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。

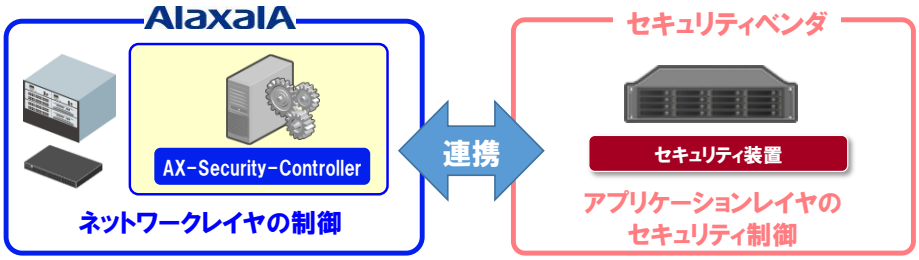

図 1-1 AX-Security-Controller-セキュリティ装置連携

AX-Security-Controller は，以下 2 通りの方法でセキュリティ装置と連携することができます。

(1) 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の連動
- インシデント抽出ルールにマッチしたことを syslog または E-mail で管理者に通知

(2) 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
- 端末の接続位置をトポロジ図形式で視覚的にわかりやすく表示
- 長期的な端末の移動履歴を通じて，後から発覚したインシデントの被疑端末を過去に遡って追跡可能
- セキュリティ装置から対策指示を受けたことを syslog で管理者に通知
- セキュリティ装置の対策指示に従い，ネットワーク装置に設定を適用したことを syslog で管理者に通知

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

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

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。

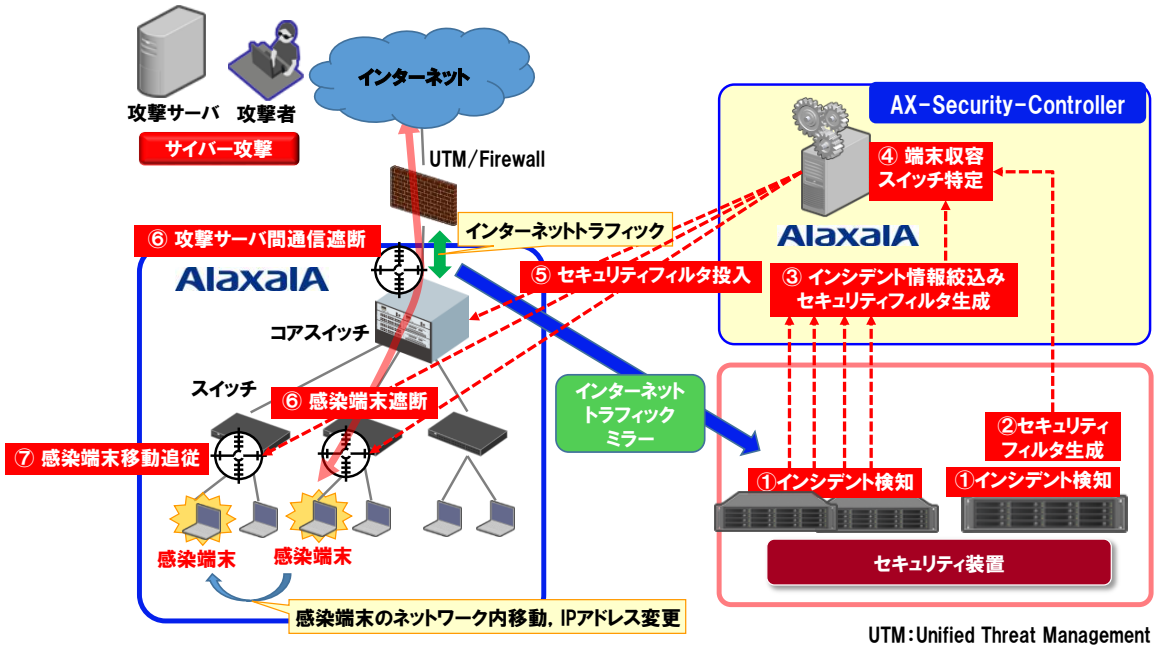

図 1-2　AX-Security-Controller-セキュリティ装置連携動作イメージ

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

2. 特徴

2.1 AX-Security-Controller の構成

AX-Security-Controller は,下記 3 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。セキュリティ装置のインシデント情報やインシデント対策指示から，トポロジ管理に基づいてインシデント対策を行うことにより，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。
- AX-Security-Controller(Tracker)
  AX-Security-Controller(Manager)が管理しているトポロジから，端末が接続している装置およびポートを定期的に収集し，最大 3650 日の履歴を保持することで，端末の移動履歴を算出します。
  また，ネットワーク管理者がこの算出結果を Web インタフェースを通して参照することができます。

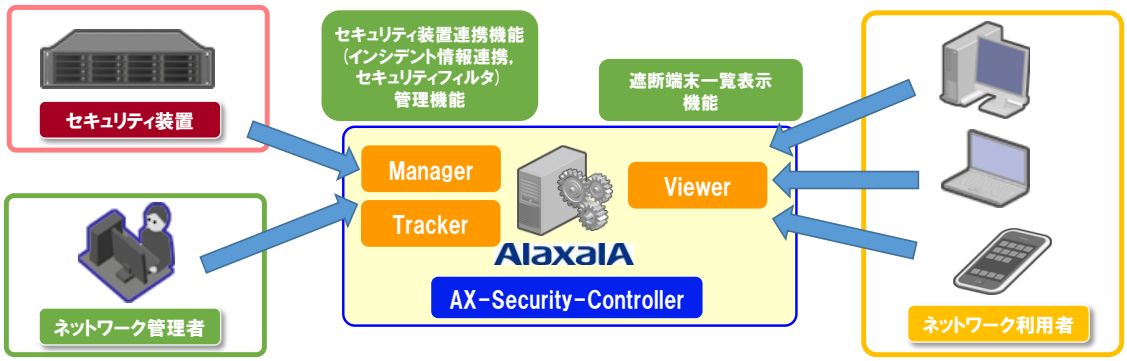

図 2-1　AX-Security-Controller の構成

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

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

検索画面表示

履歴検索結果

CSV形式で保存

表示カラム切替　10 件表示　検索:

接続開始日時	接続終了日時	接続期間	MACアドレス	IPアドレス	エイリアス：用途	エイリアス：端末名	接続先装置	ポート番号
2019/03/06 11:14:31 JST	接続中	0d0h0m22s	0000.5e00.5354	198.51.100.54	OA	端末名4	エッジスイッチ1	0/9
2019/03/06 11:03:18 JST	2019/03/06 11:13:31 JST	0d0h10m13s	0000.5e00.5354		None	None	エッジスイッチ1	0/9
2019/03/06 09:58:59 JST	2019/03/06 11:03:18 JST	0d1h4m19s	0000.5e00.5354	198.51.100.54	None	None	エッジスイッチ1	0/9
2019/03/06 11:13:31 JST	接続中	0d0h1m22s	0000.5e00.5355	198.51.100.55	OA	端末名5	エッジスイッチ1	0/9
2019/03/06 11:03:18 JST	2019/03/06 11:13:31 JST	0d0h10m13s	0000.5e00.5355		None	None	エッジスイッチ1	0/9
2019/03/06 09:58:59 JST	2019/03/06 11:03:18 JST	0d1h4m19s	0000.5e00.5355	198.51.100.55	None	None	エッジスイッチ1	0/9
2019/03/06 11:13:31 JST	接続中	0d0h1m22s	0000.5e00.5356	198.51.100.56	OA	端末名6	エッジスイッチ1	0/9
2019/03/06 11:03:18 JST	2019/03/06 11:13:31 JST	0d0h10m13s	0000.5e00.5356		None	None	エッジスイッチ1	0/9
2019/03/06 09:58:59 JST	2019/03/06 11:03:18 JST	0d1h4m19s	0000.5e00.5356	198.51.100.56	None	None	エッジスイッチ1	0/9
2019/03/06 11:13:31 JST	接続中	0d0h1m22s	0000.5e00.5357	198.51.100.57	OA	端末名7	エッジスイッチ1	0/9

45 件中 1 から 10 まで表示

前のページ 1 2 3 4 5 次のページ

図 2-3　AX-Security-Controller(Tracker)の画面イメージ

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

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。

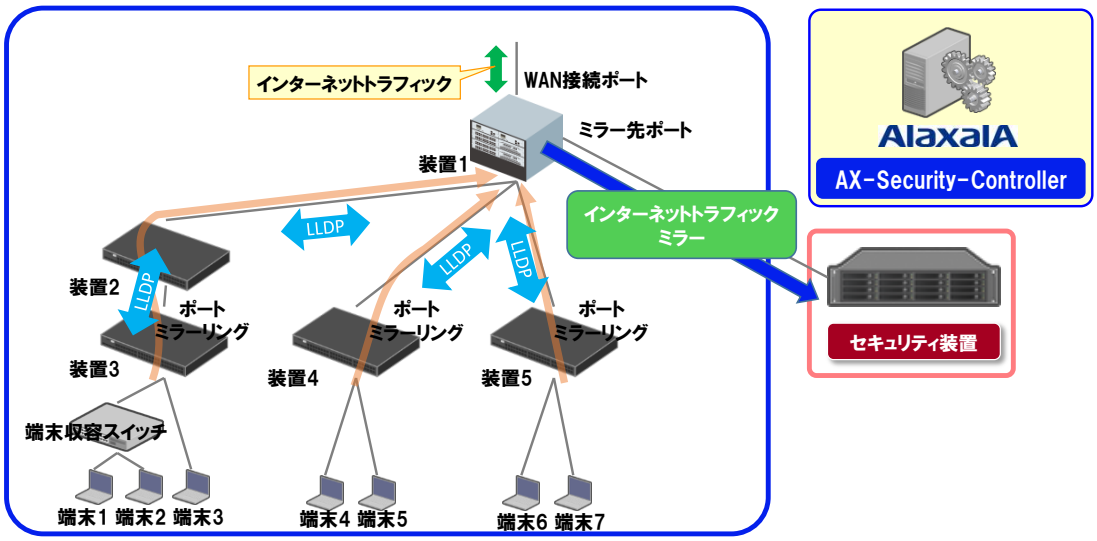

図 2-4 前提とするネットワーク構成例

(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

連携方式	セキュリティベンダ	セキュリティ装置
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
	フォーティネット，ファイア･アイなど	FortiGate，FireEye Network Security など Syslog メッセージを CEF(Common Event Format)で出力可能なセキュリティ装置

