

# AX-Security-Controller ユーザーズガイド 操作編

SOFT-AM-2238\_R14

**AjaxalA**

## ■対象製品

このマニュアルは、 AX-Security-Controller Version 1.11 の操作方法について記載しています。

## ■輸出時の注意

本製品を輸出される場合には、 外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ、 必要な手続きをお取りください。

なお、 不明な場合は、 弊社担当営業にお問い合わせください。

## ■商標一覧

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。

Microsoft, Windows, Windows Server は、 米国およびその他の国における米国 Microsoft Corp.の登録商標です。

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。

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。

そのほかの記載の会社名、 製品名は、 それぞれの会社の商標あるいは登録商標です。

## ■マニュアルはよく読み、 保管してください。

製品を使用する前に、 安全上の説明をよく読み、 十分理解してください。

このマニュアルは、 いつでも参照できるよう、 手近な所に保管してください。

## ■ご注意

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

## ■発行

2020年 9月 (第15版) S O F T - A M - 2 2 3 8 \_ R 1 4

## ■著作権

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

## 変更内容

表 第 15 版の変更内容

章・節・項・タイトル	追加・変更内容
1.4.3(3) アイコン画像の変更	<ul style="list-style-type: none"><li>マップのアイコン画像の変更の記述を追加しました。</li></ul>
2.1.6 マップ	<ul style="list-style-type: none"><li>アイコン画像ファイル登録数、アイコン画像ファイルサイズの記述を追加しました。</li></ul>
6.1.1 ナビゲーションバー	<ul style="list-style-type: none"><li>マップ設定、および画像管理の記述を追加しました。</li></ul>
6.1.7(1) マップ一覧	<ul style="list-style-type: none"><li>マップ情報に背景画像ファイル名を追加しました。</li></ul>
6.1.7(2) マップ設定	<ul style="list-style-type: none"><li>本項を追加しました。</li></ul>
6.1.8(3) 画像管理	<ul style="list-style-type: none"><li>本項を追加しました。</li></ul>
9.2.5 マップ	<ul style="list-style-type: none"><li>ZIP 形式からの一括背景画像・画像追加で画像が登録されない場合の対応方法を記載しました。</li></ul>

なお、単なる誤字・脱字などはお断りなく訂正しました。

表 第 14 版の変更内容

章・節・項・タイトル	追加・変更内容
使用可能ウェブブラウザ	<ul style="list-style-type: none"><li>Firefox 78 ESR の記述を追加しました。</li></ul>
AX-Security-Controller(Manager)起動方法	<ul style="list-style-type: none"><li>Microsoft Windows Server 2019、Red Hat Enterprise Linux 8 の追加に伴い、記述を追加しました。</li></ul>
AX-Security-Controller(Manager)停止方法	<ul style="list-style-type: none"><li>Microsoft Windows Server 2019、Red Hat Enterprise Linux 8 の追加に伴い、記述を追加しました。</li></ul>

表 第 13 版の変更内容

章・節・項・タイトル	追加・変更内容
AX-Security-Controller(Manager)起動方法	<ul style="list-style-type: none"><li>CentOS 8 の追加に伴い、記述を追加しました。</li></ul>
AX-Security-Controller(Manager)停止方法	<ul style="list-style-type: none"><li>CentOS 8 の追加に伴い、記述を追加しました。</li></ul>

表 第 12 版の変更内容

章・節・項・タイトル	追加・変更内容
インシデント抽出ルール	<ul style="list-style-type: none"><li>ユーザ定義拡張フィールドの記述を追加しました。</li></ul>
インシデント抽出ルール	<ul style="list-style-type: none"><li>ユーザ定義拡張フィールド数の記述を追加しました。</li></ul>
使用可能ウェブブラウザ	<ul style="list-style-type: none"><li>Firefox 60 ESR の記述を削除しました。</li></ul>
端末	<ul style="list-style-type: none"><li>エイリアスに、CSV 形式からのエイリアス追加の記述を追加しました。</li></ul>
装置	<ul style="list-style-type: none"><li>装置一覧に、CSV 形式からの装置追加の記述を追加しました。</li></ul>

章・節・項・タイトル	追加・変更内容
セキュリティ装置連携	<ul style="list-style-type: none"> <li>Syslog クライアント詳細に、ユーザ定義拡張フィールド追加の記述を追加しました。</li> </ul>
マップ	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>

表 第 11 版の変更内容

章・節・項・タイトル	追加・変更内容
ネットワーク構成	<ul style="list-style-type: none"> <li>ワイヤレス LAN コントローラの条件の記述を追加しました。</li> </ul>
Syslog 通知	<ul style="list-style-type: none"> <li>管理対象装置関連に関する記述を追加しました。</li> </ul>
E-mail 通知	<ul style="list-style-type: none"> <li>管理対象装置関連に関する記述を追加しました。</li> </ul>
使用可能なブラウザ	<ul style="list-style-type: none"> <li>Firefox 68 ESR の記述を追加しました。</li> </ul>
装置	<ul style="list-style-type: none"> <li>装置一覧、および装置詳細の状態に OID not increasing の記述を追加しました。</li> <li>装置一覧、および装置詳細に、コンフィグ空き容量に関する記述を追加しました。</li> <li>装置追加、装置編集、および装置検索一覧の MIB オブジェクト(WLC) に、Fortinet-1-mwConfigAp/mwConfigStation の記述を追加しました。</li> <li>装置詳細に、LLDP シャーシ ID の記述を追加しました。</li> </ul>
管理	<ul style="list-style-type: none"> <li>共通設定に、装置情報収集に関する記述を追加しました。</li> <li>通知設定に、管理対象装置関連に関する記述を追加しました。</li> </ul>
トポロジ管理	<ul style="list-style-type: none"> <li>管理対象装置からの MIB 収集において、OID not increasing エラーが発生する場合の対応方法を記載しました。</li> </ul>

表 第 10 版の変更内容

章・節・項・タイトル	追加・変更内容
ネットワーク構成	<ul style="list-style-type: none"> <li>ワイヤレス LAN コントローラの条件の記述を追加しました。</li> <li>接続情報設定を設定するケースの記述を変更しました。</li> <li>アクセリスト拡張ポートの記述を変更しました。</li> </ul>
管理対象ネットワーク	管理対象外ポートの記述を追加しました。
Syslog	受信 Syslog 保持数の記述を追加しました。
SSH	設定対象外装置の記述を変更しました。
LLDP	設定対象外装置の記述を変更しました。
アクセリスト	<ul style="list-style-type: none"> <li>AX620R の記述を追加しました。</li> <li>設定対象外装置の記述を変更しました。</li> </ul>
AX620R	本項を追加しました。

章・節・項・タイトル	追加・変更内容
AX-Security-Controller(Manager)の起動 パラメータ	<ul style="list-style-type: none"> <li>収集周期のパラメータの記述を追加しました。</li> </ul>
装置	<ul style="list-style-type: none"> <li>事前コンフィグ設定確認結果一括出力に関する記述を追加しました。</li> <li>AX620R、およびワイヤレス LAN コントローラのサポートに伴い、記述を追加しました。</li> <li>事前コンフィグ設定確認結果に関する記述を追加しました。</li> <li>管理対象外ポートに関する記述を追加しました。</li> </ul>
管理	<ul style="list-style-type: none"> <li>ライセンスに関する記述を追加しました。</li> </ul>
セキュリティフィルタ	<ul style="list-style-type: none"> <li>アクセリストの追加と削除が繰り返される場合の対応方法を記載しました。</li> </ul>

表 第9版の変更内容

章・節・項・タイトル	追加・変更内容
ネットワーク構成	<ul style="list-style-type: none"> <li>標準 MIB 対応装置の条件、標準 MIB 対応装置(VLAN 每コミュニティ)の条件に、LLDP 情報収集の記載を追加しました。</li> <li>接続情報設定を設定するケースの記述を変更しました。</li> </ul>
エイリアス機能	<ul style="list-style-type: none"> <li>タイトルと値の組み合わせの複数登録の記述を追加しました。</li> </ul>
概要	<ul style="list-style-type: none"> <li>端末移動追従で、エイリアス未登録端末の通信遮断に関する記述を追加しました。</li> </ul>
セキュリティフィルタの生成・削除契機	<ul style="list-style-type: none"> <li>タイマー解除に関する記述を追加しました。</li> </ul>
セキュリティフィルタの種別	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
Syslog 通知	<ul style="list-style-type: none"> <li>端末接続に関する記述を追加しました。</li> </ul>
E-mail 通知	<ul style="list-style-type: none"> <li>端末接続に関する記述を追加しました。</li> </ul>
端末移動履歴	<ul style="list-style-type: none"> <li>エイリアス使用時の消費に関する記述を追加しました。</li> </ul>
エイリアス	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
LLDP	<ul style="list-style-type: none"> <li>設定対象外装置の記述を変更しました。</li> </ul>
アクセリスト	<ul style="list-style-type: none"> <li>AXprimoM210 について、通常モードの IPv6 アクセスリスト名称の記述を追加しました。</li> </ul>
AX8600S・AX8300S	<ul style="list-style-type: none"> <li>「LLDP(IEEE Std.802.1AB-2009)アクセス拒否 MAC フィルタ」の記述を削除しました。</li> </ul>
装置	<ul style="list-style-type: none"> <li>装置検索一覧、ユーザ名/パスワード認証確認に関する記述を追加しました。</li> <li>接続情報検索結果に関する記述を追加しました。</li> </ul>
セキュリティ装置連携	<ul style="list-style-type: none"> <li>ルール追加に、通信遮断(タイマー解除)、詳細ミラー(タイマー解除)、およびなしに関する記述を追加しました。</li> </ul>

章・節・項・タイトル	追加・変更内容
管理	<ul style="list-style-type: none"> <li>共通に、エイリアス未登録端末に関する記述を追加しました。</li> </ul>
Web インタフェースへのアクセス	<ul style="list-style-type: none"> <li>履歴情報が大きくなつたことにより、Web インタフェースでアクセスできない場合の対応方法を記載しました。</li> </ul>
トポロジ管理	<ul style="list-style-type: none"> <li>管理対象装置で LLDP が動作していない、または管理対象装置間の接続情報設定が未設定だったことにより、端末一覧に端末が表示されない場合の対応方法を記載しました。</li> </ul>

表 第8版の変更内容

章・節・項・タイトル	追加・変更内容
ネットワーク構成	<ul style="list-style-type: none"> <li>標準 MIB 対応装置(VLAN 毎コミュニティ)のサポートに伴い、記述を追加しました。</li> </ul>
E-mail 通知	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
レポート	<ul style="list-style-type: none"> <li>本節を追加しました。</li> </ul>
端末移動履歴	<ul style="list-style-type: none"> <li>履歴保存期間を更新しました。</li> </ul>
E-mail	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
使用可能ウェブブラウザ	<ul style="list-style-type: none"> <li>ブラウザの削除に伴い、記述を変更しました。</li> </ul>
AXprimoM210	<ul style="list-style-type: none"> <li>記述を変更しました。</li> </ul>
AX-Security-Controller(Tracker)の起動パラメータ	<ul style="list-style-type: none"> <li>履歴保持日数のパラメータの記述を追加しました。</li> </ul>
端末	<ul style="list-style-type: none"> <li>端末一覧に、選択端末の通信遮断と選択端末のセキュリティフィルタ削除の記述を追加しました。</li> </ul>
装置	<ul style="list-style-type: none"> <li>標準 MIB 対応装置(VLAN 毎コミュニティ)のサポートに伴い、記述を追加しました。</li> </ul>
セキュリティ装置連携	<ul style="list-style-type: none"> <li>セキュリティフィルター一覧に、選択セキュリティフィルタの削除の記述を追加しました。</li> </ul>
マップ	<ul style="list-style-type: none"> <li>集線装置表示と端末配置固定の記述を追加しました。</li> </ul>
管理	<ul style="list-style-type: none"> <li>通知設定に、E-mail 通知の記述を追加しました。</li> <li>レポートの記述を追加しました。</li> </ul>
セキュリティ装置連携	<ul style="list-style-type: none"> <li>セキュリティフィルター一覧に、選択セキュリティフィルタの削除の記述を追加しました。</li> </ul>
セキュリティ装置連携	<ul style="list-style-type: none"> <li>セキュリティフィルター一覧に、選択セキュリティフィルタの削除の記述を追加しました。</li> </ul>
E-mail 通知	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>

表 第7版の変更内容

章・節・項・タイトル	追加・変更内容
マップ	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
概要	<ul style="list-style-type: none"> <li>通信遮断、および詳細ミラーで、追加で指定可能なフィールドを追加しました。</li> </ul>

章・節・項・タイトル	追加・変更内容
セグメンテーションセキュリティ	<ul style="list-style-type: none"> <li>本節を追加しました。</li> </ul>
Syslog 通知	<ul style="list-style-type: none"> <li>セキュリティフィルタ関連のメッセージフォーマットについて、記述を追加しました。</li> </ul>
管理対象ネットワーク	<ul style="list-style-type: none"> <li>WAN 接続ポート数を更新しました。</li> <li>永続設定ポート(受信側)数を更新しました。</li> <li>永続設定ポート(送信側)数を更新しました。</li> </ul>
セグメント	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
マップ	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
使用可能なブラウザ	<ul style="list-style-type: none"> <li>ブラウザの追加に伴い、記述を追加しました。</li> </ul>
アクセリスト	<ul style="list-style-type: none"> <li>AXprimoM210 の記述を追加しました。</li> </ul>
AXprimoM210	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
管理対象装置個別の注意事項	<ul style="list-style-type: none"> <li>本節を追加しました。</li> </ul>
セグメンテーションセキュリティの設定	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
マップの設定	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
端末	<ul style="list-style-type: none"> <li>端末一覧に、操作とマップの記述を追加しました。</li> </ul>
装置	<ul style="list-style-type: none"> <li>装置一覧に、マップの記述を追加しました。</li> <li>装置詳細に、接続端末一覧の操作とマップの記述を追加しました。</li> </ul>
セグメント	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
セキュリティ装置連携	<ul style="list-style-type: none"> <li>Syslog クライアント詳細のルール追加に、セグメントの記述を追加しました。</li> </ul>
マップ	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
管理	<ul style="list-style-type: none"> <li>共通設定の永続設定ポート(受信側)追加に、セグメントの記述を追加しました。</li> <li>共通設定の永続設定ポート(受信側)追加に、セグメントの記述を追加しました。</li> <li>共通設定のセキュリティフィルタ自動解除スケジュール追加に、セグメントの記述を追加しました。</li> </ul>

表 第6版の変更内容

章・節・項・タイトル	追加・変更内容
エイリアス機能	<ul style="list-style-type: none"> <li>ポートエイリアスサポートに伴い、エイリアスを含めた本項を追加しました。</li> </ul>
インシデント抽出ルール	<ul style="list-style-type: none"> <li>Syslog クライアント種別「パロアルトネットワーク 次世代ファイアウォール連携」の場合に追加で指定可能なフィールドを追加しました。</li> </ul>
セキュリティフィルタの生成・削除契機	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
セキュリティフィルタ使用上の注意事項	<ul style="list-style-type: none"> <li>アクセリストのモードにおける使用上の注意事項と、アクセリスト拡張ポート設定における注意事項を、本項にまとめました。</li> </ul>

章・節・項・タイトル	追加・変更内容
Syslog 通知	<ul style="list-style-type: none"> <li>通知可能な Syslog 種別追加に伴い、記述を追加しました。</li> </ul>
装置	<ul style="list-style-type: none"> <li>ポートエイリアスの記述を追加しました。</li> </ul>
セキュリティ装置連携	<ul style="list-style-type: none"> <li>Syslog クライアントのクライアント種別「パロアルトネットワークス 次世代ファイアウォール」の場合に自動で設定するルールの記述を追加しました。</li> </ul>
管理	<ul style="list-style-type: none"> <li>セキュリティフィルタ自動解除スケジュールのサポートに伴い、記述を追加しました。</li> <li>通知可能な Syslog 種別追加に伴い、記述を追加しました。</li> </ul>

表 第 5 版の変更内容

章・節・項・タイトル	追加・変更内容
セキュリティ装置	<ul style="list-style-type: none"> <li>Syslog 連携(CEF)サポートに伴い、記述を追加しました。</li> </ul>
管理対象装置	<ul style="list-style-type: none"> <li>標準 MIB 対応装置の拡張に伴い、記述を変更しました。</li> </ul>
接続情報	<ul style="list-style-type: none"> <li>標準 MIB 対応装置の拡張に伴い、記述を変更しました。</li> </ul>
アクセリスト拡張ポート	<ul style="list-style-type: none"> <li>アクセリスト拡張ポートのサポートに伴い、記述を追加しました。</li> </ul>
永続設定ポート(受信側/送信側)	<ul style="list-style-type: none"> <li>永続設定ポートのサポートに伴い、記述を追加しました。</li> </ul>
対応 Syslog フォーマット	<ul style="list-style-type: none"> <li>Syslog 連携(CEF)サポートに伴い、記述を変更しました。</li> </ul>
インシデント抽出ルール	<ul style="list-style-type: none"> <li>Syslog 連携(CEF)サポートに伴い、記述を変更しました。</li> </ul>
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	<ul style="list-style-type: none"> <li>永続設定ポートのサポートに伴い、記述を追加しました。</li> </ul>
アクセリスト拡張ポート設定における注意事項	<ul style="list-style-type: none"> <li>アクセリスト拡張ポートのサポートに伴い、記述を追加しました。</li> </ul>
管理対象ネットワーク	<ul style="list-style-type: none"> <li>管理対象装置数を更新しました。</li> <li>永続設定ポートのサポートに伴い、記述を追加しました。</li> </ul>
管理対象装置共通の事前準備	<ul style="list-style-type: none"> <li>標準 MIB 対応装置の拡張に伴い、記述を変更しました。</li> </ul>
アクセリスト	<ul style="list-style-type: none"> <li>永続設定ポートのサポートに伴い、記述を追加しました。</li> </ul>
ライセンスの設定	<ul style="list-style-type: none"> <li>Syslog 連携(CEF)サポートに伴い、記述を変更しました。</li> </ul>
管理対象装置の設定	<ul style="list-style-type: none"> <li>標準 MIB 対応装置の拡張に伴い、記述を変更しました。</li> </ul>
接続情報設定の設定	<ul style="list-style-type: none"> <li>アクセリスト拡張ポートのサポートに伴い、記述を変更しました。</li> </ul>

章・節・項・タイトル	追加・変更内容
Syslog 連携(CEF)との連携の設定	・ Syslog 連携(CEF)サポートに伴い、記述を追加しました。
ナビゲーションバー	・ 永続設定ポートのサポート及び Syslog 連携(CEF)サポートに伴い、記述を追加しました。
端末	・ 標準 MIB 対応装置の拡張に伴い、記述を変更しました。
装置	・ 永続設定ポートのサポート、標準 MIB 対応装置の拡張及びアクセリスト拡張ポートのサポートに伴い、記述を変更しました。
セキュリティ装置連携	・ 永続設定ポートのサポート及び Syslog 連携(CEF)サポートに伴い、記述を変更しました。
管理	・ 永続設定ポートのサポート及び Syslog 連携(CEF)サポートに伴い、記述を変更しました。
セキュリティフィルタ	・ 永続設定ポートのサポートに伴い、記述を変更しました。

表 第4版の変更内容

章・節・項・タイトル	追加・変更内容
AX-Security-Controller の構成	・ 端末履歴機能サポートに伴い、記述を追加しました。
ネットワーク構成	・ IPv6 アドレス対応のサポートに伴い、記述を追加しました。
インシデント抽出ルール	・ IPv6 アドレス対応のサポートに伴い、記述を追加しました。
概要	・ IPv6 アドレス対応のサポートに伴い、記述を追加しました。
セキュリティフィルタの動作モード	・ IPv6 アドレス対応のサポートに伴い、記述を追加しました。
アクセスリストのモードにおける使用上の注意事項	・ 本項を追加しました。
通知機能	・ 本節を追加しました。
端末移動履歴機能	・ 本節を追加しました。
Syslog サーバ数	・ 本項を追加しました。
端末移動履歴の 1 エントリあたりの容量	・ 本項を追加しました。
AX-Security-Controller(Tracker)で使用可能なウェブブラウザ	・ 本項を追加しました。
アクセスリスト	・ IPv6 アドレス対応のサポートに伴い、記述を追加しました。
AX8600S・AX8300S	・ IPv6 アドレス対応のサポートに伴い、記述を追加しました。
AX4600S	・ IPv6 アドレス対応のサポートに伴い、記述を追加しました。

章・節・項・タイトル	追加・変更内容
AX3800S	<ul style="list-style-type: none"> <li>IPv6 アドレス対応のサポートに伴い、記述を追加しました。</li> </ul>
AX3660S	<ul style="list-style-type: none"> <li>IPv6 アドレス対応のサポートに伴い、記述を追加しました。</li> </ul>
AX-Security-Controller(Manager)の起動 パラメータ	<ul style="list-style-type: none"> <li>IPv6 アドレス対応のサポートに伴い、記述を追加しました。</li> </ul>
AX-Security-Controller(Tracker)の起動・ 停止方法	<ul style="list-style-type: none"> <li>本節を追加しました。</li> </ul>
AX-Security-Controller(Tracker)へのアkses	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
管理対象装置の設定	<ul style="list-style-type: none"> <li>IPv6 アドレス対応のサポートに伴い、記述を追加しました。</li> </ul>
ナビゲーションバー	<ul style="list-style-type: none"> <li>IPv6 アドレス対応のサポートに伴い、記述を追加しました。</li> </ul>
端末	<ul style="list-style-type: none"> <li>IPv6 アドレス対応のサポートに伴い、記述を追加しました。</li> </ul>
装置	<ul style="list-style-type: none"> <li>IPv6 アドレス対応のサポートに伴い、記述を追加しました。</li> </ul>
セキュリティ装置連携	<ul style="list-style-type: none"> <li>IPv6 アドレス対応のサポートに伴い、記述を追加しました。</li> <li>セキュリティフィルタ履歴削除機能のサポートに伴い、記述を追加しました。</li> <li>ルールマッチ履歴削除機能のサポートに伴い、記述を追加しました。</li> <li>Syslog 受信履歴削除機能のサポートに伴い、記述を追加しました。</li> </ul>
管理	<ul style="list-style-type: none"> <li>Syslog 出力機能のサポートに伴い、記述を追加しました。</li> </ul>
AX-Security-Controller(Tracker)の Web インターフェース	<ul style="list-style-type: none"> <li>本章を追加しました。</li> </ul>

表 第3版の変更内容

章・節・項・タイトル	追加・変更内容
AX-Security-Controller の概要	<ul style="list-style-type: none"> <li>インシデント情報連携サポートに伴い、記述を追加しました。</li> </ul>
ネットワーク構成	<ul style="list-style-type: none"> <li>セキュリティ装置 パロアルトネットワークス 次世代ファイアウォールのサポートに伴い、記述を追加しました。</li> <li>標準 MIB 対応レイヤ 3 装置のサポートに伴い、記述を追加しました。</li> <li>接続情報のサポートに伴い、記述を追加しました。</li> </ul>
インシデント情報連携	<ul style="list-style-type: none"> <li>本節を追加しました。</li> </ul>
Syslog クライアント数	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>
Syslog クライアントごとルール数	<ul style="list-style-type: none"> <li>本項を追加しました。</li> </ul>

章・節・項・タイトル	追加・変更内容
AX4600S	・ 本項を追加しました。
AX3800S	・ 本項を追加しました。
AX3650S	・ 本項を追加しました。
AX2200S	・ 本項を追加しました。
AX-Security-Controller(Manager)の起動 パラメータ	・ Syslog 受信サポートに伴い、記述を追加しました。
接続情報設定の設定	・ 本項を追加しました。
パロアルトネットワークス 次世代 ファイアウォールとの連携の設定	・ 本項を追加しました。
接続情報設定	・ 追加しました。
接続情報追加	・ 追加しました。
ルールマッチ履歴	・ 追加しました。
Syslog 受信履歴	・ 追加しました。
Syslog クライアント一覧	・ 追加しました。
Syslog クライアント詳細	・ 追加しました。
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	・ 本節を追加しました。

表 第2版の変更内容

章・節・項・タイトル	追加・変更内容
AX-Security-Controller(Manager)起動方 法	・ オペレーティングシステムの追加に伴い、記述を追 加しました。
AX-Security-Controller(Manager)停止方 法	・ オペレーティングシステムの追加に伴い、記述を追 加しました。

# はじめに

## ■対象製品・対象ソフト対象製品・対象ソフトウェアおよびソフトウェアバージョン

このマニュアルは、AX-Security-Controller Version 1.11 を対象に記載しています。操作を行う前にこのマニュアルをよく読み、書かれている指示や注意を十分に理解してください。また、このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。

## ■対象読者

本製品を使用したネットワークシステムを構築し、運用するシステム管理者の方を対象としています。また、ネットワークシステム管理の基礎的な知識を理解していることを前提としています。

## ■このマニュアルでの表記

AP	Access Point
ARP	Address Resolution Protocol
Bcc	Blind carbon copy
CAPWAP	Control And Provisioning of Wireless Access Points
CEF	Common Event Format
CSS	Cascading Style Sheets
CSV	Comma-Separated Values
Cc	Carbon copy
DB	database
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
E-mail	Electronic mail
ESR	Extended Support Release
FQDN	Fully Qualified Domain Name
FW	FireWall
GIF	Graphics Interchange Format
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
IP	Internet Protocol
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
NA	Neighbor Advertisement
NDP	Neighbor Discovery Protocol
NS	Neighbor Solicitation
OID	Object Identifier
PNG	Portable Network Graphics
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol over SSL
SNMP	Simple Network Management Protocol
SSH	Secure Shell

SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTM	Unified Threat Management
VLAN	Virtual LAN
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
WAN	Wide Area Network
WLC	Wireless LAN Controller

#### ■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。

<https://www.alaxala.com>

# 目次

---

変更内容 .....	1
はじめに .....	1
目次 .....	1
<b>1. AX-SECURITY-CONTROLLER の概要 .....</b>	<b>1</b>
1.1 AX-Security-Controller の概要 .....	2
1.2 AX-Security-Controller の構成 .....	4
1.3 前提とするネットワークの構成 .....	5
1.3.1 ネットワーク構成 .....	5
1.4 トポロジ管理 .....	13
1.4.1 端末位置 .....	13
1.4.2 エイリアス機能 .....	14
1.4.3 マップ .....	15
1.5 インシデント情報連携 .....	18
1.5.1 概要 .....	18
1.5.2 対応 Syslog フォーマット .....	19
1.5.3 インシデント抽出ルール .....	20
1.6 セキュリティフィルタ (セキュリティ装置との連携) .....	27
1.6.1 概要 .....	27
1.6.2 セキュリティフィルタの生成・削除契機 .....	28
1.6.3 セキュリティフィルタの種別 .....	31
1.6.4 セキュリティフィルタの設定状態 .....	31
1.6.5 セキュリティフィルタの動作モード .....	33
1.6.6 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 .....	35
1.6.7 セキュリティフィルタの使用上の注意事項 .....	36
1.7 セグメンテーションセキュリティ .....	39
1.7.1 概要 .....	39

1.7.2	セグメント .....	40
1.7.3	セグメンテーションセキュリティの動作概要 .....	43
1.7.4	セグメンテーションセキュリティ使用時の注意事項 .....	44
<b>1.8</b>	<b>通知機能 .....</b>	<b>46</b>
1.8.1	Syslog 通知 .....	46
1.8.2	E-mail 通知 .....	59
<b>1.9</b>	<b>レポート .....</b>	<b>71</b>
1.9.1	セキュリティレポート .....	71
<b>1.10</b>	<b>端末移動履歴機能 .....</b>	<b>74</b>
1.10.1	移動履歴 .....	74
<b>1.11</b>	<b>ライセンス .....</b>	<b>75</b>
1.11.1	ライセンスの構成 .....	75
1.11.2	使用期間 .....	75
<b>2.</b>	<b>動作条件 .....</b>	<b>77</b>
<b>2.1</b>	<b>収容条件 .....</b>	<b>78</b>
2.1.1	管理対象ネットワーク .....	78
2.1.2	Syslog .....	78
2.1.3	インシデント抽出ルール .....	79
2.1.4	端末移動履歴 .....	79
2.1.5	セグメント .....	79
2.1.6	マップ .....	80
2.1.7	E-mail .....	80
2.1.8	エイリアス .....	81
<b>2.2</b>	<b>使用可能ウェブブラウザ .....</b>	<b>82</b>
2.2.1	AX-Security-Controller(Manager)で使用可能なウェブブラウザ .....	82
2.2.2	AX-Security-Controller(Viewer)で使用可能なウェブブラウザ .....	82
2.2.3	AX-Security-Controller(Tracker)で使用可能なウェブブラウザ .....	82
<b>3.</b>	<b>管理対象装置の事前準備・設定 .....</b>	<b>83</b>
<b>3.1</b>	<b>概要 .....</b>	<b>84</b>
<b>3.2</b>	<b>管理対象装置共通の事前準備 .....</b>	<b>85</b>

