AX2340S

トラブルシューティングガイド

AX23S-T001

■対象製品

このマニュアルは AX2340S を対象に記載しています。

■輸出時の注意

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

■商標一覧

Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，富士ゼロックス株式会社の登録商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
OpenSSL は，米国およびその他の国における米国 OpenSSL Software Foundation の登録商標です。
Python(R)は，Python Software Foundation の登録商標です。
RSA および RC4 は，米国およびその他の国における米国 EMC Corporation の登録商標です。
sFlow は，米国およびその他の国における米国 InMon Corp. の登録商標です。
ssh は，SSH Communications Security,Inc.の登録商標です。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
イーサネットは，富士ゼロックス株式会社の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み，保管してください。

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

■ご注意

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

２０２１年　８月　（第１版）　ＡＸ２３Ｓ－Ｔ００１

■著作権

はじめに

■対象製品

このマニュアルは AX2340S を対象に記載しています。
操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。

■このマニュアルの訂正について

このマニュアルに記載の内容は，「マニュアル訂正資料」で訂正する場合があります。

■対象読者

本装置を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。
また，次に示す知識を理解していることを前提としています。
・ネットワークシステム管理の基礎的な知識

■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しておりますので，あわせてご利用ください。
https://www.alaxala.com/

■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。

●ハードウェアの設備条件，取扱方法を調べる

ハードウェア取扱説明書
（AX23S-H001）

●ソフトウェアの機能とコマンド，コンフィグレーションの設定を知りたい

コンフィグレーションガイド Vol.1
（AX23S-S001）

Vol.2
（AX23S-S002）

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

コンフィグレーション
コマンドレファレンス
（AX23S-S003）

●運用コマンドの入力シンタックス，パラメータ詳細について知りたい

運用コマンドレファレンス
（AX23S-S004）

●メッセージとログについて調べる

メッセージ・ログレファレンス
（AX23S-S005）

●MIBについて調べる

MIBレファレンス
（AX23S-S006）

●トラブル発生時の対処方法について知りたい

トラブルシューティングガイド
（AX23S-T001）

■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
bit/s	bits per second　　*bps と表記する場合もあります。
BPDU	Bridge Protocol Data Unit
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Continuity Check
CFM	Connectivity Fault Management
CIST	Common and Internal Spanning Tree
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRR	Deficit Round Robin
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECDHE	Elliptic Curve Diffie-Hellman key exchange, Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EEE	Energy Efficient Ethernet
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
GCM	Galois/Counter Mode
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol

IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NDP	Neighbor Discovery Protocol
NTP	Network Time Protocol
OAM	Operations,Administration,and Maintenance
OUI	Organizationally Unique Identifier
packet/s	packets per second　　*pps と表記する場合もあります。
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PID	Protocol IDentifier
PoE	Power over Ethernet
PQ	Priority Queueing
PS	Power Supply
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RMON	Remote Network Monitoring MIB
RQ	ReQuest
RSA	Rivest, Shamir, Adleman
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SFD	Start Frame Delimiter

SFP	Small Form factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SSAP	Source Service Access Point
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
VLAN	Virtual LAN
WAN	Wide Area Network
WWW	World-Wide Web

■KB(キロバイト)などの単位表記について

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

目次

1 装置障害のトラブルシュート

この章では，装置障害が発生した場合の対処について説明します。

1.1 装置の障害解析

1.1.1 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。

装置の各 LED の状態については，各モデルの「ハードウェア取扱説明書」を参照してください。なお，LED の状態は，装置を目視できない場合でも，リモート運用端末から運用コマンドで確認することによって，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。

表 1-1　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	次の手順で，装置への給電をすべて停止させてください。 ・AC 電源を使用している装置 本装置に搭載されているすべての AC 電源に接続されている電源ケーブルを，コンセントから抜いてください。 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	1. MC が挿入されている場合は，MC を抜きます。 2. 装置の電源ケーブルをコンセントから抜き，再度挿入します。 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 PWR LED が消灯している	次の手順で対策を実施します。 1. 「表 1-2　電源障害の切り分け」を実施します。 2. 上記 1 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）電源を OFF にし，再度 ON にして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"の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（2）の手順で障害情報が存在しないまたは"高温注意"の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 ST1 LED が橙点灯している	装置に致命的障害が発生しています。装置を交換してください。
5	・装置の ST1 LED が橙点滅している ・装置の各ポートの LINK LED が橙点灯している	装置または回線に部分障害が発生しています。 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

表 1-2　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ます。

項番	障害内容	対策内容
2	測定した入力電源が以下の範囲外である AC100V の場合：AC90～127V AC200V の場合：AC180～254V 注　本件は入力電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。

1.1.2 装置の交換方法

装置の交換方法は,「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。

2 運用管理のトラブルシュート

この章では，運用管理でトラブルが発生した場合の対処について説明します。

2.1 ログインのトラブル

2.1.1 ログインユーザのパスワードを忘れた

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

- ログインできるユーザがほかにいる場合
  ログインできるユーザが，装置管理者モードで password コマンドを実行しパスワードを忘れたログインユーザのパスワードを再設定します。または，clear password コマンドでパスワードを削除します。これらのコマンドは，装置管理者モードで実行します。したがって，ログインするユーザは入力モードを装置管理者モードに変更するための enable コマンドのパスワードを知っている必要があります。
  パスワードを忘れた user1 のパスワードを管理者モードで再設定する例を次の図に示します。

  図 2-1　user1 のパスワードを再設定する例

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

- ログインできるユーザがいない場合
  ユーザアカウント／パスワード，ライセンス情報，スタートアップコンフィグレーションやログ情報などを初期化することができます。
  装置の電源を ON し，コンソール画面に BootROM のメッセージが出力されたら，［Ctrl］+［N］キーを同時に押下し続けてください。「Do you erase system setting ? (Y/N):」のメッセージが出力されらたら，［Y］キー（［Y］キーは大文字です）を押下してください。初期化が完了すると，自動的で装置再起動が行われ，再起動後には初期導入時のユーザで装置へログインできます。なお，コンソールの通信速度は，115200bit/s としてください。

  図 2-2　装置情報初期化の実施例

```
BootROM: Image checksum verification PASSED
BootROM: Boot image signature verification PASSED
|
Do you erase system setting ? (Y/N): Y

Boot device 0
Starting kernel ...
```

2.1.2 装置管理者モードのパスワードを忘れた

「2.1.1 ログインユーザのパスワードを忘れた」のログインできるユーザがいない場合と同じ方法で，装置管理者モードのパスワードを初期化することができます。

2.2 運用端末のトラブル

2.2.1 コンソールからの入力，表示がうまくできない

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

表 2-1　コンソールとの接続トラブルおよび対応

項番	障害内容	確認内容
1	画面に何も表示されない	次の手順で確認してください。 1. 装置の正面パネルにある ST1 LED が緑点灯になっているかを確認してください。緑点灯していない場合は，「1.1　装置の障害解析」を参照してください。 2. ケーブルの接続が正しいか確認してください。 3. 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：115200bit/s（変更している場合は設定値） データ長：8bit パリティビット：なし ストップビット：1bit フロー制御：なし
2	キー入力を受け付けない	次の手順で確認してください。 1. XON／XOFF によるフロー制御でデータの送受信を中断している可能性があります。データ送受信の中断を解除してください（［Ctrl］＋［Q］をキー入力してください）。それでもキー入力ができない場合は 2.以降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 115200bit/s に設定されているか確認してください。 2. コンフィグレーションコマンド line console 0 で CONSOLE(RS232C)の通信速度を 2400，4800，9600，または 19200bit/s に設定している場合は，通信ソフトウェアの通信速度が正しく設定されているか確認してください。
4	ユーザ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	1. 画面にログインプロンプトが出ているか確認してください。出ていなければ，装置を起動中のため，しばらくお待ちください。 2. ローカル認証でログインする場合は，装置に存在しないアカウントでログインしようとしていないか確認してください。 3. コンフィグレーションコマンド aaa authentication login console および aaa authentication login で，RADIUS/TACACS+認証が設定されていないか確認してください（詳細は「2.2.3　RADIUS/TACACS+を利用したログイン認証ができない」を参照してください）。
6	ログイン後に通信ソフト	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

項番	障害内容	確認内容
	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	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。

2.2.2 リモート運用端末からログインできない

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

表 2-2　リモート運用端末との接続トラブルおよび対応

項番	現象	対処方法，または参照個所
1	リモート接続ができない。	次の手順で確認してください。 1. PC や WS から 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 アドレスを持つ端末を使用しているかを確認してください。また，コンフィグレーションコマンドアクセスリストで設定した IP アドレスに deny を指定していないかを確認してください（詳細は「コンフィグレーションガイド」を参照してください）。 2. ローカル認証でログインする場合は，装置に存在しないアカウントでログインしようとしていないか確認してください。 3. ログインできる最大ユーザ数を超えていないか確認してください（詳細は「コンフィグレーションガイド」を参照してください）。 なお，最大ユーザ数でログインしている状態でリモート運用端末から本装置への到達性が失われ，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。 4. 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「コンフィグレーションコマンドレファレンス」を参照してください）。 5. コンフィグレーションコマンド aaa authentication login で，RADIUS/TACACS+認証が設定されていないか確認してください（詳細は「2.2.3　RADIUS/TACACS+を利用したログイン認証ができない」を参照してください）。

項番	現象	対処方法，または参照個所
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，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。

2.2.3 RADIUS/TACACS+を利用したログイン認証ができない

RADIUS／TACACS+を利用したログイン認証ができない場合，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，「7.1.1　通信できない，または切断されている」を参照してください。また，コンフィグレーションで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かかわらず，telnet や ftp が失敗する場合は，コンフィグレーションで指定した複数の RADIUS サーバの中で，稼働中の RADIUS／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. 本装置にログインできない場合の対処方法
   設定ミスなどで本装置にログインできない場合は，コンソールからログインして修正してください。

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

RADIUS／TACACS+／ローカル認証は成功して本装置にログインできたが，コマンド承認が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。また，ローカルコマンド承認を使用している場合は，コンフィグレーションどおりにコマンドリストが設定されていることを確認してください。
2. サーバ設定およびコンフィグレーションの確認
   RADIUS／TACACS+サーバ側で，本装置のコマンド承認に関する設定が正しいことを確認してください。特に RADIUS の場合はベンダー固有属性の設定，TACACS+の場合は Service と属性名などに注意してください。また，ローカルコマンド承認を使用している場合は，コンフィグレーションの設定が正しいことを確認してください。RADIUS／TACACS+／ローカル（コンフィグレーション）の設定については，「コンフィグレーションガイド」を参照してください。

   コマンドリスト記述時の注意

   本装置のコマンド承認用のコマンドリストを記述する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. コマンドがすべて制限された場合の対処方法
   設定ミスなどでコマンドがすべて制限された場合は，コンソールからログインして修正してください。