次表に弊社で接続検証済みの装置とバージョンの組み合わせを示します。この表に記載されていないセキュリティ装置とバージョンの組み合わせは検証の上ご利用ください。

表 2-2 セキュリティフィルタ連携接続検証済みセキュリティ装置

セキュリティベンダ	セキュリティ装置	バージョン
トレンドマイクロ	Trend Micro Policy Manager™	2.5 SP1※
	Deep Discovery™ Inspector	3.8 SP3

※AX-Security-Contoller はバージョン 1.4 からセキュリティフィルタ IPv6 通知をサポートします。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

表 2-3　インシデント情報連携接続検証済みセキュリティ装置

セキュリティベンダ	セキュリティ装置	バージョン
パロアルトネットワークス	次世代ファイアウォール	8.0
フォーティネット	FortiGate	5.6.2
ファイア・アイ	FireEye Network Security	8.0

(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
- 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)
  ※：管理対象装置で LLDP が動作しない場合，隣接する管理対象装置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
- 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)

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(4) セキュリティ制御を施すポート
ネットワーク内の管理対象装置のどのポートでマルウェア感染端末遮断などのセキュリティ制御を施すかを，網構成に応じて以下のいずれから選択する必要があります。

ポート名		端末直収ポート	アクセスリスト拡張ポート(図 2-5)	永続設定ポート(図 2-6)
場所		当該端末を収容する端末収容スイッチのポート	当該端末を収容する端末収容スイッチの，上流装置のポート	制御対象の全トラフィックが通過する装置/ポート群
管理対象装置が満たすべき AX-Security-Controller の機能要件	セキュリティフィルタ	端末収容スイッチが対応	上流装置が対応	永続設定ポートを有する装置が対応
	トポロジ管理(MAC アドレス情報)	端末収容スイッチから収集	端末収容スイッチから収集	―
	トポロジ管理(ARP/NDP 情報)	端末のデフォルトゲートウェイから収集	端末のデフォルトゲートウェイから収集	―
メリット		最も端末に近い場所でセキュリティ制御が可能	端末収容スイッチがセキュリティフィルタ未対応でも、セキュリティ制御が可能	端末位置が特定できない場合でもセキュリティ制御が可能

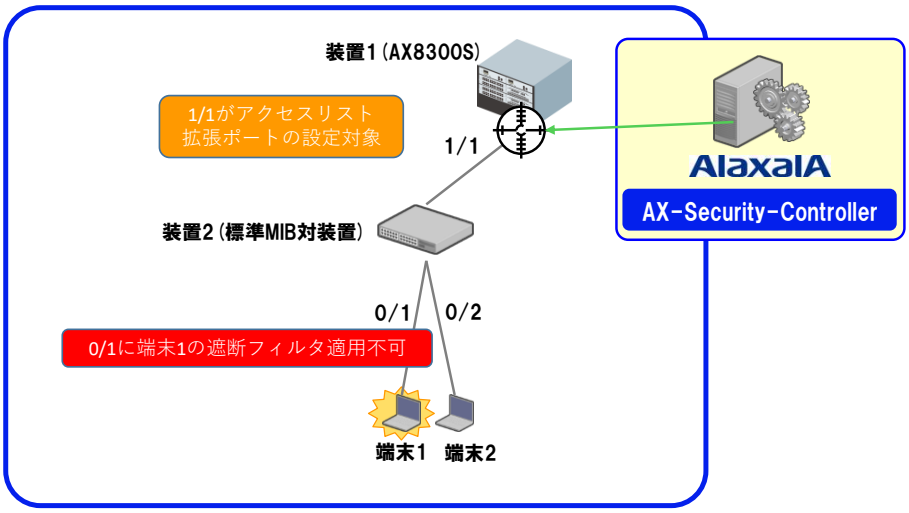

図 2-5　アクセスリスト拡張ポートを適用する構成例

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

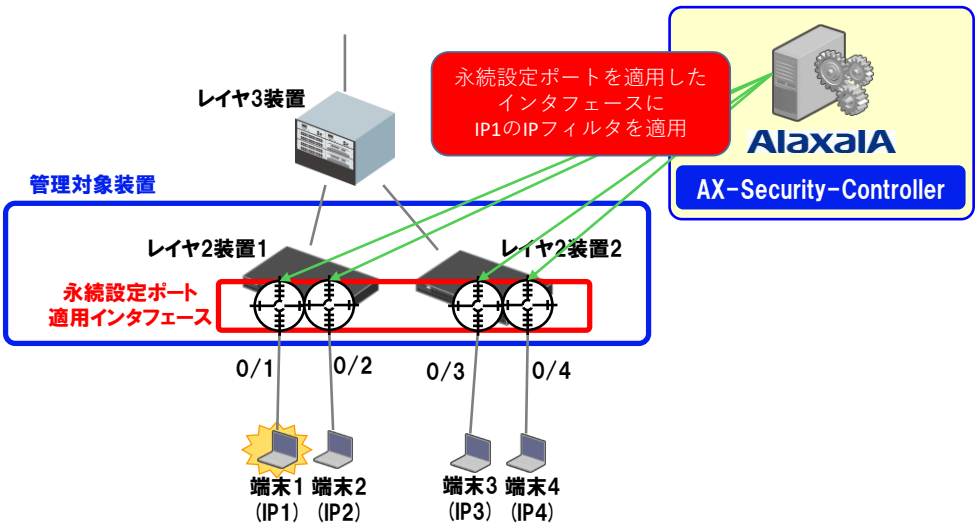

図 2-6　永続設定ポートを適用する構成例

2.3 AX-Security-Controller(Manager)

AX-Security-Controller(Manager)は,

(1) インシデント情報連携
(2) セキュリティフィルタ
(3) セグメンテーションセキュリティ
(4) トポロジ管理
(5) Web インタフェース
(6) セキュリティレポート
(7) イベント通知インタフェース

から構成され,それぞれ下記のような特徴があります。

(1) インシデント情報連携

セキュリティ装置から通知されるインシデント情報を，ユーザが定義したインシデント抽出ルールにより取捨選択し，そのアクションとしてセキュリティフィルタを適用します。
セキュリティ装置からのインシデントを受け付けるプロトコルは，以下となります。

表 2-4 インシデント受け付けプロトコル

プロトコル	説明
syslog※1	・CEF(Common Event Format)の syslog メッセージ※2

※1 準拠規格：RFC5424 Syslog Protocol
※2 AX-Security-Controller は IPv4 アドレスでのみ syslog を受信可能です

以降，syslog を通知するセキュリティ装置を Syslog クライアントとも呼びます。
インシデント抽出ルールは，1 ルールあたり，優先度と条件(CEF フィールド名と値の組み合わせ)で構成します。条件は，最大 6 つの CEF フィールド名と値の組み合わせを設定することができます。
受信した syslog メッセージは，優先度昇順にインシデント抽出ルールを検索し，条件がすべて一致した場合にインシデントとして抽出します。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

インシデント抽出ルールへのマッチングや受信した syslog メッセージの履歴も同時に残しますが，不要になった分は Web インタフェース経由で随時削除可能です。

(a) Syslog フォーマット

① パロアルトネットワークス 次世代ファイアウォール連携
下記サイトを参考にして，syslog の出力フォーマットを CEF にしてください。

https://www.paloaltonetworks.com/documentation/misc/cef.html

② Syslog 連携(CEF)
Syslog 連携(CEF)は以下の syslog フォーマットに対応します。

```
CEF: <Version>|<Device Vendor>|<Device Product>|<Device Version>|
<Device Event Class ID>|<Name>|<Severity>|<extension>
```

syslog フォーマットの各パラメータの意味を以下に示します。

表 2-5 各パラメータの説明

パラメータ		説明
ヘッダフィールド	Version	CEF のバージョン
	Device Vendor	ベンダ名称※
	Device Product	プロダクト名称
	Device Version	バージョン
	Device Event Class ID	イベント識別子
	Name	イベント名
	Severity	重要度
拡張フィールド	extension	拡張フィールド <Key 名>=<値>

※: Syslog 連携(CEF)ライセンスに関連付けたベンダ名称のみインシデント抽出ルールへのマッチング処理を実施します。登録されていないベンダ名称の syslog メッセージは syslog の受信履歴には登録されますが，ルールにマッチしているかの判定処理を行いません。

