NWD-126043-001

PF5200 シリーズ

トラブルシューティングガイド

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。

NEC

■対象製品

このマニュアルは PF5200 シリーズを対象に記載しています。

■輸出時の注意

本製品は，外国為替及び外国貿易法に基づくリスト規制の該当貨物ですので，輸出（または非居住者への技術の提供あるいは外国において技術の提供をすることを目的とする取引）を行う場合には，経済産業大臣の輸出許可（または役務取引許可）が必要となります。
また，本製品には米国の輸出関連法令の規制を受ける技術が含まれており，輸出する場合輸出先によっては米国政府の許可が必要です。

■商標一覧

■マニュアルはよく読み，保管してください。

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

■ご注意

このマニュアルの内容については，改良のため，予告なく変更する場合があります。
また，出力表示例や図は，実際と異なる部分がある場合がありますのでご了承ください。

■発行

2011 年 10 月（初版）NWD-126043-001

■著作権

はじめに

■対象製品

このマニュアルは PF5200 シリーズを対象に記載しています。

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

なお，このマニュアルでは特に断らないかぎり各モデルに共通の機能について記載します。

■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，「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

PF5200 シリーズ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

■マニュアルの読書手順

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

● 装置の開梱から，初期導入時の基本的な設定について知りたい

PF5200 シリーズ
クイックスタートガイド
(NWD-126031-001)

● ハードウェアの設備条件，取り扱い方法について知りたい

PF5200 シリーズ
ハードウェア取扱説明書
(NWD-126033-001)

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

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーションガイド Vol.1
(NWD-126034-001)

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーションガイド Vol. 2
(NWD-126034-002)

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーションガイド Vol. 3
(NWD-126034-003)

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

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーション コマンドレファレンス Vol.1
(NWD-126037-001)

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーション コマンドレファレンス Vol. 2
(NWD-126037-002)

● 運用コマンドの入力シンタックス，パラメータ詳細について知りたい

PF5200 シリーズ ソフトウェアマニュアル
運用コマンドレファレンス Vol.1
(NWD-126039-001)

PF5200 シリーズ ソフトウェアマニュアル
運用コマンドレファレンス Vol.2
(NWD-126039-002)

● メッセージとログについて知りたい

PF5200 シリーズ ソフトウェアマニュアル
メッセージ・ログレファレンス
(NWD-126041-001)

● MIB について知りたい

PF5200 シリーズ ソフトウェアマニュアル
MIB レファレンス
(NWD-126042-001)

● ソフトウェアアップデートを行う手順について知りたい

PF5200 シリーズ
ソフトウェアアップデートガイド
(NWD-126047-001)

● ネットワーク接続のセキュアな運用管理について知りたい

PF5200 シリーズ
Secure Shell (SSH) ソフトウェアマニュアル
(NWD-126044-001)

● トラブル発生時の対処方法について知りたい

PF5200 シリーズ
トラブルシューティングガイド
(NWD-126043-001)

● Secure Channel の TLS 接続について知りたい

PF5200 シリーズ
【別冊】OpenFlow 機能 TLS 対応編
(NWD-126045-001)

■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
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
E-Mail	Electronic Mail
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
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
OFC	OpenFlow Controller
OFS	OpenFlow Switch
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PFS	Programmable Flow Switch
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
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
RSI	Real Switch Instance
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
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
VSI	Virtual Switch Instance
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WoL	Wake on LAN
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■常用漢字以外の漢字の使用について

このマニュアルでは，常用漢字を使用することを基本としていますが，次に示す用語については，常用漢字以外を使用しています。

- 溢れ（あふれ）
- 迂回（うかい）
- 筐体（きょうたい）
- 毎（ごと）
- 閾値（しきいち）
- 溜まる（たまる）
- 輻輳（ふくそう）
- 漏洩（ろうえい）

■ 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 1024 バイト，1024^2 バイト，1024^3 バイト，1024^4 バイトです。

目次

安全にお取り扱いいただくために

■ PF5200 シリーズを正しく安全にお使いいただくために

- 本マニュアルには，PF5200 シリーズを安全にお使いいただくための注意点を記載しています。ご使用前に本マニュアルを最後までお読みください。
- 本マニュアルはすぐ利用できるよう，お読みになった後は取り出しやすいところに保管してください。
- 操作は，本マニュアルの指示，手順に従って行なってください。
- 装置および本マニュアルに表示されている注意事項は必ず守ってください。これを怠ると，人身上の傷害や装置の破損を引き起こすおそれがあります。

■ご使用の前に

- 表示について
  本マニュアルおよび装置への表示では，装置を安全に正しくお使いいただき，あなたや他の人々への危害や財産への損害を未然に防止するために，いろいろな表示をしています。その表示と意味は次のようになっています。内容をよく理解してから本文をお読みください。

⚠ 警告	この表示を無視して，誤った取り扱いをすると，人が死亡または重傷を負う可能性があります。
⚠ 注意	この表示を無視して，誤った取り扱いをすると，人が傷害を負う可能性があります。
注意	この表示を無視して，誤った取り扱いをすると，装置の損傷または周囲の財物の損害を引き起こす可能性があります。
NOTE	この表示は，人身の安全や装置の損害に関係しない補足説明であることを示しています。

■操作や動作は

- 本マニュアルに記載されている以外の操作や動作は行なわないでください。
  装置について何か問題が発生した場合は，電源を切り，電源ケーブルを抜いたあと，保守員をお呼びください。

■自分自身でもご注意を

装置や本マニュアルに表示されている注意事項は十分検討されたものです。
それでも予測を超えた事態が起こることが考えられます。操作にあたっては指示に従うだけでなく，常に自分自身でも注意するようにしてください。

⚠ 警告

■万一，異常が発生したときはすぐに装置の電源を切ってください。

● 万一，煙が出ている，変なにおいがするなどの異常が発生した場合や，装置の内部に異物や水などが入った場合は，以下の方法で装置の電源を切ってください。そのまま使用すると，火災・感電の原因となります。

異常発生時の対処方法

異常が発生した装置	対処方法
電源を冗長化していない場合	本装置の電源スイッチを長押し（3 秒以上）してスタンバイ状態にした後，コンセントから電源ケーブルを取り外してください。
電源を冗長化している場合	本装置の電源スイッチを長押し（3 秒以上）してスタンバイ状態にした，コンセントから本装置に搭載されているすべての電源機構の電源ケーブルを取り外してください。

■異物を入れないでください。

● 装置の入排気孔などから内部に金属類や燃えやすいものなどの異物を差し込んだり，落とし込んだりしないでください。火災・感電の原因となります。

■ RESET スイッチを押す場合，先の折れやすいものや，虫ピン，クリップなど，中に入って取り出せなくなるようなものは使用しないでください。

● RESET スイッチを押す場合，先の折れやすいものや，虫ピン，クリップなど，中に入って取り出せなくなるようなものは使用しないでください。火災・感電の原因となります。

■改造しないでください。

● 装置を改造しないでください。火災・感電の原因となります。

■衝撃を与えないでください。

● 万一，装置を落としたり部品を破損した場合は，装置の電源を切り，電源ケーブルをコンセントから抜いて保守員にご連絡ください。そのまま使用すると火災・感電の原因となります。

■装置の上に物を置かないでください。

● 装置の上に虫ピン，クリップなどの金属物や花びん，植木鉢など水の入った容器を置かないでください。中に入った場合，火災・感電の原因となります。

■故障 / 障害が発生したときは保守員をお呼びください。

● 故障 / 障害が発生したときは，電源を切り，電源ケーブルを抜いたあと，保守員をお呼びください。

⚠ 警告

■表示以外の電源で使用しないでください。

● 表示された電源電圧以外で使用しないでください。火災・感電の原因となります。

■分電盤へ給電される電流容量は，ブレーカの動作電流より大きくなるようにしてください。

● 分電盤へ給電される電流容量は，ブレーカの動作電流より大きくなるようにしてください。分電盤への電流容量がブレーカの動作電流より小さいと，異常時にブレーカが動作せず，火災の原因となることがあります。

■接地を取ってください。

● 必ず接地付きのコンセントを使用してください。接地を取らずに使用すると，感電の原因となると共に，電気的雑音により，障害発生の原因となります。

■電源ケーブルを大切にしてください。

● 電源ケーブルの上に重いものを乗せたり，引っ張ったり，折り曲げたり，加工したりしないでください。電源ケーブルが傷ついて，火災・感電の原因となります。ケーブルの上を敷きものなどでおおうことにより，それに気づかないで重い物を乗せてしまうことがあります。

● 電源ケーブルは付属または指定のものを使用してください。それ以外のものを使用すると，火災・感電の原因となります。また，付属の電源ケーブルを本製品以外で使用しないでください。本製品以外で使用した場合，火災・感電の原因となります。

● 電源ケーブルが傷んだら（芯線の露出，断線など）保守員に交換をご依頼ください。そのまま使用すると火災・感電の原因となります。

● 電源プラグはほこりが付着していない事を確認し，がたつきのないように刃の根元まで確実に差し込んでください。ほこりが付着したり接続が不完全な場合，火災・感電の原因となります。

■タコ足配線はしないでください。

● 同じコンセントに多数の電源プラグを接続するタコ足配線はしないでください。タコ足配線は，火災の原因となると共に，電力使用量がオーバーしてブレーカが落ち，ほかの機器にも影響をおよぼします。

■電源機構の取り付け，取り外しを行なう場合は電源ケーブルを取り外してください。

● 電源機構の取り付け，取り外しを行なう場合は，電源機構から電源ケーブルを取り外してください。電源ケーブルを接続していると，回路に通電してしまいます。

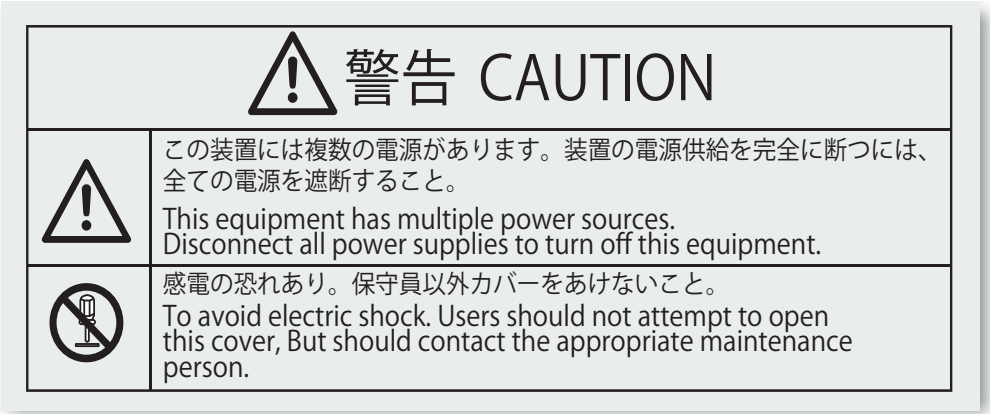
⚠ 注意

■不安定な場所に置かないでください。

● 装置をラックに搭載する場合には，装置が安定した状態にあるか十分に確認して作業してください。不安定な状態で作業した場合，落下や転倒によるけがの原因となります。

■装置のカバーを外さないでください。

● 装置のカバーを外さないでください。感電の原因となります。装置には以下のラベルを貼り付けています。



■入排気孔をふさがないでください。

● 装置の入排気孔をふさがないでください。入排気孔をふさぐと内部に熱がこもり，火災の原因となることがあります。入排気孔から 50mm 以上スペースを空けてください。

■髪の毛や物を装置の入排気孔に近づけないでください。

● 装置には冷却用のファンを搭載しています。入排気孔の近くに物を近づけないでください。内部の温度上昇により，故障の原因となるおそれがあります。また，入排気孔の近くに髪の毛や物を近づけないでください。巻き込まれてけがの原因となることがあります。

■移動させる場合は，電源機構の取っ手を持たないでください。

● 装置を移動させる場合は，電源機構の取っ手を持たないでください。取っ手が外れて装置が落下し，けがの原因となることがあります。また，変形して，火災・感電の原因となることがあります。

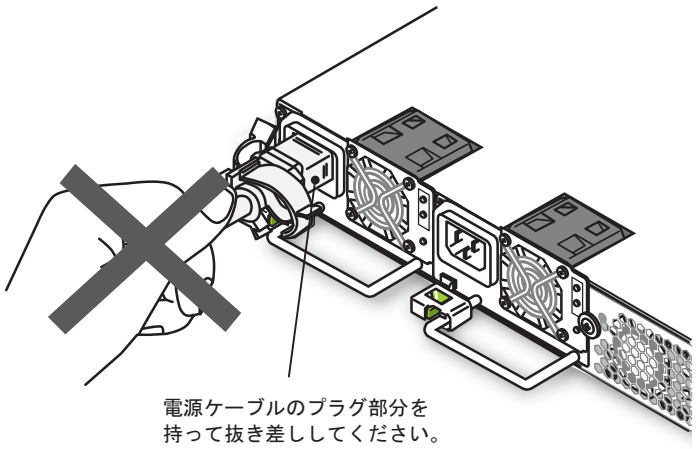
⚠ 注意

■持ち運ぶときのご注意

- 移動させる場合は装置の電源を切り，すべてのケーブル類を装置から外してから行なってください。装置やケーブルが変形したり，傷ついたりして，火災・感電の原因となることがあります。
- 輸送時に積み重ねる場合は，梱包箱に入れてください。装置が変形したり，傷ついたりして，火災・感電の原因となることがあります。

■電源ケーブルを粗雑に扱わないでください。

- 電源ケーブルを熱器具に近づけないでください。ケーブルの被覆がとけて，火災・感電の原因となることがあります。
- AC 電源ケーブルをコンセントに差し込むとき，または抜くときはケーブルのプラグ部分を持って行なってください。ケーブルを引っ張ると断線の原因となります。



電源ケーブルのプラグ部分を
持って抜き差ししてください。

■電源機構単体で電源ケーブルを取り付けないでください。

- 電源機構は装置本体に装着してから電源ケーブルを取り付けてください。電源機構単体に電源ケーブルを取り付 けてコンセントに挿入すると，電源機構の故障の原因となるだけでなく，火災・感電の原因となることがあります。

■装置の電源を切断する場合は，装置への給電をすべて停止させてください。

- 装置本体の電源スイッチを長押し（3 秒以上）しただけでは装置の電源は切断されません。電源を切断する場合は，装置本体の電源スイッチを長押し（3 秒以上）してスタンバイ状態にした後，コンセントから電源ケーブルを取り外してください。
- 電源を冗長化している場合は，装置本体の電源スイッチを長押し（3 秒以上）してスタンバイ状態にした後，コンセントから本装置に搭載されているすべての電源機構の電源ケーブルを取り外してください。

⚠ 注意

■レーザー光に注意してください。

● 本装置ではレーザー光を使用しています（レーザー光は無色透明で目には見えません）。光送受信部を直接のぞかないでください。

■湿気やほこりの多いところに置かないでください。

● 湿気やほこりの多い場所に置かないでください。火災・感電の原因となることがあります。

● 低温から高温の場所など温度差が大きい場所へ移動させた場合，表面や内部で結露することがあり，そのまま使用すると火災・感電の原因となります。そのままその場所で数時間放置してから使用してください。

■乗ったり，よりかかったり，重い物を置いたりしないでください。

● 装置に乗ったり，よりかかったりしないでください。装置を破損するおそれがあります。また，バランスがくずれて倒れたり，落下してけがの原因となることがあります。

● 装置本体の上に 5kg を超える物を置かないでください。装置を破損するおそれがあります。また，バランスがくずれて倒れたり，落下してけがの原因となることがあります。

■装置の内部に手を触れないでください。

● 装置内部に不用意に手を入れないでください。機構部等でけがの原因となることがあります。

■電源機構を搭載しないスロットのブランクパネルは取り外さないでください。

● 電源機構を搭載しないスロットのブランクパネルは取り外さないでください。ブランクパネルを取り付けずに取り扱うと，機構部等でけがの原因となることがあります。また，異物などが入った場合，故障の原因となります。

■清掃について

● 装置および装置周辺のほこりは，定期的に清掃してください。装置停止の原因となるだけでなく火災・感電の原因となることがあります。

注意

■高温になるところに置かないでください。

● 直射日光が当たる場所やストーブのような熱器具の近くに置くと，部品に悪い影響を与えますので注意してください。

■テレビやラジオを近づけないでください。

● テレビやラジオなどを隣接して設置した場合，お互いに悪影響を及ぼすことがあります。テレビやラジオに雑音が入った場合は次のようにしてください。
・テレビやラジオからできるだけ離す。
・テレビやラジオのアンテナの向きを変える。
・コンセントを別々にする。

■硫化水素の発生するところや，塩分の多いところに置かないでください。

● 温泉地など，硫化水素の発生するところや，海岸などの塩分の多いところでお使いになると本装置の寿命が短くなるおそれがあります。

■電源ケーブルの取り付け，取り外しは，電源スイッチを長押し（3 秒以上）してスタンバイ状態にして行なってください。

● 電源ケーブルの取り付け，取り外しは，装置本体の電源スイッチを長押し（3 秒以上）してスタンバイ状態にして行なってください。

■装置の電源を入れたままでファンユニットを交換する場合，制限時間を守ってください。

● 装置の電源を入れたままでファンユニットを交換する場合，取り外してから取り付けるまでを 2 分以内で行なってください。2 分を超えると，装置内部の温度上昇により，障害発生の原因となります。（※ 25 ℃環境での交換作業を想定しています。）

注意

■装置設置場所の近傍にコンセントを準備してください。

- 装置設置場所の近傍にコンセントを準備し，そのコンセントには容易にアクセスできるようにしてください。
- コンセントは指定のものを使用してください。それ以外のものを使用すると，火災・感電の原因となります。

■メモリカードの取り扱いに注意してください。

- メモリカードを取り付ける場合は，カードを強く押したり，指ではじいたりしないでください。また，取り外す場合は，ロックが掛かった状態から無理に引っ張り出したりしないでください。メモリカードスロットのコネクタ部を破損するおそれがあります。
- 装置本体を移動させる場合は，メモリカードを取り外してください。移動中にカードに無理な力が加わると，メモリカードスロットのコネクタ部を破損するおそれがあります。

■ ACC LED 点灯中はメモリカードを取り外したり，電源を切断したりしないでください。

- 装置正面パネルの ACC LED 点灯中はメモリカードにアクセス中です。アクセス中は，メモリカードを取り外したり，電源を切断したりしないでください。メモリカードを破損するおそれがあります。
  また，一部のコマンドは，コマンド入力後メモリカードのアクセスが終了するまでにしばらく時間がかかります。アクセスが終了したことを確認の上，メモリカードの取り外しや電源の切断を行なってください。

注意

■トランシーバにラベルなどを貼り付けたりしないでください。

● トランシーバには，メーカおよび弊社の標準品であることを示すラベルを貼り付けています。ただし，このラベルを貼り付けているのは，トランシーバの放熱や，ケージからの抜けを防止する機構の妨げにならない部分です。
放熱や抜け防止機構の妨げになるところにラベルなどを貼り付けると，トランシーバが故障したり，装置を破損したりするおそれがあります。

■ STATUS1 LED 緑点滅中は装置の電源を切断しないでください。

● STATUS1 LED が緑点滅から緑点灯に変わるまで装置の電源を切断しないでください。装置が故障するおそれがあります。

■装置およびオプション機構の持ち運び，梱包などを行なう場合は，静電気防止用のリストストラップを使用してください。

● 静電気防止用リストストラップを使用してください。静電気防止用リストストラップを使用しないで取り扱った場合，静電気により機器を損傷することがあります。

■オプション機構の持ち運び，梱包の際は取り扱いに注意してください。

● トランシーバ，メモリカード，電源機構，およびファンユニットの持ち運び，梱包の際には，コネクタ部には手をふれないでください。また，保管する場合は静電防止袋の中に入れてください。

■お手入れのときは

● 装置外装の汚れは，乾いたきれいな布，あるいは，布に水か中性洗剤を含ませてかたく絞ったもので，汚れた部分を拭いてください。ベンジンやシンナーなどの揮発性の有機溶剤や薬品，化学ぞうきん，殺虫剤は，変形・変色および故障の原因となることがあるので使用しないでください。

■長時間ご使用にならないとき

● 長期間の休みや旅行などで長時間装置をご使用にならないときは，安全のため電源ケーブルをコンセントから抜いてください。

■この装置の廃棄について

● この装置を廃棄する場合は，地方自治体の条例または規則に従い廃棄するか，地域の廃棄物処理施設にお問い合わせください。

■有寿命品について

● 以下に示す機器は有寿命品です。購入に関しては担当営業または保守員にお問い合わせください。
・電源機構
・ファンユニット

■環境条件について

● 周囲温度が異常に高い環境で使用された場合，もしくは FAN 故障等によるエアフロー異常のまま使用された場合，装置内部の温度が上昇し，装置を停止する機能が働きます。

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，PF5200 シリーズ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。

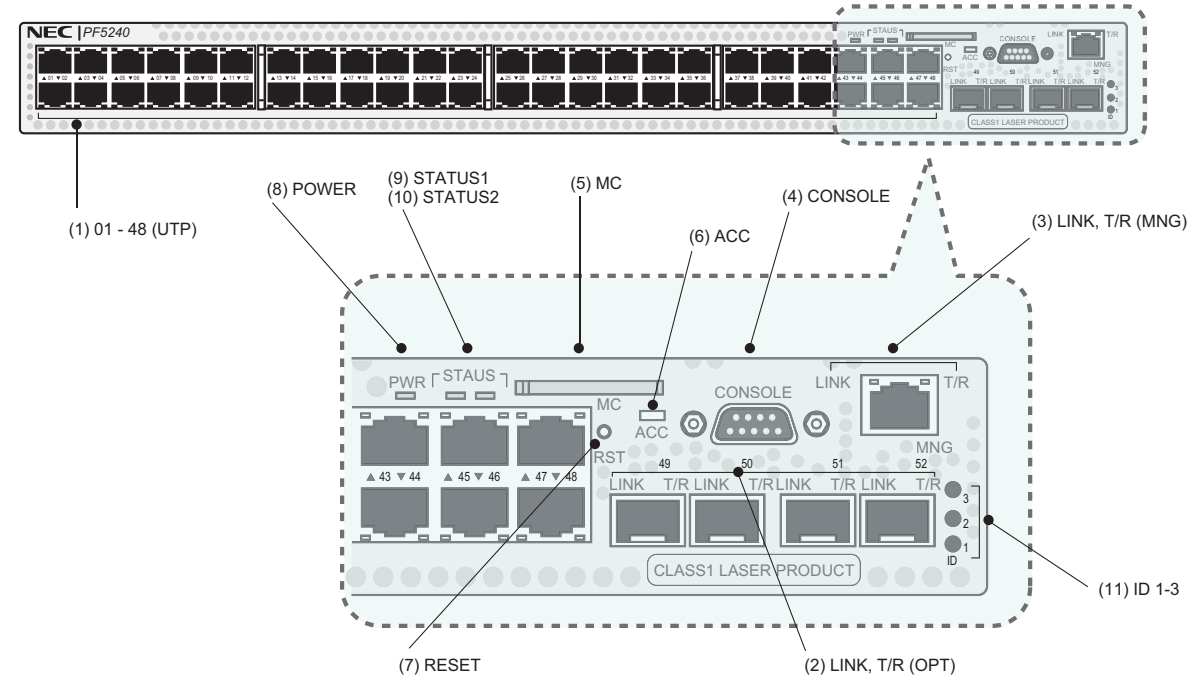
1.2 装置および装置一部障害解析概要

1.2.1 PF5200 シリーズの障害解析

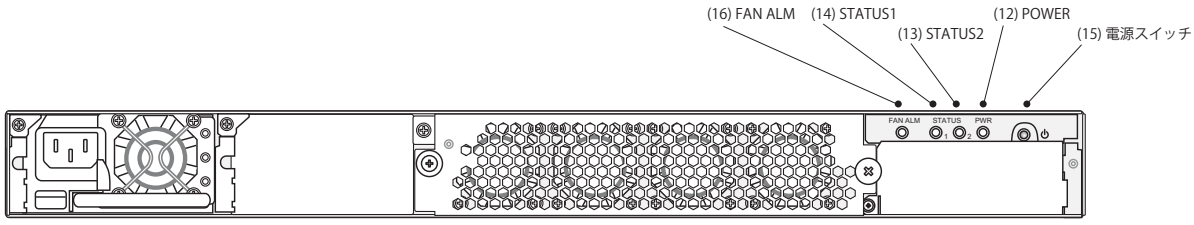
運用中に障害が発生し，装置を目視で直接確認できる場合には，「2.1 PF5200 シリーズのトラブルシュート」の対策内容に従ってトラブルシュートしてください。

なお，装置を目視で確認できない場合でも，リモート運用端末から運用コマンドで装置の LED を確認することにより，装置を目視できる場合と同様にトラブルシュートすることができます。

図 1-1 正面・背面パネルレイアウト



正面パネル側



背面パネル側

表 1-1 LED の表示，スイッチ，コネクタ

番号	名 称	種 類	状 態	内 容
(1)	01-48 (UTP)	LED: 緑 / 橙	10/100/1000BASE-Tイーサネットポートの動作状態を示す。	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：回線障害検出。 消灯 ：STATUS1 LED が緑点灯の場合，リンク障害，または閉塞。STATUS1 LED が緑点灯以外の場合，通信不可状態，または装置の部分障害発生。
(2)	LINK (OPT)	LED: 緑 / 橙	SFPスロット/SFP+スロットのイーサネットポートの動作状態を示す。	緑点灯：リンク確立。 橙点灯：回線障害検出。 消灯 ：ST1 LED が緑点灯の場合，リンク障害，または閉塞。STATUS1 LED が緑点灯以外の場合，通信不可状態，または装置の部分障害発生。
	T/R (OPT)	LED: 緑		緑点滅：フレーム送受信中。 消灯 ：フレーム非送受信。
(3)	LINK (MNG)	LED: 緑	Managementイーサネットポートの動作状態を示す。	緑点灯：リンク確立。 消灯 ：リンク障害，または装置の部分障害発生。
	T/R (MNG)	LED: 緑		緑点滅：フレーム送受信中。 消灯 ：フレーム非送受信。
(4)	CONSOLE	コネクタ	CONSOLE ポート	コンソール端末接続用 RS-232C ポート
(5)	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
(6)	ACC	LED: 緑	メモリカードの状態を示す。	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状態（メモリカード取り付け，取り外し可能），または装置の部分障害発生。
(7)	RESET	スイッチ （ノンロック）	リセットスイッチ *1	短押し（1 秒程度）：Warm リセット。*2 長押し（5 秒以上）：Cold リセット。*2
(8) (12)	POWER	LED: 緑 / 橙	装置の電源状態を示す。	緑点灯：運用可能状態。 橙点灯：スタンバイ状態。 橙点滅：WoL スタンバイ状態。 消灯 ：電源オフ，または電源異常。
(9) (14)	STATUS1	LED: 緑 / 赤	装置の状態を示す。	緑点灯：動作可能。 緑点滅：準備中（立上げ中）。 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 ：スタンバイ状態，電源オフ，または電源 / 温度異常。
(10) (13)	STATUS2	LED：青	ユーザ定義	OpenFlow メッセージ (Vendor 定義) により消灯 / 点滅 / 点灯の操作を行う。 ※ OpenFlow メッセージ (Vendor 定義) を設定していない場合，消灯。
(11)	ID1-3	―	―	未使用。
(15)	電源 スイッチ	スイッチ （ノンロック）	電源スイッチ	短押し（1 秒程度）：運用サービス可能状態へ移行。 長押し（3 秒以上）：スタンバイ状態へ移行。
(16)	FAN ALM	LED: 赤	ファンユニットの状態を示す。	赤点灯：障害。 消灯 ：正常。

*1 スイッチは正面パネルより奥にあります。先の細いドライバなどを使用して押してください。

*2 Warm リセット：設定情報が reload され，装置立ち上がり完了後，サービスを再開する。この場合，設定情報が展開されるまでは，サービスは行われない。
Cold リセット ：User password が無効となる。

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。

なお，上位レイヤの通信障害は，下位レイヤの通信障害が原因の場合があるので，下位レイヤの項目も確認してください。

表 1-2 機能障害の状況と参照個所

大項目	中項目	参照個所
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 ログインユーザのパスワードを忘れてしまった
	装置管理者パスワード忘れ	3.1.2 装置管理者のパスワードを忘れてしまった
MC のトラブル	"MC : --------" と表示された	3.2.1 show system コマンドまたは show mc コマンドで "MC : --------" と表示される
	"MC not found." と表示された	3.2.2 MC へのアクセス時に "MC not found." と表示される
運用端末のトラブル	コンソール入力・表示不可	3.3.1 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	3.3.2 リモート運用端末からログインできない
	ログイン認証不可	3.3.3 RADIUS ／ TACACS+ を利用したログイン認証ができない
	コマンド承認不可	3.3.4 RADIUS ／ TACACS+ を利用したコマンド承認ができない
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/1000BASE-T の通信障害	3.4.2 10BASE-T/100BASE-TX/1000BASE-T のトラブル発生時の対応
	1000BASE-X の通信障害	3.4.3 1000BASE-X のトラブル発生時の対応
	10GBASE-R の通信障害	3.4.4 10GBASE-R のトラブル発生時の対応
	リンクアグリゲーションでの障害	3.4.5 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
	IGMPsnooping 不可	3.5.4 IGMP snooping によるマルチキャスト中継ができない
	MLDsnooping 不可	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
	DHCP が機能しない	3.6.2 DHCP 機能で IP アドレスが割り振られない
	DynamicDNS が動かない	3.6.3 DHCP 機能で DynamicDNS 連携が動作しない