2.3 SSH のトラブル

2.3.1 本装置に対して SSH で接続できない

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

(1) リモート接続経路の確立を確認する

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

(2) SSH サーバのコンフィグレーションを確認する

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

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

(3) 本装置に登録したユーザ公開鍵が正しいか確認する

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

図 2-3　本装置でユーザ公開鍵を確認する例

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


(config)#
```

1.　正しいユーザ名で，正しい公開鍵が登録されているかどうかを確認します。

(4) ログインアカウントのパスワードが設定済みか確認する

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

(5) ログインユーザ数を確認する

本装置にログインできる最大ユーザ数を超えてログインしようとして，次の図に示す運用ログが出力されていないかを，show logging コマンドで確認してください。

図 2-4　本装置で最大ログイン数を超えている例

```
> show logging
EVT 04/13 18:03:54 E3 ACCESS 00000003 0207:000000000000 Login refused for too many users logged
in.
```

(6) 本装置に対して不正なアクセスがないか確認する

本装置の SSH サーバ機能では不正アクセスを防止するために，ログインユーザ数の制限のほかに，ログインするまでの認証途中の段階でのアクセス数や，ログイン完了までの時間（2 分間）を制限しています。

したがって，show sessions コマンドで表示する本装置上のログインユーザ数が少ないのに SSH で接続できない場合は，接続していてもログインしていないセッションが残っていることが考えられます。次の点を確認してください。

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

   図 2-5　SSH サーバへ接続中のセッションが多いために接続が拒否された例

```
> show ssh logging
Date 20XX/04/14 19:00:00 UTC
20XX/04/14 18:50:04 sshd[662] fatal: Login refused for too many sessions.
20XX/04/14 18:49:50 sshd[638] fatal: Login refused for too many sessions.
20XX/04/14 18:49:00 sshd[670] fatal: Login refused for too many sessions.
```

2. 接続していてもログインしていない不正なセッションの接続元を調査して，リモートアクセスを制限するなどの対応をしてください。
   なお，接続していてもログインしていない不正なセッションは 2 分後には解放されて，再度 SSH でログインできるようになります。

2.3.2 本装置に対してリモートでコマンドを実行できない

(1) SSH クライアントの指定オプションを確認する

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

図 2-6　本装置に対するリモートからのコマンドの実行に失敗する例

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

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

図 2-7　本装置に対するリモートからのコマンドの実行に成功する例

```
client-host> ssh -t operator@myhost show ip arp
operator@myhost's password: ******
Date 20XX/04/17 16:59:12 UTC
Total: 2 entries
 IP Address       Linklayer Address  Netif            Expire     Type
 192.168.0.1      0000.0000.0001     VLAN0001         3h55m56s   arpa
 192.168.0.2      0000.0000.0002     VLAN0001         3h58m56s   arpa
Connection to myhost closed.
client-host>
```

(2) 実行するコマンドの入力モードを確認する

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

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

ください。

(3)　y/n の入力が必要なコマンドか確認する

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

2.3.3 本装置に対してセキュアコピーができない

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

図 2-8　本装置に対するセキュアコピーが失敗するクライアント側のトレースログ

```
Not tty allocation error.
```

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

2.3.4 公開鍵認証時のパスフレーズを忘れた

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

(1)　本装置の SSH コンフィグレーションからユーザ公開鍵を削除する

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

図 2-9　本装置の SSH コンフィグレーションからユーザ公開鍵を削除する例

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

(config)# no ip ssh authkey staff1 key1

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

(2)　SSH クライアント側端末のユーザ鍵ペアを削除する

SSH クライアント側の端末で，パスフレーズを忘れたユーザのユーザ鍵ペア（ユーザ公開鍵とユーザ秘密鍵）を削除して，登録も解除してください。再度，公開鍵認証を使用する場合は，使用する SSH クライア

ントでユーザ鍵ペアを再作成したあと，本装置の SSH コンフィグレーションで改めてユーザ公開鍵を登録してください。

2.3.5 接続時にホスト公開鍵変更の警告が表示される

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

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

(1)　本装置の装置管理者へ問い合わせる

次の内容について，装置管理者へ問い合わせて確認してください。

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

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

図 2-10　SSH での接続を中断する例

```
client-host> ssh operator@myhost
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
   :
（中略）
   :
Are you sure you want to continue connecting (yes/no)? no   <-1
Host key verification failed.
client-host>
```

1.　ここで「no」を入力して，接続しません。

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

(2)　ホスト公開鍵が変更された場合に再接続する

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

1. Fingerprint の事前確認
   あらかじめ本装置にログインして，show ssh hostkey コマンドで Fingerprint を確認します。コンソール接続など，ネットワーク経由以外の安全な方法で確認すると，より安全です。
2. Fingerprint をクライアントユーザへ通知
   確認した Fingerprint を，SSH クライアントユーザに通知します。郵送や電話など，ネットワーク経由以外の安全な方法で通知すると，より安全です。
3. Fingerprint を確認して SSH 接続
   クライアントでは，本装置の SSH サーバに対して SSH 接続したときに表示される Fingerprint が，手順 2.で通知されたものと同じであることを確認してから，接続します。

クライアントによっては，Fingerprint が HEX 形式で表示されるものと bubblebabble 形式で表示されるものがあります。また，SSHv1 では Fingerprint をサポートしていないものもあります。クライアントに合った形式で確認してください。

(3)　ユーザのホスト公開鍵データベースを登録または削除する

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

2.4 コンフィグレーションのトラブル

2.4.1 コンフィグレーションモードから装置管理者モードに戻れない

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

(1)　コンソールとの接続時

次の手順で，該当するユーザを強制的にログアウトさせてください。

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

   ［実行例］

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

   下線部が該当するユーザのログイン番号です。

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

   ［実行例］

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

(2)　リモート運用端末との接続時

いったんリモート運用端末を終了させたあと，再接続してください。

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

2.5 NTP の通信障害

2.5.1 NTP による時刻同期ができない

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

表 2-3　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	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。通信が可能な場合は項番 3 へ。
		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	本装置と NTP サーバとの時刻差を確認してください。	本装置と NTP サーバとの時刻差が 1000 秒以上ある場合には，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。

2.6 MC のトラブル

2.6.1 MC の状態が表示されない

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

表 2-4　"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	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 USB ポー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 2 へ。
2	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，USB ポー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。

2.6.2 MC へのアクセス時にエラーが発生する

MC へアクセスするコマンドの実行時に"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 2-5　"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	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 USB ポー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 2 へ。
2	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，USB ポー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。

2.6.3 MC にアクセスできない

MC へアクセスするコマンドの実行に失敗した場合は，次の表に従って確認してください。

表 2-6　"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	対象の MC が弊社推奨のものか確認してください。	弊社推奨の MC でない場合は，正しくアクセスできない可能性があります。 弊社推奨の MC である場合は，項番 2 へ。
2	本装置で MC がフォーマットされたか	弊社推奨の MC を他装置（PC など）でフォーマットした場合

項番	確認内容・コマンド	対応
	確認してください。	は，正しくアクセスできない可能性があります。本装置に MC を挿入して，format mc コマンドを実行して MC をフォーマットしてください。 本装置で MC をフォーマット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，USB ポー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。

2.7 SNMP の通信障害

2.7.1 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 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)#
```

2.7.2 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，「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。

2.7.3 SNMP マネージャでインフォームが受信できない

コンフィグレーションコマンド show snmp-server を実行して，本装置のコンフィグレーションに SNMP マネージャおよびインフォームに関する情報が設定されているか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 マネージャおよびインフォーム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 informs "event-monitor" snmp
 !
(config)#
```

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

3 ネットワークインタフェースのトラブルシュート

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

3.1 イーサネットの通信障害

3.1.1 イーサネットポートの接続ができない

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

(1) ポートの状態確認

1. ログの確認
   ログは，「メッセージ・ログレファレンス」を参照してください。
2. ポートの状態による原因の切り分け
   show interfaces コマンド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 3-1　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，「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ってポートを inactive 状態にした ・ストームコントロール機能によってポートを inactive 状態にした	・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，「8.3　IEEE802.3ah/UDLD 機能のトラブル」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

項番	ポート状態	原因	対応
			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。
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，「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	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 3-1 「ポートの動作状況確認」表示例