(b) インシデント抽出ルール
インシデント抽出ルールで指定可能な CEF フィールドを下記に示します。

表 2-6 インシデント抽出に指定可能な CEF フィールド

CEF フィールド		データ型	指定可否
ヘッダフィールド	Version	Integer	×
	Device Vendor	String	×
	Device Product	String	×
	Device Version	String	×
	Signature ID	String or Integer	○
	Device Event Class ID	String or Integer	○
	Name	String	○

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

CEF フィールド		データ型	指定可否
	Severity	String or Integer	○
拡張フィールド	act	String	○
	app	String	○
	c6a1	IPv6 Address	○
	c6a1Label	String	○
	c6a2	IPv6 Address	○
	c6a2Label	String	○
	c6a3	IPv6 Address	○
	c6a3Label	String	○
	c6a4	IPv6 Address	○
	c6a4Label	String	○
	cfp1	Floating Point	○
	cfp1Label	String	○
	cfp2	Floating Point	○
	cfp2Label	String	○
	cfp3	Floating Point	○
	cfp3Label	String	○
	cfp4	Floating Point	○
	cfp4Label	String	○
	cn1	Long	○
	cn1Label	String	○
	cn2	Long	○
	cn2Label	String	○
	cn3	Long	○
	cn3Label	String	○
	cnt	Integer	○
	cs1	String	○
	cs1Label	String	○
	cs2	String	○
	cs2Label	String	○
	cs3	String	○
	cs3Label	String	○
	cs4	String	○
	cs4Label	String	○
	cs5	String	○
	cs5Label	String	○
	cs6	String	○
	cs6Label	String	○
	destinationDnsDomain	String	○
	destinationServiceName	String	○
	destinationTranslatedAddress	IPv4 Address or IPv6 Address	○
	destinationTranslatedPort	Integer	○
	deviceCustomDate1	Time Stamp	○
	deviceCustomDate1Label	String	○

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

CEF フィールド		データ型	指定可否
	deviceCustomDate2	Time Stamp	○
	deviceCustomDate2Label	String	○
	deviceDirection	Integer	○
	deviceDnsDomain	String	○
	deviceExternalId	String	○
	deviceFacility	String	○
	deviceInboundInterface	String	○
	deviceNtDomain	String	○
	deviceOutboundInterface	String	○
	devicePayloadId	String	○
	deviceProcessName	String	○
	deviceTranslatedAddress	IPv4 Address or IPv6 Address	○
	dhost	String	○
	dmac	MAC Address	○
	dntdom	String	○
	dpid	Integer	○
	dpriv	String	○
	dproc	String	○
	dpt	Integer	○
	dst	IPv4 Address or IPv6 Address	○
	dtz	String	○
	duid	String	○
	duser	String	○
	dvc	IPv4 Address or IPv6 Address	○
	dvchost	String	○
	dvcmac	MAC Address	○
	dvcpid	Integer	○
	end	Time Stamp	○
	externalId	String	○
	fileCreateTime	Time Stamp	○
	fileHash	String	○
	fileId	String	○
	fileModificationTime	Time Stamp	○
	filePath	String	○
	filePermission	String	○
	fileType	String	○
	flexDate1	Time Stamp	○
	flexDate1Label	String	○
	flexNumber1	Integer	○
	flexNumber1Label	String	○
	flexNumber2	Integer	○
	flexNumber2Label	String	○
	flexString1	String	○

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

CEF フィールド		データ型	指定可否
	flexString1Label	String	○
	flexString2	String	○
	flexString2Label	String	○
	fname	String	○
	fsize	Integer	○
	in	Integer	○
	msg	String	○
	oldFileCreateTime	Time Stamp	○
	oldFileHash	String	○
	oldFileId	String	○
	oldFileModificationTime	Time Stamp	○
	oldFileName	String	○
	oldFilePath	String	○
	oldFilePermission	String	○
	oldFileSize	Integer	○
	oldFileType	String	○
	out	Integer	○
	outcome	String	○
	proto	String	○
	reason	String	○
	request	String	○
	requestClientApplication	String	○
	requestContext	String	○
	requestCookies	String	○
	requestMethod	String	○
	rt	Time Stamp	○
	shost	String	○
	smac	MAC Address	○
	sntdom	String	○
	sourceDnsDomain	String	○
	sourceServiceName	String	○
	sourceTranslatedAddress	IPv4 Address or IPv6 Address	○
	sourceTranslatedPort	Integer	○
	spid	Integer	○
	spriv	String	○
	sproc	String	○
	spt	Integer	○
	src	IPv4 Address or IPv6 Address	○
	start	Time Stamp	○
	suid	String	○
	suser	String	○
	type	Integer	○
	agentDnsDomain	String	○
	agentNtDomain	String	○

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

CEF フィールド		データ型	指定可否
	agentTranslatedAddress	IPv4 Address or IPv6 Address	○
	agentTranslatedZoneExternalID	String	○
	agentTranslatedZoneURI	String	○
	agentZoneExternalID	String	○
	agentZoneURI	String	○
	agt	IPv4 Address or IPv6 Address	○
	ahost	String	○
	aid	String	○
	amac	MAC Address	○
	art	Time Stamp	○
	at	String	○
	atz	String	○
	av	String	○
	cat	String	○
	customerExternalID	String	○
	customerURI	String	○
	destinationTranslatedZoneExternalID	String	○
	destinationTranslatedZoneURI	String	○
	destinationZoneExternalID	String	○
	destinationZoneURI	String	○
	deviceTranslatedZoneExternalID	String	○
	deviceTranslatedZoneURI	String	○
	deviceZoneExternalID	String	○
	deviceZoneURI	String	○
	dlat	Double	○
	dlong	Double	○
	eventId	Long	○
	rawEvent	String	○
	slat	Double	○
	slong	Double	○
	sourceTranslatedZoneExternalID	String	○
	sourceTranslatedZoneURI	String	○
	sourceZoneExternalID	String	○
	sourceZoneURI	String	○

○：指定可能 ×：指定不可

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

また，パロアルトネットワークス 次世代ファイアウォールと連携する場合，追加で指定可能な CEF フィールド次の表に示します。

表 2-7　インシデント抽出に指定可能な CEF フィールド

CEF フィールド		データ型
拡張フィールド	PanOSPacketsReceived	Integer
	PanOSPacketsSent	Integer
	PanOSReferer	String
	PanOSXff	String
	PanOSDGl1	Integer
	PanOSDGl2	Integer
	PanOSDGl3	Integer
	PanOSDGl4	Integer
	PanOSVsysName	String
	PanOSXforwarderfor	IPv4 Address or IPv6 Address
	PanOSActionFlags	String
	PanOSContentVer	String
	PanOSDesc	String
	PanOSDstUUID	String
	PanOSMonitorTag	String
	PanOSParentSessionID	Integer
	PanOSParentStartTime	Time Stamp
	PanOSSrcUUID	String
	PanOSThreatCategory	String
	PanOSTunnelFragment	Integer
	PanOSTunnelType	String
	PanOSTunnelID	Integer

さらに，Syslog クライアント追加時にパロアルトネットワークス 次世代ファイアウォール連携を指定した場合，自動で次の表に示すデフォルトのルールを設定します。

表 2-8　自動で設定されるデフォルトのルール

優先度	条件	種別	値	アクション種別	送信元指定	宛先指定
5000	条件 1	Name	CORRELATION	通信遮断	src	－
5100	条件 1	Name	THREAT	通信遮断	src	－
	条件 2	Signature ID	Spyware			
	条件 3	flexString2	client-to-server			
5200	条件 1	Name	THREAT	通信遮断	dst	－
	条件 2	Signature ID	Spyware			
	条件 3	flexString2	server-to-client			
5300	条件 1	Name	通信遮断	通信遮断	src	－
	条件 2	Signature ID	url			
	条件 3	cs2	command-and-control			
	条件 4	flexString2	client-to-server			
5400	条件 1	Name	手動選択	手動選択	－	－

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

優先度	条件	種別	値	アクション種別	送信元指定	宛先指定
	条件 2	Signature ID	Wildfire			
	条件 3	cs2	Malicious			
	条件 4	act	Allow			
	条件 5	flexString2	server-to-client			

(凡例) －：未選択

表 2-6 および表 2-7 で指定可能なフィールドの他に，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。
ユーザ定義拡張フィールドは，Web インタフェースにより，拡張フィールド名称とデータ型の組を設定することで使用可能となります。指定可能なデータ型を以下の表に示します。

表 2-9　指定可能なデータ型

データ型
String
Integer
String or Integer
IPv4 Address
IPv6 Address
IPv4 Address or IPv6 Address
MAC Address
Floating Point
Double
Long
Time Stamp

最後に，フィールドの値の検索方式は，データ型ごとに条件が異なります。CEF データ型ごとの検索条件を以下の表に示します。

表 2-10　データ型ごとの検索条件

データ型	検索条件
String	部分一致検索
IPv4 Address	完全一致検索
IPv6 Address	完全一致検索
MAC Address	完全一致検索
Floating Point	完全一致検索
Double	完全一致検索
Long	完全一致検索
Integer	完全一致検索
Time Stamp	部分一致検索

(2) セキュリティフィルタ

セキュリティ装置からの指示，および AX-Security-Controller が抽出したインシデントと連携して,ネットワークを制御します。セキュリティフィルタの生成・削除契機を下図に示します。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

