec メソッドでコマンド実行失敗の例外が発生したときに，インスタンスを再生成する例を次に示します。

図 19-19　スクリプトファイル（sample3.py）記載例

```
# sample3.py
# -*- coding: utf-8 -*-
import extlib.commandline                                              …1
obj = extlib.commandline.CommandLine()                                 …2

retry_cnt = 0

# ユーザ応答なしコマンド（ls）
print("ls start")
while retry_cnt < 3:
    try:
        dict_ret = obj.exec("ls")                                      …3
        if dict_ret['result'] == extlib.commandline.OK:
            print(dict_ret['strings'])                                 …4
            print("success!!")
        else:
            print("timeout.")
        break
    except extlib.commandline.ExecuteCommandError:                     …5
        obj.exit()                                                     …6
        obj = extlib.commandline.CommandLine()                         …7
        print("Regenerate the instance")
        retry_cnt = retry_cnt + 1

obj.exit()                                                             …8
```

1. モジュールをインポートします。
2. CommandLine クラスのインスタンスを生成します。
3. exec メソッドで，実行するコマンド（ユーザ応答なし）を指定します。
4. コマンドの実行結果を出力します。
5. exec メソッドでのコマンド実行失敗の例外を捕捉します。
6. コマンド実行状態をいったん終了します。
7. CommandLine クラスのインスタンスを再生成します。

8. コマンド実行状態を終了します。

スクリプトファイル sample3.py の実行結果を次に示します。例外が発生しても，インスタンスを再生成したため，運用コマンド ls が正しく実行されています。

図 19-20　スクリプト（sample3.py）実行結果

```
# python sample3.py
ls start
Regenerate the instance
file1 file2

success!!
#
```

(2)　インスタンス生成

CommandLine クラスのインスタンスは，一つのプロセスに対して複数生成できません。インスタンスを再生成するときは，先に，既存のインスタンスに対して exit メソッドを呼び出してください。

(3)　exec メソッドでのコマンド実行

commandline モジュールの exec メソッドを使用してコマンドを実行する場合，スクリプト専用ユーザ（ユーザ名 script）によって該当コマンドが実行されます。exec メソッドを使用したコマンド実行について次の表に示します。

表 19-16　exec メソッドを使用したコマンド実行

項目	説明
初期コマンド入力モード	一般ユーザモード
無効コマンド	スクリプト専用ユーザでは，次に示す運用コマンドの実行による設定変更は無効となります。 • set exec-timeout • set terminal pager また，スクリプト専用ユーザに対する次のコンフィグレーションコマンドは無効となります。 • username コマンドの logging-console パラメータ • username コマンドの exec-timeout パラメータ • username コマンドの terminal-pager パラメータ

(4)　コマンド承認

本装置にコマンド承認を設定している場合，スクリプトから実行するコマンドにもコマンド承認が適用されます。

スクリプトから実行するコマンドは，コンフィグレーションコマンド aaa authorization commands script の username パラメータで指定したユーザ名の権限で承認されます。なお，bypass パラメータを指定すると，コマンド承認をしないで無条件にコマンドを実行できます。

コマンド承認についての特記事項を次に示します。

- aaa authorization commands script コマンドだけを設定しても，コマンド承認はしません。aaa authorization commands コマンドをあわせて設定してください。ただし，RADIUS サーバによるコ

マンド承認はサポートしないため，TACACS+サーバまたはローカルによるコマンド承認の設定が必要です。

- コンソール（RS232C）で接続した運用端末からスクリプトを起動してコマンドを実行した場合のコマンド承認は，aaa authorization commands console コマンドの設定に従います。

  aaa authorization commands console コマンドの設定がある場合

  コマンド承認の対象となります。ただし，bypass パラメータが設定されている場合は，コマンド承認をしないですべてのコマンドが実行できます。

  aaa authorization commands console コマンドの設定がない場合

  コマンド承認をしません。すべてのコマンドが実行できます。

- aaa authorization commands コマンドの設定があり，コマンド承認情報（コマンドクラスまたはコマンドリスト）を取得できなかった場合は，すべてのコマンドが実行できません。コマンド承認情報を取得できない例を次に示します。
  - aaa authorization commands script コマンドの設定がない
  - 指定したユーザ名が，TACACS+サーバまたはローカルに存在しない
  - TACACS+サーバにアクセスできない
- コマンド承認情報（コマンドクラスまたはコマンドリスト）は，CommandLine クラスのインスタンス生成時に取得します。
- コマンド承認を設定している場合，Python 標準ライブラリの os.system()などによるプログラムの起動についても，起動制限の対象となります。プログラムを起動できるのは，次に示す場合だけです。
  - aaa authorization commands コマンドの設定がない場合
  - aaa authorization commands コマンドの設定があり，aaa authorization commands script コマンドの bypass パラメータの設定がある場合
  - aaa authorization commands コマンドの設定があり，aaa authorization commands console コマンドの設定がなく，コンソール（RS232C）で接続した運用端末から起動したスクリプトでプログラムを起動する場合

19.4.2　運用メッセージ出力の設定

ここでは，sysmsg モジュールを使用して，指定した文字列を運用メッセージとして出力する方法を説明します。

sysmsg モジュールの関数一覧を次の表に示します。

表 19–17　sysmsg モジュールの関数一覧

関数名	説明
send	運用メッセージを出力します。

(1)　スクリプトファイルおよび実行結果の例

運用メッセージを出力するスクリプトファイルの例を次に示します。

図 19–21　スクリプトファイル（test1.py）記載例

```
# test1.py
# -*- coding: utf-8 -*-
import sys
import extlib.sysmsg                                                    …1
```

```
try:
    extlib.sysmsg.send("E3", 0xfedc, 0xba9876543210,"Script Start!!") …2
    print("send success.")
except extlib.sysmsg.MsgSendError:                                    …3
    print("send failed.")
    sys.exit()
```

1. モジュールをインポートします。
2. 出力する運用メッセージを，次のように指定します。
   - イベントレベル E3
   - メッセージ識別子 3e03fedc
   - 付加情報 ba9876543210
   - メッセージテキスト“Script Start!!”
3. 運用メッセージ出力失敗の例外を捕捉します。

スクリプトファイル test1.py の実行結果および運用メッセージの出力例を次に示します。

図 19-22　スクリプト（test1.py）実行結果

```
# python test1.py
send success.
#
```

図 19-23　運用メッセージ出力例

```
EVT 07/07 12:00:00 01S E3 SCRIPT 3e03fedc 2600:ba9876543210 Script Start!!
```

19.4.3　イベント監視機能の設定

ここでは，eventmonitor モジュールを使用して，イベントを登録，削除，および受信する方法を説明します。

eventmonitor モジュールは，装置やネットワークの状態などの監視と連携して，監視対象の状態変化（イベント）を起動中のスクリプトに通知する機能をサポートします。イベント監視機能に関連する関数一覧を次の表に示します。

表 19-18　イベント監視機能に関連する関数一覧

機能種別	関数名	説明
イベント登録	regist_sysmsg	監視する運用メッセージを登録します。
	regist_cron_timer	cron タイマを登録します。
	regist_interval_timer	interval タイマを登録します。
イベント削除	event_delete	登録したイベントを削除します。
イベント受信	event_receive	イベントが発生したときにイベントを受信します。

(1)　スクリプトファイルの例

(a)　運用メッセージをイベントとして監視する例

運用メッセージをイベントとして監視する，イベントの登録例を次に示します。

図 19-24 スクリプト記載例 1

```
import sys
import extlib.eventmonitor
 …1

try:
    event_sysmsg=extlib.eventmonitor.regist_sysmsg(event_level="E7",
    message_id=0xabcd1234,message_text="(Error|error)")
 …2
except Exception as e:
 …3
    print('ERROR!! regist_sysmsg()',e)
    sys.exit()

while 1:
    dict = extlib.eventmonitor.event_receive(extlib.eventmonitor.BLOCK_ON, 0)
 …4

    if dict['event_id']== event_sysmsg:
 …5
        print('EVENT OCCURRED!!')
```

1. モジュールをインポートします。
2. イベントを登録します。次の条件を満たす運用メッセージの出力を監視します。
   - イベントレベル E7
   - メッセージ識別子 abcd1234
   - メッセージテキストに文字列“Error”または“error”を含む
3. イベントが登録されたかどうか確認します。登録に失敗した場合，ログを出力して終了します。
4. イベント受信関数を呼び出します。
5. 戻り値を参照して，意図した値かどうか確認します。

(b) cron タイマによってイベントを監視する例

cron タイマによってイベントを監視する，イベントの登録例を次に示します。

図 19-25 スクリプト記載例 2

```
import sys
import extlib.eventmonitor
 …1

try:
    event_cron_timer = extlib.eventmonitor.regist_cron_timer('0 23 * * *')
 …2
except Exception as e:
 …3
    print('ERROR!! regist_cron_timer ()',e)
    sys.exit()

while 1:
    dict = extlib.eventmonitor.event_receive(extlib.eventmonitor.BLOCK_ON, 0)
 …4

    if dict['event_id']== event_cron_timer:
 …5
        print('EVENT OCCURRED!!')
```

1. モジュールをインポートします。
2. 毎日 23 時に発生するイベントを登録します。
3. イベントが登録されたかどうか確認します。登録に失敗した場合，ログを出力して終了します。
4. イベント受信関数を呼び出します。

5. 戻り値を参照して，意図した値かどうか確認します。

(c)　interval タイマによってイベントを監視する例

interval タイマによってイベントを監視する，イベントの登録例を次に示します。

図 19-26　スクリプト記載例 3

```
import sys
import extlib.eventmonitor
 …1

try:
    event_interval_timer = extlib.eventmonitor.regist_interval_timer(1800)
 …2
except Exception as e:
 …3
    print('ERROR!! regist_interval_timer()',e)
    sys.exit()

while 1:
    dict = extlib.eventmonitor.event_receive(extlib.eventmonitor.BLOCK_ON, 0)
 …4

    if dict['event_id']== event_interval_timer:
 …5
        print('EVENT OCCURRED!!')
```

1. モジュールをインポートします。
2. 1800 秒ごとに発生するイベントを登録します。
3. イベントが登録されたかどうか確認します。登録に失敗した場合，ログを出力して終了します。
4. イベント受信関数を呼び出します。
5. 戻り値を参照して，意図した値かどうか確認します。

(d)　登録したイベントを削除する例

登録したイベントを削除する例を次に示します。

図 19-27　スクリプト記載例 4

```
import sys
import extlib.eventmonitor
 …1

try:
    event_cron_timer = extlib.eventmonitor.regist_cron_timer('0 23 * * *')
 …2
except Exception as e:
 …3
    print('ERROR!! regist_cron_timer ()',e)
    sys.exit()

try:
    result_dict = extlib.eventmonitor.event_delete(event_cron_timer)
 …4
    print('EVENT DELETE!!')
except:
 …5
    print('ERROR!! event_delete()')
```

1. モジュールをインポートします。
2. イベントを登録します。
3. イベントが登録されたかどうか確認します。登録に失敗した場合，ログを出力して終了します。
4. 登録したイベントの監視イベント ID を指定して，監視を停止します。

5.停止に失敗した場合，ログを出力します。

(e) イベントを受信する例

イベントを受信する例を次に示します。

図 19-28 スクリプト記載例 5

```
import sys
import extlib.eventmonitor
 …1

try:
    event_cron_timer = extlib.eventmonitor.regist_cron_timer('0 23 * * *')
 …2
except Exception as e:
 …3
    print('ERROR!!  event_cron_timer()',e)
    sys.exit()

dict = extlib.eventmonitor.event_receive(extlib.eventmonitor.BLOCK_ON , 0)
 …4

if dict['event_id']== event_cron_timer:
 …5
    print('EVENT OCCURRED!! ')
```

1.モジュールをインポートします。

2.イベントを登録します。

3.イベントが登録されたかどうか確認します。登録に失敗した場合，ログを出力して終了します。

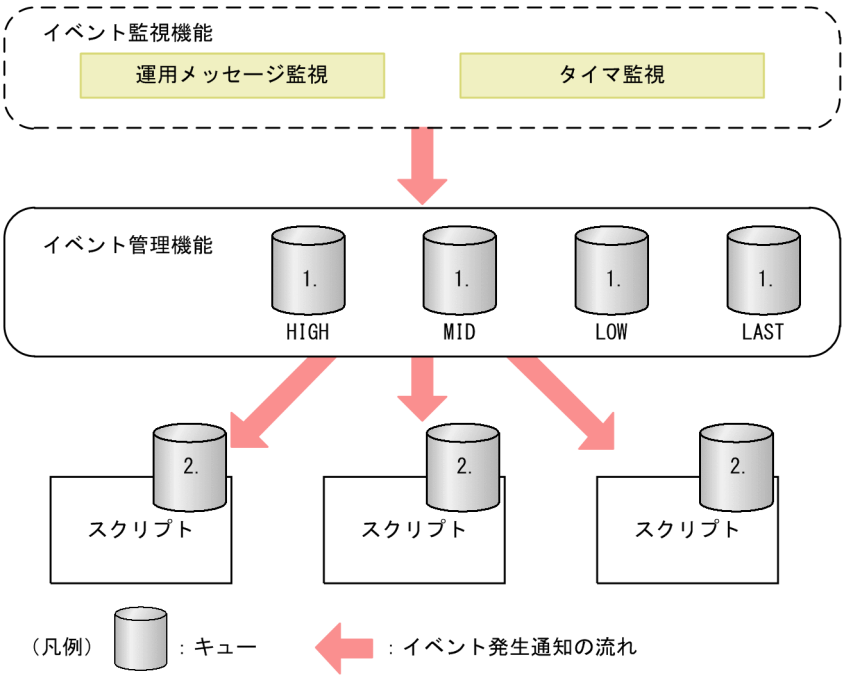
4.イベント受信関数を呼び出します。受信タイムアウトなしのブロッキングモードで受信します。

5.戻り値を参照して，意図した値かどうか確認します。

(2) 通知情報の廃棄

監視イベントの発生頻度が高い場合，イベント発生通知がスクリプトに通知される前に廃棄されることがあります。イベント発生通知の流れを次の図に示します。図中の 1.および 2.の通知受信キューが満杯になると，廃棄が発生します。

図 19-29　イベント発生通知の流れ



1. キューあふれ閾値は，優先度ごとに 1024 メッセージ
2. キューあふれ閾値は，スクリプトごとに 1024 メッセージ

なお，廃棄の発生有無は，運用コマンド show event manager monitor で表示されるイベント廃棄回数（discard）で確認できます。

19.4.4　スクリプト起動契機の取得

ここでは，eventmonitor モジュールの get_exec_trigger()関数を使用して，動作中のスクリプトから，自身が起動した要因（イベント起動スクリプトの場合は発生イベント）を取得する方法を説明します。

(1)　スクリプトファイルの例

イベント起動スクリプトの起動要因（発生イベント）を取得するスクリプトファイルの例を次に示します。

図 19-30　スクリプトファイル記載例

```
import sys
import extlib.eventmonitor                                          …1
dict = extlib.eventmonitor.get_exec_trigger ()                      …2

if dict['type'] == extlib.eventmonitor.APPLET :                     …3
# アプレット
    if dict['applet']['type'] == extlib.eventmonitor.TIMER_EVT :    …4
    # タイマイベント

        if dict['applet']['condition'][extlib.eventmonitor.TIMER_TYPE] == \
            extlib.eventmonitor.CRON :
        # cronタイマ

            # cron監視条件の文字列を表示
            print("[condition]",file=sys.stderr)
            print(dict['applet']['condition'][extlib.eventmonitor.CRON],file=sy
s.stderr)

        elif dict['applet']['condition'][extlib.eventmonitor.TIMER_TYPE] == \
```

```
            extlib.eventmonitor.INTERVAL :
        # intervalタイマ

            # interval監視条件の文字列を表示
            print("[condition]",file=sys.stderr)
            print(dict['applet']['condition'][extlib.eventmonitor.INTERVAL],
                file=sys.stderr)

    elif dict['applet']['type'] == extlib.eventmonitor.SYSMSG_EVT :   …5
    # 運用メッセージイベント

        ## 運用メッセージ監視条件の表示
        print("[condition]",file=sys.stderr)
        ## イベントレベル
        print("SYSMSG_EVENT_LEVEL:" + str(dict['applet']['condition']
            [extlib.eventmonitor.SYSMSG_EVENT_LEVEL]),file=sys.stderr)

        ## イベント発生要因の運用メッセージを表示
        print("[trigger system message]",file=sys.stderr)
        ## 発生時刻
        print("SYSMSG_TIME:" + dict['applet']['trigger']
            [extlib.eventmonitor.SYSMSG_TIME],file=sys.stderr)
        ## メッセージ識別子
        print("SYSMSG_MSG_ID:" + str(hex(dict['applet']['trigger']
            [extlib.eventmonitor.SYSMSG_MSG_ID])),file=sys.stderr)

sys.exit()
```

1. モジュールをインポートします。
2. 起動要因（発生イベント）を取得する関数を呼び出します。
3. スクリプトの起動要因がアプレット機能（イベント起動スクリプト）かどうか判定します。
4. 起動要因がタイマ監視の場合の監視条件を取得します。
5. 起動要因が運用メッセージ監視の場合の監視条件，および起動要因となった運用メッセージの情報を取得します。

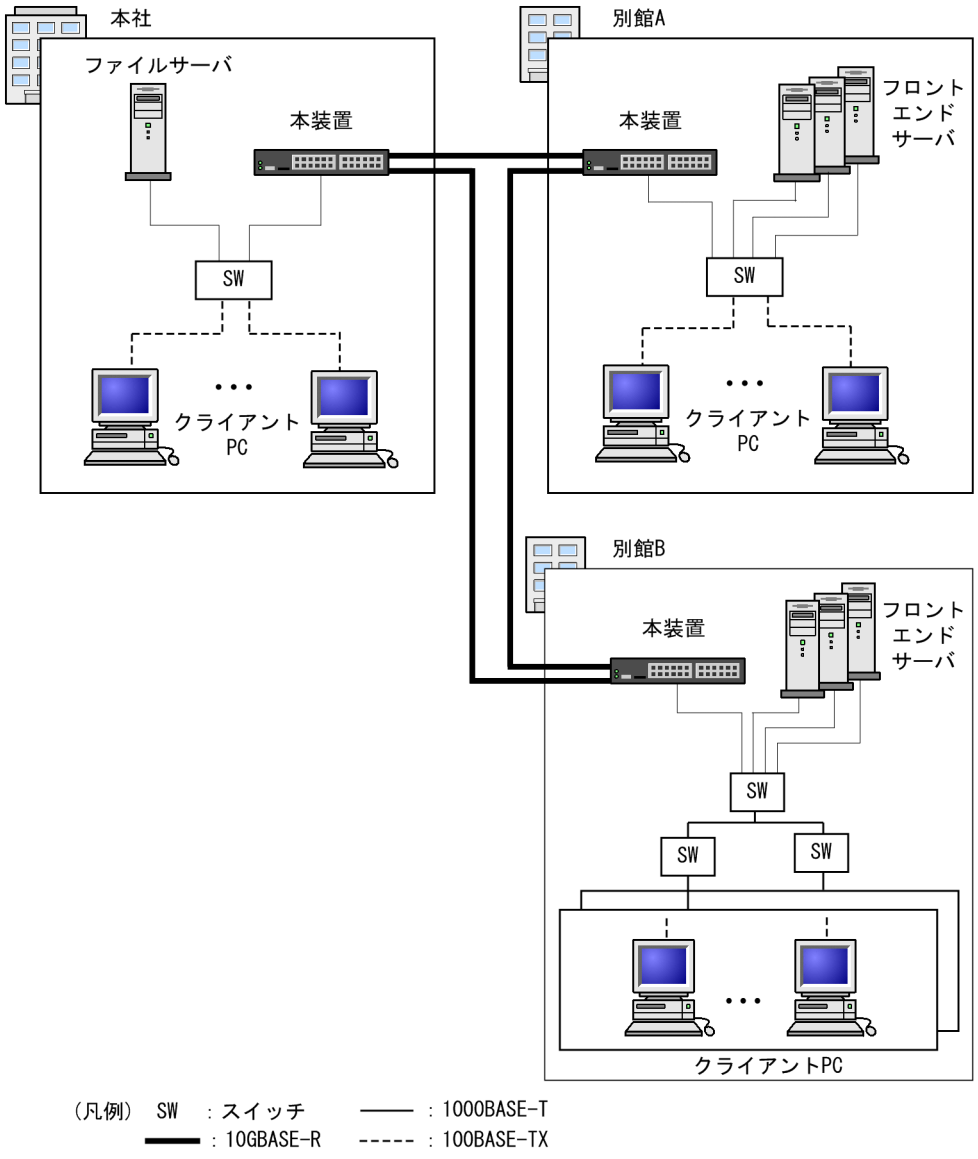
20 イーサネット

この章では，本装置のイーサネットについて説明します。

20.1　接続インタフェースの解説

本装置を使用した代表的なイーサネットの構成例を次の図に示します。各ビル間，サーバ間を 10GBASE-R で接続することによって，10BASE-T/100BASE-TX/1000BASE-T および 1000BASE-X よりもサーバ間のパフォーマンスが向上します。

図 20-1　イーサネットの構成例



20.1.1　ポートの種類とサポート機能

(1)　ポートの種類

ポートの種類と，ポートごとにサポートするイーサネット規格を次の表に示します。

表 20-1　ポートの種類とサポートするイーサネット規格

ポートの種類	イーサネット規格
10BASE-T/100BASE-TX/1000BASE-T ポート	10BASE-T，100BASE-TX，1000BASE-T
100BASE-TX/1000BASE-T/10GBASE-T ポート	100BASE-TX，1000BASE-T，10GBASE-T
SFP ポート	10BASE-T，100BASE-TX，1000BASE-T，1000BASE-X
SFP+ポート	10GBASE-R
SFP+/SFP 共用ポート	10BASE-T，100BASE-TX，1000BASE-T，1000BASE-X，10GBASE-R
QSFP+ポート（スタック専用）	40GBASE-R
QSFP28/QSFP+共用ポート	40GBASE-R，100GBASE-R

(a)　10BASE-T/100BASE-TX/1000BASE-T ポート

10BASE-T／100BASE-TX／1000BASE-T のツイストペアケーブル（UTP）を使用します。

(b)　100BASE-TX/1000BASE-T/10GBASE-T ポート

100BASE-TX／1000BASE-T／10GBASE-T のツイストペアケーブル（UTP）を使用します。

(c)　SFP ポート

10BASE-T/100BASE-TX/1000BASE-T で接続する場合，10BASE-T/100BASE-TX/1000BASE-T の SFP-T を使用します。また，SFP-T は IP8800/S3660-16S4XW および IP8800/S3660-24S8XW でサポートしています。

1000BASE-X で接続する場合，1000BASE-SX，1000BASE-LX，1000BASE-LH，1000BASE-LHB，および 1000BASE-BX の SFP をサポートしています。

(d)　SFP+ポート

10GBASE-SR，10GBASE-LR，10GBASE-ER，10GBASE-ZR，および 10GBASE-BR の SFP+をサポートしています。また，10GBASE-CU のダイレクトアタッチケーブルをサポートしています。

(e)　SFP+/SFP 共用ポート

10BASE-T/100BASE-TX/1000BASE-T で接続する場合，10BASE-T/100BASE-TX/1000BASE-T の SFP-T を使用します。また，SFP-T は IP8800/S3660-24X4QW および IP8800/S3660-48X4QW でサポートしています。

1000BASE-X で接続する場合，1000BASE-SX，1000BASE-LX，1000BASE-LH，1000BASE-LHB，および 1000BASE-BX の SFP をサポートしています。

10GBASE-R で接続する場合，10GBASE-SR，10GBASE-LR，10GBASE-ER，10GBASE-ZR，および 10GBASE-BR の SFP+をサポートしています。また，10GBASE-CU のダイレクトアタッチケーブルをサポートしています。

(f)　QSFP+ポート

40GBASE-R で接続するスタック専用ポートです。40GBASE-SR4 および 40GBASE-LR4 の QSFP+をサポートしています。また，40GBASE-CR4 のダイレクトアタッチケーブルをサポートしています。

(g)　QSFP28/QSFP+共用ポート

このポートはスタックポートとしても，通常の通信用ポートとしても使用できます。

40GBASE-SR4 および 40GBASE-LR4 の QSFP+と，100GBASE-SR4，100GBASE-CWDM4，100GBASE-LR4，および 100GBASE-4WDM-40 の QSFP28 をサポートしています。また，40GBASE-CR4 および 100GBASE-CR4 のダイレクトアタッチケーブルをサポートしています。

(2)　接続モードとサポート機能

接続インタフェースごとの接続モードとサポート機能を次の表に示します。なお, 本装置は半二重モードでの接続をサポートしていません。

表 20–2　接続インタフェースごとの接続モードとサポート機能

接続インタフェース	接続モード	サポート機能
10BASE-T	• 全二重固定 • 全二重のオートネゴシエーション	• 自動 MDI/MDIX 機能 • フローコントロール
100BASE-TX	• 全二重固定 • 全二重のオートネゴシエーション	• 自動 MDI/MDIX 機能 • フローコントロール • ジャンボフレーム
1000BASE-T	• 全二重のオートネゴシエーション	• 自動 MDI/MDIX 機能 • フローコントロール • ジャンボフレーム
10GBASE-T	• 全二重のオートネゴシエーション	• 自動 MDI/MDIX 機能 • フローコントロール • ジャンボフレーム
1000BASE-X	• 全二重固定 • 全二重のオートネゴシエーション	• フローコントロール • ジャンボフレーム
10GBASE-R	• 全二重固定	• フローコントロール • ジャンボフレーム
40GBASE-R	• 全二重固定（40GBASE-SR4 および 40GBASE-LR4 だけ） • 全二重のオートネゴシエーション（40GBASE-CR4 だけ）	• フローコントロール • ジャンボフレーム
100GBASE-R	• 全二重固定（100GBASE-SR4，100GBASE-CWDM4，100GBASE-LR4，および 100GBASE-4WDM-40 だけ） • 全二重のオートネゴシエーション（100GBASE-CR4 だけ）	• フローコントロール • ジャンボフレーム

20.1.2　10BASE-T/100BASE-TX/1000BASE-T/10GBASE-T

10BASE-T／100BASE-TX／1000BASE-T／10GBASE-T のツイストペアケーブル（UTP）を使用したインタフェースについて説明します。

(1)　接続インタフェース

10BASE-T，100BASE-TX，1000BASE-T，および 10GBASE-T では，オートネゴシエーションをサポートしています。オートネゴシエーションは，伝送速度，全二重，およびフローコントロールについて，相手装置とやりとりをして装置間で最適な接続動作を決定する機能です。本装置では，オートネゴシエーションで解決できなかった場合，リンク接続されるまで接続動作を繰り返します。

1000BASE-T および 10GBASE-T では，オートネゴシエーションによる全二重接続だけをサポートしています。

10BASE-T および 100BASE-TX では，オートネゴシエーションと全二重固定接続をサポートしています。

コンフィグレーションでは次のモードを指定できます。接続するネットワークに合わせて設定してください。本装置のデフォルト値は，オートネゴシエーションとなります。

- オートネゴシエーション
- 100BASE-TX 全二重固定
- 10BASE-T 全二重固定

(2)　接続仕様

本装置のコンフィグレーションでの指定値と相手装置の伝送速度および，全二重および半二重モードの接続仕様を次に示します。

10BASE-T および 100BASE-TX は，相手装置によってオートネゴシエーションでは接続できない場合があるため，できるだけ相手装置のインタフェースに合わせた固定設定にしてください。

10BASE-T/100BASE-TX/1000BASE-T ポート，SFP ポートで SFP-T を使用した場合，および SFP+/SFP 共用ポートで SFP-T を使用した場合の接続仕様を次の表に示します。

表 20–3　接続仕様（10BASE-T/100BASE-TX/1000BASE-T）

相手装置		本装置の設定		
設定	インタフェース	固定		オートネゴシエーション
		10BASE-T 全二重	100BASE-TX 全二重	
固定	10BASE-T 全二重	10BASE-T 全二重	×	×
	100BASE-TX 全二重	×	100BASE-TX 全二重	×
	1000BASE-T 全二重	×	×	×
オートネゴシエーション	10BASE-T 全二重	×	×	10BASE-T 全二重

相手装置		本装置の設定		
設定	インタフェース	固定		オート ネゴシエーション
		10BASE-T 全二重	100BASE-TX 全二重	
	10BASE-T 全二重および半二重	×	×	10BASE-T 全二重
	100BASE-TX 全二重	×	×	100BASE-TX 全二重
	100BASE-TX 全二重および半二重	×	×	100BASE-TX 全二重
	10BASE-T/100BASE-TX 全二重および半二重	×	×	100BASE-TX 全二重
	1000BASE-T 全二重	×	×	1000BASE-T 全二重
	1000BASE-T 全二重および半二重	×	×	1000BASE-T 全二重
	10BASE-T/100BASE-TX/1000BASE-T 全二重および半二重	×	×	1000BASE-T 全二重

（凡例）　×：接続できない

100BASE-TX/1000BASE-T/10GBASE-T ポートを使用した場合の接続仕様を次の表に示します。

表 20–4　接続仕様（100BASE-TX/1000BASE-T/10GBASE-T）

相手装置		本装置の設定	
設定	インタフェース	固定	オート ネゴシエーション
		100BASE-TX 全二重	
固定	100BASE-TX 全二重	100BASE-TX 全二重	×
	1000BASE-T 全二重	×	×
	10GBASE-T 全二重	×	×
オート ネゴシエーション	10BASE-T 全二重および半二重	×	×
	100BASE-TX 全二重	×	100BASE-TX 全二重
	100BASE-TX 全二重および半二重	×	100BASE-TX 全二重
	1000BASE-T 全二重	×	1000BASE-T 全二重

相手装置		本装置の設定	
設定	インタフェース	固定 100BASE-TX 全二重	オート ネゴシエーション
	1000BASE-T 全二重および半二重	×	1000BASE-T 全二重
	10GBASE-T 全二重	×	10GBASE-T 全二重
	10GBASE-T 全二重および半二重	×	10GBASE-T 全二重
	10BASE-T/100BASE-TX/1000BASE-T 全二重および半二重	×	1000BASE-T 全二重
	100BASE-TX/1000BASE-T/10GBASE-T 全二重および半二重	×	10GBASE-T 全二重

（凡例）　×：接続できない

(3)　自動 MDI/MDIX 機能

自動 MDI/MDIX 機能は，MDI と MDI-X を自動的に切り替える機能です。これによって，クロスケーブルまたはストレートケーブルどちらでも通信できるようになります。オートネゴシエーション時だけサポートします。全二重固定時は MDI-X となります。MDI／MDI-X のピンマッピングを次の表に示します。

表 20-5　MDI／MDI-X のピンマッピング

RJ45 Pin No.	MDI			MDI-X		
	1000BASE-T 10GBASE-T※1	100BASE-TX※2	10BASE-T※2	1000BASE-T 10GBASE-T※1	100BASE-TX※2	10BASE-T※2
1	BI_DA ＋	TD ＋	TD ＋	BI_DB ＋	RD ＋	RD ＋
2	BI_DA−	TD−	TD−	BI_DB−	RD−	RD−
3	BI_DB ＋	RD ＋	RD ＋	BI_DA ＋	TD ＋	TD ＋
4	BI_DC ＋	Unused	Unused	BI_DD ＋	Unused	Unused
5	BI_DC−	Unused	Unused	BI_DD−	Unused	Unused
6	BI_DB−	RD−	RD−	BI_DA−	TD−	TD−
7	BI_DD ＋	Unused	Unused	BI_DC ＋	Unused	Unused
8	BI_DD−	Unused	Unused	BI_DC−	Unused	Unused

注※1

1000BASE-T および 10GBASE-T では，8 ピンすべてを送信と受信が同時双方向（bi-direction）通信するため，信号名表記が異なります（BI_Dx：双方向データ信号）。

注※2

10BASE-T と 100BASE-TX では，送信（TD）と受信（RD）信号は別々の信号線を使用しています。

(4)　ダウンシフト機能

ダウンシフト機能は，オートネゴシエーション設定時に機能し，オートネゴシエーションで決定された最適な接続動作（最も速い回線速度）でリンク接続ができなかった場合（例えば，オートネゴシエーションでは 1000BASE-T が最適な接続動作と決定したが，伝送品質の劣化などによって 1000Mbit/s でリンク接続できないなど）に，オートネゴシエーションで広告する最も速い速度を無効に設定し，次に速い速度でリンク接続を試みる機能です。

(a)　回線速度の変更順序

オートネゴシエーション完了後にリンク接続できない場合，オートネゴシエーションで広告する回線速度を，フェーズ 1，フェーズ 2，…の順に下げていきます。回線速度が最低になってもリンク接続できない場合は，フェーズ 1 に戻ってダウンシフトを繰り返します。回線速度の変更順序を，ポートの種類ごとに次の表に示します。

表 20–6　回線速度の変更順序（10BASE-T/100BASE-TX/1000BASE-T ポート）

フェーズ	コンフィグレーションコマンド speed のパラメータ設定内容※1			
	auto	auto 10 100 1000	auto 10 100	auto 1000※2 or auto 100※2 or auto 10※2
1	10 100 1000	10 100 1000	10 100	−
2	10 100	10 100	10	−
3	10	10	−	−

（凡例）　−：ダウンシフト動作をしない

注※1　数値は回線速度を示します。単位は Mbit/s です。

注※2　ダウンシフト動作をさせたくない場合は，この設定をしてください。

表 20–7　回線速度の変更順序（100BASE-TX/1000BASE-T/10GBASE-T ポート）

フェーズ	コンフィグレーションコマンド speed のパラメータ設定内容※1		
	auto or auto 100 1000 10000	auto 100 1000	auto 10000※2 or auto 1000※2 or auto 100※2
1	100 1000 10000	100 1000	−
2	100 1000	100	−
3	100	−	−

（凡例）　−：ダウンシフト動作をしない

注※1　数値は回線速度を示します。単位は Mbit/s です。

注※2　ダウンシフト動作をさせたくない場合は，この設定をしてください。

(5)　接続時の注意事項

- 伝送速度，および全二重および半二重モードが相手装置と不一致の場合，接続できないので注意してください。

  不一致の状態で通信を行うと，以降の通信が停止することがあります。この場合，当該ポートに対して inactivate コマンド，activate コマンドを実行してください。
- 使用するケーブルについては，「ハードウェア取扱説明書」を参照してください。
- 全二重インタフェースはコリジョン検出とループバック機能を行わないことによって実現しています。このため，10BASE-T または 100BASE-TX を全二重インタフェース設定で使用する場合，相手接続ポートは必ず全二重インタフェースに設定して接続してください。

20.1.3　1000BASE-X

1000BASE-X の光ファイバを使用したインタフェースについて説明します。

(1)　接続インタフェース

1000BASE-SX，1000BASE-LX，1000BASE-LH，1000BASE-LHB，および 1000BASE-BX をサポートしています。回線速度は 1000Mbit/s 全二重固定です。

1000BASE-SX

短距離間を接続するために使用します（マルチモード，最大 550m）。

1000BASE-LX

中距離間を接続するために使用します（シングルモード，最大 5km／マルチモード，最大 550m）。

1000BASE-LH，1000BASE-LHB

長距離間を接続するために使用します。

- 1000BASE-LH（シングルモード，最大 70km）
- 1000BASE-LHB（シングルモード，最大 100km）

1000BASE-BX

送受信で波長の異なる光を使用することで，1 芯の光ファイバを使い，光ファイバのコストを抑えることができます。

送受信で異なる波長の光を使用するため，アップ側とダウン側で 1 対となるトランシーバを使用します。

本装置では，IEEE802.3ah で規定されている 1000BASE-BX10-D/1000BASE-BX10-U と，独自規格の 1000BASE-BX40-D/1000BASE-BX40-U をサポートします。

1000BASE-BX10-D/1000BASE-BX10-U

中距離間を接続するために使用します（シングルモード，最大 10km）。

1000BASE-BX40-D/1000BASE-BX40-U

長距離間を接続するために使用します（シングルモード，最大 40km）。

コンフィグレーションでは次のモードを指定できます。接続するネットワークに合わせて設定してください。本装置のデフォルト値は，オートネゴシエーションになります。

- オートネゴシエーション
- 1000BASE-X 全二重固定

オートネゴシエーションは，全二重およびフローコントロールについて，相手装置とやりとりをして装置間で最適な接続動作を決定する機能です。本装置では，オートネゴシエーションで解決できなかった場合，リンク接続されるまで接続動作を繰り返します。

(2)　接続仕様

本装置のコンフィグレーションでの指定値と相手装置の伝送速度および，全二重および半二重モードの接続仕様を次の表に示します。なお，1000BASE-X の物理仕様については，「ハードウェア取扱説明書」を参照してください。

表 20-8　接続仕様

相手装置		本装置の設定	
設定	インタフェース	固定	オートネゴシエーション
		1000BASE 全二重	1000BASE 全二重
固定	1000BASE 半二重	×	×
	1000BASE 全二重	1000BASE 全二重	×
オート ネゴシエーション	1000BASE 半二重	×	×
	1000BASE 全二重	×	1000BASE 全二重

（凡例）　×：接続できない

(3)　接続時の注意事項

- 相手装置（スイッチングハブなど）をオートネゴシエーションまたは全二重固定に設定してください。
- 「ハードウェア取扱説明書」に示すトランシーバ以外を使用した場合の動作は保証できません。

20.1.4　10GBASE-R

10GBASE-R の光ファイバを使用したインタフェースについて説明します。

(1)　接続インタフェース

10GBASE-SR，10GBASE-LR，10GBASE-ER，10GBASE-ZR，および 10GBASE-BR をサポートしています。回線速度は 10Gbit/s 全二重固定です。

10GBASE-SR

短距離間を接続するために使用します（マルチモード，伝送距離：最大 300m※）。

注※

伝送距離は使用するケーブルによって異なります。ケーブルごとの伝送距離は，「ハードウェア取扱説明書」を参照してください。

10GBASE-LR

中距離間を接続するために使用します（シングルモード，伝送距離：最大 10km）。

10GBASE-ER

長距離間を接続するために使用します（シングルモード，伝送距離：最大 40km）。

10GBASE-ZR

長距離間を接続するために使用します（シングルモード，伝送距離：最大 80km）。

10GBASE-BR

1000BASE-BX と同様に送受信で波長の異なる光を使用することで，1 芯の光ファイバで双方向の通信ができます。そのため，光ファイバのコストを抑えられます。

送受信で異なる波長の光を使用するため，アップ側とダウン側で 1 対となるトランシーバを使用します。

10GBASE-BR10-D/10GBASE-BR10-U

中距離間を接続するために使用します（シングルモード，最大 10km）。

10GBASE-BR40-D/10GBASE-BR40-U

長距離間を接続するために使用します（シングルモード，最大 40km）。

(2)　接続仕様

本装置の物理仕様については，「ハードウェア取扱説明書」を参照してください。

(3)　接続時の注意事項

- 「ハードウェア取扱説明書」に示すトランシーバ以外を使用した場合の動作は保証できません。
- 10GBASE-BR および 10GBASE-ZR はベンダー独自仕様ですので，他ベンダーの装置と接続した場合の動作は保証できません。
- ダイレクトアタッチケーブル使用時は，リンクアップまでに 5～8 秒掛かります。

20.1.5　40GBASE-R

40GBASE-R の光ファイバを使用したインタフェースについて説明します。

(1)　接続インタフェース

40GBASE-SR4，40GBASE-LR4，および 40GBASE-CR4 をサポートしています。回線速度は 40Gbit/s，全二重の固定接続またはオートネゴシエーションによる接続をサポートしています。

40GBASE-SR4

短距離間を接続するために使用します。全二重固定接続だけをサポートします（マルチモード，伝送距離：最大 150m※）。

40GBASE-LR4

中距離間を接続するために使用します。全二重固定接続だけをサポートします（シングルモード，伝送距離：最大 10km※）。

40GBASE-CR4

短距離間を接続するために使用します。オートネゴシエーションによる接続だけをサポートします（伝送距離：最大 5m※）。

注※

伝送距離は使用するケーブルによって異なります。ケーブルごとの伝送距離は，「ハードウェア取扱説明書」を参照してください。

(2)　接続仕様

接続インタフェースごとの接続仕様を次の表に示します。なお，40GBASE-R の物理仕様については，「ハードウェア取扱説明書」を参照してください。

表 20-9　接続仕様

相手装置		本装置の接続インタフェース	
設定	インタフェース	40GBASE-SR4 40GBASE-LR4	40GBASE-CR4
		40GBASE 全二重固定	40GBASE 全二重 オートネゴシエーション
固定	40GBASE 全二重	40GBASE 全二重	×
オート ネゴシエーション	40GBASE 全二重	×	40GBASE 全二重

（凡例）　×：接続できない

(3)　接続時の注意事項

- 「ハードウェア取扱説明書」に示すトランシーバ以外を使用した場合の動作は保証できません。
- QSFP+使用時，トランシーバを挿してから運用コマンド show interfaces の回線種別が決定するまでに 3～5 秒掛かります。
- ダイレクトアタッチケーブル使用時，トランシーバを挿してから運用コマンド show interfaces の回線種別が決定するまでに 3～5 秒掛かります。また，リンクアップまでに 5～8 秒掛かります。

20.1.6　100GBASE-R

100GBASE-R の光ファイバを使用したインタフェースについて説明します。

(1)　接続インタフェース

100GBASE-SR4, 100GBASE-CWDM4, 100GBASE-LR4, 100GBASE-4WDM-40, および 100GBASE-CR4 をサポートしています。回線速度は 100Gbit/s，全二重の固定接続またはオートネゴシエーションによる接続をサポートしています。

100GBASE-SR4

短距離間を接続するために使用します。全二重固定接続だけをサポートします（マルチモード，伝送距離：最大 100m※）。

100GBASE-CWDM4

短距離から中距離間を接続するために使用します。全二重固定接続だけをサポートします（マルチモード，伝送距離：最大 2km※）。

100GBASE-LR4

中距離間を接続するために使用します。全二重固定接続だけをサポートします（シングルモード，伝送距離：最大 10km）。

100GBASE-4WDM-40

中距離から長距離間を接続するために使用します。全二重固定接続だけをサポートします（シングルモード，伝送距離：最大 40km※）。

100GBASE-CR4

短距離間を接続するために使用します。オートネゴシエーションによる接続だけをサポートします。（伝送距離：最大 1m※）。

注※

伝送距離は使用するケーブルによって異なります。ケーブルごとの伝送距離は，「ハードウェア取扱説明書」を参照してください。

(2)　接続仕様

接続インタフェースごとの接続仕様を次の表に示します。なお，100GBASE-R の物理仕様については，「ハードウェア取扱説明書」を参照してください。

表 20–10　接続仕様

相手装置		本装置の接続インタフェース	
設定	インタフェース	100GBASE-SR4 100GBASE-CWDM4 100GBASE-LR4 100GBASE-4WDM-40	100GBASE-CR4
		100GBASE 全二重固定	100GBASE 全二重 オートネゴシエーション
固定	100GBASE 全二重	100GBASE 全二重	×
オート ネゴシエーション	100GBASE 全二重	×	100GBASE 全二重

（凡例）　×：接続できない

(3)　接続時の注意事項

- 「ハードウェア取扱説明書」に示すトランシーバ以外を使用した場合の動作は保証できません。
- QSFP28 使用時，トランシーバを挿してから運用コマンド show interfaces の回線種別が決定するまでに 3～5 秒掛かります。
- ダイレクトアタッチケーブル使用時，トランシーバを挿してから運用コマンド show interfaces の回線種別が決定するまでに 3～5 秒掛かります。また，リンクアップまでに 5～8 秒掛かります。

20.2　イーサネット共通の解説

20.2.1　フローコントロール

フローコントロールは，装置内の受信バッファ枯渇でフレームを廃棄しないように，相手装置にフレームの送信をポーズパケットによって，一時的に停止指示する機能です。自装置がポーズパケット受信時は，送信規制を行います。この機能は全二重だけサポートします。

(1)　フローコントロールの設定と動作

本装置内の受信バッファが枯渇して受信フレームを廃棄することがないようにするためには，ポーズパケットを送信して相手装置に送信規制を要求します。また，相手装置はポーズパケットを受信して送信規制できる必要があります。

相手装置からのポーズパケットを受信したとき，本装置が送信規制するかどうかは設定に従います。

フローコントロールのコンフィグレーションは，送信と受信でそれぞれ，有効，無効，またはネゴシエーション結果によって動作を決定するモードを選択できます。本装置と相手装置の設定を，送信と受信で一致させてください。

本装置のポーズパケット送信の設定と相手装置の設定を組み合わせたときのフローコントロール動作を，次の表に示します。

表 20-11　フローコントロールの送信動作

本装置の ポーズパケット送信 (send パラメータ)	相手装置の ポーズパケット受信	フローコントロール動作
on	有効	相手装置が送信規制を行う
off	無効	相手装置が送信規制を行わない
desired	Desired	相手装置が送信規制を行う

（凡例）Desired：ネゴシエーション結果によって動作を決定するモード

本装置のポーズパケット受信の設定と相手装置の設定を組み合わせたときのフローコントロール動作を，次の表に示します。

表 20-12　フローコントロールの受信動作

本装置の ポーズパケット受信 (receive パラメータ)	相手装置の ポーズパケット送信	フローコントロール動作
on	有効	本装置が送信規制を行う
off	無効	本装置が送信規制を行わない
desired	Desired	本装置が送信規制を行う

（凡例）Desired：ネゴシエーション結果によって動作を決定するモード

オートネゴシエーション時，本装置の設定が off で相手装置が Desired の場合および本装置の設定が desired の場合，フローコントロール動作はネゴシエーション結果に従います。

(2)　オートネゴシエーション使用時のフローコントロール動作

本装置では，オートネゴシエーションに対応したインタフェースでオートネゴシエーションの使用時に，相手装置とポーズパケットを送受信するかどうかを折衝できます。

オートネゴシエーション使用時のフローコントロール動作を次の表に示します。

表 20-13　オートネゴシエーション使用時のフローコントロール動作

本装置(パラメータ)		相手装置		本装置のオートネゴシエーション結果		フローコントロール動作	
ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	本装置の送信規制	相手装置の送信規制
on	desired	有効	有効	on	on	行う	行う
			無効	on	off	行わない	行わない
			Desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う
			無効	on	off	行わない	行わない
			Desired	on	on	行う	行う
		Desired	有効	on	on	行う	行う
			無効	on	off	行わない	行わない
			Desired	on	on	行う	行う
off		有効	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			Desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う
			無効	off	off	行わない	行わない
			Desired	on	on	行う	行う
		Desired	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			Desired	on	on	行う	行う
desired	on	有効	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			Desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う
			無効	off	on	行わない	行わない
			Desired	on	on	行う	行う

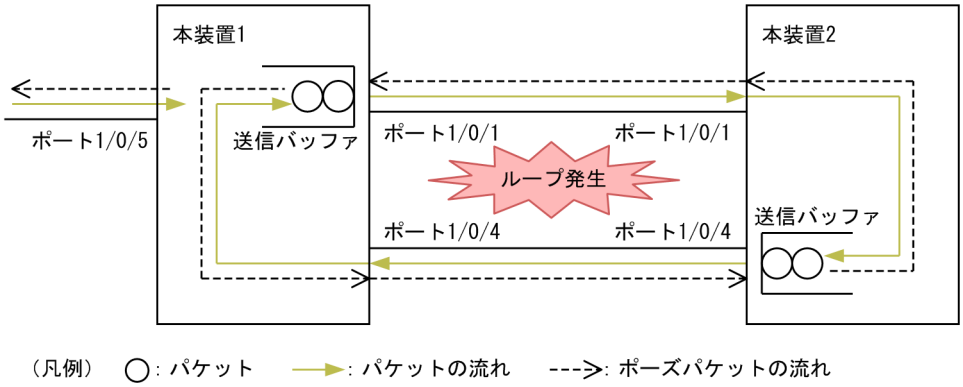
本装置（パラメータ）		相手装置		本装置のオートネゴシエーション結果		フローコントロール動作	
ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	本装置の送信規制	相手装置の送信規制
		Desired	有効	on	on	行う	行う
			無効	off	on	行わない	行わない
			Desired	on	on	行う	行う
	off	有効	有効	off	off	行わない	行わない
			無効	off	off	行わない	行わない
			Desired	off	off	行わない	行わない
		無効	有効	on	off	行わない	行う
			無効	off	off	行わない	行わない
			Desired	on	off	行わない	行う
		Desired	有効	off	off	行わない	行わない
			無効	off	off	行わない	行わない
			Desired	off	off	行わない	行わない
	desired	有効	有効	on	on	行う	行う
			無効	off	off	行わない	行わない
			Desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う
			無効	off	off	行わない	行わない
			Desired	on	on	行う	行う
		Desired	有効	on	on	行う	行う
			無効	off	off	行わない	行わない
			Desired	on	on	行う	行う

（凡例）Desired：ネゴシエーション結果によって動作を決定するモード

(3)　ルーズモード

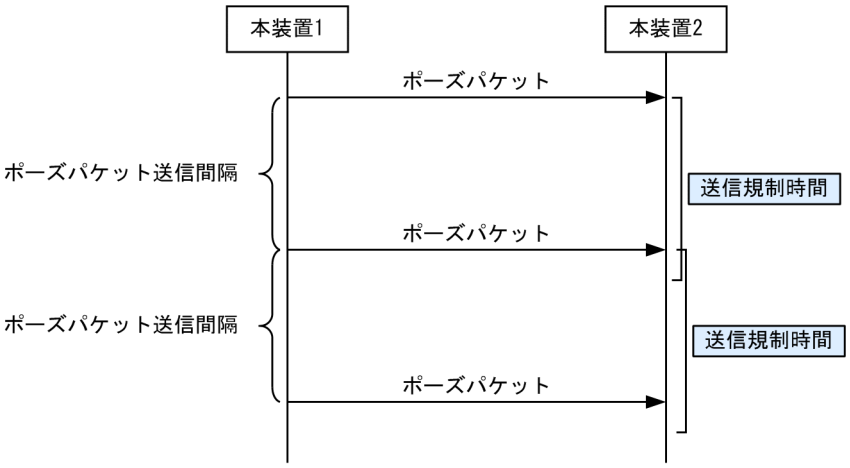
サーバへの接続などで，パケットの損失をできるだけ防ぎたい場合は，厳密なフローコントロールが求められます。しかし，相互に厳密なフローコントロールを行うと，瞬間的なループ状態を契機として次の図に示すようにお互いが送信規制されたままの状態となるおそれがあります。フローコントロールのルーズモードは，このようなネットワークでフローコントロールを行う場合に適したモードです。

図 20-2　相互に送信規制する例



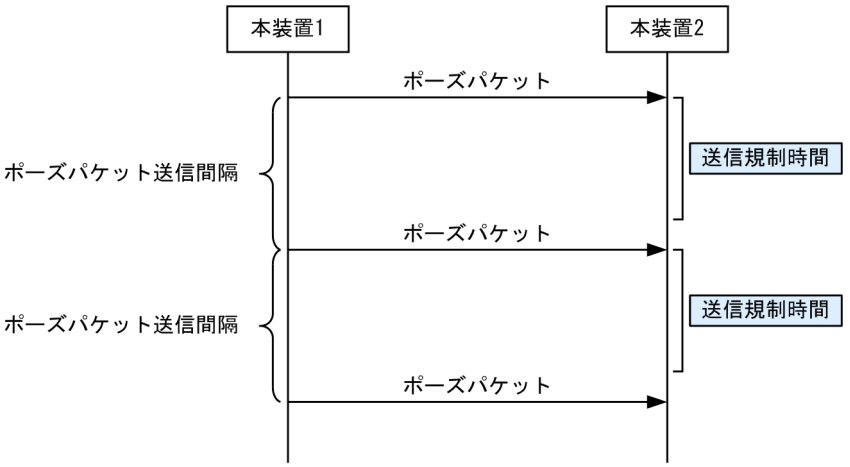
デフォルト動作の場合，“ポーズパケット送信間隔≦送信規制時間”となるため，ポーズパケットの受信側では送信が完全に停止します。デフォルトでの動作シーケンスを次の図に示します。

図 20-3　デフォルトでの動作シーケンス



ルーズモードの場合，“ポーズパケット送信間隔＞送信規制時間”となるため，本装置同士の接続でも送信が完全に停止し続けることがありません。ルーズモードでの動作シーケンスを次の図に示します。

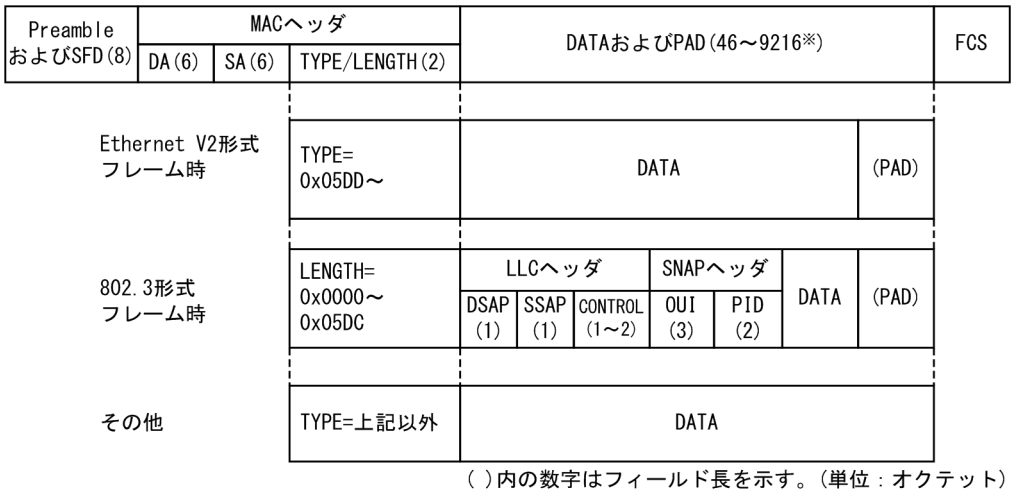
図 20-4　ルーズモードでの動作シーケンス



20.2.2　フレームフォーマット

フレームフォーマットを次の図に示します。

図 20-5　フレームフォーマット



（ ）内の数字はフィールド長を示す。（単位：オクテット）

注※　DATAおよびPADの最大長はEthernetV2形式フレーム時だけ9216。
802.3形式フレームおよびその他の形式のフレームは1500。

(1)　MAC 副層フレームフォーマット

(a)　Preamble および SFD

64 ビット長の 2 進数で「1010...1011(最初の 62 ビットは 10 繰り返し，最後の 2 ビットは 11)」のデータです。送信時にフレームの先頭に付加します。この 64 ビットパターンのないフレームは受信できません。

(b)　DA および SA

48 ビット形式をサポートします。16 ビット形式およびローカルアドレスはサポートしていません。

(c)　TYPE/LENGTH

TYPE／LENGTH フィールドの扱いを次の表に示します。

表 20-14　TYPE／LENGTH フィールドの扱い

TYPE／LENGTH 値	本装置での扱い
0x0000～0x05DC	IEEE802.3 CSMA/CD のフレーム長
0x05DD～	Ethernet V2.0 のフレームタイプ

(d)　FCS

32 ビットの CRC 演算を使用します。

(2)　LLC の扱い

Ethernet V2 と同様に扱います。

(3)　受信フレームの廃棄条件

次に示すどれかの条件によって受信したフレームを廃棄します。

- フレーム長がオクテットの整数倍でない
- 受信フレーム長（DA～FCS）が 64 オクテット未満，または 1523 オクテット以上
  ただし，ジャンボフレーム選択時は，指定したフレームサイズを超えた場合
- FCS エラー

(4)　パッドの扱い

送信フレーム長が 64 オクテット未満の場合, MAC 副層で FCS の直前にパッドを付加します。パッドの値は不定です。

20.2.3　ジャンボフレーム

ジャンボフレームは，MAC ヘッダの DA～データが 1518 オクテットを超えるフレームを中継するための機能です。コンフィグレーションコマンド ip mtu の MTU 長を合わせて変更することで, IP パケットをフラグメント化するサイズを大きくすることもできます。

本装置では，Ethernet V2 形式フレームだけをサポートします。IEEE802.3 形式フレームはサポートしていません。Tagged フレームについては,「24.1.5　VLAN Tag」の Tagged フレームのフォーマットを参照してください。ジャンボフレームのサポート機能を次の表に示します。

表 20–15　ジャンボフレームサポート機能

項目	フレーム形式		内容
	Ethernet V2	IEEE802.3	
フレーム長（オクテット）	1519～9234	×	MAC ヘッダの DA～データの長さ。FCS は含みません。
受信機能	○	×	IEEE802.3 フレームは，LENGTH フィールド値が 0x05DD（1501 オクテット）以上の場合に廃棄します。
送信機能	○	×	IEEE802.3 フレームは送信しません。

（凡例）　○：サポート　×：未サポート

なお，10BASE-T／100BASE-TX／1000BASE-T では，100BASE-TX（全二重）および 1000BASE-T（全二重）だけをサポートします。

20.2.4　本装置の MAC アドレス

(1)　装置 MAC アドレス

本装置は，装置を識別するための MAC アドレスを一つ持ちます。この MAC アドレスのことを装置 MAC アドレスと呼びます。装置 MAC アドレスは，レイヤ 3 インタフェースの MAC アドレスやスパニングツリーなどのプロトコルの装置識別子として使用します。

(2)　装置 MAC アドレスを使用する機能

装置 MAC アドレスを使用する機能を次の表に示します。

表 20–16　装置 MAC アドレスを使用する機能

機能	用途
VLAN	レイヤ 3 インタフェースの MAC アドレス
VXLAN	レイヤ 3 インタフェースの MAC アドレス
リンクアグリゲーションの LACP	装置識別子
スパニングツリー	装置識別子
Ring Protocol	装置識別子
GSRP	装置識別子
IEEE802.3ah/UDLD	装置識別子
L2 ループ検知	装置識別子
CFM	装置識別子
LLDP	装置識別子
OADP	装置識別子

20.2.5　Sync-E

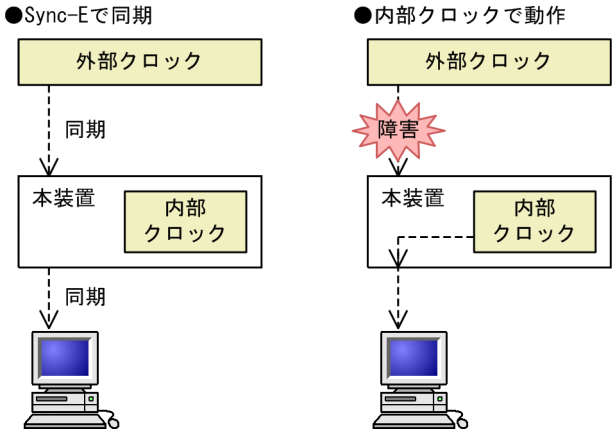
(1)　概要

Sync-E（Synchronous Ethernet）は，PHY（Physical Interface）で使用するクロック周波数の同期をイーサネットインタフェースでする技術です。一次基準クロック（PRC：Precision Reference Clock）を頂点としたマスタースレーブのネットワークでクロック周波数を同期し，システムを構成する全装置のイーサネットのクロックが単一のクロックを参照します。これによって，ネットワークの装置間で同じクロック周波数で通信ができ，システム全体の転送性能が向上します。

Sync-E による同期には，ポートで受信した信号に同期する方法と，フレームに記されたタイムスタンプを元に同期する方法があります。本装置では，ポートで受信した信号に同期する方法を使用します。

コンフィグレーションで外部クロックの受信ポートを指定すると，ほかのポートは外部クロックの周波数で動作します。外部クロックの受信ポートには，SFP+/SFP 共用ポートを指定します。外部クロックの入力がなくなった場合や，コンフィグレーションで外部クロックの受信ポートを指定していないなど Sync-E が無効な場合は，本装置の内部クロックで動作します。Sync-E の概要を次の図に示します。

図 20-6　Sync-E を適用したネットワーク



この図の構成では，外部クロックとクロック周波数の同期を取り，同期したクロック周波数で下流の装置と同期します。外部クロックとの同期が外れると，内部クロックで動作します。

(2)　サポート仕様

本装置の Sync-E は，ITU-T G.8261 および G.8262 に準拠しています。Sync-E のサポート状況を次の表に示します。

表 20-17　Sync-E のサポート状況

項目	仕様
サポート可能なモデル	• IP8800/S3660-24X4QW • IP8800/S3660-48X4QW
外部クロックを受信できるインタフェース※1	• 10GBASE-R（SFP+） • 10GBASE-CU（SFP+）
外部クロックを適用できるインタフェース※2	• 10GBASE-R（SFP+） • 10GBASE-CU（SFP+）

注※1

マネージメントポートおよび QSFP28/QSFP+共用ポートは未サポートです。SFP+/SFP 共用ポートで SFP または SFP-T を使用した場合，そのポートでのクロック同期の動作は保証外です。

注※2

マネージメントポートは未サポートです。QSFP28/QSFP+共用ポートおよび SFP+/SFP 共用ポートで SFP または SFP-T を使用した場合，そのポートでのクロック同期の動作は保証外です。

(3)　基本動作

Sync-E の動作状態によって，使用するクロック周波数が異なります。

Sync-E が有効

指定した受信ポートで外部クロックと同期が取れた場合に，全ポートが外部クロックで動作します。指定したすべての受信ポートで外部クロックとの同期が外れると，内部クロックで動作します。

Sync-E が無効

内部クロックで動作します。

(4)　クロックの切り替え動作

本装置では，Sync-E の外部クロックを優先度を付けて二つまで指定でき，内部クロックと合わせて最大三つのクロックソースから同期先を選択します。選択の優先度が高い順に，クロックソースを次に示します。

1. 高優先の外部クロック
2. 低優先の外部クロック
3. 内部クロック

クロックソースとして選択しているクロックで障害が発生して同期が外れた場合，その時点で同期が取れているクロックのうち，最も優先度が高いクロックへすぐに自動で切り替えます。また，クロックソースとして優先度が低いクロックを選択している状態で優先度が高いクロックの同期が取れた場合，自動切り戻しを抑止する時間を経過してから，自動で切り替えます。Sync-E でのクロックの切り替え動作を次の表に示します。

表 20–18　Sync-E でのクロックの切り替え動作

切り替え契機	切り替え前同期先	切り替え後同期先	切り替え動作
選択しているクロックソースの同期が外れた場合	高優先の外部クロック	低優先の外部クロック	すぐに自動で切り替え
	高優先の外部クロック	内部クロック	
	低優先の外部クロック	内部クロック	
選択しているクロックソースよりも優先度が高いクロックと同期が取れた場合	低優先の外部クロック	高優先の外部クロック	切り戻し抑止時間経過後に自動で切り替え
	内部クロック	低優先の外部クロック	
	内部クロック	高優先の外部クロック	

(5)　Sync-E 状態の LED 表示

装置正面パネルの ST2 LED で外部クロック状態を確認できます。ただし，スタック構成時の ST2 LED はスタック状態を表示します。ST2 LED の状態と意味については，「ハードウェア取扱説明書」を参照してください。

(6)　禁止構成

外部クロックを指定するときは，同期先が同期元となるような構成にしないでください。そのような構成では，外部クロックが正しく同期できません。

図 20–7　Sync-E の禁止構成例 1（双方で外部クロックとして指定する構成）

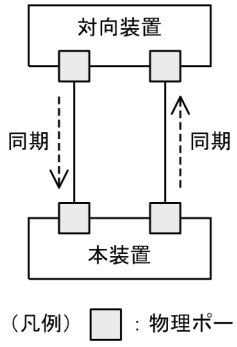
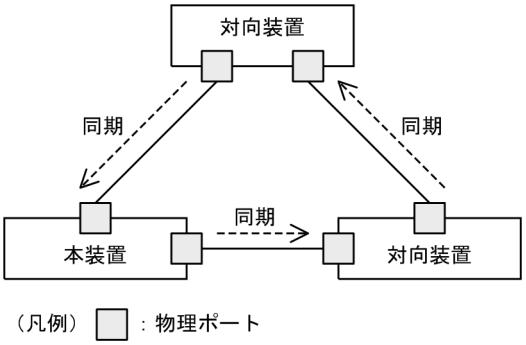


図 20–8　Sync-E の禁止構成例 2（本装置で指定した外部クロックの同期先が本装置となる構成）



(7)　注意事項

- スタックポートを経由した外部クロック同期は未サポートです。メンバスイッチごとに外部クロックを指定してください。
- 一次基準クロックを端末に同期するには，マスタースレーブのネットワークで同期するため，ネットワークのすべての装置が Sync-E に対応する必要があります。
- ポートのリンク状態に関係なく，同期が取れているポートをクロックソースとして選択します。そのため，プロトコルによる経路切り替えが発生しても，外部クロックは切り替わらない場合があります。

20.3　コンフィグレーション

20.3.1　コンフィグレーションコマンド一覧

イーサネットのコンフィグレーションコマンド一覧を次の表に示します。

表 20-19　コンフィグレーションコマンド一覧

コマンド名	説明
bandwidth	帯域幅を設定します。
description	補足説明を設定します。
duplex	duplex を設定します。
flowcontrol	フローコントロールを設定します。
frame-error-notice	フレーム受信エラーおよびフレーム送信エラー発生時のエラーの通知条件を設定します。
interface fortygigabitethernet	回線速度が最大 40Gbit/s のイーサネットインタフェースのコンフィグレーションを指定します。スタック専用ポートを実装するモデルでは, スタック機能が有効な場合にだけこのコマンドが設定されます。
interface gigabitethernet	回線速度が最大 1000Mbit/s のイーサネットインタフェースのコンフィグレーションを指定します。
interface hundredgigabitethernet	回線速度が最大 100Gbit/s のイーサネットインタフェースのコンフィグレーションを指定します。
interface tengigabitethernet	回線速度が最大 10Gbit/s のイーサネットインタフェースのコンフィグレーションを指定します。
link debounce	リンクダウン検出時間を設定します。
link up-debounce	リンクアップ検出時間を設定します。
mdix auto	自動 MDI/MDIX 機能を設定します。
mtu	イーサネットの MTU を設定します。
network-clock input-source	Sync-E の有効化と外部クロックの受信ポートを設定します。
network-clock preempt-delay	Sync-E の自動切り戻し抑止時間を設定します。
shutdown	イーサネットをシャットダウンします。
speed	速度を設定します。
system flowcontrol off	装置内の全ポートでフローコントロールを無効にします。
system mtu	イーサネットの MTU の装置としての値を設定します。

20.3.2　イーサネットインタフェースの設定

イーサネットインタフェースは, 接続するインタフェースに対応するコマンドで該当するモードに移行してから, コンフィグレーションを設定します。ポートの種類と対応するモード移行コマンドを次の表に示します。

表 20-20　ポートの種類と対応するモード移行コマンド

ポートの種類	モード移行コマンド
10BASE-T/100BASE-TX/1000BASE-T ポート	interface gigabitethernet
SFP ポート	interface gigabitethernet
100BASE-TX/1000BASE-T/10GBASE-T ポート	interface tengigabitethernet
SFP+ポート	interface tengigabitethernet
SFP+/SFP 共用ポート	interface tengigabitethernet
QSFP+ポート（スタック専用）	interface fortygigabitethernet
QSFP28/QSFP+共用ポート	interface hundredgigabitethernet

(1)　インタフェースに対するコンフィグレーションの設定

[設定のポイント]

イーサネットのコンフィグレーションでは，複数のコマンドでコンフィグレーションを設定することがあります。そのとき，コンフィグレーションの設定が完了していない状態でイーサネットがリンクアップ状態になると期待した通信ができません。したがって，最初にイーサネットをシャットダウンしてから，コンフィグレーションの設定が完了したあとにイーサネットのシャットダウンを解除することを推奨します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/10**
   イーサネットインタフェース 1/0/10 のコンフィグレーションモードに移行します。
2. **(config-if)# shutdown**
   イーサネットインタフェースをシャットダウンします。
3. **(config-if)# ＊＊＊＊＊**
   イーサネットインタフェースに対するコンフィグレーションを設定します。
4. **(config-if)# no shutdown**
   イーサネットインタフェースのシャットダウンを解除します。

(2)　インタフェースのシャットダウン

イーサネットをシャットダウンするには，該当するイーサネットインタフェースのコンフィグレーションモードに移行して，shutdown コマンドを実行します。使用しないイーサネットはシャットダウンしておいてください。

なお，運用コマンド inactivate でイーサネットの運用を停止することもできます。ただし，inactivate コマンドで inactive 状態とした場合は，装置を再起動するとイーサネットが active 状態になります。イーサネットをシャットダウンした場合は，装置を再起動してもイーサネットは disable 状態のままとなり，active 状態にするためにはコンフィグレーションで no shutdown を設定してシャットダウンを解除する必要があります。

20.3.3 複数インタフェースの一括設定

[設定のポイント]

イーサネットのコンフィグレーションでは，複数のインタフェースに同じ情報を設定することがあります。このような場合，複数のインタフェースを range 指定すると，情報を一括して設定できます。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-10, gigabitethernet 1/0/15-20, tengigabitethernet 1/0/25**
   ギガビットイーサネットインタフェース 1/0/1 から 1/0/10，1/0/15 から 1/0/20，および 10 ギガビットイーサネットインタフェース 1/0/25 のコンフィグレーションモードに移行します。
2. **(config-if-range)# ＊＊＊＊＊**
   複数のインタフェースに同じコンフィグレーションを一括して設定します。

20.3.4 速度と全二重の設定

次に示す場合は，必要に応じて各ポートに回線速度と全二重を設定します。

- 10BASE-T/100BASE-TX/1000BASE-T ポート
- 100BASE-TX/1000BASE-T/10GBASE-T ポート
- SFP ポートで SFP または SFP-T を使用
- SFP+/SFP 共用ポートで SFP または SFP-T を使用

デフォルトではオートネゴシエーションを使用します。オートネゴシエーションを使用しないで固定設定で接続する場合は，回線速度と全二重を設定します。固定設定で接続する場合は，speed コマンドと duplex コマンドの両方に固定設定をする必要があります。正しい組み合わせが設定されていない場合は，デフォルトで動作します。

なお，次に示す場合はインタフェース固有の回線速度および全二重固定のため，設定は不要です。

- SFP+ポート
- SFP+/SFP 共用ポートで SFP+を使用
- QSFP+ポート
- QSFP28/QSFP+共用ポート

(1) 回線速度と全二重を固定して相手装置と接続する場合

[設定のポイント]

オートネゴシエーションを使用しない場合は，回線速度と全二重を指定して，固定設定で接続します。ここでは，1000BASE-X ポートで，1000Mbit/s 全二重固定で相手装置と接続する場合の設定例を示します。

なお，回線速度を 1000Mbit/s に設定する場合は，必ず全二重に設定してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# shutdown
   (config-if)# speed 1000

(config-if)# duplex full

イーサネットインタフェースをシャットダウンして，相手装置と 1000Mbit/s 全二重固定で接続する設定をします。

2. **(config-if)# no shutdown**

イーサネットインタフェースのシャットダウンを解除します。

(2) オートネゴシエーションに対応していない相手装置と接続する場合

[設定のポイント]

10BASE-T および 100BASE-TX では，相手装置によってはオートネゴシエーションで接続できない場合があります。その場合は，相手装置に合わせて回線速度と全二重を指定して，固定設定で接続します。

ここでは，10BASE-T 全二重固定で相手装置と接続する場合の設定例を示します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/10**

(config-if)# shutdown

(config-if)# speed 10

(config-if)# duplex full

イーサネットインタフェースをシャットダウンして，相手装置と 10BASE-T 全二重固定で接続する設定をします。

2. **(config-if)# no shutdown**

イーサネットインタフェースのシャットダウンを解除します。

(3) オートネゴシエーションでも特定の速度を使用して相手装置と接続する場合

[設定のポイント]

本装置は，オートネゴシエーションで接続する場合でも，回線速度を設定できます。オートネゴシエーションに加えて回線速度を設定した場合，相手装置とオートネゴシエーションで接続しても，設定された回線速度にならないときはリンクがアップしません。そのため，意図しない回線速度で接続されることを防止できます。

ここでは，オートネゴシエーションを使用しても，回線速度は 1000Mbit/s だけで相手装置と接続する場合の設定例を示します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/10**

(config-if)# shutdown

(config-if)# speed auto 1000

イーサネットインタフェースをシャットダウンして，相手装置との接続にオートネゴシエーションを使用しても，回線速度は 1000Mbit/s だけで接続する設定をします。

2. **(config-if)# no shutdown**

イーサネットインタフェースのシャットダウンを解除します。

20.3.5 自動 MDI/MDIX 機能の設定

本装置はツイストペアケーブルを使用するポートで，自動 MDI/MDIX 機能をサポートしています。そのため，オートネゴシエーション時に，ケーブルのストレートまたはクロスに合わせて自動的に MDI 設定が切り替わり通信できます。また，本装置は MDI の固定機能を持っており，MDI 固定時は MDI-X（HUB 仕様）となります。

[設定のポイント]

自動 MDI/MDIX 機能を MDI-X に固定する場合に，固定したいインタフェースに設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/24**
   イーサネットインタフェース 1/0/24 のコンフィグレーションモードに移行します。
2. **(config-if)# no mdix auto**
   (config-if)# exit
   自動 MDI/MDIX 機能を無効にし，MDI-X 固定にします。

20.3.6 フローコントロールの設定

本装置では，フローコントロールをポート単位に設定したり，装置内の全ポートでフローコントロールを無効にしたりできます。装置内の全ポートでフローコントロールを無効にすると，ポート単位のフローコントロールの設定はコンフィグレーションファイルに残りますが，動作しません。

(1) ポート単位のフローコントロールの設定

[設定のポイント]

フローコントロールの設定内容は，相手装置と矛盾しないように決定してください。

[コマンドによる設定]

1. **(config)# interface tengigabitethernet 1/0/25**
   (config-if)# shutdown
   イーサネットインタフェースをシャットダウンします。
2. **(config-if)# flowcontrol send off**
   (config-if)# flowcontrol receive off
   相手装置とのポーズパケット送受信を停止します。
3. **(config-if)# no shutdown**
   イーサネットインタフェースのシャットダウンを解除します。

(2) 全ポート共通のフローコントロールの設定

[設定のポイント]

装置内の全ポートでフローコントロールを無効にします。

[コマンドによる設定]

1. **(config)# system flowcontrol off**
   全ポートで相手装置とのポーズパケット送受信の停止を設定します。

2. **(config)# save**
   (config)# exit
   保存して，コンフィグレーションモードから装置管理者モードに移行します。
3. **# restart vlan**
   VLAN プログラムを再起動します。全ポートで相手装置とのポーズパケット送受信を停止します。すべてのイーサネットインタフェースが再初期化され，VLAN を構成しているポートは一時的にデータの送受信ができなくなります。

(3) フローコントロールのルーズモード設定

[設定のポイント]

フローコントロールのルーズモードを設定します。

[コマンドによる設定]

1. **(config)# interface tengigabitethernet 1/0/25**
   (config-if)# shutdown
   イーサネットインタフェースをシャットダウンします。
2. **(config-if)# flowcontrol send on loose**
   相手装置とのポーズパケット送信をルーズモードにします。
3. **(config-if)# no shutdown**
   イーサネットインタフェースのシャットダウンを解除します。

20.3.7 ジャンボフレームの設定

イーサネットインタフェースの MTU は規格上 1500 オクテットです。本装置は，ジャンボフレームを使用して MTU を拡張し，一度に転送するデータ量を大きくすることでスループットを向上できます。

ジャンボフレームを使用するポートでは MTU を設定します。本装置は，設定された MTU に VLAN Tag が一つ付いているフレームを送受信できるようになります。

ポートの MTU の設定値は，ネットワークおよび相手装置と合わせて決定します。VLAN トンネリングなどで，VLAN Tag が二つ付く場合は，そのフレームを送受信できるように，MTU の値に 4 を加えた値を設定します。

(1) ポート単位の MTU の設定

[設定のポイント]

ポート 1/0/10 のポートの MTU を 8192 オクテットに設定します。この設定によって，8210 オクテットまでのジャンボフレームを送受信できるようになります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/10**
   (config-if)# shutdown
   (config-if)# mtu 8192
   イーサネットインタフェースをシャットダウンして，ポートの MTU を 8192 オクテットに設定します。
2. **(config-if)# no shutdown**

イーサネットインタフェースのシャットダウンを解除します。

(2) 全ポート共通の MTU の設定

[設定のポイント]

本装置の全イーサネットインタフェースでポートの MTU を 4096 オクテットに設定します。この設定によって，4114 オクテットまでのジャンボフレームを送受信できるようになります。

[コマンドによる設定]

1. **(config)# system mtu 4096**
   装置の全ポートで，ポートの MTU を 4096 オクテットに設定します。

20.3.8 リンクダウン検出タイマの設定

リンク障害を検出してからリンクダウンするまでのリンクダウン検出時間が短い場合，相手装置によってはリンクが不安定になることがあります。このような場合，リンクダウン検出タイマを設定することで，リンクが不安定になることを防ぐことができます。

[設定のポイント]

リンクダウン検出時間は，リンクが不安定とならない範囲でできるだけ短い値にします。リンクダウン検出時間を設定しなくてもリンクが不安定とならない場合は，リンクダウン検出時間を設定しないでください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/10**
   イーサネットインタフェース 1/0/10 のコンフィグレーションモードに移行します。
2. **(config-if)# link debounce time 5000**
   リンクダウン検出タイマを 5000 ミリ秒に設定します。

[注意事項]

リンクダウン検出時間を設定すると，リンクが不安定になることを防ぐことができますが，障害が発生した場合にリンクダウンするまでの時間が長くなります。リンク障害を検出してからリンクダウンするまでの時間を短くしたい場合は，リンクダウン検出タイマを設定しないでください。

20.3.9 リンクアップ検出タイマの設定

リンク障害回復を検出してからリンクアップするまでのリンクアップ検出時間が短い場合，相手装置によってはネットワーク状態が不安定になることがあります。このような場合，リンクアップ検出タイマを設定することで，ネットワーク状態が不安定になることを防ぐことができます。

[設定のポイント]

リンクアップ検出時間は，ネットワーク状態が不安定とならない範囲でできるだけ短い値にします。リンクアップ検出時間を設定しなくてもネットワーク状態が不安定とならない場合は，リンクアップ検出時間を設定しないでください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/10**
   イーサネットインタフェース 1/0/10 のコンフィグレーションモードに移行します。

2. **(config-if)# link up-debounce time 5000**
   リンクアップ検出タイマを 5000 ミリ秒に設定します。

[注意事項]

リンクアップ検出タイマを長く設定すると，リンク障害回復から通信できるまでの時間が長くなります。リンク障害回復から通信できるまでの時間を短くしたい場合は，リンクアップ検出タイマを設定しないでください。

20.3.10　フレーム送受信エラー通知の設定

軽度のエラーが発生してフレームの受信または送信に失敗した場合, 本装置はフレームが廃棄された原因を統計情報として採取します。30 秒間に発生したエラーの回数とエラーの発生する割合が閾値を超えた場合は，エラーの発生について，ログで通知し，プライベートの SNMP 通知を送信します。

本装置では，閾値とエラーが発生した場合の通知について設定ができます。設定がない場合，30 秒間に 15 回エラーが発生したときに最初の 1 回だけログを表示します。

(1)　エラーフレーム数を閾値にしての通知

[設定のポイント]

エラーの通知条件のうち，エラーの発生回数（エラーフレーム数）の閾値を本装置に設定する場合は，frame-error-notice コマンドで error-frames を設定します。

[コマンドによる設定]

1. **(config)# frame-error-notice error-frames 50**
   エラーの発生回数（エラーフレーム数）の閾値を 50 回に設定します。

(2)　エラーレートを閾値にしての通知

[設定のポイント]

エラーの通知条件のうち, エラーの発生割合（エラーレート）の閾値を本装置に設定する場合は, frame-error-notice コマンドで error-rate を設定します。

[コマンドによる設定]

1. **(config)# frame-error-notice error-rate 20**
   エラーの発生割合の閾値を 20%に設定します。

(3)　通知時のログ表示設定

[設定のポイント]

エラーの通知条件のうち，エラーが発生したときのログの表示を設定する場合は，frame-error-notice コマンドで onetime-display，または everytime-display を設定します。ログを表示しないようにする場合は，off を設定します。この設定は，プライベートの SNMP 通知には関係しません。

[コマンドによる設定]

1. **(config)# frame-error-notice everytime-display**
   エラーが発生するたびにログを表示します。

(4) 条件の組み合わせ設定

[設定のポイント]

エラーの通知条件を複数組み合わせて設定する場合は，frame-error-notice コマンドで，複数の条件を同時に設定します。frame-error-notice コマンド入力前に設定していた通知条件は無効となりますので，引き続き同じ通知条件を設定する場合は，frame-error-notice コマンドで再度設定し直してください。

[コマンドによる設定]

すでにエラーが発生するたびにログを表示することを設定していて，さらにエラーの発生割合（エラーレート）の閾値を設定する場合の設定例を示します。

1. **(config)# frame-error-notice error-frames 50 everytime-display**
   エラーの発生回数（エラーフレーム数）の閾値を 50 回に設定し，エラーが発生するたびにログを表示します。

[注意事項]

プライベートの SNMP 通知を使用する場合は，snmp-server host コマンドでフレーム受信エラー発生時の SNMP 通知とフレーム送信エラー発生時の SNMP 通知を送信するように設定してください。

20.3.11 Sync-E の設定

Sync-E の有効化と，外部クロックの受信ポート番号を設定します。

[設定のポイント]

外部クロックの受信ポート番号を設定することで，Sync-E を有効にします。この例では，外部クロックの受信ポートとして優先度の高いポートに 1/0/1，優先度の低いポートに 1/0/2 を設定します。

[コマンドによる設定]

1. **(config)# network-clock input-source 1 interface tengigabitethernet 1/0/1**
   Sync-E を有効にして，優先度 1 で外部クロックの受信ポートに 1/0/1 を設定します。
2. **(config)# network-clock input-source 2 interface tengigabitethernet 1/0/2**
   優先度 2 で外部クロックの受信ポートに 1/0/2 を設定します。

20.4　オペレーション

20.4.1　運用コマンド一覧

イーサネットの運用コマンド一覧を次の表に示します。

表 20-21　運用コマンド一覧

コマンド名	説明
show interfaces	イーサネットの情報を表示します。
clear counters	イーサネットの統計情報カウンタをクリアします。
show port	イーサネットの情報を一覧で表示します。
activate	inactive 状態のイーサネットを active 状態にします。
inactivate	active 状態のイーサネットを inactive 状態にします。
test interfaces	回線テストを実行します。
no test interfaces	回線テストを停止し，結果を表示します。
show network-clock	Sync-E の動作状態を表示します。

20.4.2　イーサネットの動作状態の確認

show port コマンドを実行すると，本装置に実装している全イーサネットの状態を確認できます。使用するイーサネットの Status の表示が up になっていることを確認します。show port コマンドの実行結果を次の図に示します。

図 20-9　show port コマンドの実行結果

```
> show port
Date 20XX/11/21 15:16:19 UTC
Port Counts: 24
Port  Name             Status   Speed       Duplex     FCtl FrLen ChGr/Status
 0/ 1 geth1/0/1        up       1000BASE-SX full(auto) off   1518   -/-
 0/ 2 geth1/0/2        down     -           -          -     -      -/-
 0/ 3 geth1/0/3        up       100BASE-TX  full(auto) off   1518   -/-
 0/ 4 geth1/0/4        up       1000BASE-SX full(auto) off   1518   -/-
      :
      :
```

20.4.3　Sync-E の確認

show network-clock コマンドを実行すると，Sync-E の情報を表示します。外部クロックで正常に同期している場合は，「Status：Sync」を表示します。show network-clock コマンドの実行結果を次の図に示します。

図 20-10　show network-clock コマンドの実行結果

```
> show network-clock synchronization
Date 20XX/07/04 11:23:45 UTC
Current input source
Priority  : 1
Port      : 1/0/1
Status    : Sync                    …1

Source status
```

```
  Pri Port   Link Clock
    1 1/0/1  Up   Lock
    2 1/0/2  Up   Lock
>
```

1.Sync-E が有効で，外部クロックの動作は同期正常状態であることを示しています。

21 リンクアグリゲーション

この章では，リンクアグリゲーションの解説と操作方法について説明します。

21.1　リンクアグリゲーション基本機能の解説

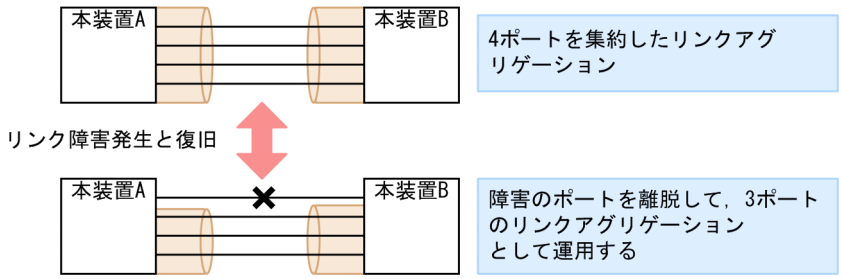
21.1.1　概要

リンクアグリゲーションは，隣接装置との間を複数のイーサネットポートで接続し，それらを束ねて一つの仮想リンクとして扱う機能です。この仮想リンクをチャネルグループと呼びます。リンクアグリゲーションによって接続装置間の帯域の拡大や冗長性を確保できます。

21.1.2　リンクアグリゲーションの構成

リンクアグリゲーションの構成例を次の図に示します。この例では四つのポートを集約しています。集約しているポートのうちの 1 本が障害となった場合には，チャネルグループから離脱し，残りのポートでチャネルグループとして通信を継続します。

図 21-1　リンクアグリゲーションの構成例



21.1.3　サポート仕様

(1)　リンクアグリゲーションのモード

本装置のリンクアグリゲーションは，モードとして LACP およびスタティックの 2 種類をサポートします。

- LACP リンクアグリゲーション

  IEEE802.1AX 準拠の LACP を利用したリンクアグリゲーションです。LACP によるネゴシエーションが成功した場合にチャネルグループとしての運用を開始します。LACP によって，隣接装置との整合性確認やリンクの正常性確認ができます。

- スタティックリンクアグリゲーション

  コンフィグレーションによるスタティックなリンクアグリゲーションです。LACP は動作させません。チャネルグループとして設定したポートがリンクアップした時点で運用を開始します。

(2)　回線速度

チャネルグループを構成するポートのうち，最速かつ同一速度のポートを集約します。異なる回線速度のポートを集約する場合は，異速度混在モードを有効にする必要があります。

21.1.4　チャネルグループの MAC アドレス

スパニングツリーなどのプロトコルを運用する際に，チャネルグループの MAC アドレスを使用します。本装置は，チャネルグループの MAC アドレスとして，グループに所属するポートのうちどれかの MAC アドレスを使用します。

チャネルグループに所属するポートから MAC アドレスを使用しているポートを削除すると，チャネルグループの MAC アドレスが変更されます。

スタック構成で運用している場合, メンバスイッチの削除に伴って MAC アドレスを使用しているポートのイーサネットインタフェースを削除すると，チャネルグループの MAC アドレスが変更されます。また，チャネルグループの MAC アドレスにマスタスイッチのポートの MAC アドレスを使用している場合，マスタスイッチに障害が発生してバックアップスイッチが新しいマスタスイッチになると, チャネルグループの MAC アドレスも変更されます。

21.1.5　フレーム送信時のポート振り分け

リンクアグリゲーションへフレームを送信するとき, 送信するフレームごとにポートを選択しトラフィックを各ポートへ分散させることで複数のポートを効率的に利用します。ポートの振り分けは, 送信するフレーム内の情報を基にポートを選択して振り分けます。

ポートの振り分けに使用する情報を次の表に示します。

表 21-1　フレーム送信時のポート振り分け（1/2）

中継	フレームの種類	振り分けに使用する情報	port-channel load-balance パラメータ				
			src-mac	dst-mac	src-dst-mac	src-ip	src-port
レイヤ 3 中継	IP ユニキャスト IP ブロードキャスト	宛先 MAC アドレス	－	○	○	－	－
		送信元 MAC アドレス	○	－	○	－	－
		受信 VLAN	○	○	○	－	－
		イーサタイプ	○	○	○	－	－
		宛先 IP アドレス	－	－	－	－	－
		送信元 IP アドレス	－	－	－	○	○
		宛先 TCP/UDP ポート番号	－	－	－	－	－
		送信元 TCP/UDP ポート番号	－	－	－	－	○
	IP マルチキャスト	宛先 IP アドレス	○	○	○	○	○
		送信元 IP アドレス	○	○	○	○	○
		受信ポート番号または受信チャネルグループ番号	○	○	○	○	○
レイヤ 2 中継	MAC アドレス未学習フレーム（ユニキャスト/ブロードキャスト/マルチキャスト）	宛先 MAC アドレス	○	○	○	○	○
		送信元 MAC アドレス	○	○	○	○	○
		受信ポート番号または受信チャネルグループ番号	○	○	○	○	○

中継	フレームの種類	振り分けに使用する情報	port-channel load-balance パラメータ				
			src-mac	dst-mac	src-dst-mac	src-ip	src-port
	MAC アドレス学習済の IP フレーム	宛先 MAC アドレス	−	○	○	−	−
		送信元 MAC アドレス	○	−	○	−	−
		VLAN	○	○	○	−	−
		イーサタイプ	○	○	○	−	−
		宛先 IP アドレス	−	−	−	−	−
		送信元 IP アドレス	−	−	−	○	○
		宛先 TCP/UDP ポート番号	−	−	−	−	−
		送信元 TCP/UDP ポート番号	−	−	−	−	○
	MAC アドレス学習済の非 IP フレーム	宛先 MAC アドレス	−	○	○	−	−
		送信元 MAC アドレス	○	−	○	○	○
		VLAN	○	○	○	○	○
		イーサタイプ	○	○	○	○	○

表 21-2　フレーム送信時のポート振り分け（2/2）

中継	フレームの種類	振り分けに使用する情報	port-channel load-balance パラメータ			
			dst-ip	dst-port	src-dst-ip	src-dst-port
レイヤ 3 中継	IP ユニキャスト IP ブロードキャスト	宛先 MAC アドレス	−	−	−	−
		送信元 MAC アドレス	−	−	−	−
		受信 VLAN	−	−	−	−
		イーサタイプ	−	−	−	−
		宛先 IP アドレス	○	○	○	○
		送信元 IP アドレス	−	−	○	○
		宛先 TCP/UDP ポート番号	−	○	−	○
		送信元 TCP/UDP ポート番号	−	−	−	○
	IP マルチキャスト	宛先 IP アドレス	○	○	○	○
		送信元 IP アドレス	○	○	○	○
		受信ポート番号または受信チャネルグループ番号	○	○	○	○

中継	フレームの種類	振り分けに使用する情報	port-channel load-balance パラメータ			
			dst-ip	dst-port	src-dst-ip	src-dst-port
レイヤ 2 中継	MAC アドレス未学習フレーム (ユニキャスト/ブロードキャスト/マルチキャスト)	宛先 MAC アドレス	○	○	○	○
		送信元 MAC アドレス	○	○	○	○
		受信ポート番号 または受信チャネルグループ番号	○	○	○	○
	MAC アドレス学習済の IP フレーム	宛先 MAC アドレス	−	−	−	−
		送信元 MAC アドレス	−	−	−	−
		VLAN	−	−	−	−
		イーサタイプ	−	−	−	−
		宛先 IP アドレス	○	○	○	○
		送信元 IP アドレス	−	−	○	○
		宛先 TCP/UDP ポート番号	−	○	−	○
		送信元 TCP/UDP ポート番号	−	−	−	○
	MAC アドレス学習済の非 IP フレーム	宛先 MAC アドレス	○	○	○	○
		送信元 MAC アドレス	−	−	○	○
		VLAN	○	○	○	○
		イーサタイプ	○	○	○	○

（凡例）○：振り分け対象　　−：振り分け対象外

リンクアグリゲーション上のトラフィックに応じて振り分け方法を適切に選択すると，効率的にロードバランスができます。例えば，単一の MAC アドレスを持つホストから複数の MAC アドレス宛てに IP フレームを送信する場合，dst-mac を選択すると，src-mac を選択したときよりも効率的に送信ポートを振り分けられます。

● スタック構成時のポート振り分け

スタック構成時のポート振り分けについては，「7.6.2　リンクアグリゲーションの転送動作」を参照してください。

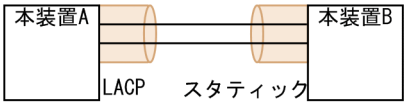
21.1.6　リンクアグリゲーション使用時の注意事項

(1)　リンクアグリゲーションが不可能な構成

リンクアグリゲーション構成時には，装置間での設定が一致している必要があります。リンクアグリゲーションが不可能な構成例を次に示します。

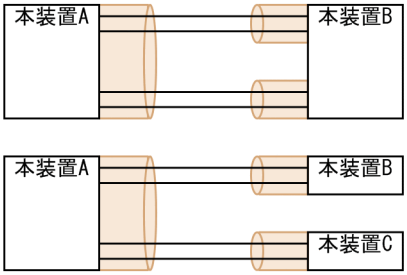
図 21-2　リンクアグリゲーションが不可能な構成例

●装置間でモードが異なる場合



この構成を実施したときの動作
・LACPのネゴシエーションが成立しないで通信断状態になる。

●装置間でチャネルグループがポイントーマルチポイントになっている場合



この構成を実施したときの動作
・本装置Aから送信したフレームが本装置Bを経由して戻る
　ループ構成になるなど，正常に動作しない。

(2)　リンクアグリゲーションの設定手順

リンクアグリゲーション構成時には，装置間での設定が一致している必要があります。一致していない状態で通信を開始しようとするとループ構成となるおそれがあります。設定はリンクダウン状態で行い，「(1) リンクアグリゲーションが不可能な構成」のような構成になっていないことを確認したあとで，ポートをリンクアップさせることをお勧めします。

(3)　CPU 過負荷時

LACP リンクアグリゲーションモード使用時に CPU が過負荷な状態になった場合，本装置が送受信する LACPDU の廃棄または処理遅延が発生して，タイムアウトのメッセージ出力，一時的な通信断になることがあります。過負荷状態が頻発する場合は，LACPDU の送信間隔を長くするか，スタティックリンクアグリゲーションを使用してください。

21.2　リンクアグリゲーション基本機能のコンフィグレーション

21.2.1　コンフィグレーションコマンド一覧

リンクアグリゲーション基本機能のコンフィグレーションコマンド一覧を次の表に示します。

表 21-3　コンフィグレーションコマンド一覧

コマンド名	説明
channel-group lacp system-priority	チャネルグループごとに LACP システム優先度を設定します。
channel-group mode	ポートをチャネルグループに登録します。
channel-group periodic-timer	LACPDU の送信間隔を設定します。
description	チャネルグループの補足説明を設定します。
interface port-channel	ポートチャネルインタフェースを設定します。 チャネルグループのパラメータもポートチャネルインタフェースコンフィグレーションモードで設定します。
lacp port-priority	LACP のポート優先度を設定します。
lacp system-priority	LACP システム優先度のデフォルト値を設定します。
port-channel load-balance	振り分け方法を指定します。
shutdown	チャネルグループの通信を停止します。
system port-channel load-balance-all-port※	フレーム送信時のポート振り分けで，すべてのメンバスイッチのポートを振り分け対象とします。

注※

「コンフィグレーションコマンドレファレンス Vol.1」「10　装置の管理」を参照してください。

21.2.2　スタティックリンクアグリゲーションの設定

[設定のポイント]

スタティックリンクアグリゲーションは，イーサネットインタフェースコンフィグレーションモードで channel-group mode コマンドを使用してチャネルグループ番号と「on」のモードを設定します。スタティックリンクアグリゲーションは channel-group mode コマンドを設定することによって動作を開始します。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**
   ポート 1/0/1，1/0/2 のイーサネットインタフェースモードに移行します。
2. **(config-if-range)# channel-group 10 mode on**
   ポート 1/0/1，1/0/2 を，スタティックモードのチャネルグループ 10 に登録します。

21.2.3　LACP リンクアグリゲーションの設定

(1)　チャネルグループの設定

[設定のポイント]

LACP リンクアグリゲーションは，イーサネットインタフェースコンフィグレーションモードで channel-group mode コマンドを使用してチャネルグループ番号と「active」または「passive」のモードを設定します。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**
   ポート 1/0/1，1/0/2 のイーサネットインタフェースモードに移行します。
2. **(config-if-range)# channel-group 10 mode active**
   ポート 1/0/1，1/0/2 を LACP モードのチャネルグループ 10 に登録します。LACP は active モードとして対向装置に関係なく LACPDU の送信を開始します。passive を指定した場合は，対向装置からの LACPDU を受信したときだけ LACPDU の送信を開始します。

(2)　システム優先度の設定

LACP のシステム優先度を設定します。本装置では，システム優先度は拡張機能の離脱ポート制限機能で使用します。通常，本パラメータを変更する必要はありません。

[設定のポイント]

LACP システム優先度は値が小さいほど高い優先度となります。

[コマンドによる設定]

1. **(config)# lacp system-priority 100**
   本装置の LACP システム優先度を 100 に設定します。
2. **(config)# interface port-channel 10**
   (config-if)# channel-group lacp system-priority 50
   チャネルグループ 10 の LACP システム優先度を 50 に設定します。本設定を行わない場合は装置のシステム優先度である 100 を使用します。

(3)　ポート優先度の設定

LACP のポート優先度を設定します。本装置では，ポート優先度は拡張機能のスタンバイリンク機能で使用します。通常，本パラメータを変更する必要はありません。

[設定のポイント]

LACP ポート優先度は値が小さいほど高い優先度となります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# lacp port-priority 100
   ポート 1/0/1 の LACP ポート優先度を 100 に設定します。

(4)　LACPDU 送信間隔の設定

[設定のポイント]

対向装置が本装置に向けて送信する LACPDU の間隔を設定します。本装置は本パラメータで設定した間隔で LACPDU を受信します。

LACPDU の送信間隔は long（30 秒），short（1 秒）のどちらかを選択します。デフォルトは long（30 秒）で動作します。送信間隔を short（1 秒）に変更した場合，リンクの障害によるタイムアウトを検知しやすくなり，障害時に通信が途絶える時間を短く抑えることができます。

