データシート

AX-Security-Controller

1. 概要

1.1 位置づけ

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-Security-Controller 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。

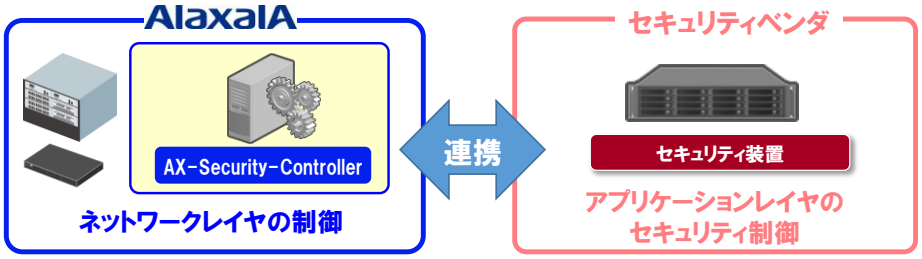

図 1-1 AX-Security-Controller-セキュリティ装置連携

AX-Security-Controller はセキュリティ装置と連携することにより,以下の機能を提供しています。

- 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

C&C(Command and Control)サーバ:
侵入したマルウェアと接続し,攻撃者からのコマンド等のやり取りを行うためのサーバ

AX-Security-Controller とセキュリティ装置が連携した際の動作イメージを下図に示します。

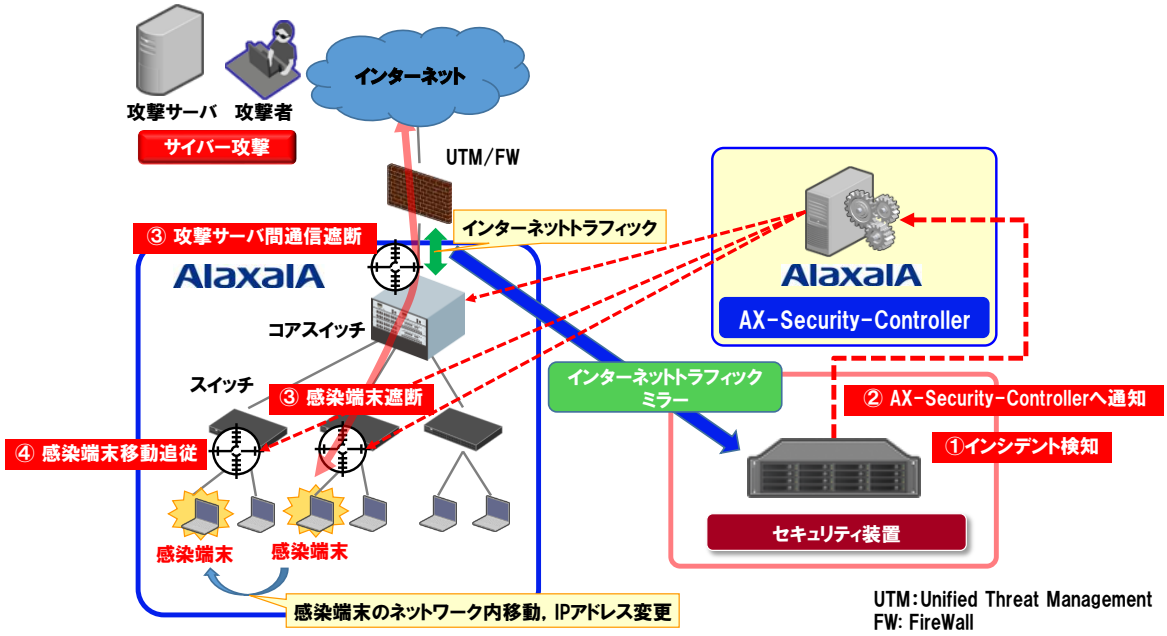

図 1-2　AX-Security-Controller-セキュリティ装置連携動作イメージ

2. 特徴

2.1 AX-Security-Controller の構成

AX-Security-Controller は,下記 2 つのソフトウェアから構成されます。

- AX-Security-Controller (Manager)
  ネットワーク上の端末位置情報を管理するトポロジ管理をおこないます。
  セキュリティ装置がインシデントを検出した場合,トポロジ管理とを連携させ,マルウェア感染端末を収容する装置で同端末をネットワークから遮断します。
  また,ネットワーク管理者が Web インタフェースを通して AX-Security-Controller を管理することができます。
- AX-Security-Controller (Viewer)
  ネットワーク利用者が,遮断中の端末の一覧を参照できます。

