データシート
ネットワークマネジメント製品

AX-Network-Manager

1. 概要

1.1 AX-Network-Manager の位置づけ

AX-Network-Manager は，ネットワーク運用を支援するネットワーク運用管理ソフトウェアです。ネットワーク運用は一般的に，

・通常運用時の稼働状況把握
・改組などによるネットワーク構成変更
・障害・インシデント発生時の切り分け・対応

を行います。これらを行うには，

・日々変わるネットワーク構成や端末位置の把握に時間を要する
・発生している障害事象やインシデント問題の把握と対応に時間を要する
・機器ごとに異なる設定方法の未把握など，運用に関するスキルが不足している
・機器障害発生時に迅速な復旧ができない
・ネットワーク機器ごとに管理が分かれていて，管理が難しい

という課題がありました。この課題に対して，AX-Network-Manager は，以下を提供します。

・ネットワークの構成管理（状態・設定の一元管理，端末位置可視化）
  - CAPWAP によりカプセル化された無線 LAN 端末位置の可視化
・作業者の要求スキル・負荷軽減
  - GUI によるネットワーク状態の把握，設定による操作の簡易化
  - ドキュメント出力機能
・マルチベンダ対応
・セキュリティ機器連携によるインシデント対策

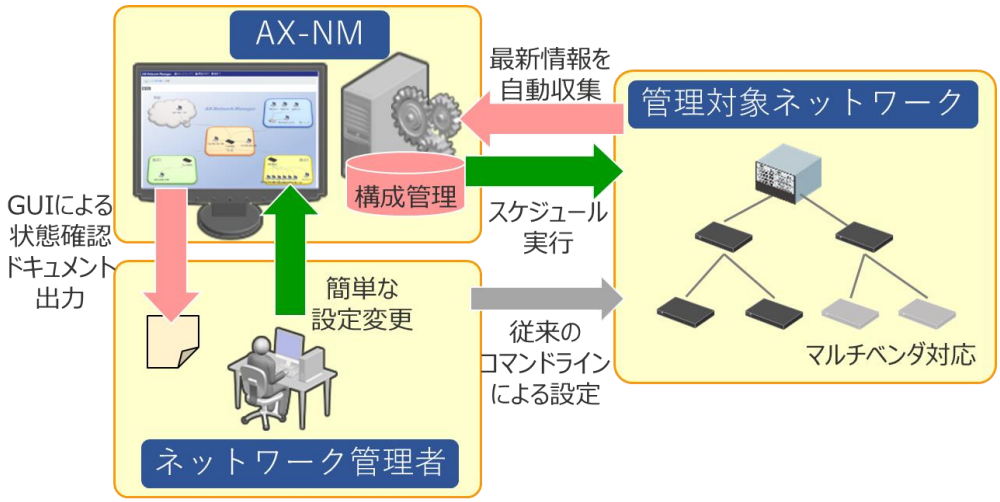

図 1-1 AX-Network-Manager による運用概要

1.2 AX-Network-Manager の特長

1.2.1 ネットワークの構成管理（状態・設定の一元管理）

AX-Network-Manager は，ネットワークの状況を自動的に収集して一元的に管理することができるネットワーク運用管理ソフトウェアです。機器のインタフェース，接続などネットワークの状態を把握できるとともに，機器を構成するハードウェアの状態も把握できます。

これまでネットワークの構成情報はドキュメントとして管理されることが多く，実態との差分が生じる場合もありました。AX-Network-Manager は，最新状況を一元的に管理することで稼働状況を容易に把握でき，障害発生時の切り分けにも役立てることが可能です。

1.2.2 作業者の要求スキル・負荷軽減

AX-Network-Manager は，ネットワークの状況を自動的に収集して一元的に管理した情報を，トポロジーマップやフロントパネルといった GUI を使って表示する機能を備えたネットワーク運用管理ソフトウェアです。文字情報とともにトポロジーマップやフロントパネルといった GUI から状況を把握できることで運用者の負担軽減，運用者に求められるスキルの低減が可能になります。また，ネットワークの構成情報をドキュメントとして別途作成していたものを一元的に管理した情報から出力することでも負担軽減が可能になります。

また，操作者ごとにユーザ権限を指定して運用，操作を把握，発生したイベントへの対応状況を管理することが可能で，ダッシュボードを複数パターンで作成し，複数人での管理にも対応します。

このように，AX-Network-Manager はネットワーク運用に不慣れなユーザでも運用管理を行うことが可能です。

1.2.3 マルチベンダ対応

AX-Network-Manager は，マルチベンダに対応したネットワーク運用管理ソフトウェアです。
ネットワークは複数ベンダの機器により構成されることが一般的です。AX-Network-Manager は，標準的な MIB をサポートする機器であればアラクサラ以外の機器でも管理対象機器として機器状態を監視できるため，既存システムの資産を生かしつつ，運用管理を行うことが可能です。

また，ネットワーク機器だけでなく，サーバや監視カメラ，IoT 機器などを Ping や任意の MIB にて状態監視することができるため，ネットワーク全体の運用管理を行うことも可能です。

また，機器ごとに異なる操作を AX-Network-Manager に一本化でき，運用者に求められるスキルの低減が可能になります。

1.2.4 CAPWAP によりカプセル化された無線 LAN 端末位置の可視化

AX-Network-Manager は，CAPWAP プロトコルによりワイヤレス LAN コントローラとアクセスポイント間で通信をおこなうネットワーク環境において，無線 LAN 端末の位置を可視化可能なネットワーク運用管理ソフトウェアです。

1.2.5 セキュリティ機器連携によるインシデント対策

AX-Network-Manager は，アプリケーションレイヤのセキュリティ制御を担うセキュリティ機器と連携することで，インシデント発生部位に対する通信遮断等のネットワークレイヤの制御をおこなうネットワーク運用管理ソフトウェアです。

2. 特徴

2.1 AX-Network-Manager の構成

AX-Network-Manager の機能概要を示します。

2.1.1 ネットワーク管理

AX-Network-Manager は，管理対象とする機器を含むネットワークを管理する機能を提供します。

(1) 機器管理

AX-Network-Manager は，管理対象機器から定期的に情報を収集し，機器の状態を管理する機能を提供します。主な提供機能は，以下のようになります。

表 2-1 機器管理の主な提供機能

項目	説明
機器情報の表示	機器情報を定期的に取得し，状態等を表示します。 管理対象機器からの情報取得は，MIB によるアクセス，または SSH/Telnet による運用コマンド実行結果より取得します。 機器の状態は以下となります。 ・初期収集中 機器追加や AX-Netowrk-Manager 起動直後の情報収集中の場合 ・正常 機器情報が取得できている場合 ・障害(<要因>) <要因>：要因を並べて表示します。 ・ハードウェア異常：ハードウェアで継続運用ができない異常が発生している場合 ・収集失敗：機器からの情報収集が失敗している状態 ・軽度障害(<要因>) <要因>：要因を並べて表示します。 ・ハードウェア異常：ハードウェアで異常は発生しているが，継続運用はできる状態 ・L2 ループ発生：L2 ループが発生している場合 ・ストーム発生：ストームが発生している場合 ・輻輳発生： 輻輳が発生している場合 ・注意(<要因>) <要因>：要因並べて表示します。 ・ハードウェア異常：ハードウェアで警告レベルの異常が発生している状態 ・ハードウェア状態不明：機器の起動中など不確定な状態の場合 ・ライセンス無効 有効なライセンスが割り当てられていない場合 ・ライセンスなし ライセンスなしに設定している場合
ハードウェア情報の表示	機器を構成するハードウェア情報を表示します。 管理対象機器からの情報取得は，MIB によるアクセスにより定期的に取得します。また，ハードウェアの稼働状態，温度状態は機器から送出される SNMP トラップ・インフォーム，syslog 情報を受信した契機でも MIB によるアクセスを行い，最新の状態に反映します。

インタフェース情報の表示	機器のインタフェース情報を表示します。インタフェース単位に状態，および使用帯域を表示します。また，インタフェースの接続先を記載するなど，管理を助けるコメントを付与することができます。インタフェースの状態には，機器から送出される Trap 情報も反映します。
チャネルグループ情報の表示	機器のチャネルグループ情報を表示します。チャネルグループ単位に状態を表示します。また，チャネルグループの接続先を記載するなど，管理を助けるコメントを付与することができます。
フロントパネルの表示	機器のフロントパネルを模した画像上にインタフェース情報を表示します。対象機種は 5.3.5(1)フロントパネル表示対応機器に示します。

(2) Web ターミナル

Web ターミナルは，ウェブブラウザにより，機器へのログインとユーザによる操作を可能とする機能です。機器へのログインは，下記 2 つのプロトコルのいずれかを使用することができます。

表 2-2　機器ログインの使用プロトコル

プロトコル	説明
SSH	機器へのログインに SSH を使用します。機器に設定したユーザ名とログインパスワードを使用して，機器へと自動的にログインします。
Telnet	機器へのログインに Telnet を使用します。機器へのログインには，ユーザによりユーザ名とパスワードを入力する必要があります。

本機能を使用すると，ユーザのクライアント環境に端末エミュレータのソフトウェアをインストールすることなく，機器を操作することができます。また，ネットワーク管理者のネットワークと，管理対象機器のネットワークが VRF により分離されているような環境で，ネットワーク管理者が直接管理対象機器への到達性がない環境においても，ウェブブラウザだけで機器を操作することができます。

※オンプレミス版では，NIC を 2 枚用意して頂くことで，VRF 等ネットワーク分離された環境でもウェブブラウザだけで機器を操作することが可能となります。クラウド版では仮想 NIC が 1 枚の環境を提供する為，本動作はできません。

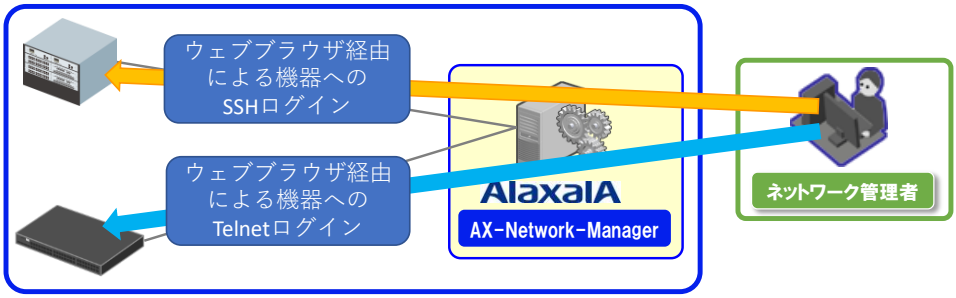

図 2-1　Web ターミナル利用例

本機能を利用するには，AX-Network-Manager が動作するオペレーティングシステム上で，値が 1024 以上である 1 つの TCP ポート番号が必要であり，インストール時に設定します。

(a)　使用上の注意事項

・　Web ターミナル上で操作をおこなわない時間が 300 秒を越えると，自動的に機器から

ログアウトします。

- Telnet により機器にログインした状態で，Web ターミナル上で Ctrl-Z を押下すると，機器への操作が中断します。fg コマンドを投入して再開してください。
- AX-Network-Manager が動作するオペレーティングシステム上の SSH の暗号方式/鍵交換方式と，機器の暗号方式/鍵交換方式が 1 つも一致しない場合，Web ターミナルによる SSH を使用した機器へのログインをおこなうことができません。この場合，機器の設定を変更するか，AX-Network-Manager が動作するオペレーティングシステム上の SSH クライアントコンフィグレーションファイル(.ssh/config，または /etc/ssh/ssh_config))の設定を変更してください。AX-Network-Manager Web ターミナル実行ユーザの SSH クライアントコンフィグレーションファイルに，198.51.100.1 への暗号方式 aes128-ctr，aes128-cbc を許容する設定例を下記に示します。SSH クライアントコンフィグレーションファイルの詳細は，AX-Network-Manager が動作するオペレーティングシステム上で man ssh_config を実行して，ご確認ください。

```
Host 198.51.100.1
        Ciphers aes128-ctr,aes128-cbc
```

(3) L2 ループ検知

AX-Network-Manager は，機器から L2 ループ検知情報を定期的に収集し，表示します。インタフェース，またはチャネルグループ単位に情報を表示します。また，L2 ループの検知，および自動遮断検知を受信し，L2 ループ検知情報に反映します。

主な提供機能は，以下のようになります。

表 2-3　L2 ループ検知の主な提供機能

項目	説明
L2 ループ検知情報状態表示	Web インタフェース上に L2 ループ検知情報を表示します。機器単位，およびインタフェース単位に表示します。
L2 ループ検知/自動遮断検知	機器からのトラップおよび syslog※受信により，L2 ループの発生検知を行います。また，機器の L2 ループ発生時自動遮断機能によるインタフェース遮断通知も受信し，L2 ループ状態を更新します。 ※AX8600S/AX8300S は syslog，それ以外の L2 ループ検知サポート機器はトラップで検知を行います。
遮断ポートの自動復旧	検知送信閉塞ポートが L2 ループ発生により遮断された場合，そのポートを一定時間経過後に自動的に復旧します。ユーザが自動復旧と手動復旧を時間帯によって切り替えられるように，自動復旧スケジュールを設定できます。 なお，機器の自動復旧機能とは同時に使用しないでください。

(4) ストーム検知

AX-Network-Manager は，機器からストームの通知を受信し，機器およびインタフェース単位にストームの発生状態を表示します。

主な提供機能は，以下のようになります。

表 2-4 ストーム検知の主な提供機能

項目	説明
ストーム検知情報表示	Web インタフェース上にストーム検知情報を表示します。機器単位，およびインタフェース単位に表示します。

項目	説明
ストーム情報検知	機器からのインフォーム，およびトラップ受信により，ストームの発生・復旧検知を行います。取りこぼしを防ぐため，インフォームをサポートしている機器はインフォームでの通知を推奨します。

(5) 輻輳管理

AX-Network-Manager は，機器の輻輳情報を受信し，機器単位に輻輳の発生状態を表示します。また，輻輳発生要因を解析するための情報としてパケット情報を表示します。

主な提供機能は，以下のようになります。

表 2-5 輻輳管理の主な提供機能

項目	説明
輻輳情報表示	Web インタフェース上に輻輳の発生状態を表示します。 機器単位でユーザに対して輻輳発生を表示します。
輻輳発生・復旧検知	syslog 受信により，輻輳の発生・復旧の検知を行います。受信した syslog を解析し，発生部位を特定します。
輻輳解析情報取得	輻輳発生要因の解析に必要な情報を取得します。 輻輳検知時： 　輻輳が発生したスイッチの輻輳解析情報を取得します 手動取得時： 　マスタスイッチから輻輳解析情報を取得します 輻輳情報解析を目的に，ローカルに保存した輻輳解析情報をアップロードすることも可能です。
輻輳情報解析	取得した輻輳解析情報の詳細表示，およびダウンロードを行えます。詳細表示では輻輳発生要因となったパケット情報の一覧を表示します。また，輻輳解析結果は CSV 形式でのダウンロードも行えます。

輻輳解析情報は，機器モデルごとに以下の方法で取得します。

表 2-6　輻輳解析情報の取得方法

機器モデル	取得方法
AX2500S シリーズ AX260A シリーズ	機器の CPU が大量のパケットを受信したときの受信パケットの内容（先頭の 64 バイト）を取得します。 show receive alarm dump ※コマンド出力結果をテキストとして保持します
AX3600S シリーズ AX3800S シリーズ AX4600S シリーズ	ネットワーク管理モジュールおよびＳＷ部の情報を取得します。 /usr/local/diag/nimdump ※gzip で圧縮してファイル化し，ファイルを転送します
AX2600S シリーズ AX2300S シリーズ	ネットワーク管理モジュールおよびＳＷ部の情報を取得します。 /usr/local/diag/nimdump ※コマンド実行後に出力されるファイルを転送します

(6) スタック切替監視

AX-Network-Manager は，管理対象機器のマスタスイッチ番号を監視し，スタック切替の発生を管理します。

主な提供機能は，以下のようになります。

表 2-7　スタック切替管理の主な提供機能

項目	説明
マスタスイッチ情報表示	Web インタフェース上にマスタスイッチを表示します。
スタック切替発生検知	MIB 情報からマスタスイッチ番号を取得し，マスタスイッチ番号が変わった際にスタック切替が発生したと判断します。また，coldstart のトラップを受信した契機において MIB を収集し，切替の判定を行います。

(7) 接続管理

AX-Network-Manager は，LLDP による自動検出より 2 つの機器間の接続関係を把握します。管理対象機器から定期的に情報を収集し，機器間の接続の状態を管理する機能を提供します。主な提供機能は，以下のようになります。

表 2-8　接続管理の主な提供機能

項目	説明
LLDP による接続検出	LLDP による機器の隣接情報を収集し，機器間の接続情報を自動で検出します。 一度検出した機器間の接続情報が不要になった場合は，Web インタフェースから削除できます。
自動検出アルゴリズムによる接続検出	機器から収集した情報を元に，機器間の接続情報を自動で検出します。自動検出した接続情報を登録する際に，接続先の機器がアクセスリストを設定できない機種の場合にアクセスリスト拡張ポートの設定を有効にすることができます。また，検出の精度を上げるために機器へと探索用の UDP パケット(ポート 7 番宛)を送信する機能※をサポートしています。
静的なポート接続情報の設定	LLDP が動作しない機器間の接続情報を Web インタフェースにより手動で設定，削除できます。
接続状態の表示	LLDP による接続検出，および静的なポート接続情報の設定により設定された機器間の接続の状態を表示します。

※：AX-Network-Manager から探索用パケットを送信するため，管理用ネットワークとユーザ収容しているネットワークが VRF などで通信できない場合には利用できません。また，AX-Network-Manager を動作させているサーバに端末への経路が登録されている必要があります。

(8) 端末管理

AX-Network-Manager は，機器管理および接続管理で定期的に収集する情報（下表参照）を利用してネットワークトポロジを把握します。把握したトポロジより，端末が，管理対象機器のポートに収容しているかを Web インタフェースにより表示することができます。

表 2-9 端末位置を把握するために使用する情報

情報
LLDP またはユーザ入力の接続情報
自動検出アルゴリズムで検出した接続情報
VLAN 複数収容ポート

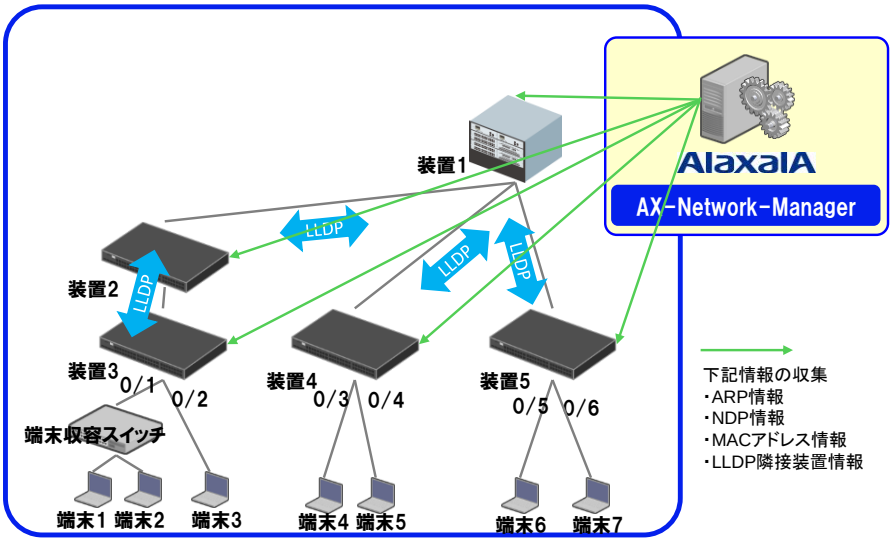

図 2-2 端末管理

上図において，AX-Network-Manager は，端末の位置を以下のように把握しています。

表 2-10 端末の位置の把握例

端末	収容管理対象機器	収容ポート
端末 1	機器 3	0/1
端末 2		
端末 3	(機器 6(WLC))	0/2
端末 4	機器 4	0/3
端末 5		0/4
端末 6	機器 5	0/5
端末 7		0/6

また，端末の IP アドレス，MAC アドレスについて，呼応する端末の名称，利用者，および連絡先などをエイリアスとして登録し，表示することができます。エイリアスには，タイトルと値の組み合わせを複数登録することが可能です。これにより，ネットワーク管理者は，端末の情報を IP アドレス，MAC アドレスだけでなく，エイリアス内容により確認することが可能です。

なお管理対象外ポート管理を設定することにより，機器のポートやチャネルグループで学習した MAC アドレスを，端末として管理しないようにすることが可能です。

(9) 端末接続履歴

AX-Network-Manager は，端末管理で定期的に収集した情報に基づき，各端末の接続履歴を算出します。算出される情報の詳細を下表に示します。

表 2-11　接続履歴に含まれる情報

項目	説明
接続開始日時	端末情報(IPv4 アドレス)，端末情報(IPv6 アドレス)，端末情報(MAC アドレス)の定期収集にて，新たな情報が収集された時刻（秒単位）
端末情報	通信開始時刻に新たに収集された端末のアドレス（MAC アドレス，ベンダ，IP アドレス，エイリアス）
位置情報	通信開始時刻に端末が存在しているネットワーク上の場所（接続先機器，接続先ポート名，VLAN，接続先 AP）
接続終了日時	通信開始時刻に収集された情報が，以降の定期収集で収集されなくなった時刻（秒単位）
接続期間	通信終了時刻と通信開始時刻の差（秒単位）

なお，下記のようなケースでは，新たな接続履歴を作成し，端末単位の通信開始および終了時刻の履歴を管理します。

- 通信終了した端末が，通信を再開
- 通信中の端末が，接続履歴とは異なるアドレスで通信実施
- 通信中の端末が移動して，異なるポートから通信実施

(10) 経路管理

AX-Network-Manager は，機器から取得する MIB により経路情報を把握します。管理対象機器から定期的に情報を収集し，経路情報を管理する機能を提供します。主な提供機能は，以下のようになります。

表 2-12　経路管理の主な提供機能

項目	説明
経路情報の収集	機器がもつ経路情報を MIB により収集します。 一度検出した経路情報が不要になった場合は，Web インタフェースから削除できます。
静的な経路情報の設定	通常運用時には生成されない代替経路情報などを Web インタフェースにより手動で設定，削除できます。
経路情報の表示	機器から MIB により収集した経路情報，および静的な経路情報の設定により設定された経路情報を表示します。

(11) フィルタ管理

AX-Network-Manager は，コンフィグ管理で収集した情報に基づき，各機器のフィルタ情報を解析します。また，主な提供機能は，以下のようになります。

表 2-13　フィルタ管理の主な提供機能

項目	説明
フィルタ情報の表示	コンフィグ管理による機器からスタートアップコンフィグレーション取得時にフィルタ情報を解析し表示します。以下のフィルタ情報に対応します。 ・アクセスリスト フィルタ種別 IPv4 アドレスフィルタ IPv4 パケットフィルタ IPv6 フィルタ MAC フィルタ Advance フィルタ ・フィルタ有効化・無効化 イーサネットインタフェース VLAN インタフェース イーサネットサブインタフェース ポートチャネルサブインタフェース
フィルタ情報の編集	アクセスリスト設定，フィルタ有効化・無効化に使用するフィルタ情報を編集します。機器から取得したフィルタ情報，または新規にフィルタを作成し，編集します。 アクセスリストは複数の機器に反映できるため，同じポリシーの機器に使用できます。 検出条件はシーケンス番号毎に許可/拒否，プロトコル，送信元/宛先 IP アドレスやポート番号を入力します。機器モデル毎にコンフィグに差分があるため，任意の追加コンフィグ入力や任意のコンフィグ直接入力もサポートします。
フィルタ情報の機器反映	フィルタ情報の編集により作成したフィルタ情報を機器に反映します。 フィルタ有効化・無効化はイーサネットインタフェース，または VLAN を選択して設定できます。
フィルタ情報カウンタ収集	登録されたフィルタ情報の統計値を収集し，グラフ表示します。

(12) QoS 管理

AX-Network-Manager は，コンフィグ管理で収集した情報に基づき，各機器の QoS 情報を解析します。また，主な提供機能は，以下のようになります。

表 2-14　QoS 管理の主な提供機能

項目	説明
QoS 情報の表示	コンフィグ管理による機器からスタートアップコンフィグレーション取得時に QoS 情報を解析し表示します。以下の QoS 情報に対応します。 ・QoS フローリスト種別 IPv4QoS フローリスト IPv6QoS フローリスト MACQoS フローリスト AdvanceQoS フローリスト ・QoS 制御有効化・無効化 イーサネットインタフェース VLAN インタフェース イーサネットサブインタフェース ポートチャネルサブインタフェース
QoS 情報の編集	QoS フローリスト設定，QoS 制御有効化・無効化に使用する QoS 情報を編集します。機器から取得した QoS 情報，または新規に QoS 情報を作成し，編集します。 QoS フローリストは複数の機器に反映できるため，同じポリシーの機器に使用できます。 検出条件はシーケンス番号毎にプロトコル，送信元/宛先 IP アドレスやポート番号を入力します。機器モデル毎にコンフィグに差分があるため，任意の追加コンフィグ入力や任意のコンフィグ直接入力もサポートします。
QoS 情報の機器反映	QoS 情報の編集により作成した QoS 情報を機器に反映します。 QoS 制御有効化・無効化はイーサネットインタフェース，または VLAN を選択して設定できます。
QoS カウンタ収集	登録された QoS 情報の統計値を収集し，グラフ表示します。

(13) ポートミラーリング管理

AX-Network-Manager は，コンフィグ管理で収集した情報に基づき，各機器のポートミラーリング情報を解析します。また，主な提供機能は，以下のようになります。

表 2-15　ポートミラーリング管理の主な提供機能

項目	説明
ポートミラーリング情報の表示	コンフィグ管理による機器からスタートアップコンフィグレーション取得時にポートミラーリング情報を解析し表示します。以下のポートミラーリング情報に対応します。 ・方向 受信，送信，送受信 ・ポートミラーリング適用インタフェース イーサネットインタフェース ポートチャネルインタフェース
ポートミラーリング情報の編集	ポートミラーリング情報を編集します。機器から取得したポートミラーリング情報，または新規にポートミラーリング情報を作成し，編集します。 ポートミラーリング情報は複数の機器に反映できるため，同じポリシーの機器に使用できます。 追加コンフィグもサポートします。

項目	説明
ポートミラーリング情報の機器反映	ポートミラーリング情報の編集により作成したポートミラーリング情報を機器に反映します。

(14) ネットワークトポロジのビジュアル表示（マップ）

機器管理，接続管理，および端末管理により把握したネットワークトポロジを，マップとしてビジュアル的に表示します。主な提供機能は，以下のようになります。

表 2-16　マップの主な提供機能

項目	説明
管理対象（機器，端末，接続，VLAN，L2 ループ検知，経路，VXLAN，監視対象）の表示	管理対象を文字情報による一覧表示でなく，アイコンを用いてビジュアル的に表示します。接続も含めて表示することで，ネットワークトポロジの把握を助けます。 アイコンを操作することにより，配置の操作や，位置を保存することができ，ユーザの理解しやすいように表示することが可能です。なお，アイコンの画像は自由にカスタマイズできます。 端末は，MAC アドレス単位に 1 つの端末として扱います。 監視対象は，ホスト名×IP アドレス単位に 1 つの端末として扱います。
管理対象（機器，端末，接続，VLAN，経路，VXLAN，監視対象）の情報および状態表示	機器，接続の状態を，機器や接続単独ではなく，それらをまとめたマップとして表示することで，状況把握を助けます。 機器の状態は機器状態を示すアイコンでわかりやすく表示し，クリックすることで情報表示画面に状態を表示，そこから機器詳細を表示することが可能です。
背景画像の指定	位置が把握できるような背景画像を用意し，管理対象として登録する機器，端末，接続をその背景画像上にプロットすることで，どの位置にあるかの把握を助けます。
複数マップ（マップの分割）	機器が多くなると 1 つのマップでは管理が困難になることから，分割して管理できるよう，複数のマップを持つことができます。 1 つの機器を複数のマップに表示することで，マップを容易に切り替えられるようになっており，マップが複数に分割されてもネットワーク構成全体を追っていきやすくなっています。

2.1.2　ネットワーク管理(セキュリティ機器連携)

(1) 概要

標的型攻撃を始めとするサイバー攻撃は，近年ますます巧妙化しており，組織内へのマルウェアの侵入を完全に防ぐことは困難になりつつあります。

万一の侵入に備え，インシデントの早期発見と迅速な初動対応による被害の最小化を図ることが課題です。

この課題への対策として，AX-Network-Manager は，アプリケーションレイヤのセキュリティ制御を担うセキュリティ装置と連携することで，インシデント発生部位に対する通信遮断等のネットワークレイヤの制御機能を提供します。

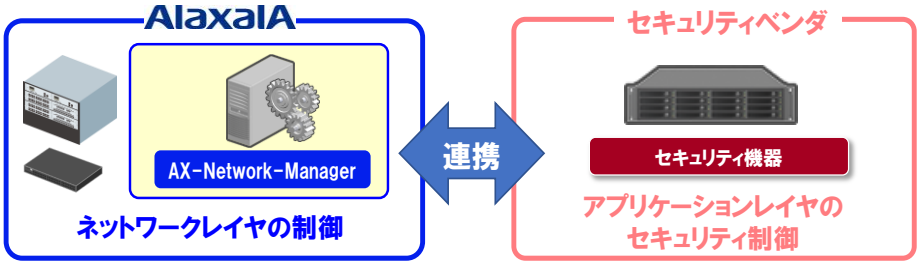

図 2-3　AX-Network-Manager－セキュリティ機器連携

AX-Network-Manager は以下の 2 通りの方法でセキュリティ機器と連携することができます。

(a)　インシデント情報連携

インシデント情報連携は，受信したインシデント情報を取捨選択して，対策の必要なインシデントのみに対策を実施する機能です。具体的には以下の機能を提供します。

- インシデント情報を取捨選択する条件を定義したインシデント抽出ルールの設定
- インシデント抽出ルールのアクションとしてインシデント対策連携と連動が可能

(b)　インシデント対策連携（セキュリティフィルタ）

セキュリティフィルタは，セキュリティ装置がインシデント情報に基づき算出した対策指示に従い，インシデント対策を実施する機能です。具体的には以下の機能を提供します。

- マルウェアに感染した端末の物理的な位置を特定し，感染端末の通信を自動的に遮断
- 端末と攻撃サーバ(C&C サーバ等)間の通信を遮断
- 感染端末がネットワーク内を移動しても，追従して遮断
- DHCP を利用した環境において，感染端末の IP アドレスが変更されても，追従して遮断