[コマンドによる設定]

1. **(config)# interface port-channel 10**
   (config-if)# channel-group periodic-timer short
   チャネルグループ 10 の LACPDU 送信間隔を short（1 秒）に設定します。

[注意事項]

LACPDU 送信間隔を short（1 秒）に設定すると，障害を検知しやすくなる一方で，LACPDU トラフィックが増加することによってリンクアグリゲーションプログラムの負荷が増加します。本パラメータを short（1 秒）にすることでタイムアウトのメッセージや一時的な通信断が頻発する場合は，デフォルトの long（30 秒）に戻すかスタティックモードを使用してください。

(5)　振り分け方法の設定

[設定のポイント]

装置単位でチャネルグループの振り分け方法を指定します。

[コマンドによる設定]

1. **(config)# port-channel load-balance src-ip**
   フレームを送信元 IP アドレスによって振り分けるように，チャネルグループの振り分け方法を設定します。

21.2.4　ポートチャネルインタフェースの設定

ポートチャネルインタフェースでは，チャネルグループ上で動作する機能を設定します。

ポートチャネルインタフェースは，コンフィグレーションコマンドで設定するか，イーサネットインタフェースコンフィグレーションモードで channel-group mode コマンドを設定することによって自動的に生成されます。

(1)　ポートチャネルインタフェースとイーサネットインタフェースの関係

ポートチャネルインタフェースは，チャネルグループ上で動作する機能を設定します。それらはイーサネットインタフェースコンフィグレーションモードでも設定することができます。このような機能を設定するコマンドはポートチャネルインタフェースとイーサネットインタフェースで関連性があり，設定する際に次のように動作します。

- ポートチャネルインタフェースとイーサネットインタフェースで関連コマンドの設定が一致している必要があります。
- ポートチャネルインタフェースを未設定の状態でイーサネットインタフェースに channel-group mode コマンドを設定すると，自動的にポートチャネルインタフェースを生成します。このとき，

channel-group mode コマンドを設定するイーサネットインタフェースに関連コマンドが設定されていてはいけません。

- ポートチャネルインタフェースがすでに設定済みの状態でイーサネットインタフェースに channel-group mode コマンドを設定する場合，関連コマンドが一致している必要があります。
- ポートチャネルインタフェースで関連コマンドを設定すると，channel-group mode コマンドで登録されているイーサネットインタフェースの設定にも同じ設定が反映されます。

ポートチャネルインタフェースとイーサネットインタフェースで一致している必要のあるポートチャネル関連コマンドを次の表に示します。

表 21-4　ポートチャネルインタフェースの関連コマンド

機能	コマンド
VLAN	switchport mode
	switchport access
	switchport trunk
	switchport protocol
	switchport mac
	switchport vlan mapping
	switchport vlan mapping enable
スパニングツリー	spanning-tree portfast
	spanning-tree bpdufilter
	spanning-tree bpduguard
	spanning-tree guard
	spanning-tree link-type
	spanning-tree port-priority
	spanning-tree cost
	spanning-tree vlan port-priority
	spanning-tree vlan cost
	spanning-tree single port-priority
	spanning-tree single cost
	spanning-tree mst port-priority
	spanning-tree mst cost
IEEE802.1X	dot1x port-control
	dot1x force-authorize-port
	dot1x multiple-hosts
	dot1x multiple-authentication

機能	コマンド
	dot1x max-supplicant
	dot1x reauthentication
	dot1x timeout reauth-period
	dot1x timeout tx-period
	dot1x timeout supp-timeout
	dot1x timeout server-timeout
	dot1x timeout keep-unauth
	dot1x timeout quiet-period
	dot1x max-req
	dot1x ignore-eapol-start
	dot1x supplicant-detection
DHCP snooping	ip dhcp snooping trust
	ip arp inspection trust
	ip verify source
GSRP	gsrp direct-link
	gsrp reset-flush-port
	gsrp no-flush-port
	gsrp exception-port
L2 ループ検知	loop-detection
OADP	oadp enable

(2)　チャネルグループ上で動作する機能の設定

[設定のポイント]

ポートチャネルインタフェースでは，VLAN やスパニングツリーなど，チャネルグループ上で動作する機能を設定します。ここでは，トランクポートを設定する例を示します。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**
   (config-if-range)# channel-group 10 mode on
   (config-if-range)# exit
   ポート 1/0/1，1/0/2 をスタティックモードのチャネルグループ 10 に登録します。また，チャネルグループ 10 のポートチャネルインタフェースが自動生成されます。
2. **(config)# interface port-channel 10**
   チャネルグループ 10 のポートチャネルインタフェースコンフィグレーションモードに移行します。
3. **(config-if)# switchport mode trunk**

チャネルグループ 10 をトランクポートに設定します。

(3) ポートチャネルインタフェースの shutdown

[設定のポイント]

ポートチャネルインタフェースを shutdown に設定すると, チャネルグループに登録されているすべてのポートの通信を停止します。リンクアップしているポートはアップ状態のまま通信停止状態になります。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**
   (config-if-range)# channel-group 10 mode on
   (config-if-range)# exit
   ポート 1/0/1，1/0/2 をスタティックモードのチャネルグループ 10 として登録します。
2. **(config)# interface port-channel 10**
   (config-if)# shutdown
   ポートチャネルインタフェースコンフィグレーションモードに移行して shutdown を設定します。
   ポート 1/0/1，1/0/2 の通信が停止し，チャネルグループ 10 は停止状態になります。

21.2.5 チャネルグループの削除

チャネルグループのポートやチャネルグループ全体を削除する場合は, 削除する対象のポートをあらかじめイーサネットインタフェースコンフィグレーションモードで shutdown に設定しておく必要があります。shutdown に設定することで，削除する際にループが発生することを防ぎます。

(1) チャネルグループ内のポートの削除

[設定のポイント]

ポートをチャネルグループから削除します。削除したポートはチャネルグループとは別のポートとして動作するため，削除時のループを回避するために事前に shutdown に設定します。

削除したポートには, 削除前に interface port-channel で設定した関連コマンド（表 21-4　ポートチャネルインタフェースの関連コマンド）は残るため，別の用途に使用する際には注意してください。

チャネルグループ内のすべてのポートを削除しても，interface port-channel の設定は自動的には削除されません。チャネルグループ全体の削除は「(2)　チャネルグループ全体の削除」を参照してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# shutdown
   ポート 1/0/1 をチャネルグループから削除するために，事前に shutdown にしてリンクダウンさせます。
2. **(config-if)# no channel-group**
   ポート 1/0/1 からチャネルグループの設定を削除します。

(2)　チャネルグループ全体の削除

[設定のポイント]

チャネルグループ全体を削除します。削除したチャネルグループに登録していたポートはそれぞれ個別のポートとして動作するため，削除時のループを回避するために事前に shutdown に設定します。

チャネルグループは interface port-channel を削除することによって，全体が削除されます。この削除によって，登録していた各ポートから channel-group mode コマンドが自動的に削除されます。ただし，各ポートには削除前に interface port-channel で設定した関連コマンド（表 21–4　ポートチャネルインタフェースの関連コマンド）は残るため，別の用途に使用する際には注意してください。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**
   (config-if-range)# shutdown
   (config-if-range)# exit
   チャネルグループ全体を削除するために，削除したいチャネルグループに登録されているポートをすべて shutdown に設定しリンクダウンさせます。
2. **(config)# no interface port-channel 10**
   チャネルグループ 10 を削除します。ポート 1/0/1，1/0/2 に設定されている channel-group mode コマンドも自動的に削除されます。

21.3　リンクアグリゲーション拡張機能の解説

21.3.1　スタンバイリンク機能

(1)　解説

チャネルグループ内にあらかじめ待機用のポートを用意しておき，運用中のポートで障害が発生したときに待機用のポートに切り替えることによって，グループとして運用するポート数を維持する機能です。この機能を使用すると，障害時に帯域の減少を防ぐことができます。

この機能は，スタティックリンクアグリゲーションだけ使用できます。

(2)　スタンバイリンクの選択方法

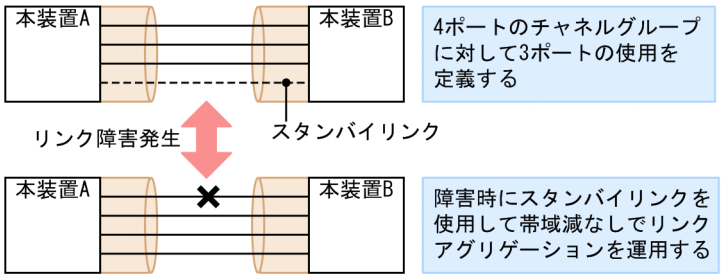
コンフィグレーションでチャネルグループとして運用する最大ポート数を設定します。グループに属するポート数が指定された最大ポート数を超えた分のポートが待機用ポートになります。

待機用ポートは，まずコンフィグレーションで設定するポート優先度，次にスイッチ番号およびポート番号の順で，選択優先度の高い順に決定されます。つまり，ポート優先度が同じ場合は，NIF 番号，ポート番号の順に判断します。待機用ポートの決定基準を，選択優先度の高い順に次に示します。

1. ポート優先度
   優先度の値の大きいポートから待機用ポートとして選択されます。
2. スイッチ番号
   スイッチ番号の大きい順に待機用ポートとして選択されます。
3. ポート番号
   ポート番号の大きい順に待機用ポートとして選択されます。

スタンバイリンク機能の例を次の図に示します。この例では，グループに属するポート数を 4，運用する最大ポート数を 3 としています。

図 21-3　スタンバイリンク機能の構成例



(3)　スタンバイリンクのモード

スタンバイリンク機能には，次に示す二つのモードがあります。

- リンクダウンモード
  スタンバイリンクをリンクダウン状態にします。スタンバイリンク機能をサポートしていない対向装置も待機用ポートにすることができます。
- 非リンクダウンモード

スタンバイリンクをリンクダウン状態にしないで，送信だけを停止します。リンクアップ状態のため，待機中のポートでも障害を監視できます。また，待機中のポートは送信だけを停止して，受信は行います。スタンバイリンク機能をサポートしていない対向装置は，リンクダウンが伝わらないためスタンバイリンク上で送信を継続しますが，そのような対向装置とも接続できます。

リンクダウンモードを使用している場合，運用中のポートが一つのとき，そのポートで障害が発生すると，待機用のポートに切り替わる際にチャネルグループがいったんダウンします。非リンクダウンモードの場合，ダウンせずに待機用ポートを使用します。

運用中のポートが一つの状態とは，次に示すどちらかの状態です。

- コンフィグレーションコマンド max-active-port で 1 を設定している状態。
- 異速度混在モードを未設定で，最高速のポートが一つだけ，そのほかのポートが一つ以上ある状態。

(4)　スタック構成での注意事項

スタンバイリンク機能をリンクダウンモードで使用して，バックアップスイッチ側のポートが待機用ポートに選択されているとき，マスタスイッチまたはスタックリンクに障害が発生してバックアップスイッチが新しいマスタスイッチに切り替わると，該当する待機用ポートはダウンしたままになります。このときは，運用コマンド activate でそのポートを active 状態にしてください。

21.3.2　離脱ポート制限機能

離脱ポート制限機能は，リンクに障害が発生したポートを離脱して残りのポートで運用を継続する機能を抑止します。チャネルグループのどれかのポートに障害が発生するとグループ全体を障害とみなして，該当チャネルグループの運用を停止します。グループ内の全ポートが復旧するとグループの運用を再開します。

GSRP などの冗長化機能と合わせて運用することで，チャネルグループ内に 1 ポートだけ障害が発生した場合でも，グループ単位で経路を切り替えることができます。

この機能は LACP リンクアグリゲーションだけ使用できます。

離脱ポート制限機能の集約動作は，チャネルグループで接続する装置間で，優先度の高い装置が，自装置および対向装置のチャネルグループ内の全ポートで集約可能な状態と判断できた場合に集約します。そうすることで，一部のポートだけが集約することがないようにしており，帯域保証しています。

優先度は，まずコンフィグレーションで設定する LACP システム優先度，次にチャネルグループの MAC アドレスの順で判断されます。つまり，LACP システム優先度が同じ場合は，チャネルグループの MAC アドレスで判断します。

チャネルグループ内の全ポートが集約可能か判定する装置の決定基準を，選択優先度の高い順に次に示します。

1. LACP システム優先度
   LACP システム優先度の値が小さい装置が優先されます。
2. チャネルグループの MAC アドレス
   MAC アドレスの小さい装置が優先されます。

21.3.3　異速度混在モード

異なる速度のポートを一つのチャネルグループで同時に使用するモードです。通常は同じ速度のポートでチャネルグループを構成しますが，異なる速度のポートで構成することで，スタンバイリンクに低速ポートを使用することや，チャネルグループの構成変更を容易に行えます。本機能の適用例を次に示します。

なお，フレーム送信時のポート振り分けにはポートの速度は反映しません。例えば，異速度混在モードで1Gbit/s のポートと 10Gbit/s のポートを使用していても，その速度の差はフレーム振り分けには反映しません。通常の運用時は同じ速度のポートで運用することをお勧めします。

(1)　スタンバイリンク機能での適用例

高速なポートに対して低速なポートを待機用ポートにすることができます。例えば，10Gbit/s ポートで接続する際に，最大ポート数を 1 としてスタンバイリンク機能を適用して，待機用ポートに 1Gbit/s のポートを設定します。10Gbit/s のポートに障害が発生した場合にも 1Gbit/s のポートで通信を継続できます。

異速度混在モードでスタンバイリンクを適用する際は，最大ポート数を 1 とすることをお勧めします。最大ポート数を 2 以上とした場合は，通常運用に異なる速度のポートが混在することがあります。また，最大ポート数を 1 として運用する場合は，非リンクダウンモードを使用することをお勧めします。リンクダウンモードで最大ポート数が 1 の場合は，切り替え時にチャネルグループがいったんダウンします。

(2)　チャネルグループの構成変更手順での適用例

本機能によって，チャネルグループで利用するポートの速度を変更（ネットワーク構成の変更）する際に，チャネルグループをダウンさせないで構成を変更できます。

異速度混在モードを利用したチャネルグループの速度移行について，移行手順の具体例を次に示します。

1. 従来状態で運用（1Gbit/s の 2 ポートとします）
2. 異速度混在モードを設定
3. チャネルグループに 10Gbit/s の 2 ポートを追加
   異速度混在モード未設定時は，この手順でリンクアグリゲーションがいったんダウンします。
4. 手順 3 で追加した 10Gbit/s の 2 ポートをリンクアップ
5. 従来の 1Gbit/s の 2 ポートをリンクダウン
6. 従来の 1Gbit/s の 2 ポートをチャネルグループから削除
7. 10Gbit/s の 2 ポートに移行完了

21.4　リンクアグリゲーション拡張機能のコンフィグレーション

21.4.1　コンフィグレーションコマンド一覧

リンクアグリゲーション拡張機能のコンフィグレーションコマンド一覧を次の表に示します。

表 21-5　コンフィグレーションコマンド一覧

コマンド名	説明
channel-group lacp system-priority	システム優先度をチャネルグループごとに設定します。離脱ポート制限機能で集約条件を判定する装置を決定します。
channel-group max-active-port	スタンバイリンク機能を設定し，最大ポート数を指定します。
channel-group max-detach-port	離脱ポート制限機能を設定します。
channel-group multi-speed	異速度混在モードを設定します。
lacp port-priority	ポート優先度を設定します。スタンバイリンクを選択するために使用します。
lacp system-priority	システム優先度のデフォルト値を設定します。離脱ポート制限機能で集約条件を判定する装置を決定します。

21.4.2　スタンバイリンク機能のコンフィグレーション

[設定のポイント]

チャネルグループにスタンバイリンク機能を設定して，同時に最大ポート数を設定します。また，リンクダウンモード，非リンクダウンモードのどちらかを設定します。スタンバイリンク機能は，スタティックリンクアグリゲーションだけで使用できます。

待機用ポートはポート優先度によって設定し，優先度が低いポートからスタンバイリンクに選択します。ポート優先度は値が小さいほど高い優先度になります。

[コマンドによる設定]

1. **(config)# interface port-channel 10**
   チャネルグループ 10 のポートチャネルインタフェースコンフィグレーションモードに移行します。
2. **(config-if)# channel-group max-active-port 3**
   チャネルグループ 10 にスタンバイリンク機能を設定して，最大ポート数を 3 に設定します。チャネルグループ 10 はリンクダウンモードで動作します。
3. **(config-if)# exit**
   グローバルコンフィグレーションモードに戻ります。
4. **(config)# interface port-channel 20**
   (config-if)# channel-group max-active-port 1 no-link-down
   (config-if)# exit
   チャネルグループ 20 のポートチャネルインタフェースコンフィグレーションモードに移行して，スタンバイリンク機能を設定します。最大ポート数を 1 とし，非リンクダウンモードを設定します。
5. **(config)# interface gigabitethernet 1/0/1**

```
(config-if)# channel-group 20 mode on
(config-if)# lacp port-priority 300
```

チャネルグループ 20 にポート 1/0/1 を登録して, ポート優先度を 300 に設定します。ポート優先度は値が小さいほど優先度が高く, ポート優先度のデフォルト値の 128 よりもスタンバイリンクに選択されやすくなります。

21.4.3 離脱ポート制限機能のコンフィグレーション

[設定のポイント]

チャネルグループに離脱ポート制限機能を設定します。本コマンドではチャネルグループから離脱することを許容する最大ポート数に 0 と 7 のどちらかを指定します。7 を指定した場合は離脱ポート制限機能を設定しない場合と同じです。

離脱ポート制限機能をサポートしている装置と接続する場合，接続先の装置と本設定を合わせてください。離脱ポート制限機能をサポートしていない装置と接続する場合, 本装置の LACP システム優先度を高くしてください。LACP システム優先度は値が小さいほど優先度が高くなります。

離脱ポート制限機能は，LACP リンクアグリゲーションだけで使用できます。

[コマンドによる設定]

1. **(config)# interface port-channel 10**
   チャネルグループ 10 のポートチャネルインタフェースコンフィグレーションモードに移行します。
2. **(config-if)# channel-group max-detach-port 0**
   チャネルグループ 10 に離脱ポート制限機能を設定します。離脱を許容する最大ポート数を 0 とし，障害などによって 1 ポートでも離脱した場合にチャネルグループ全体を障害とみなします。
3. **(config-if)# channel-group lacp system-priority 100**
   チャネルグループ 10 のシステム優先度を 100 に設定します。

21.4.4 異速度混在モードのコンフィグレーション

[設定のポイント]

チャネルグループに異速度混在モードを設定します。本機能を設定すると，ポートの速度は離脱条件ではなくなります。

[コマンドによる設定]

1. **(config)# interface port-channel 10**
   チャネルグループ 10 のポートチャネルインタフェースコンフィグレーションモードに移行します。
2. **(config-if)# channel-group multi-speed**
   チャネルグループ 10 に異速度混在モードを設定します。

21.5　リンクアグリゲーションのオペレーション

21.5.1　運用コマンド一覧

リンクアグリゲーションの運用コマンド一覧を次の表に示します。

表 21-6　運用コマンド一覧

コマンド名	説明
show channel-group	リンクアグリゲーションの情報を表示します。
show channel-group statistics	リンクアグリゲーションの統計情報を表示します。
clear channel-group statistics lacp	LACPDU の送受信統計情報をクリアします。
restart link-aggregation	リンクアグリゲーションプログラムを再起動します。
dump protocols link-aggregation	リンクアグリゲーションの詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

21.5.2　リンクアグリゲーションの状態の確認

(1)　リンクアグリゲーションの接続状態の確認

リンクアグリゲーションの情報を show channel-group コマンドで表示します。CH Status でチャネルグループの接続状態を確認できます。また，設定が正しいことを各項目で確認してください。

show channel-group コマンドの実行結果を次の図に示します。

図 21-4　show channel-group コマンドの実行結果

```
> show channel-group 1
Date 20XX/12/10 13:13:38 UTC
channel-group Counts:1
ChGr:1    Mode:LACP
  CH Status    :Up        Elapsed Time:10:10:39
  Multi Speed  :Off       Load Balance:src-dst-port
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e2ac.8301     VLAN ID:10
  Periodic Timer:Short
  Actor   information: System Priority:1     MAC: 0012.e212.ff02
                       KEY:1
  Partner information: System Priority:10000 MAC: 0012.e2f0.69be
                       KEY:10
  Port(4)         :1/0/5-8
  Up Port(2)      :1/0/5-6
  Down Port(2)    :1/0/7-8
>
```

(2)　各ポートの運用状態の確認

show channel-group detail コマンドで各ポートの詳細な状態を表示します。ポートの通信状態を Status で確認してください。Status が Down 状態のときは Reason で理由を確認できます。

show channel-group detail コマンドの実行結果を次の図に示します。

図 21-5 show channel-group detail コマンドの実行結果

```
> show channel-group detail
Date 20XX/12/10 13:13:38 UTC
channel-group Counts:1
ChGr:1    Mode:LACP
  CH Status    :Up        Elapsed Time:00:13:51
  Multi Speed  :Off       Load Balance:src-dst-port
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e205.0545     VLAN ID:10
  Periodic Timer:Long
  Actor   information: System Priority:128   MAC: 0012.e205.0540
                       KEY:1
  Partner information: System Priority:128   MAC: 0012.e2c4.2b5b
                       KEY:1
  Port Counts:4        Up Port Counts:2
  Port:1/0/5   Status:Up    Reason:-
               Speed :100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:128
  Port:1/0/6   Status:Up    Reason:-
               Speed :100M  Duplex:Full  LACP Activity:Active
               Actor   Priority:128     Partner Priority:128
  Port:1/0/7   Status:Down  Reason:Duplex Half
               Speed :100M  Duplex:Half  LACP Activity:Active
               Actor   Priority:128     Partner Priority:0
  Port:1/0/8   Status:Down  Reason:Port Down
               Speed :-     Duplex:-     LACP Activity:Active
               Actor   Priority:128     Partner Priority:0
>
```

22 レイヤ２スイッチ概説

この章では，本装置の機能のうち，OSI 階層モデルの第 2 レイヤでデータを中継するレイヤ 2 スイッチ機能の概要について説明します。

22.1　概要

22.1.1　MAC アドレス学習

レイヤ 2 スイッチはフレームを受信すると送信元 MAC アドレスを MAC アドレステーブルに登録します。MAC アドレステーブルの各エントリには，MAC アドレスとフレームを受信したポートおよびエージングタイマを記録します。フレームを受信するごとに送信元 MAC アドレスに対応するエントリを更新します。

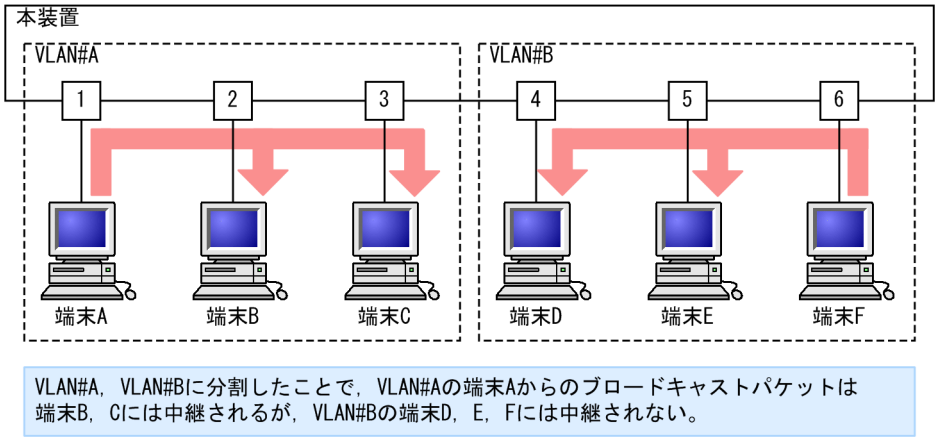
レイヤ 2 スイッチは，MAC アドレステーブルのエントリに従ってフレームを中継します。フレームの宛先 MAC アドレスに一致するエントリがあると，そのエントリのポートに中継します（エントリのポートが受信したポートである場合は中継しません）。一致するエントリがない場合，受信したポート以外のすべてのポートにフレームを中継します。この中継をフラッディングと呼びます。

22.1.2　VLAN

VLAN は，スイッチ内を仮想的なグループに分ける機能のことです。スイッチ内を複数の VLAN にグループ分けすることによってブロードキャストドメインを分割します。これによって，ブロードキャストフレームの抑制や，セキュリティの強化を図ることができます。

VLAN の概要を次の図に示します。VLAN#A と VLAN#B の間ではブロードキャストドメインが分割されるため，フレームが届くことはありません。

図 22-1　VLAN の概要



22.2　サポート機能

レイヤ 2 スイッチ機能として，本装置がサポートする機能を次の表に示します。

これらの機能は，組み合わせて利用できる機能とできない機能があります。機能の組み合わせ制限については，次項で説明します。

表 22-1　レイヤ 2 スイッチサポート機能

サポート機能		機能概要
MAC アドレス学習		MAC アドレステーブルに登録する MAC アドレスの学習機能
VLAN	ポート VLAN	ポート単位にスイッチ内を仮想的なグループに分ける機能
	プロトコル VLAN	プロトコル単位にスイッチ内を仮想的なグループに分ける機能
	MAC VLAN	送信元の MAC アドレス単位にスイッチ内を仮想的なグループに分ける機能
	デフォルト VLAN	コンフィグレーションが未設定のときにデフォルトで所属する VLAN
	ネイティブ VLAN	トランクポート，プロトコルポート，MAC ポートでの Untagged フレームを扱うポート VLAN の呼称
	トンネリング	複数ユーザの VLAN をほかの VLAN に集約して「トンネル」する機能
	Tag 変換	VLAN Tag を変換して別の VLAN に中継する機能
	L2 プロトコルフレーム透過機能	レイヤ 2 のプロトコルのフレームを中継する機能 スパニングツリー（BPDU），IEEE802.1X（EAP），LLDP（LLDPDU），IEEE802.3ah/UDLD（OAMPDU）を透過します。
	VLAN ごと MAC アドレス	レイヤ 3 インタフェースの MAC アドレスを VLAN ごとに異なるアドレスにする機能
VXLAN【SL-L3A】		レイヤ 2 イーサネットフレームをカプセル化して，レイヤ 3 ネットワーク上で仮想的なレイヤ 2 ネットワークを実現する機能
スパニングツリー	PVST+	VLAN 単位のスイッチ間のループ防止機能
	シングルスパニングツリー	装置単位のスイッチ間のループ防止機能
	マルチプルスパニングツリー	MST インスタンス単位のスイッチ間のループ防止機能
Ring Protocol		リングトポロジーでのレイヤ 2 ネットワークの冗長化機能
IGMP snooping/MLD snooping		レイヤ 2 スイッチで VLAN 内のマルチキャストトラフィック制御機能
ポート間中継遮断機能		指定したポート間ですべての通信を遮断する機能

22.3　レイヤ 2 スイッチ機能と他機能の共存について

レイヤ 2 スイッチ機能と併用する際，共存不可または制限事項がある機能があります。機能間の共存についての制限事項を次の表に示します。

なお，これらの表では各機能間の共存関係で，制限のある項目だけを示しています。

表 22–2　MAC アドレス学習での制限事項

使用したい機能	制限のある機能	制限の内容
MAC アドレス学習	アップリンク・リダンダント	一部制限あり※

注※

スタティックエントリの設定は，アップリンクポートで使用できません。

表 22–3　VLAN での制限事項

使用したい機能		制限のある機能	制限の内容
VLAN 種別	ポート VLAN	VLAN トンネリング	一部制限あり※1
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング（ミラーポート）	一部制限あり※3
		ポリシーベースミラーリング（ミラーポート）	共存不可
	プロトコル VLAN	デフォルト VLAN	共存不可
		VLAN トンネリング	
		PVST+	
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング（ミラーポート）	共存不可
		ポリシーベースミラーリング（ミラーポート）	
		PTP	
	MAC VLAN	デフォルト VLAN	共存不可
		VLAN トンネリング	
		VXLAN【SL-L3A】	
		PVST+	
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング（ミラーポート）	共存不可
		ポリシーベースミラーリング（ミラーポート）	
		PTP	

使用したい機能		制限のある機能	制限の内容
デフォルト VLAN		プロトコル VLAN	共存不可
		MAC VLAN	
		IGMP snooping	
		MLD snooping	
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング（ミラーポート）	一部制限あり※3
		ポリシーベースミラーリング（ミラーポート）	共存不可
VLAN 拡張機能	Tag 変換	VXLAN【SL-L3A】	共存不可
		PVST+	
		IGMP snooping	
		MLD snooping	
		アップリンク・リダンダント	一部制限あり※4
		PTP	共存不可
	VLAN トンネリング	ポート VLAN	一部制限あり※1
		プロトコル VLAN	共存不可
		MAC VLAN	
		VXLAN【SL-L3A】	
		PVST+	
		シングルスパニングツリー	
		マルチプルスパニングツリー	
		IGMP snooping	
		MLD snooping	
		レイヤ 2 認証	一部制限あり※2
		DHCP snooping	共存不可
		アップリンク・リダンダント	一部制限あり※4
		PTP	共存不可
	L2 プロトコルフレーム透過機能（BPDU）	PVST+	共存不可
		シングルスパニングツリー	
		MSTP	
	L2 プロトコルフレーム透過機能（EAP）	レイヤ 2 認証	一部制限あり※2

使用したい機能		制限のある機能	制限の内容
	L2 プロトコルフレーム透過機能（LLDP）	LLDP	共存不可
	L2 プロトコルフレーム透過機能（UDLD）	IEEE802.3ah/UDLD	共存不可
	ポート間中継遮断機能	DHCP snooping	一部制限あり※5

注※1

VLAN トンネリング機能を使用する場合は，トランクポートでネイティブ VLAN を使用しないでください。

注※2

「コンフィグレーションガイド Vol.2」「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

注※3

802.1Q Tag 付与機能を使用している場合だけ，使用できます。

注※4

アップリンクポートでは使用できません。

注※5

DHCP snooping を有効にした場合，ポート間中継遮断機能を設定しても本装置が受信したすべての DHCP パケットは遮断の対象になりません。また，ダイナミック ARP 検査も有効にした場合，本装置が受信したすべての ARP パケットも遮断の対象になりません。

表 22-4　VXLAN での制限事項

使用したい機能	制限のある機能	制限の内容
VXLAN【SL-L3A】	MAC VLAN	共存不可
	Tag 変換	
	VLAN トンネリング	
	IGMP snooping	
	MLD snooping	
	PTP	
	ポリシーベースルーティング	
	IPv4 マルチキャスト	
	IPv6 マルチキャスト	

表 22-5　VXLAN Access ポートおよび VXLAN Network ポートでの他機能の動作可否

機能		VXLAN Access ポート※1	VXLAN Network ポート
SNMP		×	○
リンクアグリゲーション		○	○
プロトコル VLAN		×	○
VLAN 拡張機能	L2 プロトコルフレーム透過	○	×

機能		VXLAN Access ポート※1	VXLAN Network ポート
	ポート間中継遮断	△※2	△※2
	VLAN debounce	×	×
	レイヤ 2 中継遮断	×	×
スパニングツリー		×	×
Ring Protocol		×	○
フィルタ	inbound	○※3	×
	outbound	○※3	○※4
QoS（フロー制御） • ユーザ優先度マッピング • フロー検出 • 帯域監視 • マーカー • 優先度決定		△※5	×
QoS（送信側機能） • シェーパ • 廃棄制御		○	○
レイヤ 2 認証 （IEEE802.1X，Web 認証，MAC 認証）		×	×
DHCP snooping		×	×
冗長化構成による高信頼化機能 （GSRP，VRRP，アップリンク・リダンダント）		×	×
L2 ループ検知		×	×
ストームコントロール		○	○
ポートミラーリング	inbound	○	○
	outbound	△※6	△※7
ポリシーベースミラーリング	inbound	○※3	×
sFlow		×	×
IEEE802.3ah/UDLD		×	×
CFM		×	×
LLDP		○※8	○
OADP		×	×
IPv4・ARP・ICMP		×	○
DHCP/BOOTP リレーエージェント		×	×

機能	VXLAN Access ポート※1	VXLAN Network ポート
DHCP サーバ	×	×
IPv4 ユニキャストルーティング（スタティック，RIP，OSPF，BGP4）	×	○
IPv6・NDP・ICMPv6	×	○
RA	×	×
IPv6 DHCP リレー	×	×
IPv6 DHCP サーバ	×	×
IPv6 ユニキャストルーティング（スタティック，RIPng，OSPFv3，BGP4+）	×	○
VRF	○	○

（凡例）○：サポート　△：制限あり　×：未サポート

注

VXLAN Access ポートでの動作可否は，VNI をマッピングした VLAN またはサブインタフェース上での動作可否を示します。VXLAN Network ポートでの動作可否は，VXLAN フレームを送受信する VLAN 上での動作可否を示します。

注※1

VXLAN Access ポートでサブインタフェース指定をした場合は，基本的にレイヤ 2 機能は動作できません。VNI に VLAN を適用した場合，該当 VLAN でレイヤ 2 機能は動作できません。

注※2

スタック構成時，VXLAN Access ポートまたは VXLAN Network ポートから受信したフレームが，フレームを受信したメンバスイッチと異なるメンバスイッチから送信される場合，ポート間中継遮断機能は動作しません。

注※3

カプセル化前のフレーム情報（MAC ヘッダ，IP ヘッダなど）が検出対象となります。

注※4

カプセル化後の VXLAN フレーム情報（MAC ヘッダ，IP ヘッダなど）が検出対象となります。

注※5

IP ヘッダ内の DSCP を書き換えた場合，VXLAN フレームではカプセル化前の IP ヘッダが書き換わります。

VLAN Tag 内のユーザ優先度書き換えを設定した場合，VXLAN Network ポートがトランクポートであるときは，VXLAN フレームのユーザ優先度に反映されます。

注※6

VXLAN フレームをデカプセル化した送信フレームのミラーリングでは，VLAN Tag を削除してミラーポートから出力します。

注※7

ポートミラーリングを使用して VXLAN Network ポートの送信フレーム情報を確認しても，VXLAN でカプセル化されたフレームのヘッダ情報を正しく取得できません。VXLAN Network ポートの送信内容を確認する場合は，対向装置側で確認してください。

注※8

サブインタフェースマッピングの VXLAN Access ポートでは，IEEE802.1 Organizationally Specific TLVs を送信しません。

表 22-6　スパニングツリーでの制限事項

使用したい機能	制限のある機能	制限の内容
PVST+	プロトコル VLAN	共存不可
	MAC VLAN	
	VLAN トンネリング	
	Tag 変換	
	L2 プロトコルフレーム透過機能(BPDU)	
	マルチプルスパニングツリー	
	GSRP	
	レイヤ 2 認証	一部制限あり※
	アップリンク・リダンダント	共存不可
	PTP	
シングルスパニングツリー	VLAN トンネリング	共存不可
	L2 プロトコルフレーム透過機能(BPDU)	
	マルチプルスパニングツリー	
	GSRP	
	レイヤ 2 認証	一部制限あり※
	アップリンク・リダンダント	共存不可
	PTP	
マルチプルスパニングツリー	VLAN トンネリング	共存不可
	L2 プロトコルフレーム透過機能(BPDU)	
	シングルスパニングツリー	
	PVST+	
	ループガード	
	GSRP	
	レイヤ 2 認証	一部制限あり※
	アップリンク・リダンダント	共存不可
	PTP	

注※

「コンフィグレーションガイド Vol.2」「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

表 22–7　Ring Protocol での制限事項

使用したい機能	制限のある機能	制限の内容
Ring Protocol	レイヤ 2 認証	一部制限あり※1
	アップリンク・リダンダント	一部制限あり※2
	PTP	共存不可

注※1

「コンフィグレーションガイド Vol.2」「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

注※2

リングポートでは使用できません。

表 22–8　IGMP/MLD snooping での制限事項

使用したい機能	制限のある機能	制限の内容
IGMP snooping	デフォルト VLAN	共存不可
	Tag 変換	
	VLAN トンネリング	
	VXLAN【SL-L3A】	
	レイヤ 2 認証	一部制限あり※
MLD snooping	デフォルト VLAN	共存不可
	Tag 変換	
	VLAN トンネリング	
	VXLAN【SL-L3A】	

注※

「コンフィグレーションガイド Vol.2」「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

23 MAC アドレス学習

この章では，MAC アドレス学習機能の解説と操作方法について説明します。

23.1　MAC アドレス学習の解説

本装置は，フレームを宛先 MAC アドレスによって目的のポートへ中継するレイヤ 2 スイッチングを行います。宛先 MAC アドレスによって特定のポートだけに中継することで，ユニキャストフレームのフラッディングによるむだなトラフィックを抑止します。

MAC アドレス学習では，チャネルグループを一つのポートとして扱います。

23.1.1　送信元 MAC アドレス学習

すべての受信フレームを MAC アドレス学習の対象とし，送信元 MAC アドレスを学習して MAC アドレステーブルに登録します。登録した MAC アドレスはエージングタイムアウトまで保持します。学習する単位は，VLAN 単位と VNI 単位となります。

VLAN 単位での MAC アドレス学習

MAC アドレス学習は VLAN 単位に行い，MAC アドレステーブルは MAC アドレスと VLAN のペアによって管理します。

VNI 単位での MAC アドレス学習【SL-L3A】

MAC アドレス学習は VNI 単位に行い，MAC アドレステーブルは MAC アドレスと VNI のペアによって管理します。

異なる VLAN，または異なる VNI であれば，同一の MAC アドレスを学習することもできます。

23.1.2　MAC アドレス学習の移動検出

MAC アドレス学習の移動を監視し，MAC アドレスが移動した回数をカウントします。なお，MAC アドレス学習の移動回数は，移動先のポートでカウントされます。移動の検出条件は，MAC アドレスを学習した条件によって異なります。

(1)　VLAN で MAC アドレスを学習した場合

学習済みの送信元 MAC アドレスと VLAN の組み合わせを持つフレームを学習時と異なるポートから受信した場合，その MAC アドレスが移動したものと見なして MAC アドレステーブルのエントリを再登録（移動先ポートに関する上書き）します。

(2)　VNI で MAC アドレスを学習した場合【SL-L3A】

(a)　VXLAN Access ポート

VNI マッピング方式が VLAN マッピングの場合

学習済みの送信元 MAC アドレスと VNI の組み合わせを持つフレームを学習時と異なる VXLAN Access ポートまたは VXLAN Network ポートから受信した場合, その MAC アドレスが移動したものと見なして MAC アドレステーブルのエントリを再登録（移動先ポートに関する上書き）します。

VNI マッピング方式がサブインタフェースマッピングの場合

学習済みの送信元 MAC アドレスと VNI の組み合わせを持つフレームを学習時と異なる VXLAN Access ポートと VLAN の組み合わせまたは VXLAN Network ポートから受信した場合，その MAC アドレスが移動したものと見なして MAC アドレステーブルのエントリを再登録（移動先ポートに関する上書き）します。

(b)　VXLAN Network ポート

学習済みの送信元 MAC アドレスと VNI の組み合わせを持つフレームを学習時と異なる VXLAN トンネルまたは VXLAN Access ポートから受信した場合，その MAC アドレスが移動したものと見なして MAC アドレステーブルのエントリを再登録（移動先ポートに関する上書き）します。

(3)　チャネルグループで学習した場合

チャネルグループで学習した MAC アドレスについては，そのチャネルグループに含まれないポートからフレームを受信した場合に MAC アドレスが移動したものと見なします。

23.1.3　学習 MAC アドレスのエージング

学習したエントリは，エージングタイム内に同じ送信元 MAC アドレスからフレームを受信しなかった場合はエントリを削除します。これによって，不要なエントリの蓄積を防止します。エージングタイム内にフレームを受信した場合は，エージングタイマを更新しエントリを保持します。エージングタイムを設定できる範囲を次に示します。

- エージングタイムの範囲：0，10～1000000（秒）
  0 は無限を意味し，エージングしません。
- デフォルト値：300（秒）

学習したエントリを削除するまでに最大でエージング時間の 2 倍掛かることがあります。

また，ポートがダウンした場合には該当ポートから学習したエントリをすべて削除します。チャネルグループで学習したエントリは，そのチャネルグループがダウンした場合に削除します。

23.1.4　MAC アドレスによるレイヤ 2 スイッチング

MAC アドレス学習の結果に基づいてレイヤ 2 スイッチングを行います。宛先 MAC アドレスに対応するエントリを保持している場合，学習したポートだけに中継します。

レイヤ 2 スイッチングの動作仕様を次の表に示します。

表 23-1　レイヤ 2 スイッチングの動作仕様

宛先 MAC アドレスの種類	動作概要
学習済みのユニキャスト	学習したポートへ中継します。
未学習のユニキャスト	受信した VLAN に所属する全ポートへ中継します。 VXLAN 機能が有効で，受信した VLAN が VNI に含まれる場合，VXLAN の動作に従って中継します。【SL-L3A】
ブロードキャスト	受信した VLAN に所属する全ポートへ中継します。 VXLAN 機能が有効で，受信した VLAN が VNI に含まれる場合，VXLAN の動作に従って中継します。【SL-L3A】
マルチキャスト	受信した VLAN に所属する全ポートへ中継します。ただし，IGMP snooping，MLD snooping 動作時は snooping 機能の学習結果に従って中継します。 VXLAN 機能が有効で，受信した VLAN が VNI に含まれる場合，VXLAN の動作に従って中継します。【SL-L3A】

23.1.5　スタティックエントリの登録

受信フレームによるダイナミックな学習のほかに, ユーザ指定によってスタティックに MAC アドレスを登録できます。ユニキャスト MAC アドレスに対して一つのポートまたはチャネルグループを指定できます。また，ポートを指定するのではなく「廃棄」を指定することもできます。その場合，指定の宛先 MAC アドレスまたは送信元 MAC アドレスのフレームはどのポートにも中継されないで廃棄されます。

ユニキャスト MAC アドレスに対してスタティックに登録を行うと, そのアドレスについてダイナミックな学習は行いません。すでに学習済みのエントリは MAC アドレステーブルから削除してスタティックエントリを登録します。また, 指定された MAC アドレスが送信元のフレームをポートまたはチャネルグループ以外から受信した場合は, そのフレームを廃棄します。スタティックエントリの指定パラメータを次の表に示します。

表 23–2　スタティックエントリの指定パラメータ

項番	指定パラメータ	説明
1	MAC アドレス	ユニキャスト MAC アドレスが指定できます。
2	VLAN	このエントリを登録する VLAN を指定します。
3	送信先ポート／廃棄指定	一つのポートまたはチャネルグループを指定できます。また，項番 1，2 に該当するフレームを廃棄する指定ができます。

23.1.6　MAC アドレス学習抑止

受信フレームによるダイナミックな MAC アドレス学習に制限を設けて，使用する MAC アドレステーブルのエントリを管理できます。

(1)　VLAN 単位の MAC アドレス学習抑止

VLAN ごとに，ダイナミックな MAC アドレス学習を抑止できます。ダイナミックな MAC アドレス学習を抑止すると，学習抑止の対象となる VLAN で受信したフレームはフラッディングします。

すでに MAC アドレスを学習しているときに MAC アドレス学習を抑止すると, MAC アドレス学習を抑止した VLAN で学習していた MAC アドレステーブルのエントリは削除します。

(2)　VNI 単位の MAC アドレス学習抑止【SL-L3A】

VXLAN 機能が有効な場合, VNI ごとに, ダイナミックな MAC アドレス学習を抑止できます。ダイナミックな MAC アドレス学習を抑止すると，学習抑止の対象となる VNI で受信したフレームはフラッディングします。

すでに MAC アドレスを学習しているときに MAC アドレス学習を抑止すると, MAC アドレス学習を抑止する VNI で学習していた MAC アドレステーブルのエントリは削除します。

23.1.7　MAC アドレステーブルのクリア

本装置は運用コマンドやプロトコルの動作などによって MAC アドレステーブルをクリアします。

(1)　VLAN 単位での MAC アドレス学習エントリ

VLAN 単位で MAC アドレス学習したエントリをクリアする契機を次の表に示します。

表 23-3　MAC アドレステーブルをクリアする契機（VLAN 単位）

契機	説明
ポートダウン※1	該当ポートから学習したエントリを削除します。
チャネルグループダウン※2	該当チャネルグループから学習したエントリを削除します。
運用コマンド clear mac-address-table の実行	パラメータに従って MAC アドレステーブルをクリアします。
MAC アドレステーブル Clear 用 MIB （プライベート MIB）	セット時に MAC アドレステーブルをクリアします。
スパニングツリーのトポロジー変更	[本装置でスパニングツリーを構成] トポロジー変更を検出した時に MAC アドレステーブルをクリアします。
	[スパニングツリーと Ring Protocol を併用しているネットワーク構成で本装置がリングノードとして動作] Ring Protocol と併用している装置がトポロジー変更を検出した時に送信するフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
GSRP のマスタ／バックアップ切り替え	[本装置が GSRP スイッチとして動作] バックアップ状態になった時に MAC アドレステーブルをクリアします。
	[本装置が GSRP aware として動作] GSRP スイッチがマスタ状態になった時に送信される GSRP Flush request フレームを受信した場合，MAC アドレステーブルをクリアします。
	[本装置が GSRP と Ring Protocol を併用して動作] マスタ状態になった時に MAC アドレステーブルをクリアします。
	[GSRP と Ring Protocol を併用しているネットワーク構成で本装置がリングノードとして動作] Ring Protocol と併用している装置がマスタ状態になった時に送信するフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
Ring Protocol による経路の切り替え	[本装置がマスタノードとして動作] 経路切り替え時に MAC アドレステーブルをクリアします。
	[本装置がトランジットノードとして動作] 経路切り替え時にマスタノードから送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。 フラッシュ制御フレーム受信待ち保護時間のタイムアウト時に MAC アドレステーブルをクリアします。
	多重障害監視機能適用時，バックアップリングの切り替え／切り戻しに伴い共有ノードから送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
	経路切り替え時にマスタノードから送信される隣接リング用フラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
VRRP の仮想ルータのマスタ／バックアップ切り替え	VRRP の仮想ルータがマスタ状態になった時に送信される Flush Request フレームを受信した場合，MAC アドレステーブルをクリアします。

契機	説明
アップリンク・リダンダント機能によるプライマリポートとセカンダリポートの切り替え	プライマリポートからセカンダリポートへの切り替え時，およびセカンダリポートからプライマリポートへの切り戻し時に送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
MAC アドレス学習抑止のコンフィグレーションの設定（VLAN 単位）	コンフィグレーションコマンド no mac-address-table learning で MAC アドレス学習抑止を設定した場合，該当 VLAN で学習したエントリを削除します。

注※1

回線障害，運用コマンド inactivate の実行，コンフィグレーションコマンド shutdown の設定などによるポートダウン。

注※2

LACP，回線障害，コンフィグレーションコマンド shutdown の設定などによるチャネルグループダウン。

(2)　VNI 単位での MAC アドレス学習エントリ【SL-L3A】

VNI 単位で MAC アドレス学習したエントリをクリアする契機を次の表に示します。

表 23-4　MAC アドレステーブルをクリアする契機（VNI 単位）

契機	説明
ポートダウン※1	[VXLAN Access ポート] 該当ポートから学習したエントリを削除します。
	[VXLAN Network ポート] 該当ポートから学習したエントリを削除しません。
チャネルグループダウン※2	[VXLAN Access ポート] 該当チャネルグループから学習したエントリを削除します。
	[VXLAN Network ポート] 該当チャネルグループから学習したエントリを削除しません。
運用コマンド clear mac-address-table の実行	パラメータに従って，VNI 単位で学習した MAC アドレステーブルも含めてクリアします。
運用コマンド clear vxlan mac-address-table の実行	パラメータに従って，VNI 単位で学習した MAC アドレステーブルをクリアします。
VXLAN トンネルの宛先 IP アドレスを削除	該当 VNI で学習したエントリを削除します。
スパニングツリーのトポロジー変更	[本装置でスパニングツリーを構成] トポロジー変更を検出した時に MAC アドレステーブルをクリアします。
GSRP のマスタ／バックアップ切り替え	[本装置が GSRP スイッチとして動作] バックアップ状態になった時に MAC アドレステーブルをクリアします。
	[本装置が GSRP aware として動作] GSRP スイッチがマスタ状態になった時に送信される GSRP Flush request フレームを受信した場合，MAC アドレステーブルをクリアします。
	[本装置が GSRP と Ring Protocol を併用して動作] マスタ状態になった時に MAC アドレステーブルをクリアします。

契機	説明
	[GSRP と Ring Protocol を併用しているネットワーク構成で本装置がリングノードとして動作] Ring Protocol と併用している装置がマスタ状態になった時に送信するフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
VRRP の仮想ルータのマスタ／バックアップ切り替え	VRRP の仮想ルータがマスタ状態になった時に送信される Flush Request フレームを受信した場合，MAC アドレステーブルをクリアします。
アップリンク・リダンダント機能によるプライマリポートとセカンダリポートの切り替え	フラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
MAC アドレス学習抑止のコンフィグレーションの設定（VNI 単位）	コンフィグレーションコマンド no mac-address-table learning で MAC アドレス学習抑止を設定した場合，該当 VNI で学習したエントリを削除します。

注※1

回線障害，運用コマンド inactivate の実行，コンフィグレーションコマンド shutdown の設定などによるポートダウン。

注※2

LACP，回線障害，コンフィグレーションコマンド shutdown の設定などによるチャネルグループダウン。

23.1.8　MAC アドレス学習移動監視機能

本装置は，物理ポートごとに 1 秒当たりの MAC アドレス学習の移動回数を監視して，移動回数が設定した回数を超えている状態が，設定した時間を超えて継続した場合に，ループ障害の発生と判断します。

この機能を MAC アドレス学習移動監視機能と呼び，ループ障害が発生したと判断する閾値として，コンフィグレーションコマンド mac-address-move で 1 秒当たりの MAC アドレス学習の移動回数と継続時間を設定して使用します。また，ループ障害が発生したと判断したときの動作として，次に示す動作のどちらかを選択できます。

(1)　ポートを inactive 状態にして運用メッセージを出力する

ポートを inactive 状態にして，運用メッセージを出力します。

inactive 状態にしたポートは，ループ障害の原因を解決したあとに，運用コマンド activate で active 状態にしてください。なお，自動復旧も設定でき，設定した時間が経過すると自動で active 状態に変更します。

チャネルグループを構成するポートを inactive 状態にする場合は，チャネルグループを構成する全ポートを inactive 状態にします。さらに，自動復旧が指定されていると，全ポートを active 状態にします。なお，運用メッセージは全ポート分出力されます。

(2)　ポートの状態は変更しないで運用メッセージを出力する

ポートの状態は変更しないで，運用メッセージを出力します。

ループ障害が発生したと判断したあと，移動回数が設定した回数を 30 秒間連続して下回った場合に，回復を通知する運用メッセージを出力します。なお，ループ障害を検出したポートがダウンした場合，運用メッセージは出力されません。

チャネルグループを構成するポートでループ障害が発生したと判断した場合，該当ポートに対する運用メッセージが出力されます。

23.1.9　注意事項

(1)　他機能との共存

(a)　レイヤ 2 スイッチ機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(b)　レイヤ 2 認証との共存

「コンフィグレーションガイド Vol.2」「5.2.1　レイヤ 2 認証と他機能との共存」を参照してください。

(2)　MAC アドレス学習と ARP，NDP について

本装置では，レイヤ 3 中継で ARP や NDP によってアドレス解決した NextHop の MAC アドレスは MAC アドレステーブルに登録されている必要があります。そのため，次の点に注意してください。

- MAC アドレス学習の情報をコマンドやエージングなどによってクリアすると，MAC アドレスに対応する ARP や NDP の情報がいったんクリアされます。クリアされた ARP や NDP のエントリは，通信の必要に応じて再解決を行います。
- MAC アドレス学習のエージングタイムが ARP や NDP のエージングタイムより短い場合，MAC アドレス学習のエージングによって対応する ARP や NDP のエントリをクリアします。このクリアは，MAC アドレス学習のエージングタイムを ARP や NDP のエージングタイム以上の時間にすることで回避できます。

(3)　MAC アドレス学習の移動検出について

- IP アドレスが設定された VLAN で受信したフレームの送信元 MAC アドレスが自装置と同じ MAC アドレスだった場合，MAC アドレスが移動したものと見なし，移動回数をカウントアップします。
- スタティックに MAC アドレスを登録している場合，指定しているポート以外から指定している MAC アドレスを学習すると，MAC アドレスが移動したものと見なし，移動回数をカウントアップします。

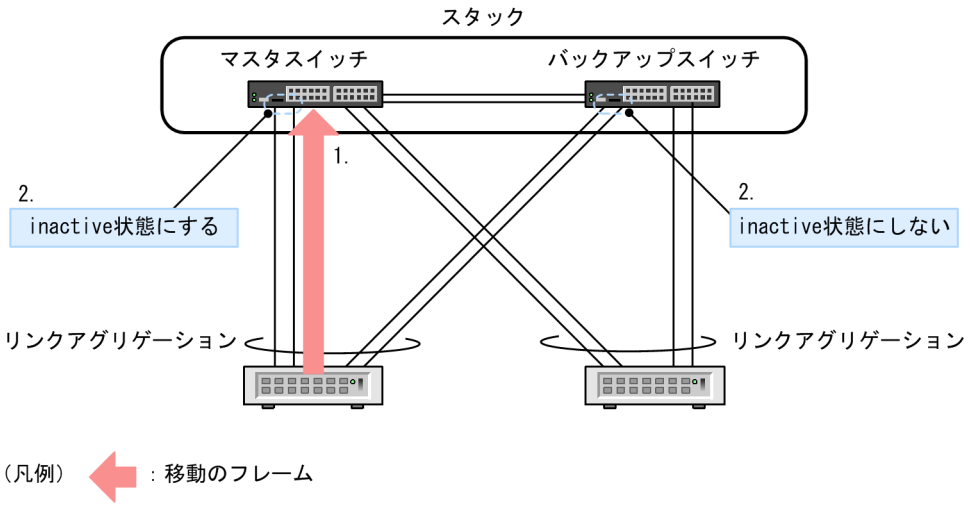
(4)　MAC アドレス学習の抑止について

MAC アドレス学習抑止を設定した VLAN は，レイヤ 3 のインタフェースとして使用できません。

(5)　MAC アドレス学習移動監視機能について

- CPU へのキューに多数の受信パケットが積まれている場合は，MAC アドレス学習の移動を検知できないことがあります。
- 3 か所以上で同時に MAC アドレス学習の移動が発生した場合は，MAC アドレス学習の移動を検知できないことがあります。
- チャネルグループを構成するポートで自動復旧が指定されていると，本機能以外で inactive 状態にしたポートも含めて，チャネルグループを構成するすべてのポートを active 状態にします。
- 異なるメンバスイッチのポートでチャネルグループを構成し，MAC アドレス学習の移動回数が閾値を超えたポートを inactive 状態にする設定では，一方のメンバスイッチ側のチャネルグループを構成するポートをすべて inactive 状態にします。自動復旧が指定されている場合も，同じメンバスイッチ側のチャネルグループを構成するポートをすべて active 状態にします。この構成で inactive 状態にするポートを次の図に示します。

図 23-1　複数のメンバスイッチと接続するリンクアグリゲーション構成での MAC アドレス学習移動監視機能によるポート状態変更例



1. 本装置のマスタスイッチ側のチャネルグループを構成するポートで, MAC アドレス学習の移動回数の閾値超えが発生します。
2. 該当ポートを含むチャネルグループのマスタスイッチ側のポートを, すべて inactive 状態にします。バックアップスイッチ側のポートは，inactive 状態にしません。

- ポートを inactive 状態にしてから自動復旧までの間にポートの状態が回線テスト状態に遷移し, 回線テスト状態のときに自動復旧する時間になった場合, 回線テスト状態が終了してもポートは inactive 状態のままとなります。なお，自動復旧までの間に回線テスト状態が終了すると，自動復旧してポートは active 状態になります。

23.2　MAC アドレス学習のコンフィグレーション

23.2.1　コンフィグレーションコマンド一覧

MAC アドレス学習のコンフィグレーションコマンド一覧を次の表に示します。

表 23-5　コンフィグレーションコマンド一覧

コマンド名	説明
mac-address-move	MAC アドレス学習の移動監視を設定します。
mac-address-table aging-time	MAC アドレス学習のエージングタイムを設定します。
mac-address-table learning	ダイナミックな MAC アドレス学習の可否を設定します。
mac-address-table static	スタティックエントリを設定します。

23.2.2　エージングタイムの設定

[設定のポイント]

MAC アドレス学習のエージングタイムを変更できます。設定は装置単位です。設定しない場合，エージングタイムは 300 秒で動作します。

[コマンドによる設定]

1. **(config)# mac-address-table aging-time 600**
   エージングタイムを 600 秒に設定します。

23.2.3　スタティックエントリの設定

スタティックエントリを登録すると，指定した MAC アドレスについて MAC アドレス学習をしないで，常に登録したエントリに従ってフレームを中継するため，MAC アドレスのエージングによるフラッディングを回避できます。本装置に直接接続したサーバなどのように，ポートの移動がなく，かつトラフィック量の多い端末などに有効な機能です。

スタティックエントリには，MAC アドレス，VLAN および出力先を指定します。出力先はポート，チャネルグループ，廃棄のどれかを指定します。

(1)　出力先にポートを指定するスタティックエントリ

[設定のポイント]

出力先にポートを指定した例を示します。

[コマンドによる設定]

1. **(config)# mac-address-table static 0012.e200.1122 vlan 10 interface gigabitethernet 1/0/1**
   VLAN 10 で，宛先 MAC アドレス 0012.e200.1122 のフレームの出力先をポート 1/0/1 に設定します。

[注意事項]

VLAN 10 で，送信元 MAC アドレス 0012.e200.1122 のフレームをポート 1/0/1 以外から受信した場合は廃棄します。

(2)　出力先にリンクアグリゲーションを指定するスタティックエントリ

[設定のポイント]

出力先にリンクアグリゲーションを指定した例を示します。

[コマンドによる設定]

1. **(config)# mac-address-table static 0012.e200.1122 vlan 10 interface port-channel 5**

   VLAN 10 で, 宛先 MAC アドレス 0012.e200.1122 のフレームの出力先をチャネルグループ 5 に設定します。

[注意事項]

VLAN 10 で, 送信元 MAC アドレス 0012.e200.1122 のフレームをチャネルグループ 5 以外から受信した場合は廃棄します。

(3)　廃棄を指定するスタティックエントリ

[設定のポイント]

指定した MAC アドレス宛および指定した MAC アドレスからのフレームを廃棄に設定します。

[コマンドによる設定]

1. **(config)# mac-address-table static 0012.e200.1122 vlan 10 drop**

   VLAN 10 で，宛先および送信元 MAC アドレス 0012.e200.1122 のフレームを廃棄に設定します。

23.2.4　MAC アドレス学習抑止の設定

[設定のポイント]

MAC アドレス学習をする場合はコンフィグレーションの設定は不要です。例えば, 特定の VLAN に対しての MAC アドレス学習を抑止したい場合に，MAC アドレス学習をしない VLAN に対してだけ MAC アドレス学習抑止を設定します。

[コマンドによる設定]

1. **(config)# no mac-address-table learning vlan 100**

   VLAN100 では MAC アドレス学習を抑止します。

23.2.5　MAC アドレス学習移動監視機能の設定

[設定のポイント]

ループ障害が発生したことを MAC アドレス学習の移動によって検知したい場合に設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# mac-address-move detect-count 10 duration 3 action inactivate auto-recover 300

```
(config-if)# exit
```

ポート 1/0/1 で 1 秒間に 11 回以上の MAC アドレスの移動があり，その状態を 3 秒継続すると，該当ポートを inactive 状態に変更します。また，inactive 状態に変更してから 300 秒後に，該当ポートを active 状態に変更します。

23.3　MAC アドレス学習のオペレーション

23.3.1　運用コマンド一覧

MAC アドレス学習の運用コマンド一覧を次の表に示します。

表 23-6　運用コマンド一覧

コマンド名	説明
show mac-address-table	MAC アドレステーブルの情報を表示します。 learning-counter パラメータを指定すると，ポート単位に MAC アドレス学習の学習アドレス数と MAC アドレス学習の移動回数を表示します。
clear mac-address-table	MAC アドレステーブルをクリアします。
show interfaces※1	MAC アドレス学習の移動回数を表示します。
clear counters※1	MAC アドレス学習の移動回数をクリアします。
show vlan※2	VLAN の MAC アドレス学習状態を表示します。
show vxlan vni※3 【SL-L3A】	VNI の MAC アドレス学習状態を表示します。

注※1
「運用コマンドレファレンス Vol.1」「21　イーサネット」を参照してください。

注※2
「運用コマンドレファレンス Vol.1」「24　VLAN」を参照してください。

注※3
「運用コマンドレファレンス Vol.1」「25　VXLAN」を参照してください。

23.3.2　MAC アドレス学習の状態の確認

MAC アドレス学習の情報は show mac-address-table コマンドで表示します。MAC アドレステーブルに登録されている MAC アドレスとその MAC アドレスを宛先とするフレームの中継先を確認してください。このコマンドで表示されない MAC アドレスを宛先とするフレームは VLAN 全体にフラッディングされます。

show mac-address-table コマンドでは，MAC アドレス学習によって登録したエントリ，スタティックエントリ，IEEE802.1X，IGMP snooping および MLD snooping によって登録したエントリを表示します。

図 23-2　show mac-address-table コマンドの実行結果

```
> show mac-address-table
Date 20XX/10/14 12:08:41 UTC
MAC address         VLAN    Type      Port-list
0012.e22d.eefa         1    Dynamic   1/0/2
0012.e212.2e5f         1    Dynamic   1/0/5
0012.e205.0641      4094    Dynamic   1/0/24
0012.e28e.0602      4094    Dynamic   1/0/24
>
```

23.3.3 MAC アドレス学習数の確認

show mac-address-table コマンド（learning-counter パラメータ）で MAC アドレス学習によって登録したダイナミックエントリの数をポート単位に表示できます。このコマンドで, ポートごとの接続端末数の状態を確認できます。

リンクアグリゲーションを使用している場合，同じチャネルグループのポートはすべて同じ値を表示します。表示する値はチャネルグループ上で学習したアドレス数です。

図 23–3 show mac-address-table コマンド（learning-counter パラメータ指定）の実行結果

```
> show mac-address-table learning-counter port 1/0/1-12
Date 20XX/10/14 12:09:40 UTC
Port counts:12
Port       Count      Movement Detect
1/0/1          3                    0
1/0/2       1000                 1000
1/0/3          0                    0
1/0/4         50                    0
1/0/5         45                    0
1/0/6          0                    0
1/0/7         22                   50
1/0/8          0                    0
1/0/9          0                    0
1/0/10         0                    0
1/0/11         0                    0
1/0/12         0                    0
>
```

show mac-address-table コマンドで learning-counter および vlan パラメータを指定すると，ダイナミックエントリの数を VLAN 単位に表示できます。

図 23–4 show mac-address-table コマンド（learning-counter および vlan パラメータ指定）の実行結果

```
> show mac-address-table learning-counter vlan
Date 20XX/09/24 20:00:57 UTC
VLAN counts:4
ID         Count  Maximum
   1           3        -
 100        1000        -
 200           0        -
4094          90        -
```

24 VLAN

VLAN はスイッチ内を仮想的なグループに分ける機能です。この章では，VLAN の解説と操作方法について説明します。

24.1 VLAN 基本機能の解説

この節では，VLAN の概要を説明します。

24.1.1 VLAN の種類

本装置がサポートする VLAN の種類を次の表に示します。

表 24-1 サポートする VLAN の種類

項目	概要
ポート VLAN	ポート単位に VLAN のグループを分けます。
プロトコル VLAN	プロトコル単位に VLAN のグループを分けます。
MAC VLAN	送信元の MAC アドレス単位に VLAN のグループを分けます。

24.1.2 ポートの種類

(1) 解説

本装置は，ポートの設定によって使用できる VLAN が異なります。使用したい VLAN の種類に応じて各ポートの種類を設定する必要があります。ポートの種類を次の表に示します。

表 24-2 ポートの種類

ポートの種類	概要	使用する VLAN
アクセスポート	ポート VLAN として Untagged フレームを扱います。 このポートでは，すべての Untagged フレームを一つのポート VLAN で扱います。	ポート VLAN MAC VLAN
プロトコルポート	プロトコル VLAN として Untagged フレームを扱います。 このポートでは，フレームのプロトコルによって VLAN を決定します。	プロトコル VLAN ポート VLAN
MAC ポート	MAC VLAN として Untagged フレームを扱います。 このポートでは，フレームの送信元 MAC アドレスによって VLAN を決定します。	MAC VLAN ポート VLAN
トランクポート	すべての種類の VLAN で Tagged フレームを扱います。 このポートでは，VLAN Tag によって VLAN を決定します。	すべての種類の VLAN
トンネリングポート	VLAN トンネリングのポート VLAN として，フレームの Untagged と Tagged を区別しないで扱います。このポートでは，すべてのフレームを一つのポート VLAN で扱います。	ポート VLAN

アクセスポート，プロトコルポート，MAC ポートは Untagged フレームを扱うポートです。これらのポートで Tagged フレームを扱うことはできません。Tagged フレームを受信したときは廃棄し，また送信することもありません。

Tagged フレームはトランクポートでだけ扱うことができます。トランクポートの Untagged フレームはネイティブ VLAN が扱います。

トンネリングポートは，VLAN トンネリングをするポートで，フレームが Untagged か，Tagged かを区別しないで扱います。

ポートの種類ごとの，使用できる VLAN の種類を次の表に示します。プロトコル VLAN と MAC VLAN は同じポートで使用できません。VLAN Tag を扱うトランクポートはすべての VLAN で同じポートを使用できます。

表 24-3　ポート上で使用できる VLAN

ポートの種類	VLAN の種類		
	ポート VLAN	プロトコル VLAN	MAC VLAN
アクセスポート	○	×	○
プロトコルポート	○	○	×
MAC ポート	○	×	○
トランクポート	○	○	○
トンネリングポート	○	×	×

(凡例)　○：使用できる　×：使用できない

(2)　ポートのネイティブ VLAN

アクセスポート，トンネリングポート以外のポート（プロトコルポート，MAC ポート，トランクポート）では, それぞれの設定と一致しないフレームを受信する場合があります。例えば, プロトコルポートで IPv4 プロトコルだけ設定していたときに IPv6 のフレームを受信した場合です。アクセスポート，トンネリングポート以外ではこのようなフレームを扱うためにポート VLAN を一つ設定することができます。この VLAN のことを，各ポートでのネイティブ VLAN と呼びます。

アクセスポート，トンネリングポート以外の各ポートでは，ポートごとに作成済みのポート VLAN をネイティブ VLAN に設定できます。コンフィグレーションで指定がないポートは，VLAN 1（デフォルト VLAN）がネイティブ VLAN になります。

24.1.3　デフォルト VLAN

(1)　概要

本装置では，コンフィグレーションが未設定の状態であっても，装置の起動後すぐにレイヤ 2 中継ができます。このとき，すべてのポートはアクセスポートとなり，デフォルト VLAN と呼ぶ VLAN ID 1 の VLAN に属します。デフォルト VLAN は常に存在し，VLAN ID「1」は変更できません。

(2)　デフォルト VLAN から除外するポート

アクセスポートは，コンフィグレーションが未設定の場合は VLAN 1（デフォルト VLAN）に属します。しかし，コンフィグレーションによってデフォルト VLAN の自動的な所属から除外する場合があります。次に示すポートはデフォルト VLAN に自動的に所属しなくなります。

- アクセスポートで VLAN 1 以外を指定したポート
- VLAN トンネリング機能を設定した場合の全ポート
- ポートミラーリングのミラーポート（802.1Q Tag 付与機能を使用していない場合）
- ポリシーベースミラーリングのミラーポート

アクセスポート以外のポート（プロトコルポート，MAC ポート，トランクポート，トンネリングポート）は自動的に VLAN に所属することはありません。

24.1.4　VLAN の優先順位

(1)　フレーム受信時の VLAN 判定の優先順位

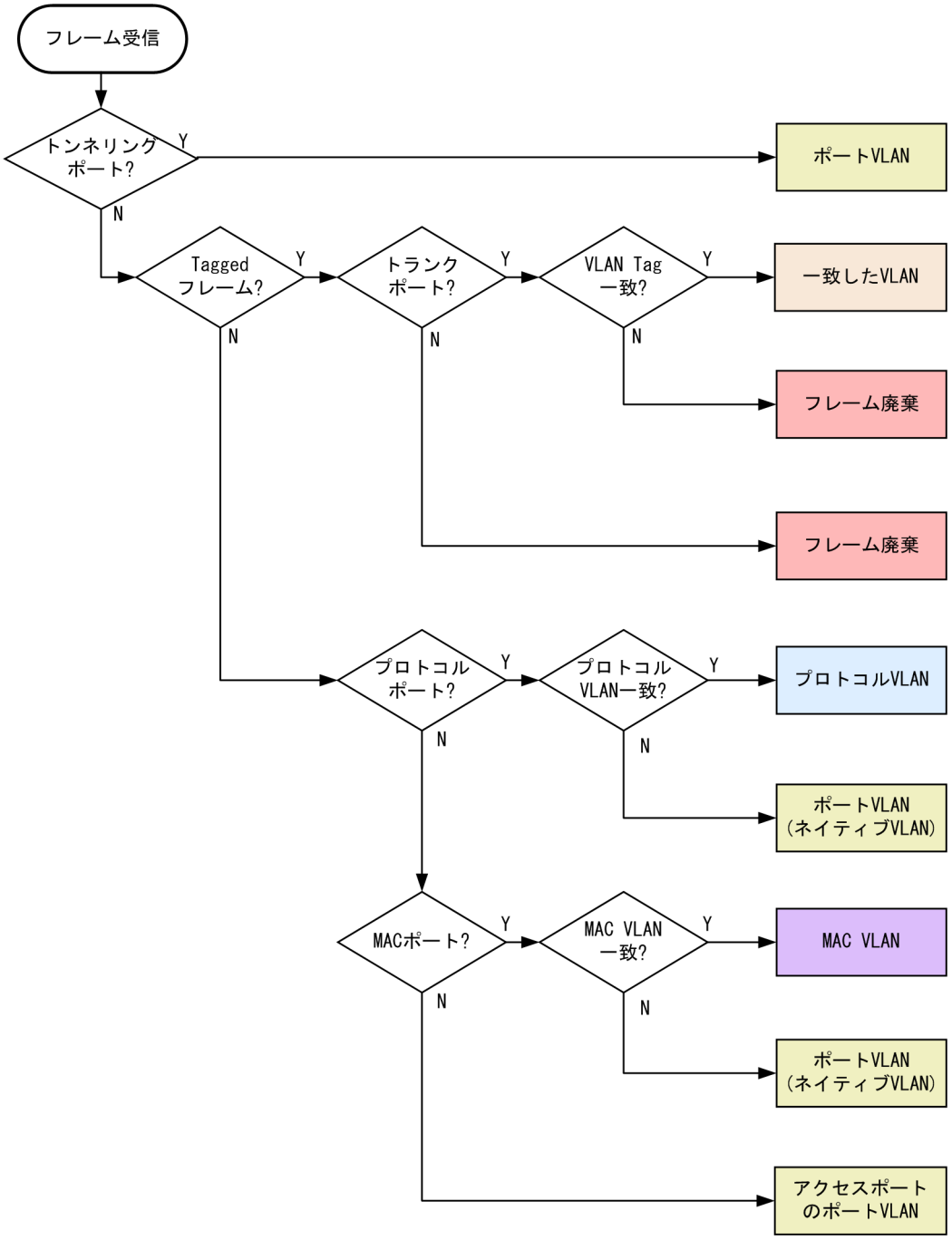
フレームを受信したとき，受信したフレームの VLAN を判定します。VLAN 判定の優先順位を次の表に示します。

表 24-4　VLAN 判定の優先順位

ポートの種類	VLAN 判定の優先順位
アクセスポート	ポート VLAN
プロトコルポート	プロトコル VLAN ＞ポート VLAN（ネイティブ VLAN）
MAC ポート	MAC VLAN ＞ポート VLAN（ネイティブ VLAN）
トランクポート	VLAN Tag ＞ポート VLAN（ネイティブ VLAN）
トンネリングポート	ポート VLAN

VLAN 判定のアルゴリズムを次の図に示します。

図 24-1　VLAN 判定のアルゴリズム



24.1.5　VLAN Tag

(1)　概要

IEEE 802.1Q 規定による VLAN Tag(イーサネットフレーム中に Tag と呼ばれる識別子を挿入する方法)を使用して，一つのポートに複数の VLAN を構築できます。

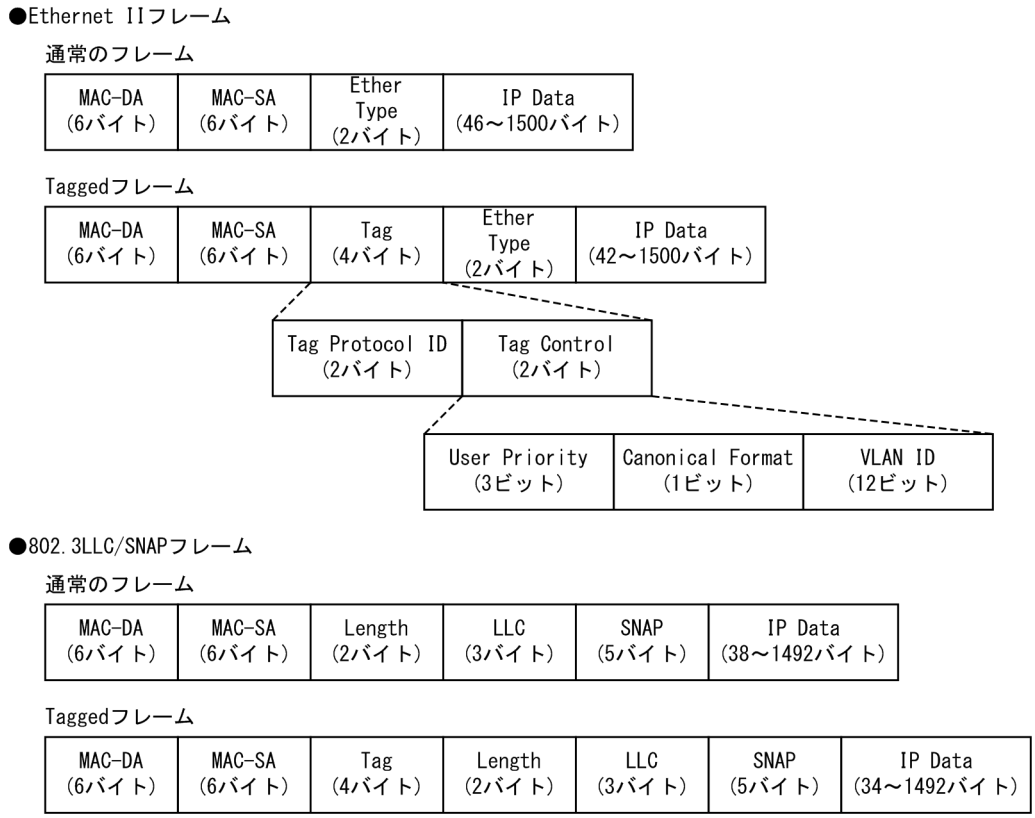
VLAN Tag はトランクポートで使用します。トランクポートはその対向装置も VLAN Tag を認識できなければなりません。

(2) プロトコル仕様

VLAN Tag はイーサネットフレームに Tag と呼ばれる識別子を埋め込むことで，VLAN 情報（=VLAN ID）を離れたセグメントへと伝えることができます。

Tagged フレームのフォーマットを次の図に示します。VLAN Tag を挿入するイーサネットフレームのフォーマットは，Ethernet V2 フォーマットと 802.3 フォーマットの 2 種類があります。

図 24-2 Tagged フレームのフォーマット



VLAN Tag のフィールドの説明を次の表に示します。

表 24-5 VLAN Tag のフィールド

フィールド	説明	本装置の条件
TPID (Tag Protocol ID)	IEEE802.1Q VLAN Tag が続くことを示す Ether Type 値を示します。	ポートごとに任意の値を設定できます。
User Priority	IEEE802.1D のプライオリティを示します。	コンフィグレーションで 8 段階のプライオリティレベルを選択できます。
CF (Canonical Format)	MAC ヘッダ内の MAC アドレスが標準フォーマットに従っているかどうかを示します。	本装置では標準(0)だけをサポートします。
VLAN ID	VLAN ID を示します。※	ユーザが使用できる VLAN ID は 1～4094 です。

注※ Tag 変換を使用している場合，Tag 変換で設定した VLAN ID を使用します。詳細は「25.3 Tag 変換の解説」を参照してください。VLAN ID=0 を受信した場合は，Untagged フレームと同様の扱いになります。VLAN ID=0 で

ある VLAN Tag フィールドが多数あると，上位プロトコルを区別できないことがあります。本装置で VLAN ID=0 の VLAN Tag を追加することはありません。

本装置がレイヤ 2 で中継するフレームの User Priority は，受信したフレームの User Priority と同じです。受信したフレームが Untagged フレームの場合は，User Priority がデフォルト値の 3 になります。なお，送信するフレームの User Priority はコンフィグレーションで変更することができます。User Priority の変更および本装置がレイヤ 3 で中継するフレームの User Priority については，「コンフィグレーションガイド Vol.2」「3.7　マーカー解説」を参照してください。

24.1.6　VLAN 使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

24.2 VLAN 基本機能のコンフィグレーション

24.2.1 コンフィグレーションコマンド一覧

VLAN 基本機能のコンフィグレーションコマンド一覧を次の表に示します。

表 24-6 コンフィグレーションコマンド一覧

コマンド名	説明
name	VLAN の名称を設定します。
state	VLAN の状態（停止／開始）を設定します。
switchport access	アクセスポートの VLAN を設定します。
switchport dot1q ethertype	ポートごとに VLAN Tag の TPID を設定します。
switchport mode	ポートの種類（アクセス，プロトコル，MAC，トランク，トンネリング）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。
vlan-dot1q-ethertype	VLAN Tag の TPID のデフォルト値を設定します。
vlan-up-message	no vlan-up-message コマンドで，VLAN の Up および Down 時の運用メッセージならびに LinkUp／LinkDown トラップの送信を抑止します。

24.2.2 VLAN の設定

[設定のポイント]

VLAN を作成します。新規に VLAN を作成するためには，VLAN ID と VLAN の種類を指定します。VLAN の種類を省略した場合はポート VLAN を作成します。VLAN ID リストによって複数の VLAN を一括して設定することもできます。

vlan コマンドによって，VLAN コンフィグレーションモードに移行します。作成済みの VLAN を指定した場合は，モードの移行だけとなります。VLAN コンフィグレーションモードでは VLAN のパラメータを設定できます。

なお，ここでは VLAN の種類によらない共通した設定について説明します。ポート VLAN，プロトコル VLAN，MAC VLAN のそれぞれについては次節以降を参照してください。

[コマンドによる設定]

1. **(config)# vlan 10**

   VLAN ID 10 のポート VLAN を作成し，VLAN 10 の VLAN コンフィグレーションモードに移行します。

2. **(config-vlan)# name "PORT BASED VLAN 10"**

   (config-vlan)# exit

   作成したポート VLAN 10 の名称を”PORT BASED VLAN 10”に設定します。

3. **(config)# vlan 100-200**

VLAN ID 100～200 のポート VLAN を一括して作成します。また，VLAN 100～200 の VLAN コンフィグレーションモードに移行します。

4. **(config-vlan)# state suspend**
   作成した VLAN ID 100～200 のポート VLAN を一括して停止状態にします。

24.2.3 ポートの設定

[設定のポイント]

イーサネットインタフェースコンフィグレーションモード，ポートチャネルインタフェースコンフィグレーションモードでポートの種類を設定します。ポートの種類は使用したい VLAN の種類に合わせて設定します。

なお，ポート VLAN，プロトコル VLAN，MAC VLAN それぞれの詳細な設定方法については次節以降を参照してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   ポート 1/0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。
2. **(config-if)# switchport mode access**
   (config-if)# exit
   ポート 1/0/1 をアクセスポートに設定します。ポート 1/0/1 はポート VLAN で Untagged フレームを扱うポートになります。
3. **(config)# interface port-channel 10**
   チャネルグループ 10 のポートチャネルインタフェースコンフィグレーションモードに移行します。
4. **(config-if)# switchport mode trunk**
   チャネルグループ 10 をトランクポートに設定します。ポートチャネル 10 は Tagged フレームを扱うポートになります。

24.2.4 トランクポートの設定

[設定のポイント]

トランクポートは VLAN の種類に関係なく，すべての VLAN で使用でき，Tagged フレームを扱います。また，イーサネットインタフェースおよびポートチャネルインタフェースで使用できます。

トランクポートは，switchport mode コマンドを設定しただけではどの VLAN にも所属していません。このポートで扱う VLAN は switchport trunk allowed vlan コマンドによって設定します。

VLAN の追加と削除は，switchport trunk allowed vlan add コマンドおよび switchport trunk allowed vlan remove コマンドによって行います。すでに switchport trunk allowed vlan コマンドを設定した状態でもう一度 switchport trunk allowed vlan コマンドを実行すると，指定した VLAN ID リストに置き換わります。

[コマンドによる設定]

1. **(config)# vlan 10-20,100,200-300**
   (config-vlan)# exit
   (config)# interface gigabitethernet 1/0/1
   (config-if)# switchport mode trunk

VLAN 10～20，100，200～300 を作成します。また，ポート 1/0/1 のイーサネットインタフェースコンフィグレーションモードに移行し，トランクポートに設定します。この状態では，ポート 1/0/1 はどの VLAN にも所属していません。

2. **(config-if)# switchport trunk allowed vlan 10-20**

   ポート 1/0/1 に VLAN 10～20 を設定します。ポート 1/0/1 は VLAN 10～20 の Tagged フレームを扱います。

3. **(config-if)# switchport trunk allowed vlan add 100**

   ポート 1/0/1 で扱う VLAN に VLAN 100 を追加します。

4. **(config-if)# switchport trunk allowed vlan remove 15,16**

   ポート 1/0/1 で扱う VLAN から VLAN 15 および VLAN 16 を削除します。この状態で，ポート 1/0/1 は VLAN 10～14，17～20，VLAN 100 の Tagged フレームを扱います。

5. **(config-if)# switchport trunk allowed vlan 200-300**

   ポート 1/0/1 で扱う VLAN を VLAN 200～300 に設定します。以前の設定はすべて上書きされ，VLAN 200～300 の Tagged フレームを扱います。

[注意事項]

トランクポートで Untagged フレームを扱うためには，ネイティブ VLAN を設定します。詳しくは，「24.4.3　トランクポートのネイティブ VLAN の設定」を参照してください。

トランクポートで，一度に削除する VLAN 数が 30 以上の場合，および所属している VLAN 数が 30 以上のときにモードをトランクポート以外に変更する場合は，該当ポートの MAC アドレステーブル，ARP および NDP 情報を削除します。そのため，L3 中継を行っている場合は，いったん ARP/NDP を再学習して通信が中断するので注意してください。

24.2.5　VLAN Tag の TPID の設定

[設定のポイント]

本装置は，VLAN Tag の TPID を任意の値に設定することができます。vlan-dot1q-ethertype コマンドで装置のデフォルト値を，switchport dot1q ethertype コマンドでポートごとの値を設定します。ポートごとの値を設定していないポートは装置のデフォルト値で動作します。

ポートごとの TPID の設定は，イーサネットインタフェースコンフィグレーションモードで設定します。

[コマンドによる設定]

1. **(config)# vlan-dot1q-ethertype 9100**

   装置のデフォルト値を 0x9100 に設定します。すべてのポートにおいて VLAN Tag を TPID 9100 として動作します。

2. **(config)# interface gigabitethernet 1/0/1**

   ポート 1/0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。

3. **(config-if)# switchport dot1q ethertype 8100**

   ポート 1/0/1 の TPID を 0x8100 に設定します。ポート 1/0/1 は 0x8100 を VLAN Tag として認識します。そのほかのポートは装置のデフォルト値である 0x9100 で動作します。

[注意事項]

TPID は，フレーム上では Untagged フレームの EtherType と同じ位置を使用します。そのため，IPv4 の EtherType である 0x0800 など，EtherType として使用している値を設定するとネットワークが正しく構築できないおそれがあります。EtherType 値として未使用の値を設定してください。

24.3　ポート VLAN の解説

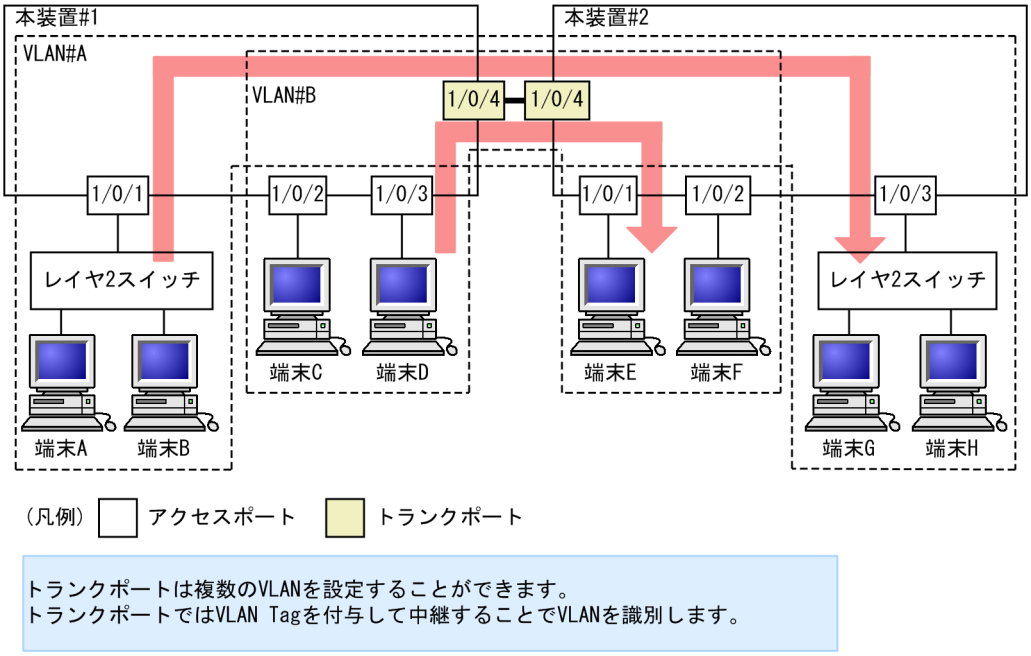
ポート単位に VLAN のグループ分けを行います。

24.3.1　アクセスポートとトランクポート

ポート VLAN は一つのポートに一つの VLAN を割り当てます。ポート VLAN として使用するポートはアクセスポートとして設定します。複数のポート VLAN をほかの LAN スイッチなどに接続するためにはトランクポートを使用します。トランクポートは VLAN Tag によって VLAN を識別するため，一つのポートに複数の VLAN を設定できます。

ポート VLAN の構成例を次の図に示します。ポート 1/0/1～1/0/3 はアクセスポートとしてポート VLAN を設定します。2 台の本装置の間はトランクポート(ポート 1/0/4)で接続します。そのとき，VLAN Tag を使います。

図 24-3　ポート VLAN の構成例



24.3.2　ネイティブ VLAN

プロトコルポート，MAC ポート，トランクポートにはコンフィグレーションに一致しないフレームを扱うネイティブ VLAN があります。各ポートのネイティブ VLAN はコンフィグレーションで指定しない場合は VLAN 1（デフォルト VLAN）です。また，ほかのポート VLAN にコンフィグレーションで変更することもできます。

例えば，「図 24-3　ポート VLAN の構成例」のトランクポートにおいて VLAN#B をネイティブ VLAN に設定すると，VLAN#B はトランクポートでも Untagged フレームで中継します。

24.3.3 ポート VLAN 使用時の注意事項

(1) アクセスポートでの Tagged フレームに関する注意事項

アクセスポートは Untagged フレームを扱うポートです。Tagged フレームを受信した場合は廃棄します。また，送信することもできません。なお，VLAN Tag 値が VLAN の ID と一致する場合および 0 の場合は，受信時に Untagged フレームと同じ扱いになります。これらのフレームを送信することはありません。

(2) MAC VLAN 混在時の注意事項

同一ポートにポート VLAN と MAC VLAN が混在する場合，マルチキャスト使用時の注意事項があります。詳細は，「24.7.5 VLAN 混在時のマルチキャストについて」を参照してください。

24.4　ポート VLAN のコンフィグレーション

24.4.1　コンフィグレーションコマンド一覧

ポート VLAN のコンフィグレーションコマンド一覧を次の表に示します。

表 24-7　コンフィグレーションコマンド一覧

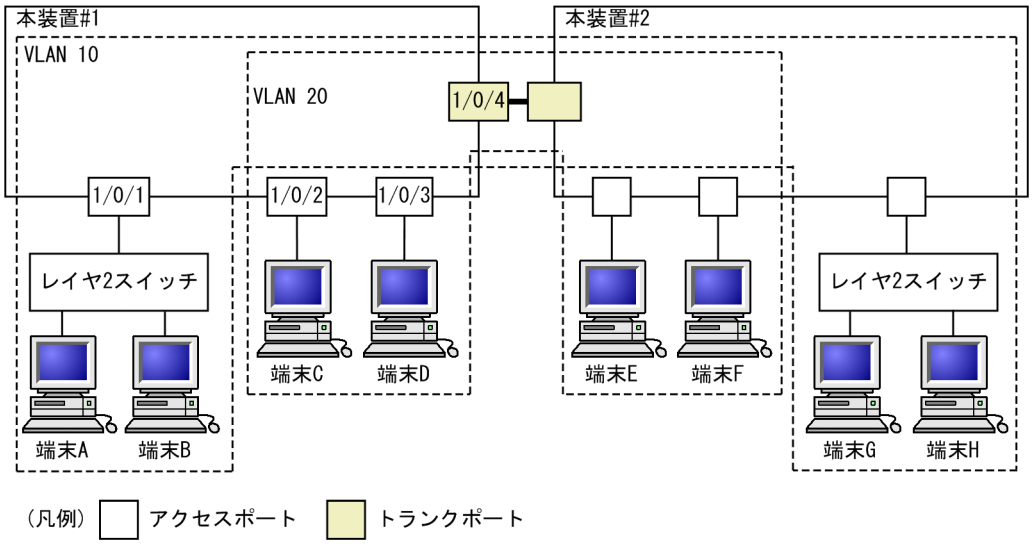
コマンド名	説明
switchport access	アクセスポートの VLAN を設定します。
switchport mode	ポートの種類（アクセス，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	ポート VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

24.4.2　ポート VLAN の設定

ポート VLAN を設定する手順を以下に示します。ここでは，次の図に示す本装置#1 の設定例を示します。

ポート 1/0/1 はポート VLAN 10 を設定します。ポート 1/0/2，1/0/3 はポート VLAN 20 を設定します。ポート 1/0/4 はトランクポートでありすべての VLAN を設定します。

図 24-4　ポート VLAN の設定例



(1)　ポート VLAN の作成

[設定のポイント]

ポート VLAN を作成します。VLAN を作成する際に VLAN ID だけを指定して VLAN の種類を指定しないで作成するとポート VLAN となります。

[コマンドによる設定]

1. **(config)# vlan 10,20**

VLAN ID 10，VLAN ID 20 をポート VLAN として作成します。本コマンドで VLAN コンフィグレーションモードに移行します。

(2) アクセスポートの設定

一つのポートに一つの VLAN を設定して Untagged フレームを扱う場合，アクセスポートとして設定します。

[設定のポイント]

ポートをアクセスポートに設定して，そのアクセスポートで扱う VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   ポート 1/0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。
2. **(config-if)# switchport mode access**
   (config-if)# switchport access vlan 10
   (config-if)# exit
   ポート 1/0/1 をアクセスポートに設定します。また，VLAN 10 を設定します。
3. **(config)# interface range gigabitethernet 1/0/2-3**
   ポート 1/0/2，1/0/3 のイーサネットインタフェースコンフィグレーションモードに移行します。ポート 1/0/2，1/0/3 は同じコンフィグレーションとなるため，一括して設定します。
4. **(config-if-range)# switchport mode access**
   (config-if-range)# switchport access vlan 20
   ポート 1/0/2，1/0/3 をアクセスポートに設定します。また，VLAN 20 を設定します。

(3) トランクポートの設定

[設定のポイント]

Tagged フレームを扱うポートはトランクポートとして設定し，そのトランクポートに VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/4**
   ポート 1/0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。
2. **(config-if)# switchport mode trunk**
   (config-if)# switchport trunk allowed vlan 10,20
   ポート 1/0/4 をトランクポートに設定します。また，VLAN 10，20 を設定します。

24.4.3 トランクポートのネイティブ VLAN の設定

[設定のポイント]

トランクポートで Untagged フレームを扱いたい場合，ネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけを設定できます。

ネイティブ VLAN の VLAN ID を switchport trunk allowed vlan コマンドで指定すると，トランクポートで Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して指定しない場合は VLAN 1（デフォルト VLAN）です。

トランクポート上で，デフォルト VLAN で Tagged フレーム（VLAN ID 1 の VLAN Tag）を扱いたい場合は，ネイティブ VLAN をほかの VLAN に変更してください。

[コマンドによる設定]

1. **(config)# vlan 10,20**

   (config-vlan)# exit

   VLAN ID 10，VLAN ID 20 をポート VLAN として作成します。

2. **(config)# interface gigabitethernet 1/0/1**

   (config-if)# switchport mode trunk

   ポート 1/0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。また，トランクポートとして設定します。この状態で，トランクポート 1/0/1 のネイティブ VLAN はデフォルト VLAN です。

3. **(config-if)# switchport trunk native vlan 10**

   (config-if)# switchport trunk allowed vlan 1,10,20

   トランクポート 1/0/1 のネイティブ VLAN を VLAN 10 に設定します。また，VLAN 1，10，20 を設定します。ネイティブ VLAN である VLAN 10 が Untagged フレームを扱い，VLAN 1（デフォルト VLAN），VLAN 20 は Tagged フレームを扱います。

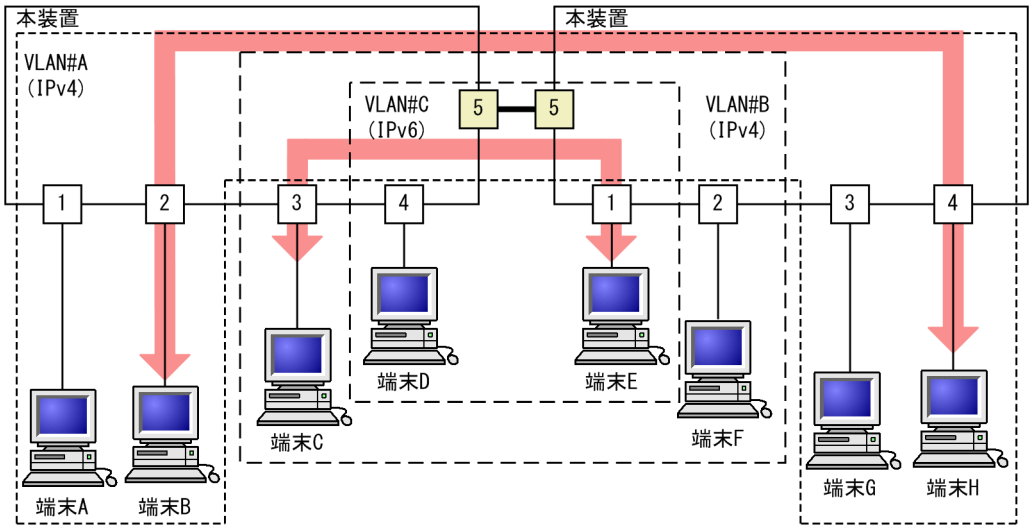
24.5　プロトコル VLAN の解説

24.5.1　概要

プロトコル単位で VLAN のグループ分けを行います。IPv4 や IPv6 といったプロトコルごとに異なる VLAN を構成できます。複数のプロトコルを同一のプロトコル VLAN に設定することもできます。

プロトコル VLAN の構成例を次の図に示します。VLAN#A，#B を IPv4 プロトコルで構成し，VLAN#C を IPv6 プロトコルで構成した例を示しています。

図 24–5　プロトコル VLAN の構成例



（凡例）：プロトコルポート　：トランクポート

・VLAN#A，#BはIPv4プロトコルのVLANです。
・VLAN#CはIPv6プロトコルのVLANです。
・端末D，EはVLAN#B，#Cの両方に属しています。
・矢印は端末Bと端末H間，端末Cと端末E間で同じVLANで通信している例です。

24.5.2　プロトコルの識別

プロトコルの識別には次の 3 種類の値を使用します。

表 24–8　プロトコルを識別する値

識別する値	概要
Ether-type 値	EthernetV2 形式フレームの Ether-type 値によってプロトコルを識別します。
LLC 値	802.3 形式フレームの LLC 値(DSAP,SSAP)によってプロトコルを識別します。
SNAP Ether-type 値	802.3 形式フレームの Ether-type 値によってプロトコルを識別します。フレームの LLC 値が AA AA 03 であるフレームだけが対象となります。

プロトコルは，コンフィグレーションによってプロトコルを作成し VLAN に対応付けます。一つのプロトコル VLAN に複数のプロトコルを対応付けることもできます。