```
> show port statistics
20XX/03/23 12:00:00
Port Counts:48
Port  Name      Status  T/R   Unicast   Multicast   Broadcast     Discard
0/ 1  geth1/0/1  up     Tx          0           0           0           0
                        Rx          0           0           0           0
0/ 2  geth1/0/2  down   Tx          0           0           0           0
                        Rx          0           0           0           0
0/ 3  geth1/0/3  down   Tx          0           0           0           0
                        Rx          0           0           0           0
        :
>
```

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。

3.1.2 10BASE-T/100BASE-TX/1000BASE-T のトラブル

10BASE-T/100BASE-TX/1000BASE-T でトラブルが発生した場合は，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，「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 3-2 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	回線品質が低下してい	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。

項番	確認内容	原因	対応
	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	ます。	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 MDI/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，「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「10.1　回線のテスト」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 MDI/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，「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「10.1　回線のテスト」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。 ・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，「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	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。

項番	確認内容	原因	対応
		speed と duplex が相手装置と不一致です。	
		上記以外の場合。	オートネゴシエーションで特定の速度を使用したい場合は，オートネゴシエーションの回線速度を設定してください。詳細は，「コンフィグレーションガイド」を参照してください。
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。 ・HOL1 ・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。

3.1.3 1000BASE-X のトラブル

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，「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 3-3　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

項番	確認内容	原因	対応
			「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「10.1　回線のテスト」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。
			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「10.1　回線のテスト」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	1000BASE-BX などの 1 芯の光ファイバを使用している場合，相手側のトランシーバと組み合わせが合っているか確認してください。	トランシーバの組み合わせが不正です。	1000BASE-BX を使用する場合，トランシーバは U タイプと D タイプを対向して使用する必要があります。トランシーバの種別が正しいか確認してください。
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	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。

項番	確認内容	原因	対応
	ください。 ・HOL1 ・Tail_drop		

3.1.4 10GBASE-R のトラブル

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，「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 3-4　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。
			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「10.1　回線のテスト」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。

項番	確認内容	原因	対応
			光レベルが正しいか確認してください。光レベルは「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「10.1　回線のテスト」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。 ・HOL1 ・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。

3.1.5 PoE 使用時の障害対応

PoE 使用時に電力供給ができないなどの問題が発生した場合は，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 3-5　PoE 使用時の通信の障害解析方法

項番	確認内容・コマンド	対応
1	show power inline コマンドで該当ポートの Status 表示を確認してください。	・Status 表示が off の場合 電力を供給していません。項番 2 へ。 ・Status 表示が denied の場合 装置全体の電力供給不足が発生しています。項番 4 へ。 ・Status 表示が faulty の場合 接続された装置に電力を供給できない状態になっています。項番 5 へ。 ・Status 表示が inact の場合 運用コマンドで電力の供給を停止しています。項番 5 へ。 ・Status 表示が wait の場合 PoE 給電分散機能によって電力供給開始を待機しています。待機時間が終わるまでお待ちください
2	show power inline コマンドで該当ポートの Priority 表示を確認してください。	・Priority 表示が never の場合 コンフィグレーションコマンド power inline で never 以外の優先度を設定してください。 ・Priority 表示が never 以外の場合 項番 3 へ。
3	該当ポートにコンフィグレーションコマンド shutdown が設定されているか確	・設定済みの場合 コンフィグレーションコマンドで no shutdown を設定してくだ

項番	確認内容・コマンド	対応
	認してください。	さい。 ・未設定の場合 受電装置が接続されているか確認してください。
4	show power inline コマンドで Threshold(W)と Total Allocate(W)を確認してください。	Total Allocate(W)の数値が Threshold(W)より大きいため供給できなくなっています。装置全体の電力供給量，ポートの電力割り当て量，およびポートの消費電力を確認してコンフィグレーションで割り当て量を調整してください。
5	activate power inline コマンドを実行し，show power inline で該当ポートの Status 表示を確認してください。	・Status 表示が off の場合 受電装置が接続されているか確認してください。 ・Status 表示が on の場合 継続してご使用ください。 ・Status 表示が faulty 表示 受電装置または接続ケーブルに問題がある可能性があります。項番 6 へ。
6	show logging コマンドを実行しログの有無を確認してください。	受電装置または接続ケーブルに問題がある可能性があります。 ・「Supplying power was stopped by the overload detection.」を表示した場合 オーバロードを検出したため，電力を供給できなくなっています。 受電装置または接続ケーブルを確認してください。回復しない場合は，ケーブル長，およびケーブル種別を「ハードウェア取扱説明書」を確認して交換してください。 また，PoE 電力供給が可能な装置同士を接続している場合，コンフィグレーションコマンド power inline で該当ポートの PoE 機能を無効にしてください。 ・「Supplying power was stopped by the thermal shutdown.」を表示した場合 PoE コントローラの温度異常を検出し，電力の供給を停止しました。 装置の設置環境を見直し，再度接続してください。回復しない場合，受電装置または接続ケーブルを確認してください。 ・「Supplying power was stopped by the PD disorder」を表示した場合 受電装置の障害を検出したため，電力の供給を停止しました。 受電装置または接続ケーブルを確認してください。

3.2 リンクアグリゲーション使用時の通信障害

リンクアグリゲーション使用時に通信ができない，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 3-6　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。
		リンクアグリゲーションのモードが一致している場合，各ポートの LACP 開始方法が両方とも passive になっていないか確認してください。両方とも passive になっていた場合，どちらか一方を active に変更してください。
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。チャネルグループ内の全ポートが Down の場合，チャネルグループが Down します。 Down ポートは Reason の表示によって以下を行ってください。 ・CH Disabled チャネルグループが 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。「3.1　イーサネットの通信障害」を参照してください。 ・Port Speed Unmatch チャネル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チャネルグループ内の全ポートの速度が一致するようにしてください。 ・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。 ・Waiting Partner Synchronization ポートアグリゲーション条件チェックを完了し接続ポートの同期待ちとなって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の確認，および設定の確認をしてください。 ・Partner System ID Unmatch 接続ポートから受信した Partner System ID がグループの Partner System ID と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相手装置の運用状態の確認，配線の確認をしてください。 ・LACPDU Expired 接続ポートからの LACPDU 有効時刻を超過したため，該当ポートが縮退状態となっています。show channel-group statistics コマンドで lacp パラメータを指定し，LACPDU の統計情報を確認してください。また相手装置の運用状態の確認をしてください。

項番	確認内容・コマンド	対応
		・Partner Key Unmatch 接続ポートから受信した Key がグループの Partner Key が不一致のため縮退状態となっています。縮退を回避する場合は相手装置の運用状態の確認，配線の確認をしてください。 ・Partner Aggregation Individual 接続ポートからリンクアグリゲーション不可を受信したため縮退状態となっています。縮退を回避する場合は相手装置の運用状態の確認，および設定の確認をしてください。 ・Partner Synchronization OUT_OF_SYNC 接続ポートから同期不可を受信したため縮退状態となっています（本装置でコンフィグレーションを変更した場合や相手装置で回線を inactive 状態にした場合に発生します）。 ・Port Moved 接続されていたポートがほかのポートと接続しました。配線の確認をしてください。 ・Operation of Detach Port Limit 離脱ポート数制限機能が動作したため，チャネルグループが Down しています。

4 レイヤ２スイッチングのトラブルシュート

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

4.1 VLAN の通信障害

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。
- トランクポートに MAC 認証を設定している VLAN と，設定していない VLAN を混在して設定していないか。

(b) プロトコル VLAN の場合の確認

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

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

(c) MAC VLAN の場合の確認

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

  ［登録元機能］

  static：コンフィグレーションによって設定された MAC アドレスです。

  macauth：MAC 認証によって設定された MAC アドレスです。

  ```
  > show vlan mac-vlan
        :
  VLAN ID:100     MAC Counts:4
      0012.e200.0001 (static)         0012.e200.0002 (static)
      0012.e200.0003 (static)         0012.e200.0004 (macauth)
  ```

- show vlan mac-vlan コマンドを実行して，レイヤ 2 認証機能とコンフィグレーションで同じ MAC アドレスを異なる VLAN に設定していないことを確認してください。*（アスタリスク）が表示されている MAC アドレスは，コンフィグレーションで同じ MAC アドレスが設定され，無効になっていることを示します。

  ```
  > show vlan mac-vlan
  ```

```
        :
VLAN ID:500     MAC Counts:4
    0012.e200.aa01 (static)         0012.e200.aa02 (static)
    0012.e200.aa03 (static)         0012.e200.aa04 (macauth)
VLAN ID:600     MAC Counts:1
  * 0012.e200.aa01 (macauth)
```

(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「3.1　イーサネットの通信障害」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。

dot1x：IEEE802.1X 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。

