IP8800/S2200・IP8800/S2100・IP8800/SS1250・IP8800/SS1240

トラブルシューティングガイド

IP8800SS1240-T001-D0

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。

■対象製品

このマニュアルは IP8800/S2200，IP8800/S2100，IP8800/SS1250，および IP8800/SS1240 モデル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

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。
Internet Explorer は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
IPX は，Novell,Inc. の商標です。
MagicPacket は，Advanced Micro Devices,Inc. の登録商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
RSA，SecurID については RSA Security Inc. の米国およびその他の国における商標もしくは登録商標です。
Wake on LAN は，IBM Corp. の登録商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
イーサネットは，富士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。

■発行

２０２０年　６月　（第１４版）　IP8800SS1240-T001-D0

■著作権

変更履歴

【第 14 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
3.1　ログインのトラブル	• [CTRL ＋ N] キー操作説明を変更しました。
3.2.1　コンソールからの入力，表示がうまくできない	• ログインできない場合，装置管理者モードへの変更できない場合の対処について記述を追加しました。【S2100】
3.2.2　リモート運用端末からログインできない	• ログインできない場合，装置管理者モードへの変更できない場合の対処について記述を追加しました。【S2100】
3.2.3　RADIUS を利用したログイン認証ができない	• ログインできない場合，装置管理者モードへの変更できない場合の対処について記述を追加しました。【S2100】

なお，単なる誤字・脱字などはお断りなく訂正しました。

【第 13 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
Ring Protocol 機能使用時の障害	• IP8800/S2100 に対応しました。
Web 認証使用時の通信障害	• IP8800/S2100 に対応しました。

【第 12 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
コマンドを入力できない	• 対応内容を変更しました。

【第 11 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
シリーズの追加	• IP8800/S2100 の記述を追加しました。
運用コマンド restore で復元できない	• IP8800/S2100 の記述を追加しました。
PoE 使用時の障害対応【S2200】【S2100】【SS1240】	• IP8800/S2100 の記述を追加しました。
セキュリティ機能の通信障害	• DHCP snooping 機能使用時の障害を移動しました。
付録 A　show tech-support コマンド表示内容詳細	• 表示内容詳細の記述を訂正しました。

【第 10 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
安全にお取り扱いいただくために	• 本章を削除しました。

【第 9 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
運用コマンド ppupdate でアップデートできない	• 旧バージョン間のアップデート失敗時の対処について記述を変更しました。【SS1240】
運用コマンド restore で復元できない	• 旧バージョンのソフトウェアを含むバックアップファイルでリストア失敗時の対処について記述を変更しました。【SS1240】

【第 8 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
シリーズの追加	• IP8800/S2200 の記述を追加しました。
運用コマンド ppupdate でアップデートできない	• Ver.2.4 より前のソフトウェアでアップデート失敗時の対処について記述を変更しました。【SS1240】
運用コマンド restore で復元できない	• Ver.2.4 より前のソフトウェアを含むバックアップファイルでリストア失敗時の対処について記述を変更しました。【SS1240】
PoE 使用時の障害対応【S2200】【SS1240】	• IP8800/S2200 の記述を追加しました。

【第 7 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
Ring Protocol 機能使用時の障害	• 多重障害監視機能を適用する場合の記述を追加しました。

【第 6 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
運用コマンド ppupdate でアップデートできない	• Ver.2.3.A より前のソフトウェアでアップデート失敗時の対処を追加しました。【SS1240】
運用コマンド restore で復元できない	• Ver.2.3.A より前のソフトウェアを含むバックアップファイルでリストア失敗時の対処を追加しました。【SS1240】

【第 5 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
NTP の通信障害	• タイムゾーンを確認する記述を変更しました。
温度監視対応時の障害	• 本項を追加しました。
付録 A　show tech-support コマンド表示内容詳細	• 本章を追加しました。

【第 4 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
シリーズの追加	• IP8800/SS1250 の記述を追加しました。
100BASE-FX【SS1250】/1000BASE-X のトラブル発生時の対応	• 100BASE-FX の記述を追加しました。

【第 3 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
ログインのトラブル	• 対応内容を修正しました。
Ring Protocol 機能使用時の障害	• 本項を追加しました。

【第 2 版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
装置および装置一部障害解析概要	• LED 説明を一部変更しました。
運用コマンド restore で復元できない	• 対応内容を修正しました。
IEEE802.1X 使用時の通信障害	• 対応内容を修正しました。
Web 認証使用時の通信障害	• 対応内容を修正しました。
MAC 認証使用時の通信障害	• 対応内容を修正しました。
セキュア Wake on LAN 使用時の通信障害【OP-WOL】	• 対応内容を修正しました。
アップリンク・リダンダント使用時の通信障害	• 解析項目を追加しました。 • 対応内容を修正しました。
省電力機能の障害	• 本項を追加しました。

はじめに

■対象製品およびソフトウェアバージョン

このマニュアルは次に示すモデル，ソフトウェアでサポートする機能を対象に記載しています。

- IP8800/S2200：Ver.2.10　OS-LT4，オプションライセンス
- IP8800/S2100：Ver.2.14　OS-LT5　（オプションライセンス未サポート）
- IP8800/SS1250：Ver.2.8　OS-LT3，オプションライセンス
- IP8800/SS1240：Ver.2.8　OS-LT2，オプションライセンス

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

なお，このマニュアルでは特に断らないかぎり IP8800/S2200，IP8800/S2100，IP8800/SS1250，IP8800/SS1240 に共通の機能について記載しますが，機種固有の機能については以下のマークで示します。

【S2200】：

IP8800/S2200 についての記述です。

【S2100】：

IP8800/S2100 についての記述です。

【SS1250】：

IP8800/SS1250 についての記述です。

【SS1240】：

IP8800/SS1240 についての記述です。

また，このマニュアルでは特に断らないかぎり OS-LT5，OS-LT4，OS-LT3，OS-LT2 の機能について記載しますが，オプションライセンスの機能については以下のマークで示します。

【OP-WOL】：

オプションライセンス OP-WOL でサポートする機能です。

【OP-OTP】：

オプションライセンス OP-OTP でサポートする機能です。

■このマニュアルの訂正について

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

■対象読者

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

また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

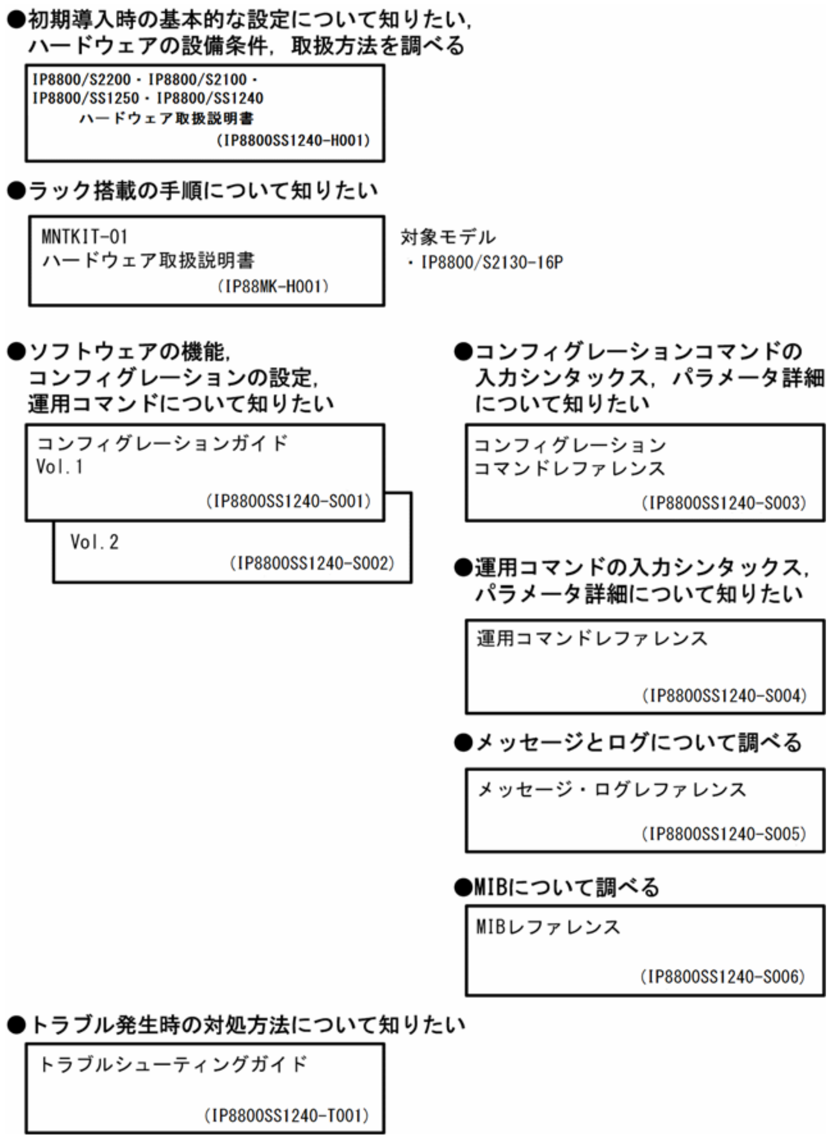
■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しておりますので，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。



■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second　　*bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol

CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
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
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance

MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second　　*ppsと表記する場合もあります。
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PoE	Power over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
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
ULR	Uplink Redundant
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VAA	VLAN Access Agent

VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■ kB(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 1,024 バイト，$1,024^2$ バイト，$1,024^3$ バイト，$1,024^4$ バイトです。

目次

1 概要

この章では，障害解析の概要について説明します。

1.1 障害解析概要

このマニュアルは，IP8800/S2200，IP8800/S2100，IP8800/SS1250，および IP8800/SS1240 の装置に問題がある場合に利用してください。

装置を目視で直接確認する場合は「1.2　装置および装置一部障害解析概要」に沿って解析を進めてください。

装置にログインして確認する場合は「1.3　機能障害解析概要」に沿って解析を進めてください。

1.2　装置および装置一部障害解析概要

運用中に障害が発生し，装置を目視で直接確認できる場合は，「2.1　装置障害の対応手順」の対策内容に従ってトラブルシュートしてください。

装置の LED については，次の図および「表 1-1　LED の表示，スイッチ，コネクタ」に IP8800/SS1240-24T2C の例を示すので参考にしてください。

図 1-1　正面パネルレイアウト

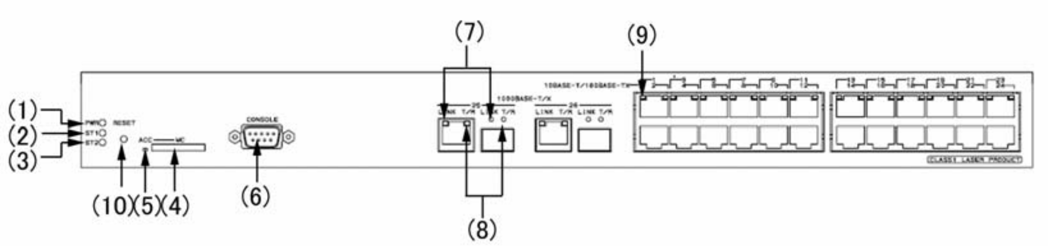


表 1-1　LED の表示，スイッチ，コネクタ

番号	名称	種類	機能	内容
1	PWR	LED：緑	電源の投入状態を示します	緑点灯：電源 ON 長い間隔の緑点滅：装置スリープ中 消灯　：電源 OFF，または電源異常
2	ST1	LED：緑 / 橙 / 赤	装置の状態を示します	緑点灯：動作可能 緑点滅：準備中（立上げ中） 長い間隔の緑点滅：LED 動作の消灯設定時 橙点灯：電源投入時の初期状態 赤点滅：装置の部分障害発生 赤点灯：装置の致命的障害発生（継続使用不可） 消灯　：電源 OFF，または電源異常
3	ST2	LED：橙	（未使用）	橙点灯：電源投入時の初期状態 消灯　：起動完了後は未使用のため消灯
4	MC	コネクタ	メモリカードスロット	メモリカードスロット
5	ACC	LED：緑	メモリカードの状態を示します	点灯　：メモリカードアクセス中（メモリカード取り外し禁止） 消灯　：メモリカードアイドル中（メモリカード取り付け，取り外し可能）
6	CONSOLE	コネクタ	CONSOLE ポート	コンソール端末接続用 RS-232C ポート
7	LINK	LED：緑	1000BASE-T/1000BASE-X のイーサネットポートの動作状態を示します	緑点灯：電源投入時の初期状態，またはリンク確立 消灯　：ST1 LED が緑点灯の場合，リンク障害，または閉塞
8	T/R	LED：緑		緑点滅：フレーム送受信中
9	1-24	LED：緑 / 橙	10BASE-T/100BASE-TX イーサネットポートの動作状態を示します	緑点灯：リンク確立 緑点滅：リンク確立およびフレーム送受信中 橙点灯：電源投入時の初期状態 消灯　：ST1 LED が緑点灯の場合，リンク障害，または閉塞
10	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	装置を再起動します スイッチを正面の LED が全点灯するまで（3 秒以上）長押しすると，装置スリープ状態を解除します

図 1-1，表 1-1 は代表的な装置を例示しています。各装置について詳細を知りたい場合には「ハードウェア取扱説明書」を参照してください。

1.3　機能障害解析概要

本装置の機能障害解析概要を次の表に示します。

表 1-2　機能障害の状況と参照箇所

大項目	中項目	参照箇所
ログインパスワードを忘れた	ログインユーザのパスワード忘れ	3.1.1　ログインのパスワードを忘れてしまった
	ログインユーザのユーザ ID 忘れ	3.1.2　ログインのユーザ ID を忘れてしまった
	装置管理者パスワード忘れ	3.1.3　装置管理者モードのパスワードを忘れてしまった
運用端末のトラブル	コンソール入力・表示不可	3.2.1　コンソールからの入力，表示がうまくできない
	リモートログインできない	3.2.2　リモート運用端末からログインできない
	ログイン認証ができない	3.2.3　RADIUS を利用したログイン認証ができない
	コマンドを入力できない	3.2.4　コマンドを入力できない
ファイル保存のトラブル	スタートアップコンフィグレーションファイルにコピーできない	3.3.1　スタートアップコンフィグレーションファイルに保存できない
	MC にコピーできない	3.3.2　MC にコピーできない，または書き込みできない
	RAMDISK にコピーできない	3.3.3　RAMDISK にコピーできない，または書き込みできない
	運用コマンド ppupdate でアップデートできない	3.3.4　運用コマンド ppupdate でアップデートできない
	運用コマンド restore で復元できない	3.3.5　運用コマンド restore で復元できない
	バインディングデータベースを保存または復元できない	3.3.6　バインディングデータベースを保存または復元できない
ネットワークインタフェースの通信障害	イーサネットポートの通信障害	3.4.1　イーサネットポートの接続ができない
	10BASE-T/100BASE-TX の通信障害	3.4.2　10BASE-T/100BASE-TX のトラブル発生時の対応【SS1250】【SS1240】
	10BASE-T/100BASE-TX/1000BASE-T の通信障害	3.4.3　10BASE-T/100BASE-TX/1000BASE-T のトラブル発生時の対応
	100BASE-FX【SS1250】/1000BASE-X の通信障害	3.4.4　100BASE-FX【SS1250】/1000BASE-X のトラブル発生時の対応
	PoE での障害【S2200】【S2100】【SS1240】	3.4.5　PoE 使用時の障害対応【S2200】【S2100】【SS1240】
	リンクアグリゲーションでの障害	3.4.6　リンクアグリゲーション使用時の通信障害
レイヤ 2 ネットワークの通信障害	VLAN 障害	3.5.1　VLAN によるレイヤ 2 通信ができない
	スパニングツリー障害	3.5.2　スパニングツリー機能使用時の障害
	Ring Protocol 障害	3.5.3　Ring Protocol 機能使用時の障害
	IGMP snooping 障害	3.5.4　IGMP snooping によるマルチキャスト中継ができない
	MLD snooping 障害	3.5.5　MLD snooping によるマルチキャスト中継ができない
IPv4 ネットワークの通信障害	通信ができない	3.6.1　通信できない，または切断されている

大項目	中項目	参照箇所
レイヤ 2 認証の通信障害	－	3.7.1　IEEE802.1X 使用時の通信障害
	－	3.7.2　Web 認証使用時の通信障害
	－	3.7.3　MAC 認証使用時の通信障害
	－	3.7.4　セキュア Wake on LAN 使用時の通信障害【OP-WOL】
セキュリティ機能の通信障害	DHCP snooping 障害	3.8.1　DHCP snooping 機能使用時の障害
冗長構成による高信頼化機能の通信障害	アップリンク・リダンダントの障害	3.9.1　アップリンク・リダンダント使用時の通信障害
SNMP の通信障害	MIB が取得できない	3.10.1　SNMP マネージャから MIB の取得ができない
	トラップ受信不可	3.10.2　SNMP マネージャでトラップが受信できない
LLDP 機能で隣接装置情報を取得できない	－	3.11.1　LLDP 機能により隣接装置情報が取得できない
NTP の通信障害	－	3.12　NTP の通信障害
IEEE802.3ah/UDLD 機能使用時の通信障害	ポートが inactive 状態になる	3.13.1　IEEE802.3ah/UDLD 機能でポートが inactive 状態となる
パケット廃棄による通信障害	－	3.14.1　フィルタ・QoS 設定情報の確認
ポートミラーリングの障害	－	3.15　ポートミラーリングの障害
省電力機能の障害	－	3.16.1　LED 輝度が動作しない
	－	3.16.2　省電力機能スケジューリングが動作しない
温度監視対応時の障害	－	3.17.1　温度履歴情報の日付が正しく表示されない
その他	－	コンフィグレーションガイドによって，再度設定を確認してください

2 装置障害におけるトラブルシュート

この章では，装置に障害が発生した場合の対処方法を説明します。

2.1 装置障害の対応手順

装置に障害が発生した場合には，以下の手順で対応します。

表 2-1 装置障害のトラブルシュート

項番	障害内容	対策内容
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	ただちに次の手順を実行してください。 1. 装置の電源を OFF する。 2. 装置の電源ケーブルを抜く。 3. 装置を交換する。
2	login プロンプトが表示されない	1. MC が挿入されている場合は，MC を抜いた上で装置の電源を OFF にし，再度 ON にして装置を再起動します。 2. MC が挿入されていない場合は，装置の電源を OFF にし，再度 ON にして装置を再起動します。 3. 装置を再起動させても問題が解決しない場合は，装置を交換します。
3	装置の PWR LED が消灯している	「(1) 装置停止および PWR LED 消灯時の対応」を参照して障害を切り分けてください。
4	装置の ST1 LED が赤点灯している	装置に障害が発生した可能性があります。 後述「4 障害情報取得方法」を参照して，運用コマンド show tech-support で装置情報を採取してください。 装置情報を採取後，装置を再起動して異常がないかを確認します。 1. 装置の電源を OFF にし，再度 ON にして装置を再起動してください。 2. 装置を再起動できた場合は，運用コマンド show critical-logging を実行して障害情報を確認します。 `>show critical-logging` 3. 採取した障害情報に「高温注意」のメッセージが存在する場合は，動作環境が原因と考えられるため，システム管理者に環境の改善を依頼してください（「メッセージ・ログレファレンス」参照)。それ以外の場合は，装置を交換してください。
5	装置の ST1 LED が赤点滅している	「(2) ST1 LED 赤点滅および LINK LED 消灯時の対応」を参照して障害を切り分けてください。
6	装置の ST1 LED が橙点灯している	電源投入後の初期状態です。しばらくお待ちください。
7	装置の各ポートの LINK LED(1000BASE-T/1000BASE-X ポート）および 1-48 LED(10BASE-T/100BASE-TX ポート）が消灯している	「(2) ST1 LED 赤点滅および LINK LED 消灯時の対応」を参照して障害を切り分けてください。