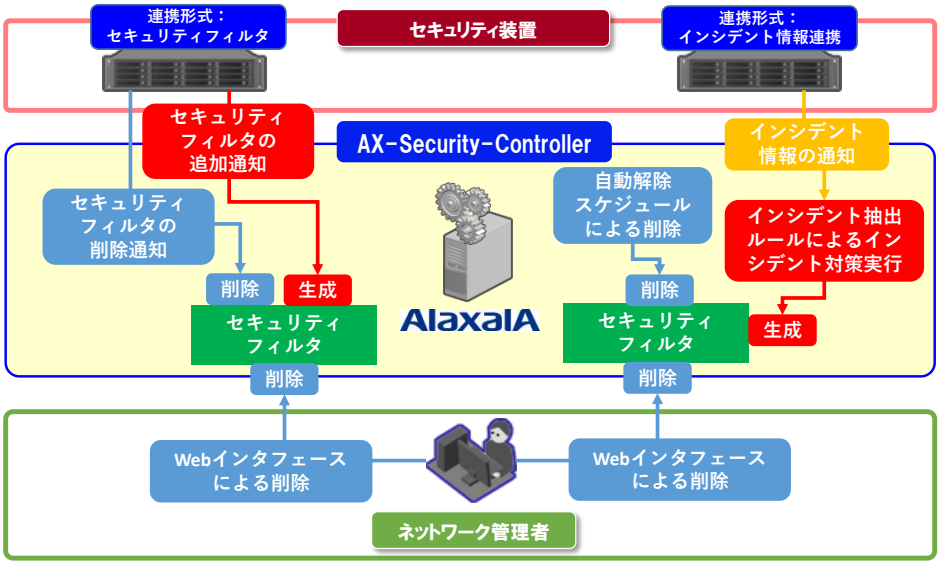

図 2-7　セキュリティフィルタの生成・削除契機

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(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,2.2(4)節のポートに,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。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,IP アドレスや MAC アドレスで通信遮断指示を受けると,遮断指示されたアドレスに呼応する MAC 情報を用いて端末の使用している IPv4 アドレスと IPv6 アドレスを特定することで，両バージョンの IP アドレスを用いた通信を遮断することができます。

(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。

(d) 永続設定ポート
端末の位置を管理できない場合に通信遮断・例外通信許可を行うための永続設定ポートを静的に設定できます。

(e) スケジュール解除
指定のタイミングで通信遮断・詳細ミラーを自動で解除することができます。解除するタイミングとして毎月指定日の指定時刻，毎週指定曜日の指定時刻，毎日の指定時刻の 3 パターンから 1 つだけ設定可能です。なお，インシデント情報連携で設定したセキュリティフィルタのみ自動解除が可能で, 後から自動解除の有効/無効を切り替えることもできます。

(f) タイマー解除
セキュリティフィルタ生成時に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。

(g) 同一フィルタの設定抑止
複数のセキュリティフィルタで同一のフィルタを管理対象装置に設定する場合，管理対象装置へと 2 個目以降の同一フィルタの設定を抑止します。これにより，管理対象装置のフィルタ数を節約し，収容効率を高めることができます。

(h) エイリアス未登録端末の自動遮断
エイリアスの登録されていない端末を管理されていない端末として，自動で通信を遮断することで，不審な端末の接続からネットワークを守ることができます。

(3) セグメンテーションセキュリティ
セグメンテーションセキュリティは，AX-Security-Contoroller 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。インシデント対策のルールをきめ細かく設定できるため，ポリシーの異なる部門毎に異なるルールを適用するなど，より柔軟なセキュリティ運用ができるようになります。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(a) 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。各基準には優先度を定義することができ，同一端末が各基準でどのセグメントに所属するかが異なる場合は，一番優先度の高いセグメントが所属セグメントになります。

表 2-11　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，標準 MIB 対応装置を指定することはできません。

(b) 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 2-12　セグメントの分類

分類	内容	適用例
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装置へのコンフィグレーションの適用をおこないません。	インシデント監視不要な特殊端末をグルーピング
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。	部門単位に，端末をグルーピング
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。	ゲスト端末や本来存在しないはずの端末をグルーピング

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(c) 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 2-13 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

(4) 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,NDP 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。管理対象装置で LLDP が動作しない場合，隣接する管理対象装置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が可能です。
これにより,端末の物理的な位置を導出します。

(a) 管理対象装置検索追加支援
入力された範囲の IP アドレスに対してアクセスを実施し，アクセスに成功した IP アドレスに対して装置の自動判別を行い一覧として表示します。一覧からは装置の一括追加が可能で，初期導入時のオペレーションを削減することができます。

(b) 管理対象装置間接続追加支援
管理対象の装置から収集した情報を元に装置間の接続情報を判別し，接続情報の候補を一覧として表示します。一覧からは装置間の接続情報の一括追加が可能で，初期導入時のオペレーションを削減することができます。

(c) 事前設定確認支援
AX-Security-Controller の初期設定において，ネットワーク管理者の設定を支援するために，管理対象装置の LLDP，アクセスリスト等のコンフィグレーションの事前設定の内容を確認する機能をサポートします。

(d) 端末位置表示
管理対象装置から定期的に収集する情報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，管理対象装置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。IP アドレスと MAC アドレスの対応がない端末についても表示が可能です。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(e) エイリアス
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。

(f) ポートエイリアス
管理対象装置のポートについて，呼応する名称，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。これにより，ネットワーク管理者は，管理対象装置のポート情報を，ポート番号だけでなく，エイリアス内容により確認することが可能です。

(g) 管理対象外ポート
管理対象装置のポートを，トポロジ管理から対象外とすることが可能です。たとえば管理用コンソールの端末を接続したポートを登録することで，管理用コンソールの端末を，端末一覧から表示しないようにすることが可能になります。

(h) マップ
マップは，管理対象装置－管理対象装置の接続，および管理対象装置－端末の接続をグラフィカルに可視化する機能です。

図 2-8　マップ画面

マップにより，ネットワーク管理者は管理対象装置や端末をトポロジ図面上で直感的に管理できるようになります。

・ 管理対象装置・端末の配置操作
画面上に表示される管理対象装置や端末の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ます。端末の配置は、接続先装置を中心に自動配置することも可能です。マップ全体で自動配置を有効化でき、接続先装置ごとに無効化できます。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

端末は，IP アドレス，MAC アドレス，エイリアス，ポートエイリアス，接続先装置，接続先ポート，VLAN ID がすべて一致する端末を 1 つの端末として扱います。このため，エイリアスやポートエイリアスの変更を行った場合，別の端末として扱われ，配置が変更されます。

・ 管理対象装置・端末情報の詳細表示
画面上に表示される管理対象装置および端末のアイコンを選択することにより，管理端末装置・端末の詳細情報を確認することが可能です。

表 2-14 管理対象装置･端末の詳細情報の表示

項目	説明
管理対象装置	装置名称，IP アドレス，MAC アドレス，装置モデル
端末	エイリアス，IP アドレス，MAC アドレス，ベンダ，ポートエイリアス，接続先装置，接続先ポート，VLAN ID

・ 端末の制御
画面上のアイコンを選択した端末について，下記の制御が可能になります。

表 2-15 端末への制御可能な機能

機能		説明
セキュリティフィルタ	通信遮断	端末の MAC アドレスに関する通信遮断のセキュリティフィルタを生成し，通信遮断をおこないます。
	通信遮断解除	端末の MAC アドレスに関する通信遮断のセキュリティフィルタを削除し，通信遮断解除をおこないます。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(5) 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 2-9 ダッシュボードの画面イメージ

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(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。
- 接続情報
  管理対象装置で LLDP が動作しない場合に，隣接する管理対象装置間のポートの接続関係の設定，および削除をおこないます。
  また端末を収容する管理対象装置に呼応するアクセスリスト拡張ポートを定義します。
- 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。
- コンフィグ空き容量監視
  装置からコンフィグ空き容量を取得して表示します。コンフィグレーションの空き容量が全容量の 20%未満の場合，Syslog と E-mail で管理者に通知する機能をサポートしています。Syslog と E-mail を通知する契機は，対象装置にコンフィグレーションを設定・削除する契機です。

図 2-10　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た以下の機能を提供します。

- セキュリティフィルタの表示
  セキュリティフィルタ一覧の表示，および個々のセキュリティフィルタの詳細表示をおこないます。
- Syslog クライアントの追加・削除
  インシデント情報を通知するセキュリティ装置の追加，および削除をおこないます。
- Syslog クライアントごとのインシデント抽出ルールの追加・削除
  インシデント抽出ルールの追加，および削除をおこないます。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

- 履歴管理
  Syslog メッセージの受信，セキュリティフィルタ適用，およびインシデント抽出ルールへのマッチングに関する，動作履歴の記録を管理します。
- セキュリティフィルタの複数選択
  複数の指定セキュリティフィルタについて，セキュリティフィルタの適用解除を実施することができます。