AX-Network-Manager とセキュリティ機器が連携した際の動作イメージを下図に示します。

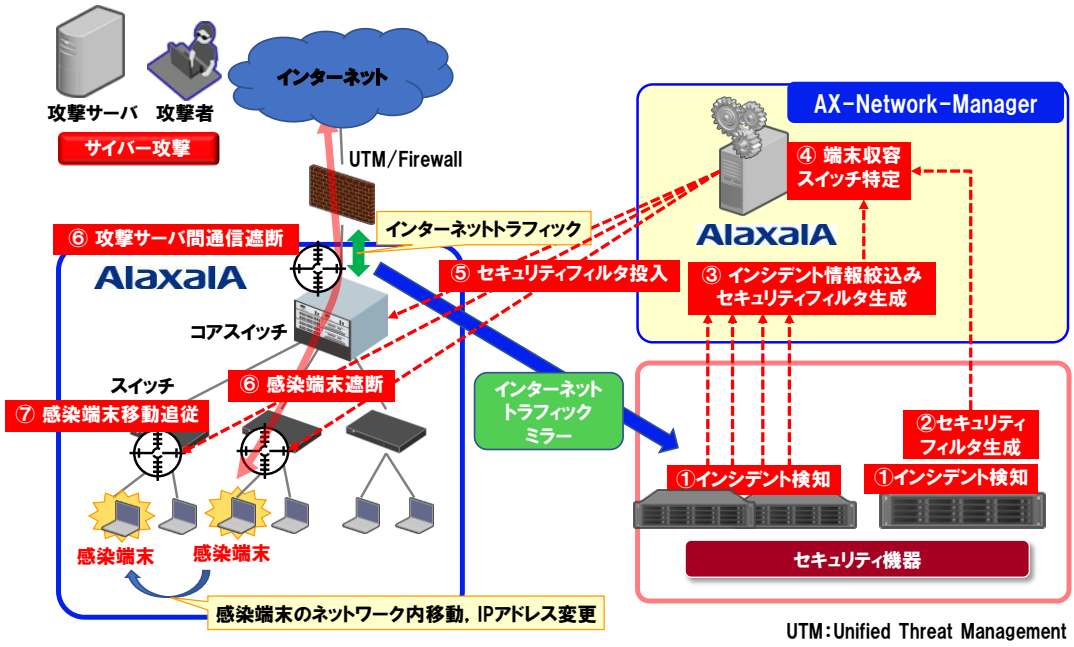

図 2-4　AX-Network-Manager－セキュリティ機器連携動作イメージ

(c) 使用上の注意事項

セキュリティ機器連携を使用する場合，設定ファイルの SYNC_ACCESSLIST を TRUE に設定し，AX-Network-Manager を再起動してください。

(2) ネットワーク構成と用語

(a) ネットワーク構成

セキュリティ機器連携を使用する上で，AX-Network-Manager が前提とするネットワーク構成を下記に示します。

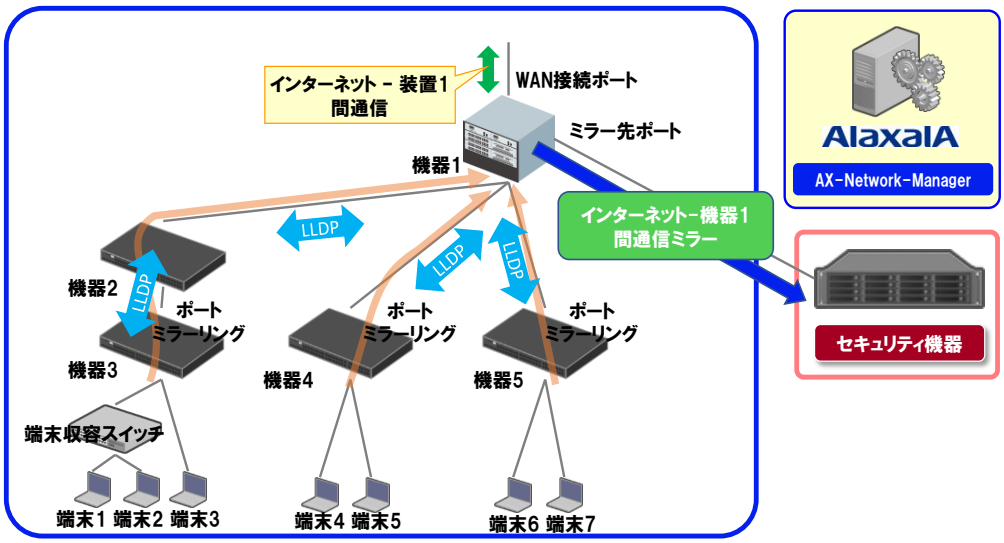

図 2-5 前提とするネットワーク構成

(b) セキュリティ機器

AX-Network-Manager が連携する下表のセキュリティ機器を網内に配備する必要があります。

表 2-17 セキュリティ機器

連携方式	セキュリティベンダ	セキュリティ機器
セキュリティフィルタ	トレンドマイクロ	Trend Micro Policy Manager™ (以下，TMPM) Deep Discovery™ Inspector (以下，DDI)
インシデント情報連携	パロアルトネットワークス	次世代ファイアウォール，および仮想化次世代ファイアウォール
	Syslog 連携(CEF)対応ベンダ	Syslog 連携(CEF)対応のセキュリティ機器

(c) 端末接続ポート

機器が端末を収容しているポートを端末接続ポートと呼びます。上図では，機器 3，機器 4，機器 5 の端末側のポートが対応します。

(d) WAN 接続ポート

インターネット接続収容に用いるポートを WAN 接続ポートと呼びます。上図では,機器 1 のイン

ターネット側ポートが対応します。
WAN 接続ポートでは，受信フレーム，送信フレームのポートミラーリングを有効にし，ミラー先ポートへインターネットトラフィックを複製する必要があります(上図のインターネットトラフィックと,インターネットトラフィックミラーが対応します)。
WAN 接続ポートは，AX-Network-Manager が，攻撃サーバ宛の通信を遮断する際に使用します。
WAN 接続ポートをリンクアグリゲーション等の複数のポートで構成している場合，Web インタフェースにてポート数分登録するようにしてください。

(e) ミラー先ポート

セキュリティ機器の収容に用いるポートをミラー先ポートと呼びます。上図では，機器 1 のセキュリティ機器側ポートに対応します。
ミラー先ポートがある機器では，(d)のポートミラーリングで受信したフレームをミラー先ポートに中継しないよう，ミラー先ポートにフレーム廃棄となるフィルタを設定する必要があります (セキュリティ機器からの通知により，必要なフレームだけがセキュリティ機器へ中継されます)。
ミラー先ポートをリンクアグリゲーション等の複数のポートで構成している場合，Web インタフェースにてポート数分登録するようにしてください。

(f) 永続設定ポート(受信側/送信側)

NAT を使用しているようなネットワーク環境において，AX-Network-Manager が端末位置を特定できない場合，固定的に遮断する機器のポートを設定することで，通信を遮断させることが可能です。この固定した機器のポートを，永続設定ポートと呼びます。また，受信側で遮断するポートを永続設定ポート(受信側)，送信側で遮断するポートを永続設定ポート(送信側)と呼びます。
永続設定ポート(受信側/送信側)をリンクアグリゲーション等の複数のポートで構成している場合，Web インタフェースにてポート数分登録するようにしてください。
なお本設定をおこなうと，端末位置の特定・不特定にかかわらず永続設定ポート(受信側/送信側)に端末遮断設定をおこなうため，機器で設定可能なアクセスリストのエントリ数を考慮した上で利用ください。

(g) アクセスリスト拡張ポート

端末を収容する管理対象機器が下記の場合，直接，通信遮断・例外通信許可のセキュリティフィルタを設定することができません。

表 2-18 端末収容している管理対象機器

管理対象機器
標準 MIB 対応機器
標準 MIB 対応機器(VLAN 毎コミュニティ)
ワイヤレス LAN コントローラ

このような構成において，上記機器と接続している弊社機器のポート間を接続情報により，弊社機器のポートをセキュリティフィルタ可能であることを示す設定をおこなうことで，セキュリティフィルタが適用可能となります。この設定において，弊社機器のポートを，アクセスリスト拡張ポートと呼びます。

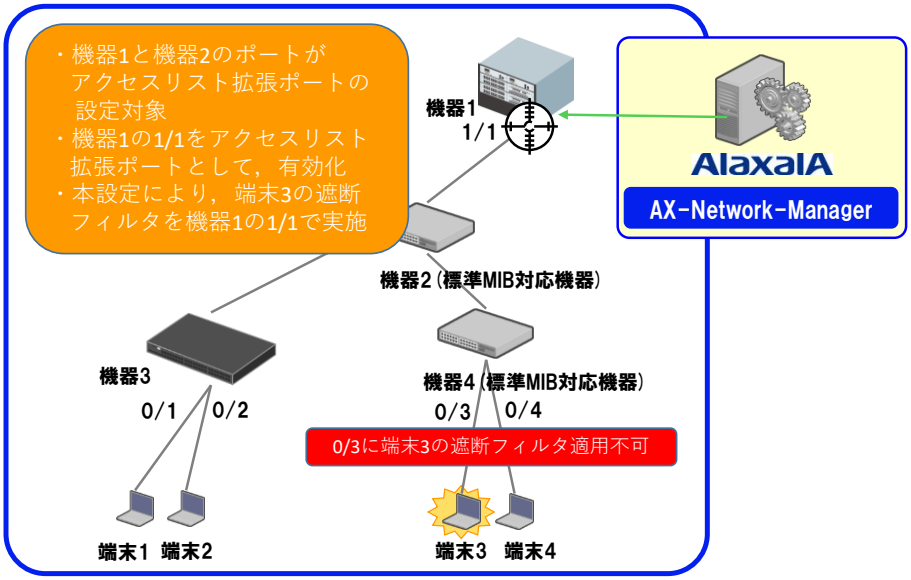

図 2-6 アクセスリスト拡張ポートを設定する構成例

(3) インシデント情報連携

(a) 概要

AX-Network-Manager にあらかじめ登録した syslog クライアントから受信し syslog（インシデント情報）について，インシデント抽出ルールに従ってインシデントを抽出し，抽出したインシデントごとにユーザが選択したインシデント対策を実行します。
ユーザ選択可能なインシデント対策には，以下の 3 つの機能があります。

(i).通信遮断

インシデントとして抽出される Syslog に含まれる IP アドレスに対して，通信遮断のセキュリティフィルタを自動で設定します。syslog に含まれる MAC アドレスに対して，通信遮断のセキュリティフィルタを自動で設定することも可能です。

(ii).詳細ミラー

インシデントとして抽出し syslog に含まれる IP アドレスの端末について，詳細ミラーのセキュリティフィルタを自動で設定します。これにより，マルウェア感染被疑端末のトラフィックだけをセキュリティ機器にて詳細分析することが可能になります。syslog に含まれる MAC アドレスの端末について，詳細ミラーのセキュリティフィルタを自動で設定することも可能です。

(iii).手動選択

抽出したインシデント情報に対して，後からインシデント対策を手動で選択したい場合に選択します。手動選択が指定され syslog はルールマッチ履歴に登録され，通信遮断ボタンまたは，詳細ミラーボタンを押下することでインシデント対策が実行可能です。

(b) 対応 syslog フォーマット

AX-Network-Manager は CEF(Common Event Format)の syslog と連携します。

(c) インシデント抽出ルール

AX-Network-Manager は syslog クライアントから syslog を受信すると，クライアントごとに登録してあるルールでインシデントとなる syslog を抽出します。ルールは，1 つあたり最大 6 組のヘッダフィールドおよび拡張フィールドの種別と値の組み合わせで構成されており，受信した syslog の内容をルールに登録されている値で検索し，すべての条件にヒットした場合にのみ，インシデントとして抽出します。なお，インシデント抽出に指定可能なヘッダフィールドは，一部のヘッダフィールドとすべての拡張フィールドが指定可能です。

(i).ユーザ定義拡張フィールド

セキュリティベンダ固有の任意の CEF フィールドを，インシデント抽出に指定可能なフィールドとして使用することが可能です。このフィールドをユーザ定義拡張フィールドと呼びます。

(4) セキュリティフィルタ (セキュリティ機器との連携)

(a) 概要

セキュリティフィルタは，セキュリティ装置からの指示，AX-Network-Manager が抽出したインシデントと連携，および AX-Network-Manager が抽出したエイリアス未登録端末に対して動作するフィルタ機能です。
セキュリティフィルタは，以下 3 つの機能があります。

(i).通信遮断・例外通信許可

マルウェア感染した端末，または端末からの任意のサーバ宛の通信について，当該端末を収容するポートに，フレーム廃棄・中継のフィルタを設定します。
これにより，感染した端末の全通信遮断や，セキュリティアップデート等を提供するサーバとの通信許可，特定のサーバとの通信遮断を与えることが可能になります。
および，セキュリティ装置が検出した攻撃サーバについて，サーバとの通信を遮断することにより，端末への攻撃を保護します。

表 2-19 通信遮断･例外通信許可

通信種別	提供機能	説明
端末通信	全通信遮断(端末 IP アドレス)	端末 IPv4 アドレスまたは IPv6 アドレスからの全通信を遮断します
	全通信遮断(端末MACアドレス)	端末 MAC アドレスからの全通信を遮断します
	特定サーバ宛通信遮断(その他は許可)	特定サーバ宛の通信を遮断し，その他の通信は許可します。
	特定サーバ宛通信許可(その他は遮断)	特定サーバ宛の通信を許可し，その他の通信は遮断します。
攻撃サーバ通信	攻撃サーバ通信遮断	攻撃サーバ間の通信を遮断します

(ii).詳細ミラー

インシデントを検出した端末，または任意のサーバ宛の通信について，ミラー先ポートに，フレーム中継のフィルタを設定します。これにより，マルウェア感染被疑端末のトラフィックだけをセキュリティ装置にて詳細分析することが可能になります。

表 2-20　詳細ミラー

通信種別	提供機能	説明
端末通信	全通信(端末 IP アドレス)	端末 IPv4 アドレスまたは IPv6 アドレスによりフィルタを設定します。
	全通信(端末 MAC アドレス)	端末 MAC アドレスによりフィルタを設定します。

(iii).端末移動追従

端末の位置をトポロジ管理機能で管理することにより，端末が別ポートに移動したり，IP アドレスが変更されたりした場合でも，追従して通信遮断・通信例外許可を提供します。

(b)　セキュリティフィルタの生成・削除契機

AX-Network-Manager におけるセキュリティフィルタの生成・削除契機を下図，および下表に示します。

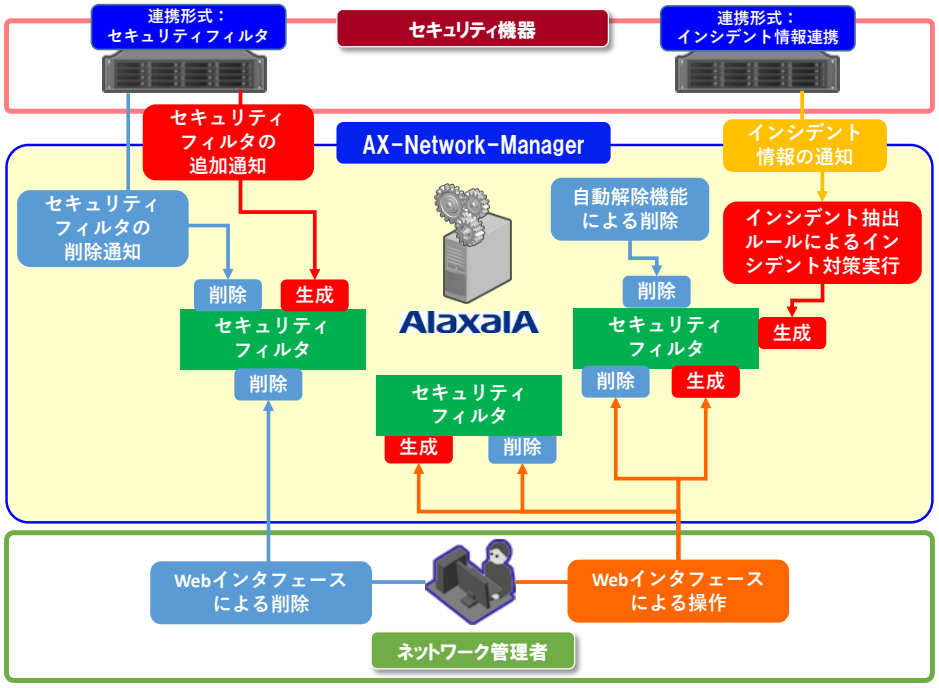

図 2-7　セキュリティフィルタの生成･削除契機

表 2-21　セキュリティフィルタの生成契機

連携形式	生成契機	備考
セキュリティフィルタ	セキュリティ機器からのセキュリティフィルタ追加通知を受信時	
インシデント情報連携	セキュリティ装置からのインシデント情報受信後，インシデント抽出ルールにより，インシデント対策実行時	
―	ネットワーク管理者の Web インタフェース操作時	

表 2-22　セキュリティフィルタの削除契機

連携形式	削除契機	備考
セキュリティフィルタ	セキュリティ機器からのセキュリティフィルタ削除通知を受信時	
	ネットワーク管理者が Web インタフェースによるセキュリティフィルタ削除時	
インシデント情報連携	自動解除機能による削除時 ・　スケジュール解除 ・　タイマー解除	
	ネットワーク管理者が Web インタフェースによるセキュリティフィルタ削除時	
－	ネットワーク管理者が Web インタフェースによるセキュリティフィルタ削除時	

セキュリティフィルタの削除は，Web インタフェースによる削除と，自動解除機能による削除があります。

(i).Web インタフェースによる削除

Web インタフェースにより，生成したセキュリティフィルタを削除します。

(ii).自動解除機能による削除

自動解除機能による削除には，下記 2 つがあります。

・スケジュール解除

生成したセキュリティフィルタを，Web インタフェースにより設定したスケジュールに従って削除します。

スケジュールは，以下のいずれかを 1 つ設定することができます。

表 2-23　設定可能な自動解除スケジュール

スケジュール単位	自動解除時刻	説明	備考
毎日	午前 0 時 0 分～午後 11 時 59 分	毎日の指定解除時刻に，生成したセキュリティフィルタを削除します。	
毎週の指定曜日		毎週指定曜日の指定解除時刻に，生成したセキュリティフィルタを削除します。	
毎月の指定日		毎月指定日の指定解除時刻に，生成したセキュリティフィルタを削除します。	※

注※：指定日が月に存在しない場合，当該月の最終日に解除を実施します(例：毎月 31 日 0:10 に自動解除スケジュールを設定した場合，4 月は，30 日の 0:10 に解除を実施します)。

自動解除スケジュールを毎月 1 日 0:10 に設定した場合の，動作イメージを下図に示します。

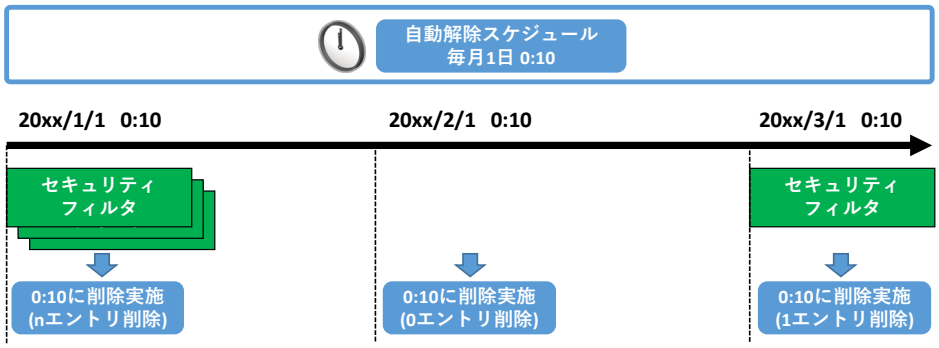

図 2-8 自動解除スケジュール動作イメージ図

なお，自動解除スケジュールが動作するように生成したセキュリティフィルタは，自動解除スケジュールの有効・無効を Web インタフェースで変更することが可能です。

・タイマー削除

セキュリティフィルタを，生成時に設定したタイマーに従って削除します。
設定可能なタイマーは下記となります。

表 2-24 設定可能なタイマー

タイマー(分)	説明
1～1440	通信遮断，詳細ミラー，または手動選択時に生成したセキュリティフィルタについて，指定したタイマーの時間経過後に当該セキュリティフィルタを削除します。

(c) セキュリティフィルタの種別

AX-Network-Manager は，個々のセキュリティフィルタについて，下記に示す種別を管理します。本状態は，Web インタフェースにて確認可能です。

表 2-25 種別

種別	説明
通信遮断(スケジュール解除有効)	スケジュール解除により生成した通信遮断のセキュリティフィルタ
通信遮断(スケジュール解除無効)	スケジュール解除により生成したセキュリティフィルタを，無効状態に変更したセキュリティフィルタ
通信遮断(タイマー解除)	タイマー解除により生成した通信遮断のセキュリティフィルタ
通信遮断	上記に記載した各通信遮断の種別を除く，通信遮断のセキュリティフィルタ
例外通信許可	例外通信許可のセキュリティフィルタ
詳細ミラー(スケジュール解除有効)	スケジュール解除により生成した詳細ミラーのセキュリティフィルタ
詳細ミラー(スケジュール解除無効)	スケジュール解除により生成した詳細ミラーのセキュリティフィルタを，無効状態に変更したセキュリティフィルタ
詳細ミラー(タイマー解除)	タイマー解除により生成した詳細ミラーのセキュリティフィルタ
詳細ミラー	上記に記載した各詳細ミラーの種別を除く，詳細ミラーのセキュリティフィルタ

(d) セキュリティフィルタの設定状態

AX-Network-Manager は，個々のセキュリティフィルタについて，下記に示す設定状態を管理します。本状態は，Web インタフェースにて確認可能です。

表 2-26 設定状態

設定状態	説明
設定中	端末のセキュリティフィルタ適用先となる管理対象機器を検索，コンフィグレーションを設定中です。
設定済み	端末のセキュリティフィルタ適用先となる管理対象機器へとコンフィグレーションの設定が完了しました。
設定削除中	セキュリティフィルタの削除により，セキュリティフィルタ適用済みの管理対象機器から，コンフィグレーションの設定を削除中です。
設定削除済み	セキュリティフィルタの削除による，コンフィグレーションの設定削除が完了しました。
設定削除済み(スケジュール解除)	セキュリティフィルタ自動解除スケジュールによる，コンフィグレーションの設定削除が完了しました。
未サポート種別	動作中のセキュリティフィルタの動作モード(「(f) セキュリティフィルタの動作モードにおける使用可能機能」参照)において，サポートしていない機能をセキュリティ機器からインシデント対策連携で通知されたことにより，セキュリティフィルタを適用しませんでした。 セキュリティフィルタ条件として IPv6 アドレスを含むセキュリティフィルタは，後述するアクセスリストのモード指定が v4-only の場合，未サポート種別と表示されます。
ライセンス無効	外部連携ライセンスの期限が切れたことにより，セキュリティフィルタを適用しませんでした。

および，個々のコンフィグレーションについて，下記に示すコンフィグ設定状態を管理します。本状態は，Web インタフェースにて確認可能です。

表 2-27 コンフィグ設定状態

設定状態	説明
設定中	コンフィグレーションを設定中です。
設定中(<失敗要因>)	コンフィグレーションを設定中です。 前回の装置へのコンフィグレーション操作が，<失敗要因>により失敗しています。 <失敗要因>は「表 2-28」を参照してください。
設定済み	コンフィグレーションの設定が完了しました。
削除中	コンフィグレーションの設定を削除中です。
削除中(<失敗要因>)	コンフィグレーションの設定を削除中です。 前回の装置へのコンフィグレーション操作が，<失敗要因>により失敗しています。 <失敗要因>は「表 2-28」を参照してください。
削除済み	コンフィグレーションの削除が完了しました。

設定状態	説明
削除済み(<失敗要因>)	管理対象装置の設定を変更または削除したことにより，コンフィグレーションの管理を削除済み(<失敗要因>)として完了しました。 最後の装置へのコンフィグレーション操作が，<失敗要因>により失敗しています。 <失敗要因>は「**表 2-28**」を参照してください。

表 2-28 失敗要因一覧

失敗要因	説明
通信失敗	・ 管理対象装置と通信できない場合 ・ SNMP コミュニティ名称不一致
認証失敗	・ SSH ログイン失敗時 ・ 同時ログイン数の上限越え
コンフィグ反映失敗	・ 装置管理者モードのパスワード不一致 ・ 事前準備・設定の不足 ・ 管理対象装置のフィルタエントリの収容条件超え ・ 管理対象装置のコンフィグレーションの一時的な設定不可状態
コンフィグモード移行失敗	・ コンフィグモードへの移行失敗

(e) セキュリティフィルタの動作モード

AX-Network-Manager は，以下 2 つの動作モードがあります。

(i).通常モード

通常モードは，セキュリティフィルタを，管理対象装置の IP パケットフィルタ(AX8600S/AX8300S は Advance フィルタ)により実現します。設定ファイルの ACCESSLIST_MODE を v4-v6 で指定している場合，IPv4 アクセスリストに加えて IPv6 のアクセスリストを設定します。IPv4 アドレスと IPv6 アドレスの両方が設定されている端末に対して，IPv4 セキュリティフィルタ設定指示がくると IPv4 アクセスリストと IPv6 アクセスリストの両方を設定することにより，管理対象端末の IPv4 通信と IPv6 通信の両方を遮断することできます。IPv6 セキュリティフィルタ設定指示時も同様です。

設定ファイルの ACCESSLIST_MODE を v4-only で指定，または省略している場合，IPv4 アクセスリストだけを設定します。

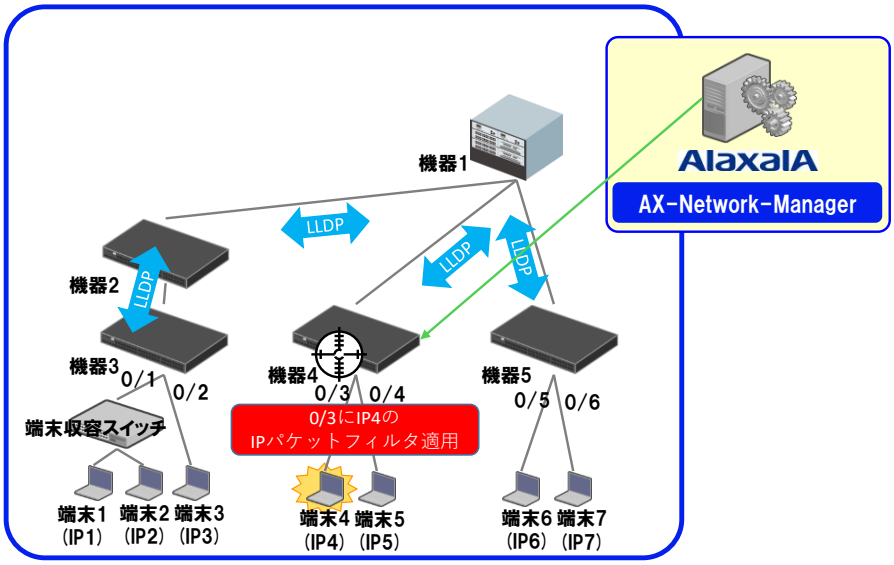

図 2-9 通常モードでの端末 4 へのセキュリティフィルタ適用例

(ii).遮断専用モード

遮断モードは，セキュリティフィルタを，管理対象装置の MAC フィルタ(AX8600S/AX8300S は Advance フィルタ)により実現します。

端末の MAC アドレスを使用してフィルタをおこなうことで，IP パケットだけでなく，端末発の通信を遮断することができます。なお，一つの MAC アドレスに対して複数の IP アドレス(IPv4 アドレスおよび IPv6 アドレスを含む)が設定されている端末には，1 つのアクセスリストが設定されます。

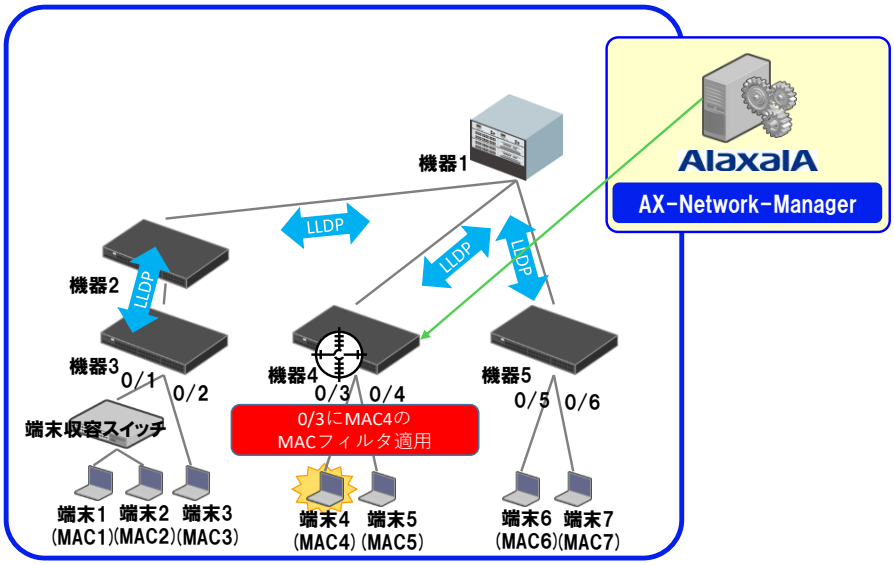

図 2-10 遮断専用モードでの端末 4 へのセキュリティフィルタ適用例

(f) セキュリティフィルタの動作モードにおける使用可能機能

セキュリティフィルタの動作モードは，AX-Network-Manager 起動時に，どちらを使用するかを設

定ファイルで指定します。
動作モードにより，セキュリティフィルタの使用可能機能が異なります。以下に動作モードにおける使用可能な機能の一覧を示します。

表 2-29　動作モードにおける使用可能機能一覧

項目	種別	提供機能	動作モード	
			通常モード	通信遮断専用モード
通信遮断・例外通信許可	端末通信	全通信遮断(IP アドレス)	○	×
		全通信遮断(MAC アドレス)	×	○
		特定サーバ宛通信遮断(その他は許可)	○	×
		特定サーバ宛通信許可(その他は遮断)	○	×
	攻撃サーバ通信	攻撃サーバ通信遮断	○	×
詳細ミラー	端末通信	全通信(端末 IP アドレス)	○	×
		全通信(端末 MAC アドレス)	×	○
端末移動追従	－	ポート移動(同一装置内，別装置)	○	○
	－	IP アドレス変更	○	○※1
特定端末への Web 通信不可表示機能※2	－	－	○	×
永続設定ポート	端末通信	全通信(端末 IP アドレス)	○	×
		全通信(端末 MAC アドレス)	×	○