3.2.1	SSH .....	85
3.2.2	SNMP .....	85
3.2.3	LLDP .....	86
3.2.4	アクセスリスト .....	87
<b>3.3</b>	<b>管理対象装置個別の事前準備.....</b>	<b>97</b>
3.3.1	AX260A .....	97
3.3.2	AX8600S・AX8300S.....	97
3.3.3	AX4600S.....	98
3.3.4	AX3800S.....	98
3.3.5	AX3660S.....	99
3.3.6	AX3650S.....	99
3.3.7	AX2500S.....	100
3.3.8	AX2200S.....	100
3.3.9	AX2100S.....	101
3.3.10	AXprimoM210.....	101
<b>3.4</b>	<b>管理対象装置個別の注意事項.....</b>	<b>102</b>
3.4.1	AXprimoM210.....	102
3.4.2	AX620R .....	102
<b>4.</b>	<b>起動・停止方法.....</b>	<b>105</b>
<b>4.1</b>	<b>AX-Security-Controller(Manager)の起動・停止方法 .....</b>	<b>106</b>
4.1.1	AX-Security-Controller(Manager)の起動パラメータ .....	106
4.1.2	AX-Security-Controller(Manager)起動方法.....	110
4.1.3	AX-Security-Controller(Manager)停止方法.....	113
<b>4.2</b>	<b>AX-Security-Controller(Viewer)の起動・停止方法 .....</b>	<b>115</b>
4.2.1	AX-Security-Controller(Viewer)の起動パラメータ .....	115
4.2.2	AX-Security-Controller(Viewer)起動方法.....	117
4.2.3	AX-Security-Controller(Viewer)停止方法.....	117
<b>4.3</b>	<b>AX-Security-Controller(Tracker)の起動・停止方法 .....</b>	<b>118</b>
4.3.1	AX-Security-Controller(Tracker)の起動パラメータ .....	118
4.3.2	AX-Security-Controller(Tracker)起動方法 .....	120
4.3.3	AX-Security-Controller(Tracker)停止方法 .....	120
<b>5.</b>	<b>操作方法.....</b>	<b>121</b>

5.1 AX-Security-Controllerへのアクセス .....	122
5.1.1 AX-Security-Controller(Manager)へのアクセス .....	122
5.1.2 AX-Security-Controller(Viewer)へのアクセス .....	122
5.1.3 AX-Security-Controller(Tracker)へのアクセス .....	122
5.2 AX-Security-Controller(Manager)の画面構成.....	124
5.2.1 画面構成.....	124
5.3 初期設定 .....	126
5.3.1 初期設定の流れ .....	126
5.3.2 ライセンスの設定 .....	127
5.3.3 管理対象装置の設定 .....	130
5.3.4 接続情報設定の設定 .....	136
5.3.5 共通設定の設定 .....	139
5.3.6 トレンドマイクロ DDI/TMPMとの連携の設定 .....	143
5.3.7 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設定 .....	145
5.3.8 Syslog 連携(CEF)との連携の設定 .....	146
5.3.9 セグメンテーションセキュリティの設定 .....	151
5.3.10 マップの設定 .....	155
<b>6. AX-SECURITY-CONTROLLER(MANAGER)のWEB インタフェース .....</b>	<b>159</b>
6.1 共通 .....	160
6.1.1 ナビゲーションバー .....	160
6.1.2 ダッシュボード .....	163
6.1.3 端末 .....	165
6.1.4 装置 .....	181
6.1.5 セグメント .....	240
6.1.6 セキュリティ装置連携 .....	257
6.1.7 マップ .....	297
6.1.8 管理 .....	336
6.2 TMPM 連携 .....	392
6.2.1 ナビゲーションバー .....	392
6.2.2 ダッシュボード .....	392
6.2.3 セキュリティ装置連携 .....	393
6.2.4 管理 .....	396
6.3 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 .....	399

6.3.1	ナビゲーションバー .....	399
6.3.2	ダッシュボード .....	400
6.3.3	セキュリティ装置連携 .....	401
6.3.4	管理 .....	410
<b>7.</b>	<b>AX-SECURITY-CONTROLLER(VIEWER)の WEB インタフェース .....</b>	<b>413</b>
7.1	遮断端末表示機能 .....	414
<b>8.</b>	<b>AX-SECURITY-CONTROLLER(TRACKER)の WEB インタフェース .....</b>	<b>415</b>
8.1	端末移動履歴機能 .....	416
8.1.1	ナビゲーションバー .....	416
8.1.2	端末移動履歴 .....	417
<b>9.</b>	<b>トラブルシューティング .....</b>	<b>423</b>
9.1	手動バックアップ・リストア .....	424
9.1.1	バックアップ .....	424
9.1.2	リストア .....	424
9.2	トラブル発生時の対応 .....	425
9.2.1	プログラム起動 .....	425
9.2.2	Web インタフェースへのアクセス .....	425
9.2.3	トポロジ管理 .....	426
9.2.4	セキュリティフィルタ .....	430
9.2.5	マップ .....	432
9.2.6	E-mail 通知 .....	432
<b>付録</b>	<b>.....</b>	<b>435</b>
謝辞 (Acknowledgments)	.....	436

# 1. AX-Security-Controller の概要

---

この章では、AX-Security-Controller の概要について説明します。

---

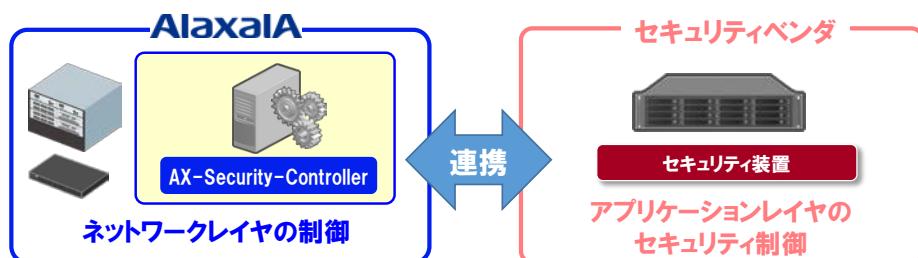
## 1.1 AX-Security-Controller の概要

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-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 は以下の 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連動が可能

### (2) 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

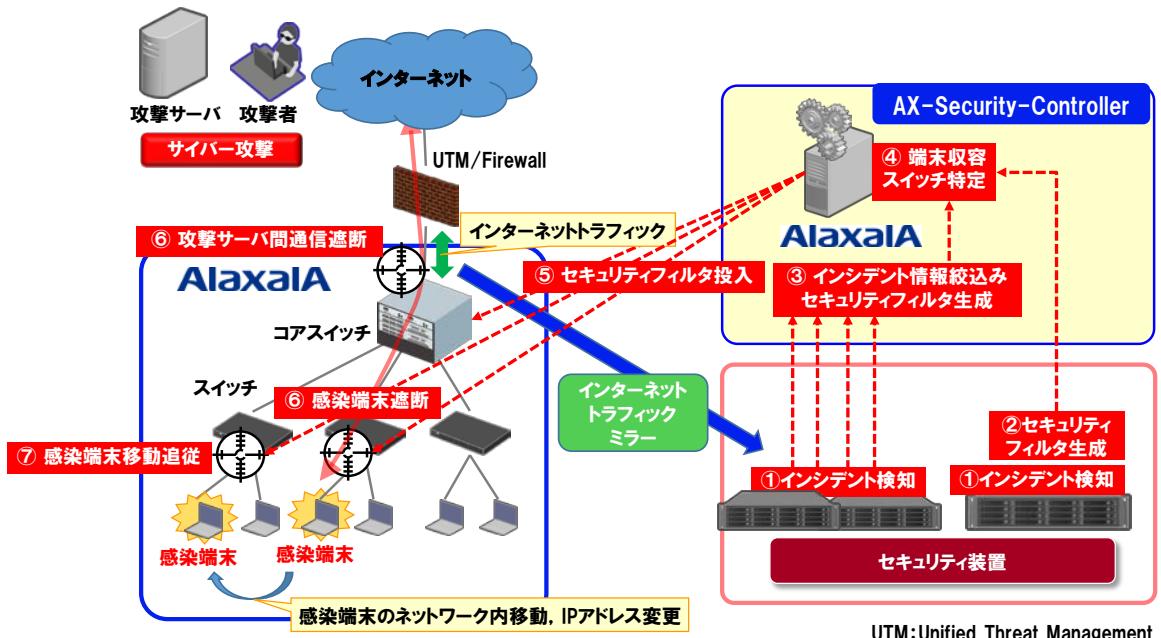
- ・ 感染端末がネットワーク内を移動しても、追従して遮断
- ・ DHCP を利用した環境において、感染端末の IP アドレスが変更されても、追従して遮断

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



## 1.2 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、表形式やトポロジー図形式で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、トポロジ管理やトポロジに応じたポリシー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。

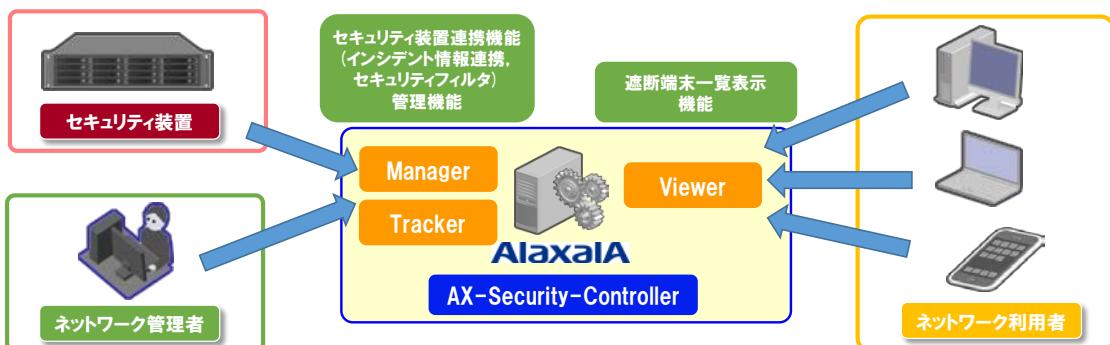
ネットワーク管理者が、遮断中の端末の一覧を、ネットワーク利用者へ参照させる場合に使用します。

- 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管理します。

また、ネットワーク管理者が移動履歴を、Web インタフェースを通して参照することができます。

図 1-3 AX-Security-Controller の構成

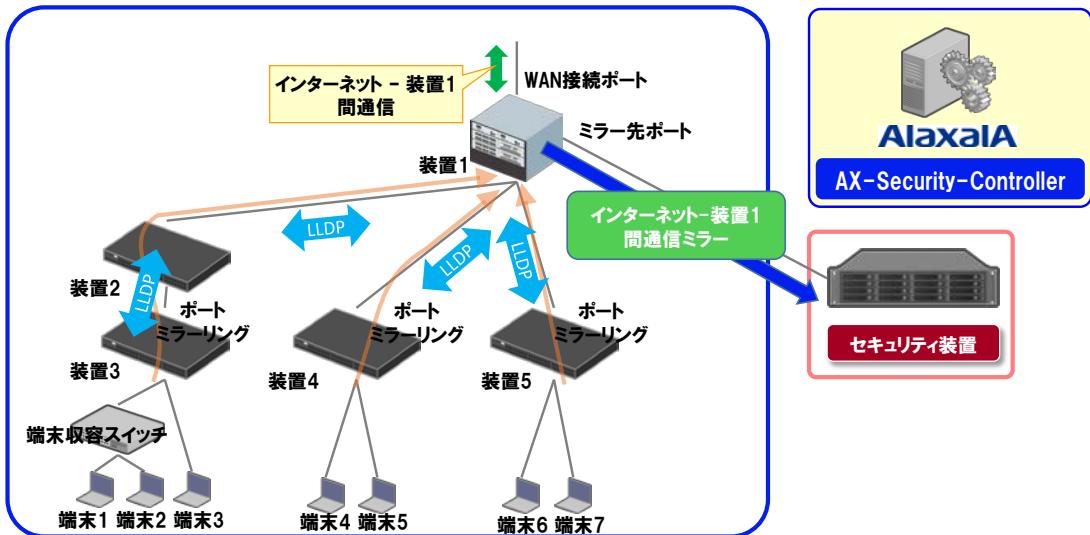


## 1.3 前提とするネットワークの構成

### 1.3.1 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 1-4 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 1-1 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, TMPPM) 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装置

#### (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。

表 1-2 管理対象装置の条件

条件
AX-Security-Controller から、SNMP および SSH でアクセス可能
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（上図では装置 1） (管理対象装置のうち、本レイヤ 3 スイッチを管理対象デフォルトゲートウェイとも呼びます)
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)

## (a) 標準 MIB 対応装置の条件

AX-Security-Controller 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装置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 対応装置と呼びます。

表 1-3 標準 MIB 対応装置の条件

使用用途	条件
装置情報収集 (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
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
LLDP 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 • dot1qTpFdbPort
	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) IPv6 リンクローカルアドレスは収集対象外です。

なお、標準 MIB 対応装置は、端末の ARP 情報、NDP 情報、MAC アドレス情報の学習のみが可能であり、後述するセキュリティフィルタの機能は使用することができません。

### (b) 標準 MIB 対応装置(VLAN 每コミュニティ)の条件

(a)の標準 MIB 対応装置とは別に、下記の条件を満たす Cisco スイッチを管理対象装置として使用することができます。この条件を満たすスイッチを標準 MIB 対応装置 (VLAN 每コミュニティ)と呼びます。

表 1-4 標準 MIB 対応装置(VLAN 每コミュニティ)の条件

使用用途	条件
装置情報収集 (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
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 每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) IPv6 リンクローカルアドレスは収集対象外です。

なお、標準 MIB 対応装置(VLAN 每コミュニティ)は、(a)の標準 MIB 対応装置と同様、後述するセキュリティフィルタの機能は使用することができません。

### (c) 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装置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 コントローラと呼びます。

表 1-5 ワイヤレス LAN コントローラ(Aruba-1)の条件

使用用途	条件
装置情報収集 (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

表 1-6 ワイヤレス LAN コントローラ(Cisco-1)の条件

使用用途	条件
装置情報収集 (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

表 1-7 ワイヤレス LAN コントローラ(Fortinet-1)の条件

使用用途	条件
装置情報収集 (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

### (3) WAN 接続ポート

インターネット接続用に用いるポートを 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)。

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-Security-Controller 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してください。

#### (4) ミラー先ポート

セキュリティ装置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、装置 1 のセキュリティ装置側ポートに対応します)。

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)。

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してください。

#### (5) 接続情報

隣接する管理対象装置間を接続するイーサネットポートで LLDP が動作しない場合、静的にポートの接続関係を AX-Security-Controller に設定することができます。この接続関係の情報を接続情報と呼びます。

以下の場合、接続情報を設定してください。

表 1-8 接続情報を設定するケース

ケース	説明
管理対象装置がスタック構成の場合	管理対象装置が下記であり、かつスタック構成の場合、LLDP が動作しないため、隣接する管理対象装置との接続情報を設定します。 <ul style="list-style-type: none"> <li>・AX4600S (Ver.11.15.F より前)</li> <li>・AX3800S</li> <li>・AX3660S (Ver.12.1.F より前)</li> <li>・AX3650S</li> </ul>

ケース	説明
管理対象装置が下記の場合 ・ AX620R ・ 標準 MIB 対応装置 ・ 標準 MIB 対応装置(VLAN 每コミュニティ) ・ ワイヤレス LAN コントローラ	管理対象装置が下記装置の場合、必要に応じて接続情報を設定します。「(a)アクセリスト拡張ポート」を参照ください。 ・ AX620R ・ 標準 MIB 対応装置 ・ 標準 MIB 対応装置(VLAN 每コミュニティ) ・ ワイヤレス LAN コントローラ
管理対象装置が AX8600S であり、隣接する管理対象装置が AX3660S かつ 100Gbit/s イーサネットポートの場合	管理対象装置が AX8600S であり、隣接する管理対象装置が AX3660S かつ 100Gbit/s イーサネットポートの場合、収集する LLDP 情報が省略されているため、隣接する管理対象装置との接続情報を設定します。

なお隣接する管理対象装置との接続をリンクアグリゲーションにより構成する場合、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。

### (a) アクセリスト拡張ポート

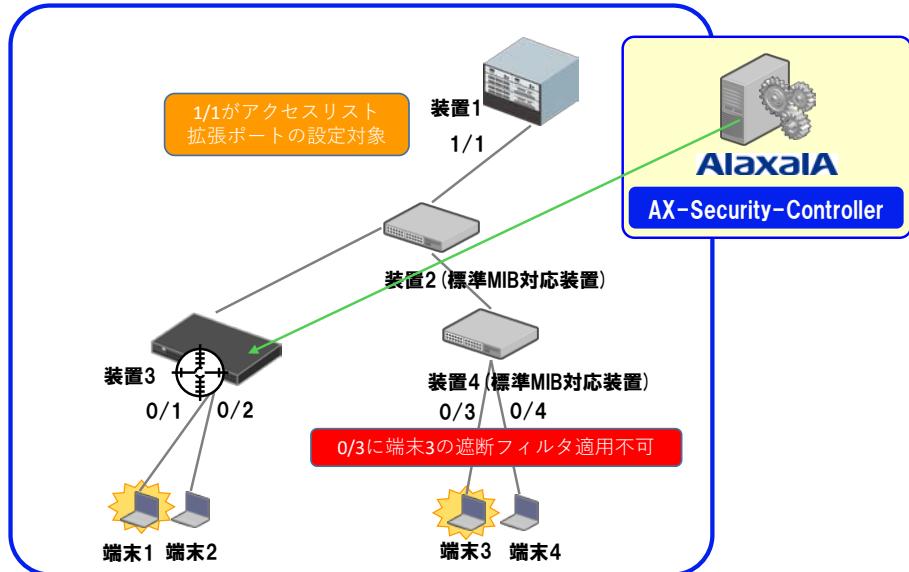
端末を収容する管理対象装置が下記の場合、後述する通信遮断・例外通信許可のセキュリティフィルタを適用するために、上位装置にアクセリスト設定を行うことができます。この設定を行うポートをアクセリスト拡張ポートと呼びます。

表 1-9 上位装置にアクセリストを設定可能な端末収容管理対象装置

管理対象装置
標準 MIB 対応装置
標準 MIB 対応装置(VLAN 每コミュニティ)
ワイヤレス LAN コントローラ

AX-Security-Controller がサポートする弊社製品に対する接続情報設定時に、ネットワーク構成に応じて設定を行ってください。設定時の注意事項は「1.6.7(2) アクセリスト拡張ポート設定における注意事項」を参照してください。

図 1-5 アクセスリスト拡張ポートを設定する構成例



## (6) 永続設定ポート(受信側/送信側)

永続設定ポート(受信側/送信側)を設定すると、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)に端末遮断設定を行います。

以下のようなケースで使用します。

- ・ AX-Security-Controller が端末位置を特定できない場合に、端末からの通信を遮断したい場合
- ・ 設定した永続設定ポート(受信側/送信側)の位置で端末からの通信を遮断したい場合

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。

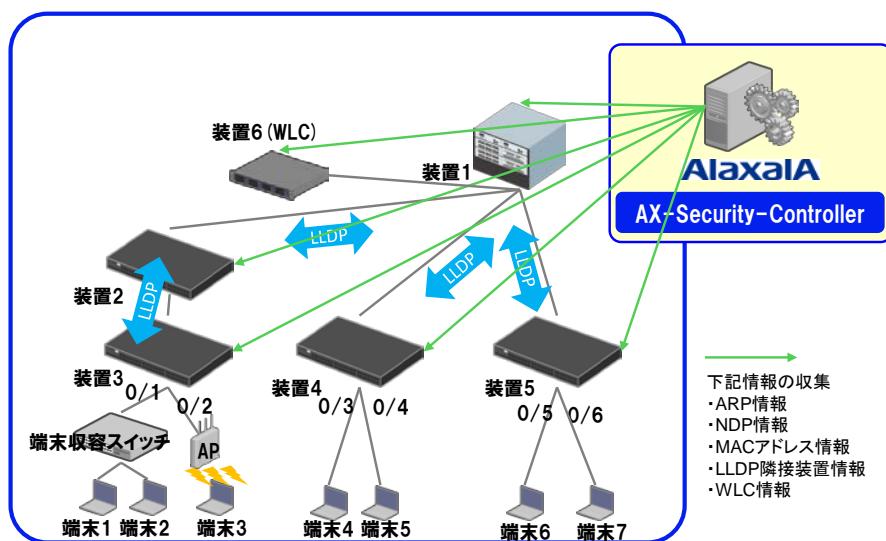
## 1.4 トポロジ管理

### 1.4.1 端末位置

AX-Security-Controller は、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。

図 1-6 端末位置



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

表 1-10 端末の位置の把握例

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

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できます。

## 1.4.2 エイリアス機能

### (1) 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できます。

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できます。

なお、Web インタフェースにおいて、タイトルカラムに対応するエイリアスのタイトルが未登録の場合、タイトルカラムに対応するエイリアスは None を表示します。

### (2) 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できます。

なお、ポートエイリアスの登録がない場合、ポートに対応するポートエイリアスは None を表示します。

図 1-7 エイリアス、ポートエイリアスを含む端末一覧画面

IPアドレス	MACアドレス	端末名	用途	接続先装置	ポートエイリアス	操作
198.51.100.54	0000.5e00.5354	OA端末54	OA	エッジスイッチ1	1Fフロア-1	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.55	0000.5e00.5355	OA端末55	OA	エッジスイッチ1	1Fフロア-1	<span style="background-color: green; color: white;">通信遮断解除</span>
198.51.100.56	0000.5e00.5356	OA端末56	OA	エッジスイッチ1	1Fフロア-1	<span style="background-color: orange; color: white;">セキュリティフィルタ解除</span>
198.51.100.57	0000.5e00.5357	OA端末57	OA	エッジスイッチ1	1Fフロア-1	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.58	0000.5e00.5358	OA端末58	OA	エッジスイッチ1	1Fフロア-1	<span style="background-color: red; color: white;">通信遮断</span>
	0000.5e00.5359	None	None	エッジスイッチ1	1Fフロア-1	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.53	0000.5e00.5353	OA端末53	OA	エッジスイッチ1	None	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.60	0000.5e00.5360	サーバ:F0	ファイルサーバ	エッジスイッチ1	None	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.61	0000.5e00.5361	サーバ:F1	None	エッジスイッチ1	None	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.62	0000.5e00.5362	サーバ:F2	None	エッジスイッチ1	None	<span style="background-color: red; color: white;">通信遮断</span>

21 件中 1 から 10 まで表示

前のページ 1 2 3 次のページ

### 1.4.3 マップ<sup>9</sup>

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。

本機能により、ネットワーク管理者は、以下のことが可能になります。

#### (1) 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。

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。

## (2) 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できます。

表 1-11 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

## (3) アイコン画像の変更

画面上に表示される装置、集線装置、端末アイコン画像をユーザが用意した画像に変更できます。以下に示すアイコン変更条件に合致した場合に、指定したアイコンを適用します。集線装置と端末は、変更条件に合致しない場合に適用されるデフォルトアイコンも変更できます。

表 1-12 装置アイコン変更条件

適用順位	変更条件	説明
1	装置	装置に対してアイコン画像を指定します。

表 1-13 集線装置アイコン変更条件

適用順位	変更条件	説明
1	接続先装置と接続先ポート	指定した接続先装置と接続先ポートに完全一致した場合にアイコンを適用します。
2	ポートエイリアス	ポートエイリアスに完全一致した場合にアイコンを適用します。

表 1-14 端末アイコン変更条件

適用順位	変更条件	説明
1	IP アドレス+MAC アドレス	指定した IP アドレスと MAC アドレスに完全一致した場合にアイコンを適用します。
2	IP アドレス	指定した IP アドレスに完全一致した場合にアイコンを適用します。
3	MAC アドレス	指定した MAC アドレスに完全一致した場合にアイコンを適用します。

適用順位	変更条件	説明
4	エイリアス	マップの表示エイリアスの値を対象に、指定したマップに表示するエイリアスに完全一致した場合にアイコンを適用します。
5	ベンダ	指定したベンダ名に完全一致した場合にアイコンを適用します。
6	MAC アドレス/マスク	指定した MAC アドレス/マスクに一致した場合にアイコンを適用します。

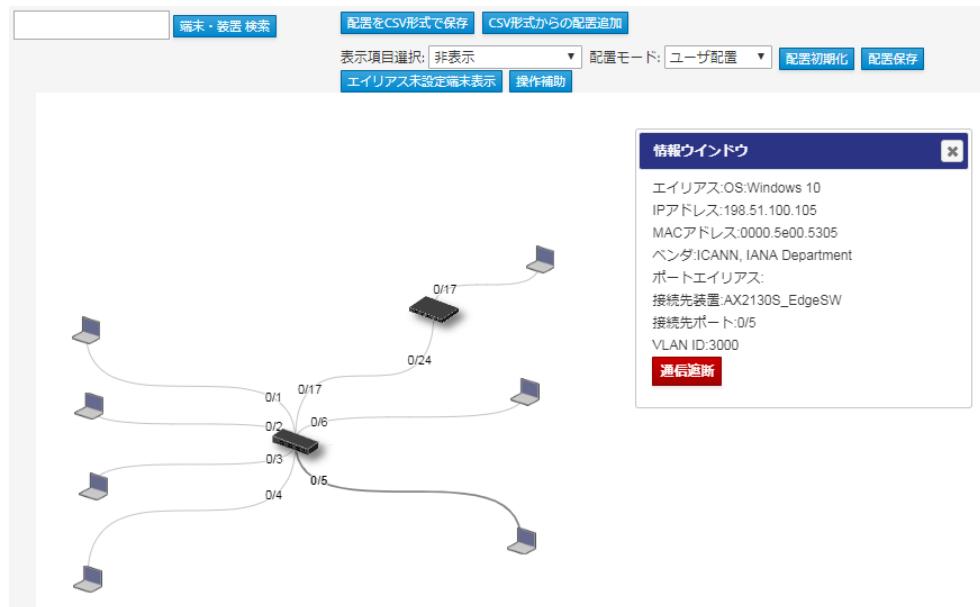
#### (4) 端末の制御

指定した端末について、下記の制御が可能になります。

表 1-15 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。

図 1-8 マップ画面



## 1.5 インシデント情報連携

### 1.5.1 概要

AX-Security-Controller にあらかじめ登録した Syslog クライアントから受信した 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。

#### (1) 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。通信遮断に使用する IP アドレスは、Syslog の中の「src」、「dst」、「sourceTranslatedAddress」、「destinationTranslatedAddress」フィールド、ユーザ定義拡張フィールドから選択して、送信元と宛先それぞれに指定してください。

使用する IP アドレスには、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、追加で「PanOSXforwarderfor」フィールドも指定可能です。

送信元指定と宛先指定に設定した IP アドレスの組み合わせごとの遮断動作について、以下に示します。

表 1-16 通信遮断で設定する IP アドレス

送信元指定	宛先指定	説明
端末の IP アドレス	指定なし(空欄)	該当 IP アドレスの端末通信を遮断します。
指定なし(空欄)	攻撃サーバの IP アドレス	該当 IP アドレスの攻撃サーバ通信を遮断します。
端末の IP アドレス	攻撃サーバの IP アドレス	該当 IP アドレスの端末をトポロジ管理で検出していると、端末通信を遮断します。それ以外の場合は、攻撃サーバ通信を遮断します。

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。通信遮断に使用する MAC アドレスは、Syslog の中の「smac」、「dmac」フィールド、ユーザ定義拡張フィールドから選択して、送信元に指定してください。

## (2) 詳細ミラー

インシデントとして抽出した 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装置にて詳細分析することが可能になります。詳細ミラーに使用する IP アドレスは、Syslog の中の「src」，「dst」，「sourceTranslatedAddress」，「destinationTranslatedAddress」フィールド、ユーザ定義拡張フィールドから選択して、送信元に指定してください。

使用する IP アドレスには、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、追加で「PanOSXforwarderfor」フィールドも指定可能です。

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。詳細ミラーに使用する MAC アドレスは、Syslog の中の「smac」，「dmac」フィールド、ユーザ定義拡張フィールドから選択して、送信元に指定してください。

## (3) 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た 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。

## 1.5.2 対応 Syslog フォーマット

AX-Security-Controller は CEF(Common Event Format)の Syslog と連携します。

### (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 を CEF で出力するようにしてください。

<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 フォーマットの各フィールドの意味を以下に示します。

表 1-17 各フィールドの説明

フィールド名称	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>

### 1.5.3 インシデント抽出ルール

AX-Security-Controller 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。

#### (1) インシデント抽出に指定可能なフィールド

インシデント抽出に指定可能なフィールドを以下の表に示します。および、Syslog クライアントの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連携」の場合に、追加で指定可能なフィールドを表 1-19 に示します。

表 1-18 インシデント抽出に指定可能なフィールド

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/Device Event Class ID String or Integer	○
	Name String	○
	Severity String or Integer	○