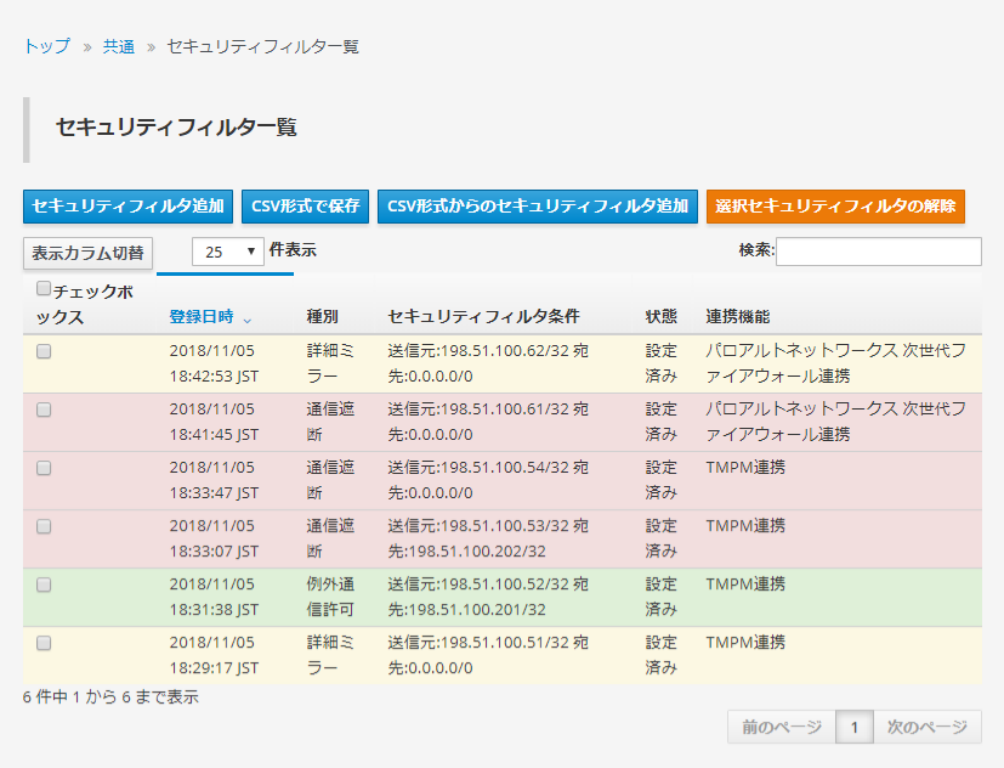

図 2-11　セキュリティフィルタの画面イメージ

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

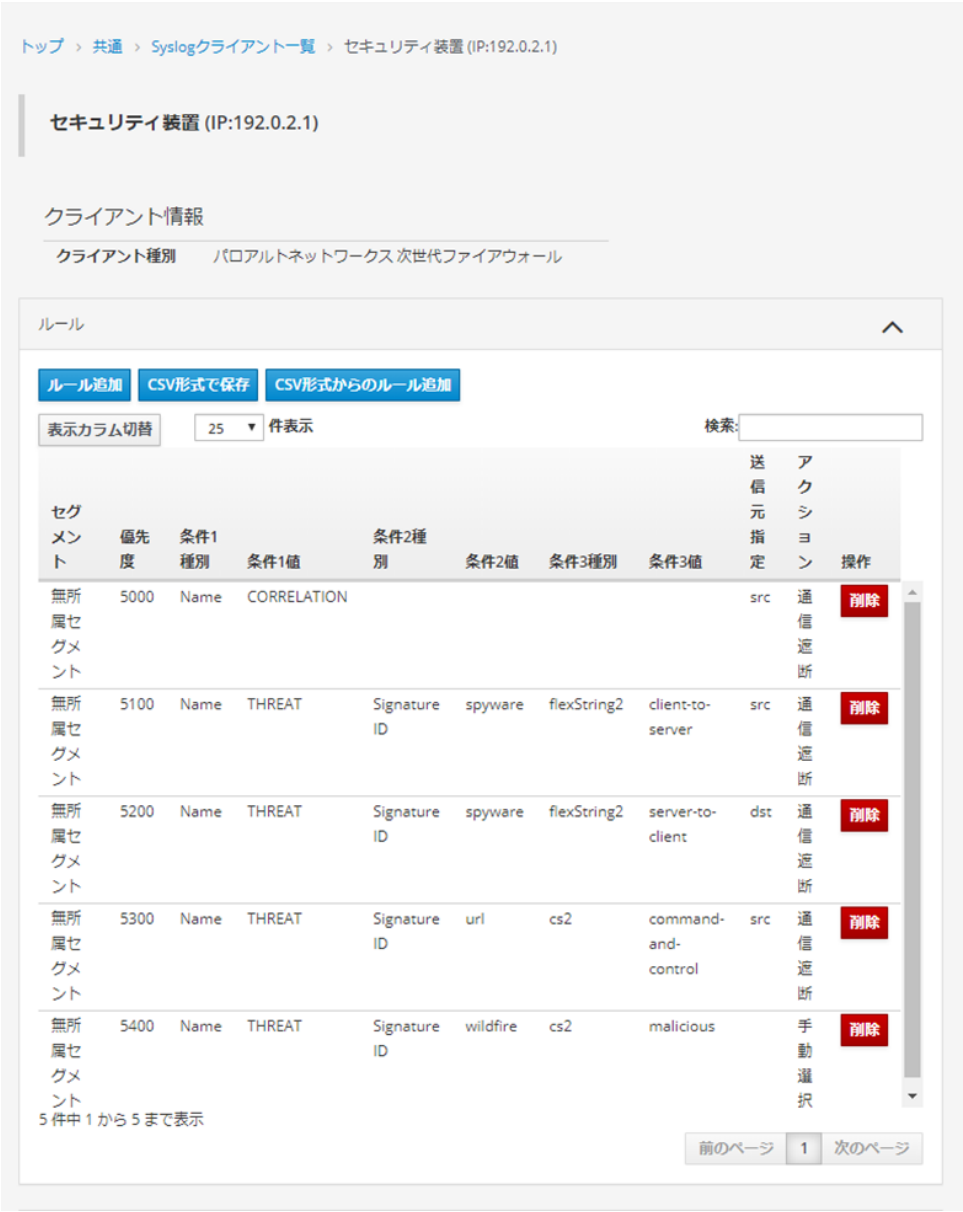

図 2-12　Syslog クライアント詳細の画面イメージ

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(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 IP 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。
- ポートエイリアス登録と表示
  装置の名称,およびポートに呼応する名称(ポートエイリアス)を登録し,そのポートエイリアスを表示します。
- MAC アドレスのベンダ表示
  MAC アドレスに呼応するベンダ名称を表示します。
- 端末一覧からのセキュリティフィルタ適用
  指定端末の通信遮断を実施することができます。また，通信遮断解除・全セキュリティフィルタの適用を解除することも可能です。
- 端末の複数選択
  複数の指定端末について，通信遮断またはセキュリティフィルタの適用解除を実施することができます。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

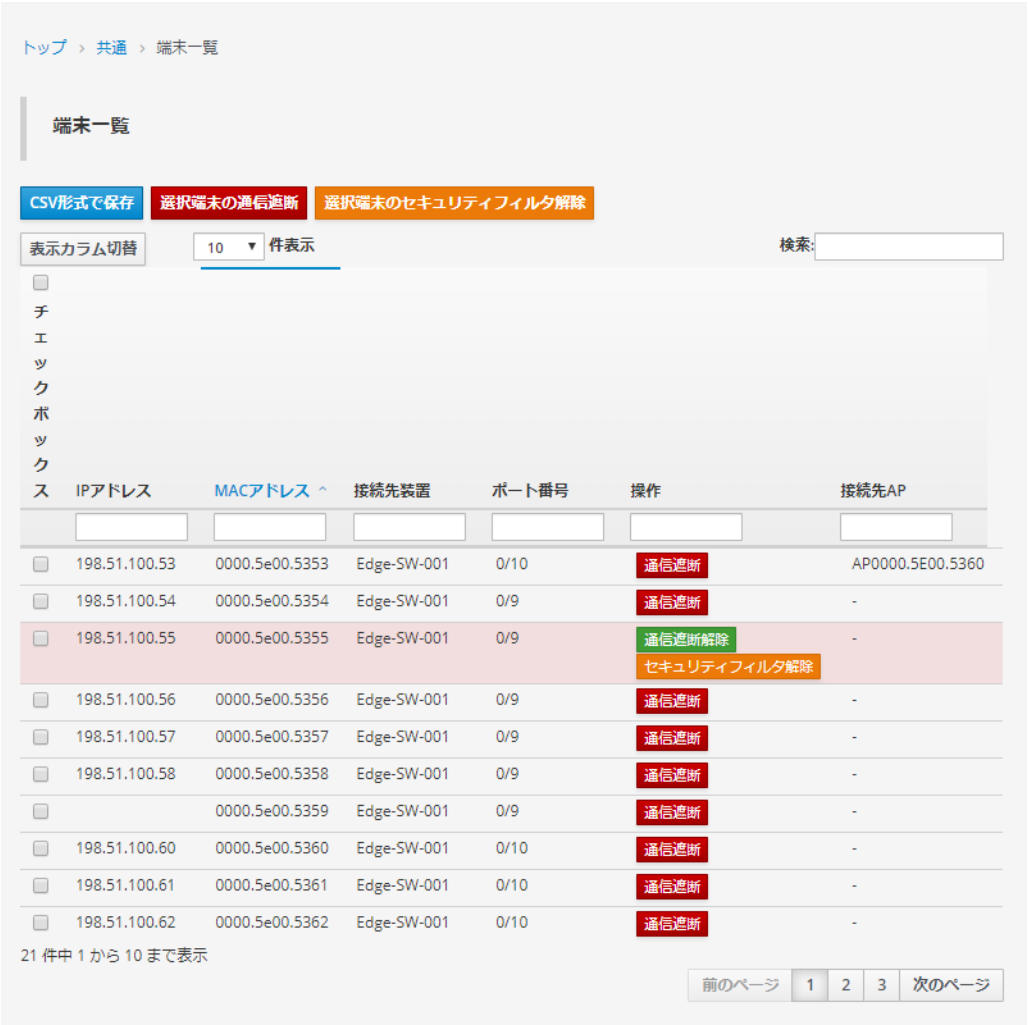

図 2-13　端末管理の画面イメージ

(e) CSV ファイル出力/入力

Web インタフェースで表示したエントリ一覧を CSV ファイル形式でダウンロードしたり，ダウンロードした CSV ファイルからエントリを複数同時に追加することが可能です。AX-Security-Controller(Manager)が CSV ファイルで出力/入力可能な機能一覧は，以下となります。