24.5.3　プロトコルポートとトランクポート

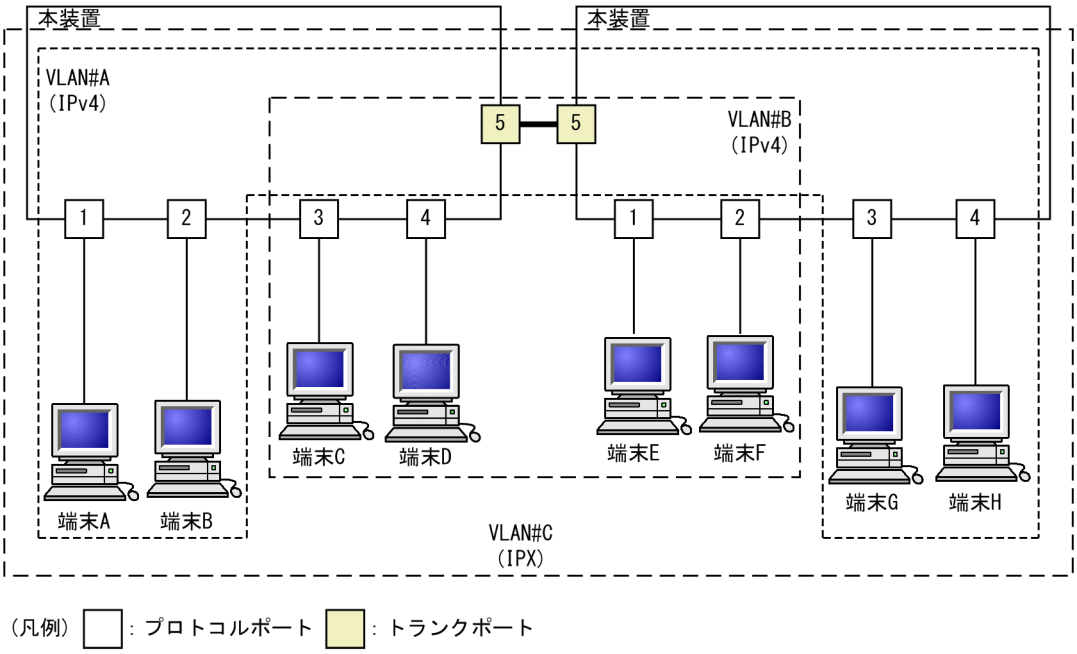
プロトコルポートは Untagged フレームのプロトコルを識別します。プロトコル VLAN として使用するポートはプロトコルポートを設定します。プロトコルポートには複数のプロトコルで異なる VLAN を割り当てることもできます。複数のプロトコル VLAN をほかの LAN スイッチなどに接続するためにはトランクポートを使用します。なお，トランクポートは VLAN Tag によって VLAN を識別するため，プロトコルによる識別は行いません。

24.5.4　プロトコルポートのネイティブ VLAN

プロトコルポートでコンフィグレーションに一致しないプロトコルのフレームを受信した場合はネイティブ VLAN で扱います。ネイティブ VLAN は，コンフィグレーションで指定しない場合は VLAN 1（デフォルト VLAN）です。また，ほかのポート VLAN にコンフィグレーションで変更することもできます。

次の図に，プロトコルポートでネイティブ VLAN を使用する構成例を示します。図の構成は，IPX プロトコルをネットワーク全体で一つの VLAN とし，そのほか（IPv4 など）のプロトコルについてはポート VLAN で VLAN を分ける例です。VLAN#A，VLAN#B を各ポートのネイティブ VLAN として設定します。なお，この構成例では，VLAN#A，VLAN#B も IPv4 のプロトコル VLAN として設定することもできます。

図 24-6　プロトコルポートでネイティブ VLAN を使用する構成例



・VLAN#A，#BはポートVLANでネイティブVLANとして設定します。
・VLAN#CはIPXプロトコルのVLANです。
・すべての端末はIPXプロトコルVLANに属しています。
・端末A,B,G,Hと端末C,D,E,Fはそれぞれ異なるポートVLANに属しています。

24.6 プロトコル VLAN のコンフィグレーション

24.6.1 コンフィグレーションコマンド一覧

プロトコル VLAN のコンフィグレーションコマンド一覧を次の表に示します。

表 24-9 コンフィグレーションコマンド一覧

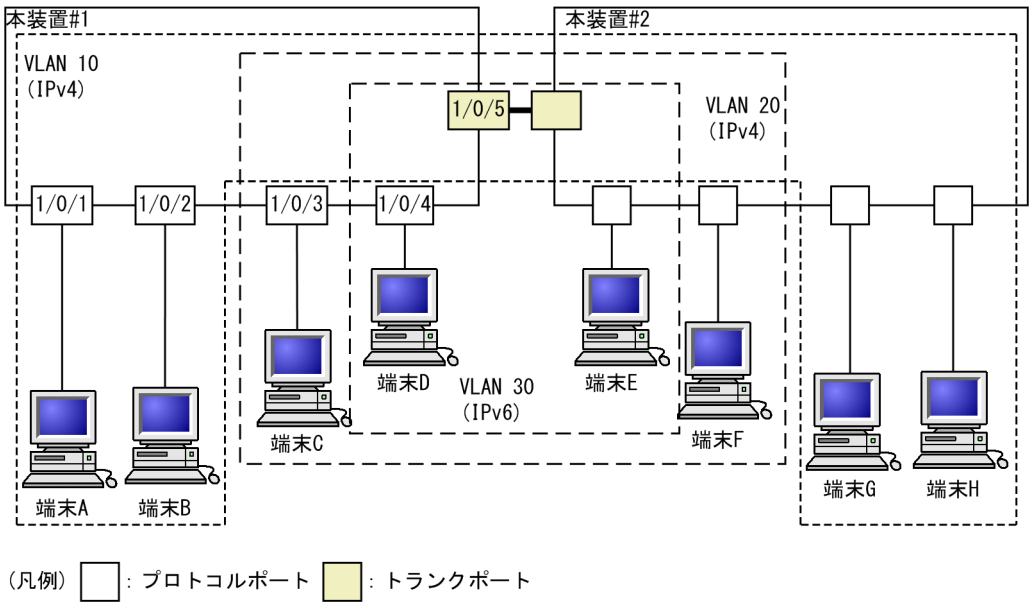
コマンド名	説明
protocol	プロトコル VLAN で VLAN を識別するプロトコルを設定します。
switchport mode	ポートの種類（プロトコル，トランク）を設定します。
switchport protocol	プロトコルポートの VLAN を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	protocol-based パラメータを指定してプロトコル VLAN を作成します。
vlan-protocol	プロトコル VLAN 用のプロトコル名称とプロトコル値を設定します。

24.6.2 プロトコル VLAN の作成

プロトコル VLAN を設定する手順を以下に示します。ここでは，次の図に示す本装置#1 の設定例を示します。

ポート 1/0/1，1/0/2 は IPv4 プロトコル VLAN 10 を設定します。ポート 1/0/3，1/0/4 は IPv4 プロトコル VLAN 20 を設定します。ポート 1/0/4 は VLAN 20 と同時に IPv6 プロトコル VLAN 30 にも所属します。ポート 1/0/5 はトランクポートであり，すべての VLAN を設定します。

図 24-7 プロトコル VLAN の設定例



(1) VLAN を識別するプロトコルの作成

[設定のポイント]

プロトコル VLAN は，VLAN を作成する前に識別するプロトコルを vlan-protocol コマンドで設定します。プロトコルは，プロトコル名称とプロトコル値を設定します。一つの名称に複数のプロトコル値を関連づけることもできます。

IPv4 プロトコルは, IPv4 の Ether-type と同時に ARP の Ether-type も指定する必要があるため, IPv4 には二つのプロトコル値を関連づけます。

[コマンドによる設定]

1. **(config)# vlan-protocol IPV4 ethertype 0800 ethertype 0806**

   名称 IPV4 のプロトコルを作成します。プロトコル値として，IPv4 の Ether-type 値 0800 と ARP の Ether-type 値 0806 を関連づけます。

   なお，この設定でのプロトコル判定は EthernetV2 形式のフレームだけとなります。

2. **(config)# vlan-protocol IPV6 ethertype 86dd**

   名称 IPV6 のプロトコルを作成します。プロトコル値として IPv6 の Ether-type 値 86DD を関連づけます。

(2) プロトコル VLAN の作成

[設定のポイント]

プロトコル VLAN を作成します。VLAN を作成する際に VLAN ID と protocol-based パラメータを指定します。また，VLAN を識別するプロトコルとして，作成したプロトコルを指定します。

[コマンドによる設定]

1. **(config)# vlan 10,20 protocol-based**

   VLAN 10, 20 をプロトコル VLAN として作成します。VLAN 10, 20 は同じ IPv4 プロトコル VLAN とするため一括して設定します。本コマンドで VLAN コンフィグレーションモードに移行します。

2. **(config-vlan)# protocol IPV4**

   (config-vlan)# exit

   VLAN 10，20 を識別するプロトコルとして，作成した IPv4 プロトコルを指定します。

3. **(config)# vlan 30 protocol-based**

   (config-vlan)# protocol IPV6

   VLAN 30 をプロトコル VLAN として作成します。また，VLAN 30 を識別するプロトコルとして，作成した IPv6 プロトコルを指定します。

(3) プロトコルポートの設定

[設定のポイント]

プロトコル VLAN でプロトコルによって VLAN を識別するポートは，プロトコルポートを設定します。このポートでは Untagged フレームを扱います。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**

   ポート 1/0/1，1/0/2 のイーサネットインタフェースコンフィグレーションモードに移行します。ポート 1/0/1，1/0/2 は同じコンフィグレーションとなるため一括して指定します。

2. **(config-if-range)# switchport mode protocol-vlan**
   (config-if-range)# switchport protocol vlan 10
   (config-if-range)# exit
   ポート 1/0/1，1/0/2 をプロトコルポートに設定します。また，VLAN 10 を設定します。
3. **(config)# interface range gigabitethernet 1/0/3-4**
   (config-if-range)# switchport mode protocol-vlan
   (config-if-range)# switchport protocol vlan 20
   (config-if-range)# exit
   ポート 1/0/3，1/0/4 をプロトコルポートに設定します。また，VLAN 20 を設定します。
4. **(config)# interface gigabitethernet 1/0/4**
   (config-if)# switchport protocol vlan add 30
   ポート 1/0/4 に VLAN 30 を追加します。ポート 1/0/4 は IPv4，IPv6 の 2 種類のプロトコル VLAN を設定しています。

[注意事項]

switchport protocol vlan コマンドは，それ以前のコンフィグレーションに追加するコマンドではなく指定した<vlan id list>に設定を置き換えます。すでにプロトコル VLAN を運用中のポートで VLAN の追加や削除を行う場合は，switchport protocol vlan add コマンドおよび switchport protocol vlan remove コマンドを使用してください。

(4) トランクポートの設定

[設定のポイント]

プロトコル VLAN においても，Tagged フレームを扱うポートはトランクポートとして設定し，そのトランクポートに VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/5**
   ポート 1/0/5 のイーサネットインタフェースコンフィグレーションモードに移行します。
2. **(config-if)# switchport mode trunk**
   (config-if)# switchport trunk allowed vlan 10,20,30
   ポート 1/0/5 をトランクポートに設定します。また，VLAN 10，20，30 を設定します。

24.6.3 プロトコルポートのネイティブ VLAN の設定

[設定のポイント]

プロトコルポートで設定したプロトコルに一致しない Untagged フレームを扱いたい場合，そのフレームを扱う VLAN としてネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけを設定できます。

ネイティブ VLAN の VLAN ID を switchport protocol native vlan コマンドで指定すると，プロトコルポート上で設定したプロトコルに一致しない Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して指定しない場合は VLAN 1（デフォルト VLAN）です。

ネイティブ VLAN に state suspend コマンドが設定されている場合は，設定したプロトコルと一致しないフレームが中継されません。

[コマンドによる設定]

1. **(config)# vlan 10,20 protocol-based**

   (config-vlan)# exit

   (config)# vlan 30

   (config-vlan)# exit

   VLAN 10，20 をプロトコル VLAN として作成します。また，VLAN 30 をポート VLAN として作成します。

2. **(config)# interface gigabitethernet 1/0/1**

   (config-if)# switchport mode protocol-vlan

   ポート 1/0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。また，プロトコルポートとして設定します。

3. **(config-if)# switchport protocol native vlan 30**

   (config-if)# switchport protocol vlan 10,20

   プロトコルポート 1/0/1 のネイティブ VLAN をポート VLAN 30 に設定し，設定したプロトコルに一致しない Untagged フレームを扱う VLAN とします。また，プロトコル VLAN 10，20 を設定します。

24.7　MAC VLAN の解説

24.7.1　概要

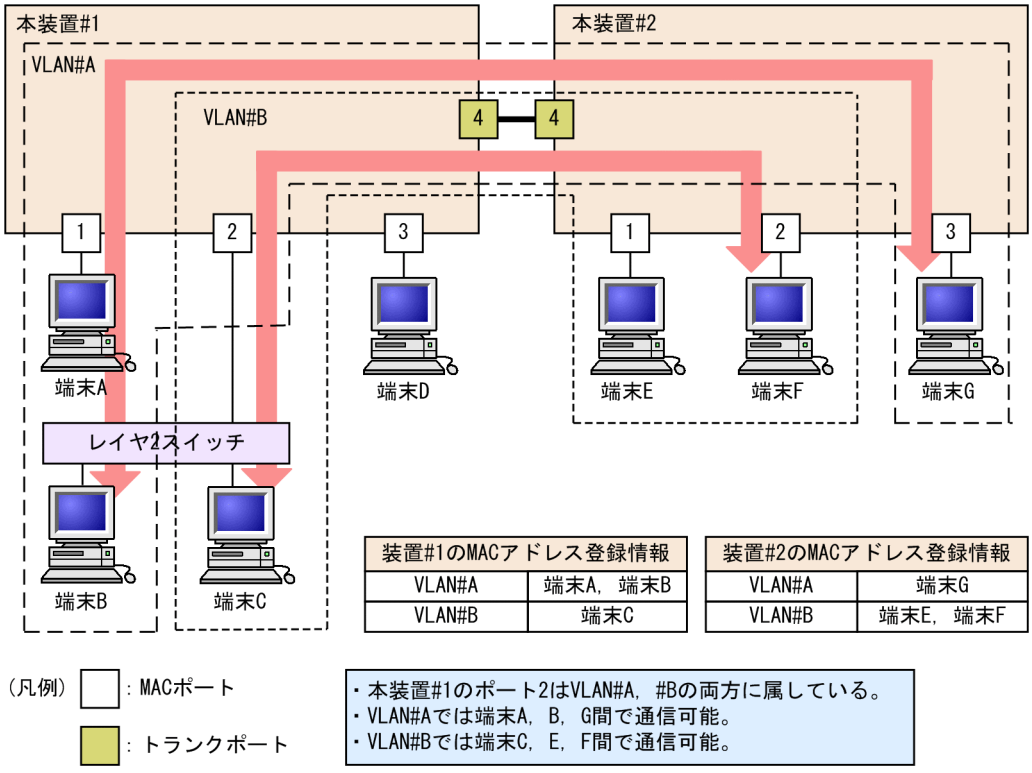
送信元の MAC アドレス単位に VLAN のグループ分けを行います。VLAN への MAC アドレスの登録は，コンフィグレーションによる登録と，レイヤ 2 認証機能による動的な登録ができます。

MAC VLAN は，許可した端末の MAC アドレスをコンフィグレーションで登録するか，レイヤ 2 認証機能で認証された MAC アドレスを登録することによって，接続を許可された端末とだけ通信できるように設定できます。

さらに，コンフィグレーションコマンド mac-based-vlan static-only を設定すると，MAC VLAN の最大収容数までコンフィグレーションコマンド mac-address で MAC アドレスを設定できます。なお，この場合，レイヤ 2 認証機能を動作させることはできません。

MAC VLAN の構成例を次の図に示します。VLAN を構成する装置間にトランクポートを設定している場合は，送信元 MAC アドレスに関係なく VLAN Tag によって VLAN を決定します。そのため，すべての装置に同じ MAC アドレスの設定をする必要はありません。装置ごとに MAC ポートに接続した端末の MAC アドレスを設定します。

図 24-8　MAC VLAN の構成例



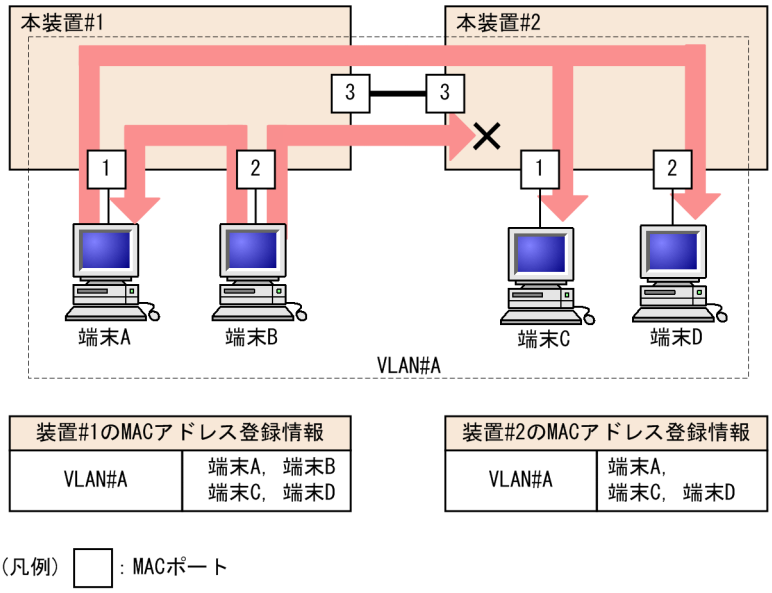
24.7.2　装置間の接続と MAC アドレス設定

複数の装置で MAC VLAN を構成する場合，装置間の接続はトランクポートをお勧めします。トランクポートで受信したフレームの VLAN 判定は VLAN Tag で行います。そのため，送信元 MAC アドレスが VLAN に設定されていなくても，MAC VLAN で通信できます。トランクポートで装置間を接続した場合については，「図 24-8　MAC VLAN の構成例」を参照してください。

MAC ポートで装置間を接続する場合は，その VLAN に属するすべての MAC アドレスをすべての装置に設定する必要があります。ルータが存在する場合は，ルータの MAC アドレスも登録してください。また，VRRP を使用している場合は，仮想ルータ MAC アドレスを登録してください。

MAC ポートで装置間を接続した場合の図を次に示します。

図 24-9　装置間を MAC ポートで接続した場合



・端末Aは，本装置#1，#2の両方に設定があるため，端末C，端末Dと通信可能。
・端末Bは，本装置#2に設定がないため，端末C，端末Dと通信不可。
　端末Aとは通信可能。

24.7.3　レイヤ 2 認証機能との連携について

MAC VLAN は，レイヤ 2 認証機能と連携して，VLAN への MAC アドレスを動的に登録できます。連携するレイヤ 2 認証機能を次に示します。

- IEEE802.1X
- Web 認証
- MAC 認証

プリンタやサーバなど，レイヤ 2 認証機能を動作させないで MAC ポートと接続する端末は，その MAC アドレスをコンフィグレーションで VLAN に登録します。

コンフィグレーションとレイヤ 2 認証機能で同じ MAC アドレスを設定した場合，コンフィグレーションの MAC アドレスを登録します。

24.7.4　MAC ポートの VLAN 設定

MAC ポートに VLAN を設定する場合，コンフィグレーションコマンド switchport mac vlan による設定と，レイヤ 2 認証機能による動的な設定ができます。

なお，同じ MAC ポートに，コンフィグレーションによる VLAN の設定と，レイヤ 2 認証機能による動的な VLAN の設定とを共存させることはできません。認証対象ポートとして設定されている MAC ポート

に対し，レイヤ 2 認証機能で VLAN が動的に設定されている状態のときにコンフィグレーションコマンド switchport mac vlan が設定された場合，該当ポートに動的に設定されていた VLAN はすべて削除されます。

動的に VLAN が設定できるレイヤ 2 認証機能と認証モードを次の表に示します。

表 24-10　動的に VLAN が設定できるレイヤ 2 認証機能と認証モード

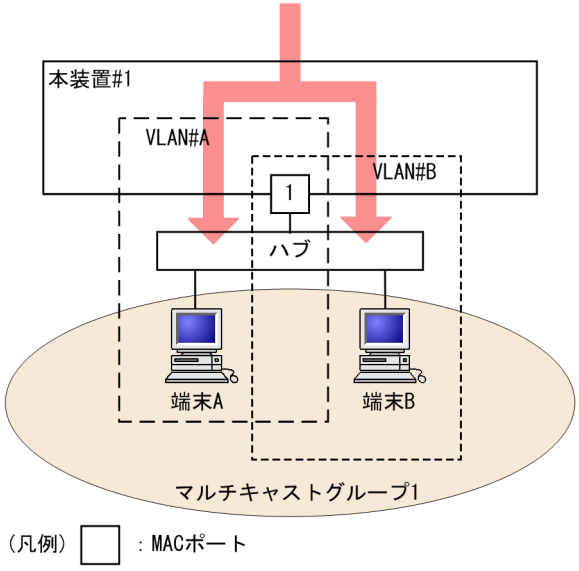
レイヤ 2 認証機能	認証モード
IEEE802.1X	VLAN 単位認証（動的）
Web 認証	ダイナミック VLAN モード
MAC 認証	ダイナミック VLAN モード

24.7.5　VLAN 混在時のマルチキャストについて

同一ポートに複数の MAC VLAN が混在した場合やポート VLAN と MAC VLAN が混在した場合，それぞれの VLAN に所属する端末が同じマルチキャストグループに所属すると，そのポートへは VLAN ごとに同じマルチキャストフレームを送信するため，端末は同じフレームを重複して受信します。

端末でマルチキャストデータを重複して受信してしまうネットワークの構成例を次に示します。

図 24-10　VLAN 混在時のマルチキャスト



・本装置#1のポート1はVLAN#A，#Bの両方に属している。
・端末A，Bは同じマルチキャストグループ1に属している。
・マルチキャストは，ポート1からVLAN#A，#Bのそれぞれに送信される。

24.8 MAC VLAN のコンフィグレーション

24.8.1 コンフィグレーションコマンド一覧

MAC VLAN のコンフィグレーションコマンド一覧を次の表に示します。

表 24-11 コンフィグレーションコマンド一覧

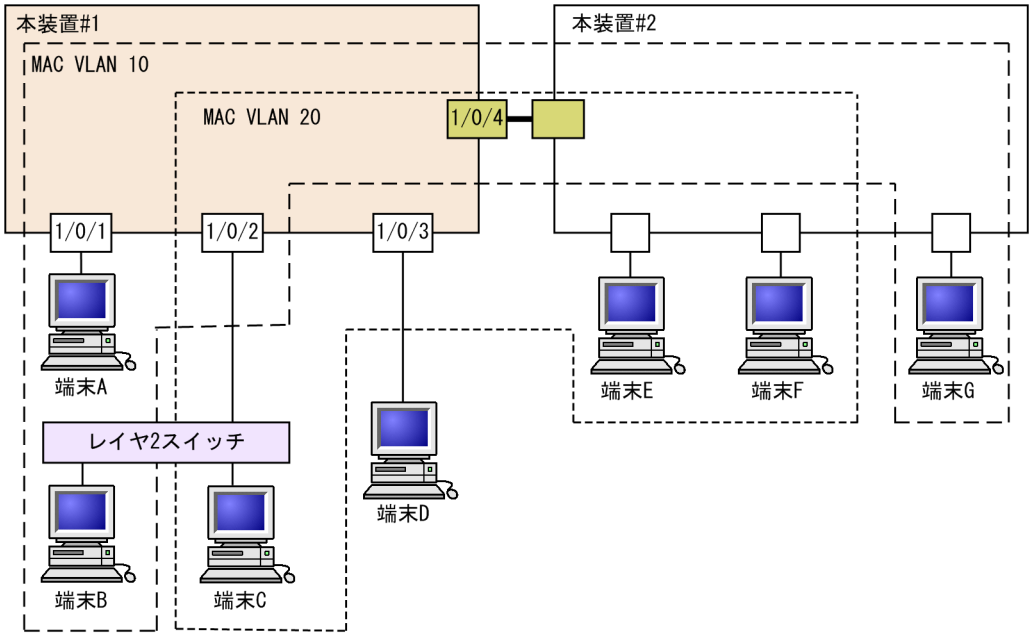
コマンド名	説明
mac-address	MAC VLAN で VLAN に所属する端末の MAC アドレスをコンフィグレーションによって設定します。
switchport mac	MAC ポートの VLAN を設定します。
switchport mode	ポートの種類（MAC，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	mac-based パラメータを指定して MAC VLAN を作成します。

24.8.2 MAC VLAN の設定

MAC VLAN を設定する手順を以下に示します。ここでは，MAC VLAN と VLAN に所属する MAC アドレスをコンフィグレーションで設定する場合の例を示します。IEEE802.1X との連携については，「コンフィグレーションガイド Vol.2」「7 IEEE802.1X の設定と運用」を参照してください。

次の図に示す本装置#1 の設定例を示します。ポート 1/0/1 は MAC VLAN 10 を設定します。ポート 1/0/2 は MAC VLAN 10 および 20，1/0/3 は MAC VLAN 20 を設定します。ただし，ポート 1/0/3 には MAC アドレスを登録していない端末 D を接続しています。

図 24-11 MAC VLAN の設定例



装置#1のMACアドレス登録情報		
VLAN 10	端末A	0012.e200.0001
	端末B	0012.e200.0002
VLAN 20	端末C	0012.e200.0003

(1) MAC VLAN の作成と MAC アドレスの登録

[設定のポイント]

MAC VLAN を作成します。VLAN を作成する際に VLAN ID と mac-based パラメータを指定します。

また，VLAN に所属する MAC アドレスを設定します。構成例の端末 A～C をそれぞれの VLAN に登録します。端末 D は MAC VLAN での通信を許可しない端末にするので登録しません。

[コマンドによる設定]

1. **(config)# vlan 10 mac-based**
   (config-vlan)# name MACVLAN10
   VLAN 10 を MAC VLAN として作成します。本コマンドで VLAN コンフィグレーションモードに移行します。
2. **(config-vlan)# mac-address 0012.e200.0001**
   (config-vlan)# mac-address 0012.e200.0002
   (config-vlan)# exit
   端末 A（0012.e200.0001），端末 B（0012.e200.0002）を MAC VLAN 10 に登録します。
3. **(config)# vlan 20 mac-based**
   (config-vlan)# name MACVLAN20
   (config-vlan)# mac-address 0012.e200.0003
   VLAN 20 を MAC VLAN として作成し，端末 C（0012.e200.0003）を MAC VLAN 20 に登録します。

[注意事項]

MAC VLAN に登録する MAC アドレスでは，同じ MAC アドレスを複数の VLAN に登録できません。

(2) MAC ポートの設定

[設定のポイント]

MAC VLAN で送信元 MAC アドレスによって VLAN を識別するポートは，MAC ポートを設定します。このポートでは Untagged フレームを扱います。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 1/0/1-2**

   ポート 1/0/1，1/0/2 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if-range)# switchport mode mac-vlan**

   (config-if-range)# exit

   ポート 1/0/1，1/0/2 を MAC ポートに設定します。ポート 1/0/1，1/0/2 はレイヤ 2 認証機能によって動的に VLAN が登録されます。

3. **(config)# interface gigabitethernet 1/0/3**

   (config-if)# switchport mode mac-vlan

   (config-if)# switchport mac vlan 20

   ポート 1/0/3 を MAC ポートに設定します。また，VLAN 20 を設定します。

[注意事項]

switchport mac vlan コマンドは，それ以前のコンフィグレーションに追加するコマンドではなく指定した<vlan id list>に設定を置き換えます。すでに MAC VLAN を運用中のポートで VLAN の追加や削除を行う場合は，switchport mac vlan add コマンドおよび switchport mac vlan remove コマンドを使用してください。

(3) トランクポートの設定

[設定のポイント]

MAC VLAN においても，Tagged フレームを扱うポートはトランクポートとして設定し，そのトランクポートに VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/4**

   ポート 1/0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# switchport mode trunk**

   (config-if)# switchport trunk allowed vlan 10,20

   ポート 1/0/4 をトランクポートに設定します。また，VLAN 10，20 を設定します。

24.8.3 MAC ポートのネイティブ VLAN の設定

[設定のポイント]

MAC ポートで MAC VLAN に登録した MAC アドレスに一致しない Untagged フレームを扱いたい場合，そのフレームを扱う VLAN としてネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけが設定できます。

ネイティブ VLAN の VLAN ID を switchport mac native vlan コマンドで指定すると，MAC ポート上で登録した MAC アドレスに一致しない Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して指定しない場合は VLAN 1（デフォルト VLAN）です。

ネイティブ VLAN に state suspend コマンドが設定されていた場合は，登録した MAC アドレスに一致しないフレームが中継されません。

[コマンドによる設定]

1. **(config)# vlan 10,20 mac-based**
   (config-vlan)# exit
   (config)# vlan 30
   (config-vlan)# exit
   VLAN 10,20 を MAC VLAN として作成します。また，VLAN 30 をポート VLAN として作成します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# switchport mode mac-vlan
   ポート 1/0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。また，MAC ポートとして設定します。
3. **(config-if)# switchport mac native vlan 30**
   ポート 1/0/1 のネイティブ VLAN をポート VLAN 30 に設定します。VLAN 30 はポート 1/0/1 で登録されていない MAC アドレスからの Untagged フレームを扱う VLAN となります。

24.9 VLAN インタフェース

24.9.1 IP アドレスを設定するインタフェース

本装置をレイヤ 3 スイッチとして使用するためには，VLAN に IP アドレスを設定します。複数の VLAN を作成し，各 VLAN に IP アドレスを設定することで本装置はレイヤ 3 スイッチとして動作します。

IP アドレスはコンフィグレーションコマンド interface vlan によって設定します。このインタフェースのことを VLAN インタフェースと呼びます。

24.9.2 VLAN インタフェースの MAC アドレス

IP アドレスを設定した VLAN インタフェースは，本装置の持つ MAC アドレスの一つをそのインタフェースの MAC アドレスとして使用します。使用する MAC アドレスを次に示します。

- 装置 MAC アドレス
- VLAN ごとの MAC アドレス

デフォルトでは装置 MAC アドレスを使用します。コンフィグレーションによって VLAN ごとの MAC アドレスを設定できます。

VLAN インタフェースの MAC アドレスは，コンフィグレーションによって運用中に変更できます。運用中に変更すると，隣接するレイヤ 3 装置（ルータ，レイヤ 3 スイッチ，端末など）が ARP や NDP で学習した MAC アドレスと，本装置の MAC アドレスが不一致となり，一時的に通信ができなくなる場合があるため注意してください。

24.10 VLAN インタフェースのコンフィグレーション

24.10.1 コンフィグレーションコマンド一覧

VLAN インタフェースに IP アドレスを設定し，レイヤ 3 スイッチとして使用するための基本的なコンフィグレーションコマンド一覧を次の表に示します。

表 24-12 コンフィグレーションコマンド一覧

コマンド名	説明
interface vlan	VLAN インタフェースを設定します。また，インタフェースモードへ移行します。
vlan-mac	VLAN ごとの MAC アドレスを使用することを設定します。
vlan-mac-prefix	VLAN ごとの MAC アドレスのプレフィックスを設定します。
ip address※	インタフェースの IPv4 アドレスを設定します。

注※
「コンフィグレーションコマンドレファレンス Vol.2」「2 IPv4・ARP・ICMP」を参照してください。

24.10.2 レイヤ 3 インタフェースとしての VLAN の設定

[設定のポイント]

VLAN は IP アドレスを設定してレイヤ 3 インタフェースとして使用できます。interface vlan コマンドおよび VLAN インタフェースコンフィグレーションモードでさまざまなレイヤ 3 機能を設定できます。

ここでは，VLAN インタフェースに IPv4 アドレスを設定する例を示します。VLAN インタフェースで設定できるレイヤ 3 機能については，使用する各機能の章を参照してください。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   VLAN 10 の VLAN インタフェースコンフィグレーションモードに移行します。interface vlan コマンドで指定した VLAN ID が未設定の VLAN ID の場合，自動的にポート VLAN を作成して vlan コマンドが設定されます。
2. **(config-if)# ip address 192.168.1.1 255.255.255.0**
   VLAN 10 に IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

24.10.3 VLAN インタフェースの MAC アドレスの設定

本装置の VLAN インタフェースの MAC アドレスは，デフォルトではすべての VLAN で装置 MAC アドレスを使用します。通常，LAN スイッチは VLAN ごとに MAC アドレス学習を行うため，異なる VLAN で同じ MAC アドレスを使用できます。しかし，VLAN ごとではなく装置単位に一つの MAC アドレステーブルを管理する LAN スイッチを同じネットワーク上で使用している場合，異なる VLAN で同じ MAC アドレスを使用すると MAC アドレス学習が安定しなくなる場合があります。そのような場合に VLAN インタフェースの MAC アドレスを VLAN ごとに変更することによってネットワークを安定させることができます。

[設定のポイント]

VLAN をレイヤ 3 インタフェースとして使用する場合，VLAN インタフェースの MAC アドレスを変更できます。MAC アドレスは vlan-mac-prefix コマンドおよび vlan-mac コマンドで設定します。

VLAN ごとの MAC アドレスは，vlan-mac-prefix コマンドで上位 34bit までのプレフィックスを指定し，かつ VLAN ごとに vlan-mac コマンドで，VLAN ごとの MAC アドレスを使用することを設定します。MAC アドレスは下位 12bit に VLAN ID を使用します。

[コマンドによる設定]

1. **(config)# vlan-mac-prefix 0012.e200.0000 ffff.ffff.c000**

   VLAN ごと MAC アドレスに使用するプレフィックス（上位 34bit）を指定します。マスクは 34bit で指定する場合 ffff.ffff.c000 になります。

2. **(config)# vlan 10**

   VLAN 10 の VLAN コンフィグレーションモードに移行します。

3. **(config-vlan)# vlan-mac**

   VLAN 10 で VLAN ごと MAC アドレスを使用することを設定します。MAC アドレスは下位 12bit に VLAN ID を使用し，この場合 VLAN 10 の MAC アドレスは 0012.e200.000a になります。

   MAC アドレスの値は運用コマンド show vlan で確認できます。

[注意事項]

VLAN ごと MAC アドレスの設定で，VLAN インタフェースの MAC アドレスが変更になります。これによって，隣接するレイヤ 3 装置（ルータ，レイヤ 3 スイッチ，端末など）が ARP や NDP で学習した MAC アドレスと本装置の VLAN インタフェースの MAC アドレスが不一致となり，一時的に通信できなくなる場合があります。本機能の設定は VLAN インタフェースの運用開始前に設定するか，または通信の影響が少ないときに行うことをお勧めします。

なお，VLAN ごと MAC アドレスの設定は，該当する VLAN インタフェースに IP アドレスが設定されているときだけ有効です。

24.11 VLAN のオペレーション

24.11.1 運用コマンド一覧

VLAN の運用コマンド一覧を次の表に示します。

表 24-13 運用コマンド一覧

コマンド名	説明
show vlan	VLAN の各種情報を表示します。
show vlan mac-vlan	MAC VLAN に登録されている MAC アドレスを表示します。
restart vlan	VLAN プログラムを再起動します。
dump protocols vlan	VLAN プログラムで採取している詳細イベントトレース情報および制御テーブルをファイルへ出力します。

24.11.2 VLAN の状態の確認

(1) VLAN の設定状態の確認

VLAN の情報は show vlan コマンドで確認できます。VLAN ID，Type，IP Address などによって VLAN に関する設定が正しいことを確認してください。また，Untagged はその VLAN で Untagged フレームを扱うポート，Tagged はその VLAN で Tagged フレームを扱うポートになります。VLAN に設定されているポートの設定が正しいことを確認してください。

図 24-12 show vlan コマンドの実行結果

```
> show vlan
Date 20XX/01/26 17:01:40 UTC
VLAN counts:4
VLAN ID:1     Type:Port based      Status:Up
  Learning:On             Tag-Translation:
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name:VLAN0001
  IP Address:10.215.201.1/24
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0001
  Spanning Tree:PVST+(802.1D)
  AXRP RING ID:       AXRP VLAN group:
  GSRP ID:       GSRP VLAN group:    L3:
  IGMP snooping:      MLD snooping:
  Untagged(18)  :1/0/1-4,13-26
VLAN ID:3     Type:Port based      Status:Up
  Learning:On             Tag-Translation:On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name:VLAN0003
  IP Address:10.215.196.1/23
             3ffe:501:811:ff08::5/64
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0003
  Spanning Tree:Single(802.1D)
  AXRP RING ID:       AXRP VLAN group:
  GSRP ID:       GSRP VLAN group:    L3:
  IGMP snooping:      MLD snooping:
  Untagged(8)   :1/0/5-12
  Tagged(2)     :1/0/25-26
  Tag-Trans(2)  :1/0/25-26
VLAN ID:120   Type:Protocol based  Status:Up
  Protocol VLAN Information  Name:ipv6
  EtherType:08dd  LLC:  Snap-EtherType:
```

```
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0120
  IP Address:
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0120
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Untagged(3)   :1/0/5,7,9
  Tagged(2)     :1/0/25-26
  Tag-Trans(2)  :1/0/25-26
VLAN ID:1340  Type:Mac based       Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN1340
  IP Address:10.215.202.1/24
  Source MAC address: 0012.e2de.053c(VLAN)
  Description:VLAN1340
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Untagged(6)   :1/0/13-18
  Tagged(2)     :1/0/25-26
  Tag-Trans(2)  :1/0/25-26
>
```

(2) VLAN の通信状態の確認

VLAN の通信状態は show vlan detail コマンドで確認できます。Port Information でポートの Up/Down，Forwarding/Blocking を確認してください。Blocking 状態の場合，括弧内に Blocking の要因が示されています。

図 24-13 show vlan detail コマンドの実行結果

```
> show vlan 3,1000-1500 detail
Date 20XX/01/26 17:01:40 UTC
VLAN counts:2
VLAN ID:3     Type:Port based      Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0003
  IP Address:10.215.196.1/23
             ee80::220:afff:fed7:8f0a/64
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0003
  Spanning Tree:Single(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Port Information
   1/0/5          Up   Forwarding      Untagged
   1/0/6          Up   Blocking(STP)   Untagged
   1/0/7          Up   Forwarding      Untagged
   1/0/8          Up   Forwarding      Untagged
   1/0/9          Up   Forwarding      Untagged
   1/0/10         Up   Forwarding      Untagged
   1/0/11         Up   Forwarding      Untagged
   1/0/12         Up   Forwarding      Untagged
   1/0/25(CH:9)   Up   Forwarding      Tagged   Tag-Translation:103
   1/0/26(CH:9)   Up   Blocking(CH)    Tagged   Tag-Translation:103
VLAN ID:1340  Type:Mac based       Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN1340
  IP Address:10.215.202.1/24
  Source MAC address: 0012.e2de.053c(VLAN)
  Description:VLAN1340
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
```

```
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Port Information
   1/0/13         Up   Forwarding      Untagged
   1/0/14         Up   Forwarding      Untagged
   1/0/15         Up   Forwarding      Untagged
   1/0/16         Up   Forwarding      Untagged
   1/0/17         Up   Forwarding      Untagged
   1/0/18         Up   Forwarding      Untagged
   1/0/25(CH:9)   Up   Forwarding      Tagged   Tag-Translation:104
   1/0/26(CH:9)   Up   Blocking(CH)    Tagged   Tag-Translation:104
>
```

(3) VLAN ID 一覧の確認

show vlan summary コマンドで，設定した VLAN の種類とその数，VLAN ID を確認できます。

図 24–14 show vlan summary コマンドの実行結果

```
> show vlan summary
Date 20XX/10/14 12:14:38 UTC
Total(4)            :1,10,20,4094
Port based(2)       :1,4094
Protocol based(1)   :10
MAC based(1)        :20
>
```

(4) VLAN のリスト表示による確認

show vlan list コマンドは VLAN の設定状態の概要を 1 行に表示します。本コマンドによって，VLAN の設定状態やレイヤ 2 冗長機能，IP アドレスの設定状態を一覧で確認できます。また，VLAN，ポートまたはチャネルグループをパラメータとして指定することで，指定したパラメータの VLAN の状態だけを一覧で確認できます。

図 24–15 show vlan list コマンドの実行結果

```
> show vlan list
Date 20XX/01/26 17:01:40 UTC
VLAN counts:4
ID   Status  Fwd/Up /Cfg Name             Type  Protocol       Ext.    IP
   1 Up       16/ 18/ 18 VLAN0001         Port  STP PVST+:1D   - - - - 4
   3 Up        9/ 10/ 10 VLAN0003         Port  STP Single:1D  - - T - 4/6
 120 Up        4/  5/  5 VLAN0120         Proto -              - - - - -
1340 Disable   0/  8/  8 VLAN1340         Mac   -              - - - - 4
     AXRP (Control-VLAN)
     GSRP GSRP ID:VLAN Group ID(Master/Backup)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured
>
```

(5) MAC VLAN の登録 MAC アドレスの確認

MAC VLAN に登録されている MAC アドレスを，show vlan mac-vlan コマンドで確認できます。

括弧内は MAC アドレスを登録した機能を示しています。

- 「static」はコンフィグレーションで登録した MAC アドレス
- 「dot1x」は IEEE802.1X で登録した MAC アドレス

図 24–16 show vlan mac-vlan コマンドの実行結果

```
> show vlan mac-vlan
Date 20XX/10/14 12:16:04 UTC
VLAN counts:2    Total MAC Counts:5
VLAN ID:20   MAC Counts:4
   0012.e200.0001 (static)    0012.e200.0002 (static)
   0012.e200.0003 (static)    0012.e200.0004 (dot1x)
VLAN ID:200  MAC Counts:1
```

```
    0012.e200.1111 (dot1x)
>
```

25 VLAN 拡張機能

この章では，VLAN に適用する拡張機能の解説と操作方法について説明します。

25.1　VLAN トンネリングの解説

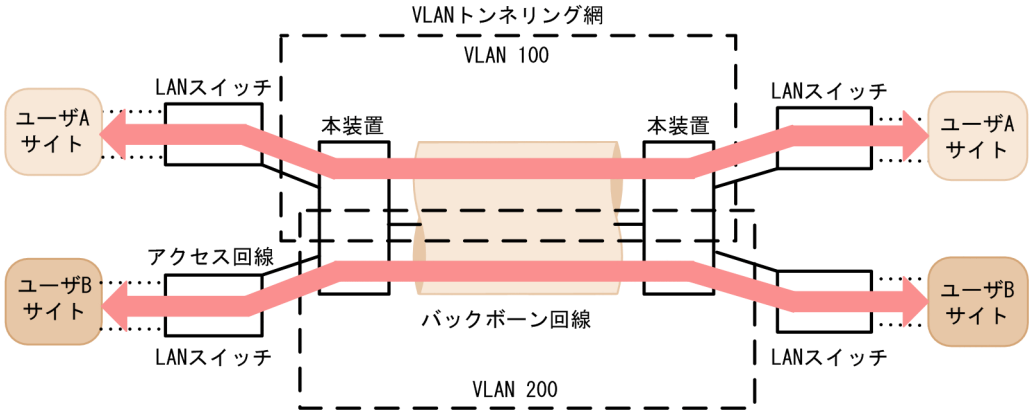
25.1.1　概要

VLAN トンネリング機能とは，複数ユーザの VLAN をほかの VLAN の中に集約して「トンネル」する機能です。IEEE802.1Q VLAN Tag をスタックすることで一つの VLAN 内にほかの VLAN に属するフレームをトランスペアレントに通すことができます。トンネルは 3 か所以上のサイトを接続するマルチポイント接続ができます。

VLAN トンネリング概要（広域イーサネットサービス適用例）を次の図に示します。VLAN トンネリングでは，VLAN Tag をスタックすることで VLAN トンネリング網内の VLAN を識別します。

この適用例は，レイヤ 2 VPN サービスである広域イーサネットサービスに適用する場合の例です。本装置に VLAN トンネリング機能を適用します。VLAN トンネリングでは，VLAN Tag をスタックすることで VLAN トンネリング網内の VLAN を識別します。ユーザサイトを収容するポートをアクセス回線，VLAN トンネリング網内に接続するポートをバックボーン回線と呼びます。アクセス回線からのフレームに VLAN Tag を追加してバックボーン回線に中継します。バックボーン回線からのフレームは VLAN Tag を外しアクセス回線へ中継します。

図 25–1　VLAN トンネリング概要（広域イーサネットサービス適用例）



25.1.2　VLAN トンネリングを使用するための必須条件

VLAN トンネリング機能を使用する場合は，次の条件に合わせてネットワークを構築する必要があります。

- ポート VLAN を使用します。
- VLAN トンネリング機能を実現する VLAN では，アクセス回線側はトンネリングポートとし，バックボーン回線側をトランクポートとします。
- VLAN トンネリング網内のバックボーン回線では VLAN Tag をスタックするため，通常より 4 バイト大きいサイズのフレームを扱える必要があります。
- 装置内で，アクセスポートとトンネリングポートは共存できません。一つでもトンネリングポートを設定すると，アクセスポートとして設定していたポートもトンネリングポートとして動作します。

25.1.3　VLAN トンネリング使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　デフォルト VLAN について

デフォルト VLAN の自動加入を行いません。すべての VLAN を明示的に設定してください。

(3)　トランクポートのネイティブ VLAN について

VLAN トンネリングのトランクポートは VLAN Tag をスタックするポートとなりますが，ネイティブ VLAN では VLAN Tag をスタックしません。本装置からフレームを送信するときはアクセスポートと同様に動作して，フレームを受信するときは Untagged フレームだけを扱います。ほかの VLAN と異なる動作となるので，VLAN トンネリング網のバックボーン回線の VLAN としては使用できません。VLAN トンネリングを使用する場合，トランクポートのネイティブ VLAN は suspend 状態とすることをお勧めします。

トランクポートのネイティブ VLAN は，コンフィグレーションコマンド switchport trunk native vlan で設定しない場合デフォルト VLAN です。デフォルト VLAN で VLAN トンネリング機能を使用する場合は，switchport trunk native vlan でネイティブ VLAN にデフォルト VLAN 以外の VLAN を設定してください。

(4)　フレームの User Priority について

VLAN トンネリングを使用する場合の User Priority については，「コンフィグレーションガイド Vol.2」「3.7　マーカー解説」を参照してください。

25.2　VLAN トンネリングのコンフィグレーション

25.2.1　コンフィグレーションコマンド一覧

VLAN トンネリングのコンフィグレーションコマンド一覧を次の表に示します。

表 25-1　コンフィグレーションコマンド一覧

コマンド名	説明
switchport access	アクセス回線をトンネリングポートで設定します。
switchport mode	アクセス回線，バックボーン回線を設定するためにポートの種類を設定します。
switchport trunk	バックボーン回線を設定します。
mtu※	バックボーン回線でジャンボフレームを設定します。

注※
「コンフィグレーションコマンドレファレンス Vol.1」「15　イーサネット」を参照してください。

25.2.2　VLAN トンネリングの設定

(1)　アクセス回線，バックボーン回線の設定

[設定のポイント]

VLAN トンネリング機能はポート VLAN を使用し，アクセス回線をトンネリングポート，バックボーン回線をトランクポートで設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   ポート 1/0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。
2. **(config-if)# switchport mode dot1q-tunnel**
   (config-if)# switchport access vlan 10
   ポート 1/0/1 をトンネリングポートに設定します。また，VLAN 10 を設定します。
   トランクポートのコンフィグレーションについては，「24.4　ポート VLAN のコンフィグレーション」を参照してください。

(2)　バックボーン回線のジャンボフレームの設定

[設定のポイント]

バックボーン回線は VLAN Tag をスタックするため通常より 4 バイト以上大きいサイズのフレームを扱います。そのため，ジャンボフレームを設定する必要があります。

[コマンドによる設定]

ジャンボフレームのコンフィグレーションについては，「20.3.7　ジャンボフレームの設定」を参照してください。

25.3　Tag 変換の解説

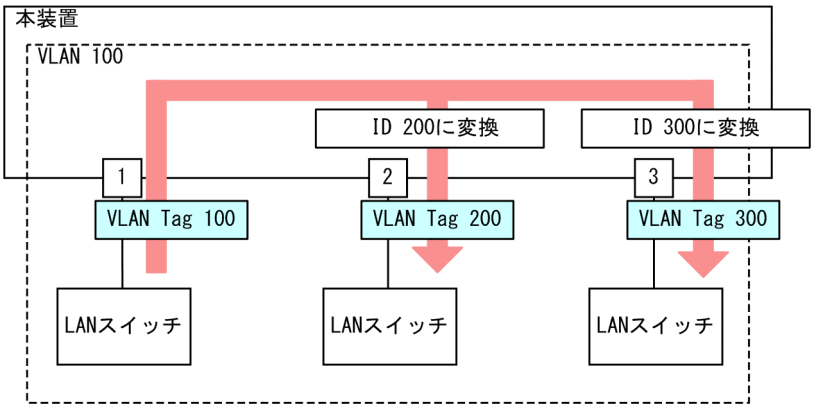
25.3.1　概要

Tag 変換は，Tagged フレームをレイヤ 2 スイッチ中継する際に，フレームの VLAN Tag の VLAN ID フィールドを別の値に変換する機能です。この機能によって，異なる VLAN ID で設定した既設の VLAN を一つの VLAN として接続できるようになります。

Tag 変換は，トランクポートで指定します。Tag 変換を使用しない場合は，VLAN Tag の VLAN ID フィールドにその VLAN の VLAN ID を使用します。Tag 変換を指定した場合はその ID を使用します。

Tag 変換の構成例を次の図に示します。図では，ポート 1 で Tag 変換が未指定であり，ポート 2 およびポート 3 にそれぞれ Tag 変換を設定し，VLAN Tag の VLAN ID フィールドを変換して中継します。また，フレームを受信する際にも，各ポートで設定した ID の VLAN Tag のフレームを VLAN 100 で扱います。

図 25-2　Tag 変換の構成例



25.3.2　Tag 変換使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

25.4　Tag 変換のコンフィグレーション

25.4.1　コンフィグレーションコマンド一覧

Tag 変換のコンフィグレーションコマンド一覧を次の表に示します。

表 25-2　コンフィグレーションコマンド一覧

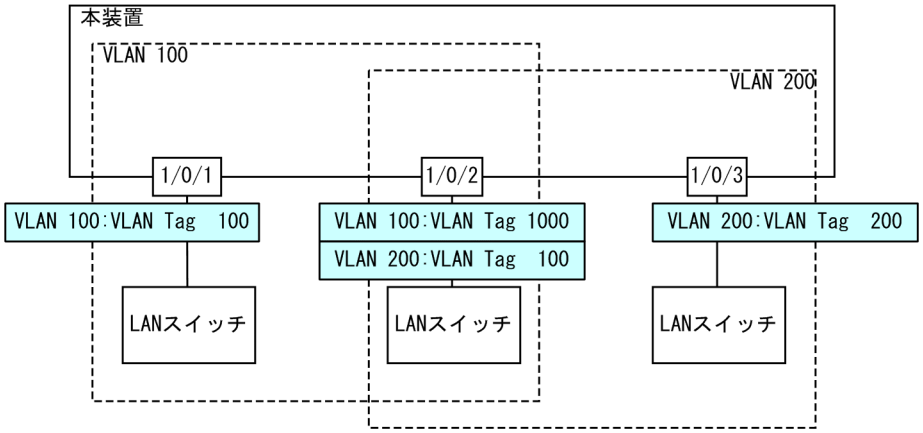
コマンド名	説明
switchport vlan mapping	変換する ID を設定します。
switchport vlan mapping enable	指定したポートで Tag 変換を有効にします。

25.4.2　Tag 変換の設定

Tag 変換を設定する手順を次の図に示します。ここでは，図に示す構成のポート 1/0/2 の設定例を示します。

構成例では，ポート 1/0/2 に Tag 変換を適用します。ポート 1/0/2 では，VLAN 100 のフレームの送受信は VLAN Tag 1000 で行い，VLAN 200 のフレームの送受信は VLAN Tag 100 で行います。このように，VLAN 100 で Tag 変換を行った場合，ほかの VLAN で VLAN Tag 100 を使用することもできます。また，ポート 1/0/2 では VLAN Tag 200 のフレームを VLAN 200 として扱わないで，未設定の VLAN Tag として廃棄します。

図 25-3　Tag 変換の設定例



[設定のポイント]

Tag 変換は，Tag 変換を有効にする設定と，変換する ID を設定することによって動作します。Tag 変換の設定はトランクポートだけ有効です。

Tag 変換は switchport vlan mapping コマンドで設定します。設定した変換を有効にするためには，switchport vlan mapping enable コマンドを設定します。Tag 変換を有効にすると，そのポートで変換を設定していない VLAN はフレームの送受信を停止します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/2**
   (config-if)# switchport mode trunk

(config-if)# switchport trunk allowed vlan 100,200

ポート 1/0/2 をトランクポートに設定して，VLAN 100，200 を設定します。

2. **(config-if)# switchport vlan mapping 1000 100**

   (config-if)# switchport vlan mapping 100 200

   ポート 1/0/2 で VLAN 100, 200 に Tag 変換を設定します。VLAN 100 では VLAN Tag 1000 でフレームを送受信して，VLAN 200 では VLAN Tag 100 でフレームを送受信するように設定します。

3. **(config-if)# switchport vlan mapping enable**

   ポート 1/0/2 で Tag 変換を有効にします。本コマンドを設定するまでは Tag 変換は動作しません。

[注意事項]

Tag 変換を使用するポートは，そのポートのすべての VLAN で Tag 変換の設定をする必要があります。変換しない VLAN の場合は，同じ値に変換する設定を行ってください。なお，Tag 変換の収容条件はコンフィグレーションの設定数で 768 で，同じ値に変換する設定も含まれます。

25.5　L2 プロトコルフレーム透過機能の解説

25.5.1　概要

この機能は，レイヤ 2 のプロトコルフレームを中継する機能です。中継するフレームにはスパニングツリーの BPDU，IEEE802.1X の EAPOL，LLDP フレーム，IEEE802.3ah/UDLD の OAMPDU があります。通常，これらレイヤ 2 のプロトコルフレームは中継しません。

中継するフレームは本装置では単なるマルチキャストフレームとして扱い，本装置のプロトコルには使用しません。

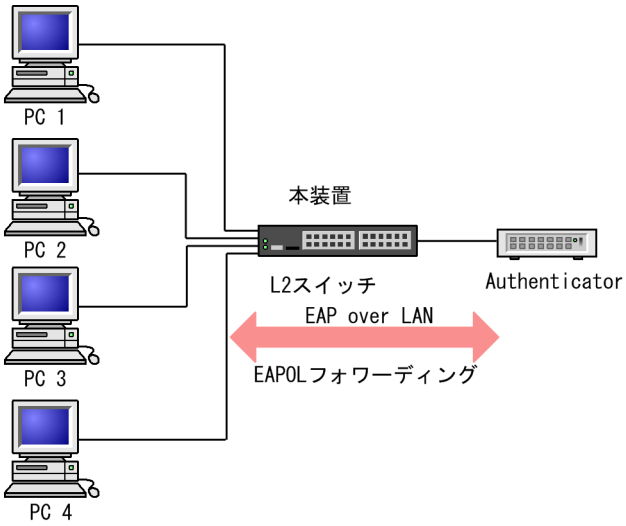
(1)　BPDU フォワーディング機能

本装置でスパニングツリーを使用しない場合に BPDU を中継できます。VLAN トンネリングでこの機能を使用すると，ユーザの BPDU を通過させることができます。その際，VLAN トンネリング網のすべてのエッジ装置，コア装置で BPDU フォワーディング機能を設定する必要があります。

(2)　EAPOL フォワーディング機能

本装置で IEEE802.1X を使用しない場合に EAPOL を中継できます。本装置を，Authenticator と端末（Supplicant）の間の L2 スイッチとして用いるときにこの機能を使用します。

図 25-4　EAPOL フォワーディング機能の適用例



(3)　LLDP フォワーディング機能

本装置で LLDP を使用しない場合に LLDP フレームを中継できます。

(4)　UDLD フォワーディング機能

本装置で UDLD を使用しない場合に OAMPDU を中継できます。

25.5.2　L2 プロトコルフレーム透過機能の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

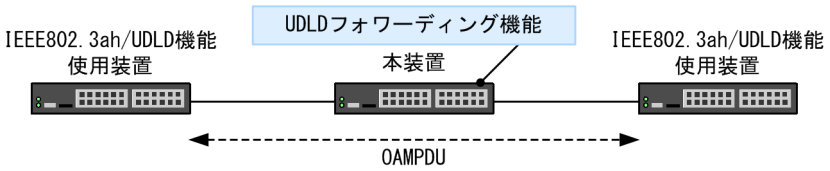
(2)　UDLD フォワーディング機能

IEEE802.3ah/UDLD 機能を使用する装置間に本装置を接続し，本装置で UDLD フォワーディング機能を使用する場合，OAMPDU をやり取りする双方の装置のポートが 1 対 1 の関係となる構成で運用してください。なお，IEEE802.3ah/UDLD 機能を使用する装置間でリンク状態の認識にずれが生じるため，片方向リンク障害を誤検知することがあります。

また，本装置で VXLAN 機能と UDLD フォワーディング機能を併用して VXLAN トンネルをフォワーディングさせる場合, VXLAN トンネルのネットワークの状況によって片方向リンク障害を誤検知することがあります。

接続構成例を次の図に示します。

図 25-5　IEEE802.3ah/UDLD 機能使用装置間で UDLD フォワーディング機能を使用する例



片方向リンク障害を誤検知する場合は，IEEE802.3ah/UDLD 機能を使用している装置について，コンフィグレーションコマンド efmoam udld-detection-count で片方向リンク障害と判断するための回数を調整してください。

また，IEEE802.3ah/UDLD 機能を使用する装置間に中継装置が接続された構成では，コンフィグレーションコマンド efmoam active で udld パラメータを設定した側の装置で片方向リンク障害を検出してポートが inactive 状態になっても，相手装置側のポートではリンクダウンを検出できません。双方の装置のポートをリンクダウンさせるには，双方の装置に efmoam active コマンドで udld パラメータを設定してください。

25.6　L2 プロトコルフレーム透過機能のコンフィグレーション

25.6.1　コンフィグレーションコマンド一覧

L2 プロトコルフレーム透過機能のコンフィグレーションコマンド一覧を次の表に示します。

表 25-3　コンフィグレーションコマンド一覧

コマンド名	説明
l2protocol-tunnel eap	IEEE802.1X の EAPOL を中継します。
l2protocol-tunnel lldp	LLDP フレームを中継します。
l2protocol-tunnel stp	スパニングツリーの BPDU を中継します。
l2protocol-tunnel udld	IEEE802.3ah/UDLD の OAMPDU を中継します。

25.6.2　L2 プロトコルフレーム透過機能の設定

(1)　BPDU フォワーディング機能の設定

[設定のポイント]

本機能の設定は装置単位で有効になります。設定すると，BPDU をすべての VLAN で中継します。

BPDU フォワーディング機能は，本装置のスパニングツリーを停止してから設定する必要があります。

[コマンドによる設定]

1. **(config)# spanning-tree disable**
   (config)# l2protocol-tunnel stp

   BPDU フォワーディング機能を設定します。事前にスパニングツリーを停止し，BPDU フォワーディング機能を設定します。本装置は BPDU をプロトコルフレームとして扱わないで中継します。

(2)　EAPOL フォワーディング機能の設定

[設定のポイント]

本機能の設定は装置単位で有効になります。設定すると，EAPOL をすべての VLAN で中継します。

EAPOL フォワーディング機能と IEEE802.1X は同時に使用することはできません。

[コマンドによる設定]

1. **(config)# l2protocol-tunnel eap**

   EAPOL フォワーディング機能を設定します。本装置は EAPOL をプロトコルフレームとして扱わないで中継します。

(3)　LLDP フォワーディング機能の設定

[設定のポイント]

本機能の設定は装置単位で有効になります。設定すると，LLDP フレームをすべての VLAN で中継します。

LLDP フォワーディング機能と LLDP は同時に使用できません。

[コマンドによる設定]

1. **(config)# l2protocol-tunnel lldp**
   LLDP フォワーディング機能を設定します。本装置は LLDP フレームをプロトコルフレームとして扱わないで中継します。

(4)　UDLD フォワーディング機能の設定

[設定のポイント]

本機能の設定は装置単位で有効になります。設定すると, OAMPDU をすべての VLAN で中継します。
UDLD フォワーディング機能と IEEE802.3ah/UDLD は同時に使用できません。

[コマンドによる設定]

1. **(config)# l2protocol-tunnel udld**
   UDLD フォワーディング機能を設定します。本装置は OAMPDU をプロトコルフレームとして扱わないで中継します。

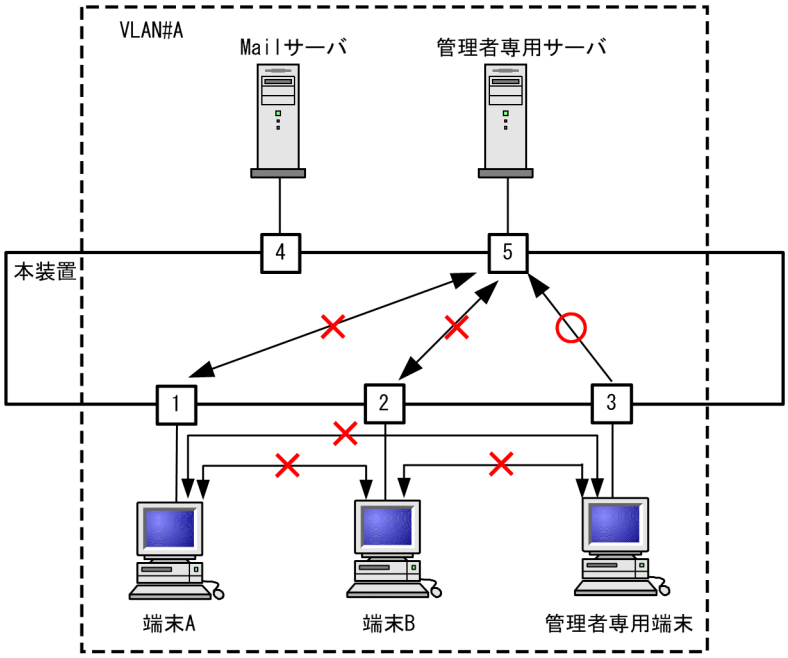
25.7　ポート間中継遮断機能の解説

25.7.1　概要

ポート間中継遮断機能は，指定したポートですべての通信を遮断する機能です。特定のポートからのアクセスだけを許可するサーバの接続や，直接の通信を遮断したい端末の接続などに適用することによってセキュリティを確保できます。

次の図に適用例を示します。この例では，管理者専用サーバは通常の端末からのアクセスを遮断して，管理者専用端末からだけアクセスできます。また，端末間は直接の通信を遮断し，各端末のセキュリティを確保します。

図 25-6　ポート間中継遮断機能の適用例



・管理者用サーバへは管理者専用端末からだけ通信を許可し，
　ほかの端末からの通信を遮断します
・端末間は直接の通信を遮断します
・Mailサーバはすべての端末から通信を可能とします

25.7.2　ポート間中継遮断機能使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　一つのポートに複数の VLAN を設定したポート間の遮断について

ポート間中継遮断機能は，VLAN 内のレイヤ 2 中継，VLAN 間のレイヤ 3 中継のどちらもすべての通信を遮断します。トランクポートなどで一つのポートに複数の VLAN を設定したポート間での通信を遮断した場合，そのポート間では VLAN 間のレイヤ 3 中継もできなくなります。

(3)　スパニングツリーを同時に使用するときの注意事項

通信を遮断したポートでスパニングツリーを運用するとトポロジーによって通信できなくなる場合があります。

(4)　ポート間中継遮断機能で遮断されないフレームについて

ポート間中継遮断機能は，ハードウェアで中継するフレームだけを遮断します。ソフトウェアで送信するフレーム（自発，IP オプション付きパケットなど）は遮断しません。

25.8　ポート間中継遮断機能のコンフィグレーション

25.8.1　コンフィグレーションコマンド一覧

ポート間中継遮断機能のコンフィグレーションコマンド一覧を次の表に示します。

表 25-4　コンフィグレーションコマンド一覧

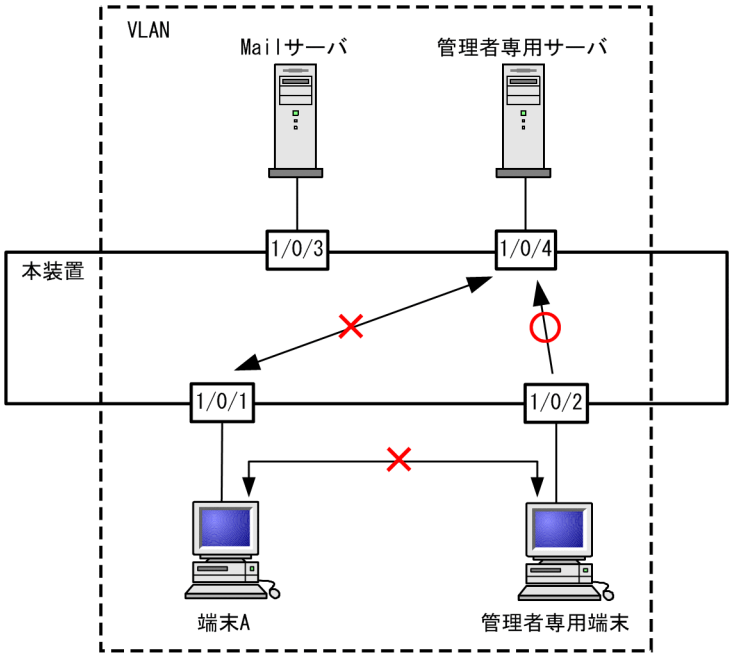
コマンド名	説明
switchport isolation	指定したポートへの中継を遮断します。

25.8.2　ポート間中継遮断機能の設定

ポート間中継遮断機能を設定する手順を次に示します。ここでは，図に示す構成の設定例を示します。

構成例では，ポート 1/0/1 からポート 1/0/4 への通信を遮断します。また，ポート 1/0/1，1/0/2 間の通信を遮断します。ポート 1/0/3 はどのポートとも通信が可能です。

図 25-7　ポート間中継遮断機能の設定例



・管理者用サーバへは管理者専用端末からだけ通信を許可し，
　ほかの端末からの通信を遮断します
・端末間は直接の通信を遮断します
・Mailサーバはすべての端末から通信を可能とします

[設定のポイント]

ポート間中継遮断機能は，イーサネットインタフェースコンフィグレーションモードで，そのポートからの通信を許可しないポートを指定することで設定します。通信を双方向で遮断するためには，遮断したい各ポートで設定する必要があります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   ポート 1/0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。
2. **(config-if)# switchport isolation interface gigabitethernet 1/0/2, gigabitethernet 1/0/4**
   (config-if)# exit
   ポート 1/0/1 でポート 1/0/2，1/0/4 からの中継を遮断します。この設定で，ポート 1/0/1 から発信する片方向の中継を遮断します。
3. **(config)# interface gigabitethernet 1/0/2**
   (config-if)# switchport isolation interface gigabitethernet 1/0/1
   (config-if)# exit
   ポート 1/0/2 のイーサネットインタフェースコンフィグレーションモードに移行し，ポート 1/0/2 でポート 1/0/1 からの中継を遮断します。この設定によって，ポート 1/0/1，1/0/2 間は双方向で通信を遮断します。
4. **(config)# interface gigabitethernet 1/0/4**
   (config-if)# switchport isolation interface gigabitethernet 1/0/1
   ポート 1/0/4 のイーサネットインタフェースコンフィグレーションモードに移行し，ポート 1/0/4 でポート 1/0/1 からの中継を遮断します。この設定によって，ポート 1/0/1，1/0/4 間は双方向で通信を遮断します。

25.8.3　遮断するポートの変更

[設定のポイント]

switchport isolation add コマンドおよび switchport isolation remove コマンドでポート間中継遮断機能で遮断するポートを変更します。すでに設定したポートで switchport isolation <interface id list>によって一括して指定した場合，指定した設定に置き換わります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# switchport isolation interface gigabitethernet 1/0/2-10
   ポート 1/0/1 のイーサネットインタフェースコンフィグレーションモードに移行し，ポート 1/0/1 からポート 1/0/2～1/0/10 への中継を遮断します。
2. **(config-if)# switchport isolation interface add gigabitethernet 1/0/11**
   (config-if)# switchport isolation interface remove gigabitethernet 1/0/5
   ポート 1/0/1 からの遮断にポート 1/0/11 を追加します。また，ポート 1/0/5 の設定を解除します。この状態で，ポート 1/0/1 はポート 1/0/2～1/0/4，1/0/6～1/0/11 への通信を遮断します。
3. **(config-if)# switchport isolation interface gigabitethernet 1/0/3-4**
   ポート 1/0/1 からの中継を遮断するポートを 1/0/3～1/0/4 に設定します。以前の設定はすべて上書きされ，ポート 1/0/3～1/0/4 だけ遮断しそのほかのポートは通信を可能とします。

25.9　VLAN debounce 機能の解説

25.9.1　概要

VLAN インタフェースは VLAN が通信可能な状態になったときにアップし，VLAN のポートがダウンした場合や，スパニングツリーなどの機能でブロッキング状態になり通信できなくなった場合にダウンします。

VLAN debounce 機能は，VLAN インタフェースのアップやダウンを遅延させて，ネットワークトポロジーの変更や，運用メッセージ，SNMP 通知などを削減する機能です。

スパニングツリーや Ring Protocol などレイヤ 2 での冗長構成を使用したときに障害が発生した場合，通常レイヤ 3 のトポロジー変更と比べて短い時間で代替経路へ切り替わります。VLAN debounce 機能によってレイヤ 2 での代替経路への切替時間まで VLAN インタフェースのダウンを遅延させると，レイヤ 3 のトポロジーを変化させずにすみ，通信の可用性を確保できます。

レイヤ 3 での冗長構成を使用する場合，マスター側に障害が発生したあとの回復時に，両系がマスターとして動作することを防ぐために VLAN インタフェースのアップを遅延させたいとき, VLAN debounce 機能で VLAN インタフェースのアップを遅延できます。

25.9.2　VLAN debounce 機能と他機能との関係

(1)　スパニングツリー

スパニングツリーでは，ポートに障害が発生して代替経路へ変更されるまでに，スパニングツリーのトポロジーの変更に必要な時間が掛かります。この間に VLAN インタフェースをダウンさせたくない場合は，VLAN インタフェースのダウン遅延時間をトポロジーの変更に必要な時間以上に設定してください。

(2)　Ring Protocol

Ring Protocol を使用する場合，マスタノードではプライマリポートがフォワーディング，セカンダリポートがブロッキングとなっています。VLAN debounce 機能を使わない場合，プライマリポートで障害が発生するといったん VLAN インタフェースがダウンし，セカンダリポートのブロッキングが解除されると再び VLAN インタフェースがアップします。

このようなときに VLAN がいったんダウンすることを防ぐためには，VLAN インタフェースのダウン遅延時間を設定してください。なお，ダウン遅延時間は health-check holdtime コマンドで設定する保護時間以上に設定してください。

(3)　その他の冗長化機能

スパニングツリーや Ring Protocol 以外の冗長化を使用する場合でも，VLAN が短時間にアップやダウンを繰り返すときには，VLAN debounce 機能を使用するとアップやダウンを抑止できます。

25.9.3　VLAN debounce 機能使用時の注意事項

(1)　ダウン遅延時間の注意事項

ダウン遅延時間を設定すると，回復しない障害が発生した場合でも VLAN のダウンが遅延します。VLAN debounce 機能でダウンが遅延している間は，通信できない状態です。ダウン遅延時間は，ネットワークの構成や運用に応じて必要な値を設定してください。

VLAN に status コマンドで suspend を設定した場合や VLAN のポートをすべて削除した場合など，コンフィグレーションを変更しないとその VLAN が通信可能とならない場合には，ダウン遅延時間を設定していても VLAN のダウンは遅延しません。

(2)　アップ遅延時間の注意事項

アップ遅延時間を設定すると，いったんアップした VLAN がダウンしたあと，再度アップするときにアップが遅延します。装置を再起動したり，restart vlan コマンドで VLAN プログラムを再起動したりすると，VLAN は初期状態になるため，アップ遅延時間を設定していても VLAN のアップは遅延しません。

(3)　遅延時間の誤差に関する注意事項

アップまたはダウン遅延時間は，ソフトウェアのタイマを使用しているため，CPU 利用率が高い場合には設定した時間より大きくなることがあります。

25.10　VLAN debounce 機能のコンフィグレーション

25.10.1　コンフィグレーションコマンド一覧

VLAN debounce 機能のコンフィグレーションコマンド一覧を次の表に示します。

表 25-5　コンフィグレーションコマンド一覧

コマンド名	説明
down-debounce	VLAN インタフェースのダウン遅延時間を指定します。
up-debounce	VLAN インタフェースのアップ遅延時間を指定します。

25.10.2　VLAN debounce 機能の設定

VLAN debounce 機能を設定する手順を次に示します。

[設定のポイント]

VLAN debounce 機能の遅延時間は，ネットワーク構成および運用に合わせて最適な値を設定します。

[コマンドによる設定]

1. **(config)# interface vlan 100**
   VLAN 100 の VLAN インタフェースモードに移行します。
2. **(config-if)# down-debounce 2**
   (config-if)# exit
   VLAN 100 のダウン遅延時間を 2 秒に設定します。
3. **(config)# interface range vlan 201-300**
   VLAN 201-300 の複数 VLAN インタフェースモードに移行します。
4. **(config-if-range)# down-debounce 3**
   (config-if-range)# exit
   VLAN 201-300 のダウン遅延時間を 3 秒に設定します。

25.11　レイヤ 2 中継遮断機能の解説

25.11.1　概要

レイヤ 2 中継遮断機能は，本装置内でレイヤ 2 中継をしないで，レイヤ 3 中継だけをする機能です。本機能を使用すると，VLAN 内でブロードキャストフレームやマルチキャストフレームを含むすべてのフレームをレイヤ 2 中継しません。

本機能は，ホテルやマンションなどで端末間の通信を遮断したい場合に利用できます。また，本機能を設定して，複数の端末を一つの VLAN に収容することで，IP アドレスも有効に活用できます。

25.12　レイヤ 2 中継遮断機能のコンフィグレーション

25.12.1　コンフィグレーションコマンド一覧

レイヤ 2 中継遮断機能のコンフィグレーションコマンド一覧を次の表に示します。

表 25-6　コンフィグレーションコマンド一覧

コマンド名	説明
l2-isolation	VLAN 内のレイヤ 2 中継を遮断します。

25.12.2　レイヤ 2 中継遮断機能の設定

レイヤ 2 中継遮断機能を設定する手順を次に示します。

[コマンドによる設定]

1. **(config)# l2-isolation**
   レイヤ 2 中継遮断機能を設定します。

25.13　VLAN 拡張機能のオペレーション

25.13.1　運用コマンド一覧

VLAN 拡張機能の運用コマンド一覧を次の表に示します。

表 25-7　運用コマンド一覧

コマンド名	説明
show vlan	VLAN 拡張機能の設定状態を確認します。

25.13.2　VLAN 拡張機能の確認

(1)　VLAN の通信状態の確認

VLAN 拡張機能の設定状態を show vlan detail コマンドで確認できます。show vlan detail コマンドによる VLAN 拡張機能の確認方法を次の表に示します。

表 25-8　show vlan detail コマンドによる VLAN 拡張機能の確認方法

機能	確認方法
VLAN トンネリング	先頭に”VLAN tunneling enabled”を表示します。
Tag 変換	Port Information で”Tag-Translation”を表示します。
L2 プロトコルフレーム透過機能	BPDU Forwarding，EAPOL Forwarding の欄に表示します。

図 25-8　show vlan detail コマンドの実行結果

```
>show vlan 10 detail
Date 20XX/10/15 16:28:23 UTC
VLAN counts:1   VLAN tunneling enabled                                    …1
VLAN ID:10    Type:Port based      Status:Up
  Learning:On             Tag-Translation:On
  BPDU Forwarding:On      EAPOL Forwarding:                               …3
                 .
                 .
                 .
                 .
  Port Information
   1/0/5          Up   Forwarding      Tagged   Tag-Translation:1000     …2
   1/0/6          Down -               Tagged   Tag-Translation:2000     …2
   1/0/7          Up   Forwarding      Tagged
>
```

1. VLAN トンネリングが有効であることを示します。
2. このポートに Tag 変換が設定されていることを示します。
3. BPDU フォワーディング機能が設定され，EAPOL フォワーディング機能が設定されていないことを示します。

26 VXLAN

VXLAN は，レイヤ 2 のフレームをカプセル化して，レイヤ 3 ネットワーク上で仮想的なレイヤ 2 ネットワークを実現します。この章では，VXLAN の解説と操作方法について説明します。

【SL-L3A】

26.1　解説

26.1.1　概要

VXLAN はレイヤ 2 のイーサネットフレームをカプセル化して，レイヤ 3 の IP ネットワーク上に論理的なレイヤ 2 ネットワーク（ネットワーク仮想化）を実現するプロトコルです。VXLAN を使用したネットワーク構成では，次に示す特長があります。

- レイヤ 3 ネットワーク越え（マルチキャリア）

  WAN には従来のキャリアサービス（IP-VPN，広域イーサネット，インターネットなど）を利用できます。

- 多拠点対応（マルチポイント）

  フラットなレイヤ 2 ネットワークを構築できるため，データセンター（クラウド）と拠点のネットワークを共通で管理できます。

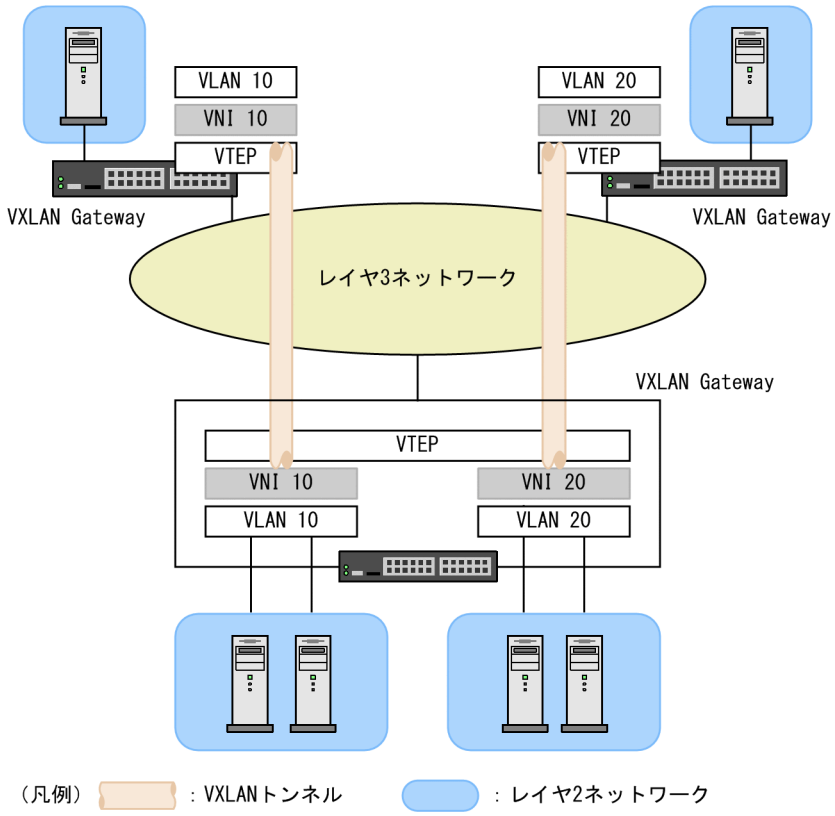
- 論理分割（マルチテナント）

  VXLAN 識別子（VNI）を VLAN，およびサブインタフェースに割り当てることで，従来の VLAN 数（4094）を超えて論理的に分割できます。

  サブインタフェースとは，イーサネットサブインタフェースとポートチャネルサブインタフェースの総称です。

VXLAN を使用したネットワーク構成例を次の図に示します。

図 26-1　VXLAN を使用したネットワーク構成例



26.1.2　VXLAN の基本動作

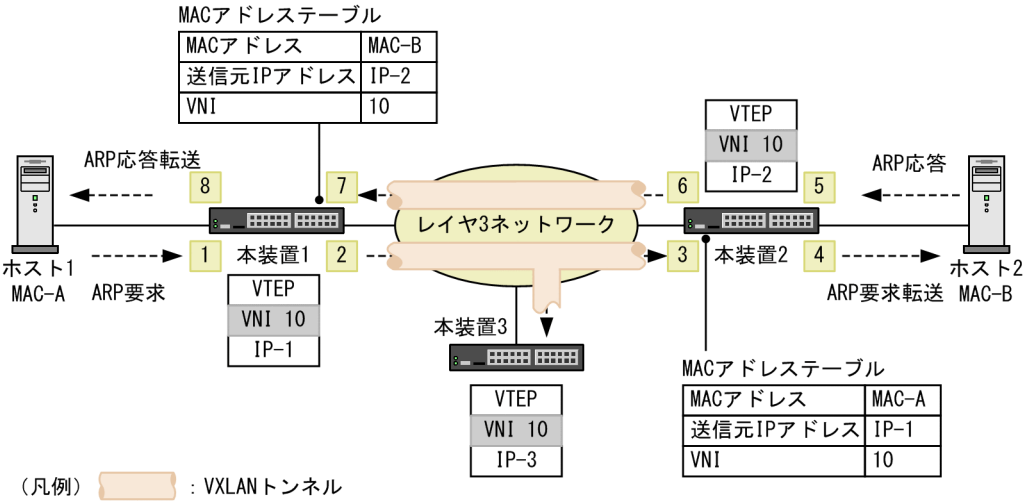
本装置では，VXLAN フレーム受信時に，装置に設定された VTEP で次の情報を学習します。

- 送信元 MAC アドレス
- 送信元 IP アドレス
- 送信元 VNI

その後，学習した情報に基づいてレイヤ 2 フレームを転送することで，レイヤ 3 ネットワーク経由の転送帯域を抑えます。

ARP 要求フレームと ARP 応答フレームの転送を例とした，VXLAN の基本動作を次の図に示します。この図の本装置 1，本装置 2，および本装置 3 には，同一 VNI ID の VXLAN トンネルが設定されているものとします。

図 26-2　VXLAN の基本動作



1. ホスト 1 から ARP 要求（ブロードキャストフレーム）を受信します。
2. 本装置 1 は受信した ARP 要求をカプセル化（VNI 付加）します。VXLAN トンネルを使用して，同一 VNI 内の本装置 2 および本装置 3 へユニキャストで転送します。
3. 本装置 2 は，受信した VXLAN フレームから学習した結果を MAC アドレステーブルに登録します。
4. 本装置 2 は VXLAN フレームをデカプセル化（VNI 削除）して，ARP 要求フレームをホスト 2 へ転送します。
5. ホスト 2 から ARP 応答を受信します。
6. 本装置 2 は受信した ARP 応答をカプセル化（VNI 付加）します。宛先は学習済みのため，VXLAN トンネルを使用して本装置 1 へユニキャストで転送します。
7. 本装置 1 は，受信した VXLAN フレームから学習した結果を MAC アドレステーブルに登録します。
8. 本装置 1 は VXLAN フレームをデカプセル化（VNI 削除）して，ARP 応答フレームをホスト 1 へ転送します。

26.1.3 VXLAN カプセル化

VXLAN トンネルでは，イーサネット，IP，UDP，および VXLAN で構成する最大 54 バイトのヘッダ情報を，VXLAN Access ポートで受信したフレームに付与してカプセル化します。

VXLAN カプセル化するときに付与する UDP ヘッダの宛先 UDP ポート番号は固定です。また，送信元 UDP ポート番号は，フレーム受信時の情報を使用した Hash 計算によって決定します。Hash 計算に使用する情報は，VXLAN Access ポートで受信したフレーム種別によって異なります。フレーム種別ごとの Hash 計算に使用する情報を次に示します。

IP パケットの場合

- 受信 VLAN ID
- 宛先 IP アドレス
- 送信元 IP アドレス
- 宛先 TCP/UDP ポート番号
- 送信元 TCP/UDP ポート番号
- 受信ポート番号または受信チャネルグループ番号

非 IP パケットの場合

- 宛先 MAC アドレス
- 送信元 MAC アドレス
- 受信 VLAN ID
- イーサネットタイプ
- 受信ポート番号または受信チャネルグループ番号

VXLAN トンネルの通信経路がリンクアグリゲーションおよびロードバランスで冗長化されている場合，VXLAN カプセル化したあとのフレーム情報で送信先を振り分けます。

リンクアグリゲーションでの振り分けについては，レイヤ 2 中継に該当します。詳細は，「21.1.5　フレーム送信時のポート振り分け」を参照してください。

ロードバランスでの振り分けについては，「コンフィグレーションガイド Vol.3」「8.4.2　ロードバランス仕様」を参照してください。

26.1.4 VXLAN のパケット長

VXLAN トンネルでカプセル化すると，最大 54byte のヘッダを付けます。この結果，VXLAN カプセル化したパケットのサイズが VXLAN Network ポート側の MTU より大きい場合，または VXLAN のカプセル化対象パケットのサイズが VXLAN PMTU 機能による MTU 設定より大きい場合に，MTU オーバとして該当するフレームをフラグメントしないで廃棄します。また，VXLAN カプセル化したパケットがレイヤ 3 ネットワーク内でフラグメントされた場合，正しく動作しません。

MTU オーバやフラグメントを発生させないために，次に示すどれかの設定が必要です。

- VXLAN Network ポート側のポート MTU を，VXLAN Access ポート側のポート MTU に 54byte を加えた値以上に設定して運用してください。
- VXLAN PMTU 機能を使用すると，VXLAN Network ポート側の MTU 設定を不要にできます。詳細は，「26.1.12　VXLAN PMTU 機能」を参照してください。

- 送信元の MTU サイズを，VXLAN の MTU オーバが発生しない値に設定してください。
- TCP 通信の場合は，通信パス上のルータなどによって TCP ヘッダに含まれる MSS（Maximum Segment Size）オプションの値を書き換えることで，パケットサイズを短くしてください。

26.1.5　サポート機能

VXLAN の各機能とサポート有無を次の表に示します。

表 26-1　VXLAN の各機能とサポート有無

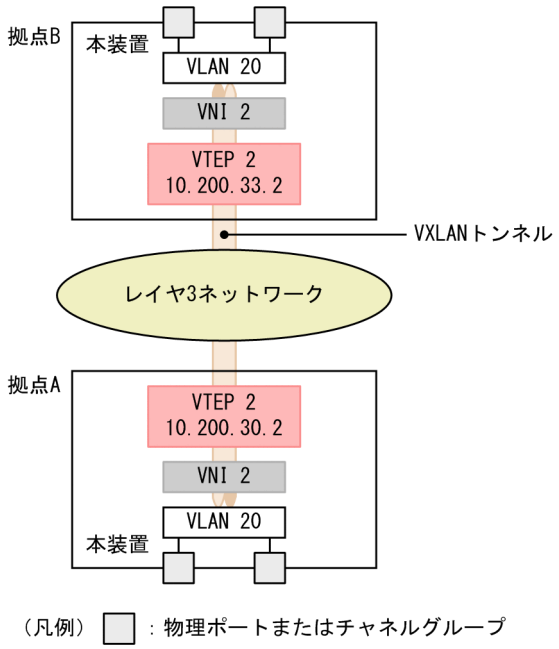
機能				サポート有無	備考
スイッチング（VXLAN フレームの中継）				○	－
VXLAN のトンネルモード	ユニキャストだけ			○	－
	ユニキャスト＋マルチキャスト			×	－
VXLAN のトンネルインタフェース	VTEP			○	255／装置
	送信元 IP アドレス	ループバック		○	IPv4 アドレス
		VLAN インタフェース		×	－
	宛先			○	256／装置
VNI マッピング	VNI マッピング方式	VLAN マッピング	VLAN Tag あり	○	－
			VLAN Tag なし	○	
		サブインタフェースマッピング	VLAN Tag あり	○	サブインタフェースは VXLAN 機能専用
			VLAN Tag なし	○	
VLAN Tag 付与	VLAN Tag 削除			○	－
	VLAN Tag 付加			×	802.1Q の Tagged フレームの VLAN Tag は引き継がれない
MAC アドレス学習	スタティック学習			×	送信元 MAC，VNI，トンネルインタフェース（送信元）
	ダイナミック学習			○	
VXLAN PMTU 機能				○	－

（凡例）○：サポート　×：未サポート　－：なし

26.1.6　VTEP

VTEP は VXLAN トンネルの終端ポイントです。カプセル化された VXLAN フレームは，VTEP 間で送受信されます。VTEP の位置づけを次の図に示します。

図 26-3　VTEP の位置づけ



本装置の VTEP 動作仕様を次の表に示します。

表 26-2　VTEP の動作仕様

項目	仕様
一つの VTEP への複数 VNI 登録	登録できます。
装置内での複数 VTEP 指定	指定できます。
VXLAN トンネルの宛先複数指定	指定できます。
VXLAN トンネルの IP アドレス	ループバックインタフェースの IPv4 アドレスを指定します。

26.1.7　VNI マッピング方式

VNI マッピング方式には，VLAN マッピングとサブインタフェースマッピングの 2 種類があります。

(1)　VLAN マッピング

VLAN に対して VNI を割り当てます。設定できる VNI 数は，VLAN の最大数（4094）までです。なお，コンフィグレーションコマンド vxlan vlan-mapping mode を設定すると，VLAN マッピングで動作できる VLAN ポート数の収容条件を拡張できます。

同一ポートに VNI を割り当てた VLAN と VNI を割り当てない VLAN を設定する場合の共存可否について，次の表に示します。

表 26-3　同一ポート内での VNI を割り当てた VLAN と VNI を割り当てない VLAN の共存可否

項目	レイヤ 2 機能用 VLAN との共存可否
収容条件を拡張しない場合	共存可※

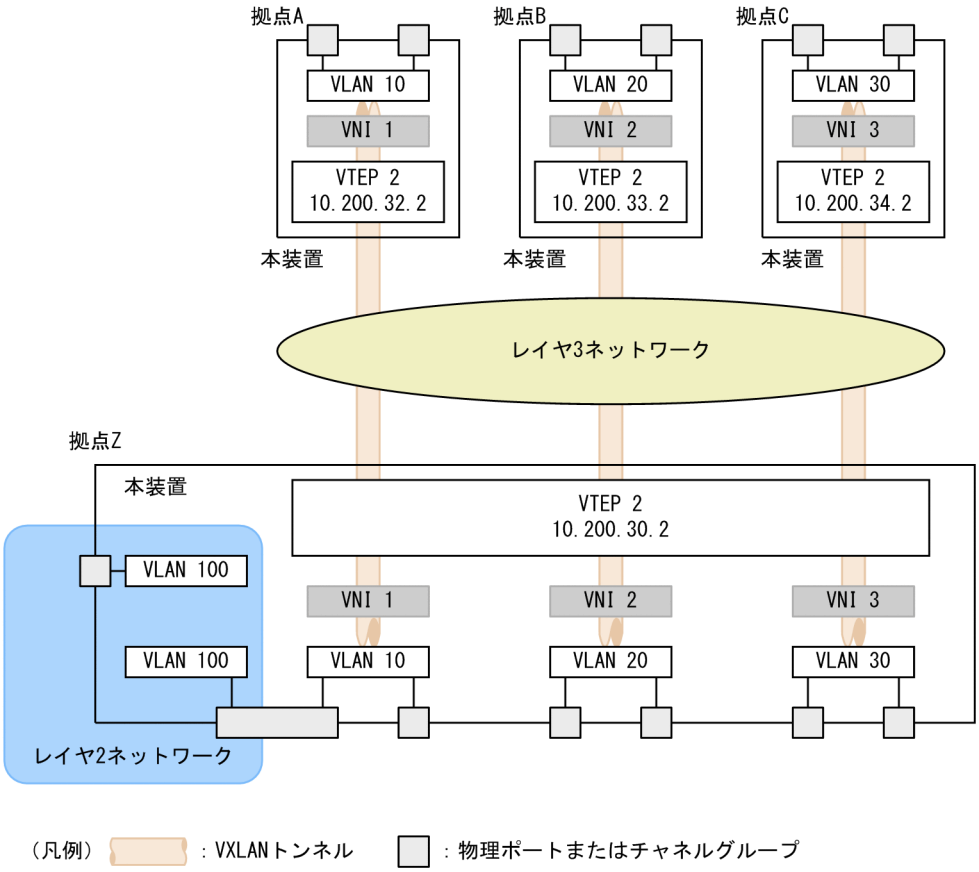
項目	レイヤ 2 機能用 VLAN との共存可否
収容条件を拡張する場合	共存不可

注※

VNI を割り当てない VLAN で使用できる機能は，VNI を割り当てた VLAN で使用できる機能と同じです。詳細は「表 22-5　VXLAN Access ポートおよび VXLAN Network ポートでの他機能の動作可否」を参照してください。また，VNI を割り当てた VLAN をネイティブ VLAN に指定した場合は，共存不可となります。

VLAN マッピングの例を次の図に示します。

図 26-4　VLAN マッピングの例



この図で示す各拠点間は，VTEP に割り当てた VNI ID で接続します。接続する拠点間では，同じ VNI ID を設定してください。

- 拠点 A と拠点 Z：VNI 1
- 拠点 B と拠点 Z：VNI 2
- 拠点 C と拠点 Z：VNI 3

なお，VNI に所属する VLAN ID として，接続先の拠点とは異なる VLAN ID も設定できます。

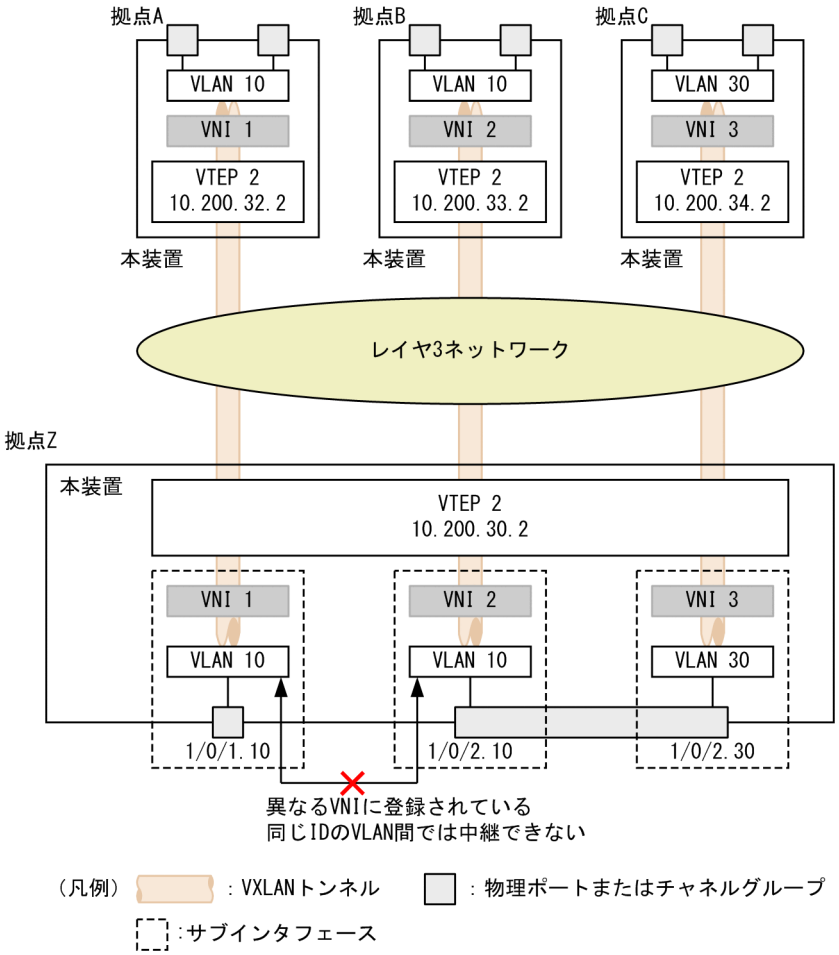
(2)　サブインタフェースマッピング

物理ポートまたはチャネルグループのサブインタフェースごとに VNI を割り当てます。

サブインタフェースは，イーサネットまたはポートチャネルと，VLAN Tag（VLAN ID）の組み合わせで，論理的なインタフェースを構築する機能です。このため，サブインタフェースを識別するための VLAN ID が同一でも元となるイーサネットまたはポートチャネルが異なる場合は，異なるインタフェースとして認識でき，同一 VLAN ID に対して異なる VNI を割り当てられます。なお，サブインタフェースマッピングでは，レイヤ 2 機能用の VLAN は共存できません。

サブインタフェースマッピングの例を次の図に示します。

図 26-5　サブインタフェースマッピングの例



この図で示す各拠点間は，VTEP に割り当てた VNI ID で接続します。接続する拠点間では，同じ VNI ID を設定してください。

- 拠点 A と拠点 Z：VNI 1
- 拠点 B と拠点 Z：VNI 2
- 拠点 C と拠点 Z：VNI 3

(3)　VNI マッピング方式の注意事項

- 同一インタフェース（物理ポートまたはチャネルグループ）内で，VLAN マッピングとサブインタフェースマッピングは混在できません。
- VLAN マッピングとサブインタフェースマッピングで，同じ VNI にできません。異なる VNI にすることで，一つの装置内で VLAN マッピングとサブインタフェースマッピングは混在できます。

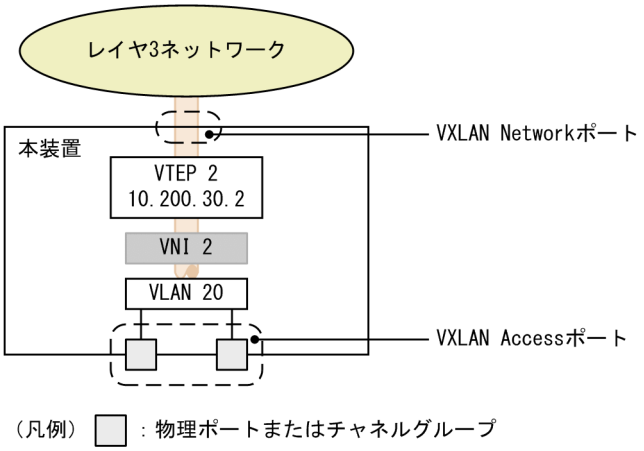
26.1.8　VXLAN Access ポートと VXLAN Network ポート

VXLAN Access ポートは，ユーザネットワーク側のポートです。

VXLAN Network ポートは，レイヤ 3 ネットワーク側のポートです。VXLAN 機能で対応できるレイヤ 3 ネットワークは，IPv4 ネットワークだけです。

