IP8800/S8600・IP8800/S8300

トラブルシューティングガイド

IP88S86-T001-70

■ 対象製品

このマニュアルは IP8800/S8600 および IP8800/S8300 を対象に記載しています。

■ 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

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，富士ゼロックス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。
IPX は，Novell,Inc.の商標です。
Python(R)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。
イーサネットは，富士ゼロックス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。
また，出力表示例や図は，実際と異なる部分がある場合がありますのでご了承ください。

■ 発行

２０２０年　１２月　(第８版)　ＩＰ８８Ｓ８６－Ｔ００１－７０

■ 著作権

変更内容

表　第 8 版の変更内容

章・節・項・タイトル	追加・変更内容
3.1.1　イーサネットポートの接続ができない	• トラッキング連携についての記述を追加しました。
5.1.1　通信できない，または切断されている	• トラッキング連携についての記述を追加しました。
5.2.1　通信できない，または切断されている	• トラッキング連携についての記述を追加しました。
5.5.1　スタティック経路情報が存在しない	• トラッキング連携についての記述を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

表　第 7 版の変更内容

項目	追加・変更内容
SSH のトラブル	• 本節を追加しました。

表　第 6 版の変更内容

項目	追加・変更内容
階層化シェーパのトラブル	• シェーパユーザ個別設定のサポートに伴い，記述を変更しました。
トラッキング機能のトラブル	• 本節を追加しました。

表　第 5 版の変更内容

項目	追加・変更内容
10GBASE-R/40GBASE-R/100GBASE-R のトラブル	• 40GBASE-R の記述を追加しました。
階層化シェーパのトラブル	• 本項を追加しました。
QoS による廃棄を確認する	• NIF の追加に伴い，記述を追加しました。 • 階層化シェーパサポートに伴い，記述を追加しました。

表　第 4 版の変更内容

項目	追加・変更内容
アクセスリストログのトラブル	• 本項を追加しました。
ポリシーベースミラーリングのトラブル	• 本節を追加しました。

表　第 3 版の変更内容

項目	追加・変更内容
装置の障害解析	• IP8800/S8300 の記述を追加しました。
PIM-SM ネットワークでマルチキャスト通信ができない	• マルチキャストチャネル参加制限機能サポートに伴い，記述を変更しました。

項目	追加・変更内容
PIM-SSM ネットワークでマルチキャスト通信ができない	• マルチキャストチャネル参加制限機能サポートに伴い，記述を変更しました。
系切替後にマルチキャスト通信が停止する	• ノンストップルーティングサポートに伴い，記述を変更しました。
QoS のトラブル	• QoS フロー廃棄サポートに伴い，記述を追加しました。
QoS による廃棄を確認する	• QoS フロー廃棄サポートに伴い，記述を追加しました。
ポート inactive 状態の確認	• 本節を追加しました。

表　第 2 版の変更内容

項目	追加・変更内容
IGMP/MLD snooping の通信障害	• 本節を追加しました。
PIM-SM ネットワークでマルチキャスト通信ができない	• IGMP/MLD snooping サポートに伴い，記述を追加しました。
PIM-SSM ネットワークでマルチキャスト通信ができない	• IGMP/MLD snooping サポートに伴い，記述を追加しました。
IEEE802.3ah OAM のトラブル	• 本節を追加しました。

はじめに

■ 対象製品

このマニュアルは IP8800/S8600 および IP8800/S8300 を対象に記載しています。

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。

■ 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，「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ので，あわせてご利用ください。

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

IP8800/S8600 クイックスタートガイド (IP88S86-Q001)	IP8800/S8300 クイックスタートガイド (IP88S83-Q001)

●ハードウェアの設備条件，取扱方法を調べる

IP8800/S8600 ハードウェア取扱説明書 (IP88S86-H001)	IP8800/S8300 ハードウェア取扱説明書 (IP88S83-H001)

●ソフトウェアの機能，コンフィグレーションの設定，運用コマンドを知りたい

▽まず，ガイドで使用する機能や収容条件についてご確認ください。

・収容条件 ・ログインなどの基本操作 ・イーサネット	・フィルタ，QoS ・ネットワークの管理	・IPパケット中継 ・ユニキャストルーティング ・マルチキャストルーティング
コンフィグレーションガイド Vol.1 (IP88S86-S001)	コンフィグレーションガイド Vol.2 (IP88S86-S002)	コンフィグレーションガイド Vol.3 (IP88S86-S003)

▽必要に応じて，レファレンスをご確認ください。

・コマンドの入力シンタックス，パラメータ詳細について

コンフィグレーション コマンドレファレンス Vol.1 (IP88S86-S004)	コンフィグレーション コマンドレファレンス Vol.2 (IP88S86-S005)	コンフィグレーション コマンドレファレンス Vol.3 (IP88S86-S006)
運用コマンドレファレンス Vol.1 (IP88S86-S007)	運用コマンドレファレンス Vol.2 (IP88S86-S008)	運用コマンドレファレンス Vol.3 (IP88S86-S009)

・システムメッセージとログについて

メッセージ・ログレファレンス (IP88S86-S010)

・MIBについて

MIBレファレンス (IP88S86-S011)

●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 (IP88S86-T001)

■ このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
AXRP	Autonomous eXtensible Ring Protocol
BCU	Basic Control Unit
BEQ	Best Effort Queueing
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。
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
C-Tag	Customer Tag

CA	Certificate Authority
CC	Continuity Check
CCM	Continuity Check Message
CFM	Connectivity Fault Management
CFP	C Form-factor Pluggable
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
CoS	Class of Service
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
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
E-mail	Electronic mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECDSA	Elliptic Curve Digital Signature Algorithm
EFM	Ethernet in the First Mile
ETH-AIS	Ethernet Alarm Indicator Signal
ETH-LCK	Ethernet Locked Signal
FAN	Fan Unit
FCS	Frame Check Sequence
FE	Forwarding Engine
HDC	Hardware Dependent Code
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLPQ	Low Latency Priority Queueing
LLQ	Low Latency Queueing
LLRLQ	Low Latency Rate Limited Queueing
LSA	Link State Advertisement
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEG	Maintenance Entity Group
MEP	Maintenance association End Point/Maintenance entity group End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MP	Maintenance Point
MRU	Maximum Receive Unit
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge

NAS	Network Access Server
NBMA	Non-Broadcast Multiple-Access
NDP	Neighbor Discovery Protocol
NIF	Network Interface
NSAP	Network Service Access Point
NSR	NonStop Routing
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PA	Protocol Accelerator
packet/s	packets per second　　*ppsと表記する場合もあります。
PAD	PADding
PC	Personal Computer
PDU	Protocol Data Unit
PE-ME	Programmable Engine Micro Engine
PE-NIF	Programmable Engine Network Interface
PGP	Pretty Good Privacy
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PQ	Priority Queueing
PRU	Packet Routing Unit
PS	Power Supply
PSINPUT	Power Supply Input
PSU	Packet Switching Unit
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
RFC	Request For Comments
RGQ	Rate Guaranteed Queueing
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RR	Round Robin
RSA	Rivest, Shamir, Adleman
S-Tag	Service Tag
SA	Source Address
SD	Secure Digital
SFD	Start Frame Delimiter
SFP	Small Form-factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SFU	Switch Fabric Unit
SHA1	Secure Hash Algorithm 1
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNPA	Subnetwork Point of Attachment
SNTP	Simple Network Time Protocol
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
SSH	Secure Shell
SSW	Sub-crossbar SWitch
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
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
URL	Uniform Resource Locator
uRPF	unicast Reverse Path Forwarding

VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WFQ	Weighted Fair Queueing
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

1 装置障害のトラブルシュート

この章では，装置障害が発生した場合の対処について説明します。

1.1　装置の障害解析

1.1.1　IP8800/S8600・IP8800/S8300 の障害解析

運用中に障害が発生したとき，装置を目視で直接確認できる場合には，「1.2　トラブルシュート」の内容に従ってトラブルシュートしてください。装置を目視で直接確認できない場合でも，リモート運用端末から運用コマンドで装置の LED を確認すると，装置を目視できる場合と同様にトラブルシュートできます。

装置の状態は，BCU に表示されます。BCU の LED について，「図 1-1　正面パネルのレイアウト例」および「表 1-1　LED 表示，スイッチ，コネクタ」に示します。なお，BCU 以外のオプション機構（SFU，PSU，NIF，電源機構，ファンユニット）の LED などの情報は，「ハードウェア取扱説明書」を参照してください。

図 1-1　正面パネルのレイアウト例

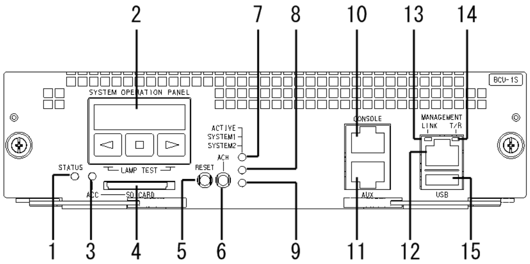


表 1-1　LED 表示，スイッチ，コネクタ

番号	名称	種類	LED の表示対象，スイッチ／コネクタの種類	内容
1	STATUS	LED：緑／赤	BCU の動作状態	緑点灯：動作可能 緑点滅：ソフトウェアロード中，または reload stop コマンドの実行で停止中 赤点灯：障害検出 消灯：電源 OFF※1
2	SYSTEM OPERATION PANEL	液晶ディスプレイおよび操作キー	システム操作パネル	装置情報の表示や動作指示，障害情報を表示する（詳細は「コンフィグレーションガイド」参照）
3	ACC	LED：緑	メモリカードの状態	緑点灯：メモリカードアクセス中（メモリカードの取り外し禁止） 消灯：メモリカードアイドル中（メモリカードの取り付けおよび取り外し可能）
4	SD CARD	コネクタ	SD カードスロット	SD カードスロット
5	RESET	スイッチ（ノンロック）	装置のマニュアルリセットスイッチ※2	1 秒押し：装置に障害が発生した場合などに行う※3 5 秒押し：ログインユーザ名またはパスワードを忘れた場合に行う※4
6	ACH	スイッチ（ノンロック）	BCU の系切替スイッチ※2	BCU を二重化している場合に，運用系と待機系とを切り替える※5

番号	名称	種類	LED の表示対象，スイッチ／コネクタの種類	内容
7	ACTIVE	LED：緑	BCU の運用状態	緑点灯：運用系 消灯：待機系
8	SYSTEM1	LED：緑／赤	装置の状態	緑点灯：動作可能 緑点滅：装置の部分障害検出 赤点灯：装置の障害検出
9	SYSTEM2	LED	装置の状態	未サポートのため，常に消灯
10	CONSOLE	コネクタ	CONSOLE ポート	運用端末接続用 RS-232C ポート
11	AUX	コネクタ	AUX ポート	運用端末接続用 RS-232C ポート
12	MANAGEMENT	コネクタ	マネージメントポート	運用端末接続用 10BASE-T/100BASE-TX/1000BASE-T イーサネットポート
13	LINK	LED：緑／橙	マネージメントポートの動作状態	緑点灯：リンク確立 橙点灯：障害検出 消灯：リンク障害※6，または運用停止中※7
14	T/R	LED：緑	マネージメントポートの動作状態	緑点灯：パケット送受信中 消灯：パケットを送受信していない
15	USB	コネクタ	USB ポート	未サポートのため，使用できない

注※1　システム操作パネルからの inactivate 操作，または運用端末からのコマンド実行で BCU の電源を OFF にできます。

注※2　スイッチはパネル表面より奥にあります。先の細いドライバなどを使用して押してください。

注※3　押す時間が 1 秒以下の場合はリセットされないことがあります。

注※4　再起動後は，ログインパスワードおよび装置管理者モードのパスワードが不要となります。また，ログインユーザ名「operator」によるログインを許可します。そのため，この方法で再起動する場合は注意が必要です。

注※5　運用系 BCU の ACH スイッチを押したときだけ系切替します。系切替後，新待機系 BCU は再起動します。

注※6　ケーブルが抜けている場合も含みます。

注※7　コマンドの実行で運用を停止できます。

1.2　トラブルシュート

1.2.1　装置障害の対応手順

装置に障害が発生した場合は，次に示す手順で対応してください。

表 1-2　装置障害のトラブルシュート

項番	障害内容	対応
1	• 装置から発煙している • 装置から異臭が発生している • 装置から異常音が発生している	すぐに次の手順で対応してください。 1. 装置の電源を OFF にしてください。 2. AC 電源の場合は，装置の電源ケーブルを抜いてください。 3. DC 電源の場合は，装置に接続している電源設備のブレーカを OFF にしてください。 これらの手順で運用を停止したあと，販売店に連絡してください。
2	login プロンプトが表示されない	次の手順で対応してください。 1. MC が挿入されている場合は，MC を抜いてから装置の電源を OFF にしたあと，再度 ON にして装置を再起動してください。 2. MC が挿入されていない場合は，装置の電源を OFF にしたあと，再度 ON にして装置を再起動してください。 3. 装置を再起動しても問題が解決しない場合は，BCU を交換してください。
3	BCU の LED がすべて消灯している	次の手順で対応してください。 1. 電源機構の LED を確認してください。 ・電源機構の ALARM LED が赤点灯している場合は，該当する電源機構を交換してください。 ・電源機構の POWER LED および ALARM LED がどちらも消灯している場合は，「表 1-3　電源障害のトラブルシュート」を参照して，該当する電源機構の障害に対応してください。問題が解決しない場合は，該当する電源機構とそれに対応する電源入力機構を交換してください。 2. 電源機構がすべて正常に動作している場合は，BCU を交換してください。
4	BCU の SYSTEM1 LED が緑点滅または赤点灯している	次の手順で対応してください。 1. システム操作パネルにシステムメッセージが表示されている場合は，「メッセージ・ログレファレンス」を参照して，該当するメッセージの記載内容に従って対応してください。 2. システム操作パネルにシステムメッセージが表示されていない場合は，STATUS LED が赤点灯しているボード（BCU，SFU，PSU，NIF）を交換してください。
5	システム操作パネルにシステムメッセージが表示されている	「メッセージ・ログレファレンス」を参照して，該当するメッセージの記載内容に従って対応してください。
6	BCU の STATUS LED が赤点灯しているが，ほかの LED はすべて消灯していて，システム操作パネルに	次の手順で対応してください。 1. BCU の構成を確認してください。 ・BCU 一重化構成の場合は，次に示す 3.以降の手順を実施してください。 ・BCU 二重化構成の場合は，次に示す 2.以降の手順を実施してください。

項番	障害内容	対応
	システムメッセージが表示されていない	2. 運用系 BCU および待機系 BCU の状態を確認してください。 ・どちらかの系だけで障害が発生している場合は，該当する BCU を交換してください。この場合，3.以降の手順は不要です。 ・両系で障害が発生している場合は，次に示す 3.以降の手順を実施してください。 3. 電源機構の LED を確認してください。 ・電源機構の ALARM LED が赤点灯している場合は，該当する電源機構を交換してください。 ・電源機構の POWER LED および ALARM LED がどちらも消灯している場合は，「表 1-3　電源障害のトラブルシュート」を参照して，該当する電源機構の障害に対応してください。問題が解決しない場合は，該当する電源機構を交換してください。 ・電源機構がすべて正常に動作している場合は，電源機構をそのままの状態で保持してください。 4. 装置に搭載されている電源入力機構のブレーカをすべて OFF にしてください。 5. 30 秒以上経過してから，装置に搭載されている電源入力機構のブレーカをすべて ON にしてください。 6. 本障害が発生した BCU を交換してください。

電源に障害が発生した場合は，次に示す手順で対応してください。なお，IP8800/S8300 には電源入力機構のブレーカ（スイッチ）がないため，電源ケーブルの取り付けおよび取り外しで電源を ON および OFF にしてください。

表 1-3　電源障害のトラブルシュート

項番	障害内容	対応
1	電源入力機構のブレーカが OFF になっている	電源入力機構のブレーカを ON にしてください。
2	• 電源ケーブルが抜けている • 電源ケーブルが正しく接続されていない	次の手順で対応してください。 1. 電源入力機構のブレーカを OFF にしてください。 2. DC 電源の場合は，装置に接続している電源設備のブレーカを OFF にしてください。 3. 電源ケーブルを正しく取り付けてください。 4. DC 電源の場合は，装置に接続している電源設備のブレーカを ON にしてください。 5. 電源入力機構のブレーカを ON にしてください。
3	電源入力機構が正しく搭載されていない（がたついている）	次の手順で対応してください。 1. 電源入力機構のブレーカを OFF にしてください。 2. DC 電源の場合は，装置に接続している電源設備のブレーカを OFF にしてください。 3. 電源ケーブルを取り外してください。 4. 電源入力機構をいったん取り外してから，しっかりと挿入してください。

項番	障害内容	対応
		5. 電源ケーブルを取り付けてください。 6. DC 電源の場合は，装置に接続している電源設備のブレーカを ON にしてください。 7. 電源入力機構のブレーカを ON にしてください。
4	電源機構が正しく搭載されていない（がたついている）	次の手順で対応してください。 1. 電源入力機構のブレーカを OFF にしてください。 2. 電源機構をいったん取り外してから，しっかりと挿入してください。 3. 電源入力機構のブレーカを ON にしてください。
5	測定した入力電源が次の値の範囲外である※ • AC100V の場合：AC90～132V • AC200V の場合：AC180～264V • DC-48V の場合：DC-40.5～-57V	設備担当者に連絡して，入力電源の対策を依頼してください。

注※　入力電源が測定できる場合だけ実施してください。

1.2.2　装置およびオプション機構の交換方法

装置およびファンユニット，電源入力機構，電源機構，BCU，SFU，PSU，NIF，メモリカード，トランシーバなどのオプション機構の取り付けおよび取り外し方法については，「ハードウェア取扱説明書」に記載されています。記載された手順に従って，取り付けたり取り外したりしてください。

2 運用管理のトラブルシュート

この章では，運用管理でトラブルが発生した場合の対処について説明します。

2.1　ログインのトラブル

2.1.1　ログインユーザのパスワードを忘れた

ログインユーザのパスワードを忘れて本装置にログインできない場合は，次に示す方法で対応してください。

(1)　ログインおよび装置管理者モードに変更できるユーザがほかにいる場合

パスワードを忘れたユーザ以外に，ログインおよび装置管理者モードに変更できるユーザがいる場合，そのユーザがコンフィグレーションコマンド username を実行して，パスワードを忘れたログインユーザのパスワードを再設定します。このコマンドは，コンフィグレーションモードで実行します。

パスワードを忘れた user1 のパスワードを再設定する例を次の図に示します。

図 2-1　user1 のパスワードを再設定する例

```
# configure
(config)# username user1 password input
New password:********                    <-1
Retype new password:********             <-2
!(config)# save
(config)# exit
#
```

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）。

(2)　ログインおよび装置管理者モードに変更できるユーザがほかにいない場合

パスワードを忘れたユーザ以外にログインおよび装置管理者モードに変更できるユーザがいない場合，装置のリセットスイッチを 5 秒以上押して，デフォルトリスタートをします。デフォルトリスタートによる起動のあと，パスワードを再設定してください。なお，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。

デフォルトリスタートで起動したあとは，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しません。また，ログインユーザ名「operator」によるログインを許可します。このようにセキュリティレベルが低下するため，パスワードを再設定したあとはすぐに装置を再起動してください。

2.1.2　装置管理者モードのパスワードを忘れた

装置管理者モードのパスワードを忘れて，入力モードを装置管理者モードに変更できない場合，装置のリセットスイッチを 5 秒以上押して，デフォルトリスタートをします。デフォルトリスタートによる起動のあと，パスワードを再設定してください。なお，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。

デフォルトリスタートで起動したあとは，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しません。また，ログインユーザ名「operator」によるログインを許可します。このようにセキュリティレベルが低下するため，パスワードを再設定したあとはすぐに装置を再起動してください。

2.1.3　ログインユーザ名を忘れた

ログインユーザ名を忘れて本装置にログインできない場合は，次に示す方法で対応してください。

(1)　ログインできるユーザがほかにいる場合

ユーザ名を忘れたユーザ以外にログインできるユーザがいる場合，そのユーザが show users コマンドを実行して，ログインユーザ名を確認してください。

(2)　ログインできるユーザがほかにいない場合

ユーザ名を忘れたユーザ以外にログインできるユーザがいない場合，装置のリセットスイッチを 5 秒以上押して，デフォルトリスタートをします。デフォルトリスタートによる起動のあと，ログインユーザ名「operator」でログインして show users コマンドを実行して，ログインユーザ名を確認してください。

デフォルトリスタートで起動したあとは，ログインユーザ名「operator」によるログインを許可します。また，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しません。このようにセキュリティレベルが低下するため，ログインユーザ名を確認したあとはすぐに装置を再起動してください。

2.2　運用端末のトラブル

2.2.1　コンソールからの入力，表示がうまくできない

コンソールとの接続トラブルが発生した場合は，次の表に従って確認してください。

表 2-1　コンソールとの接続トラブルおよび対応

項番	障害内容	確認内容
1	画面に何も表示されない	次の手順で確認してください。 1. 装置の正面パネルにある STATUS LED が緑点灯しているか確認してください。緑点灯していない場合は，「1.1　装置の障害解析」を参照してください。 2. ケーブルの接続が正しいか確認してください。 3. コンソールケーブルの結線を確認してください。詳細は，「ハードウェア取扱説明書」を参照してください。 4. ポート番号，通信速度，データ長，パリティビット，ストップビット，フロー制御などの通信ソフトウェアの設定が次のとおりになっているか確認してください。 通信速度：9600bit/s（変更している場合は設定値） データ長：8bit パリティビット：なし ストップビット：1bit フロー制御：なし
2	キー入力を受け付けない	次の手順で確認してください。 1. XON／XOFF によるフロー制御でデータの送受信を中断している可能性があります。データ送受信の中断を解除してください（[Ctrl] ＋ [Q] キーを入力してください）。それでもキー入力ができない場合は，手順 2.以降を確認してください。 2. 通信ソフトウェアの設定が正しいか確認してください。 3. [Ctrl] ＋ [S] キーによって画面が停止している可能性があります。何かキーを入力してください。
3	異常な文字が表示される	通信ソフトウェアとのネゴシエーションが正しくできていない可能性があります。通信ソフトウェアの通信速度を次の手順で確認してください。 1. コンフィグレーションコマンド line console 0 で CONSOLE（RS232C）の通信速度を設定していない場合は，通信ソフトウェアの通信速度が 9600bit/s に設定されているか確認してください。 2. コンフィグレーションコマンド line console 0 で CONSOLE（RS232C）の通信速度を 1200，2400，4800，9600，または 19200bit/s に設定している場合は，通信ソフトウェアの通信速度が正しく設定されているか確認してください。 3. 手順 1.および 2.で問題がなくても異常な文字が表示される場合は，ブレーク信号を発行してください。なお，通信ソフトウェアの通信速度によって，複数回ブレーク信号を発行しないと表示されないことがあります。
4	ユーザ名入力中に異常な文字が表示された	CONSOLE（RS232C）の通信速度が変更された可能性があります。項番 3 を参照してください。

項番	障害内容	確認内容
5	ログインできない	次の手順で確認してください。 1. 画面にログインプロンプトが表示されているか確認してください。表示されていない場合は，装置を起動中です。しばらく待ってください。 2. ローカル認証でログインする場合は，装置に存在しないアカウントでログインしようとしていないか確認してください。 3. コンフィグレーションコマンド aaa authentication login console および aaa authentication login で，RADIUS/TACACS+認証が設定されていないか確認してください（詳細は「2.2.3　RADIUS/TACACS+を利用したログイン認証ができない」を参照してください）。
6	ログイン後に通信ソフトウェアの通信速度を変更したら異常な文字が表示されて，コマンドが入力できない	ログイン後に通信ソフトウェアの通信速度を変更しても正常に表示できません。通信ソフトウェアの通信速度を元に戻してください。
7	項目名と内容がずれて表示される	1 行で表示できる文字数を超える情報を表示している可能性があります。通信ソフトウェアの設定で画面サイズを変更して，1 行で表示できる文字数を多くしてください。

モデムとの接続トラブルが発生した場合は，次の表に従って確認してください。また，モデムに付属している取扱説明書を参照してください。

表 2-2　モデムとの接続トラブルおよび対応

項番	障害内容	確認内容
1	モデムが自動着信しない	次のことを確認してください。 • ケーブルの接続が正しいこと。 • モデムの電源が ON になっていること。 • 電話番号が正しいこと。 • モデムの設定内容が正しいこと。 • 2 台の端末にモデムを接続して，ダイアルすることで回線接続できること。
2	ログイン時に異常な文字が表示される	次の手順で確認してください。 1. モデムの通信速度を 9600bit/s に設定してください。 2. モデムが V.90，K56flex，x2 またはそれ以降の通信規格に対応している場合は，V.34 通信方式以下で接続するように設定してください。
3	回線切断後，再ダイアルしても通話中でつながらない	回線が切断されてから数秒間は着信しないことがあります。モデムのマニュアルを参照してください。
4	回線障害後，再接続できない	障害によって回線が切断された場合，最大 120 秒間は再接続できないことがあります。すぐに接続したい場合は別の手段でログインして，AUX にダイアルアップ IP 接続をしているユーザを killuser コマンドで強制ログアウトさせてください。
5	回線切断後，再接続できない	ダイアルアップ IP 接続が切断された場合，すぐに再接続できないことがあります。その場合，300 秒間程度の間隔を空けてから再接続してください。

2.2.2 リモート運用端末からログインできない

リモート運用端末との接続トラブルが発生した場合は，次の表に従って確認してください。

表 2-3 リモート運用端末との接続トラブルおよび対応

項番	障害内容	確認内容
1	リモート接続できない	次の手順で確認してください。 1. リモート運用端末から ping コマンドを使用して，リモート接続のための経路が確立されているか確認してください。 2. コネクション確立のメッセージ表示後プロンプトが表示されるまで時間が掛かる場合は，DNS サーバと通信できなくなっている可能性があります（DNS サーバと通信できない場合，プロンプトが表示されるまで約 5 分掛かります。なお，この時間は目安でありネットワークの状態によって変化します）。
2	ログインできない	次の手順で確認してください。 1. コンフィグレーションコマンド line vty のモードで指定した，アクセスリストで許可された IPv4 または IPv6 アドレスを持つ端末を使用しているか確認してください。また，アクセスリストで設定した IPv4 または IPv6 アドレスに deny を指定していないか確認してください（詳細は「コンフィグレーションガイド」を参照してください）。 2. ローカル認証でログインする場合は，装置に存在しないアカウントでログインしようとしていないか確認してください。 3. ログインできる最大ユーザ数を超えていないか確認してください（詳細は「コンフィグレーションガイド」を参照してください）。 なお，最大ユーザ数でログインしている状態でリモート運用端末から本装置への到達性が失われて，その後復旧している場合，TCP プロトコルのタイムアウト時間が経過してセッションが切断されるまで，リモート運用端末からは新たにログインできません。TCP プロトコルのタイムアウト時間はリモート運用端末の状態やネットワークの状態によって変化しますが，約 10 分です。 4. コンフィグレーションコマンド line vty のモードで指定した transport input コマンドに，本装置へのアクセスを禁止しているプロトコルを使用していないか確認してください（詳細は「コンフィグレーションコマンドレファレンス」を参照してください）。 5. コンフィグレーションコマンド aaa authentication login で，RADIUS/TACACS+認証が設定されていないか確認してください（詳細は「2.2.3 RADIUS/TACACS+を利用したログイン認証ができない」を参照してください）。
3	キー入力を受け付けない	次の手順で確認してください。 1. XON／XOFF によるフロー制御でデータの送受信を中断している可能性があります。データ送受信の中断を解除してください（[Ctrl] ＋ [Q] キーを入力してください）。それでもキー入力ができない場合は，手順 2.以降を確認してください。 2. 通信ソフトウェアの設定が正しいか確認してください。 3. [Ctrl] ＋ [S] キーによって画面が停止している可能性があります。何かキーを入力してください。

項番	障害内容	確認内容
4	ユーザがログインした状態のままである	自動ログアウトするのを待つか，再度ログインしてログインした状態のままのユーザを killuser コマンドで強制ログアウトさせてください。 なお，該当ユーザがコンフィグレーションを編集中だった場合は，再度ログインして，コンフィグレーションモードでコンフィグレーションを保存するなどしたあと，編集を終了してください。

2.2.3　RADIUS/TACACS+を利用したログイン認証ができない

RADIUS/TACACS+を利用したログイン認証ができない場合，次の内容を確認してください。

1. RADIUS/TACACS+サーバへの通信

   ping コマンドで，本装置から RADIUS/TACACS+サーバに対して疎通ができているか確認してください。疎通ができない場合は，「5.1.1　通信できない，または切断されている」を参照してください。

   また，コンフィグレーションでループバックインタフェースの IP アドレスを設定している場合は，ループバックインタフェースの IP アドレスから ping コマンドで，本装置から RADIUS/TACACS+サーバに対して疎通ができているか確認してください。

2. タイムアウト値およびリトライ回数の設定

   本装置が RADIUS/TACACS+サーバと通信できないと判断する時間の最大値は，コンフィグレーションコマンドの設定によって異なります。

   RADIUS 認証の場合

   ＜ radius-server timeout で設定したタイムアウト値（秒）＞×＜ radius-server retransmit で設定したリトライ回数＞×＜ radius-server host で設定した RADIUS サーバ数＞

   TACACS+認証の場合

   ＜ tacacs-server timeout で設定したタイムアウト値（秒）＞×＜ tacacs-server host で設定した TACACS+サーバ数＞

   この時間が極端に大きくなると，リモート運用端末の telnet などのアプリケーションがタイムアウトによって終了するおそれがあります。この場合，RADIUS/TACACS+コンフィグレーションの設定かリモート運用端末で使用するアプリケーションのタイムアウトの設定を変更してください。

   また，RADIUS/TACACS+認証が成功したシステムメッセージが出力されているのに telnet や ftp が失敗する場合は，コンフィグレーションで指定した複数の RADIUS サーバの中で，稼働中の RADIUS/TACACS+サーバに接続するまでに，リモート運用端末側のアプリケーションがタイムアウトしていることが考えられます。この場合，稼働中の RADIUS/TACACS+サーバを優先するように設定するか，＜タイムアウト値（秒）＞×＜リトライ回数＞の値を小さくしてください。

3. 本装置にログインできない場合の対処方法

   設定ミスなどで本装置にログインできない場合は，コンソールからログインして設定を修正してください。なお，コンフィグレーションコマンド aaa authentication login console によってコンソールもログイン認証の対象となっている場合は，「2.1.2　装置管理者モードのパスワードを忘れた」の手順に従ってデフォルトリスタートしたあと，ログインして設定を修正してください。

2.2.4　RADIUS/TACACS+/ローカルを利用したコマンド承認ができない

RADIUS/TACACS+/ローカル認証は成功して本装置にログインできたが，コマンド承認ができない場合や，コマンドを実行しても承認エラーメッセージが表示されてコマンドが実行できない場合は，次の内容を確認してください。

1. 許可コマンドおよび制限コマンドの確認

   本装置の show whoami コマンドで，現在のユーザが許可または制限されているコマンドのリストを確認できます。RADIUS/TACACS+サーバの設定どおりにコマンドリストが取得できていることを確認してください。

   また，ローカルコマンド承認を使用している場合は，コンフィグレーションどおりにコマンドリストが設定されていることを確認してください。

2. サーバ設定およびコンフィグレーションの確認

   RADIUS/TACACS+サーバ側で，本装置のコマンド承認に関する設定が正しいことを確認してください。特に，RADIUS の場合はベンダー固有属性の設定，TACACS+の場合は Service と属性名などに注意してください。

   また，ローカルコマンド承認を使用している場合は，コンフィグレーションの設定が正しいことを確認してください。RADIUS/TACACS+/ローカル（コンフィグレーション）の設定については，「コンフィグレーションガイド」を参照してください。

   コマンドリスト記述時の注意

   本装置のコマンド承認用のコマンドリストを記述するときには，空白の扱いに注意してください。例えば，許可コマンドリストに"show ip　"（show ip の後ろに空白）が設定してある場合は，show ip interface コマンドは許可されますが，show ipv6 interface コマンドは制限されます。

3. コマンドがすべて制限された場合の対処方法

   設定ミスなどでコマンドがすべて制限された場合は，コンソールからログインして設定を修正してください。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，「2.1.2　装置管理者モードのパスワードを忘れた」の手順に従ってデフォルトリスタートしたあと，ログインして設定を修正してください。

2.3　SSH のトラブル

2.3.1　本装置に対して SSH で接続できない

他装置の SSH クライアントから本装置に対して SSH（ssh，scp，および sftp）で接続できない場合は，次に示す手順で確認してください。

(1)　リモート接続経路の確立を確認する

本装置と運用端末間の通信経路が確立できていない可能性があります。ping コマンドを使用して，通信経路を確認してください。

(2)　SSH サーバのコンフィグレーションを確認する

SSH サーバに関するコンフィグレーションが未設定の場合は，本装置に対して SSH で接続できません。また，本装置の SSH サーバの設定と他装置の SSH クライアント側の設定で，認証方式などが一致しない場合は接続できません。

コンフィグレーションに，SSH サーバの情報が正しく設定されているか確認してください。リモートアクセス制御でアクセスリストを指定している場合は，許可されたアドレスの端末から接続しているかを確認してください。

(3)　本装置に登録したユーザ公開鍵が正しいか確認する

本装置に公開鍵認証でログインする場合は，本装置のコンフィグレーションに登録したユーザ公開鍵が正しい鍵かどうか，もう一度確認してください。

図 2-2　本装置でユーザ公開鍵を確認する例

```
(config)# show ip ssh
ip ssh
ip ssh authkey staff1 key1 "xxxxxx"                              <-1
!

(config)#
```

1. 正しいユーザ名で，正しい公開鍵が登録されているかどうかを確認します。

(4)　ログインアカウントのパスワードが設定済みか確認する

SSH では，認証時にパスワードを省略すると，ログインできません。アカウントにはパスワードを設定してください。

(5)　ログインユーザ数を確認する

本装置にログインできる最大ユーザ数を超えてログインしようとして，メッセージ種別：ACCESS，メッセージ識別子：06000003 のシステムメッセージが出力されていないかを，show logging コマンドで確認してください。

(6)　本装置に対して不正なアクセスがないか確認する

本装置の SSH サーバ機能では不正アクセスを防止するために，ログインユーザ数の制限のほかに，ログインするまでの認証途中の段階でのアクセス数や，ログイン完了までの時間（2 分間）を制限しています。したがって，show sessions コマンドで表示する本装置上のログインユーザ数が少ないのに SSH で接続でき

ない場合は，接続していてもログインしていないセッションが残っていることが考えられます。次の点を確認してください。

1. 本装置で show ssh logging コマンドを実行して，SSH サーバのトレースログを確認します。
   SSH サーバへ接続中のセッションが多いために接続が拒否された例を次の図に示します。この例は，接続していてもログインしていないセッションがある場合などに表示されます。

   図 2-3　SSH サーバへ接続中のセッションが多いために接続が拒否された例

```
> show ssh logging
20XX/04/14 18:50:04 sshd[662] A fatal error occurred. Login was rejected because there are
too many SSH sessions.
20XX/04/14 18:49:50 sshd[638] A fatal error occurred. Login was rejected because there are
too many SSH sessions.
20XX/04/14 18:49:00 sshd[670] A fatal error occurred. Login was rejected because there are
too many SSH sessions.
```

2. 接続していてもログインしていない不正なセッションの接続元を調査して，リモートアクセスを制限するなどの対応をしてください。
   なお，接続していてもログインしていない不正なセッションは 2 分後には解放されて，再度 SSH でログインできるようになります。急ぎの場合は，clear tcp コマンドで強制的に TCP セッションを切断して解放することもできます。

2.3.2　本装置に対してリモートでコマンドを実行できない

(1)　SSH クライアントの指定オプションを確認する

他装置の SSH クライアントから本装置に対して，SSH でログインしないで運用コマンドを実行（リモートでコマンドを実行）した場合に，コマンドの実行結果が表示されないでエラーが表示されることがあります。本装置に対するリモートからのコマンドの実行に失敗する例を次の図に示します。

図 2-4　本装置に対するリモートからのコマンドの実行に失敗する例

```
client-host> ssh operator@myhost show ip arp
operator@myhost's password: ******
Not tty allocation error.
client-host>
```

SSH でログインしないで本装置に対してリモートでコマンドを実行する場合は，-t パラメータで仮想端末を割り当てる必要があります。本装置に対するリモートからのコマンドの実行に成功する例を次の図に示します。

図 2-5　本装置に対するリモートからのコマンドの実行に成功する例

```
client-host> ssh -t operator@myhost show ip arp
operator@myhost's password: ******
Date 20XX/04/17 16:59:12 UTC
Total: 2 entries
 IP Address       Linklayer Address  Netif             Expire     Type
 192.168.0.1      0000.0000.0001     Eth2/3            3h55m56s   arpa
 192.168.0.2      0000.0000.0002     Eth2/3            3h58m56s   arpa
Connection to myhost closed.
client-host>
```

(2)　実行するコマンドの入力モードを確認する

SSH でログインしないで本装置に対してリモートで実行できるコマンドは，一般ユーザモードのコマンドだけです。装置管理者モードのコマンドを実行すると，エラーになります。

装置管理者モードのコマンドは SSH で本装置にログインして，装置管理者モードに移行してから実行してください。

(3) y/n の入力が必要なコマンドか確認する

reload コマンドなどの確認メッセージに対して"(y/n)"の入力を促すコマンドは，本装置に対してリモートで実行できません。このようなコマンドは, 確認メッセージを出力しないで強制実行するパラメータがあればそのパラメータを指定して実行するか，SSH で本装置にログインしてから実行してください。

2.3.3 本装置に対してセキュアコピーができない

一部の SSH クライアントでは，仮想端末を割り当てないで対話型のセッション（CLI）へログインし，ログイン後にファイルを転送するものがあります。本装置では，CLI へのログインはサポートしていません。クライアント側のトレースログを確認して, 本装置から次の図に示すメッセージが届いていないか確認してください。このような SSH クライアントからは，本装置に対してセキュアコピーができません。

図 2-6 本装置に対するセキュアコピーが失敗するクライアント側のトレースログ

```
Not tty allocation error.
```

なお，このような SSH クライアントでも，セキュア FTP をサポートしている場合はそれを使用するとファイルを転送できます。

2.3.4 公開鍵認証時のパスフレーズを忘れた

本装置に対して SSH の公開鍵認証でログインするときに入力するパスフレーズを忘れた場合は，そのユーザ鍵ペア（ユーザ公開鍵とユーザ秘密鍵）は使用できません。次に示す手順に従って対応してください。

(1) 本装置の SSH コンフィグレーションからユーザ公開鍵を削除する

本装置のコンフィグレーションコマンド ip ssh authkey を使用して，パスフレーズを忘れたユーザのユーザ公開鍵を削除してください。本装置の SSH コンフィグレーションからユーザ公開鍵を削除する例を次の図に示します。