```
> show vlan detail
        :
VLAN ID:100   Type:Protocol based  Status:Up
        :
  Port Information
    1/0/1          Up   Forwarding      Untagged
    1/0/2          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
Date 20XX/10/29 11:33:50 UTC
MAC address        VLAN    Type     Port-list
0012.e22c.650c       10    Dynamic  1/0/1
0012.e22c.650b        1    Dynamic  1/0/2
        :
```

- 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】

「4.4　IGMP snooping の通信障害」および「4.5　MLD snooping の通信障害」を参照してください。

【Type 表示が Dot1x の場合】

「5.1　IEEE802.1X 使用時の通信障害」を参照してください。

【Type 表示が Macauth の場合】

「5.2　MAC 認証使用時の通信障害」を参照してください。

- 該当する MAC アドレスが表示されない場合はフラッディングされます。
  表示されないにもかか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)　フレーム廃棄の確認

フィルタまたは QoS によってフレームが廃棄されている可能性があります。確認方法と対応については，「10.2　パケット廃棄の確認」を参照してください。

4.2 スパニングツリーの通信障害

スパニングツリー機能を使用し，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 4-1　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。
		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。
		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。
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。	該当するポートがルートポートで，かつ BPDU 受信カウンタがカウントアップしている場合は項番 5 へ。
		該当するポートがルートポートで，かつ BPDU 受信カウンタがカウントアップしていない場合は，フィルタまたは QoS によって BPDU が廃棄されていないか確認してください。確認方法と対応については，「10.2　パケット廃棄の確認」を参照してください。 問題がない場合は，隣接装置を確認してください。
		該当するポートが指定ポートで，かつ BPDU 送信カウンタがカウントアップしている場合は項番 5 へ。
		該当するポートが指定ポートで，かつ BPDU 送信カウンタがカウントアップしていない場合は，「3　ネットワークインタフェースのトラブルシュート」を参照してください。
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，「コンフィグレーションガイド」を参照してください。

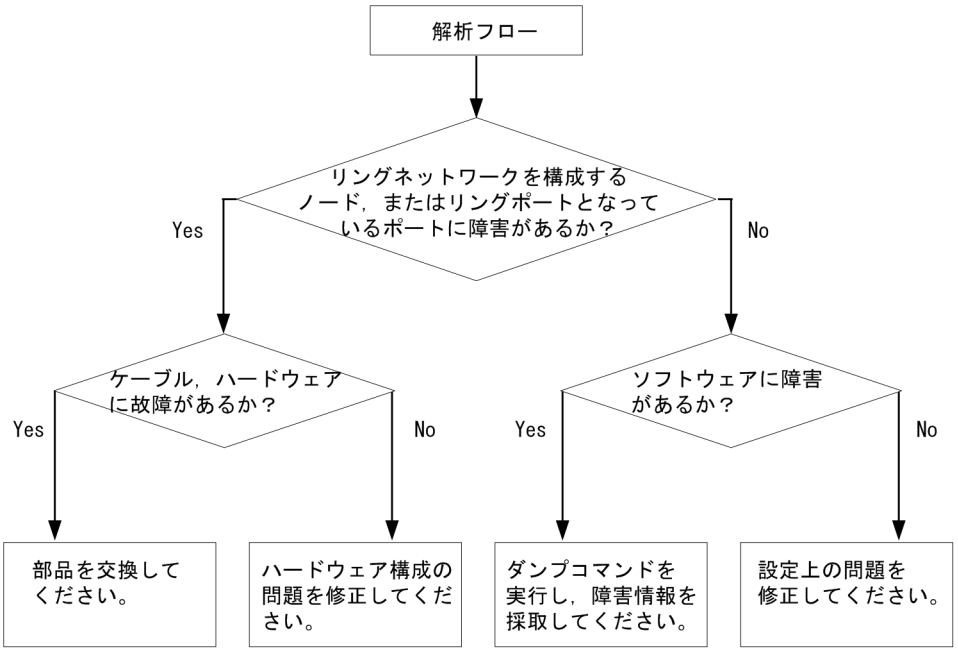
4.3 Ring Protocol の通信障害

この節では，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 4-1　解析フロー



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

表 4-2　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 2 へ。
		"Oper State"の内容に"-"が表示されている場合，Ring Protocol が動作するために必要なコンフィグレーションに設定されていないものがあります。コンフィグレーションを確認してください。
		"Oper State"の内容に"disable"が表示されている場合，Ring Protocol は無効となっています。コンフィグレーションを確認してください。
		"Oper State"の内容に"Not Operating"が表示されている場合，Ring Protocol が動作していません。コンフィグレーションに矛盾がないか，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"の内容がネットワーク構成どおりの動作モードになっている場合には，項番 3 へ。
		上記が異なる場合には，コンフィグレーションを確認してくだ

項番	確認内容・コマンド	対応
		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 4 へ。
		上記が異なる場合には，コンフィグレーションを確認してください。
4	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 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。 例：リングを構成する各装置で制御 VLAN ID が異なっている。
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 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。 例：リングを構成する各装置で VLAN グループに属している VLAN ID が異なっている。
6	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 7 へ。 また，多重障害監視機能を適用する構成の場合には項番 8 も確認してください。
		異常がある場合は，コンフィグレーションの確認も含め，その状態を復旧してください。
7	フィルタまたは QoS によって Ring Protocol で使用する制御フレームが廃棄されていないか確認してください。	確認方法と対応については，「10.2　パケット廃棄の確認」を参照してください。
8	多重障害監視機能を適用している場合は，show axrp detail コマンドを実行し，多重障害監視の監視モードを確認してください。	"transport-only"が設定されている場合は，項番 9 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。
9	show axrp detail コマンドを実行し，多重障害監視用 VLAN ID を確認してください。	"Control VLAN ID"がネットワーク構成どおりの多重障害監視用 VLAN ID になっている場合は，共有ノードの多重障害監視装置で多重障害監視，フレーム送信間隔のタイマ値，および多重障害監視フレームを受信しないで多重障害発生と判断するまでの保護時間のタイマ値を確認してください。
		上記が異なる場合には，コンフィグレーションを確認してください。

4.4 IGMP snooping の通信障害

IGMP snooping 使用時にマルチキャスト中継ができない場合は，次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。

(1)　ログの確認

show logging コマンドで物理的な障害のログがあるかを確認してください。ログの内容については，「メッセージ・ログレファレンス」を参照してください。

(2)　フレーム廃棄の確認

フィルタまたは QoS によって IGMP snooping で使用する制御フレームが廃棄されていないか確認してください。確認方法と対応については，「10.2　パケット廃棄の確認」を参照してください。

(3)　IGMP クエリアの確認

show igmp-snooping コマンドを実行して，IGMP クエリアが存在するか確認してください。IGMP クエリアが存在する場合，「IGMP querying system:」に IGMP クエリアの IP アドレスが表示されます。IGMP クエリアが存在しない場合(IP アドレスが表示されていない場合)，以下の対処を行ってください。

- 本装置を IGMP クエリアにする場合，VLAN に IP アドレスを設定し，当該 VLAN にコンフィグレーションコマンド ip igmp snooping querier を設定してください。
- 他装置が IGMP クエリアの場合，当該装置を同一 VLAN に接続してください。

(4)　マルチキャストデータ中継可能な装置の接続確認

同一 VLAN にマルチキャストデータ中継可能な装置を接続している場合，show igmp-snooping コマンドを実行して，「Mrouter-port:」に接続ポートが表示されているか確認してください。接続ポートが表示されていない場合，当該 VLAN にコンフィグレーションコマンド ip igmp snooping mrouter で接続ポートをマルチキャストルータポートに設定してください。

(5)　加入マルチキャストグループアドレスの確認

show igmp-snooping group コマンドを実行して，加入マルチキャストグループアドレスを確認してください。加入マルチキャストグループアドレスが表示されていない場合，受信者が正しく同一 VLAN に接続されているか確認してください。加入マルチキャストグループアドレスが表示されている場合，送信者が正しく同一 VLAN に接続されているか確認してください。

4.5 MLD snooping の通信障害

MLD snooping 使用時にマルチキャスト中継ができない場合は，次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。

(1) ログの確認

show logging コマンドで物理的な障害のログがあるかを確認してください。ログの内容については，「メッセージ・ログレファレンス」を参照してください。

(2) フレーム廃棄の確認

フィルタまたは QoS によって MLD snooping で使用する制御フレームが廃棄されていないか確認してください。確認方法と対応については，「10.2　パケット廃棄の確認」を参照してください。

(3) MLD クエリアの確認

show mld-snooping コマンドを実行して，MLD クエリアが存在するか確認してください。MLD クエリアが存在する場合，「MLD querying system:」に MLD クエリアの IP アドレスが表示されます。MLD クエリアが存在しない場合(IP アドレスが表示されていない場合)，以下の対処を行ってください。

- 本装置を MLD クエリアにする場合，VLAN に IP アドレスを設定し，当該 VLAN にコンフィグレーションコマンド ipv6 mld snooping querier を設定してください。
- 他装置が MLD クエリアの場合，当該装置を同一 VLAN に接続してください。

(4) マルチキャストデータ中継可能な装置の接続確認

同一 VLAN にマルチキャストデータ中継可能な装置を接続している場合，show mld-snooping コマンドを実行して，「Mrouter-port:」に接続ポートが表示されているか確認してください。接続ポートが表示されていない場合，当該 VLAN にコンフィグレーションコマンド ipv6 mld snooping mrouter で接続ポートをマルチキャストルータポートに設定してください。

(5) 加入マルチキャストグループアドレスの確認

show mld-snooping group コマンドを実行して，加入マルチキャストグループアドレスを確認してください。加入マルチキャストグループアドレスが表示されていない場合，受信者が正しく同一 VLAN に接続されているか確認してください。加入マルチキャストグループアドレスが表示されている場合，送信者が正しく同一 VLAN に接続されているか確認してください。

5 レイヤ 2 認証のトラブルシュート

この章では，レイヤ 2 認証で障害が発生した場合の対処について説明します。

5.1 IEEE802.1X 使用時の通信障害

5.1.1 IEEE802.1X 使用時に認証ができない

IEEE802.1X 使用時に認証ができない場合は，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 5-1　IEEE802.1X の認証障害解析方法

項番	確認内容・コマンド	対応
1	show dot1x コマンドを実行し，IEEE802.1X の動作状態を確認してください。	「Dot1x doesn't seem to be running」が表示された場合は，IEEE802.1X が停止しています。dot1x system-auth-control コマンドが設定されているかコンフィグレーションを確認してください。 「System 802.1X : Enable」が表示された場合は項番 2 へ。
2	show dot1x statistics コマンドを実行し，EAPOL のやりとりが行われていることを確認してください。	[EAPOL frames]の RxTotal が 0 の場合は端末から EAPOL が送信されていません。また，RxInvalid または RxLenErr が 0 でない場合は端末から不正な EAPOL を受信しています。不正な EAPOL を受信した場合はログを採取します。ログは show dotlx logging コマンドで閲覧できます。また，ログは「Invalid EAPOL frame received」メッセージと共に不正な EAPOL の内容となります。 上記に該当する場合は端末の Supplicant の設定を確認してください。 上記に該当しない場合は項番 3 へ。
3	show dot1x statistics コマンドを実行し，RADIUS サーバへの送信が行われていることを確認してください。	[EAP overRADIUS frames]の TxNoNakRsp が 0 の場合は RADIUS サーバへの送信が行われていません。以下について確認してください。 ・コンフィグレーションコマンドで aaa authentication dot1x default group radius が設定されているか確認してください。 ・コンフィグレーションコマンド radius-server host が正しく設定されているか確認してください。 上記に該当しない場合は項番 4 へ。
4	show dot1x statistics コマンドを実行し，RADIUS サーバからの受信が行われていることを確認してください。	[EAP overRADIUS frames]の RxTotal が 0 の場合は RADIUS サーバからのパケットを受信していません。以下について確認してください。 ・RADIUS サーバがリモートネットワークに収容されている場合はリモートネットワークへの経路が存在することを確認してください。 ・RADIUS サーバのポートが認証対象外となっていることを確認してください。 上記に該当しない場合は項番 5 へ。
5	show dot1x logging コマンドを実行し，RADIUS サーバとのやりとりを確認してください。	・「Invalid EAP over RADIUS frames received」がある場合 RADIUS サーバから不正なパケットを受信しています。RADIUS サーバが正常に動作しているか確認してください。 ・「Failed to connect to RADIUS server」がある場合，RADIUS サーバへの接続が失敗しています。RADIUS サーバが正常に動作しているか確認してください。 上記に該当しない場合は項番 6 へ。
6	show dot1x logging コマンドを実行し，認証が失敗していないか確認してください。	・「New Supplicant Auth Fail.」がある場合，以下の要因で認証が失敗しています。問題ないか確認してください。 (1) ユーザ ID またはパスワードが，認証サーバに登録されて

項番	確認内容・コマンド	対応
		いない。 (2) ユーザ ID またはパスワードの入力ミス。 ・「The number of supplicants on the switch is full」がある場合，装置の最大 supplicant 数を超えたため，認証が失敗しています。 ・「The number of supplicants on the interface is full」がある場合，インタフェース上の最大 supplicant 数を超えたため，認証が失敗しています。 ・「Failed to authenticate the supplicant because it could not be registered to mac-address-table.」がある場合，認証は成功したが，H/W の MAC アドレステーブル設定に失敗しています。「メッセージ・ログレファレンス」の該当個所を参照し，記載されている［対応］に従って対応してください。 上記に該当しない場合は，RADIUS サーバのログを参照して認証が失敗していないか確認してください。

5.1.2 IEEE802.1X 使用時の通信障害

IEEE802.1X が動作するポートで通信ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。該当しない場合は，「4　レイヤ 2 スイッチングのトラブルシュート」を参照してください。

表 5-2　IEEE802.1X の通信障害解析方法