(1) 装置停止および PWR LED 消灯時の対応

次の表に従って対応してください。

表 2-2 装置停止および PWR LED 消灯時のトラブルシュート

項番	障害内容	対策内容
1	装置の電源が OFF である（電源スイッチのない装置は対象外）	装置の電源を ON にしてください。

項番	障害内容	対策内容
2	電源ケーブルに抜けやゆるみがある	次の手順を実施してください。 1.　装置の電源を OFF にします。 2.　電源ケーブルを正しく挿入します。 3.　装置の電源を ON にします。
3	測定した入力電圧が下記の範囲外である AC100V の場合：AC90 ～ 127V AC200V の場合：AC180 ～ 254V 注　本件は入力電圧の測定が可能な場合だけ実施する	電源設備の障害（本装置の障害ではない）のため，設備担当者に対策を依頼してください。

（2） ST1 LED 赤点滅および LINK LED 消灯時の対応

次の表に従って対応してください。

表 2-3　ST1 LED 赤点滅および LINK LED 消灯時のトラブルシュート

項番	障害内容	対策内容
1	以下のように運用コマンド show logging を実行して，障害情報を確認可能な場合。 `>show logging`	障害情報に従い対策を実施してください（「メッセージ・ログ レファレンス」参照）。具体的には，以下の対策を実施してください。 1.　装置の交換 2.　トランシーバ（SFP）の交換 3.　コンフィグレーションの修正 4.　ソフトウェアの入れ換え 5.　ケーブルの接続の確認 6.　トランシーバ（SFP）の取り付けの確認 7.　その他
2	障害情報を確認できない場合	装置を交換してください。

3 運用中機能障害におけるトラブルシュート

本章では装置が正常に動作しない，または通信ができないといったトラブルが発生した場合の対処方法を説明します。

3.1 ログインのトラブル

3.1.1 ログインのパスワードを忘れてしまった

運用中，ログインのパスワードを忘れてしまい本装置にログインできない場合は，以下の手順で対応してください。

- 本装置を再起動し，コンソールに "login" が表示されるまで，[CTRL ＋ N] キーを同時に押下し続けてください。
  このとき，スタートアップコンフィグレーションファイルおよびパスワード情報は読み込まれません。
- 本装置起動後，運用コマンド password でパスワードを設定してください。
- 本装置を再起動してください。
  スタートアップコンフィグレーションファイルおよび設定したパスワード情報が読み込まれます。

3.1.2 ログインのユーザ ID を忘れてしまった

運用中，ログインのユーザ ID を忘れてしまい本装置にログインできない場合は，以下の手順で対応してください。

- 本装置を再起動し，コンソールに "login" が表示されるまで，[CTRL ＋ N] キーを同時に押下し続けてください。
  このとき，スタートアップコンフィグレーションファイルおよびログインユーザ ID 情報は読み込まれません。
- 本装置起動後は，ログインユーザ ID：operator でログインできます。
- ログイン後，運用コマンド rename user でログインユーザ ID を変更してください。
- 本装置を再起動してください。
  スタートアップコンフィグレーションファイルおよび変更したログインユーザ ID 情報が読み込まれます。

3.1.3 装置管理者モードのパスワードを忘れてしまった

運用中，装置管理者モードのパスワードを忘れてしまい装置管理者モードになれない場合は，以下の手順で対応してください。

- 本装置を再起動し，コンソールに "login" が表示されるまで，[CTRL ＋ N] キーを同時に押下し続けてください。
  このとき，スタートアップコンフィグレーションファイルおよびパスワード情報は読み込まれません。
- 本装置起動後，運用コマンド password で装置管理者用パスワードを設定してください。
- 本装置を再起動してください。
  スタートアップコンフィグレーションファイルおよび設定したパスワード情報が読み込まれます。

3.2 運用端末のトラブル

3.2.1 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 3-1 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 ST1 LED が緑点灯になっているかを確認してください。緑点灯していない場合は，「1.2 装置および装置一部障害解析概要」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. RS-232C クロスケーブルを用いていることを確認してください。 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以下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] をキー入力してください)。それでもキー入力ができない場合は 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] により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	ログイン時に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. 運用コマンド line console speed で CONSOLE(RS-232C) 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. 運用コマンド line console speed で CONSOLE(RS-232C) 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。
4	ユーザ ID 入力中に異常な文字が表示された。	CONSOLE(RS-232C) の通信速度を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。
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出ているか確認してください。出ていなければ，装置を起動中のため，しばらくお待ちください。 2. 「3.1 ログインのトラブル」の手順を実行してみてください。 上記の手順でもログインできない場合は，内蔵フラッシュメモリが壊れている可能性があります。運用コマンド format flash を実行してみてください。 3. コンフィグレーションコマンド aaa authentication login console【S2100】，および aaa authentication login で RADIUS 認証が設定されていないか確認してください。(詳細は「3.2.3 RADIUS 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，コマンド入力ができない。	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な表示はできません。通信ソフトウェアの通信速度を元に戻してください。

項番	障害内容	確認内容
7	Tera Term Pro を使用してログインしたいがログイン時に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。項番 3 を参照してください。［Alt］＋［B］でブレーク信号を発行します。なお，Tera Term Pro の通信速度により複数回ブレーク信号を発行しないとログイン画面が表示されないことがあります。
8	項目名と内容がずれて表示される。	1 行で表示可能な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（８０桁×２４行）に変更し，1 行で表示可能な文字数を多くしてください。
9	装置管理者モードへ変更できない。【S2100】	コンフィグレーションコマンド aaa authentication enable で RADIUS 認証が設定されていないか確認してください。(詳細は「3.2.3　RADIUS 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)。

3.2.2 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（telnet，FTP など）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 3-2　リモート運用端末との接続トラブルおよび対応

項番	現象	対処方法，または参照個所
1	リモート接続ができない。	次の手順で確認してください。 1. PC や WS から運用コマンド ping 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を確認してください。
2	ログインができない。	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 ，または ftp-server が設定されているかを確認してください（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. コンフィグレーションコマンド line vty モードのアクセスリストで許可された IP アドレスを持つ端末を使用しているかを確認してください。また，コンフィグレーションコマンドアクセスリストで設定した IP アドレスに deny を指定していないかを確認してください（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)。 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)。 4. ログイン操作が不完全な状態で放置している端末がないか確認してください。(不完全な状態：ユーザ ID，パスワードの入力待ち状態，ログイン失敗状態) 該当する端末がある場合は，その端末の通信ソフトウェアを終了させてください。 5. ログイン中にリモート運用端末から本装置への到達性が一時的に失われるような事象がなかったか確認してください。 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，その後に復旧している場合，本装置にセッション情報が残存するため，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，おおむね 10 分です。 6. コンフィグレーションコマンド aaa authentication login で，RADIUS 認証が設定されていないか確認してください（詳細は「3.2.3　RADIUS 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］をキー入力してください)。それでもキー入力できない場合は，項番 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］により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	現象	対処方法，または参照個所
4	ログインしたままの状態になっているユーザがある。	自動ログアウト（最大 30 分）するのを待ってください。また，コンフィグレーションを編集中の場合は，再度ログインしてコンフィグレーションモードになってから保存し，編集を終了してください。
5	装置管理者モードへ変更できない。【S2100】	コンフィグレーションコマンド aaa authentication enable で RADIUS 認証が設定されていないか確認してください。（詳細は「3.2.3　RADIUS 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）。

3.2.3 RADIUS を利用したログイン認証ができない

RADIUS を利用したログイン認証，装置管理者モードへの変更（enable コマンド）ができない場合，以下を確認してください。

(1) RADIUS サーバへの通信

運用コマンド ping で，本装置から RADIUS サーバに対して疎通ができているかを確認してください。疎通ができない場合は，「3.6.1　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 VLAN インタフェースに IP アドレスを設定している場合は，IP アドレスから運用コマンド ping で，本装置から RADIUS サーバに対して疎通ができているかを確認してください。

(2) 応答タイムアウト値および再送回数設定

RADIUS 認証の場合，コンフィグレーションコマンド radius-server host，radius-server retransmit，radius-server timeout の設定により，本装置が RADIUS サーバとの通信が不能と判断する時間は最大で＜設定した応答タイムアウト値 (秒) ＞×＜設定した再送回数＋１＞×＜設定した RADIUS サーバ数＞となります。

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可能性があります。この場合，RADIUS 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，運用ログに RADIUS 認証が成功したメッセージが出力されているにもかかわらず，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 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るため，稼働中の RADIUS サーバを優先するように設定するか，＜応答タイムアウト値 (秒) ＞×＜再送回数＞の値を小さくしてください。

(3) 本装置にログインまたは装置管理者モードへ変更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，aaa authentication enable によって，コンソールログインや装置管理者モードへの変更（enable コマンド）も RADIUS 認証の対象となっている場合は，以下の手順を実行してください。

1. 本装置を再起動し，コンソールに "login" が表示されるまで，[CTRL ＋ N] キーを同時に押下し続けてください。
   このとき，スタートアップコンフィグレーションファイルおよびログインユーザ情報は読み込まれません。
2. 本装置起動後は，ログインユーザ ID：operator でログインできます。
3. ログイン後，運用コマンド rename user でログインユーザ ID を変更し，運用コマンド password でパスワードを設定してください。
4. save コマンドを実行してください。

このとき，すべてのコンフィグレーション設定は消失した状態で保存されます。

5. 本装置を再起動してください。
   変更したログインユーザ ID 情報が読み込まれますので，変更したログインユーザ ID とパスワードでログインしてください。
   なお，スタートアップコンフィグレーションファイルは，すべてのコンフィグレーション設定が消失していますので，再度設定し直してください。

3.2.4　コマンドを入力できない

障害などにより装置が再起動した場合は，再起動して約 2 分後に自動で装置障害情報採取（auto-log）が開始されます※。採取中はコマンド入力ができない状態となる場合があります。しばらく経ってからご使用ください。

なお，運用コマンド reload 実行や装置の電源 OFF/ON では本現象は発生しません。

注※

再起動して自動で装置障害情報採取が開始される前に，装置へログインした場合，情報採取は行われません。運用コマンド show tech-support を実行して装置障害情報を採取してください。

3.3　ファイル保存のトラブル

3.3.1　スタートアップコンフィグレーションファイルに保存できない

運用コマンドでスタートアップコンフィグレーションファイルにコピーできないなどの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 3-3　スタートアップコンフィグレーションファイルへのコピーでのトラブルおよび対応

項番	確認内容・コマンド	確認内容
1	コマンドの応答メッセージを確認してください。	「Can’t execute.」を表示している場合は次の手順で確認してください。 1. 指定したファイルが存在しているか確認してください。 2. 指定したファイル名が間違っていないか確認してください。 3. 上記以外の場合は，項番 2 を参照してください。
2	運用コマンド format flash を実行してみてください。	次の手順で確認してください。 1. 運用コマンド format flash でファイルシステムをフォーマットしてみてください。「Flash format complete.」（フォーマット正常終了）を表示した場合は，再度コンフィグレーションを設定し，スタートアップコンフィグレーションファイルに保存してください。 2. 「Flash format complete.」以外を表示した場合，ファイルシステムが壊れている可能性があります。

3.3.2　MC にコピーできない，または書き込みできない

運用コマンドで，MC にコピーできないなどの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 3-4　MC へのコピーでのトラブルおよび対応

項番	確認内容・コマンド	確認内容
1	コマンドの応答メッセージを確認してください。	次の手順で確認してください。 1. 「MC is not inserted.」が表示された場合は，MC が挿入されていません。MC を挿入してください。 2. 「Can't access to MC by write protection.」が表示された場合は，MC が書き込み禁止状態になっています。MC をいったん外して，スイッチを「▼ Lock」状態と逆側に動かして書き込み禁止状態を解除してください。 3. 「No enough space on device.」が表示された場合は，書き込み先の MC に空き容量が不足しています。運用コマンド del で不要なファイルを削除してから，再度実行してください。 4. 「Can’t execute.」が表示された場合は，項番 2 を参照してください。
2	運用コマンド show ramdisk-file で RAMDISK のファイルを確認してください。	次の手順で確認してください。 1. 指定したファイルが存在しているか確認してください。 2. 指定したファイル名が間違っていないか確認してください。 3. 上記のいずれでもない場合は，項番 3 を参照してください。

項番	確認内容・コマンド	確認内容
3	運用コマンド format mc を実行してみてください。	次の手順で確認してください。 1. 何もメッセージが表示されず，プロンプトのみ表示された場合は，MC のフォーマットは正常終了しています。再度指定ファイルを MC に書き込んでみてください。 2. 「Can’t gain access to MC.」が表示された場合は，MC をいったん取り出し，MC および MC スロットにほこりなど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場合は，乾いた布でほこりを取ってから，再度 MC をスロットに挿入してください。挿入後，再度運用コマンド format mc を実行してください。 3. 「Can’t execute.」が表示された場合は，MC をいったん取り出し，MC および MC スロットにほこりなど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場合は，乾いた布でほこりを取ってから，再度 MC をスロットに挿入してください。挿入後，再度運用コマンド format mc を実行してください。同じメッセージが表示された場合は，MC が壊れている可能性があります。別の MC に交換してください。

3.3.3　RAMDISK にコピーできない，または書き込みできない

運用コマンドで RAMDISK にコピーできないなどの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 3-5　RAMDISK へのコピーでのトラブルおよび対応

項番	確認内容・コマンド	確認内容
1	コマンドの応答メッセージを確認してください。	次の手順で確認してください。 1. 指定したファイルが存在しているか確認してください。 2. 指定したファイル名が間違っていないか確認してください。 3. 「Not enough space on device.」が表示されている場合は，項番 2 を参照してください。
2	運用コマンド show ramdisk で RAMDISK の状態を確認してください。	次の手順で確認してください。 1. 運用コマンド show ramdisk の「free」（空き容量）で表示されるサイズは，十分余裕があるか確認してください。空き容量が少ない場合は，運用コマンド del で不要なファイルを削除してください。 2. コンフィグレーションファイルをコピーする場合は 1MB 以上の空き容量があるか確認してください。 3. 運用コマンド show critical-logging ramdisk でログファイルを RAMDISK に保存する場合は，約 300kB 以上の空き容量があるか確認してください。 4. 運用コマンド show tech-support ramdisk で装置情報を RAMDISK に保存する場合は，不要なファイルをすべて運用コマンド del で削除してください。 5. 上記以外の場合は，項番 3 を参照してください。
3	運用コマンド format flash を実行してみてください。	次の手順で確認してください。 1. 運用コマンド format flash でファイルシステムをフォーマットしてみてください。「Flash format complete.」（フォーマット正常終了）を表示した場合は，再度コンフィグレーションを設定し，スタートアップコンフィグレーションファイルに保存してください。 2. 「Flash format complete.」以外を表示した場合，ファイルシステムが壊れている可能性があります。

3.3.4 運用コマンド ppupdate でアップデートできない

運用コマンド ppupdate でアップデートできないなどの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 3-6 運用コマンド ppupdate でのトラブルおよび対応

項番	確認内容・コマンド	確認内容
1	コマンドの応答メッセージを確認してください。	1. 「Can't update software. [Hardware rev.x]」が表示された場合 **【SS1240】** 本メッセージが表示された場合は，特定のアップデート手順が必要です。詳細は「ソフトウェアアップデートガイド 3. 旧バージョン間のアップデート手順」を参照してください。 2. その他の応答メッセージを表示した場合 運用コマンド ppupdate で指定したアップデート用ファイルが対象装置のファイルか確認してください。 • アップデート用ファイルが，対象装置の装置モデルに対応していることを確認してください。 • アップデート用ファイルを確認後，運用コマンド ppupdate を再実行してみてください。 3. 上記以外の場合は項番 2 を参照してください。
2	運用コマンド show critical-logging を実行してみてください。	• 「FROM write fail [cnt=xxxxxxxx,size=xxxxxxxx,err=xxxxxxxx]」が採取されている場合 運用コマンド ppupdate を再実行してみてください。それでもエラーになる場合は，内蔵フラッシュメモリが壊れている可能性があります。装置を交換してください。

3.3.5 運用コマンド restore で復元できない

運用コマンド restore で復元できないなどの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。

(1) 復元先装置：IP8800/S2200,IP8800/S2100 シリーズで restore 実行時

表 3-7 運用コマンド restore でのトラブルおよび対応【S2200】【S2100】

項番	確認内容・コマンド	確認内容
1	コマンドの応答メッセージを確認してください。	「Restore operation failed.」が表示された場合 • 運用コマンド backup で「no-software」を指定したバックアップファイルは，運用コマンド restore でも「no-software」を指定してください。 • リストア対象の装置と同じモデル名称の装置で作成したバックアップファイルか確認してください。 • バックアップファイルを確認後，運用コマンド restore を再実行してみてください。 • それでもエラーになる場合は，バックアップファイルが壊れている可能性があります。 上記以外の場合は項番 2 を参照してください。
2	運用コマンド show critical-logging を実行してみてください。	• 「FROM write fail [cnt=xxxxxxxx,size=xxxxxxxx,err=xxxxxxxx]」が採取されている場合 運用コマンド restore を再実行してみてください。それでもエラーになる場合は，内蔵フラッシュメモリが壊れている可能性があります。装置を交換してください。

(2) 復元先装置：IP8800/SS1250 シリーズで restore 実行時

表 3-8 運用コマンド restore でのトラブルおよび対応【SS1250】

項番	確認内容・コマンド	確認内容
1	コマンドの応答メッセージを確認してください。	「Restore operation failed.」が表示された場合 • 運用コマンド backup で「no-software」を指定したバックアップファイルは，運用コマンド restore でも「no-software」を指定してください。 • バックアップファイルに IP8800/SS1240 または IP8800/SS1230 のソフトウェアを含んでいると，ソフトウェア以外の装置情報だけを復元します。 • 運用コマンド backup で「AX1230」オプションを指定したバックアップファイルは，ソフトウェア以外の装置情報で作成されています。IP8800/SS1250 のソフトウェアを含む場合は，オプション無でバックアップファイルを作成してください。 • バックアップファイルを確認後，運用コマンド restore を再実行してみてください。 • それでもエラーになる場合は，バックアップファイルが壊れている可能性があります。 上記以外の場合は項番 2 を参照してください。
2	運用コマンド show critical-logging を実行してみてください。	• 「FROM write fail [cnt=xxxxxxxx,size=xxxxxxxx,err=xxxxxxxx]」が採取されている場合 運用コマンド restore を再実行してみてください。それでもエラーになる場合は，内蔵フラッシュメモリが壊れている可能性があります。装置を交換してください。

(3) 復元先装置：IP8800/SS1240 シリーズで restore 実行時

表 3-9 運用コマンド restore でのトラブルおよび対応【SS1240】

項番	確認内容・コマンド	確認内容
1	コマンドの応答メッセージを確認してください。	「Restore operation failed.」が表示された場合 • 旧バージョンのソフトウェアを含むバックアップファイルでは，特定のアップデート手順が必要となる場合があります。 いったん復元先装置を Ver.2.4 以降のソフトウェアにアップデートしてください。その後，目的のバックアップファイルで，運用コマンド restore を再実行してください。詳細は「ソフトウェアアップデートガイド 3. 旧バージョン間のアップデート手順」を参照してください。 • 運用コマンド backup で「no-software」を指定したバックアップファイルは，運用コマンド restore でも「no-software」を指定してください。 • バックアップファイルに IP8800/SS1250 または IP8800/SS1230 のソフトウェアを含んでいると，ソフトウェア以外の装置情報だけを復元します。 • 運用コマンド backup で「AX1230」オプションを指定したバックアップファイルは，ソフトウェア以外の装置情報で作成されています。IP8800/SS1240 のソフトウェアを含む場合は，オプション無でバックアップファイルを作成してください。 • バックアップファイルを確認後，運用コマンド restore を再実行してみてください。 • それでもエラーになる場合は，バックアップファイルが壊れている可能性があります。 上記以外の場合は項番 2 を参照してください。
2	運用コマンド show critical-logging を実行してみてください。	• 「FROM write fail [cnt=xxxxxxxx,size=xxxxxxxx,err=xxxxxxxx]」が採取されている場合 運用コマンド restore を再実行してみてください。それでもエラーになる場合は，内蔵フラッシュメモリが壊れている可能性があります。装置を交換してください。

