AX-Sensor 機能マニュアル

Ver. 1.7 対応

AX-NSM-S002-80

■対象製品
このマニュアルは，AX-Sensorについて記載しています。
必ず後述するマニュアルの読書手順に記載した他のマニュアルと併せてお読みください。

■輸出時の注意
本製品を輸出される場合には，外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。
なお，ご不明な場合は，弊社担当営業にお問い合わせください。

■商標一覧
Ethernet は，富士フイルムビジネスイノベーション株式会社の登録商標です。
イーサネットは，富士フイルムビジネスイノベーション株式会社の登録商標です。
その他，各会社名，各製品名は，各社の商標または登録商標です。

■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，安全上の説明を読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

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

■発行
2022 年 9 月（第 9 版）AX-NSM-S002-80

変更履歴

【Ver.1.7 対応版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
付録 A.2 SSH	• 規格番号 RFC4255，RFC4345 を削除しました。 • 規格番号 RFC6668，RFC8270，RFC8308，RFC8332，RFC8709，RFC8731 を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver.1.6 対応版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
3.1.2 リモート運用端末	• 表 3.1-3 本装置の ssh 詳細機能サポート一覧の共通鍵暗号方式とホスト認証から非推奨のアルゴリズムを削除しました。 • 表 3.1-3 本装置の ssh 詳細機能サポート一覧にホスト認証のアルゴリズムを新規追加しました。 • 表 3.1-3 本装置の ssh 詳細機能サポート一覧のホスト認証のアルゴリズムの記載順序を一部変更しました。
4.4.1 ライセンスの概要	• 初年度ライセンス，1 年延長ライセンス，永続ライセンスの有効期間に関するルールを追加しました。 • 表 4.4-1 AX-Sensor のライセンス一覧に AX-PA1630-01P と AX-PA1630-02P を追加しました。
4.4.3 ライセンスの削除方法	• 表 4.4-2 ライセンスの削除条件に AX-PA1630-01P と AX-NS-S02 を追加しました。
5.3.1 コンフィグレーション	• syslog 出力データのヘッダ部に付ける facility に関する注意事項を追加しました。
6.1.4.3 NetFlow 設定パラメータ	• 表 6.1-3 NetFlow Exporter 機能の設定パラメータ一覧のコンフィグレーション「flow-max-entry」と「expire-time」の説明を訂正しました。
6.1.4.13 TCP 遅延測定機能	• 再送に関連するカウンタの集計機能を追加しました。
6.1.4.14 HTTP 情報測定機能	• 本項を新規追加しました。
6.1.4.15 NetFlow キャッシュエージング機能	• 本項を新規追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver.1.5 対応版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
1.3.1 本装置のモデル	• 表 1.3-1 最大ポート数ごとの対応モデルに AX-Sensor-08TL モデルを追加しました。
1.3.2 装置の外観	• 図 1.3-1 に AX-Sensor-08TL モデルを追加しました。
1.3.3 ハードウェア	• 図 1.3-3 に AX-Sensor-08TL モデルを追加しました。
2.2.1 IP アドレスを設定できるインタフェースの最大数	• 表 2.2-1 図 1.3-3 に AX-Sensor-08TL モデルを追加しました。
2.2.2 IP アドレス最大設定数	• 表 2.2-3 に AX-Sensor-08TL モデルを追加しました。
2.2.3 使用可能回線数	• 表 2.2-5 使用可能回線数に AX-Sensor-08TL モデルを追加しました。

2.3.1 ポート収容条件	• 表 2.3-1 モニタポート上限数，表 2.3-2 センサ出力ポート上限数，表 2.3-3 マネジメントポート上限数に AX-Sensor-08TL モデルを追加しました。
4.4.1 ライセンスの概要	• 表 4.4-1 に AX-NS-S02 を追加しました。
6.1.4.1 フローの識別条件	• フロー識別子 EthernetType を追加しました。
6.1.4.3 NetFlow 設定パラメータ	• 表 6.1-3 に flow send-interval の項目を追加しました。
6.1.4.5 フロー識別条件の変更	• フロー識別子 EthernetType を追加しました。
6.1.4.11 IP アドレス集約機能	• IP アドレス集約機能の対象に IPv6 フローを追加しました。 • 注意事項から“IPv4 アドレスのみサポート対象”を削除しました。
6.1.4.13 TCP 遅延測定機能	• 本項を新規追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver.1.4 対応版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
1.3.4 搭載メモリ量	• 表 1.3-2 実装メモリ量と内蔵フラッシュメモリ量の誤記を訂正しました。
2.3.2 NetFlow Exporter 機能	• フロー条件に IPv6 フローを追加しました。
4.4.4 ライセンスの失効	• 本項を新規追加しました。
4.5.3 ログインユーザの初期化	• 本項を新規追加しました。
4.7.5 コンフィグレーションの初期化	• 本項を新規追加しました。
6.1.4.1 フローの識別条件	• フロー条件に IPv6 フローを追加しました。
6.1.4.2 NetFlow パケット形式	• フロー条件に IPv6 フローを追加しました。
6.1.4.5 フロー識別条件の変更	• フロー条件に IPv6 フローを追加しました。
6.1.4.8 expire-time の複数種別指定	• フロー条件に IPv6 フローを追加しました。
6.1.4.11 IP アドレス集約機能	• 本項を新規追加しました。
6.1.4.12 オクテット数補正	• 本項を新規追加しました。
6.2.2 コンフィグレーション設定例	• IP アドレス集約およびオクテット数補正の設定，VLAN Tag を識別する TPID 値の設定を追加しました。
7.1 装置の問題，障害発生時の対応	• (6)を新規に追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver.1.3 対応版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
4.10.1 ソフトウェアのアップデート	• バージョンダウン時における注意事項を追加しました。
5.7.1 コンフィグレーション	• system temperature-warning-level コマンドの設定例を追加しました。
5.7.2 オペレーション	• show environment temperature-logging コマンドの表示例を追加しました。
6.1.4.3 NetFlow 設定パラメータ	• expire-time の説明欄を更新しました。
6.1.4.7 NetFlow 情報量計測機能	• 本項を新規追加しました。

6.1.4.8 expire-time の複数種別指定 6.1.4.7	• 本項を新規追加しました。
6.1.4.9 コレクタ宛先ごとのフロー条件指定	• 本項を新規追加しました。
6.1.4.10 NetFlow 送信間隔の平準化調節機能	• 本項を新規追加しました。
6.2.2 コンフィグレーション設定例	• expire-time の複数種別指定およびコレクタ宛先ごとのフロー条件指定の設定を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver.1.2 対応版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
1.3.1 本装置のモデル	• 内容を一部変更しました。
2.2.3 使用可能回線数	• 内容を一部変更しました。
2.2.4 テーブルエントリ数	• ルーティングテーブルエントリのテーブル項目を追加しました。
2.3.1 ポート収容条件	• 内容を一部変更しました。
5.1 ネットワーク構成例	• 内容を一部変更しました。
5.5 スタティックルーティング	• 題目を変更しました。
5.5.1 コンフィグレーション	• 宛先プレフィックス指定の設定を追加しました。
6.1.1 モニタポート	• Deny-Filter 機能の内容を追加しました。
6.1.4.6 Deny-Filter 機能	• Deny-Filter 機能の説明を追加しました。
6.2.2 コンフィグレーション設定例	• Deny-Filter 機能の設定を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver.1.1 対応版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
2.1 ログインセキュリティ	• 最大ログイン数を変更しました。
4.11.1 LED と本装置の状態	• 内容を一部変更しました。
4.11.2 障害監視	• 内容を一部変更しました。
5.1 ネットワーク構成例	• 構成例の要素を追加しました。
5.4 SNMP	• 本節を追加しました。
6.1.4.1 フローの識別条件	• フローの識別条件の項目を追加しました。
6.1.4.5 フロー識別条件の変更	• 本項を追加しました。
6.2.2 コンフィグレーション設定例	• フロー識別条件の変更設定を追加しました。
付録 A.6 SNMP	• 本節を追加しました。
付録 A.7 MIB	• 本節を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【初版　Ver.1.0 対応版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
全体	• 初版発行

はじめに

■このマニュアルについて
このマニュアルはAX-Sensorに関する取り扱いについて示したものです。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時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。

■対象読者
このマニュアルは，AX-Sensorを利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。
また，次に示す知識を理解していることを前提としています。
・ ネットワークシステム管理の基礎的な知識

■マニュアルの読書手順

●初期導入時の基本的な設定について知りたい，
ハードウェアの設置条件，取扱方法を調べる

AX-Sensor
ハードウェア取扱説明書
(AX-NSM-H001)

●ラック搭載の手順について知りたい

MNTKIT-01
ハードウェア取扱説明書
(AXMK-H001)

●ソフトウェアの機能，
コンフィグレーションの設定，
運用方法について知りたい

AX-Sensor
機能マニュアル
(AX-NSM-S002)

●MIB について知りたい

AX-Sensor
MIB レファレンス
(AX-NSM-S005)

●コマンドの入力シンタックス，
パラメータ詳細や出力メッセージ
について知りたい

AX-Sensor
コマンド・ログレファレンス
(AX-NSM-S003)

目次

1 概要

この章では，本装置の概要について説明します。

1.1 本装置の概要

近年，キャリアネットワークやサービスプロバイダ，エンタープライズなどの比較的大規模なネットワークに限らず，SMB(Small and Medium Business)やSOHO(Small Office, Home Office)などにもIP電話，インターネット接続，企業の業務通信，携帯通信などが利用されるとともにIoT(Internet of Things)技術の発展により様々な機器がネットワークにつながり，通信サービスのトラフィック量増大が顕著で，ネットワークはより大容量化／高速化されていく傾向にあります。

また，これらのネットワーク運用において，トラフィックの監視やサイバー攻撃に対するセキュリティ対策，機器の故障などを検知することは必須であるが，事象や障害の発生後に対応する傾向にあります。

本装置はこのようなネットワーク運用支援のネットワークセンサシステムを構成する，センサ機能を有するアプライアンス製品です。

製品コンセプト

本装置はトラフィック可視化やサイレント故障などの異常検知，更にネットワークレイヤセキュリティを実現するために，リアルタイムにパケットを統計，通知する機能に特化した新たなアプライアンス製品です。AX-Collectorや他社のNetFlow Collectorと連携します。

本装置は次の機能を実現します。

・NetFlow Exporter機能により，リアルタイムにパケットを統計，通知することで連携するAX-Collectorや他社のNetFlow Collectorによりネットワーク状況の可視化を実現

1.2 本装置の特長

(1) NetFlow Exporter 機能

●柔軟なフロー識別条件

・標準の NetFlow v9 に加え，アラクサラ独自のフロー識別(AX-Flow)をサポート

(2) ミッションクリティカル対応のネットワークを実現する高信頼性

●高い装置品質

・厳選した部品と厳しい設計・検査基準による装置の高い信頼性

(3) 高性能・高密度でコンパクト・環境負荷低減

●優れたパフォーマンス

・キャリアネットワークやクラウド事業者，またはデータセンタ事業者，エンタープライズから公共文教などの幅広いネットワーク分野向け小型アプライアンス製品として適用

●コンパクト・高性能

・1U ハーフサイズのコンパクトな筐体に 1Gbps×4，あるいは 10Gbps のモニタ回線を収容

●RoHS 対応の環境負荷低減を実現

1.3 本装置の構成

本装置の構成について説明します。

1.3.1 本装置のモデル

本装置の最大ポート数ごとの対応モデルを次の表に示します。

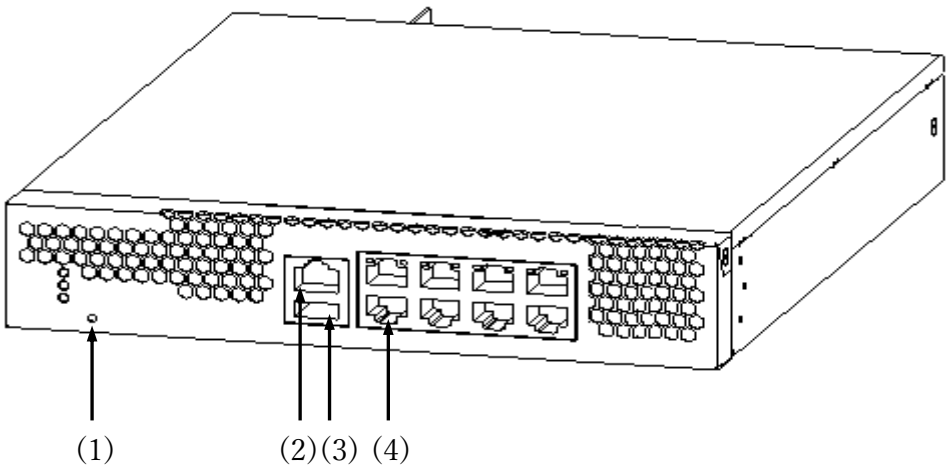
表 1.3-1 最大ポート数ごとの対応モデル

最大ポート数による分類		対応モデル
10BASE-T/100BASE-TX/1000BASE-T	8 ポート	AX-Sensor-08T AX-Sensor-08TL
10BASE-T/100BASE-TX/1000BASE-T 10GBASE-SR/LR	8 ポート 2 ポート	AX-Sensor-08T2X

1.3.2 装置の外観

装置外観を次の図に示します。ハードウェアの詳細については「ハードウェア取扱説明書」を参照ください。

図 1.3-1 AX-Sensor-08T, AX-Sensor-08TL モデル



(1) RESET スイッチ

(2) CONSOLE ポート

(3) USB ポート

(4) 10BASE-T/100BASE-TX/1000BASE-T イーサネットポート

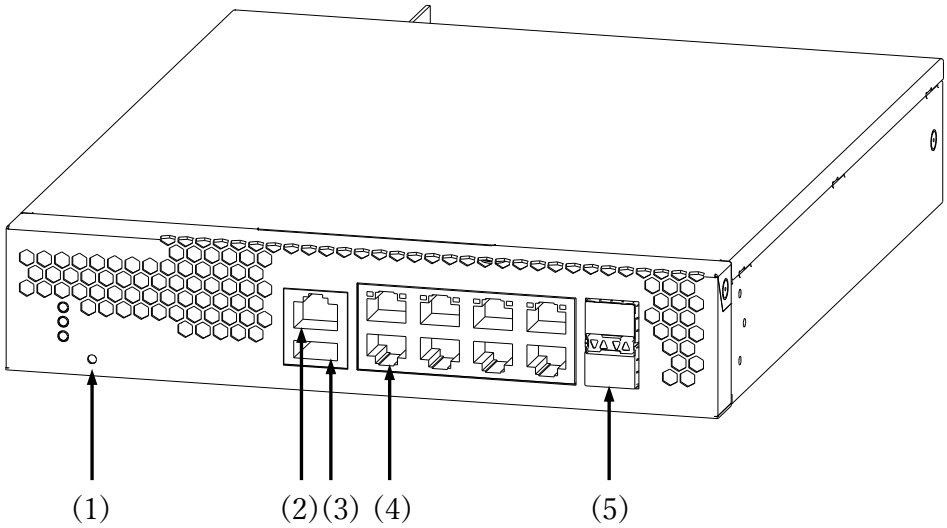


図 1.3-2 AX-Sensor-08T2X モデル

(1) RESET スイッチ

(2) CONSOLE ポート

(3) USB ポート

(4) 10BASE-T/100BASE-TX/1000BASE-T イーサネットポート

(5) SFP スロット

1.3.3 ハードウェア

本装置の各モデルは，統一したアーキテクチャで設計しています。
ハードウェア構成を次の図に示します。

図 1.3-3 ハードウェア構成(AX-Sensor-08T，AX-Sensor-08TL モデル)

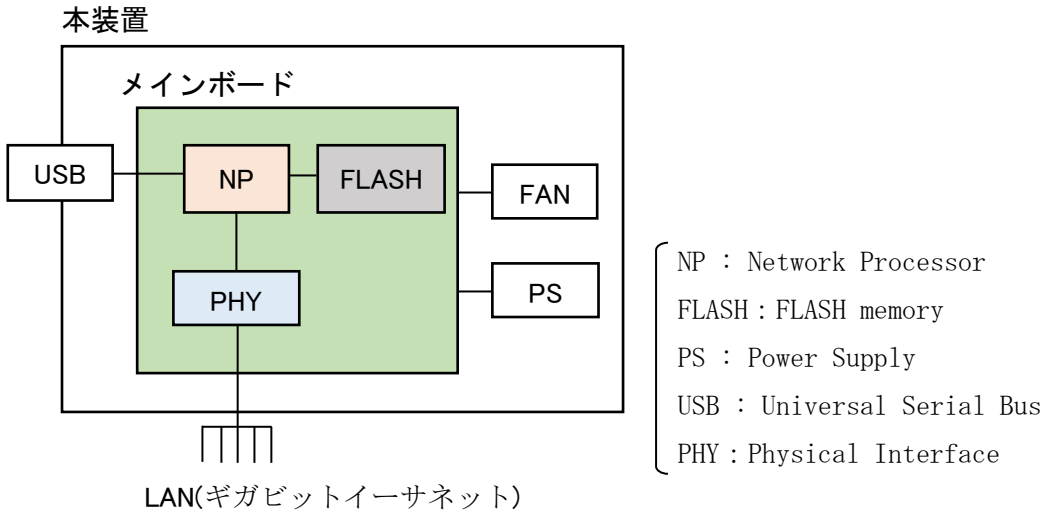
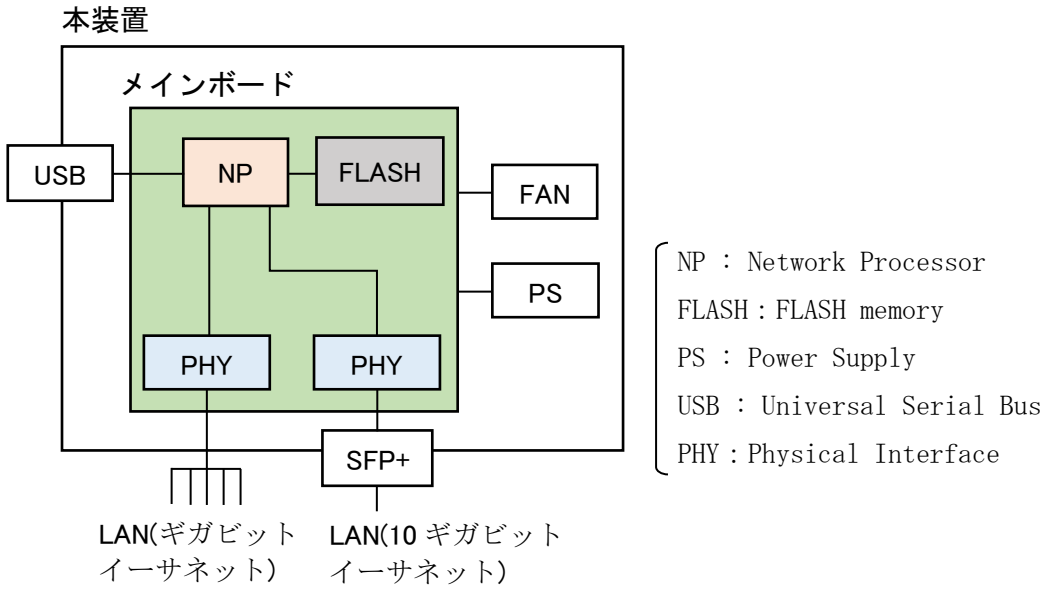