大項目	中項目	参照個所
IPv4 ユニキャストルーティングの通信障害	RIP 情報なし	3.7.1 RIP 経路情報が存在しない
	OSPF 情報なし	3.7.2 OSPF 経路情報が存在しない
	BGP4 情報なし	3.7.3 BGP4 経路情報が存在しない
IPv4 マルチキャストルーティングの通信障害	PIM-SM ネットワークで通信不可	3.8.1 IPv4 PIM-SM ネットワークで通信ができない
	PIM-SM ネットワークでデータが二重中継された	3.8.2 IPv4 PIM-SM ネットワークでマルチキャストデータが二重中継される
	PIM-SSM ネットワークで通信不可	3.8.3 IPv4 PIM-SSM ネットワークで通信ができない
	PIM-SSM ネットワークでデータが二重中継された	3.8.4 IPv4 PIM-SSM ネットワークでマルチキャストデータが二重中継される
IPv6 ネットワークの通信障害	通信できない	3.9.1 通信できない，または切断されている
	DHCP の不具合	3.9.2 IPv6 DHCP に関するトラブルシューティング
IPv6 ユニキャストルーティングの通信障害	RIPng の情報がない	3.10.1 RIPng 経路情報が存在しない
	OSPFv3 の情報がない	3.10.2 OSPFv3 経路情報が存在しない
	BGP4+ の情報がない	3.10.3 BGP4+ 経路情報が存在しない
IPv6 マルチキャストルーティングの通信障害	PIM-SM ネットワークで通信不可	3.11.1 IPv6 PIM-SM ネットワークで通信ができない
	PIM-SM ネットワークでデータが二重中継された	3.11.2 IPv6 PIM-SM ネットワークでマルチキャストデータが二重中継される
	PIM-SSM ネットワークで通信不可	3.11.3 IPv6 PIM-SSM ネットワークで通信ができない
	PIM-SSM ネットワークでデータが二重中継された	3.11.4 IPv6 PIM-SSM ネットワークでマルチキャストデータが二重中継される
IPv4 の VRRP 障害	－	3.12.1 IPv4 ネットワークの VRRP 構成で通信ができない
IPv6 の VRRP 障害	－	3.12.2 IPv6 ネットワークの VRRP 構成で通信ができない
SNMP の通信障害	MIB が取得できない	3.13.1 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	3.13.2 SNMP マネージャでトラップが受信できない
sFlow 統計の障害	sFlow パケットが届かない	3.14.1 sFlow パケットがコレクタに届かない
	フローサンプルが届かない	3.14.2 フローサンプルがコレクタに届かない
	カウンタサンプルが届かない	3.14.3 カウンタサンプルがコレクタに届かない
LLDP 機能で隣接装置情報が取れない	－	3.15.1 LLDP 機能により隣接装置情報が取得できない
OADP 機能で隣接装置情報が取れない	－	3.15.2 OADP 機能により隣接装置情報が取得できない
NTP の通信障害	－	3.16.1 NTP による時刻同期ができない
IEEE802.3ah/UDLD 機能使用時の障害	ポートが inactive 状態になる	3.17.1 IEEE802.3ah/UDLD 機能でポートが inactive 状態となる

大項目	中項目	参照個所
パケット廃棄による通信障害	－	3.19.1　フィルタ／ QoS 設定情報の確認
OpenFlow 機能の通信障害	－	3.20.1　OpenFlow コントローラとの接続が確立できない
その他	－	マニュアル「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　PF5200 シリーズのトラブルシュート

2.1.1　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。

手順内の " 装置再起動 " は，以下の手順で行ってください。

1. コンセントから電源ケーブルを取り外します。
2. 10 秒程度経過した後，コンセントに電源ケーブルを挿入します。

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	直ちに装置の電源ケーブルを抜いてください。 上記の手順のあと，装置を交換してください。
2	login プロンプトが表示されない 注　login プロンプトが表示されるまで数分かかることがあります。	1. MC が挿入されている場合は，MC を抜いた上で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には，装置を交換します。
3	装置の POWER LED が消灯している	次の手順で対策を実施します。 1.「表 2-2　電源障害の切り分け」を実施します。 2. 障害が発生している電源機構を交換します。障害が発生している電源機構は以下のどれかの状態になっています。 （a）FAULT LED が橙点灯している （b）Power Good LED が消灯している 3. 上記 1，2 に該当しない場合には，装置を再起動して環境に異常がないかを確認します。 （1）装置を再起動します。 （2）装置を再起動できた場合には，show logging コマンドを実行して障害情報を確認します。 `>show logging | grep ERR` （3）採取した障害情報に高温注意を示すメッセージが存在する場合には，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ます。 （4）上記（1）の手順で装置を再起動できない場合，上記（3）の手順で障害情報が存在しないまたは高温注意を示すメッセージが存在しない場合には，装置に障害が発生しているため，装置を交換してください。
4	装置の STATUS1 LED が赤点灯している	装置に障害が発生したか，または長期間（1 か月以上）通電しない状態から電源を ON にしています。 1. 電源機構とファンユニットのエアフローの組み合わせを確認してください。 2. 長期間通電しない状態から電源を ON にした場合，装置を再起動してください。 3. 上記 1 以外の場合には，装置に障害が発生しています。装置を交換してください。

項番	障害内容	対策内容
5	• 装置の STATUS1 LED が赤点滅している • 装置の各ポートの LINK LED（OPT）が橙点灯または消灯している	装置または回線に障害が発生しています。 1. 電源機構およびファンユニットの状態を確認し，障害が発生している場合には交換します。 ・装置背面の FAN ALM LED が赤点灯の場合にはファンユニットを交換します。 ・電源機構の FAULT LED が橙点灯または Power Good LED が消灯している場合には電源機構を交換します ・電源機構の Power Good LED, FAULT LED, AC Good LED のいづれも消灯している場合には「表 2-2　電源障害の切り分け」により電源障害の対策を実施します。対策を実施しても LED 点灯状態が変わらない場合には電源機構を交換します。 2. 上記 1 以外の場合には，エラーメッセージを参照して障害の対策を実施します。show logging コマンドを実行して障害情報を確認し，対策を実施してください。 `>show logging | grep ERR`
6	• WoL の設定を入れているにも関わらず WoL による装置起動が出来ない。 • Power ボタンを押しても装置が起動しない。	周囲温度が異常に高い環境，もしくは FAN 故障等によるエアフロー異常のまま使用し装置内部の温度が上昇している可能性があります。 コンセントから電源ケーブルを抜き，十分に冷ましてから装置を起動してください。 また，電源ケーブルを抜かずに周囲温度および，装置内部の温度が下がると自動で装置が立ち上がります。

表 2-2　電源障害の切り分け

項番	障害内容	対策内容
1	電源ケーブルに抜けやゆるみがある	電源ケーブルを正しく挿入してください。
2	電源機構がしっかり取り付けられていなくて，がたついている	次の手順を実施してください。 1.　電源ケーブルを抜きます。 2.　電源機構を正しく挿入します。 3.　電源ケーブルを挿します。
3	測定した入力電源が以下の範囲外である AC100V の場合：AC90 ～ 106V AC120V の場合：AC108 ～ 127V AC220 ～ 230V の場合：AC198 ～ 243V AC240V の場合：AC216 ～ 254V 注　本件は入力電源の測定が可能な場合だけ実施する	設備担当者に連絡して入力電源の対策を依頼してください。

2.1.2　装置およびオプション機構の交換方法

装置およびオプション機構の交換方法は，「ハードウェア取扱説明書」に記載されています。記載された手順に従って実施してください。

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。

3.20 OpenFlow 機能の通信障害

3.1　ログインパスワードのトラブル

3.1.1　ログインユーザのパスワードを忘れてしまった

運用中，ログインユーザ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。

1. 装置管理者への通知
   まずは装置管理者に連絡してください。ただし，（ほかのログインユーザ利用者がいないなどの理由で）装置管理者になれるログインユーザ利用者がいない場合は，デフォルトリスタートをして再度パスワード設定を行ってください。

   デフォルトリスタート
   　本体のリセットスイッチを 5 秒以上押します。
   　パスワードによるセキュリティチェックを行わないので，デフォルトリスタートによる起動を行う場合は十分に注意してください。なお，設定したパスワードは装置を再起動後に有効になります。
2. パスワードの変更
   パスワード変更の連絡を受けた装置管理者は，パスワードを変更して対象ログインユーザの利用者全員に通知してください（なお，パスワードを変更する場合は password コマンドを，パスワードの削除だけ行う場合は clear password コマンドを実行してください）。

図 3-1　装置管理者によるログインユーザパスワード変更

```
# password user1
Changing local password for user1.
New password:
Retype new password:
#
```

3.1.2　装置管理者のパスワードを忘れてしまった

運用中，装置管理者の権限を持っているログインユーザ利用者全員が，装置管理者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，デフォルトリスタートをして再度パスワード設定を行ってください。

デフォルトリスタート
　本体のリセットスイッチを 5 秒以上押します。
　パスワードによるセキュリティチェックを行わないので，デフォルトリスタートによる起動を行う場合は十分に注意してください。なお，設定したパスワードは装置を再起動後に有効になります。

3.2　MC のトラブル

3.2.1　show system コマンドまたは show mc コマンドで "MC : --------" と表示される

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

表 3-1　"MC : --------" と表示される場合の対応方法

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

3.2.2　MC へのアクセス時に "MC not found." と表示される

MC へアクセスするコマンドの実行時に "MC not found." と表示される場合は，次の表に従って確認してください。

表 3-2　"MC not found." と表示される場合の対応方法

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

3.3　運用端末のトラブル

3.3.1　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 3-3　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 STATUS1 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. RS232C 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：9600bps（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. 以降の確認をしてください。 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] によって画面が停止している可能性があります。何かキーを入力してください。
3	異常な文字が表示される	通信ソフトウェアとのネゴシエーションが正しくできていない可能性があります。通信ソフトウェアの通信速度を次の手順で確認してください。 1. コンフィグレーションコマンド line console 0 で CONSOLE(RS232C) の通信速度を設定していない場合は，通信ソフトウェアの通信速度が 9600bps に設定されているか確認してください。 2. コンフィグレーションコマンド line console 0 で CONSOLE(RS232C) の通信速度を 1200，2400，4800，または 19200bps 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	ユーザ名入力中に異常な文字が表示された	CONSOLE(RS232C) 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	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。
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。
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 の通信速度によって，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を変更し，1 行で表示可能な文字数を多くしてください。

3.3.2 リモート運用端末からログインできない

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

表 3-4 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 ping コマンドを使用してリモート接続のための経路が確立されているかを確認してください。 2. コネクション確立のメッセージ表示後プロンプトが表示されるまで時間がかかる場合は，DNS サーバとの通信ができなくなっている可能性があります（DNS サーバとの通信ができない場合プロンプトが表示されるまで約 5 分かかります。なお，この時間は目安でありネットワークの状態によって変化します）。
2	ログインができない。	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 モードのアクセスリストで許可された IP または IPv6 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 または IPv6 アドレスに deny を指定していないかを確認してください（詳細はマニュアル「コンフィグレーションガイド」を参照してください）。 2. 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（詳細はマニュアル「コンフィグレーションガイド」を参照してください）。 なお，最大ユーザ数でログインしている状態でリモート運用端末から本装置への到達性が失われ，その後復旧している場合，TCP プロトコルのタイムアウト時間が経過しセッションが切断されるまで，リモート運用端末からは新たにログインできません。TCP プロトコルのタイムアウト時間はリモート運用端末の状態やネットワークの状態によって変化しますが，おおむね 10 分です。 3. コンフィグレーションコマンド line vty モードの transport input で，本装置へのアクセスを禁止しているプロトコルを使用していないか確認してください（詳細はマニュアル「コンフィグレーションコマンドレファレンス」を参照してください）。
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 以降の確認をしてください。 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］によって画面が停止している可能性があります。何かキーを入力してください。
4	ログインしたままの状態になっているユーザがある。	自動ログアウトするのを待つか，再度ログインしてログインしたままの状態になっているユーザを killuser コマンドで削除します。また，コンフィグレーションを編集中の場合は，コンフィグレーションの保存がされていないなど編集中の状態になっているので，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するなどしたのち，編集を終了してください。

3.3.3 RADIUS ／ TACACS+ を利用したログイン認証ができない

RADIUS ／ TACACS+ を利用したログイン認証ができない場合，以下の確認を行ってください。

1. RADIUS ／ TACACS+ サーバへの通信
   ping コマンドで，本装置から RADIUS ／ TACACS+ サーバに対して疎通ができているか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ローカルアドレスを設定している場合は，ローカルアドレスから ping コマンドで，本装置から RADIUS ／ TACACS+ サーバに対して疎通ができているかを確認してください。

2. タイムアウト値およびリトライ回数設定
   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 の設定によって，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＜設定したタイムアウト値（秒）＞×＜設定したリトライ回数＞×＜設定した RADIUS サーバ数＞となります。
   TACACS+ 認証の場合，コンフィグレーションコマンド tacacs-server host，tacacs-server timeout の設定によって，本装置が TACACS+ サーバとの通信が不能と判断する時間は最大で＜設定したタイムアウト値（秒）＞×＜設定した TACACS+ 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 ／ TACACS+ コンフィグレーションの設定かリモート運用端末で使用するアプリケーションのタイムアウトの設定を変更してください。また，運用ログに RADIUS ／ TACACS+ 認証が成功したメッセージが出力されているにも関わらず，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 ／ TACACS+ サーバに接続するまでに，リモート運用端末側のアプリケーションがタイムアウトしていることが考えられるため，稼働中の RADIUS ／ TACACS+ サーバを優先するように設定するか，＜タイムアウト値（秒）＞×＜リトライ回数＞の値を小さくしてください。

3.3.4 RADIUS ／ TACACS+ を利用したコマンド承認ができない

RADIUS ／ TACACS+ 認証は成功して本装置にログインできたが，コマンド承認がうまくできない場合や，コマンドを実行しても承認エラーメッセージが表示されてコマンドが実行できない場合は，以下の確認を行ってください。

1. show whoami の確認
   本装置の show whoami コマンドで，現在のユーザが許可・制限されている運用コマンドのリストを表示・確認できます。RADIUS ／ TACACS+ サーバの設定どおりにコマンドリストが取得できていることを確認してください。
2. サーバ設定の確認
   RADIUS ／ TACACS+ サーバ側で，本装置のコマンド承認に関する設定が正しいことを確認してください。特に RADIUS の場合はベンダー固有属性の設定，TACACS+ の場合は Service と属性名などに注意してください。RADIUS ／ TACACS+ サーバの設定については，マニュアル「コンフィグレーションガイド」を参照してください。
3. コマンドリスト記述時の注意
   RADIUS ／ TACACS+ サーバ側で，本装置のコマンド承認用のコマンドリストを記述する際には空白の扱いに注意してください。例えば許可コマンドリストに”show ip　”（show ip の後にスペース）が設定してある場合は，show ip interface コマンドは許可されますが，show ipv6 interface コマンドは制限されます。

3.4　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

1. ログの確認
   ログは，マニュアル「メッセージ・ログレファレンス」を参照してください。
2. ポートの状態による原因の切り分け
   show interfaces コマンドによってポート状態を確認し，次の表に従って原因の切り分けを行ってください。

表 3-5　ポート状態の確認および対応

項番	ポート状態	原因	対応
1	active up	該当ポートは正常に動作中です。	なし
2	active down	該当ポートに回線障害が発生しています。	show logging コマンドによって表示される該当ポートのログより，マニュアル「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	inactive	下記のどれかによって inactive 状態となっています。 • inactivate コマンド • リンクアグリゲーションのスタンバイリンク機能 • スパニングツリーの BPDU ガード機能 • IEEE802.3ah/UDLD 機能での障害検出 • L2 ループ検知機能によるポート閉塞 • ストームコントロール機能によるポート閉塞	• リンクアグリゲーションのスタンバイリンク機能によって inactive 状態になっている場合は，正常な動作なので，activate コマンドで active 状態にしないでください。スタンバイリンク機能は show channel-group コマンドで detail パラメータを指定し確認してください。 • スパニングツリーの BPDU ガード機能によって inactive 状態になっている場合は，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，activate コマンドで該当ポートを active 状態にしてください。BPDU ガード機能は show spanning-tree コマンドで detail パラメータを指定し確認してください。 • IEEE802.3ah/UDLD 機能で片方向リンク障害または L2 ループが検出されたことによって inactive 状態になっている場合は，「3.17　IEEE802.3ah/UDLD 機能の通信障害」を参照してください。障害復旧後，activate コマンドで該当ポートを active 状態にしてください。 • L2 ループ検知機能によって inactive 状態になっている場合は，ループが発生する構成を変更した後，activate コマンドで該当ポートを active 状態にしてください。また，コンフィグレーションコマンドで loop-detection auto-restore-time が設定されている場合は，自動的に active 状態に戻ります。 • ストームコントロール機能によって inactive 状態になっている場合は，LAN がストームから回復後，activate コマンドで該当ポートを active 状態にしてください。 • 上記のどれでもない場合に，active 状態にしたいときは，使用するポートにケーブルが接続されていることを確認の上，activate コマンドで該当ポートを active 状態にしてください。
4	test	test interfaces コマンドによって，該当ポートは回線テスト中です。	通信を再開する場合は，no test interfaces コマンドで回線テストを停止後，activate コマンドで該当ポートを active 状態にしてください。

項番	ポート状態	原因	対応
5	fault	該当ポートのポート部分のハードウェアが障害となっています。	show logging コマンドによって表示される該当ポートのログより，マニュアル「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。
6	initialize	該当ポートが初期化中です。	初期化が完了するまで待ってください。
7	disable または locked	コンフィグレーションコマンド shutdown が設定されています。	使用するポートにケーブルが接続されていることを確認の上，コンフィグレーションコマンドで no shutdown を設定して該当ポートを active 状態にしてください。

（2） 統計情報の確認

show port statistics コマンドを実行し，本装置に実装されている全ポートの送受信パケット数，送受信廃棄パケット数を確認できます。

図 3-2 「ポートの動作状況確認」表示例

```
> show port statistics
2010/12/01 15:30:00
Port Counts:52
Port  Name     Status  T/R All packets    Multicast    Broadcast      Discard
0/ 1  geth0/1  up      Tx              0            0            0            0
                       Rx              0            0            0            0
0/ 2  geth0/2  down    Tx              0            0            0            0
                       Rx              0            0            0            0
0/ 3  geth0/3  down    Tx              0            0            0            0
                       Rx              0            0            0            0
(以下省略)
>
```

なお，本コマンド実行時に表示項目 "Discard" の表示が 0 より大きい場合は，パケットが廃棄される障害が発生しています。show interfaces コマンドで該当ポートの詳細情報を取得してください。

3.4.2 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. ログの確認
   ログは，マニュアル「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 3-6 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	show interfaces コマンド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。	ケーブルの種別が正しいか確認してください。種別は「ハードウェア取扱説明書」を参照してください。
			本装置の設定が次の場合はピンマッピングが MDI-X であるか確認してください。 • 該当ポートの設定が固定接続となっている場合 • 該当ポートの設定がオートネゴシエーションかつ自動 MDIX 機能を無効にしている場合
			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。
			本装置でサポートしている接続インタフェースに交換してください。本装置でサポートしている接続インタフェースについては，マニュアル「コンフィグレーションガイド」を参照してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces（イーサネット）コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1 回線をテストする」を参照してください。
2	show interfaces コマンドの受信系エラー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。カウントされている場合，原因と対応欄を参照してください。 • CRC errors • Symbol errors	回線品質が低下しています。	ケーブルの種別が正しいか確認してください。種別は「ハードウェア取扱説明書」を参照してください。
			本装置の設定が次の場合はピンマッピングが MDI-X であるか確認してください。 • 該当ポートの設定が固定接続となっている場合 • 該当ポートの設定がオートネゴシエーションかつ自動 MDIX 機能を無効にしている場合
			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。
			本装置でサポートしている接続インタフェースに交換してください。本装置でサポートしている接続インタフェースについては，マニュアル「コンフィグレーションガイド」を参照してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1 回線をテストする」を参照してください。

項番	確認内容	原因	対応
3	show interfaces コマンド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。カウントされている場合，原因と対応欄を参照してください。 • MDI cross over changed	ケーブルのピンマッピングが不正です。	ピンマッピングを正しく直してください。ピンマッピングについては，マニュアル「コンフィグレーションガイド」を参照してください。
4	show interfaces コマンドのポート 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。	ケーブルが適合していません。	ケーブルの種別が正しいか確認してください。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。
5	show interfaces コマンド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。カウントされている場合，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。
6	show qos queueing コマンド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。 • Tail_drop	パケットの廃棄が発生しています。	廃棄制御および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。

3.4.3 1000BASE-X のトラブル発生時の対応

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. ログの確認
   ログについては，マニュアル「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 3-7 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	show interfaces コマンド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。カウントされている場合，原因と対応欄を参照してください。 • Link down • Signal detect errors	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。種別は「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「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。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。
			トランシーバの接続が正しいか確認してください。
			コンフィグレーションコマンド speed と duplex を相手装置と合わせてください。
			相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1 回線をテストする」を参照してください。
2	show interfaces コマンドの受信系エラー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。カウントされている場合，原因と対応欄を参照してください。 • CRC errors • Symbol errors	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。モードは「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「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。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。
			トランシーバの接続が正しいか確認してください。
			コンフィグレーションコマンド speed と duplex を相手装置と合わせてください。
			相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。

項番	確認内容	原因	対応
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1　回線をテストする」を参照してください。
3	show interfaces コマンド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。カウントされている場合，原因と対応欄を参照してください。 • TX fault	トランシーバが故障しています。	トランシーバを交換してください。
4	show interfaces コマンド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。カウントされている場合，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。
5	show qos queueing コマンド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。 • Tail_drop	パケットの廃棄が発生しています。	廃棄制御および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。

3.4.4　10GBASE-R のトラブル発生時の対応

10GBASE-R 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. ログの確認
   ログについては，マニュアル「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 3-8　10GBASE-R 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	show interfaces コマンド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。カウントされている場合，原因と対応欄を参照してください。 • Signal detect errors	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。種別は「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「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。

項番	確認内容	原因	対応
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れを拭き取ってください。
			トランシーバの接続が正しいか確認してください。
			トランシーバを相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1　回線をテストする」を参照してください。
2	show interfaces コマンドの受信系エラー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。カウントされている場合，原因と対応欄を参照してください。 • CRC errors • Symbol errors	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。種別は「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「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。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。
			トランシーバの接続が正しいか確認してください。
			トランシーバを相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1　回線をテストする」を参照してください。
3	show interfaces コマンド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。カウントされている場合，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	show qos queueing コマンド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。 • Tail_drop	パケットの廃棄が発生しています。	廃棄制御および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。

3.4.5　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 3-9　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，show channel-group コマンドで detail パラメータを指定して確認してください。	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った場合，相手装置と同じモードに変更してください。
2	通信障害となっているポートの運用状態を show channel-group コマンドで detail パラメータを指定して確認してください。	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。 Down ポートは Reason の表示によって以下を行ってください。 • CH Disabled リンクアグリゲーショングループが Disable 状態となって DOWN しています。 • Port Down リンクダウンしています。「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。 • Port Speed Unmatch リンクアグリゲーショングループ内の他ポートと回線速度が不一致となって縮退状態になっています。縮退を回避する場合はリンクアグリゲーショングループ内の全ポートの速度が一致するようにしてください。 • Duplex Half モードが Half となって縮退状態になっています。縮退を回避する場合は Duplex モードを Full に設定してください。 • Port Selecting ポートアグリゲーション条件チェック実施中のため，縮退状態になっています。しばらく待っても回復しない場合は，相手装置の運用状態，および設定を確認してください。
		• Port Moved 接続されていたポートがほかのポートと接続しました。配線の確認をしてください。

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

show vlan コマンド，または show vlan コマンドを detail パラメータ指定で実行し，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。

（2） ポート状態の確認

● show vlan コマンドを detail パラメータ指定で実行し，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，括弧内の要因によって 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って転送停止中です。
STP：スパニングツリーによって転送停止中です。
CNF：コンフィグレーション設定不可のため転送停止中です。
AXRP：Ring Protocol によって転送停止中です。

```
# show vlan detail
      :
VLAN ID:100   Type:Port based  Status:Up
      :
  Port Information
   0/1          Up   Forwarding      Untagged
   0/2          Up   Forwarding      Tagged
```