(凡例) ○:サポート, ×:未サポート, －:対象外
※1:
MAC フィルタの設定内容に変更はありません。
※2:
本機能は，下記マニュアルを参照ください。
・AX260A ソフトウェアマニュアル
・AX2500S ソフトウェアマニュアル
・AX2200S・AX2100S・AX1250S・AX1240S ソフトウェアマニュアル

(g)　セキュリティフィルタの使用上の注意事項

(i).設定ファイル ACCESSLIST_MODE に v4-v6 使用時における注意事項

IPv6 アドレスに対して通信遮断を実施する場合，ネットワーク装置が学習した NDP のダイナミックエントリが削除されないように，NS(Neighbor Solicitation)および NA(Neighbor Advertisement)の permit フィルタを，端末が収容されるポートに設定してください。設定しない場合，端末の NDP エントリの削除契機で，該当 IPv6 アドレスに対するフィルタ設定が削除されます。

(ii).アクセスリスト拡張ポート設定における注意事項

端末を収容する機器として，AX-Network-Managerがサポートする弊社製品を使用している構成において，上位装置にアクセスリスト拡張ポートが設定されている場合，同一端末に対するセキュリティフィルタが複数装置に適用されます。

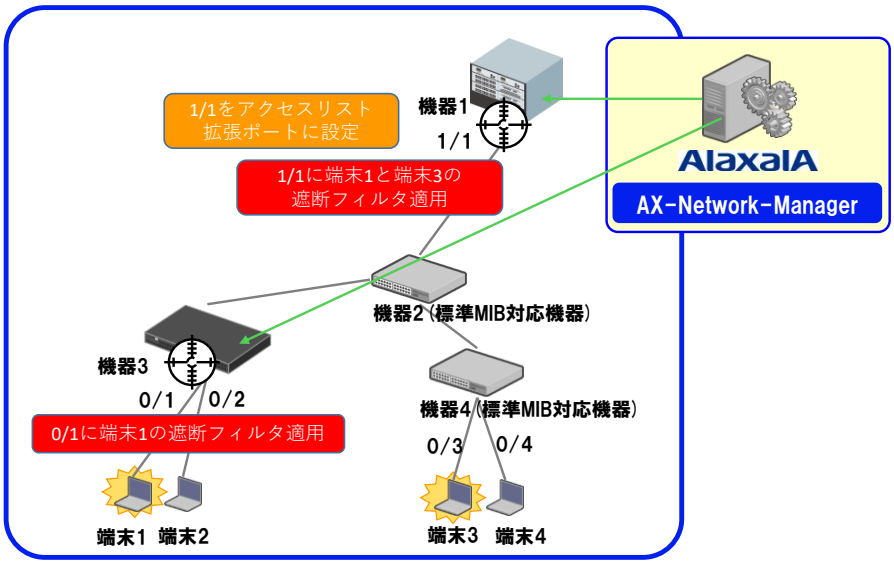

図 2-11 複数装置にセキュリティフィルタが適用される構成例

(iii).エイリアス未登録端末の通信遮断使用時における注意事項

エイリアス未登録端末の通信遮断を有効にすると，AX-Network-Manager が検出したすべてのエイリアス未登録端末に対して，通信遮断をおこないます。ネットワーク運用に影響する可能性があるため，以下で運用することを推奨します。

表 2-30 エイリアス未登録端末の通信遮断有効時の推奨運用

項番	運用
1	ネットワーク内のすべての端末・サーバ・管理対象装置の MAC アドレスを，エイリアスの条件として設定する

上記の運用をおこなわない場合，サーバを含む端末が通信遮断されることがあります。

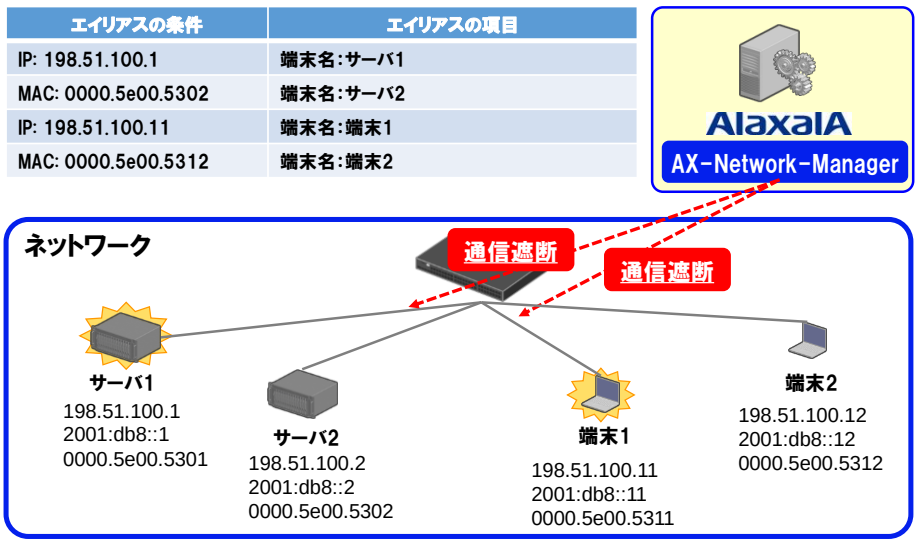

図 2-12 エイリアス未登録端末通信遮断有効時に端末が通信遮断されるケース

上図において，サーバ 1 と端末 1 は，IPv6 アドレスに対応するエイリアス登録が存在しないために通信遮断対象となります。通信遮断対象とならないように，サーバ 1 と端末 1 について，MAC アドレスに対応するエイリアス登録をおこなうようにしてください。サーバ 2 と端末 2 は MAC アドレスに対応するエイリアス登録があることから通信遮断対象となりません。

(5) セグメンテーションセキュリティ

(a) 概要

セグメンテーションセキュリティは，AX-Network-Manager が管理対象とするネットワークをセグメントと呼ぶ単位に分割し，セグメントごとにインシデント対策を実行する機能です。
セグメンテーションセキュリティの構成，および動作例を下図に示します。

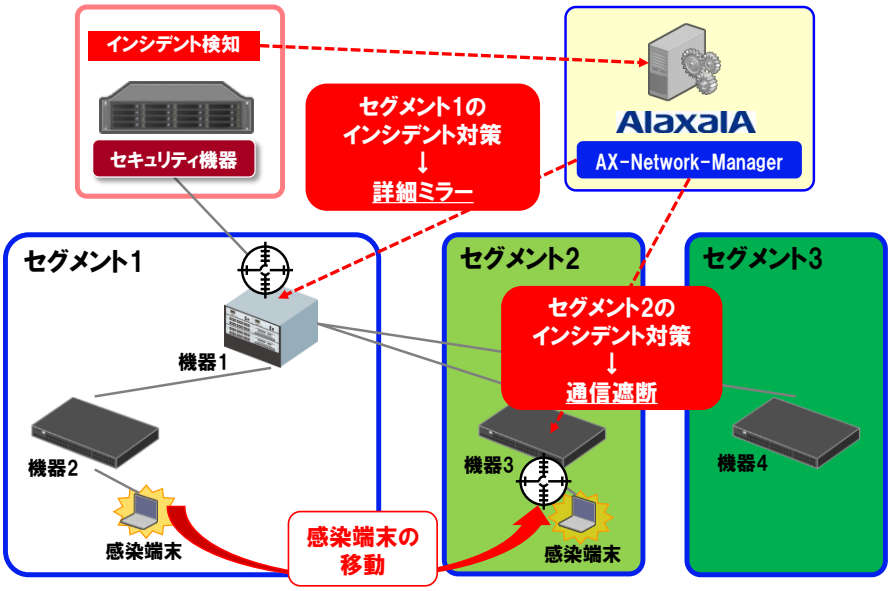

図 2-13 セグメンテーションセキュリティの構成＋動作例

上図において，AX-Network-Manager は，管理対象ネットワークを，セグメント 1，セグメント 2，

およびセグメント 3 の 3 つのセグメントに分割して管理します。
AX-Network-Manager には，セキュリティ機器から通知されるインシデント情報について，セグメント 1 でのインシデント対策を詳細ミラーによる監視，セグメント 2 でのインシデント対策を通信遮断と設定します。
AX-Network-Manager がセキュリティ機器より感染端末のインシデント情報を受信し，感染端末がセグメント 1 の機器 2 に収容していることを検知すると，機器 1 へと詳細ミラーのインシデント対策を実施します。
その後，感染端末がセグメント 2 の機器 3 に移動したことを検知すると，機器 3 へと通信遮断のインシデント対策を実施します。
セグメンテーションセキュリティは，このように，セグメントごとに適用するインシデント対策を設定することが可能になります。

(b) セグメント

セグメンテーションセキュリティにおけるセグメントを下記に示します。

(i).セグメント定義

端末がネットワークでどのセグメントに所属するかを，下記のいずれかの基準で定義します。1 セグメント内に異なる種別の基準を定義することも可能です。

表 2-31 所属情報

種別	内容
IP サブネット	セグメントに所属する IP サブネットを示します。 IPv4 アドレスとマスク，または IPv6 アドレスとプレフィックス長の組み合わせから構成します。
MAC アドレス	セグメントに所属する MAC アドレスを示します。
端末収容ポート	セグメントに所属する端末収容ポート(装置名称+ポート番号の組み合わせ)を示します。 なお端末収容ポートとして使用可能な装置には，下記の装置を指定することはできません。 ・標準 MIB 対応機器 ・標準 MIB 対応機器(VLAN 毎コミュニティ) ・ワイヤレス LAN コントローラ

(ii).セグメントの分類

セグメントは，以下に示す 3 つに分類します。

表 2-32 セグメントの分類

分類	内容
信頼済みセグメント	ネットワーク管理者のセキュリティポリシーにより，セキュリティフィルタ適用外となるセグメントです。 本セグメントに所属する端末は，インシデント情報連携，およびインシデント対策連携による管理対象機器へのコンフィグレーションの適用をおこないません。
個別セグメント	本セグメントに所属する端末は，セグメント内で定義したインシデント抽出ルールとインシデント対策により，セキュリティフィルタを適用します。管理対象のネットワーク内で，複数の個別セグメントを定義することができます。

分類	内容
無所属セグメント	信頼済みセグメント，および個別セグメントのいずれにも所属していない IP サブネット，MAC アドレス，および端末収容ポートの端末は，本セグメントに所属します。

(iii).セグメントのサポート機能

セグメントの分類により，使用可能な機能が異なります。以下にセグメントの分類における使用可能な機能の一覧を示します。

表 2-33　セグメントにおける使用可能機能一覧

項目		分類		
		信頼済みセグメント	個別セグメント	無所属セグメント
セグメント定義		○	○	－
インシデント抽出ルールの設定		－	○	○
セキュリティフィルタ	通信遮断	－	○	○
	詳細ミラー	－	○	○
	端末移動追従	－	○	○
	特定端末への Web 通信不可表示機能	－	○	○
	永続設定ポート	－	○	○
セキュリティフィルタ自動解除スケジュール		○※1	○	○

(凡例) ○:サポート，－:対象外

注※1:

無所属セグメントのセキュリティフィルタ自動解除スケジュールを適用します

(iv).セグメント間の優先度

複数のセグメントで，同一のセグメント定義をおこなうことが可能です。この際，インシデント情報により，端末がどのセグメントに所属するかは，優先度により決定します。優先度は，小さい値が優先されます。

セグメントの分類と優先度を下記に示します。

表 2-34　セグメントの分類と優先度

分類	優先度	説明
信頼済みセグメント	1	最高優先のセグメントです。 優先度の値を変更することはできません。
個別セグメント	1001 ～ 9000	Web インタフェースにより，優先度の値を変更することが可能です。
無所属セグメント	10000	最低優先のセグメントです。 優先度の値を変更することはできません。

(c)　セグメンテーションセキュリティの動作概要

セグメンテーションセキュリティの動作概要を下図に示します。

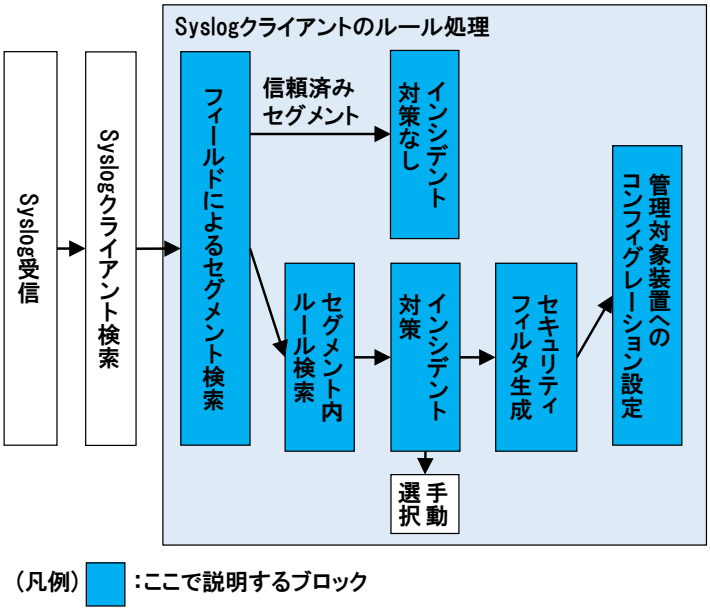

図 2-14 セグメンテーションセキュリティの処理ブロック

表 2-35 各処理ブロックの概要

部位	概要
フィールドによるセグメント検索	syslog メッセージの下記フィールドより，セグメントを検索します。 ・ src ・ dst ・ sourceTranslatedAddress ・ destinationTranslatedAddress ・ PanOSXforwarderfor (クライアント種別が「パロアルトネットワークス 次世代ファイアウォール」の場合) ・ smac ・ dmac ・ ユーザ定義拡張フィールド(データ型が IPv4 Address, IPv6 Address, IPv4 Address or IPv6 Address または MAC Address) 検索した結果，セグメントが信頼済みセグメントの場合，以降の処理を実施しません。
セグメント内ルール検索	syslog メッセージについて，セグメント内で定義したルール一覧から一致ルールを検索します。
インシデント対策	一致ルールのアクション種別より，インシデント対策を実施します。手動選択の場合，ルールマッチ履歴に情報を保存して終了します。
セキュリティフィルタ生成	アクション種別が通信遮断，または詳細ミラーの場合，セキュリティフィルタを生成します。
管理対象機器へのコンフィグレーション設定	生成したセキュリティフィルタより，適用対象の管理対象機器へとコンフィグレーションを設定します。

(d) セグメンテーションセキュリティ使用時の注意事項

(i).セグメント分割と端末移動の注意事項

セグメントを分割する際は，端末のセグメント移動を考慮してインシデント抽出ルールの設定をおこなってください。下記のルール設定(宛先指定の通信遮断)では感染端末 1 がセグメント 2 に移動した際，セグメント 1 のルールではセグメント 2 内の機器 2 へとセキュリティフィルタの適用をおこないません。

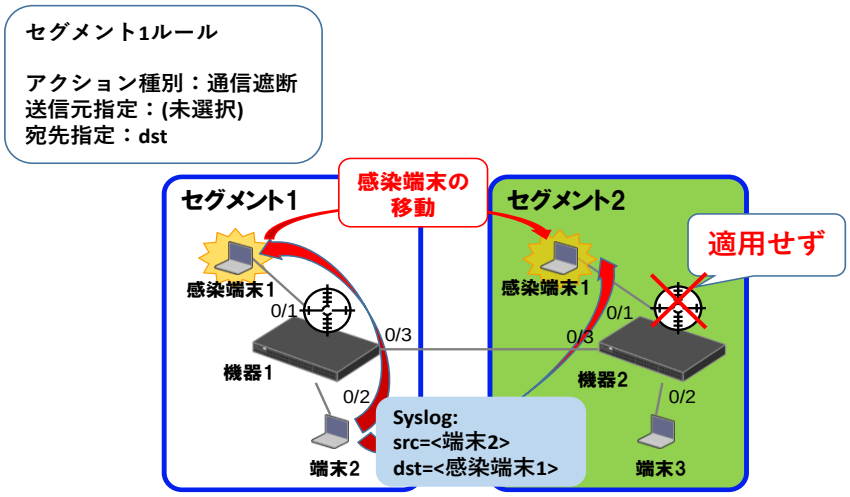

図 2-15 端末移動によりセキュリティフィルタが適用されないケース

このような構成の場合，セグメント 2 にも同一ルールを設定してください。

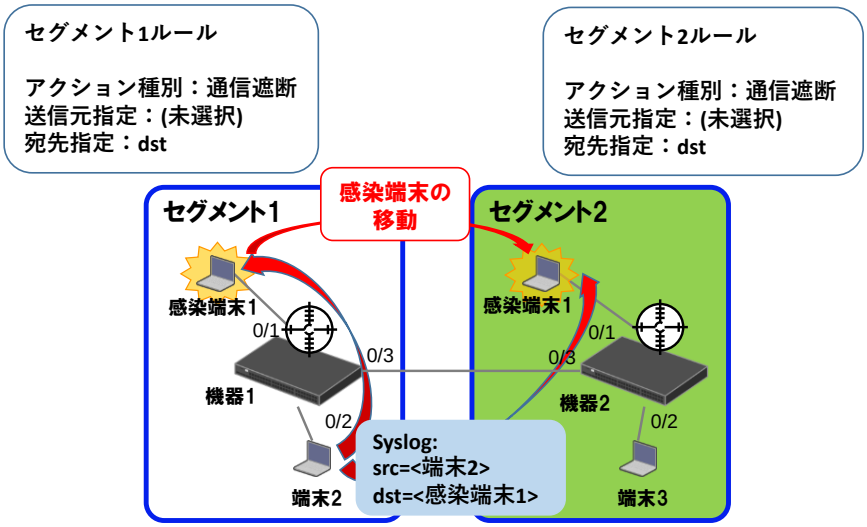

図 2-16 セグメント分割におけるルール設定例

2.1.3 監視対象管理

AX-Network-Manager は，管理対象機器だけでなくサーバや監視カメラ，IoT 機器なども監視する機能を提供します。管理対象機器以外を監視する場合は，監視対象拡張オプションライセンスが台数分必要です。

主な提供機能は，以下のようになります。

表 2-36　監視対象管理の主な提供機能

項目	説明
Ping 監視	・ホスト名または IP アドレスに対して，定期的に Ping 送信 ・Web インタフェースからすぐに Ping 送信することも可能 ・Ping の応答有無，応答時間を閾値にして状態変化・障害検出 ・状態変化・障害検出時に，各種イベント通知 ・状態変化の履歴を表示
MIB 監視	・ホスト名または IP アドレスに対して，定期的に MIB 取得 ・Web インタフェースからすぐに MIB 取得することも可能 ・MIB 取得の応答有無，応答時間，取得値の各種閾値種別にて状態変化・障害検出 ・状態変化・障害検出時に，各種イベント通知 ・MIB 取得値と状態変化の履歴をグラフで表示

Ping 監視と MIB 監視の詳細は以下となります。

(1) Ping 監視

監視対象に定期的に Ping を送出し応答有無と応答までの時間を確認することで，監視対象の状態を監視する機能を提供します。状態は現在の状態だけでなく，履歴として保持された過去の状態変化も確認できます。

監視項目にて監視パラメータを設定し，複数の監視対象（ホスト名または IP アドレス）を登録できます。監視パラメータには，以下があります。これらの監視パラメータを変更した場合，監視対象の状態や状態変化履歴は初期状態に戻ります。

表 2-37　Ping 監視パラメータ

項目	説明
応答時間	Ping 応答までの時間（ミリ秒）がこの値を超えた場合に，異常を検出します。
リトライ回数	応答が無い場合や応答時間が超えた場合に，すぐにこの回数リトライします。
監視周期間隔	この間隔時間（分）で定期的に Ping 送信し応答を監視します。
障害検出周期	異常を検出した場合でも，この周期回数連続して異常を検出するまでは，状態は「注意」となります。この周期回数連続した場合は，状態を「障害」とします。
アクション	正常・注意・障害の状態変化時通知（syslog/E-mail 通知対象）と障害・復旧時だけの通知（syslog/E-mail 通知/イベント対象）を指定できます。

(2) MIB 監視

監視対象から定期的に MIB 値を取得し取得有無，取得までの時間，取得値を各種閾値種別にて確認することで，監視対象の MIB 値と状態を監視する機能を提供します。MIB 値と状態は現在の状態だけでなく，履歴として保持された過去の MIB 値と状態変化もグラフで確認できます。

監視項目にて監視パラメータを設定し，監視項目には複数の監視対象（ホスト名または IP アドレス）を登録できます。監視パラメータには，以下があります。

表 2-38　MIB 監視パラメータ

項目	説明
応答時間	MIB 取得までの時間がこの値を超えた場合に，異常を検出します。

項目	説明
リトライ回数	応答が無い場合や応答時間が超えた場合に，すぐにこの回数リトライします。
監視 MIB コミュニティ名 ポート番号	監視する MIB の OID とコミュニティ，SNMP ポート番号を指定します。
閾値種別 　存在確認	MIB の Syntax を問わず，指定した監視 MIB が存在するかどうかを監視します。
閾値種別 　絶対値	指定した監視 MIB の存在有無と，取得値の範囲を監視します。 範囲は，設定された下方閾値と上方閾値をそれぞれ含む範囲を超えた場合に異常を検出します。 サポートする Syntax は，INTEGER, Integer32, Counter32, Gauge32, Counter64, Unsigned32, UInteger32 です。
閾値種別 　差分値（秒平均）	指定した監視 MIB の存在有無と，取得値と前回取得値の差分について，取得時刻－前回取得時刻の差分(秒)で割った値の範囲を監視します。 範囲は，設定された下方閾値と上方閾値をそれぞれ含む範囲を超えた場合に異常を検出します。 サポートする Syntax は，INTEGER, Integer32, Counter32, Gauge32, Counter64, Unsigned32, UInteger32 です。
履歴保持数	MIB 取得値と状態変化の履歴を保持する数を指定します。
監視周期間隔	この間隔で定期的に MIB 取得し監視します。
障害検出周期	異常を検出した場合でも，この周期回数連続して異常を検出するまでは，状態は「注意」となります。この周期回数連続した場合は，状態を「障害」とします。
アクション	正常・注意・障害の状態変化時通知（syslog/E-mail 通知対象）と障害・復旧時だけの通知（syslog/E-mail 通知/イベント対象）を指定できます。

(a) 使用上の注意事項

AX-Network-Manager インストール後に時刻を変更しないでください。過去の時刻に変更した場合，監視対象の MIB 履歴をすべて削除します。

2.1.4 イベント管理

AX-Network-Manager は，管理対象機器などで発生するイベントを扱います。AX-Network-Manager におけるイベントの扱いは以下のようになります。

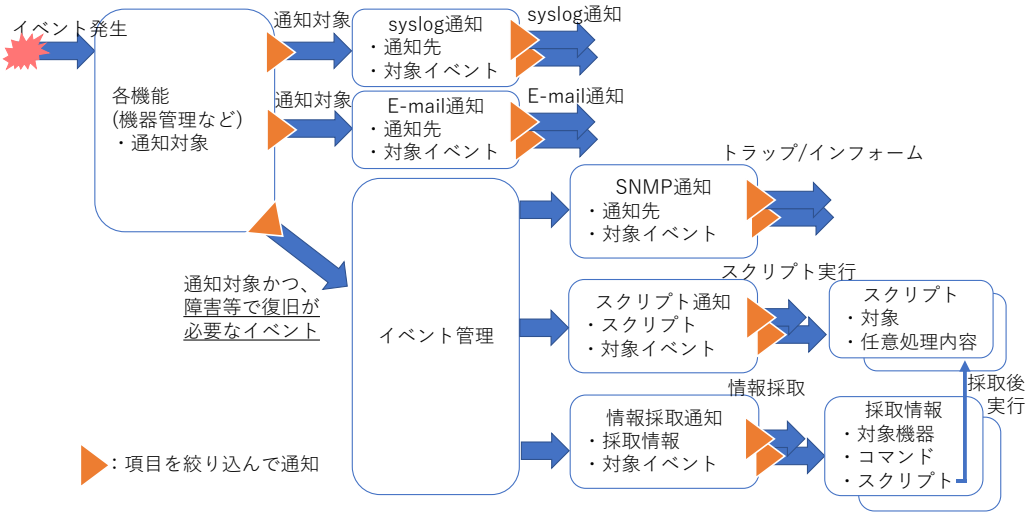

図 2-17 AX-Network-Manager におけるイベントの扱い

イベント管理をおこなう場合，機器設定や機器のインタフェース設定，監視項目設定など各機能の設定にて，通知・イベント対象とする設定を行います。

イベント管理では，障害等復旧が必要な重要なイベントを管理します。発生したイベントとその復旧状態は Web インタフェース上で一覧表示するほか，対応状況を管理する機能を提供します。

イベント管理で管理されるイベントは，SNMP 通知，スクリプト通知，採取情報通知でイベント種別と状態を指定して通知ができます。それぞれ(3)SNMP 通知，(4)スクリプト通知，(5)採取情報通知をご確認ください。

主な提供機能は，以下のようになります。

表 2-39 イベント管理の主な提供機能

項目	説明
イベント情報表示	Web インタフェース上にイベント情報を一覧表示します。 状態変化の要因となった MIB 情報などを確認することができるほか，対応状況も表示します。 イベントの状態が復旧した場合，復旧日時を表示します。
異常検知	イベント管理の対象イベントの状態が変化した際など異常を検知した場合に登録され，管理できます。 これらのイベントは，SNMP 通知，スクリプト通知，採取情報通知で通知できます。
対応状況管理	発生したイベントに対してユーザがまだ確認をしていない，対応している途中であるなど，ユーザによる対応状況を管理できます。

イベント管理の対象イベント項目を以下に示します。

表 2-40 イベント管理対象イベント項目

項目	部位	説明
機器状態異常検知	機器	管理対象機器における状態異常を検知します。 障害，軽度障害，注意の異常発生時にイベントを登録します。

項目	部位	説明
ハードウェア異常検知	ハードウェア	AX-Network-Manager で管理している機器のハードウェア状態異常の発生を検知します。 状態異常の発生でイベントを登録します。
ハードウェア温度異常検知	ハードウェア	AX-Network-Manager で管理している機器のハードウェア温度状態異常の発生を検知します。 状態異常の発生でイベントを登録します。
L2 ループ発生検知	インタフェース	AX-Network-Manager で管理している機器のインタフェースで L2 ループ発生を検知します。 L2 ループの発生でイベントを登録します。
ポート障害検知	機器間：ポート 端末間： ポート，チャネルグループ	AX-Network-Manager で管理している機器のインタフェースで障害発生を検知します。 ポート(インタフェース)障害の発生でイベントを登録します。
ストーム発生検知	ポート	AX-Network-Manager で管理している機器のインタフェースでストーム発生を検知します。 ストームの発生でイベントを登録します。
輻輳検知	機器	管理対象機器において輻輳の発生を検知します。 輻輳発生時にイベントを登録します。
スタック切替検知	機器	管理対象機器においてスタックのマスタ切替を検知します。 マスタ切替発生時にイベントを登録します。復旧管理は行いません。
監視対象状態異常検知	監視対象	監視対象の状態変化を検知します。 障害の発生でイベントを登録します。
SNMP トラップ受信監視条件合致	受信監視設定項目，IP アドレス	受信監視設定での条件に合致する SNMP トラップを受信した場合に検知します。 受信時にイベントを登録します。復旧管理は行いません。
syslog 受信監視条件合致	受信監視設定項目，IP アドレス	受信監視設定での条件に合致する syslog を受信した場合に検知します。 受信時にイベントを登録します。復旧管理は行いません。

2.1.5 操作ログ管理

AX-Network-Manager 上の操作，および機器への操作に関する管理機能を提供します。主な提供機能は，以下のようになります。

表 2-41 操作ログ管理の主な提供機能

項目	説明
操作ログ管理	・ AX-Network-Manager 上の操作，機器への操作ログの保持 (一覧表示などの参照操作は操作ログの対象外です) ・ 条件指定での操作ログの検索

	・　条件指定での操作ログの削除

操作ログの管理内容は，下記となります。

表 2-42　操作ログ管理の管理内容

項目	説明
操作分類	操作した分類となります。以下のいずれかとなります。 ・管理操作：AX-Network-Manager に対する操作 ・機器操作：機器に対する操作 ・通知操作：AX-Network-Manager からの通知
操作機器名	操作対象の機器名となります。 操作分類が管理操作の場合は，「-」となります。
操作種別	操作した種別となります。（例：ログイン，ログアウト）
ユーザ名	操作種別を実行したユーザ名となります。 AX-Network-Manager が実行した場合は，「-」となります。
詳細	操作種別の詳細内容となります。（例：操作種別がログイン，ログアウトの場合，クライアント IP アドレス）

2.1.6　SNMP トラップ受信管理

機器および監視対象(MIB 監視)から通知する SNMP トラップの管理機能を提供します。監視対象は，MIB 監視にてコミュニティが設定されているものが受信対象となります。主な提供機能は，以下のようになります。

表 2-43　SNMP トラップ受信管理の主な提供機能

項目	説明
SNMP トラップ受信管理	・受信した SNMP トラップの保持 ・条件指定での SNMP トラップの検索 ・条件指定での SNMP トラップの削除
SNMP トラップ受信監視	設定した条件の SNMP トラップを受信した際に，通知を行います。詳細は，受信監視設定を参照ください。