VXLAN Access ポートと VXLAN Network ポートを次の図に示します。

図 26-6　VXLAN Access ポートと VXLAN Network ポート



26.1.9　MAC アドレステーブル

(1)　MAC アドレスの学習

VXLAN 機能が有効な場合，MAC アドレステーブル情報に VNI が追加されます。VXLAN 機能有効時の MAC アドレス学習については，「23.1.1　送信元 MAC アドレス学習」を参照してください。

(2)　MAC アドレステーブルのクリア

VXLAN 機能が有効な場合，VNI 単位で学習したエントリもクリアされます。クリアする契機については，「23.1.7　MAC アドレステーブルのクリア」を参照してください。

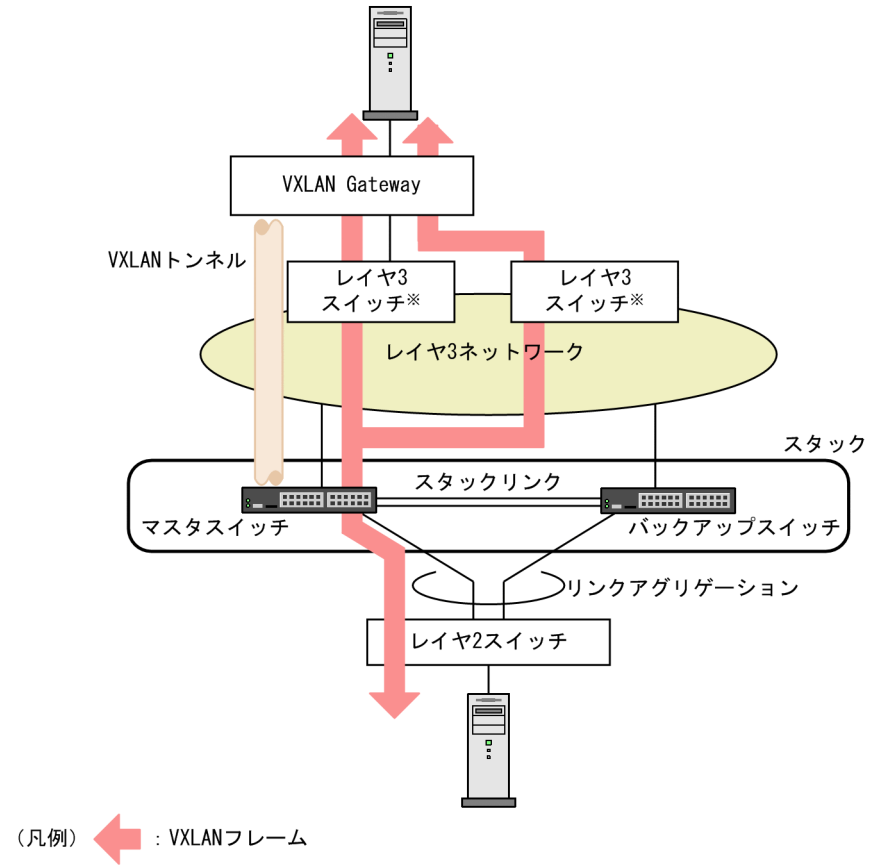
(3)　MAC アドレステーブルの学習抑止

VXLAN 機能が有効な場合，VNI 単位で MAC アドレステーブルの学習を抑止できます。VNI 単位の MAC アドレス学習抑止については，「23.1.6　MAC アドレス学習抑止」を参照してください。

26.1.10　スタック構成での動作

VXLAN 機能はスタック構成にも対応しています。スタック構成での VXLAN 使用例を次の図に示します。

図 26-7　スタック構成での VXLAN 使用例



注※　レイヤ 3 スイッチはイコールコストマルチパス

スタック構成で VXLAN を使用する場合は，VXLAN Access ポート側をリンクアグリゲーションで接続します。VXLAN Network ポート側ではイコールコストマルチパス機能を利用します。

26.1.11　カプセル化およびデカプセル化時の優先度引き継ぎ

VXLAN でフレームをカプセル化およびデカプセル化するとき，フレームに含まれる優先度を引き継ぎます。

カプセル化するときは，VXLAN Access ポートで受信したフレームの VLAN Tag のユーザ優先度を，VXLAN Network ポートから送信するフレームの IP ヘッダの TOS フィールドの上位 3bit へ引き継ぎます。L2 プロトコルフレーム透過機能を使用して，L2 プロトコルフレームが VXLAN トンネルを透過するときは，VXLAN Network ポートから送信するフレームの IP ヘッダ内 TOS フィールドの値は次の表に示す値となります。

表 26-4　L2 プロトコルフレーム透過機能使用時の TOS フィールドの値

項目	TOS フィールドの値
BPDU フォワーディング機能	7
EAPOL フォワーディング機能	5
LLDP フォワーディング機能	5

項目	TOS フィールドの値
UDLD フォワーディング機能	7

なお，次に示す構成でフロー制御による優先度決定が動作するときは，決定した CoS 値が優先度として設定されます。

- スタンドアロン構成でコンフィグレーションコマンド flow action-change cos を設定したとき
- スタック構成のとき

デカプセル化するときは，VXLAN Network ポートで受信した VXLAN パケットの IP ヘッダの TOS フィールドの上位 3bit を，VXLAN Access ポートから送信するフレームの VLAN Tag のユーザ優先度へ引き継ぎます。

26.1.12　VXLAN PMTU 機能

VXLAN PMTU 機能は，コンフィグレーションコマンド vxlan pmtu で指定した PMTU を閾値として，機能を有効にしたポートで受信したパケットのサイズがそれを超える場合に，Path MTU Discovery 相当に動作して，送信元に対して閾値以下のパケットサイズでの再送を要求する機能です。

VXLAN PMTU 機能を適用すると，送信元が Path MTU Discovery に対応している場合，接続先ネットワークでの MTU 長の変更が不要になります。VXLAN PMTU 機能適用前と適用後の動作を次の図に示します。

図 26-8　VXLAN PMTU 機能適用前の動作

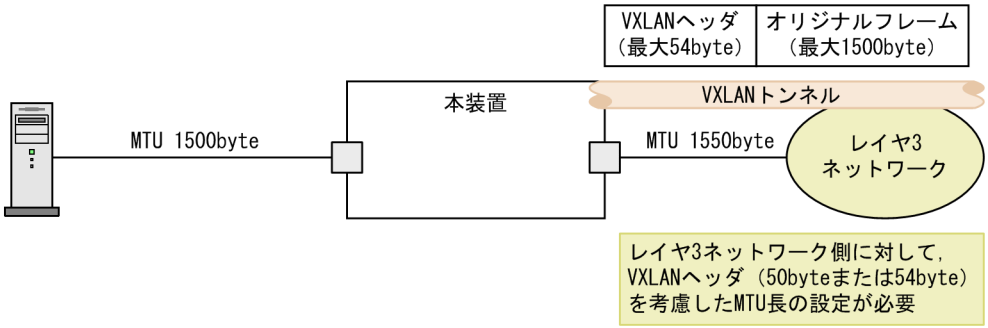
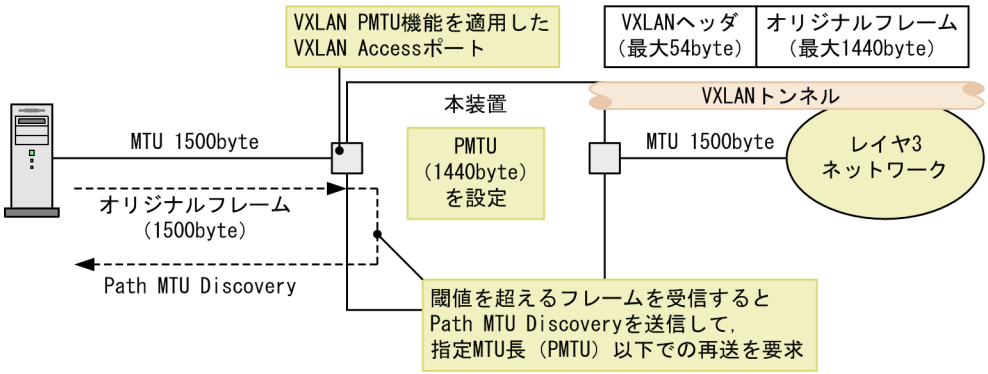


図 26-9　VXLAN PMTU 機能適用後の動作



26.1.13 VXLAN 使用時の注意事項

(1) 他機能との共存

「22.3 レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2) VXLAN フレームの送信

VXLAN Network ポートで VXLAN フレームを送信するためには，ネクストホップのアドレス解決が完了している必要があります。VXLAN フレーム送信時にネクストホップのアドレス解決が完了していない場合，該当 VXLAN フレームは廃棄されます。また，ネクストホップアドレスは動的に解決しません。

そのため，スタティック ARP を設定したり，スタティック経路の動的監視機能を使用したりして，ネクストホップアドレスが動的に解決されるように設定してください。

(3) リモート VTEP の IP アドレス

リモート側の VTEP の IP アドレス（本装置で設定する宛先アドレス）は，ホストアドレスである必要があります。

(4) サブインタフェースの VLAN 指定時のフィルタ

サブインタフェースに対するコンフィグレーションコマンド encapsulation dot1q で指定した VLAN ID と同じ VLAN インタフェースに対してフィルタを設定している場合，該当する VLAN インタフェースのフィルタで，サブインタフェースで受信したフレームを検出します。

(5) スタック構成について

スタック構成で，VNI マッピングが数百以上設定されている状態でマスタスイッチが再起動または停止した場合，マスタスイッチの変更直後に新しいマスタスイッチで運用コマンドを実行すると，結果を表示するまでに数分掛かることがあります。

(6) TPID の設定について

VXLAN Access ポートおよび装置に対して，コンフィグレーションで TPID 値を設定した場合，対象 VXLAN Access ポートでの通信ができなくなります。

(7) VLAN マッピング時の VXLAN Access ポートについて

コンフィグレーションコマンド vxlan vlan-mapping mode で extended パラメータを設定し，VNI マッピング方式に VLAN マッピングを使用する場合は，コンフィグレーションコマンド vxlan-vni を設定した VLAN を，VXLAN Access ポートのネイティブ VLAN（switchport trunk コマンドの native vlan パラメータ）に指定しないでください。

(8) IEEE802.1Q VLAN Tag がスタックされたフレームについて

VXLAN トンネル機能は未サポートとなります。

(9) VXLAN PMTU 機能の無効時について

VXLAN PMTU 機能を無効にする場合，数分掛かることがあります。コンフィグレーションコマンド vxlan pmtu または vxlan enable を削除して VXLAN PMTU 機能を無効にする場合，同時にフィルタ・QoS・ポリシーベースミラーリング機能を設定しないでください。VXLAN PMTU 機能を無効にした場合，数分経過してからフィルタ・QoS・ポリシーベースミラーリング機能を設定してください。

(10) IPv6 を扱うネットワークでの VXLAN PMTU 機能について

IPv6 パケットをカプセル化するネットワークで VXLAN PMTU 機能を使用する場合，コンフィグレーションコマンド vxlan pmtu には 1280 オクテット以上の値を設定してください。

(11) VNI マッピング対象外の VLAN での VXLAN PMTU 機能について

VNI マッピングをしていない VLAN を設定したポートで VXLAN PMTU 機能を有効にした場合，VNI マッピングをしていない VLAN に対しても VXLAN PMTU 機能が動作します。ただし，受信側フロー検出モードが IP 未設定 VLAN 抑止モードの場合, VNI マッピングをしていない VLAN では次のように動作します。

コンフィグレーションコマンド ip address が未設定のとき

PMTU を超える IPv4 パケットは廃棄されますが，ICMP パケットによる通知をしません。

コンフィグレーションコマンド ipv6 enable が未設定のとき

PMTU を超える IPv6 パケットは廃棄されますが，ICMPv6 パケットによる通知をしません。

26.2 コンフィグレーション

26.2.1 コンフィグレーションコマンド一覧

VXLAN のコンフィグレーションコマンド一覧を次の表に示します。

表 26-5 コンフィグレーションコマンド一覧

コマンド名	説明
destination-ip	VXLAN トンネルの宛先 IPv4 アドレスを設定します。
encapsulation dot1q	イーサネットサブインタフェースまたはポートチャネルサブインタフェースを VLAN Tag で論理的に多重化するための VLAN ID を設定します。
interface vxlan	VXLAN の VTEP 情報を設定します。
member vni	該当 VTEP に所属する VNI を設定します。
source-interface	VXLAN フレームに付ける送信元インタフェースを設定します。
switchport	レイヤ 2 インタフェースの設定を有効または無効にします。
vxlan enable	VXLAN 機能を有効にします。
vxlan pmtu	本装置の VXLAN PMTU 機能を有効にして，Path MTU Discovery を送信する閾値を設定します。
vxlan pmtu enable	該当するインタフェースで VXLAN PMTU 機能を有効にします。
vxlan vlan-mapping mode	VNI マッピング方式で VLAN マッピングを選択する場合に，収容条件を拡張するモードを設定します。
vxlan-vni	VNI を VLAN またはサブインタフェースにマッピングします。
interface gigabitethernet※1	最大回線速度が 1000Mbit/s のイーサネットインタフェースに関する項目を設定します。
interface hundredgigabitethernet※1	最大回線速度が 100Gbit/s のイーサネットインタフェースに関する項目を設定します。
interface tengigabitethernet※1	最大回線速度が 10Gbit/s のイーサネットインタフェースに関する項目を設定します。
interface port-channel※2	ポートチャネルインタフェースに関する項目を設定します。

注※1

「コンフィグレーションコマンドレファレンス Vol.1」「15　イーサネット」を参照してください。

注※2

「コンフィグレーションコマンドレファレンス Vol.1」「16　リンクアグリゲーション」を参照してください。

26.2.2 VXLAN 設定の流れ

VXLAN 機能を正常に動作させるには，構成に合った設定が必要です。設定の流れを次に示します。

1. VXLAN 機能の有効化

   VXLAN 機能を有効にする設定をします。

2. VTEP の設定
   VTEP 情報を設定します。
3. VXLAN Access ポートの設定
   次に示すどちらかの方法で，VXLAN Access ポートを設定します。
   - VLAN マッピングの設定
   - サブインタフェースマッピングの設定

26.2.3 VXLAN 機能の有効化

[設定のポイント]

本装置を VXLAN で動作させるには，vxlan enable コマンドを設定します。

vxlan enable コマンドの設定を有効にするには，本装置を再起動する必要があります。そのため，運用を開始する前に設定してください。

[コマンドによる設定]

1. **(config)# vxlan enable**
   After this command execute, please save configuration editing now in startup-config, and please reboot a device.
   Do you wish to continue ? (y/n):
   VXLAN 機能を有効にする設定をします。コンフィグレーションの変更確認メッセージに対して y を入力します。この設定は，装置を再起動するまで有効になりません。
2. **(config)# save**
   (config)# exit
   コンフィグレーションを保存して，コンフィグレーションコマンドモードから装置管理者モードに戻ります。
3. **# reload**
   本装置を再起動します。

26.2.4 VTEP の設定

[設定のポイント]

VTEP には次に示す情報を設定します。

- VTEP に所属させる VNI ID
- VXLAN トンネルの宛先 IPv4 アドレス
- VXLAN トンネルの送信元 IPv4 アドレス
  ループバックインタフェースの IP アドレスを使用します。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   (config-if)# ip address 10.200.30.2
   (config-if)# exit
   VTEP の送信元 IP アドレスとなるループバックインタフェースの IP アドレスを設定します。
2. **(config)# interface vxlan 2**

```
(config-if)# member vni 2
(config-if)# destination-ip 10.200.33.2
```

VTEP 2 に所属させる VNI ID と宛先 IPv4 アドレスを設定します。

3.
```
(config-if)# source-interface loopback 0
(config-if)# exit
```

VTEP の送信元インタフェースとしてループバックインタフェースを設定します。

[注意事項]

VTEP に所属している VNI ID を削除する場合は，先に該当する VNI ID を VXLAN Access ポートからすべて削除してください。VXLAN Access ポートに VTEP に所属していない VNI ID が設定されていると，該当する VNI ID で通信する場合があります。

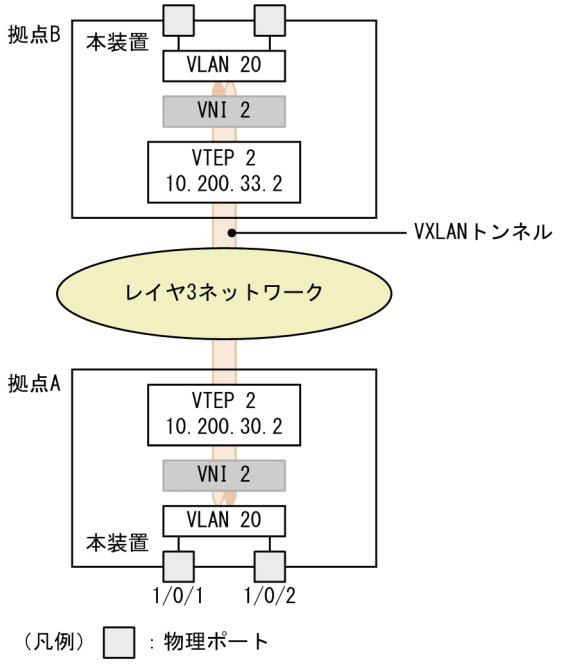
26.2.5 VXLAN Access ポートの設定

VXLAN Access ポートに VNI ID を設定する場合は，先に該当する VNI ID を VTEP に所属させてください。VXLAN Access ポートの VNI ID に VTEP に所属していない VNI ID を設定すると，該当する VNI ID で通信する場合があります。

(1) VLAN マッピング

拠点 A と拠点 B を VXLAN トンネルで接続する構成を設定します。VNI マッピング方式として VLAN マッピングを使用します。VLAN マッピングの構成例を次の図に示します。

図 26-10 VLAN マッピングの構成例



[設定のポイント]

VLAN マッピングには次に示す情報を設定します。

- モード

収容条件を拡張するモードで運用する場合は，vxlan vlan-mapping mode コマンドを設定します。vxlan vlan-mapping mode コマンドを設定するとオーバーレイ（VXLAN）プログラムが再起動するため，運用を開始する前に設定してください。

- VNI のマッピング
- VLAN のポートへのマッピング

  VLAN に VNI ID を割り当てたあとで，物理ポートまたはチャネルグループに該当する VLAN ID を設定してください。物理ポートまたはチャネルグループに VLAN ID が割り当てられた状態で該当する VLAN に VNI ID を設定すると，VXLAN Access ポートで受信したフレームが一時的に折り返して通信する場合があります。

[コマンドによる設定]

1. **(config)# vlan 20**
   (config-vlan)# vxlan-vni 2
   (config-vlan)# exit
   VLAN に VNI ID を割り当てます。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 20
   (config-if)# exit
   ポート 1/0/1 に VLAN 20 を割り当てます。
3. **(config)# interface gigabitethernet 1/0/2**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 20
   (config-if)# exit
   ポート 1/0/2 に VLAN 20 を割り当てます。
   拠点 B 側も，同じ VNI で同様に設定してください。

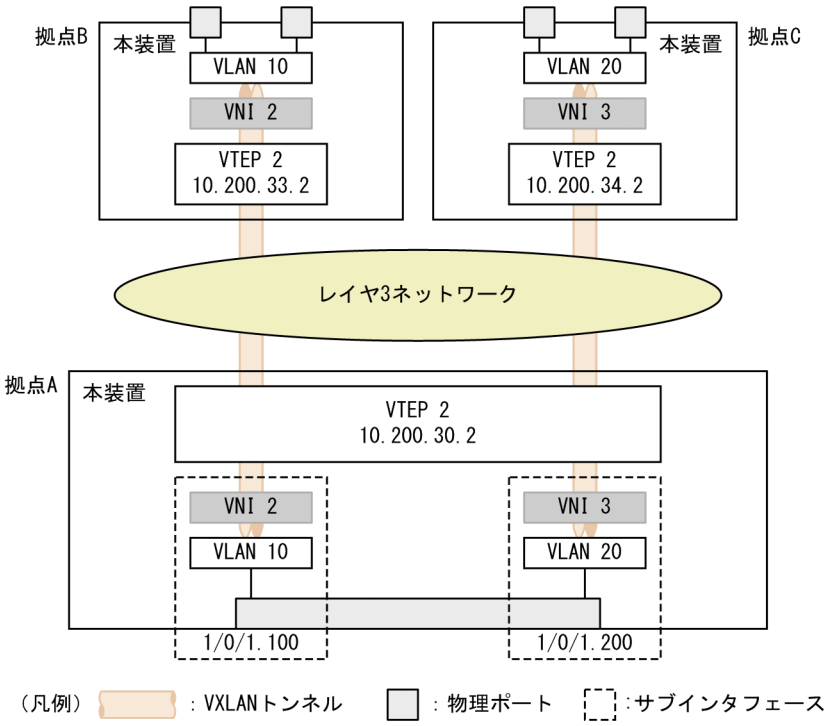
[注意事項]

VXLAN Access ポートを削除する場合は，物理ポートまたはチャネルグループから VLAN ID を削除したあと，該当する VLAN に設定されている VNI ID を削除してください。物理ポートまたはチャネルグループに VLAN ID が割り当てられた状態で該当する VLAN から VNI ID を削除すると，VXLAN Access ポートで受信したフレームが一時的に折り返して通信する場合があります。

(2) サブインタフェースマッピング

拠点 A と拠点 B，拠点 A と拠点 C を VXLAN トンネルで接続する構成を設定します。VNI マッピング方式としてサブインタフェースマッピングを使用します。サブインタフェースマッピングの構成例を次の図に示します。

図 26-11 サブインタフェースマッピングの構成例



[設定のポイント]

サブインタフェースマッピングには次に示す情報を設定します。

- サブインタフェース
- VNI のマッピング

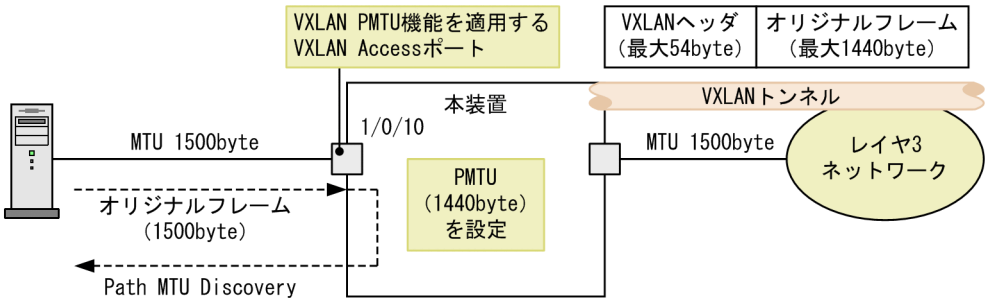
[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# no switchport
   (config-if)# exit
   ポート 1/0/1 でレイヤ 2 インタフェースの設定を無効にします。
2. **(config)# interface gigabitethernet 1/0/1.100**
   (config-subif)# encapsulation dot1q 10
   (config-subif)# vxlan-vni 2
   (config-subif)# exit
   ポート 1/0/1 にサブインタフェース 1/0/1.100，および VLAN ID として 10 を設定します。また，VNI 2 に割り当てます。
3. **(config)# interface gigabitethernet 1/0/1.200**
   (config-subif)# encapsulation dot1q 20
   (config-subif)# vxlan-vni 3
   (config-subif)# exit
   ポート 1/0/1 にサブインタフェース 1/0/1.200，および VLAN ID として 20 を設定します。また，VNI 3 に割り当てます。

26.2.6　VXLAN PMTU の設定

本装置に Path MTU Discovery を送信する閾値と，適用する VXLAN Access ポートの設定をします。VXLAN PMTU の設定例を次の図に示します。

図 26-12　VXLAN PMTU の設定例



[設定のポイント]

Path MTU Discovery を送信する閾値に 1440byte を設定します。また，VXLAN PMTU 機能を適用する VXLAN Access ポートを 1/0/10 に設定します。

VXLAN PMTU 機能を適用したポートは，閾値を超えるフレームを受信すると Path MTU Discovery を送信します。

[コマンドによる設定]

1. **(config)# vxlan pmtu 1440**

   本装置の VXLAN PMTU 機能を有効にして，Path MTU Discovery を送信する閾値に 1440byte を設定します。

2. **(config)# interface gigabitethernet 1/0/10**

   (config-if)# vxlan pmtu enable

   ポート 1/0/10 に VXLAN PMTU 機能を適用します。

26.3 オペレーション

26.3.1 運用コマンド一覧

VXLAN の運用コマンド一覧を次の表に示します。

表 26-6 運用コマンド一覧

コマンド名	説明
show vxlan	VTEP 情報を表示します。
show vxlan vni	VNI 情報を表示します。
show vxlan peers	VTEP のピア情報を表示します。
show vxlan mac-address-table	VXLAN MAC アドレステーブル情報を表示します。
clear vxlan mac-address-table	VXLAN MAC アドレステーブル情報をクリアします。
restart overlay	オーバーレイ（VXLAN）プログラムを再起動します。
dump protocols overlay	オーバーレイ（VXLAN）プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

26.3.2 VTEP ピア情報の確認

show vxlan peers コマンドで VTEP ピア情報を確認できます。「Status」に VXLAN トンネルの構築状態が表示されます。経路がマルチパス化されている場合，2 番目以降は Status，Nexthop，VRF だけを表示します。

図 26-13 VTEP ピア情報の表示

```
> show vxlan peers
Date 20XX/10/29 11:33:50 UTC
VTEP ID: 1   Source IP: 1.1.1.1
  Destination IP   Status  Nexthop          VRF
  30.10.1.8        Up      10.10.1.225      global
  30.10.1.21       Down    -                -
  110.100.100.100  Up      100.100.100.200  10
VTEP ID: 2   Source IP: 1.1.1.2
  Destination IP   Status  Nexthop          VRF
  50.20.1.30       Up      20.20.1.214      20
>
```

26.3.3 VXLAN MAC アドレステーブル情報の確認

show vxlan mac-address-table コマンドで, VNI が付いた MAC アドレステーブル情報を確認できます。

図 26-14 すべての VXLAN MAC アドレステーブル情報の表示

```
> show vxlan mac-address-table
Date 20XX/10/29 11:33:50 UTC
MAC address          VNI  Type     Port     VLAN  Connect
0012.e28e.0602  16671234  Dynamic  Network     -  100.12.5.89
0012.e205.0642  16671234  Dynamic  Access    100  1/0/5
0012.e2a8.250c       103  Dynamic  Access    200  2/0/24
0012.e205.0643       103  Dynamic  Access   4001  1/0/1-2
>
```

26.3.4 VXLAN 統計情報の確認

show vxlan statistics コマンドで，VNI 単位または VXLAN トンネル単位で VXLAN の統計情報を確認できます。

図 26-15 VNI 単位の VXLAN 統計情報の表示

```
>show vxlan statistics vni 9500
Date 20XX/11/12 14:15:00 UTC
VTEP ID: 1  VNI: 9500
            Packets                Octets
  Encap        1825                953471
  Decap          11                  7428
  AcsAcs          0                     0
>
```

27 スパニングツリー

この章では，スパニングツリー機能の解説と操作方法について説明します。

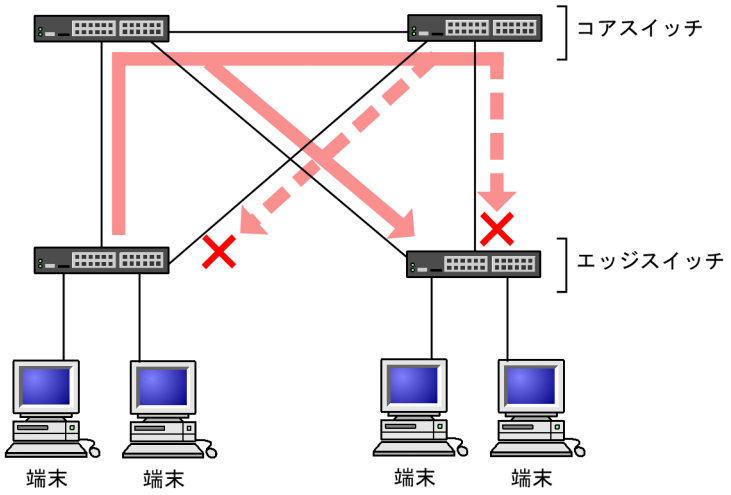
27.1　スパニングツリーの概説

27.1.1　概要

スパニングツリープロトコルは，レイヤ２のループ防止プロトコルです。スパニングツリープロトコルを使用することで，レイヤ２ネットワークを冗長化し，ループを防止できます。

スパニングツリーを適用したネットワークの概要を次の図に示します。

図 27-1　スパニングツリーを適用したネットワークの概要



（凡例）×：Blocking状態

図の構成は，ネットワークのコアを担うスイッチを冗長化し，また，端末を収容するエッジスイッチからの通信経路を冗長化しています。装置および通信経路を冗長化することで，通常の通信経路に障害が発生しても代替の経路で通信を継続できます。

レイヤ２ネットワークを冗長化するとレイヤ２ループの構成になります。レイヤ２のループはブロードキャストストームの発生や MAC アドレス学習が安定しないなどの問題を引き起こします。スパニングツリーは，冗長化してループ構成になったレイヤ２ネットワークで，通信を止める場所を選択して Blocking 状態とすることでループを防止するプロトコルです。

27.1.2　スパニングツリーの種類

本装置では，PVST+，シングルスパニングツリーおよびマルチプルスパニングツリーの３種類のスパニングツリーをサポートします。各スパニングツリーは構築の単位が異なります。スパニングツリーの種類と概要について次の表に示します。

表 27-1　スパニングツリーの種類

名称	構築単位	概要
PVST+	VLAN 単位	VLAN 単位にツリーを構築します。一つのポートに複数の VLAN が所属している場合，VLAN ごとに異なるツリー構築結果を適用します。

名称	構築単位	概要
シングルスパニングツリー	装置単位	装置全体のポートを対象としツリーを構築します。 VLAN 構成とは無関係に装置のすべてのポートにツリー構築結果を適用します。
マルチプルスパニングツリー	MST インスタンス単位	複数の VLAN をまとめた MST インスタンスというグループごとにスパニングツリーを構築します。一つのポートに複数の VLAN が所属している場合，MST インスタンス単位に異なるツリー構築結果を適用します。

本装置では，上記で記述したスパニングツリーを単独または組み合わせて使用できます。スパニングツリーの組み合わせと適用範囲を次の表に示します。

表 27-2　スパニングツリーの組み合わせと適用範囲

ツリー構築条件	トポロジー計算結果の適用範囲
PVST+単独	PVST+が動作している VLAN には VLAN ごとのスパニングツリーを適用します。そのほかの VLAN はスパニングツリーを適用しません。 本装置では，デフォルトでポート VLAN 上で PVST+が動作します。
シングルスパニングツリー単独	全 VLAN にシングルスパニングツリーを適用します。 PVST+をすべて停止した構成です。
PVST+とシングルスパニングツリーの組み合わせ	PVST+が動作している VLAN には VLAN ごとのスパニングツリーを適用します。そのほかの VLAN にはシングルスパニングツリーを適用します。
マルチプルスパニングツリー単独	全 VLAN にマルチプルスパニングツリーを適用します。

注　マルチプルスパニングツリーはほかのツリーと組み合わせて使用できません。

27.1.3　スパニングツリーと高速スパニングツリー

PVST+，シングルスパニングツリーには IEEE802.1D のスパニングツリーと IEEE802.1w の高速スパニングツリーの 2 種類があります。それぞれ，PVST+と Rapid PVST+，STP と Rapid STP と呼びます。

スパニングツリープロトコルのトポロジー計算は，通信経路を変更する際にいったんポートを通信不可状態（Blocking 状態）にしてから複数の状態を遷移して通信可能状態（Forwarding 状態）になります。IEEE 802.1D のスパニングツリーはこの状態遷移においてタイマによる状態遷移を行うため，通信可能となるまでに一定の時間が掛かります。IEEE 802.1w の高速スパニングツリーはこの状態遷移でタイマによる待ち時間を省略して高速な状態遷移を行うことで，トポロジー変更によって通信が途絶える時間を最小限にします。

なお，マルチプルスパニングツリーは IEEE802.1s として規格化されたもので，状態遷移の時間は IEEE802.1w と同等です。それぞれのプロトコルの状態遷移とそれに必要な時間を以下に示します。

表 27-3　PVST+，STP(シングルスパニングツリー)の状態遷移

状態	状態の概要	次の状態への遷移
Disable	ポートが使用できない状態です。使用可能となるとすぐに Blocking に遷移します。	−

状態	状態の概要	次の状態への遷移
Blocking	通信不可の状態で，MAC アドレス学習も行いません。リンクアップ直後またはトポロジーが安定して Blocking になるポートもこの状態になります。	20 秒(変更可能)または BPDU を受信
Listening	通信不可の状態で，MAC アドレス学習も行いません。該当ポートが Learning になる前に，トポロジーが安定するまで待つ期間です。	15 秒(変更可能)
Learning	通信不可の状態です。しかし，MAC アドレス学習は行います。該当ポートが Forwarding になる前に，事前に MAC アドレス学習を行う期間です。	15 秒(変更可能)
Forwarding	通信可能の状態です。トポロジーが安定した状態です。	－

（凡例）－：該当なし

表 27-4　Rapid PVST+，Rapid STP(シングルスパニングツリー)の状態遷移

状態	状態の概要	次の状態への遷移
Disable	ポートが使用できない状態です。使用可能となるとすぐに Discarding に遷移します。	－
Discarding	通信不可の状態で，MAC アドレス学習も行いません。該当ポートが Learning になる前に，トポロジーが安定するまで待つ期間です。	省略または 15 秒(変更可能)
Learning	通信不可の状態です。しかし，MAC アドレス学習は行います。該当ポートが Forwarding になる前に，事前に MAC アドレス学習を行う期間です。	省略または 15 秒(変更可能)
Forwarding	通信可能の状態です。トポロジーが安定した状態です。	－

（凡例）－：該当なし

Rapid PVST+，Rapid STP では，対向装置からの BPDU 受信によって Discarding と Learning 状態を省略します。この省略により，高速なトポロジー変更を行います。

高速スパニングツリーを使用する際は，以下の条件に従って設定してください。条件を満たさない場合，Discarding，Learning を省略しないで高速な状態遷移を行わない場合があります。

- トポロジーの全体を同じプロトコル（Rapid PVST+または Rapid STP）で構築する（Rapid PVST+と Rapid STP の相互接続は「27.3.2　アクセスポートの PVST+」を参照してください)。
- スパニングツリーが動作する装置間は Point-to-Point 接続する。
- スパニングツリーが動作する装置を接続しないポートでは PortFast を設定する。

27.1.4　スパニングツリートポロジーの構成要素

スパニングツリーのトポロジーを設計するためには，ブリッジやポートの役割およびそれらの役割を決定するために用いる識別子などのパラメータがあります。これらの構成要素とトポロジー設計における利用方法を以下に示します。

(1)　ブリッジの役割

ブリッジの役割を次の表に示します。スパニングツリーのトポロジー設計はルートブリッジを決定することから始まります。

表 27-5　ブリッジの役割

ブリッジの役割	概要
ルートブリッジ	トポロジーを構築する上で論理的な中心となるスイッチです。トポロジー内に一つだけ存在します。
指定ブリッジ	ルートブリッジ以外のスイッチです。ルートブリッジの方向からのフレームを転送する役割を担います。

(2)　ポートの役割

ポートの役割を次の表に示します。指定ブリッジは 3 種類のポートの役割を持ちます。ルートブリッジは，以下の役割のうち，すべてのポートが指定ポートとなります。

表 27-6　ポートの役割

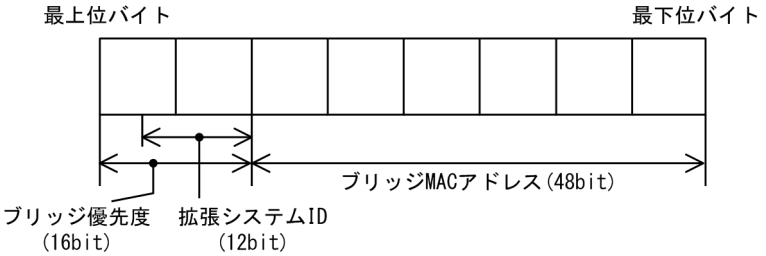
ポートの役割	概要
ルートポート	指定ブリッジからルートブリッジへ向かう通信経路のポートです。通信可能なポートとなります。
指定ポート	ルートポート以外の通信可能なポートです。ルートブリッジからの通信経路でトポロジーの下流へ接続するポートです。
非指定ポート	ルートポート，指定ポート以外のポートで，通信不可の状態のポートです。障害が発生した際に通信可能になり代替経路として使用します。

(3)　ブリッジ識別子

トポロジー内の装置を識別するパラメータをブリッジ識別子と呼びます。ブリッジ識別子が最も小さい装置が優先度が高く，ルートブリッジとして選択されます。

ブリッジ識別子はブリッジ優先度（16bit）とブリッジ MAC アドレス（48bit）で構成されます。ブリッジ優先度の下位 12bit は拡張システム ID です。拡張システム ID には，シングルスパニングツリー，マルチプルスパニングツリーの場合は 0 が設定され，PVST+の場合は VLAN ID が設定されます。ブリッジ識別子を次の図に示します。

図 27-2　ブリッジ識別子



(4)　パスコスト

スイッチ上の各ポートの通信速度に対応するコスト値をパスコストと呼びます。指定ブリッジからルートブリッジへ到達するために経由するすべてのポートのコストを累積した値をルートパスコストと呼びます。ルートブリッジへ到達するための経路が 2 種類以上ある場合，ルートパスコストが最も小さい経路を使用します。

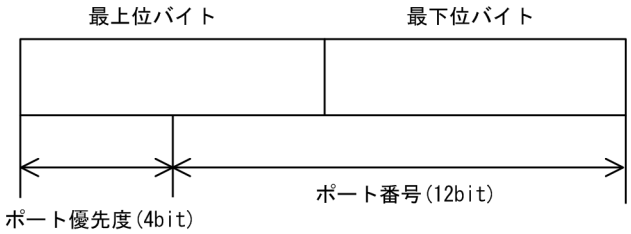
速度が速いポートほどパスコストを低くすることをお勧めしています。パスコストはデフォルト値がポートの速度に応じた値となっていて，コンフィグレーションで変更することもできます。

(5)　ポート識別子

スイッチ内の各ポートを識別するパラメータをポート識別子と呼びます。ポート識別子は 2 台のスイッチ間で 2 本以上の冗長接続をし，かつ各ポートでパスコストを変更できない場合に通信経路の選択に使用します。ただし，2 台のスイッチ間の冗長接続はリンクアグリゲーションを使用することをお勧めします。リンクアグリゲーションをサポートしていない装置と冗長接続するためにはスパニングツリーを使用してください。

ポート識別子はポート優先度（4bit）とポート番号（12bit）によって構成されます。ポート識別子を次の図に示します。

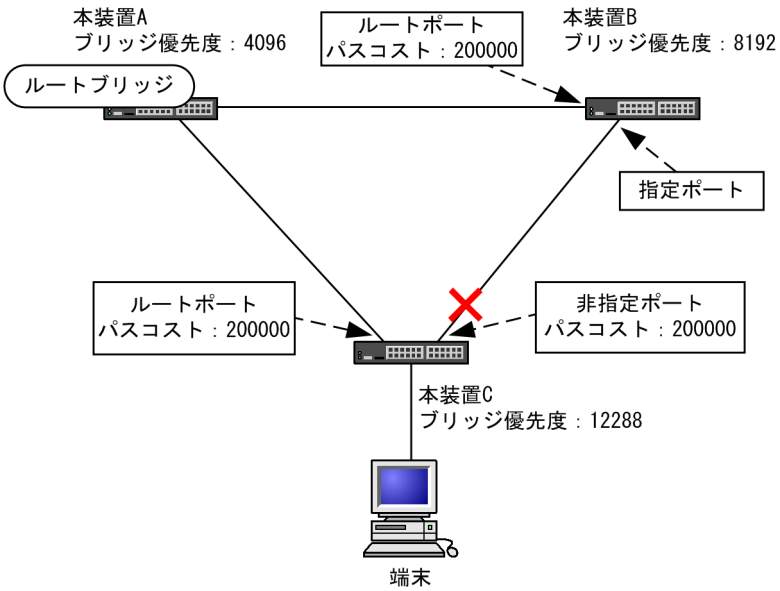
図 27-3　ポート識別子



27.1.5　スパニングツリーのトポロジー設計

スパニングツリーは，ブリッジ識別子，パスコストによってトポロジーを構築します。次の図に，トポロジー設計の基本的な手順を示します。図の構成は，コアスイッチとして 2 台を冗長化して，エッジスイッチとして端末を収容するスイッチを配置する例です。

図 27-4　スパニングツリーのトポロジー設計



（凡例）×　：Blocking状態

(1)　ブリッジ識別子によるルートブリッジの選出

ルートブリッジは，ブリッジ識別子の最も小さい装置を選出します。通常，ルートブリッジにしたい装置のブリッジ優先度を最も小さい値（最高優先度）に設定します。図の例では，本装置 A がルートブリッジになるように設定します。本装置 B，本装置 C は指定ブリッジとなります。

また，ルートブリッジに障害が発生した場合に代替のルートブリッジとして動作するスイッチを本装置 B になるように設定します。本装置 C は最も低い優先度として設定します。

スパニングツリーのトポロジー設計では，図の例のようにネットワークのコアを担う装置をルートブリッジとし，代替のルートブリッジとしてコアを冗長化する構成をお勧めします。

(2)　通信経路の設計

ルートブリッジを選出した後，各指定ブリッジからルートブリッジに到達するための通信経路を決定します。

(a)　パスコストによるルートポートの選出

本装置 B，本装置 C では，ルートブリッジに到達するための経路を最も小さいルートパスコスト値になるよう決定します。図の例は，すべてのポートがパスコスト 200000 としています。それぞれ直接接続したポートが最もルートパスコストが小さく，ルートポートとして選出します。

ルートパスコストの計算は，指定ブリッジからルートブリッジへ向かう経路で，各装置がルートブリッジの方向で送信するポートのパスコストの総和で比較します。例えば，本装置 C の本装置 B を経由する経路はパスコストが 400000 となりルートポートには選択されません。

パスコストは，ポートの速度が速いほど小さい値をデフォルト値に持ちます。また，ルートポートの選択にはルートブリッジまでのコストの総和で比較します。そのため，速度の速いポートや経由する装置の段数が少ない経路を優先して使用したい場合，通常はパスコスト値を変更する必要はありません。速度の遅いポートを速いポートより優先して経路として使用したい場合はコンフィグレーションで変更することによって通信したい経路を設計します。

(b)　指定ポート，非指定ポートの選出

本装置 B，本装置 C 間の接続はルートポート以外のポートでの接続になります。このようなポートではどれかのポートが非指定ポートとなって Blocking 状態になります。スパニングツリーは，このように片側が Blocking 状態となることでループを防止します。

指定ポート，非指定ポートは次のように選出します。

- 装置間でルートパスコストが小さい装置が指定ポート，大きい装置が非指定ポートになります。
- ルートパスコストが同一の場合，ブリッジ識別子の小さい装置が指定ポート，大きい装置が非指定ポートになります。

図の例では，ルートパスコストは同一です。ブリッジ優先度によって本装置 B が指定ポート，本装置 C が非指定ポートとなり，本装置 C が Blocking 状態となります。Blocking 状態になるポートを本装置 B にしたい場合は，パスコストを調整して本装置 B のルートパスコストが大きくなるように設定します。

27.1.6　STP 互換モード

(1)　概要

Rapid PVST+，Rapid STP，およびマルチプルスパニングツリーで，対向装置が PVST+または STP の場合，該当するポートは STP 互換モードで動作します。

STP 互換モードで動作すると，該当するポートで高速遷移が行われなくなり，通信復旧に時間が掛かるようになります。

対向装置が Rapid PVST+，Rapid STP，およびマルチプルスパニングツリーに変わった場合，STP 互換モードから復旧し，再び高速遷移が行われるようになりますが，タイミングによって該当するポートと対向装置が STP 互換モードで動作し続けることがあります。

STP 互換モード復旧機能は，STP 互換モードで動作しているポートを強制的に復旧させ，正常に高速遷移ができるようにします。

(2)　復旧機能

運用コマンド clear spanning-tree detected-protocol を実行することで，STP 互換モードから強制的に復旧します。該当するポートのリンクタイプが point-to-point，shared のどちらの場合でも動作します。

(3)　自動復旧機能

該当するポートのリンクタイプが point-to-point の場合，STP 互換モード復旧機能が自動で動作します。

該当するポートが非指定ポートで STP 互換モードで動作した場合，該当するポートから RST BPDU または MST BPDU を送信することで，STP 互換モードを解除します。

該当するポートのリンクタイプが shared の場合，自動復旧モードが正しく動作できないため，自動復旧モードは動作しません。

27.1.7　スパニングツリー共通の注意事項

(1)　CPU の過負荷について

CPU が過負荷な状態になった場合，本装置が送受信する BPDU の廃棄が発生して，タイムアウトのメッセージ出力，トポロジー変更，一時的な通信断となることがあります。

(2)　VLAN のダウンを伴うコンフィグレーションコマンドの設定について

コンフィグレーションコマンド no spanning-tree disable で本装置にスパニングツリー機能を適用すると，全 VLAN が一時的にダウンします。

27.2　スパニングツリー動作モードのコンフィグレーション

スパニングツリーの動作モードを設定します。

コンフィグレーションを設定しない状態で本装置を起動すると，動作モードは pvst で動作します。

27.2.1　コンフィグレーションコマンド一覧

スパニングツリー動作モードのコンフィグレーションコマンド一覧を次の表に示します。

表 27-7　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree disable	スパニングツリー機能の停止を設定します。
spanning-tree mode	スパニングツリー機能の動作モードを設定します。
spanning-tree single mode	シングルスパニングツリーの STP と Rapid STP を選択します。
spanning-tree vlan mode	VLAN ごとに PVST+と Rapid PVST+を選択します。

27.2.2　動作モードの設定

スパニングツリーは装置の動作モードを設定することで各種スパニングツリーを使用することができます。装置の動作モードを次の表に示します。動作モードを設定しない場合，pvst モードで動作します。

動作モードに rapid-pvst を指定しても，シングルスパニングツリーのデフォルトは STP であることに注意してください。

表 27-8　スパニングツリー動作モード

コマンド名	説明
spanning-tree disable	スパニングツリーを停止します。
spanning-tree mode pvst	PVST+とシングルスパニングツリーを使用できます。デフォルトで PVST+が動作します。シングルスパニングツリーはデフォルトでは動作しません。
spanning-tree mode rapid-pvst	PVST+とシングルスパニングツリーを使用できます。デフォルトで高速スパニングツリーの Rapid PVST+が動作します。シングルスパニングツリーはデフォルトでは動作しません。
spanning-tree mode mst	マルチプルスパニングツリーが動作します。

(1)　動作モード pvst の設定

[設定のポイント]

装置の動作モードを pvst に設定します。ポート VLAN を作成すると，その VLAN で自動的に PVST+が動作します。VLAN ごとに Rapid PVST+に変更することもできます。

シングルスパニングツリーはデフォルトでは動作しないで，設定することで動作します。その際，デフォルトでは STP で動作し，Rapid STP に変更することもできます。

[コマンドによる設定]

1. **(config)# spanning-tree mode pvst**
   スパニングツリーの動作モードを pvst に設定します。ポート VLAN で自動的に PVST+が動作します。
2. **(config)# spanning-tree vlan 10 mode rapid-pvst**
   VLAN 10 の動作モードを Rapid PVST+に変更します。ほかのポート VLAN は PVST+で動作し，VLAN 10 は Rapid PVST+で動作します。
3. **(config)# spanning-tree single**
   シングルスパニングツリーを動作させます。PVST+を使用していない VLAN に適用します。デフォルトでは STP で動作します。
4. **(config)# spanning-tree single mode rapid-stp**
   シングルスパニングツリーを Rapid STP に変更します。

(2)　動作モード rapid-pvst の設定

[設定のポイント]

装置の動作モードを rapid-pvst に設定します。ポート VLAN を作成すると，その VLAN で自動的に Rapid PVST+が動作します。VLAN ごとに PVST+に変更することもできます。

シングルスパニングツリーはデフォルトでは動作しないで，設定することで動作します。動作モードに rapid-pvst を指定しても，シングルスパニングツリーのデフォルトは STP であることに注意してください。

[コマンドによる設定]

1. **(config)# spanning-tree mode rapid-pvst**
   スパニングツリーの動作モードを rapid-pvst に設定します。ポート VLAN で自動的に Rapid PVST+が動作します。
2. **(config)# spanning-tree vlan 10 mode pvst**
   VLAN 10 の動作モードを PVST+に変更します。ほかのポート VLAN は Rapid PVST+で動作し，VLAN 10 は PVST+で動作します。
3. **(config)# spanning-tree single**
   シングルスパニングツリーを動作させます。PVST+を使用していない VLAN に適用します。デフォルトでは STP で動作します。
4. **(config)# spanning-tree single mode rapid-stp**
   シングルスパニングツリーを Rapid STP に変更します。

(3)　動作モード mst の設定

[設定のポイント]

マルチプルスパニングツリーを使用する場合，装置の動作モードを mst に設定します。マルチプルスパニングツリーはすべての VLAN に適用します。PVST+やシングルスパニングツリーとは併用できません。

[コマンドによる設定]

1. **(config)# spanning-tree mode mst**
   マルチプルスパニングツリーを動作させます。

(4)　スパニングツリーを停止する設定

［設定のポイント］

スパニングツリーを使用しない場合，disable を設定することで本装置のスパニングツリーをすべて停止します。

［コマンドによる設定］

1. **(config)# spanning-tree disable**
   スパニングツリーの動作を停止します。

27.3　PVST+解説

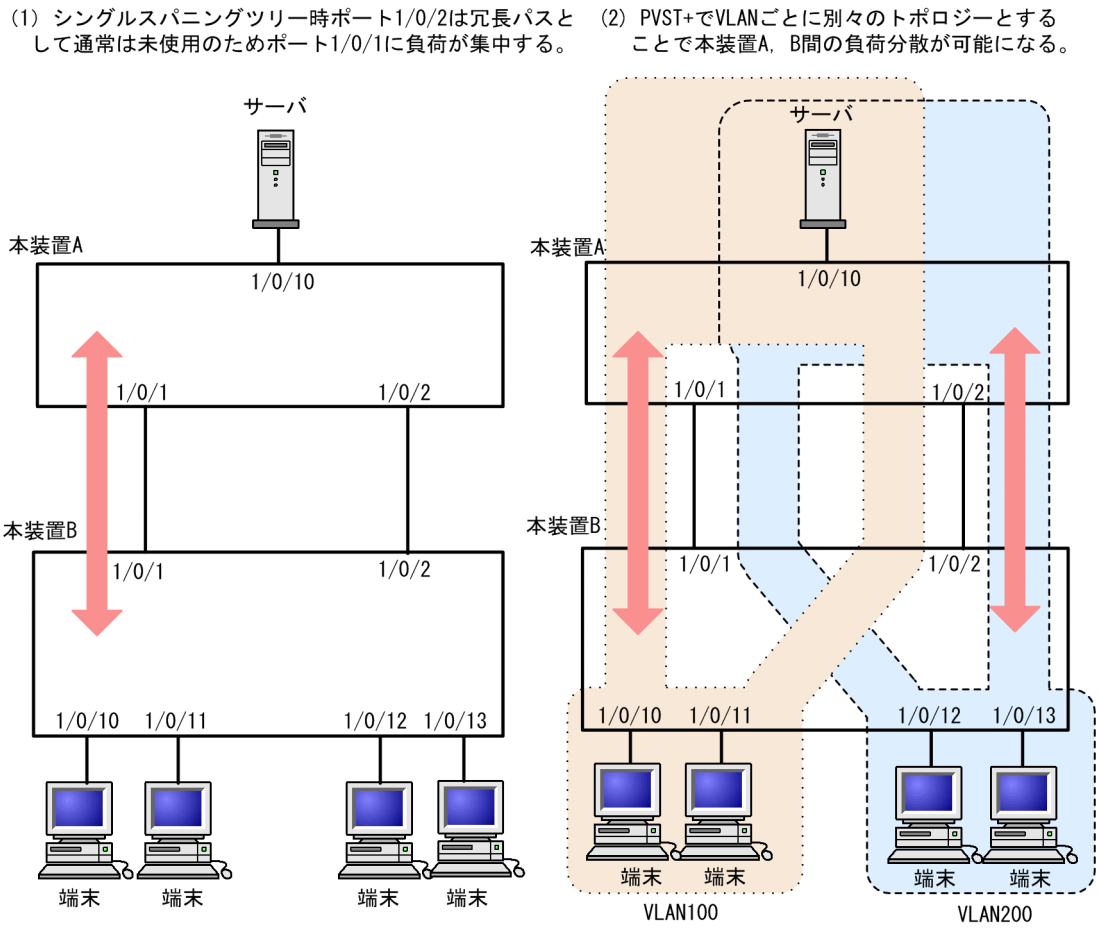
PVST+は，VLAN 単位にツリーを構築します。VLAN 単位にツリーを構築できるため，ロードバランシングが可能です。また，アクセスポートでは，シングルスパニングツリーで動作しているスイッチと接続できます。

27.3.1　PVST+によるロードバランシング

次の図に示すような本装置 A, B 間で冗長パスを組んだネットワークにおいてシングルスパニングツリーを組んだ場合，各端末からサーバへのアクセスは本装置 A，B 間のポート 1 に集中します。そこで，複数の VLAN を組み，PVST+によって VLAN ごとに別々のトポロジーとなるように設定することで冗長パスとして使用できるようになり，さらに負荷分散を図れます。ポート優先度によるロードバランシングの例を次の図に示します。

この例では，VLAN100 に対してはポート 1/0/1 のポート優先度をポート 1/0/2 より高く設定し，逆に VLAN200 に対しては 1/0/2 のポート優先度をポート 1/0/1 より高く設定することで，各端末からサーバに対するアクセスを VLAN ごとに負荷分散を行っています。

図 27-5　PVST+によるロードバランシング



27.3.2　アクセスポートの PVST+

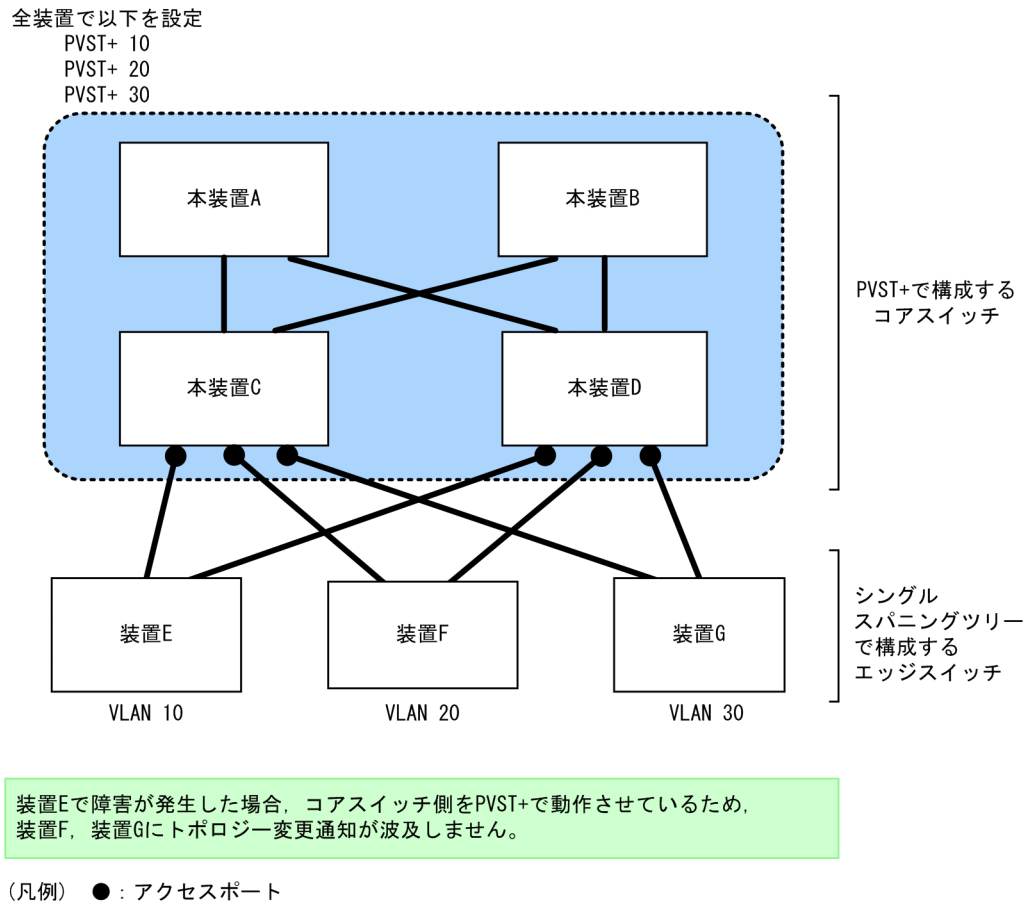
(1)　解説

シングルスパニングツリーを使用している装置，または装置で一つのツリーを持つシングルスパニングツリーに相当する機能をサポートしている装置（以降，単にシングルスパニングツリーと表記します）とPVST+を用いてネットワークを構築できます。シングルスパニングツリーで運用している装置をエッジスイッチ，本装置をコアスイッチに配置して使います。このようなネットワークを構築することで，次のメリットがあります。

- エッジスイッチに障害が発生しても，ほかのエッジスイッチにトポロジー変更の影響が及ばない。
- コアスイッチ間でロードバランスができる。

シングルスパニングツリーとは，アクセスポートで接続できます。構成例を次の図に示します。この例では，エッジスイッチでシングルスパニングツリーを動作させ，コアスイッチで PVST+を動作させています。コアスイッチではエッジスイッチと接続するポートをアクセスポートとしています。各エッジスイッチはそれぞれ単一の VLAN を設定しています。

図 27-6　シングルスパニングツリーとの接続



（凡例）　●：アクセスポート

(2)　アクセスポートでシングルスパニングツリーを混在させた場合

PVST+とシングルスパニングツリーを混在して設定している場合，アクセスポートでは，シングルスパニングツリーは停止状態（Disable）になります。

(3)　構成不一致検出機能

同一 VLAN で接続しているポートについて，本装置でアクセスポート，プロトコルポート，MAC ポートのどれかを設定（Untagged フレームを使用）し，対向装置ではトランクポートを設定（Tagged フレームを使用）した場合，該当 VLAN では通信できないポートとなります。このようなポートを構成不一致として検出します。検出する条件は，本装置がアクセスポートで，対向装置でトランクポートを設定（Tagged フレームを使用）した場合です。この場合，該当するポートを停止状態（Disable）にします。対向装置でトランクポートの設定（Tagged フレームを使用）を削除すれば，hello-time 値×3 秒（デフォルトは 6 秒）後に，自動的に停止状態を解除します。

27.3.3　PVST+使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　VLAN 1（デフォルト VLAN）の PVST+とシングルスパニングツリーについて

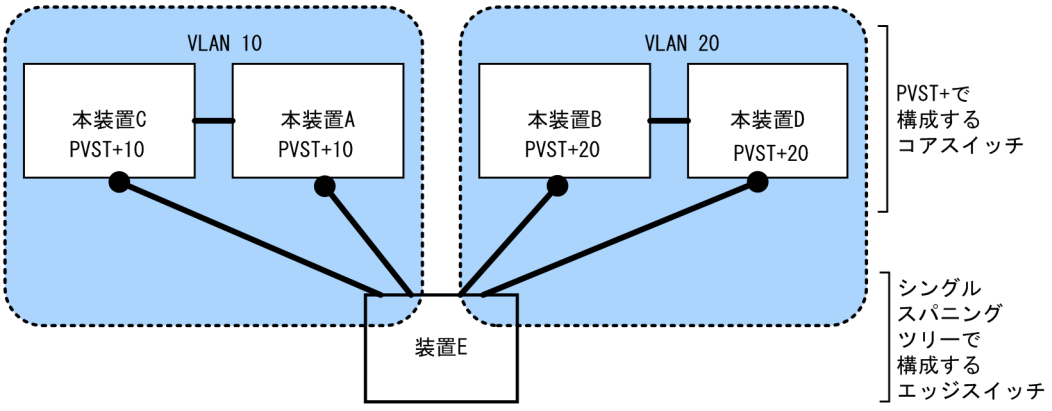
シングルスパニングツリーと VLAN 1 の PVST+を同時に動作させることはできません。シングルスパニングツリーを動作させると VLAN 1 の PVST+は停止します。

(3)　禁止構成

本装置とシングルスパニングツリーで動作する装置は，単一のスパニングツリーで構成してください。複数のスパニングツリーで構成すると正しいトポロジーになりません。

禁止構成の例を次の図に示します。この例では，装置 E のシングルスパニングツリーが複数の PVST+スパニングツリーとトポロジーを構成しているため，正しいトポロジーになりません。

図 27-7　シングルスパニングツリーとの禁止構成例



（凡例）　●：アクセスポート

装置Eは単一のスパニングツリーで構成されていないため，正しいトポロジーになりません。

27.4　PVST+のコンフィグレーション

27.4.1　コンフィグレーションコマンド一覧

PVST+のコンフィグレーションコマンド一覧を次の表に示します。

表 27-9　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree cost	ポートごとにパスコストのデフォルト値を設定します。
spanning-tree pathcost method	ポートごとにパスコストに使用する値の幅のデフォルト値を設定します。
spanning-tree port-priority	ポートごとにポート優先度のデフォルト値を設定します。
spanning-tree vlan	PVST+の動作，停止を設定します。
spanning-tree vlan cost	VLAN ごとにパスコスト値を設定します。
spanning-tree vlan forward-time	ポートの状態遷移に必要な時間を設定します。
spanning-tree vlan hello-time	BPDU の送信間隔を設定します。
spanning-tree vlan max-age	送信 BPDU の最大有効時間を設定します。
spanning-tree vlan pathcost method	VLAN ごとにパスコストに使用する値の幅を設定します。
spanning-tree vlan port-priority	VLAN ごとにポート優先度を設定します。
spanning-tree vlan priority	ブリッジ優先度を設定します。
spanning-tree vlan transmission-limit	hello-time 当たりに送信できる最大 BPDU 数を設定します。

27.4.2　PVST+の設定

[設定のポイント]

動作モード pvst，rapid-pvst を設定するとポート VLAN で自動的に PVST+が動作しますが，VLAN ごとにモードの変更や PVST+の動作，停止を設定できます。停止する場合は，no spanning-tree vlan コマンドを使用します。

VLAN を作成するときにその VLAN で PVST+を動作させたくない場合，no spanning-tree vlan コマンドを VLAN 作成前にあらかじめ設定しておくことができます。

[コマンドによる設定]

1. **(config)# no spanning-tree vlan 20**
   VLAN 20 の PVST+の動作を停止します。
2. **(config)# spanning-tree vlan 20**
   停止した VLAN 20 の PVST+を動作させます。

[注意事項]

- PVST+はコンフィグレーションに表示がないときは自動的に動作しています。no spanning-tree vlan コマンドで停止すると，停止状態であることがコンフィグレーションで確認できます。

- PVST+は最大 250 個のポート VLAN まで動作します。それ以上のポート VLAN を作成しても自動的には動作しません。

27.4.3　PVST+のトポロジー設定

(1)　ブリッジ優先度の設定

ブリッジ優先度は，ルートブリッジを決定するためのパラメータです。トポロジーを設計する際に，ルートブリッジにしたい装置を最高の優先度に設定し，ルートブリッジに障害が発生したときのために，次にルートブリッジにしたい装置を 2 番目の優先度に設定します。

[設定のポイント]

ブリッジ優先度は値が小さいほど高い優先度となり，最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置の MAC アドレスから成るブリッジ識別子で判定するため，本パラメータを設定しない場合は装置の MAC アドレスが最も小さい装置がルートブリッジになります。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 priority 4096**
   VLAN 10 の PVST+のブリッジ優先度を 4096 に設定します。

(2)　パスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジー設計において，ブリッジ優先度決定後に，指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

[設定のポイント]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによってルートポートに選択されやすくなります。設定しない場合，ポートの速度ごとに異なるデフォルト値になり，高速なポートほどルートポートに選択されやすくなります。

パスコストは，速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジーとする場合は設定する必要はありません。

パスコスト値には short（16bit 値），long（32bit 値）の 2 種類があり，トポロジーの全体で合わせる必要があります。速度が 10Gbit/s 以上のポートを使用する場合は long（32bit 値）を使用することをお勧めします。デフォルトでは short（16bit 値）で動作します。イーサネットインタフェースの速度による自動的な設定は，short（16bit 値）か long（32bit 値）かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 27-10　パスコストのデフォルト値

ポートの速度	パスコストのデフォルト値	
	short（16bit 値）	long（32bit 値）
10Mbit/s	100	2000000
100Mbit/s	19	200000
1Gbit/s	4	20000
10Gbit/s	2	2000

ポートの速度	パスコストのデフォルト値	
	short（16bit 値）	long（32bit 値）
40Gbit/s	2	500
100Gbit/s	2	200

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree cost 100
   (config-if)# exit
   ポート 1/0/1 のパスコストを 100 に設定します。
2. **(config)# spanning-tree pathcost method long**
   (config)# interface gigabitethernet 1/0/1
   (config-if)# spanning-tree vlan 10 cost 200000
   long（32bit 値）のパスコストを使用するように設定した後に，ポート 1/0/1 の VLAN 10 をコスト値 200000 に変更します。ポート 1/0/1 では VLAN 10 だけパスコスト 200000 となり，そのほかの VLAN は 100 で動作します。

[注意事項]

リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，チャネルグループ内の全ポートの合計ではなく一つのポートの速度の値となります。リンクアグリゲーションの異速度混在モードを使用している場合は，最も遅いポートの速度の値となります。

(3)　ポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し，パスコストも同じ値とする場合に，どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり，通常はリンクアグリゲーションを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていなくスパニングツリーで冗長化する必要がある場合に本機能を使用してください。

[設定のポイント]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に，ルートブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータを設定しない場合はポート番号の小さいポートが優先されます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 1/0/1 のポート優先度を 64 に設定します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree vlan 10 port-priority 144
   ポート 1/0/1 の VLAN 10 をポート優先度 144 に変更します。ポート 1/0/1 では VLAN 10 だけポート優先度 144 となり，そのほかの VLAN は 64 で動作します。

27.4.4　PVST+のパラメータ設定

各パラメータは「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time + 1)」という関係を満たすように設定する必要があります。パラメータを変える場合は，スパニングツリーを構築するすべての装置でパラメータを合わせる必要があります。

(1)　BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジー変更を検知しやすくなります。長くした場合はトポロジー変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリープログラムの負荷を軽減できます。

[設定のポイント]

設定しない場合，2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 hello-time 3**
   VLAN 10 の PVST+の BPDU 送信間隔を 3 秒に設定します。

[注意事項]

BPDU の送信間隔を短くすると，トポロジー変更を検知しやすくなる一方で BPDU トラフィックが増加することによりスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすることでタイムアウトのメッセージ出力やトポロジー変更が頻発する場合は，デフォルト値に戻して使用してください。

(2)　送信する最大 BPDU 数の設定

スパニングツリーでは，CPU 負荷の増大を抑えるために，hello-time（BPDU 送信間隔）当たりに送信する最大 BPDU 数を決めることができます。トポロジー変更が連続的に発生すると，トポロジー変更を通知，収束するために大量の BPDU が送信され，BPDU トラフィックの増加，CPU 負荷の増大につながります。送信する BPDU の最大数を制限することでこれらを抑えます。

[設定のポイント]

設定しない場合，hello-time（BPDU 送信間隔）当たりの最大 BPDU 数は 3 で動作します。本パラメータのコンフィグレーションは Rapid PVST+だけ有効であり，PVST+は 3（固定）で動作します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 transmission-limit 5**
   VLAN 10 の Rapid PVST+の hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

(3)　BPDU の最大有効時間の設定

ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加し，最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[設定のポイント]

最大有効時間を大きく設定することで，多くの装置に BPDU が届くようになります。設定しない場合，最大有効時間は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 max-age 25**
   VLAN 10 の PVST+の BPDU の最大有効時間を 25 に設定します。

(4) 状態遷移時間の設定

PVST+モードまたは Rapid PVST+モードでタイマによる動作となる場合，ポートの状態が一定時間ごとに遷移します。PVST+モードの場合は Blocking から Listening, Learning, Forwarding と遷移し, Rapid PVST+モードの場合は Discarding から Learning，Forwarding と遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

[設定のポイント]

設定しない場合, 状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合, BPDU の最大有効時間（max-age），送信間隔（hello-time）との関係が「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time + 1)」を満たすように設定してください。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 forward-time 10**
   VLAN 10 の PVST+の状態遷移時間を 10 に設定します。

27.5　PVST+のオペレーション

27.5.1　運用コマンド一覧

PVST+の運用コマンド一覧を次の表に示します。

表 27-11　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。
show spanning-tree statistics	スパニングツリーの統計情報を表示します。
clear spanning-tree statistics	スパニングツリーの統計情報をクリアします。
clear spanning-tree detected-protocol	スパニングツリーの STP 互換モードを強制回復します。
show spanning-tree port-count	スパニングツリーの収容数を表示します。
restart spanning-tree	スパニングツリープログラムを再起動します。
dump protocols spanning-tree	スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

27.5.2　PVST+の状態の確認

PVST+の情報は show spanning-tree コマンドの実行結果で示されます。Mode で PVST+，Rapid PVST+の動作モードを確認できます。トポロジーが正しく構築されていることを確認するためには，Root Bridge ID の内容が正しいこと，Port Information の Status，Role が正しいことを確認してください。

図 27-8　show spanning-tree コマンドの実行結果

```
> show spanning-tree vlan 1
Date 20XX/09/04 11:39:43 UTC
VLAN 1              PVST+ Spanning Tree:Enabled  Mode:PVST+
  Bridge ID        Priority:32769       MAC Address:0012.e205.0900
    Bridge Status:Designated
  Root Bridge ID   Priority:32769       MAC Address:0012.e201.0900
    Root Cost:1000
    Root Port:1/0/1
  Port Information
    1/0/1      Up    Status:Forwarding  Role:Root
    1/0/2      Up    Status:Forwarding  Role:Designated
    1/0/3      Up    Status:Blocking    Role:Alternate
    1/0/4      Down  Status:Disabled    Role:-
    1/0/10     Up    Status:Forwarding  Role:Designated PortFast
    1/0/11     Up    Status:Forwarding  Role:Designated PortFast
    1/0/12     Up    Status:Forwarding  Role:Designated PortFast
>
```

27.6　シングルスパニングツリー解説

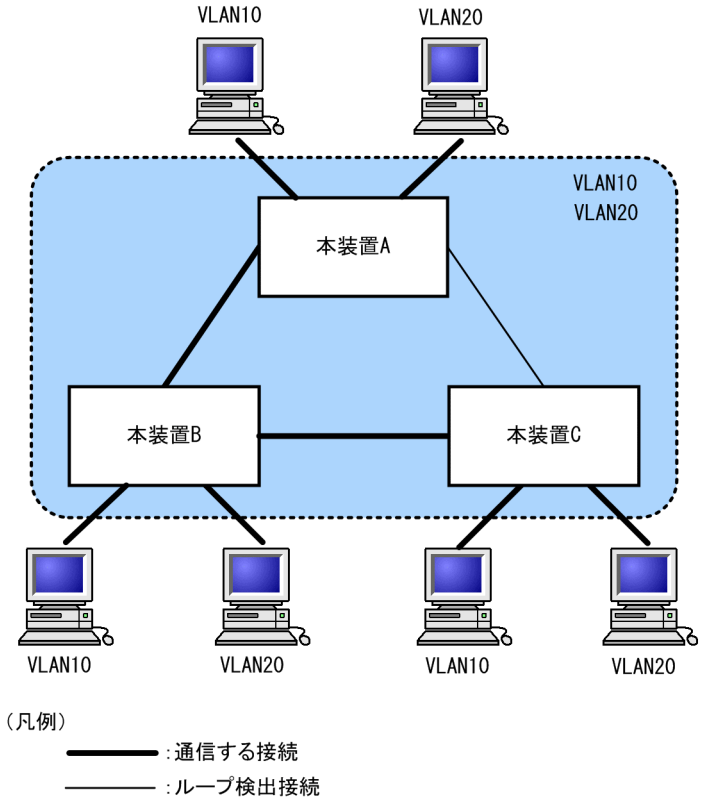
シングルスパニングツリーは装置全体を対象としトポロジーを構築します。

27.6.1　概要

シングルスパニングツリーは，一つのスパニングツリーですべての VLAN のループを回避できます。VLAN ごとに制御する PVST+よりも多くの VLAN を扱えます。

シングルスパニングツリーによるネットワーク構成を次の図に示します。この図では，本装置 A，B，C に対して，VLAN 10 および VLAN 20 を設定し，すべての VLAN で PVST+を停止しシングルスパニングツリーを適用しています。すべての VLAN で一つのトポロジーを使用して通信します。

図 27-9　シングルスパニングツリーによるネットワーク構成



27.6.2　PVST+との併用

プロトコル VLAN，MAC VLAN では PVST+を使用できません。また，PVST+が動作可能な VLAN 数は 250 個であり，それ以上の VLAN で使用することはできません。シングルスパニングツリーを使用することで，PVST+を使用しながらこれらの VLAN にもスパニングツリーを適用できます。

シングルスパニングツリーは，PVST+が動作していないすべての VLAN に対し適用します。次の表に，シングルスパニングツリーを PVST+と併用したときにシングルスパニングツリーの対象になる VLAN を示します。

表 27-12　シングルスパニングツリー対象の VLAN

項目	VLAN
PVST+対象の VLAN	PVST+が動作している VLAN。 最大 250 個のポート VLAN は自動的に PVST+が動作します。
シングルスパニングツリー対象の VLAN	251 個目以上のポート VLAN。
	PVST+を停止（no spanning-tree vlan コマンドで指定）している VLAN。
	デフォルト VLAN（VLAN ID 1 のポート VLAN）。
	プロトコル VLAN。
	MAC VLAN。

27.6.3　シングルスパニングツリー使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　VLAN 1（デフォルト VLAN）の PVST+とシングルスパニングツリーについて

シングルスパニングツリーと VLAN 1 の PVST+を同時に動作させることはできません。シングルスパニングツリーを動作させると VLAN 1 の PVST+は停止します。

27.7　シングルスパニングツリーのコンフィグレーション

27.7.1　コンフィグレーションコマンド一覧

シングルスパニングツリーのコンフィグレーションコマンド一覧を次の表に示します。

表 27-13　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree cost	ポートごとにパスコストのデフォルト値を設定します。
spanning-tree pathcost method	ポートごとにパスコストに使用する値の幅のデフォルト値を設定します。
spanning-tree port-priority	ポートごとにポート優先度のデフォルト値を設定します。
spanning-tree single	シングルスパニングツリーの動作，停止を設定します。
spanning-tree single cost	シングルスパニングツリーのパスコストを設定します。
spanning-tree single forward-time	ポートの状態遷移に必要な時間を設定します。
spanning-tree single hello-time	BPDU の送信間隔を設定します。
spanning-tree single max-age	送信 BPDU の最大有効時間を設定します。
spanning-tree single pathcost method	シングルスパニングツリーのパスコストに使用する値の幅を設定します。
spanning-tree single port-priority	シングルスパニングツリーのポート優先度を設定します。
spanning-tree single priority	ブリッジ優先度を設定します。
spanning-tree single transmission-limit	hello-time 当たりに送信できる最大 BPDU 数を設定します。

27.7.2　シングルスパニングツリーの設定

[設定のポイント]

シングルスパニングツリーの動作，停止を設定します。シングルスパニングツリーは，動作モード pvst，rapid-pvst を設定しただけでは動作しません。設定することによって動作を開始します。

VLAN 1（デフォルト VLAN）とシングルスパニングツリーは同時に使用できません。シングルスパニングツリーを設定すると VLAN 1 の PVST+は停止します。

[コマンドによる設定]

1. **(config)# spanning-tree single**

   シングルスパニングツリーを動作させます。この設定によって，VLAN 1 の PVST+が停止し，VLAN 1 はシングルスパニングツリーの対象となります。

2. **(config)# no spanning-tree single**

   シングルスパニングツリーを停止します。VLAN 1 の PVST+を停止に設定していないで，かつすでに 250 個の PVST+が動作している状態でない場合，VLAN 1 の PVST+が自動的に動作を開始します。

27.7.3　シングルスパニングツリーのトポロジー設定

(1)　ブリッジ優先度の設定

ブリッジ優先度は，ルートブリッジを決定するためのパラメータです。トポロジーを設計する際に，ルートブリッジにしたい装置を最高の優先度に設定し，ルートブリッジに障害が発生したときのために，次にルートブリッジにしたい装置を 2 番目の優先度に設定します。

[設定のポイント]

ブリッジ優先度は値が小さいほど高い優先度となり，最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置の MAC アドレスから成るブリッジ識別子で判定するため，本パラメータを設定しない場合は装置の MAC アドレスが最も小さい装置がルートブリッジになります。

[コマンドによる設定]

1. **(config)# spanning-tree single priority 4096**

   シングルスパニングツリーのブリッジ優先度を 4096 に設定します。

(2)　パスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジー設計において，ブリッジ優先度決定後に，指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

[設定のポイント]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによりルートポートに選択されやすくなります。設定しない場合，ポートの速度ごとに異なるデフォルト値になり，高速なポートほどルートポートに選択されやすくなります。

パスコストは，速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジーとする場合は設定する必要はありません。

パスコスト値には short（16bit 値），long（32bit 値）の 2 種類があり，トポロジーの全体で合わせる必要があります。速度が 10Gbit/s 以上のポートを使用する場合は long（32bit 値）を使用することをお勧めします。デフォルトでは short（16bit 値）で動作します。イーサネットインタフェースの速度による自動的な設定は，short（16bit 値）か long（32bit 値）かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 27-14　パスコストのデフォルト値

ポートの速度	パスコストのデフォルト値	
	short（16bit 値）	long（32bit 値）
10Mbit/s	100	2000000
100Mbit/s	19	200000
1Gbit/s	4	20000
10Gbit/s	2	2000
40Gbit/s	2	500
100Gbit/s	2	200

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree cost 100
   (config-if)# exit
   ポート 1/0/1 のパスコストを 100 に設定します。
2. **(config)# spanning-tree pathcost method long**
   (config)# interface gigabitethernet 1/0/1
   (config-if)# spanning-tree single cost 200000
   long（32bit 値）のパスコストを使用するように設定した後に，シングルスパニングツリーのポート 1/0/1 のパスコストを 200000 に変更します。ポート 1/0/1 ではシングルスパニングツリーだけパスコスト 200000 となり，同じポートで使用している PVST+は 100 で動作します。

[注意事項]

リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，チャネルグループ内の全ポートの合計ではなく一つのポートの速度の値になります。リンクアグリゲーションの異速度混在モードを使用している場合は，最も遅いポートの速度の値になります。

(3)　ポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し，パスコストも同じ値とする場合に，どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり，通常はリンクアグリゲーションを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていないで，スパニングツリーで冗長化する必要がある場合に本機能を使用してください。

[設定のポイント]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に，ルートブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータを設定しない場合はポート番号の小さいポートが優先されます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 1/0/1 のポート優先度を 64 に設定します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree single port-priority 144
   シングルスパニングツリーのポート 1/0/1 のポート優先度を 144 に変更します。ポート 1/0/1 ではシングルスパニングツリーだけポート優先度 144 となり，同じポートで使用している PVST+は 64 で動作します。

27.7.4　シングルスパニングツリーのパラメータ設定

各パラメータは「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time ＋ 1)」という関係が成立するように設定する必要があります。パラメータを変える場合はトポロジー全体でパラメータを合わせる必要があります。

(1)　BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジー変更を検知しやすくなります。長くした場合はトポロジー変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリープログラムの負荷を軽減できます。

[設定のポイント]

設定しない場合，2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree single hello-time 3**
   シングルスパニングツリーの BPDU 送信間隔を 3 秒に設定します。

[注意事項]

BPDU の送信間隔を短くすると，トポロジー変更を検知しやすくなる一方で BPDU トラフィックが増加することによりスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすることによってタイムアウトのメッセージ出力やトポロジー変更が頻発する場合は，デフォルト値に戻して使用してください。

(2)　送信する最大 BPDU 数の設定

スパニングツリーでは，CPU 負荷の増大を抑えるために，hello-time（BPDU 送信間隔）当たりに送信する最大 BPDU 数を決めることができます。トポロジー変更が連続的に発生すると，トポロジー変更を通知，収束するために大量の BPDU が送信され，BPDU トラフィックの増加，CPU 負荷の増大につながります。送信する BPDU の最大数を制限することでこれらを抑えます。

[設定のポイント]

設定しない場合，hello-time（BPDU 送信間隔）当たりの最大 BPDU 数は 3 で動作します。本パラメータのコンフィグレーションは Rapid STP だけ有効であり，STP は 3（固定）で動作します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree single transmission-limit 5**
   シングルスパニングツリーの hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

(3)　BPDU の最大有効時間

ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加し，最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[設定のポイント]

最大有効時間を大きく設定することで，多くの装置に BPDU が届くようになります。設定しない場合，最大有効時間は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree single max-age 25**
   シングルスパニングツリーの BPDU の最大有効時間を 25 に設定します。

(4)　状態遷移時間の設定

STP モードまたは Rapid STP モードでタイマによる動作となる場合，ポートの状態が一定時間ごとに遷移します。STP モードの場合は Blocking から Listening，Learning，Forwarding と遷移し，Rapid STP モードの場合は Discarding から Learning，Forwarding と遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

[設定のポイント]

設定しない場合，状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合，BPDU の最大有効時間（max-age），送信間隔（hello-time）との関係が「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time ＋ 1)」を満たすように設定してください。

[コマンドによる設定]

1. **(config)# spanning-tree single forward-time 10**
   シングルスパニングツリーの状態遷移時間を 10 に設定します。

27.8　シングルスパニングツリーのオペレーション

27.8.1　運用コマンド一覧

シングルスパニングツリーの運用コマンド一覧を次の表に示します。

表 27-15　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。
show spanning-tree statistics	スパニングツリーの統計情報を表示します。
clear spanning-tree statistics	スパニングツリーの統計情報をクリアします。
clear spanning-tree detected-protocol	スパニングツリーの STP 互換モードを強制回復します。
show spanning-tree port-count	スパニングツリーの収容数を表示します。
restart spanning-tree	スパニングツリープログラムを再起動します。
dump protocols spanning-tree	スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

27.8.2　シングルスパニングツリーの状態の確認

シングルスパニングツリーの情報は show spanning-tree コマンドで確認してください。Mode で STP，Rapid STP の動作モードを確認できます。トポロジーが正しく構築されていることを確認するためには，Root Bridge ID の内容が正しいこと，Port Information の Status，Role が正しいことを確認してください。

図 27-10　シングルスパニングツリーの情報

```
> show spanning-tree single
Date 20XX/09/04 11:42:06 UTC
Single Spanning Tree:Enabled  Mode:Rapid STP
  Bridge ID        Priority:32768       MAC Address:0012.e205.0900
    Bridge Status:Designated
  Root Bridge ID   Priority:32768       MAC Address:0012.e205.0900
    Root Cost:0
    Root Port:-
  Port Information
    1/0/1      Up    Status:Forwarding  Role:Root
    1/0/2      Up    Status:Forwarding  Role:Designated
    1/0/3      Up    Status:Blocking    Role:Alternate
    1/0/4      Down  Status:Disabled    Role:-
    1/0/10     Up    Status:Forwarding  Role:Designated PortFast
    1/0/11     Up    Status:Forwarding  Role:Designated PortFast
    1/0/12     Up    Status:Forwarding  Role:Designated PortFast
>
```

27.9　マルチプルスパニングツリー解説

27.9.1　概要

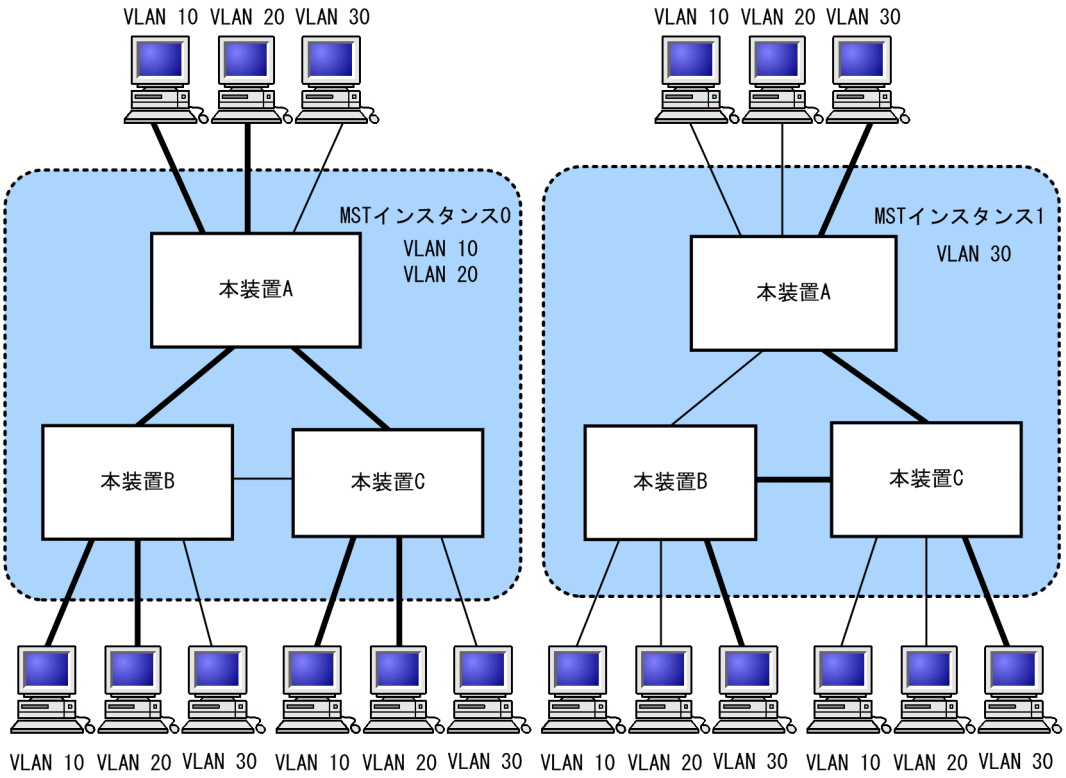
マルチプルスパニングツリーには，次の特長があります。MST インスタンスによってロードバランシングを可能にしています。また，MST リージョンによって，大規模なネットワーク構成を中小構成に分割することでネットワーク設計が容易になります。以降, これらを実現するためのマルチプルスパニングツリーの機能概要を説明します。

(1)　MST インスタンス

マルチプルスパニングツリーは, 複数の VLAN をまとめた MST インスタンス（MSTI：Multiple Spanning Tree Instance）というグループごとにスパニングツリーを構築でき，MST インスタンスごとにロードバランシングが可能です。PVST+によるロードバランシングでは，VLAN 数分のツリーが必要でしたが，マルチプルスパニングツリーでは MST インスタンスによって，計画したロードバランシングに従ったツリーだけで済みます。その結果, PVST+とは異なり VLAN 数の増加に比例した CPU 負荷およびネットワーク負荷の増加を抑えられます。本装置では最大 16 個の MST インスタンスが設定できます。

MST インスタンスイメージを次の図に示します。

図 27-11　MST インスタンスイメージ



(2)　MST リージョン

マルチプルスパニングツリーでは，複数の装置をグルーピングして MST リージョンとして扱えます。同一の MST リージョンに所属させるには，リージョン名，リビジョン番号，MST インスタンス ID と VLAN の対応を同じにする必要があります。これらはコンフィグレーションで設定します。ツリーの構築は MST リージョン間と MST リージョン内で別々に行い，MST リージョン内のトポロジーは MST インスタンス単位に構築できます。

次に，MST リージョン間や MST リージョン内で動作するスパニングツリーについて説明します。

- CST

  CST（Common Spanning Tree）は，MST リージョン間や，シングルスパニングツリーを使用しているブリッジ間の接続を制御するスパニングツリーです。このトポロジーはシングルスパニングツリーと同様で物理ポートごとに計算するのでロードバランシングすることはできません。

- IST

  IST（Internal Spanning Tree）は，MST リージョン外と接続するために，MST リージョン内で Default 動作するトポロジーのことを指し，MST インスタンス ID0 が割り当てられます。MST リージョン外と接続しているポートを境界ポートと呼びます。また，リージョン内，リージョン間で MST

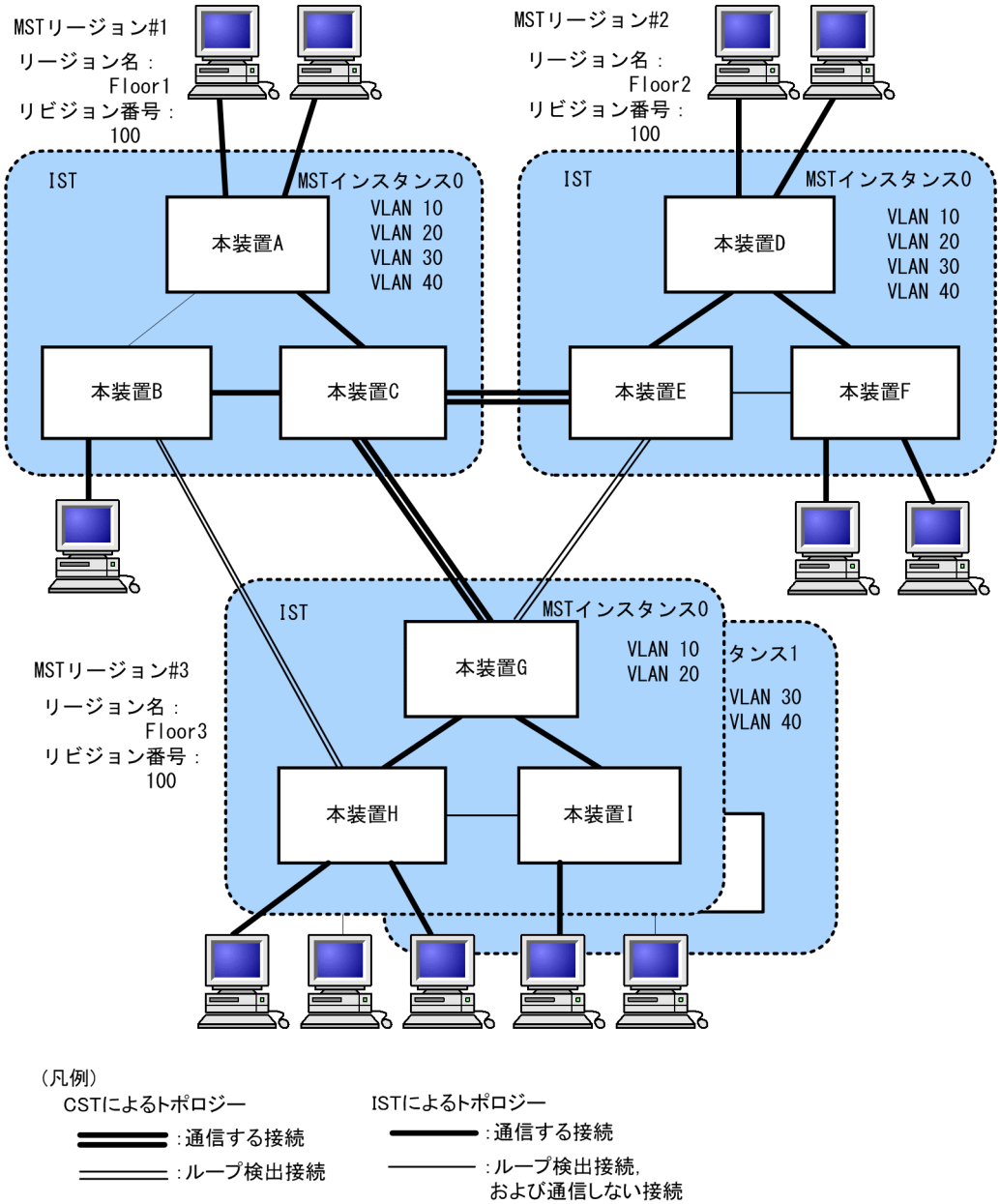
BPDU を送受信する唯一の MST インスタンスとなります。全 MST インスタンスのトポロジー情報は，MST BPDU にカプセル化し通知します。

- CIST

  CIST（Common and Internal Spanning Tree）は，IST と CST とを合わせたトポロジーを指します。

マルチプルスパニングツリー概要を次の図に示します。

図 27-12　マルチプルスパニングツリー概要

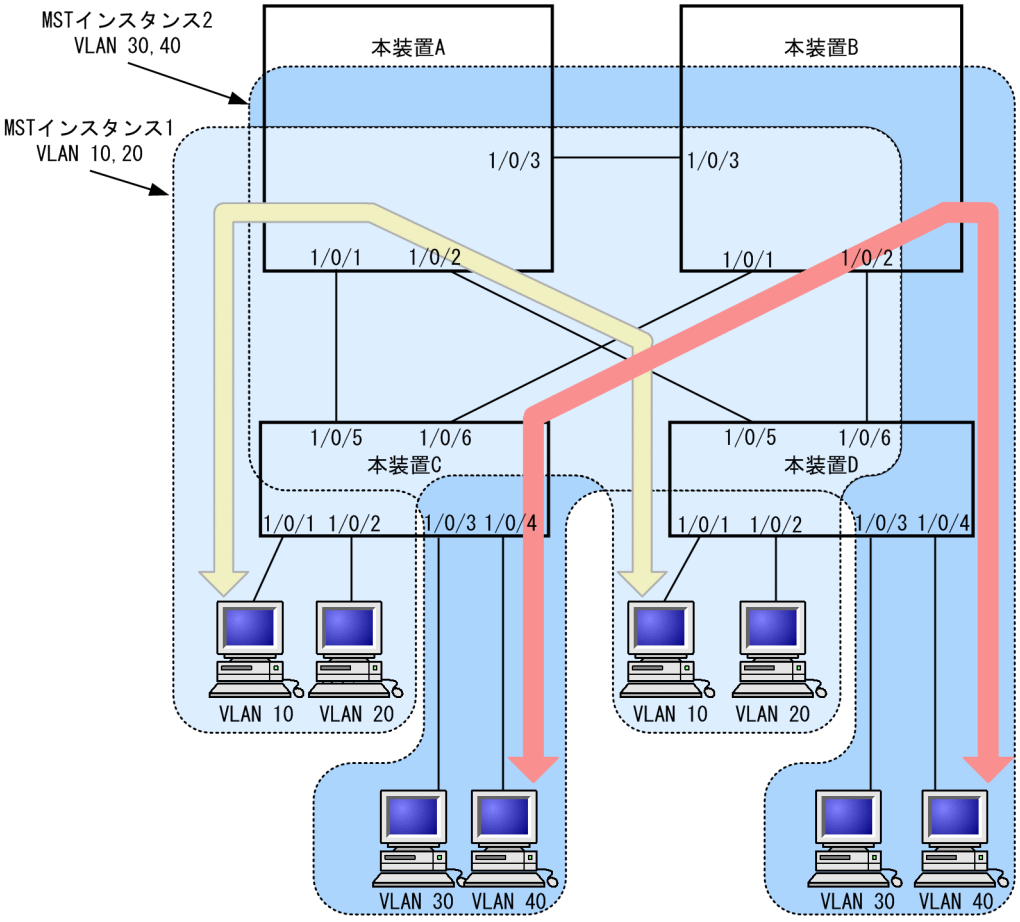


27.9.2　マルチプルスパニングツリーのネットワーク設計

(1)　MST インスタンス単位のロードバランシング構成

マルチプルスパニングツリーでは，MST インスタンス単位にロードバランシングができます。ロードバランシング構成の例を次の図に示します。この例では，VLAN 10，20 を MST インスタンス 1 に，VLAN 30，40 を MST インスタンス 2 に設定して，二つのロードバランシングを行っています。マルチプルスパニングツリーでは，この例のように四つの VLAN であっても二つのツリーだけを管理することでロードバランシングができます。

図 27-13　マルチプルスパニングツリーのロードバランシング構成



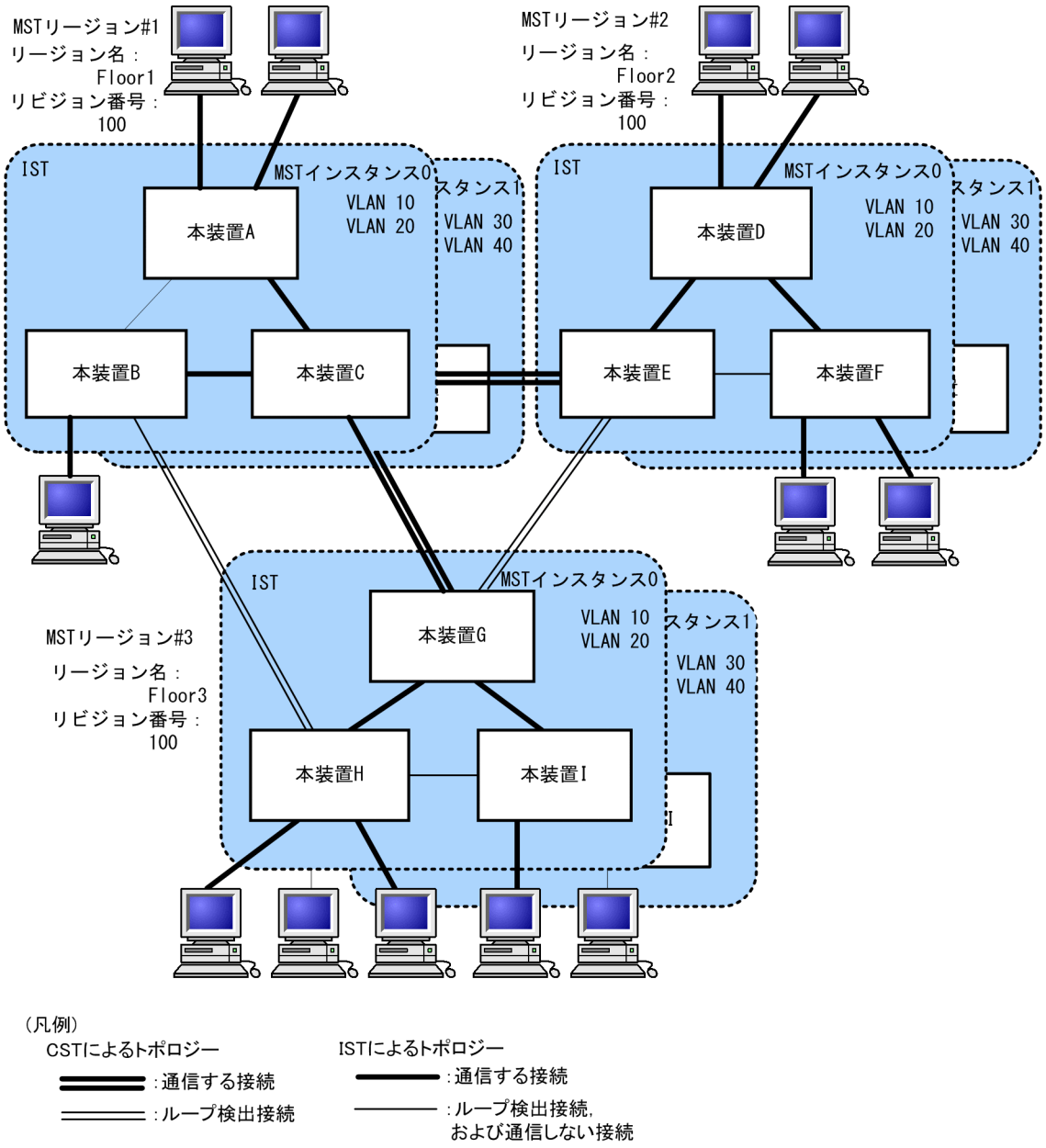
本装置Cと本装置Dに接続しているVLAN10の端末の通信経路と，本装置Cと本装置Dに接続しているVLAN40の端末で通信経路をロードバランシングしています。