3.3.6 バインディングデータベースを保存または復元できない

DHCP snooping で使用する，バインディングデータベースを保存できない，または復元できない場合の対処については，「3.8.1 DHCP snooping 機能使用時の障害」を参照してください。

3.4 ネットワークインタフェースの通信障害

3.4.1 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，ポートの状態を以下に従って確認してください。

（1） ポートの状態確認

運用コマンド show port によりポート状態を確認してください。次の表にポート状態に対する対応を示します。

表 3-10 ポート状態の確認および対応

項番	確認内容・コマンド	対応
1	運用コマンド show port で該当ポートの状態を確認してください。	「dis」の場合，項番 2 へ。 「inact」の場合，項番 3 ～ 6 へ。 「down」の場合，項番 9 へ。
2	運用コマンド show running-config で該当ポートのコンフィグレーションを確認してください。	該当ポートに no shutdown が設定されているか確認してください。 shutdown 状態の場合は，該当ポートにケーブルが接続されていることを確認の上，コンフィグレーションで no shutdown を設定してください。
3	運用コマンド show spanning-tree で detail パラメータを指定し，該当ポートの BPDUguard 状態を確認してください。	該当ポートに「Down」および「PortFast : BPDUguard(BPDU received)」を表示している場合は，スパニングツリーの BPDU ガード機能を使用していて，該当ポートが BPDU 受信によりポートを閉塞しています。 対向装置の設定を見直し，本装置で BPDU を受信しない構成にしてください。項番 7 へ。
4	運用コマンド show logging でストームコントロールの運用ログを確認してください。	「STORM : Port<IF#> inactivated because of xxxx storm detection.」を採取している場合は，該当ポートでストームを検出し，ポートを閉塞しています。 運用コマンド show logging で，該当ポートのストームが回復したことを確認してから，項番 7 へ。
5	運用コマンド show efmoam で該当ポートの状態を確認してください。	「Forced Down」を表示している場合は，IEEE802.3ah/UDLD 機能で片方向リンク障害を検出し，ポートを閉塞しています。 「3.13 IEEE802.3ah/UDLD 機能の通信障害」を参照し，片方向リンク障害を解除後，項番 7 へ。
6	運用コマンド show loop-detection で該当ポートの状態を確認してください。	「Down(loop)」を表示している場合は，L2 ループ検知フレームを受信して，ポートを閉塞しています。 項番 7 へ。
7	運用コマンド activate を実行してみてください。	運用コマンド show spanning-tree で該当ポートが Up し，「PortFast : BPDUguard(BPDU not received)」を表示していることを確認してください。
		運用コマンド show logging で，該当ポートのストームが回復していることを確認してください。
		運用コマンド show efmoam で，該当ポートが「Forced Down」「Down」以外を表示していることを確認してください。
		運用コマンド show loop-detection で L2 ループ検知フレームによるポート閉塞が解除され，Up を表示していることを確認してください。

項番	確認内容・コマンド	対応
		上記の解除確認後，リンクアグリゲーションのスタンバイリンク機能を使用している場合は，項番 8 へ。
		使用していない場合は，項番 9 へ。
8	運用コマンド show channel-group で，リンクアグリゲーションのスタンバイリンク状態を確認してください。	「Mode : Static」，「Max Active Port : ポート数 (link-down mode)」で，該当ポートに「State : Detached」を表示している場合，スタンバイ状態です。（リンクダウンのポートが運用ポートで，スタンバイリンクのためにより待機用ポートに切り替わっています。） 「State : Distributing」表示となるまでお待ちください。
9	運用コマンド show logging により，当該ポートの運用ログを確認してください。	運用コマンド show logging により表示される当該回線のログより，「メッセージ・ログレファレンス」の該当個所を参照し，記載されている［対応］に従って対応してください。

3.4.2　10BASE-T/100BASE-TX のトラブル発生時の対応【SS1250】【SS1240】

10BASE-T/100BASE-TX でトラブルが発生した場合は，以下の順序で障害の切り分けを行ってください。

1. 運用ログ情報の確認
   運用ログ情報は「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の切り分けを行ってください。

表 3-11　10BASE-T/100BASE-TX のトラブル発生時の障害解析方法【SS1250】【SS1240】

項番	確認内容	原因	対応
1	運用コマンド show interfaces の障害統計情報により該当回線で以下の統計情報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。 ・ Link down	回線品質が低下しています。	ケーブル種別を確認してください。ケーブル種別は「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。ケーブル接続は「ハードウェア取扱説明書」を参照してください。
			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は，「ハードウェア取扱説明書」および「コンフィグレーションガイド」を参照してください。
2	運用コマンド show interfaces の受信系エラー統計情報により該当回線で以下の統計情報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。 ・ CRC errors ・ Symbol errors		ケーブル種別を確認してください。ケーブル種別は「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。ケーブル接続は「ハードウェア取扱説明書」を参照してください。
			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は，「ハードウェア取扱説明書」および「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	原因	対応
3	運用コマンド show interfaces により該当回線で回線種別 / 回線速度を確認してください。不正な回線種別 / 回線速度の場合，原因と対応欄を参照してください。	ケーブルが適合していません。	ケーブル種別を確認してください。ケーブル種別は「ハードウェア取扱説明書」を参照してください。
		コンフィグレーションコマンド speed と duplex が相手装置と不一致です。	コンフィグレーションコマンド speed と duplex を相手装置と合わせてください。

3.4.3 10BASE-T/100BASE-TX/1000BASE-T のトラブル発生時の対応

10BASE-T/100BASE-TX/1000BASE-T でトラブルが発生した場合は，以下の順序で障害の切り分けを行ってください。

1. 運用ログ情報の確認
   運用ログ情報は「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の切り分けを行ってください。

表 3-12 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	原因	対応
1	運用コマンド show interfaces の障害統計情報により該当回線で以下の統計情報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。 ・ Link down	回線品質が低下しています。	ケーブル種別を確認してください。ケーブル種別は「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。ケーブル接続は「ハードウェア取扱説明書」を参照してください。
			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は，「ハードウェア取扱説明書」および「コンフィグレーションガイド」を参照してください。
2	運用コマンド show interfaces の受信系エラー統計情報により該当回線で以下の統計情報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。 ・ CRC errors ・ Symbol errors		ケーブル種別を確認してください。ケーブル種別は「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。ケーブル接続は「ハードウェア取扱説明書」を参照してください。
			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は，「ハードウェア取扱説明書」および「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	原因	対応
3	運用コマンド show interfaces により該当回線で回線種別 / 回線速度を確認してください。不正な回線種別 / 回線速度の場合，原因と対応欄を参照してください。	ケーブルが適合していません。	ケーブル種別を確認してください。ケーブル種別は「ハードウェア取扱説明書」を参照してください。
		コンフィグレーションコマンド speed と duplex が相手装置と不一致です。	コンフィグレーションコマンド speed と duplex を相手装置と合わせてください。
4	運用コマンド show interfaces の障害統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされる場合，原因と対応欄を参照してください。 ・ Long frames	受信できるフレーム長を超えたパケットを受信しています。	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。

3.4.4 100BASE-FX【SS1250】/1000BASE-X のトラブル発生時の対応

100BASE-FX【SS1250】/1000BASE-X でトラブルが発生した場合は，以下の順序で障害の切り分けを行ってください。

1. 運用ログ情報の確認
   運用ログ情報は「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の切り分けを行ってください。

表 3-13 100BASE-FX【SS1250】/1000BASE-X のトラブル発生時の障害解析方法

項番	確認内容	原因	対応
1	運用コマンド show interfaces の障害統計情報により該当回線で以下の統計情報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。 ・ Link down	受信側の回線品質が低下しています。	光ファイバの種別を確認してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。
			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（半挿し状態になっていないかなど）確認してください。ケーブル接続は「ハードウェア取扱説明書」を参照してください。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，汚れを取り除いてください。
			トランシーバ (SFP) の接続が正しいか（半挿し状態になっていないかなど）確認してください。
			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。

項番	確認内容	原因	対応
2	運用コマンド show interfaces の受信系エラー統計情報により該当回線で以下の統計情報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。 ・ CRC errors ・ Symbol errors		光ファイバの種別を確認してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。
			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。ケーブル接続は「ハードウェア取扱説明書」を参照してください。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，汚れを拭き取ってください。
			トランシーバ (SFP) の接続が正しいか確認してください。
			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。
3	運用コマンド show interfaces の障害統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされる場合，原因と対応欄を参照してください。 ・ Long frames	受信できるフレーム長を超えたパケットを受信しています。	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。
4	1000BASE-SX2 を使用時，SFP 側に自動的に切り替わらない場合は，RJ45 ポートの使用状態と media-type 設定を確認してください。	自動メディア検出設定状態で，SFP と RJ45 を両方挿しています。	1000BASE-SX2 と RJ45 を使用している場合，自動メディア検出設定状態でも，1000BASE-X(SFP) 側がリンクアップしないため自動的に SFP に切り替わりません。 1000BASE-SX2 を使用する場合は，下記のいずれかで使用してください。 ・ コンフィグレーションコマンド media-type で固定メディアを設定（sfp または rj45 を指定） ・ 光ファイバケーブルと UTP（RJ45）ケーブルを同時に挿さない運用
5	【SS1250】 100BASE-FX を使用している場合，運用コマンド show interfaces のポート detail 情報によって該当ポートで回線種別 / 回線速度を確認してください。不正な回線種別 / 回線速度の場合，原因と対応欄を参照してください。	コンフィグレーションコマンド speed, duplex, media-type の設定が不正です。	コンフィグレーションコマンドで下記を設定してください。 ・ speed：100 ・ duplex：full ・ media-type：sfp

3.4.5　PoE 使用時の障害対応【S2200】【S2100】【SS1240】

PoE 使用時に電力供給できないなどが発生している場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-14　PoE 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	運用コマンド show power inline で該当ポートの Status 表示を確認してください。	• off 表示： 電力を供給していません。項番 2 へ。 • denied 表示： 装置全体の電力供給不足が発生しています。項番 3 へ。 • faulty 表示： 接続された装置に電力を供給できない状態になっています。項番 4 へ。 • inact 表示： 運用コマンドで電力の供給を停止しています。項番 5 へ。
2	該当ポートに shutdown が設定されているか確認してください。	• 設定済みの場合： no shutdown を設定してください。 • 未設定の場合： 受電装置が接続されているか確認してください。
3	運用コマンド show power inline で Threshold(W) と Total Allocate(W) を確認してください。	Total Allocate(W) の数値が Threshold(W) より大きいため供給できなくなっています。 装置全体の電力供給量，ポートの電力割り当て量，およびポートの消費電力を確認してコンフィグレーションで割り当て量を調整してください。
4	運用コマンド activate power inline を実行し，運用コマンド show power inline で該当ポートの Status 表示を確認してください。	• off 表示： 受電装置が接続されているか確認してください。 • on 表示： 継続してご使用ください。 • faulty 表示： 受電装置または接続ケーブルに問題がある可能性があります。項番 6 へ。
5	運用コマンド activate power inline を実行し，運用コマンド show power inline で該当ポートの Status 表示を確認してください。	• off 表示： 受電装置が接続されているか確認してください。 • on 表示： 継続してご使用ください。
6	運用コマンド show logging で「POE」ログが採取されているか確認してください。	• 「0/x Supplying power was stopped by the overload detection.」を表示した場合： オーバロードを検出したため，電力を供給できなくなっています。 受電装置または接続ケーブルを確認してみてください。回復しない場合は，ケーブル長・ケーブル種別を「ハードウェア取扱説明書」を確認して交換してみてください。 また，PoE 電力供給が可能な装置同士を接続している場合，コンフィグレーションコマンド power inline で当該ポートの PoE 機能を無効にしてください。
		• 「0/x Supplying power was stopped by the thermal shutdown.」を表示した場合： PoE コントローラの温度異常を検出し，電力の供給を停止しました。 受電装置または接続ケーブルを確認してみてください。

項番	確認内容・コマンド	対応
		• 「0/x Supplying power was stopped by the PD disorder (xxxx)」を表示した場合： (xxxx) 部分の表示を確認してください。 • MPS Absent： 受電装置または接続ケーブルに異常が発生している可能性があります。 • Startup Failure： 受電装置で異常が発生している可能性があります。 • Short： 本装置と受電装置の間に流れる電流が規定値を超えている可能性があります。 • Classification Failure：【S2200】 本装置と受電装置の間で Class 識別ができませんでした。 受電装置または接続ケーブルを確認してみてください。

3.4.6 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ができない，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の切り分けを行ってください。

表 3-15 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設定を運用コマンド show channel-group detail で確認してください。	リンクアグリゲーションのモードが相手装置のモードと同じ設定になっているか確認してください。相手装置とモードが異なる場合，相手装置と同じモードに合わせてください。
		リンクアグリゲーションのモードが一致している場合 • 各ポートの LACP 開始方法が両方とも passive になっていないか確認してください。両方とも passive になっていた場合，どちらか一方を active に変更してください。 • Actor 装置の Key が正しく設定されていることを確認してください。
2	通信障害となっているポートの運用状態を運用コマンド show channel-group detail で確認してください。	各ポートの状態（Status）を確認してください。リンクアグリゲーショングループ内の全ポートが Down の場合，リンクアグリゲーションのグループが Down します。
		• Detached Down，予備，速度不一致または半二重です。
		• Attached 過度状態，ネゴシエーション中です。
		• Collecting 過度状態，ネゴシエーション中（受信可能）です。
		• Distributing 送受信可能状態です。

3.5 レイヤ 2 ネットワークの通信障害

3.5.1 VLAN によるレイヤ 2 通信ができない

VLAN 使用時にレイヤ 2 通信ができない場合は，次に示す障害解析方法に従って原因の切り分けを行ってください。

(1) VLAN 状態の確認

運用コマンド show vlan または運用コマンド show vlan detail を実行して，VLAN の状態を確認してください。以下に，VLAN 機能ごとの確認内容を示します。

(a) 全 VLAN 機能での共通確認

- ポートに VLAN を正しく設定しているか。
- ポートのモードの設定は合っているか。また，デフォルト VLAN(VLAN ID 1) で期待したポートが所属していない場合は，以下の設定を確認してください。
  - VLAN ID 1 以外のポート VLAN をアクセス VLAN またはネイティブ VLAN に指定していないか。
  - トランクポートで allowed vlan にデフォルト VLAN の設定が抜けていないか。
  - ミラーポートに指定していないか。

(b) プロトコル VLAN の場合の確認

- プロトコル VLAN を使用している場合は，運用コマンド show vlan を実行して，プロトコルが正しく設定されていることを確認してください。

```
# show vlan
        :
VLAN ID:100   Type:Protocol based  Status:Up
  Protocol VLAN Information  Name:ipv4
    EtherType:0800,0806  LLC:  Snap-EtherType:
  Learning:On   Uplink-VLAN:       Uplink-Block:    Tag-Translation:
        :
```

(c) MAC VLAN の場合の確認

- MAC VLAN を使用している場合は，運用コマンド show vlan mac-vlan を実行して，VLAN で通信を許可する MAC アドレスが正しく設定されていることを確認してください。括弧内は，MAC アドレスの登録元機能を表しています。

［登録元機能］

static：コンフィグレーションにより設定された MAC アドレスです。

dot1x：IEEE802.1X 機能により設定された MAC アドレスです。

web-auth：Web 認証機能により設定された MAC アドレスです。

mac-auth：MAC 認証機能により設定された MAC アドレスです。

```
# show vlan mac-vlan
        :
VLAN ID:100     MAC Counts:4
    0012.e200.0001 (static)        0012.e200.00:02 (static)
    0012.e200.0003 (static)        0012.e200.00:04 (dot1x)
```

● 運用コマンド show vlan mac-vlan を実行して，レイヤ 2 認証機能とコンフィグレーションで同じ MAC アドレスを異なる VLAN に設定していないことを確認してください。*（アスタリスク）が表示されている MAC アドレスは，収容条件によってハードウェア上に登録されていないエントリを示します。

```
# show vlan mac-vlan
        :
VLAN ID:500     MAC Counts:4
    0012.e200.aa01 (static)        0012.e200.aa02 (static)
    0012.e200.aa03 (static)        0012.e200.aa04 (dot1x)
VLAN ID:600     MAC Counts:1
  * 0012.e200.aa01 (dot1x)
```

（2） ポート状態の確認

● 運用コマンド show vlan detail を実行して，ポートが Up 状態であることを確認してください。Down 状態の場合は「3.4　ネットワークインタフェースの通信障害」を参照してください。

● ポートが Forwarding 状態であることを確認してください。Blocking 状態である場合は，括弧内の要因により Blocking 状態となっています。要因となっている機能の運用状態を確認してください。

［要因］

VLAN：VLAN が suspend 指定です。

CH　：リンクアグリゲーションにより転送停止中です。

STP　：スパニングツリーにより転送停止中です。

dot1x ：IEEE802.1X 機能により転送停止中です。

ULR　：アップリンク・リダンダントにより転送停止中です。

AXRP：Ring Protocol により転送停止中です。

```
> show vlan 2048 detail Date 2008/10/29 03:21:25 UTC
VLAN counts: 1
VLAN ID: 2048  Type: Port based  Status: Up
        :
        :
  Port Information
   0/3          Up   Forwarding      Untagged
   0/4          Up   Forwarding      Untagged
   0/5          Down -               Untagged
   0/6          Down -               Untagged
```

（3） MAC アドレステーブルの確認

（a） MAC アドレス学習の状態の確認

● 運用コマンド show mac-address-table を実行して，通信障害となっている宛先 MAC アドレスの情報を確認してください。

```
> show mac-address-table
Date 2009/03/16 23:24:47 UTC
Aging time : 300
MAC address         VLAN    Type     Port-list
0000.0088.7701         2    Dynamic  0/49-50
000b.972f.e22b         2    Dot1x    0/35
0000.ef01.34f4      1000    Static   0/30
0000.ef01.3d17      1000    Static   0/30
000b.9727.ee41      1024    WebAuth  0/28
0010.c6ce.e1c6      1024    MacAuth  0/29
0012.e284.c703      1024    Dynamic  0/49-50
001b.7887.a492      1024    Dynamic  0/49-50
0100.5e00.00fc      1024    Snoop    0/49-50

>
```

● Type 表示によって以下の対処を行ってください。

【Type 表示が Dynamic の場合】

MAC アドレス学習の情報が更新されていない可能性があります。運用コマンド clear mac-address-table で古い情報をクリアしてください。宛先の装置からフレームを送信することでも情報を更新できます。

【Type 表示が Static の場合】

コンフィグレーションコマンド mac-address-table static で設定している転送先ポートを確認してください。

【Type 表示が Snoop の場合】

「3.5.4　IGMP snooping によるマルチキャスト中継ができない」および「3.5.5　MLD snooping によるマルチキャスト中継ができない」を参照してください。

【Type 表示が Dot1x の場合】

「3.7.1　IEEE802.1X 使用時の通信障害」を参照してください。

【Type 表示が WebAuth の場合】

「3.7.2　Web 認証使用時の通信障害」を参照してください。

【Type 表示が MacAuth の場合】

「3.7.3　MAC 認証使用時の通信障害」を参照してください。

● 該当する MAC アドレスが表示されない場合はフラッディングされます。表示されないにも関わらず通信ができない場合は，ポート間中継抑止が設定されていないか確認してください。また，ストームコントロール機能で閾値が小さい値になっていないか確認してください。

（4） フィルタ・QoS の確認

フィルタによって特定のパケットが廃棄されているか，または QoS 制御のシェーパによってパケットが廃棄されている可能性があります。コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築でのシェーパのシステム運用が適切であるかを確認してください。手順については，「3.14.1　フィルタ・QoS 設定情報の確認」を参照してください。

3.5.2　スパニングツリー機能使用時の障害

スパニングツリー機能を使用し，レイヤ 2 通信の障害，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，次の表に示す解析方法に従って原因の切り分けを行ってください。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 3-16　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	障害となっているスパニングツリーに対して運用コマンド show spanning-tree を実行し，スパニングツリーのプロトコル動作状況を確認してください。	Enable の場合は項番 2 へ。
		Disable の場合はスパニングツリーが停止状態になっています。次のコンフィグレーションを確認してください。 ・ spanning-tree disable ・ switchport backup