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

5.2 MAC 認証使用時の通信障害

5.2.1 MAC 認証使用時のトラブル

MAC 認証使用時の障害は，次の表に従って原因を切り分けてください。

表 5-3　MAC 認証の障害解析方法

項番	確認内容・コマンド	対応
1	端末が通信できるかを確認してください。	・ローカル認証方式で認証できない場合は項番 2 へ。 ・RADIUS 認証方式で認証できない場合は項番 3 へ。 ・上記に該当しない場合は項番 5 へ。
2	show mac-authentication mac-address コマンドで MAC アドレスと VLAN ID が登録されているかを確認してください。	・MAC アドレスが登録されていない場合は，set mac-authentication mac-address コマンドで MAC アドレス，および VLAN ID を登録してください。 ・上記に該当しない場合は項番 5 へ。
3	show mac-authentication statistics コマンドで RADIUS サーバとの通信状態を確認してください。	・表示項目"[RADIUS frames]"の"TxTotal"の値が"0"の場合は，コンフィグレーションコマンド aaa authentication mac-authentication default group radius，radius-server host および mac-authentication radius-server host が正しく設定されているか確認してください。 ・dead interval 機能によって，RADIUS サーバが無応答となった状態から通信可能な状態に復旧しても，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間の間は RADIUS サーバへの照合は行われないため，認証エラーとなります。 この際，RADIUS サーバ無応答による認証失敗の時間が長すぎる場合は，コンフィグレーションコマンド authentication radius-server dead-interval の設定値を変更するか，または clear mac-authentication dead-interval-timer コマンドを実行してください。1 台目の RADIUS サーバを使用した認証動作が再開されます。 ・上記に該当しない場合は項番 4 へ。
4	RADIUS サーバに MAC アドレスおよびパスワードが登録されているかを確認してください。	・RADIUS サーバのユーザ ID として MAC アドレスが登録されていない場合は，RADIUS サーバに登録してください。 ・パスワードとして MAC アドレスを使用している場合は，ユーザ ID に設定した MAC アドレスと同一の値を設定してください。 ・パスワードとして，RADIUS サーバに共通の値を設定した場合は，コンフィグレーションコマンド mac-authentication password で設定したパスワードと一致しているかを確認してください。 ・上記に該当しない場合は項番 5 へ。
5	認証専用 IPv4 アクセスリストの設定を確認してください。	・認証前状態の端末から装置外に特定のパケット通信を行う場合，認証専用 IPv4 アクセスリストが設定されていることを確認してください。 また，通常のアクセスリストと認証専用 IPv4 アクセスリストの両方を設定した場合，認証専用 IPv4 アクセスリストに設定したフィルタ条件が通常のアクセスリストにも設定されていることを確認してください。 ・認証せずに通信できてしまう場合は，アクセスリストに，IP パケットの通信を許可するフィルタ条件（permit ip any など）が設定されていないことを確認してください。 ・認証対象ポートに設定した認証専用 IPv4 アクセスリストに deny ip any any のフィルタ条件を設定しても，受信した ARP パケットによって MAC 認証が行われます。該当ポートを MAC 認証の対象から外したい場合は，コンフィグレーションコマンド no mac-authentication port で MAC 認証の対象ポートから外してください。

項番	確認内容・コマンド	対応
		・上記に該当しない場合は項番 6 へ。
6	show mac-authentication statistics コマンドで MAC 認証の統計情報が表示されるかを確認してください。	・MAC 認証の統計情報が表示されない場合は項番 7 へ。 ・上記に該当しない場合は項番 8 へ。
7	コンフィグレーションコマンド mac-authentication system-auth-control が設定されているかを確認してください。	・コンフィグレーションコマンド mac-authentication system-auth-control が設定されていない場合は，設定してください。 ・コンフィグレーションコマンド mac-authentication port で認証対象ポートが正しく設定されているかを確認してください。 ・端末が接続されている認証対象ポートがリンクダウン，またはシャットダウンしていないことを確認してください。 ・上記に該当しない場合は項番 8 へ。
8	show mac-authentication logging コマンドを実行し，動作に問題がないかを確認してください。	・最大収容条件まで認証されている場合はほかの端末が認証解除するまでお待ちください。 ・上記に該当しない場合は MAC 認証のコンフィグレーションを確認してください。

5.2.2 MAC 認証のコンフィグレーション確認

MAC 認証に関係するコンフィグレーションは次の点を確認してください。

表 5-4　MAC 認証のコンフィグレーションの確認

項番	確認ポイント	確認内容
1	MAC 認証のコンフィグレーション設定	次のコンフィグレーションコマンドが正しく設定されていることを確認してください。 ・aaa accounting mac-authentication default start-stop group radius ・aaa authentication mac-authentication default group radius ・mac-authentication password ・mac-authentication port ・mac-authentication radius-server host ・mac-authentication static-vlan max-user ・mac-authentication system-auth-control
2	認証用アクセスフィルタの設定を確認	認証前状態の端末から装置外に通信するために必要なフィルタ条件が，コンフィグレーションコマンド authentication ip access-group および ip access-list extended で，正しく設定されていることを確認してください。

5.2.3 MAC 認証のアカウンティング確認

MAC 認証のアカウンティングに関しては次の点を確認してください。

表 5-5　MAC 認証のアカウンティングの確認

項番	確認ポイント	確認内容
1	認証結果のアカウントが正しく記録されているかの確認	・show mac-authentication login に認証状態が表示されていない場合は「表 5-3　MAC 認証の障害解析方法」を実施してください。 ・アカウンティングサーバに記録されていない場合は項番 2 へ。 ・syslog サーバに記録されていない場合は項番 3 へ。
2	show mac-authentication	・表示項目"[Account frames]"の"TxTotal"の値が"0"の場合は，コンフィグレー

項番	確認ポイント	確認内容
	statistics コマンドでのアカウンティングサーバとの通信状態の確認	ションコマンド aaa accounting mac-authentication default start-stop group radius，radius-server host，または mac-authentication radius-server host が正しく設定されているか確認してください。 ・上記に該当しない場合は MAC 認証のコンフィグレーションを確認してください。
3	syslog サーバの設定の確認	次のコンフィグレーションコマンドが正しく設定されていることを確認してください。 ・logging host で syslog サーバが設定されていることを確認してください。 ・logging event-kind でイベント種別に aut が設定されていることを確認してください。 ・mac-authentication logging enable が設定されていることを確認してください。

6 高信頼性機能のトラブルシュート

この章では，高信頼性機能で障害が発生した場合の対処について説明します。

6.1 アップリンク・リダンダントの通信障害

6.1.1 アップリンク・リダンダント構成で通信ができない

アップリンク・リダンダント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 6-1　アップリンク・リダンダントの障害解析方法

項番	確認内容・コマンド	対応
1	show switchport-backup コマンドでプライマリポートとセカンダリポートが正しく Forwarding／Blocking になっていることを確認してください。	プライマリポートとセカンダリポートのどちらにも Forwarding が存在しない場合。 ・Blocking の場合は，アクティブポート固定機能が動作している可能性があります。show switchport-backup コマンドで，アクティブポート固定機能が動作していないか，確認してください。アクティブポート固定機能が動作中の場合，プライマリポートがリンクアップするまで待ってください。または，set switchport-backup active コマンドで，セカンダリポートをアクティブにしてください。 ・Down の場合は回線状態を確認してください。確認方法は「3.1　イーサネットの通信障害」を参照してください。
		Forwarding/Blocking に問題がない場合，項番 2 へ。
2	アップリンク・リダンダントの上位装置を確認してください。	上位装置がフラッシュ制御フレーム受信機能をサポートしていない場合，アップリンク・リダンダントを使用している装置で MAC アドレスアップデート機能が有効になっているか，確認してください。MAC アドレスアップデート機能が有効になっていない場合，または MAC アドレスアップデートフレームが受信できないネットワーク構成の場合，アップリンク・リダンダントによる切り替えおよび切り戻しが発生すると，上位装置では MAC アドレステーブルがエージングアウトするまで，通信が回復しないことがあります。このような場合は，しばらく待ってから再度通信の状態を確認してください。または，上位装置で，MAC アドレステーブルのクリアを実施してください。
		上位装置がフラッシュ制御フレーム受信機能をサポートしている場合，項番 3 へ。
3	フラッシュ制御フレームの送信先 VLAN の設定が正しいか確認してください。	show switchport-backup コマンドで，フラッシュ制御フレームの送信先 VLAN がコンフィグレーションで設定したとおりに表示されることを確認してください。 意図したとおり表示されない場合，コンフィグレーションの設定が正しくありません。コンフィグレーションで設定したフラッシュ制御フレームの送信先 VLAN と，プライマリポートおよびセカンダリポートに設定してある VLAN を確認してください。
		フラッシュ制御フレームの送信先 VLAN の設定が正しい場合，項番 4 へ。
4	フラッシュ制御フレームが上位装置で受信できているか確認してください。	上位装置でフラッシュ制御フレームを受信しているか，show logging コマンドで確認してください。受信していない場合，フラッシュ制御フレームを受信できる VLAN が設定されているか，確認してください。

7 IP 通信のトラブルシュート

この章では，IP ネットワーク上の通信で障害が発生した場合の対処について説明します。

7.1 IPv4 ネットワークの通信障害

7.1.1 通信できない，または切断されている

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

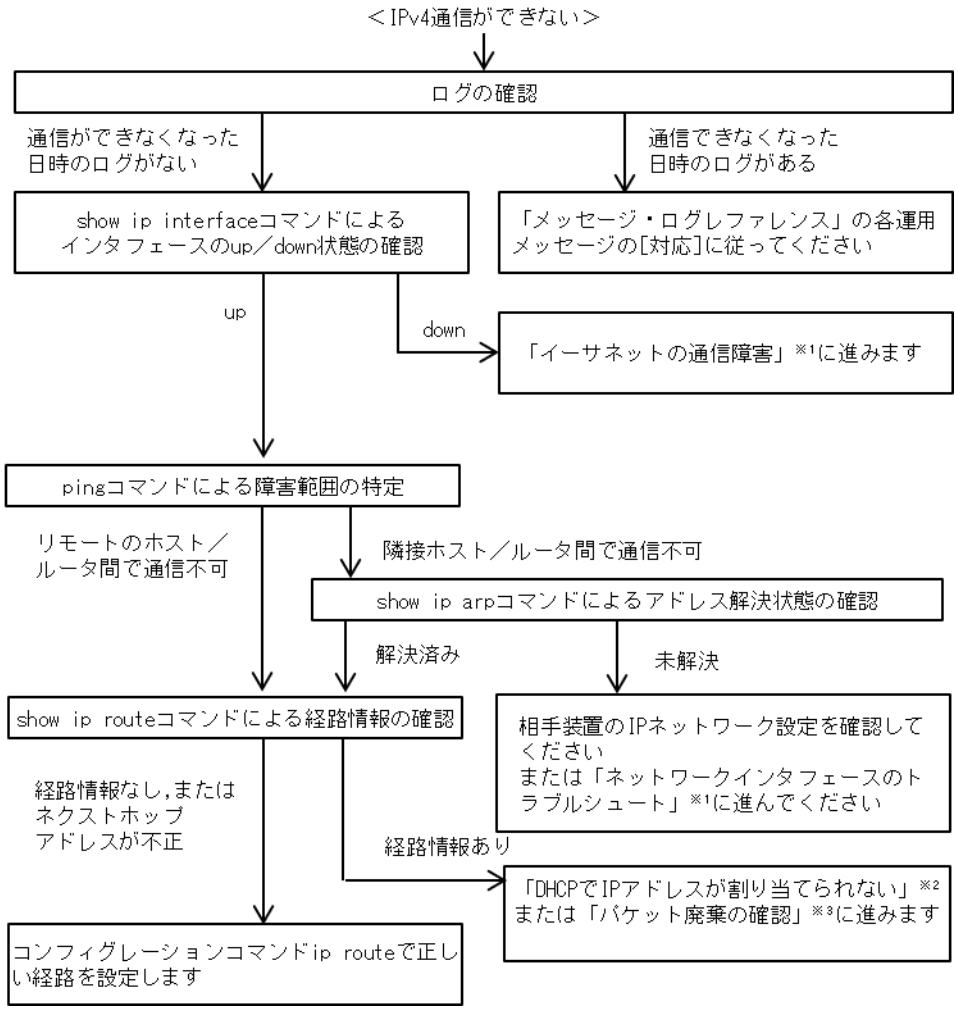
1. IP 通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

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 7-1　IPv4 通信ができない場合の障害解析手順



注※1　「3.1　イーサネットの通信障害」を参照してください。

注※2　「7.1.2　DHCP で IP アドレスが割り当てられない」を参照してください。

注※3 「10.2 パケット廃棄の確認」を参照してください。

(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，「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，「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，「3.1 イーサネットの通信障害」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，「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) 経路情報の確認」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)　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一致しているかを確認してください。
5. DHCP snooping を使用している場合はダイナミック ARP 検査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 DHCP snooping 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，「8.1　DHCP snooping のトラブル」を参照してください。

(6)　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かかわらず通信ができない場合や，IPv4 ユニキャスト通信で通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が保持する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，本装置が保持する経路情報を確認してください。
3. 本装置が保持する経路情報の中に，通信障害となっている宛先へ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，コンフィグレーションコマンド ip route で正しい経路を設定してください。
4. 本装置が保持する経路情報の中に，通信障害となっている宛先への経路情報がある場合は，通信不可の宛先への送受信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 サーバ機能
     「(7)　DHCP サーバ設定情報の確認」に進んでください。
   - フィルタ，QoS，または DHCP snooping
     「(8)　パケット廃棄の確認」に進んでください。

(7)　DHCP サーバ設定情報の確認

本装置の DHCP 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 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，「7.1.2　DHCP で IP アドレスが割り当てられない」を参照してください。

(8)　パケット廃棄の確認

フィルタまたは QoS によってパケットが廃棄されている可能性があります。確認方法と対応については，「10.2　パケット廃棄の確認」を参照してください。

また，DHCP snooping を使用している場合は端末フィルタ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 DHCP snooping 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，「8.1　DHCP snooping のトラブル」を参照してください。

7.1.2 DHCP で IP アドレスが割り当てられない

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，「(2)　運用メッセージおよびインタフェースの確認」を参照し，本装置で障害が発生しているか確認してください。本装置で障害が発生していない場合は，「(3)障害範囲の特定（本装置から実施する場合)」を参照してください。

(1)　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 DHCP 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（「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。
5. DHCP snooping を使用している場合は DHCP snooping 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 DHCP snooping 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，「8.1　DHCP snooping のトラブル」を参照してください。