表 2-16　CSV ファイルで出力/入力可能な機能

機能	CSV ファイル形式でのダウンロード	CSV ファイルからの複数追加
端末一覧	○	×
エイリアス一覧	○	○
装置一覧	○	○
接続情報設定一覧	○	○
ポートエイリアス一覧	○	○
管理対象外ポート一覧	○	○
セグメント一覧	○	○
セキュリティフィルタ一覧	○	○

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

機能	CSV ファイル形式でのダウンロード	CSV ファイルからの複数追加
セキュリティフィルタ履歴	○	×
ルールマッチ履歴	○	×
Syslog 受信履歴	○	×
Syslog クライアント一覧	○	○
ルール一覧	○	○
マップ一覧	○	○
マップ(アイコン配置)	○	○
Syslog サーバ一覧	○	○
E-mail サーバ一覧	○	○

○：可能 ×：不可能

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(f) REST API

ネットワーク管理者が,REST API を通して AX-Security-Controller の参照、設定をすることができます。AX-Security-Controller(Manager)から REST API でアクセス可能な機能一覧は，以下となります。各 API の詳細が必要な場合は，弊社担当営業に問い合わせください。

表 2-17　REST API でアクセス可能な機能

機能	GET	POST	DELETE
端末	端末一覧取得	－	－
エイリアス	エイリアス一覧取得 エイリアス取得	エイリアス追加 エイリアス編集	エイリアス削除
ポートエイリアス	ポートエイリアス一覧取得 ポートエイリアス取得	ポートエイリアス追加 ポートエイリアス編集	ポートエイリアス削除
装置	装置一覧取得 装置取得	装置追加 装置編集	装置削除
セキュリティフィルタ	セキュリティフィルタ一覧取得 セキュリティフィルタ取得	セキュリティフィルタ追加	セキュリティフィルタ削除
Syslog クライアント	Syslog クライアント一覧取得	Syslog クライアント追加	Syslog クライアント削除
Syslog クライアントルール	Syslog クライアントルール一覧取得	Syslog クライアントルール追加	Syslog クライアントルール削除
Syslog 受信履歴	－	Syslog 受信履歴削除	－
共通設定	共通設定一覧取得	WAN 接続ポート追加 永続設定ポート(受信側)追加 永続設定ポート(送信側)追加 Syslog 連携(CEF)のミラー先ポート追加	WAN 接続ポート削除 永続設定ポート(受信側)削除 永続設定ポート(送信側)削除 Syslog 連携(CEF)のミラー先ポート削除
ライセンス	ライセンス一覧取得	－	－

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(6) セキュリティレポート

AX-Security-Controller は，インシデント情報連携，およびセキュリティフィルタ情報をセキュリティレポートとして出力することが可能です。セキュリティレポートは，E-mail での通知や，Web インタフェースにより確認することができます。出力するセキュリティレポートの収集契機，および内容を下記に示します。

表 2-18　セキュリティレポートの収集契機

項目	契機
日単位	毎日 0:00 JST
週単位	毎週月曜日 0:00 JST
月単位	毎月 1 日 0:00 JST

表 2-19　セキュリティレポートの出力内容(日単位)

項目	説明
インシデント連携統計 ・　インシデント発生件数	日単位のインシデント発生件数※1 を出力します。
セキュリティフィルタ統計 ・　設定済み件数 ・　登録件数 ・　解除件数	日単位のセキュリティフィルタの設定済み件数/登録件数/解除件数※2 を出力します。
インシデント情報詳細(最新 10 件)	インシデント情報の最新 10 件を出力します。

※1：合計，Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携ごとに出力します。Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携は，ライセンス有効時に出力します。

※2：合計，Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携，TMPM 連携，手動ごとに出力します。Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携，TMPM 連携は，ライセンス有効時に出力します。

表 2-20　セキュリティレポートの出力内容(週単位)

項目	説明
インシデント連携統計 ・　インシデント発生件数	週単位のインシデント発生件数を出力します。
セキュリティフィルタ統計 ・　設定済み件数 ・　登録件数 ・　解除件数	週単位のセキュリティフィルタの設定済み件数/登録件数/解除件数※2 を出力します。
インシデント連携統計情報内訳(日単位) ・　発生件数	日単位のインシデント発生件数を出力します。
セキュリティフィルタ統計情報内訳(日単位) ・　設定済み件数 ・　登録件数 ・　解除件数	日単位のセキュリティフィルタの設定済み件数/登録件数/解除件数※2 を出力します。

※1：合計，Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携ごとに出力します。Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携は，ライセンス有効時に出力します。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

※2：合計，Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携，TMPM 連携，手動ごとに出力します。Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携，TMPM 連携は，ライセンス有効時に出力します。

表 2-21　セキュリティレポートの出力内容(月単位)

項目	説明
インシデント連携統計 ・　インシデント発生件数	月単位のインシデント発生件数※1 を出力します。
セキュリティフィルタ統計 ・　設定済み件数 ・　登録件数 ・　解除件数	月単位のセキュリティフィルタの設定済み件数/登録件数/解除件数※2 を出力します。
インシデント連携統計情報内訳(週単位) ・　発生件数	週単位のインシデント発生件数※1 を出力します。
セキュリティフィルタ統計情報内訳(週単位) ・　設定済み件数 ・　登録件数 ・　解除件数	週単位のセキュリティフィルタの設定済み件数/登録件数/解除件数※2 を出力します。
インシデント連携統計情報内訳(日単位) ・　発生件数	日単位のインシデント発生件数※1 を出力します。
セキュリティフィルタ統計情報内訳(日単位) ・　設定済み件数 ・　登録件数 ・　解除件数	日単位のセキュリティフィルタの設定済み件数/登録件数/解除件数※2 を出力します。

※1：合計，Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携ごとに出力します。Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携は，ライセンス有効時に出力します。
※2：合計，Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携，TMPM 連携，手動ごとに出力します。Syslog 連携(CEF)，パロアルトネットワークス 次世代ファイアウォール連携，TMPM 連携は，ライセンス有効時に出力します。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(7) イベント通知インタフェース

AX-Security-Controller(Manager)で発生したイベントをネットワーク管理者に通知します。

(a) 通知先

AX-Security-Controller(Manager)からの通知先は，以下となります。

表 2-22 通知先

通知先	説明
syslog (UDP) ※1	・CEF(Common Event Format)の syslog メッセージ※2
Email※3	・STMP/SMTP STARTTLS/SMTPS ・SMTP 認証は CRAM-MD5, PLAIN, LOGIN の順に，認証を試みます。

※1 準拠規格：RFC5424 Syslog Protocol

※2 AX-Security-Controller は IPv4 アドレスでのみ syslog を送信可能です

※3 準拠規格：RFC5321 Simple Mail Transfer Protocol，RFC3207 SMTP Service Extension for Secure SMTP over Transport Layer Security，RFC8314 Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access

なお，Syslog の宛先 IP アドレス，ポート番号，ファシリティ，イベント種別，Email の To，Cc，Bcc，From は各宛先毎に設定可能です。

(b) Syslog 通知項目一覧

AX-Security-Controller(Manager)が Syslog で通知する項目と契機は，以下となります。Syslog サーバ毎に必要な契機だけ通知することも可能です。

表 2-23 Syslog 通知項目一覧

Syslog 種別	イベント種別	契機	重要度
インシデント情報連携	通信遮断	ルールマッチ時	6
	詳細ミラー		5
	手動選択		4
セキュリティフィルタ関連	登録	セキュリティフィルタ登録時	2
	設定完了	全アクセスリスト設定完了	2
	削除完了	全アクセスリスト削除完了	2
	端末毎設定要因	端末毎アクセスリスト追加前	2
	端末毎設定完了	端末毎アクセスリスト設定完了	2
	端末毎設定失敗	端末毎アクセスリスト設定失敗	4
	端末毎削除要因	端末毎アクセスリスト削除完了	2
端末接続	エイリアス未登録端末※1	エイリアス未登録端末の接続を検出	2
管理対象装置関連	コンフィグ容量監視※2	操作対象装置のコンフィグレーションの空き容量が全容量の 20%未満の場合	4

※1 任意の接続端末の E-mail 通知を通知すると，10 日間，同一 MAC アドレスである当該接続端末の通知を抑止します。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

※2 任意の管理対象装置の Syslog を通知すると，翌日 0:00 まで，当該管理対象装置の通知を抑止します。

(c) Email 通知項目一覧
AX-Security-Controller(Manager)が Email で通知する項目と契機は，以下となります。Email サーバ毎に必要な契機だけ通知することも可能です。

表 2-24　Email 通知項目一覧

Email 種別	イベント種別	契機
インシデント情報連携	通信遮断	ルールマッチ時
	詳細ミラー	
	手動選択	
セキュリティレポート	日間セキュリティレポート	毎日 0:00 JST
	週間セキュリティレポート	毎週月曜日 0:00 JST
	月間セキュリティレポート	毎月 1 日 0:00 JST
ライセンス関連	ライセンス期限アラート	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
	ライセンス失効通知	ライセンス失効時 9:00 JST
端末接続	エイリアス未登録端末※1	エイリアス未登録端末の接続を検出
管理対象装置関連	コンフィグ容量監視※2	操作対象装置のコンフィグレーションの空き容量が全容量の 20%未満の場合