AX-Network-Manager では，Trap-PDU 内の Variable Binding は下記の用語で表します。

表 2-44　Trap-PDU の Variable Binding の表現

項目	AX-Network-Manager での用語
Variable-Binding 1 番目の値 (sysUpTime.0)	起動累積時間
Variable-Binding 2 番目の値 (snmpTrapOID.0)	トラップ種別
Variable-Binding 3 番目以降の値	関連 MIB

2.1.7　syslog 受信管理

機器および監視対象から通知する syslog の管理機能を提供します。主な提供機能は，以下のようになります。

表 2-45　syslog 受信管理の主な提供機能

項目	説明
syslog 受信管理	・受信した syslog の保持 ・条件指定での syslog の検索 ・条件指定での syslog の削除

syslog 受信設定	・受信する syslog を任意の条件でフィルタし，受信または破棄します。 ・以下の条件を設定できます。 ・ファシリティ ・重要度 ・内容（部分一致） ・送信元（機器名またはセキュリティ連携機器名または IP アドレス） ※フィルタの反映には syslog 受信管理の再起動が必要です（一時的に syslog 受信が停止します）。
syslog 受信監視	設定した条件の syslog を受信した際に，通知を行います。詳細は，受信監視設定を参照ください。

AX-Network-Manager では，受信した syslog を下記フィールドで管理します。これにより，条件指定での syslog 検索が容易となります。

表 2-46　受信 syslog のフィールド

項目	説明
ファシリティ	RFC3164 準拠
重要度	RFC3164 準拠
タイムスタンプ	RFC3164 準拠
ホスト名	RFC3164 準拠
タグ	RFC3164 準拠
内容	上記フィールド以外の内容を全て格納します

弊社の下記機器モデルの場合，内容フィールドは，機器モデル単位に解析します。内容フィールドのうち，下記の存在するフィールドに対して解析を実施します。

表 2-47　機器モデルごとの内容フィールドの解析

機器モデル	内容フィールドの解析
AX8600S / AX8300S	・時刻 ・BCU 番号 ・系状態 ・イベントレベル ・種別 ・部位詳細 ・アカウントおよび端末情報 ・メッセージ識別子 ・付加情報 ・メッセージテキスト
AX4600S / AX3800S / AX3660S / AX3650S / AX2600S / AX2300S	・時刻 ・スイッチ番号とスイッチ状態 ・イベントレベル ・種別 ・イベント発生部位 ・部位詳細 ・メッセージ識別子 ・付加情報 ・メッセージテキスト

機器モデル	内容フィールドの解析
AX3640S	・時刻 ・イベントレベル ・種別 ・イベント発生部位 ・部位詳細 ・メッセージ識別子 ・付加情報 ・メッセージテキスト
AX2500S / AX260A	・時刻 ・イベントレベル ・種別 ・イベント発生部位 ・部位詳細 ・メッセージ識別子 ・メッセージテキスト
AX2200S / AX2100S / AX1250S / AX1240S	・時刻 ・種別 ・イベント発生部位 ・メッセージテキスト

2.1.8 受信監視設定

機器および監視対象から，設定した条件の syslog や SNMP トラップを受信した際に，イベント登録と通知を行います。主な提供機能は，以下のようになります。

表 2-48 受信監視設定の主な提供機能

項目	説明
受信監視設定一覧	・設定された受信条件の一覧表示 ・受信監視条件の追加・変更・削除
受信監視設定	・受信監視したい syslog または SNMP トラップの条件を指定します。 ・文字列指定の条件では，以下例のワイルドカード「*」を利用できます。大文字小文字区別や，正規表現で指定することもできます。 例）ABC の文字列に合致する条件 部分一致：*B* 前方一致：AB* 後方一致：*BC ワイルドカードの指定がない場合は，完全一致となります。 文字列としてアスタリスク「*」を使用する場合は，「¥*」としてください。「¥」を使用する場合は，「¥¥」としてください。
SNMP トラップ受信監視	・以下の条件を設定できます。 ・トラップ種別（前方一致） ・関連 MIB ・トラップ種別（前方一致） ・値（文字列指定） ・送信元（機器名または IP アドレス）

項目	説明
syslog 受信監視	・以下の条件を設定できます。 ・ファシリティ ・重要度 ・内容（文字列指定） ・イベントレベル（文字列指定） ・種別（文字列指定） ・イベント発生部位（文字列指定） ・メッセージ識別子（文字列指定） ・送信元（機器名またはセキュリティ連携機器名または IP アドレス）
イベント・通知	優先度順に，指定された条件に合致する syslog または SNMP トラップを受信した場合に，イベント登録と通知を行います。

2.1.9 通知設定

AX-Network-Manager は，通知イベント発生，状態変化および操作ログを syslog サーバや E-mail 通知先に通知することができます。
下記に AX-Network-Manager で扱う通知イベント種別一覧を示します。
なお，イベント一覧として管理されている障害等復旧が必要な重要なイベントは，SNMP トラップ，スクリプト実行および情報採取コマンド実行により通知できます。
イベント一覧として管理されている障害等復旧が必要な重要なイベントは，2.1.4 イベント管理をご確認ください。

表 2-49 通知イベント種別(AX-Network-Manager 全体：AX-Network-Manager 管理)一覧

項目	説明
ライセンス失効	ライセンス関連の E-mail を出力します。 送信契機は，下記です。 ・ ライセンス失効 3 か月前 9:00 JST ・ ライセンス失効 1 か月前 9:00 JST ・ ライセンス失効 7 日前から毎日 9:00 JST ・ ライセンス失効時 9:00 JST
SSL 証明書失効	AX-Network-Manager で使用している SSL 証明書の E-mail を出力します。 送信契機は，下記です。 ・ SSL 証明書失効 3 か月前 ・ SSL 証明書失効 1 か月前 ・ SSL 証明書失効 7 日前から毎日 ・ SSL 証明書失効時
ユーザ認証トークン失効	RESTAPI でのアクセス時に使用するユーザごとの認証トークン失効時に通知します。 通知契機は，認証トークン失効 3 か月前，1 か月前，7 日前から毎日，認証トークン失効時です。
ディスク使用量閾値超過	Web インタフェースのリソース管理設定において設定するディスク使用量閾値を，実際の使用量が超過した場合に通知します。

項目	説明
データベース不要領域回収未実行検知	データベースとして使用しているPostgreSQLの各テーブルのAUTOVACUUM状況について，不要タプル数が下記閾値を超えて最終回収日時から6時間以上経過した場合に通知します。 閾値 = バキューム基礎閾値(autovacuum_vacuum_threshold) + (バキューム規模係数(autovacuum_vacuum_scale_factor) × タプル数)
起動	AX-Network-Managerの起動時に通知します。
操作ログ(管理操作)	AX-Network-Manager の操作ログ(管理操作)を通知します。
操作ログ(通知操作)	AX-Network-Manager の操作ログ(通知操作)を通知します。

表 2-50 通知イベント種別(AX-Network-Manager 全体:機器管理)一覧

項目	説明
回線数情報収集時間超過	回線送受信カウンタ収集の周期時間超過を通知します。通知契機は，収集時間が，回線送受信カウンタの周期時間の設定値を超えた場合です。
収集経路数管理上限超過	経路情報収集の収容条件超過を通知します。通知契機は，定期的に収集した経路情報の経路数が，収容条件の値を超えた場合です。
フィルタカウンタ情報収集時間超過	フィルタ管理のカウンタ収集周期時間超過を通知します。通知契機は，収集時間が，フィルタカウンタ収集の周期時間設定値を超えた場合です。
フィルタカウンタ管理上限超過	フィルタ管理のアクセスリストフロー条件登録数超過を通知します。通知契機は，現在のアクセスリストフロー条件登録数が収容条件の値を超えた場合です。超過した場合，カウンタ値の収集はおこないません。
QoS カウンタ情報収集時間超過	QoS 管理のカウンタ収集周期時間超過を通知します。通知契機は，収集時間が，QoS カウンタ収集の周期時間設定値を超えた場合です。
QoS カウンタ管理上限超過	QoS 管理の QoS フローリストフロー条件登録数超過を通知します。通知契機は，現在の QoS フローリストフロー条件登録数が収容条件の値を超えた場合です。超過した場合，カウンタ値の収集はおこないません。

表 2-51 通知イベント種別(AX-Network-Manager 全体:ネットワーク管理)一覧

項目	説明
エイリアス未登録端末検知	端末がエイリアス未登録であることを通知します。通知契機は，機器管理および接続管理により，定期的に収集した情報からネットワークトポロジを把握した契機に，端末のエイリアス未登録を検知した場合です。

表 2-52　通知イベント種別(AX-Network-Manager 全体:インシデント情報連携)一覧

項目	説明
手動選択	ルールマッチ履歴のエントリが手動選択として生成時に通知します。
通信遮断	ルールマッチ履歴のエントリが通信遮断として生成時に通知します。
詳細ミラー	ルールマッチ履歴のエントリが詳細ミラーとして生成時に通知します。

表 2-53　通知イベント種別(AX-Network-Manager 全体:セキュリティフィルタ関連)一覧

項目	説明
セキュリティフィルタ登録	セキュリティフィルタ新規登録時に，通知します。
セキュリティフィルタ設定完了	セキュリティフィルタ新規登録後，関連した機器への設定がすべて完了時に，通知します。
セキュリティフィルタ削除完了	セキュリティフィルタ削除時，関連した機器への削除設定がすべて完了時に，通知します。
端末毎設定要因	新規に機器への設定が発生した契機に，通知します。
端末毎設定完了	機器への設定成功時に，通知します。
端末毎設定失敗	機器への設定失敗時に，通知します。
端末毎削除要因	新規に機器への削除設定が発生した契機に，通知します。

表 2-54　通知イベント種別(機器:機器管理)一覧

項目	説明
機器状態変化	機器の機器状態変化発生を通知します。通知契機は，機器の状態が変化した場合です。
輻輳検知	機器の輻輳発生を通知します。通知契機は，機器の輻輳管理の輻輳状態が変化した場合です。
スタック切替検知	機器のマスタスイッチ切替発生を通知します。通知契機は，機器のマスタスイッチ番号が変化した場合です。
情報収集開始	機器の情報収集開始を通知します。
情報収集完了	機器の情報収集完了を通知します。
コンフィグ変化	機器のコンフィグレーションの変化を通知します。通知契機は，機器からコンフィグレーションの取得時に，以前取得したコンフィグレーションから変更されていた場合です。
コンフィグ保存状態変化	機器のコンフィグレーションの保存状態の変化を通知します。通知契機は，機器の保存状態確認時に保存状態が変更されていた場合です。
シリアル情報変化	機器のシリアル情報の変化を通知します。通知契機は，機器からシリアル情報の取得時に，以前取得したシリアル情報から変更されていた場合です。
操作ログ(機器操作)	AX-Network-Manager の操作ログ(機器操作)を通知します。

表 2-55　通知イベント種別(ハードウェア:機器管理)一覧

項目	説明
ハードウェア状態変化	機器のハードウェア状態変化発生を通知します。通知契機は，機器のハードウェア情報の状態が変化した場合です。

表 2-56　通知イベント種別(インタフェース:機器管理)一覧

項目	説明
ポート障害検知	機器のポート障害発生を通知します。通知契機は，機器のインタフェース情報の状態が変化した場合です。
L2 ループ検知	機器の L2 ループ発生を通知します。通知契機は，機器のインタフェースの L2 ループ情報の検知状態が変化した場合です。
ストーム検知	機器のストーム発生を通知します。通知契機は，機器のインタフェースのストーム検知情報の状態が変化した場合です。

表 2-57　通知イベント種別(監視対象:ネットワーク管理)一覧

項目	説明
監視対象状態変化	監視対象の状態変化を通知します。通知契機は，監視対象の状態が正常，注意，障害に変化した場合です。

表 2-58　通知イベント種別(受信監視条件:ネットワーク管理)一覧

項目	説明
SNMP トラップ受信監視	受信監視設定の条件に合致した SNMP トラップを受信した場合に通知します。
syslog 受信監視	受信監視設定の条件に合致した syslog を受信した場合に通知します。

(1) syslog 通知

(a) 詳細

登録した syslog サーバの IP アドレス, ポートに対して syslog 通知を行う機能です。syslog サーバ毎にファシリティを設定でき, TCP もしくは UDP での転送をサポートします。メッセージは JSON 形式で通知を行います。syslog 通知の詳細を下記に示します。

表 2-59　syslog プロトコルフォーマット

フィールド	値
<PRI の値>	ファシリティと重要度を示す数値 ファシリティは syslog 通知先設定で選択した値，重要度は通知イベントにより以下の値 ・エラー(Error) AX-Network-Manager の通常使用ができない 一部機能/機器の障害状態/動作 ・警告(Warning) AX-Network-Manager の通常使用ができなくなる予兆 一部機能/機器の異常状態/動作 ・情報(Infomational) その他イベント
タイムスタンプ	メッセージが送信された日時
ホスト名	メッセージが生成されたホスト名 AX-Network-Manager が動作しているサーバのホスト名
アプリケーション名	メッセージの生成元アプリケーション名 AX-Network-Manager
[プロセス ID]	メッセージやアプリケーションで任意に使用できる ID AX-Network-Manager のプロセス ID
メッセージ	syslog 通知のメッセージ本体 メッセージのフォーマット(UTF-8・JSON 形式)については次項を参照ください。

syslog 通知のメッセージフォーマットは下記の UTF-8･JSON 形式となります。

表 2-60　syslog メッセージフォーマット(UTF-8･JSON 形式)

項目	値
device_vendor	ベンダ名称 ALAXALA Networks Corporation
device_product	プロダクト名称 AX-Network-Manger
device_version	AX-Network-Manger のバージョン例：1.5
notification_id	通知先 ID 例：1
type	通知種別 例：ライセンス失効
category	通知種別カテゴリ 例：AX-Network-Manager 管理
subject	通知メッセージタイトル 例：1 ヶ月後に AX-Network-Manager のライセンスが失効します
body	通知メッセージ本文(JSON 形式) 例：ライセンス: [{ライセンス種別(シリアル): スタンダード機能 機器 50 台ライセンス(0000-0000-0000-0000),有効期限: 2021/4/1 08:59:59}]
help	対応方法等 例：延長ライセンスを追加してください。

(b) SELinux 使用環境での通知先ポート番号変更時の注意事項

Red Hat Enterprise Linux 8 等の SELinux を使用している環境において, TCP/UDP 問わず, 通知先ポート番号を 514 から変更する場合は, マニュアルを参照するようにしてください。

(2) E-mail 通知

E-mail 通知の詳細を下記に示します。
メール送信時に使用可能な接続プロトコルは下記のいずれかとなります。

表 2-61 接続プロトコル一覧

接続プロトコル	説明
SMTP	メールサーバとの接続に SMTP を使用します。メールサーバとの通信は暗号化されません。
SMTP STARTTLS	メールサーバとの接続に SMTP を使用し, STARTTLS により暗号化通信をおこないます。メールサーバとの通信は暗号化されます。
SMTPS	メールサーバとの接続に SMTPS を使用します。メールサーバとの通信は暗号化されます。

メールサーバとの SMTP 認証は下記のいずれかとなります。

表 2-62 SMTP 認証一覧

SMTP 認証	説明
なし	SMTP 認証をおこないません。
あり	SMTP 認証をおこないます。 CRAM-MD5, PLAIN, LOGIN の順に, 認証を試みます。

各メールで使用するメールヘッダの共通フォーマットは下記となります。

表 2-63 メールヘッダ共通フォーマット

フィールド	値
Content-Type	text/plain; charset="utf-8"
Content-Transfer-Encoding	base64
MIME-Version	1.0
To/Cc/Bcc/From	E-mail 通知先で設定された各メールアドレス
Subject	通知メッセージのタイトル 例：1 ヶ月後に AX-Network-Manager のライセンスが失効します
Date	通知メッセージが作成された日時
本文	通知メッセージ本文 例： ライセンス: ライセンス種別(シリアル): スタンダード機能 機器 50 台ライセンス(0000-0000-0000-0000) 有効期限 2021/4/1 08:59:59 延長ライセンスを追加してください。

(3) SNMP 通知

登録した SNMP 通知先の IP アドレス, ポートに対してトラップ, またはインフォームにより通知を行います。SNMP 通知の詳細を下記に示します。

(a) SNMP 通知仕様

SNMP 通知のサポート仕様を次の表に示します。

表 2-64 SNMP 通知サポート仕様

項目	説明
通知種別	SNMP トラップ インフォーム
サポートプロトコル	SNMPv2C

(b) プライベート MIB 定義ファイルの入手方法

プライベート MIB 定義ファイル(ASN.1)は，ソフトウェアと共に提供いたします。プライベート MIB 識別子，および実装仕様は，プライベート MIB 定義ファイルを参照してください。

(c) SNMP 通知の種類と送信契機

サポートする SNMP 通知の種類と送信契機を次の表に示します。

表 2-65 SNMP 通知の種類と送信契機

種類	意味	発行契機
axNmNodeStateAlertTrap	機器状態異常への遷移	機器状態が異常となった場合
axNmNodeStateRecoveryTrap	機器状態異常復旧の遷移	機器状態が異常から復旧した場合
axNmNodeCongestionAlertTrap	輻輳の発生	輻輳が発生した場合
axNmNodeCongestionRecoveryTrap	輻輳からの復旧	輻輳の発生から復旧した場合
axNmNodeStackSwitchTrap	スタック切替発生通知	スタック切替が発生した場合
axNmHardwareStateAlertTrap	ハードウェアの稼働状態異常への遷移	ハードウェアの稼働状態が異常となった場合
axNmHardwareStateRecoveryTrap	ハードウェアの稼働状態異常復旧の遷移	ハードウェアの稼働状態が異常から復旧した場合
axNmHardwareTemperatureStateAlertTrap	ハードウェアの温度状態異常への遷移	ハードウェアの温度状態が異常となった場合
axNmHardwareTemperatureStateRecoveryTrap	ハードウェアの温度状態異常復旧の遷移	ハードウェアの温度状態が異常から復旧した場合
axNmInterfacePortAlertTrap	ポート障害発生検知	機器間ポート，端末接続先ポートで障害が発生した場合
axNmInterfacePortRecoveryTrap	ポート障害復旧検知	機器間ポート，端末接続先ポートで障害から復旧した場合
axNmInterfaceL2loopAlertTrap	L2 ループ発生検知	L2 ループが発生した場合
axNmInterfaceL2loopRecoveryTrap	L2 ループ復旧検知	L2 ループの発生から復旧した場合

種類	意味	発行契機
axNmInterfaceStormAlertTrap	ストーム発生検知	ストームが発生した場合
axNmInterfaceStormRecoveryTrap	ストーム復旧検知	ストームの発生から復旧した場合
axNmWatchTargetStateAlertTrap	監視対象状態異常検知	監視対象の状態が異常となった場合
axNmWatchTargetStateRecoveryTrap	監視対象状態異常復旧	監視対象の状態が異常から復旧した場合
axNmTrapWatchStateAlertTrap	SNMP トラップ受信監視	受信監視設定の条件に合致した SNMP トラップを受信した場合
axNmSyslogWatchStateAlertTrap	syslog 受信監視	受信監視設定の条件に合致した syslog を受信した場合

(d) PDU 内パラメータ

Trap-PDU，InformRequest-PDU 内パラメータを以下に示します。

表 2-66 Trap-PDU,InformRequest-PDU 内パラメーター覧

種類	Trap-PDU，InformRequest-PDU データ値		
	Variable-Binding [1](SysUpTime.0)	Variable-Binding [2](SnmpTrapOID.0)	Variable-Binding [3～]
axNmNodeStateAlertTrap	sysUpTime の値(※1)	axNmNodeStateAlertTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.2.1.10.0.1)	axNmNodeName
axNmNodeStateRecoveryTrap	sysUpTime の値(※1)	axNmNodeStateRecoveryTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.2.1.11.0.1)	axNmNodeName
axNmNodeCongestionAlertTrap	sysUpTime の値(※1)	axNmNodeCongestionAlertTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.2.1.10.0.2)	axNmNodeName
axNmNodeCongestionRecoveryTrap	sysUpTime の値(※1)	axNmNodeCongestionRecoveryTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.2.1.11.0.2)	axNmNodeName
axNmNodeStackSwitchTrap	sysUpTime の値(※1)	axNmNodeStackSwitchTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.2.1.10.0.3)	axNmNodeName

種類	Trap-PDU，InformRequest-PDU データ値		
	Variable-Binding [1](SysUpTime.0)	Variable-Binding [2](SnmpTrapOID.0)	Variable-Binding [3～]
axNmHardwareStateAlertTrap	sysUpTime の値(※1)	axNmHardwareStateAlertTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.3.1.10.0.1)	axNmNodeName axNmHardwareState (事象発生時の MIB 情報)
axNmHardwareStateRecoveryTrap	sysUpTime の値(※1)	axNmHardwareStateRecoveryTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.3.1.10.0.2)	axNmNodeName axNmHardwareState (事象発生時の MIB 情報)
axNmHardwareTemperatureStateAlertTrap	sysUpTime の値(※1)	axNmHardwareTemperatureStateAlertTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.3.1.11.0.1)	axNmNodeName axNmHardwareTemperatureState (事象発生時の MIB 情報)
axNmHardwareTemperatureStateRecoveryTrap	sysUpTime の値(※1)	axNmHardwareTemperatureStateRecoveryTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.3.1.11.0.2)	axNmNodeName axNmHardwareTemperatureState (事象発生時の MIB 情報)
axNmInterfacePortAlertTrap	sysUpTime の値(※1)	axNmInterfacePortAlertTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.3.2.10.0.1)	axNmInterfaceName axNmInterfacePortState
axNmInterfacePortRecoveryTrap	sysUpTime の値(※1)	axNmInterfacePortRecoveryTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.3.2.11.0.1)	axNmInterfaceName axNmInterfacePortState
axNmInterfaceL2loopAlertTrap	sysUpTime の値(※1)	axNmInterfaceL2loopAlertTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.3.2.10.0.2)	axNmInterfaceName axNmInterfaceL2loopState
axNmInterfaceL2loopRecoveryTrap	sysUpTime の値(※1)	axNmInterfaceL2loopRecoveryTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.3.2.11.0.2)	axNmInterfaceName axNmInterfaceL2loopState
axNmInterfaceStormAlertTrap	sysUpTime の値(※1)	axNmInterfaceStormAlertTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.3.2.10.0.3)	axNmInterfaceName

種類	Trap-PDU，InformRequest-PDU データ値		
	Variable-Binding [1](SysUpTime.0)	Variable-Binding [2](SnmpTrapOID.0)	Variable-Binding [3～]
axNmInterfaceStormRecoveryTrap	sysUpTime の値(※1)	axNmInterfaceStormRecoveryTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.3.2.11.0.3)	axNmInterfaceName
axNmWatchTargetStateAlertTrap	sysUpTime の値(※1)	axNmWatchTargetStateAlertTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.4.2.10.0.1)	axNmWatchItemName axNmWatchTargetIpAddress axNmWatchTargetHostname (設定時のみ) axNmWatchTargetState
axNmWatchTargetStateRecoveryTrap	sysUpTime の値(※1)	axNmWatchTargetStateRecoveryTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.4.2.11.0.1)	axNmWatchItemName axNmWatchTargetIpAddress axNmWatchTargetHostname (設定時のみ) axNmWatchTargetState
axNmTrapWatchStateAlertTrap	sysUpTime の値(※1)	axNmTrapWatchStateAlertTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.5.2.10.0.1)	axNmTrapWatchNodeName axNmTrapWatchIpAddress axNmTrapWatchOID axNmReceivedItemName
axNmSyslogWatchStateAlertTrap	sysUpTime の値(※1)	axNmSyslogWatchStateAlertTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.33.5.3.10.0.1)	axNmSyslogWatchNodeName axNmSyslogWatchClientName axNmSyslogWatchIpAdress axNmSyslogWatchData axNmReceivedItemName

※ 送信する Trap PDU のタイムスタンプフィールドは，AX-NM が起動した時間からの経過時間を表示する。

(4) スクリプト通知

スクリプト通知は，イベント一覧として管理されている障害等復旧が必要な重要なイベント発生・復旧時に，スクリプト設定で設定した任意処理内容のスクリプトを実行できます。スクリプト実行時の詳細については，2.1.102.1.10 スクリプト設定をご確認ください。

(5) 採取情報通知

採取情報通知は，イベント一覧として管理されている障害等復旧が必要な重要なイベント発生・復旧時に，採取情報設定で設定した情報の採取を実行できます。採取情報実行時の詳細については，2.1.11 採取情報管理をご確認ください。

(6) 通知詳細設定

通知詳細設定は，個々の通知先に対して，下記の 1 つ以上の通知単位の組み合わせにより，通知する内容を絞り込むことができます。

表 2-67　通知単位

通知単位	説明
AX-Network-Manager 全体	AX-Network-Manager 全体の通知イベント種別を指定できます。
機器	機器のイベント種別に，1 つ以上の機器名の組み合わせを指定できます。
ハードウェア	ハードウェアのイベント種別に，1 つ以上のハードウェア名の組み合わせを指定できます。
インタフェース	インタフェースのイベント種別に，1 つ以上のインタフェース名の組み合わせを指定できます。
監視対象	監視対象のイベント種別に，1 つ以上の監視対象の組み合わせを指定できます。
受信監視条件	受信監視条件のイベント種別に，1 つ以上の受信監視設定の組み合わせを指定できます。

上記通知単位は，通知抑止スケジュールを設定することにより，土日などの期間について通知を抑止することも可能です。通知抑止スケジュールは，下記を 1 つ以上設定することにより動作します。

表 2-68　通知抑止スケジュール

期間	説明
開始曜日	月曜，火曜，水曜，木曜，金曜，土曜，日曜のいずれか
開始時刻	0:00 ～ 23:55 の 5 分単位で表した時刻
終了曜日	月曜，火曜，水曜，木曜，金曜，土曜，日曜のいずれか
終了時刻	0:00 ～ 23:55 の 5 分単位で表した時刻

2.1.10　コンフィグ管理

運用管理対象機器のコンフィグレーションを管理する機能を提供します。主な提供機能は，以下のようになります。

表 2-69　コンフィグ管理の主な提供機能

項目	説明
コンフィグ管理	機器ごとにコンフィグレーションの管理機能を提供します。 ・コンフィグレーションの世代管理 ・世代ごとにコメントの付与 ・コンフィグレーション間の比較
コンフィグ取得	機器のスタートアップコンフィグレーションを取得し，コンフィグ管理により管理します。ローカルに保存したコンフィグレーションをアップロードし管理することも可能です。 なお，テンプレート管理で生成したコンフィグレーションの反映または設定後に，連携してコンフィグレーションを取得し設定内容を確認することもできます。 フィルタ管理対応機器は，機器のスタートアップコンフィグレーション取得時にフィルタ，QoS，ポートミラーリング情報を解析します。

項目	説明
コンフィグ反映	コンフィグ管理で管理しているコンフィグレーションを機器に反映します。 機器側からコンフィグレーションを取得し，スタートアップコンフィグレーションを書き換え，機器を再起動させて反映します。 なお，テンプレート管理で生成したコンフィグレーションの反映もできます。詳細は「テンプレート管理」をご確認ください。
コンフィグ設定	テンプレート管理で生成したコンフィグレーションを機器に設定します。詳細は「テンプレート管理」をご確認ください。
コンフィグ保存・保存状態確認	機器でランニング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へ保存します。 また，機器でスタートアップコンフィグレーションが保存されているかを確認します。

2.1.1 テンプレート管理

コンフィグレーションをテンプレートとして作成することで，複数の運用管理対象機器に対して，一括してコンフィグレーションを設定・反映できる機能を提供します。
本機能はスタンダード機能もしくはワイヤレス LAN コントローラライセンスの管理対象機器にて動作します。
主な提供機能は，以下のようになります。

表 2-70 テンプレート管理の主な提供機能

項目	説明
テンプレート管理 （一覧・設定）	テンプレートを作成し管理する機能を提供します。 ・テンプレートの作成と一覧表示 ・テンプレートに任意の変数値を指定し，機器毎のコンフィグレーションを生成，各機器へ一括設定・反映
動作： コンフィグ設定 （部分設定）	複数の機器にほぼ同じコンフィグレーションを投入する場合などに利用できます。テンプレート内容と変数値から対象機器毎のコンフィグレーションを生成し，一括して各機器に設定します。(AX機器の場合，コンフィグレーションにinterface range 等を記述し，複数のインタフェースを一括設定することもできます。) 間違ったコンフィグレーションを投入した場合でも，投入が中断されエラー表示にて確認できます。（問い合わせ待ちや応答メッセージがあるコンフィグレーションは未サポートです。タイムアウトやエラーとなり中断します。） 標準 MIB 対応機器，標準 MIB 対応機器(VLAN 毎コミュニティ)およびワイヤレス LAN コントローラは，スクリプト設定で処理内容「コンフィグ設定」のスクリプトを設定することで動作します。
動作： コンフィグ反映 （置き換え）	複数の機器をほぼ同じコンフィグレーションで置き換え反映する場合などに利用できます。テンプレート内容と変数値から対象機器毎のコンフィグレーションを生成し，一括して各機器に反映（置き換え）します。 標準 MIB 対応機器，標準 MIB 対応機器(VLAN 毎コミュニティ)およびワイヤレス LAN コントローラは，スクリプト設定で処理内容「コンフィグ反映」のスクリプトを設定することで動作します。

項目	説明
動作後： コンフィグ取得	各動作：コンフィグ設定・反映の動作完了後に，連携してコンフィグ取得動作を行うか選択できます。有効にしておくことで，コンフィグ履歴にて，コンフィグ設定・反映の結果をコンフィグレーションの差分として確認できます。

2.1.2 機器への設定

フロントパネル表示やマップによるグラフィカルな表示画面から，運用管理対象機器の設定を行う機能を提供します。機器モデルによらず，同じ 操作で実施できます。また，機器への設定時，コンフィグレーションをスタートアップコンフィグに保存するかを選択できます。