図 1.3-4 ハードウェア構成(AX-Sensor-08T2X モデル)



(1) 装置筐体

装置筐体には，メインボード，PS，FAN が含まれています。

(2) メインボード

メインボードは NP 部，FLASH 部，USB，PHY 部から構成されます。

・NP 部(Network Processor)

装置全体の管理，PHY 部の制御，各種プロトコル処理をソフトウェアで行います。
ソフトウェアは FLASH 部に搭載される内蔵フラッシュメモリに格納されます。

・FLASH 部(FLASH memory)
ソフトウェア／コンフィグレーションファイル／ログ情報が格納されます。

・USB(Universal Serial Bus)
USB ポートです。未使用ポート(未サポート)となります。

・PHY 部(Physical Interface)
各種メディア対応のインタフェース部です。

(3) PS(Power Supply)
PS は外部供給電源から本装置内で使用する直流電源を生成します。PS は本装置に内蔵されているため PS 故障時には装置の交換が必要です。

(4) FAN
本装置は装置内部を冷却するための FAN を装備します。FAN は本装置に内蔵されているため FAN 故障時には装置の交換が必要です。

1.3.4 搭載メモリ量

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

表 1.3-2 実装メモリ量と内蔵フラッシュメモリ量

項目	全モデル共通
実装メモリ量	8GB
内蔵フラッシュメモリ量	2GB

2 収容条件

この章では，収容条件について説明します。

2.1 ログインセキュリティ

リモート運用端末から本装置への最大ログイン数を表 2.1-1 に示します。

表 2.1-1 リモート装置端末から本装置への最大ログイン数

プロトコル	最大ログイン数
telnet および ssh	合計で 20

初期導入時には，ユーザ ID”operator”及び“admin”はパスワードなしの設定になっています。

パスワード設定コマンドにより，パスワードを設定してご使用ください。

注意事項

・本装置で許可するリモート接続は telnet および ssh のみとなります。ftp による接続は許可しません。

2.2 IPインタフェース

この節では，IPインタフェースについて説明します。

IPアドレスを設定したインタフェースをIPインタフェースと呼びます。
ここでは，IP アドレスを設定できるインタフェースの最大数，設定できるIP アドレスの最大数，通信できる相手装置の最大数などについて説明します。

2.2.1 IPアドレスを設定できるインタフェースの最大数

本装置でサポートするIPv4アドレスを設定可能なインタフェースの最大数を次の表に示します。

表 2.2-1 AX-Sensor-08T, AX-Sensor-08TL モデル

物理インタフェース	IPアドレス設定可能インタフェース最大数
10/100/1000BASE-T	8

表 2.2-2 AX-Sensor-08T2X モデル

物理インタフェース	IPアドレス設定可能インタフェース最大数
10/100/1000BASE-T	4
SFP スロット	1

2.2.2 IPアドレス最大設定数

コンフィグレーションで本装置に設定できる IPv4 アドレスの最大数を次の表に示します。

表 2.2-3 AX-Sensor-08T, AX-Sensor-08TL モデル

物理インタフェース	各物理インタフェースに設定可能な IPv4 アドレス最大数
10/100/1000BASE-T	1

表 2.2-4 AX-Sensor-08T2X モデル

物理インタフェース	各物理インタフェースに設定可能な IPv4 アドレス最大数
10/100/1000BASE-T	1
SFP スロット	1

注意事項

・各物理インタフェースに複数の IP アドレスを設定しないでください。

2.2.3 使用可能回線数

各モデルの使用可能回線数を次の表に示します。

表 2.2-5 使用可能回線数

ポートの種類	AX-Sensor-08T	AX-Sensor-08TL	AX-Sensor-08T2X
10BASE-T/100BASE-TX/1000BASE-T ポート	8(eth1～eth8)※1	8(eth1～eth8)※1	4(eth1～eth4)※1
10GBASE-SR/LR ポート	-	-	1(eth10)※1

(凡例) -:該当なし

注※1

カッコ内は使用可能の物理インタフェース名です。

2.2.4 テーブルエントリ数

本装置のテーブルエントリ数を示します。テーブルエントリとは，telnet などで本装置自体との通信をするネットワーク機器，および端末の情報を意味します。

(1) ARP エントリ数

IPv4 の場合，LAN では ARP によって，送信しようとするフレームの宛先アドレスに対応するハードウェアアドレスを決定します。本装置でサポートする ARP エントリの最大数を表 2.2-6 に示します。

表 2.2-6 本装置の ARP テーブルエントリの最大数

テーブル	エントリ最大数
ARP	128

(2) スタティックルーティングエントリ数

本装置でサポートするスタティックルーティングエントリの最大数を表 2.2-7 に示します。

表 2.2-7 本装置のスタティックルーティングテーブルエントリの最大数

テーブル	エントリ最大数
デフォルトゲートウェイ	1
宛先プレフィックス※1	8

注※1

1 経路あたりに設定できるネクストホップアドレスは 1 つです。

2.2.5 各種サーバ設定数

本装置にコンフィグレーションで設定できる各種サーバの設定数を次に示します。

(1) SYSLOG サーバ数

SYSLOG 出力先のサーバ設定を行える最大数を次に示します。

表 2.2-8 本装置の SYSLOG サーバ設定の最大数

サーバ	サーバ設定最大数
SYSLOG サーバ	4

(2) NTP サーバ数

NTP サーバ設定を行える最大数を次に示します。

表 2.2-9 本装置の NTP サーバ設定の最大数

サーバ	サーバ設定最大数
NTP サーバ	4

2.3 センサ機能

この節では，本装置でサポートするセンサ機能の収容条件について説明します。

2.3.1 ポート収容条件

センサ機能の物理インタフェースに設定する各ポート機能の収容条件を次の表に示します。

表 2.3-1 モニタポート上限数

モデル	インタフェース種別	モニタポート上限数
AX-Sensor-08T	10/100/1000BASE-T	4
AX-Sensor-08TL	10/100/1000BASE-T	2
AX-Sensor-08T2X	10/100/1000BASE-T	2
	10GBASE-SR/LR	1

注意事項

・AX-Sensor-08T2X モデルでは 4 ポートまでモニタポート設定が可能ですが，動作上限数は上記のとおりです。

・モニタポートはセンサ出力ポート，マネジメントポートとの併用はできません。

表 2.3-2 センサ出力ポート上限数

モデル	センサ出力ポート上限数
AX-Sensor-08T	1
AX-Sensor-08TL	1
AX-Sensor-08T2X	1

注意事項

・センサ出力ポートはマネジメントポートと併用できます。

表 2.3-3 マネジメントポート上限数

モデル	マネジメントポート上限数
AX-Sensor-08T	1
AX-Sensor-08TL	1
AX-Sensor-08T2X	1

注意事項

・マネジメントポートはセンサ出力ポートと併用できます。

2.3.2 NetFlow Exporter機能

NetFlow Exporter 機能ではモニタポートから受信したトラフィックからフローごとに集計を行います。フローの最大エントリ数を次の表に示します。

なお, NetFlow Exporter 機能の詳細は 6.1.4 節「NetFlow Exporter 機能」を参照ください。

表 2.3-4 フローの最大エントリ数

フロー条件	最大エントリ数(装置当り)
MAC フロー	1,000,000
IPv4 フロー	1,000,000
IPv6 フロー	1,000,000

注意事項

・複数のフロー条件を同時動作させる場合はエントリ数の合計が 1,000,000 となるようにコンフィグレーションを設定してください。

表 2.3-5 フロー情報の送信先上限数

項目	フロー情報の送信先上限数
宛先 IPv4 アドレス / UDP ポート番号の組み合わせ	8

3 運用端末による管理

この章では，運用端末による管理について説明します。

3.1 運用端末

本装置の運用にはコンソールまたはリモート運用端末が必要です。コンソールは RS-232C に接続する端末，リモート運用端末は IP ネットワーク経由で接続する端末です。コンソールやリモート運用端末といった本装置の運用管理を行う端末を運用端末と呼びます。

コンソール接続ではコンフィグレーションを設定していなくてもログインが可能となっていますので，初期導入時にはコンソールからログインし，初期設定を行ってください。

図 3.1-1　運用環境

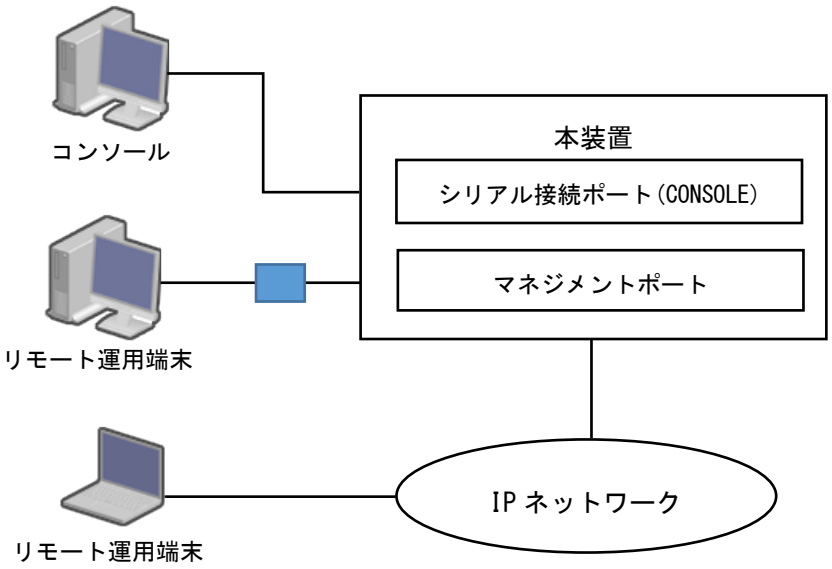


表 3.1-1 運用端末の条件

端末種別	接続形態	必要機能
コンソール	シリアル接続(RS-232C)	RS-232C(通信速度：9600)
リモート運用端末	マネジメントポート経由での TCP/IP 接続	TCP/IP(telnet，ssh)

注意事項

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

3.1.1 コンソール

コンソールは RS-232C に接続する端末で，一般的な通信端末，通信ソフトウェアが使用できます。コンソールが本装置と通信できるように，次の標準 VT-100 設定値（本装置のデフォルト設定値）が通信ソフトウェアに設定されていることを確認してください。

- **通信速度**：9600bit/s
- **データ長**：8 ビット
- **パリティビット**：なし
- **ストップビット**：1 ビット
- **フロー制御**：なし

注意事項

コンソールを使用する場合は次の点に注意してください。

- 本装置ではコンソール端末からログインする際に，自動的に VT-100 の制御文字を使用して画面サイズを取得・設定します。VT-100 に対応していないコンソール端末では，不正な文字列が表示されたり，最初の CLI プロンプトがずれて表示されたりして，画面サイズが取得・設定できません。また，ログインと同時にキー入力した場合，VT-100 の制御文字の表示結果が正常に取得できないため同様の現象となるので注意してください。この場合は，再度ログインし直してください。

3.1.2 リモート運用端末

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

注意事項

・本装置の ssh サーバはパスワードレスのログインをサポートしないため，ssh プロトコルでログインする場合は必ずログインアカウントにパスワードを設定してください。

本装置では，ssh のプロトコルとしてバージョン 2(SSHv2)のサーバ機能と一部のクライアント機能をサポートしています。

本装置でサポートする ssh の機能一覧を表 3.1-2 に示します。

表 3.1-2 本装置の ssh 機能サポート一覧

項番	機能名		実装	説明
1	ssh サーバ		○	ssh のサーバ機能です
2		セキュアリモートログイン	○	ssh のリモートログイン機能です
3		セキュアコピー	○	ssh を利用したファイルコピー機能です
4		セキュアファイル転送	×	ssh を利用したファイル転送機能です
5	ssh クライアント		○	ssh のクライアント機能です。
6		セキュアリモートログイン	×	ssh のリモートログイン機能です
7		セキュアコピー	△	ssh を利用したファイルコピー機能です 運用コマンド export dump， export conf，update でのみ使用可能です。
8		セキュアファイル転送	×	ssh を利用したファイル転送機能です
9	認証エージェント		×	認証エージェント機能です
10	ポート転送		×	ポート転送(TCP トンネリング)機能です
11	X11 プロトコル自動転送		×	X11 を自動転送する機能です
12	データ圧縮		×	通信のデータ圧縮をおこなう機能です
13	IPv6		×	IPv6 を用いて通信可能です

実装： ○ … サポート △…一部サポート × … 未サポート

本装置でサポートする ssh 詳細機能一覧を表 3.1-3 に示します。

表 3.1-3 本装置の ssh 詳細機能サポート一覧

項番	機能名				実装	説明
1	ユーザ認証機能				○	ユーザ認証を行う方法です
2		公開鍵認証	RSA	サーバ機能	×	RSA 公開鍵を用いたユーザ認証鍵をサーバ側に登録できます
3				クライアント機能	×	

4			DSA	サーバ機能	×	DSA 公開鍵を用いたユーザ認証鍵をサーバ側に登録できます
5				クライアント機能	×	
6			EDCSA	サーバ機能	×	EDCSA 公開鍵を用いたユーザ認証鍵をサーバ側に登録できます
7				クライアント機能	×	
8			ED25519	サーバ機能	×	ED25519 公開鍵を用いたユーザ認証鍵をサーバ側に登録できます
9				クライアント機能	×	
10			PGP		×	PGP 鍵を用いた認証です
11			CA 認証		×	CA 認証を用いた認証です
12		パスワード認証	ローカル	サーバ機能	○	ローカルパスワード認証です
13				クライアント機能	○	
14			RADIUS/TACACS+		×	RADIUS/TACACS+連携のパスワード認証です
15		ホストベース/RSARhost 認証			×	ホストベース認証です
16		チャレンジレスポンス認証			×	チャレンジレスポンスによる認証です
17	共通鍵暗号方式				○	通信路の暗号化に用います
18		暗号化アルゴリズム	サーバ機能	chacha20-poly1305@openssh.com	○	-
19				aes128-ctr	○	-
20				aes192-ctr	○	-
21				aes256-ctr	○	-
22				aes128-gcm@openssh.com	○	-
23				aes256-gcm@openssh.com	○	-
24				その他	×	上記以外
25			クライアント機能※1	chacha20-poly1305@openssh.com	○	-
26				aes128-ctr	○	-
27				aes192-ctr	○	-
28				aes256-ctr	○	-
29				aes128-gcm@openssh.com	○	-
30				aes256-gcm@openssh.com	○	-
31				その他	×	上記以外
32		鍵交換アルゴリズム	サーバ機能	curve25519-sha256	○	-
33				curve25519-sha256@libssh.org	○	-