（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

● show mac-address-table コマンドを実行して，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
MAC address        VLAN    Type     Port-list
0012.e22c.650c       10    Dynamic  0/1
0012.e22c.650b        1    Dynamic  0/2
```

● 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。clear mac-address-table コマンド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。

● 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 制御の帯域監視，廃棄制御もしくは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，システム構築での帯域監視，廃棄制御または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，「3.19.1　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をしてください。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 3-10　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 show spanning-tree コマンドを実行し，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。
		Ring Protocol と PVST+ を共存動作させているとき，対象 VLAN のツリー情報が表示されていない場合は項番 7 へ。
		Disable の場合はスパニングツリーが停止状態になっているためコンフィグレーションを確認してください。
		Ring Protocol とマルチプルスパニングツリーが共存動作している場合は項番 8 へ。
		PVST+ 数が収容条件内に収まっているかを確認してください。
2	障害となっているスパニングツリーに対して show spanning-tree コマンドを実行し，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。

項番	確認内容・コマンド	対応
3	障害となっているスパニングツリーに対して show spanning-tree コマンドを実行し，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。
		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 show spanning-tree statistics コマンドを実行し，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 制御の帯域監視，廃棄制御もしくはシェーパによって BPDU が廃棄されている可能性があります。「3.19.1　フィルタ／QoS 設定情報の確認」を参照し，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，show spanning-tree コマンドを detail パラメータ指定で実行し受信 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，マニュアル「コンフィグレーションガイド」を参照してください。
7	PVST+ で動作させたい VLAN が，Ring Protocol の vlan-mapping に単一で設定されていることを確認してください。	対象 VLAN を Ring Protocol の vlan-mapping に設定していない場合は設定してください。また，vlan-mapping に VLAN を複数設定している場合は，vlan-mapping の構成を見直して単一 VLAN だけを設定してください。
8	MST インスタンスで動作させたい VLAN が，Ring Protocol の vlan-mapping と一致していることを確認してください。	対象 VLAN を Ring Protocol の vlan-mapping に設定していない場合は，マルチプルスパニングツリーで動作する VLAN と一致するように設定してください。

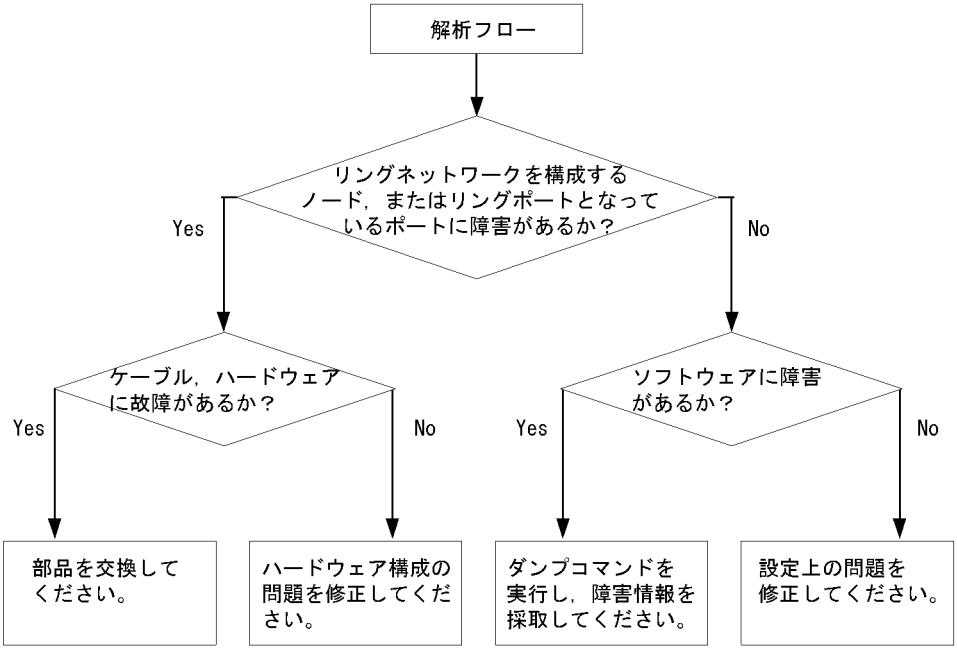
3.5.3　Ring Protocol 機能使用時の障害

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 3-3 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すべてのノードに対して，次の表に示す障害解析方法に従って，原因の切り分けを行ってください。

表 3-11 Ring Protocol の障害解析方法

項番	確認内容・コマンド	対応
1	show axrp コマンドを実行し，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 3 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。
2	show axrp コマンドを実行し，動作モードと属性を確認してください。	"Mode" と "Attribute" の内容がネットワーク構成どおりの動作モードと属性になっている場合には，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。
3	show axrp コマンドを実行し，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 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。
4	show axrp detail コマンドを実行し，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 6 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	show axrp detail コマンドを実行し，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 7 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。

項番	確認内容・コマンド	対応
6	show axrp detail コマンドを実行し，ヘルスチェックフレームの送信間隔のタイマ値とヘルスチェックフレームの保護時間のタイマ値を確認してください。	ヘルスチェックフレームの保護時間のタイマ値 "Health Check Hold Time" が，ヘルスチェックフレームの送信間隔のタイマ値 "Health Check Interval" より大きい（伝送遅延も考慮されている）場合は，項番 8 へ。
		ヘルスチェックフレームの保護時間のタイマ値がヘルスチェックフレームの送信間隔のタイマ値より小さい，または等しい（伝送遅延が考慮されていない）場合には，コンフィグレーションを確認し，設定を見直してください。
7	show vlan detail コマンドを実行し，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場合は，項番 9 および 10 へ。
		異常がある場合は，コンフィグレーションの確認も含め，その状態を復旧してください。
8	フィルタ，QoS 制御の設定を確認してください。	フィルタ，QoS 制御によって，Ring Protocol で使用する制御フレームが廃棄されている可能性があります。「3.19.1　フィルタ／ QoS 設定情報の確認」を参照し，確認してください。また，マニュアル「コンフィグレーションガイド」を参照してください。
9	スパニングツリーを併用する構成の場合，仮想リンクの設定を確認してください。	仮想リンクの設定がネットワーク構成どおりの設定となっているか，コンフィグレーションを確認してください。 • Ring Protocol とスパニングツリーを併用している装置で，仮想リンクの設定がされているか確認してください。 • リングネットワーク全体の装置で，仮想リンクに使用している VLAN が Ring Protocol の VLAN グループに設定されているか確認してください。

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 3-4　解析フロー

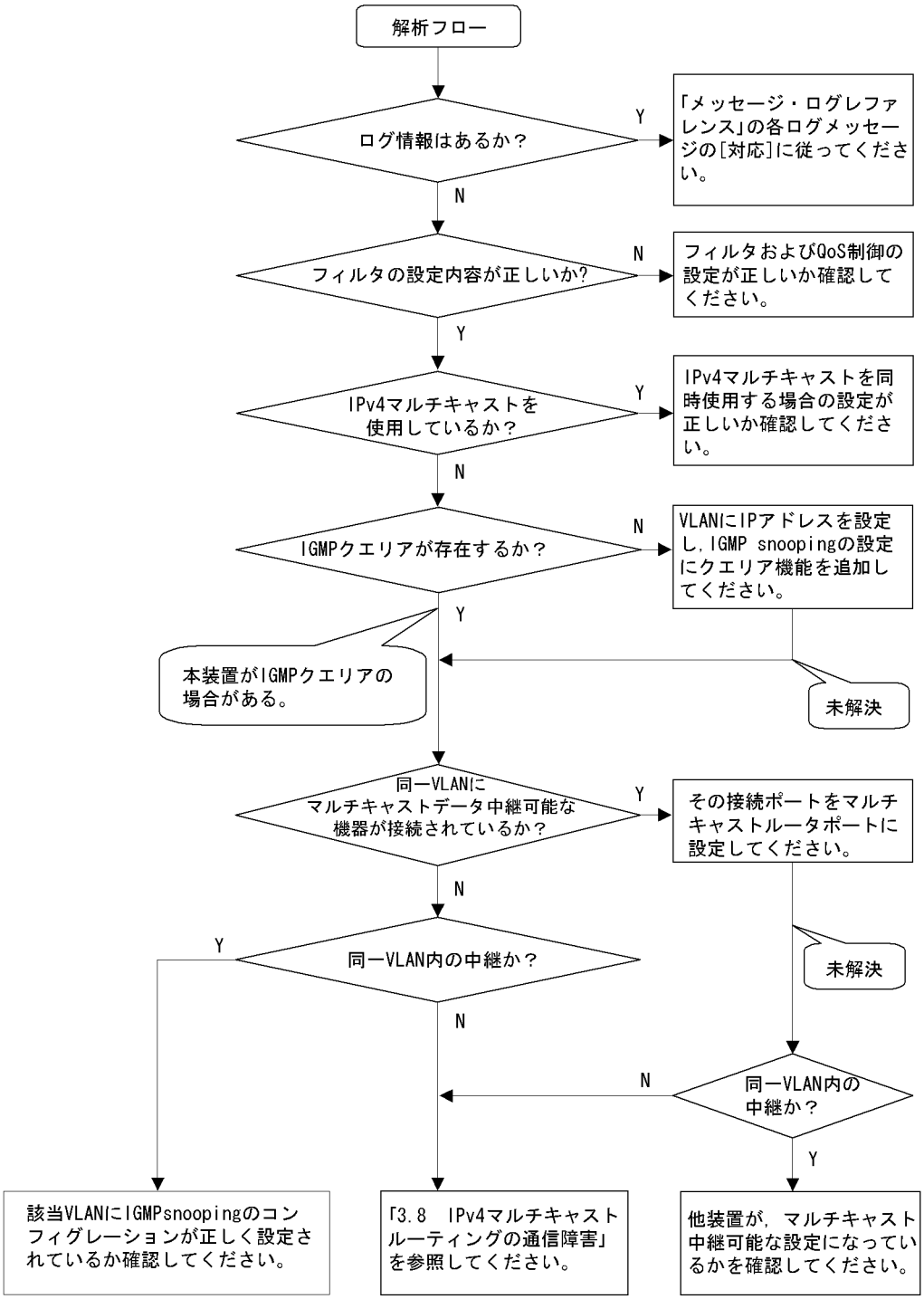


表 3-12　マルチキャスト中継の障害解析方法

項番	確認内容・コマンド	対応
1	show logging コマンドで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 制御の帯域監視，廃棄制御もしくは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，システム構築での帯域監視，廃棄制御または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，「3.19.1　フィルタ／ QoS 設定情報の確認」を参照してください。

3	IPv4 マルチキャストを同時使用する場合の設定が正しいか確認してください。	以下の内容を確認してください。
		• コンフィグレーションコマンド swrt_multicast_table の設定が反映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 swrt_multicast_table が正しく設定されている場合，show system コマンドで表示される「Current selected swrt_multicast_table:」の項目内容に On が表示されます。
		
		`Current selected swrt_multicast_table: On`
		
		コンフィグレーションコマンド swrt_multicast_table を設定しているのに項目内容が Off の場合は，装置再起動が必要です。
		
		• IPv4 マルチキャストと IGMP snooping を同時に使用する場合，該当 VLAN に IPv4 マルチキャストを必ず使用してください。
		
		該当 VLAN に IPv4 マルチキャストを使用している場合，show igmp-snooping コマンドで表示される「IPv4 Multicast routing:」の項目内容に On が表示されます。
		
		`IPv4 Multicast routing: On`
		
		• 該当 VLAN に IPv4 マルチキャストの静的グループ参加機能を使用している場合，マルチキャスト通信が必要なポートにマルチキャストルータポートを設定してください。
		
		• IGMP snooping の登録エントリ数が収容条件を超えた場合，超過後に生成した IPv4 マルチキャストのマルチキャスト中継エントリはマルチキャストルータポートだけの通信となります。IGMP snooping の登録エントリ数を超えないようにネットワークを構成してください。
		
		IGMP snooping の登録エントリ数が収容条件を超えた場合，以下のログ情報が表示されます。
		
		`IGMP snooping: The number of the IGMP snooping entry exceeded the capacity of this system.`

項番	確認内容・コマンド	対応

4	IGMP snooping の構成を show igmp-snooping コマンド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してください。
		
		(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 100`
		`Date 2010/12/01 15:30:00`
		`VLAN 100:`
		`  IP Address:192.168.11.20   Querier : enable`
		`  IGMP querying system : 192.168.11.20`
		`  Port (2): 0/1,0/3`
		`  Mrouter-port:0/1`
		`  Group Counts: 3`

5	show igmp-snooping コマンドで group パラメータを指定し 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 100`
		`Date 2010/12/01 15:30:00`
		`  VLAN 100  Group counts:3`
		`   Group Address     MAC Address`
		`    224.10.10.10   0100.5e0a.0a0a`
		`      Port-list  0/1-3`
		`    225.10.10.10   0100.5e0a.0a0a`
		`      Port-list  0/1-2`
		`    239.192.1.1    0100.5e40.1606`
		`      Port-list  0/1`

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 3-5　解析フロー

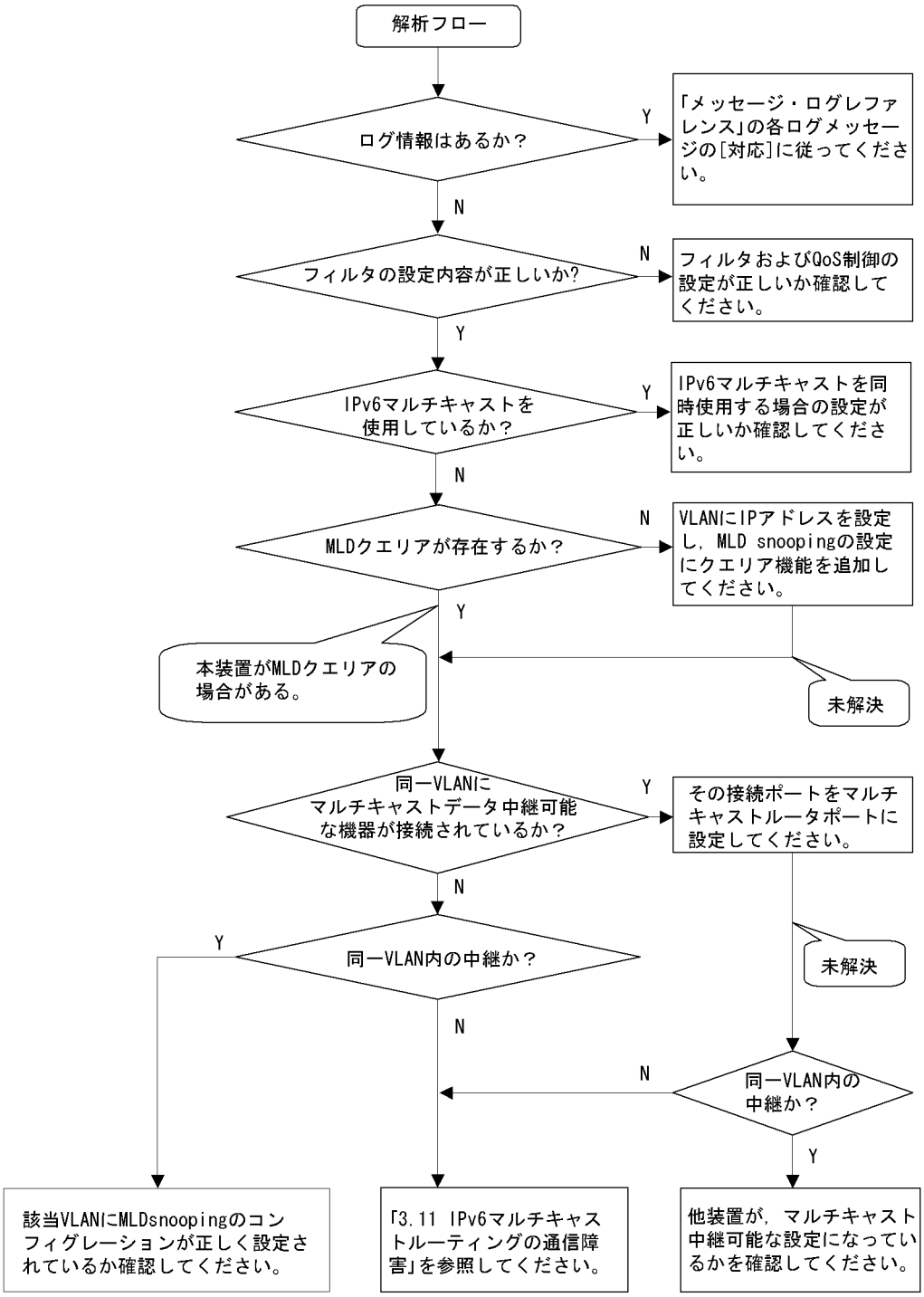


表 3-13 マルチキャスト中継の障害解析方法

項番	確認内容・コマンド	対応
1	show logging コマンドで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 制御の帯域監視，廃棄制御もしくは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，システム構築での帯域監視，廃棄制御または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，「3.19.1 フィルタ／ QoS 設定情報の確認」を参照してください。

3	IPv6 マルチキャストを同時使用する場合の設定が正しいか確認してください。	以下の内容を確認してください。
		• コンフィグレーションコマンド swrt_multicast_table の設定が反映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 swrt_multicast_table が正しく設定されている場合，show system コマンドで表示される「Current selected swrt_multicast_table:」の項目内容に On が表示されます。
		
		`Current selected swrt_multicast_table: On`
		
		コンフィグレーションコマンド swrt_multicast_table を設定しているのに項目内容が Off の場合は，装置再起動が必要です。
		
		• IPv6 マルチキャストと MLD snooping を同時に使用する場合，該当 VLAN に IPv6 マルチキャストを必ず使用してください。
		
		該当 VLAN に IPv6 マルチキャストを使用している場合，show mld-snooping コマンドで表示される「IPv6 Multicast routing:」の項目内容に On が表示されます。
		
		`IPv6 Multicast routing: On`
		
		• 該当 VLAN に IPv6 マルチキャストの静的グループ参加機能を使用している場合，マルチキャスト通信が必要なポートにマルチキャストルータポートを設定してください。
		
		• MLD snooping の登録エントリ数が収容条件を超えた場合，超過後に生成した IPv6 マルチキャストのマルチキャスト中継エントリはマルチキャストルータポートだけの通信となります。MLD snooping の登録エントリ数を超えないようにネットワークを構成してください。
		
		MLD snooping の登録エントリ数が収容条件を超えた場合，以下のログ情報が表示されます。
		
		`MLD snooping: The number of the MLD snooping entry exceeded the capacity of this system.`

項番	確認内容・コマンド	対応

4	MLD snooping の構成を show mld-snooping コマンド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してください。
		
		(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。
		`MLD querying system:`
		
		• 本装置が MLD 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，以下のメッセージが表示されます。
		`IP Address: fe80::200:87ff:fe10:1959*`
		
		(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 mld-snooping 100`
		`Date 2010/12/01 15:30:00`
		`VLAN 100:`
		`IP Address:fe80::200:87ff:fe10:1959 Querier : enable`
		`MLD querying system: fe80::200:87ff:fe10:1959`
		`Port(2): 0/1,0/3`
		`Mrouter-port: 0/1`
		`Group Count :3`

5	show mld-snooping コマンドで group パラメータを指定し 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 100`
		`Date 2010/12/01 15:30:00`
		`VLAN 100  Group count:2`
		`Group Address  MAC Address`
		`ff0e::0e0a:0a01 3333.0e0a.0a01`
		`Port-list  0/1-3`
		`ff0e::0102:0c11 3333.0102.0c11`
		`Port-list  0/1-2`

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。

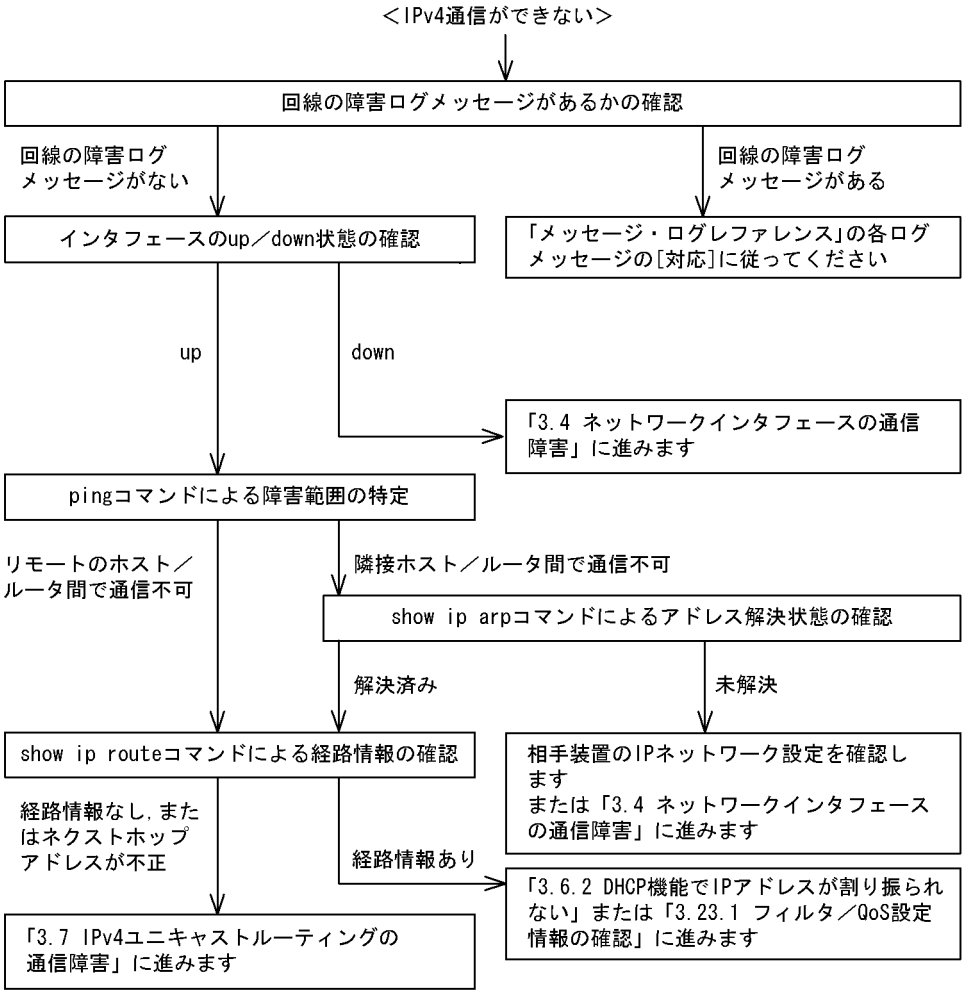
1. IP 通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

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 3-6　IPv4 通信ができない場合の障害解析手順



(1) 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，ログの内容については，マニュアル「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. show logging コマンドを使ってログを表示させます。
3. 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ログの障害の内容および障害への対応については，マニュアル「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. show ip interface コマンド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. ping コマンド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。ping コマンドの操作例および実行結果の見方は，マニュアル「コンフィグレーションガイド」を参照してください。
3. ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使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. ping コマンド実行の結果，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 ping コマンド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

ping コマンド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. show ip arp コマンド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関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. show ip route コマンドを実行して，本装置が取得した経路情報を確認してください。
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ない場合やネクストホップアドレスが不正の場合は「3.7　IPv4 ユニキャストルーティングの通信障害」に進んでください。
4. 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。
   - DHCP ／ BOOTP 機能
     「(7) DHCP ／ BOOTP 設定情報の確認」に進んでください。
   - フィルタ／ QoS 機能
     「(8) フィルタ／ QoS 設定情報の確認」に進んでください。

（7）DHCP ／ BOOTP 設定情報の確認

本装置の DHCP ／ BOOTP のリレーまたはサーバ機能によって隣接装置へ IP アドレスを割り振っている場合は，適切に IP アドレスを割り振れていない可能性があります。

コンフィグレーションの DHCP ／ BOOTP のリレーまたはサーバ機能の設定条件が正しいか見直してください。手順については，「3.6.2　DHCP 機能で IP アドレスが割り振られない」を参照してください。

（8）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 制御の帯域監視，廃棄制御もしくは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，システム構築での帯域監視，廃棄制御または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，「3.19.1　フィルタ／ QoS 設定情報の確認」を参照してください。

3.6.2　DHCP 機能で IP アドレスが割り振られない

（1） DHCP ／ BOOTP リレーの通信トラブル

DHCP ／ BOOTP リレーの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。

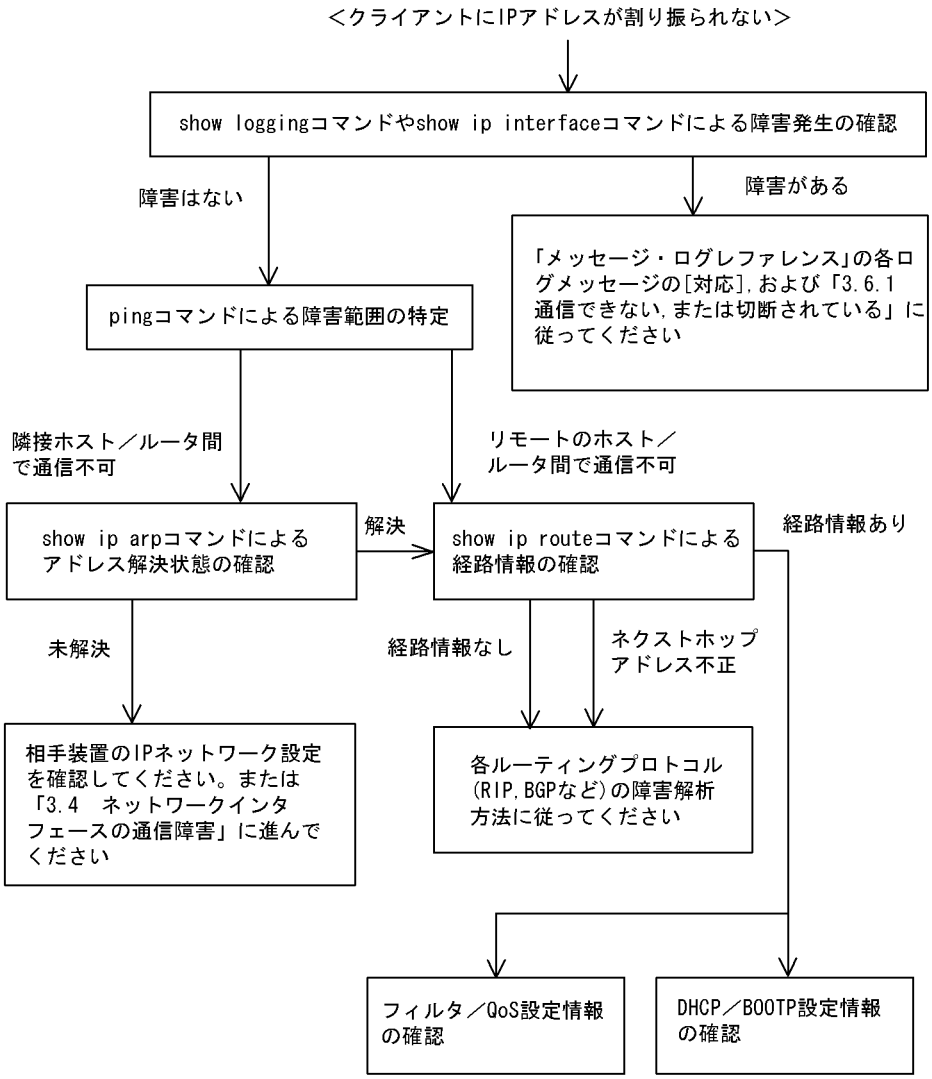
1. DHCP ／ BOOTP リレー通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. DHCP ／ BOOTP サーバの障害

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。

ここでは，クライアントの設定（ネットワークカードの設定，ケーブルの接続など）は確認されているものとし，上記 1. および 3. に示すような「コンフィグレーションの変更を行ったら，DHCP ／ BOOTP サーバから IP アドレスが割り振られなくなった」，「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，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 3-7　DHCP/BOOTP リレーの障害解析手順



(a) 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。本装置が表示するログや show ip interface コマンド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「3.6.1　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。

(b) 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。

1. 本装置にログインします。
2. ping コマンド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。ping コマンドの操作例および実行結果の見方は，マニュアル「コンフィグレーションガイド」を参照してください。
3. ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使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. ping コマンド実行の結果，障害範囲が隣接装置の場合は「(d) 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「(e) 経路情報の確認」に進んでください。

(c) 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 ping コマンド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の特定ができましたら，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。

(d) 隣接装置との ARP 解決情報の確認

ping コマンドによって隣接装置との疎通が不可のときは，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. show ip arp コマンド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，「(e) 経路情報の確認」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疎通できる設定になっているかを確認してください。

(e) 経路情報の確認

隣接装置とのアドレスが解決しているにも関わらず通信ができない，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. show ip route コマンドを使っ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ない場合やネクストホップアドレスが不正の場合は「3.7　IPv4 ユニキャストルーティングの通信障害」に進んでください。
4. 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／ QoS 機能
     「(f) フィルタ／ QoS 設定情報の確認」に進んでください。
   - DHCP ／ BOOTP 機能
     「(g) DHCP ／ BOOTP 設定情報の確認」に進んでください。

(f) 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だけを廃棄する設定になっているか，QoS 制御の帯域監視，廃棄制御または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，システム構築での帯域監視，廃棄制御または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，「3.19.1 フィルタ／QoS 設定情報の確認」を参照してください。

(g) DHCP ／ BOOTP 設定情報の確認

DHCP ／ BOOTP サーバに貸し出し用 IP アドレスが十分に残っている場合，DHCP ／ BOOTP リレーのコンフィグレーション設定ミスによってクライアントに IP アドレスが割り振られないという原因が考えられます。次にコンフィグレーションの確認手順を示します。

1. ip helper-address は DHCP ／ BOOTP サーバの IP アドレス，または DHCP ／ BOOTP リレーエージェント機能付き次ルータの IP アドレスが指定されているか確認してください。
2. クライアント側のインタフェースに ip helper-address が設定されているか確認してください。
3. ip bootp-hops の値がクライアントから見て正しい bootp hops 値となっているか確認してください。
4. マルチホーム構成の場合は ip relay-agent-address の値と DHCP/BOOTP サーバで配布する IP アドレスのサブネットが一致しているか確認してください。

(h) DHCP リレーと VRRP が同一インタフェースで運用されている場合の確認

DHCP ／ BOOTP リレーと VRRP が同一インタフェースで運用されている場合，DHCP ／ BOOTP サーバで，DHCP ／ BOOTP クライアントゲートウェイアドレス（ルータオプション）を VRRP コンフィグレーションで設定した仮想ルータアドレスに設定しなければなりません。設定しなかった場合，VRRP によるマスタ・スタンバイルータ切り替え後，DHCP ／ BOOTP クライアントが通信できなくなる可能性があります。確認方法については各 DHCP ／ BOOTP サーバの確認方法に従ってください。

(2) DHCP サーバの通信トラブル

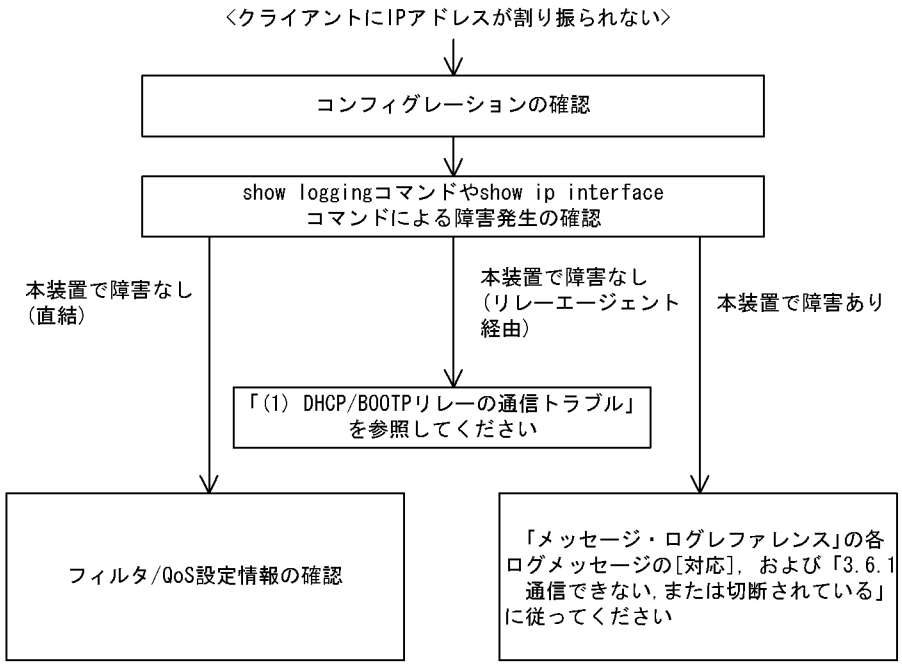
DHCP サーバの通信トラブル（クライアントにアドレス配信できない）が発生する要因として考えられるのは，次の 3 種類があります。

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) ログメッセージおよびインタフェースの確認」～「(e) フィルタ／QoS 設定情報の確認」に示します。

障害部位および原因の切り分け手順を次のフローに示します。

図 3-8　DHCP サーバの障害解析手順



(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設定ミスによってクライアントに 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。

1. 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。
2. 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。
3. クライアントが本装置からアドレスを割り振られたあと，クライアントと他装置との通信ができない場合は，デフォルトルータの設定がされていないことがあります。コンフィグレーションコマンド default-router でクライアントが接続されているネットワークのルータアドレス（デフォルトルータ）が設定されているか確認してください（マニュアル「コンフィグレーションコマンドレファレンス」を参考にしてください）。
4. 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。リレーエージェントも本装置を使用している場合，「(1) DHCP ／ BOOTP リレーの通信トラブル」を参照してください。

(b) ログメッセージ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。本装置が表示するログメッセージや show ip interface コマンド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「3.6.1　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。

(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。

1. 本装置にログインします。

2. クライアントとサーバ間にルータなどがある場合，ping コマンド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（ルータ）の疎通を確認してください。ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使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。ping コマンドの操作例および実行結果の見方については，マニュアル「コンフィグレーションガイド」を参照してください。
3. 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。
4. ping コマンドによる障害範囲が隣接装置かリモートの装置かによって，障害解析フローの次のステップに進んでください。

(d) 経路情報の確認

隣接装置とのアドレスが解決しているにも関わらず通信ができない，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. show ip route コマンドを使って本装置が取得した経路情報を確認してください。

(e) 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だけが廃棄されているか，QoS 制御の帯域監視，廃棄制御または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，システム構築での帯域監視，廃棄制御またはシェーパの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見直しを行ってください。手順については，「3.19.1　フィルタ／ QoS 設定情報の確認」を参照してください。

(f) 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。

3.6.3　DHCP 機能で DynamicDNS 連携が動作しない

(1) DHCP サーバの通信トラブル

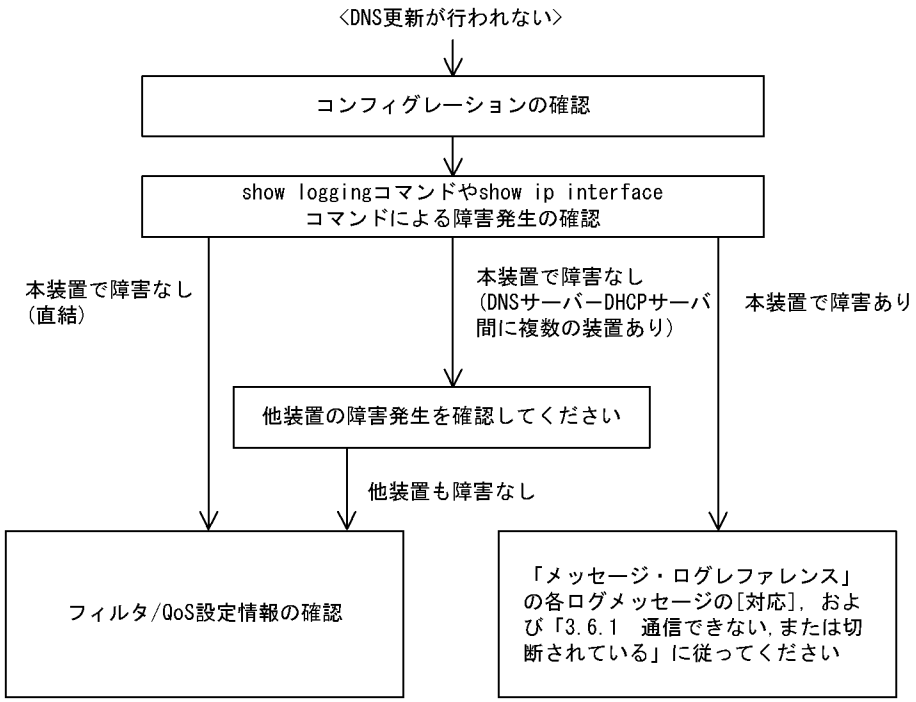
DHCP サーバの通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. 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。DNS サーバ／ DHCP 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 DynamicDNS 連携が動作しない」，というケースについては，詳細を「(b) 時刻情報の確認」～「(f) フィルタ／ QoS 設定情報の確認」に示します。

障害部位および原因の切り分け手順を次のフローに示します。

図 3-9 DNS 連携時の DHCP サーバ障害解析手順



(a) コンフィグレーションの確認

DHCP サーバ上のミス，または DNS サーバ上の設定との不一致によって DynamicDNS に対する DNS 更新が正しく動作していないことが原因と考えられます。コンフィグレーションの確認手順を次に示します。

1. 始めに DNS サーバ側で DNS 更新を許可する方法を確認してください。IP アドレス／ネットワークによるアクセス許可の場合は項目 3 以降を参照してください。認証キーによる許可の場合は項目 2 以降を参照してください。
2. DNS サーバ側で指定しているキー情報，認証キーと DHCP サーバコンフィグレーションで設定されているキー情報が同じであることを確認してください（マニュアル「コンフィグレーションコマンドレファレンス」を参考にしてください)。
3. DNS サーバ側で指定しているゾーン情報と DHCP サーバコンフィグレーションのゾーン情報が一致していることを確認してください（マニュアル「コンフィグレーションコマンドレファレンス」を参考にしてください)。また，このときに正引きと逆引きの両方が設定されていることを確認してください。
4. DNS 更新が設定されていることを確認してください（マニュアル「コンフィグレーションコマンドレファレンス」を参考にしてください)。デフォルトでは DNS 更新は無効になっているため，DNS 更新を行う場合は本設定を行う必要があります
5. クライアントが使用するドメイン名が DNS サーバに登録してあるドメイン名と一致していることを確認してください。DHCP によってドメイン名を配布する場合はコンフィグレーションで正しく設定されていることを確認してください（マニュアル「コンフィグレーションコマンドレファレンス」およびマニュアル「運用コマンドレファレンス」を参考にしてください)。

(b) 時刻情報の確認

DNS 更新で認証キーを使用するとき，本装置と DNS サーバが指す時刻の差は多くの場合 UTC 時間で 5 分以内である必要があります。show clock コマンドで本装置の時刻情報を確認して，必要ならばマニュアル「コンフィグレーションコマンドレファレンス」を参考に時刻情報の同期を行ってください。

(c) ログメッセージおよびインタフェースの確認

DNS サーバとの通信ができなくなる原因の一つに DNS サーバー DHCP 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。本装置が表示するログメッセージや show ip interface コマンド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「3.6.1　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。

(d) 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。

1. 本装置にログインします。
2. DNS サーバと DHCP サーバ間にルータなどがある場合，ping コマンドを使って通信できない相手（DNS サーバ）との間にある装置（ルータ）の疎通を確認してください。ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使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。ping コマンドの操作例および実行結果の見方については，マニュアル「コンフィグレーションガイド」を参照してください。