フィールド	データ型	指定可否
拡張フィールド		
act	String	<input type="radio"/>
app	String	<input type="radio"/>
c6a1	IPv6 Address	<input type="radio"/>
c6a1Label	String	<input type="radio"/>
c6a2	IPv6 Address	<input type="radio"/>
c6a2Label	String	<input type="radio"/>
c6a3	IPv6 Address	<input type="radio"/>
c6a3Label	String	<input type="radio"/>
c6a4	IPv6 Address	<input type="radio"/>
c6a4Label	String	<input type="radio"/>
cfp1	Floating Point	<input type="radio"/>
cfp1Label	String	<input type="radio"/>
cfp2	Floating Point	<input type="radio"/>
cfp2Label	String	<input type="radio"/>
cfp3	Floating Point	<input type="radio"/>
cfp3Label	String	<input type="radio"/>
cfp4	Floating Point	<input type="radio"/>
cfp4Label	String	<input type="radio"/>
cn1	Long	<input type="radio"/>
cn1Label	String	<input type="radio"/>
cn2	Long	<input type="radio"/>
cn2Label	String	<input type="radio"/>
cn3	Long	<input type="radio"/>
cn3Label	String	<input type="radio"/>
cnt	Integer	<input type="radio"/>
cs1	String	<input type="radio"/>
cs1Label	String	<input type="radio"/>
cs2	String	<input type="radio"/>
cs2Label	String	<input type="radio"/>
cs3	String	<input type="radio"/>
cs3Label	String	<input type="radio"/>
cs4	String	<input type="radio"/>
cs4Label	String	<input type="radio"/>
cs5	String	<input type="radio"/>
cs5Label	String	<input type="radio"/>
cs6	String	<input type="radio"/>
cs6Label	String	<input type="radio"/>
destinationDnsDomain	String	<input type="radio"/>
destinationServiceName	String	<input type="radio"/>
destinationTranslatedAddress	IPv4 Address or IPv6 Address	<input type="radio"/>
destinationTranslatedPort	Integer	<input type="radio"/>
deviceCustomDate1	Time Stamp	<input type="radio"/>
deviceCustomDate1Label	String	<input type="radio"/>
deviceCustomDate2	Time Stamp	<input type="radio"/>
deviceCustomDate2Label	String	<input type="radio"/>
deviceDirection	Integer	<input type="radio"/>
deviceDnsDomain	String	<input type="radio"/>

フィールド	データ型	指定可否
deviceExternalId	String	<input type="radio"/>
deviceFacility	String	<input type="radio"/>
deviceInboundInterface	String	<input type="radio"/>
deviceNtDomain	String	<input type="radio"/>
deviceOutboundInterface	String	<input type="radio"/>
devicePayloadId	String	<input type="radio"/>
deviceProcessName	String	<input type="radio"/>
deviceTranslatedAddress	IPv4 Address or IPv6 Address	<input type="radio"/>
dhost	String	<input type="radio"/>
dmac	MAC Address	<input type="radio"/>
dntdom	String	<input type="radio"/>
dpid	Integer	<input type="radio"/>
dpriv	String	<input type="radio"/>
dproc	String	<input type="radio"/>
dpt	Integer	<input type="radio"/>
dst	IPv4 Address or IPv6 Address	<input type="radio"/>
dtz	String	<input type="radio"/>
duid	String	<input type="radio"/>
duser	String	<input type="radio"/>
dvc	IPv4 Address or IPv6 Address	<input type="radio"/>
dvchost	String	<input type="radio"/>
dvcmac	MAC Address	<input type="radio"/>
dvcpid	Integer	<input type="radio"/>
end	Time Stamp	<input type="radio"/>
externalId	String	<input type="radio"/>
fileCreateTime	Time Stamp	<input type="radio"/>
fileHash	String	<input type="radio"/>
fileId	String	<input type="radio"/>
fileModificationTime	Time Stamp	<input type="radio"/>
filePath	String	<input type="radio"/>
filePermission	String	<input type="radio"/>
fileType	String	<input type="radio"/>
flexDate1	Time Stamp	<input type="radio"/>
flexDate1Label	String	<input type="radio"/>
flexNumber1	Integer	<input type="radio"/>
flexNumber1Label	String	<input type="radio"/>
flexNumber2	Integer	<input type="radio"/>
flexNumber2Label	String	<input type="radio"/>
flexString1	String	<input type="radio"/>
flexString1Label	String	<input type="radio"/>
flexString2	String	<input type="radio"/>
flexString2Label	String	<input type="radio"/>
fname	String	<input type="radio"/>
fsize	Integer	<input type="radio"/>

フィールド	データ型	指定可否
in	Integer	<input type="radio"/>
msg	String	<input type="radio"/>
oldFileCreateTime	Time Stamp	<input type="radio"/>
oldFileHash	String	<input type="radio"/>
oldFileDialog	String	<input type="radio"/>
oldFileModificationTime	Time Stamp	<input type="radio"/>
oldFileName	String	<input type="radio"/>
oldFilePath	String	<input type="radio"/>
oldFilePermission	String	<input type="radio"/>
oldFileSize	Integer	<input type="radio"/>
oldFileType	String	<input type="radio"/>
out	Integer	<input type="radio"/>
outcome	String	<input type="radio"/>
proto	String	<input type="radio"/>
reason	String	<input type="radio"/>
request	String	<input type="radio"/>
requestClientApplication	String	<input type="radio"/>
requestContext	String	<input type="radio"/>
requestCookies	String	<input type="radio"/>
requestMethod	String	<input type="radio"/>
rt	Time Stamp	<input type="radio"/>
shost	String	<input type="radio"/>
smac	MAC Address	<input type="radio"/>
sntdom	String	<input type="radio"/>
sourceDnsDomain	String	<input type="radio"/>
sourceServiceName	String	<input type="radio"/>
sourceTranslatedAddress	IPv4 Address or IPv6 Address	<input type="radio"/>
sourceTranslatedPort	Integer	<input type="radio"/>
spid	Integer	<input type="radio"/>
spriv	String	<input type="radio"/>
sproc	String	<input type="radio"/>
spt	Integer	<input type="radio"/>
src	IPv4 Address or IPv6 Address	<input type="radio"/>
start	Time Stamp	<input type="radio"/>
suid	String	<input type="radio"/>
suser	String	<input type="radio"/>
type	Integer	<input type="radio"/>
agentDnsDomain	String	<input type="radio"/>
agentNtDomain	String	<input type="radio"/>
agentTranslatedAddress	IPv4 Address or IPv6 Address	<input type="radio"/>
agentTranslatedZoneExternalID	String	<input type="radio"/>
agentTranslatedZoneURI	String	<input type="radio"/>
agentZoneExternalID	String	<input type="radio"/>
agentZoneURI	String	<input type="radio"/>

フィールド	データ型	指定可否
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

表 1-19 インシデント抽出に追加で指定可能なフィールド (Syslog クライアントの  
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連携の場合)

フィールド	データ型
拡張フィールド	PanOSPacketsReceived
	PanOSPacketsSent
	PanOSReferer
	PanOSXff
	PanOSDG11
	PanOSDG12
	PanOSDG13
	PanOSDG14
	PanOSVsysName

フィールド	データ型
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

## (2) ユーザ定義拡張フィールド

「表 1-18 インシデント抽出に指定可能なフィールド」, および「表 1-19 インシデント抽出に追加で指定可能なフィールド (Syslog クライアントの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連携の場合)」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できます。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 1-20 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

また, 「表 1-18 インシデント抽出に指定可能なフィールド」, および「表 1-19 インシデント抽出に追加で指定可能なフィールド (Syslog クライアントのクライアン

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連携の場合)」のフィールドを、データ型が「IPv4 Address」，「IPv6 Address」，「IPv4 Address or IPv6 Address」，または「MAC Address」であるユーザ定義拡張フィールドとして設定することで、ルールの送信元指定または宛先指定に使用することも可能です。

なお、下記フィールドのデータ型を、「IPv4 Address」，「IPv6 Address」，「IPv4 Address or IPv6 Address」，および「MAC Address」ではないデータ型とした場合、ルールの送信元指定、および宛先指定として選択できなくなりますので注意願います。

表 1-21 データ型変更によりルールの送信元指定と宛先指定に選択できなくなる可能性があるフィールド

フィールド
src
dst
sourceTranslatedAddress
destinationTranslatedAddress
smac
dmac
PanOSXforwarderfor

### (3) フィールド値のデータ型ごとの検索条件

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 1-22 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

## 1.6 セキュリティフィルタ (セキュリティ装置との連携)

### 1.6.1 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、およびAX-Security-Controller が抽出したインシデントと連携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。

#### (1) 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。

以下に、提供する機能を示します。

表 1-23 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

#### (2) 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イ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 1-24 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。

## (3) 端末移動追従

端末の位置をトポ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。

## 1.6.2 セキュリティフィルタの生成・削除契機

AX-Security-Controller 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 1-9 セキュリティフィルタの生成・削除契機

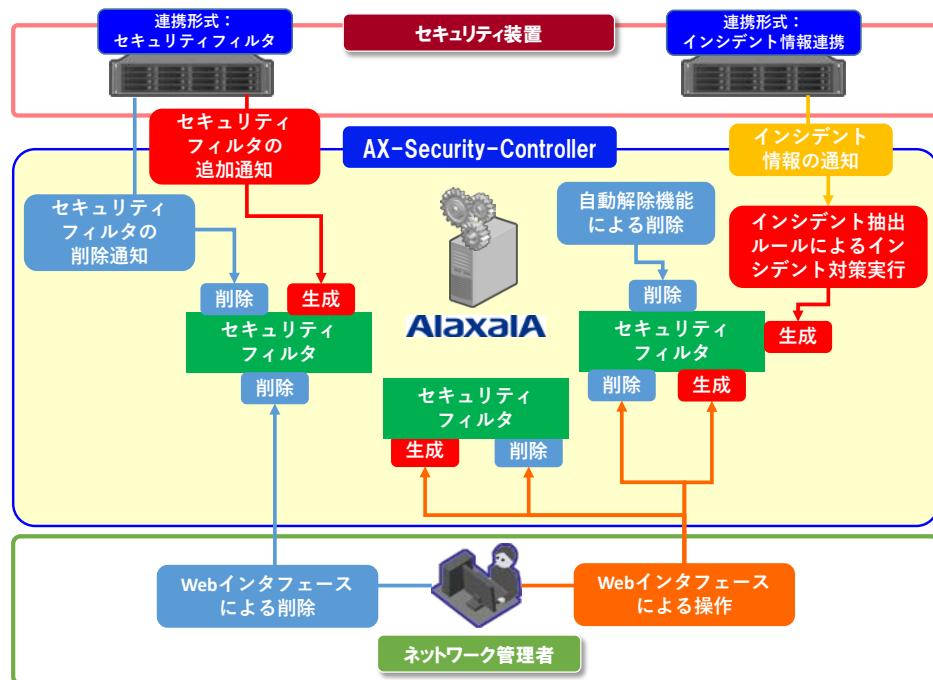


表 1-25 セキュリティフィルタの生成契機

連携形式	生成契機	備考
セキュリティ フィルタ	セキュリティ装置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 1-26 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	セキュリティ装置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。

### (1) 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。

「6.1.6(2) セキュリティフィルタ詳細」、「6.1.6(5) ルールマッチ履歴」、各セキュリティ装置連携のセキュリティフィルタ詳細画面、およびルールマッチ履歴を参照ください。

### (2) 自動解除機能による削除

#### (a) 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。

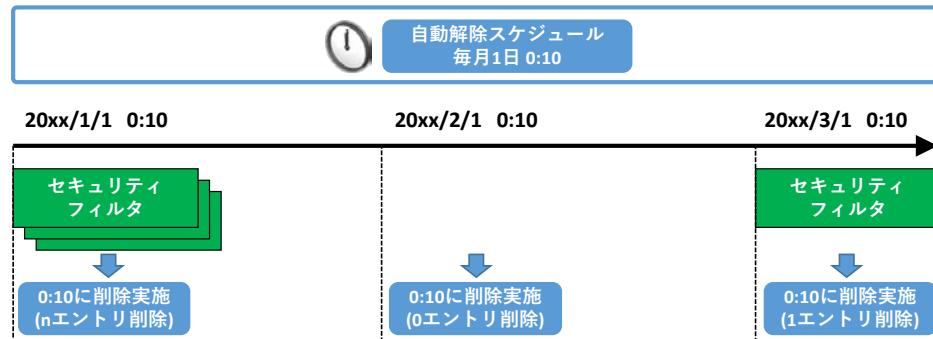
表 1-27 設定可能な自動解除スケジュール

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 1-10 自動解除スケジュール動作イメージ図



スケジュールの設定は、「6.1.8(1) 共通設定」を参照ください。

なお、自動解除スケジュールが動作するよう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。「6.1.6(2) セキュリティフィルタ詳細」、およびインシデント情報連携の各セキュリティ装置連携のセキュリティフィルタ詳細画面を参照ください。

### (b) タイマー解除

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 1-28 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。

### 1.6.3 セキュリティフィルタの種別

AX-Security-Controller 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 1-29 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

### 1.6.4 セキュリティフィルタの設定状態

AX-Security-Controller 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 1-30 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装置を検索、コンフィグレーションを設定中です。

設定状態	説明
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装置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装置から、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(「1.6.6 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装置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(「1.11 ライセンス」参照)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 1-31 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 1-32 失敗要因一覧」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 1-32 失敗要因一覧」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 1-32 失敗要因一覧」を参照してください。

表 1-32 失敗要因一覧

失敗要因	説明
通信失敗	<ul style="list-style-type: none"> <li>・管理対象装置と通信できない場合</li> <li>・SNMP コミュニティ名称不一致</li> </ul>
認証失敗	<ul style="list-style-type: none"> <li>・SSH ログイン失敗時</li> <li>・同時ログイン数の上限越え</li> </ul>
コンフィグ反映失敗	<ul style="list-style-type: none"> <li>・装置管理者モードのパスワード不一致</li> <li>・事前準備・設定の不足</li> <li>・管理対象装置のフィルタエンタリの収容条件超え</li> <li>・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</li> </ul>
コンフィグモード移行失敗	<ul style="list-style-type: none"> <li>・コンフィグモードへの移行失敗</li> </ul>

## 1.6.5 セキュリティフィルタの動作モード

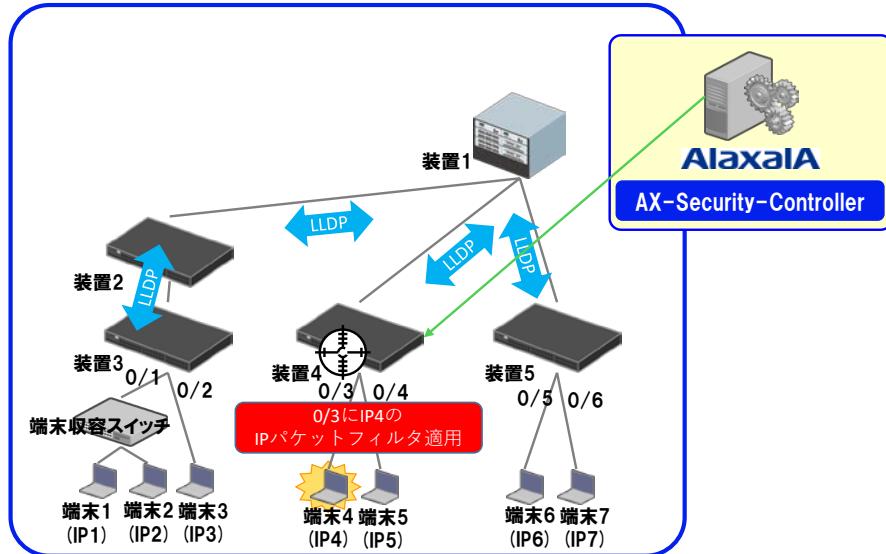
AX-Security-Controller は、以下 2 つの動作モードがあります。

### (1) 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。起動パラメータのアクセリストのモードを v4-v6 で指定している場合、IPv4 アクセリストに加えて IPv6 のアクセ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 アクセリストと IPv6 アクセ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ができます。IPv6 セキュリティフィルタ設定指示時も同様です。

起動パラメータのアクセリストのモードを v4-only で指定、または省略している場合、IPv4 アクセリストだけを設定します。

図 1-11 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

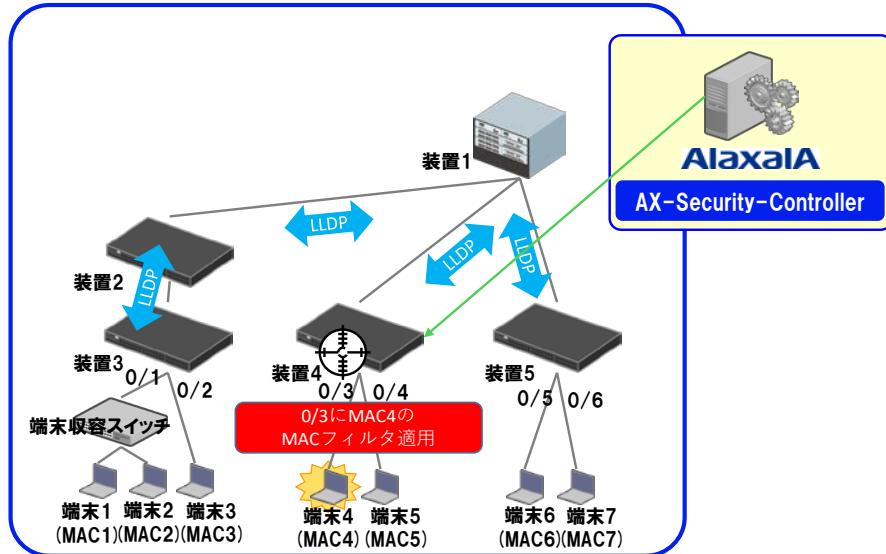


## (2) 通信遮断専用モード

通信遮断モードは、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 パケットだけではなく、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、IP アドレスの数と同数のアクセスリストが設定されます。

図 1-12 通信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



### 1.6.6 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-Security-Controller 起動時に、どちらを使用するかを指定します。

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 1-33 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(その他は許可)	○	×
		攻撃サーバ通信	○	×
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)	×	○

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
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	○	○ <sup>※1</sup>
特定端末への Web 通信不可表示機能 <sup>※2</sup>	—	—	○	×
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

## 1.6.7 セキュリティフィルタの使用上の注意事項

### (1) アクセスリストのモードにおける注意事項

#### (a) IPv4/IPv6 動作モードを使用する場合

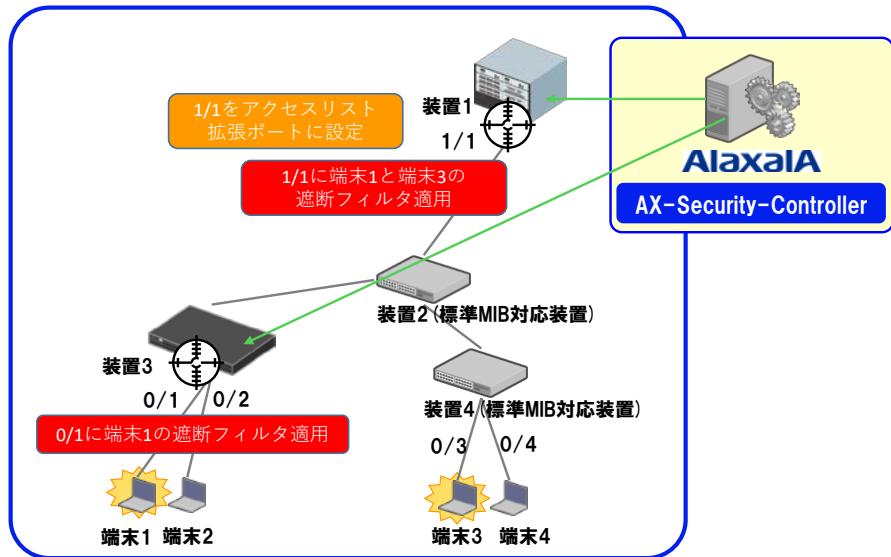
IPv6 アドレスに対して通信遮断を実施する場合、ネットワーク装置が学習した NDP のダイナミックエントリが削除されないように、NS(Neighbor Solicitation)および NA(Neighbor Advertisement)の permit フィルタを、端末が収容されるポートに設定してください。設定しない場合、端末の NDP エントリの削除契機で、該当 IPv6 アドレスに対するフィルタ設定が削除されます。

### (2) アクセスリスト拡張ポート設定における注意事項

端末を収容する装置として、AX-Security-Controller 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 1-13 複数装置にセキュリティフィルタが適用される構成例



### (3) 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

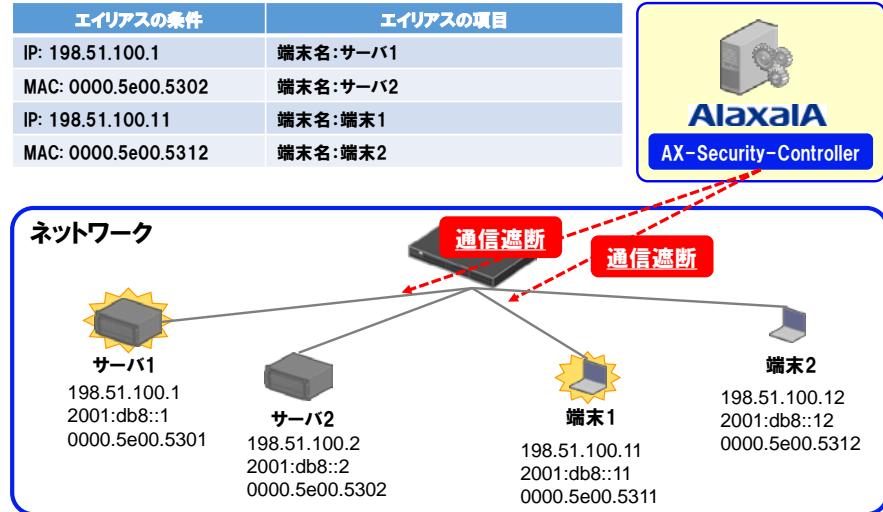
エイリアス未登録端末の通信遮断を有効(「6.1.8(1) 共通設定」)にする場合、以下で運用することを推奨します。

表 1-34 エイリアス未登録端末の通信遮断有効時の推奨運用

項目番	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 1-14 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なりません。

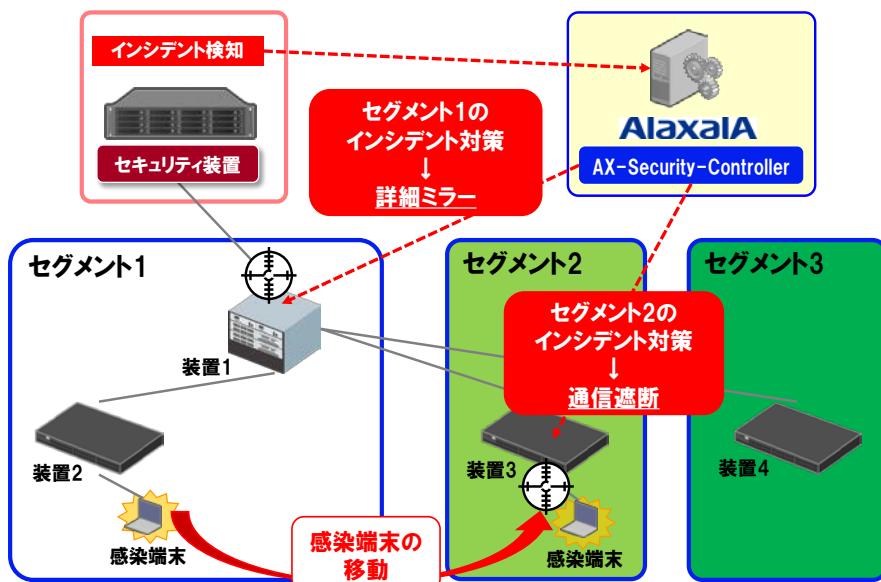
## 1.7 セグメンテーションセキュリティ

### 1.7.1 概要

セグメンテーションセキュリティは、AX-Security-Controller 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 1-15 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-Security-Controller 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-Security-Controller には、セキュリティ装置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-Security-Controller がセキュリティ装置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 の装置 2 に収容していることを検知すると、装置 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 の装置 3 に移動したことを検知すると、装置 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。

## 1.7.2 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。

### (1) 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 1-35 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。 <ul style="list-style-type: none"> <li>・標準 MIB 対応装置</li> <li>・標準 MIB 対応装置(VLAN 每コミュニティ)</li> <li>・ワイヤレス LAN コントローラ</li> </ul>

### (2) セグメントの分類

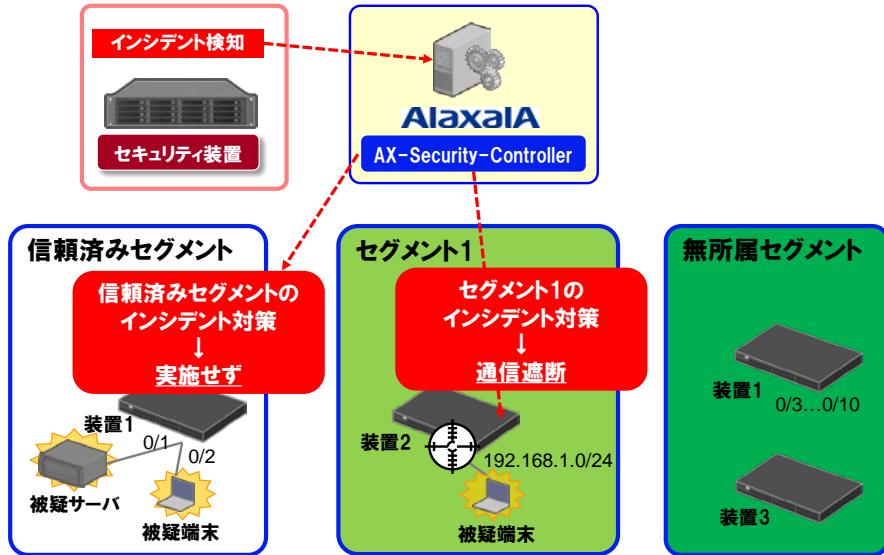
セグメントは、以下に示す3つに分類します。

表 1-36 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。
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。
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。

信頼済みセグメント、個別セグメント、および無所属セグメントの例を下図に示します。

図 1-16 セグメント分類



上図において、AX-Security-Controller は、管理対象ネットワークを、信頼済みセグメント、セグメント 1、および無所属セグメントの 3 つのセグメントに分割して管理します。

信頼済みセグメントは、装置 1 のポート 0/1, 0/2 より構成します。セグメント 1 は、192.168.1.0/24 であり、装置 2 の全ポートにより構成します。無所属セグメントは、信頼済みセグメント、セグメント 1 のどちらにも所属していない装置 1 の 0/3～0/10、および装置 3 の全ポートにより構成します。

AX-Security-Controller には、セキュリティ装置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 192.168.1.0/24 に含まれる端末には、インシデント対策を通信遮断と設定します。

AX-Security-Controller がセキュリティ装置より被疑端末のインシデント情報を受信し、被疑端末または被疑サーバが信頼済みセグメント内に収容されていることを検知すると、装置 1 へのコンフィグレーションの設定を実施しません。

被疑端末がセグメント 1 の 192.168.1.0/24 内に収容されていることを検知すると、装置 2 へと通信遮断のインシデント対策を実施します。

### (3) 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 1-37 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	○ <sup>※1</sup>	○	○

(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) 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。

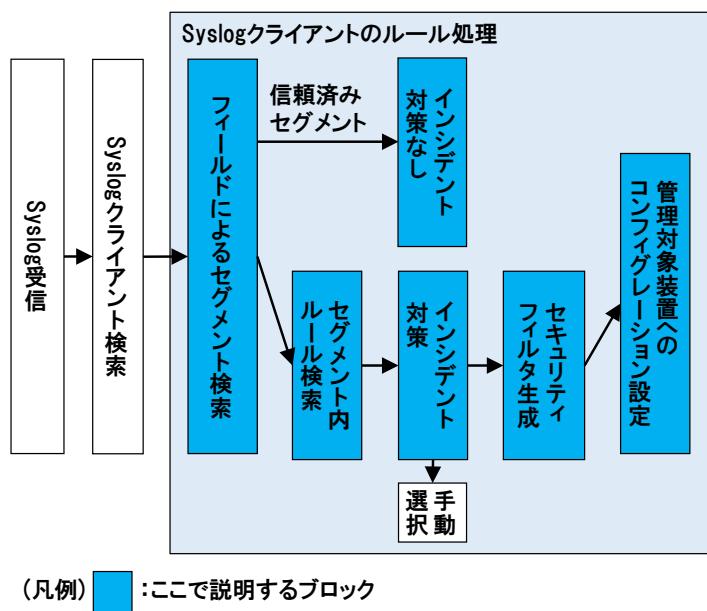
表 1-38 セグメントの分類と優先度

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。

### 1.7.3 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 1-17 セグメンテーションセキュリティの処理プロック



図に示した処理プロックの概要を下表に示します。

表 1-39 各処理プロックの概要

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。 <ul style="list-style-type: none"> <li>src</li> <li>dst</li> <li>sourceTranslatedAddress</li> <li>destinationTranslatedAddress</li> <li>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)</li> <li>smac</li> <li>dmac</li> <li>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)</li> </ul> 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により、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。

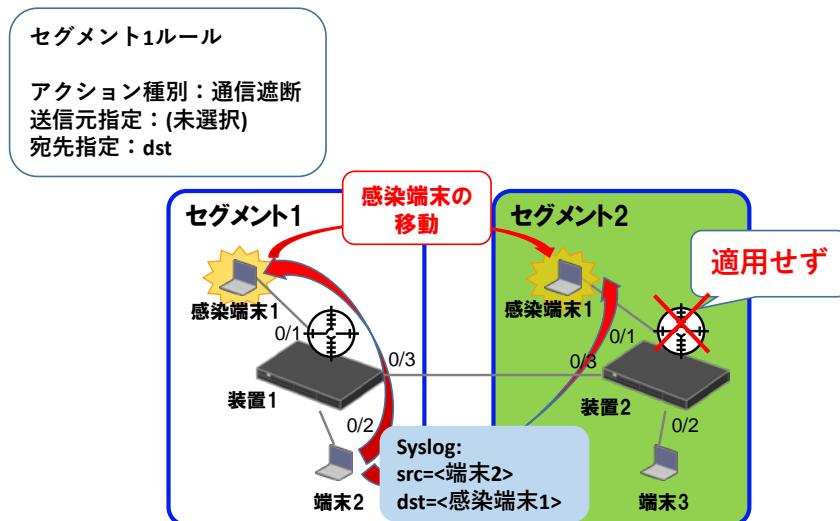
部位	概要
セキュリティフィルタ生成	アクション種別が通信遮断、または詳細ミラーの場合、セキュリティフィルタを生成します。
管理対象装置へのコンフィグレーション設定	生成したセキュリティフィルタより、適用対象の管理対象装置へとコンフィグレーションを設定します。