34				ecdh-sha2-nistp256	○	-
35				ecdh-sha2-nistp384	○	-
36				ecdh-sha2-nistp521	○	-
37				diffie-hellman-group-exchange-sha256	○	-
38				diffie-hellman-group16-sha512	○	-
39				diffie-hellman-group18-sha512	○	-
40				diffie-hellman-group14-sha256	○	-
41				その他	×	上記以外
42			クライアント機能※1	curve25519-sha256	○	-
43				curve25519-sha256@libssh.org	○	-
44				ecdh-sha2-nistp256	○	-
45				ecdh-sha2-nistp384	○	-
46				ecdh-sha2-nistp521	○	-
47				diffie-hellman-group-exchange-sha256	○	-
48				diffie-hellman-group16-sha512	○	-
49				diffie-hellman-group18-sha512	○	-
50				diffie-hellman-group14-sha256	○	-
51				ext-info-c	○	-
52				その他	×	上記以外
53	ホスト認証				○	接続先ホストの正当性を検証します
54		公開鍵暗号	サーバ機能	rsa-sha2-512	○	-
55				rsa-sha2-256	○	-
56				ecdsa-sha2-nistp256	○	-
57				ssh-ed25519	○	-
58				その他	×	上記以外
59			クライアント機能※1	ssh-ed25519-cert-v01@openssh.com	○	-
60				ecdsa-sha2-nistp256-cert-v01@openssh.com	○	-
61				ecdsa-sha2-nistp384-cert-v01@openssh.com	○	-
62				ecdsa-sha2-nistp521-cert-v01@openssh.com	○	-
63				sk-ssh-ed25519-	○	-

				cert-v01@openssh.com		
64				sk-ecdsa-sha2-nistp256-cert-v01@openssh.com	○	-
65				rsa-sha2-512-cert-v01@openssh.com	○	-
66				rsa-sha2-256-cert-v01@openssh.com	○	-
67				ssh-ed25519	○	-
68				ecdsa-sha2-nistp256	○	-
69				ecdsa-sha2-nistp384	○	-
70				ecdsa-sha2-nistp521	○	-
71				sk-ssh-ed25519@openssh.com	○	-
72				sk-ecdsa-sha2-nistp256@openssh.com	○	-
73				rsa-sha2-512	○	-
74				rsa-sha2-256	○	-
75				その他	×	上記以外
76	メッセージ認証コード				○	データの改ざん防止に用います
77		認証方式	サーバ機能	umac-64-etm@openssh.com	○	-
78				umac-128-etm@openssh.com	○	-
79				hmac-sha2-256-etm@openssh.com	○	-
80				hmac-sha2-512-etm@openssh.com	○	-
81				hmac-sha1-etm@openssh.com	○	-
82				umac-64@openssh.com	○	-
83				umac-128@openssh.com	○	-
84				hmac-sha2-512	○	-
85				hmac-sha2-256	○	-
86				hmac-sha1	○	-
87				その他	×	上記以外
88			クライアント機能※1	umac-64-etm@openssh.com	○	-
89				umac-128-etm@openssh.com	○	-
90				hmac-sha2-256-etm@openssh.com	○	-
91				hmac-sha2-512-	○	-

				etm@openssh.com		
92				hmac-sha1-etm@openssh.com	○	-
93				umac-64@openssh.com	○	-
94				umac-128@openssh.com	○	-
95				hmac-sha2-512	○	-
96				hmac-sha2-256	○	-
97				hmac-sha1	○	-
98				その他	×	上記以外

実装： ○ … サポート △…一部サポート × … 未サポート

注※1

アルゴリズムの優先順位が高い項目から順に記載しています。

3.2 運用端末の接続形態

運用端末の接続形態ごとの特徴を表 3.2-1 に示します。

表 3.2-1 コンソールとリモート運用端末の運用管理での適用範囲の違い

運用機能	シリアル接続ポート	マネジメントポート
接続運用端末	コンソール	リモート運用端末
遠隔からのログイン	不可	可
本装置から運用端末へのログイン	不可	可
アクセス制御	なし	あり
コマンド入力	可	可
ファイル転送方式	なし	コマンド(ftp 等を利用)
IP 通信	不可	IPv4
コンフィグレーション設定	不要	必要

(1) シリアル接続ポート

シリアル接続ポートには運用端末としてコンソールを接続します。コンフィグレーションの設定なしに本ポートを介してログインできるので，初期導入時には本ポートからログインし，初期設定を行えます。

(2) マネジメントポート

マネジメントポートを介して，telnet，ssh で本装置へログインするためには，本装置のコンフィグレーションで IP アドレスおよびリモートアクセスの設定をする必要があります。

4 運用ガイド

この章では，本装置での運用について説明します。

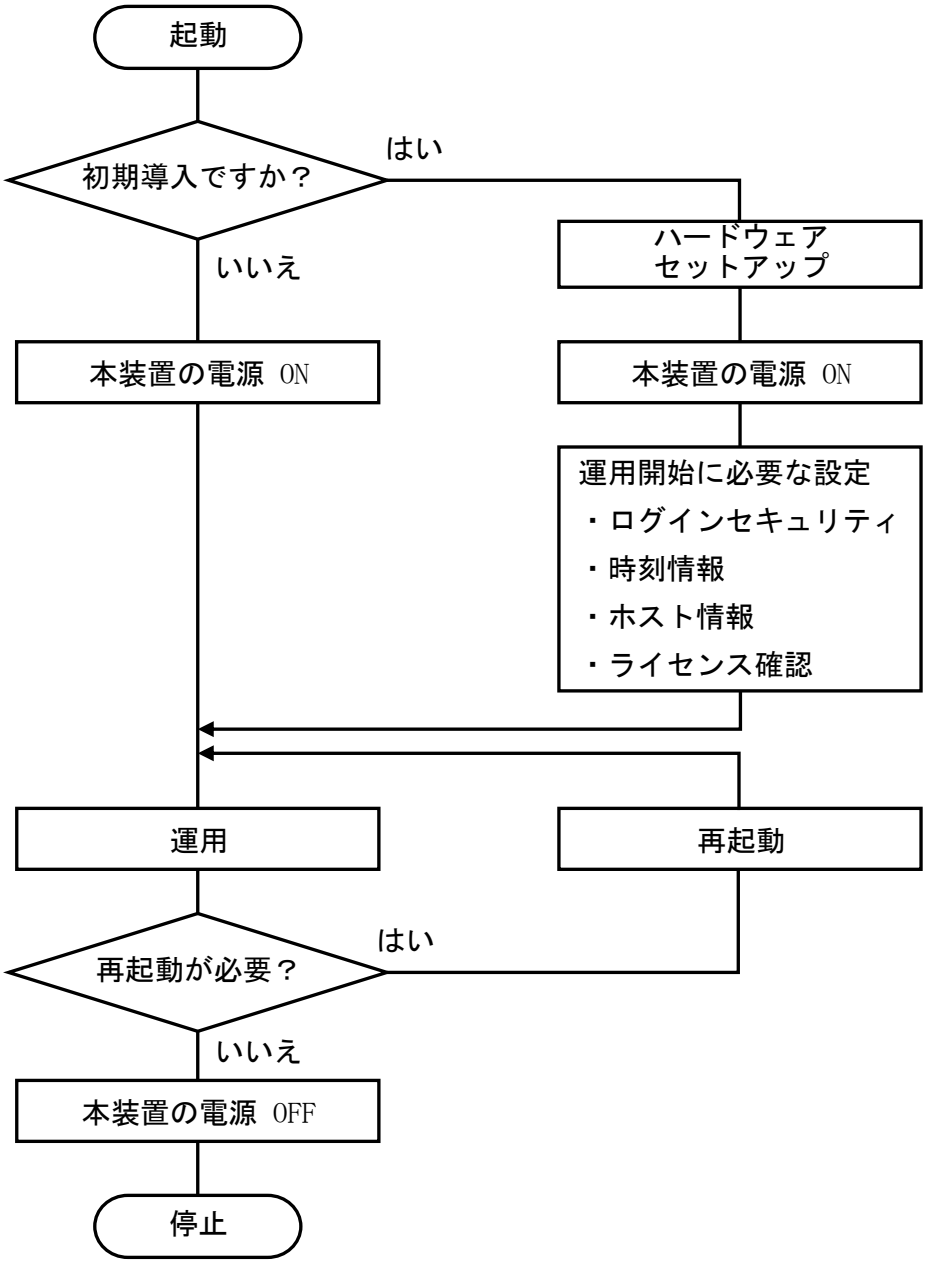
4.1 装置起動・停止

この節では，装置の起動と停止について説明します。

4.1.1 起動から停止までの概略

本装置の起動から停止までの概略フローを図 4.1-1 に示します。ハードウェアセットアップ(本装置の設置，電源ケーブルやコンソールの接続)の内容については，「ハードウェア取扱説明書」を参照してください。

図 4.1-1 本装置の起動から停止までの概略フロー



4.1.2 装置の起動

本装置の起動，再起動の方法を表 4.1-1 に示します。

表 4.1-1 コンソールとリモート運用端末の運用管理での適用範囲の違い

起動の種類	内容	操作方法
電源 ON による起動	本装置の電源 OFF からの立ち上げです。	本体の電源スイッチを ON にします。
リセットによる再起動	障害発生などによって本装置をリセットしたい場合に行います。	本体の RESET スイッチを押します。
コマンドによる再起動	ソフトウェアのアップデートや障害発生などによって本装置をリセットしたい場合に行います。	運用コマンド「reload」を実行します。

4.1.3 装置の停止

本装置の電源を OFF にする場合は，アクセス中のファイルが壊れるおそれがあるので，本装置にログインしているユーザがいない状態で行ってください。

運用コマンド「reload stop」 で装置を停止させたあとに電源を OFF にすることを推奨します。

4.2 ログイン・ログアウト

この節では，ログインとログアウトについて説明します。

4.2.1 ログイン

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

初期導入時には，ユーザ ID”admin”または”operator” でパスワードなしのログインができます。

初期導入時ログイン画面

```
login: operator
Password:
No password is set. Please set password!
SP>                              …(1)
```

(1) コマンドプロンプトが表示されます。

ログインタイムアウトについて

リモート接続の場合，接続から約１分以内にログインを完了してください。

4.2.2 ログアウト

CLI での操作を終了してログアウトしたい場合は，運用コマンド「exit」を実行してください。

ログアウト画面(コンソール接続の場合)

```
SP> exit

login:
```

自動ログアウトについて

10 分以上キーの入力がなかった場合，自動的にログアウトします。

4.3 コマンド入力モード

この節では，コマンド入力モードについて説明します。

4.3.1 コマンド入力モード

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

コマンド入力モードとプロンプトの対応を表 4.3-1 に示します。

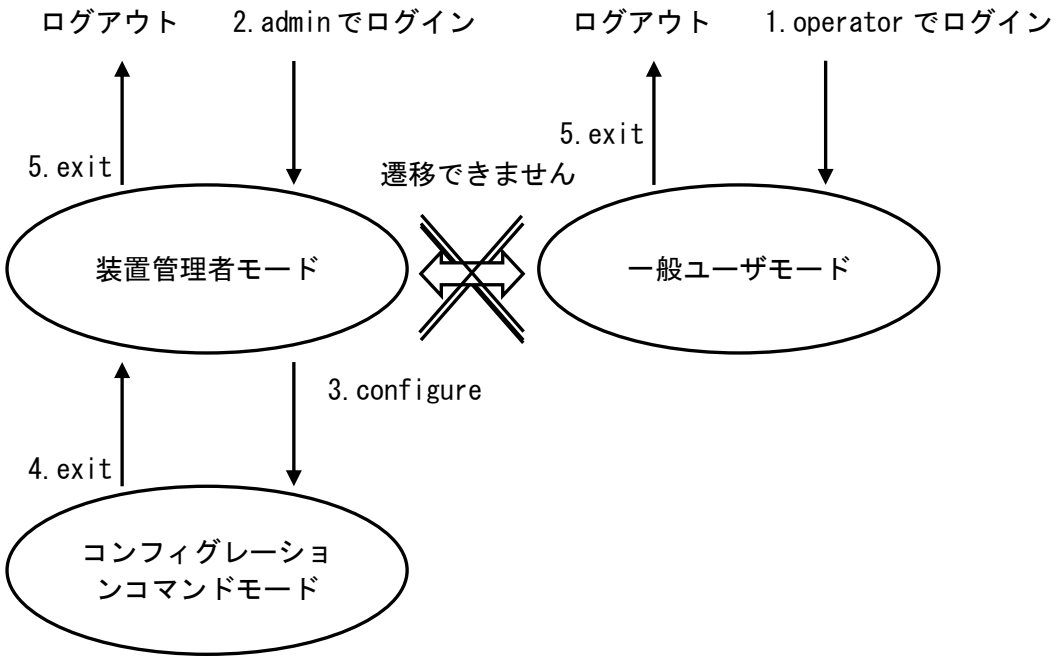
表 4.3-1 コマンド入力モードとプロンプトの対応

コマンド入力モード	実行可能なコマンド	プロンプト
一般ユーザモード	運用コマンドの一部	SP>
装置管理者モード	全ての運用コマンド	SP#
コンフィグレーションコマンドモード	コンフィグレーションコマンド	[SP]

4.3.2 コマンド入力モードの遷移

コマンド入力モードの遷移について図 4.3-1 に示します。

図 4.3-1 コマンド入力モード遷移の概要



1. operator権限でログインした場合，一般ユーザモードになります。
2. admin権限でログインした場合，装置管理者モードになります。
3. 装置管理者モードでコマンド「configure」を実行することにより，コンフィグレーションコマンドモードへと遷移します。
4. コンフィグレーションコマンドモードでコマンド「exit」を実行することで，装置管理者モードへと遷移します。
5. 一般ユーザモード，装置管理者モードでコマンド「exit」を実行することで本装置からログアウトします。

一般ユーザモードと装置管理者モードはコマンドによるモード遷移はできません。モードを変更したい場合は，いったんログアウトした後，目的のモードに合わせたユーザにて再度ログインしてください。

注意事項

・コンフィグレーションコマンドモードへは 1 ユーザのみ遷移可能です。別のユーザがコンフィグレーションコマンドモードになっている場合は，コマンド「configure」はエラーとなります。

4.4 ライセンス

この節では，ライセンスについて説明します。

4.4.1 ライセンスの概要

ライセンスはセンサ機能を有効化するためのものです。ライセンスはライセンスキーを記述した「ライセンス使用許諾契約書兼ライセンスシート」または，「ソフトウェア使用条件書」で提供します。

ライセンスは以下のルールに従います。

- 装置ごとに対応したライセンスが必要です。
- ライセンスを設定した場合，センサ機能の有効化は即時に行われます。
- ライセンスは有効期間のある初年度ライセンスおよび 1 年延長ライセンスと有効期間のない永続ライセンスがあります。
- ライセンスの有効期間を過ぎた場合は対象機能が無効化されます。有効期間を延長するには対象機能の期間延長ライセンスの設定が必要です。
- 装置の交換時にはライセンスキーの再設定が必要です。ソフトウェアのバージョンアップ時は，ライセンスの再設定は不要です。
- ライセンスキーは 32 桁の 16 進数(0～9，a～f)で表現されます。

基本ライセンスは AX-Sensor のセンサ機能を使用するために必須のライセンスです。本装置のライセンス一覧を次の表に示します。

表 4.4-1 AX-Sensor のライセンス一覧

略称	ライセンス名	内容
AX-NS-S01	AX-PA1630-01	AX-Sensor ソフトウェア 基本機能 初年度ライセンス
	AX-PA1630-01E1	AX-Sensor ソフトウェア 基本機能 1 年延長ライセンス
	AX-PA1630-01P	AX-Sensor ソフトウェア 基本機能 永続ライセンス
AX-NS-S02	AX-PA1630-02	AX-Sensor ソフトウェア AX-Sensor-08TL モデル基本機能 初年度ライセンス
	AX-PA1630-02E1	AX-Sensor ソフトウェア AX-Sensor-08TL モデル基本機能 1 年延長ライセンス
	AX-PA1630-02P	AX-Sensor ソフトウェア AX-Sensor-08TL モデル基本機能 永続ライセンス

4.4.2 ライセンスの設定方法

以下の手順でライセンスを設定してください。

１．装置管理者モードで本装置にログインしてください。

２．運用コマンド「show sp」を実行して現在のライセンスを確認してください。

３．運用コマンド「license add <ライセンスキー>」でライセンスを設定してください。

間違ったライセンスキーを指定した場合は「Invalid License Key.」と表示されますので正しいライセンスキーを指定してください。

ライセンスキーの大文字と小文字区別されるため小文字で入力してください。また，ハイフン(-)を省略した形式でもライセンスキーを指定できます。

４．運用コマンド「show sp」を実行して手順３で設定したライセンスが表示されることを確認してください。

設定したライセンスキーの先頭 16 桁が表示されます。

以上で，ライセンスの設定は終了です。

設定は即時反映され，センサ機能が有効化されます。

4.4.3 ライセンスの削除方法

以下の手順でライセンスを削除してください。

１．装置管理者モードで本装置にログインしてください。

２．運用コマンド「show sp」を実行して現在のライセンスを確認してください。

３．運用コマンド「license del 〈シリアル番号〉」でライセンスを削除してください。

〈シリアル番号〉は運用コマンド「show sp」で表示されたライセンスキーの先頭 16 桁を指定します。ハイフン(-)を省略せずに指定してください。

間違ったシリアル番号を指定した場合は「Invalid License Key.」と表示されますので正しいシリアル番号を指定してください。

シリアル番号は大文字と小文字を区別するため小文字で指定してください。

４．運用コマンド「show sp」を実行して手順３で削除したライセンスが表示されないことを確認してください。

以上で，ライセンスの削除は終了です。

削除は即時反映され，センサ機能が無効化されます。

次にライセンスの削除条件について示します。

表 4.4-2 ライセンスの削除条件

略称	ライセンス名	削除条件
AX-NS-S01	AX-PA1630-01	AX-PA1630-01E1 が設定されていない場合に削除可能
	AX-PA1630-01E1	常に削除可能
	AX-PA1630-01P	常に削除可能
AX-NS-S02	AX-PA1630-02	AX-PA1630-02E1 が設定されていない場合に削除可能
	AX-PA1630-02E1	常に削除可能
	AX-PA1630-02P	常に削除可能

4.4.4 ライセンスの失効

ラインセスの失効について説明します。

4.4.4.1 ライセンス失効前のアラート通知

ライセンスの有効期間が終了する3カ月前の月初め（1日）にライセンス失効3ヶ月前のアラート通知を行います。センサ機能は継続して使用可能です。
ライセンス失効3ヶ月前のアラート通知について以下に示します。

表 4.4-3 ライセンス失効 3 ヶ月前のアラート通知

#	アラート種別	通知	備考
1	運用メッセージ	・運用メッセージでライセンス失効 3 ヶ月前の通知を出力します。 ・ライセンス失効 3 ヶ月前に 1 回のみ通知します。 ・syslog 出力の設定がある場合には syslog サーバに通知します。	・メッセージ内容は「AX-Sensor コマンド・ログレファレンス」の「表 1.3-8 ライセンス関連運用メッセージ」を参照してください。
2	プロンプト	・コマンド入力モードで運用コマンド「show sp」の実行を促すメッセージが出力されます。 ・ライセンスの追加により有効期間が延長されるまで，プロンプトに毎回メッセージを出力します。	・プロンプトに以下のメッセージが出力されます。 You have warning messages. Use ″show sp″ to see them.
3	運用コマンド	・運用コマンド「show sp」の WARNING 情報にライセンス失効 3 ヶ月前のメッセージが出力されます。 ・ライセンスの追加により有効期間が延長されるまで，WARNING 情報に毎回メッセージを出力します。	・メッセージ内容は「AX-Sensor コマンド・ログレファレンス」の運用コマンド「show sp」および「表 1.2-5 show sp で表示される(2)の WARNING 一覧」を参照してください。