(2)　MST リージョンによるネットワーク設計

ネットワーク構成が大規模になるに従ってネットワーク設計は複雑になりますが，MST リージョンによって中小規模構成に分割することで，例えば，ロードバランシングを MST リージョン単位に実施できるため，ネットワーク設計が容易になります。

MST リージョンによるネットワーク設計例を次の図に示します。この例では，装置 A，B，C を MST リージョン#1，装置 D，E，F を MST リージョン#2，本装置 G，H，I を MST リージョン#3 に設定して，ネットワークを三つの MST リージョンに分割しています。

図 27-14　MST リージョンによるネットワーク構成



27.9.3　ほかのスパニングツリーとの互換性

(1)　シングルスパニングツリーとの互換性

マルチプルスパニングツリーは，シングルスパニングツリーで動作する STP，Rapid STP と互換性があります。これらと接続した場合，別の MST リージョンと判断し接続します。Rapid STP と接続した場合は高速な状態遷移を行います。

(2)　PVST+との互換性

マルチプルスパニングツリーは，PVST+と互換性はありません。ただし，PVST+が動作している装置のアクセスポートはシングルスパニングツリーと同等の動作をするため，マルチプルスパニングツリーと接続できます。

27.9.4　マルチプルスパニングツリー使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　MST リージョンについて

本装置と他装置で扱える VLAN の範囲が異なることがあります。そのような装置を同じ MST リージョンとして扱いたい場合は，該当 VLAN を MST インスタンス 0 に所属させてください。

(3)　トポロジーの収束に時間が掛かる場合について

CIST のルートブリッジまたは MST インスタンスのルートブリッジで，次の表に示すイベントが発生すると，トポロジーが落ち着くまでに時間が掛かる場合があります。その間，通信が途絶えたり，MAC アドレステーブルのクリアが発生したりします。

表 27-16　ルートブリッジでのイベント発生

イベント	内容	イベントの発生したルートブリッジ種別	影響トポロジー
コンフィグレーション変更	リージョン名(1)，リビジョン番号(2)，またはインスタンス番号と VLAN の対応(3)をコンフィグレーションで変更し，リージョンを分割または同じにする場合 (1) MST コンフィグレーションモードの name コマンド (2) MST コンフィグレーションモードの revision コマンド (3) MST コンフィグレーションモードの instance コマンド	CIST のルートブリッジ	CIST
		MST インスタンス 0 (IST) でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス
	ブリッジ優先度を spanning-tree mst root priority コマンドで下げた（現状より大きな値を設定した）場合	CIST のルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス
その他	本装置が停止した場合	CIST のルートブリッジ	CIST
		MST インスタンス 0 (IST) でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス
	本装置と接続している対向装置で，ループ構成となっている本装置の全ポートがダウンした場合（本装置が当該ループ構成上ルートブリッジではなくなった場合）	CIST のルートブリッジ	CIST
		MST インスタンス 0 (IST) でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	当該 MST インスタンス

27.10　マルチプルスパニングツリーのコンフィグレーション

27.10.1　コンフィグレーションコマンド一覧

マルチプルスパニングツリーのコンフィグレーションコマンド一覧を次の表に示します。

表 27-17　コンフィグレーションコマンド一覧

コマンド名	説明
instance	マルチプルスパニングツリーの MST インスタンスに所属する VLAN を設定します。
name	マルチプルスパニングツリーのリージョンを識別するための文字列を設定します。
revision	マルチプルスパニングツリーのリージョンを識別するためのリビジョン番号を設定します。
spanning-tree cost	ポートごとにパスコストのデフォルト値を設定します。
spanning-tree mode	スパニングツリー機能の動作モードを設定します。
spanning-tree mst configuration	マルチプルスパニングツリーの MST リージョンの形成に必要な情報を設定します。
spanning-tree mst cost	マルチプルスパニングツリーの MST インスタンスごとのパスコストを設定します。
spanning-tree mst forward-time	ポートの状態遷移に必要な時間を設定します。
spanning-tree mst hello-time	BPDU の送信間隔を設定します。
spanning-tree mst max-age	送信 BPDU の最大有効時間を設定します。
spanning-tree mst max-hops	MST リージョン内での最大ホップ数を設定します。
spanning-tree mst port-priority	マルチプルスパニングツリーの MST インスタンスごとのポート優先度を設定します。
spanning-tree mst root priority	MST インスタンスごとのブリッジ優先度を設定します。
spanning-tree mst transmission-limit	hello-time 当たりに送信できる最大 BPDU 数を設定します。
spanning-tree port-priority	ポートごとにポート優先度のデフォルト値を設定します。

27.10.2　マルチプルスパニングツリーの設定

(1)　マルチプルスパニングツリーの設定

[設定のポイント]

スパニングツリーの動作モードをマルチプルスパニングツリーに設定すると，PVST+，シングルスパニングツリーはすべて停止し，マルチプルスパニングツリーの動作を開始します。

[コマンドによる設定]

1. **(config)# spanning-tree mode mst**

   マルチプルスパニングツリーを使用するように設定し，CIST が動作を開始します。

[注意事項]

no spanning-tree mode コマンドでマルチプルスパニングツリーの動作モード設定を削除すると，デフォルトの動作モードである pvst になります。その際，ポート VLAN で自動的に PVST+が動作を開始します。

(2)　リージョン，インスタンスの設定

[設定のポイント]

MST リージョンは，同じリージョンに所属させたい装置はリージョン名，リビジョン番号，MST インスタンスのすべてを同じ設定にする必要があります。

MST インスタンスは，インスタンス番号と所属する VLAN を同時に設定します。リージョンを一致させるために，本装置に未設定の VLAN ID もインスタンスに所属させることができます。インスタンスに所属することを指定しない VLAN は自動的に CIST（インスタンス 0）に所属します。

MST インスタンスは，CIST（インスタンス 0）を含め 16 個まで設定できます。

[コマンドによる設定]

1. **(config)# spanning-tree mst configuration**

   (config-mst)# name "REGION TOKYO"

   (config-mst)# revision 1

   マルチプルスパニングツリーコンフィグレーションモードに移り，name（リージョン名），revision（リビジョン番号）の設定を行います。

2. **(config-mst)# instance 10 vlans 100-150**

   (config-mst)# instance 20 vlans 200-250

   (config-mst)# instance 30 vlans 300-350

   インスタンス 10，20，30 を設定し，各インスタンスに所属する VLAN を設定します。インスタンス 10 に VLAN 100～150, インスタンス 20 に VLAN 200～250, インスタンス 30 に VLAN 300～350 を設定します。指定していないそのほかの VLAN は CIST（インスタンス 0）に所属します。

27.10.3　マルチプルスパニングツリーのトポロジー設定

(1)　インスタンスごとのブリッジ優先度の設定

ブリッジ優先度は，ルートブリッジを決定するためのパラメータです。トポロジーを設計する際に，ルートブリッジにしたい装置を最高の優先度に設定し，ルートブリッジに障害が発生したときのために，次にルートブリッジにしたい装置を 2 番目の優先度に設定します。

[設定のポイント]

ブリッジ優先度は値が小さいほど高い優先度になり，最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置の MAC アドレスから成るブリッジ識別子で判定するため，本パラメータを設定しない場合は装置の MAC アドレスが最も小さい装置がルートブリッジになります。

マルチプルスパニングツリーのブリッジ優先度はインスタンスごとに設定します。インスタンスごとに値を変えた場合，インスタンスごとのロードバランシング（異なるトポロジーの構築）ができます。

[コマンドによる設定]

1. **(config)# spanning-tree mst 0 root priority 4096**
   (config)# spanning-tree mst 20 root priority 61440
   CIST（インスタンス 0）のブリッジ優先度を 4096 に，インスタンス 20 のブリッジ優先度を 61440 に設定します。

(2)　インスタンスごとのパスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジー設計において，ブリッジ優先度決定後に，指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

[設定のポイント]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによってルートポートに選択されやすくなります。設定しない場合，ポートの速度ごとに異なるデフォルト値になり，高速なポートほどルートポートに選択されやすくなります。

パスコストは，速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジーとする場合は設定する必要はありません。

パスコストのデフォルト値を次の表に示します。

表 27-18　パスコストのデフォルト値

ポートの速度	パスコストのデフォルト値
10Mbit/s	2000000
100Mbit/s	200000
1Gbit/s	20000
10Gbit/s	2000
40Gbit/s	500
100Gbit/s	200

[コマンドによる設定]

1. **(config)# spanning-tree mst configuration**
   (config-mst)# instance 10 vlans 100-150
   (config-mst)# instance 20 vlans 200-250
   (config-mst)# instance 30 vlans 300-350
   (config-mst)# exit
   (config)# interface gigabitethernet 1/0/1
   (config-if)# spanning-tree cost 2000
   MST インスタンス 10，20，30 を設定し，ポート 1/0/1 のパスコストを 2000 に設定します。CIST（インスタンス 0），MST インスタンス 10，20，30 のポート 1/0/1 のパスコストは 2000 になります。
2. **(config-if)# spanning-tree mst 20 cost 500**
   MST インスタンス 20 のポート 1/0/1 のパスコストを 500 に変更します。インスタンス 20 以外は 2000 で動作します。

[注意事項]

リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，チャネルグループ内の全ポートの合計ではなく，一つのポートの速度の値となります。リンクアグリゲーションの異速度混在モードを使用している場合は，最も遅いポートの速度の値となります。

(3)　インスタンスごとのポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し，パスコストも同じ値とする場合に，どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり，通常はリンクアグリゲーションを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていなくスパニングツリーで冗長化する必要がある場合に本機能を使用してください。

[設定のポイント]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に，ルートブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータを設定しない場合はポート番号の小さいポートが優先されます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 1/0/1 のポート優先度を 64 に設定します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# spanning-tree mst 20 port-priority 144
   インスタンス 20 のポート 1/0/1 にポート優先度 144 を設定します。ポート 1/0/1 ではインスタンス 20 だけポート優先度 144 となり，そのほかのインスタンスは 64 で動作します。

27.10.4　マルチプルスパニングツリーのパラメータ設定

各パラメータは「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time ＋ 1)」という関係が成立するように設定する必要があります。パラメータを変える場合はトポロジー全体でパラメータを合わせる必要があります。

(1)　BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジー変更を検知しやすくなります。長くした場合はトポロジー変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリープログラムの負荷を軽減できます。

[設定のポイント]

設定しない場合，2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree mst hello-time 3**
   マルチプルスパニングツリーの BPDU 送信間隔を 3 秒に設定します。

[注意事項]

BPDU の送信間隔を短くすると，トポロジー変更を検知しやすくなる一方で BPDU トラフィックが増加することによりスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値（2秒）より短くすることによってタイムアウトのメッセージ出力やトポロジー変更が頻発する場合は，デフォルト値に戻して使用してください。

(2) 送信する最大 BPDU 数の設定

スパニングツリーでは，CPU 負荷の増大を抑えるために，hello-time（BPDU 送信間隔）当たりに送信する最大 BPDU 数を決めることができます。トポロジー変更が連続的に発生すると，トポロジー変更を通知，収束するために大量の BPDU が送信され，BPDU トラフィックの増加，CPU 負荷の増大につながります。送信する BPDU の最大数を制限することによりこれらを抑えます。

[設定のポイント]

設定しない場合，hello-time（BPDU 送信間隔）当たりの最大 BPDU 数は 3 で動作します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree mst transmission-limit 5**
   マルチプルスパニングツリーの hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

(3) 最大ホップ数の設定

ルートブリッジから送信する BPDU の最大ホップ数を設定します。BPDU のカウンタは装置を経由するたびに増加し，最大ホップ数を超えた BPDU は無効な BPDU となって無視されます。

シングルスパニングツリーの装置と接続しているポートは，最大ホップ数（max-hops）ではなく最大有効時間（max-age）のパラメータを使用します。ホップ数のカウントはマルチプルスパニングツリーの装置間で有効なパラメータです。

[設定のポイント]

最大ホップ数を大きく設定することによって，多くの装置に BPDU が届くようになります。設定しない場合，最大ホップ数は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree mst max-hops 10**
   マルチプルスパニングツリーの BPDU の最大ホップ数を 10 に設定します。

(4) BPDU の最大有効時間の設定

マルチプルスパニングツリーでは，最大有効時間（max-age）はシングルスパニングツリーの装置と接続しているポートでだけ有効なパラメータです。トポロジー全体をマルチプルスパニングツリーが動作している装置で構成する場合は設定する必要はありません。

最大有効時間は，ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加して，最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[設定のポイント]

最大有効時間を大きく設定することで，多くの装置に BPDU が届くようになります。設定しない場合，最大有効時間は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree mst max-age 25**
   マルチプルスパニングツリーの BPDU の最大有効時間を 25 に設定します。

(5)　状態遷移時間の設定

タイマによる動作となる場合，ポートの状態が Discarding から Learning，Forwarding へ一定時間ごとに遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

[設定のポイント]

設定しない場合，状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合，BPDU の最大有効時間（max-age），送信間隔（hello-time）との関係が「2×(forward-time－1) ≧ max-age ≧ 2×(hello-time ＋ 1)」を満たすように設定してください。

[コマンドによる設定]

1. **(config)# spanning-tree mst forward-time 10**
   マルチプルスパニングツリーの状態遷移時間を 10 に設定します。

27.11　マルチプルスパニングツリーのオペレーション

27.11.1　運用コマンド一覧

マルチプルスパニングツリーの運用コマンド一覧を次の表に示します。

表 27-19　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。
show spanning-tree statistics	スパニングツリーの統計情報を表示します。
clear spanning-tree statistics	スパニングツリーの統計情報をクリアします。
clear spanning-tree detected-protocol	スパニングツリーの STP 互換モードを強制回復します。
show spanning-tree port-count	スパニングツリーの収容数を表示します。
restart spanning-tree	スパニングツリープログラムを再起動します。
dump protocols spanning-tree	スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

27.11.2　マルチプルスパニングツリーの状態の確認

マルチプルスパニングツリーの情報は show spanning-tree コマンドで確認してください。トポロジーが正しく構築されていることを確認するためには，次の項目を確認してください。

- リージョンの設定（Revision Level，Configuration Name，MST Instance の VLAN Mapped）が正しいこと
- Regional Root の内容が正しいこと
- Port Information の Status，Role が正しいこと

show spanning-tree コマンドの実行結果を次の図に示します。

図 27-15　show spanning-tree コマンドの実行結果

```
> show spanning-tree mst
Date 20XX/09/04 11:41:03 UTC
Multiple Spanning Tree: Enabled
Revision Level: 65535  Configuration Name: MSTP001
CIST Information
  VLAN Mapped: 1-99,151-4095                                          …1
  CIST Root      Priority: 32768       MAC      : 0012.e207.7200
  External Root Cost     : 2000        Root Port: 1/0/1
  Regional Root  Priority: 32768       MAC      : 0012.e207.7200
  Internal Root Cost     : 0
  Bridge ID      Priority: 32768       MAC      : 0012.e205.0900
  Regional Bridge Status : Designated
  Port Information
    1/0/1      Up   Status:Forwarding  Role:Root
    1/0/2      Up   Status:Discarding  Role:Backup
    1/0/3      Up   Status:Discarding  Role:Alternate
    1/0/4      Up   Status:Forwarding  Role:Designated
MST Instance 10
  VLAN Mapped: 100-150
  Regional Root  Priority: 32778       MAC      : 0012.e207.7200
  Internal Root Cost     : 2000        Root Port: 1/0/1
```

```
  Bridge ID      Priority: 32778       MAC      : 0012.e205.0900
  Regional Bridge Status : Designated
  Port Information
    1/0/1      Up   Status:Forwarding  Role:Root
    1/0/2      Up   Status:Discarding  Role:Backup
    1/0/3      Up   Status:Discarding  Role:Alternate
    1/0/4      Up   Status:Forwarding  Role:Designated
>
```

1. インスタンスマッピング VLAN（VLAN Mapped）の表示について

   本装置は 1～4094 の VLAN ID をサポートしていますが，リージョンの設定に用いる VLAN ID は規格に従い 1～4095 としています。表示は規格がサポートする VLAN ID1～4095 がどのインスタンスに所属しているか確認できるようにするため 1～4095 を明示します。

27.12　スパニングツリー共通機能解説

27.12.1　PortFast

(1)　概要

PortFast は，端末が接続されループが発生しないことがあらかじめわかっているポートのための機能です。PortFast はスパニングツリーのトポロジー計算対象外となり，リンクアップ後すぐに通信できる状態になります。

(2)　PortFast 適用時の BPDU 受信

PortFast を設定したポートは BPDU を受信しないことを想定したポートですが，もし，PortFast を設定したポートで BPDU を受信した場合は，その先にスイッチが存在しループの可能性があることになります。そのため，PortFast 機能を停止し，トポロジー計算や BPDU の送受信など，通常のスパニングツリー対象のポートとしての動作を開始します。

いったんスパニングツリー対象のポートとして動作を開始した後，リンクのダウン／アップによって再び PortFast 機能が有効になります。

なお，BPDU を受信したときに PortFast 機能を停止しないようにする場合は，BPDU フィルタ機能を併用してください。

(3)　PortFast 適用時の BPDU 送信

PortFast を設定したポートではスパニングツリーを動作させないため，BPDU の送信は行いません。

ただし，PortFast を設定したポート同士を誤って接続した状態を検出するために，PortFast 機能によって即時に通信可状態になった時点から 10 フレームだけ BPDU の送信を行います。

(4)　BPDU ガード

PortFast に適用する機能として，BPDU ガード機能があります。BPDU ガード機能を適用したポートでは，BPDU 受信時に，スパニングツリー対象のポートとして動作するのではなくポートを inactive 状態にします。

inactive 状態にしたポートを activate コマンドで解放することによって，再び BPDU ガード機能を適用した PortFast としてリンクアップして通信を開始します。

27.12.2　BPDU フィルタ

(1)　概要

BPDU フィルタ機能を適用したポートでは，BPDU の送受信を停止します。BPDU フィルタ機能は，端末が接続されループが発生しないことがあらかじめわかっている，PortFast を設定したポートに適用します。

(2)　BPDU フィルタに関する注意事項

PortFast を適用したポート以外に BPDU フィルタ機能を設定した場合，BPDU の送受信を停止するため，タイマによるポートの状態遷移が終了するまで通信断になります。

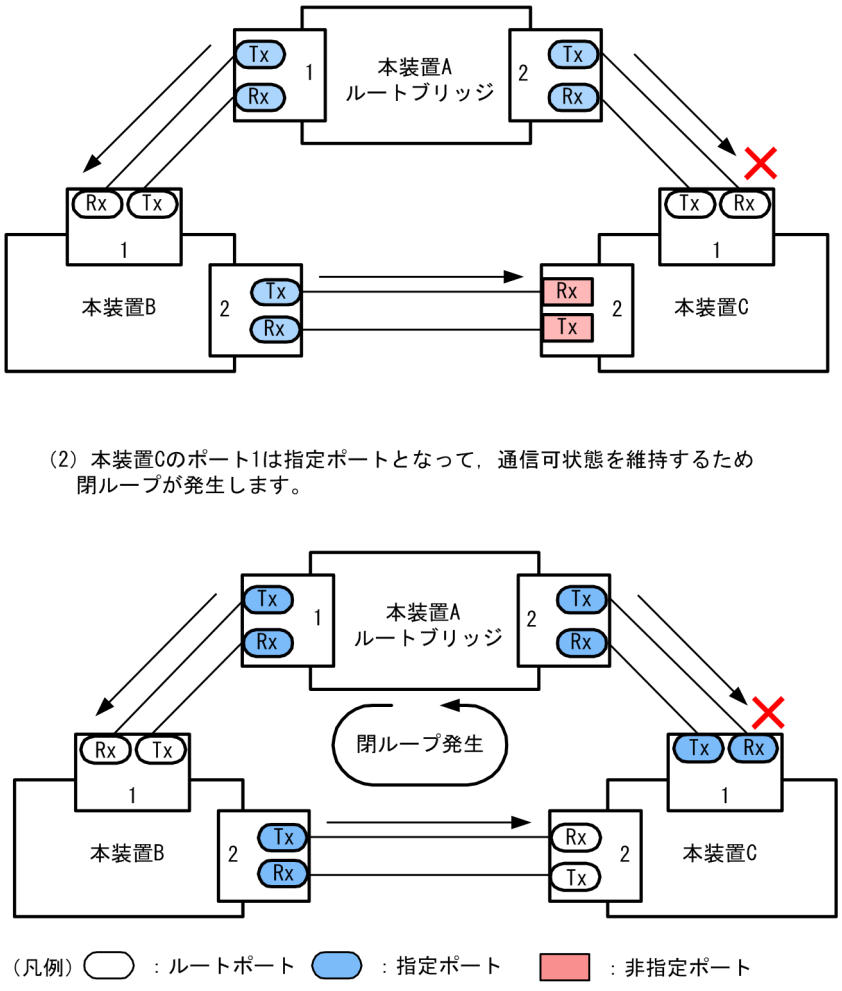
27.12.3　ループガード

(1)　概要

片線切れなどの単一方向のリンク障害が発生し，BPDU の受信が途絶えた場合，ループが発生することがあります。ループガード機能は，このような場合にループの発生を防止する機能です。

次の図に単一方向のリンク障害時の問題点を示します。

図 27-16　単一方向のリンク障害時の問題点



ループガード機能とは BPDU の受信が途絶えたポートの状態を，再度 BPDU を受信するまで転送不可状態に遷移させる機能です。BPDU 受信を開始した場合は通常のスパニングツリー対象のポートとしての動作を開始します。

ループガード機能は,端末を接続するポートを指定する機能である PortFast を設定したポート,またはルートガード機能を設定したポートには設定できません。

(2)　ループガードに関する注意事項

ループガードはマルチプルスパニングツリーでは使用できません。

ループガード機能を設定したあと，次に示すイベントが発生すると，ループガードが動作してポートをブロックします。その後，BPDU を受信するまで，ループガードは解除されません。

- 装置起動
- ポートのアップ（リンクアグリゲーションのアップも含む）
- スパニングツリープログラムの再起動
- スパニングツリープロトコルの種別変更（STP/高速 STP，PVST+/高速 PVST+）

なお，ループガード機能は，指定ポートだけでなく対向装置にも設定してください。指定ポートだけに設定すると，上記のイベントが発生しても，指定ポートは BPDU を受信しないことがあります。このような場合，ループガードの解除に時間が掛かります。ループガードを解除するには，対向装置のポートで BPDU 受信タイムアウトを検出したあとの BPDU の送信を待つ必要があるためです。

また，両ポートにループガードを設定した場合でも，指定ポートで BPDU を一度も受信せずに，ループガードの解除に時間が掛かることがあります。具体的には，対向ポートが指定ポートとなるようにブリッジやポートの優先度，パスコストを変更した場合です。対向ポートで BPDU タイムアウトを検出し，ループガードが動作します。このポートが指定ポートになった場合，BPDU を受信しないことがあり，ループガードの解除に時間が掛かることがあります。

運用中にループガード機能を設定した場合，その時点では，ループガードは動作しません。運用中に設定したループガードは，BPDU の受信タイムアウトが発生した時に動作します。

本装置と対向装置のポート間に BPDU を中継しない装置が存在し，かつポートの両端にループガード機能を設定した状態でポートがリンクアップした場合，両端のポートはループガードが動作したままになります。復旧するには，ポート間に存在する装置の BPDU 中継機能を有効にし，再度ポートをリンクアップさせる必要があります。

27.12.4　ルートガード

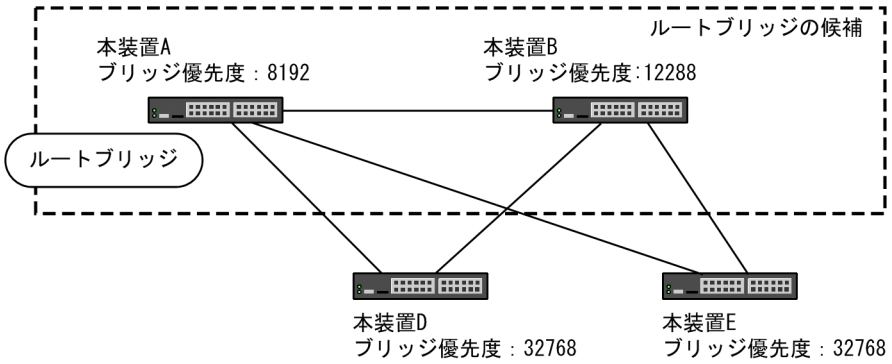
(1)　概要

ネットワークの管理の届かない個所で誤って装置が接続された場合や設定が変更された場合，意図しないトポロジーになることがあります。意図しないトポロジーのルートブリッジの性能が低い場合，トラフィックが集中するとネットワーク障害のおそれがあります。ルートガード機能は，このようなときのためにルートブリッジの候補を特定しておくことによって，ネットワーク障害を回避する機能です。

誤って装置が接続されたときの問題点を次の図に示します。

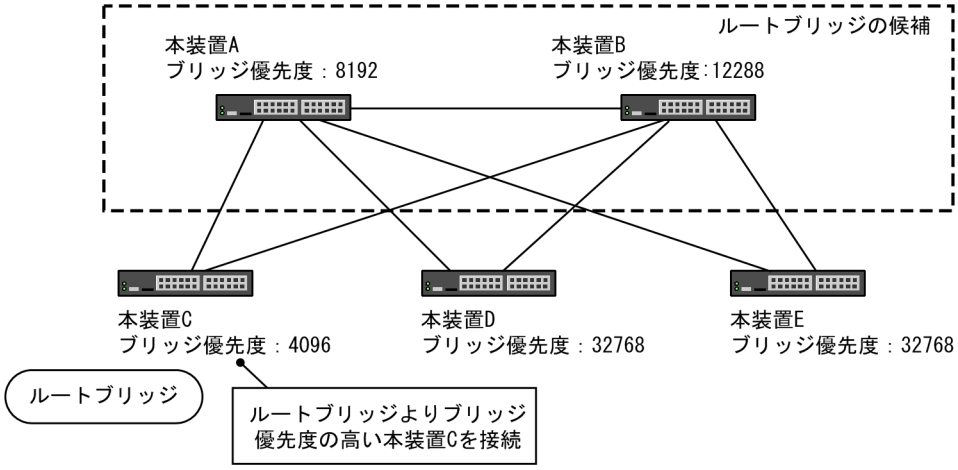
- 本装置 A，本装置 B をルートブリッジの候補として運用

図 27-17　本装置 A，本装置 B をルートブリッジの候補として運用



- 本装置 A，本装置 B よりブリッジ優先度の高い本装置 C を接続すると，本装置 C がルートブリッジになり，本装置 C にトラフィックが集中するようになる

図 27-18　本装置 A，本装置 B よりブリッジ優先度の高い本装置 C を接続



ルートガード機能は，現在のルートブリッジよりも優先度の高いブリッジを検出し，BPDU を廃棄することによってトポロジーを保護します。また，該当するポートをブロック状態に設定することでループを回避します。ルートガード機能は，ループガード機能を設定したポートには設定できません。

27.13　スパニングツリー共通機能のコンフィグレーション

27.13.1　コンフィグレーションコマンド一覧

スパニングツリー共通機能のコンフィグレーションコマンド一覧を次の表に示します。

表 27-20　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree bpdufilter	ポートごとに BPDU フィルタ機能を設定します。
spanning-tree bpduguard	ポートごとに BPDU ガード機能を設定します。
spanning-tree guard	ポートごとにループガード機能，ルートガード機能を設定します。
spanning-tree link-type	ポートのリンクタイプを設定します。
spanning-tree loopguard default	ループガード機能をデフォルトで使用するように設定します。
spanning-tree portfast	ポートごとに PortFast 機能を設定します。
spanning-tree portfast bpduguard default	BPDU ガード機能をデフォルトで使用するように設定します。
spanning-tree portfast default	PortFast 機能をデフォルトで使用するように設定します。

27.13.2　PortFast の設定

(1)　PortFast の設定

PortFast は，端末を接続するポートなど，ループが発生しないことがあらかじめわかっているポートを直ちに通信できる状態にしたい場合に適用します。

[設定のポイント]

spanning-tree portfast default コマンドを設定すると，アクセスポート，プロトコルポート，MAC ポートにデフォルトで PortFast 機能を適用します。デフォルトで適用してポートごとに無効にしたい場合は，spanning-tree portfast disable コマンドを設定します。

トランクポートでは，ポートごとの指定で適用できます。

[コマンドによる設定]

1. **(config)# spanning-tree portfast default**

   すべてのアクセスポート，プロトコルポート，MAC ポートに対して PortFast 機能を適用するように設定します。

2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# switchport mode access
   (config-if)# spanning-tree portfast disable
   (config-if)# exit

   ポート 1/0/1（アクセスポート）で PortFast 機能を使用しないように設定します。

3. **(config)# interface gigabitethernet 1/0/3**

```
(config-if)# switchport mode trunk
(config-if)# spanning-tree portfast trunk
```

ポート 1/0/3 をトランクポートに指定し，PortFast 機能を適用します。トランクポートはデフォルトでは適用されません。ポートごとに指定するためには trunk パラメータを指定する必要があります。

(2)　BPDU ガードの設定

BPDU ガード機能は，PortFast を適用したポートで BPDU を受信した場合にそのポートを inactive 状態にします。通常，PortFast 機能は冗長経路ではないポートを指定し，ポートの先にはスパニングツリー装置がないことを前提とします。BPDU を受信したことによる意図しないトポロジー変更を回避したい場合に設定します。

[設定のポイント]

BPDU ガード機能を設定するためには，PortFast 機能を同時に設定する必要があります。spanning-tree portfast bpduguard default コマンドは PortFast 機能を適用しているすべてのポートにデフォルトで BPDU ガードを適用します。デフォルトで適用するときに BPDU ガード機能を無効にしたい場合は，spanning-tree bpduguard disable コマンドを設定します。

[コマンドによる設定]

1.
```
(config)# spanning-tree portfast default
(config)# spanning-tree portfast bpduguard default
```

すべてのアクセスポート，プロトコルポート，MAC ポートに対して PortFast 機能を設定します。また，PortFast 機能を適用したすべてのポートに対し BPDU ガード機能を設定します。

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# spanning-tree bpduguard disable
(config-if)# exit
```

ポート 1/0/1(アクセスポート) で BPDU ガード機能を使用しないように設定します。ポート 1/0/1 は通常の PortFast 機能を適用します。

3.
```
(config)# interface gigabitethernet 1/0/2
(config-if)# switchport mode trunk
(config-if)# spanning-tree portfast trunk
```

ポート 1/0/2（トランクポート）に PortFast 機能を設定します。また，BPDU ガード機能を設定します。トランクポートはデフォルトでは PortFast 機能を適用しないためポートごとに設定します。デフォルトで BPDU ガード機能を設定している場合は, PortFast 機能を設定すると自動的に BPDU ガードも適用します。デフォルトで設定していない場合は，spanning-tree bpduguard enable コマンドで設定します。

27.13.3　BPDU フィルタの設定

BPDU フィルタ機能は，BPDU を受信した場合にその BPDU を廃棄します。また，BPDU を一切送信しなくなります。通常は冗長経路ではないポートを指定することを前提とします。

[設定のポイント]

インタフェース単位に BPDU フィルタ機能を設定できます。

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 1/0/1
```

(config-if)# spanning-tree bpdufilter enable

ポート 1/0/1 で BPDU フィルタ機能を設定します。

27.13.4 ループガードの設定

片線切れなどの単一方向のリンク障害が発生し，BPDU の受信が途絶えた場合，ループが発生することがあります。ループガードは，このようにループの発生を防止したい場合に設定します。

[設定のポイント]

ループガードは，PortFast 機能を設定していないポートで動作します。

spanning-tree loopguard default コマンドを設定すると，PortFast を設定したポート以外のすべてのポートにループガードを適用します。デフォルトで適用する場合に，ループガードを無効にしたい場合は spanning-tree guard none コマンドを設定します。

[コマンドによる設定]

1. **(config)# spanning-tree loopguard default**

   PortFast を設定したポート以外のすべてのポートに対してループガード機能を適用するように設定します。

2. **(config)# interface gigabitethernet 1/0/1**

   (config-if)# spanning-tree guard none

   (config-if)# exit

   デフォルトでループガードを適用するように設定した状態で，ポート 1/0/1 はループガードを無効にするように設定します。

3. **(config)# no spanning-tree loopguard default**

   (config)# interface gigabitethernet 1/0/2

   (config-if)# spanning-tree guard loop

   デフォルトでループガードを適用する設定を削除します。また，ポート 1/0/2 に対してポートごとの設定でループガードを適用します。

27.13.5 ルートガードの設定

ネットワークに誤って装置が接続された場合や設定が変更された場合，ルートブリッジが替わり，意図しないトポロジーになることがあります。ルートガードは，このような意図しないトポロジー変更を防止したい場合に設定します。

[設定のポイント]

ルートガードは指定ポートに対して設定します。ルートブリッジの候補となる装置以外の装置と接続する個所すべてに適用します。

ルートガード動作時，PVST+が動作している場合は，該当する VLAN のポートだけブロック状態に設定します。マルチプルスパニングツリーが動作している場合，該当するインスタンスのポートだけブロック状態に設定しますが，該当するポートが境界ポートの場合は，全インスタンスのポートをブロック状態に設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**

   (config-if)# spanning-tree guard root

ポート 1/0/1 でルートガード機能を設定します。

27.13.6　リンクタイプの設定

リンクタイプはポートの接続状態を表します。Rapid PVST+，シングルスパニングツリーの Rapid STP，マルチプルスパニングツリーで高速な状態遷移を行うためには，スイッチ間の接続が point-to-point である必要があります。shared の場合は高速な状態遷移はしないで，PVST+，シングルスパニングツリーの STP と同様にタイマによる状態遷移となります。

[設定のポイント]

ポートごとに接続状態を設定できます。設定しない場合，ポートが全二重の接続のときは point-to-point，半二重の接続の場合は shared となります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/0/1**

   (config-if)# spanning-tree link-type point-to-point

   ポート 1/0/1 を point-to-point 接続とみなして動作させます。

[注意事項]

実際のネットワークの接続形態が 1 対 1 接続ではない構成では，本コマンドで point-to-point を指定しないでください。1 対 1 接続ではない構成とは，一つのポートに隣接するスパニングツリー装置が 2 台以上存在する構成です。

27.14　スパニングツリー共通機能のオペレーション

27.14.1　運用コマンド一覧

スパニングツリー共通機能の運用コマンド一覧を次の表に示します。

表 27-21　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。

27.14.2　スパニングツリー共通機能の状態の確認

スパニングツリーの情報は show spanning-tree detail コマンドで確認してください。VLAN 10 の PVST+の例を次の図に示します。

PortFast はポート 1/0/3，1/0/4，1/0/5 に設定していることを PortFast の項目で確認できます。ポート 1/0/3 は PortFast を設定していて，ポート 1/0/4 は PortFast に加えて BPDU ガードを設定しています。どちらのポートも意図しない BPDU を受信しないで正常に動作していることを示しています。ポート 1/0/5 は BPDU フィルタを設定しています。

ループガードはポート 1/0/2 に設定していることを Loop Guard の項目で確認できます。ルートガードはポート 1/0/6 に設定していることを Root Guard の項目で確認できます。リンクタイプは各ポートの Link Type の項目で確認できます。すべてのポートが point-to-point で動作しています。

図 27-19　スパニングツリーの情報

```
> show spanning-tree vlan 10 detail
Date 20XX/10/21 18:13:59 UTC
VLAN 10             PVST+ Spanning Tree:Enabled  Mode:Rapid PVST+
  Bridge ID
    Priority:32778                  MAC Address:0012.e210.3004
    Bridge Status:Designated        Path Cost Method:Short
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority:32778                  MAC Address:0012.e210.1004
    Root Cost:4
    Root Port:1/0/1
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Port Information
  Port:1/0/1 Up
    Status:Forwarding               Role:Root
    Priority:128                    Cost:4
    Link Type:point-to-point        Compatible Mode:-
    Loop Guard:OFF                  PortFast:OFF
    BpduFilter:OFF                  Root Guard:OFF
    BPDU Parameters(20XX/10/21 18:13:59):
      Designated Root
        Priority:32778              MAC address:0012.e210.1004
      Designated Bridge
        Priority:32778              MAC address:0012.e210.1004
        Root Path Cost:0
      Port ID
        Priority:128                Number:1
      Message Age Time:0(3)/20
  Port:1/0/2 Up
    Status:Discarding               Role:Alternate
    Priority:128                    Cost:4
    Link Type:point-to-point        Compatible Mode:-
    Loop Guard:ON                   PortFast:OFF
```

```
  BpduFilter:OFF                  Root Guard:OFF
  BPDU Parameters(20XX/10/21 18:13:58):
    Designated Root
      Priority:32778              MAC address:0012.e210.1004
    Designated Bridge
      Priority:32778              MAC address:0012.e210.2004
      Root Path Cost:4
    Port ID
      Priority:128                Number:1
    Message Age Time:1(3)/20
Port:1/0/3 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:ON (BPDU not received)
  BpduFilter:OFF                  Root Guard:OFF
Port: 1/0/4 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:BPDU Guard(BPDU not received)
  BpduFilter:OFF                  Root Guard:OFF
Port: 1/0/5 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:ON(BPDU not received)
  BpduFilter:ON                   Root Guard:OFF
Port: 1/0/6 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:OFF
  BpduFilter:OFF                  Root Guard:ON
```

28 Ring Protocol の解説

この章は，Autonomous Extensible Ring Protocol について説明します。
Autonomous Extensible Ring Protocol は，リングトポロジーでのレイヤ 2 ネットワークの冗長化プロトコルで，以降，Ring Protocol と呼びます。

28.1　Ring Protocol の概要

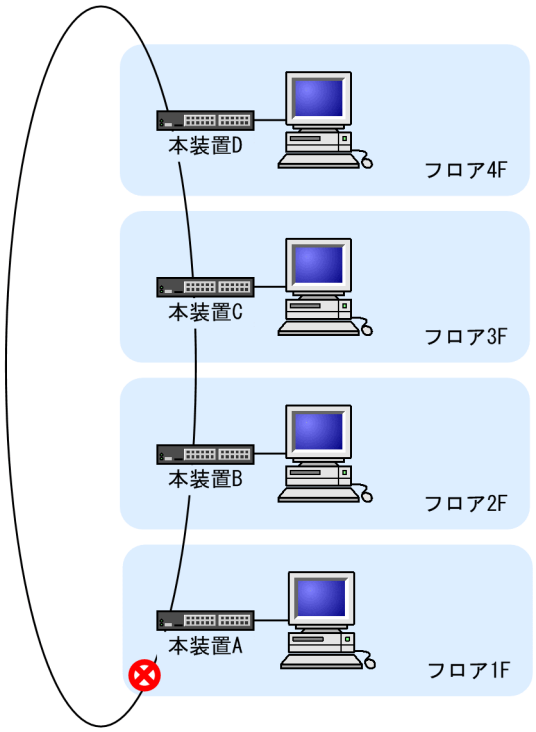
28.1.1　概要

Ring Protocol とは，スイッチをリング状に接続したネットワークでの障害の検出と，それに伴う経路切り替えを高速に行うレイヤ 2 ネットワークの冗長化プロトコルです。

レイヤ 2 ネットワークの冗長化プロトコルとして，スパニングツリーが利用されますが，障害発生に伴う切り替えの収束時間が遅いなどの欠点があります。Ring Protocol を使用すると，障害発生に伴う経路切り替えを高速にできるようになります。また，リングトポロジーを利用することで，メッシュトポロジーよりも伝送路やインタフェースの必要量が少なくて済むという利点もあります。

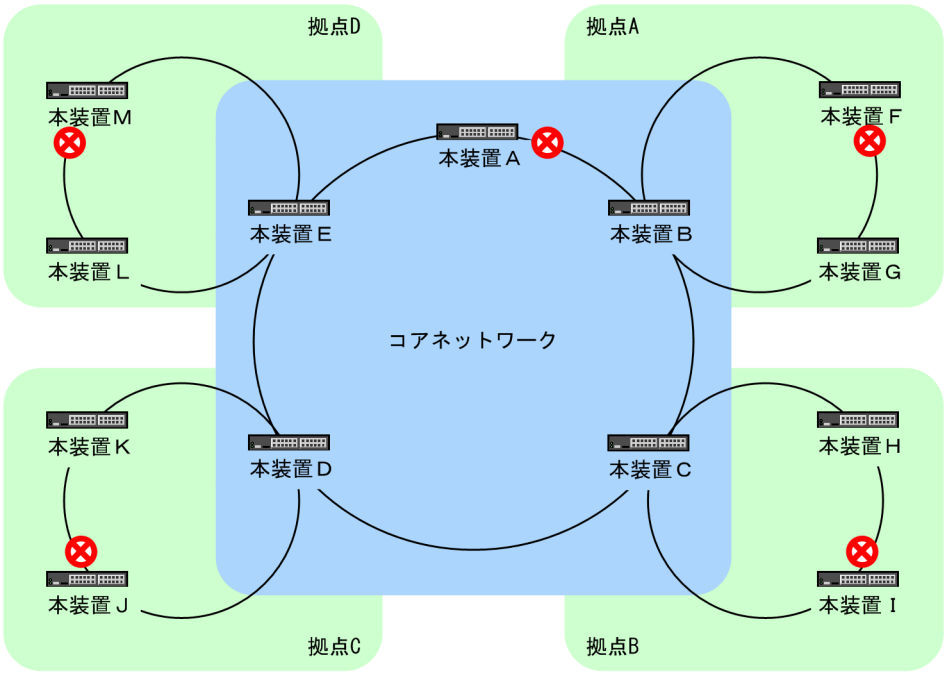
Ring Protocol の適用例を次の図に示します。

図 28–1　Ring Protocol の適用例（その 1）



（凡例）
：ブロッキング

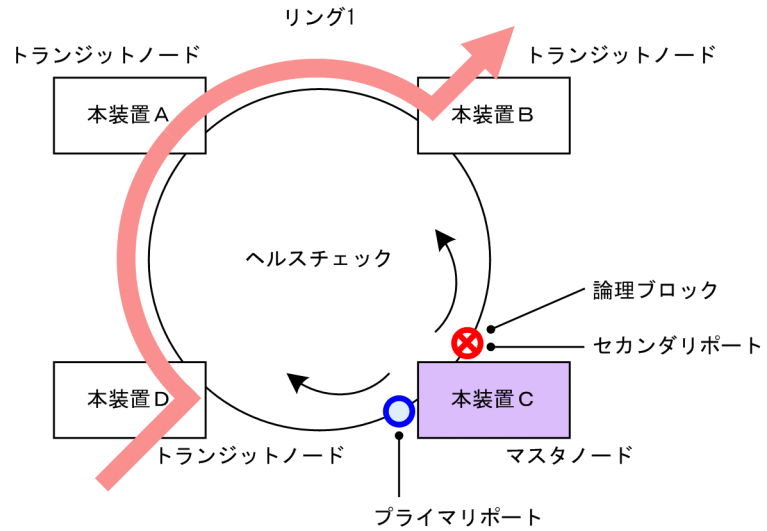
図 28-2　Ring Protocol の適用例（その 2）



（凡例）
：ブロッキング

Ring Protocol によるリングネットワークの概要を次の図に示します。

図 28-3　Ring Protocol の概要



（凡例）
：フォワーディング　：ブロッキング
：データの流れ

リングを構成するノードのうち一つをマスタノードとして，ほかのリング構成ノードをトランジットノードとします。各ノード間を接続する二つのポートをリングポートと呼び，マスタノードのリングポートにはプ

ライマリポートとセカンダリポートがあります。マスタノードはセカンダリポートを論理ブロックすることでリング構成を分断します。これによって，データフレームのループを防止しています。マスタノードはリング内の状態監視を目的とした制御フレーム（ヘルスチェックフレーム）を定期的に送信します。マスタノードは，巡回したヘルスチェックフレームの受信，未受信によって，リング内で障害が発生していないかどうかを判断します。障害または障害復旧を検出したマスタノードは，セカンダリポートの論理ブロックを設定または解除することで経路を切り替え，通信を復旧させます。

28.1.2　特長

(1)　イーサネットベースのリングネットワーク

Ring Protocol はイーサネットベースのネットワーク冗長化プロトコルです。従来のリングネットワークでは FDDI のように二重リンクの光ファイバを用いたネットワークが主流でしたが，Ring Protocol を用いることでイーサネットを用いたリングネットワークが構築できます。

(2)　シンプルな動作方式

Ring Protocol を使用したネットワークは，マスタノード 1 台とそのほかのトランジットノードで構成したシンプルな構成となります。リング状態（障害や障害復旧）の監視や経路の切り替え動作は，主にマスタノードが行い，そのほかのトランジットノードはマスタノードからの指示によって経路の切り替え動作を行います。

(3)　制御フレーム

Ring Protocol では，本プロトコル独自の制御フレームを使用します。制御フレームは，マスタノードによるリング状態の監視やマスタノードからトランジットノードへの経路の切り替え指示に使われます。制御フレームの送受信は，専用の VLAN 上で行われるため，通常のスパニングツリーのようにデータフレームと制御フレームが同じ VLAN 内に流れることはありません。また，制御フレームは優先的に処理されるため，データトラフィックが増大しても制御フレームに影響を与えません。

(4)　負荷分散方式

リング内で使用する複数の VLAN を論理的なグループ単位にまとめ，マスタノードを基点としてデータの流れを右回りと左回りに分散させる設定ができます。負荷分散や VLAN ごとに経路を分けたい場合に有効です。

28.1.3　サポート仕様

Ring Protocol でサポートする項目と仕様を次の表に示します。

表 28-1　Ring Protocol でサポートする項目・仕様

項目		内容
適用レイヤ	レイヤ 2	○
	レイヤ 3	×
リング構成	シングルリング	○
	マルチリング	○（共有リンクありマルチリング構成含む）
装置当たりのリング ID 最大数		24※1

項目		内容
		ただし，Ring Protocol とスパニングツリーの併用，Ring Protocol と GSRP の併用，または多重障害監視機能を使用する場合は，8 とする
リングポート（1 リング ID 当たりのポート数）		2（物理ポートまたはリンクアグリゲーション）
VLAN 数	1 リング ID 当たりの制御 VLAN 数	1（デフォルト VLAN の設定は不可）
	1 リング ID 当たりのデータ転送用 VLAN グループ最大数	2
	1 データ転送用 VLAN グループ当たりの VLAN マッピング最大数	128※2
	1VLAN マッピング当たりの VLAN 最大数	1023 ただし，リング内にスタック構成のノードを含む場合は，511 とする
ヘルスチェックフレーム送信間隔		200～60000 ミリ秒の範囲で 1 ミリ秒単位
ヘルスチェックフレーム送信間隔【SL-L3A】		5～60000 ミリ秒の範囲で 1 ミリ秒単位
障害監視時間		500～300000 ミリ秒の範囲で 1 ミリ秒単位
障害監視時間【SL-L3A】		15～300000 ミリ秒の範囲で 1 ミリ秒単位
負荷分散方式		二つのデータ転送用 VLAN グループを使用することで可能
多重障害監視機能	装置当たりの多重障害監視可能リング数	4
	1 リング ID 当たりの多重障害監視 VLAN 数	1（デフォルト VLAN の設定は不可）
	多重障害監視フレーム送信間隔	500～60000 ミリ秒の範囲で 1 ミリ秒単位
	多重障害監視時間※3	1000～300000 ミリ秒の範囲で 1 ミリ秒単位

（凡例）　○：サポート　×：未サポート

注※1　スタック構成時は，スタック当たりのリング ID 最大数となります。

注※2　スタック構成時は，本装置がマスタノードとして動作するリングで使用する VLAN マッピングの総数の推奨値は 128 以下となります。

注※3　スタック構成のノードを含むリングの多重障害監視は未サポートです。

28.2　Ring Protocol の基本原理

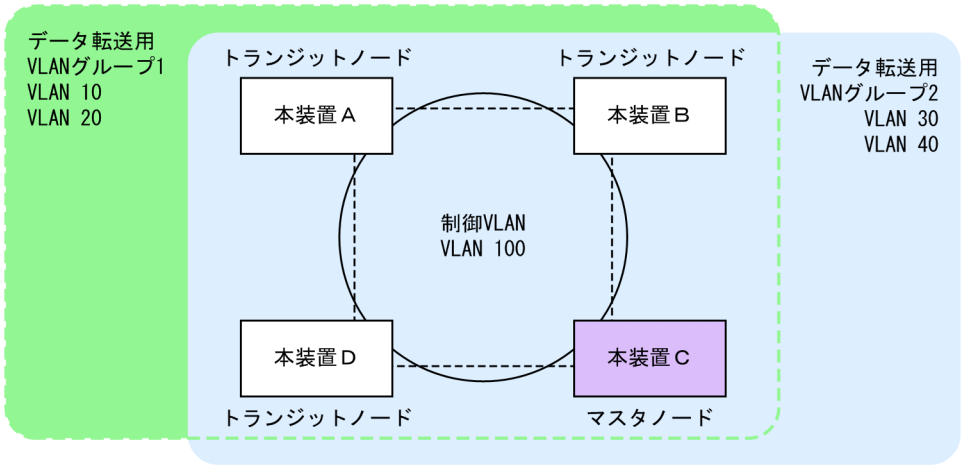
28.2.1　ネットワーク構成

Ring Protocol を使用する場合の基本的なネットワーク構成を次に示します。

(1)　シングルリング構成

シングルリング構成について，次の図に示します。

図 28–4　シングルリング構成

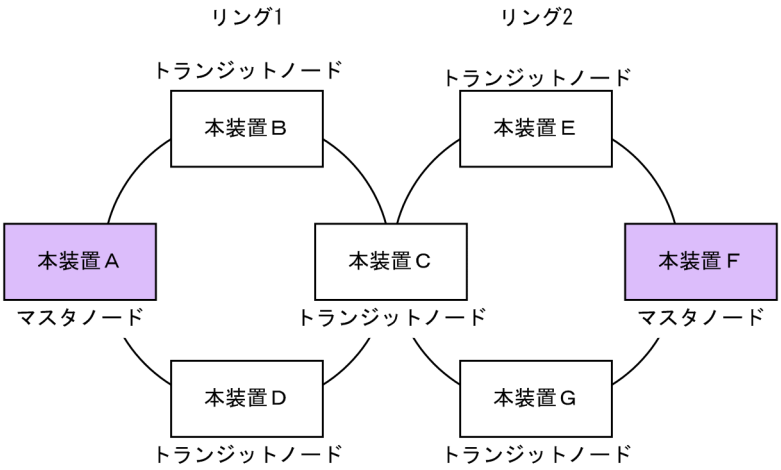


マスタノード 1 台とトランジットノード数台から成る一つのリング構成をシングルリング構成と呼びます。リングを構成するノード間は，リングポートとして，物理ポートまたはリンクアグリゲーションで接続されます。また，リングを構成するすべてのノードに，制御 VLAN として同一の VLAN，およびデータフレームの転送用として共通の VLAN を使用する必要があります。マスタノードから送信した制御フレームは，制御 VLAN 内を巡回します。データフレームの送受信に使用する VLAN は，VLAN グループと呼ばれる一つの論理的なグループに束ねて使用します。VLAN グループは複数の VLAN をまとめることができ，一つのリングにマスタノードを基点とした右回り用と左回り用の最大 2 グループを設定できます。

(2)　マルチリング構成

マルチリング構成のうち，隣接するリングの接点となるノードが一つの場合の構成について次の図に示します。

図 28-5　マルチリング構成

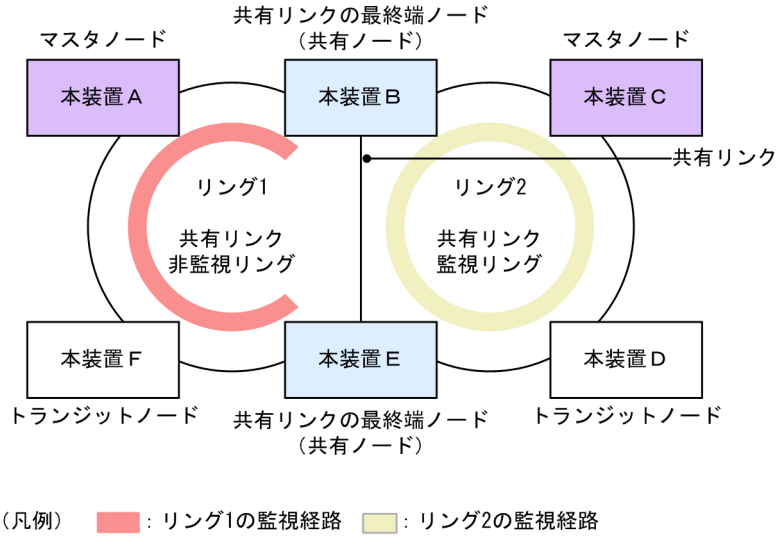


それぞれのリングを構成しているノードは独立したシングルリングとして動作します。このため，リング障害の検出および復旧の検出はそれぞれのリングで独立して行われます。

(3)　共有リンクありのマルチリング構成

マルチリング構成のうち，隣接するリングの接点となるノードが二つ以上の場合の構成について次の図に示します。

図 28-6　共有リンクありのマルチリング構成



複数のシングルリングが，二つ以上のノードで接続されている場合，複数のリングでリンクを共有することになります。このリンクを共有リンクと呼び，共有リンクのあるマルチリング構成を，共有リンクありのマルチリング構成と呼びます。これに対し，（2）のように，複数のシングルリングが一つのノードで接続されている場合には，共有リンクがありませんので，共有リンクなしのマルチリング構成と呼びます。

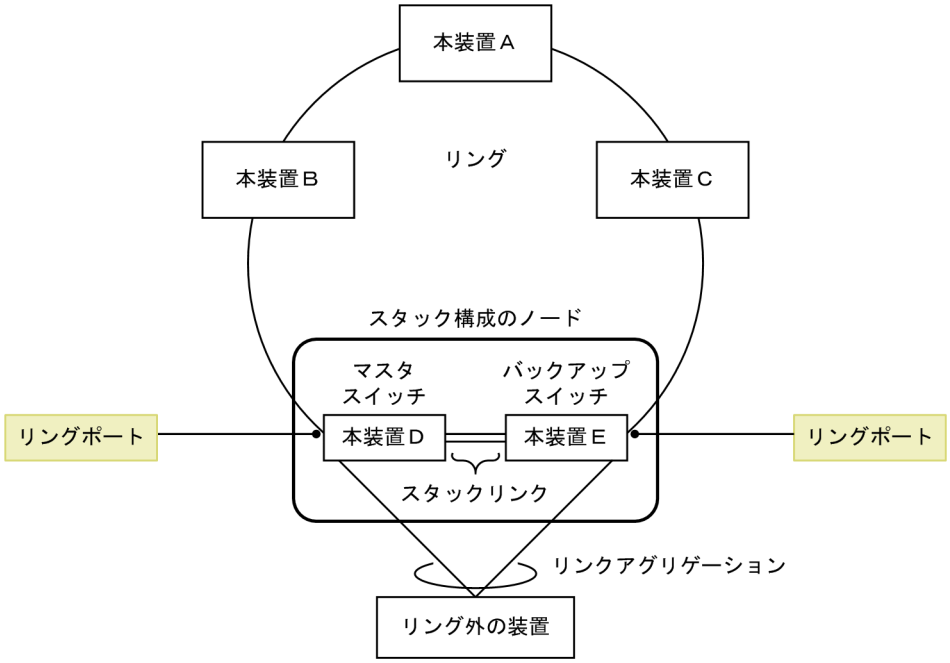
共有リンクありのマルチリング構成では，隣接するリングで共通の VLAN をデータ転送用の VLAN グループとして使用した場合に，共有リンクで障害が発生すると隣接するリングそれぞれのマスタノードが障害を検出し，複数のリングをまたいだループ（いわゆるスーパーループ）が発生します。このため，本構成ではシングルリング構成とは異なる障害検出，および切り替え動作を行う必要があります。

Ring Protocol では，共有リンクをリングの一部とする複数のリングのうち，一つを共有リンクの障害および復旧を監視するリング（共有リンク監視リング）とし，それ以外のリングを，共有リンクの障害および復旧を監視しないリング（共有リンク非監視リング）とします。また，共有リンクの両端に位置するノードを共有リンク非監視リングの最終端ノード（または，共有ノード）と呼びます。このように，各リングのマスタノードで監視対象リングを重複させないことによって，共有リンク間の障害によるループの発生を防止します。

(4)　スタック構成のノードを含むリング構成

スタック構成のノードを含むリング構成について，次の図に示します。

図 28–7　スタック構成のノードを含むリング構成



スタック構成時は，メンバスイッチ 2 台で一つのノードとして動作します。スタック構成のノードは，マスタスイッチ側とバックアップスイッチ側でそれぞれリングポートとして接続して，スタックリンクを経由する形でリングを構成します。なお，スタック構成のノードは，共有リンクありのマルチリング構成での共有ノードをサポートしていません。

スタック構成のノードでは，制御フレームおよびデータフレームの転送にスタックリンクを使用します。そのため，2 本以上のスタックリンクを設定して，リングのトラフィックに対して余裕を持った帯域を確保してください。なお，スタックポートの最大回線数については，「2.2　収容回線数」を参照してください。

28.2.2　制御 VLAN

Ring Protocol を利用するネットワークでは，制御フレームの送信範囲を限定するために，制御フレームの送受信に専用の VLAN を使用します。この VLAN を制御 VLAN と呼び，リングを構成するすべてのノードで同一の VLAN を使用します。制御 VLAN は，リングごとに共通な一つの VLAN を使用しますので，マルチリング構成時には，隣接するリングで異なる VLAN を使用する必要があります。

28.2.3　障害監視方法

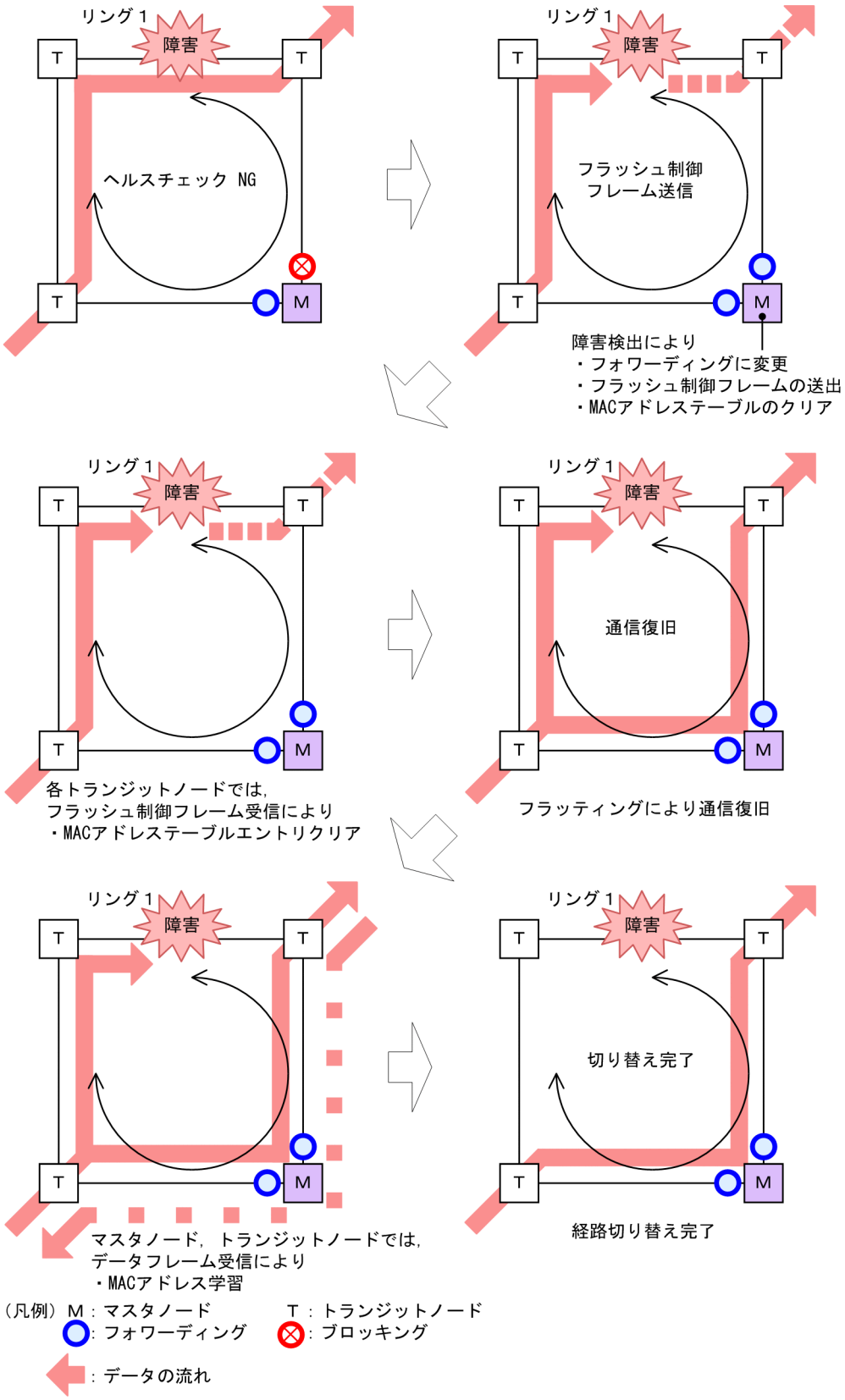
Ring Protocol のリング障害の監視は，マスタノードがヘルスチェックフレームと呼ぶ制御フレームを定期的に送信し，マスタノードがこのヘルスチェックフレームの受信可否を監視することで実現します。マスタノードでは，ヘルスチェックフレームが一定時間到達しないとリング障害が発生したと判断し，障害動作を行います。また，リング障害中に再度ヘルスチェックフレームを受信すると，リング障害が復旧したと判断し，復旧動作を行います。

28.2.4　通信経路の切り替え

マスタノードは，リング障害の検出による迂回経路への切り替えのために，セカンダリポートをブロッキングからフォワーディングに変更します。また，リング障害の復旧検出による経路の切り戻しのために，セカンダリポートをフォワーディングからブロッキングに変更します。これに併せて，早急な通信の復旧を行うために，リング内のすべてのノードで，MAC アドレステーブルエントリのクリアが必要です。MAC アドレステーブルエントリのクリアが実施されないと，切り替え（または切り戻し）前の情報に従ってデータフレームの転送が行われるため，正しくデータが届かないおそれがあります。したがって，通信を復旧させるために，リングを構成するすべてのノードで MAC アドレステーブルエントリのクリアを実施します。なお，クリアする MAC アドレステーブルのエントリは，コンフィグレーションコマンド mac-clear-mode の設定に従います。

マスタノードおよびトランジットノードそれぞれの場合の切り替え動作について次に説明します。

図 28-8　Ring Protocol の経路切り替え動作概要



(1)　マスタノードの経路切り替え

マスタノードでは，リング障害を検出するとセカンダリポートのブロッキングを解除します。また，MAC アドレステーブルエントリのクリアを行います。これによって，MAC アドレスの学習が行われるまでフラッディングを行います。セカンダリポートを経由したフレームの送受信によって MAC アドレス学習を行い，新しい経路への切り替えが完了します。

(2)　トランジットノードの経路切り替え

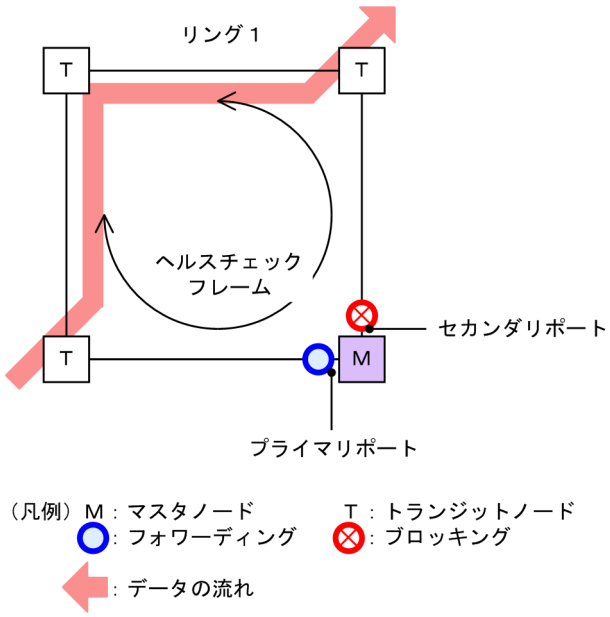
マスタノードがリングの障害を検出すると，同一の制御 VLAN を持つリング内の，そのほかのトランジットノードに対して MAC アドレステーブルエントリのクリアを要求するために，フラッシュ制御フレームと呼ぶ制御フレームを送信します。トランジットノードでは，このフラッシュ制御フレームを受信すると，MAC アドレステーブルエントリのクリアを行います。これによって，MAC アドレスの学習が行われるまでフラッディングを行います。新しい経路でのフレームの送受信によって MAC アドレス学習が行われ，通信経路の切り替えが完了します。

28.3　シングルリングの動作概要

28.3.1　リング正常時の動作

シングルリングでのリング正常時の動作について次の図に示します。

図 28–9　リング正常時の動作



(1)　マスタノード動作

片方向リンク障害による障害誤検出を防止するために，二つのリングポートからヘルスチェックフレームを送信します。あらかじめ設定された時間内に，両方向のヘルスチェックフレームを受信するか監視します。データフレームの転送は，プライマリポートで行います。セカンダリポートは論理ブロックされているため，データフレームの転送および MAC アドレス学習は行いません。

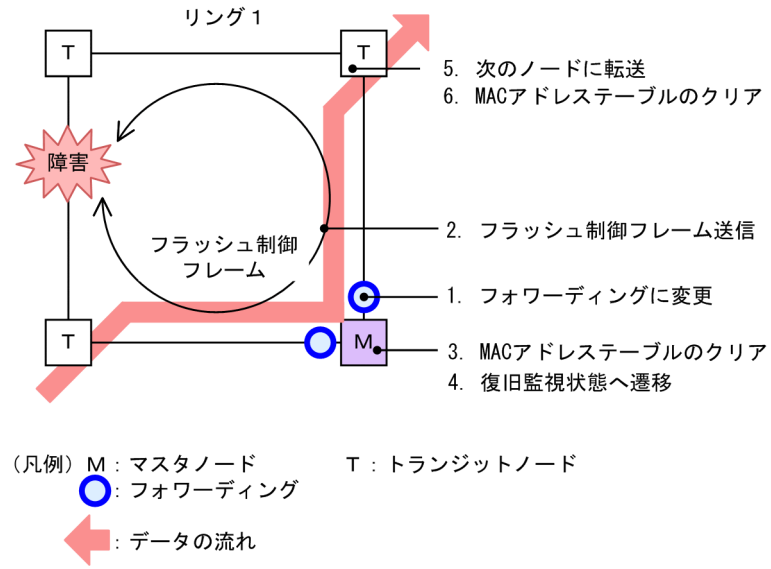
(2)　トランジットノード動作

トランジットノードでは，マスタノードが送信するヘルスチェックフレームの監視は行いません。ヘルスチェックフレームを受信すると，リング内の次ノードに転送します。データフレームの転送は，両リングポートで行います。

28.3.2　障害検出時の動作

シングルリングでのリング障害検出時の動作について次の図に示します。

図 28-10　リング障害時の動作



(1)　マスタノード動作

あらかじめ設定された時間内に，両方向のヘルスチェックフレームを受信しなければ障害と判断します。障害を検出したマスタノードは，次に示す手順で切り替え動作を行います。

1. データ転送用リング VLAN 状態の変更

セカンダリポートのリング VLAN 状態をブロッキングからフォワーディングに変更します。障害検出時のリング VLAN 状態は次の表のように変更します。

表 28-2　障害検出時のデータ転送用リング VLAN 状態

リングポート	変更前（正常時）	変更後（障害時）
プライマリポート	フォワーディング	フォワーディング
セカンダリポート	ブロッキング	フォワーディング

2. フラッシュ制御フレームの送信

マスタノードのプライマリポートおよびセカンダリポートからフラッシュ制御フレームを送信します。

3. MAC アドレステーブルのクリア

MAC アドレステーブルエントリのクリアを行います。MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

4. 監視状態の変更

リング障害を検出すると，マスタノードは障害監視状態から復旧監視状態に遷移します。

(2)　トランジットノード動作

障害を検出したマスタノードから送信されるフラッシュ制御フレームを受信すると，トランジットノードでは次に示す動作を行います。

5. フラッシュ制御フレームの転送

受信したフラッシュ制御フレームを次のノードに転送します。

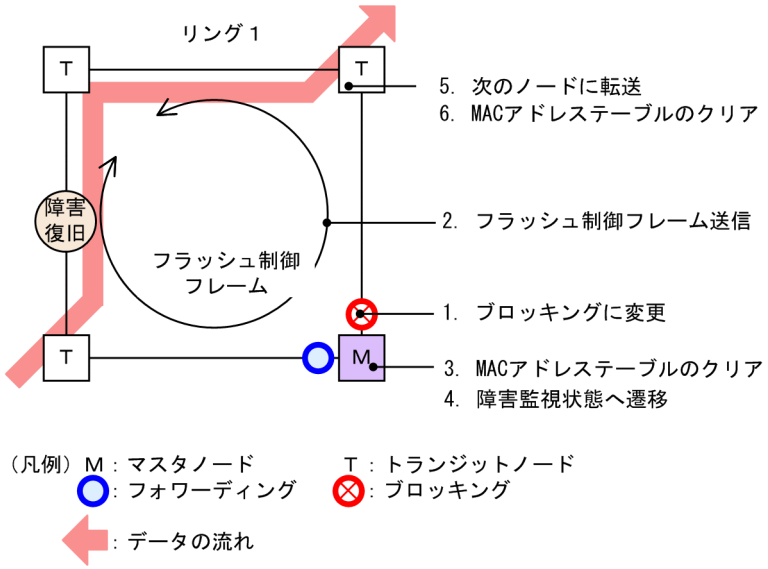
6. MAC アドレステーブルのクリア

MAC アドレステーブルエントリのクリアを行います。MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

28.3.3　復旧検出時の動作

シングルリングでのリング障害復旧時の動作について次の図に示します。

図 28-11　障害復旧時の動作



(1)　マスタノード動作

リング障害を検出している状態で，自身が送出したヘルスチェックフレームを受信すると，リング障害が復旧したと判断し，次に示す復旧動作を行います。

1. データ転送用リング VLAN 状態の変更

セカンダリポートのリング VLAN 状態をフォワーディングからブロッキングに変更します。復旧検出時のリング VLAN 状態は次の表のように変更します。

表 28-3　復旧検出時のデータ転送用リング VLAN 状態

リングポート	変更前（障害時）	変更後（復旧時）
プライマリポート	フォワーディング	フォワーディング
セカンダリポート	フォワーディング	ブロッキング

2. フラッシュ制御フレームの送信

マスタノードのプライマリポートおよびセカンダリポートからフラッシュ制御フレームを送信します。なお，リング障害復旧時は，各トランジットノードが転送したフラッシュ制御フレームがマスタノードへ戻ってきますが，マスタノードでは受信しても廃棄します。

3. MAC アドレステーブルのクリア

MAC アドレステーブルエントリのクリアを行います。

MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

4. 監視状態の変更

リング障害の復旧を検出すると，マスタノードは復旧監視状態から障害監視状態に遷移します。

(2)　トランジットノード動作

マスタノードから送信されるフラッシュ制御フレームを受信すると，次に示す動作を行います。

5. フラッシュ制御フレームの転送

受信したフラッシュ制御フレームを次のノードに転送します。

6. MAC アドレステーブルのクリア

MAC アドレステーブルエントリのクリアを行います。

MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

また，リンク障害が発生したトランジットノードでは，リンク障害が復旧した際のループの発生を防ぐため，リングポートのリング VLAN 状態はブロッキング状態となります。ブロッキング状態を解除する契機は，マスタノードが送信するフラッシュ制御フレームを受信したとき，またはトランジットノードでリングポートのフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）がタイムアウトしたときとなります。フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）は，リングポートのリンク障害復旧時に設定されます。

28.3.4　経路切り戻し抑止および解除時の動作

経路切り戻し抑止機能を適用すると，マスタノードでリングの障害復旧を検出した場合に，マスタノードは復旧抑止状態になり，すぐには復旧動作を行いません。本機能を有効にするには，コンフィグレーションコマンド preempt-delay の設定が必要です。

なお，経路切り戻し抑止状態は，次の契機で解除します。

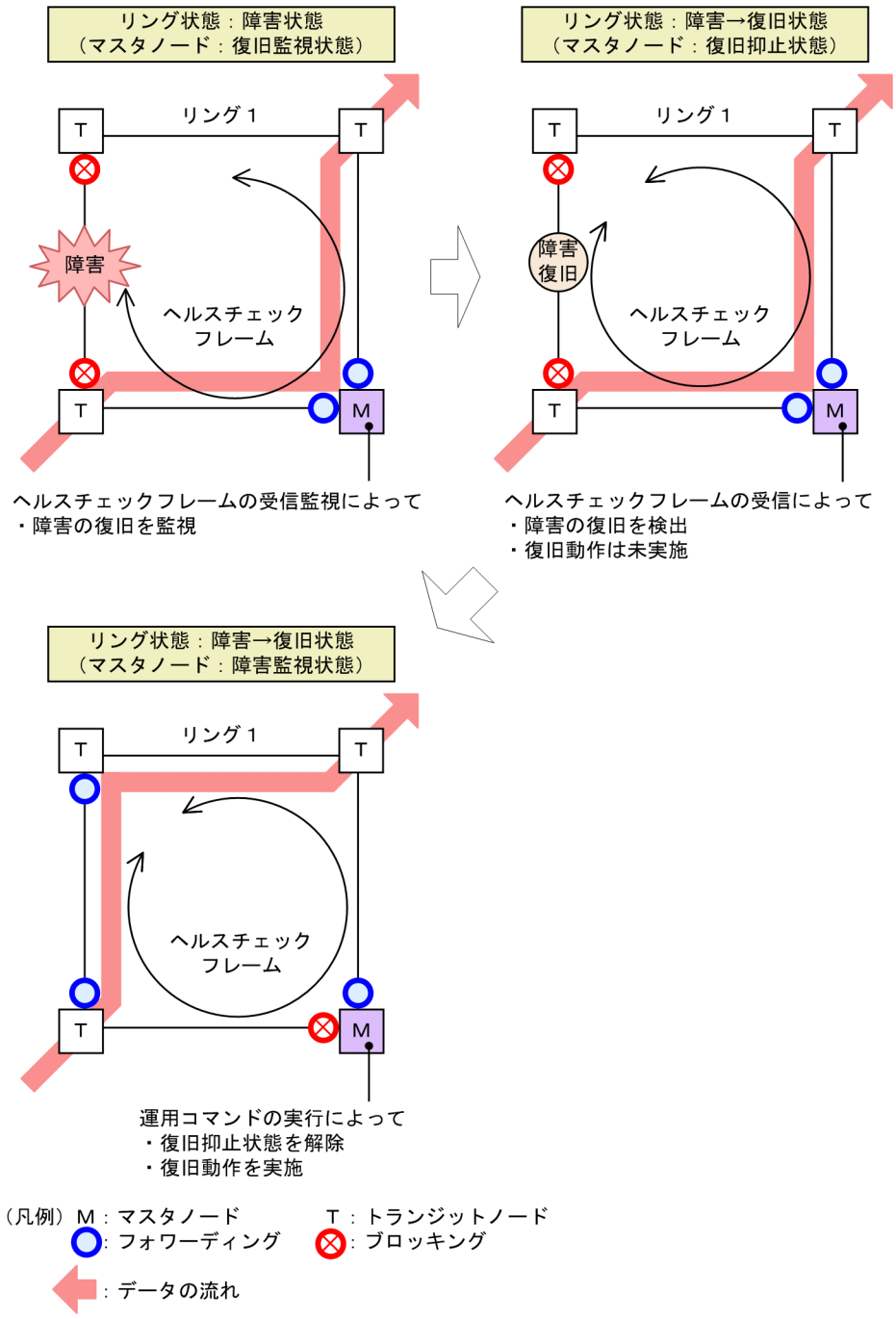
- 運用コマンド clear axrp preempt-delay の実行によって，経路切り戻し抑止が解除された場合
- コンフィグレーションコマンド preempt-delay で指定した，経路切り戻し抑止時間が経過した場合
- 経路切り戻し抑止機能を有効にするコンフィグレーションコマンド preempt-delay を削除した場合

復旧抑止状態が解除されると，復旧動作を行います。復旧が完了すると，マスタノードは障害監視状態に遷移します。

また，経路切り戻し抑止状態でリングの障害が発生すると，マスタノードは再度，復旧監視状態に遷移します。

運用コマンド clear axrp preempt-delay の実行によって経路切り戻し抑止を解除した場合の動作を次の図に示します。その他の契機で解除した場合も，同様の動作となります。

図 28-12　運用コマンドの実行によって経路切り戻し抑止を解除した場合の動作



また，次に示すイベントが発生した場合は経路の切り戻し抑止状態を解除して，マスタノードが障害監視状態に遷移します。

- 装置起動（運用コマンド reload および ppupdate の実行を含む）
- コンフィグレーションファイルの運用への反映（運用コマンド copy の実行）
- Ring Protocol プログラムの再起動（運用コマンド restart axrp の実行を含む）
- VLAN プログラムの再起動（運用コマンド restart vlan の実行を含む）

28.4　マルチリングの動作概要

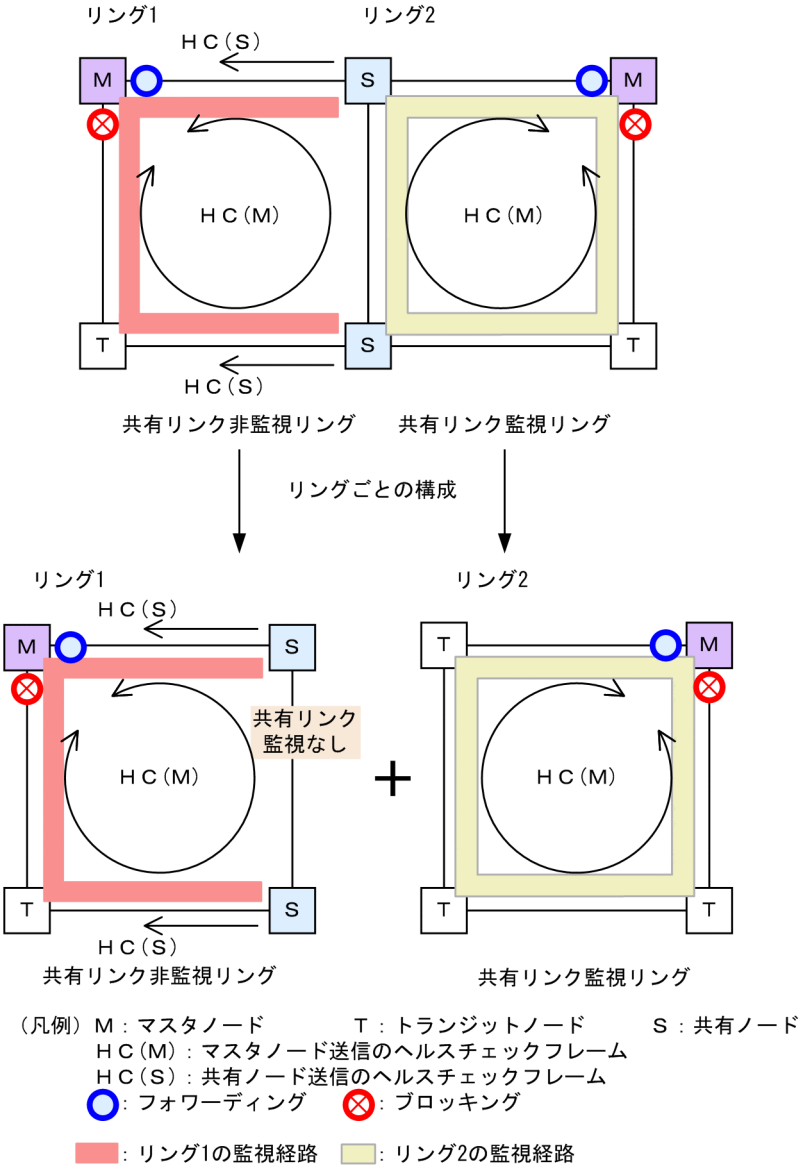
マルチリング構成のうち，共有リンクありのマルチリング構成について説明します。共有リンクなしのマルチリング構成については，シングルリング時の動作と同様ですので，「28.3　シングルリングの動作概要」を参照してください。

なお，この節以降，HC はヘルスチェックフレームを意味し，HC(M)はマスタノードが送信するヘルスチェックフレーム，HC(S)は共有ノードが送信するヘルスチェックフレームを表します。

28.4.1　リング正常時の動作

共有リンクありのマルチリング構成でのリング正常時の状態について次の図に示します。

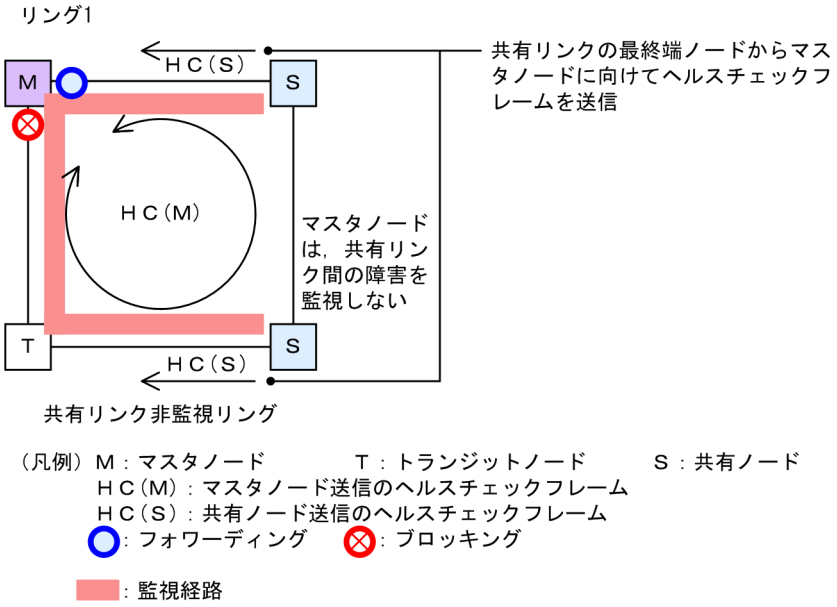
図 28-13　リング正常時の状態



(1)　共有リンク非監視リング

共有リンク非監視リングは，マスタノード 1 台とトランジットノード数台で構成します。しかし，共有リンクの障害を監視しないため，補助的な役割として，共有リンクの両端に位置する共有リンク非監視リングの最終端ノード（共有ノード）から，ヘルスチェックフレームをマスタノードに向けて送信します。このヘルスチェックフレームは，二つのリングポートのうち，共有リンクではない方のリングポートから送信します。これによって，共有リンク非監視リングのマスタノードは，共有リンクで障害が発生した場合に，自身が送信したヘルスチェックフレームが受信できなくなっても，共有リンク非監視リングの最終端ノード（共有ノード）からのヘルスチェックフレームが受信できている間は障害を検出しないようにできます。

図 28-14　共有リンク非監視リングでの正常時の動作



(a)　マスタノード動作

片方向リンク障害による障害誤検出を防止するために，二つのリングポートからヘルスチェックフレーム（HC(M)）を送信します。あらかじめ設定した時間内に，両方向の HC(M)を受信するか監視します。マスタノードが送信した HC(M)とは別に，共有リンクの両端に位置する共有リンク非監視リングの最終端ノード（共有ノード）から送信したヘルスチェックフレーム（HC(S)）についても合わせて受信を監視します。データフレームの転送は，プライマリポートで行います。セカンダリポートは論理ブロックされているため，データフレームの転送および MAC アドレス学習は行いません。

(b)　トランジットノード動作

トランジットノードの動作は，シングルリング時と同様です。トランジットノードは，HC(M)および HC(S)を監視しません。HC(M)や HC(S)を受信すると，リング内の次ノードに転送します。データフレームの転送は，両リングポートで行います。

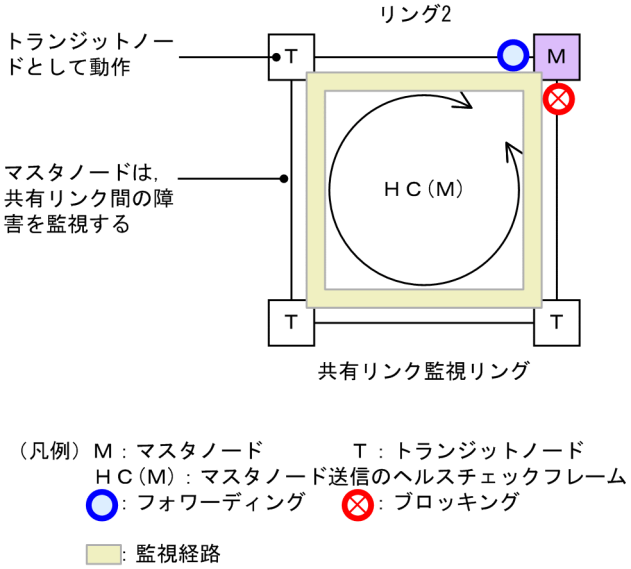
(c)　共有リンク非監視リングの最終端ノード動作

共有リンク非監視リングの最終端ノード（共有ノード）は，共有リンク非監視リングのマスタノードに向けて HC(S)の送信を行います。HC(S)の送信は，二つのリングポートのうち，共有リンクではない方のリングポートから送信します。マスタノードが送信する HC(M)や，データフレームの転送については，トランジットノードの場合と同様となります。

(2)　共有リンク監視リング

共有リンク監視リングは，シングルリング時と同様に，マスタノード 1 台と，そのほか数台のトランジットノードとの構成となります。共有リンクの両端に位置するノードは，シングルリング時と同様にマスタノードまたはトランジットノードとして動作します。

図 28–15　共有リンク監視リングでの正常時の動作



（凡例）Ｍ：マスタノード　　Ｔ：トランジットノード
ＨＣ（M）：マスタノード送信のヘルスチェックフレーム
：フォワーディング　：ブロッキング
：監視経路

(a)　マスタノード動作

片方向リンク障害による障害誤検出を防止するために，二つのリングポートからヘルスチェックフレーム（HC(M)）を送信します。あらかじめ設定された時間内に，両方向の HC(M)を受信するかを監視します。データフレームの転送は，プライマリポートで行います。セカンダリポートは論理ブロックされているため，データフレームの転送および MAC アドレス学習は行いません。

(b)　トランジットノード動作

トランジットノードの動作は，シングルリング時と同様です。トランジットノードは，マスタノードが送信した HC(M)を監視しません。HC(M)を受信すると，リング内の次ノードに転送します。データフレームの転送は，両リングポートで行います。

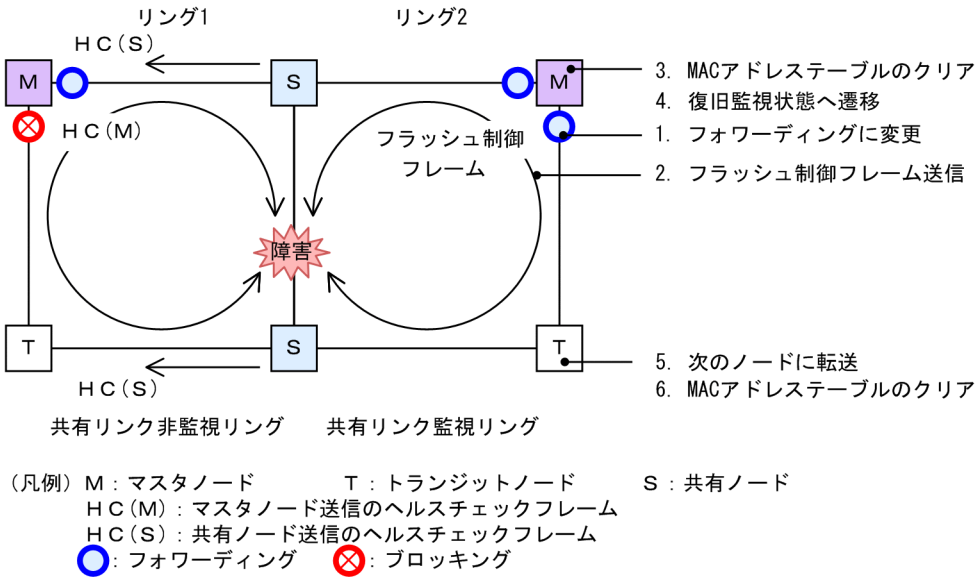
28.4.2　共有リンク障害・復旧時の動作

共有リンクありのマルチリング構成時に，共有リンク間で障害が発生した際の障害および復旧動作について説明します。

(1)　障害検出時の動作

共有リンクの障害を検出した際の動作について次の図に示します。

図 28-16　共有リンク障害時の動作



(a)　共有リンク監視リングのマスタノード動作

共有リンクで障害が発生すると，マスタノードは両方向の HC(M)を受信できなくなり，リング障害を検出します。障害を検出したマスタノードはシングルリング時と同様に，次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

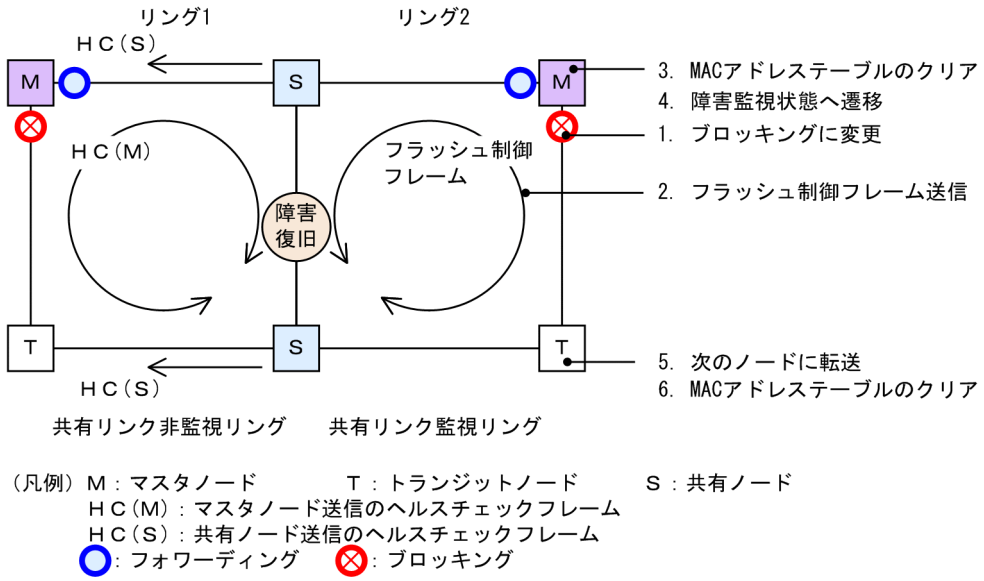
(c)　共有リンク非監視リングのマスタノードおよびトランジットノード動作

共有リンク非監視リングのマスタノードは，共有リンクでのリング障害を検出しないため，障害動作は行いません。このため，トランジットノードについても経路の切り替えは発生しません。

(2)　復旧検出時の動作

共有リンクの障害復旧を検出した際の動作について次の図に示します。

図 28-17　共有リンク復旧時の動作



(a)　共有リンク監視リングのマスタノード動作

リング障害を検出している状態で，自身が送信した HC(M)を受信すると，リング障害が復旧したと判断し，シングルリング時と同様に，次に示す手順で復旧動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c)　共有リンク非監視リングのマスタノードおよびトランジットノード動作

共有リンク非監視リングのマスタノードは，リング障害を検出していないため，トランジットノードを含め，復旧動作は行いません。

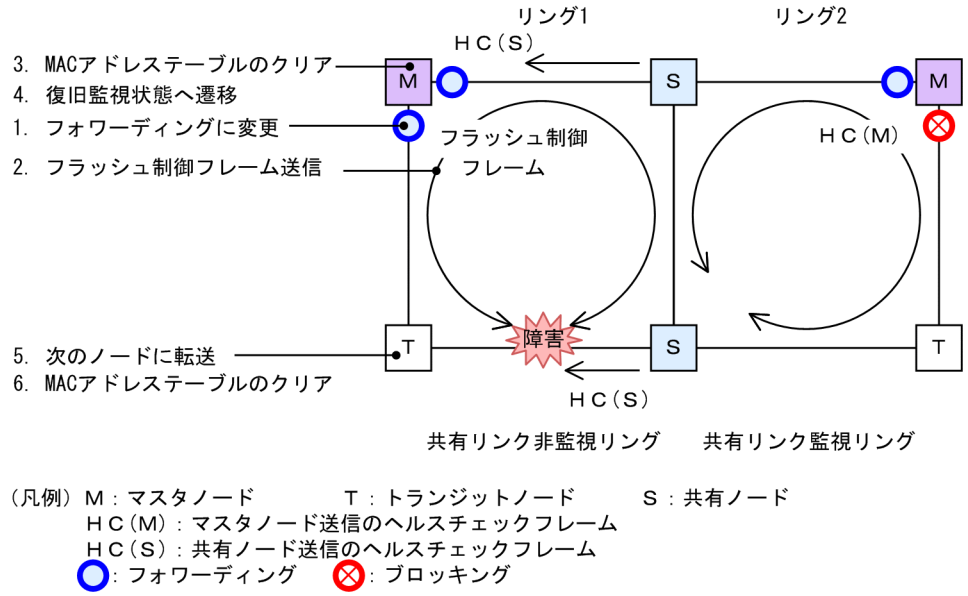
28.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作

共有リンク非監視リングでの，共有リンク以外のリング障害および復旧時の動作について説明します。

(1)　障害検出時の動作

共有リンク非監視リングでの共有リンク以外の障害を検出した際の動作について次の図に示します。

図 28-18　共有リンク非監視リングにおける共有リンク以外のリング障害時の動作



（凡例）Ｍ：マスタノード　　Ｔ：トランジットノード　　Ｓ：共有ノード
ＨＣ（Ｍ）：マスタノード送信のヘルスチェックフレーム
ＨＣ（Ｓ）：共有ノード送信のヘルスチェックフレーム
：フォワーディング　：ブロッキング

(a)　共有リンク非監視リングのマスタノード動作

共有リンク非監視リングのマスタノードは，自身が送信した両方向の HC(M)と共有ノードが送信した HC(S)が共に未受信となりリング障害を検出します。障害を検出したマスタノードの動作はシングルリング時と同様に，次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク非監視リングのトランジットノードおよび共有ノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

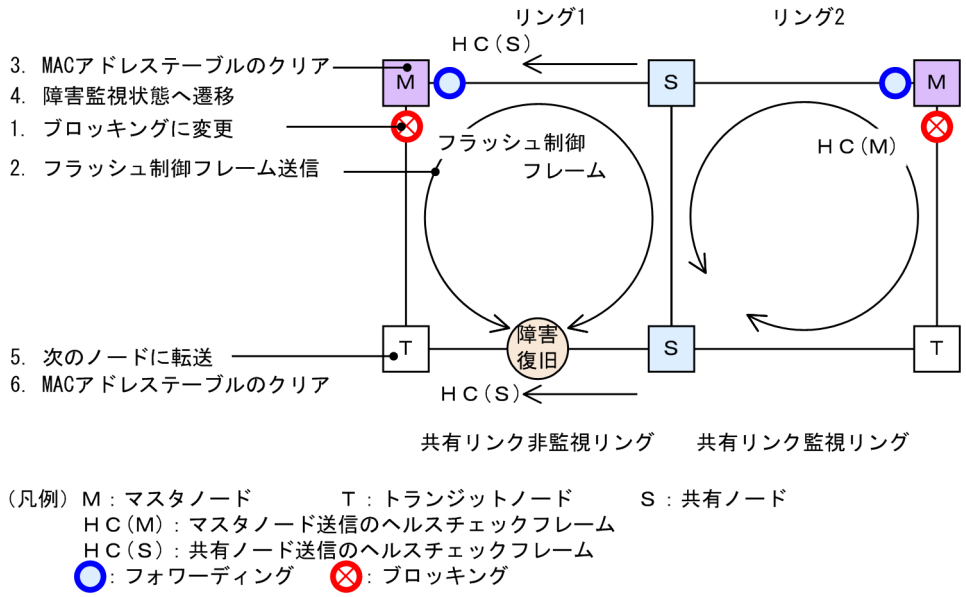
(c)　共有リンク監視リングのマスタノードおよびトランジットノード動作

共有リンク監視リング内では障害が発生していないため，障害動作は行いません。

(2)　復旧検出時の動作

共有リンク非監視リングでの共有リンク以外の障害が復旧した際の動作について次の図に示します。

図 28-19　共有リンク非監視リングでの共有リンク以外のリング障害復旧時の動作



（凡例）Ｍ：マスタノード　　Ｔ：トランジットノード　　Ｓ：共有ノード
ＨＣ（M）：マスタノード送信のヘルスチェックフレーム
ＨＣ（Ｓ）：共有ノード送信のヘルスチェックフレーム
：フォワーディング　：ブロッキング