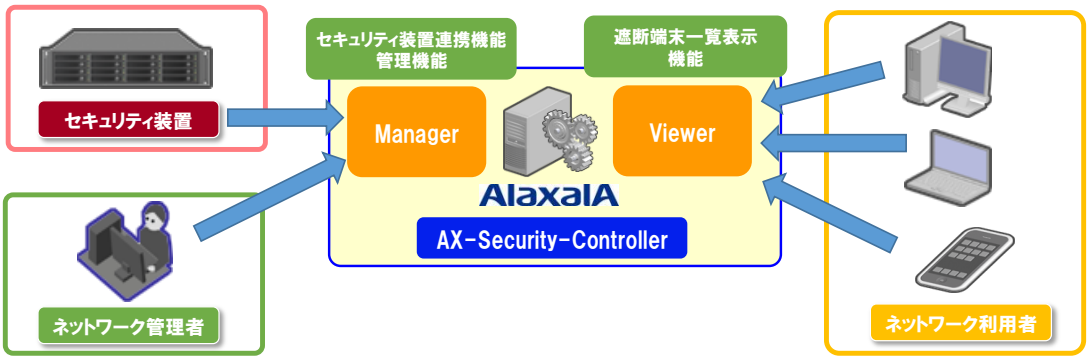

図 2-1 AX-Security-Controller (Manager)と AX-Security-Controller (Viewer)

図 2-2 AX-Security-Controller (Viewer)の画面イメージ

2.2 前提とするネットワーク構成

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

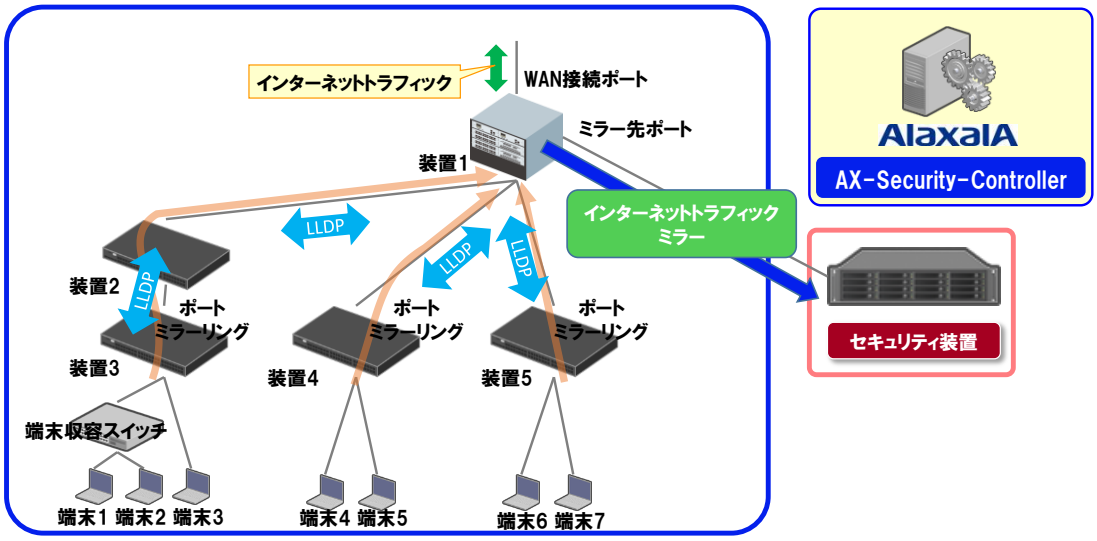

図 2-3 前提とするネットワーク構成例

(1) セキュリティ装置

AX-Security-Controller が連携する下表のセキュリティ装置を網内に配備する必要があります。

表 2-1 セキュリティ装置

セキュリティベンダ	セキュリティ装置
トレンドマイクロ	Trend Micro Policy Manager™ (以下,TMPM) Deep Discovery™ Inspector (以下,DDI)