項番	確認内容・コマンド	対応
2	障害となっているスパニングツリーに対して運用コマンド show spanning-tree を実行し，スパニングツリーのルートブリッジのブリッジ識別子を確認してください。	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になっている場合は項番 3 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，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対して運用コマンド show spanning-tree を実行し，スパニングツリーのポート状態，ポート役割を確認してください。	スパニングツリーのポート状態，ポート役割がネットワーク構成どおりになっている場合は項番 4 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ではないか確認してください。 指定ポートの場合は，ループガード機能の設定を削除してください。
		スパニングツリーのポート状態，ポート役割がネットワーク構成とは異なる場合は，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。
4	障害となっているスパニングツリーに対して運用コマンド show spanning-tree statistics を実行し，障害となっているポートで BPDU の送受信を確認してください。	BPDU の送受信カウンタを確認してください。 【ルートポートの場合】 BPDU 受信カウンタがカウントアップされている場合は項番 5 へ。 カウントアップされていない場合は，フィルタによって BPDU が廃棄されているか，または QoS 制御のシェーパによって BPDU が廃棄されている可能性があります。「3.14.1　フィルタ・QoS 設定情報の確認」を参照して確認してください。問題がない場合は，隣接装置を確認してください。 【指定ポートの場合】 BPDU 送信カウンタがカウントアップされている場合は項番 5 へ。 カウントアップされていない場合は，「3.4　ネットワークインタフェースの通信障害」を参照してください。
5	障害となっているスパニングツリーに対して運用コマンド show spanning-tree detail を実行し，受信 BPDU のブリッジ識別子を確認してください。	受信 BPDU のルートブリッジ識別子，送信ブリッジ識別子がネットワーク構成どおりになっていることを確認してください。ネットワーク構成と異なっていた場合は隣接装置の状態を確認してください。
6	障害となっているスパニングツリーの最大数が収容条件内か確認してください。	収容条件の範囲内で設定してください。 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。

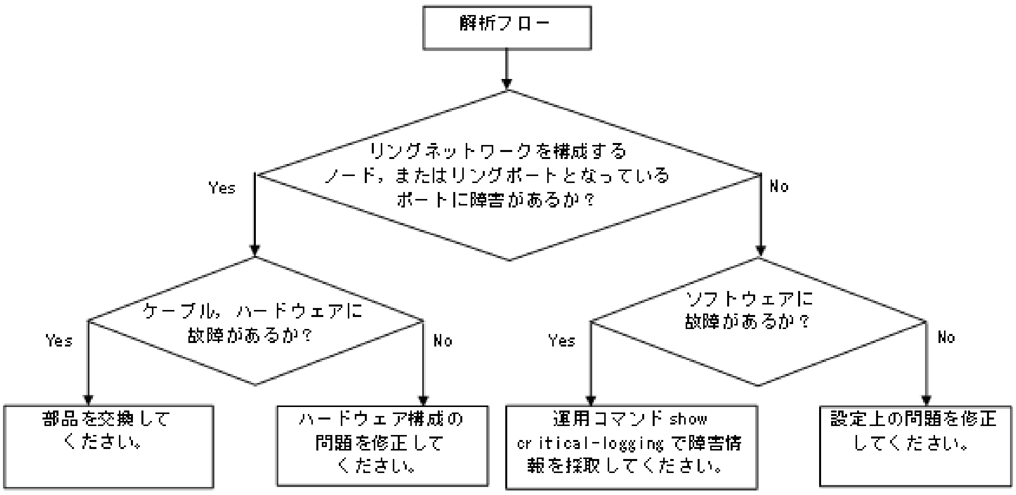
3.5.3 Ring Protocol 機能使用時の障害

この項では，Autonomous Extensible Ring Protocol の障害について説明します。

Autonomous Extensible Ring Protocol は，リングトポロジーでのレイヤ 2 ネットワークの冗長化プロトコルで，以降，Ring Protocol と呼びます。

Ring Protocol 運用時に通信ができない場合は，解析フローに従って，現象を把握し原因の切り分けを行ってください。

図 3-1 解析フロー



Ring Protocol 運用時に正常に動作しない場合，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，原因の切り分けを行ってください。

以下，IP8800/SS1250・IP8800/SS1240 シリーズについて解析方法を示します。ほかの IP8800 シリーズについては，当該シリーズのマニュアルを参照してください。

表 3-17 Ring Protocol の障害解析方法

項番	確認内容・コマンド	対応
1	運用コマンド show axrp を実行し，Ring Protocol の動作状態を確認してください。	"Oper State" の内容に "enable" が表示されている場合，項番 2 へ。
		"Oper State" の内容に "-" が表示されている場合，Ring Protocol が動作するために必要なコンフィグレーションに設定されていないものがあります。コンフィグレーションを確認してください。
		"Oper State" の内容に "disable" が表示されている場合，Ring Protocol は無効となっています。コンフィグレーションを確認してください。
		"Oper State" の内容に "Not Operating" が表示されている場合，Ring Protocol が動作していません。コンフィグレーションに矛盾がないか確認してください。
2	運用コマンド show axrp を実行し，動作モードを確認してください。	"Mode" の内容がネットワーク構成どおりの動作モードになっている場合には，項番 3 へ。
		上記が異なる場合には，コンフィグレーションを確認してください。
3	運用コマンド show axrp を実行し，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。	"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には，項番 4 へ。
		上記が異なる場合には，コンフィグレーションを確認してください。
4	運用コマンド show axrp detail を実行し，制御 VLAN ID を確認してください。	"Control VLAN ID" の内容がネットワーク構成どおりの VLAN ID となっている場合は，項番 5 へ。
		上記が異なる場合には，コンフィグレーションを確認してください。
5	運用コマンド show axrp detail を実行し，VLAN グループに属している VLAN ID を確認してください。	"VLAN ID" の内容がネットワーク構成どおりの VLAN ID となっている場合は，項番 6 へ。

項番	確認内容・コマンド	対応
6	運用コマンド show vlan detail を実行し，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。	VLAN およびそのポートの状態に異常がないか確認してください。 また，多重障害監視機能を適用する構成の場合には項番 7 も確認してください。 異常がある場合は，コンフィグレーションの確認も含め，その状態を復旧してください。
7	多重障害監視機能を適用している場合は，運用コマンド show axrp detail を実行し，多重障害監視の監視モードを確認してください。	"transport-only" が設定されている場合は，項番 8 へ。 上記が異なる場合には，コンフィグレーションを確認してください。
8	運用コマンド show axrp detail を実行し，多重障害監視用 VLAN ID を確認してください。	"Control VLAN ID" がネットワーク構成どおりの多重障害監視用 VLAN ID になっている場合は，共有ノードの多重障害監視装置で多重障害監視フレーム送信間隔のタイマ値，および多重障害監視フレームを受信しないで多重障害発生と判断するまでの保護時間のタイマ値を確認してください。 上記が異なる場合には，コンフィグレーションを確認してください。

3.5.4　IGMP snooping によるマルチキャスト中継ができない

IGMP snooping 使用時にマルチキャスト中継ができない場合は，解析フローに従い，次の表に示す対応で現象を把握し，原因の切り分けを行ってください。

図 3-2　解析フロー

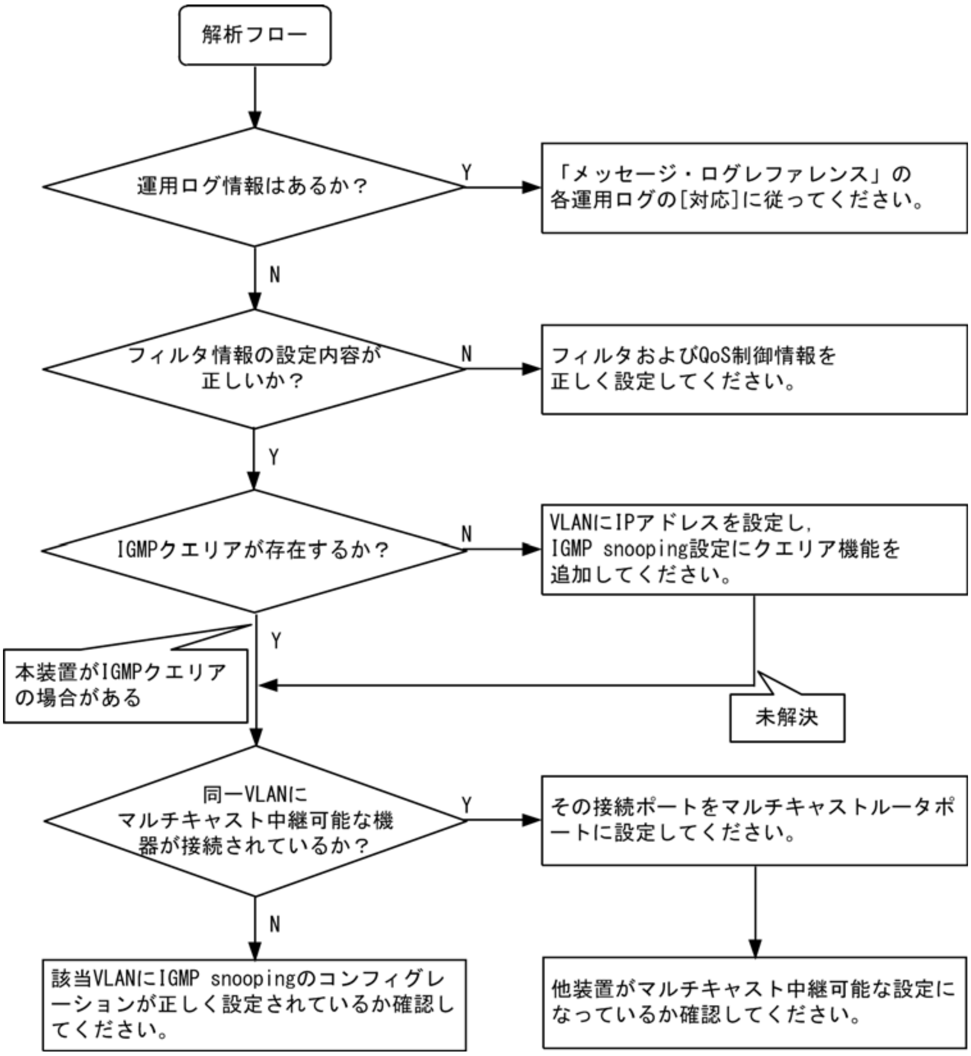


表 3-18　マルチキャスト中継の障害解析方法

項番	確認内容・コマンド	対応
1	マルチキャスト中継されない場合，運用コマンド show logging による障害発生の有無を確認してください。	以下の内容を確認してください。 ・物理的な障害のログ情報があるかを確認してください。
2	フィルタおよび QoS 制御の設定が正しいか確認してください。	フィルタによって特定のパケットが廃棄されている，または QoS 制御のシェーパによってパケットが廃棄されている可能性があります。コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築でのシェーパのシステム運用が適切であるかを確認してください。 手順については，「3.14.1　フィルタ・QoS 設定情報の確認」を参照してください。

項番	確認内容・コマンド	対応

3	マルチキャスト中継されない場合，IGMP snooping の構成を運用コマンド show igmp-snooping で確認してください。	以下の内容を確認してください。
		・グループメンバを監視する IGMP クエリアの存在を確認するため，以下に示すメッセージが表示されていることを確認する。
		(1)　IGMP クエリアが存在する場合，IGMP クエリアの IP アドレスが表示されます。
		`IGMP querying system: 192.168.11.20*`
		(2)　IGMP クエリアが存在しない場合は，「IGMP querying system:」の項目内容に何も表示されません。
		`IGMP querying system:`
		・本装置が IGMP クエリアの場合，VLAN に IP アドレスが設定されていることを確認してください。
		(1)　VLAN に IP アドレスが設定されている場合，メッセージが表示されます。
		`IP Address: 192.168.11.20*`
		(2)　VLAN に IP アドレスが設定されていない場合，「IP Address:」の項目内容に何も表示されません。
		`IP Address:`
		・マルチキャストルータを接続している場合，mrouter-port を確認してください。
		`> show igmp-snooping 3253`
		
		`Date 2008/11/14 15:59:14 UTC`
		`VLAN counts: 3`
		`VLAN 3253:`
		`  IP Address: 192.168.53.100/24   Querier: enable`
		`  IGMP querying system: 192.168.53.100`
		`  Port (4): 0/13-16`
		`  Mrouter-port: 0/13-16`
		`  Group counts: 5`

4	マルチキャスト中継されない場合，運用コマンド show igmp-snooping group で IPv4 マルチキャストグループアドレスを確認してください。	以下の内容を確認してください。
		・加入した IPv4 マルチキャストグループアドレスが show igmp-snooping group で表示されていることを確認してください。
		`> show igmp-snooping group 3253`
		
		`Date 2008/11/14 16:02:03 UTC`
		`Total Groups: 15`
		`VLAN counts: 3`
		`VLAN 3253 Group counts: 5`
		`  Group Address     MAC Address`
		`   230.0.0.11        0100.5e00.000b`
		`     Port-list: 0/13`
		`   230.0.0.10        0100.5e00.000a`
		`     Port-list: 0/13`

注※　本装置が IGMP クエリアの場合は，IGMP querying system で表示されているアドレスと IP Address で表示されているアドレスは一致するが，他装置が IGMP クエリアの場合は，IGMP querying system で表示されているアドレスと IP Address で表示されているアドレスは一致しません。

3.5.5 MLD snooping によるマルチキャスト中継ができない

MLD snooping 使用時にマルチキャスト中継ができない場合は，解析フローに従い，次の表に示す対応で現象を把握し，原因の切り分けを行ってください。

図 3-3 解析フロー

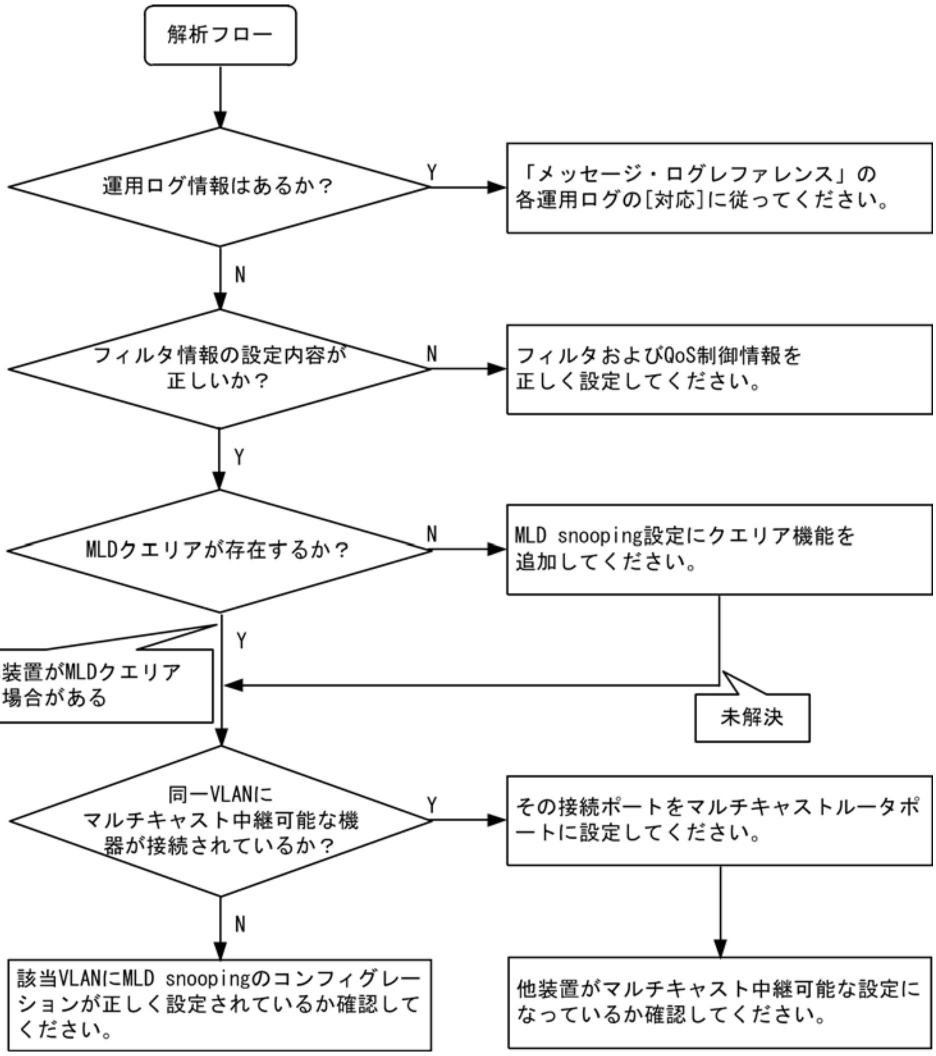


表 3-19 マルチキャスト中継の障害解析方法

項番	確認内容・コマンド	対応
1	マルチキャスト中継されない場合，運用コマンド show logging による障害発生の有無を確認してください。	以下の内容を確認してください。 ・物理的な障害のログ情報があるかを確認してください。
2	フィルタおよび QoS 制御の設定が正しいか確認してください。	フィルタによって特定のパケットが廃棄されている，または QoS 制御のシェーパによってパケットが廃棄されている可能性があります。コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築でのシェーパのシステム運用が適切であるかを確認してください。 手順については，「3.14.1 フィルタ・QoS 設定情報の確認」を参照してください。

項番	確認内容・コマンド	対応

3	マルチキャスト中継されない場合，MLD snooping の構成を運用コマンド show mld-snooping で確認してください。	以下の内容を確認してください。
		・グループメンバを監視する MLD クエリアの存在を確認するため，以下に示すメッセージが表示されていることを確認する。
		(1)　MLD クエリアが存在する場合，MLD クエリアの IP アドレスが表示されます。
		`MLD querying system: fe80::200:87ff:fe10:1959*`
		(2)　MLD クエリアが存在しない場合は，「MLD querying system:」の項目内容に何も表示されません。
		・本装置が MLD クエリアの場合，コンフィグレーションコマンド ipv6 mld snooping source で送信元 IP アドレスが設定されていることを確認してください。
		`MLD querying system:`
		(3) コンフィグレーションコマンド ipv6 mld snooping source で送信元 IP アドレスが設定されていない場合，「IP Address:」の項目内容には何も表示されません。
		`IP Address:`
		・マルチキャストルータを接続している場合，mrouter-port を確認してください。
		`> show mld-snooping 3001`
		
		`Date 2008/11/14 17:21:51 UTC`
		`VLAN counts: 3`
		`VLAN 3001:`
		`  IP Address:   Querier: enable`
		`  MLD querying system:`
		`  Querier version: v1`
		`  Port (1): 0/12`
		`  Mrouter-port: 0/12`
		`  Group counts: 1`

4	マルチキャスト中継されない場合，運用コマンド show mld-snooping group で IPv6 マルチキャストグループアドレスを確認してください。	以下の内容を確認してください。
		・加入した IPv6 マルチキャストグループアドレスが show mld-snooping group で表示されていることを確認してください。
		`> show mld-snooping group 3001`
		
		`Date 2008/11/14 17:22:10 UTC`
		`Total Groups: 3`
		`VLAN counts: 3`
		`VLAN 3001 Group counts: 1`
		`  Group Address                          MAC Address`
		`Version   Mode`
		`   ff80:0:0:0:0:0:99:a0a                 3333.0099.0a0a`
		`v1        -`
		`     Port-list: 0/12`

注※　本装置が MLD クエリアの場合は，MLD querying system で表示されているアドレスと IP Address で表示されているアドレスは一致するが，他装置が MLD クエリアの場合は，MLD querying system で表示されているアドレスと IP Address で表示されているアドレスは一致しません。