4.4.4.2 ライセンス失効後の動作

ライセンスの有効期間が終了するとラインセンス失効のアラート通知を行います。ライセンスが失効すると機能の一部が使用不可となります。
ライセンス失効時のアラート通知について以下に示します。

表 4.4-4 ライセンス失効時のアラート通知

#	アラート種別	通知	備考
1	運用メッセージ	・運用メッセージでライセンス失効の通知を出力します。 ・ライセンス失効時に 1 回のみ通知します。 ・syslog 出力の設定がある場合には syslog サーバに通知します。	・メッセージ内容は「AX-Sensor コマンド・ログレファレンス」の「表 1.3-8 ライセンス関連運用メッセージ」を参照してください。
2	プロンプト	・コマンド入力モードで運用コマンド「show sp」の実行を促すメッセージが出力されます。 ・ライセンスの追加により有効期間が延長されるまで，プロンプトに毎回メッセージを出力します。	・プロンプトに以下のメッセージが出力されます。 You have warning messages. Use ″show sp″ to see them.
3	運用コマンド	・運用コマンド「show sp」の WARNING 情報にライセンス失効のメッセージが出力されます。 ・ライセンスの追加により有効期間が延長されるまで，WARNING 情報に毎回メッセージを出力します。	・メッセージ内容は「AX-Sensor コマンド・ログレファレンス」の運用コマンド「show sp」および「表 1.2-5 show sp で表示される(2)の WARNING 一覧」を参照してください。

ライセンス失効で使用不可となる機能を以下に示します。

表 4.4-5 ライセンス失効で使用不可となる機能

#	機能	内容	備考
1	NetFlow Exporter 機能	NetFlow 情報の Data FlowSet 送信を停止します。	NetFlow 情報の Template FlowSet は継続して送信します。

4.5 ログインユーザの設定

この節では，ログインユーザの設定について説明します。

4.5.1 ログインユーザのパスワード変更

ログインユーザのパスワード変更は運用コマンド「edit system users」で行います。作成例を次の図に示します。

図 4.5-1 ログインユーザのパスワード変更

```
SP#                                                    …(1)
SP# edit system users                                  …(2)
[SP-system:users] user admin                           …(3)
[SP-system:users-test] password                        …(4)
New password:                                          …(5)
Retype new password:                                   …(6)
[SP-system:users-test] save                            …(7)
SP#
```

(1) 装置管理者モードでログインします。
(2) 運用コマンド「edit system users」を実行します。
(3) 運用コマンド「user」でパスワード変更するログインユーザ名を設定します。
(4) 運用コマンド「password」でパスワード入力に遷移します。
(5) 変更するパスワードを入力します。（入力したパスワードは表示されません）
(6) 再度，変更するパスワードを入力します。（入力したパスワードは表示されません）
(7) 運用コマンド「save」で上記(4)により設定したパスワードを反映します。

注意事項
・本装置では admin 権限のパスワードを誤って設定または消失・紛失した場合，ログインユーザの初期化ができません。セキュリティ上 admin 権限および operator 権限のログインユーザにはパスワードを設定し，パスワードを厳重に管理してください。

4.5.2 ログインユーザの作成および削除

ログインユーザの作成および削除は運用コマンド「edit system users」で行います。作成例を次の図に示します。

図 4.5-2 ログインユーザの作成

```
SP#                                                    …(1)
SP# edit system users                                  …(2)
[SP-system:users] user test                            …(3)
[SP-system:users-test] password                        …(4)
New password:                                          …(5)
Retype new password:                                   …(6)
[SP-system:users-test] group admin                     …(7)
[SP-system:users-test] userid 1234                     …(8)
[SP-system:users-test] save                            …(9)
SP#
```

(1) 装置管理者モードでログインします。
(2) 運用コマンド「edit system users」を実行します。
(3) 運用コマンド「user」で作成するログインユーザ名を設定します。
(4) 運用コマンド「password」でパスワード入力に遷移します。
(5) 変更するパスワードを入力します。（入力したパスワードは表示されません）
(6) 再度，変更するパスワードを入力します。（入力したパスワードは表示されません）
(7) 運用コマンド「group」で作成するログインユーザadminまたはoperatorの権限を設定します。デフォルトはoperatorが設定されています。
(8) 運用コマンド「userid」で作成するログインユーザのuseridを設定します。useridを設定しない場合はログインユーザ作成時に自動で割り当てられます。
(9) 運用コマンド「save」で上記(3)～(6)の設定内容を反映したログインユーザを作成します。

注意事項
・作成したログインユーザのgroupおよびuseridの変更はできません。変更を行う場合は一度ログインユーザを削除した後にログインユーザを再度作成してください。

図 4.5-3 ログインユーザの削除

```
SP#                                                    …(1)
SP# edit system users                                  …(2)
[SP-system:users] delete user test                     …(3)
[SP-system:users] save                                 …(4)
SP#
```

(1) 装置管理者モードでログインします。
(2) 運用コマンド「edit system users」を実行します。
(3) 運用コマンド「delete user」で削除するログインユーザ名を設定します。
(4) 運用コマンド「save」で上記(3)により設定したログインユーザを削除します。

4.5.3 ログインユーザの初期化

ログインユーザの初期化は運用コマンド「erase users」で行います。初期化例を次の図に示します。

図 4.5-4 ログインユーザの初期化

```
SP#                                                                    …(1)
SP# erase users                                                        …(2)
WARNING: Do you wish to erase users information?(y/n): [n]: y          …(3)
SP# reload                                                             …(4)
WARNING: Are you sure to restart system(y/n)? [n]: y                   …(5)
SP#
```

(1) 装置管理者モードでログインします。
(2) 運用コマンド「erase users」を実行します。
(3) ログインユーザ初期化の承諾確認で y を入力します。
(4) 運用コマンド「reload」で本装置の再起動を実施します。
(5) 装置再起動の承諾確認で y を入力します。

注意事項
・ログインユーザの初期化は装置再起動後に反映されます。

4.6 CLIでの操作

この節では，CLI での操作について説明します。

4.6.1 補完機能

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

補完機能を使用したコマンド入力の簡略化の例

```
[SP-netflow] net[Tab]
[SP-netflow] netflow
```

コマンド入力後に[Tab]キーを入力した場合では，使用できるパラメータやファイル名の一覧を表示します。

補完機能を使用した，指定可能パラメーター覧表示の例

```
[SP-netflow] netflow [Tab]
ipv4  mac
[SP-netflow] netflow
```

注意事項

・入力できない選択肢を表示する場合があります。「コマンド・ログレファレンス」の各コマンドの入力形式と入力範囲をご確認ください。

4.6.2 ヘルプ機能

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

[?]入力時の表示例

```
SP> show interface [?]
Valid entries at this position are:
  <Enter>     Execute command
  INTERFACE   Interface name

SP> show interface
```

注意事項

・＜＞のないパラメータ名を表示する場合があります。

・入力できない選択肢を表示する場合があります。「コマンド・ログレファレンス」の各コマンドの入力形式と入力範囲をご確認ください。

4.6.3 入力エラー指摘機能

コマンドまたはパラメータを不正に入力した際，エラー位置を「^」で指摘して，次行にエラーメッセージを表示します。[?]入力時も同様の表示となります。

「^」の指摘個所とエラーメッセージの説明によって，コマンドまたはパラメータを見直して再度入力してください。入力エラー位置指摘の表示例を次に示します。

入力エラー位置指摘の表示例

```
[SP-netflow] netflow notip
                     ^

  String error: invalid string

  Valid entries at this position are:

     ipv4      Netflow MAC-IPv4 function

     mac       Netflow MAC function

[SP-netflow]
```

4.6.4 コマンド短縮実行

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

短縮入力のコマンド実行例(show netflow statistics の短縮入力)

```
SP# show netflow [?]
statistics  status
SP# show netflow stati
Date 20XX/08/20 12:07:54 UTC
Total
  Received Packets :                0  Received Bytes   :                0
  Error Packets    :                0
IPv4
  Flow Entries     :                0  Received Packets :                0
  Expired Flows    :                0  Ignored Packets  :                0
  Overflow Packets :                0  Discard Flows    :                0
  Fragments        :                0
MAC
  Flow Entries     :                0  Received Packets :                0
  Expired Flows    :                0  Ignored Packets  :                0
  Overflow Packets :                0  Discard Flows    :                0
SP#
```

複数のパラメータ(この場合 netflow, statistics)を同時に短縮可能です。

```
SP# show net stati
Date 20XX/08/20 12:07:54 UTC
Total
  Received Packets :                0  Received Bytes   :                0
  Error Packets    :                0
IPv4
  Flow Entries     :                0  Received Packets :                0
  Expired Flows    :                0  Ignored Packets  :                0
  Overflow Packets :                0  Discard Flows    :                0
  Fragments        :                0
MAC
  Flow Entries     :                0  Received Packets :                0
  Expired Flows    :                0  Ignored Packets  :                0
  Overflow Packets :                0  Discard Flows    :                0
SP#
```

4.6.5 ヒストリ機能

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

ヒストリ機能を使用したコマンド入力の簡略化の例

```
> ping 192.168.100.2 count 1                                    …(1)
PING 192.168.100.2 (192.168.100.2): 120 data bytes
128 bytes from 192.168.100.2: icmp_seq=0 ttl=128 time=0 ms
----192.168.100.2 PING Statistics----
1 packets transmitted,  1 packets received,  0.0% packet loss
round-trip min/avg/max = 0/0/0 ms
>                                                               …(2)
> ping 192.168.100.2 count 1                                    …(3)
PING 192.168.100.2 (192.168.100.2): 120 data bytes
128 bytes from 192.168.100.2: icmp_seq=0 ttl=128 time=0 ms
----192.168.100.2 PING Statistics----
1 packets transmitted,  1 packets received,  0.0% packet loss
round-trip min/avg/max = 0/0/0 ms
>                                                               …(4)
> ping 192.168.100.3 count 1                                    …(5)
PING 192.168.100.3 (192.168.100.3): 120 data bytes
128 bytes from 192.168.100.3: icmp_seq=0 ttl=128 time=0 ms
----192.168.100.3 PING Statistics----
1 packets transmitted,  0 packets received,  100.0% packet loss
>
```

(1) 192.168.100.2 に対して ping コマンドを実行します。

(2) ［↑］キーを入力することで前に入力したコマンドを呼び出せます。この例の場合，［↑］キーを１回押すと「ping 192.168.100.2 count 1」を表示しますので，［Enter］キーの入力だけで同じコマンドを再度実行できます。

(3) 192.168.100.2 に対して ping コマンドを実行します。

(4) ［↑］キーを入力することで前に入力したコマンドを呼び出し，［←］キーおよび［Backspace］キーを使ってコマンド文字列を編集できます。この例の場合，［↑］キーを１回押すと「ping 192.168.100.2 count 1」を表示しますので，IP アドレスの「2」の部分を「3」に変更して［Enter］キーを入力しています。

(5) 192.168.100.3 に対して ping コマンドを実行します。

4.6.6 ページング

コマンドの実行により出力される結果について，表示すべき情報が一画面にすべて表示しきれない場合は，ユーザのキー入力を契機に一画面ごとに区切って表示します。なお，ページングは運用コマンド「pager」でその機能を有効にしたり無効にしたりできます。

4.6.7 キーボードコマンド機能

端末アプリケーションおよび端末の設定により，使用可能なキーが異なります。本装置では，VT100 で仕様が明確になっているキーを使用した表 4.6-1 の組み合わせでの操作を推奨します。

表 4.6-1 推奨キーボードコマンド

キーボード	説明
Backspace	カーソルの左の１文字を削除します。（ただし行の先頭まで）
Ctrl + A	コマンド行の先頭へ移動します。
Ctrl + B	１文字戻ります。（ただし行の先頭まで）
Ctrl + C	コマンドを中断します。
Ctrl + D	１文字削除します。
Ctrl + E	コマンド行の行末へ移動します。
Ctrl + F	１文字進みます。（ただし行の終わりまで）
Ctrl + L	コンソール画面をリフレッシュし，画面上のコマンド入力行以外は表示を消去します。
Ctrl + N	カレントコマンドまで次のヒストリを表示します。
Ctrl + P	一つ前のヒストリを表示します。
Ctrl + U	カーソル行のテキストを削除します。
Ctrl + W	カーソルより前方のテキストを削除します。
Ctrl + K	カーソルの後ろのテキストを削除します。
Ctrl + T	カレントの文字と前の文字を交換します。
Esc + B	１語戻ります。
Esc + F	１語進みます
Esc + D	語のカーソルから後ろを削除します。

4.6.8 CLI設定のカスタマイズ

自動ログアウト機能やCLI 機能の一部は，CLI 環境情報としてユーザごとに動作をカスタマイズできます。カスタマイズできるCLI 機能とCLI 環境情報を表 4.6-2 に示します。

表 4.6-2 カスタマイズできるCLI 機能とCLI 環境情報

機能	カスタマイズ内容と初期導入時のデフォルト設定
ページング	ページングするかどうかを設定できます。 ログイン時のデフォルト設定では，ページングを行いません。

ページングの有効/無効は，運用コマンド「pager」で設定できます。

設定内容は，コマンドが実行された直後から動作に反映されます。

4.7 コンフィグレーション

この節では，コンフィグレーションについて説明します。

4.7.1 コンフィグレーションの運用

起動時に読み込まれるコンフィグレーションをスタートアップコンフィグレーションと呼び，運用に使用されるコンフィグレーションをランニングコンフィグレーションと呼びます。

本装置の電源を入れると，内蔵フラッシュメモリ上のスタートアップコンフィグレーションファイルが読み出され，そのままランニングコンフィグレーションとして設定されて運用を開始します。

コンフィグレーションを編集，確定した場合は，ランニングコンフィグレーションが書き換えられ，運用に反映されます。変更したランニングコンフィグレーションは運用コマンド「copy conf running start」を使用することで，スタートアップコンフィグレーションに保存することが可能です。

編集した内容を保存しないで本装置を再起動すると，編集した内容は失われるので注意してください。

4.7.2 コンフィグレーションの編集

コンフィグレーションの編集について説明します。各コマンドの詳細については「コマンド・ログレファレンス」を参照してください。

(1) 編集可能なコマンドモード

コンフィグレーションの編集を行う場合は，装置管理者モードでログインし，configure コマンドを実行してください。プロンプトが[SP]になるとコンフィグレーションコマンドモードとなり，ランニングコンフィグレーションの編集が可能となります。

(2) コンフィグレーションの表示・確認

一般ユーザモードおよび装置管理者モードでコマンド「display conf running」および「 display conf start」を実行することで，それぞれランニングコンフィグレーション，スタートアップコンフィグレーションを表示・確認することができます。

コンフィグレーションコマンドモードでコマンド「display」を実行した場合は，現在編集中の内容が表示されます。運用中の内容とは異なる可能性があるので注意してください。

(3) コンフィグレーションの編集

コンフィグレーションコマンドを使用して，コンフィグレーションを編集します。また，コンフィグレーションの削除は，コマンドの先頭に「delete」を指定することで実現できます。

(4) コンフィグレーションの確定

編集したコンフィグレーションを反映させるにはコマンド「addrunning」で確定する必要があります。確定させるまではランニングコンフィグレーションに反映されることはなく，運用状態にも変化はありません。

コマンド「addrunning」で確定せずにコンフィグレーションコマンドモードを終了すると設定した内容は全て消えてしまいます。その場合には終了時に終了してよいか確認の警告が表示されます。y を入力するとそのまま終了し，n を入力すると終了せずにコンフィグレーションコマンドモードに戻ります。

コマンド「addrunning」を実行せずにコンフィグレーションコマンドモードを終了した場合に表示されるメッセージ

```
[SP] exit
WARNING: Modifications will be lost. Are you sure to exit (y/n)? [n]: n
[SP] exit
```

```
WARNING: Modifications will be lost. Are you sure to exit (y/n)? [n]: y
SP#
```

(5) コンフィグレーションの保存

運用コマンド「copy conf running start」を使用することで，ランニングコンフィグレーションがスタートアップコンフィグレーションファイルに保存されます。編集した内容を保存しないで装置を再起動すると，編集した内容が失われるので注意してください。

なお保存するにはコマンド実行時に出力される確認のメッセージに対して，以下のように 2 回「y」を入力します。

```
SP# copy conf running start
WARNING: Do you really want to overwrite the start configuration (y/n)? [n]: y
WARNING: start already exists. Do you want to overwrite it (y/n)? [n]: y
```

(6) コンフィグレーションの編集終了(exit コマンド)

コンフィグレーションの編集を終了する場合は，コンフィグレーションコマンドモードの最上位の階層で exit コマンドを実行します。

注意事項

・本装置が運用コマンド「show sp」で Status が in service になる前には，コンフィグレーション関連のオペレーションに関して以下の注意をお願いします。

・コマンド「display」でコンフィグレーションを表示しても，正しく表示されない場合があります。

・コンフィグレーションを編集しても編集内容が失われる場合があります。

・運用コマンド「show sp」で Status が in service となっていることを確認してから，コンフィグレーション関連のオペレーションを開始してください。

4.7.3 コンフィグレーションのエクスポート

編集したコンフィグレーションのバックアップを取りたい場合などは，運用コマンド「export conf」を使用してコンフィグレーションファイルのエクスポートが可能です。

ネットワークを経由してエクスポート

コマンド「export conf」のパラメータにURLを指定することでネットワーク経由でのエクスポートを実施します。ftp(またはtftp)を利用してのファイル転送ですので，エクスポート先となる機器でftp(またはtftp)サーバが起動している必要があります。