(a)　共有リンク非監視リングのマスタノード動作

リング障害を検出している状態で，自身が送信した HC(M)を受信するか，または共有ノードが送信した HC(S)を両方向から受信すると，リング障害が復旧したと判断し，シングルリング時と同様に，次に示す手順で復旧動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク非監視リングのトランジットノードおよび共有ノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c)　共有リンク監視リングのマスタノードおよびトランジットノード動作

共有リンク監視リング内では障害が発生していないため，復旧動作は行いません。

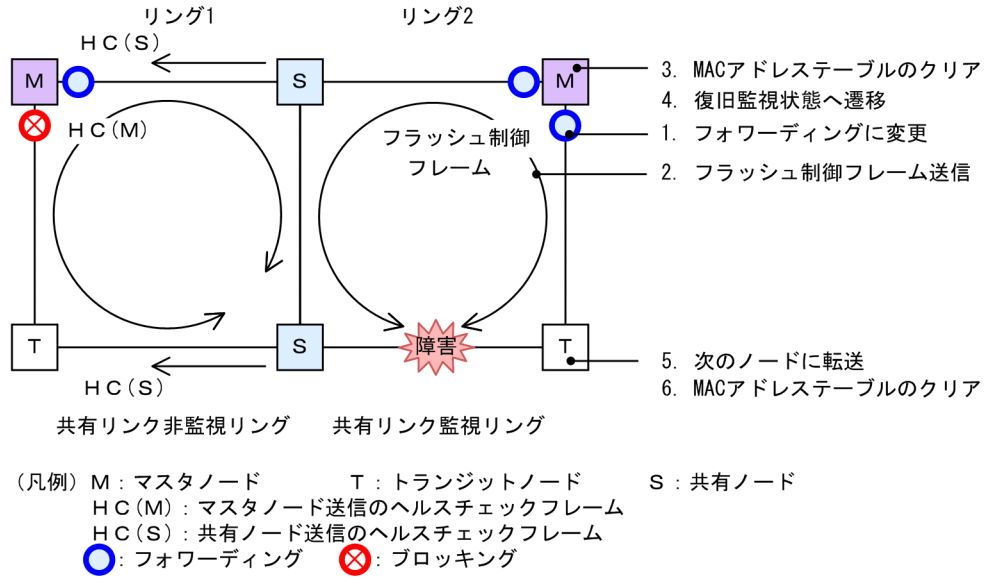
28.4.4　共有リンク監視リングでの共有リンク以外の障害・復旧時の動作

共有リンク監視リングでの共有リンク以外のリング障害および復旧時の動作について説明します。

(1)　障害検出時の動作

共有リンク監視リングでの共有リンク以外の障害を検出した際の動作について次の図に示します。

図 28-20　共有リンク監視リングでの共有リンク以外のリング障害時の動作



（凡例）Ｍ：マスタノード　　Ｔ：トランジットノード　　Ｓ：共有ノード
ＨＣ（M）：マスタノード送信のヘルスチェックフレーム
ＨＣ（S）：共有ノード送信のヘルスチェックフレーム
：フォワーディング　：ブロッキング

(a)　共有リンク監視リングのマスタノード動作

共有リンク監視リング内で障害が発生すると，マスタノードは両方向の HC(M)を受信できなくなり，リング障害を検出します。障害を検出したマスタノードはシングルリング時と同様に，次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

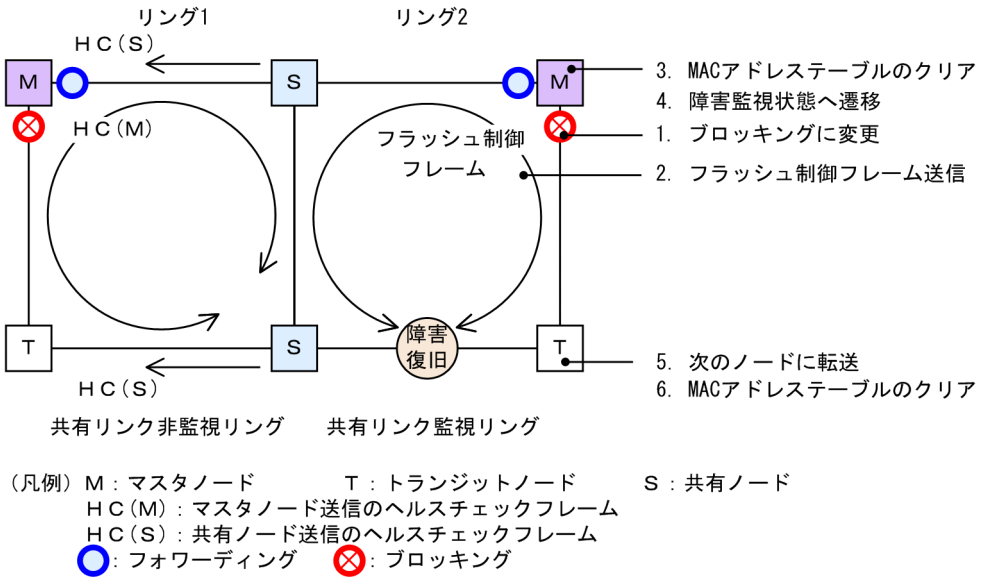
(c)　共有リンク非監視リングのマスタノードおよびトランジットノード（共有ノード）動作

共有リンク非監視リング内では障害が発生していないため，障害動作は行いません。

(2)　復旧検出時の動作

共有リンク監視リングでの共有リンク以外の障害が復旧した際の動作について次の図に示します。

図 28-21　共有リンク監視リングでの共有リンク以外のリング障害復旧時の動作



(a)　共有リンク監視リングのマスタノード動作

リング障害を検出している状態で，自身が送信した HC(M)を受信すると，リング障害が復旧したと判断し，シングルリング時と同様に，次に示す手順で復旧動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c)　共有リンク非監視リングのマスタノードおよびトランジットノード（共有ノード）動作

共有リンク非監視リング内では障害が発生していないため，復旧動作は行いません。

28.4.5　経路切り戻し抑止および解除時の動作

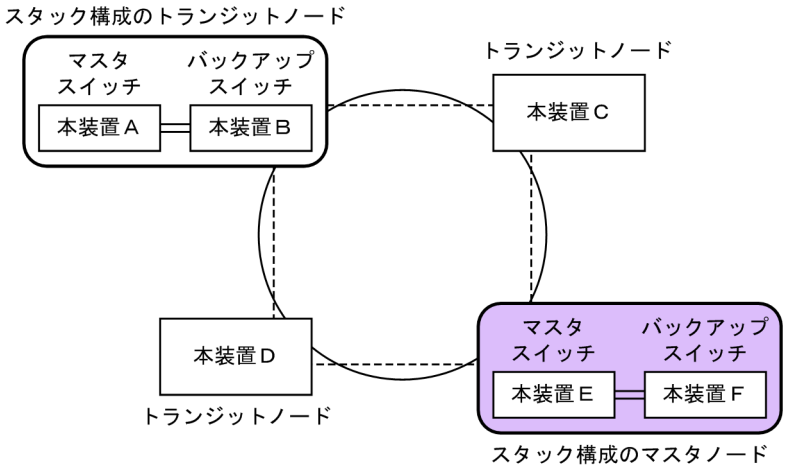
マルチリング構成での経路切り戻し抑止および解除時の動作については，シングルリング時の動作と同様ですので，「28.3　シングルリングの動作概要」を参照してください。

28.5　スタック構成のノードを含むリングの動作概要

28.5.1　シングルリングでの動作

スタック構成のノードを含むシングルリング構成について，次の図に例を示します。

図 28-22　スタック構成のノードを含むシングルリング構成



スタック構成のノードを含むシングルリング構成では，次に示す動作はスタック構成のノードを含まないシングルリング構成時と同様ですので，「28.3　シングルリングの動作概要」を参照してください。

- リング正常時の動作
- スタックを構成するメンバスイッチの障害を除く，障害検出時の動作
- スタックを構成するメンバスイッチの障害を除く，復旧検出時の動作

28.5.2　マルチリングでの動作

スタック構成のノードを含むマルチリング構成について，次の図に例を示します。

図 28-23　スタック構成のノードを含む共有リンクなしのマルチリング構成

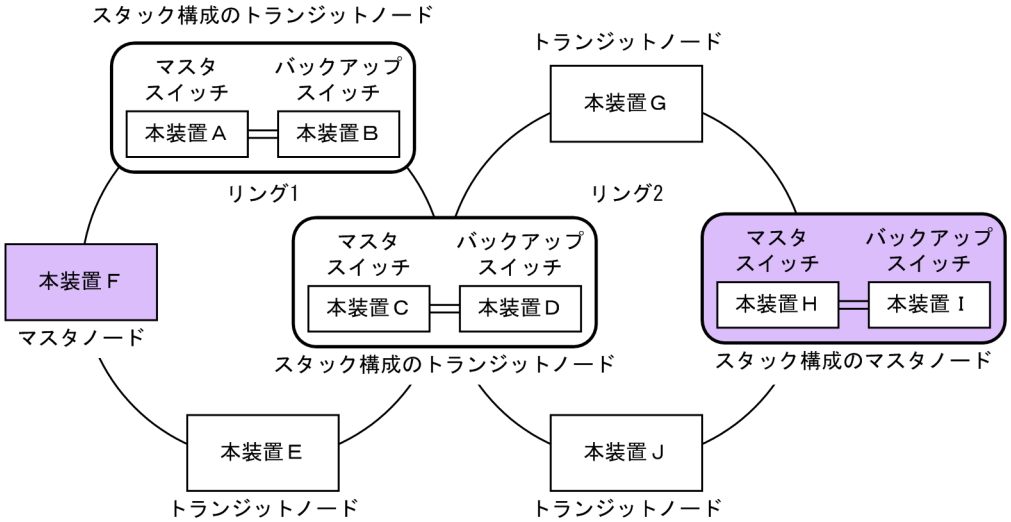
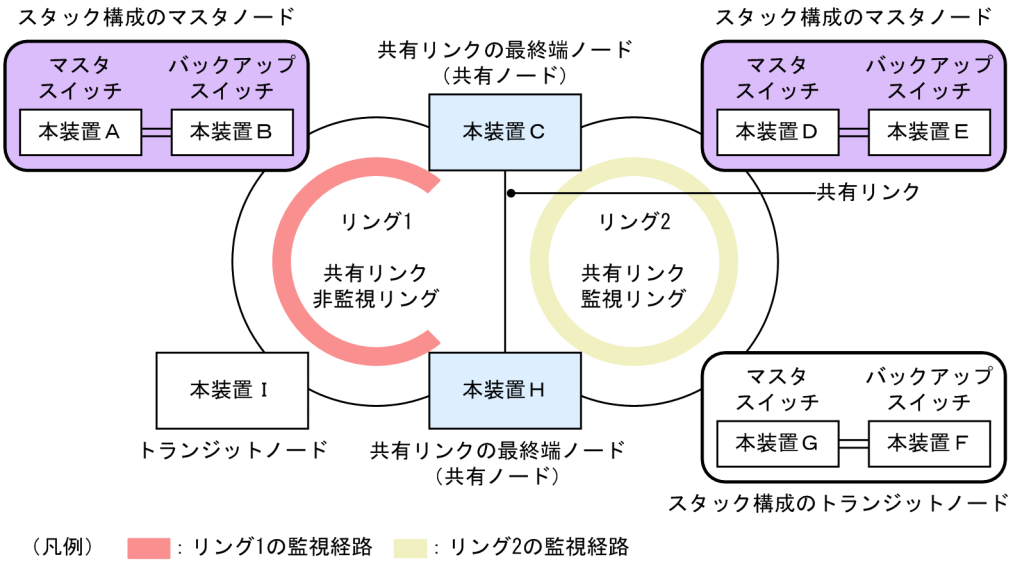


図 28-24　スタック構成のノードを含む共有リンクありのマルチリング構成



スタック構成のノードを含むマルチリング構成では，次に示す動作はスタック構成のノードを含まないマルチリング構成時と同様ですので，「28.4　マルチリングの動作概要」を参照してください。

- リング正常時の動作
- スタックを構成するメンバスイッチの障害を除く，障害検出時の動作
- スタックを構成するメンバスイッチの障害を除く，復旧検出時の動作

28.5.3　メンバスイッチの障害発生時および復旧時の動作

スタック構成のノードを含むリング構成での，メンバスイッチの障害発生時および復旧時の動作について説明します。

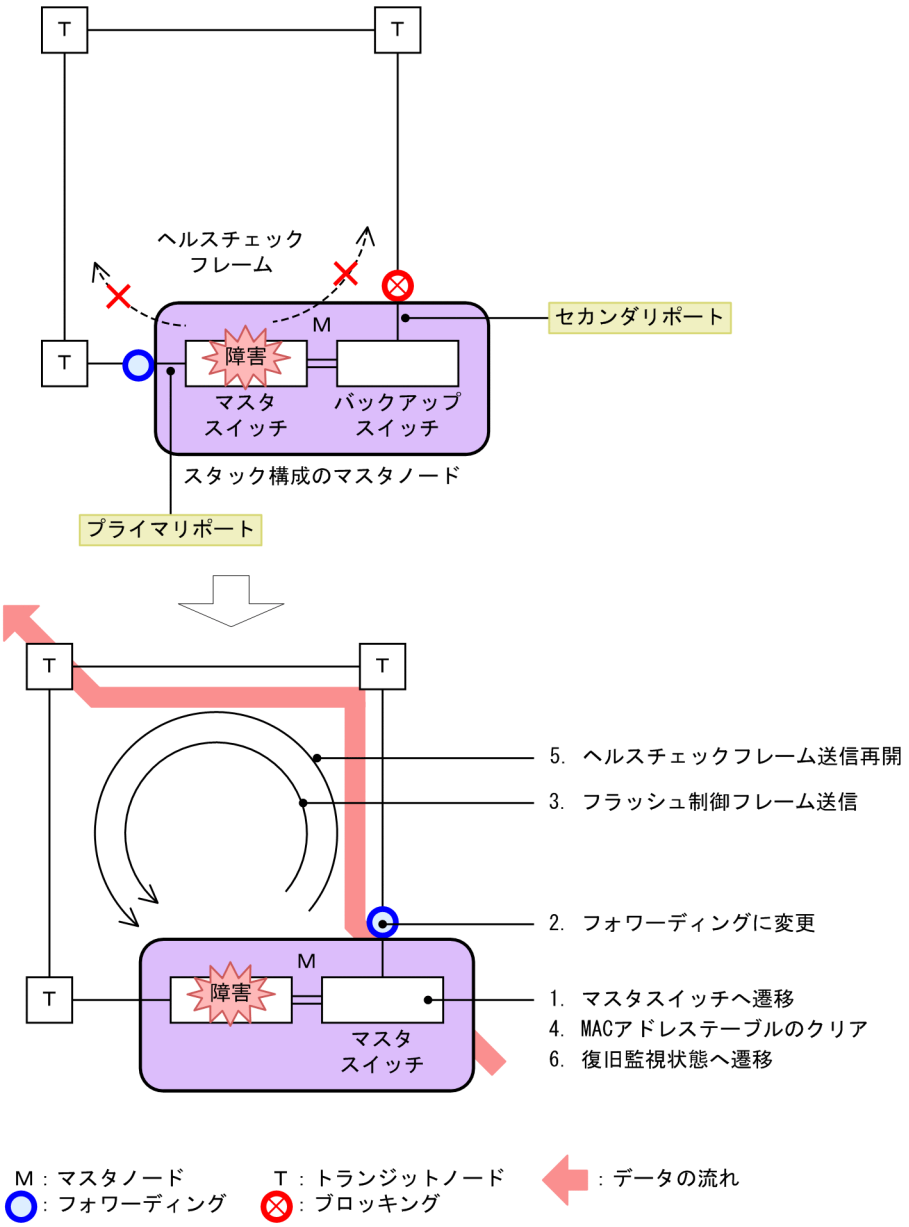
(1)　スタック構成のマスタノード動作

スタック構成のマスタノードでの，メンバスイッチの障害発生時および復旧時の動作について説明します。

(a)　マスタスイッチ障害発生時の動作

マスタスイッチに障害が発生した場合の動作について，次の図に示します。

図 28-25　マスタノードでのマスタスイッチ障害発生時の動作



マスタスイッチに障害が発生して停止すると，マスタスイッチが送信するヘルスチェックフレーム（HC(M)）が停止します。バックアップスイッチは新しいマスタスイッチに切り替わって，次に示す順序で動作します。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア

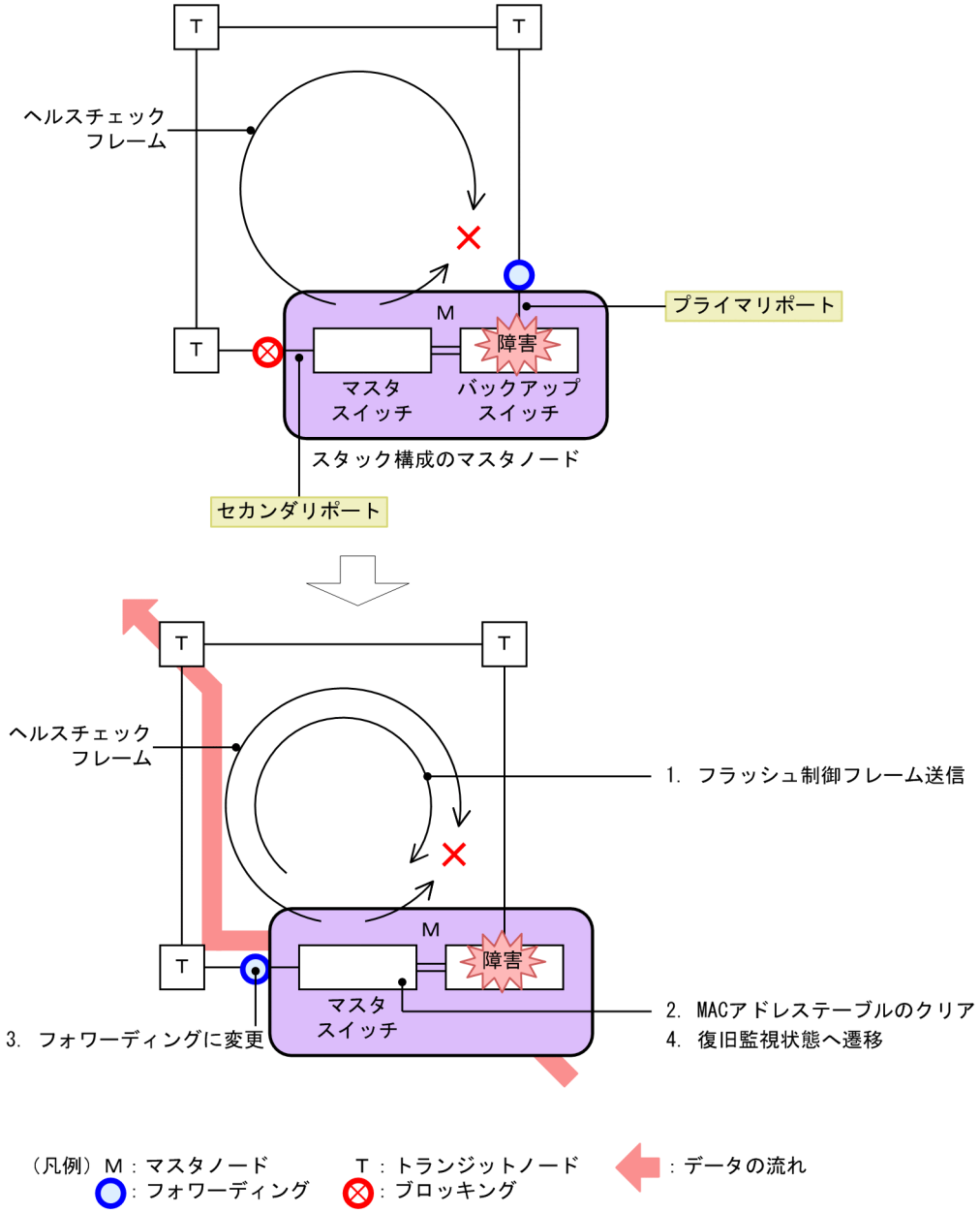
その後，マスタスイッチはリング状態の監視を開始して，ヘルスチェックフレーム（HC(M)）の送信を再開します。しかし，マスタスイッチは自身が送信するヘルスチェックフレーム（HC(M)）を受信できないため，リング障害を検出します。障害を検出したマスタスイッチは，監視状態を変更します。

マスタスイッチが切り替わるとき，新しいマスタスイッチは元のマスタスイッチのリング状態を引き継ぎません。

(b)　バックアップスイッチ障害発生時の動作

バックアップスイッチに障害が発生した場合の動作について，次の図に示します。

図 28-26　マスタノードでのバックアップスイッチ障害発生時の動作



バックアップスイッチに障害が発生して停止すると，マスタスイッチは両方向のヘルスチェックフレーム（HC(M)）を受信できなくなり，リング障害を検出します。障害を検出したマスタスイッチは，次に示す順序で動作します。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信

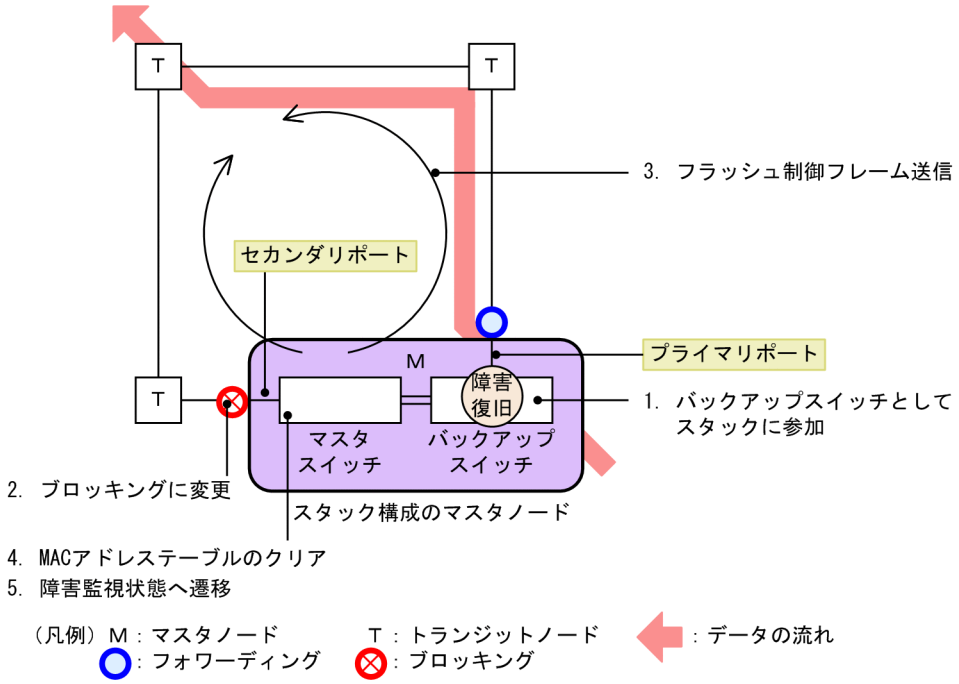
3. MAC アドレステーブルのクリア

4. 監視状態の変更

(c)　メンバスイッチ障害復旧時の動作

メンバスイッチが障害から復旧した場合の動作について，次の図に示します。

図 28-27　マスタノードでのメンバスイッチ障害復旧時の動作



メンバスイッチが障害から復旧すると，このメンバスイッチはバックアップスイッチになって，メンバスイッチ 2 台のスタックを構成します。

バックアップスイッチが復旧すると，マスタスイッチは，自身が送信するヘルスチェックフレーム（HC(M)）を受信できるようになります。リング障害を検出している状態で，自身が送信したヘルスチェックフレーム（HC(M)）を受信すると，マスタスイッチはリング障害が復旧したと判断して，次に示す順序で復旧動作をします。

1. データ転送用リング VLAN 状態の変更

2. フラッシュ制御フレームの送信

3. MAC アドレステーブルのクリア

4. 監視状態の変更

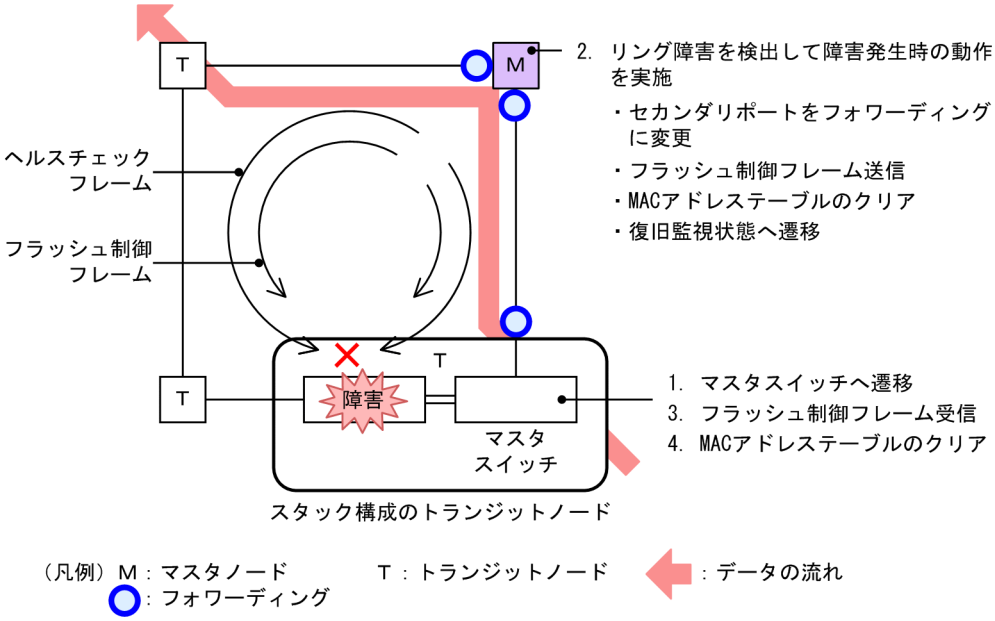
(2)　スタック構成のトランジットノード動作

スタック構成のトランジットノードでの，メンバスイッチの障害発生時および復旧時の動作について説明します。

(a)　メンバスイッチ障害発生時の動作

メンバスイッチに障害が発生した場合の動作について，次の図に示します。

図 28-28　トランジットノードでのメンバスイッチ障害発生時の動作



メンバスイッチに障害が発生すると，メンバスイッチ 1 台のスタックになります。

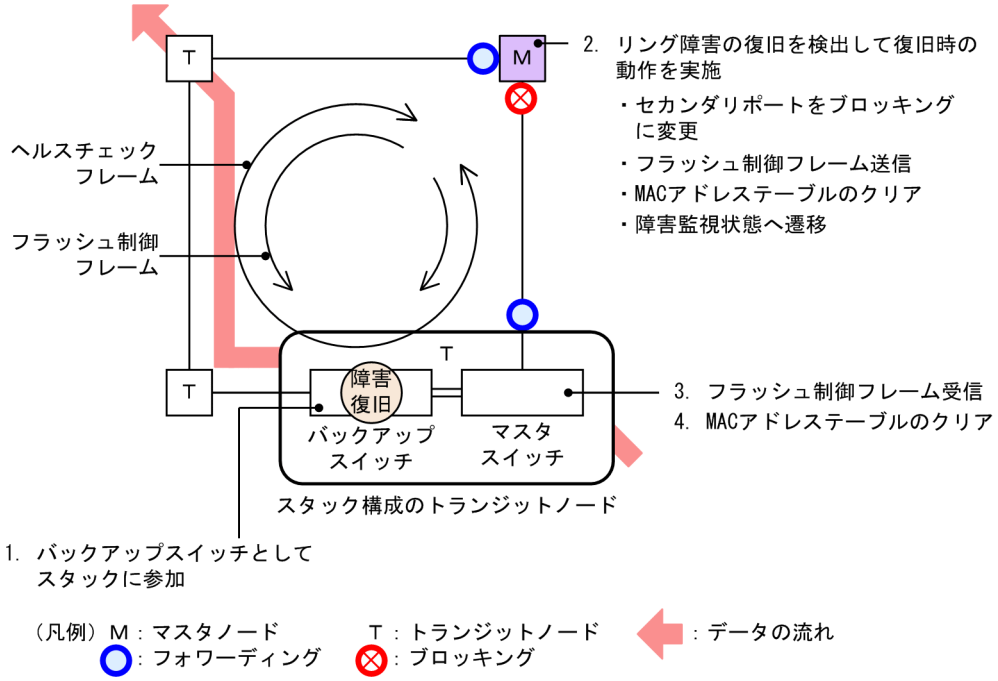
障害が発生したメンバスイッチのリングポートはダウン状態になるため，マスタノードでは両方向のヘルスチェックフレーム（HC(M)）を受信できなくなって，リング障害を検出します。障害を検出したマスタノードは，スタック構成のノードを含まないリング構成時と同様の順序で動作します。

障害が発生したトランジットノードのマスタスイッチは，マスタノードから送信されるフラッシュ制御フレームを受信すると，リングポートに関する MAC アドレステーブルエントリをクリアします。MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

(b)　メンバスイッチ障害復旧時の動作

メンバスイッチが障害から復旧した場合の動作について，次の図に示します。

図 28-29　トランジットノードでのメンバスイッチ障害復旧時の動作



メンバスイッチが障害から復旧すると，このメンバスイッチはバックアップスイッチになって，メンバスイッチ 2 台のスタックを構成します。

バックアップスイッチのリングポートが復旧することで，マスタノードでは，両方向のヘルスチェックフレーム（HC(M)）を受信できるようになります。リング障害を検出している状態で自身が送信したヘルスチェックフレーム（HC(M)）を受信すると，マスタノードはリング障害が復旧したと判断して，スタック構成のノードを含まないリング構成時と同様の順序で復旧動作をします。

障害が復旧したトランジットノードのマスタスイッチは，マスタノードから送信されるフラッシュ制御フレームを受信すると，リングポートに関する MAC アドレステーブルエントリをクリアします。MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

28.6　Ring Protocol の多重障害監視機能

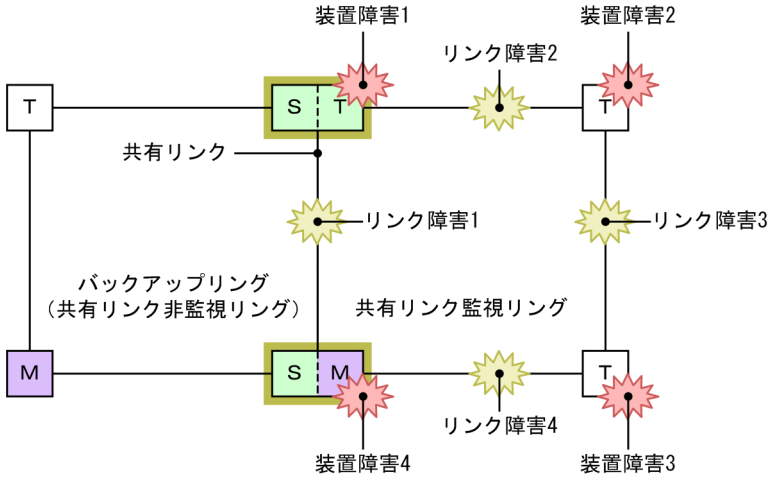
28.6.1　概要

多重障害監視機能は，共有リンクありのマルチリング構成での共有リンク監視リングの多重障害を監視して，多重障害を検出した場合に共有リンク非監視リングに経路を切り替える機能です。このとき，経路の切り替えに使用する共有リンク非監視リングを**バックアップリング**と呼びます。

多重障害監視機能で検出の対象となるのは，共有リンク障害と，共有リンク監視リング内のその他のリンク障害およびリンク障害を伴う装置障害です。

共有リンク監視リングでの障害発生例と，多重障害監視機能で検出できる障害の組み合わせを次に示します。

図 28-30　共有リンク監視リングでの障害発生例



（凡例）M：マスタノード　　T：トランジットノード
S：共有リンクの最終端ノード（トランジットノード）　　：共有ノード

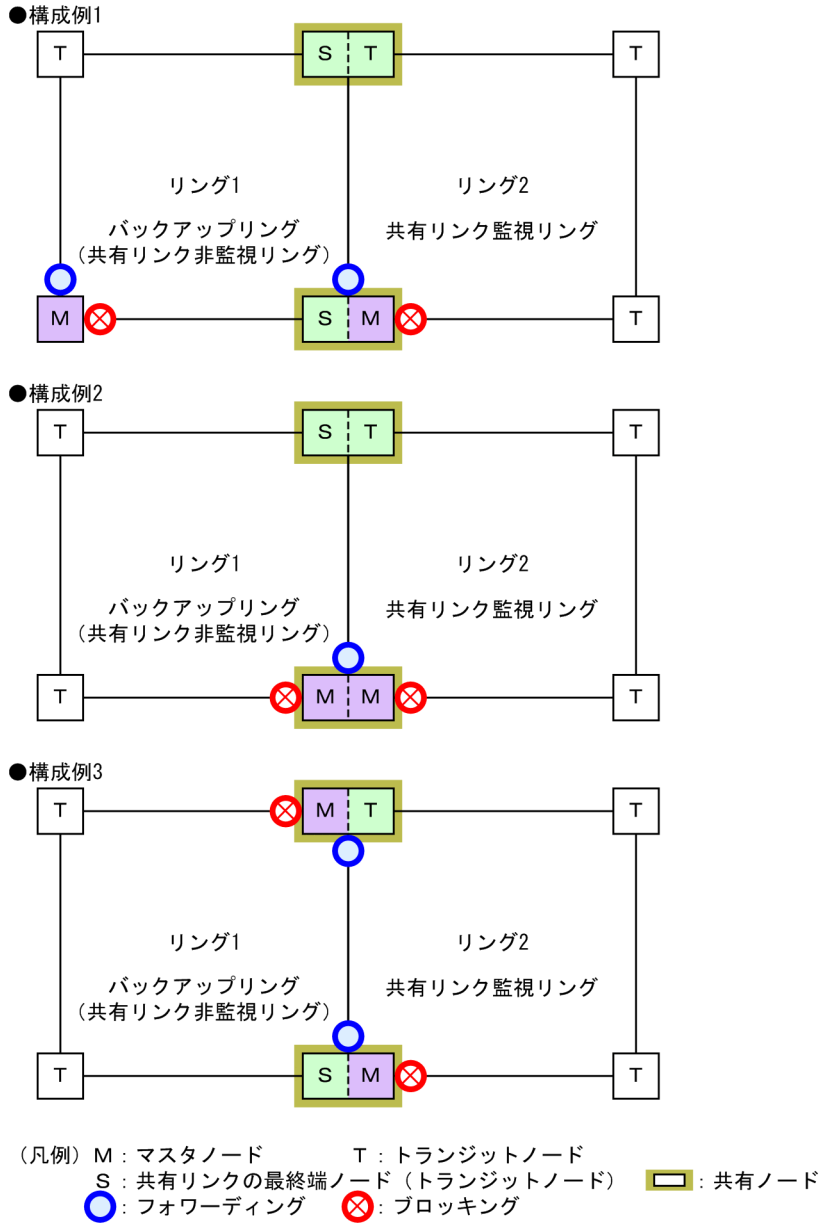
表 28-4　多重障害監視機能で検出できる障害の組み合わせ

障害種別	検出可能な組み合わせ	
リンク障害	リンク障害 1（共有リンク障害）	リンク障害 2（その他のリンク障害）
	リンク障害 1（共有リンク障害）	リンク障害 3（その他のリンク障害）
	リンク障害 1（共有リンク障害）	リンク障害 4（その他のリンク障害）
装置障害	装置障害 1（共有ノード障害）だけ	
	装置障害 4（共有ノード障害）だけ	
	装置障害 2（トランジットノード障害）	リンク障害 1（共有リンク障害）
	装置障害 3（トランジットノード障害）	リンク障害 1（共有リンク障害）

28.6.2　多重障害監視機能の基本構成

多重障害監視機能を適用できる共有リンクありのマルチリング構成は，共有リンク監視リングとバックアップリングとなる共有リンク非監視リングをそれぞれ 1 リングずつ対応づけた構成です。このとき，共有ノードを共有リンク監視リングのマスタノードとして設定します。多重障害監視機能の基本構成例を次の図に示します。

図 28-31　多重障害監視機能の基本構成例

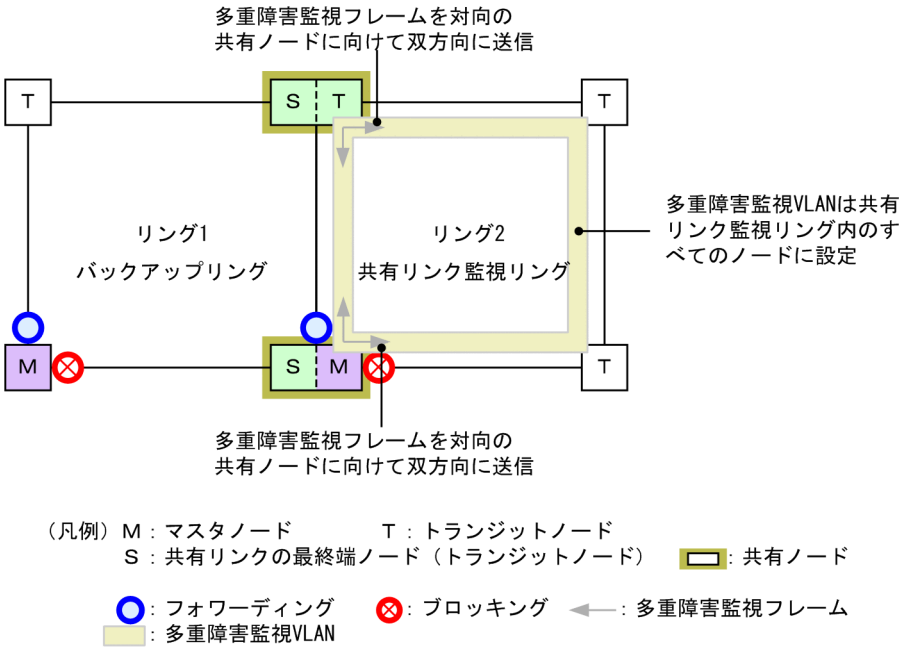


28.6.3　多重障害監視の動作概要

多重障害は，共有リンクありのマルチリング構成で共有リンクの両端に位置する共有ノードで監視します。共有ノードは，共有リンク監視リングの多重障害を監視するための制御フレーム（**多重障害監視フレーム**と呼びます）を送信します。対向の共有ノードでは，多重障害監視フレームの受信を監視します。なお，多重障害監視フレームは専用の VLAN（**多重障害監視 VLAN** と呼びます）上に送信します。

多重障害監視の動作概要を次の図に示します。

図 28–32　多重障害監視の動作概要



(1)　共有リンク監視リングの各ノードの動作

共有リンク監視リングのマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「28.4.1　リング正常時の動作　(2)　共有リンク監視リング」を参照してください。

共有ノードでは，共有リンク監視リングの多重障害を監視します。共有ノードは，多重障害監視フレームを両リングポートから送信するとともに，対向の共有ノードが両リングポートから送信した多重障害監視フレームをあらかじめ設定した時間内に受信するかを監視します。

(2)　バックアップリングの各ノードの動作

バックアップリングのマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「28.4.1　リング正常時の動作　(1)　共有リンク非監視リング」を参照してください。

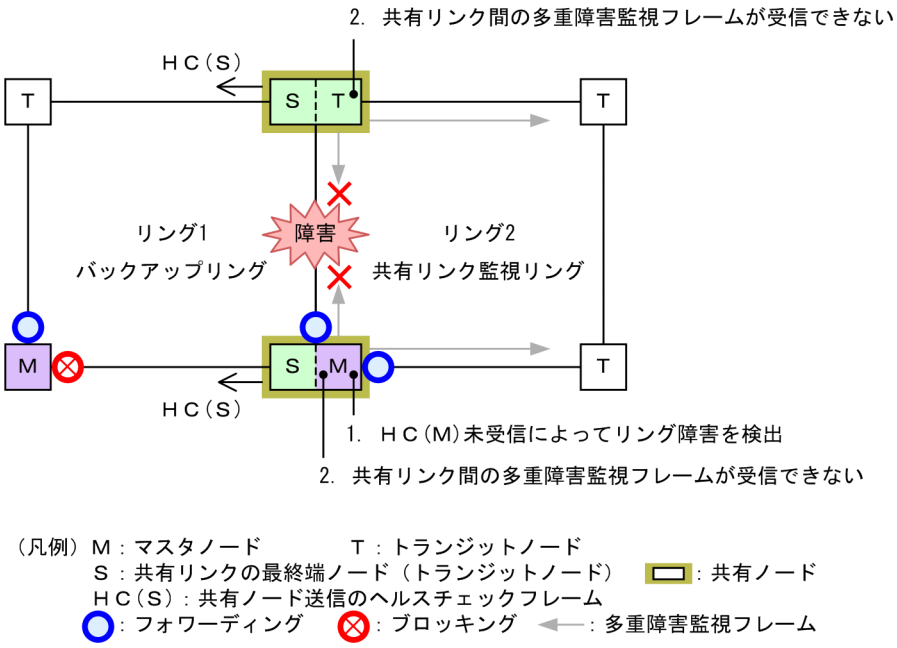
28.6.4　多重障害発生時の動作

共有リンク監視リングで，共有リンク障害とその他のリンク障害による多重障害が発生した場合の動作について説明します。

(1)　共有リンク障害時の動作

共有リンク監視リングでの共有リンク障害時の動作について，次の図に示します。

図 28-33　共有リンク障害時の動作



(a)　共有リンク監視リングの各ノードの動作

1.　HC(M)未受信によってリング障害を検出

マスタノードは両方向の HC(M)を受信できなくなり，リング障害を検出します。リング障害検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「28.4.2 共有リンク障害・復旧時の動作　(1)　障害検出時の動作」を参照してください。

2.　共有リンク間の多重障害監視フレームが受信できない

共有ノードは共有リンク間での多重障害監視フレームの受信ができなくなりますが，もう一方のリングポートでは受信できているため，多重障害の監視を継続します。

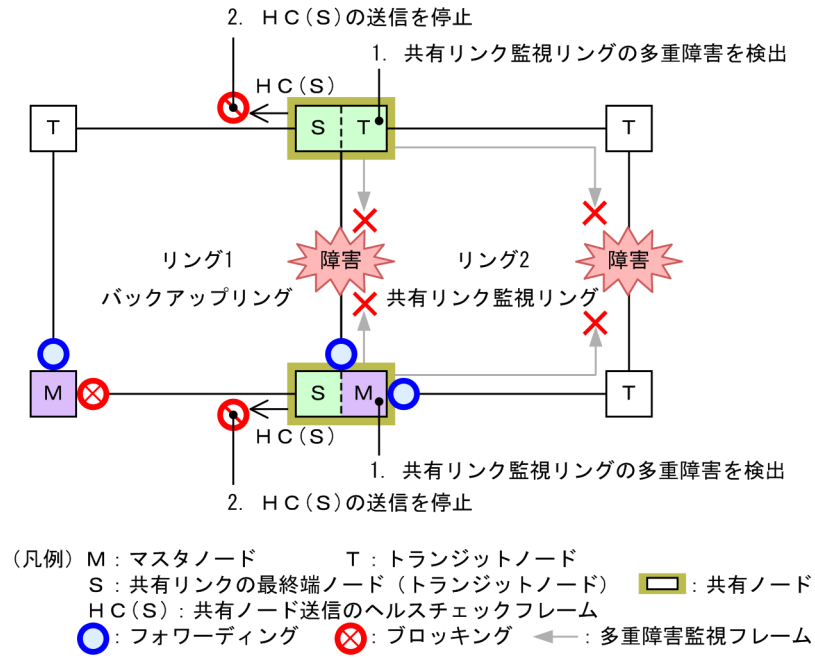
(b)　バックアップリングの各ノードの動作

バックアップリングではマスタノードが送信した HC(M)の受信はできなくなりますが，共有ノードが送信した HC(S)は受信できているため，障害検出時の動作は行いません。

(2)　多重障害発生時の動作

共有リンク障害と共有リンク監視リング内のその他のリンク障害による多重障害発生時の動作について，次の図に示します。

図 28-34　多重障害発生時の動作



(a)　共有リンク監視リングの各ノードの動作

1.　共有リンク監視リングの多重障害を検出

共有ノードは両リングポートで多重障害監視フレームを受信できなくなり，多重障害を検出します。

(b)　バックアップリングの各ノードの動作

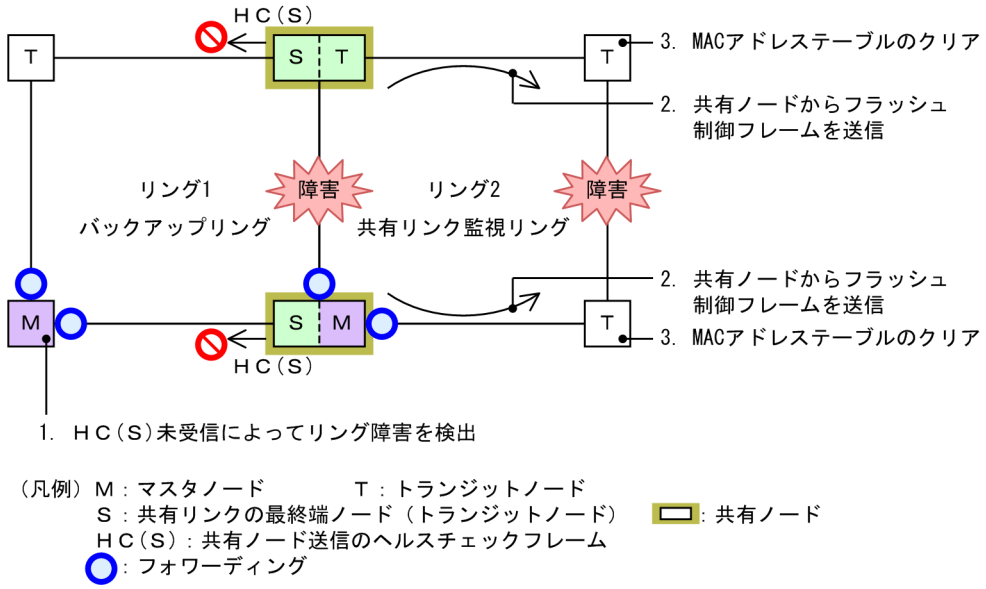
2.　HC(S)の送信を停止

多重障害を検出した共有ノードは，バックアップリングの HC(S)の送信を停止します。

(3)　バックアップリングへの切り替え動作

多重障害検出によるバックアップリングへの切り替え動作について，次の図に示します。

図 28-35　バックアップリングへの切り替え動作



(a)　バックアップリングの各ノードの動作

1.　HC(S)未受信によってリング障害を検出

マスタノードは自身が送信した両方向の HC(M)と共有ノードが送信した HC(S)がどちらも未受信となり，リング障害を検出します。リング障害検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「28.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作　(1)　障害検出時の動作」を参照してください。

(b)　共有リンク監視リングの各ノードの動作

2.　共有ノードからフラッシュ制御フレームを送信

バックアップリングのマスタノードから送信されたフラッシュ制御フレームを受信すると，共有ノードは共有リンク監視リングに向けて，MAC アドレステーブルのクリアだけをするフラッシュ制御フレームを送信します。

3.　MAC アドレステーブルのクリア

トランジットノードは共有ノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

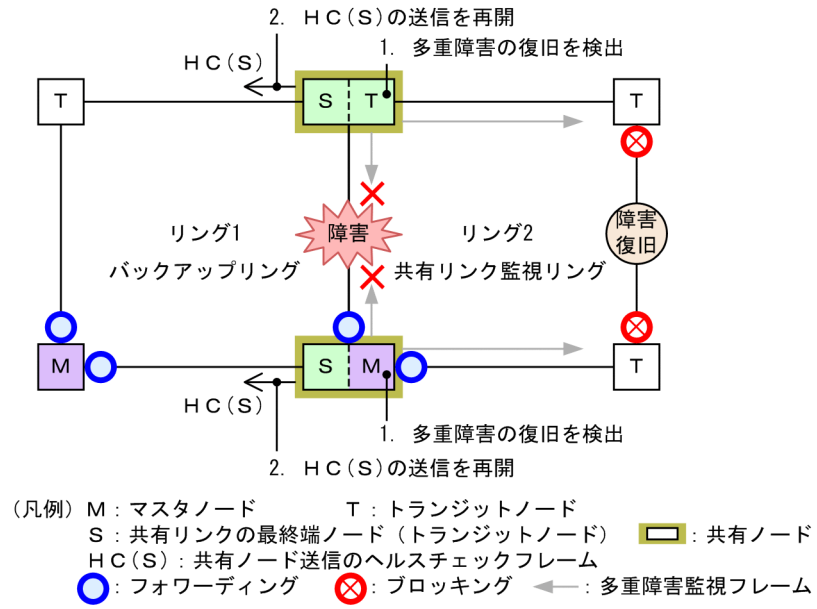
28.6.5　多重障害復旧時の動作

共有リンク監視リングでの多重障害が復旧した場合の動作について説明します。

(1)　多重障害からの一部復旧時の動作

共有リンク監視リングで多重障害からの一部復旧時の動作について，次の図に示します。

図 28-36　多重障害からの一部復旧時の動作



(a)　共有リンク監視リングの各ノードの動作

1.　多重障害の復旧を検出

共有ノードは対向の共有ノードが送信した多重障害監視フレームを受信して，多重障害の復旧を検出します。

(b)　バックアップリングの各ノードの動作

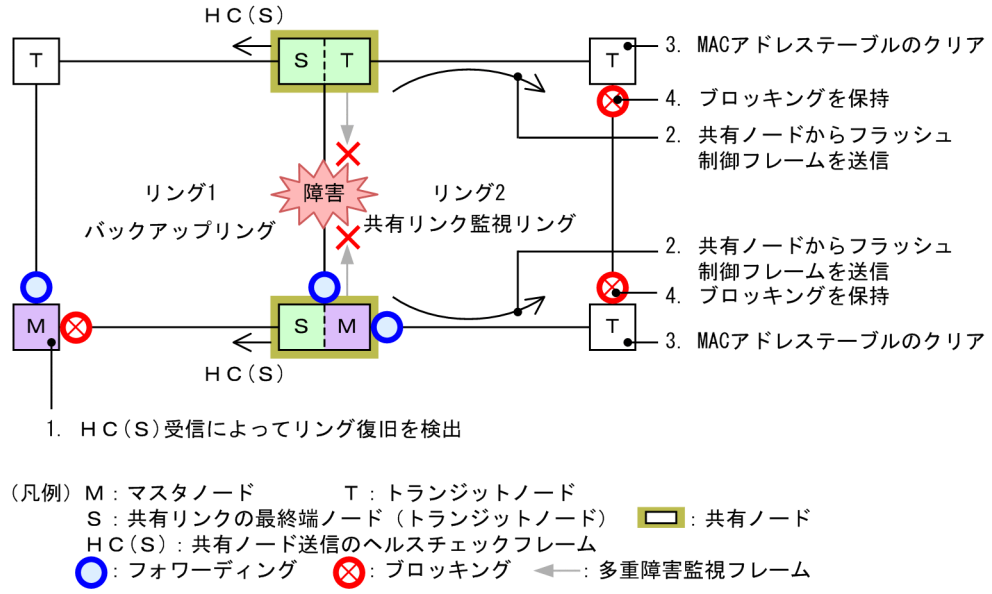
2.　HC(S)の送信を再開

多重障害の復旧を検出した共有ノードは，バックアップリングの HC(S)の送信を再開します。

(2)　バックアップリングからの切り戻し動作

バックアップリングからの切り戻し動作について，次の図に示します。

図 28-37　バックアップリングからの切り戻し動作



(a)　バックアップリングの各ノードの動作

1.　HC(S)受信によってリング復旧を検出

マスタノードは共有ノードが送信した HC(S)を両方向から受信すると，リング障害が復旧したと判断して復旧動作を行います。復旧検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「28.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作　(2)　復旧検出時の動作」を参照してください。

(b)　共有リンク監視リングの各ノードの動作

2.　共有ノードからフラッシュ制御フレームを送信

バックアップリングのマスタノードから送信されたフラッシュ制御フレームを受信すると，共有ノードは共有リンク監視リングに向けて，MAC アドレステーブルのクリアだけをするフラッシュ制御フレームを送信します。

3.　MAC アドレステーブルのクリア

トランジットノードは共有ノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

4.　ブロッキングを保持

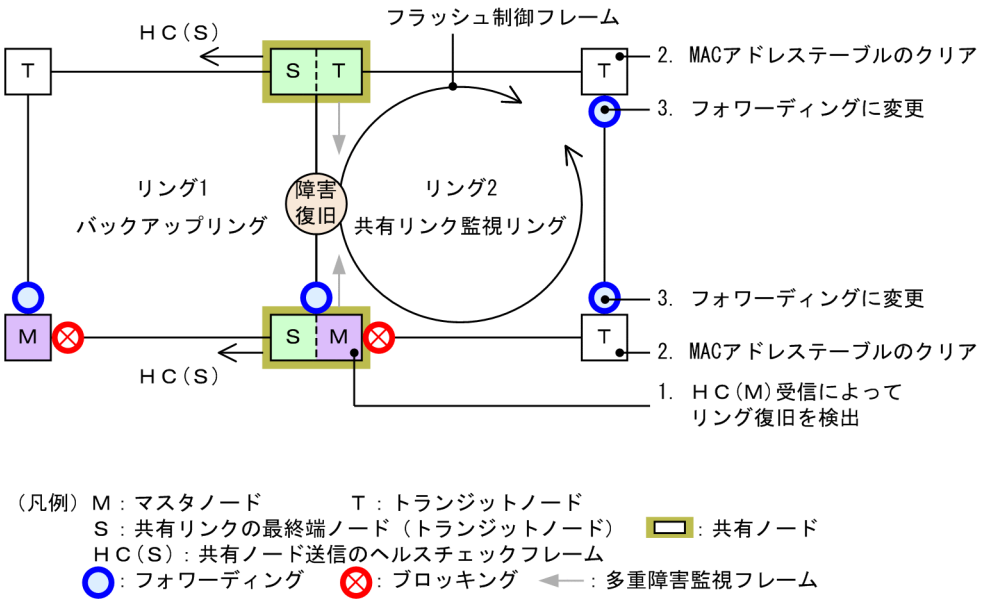
リンク障害から復旧したリングポートのリング VLAN 状態は，マスタノードがリング復旧を検出していないため，ブロッキングを保持します。

なお，ブロッキングの解除については「28.8　Ring Protocol 使用時の注意事項　(18)　多重障害の一部復旧時の通信について」を参照してください。

(3)　共有リンク障害復旧時の動作

共有リンク障害復旧時の動作について，次の図に示します。

図 28-38　共有リンク障害復旧時の動作



(a)　共有リンク監視リングの各ノードの動作

1. HC(M)受信によってリング復旧を検出

マスタノードは自身が送信した HC(M)を受信すると，リング障害が復旧したと判断して復旧動作を行います。復旧検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「28.4.2　共有リンク障害・復旧時の動作　(2)　復旧検出時の動作」を参照してください。

2. MAC アドレステーブルのクリア

トランジットノードはマスタノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

3. フォワーディングに変更

トランジットノードはマスタノードが送信したフラッシュ制御フレームの受信によって，リンク障害から復旧したリングポートのリング VLAN 状態をフォワーディングに変更します。

28.7　Ring Protocol のネットワーク設計

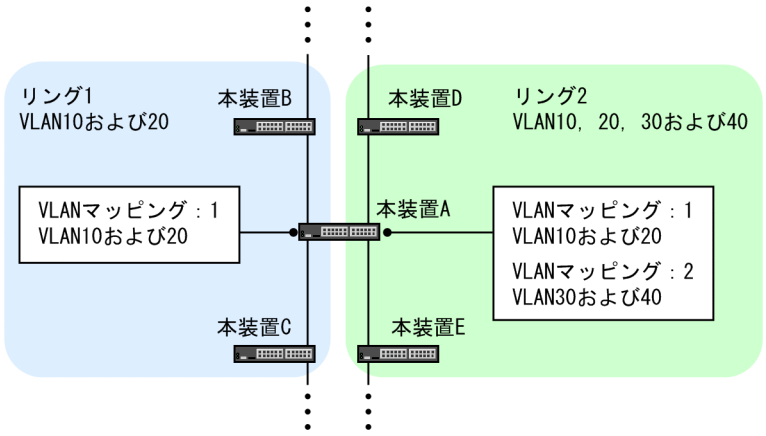
28.7.1　VLAN マッピングの使用方法

(1)　VLAN マッピングとデータ転送用 VLAN

マルチリング構成などで，一つの装置に複数のリング ID を設定するような場合，それぞれのリング ID に複数の同一 VLAN を設定する必要があります。このとき，データ転送用 VLAN として使用する VLAN のリスト（これを **VLAN マッピング**と呼びます）をあらかじめ設定しておくと，マルチリング構成時のデータ転送用 VLAN の設定を簡略できたり，コンフィグレーションの設定誤りによるループなどを防止できたりします。

VLAN マッピングは，データ転送用に使用する VLAN を VLAN マッピング ID に割り当てて使用します。この VLAN マッピング ID を VLAN グループに設定して，データ転送用 VLAN として管理します。

図 28–39　リングごとの VLAN マッピングの割り当て例



(2)　PVST+と併用する場合の VLAN マッピング

Ring Protocol と PVST+を併用する場合は，PVST+に使用する VLAN を VLAN マッピングにも設定します。このとき，VLAN マッピングに割り当てる VLAN は一つだけにしてください。PVST+と併用する VLAN 以外のデータ転送用 VLAN は，別の VLAN マッピングに設定して，PVST+と併用する VLAN マッピングと合わせて VLAN グループに設定します。

28.7.2　制御 VLAN の forwarding-delay-time の使用方法

トランジットノードの装置起動やプログラム再起動（運用コマンド restart axrp）など，Ring Protocol が初期状態から動作する場合，データ転送用 VLAN は論理ブロックされています。トランジットノードは，マスタノードが送信するフラッシュ制御フレームを受信することでこの論理ブロックを解除します。しかし，プログラム再起動時などは，マスタノードの障害監視時間（health-check holdtime）が長いと，リングネットワークの状態変化を認識できないおそれがあります。この場合，フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）がタイムアウトするまで論理ブロックは解除されないため，トランジットノードのデータ VLAN は通信できない状態になります。制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）を設定すると次に示す手順で動作するため，このようなケースを回避できます。

1. トランジットノードは，装置起動やプログラム再起動直後に，制御 VLAN をいったん論理ブロックします。

2. トランジットノードの制御 VLAN が論理ブロックされたので，マスタノードで障害を検出します（ただし，装置起動時はこれ以前に障害を検出しています）。このため，通信は迂回経路に切り替わります。
3. トランジットノードは，制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）のタイムアウトによって制御 VLAN のブロッキングを解除します。
4. マスタノードはヘルスチェックフレームを受信することで復旧を検出し，フラッシュ制御フレームを送信します。
5. トランジットノードは，このフラッシュ制御フレームを受信することでデータ転送用 VLAN の論理ブロックを解除します。これによってデータ転送用 VLAN での通信が再開され，リングネットワーク全体でも通常の通信経路に復旧します。

(1) 制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）と障害監視時間（health-check holdtime）の関係について

制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）は，障害監視時間（health-check holdtime）より大きな値を設定してください。制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）は，障害監視時間（health-check holdtime）の 2 倍程度を目安として設定することを推奨します。障害監視時間（health-check holdtime）より小さな値を設定した場合，マスタノードで障害を検出できません。したがって，迂回経路への切り替えが行われないため，通信断の時間が長くなるおそれがあります。

28.7.3　プライマリポートの自動決定

マスタノードのプライマリポートは，ユーザが設定した二つのリングポートの情報に従って，自動で決定します。次の表に示すように，優先度の高い方がプライマリポートとして動作します。また，VLAN グループごとに優先度を逆にすることで，ユーザが特に意識することなく，経路の振り分けができるようになります。

表 28-5　プライマリポートの選択方式（VLAN グループ＃1）

リングポート＃1	リングポート＃2	優先ポート
物理ポート	物理ポート	ポート番号の小さい方がプライマリポートとして動作※
物理ポート	チャネルグループ	物理ポート側がプライマリポートとして動作
チャネルグループ	物理ポート	物理ポート側がプライマリポートとして動作
チャネルグループ	チャネルグループ	チャネルグループ番号の小さい方がプライマリポートとして動作

注※

スタック構成時は，スイッチ番号の小さい方がプライマリポートとして動作します。

表 28-6　プライマリポートの選択方式（VLAN グループ＃2）

リングポート＃1	リングポート＃2	優先ポート
物理ポート	物理ポート	ポート番号の大きい方がプライマリポートとして動作※
物理ポート	チャネルグループ	チャネルグループ側がプライマリポートとして動作
チャネルグループ	物理ポート	チャネルグループ側がプライマリポートとして動作

リングポート＃1	リングポート＃2	優先ポート
チャネルグループ	チャネルグループ	チャネルグループ番号の大きい方がプライマリポートとして動作

注※

スタック構成時は，スイッチ番号の大きい方がプライマリポートとして動作します。

また，上記の決定方式以外に，コンフィグレーションコマンド axrp-primary-port を使って，ユーザが VLAN グループごとにプライマリポートを設定することもできます。

28.7.4　同一装置内でのノード種別混在構成

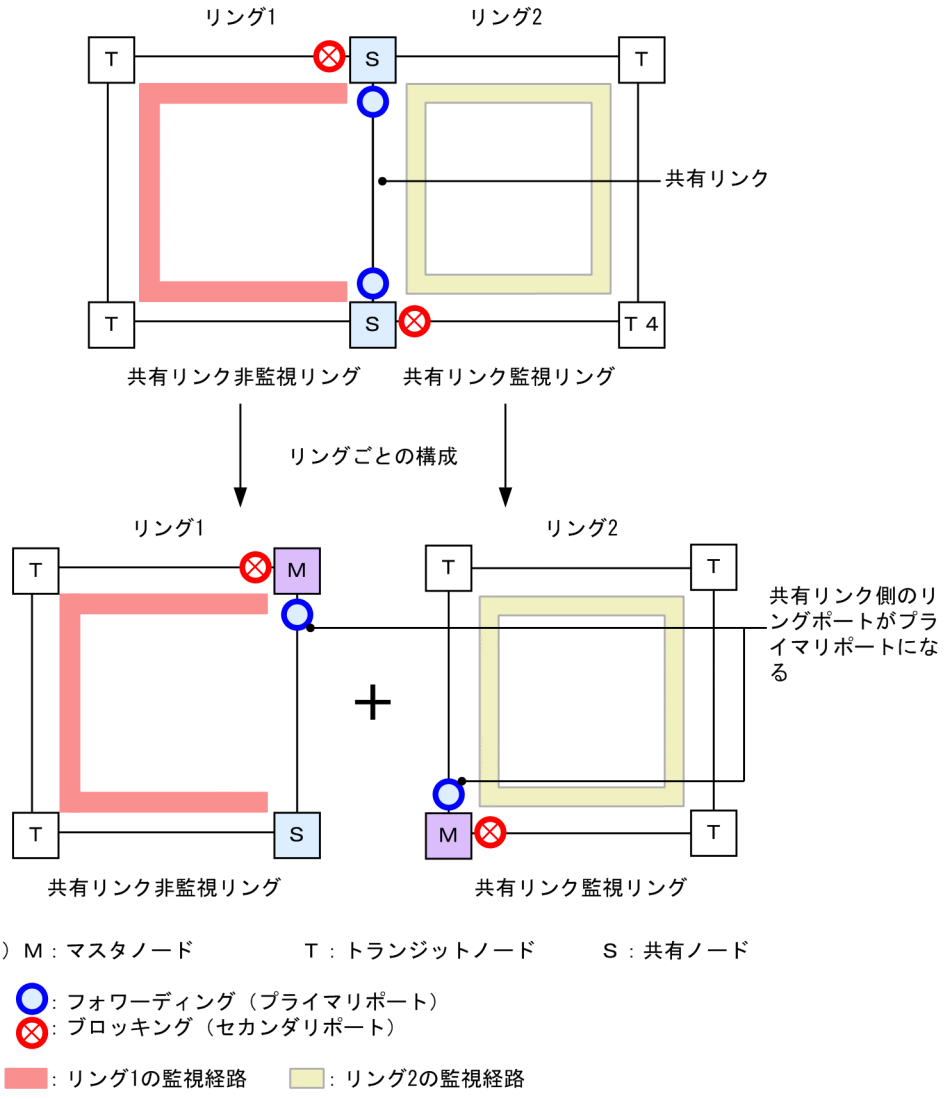
(1)　ノード種別の混在設定

本装置が，二つの異なるリングに属している場合に，一方のリングではマスタノードとして動作し，もう一方のリングではトランジットノードとして動作させることができます。

28.7.5　共有ノードでのノード種別混在構成

共有リンクありのマルチリング構成で，共有リンクの両端に位置するノードをマスタノードとして動作させることができます。この場合，マスタノードのプライマリポートは，データ転送用の VLAN グループによらず，必ず共有リンク側のリングポートになります。このため，本構成では，データ転送用の VLAN グループを二つ設定したことによる負荷分散は実現できません。

図 28-40　共有ノードをマスタノードとした場合のポート状態



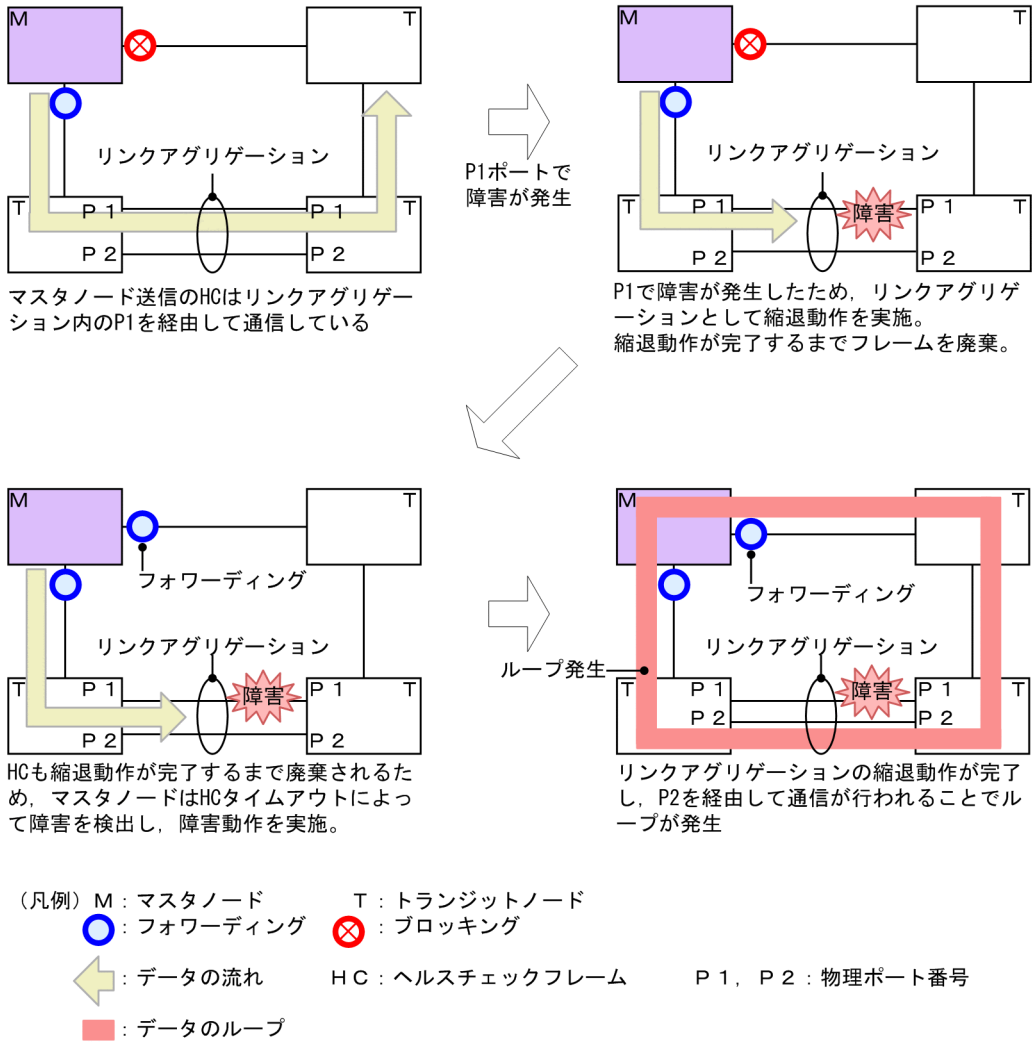
28.7.6　リンクアグリゲーションを用いた場合の障害監視時間の設定

リングポートをリンクアグリゲーションで構成した場合に，ヘルスチェックフレームが転送されているリンクアグリゲーション内のポートに障害が発生すると，リンクアグリゲーションの切り替えまたは縮退動作が完了するまでの間，制御フレームが廃棄されてしまいます。このため，マスタノードの障害監視時間（health-check holdtime）がリンクアグリゲーションの切り替えまたは縮退動作が完了する時間よりも短いと，マスタノードがリングの障害を誤検出し，経路の切り替えを行います。この結果，ループが発生するおそれがあります。

リングポートをリンクアグリゲーションで構成した場合は，マスタノードの障害監視時間をリンクアグリゲーションによる切り替えまたは縮退動作が完了する時間よりも大きくする必要があります。

なお，LACP によるリンクアグリゲーションを使用する場合は，LACPDU の送信間隔の初期値が long（30 秒）となっていますので，初期値を変更しないまま運用すると，ループが発生するおそれがあります。LACP によるリンクアグリゲーションを使用する際は，マスタノードの障害監視時間を変更するか，LACPDU の送信間隔を short（1 秒）に設定してください。

図 28-41　リンクアグリゲーション使用時の障害検出



28.7.7　IEEE802.3ah/UDLD 機能との併用

本プロトコルでは，片方向リンク障害での障害の検出および切り替え動作は実施しません。片方向リンク障害発生時にも切り替え動作を実施したい場合は，IEEE802.3ah/UDLD 機能を併用してください。リング内のノード間を接続するリングポートに対して IEEE802.3ah/UDLD 機能の設定を行います。
IEEE802.3ah/UDLD 機能によって，片方向リンク障害が検出されると，該当ポートを閉塞します。これによって，該当リングを監視するマスタノードはリング障害を検出し，切り替え動作を行います。

28.7.8　リンクダウン検出タイマおよびリンクアップ検出タイマとの併用

リングポートに使用しているポート（物理ポートまたはリンクアグリゲーションに属する物理ポート）のリンク状態が不安定な場合，マスタノードがリング障害やリング障害復旧を連続で検出してリングネットワークが不安定な状態になり，ループや長時間の通信断が発生するおそれがあります。このような状態を防ぐには，リングポートに使用しているポートに対して，リンクダウン検出タイマおよびリンクアップ検出タイマを設定します。リンクダウン検出タイマおよびリンクアップ検出タイマの設定については，「20.3.8　リンクダウン検出タイマの設定」および「20.3.9　リンクアップ検出タイマの設定」を参照してください。

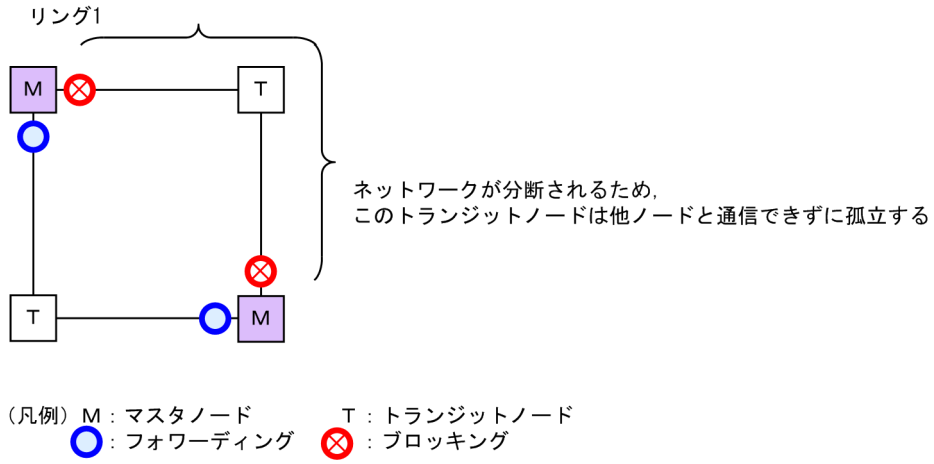
28.7.9　Ring Protocol の禁止構成

Ring Protocol を使用したネットワークでの禁止構成を次に示します。

(1)　同一リング内に複数のマスタノードを設定

同一のリング内に 2 台以上のマスタノードを設定しないでください。同一リング内に複数のマスタノードがあると，セカンダリポートが論理ブロックされるためにネットワークが分断されてしまい，適切な通信ができなくなります。

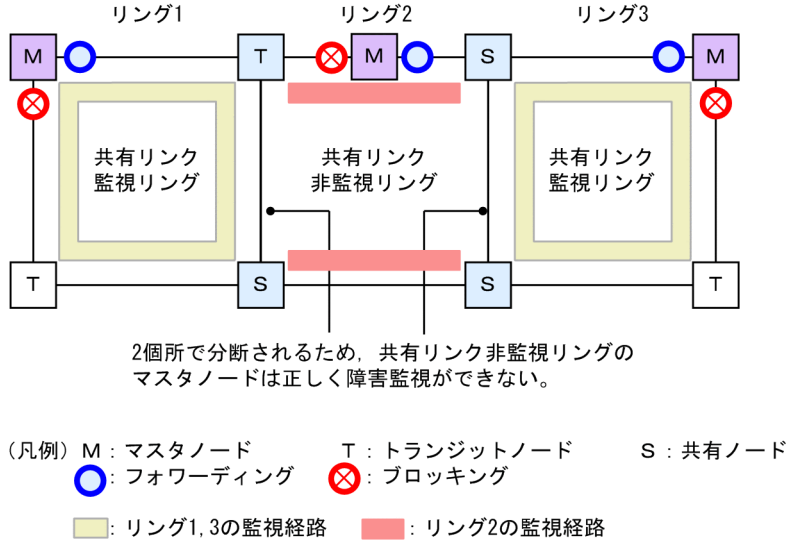
図 28-42　同一リング内に複数のマスタノードを設定



(2)　共有リンク監視リングが複数ある構成

共有リンクありのマルチリング構成では，共有リンク監視リングはネットワーク内で必ず一つとなるように構成してください。共有リンク監視リングが複数あると，共有リンク非監視リングでの障害監視が分断されるため，正しい障害監視ができなくなります。

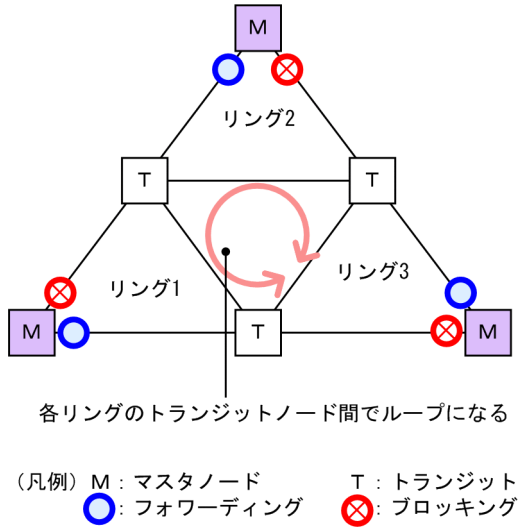
図 28-43　共有リンク監視リングが複数ある構成



(3)　ループになるマルチリング構成例

次に示す図のようなマルチリング構成を組むとトランジットノード間でループ構成となります。

図 28-44　ループになるマルチリング構成

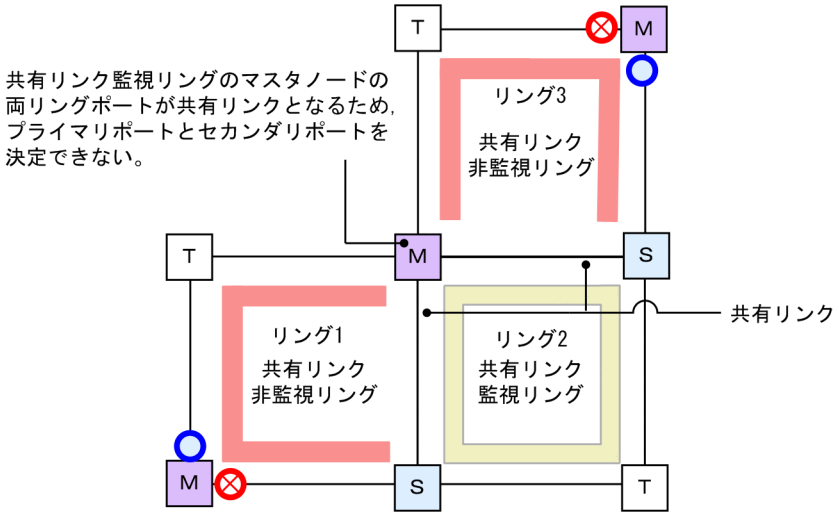


（凡例）M：マスタノード　T：トランジットノード
：フォワーディング　：ブロッキング

(4)　マスタノードのプライマリポートが決定できない構成

次の図のように，二つの共有リンク非監視リングの最終端に位置するノードにマスタノードを設定しないでください。このような構成の場合，マスタノードの両リングポートが共有リンクとなるため，プライマリポートを正しく決定できません。

図 28-45　マスタノードのプライマリポートが決定できない構成



（凡例）M：マスタノード　T：トランジットノード　S：共有ノード
：フォワーディング　：ブロッキング
：リング1，3の監視経路　：リング2の監視経路

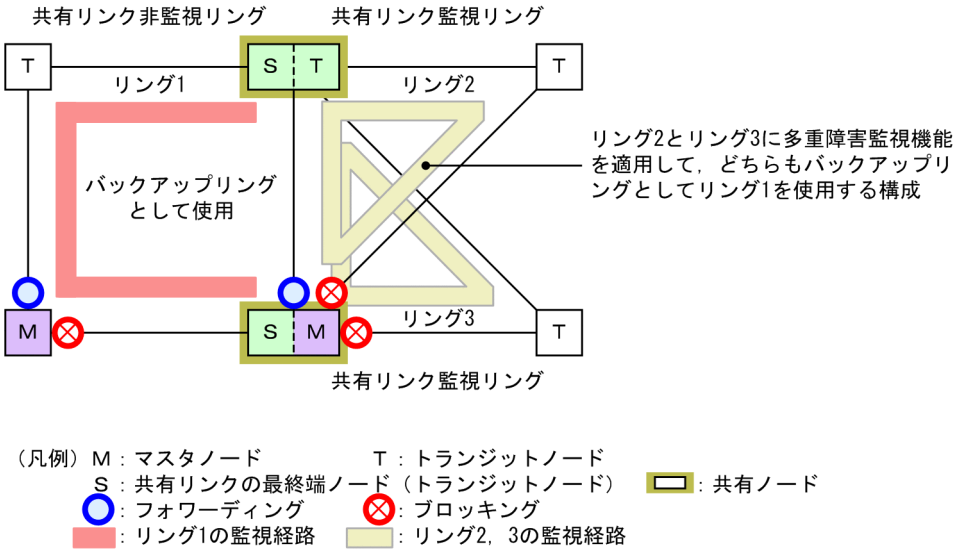
28.7.10　多重障害監視機能の禁止構成

多重障害監視機能使用時の禁止構成について次に示します。

(1)　複数の共有リンク監視リングが同じバックアップリングを使用する構成

共有リンク監視リングと，多重障害検出時にバックアップリングとして使用する共有リンク非監視リングは，1 対 1 に対応づけて構成する必要があります。複数の共有リンク監視リングが同じ共有リンク非監視リングをバックアップリングとして使用した場合，ある共有リンク監視リングで多重障害を検出したときに，別の共有リンク監視リングがバックアップリングにわたるループ構成となります。

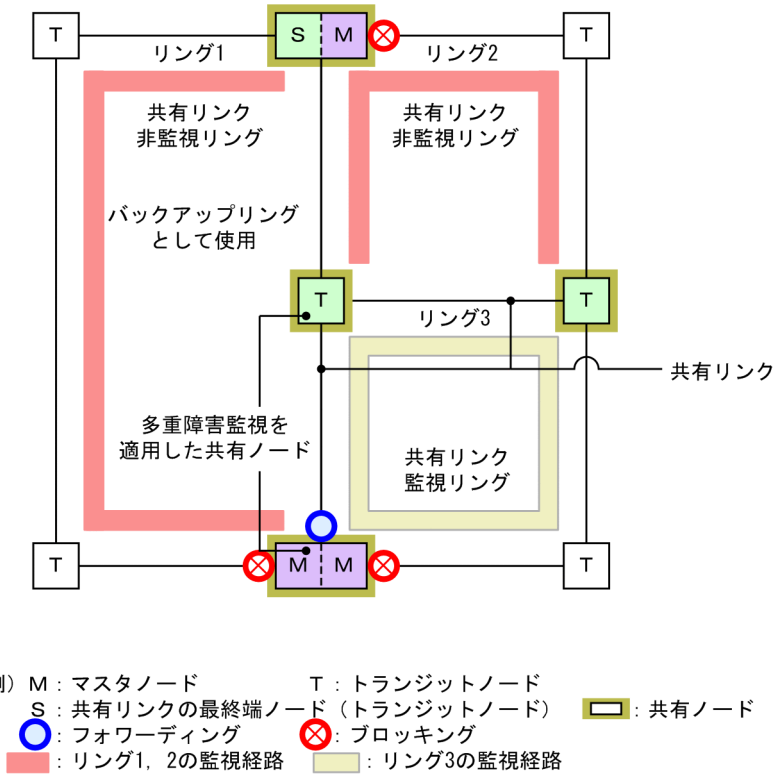
図 28-46　複数の共有リンク監視リングが同じバックアップリングを使用する構成



(2)　共有リンク内の共有ノードで多重障害を監視する構成

多重障害を監視する共有ノードは，共有リンクの最終端に位置する必要があります。このため，次の図に示すような構成では，共有リンク内の共有ノードが多重障害を監視することになり正常に監視できません。また，多重障害発生時にバックアップリングへの切り替えが正常にできません。

図 28-47　共有リンク内の共有ノードで多重障害を監視する構成

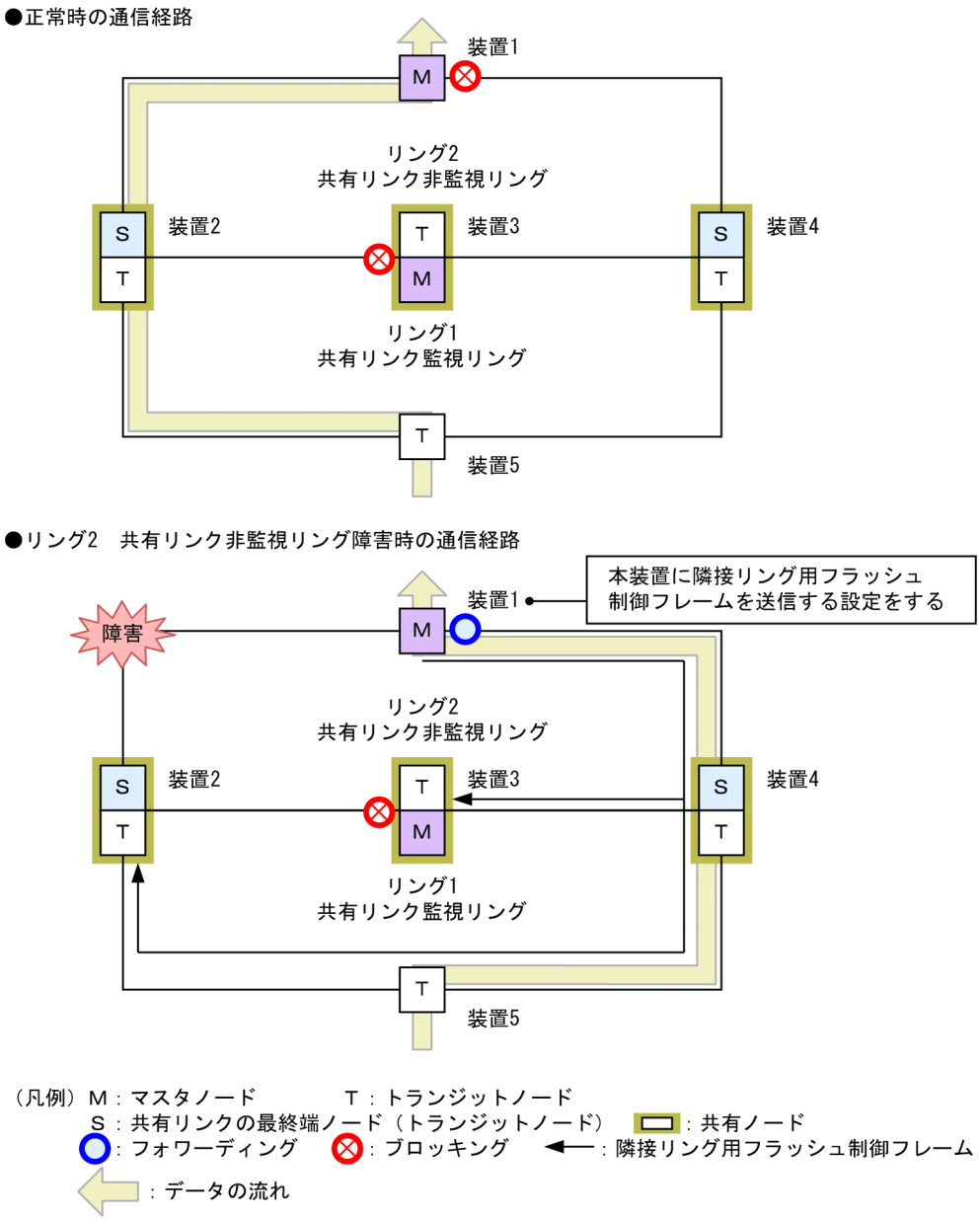


28.7.11　マスタノードの両リングポートが共有リンクとなる構成

次の図のように両リングポートが共有リンクとなるマスタノード（リング 1 の装置 3）が存在する共有リンクありのマルチリング構成では，共有リンク非監視リングのマスタノード（リング 2 の装置 1）に，コンフィグレーションコマンド flush-request-transmit vlan で隣接リング用フラッシュ制御フレームを送信する設定をしてください。

この設定によって，共有リンク非監視リングでリング障害が発生するとマスタノードは隣接するリングを構成する装置（以降，隣接リング構成装置）に隣接リング用フラッシュ制御フレームを送信するため，すぐに新しい通信経路に切り替えられます。なお，共有リンク非監視リングのリング障害が復旧した場合も同様になります。

図 28-48　マスタノードの両リングポートが共有リンクとなる構成例



このような構成で隣接リング用フラッシュ制御フレームを送信する設定をしない場合，共有リンク非監視リングでリング障害が発生すると，共有リンク非監視リングでは経路の切り替えが実施されますが，隣接する共有リンク監視リングでは実施されません。この結果，共有リンク監視リングを構成する装置では古い MAC アドレス学習の情報が残るため，すぐに新しい通信経路に切り替わらないおそれがあります。また，共有リンク非監視リングのリング障害が復旧した場合も同様になります。

28.7.12　スタック構成のノードを含むリングの障害監視時間の設定

スタックでは，複数のスタックリンクが設定されている場合，メンバスイッチ間の通信をロードバランスします。スタックリンクに障害が発生すると，障害が発生したスタックリンクに振り分けないよう切り替えますが，切り替えが完了するまでの間，一時的に通信が停止します。

そのとき，マスタノードの障害監視時間（health-check holdtime）がスタックリンクの切り替えが完了する時間よりも短いと，ヘルスチェックフレームが廃棄されるため，マスタノードがリング障害を誤検出して，経路を切り替えます。その結果，ループが発生するおそれがあります。このため，リング内にスタック構成のノードを含む場合は，マスタノードの障害監視時間を 1 秒以上に設定してください。

28.7.13　50 ミリ秒での経路切り替え【SL-L3A】

本装置では，次の表に示す条件をすべて満たすと，障害および障害復旧に伴うレイヤ 2 で中継するフレームの経路切り替えを 50 ミリ秒で実現できます。なお，リングネットワークを構築するすべてのマスタノードおよびトランジットノードが，これらの設定条件を満たす必要があります。50 ミリ秒での経路切り替えに必要な設定条件を次の表に示します。

表 28–7　50 ミリ秒での経路切り替えに必要な設定条件

設定項目	設定条件
1 リング当たりの総延長	100km 以内
1 リング当たりのノード数	100 台以内
リングポートの回線速度	1Gbit/s 以上
ヘルスチェックフレームの送信間隔	5 ミリ秒
障害監視時間	18 ミリ秒
装置当たりのリング数	2
1 リング当たりの VLAN マッピング数	2
コンフィグレーションコマンド mac-clear-mode の設定	MAC アドレステーブルの全エントリをクリア対象に指定
ルーティングテーブルエントリ数の配分パターン	次のどれかのモードであること • IPv4 モード • IPv4/IPv6 モード • IPv6 ユニキャスト優先モード

なお，次に示す条件に一致する場合，50 ミリ秒での経路切り替えの対象外となります。

- スタック機能が有効である
- 多重障害監視機能によって検知した障害または障害復旧である
- マスタノードの両リングポートが共有リンクとなるネットワーク構成である
- リングポートをリンクアグリゲーションで構成している
- 次を契機とした MAC アドレステーブルエントリのクリア処理中に発生した障害または障害復旧である
  - ほかのリングが障害中または復旧処理中
  - 運用コマンド clear mac-address-table の実行
  - スパニングツリーなど，ほかのレイヤ 2 ネットワークの冗長化機能による通信経路の切り替え
- 該当リングに対するコンフィグレーション変更（VLAN マッピングの追加など）の直後に発生した障害または障害復旧である

- 障害復旧による切り戻しの直後に発生した障害である

28.8　Ring Protocol 使用時の注意事項

(1)　運用中のコンフィグレーション変更について

運用中に，Ring Protocol の次に示すコンフィグレーションを変更する場合は，ループ構成にならないように注意が必要です。

- Ring Protocol 機能の停止（disable コマンド）
- 動作モード（mode コマンド）の変更および属性（ring-attribute パラメータ）の変更
- 制御 VLAN（control-vlan コマンド）の変更および制御 VLAN に使用している VLAN ID（vlan コマンド，switchport trunk コマンド，state コマンド）の変更
- データ転送用 VLAN（axrp vlan-mapping コマンド，vlan-group コマンド）の変更
- プライマリポート（axrp-primary-port コマンド）の変更
- 共有リンク監視リングのマスタノードが動作している装置に，共有リンク非監視リングの最終端ノードを追加（動作モードの属性に rift-ring-edge パラメータ指定のあるリングを追加）

これらのコンフィグレーションは，次の手順で変更することを推奨します。

1. コンフィグレーションを変更する装置のリングポート，またはマスタノードのセカンダリポートを shutdown コマンドなどでダウン状態にします。
2. コンフィグレーションを変更する装置の Ring Protocol 機能を停止（disable コマンド）します。
3. コンフィグレーションを変更します。
4. Ring Protocol 機能の停止を解除（no disable コマンド）します。
5. 事前にダウン状態としたリングポートをアップ（shutdown コマンドなどの解除）します。

(2)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(3)　制御フレームを送受信する VLAN について

- Ring Protocol の制御フレームは Tagged フレームになります。このため，Ring Protocol の制御フレームを送受信する次の VLAN は，トランクポートの allowed vlan（ネイティブ VLAN は不可）に設定してください。
  - 制御 VLAN
  - 多重障害監視用の VLAN
  - 隣接リング用フラッシュ制御フレームを送受信する VLAN
- Ring Protocol の制御フレームを送受信する VLAN を Tag 変換によって異なる VLAN ID に変換すると，正常に障害・復旧検出ができなくなります。Ring Protocol の制御フレームを送受信する VLAN に対して，Tag 変換は設定しないでください。

(4)　トランジットノードのリング VLAN 状態について

トランジットノードでは，装置またはリングポートが障害となり，その障害が復旧した際，ループの発生を防ぐために，リングポートのリング VLAN 状態はブロッキング状態となります。このブロッキング状態解除の契機の一つとして，フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）のタイムアウトがあります。このとき，フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）がマス

タノードのヘルスチェック送信間隔（health-check interval）よりも短い場合，マスタノードがリング障害の復旧を検出して，セカンダリポートをブロッキング状態に変更するよりも先に，トランジットノードのリングポートがフォワーディング状態となることがあり，ループが発生するおそれがあります。したがって，フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）はヘルスチェック送信間隔（health-check interval）より大きい値を設定してください。

スタック構成のマスタノードでメンバスイッチに障害が発生した場合，その障害が復旧するときに，スタックのメンバスイッチを追加します。このとき，隣接するトランジットノードのフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）がメンバスイッチの追加が完了する時間よりも短いと，トランジットノードのリングポートがフォワーディング状態となり，ループが発生するおそれがあります。このため，スタック構成のマスタノードに隣接するトランジットノードのフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）は，60 秒以上に設定してください。

(5)　共有リンクありのマルチリングでの VLAN 構成について

複数のリングで共通に使用する共有リンクでは，それぞれのリングで同じ VLAN を使用する必要があります。共有リンク間での VLAN のポートのフォワーディング／ブロッキング制御は共有リンク監視リングで行います。このため，共有リンク監視／非監視リングで異なる VLAN を使用すると，共有リンク非監視リングで使用している VLAN はブロッキングのままとなり，通信ができなくなります。

(6)　Ring Protocol 使用時のネットワーク構築について

Ring Protocol を利用するネットワークはループ構成となります。したがって，次の手順でネットワークを構築し，ループを防止してください。

1. 事前に，リング構成ノードのリングポート（物理ポートまたはチャネルグループ）を shutdown コマンドなどでダウン状態にしてください。
2. Ring Protocol のコンフィグレーションを設定するか，Ring Protocol の設定を含むコンフィグレーションファイルのコピー（copy コマンド）をして，Ring Protocol を有効にしてください。
3. ネットワーク内のすべての装置に Ring Protocol の設定が完了した時点でリングポートをアップ（shutdown コマンドなどの解除）してください。

(7)　ヘルスチェックフレームの送信間隔と障害監視時間について

障害監視時間（health-check holdtime）は送信間隔（health-check interval）より大きな値を設定してください。送信間隔よりも小さな値を設定すると，受信タイムアウトとなり障害を誤検出します。また，障害監視時間と送信間隔はネットワーク構成や運用環境などを十分に考慮した値を設定してください。障害監視時間は送信間隔の 3 倍以上を目安として設定することを推奨します。なお，送信間隔を 10 ミリ秒以下で設定する場合は，障害監視時間に送信間隔の 3 倍に 3 ミリ秒を加えた値を設定してください。推奨値を下回る値を設定した場合，ネットワークの負荷や装置の CPU 負荷などによって遅延が発生した場合に障害を誤検出するおそれがあります。

(8)　相互運用

Ring Protocol は，本装置独自仕様の機能です。他社スイッチとは相互運用できません。

(9)　リングを構成する装置について

- Ring Protocol を用いたネットワーク内で，本装置間に Ring Protocol をサポートしていない他社スイッチや伝送装置などを設置した場合，本装置のマスタノードが送信するフラッシュ制御フレームを解釈できないため，即時に MAC アドレステーブルエントリがクリアされません。その結果，通信経路の

切り替え（もしくは切り戻し）前の情報に従ってデータフレームの転送が行われるため，正しくデータが届かないおそれがあります。

(10) マスタノード障害時について

マスタノードが装置障害などによって通信できない状態になると，リングネットワークの障害監視が行われなくなります。このため，迂回経路への切り替えは行われずに，マスタノード以外のトランジットノード間の通信はそのまま継続されます。また，マスタノードが装置障害から復旧する際には，フラッシュ制御フレームをリング内のトランジットノードに向けて送信します。このため，一時的に通信が停止するおそれがあります。

(11) ネットワーク内の多重障害時について

同一リング内の異なるノード間で 2 個所以上の障害が起きた場合（多重障害），マスタノードは既に 1 個所目の障害で障害検出を行っているため，2 個所目以降の障害を検出しません。また，多重障害での復旧検出についても，最後の障害が復旧するまでマスタノードが送信しているヘルスチェックフレームを受信できないため，復旧を検出できません。その結果，多重障害のうち，一部の障害が復旧した（リングとして障害が残っている状態）ときには一時的に通信できないことがあります。

なお，多重障害監視機能を適用すると，障害の組み合わせによっては多重障害を検出できる場合があります。多重障害監視機能については，「28.6 Ring Protocol の多重障害監視機能」を参照してください。

(12) VLAN のダウンを伴う障害発生時の経路の切り替えについて

マスタノードのプライマリポートでリンクダウンなどの障害が発生すると，データ転送用の VLAN グループに設定されている VLAN が一時的にダウンする場合があります。このような場合，経路の切り替えによる通信の復旧に時間がかかることがあります。

なお，VLAN debounce 機能を使用することで VLAN のダウンを回避できる場合があります。VLAN debounce 機能の詳細については，「25.9 VLAN debounce 機能の解説」を参照してください。

(13) フラッシュ制御フレームの送信回数について

リングネットワークに適用している VLAN 数や VLAN マッピング数などの構成に応じて，マスタノードが送信するフラッシュ制御フレームの送信回数を調整してください。