(2)　運用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。本装置が表示する運用メッセージや 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「7.1.1　通信できない，または切断されている」を参照してください。

(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. show ip route コマンドを使用して経路情報を確認してください。DHCP リレーを経由している場合，クライアント向きの経路が正しく登録されていることを確認してください。また，ping コマンドなどで DHCP リレーとして動作しているルータなどとの疎通を確認してください。
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) パケット廃棄の確認

フィルタまたは QoS によってパケットが廃棄されている可能性があります。確認方法と対応については，「10.2　パケット廃棄の確認」を参照してください。

また，DHCP snooping を使用している場合は端末フィルタ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 DHCP snooping 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，「8.1　DHCP snooping のトラブル」を参照してください。

(5) レイヤ 2 ネットワークの確認

(1)から(4)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。「4　レイヤ 2 スイッチングのトラブルシュート」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。

7.1.3 DHCP サーバ機能の DynamicDNS 連携が動作しない

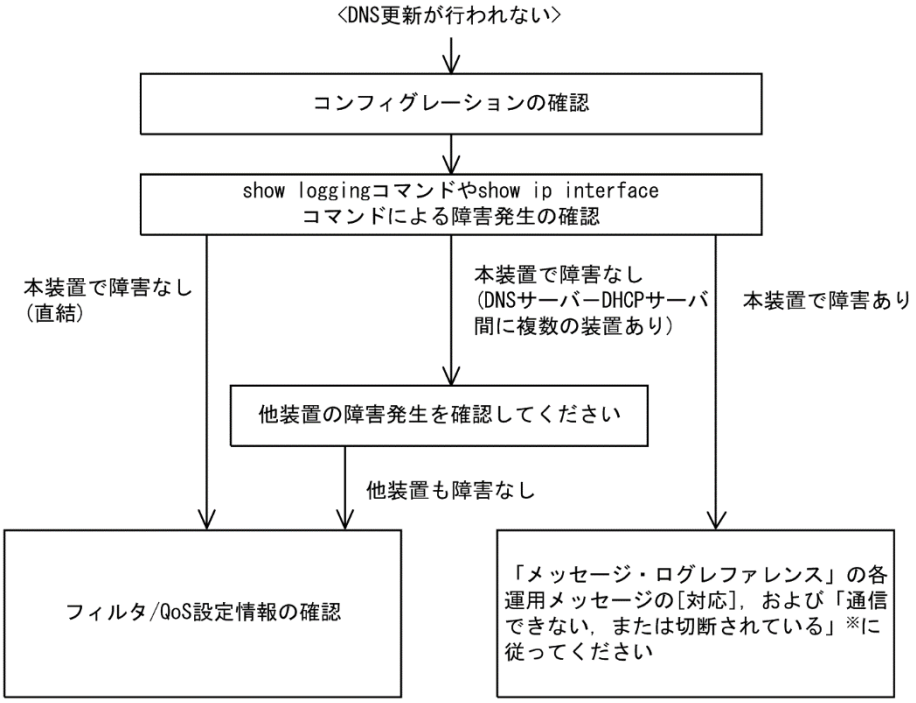
DHCP サーバの通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

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「(2) 時刻情報の確認」～「(5)　パケット廃棄の確認」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 7-2　DNS 連携時の DHCP サーバ障害解析手順



注※　「7.1.1　通信できない，または切断されている」を参照してください。

(1)　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（「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（「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（「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（「コンフィグレーションコマンドレファレンス」および「運用コマンドレファレンス」を参考にしてください)。

(2)　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「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。

(3)　運用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。本装置が表示する運用メッセージや 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「7.1.1　通信できない，または切断されている」を参照してください。

(4)　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. show ip route コマンドを使用して経路情報を確認してください。DNS サーバがリモートのネットワークに接続している場合，DNS サーバ向きの経路が正しく登録されていることを確認してください。
3. 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，「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。

(5)　パケット廃棄の確認

フィルタまたは QoS によってパケットが廃棄されている可能性があります。確認方法と対応については，「10.2　パケット廃棄の確認」を参照してください。

また，DHCP snooping を使用している場合は端末フィルタ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 DHCP snooping 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，「8.1　DHCP snooping のトラブル」を参照してください。

(6)　レイヤ 2 ネットワークの確認

(1)から(5)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。「4　レイヤ 2 スイッチングのトラブルシュート」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。

8 機能ごとのトラブルシュート

この章では，機能ごとにトラブルが発生した場合の対処方法を説明します。

8.1 DHCP snooping のトラブル

8.1.1 DHCP に関するトラブル

DHCP snooping 構成で DHCP の IP アドレス配布ができない場合は，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 8-1　DHCP snooping 構成で DHCP の IP アドレス配布ができない場合の障害解析方法

項番	確認内容	対応
1	show logging コマンドを実行して，運用ログにハードウェア障害が記録されていないかを確認してください。	運用ログにハードウェア障害が記録されていた場合は，装置を交換してください。
		上記に該当しない場合は項番 2 へ。
2	IP アドレスの新規配布ができないのか，IP アドレス更新だけができないのか確認してください。	IP アドレスが配布できない場合は，項番 3 へ。
		IP アドレスが更新できない場合は，項番 9 へ。
3	show ip dhcp snooping statistics コマンドを実行し，DHCP snooping の動作状況を確認してください。	DHCP snooping が有効な untrust ポートとして表示されるポートが，対象装置（IP アドレスが配布できない装置）に接続されているポートと一致している場合は，項番 4 へ。
		それ以外のポートに接続されている場合は，DHCP snooping の対象外となっています。 ネットワーク構成や DHCP サーバなどの設定を確認して，問題が見つからない場合は項番 10 へ。
4	クライアントとサーバ間がどの形態で接続されているかを確認してください。	本装置がレイヤ 2 スイッチとしてクライアントとサーバの間に接続されている場合は，項番 8 へ。
		本装置の DHCP サーバを使用している場合は，項番 5 へ。
		本装置とクライアントの間に DHCP リレーが存在する場合は，項番 6 へ。
		本装置とクライアントの間に Option82 を付与する装置がある場合は，項番 7 へ。
		上記の複数の条件に一致する場合は，該当する項番を順番に参照してください。
5	DHCP サーバ動作が問題ないことを確認してください。	DHCP サーバで IP アドレスが配布できる状態となっていることを確認してください。 問題がない場合は項番 8 へ。
6	DHCP リレー経由のパケットを中継する場合は，コンフィグレーションコマンド no ip dhcp snooping verify mac-address が設定されているか確認してください。	DHCP リレー経由の DHCP パケットはクライアントハードウェアアドレスと送信元 MAC アドレスが異なるため，パケットが廃棄されます。 該当パケットを中継する場合はコンフィグレーションコマンド no ip dhcp snooping verify mac-address を設定してください。
7	リレーエージェント情報オプションを含むパケットを中継する場合は，コンフィグレーションコマンド ip dhcp snooping information option allow-untrusted が設定されているか確認してください。	リレーエージェント情報オプション（Option82）を含むパケットはデフォルトでは廃棄されます。 該当パケットを中継する場合はコンフィグレーションコマンド ip dhcp snooping information option allow-untrusted を設定してください。
8	DHCP サーバを接続しているポートが trust ポートになっていることを確認してください。	untrust ポートからの DHCP サーバ応答パケットは廃棄されます。 対象とする DHCP サーバが正規のものである場合，接続されているポートにコンフィグレーションコマンド ip dhcp snooping

項番	確認内容	対応
		trust を設定してください。 なお，本装置の DHCP サーバを使用する場合は untrust ポートで問題ありません。また，本装置の DHCP リレーを使用する場合は，DHCP サーバが接続されている VLAN が DHCP snooping の対象外か，trust ポートになっている必要があります。
9	show ip dhcp snooping binding コマンドでバインディング情報を確認してください。	装置を再起動したあとに IP アドレス更新ができない場合は，バインディングデータベースの保存を確認してください。 「8.1.2　バインディングデータベースの保存に関するトラブル」を参照してください。
		バインディング情報で表示される該当（MAC アドレス／IP アドレスが一致する）エントリのポートや VLAN ID が異なる場合は，IP アドレスを取得したあとで接続ポートや VLAN の収容を変更した可能性があります。 現在のポートや VLAN で使用を続ける場合は，再度 IP アドレスを取得してください。
10	その他	上記のどれでも解決しない場合は，本書を参考に，装置で使用しているその他の機能を確認してください。

8.1.2 バインディングデータベースの保存に関するトラブル

装置再起動時などにバインディング情報が引き継げない場合は，バインディングデータベースの保存に関するトラブルが考えられます。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 8-2　バインディングデータベースの保存に関するトラブルの障害解析方法

項番	確認内容	対応
1	show mc コマンドまたは show flash コマンドで，flash または MC に十分な未使用容量があることを確認してください。	未使用容量がない場合は，不要なファイルを消すなどして未使用容量を確保してください。
		問題が見つからない場合，項番 2 へ。
2	バインディングデータベースの保存先を確認してください。	flash に保存する場合は，項番 4 へ。
		MC に保存する場合は，項番 3 へ。
3	ls mc-dir コマンドで，MC の保存ディレクトリが存在することを確認してください。	ディレクトリが存在しない場合は，mkdir コマンドでディレクトリを作成してください。
		問題が見つからない場合，項番 4 へ。
4	コンフィグレーションコマンド ip dhcp snooping database write-delay の設定と，show ip dhcp snooping binding コマンドでバインディングデータベースの最終保存時間を確認してください。	バインディング情報が更新されても指定した時間が経過するまでバインディングデータベースは保存されません。IP アドレス配布後に指定時間が経過するのを待って，バインディングデータベースの最終保存時間が更新されていることを確認してください。
		問題が見つからない場合，項番 5 へ。
5	DHCP クライアントに配布された IP アドレスのリース時間が，データベース保存時の待ち時間より長いことを確認してください。	リース時間の方が短い場合，バインディングデータベースを読み込む前に IP アドレスがリース切れとなる可能性があります。 コンフィグレーションコマンド ip dhcp snooping database write-delay で本装置のデータベース保存時の待ち時間を短くするか，DHCP サーバで IP アドレスのリース時間を長くしてください。
		問題が見つからない場合，項番 6 へ。
6	その他	バインディングデータベースを flash に保存したときは問題がなく，MC に保存したときにバインディング情報が引き継げない場

項番	確認内容	対応
		合は，MC を交換してください。 なお，長期間の運用を前提とする場合は，バインディングデータベースの保存先を MC にしてください。

8.1.3 ARP に関するトラブル

ARP パケットが廃棄されていると IPv4 通信ができなくなります。ARP パケットが廃棄される原因として，ダイナミック ARP 検査が考えられます。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 8-3　ダイナミック ARP 検査によって発生したトラブルの障害解析方法

項番	確認内容	対応
1	DHCP snooping 設定情報を確認してください。	「8.1.1　DHCP に関するトラブル」を参照して，DHCP snooping が正常に動作していることを確認してください。
		問題が見つからない場合，項番 2 へ。
2	show ip arp inspection statistics コマンドを実行して，ダイナミック ARP 検査の動作状況を確認してください。	ダイナミック ARP 検査が有効な untrust ポートとして表示されるポートが，IPv4 通信のできないポートと一致している場合は，項番 3 へ。
		それ以外のポートに接続されている場合は，ダイナミック ARP 検査の対象外となっています。ネットワーク構成や IPv4 通信ができない装置の設定を確認して問題が見つからない場合，項番 4 へ。
3	show ip dhcp snooping binding コマンドを実行して，通信できない装置に対するバインディング情報があるか確認してください。	バインディング情報がない場合，対象装置が固定 IP アドレスを持つ装置であれば，コンフィグレーションコマンド ip source binding を設定してください。また，DHCP によって IP アドレスを取得する装置であれば，IP アドレスを再取得してください。
4	その他	上記のどれでも解決しない場合は，本書を参考に，装置で使用しているその他の機能を確認してください。

8.1.4 DHCP，ARP 以外の通信に関するトラブル

端末フィルタを有効にした場合，バインディング情報にない装置からの DHCP/ARP 以外のすべてのパケットを廃棄します。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 8-4　端末フィルタによって発生したトラブルの障害解析方法

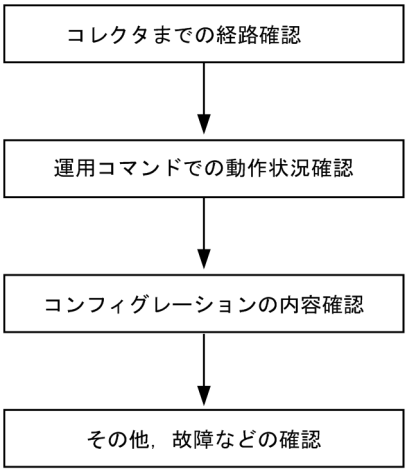
項番	確認内容	対応
1	DHCP snooping 設定情報を確認してください。	「8.1.1　DHCP に関するトラブル」を参照して，DHCP snooping が正常に動作していることを確認してください。
		問題が見つからない場合，項番 2 へ。
2	コンフィグレーションコマンド ip verify source が対象ポートに設定されているか確認してください。	ip verify source が設定されている場合はバインディング情報にない装置からのパケットを廃棄します。問題がない場合，項番 3 へ。
		ip verify source が設定されていない場合は，項番 4 へ。
3	show ip dhcp snooping binding コマンドを実行して，通信できない装置に対するバインディング情報があるか確認してください。	バインディング情報がない場合，対象装置が固定 IP アドレスを持つ装置であれば，コンフィグレーションコマンド ip source binding を設定してください。また，DHCP によって IP アドレスを取得する装置であれば，IP アドレスを再取得してください。

項番	確認内容	対応
4	その他	上記のどれでも解決しない場合は，本書を参考に，装置で使用しているその他の機能を確認してください。

8.2 sFlow 統計のトラブル

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 8-1　sFlow 統計機能のトラブルシューティングの流れ



8.2.1 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

「7.1.1　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，「7.1.1　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 8-2　show sflow コマンドの表示例