※1 任意の接続端末の E-mail 通知を通知すると，10 日間，同一 MAC アドレスである当該接続端末の通知を抑止します。

※2 任意の管理対象装置の Syslog を通知すると，翌日 0:00 まで，当該管理対象装置の通知を抑止します。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

2.4 AX-Security-Controller(Tracker)

AX-Security-Controller(Tracker)は，AX-Security-Controller(Manager)のトポロジ管理機能で周期収集した情報に基づき，各端末の移動履歴を算出します。算出される情報の詳細を下表に示します。

下記のようなケースでは，新たな移動履歴を作成し，端末単位の通信開始および終了時刻を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，移動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

表 2-25　移動履歴に含まれる情報

	説明
接続開始日時	ARP 情報，NDP 情報,MAC アドレス情報の周期収集にて，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 （接続先装置，VLAN，ポート番号，ポートエイリアス，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，以降の周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）

移動履歴の情報は，ネットワーク管理者向け Web インタフェースを通して表示されます。表示された文字列に対して絞込み表示を行うことで， 特定端末の移動履歴を表示したり，特定位置に存在する端末一覧を表示したり，特定時刻にネットワーク内に存在していた端末一覧を表示したりすることができます。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

2.5 Ver.1.10 での新機能の概要

2.5.1 インシデント情報連携

(1) 任意 CEF フィールド登録のサポート

セキュリティベンダ固有の任意の CEF フィールドを登録できるようにしました。
本機能により，セキュリティベンダ固有の CEF フィールドを使用して，インシデント抽出ルールを記述することが可能になります。

2.5.2 管理機能

(1) CSV 形式ファイルによる装置追加時の機能改善

CSV 形式のファイルを使用して装置を追加する際，更新反映の機能だけでなく，CSV ファイルの内容に置き換えができるように改善しました。
たとえば CSV 形式で保存した装置一覧に設定を戻す場合，Web インタフェースを使用して 1 つずつ管理対象装置の削除と追加をおこなうことなく，1 回の作業でリストアすることが可能になります。

(2) CSV 形式ファイルによるエイリアス追加時の機能改善

CSV 形式のファイルを使用してエイリアスを追加する際，更新反映の機能だけでなく，CSV ファイルの内容に置き換えができるように改善しました。
たとえば CSV 形式で保存したエイリアス一覧に設定を戻す場合，Web インタフェースを使用して 1 つずつエイリアスの削除と追加をおこなうことなく，1 回の作業でリストアすることが可能になります。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

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)
管理対象ワイヤレス LAN コントローラ拡張ライセンス	管理対象ワイヤレスLANコントローラ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)
管理対象ワイヤレス LAN コントローラ拡張ライセンス (初年度ライセンス)	管理対象ワイヤレス LAN コントローラ拡張ライセンス (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)

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

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
インシデント情報連携(セキュリティ装置連携)	インシデント受け付けプロトコル	syslog	CEFのsyslogメッセージ	(注 3)
	インシデント抽出	syslogメッセージ抽出		
	Syslogクライアント管理			
	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		(注 4)
		Syslog連携(CEF)		(注 5)
		任意CEFフィールドの登録		
		抽出インシデントのsyslogサーバ通知		
		抽出インシデントのE-mail通知		
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		
		永続設定ポート		
	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		
		IPv6アドレス変更		
	IPv4アドレス・IPv6アドレス連携			
	自動解除スケジュール			(注 6)
	タイマー解除			(注 6)
	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)
セグメンテーションセキュリティ	セグメントごとインシデント情報連携			
	信頼済みセグメント			
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			
			管理対象外ポート	
	接続情報設定			
	LLDP情報収集	axslldp		
		LLDP-MIB		
		LLDP-V2-MIB		
	アクセスリスト拡張ポート設定			
	マップ			
管理機能	管理者機能	ダッシュボード		
		装置管理		
			設定支援による登録	
			事前設定確認支援	
		端末管理		
		端末移動履歴		
		セキュリティフィルタ管理	フィルタ表示	
			Syslogクライアント表示	
			インシデント抽出ルール表示	
			履歴管理	
		セグメント管理		
		マップ管理		
		ライセンス管理	アラートE-mail通知	
	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		

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

分類	機能			備考
		テクニカルサポート情報採取		
		レポート	ダウンロード	
			E-mail通知	
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			
	管理対象ワイヤレスLANコントローラ1台まで ・初年度ライセンス			
	管理対象ワイヤレスLANコントローラ1台まで ・1年延長ライセンス			
	外部連携: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			
	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 ・初年度ライセンス			
	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 ・1 年延長ライセンス			
	外部連携:Syslog 連携(CEF) ・初年度ライセンス			
	外部連携:Syslog 連携(CEF) ・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。

(注 3) 準拠規格:RFC5424 Syslog Protocol

(注 4) 使用には,ライセンス 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(初年度ライセンス,1 年延長ライセンス)が必要です。

(注 5) 使用には,ライセンス 外部連携:Syslog 連携(CEF)(初年度ライセンス,1 年延長ライセンス)が必要です。また, 有効な外部連携:Syslog 連携(CEF)ライセンス 1 つごとに 1 つのベンダ名称が登録可能です。

(注 6) インシデント情報連携により生成したセキュリティフィルタが対象です。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

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 Xeon プロセッサー・ファミリー コア数 16 以上
メモリ	4GB	16GB 以上
ハードディスクの空き容量	20GB 以上+マップでの必要分※	
イーサネットインタフェース	1 つ	

※マップの必要容量は，ユーザーズガイド 操作編を参照ください。

表 5-2 動作スペック(端末移動履歴機能利用時)

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 Xeon プロセッサー・ファミリー コア数 16 以上
メモリ	8GB	32GB 以上
ハードディスクの空き容量	20GB＋端末移動履歴での必要分※	
イーサネットインタフェース	1 つ	

※端末移動履歴の容量は，1 エントリあたり 1024byte として，必要な容量を確保してください。

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)
64bit 版を利用ください。

表 5-3 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	
2	Microsoft Windows Server 2016	
3	CentOS 7	
4	CentOS 8	
5	Red Hat Enterprise Linux 7	

(2) 動作可能 Python バージョン

表 5-4 動作可能 Python バージョン

#	Python	備考
1	Python 3.5 以降 (3.5, 3.6, 3.7, 3.8 のいずれか)	

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

[入手方法]

Microsoft Windows 10 / Microsoft Windows Server 2016:	https://www.python.org/downloads/ より入手してください。
CentOS 7 / CentOS 8 / Red Hat Enterprise Linux 7:	yum により入手してください。

(3) 追加 Python ライブラリ

表 5-5 追加 Python ライブラリ

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

[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 5-6 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 68 ESR	
2	Google Chrome (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 5-7 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	

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

表 5-8 AX-Security-Controller(Tracker)動作可能ウェブブラウザ

#	ウェブブラウザ名	備考
1	Firefox 68 ESR	
2	Google Chrome (最新版)	

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

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 5-9 サポート装置一覧

分類	装置名
セキュリティフィルタの機能が動作可能な弊社装置	AX260A AX2100S AX2200S AX2500S AX3640S AX3650S AX3660S AX3800S AX4600S AX8300S AX8600S AXprimoM210 AX620R
標準 MIB 対応装置	AX8600R AX1230S AX1240S AX1250S AX2400S AX6300S AX6600S AX6700S 弊社製品の他、他社製品にも対応
標準MIB対応装置(VLAN毎コミュニティ)	Cisco スイッチ
ワイヤレス LAN コントローラ	Aruba ・ MIB: wlsxUserAllInfoGroup/wlsxWlanAccessPointInfoGroup オブジェクト収集可能装置 Cisco ・ MIB: bsnEss/bsnAP オブジェクト収集可能装置 Fortinet ・ MIB: mwConfigAp/mwConfigStation オブジェクト収集可能装置

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

標準 MIB 対応装置がそれぞれの情報を収集するための要件を下表に示します。

表 5-10 標準 MIB 対応装置の要件

収集対象※1	収集手段
装置情報(必須)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記 MIB オブジェクトの取得をサポートしていること。 ・sysDescr ・sysName
ARP 情報(オプション)	RFC4293(Management Information Base for the Internet Protocol (IP)) の下記 MIB オブジェクトの取得をサポートしていること。 ・ipNetToMediaPhysAddress または，RFC1213(Management Information Base for Network Management of TCP/IP-based internets) または RFC4293 (Management Information Base for the Internet Protocol (IP)の下記 MIB オブジェクトをサポートしていること。・ipNetToPhysicalPhysAddress
NDP 情報※2(オプション)	RFC2465(Management Information Base for IP Version 6:Textual Conventions and General Group)の下記 MIB オブジェクトの取得をサポートしていること。 ・ipv6NetToMediaPhysAddress または，RFC1213(Management Information Base for Network Management of TCP/IP-based internets) または RFC4293 (Management Information Base for the Internet Protocol (IP)の下記 MIB オブジェクトをサポートしていること。 ・ipNetToPhysicalPhysAddress※3
MAC アドレス情報(オプション)	RFC2674 (Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions)および RFC4363(Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions)の下記 MIB オブジェクトの取得をサポートしていること。 ・dot1qTpFdbPort または，RFC1493(Definitions of Managed Objects for Bridges)および RFC4188(Definitions of Managed Objects for Bridges)の下記 MIB オブジェクトの取得をサポートしていること。 ・dot1dTpFdbPort