3. DNS サーバと DHCP サーバが直結の場合，HUB やケーブルの接続を確認してください。
4. ping コマンドによる障害範囲が隣接装置かリモートの装置かによって，障害解析フローの次のステップに進んでください。

(e) 経路情報の確認

隣接装置とのアドレスが解決しているにも関わらず通信ができない，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. show ip route コマンドを使って本装置が取得した経路情報を確認してください。

(f) 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だけが廃棄されているか，QoS 制御の帯域監視，廃棄制御または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，システム構築での帯域監視，廃棄制御またはシェーパのシステム運用が適切であるか，本装置および DNS サーバ・DHCP 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，「3.19.1　フィルタ／ QoS 設定情報の確認」を参照してください。

(g) レイヤ 2 ネットワークの確認

(a) から (f) 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　IPv4 ユニキャストルーティングの通信障害

3.7.1　RIP 経路情報が存在しない

本装置が取得した経路情報の表示に，RIP の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-14　RIP の障害解析方法

項番	確認内容・コマンド	対応
1	RIP の隣接情報を表示します。 show ip rip neighbor	隣接ルータのインタフェースが表示されていない場合は項番 2 へ。
		隣接ルータのインタフェースが表示されている場合は項番 3 へ。
2	コンフィグレーションで RIP 設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが RIP 経路を広告しているか確認してください。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。

3.7.2　OSPF 経路情報が存在しない

本装置が取得した経路情報の表示に，OSPF の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-15　OSPF の障害解析方法

項番	確認内容・コマンド	対応
1	OSPF のインタフェース状態を確認します。 show ip ospf interface <IP Address>	インタフェースの状態が DR の場合は項番 3 へ。
		インタフェースの状態が BackupDR または DR Other の場合は項番 2 へ。
		インタフェースの状態が Waiting の場合は，時間を置いてコマンドを再実行してください。項番 1 へ。
2	Neighbor List より DR との隣接ルータ状態を確認します。	DR との隣接ルータ状態が Full 以外の場合は項番 4 へ。
		DR との隣接ルータ状態が Full の場合は項番 5 へ。
3	Neighbor List より全隣接ルータ状態を確認します。	一部の隣接ルータ状態が Full 以外の場合は項番 4 へ。
		全隣接ルータ状態が Full の場合は項番 5 へ。
4	コンフィグレーションで OSPF の設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 5 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。

項番	確認内容・コマンド	対応
5	OSPF 経路を学習している経路を確認してください。 show ip route all-routes	経路が InActive の場合には項番 6 へ。
		経路が存在しない場合は隣接ルータが OSPF 経路を広告しているか確認してください。
6	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが OSPF 経路を広告しているか確認してください。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。

3.7.3 BGP4 経路情報が存在しない

本装置が取得した経路情報の表示に，BGP4 の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-16 BGP4 の障害解析方法

項番	確認内容・コマンド	対応
1	BGP4 のピア状態を確認します。 show ip bgp neighbors	ピア状態が Established 以外の場合は項番 2 へ。
		ピア状態が Established の場合は項番 3 へ。
2	コンフィグレーションで BGP4 の設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	BGP4 経路を学習しているか確認してください。 show ip bgp received-routes	経路が存在するが active 状態でない場合は項番 4 へ。
		経路が存在しない場合は項番 5 へ。
4	BGP4 経路のネクストホップアドレスを解決する経路情報が存在するか確認してください。 show ip route	ネクストホップアドレスを解決する経路情報がある場合は項番 5 へ。
		ネクストホップアドレスを解決する経路情報がない場合はその経路情報を学習するためのプロトコルの障害解析を実施してください。
5	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが BGP4 経路を広告しているか確認してください。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。

3.8　IPv4 マルチキャストルーティングの通信障害

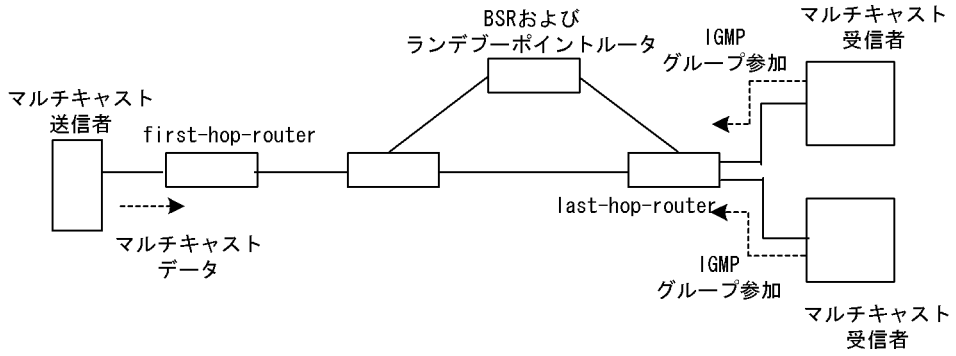
本装置で IPv4 マルチキャスト通信障害が発生した場合の対処について説明します。

3.8.1　IPv4 PIM-SM ネットワークで通信ができない

IPv4 PIM-SM ネットワーク構成でマルチキャスト中継ができない場合は，以下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。

IPv4 PIM-SM のネットワーク例を次の図に示します。

図 3-10　IPv4 PIM-SM ネットワーク例



注

- BSR：ランデブーポイントの情報を配信するルータ（詳細は，マニュアル「コンフィグレーションガイド」を参照してください）
- ランデブーポイントルータ：中継先が確定していないパケットをマルチキャスト受信者方向に中継するルータ（詳細は，マニュアル「コンフィグレーションガイド」を参照してください）
- first-hop-router：マルチキャスト送信者と直接接続するルータ
- last-hop-router：マルチキャスト受信者と直接接続するルータ

（1）共通確認内容

次の表に，IPv4 PIM-SM ネットワーク構成のすべての本装置に対する共通確認内容を示します。

表 3-17　共通確認内容

項番	確認内容・コマンド	対応
1	コンフィグレーションにマルチキャスト機能を使用する指定（ip multicast routing）があることを確認してください。 show running-config	マルチキャスト機能を使用する指定がない場合は，コンフィグレーションを修正してください。
2	一つ以上のインタフェースで PIM が動作していることを確認してください。 show ip pim interface	動作していない場合はコンフィグレーションを確認し，どれか一つ以上のインタフェースで PIM が動作するように設定してください。 コンフィグレーションで PIM の動作設定をしたインタフェースが，show ip pim interface コマンドで表示されない場合は，該当インタフェースにマルチホームの設定がされていないことを確認してください。

項番	確認内容・コマンド	対応
3	PIM が動作するインタフェースに，IGMP snooping が設定されているか確認してください。 show igmp-snooping	IGMP snooping が設定されている場合は，以下の内容を確認してください。 • 隣接ルータと接続しているポートに対して IGMP snooping のマルチキャストルータポートの設定がされているか確認してください。 •「3.5.4　IGMP snooping によるマルチキャスト中継ができない」を参照してください。
4	PIM および IGMP が動作するインタフェースで，フィルタなどによるプロトコルパケットおよびマルチキャストパケット中継を抑止する設定がないことを，コンフィグレーションで確認してください。 show running-config	プロトコルパケットおよびマルチキャストパケット中継を抑止する設定がある場合は，コンフィグレーションを修正してください。
5	PIM の隣接情報を確認してください。 show ip pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ip pim interface コマンドで確認してください。 • 隣接ルータの設定を確認してください。
6	マルチキャストデータ送信者へのユニキャスト経路が存在するか確認してください。 show ip route	ユニキャスト経路が存在しない場合は「3.7　IPv4 ユニキャストルーティングの通信障害」を参照してください。
7	マルチキャストデータ送信者への次ホップアドレスと接続しているインタフェースで，PIM が動作していることを確認してください。 show ip pim interface	動作していない場合はコンフィグレーションを確認し，マルチキャストデータ送信者への次ホップアドレスと接続しているインタフェースで PIM が動作するように設定してください。
8	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていないことを，コンフィグレーションで確認してください。 show running-config	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれている場合は，コンフィグレーションを修正してください。
9	BSR が決定されていることを確認してください。ただし，中継対象グループアドレスに対するランデブーポイントが静的ランデブーポイントの場合は，確認不要です。 show ip pim bsr	BSR が決定されていない場合は BSR へのユニキャスト経路が存在するか確認してください。ユニキャスト経路が存在しない場合は，「3.7　IPv4 ユニキャストルーティングの通信障害」を参照してください。 ユニキャスト経路が存在する場合は，BSR の設定を確認してください。BSR が本装置の場合は，「(2) BSR 確認内容」を参照してください。
10	ランデブーポイントが決定されていることを確認してください。 show ip pim rp-mapping	ランデブーポイントが決定されていない場合は，ランデブーポイントへのユニキャスト経路が存在するか確認してください。ユニキャスト経路が存在しない場合は，「3.7　IPv4 ユニキャストルーティングの通信障害」を参照してください。 ユニキャスト経路が存在する場合は，ランデブーポイントの設定を確認してください。ランデブーポイントが本装置の場合は，「(3) ランデブーポイントルータ確認内容」を参照してください。
11	ランデブーポイントのグループアドレスに，中継対象グループアドレスが含まれていることを確認してください。 show ip pim rp-mapping	中継対象グループアドレスが含まれていない場合は，ランデブーポイントルータの設定を確認してください。ランデブーポイントが本装置の場合は，「(3) ランデブーポイントルータ確認内容」を参照してください。
12	マルチキャスト中継エントリが存在することを確認してください。 show ip mcache	マルチキャスト中継エントリが存在しない場合は，上流ポートにマルチキャストデータが届いていることを確認してください。マルチキャストデータが届いていない場合は，マルチキャスト送信者あるいは上流ルータの設定を確認してください。

項番	確認内容・コマンド	対応
13	マルチキャスト経路情報が存在することを確認してください。 show ip mroute	マルチキャスト経路情報が存在しない場合は，下流ルータの設定を確認してください。
14	マルチキャスト経路情報かマルチキャスト中継エントリが上限を超えていないか確認してください。 マルチキャスト経路情報： 　show ip mroute マルチキャスト中継エントリ： 　show ip mcache 　netstat multicast	Warning が出力されている場合は，想定していないマルチキャスト経路情報またはマルチキャスト中継エントリが作成されていないか確認してください。マルチキャスト中継エントリでネガティブキャッシュが多い場合は，不要なパケットを送信している端末が存在しないか確認してください。

（2） BSR 確認内容

次の表に，IPv4 PIM-SM ネットワーク構成で本装置が BSR の場合の確認内容を示します。

表 3-18　BSR 確認内容

項番	確認内容・コマンド	対応
1	本装置が BSR 候補であることを確認してください。 show ip pim bsr	本装置が BSR 候補でない場合はコンフィグレーションを確認し，BSR 候補として動作するように設定してください。また，loopback インタフェースにアドレスが設定されていないと BSR 候補として動作しないため，loopback インタフェースにアドレスが設定されていることも確認してください。
2	本装置が BSR であることを確認してください。 show ip pim bsr	本装置が BSR でない場合は，ほかの BSR 候補の優先度を確認してください。優先度は値の大きい方が高くなります。優先度が同じ場合は，BSR アドレスが一番大きい BSR 候補が BSR となります。

（3） ランデブーポイントルータ確認内容

次の表に，IPv4 PIM-SM ネットワーク構成で本装置がランデブーポイントルータの場合の確認内容を示します。

表 3-19　ランデブーポイントルータ確認内容

項番	確認内容・コマンド	対応
1	本装置が中継対象グループアドレスに対するランデブーポイント候補であることを確認してください。 show ip pim rp-mapping	本装置が中継対象グループアドレスに対するランデブーポイント候補でない場合は，コンフィグレーションを確認し，中継対象グループアドレスに対するランデブーポイント候補として動作するように設定してください。また，loopback インタフェースにアドレスが設定されていないとランデブーポイント候補として動作しないため，loopback インタフェースにアドレスが設定されていることも確認してください
2	本装置が中継対象グループアドレスに対するランデブーポイントであることを確認してください。 show ip pim rp-hash <Group Address>	本装置がランデブーポイントでない場合は，ほかのランデブーポイント候補の優先度を確認してください。優先度は値の小さい方が高くなります。ほかのランデブーポイント候補の優先度が高い場合はランデブーポイントとして動作せず，優先度が同一の場合は，プロトコルの仕様でグループアドレス単位に分散され，該当グループに対してランデブーポイントとして動作しないことがあります。本装置を優先的にランデブーポイントとして動作させる場合は，ほかのランデブーポイント候補より高い優先度を設定してください。

（4） last-hop-router 確認内容

次の表に，IPv4 PIM-SM ネットワーク構成で本装置が last-hop-router の場合の確認内容を示します。

表 3-20 last-hop-router 確認内容

項番	確認内容・コマンド	対応
1	マルチキャスト受信者と接続しているインタフェースで，IGMP が動作していることを確認してください。 show ip igmp interface	動作していない場合はコンフィグレーションを確認し，IGMP が動作するように設定してください。
2	マルチキャスト受信者が，IGMP で中継対象グループに参加していることを確認してください。 show ip igmp group	中継対象グループに参加していない場合は，マルチキャスト受信者の設定を確認してください。
3	中継対象グループが参加しているインタフェースがある場合は，本装置が DR であることを確認してください。 show ip pim interface	本装置が DR でない場合は，中継対象インタフェースの DR を調査してください。
4	静的グループ参加機能が動作するインタフェースに，IGMP snooping が設定されているか確認してください。 show igmp-snooping	IGMP snooping が設定されている場合は，以下の内容を確認してください。 • 中継先ポートに対して IGMP snooping のマルチキャストルータポートの設定がされているか確認してください。 •「3.5.4 IGMP snooping によるマルチキャスト中継ができない」を参照してください。
5	各インタフェースで異常を検出していないか確認してください。 show ip igmp interface	Notice を確認し，警告情報が出力されていないことを確認してください。 警告情報が出力されている場合は以下を確認してください。 • L：想定した最大数を超えて参加要求が発生しています。接続ユーザ数を確認してください。 • Q：隣接するルータと IGMP のバージョンが不一致となっています。IGMP のバージョンを合わせてください。 • R：現在の設定では受信できない Report を送信しているユーザが存在します。本装置の IGMP のバージョンを変更するか，参加ユーザの設定を確認してください。 • S：IGMPv3 で 1 メッセージ内に格納できるソース数が上限を超えたため参加情報を一部廃棄しています。参加ユーザの設定を確認してください。

（5） first-hop-router 確認内容

次の表に，IPv4 PIM-SM ネットワーク構成で本装置が first-hop-router の場合の確認内容を示します。

表 3-21 first-hop-router 確認内容

項番	確認内容・コマンド	対応
1	本装置がマルチキャスト送信者と直接接続していることを確認してください。	直接接続していない場合はネットワーク構成を確認してください。

項番	確認内容・コマンド	対応
2	マルチキャスト送信者と接続しているインタフェースで，PIM または IGMP が動作していることを確認してください。 show ip pim interface show ip igmp interface	動作していない場合はコンフィグレーションを確認し，PIM または IGMP が動作するように設定してください。
3	マルチキャスト経路情報が存在するか確認してください。 show ip mroute	マルチキャスト経路情報が存在しない場合は，マルチキャストデータ送信元アドレスが，マルチキャスト送信者と直接接続しているインタフェースのネットワークアドレスであることを確認してください。

3.8.2　IPv4 PIM-SM ネットワークでマルチキャストデータが二重中継される

IPv4 PIM-SM ネットワーク構成でマルチキャストデータが二重中継される場合は，各ルータの設定内容を確認し，同一ネットワークに複数のルータが存在するインタフェースでは PIM が動作するように設定してください。

上記の設定をしても二重中継が継続する場合の確認内容を次の表に示します。

表 3-22　二重中継が継続する場合の確認

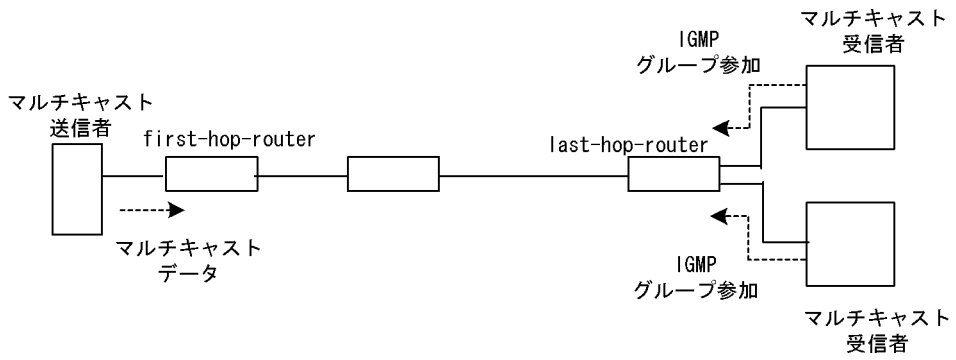
項番	確認内容・コマンド	対応
1	同一ネットワークに複数のルータが存在するインタフェースの PIM の隣接情報を確認してください。 show ip pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ip pim interface コマンドで確認してください。 • フィルタなどによるプロトコルパケットの中継を抑止する設定がないことを，コンフィグレーションで確認してください。 • 隣接ルータの設定を確認してください。

3.8.3　IPv4 PIM-SSM ネットワークで通信ができない

IPv4 PIM-SSM ネットワーク構成でマルチキャスト中継ができない場合は，以下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。

IPv4 PIM-SSM のネットワーク例を次の図に示します。

図 3-11　IPv4 PIM-SSM ネットワーク例



注

- first-hop-router：マルチキャスト送信者と直接接続するルータ
- last-hop-router：マルチキャスト受信者と直接接続するルータ

(1) 共通確認内容

次の表に，IPv4 PIM-SSM ネットワーク構成のすべての本装置に対する共通確認内容を示します。

表 3-23 共通確認内容

項番	確認内容・コマンド	対応
1	コンフィグレーションにマルチキャスト機能を使用する指定（ip multicast routing）があることを確認してください。 show running-config	マルチキャスト機能を使用する指定がない場合は，コンフィグレーションを修正してください。
2	一つ以上のインタフェースで PIM が動作していることを確認してください。 show ip pim interface	動作していない場合はコンフィグレーションを確認し，どれか一つ以上のインタフェースで PIM が動作するように設定してください。コンフィグレーションで PIM の動作設定をしたインタフェースが，show ip pim コマンドの interface パラメータ指定時に表示されない場合は，該当インタフェースにマルチホームの設定がされていないことを確認してください。
3	PIM が動作するインタフェースに，IGMP snooping が設定されているか確認してください。 show igmp-snooping	IGMP snooping が設定されている場合は，以下の内容を確認してください。 • 隣接ルータと接続しているポートに対して IGMP snooping のマルチキャストルータポートの設定がされているか確認してください。 •「3.5.4 IGMP snooping によるマルチキャスト中継ができない」を参照してください。
4	PIM および IGMP が動作するインタフェースで，フィルタなどによるプロトコルパケットおよびマルチキャストパケット中継を抑止する設定がないことをコンフィグレーションで確認してください。 show running-config	プロトコルパケットおよびマルチキャストパケット中継を抑止する設定がある場合は，コンフィグレーションを修正してください。
5	PIM の隣接情報を確認してください。 show ip pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ip pim で interface パラメータを指定して確認してください。 • 隣接ルータの設定を確認してください。
6	マルチキャストデータ送信者へのユニキャスト経路が存在するか確認してください。 show ip route	ユニキャスト経路が存在しない場合は，「3.7 IPv4 ユニキャストルーティングの通信障害」を参照してください。
7	マルチキャストデータ送信者へのユニキャスト経路送出インタフェースで，PIM が動作していることを確認してください。 show ip pim interface	動作していない場合はコンフィグレーションを確認し，ユニキャスト経路送出インタフェースで PIM が動作するように設定してください。
8	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていることを，コンフィグレーションで確認してください。 show running-config	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていない場合は，コンフィグレーションを修正してください。

項番	確認内容・コマンド	対応
9	マルチキャスト経路情報が存在するか確認してください。 show ip mroute	マルチキャスト経路情報が存在しない場合は，下流ルータの設定を確認してください。
10	マルチキャスト経路情報かマルチキャスト中継エントリが上限を超えていないか確認してください。 マルチキャスト経路情報： 　show ip mroute マルチキャスト中継エントリ： 　show ip mcache 　netstat multicast	Warning が出力されている場合は，想定していないマルチキャスト経路情報またはマルチキャスト中継エントリが作成されていないか確認してください。マルチキャスト中継エントリでネガティブキャッシュが多い場合は，不要なパケットを送信している端末が存在しないか確認してください。

（2） last-hop-router 確認内容

次の表に，IPv4 PIM-SSM ネットワーク構成で本装置が last-hop-router の場合の確認内容を示します。

表 3-24　last-hop-router 確認内容

項番	確認内容・コマンド	対応
1	コンフィグレーションに IGMPv1/IGMPv2 で PIM-SSM の連携動作が使用できる指定（ip igmp ssm-map enable）があることを確認してください。 show running-config	IGMPv1/IGMPv2 で PIM-SSM の連携動作が使用できる指定がない場合は，コンフィグレーションを修正してください。
2	コンフィグレーションに PIM-SSM で中継するグループアドレスと送信元アドレスが，IGMPv1/IGMPv2 で PIM-SSM と連携動作する設定（ip igmp ssm-map static）があることを確認してください。 show running-config	IGMPv1/IGMPv2 で PIM-SSM と連携動作する設定がない場合は，コンフィグレーションを修正してください。
3	マルチキャスト受信者と接続しているインタフェースで IGMP が動作していることを確認してください。 show ip igmp interface	動作していない場合は，コンフィグレーションを確認し IGMP が動作するように設定してください。
4	マルチキャスト受信者が IGMP で中継対象グループに参加していることを確認してください。 show ip igmp group	中継対象グループにグループ参加していない場合は，マルチキャスト受信者の設定を確認してください。
5	中継対象グループが参加しているインタフェースがある場合は，本装置が DR であることを確認してください。 show ip pim interface	本装置が DR でない場合は，中継対象インタフェースの DR を調査してください。

項番	確認内容・コマンド	対応
6	静的グループ参加機能が動作するインタフェースに，IGMP snooping が設定されているか確認してください。 show igmp-snooping	IGMP snooping が設定されている場合は，以下の内容を確認してください。 • 中継先ポートに対して IGMP snooping のマルチキャストルータポートの設定がされているか確認してください。 •「3.5.4　IGMP snooping によるマルチキャスト中継ができない」を参照してください。
7	各インタフェースで異常を検出していないか確認してください。 show ip igmp interface	Notice を確認し，警告情報が出力されていないことを確認してください。 警告情報が出力されている場合は以下を確認してください。 • L：想定した最大数を超えて参加要求が発生しています。接続ユーザ数を確認してください。 • Q：隣接するルータと IGMP のバージョンが不一致となっています。IGMP のバージョンを合わせてください。 • R：現在の設定では受信できない Report を送信しているユーザが存在します。本装置の IGMP のバージョンを変更するか，参加ユーザの設定を確認してください。 • S：IGMPv3 で 1 メッセージ内に格納できるソース数が上限を超えたため参加情報を一部廃棄しています。参加ユーザの設定を確認してください。

（3） first-hop-router 確認内容

次の表に，IPv4 PIM-SSM ネットワーク構成で本装置が first-hop-router の場合の確認内容を示します。

表 3-25　first-hop-router 確認内容

項番	確認内容・コマンド	対応
1	本装置がマルチキャスト送信者と直接接続していることを確認してください。	直接接続していない場合はネットワーク構成を確認してください。
2	マルチキャスト送信者と接続しているインタフェースで，PIM または IGMP が動作していることを確認してください。 show ip pim interface show ip igmp interface	動作していない場合はコンフィグレーションを確認し，PIM または IGMP が動作するように設定してください。
3	マルチキャストデータが本装置に届いているか確認してください。	マルチキャストデータが届いていない場合は，マルチキャスト送信者の設定を確認してください。
4	マルチキャストデータとマルチキャスト経路情報のグループアドレスと送信元アドレスが一致するか確認してください。 show ip mroute show netstat multicast	グループアドレスと送信元アドレスが一致しない場合は，マルチキャスト送信者と last-hop-router の設定内容を確認してください。

3.8.4　IPv4 PIM-SSM ネットワークでマルチキャストデータが二重中継される

IPv4 PIM-SSM ネットワーク構成でマルチキャストデータが二重中継される場合は，各ルータの設定内容を確認し，同一ネットワークに複数のルータが存在するインタフェースでは PIM が動作するように設定してください。

上記の設定をしても二重中継が継続する場合の確認内容を次の表に示します。

表 3-26 二重中継が継続する場合の確認内容

項番	確認内容・コマンド	対応
1	同一ネットワークに複数のルータが存在するインタフェースの PIM の隣接情報を確認してください。 show ip pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ip pim コマンドで interface パラメータを指定して確認してください。 • フィルタなどによるプロトコルパケットの中継を抑止する設定がないことを，コンフィグレーションで確認してください。 • 隣接ルータの設定を確認してください。

3.9　IPv6 ネットワークの通信障害

3.9.1　通信できない，または切断されている

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

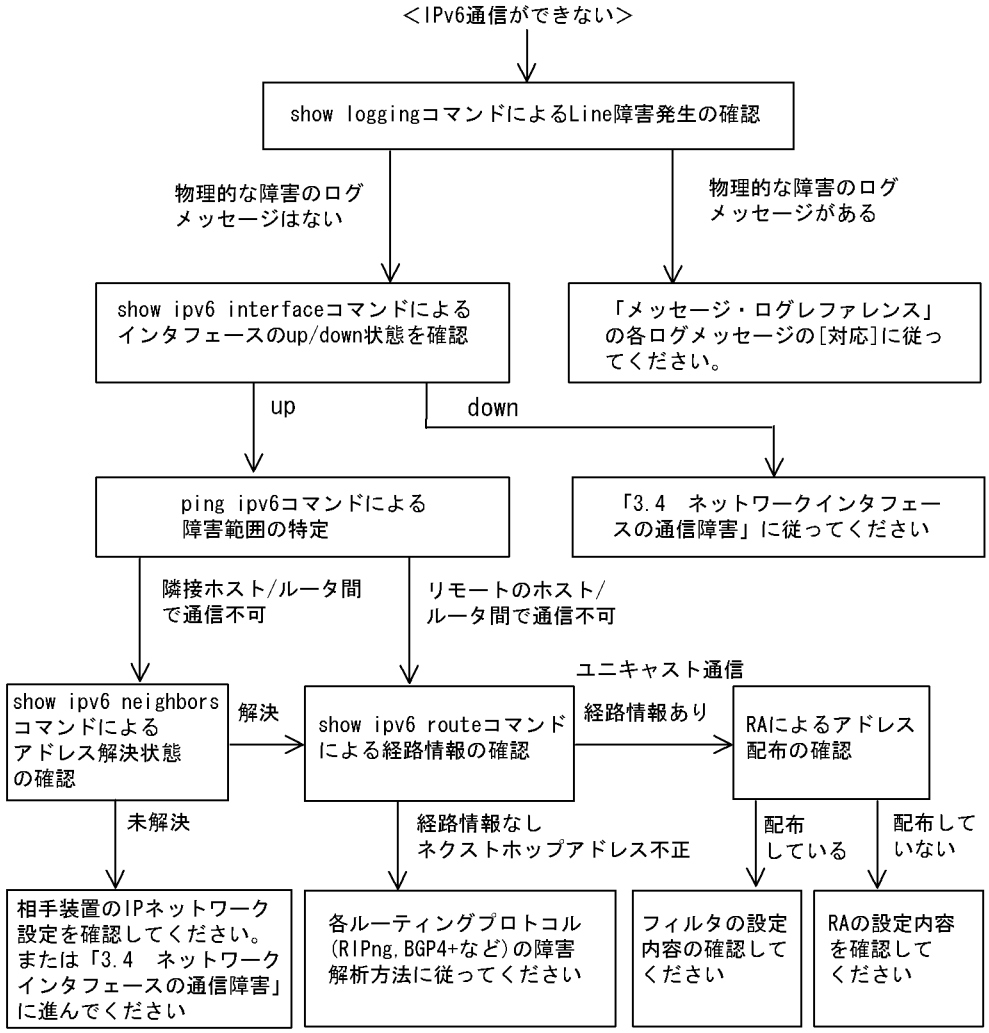
1. IPv6 通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

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 IPv6 通信ができない」，「これまで正常に動いていたのに IPv6 通信ができなくなった」というケースを中心に，障害部位および原因の切り分け手順を説明いたします。

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 3-12　IPv6 通信ができない場合の障害解析手順



(1) ログおよびインタフェースの確認

通信ができなくなる原因として，回線の障害（または壊れ）や，隣接装置の障害が考えられます。本装置が表示するログや show ipv6 interface コマンド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，「3.6.1　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。

(2) 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. ping ipv6 コマンド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。ping ipv6 コマンドの操作例および実行結果の見方については，マニュアル「コンフィグレーションガイド」を参照してください。
3. ping ipv6 コマンドで通信相手との疎通が確認できなかった場合は，さらに ping ipv6 コマンド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. ping ipv6 コマンド実行の結果，障害範囲が隣接装置の場合は「(4) 隣接装置との NDP 解決情報の確認」に，リモート先の装置の場合は「(5) ユニキャストインタフェース情報の確認」に進んでください。

(3) 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 ipv6 機能があることを確認してください。
2. ping ipv6 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 ipv6 機能で通信相手との疎通が確認できなかった場合は，さらに ping ipv6 コマンド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 ipv6 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。

(4) 隣接装置との NDP 解決情報の確認

ping ipv6 コマンドの実行結果によって隣接装置との疎通が不可の場合は，NDP 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. show ipv6 neighbors コマンドを使って隣接装置間とのアドレス解決状態（NDP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（NDP エントリ情報あり）場合は，「(5) ユニキャストインタフェース情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（NDP エントリ情報なし）場合は，隣接装置と本装置の IP ネットワーク設定が一致しているかを確認してください。

(5) ユニキャストインタフェース情報の確認

隣接装置とのアドレスが解決しているにも関わらず通信ができない場合や，IPv6 ユニキャスト通信で通信相手との途中の経路で疎通が不可となる，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. show ipv6 route コマンドを実行して，本装置が取得した経路情報を確認してください。
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ない場合やネクストホップアドレスが不正の場合は「3.10　IPv6 ユニキャストルーティングの通信障害」に進んでください。
4. 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。
   - RA 機能

     「(7) RA 設定情報の確認」に進んでください。

（6） 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 制御の帯域監視，廃棄制御または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，システムの構築での帯域監視ならびに廃棄制御・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，「3.19.1 フィルタ／ QoS 設定情報の確認」を参照してください。

（7） RA 設定情報の確認

本装置と本装置に直接接続されている端末との間で通信ができない場合は，RA によるアドレス情報配布が正常に行われていない可能性が考えられます。したがって，コンフィグレーションの RA 機能の設定が正しいか確認してください。確認手順を次に示します。

1. 本装置にログインします。
2. show ipv6 routers コマンドを実行して，本装置の RA 情報を確認してください。
3. IPv6 アドレス情報が正しく配布されていた場合，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／ QoS 機能
     「（6）フィルタ／ QoS 設定情報の確認」を参照してください。

3.9.2 IPv6 DHCP に関するトラブルシューティング

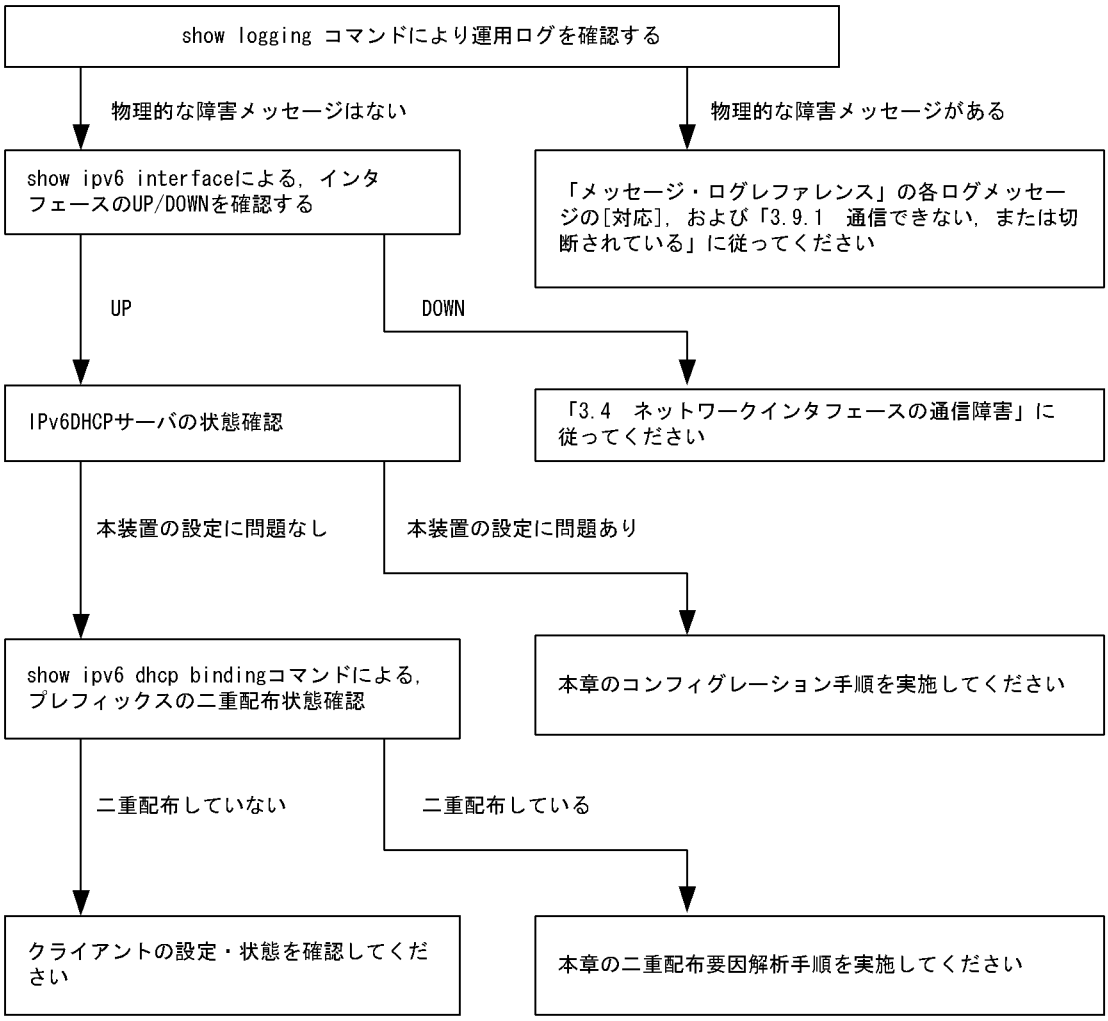
（1） コンフィグレーションが配布されない

本装置 IPv6 DHCP サーバのプレフィックス配布機能を使用するに当たり，サービスが正常に動作しない原因としては，以下の 5 点が考えられます。

1. プレフィックス配布設定数に対して，クライアント数が多い。
2. クライアント DUID（DHCP Unique Identifier）の指定を誤っている。
3. ipv6 dhcp server 設定を誤っている。
4. IPv6 DHCP 運用中の障害
5. その他の障害

上記は，以下の手順で障害個所を切り分け，確認できます。

図 3-13　IPv6 DHCP サーバの障害解析手順



(a) ログおよびインタフェースの確認

通信ができなくなる原因として，NIM，インタフェースの障害（または壊れ）や，隣接装置の障害が考えられます。本装置が表示するログや，show ipv6 interface コマンド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「3.9.1　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。

(b) 本装置の IPv6 DHCP サーバ状態確認

1. IPv6 DHCP サーバサービスの起動確認

   show ipv6 dhcp server statistics コマンドで，IPv6 DHCP サーバデーモンから情報が取得できるか確認してください。show ipv6 dhcp server statistics コマンドの実行結果が以下の場合は，コンフィグレーションコマンド service ipv6 dhcp で IPv6 DHCP サーバ機能を再設定してください。

   [実行結果]