主な提供機能は，以下のようになります。

表 2-71 機器への設定の主な提供機能

項目	説明
ポート設定	機器詳細画面のフロントパネル表示から対象ポートの設定を変更します。 設定項目： ポート状態の変更 ポート閉塞 / ポート閉塞解除
VLAN 設定	マップで VLAN 設定を行う機器を選択し，情報ウインドウ内に表示する VLAN 設定ボタンから VLAN 設定をおこないます。なお設定する VLAN がループ構成とならないように，あらかじめレイヤ 2 ネットワークの冗長化プロトコルを設定しておくか，ツリー型のネットワーク構成としてください。 設定項目： 機器 VLAN の追加・削除※ ポート tagged / untagged / 設定なし ※ VLAN 設定を行う機器において，対象の VLAN が使用されなくなった場合に，削除を選択できます。
VXLAN 設定	マップで VXLAN 設定を行う機器を選択し，情報ウインドウ内に表示する VXLAN 設定ボタンから VXLAN 設定をおこないます。 設定項目： VXLAN トンネルの設定※1 VLAN マッピングの設定 サブインタフェースマッピングの設定※2 ※1: 事前に，機器の VTEP に source-interface の設定をおこなう必要があります。 ※2: 機器に設定する<subinterface index>は VLAN ID となります。untagged の場合は 4096 となります。

項目	説明
アクセスリスト設定	フィルタ管理でフィルタ配布する配布名を選択し，アクセスリストを反映する機器を選択します。 設定項目： アクセスリストの反映/削除
フィルタ有効化・無効化設定	フィルタ管理でフィルタ配布する配布名を選択し，フィルタを有効化・無効化する機器のインタフェースを選択します。 設定項目： インタフェース(ポート/VLAN)のフィルタを有効化・無効化
QoS フローリスト設定	QoS 管理で QoS 配布する配布名を選択し，QoS フローリストを反映する機器を選択します。 設定項目： QoS フローリストの反映/削除
QoS 制御有効化・無効化設定	QoS 管理で QoS 配布する配布名を選択し，QoS を有効化・無効化する機器のインタフェースを選択します。 設定項目： インタフェース(ポート/VLAN)の QoS を有効化・無効化
ポートミラーリング設定	ポートミラーリング管理でポートミラーリング配布する配布名を選択し，ポートミラーリング設定を反映します。 設定項目： ポートミラーリング設定の反映/削除
ポート状態変更	機器詳細画面のフロントパネル表示から，コンフィグレーションを変更せずに，一時的に対象ポートの状態を変更します。 設定項目： ポート状態の変更 ポート閉塞（inactivate 状態への変更） / ポート閉塞解除（activate 状態への変更）

機器への設定は，以下の方法で設定します。

表 2-72　ポート設定の設定内容

実施項目	設定内容
ポート状態の変更	対象インタフェースに対して，以下のコンフィグレーションを設定します。 対象インタフェース： イーサネットインタフェース コンフィグレーションコマンド： ポート閉塞： shutdown ポート閉塞解除： no shutdown

表 2-73　VLAN 設定の設定内容

実施項目	機器モデル	設定方法
VLAN 設定	AXprimoM210	IEEE 802.1Q VLAN によるポートベースの VLAN を用いて，機器に設定を行います。機器毎に共存できない，または制限のある機能が存在する場合があります。CLI レファレンスガイドの各コマンドを参照してください。 設定する VLAN ID に対して以下のコンフィグレーションコマンドを設定します。 新規 VLAN 設定時： vlan database，vlan 機器内に設定対象の VLAN がなくなった場合※: vlan database，no vlan 対象インタフェースに対して以下のコンフィグレーションコマンドにより VLAN を設定します。 switchport mode hybrid switchport allowed vlan untagged switchport allowed vlan tagged switchport allowed vlan remove switchport native vlan
	上記を除く機器	ポート VLAN を用いて，機器に設定を行います。機器毎に共存できない，または制限のある機能が存在する場合があります。各機器のコンフィグレーションガイド「レイヤ 2 スイッチ機能と他機能の共存について」，およびコンフィグレーションコマンドレファレンスの各コマンドを参照してください。 設定する VLAN ID に対して以下のコンフィグレーションコマンドを設定します。 新規 VLAN 設定時： vlan 機器内に設定対象の VLAN がなくなった場合※: no vlan 対象インタフェースに対して以下のコンフィグレーションコマンドにより VLAN を設定します。対象インタフェースに所属する VLAN に応じてインフェースの属性変更が行われます。インタフェースの属性変更により通信影響が生じる場合があります。 Untagged のみのインタフェース： switchport mode access switchport access vlan tagged を含むインタフェース： switchport mode trunk switchport trunk allowed vlan switchport trunk native vlan

※所属ポートなし VLAN 削除設定が有効の場合のみ。設定変更により機器内のインタフェースで VLAN ID が使用されていない場合に，コンフィグレーションコマンド no vlan

で vlan を削除します。この時，コンフィグレーションコマンド vlan，および interface vlan など，削除する VLAN ID に関連する設定も削除されます。

表 2-74　VXLAN 設定の設定内容

実施項目	設定項目	設定内容
VXLAN 設定	VXLAN トンネルの設定	以下のコンフィグレーションを設定します。 ・機器設定時 interface vxlan <vtep id> member vni add <vni> destination-ip <ip address> ・設定削除時 interface vxlan <vtep id> member vni remove <vni> no destination-ip <ip address>
	VLAN マッピングの設定	以下のコンフィグレーションを設定します。 ・機器設定時 vlan <vlan id> vxlan-vni <vni> ・機器設定削除時 vlan <vlan id> no vxlan-vni
	サブインタフェースマッピングの設定	以下のコンフィグレーションを設定します。 ・機器設定時(サブインタフェースの追加) interface gigabitethernet <switch no.>/<nif no.>/<port no.>※ no switchport interface gigabitethernet <switch no.>/<nif no.>/<port no.>.<subinterface index>※ encapsulation dot1q { <vlan id> | untagged } vlan-vni <vni> ・機器設定時(サブインタフェースの削除) no interface gigabitethernet <switch no.>/<nif no.>/<port no.>.<subinterface index>※ ※: 一例であり，10Gbit/s のイーサネットインタフェースや，ポートチャネルインタフェース等の場合，インタフェースのタイプに応じてコンフィグレーションが生成されます。

表 2-75　フィルタ管理の設定内容

実施項目	設定項目	設定内容
フィルタ管理	アクセスリストの設定	以下のコンフィグレーションを設定します。 アクセスリストを反映する場合は，そのアクセスリストの配布名の識別子を一旦削除したあとに反映します。 ・IPv4 フィルタ(IPv4 アドレスフィルタ)反映 ip access-list standard <配布名の識別子> <シーケンス番号> {permit | deny} <フィルタ条件> no <シーケンス番号> ・IPv4 フィルタ(IPv4 アドレスフィルタ)削除 no ip access-list standard <配布名の識別子> ・IPv4 フィルタ(IPv4 パケットフィルタ)反映 ip access-list extended <配布名の識別子> <シーケンス番号> {permit | deny} <フィルタ条件> no <シーケンス番号> ・IPv4 フィルタ(IPv4 パケットフィルタ)削除 no ip access-list extended <配布名の識別子> ・IPv6 フィルタ反映 ipv6 access-list　<配布名の識別子> <シーケンス番号> {permit | deny} <フィルタ条件> no <シーケンス番号> ・IPv6 フィルタ削除 no ipv6 access-list　<配布名の識別子> ・MAC フィルタ反映 mac access-list extended <配布名の識別子> <シーケンス番号> {permit | deny} <フィルタ条件> no <シーケンス番号> ・MAC フィルタ削除 no mac access-list extended <配布名の識別子> ・Advance フィルタ反映 advance access-list <配布名の識別子> <シーケンス番号> {permit | deny} <フィルタ条件> no <シーケンス番号> ・Advance フィルタ削除 no advance access-list <配布名の識別子>

実施項目	設定項目	設定内容
	フィルタ有効化・無効化設定	対象インタフェースに対して以下のコンフィグレーションコマンドによりフィルタ有効化・無効化を設定します。 ・IPv4 フィルタ有効化 ip access-group <配布名の識別子> {in | out | in-mirror | out-mirror} ・IPv4 フィルタ無効化 no ip access-group <配布名の識別子> {in | out | in-mirror | out-mirror} ・IPv6 フィルタ有効化 ipv6 traffic-filter <配布名の識別子> {in | out | in-mirror | out-mirror} ・IPv6 フィルタ無効化 no ipv6 traffic-filter <配布名の識別子> {in | out | in-mirror | out-mirror} ・MAC フィルタ有効化 mac access-group <配布名の識別子> {in | out | in-mirror | out-mirror} ・MAC フィルタ無効化 no mac access-group <配布名の識別子> {in | out | in-mirror | out-mirror} ・Advance フィルタ有効化 advence access-group <配布名の識別子> {in | out | in-mirror | out-mirror} ・Advance フィルタ無効化 no advence access-group <配布名の識別子> {in | out | in-mirror}

表 2-76　QoS 管理の設定内容

実施項目	設定項目	設定内容
QoS 管理	QoS フローリストの設定	以下のコンフィグレーションを設定します。 QoS フローリストを反映する場合は，その QoS フローリストの配布名の識別子を一旦削除したあとに反映します。 ・IPv4 QoS フローリスト反映 ip qos-flow-list <配布名の識別子> <シーケンス番号> qos <フロー検出条件> no <シーケンス番号> ・IPv4 QoS フローリスト削除 no ip qos-flow-list <配布名の識別子> ・IPv6 QoS フローリスト反映 ipv6 qos-flow-list <配布名の識別子> <シーケンス番号> qos <フロー検出条件> no <シーケンス番号> ・IPv6 QoS フローリスト削除 no ipv6 qos-flow-list <配布名の識別子> ・MAC QoS フローリスト反映 mac qos-flow-list <配布名の識別子> <シーケンス番号> qos <フロー検出条件> no <シーケンス番号> ・MAC QoS フローリスト削除 no mac qos-flow-list <配布名の識別子> ・Advance QoS フローリスト反映 advance qos-flow-list <配布名の識別子> <シーケンス番号> qos <フロー検出条件> no <シーケンス番号> ・Advance QoS フローリスト削除 no advance qos-flow-list <配布名の識別子>
	QoS 制御有効化・無効化設定	対象インタフェースに対して以下のコンフィグレーションコマンドによりフィルタ有効化・無効化を設定します。 ・IPv4 QoS フローリスト有効化 ip qos-flow-group <配布名の識別子> {in | out} ・IPv4 QoS フローリスト無効化 no ip qos-flow-group <配布名の識別子> {in | out} ・IPv6 QoS フローリスト有効化 ipv6 qos-flow-group <qos flow list name> {in | out} ・IPv6 QoS フローリスト無効化 no ipv6 qos-flow-group <qos flow list name> {in | out} ・MAC QoS フローリスト有効化 mac qos-flow-group <qos flow list name> {in | out} ・MAC QoS フローリスト無効化 no mac qos-flow-group <qos flow list name> {in | out} ・Advance QoS フローリスト有効化 advance qos-flow-group <qos flow list name> {in | out} ・Advance QoS フローリスト無効化 no advance qos-flow-group <qos flow list name> {in | out}

表 2-77　ポートミラーリング管理の設定内容

実施項目	設定項目	設定内容
ポートミラーリング管理	ポートミラーリングの設定	以下のコンフィグレーションを設定します。 ・ポートミラーリング反映 monitor session <セッション ID> source interface <選択済みポート> [方向] destination interface <ミラー@ポート選択済みポート> [<追加コンフィグ>] ・ポートミラーリング削除 no monitor session <セッション ID>　または， no monitor session <セッション ID> source

表 2-78　ポート状態変更の設定内容

実施項目	設定内容
ポート状態の変更	対象インタフェースに対して，以下の運用コマンドを実行し，状態を変更します。 対象インタフェース： イーサネットインタフェース 運用コマンド： ポート閉塞： inactivate ポート閉塞解除： activate

機器への設定に対応する機器モデルは，5.3.5(1)フロントパネル表示対応機器に示します。

2.1.3　ソフトウェア管理

管理対象機器のソフトウェアを管理する機能を提供します。主な提供機能は，以下のようになります。

表 2-79　ソフトウェア管理の主な提供機能

項目	説明
ソフトウェア管理	機器モデルごとにソフトウェアの管理機能を提供します。 ・ソフトウェアの世代管理 ・世代ごとにコメントの付与 ・ソフトウェアの登録
ソフトウェア反映	ソフトウェア管理で管理しているソフトウェアを機器に反映します。 機器側からソフトウェアを取得し，アップデートコマンドにより機器に反映し，機器を再起動させて反映します。 なお，無停止ソフトウェアアップデートはサポートしていません。

ソフトウェア管理対象の機器モデルは，5.3.5(9)ソフトウェア管理対応機器に示します。

2.1.4　バックアップ管理

管理対象機器のバックアップを管理する機能を提供します。バックアップとは機器で稼働中のソフトウェア，および機器情報です。主な提供機能は，以下のようになります。

表 2-80　バックアップ管理の主な提供機能

項目	説明
機器ごとのバックアップの管理	機器ごとにバックアップを管理します。 AX2600S・AX2500S・AX2300S・AX2100S・AX260A シリーズはリストア用途にバックアップファイルをダウンロードできます。
取得したバックアップの機器への適用	ゼロタッチプロビジョニングにより機器へ適用します。

バックアップは，機器モデルごとに以下の方法で取得します。

表 2-81　バックアップの取得方法

機器モデル	取得方法
AX2600S シリーズ	運用コマンド backup
AX2500S シリーズ	運用コマンド backup
AX2300S シリーズ	運用コマンド backup
AX2100S シリーズ	運用コマンド backup
AXprimoM210 シリーズ	運用コマンド show startup-config によるコンフィグ取得，運用コマンド copy によるソフトウェアの取得
AX260A シリーズ	運用コマンド backup

(1) ゼロタッチプロビジョニングによる機器交換

機器でサポートされているゼロタッチプロビジョニング機能を利用して簡単に機器を交換する機能を提供します。主な提供機能は，以下のようになります。

表 2-82　ゼロタッチプロビジョニングによる機器交換の主な提供機能

項目	説明
機器交換の開始・終了	Web インタフェースから交換機器の筐体ラベルに記載されている MAC アドレスを入力し，ゼロタッチプロビジョニングによる機器交換の開始と終了ができます。
進捗の表示	機器交換の開始から完了までの進捗をグラフィカルに表示し，交換が完了したことを確認できます。
ゼロタッチプロビジョニングに必要な各種サーバ機能	ゼロタッチプロビジョニングに必要な各種サーバ機能(DHCP/TFTP)は AX-Network-Manager に組み込まれています。 機器交換中に，IP アドレスの割り当て，コンフィグレーション/バックアップファイルの配布，ソフトウェアの更新，起動を確認します。 なお，ゼロタッチプロビジョニングで交換機器に割り当てる IP アドレスは，すでに AX-Network-Manager で設定されている機器の IP アドレスとなります。
事前設定	Web インタフェースの構成管理設定のゼロタッチプロビジョニングで交換機器のサブネットとデフォルトゲートウェイの設定を行います。

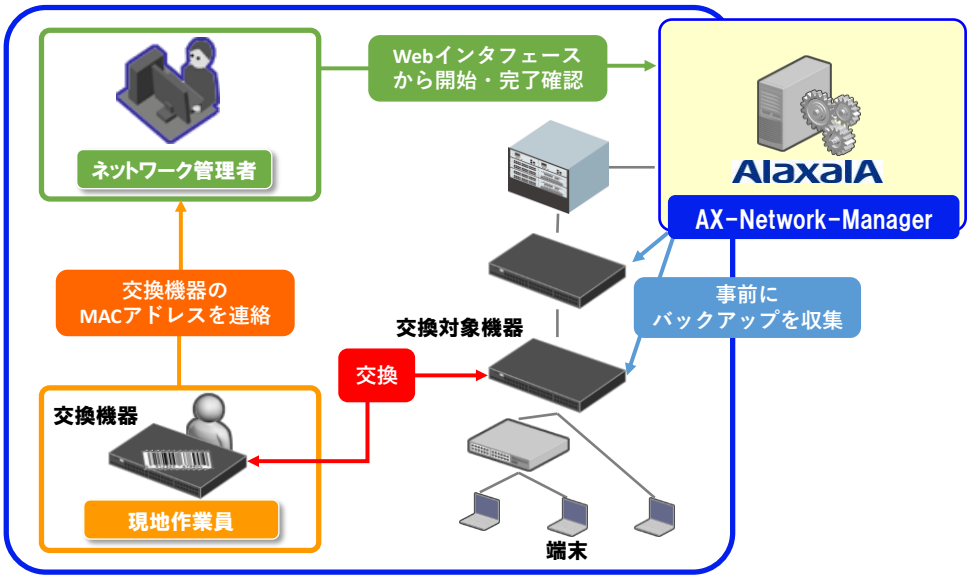

図 2-18　ゼロタッチプロビジョニングによる機器交換概要

2.1.5 シリアル情報管理

運用管理対象機器のシリアル情報を管理する機能を提供します。主な提供機能は，以下のようになります。

表 2-83 シリアル情報管理の主な提供機能

項目	説明
シリアル情報管理	機器ごとにシリアル情報の管理機能として以下を提供します。 ・シリアル情報の世代管理 ・世代ごとにコメントの付与 ・シリアル情報間の比較
シリアル情報取得	機器のシリアル情報を取得し，シリアル情報管理により管理します。

機器からのシリアル情報取得に対応する機器モデルは，5.3.5(11)シリアル情報管理対応機器に示します。

2.1.6 Web 管理情報配布

運用管理対象機器の SSL 証明書と Web 認証画面を配布する機能を提供します。主な提供機能は，以下のようになります。

表 2-84 Web 管理情報配布の主な提供機能

項目	説明
SSL 証明書管理	機器の SSL 証明書の管理機能として以下を提供します。 ・機器（配布グループ）で SSL 証明書を管理 ・機器（配布グループ）に SSL 証明書を反映
Web 認証画面管理	機器の Web 認証画面の管理機能として以下を提供します。 ・機器（配布グループ）で Web 認証画面を管理 ・機器（配布グループ）に Web 認証画面を反映 ・機器に適用済みの Web 認証画面を取得して配布グループを作成

Web 管理情報配布に対応する機器モデルは，5.3.5(12)Web 管理情報配布対応機器に示します。

2.1.7 ドキュメント出力

AX-Network-Manager が機器から収集している情報を用いて，ネットワーク構成に関する情報をドキュメントとして出力する機能を提供します。

AX-Network-Manager では，機器の情報を定期的に収集しており，最新の情報を用いてドキュメントを生成します。手動で作成する場合に比べ，機器から取得した情報から生成するため，変更の反映漏れが生じることが少なくなります。また，自動で情報収集し出力するため，作業量を減らすことが可能になります。

生成したドキュメントの保存には Excel ファイルでの書き出し，またはブラウザが備える印刷機能を用い，印刷や PDF での保存を行います。

ドキュメント出力の主な提供機能は，以下のようになります。

表 2-85 ドキュメント出力の機能概要

項目	説明
出力対象	ドキュメント出力対象を選択します。 ・全ての機器 ・ユーザが作成したマップ単位

項目	説明
ドキュメント情報	選択した出力対象の情報を出力します。出力する項目は以下から選択できます。 ・マップ一覧 ・各マップ情報 ・機器一覧 ・フロントパネル表示 ・機器情報 ・ハードウェア情報 ・インタフェース情報 ・チャネルグループ情報 ・L2 ループ検知情報 ・ストーム検知情報 ・輻輳情報 ・端末情報 ・WLC 接続端末情報 ・経路情報 ・VXLAN 情報（VXLAN トンネル情報，VLAN マッピング情報，サブインタフェースマッピング情報） ・コンフィグ情報 ・フィルタ情報 ・QoS 情報 ・ポートミラーリング情報 ・シリアル情報 ・Web 管理情報（SSL 証明書，Web 認証画面） ・ライセンス概要 ・ライセンス一覧
ドキュメントの保存	ドキュメントの保存方法は以下をサポートします。 ・Excel ファイル形式での保存 ・ブラウザが備える印刷機能による保存

2.1.8 タスク・スケジュール設定

機器の操作などを実行する単位をタスクと呼びます。タスクの種類は以下です。

表 2-86 タスクの種類

タスク
コンフィグレーションの取得
コンフィグレーションの設定（テンプレート）
コンフィグレーションの反映（含むテンプレート）
コンフィグレーションの保存
コンフィグレーションの保存状態確認
VLAN 設定
VXLAN トンネル設定
VXLAN VLAN マッピング設定
VXLAN サブインタフェースマッピング設定
セキュリティフィルタ追加
セキュリティフィルタ削除
セキュリティフィルタ変更
ポート設定
ポート状態設定

アクセスリスト設定
フィルタ有効化・無効化設定
QoS フローリスト設定
QoS 有効化・無効化設定
ポートミラーリング設定
バックアップの取得
ゼロタッチプロビジョニングによる機器交換
ソフトウェアの更新
シリアル情報の取得
SSL 証明書の反映
Web 認証画面の反映
Web 認証画面の取得
任意：<スクリプト任意処理内容>
情報採取：＜採取情報名＞
輻輳解析情報取得
スクリプト実行

タスクは Web インタフェースでの操作または，事前に定義したスケジュールによって，実行されます。
同一機器に対して一度に動作するタスクは一つです。タスクは順番に実行します。
スケジュールは，タスクの実行を登録することができ，繰り返しの実行または 1 回のみの実行として定義することができます。
繰り返しの実行は，毎月，毎週，毎日から選択し，実行する条件を指定します。1 回のみ実行する場合は，実行する日時を指定します。
スケジュール登録可能なタスクの種類は以下です。

表 2-87　スケジュール登録可能なタスクの種類

スケジュール登録可能なタスク
コンフィグレーションの取得
コンフィグレーションの設定（テンプレート）
コンフィグレーションの反映（含むテンプレート）
コンフィグレーションの保存
コンフィグレーションの保存状態確認
バックアップの取得
ソフトウェアの更新
シリアル情報の取得
SSL 証明書の反映
Web 認証画面の反映
情報採取：＜採取情報名＞

2.1.9　アイコン・画像設定

マップ等で表示される機器，ハブ，端末のアイコン画像をユーザが用意または AX-Network-Manager であらかじめ用意(プリセット)した画像に変更できます。
以下に示すアイコン条件に合致した場合に，指定したアイコン画像で表示します。ハブと端末は，条件に合致しない場合のデフォルト条件も設定できます。

表 2-88　機器アイコン条件

優先順位	条件	説明
1	機器名	個別指定として，機器ごとにアイコン画像を指定します。

優先順位	条件	説明
2	機器モデル	機器モデル指定として，機器モデルごとにアイコン画像を指定します。

表 2-89　ハブアイコン条件

優先順位	条件	説明
1	接続機器名 チャネルグループ名	個別指定として，接続機器のチャネルグループごとにアイコン画像を指定します。
2	接続機器名 ポート名	個別指定として，接続機器のポートごとにアイコン画像を指定します。
3	デフォルト	デフォルト指定として，上記条件に合致しない場合のアイコン画像を指定します。

表 2-90　端末アイコン条件

優先順位	条件	説明
1	MAC アドレス	個別指定として，端末（MAC アドレス）ごとにアイコン画像を指定します。
2	IP アドレス	個別指定として，端末（IP アドレス）ごとにアイコン画像を指定します。
3	端末エイリアスタイトル 1 端末エイリアス 1	端末エイリアス指定として，端末エイリアスタイトルとその端末エイリアスごとにアイコン画像を指定します。 端末アイコン条件に使用する端末エイリアスタイトルは 3 つまで選択できます。
4	端末エイリアスタイトル 2 端末エイリアス 2	
5	端末エイリアスタイトル 3 端末エイリアス 3	
6	ベンダ	ベンダ指定として，ベンダ名ごとにアイコン画像を指定します。
7	MAC アドレス/マスク	ベンダ指定として，MAC アドレス/MAC アドレスマスクごとにアイコン画像を指定します。 MAC アドレスマスクは優先順位順に，36/28/24bit を指定できます。

2.1.10　スクリプト設定

AX-Network-Manager の各種処理について，ユーザが自由に定義できるスクリプトを利用して処理を行います。
あらかじめ規定されている各種処理内容では，標準 MIB 対応機器，標準 MIB 対応機器(VLAN 毎コミュニティ)およびワイヤレス LAN コントローラを対象に処理を行います。任意に命名定義した処理（任意処理内容）については，機器もしくは IP アドレスを対象として，処理を行います。
各種処理を利用するためには，スクリプト設定にてスクリプトを登録してください。
スクリプト設定の主な提供機能は，以下です。

表 2-91　スクリプト設定の主な提供機能

項目	説明
スクリプト管理	スクリプトの管理機能を提供します。 ・各種処理内容のスクリプトと対象の登録 ・スクリプト一覧画面と RESTAPI からのスクリプトの実行 ・スクリプトの実行ログと結果の表示
スクリプトの登録	スクリプトは Ansible の playbook を利用します。 各種処理内容に，あらかじめ用意されているプリセット，もしくはカスタマイズしたスクリプトの内容と，対象とする機器を割り当てます。任意処理内容の場合は，対象として IP アドレス（全 IP アドレス対象のみ）も割り当てることもできます。
スクリプトによる各種処理	各種機能の処理動作時に，スクリプトが登録されている場合に，スクリプトを利用して処理を行います。
スクリプト一覧画面と RESTAPI からのスクリプト実行	スクリプト一覧画面と RESTAPI から複数の機器を対象にスクリプトを実行できます。任意処理内容のスクリプト（playbook）に任意の変数を埋め込み，実行時に値を指定して処理させることもできます。 なお，RESTAPI からのスクリプト実行の詳細については，別途，営業経由で問い合わせください。

スクリプトを利用する実行元，処理内容と対象は以下です。

表 2-92　スクリプト設定を利用する機能

実行元	処理内容	対象
コンフィグ取得	コンフィグ取得	標準 MIB 対応機器 標準 MIB 対応機器(VLAN 毎コミュニティ) ワイヤレス LAN コントローラ
コンフィグ設定	コンフィグ設定	
コンフィグ反映	コンフィグ反映	
コンフィグ保存	コンフィグ保存	
コンフィグ保存状態確認	コンフィグ保存状態確認	
シリアル取得	シリアル情報取得	
スクリプト通知	<任意処理内容>	全機器，全 IP アドレス
情報採取連携	<任意処理内容>	全機器

処理の一例をプリセットで提供します。スクリプト設定で利用可能なプリセットは以下です。

表 2-93　プリセット一覧

処理内容	対象	前提条件・動作説明	確認機種 (バージョン)
コンフィグ取得	AX6700S AX6600S AX6300S	-	AX6700S (11.9.V)
	Cisco IOS	-	Cisco Catalyst 3650 (16.3.1)
コンフィグ設定	AX6700S AX6600S AX6300S	コンフィグレーションを階層毎に順に投入し，設定により save します。（途中，規定外の応答があればエラーとしてコマンド投入を中断し失敗とします。）	AX6700S (11.9.V)

処理内容	対象	前提条件・動作説明	確認機種 (バージョン)
	Cisco IOS	scp サーバの有効化設定(ip scp server enable 等)と enable 権限のユーザ登録が必要です。 scp にてコンフィグレーションファイルを put し，copy flash:<file> running-config にてコンフィグレーションをまとめて設定し，設定により save します。 （途中，規定外の応答があればエラーとして失敗とします。）	Cisco Catalyst 3650 (16.3.1)
コンフィグ反映	AX6700S AX6600S AX6300S	scp にてコンフィグレーションファイルを put し，copy <file> startup-config にてコピーし，reload します。 （途中，規定外の応答があればエラーとして失敗とします。）	AX6700S (11.9.V)
	Cisco IOS	scp サーバの有効化設定(ip scp server enable 等)と enable 権限のユーザ登録が必要です。 scp にてコンフィグレーションファイルを put し，copy flash:<file> startup-config にてコピーし，reload します。 （途中，規定外の応答があればエラーとして失敗とします。）	Cisco Catalyst 3650 (16.3.1)
コンフィグ保存	AX6700S AX6600S AX6300S	-	AX6700S (11.9.V)
	Cisco IOS	-	Cisco Catalyst 3650 (16.3.1)
コンフィグ保存状態確認	AX6700S AX6600S AX6300S	-	AX6700S (11.9.V)
	Cisco IOS	-	Cisco Catalyst 3650 (16.3.1)
シリアル情報取得	AX6700S AX6600S AX6300S	-	AX6700S (11.9.V)
	Cisco IOS	-	Cisco Catalyst 3650 (16.3.1)
任意処理内容 （スクリプト通知）	AX- Network- Manager	-	CentOS7
任意処理内容 （情報採取連携）	AX- Network- Manager	-	CentOS7

スクリプトは Ansible の playbook を登録できます。カスタマイズする場合の仕様を次表に示します。なお，一般的な playbook の作成方法は以下も参考にしてください。また，運用前には十分なテストをおこなってください。
https://github.com/alaxalanetworks/ansible-guidebook/blob/master/N18R001_Ansible_Guide_Chapter3.md