図 2-7 本装置の SSH コンフィグレーションからユーザ公開鍵を削除する例

```
(config)# show ip ssh
ip ssh
ip ssh version 2
ip ssh authentication publickey
ip ssh authkey staff1 key1 "xxxxxxxxxx"
ip ssh authkey staff1 key2 "xxxxxxxxxx"
!

(config)# no ip ssh authkey staff1 key1

(config)# show ip ssh
ip ssh
ip ssh version 2
ip ssh authentication publickey
ip ssh authkey staff1 key2 "xxxxxxxxxx"
!
```

(2) SSH クライアント側端末のユーザ鍵ペアを削除する

SSH クライアント側の端末で，パスフレーズを忘れたユーザのユーザ鍵ペア（ユーザ公開鍵とユーザ秘密鍵）を削除して，登録も解除してください。再度，公開鍵認証を使用する場合は，使用する SSH クライアントでユーザ鍵ペアを再作成したあと，本装置の SSH コンフィグレーションで改めてユーザ公開鍵を登録してください。

2.3.5　接続時にホスト公開鍵変更の警告が表示される

他装置から本装置に対して SSH で接続したときに，「@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @」のメッセージが表示される場合は，前回の接続時から本装置側のホスト公開鍵が変更されていることを示しています。

このメッセージが表示されたときは，悪意のある第三者が本装置になりすましているおそれもあるため，次の手順に従って十分に確認してから SSH で接続してください。

(1)　本装置の装置管理者へ問い合わせる

次の内容について，装置管理者へ問い合わせて確認してください。

- set ssh hostkey コマンドを使用して，意図的にホスト鍵ペアを変更していないか
- 装置構成の変更などをしていないか

本装置で装置管理者がホスト鍵ペアを変更していない場合は，なりすまし攻撃にあっている危険性，またはほかのホストへ接続しているおそれがあるため，SSH 接続を中断し，ネットワーク管理者に連絡してください。SSH での接続を中断する例を次の図に示します。

図 2-8　SSH での接続を中断する例

```
client-host> ssh operator@myhost
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
   :
   :
Are you sure you want to continue connecting? (y/n): n      <-1
Host key verification failed.
client-host>
```

1. ここで「n」を入力して，接続しません。

なりすましの危険性がなく，本装置のホスト公開鍵が変更されていた場合は，以降の手順に従って再接続してください。

(2)　ホスト公開鍵が変更された場合に再接続する

SSH クライアントから SSHv2 プロトコルを使用して，ホスト鍵ペアが変更された本装置の SSH サーバに接続します。より安全に接続するために，次の手順に従って，接続しようとしている本装置の SSH サーバが正しい接続対象のホストであることを Fingerprint で確認します。

1. Fingerprint の事前確認
   あらかじめ本装置にログインして，show ssh hostkey コマンドで Fingerprint を確認します。コンソール接続など，ネットワーク経由以外の安全な方法で確認すると，より安全です。
2. Fingerprint をクライアントユーザへ通知
   確認した Fingerprint を，SSH クライアントユーザに通知します。郵送や電話など，ネットワーク経由以外の安全な方法で通知すると，より安全です。
3. Fingerprint を確認して SSH 接続
   クライアントでは，本装置の SSH サーバに対して SSH 接続したときに表示される Fingerprint が，手順 2.で通知されたものと同じであることを確認してから，接続します。
   クライアントによっては，Fingerprint が HEX 形式で表示されるものと bubblebabble 形式で表示されるものがあります。また，SSHv1 では Fingerprint をサポートしていないものもあります。クライアントに合った形式で確認してください。

(3)　ユーザのホスト公開鍵データベースを登録または削除する

使用する SSH クライアントによっては，ユーザのホスト公開鍵データベースに登録された，本装置の SSH サーバのホスト公開鍵が自動で削除されないで，接続するたびに警告が表示される，または接続できない場合があります。このような場合は，手動でファイルを編集または削除して，再接続してください。

2.3.6　系切替後に SSH で接続できない

この項目は，BCU を二重化構成で運用している場合だけの確認項目です。コンソールまたは telnet で本装置にログインして，次に示す内容を確認してください。

(1)　synchronize コマンドで確認する

系切替後の新運用系 BCU で synchronize コマンドを実行して，コンフィグレーションの情報が新待機系（旧運用系）BCU と差分がないか確認してください。

図 2-9　synchronize コマンドによる確認例

```
> enable
# synchronize diff

<Synchronize Status>
(1) configuration                  [OK]            <-1
(2) home directory files           [OK]
(3) SSH hostkey files              [OK]

#
```

1. コンフィグレーションファイル情報

(2)　SSH コンフィグレーションを確認する

系切替後の新運用系 BCU でコンフィグレーションコマンド show ip ssh を実行して，SSH 機能のコンフィグレーションの内容を確認してください。

本装置のコンフィグレーションで SSH サーバに関する情報が未設定の場合は，本装置に対して SSH で接続できません。また，本装置の SSH サーバの設定と他装置の SSH クライアント側の設定で，認証方式などが一致しない場合は接続できません。

(3)　ユーザアカウントを確認する

系切替後の新運用系 BCU で，ログインしようとしているユーザアカウントが存在しない場合，SSH のローカル認証で接続できません。

SSH でローカル認証を使用して本装置にログインできるアカウントは，コンフィグレーションコマンド username で作成された，パスワードが設定されているユーザアカウントだけです。SSH では，認証時にパスワードを省略するとログインできません。なお，本装置に設定されているユーザアカウントは show users コマンドで確認できます。

(4)　SSH ホスト鍵の存在を確認する

次の条件をどちらも満たす場合，系切替後の新運用系 BCU にホスト鍵が存在しないため，SSH で接続できません。

- 系切替後の新運用系 BCU が，系切替前に旧運用系 BCU と同時に初期起動されなかった
- 旧運用系 BCU の synchronize コマンドで一度もホスト鍵を同期していない

新運用系 BCU で show ssh hostkey コマンドを実行して，ホスト鍵が存在するか確認してください。次の例のようにエラーになった場合は，ホスト鍵が存在しません。この場合は，set ssh hostkey コマンドを実行して，ホスト鍵を生成してください。

図 2-10　本装置でのホスト鍵の存在確認例

```
# show ssh hostkey
Date 20XX/01/20 12:00:00 UTC
The command cannot be executed. Wait a while, and then try again. If necessary, use 'set ssh ho
stkey' to set a key. (reason = show ssh hostkey [error code:01(/usr/local/etc/ssh_host_key.pub)
])
#
```

2.4 コンフィグレーションのトラブル

2.4.1 コンフィグレーションモードから装置管理者モードに戻れない

コンフィグレーションモードから装置管理者モードに戻れなくなった場合は，次に示す方法で対応してください。

(1) コンソールとの接続時

次の手順で，該当するユーザを強制的にログアウトさせてください。

[実行例]

1. show sessions コマンドで，該当するユーザのログイン番号を確認します。

```
(config)# $show sessions
operator console admin 1 Jan 6 14:16
```

下線部が該当するユーザのログイン番号です。

2. killuser コマンドで，該当するユーザを強制的にログアウトさせます。<login no.>パラメータには，手順 1.で調べたログイン番号を指定してください。

```
(config)# $killuser 1
```

(2) リモート運用端末との接続時

いったんリモート運用端末を終了させたあと，再接続してください。

ログインした状態のままになっているユーザがいる場合は，「表 2-3　リモート運用端末との接続トラブルおよび対応」の項番 4 に従って対処してください。

2.4.2 コンフィグレーションが反映されない

(1) ランニングコンフィグレーションに反映されない

コンフィグレーションを編集しても，ランニングコンフィグレーションにまったく反映されない場合は，コミットモードを確認してください。コミットモードが手動コミットモードになっていると，編集したコンフィグレーションがすぐにランニングコンフィグレーションに反映されません。

[実行例]

1. コンフィグレーションコマンド status を実行して，コミットモードを確認します。

```
(config)# status
File name          : running-config
Commit mode        : Manual commit
Last modified time : Thu Oct 11 12:00:00 20XX UTC by operator (not modified)
Buffer             : Total     XXXXXXXXXX Bytes
                     Available XXXXXXXXXX Bytes (XXXX%)
                     Fragments XX Bytes (XXXX%)
Login user         : USER  operator  LOGIN  Fri Oct 12 12:00:00 20XX UTC edit
```

Commit mode が Manual commit の場合，手動コミットモードが設定されています。

手動コミットモードで，編集した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へ反映するには，コンフィグレーションコマンド commit を実行してください。

(2) BGP4 経路または BGP4+経路の学習または広告に反映されない

経路フィルタリングのコンフィグレーションを変更したあと，変更した内容がランニングコンフィグレーションに反映されているが，BGP4 経路または BGP4+経路の学習または広告にその内容が反映されていない場合は，clear ip bgp または clear ipv6 bgp コマンドに* { in | out | both }パラメータを指定して，実行してください。

2.5　NTP/SNTP の通信障害

2.5.1　NTP による時刻同期ができない

NTP による時刻同期ができない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 2-4　NTP の障害解析方法

項番	確認内容・コマンド	対応
1	本装置が NTP サーバと同期していることを確認してください。 • show ntp associations	本装置が NTP サーバと同期していて，本装置に対して NTP クライアントが同期していない場合は, NTP クライアントの設定を確認してください。
		本装置を NTP サーバと同期させないで，本装置に対して NTP クライアントを同期させる場合は, コンフィグレーションコマンド ntp master を設定してください。
		本装置が NTP サーバと同期していない場合は，項番 2 へ。
2	NTP サーバと IPv4 で通信できることを確認してください。 ループバックインタフェースに IPv4 アドレスを設定している場合は，source パラメータでループバックインタフェースの IPv4 アドレスを指定してください。 • ping	NTP サーバと IPv4 で通信できない場合は,「5.1　IPv4 ネットワークの通信障害」を参照してください。
		NTP サーバと IPv4 で通信できる場合は，項番 3 へ。
3	NTP のコンフィグレーションでアクセスが許可されているか，許可されている場合は，フィルタまたは QoS によって NTP パケットが廃棄されていないか確認してください。	フィルタおよび QoS の確認方法と対応については,「8.1　パケット廃棄の確認」を参照してください。
		NTP パケットが廃棄されていない場合は，項番 4 へ。
4	本装置と NTP サーバとの時刻差を確認してください。	本装置と NTP サーバとの時刻差が 1000 秒以上ある場合は，set clock コマンドを使用して本装置の時刻を NTP サーバと合わせてください。
		NTP サーバとタイムゾーンまたはサマータイムの設定が異なる場合は，UTC に変換した時刻が合うように，NTP サーバと本装置の時刻を設定してください。

2.5.2　SNTP による時刻同期ができない

SNTP による時刻同期ができない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 2-5　SNTP の障害解析方法

項番	確認内容・コマンド	対応
1	本装置が SNTP サーバと同期していることを確認してください。 • show sntp status	本装置が SNTP サーバと同期していて，本装置に対して SNTP クライアントが同期していない場合は，SNTP クライアントの設定を確認してください。

項番	確認内容・コマンド	対応
		本装置を SNTP サーバと同期させないで，本装置に対して SNTP クライアントを同期させる場合は，コンフィグレーションコマンド sntp master を設定してください。
		本装置が SNTP サーバと同期していない場合は，項番 2 へ。
2	SNTP サーバと IPv4 または IPv6 で通信できることを確認してください。 ループバックインタフェースに IPv4 アドレスまたは IPv6 アドレスを設定している場合は，source パラメータでループバックインタフェースの IPv4 アドレスまたは IPv6 アドレスを指定してください。 • ping • ping ipv6	SNTP サーバと IPv4 または IPv6 で通信できない場合は，「5.1　IPv4 ネットワークの通信障害」または「5.2　IPv6 ネットワークの通信障害」を参照してください。
		SNTP サーバと IPv4 または IPv6 で通信できる場合は，項番 3 へ。
3	SNTP のコンフィグレーションでアクセスが許可されているか，許可されている場合は，フィルタまたは QoS によって SNTP パケットが廃棄されていないか確認してください。	フィルタおよび QoS の確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。
		SNTP パケットが廃棄されていない場合は，項番 4 へ。
4	本装置と SNTP サーバとの時刻差を確認してください。	本装置と SNTP サーバとの時刻差が 1000 秒以上ある場合は，set clock コマンドを使用して本装置の時刻を SNTP サーバと合わせてください。
		SNTP サーバとタイムゾーンまたはサマータイムの設定が異なる場合は，UTC に変換した時刻が合うように，SNTP サーバと本装置の時刻を設定してください。

2.6　MC のトラブル

2.6.1　MC の状態が表示されない

show system コマンドまたは show mc コマンドで MC に"--------"と表示される場合は，次の表に従って確認してください。

表 2-6　MC に"--------"と表示される場合の対応方法

項番	確認内容・コマンド	対応
1	ACC LED を確認してください。	ACC LED が緑点灯の場合は，ほかのプロセスが MC にアクセス中の可能性があります。ACC LED が消灯したあと，コマンドを再実行してください。
		ACC LED が緑点灯でない場合は，項番 2 へ。
2	一度 MC を抜いて，再度挿入してください。	MC を抜き差ししたあと，コマンドを再実行してください。 MC を挿入する際には，MC および装置のメモリカードスロットにほこりが付着していないか確認してください。ほこりが付着しているときは，乾いた布などでほこりを取ってから MC を挿入してください。
		MC の抜き差しを数回繰り返しても現象が改善しない場合は，項番 3 へ。
3	MC を交換してください。	MC を交換したあと，コマンドを再実行してください。 MC を交換しても現象が改善しない場合は，メモリカードスロットが故障している可能性があります。BCU を交換してください。

2.6.2　MC へのアクセス時にエラーが発生する

MC へアクセスするコマンドの実行時にメッセージ"The memory card was not found."が表示される場合は，次の表に従って確認してください。

表 2-7　メッセージ"The memory card was not found."が表示される場合の対応方法

項番	確認内容・コマンド	対応
1	ACC LED を確認してください。	ACC LED が緑点灯の場合は，ほかのプロセスが MC にアクセス中の可能性があります。ACC LED が消灯したあと，コマンドを再実行してください。
		ACC LED が緑点灯でない場合は，項番 2 へ。
2	一度 MC を抜いて，再度挿入してください。	MC を抜き差ししたあと，コマンドを再実行してください。 MC を挿入する際には，MC および装置のメモリカードスロットにほこりが付着していないか確認してください。ほこりが付着しているときは，乾いた布などでほこりを取ってから MC を挿入してください。

項番	確認内容・コマンド	対応
		MC の抜き差しを数回繰り返しても現象が改善しない場合は，項番 3 へ。
3	MC を交換してください。	MC を交換したあと，コマンドを再実行してください。 MC を交換しても現象が改善しない場合は，メモリカードスロットが故障している可能性があります。BCU を交換してください。

2.7　BCU の二重化構成によるトラブル

2.7.1　運用系 BCU の切替ができない

運用系 BCU と待機系 BCU の切替ができない場合は，次の表に従って確認してください。

表 2-8　運用系 BCU の切替時のトラブルおよび対応

項番	切替不可要因	確認内容	
1	待機系 BCU が起動していない。 待機系 BCU の STATUS LED を確認してください。	赤点灯	待機系 BCU に障害が発生しています。待機系 BCU のボードを交換してください。
		消灯	待機系 BCU が起動していません。運用系 BCU から inactivate bcu standby および activate bcu standby コマンドを実行して，待機系 BCU を起動してください。
		緑点滅	待機系 BCU が起動中です。緑点灯になるまでしばらく待ってください。
		緑点灯	待機系 BCU は起動しているため，別の切替不可要因が考えられます。ほかの項番を参照してください。
2	待機系 BCU の切替準備ができていない。 運用系 BCU にログインして，show system コマンドで待機系 BCU の状態を確認してください。	fault	待機系 BCU に障害が発生しています。待機系 BCU のボードを交換してください。
		inactive	待機系 BCU の起動が抑止されています。activate bcu standby コマンドを実行して，待機系 BCU を起動してください。
		notconnect	待機系 BCU が搭載されていません。待機系 BCU を搭載したあと，activate bcu standby コマンドを実行して待機系 BCU を起動してください。
		initialize	待機系 BCU が起動中です。起動が完了するまでしばらく待ってください。
		standby(configuration discord)	運用系 BCU と待機系 BCU の間でコンフィグレーションが一致していません。save コマンドまたは synchronize コマンドを使用して，BCU 間のコンフィグレーションを一致させてください。
		notsupport	未サポートの BCU が搭載されています。待機系 BCU のボードを交換してください。
		standby	別の切替不可要因が考えられます。ほかの項番を参照してください。
3	コンフィグレーションの操作をしている。操作中に運用コマンドで系切替をするとコマンドが失敗する。 コンフィグレーションの操作中でないか確認してください。	コンフィグレーションの操作中は運用コマンドによる系切替が抑止されます。運用系 BCU からコンフィグレーションコマンド status を実行して，コンフィグレーションを操作中のユーザをすべてログアウトさせたあと，運用コマンドによる系切替をしてください。	

2.8　SNMP の通信障害

2.8.1　SNMP マネージャから MIB が取得できない

次に示す説明に従って，コンフィグレーションの設定を確認してください。

(1)　SNMPv1 または SNMPv2C を使用する場合

コンフィグレーションコマンド show ip access-list を実行して，アクセスリストに SNMP マネージャの IP アドレスが設定されているか確認してください。アクセスリストに SNMP マネージャの IP アドレスが設定されてない場合は，SNMP マネージャの IP アドレスを追加してください。

そのあと，コンフィグレーションコマンド show snmp-server を実行して，コミュニティ名とアクセスリストが正しく設定されているか確認してください。正しく設定されていない場合は, コンフィグレーションコマンド snmp-server community 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。

[実行例]

```
(config)# show ip access-list
 ip access-list standard ACL
 10 permit 20.1.1.1
 !
(config)# show snmp-server
 snmp-server community "event-monitor" ro ACL
 !
(config)#
```

(2)　SNMPv3 を使用する場合

コンフィグレーションコマンド show snmp-server を実行して，本装置のコンフィグレーションに SNMP に関する情報が正しく設定されているか確認してください。正しく設定されていない場合は, 次のコンフィグレーションコマンドを実行して，SNMP に関する情報を設定してください。

- snmp-server engineID local
- snmp-server group
- snmp-server user
- snmp-server view

[実行例]

```
(config)# show snmp-server
  snmp-server engineID local "engine-ID"
  snmp-server group "v3group" v3 priv read "view1" write "view1"
  snmp-server user "v3user" "v3group" v3 auth md5 "abc*_1234" priv des "xyz/+6789"
  snmp-server view "view1" 1.3.6.1.2.1.1 included
  !
(config)#
```

2.8.2　SNMP マネージャでトラップが受信できない

次に示す説明に従って，コンフィグレーションの設定を確認してください。

また，一部の SNMP マネージャシステムでは，SNMPv2C または SNMPv3 で送信された ospf，bgp のトラップを受信できない場合があります。その場合は，「MIB レファレンス」に記載されている各トラップのオブジェクト ID に合わせて，SNMP マネージャのトラップの受信設定を見直してください。

(1) SNMPv1 または SNMPv2C を使用する場合

コンフィグレーションコマンド show snmp-server を実行して，本装置のコンフィグレーションに SNMP マネージャおよびトラップに関する情報が設定されているか確認してください。設定されていない場合は，コンフィグレーションコマンド snmp-server host を実行して，SNMP マネージャおよびトラップに関する情報を設定してください。

[実行例]

```
(config)# show snmp-server
 snmp-server host    192.0.2.0 traps "event-monitor" snmp
 !
(config)#
```

(2) SNMPv3 を使用する場合

コンフィグレーションコマンド show snmp-server を実行して，本装置のコンフィグレーションに SNMP およびトラップに関する情報が正しく設定されているか確認してください。正しく設定されていない場合は，次のコンフィグレーションコマンドを実行して，SNMP およびトラップに関する情報を設定してください。

- snmp-server engineID local
- snmp-server group
- snmp-server host
- snmp-server user
- snmp-server view

[実行例]

```
(config)# show snmp-server
  snmp-server engineID local "engine-ID"
  snmp-server group "v3group" v3 priv notify "view1"
  snmp-server host    192.0.2.0 traps "v3user" version 3 priv snmp
  snmp-server user "v3user" "v3group" v3 auth md5 "abc*_1234" priv des "xyz/+6789"
  snmp-server view "view1" 1.3.6.1 included
  !
(config)#
```

2.8.3 SNMP マネージャでインフォームが受信できない

コンフィグレーションコマンド show snmp-server を実行して，本装置のコンフィグレーションに SNMP マネージャおよびインフォームに関する情報が設定されているか確認してください。設定されていない場合は，コンフィグレーションコマンド snmp-server host を実行して，SNMP マネージャおよびインフォームに関する情報を設定してください。

[実行例]

```
(config)# show snmp-server
  snmp-server host 192.0.2.0 informs "event-monitor" snmp
 !
(config)#
```

一部の SNMP マネージャシステムでは，SNMPv2C または SNMPv3 で送信された ospf，bgp のインフォームを受信できない場合があります。その場合は，「MIB レファレンス」に記載されている各インフォームのオブジェクト ID に合わせて，SNMP マネージャのインフォームの受信設定を見直してください。

3 ネットワークインタフェースのトラブルシュート

この章では，ネットワークインタフェースで障害が発生した場合の対処について説明します。

3.1　イーサネットの通信障害

3.1.1　イーサネットポートの接続ができない

通信障害の原因がイーサネットポートにあると考えられる場合は，NIF の状態，ポートの状態，ポートの統計情報の順に確認してください。

(1)　NIF の状態確認

1. ログの確認
   ログの内容および対応については，「メッセージ・ログレファレンス」を参照してください。
2. NIF の状態による原因の切り分け
   show interfaces コマンドで NIF の状態を確認して，次の表に従って原因を切り分けてください。

表 3-1　NIF の状態の確認および対応

項番	NIF の状態	原因	対応
1	active	該当 NIF は正常に動作中である	「表 3-2　ポートの状態の確認および対応」に従って，ポートの状態を確認してください。
2	notconnect	該当 NIF が搭載されていない	NIF を搭載してください。
3	inactive	inactivate コマンドが設定されている	activate コマンドで該当 NIF の状態を active にしてください。
		NIF の搭載に誤りがある	show version コマンドで，搭載されている PSU と NIF の組み合わせを確認してください。 PSU と NIF の組み合わせによる NIF の搭載条件については，「コンフィグレーションガイド」を参照してください。
4	fault	該当 NIF に障害が発生している	show logging コマンドで表示される該当 NIF のログについて，「メッセージ・ログレファレンス」を参照して，記載内容に従って対応してください。
5	initialize	該当 NIF が初期化中である	初期化が完了するまで待ってください。
6	disable	コンフィグレーションコマンドで no power enable が設定されている	使用する NIF が搭載されていることを確認したあと，コンフィグレーションコマンド power enable を設定して該当 NIF の状態を active にしてください。
7	power shortage	電力不足による運用停止状態である	show environment コマンドで電源の情報，および装置の余剰電力を確認してください。 • PS の状態が fault の場合は，電源機構を交換してください。 • PS の状態が active の場合は，装置の余剰電力を確認して，電源機構を追加してください。
8	notsupport	本装置で未サポートの NIF が搭載されている	NIF を交換してください。

項番	NIF の状態	原因	対応
		ソフトウェアバージョンで未サポートの NIF が搭載されている	NIF 種別とソフトウェアのバージョンを確認して，NIF を交換するか，ソフトウェアをアップデートしてください。

(2)　ポートの状態確認

1. ログの確認
   ログの内容および対応については，「メッセージ・ログレファレンス」を参照してください。
2. ポートの状態による原因の切り分け
   show interfaces コマンドでポートの状態を確認して，次の表に従って原因を切り分けてください。

表 3-2　ポートの状態の確認および対応

項番	ポートの状態	原因	対応
1	active up	該当ポートは正常に動作中である	ありません。
2	active down	該当ポートに回線障害が発生している	show logging コマンドで表示される該当ポートのログについて，「メッセージ・ログレファレンス」を参照して，記載内容に従って対応してください。
3	inactive	inactivate コマンドが設定されている	active up にする場合は，使用するポートにケーブルが接続されていることを確認したあと，activate コマンドで該当ポートを active 状態にしてください。
		ネットワーク監視またはネットワーク管理の機能が動作した	「8.2　ポート inactive 状態の確認」を参照してください。
4	fault	該当ポートのポート部分のハードウェアに障害が発生している	show logging コマンドで表示される該当ポートのログについて，「メッセージ・ログレファレンス」を参照して，記載内容に従って対応してください。
5	initialize	該当ポートが初期化中である	初期化が完了するまで待ってください。
6	standby	リンクアグリゲーションのスタンバイリンク機能によって待機している	リンクアグリゲーションのスタンバイリンク機能によって standby 状態になっているため，正常な動作です。 スタンバイリンク機能については，show channel-group コマンドで detail パラメータを指定して確認してください。
7	disable(track)	トラッキング連携によって運用停止されている	コンフィグレーションで連携を指定した静的監視トラックの状態に合わせて，運用停止状態になっています。正常な動作です。 トラック状態を確認するには，show track コマンドを使用してください。トラック状態が想定される状態でない場合は，「6.3　トラッキング機能のトラブル」を参照してください。

項番	ポートの状態	原因	対応
8	disable	コンフィグレーションコマンド shutdown が設定されている	active up にする場合は，使用するポートにケーブルが接続されていることを確認したあと，コンフィグレーションコマンドで no shutdown を設定して該当ポートを active 状態にしてください。
9	suspend	次の要因でポートの起動が抑止されている • SFU の運用枚数不足 • PSU の初期化中 • NIF が運用系として稼働中以外	show system コマンドで SFU，PSU，および NIF の状態を確認してください。 • active になっている SFU の枚数を確認してください。 • PSU の状態が initialize の場合は，PSU の初期化が完了するまで待ってください。 • NIF の状態が initialize の場合は，NIF の初期化が完了するまで待ってください。
10	unused	コンフィグレーションが生成されていない	取り付けた NIF に対応するポートのコンフィグレーションが生成されるまで待ってください。
11	mismatch	取り付けた NIF に収容されているイーサネット種別と，ランニングコンフィグレーションのイーサネット種別が一致していない	• 取り付けた NIF の種別を確認してください。取り付けた NIF の種別が誤っている場合は，NIF を交換してください。 • show running-config コマンドでランニングコンフィグレーションを確認してください。ランニングコンフィグレーションが誤っている場合は，取り付け前のポートのコンフィグレーションを削除してください。 コンフィグレーションの削除については，「コンフィグレーションガイド」を参照してください。
12	show interfaces コマンドではポートが表示されない	NIF が搭載されていないか，NIF を正しく認識できていない	「表 3-1　NIF の状態の確認および対応」に従って，NIF の状態を確認してください。

(3)　統計情報の確認

show port statistics コマンドを実行して，本装置に搭載されている全ポートの送受信パケット数および送受信廃棄パケット数を確認してください。

図 3-1　ポートの統計情報の表示

```
> show port statistics
Date 20XX/04/01 12:00:00 UTC
Port Counts: 12
Port  Name          Status   Packets                    Tx                   Rx
 1/1  geth1/1       down     Ucast                       0                    0
                             Mcast                       0                    0
                             Bcast                       0                    0
                             Discard                     0                    0
 1/2  geth1/2       down     Ucast                       0                    0
                             Mcast                       0                    0
                             Bcast                       0                    0
                             Discard                     0                    0
 1/3  geth1/3       down     Ucast                       0                    0
                             Mcast                       0                    0
                             Bcast                       0                    0
```

```
                  Discard              0              0
     :
>
```

なお，本コマンド実行時に Discard の値が 0 より大きい場合は，パケットが廃棄される障害が発生しています。show interfaces コマンドで該当ポートの詳細情報を確認してください。

3.1.2　SFU/PSU のトラブル

通信障害の原因が SFU または PSU にあると考えられる場合は，次の内容に従って確認してください。

(1)　SFU の状態確認

1. ログの確認
   ログの内容および対応については，「メッセージ・ログレファレンス」を参照してください。
2. SFU の状態による原因の切り分け
   show system コマンドで SFU の状態を確認して，次の表に従って原因を切り分けてください。

表 3–3　SFU の状態の確認および対応

項番	SFU の状態	原因	対応
1	active	該当 SFU は運用系として正常に動作中である	「3.1.1　イーサネットポートの接続ができない」を参照してください。 active になっている SFU の枚数が少ないと，帯域が減少することがあります。
2	fault	該当 SFU に障害が発生している	show logging コマンドで表示される該当 SFU のログについて，「メッセージ・ログレファレンス」を参照して，記載内容に従って対応してください。
3	initialize	該当 SFU が初期化中である	初期化が完了するまで待ってください。
4	inactive	inactivate sfu コマンドが設定されている	activate sfu コマンドで該当 SFU の状態を active にしてください。
5	notsupport	本装置で未サポートの SFU が搭載されている	SFU を交換してください。
6	disable	コンフィグレーションコマンドで no power enable が設定されている	使用する SFU が搭載されていることを確認したあと，コンフィグレーションコマンド power enable を設定して該当 SFU の状態を active にしてください。
7	notconnect	該当 SFU が搭載されていない	SFU を搭載してください。

(2)　PSU の状態確認

1. ログの確認
   ログの内容および対応については，「メッセージ・ログレファレンス」を参照してください。
2. PSU の状態による原因の切り分け
   show system コマンドで PSU の状態を確認して，次の表に従って原因を切り分けてください。

表 3-4 PSU の状態の確認および対応

項番	PSU の状態	原因	対応
1	active	該当 PSU は正常に動作中である	「3.1.1 イーサネットポートの接続ができない」を参照してください。
2	fault	該当 PSU に障害が発生している	show logging コマンドで表示される該当 PSU のログについて，「メッセージ・ログレファレンス」を参照して，記載内容に従って対応してください。
3	initialize	該当 PSU が初期化中である	初期化が完了するまで待ってください。
4	inactive	inactivate psu コマンドが設定されている	activate psu コマンドで該当 PSU の状態を active にしてください。
5	notsupport	本装置で未サポートの PSU が搭載されている	PSU を交換してください。
6	power shortage	電力不足による運用停止状態である	show environment コマンドで電源の情報，および装置の余剰電力を確認してください。 • PS の状態が fault の場合は，電源機構を交換してください。 • PS の状態が active の場合は，装置の余剰電力を確認して，電源機構を追加してください。
7	disable	コンフィグレーションコマンドで no power enable が設定されている	使用する PSU が搭載されていることを確認したあと，コンフィグレーションコマンド power enable を設定して該当 PSU の状態を active にしてください。
8	notconnect	該当 PSU が搭載されていない	PSU を搭載してください。

3.1.3 10BASE-T/100BASE-TX/1000BASE-T のトラブル

10BASE-T/100BASE-TX/1000BASE-T でトラブルが発生した場合は，次の順序で障害を切り分けてください。

1. ログの確認
   ログの内容および対応については，「メッセージ・ログレファレンス」を参照してください。
2. 障害解析方法に従った原因の切り分け
   次の表に示す障害解析方法に従って原因を切り分けてください。

表 3-5 10BASE-T/100BASE-TX/1000BASE-T のトラブル発生時の障害解析方法

項番	確認内容・コマンド	原因	対応
1	該当ポートの障害統計情報で，Link down がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • show interfaces	回線品質が低下している	ケーブルの種別が正しいか確認してください。種別については，「ハードウェア取扱説明書」を参照してください。
			本装置の設定が次の場合は，ピンマッピングが MDI-X であるか確認してください。 • 該当ポートの設定が固定接続である

項番	確認内容・コマンド	原因	対応
			• 該当ポートの設定がオートネゴシエーションかつ自動 MDI/MDIX 機能を無効にしている
			ケーブル長を確認してください。ケーブル長については，「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。
			本装置でサポートしている接続インタフェースに交換してください。本装置でサポートしている接続インタフェースについては，「コンフィグレーションガイド」を参照してください。
2	該当ポートの受信系エラー統計情報で，CRC errors または Symbol errors がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • show interfaces	回線品質が低下している	ケーブルの種別が正しいか確認してください。種別については，「ハードウェア取扱説明書」を参照してください。
			本装置の設定が次の場合は，ピンマッピングが MDI-X であるか確認してください。 • 該当ポートの設定が固定接続である • 該当ポートの設定がオートネゴシエーションかつ自動 MDI/MDIX 機能を無効にしている
			ケーブル長を確認してください。ケーブル長については，「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。
			本装置でサポートしている接続インタフェースに交換してください。本装置でサポートしている接続インタフェースについては，「コンフィグレーションガイド」を参照してください。
3	該当ポートの障害統計情報で，MDI cross over changed がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • show interfaces	ケーブルのピンマッピングが不正である	ピンマッピングを正しく修正してください。ピンマッピングについては，「コンフィグレーションガイド」を参照してください。
4	該当ポートのポート情報で，回線種別および回線速度が正しいか確認してください。不正な回線種別または回線速度の場合，原因と対応欄を参照してください。 • show interfaces	ケーブルが適合していない	ケーブルの種別が正しいか確認してください。種別については，「ハードウェア取扱説明書」を参照してください。
		回線速度と duplex が相手装置と不一致である	コンフィグレーションコマンド speed および duplex の設定を相手装置と合わせてください。
		上記以外の場合	オートネゴシエーションで特定の速度を使用する場合は，オートネゴシエーションの回線速度を設定してください。詳細は，「コンフィグレーションガイド」を参照してください。

項番	確認内容・コマンド	原因	対応
5	該当ポートの受信系エラー統計情報で，Long frames がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • show interfaces	受信できるフレーム長を超えたパケットを受信している	ジャンボフレームの設定を相手装置と合わせてください。

3.1.4 1000BASE-X のトラブル

1000BASE-X でトラブルが発生した場合は，次の順序で障害を切り分けてください。

1. ログの確認
   ログの内容および対応については，「メッセージ・ログレファレンス」を参照してください。
2. 障害解析方法に従った原因の切り分け
   次の表に示す障害解析方法に従って原因を切り分けてください。

表 3-6　1000BASE-X のトラブル発生時の障害解析方法

項番	確認内容・コマンド	原因	対応
1	該当ポートの障害統計情報で，Link down または Signal detect errors がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • show interfaces	受信側の回線品質が低下している	光ファイバの種別を確認してください。種別については，「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合は，減衰値を確認してください。光レベルについては，「ハードウェア取扱説明書」を参照してください。
			ケーブル長を確認してください。ケーブル長については，「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合は，汚れを拭き取ってください。
			トランシーバの接続が正しいか確認してください。
			コンフィグレーションコマンド speed および duplex の設定を相手装置と合わせてください。
			相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルについては，「ハードウェア取扱説明書」を参照してください。
2	該当ポートの受信系エラー統計情報で，CRC errors または Symbol errors がカウントされていないか確認してください。カウントされている場	受信側の回線品質が低下している	光ファイバの種別を確認してください。種別については，「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合は，減衰値を確認してください。光レベルについては，「ハードウェア取扱説明書」を参照してください。

項番	確認内容・コマンド	原因	対応
	合，原因と対応欄を参照してください。 • show interfaces		ケーブル長を確認してください。ケーブル長については，「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合は，汚れを拭き取ってください。
			トランシーバの接続が正しいか確認してください。
			コンフィグレーションコマンド speed および duplex の設定を相手装置と合わせてください。
			相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルについては，「ハードウェア取扱説明書」を参照してください。
3	1000BASE-BX などの 1 芯の光ファイバを使用している場合，相手側のトランシーバと組み合わせが正しいか確認してください。	トランシーバの組み合わせが不正である	1000BASE-BX を使用する場合，トランシーバは U タイプと D タイプを対向して使用する必要があります。トランシーバの種別が正しいか確認してください。
4	該当ポートの受信系エラー統計情報で，Long frames がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • show interfaces	受信できるフレーム長を超えたパケットを受信している	ジャンボフレームの設定を相手装置と合わせてください。

3.1.5　10GBASE-R/40GBASE-R/100GBASE-R のトラブル

10GBASE-R，40GBASE-R，または 100GBASE-R でトラブルが発生した場合は，次の順序で障害を切り分けてください。

1. ログの確認
   ログの内容および対応については，「メッセージ・ログレファレンス」を参照してください。
2. 障害解析方法に従った原因の切り分け
   次の表に示す障害解析方法に従って原因を切り分けてください。

表 3–7　10GBASE-R/40GBASE-R/100GBASE-R のトラブル発生時の障害解析方法

項番	確認内容・コマンド	原因	対応
1	該当ポートの障害統計情報で，Signal detect errors，LOS of sync，HI_BER，または LF がカウントされていないか確認してください。カウ	受信側の回線品質が低下している	光ファイバの種別を確認してください。種別については，「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合は，減衰値を確認してください。光レベルについては，「ハードウェア取扱説明書」を参照してください。

項番	確認内容・コマンド	原因	対応
	ントされている場合，原因と対応欄を参照してください。 • show interfaces		ケーブル長を確認してください。ケーブル長については，「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合は，汚れを拭き取ってください。
			トランシーバの接続が正しいか確認してください。
			トランシーバを相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルについては，「ハードウェア取扱説明書」を参照してください。
2	該当ポートの受信系エラー統計情報で，CRC errors または Symbol errors がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • show interfaces	受信側の回線品質が低下している	光ファイバの種別を確認してください。種別については，「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合は，減衰値を確認してください。光レベルについては，「ハードウェア取扱説明書」を参照してください。
			ケーブル長を確認してください。ケーブル長については，「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合は，汚れを拭き取ってください。
			トランシーバの接続が正しいか確認してください。
			トランシーバを相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルについては，「ハードウェア取扱説明書」を参照してください。
3	該当ポートの障害統計情報で，RF がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • show interfaces	送信側の回線品質が低下している	光ファイバの種別を確認してください。種別については，「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合は，減衰値を確認してください。光レベルについては，「ハードウェア取扱説明書」を参照してください。
			ケーブル長を確認してください。ケーブル長については，「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合は，汚れを拭き取ってください。
			トランシーバの接続が正しいか確認してください。
			トランシーバを相手装置のセグメント規格と合わせてください。

項番	確認内容・コマンド	原因	対応
			光レベルが正しいか確認してください。光レベルについては，「ハードウェア取扱説明書」を参照してください。
4	該当ポートの受信系エラー統計情報で，Long frames がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • show interfaces	受信できるフレーム長を超えたパケットを受信している	ジャンボフレームの設定を相手装置と合わせてください。

3.2　リンクアグリゲーション使用時の通信障害

リンクアグリゲーション使用時に通信できない，または縮退運転している場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 3-8　リンクアグリゲーション使用時の通信の障害解析方法