```
> show ipv6 dhcp server statistics
> < show statistics >: dhcp6_server doesn't seem to be running.
```

2. 配布可能なプレフィックスの残数を確認する
   show ipv6 dhcp server statistics コマンドで，IPv6 DHCP サーバがあといくつプレフィックスを配布できるかを確認してください。確認手順については，マニュアル「コンフィグレーションガイド」を参照してください。確認の結果，配布可能なプレフィックス数が 0 である場合は配布するプレフィックス数を増やしてください。なお，配布可能なプレフィックス数の上限は 1024 です。

(c) コンフィグレーション確認手順

1. IPv6 DHCP サーバ機能の有効設定の確認
   コンフィグレーションコマンド show service で，IPv6 DHCP サーバ設定が有効になっているかを確認してください。実行結果で示す下線部が表示されなければ IPv6 DHCP サーバ機能は有効です。

   [実行結果]

```
(config)# show service
no service ipv6 dhcp
!
(config)#
```

2. ipv6 dhcp server の設定を確認する
   コンフィグレーションコマンド show で，ipv6 dhcp server 設定の有無を確認してください。設定がない場合は追加してください。設定がある場合は，設定しているインタフェースが，クライアント接続ネットワーク向けの設定であることを確認してください。

   [実行結果]

```
(config)# show
interface vlan 10
  ipv6 address 3ffe:1:2:: linklocal
  ipv6 enable
  ipv6 dhcp server Tokyo preference 100
!
(config)#
```

3. ipv6 dhcp pool ／ ipv6 local pool ／ prefix-delegation ／ prefix-delegation pool の設定を確認する
   コンフィグレーションコマンド show ipv6 dhcp で，IPv6 DHCP サーバで配布しようとしているプレフィックス配布設定の有無を確認してください。設定がない場合は追加してください。設定がある場合は，配布するプレフィックスを指定する prefix-delegation ／ ipv6 local pool の設定値，配布クライアントを決める duid の設定有無，ならびに duid に指定したクライアント DUID の値が正しいかを確認してください。

   [実行結果]

```
(config)# show ipv6 dhcp
ipv6 dhcp pool Tokyo
  prefix-delegation 3ffe:1:2::/48 00:03:00:01:11:22:33:44:55
!
(config)#
```

(d) クライアントによる二重取得

1. binding 情報の確認
   show ipv6 dhcp binding コマンドを detail パラメータ指定で実行し，同一 DUID に対してプレフィックスが二重に配布されていないかを確認します。以下に表示例を示します。

   [実行結果]

```
> show ipv6 dhcp binding detail
Total: 2 prefixes
<Prefix>             <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48      10/12/01 15:30:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48      10/12/01 15:30:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
>
```

下線で示すように，同一 DUID が 2 個以上存在する場合は，プレフィックス情報を不当に取得しているクライアントである可能性があります。各クライアントを確認し，配布を受けたプレフィックス値を確認してください。

2. 配布済みプレフィックスとクライアントの対応をとる
   show ipv6 dhcp binding detail の結果で，プレフィックスを二重取得しているクライアントが見つからない場合は，表示される DUID とクライアント装置の対応を取る手順が必要となります。対応付けは，binding 情報に示される「配布済みプレフィックスの値」と「クライアント装置が配布を受けたプレフィックスの情報」を比較することで確認してください。

(e) クライアントの設定状態を確認する

クライアントの設定状態を確認する場合は，クライアント付属のマニュアルに従ってください。

(f) 二重配布からの回復手順

本装置 IPv6 DHCP サーバで，同一クライアントへプレフィックスを二重配布したことを確認した場合は，表示される DUID とクライアントの対応から，現在未使用のプレフィックスを調査してください。現在未使用のプレフィックスについては，clear ipv6 dhcp binding < 未使用プレフィックス > コマンドによって，binding 情報を削除してください。

[実行結果]

```
> show ipv6 dhcp binding detail
Total: 2 prefixes
<Prefix>              <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48       10/12/01 15:30:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48       10/12/01 15:30:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
> clear ipv6 dhcp binding 3ffe:1234:5678::/48
> show ipv6 dhcp binding detail
<Prefix>              <Lease expiration>  <Type>
  <DUID>
3ffe:aaaa:1234::/48       10/12/01 15:30:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
>
```

(2) プレフィックス配布先への通信ができない

本装置 DHCP サーバのプレフィックス配布先への自動経路情報設定機能を利用する場合，経路情報が設定されない要因は以下の二つがあります。

1. コンフィグレーション設定済みだが，未配布である。
2. 自動経路情報設定に関連する機能に影響がある操作，またはイベントが発生した。

上記は経路情報を確認する show ipv6 route -s コマンドの結果と show ipv6 dhcp server binding コマンドでの配布済みプレフィックス情報を比較することで切り分けることができます。

表 3-27 プレフィックス配布先への経路情報関連障害切り分け

条件		発生要因
binding 情報	経路情報	
あり	経路あり	該当なし。active 状態。
あり	経路なし	要因 2
なし	経路あり	要因 2
なし	経路なし	要因 1，2

プレフィックス配布先への経路情報の保有性については，次の表に示す制限があります。

表 3-28 プレフィックス配布先への経路情報の保有性

プレフィックスに関する保有情報	発生イベントと保有性			
	サーバ機能再起動		ルーティングマネージャ再起動	本装置再起動
	コマンド実行	サーバ障害		
クライアントへの経路情報	○	△	○	×

（凡例）
○：保証される
△：保証されない（各状態の情報が保有される場合もある）
×：保証されない（初期化されるため，再設定要）

注
プレフィックス配布先への経路情報設定を行う際に必要な経路管理機能
なお，その他の障害については，「3.9.1 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。

(a) 経路情報の確認

本装置 IPv6 DHCP サーバのプレフィックス配布先への自動経路設定機能を利用する場合，プレフィックス配布後の経路情報は，show ipv6 route コマンドで -s パラメータを指定して確認できます。

図 3-14 運用コマンドによる経路情報の確認