#### 1.7.4 セグメンテーションセキュリティ使用時の注意事項

##### (1) セグメント分割と端末移動の注意事項

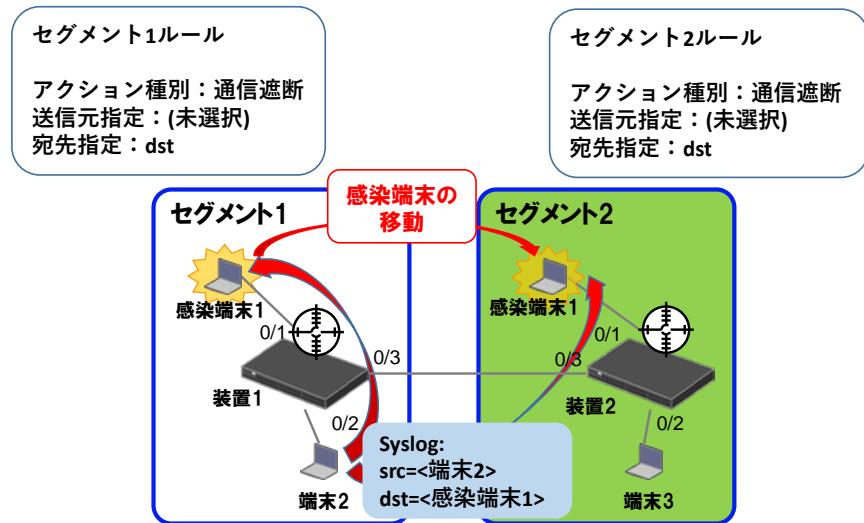
セグメントを分割する際は、端末のセグメント移動を考慮してインシデント抽出ルールの設定をおこなってください。下記のルール設定(宛先指定の通信遮断)では感染端末1がセグメント2に移動した際、セグメント1のルールではセグメント2内の装置2へとセキュリティフィルタの適用をおこないません。

図 1-18 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 1-19 セグメント分割におけるルール設定例



## 1.8 通知機能

### 1.8.1 Syslog 通知

AX-Security-Controller はイベント発生および状態を Syslog サーバに Syslog 通知することができます。

表 1-40 Syslog 通知種別一覧

項目	説明
インシデント情報連携	インシデント情報連携で発生したイベントに応じた Syslog を出力します。
セキュリティフィルタ関連	セキュリティフィルタで発生したイベントに応じた Syslog を出力します。
端末接続	端末関連で発生したイベントに応じた Syslog を出力します。
管理対象装置関連	管理対象装置関連で発生したイベントに応じた Syslog を出力します。

#### (1) Syslog フォーマット

Syslog 通知で送信する Syslog は CEF(Common Event Format)を使用します。各 Syslog で共通する CEF ヘッダフィールドの設定項目は以下となります。

表 1-41 Syslog 通知種別一覧

ヘッダフィールド	説明	値
Version	CEF フォーマットのバージョン	0
Device Vendor	ベンダ名称	ALAXALA Networks Corporation
Device Product	プロダクト名称	AX-Security-Controller
Device Version	バージョン	<AX-Security-Controller のバージョン>
Device Event Class ID	イベント識別子	-(syslog 出力イベント毎に異なる)
Name	イベント名	-(syslog 出力イベント毎に異なる)
Severity	重要度	-(syslog 出力イベント毎に異なる)

表 1-42 イベント識別子、イベント名、重要度の設定値

Syslog 種別	イベント種別	Device Event Class ID	Name	Severity
インシデント情報連携	通信遮断	Incident	Match the block rule	6
	詳細ミラー	Incident	Match the mirror rule	5

Syslog 種別	イベント種別	Device Event Class ID	Name	Severity
	手動選択	Incident	Match the blocking pending rule	4
セキュリティフィルタ関連	登録	Action	Registered the action	2
	設定完了	Action	Completed to set the action	2
	削除完了	Action	Completed to delete the action	2
	端末毎設定要因	Action	Action registered	セキュリティフィルタ追加
		Action	Wanport registered	WAN 接続ポート追加
		Action	Mirrorport registered	ミラー先ポート追加
		Action	Permanentportin registered	永続設定ポート(受信側)追加
		Action	Permanentportout registered	永続設定ポート(送信側)追加
		Action	Host port moved	ポート移動
		Action	Host ipaddress changed	IP アドレス変更
	端末毎設定完了	Action	Completed to apply the configuration	コンフィグ反映完了
	端末毎設定失敗	Action	Failed to apply the configuration	4
端末毎削除要因	Action	Not supported	未サポート種別	2
	Action	Applying failed	アクセスリスト適用失敗	2
	Action	Node deleted	管理対象装置削除	2
	Action	Node not licensed	ライセンス無効	2
	Action	Node under maintenance	メンテナンス実施	2
	Action	Action deleted	セキュリティフィルタ削除	2

Syslog 種別	イベント種別	Device Event Class ID	Name	Severity
	Action		Registering action failed セキュリティフィルタ追加失敗	2
	Action		Wanport deleted WAN 接続ポート削除	2
	Action		Deleting wanport failed WAN 接続ポート削除失敗	2
	Action		Mirrorport deleted ミラー先ポート削除	2
	Action		Deleting mirrorport failed ミラー先ポート削除失敗	2
	Action		Permanentportin deleted 永続設定ポート(受信側)削除	2
	Action		Deleting permanentportin failed 永続設定ポート(受信側)削除失敗	2
	Action		Permanentportout deleted 永続設定ポート(送信側)削除	2
	Action		Deleting permanentportout failed 永続設定ポート(送信側)削除失敗	2
	Action		Host moved from WAN port to host port ポート移動	2
	Action		Host aged out エージアウト	2
	Action		Changed to trusted host 信頼済みセグメント追加	2
	Action		Changed to untrusted host 信頼済みセグメント削除	2
端末接続	エイリアス未登録接続	Host	Connection of the unregistered host	2
管理対象装置関連	コンフィグ容量監視	Node	Check configuration capacity	4

Syslog のメッセージフォーマットで使用する連携機能名称と対応する機能を、下表に示します。

表 1-43 連携機能名称一覧

連携機能名称	機能
base	手動追加
tmpm	TMPM 連携
pa	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
cef	Syslog 連携(CEF)

Syslog のメッセージフォーマットで使用する設定先ポートの説明を、下表に示します。

表 1-44 設定先ポート名称一覧

設定先ポート名称	説明
wan	WAN 接続ポート
mirror	ミラー先ポート
permanentportin	永続設定ポート(受信側)
permanentportout	永続設定ポート(送信側)
host	端末接続ポート

## (2) インシデント情報連携メッセージフォーマット

インシデント情報連携のメッセージフォーマットは以下となります。

表 1-45 インシデント情報連携のメッセージフォーマット

種別	メッセージ
	内容
通信遮断	<p>CEF:0 ALAXALA Networks Corporation AX-Security-Controller &lt;AX-Security-Controller のバージョン&gt; Incident Match the block rule 6 rt=&lt;MMM dd yyyy HH:mm:ss zzz&gt; dvchost=&lt;syslog client name&gt; cs1Label=Rule Number cs1=&lt;rule number&gt;</p> <p>[Extension Field]        rt: &lt;MMM dd yyyy HH:mm:ss zzz&gt;            イベント発生日時        dvchost: &lt;syslog client name&gt;            syslog クライアント名称        cs1Label: cs1 の説明        cs1: &lt;rule number&gt;            マッチしたルールの優先度</p>
詳細ミラー	<p>CEF:0 ALAXALA Networks Corporation AX-Security-Controller &lt;AX-Security-Controller のバージョン&gt; Incident Match the mirror rule 5 rt=&lt;MMM dd yyyy HH:mm:ss zzz&gt; dvchost=&lt;syslog client name&gt; cs1Label=Rule Number cs1=&lt;rule number&gt;</p> <p>[Extension Field]        rt: &lt; MMM dd yyyy HH:mm:ss zzz &gt;            イベント発生日時        dvchost: &lt;syslog client name&gt;            syslog クライアント名称        cs1Label: cs1 の説明        cs1: &lt;rule number&gt;            マッチしたルールの優先度</p>
手動選択	<p>CEF:0 ALAXALA Networks Corporation AX-Security-Controller &lt;AX-Security-Controller のバージョン&gt; Incident Match the blocking pending rule 4 rt=&lt;MMM dd yyyy HH:mm:ss zzz&gt; dvchost=&lt;syslog client name&gt; cs1Label=Rule Number cs1=&lt;rule number&gt;</p> <p>[Extension Field]        rt: &lt; MMM dd yyyy HH:mm:ss zzz &gt;            イベント発生日時        dvchost: &lt;syslog client name&gt;            syslog クライアント名称        cs1Label: cs1 の説明        cs1: &lt;rule number&gt;            マッチしたルールの優先度</p>

### (3) セキュリティフィルタ関連のメッセージフォーマット

セキュリティフィルタ関連のメッセージフォーマットは以下となります。

表 1-46 セキュリティフィルタ関連のメッセージフォーマット

種別	メッセージ 内容
セキュリティ フィルタ登録	<p>CEF:0 ALAXALA Networks Corporation AX-Security-Controller &lt;AX-Security-Controller のバージョン&gt; Action Registered the action 2 rt=&lt;MMM dd yyyy HH:mm:ss zzz&gt;  flexString1Label=SourceAddress flexString1=&lt;source address&gt;  flexString2Label=DestinationAddress flexString2=&lt;destination address&gt;  act=&lt;filter type&gt; cs1Label=Function cs1=&lt;function&gt; cs2Label=Request IP cs2=&lt;ip address&gt;</p> <p>[Extension Field]  rt: &lt;MMM dd yyyy HH:mm:ss zzz&gt;  イベント発生日時</p> <p>flexString1Label: SourceAddress  flexString1: &lt;source address&gt;  セキュリティフィルタの送信元アドレス条件(&lt;ip address&gt;/&lt;prefixlen&gt;), またはセキュリティフィルタの送信元 MAC アドレス条件(&lt;mac address&gt;)</p> <p>flexString2Label: DestinationAddress  flexString2: &lt;destination address&gt;  セキュリティフィルタの宛先アドレス条件(&lt;ip address&gt;/&lt;prefixlen&gt;), または flexString1 が送信元 MAC アドレス条件の場合は空白</p> <p>act: &lt;filter type&gt;  セキュリティフィルタ種別</p> <p>cs1Label: cs1 の説明  cs1: &lt;function&gt;  連携機能名称</p> <p>cs2Label: cs2 の説明  cs2: &lt;ip address&gt;  セキュリティフィルタの要求元 IP アドレス</p>

種別	メッセージ
	内容
セキュリティ フィルタ設定 完了	<p>CEF:0 ALAXALA Networks Corporation AX-Security-Controller &lt;AX-Security-Controller のバージョン&gt; Action Completed to set the action 2 rt=&lt;MMM dd yyyy HH:mm:ss zzz&gt;  flexString1Label=SourceAddress flexString1=&lt;source address&gt;  flexString2Label=DestinationAddress flexString2=&lt;destination address&gt;  act=&lt;filter type&gt; cs1Label=Function cs1=&lt;function&gt; cs2Label=Request IP cs2=&lt;ip address&gt; cs3Label=Host MAC cs3=&lt;mac address&gt;</p> <p>[Extension Field]  rt: &lt;MMM dd yyyy HH:mm:ss zzz&gt;  イベント発生日時  flexString1Label: SourceAddress  flexString1: &lt;source address&gt;  セキュリティフィルタの送信元アドレス条件(&lt;ip address&gt;/&lt;prefixlen&gt;), またはセキュリティフィルタの送信元 MAC アドレス条件(&lt;mac address&gt;)  flexString2Label: DestinationAddress  flexString2: &lt;destination address&gt;  セキュリティフィルタの宛先アドレス条件(&lt;ip address&gt;/&lt;prefixlen&gt;), または flexString1 が送信元 MAC アドレス条件の場合は空白  act: &lt;filter type&gt;  セキュリティフィルタ種別  cs1Label: cs1 の説明  cs1: &lt;function&gt;  連携機能名称  cs2Label: cs2 の説明  cs2: &lt;ip address&gt;  セキュリティフィルタの要求元 IP アドレス  cs3Label: cs3 の説明  cs3: &lt;mac address&gt;  端末 MAC アドレス</p>

種別	メッセージ
	内容
セキュリティ フィルタ削除 完了	<p>CEF:0 ALAXALA Networks Corporation AX-Security-Controller &lt;AX-Security-Controller のバージョン&gt; Action Completed to delete the action 2 rt=&lt;MMM dd yyyy HH:mm:ss zzz&gt;  flexString1Label=SourceAddress flexString1=&lt;source address&gt;  flexString2Label=DestinationAddress flexString2=&lt;destination address&gt;  act=&lt;filter type&gt; cs1Label=Function cs1=&lt;function&gt; cs2Label=Request IP cs2=&lt;ip address&gt; cs3Label=Host MAC cs3=&lt;mac address&gt;</p> <p>[Extension Field]  rt: &lt;MMM dd yyyy HH:mm:ss zzz&gt;  イベント発生日時  flexString1Label: SourceAddress  flexString1: &lt;source address&gt;  セキュリティフィルタの送信元アドレス条件(&lt;ip address&gt;/&lt;prefixlen&gt;), またはセキュリティフィルタの送信元 MAC アドレス条件(&lt;mac address&gt;)  flexString2Label: DestinationAddress  flexString2: &lt;destination address&gt;  セキュリティフィルタの宛先アドレス条件(&lt;ip address&gt;/&lt;prefixlen&gt;), または flexString1 が送信元 MAC アドレス条件の場合は空白  act: &lt;filter type&gt;  セキュリティフィルタ種別  cs1Label: cs1 の説明  cs1: &lt;function&gt;  連携機能名称  cs2Label: cs2 の説明  cs2: &lt;ip address&gt;  セキュリティフィルタの要求元 IP アドレス  cs3Label: cs3 の説明  cs3: &lt;mac address&gt;  端末 MAC アドレス</p>
端末毎設定要 因	<p>CEF:0 ALAXALA Networks Corporation AX-Security-Controller &lt;AX-Security-Controller のバージョン&gt; Action &lt;Name&gt; 2 rt=&lt;MMM dd yyyy HH:mm:ss zzz&gt; dvchost=&lt;host name&gt; act=&lt;filter type&gt;  cs1Label=Host IP cs1=&lt;ip address&gt; cs2Label=AccessList Name  cs2=&lt;accesslist name&gt; cs3Label=Direction cs3=&lt;direction&gt;  cs4Label=Sequence Number cs4=&lt;sequence number&gt;  cs5Label=Configuration cs5=&lt;configuration&gt; cs6Label=porttype  cs6=&lt;port type&gt;</p> <p>[Extension Field]  rt: &lt;MMM dd yyyy HH:mm:ss zzz&gt;  イベント発生日時  dvchost: &lt;host name&gt;  装置名称  act: &lt;filter type&gt;  セキュリティフィルタ種別  cs1Label: cs1 の説明  cs1: &lt;ip address&gt;  端末 IP アドレス (端末 IP アドレスが存在しない場合, 空白)</p>

種別	メッセージ
	内容
	<p>cs2Label: cs2 の説明      cs2: &lt;accesslist name&gt;          アクセリスト名称</p> <p>cs3Label: cs3 の説明      cs3: &lt;direction&gt;          検出方向</p> <p>cs4Label: cs4 の説明      cs4: &lt;sequence number&gt;          アクセリストのシーケンス番号</p> <p>cs5Label: cs5 の説明      cs5: &lt;configuration&gt;          検出条件</p> <p>cs6Label: cs6 の説明      cs6: &lt;port type&gt;          設定先のポート(wan / mirror / permanentportin / permanentportout / host)</p>
端末毎設定完了	<p>CEF:0 ALAXALA Networks Corporation AX-Security-Controller &lt;AX-Security-Controller のバージョン&gt; Action Completed to apply the configuration 2 rt=&lt;MMM dd yyyy HH:mm:ss zzz&gt; dvchost=&lt;host name&gt; act=&lt;filter type&gt; cs1Label=Host IP cs1=&lt;ip address&gt; cs2Label=AccessList Name cs2=&lt;accesslist name&gt; cs3Label=Direction cs3=&lt;direction&gt; cs4Label=Sequence Number cs4=&lt;sequence number&gt; cs5Label=Configuration cs5=&lt;configuration&gt; cs6Label=porttype cs6=&lt;port type&gt; axscSkipConfigurationReason=&lt;skip reason&gt;</p> <p>[Extension Field]</p> <p>rt: &lt;MMM dd yyyy HH:mm:ss zzz&gt;          イベント発生日時</p> <p>dvchost: &lt;host name&gt;          装置名称</p> <p>act: &lt;filter type&gt;          セキュリティフィルタ種別</p> <p>cs1Label: cs1 の説明      cs1: &lt;ip address&gt;          端末 IP アドレス (端末 IP アドレスが存在しない場合、空白)</p> <p>cs2Label: cs2 の説明</p>

種別	メッセージ
	内容
	<p>cs2: &lt;accesslist name&gt; アクセスリスト名称</p> <p>cs3Label: cs3 の説明</p> <p>cs3: &lt;direction&gt; 検出方向</p> <p>cs4Label: cs4 の説明</p> <p>cs4: &lt;sequence number&gt; アクセスリストのシーケンス番号</p> <p>cs5Label: cs5 の説明</p> <p>cs5: &lt;configuration&gt; 検出条件</p> <p>cs6Label: cs6 の説明</p> <p>cs6: &lt;port type&gt; 設定先のポート(wan / mirror / permanentportin / permanentportout / host)</p> <p>axscSkipConfigurationReason: &lt;skip reason&gt;</p> <p>none: コンフィグレーションを適用しました</p> <p>already applied: 既に適用済みのため、コンフィグレーションの適用をスキップしました</p>
端末毎設定失敗	<p>CEF:0 ALAXALA Networks Corporation AX-Security-Controller &lt;AX-Security-Controller のバージョン&gt; Action Failed to apply the configuration 4 rt=&lt;MMM dd yyyy HH:mm:ss zzz&gt; dvchost=&lt;host name&gt; act=&lt;filter type&gt; reason=&lt;reason&gt; cs1Label=Host IP cs1=&lt;ip address&gt; cs2Label=AccessList Name cs2=&lt;accesslist name&gt; cs3Label=Direction cs3=&lt;direction&gt; cs4Label=Sequence Number cs4=&lt;sequence number&gt; cs5Label=Configuration cs5=&lt;configuration&gt; cs6Label=porttype cs6=&lt;port type&gt;</p> <p>[Extension Field]</p> <p>rt: &lt;MMM dd yyyy HH:mm:ss zzz&gt; イベント発生日時</p> <p>dvchost: &lt;host name&gt; 装置名称</p> <p>act: &lt;filter type&gt; セキュリティフィルタ種別</p> <p>reason: &lt;reason&gt; 設定失敗要因</p> <p>cs1Label: cs1 の説明</p> <p>cs1: &lt;ip address&gt; 端末 IP アドレス (端末 IP アドレスが存在しない場合、空白)</p>

種別	メッセージ
	内容
	<p>cs2Label: cs2 の説明      cs2: &lt;accesslist name&gt;          アクセリスト名称</p> <p>cs3Label: cs3 の説明      cs3: &lt;direction&gt;          検出方向</p> <p>cs4Label: cs4 の説明      cs4: &lt;sequence number&gt;          アクセリストのシーケンス番号</p> <p>cs5Label: cs5 の説明      cs5: &lt;configuration&gt;          検出条件</p> <p>cs6Label: cs6 の説明      cs6: &lt;port type&gt;          設定先のポート(wan / mirror / permanentportin / permanentportout / host)</p>
端末毎削除要因	<p>CEF:0 ALAXALA Networks Corporation AX-Security-Controller &lt;AX-Security-Controller のバージョン&gt; Action &lt;Name&gt; 2 rt=&lt;MMM dd yyyy HH:mm:ss zzz&gt; dvchost=&lt;host name&gt; act=&lt;filter type&gt;      cs1Label=Host IP cs1=&lt;ip address&gt; cs2Label=AccessList Name      cs2=&lt;accesslist name&gt; cs3Label=Direction cs3=&lt;direction&gt;      cs4Label=Sequence Number cs4=&lt;sequence number&gt;      cs5Label=Configuration cs5=&lt;configuration&gt; cs6Label=porttype      cs6=&lt;port type&gt; axscSkipConfigurationReason=&lt;skip reason&gt;</p> <p>[Extension Field]      rt: &lt;MMM dd yyyy HH:mm:ss zzz&gt;          イベント発生日時</p> <p>dvchost: &lt;host name&gt;          装置名称</p> <p>act: &lt;filter type&gt;          セキュリティフィルタ種別</p> <p>cs1Label: cs1 の説明      cs1: &lt;ip address&gt;          端末 IP アドレス (端末 IP アドレスが存在しない場合、空白)</p>

種別	メッセージ
	内容
	cs2Label: cs2 の説明 cs2: <accesslist name> アクセスリスト名称 cs3Label: cs3 の説明 cs3: <direction> 検出方向 cs4Label: cs4 の説明 cs4: <sequence number> アクセスリストのシーケンス番号 cs5Label: cs5 の説明 cs5: <configuration> 検出条件 cs6Label: cs6 の説明 cs6: <port type> 設定先のポート(wan / mirror / permanentportin / permanentportout / host) axscSkipConfigurationReason: <skip reason> none: コンフィグレーションを削除しました currently applied: 他のコンフィグレーションが適用中のため、コンフィグレーションの削除をスキップしました

#### (4) 端末接続のメッセージフォーマット

端末接続のメッセージフォーマットは以下となります。

表 1-47 端末接続のメッセージフォーマット

種別	メッセージ
	内容
エイリアス未登録接続*	CEF:0 ALAXALA Networks Corporation AX-Security-Controller <AX-Security-Controller のバージョン> Host Connection of the unregistered host rt=<MMM dd yyyy HH:mm:ss zzz> dvchost=<host name> cs1Label=Port Number cs1=<port number> cs2Label=Port Alias cs2=<port alias> cs3Label=VLAN ID cs3=<vlan id> cs4Label=Host MAC cs4=<mac address> cs5Label=Host IP cs5=<ip address> [Extension Field] rt: <MMM dd yyyy HH:mm:ss zzz> イベント発生日時 dvchost: <host name> 接続装置名称 cs1Label: cs1 の説明 cs1: <port number> 接続装置のポート番号 cs2Label: cs2 の説明 cs2: <port alias> 接続装置のポート番号に対応するポートエイリアス(ポートエイリアスが未登録の場合、空白)

種別	メッセージ
	内容
	<p>cs3Label: cs3 の説明      cs3:          接続装置の VLAN ID(VLAN ID が未取得の場合、空白)</p> <p>cs4Label: cs4 の説明      cs4:          接続端末の MAC アドレス</p> <p>cs5Label: cs5 の説明      cs5:          接続端末の IP アドレス(IP アドレスが存在しない場合、空白)</p>

注※ :

任意の接続端末の Syslog 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。

## (5) 管理対象装置関連のメッセージフォーマット

管理対象装置関連のメッセージフォーマットは以下となります。

表 1-48 管理対象装置関連のメッセージフォーマット

種別	メッセージ
	内容
コンフィグ容量監視 <sup>※1※2</sup>	<p>CEF:0 ALAXALA Networks Corporation AX-Security-Controller &lt;AX-Security-Controller のバージョン&gt; Node Check configuration capacity 4 rt=&lt;MMM dd yyyy HH:mm:ss zzz&gt;      dvchost=&lt;host name&gt; dvc=&lt;ip address&gt; cs1Label=NodeType      cs1=&lt;node type&gt; cs2Label=TotalMemory cs2=&lt;total memory&gt;      cs3Label=AvailableMemory cs3=&lt;available memory&gt;      cs4Label=FragmentsMemory cs4=&lt;fragments memory&gt;</p> <p>[Extension Field]      rt: &lt;MMM dd yyyy HH:mm:ss zzz&gt;          コンフィグ容量を確認した日時</p> <p>dvchost: &lt;host name&gt;          管理対象装置名称</p> <p>cs1Label: cs1 の説明      cs1: &lt;node type&gt;          管理対象装置の装置モデル</p> <p>cs2Label: cs2 の説明      cs2: &lt;total memory&gt;          コンフィグレーションファイルとして利用できる全容量</p> <p>cs3Label: cs3 の説明      cs3: &lt;available memory&gt;          コンフィグレーションファイルとして利用できる残容量</p> <p>cs4Label: cs4 の説明      cs4: &lt;fragments memory&gt;          コンフィグレーションファイルの中で、削除などで断片化が発生した無効エリア容量</p>

注※1 :

下記装置モデルのコンフィグレーションの空き容量が全容量の 20%未満の場合に通知

- ・ AX8600S/AX8300S/AX4600S/AX3800S/AX3660S/AX3650S/X3640S

注※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。

## 1.8.2 E-mail 通知

AX-Security-Controller は、イベント発生および状態を E-mail 通知先に通知することができます。

表 1-49 E-mail 通知種別一覧

項目	説明
インシデント情報連携	インシデント情報連携で発生したイベントの E-mail を出力します。 送信契機は、イベント発生時です。
定期レポート	日、週、月単位に収集したレポート情報の E-mail を出力します。 送信契機は、下記です。 <ul style="list-style-type: none"> <li>・ 日単位：毎日 0:00 JST</li> <li>・ 週単位：毎週月曜日 0:00 JST</li> <li>・ 月単位：毎月 1 日 0:00 JST</li> </ul>
ライセンス関連	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。 <ul style="list-style-type: none"> <li>・ ライセンス失効 3 か月前 9:00 JST</li> <li>・ ライセンス失効 1 か月前 9:00 JST</li> <li>・ ライセンス失効 7 日前から毎日 9:00 JST</li> <li>・ ライセンス失効時 9:00 JST</li> </ul>
テストメール	Web インタフェースにより、E-mail 通知先のサーバへとテストメールの E-mail を出力します。 送信契機は、Web インタフェースによるボタン押下時です。
端末接続	端末関連の E-mail を出力します。 送信契機は、イベント発生時です。
管理対象装置関連	管理対象装置関連の E-mail を出力します。 送信契機は、イベント発生時です。

### (1) プロトコル

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 1-50 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 1-51 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。

### (2) メールヘッダの共通フォーマット

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 1-52 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

### (3) インシデント情報連携メッセージフォーマット

インシデント情報連携のメッセージフォーマットは以下となります。

表 1-53 インシデント情報連携のメッセージフォーマット

Subject	本文 内容
インシデント発生(通信遮断)	<p>受信日時 : &lt;受信日時&gt;          クライアント名称 : &lt;クライアント名称&gt;          クライアント種別 : &lt;クライアント種別&gt;          セグメント名称 : &lt;セグメント名称&gt;          ルール優先度 : &lt;ルール優先度&gt;          セキュリティフィルタ条件 : &lt;セキュリティフィルタ条件&gt;          ログ : &lt;受信 Syslog&gt;</p> <p>&lt;受信日時&gt;          インシデント検知日時          &lt;クライアント名称&gt;          Syslog を受信したクライアント名称          &lt;クライアント種別&gt;          Syslog を受信したクライアント種別          &lt;セグメント名称&gt;          インシデントが発生したセグメント名称          &lt;ルール優先度&gt;          マッチしたルール優先度          &lt;セキュリティフィルタ条件&gt;          登録セキュリティフィルタ条件          &lt;受信 Syslog&gt;          受信した Syslog</p>
インシデント発生(詳細ミラー)	<p>受信日時 : &lt;受信日時&gt;          クライアント名称 : &lt;クライアント名称&gt;          クライアント種別 : &lt;クライアント種別&gt;          セグメント名称 : &lt;セグメント名称&gt;          ルール優先度 : &lt;ルール優先度&gt;          セキュリティフィルタ条件 : &lt;セキュリティフィルタ条件&gt;          ログ : &lt;受信 Syslog&gt;</p> <p>&lt;受信日時&gt;          インシデント検知日時          &lt;クライアント名称&gt;          Syslog を受信したクライアント名称          &lt;クライアント種別&gt;          Syslog を受信したクライアント種別          &lt;セグメント名称&gt;          インシデントが発生したセグメント名称          &lt;ルール優先度&gt;          マッチしたルール優先度          &lt;セキュリティフィルタ条件&gt;          登録セキュリティフィルタ条件          &lt;受信 Syslog&gt;          受信した Syslog</p>

Subject	<b>本文</b>
	<b>内容</b>
インシデント発生(手動選択)	<p>受信日時 : &lt;受信日時&gt;          クライアント名称 : &lt;クライアント名称&gt;          クライアント種別 : &lt;クライアント種別&gt;          セグメント名称 : &lt;セグメント名称&gt;          ルール優先度 : &lt;ルール優先度&gt;          セキュリティフィルタ条件 : &lt;セキュリティフィルタ条件&gt;          ログ : &lt;受信 Syslog&gt;</p> <p>&lt;受信日時&gt;            インシデント検知日時            &lt;クライアント名称&gt;              Syslog を受信したクライアント名称            &lt;クライアント種別&gt;              Syslog を受信したクライアント種別            &lt;セグメント名称&gt;              インシデントが発生したセグメント名称            &lt;ルール優先度&gt;              マッチしたルール優先度            &lt;セキュリティフィルタ条件&gt;              空白            &lt;受信 Syslog&gt;              受信した Syslog</p>