※本装置のftp/tftpサーバは起動していないため，外部から本装置へのftp/tftp接続はできません。

注意事項

・エクスポート可能なコンフィグレーションは，スタートアップコンフィグレーション「start」またはランニングコンフィグレーション「running」です。

4.7.4 コンフィグレーションのインポート

バックアップしていたコンフィグレーションファイルを取り込んで再運用したい場合などは，運用コマンド「import conf」を使用してコンフィグレーションファイルのインポートが可能です。

ネットワークを経由してインポート

コマンド「import conf」のパラメータにURLを指定することでネットワーク経由でのインポートを実施します。ftp(またはtftp)を利用してのファイル転送ですので，インポート元となる機器でftp(またはtftp)サーバが起動している必要があります。

※本装置のftp/tftpサーバは起動していないため，外部から本装置へのftp/tftp接続はできません。

インポート後，運用コマンド「reload」で本装置を再起動することでインポートしたコンフィグレーションでの運用が開始されます。

注意事項

・インポートするコンフィグレーションファイルは，スタートアップコンフィグレーションのみを対象としますので，コマンド「import conf」のパラメータであるインポート先のファイル名は，必ず「start」とする必要があります。元のファイル名が「start」である場合はインポート先のファイル名は指定する必要ありません。

4.7.5 コンフィグレーションの初期化

コンフィグレーションの初期化は運用コマンド「erase configuration」で行います。初期化例を次の図に示します。

図 4.7-1 コンフィグレーションの初期化

```
SP#                                                                    …(1)
SP# erase configuration startup                                        …(2)
WARNING: Do you wish to erase startup-config?(y/n): [n]: y             …(3)
SP# reload                                                             …(4)
WARNING: Are you sure to restart system(y/n)? [n]: y                   …(5)
SP#
```

(1) 装置管理者モードでログインします。
(2) 運用コマンド「erase configuration startup」を実行します。
(3) コンフィグレーション初期化の承諾確認で y を入力します。
(4) 運用コマンド「reload」で本装置の再起動を実施します。
(5) 装置再起動の承諾確認で y を入力します。

注意事項
・コンフィグレーションの初期化は装置再起動後に反映されます。

4.8 telnet/ssh によるログイン

通信用ポートを介して，リモート運用端末から本装置へログインするには，本装置で IP アドレスの設定が必要です。ただし，初期導入時には IP アドレスの設定が行われていません。そのため，コンソールからログインして，コンフィグレーションを設定する必要があります。

telnet によるログインを可能とするには本装置のマネジメントポートの IP アドレスを設定する必要があります。telnet サーバは本装置の起動時に自動で起動しますので，他に必要な設定はありません。

ssh によるログインを可能とするには，更に本装置の ssh サーバを有効化する必要があります。5.7.1 節「コンフィグレーション」を参照ください。

以下にインタフェース(eth1)への IP アドレスの設定例を示します。

インタフェース(eth1)への IP アドレスの設定例

```
SP# configure                              …(1)
[SP] eth1                                  …(2)
[SP-eth1] ipaddress 192.168.100.100/24     …(3)
[SP-eth1] addrunning                       …(4)
[SP-eth1] display                          …(5)
```

(1) 装置管理者モードでログインし，コマンド「configure」でコンフィグレーションコマンドモードへと切り替わります。

(2) eth1 に入ります。

(3) コマンド「ipaddress」で任意の IP アドレスを設定します。

(4) コマンド「addrunning」で反映します。

(5) コマンド「display」で設定内容を表示して確認します。

4.9 ftpによるログイン

本装置では一部運用コマンドでのみ ftp クライアント機能によるファイル転送を提供しています。

表 4.9-1 ftp を利用したファイル転送コマンド一覧

コマンド名	コマンド説明
export dump-file	解析情報ファイルを収集し，指定された転送先へ転送します。
export conf	コンフィグレーションファイルをエクスポートします。
import conf	コンフィグレーションファイルをインポートします。
export log-session	本装置で収集しているログファイルをエクスポートします。
update	ソフトウェアを取得しアップデートします。

4.10 ソフトウェアのアップデート

この節ではソフトウェアのアップデートについて説明します。

4.10.1 ソフトウェアのアップデート

ソフトウェアのアップデートとは，旧バージョンのソフトウェアから新バージョンのソフトウェアにバージョンアップすることを指します。アップデートを実施するには装置管理者モードで，運用コマンド「update」を実行します。

アップデート時，装置管理のコンフィグレーション，ユーザ情報（ログインアカウント，パスワードなど）およびライセンス情報はそのまま引き継がれます。

アップデートを実施するには以下の方法があります。

(1) ネットワーク経由でアップデートファイルを入手してアップデートする

コマンド「update」でアップデートファイルの入手先に URL を指定して実行することで，アップデートを行います。ftp(または tftp)を利用してのファイル転送を行うので，入手先となる機器で ftp(または tftp)サーバが起動している必要があります。

アップデート後，運用コマンド「reload」で本装置を再起動することで新しいソフトウェアでの運用が開始されます。自動で装置再起動は行いませんのでご注意ください。

なお，バージョンダウンする場合，未サポートになるコンフィグレーションはあらかじめ削除してください。未サポートのコンフィグレーションを削除しないでバージョンダウンを実行した場合，意図しないネットワーク構成や動作となるおそれがあります。

4.10.2 装置内バックアップ

装置内バックアップとは，現在動作しているソフトウェアを装置内に 1 世代分のバックアップを行うことで，スタートアップ面とバックアップ面の 2 面でソフトウェア管理が行えます。

スタートアップ面からバックアップ面へのバックアップだけでなく，バックアップしたソフトウェアをリストアすることも可能です。

以下にバックアップおよびリストアの手順を示します。

(1) スタートアップ面からバックアップ面へのバックアップ

1. 装置管理者モードでログインしてください。
2. 運用コマンド「copy lm start」を実行してください。スタートアップ面をバックアップ面にコピーします。
3. 運用コマンド「show version」で F/W の「Backup」に「Startup」と同じソフトウェアバージョン情報が示されていることを確認してください。

(2) バックアップ面からスタートアップ面へのリストア

1. 装置管理者モードでログインしてください。
2. 運用コマンド「copy lm backup」を実行してください。バックアップ面をスタートアップ面にコピーします。
3. 運用コマンド「show version」で F/W の「Startup」に「Backup」と同じソフトウェアバージョン情報が示されていることを確認してください。
4. 運用コマンド「reload」で装置を再起動してください。リストアしたソフトウェアで運用を開始します。

4.11 装置管理機能

この節では，本装置の管理を行う機能について説明します。

4.11.1 LEDと本装置の状態

本装置はLEDの表示により装置の状態をお知らせします。
次にLEDの表示内容について示します。

表 4.11-1 LED の表示内容

名称	種類	状態		内容
PWR	LED:緑	電源の投入状態を示します。	緑点灯	電源ON
			消灯	電源OFF，または電源異常
ST1	LED:緑/赤	装置の状態を示します。	緑点灯	動作可能
			緑点滅	準備中（立ち上げ中），または終了処理中
			赤点滅	装置の部分障害発生（警報）
			赤点灯	装置の致命的障害発生（継続使用不可）
			消灯	電源OFF，または電源異常
ST2	LED:緑/赤	装置の状態を示します。	緑点灯	動作可能
			緑点滅	ソフトウェア更新中，または終了処理中
			赤点滅	装置の部分障害発生（警報）
			赤点灯	装置の致命的障害発生（継続使用不可）
			消灯	電源OFF，または電源異常

4.11.2 障害監視

本装置で発生するハードウェア，およびソフトウェアの障害を検知します。

障害，警報が発生した場合には，LED による通知，syslog への障害情報の出力，本装置の再起動を状態に合わせて実施します。

障害が 3 回連続で発生した場合には，通常起動しているソフトウェアとは別の，バックアップされているソフトウェアを起動します。それでも正常起動しなかった場合には，本装置は停止します。

バックアップ方法については 4.10.2 節「装置内バックアップ」を参照して下さい。

(1) 電源ユニット/ファンの監視

電源で異常(温度異常または故障)を検知した場合に再起動を実施します。

表 4.11-2 電源ユニット/ファンの状態と動作一覧

装置の状態	運用の継続	動作
電源異常	×	運用メッセージを出力，および syslog サーバへ出力を行います。 再起動を行います。
ファン停止	○	運用メッセージを出力，および syslog サーバへ出力を行います。

(凡例) ○：継続可能。×：継続不可。

(2) 温度監視

本装置の温度が 70℃以上で再起動を実施します。

表 4.11-3 本装置の温度と動作一覧

装置の状態	運用の継続	動作
異常高温(70℃以上)	×	運用メッセージを出力，および syslog サーバへ出力を行います。 再起動を行います。
低温警報(0℃以下)	○	運用メッセージを出力，および syslog サーバへ出力を行います。
低温復旧(5℃以上)	○	運用メッセージを出力，および syslog サーバへ出力を行います。
高温警報(50℃以上)	○	運用メッセージを出力，および syslog サーバへ出力を行います。
高温復旧(45℃以下)	○	運用メッセージを出力，および syslog サーバへ出力を行います。

(凡例) ○：継続可能。×：継続不可。

(3) メモリ残量監視

メモリの使用量を監視し，未使用メモリが 5%以下となった場合に警告をログに出力し，再起動は実施しません。

表 4.11-4 メモリ残量と動作一覧

装置の状態	運用の継続	動作
メモリ残量警報	○	運用メッセージを出力，および syslog サーバへ出力を行います。
メモリ残量復旧	○	運用メッセージを出力，および syslog サーバへ出力を行います。

(凡例) ○：継続可能。×：継続不可。

(4) その他の障害

表 4.11-5 その他の障害と動作一覧

装置の状態	運用の継続	動作
ハードウェア重度障害	×	運用メッセージを出力，および syslog サーバへ出力を行います。再起動を行います。
ハードウェア軽度障害	○	運用メッセージを出力，および syslog サーバへ出力を行います。
ハードウェア軽度障害連続発生 (1 分間に 3 回発生)	×	運用メッセージを出力，および syslog サーバへ出力を行います。再起動を行います。
ソフトウェア障害	×	運用メッセージを出力，および syslog サーバへ出力を行います。再起動を行います。

(凡例) ○：継続可能。×：継続不可。

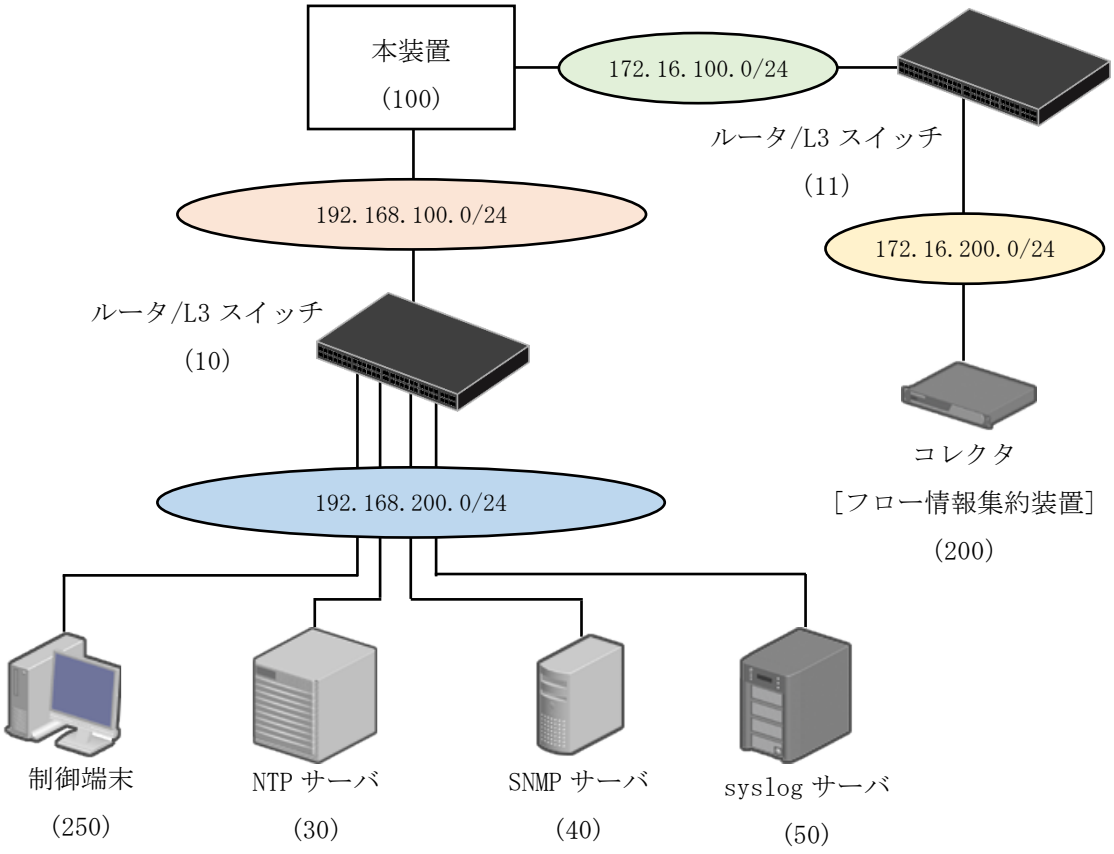
5 ネットワーク機能

この章では，ネットワーク機能について説明します。

5.1 ネットワーク構成例

本章で説明する設定内容は，次に示すネットワーク構成例の図を前提としています。

図 5.1-1 ネットワーク構成例



※カッコ内はネットワークのホスト番号を示す。

5.2 インタフェース設定

物理インタフェースの設定を説明します。

注意事項
・リンクアグリゲーションやVLANの設定はできません。

5.2.1 コンフィグレーション

インタフェース設定のコンフィグレーション設定例を次に示します。

図 5.2-1 インタフェース設定例

```
SP# configure
[SP] eth1                                    …(1)
[SP-eth1] ipaddress 192.168.100.100/24       …(2)
[SP-eth1] addrunning                         …(3)
[SP-eth1] display                            …(4)
# INTERFACE STATEMENTS
# IPV4 STATEMENTS
# IPV4 ADDRESSES
  ipaddress 192.168.100.100/24
# IPV6 STATEMENTS
# IPV6 ADDRESSES
# IPV6 PREFIXES
# ETHERNET STATEMENTS
```

(1)　インタフェースeth1を有効化します。
(2)　IPv4アドレスを設定します。
(3)　コンフィグレーション設定を反映します。
(4)　コンフィグレーション設定を表示します。

5.2.2 オペレーション

インタフェース設定に関連する運用コマンドを次に示します。

(1)　show interface
コンフィグレーションで設定したIPアドレスを表示します。

```
SP# show interface
# vrf0
eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 00:12:e2:95:c8:51 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.100/24 brd 192.168.100.255 scope global eth1
       valid_lft forever preferred_lft forever
```

(2)　show interface <物理インタフェース名> statistics detail
インタフェースの統計情報を表示します。

```
SP# show interface eth1 statistics detail
statistics:
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth1      1500      175      0      0 0             5      0      0      0 BMRU
    RX: bytes  packets  errors  dropped overrun mcast
    16942      175      0       0       0       7
    TX: bytes  packets  errors  dropped carrier collsns
    490        5        0       0       0       0
    RX rate  :         0bps(   0.0Mbps)          0pps(   0.0kpps)
    TX rate  :         0bps(   0.0Mbps)          0pps(   0.0kpps)
```

5.3 syslog出力

運用メッセージのsyslog出力設定について説明します。

5.3.1 コンフィグレーション

syslog出力設定のコンフィグレーション設定例を次に示します。

図 5.3-1 syslog 出力設定例

```
SP# configure
[SP] log
[SP-log] log-session SYSLOG remote 192.168.200.50  …(1)
[SP-log] log mng SYSLOG info                       …(2)
[SP-log] addrunning                                …(3)
[SP-log] display                                   …(4)
# LOG SESSIONS
  log-session MNG local 2 MB
  log-session NTP local 512 KB
  log-session SNMP local 512 KB
  log-session SYSLOG remote 192.168.200.50
# SERVICES LOG SESSIONS
  log mng SYSLOG info
  log ntp NTP info
  log snmp SNMP info
# DAEMONS LOG SESSIONS
```

(1) syslog出力設定を行う任意の文字列(SYSLOG)およびsyslogサーバ宛先を設定します。
(2) syslog出力設定を行う任意の文字列(SYSLOG)にsyslogサーバへ出力するメッセージ内容を設定します。
(3) コンフィグレーション設定を反映します。
(4) コンフィグレーション設定を表示します。

注意事項
・複数のsyslogサーバ宛先の設定を行えますが，最大4つとなります。
・syslog出力データのヘッダ部に付けるfacilityには常に「local0」を使用します。

5.3.2 オペレーション

syslog設定に関連する運用コマンドを次に示します。

(1)　show log-session MNG
装置内に保存している運用メッセージを表示します。

```
SP# show log-session MNG
Sep 12 08:57:02 SP MNG: spmd-INFO EVT NIF:00 20012010 Initialization started.
Sep 12 08:57:03 SP MNG: spmd-INFO EVT NIF:00 23024011 Initialization is complete.
Sep 12 08:57:14 SP MNG: ----INFO KEY NIF:00 00000000 admin: display conf running
```

5.4 SNMP

SNMP設定について説明します。

5.4.1 コンフィグレーション

SNMPのコンフィグレーション設定例を次に示します。

図 5.4-1 SNMP 設定例

```
SP# configure
[SP] snmp
[SP-snmp] snmp enable                                          …(1)
[SP-snmp] rocommunity public 192.168.200.40/24                 …(2)
[SP-snmp] authtrap enable                                      …(3)
[SP-snmp] trap2sink 192.168.200.40 public                      …(4)
[SP-snmp] addrunning                                           …(5)
[SP-snmp] display                                              …(6)
    # SNMP STATEMENTS
      snmp enable
      sysdescr none
      authtrap enable
    # COMMUNITIES
      rocommunity public 192.168.200.40/24
    # TRAPS
      trap2sink 192.168.200.40 public
    # SYSTEM
    # LOG SERVICE
      log snmp SNMP info
```