```
> show ipv6 route -s
Total: 10routes
Destination              Next Hop      Interface        Metric  Protocol  Age
3ffe:1234:5678::/48      ::1           tokyo            0/0      Static   45m
        <Active Gateway Dhcp>
3ffe:aaaa:1234::/48      ::1           osaka            0/0      Static   23m
        <Active Gateway Dhcp>
:
>
```

(b) 経路情報の再設定を行う

本装置 IPv6 DHCP サーバのプレフィックス配布先への自動経路設定機能を利用する場合，障害などで経路情報がクリアされるイベントが発生したとき，その復旧にはプレフィックスの再配布が必要です。クライアント装置で，プレフィックス情報を再取得する操作を行ってください。

(3) 本装置 DUID が他装置と重複した場合

本装置を含む IPv6 DHCP サーバを同一ネットワーク上で 2 台以上運用する構成で，DUID が重複する場合は，以下の手順で本装置の DUID を再設定してください。

(a) DUID 情報保存ファイルを削除する

本装置 DUID は /usr/var/dhcp6/dhcp6s_duid に保存されています。運用コマンドラインより，rm コマンドを使用し，明示的に削除してください。

(b) DUID を再生成させる

DUID ファイルを削除後は，restart ipv6-dhcp server コマンドによって再起動させるか，コンフィグレーションへ IPv6 DHCP サーバ設定を追加してください。本装置 IPv6 DHCP サーバは起動時に IPv6 DHCP サーバインタフェースとして使用する ipv6 インタフェースの MAC アドレスを取得し，これと時刻情報を基に新たに生成します。

(c) DUID の確認

show ipv6 dhcp server statistics コマンドの「< Server DUID >」の項目によって確認できます。詳細は，マニュアル「コンフィグレーションガイド」を参照してください。

3.10 IPv6 ユニキャストルーティングの通信障害

3.10.1 RIPng 経路情報が存在しない

本装置が取得した経路情報の表示に，RIPng の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-29 RIPng の障害解析方法

項番	確認内容・コマンド	対応
1	RIPng の隣接情報を表示します。 show ipv6 rip neighbor	隣接ルータのインタフェースが表示されていない場合は項番 2 へ。
		隣接ルータのインタフェースが表示されている場合は項番 3 へ。
2	コンフィグレーションで RIPng 設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが RIPng 経路を広告しているか確認してください。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。

3.10.2 OSPFv3 経路情報が存在しない

本装置が取得した経路情報の表示に，OSPFv3 の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-30 OSPFv3 の障害解析方法

項番	確認内容・コマンド	対応
1	OSPFv3 のインタフェース状態を確認します。 show ipv6 ospf interface <Interface Name>	インタフェース状態が DR の場合は項番 3 へ。
		インタフェース状態が BackupDR または DR Other の場合は項番 2 へ。
		インタフェースの状態が Waiting の場合は，時間を置いてコマンドを再実行してください。項番 1 へ。
2	Neighbor List 内より DR との隣接ルータ状態を確認します。	DR との隣接ルータ状態が Full 以外の場合は項番 4 へ。
		DR との隣接ルータ状態が Full の場合は項番 5 へ。
3	Neighbor List 内より全隣接ルータとの状態を確認します。	一部の隣接ルータ状態が Full 以外の場合は項番 4 へ。
		全隣接ルータ状態が Full の場合は項番 5 へ。
4	コンフィグレーションで OSPFv3 の設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 5 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。

項番	確認内容・コマンド	対応
5	OSPFv3 経路を学習している経路を確認してください。 show ipv6 route all-routes	経路が InActive の場合には項番 6 へ。
		経路が存在しない場合は隣接ルータが OSPFv3 経路を広告しているか確認してください。
6	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが OSPFv3 経路を広告しているか確認してください。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。

3.10.3 BGP4+ 経路情報が存在しない

本装置が取得した経路情報の表示に，BGP4+ の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-31 BGP4+ の障害解析方法

項番	確認内容・コマンド	対応
1	BGP4+ のピア状態を確認します。 show ipv6 bgp neighbors	ピア状態が Established 以外の場合は項番 2 へ。
		ピア状態が Established の場合は項番 3 へ。
2	コンフィグレーションで BGP4+ の設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	BGP4+ 経路を学習しているか確認してください。 show ipv6 bgp received-routes	経路が存在するが active 状態でない場合は項番 4 へ。
		経路が存在しない場合は項番 5 へ。
4	BGP4+ 経路のネクストホップアドレスを解決する経路情報が存在するか確認してください。 show ipv6 route	ネクストホップアドレスを解決する経路情報がある場合は項番 5 へ。
		ネクストホップアドレスを解決する経路情報がない場合は，その経路情報を学習するためのプロトコルの障害解析を実施してください。
5	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが BGP4+ 経路を広告しているか確認してください。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。

3.11　IPv6 マルチキャストルーティングの通信障害

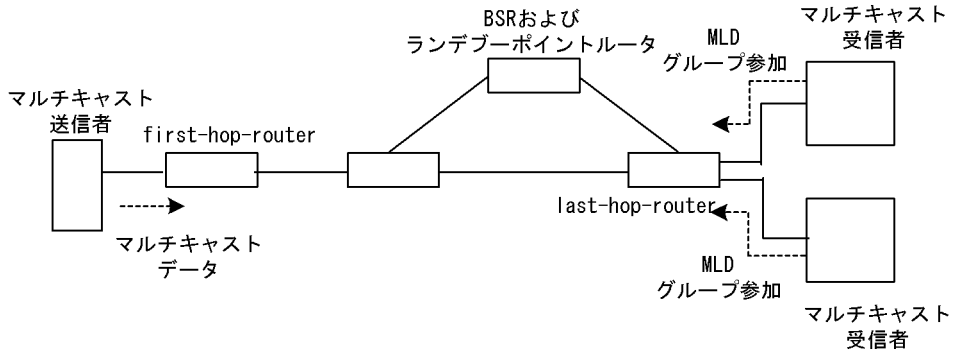
本装置で IPv6 マルチキャスト通信障害が発生した場合の対処について説明します。

3.11.1　IPv6 PIM-SM ネットワークで通信ができない

IPv6 PIM-SM ネットワーク構成でマルチキャスト中継ができない場合は，以下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。

IPv6 PIM-SM のネットワーク例を次の図に示します。

図 3-15　IPv6 PIM-SM ネットワーク例



注

- BSR：ランデブーポイントの情報を配信するルータ（詳細は，マニュアル「コンフィグレーションガイド」を参照してください）
- ランデブーポイントルータ：中継先が確定していないパケットをマルチキャスト受信者方向に中継するルータ（詳細は，マニュアル「コンフィグレーションガイド」を参照してください）
- first-hop-router：マルチキャスト送信者と直接接続するルータ
- last-hop-router：マルチキャスト受信者と直接接続するルータ

（1）共通確認内容

次の表に，IPv6 PIM-SM ネットワーク構成のすべての本装置に対する共通確認内容を示します。

表 3-32　共通確認内容

項番	確認内容・コマンド	対応
1	コンフィグレーションにマルチキャスト機能を使用する指定（ipv6 multicast routing）があることを確認してください。 show running-config	マルチキャスト機能を使用する指定がない場合は，コンフィグレーションを修正してください。
2	コンフィグレーションに loopback インタフェースのアドレス設定があることを確認してください。 show running-config	loopback インタフェースのアドレス設定がない場合はコンフィグレーションを修正してください。
3	一つ以上のインタフェースで PIM が動作していることを確認してください。 show ipv6 pim interface	動作していない場合はコンフィグレーションを確認し，どれか一つ以上のインタフェースで PIM が動作するように設定してください。

項番	確認内容・コマンド	対応
4	PIM が動作するインタフェースに，MLD snooping が設定されているか確認してください。 show mld-snooping	MLD snooping が設定されている場合は，以下の内容を確認してください。 • 隣接ルータと接続しているポートに対して MLD snooping のマルチキャストルータポートの設定がされているか確認してください。 •「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。
5	PIM および MLD が動作するインタフェースで，フィルタなどによるプロトコルパケットおよびマルチキャストパケット中継を抑止する設定がないことを，コンフィグレーションで確認してください。 show running-config	プロトコルパケットおよびマルチキャストパケット中継を抑止する設定がある場合は，コンフィグレーションを修正してください。
6	PIM の隣接情報を確認してください。 show ipv6 pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ipv6 pim コマンドで interface パラメータを指定して確認してください。 • 隣接ルータの設定を確認してください。
7	マルチキャストデータ送信者へのユニキャスト経路が存在するか確認してください。 show ipv6 route	ユニキャスト経路が存在しない場合は「3.10　IPv6 ユニキャストルーティングの通信障害」を参照してください。
8	マルチキャストデータ送信者への次ホップアドレスと接続しているインタフェースで，PIM が動作していることを確認してください。 show ipv6 pim interface	動作していない場合はコンフィグレーションを確認し，マルチキャストデータ送信者への次ホップアドレスと接続しているインタフェースで PIM が動作するように設定してください。
9	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていないことをコンフィグレーションで確認してください。 show running-config	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれている場合は，コンフィグレーションを修正してください。
10	BSR が決定されていることを確認してください。ただし，中継対象グループアドレスに対するランデブーポイントが静的ランデブーポイントの場合は，確認不要です。 show ipv6 pim bsr	BSR が決定されていない場合は BSR へのユニキャスト経路が存在するか確認してください。ユニキャスト経路が存在しない場合は，「3.10　IPv6 ユニキャストルーティングの通信障害」を参照してください。 ユニキャスト経路が存在する場合は，BSR の設定を確認してください。BSR が本装置の場合は，「(2) BSR 確認内容」を参照してください。
11	ランデブーポイントが決定されていることを確認してください。 show ipv6 pim rp-mapping	ランデブーポイントが決定されていない場合は，ランデブーポイントへのユニキャスト経路が存在するか確認してください。ユニキャスト経路が存在しない場合は，「3.10　IPv6 ユニキャストルーティングの通信障害」を参照してください。 ユニキャスト経路が存在する場合は，ランデブーポイントの設定を確認してください。ランデブーポイントが本装置の場合は，「(3) ランデブーポイントルータ確認内容」を参照してください。
12	ランデブーポイントのグループアドレスに中継対象グループアドレスが含まれていることを確認してください。 show ipv6 pim rp-mapping	中継対象グループアドレスが含まれていない場合は，ランデブーポイントルータの設定を確認してください。
13	マルチキャスト中継エントリが存在することを確認してください。 show ipv6 mcache	マルチキャスト中継エントリが存在しない場合は，上流ポートにマルチキャストデータが届いていることを確認してください。マルチキャストデータが届いていない場合は，マルチキャスト送信者あるいは上流ルータの設定を確認してください。

項番	確認内容・コマンド	対応
14	マルチキャスト経路情報が存在することを確認してください。 show ipv6 mroute	マルチキャスト経路情報が存在しない場合は，下流ルータの設定を確認してください。
15	マルチキャスト経路情報かマルチキャスト中継エントリが上限を超えていないか確認してください。 マルチキャスト経路情報： 　show ipv6 mroute マルチキャスト中継エントリ： 　show ipv6 mcache 　netstat multicast	Warning が出力されている場合は，想定していないマルチキャスト経路情報またはマルチキャスト中継エントリが作成されていないか確認してください。マルチキャスト中継エントリでネガティブキャッシュが多い場合は，不要なパケットを送信している端末が存在しないか確認してください。

（2） BSR 確認内容

次の表に，IPv6 PIM-SM ネットワーク構成で本装置が BSR の場合の確認内容を示します。

表 3-33　BSR 確認内容

項番	確認内容・コマンド	対応
1	本装置が BSR 候補であることを確認してください。 show ipv6 pim bsr	本装置が BSR 候補でない場合はコンフィグレーションを確認し，BSR 候補として動作するように設定してください。また，loopback インタフェースにアドレスが設定されていないと BSR 候補として動作しないため，loopback インタフェースにアドレスが設定されていることも確認してください。
2	本装置が BSR であることを確認してください。 show ipv6 pim bsr	本装置が BSR でない場合は，ほかの BSR 候補の優先度を確認してください。優先度は値の大きい方が高くなります。優先度が同じ場合は，BSR アドレスが一番大きい BSR 候補が BSR となります。

（3） ランデブーポイントルータ確認内容

次の表に，IPv6 PIM-SM ネットワーク構成で本装置がランデブーポイントルータの場合の確認内容を示します。

表 3-34　ランデブーポイントルータ確認内容

項番	確認内容・コマンド	対応
1	本装置が中継対象グループアドレスに対するランデブーポイント候補であることを確認してください。 show ipv6 pim rp-mapping	本装置が中継対象グループアドレスに対するランデブーポイント候補でない場合は，コンフィグレーションを確認し，中継対象グループアドレスに対するランデブーポイント候補として動作するように設定してください。また，loopback インタフェースにアドレスが設定されていないとランデブーポイント候補として動作しないため，loopback インタフェースにアドレスが設定されていることも確認してください。
2	本装置が中継対象グループアドレスに対するランデブーポイントであることを確認してください。 show ipv6 pim rp-hash <Group Address>	本装置がランデブーポイントでない場合は，ほかのランデブーポイント候補の優先度を確認してください。優先度は値の小さい方が高くなります。ほかのランデブーポイント候補の優先度が高い場合はランデブーポイントとして動作せず，優先度が同一の場合はプロトコルの仕様でグループアドレス単位に分散され，該当グループに対してランデブーポイントとして動作しないことがあります。本装置を優先的にランデブーポイントとして動作させる場合は，ほかのランデブーポイント候補より高い優先度を設定してください。

（4） last-hop-router 確認内容

次の表に，IPv6 PIM-SM ネットワーク構成で本装置が last-hop-router の場合の確認内容を示します。

表 3-35 last-hop-router 確認内容

項番	確認内容・コマンド	対応
1	マルチキャスト受信者と接続しているインタフェースで，MLD が動作していることを確認してください。 show ipv6 mld interface	動作していない場合はコンフィグレーションを確認し，MLD が動作するように設定してください。
2	マルチキャスト受信者が MLD で中継対象グループに参加していることを確認してください。 show ipv6 mld group	中継対象グループに参加していない場合は，マルチキャスト受信者の設定を確認してください。
3	中継対象グループが参加し，PIM が動作しているインタフェースがある場合は，本装置が DR であることを確認してください。 show ipv6 pim interface	本装置が DR でない場合は，中継対象インタフェースの DR を調査してください。
4	静的グループ参加機能が動作するインタフェースに，MLD snooping が設定されているか確認してください。 show mld-snooping	MLD snooping が設定されている場合は，以下の内容を確認してください。 • 中継先ポートに対して MLD snooping のマルチキャストルータポートの設定がされているか確認してください。 •「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。
5	各インタフェースで異常を検出していないか確認してください。 show ipv6 mld interface	Notice を確認し，警告情報が出力されていないことを確認してください。 警告情報が出力されている場合は以下を確認してください。 • L：想定した最大数を超えて参加要求が発生しています。接続ユーザ数を確認してください。 • Q：隣接するルータと MLD のバージョンが不一致となっています。MLD のバージョンを合わせてください。 • R：現在の設定では受信できない Report を送信しているユーザが存在します。本装置の MLD のバージョンを変更するか，参加ユーザの設定を確認してください。 • S：MLDv2 で 1 メッセージ内に格納できるソース数が上限を超えたため参加情報を一部廃棄しています。参加ユーザの設定を確認してください。

（5） first-hop-router 確認内容

次の表に，IPv6 PIM-SM ネットワーク構成で本装置が first-hop-router の場合の確認内容を示します。

表 3-36 first-hop-router 確認内容

項番	確認内容・コマンド	対応
1	本装置がマルチキャスト送信者と直接接続していることを確認してください。	直接接続していない場合はネットワーク構成を確認してください。

項番	確認内容・コマンド	対応
2	マルチキャスト送信者と接続しているインタフェースで，PIM または MLD が動作していることを確認してください。 show ipv6 pim interface show ipv6 mld interface	動作していない場合はコンフィグレーションを確認し，PIM または MLD が動作するように設定してください。
3	マルチキャスト経路情報が存在するか確認してください。 show ipv6 mroute	マルチキャスト経路情報が存在しない場合は，マルチキャストデータ送信元アドレスが，マルチキャスト送信者と直接接続しているインタフェースのネットワークアドレスであることを確認してください。

3.11.2 IPv6 PIM-SM ネットワークでマルチキャストデータが二重中継される

IPv6 PIM-SM ネットワーク構成でマルチキャストデータが二重中継される場合は，各ルータの設定内容を確認し，同一ネットワークに複数のルータが存在するインタフェースでは PIM が動作するように設定してください。

上記の設定をしても二重中継が継続する場合の確認内容を次の表に示します。

表 3-37 二重中継が継続する場合の確認内容

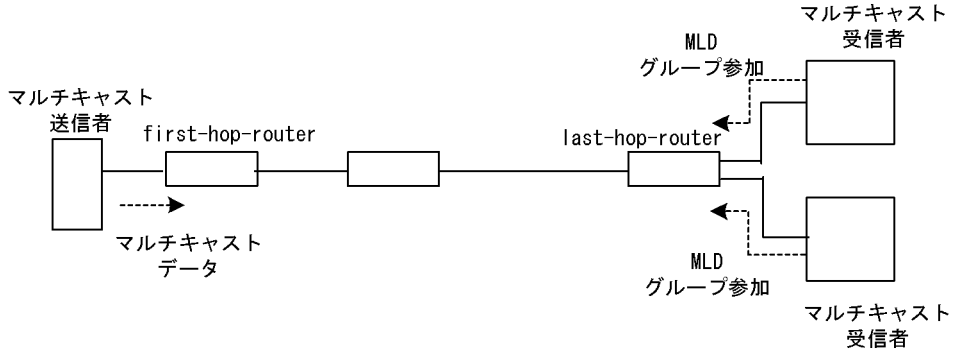
項番	確認内容・コマンド	対応
1	同一ネットワークに複数のルータが存在するインタフェースの，PIM の隣接情報を確認してください。 show ipv6 pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ipv6 pim コマンドで interface パラメータを指定して確認してください。 • フィルタなどによるプロトコルパケットの中継を抑止する設定がないことを，コンフィグレーションで確認してください。 • 隣接ルータの設定を確認してください。

3.11.3 IPv6 PIM-SSM ネットワークで通信ができない

IPv6 PIM-SSM ネットワーク構成でマルチキャスト中継ができない場合は，以下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。

IPv6 PIM-SSM のネットワーク例を次の図に示します。

図 3-16 IPv6 PIM-SSM ネットワーク例



注

- first-hop-router：マルチキャスト送信者と直接接続するルータ
- last-hop-router：マルチキャスト受信者と直接接続するルータ

（1） 共通確認内容

次の表に，IPv6 PIM-SSM ネットワーク構成のすべての本装置に対する共通確認内容を示します。

表 3-38　共通確認内容

項番	確認内容・コマンド	対応
1	コンフィグレーションにマルチキャスト機能を使用する指定（ipv6 multicast routing）があることを確認してください。 show running-config	マルチキャスト機能を使用する指定がない場合は，コンフィグレーションを修正してください。
2	コンフィグレーションに loopback インタフェースのアドレス設定があることを確認してください。 show running-config	loopback インタフェースのアドレス設定がない場合はコンフィグレーションを修正してください。
3	一つ以上のインタフェースで PIM が動作していることを確認してください。 show ipv6 pim interface	動作していない場合はコンフィグレーションを確認し，どれか一つ以上のインタフェースで PIM が動作するように設定してください。
4	PIM が動作するインタフェースに，MLD snooping が設定されているか確認してください。 show mld-snooping	MLD snooping が設定されている場合は，以下の内容を確認してください。 • 隣接ルータと接続しているポートに対して MLD snooping のマルチキャストルータポートの設定がされているか確認してください。 •「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。
5	PIM および MLD が動作するインタフェースで，フィルタなどによるプロトコルパケットおよびマルチキャストパケット中継を抑止する設定がないことを，コンフィグレーションで確認してください。 show running-config	プロトコルパケットおよびマルチキャストパケット中継を抑止する設定がある場合は，コンフィグレーションを修正してください。
6	PIM の隣接情報を確認してください。 show ipv6 pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ipv6 pim コマンドで interface パラメータを指定して確認してください。 • 隣接ルータの設定を確認してください。
7	マルチキャストデータ送信者へのユニキャスト経路が存在するか確認してください。 show ipv6 route	ユニキャスト経路が存在しない場合は「3.10　IPv6 ユニキャストルーティングの通信障害」を参照してください。
8	マルチキャストデータ送信者へのユニキャスト経路送出インタフェースで，PIM が動作していることを確認してください。 show ipv6 pim interface	動作していない場合はコンフィグレーションを確認し，ユニキャスト経路送出インタフェースで PIM が動作するように設定してください。
9	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていることを，コンフィグレーションで確認してください。 show running-config	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていない場合は，コンフィグレーションを修正してください。

項番	確認内容・コマンド	対応
10	マルチキャスト経路情報が存在するか確認してください。 show ipv6 mroute	マルチキャスト経路情報が存在しない場合は，下流ルータの設定を確認してください。
11	マルチキャスト経路情報かマルチキャスト中継エントリが上限を超えていないか確認してください。 マルチキャスト経路情報： show ipv6 mroute マルチキャスト中継エントリ： show ipv6 mcache netstat multicast	Warning が出力されている場合は，想定していないマルチキャスト経路情報またはマルチキャスト中継エントリが作成されていないか確認してください。マルチキャスト中継エントリでネガティブキャッシュが多い場合は，不要なパケットを送信している端末が存在しないか確認してください。

（2） last-hop-router 確認内容

次の表に，IPv6 PIM-SSM ネットワーク構成で本装置が last-hop-router の場合の確認内容を示します。

表 3-39　last-hop-router 確認内容

項番	確認内容・コマンド	対応
1	マルチキャスト受信者のモードが MLDv1/MLDv2（EXCLUDE モード）の場合は，コンフィグレーションに MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM が使用できる指定（ipv6 mld ssm-map enable）があることを確認してください。 show running-config	MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM が使用できる指定がない場合は，コンフィグレーションを修正してください。
2	マルチキャスト受信者のモードが MLDv1/MLDv2（EXCLUDE モード）の場合は，コンフィグレーションに PIM-SSM で中継するグループアドレスと送信元アドレスが，MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM と連携動作する設定（ipv6 mld ssm-map static）があることを確認してください。 show running-config	MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM と連携動作する設定がない場合は，コンフィグレーションを修正してください。
3	マルチキャスト受信者と接続しているインタフェースで，MLD が動作していることを確認してください。 show ipv6 mld interface	動作していない場合はコンフィグレーションを確認し，MLD が動作するように設定してください。
4	マルチキャスト受信者と接続しているインタフェースで，MLD 警告情報が表示されていないことを確認してください。 show ipv6 mld interface	表示されている場合は，それぞれの警告にあった対応をしてください。警告の内容については，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。
5	マルチキャスト受信者が MLD で中継対象グループに参加していることを確認してください。 show ipv6 mld group	中継対象グループにグループ参加していない場合は，マルチキャスト受信者の設定を確認してください。
6	MLD グループ情報に送信元アドレスが登録されていることを確認してください。 show ipv6 mld group	マルチキャスト受信者のモードが MLDv2（INCLUDE モード）で送信元アドレスが登録されていない場合は，マルチキャスト受信者を調査してください。マルチキャスト受信者のモードが MLDv1/MLDv2（EXCLUDE モード）の場合は，PIM-SSM と連携動作する設定があることをコンフィグレーションで確認してください。
7	中継対象グループが参加し，PIM が動作しているインタフェースがある場合は，本装置が DR であることを確認してください。 show ipv6 pim interface	本装置が DR でない場合は，中継対象インタフェースの DR を調査してください。

項番	確認内容・コマンド	対応
8	静的グループ参加機能が動作するインタフェースに，MLD snooping が設定されているか確認してください。 show mld-snooping	MLD snooping が設定されている場合は，以下の内容を確認してください。 • 中継先ポートに対して MLD snooping のマルチキャストルータポートの設定がされているか確認してください。 •「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。
9	各インタフェースで異常を検出していないか確認してください。 show ipv6 mld interface	Notice を確認し，警告情報が出力されていないことを確認してください。 警告情報が出力されている場合は以下を確認してください。 • L：想定した最大数を超えて参加要求が発生しています。接続ユーザ数を確認してください。 • Q：隣接するルータと MLD のバージョンが不一致となっています。MLD のバージョンを合わせてください。 • R：現在の設定では受信できない Report を送信しているユーザが存在します。本装置の MLD のバージョンを変更するか，参加ユーザの設定を確認してください。 • S：MLDv2 で 1 メッセージ内に格納できるソース数が上限を超えたため参加情報を一部廃棄しています。参加ユーザの設定を確認してください。

（3） first-hop-router 確認内容

次の表に，IPv6 PIM-SSM ネットワーク構成で本装置が first-hop-router の場合の確認内容を示します。

表 3-40　first-hop-router 確認内容

項番	確認内容・コマンド	対応
1	本装置がマルチキャスト送信者と直接接続していることを確認してください。	直接接続していない場合は，ネットワーク構成を確認してください。
2	マルチキャスト送信者と接続しているインタフェースで，PIM または MLD が動作していることを確認してください。 show ipv6 pim interface show ipv6 mld interface	動作していない場合はコンフィグレーションを確認し，PIM または MLD が動作するように設定してください。
3	マルチキャストデータが本装置に届いているか確認してください。	マルチキャストデータが届いていない場合は，マルチキャスト送信者の設定を確認してください。
4	マルチキャストデータとマルチキャスト経路情報のグループアドレスと送信元アドレスが一致するか確認してください。 show ipv6 mroute show netstat multicast	グループアドレスと送信元アドレスが一致しない場合は，マルチキャスト送信者と last-hop-router の設定内容を確認してください。

3.11.4　IPv6 PIM-SSM ネットワークでマルチキャストデータが二重中継される

IPv6 PIM-SSM ネットワーク構成でマルチキャストデータが二重中継される場合は，各ルータの設定内容を確認し，同一ネットワークに複数のルータが存在するインタフェースでは PIM が動作するように設定してください。

上記の設定をしても二重中継が継続する場合の確認内容を次の表に示します。

表 3-41 二重中継が継続する場合の確認内容

項番	確認内容・コマンド	対応
1	同一ネットワークに複数のルータが存在するインタフェースの，PIM の隣接情報を確認してください。 show ipv6 pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ipv6 pim コマンドで interface パラメータを指定して確認してください。 • フィルタなどによるプロトコルパケットの中継を抑止する設定がないことを，コンフィグレーションで確認してください。 • 隣接ルータの設定を確認してください。

3.12　高信頼性機能の通信障害

3.12.1　IPv4 ネットワークの VRRP 構成で通信ができない

VRRP 構成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。

表 3-42　VRRP の障害解析方法

項番	確認内容・コマンド	対応
1	同一仮想ルータを構成する相手装置と本装置で仮想ルータの状態を確認し，マスタとなっている装置が 1 台であり，ほかの装置はバックアップになっていることを確認してください。	同一仮想ルータを構成する装置間で，マスタとなっている装置が 1 台だけであり，そのほかはバックアップとなっている場合には，次の点を確認してください。 • 仮想ルータの配下に，ほかのルータを介さずに端末が接続されている場合，各端末のネットワーク設定でデフォルトゲートウェイとして仮想ルータの仮想 IP アドレスが設定されていることを確認してください。 • 本装置を含めた通信経路上の装置での経路情報を確認してください。 端末の設定に問題がなく，通信経路上の装置での経路情報も問題ない場合は，項番 2 へ。
		仮想ルータの状態が正しくない場合は項番 3 へ。
2	show vlan コマンドで detail パラメータを指定し，仮想ルータが設定されている VLAN 内の物理ポートの状態が Forwarding であることを確認してください。	• 物理ポートの状態が Blocking の場合，STP のトポロジチェンジなどによって，一時的に通信が遮断されている可能性があります。しばらく待ってから，再度物理ポートの状態が Forwarding であることを確認してください。しばらく待っても物理ポートの状態が Forwarding にならない場合は，コンフィグレーションおよび物理的なネットワーク構成を確認してください。 • 物理ポートの状態が down の場合，物理的に接続されていません。コネクタの接続やケーブルに問題がないか，確認してください。
		物理ポートの状態が Forwarding の場合は，ルーティング先ネットワークの負荷が高くないか，確認してください。
3	同一仮想ルータを構成する相手装置と本装置の仮想ルータの状態が，お互いにマスタとなっていないことを確認してください。	複数の仮想ルータがマスタとなっている場合は項番 6 へ。
		複数の仮想ルータがマスタとなっていない場合は項番 10 へ。
4	ping コマンドで，仮想ルータを構成するルータ間の通信を実 IPv4 アドレスで確認してください。	仮想ルータを構成するルータ間の実 IPv4 アドレスによる通信ができない場合，物理的なネットワーク構成を確認してください。
		ping コマンドで，仮想ルータを構成するルータ間の実 IPv4 アドレスによる通信を確認できた場合は項番 7 へ。

項番	確認内容・コマンド	対応
5	show logging コマンド，および show vrrpstatus コマンドでの statistics パラメータ指定で，ADVERTISEMENT パケットの受信状況を確認してください。	• 「Virtual router <VRID> of <Interface Name> received VRRP packet for which the advertisement interval is different than the one configured for local virtual router.」が種別ログに登録されており，統計情報の "<Number of packets> with bad advertisement interval" が増加する場合は，本装置と相手装置で ADVERTISEMENT パケット送信間隔の設定値が一致していることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check.」が種別ログに登録されており，統計情報の " <Number of packets> with authentication failed" が増加する場合は，本装置と相手装置で認証パスワードの設定内容が一致していることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet with IP TTL not equal to 255.」が種別ログに登録されており，統計情報の " <Number of packets> with bad ip ttl" が増加する場合は，本装置と相手装置間にほかのルータがないことを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet for which the address list does not match the locally configured list for the virtual router.」が種別ログに登録されており，統計情報の " <Number of packets> with bad ip address list" が増加する場合は，仮想 IP アドレスの設定が同一であることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check.」が種別ログに登録されており，統計情報の " <Number of packets> with bad authentication type" が増加する場合は，本装置と相手装置で認証パスワードの設定有無を確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that length less than the length of the VRRP header.」が種別ログに登録されており，統計情報の " <Number of packets> with packet length error" が増加する場合は，本装置と相手装置で VRRP 動作モードの設定が同一であることを確認してください。 • 「VRRP packet received with unsupported version number.」が種別ログに登録されており，統計情報の”<Number of packets> with invalid type”が増加する場合は，本装置と相手装置で VRRP 動作モードの設定が同一であることを確認してください。
		ADVERTISEMENT パケットが正常に受信されている場合は，相手装置を確認してください。 ADVERTISEMENT パケットが受信されていない場合には，項番 8 へ。
6	show interfaces コマンドで，同一仮想ルータを構成する相手装置が接続されている物理ポートの統計情報を確認してください。 また，show cpu コマンドで CPU 使用率を確認してください。	同一仮想ルータを構成する相手装置が接続されている物理ポートの Input rate および Output rate が高く，回線の負荷が高い場合，および show cpu コマンドで確認した CPU 使用率が高い場合は，以下の対策を行ってください。 • 回線がループしている場合，STP などの利用や物理的なネットワーク構成を見直してループを解消してください。 • コンフィグレーションコマンド vrrp timers advertise で ADVERTISEMENT パケットの送出間隔を長めに設定してください。 • コンフィグレーションコマンド vrrp preempt delay で自動切り戻し抑止時間を設定してください。
		物理ポートの負荷が低い場合は項番 9 へ。
7	フィルタの設定で ADVERTISEMENT パケットを廃棄する設定がないことを確認してください。	該当するフィルタの設定がある場合，ADVERTISEMENT パケットを廃棄しないようにフィルタの設定を変更してください。
		フィルタの設定がない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。

項番	確認内容・コマンド	対応
8	障害監視インタフェース設定がある場合，障害監視インタフェースの状態を確認してください。	障害監視インタフェースを設定したインタフェースに別の仮想ルータの設定があり，その仮想ルータの障害監視インタフェースが該当仮想ルータのインタフェースになっていないことを確認してください。なっている場合は，どちらかの障害インタフェースの設定を削除してください。
		上記の障害監視インタフェースの設定がない場合は項番 11 へ。
9	show vrrpstatus コマンドで detail パラメータを指定し，仮想ルータの状態が Initial でないことを確認してください。	仮想ルータの状態が Initial の場合は，次の点を確認してください。 • 現在の優先度が 0 でない場合，Admin State 欄に表示されている非動作要因を排除してください。（非動作要因については，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。） • show logging コマンドでログを確認し，「The VRRP virtual MAC address entry can't be registered at hardware tables.」がある場合，H/W の MAC アドレステーブル設定に失敗しています。いったん該当仮想ルータのコンフィグレーションを削除し，異なる仮想ルータ番号でコンフィグレーションを設定し直すか，仮想ルータを設定する VLAN の VLAN ID を変更することで，仮想ルータが動作する可能性があります。
		仮想ルータの状態が Initial でない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。

3.12.2 IPv6 ネットワークの VRRP 構成で通信ができない

VRRP 構成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。

表 3-43 VRRP の障害解析方法

項番	確認内容・コマンド	対応
1	同一仮想ルータを構成する相手装置と本装置で仮想ルータの状態を確認し，マスタとなっている装置が 1 台であり，ほかの装置はバックアップになっていることを確認してください。	同一仮想ルータを構成する装置間で，マスタとなっている装置が 1 台だけであり，そのほかはバックアップとなっている場合には，次の点を確認してください。 • 仮想ルータの配下に，ほかのルータを介さずに端末が接続されている場合，各端末のネットワーク設定でデフォルトゲートウェイとして仮想ルータの仮想 IP アドレスが設定されていることを確認してください。 • 本装置を含めた通信経路上の装置での経路情報を確認してください。 端末の設定に問題がなく，通信経路上の装置での経路情報も問題ない場合は，項番 2 へ。
		仮想ルータの状態が正しくない場合は項番 3 へ。
2	show vlan コマンドで detail パラメータを指定し，仮想ルータが設定されている VLAN 内の物理ポートの状態が Forwarding であることを確認してください。	• 物理ポートの状態が Blocking の場合，STP のトポロジチェンジなどによって，一時的に通信が遮断されている可能性があります。しばらく待ってから，再度物理ポートの状態が Forwarding であることを確認してください。しばらく待っても物理ポートの状態が Forwarding にならない場合は，コンフィグレーションおよび物理的なネットワーク構成を確認してください。 • 物理ポートの状態が down の場合，物理的に接続されていません。コネクタの接続やケーブルに問題がないか，確認してください。
		物理ポートの状態が Forwarding の場合は，ルーティング先ネットワークの負荷が高くないか，確認してください。
3	同一仮想ルータを構成する相手装置と本装置の仮想ルータの状態が，お互いにマスタとなっていないことを確認してください。	複数の仮想ルータがマスタとなっている場合は項番 4 へ。

項番	確認内容・コマンド	対応
		複数の仮想ルータがマスタとなっていない場合は項番 8 へ。
4	ping ipv6 コマンドで，仮想ルータを構成するルータ間の通信を実 IPv6 アドレスで確認してください。	仮想ルータを構成するルータ間の実 IPv6 アドレスによる通信ができない場合，物理的なネットワーク構成を確認してください。
		ping ipv6 コマンドで，仮想ルータを構成するルータ間の実 IPv6 アドレスによる通信を確認できた場合は項番 5 へ。
5	show vrrpstatus コマンドで statistics パラメータを指定し，ADVERTISEMENT パケットの受信状況を確認してください。	• 「Virtual router <VRID> of <Interface Name> received VRRP packet for which the advertisement interval is different than the one configured for local virtual router.」が種別ログに登録されており，統計情報の "<Number of packets> with bad advertisement interval" が増加する場合は，本装置と相手装置で ADVERTISEMENT パケット送信間隔の設定値が同一であること，および VRRP 動作モードの設定が同一であることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check.」が種別ログに登録されており，統計情報の " <Number of packets> with authentication failed" が増加する場合は，本装置と相手装置で認証パスワードの設定内容が同一であることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet with IP HopLimit not equal to 255.」が種別ログに登録されており，統計情報の " <Number of packets> with bad ipv6 hoplimit" が増加する場合は，本装置と相手装置間にほかのルータがないことを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet for which the address list does not match the locally configured list for the virtual router.」が種別ログに登録されており，統計情報の " <Number of packets> with bad ipv6 address" が増加する場合は，仮想 IP アドレス，および VRRP 動作モードの設定が同一であることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check.」が種別ログに登録されており，統計情報の " <Number of packets> with bad authentication type" が増加する場合は，本装置と相手装置で認証パスワードの設定有無を確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that length less than the length of the VRRP header.」が種別ログに登録されており，統計情報の " <Number of packets> with packet length error" が増加する場合は，本装置と相手装置で VRRP 動作モードの設定が同一であることを確認してください。 • 「VRRP packet received with unsupported version number.」が種別ログに登録されており，統計情報の " <Number of packets> with invalid type" が増加する場合は，本装置と相手装置で VRRP 動作モードの設定が同一であることを確認してください。
		ADVERTISEMENT パケットが正常に受信されている場合は，相手装置を確認してください。 ADVERTISEMENT パケットが受信されていない場合には項番 6 へ。
6	show interfaces コマンドで，同一仮想ルータを構成する相手装置が接続されている物理ポートの統計情報を確認してください。 また，show cpu コマンドで CPU 使用率を確認してください。	同一仮想ルータを構成する相手装置が接続されている物理ポートの Input rate および Output rate が高く，回線の負荷が高い場合，および show cpu コマンドで確認した CPU 使用率が高い場合は，以下の対策を行ってください。 • 回線がループしている場合，STP などの利用や物理的なネットワーク構成を見直してループを解消してください。 • コンフィグレーションコマンド vrrp timers advertise で ADVERTISEMENT パケットの送出間隔を長めに設定してください。 • コンフィグレーションコマンド vrrp preempt delay で自動切り戻し抑止時間を設定してください。

項番	確認内容・コマンド	対応
		物理ポートの負荷が低い場合は項番 7 へ。
7	フィルタの設定で ADVERTISEMENT パケットを廃棄する設定がないことを確認してください。	該当するフィルタの設定がある場合，ADVERTISEMENT パケットを廃棄しないようにフィルタの設定を変更してください。
		フィルタの設定がない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。
8	障害監視インタフェース設定がある場合，障害監視インタフェースの状態を確認してください。	障害監視インタフェースを設定したインタフェースに別の仮想ルータの設定があり，その仮想ルータの障害監視インタフェースが該当仮想ルータのインタフェースになっていないことを確認してください。なっている場合は，どちらかの障害インタフェースの設定を削除してください。
		上記の障害監視インタフェースの設定がない場合は項番 9 へ。
9	show vrrpstatus コマンドで detail パラメータを指定し，仮想ルータの状態を確認してください。	仮想ルータの状態が Initial の場合は，次の点を確認してください。 • 現在の優先度が 0 でない場合，Admin State 欄に表示されている非動作要因を排除してください。（非動作要因については，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。） • show logging コマンドでログを確認し，「The VRRP virtual MAC address entry can't be registered at hardware tables.」がある場合，H/W の MAC アドレステーブル設定に失敗しています。いったん該当仮想ルータのコンフィグレーションを削除し，異なる仮想ルータ番号でコンフィグレーションを設定し直すか，仮想ルータを設定する VLAN の VLAN ID を変更することで，仮想ルータが動作する可能性があります。
		仮想ルータの状態が Initial でない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。

3.13　SNMP の通信障害

3.13.1　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設定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

コンフィグレーションコマンド show access-list を実行し，コンフィグレーションのアクセスリストに SNMP マネージャの IP アドレスが設定されているかどうかを確認してください。その後，コンフィグレーションコマンド show snmp-server を実行し，コミュニティ名とアクセスリストが正しく設定されているかどうかを確認してください。
設定されていない場合は，コンフィグレーションコマンド snmp-server 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。