表 2-94　カスタマイズ仕様（共通）

項目	内容	詳細
対象	対象は 1 台です。1 台ずつ実行します。	hosts には”node”を指定してください。(例：- hosts: node) 対象は機器となります。ただし，実行元が，スクリプト通知で機器からの通知以外（監視対象状態異常検知等）の場合，対象は IP アドレスとなります。
変数	ansible_host	対象（機器または IP アドレス）の IP アドレスを利用できます。
	ansible_user	各機器設定で設定済のユーザ名を利用できます。（対象が機器の場合のみ）
	ansible_password	各機器設定で設定済のログインパスワードを利用できます。（対象が機器の場合のみ）
	ansible_become_password	各機器設定で設定済の管理者パスワードを利用できます。(対象が機器の場合のみ)
	axnm_result	スクリプトの実行結果をこの変数に格納されているファイルパスへ保存してください。 実行結果の仕様は，表 2-95　カスタマイズ仕様（各処理内容）に詳細を規定します。
	axnm_watch_name	監視対象が属する監視項目名を利用できます。(実行元が，スクリプト通知の監視対象状態異常検知の場合のみ) 例：対象 IP アドレス(127.0.0.1)のスクリプト実行の場合 「監視項目名(スクリプト実行)」
	axnm_watch_target_hostname	監視対象のホスト名（設定が無い場合は空文字）を利用できます。(実行元が，スクリプト通知の監視対象状態異常検知の場合のみ) 例：対象 IP アドレス(127.0.0.1)のスクリプト実行の場合 「localhost」
	axnm_collect_filepath	採取情報管理機能で情報採取したファイルのパスを利用できます。（実行元が，情報採取の場合のみ） 例：対象機器へのスクリプト実行の場合 「/usr/local/share/axnm/static/collection/collect_test.txt」
	axnm_config_filepath	反映するコンフィグレーションが格納されたローカルファイルパスを利用できます。(処理内容が，「コンフィグ反映」の場合のみ) なお，このファイルは変更・削除しないでください。 例：対象機器へのスクリプト実行の場合 「コンフィグ管理で最新に登録されているコンフィグレーションのファイルパス」(登録されていない場合は，このファイルパスにはアクセスできません)
	axnm_config_filesize	反映するコンフィグレーションが格納されたローカルファイルのサイズを利用できます。（処理内容が，「コンフィグ反映」の場合のみ） 例：対象機器へのスクリプト実行の場合 「コンフィグ管理で最新に登録されているコンフィグレーションのファイルサイズ」（登録されていない場合は，0）
	axnm_config_text	テンプレートで生成されたコンフィグレーションの文字列を利用できます。(処理内容が，「コンフィグ設定」の場合のみ) 例：対象機器へのスクリプト実行の場合 「'hostname TEST'」

項目	内容	詳細
	axnm_config_lines	テンプレートで生成されたコンフィグレーションを行単位に分割した文字列のリストを利用できます。（処理内容が，「コンフィグ設定」の場合のみ） 例：対象機器へのスクリプト実行の場合 「['hostname TEST']」
	axnm_config_parent_lines	テンプレートで生成されたコンフィグレーションを階層単位に分割したリストを利用できます。（処理内容が，「コンフィグ設定」の場合のみ） 例：対象機器へのスクリプト実行の場合 「[{'lines': ['hostname TEST'], 'parent': []}]」
	axnm_config_command_timeout	テンプレートで設定されているコマンド毎のタイムアウト時間(秒)を利用できます。（処理内容が，「コンフィグ設定」の場合のみ） 例：対象機器へのスクリプト実行の場合 「30」
	axnm_config_save	テンプレートの動作後コンフィグ取得設定または構成管理設定のコンフィグ変更時保存設定による，コンフィグ設定後のコンフィグ保存有無(True/False)を利用できます。（処理内容が，「コンフィグ設定」の場合のみ） 例：対象機器へのスクリプト実行の場合 「False」
	axnm_custom_< 任意の英数字とアンダースコア>	スクリプト（playbook）に埋め込まれた任意の変数を利用できます。（スクリプト実行［スクリプト設定画面または RESTAPI からの実行］の場合のみ）
リターンコード	正常終了時は 0 を返してください	0 以外は，各処理内容が失敗となります。

表 2-95　カスタマイズ仕様(各処理内容)

処理内容	実行結果	リターンコード
コンフィグ取得	コンフィグレーションの文字列を入れてください。文字列が空の場合は登録しません。	0 以外は処理が失敗となります。 この場合，実行結果にエラーメッセージを入れることで，スクリプトログやタスクの実行結果で表示することができます。
コンフィグ設定	不要です。	
コンフィグ反映	不要です。	
コンフィグ保存	不要です。	
コンフィグ保存状態確認	未保存(差分あり)の場合は”True”，保存済み(差分なし)の場合は”False”の文字列を入れてください。	
シリアル情報取得	シリアル情報の文字列を入れてください。文字列が空の場合は登録しません。	
<任意処理内容>（情報採取テキスト出力の場合)	コマンド実行応答の文字列を入れてください。	
<任意処理内容>（その他の場合）	不要です。	

2.1.11 採取情報管理

管理対象機器から任意コマンドによる情報採取を行い，管理する機能を提供します。主な提供機能は，以下のようになります。

表 2-96 採取情報管理の主な提供機能

項目	説明
採取情報管理	任意の情報採取コマンドなどの情報を採取情報として管理します。採取情報は 1 つの採取コマンドセットに対して複数機器を対応付ける形となります。 ・任意の情報採取コマンド 情報採取に使用する機器のコマンドとして以下を登録できます。 ➢ CLI コマンド (管理者モードで実行, AX620R はコンフィグモードで実行します。) ➢ シェルコマンド (AX8600S,AX8300S,AX4600S,AX3800S,AX3660S,AX3650S,AX3640S,AX2600S,AX2300S シリーズのみサポート) CLI コマンドの場合は’#’，シェルコマンドの場合は’$’ ’ >’を応答プロンプトとして待ち合わせる動作となります。シェルコマンドでは exit，return，不正なシェルコマンドを指定した場合，情報採取が応答タイムアウトで失敗となります。 管理者パスワードが設定されている機器で show tech-support コマンドを実行した場合は, AX-Network-Manager がパスワード入力をおこないます。 ・採取方法 以下の採取方法をサポートします。 ➢ テキスト出力 任意のコマンドを実行した画面出力結果を採取情報としてテキストファイルで保存します。 ➢ ファイル転送(FTP) 任意コマンド実行後，機器から AX-Network-Manager に対してファイルを転送し，転送したファイルを保存します。 (AX8600S,AX8300S,AX4600S,AX3800S,AX3660S,AX3650S,AX3640S,AX2600S,AX2300S シリーズのみサポート)
機器からの情報採取	telnet/SSH により機器にログインし，登録した任意の情報採取コマンドを実行し，その結果を AX-Network-Manager に登録し保存します。採取契機は手動登録，イベント連携の 2 種類をサポートします。 ・手動登録 Web インタフェースから採取し登録できます。 ・イベント連携 イベント一覧に登録される障害等復旧が必要な重要なイベント発生契機で採取します。情報採取通知先情報として，採取情報とイベント種別を紐づけて登録し，イベント発生時に対応付けられた採取情報の任意コマンドを実行します。

項目	説明
採取情報履歴管理	情報採取で登録保存した情報の履歴を管理します。 Web インタフェース上で機器×採取情報毎に保存情報の履歴を表示し，ダウンロードや削除操作を可能とします。また，テキスト情報の場合はテキスト表示や他履歴との差分表示が可能です。 履歴情報は採取情報毎に設定した最大履歴保持数を超過すると，古いものから自動的に削除を行います。この際，採取したファイルもディスク上から削除します。
情報採取後のスクリプト実行	情報採取後にスクリプト設定にて登録した任意処理内容のスクリプトを実行します。スクリプトでは採取したファイルに対する操作も可能です。 ・手動登録 Web インタフェースからの採取時に，スクリプト実行有無を選択できます ・イベント連携 情報採取通知先毎にスクリプト実行有無を設定します

以下に採取情報の設定例を示します。

表 2-97　採取情報設定例

採取例	機能	項目	設定例
機器状態異常検知（障害，軽度障害，注意）時に，ハードウェアおよびソフトウェアの状態を示す基本情報の採取	情報採取通知先情報	通知先名称	他の通知先名称と重複しない名称を設定してください
		採取情報	採取情報設定で設定した採取情報名を設定してください
		通知	有効
		通知時の操作ログ出力	有効
		イベント	機器状態異常検知 : 障害，軽度障害，注意
	採取情報設定	採取情報名	他の採取情報名と重複しない名称を設定してください
		採取方法	テキスト出力
		コマンド	# show tech-support
		タイムアウト時間(秒)	600
		履歴保持数	10
		対象機器名	本コマンドの対象機器を選択します
		スクリプト任意処理内容	実行後にスクリプトを実施する場合，スクリプト設定で設定したスクリプト任意処理内容を指定します。
ネットワーク管理モジュールおよび SW 部の情報を採取	情報採取通知先情報	通知先名称	他の通知先名称と重複しない名称を設定してください
		採取情報	採取情報設定で設定した採取情報名を設定してください
		通知	有効

採取例	機能	項目	設定例
		通知時の操作ログ出力	有効
		イベント	機器状態異常検知 : 障害，軽度障害，注意
	採取情報設定	採取情報名	他の採取情報名と重複しない名称を設定してください
		採取方法	ファイル転送(FTP)
		コマンド	# /usr/local/diag/nimdump | gzip > nimdump.gz
		タイムアウト時間(秒)	600
		履歴保持数	10
		転送ファイル名	nimdump.gz
		転送後ファイル削除	有効
		対象機器名	本コマンドの対象機器を選択します
		スクリプト任意処理内容	実行後にスクリプトを実施する場合，スクリプト設定で設定したスクリプト任意処理内容を指定します

2.1.12 ダッシュボード

ネットワークの運用状態や AX-Network-Manager の状態，マップへのリンクおよび各種グラフを表示し，ユーザがアクションをとるのに有用な情報を提供します。

ユーザ毎に複数のダッシュボードを作成することができ，各種状況やグラフなどのアイテムを追加し，移動・リサイズ・削除と自由にカスタマイズができます。

表 2-98 ダッシュボードの主な提供機能

項目	説明
ダッシュボードカスタマイズ	項目枠内に各種アイテムを自由に配置し，ダッシュボードをカスタマイズできます。 ・項目枠 名前を付けて，複数のアイテムを配置・表示できる枠です。 ・アイテム 各種状態やグラフなどの情報表示部分です。 カスタマイズしたダッシュボードは，ユーザ毎または全ユーザ共用として保存できます。 なお，トップページに表示されるダッシュボードは，ユーザ毎に以下の優先度で選択されます。 1. ユーザ毎ダッシュボード（デフォルト表示設定のもの） 2. 全ユーザ共用ダッシュボード（デフォルト表示設定のもの） 3. ユーザ毎ダッシュボード 4. 全ユーザ共用ダッシュボード
ユーザ毎ダッシュボード	ユーザ毎に，ダッシュボードに名前を付けて複数のパターンで保存・表示ができます。ユーザ毎ダッシュボードは自ユーザだけが表示・保存・削除できます。

項目	説明
全ユーザ共用ダッシュボード	全ユーザ共用として，全ユーザが表示できるダッシュボードを保存できます。全ユーザ共用ダッシュボードはアドミニストレータまたはネットワーク管理者だけが保存・削除できます。参照ユーザは，表示されたものをコピーして自ユーザのダッシュボードとして保存できます。
アイテム	ダッシュボードに表示できるアイテムは以下です。 ・状況 ・イベント対応 ・機器 ・接続 ・監視対象 ・コンフィグ ・バックアップ ・ライセンス ＜ライセンス種別＞ ・グラフ ・機器回線（使用帯域グラフ） ・監視対象（MIB 監視履歴グラフ） ・フィルタ（パケット数グラフ） ・QoS（パケット数グラフ） ・グラフオプション ・機器回線（使用帯域収集状況） ・フィルタ（パケット数収集状況） ・QoS（パケット数収集状況） ・マップ

2.1.13 ユーザ設定

AX-Network-Manager を操作するには，Web インタフェースからユーザ名とパスワードを用いてログイン認証する必要があります。ログインするユーザは，ユーザ設定から登録しておきます。

ユーザには以下の種類の権限を指定でき，権限により操作範囲を限定して運用させることができます。なお，操作できない項目は Web インタフェースに表示されません。

表 2-99 ユーザ権限の種類と操作範囲

権限 / 操作範囲	アドミニストレータ	ネットワーク管理者	参照ユーザ
参照	○	○	△ ※機器一覧の CSV 出力等は，管理情報等が含まれるため不可
AX-Network-Manager や機器への変更を伴う操作	○	○	×
ダッシュボードの変更等操作	△ ※自ユーザと共用のものは可	△ ※自ユーザと共用のものは可	△ ※自ユーザのものは可
ライセンス変更	○	×	×
ユーザ設定	○	△ ※自ユーザのパスワード変更は可	△ ※自ユーザのパスワード変更は可

【凡例】○:操作可　△:一部可　×:操作不可

2.1.14 リソース管理

AX-Network-Manager を動作させているサーバのリソース状態を管理し，リソースの異常状態を検知，また通知を行います。リソース管理の主な提供機能は，以下です。

表 2-100 リソース管理の主な提供機能

項目	説明
ディスク使用量監視	ディスク使用量を周期的に監視し，設定した閾値の超過を検知します。監視対象はディレクトリ単位に複数の監視対象を設定できます。
データベース状態監視	データベースシステムが正常に動作していることを監視し，異常発生を検知します。 監視対象は以下になります。 ・AUTOVACUUM 実行状態 PostgreSQL において，AUTOVACUUM 機能によって不要になったディスク領域を空き領域として管理しています。AUTOVACUUM が長時間実施されないと，データベースを更新/削除する度にディスク使用量が増加し続けるため，状態を監視し，一定時間動作していないことを検知した場合には通知を行います。

2.1.15 RESTAPI

外部のアプリケーションから AX-Network-Manager の情報を収集，または操作することができる RESTAPI を用意しています。RESTAPI でのアクセス時には，AX-Network-Manager のユーザ認証が必要です。認証方式として，トークン認証をサポートしており，事前にユーザ設定で設定しておく必要があります。
RESTAPI の仕様については，別途，営業経由で問い合わせください。

2.2 Ver.1.7 での新機能の概要

2.2.1 ネットワーク管理

(1) フロントパネル表示対応機器の追加

下記機器モデルのフロントパネル表示対応をおこないました。

・AX2340S
　　・AX2340S-16P8MP2X
・AX2130S
　　・AX2130S-24PH

(2) AX2600S のサポート

管理対象機器モデルとして AX2600S をサポートしました。本機器モデルでは，フロントパネル表示，L2 ループ検知，ストーム検知，輻輳管理，Web ターミナル，コンフィグ管理，ソフトウェア管理，バックアップ管理，シリアル情報管理，Web 管理情報配布，フィルタ管理，QoS 管理，およびポートミラーリング管理の各機能が利用できます。

(3) AX2500S シリーズ用予備電源機構の監視機能サポート

AX2500S シリーズ用予備電源機構の状態を監視する機能をサポートしました。

(4) AXprimoW 対応アクセスポイント機器の追加

AXprimoW アクセスポイントである EAP101，EAP102 からの端末情報の取得をサポートしました。EAP101, EAP102 は，バージョン 1.14.1 以降で動作している必要があります。

(5) 標準 MIB 対応機器，標準 MIB 対応機器(VLAN 毎コミュニティ)，ワイヤレス LAN コントローラのフロントパネルカスタマイズ機能のサポート

標準 MIB 対応機器，標準 MIB 対応機器(VLAN 毎コミュニティ)，ワイヤレス LAN コントローラの機器モデルを対象に，機器詳細上でのフロントパネルの表示，およびカスタマイズ機能をサポートしました。本機能により，ポートの状態を GUI で確認可能となります。

(6) 収容条件：管理対象機器数の拡大

管理対象機器数を 1,000 台から 1,500 台に拡大しました。

(7) マップ表示：監視対象の表示

マップ上で，監視対象の表示をサポートしました。本機能を使用することで，監視対象の位置，状態を確認することが可能となります。

(8) マップ表示：CEF の syslog メッセージ該当端末の表示

マップ上で，CEF の syslog メッセージ該当端末の表示をサポートしました。本機能を使用することで，CEF の syslog メッセージ該当端末の位置を確認することが可能となります。

2.2.2 監視対象管理

(1) MIB 監視履歴の一括ダウンロード機能のサポート

監視対象から取得した MIB 監視履歴について，一括してダウンロードする機能をサポートしました。

2.2.3 セキュリティフィルタ管理

(1) エイリアス未登録端末の通信遮断のサポート

エイリアス未登録端末を検出した際，当該端末を通信遮断する機能をサポートしました。

2.2.4 SNMP トラップ受信管理

(1) SNMP トラップの受信監視機能のサポート

受信した任意の SNMP トラップをイベント管理に登録・通知する受信監視機能をサポートしました。

2.2.5 syslog 受信管理

(1) syslog 受信フィルタ設定機能のサポート

機器，サーバ等から通知される syslog について，ファシリティ，重要度，内容，送信元を元に，受信または廃棄を制御する機能をサポートしました。

(2) syslog の受信監視機能のサポート

受信した任意の syslog をイベント管理に登録・通知する受信監視機能をサポートしました。

(3) 収容条件：受信 syslog 保持数の拡大

受信 syslog 保持数を 100,000 から 2,000,000 に拡大しました。

2.2.6 通知管理

(1) 通知詳細設定・抑止スケジュール設定機能のサポート

syslog 通知先等の個々の通知先について，通知元(AX-Network-Manager 全体，機器，ハードウェア，インタフェース，監視対象，受信監視条件)を絞り込むことが可能な通知詳細設定機能をサポートしました。および，通知詳細設定単位に，通知を抑止するスケジュール設定機能もサポートしました。

2.2.7 コンフィグ管理

(1) コンフィグレーションの一括ダウンロード機能のサポート

機器から収集した最新のコンフィグレーションについて，一括してダウンロードする機能をサポートしました。

2.2.8 テンプレート管理

(1) テンプレート管理機能のサポート

コンフィグレーションをテンプレートとして作成することで，複数の運用管理対象機器に対して，一括してコンフィグレーションを設定・反映できる機能をサポートしました。本機能の使用には，スタンダードライセンスが必要となります。

2.2.9 フィルタ管理

(1) アクセスリスト抽出と機器反映の対応機器の追加

下記機器について，アクセスリスト抽出と機器反映の対応をおこないました。機器反映機能の使用には，スタンダードライセンスが必要となります。

- AX8600S/AX8300S シリーズ
- AX2200S シリーズ
- AX1200S シリーズ
- AX260A シリーズ

(2) フィルタ情報カウンタのグラフ表示機能のサポート

下記機器について，機器から MIB カウンタ情報を収集し，グラフ表示する機能をサポートしました。本機能の使用には，スタンダードライセンスが必要となります。

- AX8600S/AX8300S シリーズ
- AX4600S シリーズ
- AX3800S シリーズ
- AX3660S
- AX3650S
- AX3640S
- AX2600S シリーズ
- AX2300S シリーズ

2.2.10 QoS 管理

(1) QoS 管理機能のサポート

下記機器について，収集したコンフィグレーションから QoS フローリストを抽出，および抽出した QoS フローリストを使用して，機器に反映する機能をサポートしました。
本機能の使用には，スタンダードライセンスが必要となります。

- AX8600S/AX8300S シリーズ
- AX4600S シリーズ
- AX3800S シリーズ
- AX3660S
- AX3650S
- AX3640S
- AX2600S シリーズ
- AX2500S シリーズ
- AX2300S シリーズ
- AX2200S シリーズ
- AX2100S シリーズ
- AX1200S シリーズ
- AX260A シリーズ

および下記機器について，機器から MIB カウンタ情報を収集し，グラフ表示する機能をサポートしました。本機能の使用には，スタンダードライセンスが必要となります。

- AX8600S/AX8300S シリーズ
- AX4600S シリーズ
- AX3800S シリーズ
- AX3660S
- AX3650S
- AX3640S
- AX2600S シリーズ
- AX2300S シリーズ

2.2.11 ポートミラーリング管理

(1) ポートミラーリング管理機能のサポート

下記機器について，収集したコンフィグレーションからポートミラーリングを抽出，および抽出したポートミラーリングを使用して，機器に反映する機能をサポートしました。本機能の使用には，スタンダードライセンスが必要となります。

- AX8600S/AX8300S シリーズ
- AX4600S シリーズ
- AX3800S シリーズ
- AX3660S
- AX3650S
- AX3640S
- AX2600S シリーズ
- AX2500S シリーズ
- AX2300S シリーズ
- AX2200S シリーズ
- AX2100S シリーズ
- AX1200S シリーズ
- AX260A シリーズ

2.2.12 管理機能

(1) ダッシュボードにおけるユーザ単位カスタマイズ機能のサポート
ユーザ毎に複数のダッシュボードを作成するカスタマイズ機能をサポートしました。本機能により，各種状況やグラフなどのアイテムを追加し，移動・リサイズ・削除と自由にカスタマイズすることができます。

(2) 機器間の隣接関係自動抽出機能のサポート
LLDP(Link Layer Discovery Protocol)を使用できないような構成においても，機器間のポートの隣接関係を自動的に抽出する機能をサポートしました。本機能により，手動で接続情報を設定せずとも，端末を収容しているポートの特定が可能になります。

(3) 端末管理におけるエイリアス未登録端末の syslog 通知と E-mail 通知機能のサポート
エイリアス未登録端末を検知した際，syslog や E-mail で通知する機能をサポートしました。

(4) 収容条件：管理対象外ポート数の拡大
管理対象外ポート数を 64 から 128 に拡大しました。

(5) タスク・スケジュール管理における採取情報スケジュール機能の追加
タスク・スケジュール管理において，採取情報をスケジュールする機能をサポートしました。

(6) スクリプト管理における任意処理の実行機能のサポート
スクリプト管理において，Ansible Playbook を使用した任意の処理を実行する機能をサポートしました。

(7) 採取情報管理における一括ダウンロード機能のサポート
機器の採取情報単位に，取得した採取情報を一括してダウンロードする機能をサポートしました。

(8) リソース管理機能のサポート
AX-Network-Manager が動作するサーバのディスク容量や，データベースのテーブルの状態を監視する機能をサポートしました。

2.2.13 その他

(1) オペレーティングシステム MIRACLE LINUX8 の追加
オペレーティングシステムに，MIRACLE LINUX8 を追加しました。

(2) 画面自動更新機能のサポート
Web インタフェースの画面を自動更新する機能をサポートしました。

3. ライセンス

3.1 ライセンスの構成

AX-Network-Manager は，サブスクリプション形式のソフトウェアです。

本ソフトウェアは，使用する機能に応じたライセンス種別の，管理対象機器台数分のライセンスを導入する必要があります。また，動作環境に合わせて「オンプレミス版」「クラウド版」を選択しご購入ください。

本ソフトウェアは，下記のライセンスからなります。

表 3-1　ライセンスの内訳

項目	説明
エッセンシャル機能ライセンス	AX-Network-Manager を使用するためのライセンス。 管理対象機器は，エッセンシャル機能として定めた機能を使用できます。 購入した管理対象機器台数分を管理対象にできます。
スタンダード機能ライセンス	AX-Network-Manager を使用するためのライセンス。 管理対象機器は，スタンダード機能として定めた機能を使用できます。エッセンシャル機能ライセンスよりも上位に位置付けられ，エッセンシャル機能ライセンスで提供する機能を包含します。 購入した管理対象機器台数分を管理対象にできます。
ワイヤレス LAN コントローラライセンス	ワイヤレス LAN コントローラ，および AXprimoW を管理するためのライセンスです。 購入した管理対象機器台数分を管理対象にできます。
外部連携ライセンス：トレンドマイクロ DDI/PM との連携	トレンドマイクロ DDI/PM との連携のためのライセンスです。 スタンダード機能ライセンスも必要です。
外部連携ライセンス：パロアルトネットワークス 次世代ファイアウォールとの連携	パロアルトネットワークス 次世代ファイアウォールとの連携のためのライセンスです。 スタンダード機能ライセンスも必要です。
外部連携ライセンス：Syslog 連携(CEF)	Syslog(CEF)との連携のためのライセンスです。 スタンダード機能ライセンスも必要です。
監視対象拡張オプションライセンス	管理対象機器以外で監視機能を使用するためのライセンスです（管理対象機器でも，ライセンス無効・なしの場合は，本ライセンスの対象となります）。購入した監視対象台数分を監視対象にできます。

オンプレミス版では，エッセンシャル機能ライセンス/スタンダード機能ライセンスで必要となる管理対象機器台数分をご購入ください。クラウド版では，まずエッセンシャル機能基本ライセンス/スタンダード機能基本ライセンスをご購入頂いたうえで，必要となる管理対象機器台数分を追加ご購入ください。

ライセンス種別ごとのサポート機能は，以下のようになります。

表 3-2　ライセンス種別ごとのサポート機能

機能名	エッセンシャル機能ライセンス	スタンダード機能ライセンス	ワイヤレス LAN コントローラライセンス
ネットワーク管理※2	○	○	○
ネットワーク管理(セキュリティ機器連携)	×	○	×
監視対象管理	○※1	○※1	○※1
イベント管理	○	○	○
操作ログ管理	○	○	○
SNMP トラップ受信管理	○※1	○※1	○※1
syslog 受信管理	○※1	○※1	○※1
受信監視設定	○※1	○※1	○※1
通知設定	○	○	○
コンフィグ管理	○	○	○
テンプレート管理	×	○	○
機器への設定 ・ポート設定 ・VLAN 設定 ・VXLAN 設定 ・アクセスリスト設定， フィルタ有効化・無効化設定 ・QoS フローリスト設定， QoS 制御有効化・無効化設定 ・ポートミラーリング設定	×	○	×
機器への設定 ・　ポート状態変更	○	○	－
ソフトウェア管理	○	○	－
バックアップ管理	○	○	－
シリアル情報管理	○	○	○
Web 管理情報配布	○	○	－
ドキュメント出力	○	○	○
タスク・スケジュール設定	○	○	○
アイコン・画像設定	○	○	○
スクリプト設定	○	○	○
採取情報管理	○	○	○
ダッシュボード	○	○	○
リソース管理	○	○	○
ユーザ設定	○	○	○
RESTAPI	○	○	○

【凡例】○:対応　×:非対応　－:未サポート

※1 管理対象機器以外の監視対象については，監視対象拡張オプションライセンスが必要です。

※2 フィルタ情報カウンタ収集，および QoS カウンタ収集については，スタンダードライセンスが必要です。

3.2 使用期間

オンプレミス版ライセンスは，初年度ライセンス(納入日翌月から 15 か月後の月末まで有効)と，1 年延長ライセンス(12 か月有効)の 2 つに分類されます。クラウド版ライセンスは，初年度ライセンス(納入日翌月 1 日を起点とし，12 か月後の月末まで有効)と，1 年延長ライセンス(12 か月有効)の 2 つに分類されます。初回は初年度ライセンスを購入いただき，2 年目以降継続利用する場合は，初年度ライセンスと同じ種別の同じ管理対象機器台数の 1 年延長ライセンスの購入が必要です。

使用期間を超過すると，AX-Network-Manager で機器を管理できなくなります。また，有効なライセンスが 1 つもなくなると，AX-Network-Manager で収集した情報が参照できなくなります。

ライセンスの使用期間例を下記に示します。

表 3-3 ライセンスの使用期間例

1 年目	2 年目以降
エッセンシャル機能 機器 50 台ライセンス (初年度ライセンス)	エッセンシャル機能 機器 50 台ライセンス (1 年延長ライセンス)
スタンダード機能 機器 10 台ライセンス (初年度ライセンス)	スタンダード機能 機器 10 台ライセンス (1 年延長ライセンス)

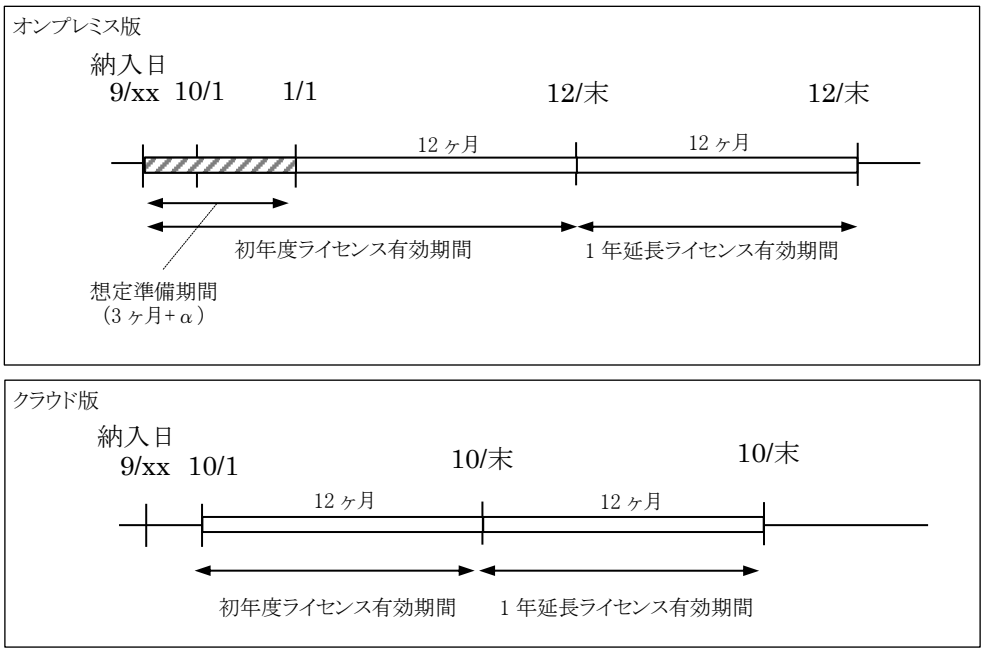

図 3-1 使用期間例

4. 機能一覧

AX-Network-Manager の機能一覧を下記に示します。

表 4-1 機能一覧

分類	機能			備考
ネットワーク管理	機器情報表示			
		ハードウェア情報表示		
		インタフェース情報表示		
		チャネルグループ情報の表示		
		回線使用帯域グラフ表示		
		フロントパネル表示		
		フロントパネル表示(標準MIB対応機器等)		
	Webターミナル			
	ハードウェア状態監視			
	L2ループ検知			
	ストーム検知			
	輻輳検知			
	接続情報表示			
	端末情報表示			
		無線LAN端末位置の表示		
	端末接続履歴管理			
	経路管理			
	マップ表示			
		VLANの表示		
		VXLANの表示		
		L2ループ発生箇所の表示		
		経路情報(IPv4)の表示		
		監視対象の表示		
		CEFのsyslogメッセージ該当端末の表示		
監視対象管理	Ping監視			
	MIB監視			
セキュリティフィルタ管理	通信遮断・例外通信許可			
	詳細ミラー			
	端末移動追従			
	IPv4アドレス・IPv6アドレス連携			
	自動解除	スケジュール解除		
		タイマー解除		
	特定端末へのWeb通信不可表示機能			
	未登録エイリアス端末の通信遮断			
	外部連携	トレンドマイクロ DDI/PMとの連携		
ルールマッチ履歴管理	セキュリティフィルタ適用			
セキュリティ連携機器管理	インシデント受け付けプロトコル	syslog	CEFのsyslogメッセージ	
	インシデント抽出	syslogメッセージ抽出		
	インシデント抽出ルール管理			
	外部連携	パロアルトネットワークス 次世代ファイアウォールとの連携		
		Syslog連携(CEF)		
		任意CEFフィールドの登録		
イベント管理	イベント表示・対応状況管理			
操作ログ管理	操作ログ表示			
SNMPトラップ受信管理	受信SNMPトラップの表示			
	SNMPトラップの受信監視			
syslog 受信管理	受信syslogの表示			
	syslog受信フィルタ設定			
	syslogの受信監視			
通知管理	syslog通知			
	E-mail通知			
	SNMP通知			
	スクリプト通知			
	情報採取通知			