(1)　SNMP機能を有効化します。
(2)　読み取り可能なコミュニティを設定します。
(3)　Authentication Failure Trap機能を有効化します。
(4)　Trap機能を有効化し，出力先を設定します。
(5)　コンフィグレーション設定を反映します。
(6)　コンフィグレーション設定を表示します。

5.5 スタティックルーティング

スタティックルーティング設定について説明します。

5.5.1 コンフィグレーション

スタティックルーティングのコンフィグレーション設定例を次に示します。

図 5.5-1 スタティックルーティング設定例

```
SP# configure
[SP] rtg
[SP-rtg] route default-ipv4 192.168.100.10          …(1)
[SP-rtg] route 172.16.200.0/24 172.16.100.11        …(2)
[SP-rtg] addrunning                                 …(3)
[SP-rtg] display                                    …(4)
    # IPV4 ROUTES
      route default-ipv4 192.168.100.10
      route 172.16.200.0/24 172.16.100.11
    # IPV6 ROUTES
    # LOG SERVICE
    # GLOBAL INFO
    # ACCESS LIST & PREFIX LIST
    # COMMUNITY-LIST & EXTCOMMUNITY-LIST
    # ROUTE-MAPS
    # INTERFACES
    # DYNAMIC ROUTING
```

(1)　デフォルトゲートウェイを設定します。
(2)　宛先プレフィックス指定を設定します。
(3)　コンフィグレーション設定を反映します。
(4)　コンフィグレーション設定を表示します。

5.5.2 オペレーション

ルーティング設定に関連する運用コマンドを次に示します。

(1)　show ip route
ルーティングテーブル情報を表示します。

```
SP# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, M - SMR,
       > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.100.10, eth1
C>* 127.0.0.0/8 is directly connected, lo
C>* 172.16.100.0/24 is directly connected, eth2
S>* 172.16.200.0/24 [1/0] via 172.16.100.11, eth2
C>* 192.168.100.0/24 is directly connected, eth1
```

5.6 NTPクライアント

NTPクライアント設定について説明します。

5.6.1 コンフィグレーション

NTPクライアントのコンフィグレーション設定例を次に示します。

図 5.6-1 NTP クライアント設定例

```
SP# configure
[SP] ntp
[SP-ntp] ntp enable                          …(1)
[SP-ntp] remoteserver 192.168.200.30         …(2)
[SP-ntp] addrunning                          …(3)
[SP-ntp] display                             …(4)
    # NTP STATEMENTS
      ntp enable
      default-version 4
      default-polling 8
    # REMOTE SERVERS
      remoteserver 192.168.200.30 version 4
    # LOG SERVICE
      log ntp NTP info
```

(1)　NTPクライアント機能を有効化します。
(2)　接続先のNTPサーバを設定します。
(3)　コンフィグレーション設定を反映します。
(4)　コンフィグレーション設定を表示します。

5.6.2 オペレーション

NTPクライアント設定に関連する運用コマンドを次に示します。

(1)　show ntp associations

接続されているNTPサーバの動作状態を表示します。

```
SP# show ntp associations
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 192.168.200.30  .LOCL.           1 u   11  256     1    0.826   -0.243   0.004
```

5.7 その他の装置関連情報

ホスト名，タイムゾーン，リモートアクセスなどの設定について説明します。

5.7.1 コンフィグレーション

ホスト名，タイムゾーン，リモートアクセスなど，その他の装置関連情報のコンフィグレーション設定例を次に示します。

図 5.7-1 その他の装置関連情報の設定例

```
SP# configure
[SP] gen
[SP-gen] hostname AX-Sensor                              …(1)
[SP-gen] clock timezone JST 9                            …(2)
[SP-gen] ssh enable                                      …(3)
[SP-gen] system temperature-warning-level 40             …(4)
[SP-gen] addrunning                                      …(5)
[AX-Sensor-gen] display                                  …(6)
    # GEN STATEMENT
      hostname AX-Sensor
      clock timezone JST 9
      telnet enable
      ssh enable
      icmp limit rate 1000
      icmp limit type unreach quench redirect time_exceed param_prob
      system temperature-warning-level 40

    # ARP TABLE
    # NDP TABLE
    # HOST
    # LOG
```

(1)　ホスト名を設定します。
(2)　タイムゾーンをJSTに設定します。
(3)　sshサーバを有効化します。
(4)　運用メッセージで警告する装置の入気温度を設定します。
(5)　コンフィグレーション設定を反映します。
(6)　コンフィグレーション設定を表示します。

5.7.2 オペレーション

装置関連情報に関連する運用コマンドを次に示します。

(1)　show date

タイムゾーンを含めた日時情報を表示します。

```
AX-Sensor# show date
Wed 12 Sep 20XX 18:20:54 JST +0900 (Asia/Tokyo)
```

(2)　show service

telnet/sshなどのリモートアクセス機能の稼動状況を表示します。

```
AX-Sensor# show service
Service  TELNET          is active
Service  SSH             is active
Service  SNMP            is inactive
Service  NTP             is inactive
```

(3)　show environment temperature-logging

装置の温度履歴情報を表示します。

```
AX-Sensor# show environment temperature-logging
Date 20XX/05/31 15:00:00 JST
Date         0:00  6:00 12:00 18:00
20XX/05/31   24.3  24.2  26.0
20XX/05/30   21.8  25.1  26.0  24.0
20XX/05/29   25.6     -  26.0  24.0
```

6 センサ機能

この章では，センサ機能について説明します。

6.1 解説

センサ機能は，ネットワーク上を流れるトラフィックを把握する技術の一つです。
NetFlow Exporter機能では，モニタポート，センサ出力ポート，マネジメントポートの各ポート機能に特化した処理を行うことで実現します。

6.1.1 モニタポート

モニタポートは観測対象ネットワークからミラーリングされたトラフィックを受信する専用ポートです。観測対象ネットワークにジャンボフレームが含まれている場合，mtuの値を大きくすることを推奨します。
モニタポートにはDeny-Filter機能が設定可能です。Deny-Filter機能の詳細は「6.1.4.6 Deny-Filter機能」を参照してください。

注意事項
・モニタポートにはIPアドレスの設定をしないでください。

6.1.2 センサ出力ポート

センサ出力ポートはNetFlow情報を出力するためのポートです。NetFlow情報の出力先装置と直接接続する必要はなく，センサ出力ポートとの間にルータやスイッチを介しての接続が可能です。

注意事項
・センサ出力ポートはマネジメントポートと併用が可能です。

6.1.3 マネジメントポート

マネジメントポートは操作端末やNTPサーバなどのサーバ類と接続するポートです。操作端末やサーバと直接接続する必要はなく，マネジメントポートとの間にルータやスイッチを介しての接続が可能です。

注意事項
・マネジメントポートはセンサ出力ポートと併用が可能です。

6.1.4 NetFlow Exporter機能

本装置で実現するNetFlow Exporter機能は，本装置のモニタポートで受信したトラフィックを，フローごとにパケット数やオクテット数を一定の時間で集計し，本装置のセンサ出力ポートからNetFlowパケット形式でコレクタ(NetFlow情報を集約する装置)へ送信する機能です。NetFlow情報はトラフィックを受信してフローを集計し始めてから一定時間後に送信され，一定時間内に集計対象となるフローが無い場合はNetFlow情報を送信しません。

6.1.4.1 フローの識別条件

トラフィックのフローごと集計に際して，フローは「表 6.1-1」の識別項目のセットで識別されます。この識別項目のセットをフロー条件と呼びます。受信したトラフィックで識別対象が同じものは，該当フロー条件にて同じフローとして扱われます。

表 6.1-1 フロー条件とフロー識別条件の関係

#	識別項目	IPv4 フロー	IPv6 フロー	MAC フロー
1	受信モニタポート番号	○	○	○
2	MAC アドレス(DA)	○	○	○
3	MAC アドレス(SA)	○	○	○
4	VID※1	○	○	○
5	EthernetType	－	－	○
6	IPv4 アドレス(SIP)	○	－	－
7	IPv4 アドレス(DIP)	○	－	－
8	IPv6 アドレス(SIP)	－	○	－
9	IPv6 アドレス(DIP)	－	○	－
10	IP Protocol	○	○	－
11	L4 ポート番号(SP)	○※2	○	－
12	L4 ポート番号(DP)	○※2	○	－
13	ICMP メッセージ(タイプ，コード)	○	○	－

凡例　○：識別対象，－：識別対象外

- 注※1
  TPID 値：0x8100，0x88A8，0x9100 またはコンフィグレーションコマンド「vlan-tpid」の設定値
- 注※2
  フラグメントパケット(先頭パケット以外)の場合，0 となります。

6.1.4.2 NetFlowパケット形式

NetFlowパケットはVersion 9(RFC3954)に従った形式で送信します。
フロー条件ごとのTemplate IDを表 6.1-2に示します。

表 6.1-2 Template ID

フロー条件	Template ID
IPv4 フロー	1024
IPv6 フロー	2048
MAC フロー	4096

6.1.4.3 NetFlow設定パラメータ

次にNetFlow Exporter機能の設定パラメータについて以下に示します。

表 6.1-3 NetFlow Exporter 機能の設定パラメーター覧

#	コンフィグレーション	デフォルト値	説明
1	flow-max-entry	200,000 エントリ	フローのエントリ上限数
2	expire-time	30 秒	ユニキャスト，マルチキャスト，ブロードキャストの各種別エントリのフロー集計期間。
3	flow packet max size	500byte	NetFlow ヘッダ以降(UDP ペイロード長)のサイズを指定する。 IP ヘッダ，UDP ヘッダは対象外。
4	flow source ipaddress	-	NetFlow 情報の送信元 IPv4 アドレスを任意の IPv4 アドレスに変更する。本パラメータに設定が無い場合は物理インタフェースに設定された IPv4 アドレスが NetFlow 情報の送信元 IPv4 アドレスとなる。
5	flow source-id	0x0	NetFlow 情報の NetFlow ヘッダに格納する ID。 複数のセンサから NetFlow 情報を受信した際の判別に利用可能。
6	flow send-interval	100 マイクロ秒	NetFlow DataFlowSet の最小送信間隔

(凡例) -:対象外

6.1.4.4 NetFlow DataFlowSetの送信契機

本装置は，フローの集計を開始してから設定パラメータ「expire-time」の期間が経過すると当該フローの集計結果を NetFlow DataFlowSet パケットとして送信します。

ただし，当該フローが TCP かつセッションが終了している場合（TCP ヘッダの FIN フラグまたは RST フラグが 1 のパケットを受信した場合）は expire-time の経過を待たずに当該フローの集計結果を NetFlow DataFlowSet パケットとして送信します。

6.1.4.5 フロー識別条件の変更

コンフィグレーションの設定によりフローの識別条件(表6.1-1「フロー条件とフロー識別条件の関係」)を対象外に変更できます。
必要最小限となるフローの識別条件に変更することで顧客情報の保護やNetFlowパケットの情報量を減らすことによるフロー情報収集装置（コレクタ）への負荷低減を期待できます。
次にフロー識別条件の変更によるコンフィグレーション対応について示します。

表 6.1-4 フロー識別条件の変更によるコンフィグレーション対応

#	フローの識別条件	コンフィグレーション対応		
		IPv4 フロー	IPv6 フロー	MAC フロー
1	受信モニタポート番号	○	○	○
2	MAC アドレス(DA)	○	○	○
3	MAC アドレス(SA)	○	○	○
4	VID	○	○	○
5	EthernetType	-	-	○
6	IPv4 アドレス(SIP)	○	-	-
7	IPv4 アドレス(DIP)	○	-	-

8	IPv6 アドレス(SIP)	-	○	-
9	IPv6 アドレス(DIP)	-	○	-
10	IP Protocol	○	○	-
11	L4 ポート番号(SP)	○	○	-
12	L4 ポート番号(DP)	○	○	-
13	ICMP メッセージ(タイプ，コード)	○	○	-

(凡例) ○：対象，-:対象外

6.1.4.6 Deny-Filter機能

Deny-Filter機能はモニタポート専用の機能で，モニタポートごとに設定します。
モニタポートで受信したフレームの宛先MACアドレスを判別し，マルチキャストのみ，ブロードキャストのみ，マルチキャストとブロードキャストの両方を設定条件に合わせて廃棄します。廃棄されたフレームはNetFlow情報のフロー集計，およびインタフェース統計情報関連（カウンタ，MIBなど）の対象外となります。

廃棄されたフレームの統計情報は運用コマンド「show netflow statistics detail」でモニタポートごとに確認でき，マルチキャストとブロードキャストの合計値です。

6.1.4.7 NetFlow情報量計測機能

NetFlow情報量計測機能は，モニタポートで受信した観測対象ネットワークのフロー情報(flow/sec)とセンサ出力ポートから送信するコレクタごとのNetFlowパケットの通信量(bit/sec)を計測する機能です。
運用コマンド「show netflow statistics deteil」で計測結果を表示します。
検証時や環境構築時などに本装置のみ設置することでコレクタへのNetFlow送信負荷の目安を確認することができます。

計測に必要となるコンフィグレーション設定を以下に示します。

表 6.1-5 NetFlow 情報量計測機能に必要なコンフィグレーション設定

#	コンフィグレーションコマンド	計測内容	
		フロー情報量 (flow/sec)	NetFlow 通信量 (bit/sec)
1	netflow {フロー条件} enable	○	○
2	flow ipaddress	-	○

(凡例) ○：対象，-:対象外

注意事項
・NetFlow通信量(bit/sec)の計測をするためには，コンフィグレーションコマンド「netflow {フロー条件} enable」と「flow ipaddress」の両方を設定する必要があります。

運用コマンド「show netflow statistics」の計測表示について以下に示します。

表 6.1-6 show netflow statistics コマンドの計測表示

#	運用コマンド	計測内容	
		フロー情報量 (flow/sec)	NetFlow 通信量 (bit/sec)
1	show netflow statistics	○	-
2	show netflow statistics detail	○	○

(凡例) ○：対象，-:対象外

6.1.4.8 expire-timeの複数種別指定

expire-timeの複数種別指定は，モニタポートで受信したフレームをユニキャスト，マルチキャスト，ブロードキャストの種別に判別し，フロー条件ごとにexpire-timeをコンフィグレーションで設定できます。

表 6.1-7 expire-time のコンフィグレーション対応

#	フロー条件	コンフィグレーション対応		
		ユニキャスト	マルチキャスト	ブロードキャスト
1	IPv4 フロー	○	○	○
2	IPv6 フロー	○	○	○※1
3	MAC フロー	○	○	○

(凡例) ○：対象， -：対象外

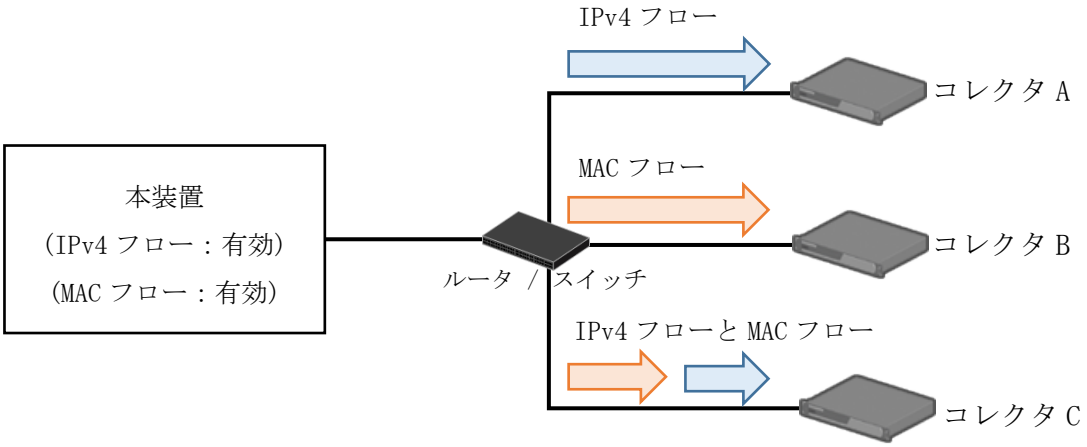
・ 注※1

コンフィグレーション設定は可能ですが，該当するフレームはありません。

6.1.4.9 コレクタ宛先ごとのフロー条件指定

コレクタ宛先ごとのフロー条件指定は，任意のコレクタ宛先に任意のフロー条件を指定する機能です。
複数のフロー条件を有効にして利用する場合，センサ出力ポートにコンフィグレーションで設定するコレクタ宛先にフロー条件を指定することにより，複数のフロー条件で集計したフロー情報(NetFlowパケット)を任意のコレクタ宛先に任意のフロー条件を指定して送信できます。

図 6.1-1 コレクタ宛先ごとのフロー条件指定例



6.1.4.10 NetFlow送信間隔の平準化調節機能

NetFlow送信間隔の平準化調節機能は，NetFlowパケットの送信間隔を調節することでコレクタ（フロー情報集約装置）への回線負荷を平準化する機能です。

モニタポートで一度に受信したトラフィックのフロー量が多い場合，expire-time経過後に連続してNetFlowパケットを送信するため，バーストトラフィックとなりコレクタ（フロー情報集約装置）への回線負荷が瞬間的に増大する恐れがあります。
コンフィグレーションコマンド「flow send-interval」によりNetFlowパケットの送信間隔を設定できます。

コレクタ宛先を複数指定している場合，またはフロー条件とコレクタ宛先の両方を複数設定している場合においては，1つのフロー条件から各コレクタ宛先へNetFlowパケットを送信する単位で間隔を調節できます。