一つのリングポートに 64 個以上の VLAN マッピングを使用している場合には，送信回数を 4 回以上に設定してください。3 回以下の場合，MAC アドレステーブルエントリが適切にクリアできず，経路の切り替えに時間がかかることがあります。

(14) VLAN のダウンを伴うコンフィグレーションコマンドの設定について

Ring Protocol に関するコンフィグレーションコマンドが設定されていない状態で，一つ目の Ring Protocol に関するコンフィグレーションコマンド（次に示すどれかのコマンド）を設定した場合に，すべての VLAN が一時的にダウンします。そのため，Ring Protocol を用いたリングネットワークを構築する場合には，あらかじめ次に示すコンフィグレーションコマンドを設定しておくことを推奨します。

- axrp
- axrp vlan-mapping
- axrp-ring-port
- axrp-primary-port
- axrp virtual-link

なお，VLAN マッピング（axrp vlan-mapping コマンド）については，新たに追加設定した場合でも，その VLAN マッピングに関連づけられる VLAN が一時的にダウンします。すでに設定されている VLAN マッピング，およびその VLAN マッピングに関連づけられているその他の VLAN には影響ありません。

(15)　マスタノードの装置起動時のフラッシュ制御フレーム送受信について

マスタノードの装置起動時に，トランジットノードがマスタノードと接続されているリングポートのリンクアップをマスタノードよりも遅く検出すると，マスタノードが初期動作時に送信するフラッシュ制御フレームを受信できない場合があります。このとき，フラッシュ制御フレームを受信できなかったトランジットノードのリングポートはブロッキング状態となります。該当するリングポートはフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）が経過するとフォワーディング状態となり，通信が復旧します。

隣接するトランジットノードでフラッシュ制御フレームが受信できない場合には，マスタノードのフラッシュ制御フレームの送信回数を調節すると，受信できることがあります。また，フラッシュ制御フレーム未受信による通信断の時間を短縮したい場合は，トランジットノードのフラッシュ制御フレーム受信待ち保護時間（初期値：10 秒）を短くしてください。

なお，次の場合も同様です。

- VLAN プログラムの再起動（運用コマンド restart vlan の実行）
- コンフィグレーションファイルの運用への反映（運用コマンド copy の実行）

(16)　経路切り戻し抑止機能適用時のフラッシュ制御フレーム受信待ち保護時間の設定について

経路切り戻し抑止機能を動作させる場合，トランジットノードでのフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）には infinity を指定するか，または経路切り戻し抑止時間（preempt-delay）よりも大きな値を指定してください。経路切り戻し抑止中，トランジットノードでのフラッシュ制御フレーム受信待ち保護時間がタイムアウトして該当リングポートの論理ブロックを解除してしまうと，マスタノードはセカンダリポートの論理ブロック状態を解除しているため，ループが発生するおそれがあります。

(17)　多重障害監視機能の監視開始タイミングについて

共有ノードでは，多重障害監視機能を適用したあと，対向の共有ノードが送信する多重障害監視フレームを最初に受信したときに多重障害の監視を開始します。このため，多重障害監視機能を設定するときにリングネットワークに障害が発生していると，多重障害の監視を開始できません。多重障害監視機能は，リングネットワークが正常な状態で設定してください。

(18)　多重障害の一部復旧時の通信について

多重障害の一部復旧時はマスタノードがリング復旧を検出しないため，トランジットノードのリングポートはフラッシュ制御フレームの受信待ち保護時間（forwarding-shift-time）が経過するまでの間，論理ブロック状態となります。論理ブロック状態を解除したい場合は，フラッシュ制御フレーム受信待ち保護時間（初期値：10 秒）を短くするか，残りのリンク障害を復旧してマスタノードにリング復旧を検出させてください。なお，フラッシュ制御フレームの受信待ち保護時間を設定するときは，多重障害監視フレームの送信間隔（コンフィグレーションコマンド multi-fault-detection interval）よりも大きい値を設定してください。小さい値を設定すると，一時的にループが発生するおそれがあります。

(19)　多重障害監視機能と経路切り戻し抑止機能の併用について

共有リンク非監視リングに経路切り戻し抑止機能を設定すると，多重障害が復旧したときに，セカンダリポートは復旧抑止状態を解除するまでの間フォワーディング状態を維持するため，ループ構成となるおそれ

があります。多重障害監視機能と経路切り戻し抑止機能を併用する場合は，次のどれかで運用してください。

- 共有リンク監視リングだけに経路切り戻し抑止機能を設定する
- 共有リンク監視リングの切り戻し抑止時間を，共有リンク非監視リングの切り戻し抑止時間よりも十分に長くなるように設定する
- 共有リンク監視リングおよび共有リンク非監視リングの切り戻し抑止時間に infinity を設定する場合は，共有リンク非監視リングの復旧抑止状態を解除してから共有リンク監視リングの復旧抑止状態を解除する

(20) リングポートに指定したリンクアグリゲーションのダウンについて

リングネットワークを構成するノード間をリンクアグリゲーション（スタティックモードまたは LACP モード）で接続していた場合，リンクアグリゲーションの該当チャネルグループを shutdown コマンドでダウン状態にするときは，あらかじめチャネルグループに属するすべての物理ポートを shutdown コマンドでダウン状態に設定してください。

なお，該当チャネルグループを no shutdown コマンドでアップ状態にするときは，あらかじめチャネルグループに属するすべての物理ポートを shutdown コマンドでダウン状態に設定してください。

(21) スタック構成のノードの適用について

スタック構成時，複数のメンバスイッチと接続するリンクアグリゲーションは，リングポートとして使用できません。

スタック構成のノードは，Ring Protocol とスパニングツリーの併用，Ring Protocol と GSRP の併用をサポートしていません。スパニングツリーや GSRP を併用しているリングネットワークにスタック構成のノードを追加すると，仮想リンクを構築できないため意図したトポロジーが構築されません。その結果，ループが発生するおそれがあります。スタック構成のノードを使用する場合は，リングを構成するすべてのノードで，スパニングツリーおよび GSRP を停止してください。

スタンドアロンで動作しているノードに本装置を追加して，スタック構成のノードを構築する場合は，次の点に注意してください。

- 共有ノードとして動作しているノードは，スタック構成にできません。
- スタック機能を有効にする前に，既存のリングポートの設定を一つ削除してください。二つ目のリングポートは，スタック機能を有効にしたあと，追加したメンバスイッチのインタフェースに設定してください。
- 仮想リンクの設定を削除してから，スタック機能を有効にしてください。

(22) restart コマンドの実行について

トランジットノードで次に示す運用コマンドを実行すると，リングポートの VLAN がダウン状態になるため，マスタノードがリング障害を誤検出してセカンダリポートをフォワーディングにします。トランジットノードのリングポートは一時的なダウン状態であるため，マスタノードがリング障害の復旧を検出するまでループが発生します。

- restart spanning-tree
- restart uplink-redundant
- restart gsrp

トランジットノードでこれらのコマンドを実行する場合, ループを防止するため次に示す手順を実施してください。

1. リングポートを shutdown コマンドなどでダウン状態にします。
2. 上記の restart コマンドを実行します。
3. 手順 1 でダウン状態としたリングポートをアップ状態（shutdown コマンドなどの解除）にします。

29 Ring Protocol の設定と運用

この章では，Ring Protocol の設定例について説明します。

29.1　コンフィグレーション

Ring Protocol 機能が動作するためには，axrp，axrp vlan-mapping，mode，control-vlan，vlan-group，axrp-ring-port の設定が必要です。すべてのノードについて，構成に即したコンフィグレーションを設定してください。

29.1.1　コンフィグレーションコマンド一覧

Ring Protocol のコンフィグレーションコマンド一覧を次の表に示します。

表 29–1　コンフィグレーションコマンド一覧

コマンド名	説明
axrp	リング ID を設定します。
axrp vlan-mapping	VLAN マッピング，およびそのマッピングに参加する VLAN を設定します。
axrp-primary-port	プライマリポートを設定します。
axrp-ring-port	リングポートを設定します。
control-vlan	制御 VLAN として使用する VLAN を設定します。
disable	Ring Protocol 機能を無効にします。
flush-request-count	フラッシュ制御フレームを送信する回数を設定します。
flush-request-transmit vlan	隣接するリング構成の装置に対して，隣接リング用フラッシュ制御フレームを送信する VLAN を設定します。
forwarding-shift-time	フラッシュ制御フレームの受信待ちを行う保護時間を設定します。
health-check holdtime	ヘルスチェックフレームの保護時間を設定します。
health-check interval	ヘルスチェックフレームの送信間隔を設定します。
mac-clear-mode	Ring Protocol 機能でクリアする MAC アドレステーブルのエントリ対象を設定します。
mode	リングでの動作モードを設定します。
multi-fault-detection holdtime	多重障害監視フレームの受信待ち保護時間を設定します。
multi-fault-detection interval	多重障害監視フレームの送信間隔を設定します。
multi-fault-detection mode	多重障害監視の監視モードを設定します。
multi-fault-detection vlan	多重障害監視 VLAN として使用する VLAN を設定します。
name	リングを識別するための名称を設定します。
preempt-delay	経路切り戻し抑止機能を有効にして抑止時間を設定します。
vlan-group	Ring Protocol 機能で運用する VLAN グループ，および VLAN マッピング ID を設定します。

29.1.2　Ring Protocol 設定の流れ

Ring Protocol 機能を正常に動作させるには，構成に合った設定が必要です。設定の流れを次に示します。

(1)　スパニングツリーの停止

Ring Protocol を使用する場合には，事前にスパニングツリーを停止することを推奨します。ただし，本装置で Ring Protocol とスパニングツリーを併用するときは，停止する必要はありません。スパニングツリーの停止については，「27　スパニングツリー」を参照してください。

(2)　Ring Protocol 共通の設定

リングの構成，またはリングでの本装置の位置づけに依存しない共通の設定を行います。

- リング ID
- 制御 VLAN
- VLAN マッピング
- VLAN グループ

(3)　モードとポートの設定

リングの構成，またはリングでの本装置の位置づけに応じた設定を行います。設定の組み合わせに矛盾がある場合，Ring Protocol 機能は正常に動作しません。

- モード
- リングポート

(4)　各種パラメータ設定

Ring Protocol 機能は，次に示すコンフィグレーションの設定がない場合，初期値で動作します。値を変更したい場合はコマンドで設定してください。

- 機能の無効化
- ヘルスチェックフレーム送信間隔
- ヘルスチェックフレーム受信待ち保護時間
- フラッシュ制御フレーム受信待ち保護時間
- フラッシュ制御フレーム送信回数
- プライマリポート
- 経路切り戻し抑止機能の有効化および抑止時間
- Ring Protocol でクリアする MAC アドレステーブルのエントリ対象

29.1.3　リング ID の設定

[設定のポイント]

リング ID を設定します。同じリングに属する装置にはすべて同じリング ID を設定する必要があります。

[コマンドによる設定]

1. **(config)# axrp 1**
   リング ID 1 を設定します。

29.1.4　制御 VLAN の設定

(1)　制御 VLAN の設定

[設定のポイント]

制御 VLAN として使用する VLAN を指定します。データ転送用 VLAN に使われている VLAN は使用できません。また，異なるリングで使われている VLAN ID と同じ値の VLAN ID は使用できません。

[コマンドによる設定]

1. **(config)# axrp 1**
   リング ID 1 の axrp コンフィグレーションモードに移行します。
2. **(config-axrp)# control-vlan 2**
   制御 VLAN として VLAN2 を指定します。

(2)　制御 VLAN のフォワーディング遷移時間の設定

[設定のポイント]

Ring Protocol が初期状態の場合に，トランジットノードでの制御 VLAN のフォワーディング遷移時間を設定します。それ以外のノードでは，本設定を実施しても無効となります。トランジットノードでの制御 VLAN のフォワーディング遷移時間（forwarding-delay-time パラメータでの設定値）は，マスタノードでのヘルスチェックフレームの保護時間（health-check holdtime コマンドでの設定値）よりも大きな値を設定してください。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# control-vlan 2 forwarding-delay-time 10
   制御 VLAN のフォワーディング遷移時間を 10 秒に設定します。

29.1.5　VLAN マッピングの設定

(1)　VLAN 新規設定

[設定のポイント]

データ転送用に使用する VLAN を VLAN マッピングに括り付けます。一つの VLAN マッピングを共通定義として複数のリングで使用できます。設定できる VLAN マッピングの最大数は 128 個です。VLAN マッピングに設定する VLAN はリストで複数指定できます。

リングネットワーク内で使用するデータ転送用 VLAN は，すべてのノードで同じにする必要があります。ただし，VLAN グループに指定した VLAN マッピングの VLAN が一致していればよいため，リングネットワーク内のすべてのノードで VLAN マッピング ID を一致させる必要はありません。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan 5-7**
   VLAN マッピング ID 1 に，VLAN ID 5，6，7 を設定します。

(2)　VLAN 追加

[設定のポイント]

設定済みの VLAN マッピングに対して，VLAN ID を追加します。追加した VLAN マッピングを適用したリングが動作中の場合には，すぐに反映されます。また，複数のリングで適用されている場合には，同時に反映されます。リング運用中に VLAN マッピングを変更すると，ループが発生することがあります。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan add 8-10**
   VLAN マッピング ID 1 に VLAN ID 8，9，10 を追加します。

(3)　VLAN 削除

[設定のポイント]

設定済みの VLAN マッピングから，VLAN ID を削除します。削除した VLAN マッピングを適用したリングが動作中の場合には，すぐに反映されます。また，複数のリングで適用されている場合には，同時に反映されます。リング運用中に VLAN マッピングを変更すると，ループが発生することがあります。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan remove 8-9**
   VLAN マッピング ID 1 から VLAN ID 8，9 を削除します。

29.1.6　VLAN グループの設定

[設定のポイント]

VLAN グループに VLAN マッピングを割り当てることによって，VLAN ID を Ring Protocol で使用する VLAN グループに所属させます。VLAN グループは一つのリングに最大二つ設定できます。
VLAN グループには，リスト指定によって最大 128 個の VLAN マッピング ID を設定できます。

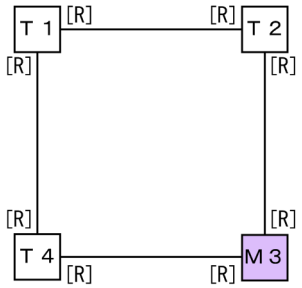
[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# vlan-group 1 vlan-mapping 1
   VLAN グループ 1 に，VLAN マッピング ID 1 を設定します。

29.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）

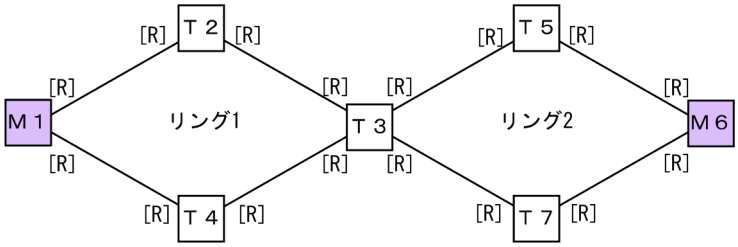
シングルリング構成を「図 29–1　シングルリング構成」に，共有リンクなしマルチリング構成を「図 29–2　共有リンクなしマルチリング構成」に示します。

図 29-1　シングルリング構成



（凡例）　M：マスタノード　　T：トランジットノード
　　[R]：リングポート

図 29-2　共有リンクなしマルチリング構成



（凡例）　M：マスタノード　　T：トランジットノード
　　[R]：リングポート

シングルリング構成と共有リンクなしマルチリング構成での，マスタノード，およびトランジットノードに関するモードとリングポートの設定は同様になります。

(1)　マスタノード

[設定のポイント]

リングでの本装置の動作モードをマスタモードに設定します。イーサネットインタフェースまたはポートチャネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 29-1　シングルリング構成」では M3 ノード，「図 29-2　共有リンクなしマルチリング構成」では M1 および M6 ノードがこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 2**
   (config-axrp)# mode master
   リング ID 2 の動作モードをマスタモードに設定します。
2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# axrp-ring-port 2
   (config-if)# exit
   (config)# interface gigabitethernet 1/0/2
   (config-if)# axrp-ring-port 2
   ポート 1/0/1 および 1/0/2 のインタフェースモードに移行し，該当するインタフェースをリング ID 2 のリングポートとして設定します。

[注意事項]

スタックを構成するメンバスイッチ 1 台に対して，同じリング ID のリングポートを設定できるのは一つのインタフェースだけです。二つ目のリングポートは，別のメンバスイッチのインタフェースに設定してください。

(2)　トランジットノード

[設定のポイント]

リングでの本装置の動作モードをトランジットモードに設定します。イーサネットインタフェースまたはポートチャネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 29-1　シングルリング構成」では T1，T2 および T4 ノード，「図 29-2　共有リンクなしマルチリング構成」では T2，T3，T4，T5 および T7 ノードがこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 2**

   (config-axrp)# mode transit

   リング ID 2 の動作モードをトランジットモードに設定します。

2. **(config)# interface gigabitethernet 1/0/1**

   (config-if)# axrp-ring-port 2

   (config-if)# exit

   (config)# interface gigabitethernet 1/0/2

   (config-if)# axrp-ring-port 2

   ポート 1/0/1 および 1/0/2 のインタフェースモードに移行し，該当するインタフェースをリング ID 2 のリングポートとして設定します。

[注意事項]

スタックを構成するメンバスイッチ 1 台に対して，同じリング ID のリングポートを設定できるのは一つのインタフェースだけです。二つ目のリングポートは，別のメンバスイッチのインタフェースに設定してください。

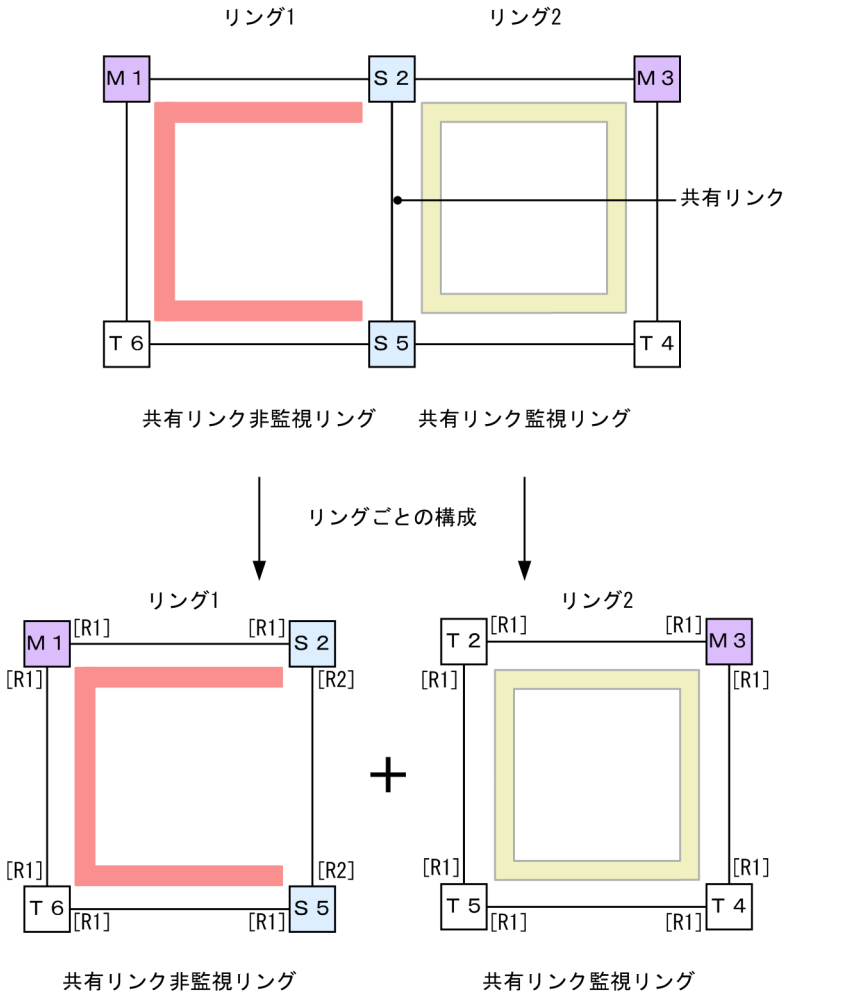
29.1.8　モードとリングポートに関する設定（共有リンクありマルチリング構成）

共有リンクありマルチリング構成について，モードとリングポートのパラメータ設定パターンを示します。

(1)　共有リンクありマルチリング構成（基本構成）

共有リンクありマルチリング構成（基本構成）を次の図に示します。

図 29-3　共有リンクありマルチリング構成（基本構成）



（凡例）　M：マスタノード　　T：トランジットノード　　S：共有ノード
[R1]：リングポート
[R2]：リングポート（共有リンク非監視リング最終端ノードの共有リンク側ポート）
：リング1の監視経路　　：リング2の監視経路

(a)　共有リンク監視リングのマスタノード

シングルリングのマスタノード設定と同様です。「29.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）(1)　マスタノード」を参照してください。「図 29-3　共有リンクありマルチリング構成（基本構成）」では M3 ノードがこれに該当します。

(b)　共有リンク監視リングのトランジットノード

シングルリングのトランジットノード設定と同様です。「29.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）(2)　トランジットノード」を参照してください。「図 29-3　共有リンクありマルチリング構成（基本構成）」では T2，T4 および T5 ノードがこれに該当します。

(c)　共有リンク非監視リングのマスタノード

[設定のポイント]

リングでの本装置の動作モードをマスタモードに設定します。また，本装置が構成しているリングの属性，およびそのリングでの本装置の位置づけを共有リンク非監視リングに設定します。イーサネットインタフェースまたはポートチャネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 29-3　共有リンクありマルチリング構成（基本構成）」では M1 ノードがこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 1**

   (config-axrp)# mode master ring-attribute rift-ring

   リング ID 1 の動作モードをマスタモード，リング属性を共有リンク非監視リングに設定します。

2. **(config)# interface gigabitethernet 1/0/1**

   (config-if)# axrp-ring-port 1

   (config-if)# exit

   (config)# interface gigabitethernet 1/0/2

   (config-if)# axrp-ring-port 1

   ポート 1/0/1 および 1/0/2 のインタフェースモードに移行し，該当するインタフェースをリング ID 1 のリングポートとして設定します。

[注意事項]

スタックを構成するメンバスイッチ 1 台に対して，同じリング ID のリングポートを設定できるのは一つのインタフェースだけです。二つ目のリングポートは，別のメンバスイッチのインタフェースに設定してください。

(d)　共有リンク非監視リングのトランジットノード

シングルリングのトランジットノード設定と同様です。「29.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）(2)　トランジットノード」を参照してください。「図 29-3　共有リンクありマルチリング構成（基本構成）」では T6 ノードがこれに該当します。

(e)　共有リンク非監視リングの最終端ノード（トランジット）

[設定のポイント]

リングでの本装置の動作モードをトランジットモードに設定します。また，本装置が構成しているリングの属性，およびそのリングでの本装置の位置づけを共有リンク非監視リングの最終端ノードに設定します。構成上二つ存在する共有リンク非監視リングの最終端ノードの区別にはエッジノード ID（1 または 2）を指定します。「図 29-3　共有リンクありマルチリング構成（基本構成）」では S2 および S5 ノードがこれに該当します。リングポート設定は共有リンク側のポートにだけ shared-edge を指定します。「図 29-3　共有リンクありマルチリング構成（基本構成）」では S2 および S5 ノードのリングポート[R2]がこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 1**

   (config-axrp)# mode transit ring-attribute rift-ring-edge 1

   リング ID 1 での動作モードをトランジットモード，リング属性を共有リンク非監視リングの最終端ノード，エッジノード ID を 1 に設定します。

2. **(config)# interface gigabitethernet 1/0/1**
   (config-if)# axrp-ring-port 1
   (config-if)# exit
   (config)# interface gigabitethernet 1/0/2
   (config-if)# axrp-ring-port 1 shared-edge
   ポート 1/0/1 および 1/0/2 のインタフェースモードに移行し，該当するインタフェースをリング ID 1 のリングポートとして設定します。このとき，ポート 1/0/2 を共有リンクとして shared-edge パラメータも設定します。

[注意事項]

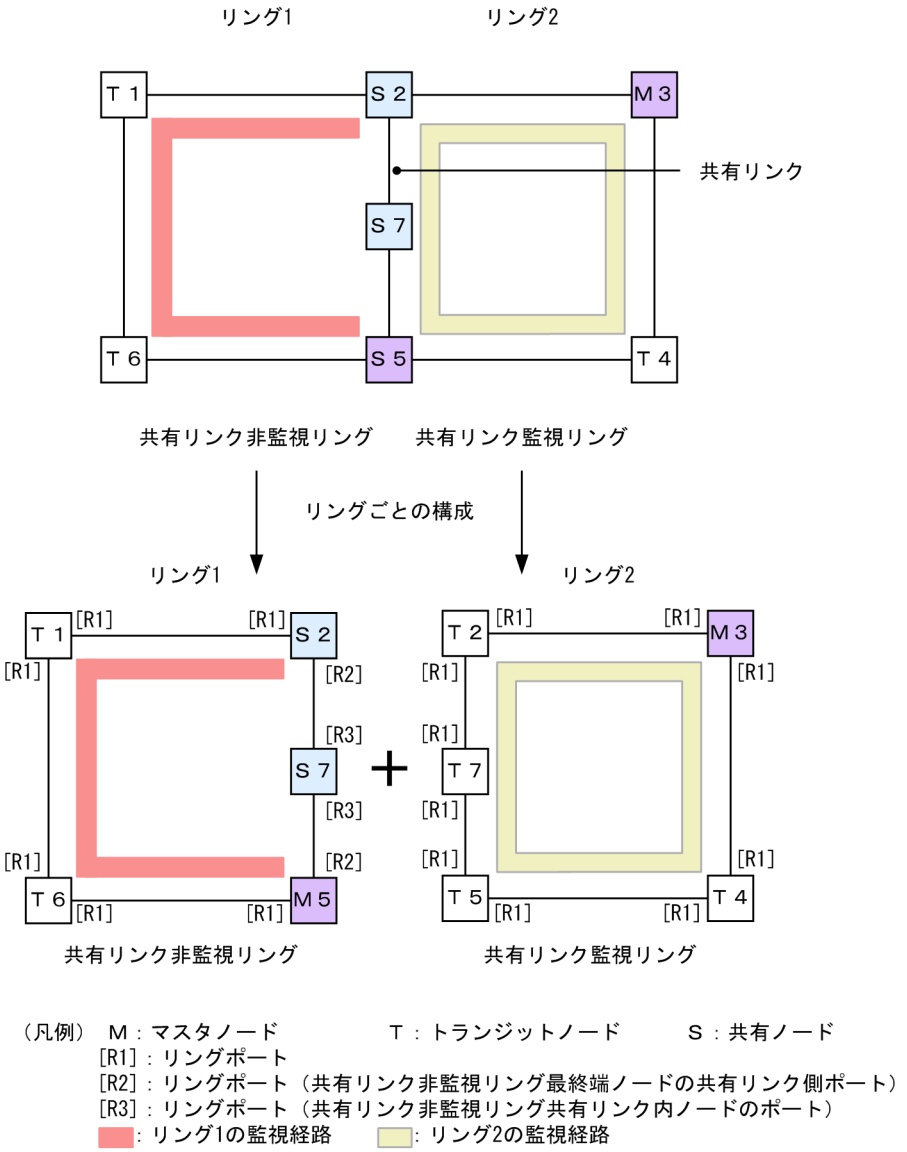
エッジノード ID は, 二つある共有リンク非監視リングの最終端ノードで他方と異なる ID を設定してください。

スタック構成時は，リング属性に共有リンク非監視リングの最終端ノード（rift-ring-edge パラメータ）を設定できません。

(2) 共有リンクありのマルチリング構成（拡張構成）

共有リンクありマルチリング構成（拡張構成）を次の図に示します。共有リンク非監視リングの最終端ノード（マスタノード）および共有リンク非監視リングの共有リンク内ノード（トランジット）以外の設定については，「(1) 共有リンクありマルチリング構成（基本構成）」を参照してください。

図 29-4　共有リンクありのマルチリング構成（拡張構成）



（凡例）　M：マスタノード　　T：トランジットノード　　S：共有ノード
[R1]：リングポート
[R2]：リングポート（共有リンク非監視リング最終端ノードの共有リンク側ポート）
[R3]：リングポート（共有リンク非監視リング共有リンク内ノードのポート）
：リング1の監視経路　　：リング2の監視経路

(a)　共有リンク非監視リングの最終端ノード（マスタノード）

[設定のポイント]

リングでの本装置の動作モードをマスタモードに設定します。また，本装置が構成しているリングの属性，およびそのリングでの本装置の位置づけを共有リンク非監視リングの最終端ノードに設定します。構成上二つ存在する共有リンク非監視リングの最終端ノードの区別にはエッジノード ID（1 または 2）を指定します。「図 29-4　共有リンクありのマルチリング構成（拡張構成）」では M5 ノードがこれに該当します。リングポート設定は共有リンク側のポートにだけ shared-edge を指定します。「図 29-4　共有リンクありのマルチリング構成（拡張構成）」では M5 ノードのリングポート[R2]がこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# mode master ring-attribute rift-ring-edge 2

リング ID 1 での動作モードをマスタモード，リング属性を共有リンク非監視リングの最終端ノード，エッジノード ID を 2 に設定します。

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# axrp-ring-port 1
(config-if)# exit
(config)# interface gigabitethernet 1/0/2
(config-if)# axrp-ring-port 1 shared-edge
```
ポート 1/0/1 および 1/0/2 のインタフェースモードに移行し，該当するインタフェースをリング ID 1 のリングポートとして設定します。このとき，ポート 1/0/2 を共有リンクとして shared-edge パラメータも設定します。

[注意事項]

エッジノード ID は，二つある共有リンク非監視リングの最終端ノードで他方と異なる ID を設定してください。

スタック構成時は，リング属性に共有リンク非監視リングの最終端ノード（rift-ring-edge パラメータ）を設定できません。

(b)　共有リンク非監視リングの共有リンク内ノード（トランジット）

[設定のポイント]

リングでの本装置の動作モードをトランジットモードに設定します。「図 29–4　共有リンクありのマルチリング構成（拡張構成）」では S7 ノードがこれに該当します。リングポートは両ポート共に shared パラメータを指定し，共有ポートとして設定します。「図 29–4　共有リンクありのマルチリング構成（拡張構成）」では S7 ノードのリングポート[R3]がこれに該当します。

[コマンドによる設定]

1.
```
(config)# axrp 1
(config-axrp)# mode transit
```
リング ID 1 の動作モードをトランジットモードに設定します。

2.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# axrp-ring-port 1 shared
(config-if)# exit
(config)# interface gigabitethernet 1/0/2
(config-if)# axrp-ring-port 1 shared
```
ポート 1/0/1 および 1/0/2 のインタフェースモードに移行し，該当するインタフェースをリング ID 1 の共有リンクポートに設定します。

[注意事項]

1. 共有リンク監視リングの共有リンク内トランジットノードに shared 指定でポート設定をした場合，Ring Protocol 機能は正常に動作しません。
2. 共有リンク非監視リングの共有リンク内で shared 指定したノードにマスタモードは指定できません。

29.1.9　各種パラメータの設定

(1)　Ring Protocol 機能の無効

[設定のポイント]

コマンドを指定して Ring Protocol 機能を無効にします。ただし，運用中に Ring Protocol 機能を無効にすると，ネットワークの構成上，ループが発生するおそれがあります。このため，先に Ring Protocol 機能を動作させているインタフェースを shutdown コマンドなどで停止させてから，Ring Protocol 機能を無効にしてください。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# disable
   該当するリング ID 1 の axrp コンフィグレーションモードに移行します。disable コマンドを実行することで，Ring Protocol 機能が無効となります。

(2)　ヘルスチェックフレーム送信間隔

[設定のポイント]

マスタノード，または共有リンク非監視リングの最終端ノードでのヘルスチェックフレームの送信間隔を設定します。それ以外のノードでは，本設定を実施しても，無効となります。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# health-check interval 500
   ヘルスチェックフレームの送信間隔を 500 ミリ秒に設定します。

[注意事項]

マルチリングの構成をとる場合，同一リング内のマスタノードと共有リンク非監視リングの最終端ノードでのヘルスチェックフレーム送信間隔は同じ値を設定してください。値が異なる場合，障害検出処理が正常に行われません。

(3)　ヘルスチェックフレーム受信待ち保護時間

[設定のポイント]

マスタノードでのヘルスチェックフレームの受信待ち保護時間を設定します。それ以外のノードでは，本設定を実施しても，無効となります。受信待ち保護時間を変更することで，障害検出時間を調節できます。

受信待ち保護時間（health-check holdtime コマンドでの設定値）は，送信間隔（health-check interval コマンドでの設定値）よりも大きい値を設定してください。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# health-check holdtime 1500
   ヘルスチェックフレームの受信待ち保護時間を 1500 ミリ秒に設定します。

(4) フラッシュ制御フレーム受信待ち保護時間

[設定のポイント]

トランジットノードでのフラッシュ制御フレームの受信待ち保護時間を設定します。それ以外のノードでは，本設定を実施しても，無効となります。トランジットノードでのフラッシュ制御フレームの受信待ちの保護時間（forwarding-shift-time コマンドでの設定値）は，マスタノードでのヘルスチェックフレームの送信間隔（health-check interval コマンドでの設定値）よりも大きい値を設定してください。設定誤りからマスタノードが復旧を検出するよりも先にトランジットノードのリングポートがフォワーディング状態になってしまった場合，一時的にループが発生するおそれがあります。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# forwarding-shift-time 100
   フラッシュ制御フレームの受信待ちの保護時間を 100 秒に設定します。

[注意事項]

隣接のノードがスタック構成のマスタノードの場合は，フラッシュ制御フレーム受信待ち保護時間を 60 秒以上に設定してください。

(5) プライマリポートの設定

[設定のポイント]

マスタノードでプライマリポートを設定できます。マスタノードでリングポート（axrp-ring-port コマンド）指定のあるインタフェースに設定してください。本装置が共有リンク非監視リングの最終端となっている場合は設定されても動作しません。通常，プライマリポートは自動で割り振られますので，axrp-primary-port コマンドの設定または変更によってプライマリポートを切り替える場合は，リング動作がいったん停止します。

[コマンドによる設定]

1. **(config)# interface port-channel 10**
   (config-if)# axrp-primary-port 1 vlan-group 1
   ポートチャネルインタフェースコンフィグレーションモードに移行し，該当するインタフェースをリング ID 1，VLAN グループ ID 1 のプライマリポートに設定します。

(6) 経路切り戻し抑止機能の有効化および抑止時間の設定

[設定のポイント]

マスタノードで障害復旧検出後，経路切り戻し動作を抑止する時間を設定します。なお，抑止時間として infinity を指定した場合，運用コマンド clear axrp preempt-delay が入力されるまで経路切り戻し動作を抑止します。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# preempt-delay infinity
   リング ID 1 のコンフィグレーションモードに移行し，経路切り戻し抑止時間を infinity に設定します。

29.1.10　多重障害監視機能の設定

(1)　多重障害監視 VLAN の設定

[設定のポイント]

共有リンク監視リングの各ノードに多重障害監視 VLAN として使用する VLAN を設定します。なお，制御 VLAN とデータ転送用 VLAN に使われている VLAN は使用できません。また，異なるリングで使用されている多重障害監視 VLAN の VLAN ID と同じ値の VLAN ID は使用できません。

[コマンドによる設定]

1. **(config)# axrp 1**
   リング ID 1 の axrp コンフィグレーションモードに移行します。
2. **(config-axrp)# multi-fault-detection vlan 20**
   多重障害監視 VLAN として VLAN 20 を設定します。

[注意事項]

多重障害監視 VLAN は多重障害監視機能を適用する共有リンク監視リングのすべてのノードに設定してください。

(2)　多重障害監視機能の監視モードの設定

[設定のポイント]

共有リンク監視リングの各ノードに多重障害監視の監視モードと，多重障害検出時にバックアップリングに使用する共有リンク非監視リングのリング ID を設定します。監視モードは，多重障害監視を行う共有ノードに monitor-enable，その他の装置に transport-only を設定します。バックアップリングのリング ID は共有ノードに設定します。

(a)　共有リンク監視リングの共有ノード

[コマンドによる設定]

1. **(config)# axrp 1**
   リング ID 1 の axrp コンフィグレーションモードに移行します。
2. **(config-axrp)# multi-fault-detection mode monitor-enable backup-ring 2**
   多重障害監視の監視モードを monitor-enable，バックアップリングのリング ID を 2 に設定します。

[注意事項]

多重障害監視の監視モード monitor-enable は，共有リンクの両端に位置する 2 台の共有ノードに設定してください。1 台だけ設定した場合，多重障害監視は行われません。

スタック構成時は，監視モードに monitor-enable を設定できません。

(b)　共有リンク監視リングのその他のノード

[コマンドによる設定]

1. **(config)# axrp 1**
   リング ID 1 の axrp コンフィグレーションモードに移行します。
2. **(config-axrp)# multi-fault-detection mode transport-only**
   多重障害監視の監視モードを transport-only に設定します。

(3)　多重障害監視フレームの送信間隔

[設定のポイント]

共有リンク監視リングの共有ノードでの多重障害監視フレームの送信間隔を設定します。それ以外のノードでは，本設定を実施しても無効となります。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# multi-fault-detection interval 1000
   多重障害監視フレームの送信間隔を 1000 ミリ秒に設定します。

(4)　多重障害監視フレームの受信待ち保護時間

[設定のポイント]

共有リンク監視リングの共有ノードでの多重障害監視フレームの受信待ち保護時間を設定します。それ以外のノードでは，本設定を実施しても無効となります。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# multi-fault-detection holdtime 3000
   多重障害監視フレームの受信待ち保護時間を 3000 ミリ秒に設定します。

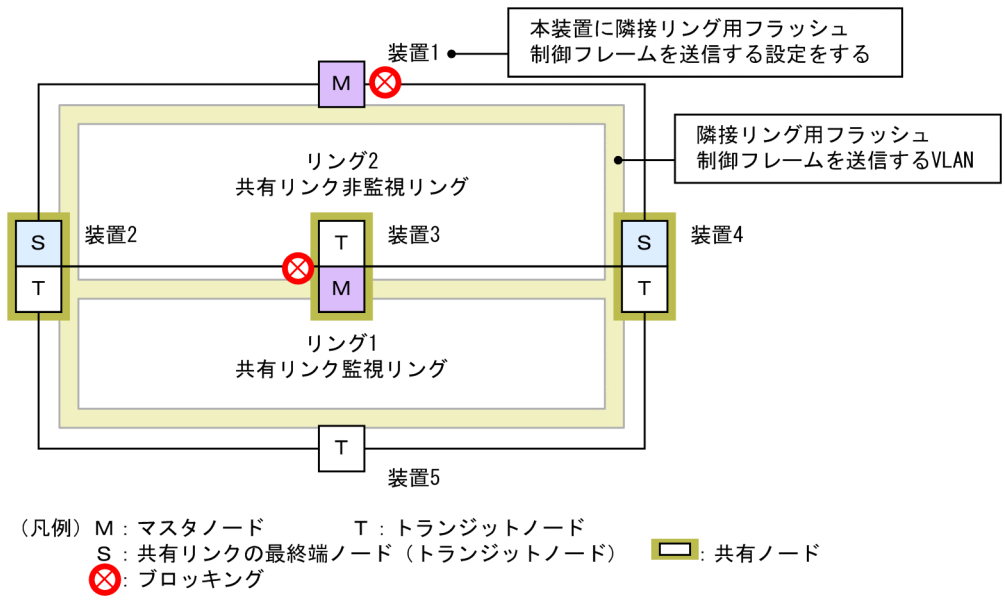
[注意事項]

受信待ち保護時間（multi-fault-detection holdtime コマンドでの設定値）には，対向の共有ノードの送信間隔（multi-fault-detection interval コマンドでの設定値）よりも大きい値を設定してください。

29.1.11　隣接リング用フラッシュ制御フレームの送信設定

マスタノードの両リングポートが共有リンクとなる構成を次の図に示します。このような構成では，共有リンク非監視リングのマスタノードで隣接リング用フラッシュ制御フレームを送信する設定をしてください。

図 29-5　マスタノードの両リングポートが共有リンクとなる構成



[設定のポイント]

「図 29-5　マスタノードの両リングポートが共有リンクとなる構成」のように両リングポートが共有リンクとなるマスタノード（リング 1 の装置 3）が存在する共有リンクありのマルチリング構成では，共有リンク非監視リングのマスタノード（リング 2 の装置 1）で隣接リング用フラッシュ制御フレームを送信する設定をしてください。

このとき，隣接リング用フラッシュ制御フレームの送信に使用する VLAN として，この図にあるように送信対象となるリングの各ノードで VLAN マッピングに括り付けられた VLAN を設定してください。

また，この VLAN は隣接リング用フラッシュ制御フレームの送信専用として，データ転送に使用しないでください。

[コマンドによる設定]

1. **(config)# axrp 2**

   (config-axrp)# flush-request-transmit vlan 10

   リング ID 2（共有リンク非監視リングのマスタノード）のコンフィグレーションモードに移行して，リング ID 2 の障害発生／復旧時に VLAN ID 10 に対して隣接リング用フラッシュ制御フレームを送信する設定をします。

29.2　オペレーション

29.2.1　運用コマンド一覧

Ring Protocol の運用コマンド一覧を次の表に示します。

表 29-2　運用コマンド一覧

コマンド名	説明
show axrp	Ring Protocol 情報を表示します。
clear axrp	Ring Protocol の統計情報をクリアします。
clear axrp preempt-delay	リングの経路切り戻し抑止状態を解除します。
restart axrp	Ring Protocol プログラムを再起動します。
dump protocols axrp	Ring Protocol プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。
show port※1	ポートの Ring Protocol 使用状態を表示します。
show vlan※2	VLAN の Ring Protocol 使用状態を表示します。

注※1
「運用コマンドレファレンス Vol.1」「21　イーサネット」を参照してください。

注※2
「運用コマンドレファレンス Vol.1」「24　VLAN」を参照してください。

29.2.2　Ring Protocol の状態確認

(1)　コンフィグレーション設定と運用の状態確認

show axrp コマンドで Ring Protocol の設定と運用状態を確認できます。コンフィグレーションコマンドで設定した Ring Protocol の設定内容が正しく反映されているかどうかを確認してください。リング単位の状態情報確認には show axrp <ring id list>コマンドを使用できます。

表示される情報は，項目"Oper State"の内容により異なります。"Oper State"に"enable"が表示されている場合は Ring Protocol 機能が動作しています。このとき，表示内容は全項目について運用の状態を示しています。"Oper State"に"-"が表示されている場合は必須であるコンフィグレーションコマンドが揃っていない状態です。また，"Oper State"に"Not Operating"が表示されている場合，コンフィグレーションに矛盾があるなどの理由で，Ring Protocol 機能が動作できていない状態です。"Oper State"の表示状態が"-"，または"Not Operating"時には，コンフィグレーションを確認してください。

show axrp コマンド，show axrp detail コマンドの表示例を次に示します。

図 29-6　show axrp コマンドの実行結果

```
> show axrp
Date 20XX/01/27 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
 Name:RING#1
 Oper State:enable           Mode:Master     Attribute:-
 MAC Clear Mode:system
```

```
 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              1/0/1      primary/forwarding    1/0/2      secondary/blocking
 2              1/0/1      secondary/blocking    1/0/2      primary/forwarding

Ring ID:2
 Name:RING#2
 Oper State:enable           Mode:Transit    Attribute:-
 MAC Clear Mode:system

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              1(ChGr)    -/forwarding          2(ChGr)    -/forwarding
 2              1(ChGr)    -/forwarding          2(ChGr)    -/forwarding

Ring ID:3
 Name:
 Oper State:disable          Mode:-          Attribute:-
 MAC Clear Mode:-

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              -          -/-                   -          -/-
 2              -          -/-                   -          -/-

Ring ID:4
 Name:RING#4
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(1)
 MAC Clear Mode:-
 Shared Edge Port:1/0/3

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              1/0/3      -/-                   1/0/4      -/forwarding
 2              1/0/3      -/-                   1/0/4      -/forwarding
>
```

show axrp detail コマンドを使用すると，統計情報やマスタノードのリング状態などについての詳細情報を確認できます。統計情報については，Ring Protocol 機能が有効（"Oper State"が"enable"）でない限り 0 を表示します。

図 29-7　show axrp detail コマンドの実行結果

```
> show axrp detail
Date 20XX/01/27 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
 Name:RING#1
 Oper State:enable           Mode:Master     Attribute:-
 MAC Clear Mode:system
 Control VLAN ID:5           Ring State:normal
 Health Check Interval  (msec):1000
 Health Check Hold Time (msec):3000
 Flush Request Counts:3

 VLAN Group ID:1
  VLAN ID:6-10,12
  Ring Port:1/0/1       Role:primary      State:forwarding
  Ring Port:1/0/2       Role:secondary    State:blocking

 VLAN Group ID:2
  VLAN ID:16-20,22
  Ring Port:1/0/1       Role:secondary    State:blocking
  Ring Port:1/0/2       Role:primary      State:forwarding

Last Transition Time:20XX/01/24 10:00:00
Fault Counts    Recovery Counts    Total Flush Request Counts
1               1                  12

Ring ID:2
 Name:RING#2
 Oper State:enable           Mode : Transit    Attribute : -
 MAC Clear Mode:system
 Control VLAN ID:15
```

```
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID  :26-30,32
  Ring Port:1(ChGr)     Role:-            State:forwarding
  Ring Port:2(ChGr)     Role:-            State:forwarding

 VLAN Group ID:2
  VLAN ID:36-40,42
  Ring Port:1(ChGr)     Role:-            State:forwarding
  Ring Port:2(ChGr)     Role:-            State:forwarding

Ring ID:3
 Name:
 Oper State:disable          Mode:-          Attribute:-
 MAC Clear Mode:-
 Control VLAN ID:-

 VLAN Group ID:1
  VLAN ID:-
  Ring Port:-           Role:-            State:-
  Ring Port:-           Role:-            State:-

 VLAN Group ID:2
  VLAN ID:-
  Ring Port:-           Role:-            State:-
  Ring Port:-           Role:-            State:-

Ring ID:4
 Name:RING#4
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(1)
 MAC Clear Mode:-
 Shared Edge Port:1/0/3
 Control VLAN ID:45
 Health Check Interval  (msec):1000
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID:46-50,52
  Ring Port:1/0/3       Role:-            State:-
  Ring Port:1/0/4       Role:-            State:forwarding

 VLAN Group ID:2
  VLAN ID:56-60,62
  Ring Port:1/0/3       Role:-            State:-
  Ring Port:1/0/4       Role:-            State:forwarding
>
```

多重障害監視機能を適用すると，show axrp detail コマンドで多重障害の監視状態についての情報を確認できます。

図 29-8　多重障害監視機能適用時の show axrp detail コマンドの実行結果

```
> show axrp detail
Date 20XX/03/10 12:00:00 UTC

Total Ring Counts:2

Ring ID:10
 Name:RING#10
 Oper State:enable           Mode:Master     Attribute:-
 MAC Clear Mode:-
 Control VLAN ID:10          Ring State:normal
 Health Check Interval  (msec):1000
 Health Check Hold Time (msec):3000
 Flush Request Counts:3

 VLAN Group ID:1
  VLAN ID:100-150
  Ring Port:1/0/1       Role:primary      State:forwarding
  Ring Port:1/0/2       Role:secondary    State:blocking
```

```
 VLAN Group ID:2
  VLAN ID:151-200
  Ring Port:1/0/1       Role:primary      State:forwarding
  Ring Port:1/0/2       Role:secondary    State:blocking

Last Transition Time:20XX/03/01 10:00:00
Fault Counts    Recovery Counts    Total Flush Request Counts
1               1                  12

Multi Fault Detection State:normal
 Mode:monitoring    Backup Ring ID:20
 Control VLAN ID:500
 Multi Fault Detection Interval  (msec):2000
 Multi Fault Detection Hold Time (msec):6000

Ring ID:20
 Name:RING#20
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(1)
 MAC Clear Mode:-
 Shared Edge Port:1/0/1
 Control VLAN ID:20
 Health Check Interval  (msec):1000
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID:100-150
  Ring Port:1/0/1       Role:-            State:-
  Ring Port:1/0/3       Role:-            State:forwarding

 VLAN Group ID:2
  VLAN ID:151-200
  Ring Port:1/0/1       Role:-            State:-
  Ring Port:1/0/3       Role:-            State:forwarding
>
```

30 Ring Protocol とスパニングツリー/GSRP の併用

この章では，同一装置での Ring Protocol とスパニングツリーの併用，および同一装置での Ring Protocol と GSRP の併用について説明します。

30.1　Ring Protocol とスパニングツリーとの併用

本装置では，Ring Protocol とスパニングツリーの併用ができます。Ring Protocol と併用可能なスパニングツリーのプロトコル種別については，「22.3　レイヤ 2 スイッチ機能と他機能の共存について」，Ring Protocol の詳細については，「28　Ring Protocol の解説」を参照してください。

30.1.1　概要

同一装置で Ring Protocol とスパニングツリーを併用して，コアネットワークを Ring Protocol，アクセスネットワークをスパニングツリーとしたネットワークを構成できます。例えば，すべてをスパニングツリーで構成していたネットワークを，コアネットワークだけ Ring Protocol に変更することで，アクセスネットワークの既存設備の多くを変更することなく流用できます。なお，Ring Protocol は，シングルリングおよびマルチリング（共有リンクありのマルチリングを含む）のどちらの構成でも，スパニングツリーと併用できます。

シングルリング構成，またはマルチリング構成での Ring Protocol とスパニングツリーとの併用例を次の図に示します。本装置 A－G－I 間，B－F－J 間，C－D－K 間でそれぞれスパニングツリートポロジーを構成しています。なお，本装置 A～D および F～G では，Ring Protocol とスパニングツリーが同時に動作しています。

図 30-1　Ring Protocol とスパニングツリーの併用例（シングルリング構成）

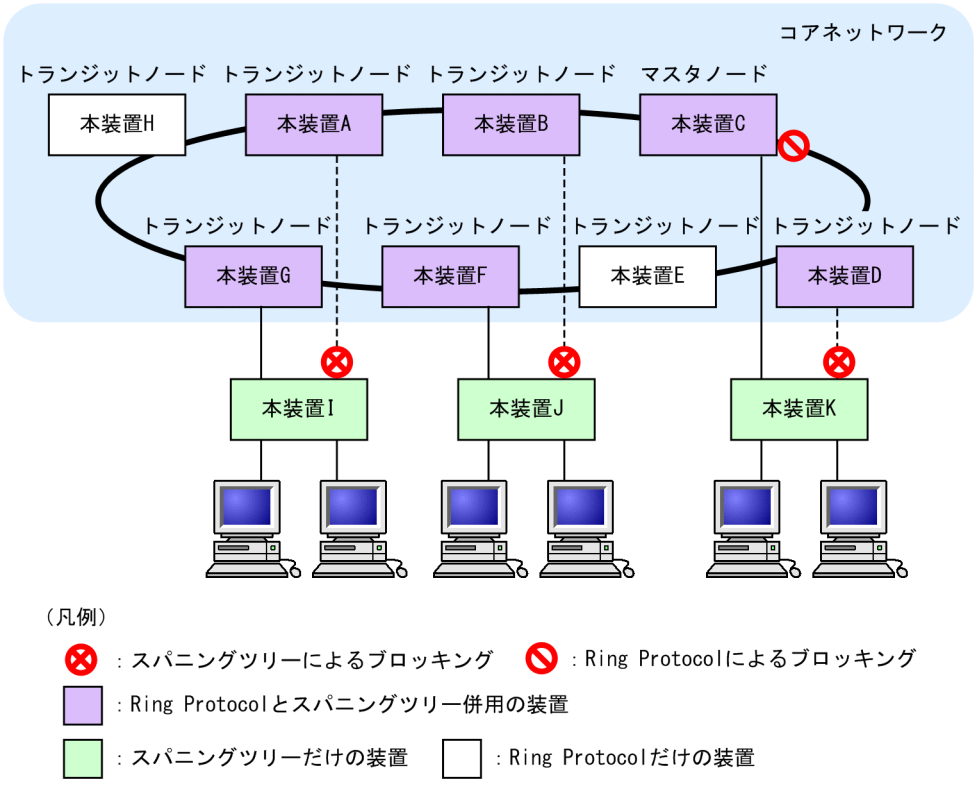
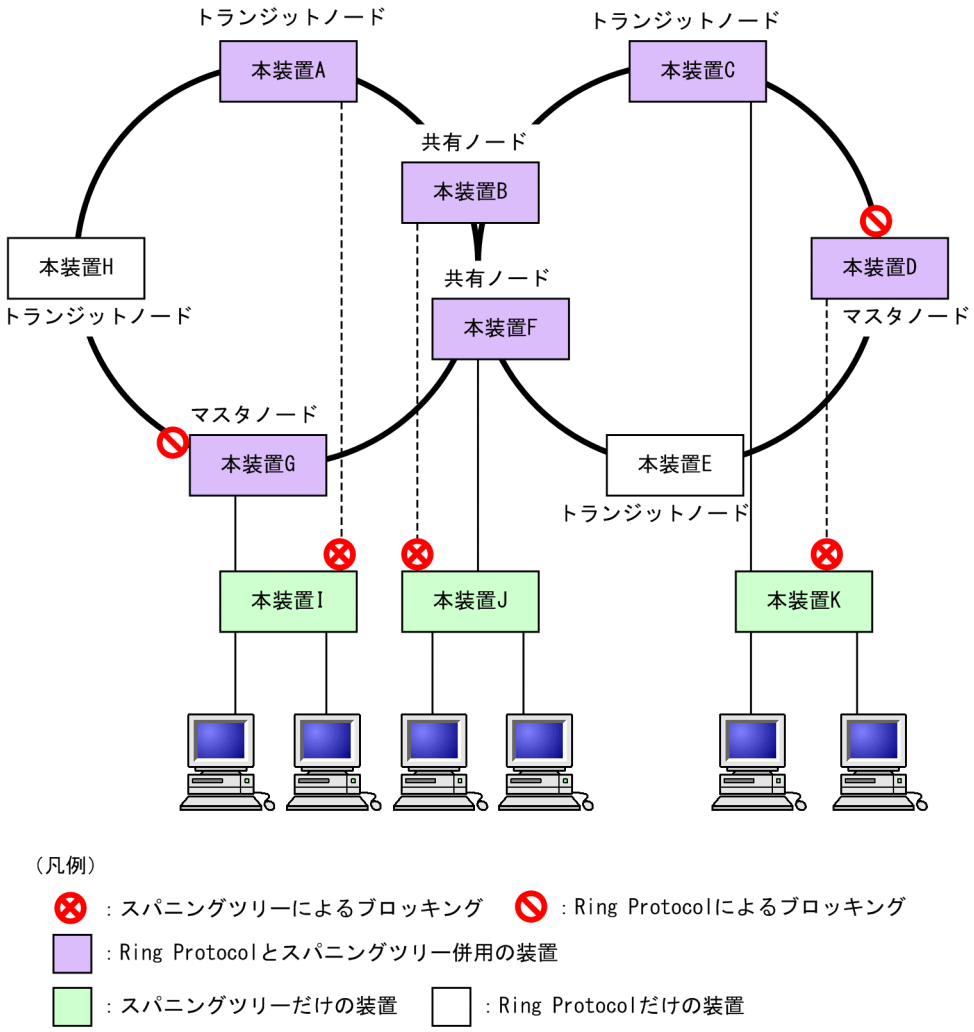


図 30-2　Ring Protocol とスパニングツリーの併用例（マルチリング構成）



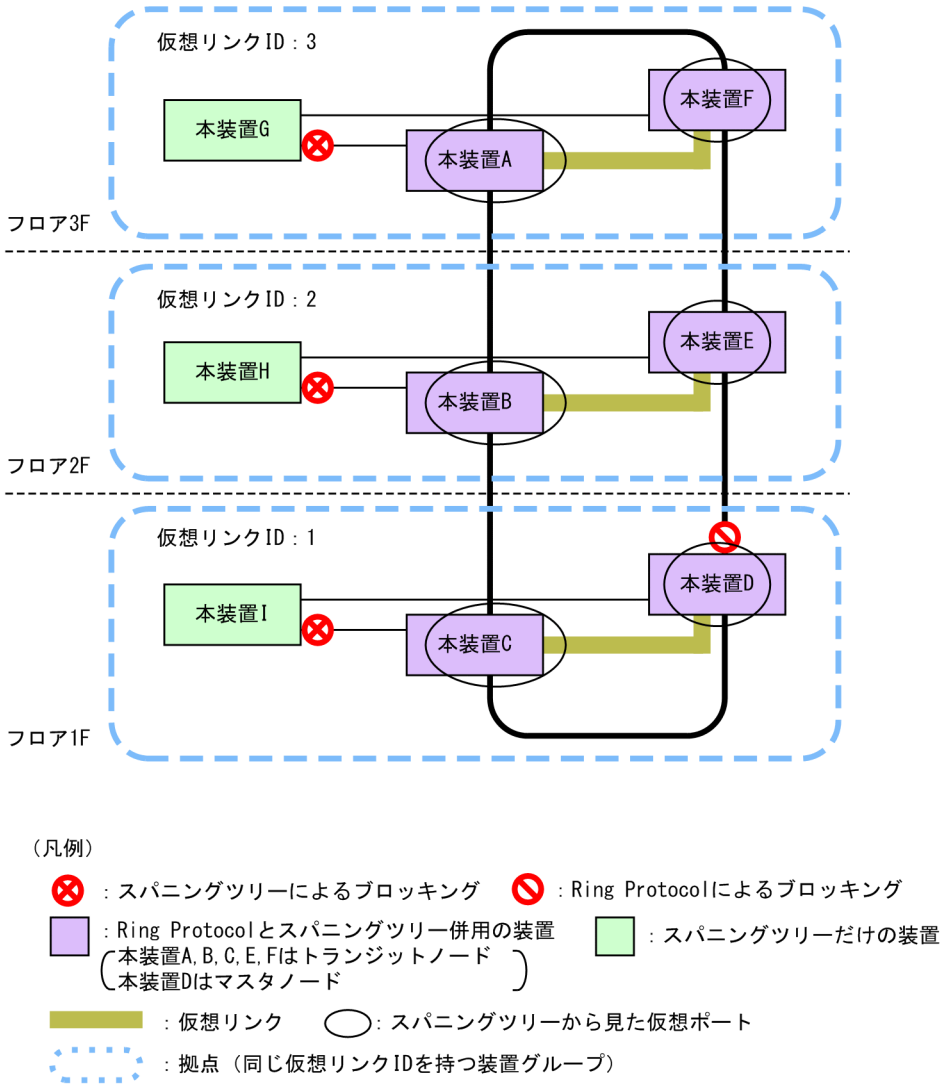
30.1.2　動作仕様

Ring Protocol とスパニングツリーを併用するには，二つの機能が共存している任意の 2 装置間を仮想的な回線で接続する必要があります。この仮想的な回線を仮想リンクと呼びます。仮想リンクは，リングネットワーク上の 2 装置間に構築されます。仮想リンクの構築には，仮想リンクを識別するための仮想リンク ID と，仮想リンク間で制御フレームの送受信を行うための仮想リンク VLAN が必要です。

Ring Protocol とスパニングツリーを併用するノードは，自装置の仮想リンク ID と同じ仮想リンク ID を持つ装置同士でスパニングツリートポロジーを構成します。同じ仮想リンク ID を持つ装置グループを拠点と呼び，各拠点では独立したスパニングツリートポロジーを構成します。

仮想リンクの概要を次の図に示します。

図 30-3　仮想リンクの概要



注　各フロアはそれぞれ独立したスパニングツリートポロジーを構成しています。

(1)　仮想リンク VLAN

仮想リンク間での制御フレームの送受信には，仮想リンク VLAN を使用します。この仮想リンク VLAN は，リングポートのデータ転送用 VLAN として管理している VLAN のうち一つを使用します。また，仮想リンク VLAN は，複数の拠点で同一の VLAN ID を使用できます。

(2)　Ring Protocol の制御 VLAN の扱い

Ring Protocol の制御 VLAN は，スパニングツリーの対象外となります。

そのため，PVST+では当該 VLAN のツリーを構築しません。また，シングルスパニングツリーおよびマルチプルスパニングツリーの転送状態も適用されません。

(3)　リングポートの状態とコンフィグレーションの設定値

リングポートのデータ転送用 VLAN の転送状態は，Ring Protocol で決定されます。

例えば，スパニングツリートポロジーでブロッキングと判断しても，Ring Protocol でフォワーディングと判断すれば，そのポートはフォワーディングとなります。したがって，スパニングツリーでリングポートがブロッキングとなるトポロジーを構築すると，ループとなるおそれがあります。このため，リングポートが常にフォワーディングとなるよう，Ring Protocol と共存したスパニングツリーでは，本装置がルートブリッジまたは 2 番目の優先度になるようにブリッジ優先度の初期値を自動的に高くして動作します。なお，コンフィグレーションで値を設定している場合は，設定した値で動作します。

ブリッジ優先度の設定値を次の表に示します。

表 30–1　ブリッジ優先度の設定値

設定項目	関連するコンフィグレーション	初期値
ブリッジ優先度	spanning-tree single priority spanning-tree vlan priority spanning-tree mst root priority	0

また，仮想リンクのポートは固定値で動作し，コンフィグレーションによる設定値は適用されません。

仮想リンクのポートの設定値を次の表に示します。

表 30–2　仮想リンクポートの設定値

設定項目	関連するコンフィグレーション	初期値（固定）
リンクタイプ	spanning-tree link-type	point-to-point
ポート優先度	spanning-tree port-priority spanning-tree single port-priority spanning-tree vlan port-priority spanning-tree mst port-priority	0
パスコスト	spanning-tree cost spanning-tree single cost spanning-tree vlan cost spanning-tree mst cost	1

(4)　リングポートでのスパニングツリー機能について

リングポートでは次に示すスパニングツリー機能は動作しません。

- BPDU フィルタ
- BPDU ガード
- ループガード機能
- ルートガード機能
- PortFast 機能

(5)　スパニングツリートポロジー変更時の MAC アドレステーブルクリア

スパニングツリーでのトポロジー変更時に，シングルリングまたはマルチリングネットワーク全体に対して，MAC アドレステーブルエントリのクリアを促すフラッシュ制御フレームを送信します。これを受信したリングネットワーク内の各装置は，Ring Protocol が動作中のリングポートに対する，MAC アドレス

テーブルエントリをクリアします。なお，トポロジー変更が発生した拠点の装置は，スパニングツリープロトコルで MAC アドレステーブルエントリをクリアします。

(6)　リングポート以外のポートの一時的なブロッキングについて

Ring Protocol とスパニングツリーを併用する装置で，次に示すイベントが発生した場合，リングポート以外のスパニングツリーが動作しているポートを一時的にブロッキング状態にします。

- 装置起動（装置再起動も含む）
- コンフィグレーションファイルのランニングコンフィグレーションへの反映
- restart vlan コマンド
- restart spanning-tree コマンド

スパニングツリーが仮想リンク経由の制御フレームを送受信できるようになる前にアクセスネットワーク内だけでトポロジを構築した場合，それだけではループ構成とならないためどのポートもブロッキングされません。したがって，このままでは，リングネットワークとアクセスネットワークにわたるループ構成となります。このため，本機能で一時的にブロッキングしてループを防止します。本機能は PortFast 機能を設定しているポートでも動作します。本機能でのブロッキングは，次のどちらかで行われます。

- イベント発生から 20 秒間
- イベント発生から 20 秒以内に仮想リンク経由で制御フレームを受信した場合は受信から 6 秒間

本機能を有効に動作させるため，次の表に示すコンフィグレーションを「設定値」の範囲内で設定してください。範囲内の値で設定しなかった場合，一時的にループが発生するおそれがあります。

表 30-3　リングポート以外のポートを一時的にブロッキング状態にするときの設定値

設定項目	関連するコンフィグレーション	設定値
Ring Protocol フラッシュ制御フレームの受信待ち保護時間	forwarding-shift-time	10 秒以下 （デフォルト値 10 秒）
スパニングツリー制御フレーム送信間隔	spanning-tree single hello-time spanning-tree vlan hello-time spanning-tree mst hello-time	2 秒以下 （デフォルト値 2 秒）

30.1.3　各種スパニングツリーとの共存について

(1)　PVST+との共存

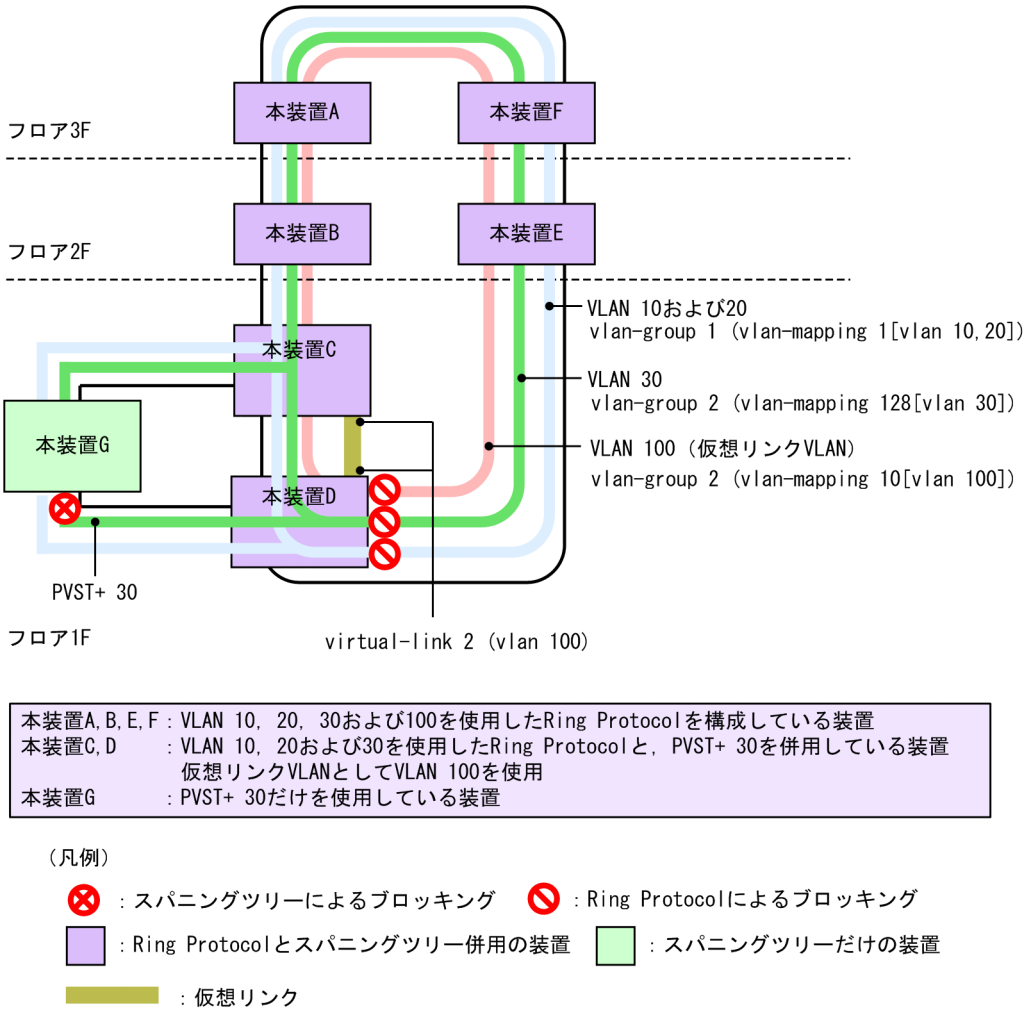
PVST+は，Ring Protocol の VLAN マッピングに設定された VLAN が一つだけであれば，その VLAN で Ring Protocol と共存できます。コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定すると，仮想リンクによるトポロジーを構築し Ring Protocol との共存を開始します。

最初の Ring Protocol のコンフィグレーション設定によって，動作中の PVST+はすべて停止します。その後，VLAN マッピングが設定された VLAN で順次 PVST+が動作します。VLAN マッピングに複数の VLAN を設定した場合，その VLAN では PVST+は動作しません。なお，PVST+が停止している VLAN はループとなるおそれがあります。ポートを閉塞するなどしてループ構成にならないように注意してください。

また，コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定していない場合は，仮想リンクを構築できないので意図したトポロジーが構築されません。その結果，ループが発生するおそれがあります。

PVST+と Ring Protocol の共存構成を次の図に示します。ここでは，VLAN マッピング 128 には VLAN 30 が一つだけ設定されているので，PVST+が動作します。VLAN マッピング 1 には複数 VLAN が設定されているので，PVST+は動作しません。また，装置 C および D では VLAN 100 を仮想リンク VLAN に設定しているので，両装置間に仮想リンクを構築します。

図 30-4　PVST+と Ring Protocol の共存構成



(2)　シングルスパニングツリーとの共存

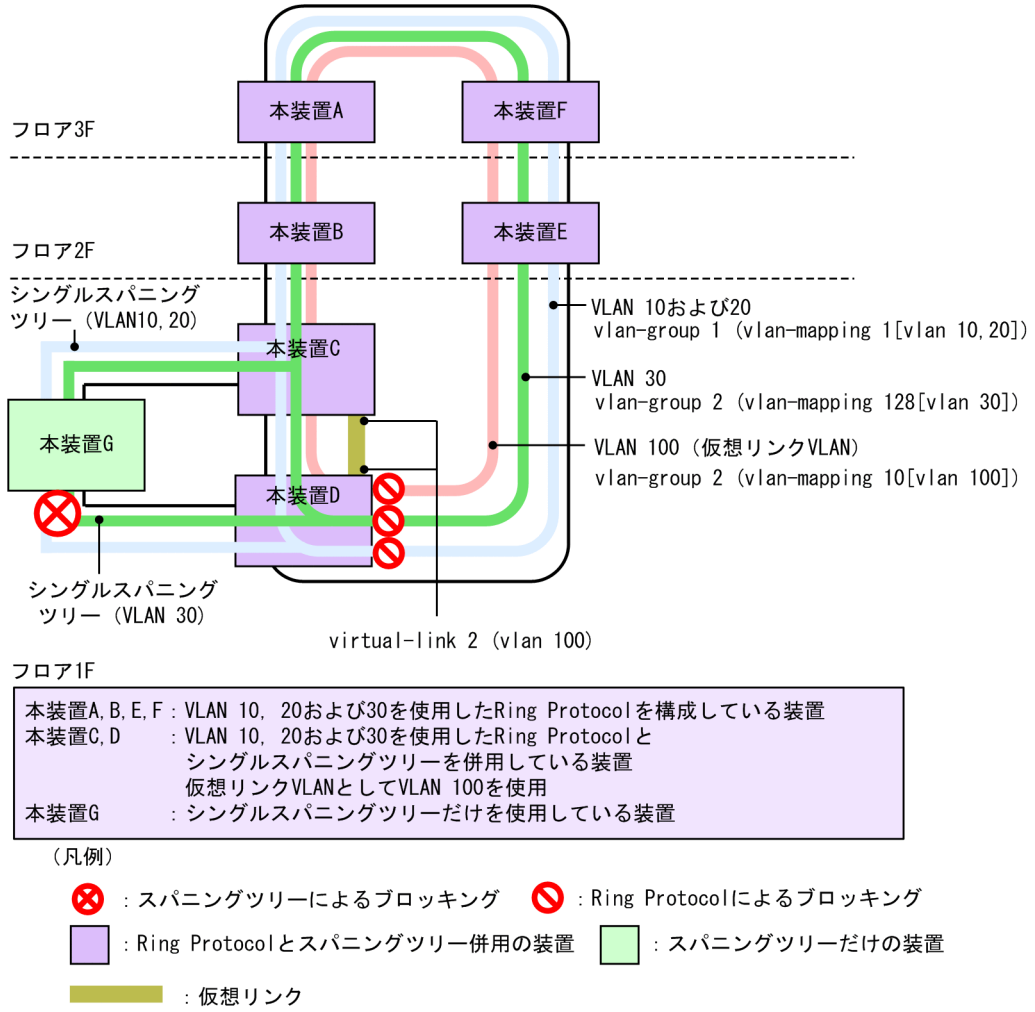
シングルスパニングツリーは Ring Protocol で運用するすべてのデータ VLAN と共存できます。

シングルスパニングツリーは，コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定すると，仮想リンクによるトポロジーを構築し Ring Protocol との共存を開始します。コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定していない場合は，仮想リンクを構築できないので意図したトポロジーが構築されません。その結果ループが発生するおそれがあります。

シングルスパニングツリーと Ring Protocol の共存構成を次の図に示します。ここでは，装置 C，D，および G にシングルスパニングツリーを設定し，装置 A，B，C，D，E，および F に Ring Protocol の VLAN

グループを二つ設定しています。シングルスパニングツリーのトポロジーは，全 VLAN グループ（全 VLAN マッピング）に所属している VLAN にそれぞれ反映されます。また，装置 C および D では VLAN 100 を仮想リンク VLAN に設定しているので，両装置間に仮想リンクを構築します。

図 30-5　シングルスパニングツリーと Ring Protocol の共存構成

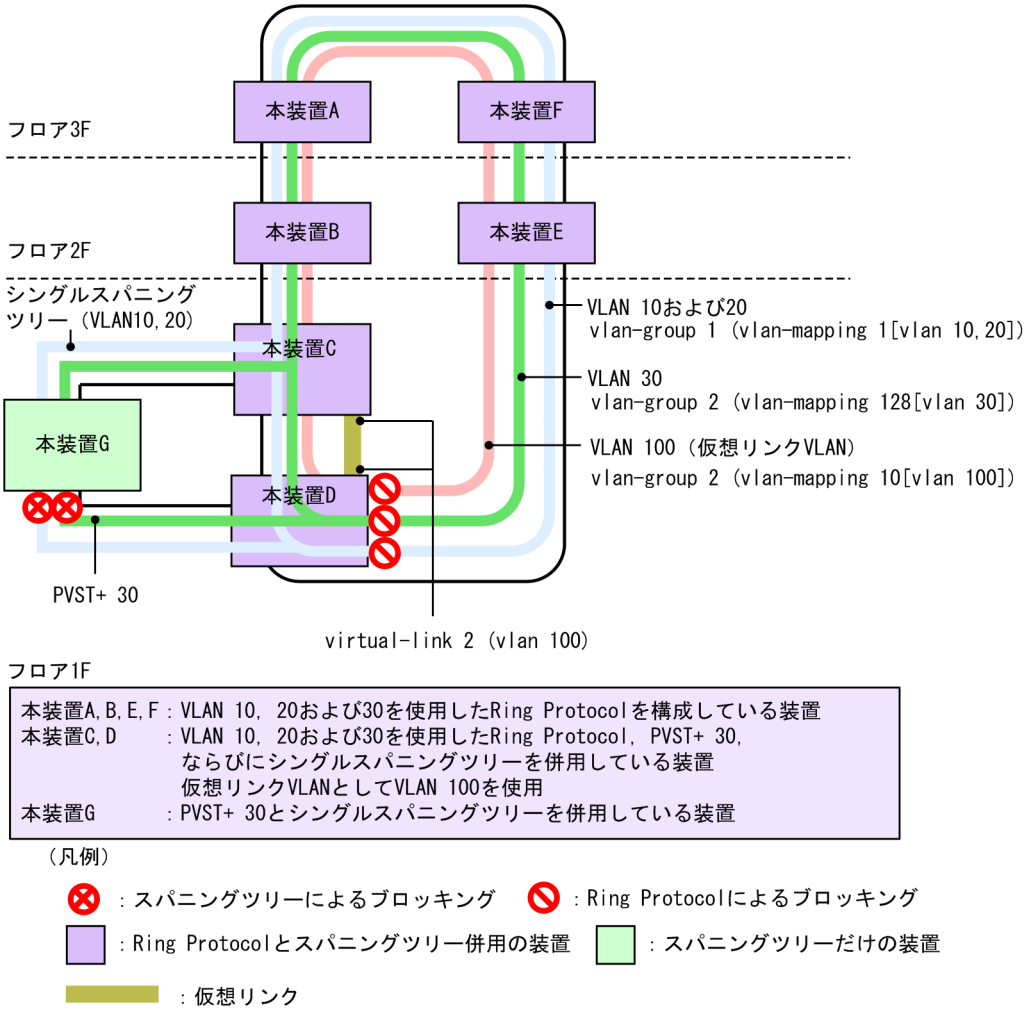


(3)　PVST+とシングルスパニングツリーの同時動作について

Ring Protocol と共存している場合でも，PVST+とシングルスパニングツリーの同時動作は可能です。この場合，PVST+で動作していない VLAN はすべてシングルスパニングツリーとして動作します（通常の同時動作と同じです）。

シングルスパニングツリー，PVST+，および Ring Protocol の共存構成を次の図に示します。ここでは，VLAN マッピング 128 には VLAN 30 が一つだけ設定されているので，PVST+が動作します。VLAN マッピング 1 では PVST+が動作しないので，シングルスパニングツリーとして動作し，トポロジーを反映します。また，装置 C および D では VLAN 100 を仮想リンク VLAN に設定しているので，両装置間に仮想リンクを構築します。

図 30-6　シングルスパニングツリー，PVST+，および Ring Protocol の共存構成



(4)　マルチプルスパニングツリーとの共存

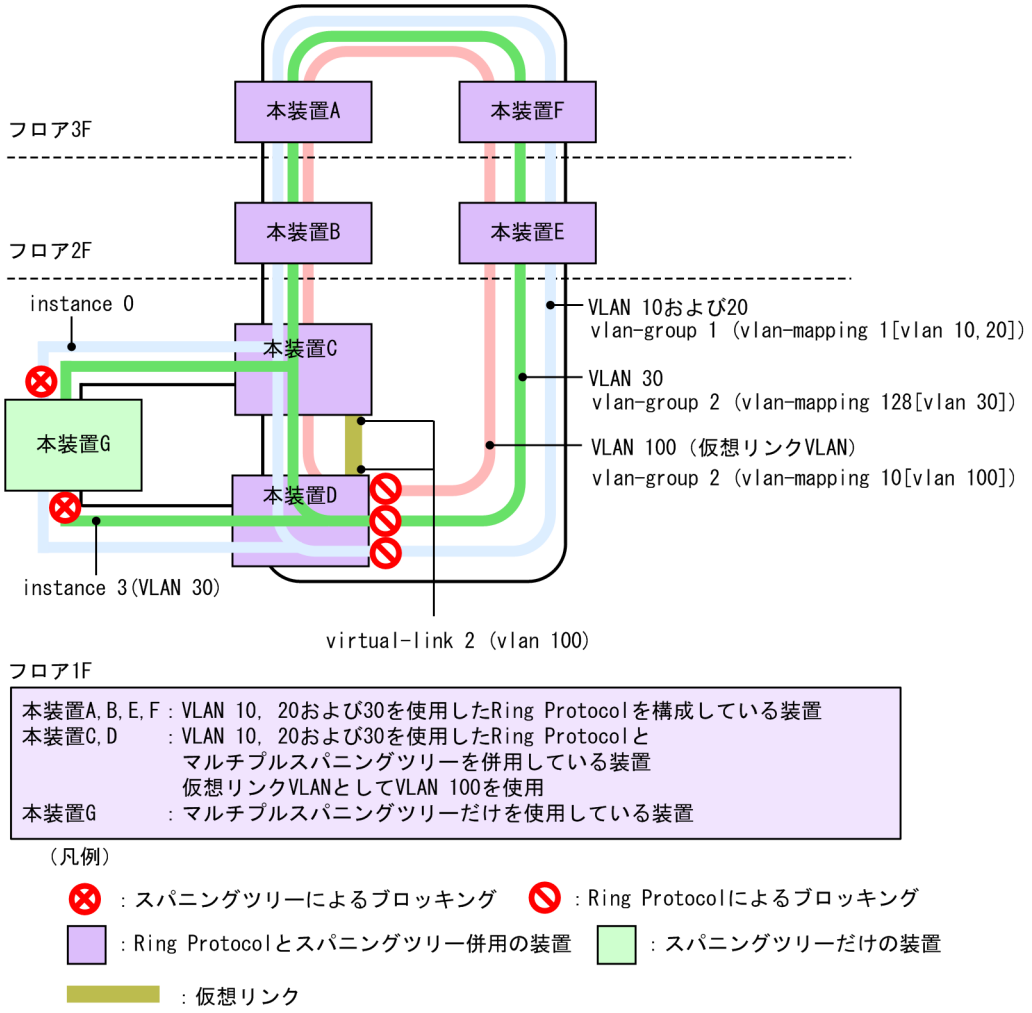
マルチプルスパニングツリーは Ring Protocol で運用するすべてのデータ転送用 VLAN と共存できます。

マルチプルスパニングツリーは，コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定すると，仮想リンクによるトポロジーを構築し Ring Protocol との共存を開始します。コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定していない場合は，仮想リンクを構築できないので意図したトポロジーが構築されません。その結果ループが発生するおそれがあります。

MST インスタンスに所属する VLAN と，Ring Protocol の VLAN マッピングで同じ VLAN を設定すると，MST インスタンスと Ring Protocol で共存動作できるようになります。設定した VLAN が一致しない場合，一致していない VLAN はブロッキング状態になります。

マルチプルスパニングツリーと Ring Protocol の共存構成を次の図に示します。ここでは，装置 C，D，および G にマルチプルスパニングツリーを設定し，装置 A，B，C，D，E，および F に Ring Protocol の VLAN グループを二つ設定しています。Ring Protocol の VLAN グループ 1 は CIST，VLAN グループ 2 は MST インスタンス 3 としてマルチプルスパニングツリーのトポロジーに反映されます。また，装置 C および D では VLAN 100 を仮想リンク VLAN に設定しているので，両装置間に仮想リンクを構築します。

図 30-7　マルチプルスパニングツリーと Ring Protocol の共存構成



(5)　共存して動作させない VLAN について

- Ring Protocol だけを適用させる VLAN

  PVST+をコンフィグレーション設定などで停止させると，その VLAN は Ring Protocol だけが適用される VLAN となります。

  シングルスパニングツリー動作時，またはマルチプルスパニングツリー動作時，Ring Protocol が扱うデータ転送用 VLAN は必ず共存して動作します。

- PVST+だけを適用させる VLAN

  Ring Protocol で VLAN グループに所属しない VLAN マッピングを設定すると，PVST+だけが適用される VLAN となります。

- シングルスパニングツリーだけを適用させる VLAN

  Ring Protocol で VLAN グループに所属しない VLAN は，シングルスパニングツリーだけが適用される VLAN となります。

- マルチプルスパニングツリーだけを適用させる VLAN

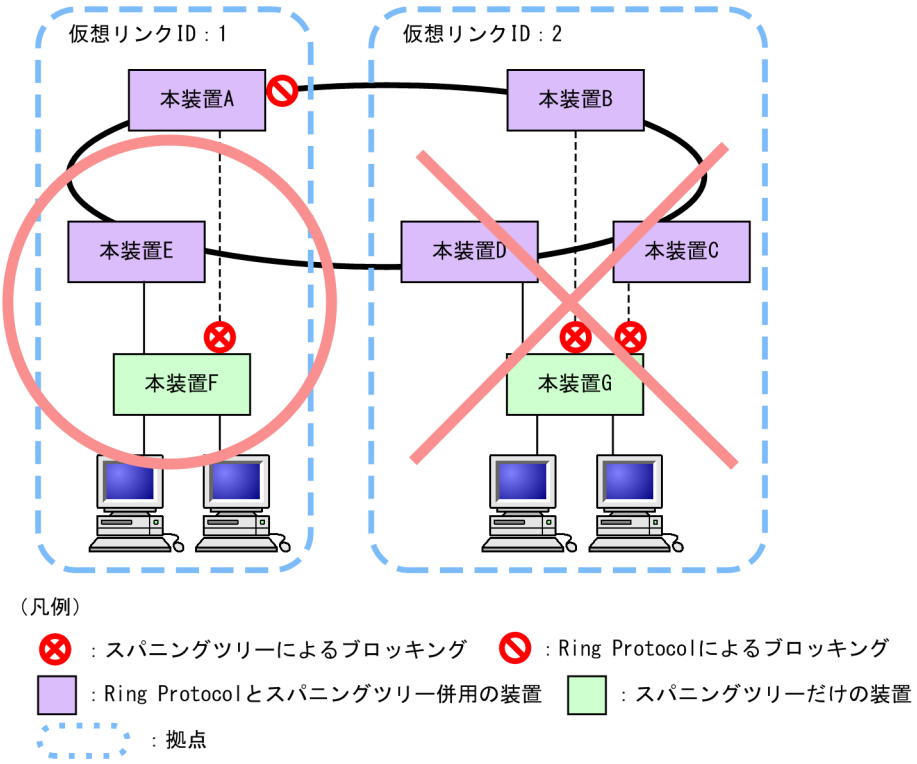
  Ring Protocol で VLAN グループに所属しない VLAN は，マルチプルスパニングツリーだけが適用される VLAN となります。

30.1.4　禁止構成

(1)　1 拠点当たりの装置数

Ring Protocol とスパニングツリーを併用した本装置は，1 拠点に 2 台配置できます。3 台以上で 1 拠点を構成することはできません。仮想リンクの禁止構成を次の図に示します。

図 30-8　仮想リンクの禁止構成



30.1.5　Ring Protocol とスパニングツリー併用時の注意事項

(1)　仮想リンク VLAN と VLAN マッピングの対応づけについて

仮想リンク VLAN に指定する VLAN は，リング内のデータ転送用 VLAN に所属（VLAN マッピングおよび VLAN グループに設定）している必要があります。

(2)　仮想リンク VLAN の設定範囲について

- リングネットワークへの設定

  仮想リンクを構成しているリングネットワークでは，シングルリングおよびマルチリング（共有リンクありのマルチリング構成も含む）どちらの場合でも，仮想リンク間で制御フレームを送受信する可能性のあるすべてのノードに対して仮想リンク VLAN をデータ転送用 VLAN に設定しておく必要があります。設定が不足していると，拠点ノード間で仮想リンクを使って制御フレームの送受信ができず，障害の誤検出を起こすおそれがあります。

- スパニングツリーネットワークへの設定

  仮想リンク VLAN は，リングネットワーク内で使用するため，下流側のスパニングツリーには使用できません。このため，スパニングツリーで制御する下流ポートに対して仮想リンク VLAN を設定すると，ループするおそれがあります。

(3) 仮想リンク VLAN を設定していない場合のスパニングツリーについて

仮想リンク VLAN を設定していない場合は，仮想リンクを構築できないので意図したトポロジーが構築されません。その結果ループが発生するおそれがあります。

(4) Ring Protocol の設定および削除によるスパニングツリー停止について

Ring Protocol のコンフィグレーションの設定および削除によって，動作中のスパニングツリーが停止することがあります。スパニングツリーが停止すると，該当する VLAN はループになるなど，スパニングツリーのトポロジーに影響を与えるおそれがあります。

- PVST+が動作している状態で，Ring Protocol の最初のコンフィグレーションを設定すると，動作中の PVST+が停止します。Ring Protocol の最初のコンフィグレーションを設定するときは，該当 VLAN に所属するポート（物理ポートまたはチャネルグループ）を shutdown に設定するなどダウン状態にした上で実施してください。コンフィグレーションコマンド axrp vlan-mapping を設定して，すべての VLAN のトポロジーを構築する準備が完了したあとで，ダウン状態にしていたポートをアップ状態にしてください。
- Ring Protocol と PVST+を併用している状態で，コンフィグレーションコマンド axrp vlan-mapping を削除すると，動作中の PVST+が停止します。axrp vlan-mapping コマンドを削除するときは，該当 VLAN に所属するポート（物理ポートまたはチャネルグループ）を shutdown に設定するなどダウン状態にした上で実施してください。該当する VLAN の設定を削除するか，または Ring Protocol のすべてのコンフィグレーションを削除したあとで，ダウン状態にしていたポートをアップ状態にしてください。
- Ring Protocol とマルチプルスパニングツリーを併用している状態で，Ring Protocol の最後のコンフィグレーションを削除すると，動作中のマルチプルスパニングツリーの一部が停止します。Ring Protocol の最後のコンフィグレーションを削除するときは，スパニングツリーを構成するポート（物理ポートまたはチャネルグループ）を shutdown に設定するなどダウン状態にした上で実施してください。Ring Protocol の最後のコンフィグレーションを削除したあとで，ダウン状態にしていたポートをアップ状態にしてください。

(5) Ring Protocol とスパニングツリー併用時のネットワーク構築について

Ring Protocol およびスパニングツリーを利用するネットワークは基本的にループ構成となります。既設のリングネットワークに対し，アクセスネットワークにスパニングツリーを構築する際は，スパニングツリーネットワーク側の構成ポート（物理ポートまたはチャネルグループ）を shutdown に設定するなどダウン状態にした上で構築してください。

(6) Ring Protocol の障害監視時間とスパニングツリーの BPDU の送信間隔について

Ring Protocol のヘルスチェックフレームの障害監視時間（health-check holdtime）は，スパニングツリーの BPDU のタイムアウト検出時間（hello-time×3(秒)）よりも小さな値を設定してください。大きな値を設定すると，リングネットワーク内で障害が発生した際に，Ring Protocol が障害を検出する前にスパニングツリーが BPDU のタイムアウトを検出してしまい，トポロジー変更が発生し，ループするおそれがあります。

(7) トランジットノードでのプログラム再起動時の対応について

Ring Protocol プログラムを再起動（運用コマンド restart axrp）する際は，スパニングツリーネットワーク側の構成ポート（物理ポートまたはチャネルグループ）を shutdown に設定するなどダウン状態にした上で実施してください。再起動後は，トランジットノードのフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）のタイムアウトを待つか，制御 VLAN のフォワーディング遷移時間

（forwarding-delay-time）を利用して経路を切り替えたあとで，ダウン状態にしたポートの shutdown などを解除してください。

(8)　リングネットワークでの片方向リンク障害の対応について

Ring Protocol は，片方向リンク障害でのリング障害は検出しません。リングネットワークで片方向リンク障害が発生すると，仮想リンク制御フレームを送受信できなくなるため，スパニングツリーが BPDU タイムアウトを誤検出してしまうことがあります。その結果，ループが発生し，ループ状態は片方向リンク障害が解消されるまで継続するおそれがあります。

Ring Protocol と IEEE802.3ah/UDLD 機能を併用すれば，片方向リンク障害を検出できるようになるため，片方向リンク障害によるループの発生を防止できます。

(9)　スパニングツリー併用環境での多重障害からの復旧手順について

リングネットワーク内で 2 か所以上の障害（多重障害）が発生したことによって，仮想リンク制御フレームを送受信できなくなり，スパニングツリーのトポロジー変更が発生する場合があります。多重障害には，Ring Protocol とスパニングツリーを併用した装置で両リングポートに障害が発生した場合も含みます。この状態からリングネットワーク内のすべての障害を復旧する際は，次に示す手順で復旧してください。

1. スパニングツリーネットワークの構成ポート（物理ポートまたはチャネルグループ）を shutdown にするなどダウン状態にします。
2. リングネットワーク内の障害個所を復旧し，マスタノードでリング障害の復旧を検出させます。
3. スパニングツリーネットワーク側の構成ポートの shutdown などを解除し，復旧させます。

(10)　Ring Protocol の VLAN マッピングとマルチプルスパニングツリーの MST インスタンスに所属する VLAN との整合性について

コンフィグレーションの変更過程で，Ring Protocol の VLAN マッピングとマルチプルスパニングツリーの MST インスタンスに所属する VLAN の設定が完全に一致しない場合，一致していない VLAN はブロッキング状態になり，通信できないおそれがあります。

30.2　Ring Protocol と GSRP との併用

本装置では，Ring Protocol と GSRP との併用ができます。Ring Protocol の詳細については，「28　Ring Protocol の解説」を参照してください。

30.2.1　動作概要

Ring Protocol と GSRP が併用して動作している装置では，Ring Protocol の VLAN マッピングと GSRP の VLAN グループの VLAN 情報が一致している必要があります。この装置のリングポートは GSRP の制御対象外となり，リングポートのデータ転送状態は Ring Protocol で制御します。

障害の監視や障害発生時の経路切り替えは，リングネットワークでは Ring Protocol で，GSRP ネットワークでは GSRP で，独立して実施します。ただし，GSRP ネットワークで経路の切り替え時にマスタに遷移した装置は，GSRP スイッチおよび aware/unaware 装置の MAC アドレステーブルをクリアします。同時に，リングネットワーク用のフラッシュ制御フレームを送信して，リングネットワークを構成する装置の MAC アドレステーブルもクリアします。

GSRP のダイレクトリンクは，リングネットワークと同じ回線を使用できます。また，別の回線にすることもできます。

Ring Protocol と GSRP との併用例を次の図に示します。

図 30-9　Ring Protocol と GSRP の併用例（ダイレクトリンクをリングネットワークで使用する場合）

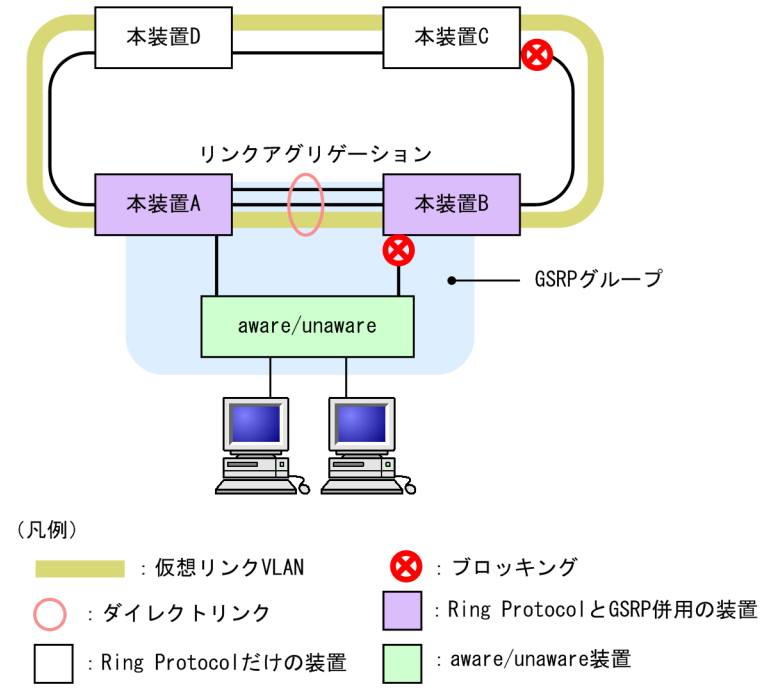
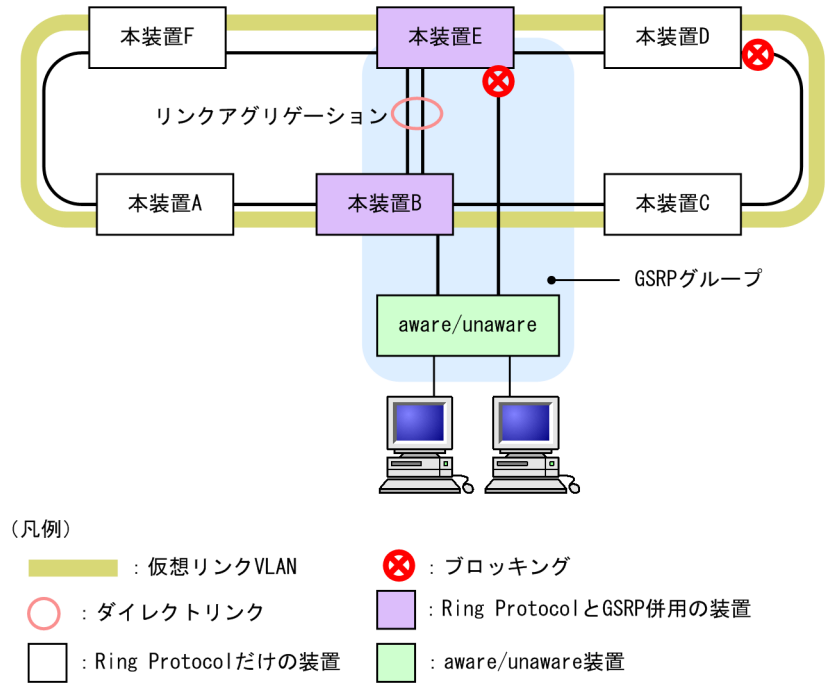


図 30-10　Ring Protocol と GSRP の併用例 (ダイレクトリンクをリングネットワークで使用しない場合)



30.2.2　併用条件

Ring Protocol と GSRP の併用条件を示します。

(1)　Ring Protocol と GSRP を併用動作させたい VLAN の設定条件

Ring Protocol の VLAN マッピングの VLAN と GSRP の VLAN グループの VLAN をすべて一致させてください。

(2)　Ring Protocol または GSRP を単独で動作させたい VLAN の設定条件

すべての VLAN を共存動作させる必要はありません。VLAN 単位に別々のプロトコルを動作させる場合は，Ring Protocol の VLAN マッピングの VLAN と GSRP の VLAN グループの VLAN で一致する VLAN がないようにしてください。

30.2.3　リングポートの扱い

リングポートはコンフィグレーションコマンド gsrp exception-port の設定有無にかかわらず，GSRP の制御対象外ポートとして動作します。リングポートのデータ転送状態は Ring Protocol だけが制御します。

また，リングポートに次のコンフィグレーションコマンドを設定しても無効になります。

- gsrp reset-flush-port（ポートリセット機能を実施するポート）
- gsrp no-flush-port（GSRP Flush request フレームを送信しないポート）

30.2.4　Ring Protocol の制御 VLAN の扱い

Ring Protocol の制御 VLAN を GSRP の VLAN グループに設定した場合，該当する VLAN を VLAN グループの所属外にします。VLAN グループの所属外になった VLAN については，運用コマンド show gsrp では表示されません。