(2) 管理対象装置

AX-Security-Controller が端末遮断などのセキュリティ制御を施す対象のスイッチを,管理対象装置(または管理対象スイッチ)と呼びます (上図では,装置 1, 装置 2, 装置 3, 装置 4, 装置 5 が対応します)。管理対象装置は,以下の条件を満たす必要があります。

- AX-Security-Controller から,SNMP および SSH でアクセス可能
- 最低 1 台はレイヤ 3 スイッチであり,端末の ARP 情報を学習 (上図では装置 1)
- 端末(もしくは端末収容スイッチ)を収容する管理対象装置はスイッチであり,端末の MAC アドレス情報を学習 (上図では装置 3, 装置 4, 装置 5)
- 隣接する管理対象装置とのイーサネットポートで,LLDP が有効
  (上図では,装置 1 - 装置 2,装置 1 - 装置 4,装置 1 - 装置 5,装置 2 - 装置 3 間)
- セキュリティ装置と直接接続していない管理対象装置において,端末を収容するイーサネットポートで,802.1Q Tag 付与機能を含むポートミラーリングを行い,セキュリティ装置方向のイーサネットポートへ端末トラフィックを複製
  (上図の装置 3 の端末収容スイッチのポート,端末 3 とのポート, 装置 4 の端末 4,端末 5 とのポート, 装置 5 の端末 6,端末 7 とのポートが対応し,装置 1 に接続するポートへミラーリングしています)

(3) WAN 接続ポート・ミラー先ポート

ネットワーク内の管理対象装置のいずれかで,下記 2 つの収容を行う必要があります。
- 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,装置 1 のインターネット側ポートに対応します）
- セキュリティ装置（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,装置 1 のセキュリティ装置側ポートに対応します）

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)
またミラー先ポートがある装置では,(1)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。(セキュリティ装置からの通知により,必要なフレームだけがセキュリティ装置へ中継されます)

2.3 AX-Security-Controller(Manager)

AX-Security-Controller(Manager)は,
(1) セキュリティフィルタ
(2) トポロジ管理
(3) Web インタフェース
から構成され,それぞれ下記のような特徴があります。

(1) セキュリティフィルタ
セキュリティ装置と連携して,ネットワークを制御します。

(a) 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。
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。

(b) 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。

(c) 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。

(2) トポロジ管理
ネットワーク上の端末の位置管理をおこないます。
管理対象装置から周期的に,ARP 情報,MAC アドレス情報,および LLDP 隣接装置情報を収集します。
これにより,端末の物理的な位置を導出します。