```
> show sflow
Date 20XX/12/09 11:03:00 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  1:17:49
sFlow agent data :
 sFlow service version  : 4
 CounterSample interval rate: 2 seconds
 Default configured rate: 1 per 10430000 packets
 Default actual rate    : 1 per 2097152 packets
 Configured sFlow ingress ports : 1/0/3
 Configured sFlow egress  ports : ----
 Received sFlow samples :      2023   Dropped sFlow samples         :          0
 Exported sFlow samples :      2023   Couldn't export sFlow samples :          0
 Overflow time of sFlow queue: 0 seconds
```

```
sFlow collector data :
 Collector IP address: 192.168.0.251  UDP: 6343  Source IP address: 192.168.0.9
  Send FlowSample UDP packets    :      1667  Send failed packets:         0
  Send CounterSample UDP packets:      1759  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 8-3　コンフィグレーションの表示例 1

```
(config)# show sflow
sflow destination 192.168.0.251   <-1
sflow extended-information-type url
sflow max-packet-size 1400
sflow polling-interval 2
sflow sample 10430000
sflow source 192.168.0.9
!
```

1.　コレクタの情報が正しく設定されていること

- 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 8-4　コンフィグレーションの表示例 2

```
(config)# show sflow
sflow destination 192.168.0.251
sflow extended-information-type url
sflow max-packet-size 1400
sflow polling-interval 2
sflow sample 10430000       <-1
sflow source 192.168.0.9
!
```

1.　適切なサンプリング間隔が設定されていること

図 8-5　運用コマンドの表示例

```
> show sflow
Date 20XX/12/09 11:03:00 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  1:17:49
sFlow agent data :
 sFlow service version  : 4
 CounterSample interval rate: 2 seconds
 Default configured rate: 1 per 10430000 packets
 Default actual rate    : 1 per 2097152 packets
 Configured sFlow ingress ports : 1/0/3
```

```
 Configured sFlow egress  ports : ----
 Received sFlow samples :      2023   Dropped sFlow samples         :           0
 Exported sFlow samples :      2023   Couldn't export sFlow samples :           0
 Overflow time of sFlow queue: 0 seconds
sFlow collector data :
 Collector IP address: 192.168.0.251  UDP: 6343  Source IP address: 192.168.0.9
  Send FlowSample UDP packets   :      1667  Send failed packets:         0
  Send CounterSample UDP packets:      1759  Send failed packets:         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 8-6　コンフィグレーションの表示例 3

```
(config)# show interface gigabitethernet 1/0/3
  interface gigabitethernet 1/0/3
  switchport mode trunk
  switchport trunk allowed vlan 20,2001,2251,2501,2751,3001-3004
                          :
  sflow forward ingress      <-1
!
```

1. ここに"sflow forward"が設定されていること

- フロー統計を実施する物理ポートに対して，フィルタまたは QoS によって sFlow パケットが廃棄されていないか確認してください。確認方法と対応については，「10.2　パケット廃棄の確認」を参照してください。
- "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 8-7　コンフィグレーションの表示例 4

```
(config)# show sflow
sflow destination 192.168.0.251
sflow extended-information-type url
sflow max-packet-size 1400
sflow polling-interval 2
sflow sample 10430000
sflow source 192.168.0.9      <-1
!
```

1. 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

(4) 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 8-8　ポート状態の表示例

```
> show interfaces gigabitethernet 1/0/3
Date 20XX/12/09 11:03:36 UTP
NIF0: -
Port3: active up  1000BASE-T full(auto)    0012.e23e.f43f
        Time-since-last-status-change:1:17:21
        Bandwidth:1000000kbps  Average out:1Mbps  Average in:861Mbps
```

```
        Peak out:4Mbps at 10:57:49  Peak in:1000Mbps at 09:47:16
        Output rate:      9600bps          15pps
        Input  rate:     865.8Mbps      850.0kpps
        Flow control send   :off
        Flow control receive:off
        TPID:8100
                              :
>
```

注　下線部が"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，「7.1.1　通信できない，または切断されている」を参照してください。

(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。

8.2.2 フローサンプルがコレクタに届かない

「8.2.1　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 8-9　ポート状態の表示例

```
> show interfaces gigabitethernet 1/0/3
Date 20XX/12/09 11:03:36 UTP
NIF0: -
Port3: active up  1000BASE-T full(auto)    0012.e23e.f43f
        Time-since-last-status-change:1:17:21
        Bandwidth:1000000kbps  Average out:1Mbps  Average in:861Mbps
        Peak out:4Mbps at 10:57:49  Peak in:1000Mbps at 09:47:16
        Output rate:      9600bps          15pps
        Input  rate:     865.8Mbps      850.0kpps
        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。

8.2.3 カウンタサンプルがコレクタに届かない

「8.2.1　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 8-10　コンフィグレーションの表示例

```
(config)# show sflow
sflow destination 192.168.0.251
sflow extended-information-type url
sflow max-packet-size 1400
sflow polling-interval 2       <-1
sflow sample 10430000
sflow source 192.168.0.9
!
```

1.　ここに 0 が設定されていないこと

8.3 IEEE802.3ah/UDLD 機能のトラブル

8.3.1 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 8-5　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	フィルタまたは QoS によって IEEE802.3ah/UDLD 機能で使用する制御フレームが廃棄されていないか確認してください。	確認方法と対応については，「10.2　パケット廃棄の確認」を参照してください。
		制御フレームが廃棄されていない場合は項番 7 へ。
7	回線のテストをしてください。	「10.1　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

8.4 隣接装置管理機能のトラブル

8.4.1 LLDP 機能で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 8-6　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「3.1　イーサネットの通信障害」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 によって LLDP の制御フレームが廃棄されていないか確認してください。確認方法と対応については，「10.2　パケット廃棄の確認」を参照してください。

9 障害情報取得方法

この章では，主に障害情報を取得するときの作業手順について説明します。

9.1 保守情報の採取

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

9.1.1 保守情報

保守情報を次の表に示します。

表 9-1　保守情報

項目	格納場所およびファイル名	備考
装置再起動時のダンプ情報ファイル	/dump/rmdump /dump/osdump /usr/var/hardware/ni00.000 /usr/var/hardware/reg_dump.gz /usr/var/hardware/sw_dump.gz /usr/var/hardware/tbl_dump.gz	・ftp コマンドでファイル転送をする際はバイナリモードで実施してください。 ・ファイル転送後は削除してください。
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/ni00.000 /usr/var/hardware/reg_dump.gz /usr/var/hardware/sw_dump.gz /usr/var/hardware/tbl_dump.gz	
ログ情報	運用コマンド show logging でログ情報を確認できます。	・CLI リダイレクト機能を利用しファイルへ出力することができます。 ・ftp コマンドでファイル転送をする際はアスキーモードで実施してください。
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	・ftp コマンドでファイル転送をする際はバイナリモードで実施してください。 ・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。
障害待避情報	/usr/var/core/*.core	・ftp コマンドでファイル転送をする際はバイナリモードで実施してください。 ・ファイル転送後は削除してください。