項番	確認内容・コマンド	対応
1	通信障害となっているリンクアグリゲーションのモードが，相手装置のモードと一致していることを確認してください。 • show channel-group detail	リンクアグリゲーションのモードが相手装置と異なる場合は，相手装置と同じモードに変更してください。
		リンクアグリゲーションのモードが相手装置と一致していて，かつ LACP リンクアグリゲーションの場合は，各ポートの LACP 開始方法が本装置および相手装置の両方とも passive でないか確認してください。 両方とも passive の場合は，本装置または相手装置のどちらか一方を active に変更してください。 本装置または相手装置のどちらか一方が active の場合は，項番 2 へ。
		リンクアグリゲーションのモードが相手装置と一致していて，かつスタティックリンクアグリゲーションの場合は，項番 3 へ。
2	通信障害となっているリンクアグリゲーションの統計情報で，TxLACPDUs および RxLACPDUs の値が増加していることを確認してください。 • show channel-group statistics lacp	TxLACPDUs および RxLACPDUs のどちらかが増加しない場合は，「3　ネットワークインタフェースのトラブルシュート」を参照して，回線状態を確認してください。 回線状態に問題がないときは，フィルタまたは QoS によって LACPDU が廃棄されていないか確認してください。確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。
		TxLACPDUs および RxLACPDUs のどちらも増加している場合は，項番 3 へ。
3	通信障害となっているポートの運用状態を，Status で確認してください。 • show channel-group detail	チャネルグループ内の全ポートが Down の場合，チャネルグループが Down します。 Down 状態のポートでは Reason の表示内容によって，次のように対応してください。 • Standby 本装置のチャネルグループのポートがスタンバイ状態になっています。スタンバイ状態を解除する場合は，ポートチャネルインタフェースのコンフィグレーションから channel-group max-active-port の設定を削除してください。 • CH Disabled チャネルグループが Disable 状態のため Down しています。Disable 状態を解除する場合は，ポートチャネルインタフェースのコンフィグレーションから shutdown の設定を削除してください。 • Port Down

項番	確認内容・コマンド	対応
		リンクダウンしています。「3　ネットワークインタフェースのトラブルシュート」を参照してください。 • Port Speed Unmatch チャネルグループ内のほかのポートと回線速度が不一致のため縮退状態になっています。縮退を回避する場合は，チャネルグループ内の全ポートの速度が一致するように設定してください。 • Duplex Half Duplex モードが Half のため縮退状態になっています。縮退を回避する場合は，Duplex モードを Full に設定してください。 • Port Selecting ポートアグリゲーション条件チェック実施中のため縮退状態になっています。しばらく待っても回復しない場合は，相手装置の運用状態および設定を確認してください。 • Waiting Partner Synchronization ポートアグリゲーション条件チェックを完了して接続ポートの同期待ちのため縮退状態になっています。しばらく待っても回復しない場合は，相手装置の運用状態および設定を確認してください。 • Partner System ID Unmatch 接続ポートから受信した Partner System ID とグループの Partner System ID が不一致のため縮退状態になっています。縮退を回避する場合は，相手装置の運用状態および配線を確認してください。 • LACPDU Expired 接続ポートからの LACPDU 有効時刻を超過したため，該当ポートが縮退状態となっています。show channel-group statistics コマンドで lacp パラメータを指定して，LACPDU の統計情報を確認してください。また，相手装置の運用状態および設定を確認してください。 • Partner Key Unmatch 接続ポートから受信した Key とグループの Partner Key が不一致のため縮退状態となっています。縮退を回避する場合は，相手装置の運用状態および配線を確認してください。 • Partner Aggregation Individual 接続ポートからリンクアグリゲーション不可を受信したため縮退状態となっています。縮退を回避する場合は，相手装置の運用状態および設定を確認してください。 • Partner Synchronization OUT_OF_SYNC 接続ポートから同期不可を受信したため縮退状態となっています（相手装置でリンクアグリゲーションを Disable 状態にした場合に発生します）。 • Port Moved 接続されていたポートがほかのポートと接続しました。配線を確認してください。

項番	確認内容・コマンド	対応
		• Operation of Detach Port Limit 離脱ポート数制限機能が動作したため，チャネルグループが Down しています。

4 レイヤ 2 スイッチングのトラブルシュート

この章では，レイヤ 2 スイッチングで障害が発生した場合の対処について説明します。

4.1　VLAN の通信障害

(1)　通信できない

VLAN 使用時に通信できない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 4-1　VLAN の障害解析方法

項番	確認内容・コマンド	対応
1	VLAN で通信するポートおよび VLAN ID について，VLAN の設定が正しいか，コンフィグレーションを確認してください。 • show vlan configuration	コンフィグレーションが正しい場合は，項番 2 へ。
		コンフィグレーションが正しくない場合は，コンフィグレーションを修正してください。
2	VLAN ポート数が収容条件に達しているシステムメッセージ（メッセージ種別：VLAN，メッセージ識別子：2510001b）が表示されていないか確認してください。 • show logging • show vlan summary	システムメッセージが表示されていない場合は，項番 3 へ。
		システムメッセージが表示されている場合は，VLAN ポート数が収容条件に達しています。 VLAN ポート数が収容条件を超えた状態での運用は推奨しません。show vlan summary コマンドで Number of VLAN ports の値を確認して，収容条件内で運用してください。
3	VLAN の状態を確認してください。 • show vlan detail	Status が Up の場合は，項番 5 へ。
		Status が Up で，かつ VLAN を設定した特定のポートで通信できない場合は，項番 4 へ。
		Status が Down の場合は，通信できるポートがない，または VLAN debounce 機能によって VLAN の Up 状態への遷移が抑止されています。 • ポート状態を確認する場合は，項番 4 へ。 • VLAN debounce 機能の設定をコンフィグレーションで確認してください。
4	VLAN に所属しているポートの状態を確認してください。 • show vlan detail	Port Information でポート状態が Up，かつデータ転送状態が Forwarding の場合は，項番 5 へ。
		Port Information でポート状態が Up，かつデータ転送状態が Blocking(CH)の場合は，リンクアグリゲーションによって通信できない状態になっています。「3.2　リンクアグリゲーション使用時の通信障害」を参照してください。
		Port Information でポート状態が Up，かつデータ転送状態が Blocking(STP)の場合は，スパニングツリーによって通信できない状態になっています。「4.2　スパニングツリーの通信障害」を参照してください。
		Port Information でポート状態が Up，かつデータ転送状態が Blocking(AXRP)の場合は，Ring Protocol によって通信できない状態になっています。「4.3　Ring Protocol の通信障害」を参照してください。

項番	確認内容・コマンド	対応
		Port Information でポート状態が Down の場合は,「3.1.1 イーサネットポートの接続ができない」を参照して，イーサネットポートの状態を確認してください。
5	MAC アドレステーブルを表示して, MAC アドレスの情報が正しいか確認してください。 • show mac-address-table • clear mac-address-table	MAC アドレスが表示されていない場合は，項番 6 へ。
		MAC アドレスが表示されていてもポート番号が異なる場合は，相手装置の設定内容の変更などによって情報が古くなっています。 clear mac-address-table コマンドで，MAC アドレステーブルの情報をクリアしてください。
6	装置間で VLAN Tag の TPID が一致しているか確認してください。 • show interfaces	装置間で VLAN Tag の TPID が一致している場合は，項番 7 へ。
		装置間で VLAN Tag の TPID が異なる場合は，本装置のコンフィグレーション変更をするか，相手装置の設定を変更してください。
7	フィルタまたは QoS によってフレームが廃棄されていないか確認してください。	確認方法と対応については,「8.1　パケット廃棄の確認」を参照してください。

(2)　MAC アドレス学習の異常

VLAN の通信は，MAC アドレステーブルによって管理されています。MAC アドレスが MAC アドレステーブルに正しく登録されていないと, 通信に影響することがあります。次の表に示す障害解析方法に従って原因を切り分けてください。

表 4-2　MAC アドレス学習の障害解析方法

項番	確認内容・コマンド	対応
1	MAC アドレステーブルに登録されている MAC アドレスの数（エントリ数）が，収容条件に達しているシステムメッセージ（メッセージ種別：PSU，メッセージ識別子：22001002）が表示されていないか確認してください。 • show logging MAC アドレステーブルで使用中のエントリ数と，使用できる最大エントリ数を確認してください。 • show psu resources	システムメッセージが表示されている場合は，MAC アドレステーブルのエントリ数が収容条件に達しています。 収容条件を超えるとフレームはフラッディングされます。ネットワーク構成を見直して収容条件内で運用してください。 ネットワーク構成を見直しても回復しない場合は，PSU を再起動してください。

4.2　スパニングツリーの通信障害

スパニングツリー使用時に，レイヤ 2 通信で障害が発生する，またはスパニングツリーの運用状態がネットワーク構成どおりでない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

なお，マルチプルスパニングツリーの場合は，CIST または MST インスタンスごとに確認してください。例えば，ルートブリッジに関して確認するときは，CIST のルートブリッジまたは MST インスタンスごとのルートブリッジと読み替えて確認してください。

表 4-3　スパニングツリーの障害解析方法

項番	確認内容・コマンド	対応
1	スパニングツリーの収容数が収容条件内かどうか確認してください。 • show spanning-tree port-count	収容条件内で設定してください。なお，収容条件については，「コンフィグレーションガイド」を参照してください。 収容条件内の場合は，項番 2 へ。
2	障害となっているスパニングツリーについて，プロトコル動作状況を確認してください。 • show spanning-tree	Enabled の場合は，項番 3 へ。
		Disabled の場合は，スパニングツリーが停止状態になっています。コンフィグレーションを確認してください。
3	障害となっているスパニングツリーについて，ルートブリッジのブリッジ識別子を確認してください。 • show spanning-tree	ルートブリッジのブリッジ識別子がネットワーク構成どおりのルートブリッジである場合は，項番 4 へ。
		ルートブリッジのブリッジ識別子がネットワーク構成どおりのルートブリッジでない場合は，ネットワーク構成およびコンフィグレーションを確認してください。
4	障害となっているスパニングツリーについて，ポート状態およびポート役割を確認してください。 • show spanning-tree	ポート状態およびポート役割がネットワーク構成どおりの場合は，項番 5 へ。
		ループガード機能を適用しているポートのポート状態が Blocking または Discarding の場合は，そのポートが指定ポートかどうか確認してください。指定ポートであれば，ループガード機能の設定を削除してください。
		ポート状態およびポート役割がネットワーク構成と異なる場合は，隣接装置の状態とコンフィグレーションを確認してください。
5	障害となっているスパニングツリーについて，障害となっているポートでの BPDU の送受信カウンタを確認してください。 • show spanning-tree statistics	該当するポートがルートポートで，かつ BPDU 受信カウンタがカウントアップしている場合は，項番 6 へ。
		該当するポートがルートポートで，かつ BPDU 受信カウンタがカウントアップしていない場合は，フィルタまたは QoS によって BPDU が廃棄されていないか確認してください。確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。 問題がない場合は，隣接装置を確認してください。
		該当するポートが指定ポートで，かつ BPDU 送信カウンタがカウントアップしている場合は，項番 6 へ。

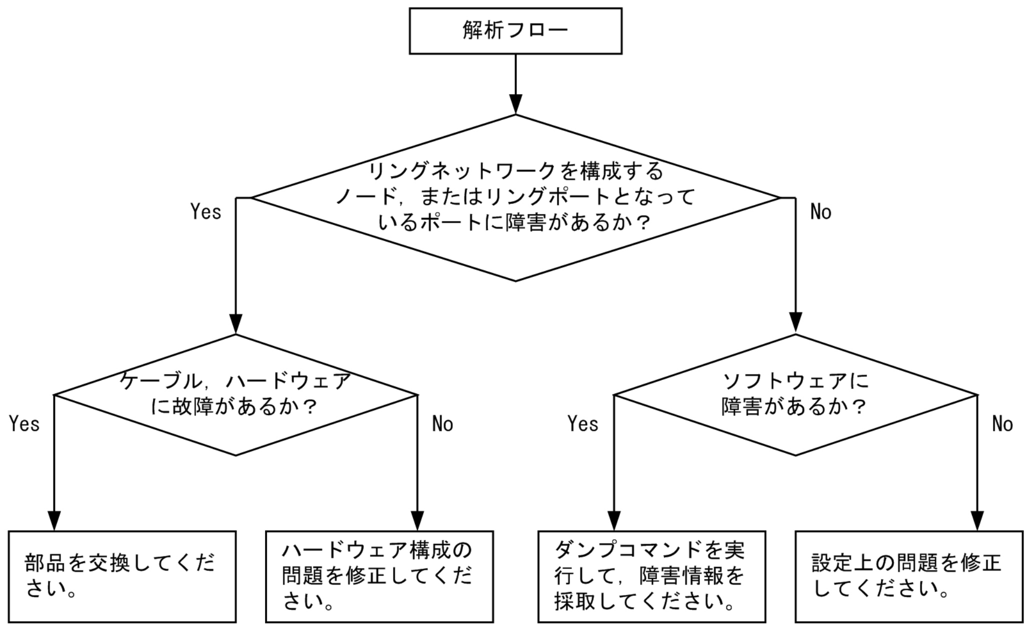
項番	確認内容・コマンド	対応
		該当するポートが指定ポートで，かつ BPDU 送信カウンタがカウントアップしていない場合は，「3　ネットワークインタフェースのトラブルシュート」を参照してください。
6	障害となっているスパニングツリーについて，受信 BPDU のルートブリッジ識別子および送信ブリッジ識別子がネットワーク構成どおりであることを確認してください。 • show spanning-tree detail	受信 BPDU のルートブリッジ識別子および送信ブリッジ識別子がネットワーク構成と異なる場合は，隣接装置の状態を確認してください。

4.3 Ring Protocol の通信障害

Autonomous Extensible Ring Protocol は，リングトポロジでのレイヤ 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。

Ring Protocol 運用時に通信ができない場合は，次の図に示す解析フローに従って，現象を把握して原因を切り分けてください。

図 4-1　解析フロー



Ring Protocol 運用時に，正常に動作しない，またはリングネットワークの障害を検出する場合は，該当のリングネットワークを構成するすべてのノードに対して，次の表に示す障害解析方法に従って原因を切り分けてください。

表 4-4　Ring Protocol の障害解析方法

項番	確認内容・コマンド	対応
1	Ring Protocol の動作状態を確認してください。 • show axrp	Oper State に enable が表示されている場合は，項番 2 へ。
		Oper State に"-"が表示されている場合は, Ring Protocol が動作するために必要なコンフィグレーションがそろっていません。コンフィグレーションを確認してください。
		Oper State に disable が表示されている場合は，Ring Protocol が無効になっています。コンフィグレーションを確認してください。
		Oper State に Not Operating が表示されている場合は，Ring Protocol が動作していません。コンフィグレーションに矛盾（本装置の動作モード，および属性とリングポートの組み合わせが適切でないなど）がないか, コンフィグレーションを確認してください。 コンフィグレーションに矛盾がない場合は，項番 2 へ。

項番	確認内容・コマンド	対応
2	動作モードと属性を確認してください。 • show axrp	Mode と Attribute の内容がネットワーク構成どおりの動作モードと属性になっている場合は，項番 3 へ。
		上記が異なる場合は，コンフィグレーションを確認してください。
3	各 VLAN グループのリングポート，およびその状態を確認してください。 • show axrp	Ring Port と Role/State の内容がネットワーク構成どおりのポートと状態になっている場合は，項番 4 へ。
		上記が異なる場合は，コンフィグレーションを確認してください。
4	制御 VLAN ID を確認してください。 • show axrp detail	Control VLAN ID の内容がネットワーク構成どおりの VLAN ID になっている場合は，項番 5 へ。
		リングを構成する各装置で制御 VLAN ID が異なるなど，上記が異なる場合は，コンフィグレーションを確認してください。
5	VLAN グループに属している VLAN ID を確認してください。 • show axrp detail	VLAN ID の内容がネットワーク構成どおりの VLAN ID になっている場合は，項番 6 へ。
		リングを構成する各装置で VLAN グループに属している VLAN ID が異なるなど，上記が異なる場合は，コンフィグレーションを確認してください。
6	ヘルスチェックフレームの送信間隔のタイマ値（Health Check Interval）とヘルスチェックフレームの保護時間のタイマ値（Health Check Hold Time）を確認してください。 • show axrp detail	ヘルスチェックフレームの保護時間のタイマ値が，ヘルスチェックフレームの送信間隔のタイマ値より大きい（伝送遅延も考慮されている）場合は，項番 7 へ。
		ヘルスチェックフレームの保護時間のタイマ値が，ヘルスチェックフレームの送信間隔のタイマ値より小さい，または等しい（伝送遅延が考慮されていない）場合は，コンフィグレーションを確認して，設定を見直してください。
7	Ring Protocol で使用している VLAN とそのポートの状態を確認してください。 • show vlan detail	VLAN およびそのポートの状態に異常がない場合は，項番 8 へ。
		異常がある場合は，コンフィグレーションの確認も含めて，その状態を復旧してください。
8	フィルタまたは QoS によって Ring Protocol で使用する制御フレームが廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。
		Ring Protocol で使用する制御フレームが廃棄されていない場合は，項番 9 へ。
9	マスタノードおよび共有リンク非監視リングの最終端ノードで，ヘルスチェックフレームの送受信状態を確認してください。 • show axrp detail	ヘルスチェックフレームを正常に送受信できない場合は，コンフィグレーションを確認して，設定を見直してください。

4.4　IGMP/MLD snooping の通信障害

IGMP/MLD snooping 使用時にマルチキャスト中継ができない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 4-5　IGMP/MLD snooping の障害解析方法

項番	確認内容・コマンド	対応
1	IGMP/MLD snooping を使用している VLAN で，障害が発生しているシステムメッセージが表示されていないか確認してください。 • show logging	VLAN で障害が発生していない場合は，項番 2 へ。
		VLAN で障害が発生している場合は「メッセージ・ログレファレンス」を参照して，各システムメッセージの「対応」に従ってください。
2	IGMP/MLD snooping を使用している VLAN 内のポートまたはチャネルグループで，障害が発生しているシステムメッセージが表示されていないか確認してください。 • show logging	ポートまたはチャネルグループで障害が発生していない場合は，項番 3 へ。
		ポートまたはチャネルグループで障害が発生している場合は「メッセージ・ログレファレンス」を参照して，各システムメッセージの「対応」に従ってください。
3	IGMP/MLD snooping の登録エントリ数が収容条件を超えているシステムメッセージが表示されていないか確認してください。 • show logging	システムメッセージが表示されていない場合は，項番 4 へ。
		次のシステムメッセージが表示されている場合，IGMP snooping または MLD snooping の登録エントリ数が収容条件を超えています。エントリ数を削減できるようにシステム構成を見直してください。 • メッセージ種別：IGMPsnoop，メッセージ識別子：21010004 • メッセージ種別：MLDsnoop，メッセージ識別子：21020004
4	MAC アドレステーブルの使用量が収容条件を超えているシステムメッセージが表示されていないか確認してください。 • show logging	システムメッセージが表示されていない場合は，項番 5 へ。
		メッセージ種別：PSU，メッセージ識別子：22003001 が表示されている場合，MAC アドレステーブルの使用量が収容条件を超えているため，IGMP snooping のエントリが登録できません。システム構成を見直したあと，clear igmp-snooping group コマンドを実行してください。
		メッセージ種別：PSU，メッセージ識別子：22003002 が表示されている場合，MAC アドレステーブルの使用量が収容条件を超えているため，MLD snooping のエントリが登録できません。システム構成を見直したあと，clear mld-snooping group コマンドを実行してください。
		メッセージ種別：PSU，メッセージ識別子：22003003 が表示されている場合，MAC アドレステーブルの使用量が収容条件を超えているため，IGMP snooping を制御するためのエントリが登録できません。システム構成を見直したあと，restart snooping コマンドを実行してください。
		メッセージ種別：PSU，メッセージ識別子：22003004 が表示されている場合，MAC アドレステーブルの使用量が収容

<table>
<tr><th>項番</th><th>確認内容・コマンド</th><th>対応</th></tr>
<tr><td></td><td></td><td>条件を超えているため，MLD snooping を制御するためのエントリが登録できません。システム構成を見直したあと，restart snooping コマンドを実行してください。</td></tr>
<tr><td rowspan="2">5</td><td rowspan="2">フィルタまたは QoS によって，IGMP/MLD snooping で使用する制御フレームが廃棄されていないか確認してください。</td><td>確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。</td></tr>
<tr><td>IGMP/MLD snooping で使用する制御フレームが廃棄されていない場合は，項番 6 へ。</td></tr>
<tr><td rowspan="2">6</td><td rowspan="2">IPv4/IPv6 マルチキャストを同時使用する場合の設定が正しいか確認してください。</td><td>IPv4/IPv6 マルチキャストを同時使用する場合の設定が正しい場合は，項番 7 へ。</td></tr>
<tr><td>該当 VLAN に IPv4/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場合，マルチキャスト通信が必要なポートにマルチキャストルータポートを設定してください。</td></tr>
<tr><td rowspan="2">7</td><td rowspan="2">IGMP クエリアまたは MLD クエリアの設定が正しいか確認してください。
• show igmp-snooping
• show mld-snooping</td><td>IGMP querying system または MLD querying system の表示が正しい場合は，項番 8 へ。</td></tr>
<tr><td>IGMP querying system または MLD querying system に IP アドレスが表示されていない場合は，次に示すとおりに対応してください。
• IPv4/IPv6 マルチキャストを同時使用していないとき
VLAN 内に IGMP クエリアまたは MLD クエリアが存在しません。ネットワーク構成またはコンフィグレーションを見直してください。
また，本装置に IGMP クエリア機能または MLD クエリア機能を設定しているときは，VLAN に IP アドレスが設定されているか確認してください。
• IPv4/IPv6 マルチキャストを同時使用しているとき
IPv4 Multicast routing または IPv6 Multicast routing に On が表示されていることを確認してください。On が表示されていれば，IP アドレスが表示されていなくても問題ありません。</td></tr>
<tr><td rowspan="2">8</td><td rowspan="2">VLAN 内にマルチキャストパケット中継ができる機器を接続している場合，マルチキャストルータポートの設定が正しいか確認してください。
• show igmp-snooping
• show mld-snooping</td><td>Mrouter-port にマルチキャストルータポートが表示されている場合は，項番 9 へ。</td></tr>
<tr><td>Mrouter-port にマルチキャストルータポートが表示されていない場合は，コンフィグレーションを確認してください。また，接続機器がマルチキャスト中継できる設定になっているか確認してください。</td></tr>
<tr><td rowspan="2">9</td><td rowspan="2">IGMP/MLD snooping のエントリが学習されていることを確認してください。
• show igmp-snooping group
• show mld-snooping group</td><td>IGMP/MLD snooping のエントリが表示されている場合は，項番 10 へ。</td></tr>
<tr><td>参加グループアドレスが表示されていることを確認してください。表示されていない場合は，受信者側の設定が正しいか確認してください。</td></tr>
<tr><td>10</td><td>マルチキャストパケットの中継が同一 VLAN 内の中継か確認してください。</td><td>同一 VLAN 内での中継でない場合は，「5.6　マルチキャストルーティングの通信障害」を参照してください。</td></tr>
</table>

5 IP およびルーティングのトラブルシュート

この章では，IP ネットワーク上の通信およびルーティングで障害が発生した場合の対処について説明します。

5.1　IPv4 ネットワークの通信障害

5.1.1　通信できない，または切断されている

本装置を使用している IPv4 ネットワーク上で通信トラブルが発生する要因として，次の 3 種類が考えられます。

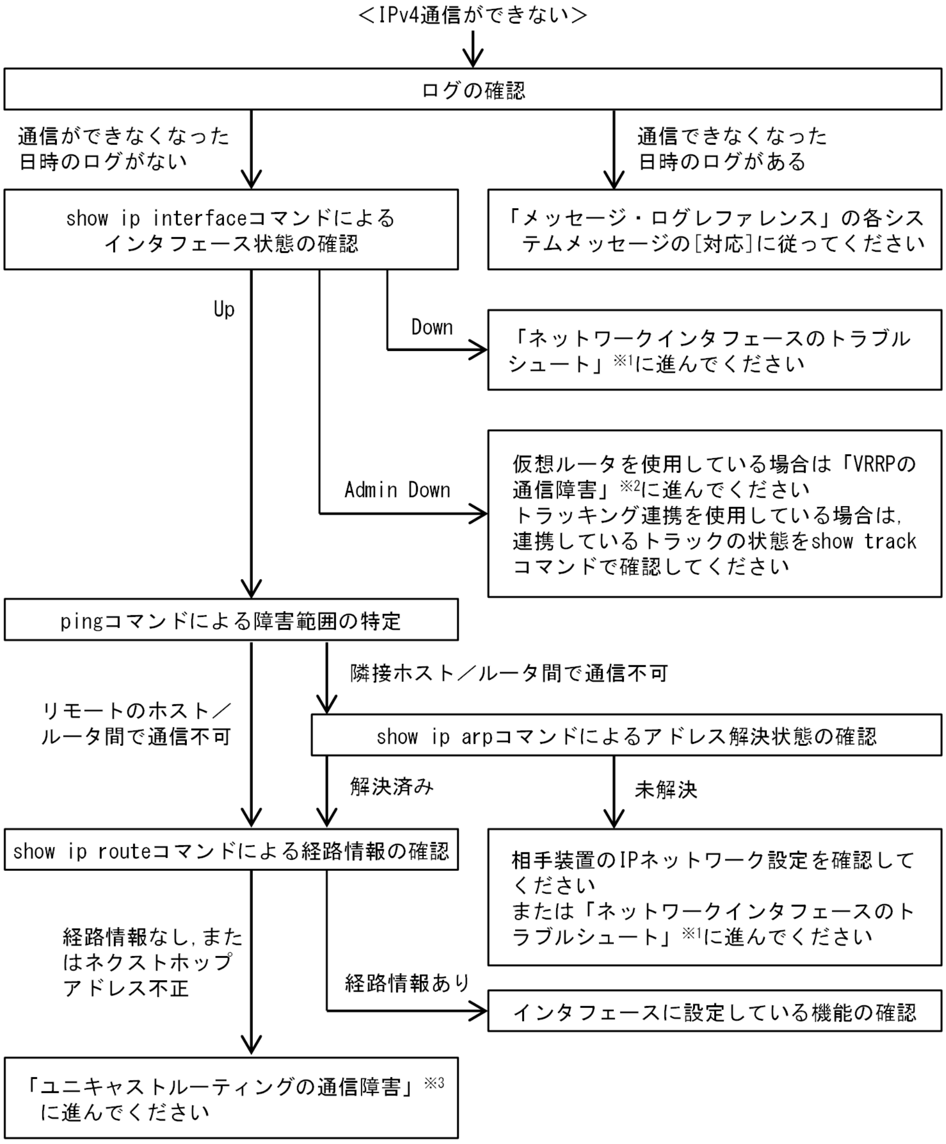
1. IPv4 通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

1.および 2.については，コンフィグレーションおよびネットワーク構成の変更前と変更後の差分を取得して，通信できなくなる原因がないか確認してください。

ここでは，3.に示すように「コンフィグレーションおよびネットワーク構成は正しいのに IPv4 通信ができない」，「これまで正常に動いていたのに IPv4 通信ができなくなった」というケースを中心に，障害部位および原因の切り分け手順を説明します。

障害部位および原因の切り分け方法は，次のフローに従ってください。

図 5-1　IPv4 通信ができない場合の障害解析フロー



注※1 「3　ネットワークインタフェースのトラブルシュート」を参照してください。

注※2 「5.4　VRRP の通信障害」を参照してください。

注※3 「5.5　ユニキャストルーティングの通信障害」を参照してください。

(1)　ログの確認

ログを表示して，障害発生を示すシステムメッセージがあるか確認します。回線の障害（または壊れ）などによって通信できなくなった場合には，システムメッセージが出力されます。ログの確認手順を次に示します。

1. 本装置にログインします。
2. show logging コマンドを実行して，ログを表示します。
3. ログにはそれぞれ発生した日時が表示されます。通信できなくなった日時にログが表示されていないか確認してください。

4. 通信できなくなった日時に表示されているログの障害の内容および障害への対応については，「メッセージ・ログレファレンス」を参照して，その指示に従ってください。
5. 通信できなくなった日時にログの表示がないときは，「(2)　インタフェース状態の確認」に進んでください。

(2)　インタフェース状態の確認

本装置のハードウェアは正常に動作している場合でも，本装置と接続している隣接装置のハードウェアに障害が発生していることも考えられます。

本装置と隣接装置間の，インタフェース状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ip interface コマンドを使用して，該当装置間のインタフェース状態を確認してください。
3. 該当インタフェースが Down 状態のときは，「3　ネットワークインタフェースのトラブルシュート」を参照してください。
4. 該当インタフェースが Admin Down 状態のときは，該当インタフェースで動作している仮想ルータまたはトラッキング連携によって，運用停止状態になっています。
   仮想ルータを使用している場合は「5.4　VRRP の通信障害」を参照してください。
   トラッキング連携を使用している場合は，連携しているトラックの状態を show track コマンドで確認してください。トラック状態が想定される状態でない場合は，「6.3　トラッキング機能のトラブル」を参照してください。
5. 該当インタフェースが Up 状態のときは，「(3)　障害範囲の特定（本装置から実施する場合）」に進んでください。

(3)　障害範囲の特定（本装置から実施する場合）

本装置に障害がない場合は，通信していた相手との間のどこかに障害が発生している可能性があります。通信相手とのどの部分で障害が発生しているか，障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. ping コマンドを使用して，通信できない両方の相手との疎通を確認してください。ping コマンドの操作例および実行結果の見方については，「運用コマンドレファレンス」を参照してください。
3. ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使用して，本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping コマンドを実行した結果，障害範囲が隣接装置の場合は「(5)　隣接装置との ARP 解決情報の確認」に，リモート先の装置の場合は「(6)　ユニキャストルーティング情報の確認」に進んでください。

(4)　障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインできない環境にある場合に，お客様の端末装置から通信相手とのどの部分で障害が発生しているか，障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping 機能があることを確認してください。
2. ping 機能を使用して，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping 機能で通信相手との疎通が確認できなかったときは，さらに ping コマンドを使用して，お客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。

4. ping 機能によって障害範囲が特定できたら，本装置に障害があると考えられる場合は本装置にログインして，障害解析フローに従って障害原因を調査してください。

(5) 隣接装置との ARP 解決情報の確認

ping コマンドを実行した結果，隣接装置との疎通ができない場合は，ARP によるアドレス解決ができていないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ip arp コマンドを使用して，隣接装置間とのアドレス解決状態（ARP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（ARP エントリ情報あり）場合は，「(6)　ユニキャストルーティング情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（ARP エントリ情報なし）場合は，隣接装置と本装置の IP ネットワーク設定が一致しているか確認してください。

(6) ユニキャストルーティング情報の確認

隣接装置とのアドレスが解決しているのに通信できない場合や，IPv4 ユニキャスト通信で通信相手との途中の経路で疎通できなくなる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。経路情報を確認する手順を次に示します。

1. 本装置にログインします。
2. show logging コマンドを実行して，IPv4 ユニキャスト経路数が収容条件に達しているメッセージ（メッセージ種別：PSU，メッセージ識別子：41011002）が表示されていないか確認してください。

   システムメッセージが表示されている場合，IPv4 ユニキャスト経路数が収容条件に達しているため，これ以上 IPv4 ユニキャスト経路を登録できません。ネットワーク構成を見直して，収容条件内で運用することを推奨します。

   ネットワーク構成を見直したあとで，clear ip route コマンドで vrf all *パラメータを指定して，IPv4 ユニキャスト経路を再登録してください。
3. show ip route コマンドを実行して，本装置が取得した経路情報を確認してください。
4. Null インタフェースでパケットが廃棄されていないか確認してください。通信障害となっている経路情報の送出インタフェースが null0 の場合は，Null インタフェースでパケットが廃棄されています。スタティックルーティングのコンフィグレーション設定を見直してください。
5. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「5.5　ユニキャストルーティングの通信障害」に進んでください。
6. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信できないインタフェースに設定している次の機能に問題があると考えられます。該当する機能を調査してください。
   - DHCP/BOOTP リレーエージェント
     「(7)　DHCP/BOOTP リレーエージェント設定の確認」に進んでください。
   - フィルタ，QoS，または uRPF
     「(8)　パケット廃棄の確認」に進んでください。
   - ポリシーベースルーティング
     「5.3.1　ポリシーベースルーティングによる通信障害の確認」に進んでください。

(7)　DHCP/BOOTP リレーエージェント設定の確認

本装置の DHCP/BOOTP リレーエージェントによって隣接装置へ IP アドレスを割り当てている場合は，適切に IP アドレスを割り当てられていない可能性があります。

DHCP/BOOTP リレーエージェントのコンフィグレーション設定を確認してください。手順については，「5.1.2　DHCP/BOOTP リレーエージェントで IP アドレスが割り当てられない」を参照してください。

(8)　パケット廃棄の確認

フィルタ，QoS，または uRPF によってパケットが廃棄されている可能性があります。確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。

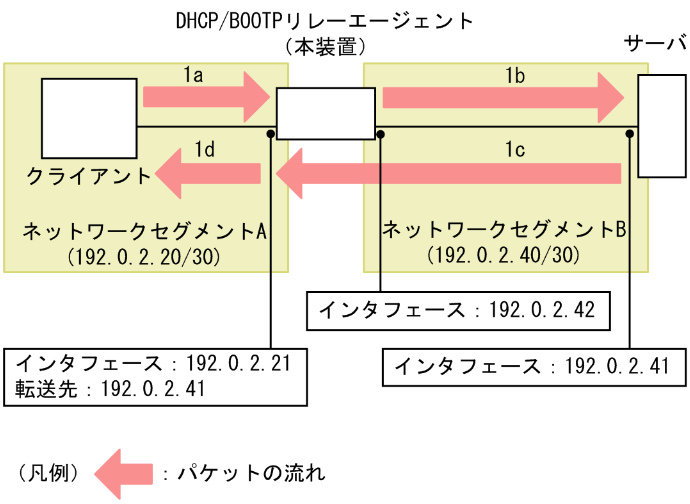
5.1.2　DHCP/BOOTP リレーエージェントで IP アドレスが割り当てられない

DHCP/BOOTP リレーエージェントの通信トラブルが発生する要因として，次の 4 種類が考えられます。

- DHCP/BOOTP リレーエージェントのコンフィグレーション設定
- DHCP/BOOTP サーバ（以降，サーバ）のコンフィグレーション設定
- DHCP/BOOTP クライアント（以降，クライアント）のコンフィグレーション設定
- IPv4 ネットワークの通信障害

ここでは，次に示すネットワーク構成を例として，障害部位および原因の切り分け手順を説明します。

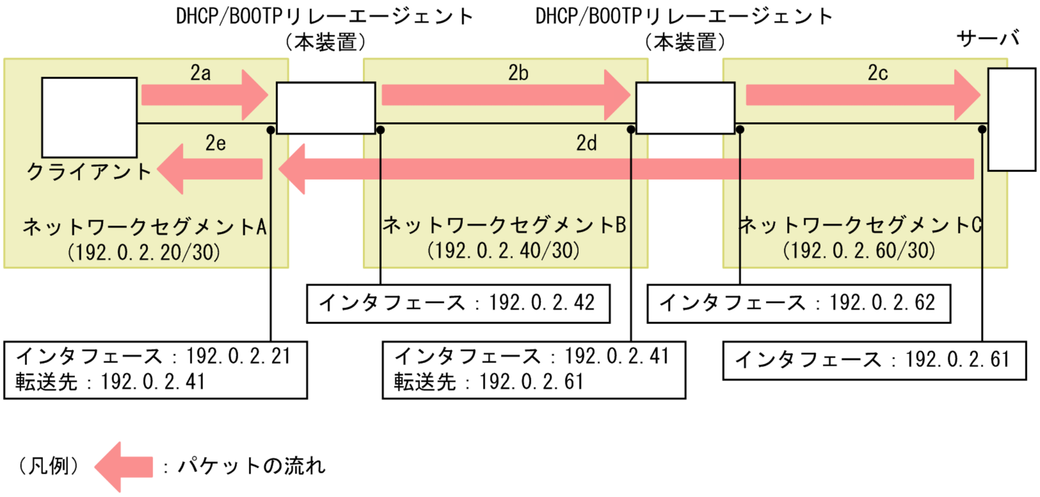
図 5-2　DHCP/BOOTP リレーエージェントのネットワーク構成例（1 段）



確認ポイント（図中の記号）	パケット内の値			
	宛先 IP アドレス	送信元 IP アドレス	宛先 UDP ポート番号	送信元 UDP ポート番号
1a	255.255.255.255	0.0.0.0	67	任意
1b	192.0.2.41	192.0.2.42	67	68
1c	192.0.2.21	192.0.2.41	67	任意

確認ポイント（図中の記号）	パケット内の値			
	宛先 IP アドレス	送信元 IP アドレス	宛先 UDP ポート番号	送信元 UDP ポート番号
1d	割り当て DHCP アドレス	192.0.2.21	68	67

図 5-3　DHCP/BOOTP リレーエージェントのネットワーク構成例（多段）



確認ポイント（図中の記号）	パケット内の値			
	宛先 IP アドレス	送信元 IP アドレス	宛先 UDP ポート番号	送信元 UDP ポート番号
2a	255.255.255.255	0.0.0.0	67	任意
2b	192.0.2.41	192.0.2.42	67	68
2c	192.0.2.61	192.0.2.62	67	68
2d	192.0.2.21	192.0.2.61	67	任意
2e	割り当て DHCP アドレス	192.0.2.21	68	67

なお，図中の 1a および 1d，または 2a および 2e を確認する場合，あらかじめクライアントに対して，割り当て DHCP アドレスの代わりに一時的に固定 IP アドレスを設定してください。

(1)　DHCP/BOOTP リレーエージェントの状態および統計情報の確認

DHCP/BOOTP リレーエージェントの状態および統計情報を確認して，次の表に示す障害解析方法に従って原因を切り分けてください。

表 5-1　DHCP/BOOTP リレーエージェントの障害解析方法

項番	確認内容・コマンド	対応
1	クライアント側インタフェースで，クライアントから受信したパケット数（DHCP/	カウントされている場合は，項番 2 へ。

項番	確認内容・コマンド	対応
	BOOTP Request Packets Count の Receive Packets）がカウントされているか確認してください。 • show ip dhcp relay statistics	カウントされていない場合は，次の内容を確認してください。 • 「(2)　DHCP/BOOTP リレーエージェント設定の確認」を参照して，DHCP/BOOTP パケットの転送先を確認してください。 • 本装置のクライアント側ネットワークセグメント（図中の確認ポイント 1a，または 2a および 2b）について確認してください。手順については，「5.1.1　通信できない，または切断されている」を参照してください。 • 該当クライアントの要因切り分け手順に従って，コンフィグレーションを確認してください。
2	ホップ数が最大数以上のため廃棄されたパケット数（DHCP/BOOTP Error Packets Count の Hops Over）がカウントされているか確認してください。 • show ip dhcp relay statistics	カウントされている場合は，「(2)　DHCP/BOOTP リレーエージェント設定の確認」を参照して，DHCP/BOOTP パケットの最大ホップ数を確認してください。
		カウントされていない場合は，項番 3 へ。
3	クライアント側インタフェースの転送先で，サーバ（転送先）宛てへの送信に成功したパケット数（DHCP/BOOTP Request Packets Count の Send Packets）がカウントされているか確認してください。 • show ip dhcp relay statistics	カウントされている場合は，項番 4 へ。
		カウントされていない場合は，次の内容を確認してください。 • 「(2)　DHCP/BOOTP リレーエージェント設定の確認」を参照して，DHCP/BOOTP リレーエージェント IP アドレスを確認してください。 • 図中の確認ポイント 1b，または 2b および 2c について確認してください。手順については，「5.1.1　通信できない，または切断されている」を参照してください。
4	サーバから受信したパケット数（DHCP/BOOTP Reply Packets Count の Receive Packets）がカウントされているか確認してください。 • show ip dhcp relay statistics	カウントされている場合は，項番 5 へ。
		カウントされていない場合は，次の内容を確認してください。 • 「(2)　DHCP/BOOTP リレーエージェント設定の確認」を参照して，DHCP/BOOTP リレーエージェント IP アドレスを確認してください。 • 図中の確認ポイント 1c，または 2c および 2d について確認してください。手順については，「5.1.1　通信できない，または切断されている」を参照してください。 • 該当サーバの要因切り分け手順に従ってコンフィグレーションを確認して，ネットワークセグメントが一致しているかなどを確認してください。
5	クライアント宛てへの送信に成功したパケット数（DHCP/BOOTP Reply Packets Count の Send Packets）がカウントされているか確認してください。 • show ip dhcp relay statistics	カウントされている場合は，次の内容を確認してください。 • 該当サーバの要因切り分け手順に従ってコンフィグレーションを確認して，割り当てる IP アドレスが十分にあるかなどを確認してください。 • 該当クライアントの要因切り分け手順に従って，コンフィグレーションを確認してください。
		カウントされていない場合は，次の内容を確認してください。