3.6　IPv4 ネットワークの通信障害

3.6.1　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考えられるのは，次の 3 種類があります。

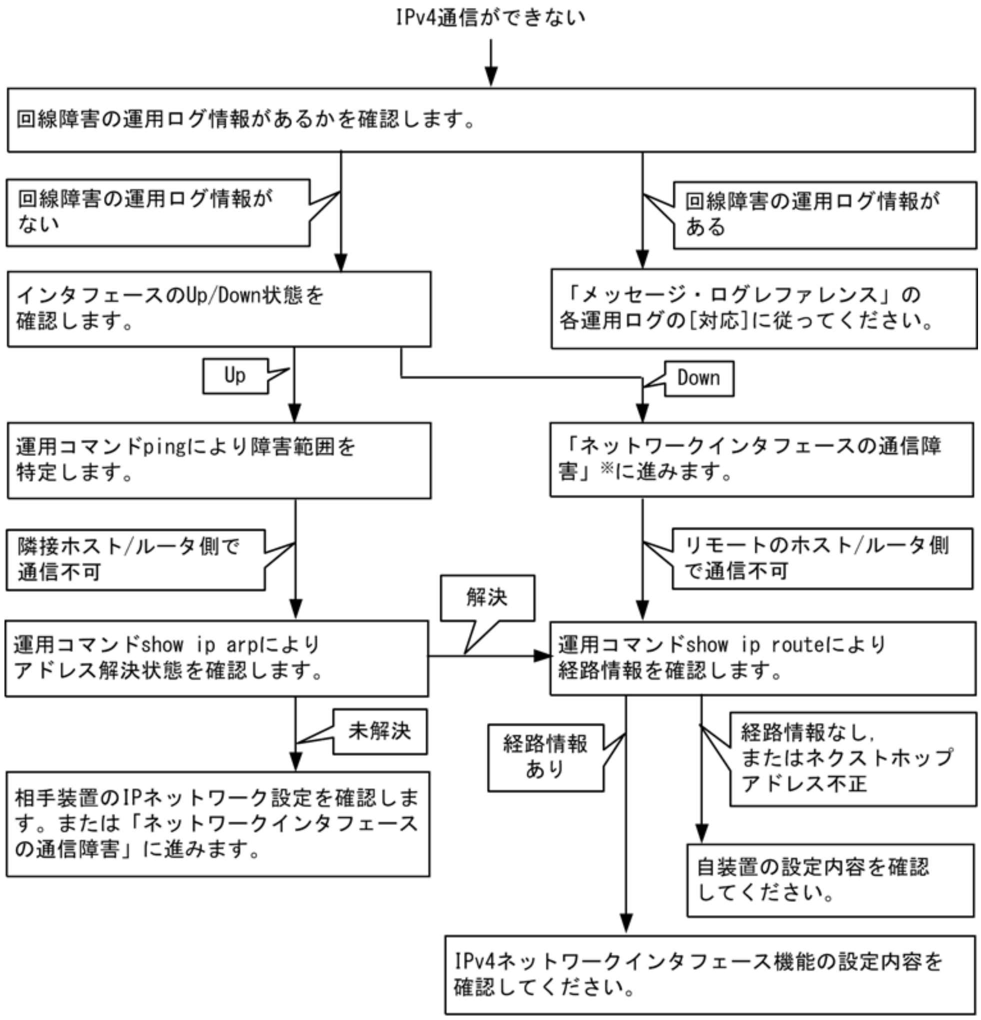
1. IP 通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

上記 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調べていただき，通信ができなくなるような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 IP 通信ができない」，「これまで正常に動いていたのに IP 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いたします。

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 3-4　解析フロー



注※「3.4　ネットワークインタフェースの通信障害」を参照してください。

(1) 装置障害ログの確認

通信ができなくなる原因の一つには，回線の障害（または壊れ）が考えられます。本装置が表示する装置障害ログで，ハードウェアの障害を示すメッセージの表示手順を示します。

なお，装置障害ログの内容については，「メッセージ・ログレファレンス」を参照してください。

1. 本装置にログインします。
2. 運用コマンド show critical-logging を使って装置障害ログを表示させます。
3. 装置障害ログには各々発生した日時が表示されます。通信ができなくなった日時に装置障害ログが表示されていないか確認してください。
4. 通信ができなくなった日時に表示されている装置障害ログの障害の内容および障害への対応は「メッセージ・ログレファレンス」に記載しています。その指示に従ってください。
5. 通信ができなくなった日時に装置障害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の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。

本装置と隣接の装置間の，インタフェースの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. 運用コマンド show ip interface を使って該当装置間のインタフェースの Up ／ Down 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，「3.4　ネットワークインタフェースの通信障害」を参照してください。
4. 該当インタフェースとの間のインタフェースが”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，通信を行っ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。通信相手とのどこ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. 運用コマンド ping を使っ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。運用コマンド ping の操作例および実行結果の見方は，「コンフィグレーションガイド」を参照してください。
3. 運用コマンド ping で通信相手との疎通が確認できなかったときは，さらに運用コマンド ping を使っ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. 運用コマンド ping 実行の結果，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こ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 機能をお使いになり，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，さらに運用コマンド ping を使ってお客様の

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 機能による障害範囲が特定できましたら，障害と考えられる装置が本装置である場合は本装置にログインしていただき，障害解析フローに従って障害原因の調査を行ってください。

(5) 隣接装置との ARP 解決情報の確認

運用コマンド ping の実行結果によって隣接装置との疎通が不可の場合は，ARP によるアドレスが解決し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. 運用コマンド show ip arp を使っ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を確認してください。

(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にもかかわらず通信ができない場合や，IPv4 ユニキャスト通信で通信相手との途中の経路で疎通が不可となる，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。確認手順を次に示します。

1. 本装置にログインします。
2. 運用コマンド show ip route 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。
3. 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，通信不可の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。該当する機能の調査を行ってください。
   - フィルタ機能

   「(7) フィルタ・QoS 設定情報の確認」に進んでください。

(7) フィルタ・QoS 設定情報の確認

フィルタによって特定のパケットが廃棄されているか，QoS 制御のシェーパによってパケットが廃棄されている可能性があります。

コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築でのシェーパのシステム運用が適切であるか見直してください。手順については，「3.14.1　フィルタ・QoS 設定情報の確認」を参照してください。

3.7　レイヤ 2 認証の通信障害

3.7.1　IEEE802.1X 使用時の通信障害

IEEE802.1X 使用時に通信ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-20　IEEE802.1X の障害解析方法

項番	確認内容・コマンド	対応
1	運用コマンド show dot1x を実行し，IEEE802.1X の動作状態を確認してください。	• 「System 802.1X：Disable」または「Dot1x doesn't seem to be running」の場合 IEEE802.1X が停止しています。コンフィグレーションコマンド dot1x system-auth-control が設定されているかコンフィグレーションを確認してください。 • 「System 802.1X：Enable」の場合は項番 2 へ。
2	運用コマンド show dot1x statistics を実行し，EAPOL のやりとりが行われていることを確認してください。	• [EAPOL frames] の RxTotal が 0 の場合は端末から EAPOL が送信されていません。また，RxInvalid または RxLenErr が 0 でない場合は端末から不正な EAPOL を受信しています。不正な EAPOL を受信した場合はログを採取します。ログは運用コマンド show dot1x logging で閲覧できます。また，ログは「Invalid EAPOL frame received」メッセージと共に不正な EAPOL の内容となります。上記に該当する場合は端末の Supplicant の設定を確認してください。 • 上記に該当しない場合は項番 3 へ。
3	運用コマンド show dot1x statistics を実行し，RADIUS サーバへの送信が行われていることを確認してください。	[EAPoverRADIUS frames] の TxTotal が 0 の場合は RADIUS サーバへの送信が行われていません。以下について確認してください。 • コンフィグレーションコマンドで aaa authentication dot1x default group radius が設定されているか確認してください。 • コンフィグレーションコマンド dot1x radius-server host または radius-server host が正しく設定されているか確認してください。 【ポート単位認証（静的）】 • 認証端末の MAC アドレスがコンフィグレーションコマンド mac-address-table static で登録されていないことを確認してください。 【ポート単位認証（動的）】 • 認証端末の MAC アドレスがコンフィグレーションコマンド mac-address-table static と mac-address で登録されていないことを確認してください。 【VLAN 単位認証（動的）】 • 認証端末の MAC アドレスがコンフィグレーションコマンド mac-address で登録されていないことを確認してください。 • コンフィグレーションコマンドで aaa authentication network default group radius が設定されているか確認してください。 • 上記に該当しない場合は項番 4 へ。
4	運用コマンド show dot1x statistics を実行し，RADIUS サーバからの受信が行われていることを確認してください。	[EAPoverRADIUS frames] の RxTotal が 0 の場合は RADIUS サーバからのパケットを受信していません。以下について確認してください。 • RADIUS サーバがリモートネットワークに収容されている場合はリモートネットワークへの経路が存在することを確認してください。 • RADIUS サーバのポートが認証対象外となっていることを確認してください。 • 上記に該当しない場合は項番 5 へ。

項番	確認内容・コマンド	対応
5	運用コマンド show dot1x logging を実行し，RADIUS サーバとのやりとりを確認してください。	• 「Invalid EAP over RADIUS frames received」がある場合 RADIUS サーバから不正なパケットを受信しています。RADIUS サーバが正常に動作しているか確認してください。 • 「Failed to connect to RADIUS server」がある場合，RADIUS サーバへの接続が失敗しています。RADIUS サーバが正常に動作しているか確認してください。 • 上記に該当しない場合は項番 6 へ。
6	運用コマンド show dot1x logging を実行し，認証が失敗していないか確認してください。	• 「RADIUS authentication failed」がある場合 以下の要因で認証が失敗しています。問題ないか確認してください。 (1) ユーザ ID またはパスワードが認証サーバに登録されていない。 (2) ユーザ ID またはパスワードの入力ミス。 • 「The number of supplicants on the switch is full」がある場合 装置の最大 supplicant 数を超えたため，認証が失敗しています。 • 「The number of supplicants on the interface is full」がある場合 インタフェース上の最大 supplicant 数を超えたため，認証が失敗しています。 • 「Failed to authenticate the supplicant because it could not be registered to mac-address-table.」がある場合 認証は成功したが，ハードウェアの MAC アドレステーブル設定に失敗しています。 「メッセージ・ログレファレンス」の該当個所を参照し，記載されている［対応］に従って対応してください。 • 認証モードが VLAN 単位認証 (動的) で，「Failed to assign VLAN.」がある場合 RADIUS サーバによる認証は成功したが，VLAN の割り当てに失敗しています。 • 「Failed to authenticate the supplicant because it could not be registered to MAC VLAN.」がある場合 認証は成功したが，H/W の MAC VLAN テーブル設定に失敗しています。 「メッセージ・ログレファレンス」の該当個所を参照し，記載されている［対応］に従って対応してください。 • 上記に該当しない場合で認証モードがポート単位認証（動的）または VLAN 単位認証（動的）は項番 7 へ，それ以外は RADIUS サーバのログを参照して認証が失敗していないか確認してください。
7	運用コマンド show dot1x logging を実行し，VLAN 単位認証（動的）の動的割り当てが失敗していないか確認してください。	「Failed to assign VLAN (Reason:xxxxx)」がある場合，以下の (Reason:xxxxx) を確認してください。 • 「(Reason: No Tunnel-Type Attribute)」 【ポート単位認証（動的）】【VLAN 単位認証（動的）】 RADIUS 属性に Tunnel-Type 属性がないため，動的割り当てに失敗しています。 RADIUS サーバの RADIUS 属性に Tunnel-Type 属性を設定してください。 • 「 (Reason: Tunnel-Type Attribute is not VLAN(13)」 【ポート単位認証（動的）】【VLAN 単位認証（動的）】 RADIUS 属性の Tunnel-Type 属性が値 (13) でないため，動的割り当てに失敗しています。 RADIUS サーバの RADIUS 属性の Tunnel-Type 属性に VLAN(13) を設定してください。

項番	確認内容・コマンド	対応
44		• 「(Reason: No Tunnel-Medium-Type Attribute)」 【ポート単位認証（動的)】【VLAN 単位認証（動的)】 RADIUS 属性の Tunnel-Medium-Type 属性がないため，動的割り当てに失敗しています。 RADIUS サーバの RADIUS 属性に Tunnel-Medium-Type 属性を設定してください。 • 「(Reason: Tunnel-Medium-Type Attribute is not IEEE802(6))」 【ポート単位認証（動的)】【VLAN 単位認証（動的)】 Tunnel-Medium-Type 属性の値が IEEE802(6) でないか，または Tunnel-Medium-Type の値は一致しているが Tag 値が Tunnel-Type 属性の Tag と一致していないため動的割り当てに失敗しています。 RADIUS サーバの RADIUS 属性の Tunnel-Medium-Type 属性の値または Tag を正しい値に設定してください。 • 「(Reason: No Tunnel-Private-Group-ID Attribute)」 【ポート単位認証（動的)】【VLAN 単位認証（動的)】 RADIUS サーバの RADIUS 属性に Tunnel-Private-Group-ID 属性が設定されていないため，動的割り当てに失敗しています。 RADIUS サーバの RADIUS 属性に Tunnel-Private-Group-ID 属性を設定してください。 • 「(Reason: Invalid Tunnel-Private-Group-ID Attribute)」 【ポート単位認証（動的)】【VLAN 単位認証（動的)】 RADIUS 属性の Tunnel-Private-Group-ID 属性に不正な値が入っているため，動的割り当てに失敗しています。 RADIUS サーバの RADIUS 属性の Tunnel-Private-Group-ID 属性に正しい VLAN ID を設定してください。 RADIUS サーバに VLAN 名称で登録している場合は，該当 VLAN のコンフィグレーションコマンド name ※2 と一致しているか確認してください。 • 「(Reason: The port doesn't belong to VLAN)」 【ポート単位認証（動的)】 認証ポートが RADIUS 属性の Tunnel-Private-Group-ID 属性に指定された VLAN ID に属していないため，動的割り当てに失敗しています。 RADIUS サーバの RADIUS 属性の Tunnel-Private-Group-ID 属性に設定された VLAN ID と，認証対象ポートのコンフィグレーションコマンド switchport mac vlan ※1 の VLAN ID が一致するように設定してください。 RADIUS サーバに VLAN 名称で登録している場合は，該当 VLAN のコンフィグレーションコマンド name ※2 と一致しているか確認してください。 • 「(Reason: The VLAN ID is not set to radius-vlan)」 【VLAN 単位認証（動的)】 RADIUS サーバの RADIUS 属性の Tunnel-Private-Group-ID 属性に指定された VLAN ID が，VLAN 単位認証（動的）の対象外です。 RADIUS サーバの RADIUS 属性の Tunnel-Private-Group-ID 属性に設定された VLAN ID と，VLAN 単位認証（動的）ののコンフィグレーションコマンド dot1x vlan dynamic radius-vlan の VLAN ID が一致するように設定してください。 RADIUS サーバに VLAN 名称で登録している場合は，該当 VLAN のコンフィグレーションコマンド name ※2 と一致しているか確認してください。

項番	確認内容・コマンド	対応
		• 上記に該当しない場合は，RADIUS サーバのログを参照して認証が失敗していないか確認してください。
8	ポート単位認証（静的）使用時に NAP 検疫システムと連携して認証できないときは，認証専用 IPv4 アクセスリストの設定を確認してください。	【ポート単位認証（静的）】 • 認証専用 IPv4 アクセスリストに検疫サーバ宛のアクセス許可が設定されていることを確認してください。 • RADIUS サーバの RADIUS 属性の Filter-ID と，本装置の認証専用 IPv4 アクセスリスト名が一致するよう設定してください。

注※ 1

コンフィグレーションコマンド switchport mac vlan 未設定のときは，コンフィグレーションコマンド vlan の mac-based で，RADIUS サーバの VLAN ID が設定されているか確認してください。

注※ 2

コンフィグレーションコマンド name で設定する VLAN 名称を，RADIUS 認証の認証後 VLAN として使用するときは下記に注意してください。

- VLAN 名称が，複数の VLAN で重複しないように設定してください。VLAN 名称が重複していると，重複しているうちで最も小さい VLAN ID が RADIUS 認証の認証後 VLAN として割り当てられます。
- VLAN 名称の先頭に数字を指定しないでください。先頭の数字を VLAN ID として認識し，認証に失敗する場合があります。

IEEE802.1X が動作するポートまたは VLAN で通信ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。該当しない場合は，「3.5　レイヤ 2 ネットワークの通信障害」を参照してください。

表 3-21　IEEE802.1X の通信障害解析方法

項番	確認内容・コマンド	対応
1	認証済み端末が同一 VLAN 内の非認証ポートに移動していないか確認してください。	本装置で認証している端末が，非認証ポートに移動した場合，認証情報が解除されないと通信ができません。運用コマンド clear dot1x auth-state を使用して，対象端末の認証状態を解除してください。

3.7.2 Web 認証使用時の通信障害

Web 認証使用時の障害については，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-22 Web 認証の障害解析方法

項番	確認内容・コマンド	対応
1	端末にログイン画面が表示されるかを確認してください。	• ログイン画面とログアウト画面が表示されない場合は項番 2 へ。 • ローカル認証方式でログイン画面が表示される場合は項番 5 へ。 • RADIUS 認証方式でログイン画面が表示される場合は項番 7 へ。
2	ログイン，ログアウトの URL が合っているかを確認してください。	• ログイン，ログアウトの URL が違っている場合は，正しい URL を使用してください。 • Web 認証専用 IP アドレスを設定している場合，Web 認証を実施する VLAN（ダイナミック VLAN・固定 VLAN）に IP アドレスがコンフィグレーションコマンド ip address で設定されていることを確認してください。 • 固定 VLAN モードまたはダイナミック VLAN モードの場合は項番 3 へ。 • 上記に該当しない場合は項番 9 へ。
3	固定 VLAN モード，ダイナミック VLAN モードで Web 認証専用 IP アドレスまたは URL リダイレクトの設定を確認してください。	【固定 VLAN モード】【ダイナミック VLAN モード】 • Web 認証専用 IP アドレスがコンフィグレーションコマンド web-authentication ip address で設定されているか，または URL リダイレクトがコンフィグレーションコマンド web-authentication redirect enable で有効となっているか確認してください。 • URL リダイレクトが有効な場合，固定 VLAN モードまたはダイナミック VLAN モードの認証対象 VLAN に，IP アドレスがコンフィグレーションコマンド ip address で設定されていることを確認してください。 • 上記に該当しない場合は項番 4 へ。
4	認証専用 IPv4 アクセスリストの設定を確認してください。	【固定 VLAN モード】【ダイナミック VLAN モード】 • 認証前状態の端末から本装置外に特定のパケット通信を行う場合，認証専用 IPv4 アクセスリストが設定されていることを確認してください。 また，認証対象ポートに通常のアクセスリストと認証専用 IPv4 アクセスリストの両方を設定した場合，認証専用 IPv4 アクセスリストに設定したフィルタ条件が通常のアクセスリストにも設定されていることを確認してください。 • 認証対象ポートに対する通常のアクセスリストおよび認証専用 IPv4 アクセスリストに，IP パケットを廃棄するフィルタ条件（deny ip など）が設定されていないことを確認してください。 • 認証専用 IPv4 アクセスリストのフィルタ条件の宛先 IP アドレスに，any が設定されていないことを確認してください。 • 上記に該当しない場合は項番 10 へ。
5	運用コマンド show web-authentication user でユーザ ID が登録されているかを確認してください。	• ユーザ ID が登録されていない場合は，運用コマンド set web-authentication user でユーザ ID，パスワード，および VLAN ID を登録してください。登録後は，運用コマンド commit web-authentication で運用に反映してください。 • 上記に該当しない場合は項番 6 へ。