(3) Web インタフェース

ネットワーク管理者が,Web インタフェースを通して AX-Security-Controller の設定,管理をおこないます。

(a) ダッシュボード

AX-Security-Controller(Manager)が提供する機能のサマリーを表示します。

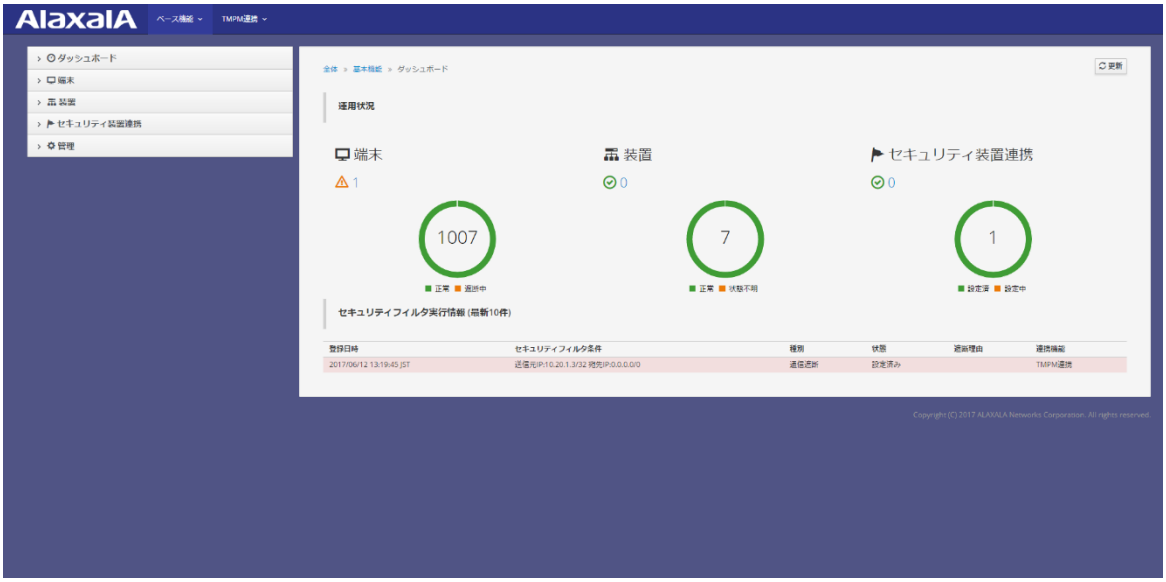

図 2-4 ダッシュボードの画面イメージ

(b) 装置管理

AX-Security-Controller(Manager)の管理対象装置について,以下の機能を提供します。

- 管理対象装置の追加・変更・削除
  管理対象装置の新規追加,変更,および削除をおこないます。
- 管理対象装置の詳細表示
  隣接する管理対象装置一覧の表示,および接続端末一覧を表示します。
- メンテナンスモード
  運用により,特定の管理対象装置を一時的に管理対象外とする場合に設定する機能です。