分類	機能			備考
	通知詳細設定・抑止スケジュール設定			
コンフィグ管理	コンフィグレーションの履歴管理			
	コンフィグレーションを機器から取得			
	コンフィグレーションを機器へ反映			
テンプレート管理	テンプレートからのコンフィグレーション反映・設定			
機器への設定	ポート設定			
	VLAN設定			
	VXLAN設定			
ソフトウェア管理	ソフトウェアの世代管理			
	ソフトウェアの機器反映			
バックアップ管理	バックアップの収集			
	バックアップの機器反映	ゼロタッチプロビジョニング		
シリアル情報管理	シリアル情報の収集			
Web 管理情報配布	SSL証明書の配布			
	Web認証画面の配布			
フィルタ管理	フィルタの機器反映			
	フィルタ情報カウンタのグラフ表示			
QoS 管理	QoSの機器反映			
	QoSカウンタのグラフ表示			
ポートミラーリング管理	ポートミラーリングの機器反映			
ドキュメント出力	Web表示			
	Excelファイル形式			
管理機能	管理者機能	ダッシュボード		
			ユーザ単位カスタマイズ	
		機器管理		
			設定支援による登録	
		接続管理		
			LLDPによる接続検出	
			静的なポート接続情報設定	
			アクセスリスト拡張ポート	
		端末管理		
			端末エイリアス管理	
			管理対象外ポート管理	
		マップ管理		
		タスク・スケジュール管理		
		スクリプト管理		
			任意処理の実行	
		採取情報管理		
		アイコン管理		
		画像管理		
		ユーザ管理		
		セグメント管理		
		セキュリティ連携設定		
		リソース管理設定		
	RESTAPI			
	運用・保守	バックアップ・リストア		
		保守情報採取		
ライセンス	AX-NMエッセンシャル機能 機器10台 ・初年度ライセンス			
	AX-NMエッセンシャル機能 機器10台 ・1年延長ライセンス			
	AX-NMエッセンシャル機能 機器20台 ・初年度ライセンス			
	AX-NMエッセンシャル機能 機器20台 ・1年延長ライセンス			
	AX-NMエッセンシャル機能 機器50台 ・初年度ライセンス			
	AX-NMエッセンシャル機能 機器50台 ・1年延長ライセンス			

分類	機能	備考
	AX-NMスタンダード機能 機器10台 ・初年度ライセンス	
	AX-NMスタンダード機能 機器10台 ・1年延長ライセンス	
	AX-NMスタンダード機能 機器20台 ・初年度ライセンス	
	AX-NMスタンダード機能 機器20台 ・1年延長ライセンス	
	AX-NMスタンダード機能 機器50台 ・初年度ライセンス	
	AX-NMスタンダード機能 機器50台 ・1年延長ライセンス	
	ワイヤレスLANコントローラ1台まで ・初年度1年ライセンス	
	ワイヤレスLANコントローラ1台まで ・1年延長ライセンス	
	外部連携ライセンス:トレンドマイクロ DDI/PMとの連携 ・初年度1年ライセンス	
	外部連携ライセンス:トレンドマイクロ DDI/PMとの連携 ・1年延長ライセンス	
	外部連携ライセンス:パロアルトネットワークス 次世代ファイアウォールとの連携 ・初年度1年ライセンス	
	外部連携ライセンス:パロアルトネットワークス 次世代ファイアウォールとの連携 ・1年延長ライセンス	
	外部連携ライセンス:Syslog連携(CEF) ・初年度1年ライセンス	
	外部連携ライセンス:Syslog連携(CEF) ・1年延長ライセンス	
	AX-NMクラウド エッセンシャル機能 基本(機器20台) ・初年度ライセンス	
	AX-NMクラウド エッセンシャル機能 基本(機器20台) ・1年延長ライセンス	
	AX-NMクラウド エッセンシャル機能 機器10台 ・初年度ライセンス	
	AX-NMクラウド エッセンシャル機能 機器10台 ・1年延長ライセンス	
	AX-NMクラウド エッセンシャル機能 機器20台 ・初年度ライセンス	
	AX-NMクラウド エッセンシャル機能 機器20台 ・1年延長ライセンス	
	AX-NMクラウド エッセンシャル機能 機器50台 ・初年度ライセンス	
	AX-NMクラウド エッセンシャル機能 機器50台 ・1年延長ライセンス	
	AX-NMクラウド スタンダード機能 基本(機器20台) ・初年度ライセンス	
	AX-NMクラウド スタンダード機能 基本(機器20台) ・1年延長ライセンス	
	AX-NMクラウド スタンダード機能 機器10台 ・初年度ライセンス	
	AX-NMクラウド スタンダード機能 機器10台 ・1年延長ライセンス	
	AX-NMクラウド スタンダード機能 機器20台 ・初年度ライセンス	
	AX-NMクラウド スタンダード機能 機器20台 ・1年延長ライセンス	
	AX-NMクラウド スタンダード機能 機器50台 ・初年度ライセンス	
	AX-NMクラウド スタンダード機能 機器50台 ・1年延長ライセンス	

分類	機能	備考
	AX-NMクラウド ワイヤレスLANコントローラ 機器1台 ・初年度1年ライセンス	
	AX-NMクラウド ワイヤレスLANコントローラ 機器1台 ・1年延長ライセンス	
	AX-NMクラウド 外部連携ライセンス:トレンドマイクロ DDI/PMとの連携 ・初年度1年ライセンス	
	AX-NMクラウド 外部連携ライセンス:トレンドマイクロ DDI/PMとの連携 ・1年延長ライセンス	
	AX-NMクラウド 外部連携ライセンス:パロアルトネットワークス 次世代ファイアウォールとの連携 ・初年度1年ライセンス	
	AX-NMクラウド 外部連携ライセンス:パロアルトネットワークス 次世代ファイアウォールとの連携 ・1年延長ライセンス	
	AX-NMクラウド 外部連携ライセンス:Syslog連携(CEF) ・初年度1年ライセンス	
	AX-NMクラウド 外部連携ライセンス:Syslog連携(CEF) ・1年延長ライセンス	
	監視対象拡張オプション 10台ライセンス ・初年度1年ライセンス	
	監視対象拡張オプション 10台ライセンス ・1年延長ライセンス	
	監視対象拡張オプション 20台ライセンス ・初年度1年ライセンス	
	監視対象拡張オプション 20台ライセンス ・1年延長ライセンス	
	監視対象拡張オプション 50台ライセンス ・初年度1年ライセンス	
	監視対象拡張オプション 50台ライセンス ・1年延長ライセンス	
	AX-NMクラウド監視対象拡張オプション 10台ライセンス ・初年度1年ライセンス	
	AX-NMクラウド監視対象拡張オプション 10台ライセンス ・1年延長ライセンス	
	AX-NMクラウド監視対象拡張オプション 20台ライセンス ・初年度1年ライセンス	
	AX-NMクラウド監視対象拡張オプション 20台ライセンス ・1年延長ライセンス	
	AX-NMクラウド監視対象拡張オプション 50台ライセンス ・初年度1年ライセンス	
	AX-NMクラウド監視対象拡張オプション 50台ライセンス ・1年延長ライセンス	

5. 動作環境

5.1 ハードウェア構成[オンプレミス版のみ]

AX-Network-Manager が動作可能なハードウェアの条件を下記に示します。

表 5-1 動作スペック

#	項目	要件
1	CPU	最新のマルチコアプロセッサ (8 コア以上を推奨)
2	メモリ	8GB 以上※1
3	ストレージの空き容量	300GB 以上※2
4	イーサネットインタフェース	1 ポート以上

※1 安定動作のためにスワップ領域の割当を強く推奨します。割当サイズについては https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux/7/html/storage_administration_guide/ch-swapspace を参考に設定ください。

※2 機器から取得するファイルサイズや，回線使用帯域の履歴の保存数，マップやアイコンの画像ファイルサイズ，端末接続履歴の保存数，監視対象履歴の保存量，採取情報履歴の保存量等で必要な空き容量は増減します。十分余裕を持った空き容量を確保してください。

5.2 ソフトウェア構成[オンプレミス版のみ]

(1) 動作可能オペレーティングシステム(OS)

AX-Network-Manager が動作可能なオペレーションシステムの条件を下記に示します。

表 5-2 動作可能オペレーティングシステム一覧

#	オペレーティングシステム名※	備考
1	CentOS 7	動作確認済み Ver. 7.6
2	Red Hat Enterprise Linux 7	動作確認済み Ver. 7.8
3	Red Hat Enterprise Linux 8	動作確認済み Ver. 8.4
4	MIRACLE LINUX 8	動作確認済み Ver. 8.4
5	Ubuntu 20.04 LTS	動作確認済み Ver. 20.04

※オペレーティングシステムは，64bit 版を利用ください。

(2) ウェブブラウザ

AX-Network-Manager で使用可能なウェブブラウザを下記に示します。

表 5-3 AX-Network-Manager 動作可能ウェブブラウザ

#	ウェブブラウザ名	備考
1	Google Chrome (最新版)	
2	Microsoft Edge(Chromium ベース) (最新版)	

(3) ドキュメント出力対応 Excel ビューア

ドキュメント出力に対応する Excel ビューアを下記に示します。

表 5-4 ドキュメント出力対応 Excel ビューア

#	ソフトウェア名	備考
1	Microsoft Excel 2016/2019	デスクトップアプリ版のみ 動作確認済み Microsoft Excel 2019

5.3 前提とするネットワーク構成

AX-Network-Manager が前提とするネットワーク構成を下記に示します。

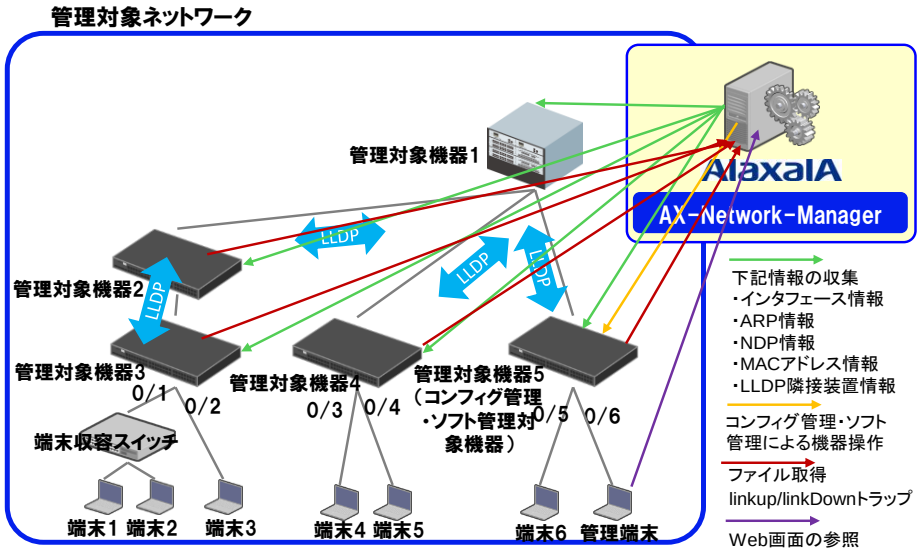

図 5-1 前提とするネットワーク構成例

5.3.1 管理対象機器

AX-Network-Manager の管理対象にできる機器を以下に示します。
管理対象機器は，以下の条件を満たす必要があります。

表 5-5 管理対象機器の条件

条件
AX-Network-Manager から，管理対象機器へ SNMP でアクセス可能であること。
コンフィグ管理，およびソフト管理対象機器へは AX-Network-Manager から SSH/Telnet でアクセス可能であること。
IP ネットワークで構築している場合，最低 1 台はレイヤ 3 スイッチであり，端末の ARP 情報および NDP 情報を学習できること（上図では管理対象機器 1）。
端末(もしくは端末収容スイッチ)を収容する管理対象機器はスイッチであり，端末の MAC アドレス情報を学習できること（上図では管理対象機器 3，管理対象機器 4，管理対象機器 5）。
隣接する管理対象機器とのイーサネットポートで，LLDP を有効にし，隣接情報を学習できること。 (上図では，管理対象機器 1 - 管理対象機器 2，管理対象機器 1 - 管理対象機器 4，管理対象機器 1 - 管理対象機器 5，管理対象機器 2 - 管理対象機器 3 間) ※：管理対象機器で LLDP が動作しない場合，隣接する管理対象機器間のポートの接続関係を，Web インタフェースにより静的に設定することで代替可能
管理対象機器から物理ポートの linkUp/linkDown トラップの送信をサポートしていること。 ※：管理対象機器からインタフェース情報を収集することで代替可能

5.3.2 標準 MIB 対応機器の条件

AX-Network-Manager がサポートする弊社製品の他に，使用用途に応じて下記の条件を満たすスイッチを管理対象機器として使用することが可能です。この条件を満たすスイッチを標準 MIB 対応機器と呼びます。

表 5-6　標準 MIB 対応機器の条件

使用用途	条件
機器情報収集 (必須)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記オブジェクトの取得をサポートしていること ・sysDescr ・sysName
インタフェース情報収集 (オプション)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記オブジェクトの取得をサポートしていること ・ifIndex ・ifDescr ・ifType ・ifMtu ・ifPhysAddress ・ifAdminStatus ・ifOperStatus ・ifInOctets※2 ・ifOutOctets※2 RFC2233(The Interfaces Group MIB using SMIv2)の下記オブジェクトの取得をサポートしていること ・ifName ・ifHCInOctets※2 ・ifHCOutOctets※2 ・ifHighSpeed ・ifAlias
ARP 情報収集 (オプション)	RFC4293(Management Information Base for the Internet Protocol (IP)) の下記オブジェクトの取得をサポートしていること ・ipNetToMediaPhysAddress
NDP 情報収集 (オプション)	RFC2465(Management Information Base for IP Version 6:Textual Conventions and General Group)の下記オブジェクトの取得をサポートしていること ・ipv6NetToMediaPhysAddress※1
ARP/NDP 情報収集 (オプション)	RFC4293(Management Information Base for the Internet Protocol (IP))の下記オブジェクトの取得をサポートしていること ・ipNetToPhysicalPhysAddress※1
MAC アドレス情報収集 (オプション)	RFC1493 または RFC4188(Definitions of Managed Objects for Bridges) の下記オブジェクトの取得をサポートしていること ・dot1dTpFdbPort
	RFC2674 または RFC4363(Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions) の下記オブジェクトの取得をサポートしていること ・dot1qTpFdbPort
LLDP 情報収集 (オプション)	下記いずれかのオブジェクトの取得をサポートしていること IEEE Std 802.1AB-2005 LLDP-MIB ・lldpRemChassisId ・lldpRemChassisIdSubype ・lldpRemPortDesc ・lldpLocPortDesc

使用用途	条件
	IEEE Std 802.1AB-2009 LLDP-V2-MIB ・lldpV2RemChassisId ・lldpV2RemChassisIdSubype ・lldpV2RemPortDesc
	弊社製品の axslldp ・axslldpRemRemoteChassis ・axslldpRemPortDesc
VLAN 情報収集(オプション)	RFC2674 または RFC4363(Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions) の下記オブジェクトの取得をサポートしていること ・dot1qVlanStaticEgressPorts ・dot1qVlanStaticUntaggedPorts
経路情報収集（オプション）	下記いずれかのオブジェクトの取得をサポートしていること RFC1354(IP Forwarding Table MIB) ・ipForwardMask
	RFC1354(IP Forwarding Table MIB) ・ipCidrRouteTable
	RFC1213(Management Information Base for Network Management of TCP/IP-based internets:MIB-II) ・ipRouteMask ・ipRouteNextHop
トラップの送信(オプション)	RFC2233(The Interfaces Group MIB using SMIv2)の物理ポートの linkUp/linkDown トラップの送信をサポートしていること。

※1：IPv6 リンクローカルアドレスは収集対象外です。
※2：ifInOctets と ifOutOctets の組み合わせ，または ifHCInOctets と ifHCOutOctets の組み合わせどちらかをサポートしている必要があります。

5.3.3 標準 MIB 対応機器(VLAN 毎コミュニティ)の条件

5.3.2 の標準 MIB 対応機器とは別に，下記の条件を満たす Cisco スイッチを管理対象機器として使用することが可能です。この条件を満たすスイッチを標準 MIB 対応機器(VLAN 毎コミュニティ)と呼びます。

表 5-7 標準 MIB 対応機器(VLAN 毎コミュニティ)の条件

使用用途	条件
機器情報収集(必須)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記オブジェクトの取得をサポートしていること ・sysDescr ・sysName

使用用途	条件
インタフェース情報収集 (オプション)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記オブジェクトの取得をサポートしていること ・ifIndex ・ifDescr ・ifType ・ifMtu ・ifPhysAddress ・ifAdminStatus ・ifOperStatus ・ifInOctets※2 ・ifOutOctets※2 RFC2233(The Interfaces Group MIB using SMIv2)の下記オブジェクトの取得をサポートしていること ・ifName ・ifHCInOctets※2 ・ifHCOutOctets※2 ・ifHighSpeed ・ifAlias
ARP 情報収集 (オプション)	RFC4293(Management Information Base for the Internet Protocol (IP)) の下記オブジェクトの取得をサポートしていること ・ipNetToMediaPhysAddress
NDP 情報収集 (オプション)	RFC2465(Management Information Base for IP Version 6:Textual Conventions and General Group)の下記オブジェクトの取得をサポートしていること ・ipv6NetToMediaPhysAddress※1
ARP/NDP 情報収集 (オプション)	RFC4293(Management Information Base for the Internet Protocol (IP))の下記オブジェクトの取得をサポートしていること ・ipNetToPhysicalPhysAddress※1
MAC アドレス情報収集 (オプション)	RFC1493 または RFC4188(Definitions of Managed Objects for Bridges) の下記オブジェクトの取得をサポートしていること ・dot1dTpFdbPort VLAN 毎の上記オブジェクトを取得する際, SNMP コミュニティ名称が，下記であること ・<SNMP コミュニティ名称>@<VLAN ID>
LLDP 情報収集 (オプション)	下記いずれかのオブジェクトの取得をサポートしていること IEEE Std 802.1AB-2005 LLDP-MIB ・lldpRemChassisId ・lldpRemChassisIdSubtype ・lldpRemPortDesc ・lldpLocPortDesc
	IEEE Std 802.1AB-2009 LLDP-V2-MIB ・lldpV2RemChassisId ・lldpV2RemChassisIdSubtype ・lldpV2RemPortDesc

使用用途	条件
VLAN 情報収集 (オプション)	CISCO-VTP-MIB の下記オブジェクトの取得をサポートしていること ・vtpVlanState ・vlanTrunkPortVlansEnabled ・vlanTrunkPortVlansEnabled2k ・vlanTrunkPortVlansEnabled3k ・vlanTrunkPortVlansEnabled4k ・vlanTrunkPortNativeVlan CISCO-VLAN-MEMBERSHIP-MIB の下記オブジェクトの取得をサポートしていること ・vmVlan
経路情報収集 （オプション）	下記いずれかのオブジェクトの取得をサポートしていること RFC1354(IP Forwarding Table MIB) ・ipForwardMask
	RFC1354(IP Forwarding Table MIB) ・ipCidrRouteTable
	RFC1213(Management Information Base for Network Management of TCP/IP-based internets:MIB-II) ・ipRouteMask ・ipRouteNextHop
トラップの送信 (オプション)	RFC2233(The Interfaces Group MIB using SMIv2)の物理ポートの linkUp/linkDown トラップの送信をサポートしていること。

※1：IPv6 リンクローカルアドレスは収集対象外です。
※2：ifInOctets と ifOutOctets の組み合わせ，または ifHCInOctets と ifHCOutOctets の組み合わせどちらかをサポートしている必要があります。

5.3.4 ワイヤレス LAN コントローラの条件

下記の条件を満たすスイッチを管理対象機器として使用することが可能です。この条件を満たすスイッチをワイヤレス LAN コントローラ(WLC)と呼びます。

表 5-8 ワイヤレス LAN コントローラ(Aruba-1)の条件

使用用途	条件
機器情報収集 (必須)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記オブジェクトの取得をサポートしていること ・sysDescr ・sysName
WLC 情報収集 (必須)	下記オブジェクトの取得をサポートしていること ・wlsxUserAllInfoGroup ・wlsxWlanAccessPointInfoGroup

使用用途	条件
インタフェース情報収集 (オプション)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記オブジェクトの取得をサポートしていること ・ifIndex ・ifDescr ・ifType ・ifMtu ・ifPhysAddress ・ifAdminStatus ・ifOperStatus ・ifInOctets※2 ・ifOutOctets※2 RFC2233(The Interfaces Group MIB using SMIv2)の下記オブジェクトの取得をサポートしていること ・ifName ・ifHCInOctets※2 ・ifHCOutOctets※2 ・ifHighSpeed ・ifAlias
ARP 情報収集 (オプション)	RFC4293(Management Information Base for the Internet Protocol (IP))の下記オブジェクトの取得をサポートしていること ・ipNetToMediaPhysAddress
NDP 情報収集 (オプション)	RFC2465(Management Information Base for IP Version 6:Textual Conventions and General Group)の下記オブジェクトの取得をサポートしていること ・ipv6NetToMediaPhysAddress※1
ARP/NDP 情報収集 (オプション)	RFC4293(Management Information Base for the Internet Protocol (IP))の下記オブジェクトの取得をサポートしていること ・ipNetToPhysicalPhysAddress※1
MAC アドレス情報収集 (オプション)	RFC1493 または RFC4188(Definitions of Managed Objects for Bridges)の下記オブジェクトの取得をサポートしていること ・dot1dTpFdbPort
	RFC2674 または RFC4363(Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions)の下記オブジェクトの取得をサポートしていること ・dot1qTpFdbPort
LLDP 情報収集 (オプション)	下記いずれかのオブジェクトの取得をサポートしていること IEEE Std 802.1AB-2005 LLDP-MIB ・lldpRemChassisId ・lldpRemChassisIdSubtype ・lldpRemPortDesc ・lldpLocPortDesc
	IEEE Std 802.1AB-2009 LLDP-V2-MIB ・lldpV2RemChassisId ・lldpV2RemChassisIdSubtype ・lldpV2RemPortDesc
	弊社製品の axslldp ・axslldpRemRemoteChassis ・axslldpRemPortDesc

使用用途	条件
VLAN 情報収集 (オプション)	RFC2674 または RFC4363(Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions)の下記オブジェクトの取得をサポートしていること ・dot1qVlanStaticEgressPorts ・dot1qVlanStaticUntaggedPorts
トラップの送信 (オプション)	RFC2233(The Interfaces Group MIB using SMIv2)の物理ポートの linkUp/linkDown トラップの送信をサポートしていること。

※1: IPv6 リンクローカルアドレスは収集対象外です。
※2: ifInOctets と ifOutOctets の組み合わせ, または ifHCInOctets と ifHCOutOctets の組み合わせどちらかをサポートしている必要があります。

表 5-9　ワイヤレス LAN コントローラ(Cisco-1)の条件

使用用途	条件
機器情報収集 (必須)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記オブジェクトの取得をサポートしていること ・sysDescr ・sysName
WLC 情報収集 (必須)	下記オブジェクトの取得をサポートしていること ・bsnEss ・bsnAP
インタフェース情報収集 (オプション)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記オブジェクトの取得をサポートしていること ・ifIndex ・ifDescr ・ifType ・ifMtu ・ifPhysAddress ・ifAdminStatus ・ifOperStatus ・ifInOctets※2 ・ifOutOctets※2 RFC2233(The Interfaces Group MIB using SMIv2)の下記オブジェクトの取得をサポートしていること ・ifName ・ifHCInOctets※2 ・ifHCOutOctets※2 ・ifHighSpeed ・ifAlias
ARP 情報収集 (オプション)	RFC4293(Management Information Base for the Internet Protocol (IP))の下記オブジェクトの取得をサポートしていること ・ipNetToMediaPhysAddress
NDP 情報収集 (オプション)	RFC2465(Management Information Base for IP Version 6:Textual Conventions and General Group)の下記オブジェクトの取得をサポートしていること ・ipv6NetToMediaPhysAddress※1
ARP/NDP 情報収集 (オプション)	RFC4293(Management Information Base for the Internet Protocol (IP))の下記オブジェクトの取得をサポートしていること ・ipNetToPhysicalPhysAddress※1

使用用途	条件
MAC アドレス情報収集 (オプション)	RFC1493 または RFC4188(Definitions of Managed Objects for Bridges)の下記オブジェクトの取得をサポートしていること ・dot1dTpFdbPort
	RFC2674 または RFC4363(Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions)の下記オブジェクトの取得をサポートしていること ・dot1qTpFdbPort
LLDP 情報収集 (オプション)	下記いずれかのオブジェクトの取得をサポートしていること IEEE Std 802.1AB-2005 LLDP-MIB ・lldpRemChassisId ・lldpRemChassisIdSubtype ・lldpRemPortDesc ・lldpLocPortDesc
	IEEE Std 802.1AB-2009 LLDP-V2-MIB ・lldpV2RemChassisId ・lldpV2RemChassisIdSubtype ・lldpV2RemPortDesc
	弊社製品の axslldp ・axslldpRemRemoteChassis ・axslldpRemPortDesc
VLAN 情報収集 (オプション)	RFC2674 または RFC4363(Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions)の下記オブジェクトの取得をサポートしていること ・dot1qVlanStaticEgressPorts ・dot1qVlanStaticUntaggedPorts
トラップの送信 (オプション)	RFC2233(The Interfaces Group MIB using SMIv2)の物理ポートの linkUp/linkDown トラップの送信をサポートしていること。

※1: IPv6 リンクローカルアドレスは収集対象外です。
※2: ifInOctets と ifOutOctets の組み合わせ, または ifHCInOctets と ifHCOutOctets の組み合わせどちらかをサポートしている必要があります。

表 5-10　ワイヤレス LAN コントローラ(Fortinet-1)の条件

使用用途	条件
機器情報収集 (必須)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記オブジェクトの取得をサポートしていること ・sysDescr ・sysName
WLC 情報収集 (必須)	下記オブジェクトの取得をサポートしていること ・mwConfigAp ・mwConfigStation

使用用途	条件
インタフェース情報収集 (オプション)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記オブジェクトの取得をサポートしていること ・ifIndex ・ifDescr ・ifType ・ifMtu ・ifPhysAddress ・ifAdminStatus ・ifOperStatus ・ifInOctets※2 ・ifOutOctets※2 RFC2233(The Interfaces Group MIB using SMIv2)の下記オブジェクトの取得をサポートしていること ・ifName ・ifHCInOctets※2 ・ifHCOutOctets※2 ・ifHighSpeed ・ifAlias
ARP 情報収集 (オプション)	RFC4293(Management Information Base for the Internet Protocol (IP))の下記オブジェクトの取得をサポートしていること ・ipNetToMediaPhysAddress
NDP 情報収集 (オプション)	RFC2465(Management Information Base for IP Version 6:Textual Conventions and General Group)の下記オブジェクトの取得をサポートしていること ・ipv6NetToMediaPhysAddress※1
ARP/NDP 情報収集 (オプション)	RFC4293(Management Information Base for the Internet Protocol (IP))の下記オブジェクトの取得をサポートしていること ・ipNetToPhysicalPhysAddress※1
MAC アドレス情報収集 (オプション)	RFC1493 または RFC4188(Definitions of Managed Objects for Bridges)の下記オブジェクトの取得をサポートしていること ・dot1dTpFdbPort
	RFC2674 または RFC4363(Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions)の下記オブジェクトの取得をサポートしていること ・dot1qTpFdbPort
LLDP 情報収集 (オプション)	下記いずれかのオブジェクトの取得をサポートしていること IEEE Std 802.1AB-2005 LLDP-MIB ・lldpRemChassisId ・lldpRemChassisIdSubtype ・lldpRemPortDesc ・lldpLocPortDesc
	IEEE Std 802.1AB-2009 LLDP-V2-MIB ・lldpV2RemChassisId ・lldpV2RemChassisIdSubtype ・lldpV2RemPortDesc
	弊社製品の axslldp ・axslldpRemRemoteChassis ・axslldpRemPortDesc

使用用途	条件
VLAN 情報収集 (オプション)	RFC2674 または RFC4363(Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions)の下記オブジェクトの取得をサポートしていること ・dot1qVlanStaticEgressPorts ・dot1qVlanStaticUntaggedPorts
トラップの送信 (オプション)	RFC2233(The Interfaces Group MIB using SMIv2)の物理ポートの linkUp/linkDown トラップの送信をサポートしていること。

※1: IPv6 リンクローカルアドレスは収集対象外です。
※2: ifInOctets と ifOutOctets の組み合わせ，または ifHCInOctets と ifHCOutOctets の組み合わせどちらかをサポートしている必要があります。

5.3.5 機能別対応機器

AX-Network-Manager の管理対象にできる機器のうち，各機能に対応した機器を示します。

(1) フロントパネル表示対応機器

フロントパネル表示に対応する機器を次に示します。

表 5-11 フロントパネル表示対応機器

対応機器		対応機器モデルおよびパッケージ	
AX8600S・AX8300S シリーズ	AX8600S	AX8608S AX8616S AX8632S BCU-1S BCU-2S PSU-11 PSU-12 PSU-21 PSU-22 PSU-23	NL1G-12T NL1G-12S NL1GA-12S NLXG-6RS NLXGA-12RS NLXLG-4Q NLCG-1Q NMCG-1C PS-A21 PS-D21
	AX8300S	AX8304S AX8308S BCU-ES BCU-FS PSU-C1 PSU-C2 PSU-E1A PSU-E2A PSU-E1 PSU-E2	NL1G-12T NL1G-12S NL1GA-12S NL1G-24T NL1G-24S NLXG-6RS NLXGA-12RS NLXLG-4Q NLCG-1Q PS-A42 PS-D42
AX4600S シリーズ	AX4630S	AX4630S-4M NA1G-24T NA1G-24S NAXG-24RS NAXLG-6Q	
AX3800S シリーズ	AX3830S	AX3830S-32X4QW AX3830S-44XW AX3830S-44X4QW AX3830S-44X4QS	