図 6.1-2　NetFlowパケット送信間隔の調節単位

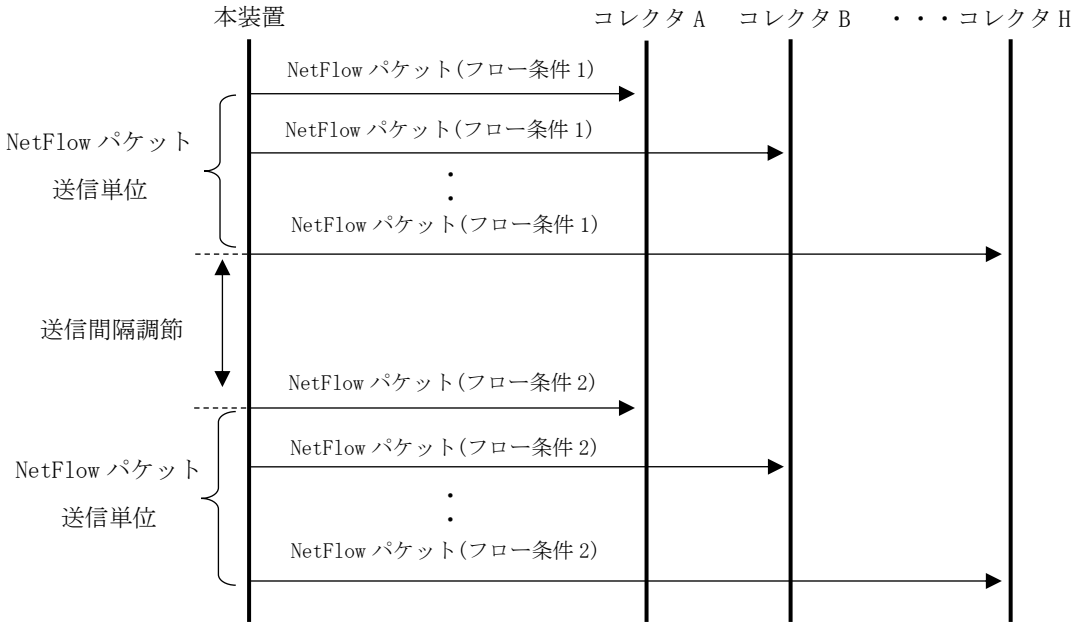
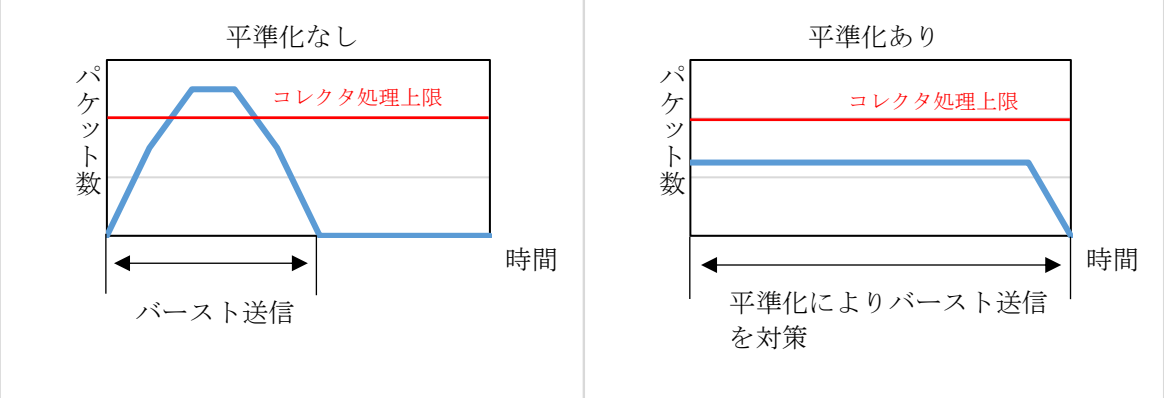


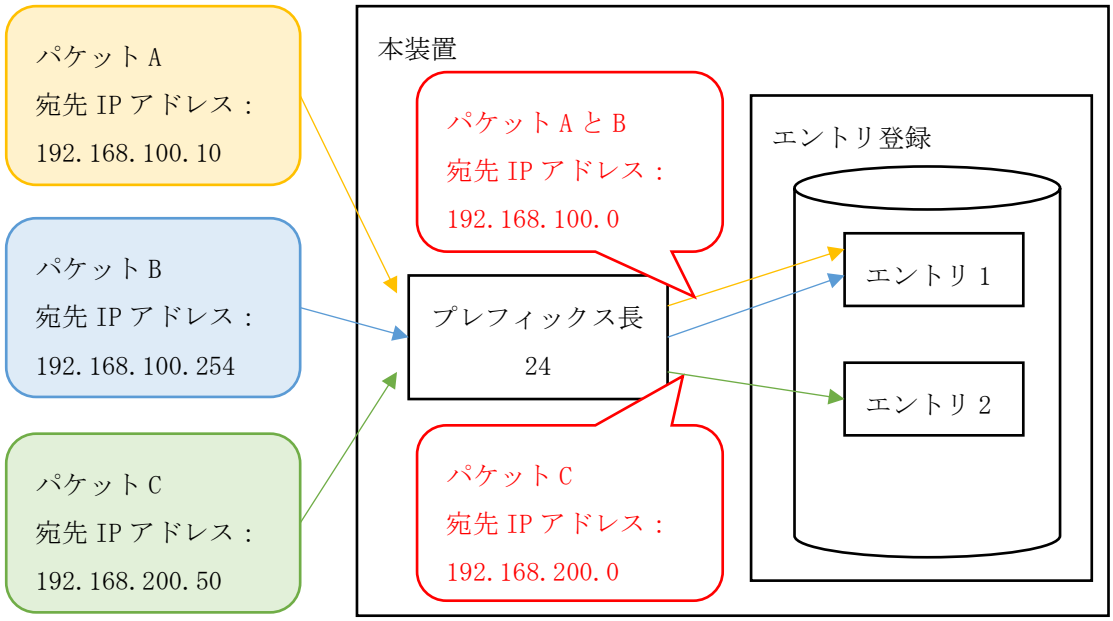
図 6.1-3　NetFlowパケット送信間隔による平準化のグラフイメージ



6.1.4.11　IPアドレス集約機能

IPアドレス集約機能は，モニタポートで受信したパケットの送信元IPアドレスおよび宛先IPアドレスに対して，設定したプレフィックス長までのIPアドレスが同じ場合，同じフローとしてエントリに登録する機能です。
プレフィックス長より下位ビットのIPアドレスは0になります。

図 6.1-4　**宛先IPアドレス集約の例**



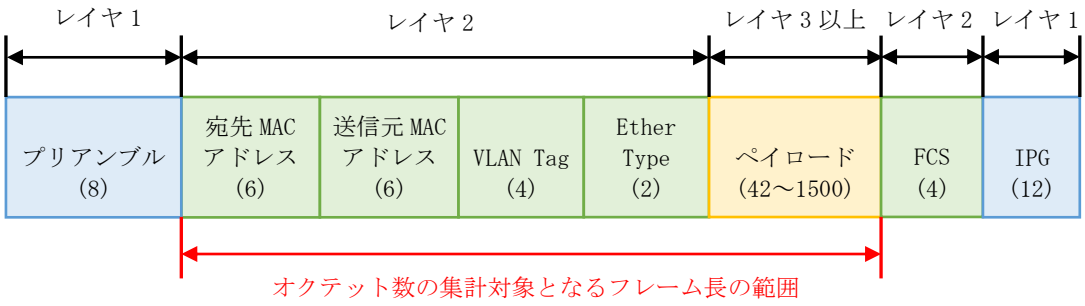
注意事項
・一度エントリに登録すると，集約前のIPアドレスに戻すことはできません。
・本機能は集約したIPアドレスの他にフローの識別条件が全て一致する必要があります。フローの識別条件が異なる場合は，異なるフローとしてエントリ登録されます。フローの識別条件は6.1.4.1 フローの識別条件を参照してください。

6.1.4.12 オクテット数補正

オクテット数補正は，NetFlow Exporter機能でフローごとに集計しているオクテット数（IN_BYTESフィールド）に対して，フレームごとに設定された補正値（固定値）を加減算します。

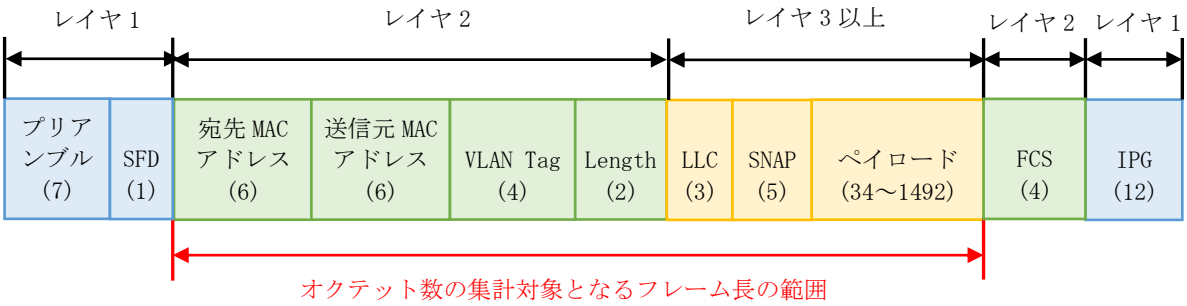
本装置はFCSを除く，レイヤ2以上のフレーム長をオクテット数の集計対象としているため，目的に応じて補正値を算出してください。
以下にオクテット数の集計対象について示します。

図 6.1-5　Ethernet IIフレーム（VLAN Tag有りの場合）



()内はオクテット数を示す。

図 6.1-6　802.3LLC/SNAPフレーム（VLAN Tag有りの場合）



()内はオクテット数を示す。

以下に算出例を示します。

例1)
レイヤ1以上の情報をオクテット数に補正（加算）したい場合は以下の値を設定します。
　プリアンブル（＋ SFD）＋ FCS ＋ IPG ＝ 24

例2)
レイヤ3以上の情報をオクテット数に補正（減算）したい場合は以下の値を設定します。
　宛先MACアドレス ＋ 送信元MACアドレス ＋ VLAN Tag ＋ Ether TypeまたはLength ＝ -18

注意事項
・補正値は固定となるため，監視対象ネットワークにVLAN Tag有りとVLAN Tag無しのフレームが混在している場合は正確なオクテット数補正ができません。

6.1.4.13 TCP遅延測定機能

TCP遅延測定機能は，本装置がIPv4フローおよびIPv6フローで集計しているTCP通信のRound Trip Time（RTT），サーバ応答時間，データ伝送遅延時間，再送に関連するカウンタを測定し，測定結果をNetFlow情報に付与する機能です。

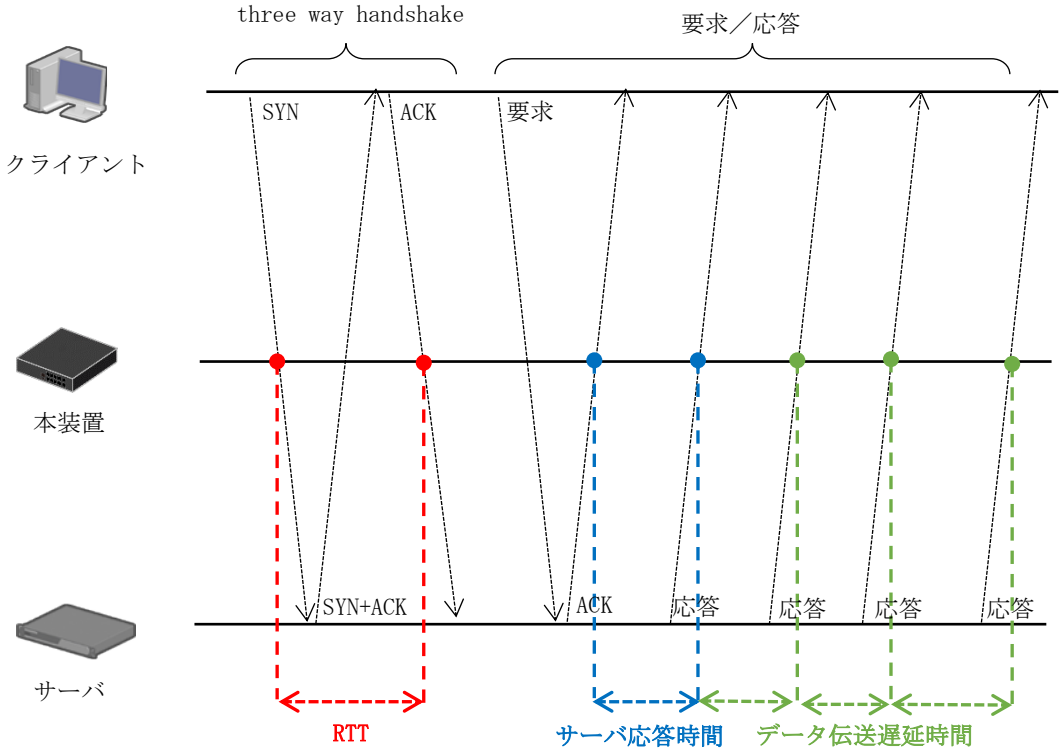
本装置でTCP通信のパフォーマンスを測定し，コレクタでサーバやアプリケーションの通信状態，応答性を確認することができます。

下記に本装置でのTCP通信の測定項目と測定方法を示します。

表 6.1-8 TCP 通信の測定項目

#	測定項目	説明
1	Round Trip Time (RTT)	TCP 接続の確立（three way handshake）時にクライアントが送信した SYN パケットと ACK パケット間の時間を測定します。
2	サーバ応答時間	サーバがクライアントの要求を受信して（クライアントに ACK パケットを送信して）から最初の応答パケットを送信するまでの時間を測定します。
3	データ伝送遅延時間	サーバが送信する応答パケットの間隔を測定します。
4	再送パケット数	再送パケットの数を測定します。
5	再送バイト数	再送パケットのデータサイズを測定します。
6	パケットロス検知数	パケットロスが発生した回数を測定します。
7	重複 ACK パケット数	重複 ACK パケットの数を測定します。

図 6.1-7 RTT，サーバ応答時間，データ伝送遅延時間の測定方法



サーバ応答時間およびデータ伝送遅延の測定では，ヘルスチェック通信のような周期的な通信の通信間隔が測定結果に含まれる場合があります。一定時間以上の測定結果をコレクタに通知したくない場合は，コンフィグレーションコマンド「tcp-monitor-timeout」によりサーバ応答時間およびデータ伝送遅延の最大測定時間を設定してください。

注意事項
・本機能はMACフローと排他になっており，MACフローと同時に使用できません。
・フロー識別条件の変更により，IPv4アドレス(SIP)，IPv4アドレス(DIP)，IPv6アドレス(SIP)，IPv6アドレス(DIP)，IP Protocol，L4ポート番号(SP)，L4ポート番号(DP)のどれか1つ以上をフロー識別の対象外にした場合は測定できません。
・IPアドレス集約機能を有効にしている場合は測定できません。

6.1.4.14 HTTP情報測定機能

HTTP情報測定機能は，本装置がIPv4フローおよびIPv6フローで集計しているHTTPまたはHTTPSの通信から接続先情報を取得し，測定結果をNetFlow情報に付与する機能です。

本装置でHTTP通信に関する情報を測定し，コレクタでHTTP通信の接続先ごとの通信状態，応答性等を確認することができます。

下記にHTTP情報測定機能の測定項目を示します。

表 6.1-9 HTTP 情報測定機能の測定項目

#	測定項目	説明
1	HTTP サーバ名	接続先のサーバ名(文字列)を取得します。集計対象の通信が TCP パケットかつ L4 ポート番号が 80，443 または 8080 のいずれかの場合に接続先サーバ名をパケット内から抽出します。

注意事項
- フロー識別条件の変更により，IPv4アドレス(SIP)，IPv4アドレス(DIP)，IPv6アドレス(SIP)，IPv6アドレス(DIP)，IP Protocol，L4ポート番号(SP)，L4ポート番号(DP)のどれか1つ以上をフロー識別の対象外にした場合は測定できません。
- IPアドレス集約機能を有効にしている場合は測定できません。

6.1.4.15 NetFlowキャッシュエージング機能

NetFlowキャッシュエージング機能は，最後に当該フローを受信してから本機能で設定した期間が満了するまで，集計中フローエントリのキャッシュ情報を保持する機能です。本機能により，TCP遅延測定やHTTP情報測定において，設定パラメータ「expire-time」より長い期間の通信に対する測定が可能になります。

下記にNetFlowキャッシュエージング期間とexpire-timeの関係を示します。

図 6.1-8 NetFlowキャッシュエージング期間とexpire-timeの関係

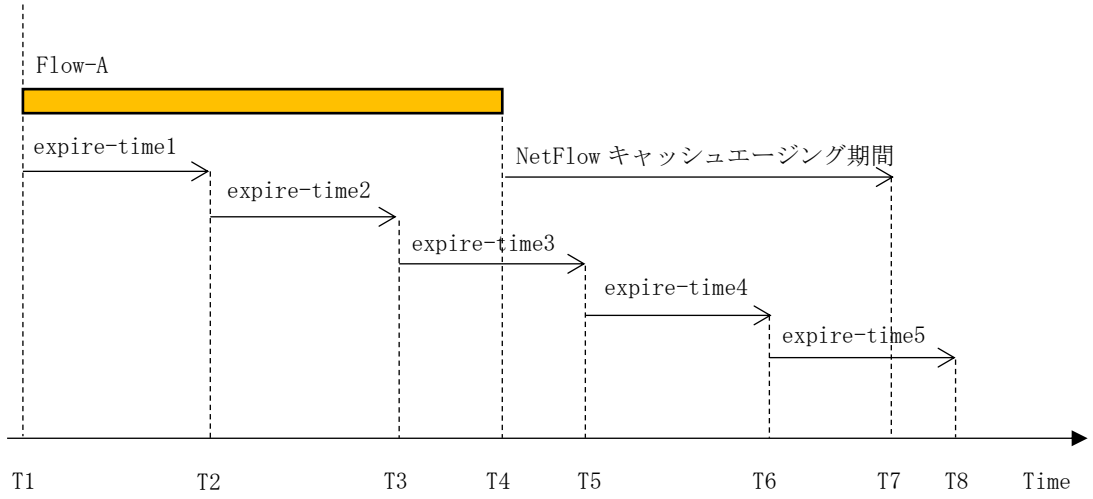


図 6.1-8の例は，T1からT4まで通信が発生したフロー(Flow-A)とNetFlowキャッシュエージング期間およびexpire-timeの関係を示しています。フローエントリの削除は，NetFlowキャッシュエージング期間が満了後，次にexpire-timeが満了したタイミング(T8)で行います。