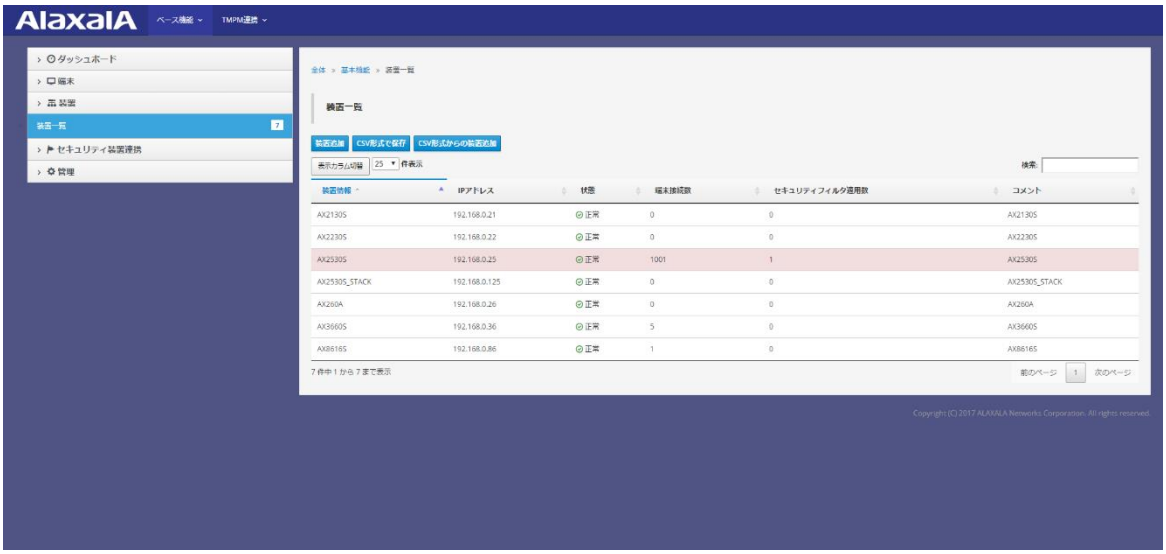

図 2-5 装置管理の画面イメージ

(c) セキュリティフィルタ管理
セキュリティ装置と連携して,追加されたセキュリティフィルタの一覧の表示,および個々のセキュリティフィルタの詳細を表示します。

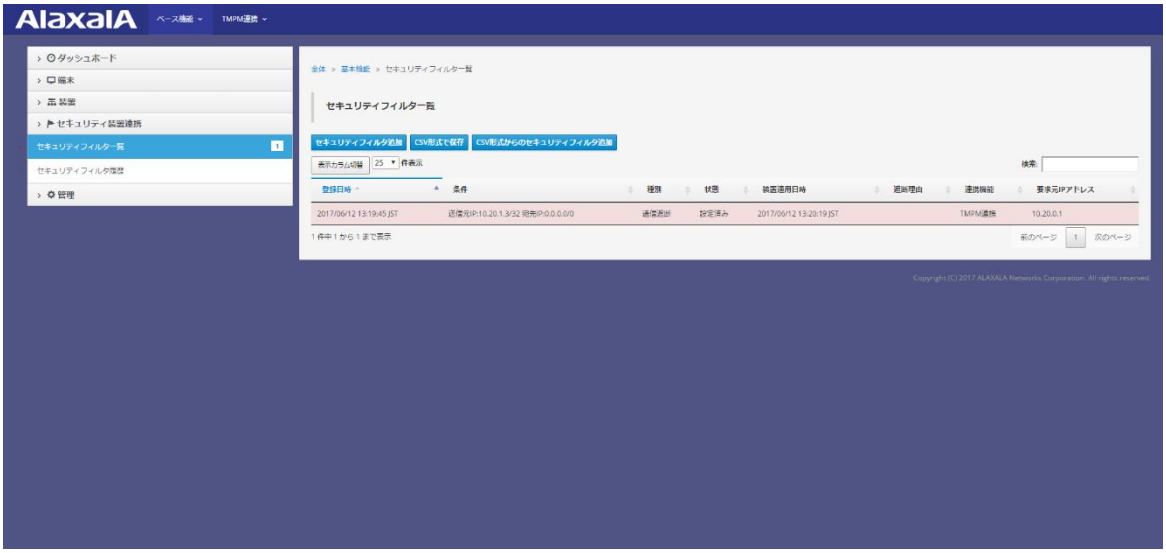

図 2-6　セキュリティフィルタ管理の画面イメージ

(d) 端末管理

収集した端末情報について,以下の機能を提供します。

- 端末一覧の表示
  管理対象装置から収集した端末一覧を表示します。
- エイリアス登録と表示
  端末の IPv4 アドレス,MAC アドレスに呼応する名称(エイリアス)を登録し,そのエイリアスを表示します。端末を表す情報として,端末の名称,利用者,および連絡先等を登録することができます。