項番	確認内容・コマンド	対応
		• 「(2)　DHCP/BOOTP リレーエージェント設定の確認」を参照して，DHCP/BOOTP リレーエージェント IP アドレスを確認してください。 • 本装置のクライアント側ネットワークセグメント（図中の確認ポイント 1d，または 2e）について確認してください。手順については，「5.1.1　通信できない，または切断されている」を参照してください。 • 該当クライアントの要因切り分け手順に従って，コンフィグレーションを確認してください。

(2)　DHCP/BOOTP リレーエージェント設定の確認

DHCP/BOOTP リレーエージェントのコンフィグレーション設定ミスによって，クライアントに IP アドレスが割り当てられないという原因が考えられます。DHCP/BOOTP リレーエージェントのコンフィグレーションを確認する手順を次に示します。

1. クライアント側の IP インタフェースに，DHCP/BOOTP パケットの転送先が設定（コンフィグレーションコマンド ip helper-address）されていることを確認してください。
2. DHCP/BOOTP パケットの最大ホップ数が，本装置とクライアント間の DHCP/BOOTP リレーエージェントの数よりも大きな値に設定（コンフィグレーションコマンド ip dhcp relay maximum-hop-count）されていることを確認してください。
3. マルチホーム構成の場合，DHCP/BOOTP リレーエージェント IP アドレス（giaddr）に，クライアントのネットワークセグメントと一致する IP アドレスが設定（コンフィグレーションコマンド ip dhcp relay gateway）されていることを確認してください。
   なお，show ip dhcp relay interface コマンドで表示される DHCP/BOOTP リレーエージェントのインタフェース情報でも，コンフィグレーションの設定を確認できます。

(3)　DHCP/BOOTP リレーエージェントと VRRP を同一 IP インタフェースで運用している場合の確認

DHCP/BOOTP リレーエージェントと VRRP を同一 IP インタフェースに設定する場合，VRRP によって別装置に切り替わってもクライアントからサーバへのゲートウェイが同じになることを確認してください。例えば，サーバでは，仮想ルータアドレスをデフォルトルータ（ルータオプション）としてクライアントに割り当てられるように設定しているか確認してください。

5.2　IPv6 ネットワークの通信障害

5.2.1　通信できない，または切断されている

本装置を使用している IPv6 ネットワーク上で通信トラブルが発生する要因として，次の 3 種類が考えられます。

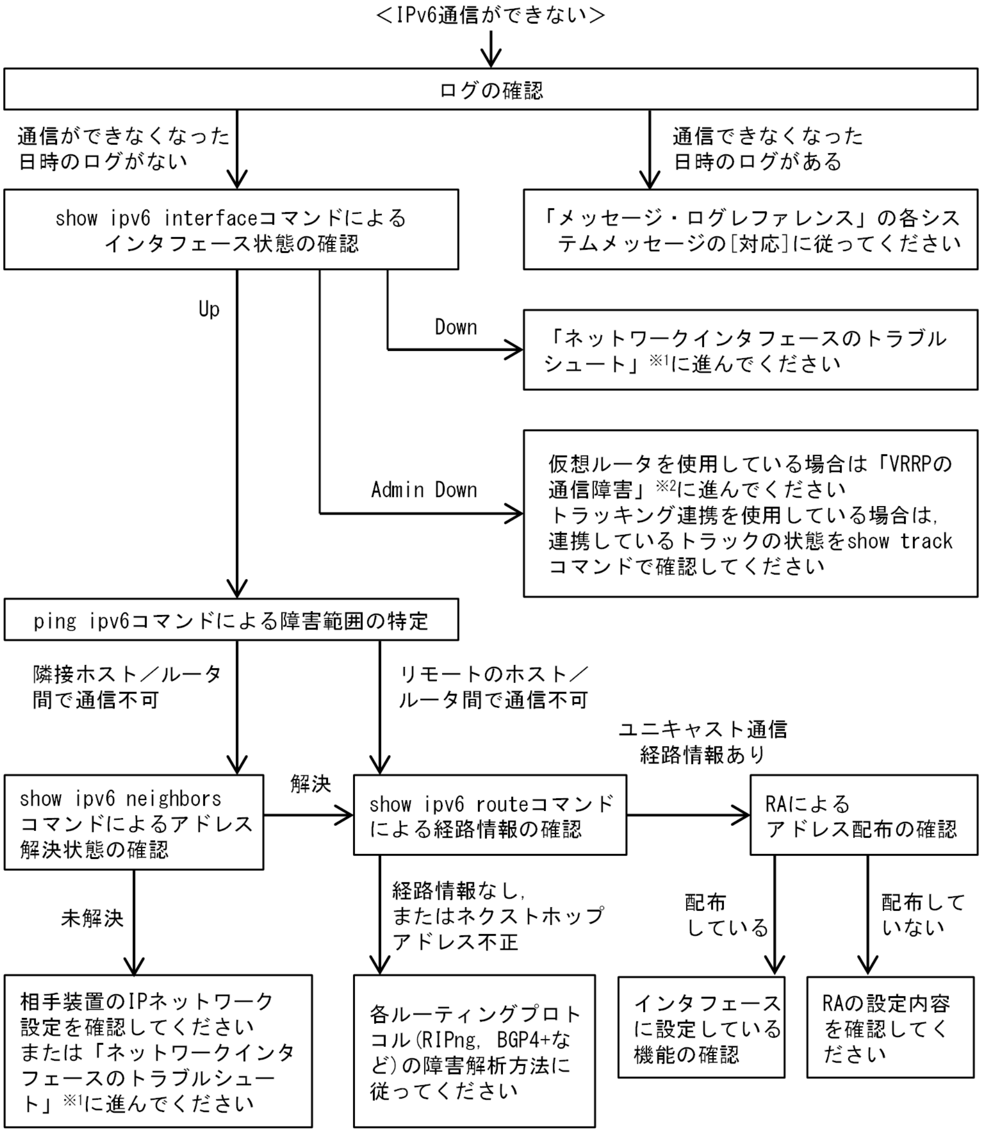
1. IPv6 通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

1.および 2.については，コンフィグレーションおよびネットワーク構成の変更前と変更後の差分を取得して，通信できなくなる原因がないか確認してください。

ここでは，3.に示すように「コンフィグレーションおよびネットワーク構成は正しいのに IPv6 通信ができない」,「これまで正常に動いていたのに IPv6 通信ができなくなった」というケースを中心に，障害部位および原因の切り分け手順を説明します。

障害部位および原因の切り分け方法は，次のフローに従ってください。

図 5-4 IPv6 通信ができない場合の障害解析フロー



注※1 「3　ネットワークインタフェースのトラブルシュート」を参照してください。

注※2 「5.4　VRRP の通信障害」を参照してください。

(1) ログの確認

ログを表示して，障害発生を示すシステムメッセージがあるか確認します。回線の障害（または壊れ）などによって通信できなくなった場合には，システムメッセージが出力されます。ログの確認手順を次に示します。

1. 本装置にログインします。
2. show logging コマンドを実行して，ログを表示します。
3. ログにはそれぞれ発生した日時が表示されます。通信できなくなった日時にログが表示されていないか確認してください。
4. 通信できなくなった日時に表示されているログの障害の内容および障害への対応については，「メッセージ・ログレファレンス」を参照して，その指示に従ってください。

5. 通信できなくなった日時にログの表示がないときは，「(2)　インタフェース状態の確認」に進んでください。

(2)　インタフェース状態の確認

本装置のハードウェアは正常に動作している場合でも，本装置と接続している隣接装置のハードウェアに障害が発生していることも考えられます。

本装置と隣接装置間の，インタフェース状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ipv6 interface コマンドを使用して，該当装置間のインタフェース状態を確認してください。
3. 該当インタフェースが Down 状態のときは，「3　ネットワークインタフェースのトラブルシュート」を参照してください。
4. 該当インタフェースが Admin Down 状態のときは，該当インタフェースで動作している仮想ルータまたはトラッキング連携によって，運用停止状態になっています。
   仮想ルータを使用している場合は「5.4　VRRP の通信障害」を参照してください。
   トラッキング連携を使用している場合は，連携しているトラックの状態を show track コマンドで確認してください。トラック状態が想定される状態でない場合は，「6.3　トラッキング機能のトラブル」を参照してください。
5. 該当インタフェースが Up 状態のときは，「(3)　障害範囲の特定（本装置から実施する場合）」に進んでください。

(3)　障害範囲の特定（本装置から実施する場合）

本装置に障害がない場合は，通信していた相手との間のどこかに障害が発生している可能性があります。通信相手とのどの部分で障害が発生しているか，障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. ping ipv6 コマンドを使用して，通信できない両方の相手との疎通を確認してください。ping ipv6 コマンドの操作例および実行結果の見方については，「運用コマンドレファレンス」を参照してください。
3. ping ipv6 コマンドで通信相手との疎通が確認できなかったときは，さらに ping ipv6 コマンドを使用して，本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping ipv6 コマンドを実行した結果，障害範囲が隣接装置の場合は「(5)　隣接装置との NDP 解決情報の確認」に，リモート先の装置の場合は「(6)　ユニキャストルーティング情報の確認」に進んでください。

(4)　障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインできない環境にある場合に，お客様の端末装置から通信相手とのどの部分で障害が発生しているか，障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping ipv6 機能があることを確認してください。
2. ping ipv6 機能を使用して，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping ipv6 機能で通信相手との疎通が確認できなかったときは，さらに ping ipv6 コマンドを使用して，お客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping ipv6 機能によって障害範囲が特定できたら，本装置に障害があると考えられる場合は本装置にログインして，障害解析フローに従って障害原因を調査してください。

(5) 隣接装置との NDP 解決情報の確認

ping ipv6 コマンドを実行した結果，隣接装置との疎通ができない場合は，NDP によるアドレス解決ができていないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ipv6 neighbors コマンドを使用して，隣接装置間とのアドレス解決状態（NDP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（NDP エントリ情報あり）場合は，「(6) ユニキャストルーティング情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（NDP エントリ情報なし）場合は，隣接装置と本装置の IP ネットワーク設定が一致しているか確認してください。

(6) ユニキャストルーティング情報の確認

隣接装置とのアドレスが解決しているのに通信できない場合や，IPv6 ユニキャスト通信で通信相手との途中の経路で疎通できなくなる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。経路情報を確認する手順を次に示します。

1. 本装置にログインします。
2. show logging コマンドを実行して，IPv6 ユニキャスト経路数が収容条件に達しているメッセージ（メッセージ種別：PSU，メッセージ識別子：41012002）が表示されていないか確認してください。

   システムメッセージが表示されている場合，IPv6 ユニキャスト経路数が収容条件に達しているため，これ以上 IPv6 ユニキャスト経路を登録できません。ネットワーク構成を見直して，収容条件内で運用することを推奨します。

   ネットワーク構成を見直したあとで，clear ipv6 route コマンドで vrf all *パラメータを指定して，IPv6 ユニキャスト経路を再登録してください。
3. show ipv6 route コマンドを実行して，本装置が取得した経路情報を確認してください。
4. Null インタフェースでパケットが廃棄されていないか確認してください。通信障害となっている経路情報の送出インタフェースが null0 の場合は，Null インタフェースでパケットが廃棄されています。スタティックルーティングのコンフィグレーション設定を見直してください。
5. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「5.5 ユニキャストルーティングの通信障害」に進んでください。

(7) IPv6 アドレスの配布情報設定の確認

本装置と本装置に直接接続されている端末との間で通信できない場合は，RA または DHCPv6 リレーエージェントによってアドレス情報が正常に配布されていない可能性があります。

- RA

  RA のコンフィグレーション設定が正しいか確認する手順を次に示します。

  1. 本装置にログインします。
  2. show ipv6 routers コマンドを実行して，本装置の RA 情報を確認してください。RA で配布する情報については，「コンフィグレーションガイド」を参照してください。
- DHCPv6 リレーエージェント

  DHCPv6 リレーエージェントを使用している場合，「5.2.2 DHCPv6 リレーエージェントで IPv6 アドレスが割り当てられない」に進んでください。

(8)　パケット廃棄の確認

フィルタ，QoS，uRPF，またはポリシーベースルーティングによってパケットが廃棄されている可能性があります。

- フィルタ，QoS または uRPF
  確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。
- ポリシーベースルーティング
  確認方法と対応については，「5.3.1　ポリシーベースルーティングによる通信障害の確認」を参照してください。

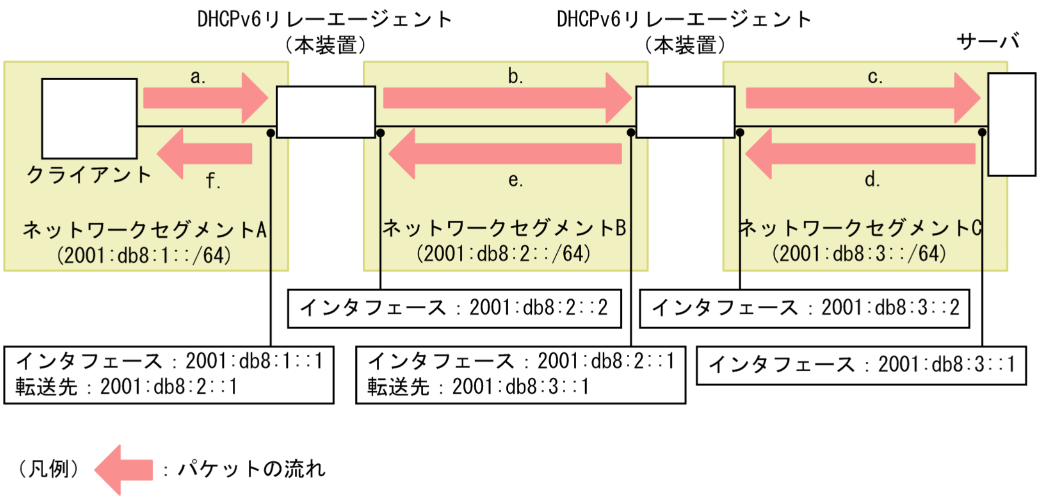
5.2.2　DHCPv6 リレーエージェントで IPv6 アドレスが割り当てられない

DHCPv6 リレーエージェントの通信トラブルが発生する要因として，次の 5 種類が考えられます。

- DHCPv6 リレーエージェントのコンフィグレーション設定
- DHCPv6 サーバ（以降，サーバ）のコンフィグレーション設定
- DHCPv6 クライアント（以降，クライアント）のコンフィグレーション設定
- RA のコンフィグレーション設定
- IPv6 ネットワークの通信障害

ここでは，次に示すネットワーク構成を例として，障害部位および原因の切り分け手順を説明します。

図 5-5　DHCPv6 リレーエージェントのネットワーク構成例



確認ポイント（図中の記号）	パケット内の値			
	宛先 IPv6 アドレス	送信元 IPv6 アドレス	宛先 UDP ポート番号	送信元 UDP ポート番号
a.	ff02::1:2	クライアントリンクローカルアドレス	547	任意
b.	2001:db8:2::1	2001:db8:2::2	547	546

確認ポイント（図中の記号）	パケット内の値			
	宛先 IPv6 アドレス	送信元 IPv6 アドレス	宛先 UDP ポート番号	送信元 UDP ポート番号
c.	2001:db8:3::1	2001:db8:3::2	547	546
d.	2001:db8:3::2	2001:db8:3::1	547	任意
e.	2001:db8:2::2	2001:db8:2::1	547	547
f.	クライアントリンクローカルアドレス	2001:db8:1::1	546	547

(1) DHCPv6 リレーエージェントの状態および統計情報の確認

DHCPv6 リレーエージェントの状態および統計情報を確認して，次の表に示す障害解析方法に従って原因を切り分けてください。

表 5-2 DHCPv6 リレーエージェントの障害解析方法

項番	確認内容・コマンド	対応
1	クライアント側インタフェースで，クライアントから受信したパケット数（DHCPv6 Request Packets Count の Receive Packets）がカウントされているか確認してください。 • show ipv6 dhcp relay statistics	カウントされている場合は，項番 2 へ。
		カウントされていない場合は，次の内容を確認してください。 •「(2) DHCPv6 リレーエージェント設定の確認」を参照して，DHCPv6 パケットの転送先が設定されていることを確認してください。 • クライアントを直接接続している場合は，RA の設定を確認してください。手順については，「(3) RA 設定の確認」を参照してください。 • 本装置のクライアント側ネットワークセグメント（図中の確認ポイント a.）について確認してください。手順については，「5.2.1 通信できない，または切断されている」を参照してください。 • 該当クライアントの要因切り分け手順に従って，コンフィグレーションを確認してください。
2	ホップ数が最大数以上のため廃棄されたパケット数（DHCPv6 Error Packets Count の Hops Over）がカウントされているか確認してください。 • show ipv6 dhcp relay statistics	カウントされている場合は，「(2) DHCPv6 リレーエージェント設定の確認」を参照して，DHCPv6 パケットの最大ホップ数を確認してください。
		カウントされていない場合は，項番 3 へ。
3	クライアント側インタフェースの転送先で，サーバ（転送先）宛てへの送信に成功したパケット数（DHCPv6 Request Packets Count の Send Packets）がカウントされているか確認してください。 • show ipv6 dhcp relay statistics	カウントされている場合は，項番 4 へ。
		カウントされていない場合は，次の内容を確認してください。 •「(2) DHCPv6 リレーエージェント設定の確認」を参照して，DHCPv6 パケットの転送先が正しいことを確認してください。 • 図中の確認ポイント b.および c.について確認してください。手順については，「5.2.1 通信できない，または切断されている」を参照してください。

項番	確認内容・コマンド	対応
4	サーバから受信したパケット数（DHCPv6 Reply Packets Count の Receive Packets）がカウントされているか確認してください。 • show ipv6 dhcp relay statistics	カウントされている場合は，項番５へ。
		カウントされていない場合は，次の内容を確認してください。 • 「(2)　DHCPv6 リレーエージェント設定の確認」を参照して，DHCPv6 パケットの転送先が正しいことを確認してください。 • 図中の確認ポイント d.および e.について確認してください。手順については，「5.2.1　通信できない，または切断されている」を参照してください。 • 該当サーバの要因切り分け手順に従ってコンフィグレーションを確認して，ネットワークセグメントが一致しているかなどを確認してください。
5	クライアント宛てへの送信に成功したパケット数（DHCPv6 Reply Packets Count の Send Packets）がカウントされているか確認してください。 • show ipv6 dhcp relay statistics	カウントされている場合は，次の内容を確認してください。 • クライアントを直接接続している場合は，RA の設定を確認してください。手順については，「(3)　RA 設定の確認」を参照してください。 • 該当サーバの要因切り分け手順に従ってコンフィグレーションを確認して，割り当てる IPv6 アドレスが十分にあるかなどを確認してください。 • 該当クライアントの要因切り分け手順に従って，コンフィグレーションを確認してください。
		カウントされていない場合は，項番６へ。
6	バインディング（IA_PD）エントリ数が最大数を超えたため破棄されたパケット数（DHCPv6 Error Packets Count の Lease Prefix Over）がカウントされているか確認してください。 • show ipv6 dhcp relay statistics	カウントされている場合は，アドレス割り当て数（IA_PD）が本装置の最大数を超えないように，ネットワーク構成を見直してください。
		カウントされていない場合は，次の内容を確認してください。 • 本装置のクライアント側ネットワークセグメント（図中の確認ポイント f.）について確認してください。手順については，「5.2.1　通信できない，または切断されている」を参照してください。 • 該当クライアントの要因切り分け手順に従って，コンフィグレーションを確認してください。

(2)　DHCPv6 リレーエージェント設定の確認

DHCPv6 リレーエージェントのコンフィグレーション設定ミスによって，クライアントに IPv6 アドレスが割り当てられないという原因が考えられます。DHCPv6 リレーエージェントのコンフィグレーションを確認する手順を次に示します。

1. クライアント側の IPv6 インタフェースに，DHCPv6 パケットの転送先が設定（コンフィグレーションコマンド ipv6 dhcp relay destination）されていることを確認してください。
2. DHCPv6 パケットの転送先として設定（コンフィグレーションコマンド ipv6 dhcp relay destination）されている，サーバもしくは DHCPv6 リレーエージェントの IPv6 アドレス，または IPv6 インタフェースが，ネットワーク構成と一致していることを確認してください。

3. DHCPv6 パケットの最大ホップ数が，本装置とクライアント間の DHCPv6 リレーエージェントの数よりも大きな値に設定（コンフィグレーションコマンド ipv6 dhcp relay maximum-hop-count）されていることを確認してください。

(3) RA 設定の確認

クライアントを直接接続している場合，RA のコンフィグレーション設定ミスによってクライアントに IPv6 アドレスが割り当てられないという原因が考えられます。RA のコンフィグレーションを確認する手順を次に示します。

1. クライアント側の IPv6 インタフェースに，アドレス自動管理設定フラグを有効にする設定（コンフィグレーションコマンド ipv6 nd managed-config-flag）がされていることを確認してください。アドレス自動管理設定フラグとは，RA によるアドレス自動設定とは別に，DHCPv6 などの RA 以外の手段によって IPv6 アドレスを端末に自動で設定させるフラグです。

   なお，DHCPv6 によって IPv6 アドレス以外の情報だけを取得する場合は，上記のコンフィグレーションが設定されていないことを確認してください。

2. クライアント側の IPv6 インタフェースに，アドレス以外情報設定フラグを有効にする設定（コンフィグレーションコマンド ipv6 nd other-config-flag）がされていることを確認してください。アドレス以外情報設定フラグとは，DHCPv6 などの RA 以外の手段によって IPv6 アドレス以外の情報を端末に自動で取得させるフラグです。

   なお，DHCPv6 によって IPv6 アドレスだけを割り当てる場合は，上記のコンフィグレーションが設定されていないことを確認してください。

(4) DHCPv6 リレーエージェントと IPv6 マルチキャストを同時に運用している場合の確認

本装置で DHCPv6 リレーエージェントと IPv6 マルチキャストを同時に使用する場合，DHCPv6 リレーエージェントの転送先として各サーバを個別に設定していることを確認してください。もし，DHCPv6 パケットの転送先として全サーバ宛てを指定しているときは，次の点を確認してください。

- 本装置の対向ルータ側で，本装置と接続する IPv6 インタフェースのリンクローカルアドレスを IPv6 インタフェース内の最大値に設定して，IPv6 マルチキャストでの中継代表ルータ（DR）になるようにしているか

  なお，詳細な設定方法は対向ルータのマニュアルを参照してください。

- 対向ルータがランデブーポイントとなるように，本装置および対向ルータの IPv6 マルチキャストが設定されているか

5.3　ポリシーベースルーティングの通信障害

5.3.1　ポリシーベースルーティングによる通信障害の確認

本装置を使用しているネットワーク上で通信トラブルが発生する要因として，ポリシーベースルーティングが原因でパケットが期待したとおりに中継されていない，または廃棄されている可能性があります。

ポリシーベースルーティングによって，パケットを他インタフェースへ中継していないか，またはパケットを廃棄していないか確認する方法を次に示します。

1. show access-filter コマンドを実行して，ポリシーベースルーティングリストを動作に指定しているアクセスリストのフィルタ条件と，フィルタ条件に一致したパケット数を確認してください。
2. show ip interface コマンドまたは show ipv6 interface コマンドを実行して，エラー以外の受信廃棄パケット数を確認してください。
3. 1.および 2.で確認したパケット数と通信できないパケット数が一致している場合，フィルタ条件の動作に設定しているポリシーベースルーティングリストが原因でパケットが期待したとおりに中継されていない，または廃棄されている可能性があります。
4. ポリシーベースルーティングのコンフィグレーションが適切か確認してください。

5.3.2　ポリシーベースルーティングのトラブル

ポリシーベースルーティングの使用中に指定したネクストホップに中継されない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

また，ポリシーベースルーティングリストを動作に指定しているフィルタによるトラブルの可能性もあるため，次の手順に加えて，「6.1.1　フィルタのトラブル」を参照してください。

表 5–3　ポリシーベースルーティングの障害解析方法

項番	確認内容・コマンド	対応
1	ポリシーベースルーティングリストを設定しているフィルタの動作で，フィルタ条件に一致したパケット数を Matched packets で確認してください。 • show access-filter	通信できないパケット数と Matched packets の値が異なる場合は，次のどちらかの可能性があります。 ポリシーベースルーティングの対象外パケットである場合 　ポリシーベースルーティングの対象パケットについては，「コンフィグレーションガイド」を参照してください。 フィルタの検出条件が誤っている場合 　フィルタの設定を見直してください。 上記に該当しない場合は，項番 2 へ。
		通信できないパケット数と Matched packets の値が同じ場合は，項番 3 へ。
2	ポリシーベースルーティングリストを動作に指定しているフィルタを設定しているインタフェースで，エラー以外の受信廃棄パケット数を確認してください。 • show ip interface	通信できないパケット数とエラー以外の受信廃棄パケット数が異なる場合は，次のどちらかの可能性があります。

項番	確認内容・コマンド	対応
	• show ipv6 interface	ポリシーベースルーティングの対象外パケットである場合 ポリシーベースルーティングの対象パケットについては，「コンフィグレーションガイド」を参照してください。 フィルタの検出条件が誤っている場合 フィルタの設定を見直してください。
		通信できないパケット数とエラー以外の受信廃棄パケット数が同じ場合は，項番 3 へ。
3	ポリシーベースルーティングの動作で，"*>"が表示されている現在使用中のネクストホップを確認してください。 • show ip cache policy • show ipv6 cache policy	"*>"が表示されていない場合は，ネクストホップ選択抑止中の可能性があります。項番 4 へ。
		デフォルト動作に"*>"が表示されている場合は，項番 5 へ。
		期待していないネクストホップに"*>"が表示されている場合は，項番 5 へ。
		期待したネクストホップに"*>"が表示されている場合は，項番 6 へ。
4	ポリシーベースルーティングのネクストホップ選択抑止の開始日時と終了日時を確認してください。 • show ip cache policy • show ipv6 cache policy	End Time にだけ"-"が表示されている場合，ネクストホップ選択抑止中のため次の動作になっている可能性があります。 • 期待していないネクストホップへ中継 • ルーティングプロトコルに従った中継 • 廃棄 ネクストホップ選択抑止が終了するまで待ってください。
		Start Time および End Time のどちらも"-"，または日時が表示されている場合は，項番 7 へ。
5	ポリシーベースルーティングの送信先インタフェースの状態を確認してください。 • show ip interface • show ipv6 interface	期待したネクストホップの送信先インタフェースの状態が Up でない場合，次の動作になっている可能性があります。 • 期待していないネクストホップへ中継 • ルーティングプロトコルに従った中継 • 廃棄 送信先インタフェースの状態を Up にしてください。
		期待したネクストホップの送信先インタフェースの状態が Up の場合は，項番 6 へ。
6	期待したネクストホップの送信先インタフェースで，ネットワークの通信障害が発生していないか確認してください。	通信障害が発生している可能性があります。確認方法は，「5.1 IPv4 ネットワークの通信障害」および「5.2 IPv6 ネットワークの通信障害」を参照してください。 通信障害が発生している場合，参照先の対応に従ってください。 参照先の対応で解決できない場合は，項番 7 へ。
		通信障害が発生していない場合は，項番 7 へ。

項番	確認内容・コマンド	対応
7	リソース不足によってポリシーベースルーティングが未反映になっていないか確認してください。 • システムメッセージ（メッセージ種別：PSU，メッセージ識別子：3f000002）の出力を確認してください。 show logging • 使用中のエントリ数と使用できる最大エントリ数を確認してください。 show psu resources	該当するシステムメッセージが出力されている場合，または Shared resources Used/Max で使用中のエントリ数と使用できる最大エントリ数が等しい場合，収容条件に達したためにポリシーベースルーティングが未反映になっている可能性があります。ネットワーク構成を見直したあと，restart policy-based-routing コマンドを実行して，ポリシーベースルーティングを再反映してください。 上記の対応で解決できない場合は，項番８へ。
		該当するシステムメッセージが出力されていない場合，または Shared resources Used/Max で使用中のエントリ数が使用できる最大エントリ数より少ない場合は，項番８へ。
8	uRPF によってパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1.3　uRPF による廃棄を確認する」を参照してください。
		uRPF によってパケットが廃棄されていない場合は，項番９へ。
9	QoS によってフレームが廃棄されていないか確認してください。	確認方法と対応については，「8.1.2　QoS による廃棄を確認する」を参照してください。

5.4　VRRP の通信障害

5.4.1　VRRP 構成で通信できない

VRRP 構成で通信できない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 5-4　VRRP の障害解析方法

項番	確認内容・コマンド	対応
1	同一の仮想ルータを構成する相手装置と本装置で仮想ルータの状態を確認して，マスタとなっている装置が 1 台だけであり，ほかの装置はバックアップになっていることを確認してください。 • show vrrpstatus	仮想ルータの状態が正しい場合は，項番 2 へ。
		仮想ルータの状態が正しくない場合は，項番 3 へ。
2	仮想ルータの配下にほかのルータを経由しないで端末が接続されている場合，各端末のネットワーク設定でデフォルトゲートウェイとして仮想ルータの仮想 IP アドレスが設定されていることを確認してください。	• 本装置を含めた通信経路上の装置での経路情報を確認してください。 • 仮想ルータの配下にある各端末のネットワーク設定で，デフォルトゲートウェイとして仮想ルータの仮想 IP アドレスが設定されていない場合は，仮想ルータの仮想 IP アドレスをデフォルトゲートウェイに設定してください。
		通信経路上の装置での経路情報に問題がない場合は，項番 5 へ。
3	仮想ルータの状態が INITIAL でないことを確認してください。 • show vrrpstatus detail	仮想ルータの状態が INITIAL の場合は，次の点を確認してください。 • 現在の優先度が 0 でない場合，Admin State に表示されている非動作の要因を取り除いてください（非動作要因については，「運用コマンドレファレンス」を参照してください）。 • 現在の優先度が 0，かつ Admin State が(TRACK DOWN)の場合，トラッキング連携によって優先度が 0 になっています。トラック状態が想定される状態でない場合は，「6.3　トラッキング機能のトラブル」を参照してください。
		仮想ルータの状態が INITIAL でない場合は，項番 4 へ。
4	仮想ルータが設定されているインタフェースが運用中であることを確認してください。 • show port • show channel-group • show vlan detail	インタフェース状態が Up でも Forwarding でもない場合は，「3　ネットワークインタフェースのトラブルシュート」を参照してください。
		インタフェース状態が Up または Forwarding の場合は，項番 5 へ。
5	グループ切替機能が設定されているか確認してください。 • show vrrpstatus detail	グループ切替機能が設定されている場合は，項番 6 へ。
		グループ切替機能が設定されていない場合は，項番 7 へ。
6	従っているプライマリ仮想ルータの VRID と VLAN Tag の TPID が仮想ルータを構成し	プライマリ仮想ルータの VRID と VLAN Tag の TPID が仮想ルータを構成する装置間で異なる場合，複数の仮想ルータ

項番	確認内容・コマンド	対応
	ている装置間で一致しているか確認してください。 • show vrrpstatus • show ip interface	がマスタになります。仮想ルータを構成する装置のコンフィグレーションは必ず合わせてください。
		プライマリ仮想ルータの VRID と VLAN Tag の TPID が仮想ルータを構成する装置間で一致している場合は，項番 7 へ。 なお，項番 7 以降は，プライマリ仮想ルータについて確認してください。
7	仮想ルータを構成するルータ間の通信を，実 IPv4 アドレスまたは IPv6 アドレスで確認してください。 • ping • ping ipv6	仮想ルータを構成するルータ間が実 IPv4 アドレスまたは IPv6 アドレスで通信できない場合は，「5.1　IPv4 ネットワークの通信障害」および「5.2　IPv6 ネットワークの通信障害」を参照してください。
		仮想ルータを構成するルータ間が実 IPv4 アドレスまたは IPv6 アドレスで通信できる場合は，項番 8 へ。
8	フィルタまたは QoS によって ADVERTISEMENT パケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。 フィルタまたは QoS の設定がない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。
		ADVERTISEMENT パケットが廃棄されていない場合は，項番 9 へ。
9	ADVERTISEMENT パケットの送信間隔だけ時間を置いて次のコマンドを実行して，ADVERTISEMENT パケットの統計情報が増加するか確認してください。 • show vrrpstatus statistics	• 統計情報の<number of packets> with bad advertisement interval が増加する場合は，本装置と相手装置で ADVERTISEMENT パケット送信間隔の設定値が一致していることを確認してください。 • 統計情報の<number of packets> with authentication failed が増加する場合は，本装置と相手装置で認証パスワードの設定内容が一致していることを確認してください。 • 統計情報の<number of packets> with bad ip ttl が増加する場合は，本装置と相手装置間にほかのルータがないことを確認してください。 • 統計情報の<number of packets> with bad ipv6 hoplimit が増加する場合は，本装置と相手装置間にほかのルータがないことを確認してください。 • 統計情報の<number of packets> with bad ip address list が増加する場合は，仮想 IP アドレスの設定が同じであることを確認してください。 • 統計情報の<number of packets> with bad ipv6 address が増加する場合は，仮想 IP アドレスおよび VRRP 動作モードの設定が同じであることを確認してください。 • 統計情報の<number of packets> with bad authentication type が増加する場合は，本装置と相手装置で認証パスワードの設定有無を確認してください。 • 統計情報の<number of packets> with packet length error が増加する場合は，本装置と相手装置で VRRP 動作モードの設定が同じであることを確認してください。

項番	確認内容・コマンド	対応
		• 統計情報の<number of packets> with invalid type が増加する場合は，本装置と相手装置で VRRP 動作モードの設定が同じであることを確認してください。
		ADVERTISEMENT パケットが正常に受信されている場合は，相手装置を確認してください。 ADVERTISEMENT パケットが受信されていない場合は, 項番 10 へ。
10	イーサネットおよび装置の負荷を確認してください。 • 同一の仮想ルータを構成する相手装置が接続されているイーサネットの統計情報を確認してください。 show interfaces • CPU 使用率を確認してください。 show cpu bcu	同一の仮想ルータを構成する相手装置が接続されているイーサネットの Input rate および Output rate が高く, 回線の負荷が高い場合，および確認した CPU 使用率が高い場合は, 次に示す対策をしてください。 • 回線がループしている場合, ループ構成を見直してください。 • コンフィグレーションコマンド vrrp timers advertise で ADVERTISEMENT パケット送信間隔を長めに設定してください。 • コンフィグレーションコマンド vrrp preempt delay で自動切り戻し抑止時間を設定してください。
		イーサネットの負荷が低い場合は，同一の仮想ルータを構成する相手装置の動作を確認してください。

5.5　ユニキャストルーティングの通信障害

5.5.1　スタティック経路情報が存在しない

(1)　スタティック経路情報が存在しない

本装置が取得した経路情報の中に，スタティック経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

なお，DHCPv6 リレーエージェントが自動生成する IPv6 スタティック経路情報が存在しない場合は，「(2)　DHCPv6 リレーエージェントが自動生成する IPv6 スタティック経路情報が存在しない」の障害解析方法に従ってください。

また，VRF を使用していて，コンフィグレーションコマンド maximum routes または ipv6 maximum routes で経路の上限値を設定している場合，まず「5.5.5　VRF でユニキャスト経路情報が存在しない」の障害解析方法に従ってください。

表 5-5　スタティック経路の障害解析方法

項番	確認内容・コマンド	対応
1	スタティック経路の設定が正しいか，コンフィグレーションを確認してください。	コンフィグレーションが正しい場合は，項番 2 へ。
		コンフィグレーションが正しくない場合は，コンフィグレーションを修正してください。
2	スタティック経路のネクストホップアドレスを解決する経路情報が存在するか確認してください。 • show ip route • show ipv6 route	ネクストホップアドレスを解決する経路情報があり，動的監視機能を使用している場合は，項番 3 へ。
		ネクストホップアドレスを解決する経路情報があり，トラッキング連携を使用している場合は，連携しているトラックの状態を show track コマンドで確認してください。トラック状態が想定される状態でない場合は，「6.3　トラッキング機能のトラブル」を参照してください。
		ネクストホップアドレスを解決する経路情報がない場合は，その経路情報を学習するためのプロトコルの障害解析を実施してください。
3	スタティック経路のゲートウェイ情報を確認してください。 • show ip static gateway • show ipv6 static gateway	ポーリングが連続して成功した回数がカウントされている場合は，ゲートウェイへの到達性が安定するまで待ってください。
		ポーリングが連続して成功した回数が 0 のままカウントされていない場合は，項番 4 へ。
4	フィルタまたは QoS によって ICMP または ICMPv6 のパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。

(2)　DHCPv6 リレーエージェントが自動生成する IPv6 スタティック経路情報が存在しない

本装置が取得した経路情報の中に，DHCPv6 リレーエージェントが自動生成する IPv6 スタティック経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 5-6 DHCPv6 リレーエージェントの障害解析方法

項番	確認内容・コマンド	対応
1	DHCPv6 リレーエージェントのバインディング（IA_PD）を確認してください。 • show ipv6 dhcp relay binding	バインディング（IA_PD）が学習済みの場合は，項番 2 へ。
		バインディング（IA_PD）が学習されていない場合は，「5.2.2 DHCPv6 リレーエージェントで IPv6 アドレスが割り当てられない」を参照してください。
2	DHCPv6 リレーエージェントの設定（コンフィグレーションコマンド ipv6 dhcp relay static-route-setting）が正しいか，コンフィグレーションを確認してください。	DHCPv6 リレーエージェントで IPv6 スタティック経路を自動生成する設定がない場合は，コンフィグレーションを修正してください。

5.5.2 RIP または RIPng の経路情報が存在しない

本装置が取得した経路情報の中に，RIP または RIPng の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

また，VRF を使用していて，コンフィグレーションコマンド maximum routes または ipv6 maximum routes で経路の上限値を設定している場合，まず「5.5.5 VRF でユニキャスト経路情報が存在しない」の障害解析方法に従ってください。

表 5-7 RIP または RIPng の障害解析方法

項番	確認内容・コマンド	対応
1	RIP または RIPng の隣接情報を確認してください。 • show ip rip neighbor • show ipv6 rip neighbor	隣接ルータのインタフェースが表示されていない場合は，項番 2 へ。
		隣接ルータのインタフェースが表示されている場合は，項番 3 へ。
2	動作インタフェースまたはネットワーク，および RIP のバージョンについて，RIP または RIPng の設定が正しいか，コンフィグレーションを確認してください。	コンフィグレーションが正しい場合は，項番 3 へ。
		コンフィグレーションが正しくない場合は，コンフィグレーションを修正してください。
3	フィルタまたは QoS によって RIP または RIPng のパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1 パケット廃棄の確認」を参照してください。
		パケットが廃棄されていない場合は，隣接ルータが RIP 経路または RIPng 経路を広告しているか確認してください。