#### (4) 定期レポートメッセージフォーマット

定期レポートのメッセージフォーマットは以下となります。

表 1-54 定期レポートのメッセージフォーマット

Subject	本文 内容
日間セキュリティレポート(<収集日>)	<p>日間セキュリティレポート(&lt;収集開始日時&gt;～&lt;収集終了日時&gt;)</p> <p>■インシデント連携統計(インシデント発生件数)      合計 : &lt;インシデント発生件数(合計)&gt;      Syslog 連携(CEF) : &lt;インシデント発生件数(CEF)&gt;      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 : &lt;インシデント発生件数(Palo)&gt;</p> <p>■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)      合計 : &lt;セキュリティフィルタ統計(合計)&gt;      Syslog 連携(CEF) : &lt;セキュリティフィルタ統計(CEF)&gt;      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 : &lt;セキュリティフィルタ統計(Palo)&gt;      TMPM 連携 : &lt;セキュリティフィルタ統計(TMPM)&gt;      手動追加 : &lt;セキュリティフィルタ統計(手動)&gt;</p> <p>■インシデント情報詳細(最新 10 件)      受信日時 : &lt;受信日時&gt;      クライアント名称 : &lt;クライアント名称&gt;      クライアント種別 : &lt;クライアント種別&gt;      セグメント名称 : &lt;セグメント名称&gt;      セキュリティフィルタ条件 : &lt;セキュリティフィルタ条件&gt;      ログ : &lt;受信 Syslog&gt;</p> <p>受信日時 : &lt;受信日時&gt;      クライアント名称 : &lt;クライアント名称&gt;      クライアント種別 : &lt;クライアント種別&gt;      セグメント名称 : &lt;セグメント名称&gt;      セキュリティフィルタ条件 : &lt;セキュリティフィルタ条件&gt;      ログ : &lt;受信 Syslog&gt;</p> <p>:</p> <p>&lt;収集日&gt;      収集日(YYYY/mm/dd 形式)      &lt;収集開始日時&gt;      収集開始日時(YYYY/mm/dd HH:MM:SS 形式)      &lt;収集終了日時&gt;      収集終了日時(YYYY/mm/dd HH:MM:SS 形式)      &lt;インシデント発生件数(合計)&gt;      収集対象期間に発生を検知したインシデント件数(&lt;件数&gt;件)<sup>*1</sup>      ※1: 「Syslog 連携(CEF)」または「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」のライセンス有効時のみ出力</p>

Subject	本文 内容
	<p>&lt;インシデント発生件数(CEF)&gt;      収集対象期間に Syslog 連携(CEF)の Syslog クライアントで発生を検知したインシデント件数(&lt;件数&gt;件)<sup>※2</sup>      ※2: 「Syslog 連携(CEF)」のライセンス有効時のみ出力</p> <p>&lt;インシデント発生件数(Palo)&gt;      収集対象期間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の Syslog クライアントで発生を検知したインシデント件数(&lt;件数&gt;件)<sup>※3</sup>      ※3: 「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」のライセンス有効時のみ出力</p> <p>&lt;セキュリティフィルタ統計(合計)&gt;      収集終了時点での設定済みセキュリティフィルタ件数、収集対象期間に登録/解除したセキュリティフィルタ件数(&lt;設定済み件数&gt;件/&lt;登録件数&gt;件/&lt;解除件数&gt;件)</p> <p>&lt;セキュリティフィルタ統計(CEF)&gt;      連携機能が Syslog 連携(CEF)のセキュリティフィルタに対する設定済み/登録/解除件数(&lt;設定済み件数&gt;件/&lt;登録件数&gt;件/&lt;解除件数&gt;件)<sup>※4</sup>      ※4: 「Syslog 連携(CEF)」のライセンス有効時のみ出力</p> <p>&lt;セキュリティフィルタ統計(Palo)&gt;      連携機能が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のセキュリティフィルタに対する設定済み/登録/解除件数(&lt;設定済み件数&gt;件/&lt;登録件数&gt;件/&lt;解除件数&gt;件)<sup>※5</sup>      ※5: 「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」のライセンス有効時のみ出力</p> <p>&lt;セキュリティフィルタ統計(TMPM)&gt;      連携機能が TMPM 連携のセキュリティフィルタに対する設定済み/登録/解除件数(&lt;設定済み件数&gt;件/&lt;登録件数&gt;件/&lt;解除件数&gt;件)<sup>※6</sup>      ※6: 「外部連携トレンドマイクロ DDI/TMPM との連携」のライセンス有効時のみ出力</p> <p>&lt;セキュリティフィルタ統計(手動)&gt;      連携機能が手動追加のセキュリティフィルタに対する設定済み/登録/解除件数(&lt;設定済み件数&gt;件/&lt;登録件数&gt;件/&lt;解除件数&gt;件)</p> <p>&lt;受信日時&gt;      インシデント検知日時</p> <p>&lt;クライアント名称&gt;      Syslog を受信したクライアント名称</p> <p>&lt;クライアント種別&gt;      Syslog を受信したクライアント種別</p> <p>&lt;セグメント名称&gt;      インシデントが発生したセグメント名称</p> <p>&lt;セキュリティフィルタ条件&gt;      登録セキュリティフィルタ条件</p> <p>&lt;受信 Syslog&gt;      受信した Syslog</p>

Subject	本文 内容
週間セキュリティレポート(<収集期間>)	<p>週間セキュリティレポート(&lt;収集開始日時&gt;～&lt;収集終了日時&gt;)</p> <p>■インシデント連携統計(インシデント発生件数)      合計 : &lt;インシデント発生件数(合計)&gt;      Syslog 連携(CEF) : &lt;インシデント発生件数(CEF)&gt;      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 : &lt;インシデント発生件数(Palo)&gt;</p> <p>■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)      合計 : &lt;セキュリティフィルタ統計(合計)&gt;      Syslog 連携(CEF) : &lt;セキュリティフィルタ統計(CEF)&gt;      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 : &lt;セキュリティフィルタ統計(Palo)&gt;      TMPM 連携 : &lt;セキュリティフィルタ統計(TMPM)&gt;      手動追加 : &lt;セキュリティフィルタ統計(手動)&gt;</p> <p>■インシデント連携統計情報内訳(日単位)      収集日 : 発生件数      YYYY/mm/dd : &lt;件数&gt;      YYYY/mm/dd : &lt;件数&gt;      :      YYYY/mm/dd : &lt;件数&gt;</p> <p>■セキュリティフィルタ統計情報内訳(日単位)      収集日 : 設定済み件数/登録件数/解除件数      YYYY/mm/dd : &lt;設定済み件数&gt;/&lt;登録件数&gt;/&lt;解除件数&gt;      YYYY/mm/dd : &lt;設定済み件数&gt;/&lt;登録件数&gt;/&lt;解除件数&gt;      :      &lt;収集期間&gt;      収集期間(YYYY/mm/dd～YYYY/mm/dd 形式)      &lt;収集開始日時&gt;      &lt;収集終了日時&gt;      &lt;インシデント発生件数(合計)&gt;      &lt;インシデント発生件数(CEF)&gt;      &lt;インシデント発生件数(Palo)&gt;      &lt;セキュリティフィルタ統計(合計)&gt;      &lt;セキュリティフィルタ統計(CEF)&gt;      &lt;セキュリティフィルタ統計(Palo)&gt;      &lt;セキュリティフィルタ統計(TMPM)&gt;      &lt;セキュリティフィルタ統計(合計)&gt;      日間セキュリティレポート(&lt;収集日&gt;)の各説明を参照</p>

Subject	本文 内容
月間セキュリティレポート(<収集期間>)	<p>月間セキュリティレポート(&lt;収集開始日時&gt;～&lt;収集終了日時&gt;)</p> <p>■インシデント連携統計(インシデント発生件数)      合計 : &lt;インシデント発生件数(合計)&gt;      Syslog 連携(CEF) : &lt;インシデント発生件数(CEF)&gt;      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 : &lt;インシデント発生件数(Palo)&gt;</p> <p>■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)      合計 : &lt;セキュリティフィルタ統計(合計)&gt;      Syslog 連携(CEF) : &lt;セキュリティフィルタ統計(CEF)&gt;      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 : &lt;セキュリティフィルタ統計(Palo)&gt;      TMPM 連携 : &lt;セキュリティフィルタ統計(TMPM)&gt;      手動追加 : &lt;セキュリティフィルタ統計(手動)&gt;</p> <p>■インシデント連携統計情報内訳(週単位)      収集期間 : 発生件数      YYYY 年 mm 月 第 1 週 : &lt;件数&gt;      :      ■セキュリティフィルタ統計情報内訳(週単位)      収集期間 : 設定済み件数/登録件数/解除件数      YYYY 年 mm 月 第 1 週 : &lt;設定済み件数&gt;/&lt;登録件数&gt;/&lt;解除件数&gt;      YYYY 年 mm 月 第 2 週 : &lt;設定済み件数&gt;/&lt;登録件数&gt;/&lt;解除件数&gt;      :      ■インシデント連携統計情報内訳(日単位)      収集日 : 発生件数      YYYY/mm/dd : &lt;件数&gt;      YYYY/mm/dd : &lt;件数&gt;      :      ■セキュリティフィルタ統計情報内訳(日単位)      収集日 : 設定済み件数/登録件数/解除件数      YYYY/mm/dd : &lt;設定済み件数&gt;/&lt;登録件数&gt;/&lt;解除件数&gt;      YYYY/mm/dd : &lt;設定済み件数&gt;/&lt;登録件数&gt;/&lt;解除件数&gt;      :</p>

Subject	本文
	内容
	<p>&lt;収集期間&gt; 収集期間(YYYY/mm/dd～YYYY/mm/dd 形式)</p> <p>&lt;収集開始日時&gt;</p> <p>&lt;収集終了日時&gt;</p> <p>&lt;インシデント発生件数(合計)&gt;</p> <p>&lt;インシデント発生件数(CEF)&gt;</p> <p>&lt;インシデント発生件数(Palo)&gt;</p> <p>&lt;セキュリティフィルタ統計(合計)&gt;</p> <p>&lt;セキュリティフィルタ統計(CEF)&gt;</p> <p>&lt;セキュリティフィルタ統計(Palo)&gt;</p> <p>&lt;セキュリティフィルタ統計(TMPM)&gt;</p> <p>&lt;セキュリティフィルタ統計(合計)&gt;</p> <p>日間セキュリティレポート(&lt;収集日&gt;)の各説明を参照</p>

## (5) ライセンス関連メッセージフォーマット

ライセンス関連のメッセージフォーマットは以下となります。

表 1-55 ライセンス関連のメッセージフォーマット

Subject	本文
	内容
<ライセンス失効までの期間>後に ライセンスが失効します	<p>ライセンス種別(シリアル) : &lt;ライセンス種別&gt;(&lt;シリアル番号&gt;)</p> <p>　　－延長ライセンス種別(シリアル) : &lt;ライセンス種別&gt;(&lt;シリアル番号&gt;)</p> <p>　　：</p> <p>　　延長ライセンスが複数ある場合、延長ライセンス分を列挙 有効期限 : &lt;有効期限&gt;</p> <p>ライセンスが&lt;ライセンス失効までの期間&gt;後に失効します。 延長ライセンスを追加してください。</p>
	<p>&lt;ライセンス種別&gt; 　　ライセンスの種類 &lt;シリアル番号&gt; 　　ライセンスのシリアル番号 &lt;有効期限&gt; 　　ライセンスが失効する日時</p>

Subject	本文 内容
ライセンスが失効しました	<p>ライセンス種別(シリアル) : &lt;ライセンス種別&gt;(&lt;シリアル番号&gt;)</p> <p>　　－延長ライセンス種別(シリアル) : &lt;ライセンス種別&gt;(&lt;シリアル番号&gt;)</p> <p>　　：</p> <p>　　延長ライセンスが複数ある場合、延長ライセンス分を列挙</p> <p>有効期限 : &lt;有効期限&gt;</p> <p>ライセンスが失効しました。</p> <p>&lt;ライセンス種別&gt;           　　ライセンスの種類           　　&lt;シリアル番号&gt;           　　ライセンスのシリアル番号           　　&lt;有効期限&gt;           　　ライセンスが失効する日時</p>

## (6) テストメールメッセージフォーマット

テストメールのメッセージフォーマットは以下となります。

表 1-56 テストメールのメッセージフォーマット

Subject	本文 内容
AX-Security-Controller 接続テスト	<p>AX-Security-Controller 接続テスト</p> <p>通知先名称 : &lt;通知先名称&gt;            送信日時 : &lt;送信日時&gt;</p> <p>&lt;通知先名称&gt;            通知先名称            &lt;送信日時&gt;            メールを送信した日時</p>

## (7) 端末接続メッセージフォーマット

端末接続のメッセージフォーマットは以下となります。

表 1-57 端末接続のメッセージフォーマット

Subject	本文 内容
エイリアス未登録端末の接続を検知しました	<p>接続日時 : &lt;接続日時&gt;      通知抑止満了日時 : &lt;通知抑止満了日時&gt;      接続端末数 : &lt;host number&gt;台</p> <p>■接続装置名称 : &lt;host name&gt;      ポート番号 : &lt;port number&gt;      ポートエイリアス : &lt;port alias&gt;      VLAN ID : &lt;vlan id&gt;</p> <p>端末 MAC アドレス : &lt;mac address&gt;, 端末 IP アドレス :      &lt;ip address&gt;      :      端末 MAC アドレスが複数ある場合, 端末 MAC アドレス      数分を列挙</p> <p>エイリアス未登録端末の接続を検知しました。</p> <p>&lt;接続日時&gt;      エイリアス未登録端末の接続を検知した日時      &lt;通知抑止満了日時&gt;      通知抑止が満了する日時      &lt;host number&gt;      エイリアス未登録端末の接続数      &lt;host name&gt;      接続装置名称      &lt;port number&gt;      接続装置のポート番号      &lt;port alias&gt;      接続装置のポート番号に対応するポートエイリアス(ポートエイリアスが未登録の場合, 空白)      &lt;vlan id&gt;      接続装置の VLAN ID(VLAN ID が未取得の場合, 空白)      &lt;mac address&gt;      接続端末の MAC アドレス      &lt;ip address&gt;      接続端末の IP アドレス(IP アドレスが存在しない場合, 空白)</p>

注※ :

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。

## (8) 管理対象装置関連メッセージフォーマット

管理対象装置関連のメッセージフォーマットは以下となります。

表 1-58 管理対象装置関連のメッセージフォーマット

Subject	本文 内容
コンフィグ容量 監視※1※2	<p>管理対象装置名称 : &lt;装置名称&gt;      管理対象装置 IP アドレス : &lt;ip address&gt;      管理対象装置モデル : &lt;装置モデル&gt;</p> <p>■コンフィグ容量      &lt;コンフィグ容量&gt;</p> <p>管理対象装置のコンフィグレーションが編集不可となる可能性があります。      コンフィグレーションの save を行ってください。</p> <p>&lt;装置名称&gt;      管理対象装置名称      &lt;ip address&gt;      管理対象装置の IP アドレス      &lt;装置モデル&gt;      管理対象装置の装置モデル      &lt;コンフィグ容量&gt;      管理対象装置のコンフィグレーション容量</p>

注※1 :

下記装置モデルのコンフィグレーションの空き容量が全容量の 20%未満の場合に通知

- AX8600S/AX8300S/AX4600S/AX3800S/AX3660S/AX3650S/AX3640S

注※2 :

任意の管理対象装置の E-mail 通知を通知すると、翌日 0:00 まで、当該管理対象装置の通知を抑止します。

## 1.9 レポート

### 1.9.1 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できます。

セキュリティレポートは、E-mail (1.8.2) や、Web インタフェース(6.1.8(3))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 1-59 セキュリティレポートの収集契機

項目	契機	説明
日単位	毎日 0:00 JST	前日の 0:00 JST から、23:59 JST までの情報を収集します
週単位	毎週月曜日 0:00 JST	前週の月曜日 0:00 JST から、日曜日 23:59 JST までの情報を収集します
月単位	毎月 1 日 0:00 JST	先月の 1 日 0:00 JST から、月末 23:59 JST までの情報を収集します

表 1-60 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。

注※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。

注※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、TPMP 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、TPMP 連携は、ライセンス有効時に出力します。

表 1-61 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 <sup>※2</sup> 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 <sup>※2</sup> を出力します。

注※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。

注※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 1-62 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 <sup>※1</sup> 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 <sup>※2</sup> 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 <sup>※1</sup> 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 <sup>※2</sup> 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 <sup>※1</sup> 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 <sup>※2</sup> を出力します。

注※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。

注※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、TPMP 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、TPMP 連携は、ライセンス有効時に出力します。

## 1.10 端末移動履歴機能

### 1.10.1 移動履歴

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。

表 1-63 移動履歴に含まれる情報

項目	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）

なお、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

## 1.11 ライセンス

### 1.11.1 ライセンスの構成

AX-Security-Controller 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、下記のライセンスからなります。

表 1-64 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)

### 1.11.2 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 1-65 ライセンスの使用期間例

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)
外部連携ライセンス (初年度ライセンス)	外部連携ライセンス (1年延長ライセンス)



## 2. 動作条件

---

この章では、AX-Security-Controller の動作条件とする収容条件と使用可能ウェブブラウザについて説明します。

---

## 2.1 収容条件

### 2.1.1 管理対象ネットワーク

管理するネットワークに関する AX-Security-Controller の収容条件を次に示します。

表 2-1 管理対象ネットワークに関する収容条件

#	項目	収容条件
1	管理対象装置数 <sup>※1※2※5</sup>	最大 1000 装置
2	WAN 接続ポート数 <sup>※3※4</sup>	最大 64 ポート
3	セキュリティ装置単位ミラー先ポート <sup>※3</sup>	最大 5 ポート
4	永続設定ポート(受信側)数 <sup>※3※4</sup>	最大 64 ポート
5	永続設定ポート(送信側)数 <sup>※3※4</sup>	最大 64 ポート
6	管理対象外ポート <sup>※3※4</sup>	最大 64 ポート

注※1 管理対象スイッチ拡張ライセンスにより、上表の値より大きい値を登録しても、動作保証する管理対象装置数は上表の値となります。

注※2 1000 装置以上の環境で動作させたい場合、担当営業に問い合わせください。

注※3 リンクアグリゲーションポートの場合は、構成する物理ポート分の数で勘定します。

注※4 上表の値より大きい値を登録しても、動作保証するポート数は上表の値となります。

注※5 管理対象装置は、装置の構成(冗長構成やスタッカ構成)にかかわらず、AX-Security-Controller に登録する IP アドレス 1 つで 1 台と数えます。

### 2.1.2 Syslog

Syslog に関する AX-Security-Controller の収容条件を次に示します。

表 2-2 Syslog に関する収容条件

#	項目	収容条件
1	Syslog クライアント数	最大 10 クライアント
2	Syslog サーバ数	最大 10 サーバ
3	受信 Syslog 保持数	最大 10,000 メッセージ <sup>※</sup>

注※：すべての Syslog クライアントの合計で保持する値です。

### 2.1.3 インシデント抽出ルール

インシデント抽出ルールに関する、Syslog クライアントごとの AX-Security-Controller の収容条件を次に示します。

表 2-3 インシデント抽出ルールに関する収容条件

#	項目	収容条件
1	インシデント抽出ルール数	1000
2	ルール内に記載できる条件の種類数	最大 6 種類
3	ユーザ定義拡張フィールド数	10

### 2.1.4 端末移動履歴

端末移動履歴に関する AX-Security-Controller の収容条件を次に示します。

表 2-4 端末移動履歴に関する収容条件

#	項目	収容条件
1	履歴保存期間	最大 3650 日 <sup>*1</sup>
2	履歴の保存量 (履歴保存対象の端末数、端末移動の発生頻度)	ハードディスクの空き容量の許す限り <sup>*2</sup>

注※1 1～3650 の指定履歴保存期間+1 日以上前の履歴は、ハードディスクの残量に係わらず、自動で削除されます。

注※2 下記のバイト数以上の空き領域がハードディスクに必要です。ハードディスク容量をオーバーすると新しい履歴が記録できなくなるため、ハードディスクの空き容量を十分に確保した上で運用してください。

1 端末の 1 日あたりの通信開始/終了頻度(回/日/端末) × 指定履歴保存期間(日) × 端末数 × 1<sup>\*3</sup>[Kbyte/回]

注※3 エイリアス未使用時の消費量。使用しているエイリアスの大きさで最大 64Kbyte まで消費します。

### 2.1.5 セグメント

管理する個別セグメントに関する AX-Security-Controller の収容条件を次に示します。

表 2-5 セグメントに関する収容条件

#	項目	収容条件
1	個別セグメント数 <sup>*1</sup>	最大 10

#	項目	収容条件
2	インシデント抽出ルール数	1000(セグメント単位)
3	永続設定ポート(受信側)数 <sup>※1※2</sup>	最大 64 ポート(セグメント単位)
4	永続設定ポート(送信側)数 <sup>※1※2</sup>	最大 64 ポート(セグメント単位)
5	セキュリティフィルタ自動解除スケジュール数	最大 1(セグメント単位)

注※1 上表の値より大きい値を登録しても、動作可能なセグメント数は上表の値となります。なお信頼済みセグメント、および無所属セグメントは、この収容条件の数に含みません。

注※1 リンクアグリゲーションポートの場合は、構成する物理ポート分の数で勘定します。

注※2 上表の値より大きい値を登録しても、動作保証するポート数は上表の値となります。

## 2.1.6 マップ

マップに関する AX-Security-Controller の収容条件を次に示します。

表 2-6 マップに関する収容条件

#	項目	収容条件
1	マップ数	500
2	マップあたりの表示対象数 <sup>※1</sup>	500
3	マップあたりの背景画像ファイルサイズ <sup>※2</sup>	1MB
4	アイコン画像ファイル登録数	8000
5	アイコン画像ファイルサイズ <sup>※2</sup>	500KB

注※1：管理対象装置+端末の台数です。動作保証する表示対象数は上表の値となります。

注※2：背景画像ファイルサイズの合計と、アイコン画像ファイルサイズの合計の空き領域がハードディスクに必要です。ハードディスク容量をオーバーすると新しい背景画像ファイルやアイコン画像ファイルが登録できなくなるため、ハードディスクの空き容量を十分に確保した上で運用してください。

## 2.1.7 E-mail

E-mail に関する AX-Security-Controller の収容条件を次に示します。

表 2-7 E-mail に関する収容条件

#	項目	収容条件
1	E-mail 通知先数	最大 10

### 2.1.8 エイリアス

エイリアスに関する AX-Security-Controller の収容条件を次に示します。

表 2-8 エイリアスに関する収容条件

#	項目	収容条件
1	エイリアスのタイトル数	最大 16

---

## 2.2 使用可能なウェブブラウザ

### 2.2.1 AX-Security-Controller(Manager)で使用可能なウェブブラウザ

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

表 2-9 使用可能なウェブブラウザ

ウェブブラウザ
Firefox 68 ESR (Extended Support Release)
Firefox 78 ESR
Google Chrome (最新版)

### 2.2.2 AX-Security-Controller(Viewer)で使用可能なウェブブラウザ

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

表 2-10 使用可能なウェブブラウザの条件

ウェブブラウザの条件
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
HTML5 が解釈可能であること
CSS3 が解釈可能であること
JavaScript(ECMA Script 2015)が解釈可能であること

### 2.2.3 AX-Security-Controller(Tracker)で使用可能なウェブブラウザ

AX-Security-Controller(Tracker)で使用可能なウェブブラウザの条件を次に示します。

表 2-11 使用可能なウェブブラウザ

ウェブブラウザ
Firefox 68 ESR
Firefox 78 ESR
Google Chrome (最新版)

### 3. 管理対象装置の事前準備・設定

---

この章では、管理対象装置であるスイッチの事前準備・設定について説明します。

---

### 3.1 概要

ここでは、AX-Security-Controller が管理対象装置から情報を収集、およびフィルタのコンフィグレーション設定をおこなう上で、管理対象装置共通の設定、および管理対象装置個別の設定について説明します。

## 3.2 管理対象装置共通の事前準備

管理対象装置共通の事前準備を説明します。

### 3.2.1 SSH

#### (1) 設定内容

AX-Security-Controller は、管理対象装置へと以下のユーザ認証方法を使用して、コンフィグレーション設定、および装置モデルに応じて情報収集を行います。

表 3-1 ユーザ認証方法

項目	SSH プロトコルバージョン	説明
パスワード認証	v2	ローカルパスワード認証

管理対象装置は、SSH の有効化とリモートアクセス許可のコンフィグレーションを設定する必要があります。

なおリモートアクセス許可設定時において、ログインできるユーザ数は、AX-Security-Controller がログインする数を考慮した上で、設定してください。なお、AX-Security-Controller が 1 装置に対して同時にログインする数は最大 2 ユーザです。

#### (2) 設定対象外装置

管理対象装置が下記の場合、本設定は不要です。

表 3-2 設定対象外装置

管理対象装置
標準 MIB 対応装置
標準 MIB 対応装置(VLAN 每コミュニティ)
ワイヤレス LAN コントローラ

### 3.2.2 SNMP

#### (1) 設定内容

AX-Security-Controller は、管理対象装置へと以下の SNMP バージョンのオペレーションにより情報の収集を行います。

表 3-3 SNMP バージョン

SNMP バージョン
SNMPv2C

管理対象装置は、SNMP エージェント機能を有効化するコンフィグレーションを設定する必要があります。

### 3.2.3 LLDP

#### (1) 設定内容

AX-Security-Controller では、LLDP の隣接情報を利用してトポロジ計算を行います。管理対象装置は、隣接する管理対象装置とのイーサネットポートについて LLDP を有効化するコンフィグレーションを設定する必要があります。

隣接する管理対象装置との接続をリンクアグリゲーションにより構成する場合、リンクアグリゲーションを構成するすべてのイーサネットポートについて LLDP を有効化するコンフィグレーションを設定してください。

#### (2) 設定対象外装置

管理対象装置が下記の場合、本設定は不要です。「1.3.1(5) 接続情報」の設定をおこなってください。

表 3-4 設定対象外装置

管理対象装置
AX4600S (スタック構成で使用)(Ver. 11.15.F より前)
AX3800S (スタック構成で使用)
AX3660S (スタック構成で使用)(Ver. 12.1.F より前)
AX3650S (スタック構成で使用)
AX620R
標準 MIB 対応装置*
標準 MIB 対応装置(VLAN 毎コミュニティ) *
ワイヤレス LAN コントローラ

注※：管理対象装置で LLDP が動作しない場合、設定対象外となります。および「1.3.1(5)(a) アクセスリスト拡張ポート」の設定が必要なポートの場合、当該ポートは設定対象外となります。

### 3.2.4 アクセスリスト

#### (1) 設定内容

AX-Security-Controller は、セキュリティフィルタの反映に、管理対象装置のアクセスリストに permit または deny のコンフィグレーションの設定をおこなうことで実現します。

このため、事前に管理対象装置に以下 2 つの設定をおこなう必要があります。

表 3-5 アクセスリストの設定

項目	説明
アクセスリストの作成	<ul style="list-style-type: none"> <li>• 通常モード、または遮断専用モードにより、(a)通常モードまたは(b)通信遮断専用モードに示す専用アクセスリストを作成してください。なお、専用アクセスリストの名称により、設定するフィルタ種別が決まります。アクセスリスト名称は AUTO_ACL_&lt;種別&gt;_...であり、&lt;種別&gt;毎のフィルタ種別を以下に示します(AX620R を除く)。           <ul style="list-style-type: none"> <li>IPV4: IPv4 パケットフィルタ</li> <li>IPV6: IPv6 フィルタ</li> <li>MAC: MAC フィルタ</li> <li>ADVANCE: Advance フィルタ</li> </ul> </li> <li>専用アクセスリストは、シーケンス番号空間として、以下の範囲を AX-Security-Controller(Manager)が使用するのに予約します。ネットワーク管理者は、下記の範囲を使用しないでください(AXprimoM210、および AX620R を除く)。およびシーケンス番号を再設定するコンフィグレーションコマンド(例 : ip access-list resequence)を使用しないようにしてください。           <ul style="list-style-type: none"> <li>100000–163999 : 例外通信許可の設定に使用</li> <li>200000–263999 : 詳細ミラーの設定に使用</li> <li>300000–363999 : 通信遮断の設定に使用</li> </ul> </li> </ul>