```
(config)#  show access-list
 access-list enable
 access-list 1 permit ip 20.1.1.1 0.0.0.255
 !
(config)#  show snmp-server
 snmp-server community "event-monitor" ro 1
 !
(config)#
```

SNMPv3 を使用する場合

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

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

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

3.13.2 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設定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

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

```
(config)#  show snmp-server
 snmp-server host    20.1.1.1 traps "event-monitor" snmp
 !
(config)#
```

SNMPv3 を使用する場合

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

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

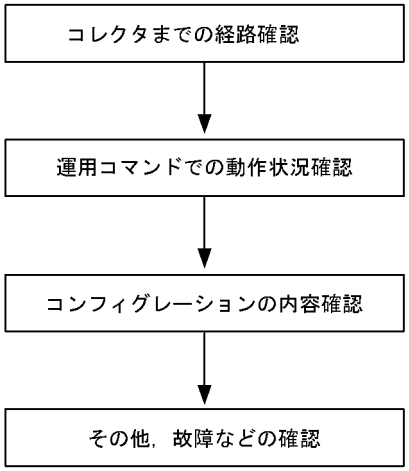
```
(config)# show snmp-server
  snmp-server engineID local "engine-ID"
  snmp-server group "v3group" v3 priv notify "view1"
  snmp-server host   20.1.1.1 traps "v3user" version 3 priv snmp
  snmp-server user "v3user" "v3group" v3 auth md5 "abc*_1234" priv des "xyz/
+6789"
  snmp-server view "view1" 1.3.6.1 included
  !
(config)#
```

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

3.14　sFlow 統計（フロー統計）機能のトラブルシューティング

本装置で，sFlow 統計機能のトラブルシューティングをする場合の流れは次のとおりです。

図 3-17　sFlow 統計機能のトラブルシューティングの流れ



3.14.1　sFlow パケットがコレクタに届かない

（1）コレクタまでの経路確認

「3.6.1　通信できない，または切断されている」および「3.9.1　通信できない，または切断されている」を参照し，コレクタに対してネットワークが正しく接続されているかを確認してください。もし，コンフィグレーションで sFlow パケットの最大サイズ（max-packet-size）を変更している場合は，指定しているパケットサイズでコレクタまで接続できるか確認してください。

（2）運用コマンドでの動作確認

show sflow コマンドを数回実行して sFlow 統計情報を表示し，sFlow 統計機能が稼働しているか確認してください。下線部の値が増加していない場合は，「(3) コンフィグレーションの確認」を参照してください。増加している場合は，「3.6.1　通信できない，または切断されている」，「3.9.1　通信できない，または切断されている」および「(5) コレクタ側の設定確認」を参照し，コレクタに対してネットワークが正しく接続されているかを確認してください。

図 3-18　show sflow コマンドの表示例

```
> show sflow
Date 2010/12/01 15:30:00 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  16:00:05
sFlow agent data :
  sFlow service version  : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate    : 1 per 2048 packets
  Configured sFlow ingress ports :  0/ 2-4
  Configured sFlow egress ports  :  ----
```

```
  Received sFlow samples : 37269  Dropped sFlow samples :    2093
  Exported sFlow samples : 37269  Couldn't exported sFlow samples    :       0
sFlow collector data :
  Collector IP address: 192.168.4.199  UDP:6343  Source IP address: 130.130.130.1
  Send FlowSample UDP packets    : 12077  Send failed packets:     0
  Send CounterSample UDP packets:   621  Send failed packets:     0
  Collector IP address: 192.168.4.203  UDP:65535  Source IP address: 130.130.130.1
  Send FlowSample UDP packets    : 12077  Send failed packets:     0
  Send CounterSample UDP packets:   621  Send failed packets:     0
>
```

注　下線部の値が，増加していることを確認してください。

（3）コンフィグレーションの確認

以下の内容について，運用中のコンフィグレーションを確認してください。

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

図 3-19　コンフィグレーションの表示例 1

```
(config)# show sflow
sflow destination 192.1.1.1 6455    ←コレクタの情報が正しく設定されていること
sflow sample 2048
!
(config)#
```

● サンプリング間隔が設定されていることを確認してください。
サンプリング間隔が設定されていないと，デフォルト値（＝大きな値）で動作するため値が大き過ぎ，フローサンプルがコレクタにほとんど送信されません。そのため，適切なサンプリング間隔を設定してください。ただし，推奨値より極端に小さな値を設定した場合，CPU 使用率が高くなる可能性があります。

図 3-20　コンフィグレーションの表示例 2

```
(config)# show sflow
sflow destination 192.1.1.1 6455
sflow sample 2048       ←適切なサンプリング間隔が設定されていること
!
(config)#
```

図 3-21　運用コマンドの表示例

```
> show sflow
Date 2010/12/01 15:30:00 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  16:00:05
  sFlow agent data :
  sFlow service version  : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate    : 1 per 2048 packets
  Configured sFlow ingress ports :  0/ 2-4
  Configured sFlow egress ports  :  ----
  Received sFlow samples : 37269  Dropped sFlow samples :    2093
  Exported sFlow samples : 37269  Couldn't exported sFlow samples    :       0
                           :
>
```

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

● フロー統計を行いたい物理ポートに対し，"sflow forward" が設定されていることを確認してください。

図 3-22 コンフィグレーションの表示例 3

```
(config)# show interfaces
interface gigabitethernet 0/2
  switchport mode access
  sflow forward ingress       ←ここに"sflow forward"が設定されていること
!
(config)#
```

● フロー統計を行いたい物理ポートに対し，"filter" が設定されていないことを「3.19.1 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。

● "sflow source" によって，sFlow パケットの送信元（エージェント）IP アドレスを指定した場合，その IP アドレスが本装置のポートに割り付けられていることを確認してください。

図 3-23 コンフィグレーションの表示例 4

```
(config)# show sflow
sflow destination 192.1.1.1 6455
sflow sample 2048
sflow source 192.1.1.100      ←本装置のポートに割り付けられているIPアドレスであること
!
(config)#
```

（4） NIF 状態・ポート状態の確認

show interfaces コマンドを実行し，sFlow 統計で監視する本装置の物理ポートやコレクタとつながる物理ポートの up/down 状態が，"active"（正常動作中）であることを確認してください。

図 3-24 ポート状態の表示例

```
> show interfaces gigabitethernet 0/5
Date 2010/12/01 15:30:00 UTC
NIF0:
Port5: active up  100BASE-TX full(auto)    0012.e220.ec31
       Time-since-last-status-change:1:47:47
       Bandwidth:10000kbps  Average out:5Mbps  Average in:5Mbps
       Peak out:5Mbps at 15:44:36  Peak in:5Mbps at 15:44:18
       Output rate:    4893.5kbps       16.8kpps
       Input  rate:    4893.5kbps       16.8kpps
       Flow control send   :off
       Flow control receive:off
       TPID:8100
                          :
>
```

注 下線部が，"active"または"active up"であることを確認してください。

ポートが DOWN 状態の場合は，「3.6.1 通信できない，または切断されている」および「3.9.1 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。

（5） コレクタ側の設定確認

- コレクタ側で UDP ポート番号（デフォルト値は 6343）が受信可能になっているか確認してください。受信可能になっていない場合，ICMP（[Type]Destination Unreachable [Code]Port Unreachable）が本装置に送られます。
- その他，利用しているコレクタ側の設定が正しいか確認してください。

3.14.2 フローサンプルがコレクタに届かない

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

(1) 中継パケット有無の確認

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

図 3-25 ポート状態の表示例

```
> show interfaces gigabitethernet 1/5
Date 2010/12/01 15:30:00 UTC
NIF0:
Port5: active up  100BASE-TX full(auto)    0012.e220.ec31
       Time-since-last-status-change:1:47:47
       Bandwidth:10000kbps  Average out:5Mbps  Average in:5Mbps
       Peak out:5Mbps at 15:44:36  Peak in:5Mbps at 15:44:18
       Output rate:    4893.5kbps       16.8kpps
       Input  rate:    4893.5kbps       16.8kpps
       Flow control send   :off
       Flow control receive:off
       TPID:8100
                                  :
>
```

注　下線部の表示で，パケットが中継されていることを確認してください。

(2) コレクタ側の設定確認

利用しているコレクタ側の設定が正しいか確認してください。

3.14.3 カウンタサンプルがコレクタに届かない

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

(1) カウンタサンプルの送信間隔の確認

本装置のコンフィグレーションで，フロー統計に関するカウンタサンプルの送信間隔の情報が 0 になっていないかを確認してください。この値が 0 になっているとカウンタサンプルのデータがコレクタへ送信されません。

図 3-26 コンフィグレーションの表示例

```
(config)# show sflow
sflow destination 192.1.1.1 6455
sflow sample 2048
sflow polling-interval 60       ←ここに0が設定されていないこと
!
(config)#
```

3.15　隣接装置管理機能の通信障害

3.15.1　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 3-44　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	show lldp コマンドを実行し，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。
		Status が Disabled の場合は 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	show lldp コマンドを実行し，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	show lldp statistics コマンドを実行し，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	show lldp コマンドを実行し，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	show lldp コマンドを実行し，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。 また，フィルタまたは QoS 制御によって LLDP の制御フレームが廃棄されている可能性があります。「3.19.1　フィルタ／QoS 設定情報の確認」を参照し確認してください。

3.15.2 OADP 機能により隣接装置情報が取得できない

OADP 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 3-45 OADP 機能使用時の障害解析方法

項番	確認内容・コマンド	対応
1	show oadp コマンドを実行し，OADP 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。
		Status が Disabled の場合は OADP 機能が停止状態となっています。OADP 機能を有効にしてください。
2	show oadp コマンドを実行し，ポート情報の表示を確認してください。	Enabled Port に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。
		Enabled Port に隣接装置が接続されているポートが表示されていない場合は OADP 機能の動作対象外となっています。ポートに対し OADP 機能を有効にしてください。なお，チャネルグループに属するポートでは OADP 機能の対象外となります。チャネルグループに対して OADP 機能を有効にしてください。
3	show oadp statistics コマンドを実行し，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りますので接続を確認してください。
		Discard/ERR 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	show interfaces コマンドを実行し，隣接装置が接続されているポートの状態を確認してください。	該当するポートの状態が active up の場合は項番 5 へ。
		その他の場合は「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。
5	show vlan コマンドを実行し，隣接装置が接続されているポートの所属する VLAN の状態を確認してください。	Status が Up の場合は項番 6 へ。
		Status が Disable の場合は OADP 機能の動作対象外になります。VLAN の状態を有効にしてください。
		その他の場合は「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。
6	show oadp コマンドを実行し，隣接装置が接続されているポートの隣接装置情報を確認してください。	表示されない場合は隣接装置側で項番 1 から項番 6 を調査してください。隣接装置側でも該当ポートの隣接装置情報が表示されない場合は，装置間の接続が誤っている可能性があるため，接続を確認してください また，フィルタまたは QoS 制御によって OADP の制御フレームが廃棄されている可能性があります。「3.19.1 フィルタ／ QoS 設定情報の確認」を参照し確認してください。

3.16　NTP の通信障害

3.16.1　NTP による時刻同期ができない

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

表 3-46　NTP の障害解析方法

項番	確認内容・コマンド	対応
1	show clock コマンド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	本装置と NTP サーバとの時刻差を確認してください。	本装置と NTP サーバとの時刻差が 1000 秒以内の場合は項番 3 へ。
		本装置と NTP サーバとの時刻差が 1000 秒以上ある場合には，set clock コマンドを使用して本装置の時刻を NTP サーバと合わせてください。
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，ping コマンドで確認してください。
		NTP サーバまたは本装置の設定で，UDP ポート番号 123 のパケットを廃棄する設定がないことを確認してください。

3.17 IEEE802.3ah/UDLD 機能の通信障害

3.17.1 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 3-47 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	show efmoam コマンドを実行し，IEEE802.3ah/UDLD 機能で inactive 状態にしたポートの障害種別を確認してください。	Link status に "Down(loop)" が表示されている場合は，L2 ループが起こる構成となっている可能性があります。ネットワーク構成を見直してください。
		Link status に "Down(uni-link)" が表示されている場合は，項番 2 へ。
2	対向装置で IEEE802.3ah/OAM 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	show efmoam statistics コマンドを実行し，禁止構成となっていないことを確認してください。	Info TLV の Unstable がカウントアップされている場合は，IEEE802.3ah/UDLD 機能での禁止構成となっている可能性があります。該当物理ポートの接続先の装置が 1 台であることを確認してください。
		Info TLV の Unstable がカウントアップされていない場合は項番 4 へ。
4	対向装置と直接接続されていることを確認してください。	メディアコンバータやハブなどが介在している場合は，対向装置と直接接続できるよう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	show efmoam コマンドを実行し，障害を検出するための応答タイムアウト回数を確認してください。	udld-detection-count 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。「3.19.1 フィルタ／QoS 設定情報の確認」を参照し確認してください。問題がない場合は項番 7 へ。
7	回線のテストをしてください。	「5 回線のテスト」を参照し，回線のテストをしてください。問題がない場合は項番 8 へ。
8	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，本装置特有の片方向リンク障害検出機能

3.18　CPU で処理するパケットの輻輳が回復しない

CPU で処理するパケットの輻輳が回復しない場合の対処方法について説明します。

CPU で処理するパケットの輻輳は，ソフトウェア処理が必要なパケットを多数受信した場合に，CPU 宛ての受信キューが溢れることで発生します。

CPU 宛てのキューでパケットの輻輳を検出すると，次のメッセージが出力されます。

”E3 SOFTWARE 00003301 1000:000000000000 CPU congestion detected.”

パケットの輻輳が回復すると，次のメッセージが出力されます。

”E3 SOFTWARE 00003302 1000:000000000000 CPU has recovered from congestion.”

CPU で処理するパケットの輻輳は，経路情報のエージングによって一時的に宛先不明のパケットを大量に受信した場合など，正常に動作していても発生することがあります。パケットの輻輳が回復しない，またはパケットの輻輳の発生と回復を頻繁に繰り返す場合は，本装置の設定またはネットワーク構成に問題がある可能性があります。本事象発生中に，次の表に従って対応してください。

表 3-48　CPU で処理するパケットの輻輳が回復しない場合の対処方法

項番	確認内容・コマンド	対応
1	パケット種別の特定 • show netstat statistics コマンドを 20 秒間隔で続けて実行して，結果を比較してください。	比較した結果，パケット種別が ip または ip6 の統計項目にある total packets received で大幅にカウントが増加している場合は項番 2 へ。
		比較した結果，パケット種別が arp の統計項目にある packets received で大幅にカウントが増加している場合は項番 2 へ。
		上記以外の場合は項番 4 へ。
2	受信 VLAN インタフェースの特定 • show netstat interface コマンドを 20 秒間隔で続けて実行して，結果を比較してください。	比較した結果，特定の VLAN インタフェースの統計項目にある Ipkts で大幅にカウントが増加している場合は項番 3 へ。
		上記以外の場合は項番 4 へ。
3	パケットの送信元／宛先アドレスの特定 • 項番 2 で特定した VLAN インタフェースに対して show tcpdump interface コマンドを実行して，項番 1 で特定したパケット種別の送信元アドレスと宛先アドレスを確認してください。	パケット種別が ip または ip6 で該当パケットの宛先アドレスが本装置の場合は，不正に送信されている可能性があります。送信元アドレスを持つ端末の設定を見直すか，ネットワーク構成を見直して，本装置宛てに該当パケットが送信されないようにしてください。
		パケット種別が ip または ip6 で該当パケットの宛先アドレスが他装置の場合は，ARP 情報のアドレスが解決していない，または宛先不明のパケットを大量に受信していることが考えられます。 • パケット種別が ip の場合は，「3.6.1　通信できない，または切断されている　(5) 隣接装置との ARP 解決情報の確認」を参照してください。 • パケット種別が ip6 の場合は，「3.9.1　通信できない，または切断されている　(4) 隣接装置との NDP 解決情報の確認」を参照してください。

項番	確認内容・コマンド	対応
		パケット種別が arp の場合は，ARP パケットを大量に受信しています。この場合，L2 ループ構成となっている可能性があります。ネットワーク構成を見直してください。ネットワーク構成に問題がなければ，送信元アドレスを持つ端末の設定を見直してください。
4	解析情報の採取 • show tech-support コマンドを 2 回実行してください。	収集した情報を支援部署に送付してください。

3.19　フィルタ／QoS の設定により生じる通信障害

3.19.1　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 制御の帯域監視，廃棄制御もしくは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. show access-filter コマンドを実行し，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 制御の帯域監視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. show qos-flow コマンドを実行し，インタフェースに適用している帯域監視のフロー検出条件と動作指定，フロー検出条件に一致したパケット数を確認します。
3. 2. で確認したフロー検出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。最大帯域制御を違反したパケットは廃棄し，統計情報の "matched packets(max-rate over)" をカウントアップします。本統計情報をカウントアップしている場合，インタフェースに適用している帯域監視によって，パケットを廃棄している可能性があります。
4. QoS 制御のコンフィグレーションの設定条件が正しいか，およびシステム構築での帯域監視の設定が適切であるかを見直してください。

（3） QoS 制御の廃棄制御およびレガシー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. show qos queueing コマンドを使って，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. 2. で確認した統計情報がカウントアップしている場合，QoS 制御の廃棄制御およびレガシーシェーパによってパケットを廃棄しています。
4. 廃棄制御およびレガシー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。

3.20 OpenFlow 機能の通信障害

3.20.1 OpenFlow コントローラとの接続が確立できない

OpenFlow コントローラとの接続が確立できない場合は，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 3-49 OpenFlow 機能の障害解析方法

項番	確認内容・コマンド	対応
1	本装置と OpenFlow コントローラ間のネットワーク到達性を確認してください。	本装置と OpenFlow コントローラ間でネットワーク到達性が確保されているか，ping コマンドで確認してください。
2	show openflow コマンドを実行し，Secure Channel の接続状態を確認してください。	本装置のサポートする OpenFlow プロトコルバージョンは v1.0.0 です。Secure Channel の接続状態が version-mismatched の場合，OpenFlow コントローラのバージョンを v1.0.0 対応にしてください。
3	show openflow detail コマンドを実行し，Secure Channel 接続しているポートが OpenFlow 機能の制御対象外になっているか確認してください。	l2-inband-secure-channel コマンドで OpenFlow 機能の制御対象から Secure Channel 接続する VLAN およびポートを除外してください。

3.20.2 同一サブネット内の通信速度が遅くなった

OpenFlow 機能を有効にし，本端末に他の通信端末を利用していて通信速度が遅くなったと感じる場合，PacketIn と PacketOut によるコントローラを経由したソフトウェア転送になっている可能性があります。下記の観点で確認してください。

（1） フローエントリーの確認

show openflow table コマンドで転送に使用するフローが登録されているかどうか確認を行ないます。

登録が行なえていない場合は（2）を行なってください。

（2） Open Flow コントローラへのメッセージ送信の正常性確認

本装置にて show openflow statistics コマンドを数回実行し，<Sent Error counter> カウンタが増加していないか確認してください。

このカウンターの値が増加しているようであれば同コマンドで表示される FLOW MOD FAILED：内の EPERM カウンタを確認してください。こちらのカウンタも同様に増加しているのであればコントローラと本装置の VLAN 設定に差異がありますので設定を確認してください。

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

show tech-support コマンドを使用して，障害発生時の情報採取を一括して採取できます。また，本コマンドでは，採取した障害情報を指定した ftp サーバに転送できます（「4.2.3 show tech-support コマンドを使用した保守情報のファイル転送」を参照）。

dump コマンドを使用して，障害発生時のメモリダンプを採取できます。

4.1.1 運用端末から ftp コマンドを使用した障害情報の取得

（1） リモート運用端末から障害情報を取得する

表 4-1 ftp コマンドで取得できる情報

項番	get 指定ファイル名	取得情報
1	.show-tech	show tech-support の表示結果
2	.show-tech-unicast	show tech-support unicast の表示結果
3	.show-tech-multicast	show tech-support multicast の表示結果
4	.show-tech-layer-2	show tech-support layer-2 の表示結果

図 4-1 リモート運用端末からの障害情報の取得

```
基本情報の取得
client-host> ftp 192.168.0.60                        <---1
Connected to 192.168.0.60.
220 192.168.0.60 FTP server (NetBSD-ftpd) ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get .show-tech show-tech.txt                    <---2
local: show-tech.txt remote: .show-tech
150 Opening BINARY mode data connection for '/etc/ftpshowtech'.
226 Transfer complete.
270513 bytes received in 8.22 seconds (32.12 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>
クライアントホストにshow-tech.txtファイルが取得されます。

ユニキャスト情報の取得
client-host> ftp 192.168.0.60                        <---3
Connected to 192.168.0.60.
220 192.168.0.60 FTP server (NetBSD-ftpd) ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get .show-tech-unicast show-tech-uni.txt        <---4
local: show-tech-uni.txt remote: .show-tech-uni.txt
150 Opening BINARY mode data connection for '/etc/ftpshowtech'.
226 Transfer complete.
343044 bytes received in 30.43 seconds (11.01 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>
クライアントホストにshow-tech-uni.txtファイルが取得されます。
```

1. ftp クライアントから装置に ftp 接続
2. .show-tech ファイルの転送
3. ftp クライアントから装置に ftp 接続
4. ファイルの転送

注

- ftp の ls などのコマンドで，get 指定すべきファイルは見えないので，事前のファイルの容量確認などはできません。
- 本情報の取得時は，装置側でコマンドを実行するため，転送中の状態が長く続きますが，途中で転送を中断しないでください。
- 装置の負荷状態や通信路の状態によっては，クライアント側がネットワークタイムアウトで切断することがあります。その場合は，クライアントのタイムアウト時間を長く設定してください。
- ftp での障害情報取得では show running-config コマンドなど，装置管理者専用コマンドの実行結果は採取しません。
- show tech-support を取得したときに，ログ情報に残るユーザ名は ftpuser となります。

4.2 保守情報のファイル転送

装置運用中に障害発生により自動的に採取されたログ情報やダンプ情報，またはコマンドを用いることで採取したダンプ情報をコンソールまたはリモート運用端末にファイル転送する方法を示します。ファイル転送を行うには ftp コマンド，zmodem コマンド，および show tech-support コマンドの三つの方法があります。なお，保守情報には次の表に示すものがあります。

表 4-2 保守情報

項番	項目	格納場所およびファイル名	ftp コマンドのファイルの転送形式
1	装置再起動時のダンプ情報ファイル	/dump0/rmdump ファイル転送後は削除してください。	binary
2	ネットワークインタフェース障害時のダンプ情報ファイル	/usr/var/hardware/ni**.*** *：0 ～ 9 の数字 ***：ダンプが採取されてからの通番。最も古いものと最新のものとの 2 ファイルまで格納されます。 ファイル転送後は削除してください。	binary
3	ログ情報	採取したディレクトリ（「図 4-3 ログ情報のリモート運用端末へのファイル転送」を参照）から次の名前で格納します。 運用ログ：log.txt 種別ログ：log_ref.txt	ASCII
4	コンフィグレーションファイル障害時の情報	装置管理者モードで次のコマンドを実行し，二つのファイルをホームディレクトリにコピーします。その後，ファイル転送してください。 cp /config/system.cnf system.cnf cp /config/system.txt system.txt ファイル転送後はコピーしたファイルを削除してください。	binary
11	障害待避情報	/usr/var/core/*.core ファイル転送後は削除してください。	binary

4.2.1 ftp コマンドを使用したファイル転送

リモート運用端末との間でファイル転送を行う場合は ftp コマンドを使用します。

(1) ダンプファイルをリモート運用端末に転送する

図 4-2 ダンプファイルのリモート運用端末へのファイル転送

```
> cd ダンプ格納ディレクトリ                          <---1
> ftp 192.168.0.1                                  <---2
Connected to 192.168.0.1.
220 FTP server (Version 6.00LS) ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> prompt                                       <---3
Interactive mode off.
ftp> bin                                          <---4
200 Type set to I.
ftp>cd 転送先ディレクトリ                          <---5
250 CMD command successful.
ftp> put ダンプファイル名                          <---6
local: ダンプファイル名 remote: ダンプファイル名
200 EPRT command successful.
150 Opening BINARY mode data connection for 'ダンプファイル名'.
100% |***********************************|  3897       2.13 MB/s    00:00 ETA
226 Transfer complete.
3897 bytes sent in 00:00 (82.95 KB/s)
ftp> bye
221 Goodbye.
>
```

1. 転送元ディレクトリの指定
2. 転送先端末のアドレスを指定
3. 対話モードを変更
4. バイナリモードに設定※
5. 転送先ディレクトリの指定
6. ダンプファイルの転送

注※

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

(2) ログ情報をリモート運用端末に転送する

図 4-3 ログ情報のリモート運用端末へのファイル転送

```
> show logging > log.txt
> show logging reference > log_ref.txt
> ftp 192.168.0.1                                  <---1
Connected to 192.168.0.1.
220 FTP server (Version 6.00LS) ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii                                        <---2
200 Type set to A.
ftp>cd 転送先ディレクトリ                                <---3
250 CMD command successful.
ftp> put log.txt                                  <---4
local: log.txt remote: log.txt
200 EPRT command successful.
150 Opening ASCII mode data connection for 'log.txt'.
100% |************************************| 89019     807.09 KB/s    --:-- ETA
226 Transfer complete.
89019 bytes sent in 00:00 (315.22 KB/s)
ftp> put log_ref.txt
local: log_ref.txt remote: log_ref.txt
200 EPRT command successful.
150 Opening ASCII mode data connection for 'log_ref.txt'.
100% |************************************|  4628       1.04 MB/s    --:-- ETA
226 Transfer complete.
4628 bytes sent in 00:00 (102.86 KB/s)
ftp> bye
221 Goodbye.
>
```

1. 転送先端末のアドレスを指定
2. アスキーモードに設定
3. 転送先ディレクトリの指定
4. ログ情報の転送

(3) 障害退避情報ファイルをリモート運用端末に転送する

図 4-4 障害退避情報ファイルのリモート運用端末へのファイル転送

```
> cd /usr/var/core/
> ls                                                    <---1
nimd.core       nodeInit.core
> ftp 192.168.0.1                                       <---2
Connected to 192.168.0.1.
220 FTP server (Version 6.00LS) ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> prompt                                            <---3
Interactive mode off.
ftp> bin                                               <---4
200 Type set to I.
ftp>cd 転送先ディレクトリ                                <---5
250 CMD command successful.
ftp> mput *.core                                       <---6
local: nimd.core remote: nimd.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'nimd.core'.
100% |*****************************************************************|
272 KB    1.12 MB/s    00:00 ETA
226 Transfer complete.
278528 bytes sent in 00:00 (884.85 KB/s)
local: nodeInit.core remote: nodeInit.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'nodeInit.core'.
100% |*****************************************************************|
1476 KB    1.40 MB/s    00:00 ETA
226 Transfer complete.
1511424 bytes sent in 00:01 (1.33 MB/s)
ftp> bye
221 Goodbye.
>
```

1. 障害退避情報ファイルが存在することを確認
   ファイルが存在しない場合は，何もせずに終了
2. 転送先端末のアドレスを指定
3. 対話モードを変更
4. バイナリモードに設定※
5. 転送先ディレクトリの指定
6. 障害退避情報ファイルの転送

注※

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

4.2.2 zmodem コマンドを使用したファイル転送

本装置と RS232C ケーブルで接続されているコンソールとの間でファイル転送を行う場合は zmodem コマンドを使用します。なお，通信を始めるに当たり，あらかじめコンソール側通信プログラムの受信操作を行ってください。

(1) ダンプファイルをコンソールに転送する

図 4-5 ダンプファイルのコンソールへのファイル転送

```
> cd ダンプ格納ディレクトリ                                <---1
> zmodem put ダンプファイル名                              <---2
>
```

1. 転送元ディレクトリの指定
2. ダンプファイルの転送

(2) ログ情報をコンソールに転送する

図 4-6 ログファイルのコンソールへのファイル転送

```
> show logging > log.txt
> show logging reference > log_ref.txt
> zmodem put log.txt                                       <---1
> zmodem put log_ref.txt
>
```

1. ログファイルの転送

(3) 障害退避情報ファイルをコンソールに転送する

図 4-7 障害退避情報ファイルのコンソールへのファイル転送

```
> cd /usr/var/core/
> ls                                                       <---1
interfaceControl.core    nodeInit.core
> zmodem put interfaceControl.core                         <---2
> zmodem put nodeInit.core
>
```

1. 障害退避情報ファイルが存在することを確認
   ファイルが存在しない場合は，何もしないで終了
2. ログファイルの転送

4.2.3 show tech-support コマンドを使用した保守情報のファイル転送

リモート運用端末またはリモートホストに対して保守情報のファイル転送を行う場合は show tech-support コマンドを使用します。

(1) 保守情報をリモート運用端末またはリモートホストに転送する

図 4-8 保守情報のリモート運用端末またはリモートホストへのファイル転送