5.5.3 OSPF または OSPFv3 の経路情報が存在しない

本装置が取得した経路情報の中に，OSPF または OSPFv3 の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

また，VRF を使用していて，コンフィグレーションコマンド maximum routes または ipv6 maximum routes で経路の上限値を設定している場合，まず「5.5.5 VRF でユニキャスト経路情報が存在しない」の障害解析方法に従ってください。

表 5-8 OSPF または OSPFv3 の障害解析方法

項番	確認内容・コマンド	対応
1	OSPF または OSPFv3 のインタフェース状態を確認してください。 • show ip ospf interface <ip address> • show ipv6 ospf interface <interface type> <interface number>	インタフェース状態が BackupDR または DR Other の場合は，項番 2 へ。
		インタフェース状態が DR または P to P の場合は，項番 3 へ。
2	Neighbor List で DR との隣接ルータ状態を確認してください。	DR との隣接ルータ状態が Full 以外の場合は，項番 4 へ。
		DR との隣接ルータ状態が Full の場合は，項番 5 へ。
3	Neighbor List で全隣接ルータ状態を確認してください。	一部の隣接ルータ状態が Full 以外の場合は，項番 4 へ。
		全隣接ルータ状態が Full の場合は，項番 5 へ。
4	エリア，各種インターバル，および OSPF の認証について，OSPF または OSPFv3 の設定が正しいか，コンフィグレーションを確認してください。	コンフィグレーションが正しい場合は，項番 5 へ。
		コンフィグレーションが正しくない場合は，コンフィグレーションを修正してください。
5	OSPF 経路または OSPFv3 経路を学習している経路を確認してください。 • show ip route all-routes • show ipv6 route all-routes	経路が InActive の場合は，項番 6 へ。
		経路が存在しない場合は，隣接ルータが OSPF 経路または OSPFv3 経路を広告しているか確認してください。
6	フィルタまたは QoS によって OSPF または OSPFv3 のパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1 パケット廃棄の確認」を参照してください。
		パケットが廃棄されていない場合は，隣接ルータが OSPF 経路または OSPFv3 経路を広告しているか確認してください。

5.5.4 BGP4 または BGP4+の経路情報が存在しない

本装置が取得した経路情報の中に，BGP4 または BGP4+の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

また，VRF を使用していて，コンフィグレーションコマンド maximum routes または ipv6 maximum routes で経路の上限値を設定している場合，まず「5.5.5 VRF でユニキャスト経路情報が存在しない」の障害解析方法に従ってください。

表 5-9 BGP4 または BGP4+の障害解析方法

項番	確認内容・コマンド	対応
1	BGP4 または BGP4+のピア状態を確認してください。 • show ip bgp neighbors • show ipv6 bgp neighbors	ピア状態が Established 以外の場合は，項番 2 へ。
		ピア状態が Established の場合は，項番 3 へ。

項番	確認内容・コマンド	対応
2	AS 番号，ピアのアドレス，および認証について，BGP4 または BGP4+の設定が正しいか，コンフィグレーションを確認してください。	コンフィグレーションが正しい場合は，項番 3 へ。
		コンフィグレーションが正しくない場合は，コンフィグレーションを修正してください。
3	BGP4 経路または BGP4+経路を学習しているか確認してください。 • show ip bgp received-routes • show ipv6 bgp received-routes	経路が存在するが active でない場合は，項番 4 へ。
		経路が存在しない場合は，項番 5 へ。
4	BGP4 経路または BGP4+経路のネクストホップアドレスを解決する経路情報が存在するか確認してください。 • show ip route • show ipv6 route	ネクストホップアドレスを解決する経路情報がある場合は，項番 5 へ。
		ネクストホップアドレスを解決する経路情報がない場合は，その経路情報を学習するためのプロトコルの障害解析を実施してください。
5	フィルタまたは QoS によって BGP4 または BGP4+のパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。
		パケットが廃棄されていない場合は，隣接ルータが BGP4 経路または BGP4+経路を広告しているか確認してください。

5.5.5 VRF でユニキャスト経路情報が存在しない

本装置が取得した経路情報の中に，各プロトコルの経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 5-10　VRF の障害解析方法

項番	確認内容・コマンド	対応
1	VRF 内の経路数がコンフィグレーションで設定した上限値以上でないか確認してください。 • show ip vrf • show ipv6 vrf	経路数が上限値以上の場合は，項番 2 へ。
		経路数が上限値未満の場合は，存在しない経路のプロトコルの障害解析を実施してください。 • RIP または RIPng 「5.5.2　RIP または RIPng の経路情報が存在しない」 • OSPF または OSPFv3 「5.5.3　OSPF または OSPFv3 の経路情報が存在しない」 • BGP4 または BGP4+ 「5.5.4　BGP4 または BGP4+の経路情報が存在しない」
2	コンフィグレーションで VRF 内の経路数の上限値を確認してください。	上限値を増やすか，経路を集約するなどして経路数を減らしてください。

5.6 マルチキャストルーティングの通信障害

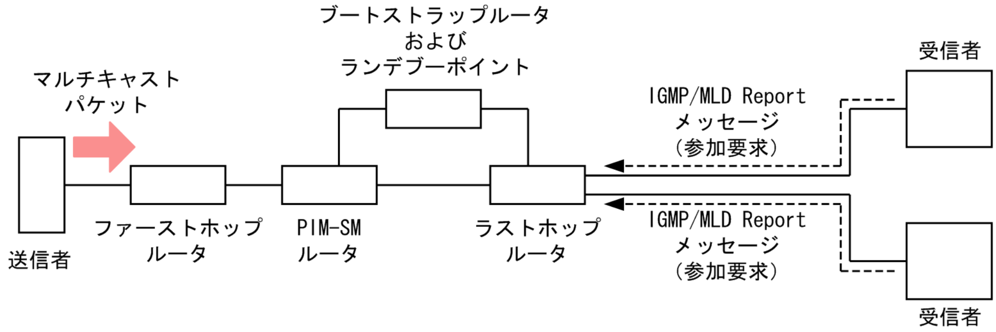
本装置で IPv4 マルチキャストまたは IPv6 マルチキャストの通信障害が発生した場合の対処について説明します。

5.6.1 PIM-SM ネットワークでマルチキャスト通信ができない

PIM-SM ネットワーク構成でマルチキャスト中継ができない場合は，次に示す障害解析方法に従って原因を切り分けてください。

PIM-SM ネットワーク例を次の図に示します。

図 5-6 PIM-SM ネットワーク例



図中の各ルータの役割は次のとおりです。

- ブートストラップルータ：ランデブーポイントの情報を送信するルータ
- ランデブーポイント：中継先が確定していないマルチキャストパケットを受信者方向に中継するルータ
- ファーストホップルータ：送信者と直接接続するルータ
- ラストホップルータ：受信者と直接接続するルータ
- PIM-SM ルータ：上記以外の PIM-SM が動作しているルータ

(1) 共通確認内容

PIM-SM ネットワーク構成で，すべての本装置に対する共通確認内容を次の表に示します。

表 5-11 共通確認内容

項番	確認内容・コマンド	対応
1	IPv4 マルチキャストルーティングプログラムまたは IPv6 マルチキャストルーティングプログラムが動作していることを確認してください。 • show ip pim interface • show ipv6 pim interface	IPv4 マルチキャストルーティングプログラムまたは IPv6 マルチキャストルーティングプログラムが動作していない場合は，項番 2 へ。
		IPv4 マルチキャストルーティングプログラムまたは IPv6 マルチキャストルーティングプログラムが動作している場合は，項番 6 へ。
2	マルチキャストルーティング機能を有効にする設定（コンフィグレーションコマンド ip multicast routing または ipv6 multicast	IPv4 マルチキャストルーティング機能を有効にする設定がある場合は，項番 3 へ。

項番	確認内容・コマンド	対応
	routing）があることを，コンフィグレーションで確認してください。 • show running-config	IPv6 マルチキャストルーティング機能を有効にする設定がある場合は，項番 4 へ。
		マルチキャストルーティング機能を有効にする設定がない場合は，コンフィグレーションを修正してください。
3	IPv4 マルチキャスト使用時は，該当インタフェースにマルチホームを設定していないことを，コンフィグレーションで確認してください。 • show running-config	マルチホームを設定していない場合は，項番 5 へ。
		マルチホームは未サポートです。マルチホームを設定している場合は，コンフィグレーションを修正してください。
4	IPv6 マルチキャスト使用時は，ループバックインタフェースに IPv6 アドレスを設定していることを，コンフィグレーションで確認してください。 • show running-config	ループバックインタフェースに IPv6 アドレスを設定している場合は，項番 5 へ。
		ループバックインタフェースに IPv6 アドレスを設定していない場合は，コンフィグレーションを修正してください。
5	一つ以上のインタフェースで PIM-SM が動作していることを確認してください。 • show ip pim interface • show ipv6 pim interface	PIM-SM が動作している場合は，項番 6 へ。
		PIM-SM が動作していない場合は，一つ以上のインタフェースで PIM-SM が動作するようにコンフィグレーションを修正してください。
6	マルチキャストが使用できる経路配分パターンを設定しているか，コンフィグレーションを確認してください。 • show running-config	マルチキャストが使用できる経路配分パターンを設定している場合は，項番 7 へ。
		マルチキャストが使用できる経路配分パターンを設定していない場合は，コンフィグレーションを修正してください。経路配分パターンの変更方法については,「コンフィグレーションコマンドレファレンス」を参照してください。 経路配分パターンを変更したあと，項番 23 へ。
7	IPv4 PIM-SM が動作するインタフェースに，IGMP snooping を設定しているか確認してください。 IPv6 PIM-SM が動作するインタフェースに，MLD snooping を設定しているか確認してください。 • show igmp-snooping • show mld-snooping	IGMP/MLD snooping を設定していない場合は，項番 8 へ。
		IGMP/MLD snooping を設定している場合は，次の内容を確認してください。 • 隣接ルータと接続しているポートに対して IGMP/MLD snooping のマルチキャストルータポートの設定をしているか確認してください。 •「4.4　IGMP/MLD snooping の通信障害」を参照して，IGMP/MLD snooping の設定を確認してください。 IGMP/MLD snooping の設定が正しい場合は，項番 8 へ。
8	PIM-SM，IGMP および MLD が動作するインタフェースで, フィルタまたは QoS によってプロトコルパケットやマルチキャストパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。
		パケットが廃棄されていない場合は，項番 9 へ。
9	送信者，ランデブーポイントおよびブートストラップルータへのユニキャスト経路が存在するか確認してください。	ユニキャスト経路が存在する場合は，項番 10 へ。

項番	確認内容・コマンド	対応
	• show ip route • show ipv6 route	ユニキャスト経路が存在しない場合は，「5.5　ユニキャストルーティングの通信障害」を参照してください。
10	送信者，ランデブーポイントおよびブートストラップルータへのネクストホップアドレスと接続しているインタフェースで，PIM-SM が動作していることを確認してください。 • show ip pim interface • show ipv6 pim interface	PIM-SM が動作している場合は，項番 11 へ。
		PIM-SM が動作していない場合は，送信者，ランデブーポイントおよびブートストラップルータへのネクストホップアドレスと接続しているインタフェースで PIM-SM が動作するようにコンフィグレーションを修正してください。
11	PIM-SM の隣接情報を確認してください。 • show ip pim neighbor • show ipv6 pim neighbor	項番 9 で確認した経路のネクストホップがすべて隣接ルータとして表示されている場合は，項番 12 へ。
		項番 9 で確認した経路のネクストホップのうち隣接ルータとして表示されていないものがある場合は，表示されていない隣接ルータの設定を確認してください。
12	PIM-SSM で使用するアドレス範囲に中継対象グループアドレスが含まれていないことを，コンフィグレーションで確認してください。 • show running-config	PIM-SSM で使用するアドレス範囲に中継対象グループアドレスが含まれていない場合は，項番 13 へ。
		PIM-SSM で使用するアドレス範囲に中継対象グループアドレスが含まれている場合は，コンフィグレーションを修正してください。
13	中継対象グループアドレスに対するランデブーポイントが静的ランデブーポイントでない場合は，ブートストラップルータが決定していることを確認してください。 • show ip pim bsr • show ipv6 pim bsr	ブートストラップルータが決定している場合は，項番 14 へ。
		ブートストラップルータが決定していない場合は，ブートストラップルータへのユニキャスト経路が存在するか確認してください。ユニキャスト経路が存在しない場合は，「5.5　ユニキャストルーティングの通信障害」を参照してください。 ユニキャスト経路が存在する場合は，ブートストラップルータの設定を確認してください。ブートストラップルータが本装置の場合は，「(2)　ブートストラップルータ確認内容」を参照してください。
14	ランデブーポイントが決定していることを確認してください。 • show ip pim rp-mapping • show ipv6 pim rp-mapping	ランデブーポイントが決定している場合は，項番 15 へ。
		ランデブーポイントが決定していない場合は，ランデブーポイントへのユニキャスト経路が存在するか確認してください。ユニキャスト経路が存在しない場合は，「5.5　ユニキャストルーティングの通信障害」を参照してください。 ユニキャスト経路が存在する場合は，ランデブーポイントの設定を確認してください。ランデブーポイントが本装置の場合は，「(3)　ランデブーポイント確認内容」を参照してください。
15	ランデブーポイントのグループアドレスに，中継対象グループアドレスが含まれていることを確認してください。 • show ip pim rp-mapping • show ipv6 pim rp-mapping	中継対象グループアドレスが含まれている場合は，項番 16 へ。
		中継対象グループアドレスが含まれていない場合は，ランデブーポイントの設定を確認してください。ランデブーポイントが本装置の場合は，「(3)　ランデブーポイント確認内容」を参照してください。

項番	確認内容・コマンド	対応
16	ネットワーク内のすべての本装置で，中継対象グループアドレスのランデブーポイントが同じことを確認してください。 • show ip pim rp-hash • show ipv6 pim rp-hash	ランデブーポイントが同じ場合は，項番 17 へ。
		ランデブーポイントが異なる場合は，ランデブーポイントの設定を確認してください。
17	ネットワーク内のすべての本装置で，ランデブーポイント選出アルゴリズムが同じことを確認してください。 • show running-config	ランデブーポイント選出アルゴリズムが同じ場合は，項番 18 へ。
		ランデブーポイント選出アルゴリズムが異なる場合は，コンフィグレーションを修正してください。
18	マルチキャスト中継エントリが存在することを確認してください。 • show ip mcache • show ipv6 mcache	マルチキャスト中継エントリが存在する場合は，項番 19 へ。
		マルチキャスト中継エントリが存在しない場合は，上流インタフェースにマルチキャストパケットが届いていることを確認してください。マルチキャストパケットが届いていない場合は，送信者または上流ルータの設定を確認してください。
19	マルチキャスト中継エントリ数が最大数（コンフィグレーションコマンド ip pim mcache-limit または ipv6 pim mcache-limit の設定値）に到達していないか確認してください。 • show ip mcache • show ipv6 mcache	Warning が表示されていない場合は，項番 20 へ。
		Warning が表示されている場合は，マルチキャスト中継エントリ数が最大数に到達しています。ネットワーク構成を見直して範囲内で運用してください。 また，ネガティブキャッシュエントリが想定以上に生成されている場合は，不要なマルチキャストパケットを送信している端末が存在しないか確認してください。
20	マルチキャスト経路情報が存在することを確認してください。 • show ip mroute • show ipv6 mroute	マルチキャスト経路情報が存在する場合は，項番 21 へ。
		マルチキャスト経路情報が存在しない場合は，下流ルータの設定を確認してください。
21	マルチキャスト経路情報数が最大数（コンフィグレーションコマンド ip pim mroute-limit または ipv6 pim mroute-limit の設定値）に到達していないか確認してください。 • show ip mroute • show ipv6 mroute	Warning が表示されていない場合は，項番 22 へ。
		Warning が表示されている場合は，マルチキャスト経路情報数が最大数に到達しています。ネットワーク構成を見直して範囲内で運用してください。
22	IPv4 マルチキャスト使用時は TTL 値が 1，IPv6 マルチキャスト使用時はホップリミット値が 1 のマルチキャストパケットを受信していないか確認してください。 • show tcpdump	TTL 値またはホップリミット値が 1 でない場合は，項番 23 へ。
		TTL 値またはホップリミット値が 1 の場合は，本装置では該当するマルチキャストパケットを中継しません。送信者の設定を修正してください。
23	マルチキャスト中継エントリ数が収容条件に到達しているシステムメッセージ※が表示されていないか確認してください。 • show logging	システムメッセージが表示されていない場合は，項番 24 へ。
		システムメッセージが表示されている場合は，マルチキャスト中継エントリ数が収容条件に到達しています。 収容条件に到達したあとはマルチキャスト中継エントリを設定できないため，収容条件に到達した状態での運用は推奨し

項番	確認内容・コマンド	対応
		ません。ネットワーク構成を見直して収容条件内で運用してください。 ネットワーク構成を見直したあと，restart ipv4-multicast または restart ipv6-multicast コマンドを実行して，マルチキャスト中継エントリを再設定してください。
24	マルチキャスト中継エントリの延べ下流インタフェース数が収容条件に到達しているシステムメッセージ（メッセージ種別：PSU，メッセージ識別子：41023002）が表示されていないか確認してください。 • show logging	システムメッセージが表示されている場合は，マルチキャスト中継エントリの延べ下流インタフェース数が収容条件に到達しています。 収容条件に到達したあとは下流インタフェースを設定できないため，収容条件に到達した状態での運用は推奨しません。ネットワーク構成を見直して収容条件内で運用してください。なお，延べ下流インタフェース数は，IPv4 マルチキャストと IPv6 マルチキャストの合計です。 ネットワーク構成を見直したあと，restart ipv4-multicast および restart ipv6-multicast コマンドをどちらも実行して，マルチキャスト中継エントリを再設定してください。

注※

IPv4 マルチキャスト中継エントリ数が収容条件に到達しているときはシステムメッセージ（メッセージ種別：PSU，メッセージ識別子：41021002），IPv6 マルチキャスト中継エントリ数が収容条件に到達しているときはシステムメッセージ（メッセージ種別：PSU，メッセージ識別子：41022002）が表示されます。

(2) ブートストラップルータ確認内容

PIM-SM ネットワーク構成で，本装置がブートストラップルータの場合の確認内容を次の表に示します。

表 5-12 ブートストラップルータ確認内容

項番	確認内容・コマンド	対応
1	本装置がブートストラップルータ候補であることを確認してください。 • show ip pim bsr • show ipv6 pim bsr	本装置がブートストラップルータ候補でない場合は，項番 2 へ。
		本装置がブートストラップルータ候補の場合は，項番 4 へ。
2	ループバックインタフェースに IPv4 マルチキャスト使用時は IPv4 アドレスを，IPv6 マルチキャスト使用時は IPv6 アドレスを設定しているか，コンフィグレーションを確認してください。 • show running-config	ループバックインタフェースに IPv4 アドレスまたは IPv6 アドレスを設定している場合は，項番 3 へ。
		ループバックインタフェースに IPv4 アドレスまたは IPv6 アドレスを設定していない場合は，コンフィグレーションを修正してください。
3	ブートストラップルータ候補の設定で，IPv4 マルチキャスト使用時はループバックインタフェース番号を，IPv6 マルチキャスト使用時はループバックインタフェースの IPv6 アドレスを指定しているか，コンフィグレーションを確認してください。 • show running-config	ブートストラップルータ候補の設定が正しい場合は，項番 4 へ。
		ブートストラップルータ候補の設定が正しくない場合は，コンフィグレーションを修正してください。

項番	確認内容・コマンド	対応
4	本装置がブートストラップルータであることを確認してください。 • show ip pim bsr • show ipv6 pim bsr	本装置がブートストラップルータでない場合は，ほかのブートストラップルータ候補の優先度を確認してください。優先度は値の大きい方が高くなります。優先度が同じ場合は，IPv4 アドレスまたは IPv6 アドレスがいちばん大きいブートストラップルータ候補がブートストラップルータとなります。

(3)　ランデブーポイント確認内容

PIM-SM ネットワーク構成で，本装置がランデブーポイントの場合の確認内容を次の表に示します。

表 5-13　ランデブーポイント確認内容

項番	確認内容・コマンド	対応
1	本装置が中継対象グループアドレスに対するランデブーポイント候補であることを確認してください。 • show ip pim rp-mapping • show ipv6 pim rp-mapping	本装置がランデブーポイント候補でない場合は，項番 2 へ。 本装置がランデブーポイント候補の場合は，項番 4 へ。
2	ループバックインタフェースに IPv4 マルチキャスト使用時は IPv4 アドレスを，IPv6 マルチキャスト使用時は IPv6 アドレスを設定しているか，コンフィグレーションを確認してください。 • show running-config	ループバックインタフェースに IPv4 アドレスまたは IPv6 アドレスを設定している場合は，項番 3 へ。 ループバックインタフェースに IPv4 アドレスまたは IPv6 アドレスを設定していない場合は，コンフィグレーションを修正してください。
3	ランデブーポイント候補の設定で，IPv4 マルチキャスト使用時はループバックインタフェース番号を，IPv6 マルチキャスト使用時はループバックインタフェースの IPv6 アドレスを指定しているか，コンフィグレーションを確認してください。 • show running-config	ランデブーポイント候補の設定が正しい場合は，項番 4 へ。 ランデブーポイント候補の設定が正しくない場合は，コンフィグレーションを修正してください。
4	本装置が中継対象グループアドレスに対するランデブーポイントであることを確認してください。 • show ip pim rp-hash • show ipv6 pim rp-hash	本装置がランデブーポイントでない場合は，ほかのランデブーポイント候補の優先度を確認してください。優先度は値の小さい方が高くなります。優先度が同じ場合は，プロトコルの仕様でグループアドレス単位に分散され，該当マルチキャストグループに対してランデブーポイントとして動作しないことがあります。 本装置を優先的にランデブーポイントとして動作させる場合は，ほかのランデブーポイント候補より高い優先度を設定してください。

(4)　ラストホップルータ確認内容

PIM-SM ネットワーク構成で，本装置がラストホップルータの場合の確認内容を次の表に示します。

表 5-14　ラストホップルータ確認内容

項番	確認内容・コマンド	対応
1	受信者と接続しているインタフェースで，IGMP または MLD が動作していることを確認してください。 • show ip igmp interface • show ipv6 mld interface	IGMP または MLD が動作していない場合は，IGMP または MLD が動作するようにコンフィグレーションを修正してください。
2	受信者が，IGMP または MLD で中継対象マルチキャストグループに参加していることを確認してください。 • show ip igmp group • show ipv6 mld group	受信者が中継対象マルチキャストグループに参加していない場合は，受信者の設定を確認してください。
3	中継対象マルチキャストグループに参加しているインタフェースがある場合は，本装置が DR であることを確認してください。 • show ip pim interface • show ipv6 pim interface	本装置が DR でない場合は，中継対象インタフェースの DR を確認してください。
4	静的グループ参加機能を使用しているインタフェースがある場合は，本装置が DR であることを確認してください。 • show ip pim interface • show ipv6 pim interface	本装置が DR でない場合は，中継対象インタフェースの DR である装置に静的グループ参加機能を設定してください。
5	静的グループ参加機能が動作するインタフェースに，IGMP snooping または MLD snooping を設定しているか確認してください。 • show igmp-snooping • show mld-snooping	IGMP/MLD snooping を設定している場合は，次の内容を確認してください。 • 中継先ポートに対して IGMP/MLD snooping のマルチキャストルータポートの設定をしているか確認してください。 • 「4.4　IGMP/MLD snooping の通信障害」を参照して，IGMP/MLD snooping の設定を確認してください。
6	各インタフェースで異常を検出していないか確認してください。 • show ip igmp interface • show ipv6 mld interface	Notice に警告情報が表示されていないことを確認してください。 警告情報が表示されている場合は，次の内容を確認してください。 L： 次のどれかの上限値に到達しているため，IGMP Report メッセージまたは MLD Report メッセージ（もしくはメッセージ内の Record 情報）を廃棄しています。受信者数を確認してください。 • マルチキャストグループ数（コンフィグレーションコマンド ip igmp group-limit または ipv6 mld group-limit の設定値） • ソース数（コンフィグレーションコマンド ip igmp source-limit または ipv6 mld source-limit の設定値）

項番	確認内容・コマンド	対応
		• マルチキャストチャネル数（コンフィグレーションコマンド ipv6 mld channel-limit の設定値） • ホストトラッキング機能で保持している受信者数（コンフィグレーションコマンド ipv6 mld explicit-tracking の設定値） Q： 隣接するルータと IGMP または MLD のバージョンが不一致です。IGMP または MLD のバージョンを一致させてください。 R： 現在の設定では受信できない IGMP Report メッセージまたは MLD Report メッセージを送信している受信者が存在します。本装置の IGMP または MLD のバージョンを変更するか，受信者の設定を確認してください。 S： IGMPv3 または MLDv2 で 1 メッセージ内に格納できるソース数が上限を超えたため，参加情報を一部廃棄しています。受信者の設定を確認してください。 F： マルチキャストチャネルフィルタ機能（コンフィグレーションコマンド ipv6 mld access-group）によって，MLD Report メッセージまたは MLD Report メッセージ内の Record 情報を廃棄しています。show ipv6 mld access-group コマンドを実行して，対象の参加要求が許可されているかどうかを確認してください。 B： MLD インタフェース単位の帯域管理機能（コンフィグレーションコマンド ipv6 mld bandwidth-limit）によって，MLD Report メッセージまたは MLD Report メッセージ内の Record 情報を廃棄しています。show ipv6 mld bandwidth コマンドを実行して，対象 MLD インタフェースの帯域使用状況を確認してください。

(5)　ファーストホップルータ確認内容

PIM-SM ネットワーク構成で，本装置がファーストホップルータの場合の確認内容を次の表に示します。

表 5-15　ファーストホップルータ確認内容

項番	確認内容・コマンド	対応
1	本装置が送信者と直接接続していて，送信者からのマルチキャストパケットが本装置に届いていることを確認してください。 • show interface	マルチキャストパケットが届いていない場合は，ネットワーク構成および送信者の設定を確認してください。
2	送信者と接続しているインタフェースで，PIM-SM，IGMP または MLD が動作していることを確認してください。	PIM-SM，IGMP または MLD が動作していない場合は，PIM-SM，IGMP または MLD が動作するようにコンフィグレーションを修正してください。

項番	確認内容・コマンド	対応
	• show ip pim interface • show ip igmp interface • show ipv6 pim interface • show ipv6 mld interface	
3	マルチキャスト経路情報が存在するか確認してください。 • show ip mroute • show ipv6 mroute	マルチキャスト経路情報が存在しない場合は，マルチキャストパケットの送信元アドレスが，送信者と直接接続しているインタフェースのネットワークアドレスであることを確認してください。

5.6.2　PIM-SM ネットワークでマルチキャストパケットが二重中継される

PIM-SM ネットワーク構成でマルチキャストパケットが二重中継される場合は，各ルータの設定内容を確認して，同一ネットワークに複数のルータが存在するインタフェースでは PIM-SM が動作するように設定してください。

また，MLD の静的グループ参加機能（コンフィグレーションコマンド ipv6 mld static-group）で ignore-dr パラメータを設定している場合，本装置は DR でなくてもマルチキャストパケットを中継します。そのため，PIM-SM が動作している場合でも，一時的に二重中継が発生することがあります。なお，この二重中継は PIM Assert メッセージの送受信で停止します。

PIM-SM の設定をしても二重中継が継続する場合の確認内容を次の表に示します。

表 5–16　二重中継が継続する場合の確認内容

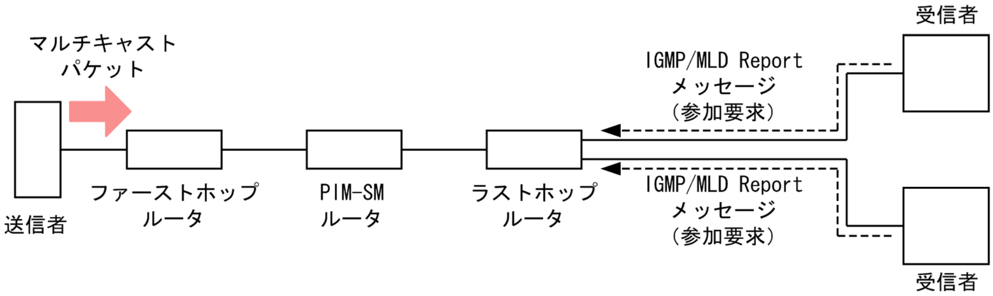
項番	確認内容・コマンド	対応
1	同一ネットワークに複数のルータが存在するインタフェースの PIM-SM の隣接情報を確認してください。 • show ip pim neighbor • show ipv6 pim neighbor	隣接ルータが表示されない場合は，次の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM-SM が動作していることを，show ip pim interface または show ipv6 pim interface コマンドで確認してください。 • フィルタまたは QoS によってプロトコルパケットが廃棄されていないか確認してください。確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。 • 隣接ルータの設定を確認してください。

5.6.3　PIM-SSM ネットワークでマルチキャスト通信ができない

PIM-SSM ネットワーク構成でマルチキャスト中継ができない場合は，次に示す障害解析方法に従って原因を切り分けてください。

PIM-SSM ネットワーク例を次の図に示します。

図 5-7　PIM-SSM ネットワーク例



図中の各ルータの役割は次のとおりです。

- ファーストホップルータ：送信者と直接接続するルータ
- ラストホップルータ：受信者と直接接続するルータ
- PIM-SM ルータ：上記以外の PIM-SM が動作しているルータ

(1)　共通確認内容

PIM-SSM ネットワーク構成で，すべての本装置に対する共通確認内容を次の表に示します。

表 5-17　共通確認内容

項番	確認内容・コマンド	対応
1	IPv4 マルチキャストルーティングプログラムまたは IPv6 マルチキャストルーティングプログラムが動作していることを確認してください。 • show ip pim interface • show ipv6 pim interface	IPv4 マルチキャストルーティングプログラムまたは IPv6 マルチキャストルーティングプログラムが動作していない場合は，項番 2 へ。
		IPv4 マルチキャストルーティングプログラムまたは IPv6 マルチキャストルーティングプログラムが動作している場合は，項番 6 へ。
2	マルチキャストルーティング機能を有効にする設定（コンフィグレーションコマンド ip multicast routing または ipv6 multicast routing）があることを，コンフィグレーションで確認してください。 • show running-config	IPv4 マルチキャストルーティング機能を有効にする設定がある場合は，項番 3 へ。
		IPv6 マルチキャストルーティング機能を有効にする設定がある場合は，項番 4 へ。
		マルチキャストルーティング機能を有効にする設定がない場合は，コンフィグレーションを修正してください。
3	IPv4 マルチキャスト使用時は，該当インタフェースにマルチホームを設定していないことを，コンフィグレーションで確認してください。 • show running-config	マルチホームを設定していない場合は，項番 5 へ。
		マルチホームは未サポートです。マルチホームを設定している場合は，コンフィグレーションを修正してください。
4	IPv6 マルチキャスト使用時は，ループバックインタフェースに IPv6 アドレスを設定していることを，コンフィグレーションで確認してください。 • show running-config	ループバックインタフェースに IPv6 アドレスを設定している場合は，項番 5 へ。
		ループバックインタフェースに IPv6 アドレスを設定していない場合は，コンフィグレーションを修正してください。

項番	確認内容・コマンド	対応
5	一つ以上のインタフェースで PIM-SM が動作していることを確認してください。 • show ip pim interface • show ipv6 pim interface	PIM-SM が動作している場合は，項番 6 へ。
		PIM-SM が動作していない場合は，一つ以上のインタフェースで PIM-SM が動作するようにコンフィグレーションを修正してください。
6	マルチキャストが使用できる経路配分パターンを設定しているか，コンフィグレーションを確認してください。 • show running-config	マルチキャストが使用できる経路配分パターンを設定している場合は，項番 7 へ。
		マルチキャストが使用できる経路配分パターンを設定していない場合は，コンフィグレーションを修正してください。経路配分パターンの変更方法については，「コンフィグレーションコマンドレファレンス」を参照してください。 経路配分パターンを変更したあと，項番 17 へ。
7	IPv4 PIM-SM が動作するインタフェースに，IGMP snooping を設定しているか確認してください。 IPv6 PIM-SM が動作するインタフェースに，MLD snooping を設定しているか確認してください。 • show igmp-snooping • show mld-snooping	IGMP/MLD snooping を設定していない場合は，項番 8 へ。
		IGMP/MLD snooping を設定している場合は，次の内容を確認してください。 • 隣接ルータと接続しているポートに対して IGMP/MLD snooping のマルチキャストルータポートの設定をしているか確認してください。 • 「4.4　IGMP/MLD snooping の通信障害」を参照して，IGMP/MLD snooping の設定を確認してください。 IGMP/MLD snooping の設定が正しい場合は，項番 8 へ。
8	PIM-SM，IGMP および MLD が動作するインタフェースで，フィルタまたは QoS によってプロトコルパケットやマルチキャストパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。
		パケットが廃棄されていない場合は，項番 9 へ。
9	送信者へのユニキャスト経路が存在するか確認してください。 • show ip route • show ipv6 route	ユニキャスト経路が存在する場合は，項番 10 へ。
		ユニキャスト経路が存在しない場合は，「5.5　ユニキャストルーティングの通信障害」を参照してください。
10	送信者へのネクストホップアドレスと接続しているインタフェースで，PIM-SM が動作していることを確認してください。 • show ip pim interface • show ipv6 pim interface	PIM-SM が動作している場合は，項番 11 へ。
		PIM-SM が動作していない場合は，送信者へのネクストホップアドレスと接続しているインタフェースで PIM-SM が動作するようにコンフィグレーションを修正してください。
11	PIM-SM の隣接情報を確認してください。 • show ip pim neighbor • show ipv6 pim neighbor	項番 9 で確認した経路のネクストホップがすべて隣接ルータとして表示されている場合は，項番 12 へ。
		項番 9 で確認した経路のネクストホップのうち隣接ルータとして表示されていないものがある場合は，表示されていない隣接ルータの設定を確認してください。

項番	確認内容・コマンド	対応
12	PIM-SSM で使用するアドレス範囲に中継対象グループアドレスが含まれていることを，コンフィグレーションで確認してください。 • show running-config	PIM-SSM で使用するアドレス範囲に中継対象グループアドレスが含まれている場合は，項番 13 へ。
		PIM-SSM で使用するアドレス範囲に中継対象グループアドレスが含まれていない場合は，コンフィグレーションを修正してください。
13	マルチキャスト中継エントリが存在することを確認してください。 • show ip mcache • show ipv6 mcache	マルチキャスト中継エントリが存在する場合は，項番 14 へ。
		マルチキャスト中継エントリが存在しない場合は，上流インタフェースにマルチキャストパケットが届いていることを確認してください。マルチキャストパケットが届いていない場合は，送信者または上流ルータの設定を確認してください。
14	マルチキャスト中継エントリ数が最大数（コンフィグレーションコマンド ip pim mcache-limit または ipv6 pim mcache-limit の設定値）に到達していないか確認してください。 • show ip mcache • show ipv6 mcache	Warning が表示されていない場合は，項番 15 へ。
		Warning が表示されている場合は，マルチキャスト中継エントリ数が最大数に到達しています。ネットワーク構成を見直して範囲内で運用してください。 また，ネガティブキャッシュエントリが想定以上に生成されている場合は，不要なマルチキャストパケットを送信している端末が存在しないか確認してください。
15	マルチキャスト経路情報が存在することを確認してください。 • show ip mroute • show ipv6 mroute	マルチキャスト経路情報が存在する場合は，項番 16 へ。
		マルチキャスト経路情報が存在しない場合は，下流ルータの設定を確認してください。
16	マルチキャスト経路情報数が最大数（コンフィグレーションコマンド ip pim mroute-limit または ipv6 pim mroute-limit の設定値）に到達していないか確認してください。 • show ip mroute • show ipv6 mroute	Warning が表示されていない場合は，項番 17 へ。
		Warning が表示されている場合は，マルチキャスト経路情報数が最大数に到達しています。ネットワーク構成を見直して範囲内で運用してください。
17	IPv4 マルチキャスト使用時は TTL 値が 1，IPv6 マルチキャスト使用時はホップリミット値が 1 のマルチキャストパケットを受信していないか確認してください。 • show tcpdump	TTL 値またはホップリミット値が 1 でない場合は，項番 18 へ。
		TTL 値またはホップリミット値が 1 の場合は，本装置では該当するマルチキャストパケットを中継しません。送信者の設定を修正してください。
18	マルチキャスト中継エントリ数が収容条件に到達しているシステムメッセージ※が表示されていないか確認してください。 • show logging	システムメッセージが表示されていない場合は，項番 19 へ。
		システムメッセージが表示されている場合は，マルチキャスト中継エントリ数が収容条件に到達しています。 収容条件に到達したあとはマルチキャスト中継エントリを設定できないため，収容条件に到達した状態での運用は推奨しません。ネットワーク構成を見直して収容条件内で運用してください。 ネットワーク構成を見直したあと，restart ipv4-multicast または restart ipv6-multicast コマンドを実行して，マルチキャスト中継エントリを再設定してください。

項番	確認内容・コマンド	対応
19	マルチキャスト中継エントリの延べ下流インタフェース数が収容条件に到達しているシステムメッセージ（メッセージ種別：PSU，メッセージ識別子：41023002）が表示されていないか確認してください。 • show logging	システムメッセージが表示されている場合は，マルチキャスト中継エントリの延べ下流インタフェース数が収容条件に到達しています。 収容条件に到達したあとは下流インタフェースを設定できないため，収容条件に到達した状態での運用は推奨しません。ネットワーク構成を見直して収容条件内で運用してください。なお，延べ下流インタフェース数は，IPv4 マルチキャストと IPv6 マルチキャストの合計です。 ネットワーク構成を見直したあと，restart ipv4-multicast および restart ipv6-multicast コマンドをどちらも実行して，マルチキャスト中継エントリを再設定してください。

注※

IPv4 マルチキャスト中継エントリ数が収容条件に到達しているときはシステムメッセージ（メッセージ種別：PSU，メッセージ識別子：41021002），IPv6 マルチキャスト中継エントリ数が収容条件に到達しているときはシステムメッセージ（メッセージ種別：PSU，メッセージ識別子：41022002）が表示されます。