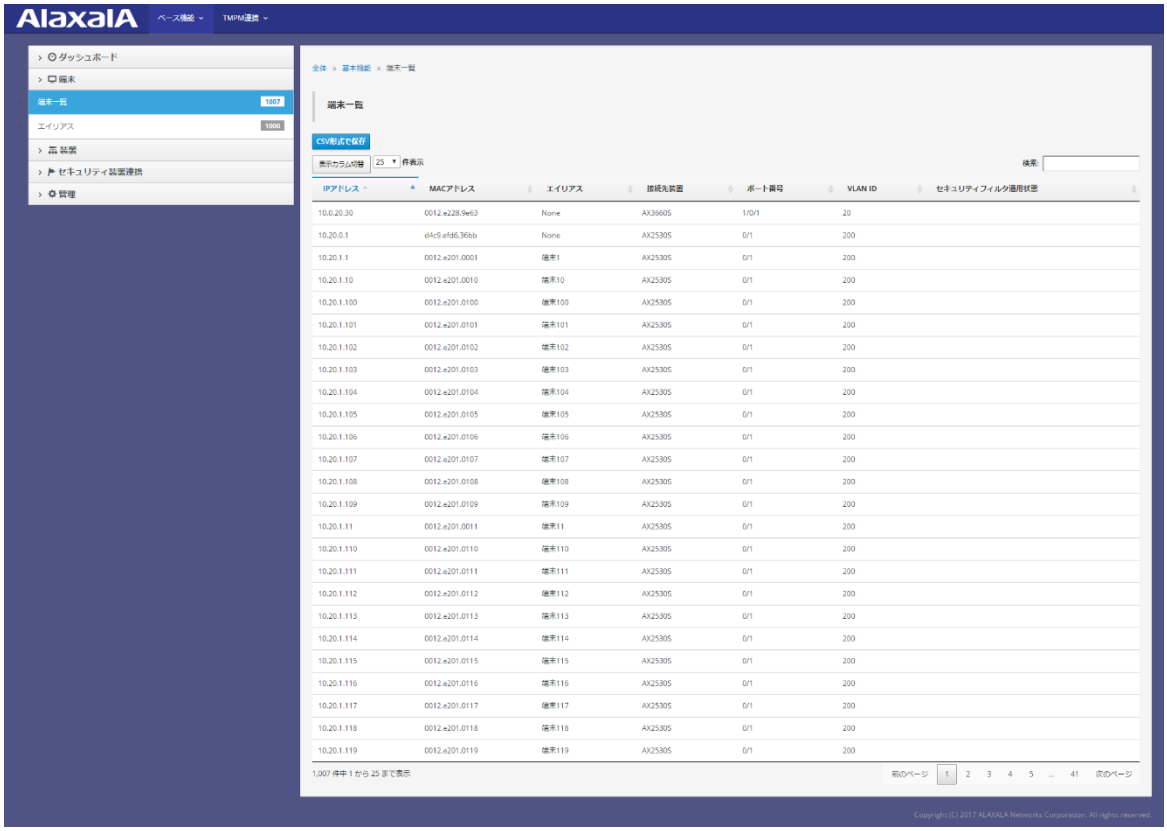

図 2-7　端末管理の画面イメージ

3. ライセンス

3.1 ライセンスの構成

AX-Security-Controller はサブスクリプション方式のソフトウェアです。本ソフトウェアは,下記 3 種類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
基本ライセンス	AX-Security-Controller を使用するためのライセンス(必須)
管理対象スイッチ拡張ライセンス	管理対象スイッチ数を拡張するためのライセンス(オプション)
外部連携ライセンス	セキュリティ装置と連携するためのライセンス(オプション)

3.2 使用期間

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。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, 1 年延長ライセンスの購入が必要です。

表 3-2 ライセンスの使用期間

1 年目	2 年目以降
基本ライセンス(初年度ライセンス)	基本ライセンス(1 年延長ライセンス)
管理対象スイッチ拡張ライセンス (初年度ライセンス)	管理対象スイッチ拡張ライセンス (1 年延長ライセンス)
外部連携(初年度ライセンス)	外部連携(1 年延長ライセンス)