```
> show tech-support ftp                                          <---1
Specify Host Name of FTP Server.       : 192.168.0.1            <---2
Specify User ID for FTP connections.   : staff1                 <---3
Specify Password for FTP connections.  :                        <---4
Specify Path Name on FTP Server.       : /usr/home/staff1       <---5
Specify File Name of log and Dump files: support                <---6
Wed Dec  1 15:30:00 UTC 2010
Transferred support.txt .
Executing.
.....................................................................
...........
.....................................................................
```

```
.................................................
Operation normal end.
########## Dump files' Information ##########
***** ls -l /dump0 *****
total 2344
-rwxrwxrwx  1 root  wheel  2400114 Dec  8 16:46 rmdump
***** ls -l /usr/var/hardware *****
-rwxrwxrwx  1 root  wheel  264198 Dec  8 16:43 ni00.000
########## End of Dump files' Information ##########
########## Core files' Information ##########
***** ls -l /usr/var/core *****
No Core files
########## End of Core files' Information ##########
Transferred support.tgz .
Executing.
.....................................................................
...........
.....................................................................
.....................................................
Operation normal end.
>
```

1. コマンドの実行
2. リモートホスト名を指定
3. ユーザ名を指定
4. パスワードを入力
5. 転送先ディレクトリの指定
6. ファイル名を指定

4.2.4 運用端末から ftp コマンドを使用したファイル転送

（1）リモート運用端末からダンプ情報ファイルを取得する

表 4-3 ftp コマンドで取得できるファイル

項番	get 指定ファイル名	取得ファイル
1	.dump	/dump0 と /usr/var/hardware 以下のファイル（圧縮）
2	.dump0	/dump0 以下のファイル（圧縮）
3	.hardware	/usr/var/hardware 以下のファイル（圧縮）

図 4-9 リモート運用端末からのダンプファイルの取得

```
client-host> ftp 192.168.0.60                      <---1
Connected to 192.168.0.60.
220 192.168.0.60 FTP server (NetBSD-ftpd) ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary                                        <---2
200 Type set to I.
ftp> get 指定ファイル名 dump.tgz                    <---3
local: dump.tgz remote: 指定ファイル名
150 Opening BINARY mode data connection for '/etc/ftpdump'.
226 Transfer complete.
2411332 bytes received in 5.78 seconds (407.13 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>
```

クライアントホストにdump.tgzファイルが取得されます。

1. ftp クライアントから装置に ftp 接続
2. ダンプ情報ファイルは必ずバイナリモードで転送してください。
   アスキーモードでは転送できません。
3. ダンプファイルの転送

注

- ftp の ls などのコマンドで，get 指定すべきファイルは見えないので，事前のファイルの容量確認などはできません。
- 装置の負荷状態や通信路の状態によっては，クライアント側がネットワークタイムアウトで切断することがあります。その場合は，クライアントのタイムアウト時間を長く設定してください。

4.3 MC への書き込み

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

4.3.1 運用端末による MC へのファイル書き込み

運用端末で装置の情報を MC に書き込みます。

図 4-10 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。

ls -l コマンドでコピー元ファイル(tech.log)の容量を確認する。

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

show mcコマンドで空き容量を確認する。

```
#show mc
Date 2010/12/01 15:30:00 JST
MC  : enabled
    Manufacture ID : 00000030
        269kB used
    994,816kB free                                  <---1
    995,085kB total
```

cpコマンドでコピー元ファイルをtech-1.logというファイル名称でMCにコピーする。

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

MCにファイルが書き込めていることを確認する。

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

1. 空き容量

5 回線のテスト

5.1　回線をテストする

5.1.1　イーサネットポート

回線テストでは，指定するテスト種別により，テスト用に送出するフレームまたはデータの折り返し位置が異なります。テスト種別によるフレームの折り返し位置を次の図に示します。

図 5-1　回線テストのテスト種別によるフレームの折り返し位置

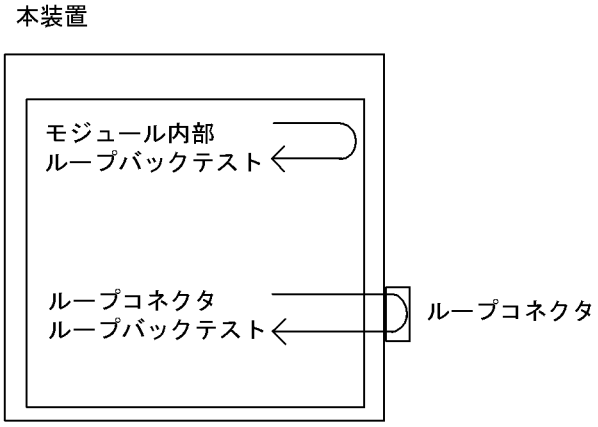


表 5-1　フレーム折り返し位置ごとの回線テスト種別

フレームの折り返し位置	回線テスト種別	確認できる障害部位
装置	モジュール内部ループバックテスト	装置（RJ45 コネクタおよびトランシーバを除く）
ループコネクタ	ループコネクタループバックテスト	装置（RJ45 コネクタおよびトランシーバ含む）

また，回線種別により，実行可能なテスト種別が異なります。回線種別と実行可能なテスト種別については，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。

次にテスト種別ごとのテスト方法を説明します。

（1）装置内でのフレーム折り返しを確認する

装置内でのフレーム折り返しを確認する場合，モジュール内部ループバックテストを実行してください。モジュール内部ループバックテストを実行する場合は，inactivate コマンドでポートを inactive 状態にしてから行ってください。テストを終了するときは，activate コマンドでポートを inactive 状態から active 状態に戻してください。本テストでは，装置障害（RJ45 コネクタおよびトランシーバを除く）の有無を確認するため，テスト用フレームを本装置内で折り返します。本テストは全回線種別で実行できます。

テスト例として，NIF 番号 0，ポート番号 1 で送信間隔 1 秒としてテストを行ったケースを示します。

運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> inactivate gigabitethernet 0/1  [Enter]
> test interfaces gigabitethernet 0/1 internal  [Enter]
```

（約1分間待つ）

```
> no test interfaces gigabitethernet 0/1  [Enter]
> activate gigabitethernet 0/1  [Enter]
```

コマンド実行結果として，「図 5-2　test interfaces，no test interfaces コマンド実行結果例」に示す画面を表示するので，次のことを確認してください。

”Send-NG”および”Receive-NG”が 0 であること。

”Send-NG”および”Receive-NG”が 0 の場合，回線テスト結果は正常です。

”Send-NG”および”Receive-NG”が 0 でない場合は，何らかの異常があるので，マニュアル「運用コマンドレファレンス」の回線テスト実行結果の表示内容を参照してください。

10GBASE-R で”Send-NG”および”Receive-NG”が 0 でない場合は再度回線テストを実行し，”Send-NG”および”Receive-NG”が 0 であることを確認してください。0 でない場合は，何らかの異常があるので，マニュアル「運用コマンドレファレンス」の回線テスト実行結果の表示内容を参照してください。

図 5-2　test interfaces，no test interfaces コマンド実行結果例

```
> inactivate gigabitethernet 0/1
> test interfaces gigabitethernet 0/1 internal interval 2 pattern 4

> no test interfaces gigabitethernet 0/1
> activate gigabitethernet 0/1
Date 2010/12/01 15:30:00 UTC
Interface type              :100BASE-TX
Test count                  :12
Send-OK                     :12             Send-NG                 :0
Receive-OK                  :12             Receive-NG              :0
Data compare error          :0
Out buffer hunt error       :0              Out line error          :0
In CRC error                :0              In frame alignment      :0
In monitor time out         :0              In line error           :0
H/W error                   :none
```

（2）ループコネクタでのフレーム折り返しを確認する

ループコネクタでのフレーム折り返しを確認する場合，ループコネクタループバックテストを実行してください。ループコネクタループバックテストを実行する場合，およびループコネクタを接続する場合は，inactivate コマンドでポートを inactive 状態にしてから行ってください。テストを終了するときは，接続を戻してから activate コマンドでポートを inactive 状態から active 状態に戻してください。本テストでは，装置障害（RJ45 コネクタおよびトランシーバ含む）を確認するため，テスト用フレームを本装置に接続したループコネクタ内で折り返します。本テストは全回線種別で実行できます。

回線種別ごとにテストする対象のポート番号のケーブルを抜いて各回線種別ごとのループコネクタを接続しテストを実施します。ループコネクタ未接続，またはそのポートに対応するループコネクタを接続しない場合，正しくテストが実施できないので注意してください。

テスト例として，NIF 番号 0，ポート番号 1 で送信間隔 1 秒としてケーブルを抜いて各回線種別ごとのループコネクタを接続しテストを行ったケースを示します。
運用端末から test interfaces，no test interfaces の順でコマンドを実行します。

```
> inactivate gigabitethernet 0/1  [Enter]
```

（該当ポートにループコネクタを接続する）

```
> test interfaces gigabitethernet 0/1 connector  [Enter]
```

（約1分間待つ）

```
> no test interfaces gigabitethernet 0/1  [Enter]
```

（該当ポートのループコネクタを外し，接続を元に戻す）

```
> activate gigabitethernet 0/1  [Enter]
```

なお，テスト実行結果の確認は「(1) 装置内でのフレーム折り返しを確認する」のテスト実行結果と同様に行ってください。

6 装置の再起動

この章では，主に装置を再起動する場合の作業手順について説明します。

6.1　装置を再起動する

6.1.1　装置の再起動

reload コマンドを使用して，装置を再起動できます。また，再起動時にログを保存します。

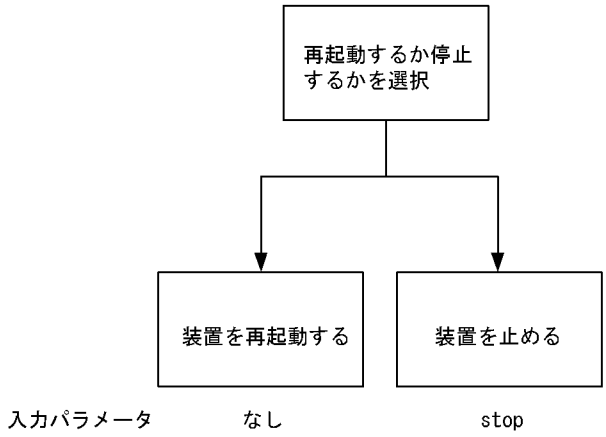
コマンドの入力形式，パラメータについてはマニュアル「運用コマンドレファレンス」を参照してください。

実行例として，「装置を再起動」し，CPU メモリダンプ採取については確認メッセージに従って行う場合の，reload コマンドのパラメータ選択について説明します。

Step1

装置を再起動するか，停止するかを選択します。

図 6-1　装置再起動・停止選択

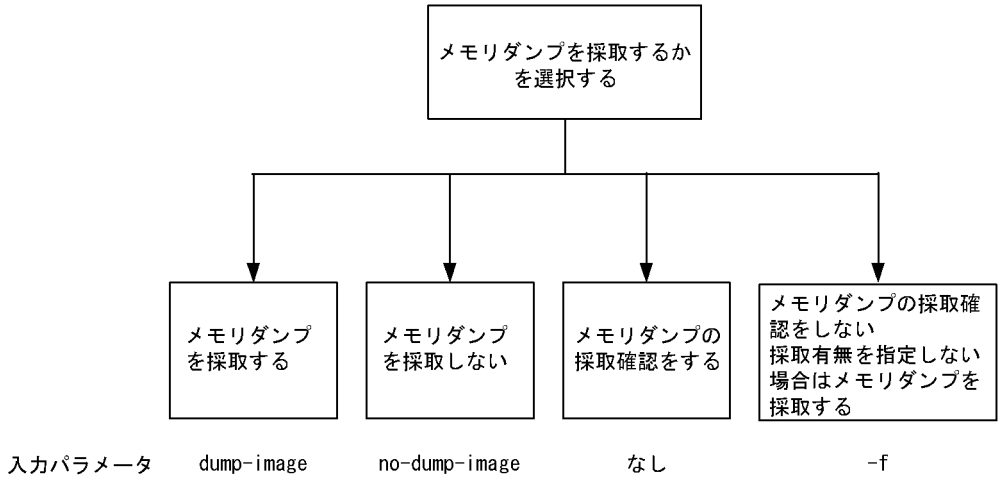


Step1 では，装置を再起動させるので，上記の図によりパラメータは選択しません。

Step2

次にダンプ採取するかどうかを選択します。

図 6-2　CPU メモリダンプ採取選択

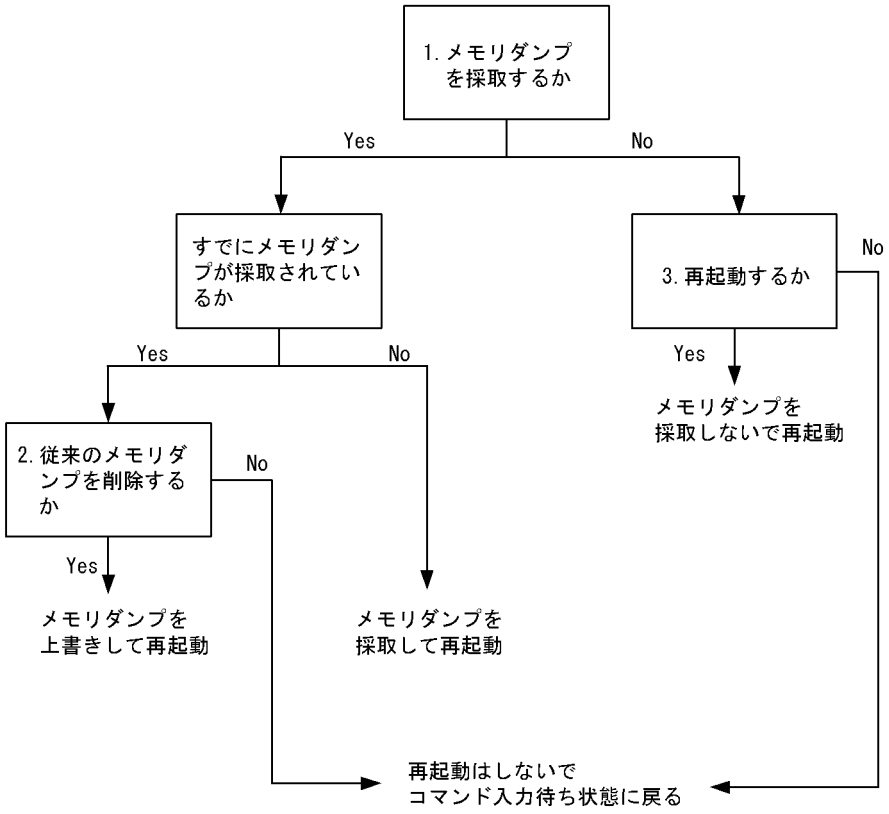


Step2 では，CPU メモリダンプ採取の確認をするので，上記の図によりパラメータは選択しません。Step1 から Step2 で選択したパラメータを組み合わせると「reload」となります。このコマンドを入力すると，以下のような，ダンプ採取確認メッセージが出力されます。

1. Dump information extracted?(y/n):_
2. old dump file(rmdump 01/01 00:00) delete OK? (y/n):_
3. Restart OK? (y/n):_

上記のメッセージが出力されるタイミングは，次に示すフローチャートの番号に対応しています。

図 6-3　CPU メモリダンプ採取確認メッセージ



付録

付録 A　show tech-support コマンド表示内容詳細

付録 A.1　show tech-support コマンド表示内容詳細

show tech-support コマンドでプロトコルのパラメータ指定ごとに表示されるコマンドの内容を次の表に示します。

なお，表示内容の詳細については，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。

【注意】

show tech-support コマンドで表示される情報の一部については，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	unicast	multicast	layer-2
1	show version	本装置のソフトウェアバージョン情報およびハードウェア情報	○	○	○	○
2	show license	オプションライセンス情報	○	○	○	○
3	show system	装置の運用状態	○	○	○	○
4	show environment	FAN/ 電源 / 稼働時間情報	○	○	○	○
5	show process cpu	プロセスの CPU 使用情報	○	○	○	○
6	show process memory	プロセスのメモリ使用情報	○	○	○	○
7	show cpu days hours minutes seconds	CPU 使用率	○	○	○	○
8	show memory summary	装置のメモリ使用情報	○	○	○	○
9	/sbin/dmesg	カーネル内イベント情報	○	○	○	○
10	cat /var/run/dmesg.boot	カーネル内イベント情報	○	○	○	○
11	cat /var/log/messages	カーネルおよびデーモンの内部情報	○	○	○	○
12	/usr/local/diag/statShow	カーネル内部統計情報	○	○	○	○
13	fstat	ファイルデスクリプタ情報	○	○	○	○
14	/usr/local/diag/rtsystat	内部デバイス関連情報	○	○	○	○
15	/usr/local/diag/rtastat	経路配布関連情報	○	○	○	○
16	show netstat all-protocol-address numeric	レイヤ 4 関連統計情報	○	○	○	○
17	show netstat statistics	レイヤ 3 関連統計情報	○	○	○	○
18	show dumpfile	採取済みのダンプファイル情報	○	○	○	○
19	ls -lTiR /dump0	ダンプファイル情報	○	○	○	○
20	ls -lTiR /usr/var/hardware	ハードウェアダンプファイル情報	○	○	○	○
21	ls -lTiR /usr/var/core	core ファイル情報	○	○	○	○
22	ls -lTiR /config	config ファイル情報	○	○	○	○
23	ls -lTiR /var	メモリファイルシステム情報	○	○	○	○

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
24	df -ik	パーティション情報	○	○	○	○
25	du -Pk /	ファイルシステム使用状況	○	○	○	○
26	show logging	運用系時系列ログ情報	○	○	○	○
27	show logging reference	運用系種別ログ情報	○	○	○	○
28	show ntp associations	ntp サーバの動作情報	○	○	○	○
29	/usr/bin/w -n	ログイン関連情報	○	○	○	○
30	show session	ログインセッション情報	○	○	○	○
31	/usr/sbin/pstat -t	端末情報	○	○	○	○
32	stty -a -f /dev/tty00	コンソール端末情報	○	○	○	○
33	cat /var/log/clitrace1	CLI トレース情報 1	○	○	○	○
34	cat /var/log/clitrace2	CLI トレース情報 2	○	○	○	○
35	cat /var/log/mmitrace	運用コマンドトレース情報	○	○	○	○
36	cat /var/log/kern.log	カーネル内部トレース情報	○	○	○	○
37	cat /var/log/daemon.log	デーモン関連内部トレース情報	○	○	○	○
38	cat /var/log/fixsb.log	カーネル内部トレース情報	○	○	○	○
39	cat /usr/var/pplog/ppupdate.log	ソフトウェアアップデート実行時のログ情報	○	○	○	○
40	cat /usr/var/pplog/ppupdate2.log	ソフトウェアアップデート実行時のログ情報	○	○	○	○
41	tail -n 30 /var/log/authlog	認証トレース情報	○	○	○	○
42	tail -n 30 /var/log/xferlog	FTP トレース情報	○	○	○	○
43	cat /var/log/ssh.log	SSH ログ情報	○	○	○	○
44	show accounting	アカウンティング情報	○	○	○	○
45	cat /var/tmp/gen/trace/mng.trc	コンフィグレーションコマンドトレース情報 1	○	○	○	○
46	cat /var/tmp/gen/trace/mng_sub.trc	コンフィグレーションコマンドトレース情報 2	○	○	○	○
47	tail -n 400 /var/tmp/gen/trace/api.trc	コンフィグレーションコマンドトレース情報 3	○	○	○	○
48	tail -n 400 /var/tmp/gen/trace/ctl.trc	コンフィグレーションコマンドトレース情報 4	○	○	○	○
49	show netstat interface	カーネル内インタフェース情報	○	○	○	○
50	show vlan list	VLAN 情報一覧	○	○	○	○
51	show port	ポートの情報	○	○	○	○
52	show port statistics	ポートの統計情報	○	○	○	○
53	show port protocol	ポートのプロトコル情報	○	○	○	○
54	show port transceiver debug	ポートのトランシーバ詳細情報	○	○	○	○
55	show interfaces nif XXX_NIF line XXX_LINE debug	ポートの詳細統計情報	○	○	○	○
56	show running-config	運用面のコンフィグレーション	○	○	○	○

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
57	show channel-group detail	リンクアグリゲーションの詳細情報	○	○	○	○
58	show spanning-tree detail	スパニングツリーの詳細情報	○	○	○	○
59	show axrp detail	Ring Protocol の詳細情報	○	○	○	○
60	show efmoam detail	IEEE802.3ah/OAM 機能の設定情報およびポートの状態	○	○	○	○
61	show efmoam statistics	IEEE802.3ah/OAM 機能の統計情報	○	○	○	○
62	show lldp detail	LLDP 機能の隣接装置情報	○	○	○	○
63	show oadp detail	OADP 機能の隣接装置情報	○	○	○	○
64	show loop-detection	L2 ループ検知機能の情報	×	×	×	○
65	show loop-detection statistics	L2 ループ検知機能の統計情報	×	×	×	○
66	show loop-detection logging	L2 ループ検知機能のログ情報	×	×	×	○
67	show channel-group statistics	リンクアグリゲーション統計情報	×	×	×	○
68	show spanning-tree statistics	スパニングツリーの統計情報	×	×	×	○
69	show vlan detail	VLAN 情報詳細	×	○	○	○
70	show qos queueing	全キューの統計情報	○	○	○	○
71	show access-filter	フィルタ機能の統計情報	×	○	○	○
72	show qos-flow	QoS 制御機能の統計情報	×	○	○	○
73	show lldp statistics	LLDP 機能の統計情報	×	×	×	○
74	show oadp statistics	OADP 機能の統計情報	×	×	×	○
75	show mac-address-table	mac-address-table 情報	×	○	○	○
76	show igmp-snooping	IGMP snooping 情報	×	×	×	○
77	show igmp-snooping group	IGMP snooping のグループ情報	×	×	×	○
78	show igmp-snooping statistics	IGMP snooping の統計情報	×	×	×	○
79	show mld-snooping	MLD snooping 情報	×	×	×	○
80	show mld-snooping group	MLD snooping のグループ情報	×	×	×	○
81	show mld-snooping statistics	MLD snooping の統計情報	×	×	×	○
82	show netstat routing-table numeric	カーネル内経路関連情報（ユニキャスト）	×	○	○	×
83	show netstat multicast numeric	カーネル内経路関連情報（マルチキャスト）	×	×	○	×
84	show ip multicast statistics	IPv4 マルチキャスト統計情報	×	×	○	×
85	show ipv6 multicast statistics	IPv6 マルチキャスト統計情報	×	×	○	×
86	show ip igmp interface	IGMP が動作するインタフェース情報	×	×	○	×
87	show ip igmp group	IGMP が管理するグループ情報	×	×	○	×
88	show ip pim interface (detail)	IPv4 PIM が動作するインタフェース情報	×	×	○	×
89	show ip pim neighbor (detail)	IPv4 PIM の近隣情報	×	×	○	×

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
90	show ip pim bsr	IPv4 PIM の BSR 情報	×	×	○	×
91	show ip pim rp-mapping	IPv4 PIM のランデブーポイント情報	×	×	○	×
92	show ip mroute	IPv4 マルチキャスト経路情報	×	×	○	×
93	show ip mcache	IPv4 マルチキャスト中継エントリ	×	×	○	×
94	show ipv6 mld interface	MLD が動作するインタフェース情報	×	×	○	×
95	show ipv6 mld group	MLD が管理するグループ情報	×	×	○	×
96	show ipv6 pim interface (detail)	IPv6 PIM が動作するインタフェース情報	×	×	○	×
97	show ipv6 pim neighbor (detail)	IPv6 PIM の近隣情報	×	×	○	×
98	show ipv6 pim bsr	IPv6 PIM の BSR 情報	×	×	○	×
99	show ipv6 pim rp-mapping	IPv6 PIM のランデブーポイント情報	×	×	○	×
100	show ipv6 mroute	IPv6 マルチキャスト経路情報	×	×	○	×
101	show ipv6 mcache	IPv6 マルチキャスト中継エントリ	×	×	○	×
102	show ip multicast statistics	IPv4 マルチキャスト統計情報	×	×	○	×
103	show ipv6 multicast statistics	IPv6 マルチキャスト統計情報	×	×	○	×
104	show vrrpstatus detail statistics	VRRP の仮想ルータの状態と統計情報	×	○	×	×
105	show track detail	VRRP の障害監視インタフェース情報	×	○	×	×
106	show ip interface ipv4-unicast	ユニキャストルーティングプログラムが認識している本装置のインタフェース情報	×	○	×	×
107	show processes memory unicast	ユニキャストルーティングプログラムでのメモリの確保状況および使用状況	×	○	×	×
108	show processes cpu minutes unicast	ユニキャストルーティングプログラムの CPU 使用率	×	○	×	×
109	show dhcp giaddr all	DHCP リレーエージェントの DHCP パケットの受信先 IP アドレス情報	×	○	×	×
110	show dhcp traffic	DHCP リレーエージェント統計情報	×	○	×	×
111	show ip dhcp server statistics	DHCP サーバ統計情報	×	○	×	×
112	show ip dhcp conflict	DHCP サーバ衝突 IP アドレス情報	×	○	×	×
113	show ipv6 dhcp server statistics	IPv6 DHCP サーバ統計情報	×	○	×	×
114	show ip route summary	ルーティングプロトコルが保有するアクティブ経路数と非アクティブ経路数	○	○	○	○
115	show ip rip statistics	RIP の統計情報	×	○	×	×
116	show ip rip advertised-routes summary	RIP で広告した経路数	×	○	×	×
117	show ip rip received-routes summary	RIP で学習した経路数	×	○	×	×
118	show ip ospf	OSPF のグローバル情報	×	○	×	×

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
119	show ip ospf discard-packets	OSPF で廃棄されたパケット情報	×	○	×	×
120	show ip ospf statistics	OSPF で収集されている送受信パケットの統計情報	×	○	×	×
121	show ip ospf neighbor detail	OSPF の隣接ルータの詳細情報	×	○	×	×
122	show ip ospf virtual-links detail	OSPF の仮想リンク情報の詳細情報	×	○	×	×
123	show ip ospf database database-summary	OSPF の LS タイプごとの LSA 数	×	○	×	×
124	show ip bgp neighbor detail	BGP4 のピアリング情報	×	○	×	×
125	show ip bgp notification-factor	BGP4 のコネクションを切断する要因となったメッセージ	×	○	×	×
126	show ip bgp received-routes summary	BGP4 のピアから受信した経路情報数	×	○	×	×
127	show ip bgp advertised-routes summary	BGP4 のピアへ広告した経路情報数	×	○	×	×
128	show ipv6 interface ipv6-unicast	ユニキャストルーティングプログラムが認識している本装置のインタフェース情報	×	○	×	×
129	show ipv6 route summary	ユニキャストルーティングプログラムが保有するアクティブ経路数と非アクティブ経路数	○	○	○	○
130	show ipv6 rip advertised-routes summary	RIPng で広告した経路数	×	○	×	×
131	show ipv6 rip received-routes summary	RIPng で学習した経路数	×	○	×	×
132	show ipv6 rip statistics	RIPng の統計情報	×	○	×	×
133	show ipv6 ospf	OSPFv3 のグローバル情報	×	○	×	×
134	show ipv6 ospf discard-packets	OSPFv3 で廃棄されたパケットの情報	×	○	×	×
135	show ipv6 ospf statistics	OSPFv3 で収集したパケットの統計情報	×	○	×	×
136	show ipv6 ospf neighbor detail	OSPFv3 の隣接ルータの状態	×	○	×	×
137	show ipv6 ospf virtual-links detail	OSPFv3 の仮想リンク情報	×	○	×	×
138	show ipv6 ospf database database-summary	OSPFv3 の LS-Database の数	×	○	×	×
139	show ipv6 bgp neighbor detail	BGP4+ のピアリング情報	×	○	×	×
140	show ipv6 bgp notification-factor	BGP4+ のコネクションを切断する要因となったパケット	×	○	×	×
141	show ipv6 bgp received-routes summary	BGP4+ のピアから受信した経路情報数	×	○	×	×
142	show ipv6 bgp advertised-routes summary	BGP4+ のピアへ広告した経路情報数	×	○	×	×
143	show sflow detail	sFlow 統計情報（詳細）の表示	○	○	○	○
144	port snd/rcv statistics	ポート送受信統計情報	○	○	○	○

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
145	internal SW HW event statistics0	内部 SW イベント統計情報 0	○	○	○	○
146	internal SW HW event statistics1	内部 SW イベント統計情報 1	○	○	○	○
147	swdev logging	SW 部ログの表示	○	○	○	○
148	show openflow detail	OpenFlow 機能の一般情報詳細	○	○	○	○
149	show openflow resource	OpenFlow 機能のテーブル使用状況	○	○	○	○
150	show openflow statistics	OpenFlow 機能の Secure Channel 統計情報	×	×	×	○
151	show openflow table	OpenFlow 機能のフローエントリ情報詳細	×	×	×	○
152	wol kernel-dump	WoL カーネル設定情報	○	○	○	○

（凡例）　○：表示対象　×：非表示対象

注　コマンド（表示）列の（　）は，ソフトウェアのバージョンによっては表示されることを示しています。

索引

数字

B

C

D

F

I

L

M

N

O

P

R

S

V

Z

い

う

か

き

こ

し

す

そ

つ

と

ね

ふ

ほ

り

れ

ろ