対応機器		対応機器モデルおよびパッケージ
AX3600S シリーズ	AX3660S	AX3660S-24T4X AX3660S-24T4XW AX3660S-16S4XW AX3660S-24S8XW AX3660S-48T4XW AX3660S-48XT4QW AX3660S-24X4QW AX3660S-48X4QW
	AX3650S※	AX3650S-24T6XW AX3650S-20S6XW AX3650S-48T4XW
AX2600S シリーズ	AX2630S	AX2630S-24T4XW AX2630S-24P4XW AX2630S-48T4XW AX2630S-48P4XW
AX2500S シリーズ	AX2530SE	AX2530SE-24T AX2530SE-24T4X AX2530SE-24S4X AX2530SE-48T AX2530SE-48T2X
	AX2530S	AX2530S-24T AX2530S-24TD AX2530S-24T4X AX2530S-24S4X AX2530S-24S4XD AX2530S-48T AX2530S-48TD AX2530S-48T2X AX2530S-48P2X AX2530S-08P AX2530S-08PD1 AX2530S-08PD2 AX2530S-08TC1 AX2530S-16P4X
AX2300S シリーズ	AX2340S	AX2340S-24T4X AX2340S-24P4X AX2340S-48T4X AX2340S-48P4X AX2340S-16P8MP2X
AX2200S シリーズ	AX2230S	AX2230S-24T AX2230S-24P
AX2100S シリーズ	AX2130S	AX2130S-16T AX2130S-16P AX2130S-24T AX2130S-24TH AX2130S-24P AX2130S-24PH
AXprimoM210 シリーズ	AXprimoM210	AXprimoM210-08T AXprimoM210-08P
AX260A シリーズ	AX260A	AX260A-08T AX260A-08TF

対応機器		対応機器モデルおよびパッケージ
AX620R シリーズ	AX620R	AX620R-2105 AX620R-2106 AX620R-2025 AX620R-2215 AX620R-3110 AX620R-3315

注※: AX3650S は Ver.11.10 以降でサポートしています。

(2) L2 ループ検知対応機器

L2 ループ検知に対応する機器を次に示します。

表 5-12 L2 ループ検知対応機器

対応機器	
AX8600S・AX8300S シリーズ	AX8600S
	AX8300S
AX4600S シリーズ	AX4630S
AX3800S シリーズ	AX3830S
AX3600S シリーズ	AX3660S
	AX3650S
	AX3640S
AX2600S シリーズ	AX2630S
AX2500S シリーズ	AX2530SE
	AX2530S
AX2300S シリーズ	AX2340S
AX2200S シリーズ	AX2230S
AX2100S シリーズ	AX2130S
AX1200S シリーズ	AX1250S
	AX1240S
AX260A シリーズ	AX260A

(3) ストーム検知対応機器

ストーム検知に対応する機器を次に示します。

表 5-13 ストーム検知対応機器

対応機器	
AX8600S・AX8300S シリーズ	AX8600S
	AX8300S
AX4600S シリーズ	AX4630S
AX3800S シリーズ	AX3830S
AX3600S シリーズ	AX3660S
	AX3650S
	AX3640S
AX2600S シリーズ	AX2630S
AX2500S シリーズ	AX2530SE
	AX2530S
AX2300S シリーズ	AX2340S
AX2200S シリーズ	AX2230S
AX2100S シリーズ	AX2130S
AX1200S シリーズ	AX1250S
	AX1240S
AX260A シリーズ	AX260A

(4) 輻輳管理対応機器

輻輳管理に対応する機器を次に示します。

表 5-14 輻輳管理対応機器

対応機器	
AX4600S シリーズ	AX4630S
AX3800S シリーズ	AX3830S
AX3600S シリーズ	AX3660S
	AX3650S
	AX3640S
AX2600S シリーズ	AX2630S
AX2500S シリーズ	AX2530SE
	AX2530S
AX2300S シリーズ	AX2340S
AX260A シリーズ	AX260A

(5) スタック切替監視対応機器

スタック切替監視に対応する機器を次に示します。

表 5-15 スタック切替監視対応機器

対応機器	
AX2500S シリーズ	AX2530SE
	AX2530S
AX260A シリーズ	AX260A

(6) Web ターミナル

プロトコルに SSH を使用時, コマンド入力モードを自動的に装置管理者モードへの変更に対応する機器を次に示します。

表 5-16 Web ターミナル(装置管理者モードへの変更)対応機器

対応機器	
AX8600S・AX8300S シリーズ	AX8600S
	AX8300S
AX4600S シリーズ	AX4630S
AX3800S シリーズ	AX3830S
AX3600S シリーズ	AX3660S
	AX3650S
	AX3640S
AX2600S シリーズ	AX2630S
AX2500S シリーズ	AX2530SE
	AX2530S
AX2300S シリーズ	AX2340S
AX2200S シリーズ	AX2230S
AX2100S シリーズ	AX2130S
AX1200S シリーズ	AX1250S
	AX1240S
AX260A シリーズ	AX260A

(7) 経路管理対応機器

経路管理に対応する機器を次に示します。

表 5-17　経路管理対応機器

対応機器	
AX8600S・AX8300S シリーズ	AX8600S
	AX8300S
AX4600S シリーズ	AX4630S
AX3800S シリーズ	AX3830S
AX3600S シリーズ	AX3660S
	AX3650S
	AX3640S
AX620R シリーズ	AX620R-3315 AX620R-3110 AX620R-2215 AX620R-2106 AX620R-2105 AX620R-2025
標準 MIB 対応機器※1	AX6700S，AX6600S，AX6300S， 弊社製品の他，他社製品にも対応
標準 MIB 対応機器 (VLAN 毎コミュニティ)※1	Cisco スイッチ

注※1:

5.3.2 標準 MIB 対応機器の条件, および 5.3.3 標準 MIB 対応機器(VLAN 毎コミュニティ)の条件の経路情報収集条件を満たすスイッチに対応します。

(8) コンフィグ管理・テンプレート管理対応機器

コンフィグ管理およびテンプレート管理に対応する機器を次に示します。

表 5-18　コンフィグ管理・テンプレート管理対応機器

対応機器	
AX8600S・AX8300S シリーズ	AX8600S
	AX8300S
AX4600S シリーズ	AX4630S
AX3800S シリーズ	AX3830S
AX3600S シリーズ	AX3660S
	AX3650S
	AX3640S
AX2600S シリーズ	AX2630S
AX2500S シリーズ	AX2530SE
	AX2530S
AX2300S シリーズ	AX2340S
AX2200S シリーズ	AX2230S
AX2100S シリーズ	AX2130S
AXprimoM210 シリーズ	AXprimoM210
AX1200S シリーズ	AX1250S
	AX1240S
AX260A シリーズ	AX260A
AX620R シリーズ	AX620R-3315
	AX620R-3110
	AX620R-2215

対応機器	
	AX620R-2106
	AX620R-2105
	AX620R-2025
標準 MIB 対応機器※1	AX6700S，AX6600S，AX6300S，弊社製品の他，他社製品にも対応
標準 MIB 対応機器(VLAN 毎コミュニティ)※1	Cisco スイッチ
ワイヤレス LAN コントローラ※1	5.3.4　ワイヤレス LAN コントローラの条件を満たすスイッチ

注※1:
スクリプト設定を行うことにより対応します。

(9) ソフトウェア管理対応機器

ソフトウェア管理に対応する機器を次に示します。

表 5-19　ソフトウェア管理対応機器

対応機器		対応 ソフトウェアバージョン
AX8600S・AX8300S シリーズ	AX8600S	Ver. 12.7.B 以降
	AX8300S	Ver. 12.7.B 以降
AX4600S シリーズ	AX4630S	指定なし
AX3800S シリーズ	AX3830S	Ver. 11.14.L 以降
AX3600S シリーズ	AX3660S	指定なし
	AX3650S	Ver. 11.14.L 以降
	AX3640S	指定なし
AX2600S シリーズ	AX2630S	指定なし
AX2500S シリーズ	AX2530SE	指定なし
	AX2530S	指定なし
AX2300S シリーズ	AX2340S	指定なし
AX2200S シリーズ	AX2230S	指定なし
AX2100S シリーズ	AX2130S	指定なし
AXprimoM210 シリーズ	AXprimoM210	指定なし
AX1200S シリーズ	AX1250S	指定なし
	AX1240S	指定なし
AX260A シリーズ	AX260A	指定なし
AX620R シリーズ	AX620R-3315	指定なし
	AX620R-3110	Ver.9.5.13 以降
	AX620R-2215	Ver.9.5.13 以降
	AX620R-2106	指定なし
	AX620R-2105	Ver.9.5.13A 以降
	AX620R-2025	Ver.9.5.13 以降

(10) バックアップ管理対応機器

バックアップ管理に対応する機器と，ゼロタッチプロビジョニングによる機器交換に対応するソフトウェアバージョンを次に示します。

表 5-20　バックアップ管理対応機器

対応機器		ゼロタッチプロビジョニング対応ソフトウェアバージョン
AX2600S シリーズ	AX2630S	指定なし
AX2500S シリーズ	AX2530SE	Ver.4.15～
	AX2530S	
AX2300S シリーズ	AX2340S	指定なし
AX2100S シリーズ	AX2130S	Ver.2.11～
AXprimoM210 シリーズ	AXprimoM210	Ver.1.2.3.3～
AX260A シリーズ	AX260A	Ver.4.15～

(11) シリアル情報管理対応機器

シリアル情報管理に対応する機器を次に示します。

表 5-21　シリアル管理対応機器

対応機器	
AX8600S・AX8300S シリーズ	AX8600S
	AX8300S
AX4600S シリーズ	AX4630S
AX3800S シリーズ	AX3830S
AX3600S シリーズ	AX3660S
	AX3650S
	AX3640S
AX2600S シリーズ	AX2630S
AX2500S シリーズ	AX2530SE
	AX2530S
AX2300S シリーズ	AX2340S
AX2200S シリーズ	AX2230S
AX2100S シリーズ	AX2130S
AXprimoM210 シリーズ	AXprimoM210
AX1200S シリーズ	AX1250S
	AX1240S
AX260A シリーズ	AX260A
AX620R シリーズ	AX620R-3315
	AX620R-3110
	AX620R-2215
	AX620R-2106
	AX620R-2105
	AX620R-2025
標準 MIB 対応機器※1	AX6700S AX6600S AX6300S 弊社製品の他， 他社製品にも対応
標準 MIB 対応機器 (VLAN 毎コミュニティ) ※1	Cisco スイッチ

対応機器	
ワイヤレス LAN コントローラ※1	5.3.4　ワイヤレス LAN コントローラの条件を満たすスイッチ

注※1:
スクリプト設定を行うことにより対応します。

(12) Web 管理情報配布対応機器

Web 管理情報配布に対応する機器を次に示します。

表 5-22　Web 管理情報配布対応機器

対応機器	
AX4600S シリーズ	AX4630S
AX3800S シリーズ	AX3830S
AX3600S シリーズ	AX3660S
	AX3650S
	AX3640S
AX2600S シリーズ	AX2630S
AX2500S シリーズ	AX2530SE
	AX2530S
AX2200S シリーズ	AX2230S
AX2100S シリーズ	AX2130S
AX1200S シリーズ	AX1250S
	AX1240S
AX260A シリーズ	AX260A

(13) フィルタ管理対応機器

フィルタ管理に対応する機器を次に示します。

表 5-23　フィルタ管理対応機器

対応機器		フィルタ情報カウンタ収集サポート有無
AX8600S・AX8300S シリーズ	AX8600S	○
	AX8300S	○
AX4600S シリーズ	AX4630S	○※1
AX3800S シリーズ	AX3830S	○※1
AX3600S シリーズ	AX3660S	○※1
	AX3650S	○※1
	AX3640S	○
AX2600S シリーズ	AX2630S	○
AX2500S シリーズ	AX2530SE	－
	AX2530S	－
AX2300S シリーズ	AX2340S	○
AX2200S シリーズ	AX2230S	－
AX2100S シリーズ	AX2130S	－
AX1200S シリーズ	AX1250S	－
	AX1240S	－
AX260A シリーズ	AX260A	－

注※1:スタック構成時にはフィルタ情報カウンタ収集に対応しません。

(14) QoS 管理対応機器

QoS 管理に対応する機器を次に示します。

表 5-24　QoS 管理対応機器

対応機器		QoS 情報カウンタ収集サポート有無
AX8600S・AX8300S シリーズ	AX8600S	○
	AX8300S	○
AX4600S シリーズ	AX4630S	○※1
AX3800S シリーズ	AX3830S	○※1
AX3600S シリーズ	AX3660S	○※1
	AX3650S	○※1
	AX3640S	○
AX2600S シリーズ	AX2630S	○
AX2500S シリーズ	AX2530SE	－
	AX2530S	－
AX2300S シリーズ	AX2340S	○
AX2200S シリーズ	AX2230S	－
AX2100S シリーズ	AX2130S	－
AX1200S シリーズ	AX1250S	－
	AX1240S	－
AX260A シリーズ	AX260A	－

注※1:スタック構成時には QoS 情報カウンタ収集に対応しません。

(15) ポートミラーリング管理対応機器

ポートミラーリング管理に対応する機器を次に示します。

表 5-25　ポートミラーリング管理対応機器

対応機器	
AX8600S・AX8300S シリーズ	AX8600S
	AX8300S
AX4600S シリーズ	AX4630S
AX3800S シリーズ	AX3830S
AX3600S シリーズ	AX3660S
	AX3650S
	AX3640S
AX2600S シリーズ	AX2630S
AX2500S シリーズ	AX2530SE
	AX2530S
AX2300S シリーズ	AX2340S
AX2200S シリーズ	AX2230S
AX2100S シリーズ	AX2130S
AX1200S シリーズ	AX1250S
	AX1240S
AX260A シリーズ	AX260A

5.3.6 ゼロタッチプロビジョニング機能利用のためのネットワーク要件

ゼロタッチプロビジョニング機能を利用するためのネットワーク要件を示します。要件には，交換機器を購入時の初期状態のまま使用できる場合(1)と，事前にコンフィグレーションが必要な場合(2)の 2 通りがあります。

なおいずれの場合でも，スタック構成，SML など，ゼロタッチプロビジョニング機能とは同時に使用できない機能があります。詳細は機器のマニュアルをご確認ください。

(1) 購入時の初期状態のままの交換機器を使用できるネットワーク要件

以下の要件を満たすようにネットワーク設計されていれば，購入時初期状態のままの交換機器ですぐに機器交換ができます。

1. 交換対象機器の AX-Network-Manager 向けの回線について

対象機器のデフォルトコンフィグレーションで AX-Network-Manager と通信ができること

リンクアグリゲーションなどのデフォルトコンフィグレーションでは無効となっている機能を使用せず，タグ無しのデフォルト VLAN(interface vlan 1)で AX-Network-Manager と通信できることが必要です。

端末等が DHCP を使用する場合，ネットワークが分離されていること

交換対象機器の配下で端末等が DHCP を使用する場合，VLAN などでネットワーク分離するなどして，端末からの DHCP パケットが AX-Network-Manager へ届かないようにしてください。AX-Network-Manager では端末からの DHCP パケットは処理できません。

2. 交換対象機器の AX-Network-Manager 向けの L3 スイッチ/ルータで DHCP リレーを有効にする

交換対象機器が AX-Network-Manager と同じネットワーク上にない場合，交換対象機器の AX-Network-Manager 向けの L3 スイッチ/ルータで DHCP リレーを設定し，AX-Network-Manager へ DHCP パケットを転送してください。

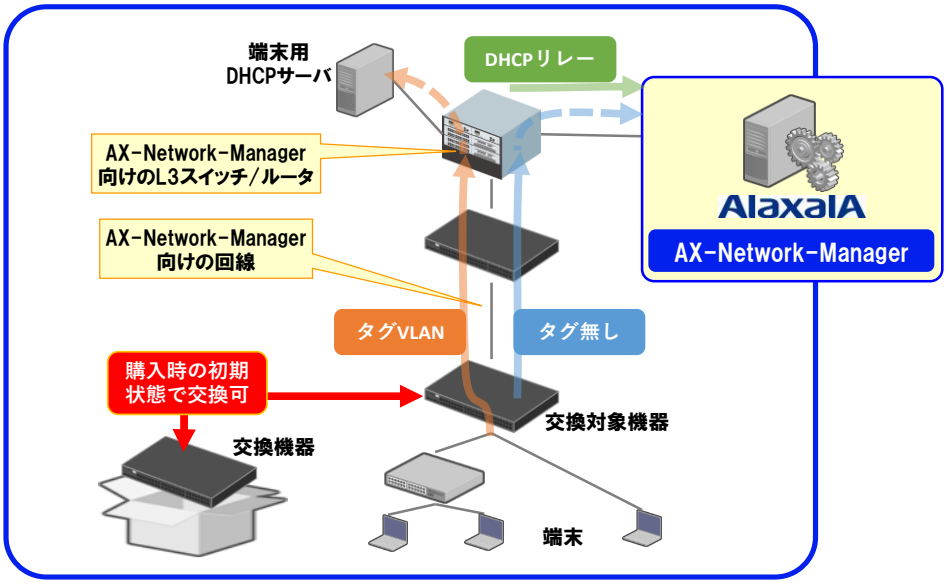

図 5-2 購入時の初期状態のままの交換機器を使用できるネットワーク例

(2) 事前に交換機器にコンフィグレーションが必要なネットワーク要件

先の要件を満たせない場合でも，事前に交換機器に最小限のコンフィグレーションを入れて予備機としておくことで，予備機からゼロタッチプロビジョニング機能を利用して機器交換ができます。

複数の交換対象機器がある場合，AX-Network-Manager 向けの回線をなるべく共通となるような構成にすることで，コンフィグレーションのパターンを削減し予備機の数を減らすことができます。以下にネットワーク要件を示します。

1. 交換対象機器の AX-Network-Manager 向けの回線について

交換機器に AX-Network-Manager と通信可能なコンフィグレーションを設定

リンクアグリゲーションやタグ付きの VLAN などを使用している場合でも，AX-Network-Manager と通信できる設定とゼロタッチプロビジョニングを有効とする設定を交換機器に事前に入れ，予備機としておきます。

端末等が DHCP を使用する場合，ネットワークが分離されていること

交換対象機器の配下で端末等が DHCP を使用する場合，VLAN などでネットワーク分離するなどして，端末からの DHCP パケットが AX-Network-Manager へ届かないようにしてください。AX-Network-Manager では端末からの DHCP パケットは処理できません。

2. 交換対象機器の AX-Network-Manager 向けの L3 スイッチ/ルータで DHCP リレーを有効にする

交換対象機器が AX-Network-Manager と同じネットワークにない場合，交換対象機器の AX-Network-Manager 向けの L3 スイッチ/ルータで DHCP リレーを設定し，AX-Network-Manager へ DHCP パケットを転送してください。

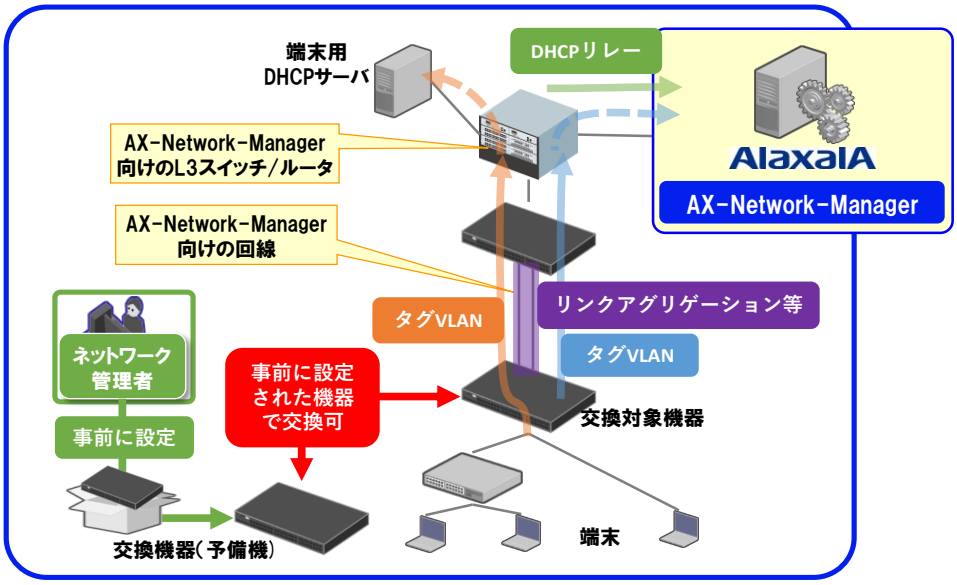

図 5-3 事前に交換機器にコンフィグレーションが必要なネットワーク例

6. 発注情報

項番	形名	略称	概略仕様
ソフトウェア製品			
1	AX-P1710-01	AX-NME10	エッセンシャル機能機器 10 台ライセンス ・初年度ライセンス
2	AX-P1710-01E1	AX-NME10	エッセンシャル機能機器 10 台ライセンス ・1 年延長ライセンス
3	AX-P1710-02	AX-NME20	エッセンシャル機能機器 20 台ライセンス ・初年度ライセンス
4	AX-P1710-02E1	AX-NME20	エッセンシャル機能機器 20 台ライセンス ・1 年延長ライセンス
5	AX-P1710-03	AX-NME50	エッセンシャル機能機器 50 台ライセンス ・初年度ライセンス
6	AX-P1710-03E1	AX-NME50	エッセンシャル機能機器 50 台ライセンス ・1 年延長ライセンス
7	AX-P1720-01	AX-NMS10	スタンダード機能機器 10 台ライセンス ・初年度ライセンス
8	AX-P1720-01E1	AX-NMS10	スタンダード機能機器 10 台ライセンス ・1 年延長ライセンス
9	AX-P1720-02	AX-NMS20	スタンダード機能機器 20 台ライセンス ・初年度ライセンス
10	AX-P1720-02E1	AX-NMS20	スタンダード機能機器 20 台ライセンス ・1 年延長ライセンス
11	AX-P1720-03	AX-NMS50	スタンダード機能機器 50 台ライセンス ・初年度ライセンス
12	AX-P1720-03E1	AX-NMS50	スタンダード機能機器 50 台ライセンス ・1 年延長ライセンス
13	AX-P1740-01	AX-NMW01	ワイヤレス LAN コントローラ 1 台まで ・初年度 1 年ライセンス
14	AX-P1740-01E1	AX-NMW01	ワイヤレス LAN コントローラ 1 台まで ・1 年延長ライセンス
15	AX-P1750-F1	OP-TM	外部連携ライセンス:トレンドマイクロ DDI/PM との連携 ・初年度 1 年ライセンス
16	AX-P1750-F1E1	OP-TM	外部連携ライセンス:トレンドマイクロ DDI/PM との連携 ・1 年延長ライセンス
17	AX-P1750-F2	OP-PA	外部連携ライセンス:パロアルトネットワークス 次世代ファイアウォールとの連携 ・初年度 1 年ライセンス
18	AX-P1750-F2E1	OP-PA	外部連携ライセンス:パロアルトネットワークス 次世代ファイアウォールとの連携 ・1 年延長ライセンス
19	AX-P1750-F3	OP-CEF	外部連携ライセンス:Syslog 連携(CEF) ・初年度 1 年ライセンス
20	AX-P1750-F3E1	OP-CEF	外部連携ライセンス:Syslog 連携(CEF) ・1 年延長ライセンス
21	AX-P1711-00	AX-NMECB	AX-NM クラウドエッセンシャル機能基本(20 台)ライセンス ・初年度ライセンス
22	AX-P1711-00E1	AX-NMECB	AX-NM クラウドエッセンシャル機能基本(20 台)ライセンス ・1 年延長ライセンス
23	AX-P1711-01	AX-NMEC1	AX-NM クラウドエッセンシャル機能機器 10 台ライセンス ・初年度ライセンス
24	AX-P1711-01E1	AX-NMEC1	AX-NM クラウドエッセンシャル機能機器 10 台ライセンス ・1 年延長ライセンス
25	AX-P1711-02	AX-NMEC2	AX-NM クラウドエッセンシャル機能機器 20 台ライセンス ・初年度ライセンス
26	AX-P1711-02E1	AX-NMEC2	AX-NM クラウドエッセンシャル機能機器 20 台ライセンス ・1 年延長ライセンス
27	AX-P1711-03	AX-NMEC5	AX-NM クラウドエッセンシャル機能機器 50 台ライセンス ・初年度ライセンス
28	AX-P1711-03E1	AX-NMEC5	AX-NM クラウドエッセンシャル機能機器 50 台ライセンス ・1 年延長ライセンス

項番	形名	略称	概略仕様
29	AX-P1721-00	AX-NMSCB	AX-NM クラウドスタンダード機能基本(20 台)ライセンス ・初年度ライセンス
30	AX-P1721-00E1	AX-NMSCB	AX-NM クラウドスタンダード機能基本(20 台)ライセンス ・1 年延長ライセンス
31	AX-P1721-01	AX-NMSC1	AX-NM クラウドスタンダード機能機器 10 台ライセンス ・初年度ライセンス
32	AX-P1721-01E1	AX-NMSC1	AX-NM クラウドスタンダード機能機器 10 台ライセンス ・1 年延長ライセンス
33	AX-P1721-02	AX-NMSC2	AX-NM クラウドスタンダード機能機器 20 台ライセンス ・初年度ライセンス
34	AX-P1721-02E1	AX-NMSC2	AX-NM クラウドスタンダード機能機器 20 台ライセンス ・1 年延長ライセンス
35	AX-P1721-03	AX-NMSC5	AX-NM クラウドスタンダード機能機器 50 台ライセンス ・初年度ライセンス
36	AX-P1721-03E1	AX-NMSC5	AX-NM クラウドスタンダード機能機器 50 台ライセンス ・1 年延長ライセンス
37	AX-P1741-01	AX-NMWC1	AX-NM クラウドワイヤレス LAN コントローラ 1 台まで ・初年度 1 年ライセンス
38	AX-P1741-01E1	AX-NMWC1	AX-NM クラウドワイヤレス LAN コントローラ 1 台まで ・1 年延長ライセンス
39	AX-P1751-F1	OP-C-TM	AX-NM クラウド外部連携ライセンス:トレンドマイクロ DDI/PM との連携 ・初年度 1 年ライセンス
40	AX-P1751-F1E1	OP-C-TM	AX-NM クラウド外部連携ライセンス:トレンドマイクロ DDI/PM との連携 ・1 年延長ライセンス
41	AX-P1751-F2	OP-C-PA	AX-NM クラウド外部連携ライセンス:パロアルトネットワークス 次世代ファイアウォールとの連携 ・初年度 1 年ライセンス
42	AX-P1751-F2E1	OP-C-PA	AX-NM クラウド外部連携ライセンス:パロアルトネットワークス 次世代ファイアウォールとの連携 ・1 年延長ライセンス
43	AX-P1751-F3	OP-C-CEF	AX-NM クラウド外部連携ライセンス:Syslog 連携(CEF) ・初年度 1 年ライセンス
44	AX-P1751-F3E1	OP-C-CEF	AX-NM クラウド外部連携ライセンス:Syslog 連携(CEF) ・1 年延長ライセンス
45	AX-P1750-F4	OP-MO1	監視対象拡張オプション 10 台ライセンス ・初年度 1 年ライセンス
46	AX-P1750-F4E1	OP-MO1	監視対象拡張オプション 10 台ライセンス ・1 年延長ライセンス
47	AX-P1750-F5	OP-MO2	監視対象拡張オプション 20 台ライセンス ・初年度 1 年ライセンス
48	AX-P1750-F5E1	OP-MO2	監視対象拡張オプション 20 台ライセンス ・1 年延長ライセンス
49	AX-P1750-F6	OP-MO3	監視対象拡張オプション 50 台ライセンス ・初年度 1 年ライセンス
50	AX-P1750-F6E1	OP-MO3	監視対象拡張オプション 50 台ライセンス ・1 年延長ライセンス
51	AX-P1751-F4	OP-C-MO1	AX-NM クラウド監視対象拡張オプション 10 台ライセンス ・初年度 1 年ライセンス
52	AX-P1751-F4E1	OP-C-MO1	AX-NM クラウド監視対象拡張オプション 10 台ライセンス ・1 年延長ライセンス
53	AX-P1751-F5	OP-C-MO2	AX-NM クラウド監視対象拡張オプション 20 台ライセンス ・初年度 1 年ライセンス
54	AX-P1751-F5E1	OP-C-MO2	AX-NM クラウド監視対象拡張オプション 20 台ライセンス ・1 年延長ライセンス
55	AX-P1751-F6	OP-C-MO3	AX-NM クラウド監視対象拡張オプション 50 台ライセンス ・初年度 1 年ライセンス
56	AX-P1751-F6E1	OP-C-MO3	AX-NM クラウド監視対象拡張オプション 50 台ライセンス ・1 年延長ライセンス

【発行】
2019 年　10 月　（Ver.1.0　第 1 版）
2020 年　 2 月　（Ver.1.1　第 2 版）
2020 年　 6 月　（Ver.1.2　第 3 版）
2020 年　 9 月　（Ver.1.3　第 4 版）
2020 年　10 月　（Ver.1.3　第 5 版）
2021 年　 1 月　（Ver.1.4　第 6 版）
2021 年　 4 月　（Ver.1.5　第 7 版）
2021 年　 5 月　（Ver.1.5.A　第 8 版）
2021 年　10 月　（Ver.1.6　第 9 版）
2022 年　 4 月　（Ver.1.7　第 10 版）

AlaxalA

アラクサラネットワークス株式会社
URL：https://www.alaxala.com/
〒212-0058
神奈川県川崎市幸区鹿島田 1 丁目 1 番 2 号
新川崎三井ビル西棟
お問合せ用 URL：
https://www.alaxala.com/jp/contact/

お問い合わせ先