9.2 保守情報のファイル転送

この節では，ログ情報やダンプ情報をファイル転送する手順について説明します。

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

9.2.1 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 9-1　ダンプファイルのリモート運用端末へのファイル転送

```
> cd /dump                                          <-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 /usr/home/operator                          <-5
250 CMD command successful.
ftp> put rmdump                                    <-6
local: rmdump remote: rmdump
200 EPRT command successful.
150 Opening BINARY mode data connection for 'rmdump'.
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 9-2 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 /usr/home/operator                          <-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 9-3 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 /usr/home/operator                      <-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。

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

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

(1) show tech-support コマンドで情報を採取してファイル転送をする

図 9-4　保守情報のリモート運用端末へのファイル転送

```
> show tech-support ftp                                    <-1
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
Mon Dec 18 20:42:58 UTC 20XX
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

9.4 リモート運用端末の ftp コマンドによる情報採取とファイル転送

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

(1) show tech-support の情報を取得する

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

表 9-2　ftp コマンドで取得できる情報

get 指定ファイル名	取得情報
.show-tech	show tech-support の表示結果

図 9-5　show tech-support 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 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>
```

1.　クライアントから本装置に ftp 接続

2.　.show-tech ファイルをクライアントに転送（ファイル名は show-tech.txt を指定）

(2) ダンプ情報ファイルを取得する

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

表 9-3　ftp コマンドで取得できるファイル

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

図 9-6　リモート運用端末からのダンプファイルの取得

```
client-host> ftp 192.168.0.60                    <-1
```

```
Connected to 192.168.0.60.
220 192.168.0.60 FTP server ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary                                    <-2
200 Type set to I.
ftp> get .dump dump.tgz                        <-3
local: dump.tgz remote: .dump
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>
```

1. 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. .dump ファイルをクライアントに転送（ファイル名は dump.tgz を指定）

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。

9.5 MC への書き込み

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

9.5.1 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。

1. 書き込むための MC を装置に挿入する。
2. 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
```
3. show mc コマンドで空き容量を確認する。
```
>show mc
Date 20XX/11/15 15:50:40 UTC
MC  : Enabled
    Manufacture ID : 00000003
    16,735kB used
    106,224kB free
    122,959kB total
```
下線部が空き容量です。
4. cp コマンドでコピー元ファイルを tech-1.log というファイル名称で MC にコピーする。
```
> cp tech.log mc-file tech-1.log
```
5. MC にファイルが書き込めていることを確認する。
```
> ls mc-dir
 Volume in drive C has no label
 Volume Serial Number is C2E0-C0F0
Directory for C:/

tech-1   log    648467 2021-05-26  12:11
        1 file              648 467 bytes
                        837 599 232 bytes free
>
```

10 通信障害の解析

この章では，通信障害が発生した場合の対処について説明します。

10.1 回線のテスト

回線テストでは，テスト種別ごとに，テストフレームの折り返し位置が異なります。回線テスト種別ごとのフレームの折り返し位置を次の図に示します。

図 10-1　回線テスト種別ごとのフレームの折り返し位置

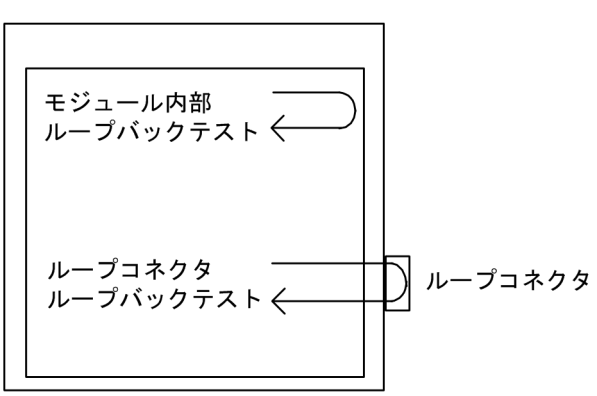


表 10-1　テスト種別と確認できる障害部位

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

10.1.1 モジュール内部ループバックテスト

モジュール内部ループバックテストは装置内でフレームを折り返し，障害の有無を確認します。このテストはすべての回線種別で実行できます。

テストの手順を次に示します。

1. inactivate コマンドでテスト対象のポートを inactive 状態にします。
2. test interfaces コマンドに internal パラメータを指定し実行します。その後，約 1 分間待ちます。
3. no test interfaces コマンドを実行し，表示される結果を確認します。
4. activate コマンドでポートを active 状態に戻します。

ポート番号 1 に対し，テストフレームの送信間隔を 2 秒に設定してテストした例を次の図に示します。

図 10-2　モジュール内部ループバックテストの例

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

> no test interfaces gigabitethernet 0/1
Date 20XX/03/10 00:20:21 UTC
Interface type            :100BASE-TX
Test count                :30
Send-OK                   :30           Send-NG                :0
Receive-OK                :30           Receive-NG             :0
Data compare error        :0            Out underrun           :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
> activate gigabitethernet 1/0/1
```

テストを実施後，次のことを確認してください。

”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，何らかの異常があります。「運用コマンドレファレンス」の，no test interfaces コマンドの表示内容を参照してください。

10.1.2 ループコネクタループバックテスト

ループコネクタループバックテストはループコネクタでフレームを折り返し，障害の有無を確認します。このテストはすべての回線種別で実行できます。

テストの手順を次に示します。

1. inactivate コマンドでテスト対象のポートを inactive 状態にします。
2. 対象ポートのケーブルを抜き，ループコネクタを接続します※。
3. test interfaces コマンドに connector パラメータを指定して実行します。その後，約 1 分間待ちます。
4. no test interfaces コマンドを実行し，表示される結果を確認します。
5. ループコネクタを外し，ケーブルを元に戻します。
6. activate コマンドでポートを active 状態に戻します。

注※

ループコネクタが未接続の場合，またはそのポートに対応したループコネクタが接続されていない場合，正しくテストができないので注意してください。

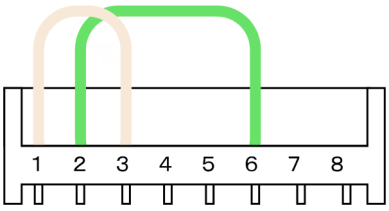
なお，テストの実行結果は「10.1.1　モジュール内部ループバックテスト」と同様に確認してください。

10.1.3 ループコネクタの配線仕様

(1)　10BASE-T/100BASE-TX 用ループコネクタ

次の図のように，ケーブルをコネクタに差込み，圧着工具で圧着します。

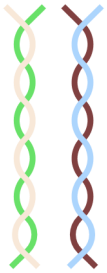
図 10-3　10BASE-T/100BASE-TX 用ループコネクタの配線仕様



(2)　10BASE-T/100BASE-TX/1000BASE-T 用ループコネクタ

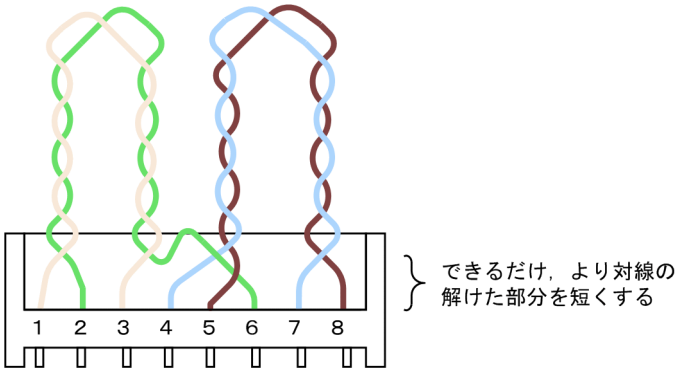
1. あらかじめ 6～7cm の 2 本のより対線を作ります。

図 10-4　より対線



2.　次の図のように，ケーブルをコネクタに差込み，圧着工具で圧着します。

図 10-5　10BASE-T/100BASE-TX/1000BASE-T 用ループコネクタの配線仕様



なお，1000BASE-T のコネクタを使用するループ動作は，規格で規定されていない独自動作のため回線テストでだけ利用可能です。

10.2 パケット廃棄の確認

10.2.1 フィルタによる廃棄を確認する

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

(1)　フィルタによるフレーム廃棄の確認方法

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

10.2.2 QoS による廃棄を確認する

本装置を使用しているネットワーク上で通信トラブルが発生する要因として，QoS 制御の廃棄制御，またはシェーパによってフレームが廃棄されている可能性が考えられます。QoS によるフレーム廃棄の確認方法を次に示します。

(1)　廃棄制御およびレガシーシェーパによるフレーム廃棄の確認方法

1. show qos queueing コマンドを実行して，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。
2. 1.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フレームを廃棄しています。
3. 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。

10.3 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 00003303 1000:XXXXXXXXXXXX Received many packets and loaded into the queue to CPU.”

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 00003304 1000:XXXXXXXXXXXX Processed the packets in the queue to CPU.”

CPU で処理するパケットの輻輳は，ネットワークトポロジーの変更などによって一時的に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 10-2　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 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 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 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。

11 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。

11.1 装置を再起動する

11.1.1 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。

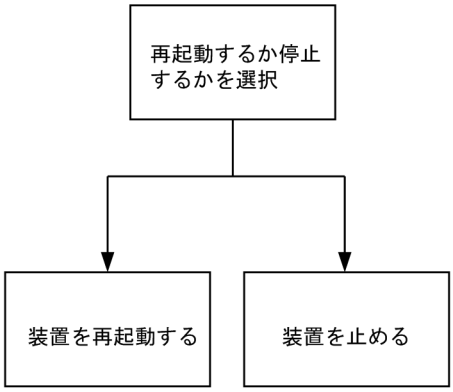
コマンドの入力形式，パラメータについては「運用コマンドレファレンス」を参照してください。

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 11-1　装置再起動・停止選択

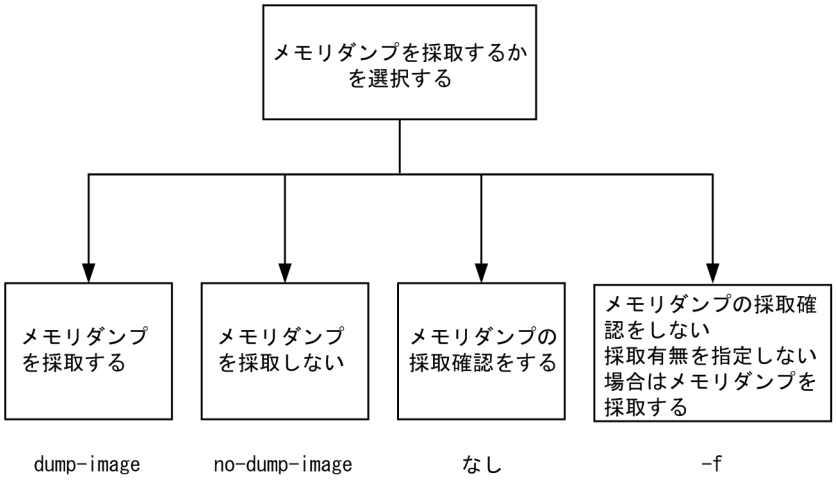


Step1 では，装置を再起動させるので，上記の図によりパラメータは選択しません。

Step2

次にダンプ採取するかどうかを選択します。

図 11-2　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 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 11-3　CPU メモリダンプ採取確認メッセージ