30.2.5　GSRP ネットワーク切り替え時の MAC アドレステーブルクリア

Ring Protocol と GSRP を併用する場合，GSRP ネットワークの経路切り替え時にはリングネットワークを構成する装置の MAC アドレステーブルをクリアする必要があります。MAC アドレステーブルをクリアしないと，すぐに通信が復旧しないおそれがあります。リングネットワーク上の装置の MAC アドレステーブルをクリアするために，GSRP のマスタに遷移した際，リングネットワーク上に設定した仮想リンク VLAN を使用して，リングネットワーク用のフラッシュ制御フレームを送信します。この仮想リンク VLAN は，Ring Protocol のデータ転送用 VLAN グループに所属する必要があります。

GSRP のマスタが送信したフラッシュ制御フレームをリング構成装置が受信すると，MAC アドレステーブルをクリアします。また，送信回数は GSRP のコンフィグレーション（flush-request-count）に従います。

なお，Ring Protocol と GSRP を異なる VLAN で単独動作させる場合は，障害発生時に経路切り替えが発生しても互いのプロトコルに影響を与えません。したがって，MAC アドレステーブルをクリアする必要がないため，仮想リンク VLAN を設定する必要はありません。

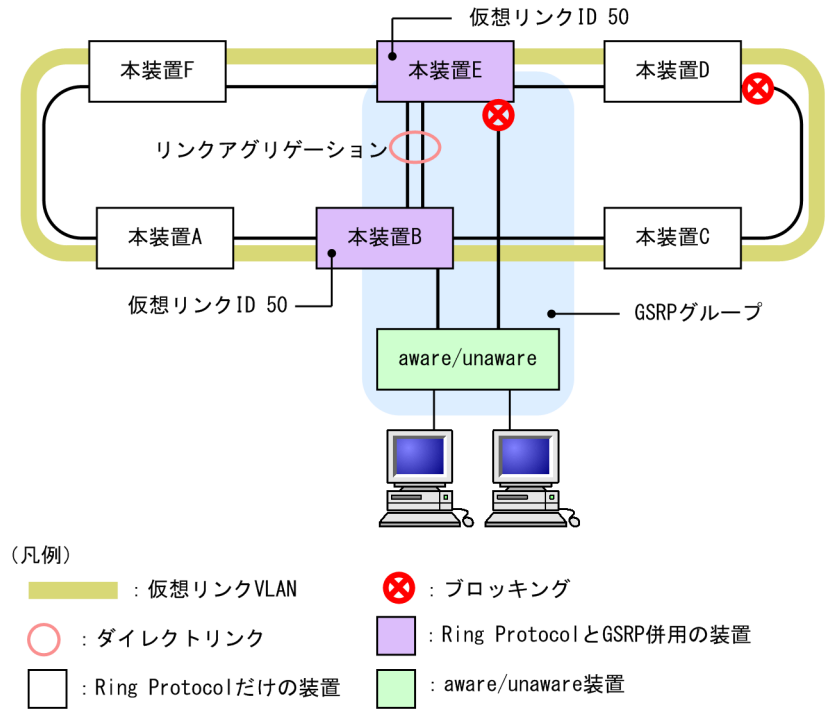
30.2.6　Ring Protocol と GSRP 併用動作時の注意事項

(1)　仮想リンク VLAN の設定について

Ring Protocol と GSRP を併用する場合は，フラッシュ制御フレームを送信するために仮想リンク VLAN の設定が必要です。この仮想リンク VLAN は, Ring Protocol のデータ転送用 VLAN グループに所属する必要があります。

仮想リンク ID の設定を次の図に示します。仮想リンク ID には，同じ GSRP グループ装置で同一の仮想リンク ID を設定する必要があります。また，同じ仮想リンク VLAN が設定されているリングネットワーク内で一意となる値を設定する必要があります。同じ GSRP グループではない本装置 A，C，D，および F に仮想リンク ID 50 を設定すると，該当装置では，フラッシュ制御フレームによる MAC アドレステーブルのクリアができなくなります。

図 30-11　仮想リンク ID の設定



(2)　Ring Protocol の VLAN マッピングまたは GSRP の VLAN グループの変更について

Ring Protocol と GSRP を併用する場合は，Ring Protocol の VLAN マッピングの VLAN と GSRP の VLAN グループの VLAN をすべて一致させる必要があります。コンフィグレーションの変更過程で一致しない状態になった場合，設定された VLAN の中で，ブロッキング状態となり，通信できない VLAN が発生するおそれがあります。

このため，Ring Protocol と GSRP を併用するためにコンフィグレーションを変更する場合は，GSRP のバックアップ装置で，priority コマンドや backup-lock コマンドなどの設定によって，マスタへの切り替えが発生しないようにしてから，変更する必要があります。

(3)　1VLAN グループ当たりに設定可能な VLAN 数について

Ring Protocol と併用している VLAN グループに 511 以上の VLAN 数を所属させると，該当する VLAN グループの状態が遷移したときにリングポートが一時的にブロッキング状態になります。

Ring Protocol と併用している VLAN グループに所属させる VLAN 数は 510 以下にしてください。

(4)　GSRP VLAN グループ限定制御機能について

Ring Protocol と GSRP の併用時，次に示す状態では，GSRP VLAN グループ限定制御機能を設定していても，VLAN グループに所属しない VLAN のポートがブロッキング状態になるおそれがあります。

・Ring Protocol のコンフィグレーションが適切に設定されていないなどの要因で Ring Protocol が動作していない

Ring Protocol 機能が正常に動作していないリング ID の，制御 VLAN に設定している VLAN がブロッキング状態になるおそれがあります。ただし，リングポートはブロッキング状態になりません。

・disable コマンドによって，Ring Protocol 機能を無効にしている

Ring Protocol 機能を無効にしているリング ID の，制御 VLAN に設定している VLAN がブロッキング状態になるおそれがあります。ただし，リングポートはブロッキング状態になりません。

・「30.2.2　併用条件」にある Ring Protocol と GSRP の併用条件を満たしていない

Ring Protocol と GSRP との併用条件を満たしていない VLAN がブロッキング状態になるおそれがあります。

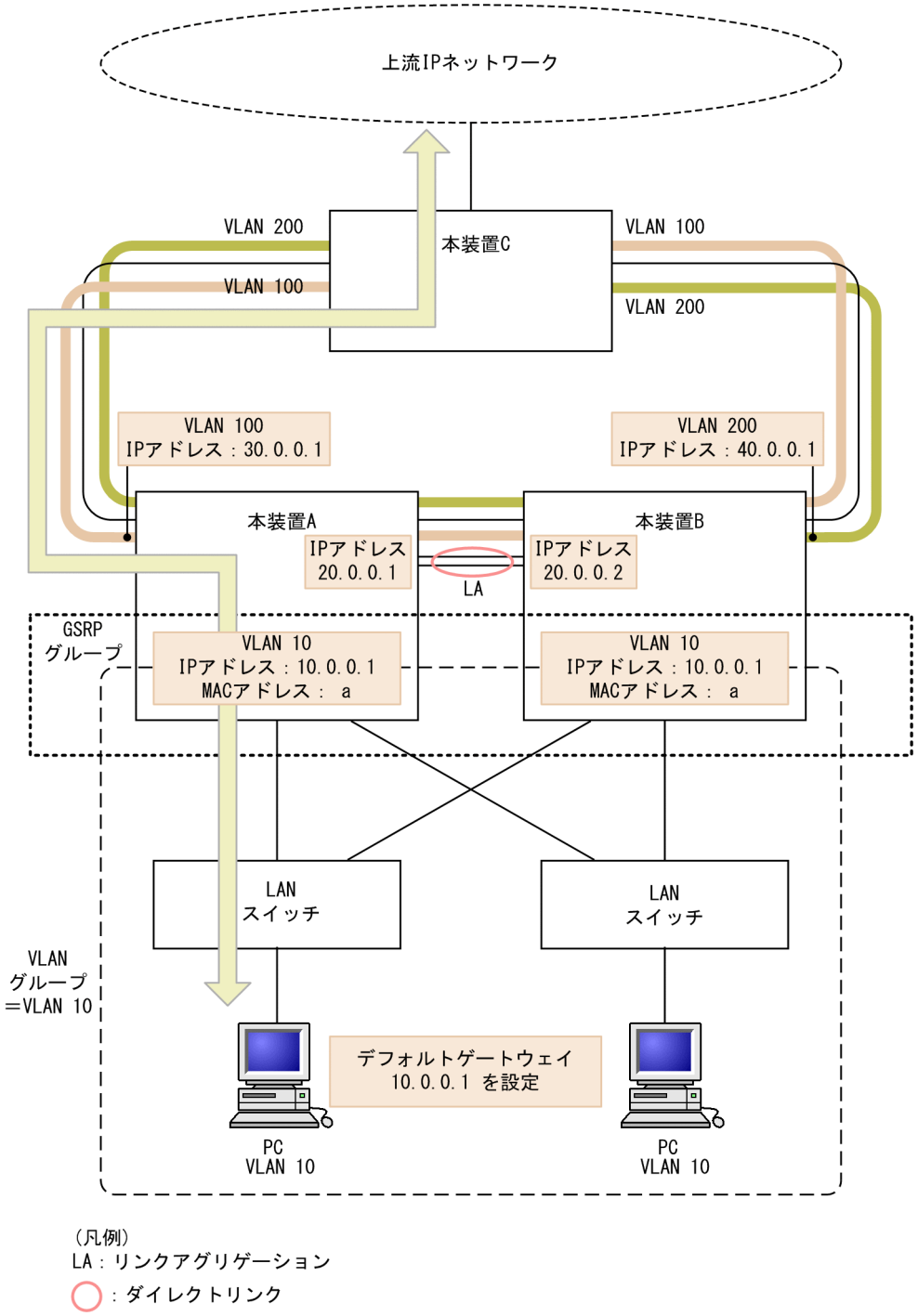
(5)　レイヤ 3 冗長切替機能の適用について

Ring Protocol と GSRP を同じデータ VLAN で併用動作させる場合は，レイヤ 3 冗長切替機能を適用できません。レイヤ 3 冗長切替機能を適用して GSRP ネットワークとリングネットワークを接続する場合は，Ring Protocol と GSRP でそれぞれ異なるデータ VLAN を設定して，単独動作させてください。

30.2.7　単独動作時の動作概要（レイヤ 3 冗長切替機能の適用例）

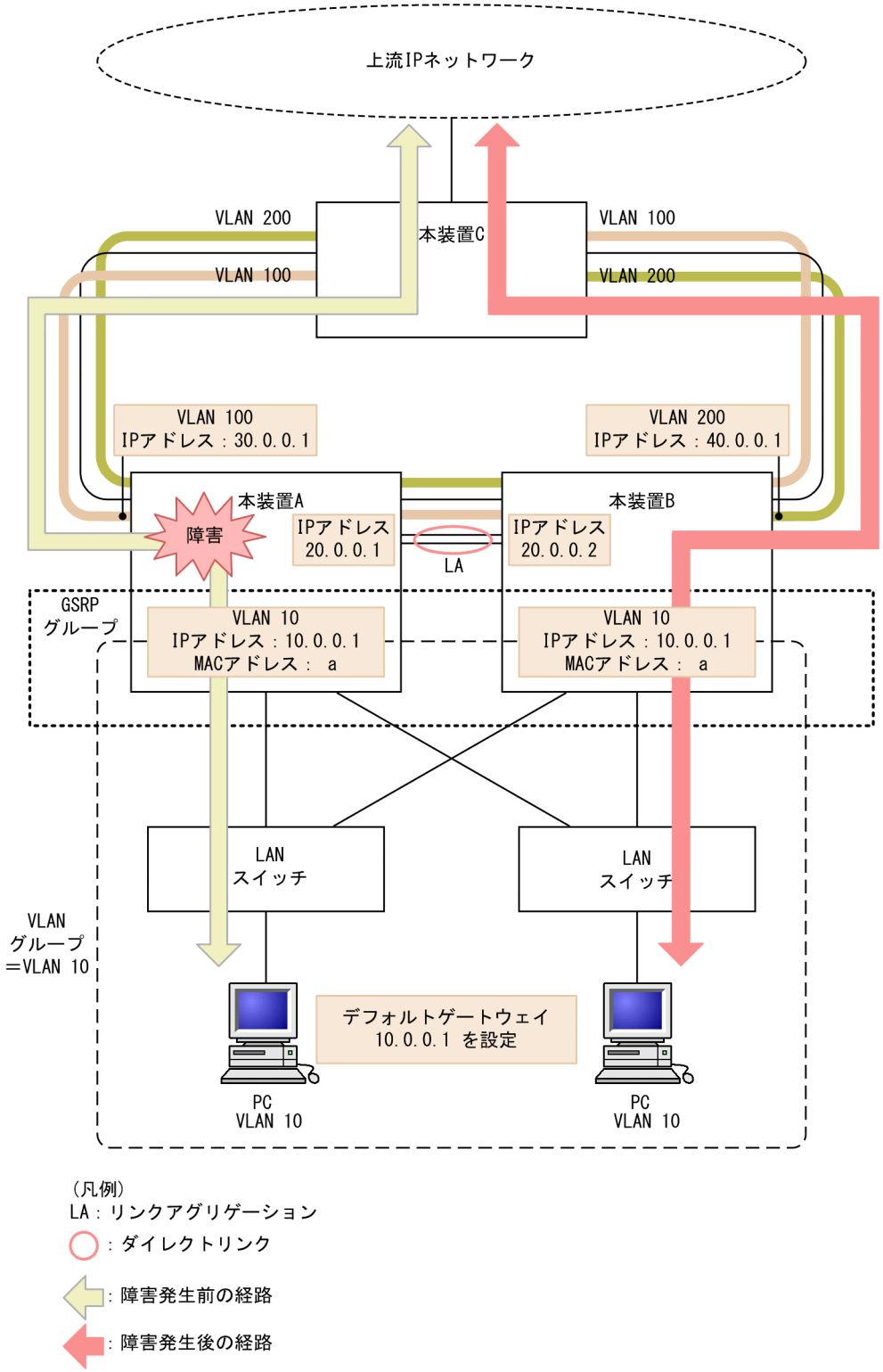
Ring Protocol と GSRP をそれぞれ異なる VLAN で単独動作させている場合は，レイヤ 3 冗長切替機能でリングネットワークと接続します。この場合の例を次の図に示します。下流ネットワーク（PC など）から本装置 A でレイヤ 3 中継し，VLAN 100 のリングネットワークを介して上流ネットワークと通信を行っています。このとき，本装置 A に障害が発生すると，下流ネットワークと上流ネットワークは装置 B（ダイレクトリンク障害検出機能を設定時）でレイヤ 3 中継し，VLAN 200 のリングネットワークを介して通信を行います。

図 30-12　レイヤ 3 冗長切替機能（通常運用時）



（凡例）
LA：リンクアグリゲーション
○：ダイレクトリンク

図 30-13　レイヤ 3 冗長切替機能（障害発生時）



（凡例）
LA：リンクアグリゲーション
：ダイレクトリンク
：障害発生前の経路
：障害発生後の経路

30.3　仮想リンクのコンフィグレーション

Ring Protocol とスパニングツリープロトコルを同一装置で併用するための仮想リンクを設定します。また，Ring Protocol と GSRP を併用する場合は，フラッシュフレームを送信するために仮想リンク VLAN の設定が必要です。

30.3.1　コンフィグレーションコマンド一覧

仮想リンクのコンフィグレーションコマンド一覧を次の表に示します。

表 30-4　コンフィグレーションコマンド一覧

コマンド名	説明
axrp virtual-link	仮想リンク ID を設定します。

30.3.2　仮想リンクの設定

[設定のポイント]

仮想リンク ID および仮想リンク VLAN を設定します。仮想リンクを設定することで，Ring Protocol とスパニングツリー, または Ring Protocol と GSRP の併用が可能になります。同一拠点内の対向装置にも，同じ仮想リンク ID と仮想リンク VLAN を設定してください。また，仮想リンク VLAN は必ずデータ転送用 VLAN に使用している VLAN から一つ選んで使用してください。

[コマンドによる設定]

1. **(config)# axrp virtual-link 10 vlan 100**
   仮想リンク ID を 10 に，仮想リンク VLAN を 100 に設定します。

30.3.3　Ring Protocol と PVST+との併用設定

[設定のポイント]

Ring Protocol と PVST+とを併用する場合は, 併用したい VLAN ID を VLAN マッピングに設定する必要があります。その際，VLAN マッピングに指定する VLAN ID は一つだけです。VLAN マッピングに対して，PVST+と併用する VLAN 以外の VLAN ID が設定されている場合，その VLAN では PVST+が動作しません。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan 10**
   VLAN マッピング ID を 1 として，PVST+と併用する VLAN ID 10 を設定します。
2. **(config)# axrp vlan-mapping 2 vlan 20,30**
   VLAN マッピング ID を 2 として, Ring Protocol だけで使用する VLAN ID 20 および 30 を設定します。
3. **(config)# axrp 1**
   (config-axrp)# vlan-group 1 vlan-mapping 1-2
   VLAN グループ 1 に，VLAN マッピング ID 1 および 2 を設定します。

30.3.4　Ring Protocol とマルチプルスパニングツリーとの併用設定

[設定のポイント]

Ring Protocol とマルチプルスパニングツリーを併用する場合は，併用したい VLAN ID を VLAN マッピングに設定する必要があります。その際，VLAN マッピングに指定する VLAN ID と MST インスタンスに所属する VLAN に指定する VLAN ID を一致させる必要があります。VLAN マッピングと MST インスタンスに所属する VLAN の VLAN ID が一致していない場合，一致していない VLAN の全ポートがブロッキング状態になります。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan 10,20,30**

   VLAN マッピング ID を 1 として，MST インスタンス 10 と併用する VLAN ID 10，20，および 30 を設定します。

2. **(config)# axrp vlan-mapping 2 vlan 40,50**

   VLAN マッピング ID を 2 として，MST インスタンス 20 と併用する VLAN ID 40 および 50 を設定します。

3. **(config)# axrp 1**

   (config-axrp)# vlan-group 1 vlan-mapping 1-2

   (config-axrp)# exit

   VLAN グループ 1 に，VLAN マッピング ID 1 および 2 を設定します。

4. **(config)# spanning-tree mst configuration**

   (config-mst)# instance 10 vlans 10,20,30

   MST インスタンス 10 に所属する VLAN に vlan-mapping 1 で指定した VLAN ID 10，20，および 30 を設定し，Ring Protocol との共存を開始します。

5. **(config-mst)# instance 20 vlans 40,50**

   MST インスタンス 20 に所属する VLAN に vlan-mapping 2 で指定した VLAN ID 40 および 50 を設定し，Ring Protocol との共存を開始します。

30.3.5　Ring Protocol と GSRP との併用設定

[設定のポイント]

Ring Protocol と GSRP とを併用する際には，併用したい VLAN ID を VLAN マッピングと GSRP の VLAN グループに設定する必要があります。この際，VLAN マッピング ID と GSRP の VLAN グループ ID は一致している必要はありません。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan 10,15**

   VLAN マッピング ID を 1 に，GSRP と併用する VLAN ID 10 および 15 を設定します。

2. **(config)# axrp 1**

   (config-axrp)# vlan-group 1 vlan-mapping 1

   (config-axrp)# exit

   VLAN グループ 1 に，VLAN マッピング ID 1 を設定します。

3. **(config)# gsrp 1**

   (config-gsrp)# vlan-group 3 vlan 10,15

GSRP の VLAN グループ 3 に Ring Protocol と併用する VLAN ID 10 および 15 を設定します。

30.4　仮想リンクのオペレーション

30.4.1　運用コマンド一覧

仮想リンクの運用コマンド一覧を次の表に示します。

表 30-5　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリーでの仮想リンクの適用状態を表示します。
show gsrp	GSRP での仮想リンクの適用を表示します。

30.4.2　仮想リンクの状態の確認

仮想リンクの情報は show spanning-tree コマンドで確認してください。Port Information で仮想リンクポートが存在していることを確認してください。

show spanning-tree コマンドの実行結果を次の図に示します。

図 30-14　show spanning-tree コマンドの実行結果

```
> show spanning-tree vlan 2
Date 20XX/11/04 11:39:43 UTC
VLAN 2              PVST+ Spanning Tree:Enabled  Mode:PVST+
  Bridge ID        Priority:4096      MAC Address:0012.e205.0900
    Bridge Status:Designated
  Root Bridge ID   Priority:0         MAC Address:0012.e201.0900
    Root Cost:0
    Root Port:1/0/2-3(VL:10)                              … 1
  Port Information
    1/0/1   Up     Status:Forwarding  Role:Designated
    VL(10)  Up     Status:Forwarding  Role:Root           … 1
>
```

1. VL は，仮想リンク ID を示しています。

show gsrp detail コマンドで仮想リンクが運用されているか確認できます。Virtual Link ID で仮想リンク ID と仮想リンク VLAN を確認してください。

図 30-15　show gsrp detail コマンドの実行結果

```
>show gsrp detail
Date 20XX/04/10 12:00:00 UTC

GSRP ID: 3
 Local MAC Address       : 0012.e2a8.2527
 Neighbor MAC Address    : 0012.e2a8.2505
 Total VLAN Group Counts : 3
 GSRP VLAN ID            : 105
 Direct Port             : 0/10-11
 GSRP Exception Port     : 0/1-5
 No Neighbor To Master   : manual
 Backup Lock             : disable
 Port Up Delay           : 0
 Last Flush Receive Time : -
 Layer 3 Redundancy      : On
 Virtual Link ID         : 100(VLAN ID : 20)

                         Local               Neighbor
 Advertise Hold Time     : 5                   5
 Advertise Hold Timer    : 4                   -
 Advertise Interval      : 1                   1
```

```
 Selection Pattern       : ports-priority-mac  ports-priority-mac

 VLAN Group ID      Local State         Neighbor State
 1                  Backup              Master
 2                  (disable)           -
 8                  Master              -
>
```

31 IGMP snooping/MLD snooping の解説

IGMP snooping/MLD snooping はレイヤ 2 スイッチで VLAN 内のマルチキャストトラフィックを制御する機能です。この章では，IGMP snooping/MLD snooping について説明します。

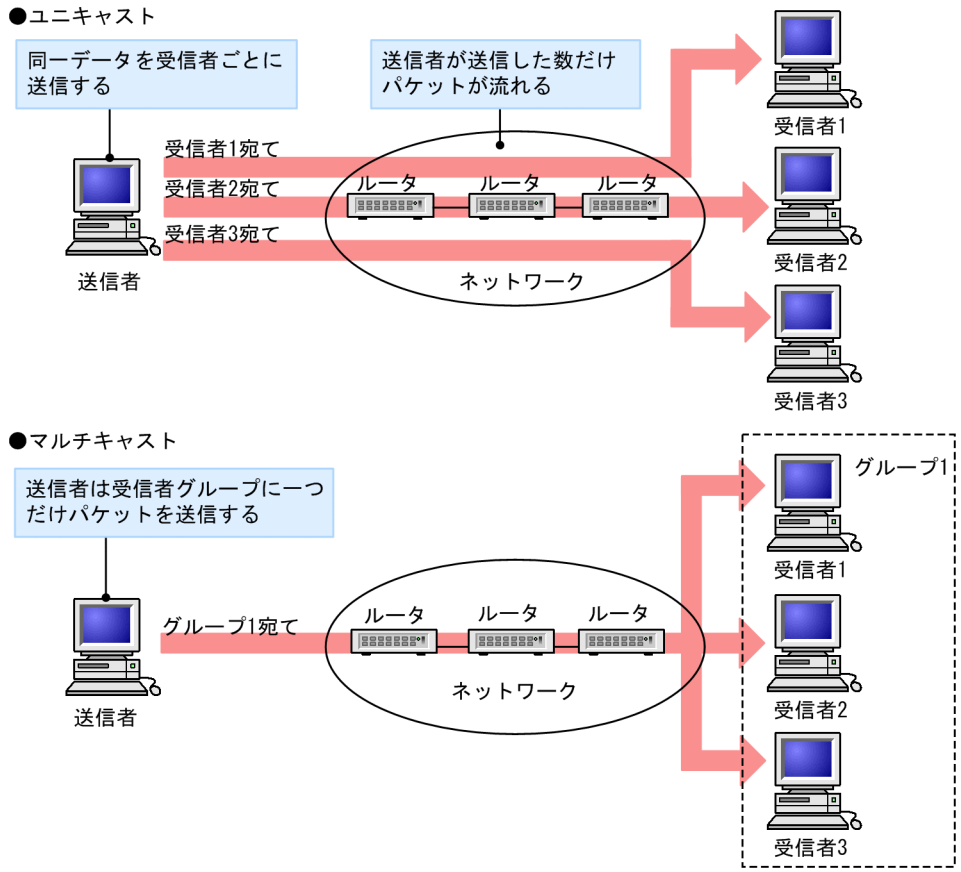
31.1　IGMP snooping/MLD snooping の概要

この節では，マルチキャスト，IGMP snooping および MLD snooping の概要について説明します。

31.1.1　マルチキャスト概要

同一の情報を複数の受信者に送信する場合，ユニキャストでは送信者が受信者の数だけデータを複製して送信するため，送信者とネットワークの負荷が高くなります。マルチキャストでは送信者がネットワーク内で選択されたグループに対してデータを送信します。送信者は受信者ごとにデータを複製する必要がないため，受信者の数に関係なくネットワークの負荷を軽減できます。マルチキャスト概要を次の図に示します。

図 31-1　マルチキャスト概要



マルチキャストで送信する場合に，宛先アドレスにはマルチキャストグループアドレスを使用します。マルチキャストグループアドレスを次の表に示します。

表 31-1　マルチキャストグループアドレス

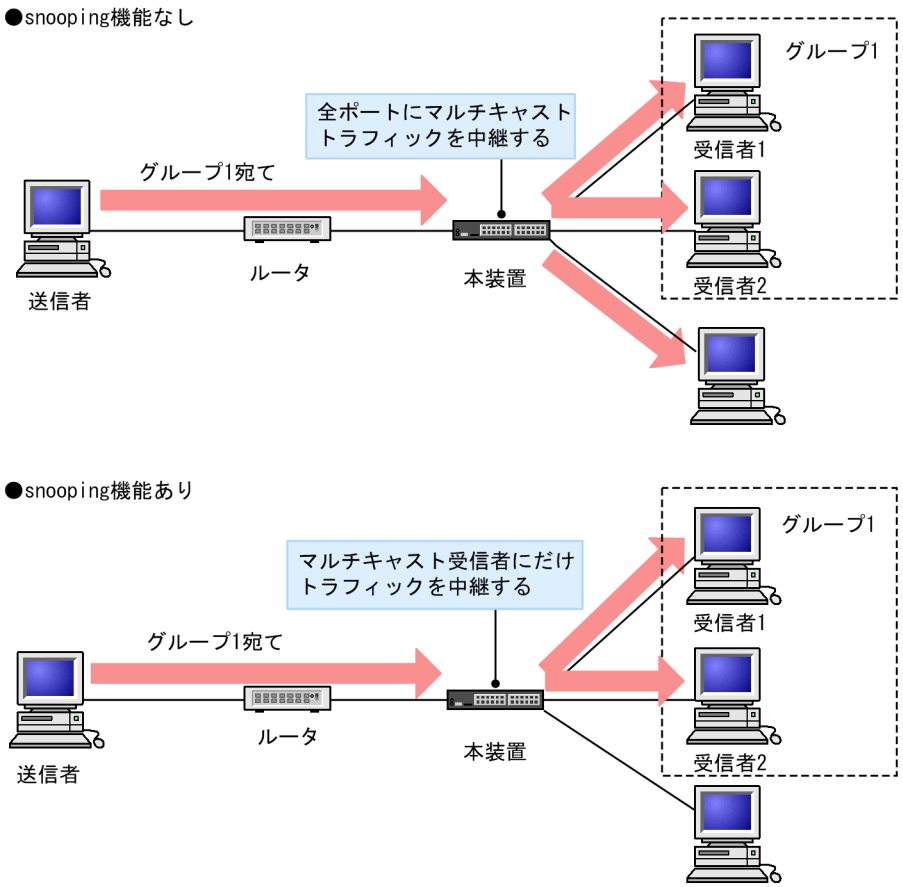
プロトコル	アドレス範囲
IPv4	224.0.0.0～239.255.255.255
IPv6	上位 8 ビットが ff(16 進数)となる IPv6 アドレス

31.1.2　IGMP snooping および MLD snooping 概要

レイヤ 2 スイッチはマルチキャストトラフィックを VLAN 内の全ポートに中継します。そのため，レイヤ 2 スイッチが接続されているネットワークでマルチキャストを使用すると，マルチキャストトラフィックの受信者がいないポートに不要なマルチキャストトラフィックが流れることになります。

IGMP snooping および MLD snooping は，IGMP あるいは MLD メッセージを監視して，受信者が接続しているポートに対してマルチキャストトラフィックを中継します。この機能を利用することで，不要なマルチキャストトラフィックの中継を抑止し，ネットワークを効率的に利用することができます。IGMP snooping/MLD snooping 概要を次の図に示します。

図 31-2　IGMP snooping/MLD snooping 概要



マルチキャストトラフィックの受信者が接続するポートを検出するため，本装置はグループ管理プロトコルのパケットを監視します。グループ管理プロトコルは，ルータホスト間でグループメンバーシップ情報を送受信するプロトコルで，IPv4 ネットワークでは IGMP が使用され，IPv6 ネットワークでは MLD が使用されます。ホストから送信されるグループ参加・離脱報告を示すパケットを検出することで，どの接続ポートへマルチキャストトラフィックを中継すべきかを学習します。

31.2　IGMP snooping/MLD snooping サポート機能

本装置がサポートする IGMP snooping/MLD snooping 機能を次の表に示します。

表 31-2　サポート機能

項 目		サポート内容	備考
インタフェース種別		全イーサネットをサポート フレーム形式は Ethernet V2 だけ	－
IGMP サポートバージョン MLD サポートバージョン		IGMP: Version 1，2，3 MLD: Version 1，2	－
この機能による学習 MAC アドレス範囲※1	IPv4	0100.5e00.0000 ～ 0100.5e7f.ffff	RFC1112 を参照
	IPv6	3333.0000.0000 ～ 3333.ffff.ffff	RFC2464 を参照
この機能による学習 IP アドレス範囲※2	IPv4	224.0.0.0～239.255.255.255	－
	IPv6	上位 8 ビットが ff（16 進数）となる IPv6 アドレス	－
IGMP クエリア MLD クエリア		クエリア動作は IGMPv2/IGMPv3，MLDv1/MLDv2 の仕様に従う	－
マルチキャストルータ接続ポートの設定		コンフィグレーションによる static 設定	－
IGMP 即時離脱機能		IGMPv2 Leave メッセージ，またはマルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージの受信による即時離脱	－

(凡例)　－：該当なし

注※1　IPv4/IPv6 マルチキャストを同時に使用しない場合

注※2　IPv4/IPv6 マルチキャストを同時に使用する場合

31.3　IGMP snooping

ここでは，IGMP snooping の機能と動作について説明します。本装置が送受信する IGMP メッセージのフォーマットおよびタイマは RFC2236 に従います。また，IGMP バージョン 3（以降，IGMPv3）メッセージのフォーマットおよび設定値は RFC3376 に従います。

IGMP snooping は IPv4 マルチキャストまたは IPv6 マルチキャストと同時に使用しない場合，MAC アドレス制御方式でマルチキャストトラフィックの中継制御を行います。IPv4 マルチキャストまたは IPv6 マルチキャストと同時にする場合は，IP アドレス制御方式でマルチキャストトラフィックの中継制御を行います。

31.3.1　MAC アドレス制御方式

(1)　MAC アドレスの学習

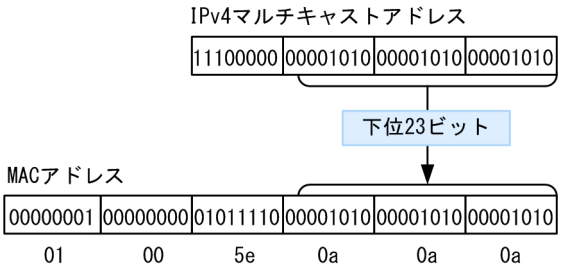
IGMP snooping が設定された VLAN で IGMP メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

(a)　エントリの登録

IGMPv1/IGMPv2 Report メッセージおよび，IGMPv3 Report（加入要求）メッセージを受信すると，メッセージに含まれるマルチキャストグループアドレスからマルチキャスト MAC アドレスを学習し，IGMPv1/IGMPv2/IGMPv3 Report メッセージを受信したポートにだけマルチキャストグループ宛てのトラフィックを転送するエントリを作成します。

IPv4 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 23 ビットを MAC アドレスにコピーして生成します。そのため，下位 23 ビットが同じ IP アドレスは MAC アドレスが重複します。例えば，224.10.10.10 と 225.10.10.10 はどちらもマルチキャスト MAC アドレスは 0100.5E0A.0A0A となります。これらのアドレスについては，レイヤ 2 中継で同一 MAC アドレス宛てのパケットとして取り扱います。IPv4 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 31-3　IPv4 マルチキャストアドレスと MAC アドレスの対応



(b)　エントリの削除

学習したマルチキャスト MAC アドレスは次のどちらかの場合に，すべてのポートにグループメンバーが存在しなくなった時点で削除されます。

- IGMPv2 Leave メッセージを受信した場合

  IGMPv2 Leave メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削

除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。

IGMP 即時離脱機能を使用している場合は，IGMPv2 Leave メッセージを受信すると，エントリから該当ポートをすぐに削除します。クエリアを設定していても，Group-Specific Query メッセージは送信しません。

- IGMPv3 Report（離脱要求）メッセージを受信した場合

  IGMPv3 Report（離脱要求）メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。ただし，マルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の IGMPv3 Report メッセージを受信した場合は，自装置へのクエリア設定を行っている場合だけ Group-Specific Query メッセージの送信および，エントリ削除処理を実行します。

  IGMP 即時離脱機能を使用している場合は，マルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージを受信すると，エントリから該当ポートをすぐに削除します。クエリアを設定していても，Group-Specific Query メッセージは送信しません。

- IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信してから一定時間経過した場合

  マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するため，定期的に Query メッセージを送信します。本装置はルータからの IGMP Query メッセージを受信した場合，VLAN 内の全ポートに中継します。IGMP Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。

  本装置では Group Membership Interval 時間，IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信しない場合，対応するエントリを削除します。

  注

  Group Membership Interval は，Robustness Variable（RV）×Query Interval（QI）＋ Query Response Interval（QRI）で算出します。

  RV，QI，QRI の値を次に示します。

  ・他装置が代表クエリアで IGMPv3 で運用している場合

  RV，QI=受信した Query メッセージから取得

  QRI=10 秒

  ・自装置が代表クエリアで IGMPv3 で運用している場合，または IGMPv2 で運用している場合

  RV=2

  QI=125 秒

  QRI=10 秒

(2) IPv4 マルチキャストパケットのレイヤ 2 中継

IPv4 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は MAC アドレスベースで処理します。IGMP snooping の結果によるレイヤ 2 中継は，同一 MAC アドレスにマッピングされる IP マルチキャストアドレスの IGMP Report（加入要求）メッセージを受信したポートすべてに中継します。

「(1) MAC アドレスの学習 (a) エントリの登録」の例で述べた 224.10.10.10 と 225.10.10.10 のマルチキャスト MAC アドレスはどちらも 0100.5E0A.0A0A となるので，224.10.10.10 宛てのマルチキャス

トデータをレイヤ 2 中継する際に，225.10.10.10 への IGMP Report（加入要求）メッセージを受信したポートへも中継します。

31.3.2　IP アドレス制御方式

本装置では swrt_multicast_table コマンドを設定することによって，IPv4 マルチキャストと IGMP snooping の両方を同一の VLAN 上で同時に使用できます。IPv4 マルチキャストと IGMP snooping を同時に使用する場合，該当する VLAN に必ず IPv4 マルチキャストを使用してください。

(1)　IP アドレスの学習

IGMP snooping が設定された VLAN で IGMP メッセージを受信することによってマルチキャスト IP アドレスをダイナミックに学習します。学習したマルチキャスト IP アドレスの情報は IPv4 マルチキャストのマルチキャスト中継エントリに設定します。

(a)　エントリの登録

IGMPv1/IGMPv2 Report メッセージおよび IGMPv3 Report（加入要求）メッセージを受信すると，メッセージに含まれるマルチキャストグループアドレスからマルチキャスト IP アドレスを学習し，IGMPv1/IGMPv2/IGMPv3 Report メッセージを受信したポートにだけマルチキャストグループ宛てのトラフィックを転送するエントリを作成します。

(b)　エントリの削除

学習したマルチキャスト IP アドレスは次のどれかの場合に，すべてのポートにグループメンバーが存在しなくなった時点で削除されます。

- IGMPv2 Leave メッセージを受信した場合

  IGMPv2 Leave メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，本装置が代表クエリアのときだけです）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。

  IGMP 即時離脱機能を使用している場合は，IGMPv2 Leave メッセージを受信すると，エントリから該当ポートをすぐに削除します。

- IGMPv3 Report（離脱要求）メッセージを受信した場合

  IGMPv3 Report（離脱要求）メッセージでマルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージを受信した場合，受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，本装置が代表クエリアのときだけです）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。マルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の IGMPv3 Report メッセージを受信した場合は，本装置から Group-and-Source-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-and-Source-Specific Query メッセージの送信は，本装置が代表クエリアのときだけです）。Group-Source-and-Specific Query メッセージの応答に関わらず，エントリはタイムアウトで削除処理を行います。

  IGMP 即時離脱機能を使用している場合は，マルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージを受信すると，エントリから該当ポートをすぐに削除します。

注

タイムアウト時間は，Group Membership Interval 時間とします。

- IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信してから一定時間経過した場合

  マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するため，定期的に Query メッセージを送信します。本装置はルータからの IGMP Query メッセージを受信した場合，VLAN 内の全ポートに中継します。IGMP Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。

  本装置では，Group Membership Interval 時間，IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信しない場合，対応するエントリを削除します。

  注

  Group Membership Interval は，Robustness Variable（RV）×Query Interval（QI）＋ Query Response Interval（QRI）で算出します。

  RV，QI，QRI の値を次に示します。

  ・他装置が代表クエリアで IGMPv3 で運用している場合

  RV，QI=受信した Query メッセージから取得

  QRI=10 秒

  ・自装置が代表クエリアで IGMPv3 で運用している場合，または IGMPv2 で運用している場合

  RV=2

  QI=125 秒

  QRI=10 秒

(2)　IPv4 マルチキャストパケットのレイヤ 2 中継

IPv4 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は IP アドレスベースで処理します。IGMP snooping の結果によるレイヤ 2 中継は，IGMP Report（加入要求）メッセージを受信したポートすべてに中継します。

(3)　IPv4 マルチキャストパケットのレイヤ 3 中継

IPv4 マルチキャストによる VLAN 間のレイヤ 3 中継時に，中継先の VLAN で IGMP snooping が動作している場合，レイヤ 3 中継されたマルチキャストトラフィックは，中継先の VLAN 内で IGMP snooping の学習結果に従って中継されます。

(4)　IPv4 マルチキャスト同時使用時の Specific Query 送信

IPv4 マルチキャストが動作することで本装置が VLAN 内の代表クエリアである場合，IGMP Leave メッセージまたは IGMPv3 Report（離脱要求）メッセージ受信による Group-Specific Query または Group-and-Source-Specific Query の送信は，受信ポートだけでなく VLAN 内の全ポートに送信します。

31.3.3　マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して IGMP snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また，IGMP はルータホスト間で送受信するプロトコルであるため，IGMP メッセージはルータおよびホストが受け取ります。本装置は IGMP メッセージを次の表に示すように中継します。

表 31-3　IGMPv1/IGMPv2 メッセージごとの動作

IGMP メッセージの種類	VLAN 内転送ポート	備考
Membership Query	全ポートへ中継します。	
Version 2 Membership Report	マルチキャストルータポートにだけ中継します。	
Leave Group	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。 ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※
Version 1 Membership Report	マルチキャストルータポートにだけ中継します。	

注※

自装置にクエリアを設定し，他装置が代表クエリアの場合の中継動作です。自装置が代表クエリアの場合は，IGMPv2 Leave メッセージは中継しません。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信していないポートで IGMPv2 Leave メッセージを受信した場合，クエリアの設定にかかわらず IGMPv2 Leave メッセージは中継しません。

表 31-4　IGMPv3 メッセージごとの動作

IGMPv3 メッセージの種類		VLAN 内転送ポート	備考
Version3 Membership Query		全ポートへ中継します。	
Version 3 Membership Report	加入要求の Report	マルチキャストルータポートにだけ中継します。	
	離脱要求の Report	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※

注※

自装置にクエリアを設定し，他装置が代表クエリアの場合の中継動作です。自装置が代表クエリアの場合は，IGMPv3 Report（離脱要求）メッセージは中継しません。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信していないポートで離脱要求の IGMPv3 Report メッセージを受信した場合，クエリアの設定にかかわらず IGMPv3 Report（離脱要求）メッセージは中継しません。

31.3.4　IGMP クエリア機能

IGMP クエリア機能は，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が IGMP Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に IGMP Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能によって，VLAN 内にマルチキャストルータが存在しない場合でも，IGMP snooping 機能を使用可能とします。本装置では IGMP Query メッセージを 125 秒間隔で送信します。

注

IGMPv2 で運用する場合，該当する VLAN では Query Interval を 125 秒で統一してください。

IGMP クエリア機能を利用するためには，IGMP snooping 機能を利用する VLAN に IP アドレスを設定する必要があります。

VLAN 内に IGMP Query メッセージを送信する装置が存在する場合，IGMP Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって IGMP Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は IGMP クエリア機能による Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると Query メッセージの送信を開始します。本装置では代表クエリアの監視時間は，Other Querier Present Interval に従います。

注

Other Querier Present Interval は，Robustness Variable（RV）×Query Interval（QI）＋ Query Response Interval（QRI）/2 で算出します。

RV，QI，QRI の値を次に示します。

- 他装置が代表クエリアで IGMPv3 で運用している場合
  RV，QI=受信した Query メッセージから取得
  QRI=10 秒
- 本装置が代表クエリアで IGMPv3 で運用している場合，または IGMPv2 で運用している場合
  RV=2
  QI=125 秒
  QRI=10 秒

本装置で送信する IGMP Query のバージョンは，IGMPv2 をデフォルト値としています。装置起動以降，IGMP Query のバージョンは，代表クエリアの IGMP バージョンに従います。

31.3.5　IGMP 即時離脱機能

IGMP 即時離脱機能は，IGMPv2 Leave および IGMPv3 Report（離脱要求）メッセージを受信した場合に，該当ポートへのマルチキャスト通信をすぐに停止する機能です。

IGMPv3 Report（離脱要求）メッセージでは，マルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージだけを，本機能のサポート対象とします。

31.3.6　マルチホームでの使用

(1)　代表クエリアの選定

マルチホームの VLAN で IGMP snooping を使用する場合，ネットワークごとに代表クエリアを選定します。マルチホームの VLAN で IGMP クエリア機能を有効にした場合，本装置が代表クエリアのネットワークに定期的に IGMP Query メッセージを送信します。

(2)　IGMP クエリア機能の有効化

マルチホームの VLAN で IGMPv2 Leave メッセージまたは IGMPv3 Report（離脱要求）メッセージを受信した場合，すべてのネットワークに対してグループメンバーの存在を確認できるように IGMP クエリア機能を有効にしてください。ただし，本装置が代表クエリアになる必要はありません。

(3)　エントリのタイムアウト時間

マルチホームの VLAN でエントリを登録する場合，エントリのタイムアウト時間は，該当 VLAN のネットワーク内で最長のタイムアウト時間になります。

注

タイムアウト時間は，Query Interval×Robustness Variable ＋ Query Response Interval（10 秒）で算出します。

Query Interval および Robustness Variable の値を次に示します。

- 他装置が代表クエリアで，IGMPv3 で運用している場合。
  Query Interval：IGMPv3 Query メッセージの QQIC フィールドの値
  Robustness Variable：IGMPv3 Query メッセージの QRV フィールドの値
- 自装置が代表クエリアで IGMPv3 で運用している場合，または IGMPv2 で運用している場合。
  Query Interval：125 秒
  Robustness Variable：2

31.4　MLD snooping

ここでは，MLD snooping の機能と動作について説明します。本装置が送受信する MLD メッセージのフォーマットおよび既定値は RFC2710 に従います。また，MLD バージョン 2（以降，MLDv2）メッセージのフォーマットおよび設定値は RFC3810 に従います。

MLD snooping は IPv6 マルチキャストと同時に使用しない場合，MAC アドレス制御方式でマルチキャストトラフィックの中継制御を行います。IPv6 マルチキャストと同時にする場合は，IP アドレス制御方式でマルチキャストトラフィックの中継制御を行います。

31.4.1　MAC アドレス制御方式

(1)　MAC アドレスの学習

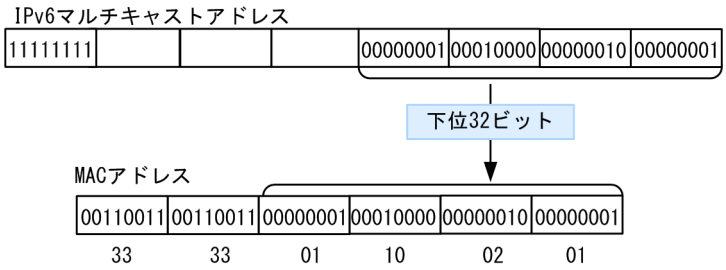
MLD snooping が設定された VLAN で MLD メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

(a)　エントリの登録

MLDv1 Report メッセージおよび，MLDv2 Report（加入要求）メッセージを受信すると，メッセージに含まれるマルチキャストグループアドレスからマルチキャスト MAC アドレスを学習し，MLDv1/MLDv2 Report メッセージを受信したポートにだけマルチキャストグループ宛てのトラフィックを転送するエントリを作成します。IPv6 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 32 ビットを MAC アドレスにコピーして生成します。

IPv6 マルチキャストアドレスはマルチキャストグループを識別するグループ ID フィールドが 112 ビット長のフォーマットと 32 ビット長のフォーマットの 2 種類が規定されています。グループ ID フィールドが 112 ビット長のアドレスフォーマットを使用する場合は，IPv4 マルチキャストアドレスと同様に MAC アドレスの重複が発生します。IPv6 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 31–4　IPv6 マルチキャストアドレスと MAC アドレスの対応



(b)　エントリの削除

学習したマルチキャスト MAC アドレスは次のどちらかの場合に，すべてのポートにグループメンバーが存在しなくなった時点で削除されます。

- MLDv1 Done メッセージを受信した場合

  MLDv1 Done メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削

除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。

- MLDv2 Report（離脱要求）メッセージを受信した場合

  MLDv2 Report（離脱要求）メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。ただし，マルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の MLDv2 Report メッセージを受信した場合は，自装置へのクエリア設定を行っている場合だけ Group-Specific Query メッセージの送信および，エントリ削除処理を実行します。

- MLDv1/MLDv2 Report（加入要求）メッセージを受信してから一定時間経過した場合

  マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するために，定期的に MLD Query メッセージを送信します。本装置はルータからの MLD Query メッセージを受信した場合，VLAN 内の全ポートに中継します。MLD Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。

  本装置では Multicast Listener Interval 時間，MLDv1/MLDv2 Report（加入要求）メッセージを受信しない場合，対応するエントリを削除します。

  注

  Multicast Listener Interval は，Robustness Variable（RV）×Query Interval（QI）＋ Query Response Interval（QRI）で算出します。

  RV，QI，QRI の値を次に示します。

  ・他装置が代表クエリアで MLDv2 で運用している場合

  RV，QI=受信した Query メッセージから取得

  QRI=10 秒

  ・本装置が代表クエリアで MLDv2 で運用している場合，または MLDv1 で運用している場合

  RV=2

  QI=125 秒

  QRI=10 秒

(2)　IPv6 マルチキャストパケットのレイヤ 2 中継

IPv6 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は IPv4 マルチキャストパケット同様に MAC アドレスベースで処理します。MLD snooping の結果によるレイヤ 2 中継は，同一 MAC アドレスにマッピングされる IPv6 マルチキャストアドレスの MLD Report（加入要求）メッセージを受信したポートすべてに中継します。

31.4.2　IP アドレス制御方式

本装置では swrt_multicast_table コマンドを設定することによって，IPv6 マルチキャストと MLD snooping の両方を同一の VLAN 上で同時に使用できます。IPv6 マルチキャストと MLD snooping を同時に使用する場合，該当する VLAN に必ず IPv6 マルチキャストを使用してください。

(1) IP アドレスの学習

MLD snooping が設定された VLAN で MLD メッセージを受信することによってマルチキャスト IP アドレスをダイナミックに学習します。学習したマルチキャスト IP アドレスの情報は IPv6 マルチキャストのマルチキャスト中継エントリに設定します。

(a) エントリの登録

MLDv1 Report メッセージおよび MLDv2 Report（加入要求）メッセージを受信すると，メッセージに含まれるマルチキャストグループアドレスからマルチキャスト IP アドレスを学習し，MLDv1/MLDv2 Report メッセージを受信したポートにだけマルチキャストグループ宛てのトラフィックを転送するエントリを作成します。

(b) エントリの削除

学習したマルチキャスト IP アドレスは次のどれかの場合に，すべてのポートにグループメンバーが存在しなくなった時点で削除されます。

- MLDv1 Done メッセージを受信した場合

  MLDv1 Done メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，本装置が代表クエリアのときだけです）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。

- MLDv2 Report（離脱要求）メッセージを受信した場合

  MLDv2 Report（離脱要求）メッセージでマルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の MLDv2 Report（離脱要求）メッセージを受信した場合，受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，本装置が代表クエリアのときだけです）。応答がない場合にエントリからこのポートだけを削除します。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。マルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の MLDv2 Report メッセージを受信した場合は，本装置から Group-and-Source-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-and-Source-Specific Query メッセージの送信は，本装置が代表クエリアの時だけです）。Group-and-Source-Specific Query メッセージの応答に関わらず，エントリはタイムアウトで削除処理を行います。

  注

  タイムアウト時間は，Multicast Listener Interval 時間とします。

- MLDv1/MLDv2 Report（加入要求）メッセージを受信してから一定時間経過した場合

  マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するために，定期的に MLD Query メッセージを送信します。本装置はルータからの MLD Query メッセージを受信した場合, VLAN 内の全ポートに中継します。MLD Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。

  本装置では Multicast Listener Interval 時間，MLDv1/MLDv2 Report（加入要求）メッセージを受信しない場合，対応するエントリを削除します。

  注

  Multicast Listener Interval は，Robustness Variable（RV）×Query Interval（QI）＋ Query Response Interval（QRI）で算出します。

  RV，QI，QRI の値を次に示します。

・他装置が代表クエリアで MLDv2 で運用している場合
RV，QI=受信した Query メッセージから取得
QRI=10 秒
・本装置が代表クエリアで MLDv2 で運用している場合，または MLDv1 で運用している場合
RV=2
QI=自装置に設定した Query Interval（コンフィグレーションコマンド ipv6 mld query-interval の設定値）。設定していなければ 125 秒。
QRI=10 秒

(2)　IPv6 マルチキャストパケットのレイヤ 2 中継

IPv6 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は IP アドレスベースで処理します。MLD snooping の結果によるレイヤ 2 中継は，MLD Report（加入要求）メッセージを受信したポートすべてに中継します。

(3)　IPv6 マルチキャストパケットのレイヤ 3 中継

IPv6 マルチキャストによる VLAN 間のレイヤ 3 中継時に，中継先の VLAN で MLD snooping が動作している場合，レイヤ 3 中継されたマルチキャストトラフィックは，中継先の VLAN 内で MLD snooping の学習結果に従って中継されます。

(4)　IPv6 マルチキャスト同時使用時の Specific Query 送信

IPv6 マルチキャストが動作することで本装置が VLAN 内の代表クエリアである場合，MLD Done メッセージまたは MLDv2 Report（離脱要求）メッセージ受信による Group-Specific Query または Group-and-Source-Specific Query の送信は，受信ポートだけでなく VLAN 内の全ポートに送信します。

31.4.3　マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して MLD snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また，MLD はルータホスト間で送受信するプロトコルであるため，MLD メッセージはルータおよびホストが受け取ります。本装置では MLD メッセージを次の表に示すように中継します。

表 31-5　MLDv1 メッセージごとの動作

MLDv1 メッセージの種類	VLAN 内転送ポート	備考
Multicast Listener Query	全ポートへ中継します。	
Multicast Listener Report	マルチキャストルータポートにだけ中継します。	
Multicast Listener Done	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。 ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※

注※

自装置にクエリアを設定し，他装置が代表クエリアの場合の中継動作です。自装置が代表クエリアの場合は，MLDv1 Done メッセージは中継しません。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，MLDv1/MLDv2 Report（加入要求）メッセージを受信していないポートで MLDv1 Done メッセージを受信した場合，クエリアの設定にかかわらず MLDv1 Done メッセージは中継しません。

表 31-6　MLDv2 メッセージごとの動作

MLDv2 メッセージの種類		VLAN 内転送ポート	備考
Version2 Multicast Listener Query		全ポートへ中継します。	
Version2 Multicast Listener Report	加入要求の Report	マルチキャストルータポートにだけ中継します。	
	離脱要求の Report	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※

注※

自装置にクエリアを設定し，他装置が代表クエリアの場合の中継動作です。自装置が代表クエリアの場合は，MLDv2 Report（離脱要求）メッセージは中継しません。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，MLDv1/MLDv2 Report（加入要求）メッセージを受信していないポートで離脱要求の MLDv2 Report メッセージを受信した場合，クエリアの設定にかかわらず MLDv2 Report（離脱要求）メッセージは中継しません。

31.4.4　MLD クエリア機能

MLD クエリア機能とは，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が MLD Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に MLD Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能によって，VLAN 内にマルチキャストルータが存在しない場合でも，MLD snooping 機能を使用可能とします。本装置では Query メッセージを 125 秒間隔で送信します。

注

MLDv1 で運用する場合，該当する VLAN では Query Interval を統一してください。

MLD クエリア機能を利用するためには，MLD snooping 機能を利用する VLAN に IP アドレスを設定する必要があります。

VLAN 内に MLD Query メッセージを送信する装置が存在する場合，MLD Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって MLD Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は MLD クエリア機能による MLD Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると MLD Query メッセージの送信を開始します。本装置では代表クエリアの監視時間は Other Querier Present Interval に従います。

注

Other Querier Present Interval は，Robustness Variable（RV）×Query Interval（QI）＋ Query Response Interval（QRI）/2 で算出します。

RV，QI，QRI の値を次に示します。

- 他装置が代表クエリアで MLDv2 で運用している場合

  RV，QI=受信した Query メッセージから取得

  QRI=10 秒

- 本装置が代表クエリアで MLDv2 で運用している場合，または MLDv1 で運用している場合

  RV=2

  QI=自装置に設定した Query Interval（IP アドレス制御方式の場合，コンフィグレーションコマンド ipv6 mld query-interval の設定値）。設定していなければ 125 秒。

  QRI=10 秒

本装置で送信する MLD Query のバージョンは，MLDv1 をデフォルト値としています。装置起動以降，MLD Query のバージョンは，代表クエリアの MLD バージョンに従います。

31.5　IGMP snooping/MLD snooping 使用時の注意事項

(1)　他機能との共存

「22.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　制御パケットのフラッディング

IGMP snooping/MLD snooping が抑止対象とするマルチキャストトラフィックはデータトラフィックであり，ルーティングプロトコルなどの制御パケットは VLAN 内の全ルータや全ホストが受信できるように VLAN 内に flooding する必要があります。そのため，本装置では，次の表に示すアドレス範囲に含まれる宛先 IP アドレスを持つパケットは，VLAN 内の全ポートに中継します。次の表に示すアドレス範囲外の宛先 IP アドレスを持つパケットは，IGMP snooping/MLD snooping の学習結果に従って中継します。

表 31-7　制御パケットのフラッディング

プロトコル	アドレス範囲
IGMP snooping	224.0.0.0/24
MLD snooping	ff02::/16

ただし，制御パケットのマルチキャスト MAC アドレスと重複するマルチキャストグループアドレスは使用できません。上の表に示したアドレス範囲以外のアドレスで，使用できないマルチキャストグループアドレスを次の表に示します。

表 31-8　MAC アドレス制御方式で使用できないマルチキャストグループアドレス

プロトコル	マルチキャストグループアドレス
IGMP snooping	224.128.0.0/24
	225.0.0.0/24
	225.128.0.0/24
	226.0.0.0/24
	226.128.0.0/24
	227.0.0.0/24
	227.128.0.0/24
	228.0.0.0/24
	228.128.0.0/24
	229.0.0.0/24
	229.128.0.0/24
	230.0.0.0/24
	230.128.0.0/24
	231.0.0.0/24

プロトコル	マルチキャストグループアドレス
	231.128.0.0/24
	232.0.0.0/24
	232.128.0.0/24
	233.0.0.0/24
	233.128.0.0/24
	234.0.0.0/24
	234.128.0.0/24
	235.0.0.0/24
	235.128.0.0/24
	236.0.0.0/24
	236.128.0.0/24
	237.0.0.0/24
	237.128.0.0/24
	238.0.0.0/24
	238.128.0.0/24
	239.0.0.0/24
	239.128.0.0/24

上の表に示したアドレスをマルチキャストグループアドレスに使用した場合，該当マルチキャストグループアドレス宛てのマルチキャストデータは，VLAN 内の全ポートに中継します。

トランクポートを設定している場合は，Untagged 制御パケットを受信しないように注意してください。構成上，トランクポートで Untagged 制御パケットを扱う場合は，ネイティブ VLAN を設定してください。

(3)　マルチキャストルータポートの設定

(a)　冗長構成時

スパニングツリーによって冗長構成を採り，スパニングツリーによってトポロジー変更でルータとの接続が変わる可能性がある場合は，ルータと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

(b)　レイヤ 2 スイッチ間の接続時

複数のレイヤ 2 スイッチだけで構成される VLAN で，マルチキャストトラフィックの送信ホストを収容するレイヤ 2 スイッチと接続するポートをマルチキャストルータポートに設定しておく必要があります。

冗長構成を採る場合は，送信ホストを収容するレイヤ 2 スイッチと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

(4) IGMP バージョン 3 ホストとの接続

本装置に IGMPv3 ホストを接続する場合，次のどちらかの対応が必要です。

- 該当する VLAN に IPv4 マルチキャストを使用して，IGMP バージョンを 3 に設定してください。
- IGMPv3 ルータを接続して該当するルータが代表クエリアになるように IP アドレスを設定してください。

また，IGMPv3 ホストからの IGMPv3 メッセージがフラグメント化されない構成で運用してください。

(5) MLD バージョン 2 ホストとの接続

本装置に MLDv2 ホストを接続する場合，次のどちらかの対応が必要です。

- 該当する VLAN に IPv6 マルチキャストを使用して，MLD バージョンを 2 に設定してください。
- MLDv2 ルータを接続して該当するルータが代表クエリアになるように IP アドレスを設定してください。

また，MLDv2 ホストからの MLDv2 メッセージがフラグメント化されない構成で運用してください。

(6) 運用コマンド実行によるエントリの再学習

IGMP/MLD snooping の運用コマンドのほかに，下記のコマンドを実行した場合，それまでに学習したエントリをクリアし，再学習を行います。運用コマンド実行後は，一時的にマルチキャスト通信が中断します。

- copy コマンドで running-config に上書きした場合
- restart vlan コマンド

(7) IPv4 マルチキャスト機能との同時使用

(a) コンフィグレーションコマンド swrt_multicast_table の設定

IPv4 マルチキャスト機能と IGMP snooping を同時に使用する場合，コンフィグレーションコマンド swrt_multicast_table を設定して，該当する VLAN に IPv4 マルチキャストを使用してください。

(b) IGMP snooping 設定追加時の一時的通信停止

IPv4 マルチキャストを使用している VLAN に IGMP snooping を追加設定した場合，一時的にマルチキャスト通信が停止します。IGMP snooping 設定後，IGMP Report（加入要求）を受信することでマルチキャスト通信が再開します。

(c) 静的グループ参加機能との併用

IPv4 マルチキャストの静的グループ参加機能を使用している VLAN では，ホストから IGMP Report（加入要求）が送信されないおそれがあります。IGMP snooping と同時使用する場合，IGMP Report（加入要求）が送信されないとマルチキャスト通信ができないため，静的グループ参加機能を使用している VLAN でマルチキャスト通信が必要なポートにはマルチキャストルータポートを設定してください。

(d) IPv4 マルチキャストパケットのフラッディング

IPv4 マルチキャストと IGMP snooping を同時に使用している VLAN で，次に示す IPv4 マルチキャストパケットは，受信した VLAN 内の全ポートに中継されます。

- IPv4 マルチキャストがマルチキャスト中継エントリ（ネガティブキャッシュも含む）を登録するまでに受信した IPv4 マルチキャストパケット
- TTL が 1 の IPv4 マルチキャストパケット

(e)　上流インタフェース以外で受信した IPv4 マルチキャストパケットのフラッディング

IPv4 マルチキャストと IGMP snooping を同時に使用してマルチキャスト中継をしている場合，登録したマルチキャスト中継エントリの上流インタフェース以外の VLAN で IPv4 マルチキャストパケットを受信すると，該当する IPv4 マルチキャストパケットは受信した VLAN 内の全ポートに中継されます。

(8)　IPv6 マルチキャスト機能との同時使用

(a)　コンフィグレーションコマンド swrt_multicast_table の設定

IPv6 マルチキャスト機能と MLD snooping を同時に使用する場合，コンフィグレーションコマンド swrt_multicast_table を設定して，該当する VLAN に IPv6 マルチキャストを使用してください。

(b)　MLD snooping 設定追加時の一時的通信停止

IPv6 マルチキャストを使用している VLAN に MLD snooping を追加設定した場合，一時的にマルチキャスト通信が停止します。MLD snooping 設定後，MLD Report（加入要求）を受信することでマルチキャスト通信が再開します。

(c)　静的グループ参加機能との併用

IPv6 マルチキャストの静的グループ参加機能を使用している VLAN では，ホストから MLD Report（加入要求）が送信されないおそれがあります。MLD snooping と同時使用する場合，MLD Report（加入要求）が送信されないとマルチキャスト通信ができないため，静的グループ参加機能を使用している VLAN でマルチキャスト通信が必要なポートにはマルチキャストルータポートを設定してください。

(d)　IPv6 マルチキャストパケットのフラッディング

IPv6 マルチキャストと MLD snooping を同時に使用している VLAN で，次に示す IPv6 マルチキャストパケットは，受信した VLAN 内の全ポートに中継されます。

- IPv6 マルチキャストがマルチキャスト中継エントリ（ネガティブキャッシュも含む）を登録するまでに受信した IPv6 マルチキャストパケット
- ホップリミットが 1 の IPv6 マルチキャストパケット

(e)　上流インタフェース以外で受信した IPv6 マルチキャストパケットのフラッディング

IPv6 マルチキャストと MLD snooping を同時に使用してマルチキャスト中継をしている場合，登録したマルチキャスト中継エントリの上流インタフェース以外の VLAN で IPv6 マルチキャストパケットを受信すると，該当する IPv6 マルチキャストパケットは受信した VLAN 内の全ポートに中継されます。

(9)　IGMP 即時離脱機能

IGMP 即時離脱機能を使用した場合，IGMPv2 Leave および IGMPv3 Report（離脱要求）メッセージを受信すると，該当ポートへのマルチキャスト通信をすぐに停止します。このため，本機能を使用する場合は，接続ポートに各マルチキャストグループの受信者の端末を 1 台だけ設置することを推奨します。

接続ポートに同一マルチキャストグループの受信者の端末を複数台設置した場合は，一時的にほかの受信者へのマルチキャスト通信が停止します。この場合，受信者からの IGMP Report（加入要求）メッセージを再度受信することで，マルチキャスト通信は再開します。

(10) スタックでの IGMP snooping の使用

スタックで IGMP snooping を使用する場合，IP アドレス制御方式を使用する必要があります。そのため，コンフィグレーションコマンド swrt_multicast_table を設定し，該当する VLAN に IPv4 マルチキャストを使用してください。

32 IGMP snooping/MLD snooping の設定と運用

IGMP snooping/MLD snooping はレイヤ 2 で VLAN 内のマルチキャストトラフィックを制御する機能です。この章では，IGMP snooping/MLD snooping の設定と運用方法について説明します。

32.1　IGMP snooping のコンフィグレーション

32.1.1　コンフィグレーションコマンド一覧

IGMP snooping のコンフィグレーションコマンド一覧を次の表に示します。

表 32-1　コンフィグレーションコマンド一覧

コマンド名	説明
ip igmp snooping (global)	no ip igmp snooping で，本装置の IGMP snooping 機能を抑止します。
ip igmp snooping (interface)	指定したインタフェースの IGMP snooping 機能を設定します。
ip igmp snooping fast-leave	IGMP 即時離脱機能を設定します。
ip igmp snooping mrouter interface	IGMP マルチキャストルータポートを設定します。
ip igmp snooping querier	IGMP クエリア機能を設定します。

32.1.2　IGMP snooping の設定

[設定のポイント]

IGMP snooping を動作させるには，使用する VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。

VLAN2 に IGMP snooping 機能を有効にする場合を示します。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ip igmp snooping
   VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，IGMP snooping 機能を有効にします。

32.1.3　IGMP クエリア機能の設定

[設定のポイント]

IGMP snooping を設定した VLAN 内にマルチキャストルータが存在しない場合，IGMP クエリア機能を動作させる必要があります。該当 VLAN の VLAN インタフェースコンフィグレーションモードで次の設定を行います。

[コマンドによる設定]

1. **(config-if)# ip igmp snooping querier**
   IGMP クエリア機能を有効にします。

[注意事項]

本設定は該当インタフェースに IPv4 アドレスの設定がないと有効になりません。

32.1.4　マルチキャストルータポートの設定

[設定のポイント]

IGMP snooping を設定した VLAN 内にマルチキャストルータを接続している場合，該当 VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。例として，該当 VLAN 内のポート 1/0/1 のギガビット・イーサネットインタフェースにマルチキャストルータを接続している場合を示します。

[コマンドによる設定]

1. **(config-if)# ip igmp snooping mrouter interface gigabitethernet 1/0/1**
   該当インタフェースで，マルチキャストルータポートを指定します。

32.1.5　スタックでの IGMP snooping の設定

[設定のポイント]

スタックで IGMP snooping を使用する場合, IPv4 マルチキャストと同時使用するための設定と, IPv4 マルチキャストを動作させるための設定をします。IPv4 マルチキャストを動作させるためには，ip pim sparse-mode コマンドを使用して，一つ以上のインタフェースで IPv4 PIM の設定をします。また，ip pim sparse-mode コマンドまたは ip igmp router コマンドのどちらかを使用して，IGMP snooping を使用する VLAN で IGMP を使用する設定をします。

例として，VLAN2 に IPv4 PIM を使用し，VLAN3 で IGMP snooping を有効にする設定を示します。あらかじめ，スタックを動作させる設定をしてください。

[コマンドによる設定]

1. **(config)# swrt_multicast_table**
   IPv4 マルチキャストと IGMP snooping を同時に使用する設定をします。
2. **(config)# ip multicast-routing**
   IPv4 マルチキャストを使用できるようにします。
3. **(config)# interface vlan 2**
   (config-if)# ip address 172.16.1.100 255.255.255.0
   VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，IPv4 アドレスを設定します。
4. **(config-if)# ip pim sparse-mode**
   VLAN2 で IPv4 PIM を使用する設定をします。
5. **(config-if)# interface vlan 3**
   (config-if)# ip address 172.16.2.100 255.255.255.0
   VLAN3 の VLAN インタフェースコンフィグレーションモードに移行して，IPv4 アドレスを設定します。
6. **(config-if)# ip igmp router**
   VLAN3 で IGMP を使用する設定をします。
7. **(config-if)# ip igmp snooping**
   VLAN3 で IGMP snooping を有効にする設定をします。

32.2　IGMP snooping のオペレーション

32.2.1　運用コマンド一覧

IGMP snooping の運用コマンド一覧を次の表に示します。

表 32-2　運用コマンド一覧

コマンド名	説明
show igmp-snooping	IGMP snooping 情報を表示します。
clear igmp-snooping	IGMP snooping 情報をクリアします。
restart snooping	snooping プログラムを再起動します。
dump protocols snooping	イベントトレース情報および制御テーブル情報のファイルを出力します。

32.2.2　IGMP snooping の確認

IGMP snooping 機能を使用した場合の IGMP snooping に関する確認内容には次のものがあります。

(1)　コンフィグレーション設定後の確認

show igmp-snooping コマンドを実行し，IGMP snooping に関する設定が正しいことを確認してください。

図 32-1　IGMP snooping の設定状態表示

```
> show igmp-snooping 100
Date 20XX/10/01 15:20:00 UTC
VLAN: 100
  IP address: 192.168.11.20/24    Querier: enable
  IGMP querying system: 192.168.11.20
  Querier version: V2
  IPv4 Multicast routing: Off
  Fast-leave: On
  Port(5): 1/0/1-5
  Mrouter-port: 1/0/1,3
  Group Counts: 3
```

(2)　運用中の確認

次のコマンドで，IGMP snooping の運用中の状態を確認してください。

- 学習した MAC アドレス，VLAN 内に中継される IPv4 マルチキャストアドレスとその中継先ポートリストの状態は，show igmp-snooping group コマンドで確認してください。

  図 32-2　show igmp-snooping group コマンドの実行結果

  ```
  > show igmp-snooping group 100
  Date 20XX/02/01 15:20:00 UTC
  VLAN counts: 1
  VLAN: 100  Group counts: 3  IPv4 Multicast routing: Off
    Group Address      MAC Address          Version          Mode
    224.10.10.10       0100.5e0a.0a0a       V2               -
      Port-list:1/0/1-3
    225.10.10.10       0100.5e0a.0a0a       V3               INCLUDE
      Port-list:1/0/1-2
    239.192.1.1        0100.5e40.0101       V2,V3            EXCLUDE
      Port-list:1/0/1
  ```

- ポートごとの参加グループ表示例を show igmp-snooping port コマンドで確認してください。

図 32-3　show igmp-snooping port コマンドの実行結果

```
> show igmp-snooping port 1/0/1
Date 20XX/10/01 15:20:00 UTC
Port 1/0/1  VLAN counts: 2
  VLAN: 100  Group counts: 2
    Group Address     Last Reporter      Uptime     Expires
    224.10.10.10      192.168.1.3        00:10      04:10
    239.192.1.1       192.168.1.3        02:10      03:00
  VLAN: 150  Group counts: 1
    Group Address     Last Reporter      Uptime     Expires
    239.10.120.1      192.168.15.10      01:10      02:30
```

32.3　MLD snooping のコンフィグレーション

32.3.1　コンフィグレーションコマンド一覧

MLD snooping のコンフィグレーションコマンド一覧を次の表に示します。

表 32-3　コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 mld snooping	MLD snooping 機能を使用することを設定します。
ipv6 mld snooping mrouter interface	MLD マルチキャストルータポートを設定します。
ipv6 mld snooping querier	MLD クエリア機能を設定します。
no ipv6 mld snooping	MLD snooping 機能の抑止を設定します。

32.3.2　MLD snooping の設定

[設定のポイント]

MLD snooping を動作させるには，使用する VLAN の VLAN インタフェースのインタフェースコンフィグレーションモードで，次の設定を行います。例として，VLAN2 に MLD snooping 機能を有効にする場合を示します。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ipv6 mld snooping
   VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，MLD snooping 機能を有効にします。

32.3.3　MLD クエリア機能の設定

[設定のポイント]

MLD snooping を設定した VLAN 内にマルチキャストルータが存在しない場合，MLD クエリア機能を動作させる必要があります。該当 VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。

[コマンドによる設定]

1. **(config-if)# ipv6 mld snooping querier**
   MLD クエリア機能を有効にします。

[注意事項]

本設定は該当インタフェースに IPv6 アドレスの設定がないと有効となりません。

32.3.4　マルチキャストルータポートの設定

[設定のポイント]

MLD snooping を設定した VLAN 内にマルチキャストルータを接続している場合，該当 VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。例として，該当 VLAN 内のポート 1/0/1 のギガビット・イーサネットインタフェースにマルチキャストルータを接続している場合を示します。

[コマンドによる設定]

1. **(config-if)# ipv6 mld snooping mrouter interface gigabitethernet 1/0/1**
   該当インタフェースでマルチキャストルータポートを指定します。

32.4　MLD snooping のオペレーション

32.4.1　運用コマンド一覧

MLD snooping の運用コマンド一覧を次の表に示します。

表 32-4　運用コマンド一覧

コマンド名	説明
show mld-snooping	MLD snooping 情報を表示します。
clear mld-snooping	MLD snooping 情報をクリアします。
restart snooping	snooping プログラムを再起動します。
dump protocols snooping	イベントトレース情報および制御テーブル情報のファイルを出力します。

32.4.2　MLD snooping の確認

MLD snooping 機能を使用した場合の MLD snooping に関する確認内容には次のものがあります。

(1)　コンフィグレーション設定後

show mld-snooping コマンドを実行し，MLD snooping に関する設定が正しいことを確認してください。

図 32-4　MLD snooping の設定状態表示

```
> show mld-snooping 100
Date 20XX/02/01 15:20:00 UTC
VLAN: 100
  IP address: fe80::b1    Querier: enable
  MLD querying system: fe80::b1
  Querier version: V1
  IPv6 Multicast routing: Off
  Querier version: V2
  Port(5): 0/1-5
  Mrouter-port: 0/1,3
  Group Counts: 3
```

(2)　運用中の確認

以下のコマンドで，MLD snooping の運用中の状態を確認してください。

- 学習した MAC アドレス，VLAN 内に中継される IPv6 マルチキャストアドレスとその中継先ポートリストの状態は，show mld-snooping group コマンドで確認してください。

  図 32-5　show mld-snooping group コマンドの実行結果

  ```
  > show mld-snooping group 100
  Date 20XX/02/01 15:20:00 UTC
  VLAN: counts: 1
  VLAN: 100  Group counts: 2  IPv6 Multicast routing: Off
    Group Address     MAC Address          Version      Mode
    ff35::1           3333:0000:0001       V1,V2        EXCLUDE
      Port-list:0/1-3
    ff35::2           3333:0000:0002       V2           EXCLUDE
      Port-list:0/1-2
  ```

- ポートごとの参加グループ表示例を show mld-snooping port コマンドで確認してください。

図 32-6　show mld-snooping port コマンドの実行結果

```
> show mld-snooping port 0/1
Date 20XX/12/01 15:20:00 UTC
Port   0/1   VLAN counts: 1
  VLAN: 100   Group counts: 2
    Group Address       Last Reporter       Uptime     Expires
    ff35::1             fe80::b2            00:10      04:10
    ff35::2             fe80::b3            02:10      03:00
```

付録

付録 A　準拠規格

付録 A.1　TELNET/FTP

表 A–1　TELNET/FTP の準拠する規格および勧告

規格番号(発行年月)	規格名
RFC854(1983 年 5 月)	TELNET PROTOCOL SPECIFICATION
RFC855(1983 年 5 月)	TELNET OPTION SPECIFICATIONS
RFC959(1985 年 10 月)	FILE TRANSFER PROTOCOL (FTP)

付録 A.2　RADIUS/TACACS+

表 A–2　RADIUS/TACACS+の準拠する規格および勧告

規格番号(発行年月)	規格名
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service(RADIUS)
RFC2866(2000 年 6 月)	RADIUS Accounting
RFC3162(2001 年 8 月)	RADIUS and IPv6
draft-grant-tacacs-02 (1997 年 1 月)	The TACACS+ Protocol Version 1.78

付録 A.3　SSH

表 A–3　SSH の準拠する規格および勧告

規格番号(発行年月)	規格名
RFC4251(2006 年 1 月)	The Secure Shell (SSH) Protocol Architecture
RFC4252(2006 年 1 月)	The Secure Shell (SSH) Authentication Protocol
RFC4253(2006 年 1 月)	The Secure Shell (SSH) Transport Layer Protocol
RFC4254(2006 年 1 月)	The Secure Shell (SSH) Connection Protocol
RFC4344(2006 年 1 月)	The Secure Shell (SSH) Transport Layer Encryption Modes
RFC4419(2006 年 3 月)	Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
RFC4716(2006 年 11 月)	The Secure Shell (SSH) Public Key File Format
RFC5656(2009 年 12 月)	Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer
RFC6668(2012 年 7 月)	SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol
RFC8268(2017 年 12 月)	More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH)

規格番号(発行年月)	規格名
draft-ylonen-ssh-protocol-00 (1995 年 11 月)	The SSH (Secure Shell) Remote Login Protocol
draft-ietf-secsh-filexfer-01 (2001 年 3 月)	SSH File Transfer Protocol

付録 A.4　NTP

表 A–4　NTP の準拠する規格および勧告

規格番号(発行年月)	規格名
RFC1305(1992 年 3 月)	Network Time Protocol (Version 3) Specification, Implementation and Analysis

付録 A.5　DNS

表 A–5　DNS リゾルバの準拠する規格および勧告

規格番号(発行年月)	規格名
RFC1034(1987 年 3 月)	Domain names - concepts and facilities
RFC1035(1987 年 3 月)	Domain names - implementation and specification

付録 A.6　SYSLOG

表 A–6　SYSLOG の準拠する規格および勧告

規格番号(発行年月)	規格名
RFC3164(2001 年 8 月)	The BSD syslog Protocol

付録 A.7　SNMP

表 A–7　SNMP の準拠規格および勧告

規格番号(発行年月)	規格名
RFC1155(1990 年 5 月)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC1157(1990 年 5 月)	A Simple Network Management Protocol (SNMP)
RFC1901(1996 年 1 月)	Introduction to Community-based SNMPv2
RFC1902(1996 年 1 月)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1903(1996 年 1 月)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)

規格番号(発行年月)	規格名
RFC1904(1996 年 1 月)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1905(1996 年 1 月)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1906(1996 年 1 月)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1907(1996 年 1 月)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1908(1996 年 1 月)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC2578(1999 年 4 月)	Structure of Management Information Version 2 (SMIv2)
RFC2579(1999 年 4 月)	Textual Conventions for SMIv2
RFC2580(1999 年 4 月)	Conformance Statements for SMIv2
RFC3410(2002 年 12 月)	Introduction and Applicability Statements for Internet Standard Management Framework
RFC3411(2002 年 12 月)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC3412(2002 年 12 月)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC3413(2002 年 12 月)	Simple Network Management Protocol (SNMP) Applications
RFC3414(2002 年 12 月)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC3415(2002 年 12 月)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC3416(2002 年 12 月)	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC3417(2002 年 12 月)	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC3584(2003 年 8 月)	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC3826(2004 年 6 月)	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
RFC7860(2016 年 4 月)	HMAC-SHA-2 Authentication Protocols in User-Based Security Model (USM) for SNMPv3

表 A-8　MIB の準拠規格および勧告

規格番号(発行年月)	規格名
IEEE8023-LAG-MIB(2000 年 3 月)	Aggregation of Multiple Link Segments

規格番号(発行年月)	規格名
IEEE8021-PAE-MIB(2001 年 6 月)	Port-Based Network Access Control
IEEE8021-CFM-MIB(2007 年 12 月)	Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management
LLDP-V2-MIB(2009 年 6 月)	Management Information Base module for LLDP configuration, statistics, local system data and remote systems data components.
RFC1158(1990 年 5 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1213(1991 年 3 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1354(1992 年 7 月)	IP Forwarding Table MIB
RFC1493(1993 年 6 月)	Definitions of Managed Objects for Bridges
RFC1643(1994 年 7 月)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1657(1994 年 7 月)	Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2
RFC1757(1995 年 2 月)	Remote Network Monitoring Management Information Base
RFC1850(1995 年 11 月)	OSPF Version2 Management Information Base
RFC2233(1997 年 11 月)	The Interfaces Group MIB using SMIv2
RFC2452(1998 年 12 月)	IP Version 6 Management Information Base for the Transmission Control Protocol
RFC2454(1998 年 12 月)	IP Version 6 Management Information Base for the User Datagram Protocol
RFC2465(1998 年 12 月)	Management Information Base for IP Version 6: Textual Conventions and General Group
RFC2466(1998 年 12 月)	Management Information Base for IP Version 6: ICMPv6 Group
RFC2674(1999 年 8 月)	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
RFC2787(2000 年 3 月)	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC2934(2000 年 10 月)	Protocol Independent Multicast MIB for IPv4
RFC3411(2002 年 12 月)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC3412(2002 年 12 月)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC3413(2002 年 12 月)	Simple Network Management Protocol (SNMP) Applications
RFC3414(2002 年 12 月)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

規格番号(発行年月)	規格名
RFC3415(2002 年 12 月)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC3418(2002 年 12 月)	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC3621(2003 年 12 月)	Power Ethernet MIB
draft-ietf-ospf-ospfv3-mib-03 (2000 年 11 月)	Management Information Base for OSPFv3
draft-ietf-vrrp-unified-mib-04 (2005 年 9 月)	Definitions of Managed Objects for the VRRP over IPv4 and IPv6

付録 A.8　イーサネット

表 A-9　イーサネットインタフェースの準拠規格

種別	規格	名称
10BASE-T, 100BASE-TX, 1000BASE-T, 1000BASE-X, 10GBASE-R, 40GBASE-R, 100GBASE-R	IEEE802.3x-1997	IEEE Standards for Local and Metropolitan Area Networks:Specification for 802.3 Full Duplex Operation
	IEEE802.2 1998 Edition	IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 2: Logical Link Control
	IEEE802.3 2000 Edition	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer Specifications
1000BASE-X	IEEE802.3ah 2004	Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks
	IEEE802.3z 1998	Media Access Control Parameters, Physical Layers, Repeater and Management Parameters for 1,000 Mb/s Operation, Supplement to Information Technology
10GBASE-T	IEEE802.3 2012 Edition	IEEE Standard for Ethernet
	IEEE802.2 1998 Edition	IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 2: Logical Link Control
10GBASE-R	IEEE802.3ae Standard-2002	Media Access Control(MAC) Parameters, Physical Layer, and Management Parameters for 10 Gb/s Operation
	IEEE802.3aq Standard-2006	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

種別	規格	名称
40GBASE-R	IEEE802.3ba Standard-2010	Media Access Control Parameters, Physical Layers, and Management Parameters for 40 Gb/s and 100 Gb/s Operation
100GBASE-R	IEEE802.3bm Standard-2015	Physical Layer Specifications and Management Parameters for 40 Gb/s and 100 Gb/s Operation over Fiber Optic Cables

表 A–10　Sync-E の準拠規格

規格	名称
ITU-T G.8261(08/2013)	Timing and synchronization aspects in packet networks
ITU-T G.8262(01/2015)	Timing characteristics of a synchronous Ethernet equipment slave clock

付録 A.9　リンクアグリゲーション

表 A–11　リンクアグリゲーションの準拠規格

規格	名称
IEEE802.1AX (IEEE Std 802.1AX-2008)	Aggregation of Multiple Link Segments

付録 A.10　VLAN

表 A–12　VLAN の準拠規格および勧告

規格	名称
IEEE802.1Q (IEEE Std 802.1Q-2003)	Virtual Bridged Local Area Networks※

注※　GVRP/GMRP はサポートしていません。

付録 A.11　VXLAN

表 A–13　VXLAN の準拠規格および勧告

規格	名称
RFC7348(2014 年 8 月)	Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks

付録 A.12　スパニングツリー

表 A–14　スパニングツリーの準拠規格および勧告

規格	名称
IEEE802.1D	Media Access Control (MAC) Bridges

規格	名称
(ANSI/IEEE Std 802.1D-1998 Edition)	(The Spanning Tree Algorithm and Protocol)
IEEE802.1t (IEEE Std 802.1t-2001)	Media Access Control (MAC) Bridges - Amendment 1
IEEE802.1w (IEEE Std 802.1w-2001)	Media Access Control (MAC) Bridges - Amendment 2: Rapid Reconfiguration
IEEE802.1s (IEEE Std 802.1s-2002)	Virtual Bridged Local Area Networks - Amendment 3: Multiple Spanning Trees

付録 A.13　IGMP snooping/MLD snooping

表 A–15　IGMP snooping/MLD snooping の準拠規格および勧告

規格番号(発行年月)	規格名
RFC4541(2006 年 5 月)	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

付録 B　謝辞(Acknowledgments)

[OpenSSL]

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

[OpenSSH]

This product includes software developed by Niels Provos.

This product includes software developed by the University of California, Berkeley.

[SNMP]

****

Copyright 1988-1996 by Carnegie Mellon University

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

****

Some of this software has been modified by BBN Corporation and is a derivative of software developed by Carnegie Mellon University. Use of the software remains subject to the original conditions set forth above.

****

Some of this software is Copyright 1989 by TGV, Incorporated but subject to the original conditions set forth above.

****

Some of this software is Copyright (C) 1983,1988 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of California at Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.

****

* Primary Author:

Steve Waldbusser

* Additional Contributors:

Erik Schoenfelder (schoenfr@ibr.cs.tu-bs.de): additions, fixes and enhancements for Linux by 1994/1995.

David Waitzman: Reorganization in 1996.

Wes Hardaker <hardaker@ece.ucdavis.edu>: Some bug fixes in his UC

Davis CMU SNMP distribution were adopted by David Waitzman

David Thaler <thalerd@eecs.umich.edu>: Some of the code for making the agent embeddable into another application were adopted by David Waitzman

Many more over the years...

[NTP]

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

Copyright (C) David L. Mills 1992-2003 Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

[PIM sparse-mode pimd]

/*

* Copyright (c) 1998 by the University of Southern California.

* All rights reserved.

*

* Permission to use, copy, modify, and distribute this software and

* its documentation in source and binary forms for lawful

* purposes and without fee is hereby granted, provided

* that the above copyright notice appear in all copies and that both

* the copyright notice and this permission notice appear in supporting

* documentation, and that any documentation, advertising materials,

* and other materials related to such distribution and use acknowledge

* that the software was developed by the University of Southern

* California and/or Information Sciences Institute.

* The name of the University of Southern California may not

* be used to endorse or promote products derived from this software

* without specific prior written permission.

*

* THE UNIVERSITY OF SOUTHERN CALIFORNIA DOES NOT MAKE ANY REPRESENTATIONS

* ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. THIS SOFTWARE IS

* PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES,

```
 * INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF
 * MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND
 * NON-INFRINGEMENT.
 *
 * IN NO EVENT SHALL USC, OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY
 * SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT,
 * TORT, OR OTHER FORM OF ACTION, ARISING OUT OF OR IN CONNECTION WITH,
 * THE USE OR PERFORMANCE OF THIS SOFTWARE.
 *
 * Other copyrights might apply to parts of this software and are so
 * noted when applicable.
 */
/*
 * Questions concerning this software should be directed to
 * Pavlin Ivanov Radoslavov (pavlin@catarina.usc.edu)
 *
 */
/*
 * Part of this program has been derived from mrouted.
 * The mrouted program is covered by the license in the accompanying file
 * named "LICENSE.mrouted".
 *
 * The mrouted program is COPYRIGHT 1989 by The Board of Trustees of
 * Leland Stanford Junior University.
 *
 */
```

[pim6dd]

```
/*
 * Copyright (C) 1998 WIDE Project.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the project nor the names of its contributors
 * may be used to endorse or promote products derived from this software
 * without specific prior written permission.
```

[pim6sd]

* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*/
/*
* Questions concerning this software should be directed to
* Mickael Hoerdt (hoerdt@clarinet.u-strasbg.fr) LSIIT Strasbourg.
*
*/
/*
* This program has been derived from pim6dd.
* The pim6dd program is covered by the license in the accompanying file
* named "LICENSE.pim6dd".
*/
/*
* This program has been derived from pimd.
* The pimd program is covered by the license in the accompanying file
* named "LICENSE.pimd".
*
*/

[RADIUS]

Copyright 1992 Livingston Enterprises,　Inc.
Livingston Enterprises,　Inc. 6920 Koll Center Parkway Pleasanton,　CA 94566
Permission to use,　copy,　modify,　and distribute this software for any
purpose and without fee is hereby granted,　provided that this copyright
and permission notice appear on all copies and supporting documentation,
the name of Livingston Enterprises,　Inc. not be used in advertising or
publicity pertaining to distribution of the program without specific
prior permission,　and notice be given in supporting documentation that
copying and distribution is by permission of Livingston Enterprises,　Inc.
Livingston Enterprises,　Inc. makes no representations about the suitability
of this software for any purpose. It is provided "as is" without express
or implied warranty.

[totd]

WIDE
Copyright (C) 1998 WIDE Project. All rights reserved.

INVENIA INNOVATION A.S. ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS" CONDITION. INVENIA INNOVATION A.S. DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

The author requests users of this software to send back any improvements or extensions that they make and grant him and/or the Invenia Innovation the rights to redistribute these changes without restrictions.

Todd C. Miller

Copyright (C) 1998 Todd C. Miller <Todd.Miller@courtesan.com> All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[libtacplus]

Copyright (C) 1998, 2001, 2002, Juniper Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE

OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[tftp]

Copyright (C) 1983, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[libfetch]

Copyright (C) 1998 Dag-Erling Coïdan Smørgrav

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer in this position and unchanged.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[IPv6 DHCP]

Copyright (C) 1998-2004 WIDE Project.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

3. Neither the name of the project nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

[iides]

Internet Initiative Japan Inc.

Copyright (c) 1996 Internet Initiative Japan Inc.

All rights reserved.

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistribution with functional modification must include prominent notice stating how and when and by whom it is modified.

3. Redistributions in binary form have to be along with the source code or documentation which include above copyright notice, this list of conditions and the following disclaimer.

4. All commercial advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by Internet Initiative Japan Inc.

THIS SOFTWARE IS PROVIDED BY ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

[Net-SNMP]

CMU/UCD

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Networks Associates Technology, Inc

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cambridge Broadband Ltd.

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Sun Microsystems, Inc.

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Sparta, Inc

Copyright (c) 2003-2004, Sparta, Inc

All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cisco/BUPTNIC

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[Apache License Version 2.0]

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.
4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");

you may not use this file except in compliance with the License.

You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

[Python]

Copyright (c) 2001-2012 Python Software Foundation.
All Rights Reserved.
Copyright (c) 2000 BeOpen.com.
All Rights Reserved.
Copyright (c) 1995-2001 Corporation for National Research Initiatives.
All Rights Reserved.
Copyright (c) 1991-1995 Stichting Mathematisch Centrum, Amsterdam.
All Rights Reserved.
A. HISTORY OF THE SOFTWARE
==========
Python was created in the early 1990s by Guido van Rossum at Stichting Mathematisch Centrum (CWI, see http://www.cwi.nl) in the Netherlands as a successor of a language called ABC. Guido remains Python's principal author, although it includes many contributions from others.
In 1995, Guido continued his work on Python at the Corporation for National Research Initiatives (CNRI, see http://www.cnri.reston.va.us) in Reston, Virginia where he released several versions of the software.
In May 2000, Guido and the Python core development team moved to BeOpen.com to form the BeOpen PythonLabs team. In October of the same year, the PythonLabs team moved to Digital Creations (now Zope Corporation, see http://www.zope.com). In 2001, the Python Software Foundation (PSF, see http://www.python.org/psf/) was formed, a non-profit organization created specifically to own Python-related Intellectual Property. Zope Corporation is a sponsoring member of the PSF.
All Python releases are Open Source (see http://www.opensource.org for the Open Source Definition). Historically, most, but not all, Python releases have also been GPL-compatible; the table below summarizes the various releases.

Release	Derived from	Year	Owner	GPL-compatible? (1)
0.9.0 thru 1.2		1991-1995	CWI	yes
1.3 thru 1.5.2	1.2	1995-1999	CNRI	yes
1.6	1.5.2	2000	CNRI	no
2.0	1.6	2000	BeOpen.com	no
1.6.1	1.6	2001	CNRI	yes (2)
2.1	2.0+1.6.1	2001	PSF	no
2.0.1	2.0+1.6.1	2001	PSF	yes
2.1.1	2.1+2.0.1	2001	PSF	yes
2.2	2.1.1	2001	PSF	yes
2.1.2	2.1.1	2002	PSF	yes

2.1.3	2.1.2	2002	PSF	yes
2.2.1	2.2	2002	PSF	yes
2.2.2	2.2.1	2002	PSF	yes
2.2.3	2.2.2	2003	PSF	yes
2.3	2.2.2	2002-2003	PSF	yes
2.3.1	2.3	2002-2003	PSF	yes
2.3.2	2.3.1	2002-2003	PSF	yes
2.3.3	2.3.2	2002-2003	PSF	yes
2.3.4	2.3.3	2004	PSF	yes
2.3.5	2.3.4	2005	PSF	yes
2.4	2.3	2004	PSF	yes
2.4.1	2.4	2005	PSF	yes
2.4.2	2.4.1	2005	PSF	yes
2.4.3	2.4.2	2006	PSF	yes
2.4.4	2.4.3	2006	PSF	yes
2.5	2.4	2006	PSF	yes
2.5.1	2.5	2007	PSF	yes
2.5.2	2.5.1	2008	PSF	yes
2.5.3	2.5.2	2008	PSF	yes
2.6	2.5	2008	PSF	yes
2.6.1	2.6	2008	PSF	yes
2.6.2	2.6.1	2009	PSF	yes
2.6.3	2.6.2	2009	PSF	yes
2.6.4	2.6.3	2009	PSF	yes
2.6.5	2.6.4	2010	PSF	yes
3.0	2.6	2008	PSF	yes
3.0.1	3.0	2009	PSF	yes
3.1	3.0.1	2009	PSF	yes
3.1.1	3.1	2009	PSF	yes
3.1.2	3.1.1	2010	PSF	yes
3.1.3	3.1.2	2010	PSF	yes
3.1.4	3.1.3	2011	PSF	yes
3.2	3.1	2011	PSF	yes
3.2.1	3.2	2011	PSF	yes
3.2.2	3.2.1	2011	PSF	yes
3.2.3	3.2.2	2012	PSF	yes

Footnotes:

(1) GPL-compatible doesn't mean that we're distributing Python under the GPL. All Python licenses, unlike the GPL, let you distribute a modified version without making your changes open source. The GPL-compatible licenses make it possible to combine Python with other software that is released under the GPL; the others don't.

(2) According to Richard Stallman, 1.6.1 is not GPL-compatible, because its license has a choice of law clause. According to CNRI, however, Stallman's lawyer has told CNRI's lawyer that 1.6.1 is "not incompatible" with the GPL.

Thanks to the many outside volunteers who have worked under Guido's direction to make these releases possible.

B. TERMS AND CONDITIONS FOR ACCESSING OR OTHERWISE USING PYTHON

==========

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

---

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby

grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce,
analyze, test, perform and/or display publicly, prepare derivative works,
distribute, and otherwise use Python alone or in any derivative version,
provided, however, that PSF's License Agreement and PSF's notice of copyright,
i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010,
2011, 2012 Python Software Foundation; All Rights Reserved" are retained in Python
alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on
or incorporates Python or any part thereof, and wants to make
the derivative work available to others as provided herein, then
Licensee hereby agrees to include in any such work a brief summary of
the changes made to Python.
4. PSF is making Python available to Licensee on an "AS IS"
basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR
IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR
FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR
ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT
OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY
DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material
breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any
relationship of agency, partnership, or joint venture between PSF and
Licensee. This License Agreement does not grant permission to use PSF
trademarks or trade name in a trademark sense to endorse or promote
products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python, Licensee
agrees to be bound by the terms and conditions of this License
Agreement.
BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1
1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an
office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the
Individual or Organization ("Licensee") accessing and otherwise using
this software in source or binary form and its associated
documentation ("the Software").
2. Subject to the terms and conditions of this BeOpen Python License
Agreement, BeOpen hereby grants Licensee a non-exclusive,
royalty-free, world-wide license to reproduce, analyze, test, perform

Reserved" are retained in Python 1.6.1 alone or in any derivative version prepared by Licensee. Alternately, in lieu of CNRI's License Agreement, Licensee may substitute the following text (omitting the quotes): "Python 1.6.1 is made available subject to the terms and conditions in CNRI's License Agreement. This Agreement together with Python 1.6.1 may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1013. This Agreement may also be obtained from a proxy server on the Internet using the following URL: http://hdl.handle.net/1895.22/1013".

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6.1 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 1.6.1.

4. CNRI is making Python 1.6.1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6.1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 1.6.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 1.6.1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. This License Agreement shall be governed by the federal intellectual property law of the United States, including without limitation the federal copyright law, and, to the extent such U.S. federal law does not apply, by the law of the Commonwealth of Virginia, excluding Virginia's conflict of law provisions. Notwithstanding the foregoing, with regard to derivative works based on Python 1.6.1 that incorporate non-separable material that was previously distributed under the GNU General Public License (GPL), the law of the Commonwealth of Virginia shall govern this License Agreement only as to issues arising under or with respect to Paragraphs 4, 5, and 7 of this License Agreement. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee. This License Agreement does not grant permission to use CNRI trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By clicking on the "ACCEPT" button where indicated, or by copying,

A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Any feedback is very welcome.
http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html
email: m-mat @ math.sci.hiroshima-u.ac.jp (remove space)

/ Copyright (c) 1996. ¥
| The Regents of the University of California. |
| All rights reserved. |
| |
| Permission to use, copy, modify, and distribute this software for |
| any purpose without fee is hereby granted, provided that this en- |
| tire notice is included in all copies of any software which is or |
| includes a copy or modification of this software and in all |
| copies of the supporting documentation for such software. |
| |
| This work was produced at the University of California, Lawrence |
| Livermore National Laboratory under contract no. W-7405-ENG-48 |
| between the U.S. Department of Energy and The Regents of the |
| University of California for the operation of UC LLNL. |
| |
| DISCLAIMER |
| |
| This software was prepared as an account of work sponsored by an |
| agency of the United States Government. Neither the United States |
| Government nor the University of California nor any of their em- |
| ployees, makes any warranty, express or implied, or assumes any |
| liability or responsibility for the accuracy, completeness, or |
| usefulness of any information, apparatus, product, or process |
| disclosed, or represents that its use would not infringe |
| privately-owned rights. Reference herein to any specific commer- |
| cial products, process, or service by trade name, trademark, |
| manufacturer, or otherwise, does not necessarily constitute or |
| imply its endorsement, recommendation, or favoring by the United |

索引

P

R

S

T

V

あ

い

う

え

お

か

き

こ

さ

し

す

せ

そ

た

つ

て

と

に

ね

は

ひ

ふ

へ

ほ

ま

め

ゆ

ら

り

る

れ

ろ