(2) ラストホップルータ確認内容

PIM-SSM ネットワーク構成で，本装置がラストホップルータの場合の確認内容を次の表に示します。

表 5-18　ラストホップルータ確認内容

項番	確認内容・コマンド	対応
1	受信者と接続しているインタフェースで，IGMP または MLD が動作していることを確認してください。 • show ip igmp interface • show ipv6 mld interface	IGMP または MLD が動作していない場合は，IGMP または MLD が動作するようにコンフィグレーションを修正してください。
2	受信者が IGMPv1/IGMPv2/IGMPv3（EXCLUDE モード）または MLDv1/MLDv2（EXCLUDE モード）を使用する場合は，IGMP/MLD PIM-SSM 連携機能の設定（コンフィグレーションコマンド ip igmp ssm-map enable または ipv6 mld ssm-map enable）があることを，コンフィグレーションで確認してください。 • show running-config	IGMP/MLD PIM-SSM 連携機能の設定がない場合は，コンフィグレーションを修正してください。
3	受信者が IGMPv1/IGMPv2/IGMPv3（EXCLUDE モード）または MLDv1/MLDv2（EXCLUDE モード）を使用する場合は，PIM-SSM で中継するグループアドレスと送信元アドレスを IGMP/MLD PIM-SSM 連携機能の設定（コンフィグレーションコマンド ip igmp ssm-map static または ipv6 mld ssm-map static）で指定していることを，コンフィグレーションで確認してください。 • show running-config	PIM-SSM で中継するグループアドレスと送信元アドレスを指定していない場合は，コンフィグレーションを修正してください。

項番	確認内容・コマンド	対応
4	受信者が，IGMP または MLD で中継対象マルチキャストグループに参加していることを確認してください。 • show ip igmp group • show ipv6 mld group	受信者が中継対象マルチキャストグループに参加していない場合は，受信者の設定を確認してください。
5	IGMP/MLD PIM-SSM 連携機能を使用している場合は，該当するマルチキャストグループの Source Address に送信元アドレスが表示されていることを確認してください。 • show ip igmp group • show ipv6 mld group	Source Address に送信元アドレスが表示されていない場合は，IGMP/MLD PIM-SSM 連携機能の設定が不正です。コンフィグレーションを修正してください。
6	中継対象マルチキャストグループに参加しているインタフェースがある場合は，本装置が DR であることを確認してください。 • show ip pim interface • show ipv6 pim interface	本装置が DR でない場合は，中継対象インタフェースの DR を確認してください。
7	静的グループ参加機能を使用しているインタフェースがある場合は，本装置が DR であることを確認してください。 • show ip pim interface • show ipv6 pim interface	本装置が DR でない場合は，中継対象インタフェースの DR である装置に静的グループ参加機能を設定してください。
8	静的グループ参加機能が動作するインタフェースに，IGMP snooping または MLD snooping を設定しているか確認してください。 • show igmp-snooping • show mld-snooping	IGMP/MLD snooping を設定している場合は，次の内容を確認してください。 • 中継先ポートに対して IGMP/MLD snooping のマルチキャストルータポートの設定をしているか確認してください。 • 「4.4　IGMP/MLD snooping の通信障害」を参照して，IGMP/MLD snooping の設定を確認してください。
9	各インタフェースで異常を検出していないか確認してください。 • show ip igmp interface • show ipv6 mld interface	Notice に警告情報が表示されていないことを確認してください。 警告情報が表示されている場合は，次の内容を確認してください。 L： 次のどれかの上限値に到達しているため，IGMP Report メッセージまたは MLD Report メッセージ（もしくはメッセージ内の Record 情報）を廃棄しています。受信者数を確認してください。 • マルチキャストグループ数（コンフィグレーションコマンド ip igmp group-limit または ipv6 mld group-limit の設定値） • ソース数（コンフィグレーションコマンド ip igmp source-limit または ipv6 mld source-limit の設定値）

項番	確認内容・コマンド	対応
		• マルチキャストチャネル数（コンフィグレーションコマンド ipv6 mld channel-limit の設定値） • ホストトラッキング機能で保持している受信者数（コンフィグレーションコマンド ipv6 mld explicit-tracking の設定値） Q： 隣接するルータと IGMP または MLD のバージョンが不一致です。IGMP または MLD のバージョンを一致させてください。 R： 現在の設定では受信できない IGMP Report メッセージまたは MLD Report メッセージを送信している受信者が存在します。本装置の IGMP または MLD のバージョンを変更するか，受信者の設定を確認してください。 S： IGMPv3 または MLDv2 で 1 メッセージ内に格納できるソース数が上限を超えたため，参加情報を一部廃棄しています。受信者の設定を確認してください。 F： マルチキャストチャネルフィルタ機能（コンフィグレーションコマンド ipv6 mld access-group）によって，MLD Report メッセージまたは MLD Report メッセージ内の Record 情報を廃棄しています。show ipv6 mld access-group コマンドを実行して，対象の参加要求が許可されているかどうかを確認してください。 B： MLD インタフェース単位の帯域管理機能（コンフィグレーションコマンド ipv6 mld bandwidth-limit）によって，MLD Report メッセージまたは MLD Report メッセージ内の Record 情報を廃棄しています。show ipv6 mld bandwidth コマンドを実行して，対象 MLD インタフェースの帯域使用状況を確認してください。

(3) ファーストホップルータ確認内容

PIM-SSM ネットワーク構成で，本装置がファーストホップルータの場合の確認内容を次の表に示します。

表 5‒19 ファーストホップルータ確認内容

項番	確認内容・コマンド	対応
1	本装置が送信者と直接接続していて，送信者からのマルチキャストパケットが本装置に届いていることを確認してください。 • show interface	マルチキャストパケットが届いていない場合は，ネットワーク構成および送信者の設定を確認してください。
2	送信者と接続しているインタフェースで，PIM-SM，IGMP または MLD が動作していることを確認してください。	PIM-SM，IGMP または MLD が動作していない場合は，PIM-SM，IGMP または MLD が動作するようにコンフィグレーションを修正してください。

項番	確認内容・コマンド	対応
	• show ip pim interface • show ip igmp interface • show ipv6 pim interface • show ipv6 mld interface	
3	マルチキャストパケットとマルチキャスト経路情報のグループアドレスと送信元アドレスが一致するか確認してください。 • show ip mroute • show ipv6 mroute	グループアドレスと送信元アドレスが一致しない場合は，送信者とラストホップルータの設定を確認してください。

5.6.4 PIM-SSM ネットワークでマルチキャストパケットが二重中継される

PIM-SSM ネットワーク構成でマルチキャストパケットが二重中継される場合は，各ルータの設定内容を確認して，同一ネットワークに複数のルータが存在するインタフェースでは PIM-SM が動作するように設定してください。

また，MLD の静的グループ参加機能（コンフィグレーションコマンド ipv6 mld static-group）で ignore-dr パラメータを設定している場合，本装置は DR でなくてもマルチキャストパケットを中継します。そのため，PIM-SM が動作している場合でも，一時的に二重中継が発生することがあります。なお，この二重中継は PIM Assert メッセージの送受信で停止します。

PIM-SM の設定をしても二重中継が継続する場合の確認内容を次の表に示します。

表 5-20　二重中継が継続する場合の確認内容

項番	確認内容・コマンド	対応
1	同一ネットワークに複数のルータが存在するインタフェースの PIM-SM の隣接情報を確認してください。 • show ip pim neighbor • show ipv6 pim neighbor	隣接ルータが表示されない場合は，次の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM-SM が動作していることを，show ip pim interface または show ipv6 pim interface コマンドで確認してください。 • フィルタまたは QoS によってプロトコルパケットが廃棄されていないか確認してください。確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。 • 隣接ルータの設定を確認してください。

5.6.5 VRF でマルチキャスト通信ができない

VRF でマルチキャスト通信ができない場合の確認内容を次の表に示します。

表 5-21　VRF での確認内容

項番	確認内容・コマンド	対応
1	本装置をランデブーポイントまたはブートストラップルータとして使用する場合は，該当 VRF のループバックインタフェースに IPv4 マルチキャスト使用時は IPv4 アドレスを，IPv6 マルチキャスト使用時は IPv6 アドレスを設定しているか，コンフィグレーションを確認してください。 • show running-config	該当 VRF のループバックインタフェースに IPv4 アドレスまたは IPv6 アドレスを設定している場合は，項番 2 へ。
		本装置をランデブーポイントまたはブートストラップルータとして使用しない場合は，項番 6 へ。
		該当 VRF のループバックインタフェースに IPv4 アドレスまたは IPv6 アドレスを設定していない場合は，コンフィグレーションを修正してください。
2	該当 VRF で本装置がランデブーポイント候補として動作していることを確認してください。 • show ip pim vrf all rp-mapping • show ipv6 pim vrf all rp-mapping	本装置がランデブーポイント候補として動作していない場合は，項番 3 へ。
		本装置がランデブーポイント候補として動作している場合は，項番 4 へ。
3	ランデブーポイント候補の設定で，IPv4 マルチキャスト使用時は該当 VRF のループバックインタフェース番号を，IPv6 マルチキャスト使用時は該当 VRF のループバックインタフェースの IPv6 アドレスを指定しているか，コンフィグレーションを確認してください。 • show running-config	ランデブーポイント候補の設定が正しい場合は，項番 4 へ。
		ランデブーポイント候補の設定が正しくない場合は，コンフィグレーションを修正してください。
4	該当 VRF で本装置がブートストラップルータ候補として動作していることを確認してください。 • show ip pim vrf all bsr • show ipv6 pim vrf all bsr	本装置がブートストラップルータ候補として動作していない場合は，項番 5 へ。
		本装置がブートストラップルータ候補として動作している場合は，項番 6 へ。
5	ブートストラップルータ候補の設定で，IPv4 マルチキャスト使用時は該当 VRF のループバックインタフェース番号を，IPv6 マルチキャスト使用時は該当 VRF のループバックインタフェースの IPv6 アドレスを指定しているか，コンフィグレーションを確認してください。 • show running-config	ブートストラップルータ候補の設定が正しい場合は，項番 6 へ。
		ブートストラップルータ候補の設定が正しくない場合は，コンフィグレーションを修正してください。
6	複数の VRF で運用している場合は，グローバルネットワークまたは特定の VRF がマルチキャスト中継エントリを想定以上に占有していないか確認してください。 • show ip mcache vrf all • show ipv6 mcache vrf all	ネットワーク設計の想定以上にマルチキャスト中継エントリを占有しているグローバルネットワークまたは VRF がない場合は，項番 7 へ。
		ネットワーク設計の想定以上にマルチキャスト中継エントリを占有しているグローバルネットワークまたは VRF がある場合は，想定していないマルチキャスト中継エントリが生成されていないか確認してください。ネガティブキャッシュエントリが多い場合は，不要なマルチキャストパケットを送信している端末が存在しないか確認してください。 なお，一つのグローバルネットワークまたは特定の VRF がマルチキャスト中継エントリを不正に占有することを防止する

項番	確認内容・コマンド	対応
		ために，次に示すコンフィグレーションで VRF ごとにマルチキャスト中継エントリの最大数を設定することを推奨します。 • ip pim vrf <vrf id> mcache-limit <number> • ipv6 pim vrf <vrf id> mcache-limit <number>
7	各 VRF に対して，「5.6.1　PIM-SM ネットワークでマルチキャスト通信ができない」～「5.6.4　PIM-SSM ネットワークでマルチキャストパケットが二重中継される」の確認をしてください。	情報確認のための各コマンドでは，VRF を指定する必要があります。VRF 指定の方法は，「運用コマンドレファレンス」を参照してください。

5.6.6　エクストラネットでマルチキャスト通信ができない

エクストラネットでマルチキャスト通信ができない場合は，まず，「5.6.5　VRF でマルチキャスト通信ができない」を確認して，各 VRF でマルチキャスト通信ができることを確認してください。そのあと，次の表に示す内容を確認してください。

表 5-22　エクストラネットでの確認内容

項番	確認内容・コマンド	対応
1	中継先 VRF から送信元アドレスへのユニキャスト経路が，期待する VRF またはグローバルネットワークであることを確認してください。 • show ip rpf vrf <vrf id> • show ipv6 rpf vrf <vrf id>	ユニキャスト経路が正しくない場合は，ユニキャストエクストラネットの設定を修正してください。
2	上流側 VRF で，送信元アドレスへのユニキャスト経路が，さらに別の VRF になっていないか確認してください。 • show ip rpf vrf <vrf id> • show ipv6 rpf vrf <vrf id>	送信元アドレスへのユニキャスト経路が別の VRF になっている場合は，装置内での二段以上の VRF 中継となります。二段以上の VRF 中継は未サポートのため，ネットワーク構成を見直してください。
3	(S,G)マルチキャスト経路情報の incoming に(denied)が表示されていないか確認してください。 • show ip mroute vrf all • show ipv6 mroute vrf all	(S,G)マルチキャスト経路情報の incoming に(denied)が表示されている場合は，上流側 VRF のマルチキャスト経路フィルタリングにエクストラネット通信で使用するグループアドレスと中継先 VRF を設定してください。 なお，マルチキャスト経路フィルタリングにグループアドレスおよび中継先 VRF を設定していない場合は，すべてのグループアドレスおよび VRF が中継先として許可されています。
4	該当する VRF の extranet filter に，想定しているフィルタ数が表示されることを確認してください。 • show ip multicast resources • show ipv6 multicast resources	想定しているフィルタ数と異なる場合は，マルチキャスト経路フィルタリングの設定が不正です。マルチキャスト経路フィルタリングの設定を修正してください。

5.6.7　系切替後にマルチキャスト通信が停止する

二重化装置で，系切替後の再学習時間中または再学習時間終了時に，マルチキャスト通信が停止した場合の確認内容を次の表に示します。

系切替時の無停止マルチキャスト中継機能は，IPv4 マルチキャストの PIM-SM/PIM-SSM，および IPv6 マルチキャストの PIM-SSM をサポートしています。

表 5-23　系切替後にマルチキャスト通信が停止する場合の確認内容

項番	確認内容・コマンド	対応
1	本装置に無停止マルチキャスト中継機能の設定（コンフィグレーションコマンド ip pim nonstop-forwarding または ipv6 pim nonstop-forwarding）があることを，コンフィグレーションで確認してください。 • show running-config	無停止マルチキャスト中継機能の設定がある場合は，項番 2 以降を確認してください。
		無停止マルチキャスト中継機能の設定がない場合は，コンフィグレーションを修正してください。
2	本装置で，ユニキャストルーティング高可用機能が有効であることを確認してください。 • show running-config	無停止マルチキャスト中継機能を使用するためには，本装置でユニキャストルーティング高可用機能を有効にしてください。 ユニキャストルーティング高可用機能を有効にしない場合は，送信元への経路をスタティックで設定してください。 ユニキャストルーティング高可用機能については,「コンフィグレーションガイド」を参照してください。
3	系切替する装置の隣接装置が，Generation ID オプションをサポートしているか確認してください。 • show ip pim neighbor detail • show ipv6 pim neighbor detail	GenID に"-"が表示される隣接装置は，Generation ID オプションをサポートしていません。無停止マルチキャスト中継機能を使用するためには，隣接装置に Generation ID オプションをサポートしている装置を設置してください。
4	再学習時間の設定（コンフィグレーションコマンド ip pim nonstop-forwarding または ipv6 pim nonstop-forwarding の aging-time パラメータ）が適切か，コンフィグレーションを確認してください。 • show running-config	再学習時間が短いと，再学習時間終了後にマルチキャスト通信が停止することがあります。 運用しているネットワーク構成に適した再学習時間を算出して，コンフィグレーションを修正してください。算出方法については,「コンフィグレーションガイド」を参照してください。
5	本装置がランデブーポイントの場合，RP-Holdtime の設定(コンフィグレーションコマンド ip pim rp-candidate の holdtime パラメータ）が適切か，コンフィグレーションを確認してください。 • show running-config	系切替後に，他装置で本装置のランデブーポイント情報がタイムアウトしたために通信が停止した場合は，RP-Holdtime が短い可能性があります。 運用しているネットワーク構成に適した RP-Holdtime を算出して，コンフィグレーションを修正してください。算出方法については,「コンフィグレーションガイド」を参照してください。

6 機能ごとのトラブルシュート

この章では，機能ごとにトラブルが発生した場合の対処方法を説明します。

6.1 フィルタのトラブル

6.1.1 フィルタのトラブル

フィルタで指定したフレームが通過または廃棄されない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 6-1 フィルタでフレームが通過または廃棄されない場合の障害解析方法

項番	確認内容・コマンド	対応
1	通過または廃棄するフレームを指定したフィルタが設定されていることを，コンフィグレーションで確認してください。 • show running-config	通過または廃棄するフレームを指定したフィルタが設定されていない場合は，コンフィグレーションを修正してください。
		通過または廃棄するフレームを指定したフィルタが設定されている場合は，項番 2 へ。
2	PSU の更新状態に(restart required)が表示されているか確認してください。 • show system • show psu resources	PSU の更新状態に(restart required)が表示されている場合は，PSU を再起動してください。
		PSU の更新状態に(restart required)が表示されていない場合は，項番 3 へ。
3	通過または廃棄するフレームを指定したフィルタエントリについて，PSU ごとの Matched packets に Unset が表示されているか確認してください。 • show access-filter	該当するフィルタエントリについて，PSU ごとの Matched packets に Unset が表示されている場合は，フィルタエントリを装置へ反映中です。Unset が消えるまで，しばらく待ってください。
		該当するフィルタエントリについて，PSU ごとの Matched packets に Unset が表示されていない場合は，項番 4 へ。
4	フィルタ条件に一致したパケット数を Matched packets で確認してください。 • show access-filter	通過または廃棄したいフレーム数と Matched packets の値が異なる場合は，フィルタの検出条件が誤っていて，暗黙の廃棄をしている可能性があります。フィルタエントリの設定を見直してください。
		通過または廃棄したいフレーム数より Matched packets の値が小さい場合は，項番 5 へ。
5	uRPF によってパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1.3 uRPF による廃棄を確認する」を参照してください。

6.1.2 アクセスリストログのトラブル

アクセスリストロギングを使用中に対象のアクセスリストログが出力されない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

また，アクセスリストロギングを動作に指定しているフィルタによるトラブルの可能性もあるため，次の手順に加えて，「6.1.1 フィルタのトラブル」を参照してください。

表 6-2　アクセスリストログが出力されない場合の障害解析方法

項番	確認内容・コマンド	対応
1	アクセスリストロギングを動作に指定しているフィルタに一致したパケット数を，Matched packets で確認してください。 • show access-filter	アクセスリストログが出力されないパケット数と Matched packets の値が異なる場合は，フィルタの設定が誤っている可能性があります。コンフィグレーションを見直してください。
		アクセスリストログが出力されないパケット数より Matched packets の値が小さい場合は，項番 2 へ。
2	アクセスリストロギングの動作状況を確認してください。 • show access-log	応答メッセージ"Access-list logging is not enabled."が出力された場合は，コンフィグレーションコマンドでアクセスリストロギングの設定が有効となっているか確認してください。
		コマンドの実行結果が表示された場合は，項番 3 へ。
3	アクセスリストログ統計情報が最大数を超えていないか確認してください。 • show access-log	flow table full の値が 0 でない場合は，管理できるアクセスリストログ統計情報数を超えるパケットをフィルタで検出した可能性があります。
		flow table full の値が 0 の場合は，項番 4 へ。
4	アクセスリストログ（メッセージ種別 ACLLOG のシステムメッセージ）の出力が抑止されていないことを，コンフィグレーションで確認してください。 • show running-config	出力が抑止されている場合は，コンフィグレーションコマンド message-type で該当するメッセージ種別を出力するように設定してください。
		出力対象となっている場合は，項番 5 または項番 6 へ。
5	アクセスリストログを出力する時間間隔を，interval(minutes)で確認してください。 • show access-log	unlimit の場合は，時間間隔を契機としてアクセスリストログを出力しません。
		5～1440 の場合は，該当する時間間隔でアクセスリストログを出力します。出力するまで待ってください。
6	アクセスリストログを出力するスレッシュホールドを，threshold(packets)で確認してください。 • show access-log	"-"の場合は，スレッシュホールドを契機としてアクセスリストログを出力しません。
		1～4294967295 の場合は，パケットの検出数が該当するスレッシュホールドの N 倍に一致したとき，アクセスリストログを出力します。出力するまで待ってください。

6.2　QoS のトラブル

6.2.1　ポリサーのトラブル

ポリサーが動作しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 6–3　ポリサーが動作しない場合の障害解析方法

項番	確認内容・コマンド	対応
1	監視するフレームを指定した QoS フローおよびポリサーが設定されていることを，コンフィグレーションで確認してください。 • show running-config	監視するフレームを指定した QoS フローおよびポリサーが設定されていない場合は，コンフィグレーションを修正してください。
		監視するフレームを指定した QoS フローおよびポリサーが設定されている場合は，項番 2 へ。
2	PSU の更新状態に(restart required)が表示されているか確認してください。 • show system • show psu resources	PSU の更新状態に(restart required)が表示されている場合は，PSU を再起動してください。
		PSU の更新状態に(restart required)が表示されていない場合は，項番 3 へ。
3	監視するフレームを指定した QoS フローエントリについて，PSU ごとの Matched packets に Unset が表示されているか確認してください。 • show qos-flow	該当する QoS フローエントリについて，PSU ごとの Matched packets に Unset が表示されている場合は，QoS フローエントリを装置へ反映中です。Unset が消えるまで，しばらく待ってください。
		該当する QoS フローエントリについて，PSU ごとの Matched packets に Unset が表示されていない場合は，項番 4 へ。
4	監視するフレームを指定した QoS フローエントリで指定したポリサーエントリについて，PSU ごとのパケット数に Unset が表示されているか確認してください。 • show policer	該当するポリサーエントリについて，PSU ごとのパケット数に Unset が表示されている場合は，ポリサーエントリを装置へ反映中です。Unset が消えるまで，しばらく待ってください。
		該当するポリサーエントリについて，PSU ごとのパケット数に Unset が表示されていない場合は，項番 5 へ。
5	Max-rate over，Max-rate under，Min-rate over，および Min-rate under で，ポリサーの遵守フレーム数および違反フレーム数を確認してください。 • show policer	監視したいフレーム数と show policer コマンドで表示した値が異なる場合は，QoS フローの検出対象外である可能性があります。詳細は，「コンフィグレーションガイド」を参照してください。
		監視したいフレーム数と show policer コマンドで表示した値が異なる場合は，QoS フローの検出条件が誤っている可能性があります。QoS フローエントリの設定を見直してください。
		監視したいフレーム数に対して show policer コマンドで表示した遵守フレーム数および違反フレーム数が適正でない場合は，ポリサーの監視帯域値やバーストサイズが誤っている可能性があります。ポリサーの設定を見直してください。
		監視したいフレーム数より show policer コマンドで表示した値が小さい場合は，項番 6 へ。

項番	確認内容・コマンド	対応
6	uRPF によってパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1.3　uRPF による廃棄を確認する」を参照してください。
		uRPF によってパケットが廃棄されていない場合は，項番 7 へ。
7	フィルタによってフレームが廃棄されていないか確認してください。	確認方法と対応については，「8.1.1　フィルタによる廃棄を確認する」を参照してください。

6.2.2　マーカー，優先度変更，および QoS フロー廃棄のトラブル

マーカー，優先度変更，および QoS フロー廃棄が動作しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 6-4　マーカー，優先度変更，および QoS フロー廃棄が動作しない場合の障害解析方法

項番	確認内容・コマンド	対応
1	マーカー，優先度変更，および QoS フロー廃棄するフレームを指定した QoS フローが設定されていることを，コンフィグレーションで確認してください。 • show running-config	マーカー，優先度変更，および QoS フロー廃棄するフレームを指定した QoS フローが設定されていない場合は，コンフィグレーションを修正してください。
		マーカー，優先度変更，および QoS フロー廃棄するフレームを指定した QoS フローが設定されている場合は，項番 2 へ。
2	PSU の更新状態に(restart required)が表示されているか確認してください。 • show system • show psu resources	PSU の更新状態に(restart required)が表示されている場合は，PSU を再起動してください。
		PSU の更新状態に(restart required)が表示されていない場合は，項番 3 へ。
3	マーカー，優先度変更，および QoS フロー廃棄するフレームを指定した QoS フローエントリについて，PSU ごとの Matched packets に Unset が表示されているか確認してください。 • show qos-flow	該当する QoS フローエントリについて，PSU ごとの Matched packets に Unset が表示されている場合は，QoS フローエントリを装置へ反映中です。Unset が消えるまで，しばらく待ってください。
		該当する QoS フローエントリについて，PSU ごとの Matched packets に Unset が表示されていない場合は，項番 4 へ。
4	QoS フロー条件に一致したパケット数を Matched packets で確認してください。 • show qos-flow	マーカー，優先度変更，および QoS フロー廃棄したいフレーム数と Matched packets の値が異なる場合は，QoS フローの検出対象外である可能性があります。詳細は，「コンフィグレーションガイド」を参照してください。
		マーカー，優先度変更，および QoS フロー廃棄したいフレーム数と Matched packets の値が異なる場合は，QoS フローの検出条件が誤っている可能性があります。QoS フローエントリの設定を見直してください。
		マーカー，優先度変更，および QoS フロー廃棄したいフレーム数より Matched packets の値が小さい場合は，項番 5 へ。

項番	確認内容・コマンド	対応
5	階層化シェーパのポートで優先度変更が動作しない場合は，ユーザ優先度マッピングを設定していないか確認してください。 • show shaper	User-priority-map の Current が Enable の場合は，ユーザ優先度マッピングが動作しています。 ユーザ優先度マッピングを使用している場合は VLAN Tag の付いたフレームのキュー番号をユーザ優先度マッピングによって決定するため，コンフィグレーションを見直してください。
		階層化シェーパを使用していない場合，またはユーザ優先度マッピングを使用していない場合は，項番 6 へ。
6	uRPF によってパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1.3　uRPF による廃棄を確認する」を参照してください。
		uRPF によってパケットが廃棄されていない場合は，項番 7 へ。
7	フィルタによってフレームが廃棄されていないか確認してください。	確認方法と対応については，「8.1.1　フィルタによる廃棄を確認する」を参照してください。

6.2.3　ポートシェーパのトラブル

ポートシェーパが動作しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 6-5　ポートシェーパが動作しない場合の障害解析方法

項番	確認内容・コマンド	対応
1	対象のイーサネットインタフェースの動作状況を Schedule-mode，Port-rate-limit，Active-rate，Qlen，Peak-Qlen，Limit-Qlen，および Drop-mode で確認してください。 • show qos queueing port	"-"の場合は，ポートシェーパの設定が反映されていない可能性があります。対象のイーサネットインタフェースを正常運用中にしてください。
		"-"でない場合は，項番 2 へ。
2	フレームが廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。

6.2.4　階層化シェーパのトラブル

階層化シェーパで，次に示すトラブルが発生した場合の対処方法を説明します。

- シェーパユーザ決定が動作しない
- 優先度決定が動作しない
- シェーパモード，スケジューリング，キュー数，またはキュー長が設定されない
- 帯域制御が動作しない

(1)　シェーパユーザ決定が動作しない場合

シェーパユーザ決定が動作しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 6-6 シェーパユーザ決定が動作しない場合の障害解析方法

項番	確認内容・コマンド	対応
1	対象 NIF にシェーパユーザ決定のコンフィグレーションが設定されているか確認してください。 • show running-config	該当するシェーパユーザ決定のコンフィグレーションに対象 NIF が指定されていない場合は，動作しません。コンフィグレーションコマンド shaper flow-distribution で対象 NIF を追加してください。
		コンフィグレーションが設定されている場合は，項番 2 へ。
2	対象ポートでシェーパユーザ決定のコンフィグレーションと動作内容が一致しているか確認してください。 • show shaper	コンフィグレーションで，ランダム振り分けまたは VLAN ID マッピングを設定していて，Flow-distribution に"-"が表示されている場合，またはコンフィグレーションと異なる場合は，動作に反映されていません。NIF を再起動して運用に反映させてください。
		コンフィグレーションと動作内容が一致している場合は，項番 3 へ。
3	対象 NIF の更新状態を確認してください。 • show nif	NIF の更新状態に restart required が表示されている場合は，NIF の再起動が必要です。NIF を再起動して運用に反映させてください。
		NIF の更新状態に restart required が表示されていない場合は，項番 4 へ。
4	振り分け先のシェーパユーザの設定について，次のどちらかで確認してください。 • show shaper <port list> llrlq • show shaper <port list> user <user id list>	応答メッセージ"There is no operational user."が表示される場合は，シェーパユーザが設定されていません。シェーパユーザのコンフィグレーションが設定されているか確認してください。
		シェーパユーザが表示される場合は，項番 5 へ。
5	ランダム振り分けを使用している場合，デフォルトユーザからフレームが送信されていないか確認してください。 • show shaper <port list> default	ランダム振り分けのキー情報となるフレーム情報を持たないフレームは，デフォルトユーザにキューイングされます。 キー情報として使用できるフレーム情報については，「コンフィグレーションガイド」のシェーパユーザ決定を参照してください。
		ランダム振り分けを使用していない場合，および対象パケットの場合は，項番 6 へ。
6	VLAN ID マッピングを使用している場合，デフォルトユーザからパケットが送信されていないか確認してください。 • show shaper <port list> default	振り分け範囲外の VLAN ID を持つフレームは，デフォルトユーザにキューイングされます。 使用できる VLAN ID については,「コンフィグレーションガイド」のシェーパユーザ決定を参照してください。
		VLAN ID マッピングを使用していない場合，および対象 VLAN ID の場合は，項番 7 へ。
7	フロー検出によるシェーパユーザ決定を使用している場合，デフォルトユーザからパケットが送信されていないか確認してください。 • show shaper <port list> default	設定されていないシェーパユーザを指定している場合，デフォルトユーザにキューイングされます。 使用できるシェーパユーザ番号については,「コンフィグレーションガイド」のシェーパユーザ決定を参照してください。
		フロー検出によるシェーパユーザ決定を使用していない場合，および対象シェーパユーザ番号の場合は，項番 8 へ。

項番	確認内容・コマンド	対応
8	フレームが廃棄されていないか確認してください。	確認方法と対応については,「8.1　パケット廃棄の確認」を参照してください。

(2)　優先度決定が動作しない場合

優先度決定が動作しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。なお，優先度決定を QoS フローの優先度変更で決定している場合は,「6.2.2　マーカー，優先度変更，および QoS フロー廃棄のトラブル」を参照してください。

表 6-7　優先度決定が動作しない場合の障害解析方法

項番	確認内容・コマンド	対応
1	ユーザ優先度マッピングがコンフィグレーションに設定されているか確認してください。 • show running-config	ユーザ優先度マッピングが設定されていない場合は，動作しません。コンフィグレーションコマンド shaper user-priority-map を設定してください。
		コンフィグレーションが設定されている場合は，項番 2 へ。
2	対象 NIF でユーザ優先度マッピングのコンフィグレーションと動作内容が一致しているか確認してください。 • show shaper	User-priority-map の Current に"-"が表示されている場合，または Configuration と異なる場合は，動作に反映されていません。NIF を再起動して運用に反映させてください。
		コンフィグレーションと動作内容が一致している場合は，項番 3 へ。
3	対象 NIF の更新状態を確認してください。 • show nif	NIF の更新状態に restart required が表示されている場合は，NIF の再起動が必要です。NIF を再起動して運用に反映させてください。
		NIF の更新状態に restart required が表示されていない場合は，項番 4 へ。
4	フレームが廃棄されていないか確認してください。	確認方法と対応については,「8.1　パケット廃棄の確認」を参照してください。

(3)　シェーパモード，スケジューリング，キュー数，またはキュー長が設定されない場合

シェーパモード，スケジューリング，キュー数，またはキュー長が設定されない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 6-8　シェーパモード，スケジューリング，キュー数，またはキュー長が設定されない場合の障害解析方法

項番	確認内容・コマンド	対応
1	対象 NIF にシェーパモードのコンフィグレーションが設定されているか確認してください。 • show running-config	該当するシェーパモードのコンフィグレーションに対象 NIF が指定されていない場合は，動作しません。シェーパモードのコンフィグレーションに対象 NIF を追加してください。
		コンフィグレーションが設定されている場合は，項番 2 へ。

項番	確認内容・コマンド	対応
2	対象 NIF でシェーパモードのコンフィグレーションと動作内容が一致しているか確認してください。 • show shaper	Shaper-mode，Scheduling-mode，Max-queue，および Queue-length の Current に"-"が表示されている場合，または Configuration と異なる場合は，動作に反映されていません。NIF を再起動して運用に反映させてください。
		コンフィグレーションと動作内容が一致している場合は，項番 3 へ。
3	対象 NIF の更新状態を確認してください。 • show nif	NIF の更新状態に restart required が表示されている場合は，NIF の再起動が必要です。NIF を再起動して運用に反映させてください。
		NIF の更新状態に restart required が表示されていない場合は，項番 4 へ。
4	振り分け先のシェーパユーザの設定について，次のどれかで確認してください。 • show shaper <port list> llrlq • show shaper <port list> default • show shaper <port list> user <user id list>	応答メッセージ"There is no operational user."が表示される場合は，シェーパユーザが設定されていません。シェーパユーザのコンフィグレーションが設定されているか確認してください。
		シェーパユーザが表示される場合は，項番 5 へ。
5	フレームが廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。

(4)　帯域制御が動作しない場合

帯域制御が動作しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 6-9　帯域制御が動作しない場合の障害解析方法

項番	確認内容・コマンド	対応
1	対象 NIF のシェーパモードのコンフィグレーションに各帯域が設定されているか確認してください。 • show running-config	シェーパユーザワンタッチ設定機能を使用していて，該当するシェーパモードのコンフィグレーションで帯域が指定されていない場合は，LLRLQ ユーザ最大帯域およびデフォルトユーザ最大帯域を制限しません。コンフィグレーションコマンド shaper mode で各帯域を追加してください。
		コンフィグレーションに帯域が設定されている場合は，項番 2 へ。
2	対象 NIF で各帯域のコンフィグレーションと動作内容が一致しているか確認してください。 • show shaper	各帯域の Current に"-"が表示されている場合，または Configuration と異なる場合は，対象の帯域が動作に反映されていません。NIF を再起動して運用に反映させてください。
		コンフィグレーションと動作内容が一致している場合は，項番 3 へ。
3	対象 NIF の更新状態を確認してください。 • show nif	NIF の更新状態に restart required が表示されている場合は，NIF の再起動が必要です。NIF を再起動して運用に反映させてください。

項番	確認内容・コマンド	対応
		NIF の更新状態に restart required が表示されていない場合は，項番 4 へ。
4	対象 NIF でポート帯域制御が設定されているか確認してください。 • show shaper	対象ポートにポート帯域制御が設定されていない場合は，ポート帯域を制限しません。コンフィグレーションを見直してください。
		ポート帯域制御が設定されている場合は，項番 5 へ。
5	振り分け先のシェーパユーザの設定について，次のどれかで確認してください。 • show shaper <port list> llrlq • show shaper <port list> default • show shaper <port list> user <user id list>	応答メッセージ"There is no operational user."が表示される場合は，シェーパユーザが設定されていません。シェーパユーザのコンフィグレーションが設定されているか確認してください。
		シェーパユーザが表示される場合は，項番 6 へ。
6	シェーパユーザ決定を確認してください。 • show shaper	シェーパユーザ決定でランダム振り分けを使用している場合は，複数のフローが同一シェーパユーザに割り当てられることがあります。ランダム振り分けのキー情報を見直すか，シェーパユーザ数を標準モードで使用している場合は拡張モードに変更すると，複数のフローによる競合が発生しにくくなります。
		適切に設定されている場合は，項番 7 へ。
7	フレームが廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。

6.3　トラッキング機能のトラブル

本節では，トラッキング機能と静的監視トラックについての解析方法を説明します。BFD と動的監視トラックについては，「6.8　BFD のトラブル」を参照してください。

6.3.1　トラック状態が予想される状態と異なる

本装置のトラック状態が予想される状態と異なる場合は, 次の表に示す解析方法に従って原因を切り分けてください。

表 6-10　トラック状態が予想される状態と異なる場合の障害解析方法

項番	確認内容・コマンド	対応
1	トラック情報を確認してください。 • show track name <track name> detail	表示されない場合や，トラック種別が UNSPECIFIED の場合は，トラックが設定されていません。 トラックの動作状態に(Disable)が表示されている場合は，コンフィグレーションコマンド shutdown によってトラックが停止しています。 コンフィグレーションを確認してください。
		トラックが動作していて，かつトラック種別が LIST（リスト監視）の場合は，表示されているリスト監視のトラック対象とそのトラック状態を確認してください。
		トラックが動作していて，かつトラック種別が ICMP（ICMP 監視）の場合は，項番 2 へ。
		トラックが動作していて，かつトラック種別が INTERFACE（インタフェース監視）の場合は，項番 6 へ。
2	ICMP 監視状態を確認してください。 • show track-icmp name <track name> detail	動作状態が Init の場合は，BCU が起動直後のため，監視を開始していません。起動待ち時間が経過するまで待ってください。 なお, 起動待ち時間や監視開始前のトラック状態は, コンフィグレーションコマンドで変更できます。
		動作状態が Aging の場合は，系切替中です。系切替直前のトラック状態を維持しています。系切替待ち時間が経過するまで待ってください。 なお，系切替待ち時間は，コンフィグレーションコマンドで変更できます。
		動作状態が Active または Transit の場合は，項番 3 へ。
3	トラック対象と通信できるかどうかを確認してください。 宛先アドレス, 送信元アドレス, ネクストホップ，送信インタフェース（IPv6），DSCP，TTL（IPv4），HopLimit（IPv6）について，トラックの設定と同じ値を指定してください。 • ping • ping ipv6	ping の宛先 IPv4 アドレスと応答 IPv4 アドレスが異なる場合は，宛先 IPv4 アドレスにブロードキャストアドレスを指定しています。 ICMPv4 監視は，ブロードキャストアドレス宛てでは動作しません。コンフィグレーションを確認してください。
		応答がある場合は，コンフィグレーションコマンド icmp check-reply-interface を設定しているか確認してください。設定している場合，指定したインタフェース以外から ICMP Echo Reply を受信しても応答なしと判断します。

<table>
<tr><th>項番</th><th>確認内容・コマンド</th><th>対応</th></tr>
<tr><td></td><td></td><td>応答がない場合は，項番 4 へ。</td></tr>
<tr><td rowspan="3">4</td><td rowspan="3">トラック対象と通信できるかどうかを確認してください。
宛先アドレス, 送信元アドレス, ネクストホップ，送信インタフェース（IPv6）について，トラックの設定と同じ値を指定してください。
• ping
• ping ipv6</td><td>応答がある場合は，コンフィグレーショコマンド icmp の設定を見直してください。</td></tr>
<tr><td>応答がなく，送信元アドレス，ネクストホップ，または送信インタフェース（IPv6）のどれかを設定している場合は，項番 5 へ。</td></tr>
<tr><td>応答がなく，送信元アドレス，ネクストホップ，および送信インタフェース（IPv6）のどれも設定していない場合は,「5　IP およびルーティングのトラブルシュート」を参照してください。</td></tr>
<tr><td rowspan="2">5</td><td rowspan="2">トラック対象と通信できるかどうかを確認してください。
宛先アドレスは，トラックの設定と同じ値を指定してください。宛先アドレスが IPv6 リンクローカルアドレスの場合は，送信インタフェースもトラックの設定と同じ値を指定してください。
• ping
• ping ipv6</td><td>応答がある場合は，送信元アドレス，ネクストホップ，および送信インタフェース（IPv6）について，次の点を確認してください。
• 送信元アドレスは，本装置に設定されている受信できる IP アドレスである必要があります。IP アドレスを設定しているインタフェースが up していない場合は,「3　ネットワークインタフェースのトラブルシュート」を参照してください。
• ネクストホップは，ARP／NDP 解決されている必要があります。未解決の場合は，隣接装置の IP ネットワーク設定，および「3　ネットワークインタフェースのトラブルシュート」を確認してください。
• 送信インタフェースは，該当するインタフェースが up している必要があります。up していない場合は，「3　ネットワークインタフェースのトラブルシュート」を参照してください。
これらの内容について問題がない場合は,「5　IP およびルーティングのトラブルシュート」を参照してください。</td></tr>
<tr><td>応答がない場合は，「5　IP およびルーティングのトラブルシュート」を参照してください。</td></tr>
<tr><td rowspan="3">6</td><td rowspan="3">インタフェース監視が開始されているかどうかを確認するため, BCU 起動および系切替をしてからの経過時間を確認してください。
• show logging</td><td>BCU が起動してからコンフィグレーションコマンド track-target init-interval で指定した時間が経過していない場合は，起動直後のため監視を開始していません。起動待ち時間が経過するまで待ってください。
なお, 起動待ち時間や監視開始前のトラック状態は, コンフィグレーションコマンドで変更できます。</td></tr>
<tr><td>系切替が発生してからコンフィグレーションコマンド track-target aging-interval で指定した時間が経過していない場合は，系切替中です。系切替直前のトラック状態を維持しています。系切替待ち時間が経過するまで待ってください。
なお，系切替待ち時間は，コンフィグレーションコマンドで変更できます。</td></tr>
<tr><td>BCU 起動または系切替が発生してから十分な時間が経過している場合は，項番 7 へ。</td></tr>
</table>