項番	確認内容・コマンド	対応
6	入力したパスワードが合っているかを確認してください。	• パスワードが一致していない場合は，運用コマンド set web-authentication passwd でパスワードを変更するか，運用コマンド remove web-authentication user でユーザ ID をいったん削除したあとに，運用コマンド set web-authentication user で，再度ユーザ ID，パスワード，および VLAN ID を登録してください。変更後は，運用コマンド commit web-authentication で運用に反映してください。 • 上記に該当しない場合は項番 10 へ。
7	運用コマンド show web-authentication statistics で RADIUS サーバとの通信状態を確認してください。	• 表示項目 "[RADIUS frames]" の "TxTotal" の値が "0" の場合は，下記のコンフィグレーションが正しく設定されているか確認してください。 aaa authentication web-authentication default web-authentication radius-server host または radius-server host • 上記に該当しない場合は項番 8 へ。
8	RADIUS サーバにユーザ ID およびパスワードが登録されているかを確認してください。	• ユーザ ID が登録されていない場合は，RADIUS サーバに登録してください。 【固定 VLAN モード】 • RADIUS サーバの NAS-Identifier の VLAN ID が認証対象端末が所属する VLAN ID と一致しているか確認してください。 【ダイナミック VLAN モード】 • RADIUS サーバの VLAN ID と認証対象ポートのコンフィグレーションコマンド switchport mac vlan ※1 の VLAN ID が一致しているか確認してください。 • RADIUS サーバに VLAN 名称で登録している場合は，該当 VLAN のコンフィグレーションコマンド name ※2 と一致しているか確認してください。 【レガシーモード】 • RADIUS サーバの VLAN ID と，コンフィグレーションコマンド web-authentication vlan および認証対象端末接続ポートのコンフィグレーションコマンド switchport mac vlan の VLAN ID が一致しているか確認してください。 • RADIUS サーバに VLAN 名称で登録している場合は，該当 VLAN のコンフィグレーションコマンド name ※2 と一致しているか確認してください。 • 上記に該当しない場合は項番 10 へ。
9	運用コマンド show logging で "HTTP server initialization failed." が採取されているか確認してください。	• 採取されている場合は，SSL の証明書および秘密鍵が正しくありません。正しい証明書および秘密鍵を入手し，装置に再インストールしてください。 • 上記に該当しない場合は項番 10 へ。
10	運用コマンド show web-authentication statistics で Web 認証の統計情報が表示されるかを確認してください。	• Web 認証の統計情報が表示されない場合は項番 11 へ。 • 上記に該当しない場合は項番 12 へ。
11	コンフィグレーションコマンド web-authentication system-auth-control が設定されているかを確認してください。	• コンフィグレーションコマンド web-authentication system-auth-control が設定されていない場合は，設定してください。 • 上記に該当しない場合は項番 12 へ。
12	show web-authentication logging コマンドを実行し，動作に問題がないかを確認してください。	動作ログ種別 LOGIN で，下記の動作ログが表示されていない場合は認証に失敗しています。 • 「Login succeeded」 • 「Login update succeeded」 動作ログ内容を確認して，RADIUS サーバ，内蔵 Web 認証 DB，コンフィグレーションなどの設定内容を見直してください。(動作ログ内容は，運用コマンドレファレンスを参照してください。)

項番	確認内容・コマンド	対応
		【固定 VLAN モード】【ダイナミック VLAN モード】 • 認証端末が接続されているポートの認証情報が表示されない場合は，コンフィグレーションコマンド web-authentication port で認証対象ポートが正しく設定されているか確認してください。
		【Web 認証共通】 • 端末が接続されている認証対象ポートがリンクダウンまたはシャットダウンしていないことを確認してください。 • 上記以外の場合は Web 認証のコンフィグレーションを確認してください。

注※ 1

コンフィグレーションコマンド switchport mac vlan 未設定のときは，コンフィグレーションコマンド vlan の mac-based で，RADIUS サーバの VLAN ID が設定されているか確認してください。

注※ 2

コンフィグレーションコマンド name で設定する VLAN 名称を，RADIUS 認証の認証後 VLAN として使用するときは下記に注意してください。

- VLAN 名称が，複数の VLAN で重複しないように設定してください。VLAN 名称が重複していると，重複しているうちで最も小さい VLAN ID が RADIUS 認証の認証後 VLAN として割り当てられます。
- VLAN 名称の先頭に数字を指定しないでください。先頭の数字を VLAN ID として認識し，認証に失敗する場合があります。

Web 認証に関係するコンフィグレーションは次の点を確認してください。

表 3-23　Web 認証のコンフィグレーションの確認

項番	確認内容・コマンド	対応
1	Web 認証のコンフィグレーション	次のコンフィグレーションコマンドが正しく設定されていることを確認してください。 【Web 認証共通】 • aaa authentication web-authentication default group radius • web-authentication auto-logout • web-authentication max-timer • web-authentication system-auth-control 【固定 VLAN モード】 • web-authentication port • web-authentication static-vlan max-user • authentication arp-relay • authentication ip access-group • web-authentication redirect enable • web-authentication redirect-mode 【ダイナミック VLAN モード】 • web-authentication port • web-authentication max-user • authentication arp-relay • authentication ip access-group • web-authentication redirect enable • web-authentication redirect-mode 【レガシーモード】 • web-authentication max-user • web-authentication vlan

項番	確認内容・コマンド	対応
2	VLAN インタフェースの IP アドレス設定	【固定 VLAN モード】 対象 VLAN インタフェースに IP アドレスが正しく設定されていることを確認してください。 【ダイナミック VLAN モード】【レガシーモード】 次の各 VLAN インタフェースに IP アドレスが正しく設定されていることを確認してください。 • 認証前 VLAN • 認証後 VLAN
3	DHCP サーバの設定	DHCP サーバ使用時は，「(1) DHCP サーバ使用時の通信障害」を参照してください。
4	フィルタ設定	フィルタによって特定のパケットが廃棄されているか，または QoS 制御のシェーパによってパケットが廃棄されている可能性があります。コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築でのシェーパのシステム運用が適切であるかを確認してください。手順については「3.14.1　フィルタ・QoS 設定情報の確認」を参照してください。
5	認証専用 IPv4 アクセスリストの設定	【固定 VLAN モード】【ダイナミック VLAN モード】 認証前状態の端末から本装置外に通信するために必要なフィルタ条件が，コンフィグレーションコマンド authentication ip access-group および ip access-list extended で正しく設定されていることを確認してください。
6	ARP パケット中継の設定	【固定 VLAN モード】【ダイナミック VLAN モード】 認証前状態の端末から本装置外の機器宛に ARP パケットを通信させるためのコンフィグレーションコマンド authentication arp-relay が正しく設定されていることを確認してください。

(1) DHCP サーバ使用時の通信障害

DHCP サーバの通信トラブル（クライアントにアドレス配信できない）が発生する要因として考えられるのは，次の 3 種類があります。

1. コンフィグレーションの設定ミス
2. ネットワークの構成変更
3. DHCP サーバの障害

まず上記 1. の確認を行ってください。コンフィグレーションの設定で間違えやすいものを例にとり説明します。上記 2. については，ネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。クライアント／サーバの設定（ネットワークカードの設定，ケーブルの接続など）は確認されている場合，上記 3. に示すような「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クライアントに IP アドレスが割り振られず，IP 通信できない」，というケースについては，詳細を「(b) 運用ログおよびインタフェースの確認」～「(d) フィルタ・QoS 設定情報の確認」に示します。

(a) コンフィグレーションの確認

DHCP サーバ上のリソース類のコンフィグレーションの設定ミスによりクライアントに IP アドレスが割り振られないという原因が考えられます。コンフィグレーションの確認手順を次に示します。

- DHCP クライアントに割り付ける IP アドレスの network 設定を含む ip dhcp pool 設定が存在することを，コンフィグレーションで確認してください。
- DHCP クライアントに割り付ける IP アドレスプール数がコンフィグレーションコマンド ip dhcp

excluded-address によって同時使用するクライアントの台数分以下になっていないかを，コンフィグレーションで確認してください。
- 外部 DHCP サーバを使用している場合は，DHCP リレーエージェントとなる装置の設定を確認してください。

(b) 運用ログおよびインタフェースの確認

クライアントに IP アドレスが割り振られなくなる原因の一つにクライアントーサーバ間で通信ができなくなっていることが考えられます。本装置が表示する運用ログや運用コマンド show ip interface によるインタフェースの up ／ down 状態を確認してください。手順については「3.4　ネットワークインタフェースの通信障害」を参照してください。

(c) 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ときは通信を行っ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。通信相手とのどこ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。

- 本装置にログインします。
- クライアントとサーバ間に L3 スイッチなどがある場合，運用コマンド ping を使って通信できない相手（DHCP クライアント）との間にある装置（L3 スイッチ）の疎通を確認してください。運用コマンド ping で通信相手との疎通が確認できなかったときは，さらに運用コマンド ping を使って本装置からクライアント側に向けて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。運用コマンド ping の操作例および実行結果の見方は，「コンフィグレーションガイド」を参照してください。
- サーバとクライアントが直結の場合，HUB やケーブルの接続を確認してください。

(d) フィルタ・QoS 設定情報の確認

本装置において物理的障害がないにもかかわらず通信ができない場合は，フィルタ機能により特定のパケットだけが廃棄されているか，あるいは QoS 機能のシェーパによりパケットが廃棄されている可能性があります。従って，コンフィグレーションのフィルタ機能および QoS 機能の設定条件が正しいか，システム構築でのシェーパがシステム運用が適切であるか，本装置およびクライアント・サーバ間にある中継装置でも見直しを行ってください。手順については「3.14.1　フィルタ・QoS 設定情報の確認」を参照してください。

(e) レイヤ２ネットワークの確認

(a) から (e) までの手順で設定ミスや障害が見つからない場合は，レイヤ 2 ネットワークに問題がある可能性があります。「3.5　レイヤ 2 ネットワークの通信障害」を参考にレイヤ 2 ネットワークの確認を行ってください。

3.7.3　MAC 認証使用時の通信障害

MAC 認証使用時に通信ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-24　MAC 認証使用時の障害解析方法

項番	確認内容・コマンド	対応
1	端末が通信できるか確認してください。	• ローカル認証方式で認証できない場合は項番 2 へ。 • RADIUS 認証方式で認証できない場合は項番 3 へ。 • 上記に該当しない場合は項番 6 へ。
2	運用コマンド show mac-authentication mac-address で MAC アドレスと VLAN ID が登録されていることを確認してください。	• MAC アドレスが登録されていない場合は，運用コマンド set mac-authentication mac-address で MAC アドレスおよび VLAN ID を登録してください。登録後は，運用コマンド commit mac-authentication で運用に反映してください。 【固定 VLAN モード】 • コンフィグレーションコマンド mac-authentication vlan-check を設定している場合は，MAC アドレスと認証対象端末が所属する VLAN ID が登録されていることを確認してください。 【ダイナミック VLAN モード】【レガシーモード】 • MAC アドレスと認証後 VLAN ID が登録されていることを確認してください。 • 上記以外で固定 VLAN モードまたはダイナミック VLAN モードの場合は項番 5 へ。 • 上記に該当しない場合は項番 6 へ。
3	RADIUS サーバに MAC アドレスが登録されているかを確認してください。	• RADIUS サーバのユーザ ID として，MAC アドレスが登録されていない場合は，RADIUS サーバに登録してください。 • ユーザ ID およびパスワードに MAC アドレスが登録されている場合は，MAC アドレスの値を確認してください。 また，MAC アドレス形式が，コンフィグレーションコマンド mac-authentication id-format の設定と一致しているか確認してください。 • パスワードに任意文字列を登録している場合は，コンフィグレーションコマンド mac-authentication password で設定した文字列と一致しているか確認してください。 【固定 VLAN モード】 • RADIUS サーバの NAS-Identifier の VLAN ID が認証対象端末が所属する VLAN ID と一致しているか確認してください。 • コンフィグレーションコマンド mac-authentication vlan-check を設定している場合は，ユーザ ID の登録文字列が mac-authentication vlan-check で設定した区切り文字列および VLAN ID と一致しているか確認してください。 【ダイナミック VLAN モード】 • RADIUS サーバの VLAN ID と認証対象ポートのコンフィグレーションコマンド switchport mac vlan※1 の VLAN ID が一致しているか確認してください。 • RADIUS サーバに VLAN 名称で登録している場合は，該当 VLAN のコンフィグレーションコマンド name※2 と一致しているか確認してください。

項番	確認内容・コマンド	対応
		【レガシーモード】 • RADIUS サーバの VLAN ID と，コンフィグレーションコマンド mac-authentication vlan および認証対象端末接続ポートのコンフィグレーションコマンド switchport mac vlan の VLAN ID が一致しているか確認してください。 • RADIUS サーバに VLAN 名称で登録している場合は，該当 VLAN のコンフィグレーションコマンド name※2 と一致しているか確認してください。 • 上記に該当しない場合は項番 4 へ。
4	運用コマンド show mac-authentication statistics で RADIUS サーバとの通信状態を確認してください。	• 表示項目 "[RADIUS frames]" の "TxTotal" の値が "0" の場合は，下記のコンフィグレーションが正しく設定されているか確認してください。 aaa authentication mac-authentication default mac-authentication radius-server host または radius-server host • 固定 VLAN モードまたはダイナミック VLAN モードの場合は項番 5 へ。 • 上記に該当しない場合は項番 6 へ。
5	認証専用 IPv4 アクセスリストの設定を確認してください。	【固定 VLAN モード】【ダイナミック VLAN モード】 • 認証前状態の端末から本装置外に特定のパケット通信を行う場合，認証専用 IPv4 アクセスリストが設定されていることを確認してください。 また，認証対象ポートに通常のアクセスリストと認証専用 IPv4 アクセスリストの両方を設定した場合，認証専用 IPv4 アクセスリストに設定したフィルタ条件が通常のアクセスリストにも設定されていることを確認してください。 • 認証専用 IPv4 アクセスリストのフィルタ条件の宛先 IP アドレスに，any が設定されていないことを確認してください。 • 上記に該当しない場合は項番 6 へ。
6	運用コマンド show mac-authentication statistics で MAC 認証の統計情報が表示されるかを確認してください。	• MAC 認証の統計情報が表示されない場合は項番 7 へ。 • 上記に該当しない場合は項番 8 へ。
7	コンフィグレーションコマンド mac-authentication system-auth-control が設定されているかを確認してください。	• コンフィグレーションコマンド mac-authentication system-auth-control が設定されていない場合は，設定してください。 • 上記に該当しない場合は項番 8 へ。
8	運用コマンド show mac-authentication logging を実行し，動作に問題がないかを確認してください。	動作ログ種別 LOGIN で，下記の動作ログが表示されている合は認証に失敗しています。 • 「Login failed：xxxxxxxxxxx」 動作ログ内容を確認して，RADIUS サーバ，内蔵 MAC 認証 DB，コンフィグレーションなどの設定内容を見直してください。 動作ログ内容は，運用コマンドレファレンスを参照してください。 【固定 VLAN モード】【ダイナミック VLAN モード】 • 認証端末が接続されているポートの認証情報が表示されない場合は，コンフィグレーションコマンド mac-authentication port で認証対象ポートが正しく設定されているか確認してください。
		【MAC 認証共通】 • 端末が接続されている認証対象ポートがリンクダウンまたはシャットダウンしていないことを確認してください。 • 上記以外の場合は，MAC 認証のコンフィグレーションを確認してください。

注※ 1

コンフィグレーションコマンド switchport mac vlan 未設定のときは，コンフィグレーションコマンド vlan の mac-based で，RADIUS サーバの VLAN ID が設定されているか確認してください。

注※ 2

コンフィグレーションコマンド name で設定する VLAN 名称を，RADIUS 認証の認証後 VLAN として使用するときは下記に注意してください。

- VLAN 名称が，複数の VLAN で重複しないように設定してください。VLAN 名称が重複していると，重複しているうちで最も小さい VLAN ID が RADIUS 認証の認証後 VLAN として割り当てられます。
- VLAN 名称の先頭に数字を指定しないでください。先頭の数字を VLAN ID として認識し，認証に失敗する場合があります。

MAC 認証に関係するコンフィグレーションは次の点を確認してください。

表 3-25 MAC 認証のコンフィグレーションの確認

項番	確認内容・コマンド	対応
1	MAC 認証のコンフィグレーション	次のコンフィグレーションコマンドが正しく設定されていることを確認してください。 【MAC 認証共通】 • aaa authentication mac-authentication default group radius • mac-authentication access-group • mac-authentication auto-logout • mac-authentication id-format • mac-authentication interface • mac-authentication max-timer • mac-authentication password • mac-authentication system-auth-control 【固定 VLAN モード】 • mac-authentication port • mac-authentication static-vlan max-user • mac-authentication vlan-check • authentication arp-relay • authentication ip access-group 【ダイナミック VLAN モード】 • mac-authentication port • mac-authentication max-user • authentication arp-relay • authentication ip access-group 【レガシーモード】 • mac-authentication max-user • mac-authentication vlan
2	VLAN インタフェースの設定	【固定 VLAN モード】 対象 VLAN インタフェースに IP アドレスが正しく設定されていることを確認してください。 【ダイナミック VLAN モード】【レガシーモード】 次の各 VLAN インタフェースに IP アドレスが正しく設定されていることを確認してください。 • 認証前 VLAN • 認証後 VLAN
3	フィルタ設定	フィルタによって特定のパケットが廃棄されているか，または QoS 制御のシェーパによってパケットが廃棄されている可能性があります。コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築でのシェーパのシステム運用が適切であるかを確認してください。手順については「3.14.1 フィルタ・QoS 設定情報の確認」を参照してください。

項番	確認内容・コマンド	対応
4	認証専用 IPv4 アクセスリストの設定	【固定 VLAN モード】【ダイナミック VLAN モード】 認証前状態の端末から本装置外に通信するために必要なフィルタ条件が，コンフィグレーションコマンド authentication ip access-group および ip access-list extended で正しく設定されていることを確認してください。
5	ARP パケット中継の設定	【固定 VLAN モード】【ダイナミック VLAN モード】 認証前状態の端末から本装置外の機器宛に ARP パケットを通信させるためのコンフィグレーションコマンド authentication arp-relay が正しく設定されていることを確認してください。

3.7.4 セキュア Wake on LAN 使用時の通信障害【OP-WOL】

セキュア Wake on LAN 使用時の障害については，次の表に示す障害解析に従って原因の切り分けを行ってください。

- 起動コマンド送信端末登録用内蔵 DB：WOL 端末 DB
- ユーザ認証用内蔵 DB：WOL ユーザ DB

表 3-26　セキュア Wake on LAN の障害解析方法

項番	確認内容・コマンド	対応
1	端末にセキュア Wake on LAN 用ユーザ認証画面が表示されるか確認してください。	ユーザ認証画面が表示されない場合：項番 2 へ。
		ユーザ認証画面が表示される場合： • ユーザ認証できない　項番 3 へ。 • ユーザ認証できる 端末選択＆起動コマンド送信画面に「Not available.」表示　項番 5 へ。 起動コマンド送信後，端末起動確認できない　項番 6 へ。
2	ユーザ認証画面の URL が間違っていないか確認してください。	ユーザ認証画面の URL が違っている場合は，正しい URL を使用してください。URL の IP アドレスは，セキュア Wake on LAN で使用する VLAN の IP アドレスを指定してください。
3	運用コマンド show wol-authentication user でユーザ情報が登録されているか確認してください。	ユーザ未登録の場合，運用コマンド set wol-authentication user で登録してください。 ユーザ ID が間違っている場合は，運用コマンド remove wol-authentication user で削除してから，運用コマンド set wol-authentication user で正しいユーザ ID を登録してください。 変更後は，運用コマンド commit wol-authentication で運用に反映してください。 上記に該当しない場合は，項番 4 へ。
4	運用コマンド show wol で使用しているユーザ数を確認してください。	本機能の同時使用ユーザ数は最大 32 です。最大使用ユーザ数を超えているときは使用できません。ほかのユーザの処理が終了するまでしばらくお待ちください。
5	運用コマンド show wol-authentication user で該当ユーザ ID と detail オプションを指定し，端末アクセス権と端末名を確認してください。	該当ユーザのエントリに「*」が表示されている場合： 端末名が WOL 端末 DB に登録されていません。運用コマンド show wol-device name で端末名を確認し，運用コマンド set wol-authentication permit で変更してください。変更後は，運用コマンド commit wol-authentication で運用に反映してください。