4. 機能一覧

AX-Security-Controller 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
セキュリティフィルタ (セキュリティ装置連携)	通信遮断・例外通信許可	端末通信	全通信遮断(端末IPアドレス)	
			全通信遮断(端末MACアドレス)	(注 1)
			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)	(注 1)
	端末移動追従	ポート移動(同一装置内,別装置)		
		IPv4 アドレス変更		
	特定端末への Web 通信不可表示機能			
	外部連携	トレンドマイクロDDI/TMPMとの連携		(注 2)
トポロジ管理	端末位置(収容管理対象装置,収容ポート)特定			
管理機能	管理者機能	ダッシュボード		
		装置管理		
		端末管理		
		セキュリティフィルタ管理		
	遮断端末表示機能	遮断端末一覧表示		
	運用保守	バックアップ・リストア		
		テクニカルサポート情報採取		
ライセンス	基本ライセンス(管理対象スイッチ 10台まで) ・初年度ライセンス			
	基本ライセンス(管理対象スイッチ 10台まで) ・1年延長ライセンス			
	管理対象スイッチ拡張ライセンス +20台 ・初年度ライセンス			
	管理対象スイッチ拡張ライセンス +20 台 ・1 年延長ライセンス			
	管理対象スイッチ拡張ライセンス +50 台 ・初年度ライセンス			
	管理対象スイッチ拡張ライセンス +50 台 ・1 年延長ライセンス			
	管理対象スイッチ拡張ライセンス +100 台 ・初年度ライセンス			
	管理対象スイッチ拡張ライセンス +100 台 ・1 年延長ライセンス			
	外部連携:トレンドマイクロ DDI/TMPM との連携 ・初年度ライセンス			
	外部連携:トレンドマイクロ DDI/TMPM との連携 ・1 年延長ライセンス			

(注 1) 通信遮断・例外通信許可 端末通信の全通信遮断(端末 MAC アドレス)機能を使用する場合,以下の機能は使用できません。詳細ミラー 端末通信の全通信(端末 MAC アドレス)機能も同様です。

- ・通信遮断 端末通信の全通信遮断(端末 IP アドレス)
- ・通信遮断 端末通信の特定サーバ宛通信遮断(その他は許可)
- ・通信遮断 端末通信の特定サーバ宛通信許可(その他は遮断)
- ・詳細ミラー 端末通信の全通信(端末 IP アドレス)
- ・特定端末への Web 通信不可表示機能

(注 2) 使用には,ライセンス 外部連携:トレンドマイクロ DDI/TMPM との連携(初年度ライセンス,1 年延長ライセンス)が必要です。

5. 動作環境

5.1 ハードウェア構成

表 5-1 動作スペック

項目	最小	推奨
CPU	Intel Core プロセッサー・ファミリー コア数 2	Intel Core プロセッサー・ファミリー コア数 4 以上
メモリ	4GB	8GB 以上
ハードディスクの空き容量	20GB 以上	
イーサネットインタフェース	1 つ	

5.2 ソフトウェア構成

(1) 動作可能オペレーティングシステム(OS)

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	Microsoft Windows 10 (64bit)	
2	CentOS 7 (64bit)	
3	Red Hat Enterprise Linux 7	

(2) 動作可能 Python バージョン

表 5-3 動作可能 Python バージョン

#	Python	備考
1	Python 3.3 以降	3.5 以上推奨

[入手方法]

Microsoft Windows 10(64bit): https://www.python.org/downloads/ より入手してください。

CentOS7(64bit):
Red Hat Enterprise Linux 7: yum リポジトリに IUS Community Project (https://ius.io/)追加後に入手してください。

(3) 追加 Python ライブラリ

表 5-4 追加 Python ライブラリ

#	Python ライブラリ	備考
1	paramiko 2.1.2	
2	pysnmp 4.3.5	
3	pytz 2017.2	

[入手方法]

Python Package Index(https://pypi.python.org/pypi) より,パッケージ管理システム pip を使用して入手してください。

(4) ウェブブラウザ

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

表 5-5 AX-Security-Controller(Manager)動作可能ウェブブラウザ

#	ウェブブラウザ名	備考
1	Firefox 52 ESR	
2	Google Chrome 57 (以降の最新版)	

AX-Security-Controller(Viewer)で使用可能なウェブブラウザの条件を下記に示します。下記の条件を全て満たしている必要があります。

表 5-6 AX-Security-Controller(Viewer)動作可能ウェブブラウザ条件

#	ウェブブラウザ条件	備考
1	2017 年以降にリリースしたウェブブラウザのバージョンであること	
2	HTML5 が解釈可能であること	
3	CSS3 が解釈可能であること	
4	JavaScript(ECMA Script 2015)が解釈可能であること	