項番	確認内容・コマンド	対応
7	インタフェースの状態を確認してください。	確認方法と対応については，次を参照してください。 • イーサネットインタフェース監視の場合は「3.1　イーサネットの通信障害」 • ポートチャネルインタフェース監視の場合は「3.2　リンクアグリゲーション使用時の通信障害」

6.4　ポリシーベースミラーリングのトラブル

6.4.1　ミラーリングされない

ポリシーベースミラーリングを使用中に対象フローがミラーリングされない場合は, 次の表に示す障害解析方法に従って原因を切り分けてください。

表 6-11　対象フローがミラーリングされない場合の障害解析方法

項番	確認内容・コマンド	対応
1	ポリシーベースミラーリングの送信先インタフェースリストを動作に指定しているアクセスリストが設定されていることを，コンフィグレーションで確認してください。 • show running-config	ポリシーベースミラーリングの送信先インタフェースリストを動作に指定しているアクセスリストが設定されていない場合は，コンフィグレーションを修正してください。
		ポリシーベースミラーリングの送信先インタフェースリストを動作に指定しているアクセスリストが設定されている場合は，項番 2 へ。
2	PSU の更新状態に(restart required)が表示されているか確認してください。 • show system • show psu resources	PSU の更新状態に(restart required)が表示されている場合は，PSU を再起動してください。
		PSU の更新状態に(restart required)が表示されていない場合は，項番 3 へ。
3	ポリシーベースミラーリングの送信先インタフェースリストを動作に指定しているアクセスリストのエントリについて，PSU ごとの Matched packets に Unset が表示されているか確認してください。 • show access-filter	該当するエントリについて，PSU ごとの Matched packets に Unset が表示されている場合は，エントリを装置へ反映中です。Unset が消えるまで，しばらく待ってください。
		該当するエントリについて，PSU ごとの Matched packets に Unset が表示されていない場合は，項番 4 へ。
4	ポリシーベースミラーリングの送信先インタフェースリストを動作に指定しているアクセスリストに一致したフレーム数を，Matched packets で確認してください。 • show access-filter	ポリシーベースミラーリングの対象フレーム数と Matched packets の値が異なる場合は，アクセスリストの設定が誤っている可能性があります。コンフィグレーションを見直してください。
		ポリシーベースミラーリングの対象フレーム数より Matched packets の値が小さい場合は，項番 5 へ。
5	送信先インタフェースリストに設定しているミラーポートの設定を，コンフィグレーションで確認してください。 • show running-config	ミラーポートが期待したインタフェースとなっていない場合は，コンフィグレーションを見直してください。
		ミラーポートが期待したインタフェースとなっている場合は，項番 6 へ。
6	ミラーポートの状態を確認してください。 • show interfaces • show channel-group	ミラーポートがイーサネットインタフェースの場合，かつポート状態が active up 以外の場合は，ポート状態を active up にしてください。
		ミラーポートがポートチャネルインタフェースの場合，かつチャネルグループ状態が Up 以外の場合は，チャネルグループ状態を Up にしてください。
		上記に該当しない場合は，項番 7 へ。

項番	確認内容・コマンド	対応
7	受信側でのポリシーベースミラーリングの場合，uRPF によってフレームが廃棄されていないか確認してください。	確認方法と対応については，「8.1.3　uRPF による廃棄を確認する」を参照してください。
		uRPF によってフレームが廃棄されていない場合は，項番 8 へ。
8	送信側でのポリシーベースミラーリングの場合，フィルタによってフレームが廃棄されていないか確認してください。	確認方法と対応については，「8.1.1　フィルタによる廃棄を確認する」を参照してください。
		フィルタによってフレームが廃棄されていない場合は，項番 9 へ。
9	送信側でのポリシーベースミラーリングの場合，QoS によってフレームが廃棄されていないか確認してください。	確認方法と対応については，「8.1.2　QoS による廃棄を確認する」を参照してください。

6.5 sFlow 統計（フロー統計）機能のトラブル

本装置の sFlow 統計機能で，次に示すトラブルが発生した場合の対処方法を説明します。

- sFlow パケットがコレクタに届かない
- フローサンプルがコレクタに届かない
- カウンタサンプルがコレクタに届かない

6.5.1 sFlow パケットがコレクタに届かない

本装置で sFlow パケットがコレクタに届かない場合のトラブルシューティングの流れは次のとおりです。

1. 運用コマンドで動作状況を確認する
2. コンフィグレーションの内容を確認する
3. コレクタまでの経路を確認する
4. その他，故障などを確認する

(1) 運用コマンドでの動作確認

show sflow コマンドを数回実行して sFlow 統計情報を表示して，sFlow 統計機能が動作しているか確認してください。下線部の値が増加していない場合は，「(2)　コンフィグレーションの確認」および「(3)　コレクタまでの経路確認」を参照してください。増加している場合は，「(3)　コレクタまでの経路確認」および「(4)　コレクタ側の設定確認」を参照して，コレクタに対してネットワークが正しく接続されているか確認してください。

図 6-1　show sflow コマンドの表示例

```
> show sflow
Date 20XX/07/19 12:00:00 UTC
sFlow service status : enable
Elapsed time from the last statistics clearance : 12:00:05
sFlow agent data :
 sFlow service version  : 4
 CounterSample interval rate : 60 seconds
 Received sFlow samples :      37269  Dropped sFlow samples      :       2093
 Exported sFlow samples :      37269  Non-exported sFlow Samples :          0
sFlow collector data :
 Collector IP address : 192.168.1.20  UDP :  6343  Source IP address : 192.168.1.1
  Send FlowSample UDP packets    :      12077  Send failed packets :          0
  Send CounterSample UDP packets :        621  Send failed packets :          0
sFlow sampling data :
 Configured rate(actual rate) : 1 per 2048 packets(1 per 2048 packets)
  Configured sFlow ingress ports : 1/2-4
>
```

注　下線部の値が，増加していることを確認してください。

(2) コンフィグレーションの確認

次の内容について，運用中のコンフィグレーションを確認してください。

- コンフィグレーションに，sFlow パケットの送信先であるコレクタの IP アドレスと UDP ポート番号が正しく設定されていることを確認してください。

```
(config)# show sflow
sflow destination 192.168.1.20 6343   <-1
sflow sample 2048
!
(config)#
```

1. コレクタの情報が正しく設定されていることを確認してください。

- サンプリング間隔が設定されていることを確認してください。

  サンプリング間隔が設定されていないと，デフォルト値（＝大きな値）で動作するため値が大き過ぎ，フローサンプルがコレクタにほとんど送信されません。そのため，適切なサンプリング間隔を設定してください。

  コンフィグレーションの表示例を次に示します。

```
(config)# show sflow
sflow destination 192.168.1.20 6343
sflow sample 2048      <-1
!
(config)#
```

  1. 適切なサンプリング間隔が設定されていることを確認してください。

  運用コマンドの実行例を次に示します。

```
> show sflow
Date 20XX/07/19 12:00:00 UTC
sFlow service status : enable
Elapsed time from the last statistics clearance : 12:00:05
sFlow agent data :
 sFlow service version  : 4
 CounterSample interval rate : 60 seconds
 Received sFlow samples :      37269  Dropped sFlow samples      :       2093
 Exported sFlow samples :      37269  Non-exported sFlow Samples :          0
sFlow collector data :
 Collector IP address : 192.168.1.20  UDP :  6343  Source IP address : 192.168.1.1
  Send FlowSample UDP packets    :      12077  Send failed packets :          0
  Send CounterSample UDP packets :        621  Send failed packets :          0
sFlow sampling data :
 Configured rate(actual rate) : 1 per 2048 packets(1 per 2048 packets)
  Configured sFlow ingress ports : 1/2-4
>
```

  注　下線部に，適切なサンプリング間隔が表示されていることを確認してください。

- sFlow 統計を実施する物理ポートに対して，sflow forward ingress が設定されていることを確認してください。

```
(config)# show interfaces tengigabitethernet 1/2
interface tengigabitethernet 1/2
  sflow forward ingress           <-1
!
(config)#
```

  1. ここに sflow forward ingress が設定されていることを確認してください。

- sFlow 統計を実施する物理ポートに対して，フィルタまたは QoS によって sFlow パケットが廃棄されていないか確認してください。確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。

- コンフィグレーションコマンド sflow source で sFlow パケットの送信元（エージェント）IP アドレスを指定した場合，その IP アドレスが本装置のインタフェースに設定されていることを確認してください。

```
(config)# show sflow
sflow destination 192.168.1.20 6343
sflow sample 2048
sflow source 192.168.1.1     <-1
!
(config)#
```

  1. 本装置のインタフェースに設定されている IP アドレスであることを確認してください。

(3) コレクタまでの経路確認

「5.1.1　通信できない，または切断されている」および「5.2.1　通信できない，または切断されている」を参照して，コレクタに対してネットワークが正しく接続されているかを確認してください。もし，コンフィグレーションで sFlow パケットの最大サイズ（sflow max-packet-size）を変更している場合は，指定しているパケットサイズでコレクタまで接続できるか確認してください。

(4) コレクタ側の設定確認

利用しているコレクタ側の設定が正しいか確認してください。

6.5.2 フローサンプルがコレクタに届かない

「6.5.1　sFlow パケットがコレクタに届かない」を確認しても解決しない場合は，次の内容を確認してください。

(1) 中継パケット有無の確認

show interfaces コマンドを実行して，パケットが中継されているか確認してください。

図 6-2　ポート状態の表示例

```
>show interfaces tengigabitethernet 1/2
Date 20XX/07/19 12:00:00 UTC
NIF1: active 6-port 10GBASE-R(SFP+) retry:0
        Average:7000Mbps/120Gbps Peak:7500Mbps at 08:10:30
Port2: active up 10GBASE-LR 0012.e240.0a04
        SFP+ connect
        Time-since-last-status-change:10:30:30
        Bandwidth:10000000kbps Average out:3500Mbps Average in:3500Mbps
        Peak out:3800Mbps at 08:10:30 Peak in:3700Mbps at 08:10:30
        Output rate:2900.0Mbps 3400pps
        Input rate:2900.0Mbps 3400pps      <-1
        Flow control send :on
        Flow control receive:on
        TPID:8100
                                :
>
```

1. フローサンプルを収集する物理ポートで，パケットが中継されていることを確認してください。

6.5.3 カウンタサンプルがコレクタに届かない

「6.5.1　sFlow パケットがコレクタに届かない」を確認しても解決しない場合は，次の内容を確認してください。

(1) カウンタサンプルの送信間隔の確認

本装置のコンフィグレーションで，カウンタサンプルの送信間隔が 0 になっていないか確認してください。この値が 0 になっているとカウンタサンプルがコレクタへ送信されません。

図 6-3　コンフィグレーションの表示例

```
(config)# show sflow
sflow destination 192.168.1.20 6343
sflow sample 2048
sflow polling-interval 60      <-1
!
(config)#
```

1. ここに 0 が設定されていないことを確認してください。

6.6　IEEE802.3ah OAM のトラブル

6.6.1　ポートが inactive 状態となる

UDLD（片方向リンク障害検出）またはループ検出機能によってポートが inactive 状態となる場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 6-12　UDLD またはループ検出機能使用時の障害解析方法

項番	確認内容・コマンド	対応
1	show efmoam コマンドを実行し，inactive 状態にしたポートの障害種別を確認してください。	Link status に Down(loop)が表示されている場合は，ループ構成となっている可能性があります。ネットワーク構成を見直してください。
		Link status に Down(uni-link)が表示されている場合は，項番 2 へ。
2	対向装置で IEEE802.3ah OAM が有効であることを確認してください。	対向装置側で IEEE802.3ah OAM が有効となっていない場合は，有効にしてください。
		対向装置側で IEEE802.3ah OAM が有効となっている場合は項番 3 へ。
3	show efmoam statistics コマンドを実行し，1 ポートに複数の装置が接続されていないことを確認してください。	Info TLV の Unstable がカウントアップされている場合は，該当物理ポートに複数の装置が接続されている可能性があります。該当物理ポートの接続先の装置が 1 台であることを確認してください。
		Info TLV の Unstable がカウントアップされていない場合は項番 4 へ。
4	対向装置と直接接続されていることを確認してください。	メディアコンバータやハブなどが介在している場合は，対向装置と直接接続できるようにネットワーク構成を見直してください。中継装置が必要な場合は，UDLD で使用する制御フレーム OAMPDU を透過し，両側のリンク状態が連動するメディアコンバータを使用してください。
		直接接続されている場合は項番 5 へ。
5	show efmoam コマンドを実行し，障害を検出するための応答タイムアウト回数を確認してください。	udld-detection-count の値が初期値未満の場合，実際に障害となっていなくても片方向リンク障害を誤検出する可能性が高まります。コンフィグレーションコマンド efmoam udld-detection-count で，初期値以上の値を指定してください。 値を変更したあともポートが inactive 状態になる場合は，項番 6 へ。
		udld-detection-count の値が初期値以上の場合は項番 6 へ。
6	フィルタまたは QoS によって OAMPDU が廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。
		OAMPDU が廃棄されていない場合は項番 7 へ。
7	ケーブルを確認してください。	ケーブル不良の可能性があります。該当ポートで使用しているケーブルを交換してください。

6.7 LLDP のトラブル

6.7.1 LLDP で隣接装置情報が取得できない

LLDP で隣接装置の情報が正しく取得できない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 6-13 LLDP 使用時の障害解析方法

項番	確認内容・コマンド	対応
1	LLDP の動作状態を確認してください。 • show lldp	Status が Enabled の場合は，項番 2 へ。
		Status が Enabled でない場合は，LLDP が停止状態になっています。LLDP を有効にしてください。
2	ポート情報を確認してください。 • show lldp detail	隣接装置が接続されているポート情報が表示されている場合は，項番 3 へ。
		隣接装置が接続されているポート情報が表示されていない場合は，該当ポートが LLDP の動作対象外になっています。該当ポートに対して LLDP を有効にしてください。
3	隣接装置が接続されているポートのリンク状態を確認してください。 • show lldp detail	Link が Up の場合は，項番 4 へ。
		Link が Down の場合は，回線状態を確認してください。確認方法は，「3 ネットワークインタフェースのトラブルシュート」を参照してください。
4	隣接装置側で LLDP フレームの送信統計情報を確認してください。	隣接装置側で LLDP フレームの送信数が増加していない場合は，隣接装置側の設定を確認してください。
		隣接装置側で LLDP フレームの送信数が増加している場合は，装置間の接続が誤っている可能性があるため接続を確認してください。 また，フィルタまたは QoS によって LLDP フレームが廃棄されていないか確認してください。確認方法と対応については，「8.1 パケット廃棄の確認」を参照してください。

6.8　BFD のトラブル

6.8.1　BFD セッションが生成できない

show bfd session コマンドで BFD 監視対象と対応する BFD セッションが表示されない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 6-14　BFD セッションが生成できない場合の障害解析方法

項番	確認内容・コマンド	対応
1	本装置で，BFD 監視のコンフィグレーションが正しく設定されていることを確認してください。 • show running-config	BFD 監視のコンフィグレーション（track name，type bfd，および連携プロトコルによるトラックの指定）が正しく設定されていない場合は，修正してください。
2	BFD セッション数が収容条件を超えていないことを確認してください。 • show logging	該当するシステムメッセージ（メッセージ種別：BFD，メッセージ識別子：47010101）が出力されている場合は，不要な BFD 監視をコンフィグレーションから削除したあと，restart bfd コマンドを実行してください。 BFD プログラムの再起動後に，同様のシステムメッセージが出力されないことを確認してください。
3	送信レートが収容条件を超えていないことを確認してください。 • show logging	該当するシステムメッセージ（メッセージ種別：BFD，メッセージ識別子：47010102）が出力されている場合は，不要な BFD 監視を削除するか，BFD 監視の送受信間隔を見直したあと，restart bfd コマンドを実行してください。 BFD プログラムの再起動後に，同様のシステムメッセージが出力されないことを確認してください。
4	BFD セッションの設定に失敗していないか確認してください。 • show logging	該当するシステムメッセージ（メッセージ種別：BFD，メッセージ識別子：47010103）が出力されている場合は，BFD プログラムが正しく動作していません。restart bfd コマンドを実行してください。 BFD プログラムの再起動後に，同様のシステムメッセージが出力されないことを確認してください。
5	BFD 監視対象のアドレスに対して通信できることを確認してください。 • ping マルチホップ監視の場合は，source パラメータを使用して送信元アドレスにループバックアドレスを指定してください。	通信できない場合は，「5.1　IPv4 ネットワークの通信障害」を参照してください。
6	フィルタ，QoS，または uRPF によってパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。
7	対向装置の設定を確認してください。	BFD の連携プロトコルが対向装置を認識できていない，または監視対象として選択できていない可能性があります。対向装置でも，連携プロトコルを正しく設定してください。

6.8.2　BFD セッションが確立できない

BFD セッションが確立しない，または確立してもセッション状態が不安定な場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 6-15　BFD セッションが確立できない場合の障害解析方法

項番	確認内容・コマンド	対応
1	送信レートが収容条件を超えていないことを確認してください。 • show logging	該当するシステムメッセージ（メッセージ種別：BFD，メッセージ識別子：47010102）が出力されている場合は，不要な BFD 監視を削除するか，BFD 監視の送受信間隔を見直したあと，restart bfd コマンドを実行してください。 BFD プログラムの再起動後に，同様のシステムメッセージが出力されないことを確認してください。
2	BFD セッションの設定に失敗していないか確認してください。 • show logging	該当するシステムメッセージ（メッセージ種別：BFD，メッセージ識別子：47010103）が出力されている場合は，BFD プログラムが正しく動作していません。restart bfd コマンドを実行してください。 BFD プログラムの再起動後に，同様のシステムメッセージが出力されないことを確認してください。
3	マルチホップ監視の場合は，ループバックインタフェースの IP アドレスを確認してください。 • show logging • show running-config	該当するシステムメッセージ（メッセージ種別：BFD，メッセージ識別子：47010201）が出力されている場合は，ループバックインタフェースに IP アドレスが設定されていないため，BFD パケットを送信しません。送信を開始するには，ループバックインタフェースに IP アドレスを設定してください。 対向装置への経路に VRF を使用している場合は，ループバックインタフェースにも VRF の設定が必要です。
4	BFD 監視対象のアドレスに対して通信できることを確認してください。 • ping マルチホップ監視の場合は，source パラメータを使用して送信元アドレスにループバックアドレスを指定してください。	通信できない場合は，「5.1　IPv4 ネットワークの通信障害」または「5.2　IPv6 ネットワークの通信障害」を参照してください。
5	BFD パケットが廃棄されていないことを確認してください。 • show bfd discard-packets	有効な BFD パケットを受信するまで，BFD セッションは確立できません。廃棄パケットの数を確認してください。 • Unknown Session が増加 対応する BFD セッションが本装置に設定されていません。本装置の設定を見直してください。 • Invalid TTL/HopLimit が増加 意図しないパケットを中継していないことを確認してください。マルチホップ監視の BFD セッションを確立させるには，コンフィグレーションコマンド type bfd で multihop パラメータを指定してください。 • Authentication Failure が増加 対向装置から，サポートしていない認証方式の使用を要求されています。対向装置の設定を見直してください。 • Other Errors が増加

項番	確認内容・コマンド	対応
		対向装置から，障害検出時間が 300 秒を超えるような設定を要求されている可能性があります。対向装置の設定を見直してください。 • その他 不正な値の BFD パケットです。設定およびネットワークの状態を見直してください。
6	フィルタ, QoS, または uRPF によってパケットが廃棄されていないか確認してください。	確認方法と対応については，「8.1　パケット廃棄の確認」を参照してください。
7	セッション状態が不安定な場合は，BFD セッションのダウン要因を確認してください。 • show bfd session	Diagnostic が Control Detection Time Expired の場合は，対向装置からの BFD パケットを一定時間受信できていません。 • 通信障害が発生している可能性があります。経路および対向装置を確認してください。 • 検出乗数（Multiplier）が 3 未満の場合，パケットの遅延を障害として検出しやすくなります。BFD セッションを安定させたいときは，検出乗数を 3 以上に設定してください。
		Diagnostic が Neighbor Signaled Session Down の場合は，対向装置が BFD セッションをダウンさせています。 • 対向装置で，BFD 監視の設定を変更および削除していないことを確認してください。 • 対向装置で，BFD セッションを切断していないことを確認してください。 • 本装置からの BFD パケットを，対向装置が受信できていない可能性があります。経路および BFD の設定を確認してください。
		Diagnostic が Path Down の場合は，有効な経路が存在しない，またはダウンしています。 • 送信元インタフェースがマネージメントポートではないことを確認してください。 • 送信元インタフェースの状態を確認してください。確認方法は，「3　ネットワークインタフェースのトラブルシュート」を参照してください。
		Diagnostic が Forwarding Plane Reset の場合は，転送機構がリセットされています。 • clear bfd session コマンドが実行されています。BFD セッションが再確立しないときは，restart bfd コマンドを実行してください。
		Diagnostic が Administratively Down の場合は，本装置の運用状態による意図的な BFD セッションの抑止です。 • 本装置または対向装置で，BFD 監視の設定を変更したり削除したりしていないことを確認してください。 • この表の項番 1～3 に従って，収容条件およびコンフィグレーションを確認してください。

項番	確認内容・コマンド	対応
		• 上記のどちらにも該当しないときは，clear bfd session コマンドを実行してください。復旧しないときや頻発するときは，restart bfd コマンドを実行してください。
8	本装置で，対向装置に対して BFD 監視が正しく設定されていることを，コンフィグレーションで確認してください。 • show running-config	BFD 監視が正しく設定されていない場合は，コンフィグレーションを修正してください。
9	対向装置の設定を確認してください。	BFD は双方向で設定する必要があります。対向装置でも，BFD を正しく設定してください。

7 障害情報取得方法

この章では，主に障害情報を取得するときの作業手順について説明します。

7.1　保守情報の採取

装置の運用中に障害が発生した場合，ログ情報やダンプ情報などが自動的に採取されます。また，運用コマンドを使用してダンプ情報を採取できます。

7.1.1　保守情報

本装置の保守情報を次の表に示します。

表 7-1　保守情報

項目	格納場所およびファイル名	ftp コマンドでの転送モード	転送後のファイルの削除
装置再起動時のダンプファイル	障害が発生した系の/dump0/bcu**.000 **：障害が発生した BCU 番号	バイナリモード	○
PA 障害時のダンプファイル	障害が発生した系の/usr/var/hardware/pa**.*** **：障害が発生した BCU 番号 ***：ダンプが採取されてからの通番。最古のものと最新のものとの 2 ファイルまで格納されます。	バイナリモード	○
dump pa コマンド実行時の PA ダンプファイル	コマンドを実行した系の/usr/var/hardware/pa**.cmd **：コマンドを実行した BCU 番号	バイナリモード	○
SFU 障害時のダンプファイル	障害が発生した系の/usr/var/hardware/sfu**.*** **：障害が発生した SFU 番号 ***：ダンプが採取されてからの通番。最古のものと最新のものとの 2 ファイルまで格納されます。	バイナリモード	○
dump sfu コマンド実行時の SFU ダンプファイル	コマンドを実行した系の/usr/var/hardware/sfu**.cmd **：指定した SFU 番号	バイナリモード	○
PSU 障害時のダンプファイル	障害が発生した系の/usr/var/hardware/psu**.*** **：障害が発生した PSU 番号 ***：ダンプが採取されてからの通番。最古のものと最新のものとの 2 ファイルまで格納されます。	バイナリモード	○
dump psu コマンド実行時の PSU ダンプファイル	コマンドを実行した系の/usr/var/hardware/psu**.cmd **：指定した PSU 番号	バイナリモード	○
NIF 障害時のダンプファイル	障害が発生した系の/usr/var/hardware/nif**.*** **：障害が発生した NIF 番号 ***：ダンプが採取されてからの通番。最古のものと最新のものとの 2 ファイルまで格納されます。	バイナリモード	○
dump nif コマンド実行時の NIF ダンプファイル	コマンドを実行した系の/usr/var/hardware/nif**.cmd **：指定した NIF 番号	バイナリモード	○

項目	格納場所およびファイル名	ftp コマンドでの転送モード	転送後のファイルの削除
PS 障害時のダンプファイル	障害が発生した系の/usr/var/hardware/ps**.000 **：障害が発生した PS 番号	バイナリモード	○
ファンユニット障害時のダンプファイル	障害が発生した系の/usr/var/hardware/fan**.000 **：障害が発生したファンユニット番号	バイナリモード	○
ログ	採取したログのディレクトリに，次の名前で格納します。 運用ログ：log.txt 統計ログ：log_ref.txt	アスキーモード	○
コンフィグレーションファイル障害時の情報	装置管理者モードで次のコマンドを実行して，二つのファイルをホームディレクトリにコピーします。そのあと，ファイルを転送してください。 • cp /config/cnf/system.cnf system.cnf • cp /config/cnf/system.txt system.txt	バイナリモード	○※
障害待避情報	/usr/var/core/*.core	バイナリモード	○

（凡例）　○：削除してください

注※　コピーしたファイルを削除してください。

7.1.2　dump コマンドを使用した障害情報の採取

本装置では，運用コマンドを使用して，装置を構成するボードや構成部位のダンプを採取できます。

通信障害が発生した場合は，運用系 BCU で次に示すコマンドをすべて実行して，メモリダンプを採取してください。

1. active 状態のすべての SFU に対して，dump sfu コマンドを実行します。
2. 障害が発生しているポートが収容されている PSU に対して，dump psu コマンドを実行します。
3. 障害が発生しているポートが収容されている NIF に対して，dump nif コマンドを実行します。

採取されたメモリダンプは，コマンドが実行された系の/usr/var/hardware にメモリダンプファイルとして格納されます。採取後はメモリダンプファイルを削除してください。

[実行例]

NIF 番号 1，ポート番号 1 で通信障害が発生している場合の例を次に示します。

1. 運用系 BCU にログインして，active 状態のすべての SFU に対して dump sfu コマンドを実行します。
   システムメッセージが表示されたら，次の dump sfu コマンドを実行します。

```
> dump sfu 1
The dump-collection command was accepted.
>
20XX/01/01 08:18:23 UTC 1-1(A) S6 SFU SFU:1 350e0501 00 000000000000 The SFU online dump co
mmand was executed.
>
> dump sfu 2
The dump-collection command was accepted.
>
20XX/01/01 08:28:23 UTC 1-1(A) S6 SFU SFU:2 350e0501 00 000000000000 The SFU online dump co
mmand was executed.
>
```

```
> dump sfu 3
The dump-collection command was accepted.
>
20XX/01/01 08:38:23 UTC 1-1(A) S6 SFU SFU:3 350e0501 00 000000000000 The SFU online dump co
mmand was executed.
>
> dump sfu 4
The dump-collection command was accepted.
>
20XX/01/01 08:48:23 UTC 1-1(A) S6 SFU SFU:4 350e0501 00 000000000000 The SFU online dump co
mmand was executed.
>
```

2. 最後の SFU のシステムメッセージが表示されたあとで，障害が発生しているポート（ポート番号 1）が収容されている PSU に対して dump psu コマンドを実行します。

```
> dump psu 1
The dump-collection command was accepted.
>
20XX/01/01 08:58:52 UTC 1-1(A) S6 PSU PSU:1 350e0601 00 000000000000 The PSU online dump co
mmand was executed.
>
```

3. PSU のシステムメッセージが表示されたあとで，障害が発生しているポート（ポート番号 1）が収容されている NIF（NIF 番号 1）に対して，dump nif コマンドを実行します。

```
> dump nif 1
The dump-collection command was accepted.
>
20XX/01/01 09:04:14 UTC 1-1(A) S6 NIF NIF:1 350e0701 00 000000000000 The NIF online dump co
mmand was executed.
>
```

7.2 ftp コマンドによる保守情報のファイル転送

本装置の ftp コマンドを使用すると，ログやダンプファイルなどの保守情報をリモート運用端末やリモートホストにファイル転送できます。

7.2.1 ダンププファイルをリモート運用端末に転送する

ftp コマンドを使用して，採取したダンプファイルをリモート運用端末に転送する手順を次に示します。

図 7-1 ダンプファイルのリモート運用端末へのファイル転送

```
> cd /dump0                                      <---1
> ftp 192.168.0.1                                <---2
Connected to 192.168.0.1.
220 192.168.0.1 FTP server ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary                                      <---3
200 Type set to I.
ftp> cd /usr/home/staff1                         <---4
250 CWD command successful.
ftp> put bcu01.000                               <---5
local: bcu01.000 remote: bcu01.000
200 EPRT command successful.
150 Opening BINARY mode data connection for 'bcu01.000'.
100% |*************************|  2780 KiB    1.55 MiB/s    00:00 ETA
226 Transfer complete.
2846953 bytes sent in 00:01 (1.55 MiB/s)
ftp> bye
221 Thank you for using the FTP service on 192.168.0.1.
>
```

1. 転送元ディレクトリを指定します。
2. 転送先の端末アドレスを指定します。
3. バイナリモードに設定※します。
4. 転送先ディレクトリを指定します。
5. ダンプファイルを転送します。

注※

ダンプファイルは必ずバイナリモードで転送してください。ダンプファイルをアスキーモードで転送すると，正確なダンプ情報が取得できなくなります。

7.2.2 ログをリモート運用端末に転送する

ftp コマンドを使用して，採取したログをリモート運用端末に転送する手順を次に示します。

図 7-2 ログのリモート運用端末へのファイル転送

```
> show logging > log.txt
> show logging reference > log_ref.txt
> ftp 192.168.0.1                                <---1
Connected to 192.168.0.1.
220 192.168.0.1 FTP server ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
```

```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii                                        <---2
200 Type set to A.
ftp> cd /usr/home/staff1                          <---3
250 CWD command successful.
ftp> put log.txt                                  <---4
local: log.txt remote: log.txt
200 EPRT command successful.
150 Opening ASCII mode data connection for 'log.txt'.
100% |*************************|   251 KiB   11.13 MiB/s    --:-- ETA
226 Transfer complete.
257490 bytes sent in 00:00 (1.21 MiB/s)
ftp>
ftp> put log_ref.txt                              <---4
local: log_ref.txt remote: log_ref.txt
200 EPRT command successful.
150 Opening ASCII mode data connection for 'log_ref.txt'.
100% |*************************| 33165        7.48 MiB/s    --:-- ETA
226 Transfer complete.
33165 bytes sent in 00:00 (160.98 KiB/s)
ftp> bye
221 Thank you for using the FTP service on 192.168.0.1.
>
```

1. 転送先の端末アドレスを指定します。
2. アスキーモードに設定します。
3. 転送先ディレクトリを指定します。
4. ログを転送します。

7.2.3　コアファイルをリモート運用端末に転送する

ftp コマンドを使用して，採取したコアファイルをリモート運用端末に転送する手順を次に示します。

図 7-3　コアファイルのリモート運用端末へのファイル転送

```
> cd /usr/var/core/
> ls                                              <---1
configManager.core snmpd.core
> ftp 192.168.0.1                                 <---2
Connected to 192.168.0.1.
220 192.168.0.1 FTP server ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> prompt                                       <---3
Interactive mode off.
ftp> binary                                       <---4
200 Type set to I.
ftp> cd /usr/home/staff1                          <---5
250 CWD command successful.
ftp> mput *.core                                  <---6
local: configManager.core remote: configManager.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'configManager.core'.
100% |*************************|  6740 KiB    0.98 MiB/s    00:00 ETA
226 Transfer complete.
6902471 bytes sent in 00:06 (0.98 MiB/s)
local: snmpd.core remote: snmpd.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'snmpd.core'.
100% |*************************|   843 KiB   12.83 MiB/s    00:00 ETA
226 Transfer complete.
863812 bytes sent in 00:00 (4.10 MiB/s)
ftp> bye
```

```
221 Thank you for using the FTP service on 192.168.0.1.
>
```

1. コアファイルが存在することを確認します。
   ファイルが存在しない場合は，何もしないで終了します。
2. 転送先の端末アドレスを指定します。
3. 対話モードを変更します。
4. バイナリモードに設定※します。
5. 転送先ディレクトリを指定します。
6. コアファイルを転送します。

注※

コアファイルは必ずバイナリモードで転送してください。コアファイルをアスキーモードで転送すると，正確な障害退避情報が取得できなくなります。

7.3　show tech-support コマンドによる情報採取とファイル転送

show tech-support コマンドを使用すると，障害発生時の情報を一括して採取できます。また，ftp パラメータを指定することで，採取した情報をリモート運用端末やリモートホストに転送できます。

show tech-support コマンドを使用して，保守情報を採取してリモート運用端末に転送する手順を次に示します。

図 7-4　保守情報のリモート運用端末へのファイル転送

```
> show tech-support ftp                                                   <-1
Enter the host name of the FTP server.           : 192.168.0.1            <-2
Enter the user ID for the FTP server connection. : staff1                 <-3
Enter the password for the FTP server connection. :                       <-4
Enter the path name of the FTP server.           : /usr/home/staff1       <-5
Enter the file names for the log and dump files.  : support               <-6
Do you want to check and extract dump files on a standby system? (y/n): y  <-7
Mon Dec 31 12:00:00 UTC 20XX
Transferred support.txt .
Executing...............................
File transfer ended successfully.
########## Dump files' Information ##########
***** ls -l /dump0 *****
total 4568
-rwxrwxrwx  1 root  wheel  4677464 Dec 18 21:16:16 20XX bcu01.000
***** ls -l /usr/var/hardware *****
total 1368
-rwxrwxrwx  1 root  wheel  1002811 Dec 27 11:56:16 20XX nif05.000
***** ls -l /standby/dump0 *****
***** ls -l /standby/usr/var/hardware/ *****
########## End of Dump files' Information ##########
########## Core files' Information ##########
***** ls -l /usr/var/core *****
***** ls -l /standby/usr/var/core *****
No Core files
########## End of Core files' Information ##########
Transferred support.tgz .
Executing...
File transfer ended successfully.
>
```

1. コマンドを実行します。
2. リモートホスト名を指定します。
3. ユーザ名を指定します。
4. パスワードを入力します。
5. 転送先ディレクトリを指定します。
6. ファイル名を指定します。
7. 待機系のダンプファイル採取を選択します。

7.4　リモート運用端末の ftp コマンドによる情報採取とファイル転送

リモート運用端末やリモートサーバから ftp コマンドで本装置に接続して，ファイル名を指定することで，障害情報や保守情報を取得できます。

(1)　show tech-support の情報を取得する

リモート運用端末をクライアントとして ftp コマンドで本装置に接続して，必要な show tech-support 情報のファイル名を指定して情報を取得する手順を次に示します。

図 7-5　show tech-support 情報の取得

```
client-host> telnet 192.168.0.21                    <---1
Trying 192.168.0.21...
Connected to 192.168.0.21
Escape character is '^]'.

login: staff1
Password:

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

>show tech-support > show-tech.txt                  <---2
>exit
Connection closed by foreign host.
client-host> ftp 192.168.0.21                       <---3
Connected to 192.168.0.21.
220 192.168.0.21 FTP server ready.
Name (192.168.0.21:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get show-tech.txt                              <---4
local: show-tech.txt remote: show-tech.txt
200 EPRT command successful.
150 Opening BINARY mode data connection for 'show-tech.txt' (3784076 bytes).
100% |*************************************|  3695 KiB    1.02 MiB/s    00:00 ETA
226 Transfer complete.
3784076 bytes received in 00:03 (1.02 MiB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.21.
client-host>
```

1. クライアントから本装置に telnet で接続します。
2. 本装置で show tech-support 情報をファイルに保存します（ファイル名として show-tech.txt を指定）。
3. クライアントから本装置に ftp で接続します。
4. show-tech.txt ファイルをクライアントに転送します。

注

装置の負荷状態や通信路の状態によっては，クライアント側がネットワークタイムアウトで切断することがあります。その場合は，クライアントのタイムアウト時間を長く設定してください。

(2)　ダンプファイルおよびコアファイルを取得する

リモート運用端末をクライアントとして ftp コマンドで本装置に接続して，必要なファイル名を指定してダンプファイルおよびコアファイルを取得します。ftp コマンドで専用のファイル名を get 指定すると，複数のファイルを一括取得できます。コアファイルを取得するときは，個別にファイルを指定できます。

get 指定で使用する専用のファイル名と取得できるファイルの対応を次の表に示します。

表 7-2　ftp コマンドの get 指定で取得できるファイル

get 指定する専用のファイル名	取得ファイル
.dump	/dump0 と/usr/var/hardware と/usr/var/core 以下のファイル（圧縮）
.dump0	/dump0 以下のファイル（圧縮）
.hardware	/usr/var/hardware 以下のファイル（圧縮）
.core	/usr/var/core 以下のファイル（圧縮）

ftp コマンドで get 指定してダンプファイルを一括取得する手順を次に示します。

図 7-6　リモート運用端末からのダンプファイルの取得

```
client-host> ftp 192.168.0.60                          <---1
Connected to 192.168.0.60.
220 192.168.0.60 FTP server ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary                                            <---2
200 Type set to I.
ftp> get .dump dump.tgz                                <---3
local: dump.tgz remote: .dump
200 EPRT command successful.
150 Opening BINARY mode data connection for '/etc/ftpdump'.
 16539 KiB  816.40 KiB/s
226 Transfer complete.
16936547 bytes received in 00:20 (813.99 KiB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>
```

1. クライアントから本装置に ftp で接続します。
2. バイナリモードに設定します。
   ダンプファイルおよびコアファイルは必ずバイナリモードで転送してください。アスキーモードでは，正確な情報が転送できません。
3. .dump のファイルを，クライアントに転送します（ファイル名として dump.tgz を指定)。