項目	説明
	<ul style="list-style-type: none"> <li>ネットワーク管理者は、AXprimoM210、およびAX620Rに対し、専用アクセリストのフィルタの編集をおこなわないようしてください。</li> <li>端末を収容するイーサネットポートに適用するアクセリストの場合、上記の予約シーケンス番号より大きい値のシーケンス番号で、全通信アクセス許可のエントリを作成してください(AXprimoM210を除く)。</li> <li>AX620Rの場合、適用するアクセリストのシーケンス番号より大きい値のシーケンス番号で、全通信アクセス許可のエントリを作成してください。</li> <li>WAN接続ポートのイーサネットポートに適用するアクセリストの場合、上記の予約シーケンス番号より大きい値のシーケンス番号で、全通信アクセス許可のエントリを作成してください。</li> <li>セキュリティ装置へのミラー先ポートに適用するアクセリストの場合、上記の予約シーケンス番号より大きい値のシーケンス番号で、全通信アクセス拒否のエントリを作成してください。</li> <li>永続設定ポート(受信側/送信側)のイーサネットポートに適用するアクセリストの場合、上記の予約シーケンス番号より大きい値のシーケンス番号で、全通信アクセス許可のエントリを作成してください(AXprimoM210を除く)。</li> <li>AX620Rの場合、適用するアクセリストのシーケンス番号より大きい値のシーケンス番号で、全通信アクセス許可のエントリを作成してください。</li> </ul>
ポートへのアクセリストの適用	<p>下記のイーサネットポートに、作成したアクセリストを適用してください。</p> <ul style="list-style-type: none"> <li>端末を収容するイーサネットポート(Inbound)</li> <li>WAN接続ポートのイーサネットポート(Inbound, Outbound)</li> <li>セキュリティ装置へのミラー先ポートのイーサネットポート(Outbound)</li> <li>永続設定ポート(受信側)のイーサネットポート(Inbound)</li> <li>永続設定ポート(送信側)のイーサネットポート(Outbound)</li> <li>アクセリスト拡張ポート(Inbound)</li> </ul>

アクセリスト名称と、適用するポートについて下記に説明します。

#### (a) 通常モード

適用するアクセリスト名称は、管理対象装置の装置モデルにより異なります。

なお、IPv6のアクセリスト名称は、起動パラメータ「--accesslist-mode v4-v6」を指定している場合のみ必要です。

<検出方向>は、INまたはOUTになります。

① AX4600S・AX3800S・AX3660S・AX3650S・AX2500S(スタック使用時)

AUTO\_ACL\_IPV4\_<検出方向>\_<switch no.>\_0\_<port no.>

AUTO\_ACL\_IPV6\_<検出方向>\_<switch no.>\_0\_<port no.>

② AX8600S・AX8300S

AUTO\_ACL\_ADVANCE\_<検出方向>\_<nif no.>\_<port no.>

③ AX260A・AX3640S・AX2500S(スタック未使用時)

AUTO\_ACL\_IPV4\_<検出方向>\_0\_<port no.>

AUTO\_ACL\_IPV6\_<検出方向>\_0\_<port no.>

④ AX2200S・AX2100S

AUTO\_ACL\_IPV4\_<検出方向>\_0\_<port no.>

⑤ AXPrimoM210

AUTO\_ACL\_IPV4\_IN\_1\_<port no.>

AUTO\_ACL\_IPV6\_IN\_1\_<port no.>

AX620R は、以下となります。

- GigaEthernet/FastEthernet の場合

<ACL 種別><検出方向>eth<slot><port><sub-if><フィルタ種別>

- Tunnel の場合

<ACL 種別><検出方向>tun<device>00<フィルタ種別>

表 3-6 AX620R のアクセリスト名称のフィールドの説明

項目	値	説明
ACL 種別	ip4	IPv4 パケットに対するフィルタを示します。
	ip6	IPv6 パケットに対するフィルタを示します。
検出方向	i	Inbound 側へのフィルタを示します。
	o	Outbound 側へのフィルタを示します。
slot	0-9	Slot 番号を示します。Slot 番号が存在しない装置モデルの場合、0 としてください。
port	00-99	Port 番号を示します。ゼロパディングにより 2 衔の数値としてください。
sub-if	0000-9999	サブインターフェース番号を示します。ゼロパディングにより 4 衔の数値としてください。
device	0000-9999	デバイス番号を示します。ゼロパディングにより 4 衔の数値としてください。

項目	値	説明
フィルタ種別	b	通信遮断を示します。

アクセスリストをあらかじめ適用する必要のあるポートを下記に示します。

① 端末を収容するポート

受信側の検出方向にアクセスリストを適用します。

② WAN と接続するポート

送受信両側の検出方向にアクセスリストを適用します。

③ セキュリティ装置へのミラー先ポート

送信側の検出方向にアクセスリストを適用します。

④ 永続設定ポート(受信側)

受信側の検出方向にアクセスリストを適用します。

⑤ 永続設定ポート(送信側)

送信側の検出方向にアクセスリストを適用します。

⑥ アクセスリスト拡張ポート

受信側の検出方向にアクセスリストを適用します。

AX3660S, AX2500S, および AX620R におけるアクセスリストの適用例を下記に示します。

表 3-7 AX3660S のアクセスリストの適用例

種別	イーサネットポート
端末収容ポート	interface gigabitethernet 1/0/1 interface gigabitethernet 1/0/2
WAN 接続ポート	interface gigabitethernet 1/0/3 interface gigabitethernet 1/0/4
ミラー先ポート	interface gigabitethernet 1/0/5 interface gigabitethernet 1/0/6
永続設定ポート(受信側)	interface gigabitethernet 1/0/7
永続設定ポート(送信側)	interface gigabitethernet 1/0/8

<pre> interface gigabitethernet 1/0/1     ip access-group AUTO_ACL_IPV4_IN_1_0_1 in     ipv6 traffic-filter AUTO_ACL_IPV6_IN_1_0_1 in ! interface gigabitethernet 1/0/2     ip access-group AUTO_ACL_IPV4_IN_1_0_2 in     ipv6 traffic-filter AUTO_ACL_IPV6_IN_1_0_2 in ! interface gigabitethernet 1/0/3     ip access-group AUTO_ACL_IPV4_IN_1_0_3 in     ip access-group AUTO_ACL_IPV4_OUT_1_0_3 out     ipv6 traffic-filter AUTO_ACL_IPV6_IN_1_0_3 in     ipv6 traffic-filter AUTO_ACL_IPV6_OUT_1_0_3 out ! interface gigabitethernet 1/0/4     ip access-group AUTO_ACL_IPV4_IN_1_0_4 in     ip access-group AUTO_ACL_IPV4_OUT_1_0_4 out     ipv6 traffic-filter AUTO_ACL_IPV6_IN_1_0_4 in     ipv6 traffic-filter AUTO_ACL_IPV6_OUT_1_0_4 out ! interface gigabitethernet 1/0/5     ip access-group AUTO_ACL_IPV4_OUT_1_0_5 out     ipv6 traffic-filter AUTO_ACL_IPV6_OUT_1_0_5 out ! interface gigabitethernet 1/0/6     ip access-group AUTO_ACL_IPV4_OUT_1_0_6 out     ipv6 traffic-filter AUTO_ACL_IPV6_OUT_1_0_6 out ! interface gigabitethernet 1/0/7     ip access-group AUTO_ACL_IPV4_IN_1_0_7 in     ipv6 traffic-filter AUTO_ACL_IPV6_IN_1_0_7 in ! interface gigabitethernet 1/0/8     ip access-group AUTO_ACL_IPV4_OUT_1_0_8 out     ipv6 traffic-filter AUTO_ACL_IPV6_OUT_1_0_8 out </pre>	<pre> ip access-list extended AUTO_ACL_IPV4_IN_1_0_1 4294967294 permit ip any any ! ip access-list extended AUTO_ACL_IPV4_IN_1_0_2 4294967294 permit ip any any ! ip access-list extended AUTO_ACL_IPV4_IN_1_0_3 4294967294 permit ip any any ! ip access-list extended AUTO_ACL_IPV4_IN_1_0_4 4294967294 permit ip any any ! ip access-list extended AUTO_ACL_IPV4_IN_1_0_7 4294967294 permit ip any any ! ip access-list extended AUTO_ACL_IPV4_OUT_1_0_3 4294967294 permit ip any any ! ip access-list extended AUTO_ACL_IPV4_OUT_1_0_4 4294967294 permit ip any any ! ip access-list extended AUTO_ACL_IPV4_OUT_1_0_5 4294967294 deny ip any any ! ip access-list extended AUTO_ACL_IPV4_OUT_1_0_6 4294967294 deny ip any any ! ip access-list extended AUTO_ACL_IPV4_OUT_1_0_8 4294967294 deny ip any any ! ipv6 access-list AUTO_ACL_IPV6_IN_1_0_1 4294967294 permit ip any any ! ipv6 access-list AUTO_ACL_IPV6_IN_1_0_2 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 permit ipv6 any any ! ipv6 access-list AUTO_ACL_IPV6_IN_1_0_3 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 permit ipv6 any any ! ipv6 access-list AUTO_ACL_IPV6_IN_1_0_4 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 permit ipv6 any any ! ipv6 access-list AUTO_ACL_IPV6_IN_1_0_7 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 permit ipv6 any any ! ipv6 access-list AUTO_ACL_IPV6_OUT_1_0_3 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 permit ipv6 any any ! ipv6 access-list AUTO_ACL_IPV6_OUT_1_0_4 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 permit ipv6 any any ! ipv6 access-list AUTO_ACL_IPV6_OUT_1_0_5 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 deny ipv6 any any ! ipv6 access-list AUTO_ACL_IPV6_OUT_1_0_6 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 deny ipv6 any any !</pre>
--	---

	<pre>ipv6 access-list AUTO_ACL_IPV6_OUT_1_0_8 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 deny ipv6 any any !</pre>
--	--

表 3-8 AX2500S のアクセリストの適用例

種別	イーサネットポート
端末収容ポート	interface gigabitethernet 0/3 interface gigabitethernet 0/4
永続設定ポート(受信側)	interface gigabitethernet 0/7

interface gigabitethernet 0/3  ip access-group AUTO_ACL_IPV4_IN_0_3 in ipv6 traffic-filter AUTO_ACL_IPV6_IN_0_3 in !  interface gigabitethernet 0/4  ip access-group AUTO_ACL_IPV4_IN_0_4 in ipv6 traffic-filter AUTO_ACL_IPV6_IN_0_4 in !  interface gigabitethernet 0/7  ip access-group AUTO_ACL_IPV4_IN_0_7 in ipv6 traffic-filter AUTO_ACL_IPV6_IN_0_7 in !	ip access-list extended AUTO_ACL_IPV4_IN_0_3 4294967294 permit ip any any ! ip access-list extended AUTO_ACL_IPV4_IN_0_4 4294967294 permit ip any any ! ip access-list extended AUTO_ACL_IPV4_IN_0_7 4294967294 permit ip any any ! ipv6 access-list AUTO_ACL_IPV6_IN_0_3 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 permit ipv6 any any ! ip access-list AUTO_ACL_IPV6_IN_0_4 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 permit ipv6 any any ! ip access-list AUTO_ACL_IPV6_IN_0_7 99998 permit icmp any any nd-ns 99999 permit icmp any any nd-na 4294967294 permit ipv6 any any !
--	---

表 3-9 AX620R のアクセリストの適用例

種別	ポート
端末収容ポート	interface GigaEthernet1.15
WAN 接続ポート	interface Tunnel127.0

<pre> ! ip access-list ip4ieth0010015a permit ip src any dest any ip access-list ip4itun012700a permit ip src any dest any ip access-list ip4otun012700a permit ip src any dest any !  ipv6 access-list ip6ieth0010015a permit ip src any dest any ipv6 access-list ip6ieth0010015c permit icmp neighbor-advertisement src any dest any ipv6 access-list ip6ieth0010015c permit icmp neighbor-solicitation src any dest any ipv6 access-list ip6itun012700a permit ip src any dest any ipv6 access-list ip6otun012700a permit ip src any dest any </pre>	<pre> ! interface GigaEthernet1.15   ip filter ip4ieth0010015b 65534 in   ip filter ip4ieth0010015a 65535 in   ipv6 filter ip6ieth0010015c 65531 in   ipv6 filter ip6ieth0010015b 65534 in   ipv6 filter ip6ieth0010015a 65535 in ! interface Tunnel127.0   ip filter ip4itun012700b 65534 in   ip filter ip4itun012700a 65535 in   ip filter ip4otun012700b 65534 out   ip filter ip4otun012700a 65535 out   ipv6 filter ip6itun012700b 65534 in   ipv6 filter ip6itun012700a 65535 in   ipv6 filter ip6otun012700b 65534 out   ipv6 filter ip6otun012700a 65535 out </pre>
--	--

上記で使用している ip6ieth0010015a, ip6ieth0010015c, ip6itun012700a, および ip6otun012700a の名称は一例です。

### (b) 通信遮断専用モード

適用するアクセスリスト名称は、管理対象装置の装置モデルにより異なります。

<検出方向>は、IN または OUT になります。

- ① AX4600S・AX3800S・AX3660S・AX3650S・AX2500S(スタック使用時)

AUTO\_ACL\_MAC\_<検出方向>\_<switch no.>\_0\_<port no.>

- ② AX8600S・AX8300S

AUTO\_ACL\_ADVANCE\_<検出方向>\_<nif no.>\_<port no.>

- ③ AX260A・AX3640S・AX2500S(スタック未使用時)・AX2200S・AX2100S

AUTO\_ACL\_MAC\_<検出方向>\_0\_<port no.>

- ④ AXprimoM210

AUTO\_ACL\_MAC\_IN\_1\_<port no.>

AX620R は、以下となります。

- GigaEthernet/FastEthernet の場合

<ACL 種別><検出方向>eth<slot><port><sub-if><フィルタ種別>

表 3-10 AX620R のアクセリスト名称のフィールドの説明

項目	値	説明
ACL 種別	mac	MAC パケットに対するフィルタを示します。
検出方向	i	Inbound 側へのフィルタを示します。
slot	0-9	Slot 番号を示します。Slot 番号が存在しない装置モデルの場合、0 としてください。
port	00-99	Port 番号を示します。ゼロパディングにより 2 桁の数値としてください。
sub-if	0000-9999	サブインターフェース番号を示します。ゼロパディングにより 4 桁の数値としてください。
フィルタ種別	b	通信遮断を示します。

アクセリストをあらかじめ適用する必要のあるポートを下記に示します。

① 端末を収容するポート

受信側の検出方向にアクセリストを適用します。

② セキュリティ装置へのミラー先ポート

送信側の検出方向にアクセリストを適用します。

③ アクセリスト拡張ポート

受信側の検出方向にアクセリストを適用します。

AX3660S、AX2500S、および AX620R におけるアクセリストの適用例を下記に示します。

表 3-11 AX3660S のアクセリストの適用例

種別	イーサネットポート
端末収容ポート	interface gigabitethernet 1/0/1 interface gigabitethernet 1/0/2
ミラー先ポート	interface gigabitethernet 1/0/5 interface gigabitethernet 1/0/6

<pre> interface gigabitethernet 1/0/1   mac access-group AUTO_ACL_MAC_IN_1_0_1 in ! interface gigabitethernet 1/0/2   mac access-group AUTO_ACL_MAC_IN_1_0_2 in ! interface gigabitethernet 1/0/5   mac access-group AUTO_ACL_MAC_OUT_1_0_5 out ! interface gigabitethernet 1/0/6   mac access-group AUTO_ACL_MAC_OUT_1_0_6 out </pre>	<pre> mac access-list extended AUTO_ACL_MAC_IN_1_0_1   4294967294 permit any any ! mac access-list extended AUTO_ACL_MAC_IN_1_0_2   4294967294 permit any any ! mac access-list extended AUTO_ACL_MAC_OUT_1_0_5   4294967294 deny any any ! mac access-list extended AUTO_ACL_MAC_OUT_1_0_6   4294967294 deny any any !</pre>
--	---

表 3-12 AX2500S のアクセリストの適用例

種別	イーサネットポート
端末収容ポート	interface gigabitethernet 0/3 interface gigabitethernet 0/4

<pre> interface gigabitethernet 0/3   mac access-group AUTO_ACL_MAC_IN_0_3 in ! interface gigabitethernet 0/4   mac access-group AUTO_ACL_MAC_IN_0_4 in </pre>	<pre> mac access-list extended AUTO_ACL_MAC_IN_0_3   4294967294 permit any any ! mac access-list extened AUTO_ACL_MAC_IN_0_4   4294967294 permit any any !</pre>
--	--

表 3-13 AX620R のアクセリストの適用例

種別	ポート
端末収容ポート	interface GigaEthernet1.15

<pre> ! access-list macieth0010015a permit src any dest any </pre>	<pre> ! interface GigaEthernet1.15   filter macieth0010015b 65534 in   filter macieth0010015a 65535 in </pre>
--	---

上記で使用している macieth0010015a の名称は一例です。

## (2) 設定対象外装置

管理対象装置が下記の場合、本設定は不要です。

表 3-14 設定対象外装置

管理対象装置
標準 MIB 対応装置
標準 MIB 対応装置(VLAN 每コミュニティ)
ワイヤレス LAN コントローラ

### 3.3 管理対象装置個別の事前準備

管理対象装置個別の事前準備を説明します。

#### 3.3.1 AX260A

##### (1) SSH ホスト鍵ペア

工場出荷時の SSH ホスト鍵ペア(公開鍵・秘密鍵)の場合、AX-Security-Controller は、AX260A と SSH を使用した接続ができません。工場出荷時のままの場合、必ず、SSH ホスト鍵ペアの変更をおこなってください。SSH ホスト鍵ペアの変更方法は、下記を参照してください。

「AX260A Secure Shell(SSH)ソフトウェアマニュアル 運用コマンドレファレンス編  
set ssh hostkey」

##### (2) LLDP のバージョン

隣接する管理対象装置とのイーサネットポートで LLDP の運用を有効にする際、LLDP のバージョンは IEEE802.1AB/D6(2003 年 10 月)を設定するようにしてください。

LLDP バージョンの設定方法は、下記を参照してください。

「AX260A ソフトウェアマニュアル コンフィグレーションコマンドレファレンス  
LLDP の lldp version」

#### 3.3.2 AX8600S・AX8300S

##### (1) 端末収容 IP インタフェース

端末の ARP 情報および NDP 情報を学習する IP インタフェースは VLAN インタフェースとしてください。

マネージメントポートインターフェース等で学習した ARP 情報および NDP 情報は、端末として管理しません。

##### (2) VRF

VRF を使用する場合、グローバルネットワーク、および各 VRF インスタンスで学習する端末の IP アドレスは重複しないようにしてください。

重複した場合、セキュリティ装置から指示された端末と異なる端末について、セキュリティフィルタを適用する場合があります。

### (3) コンフィグレーションのコミットモード

コンフィグレーションのコミットモードは、手動コミットモードとせず、逐次コミットモードとしてください。手動コミットモードの場合、AX-Security-Controllerからのコンフィグレーション設定指示が反映されません。

### (4) フィルタ・QoS フロー機能のフロー検出モード

フィルタ・QoS フロー機能のフロー検出モードは検出条件数重視モードを使用してください。

## 3.3.3 AX4600S

### (1) 端末収容 IP インタフェース

端末の ARP 情報および NDP 情報を学習する IP インタフェースは VLAN インタフェースとしてください。

マネージメントポートインターフェース等で学習した ARP 情報および NDP 情報は、端末として管理しません。

### (2) VRF

VRF を使用する場合、グローバルネットワーク、および各 VRF インスタンスで学習する端末の IP アドレスは重複しないようにしてください。

重複した場合、セキュリティ装置から指示された端末と異なる端末について、セキュリティフィルタを適用する場合があります。

## 3.3.4 AX3800S

### (1) 端末収容 IP インタフェース

端末の ARP 情報および NDP 情報を学習する IP インタフェースは VLAN インタ

フェースとしてください。

マネージメントポートインターフェース等で学習した ARP 情報および NDP 情報は、端末として管理しません。

## (2) VRF

VRF を使用する場合、グローバルネットワーク、および各 VRF インスタンスで学習する端末の IP アドレスは重複しないようにしてください。

重複した場合、セキュリティ装置から指示された端末と異なる端末について、セキュリティフィルタを適用する場合があります。

### 3.3.5 AX3660S

#### (1) 端末収容 IP インタフェース

端末の ARP 情報および NDP 情報を学習する IP インタフェースは VLAN インタフェースとしてください。

マネージメントポートインターフェース等で学習した ARP 情報および NDP 情報は、端末として管理しません。

#### (2) VRF

VRF を使用する場合、グローバルネットワーク、および各 VRF インスタンスで学習する端末の IP アドレスは重複しないようにしてください。

重複した場合、セキュリティ装置から指示された端末と異なる端末について、セキュリティフィルタを適用する場合があります。

### 3.3.6 AX3650S

#### (1) VRF

VRF を使用する場合、グローバルネットワーク、および各 VRF インスタンスで学習する端末の IP アドレスは重複しないようにしてください。

重複した場合、セキュリティ装置から指示された端末と異なる端末について、セキュリティフィルタを適用する場合があります。

### 3.3.7 AX2500S

#### (1) SSH ホスト鍵ペア

工場出荷時の SSH ホスト鍵ペア(公開鍵・秘密鍵)の場合、AX-Security-Controller は、AX2500S と SSH を使用した接続ができません。工場出荷時から変更していない場合、必ず、SSH ホスト鍵ペアの変更をおこなってください。SSH ホスト鍵ペアの変更方法は、下記を参照してください。

「AX2500S・AX2200S・AX2100S・AX1250S・AX1240S Secure Shell(SSH)ソフトウェアマニュアル 運用コマンドレファレンス編 set ssh hostkey」

#### (2) LLDP のバージョン

隣接する管理対象装置とのイーサネットポートで LLDP の運用を有効にする際、LLDP のバージョンは IEEE802.1AB/D6(2003 年 10 月)を設定するようにしてください。

LLDP バージョンの設定方法は、下記を参照してください。

「AX2500S ソフトウェアマニュアル コンフィグレーションコマンドレファレンス LLDP の lldp version」

### 3.3.8 AX2200S

#### (1) SSH ホスト鍵ペア

工場出荷時の SSH ホスト鍵ペア(公開鍵・秘密鍵)の場合、AX-Security-Controller は、AX2200S と SSH を使用した接続ができません。工場出荷時から変更していない場合、必ず、SSH ホスト鍵ペアの変更をおこなってください。SSH ホスト鍵ペアの変更方法は、下記を参照してください。

「AX2500S・AX2200S・AX2100S・AX1250S・AX1240S Secure Shell(SSH)ソフトウェアマニュアル 運用コマンドレファレンス編 set ssh hostkey」

### 3.3.9 AX2100S

#### (1) SSH ホスト鍵ペア

工場出荷時の SSH ホスト鍵ペア(公開鍵・秘密鍵)の場合、AX-Security-Controller は、AX2100S と SSH を使用した接続ができません。工場出荷時から変更していない場合、必ず、SSH ホスト鍵ペアの変更をおこなってください。SSH ホスト鍵ペアの変更方法は、下記を参照してください。

「AX2500S・AX2200S・AX2100S・AX1250S・AX1240S Secure Shell(SSH)ソフトウェアマニュアル 運用コマンドレファレンス編 set ssh hostkey」

### 3.3.10 AXprimoM210

ありません。

## 3.4 管理対象装置個別の注意事項

管理対象装置個別の注意事項を説明します。

### 3.4.1 AXprimoM210

#### (1) 専用アクセリストの全フィルタエントリの削除

専用アクセリストの全フィルタエントリは、以下の契機で削除します。

表 3-15 全フィルタエントリの削除契機

契機	備考
AXprimoM210 の装置再起動を検知	
AXprimoM210 のメンテナンスマードを有効から無効に反映	
AX-Security-Controller を起動	

全フィルタエントリ削除完了後、AX-Security-Controller は、必要なフィルタエントリの再設定をおこないます。フィルタエントリの削除により、一時的に、通信遮断した端末からの通信がおこなわれる場合があります。

### 3.4.2 AX620R

#### (1) 専用アクセリストの全フィルタエントリの削除

専用アクセリストの全フィルタエントリは、以下の契機で削除します。

表 3-16 全フィルタエントリの削除契機

契機	備考
AX620R の装置再起動を検知	
AX620R のメンテナンスマードを有効から無効に反映	
AX-Security-Controller を起動	

全フィルタエントリ削除完了後、AX-Security-Controller は、必要なフィルタエントリの再設定をおこないます。フィルタエントリの削除により、一時的に、通信遮断した端末からの通信がおこなわれる場合があります。

## (2) IPv6 アクセスリストの ICMP 許可設定

通常モードで運用し、AX620R のポート配下で IPv6 端末を直接収容している構成において、当該端末が通信遮断対象となる場合、IPv6 アクセスリストの追加と削除が繰り返されます。

この場合、ICMP の Neighbor discovery router advertisements(タイプ 134)、および Neighbor discovery router solicitations(タイプ 133)を許可するように、IPv6 アクセスリストの設定を検討ください。

表 3-17 IPv6 アクセスリストの ICMP 許可設定例

```
ipv6 access-list ip6ieth0010015c permit icmp neighbor-advertisement src any dest any  
ipv6 access-list ip6ieth0010015c permit icmp neighbor-solicitation src any dest any
```



## 4. 起動・停止方法

---

この章では、AX-Security-Controller の起動・停止方法について説明します。

---

## 4.1 AX-Security-Controller(Manager)の起動・停止方法

AX-Security-Controller(Manager)を動作させるための起動パラメータ、起動方法、および停止方法を説明します。

### 4.1.1 AX-Security-Controller(Manager)の起動パラメータ

プログラム実行時は、<Python プログラム>、および<インストールパス>の部分を、使用環境に応じたプログラム名、およびインストールパスに読み替えてください。なお、<インストールパス>の最後の文字は、使用環境に応じたディレクトリの区切り文字(スラッシュ(/)またはバックスラッシュ(\))としてください。

および、同時に複数の AX-Security-Controller(Manager)プログラムを実行しないようにしてください。

[入力形式]

```
<Python プログラム> <インストールパス>axsc_manager.py [--addr <IP Address>]
[--ssl <Cert> <Key>] [--port <TCP Port>] [--syslog-udp-port <UDP Port>] [--block-dedicated-mode] [--accesslist-mode <Mode>] [--reset-basic-auth] [--core <Core>] [--gathering-interval <Seconds>] [--factory-reset]
```

[パラメータ]

--addr <IP Address>

AX-Security-Controller(Manager)が要求を受け付ける IP アドレスを指定します。

1. 本パラメータ未指定時の初期値

0.0.0.0<sup>※1</sup>

2. 値の設定範囲

0.0.0.0～255.255.255.255<sup>※2</sup>

※1 :

AX-Security-Controller(Manager)が動作するオペレーティングシステム上のすべての IP アドレスからの要求を受け付けます。

※2 :

AX-Security-Controller(Manager)が動作するオペレーティングシステム上の IP

アドレスを指定してください。

--ssl <Cert> <Key>

SSL による受け付けを有効にします。事前に、サーバ証明書ファイル、および秘密鍵ファイルを用意する必要があります。

<Cert>

サーバ証明書ファイル

<Key>

秘密鍵ファイル

1. 本パラメータ未指定時の初期値

SSL による受け付けを有効にしません。

--port <TCP Port>

AX-Security-Controller(Manager)が要求を受け付ける TCP ポート番号を指定します。

1. 本パラメータ未指定時の初期値

SSL 無効時 80, SSL 有効時 443

2. 値の設定範囲

0~65535

--syslog-udp-port <UDP Port>

AX-Security-Controller(Manager)が Syslog を受け付ける UDP ポート番号を指定します。

1. 本パラメータ未指定時の初期値

514

2. 値の設定範囲

0~65535

**--block-dedicated-mode**

通信遮断専用モードを有効にします。

1. 本パラメータ未指定時の初期値

通信遮断専用モードを有効にしません。通常モードで動作します。

**--access-list-mode <Mode>**

アクセリストのモードを指定します。

1. 本パラメータ未指定時の初期値

v4-only

2. 値の設定範囲

v4-only または v4-v6

**--reset-basic-auth**

Basic 認証有効時において、ユーザ名、またはパスワードを忘れた場合に、

Basic 認証を一時的に無効にして起動するパラメータです。本パラメータを指定して起動した場合、再度 Basic 認証の設定を行ってください。

1. 本パラメータ未指定時の初期値

Basic 認証有効時は、Basic 認証を無効にしません。

**--core <Core>**

AX-Security-Controller(Manager)が、管理対象装置との通信に使用するプロセスの最大数を指定します。

1. 本パラメータ未指定時の初期値

4

2. 値の設定範囲

1 以上の数値 (CPU のコア数の 2 倍まで)

--gathering-interval <Seconds>

AX-Security-Controller(Manager)の収集周期(秒)を指定します。

なお、全管理対象装置からの情報収集とセキュリティフィルタの設定が収集周期を越えた場合、前の周期の収集を完了後に、ただちに次の周期の収集を開始します。

1. 本パラメータ未指定時の初期値

30

2. 値の設定範囲

30 ~ 86400

--factory-reset

AX-Security-Controller が内部で管理するデータベースとマップの背景画像をクリアします。本パラメータを指定して起動した場合、AX-Security-Controller(Manager)はデータベースとマップの背景画像をクリア後、停止します。

[応答メッセージ]

表 4-1 axsc\_manager.pyc 応答メッセージ

メッセージ	内容
FACTORY RESET: success (DB is empty).	データベースとマップの背景画像のクリアに成功しました。
FACTORY RESET: success.	データベースとマップの背景画像のクリアに成功しました。
FACTORY RESET: failed.	データベースとマップの背景画像のクリアに失敗しました。アクセス権限を確認し、再度実行してください。
Invalid IP address: <IP Address>	IP アドレスが不正です。IP アドレスを見直してください。
Cannot open certificate file: <Cert>	サーバ証明書ファイルが見つかりません。サーバ証明書ファイルのパスを見直してください。
Cannot open key file: <Key>	秘密鍵ファイルが見つかりません。秘密鍵ファイルのパスを見直してください。
Invalid TCP port number: <TCP Port>	TCP ポート番号が不正です。TCP ポート番号を見直してください。
Invalid UDP port number: <UDP Port>	UDP ポート番号が不正です。UDP ポート番号を見直してください。