5.3 管理対象装置

5.3.1 サポート装置一覧

下記の装置を管理対象装置としてサポートします。

表 5-7 サポート装置一覧

装置名	備考
AX260A	
AX8600S	
AX8300S	
AX3660S	スタック構成は未サポート
AX2500S	
AX2100S	

5.3.2 AX-Security-Controller バージョンと管理対象装置側 OS バージョンの組み合わせ

AX-Security-Controller バージョンと,管理対象装置側 OS のバージョンの組み合わせにより,動作可能な機能が異なります。組み合わせで動作する機能を以下に示します。

(1) AX260A

分類	機能		
セキュリティフィルタ(セキュリティ装置連携)	通信遮断・例外通信許可	端末通信	全通信遮断(端末 IP アドレス)
			全通信遮断(端末 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)
	端末移動追従	ポート移動(同一装置内,別装置)	
		IPv4 アドレス変更	
	特定端末への Web 通信不可表示機能		

装置の対応バージョン：4.7～

(2) AX8600S / AX8300S

分類	機能		
セキュリティフィルタ(セキュリティ装置連携)	通信遮断・例外通信許可	端末通信	全通信遮断(端末 IP アドレス)
			全通信遮断(端末 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)	
		IPv4 アドレス変更	

装置の対応バージョン：12.7.B～

(3) AX3660S

分類	機能		
セキュリティフィルタ(セキュリティ装置連携)	通信遮断・例外通信許可	端末通信	全通信遮断(端末 IP アドレス)
			全通信遮断(端末 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)	
		IPv4 アドレス変更	

装置の対応バージョン：12.1～

(4) AX2500S

分類	機能		
セキュリティフィルタ(セキュリティ装置連携)	通信遮断・例外通信許可	端末通信	全通信遮断(端末 IP アドレス)
			全通信遮断(端末 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)
	端末移動追従	ポート移動(同一装置内,別装置)	
		IPv4 アドレス変更	
	特定端末への Web 通信不可表示機能		

装置の対応バージョン：4.7～

(5) AX2100S

分類	機能		
セキュリティフィルタ(セキュリティ装置連携)	通信遮断・例外通信許可	端末通信	全通信遮断(端末 IP アドレス)
			全通信遮断(端末 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)
	端末移動追従	ポート移動(同一装置内,別装置)	
		IPv4 アドレス変更	
	特定端末への Web 通信不可表示機能		

装置の対応バージョン：2.6～

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-P1560-01	AX-SC	基本ライセンス(管理対象スイッチ 10台まで) ・初年度ライセンス
2	AX-P1560-01E1	AX-SC	基本ライセンス(管理対象スイッチ 10 台まで) ・1 年延長ライセンス
3	AX-P1560-F1	OP-20	管理対象スイッチ拡張ライセンス ＋20 台 ・初年度ライセンス
4	AX-P1560-F1E1	OP-20	管理対象スイッチ拡張ライセンス ＋20 台 ・1 年延長ライセンス
5	AX-P1560-F2	OP-50	管理対象スイッチ拡張ライセンス ＋50 台 ・初年度ライセンス
6	AX-P1560-F2E1	OP-50	管理対象スイッチ拡張ライセンス ＋50 台 ・1 年延長ライセンス
7	AX-P1560-F3	OP-100	管理対象スイッチ拡張ライセンス ＋100 台 ・初年度ライセンス
8	AX-P1560-F3E1	OP-100	管理対象スイッチ拡張ライセンス ＋100 台 ・1 年延長ライセンス
9	AX-P1570-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 ・初年度ライセンス
10	AX-P1570-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

【発行】
2017 年　6 月　（Ver.1.0　第 1 版）
2017 年　8 月　（Ver.1.0　第 2 版）

AlaxalA

アラクサラネットワークス株式会社
URL：http://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：
http://www.alaxala.com/jp/contact/

お問い合わせ先