注

- ftp コマンドの ls などでは，「表 7-2　ftp コマンドの get 指定で取得できるファイル」に示す get 指定する専用のファイル名は表示されません。そのため，一括取得するファイルの容量確認などはできません。
- 装置の負荷状態や通信路の状態によっては，クライアント側がネットワークタイムアウトで切断することがあります。その場合は，クライアントのタイムアウト時間を長く設定してください。

- 「表 7-2　ftp コマンドの get 指定で取得できるファイル」に示す get 指定する専用のファイル名と同じ名前のファイルがカレントディレクトリに存在する場合，そのファイルを取得するため，ダンプファイルの一括取得はできません。ダンプファイルを一括取得する場合は，同じ名前のファイルを削除するか，cd などのコマンドで異なるディレクトリに移動したあと，取得してください。

7.5 MC への書き込み

障害情報や保守情報は MC に書き込めます。ただし，MC の容量制限があるので注意してください。

7.5.1 運用端末での MC へのファイル書き込み

運用端末で装置の情報を MC に書き込むときの手順を次に示します。

［実行例］

1. 書き込むための MC を装置に挿入します。
2. ls コマンドで，コピー元ファイル（tech.log）の容量を確認します。

```
> ls -l tech.log
-rw-r--r--  1 operator  users  234803 Nov 15 15:52 tech.log
```

3. show mc コマンドで，MC の空き容量を確認します。

```
> show mc
Date 20XX/04/01 07:20:11 UTC
BCU1 MC: enabled
     CID: 00c7000910d06b224734304653415001
     used:        189,792KB
     free:      3,680,928KB
     total:     3,870,720KB
BCU2 MC: --------
>
```

下線部が空き容量です。

4. cp コマンドで，コピー元ファイルを tech-1.log というファイル名で，MC にコピーします。

```
> cp tech.log mc-file tech-1.log
```

5. ls コマンドで，MC にファイルが書き込めていることを確認します。

```
> ls mc-dir
Name             Size
tech-1.log               234803
>
```

8 通信障害の解析

この章では，通信障害が発生した場合の対処について説明します。

8.1　パケット廃棄の確認

8.1.1　フィルタによる廃棄を確認する

本装置を使用しているネットワーク上で通信トラブルが発生する要因として，フィルタによって特定のフレームが廃棄されている可能性が考えられます。フィルタによるフレーム廃棄の確認方法を次に示します。

なお，フィルタの動作にポリシーベースルーティングを指定している場合は，次の確認方法に加えて，「5.3.1　ポリシーベースルーティングによる通信障害の確認」を参照してください。

(1)　フィルタによるフレーム廃棄の確認方法

1. show access-filter コマンドを実行して，インタフェースに適用しているアクセスリストのフィルタ条件とフィルタ条件に一致したパケット数，暗黙の廃棄のフィルタエントリで廃棄したパケット数を確認します。
2. 1.で確認したフィルタ条件と通信できないフレームの内容を比較して，該当フレームが廃棄されていないか確認します。通信できないフレームの内容が適用しているすべてのフィルタ条件に一致していない場合，暗黙の廃棄のフィルタエントリでフレームが廃棄されている可能性があります。
3. フィルタでフレームが廃棄されている場合，フィルタのコンフィグレーションの設定が適切か見直してください。
4. コンフィグレーションが正しく設定されている場合は，アクセスリストロギングを使用して，廃棄したパケットの情報を確認してください。

8.1.2　QoS による廃棄を確認する

本装置を使用しているネットワーク上で通信トラブルが発生する要因として，QoS のポリサー，QoS フロー廃棄，ポートシェーパ，または装置内キューによってフレームの廃棄または滞留が発生している可能性が考えられます。QoS によって本装置内でフレームの廃棄または滞留が発生している場合に，廃棄または滞留個所を特定する方法を次に示します。

(1)　ポリサーによるフレーム廃棄の確認方法

1. show qos-flow および show policer コマンドを実行して，インタフェースに適用しているポリサーのフロー検出条件と動作指定，ポリサーの統計情報を確認します。
2. 1.で確認したフロー検出条件と通信できないフレームの内容を比較して，該当フレームが廃棄されていないか確認します。

   最大帯域監視を違反したフレームは廃棄されて，統計情報の Matched packets(Max-rate over)にカウントされます。この値がカウントされている場合，インタフェースに適用しているポリサーによってフレームが廃棄されています。
3. ポリサーでフレームが廃棄されている場合, QoS のコンフィグレーションの設定およびポリサーの設定が適切か見直してください。

(2)　QoS フロー廃棄によるフレーム廃棄の確認方法

1. show qos-flow コマンドを実行して，インタフェースに適用している QoS フローリストの QoS フロー廃棄を指定しているフロー検出条件と，フロー検出条件に一致したパケット数を確認します。
2. 1.で確認したフロー検出条件と通信できないフレームの内容を比較して，該当フレームが廃棄されていないか確認します。

3. QoS フロー廃棄でフレームが廃棄されている場合，QoS のコンフィグレーションの設定が適切か見直してください。

(3)　ポートシェーパによるフレームの廃棄および滞留の確認方法

1. show qos queueing port コマンドを実行して，通信で使用する出力インタフェースのポート送信キューの統計情報に表示される Discard packets，Send packets，および Qlen を確認します。
2. 1.で確認した Discard packets がカウントされている場合，廃棄制御によってフレームが廃棄されています。
3. 1.で確認した Send packets がカウントされていなくて，Qlen がカウントされている場合，スケジューリングによってフレームが滞留しています。
4. フレームの廃棄および滞留が発生している場合，ポートシェーパのコンフィグレーションの設定が適切か見直してください。

(4)　階層化シェーパによるフレームの廃棄および滞留の確認方法

1. show shaper コマンドを実行して, 通信で使用する出力インタフェースのユーザ送信キューの統計情報に表示される Discard packets，Send packets，および Qlen を確認します。
2. 1.で確認した Discard packets がカウントされている場合，廃棄制御によってフレームが廃棄されています。
3. 1.で確認した Send packets がカウントされ，Qlen がカウントされている場合，スケジューリングによってフレームが滞留しています。
4. フレームの廃棄および滞留が発生している場合，階層化シェーパのコンフィグレーションの設定が適切か見直してください。

(5)　装置内キューによるフレームの廃棄および滞留の確認方法

1. show qos queueing コマンドおよび show shaper コマンドを実行して，次に示すキューの Discard packets，Send packets，および Qlen を確認します。

   ユニキャストフレームの場合

   - ポート受信キュー
   - NIF FE 送信キュー
   - PSU-FE NIF 受信キュー
   - PSU-FE SSW 送信（中継）キュー
   - PSU-SSW FE 受信（ユニキャスト）キュー
   - PSU-SSW FE 送信（ユニキャスト）キュー
   - PSU-FE SSW 受信（中継）キュー
   - PSU-FE NIF 送信キュー
   - NIF FE 受信キュー
   - ポート送信キューまたはユーザ送信キュー

   マルチキャストフレームの場合

   - ポート受信キュー
   - NIF FE 送信キュー
   - PSU-FE NIF 受信キュー
   - PSU-FE SSW 送信（中継）キュー
   - PSU-SSW FE 受信（マルチキャスト）キュー

- PSU-SSW FE 送信（マルチキャスト）キュー
- PSU-FE SSW 受信（中継）キュー
- PSU-FE NIF 送信キュー
- NIF FE 受信キュー
- ポート送信キューまたはユーザ送信キュー

BCU を経由するフレームの場合

- ポート受信キュー
- NIF FE 送信キュー
- PSU-FE NIF 受信キュー
- PSU-FE CPU 送信キュー
- BCU-PA PSU 受信キュー
- BCU-CPU PA 受信キュー
- BCU-CPU 送信キュー
- PSU-FE SSW 送信（制御）キュー
- PSU-SSW FE 受信キュー
- PSU-SSW FE 送信キュー
- PSU-FE SSW 受信（制御）キュー
- PSU-FE NIF 送信キュー
- NIF FE 受信キュー
- ポート送信キューまたはユーザ送信キュー

2. 1.で確認した Discard packets がカウントされている場合，装置内キューによってフレームが廃棄されています。
3. 1.で確認した Send packets がカウントされていなくて，Qlen がカウントされている場合，装置内キューによってフレームが滞留しています。
4. フレームの廃棄および滞留が発生している場合，対象フレームの流量を見直してください。

8.1.3 uRPF による廃棄を確認する

本装置を使用しているネットワーク上で通信トラブルが発生する要因として，uRPF によって特定のパケットが廃棄されている可能性が考えられます。uRPF によるパケット廃棄の確認方法を次に示します。

1. show ip urpf statistics コマンドまたは show ipv6 urpf statistics コマンドで interface パラメータを指定して実行して，Discarded IPv4 packets または Discarded IPv6 packets を確認します。
2. 1.で確認した Discarded IPv4 packets または Discarded IPv6 packets がカウントされている場合，uRPF によってパケットが廃棄されています。
3. uRPF でパケットが廃棄されている場合，ネットワーク構成を見直して，uRPF の廃棄対象となるパケットが本装置宛てに送信されないようにしてください。

8.2　ポート inactive 状態の確認

8.2.1　スパニングツリーによる inactive 状態を確認する

BPDU ガード機能による inactive 状態は，show spanning-tree コマンドで detail パラメータを指定して確認してください。ポートの状態や役割がネットワーク構成と異なる場合は,「4.2　スパニングツリーの通信障害」を参照してください。

8.2.2　L2 ループ検知による inactive 状態を確認する

L2 ループ検知による inactive 状態は，show loop-detection コマンドでポートの状態を確認してください。

L2 ループ検知による inactive 状態の場合は，ループが発生する構成を変更したあと，activate コマンドで該当ポートを active 状態にしてください。また，コンフィグレーションコマンド loop-detection auto-restore-time が設定されている場合は，自動的に active 状態に戻ります。

8.2.3　ストームコントロールによる inactive 状態を確認する

ストームコントロールによる inactive 状態は, show logging コマンドで確認してください。次のメッセージが出力される場合は，ストームから回復後，activate コマンドで該当ポートを active 状態にしてください。

- メッセージ種別：STMCTL，メッセージ識別子：52000002
- メッセージ種別：STMCTL，メッセージ識別子：52000003
- メッセージ種別：STMCTL，メッセージ識別子：52000004

8.2.4　IEEE802.3ah OAM による inactive 状態を確認する

UDLD（片方向リンク障害検出）またはループ検出機能による inactive 状態は，show efmoam コマンドでポートの障害種別を確認してください。障害の解析方法については，「6.6　IEEE802.3ah OAM のトラブル」を参照してください。

9 装置の再起動

この章では，主に装置を再起動する場合の作業手順について説明します。

9.1 装置を再起動する

9.1.1 装置の再起動

運用系 BCU で reload コマンドを使用して，装置を再起動できます。コマンドの入力形式およびパラメータについては，「運用コマンドレファレンス」を参照してください。

(1) メモリダンプを採取して再起動する

BCU を再起動するときにメモリダンプを採取する場合の手順を次に示します。

[実行例 1]

待機系 BCU を再起動して，その際メモリダンプを採取します。

1. 次の reload コマンドを実行します。なお，dump-image パラメータは省略できます。

```
> reload -f dump-image standby
>
```

[実行例 2]

運用系 BCU を再起動して，その際メモリダンプを採取します。運用系 BCU が再起動すると，系切替が発生します。

1. 次の reload コマンドを実行します。なお，dump-image パラメータは省略できます。

```
> reload -f dump-image active
>
```

[実行例 3]

両系の BCU を再起動して，その際メモリダンプを採取します。

1. 次の reload コマンドを実行します。なお，dump-image パラメータは省略できます。

```
> reload -f dump-image
>
```

(2) メモリダンプを採取しないで再起動する

BCU を再起動するときにメモリダンプを採取しない場合の手順を次に示します。

[実行例 1]

待機系 BCU を再起動しますが，その際メモリダンプを採取しません。

1. 次の reload コマンドを実行します。

```
> reload -f no-dump-image standby
>
```

[実行例 2]

運用系 BCU を再起動しますが，その際メモリダンプを採取しません。運用系 BCU が再起動すると，系切替が発生します。

1. 次の reload コマンドを実行します。

```
> reload -f no-dump-image active
>
```

[実行例 3]

両系の BCU を再起動しますが，その際メモリダンプを採取しません。

1. 次の reload コマンドを実行します。

```
> reload -f no-dump-image
>
```

(3)　装置を停止する

BCU および装置を停止する場合の手順を次に示します。停止したときは，メモリダンプを採取しません。

[実行例 1]

待機系 BCU を停止します。

1. 次の reload コマンドを実行します。

```
> reload -f stop standby
>
```

[実行例 2]

運用系 BCU を停止します。運用系 BCU が停止すると，系切替が発生します。

1. 次の reload コマンドを実行します。

```
> reload -f stop active
>
```

[実行例 3]

装置を停止します。

1. 次の reload コマンドを実行します。

```
> reload -f stop
>
```

付録

付録 A　show tech-support コマンド表示内容詳細

付録 A.1　show tech-support コマンド表示内容詳細

show tech-support コマンドで，プロトコルのパラメータ指定ごとに表示されるコマンドの内容を次の表に示します。なお，表示内容の詳細は，「運用コマンドレファレンス」を参照してください。

【注意】

show tech-support コマンドで表示される情報の一部については，「運用コマンドレファレンス」に記載していません。これらの情報は装置の内部情報を含んでいるため，非開示としています。

また，ソフトウェアバージョンによって一部表示されるものとされないものがあります。あらかじめご了承ください。

表 A-1　表示内容詳細

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
1	show version	本装置のソフトウェアバージョン情報およびハードウェア情報	○	○	○	○
2	show system	本装置の運用情報	○	○	×	×
3	show process cpu bcu	BCU プロセス単位の CPU 使用量	○	○	○	○
4	show cpu bcu detail	BCU-CPU の使用率	○	○	○	○
5	show process memory bcu	BCU プロセス単位のメモリ使用量	○	○	○	○
6	/usr/local/diag/statShow	OS 内リソースのカウンタ情報	○	○	○	○
7	show memory	BCU のメモリ情報	○	○	○	○
8	show processes cpu pa	PA のプロセス CPU 使用率情報	○	○	○	○
9	show cpu pa detail	PA の CPU 使用率情報	○	○	○	○
10	show processes memory pa	PA のプロセスメモリ使用率情報	○	○	○	○
11	show memory pa	PA のメモリ使用率情報	○	○	○	○
12	show processes cpu psu	PSU-CPU のプロセス CPU 使用率情報	○	○	○	○
13	show cpu psu detail	PSU-CPU の CPU 使用率情報	○	○	○	○
14	show processes memory psu	PSU-CPU のプロセスメモリ使用率情報	○	○	○	○
15	show memory psu	PSU-CPU のメモリ使用率情報	○	○	○	○
16	fstat	BCU 内の装置ファイルデスクリプタ使用情報	○	○	○	○

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
17	/usr/local/diag/krtstat	OS 内経路情報･内部制御情報カウンタ	○	○	○	○
18	/usr/local/diag/showtcp -a	BCU 内の装置 TCP ソケット情報	○	○	○	○
19	show tcp ha connections	TCP 高可用の TCP コネクション情報	○	○	○	○
20	netstat -An	BCU 内部通信情報	○	○	○	○
21	show netstat interface	BCU 内部通信情報	○	○	○	○
22	show netstat statistics	BCU 内部通信情報	○	○	×	×
23	pstat -f	デスクリプタ情報	○	○	○	○
24	/sbin/dmesg	OS トレース情報	○	○	○	○
25	cat /var/run/dmesg.boot	BCU OS 起動ログ	○	○	○	○
26	cat /var/log/messages.old	BCU OS 動作ログ	○	○	○	○
27	cat /var/log/messages	BCU OS 動作ログ	○	○	○	○
28	gzcat /var/run/dmesg.pon.old.gz	OS トレース情報	○	○	○	○
29	gzcat /var/run/dmesg.pon.gz	OS トレース情報	○	○	○	○
30	cat /standby/var/run/dmesg.boot	OS トレース情報	○	○	×	×
31	cat /standby/var/log/messages.old	OS トレース情報	○	○	×	×
32	cat /standby/var/log/messages	OS トレース情報	○	○	×	×
33	gzcat /standby/var/run/dmesg.pon.old.gz	OS トレース情報	○	○	×	×
34	gzcat /standby/var/run/dmesg.pon.gz	OS トレース情報	○	○	×	×
35	cat /var/log/clitrace1	CLI 内部のエラー情報	○	○	○	○
36	cat /var/log/clitrace2	CLI 上で実行されたコマンドのログ	○	○	○	○
37	cat /var/log/clitrace3	CLI 起動時の装置情報	○	○	○	○
38	cat /standby/var/log/clitrace1	待機系の CLI 内部のエラー情報	○	○	×	×
39	cat /standby/var/log/clitrace2	待機系の CLI 上で実行されたコマンドのログ	○	○	×	×
40	cat /standby/var/log/clitrace3	待機系の CLI 起動時の装置情報	○	○	×	×
41	cat /var/log/mmitrace	運用コマンドトレース情報	○	○	○	○

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
42	cat /standby/var/log/mmitrace	待機系の運用コマンドトレース情報	○	○	×	×
43	show psu resources	PSU のリソース情報	○	○	×	×
44	show dumpfile	採取済みのダンプファイル情報	○	○	×	×
45	df -ik	BCU 内部ディスク使用量	○	○	○	○
46	show environment	本装置の環境情報	○	○	×	×
47	du -Pk /	BCU 内部ディスク使用量	○	○	○	○
48	ls -lTiR /dump0	BCU 内部ディスク使用量	○	○	○	○
49	ls -lTiR /dump1	BCU 内部ディスク使用量	○	○	○	○
50	ls -lTiR /log	BCU 内部ディスク使用量	○	○	○	○
51	ls -lTiR /tmp	BCU 内部ディスク使用量	○	○	○	○
52	ls -lTiR /config	BCU 内部ディスク使用量	○	○	○	○
53	ls -lTiR /standby/dump0	BCU 内部ディスク使用量	○	○	×	×
54	ls -lTiR /var	BCU 内部ディスク使用量	○	○	○	○
55	ls -lTiR /standby/config	BCU 内部ディスク使用量	○	○	×	×
56	ls -lTiR /standby/log	BCU 内部ディスク使用量	○	○	×	×
57	ls -lTiR /standby/dump1	BCU 内部ディスク使用量	○	○	×	×
58	ls -lTiR /standby/var	BCU 内部ディスク使用量	○	○	×	×
59	ls -lTiR /standby/tmp	BCU 内部ディスク使用量	○	○	×	×
60	show sessions	ログインセッション情報	○	○	○	○
61	stty -a -f /dev/tty00	コンソール端末情報	○	○	○	○
62	show accounting	アカウンティング情報	○	○	○	○
63	show users	本装置に設定されているログインユーザアカウント情報	○	○	○	○
64	/usr/sbin/pstat -t	端末情報	○	○	○	○
65	show ntp associations	接続されている NTP サーバの動作状態	○	○	○	○
66	show logging count 10000	運用系運用ログ情報	○	○	○	○
67	show logging reference	運用系統計ログ情報	○	○	○	○
68	show logging count 10000 standby	待機系運用ログ情報	○	○	○	○

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
69	show logging reference standby	待機系統計ログ情報	○	○	○	○
70	cat /var/log/kern.log.old	BCU 内部ディスク使用量	○	○	○	○
71	cat /var/log/kern.log	BCU 内部ディスク使用量	○	○	○	○
72	cat /var/log/daemon.log.old	BCU 内部ディスク使用量	○	○	○	○
73	cat /var/log/daemon.log	BCU 内部ディスク使用量	○	○	○	○
74	cat /var/run/cons.boot1	BCU 起動情報	○	○	○	○
75	cat /var/run/cons.boot2	BCU 起動情報	○	○	○	○
76	cat /standby/var/log/kern.log.old	BCU 内部ディスク使用量	○	○	×	×
77	cat /standby/var/log/kern.log	BCU 内部ディスク使用量	○	○	×	×
78	cat /standby/var/log/daemon.log.old	BCU 内部ディスク使用量	○	○	×	×
79	cat /standby/var/log/daemon.log	BCU 内部ディスク使用量	○	○	×	×
80	cat /standby/var/run/cons.boot1	待機系の BCU 起動情報	○	○	×	×
81	cat /standby/var/run/cons.boot2	待機系の BCU 起動情報	○	○	×	×
82	/usr/local/diag/gentrcinfo -s	コンフィグレーションコマンドトレース情報	○	○	○	○
83	/usr/local/diag/inci_info -T -c nodeProc	nodeProc デバッグ情報	○	○	○	○
84	/usr/local/diag/inci_info -T -c nodeCtl	nodeCtl デバッグ情報	○	○	○	○
85	/usr/local/diag/inci_info -T -c nodeDev	nodeDev デバッグ情報	○	○	○	○
86	/usr/local/diag/inci_info -T -c logCtl	logCtl デバッグ情報	○	○	○	○
87	cat /var/tmp/logctl/trace/logCtl.log	logCtl トレース情報	○	○	○	○
88	cat /var/tmp/logctl/trace/logSysMsgCtl.log	logSysMsgCtl トレース情報	○	○	○	○
89	cat /var/tmp/logctl/trace/logSyslogCtl.log	logSyslogCtl トレース情報	○	○	○	○
90	cat /var/tmp/logctl/trace/logEmailCtl.log	logEmailCtl トレース情報	○	○	○	○

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
91	cat /var/tmp/logctl/trace/logMateSend.log	logMateSend トレース情報	○	○	○	○
92	cat /var/tmp/logctl/trace/logSave-l.log	logSave トレース情報	○	○	○	○
93	cat /standby/var/tmp/logctl/trace/logCtl.log	待機系の logCtl トレース情報	○	○	×	×
94	cat /standby/var/tmp/logctl/trace/logSysMsgCtl.log	待機系の logSysMsgCtl トレース情報	○	○	×	×
95	cat /standby/var/tmp/logctl/trace/logSyslogCtl.log	待機系の logSyslogCtl トレース情報	○	○	×	×
96	cat /standby/var/tmp/logctl/trace/logEmailCtl.log	待機系の logEmailCtl トレース情報	○	○	×	×
97	cat /standby/var/tmp/logctl/trace/logMateSend.log	待機系の logMateSend トレース情報	○	○	×	×
98	cat /standby/var/tmp/logctl/trace/logSave-l.log	待機系の logSave トレース情報	○	○	×	×
99	cat /usr/var/pplog/ppupdate.log	アップデートのログ情報	○	○	○	○
100	cat /usr/var/pplog/ppupdate2.log	アップデートのログ情報	○	○	○	○
101	cat /standby/usr/var/pplog/ppupdate.log	待機系のアップデートのログ情報	○	○	×	×
102	cat /standby/usr/var/pplog/ppupdate2.log	待機系のアップデートのログ情報	○	○	×	×
103	cat /var/log/authlog	認証トレース情報	○	○	○	○
104	cat /standby/var/log/authlog	待機系の認証トレース情報	○	○	×	×
105	cat /var/log/xferlog	FTP トレース情報	○	○	○	○
106	cat /standby/var/log/xferlog	待機系の FTP トレース情報	○	○	×	×
107	cat /var/log/policy/policyd.log	ポリシーベースルーティング制御プログラムのログ情報	○	×	○	×
108	cat /standby/var/log/policy/policyd.log	待機系のポリシーベースルーティング制御プログラムのログ情報	○	×	×	×
109	cat /var/log/ssh.log	SSH ログ情報	○	○	○	○
110	cat /standby/var/log/ssh.log	待機系の SSH ログ情報	○	○	×	×

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
111	/usr/local/diag/mqlib_trace -w 0	使用しているメッセージキュー情報一覧	○	×	○	×
112	/usr/local/diag/genbintrns -s	変更リスト，コンフィグレーションアクセス状況情報	○	○	○	○
113	cat /var/log/flowctl/flowctld.log	フィルタ・QoS フロー制御プログラムのログ情報	○	×	○	×
114	cat /standby/var/log/flowctl/flowctld.log	待機系のフィルタ・QoS フロー制御プログラムのログ情報	○	×	×	×
115	access-log tool tech	フローログ制御プログラムの内部情報	○	○	○	○
116	/usr/local/diag/padctrl -l tech	pad, PA の show tech 用 diag コマンド情報	×	○	×	○
117	/usr/local/diag/padctrl -l techd	pad，PA の show tech detail 用 diag コマンド情報	○	×	○	×
118	/usr/local/diag/bpifc tech	装置内制御データの配布情報	○	○	○	○
119	/usr/local/diag/iswdiag	ISW デバイス情報	○	○	○	○
120	/usr/local/diag/showdev -s	デバイス詳細状態	○	○	○	○
121	/usr/local/diag/qosdiag quectl tech	キュー制御プログラムの内部情報	○	○	○	○
122	/usr/local/diag/qosdiag queinfo tech	キュー統計制御プログラムの内部情報	○	○	○	○
123	/usr/local/diag/ppuapinfo rctl all tech	RCTL 制御の詳細情報	○	○	×	×
124	/usr/local/diag/ppuapinfo rctlcom all tech	RCTL 共通の詳細情報	○	○	×	×
125	/usr/local/diag/ppuapinfo rctlstat all tech	RCTL 統計の詳細情報	○	○	×	×
126	/usr/local/diag/cmddrvif show stat	運用コマンドによるハードウェア制御，情報取得に関する内部統計情報	○	×	○	×
127	/usr/local/diag/flowctl tech	フィルタ・QoS フロー制御プログラムの内部情報	○	×	○	×
128	/usr/local/diag/shaper tech	階層化シェーパ制御プログラムの内部情報	○	×	○	×
129	/usr/local/diag/qosdiag flowinfo tech	フィルタ・QoS フロー統計制御プログラムの内部情報	○	×	○	×

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
130	/usr/local/diag/dupctl tech	冗長化制御で管理している引き継ぎ状態の情報および統計情報	○	×	○	×
131	show port	ポートの情報	○	○	×	×
132	show port statistics	ポートの統計情報	○	○	×	×
133	show port transceiver debug	ポートのトランシーバ詳細情報	○	○	×	×
134	show port vlan	ポートの VLAN 情報	○	○	×	×
135	show interfaces nif XXX_NIF line XXX_LINE debug	ポートの詳細統計情報	○	○	×	×
136	show channel-group detail	リンクアグリゲーションの詳細情報	○	×	×	×
137	show channel-group statistics lacp	リンクアグリゲーションの LACPDU 送受信統計情報	○	×	×	×
138	show axrp detail	Ring Protocol の詳細情報	○	×	×	×
139	show loop-detection statistics	L2 ループ検知の統計情報	○	×	×	×
140	show loop-detection logging	L2 ループ検知のログ情報	○	×	×	×
141	show spanning-tree statistics	スパニングツリーの BPDU 送受信統計情報	○	×	×	×
142	show spanning-tree detail	スパニングツリーの詳細情報表示	○	×	×	×
143	show efmoam detail	IEEE802.3ah OAM, UDLD およびループ検出機能の設定情報ならびにポートの状態	○	×	×	×
144	show efmoam statistics	IEEE802.3ah OAM, UDLD およびループ検出機能の統計情報	○	×	×	×
145	show lldp detail	LLDP の設定情報および隣接装置情報	○	×	×	×
146	show lldp statistics	LLDP の統計情報	○	×	×	×
147	show cfm detail	本装置の CFM の詳細情報および障害検出情報	○	×	×	×
148	show igmp-snooping	IGMP snooping の VLAN 情報	○	×	○	×
149	show igmp-snooping group	IGMP snooping の学習情報	○	×	○	×
150	show igmp-snooping statistics	IGMP snooping の統計情報（1 回目）	○	×	○	×
151	show mld-snooping	MLD snooping の VLAN 情報	○	×	○	×

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
152	show mld-snooping group	MLD snooping の学習情報	○	×	○	×
153	show mld-snooping statistics	MLD snooping の統計情報（1 回目）	○	×	○	×
154	show vlan list	本装置の VLAN の情報	×	○	×	×
155	show vlan summary	本装置の VLAN のサマリー情報	○	○	×	×
156	show vlan detail	本装置の VLAN の詳細情報	○	×	×	×
157	show vrrpstatus detail statistics	VRRP の仮想ルータの状態および統計情報	○	×	×	×
158	show vrrpstatus group	VRRP の仮想ルータのグループ化情報	○	×	×	×
159	show sflow detail	sFlow 統計についてのコンフィグレーション設定状態および動作状況	○	×	×	×
160	show snmp	SNMP 情報	○	×	×	×
161	/usr/local/diag/snmp_dp -mem	SNMP 機能のメモリカウンタ	○	×	×	×
162	/usr/local/diag/snmp_dp -resource	SNMP 機能のリソースカウンタ	○	×	×	×
163	show environment temperature-logging	本装置の温度履歴情報	○	○	×	×
164	show running-config	運用面のコンフィグレーション	○	○	○	○
165	show qos queueing	装置内のキュー情報	○	○	○	○
166	show qos queueing tech-support	装置内制御キューの情報	○	○	○	○
167	show ip cache policy	IPv4 ポリシーベースルーティングのポリシーベースルーティングリストの送信先経路情報および状態	○	×	×	×
168	show ipv6 cache policy	IPv6 ポリシーベースルーティングのポリシーベースルーティングリストの送信先経路情報および状態	○	×	×	×
169	show track detail	トラックの詳細情報	○	×	○	×
170	/usr/local/bin/track -t |tail -n 1024	トラックプログラムのトレース情報	○	×	○	×
171	show bfd session detail	BFD セッション情報	○	×	×	×
172	show processes memory unicast	ユニキャストルーティングプログラムでのメモリの確保状況および使用状況	○	×	○	×

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
173	show processes cpu minutes unicast	ユニキャストルーティングプログラムの CPU 使用率	○	×	○	×
174	show graceful-restart unicast	ユニキャストルーティングプロトコルのグレースフル・リスタートのリスタートルータの動作状態	○	×	×	×
175	show ip interface ipv4-unicast	ユニキャストルーティングプログラムが認識している本装置のインタフェース情報	○	×	○	×
176	show ip route vrf all summary	各 VRF のルーティングプロトコルが保有するアクティブ経路数と非アクティブ経路数	○	×	○	×
177	show ip vrf all	各 VRF の学習経路数	○	×	×	×
178	/usr/local/diag/rtdist -m	ユニキャスト経路配布の管理情報	○	×	○	×
179	/usr/local/diag/rtdist -t	ユニキャスト経路配布の統計情報	○	×	○	×
180	/usr/local/diag/rtdist -d	ユニキャスト経路配布の状態通知メモリ情報	○	×	○	×
181	show ip dhcp relay statistics	DHCP/BOOTP リレーエージェント統計情報	○	×	×	×
182	show ip rip vrf all statistics	各 VRF の RIP の統計情報	○	×	○	×
183	show ip rip vrf all advertised-routes summary	各 VRF の RIP で広告した経路数	○	×	×	×
184	/usr/local/diag/ppuapinfo uni all tech	ユニキャストドライバの制御管理情報 （IPv4/IPv6 ユニキャスト経路，ARP，NDP 関連情報）	○	×	×	×
185	show ip rip vrf all received-routes summary	各 VRF の RIP で学習した経路数	○	×	×	×
186	/usr/local/diag/ppuapinfo mlt all tech	マルチキャストドライバの制御管理情報 （IPv4/IPv6 マルチキャスト経路関連情報）	○	×	×	×
187	show ip ospf discard-packets	OSPF で廃棄されたパケット情報	○	×	○	×
188	show ip ospf vrf all statistics	各 VRF の OSPF で収集されている送受信パケットの統計情報	○	×	○	×
189	show ip ospf vrf all neighbor detail	各 VRF の OSPF の隣接ルータの詳細情報	○	×	○	×

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
190	show ip ospf vrf all virtual-links detail	各 VRF の OSPF の仮想リンク情報の詳細情報	○	×	○	×
191	show ip ospf vrf all database database-summary	各 VRF の OSPF の LS タイプごとの LSA 数	○	×	×	×
192	show ip ospf vrf all	各 VRF の OSPF のグローバル情報	○	×	×	×
193	show ip ospf nsr	OSPF のノンストップルーティング同期情報	○	×	×	×
194	show ip bgp vpnv4 vrf all neighbors detail	各 VRF の BGP4 のピアリング情報	○	×	○	×
195	show ip bgp vpnv4 vrf all nsr	各 VRF の BGP4 のノンストップルーティング同期情報	○	×	×	×
196	show ip bgp vpnv4 vrf all received-routes summary	各 VRF の BGP4 のピアから受信した経路情報数	○	×	○	×
197	show ip bgp vpnv4 vrf all advertised-routes summary	各 VRF の BGP4 のピアへ広告した経路情報数	○	×	×	×
198	show ip bgp vpnv4 vrf all notification-factor	各 VRF の BGP4 のコネクションを切断する要因となったメッセージ	○	×	○	×
199	show ipv6 interface ipv6-unicast	ユニキャストルーティングプログラムが認識している本装置のインタフェース情報	○	×	○	×
200	show ipv6 route vrf all summary	各 VRF のユニキャストルーティングプログラムが保有するアクティブ経路数と非アクティブ経路数	○	×	○	×
201	show ipv6 vrf all	各 VRF の学習経路数	○	×	×	×
202	show ipv6 dhcp relay statistics	DHCPv6 リレーエージェント統計情報	○	×	×	×
203	show ipv6 rip vrf all advertised-routes summary	各 VRF の RIPng で広告した経路数	○	×	×	×
204	show ipv6 rip vrf all received-routes summary	各 VRF の RIPng で学習した経路数	○	×	×	×
205	show ipv6 rip vrf all statistics	各 VRF の RIPng の統計情報	○	×	○	×
206	show ipv6 ospf discard-packets	OSPFv3 で廃棄されたパケットの情報	○	×	○	×
207	show ipv6 ospf vrf all statistics	各 VRF の OSPFv3 で収集したパケットの統計情報	○	×	○	×

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
208	show ipv6 ospf vrf all neighbor detail	各 VRF の OSPFv3 の隣接ルータの状態	○	×	○	×
209	show ipv6 ospf vrf all virtual-links detail	各 VRF の OSPFv3 の仮想リンク情報	○	×	○	×
210	show ipv6 ospf vrf all database database-summary	OSPFv3 の LS-Database の数	○	×	×	×
211	show ipv6 ospf vrf all	各 VRF の OSPFv3 のグローバル情報	○	×	×	×
212	show ipv6 ospf nsr	OSPFv3 のノンストップルーティング同期情報	○	×	×	×
213	show ipv6 bgp vpnv6 vrf all neighbors detail	各 VRF の BGP4+のピアリング情報	○	×	○	×
214	show ipv6 bgp vpnv6 vrf all nsr	各 VRF の BGP4+のノンストップルーティング同期情報	○	×	×	×
215	show ipv6 bgp vpnv6 vrf all received-routes summary	各 VRF の BGP4+のピアから受信した経路情報数	○	×	○	×
216	show ipv6 bgp vpnv6 vrf all advertised-routes summary	各 VRF の BGP4+のピアへ広告した経路情報数	○	×	×	×
217	show ipv6 bgp vpnv6 vrf all notification-factor	各 VRF の BGP4+のコネクションを切断する要因となったパケット	○	×	○	×
218	show netstat multicast numeric	BCU OS マルチキャスト統計	○	×	○	×
219	show ip multicast vrf all statistics	IPv4 マルチキャスト統計情報（1 回目）	○	×	○	×
220	show ipv6 multicast vrf all statistics	IPv6 マルチキャスト統計情報（1 回目）	○	×	○	×
221	show ip multicast vrf all resources	IPv4 マルチキャストルーティング機能で使用している各種エントリ情報	○	×	○	×
222	show ip igmp vrf all interface detail	IGMP のインタフェース情報	○	×	○	×
223	show ip igmp vrf all group	IGMP のマルチキャストグループ情報	○	×	○	×
224	show ip pim vrf all interface detail	IPv4 PIM のインタフェース情報	○	×	○	×
225	show ip pim vrf all neighbor detail	IPv4 マルチキャストインタフェースの隣接情報	○	×	○	×

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
226	show ip pim vrf all bsr	IPv4 PIM-SM ブートストラップルータ情報	○	×	○	×
227	show ip pim vrf all rp-mapping	IPv4 PIM-SM ランデブーポイント情報	○	×	○	×
228	show ip mroute vrf all	IPv4 マルチキャスト経路情報	○	×	○	×
229	show ip mcache vrf all	IPv4 マルチキャスト中継エントリ情報	○	×	○	×
230	show ipv6 multicast vrf all resources	IPv6 マルチキャストルーティング機能で使用している各種エントリ情報	○	×	○	×
231	show ipv6 mld vrf all interface	MLD のインタフェース情報	○	×	○	×
232	show ipv6 mld vrf all group	MLD のマルチキャストグループ情報	○	×	○	×
233	show ipv6 mld vrf all group explicit	MLD のホストトラッキング機能で管理する受信者情報	○	×	○	×
234	show ipv6 pim vrf all interface detail	IPv6 PIM のインタフェース情報	○	×	○	×
235	show ipv6 pim vrf all neighbor detail	IPv6 マルチキャストインタフェースの隣接情報	○	×	○	×
236	show ipv6 pim vrf all bsr	IPv6 PIM-SM ブートストラップルータ情報	○	×	○	×
237	show ipv6 pim vrf all rp-mapping	IPv6 PIM-SM ランデブーポイント情報	○	×	○	×
238	show ipv6 mroute vrf all	IPv6 マルチキャスト経路情報	○	×	○	×
239	show ipv6 mcache vrf all	IPv6 マルチキャスト中継エントリ情報	○	×	○	×
240	show ipv6 mld vrf all access-group detail	IPv6 マルチキャストチャネルフィルタの統計情報	○	×	○	×
241	show ipv6 mld vrf all bandwidth interface detail	IPv6 マルチキャスト帯域管理情報	○	×	○	×
242	show ip multicast vrf all statistics	IPv4 マルチキャスト統計情報（2 回目）	○	×	○	×
243	show ipv6 multicast vrf all statistics	IPv6 マルチキャスト統計情報（2 回目）	○	×	○	×

項番	コマンド（表示）	内容	運用系実行時		待機系実行時	
			パラメータ指定なし	basic	パラメータ指定なし	basic
244	show igmp-snooping statistics	IGMP snooping の統計情報（2 回目）	○	×	○	×
245	show mld-snooping statistics	MLD snooping の統計情報（2 回目）	○	×	○	×
246	show qos queueing tech-support	装置内制御キューの情報（2 回目）	○	○	○	○
247	show qos queueing	装置内のキュー情報（2 回目）	○	○	○	○
248	show event manager monitor script detail	スクリプトから登録した監視中のイベント情報	○	×	×	×
249	show event manager monitor applet detail	アプレット機能で監視中のイベント情報	○	×	×	×
250	show event manager history script	スクリプトから監視登録したイベント発生履歴	○	×	○	×
251	show event manager history applet	アプレット機能で監視中のイベント発生履歴	○	×	○	×
252	show script installed-file	インストールしたスクリプトファイル一覧	○	×	○	×
253	show script running-state	高機能スクリプトの動作状況	○	×	×	×
254	/usr/local/diag/hfcdiag tech	ハード機能制御情報	○	○	○	○

（凡例）　○：表示対象　×：非表示対象

索引

数字

A

B

D

F

I

L

M

N

O

P

Q

R

S

ね

は

ふ

ほ

ま

み

ゆ

り

ろ