項番	確認内容・コマンド	対応
6	運用コマンド show wol-device name でWOL 端末 DB の登録内容を確認してください。	端末名，端末の MAC アドレス，端末の所属する VLAN 情報が間違っていないか確認してください。間違っていると起動コマンドが送信されません。 • 間違っていた場合： 運用コマンド set wol-device mac，set wol-device vlan で変更してください。変更後は，運用コマンド commit wol-device で運用に反映してください。 • 間違っていない場合：項番 7 へ。
7	運用コマンド show wol-device name で端末の Alive 表示を確認してください。	• no-check を表示： 起動確認なしで登録されています。運用コマンド set wol-device alive で起動確認ありに変更し，運用コマンド set wol-device ip で IP アドレス情報※を追加してください。変更後は，運用コマンド commit wol-device で運用に反映してください。 注※ IP アドレス情報 DHCP クライアントの場合： dhcp を設定し，本装置の DHCP snooping も設定 固定 IP アドレス端末の場合： 端末の IP アドレスを設定 • 上記に該当しない場合は，項番 8 へ。
8	起動確認ありのとき，IP アドレス情報を確認してください。	• DHCP クライアントの場合： dhcp を登録していること 本装置の DHCP snooping も設定していること • 固定 IP アドレス端末の場合： 端末の IP アドレスを登録していること 設定が間違っている場合は，運用コマンド set wol-device ip で変更してください。変更後は，運用コマンド commit wol-device で運用に反映してください。 • IP アドレス情報が正しい場合は，項番 9 へ。
9	運用コマンド show running-config で VLAN インタフェースの設定情報を確認してください。	端末が所属している VLAN に IP アドレスが設定されているか確認してください。 未設定の場合は，IP アドレスを設定してください。

3.8　セキュリティ機能の通信障害

3.8.1　DHCP snooping 機能使用時の障害

(1) DHCP クライアント端末から通信ができない場合

DHCP snooping 機能を使用時に，DHCP クライアント端末から通信ができない場合は，次の表に従って対処してください。

表 3-27　DHCP クライアント端末から通信ができない場合の対処方法

項番	確認内容・コマンド	対応
1	運用コマンド show ip dhcp snooping binding でバインディングデータベースに該当端末の IP アドレスと MAC アドレスが登録されているか確認してください。	登録されている場合，項番 4 へ。
		登録されていない場合，項番 2 へ。
2	DHCP サーバおよび DHCP クライアント端末の接続を確認してください。	DHCP サーバが trust ポートに接続されているか確認してください。untrust ポートに接続されている場合は，trust ポートに接続しなおしてください。
		DHCP クライアント端末が untrust ポートに接続されているか確認してください。trust ポートに接続されている場合は，untrust ポートに接続しなおしてください。
		接続があっている場合，項番 3 へ。
3	DHCP クライアント端末側で，IP アドレスの解放を実行してみてください。	本装置が電源 OFF/ON などで再起動した可能性があります。IP アドレスの解放を実行してください。 例）Windows の場合は，コマンドプロンプトから，ipconfig /release を実行した後に，ipconfig /renew を実行してください。
4	フィルタやレイヤ 2 認証機能の設定が正しいか確認してください。	フィルタによって特定のパケットが廃棄されている，または端末を接続しているポートや VLAN がレイヤ 2 認証機能の対象のため，認証されていない可能性があります。 コンフィグレーションのフィルタやレイヤ 2 認証機能の設定条件が正しいか確認してください。

(2) バインディングデータベースを保存できない場合

DHCP snooping 機能使用時に，バインディングデータベースを保存できない場合は，次の表に従って対処してください。

(a) 内蔵フラッシュメモリに保存できない

表 3-28 バインディングデータベースの保存先が内蔵フラッシュメモリの場合

項番	確認内容・コマンド	対応
1	運用コマンド show ip dhcp snooping binding で保存時間を確認してください。	Agent URL に " － " を表示している場合は，項番２へ。
		保存契機※から，コンフィグレーションで設定した書き込み指定時間※が経過していないため，保存を実施していない可能性があります。しばらくおまちください。
		保存契機※から，書込み指定時間※が満了している場合で Last succeeded time：－　の場合は，項番３へ。 Last succeeded time：時間が保存契機より以前の時間の場合は，項番３へ。
2	運用コマンド show running-config でコンフィグレーションを確認してください。	ip dhcp snooping database url flash が設定されている場合は，項番３へ。
		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 ip dhcp snooping database url flash を設定してください。
3	装置正面の ST1 LED の状態と，運用コマンド show logging でバインディングデータベース保存の運用ログを確認してください。	ST1 LED が赤点滅状態で,「It was not able to store binding database in flash.」が採取されている場合は，下記の手順で保存先を MC に変更してみてください。 1. コンフィグレーションコマンド ip dhcp snooping database url で保存先を MC に変更します。 2. save コマンドでコンフィグレーションを保存します。 3. 装置に MC を挿入します。 4. 装置を再起動してください。 5. 保存先を再び内蔵フラッシュメモリに戻します。 6. save コマンドでコンフィグレーションを保存します。 7. 装置を再起動してください。 項番４へ。
4	再起動後，再度装置正面の ST1 LED の状態と，運用コマンド show logging でバインディングデータベース保存の運用ログを確認してください。	項番３と同じだった場合は，内蔵フラッシュメモリが壊れている可能性があります。下記の手順で装置を交換してください。 1. 運用コマンド backup を実行します。 （このとき MC 内には，運用コマンド backup で指定したファイルと，項番３の対応で保存したコンフィグレーションコマンド ip dhcp snooping database url mc で指定したファイルが保存されています。） 2. 装置を交換します。 3. 交換した装置に MC を挿入します。 4. 運用コマンド restore を実行します。（運用コマンド backup でバックアップした内容が装置に復元されます。） 5. コンフィグレーションコマンド ip dhcp snooping database url で保存先を MC に変更します。 6. save コマンドでコンフィグレーションを保存します。 7. 装置を再起動します。MC 内のバインディングデータベースが復元されます。

注※
保存契機および書き込み指定時間については，「コンフィグレーションガイド Vol.2」を参照してください。

(b) MC に保存できない

表 3-29 バインディングデータベースの保存先が MC の場合

項番	確認内容・コマンド	対応
1	運用コマンド show ip dhcp snooping binding で保存時間を確認してください。	Agent URL に " − " を表示している場合は，項番 2 へ。
		保存契機※から，コンフィグレーションで設定した書き込み指定時間※が経過していないため，保存を実施していない可能性があります。しばらくおまちください。
		保存契機※から，書込み指定時間※が満了している場合で Last succeeded time : −　の場合は，項番 3 へ。 Last succeeded time : 時間が保存契機より以前の時間の場合は，項番 3 へ。
2	運用コマンド show running-config でコンフィグレーションを確認してください。	ip dhcp snooping database url mc が設定されている場合は，項番 3 へ。
		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 ip dhcp snooping database url mc < 保存ファイル名 > を設定してください。
3	運用コマンド show logging でバインディングデータベース保存の運用ログを確認してください。	「It was not able to store binding database in mc.<retry> <reason>」がある場合は，MC への保存に失敗しています。
		<reason> に「MC file is not inserted.」が表示されている場合は，MC が挿入されていないか，半挿し状態の可能性があります。 未挿入の場合は MC を挿入してください。 MC を挿入している場合は，いったん MC を取り外し，「カチッ」と音がするまで挿入してください。（挿入時は強く押したり，指ではじいたりしないでください。） 項番 5 へ。
		<reason> に「Can't access to MC by write protection.」が表示されている場合は，MC が書き込み禁止状態になっています。 MC をいったん外して，スイッチを「▼ Lock」状態と逆側に動かして書き込み禁止状態を解除し，再度装置に挿入してください。（挿入時は強く押したり，指ではじいたりしないでください。） 項番 5 へ。
		<reason> に「MC file is not writing.」が表示されている場合は，空き容量不足の可能性があります。 項番 4 へ。
4	運用コマンド show mc で MC の空き容量を確認してください。	1 M バイト以下の場合は，運用コマンド del で不要なファイルを削除してから，再度実行してください。 項番 5 へ。
5	運用コマンド backup を実行し，バックアップ終了後に運用コマンド show mc-file を実行してみてください。	運用コマンド backup で指定したファイルのほかに，コンフィグレーションコマンド ip dhcp snooping database url mc で指定したファイルがあれば，バインディングデータベースが保存されています。 保存されていなかった場合は，MC が壊れている可能性があります。 項番 6 へ。

項番	確認内容・コマンド	対応
6	運用コマンド format mc を実行してみてください。	何もメッセージが表示されず，プロンプトのみ表示された場合は，MC のフォーマットは正常終了しています。 項番 5 を実行してみてください。
		「Can't gain access to MC」が表示された場合は，MC をいったん取り出し，MC および MC スロットにほこりなど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場合は，乾いた布でほこりを取ってから，再度 MC をスロットに挿入してください。 挿入後，再度運用コマンド format mc を実行してください。
		「Can't execute」が表示された場合は，MC をいったん取り出し，MC および MC スロットにほこりなど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場合は，乾いた布でほこりを取ってから，再度 MC をスロットに挿入してください。 挿入後，再度運用コマンド format mc を実行してください。 同じメッセージが表示された場合は，MC が壊れている可能性があります。別の MC に交換してください。

注※
保存契機および書き込み指定時間については，「コンフィグレーションガイド Vol.2」を参照してください。

(3) バインディングデータベースを復元できない場合

DHCP snooping 機能使用時に，バインディングデータベースを復元できない場合は，次の表に従って対処してください。

(a) 内蔵フラッシュメモリから復元できない

表 3-30 バインディングデータベースの保存先が内蔵フラッシュメモリの場合

項番	確認内容・コマンド	対応
1	運用コマンド show ip dhcp snooping binding で保存時間を確認してください。	Agent URL に " − " を表示している場合は，項番 2 へ。
		Last succeeded time の保存時間が古すぎる場合は，項番 3 へ。
2	運用コマンド show running-config でコンフィグレーションを確認してください。	ip dhcp snooping database url flash が設定されている場合は，項番 3 へ。
		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 ip dhcp snooping database url flash を設定してください。
3	運用コマンド show logging でバインディングデータベース復元の運用ログを確認してください。	「It was not able to restore binding database from flash.」がある場合，復元に失敗しています。 内蔵フラッシュメモリに保存したバインディングデータベースが壊れている可能性があります。 DHCP クライアント端末側で IP アドレスの解放を実行してください。(Windows の場合は，コマンドプロンプトから ipconfig/release, ipconfig/renew を実行)

(b) MC から復元できない

表 3-31 バインディングデータベースの保存先が MC の場合

項番	確認内容・コマンド	対応
1	運用コマンド show ip dhcp snooping binding で保存時間を確認してください。	Agent URL に " − " を表示している場合は，項番 2 へ。
		Last succeeded time の保存時間が古すぎる場合は，項番 3 へ。
2	運用コマンド show running-config でコンフィグレーションを確認してください。	ip dhcp snooping database url mc が設定されている場合は，項番 3 へ。
		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 ip dhcp snooping database url mc < 保存ファイル名 > を設定してください。
3	運用コマンド show logging でバインディングデータベース復元の運用ログを確認してください。	「It was not able to restore binding database from mc.<retry><reason>」がある場合，MC からの復元に失敗しています。
		<reason> に「MC is not inserted.」が表示されている場合は，MC が挿入されていないか，半挿し状態の可能性があります。 未挿入の場合は MC を挿入してください。 MC を挿入している場合は，いったん MC を取り外し，「カチッ」と音がするまで挿入してください。（挿入時は強く押したり，指ではじいたりしないでください。） 項番 4 へ。
		<reason> に「MC file is not found.」が表示されている場合は，ファイルの入っていない MC を挿入しているか，コンフィグレーションコマンド ip dhcp snooping database url mc で指定したファイル名と異なるファイルの MC が挿入されています。 バインディングデータベースを保存した MC に交換してください。 項番 4 へ。
		上記以外の <reason> が表示されている場合は，MC からの復元に失敗しています。 項番 4 へ。
4	装置を再起動してみてください。	<reason> に「MC file is not reading.」が表示されている場合は，MC に保存したファイルまたは MC が壊れている可能性があります。 DHCP クライアント端末側で IP アドレスの解放を実行してください。（Windows の場合は，コマンドプロンプトから ipconfig/release，ipconfig/renew を実行）

3.9 冗長構成による高信頼化機能の通信障害

3.9.1 アップリンク・リダンダント使用時の通信障害

アップリンク・リダンダント使用時，意図したとおりに切り替えできないときは，次の表に示す障害解析に従って原因の切り分けを行ってください。

表 3-32 アップリンク・リダンダントの障害解析方法

項番	確認内容・コマンド	対応
1	運用コマンド show switchport backup でプライマリ・セカンダリペア情報を確認してください。	• ペア情報が表示されない：項番 2 へ。 • ペア情報が表示されている ・物理ポートのリンクダウン後，運用コマンド show switchport backup のポート Status 表示がすぐに変わらないとき：項番 3 へ。 ・プライマリポートのリンクアップ後，自動切り戻しまたはタイマ切り戻しができないとき：項番 4 へ。
2	運用コマンド show running-config でアップリンク・リダンダントの設定内容を確認してください。	セカンダリポートにポートチャネルインタフェースを指定： 該当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が設定されていない可能性があります。 該当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を確認し，未設定の場合は設定してください。
3	該当ポートのリンクデバウンス設定を確認してください。	コンフィグレーションコマンド link debounce 未設定（デフォルト 2000 ミリ秒で動作）または 2000 ミリ秒より長い設定のときは，短い時間に変更してみてください。
4	プライマリポートへ自動切り戻しまたはタイマ切り戻しができないとき，運用コマンド show switchport backup でプライマリポートの Status 表示を確認してください。	• Blocking 表示： ・Preemption の Delay に "－" を表示しているときは，自動切り戻しもタイマ切り戻しも未設定です。コンフィグレーションコマンド switchport backup interface で設定してください。 ・Preemption の Limit 時間が 0 以外のときは，切り戻しまでの時間に達していません。しばらくお待ちください。 または，運用コマンド select switchport backup interface を実行してみてください。 • Down 表示： リンクダウンしています。上位スイッチの状態やケーブル接続などを確認してください。 • 上記に該当しない場合は，項番 5 へ。
5	プライマリポートの上位スイッチでスパニングツリーが動作していないか確認してください。	スパニングツリーが動作している場合は，リンクダウンから復帰すると「Listening」または「Learning」状態となるため，すぐには通信できません。上位スイッチでスパニングツリーを動作しているときは，タイマ切り戻し時間を 30 秒以上に設定してご使用ください。 上記に該当しない場合は，項番 6 へ。
6	上位スイッチがフラッシュ制御フレームを受信可能か確認してください。	受信可能の場合：項番 7 へ。 受信不可の場合：項番 8 へ。
7	本装置のフラッシュ制御フレーム送信設定を確認してください。	• 未設定の場合： 上位スイッチの MAC アドレステーブルがエージングされるまでしばらくお待ちください。 • 設定済みの場合： フラッシュ制御フレーム送信を設定したポートおよび送信 VLAN の設定内容を確認してください。間違っていた場合は，設定しなおしてください。

項番	確認内容・コマンド	対応
8	本装置の MAC アドレスアップデートフレームの送信設定を確認してください。	• 未設定の場合： 上位スイッチの MAC アドレステーブルがエージングされるまでしばらくお待ちください。 • 設定済みの場合： ・端末接続ポートで MAC アドレスを学習した VLAN が，アップリンクポートに含まれているか確認してください。含まれていない場合は，設定しなおしてください。 ・アップリンクポートのペア（プライマリ・セカンダリ）に，同じ VLAN を設定しているか確認してください。違っていた場合は，同じ VLAN を設定しなおしてください。 上記に該当しない場合は，項番 9 へ。
9	運用コマンド show switchport backup mac-address-table update statistics で "Transmission over flows" が計上されているか確認してください。	計上されている場合は，MAC アドレスアップデートフレームの対象 MAC アドレスが 1,024 件を超えています。 • 対象外 MAC アドレスを VLAN 単位で削減できる場合 対象外 VLAN を設定してください。 • 対象外 VLAN を設定できない場合 上位スイッチの MAC アドレステーブルがエージングされるまでしばらくお待ちください。

3.10 SNMP の通信障害

3.10.1 SNMP マネージャから MIB の取得ができない

コンフィグレーションが正しく登録されていることを確認してください。

SNMPv1，または SNMPv2c を使用する場合

運用コマンド show running-config を実行し，コミュニティ名とアクセスリストが正しく登録されているかどうかを確認してください。アクセスを許可する SNMP マネージャの IP アドレスを制限しない場合は，アクセスリストの設定は不要です。

登録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。

```
# show running-config
  :
  :
ip access-list standard SNMPMNG
  permit host 128.1.1.2

snmp-server community "NETWORK" ro SNMPMNG

#
```

3.10.2 SNMP マネージャでトラップが受信できない

コンフィグレーションが正しく登録されていることを確認してください。

SNMPv1，または SNMPv2c を使用する場合

運用コマンド show running-config を実行し，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登録されているかどうかを確認してください。

登録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。

```
# show running-config
  :
  :
snmp-server host 20.1.1.1 traps "event-monitor" snmp

#
```

3.11　隣接装置管理機能の通信障害

3.11.1　LLDP 機能により隣接装置情報が取得できない

LLDP 機能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の切り分けを行ってください。

表 3-33　LLDP 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	運用コマンド show lldp を実行し，LLDP 機能の動作状態を確認してください。	Status が Enabled の場合は項番 2 へ。
		応答メッセージ「LLDP is not configured」を表示した場合は，LLDP 機能が停止状態となっています。LLDP 機能を有効にしてください。
2	運用コマンド show lldp を実行し，ポート情報を確認してください。	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 機能の動作対象外となっています。該当ポートに対し LLDP 機能を有効にしてください。
3	運用コマンド show lldp statistics を実行し，隣接装置が接続されているポートの統計情報を確認してください。	Tx カウントは増加し Rx カウントが増加しない場合は，隣接装置側でも項番 1 から項番 3 を調査してください。隣接装置側でも Tx カウント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ので接続を確認してください。
		Discard カウントが増加している場合は，装置間の接続を確認してください。
		その他の場合は項番 4 へ。
4	運用コマンド show lldp を実行し，隣接装置が接続されているポート情報のポート状態を確認してください。	Link が Up 状態の場合は項番 5 へ。
		Link が Down 状態の場合は回線状態を確認してください。確認方法は「3.4　ネットワークインタフェースの通信障害」を参照してください。
5	運用コマンド show lldp を実行し，隣接装置が接続されているポートの隣接装置情報数を確認してください。	• Neighbor Counts が 0 の場合は隣接装置側で項番 1 から項番 5 を調査してください。隣接装置側でも隣接装置情報数が 0 の場合は，装置間の接続が誤っている可能性があるので接続を確認してください。 • フィルタによって特定のパケットが廃棄されているか，または QoS 制御のシェーパによってパケットが廃棄されている可能性があります。コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築でのシェーパのシステム運用が適切であるかを確認してください。手順については「3.14.1　フィルタ・QoS 設定情報の確認」を参照してください。

3.12　NTP の通信障害

3.12.1　NTP サーバから時刻情報が取得できない

NTP サーバから時刻情報が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の切り分けを行ってください。

表 3-34　NTP の障害解析方法

項番	確認内容・コマンド	対応
1	運用コマンドshow clockでタイムゾーンの設定があることを確認してください。	コマンドの表示結果にタイムゾーンが設定されている場合は項番 2 へ。
		コマンドの表示結果にタイムゾーンが設定されていない場合はタイムゾーンの設定をしてください。
2	運用コマンド show ntp-client で NTP サーバからの取得状況を確認してください。	「NTP Execute History」の最も新しい履歴の Status が”Timeout”または”Error”を表示している場合は，項番 3 へ。
3	NTP サーバとの IPv4 による通信を確認してください。	NTP サーバと本装置間で IPv4 の通信が可能か，運用コマンド ping で確認してください。

3.13 IEEE802.3ah/UDLD 機能の通信障害

3.13.1 IEEE802.3ah/UDLD 機能でポートが inactive 状態となる

IEEE802.3ah/UDLD 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の切り分けを行ってください。