メッセージ	内容
Invalid CPU core number: <Core>	プロセスの最大数が不正です。プロセスの最大数を見直してください。
Invalid gathering interval: <Seconds>	収集周期が不正です。値を見直してください。
Failed DB initialization	データベースの初期化に失敗しました。axsc_manager.pyc が他に起動していないか確認してください。
Invalid accesslist mode: <Mode>	アクセスリストのモード指定が不正です。設定内容を見直してください。
HTTP Server: <エラーメッセージ>	HTTP サーバの起動に失敗しました。<エラーメッセージ>を確認してください。
Syslog Server: <エラーメッセージ>	Syslog サーバの起動に失敗しました。<エラーメッセージ>を確認してください。

#### 4.1.2 AX-Security-Controller(Manager)起動方法

##### (1) Windows 10 / Windows Server 2016 / Windows Server 2019

Python スクリプトを実行することで起動します。

ここでは、AX-Security-Controller を HTTPS で起動する例を示しますが、あくまで一例であるため環境によっては異なる部分があります。適宜該当部分についてはご利用の環境に合わせて読み替えてください。なお、SSL 証明書の証明書ファイル(axsc.crt)と鍵ファイル(axsc.key)はあらかじめ用意されているものとします。

- ① バッチファイルを作成する場合は下記ファイルを作成し、ダブルクリックまたはコマンドプロンプトから実行して起動します。起動後に「AX-Security-Controller(Manager): Serving HTTPS on 0.0.0.0 port 443 ...」と表示されれば起動は成功です。

```
@ECHO OFF
python C:\axsc\axsc_manager.pyc --ssl C:\axsc\axsc.crt C:\axsc\axsc.key
```

- ② コマンドプロンプトから起動する場合はバッチファイルを作成する場合と同様の起動パラメータで起動します。起動後に「AX-Security-Controller(Manager): Serving HTTPS on 0.0.0.0 port 443 ...」と表示されれば起動は成功です。

```
C:\Users\ユーザー名> python C:\axsc\axsc_manager.py --ssl C:\axsc\axsc.crt  
C:\axsc\axsc.key  
  
AX-Security-Controller(Manager): Serving Syslog(UDP) on 0.0.0.0 port 514 ...  
AX-Security-Controller(Manager): Serving HTTPS on 0.0.0.0 port 443 ...
```

## (2) CentOS 7 / CentOS 8 / Red Hat Enterprise Linux 7 / Red Hat Enterprise Linux 8

Python スクリプトを実行することで起動します。

ここでは、AX-Security-Controller を HTTPS で起動する例を示しますが、あくまで一例であるため環境によっては異なる部分があります。適宜該当部分についてはご利用の環境に合わせて読み替えてください。なお、SSL 証明書の証明書ファイル(axsc.crt)と鍵ファイル(axsc.key)はあらかじめ用意されているものとします。

- ① Systemd に axsc としてサービス登録済みの場合は systemctl コマンドから起動します。「systemctl status axsc」の実行結果に「active (running)」と表示されれば起動は成功です。

```
# systemctl start axsc

# systemctl status axsc
● axsc.service — AX-Security-Controller
   Loaded: loaded (/etc/112system/system/axsc.service; enabled; vendor preset: disabled)
   Active: active (running) since 木 2017-06-22 14:33:28 JST; 6s ago
     Main PID: 11793 (python3.6)
        Cgroup: /system.slice/axsc.service
                  tq11793 /bin/python3.6 /usr/local/share/axsc/axsc_manager.pyc —ss...
                  tq11796 /bin/python3.6 /usr/local/share/axsc/module/scheduler.pyc ...
                  tq11798 /bin/python3.6 /usr/local/share/axsc/module/scheduler.pyc ...
                  tq11799 /bin/python3.6 /usr/local/share/axsc/module/scheduler.pyc ...
                  tq11800 /bin/python3.6 /usr/local/share/axsc/module/scheduler.pyc ...
                  mq11801 /bin/python3.6 /usr/local/share/axsc/module/scheduler.pyc ...

6月 22 14:33:28 localhost.localdomain 112system[1]: Started AX-Security-Contr...
6月 22 14:33:28 localhost.localdomain 112system[1]: Starting AX-Security-Cont...
Hint: Some lines were ellipsized, use —l to show in full.
```

- ② ターミナルから実行する場合は起動パラメータの--ssl オプションを有効にして実行します。起動後に「AX-Security-Controller(Manager): Serving HTTPS on 0.0.0.0 port 443 ...」と表示されれば起動は成功です。

```
# python3.6 /usr/local/share/axsc/axsc_manager.py --ssl /usr/local/share/axsc/axsc.crt  
/usr/local/share/axsc/axsc.key  
  
AX-Security-Controller(Manager): Serving Syslog(UDP) on 0.0.0.0 port 514 ...  
AX-Security-Controller(Manager): Serving HTTPS on 0.0.0.0 port 443 ...
```

#### 4.1.3 AX-Security-Controller(Manager)停止方法

##### (1) Windows 10 / Windows Server 2016 / Windows Server 2019

Python スクリプトに Ctrl + Break を送ることで停止します。タスクマネージャで Python スクリプトを実行していた python.exe が終了していれば停止は成功です。

##### (2) CentOS 7 / CentOS 8 / Red Hat Enterprise Linux 7 / Red Hat Enterprise Linux 8

- ① Systemd に axsc としてサービス登録済みの場合は systemctl コマンドから停止します。「systemctl status axsc」の実行結果に「inactive (dead)」と表示されれば停止は成功です。

```
# systemctl stop axsc

# systemctl status axsc

● axsc.service — AX-Security-Controller

    Loaded: loaded (/etc/114system/system/axsc.service; enabled; vendor preset: disabled)
      Active: inactive (dead) since 木 2017-06-22 14:50:04 JST; 1s ago
        Process: 15398 ExecStart=/bin/python3.6 /usr/local/share/axsc/axsc_manager.pyc --ssl
          /usr/local/share/axsc/axsc.crt /usr/local/share/axsc/axsc.key (code=exited,
           status=0/SUCCESS)

    Main PID: 15398 (code=exited, status=0/SUCCESS)

6月 22 14:49:56 localhost.localdomain 114system[1]: Started AX-Security-Contr...
6月 22 14:49:56 localhost.localdomain 114system[1]: Starting AX-Security-Cont...
6月 22 14:50:02 localhost.localdomain 114system[1]: Stopping AX-Security-Cont...
6月 22 14:50:02 localhost.localdomain python3.6[15398]: AX-Security-Control...
6月 22 14:50:04 localhost.localdomain 114system[1]: Stopped AX-Security-Contr...

Hint: Some lines were ellipsized, use —l to show in full.
```

ターミナルから実行している場合は Python スクリプトに SIGTERM(Ctrl+Break)を送ることで停止します。ps コマンドで python スクリプトを実行していた python プロセスが終了していれば停止は成功です。

## 4.2 AX-Security-Controller(Viewer)の起動・停止方法

AX-Security-Controller(Viewer)を動作させるための起動パラメータ、起動方法、および停止方法を説明します。

ネットワーク管理者が、遮断中の端末の一覧を、ネットワーク利用者へ参照をおこなわせる場合に起動してください。

### 4.2.1 AX-Security-Controller(Viewer)の起動パラメータ

プログラム実行時は、<Python プログラム>、および<インストールパス>の部分を、使用環境に応じたプログラム名、およびインストールパスに読み替えてください。なお、<インストールパス>の最後の文字は、使用環境に応じたディレクトリの区切り文字(スラッシュ(/)またはバックスラッシュ(\))としてください。

および、同時に複数の AX-Security-Controller(Viewer)プログラムを実行しないようにしてください。

[入力形式]

```
<Python プログラム> <インストールパス>axsc_viewer.py [--addr <IP Address>]
[--ssl <Cert> <Key>] [--port <TCP Port>]
```

[パラメータ]

--addr <IP Address>

AX-Security-Controller(Viewer)が要求を受け付ける IP アドレスを指定します。

1. 本パラメータ未指定時の初期値

0.0.0.0<sup>※1</sup>

2. 値の設定範囲

0.0.0.0～255.255.255.255<sup>※2</sup>

※1 :

AX-Security-Controller(Viewer)が動作するオペレーティングシステム上のすべての IP アドレスからの要求を受け付けます。

※2 :

AX-Security-Controller(Viewer)が動作するオペレーティングシステム上の IP

アドレスを指定してください。

--ssl <Cert> <Key>

SSL による受け付けを有効にします。事前に、サーバ証明書ファイル、および秘密鍵ファイルを用意する必要があります。

<Cert>

サーバ証明書ファイル

<Key>

秘密鍵ファイル

1. 本パラメータ未指定時の初期値

SSL による受け付けを有効にしません。

--port <TCP Port>

AX-Security-Controller(Viewer)が要求を受け付ける TCP ポート番号を指定します。AX-Security-Controller(Manager)が要求を受け付ける TCP ポート番号と重複しないようにしてください。

1. 本パラメータ未指定時の初期値

SSL 無効時 80, SSL 有効時 443

2. 値の設定範囲

0~65535

[応答メッセージ]

表 4-2 axsc\_viewer.pyc 応答メッセージ

メッセージ	内容
Invalid IP address: <IP Address>	IP アドレスが不正です。IP アドレスを見直してください。
Cannot open certificate file: <Cert>	サーバ証明書ファイルが見つかりません。サーバ証明書ファイルのパスを見直してください。
Cannot open key file: <Key>	秘密鍵ファイルが見つかりません。秘密鍵ファイルのパスを見直してください。
Invalid port number: <TCP Port>	TCP ポート番号が不正です。TCP ポート番号を見直してください。
HTTP Server: <エラーメッセージ>	HTTP サーバの起動に失敗しました。<エラーメッセージ>を確認してください。

## 4.2.2 AX-Security-Controller(Viewer)起動方法

起動方法は、AX-Security-Controller(Manager)と同様です。

「4.1.2 AX-Security-Controller(Manager)起動方法」を参照してください。

## 4.2.3 AX-Security-Controller(Viewer)停止方法

停止方法は、AX-Security-Controller(Manager)と同様です。

「4.1.3 AX-Security-Controller(Manager)停止方法」を参照してください。

## 4.3 AX-Security-Controller(Tracker)の起動・停止方法

AX-Security-Controller(Tracker)を動作させるための起動パラメータ、起動方法、および停止方法を説明します。

### 4.3.1 AX-Security-Controller(Tracker)の起動パラメータ

プログラム実行時は、<Python プログラム>、および<インストールパス>の部分を、使用環境に応じたプログラム名、およびインストールパスに読み替えてください。なお、<インストールパス>の最後の文字は、使用環境に応じたディレクトリの区切り文字(スラッシュ(/)またはバックスラッシュ(\))としてください。

および、同時に複数の AX-Security-Controller(Tracker)プログラムを実行しないようにしてください。

[入力形式]

```
<Python プログラム> <インストールパス>axsc_tracker.pyc [--addr <IP Address>]
[--ssl <Cert> <Key>] [--port <TCP Port>] [--retention-period <Days>]
```

[パラメータ]

--addr <IP Address>

AX-Security-Controller(Tracker)が要求を受け付ける IP アドレスを指定します。

1. 本パラメータ未指定時の初期値

0.0.0.0<sup>※1</sup>

2. 値の設定範囲

0.0.0.0～255.255.255.255<sup>※2</sup>

※1 :

AX-Security-Controller(Tracker)が動作するオペレーティングシステム上のすべての IP アドレスからの要求を受け付けます。

※2 :

AX-Security-Controller(Tracker)が動作するオペレーティングシステム上の IP アドレスを指定してください。

--ssl <Cert> <Key>

SSL による受け付けを有効にします。事前に、サーバ証明書ファイル、および秘密鍵ファイルを用意する必要があります。

<Cert>

サーバ証明書ファイル

<Key>

秘密鍵ファイル

1. 本パラメータ未指定時の初期値

SSL による受け付けを有効にしません。

--port <TCP Port>

AX-Security-Controller(Tracker)が要求を受け付ける TCP ポート番号を指定します。

1. 本パラメータ未指定時の初期値

SSL 無効時 80, SSL 有効時 443

2. 値の設定範囲

0～65535

--retention-period <Days>

履歴保持日数を指定します。

1. 本パラメータ未指定時の初期値

365

2. 値の設定範囲

1～3650

[応答メッセージ]

表 4-3 axsc\_tracker.py 応答メッセージ

メッセージ	内容
Invalid IP address: <IP Address>	IP アドレスが不正です。IP アドレスを見直してください。
Cannot open certificate file: <Cert>	サーバ証明書ファイルが見つかりません。サーバ証明書ファイルのパスを見直してください。
Cannot open key file: <Key>	秘密鍵ファイルが見つかりません。秘密鍵ファイルのパスを見直してください。
Invalid TCP port number: <TCP Port>	TCP ポート番号が不正です。TCP ポート番号を見直してください。
HTTP Server: <エラーメッセージ>	HTTP サーバの起動に失敗しました。<エラーメッセージ>を確認してください。
Invalid retention period: <Days>	履歴保持日数が不正です。履歴保持日数を見直してください。

### 4.3.2 AX-Security-Controller(Tracker)起動方法

起動方法は、AX-Security-Controller(Manager)と同様です。

「4.1.2 AX-Security-Controller(Manager)起動方法」を参照してください。

なお、AX-Security-Controller を初めて導入、またはバージョンアップ後の初回起動時は、AX-Security-Controller(Manager)の起動完了後に AX-Security-Controller(Tracker)を起動するようにしてください。

### 4.3.3 AX-Security-Controller(Tracker)停止方法

停止方法は、AX-Security-Controller(Manager)と同様です。

「4.1.3 AX-Security-Controller(Manager)停止方法」を参照してください。

## 5. 操作方法

---

この章では、AX-Security-Controller の操作方法について説明します。

---

## 5.1 AX-Security-Controllerへのアクセス

### 5.1.1 AX-Security-Controller(Manager)へのアクセス

AX-Security-Controller(Manager)へのアクセスは、「4.1.2 AX-Security-Controller(Manager)起動方法」で起動したIPアドレス、およびTCPポート番号に対して、「2.2.1 AX-Security-Controller(Manager)で使用可能なウェブブラウザ」で示すブラウザでアクセスしてください。

下記に、SSLあり、ホスト名 ax-sc.example.com、TCPポート番号 443 でアクセスした際の例を示します。

図 5-1 AX-Security-Controller (Manager)へのアクセス例



### 5.1.2 AX-Security-Controller(Viewer)へのアクセス

AX-Security-Controller(Viewer)へのアクセスは、「4.2.2 AX-Security-Controller(Viewer)起動方法」で起動したIPアドレス、およびTCPポート番号に対して、「2.2.2 AX-Security-Controller(Viewer)で使用可能なウェブブラウザ」で示すブラウザでアクセスしてください。

下記に、SSLなし、ホスト名 ax-sc.example.com、TCPポート番号 8080 でアクセスした際の例を示します。

図 5-2 AX-Security-Controller (Viewer)へのアクセス例



### 5.1.3 AX-Security-Controller(Tracker)へのアクセス

AX-Security-Controller(Tracker)へのアクセスは、「4.3.2 AX-Security-Controller(Tracker)

起動方法」で起動した IP アドレス、および TCP ポート番号に対して、「2.2.3 AX-Security-Controller(Tracker)で使用可能なウェブブラウザ」で示すブラウザでアクセスしてください。

下記に、SSL なし、ホスト名 ax-sc.example.com、TCP ポート番号 8888 でアクセスした際の例を示します。

図 5-3 AX-Security-Controller (Tracker)へのアクセス例



## 5.2 AX-Security-Controller(Manager)の画面構成

### 5.2.1 画面構成

AX-Security-Controller(Manager)の画面構成を、下記に示します。

図 5-4 画面構成

登録日時	種別	セキュリティフィルタ条件	状態	連携機能	遮断理由	要求元IPアドレス
2018/08/29 13:53:12 JST	通信遮断	送信元:10.0.30.164/32宛 先:0.0.0.0/0	設定済み	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		10.200.0.250
2018/08/29 13:52:54 JST	詳細表示	送信元:10.0.30.163/32宛 先:0.0.0.0/0	設定済み	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		10.200.0.250
2018/08/29 13:52:09 JST	詳細表示	送信元:10.0.10.54/32宛 先:0.0.0.0/0	設定済み	TMPM連携		10.200.0.250
2018/08/29 13:51:13 JST	例外通信許可	送信元:10.0.10.53/32宛 先:172.16.0.44/32	設定済み	TMPM連携		10.200.0.250
2018/08/29 13:49:09 JST	通信遮断	送信元:0.0.0.0/0宛 先:198.51.100.222/32	設定済み	TMPM連携		10.200.0.250
2018/08/29 13:47:55 JST	通信遮断	送信元:10.0.10.53/32宛 先:0.0.0.0/0	設定済み	TMPM連携		10.200.0.250

AX-Security-Controller 1.5  
Copyright (c) 2017, 2018 ALAXALA Networks Corporation. All rights reserved.

画面構成は、以下の要素より構成されます。

表 5-1 構成要素

項目番号	内容	説明
①	トップ画面へのリンク	AX-Security-Controller(Manager) トップ画面へのリンクです。 各機能画面で操作中、トップ画面へのリンクを選択することで、トップ画面へと移動することができます。
②	ナビゲーションバー	提供する各機能への移動を管理するメニュー機能です。メニュー内の機能を選択することで、各機能画面へと移動します。

項目番号	内容	説明
③	機能グループメニュー	<p>ナビゲーションバーで提供する機能のうち、グループ化したメニュー機能です。</p> <p>以下の機能を提供しています。</p> <ul style="list-style-type: none"> <li>・ 共通 AX-Security-Controller(Manager)単独で提供する機能</li> <li>・ TMPM 連携 トレンドマイクロ DDI/TMPM との連携で提供する機能(ライセンス「外部連携 トレンドマイクロ DDI/TMPM との連携」有効時)</li> <li>・ 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 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で提供する機能(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」有効時)</li> </ul>
④	機能画面	各機能の画面です。

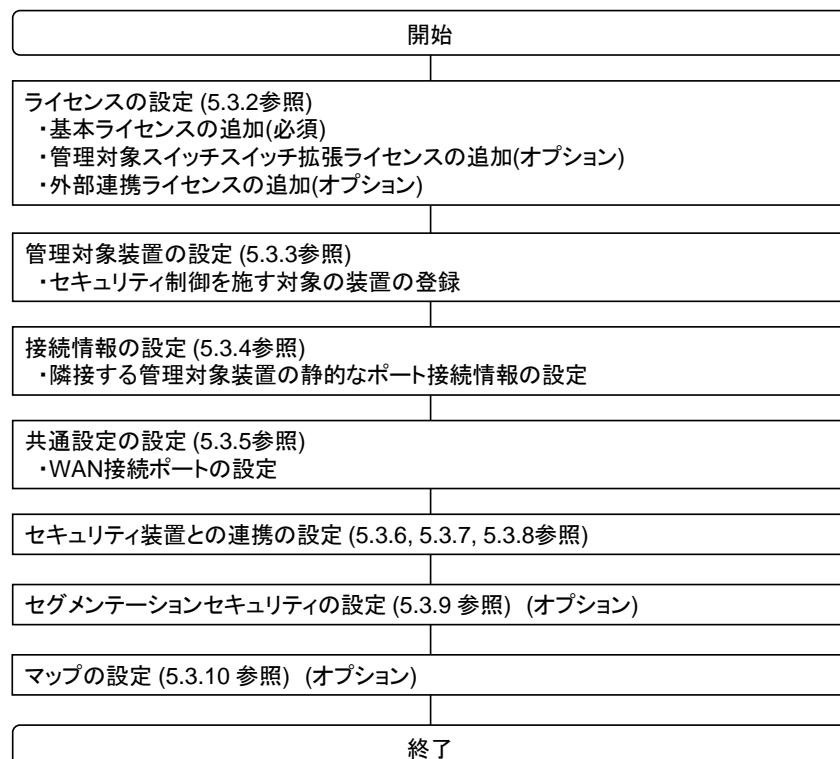
## 5.3 初期設定

AX-Security-Controller(Manager)を新規に起動した場合におこなう初期設定について記載します。

### 5.3.1 初期設定の流れ

初期設定は、以下の流れで設定をおこなってください。

図 5-5 初期設定フロー



### 5.3.2 ライセンスの設定

AX-Security-Controller(Manager)を動作するのに必要なライセンスを設定します。

#### (1) ライセンス画面の表示

ナビゲーションバーより、「管理」を選択し、そこから「ライセンス」を選択します。

図 5-6 ナビゲーションバーでの選択



図 5-7 ライセンス画面の表示



## (2) ライセンスの設定

「機能ライセンス追加」ボタンを押し、機能ライセンス追加画面を表示してください。

図 5-8 機能ライセンス追加ボタンの押下



ライセンスキーのテキストボックスにライセンスキーを入力し、追加ボタンを押下してください。必要なライセンス分、実施してください。

図 5-9 機能ライセンスの追加

トップ > 共通 > ライセンス > 機能ライセンス追加

機能ライセンス

ライセンス追加

ライセンスキード

**追加** キャンセル

基本ライセンス、管理対象スイッチ拡張、および外部連携ライセンスを追加した場合の画面を下記に示します。

図 5-10 ライセンス画面

トップ » 共通 » ライセンス

ライセンス

ライセンス情報

機能	基本部 Syslog連携(CEF)
最大装置管理数	130 台
最大ワイヤレスLANコントローラ管理数	0 台

**機能ライセンス追加**

ライセンス種別	シリアル番号	有効期限		
■ 基本部	■ ■	2020/05/01 08:59:59 JST	<b>延長ライセンス追加</b>	<b>機能ライセンス削除</b>
■ 管理対象スイッチ拡張 +20台	■ ■	2020/05/01 08:59:59 JST	<b>延長ライセンス追加</b>	<b>機能ライセンス削除</b>
■ 管理対象スイッチ拡張 +100台	■ ■	2020/05/01 08:59:59 JST	<b>延長ライセンス追加</b>	<b>機能ライセンス削除</b>
■ Syslog連携(CEF)	■ ■	2020/05/01 08:59:59 JST	<b>ベンダ編集</b>	<b>延長ライセンス追加</b>

### 5.3.3 管理対象装置の設定

情報収集、およびセキュリティ制御を施す管理対象装置を追加します。

#### (1) 装置一覧画面の表示

ナビゲーションバーより、「装置」を選択し、そこから「装置一覧」を選択します。

図 5-11 ナビゲーションバーでの選択



図 5-12 装置一覧画面の表示



## (2) 装置の設定

「装置追加」ボタンを押下し、装置追加画面を表示してください。

図 5-13 装置追加ボタンの押下



管理対象装置として必要な情報を入力し、追加ボタンを押下してください。必要な装置分、実施してください。

下記例では、以下を入力しています。

表 5-2 装置追加の入力例

大項目	項目	内容
装置情報	装置名称	管理対象装置の名称として AX3660S_CoreSW を入力
	IP アドレス	管理対象装置のアクセス先 IP アドレスである 198.51.100.152 を入力
	装置モデル	管理対象装置の装置モデルである AX3660S を選択
	装置 MAC アドレス	AX3660S では装置 MAC アドレスは入力不可
	メンテナンスモード	メンテナンスモードとしないので、無効のまま
	コメント	管理対象装置の情報を示す情報としてコアスイッチを入力
収集情報	—	収集情報として ARP, MAC アドレスと LLDP を選択
SNMP アクセス情報	コミュニティ	管理対象装置の SNMP コミュニティ名称 public を入力
SSH ログイン情報	ログインユーザ名	管理対象装置の SSH ログインユーザ名である axsc を入力
	パスワード	管理対象装置の SSH ログインパスワードである HMjN1Ryq を入力
装置管理情報	装置管理者モードのパスワード	管理対象装置の装置管理者モードのパスワードである KpN4xmSc を入力
特定端末への Web 通信不可表示	有効/無効	AX3660S では特定端末への Web 通信不可表示は動作しないので、無効のまま
	ポート番号	AX3660S では特定端末への Web 通信不可表示は動作しないので、80 のまま

図 5-14 装置追加(1/2)

トップ > 共通 > 装置一覧 > 装置追加

### 装置追加

装置情報

装置名称	AX3660S_CoreSW
IPアドレス	198.51.100.152
装置モデル	AX3660S
装置MACアドレス	
メンテナンスマード	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
コメント	コアスイッチ

収集情報

<input checked="" type="checkbox"/> ARP	<input type="checkbox"/> NDP	<input checked="" type="checkbox"/> MACアドレス	<input checked="" type="checkbox"/> LLDP
<input type="checkbox"/> WLC			

図 5-15 装置追加(2/2)

The screenshot displays a configuration interface for adding a device, divided into four main sections:

- SNMPアクセス情報**:
  - コミュニティ:  (highlighted by a red box)
  - MIBオブジェクト(ARP/NDP):
  - MIBオブジェクト(MACアドレス):
  - MIBオブジェクト(LLDP):
    - LLDP-MIB
    - LLDP-V2-MIB
    - axslldp
  - MIBオブジェクト(WLC):
  - VLANリスト:  (highlighted by a red box) VLAN取得
- SSHログイン情報**:
  - ログインユーザ名:  (highlighted by a red box)
  - パスワード:  (highlighted by a red box) ログイン確認
- 装置管理情報**:
  - 装置管理者モードのパスワード:  (highlighted by a red box) 認証確認
- 特定端末へのWeb通信不可表示**:
  - 有効/無効:  有効  無効 (highlighted by a red box)
  - ポート番号:  (highlighted by a red box)

At the bottom right of the fourth panel are the buttons 追加 (highlighted by a red box) and キャンセル.

図 5-16 装置一覧画面の表示

The screenshot shows a web-based interface for managing devices. At the top, there's a breadcrumb navigation: トップ > 共通 > 装置一覧. Below it is a title bar with tabs: 装置追加, 装置検索, CSV形式で保存, CSV形式からの装置追加, and 事前コンフィグ設定確認結果一括出力. The 'CSV形式での装置追加' tab is currently selected. Underneath is a search bar with '表示カラム切替' (Column Switch), a dropdown for '件表示' (Items Displayed) set to 25, and a search input field labeled '検索'. A table follows, with columns: 装置情報 (Device Information), IPアドレス (IP Address), 装置モデル (Device Model), 端末状態 (Terminal Status), 接続数 (Connection Count), 遮断端末数 (Breakthrough Terminal Count), コンフィグ空き容量 (Config Free Capacity), and マントップ (Mantop). The table contains one row: AX3660S\_CoreSW, 198.51.100.152, AX3660S, ▲状態不明 (▲ Status Unknown), 0, 0, 未確認 (Not confirmed), and マントップ (Mantop). Below the table, a message says '1 件中 1 から 1 まで表示' (1 item from 1 to 1 displayed). At the bottom right are buttons for '前のページ' (Previous Page), '1' (Page 1), and '次のページ' (Next Page).