注意事項
- 本機能は集計対象のフローがTCPの場合にのみ動作します。
- NetFlowキャッシュエージング期間を長くするほど本装置のフローエントリ数が増加しやすくなります。

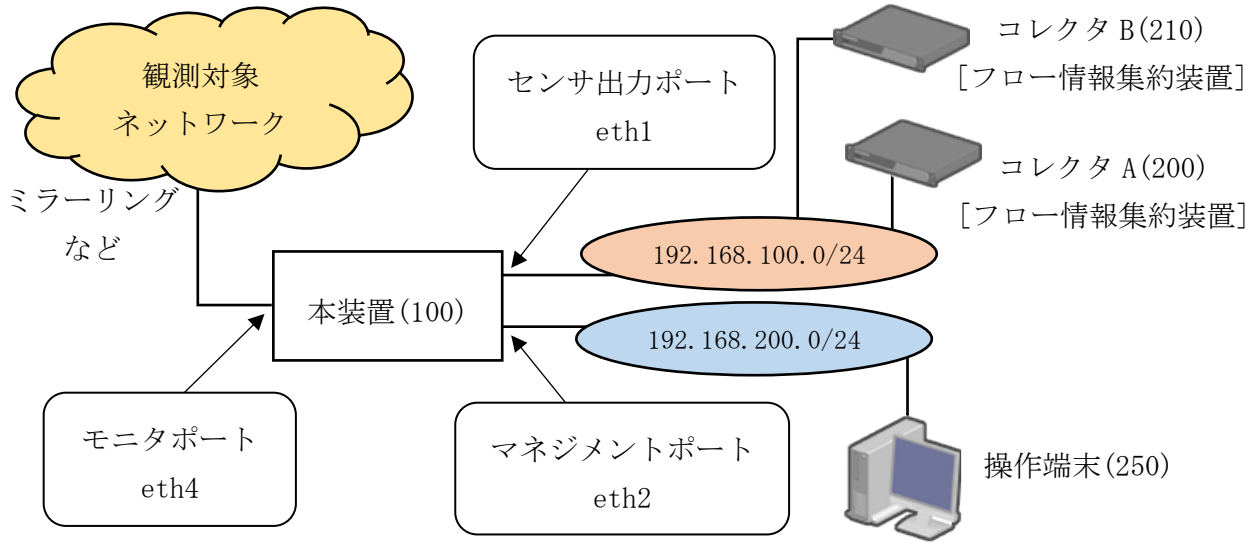
6.2 コンフィグレーション

センサ機能のコンフィグレーションについて説明します。

6.2.1 NetFlow Exporter機能のネットワーク構成例

次にNetFlow Exporter機能を使用したネットワーク構成例を次に示します。

図 6.2-1 NetFlow Exporter 機能を使用したネットワーク構成例



※カッコ内はネットワークのホスト番号を示す。

6.2.2 コンフィグレーション設定例

図6.2-1で示したNetFlow Exporter機能を使用したネットワーク構成例のコンフィグレーション設定例について次に示します。

図 6.2-2 構成例のコンフィグレーション設定例

```
SP# configure
[SP] eth1                                          …物理インタフェースeth1を有効化
[SP-eth1] ipaddress 192.168.100.100/24             …IPアドレスを設定
[SP-eth1] exit
[SP] eth2                                          …物理インタフェースeth2を有効化
[SP-eth2] ipaddress 192.168.200.100/24             …IPアドレスを設定
[SP-eth2] exit
[SP] eth4                                          …物理インタフェースeth4を有効化
[SP-eth4] mtu 9216                                 …mtuを9216に設定(観測対象ネットワークにジャンボフレームが流れている場合はmtuを大きな値にすることを推奨します)
[SP-eth4] exit
[SP] netflow
[SP-netflow] netflow ipv4 enable                   …フロー条件のIPv4フローを有効化
[SP-netflow] netflow mac enable expire-time 30 60 60        …フロー条件のMACフローを有効化, expire-timeのユニキャスト・マルチキャスト・ブロードキャストをそれぞれの時間に設定
[SP-netflow] exclude-field ipv4 src-ip             …IPv4フローのフロー識別条件から送信元IPv4アドレスを対象外に設定
[SP-netflow] adjust-in-bytes-field 24              …オクテット数補正値を設定
[SP-netflow] ipv4-prefix-mask dst-ip 24            …宛先IPアドレス集約のプレフィックス長を設定
[SP-netflow] vlan-tpid 0x1111 0x2222 0x3333        …VLAN Tagを識別するTPID値を設定
[SP-netflow] traffic-monitor-port eth4             …モニタポートをeth4に設定
[SP-netflow] deny-filter eth4 broadcast            …モニタポートにDeny-Filterのブロードキャストパケット条件を設定
[SP-netflow] mgmt-port eth2                        …マネジメントポートをeth2に設定
[SP-netflow] output-port eth1                      …センサ出力ポートをeth1に設定
[SP-netflow-output-port-eth1] flow ipaddress 192.168.100.200 port 9996       …コレクタAのIPアドレスおよびL4ポート番号を設定
[SP-netflow-output-port-eth1] flow ipaddress 192.168.100.210 port 9996 mac   …コレクタBのIPアドレスおよびL4ポート番号, MACフローのみの送信に設定
[SP-netflow-output-port-eth1] exit
[SP-netflow] exit
[SP] addrunning                                    …設定を反映
[SP] exit
SP#
SP# copy conf running start                        …コンフィグレーションを保存
WARNING: Do you really want this config to become the start config (y/n)? [n]: y
SP#
SP# display conf running                           …コンフィグレーションを表示
#############
# Ethernet  #
#############
eth1
    # INTERFACE STATEMENTS
    # IPV4 STATEMENTS
    # IPV4 ADDRESSES
      ipaddress 192.168.100.100/24
    # IPV6 STATEMENTS
    # IPV6 ADDRESSES
    # IPV6 PREFIXES
```

```
    # ETHERNET STATEMENTS
eth2
    # INTERFACE STATEMENTS
    # IPV4 STATEMENTS
    # IPV4 ADDRESSES
      ipaddress 192.168.200.100/24
    # IPV6 STATEMENTS
    # IPV6 ADDRESSES
    # IPV6 PREFIXES
    # ETHERNET STATEMENTS
eth4
    # INTERFACE STATEMENTS
      mtu 9216
    # IPV4 STATEMENTS
    # IPV4 ADDRESSES
    # IPV6 STATEMENTS
    # IPV6 ADDRESSES
    # IPV6 PREFIXES
    # ETHERNET STATEMENTS
####################
#  LOG SESSIONS    #
####################
log
    # LOG SESSIONS
      log-session MNG local 2 MB
      log-session NTP local 512 KB
      log-session SNMP local 512 KB
    # SERVICES LOG SESSIONS
      log ntp NTP info
      log snmp SNMP info
    # DAEMONS LOG SESSIONS
#############
#  SNMP     #
#############
snmp
#################
#  ROUTING      #
#################
rtg
    # LOG SERVICE
    # GLOBAL INFO
    # ACCESS LIST & PREFIX LIST
    # COMMUNITY-LIST & EXTCOMMUNITY-LIST
    # ROUTE-MAPS
    # INTERFACES
    # DYNAMIC ROUTING
#############
#    FIL    #
#############
fil
###########
#  NTP    #
###########
ntp
    # NTP STATEMENTS
      ntp disable
      default-version 4
      default-polling 8
    # REMOTE SERVERS
    # LOG SERVICE
      log ntp NTP info
```

```
###############
#   LOOPBACK   #
###############
###########
#  GEN    #
###########
gen
    # GEN STATEMENT
      hostname SP
      clock timezone UTC
      telnet enable
      ssh disable
      icmp limit rate 1000
      icmp limit type unreach quench redirect time_exceed param_prob

    # ARP TABLE
    # NDP TABLE
    # HOST
###############
#   NETFLOW   #
###############
netflow
    # NETFLOW STATEMENTS
      netflow ipv4 enable
      netflow mac enable expire-time 30 60 60
      exclude-field ipv4 src-ip

    # ADVANCED
      adjust-in-bytes-field 24
      ipv4-prefix-mask dst-ip 24
      vlan-tpid 0x1111 0x2222 0x3333

    # TRAFFIC MONITOR PORT
      traffic-monitor-port eth4

    # DENY FILTER
      deny-filter eth4 broadcast

    # MANAGEMENT PORT
      mgmt-port eth2

    # OUTPUT PORT
      output-port eth1
      # FLOW INFORMATION
        flow ipaddress 192.168.100.200 port 9996
        flow ipaddress 192.168.100.210 port 9996 mac


[SP]
```

7 トラブル発生時の対応

この章では，トラブル発生時の対応について説明します。

7.1 装置の問題，障害発生時の対応

(1) 本装置の電源が入らない

本装置の電源を OFF にし，電源ケーブルの接続および電源設備を確認してください。

電源ケーブルの接続および電源設備に問題がなく，本装置の電源が入らない場合は販売店に連絡してください。

(2) ログインパスワードのトラブル

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

1. 装置管理者へ連絡してください。
2. 運用コマンド「edit system users」でログインユーザのパスワードを変更してください。パスワードの変更は装置管理者が実施してください。

装置管理者がパスワードを失念・紛失した場合は販売店に連絡してください。

(3) ハードウェア，ソフトウェアの障害による再起動

ハードウェアやソフトウェアの障害により，自動で本装置の再起動が行われることがあります。その場合は障害情報を保存した後に再起動しますので，起動完了後に障害情報を取得してください。取得した障害情報は装置管理者に送付してください。障害情報の取得方法は「7.2 障害情報取得方法」を参照してください。

(4) 接続したケーブルを見直してもインタフェースがリンクアップしない

接続したケーブルのインタフェースがリンクアップしない場合は以下の手順で対応してください。

1. 本装置の物理インタフェースのコンフィグレーションに「interface down」が設定されていないか確認してください。「interface down」となっている場合はコンフィグレーションで「interface up」に設定してください。
2. 隣接装置のインタフェース設定が固定モードとなっていないか確認してください。本装置の 1G インタフェースは 10/100/1000Mbps のオートネゴシエーションのみに対応しています。

(5) ジャンボフレームの NetFlow 情報だけが出力されない

モニタポートの mtu 設定を適切な値に設定してください。

(6) プロンプトに「You have warning messages. Use "show sp" to see them.」のメッセージが出力される。

運用コマンド「show sp」を実行して WARNING の内容を確認してください。WARNING の詳細は AX-Sensor コマンド・ログレファレンスの「表 1.2-5 show sp で表示される(2)の WARNING 一覧」を参照してください。

7.2 障害情報取得方法

障害情報の取得方法について説明します。

下記手順にしたがって解析情報ファイルを取得してください。

1. 装置管理者モードでログインしてください。
2. 運用コマンド「show tech-support」を実行してください。
3. 運用コマンド「export dump-file」を実行してください。

実行すると取得可能な解析ファイルを収集し，エクスポートまでが行われます。解析情報の取得にはネットワークを経由してエクスポートを行います。

ネットワークを経由してエクスポート

コマンド「export dump-file」のパラメータにURLを指定することでネットワーク経由でのエクスポートを実施します。ftp(またはtftp)を利用してのファイル転送ですので，エクスポート先となる機器でftp(またはtftp)サーバが起動している必要があります。

※本装置のftp/tftpサーバは起動していないため，外部から本装置へのftp/tftp接続はできません。

7.3 本装置の再起動

障害が回復しない場合は，本装置の再起動により回復する可能性があります。

下記手順にしたがって本装置を再起動してください。

1. 装置管理者モードでログインしてください。
2. 運用コマンド「reload」を実行してください。

リモート端末，コンソールのどちらからもログイン，操作ができない場合，リセットボタンを押すことで再起動が可能です。

8 注意事項

この章では，注意事項について説明します。

8.1 注意事項

8.1 注意事項

(1) 運用コマンド「show netflow statistics detail」のカウンタに関する注意事項

・Total の「Received Packets」「Received Bytes」がカウントアップされない。

観測対象ネットワークからトラフィックを受信していない可能性があります。モニタポートのコンフィグレーション設定，または物理インタフェースの設定および統計情報を確認してください。

・各フロー条件の「Overflow Packets」がカウントアップされる

フローエントリ数超過によりエントリが登録できません。コンフィグレーション「flow-max-entry」の設定で最大エントリ数の設定を見直してください。

・各フロー条件の「Discard Flows」がカウントアップされる。

ライセンスが設定されているか確認してください。

センサ出力ポートに送信先(コレクタ)のコンフィグレーション設定がされているか確認してください。

観測対象ネットワークからトラフィック受信中にコンフィグレーション「netflow」で集約フローを disable の設定にしていないか確認してください。

・Collector の「Discard Packets」，「Discard Templates」，「Discard Flows」がカウントアップされる

センサ出力ポートがリンクダウンしていないか確認してください。

運用コマンド「show ip route」でセンサ出力ポートと送信先(コレクタ)のルーティングテーブル情報が正しいか確認してください。

(2) モニタポート設定における注意事項

センサ出力ポートおよびマネジメントポートで使用していたインタフェースを IP アドレスの削除を行わないでモニタポートに設定した場合，該当インタフェースに ARP エントリが存在する間は，モニタポートからパケットが出力されます。

付録

付録A　準拠規格

付録A.1　NetFlow

表 A-1 NetFlow の準拠規格および勧告

規格番号(発行年月)	規格名
RFC3954(2004 年 10 月)	Cisco Systems NetFlow Services Export Version 9

付録A.2　SSH

表 A-2 SSH の準拠規格および勧告

規格番号(発行年月)	規格名
RFC4250(2006 年 1 月)	The Secure Shell (SSH) Protocol Assigned Numbers
RFC4251(2006 年 1 月)	The Secure Shell (SSH) Protocol Architecture
RFC4252(2006 年 1 月)	The Secure Shell (SSH) Authentication Protocol
RFC4253(2006 年 1 月)	The Secure Shell (SSH) Transport Layer Protocol
RFC4254(2006 年 1 月)	The Secure Shell (SSH) Connection Protocol
RFC4256(2006 年 1 月)	Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)
RFC4335(2006 年 1 月)	The Secure Shell (SSH) Session Channel Break Extension
RFC4344(2006 年 1 月)	The Secure Shell (SSH) Transport Layer Encryption Modes
RFC4419(2006 年 3 月)	Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
RFC4716(2006 年 11 月)	The Secure Shell (SSH) Public Key File Format
RFC5656(2009 年 12 月)	Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer
RFC6668(2012 年 7 月)	SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol
RFC8270(2017 年 12 月)	Increase the Secure Shell Minimum Recommended Diffie-Hellman Modulus Size to 2048 Bits
RFC8308(2018 年 3 月)	Extension Negotiation in the Secure Shell (SSH) Protocol
RFC8332(2018 年 3 月)	Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol
RFC8709(2020 年 2 月)	Ed25519 and Ed448 Public Key Algorithms for the Secure Shell (SSH) Protocol
RFC8731(2020 年 2 月)	Secure Shell (SSH) Key Exchange Method Using Curve25519 and Curve448

付録A.3　NTP

表 A-3 NTP の準拠規格および勧告

規格番号(発行年月)	規格名
RFC1305(1992 年 3 月)	Network Time Protocol (Version 3) Specification, Implementation and Analysis
RFC5905(2010 年 6 月)	Network Time Protocol Version 4: Protocol and Algorithms Specification

付録A.4　SYSLOG

表 A-4 SYSLOG の準拠規格および勧告

規格番号(発行年月)	規格名
RFC3164(2001 年 8 月)	The BSD syslog Protocol

付録A.5　イーサネット

表 A-5 イーサネットインタフェースの準拠規格および勧告

種別	規格	規格名
10BASE-T, 100BASE-TX, 1000BASE-T,	IEEE802.3 2008 Edition	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer Specifications
10GBASE-R	IEEE802.3ae Standard-2002	Media Access Control(MAC) Parameters, Physical Layer, and Management Parameters for 10Gb/s Operation

付録A.6　SNMP

表 A-6 SNMP の準拠規格および勧告

規格番号(発行年月)	規格名
RFC1901(1996 年 1 月)	Introduction to Community-based SNMPv2
RFC1902(1996 年 1 月)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1903(1996 年 1 月)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1904(1996 年 1 月)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1905(1996 年 1 月)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1906(1996 年 1 月)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1907(1996 年 1 月)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1908(1996 年 1 月)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework

付録A.7　MIB

表 A-7 MIB の準拠規格および勧告

規格番号(発行年月)	規格名
RFC1213(1991 年 3 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC2863(2000 年 6 月)	The Interfaces Group MIB
RFC3418(2002 年 12 月)	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC3635(2003 年 9 月)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC4022(2005 年 3 月)	Management Information Base for the Transmission Control Protocol (TCP)
RFC4113(2005 年 6 月)	Management Information Base for the User Datagram Protocol (UDP)
RFC4293(2006 年 4 月)	Management Information Base for the Internet Protocol (IP)