表 3-35 IEEE802.3ah/UDLD 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	運用コマンド show efmoam を実行し，IEEE802.3ah/UDLD 機能で inactive 状態にしたポートの生涯種別を確認してください。	Link status に "Down" が表示されている場合は項番 2 へ。
2	対向装置でIEEE802.3ah/OAM機能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 機能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 機能が有効となっている場合は項番 3 へ。
3	運用コマンド show efmoam statistics を実行し，Thrashings を確認してください。	• Thrashings がカウントアップし続ける場合は，禁止構成（接続先が複数）となっています。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。 • Thrashings 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 HUB 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ネットワーク構成を見直してください。どうしても中継装置が必要な場合は，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。（ただし，推奨はしません） • 直接接続されている場合は項番 5 へ。
5	運用コマンド show efmoam 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 が初期値未満の場合，実際に障害となっていない場合でも片方向リンク障害を誤検出する可能性が高まります。この値を変更してください。 • udld-detection-count が初期値以上の場合は項番 6 へ。
6	フィルタ・QoS 制御の設定を確認してください。	• フィルタまたは QoS 制御によって IEEE802.3ah/UDLD 機能で使用する制御フレーム（slow-protocol）が廃棄されている可能性があります。「3.14.1 フィルタ・QoS 設定情報の確認」を参照してください。 • 問題がない場合は項番 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。

注 IEEE802.3ah/OAM：IEEE802.3ah で規定されている OAM プロトコル
IEEE802.3ah/UDLD：IEEE802.3ah/OAM を使用した片方向リンク障害検出機能

3.14　フィルタ・QoS 設定で生じる通信障害

3.14.1　フィルタ・QoS 設定情報の確認

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，フィルタによって特定のパケットが廃棄されているか，または QoS 制御のシェーパによってパケットが廃棄されている可能性が考えられます。

フィルタおよび QoS 制御によって本装置内でパケットが廃棄されている場合に，廃棄個所を特定する方法の手順を次に示します。

（1） フィルタによるパケット廃棄の確認方法

1. 本装置にログインします。
2. 運用コマンド show access-filter を実行し，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。
3. ２で確認したフィルタ条件と通信できないパケットの内容を比較して，該当パケットを廃棄していないか確認します。通信できないパケットの内容が，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，暗黙的に廃棄している可能性があります。
4. フィルタのコンフィグレーションの設定条件が正しいかを見直してください。

（2） QoS 制御のシェーパによるパケット廃棄の確認方法

1. 本装置にログインします。
2. 運用コマンド show qos queueing を使って，出力インタフェースの統計情報の "discard packets" を確認してください。
3. シェーパのシステム運用が適切であるかを見直してください。

3.15　ポートミラーリングの障害

3.15.1　ミラーポートから BPDU が送出される

ポートミラーリング機能で，ミラーポートからの BPDU 送出を止める場合は，ミラーポートに BPDU フィルタ機能（コンフィグレーションコマンド spanning-tree bpdufilter）を設定してください。

3.16　省電力機能の障害

3.16.1　LED 輝度が動作しない

省電力運用中の LED 輝度の動作で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 3-36　省電力運用のトラブルおよび対応

項番	確認内容・コマンド	対応
1	ポートがリンクアップしても LED が点灯しない。	次の手順で確認してください。 1. 運用コマンド show system で「Brightness mode」表示を確認してください。 • 「off」を表示： LED 動作は消灯設定となっています。 • 「economy」を表示：【SS1250】【SS1240】 LED 動作は省電力輝度設定となっています。 2. 運用コマンド show power-control schedule で，スケジュール時間帯に入っていないか確認してください。 • スケジュール時間帯に入っている場合 コンフィグレーションコマンド schedule-power-control port-led で enable を設定してください。 • 通常時間帯の場合 コンフィグレーションコマンド system port-led で enable を設定してください。
2	ポートがリンクアップしても LED が通常輝度で点灯しない（自動動作しない）。	運用コマンド show system で「Brightness mode」表示を確認してください。 • 「normal」を表示： LED 動作は通常輝度設定となっています。コンフィグレーションコマンド system port-led trigger の設定を確認してください。 system port-led trigger に interface 未設定の場合は，自動動作の契機に物理ポートが指定されていません。物理ポートを自動動作の契機として設定してください。 • 上記以外： コンフィグレーションの設定を見直してください。
3	MC を挿抜しても LED が通常輝度で点灯しない（自動動作しない）。	運用コマンド show system で「Brightness mode」表示を確認してください。 • 「normal」を表示： LED 動作は通常輝度設定となっています。コンフィグレーションコマンド system port-led trigger の設定を確認してください。 system port-led trigger に mc 未設定の場合は，自動動作の契機に MC の挿抜が指定されていません。MC の挿抜を自動動作の契機として設定してください。 • 上記以外： コンフィグレーションの設定を見直してください。
4	コンソール（RS-232C）でログインしても LED が通常輝度で点灯しない（自動動作しない）。	運用コマンド show system で「Brightness mode」表示を確認してください。 • 「normal」を表示： LED 動作は通常輝度設定となっています。コンフィグレーションコマンド system port-led trigger の設定を確認してください。 system port-led trigger に console 未設定の場合，自動動作の契機にコンソールが指定されていません。コンソールを自動動作の契機として設定してください。 • 上記以外： コンフィグレーションの設定を見直してください。

3.16.2　省電力機能スケジューリングが動作しない

省電力スケジューリングの実施で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 3-37　省電力スケジューリングのトラブルおよび対応

項番	確認内容・コマンド	対応
1	スケジュール実行時間帯になっても装置スリープしない。 【SS1250】【SS1240】	本装置にログインしているユーザ（シリアル・telnet）が，コンフィグレーションコマンドモードで操作していないか確認してください。 該当ユーザがいる場合は，設定内容を保存してコンフィグレーションコマンドモードを終了してください。
		スケジュール時間帯の設定（schedule-power-control time-range）が，action disable になっていないか確認してください。 該当する場合は，action enable に変更して保存してください。
2	スリープ期間終了後の装置が設定したコンフィグで動作していない。 【SS1250】【SS1240】	スケジューリングで装置スリープを実行すると，保存していないコンフィグレーションは破棄されます。 コンフィグレーションを再設定し，save コマンドで必ず保存してください。
3	臨時で装置スリープを解除したい。 【SS1250】【SS1240】	装置の RESET スイッチを正面 LED が全点灯するまで（3秒以上）長押ししてください。 なお，スリープ解除後はスケジュール抑止モードになっています。スリープ解除後，スケジュール適用モードに戻すときは，運用コマンド set power-control schedule enable を実行してください。

3.17 温度監視対応時の障害

3.17.1 温度履歴情報の日付が正しく表示されない

運用コマンド show environment temperature-logging で，途中で採取日時が抜けている場合，次の事象が発生した可能性があります。

1. 内蔵フラッシュメモリに温度履歴情報を保存中に，本装置の電源 OFF/ON などの装置再起動操作が行われ，温度履歴情報を保存できなかった。
2. 本装置の時刻設定が変更され，収集時刻が以前の履歴情報よりも古くなった。

温度履歴情報の採取は停止していませんので，継続してご使用ください。

4 障害情報取得方法

この章では，主に障害情報取得作業を行うときの作業手順について説明しています。

4.1　障害情報の取得

運用コマンド show tech-support を使用して，障害発生時の情報採取を一括して採取できます。

運用コマンド show tech-support で画面に情報を表示すると，数十分以上かかる場合があります。下記に説明するように RAMDISK に保存し，MC に書き込むか FTP で転送することをお勧めします。

本コマンドでは，採取した障害情報を RAMDISK にテキスト形式で保存し，MC に書き込んだり，FTP で転送したりすることができます。

図 4-1　show tech-support で採取した情報を RAMDISK に保存

```
# show tech-support ramdisk
```

ファイルは showtech.txt というファイル名で保存されます。MC への書き込みについては，「4.2　MC への書き込み」を参照してください。FTP での転送については，「4.3　FTP によるファイル転送」を参照してください。なお，運用コマンド show tech-support ramdisk を実行する前に，あらかじめ RAMDISK のファイルやディレクトリを削除しておくことをお勧めします。

4.2 MC への書き込み

RAMDISK にコピーした障害情報は 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。運用端末で装置の情報を MC に書き込みます。

図 4-2 MC への情報書き込み

```
書き込むためのMCを装置に挿入する。

運用コマンドshow ramdisk-file でコピー元ファイル(showtech.txt)の容量を確認する。
> show ramdisk-file

Date 2008/11/13 10:19:31 UTC
    File Date               Size Name
    2008/11/13 10:15       1,265 showtech.txt

>

運用コマンドshow mcで空き容量を確認する。
>show mc

Date 2008/11/13 10:19:51 UTC
    MC : enable
    Manufacture ID : 00000003
       used      5,750,272 byte
       free    120,160,256 byte   ←空き容量
       total   125,910,528 byte

>

運用コマンドcopyでコピー元ファイルをshowtech.txtというファイル名称でMCにコピーする。
> copy ramdisk showtech.txt mc showtech.txt

MCにファイルが書き込めていることを確認する。
> show mc-file

Date 2008/11/13 10:20:53 UTC
    File Date               Size Name
    2008/11/13 10:20       1,265 showtech.txt


>
```

4.3 FTP によるファイル転送

RAMDISK にコピーした障害情報は本装置に FTP でログインすることにより，リモート端末へ FTP でファイル転送することができます。

FTP で接続するポートに VLAN と IP アドレスを設定されていることを確認してください。

PC でコマンドプロンプト画面を開きます。（Windows 標準の PC の場合，「スタート」⇒「すべてのプログラム」⇒「アクセサリ」⇒「コマンドプロンプト」の順に開きます。）

下記は，PC の "C:\TEMP" に転送する操作例です。(本装置の IP アドレス：192.168.0.1 の場合)

図 4-3 FTP によるファイル転送

```
FTPクライアントPCから本装置にFTPでログインする。

C:\TEMP>ftp 192.168.0.1          ・・・・PC(FTPクライアント)から本装置にログイン
Connected to 192.168.0.1
220 AX1200 FTP server ready
User (192.168.0.1:(none)): operator
331 Password required
Password:
230 User logged in
ftp> asc
200 Type set to A, ASCII mode
ftp> get showteck.txt            ・・・・障害情報ファイルの転送
200 Port set okay
150 Opening ASCII mode data connection
226 Transfer complete
ftp:xxxxxx bytes sent in xx.x Seconds (xx.xx Kbytes/sec)
ftp> bye
221 Bye…see you later
C:\TEMP>

PC(FTPクライアント)に障害情報ファイルが転送されました。
```

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

運用コマンド show tech-support 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，表示内容の詳細については，マニュアル「運用コマンドレファレンス」を参照してください。次の表で「内容欄」に "OAN" と記載のあるコマンドについては，OAN のマニュアルを参照してください。

【注意】

運用コマンド show tech-support で表示される情報の一部については，マニュアル「運用コマンドレファレンス」に記載されません。これらの情報は装置の内部情報（次の表で「内容欄」に " 装置内部情報 " と記載のあるコマンド）を含んでいるため一般公開いたしません。
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	パラメータ指定なし
1	show clock	本装置に設定されている時刻	○
2	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	○
3	show system	装置の運用状態	○
4	show environment	FAN/ 電源 / 稼働時間情報	○
5	show environment temperature-logging	温度履歴情報	○
6	show running-config	運用中のコンフィグレーション	○
7	show startup-config	スタートアップコンフィグレーションファイル	○
8	show sessions	ログインセッション情報	○
9	show radius-server	RADIUS サーバ情報	○
10	show radius-server statistics	RADIUS サーバ統計情報	○
11	show radius-server statistics summary	RADIUS サーバ統計サマリ情報	○
12	show ntp-client	NTP クライアント情報	○
13	show power-control port	ポート省電力動作状態情報	○
14	show power-control schedule	省電力スケジュール情報	○
15	show mc-file	MC 内ファイル情報	○
16	show ramdisk-file	RAMDISK 内ファイル情報	○
17	show mc	MC 使用量	○
18	show ramdisk	RAMDISK 使用量	○
19	show critical-logging summary	装置障害ログ情報	○
20	show critical-logging	装置障害ログ詳細情報	○
21	show logging	運用ログ情報	○
22	show cpu (days/hours)	CPU 使用率（日単位，時単位）	○

項番	コマンド（表示）	内容	パラメータ指定なし
23	show cpu (minutes/seconds)	CPU 使用率（分単位，秒単位）	○
24	show memory summary	装置のメモリ使用情報	○
25	show interfaces	ポートの詳細統計情報	○
26	show port	ポート情報	○
27	show port statistics	ポートの統計情報	○
28	show port protocol	ポートのプロトコル情報	○
29	show port transceiver	ポートのトランシーバ情報	○
30	show power inline	PoE 情報	○
31	show channel-group summary	リンクアグリゲーション情報	○
32	show channel-group detail	リンクアグリゲーション詳細情報	○
33	show channel-group statistics	リンクアグリゲーション統計情報	○
34	show channel-group statistics lacp	リンクアグリゲーションの LACP 統計情報	○
35	show mac-address-table	MAC アドレステーブル情報	○
36	show mac-address-table learning-counter	MAC アドレステーブルの学習アドレス数	○
37	show vlan summary	VLAN 情報	○
38	show vlan detail	VLAN 詳細情報	○
39	show vlan mac-vlan	MAC VLAN 情報	○
40	show spanning-tree detail	スパニングツリーの詳細情報	○
41	show spanning-tree port-count	スパニングツリーの収容数	○
42	show spanning-tree statistics	スパニングツリーの統計情報	○
43	show axrp detail	Ring Protocol の詳細情報	○
44	show ip dhcp snooping	DHCP snooping 情報	○
45	show ip dhcp snooping binding	DHCP snooping のバインディングデータベース情報	○
46	show ip dhcp snooping statistics	DHCP snooping の統計情報	○
47	show ip arp inspection statistics	ダイナミック ARP 検査の統計情報	○
48	show igmp-snooping	IGMP snooping 情報	○
49	show igmp-snooping group	IGMP snooping のグループ情報	○
50	show igmp-snooping statistics	IGMP snooping の統計情報	○
51	show mld-snooping	MLD snooping 情報	○
52	show mld-snooping group	MLD snooping のグループ情報	○
53	show mld-snooping statistics	MLD snooping の統計情報	○
54	show ip interface	IP インタフェース情報	○
55	show ip arp	ARP 情報	○
56	show ip route	スタティックルート情報	○
57	show access-filter	フィルタ機能の統計情報	○
58	show qos-flow	QoS 制御機能の統計情報	○
59	show qos queueing	全ポートの送信キューの統計情報	○

項番	コマンド（表示）	内容	パラメータ指定なし
60	show authentication fail-list	レイヤ 2 認証で認証に失敗した端末の情報	○
61	show authentication logging	レイヤ 2 認証全体の動作ログ情報	○
62	show dot1x detail	IEEE802.1X の認証状態情報	○
63	show dot1x statistics	IEEE802.1X の統計情報	○
64	show dot1x logging	IEEE802.1X の動作ログ情報	○
65	show web-authentication	Web 認証の設定情報	○
66	show web-authentication html-files detail	Web 認証の認証画面ファイル登録情報	○
67	show web-authentication user edit	内蔵 Web 認証 DB の登録・変更内容	○
68	show web-authentication user commit	内蔵 Web 認証 DB の登録内容	○
69	show web-authentication login select-option detail	Web 認証で認証済みのユーザ詳細情報	○
70	show web-authentication login summary port	Web 認証で認証済みのユーザ情報（ポート単位）	○
71	show web-authentication login summary vlan	Web 認証で認証済みのユーザ情報（VLAN 単位）	○
72	show web-authentication logging	Web 認証の動作ログ情報	○
73	show web-authentication statistics	Web 認証の統計情報	○
74	show ip dhcp binding	DHCP サーバ情報の結合情報	○
75	show ip dhcp conflict	DHCP サーバで検出した衝突 IP アドレス情報	○
76	show ip dhcp server statistics	DHCP サーバの統計情報	○
77	show mac-authentication	MAC 認証の設定情報	○
78	show mac-authentication login select-option detail	MAC 認証で認証済みの端末詳細情報	○
79	show mac-authentication login summary port	MAC 認証で認証済みの端末情報（ポート単位）	○
80	show mac-authentication login summary vlan	MAC 認証で認証済みの端末情報（VLAN 単位）	○
81	show mac-authentication logging	MAC 認証の動作ログ情報	○
82	show mac-authentication statistics	MAC 認証の統計情報	○
83	show mac-authentication mac-address edit	内蔵 MAC 認証 DB の登録・変更内容	○
84	show mac-authentication mac-address commit	内蔵 MAC 認証 DB の登録内容	○
85	show authentication multi-step	マルチステップ認証の認証端末情報	○
86	show wol	セキュア Wake on LAN を使用しているユーザ情報	○
87	show wol-authentication user edit	セキュア Wake on LAN のユーザ認証用内蔵 DB 登録・変更内容	○
88	show wol-authentication user commit	セキュア Wake on LAN のユーザ認証用内蔵 DB 登録内容	○
89	show wol-device name edit	セキュア Wake on LAN の起動コマンド送信端末登録用内蔵 DB 登録・変更内容	○
90	show wol-device name commit	セキュア Wake on LAN の起動コマンド送信端末登録用内蔵 DB 登録内容	○

項番	コマンド（表示）	内容	パラメータ指定なし
91	show license	ライセンス情報	○
92	show gsrp aware	GSRP aware 情報	○
93	show switchport backup	アップリンク・リダンダントの情報	○
94	show switchport backup statistics	アップリンク・リダンダントのフラッシュ制御フレーム送受信機能の統計情報	○
95	show switchport backup mac-address-table update	アップリンク・リダンダントの MAC アドレスアップデート機能の設定情報	○
96	show switchport backup mac-address-table update statistics	アップリンク・リダンダントの MAC アドレスアップデート機能の統計情報	○
97	show efmoam	IEEE802.3ah/OAM 機能の情報	○
98	show efmoam statistics	IEEE802.3ah/OAM 機能の統計情報	○
99	show storm-control detail	ストームコントロールの情報	○
100	show loop-detection	L2 ループ検知機能の情報	○
101	show loop-detection logging	L2 ループ検知機能のログ情報	○
102	show loop-detection statistics	L2 ループ検知機能の統計情報	○
103	show cfm	CFM 情報	○
104	show cfm summary	CFM の詳細情報（MP や CFM ポートの収容数）	○
105	show cfm remote-mep	CFM のリモート MEP 情報	○
106	show cfm remote-mep detail	CFM のリモート MEP 詳細情報	○
107	show cfm fault	CFM の CC で検出した障害情報	○
108	show cfm fault detail	CFM の CC で検出した障害の詳細情報	○
109	show cfm l2traceroute-db	CFM の Linktrace データベース情報	○
110	show cfm l2traceroute-db detail	CFM の Linktrace データベースの詳細情報	○
111	show cfm statistics	CFM の統計情報	○
112	show lldp detail	LLDP 機能の隣接装置情報	○
113	show lldp statistics	LLDP 機能の統計情報	○
114	show auto-config	OAN：AUTOCONF 機能のステータス情報	○
115	show auto-config neighbor	OAN：AUTOCONF 機能の隣接情報	○
116	show config-lock-status	OAN：ロック機能の状態	○
117	show netconf	OAN：NETCONF 機能のステータス情報	○
118	show netconf denied-host	OAN：アクセス拒否状態情報	○
119	show software-update user	OAN：ソフトウェアアップデート機能用のユーザー一覧情報	○
120	show on-api webauth-html-file user	OAN：Web 認証ログイン画面 HTML ファイル入れ替え機能用のユーザー一覧情報	○
121	show on-api energy-saving user	OAN：省電力設定機能用のユーザー一覧情報	○
122	show access-redirect logging	特定端末への Web 通信不可表示機能のアクセスログ情報	○

項番	コマンド（表示）	内容	パラメータ指定なし
123	show access-redirect statistics	特定端末への Web 通信不可表示機能の統計情報	○
124	Detail Information	装置内部情報	○

（凡例）　○：表示対象

索引

数字

D

F

I

L

M

N

P

R

S

V

W

あ

い

う

お

か

き

こ