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

収集対象※1	収集手段
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 ・lldpRemChassisIdSubtype ・lldpRemChassisId ・lldpRemPortDesc ・lldpLocChassisIdSubtype ・lldpLocChassisId ・lldpLocPortDesc IEEE Std 802.1AB-2009 LLDP-V2-MIB ・lldpV2RemChassisIdSubtype ・lldpV2RemChassisId ・lldpV2RemPortDesc ・lldpV2LocChassisIdSubtype ・lldpV2LocChassisId 弊社製品の axslldp ・axslldpRemRemoteChassis ・axslldpRemPortDesc ・axslldpLocChassisId

※1:AX-Security-Controller が管理対象装置から収集する情報(ARP 情報, NDP 情報, MAC アドレス情報)は, 装置毎, 情報毎に収集するか否か, 選択することができます。ただし, 装置情報は必須で収集できる必要があります。

※2:IPv6 リンクローカルアドレスは収集対象外です。

※3:NDP の収集に ipNetToPhysicalPhysAddress MIB を使用する場合は ARP の収集も ipNetToPhysicalPhysAddress MIB で収集する必要があります。

標準 MIB 対応装置(VLAN 毎コミュニティ)がそれぞれの情報を収集するための要件を下表に示します。

表 5-11 標準 MIB 対応装置(VLAN 毎コミュニティ)の要件

収集対象※1	収集手段
装置情報(必須)	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記 MIB オブジェクトの取得をサポートしていること。 ・sysDescr ・sysName
ARP 情報(オプション)	RFC4293(Management Information Base for the Internet Protocol (IP)) の下記 MIB オブジェクトの取得をサポートしていること。 ・ipNetToMediaPhysAddress または, RFC1213(Management Information Base for Network Management of TCP/IP-based internets) または RFC4293 (Management Information Base for the Internet Protocol (IP)の下記 MIB オブジェクトをサポートしていること。・ipNetToPhysicalPhysAddress

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

収集対象※1	収集手段
NDP 情報※2(オプション)	RFC2465(Management Information Base for IP Version 6:Textual Conventions and General Group)の下記 MIB オブジェクトの取得をサポートしていること。 ・ipv6NetToMediaPhysAddress または，RFC1213(Management Information Base for Network Management of TCP/IP-based internets) または RFC4293（Management Information Base for the Internet Protocol (IP)の下記 MIB オブジェクトをサポートしていること。 ・ipNetToPhysicalPhysAddress※3
MAC アドレス情報(オプション)	RFC1493(Definitions of Managed Objects for Bridges)および RFC4188(Definitions of Managed Objects for Bridges)の下記 MIB 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 ・lldpRemChassisIdSubtype ・lldpRemChassisId ・lldpRemPortDesc ・lldpLocChassisIdSubtype ・lldpLocChassisId ・lldpLocPortDesc IEEE Std 802.1AB-2009 LLDP-V2-MIB ・lldpV2RemChassisIdSubtype ・lldpV2RemChassisId ・lldpV2RemPortDesc ・lldpV2LocChassisIdSubtype ・lldpV2LocChassisId

※1：AX-Security-Controller が管理対象装置から収集する情報(ARP 情報，NDP 情報，MAC アドレス情報)は，装置毎，情報毎に収集するか否か，選択することができます。ただし，装置情報は必須で収集できる必要があります。

※2：IPv6 リンクローカルアドレスは収集対象外です。

※3：NDP の収集に ipNetToPhysicalPhysAddress MIB を使用する場合は ARP の収集も ipNetToPhysicalPhysAddress MIB で収集する必要があります。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

ワイヤレス LAN コントローラが情報を収集するための要件を下表に示します。

表 5-12 ワイヤレス LAN コントローラ(Aruba-1)の要件

収集対象※1	収集手段
装置情報（必須）	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記 MIB 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（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

※1：AX-Security-Controller が管理対象装置から収集する情報(WLC 情報)は，装置毎，および情報毎に収集するか否か，選択することができます。ただし，装置情報は必須で収取できる必要があります。

表 5-13 ワイヤレス LAN コントローラ(Cisco-1)の要件

収集対象※1	収集手段
装置情報（必須）	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記 MIB 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（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

※1：AX-Security-Controller が管理対象装置から収集する情報(WLC 情報)は，装置毎，および情報毎に収集するか否か，選択することができます。ただし，装置情報は必須で収取できる必要があります。

表 5-14 ワイヤレス LAN コントローラ(Fortinet-1)の要件

収集対象※1	収集手段
装置情報（必須）	RFC1213(Management Information Base for Network Management of TCP/IP-based internets)の下記 MIB 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（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

※1：AX-Security-Controller が管理対象装置から収集する情報(WLC 情報)は，装置毎，および情報毎に収集するか否か，選択することができます。ただし，装置情報は必須で収集できる必要があります。

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

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

管理対象装置側 OS のバージョンにより,動作可能な機能が異なります。動作するセキュリティフィルタ機能(セキュリティ装置連携)を以下に示します。

なお標準 MIB 対応装置は, MAC アドレス情報や ARP 情報や NDP 情報の収集のみを行うだけであり, セキュリティフィルタの機能は動作しません。

(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)
		永続設定ポート	
	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	
		IPv6 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	
		永続設定ポート	
	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	
		IPv6 アドレス変更	

装置の対応バージョン：12.7.B～

(3) AX4600S

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	
		永続設定ポート	
	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	
		IPv6 アドレス変更	

装置の対応バージョン：11.14.D～

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(4) AX3800S

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	
		永続設定ポート	
	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	
		IPv6 アドレス変更	

装置の対応バージョン：11.14.L～

(5) 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	
		永続設定ポート	
	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	
		IPv6 アドレス変更	

装置の対応バージョン：12.1～

(6) AX3650S

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	
		永続設定ポート	
	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	
		IPv6 アドレス変更	

装置の対応バージョン：11.14.L～

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(7) AX3640S

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	
		永続設定ポート	
	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	
		IPv6 アドレス変更	

装置の対応バージョン：11.14.F～

(8) 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)
		永続設定ポート	
	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	
		IPv6 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～

(9) AX2200S

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)
		永続設定ポート	
	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：2.5.B～

(10)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)
		永続設定ポート	
	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～

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

(11)AXprimoM210

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)
		永続設定ポート(受信側)	
	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	
		IPv6 アドレス変更※	

装置の対応バージョン：1.2.2.22～
※：1.2.2.23～

(12)AX620R

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	
		永続設定ポート	
	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	
		IPv6 アドレス変更	

装置の対応バージョン:10.0.15～
9.7.55～

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

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-P1560-F4	OP-WC1	管理対象ワイヤレス LAN コントローラ 1 台まで ・初年度ライセンス
10	AX-P1560-F4E1	OP-WC1	管理対象ワイヤレス LAN コントローラ 1 台まで ・1 年延長ライセンス
11	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
12	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
13	AX-P1570-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 ・初年度ライセンス
14	AX-P1570-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
15	AX-P1570-F3	OP-CEF	外部連携ライセンス:Syslog 連携(CEF) ・初年度ライセンス
16	AX-P1570-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

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

【著作権】
All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.

【発行】
2017 年　6 月　（Ver.1.0　第 1 版）
2017 年　8 月　（Ver.1.0　第 2 版）
2017 年　10 月　（Ver.1.1　第 3 版）
2018 年　1 月　（Ver.1.2　第 4 版）
2018 年　4 月　（Ver.1.3　第 5 版）
2018 年　7 月　（Ver.1.4　第 6 版）
2018 年　10 月　（Ver.1.5　第 7 版）
2018 年　12 月　（Ver.1.6　第 8 版）
2019 年　3 月　（Ver.1.7　第 9 版）
2019 年　7 月　（Ver.1.8　第 10 版）
2019 年　10 月　（Ver.1.9　第 11 版）
2020 年　1 月　（Ver.1.10　第 12 版）
2020 年　4 月　（Ver.1.10　第 13 版）

・TREND MICRO,Trend Micro Policy Manager,Deep Discovery Inspector は,トレンドマイクロ株式会社の登録商標です。
・Palo Alto Networks, PAN-OS, Palo Alto Networks ロゴは米国と司法管轄権を持つ各国での Palo Alto Networks, Inc.の商標です。
・Fortinet®,FortiGate®は, Fortinet, Inc.の登録商標です。
・FireEye は,FireEye, Inc.の登録商標です。
・Microsoft,Windows,Windows Server またはその他のマイクロソフト製品の名称および製品名は,米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
・CentOS の名称およびそのロゴは,Red Hat, Inc.の商標または登録商標です。
・Linux は,Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。
・Red Hat,Red Hat Enterprise Linux は米国およびその他の国において Red Hat, Inc.の登録商標または商標です。
・Firefox は,Mozilla Foundation の登録商標です。
・Google Chrome は,Google Inc.の登録商標です。
・Intel Core,Xeon は,アメリカ合衆国およびその他の国における Intel Corporation またはその子会社の商標です。
・Cisco は, Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商標または商標です。
・本データシートの会社名/製品名/各社固有の機能名は商標もしくは,登録商標です。
・製品の概観,仕様は予告なく変更することがあります。
・記載されている形名の製品は日本国内での利用を前提としており,日本国内専用となっております。海外向け形名の有無については,販売店にお問い合わせください。本製品を輸出される場合には,外国為替及び外国貿易法の規制並びに米国輸出管理規制など外国の輸出関連法規をご確認の上,必要な手続きをおとりください。なお,不明な場合は,弊社担当営業にお問い合わせください。

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

All Rights Reserved, Copyright (C), 2017, 2020, ALAXALA Networks, Corp.