装置情報 ^	IPアドレス	装置モデル	端末状態	接続数	遮断端末数	コンフィグ空き容量	マントップ
AX3660S_CoreSW	198.51.100.152	AX3660S	▲状態不明	0	0	未確認	マントップ

### 5.3.4 接続情報設定の設定

「5.3.3 管理対象装置の設定」で設定した管理対象装置のうち、隣接する管理対象装置について、静的なポート接続情報の設定をおこないます。

#### (1) 接続情報設定の表示

ナビゲーションバーより、「装置」を選択し、そこから「接続情報設定」を選択します。

図 5-17 ナビゲーションバーでの選択



図 5-18 接続情報設定画面の表示



## (2) 接続情報の設定

「接続情報追加」ボタンを押下し、接続情報追加画面を表示してください。

図 5-19 接続情報追加ボタンの押下



接続情報として必要な情報を入力し、追加ボタンを押下してください。必要な接続情報分、実施してください。

下記例では、以下を入力しています。

表 5-3 接続情報追加の入力例

大項目	項目	内容
装置 A	名称	隣接する管理対象装置(装置 A-装置 B)の装置 A の名称として AX3660S_CoreSW を入力
	ポート番号	ポートとして、AX3660S_CoreSW の 1/0/1 を入力
	アクセスリスト拡張ポート	隣接する装置 B がセキュリティフィルタを適用できる AX2500S であるため、無効のまま

大項目	項目	内容
装置 B	名称	隣接する管理対象装置(装置 A-装置 B)の装置 B の名称として AX2500S_Edge を入力
	ポート番号	ポートとして、AX2500S_Edge の 0/1 を入力
	アクセリスト 拡張ポート	隣接する装置 A がセキュリティフィルタを適用できる AX3660S であるため、無効のまま

図 5-20 接続情報追加

トップ > 共通 > 接続情報設定 > 接続情報追加

接続情報追加

接続情報追加	
装置A	名称 AX3660S_CoreSW
	ポート番号 1/0/1
アクセスリスト 拡張ポート	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
装置B	名称 AX2500S_Edge
	ポート番号 0/1
アクセスリスト 拡張ポート	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
<b>追加</b> <b>キャンセル</b>	

### 5.3.5 共通設定の設定

「5.3.3 管理対象装置の設定」で設定した管理対象装置のうち、WAN 接続ポートであるインターネット回線やサーバ向けの回線に接続した管理対象装置について、WAN 接続ポートの設定をおこないます。

#### (1) 共通設定画面の表示

ナビゲーションバーより、「管理」を選択し、そこから「共通設定」を選択します。

図 5-21 ナビゲーションバーでの選択



図 5-22 共通設定画面の表示

トップ > 共通 > 共通設定

### 共通設定

ベーシック認証

ベーシック認証  有効  無効

ユーザ名

パスワード

エイリアス未登録端末

通信遮断  有効  無効

(略)

WAN接続ポート

**WAN接続ポート追加**

表示カラム切替	25 ▾ 件表示	検索: <input type="text"/>
装置名称 ^	ポート番号	操作
データがありません 0 件中 0 から 0 まで表示		

前のページ 次のページ

## (2) WAN 接続ポートの設定

「WAN 接続ポート追加」ボタンを押下し、WAN 接続ポート追加画面を表示してください。

図 5-23 WAN 接続ポート追加ボタンの押下



WAN 接続ポートとして必要な情報を入力し、追加ボタンを押下してください。必要な WAN 接続ポート分、実施してください。

下記例では、以下を入力しています。

表 5-4 WAN 接続ポート追加の入力例

大項目	項目	内容
WAN 接続ポート	装置	管理対象装置として AX3660S_CoreSW を入力
	ポート	ポートとして、AX3660S_CoreSW の 1/0/1 を入力

図 5-24 WAN 接続ポート追加

トップ » 共通 » 共通設定 » WAN接続ポート追加

### WAN接続ポート追加

WAN接続ポート

装置  
AX3660S\_CoreSW

ポート  
1/0/1

追加 キャンセル

### 5.3.6 トレンドマイクロ DDI/TMPM との連携の設定

トレンドマイクロ DDI/TMPM との連携の設定をおこないます。

#### (1) TMPM 連携設定

トレンドマイクロ DDI/TMPM 連携において、ミラー先ポートの設定をおこないます。ライセンス「外部連携：トレンドマイクロ DDI/PM との連携」が有効である必要があります。

##### (a) TMPM 連携設定画面の表示

ナビゲーションバーより、「管理」を選択し、そこから「TMPM 連携設定」を選択します。

図 5-25 ナビゲーションバーでの選択



図 5-26 TMPM 連携設定画面の表示



## (b) 詳細ミラー用のミラー先ポートの設定

「ミラー先ポート追加」ボタンを押下し、ミラー先ポート追加画面を表示してください。

図 5-27 ミラー先ポート追加ボタンの押下



詳細ミラー用のミラー先ポートとして必要な情報を入力し、追加ボタンを押下してください。必要なミラー先ポート分、実施してください。

下記例では、以下を入力しています。

表 5-5 ミラー先ポート追加の入力例

大項目	項目	内容
ミラー先ポート	装置	管理対象装置として AX3660S_CoreSW を入力
	ポート	ポートとして、AX3660S_CoreSW の 1/0/2 を入力

図 5-28 ミラー先ポート追加



### 5.3.7 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設定

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設定をおこないます。

#### (1) 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設定

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において、ナビゲーションバーより、「管理」を選択し、そこから「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設定」を選択してミラー先ポートの設定をおこないます。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」

が有効である必要があります。設定方法については TMPM 連携設定画面を参照してください。

### 5.3.8 Syslog 連携(CEF)との連携の設定

Syslog 連携(CEF)との連携の設定をおこないます。

#### (1) Syslog 連携(CEF)との連携設定

CEF(Common Event Format)の Syslog 送信をサポートしているセキュリティ装置との連携において、ミラー先ポートの設定をおこないます。

##### (a) 共通設定画面の表示

ナビゲーションバーより、「管理」を選択し、そこから「共通設定」を選択します。

図 5-29 ナビゲーションバーでの選択



図 5-30 共通設定画面の表示

The screenshot shows the 'Common Settings' page with two main sections:

- ベーシック認証 (Basic Authentication):** Contains fields for 'ユーザ名' (User Name) and 'パスワード' (Password), both with masked input fields.
- エイリアス未登録端末 (Unregistered Alias Device):** Contains a '通信遮断' (Communication Blocking) section with radio buttons for '有効' (Enabled) and '無効' (Disabled).

(略)

This is a sub-page for adding mirror ports. It has a header 'Syslog連携(CEF)のミラー先ポート' and a button 'ミラー先ポート追加' (Mirror Port Addition) which is highlighted with a red box. Below the button are two columns: '装置名称' (Device Name) and 'ポート番号' (Port Number).

### (b) 詳細ミラー用のミラー先ポートの設定

「ミラー先ポート追加」ボタンを押下し、ミラー先ポート追加画面を表示してください。

図 5-31 ミラー先ポート追加ボタンの押下

This screenshot is identical to the one above, but the 'ミラー先ポート追加' (Mirror Port Addition) button is explicitly highlighted with a red rectangular box.

詳細ミラー用のミラー先ポートとして必要な情報を入力し、追加ボタンを押下してください。必要なミラー先ポート分、実施してください。

下記例では、以下を入力しています。

表 5-6 ミラー先ポート追加の入力例

大項目	項目	内容
ミラー先ポート	装置	管理対象装置として AX3660S_CoreSW を入力
	ポート	ポートとして、AX3660S_CoreSW の 1/0/2 を入力

図 5-32 ミラー先ポート追加



## (2) Syslog 連携(CEF)で連携するセキュリティ装置のベンダ設定

### (a) ライセンス設定画面の表示

ナビゲーションバーより、「管理」を選択し、そこから「ライセンス」を選択します。

図 5-33 ナビゲーションバーでの選択



## (b) ベンダ編集画面の表示

ライセンス一覧画面から「Syslog 連携(CEF)」の「ベンダ編集」ボタンを押下し、ベンダ編集画面を表示してください。

図 5-34 ベンダ編集画面の表示

機能	シリアル番号	有効期限	操作
基本部		2020/11/01 08:59:59 JST	<button>延長ライセンス追加</button> <button>機能ライセンス削除</button>
管理対象スイッチ拡張 +20台		2020/11/01 08:59:59 JST	<button>延長ライセンス追加</button> <button>機能ライセンス削除</button>
管理対象スイッチ拡張 +100台		2020/11/01 08:59:59 JST	<button>延長ライセンス追加</button> <button>機能ライセンス削除</button>
トレンドマイクロ DDI/TMPM連携		2020/11/01 08:59:59 JST	<button>延長ライセンス追加</button> <button>機能ライセンス削除</button>
Syslog連携 (CEF)		2020/11/01 08:59:59 JST	<button>ベンダ編集</button> <button>延長ライセンス追加</button> <button>機能ライセンス削除</button>

## (c) ベンダ名称の登録

ベンダ編集画面のベンダ名称に連携するセキュリティ装置が送信する syslog の「Device Vendor」に格納されているベンダ名称を入力し、追加ボタンを押下してください。

下記例では、以下を入力しています。

表 5-7 ベンダ編集の入力例

大項目	項目	内容
ベンダ名称登録	ベンダ名称	ベンダ名称として ALAXALA Networks を入力

図 5-35 ベンダ編集画面の表示



### 5.3.9 セグメンテーションセキュリティの設定

セグメンテーションセキュリティを使用する場合、セグメントの設定をおこないます。

#### (1) 信頼済みセグメントの設定

セキュリティフィルタ適用外とする信頼済みセグメントに、セグメント定義をおこないます。

##### (a) セグメント一覧画面の表示

ナビゲーションバーより、「セグメント」を選択し、そこから「セグメント一覧」を選択します。

図 5-36 ナビゲーションバーでの選択



図 5-37 セグメント一覧画面の表示

セグメント一覧画面の表示内容：

トップ > 共通 > セグメント一覧

セグメント一覧

セグメント追加	CSV形式で保存	CSV形式からのセグメント追加				
表示カラム切替	25 ▾ 件表示	検索: <input type="text"/>				
セグメント名称 ^	優先度	状態	端末接続数	遮断端末数	コメント	操作
信頼済みセグメント	1	設定済み	0	0		
無所属セグメント	10000	設定済み	0	0		

2 件中 1 から 2 まで表示

前のページ 1 次のページ

### (b) 信頼済みセグメントの表示

セグメント一覧画面から信頼済みセグメントを選択し、セグメント設定画面を表示してください。

図 5-38 信頼済みセグメントの選択

The screenshot shows a web-based application interface for managing segments. At the top, there is a breadcrumb navigation: トップ > 共通 > セグメント一覧. Below it, a title 'セグメント一覧' is displayed. A horizontal menu bar contains three buttons: 'セグメント追加' (Segment Add), 'CSV形式で保存' (Save in CSV format), and 'CSV形式からのセグメント追加' (Add segments from CSV format). Below the menu, there are search and filter options: '表示カラム切替' (Change display columns), '件表示' (Number of items displayed) set to 25, and a search input field labeled '検索'. The main table lists segments with the following columns: 'セグメント名称' (Segment Name), '優先度' (Priority), '状態' (Status), '端末接続数' (Number of connected devices), '遮断端末数' (Number of blocked devices), 'コメント' (Comment), and '操作' (Operations). Two rows are visible: '信頼済みセグメント' (Priority 1, Status: 設定済み, 0 devices, 0 blocked devices) and '無所属セグメント' (Priority 10000, Status: 設定済み, 0 devices, 0 blocked devices). The first row is highlighted with a red border. At the bottom of the table, it says '2 件中 1 から 2 まで表示' (Displaying 1 to 2 of 2 items). Navigation buttons at the bottom right include '前のページ' (Previous page), a page number '1', and '次のページ' (Next page).

図 5-39 セグメント設定画面の表示

The screenshot shows a detailed configuration page for the selected segment. At the top, the breadcrumb navigation includes 'セグメント一覧 > セグメント設定 (信頼済みセグメント)'. The title of the page is 'セグメント設定 (信頼済みセグメント)'. The first section, 'セグメント情報', contains fields for 'セグメント名称' (Segment Name) with the value '信頼済みセグメント', '優先度' (Priority) with the value '1', and 'コメント' (Comment) with an empty input field. A blue '更新' (Update) button is located to the right of this section. The second section, 'セグメント定義', has a similar header and includes a horizontal menu bar with 'セグメント定義追加', 'CSV形式で保存', and 'CSV形式からのセグメント定義追加'. It also features a search input field and filter options. Below this, it displays a message 'データがありません' (No data available) and '0 件中 0 から 0 まで表示' (Displaying 0 to 0 of 0 items). Navigation buttons at the bottom right are identical to those in the previous screenshot.

### (c) セグメント定義の追加

「セグメント定義追加」ボタンを押下し、セグメント定義追加画面を表示してください。

図 5-40 セグメント定義追加ボタンの押下

セグメント定義を入力し、追加ボタンを押下してください。

下記例では、以下を入力しています。

表 5-8 セグメント定義追加の入力例

大項目	項目	内容
セグメント定義	セグメント種別	セグメント種別として IP サブネットを選択
	IP アドレス/マスク	IP アドレス/マスクとして、192.168.9.0/24 を入力

図 5-41 セグメント定義追加

トップ > 共通 > セグメント一覧 > セグメント設定(信頼済みセグメント) > セグメント定義追加

セグメント定義追加(信頼済みセグメント)

セグメント定義

セグメント種別	IPサブネット
IPアドレス/マスク	192.168.9.0/24
MACアドレス	[Input Field]
装置名称	[Input Field]
ポート番号	<nif>/<port> or <switch>/<nif>/<port>

追加 キャンセル

### 5.3.10 マップの設定

マップを使用する場合、マップの設定をおこないます。

#### (1) マップ一覧画面の表示

ナビゲーションバーより、「マップ」を選択し、そこから「マップ一覧」を選択します。

図 5-42 ナビゲーションバーでの選択



図 5-43 マップ一覧画面の表示

マップ一覧画面には、ナビゲーションメニュー（トップ &gt; 共通 &gt; マップ一覧）と「マップ一覧」セクションがあります。セクション内には、マップ追加、CSV形式で保存、CSV形式からのマップ追加、背景画像保存、背景画像追加などのボタンがあります。表示カラム切替、件数表示（25）、検索欄、マップ名検索、背景画像、コメント、操作などのフィルタリングオプションがあります。メッセージには「データがありません」と表示され、「0 件中 0 から 0 まで表示」とあります。ページ底部には「前のページ」「次のページ」ボタンがあります。

## (2) マップの追加

「マップ追加」ボタンを押下し、マップ追加画面を表示してください。

図 5-44 マップ追加ボタンの押下



マップとして必要な情報を入力し、追加ボタンを押下してください。必要なマップ分、実施してください。

下記例では、以下を入力しています。

表 5-9 マップ追加の入力例

大項目	項目	内容
マップ情報	マップ名称	マップ名称としてフロア 1F マップを入力
対象装置	チェックボックス	マップの対象装置として、装置情報 AX2500S_Edge のチェックボックスをチェック

図 5-45 マップ追加

トップ > 共通 > マップ一覧 > マップ追加

### マップ追加

マップ情報

マップ名称  (赤枠)

背景画像  
別のマップで使用している背景画像から選択する：

新たに画像ファイルをアップロードする：  
 選択されていません

集線装置表示  有効  無効

表示エイリアス

コメント

対象装置

表示カラム切替	25 ▼ 件表示	検索:						
チェックボックス	装置情報 ^	IPアドレス	装置モデル	状態	端末接続数	遮断端末数	コメント	所属マップ
<input checked="" type="checkbox"/>	AX2130S_EdgeSW	192.0.2.3	AX2100S	正常	8	0		フロア1Fマップ
<input type="checkbox"/>	AX3660S_CoreSW	192.0.2.2	AX3660S	正常	1	0		フロア1Fマップ

2 件中 1 から 2 まで表示

前のページ 1 次のページ

## 6. AX-Security-Controller(Manager)の Web インタフェース

---

この章では、AX-Security-Controller(Manager)の Web インタフェースについて説明します。

---

## 6.1 共通

共通の Web インタフェースを説明します。

### 6.1.1 ナビゲーションバー

図 6-1 ナビゲーションバー



表 6-1 ナビゲーションバーより移動可能な機能の一覧

項目	機能	説明	参照先
ダッシュボード	—	機能のサマリーを表示します。AX-Security-Controller(Manager)のトップ画面です。	6.1.2
端末	端末一覧	管理対象装置から収集した端末の一覧を表示します。	6.1.3(1)
	エイリアス	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)の一覧を表示します。およびエイリアスの追加、編集、削除を管理します。	6.1.3(2)
装置	装置一覧	管理対象装置の一覧を表示します。および管理対象装置の追加、変更、および削除を管理します。	6.1.4(1)
	接続情報設定	接続情報の一覧を表示します。および接続情報の追加、削除を管理します。	6.1.4(2)

項目	機能	説明	参照先
	ポートエイリアス	装置名称とポート番号に呼応するポートエイリアスの一覧を表示します。およびポートエイリアスの追加, 編集, 削除を管理します。	6.1.4(3)
	管理対象外ポート	装置名称とポート番号に呼応する管理対象外ポート一覧を表示します。および管理対象外ポートの追加, 削除を管理します。	6.1.4(4)
セグメント	セグメント一覧	セグメントの一覧を表示します。およびセグメントの追加, 変更, および削除を管理します。	6.1.5(1)
	セグメント詳細	セグメントの詳細を表示します。	6.1.5(2)
セキュリティ装置連携	セキュリティフィルター一覧	適用中のセキュリティフィルターの一覧を表示します。	6.1.6(1)
	セキュリティフィルタ履歴	削除したすべてのセキュリティフィルターの一覧を表示します。	6.1.6(3)
	ルールマッチ履歴	Syslog クライアントのインシデント抽出ルールにマッチした一覧を表示します。	6.1.6(5)
	Syslog 受信履歴	Syslog クライアントから受信した Syslog メッセージ一覧を表示します。	6.1.6(6)
	Syslog クライアント一覧	Syslog クライアント一覧を表示します。および Syslog クライアントの追加, 削除と, Syslog クライアントごとのインシデント抽出ルールの追加, 削除を管理します。	6.1.6(7)
マップ	マップ一覧	マップの一覧を表示します。およびマップの追加, 編集, および削除を管理します。	6.1.7(1)
	マップ設定	マップに表示する下記のアイコンを設定します。 ・装置アイコンの一覧を表示します。および、装置アイコンの編集, 削除を管理します。 ・集線装置アイコンの一覧を表示します。および、集線装置アイコンの追加, 編集, 削除を管理します。 ・端末アイコンの一覧を表示します。および端末アイコンの追加, 編集, 削除を管理します。	6.1.7(2)

項目	機能	説明	参照先
管理	共通設定	<p>下記の設定を管理します。</p> <ul style="list-style-type: none"> <li>・ Basic 認証の設定</li> <li>・ エイリアス未登録端末の設定</li> <li>・ 遮断端末一覧(AX-Security-Controller(Viewer)用の見出し)の設定</li> <li>・ 装置情報収集の設定</li> <li>・ WAN 接続ポートの設定</li> <li>・ 永続設定ポート(受信側)の設定</li> <li>・ 永続設定ポート(送信側)の設定</li> <li>・ Syslog 連携(CEF)のミラーポートの設定</li> <li>・ セキュリティフィルタ自動解除スケジュールの設定</li> </ul>	6.1.8(1)
	通知設定	<p>コントローラで発生したイベントや状態を通知するための設定をおこないます。</p> <ul style="list-style-type: none"> <li>・ Syslog 通知</li> <li>・ E-mail 通知</li> </ul>	6.1.8(2)
	画像管理	AX-Security-Controller(Manager)で扱う画像の一覧を表示します。および画像の追加、編集、削除を管理します。	6.1.8(3)
	レポート	コントローラで発生したイベントに関するレポートの一覧を表示します。	6.1.8(4)
	ライセンス	ライセンスの追加、削除を管理します。	6.1.8(5)
	メンテナンス	保守情報の保存をおこないます。	6.1.8(6)
	TMPM 連携設定	TMPM 連携の設定をおこないます(ライセンス「外部連携トレンドマイクロ DDI/TMPM との連携」有効時)。	6.2
	パロアルトネットワークス 次世代ファイアーウォール連携設定	パロアルトネットワークス 次世代ファイアーウォール連携の設定をおこないます(ライセンス「外部連携パロアルトネットワークス 次世代ファイアーウォールとの連携」有効時)。	6.3

## 6.1.2 ダッシュボード

図 6-2 ダッシュボード画面



表 6-2 ダッシュボードに表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	更新ボタン	ボタン押下で画面を更新します。

項目番	内容	説明
③	運用状況	<p>各種収集した情報を円グラフで表示します。</p> <ul style="list-style-type: none"> <li>・端末 AX-Security-Controller が認識している端末数(円グラフの中の数値)と、通信遮断中の端末数(左上の数値)を表示します。 円グラフは、正常と遮断中の端末数を表示します。</li> <li>・装置 追加済み装置について、登録した装置数(円グラフの中)と、失敗して状態が不明な装置数(左上の数値)を表示します。 円グラフは、正常、メンテナンス中、状態不明、およびライセンス上限オーバーの装置数を表示します。</li> <li>・セキュリティ装置連携 セキュリティ装置からのセキュリティフィルタについて、登録した数(円グラフの中)と、設定中の数(左上の数値)を表示します。 円グラフは、設定済と設定中のセキュリティフィルタ数を表示します。</li> </ul>
④	セキュリティフィルタ実行情報	最新 10 件のセキュリティフィルタを表示します。 セキュリティフィルタのエントリを押下すると、「6.1.6(2) セキュリティフィルタ詳細」に移動します。

### 6.1.3 端末

#### (1) 端末一覧

図 6-3 端末一覧画面

The screenshot shows the 'Device List' page of the AX-Security-Controller(Manager) web interface. The page has a header with a breadcrumb trail: 'トップ > 共通 > 端末一覧'. Below the header are several buttons: 'CSV形式で保存' (②), '選択端末の通信遮断' (③), and '選択端末のセキュリティフィルタ解除' (④). There is also a '表示カラム切替' button (⑤), a dropdown for '件表示' (⑥), a search input field (⑦), and a column header for '接続先AP' (⑩). The main table lists 12 device entries, each with columns for IP Address, MAC Address, Connection Target Device, Port Number, Operation, and Connection Target AP. The third entry in the list (IP 198.51.100.55) is highlighted with a red box, and its 'Operation' column contains two buttons: '通信遮断解除' (⑪) and 'セキュリティフィルタ解除'. At the bottom, there is a pagination bar with buttons for '前のページ', page numbers 1, 2, 3, and '次のページ', and a red box around the page number 1.

IPアドレス	MACアドレス	接続先装置	ポート番号	操作	接続先AP
198.51.100.53	0000.5e00.5353	Edge-SW-001	0/10	<span style="background-color: #f00; color: white;">通信遮断</span>	AP0000.5E00.5360
198.51.100.54	0000.5e00.5354	Edge-SW-001	0/9	<span style="background-color: #f00; color: white;">通信遮断</span>	-
198.51.100.55	0000.5e00.5355	Edge-SW-001	0/9	<span style="background-color: #00c080; color: white;">通信遮断解除</span>	-
198.51.100.56	0000.5e00.5356	Edge-SW-001	0/9	<span style="background-color: #f00; color: white;">通信遮断</span>	-
198.51.100.57	0000.5e00.5357	Edge-SW-001	0/9	<span style="background-color: #f00; color: white;">通信遮断</span>	-
198.51.100.58	0000.5e00.5358	Edge-SW-001	0/9	<span style="background-color: #f00; color: white;">通信遮断</span>	-
	0000.5e00.5359	Edge-SW-001	0/9	<span style="background-color: #f00; color: white;">通信遮断</span>	-
198.51.100.60	0000.5e00.5360	Edge-SW-001	0/10	<span style="background-color: #f00; color: white;">通信遮断</span>	-
198.51.100.61	0000.5e00.5361	Edge-SW-001	0/10	<span style="background-color: #f00; color: white;">通信遮断</span>	-
198.51.100.62	0000.5e00.5362	Edge-SW-001	0/10	<span style="background-color: #f00; color: white;">通信遮断</span>	-

表 6-3 端末一覧に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	CSV 形式で保存ボタン	ボタンを押下すると、一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「hosts.csv」になります。

項目番号	内容	説明
③	選択端末の通信遮断ボタン	ボタンを押下すると、 選択した端末 MAC アドレスを通信遮断します(<個別選択チェックボックスの選択済み端末件数>件) 通信遮断されるまで時間がかかる場合があります の確認ダイアログを表示します。了承した場合、 実行する場合は YES と入力してください  の確認ダイアログを表示します。YES を入力して 了承した場合、選択した個別選択チェックボックス の端末 <sup>※1</sup> について、セキュリティフィルタの通 信遮断を適用します。反映が失敗すると、「表 6-7 選択端末の通信遮断の反映失敗時のダイア ログ一覧」に示すダイアログを表示します。
④	選択端末のセキュリティフィルタ解除ボタン	ボタンを押下すると、 選択した端末 MAC アドレスのセキュリティフィ ルタを解除します(<個別選択チェックボックスの 選択済み端末件数>件) セキュリティフィルタが解除されるまで時間がか かる場合があります  の確認ダイアログを表示します。了承した場合、 実行する場合は YES と入力してください  の確認ダイアログを表示します。YES を入力して 了承した場合、選択した個別選択チェックボックス の端末 <sup>※1</sup> について、該当する端末に適用してい るすべてのセキュリティフィルタを解除します。 反映が失敗すると、「表 6-8 選択端末のセキュ リティフィルタ解除の反映失敗時のダイアロー グ一覧」に示すダイアログを表示します。
⑤	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑥	ページあたり表示件数 切替プルダウン	1 ページあたりに表示する件数を切り替えること ができます。件数のパターンは 10/25/50/100/全 ての 5 パターンです。
⑦	検索テキストボックス	テキストボックスに入力した文字列に該当する行 のみに一覧を絞り込むことができます。
⑧	全選択チェックボックス	検索テキストボックス、および表示カラムごと検 索テキストボックスにより絞り込んだ、すべての 端末を通信遮断、またはセキュリティフィルタ解 除対象とします。もう一度選択すると、すべての 端末を通信遮断、またはセキュリティフィルタ解 除対象から外します。

項目番	内容	説明
⑨	個別選択チェックボックス	選択した端末を通信遮断、またはセキュリティフィルタ解除対象とします。もう一度選択すると、通信遮断、またはセキュリティフィルタ解除対象から外します。
⑩	表示カラムごと検索テキストボックス	表示カラムごとに、テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑪	端末一覧	<p>収集した情報から端末の一覧を表示します。表示項目は、端末の IP アドレス/MAC アドレス/ベンダ/エイリアス<sup>*2</sup>/接続先装置/ポート番号/ポートエイリアス/VLAN ID<sup>*3</sup>/セグメント/操作/セキュリティフィルタ適用状態/マップ/接続先 AP です。接続先装置の装置モデルが標準 MIB 対応装置かつ MIB オブジェクト(MAC アドレス)が dot1dTpFdbPort の場合、VLAN ID は空文字列です。</p> <p>操作は、通信遮断、または通信遮断解除・セキュリティフィルタ解除ボタンが表示され、以下に示す動作をおこないます。なお、信頼済みセグメントに所属している場合、ボタンを押下することはできません。</p> <ul style="list-style-type: none"> <li>「通信遮断」ボタンを押下すると、</li> </ul> <p style="margin-left: 2em;">端末 MAC アドレス &lt;MAC アドレス&gt; を通信遮断します</p> <p style="margin-left: 2em;">の確認ダイアログを表示します。了承した場合、セキュリティフィルタの通信遮断を適用します。反映が失敗すると、「表 6-4 通信遮断の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p> <ul style="list-style-type: none"> <li>「通信遮断解除」ボタンを押下すると、</li> </ul> <p style="margin-left: 2em;">端末 MAC アドレス &lt;MAC アドレス&gt; のセキュリティフィルタの通信遮断を解除します</p> <p style="margin-left: 2em;">の確認ダイアログを表示します。了承した場合、該当する端末に適用しているすべてのセキュリティフィルタの通信遮断を解除します。反映が失敗すると、「表 6-5 通信遮断解除の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p>

項目番号	内容	説明
		<ul style="list-style-type: none"> <li>「セキュリティフィルタ解除」ボタンを押下すると、 端末 MAC アドレス &lt;MAC アドレス&gt; のセキュリティフィルタを一括解除します  の確認ダイアログを表示します。了承した場合、 該当する端末に適用しているすべてのセキュリ ティフィルタを解除します。 反映が失敗すると、「表 6-6 セキュリティフィ ルタ解除の反映失敗時のダイアログ一覧」に示す ダイアログを表示します。 セキュリティフィルタ適用状態は、該当する端末 に適用しているセキュリティフィルタの一覧をボ タンで表示します。ボタンを押下すると、 「6.1.6(2) セキュリティフィルタ詳細」に移動し ます。</li> <li>「表示」ボタンを押下すると、「6.1.7(1)(b) マップ」に移動し、該当する端末のアイコンに影 を付与して明示します（表示例：）。</li> </ul>
(12)	ページ切替ボタン	ボタンを押下すると、指定のページを表示しま す。

## 注※1

任意の端末の個別選択チェックボックスが選択された状態で、検索テキストボックスまたはカラムごと検索テキストボックスで絞り込みをおこない、該当端末が表示されない場合でも、該当端末は通信遮断、またはセキュリティフィルタ解除対象のままです。この状態でボタンを押下すると、該当端末の通信遮断、またはセキュリティフィルタ解除が実施されることに注意してください。

個別選択チェックボックスの選択は、検索テキストボックスまたはカラムごと検索テキストボックスで絞り込みをおこなった後におこなうようにしてください。

## 注※2

「(2)(a), (2)(c)」で1つ以上のエイリアスの設定をおこなった場合、複数のタイトルカラムに展開して表示します。タイトルカラムと、端末に対応する「(2) エイリアス」のタイトルが一致しない場合、値には None を表示します。

## 注※3

下記管理対象装置で学習した端末の VLAN は、VLAN ID を表示しません。

- 標準 MIB 対応装置

MIB オブジェクト(MAC アドレス)が「dot1dTpFdbPort」の場合、「空白("")」になります。

MIB オブジェクト(MAC アドレス)が「dot1qTpFdbPort」の場合、  
「dot1qTpFdbPort で収集した dot1qFdbId の値」になります。

表 6-4 通信遮断の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	要求パラメータに間違があります	要求のパラメータに間違があります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

表 6-5 通信遮断解除の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	要求パラメータに間違があります	要求のパラメータに間違があります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

表 6-6 セキュリティフィルタ解除の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	要求パラメータに間違があります	要求のパラメータに間違があります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

表 6-7 選択端末の通信遮断の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	端末が選択されていません	端末が選択されていません。個別選択チェックボックスを1つ以上選択してください。
2	選択端末の通信遮断で選択可能な端末は最大 500 件です	選択端末の通信遮断で選択可能な端末は最大 500 件です。選択した個別選択チェックボックスを見直してください。
3	選択した端末はすべて通信遮断が適用されています	選択した端末はすべて通信遮断が適用されています。選択した個別選択チェックボックスを見直してください。

項目番号	内容	説明
4	要求パラメータに間違があります	要求のパラメータに間違いがあります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
5	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

表 6-8 選択端末のセキュリティフィルタ解除の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	端末が選択されていません	端末が選択されていません。個別選択チェックボックスを1つ以上選択してください。
2	選択端末のセキュリティフィルタ解除で選択可能な端末は最大 50000 件です	選択端末のセキュリティフィルタ解除で選択可能な端末は最大 50000 件です。選択した個別選択チェックボックスを見直してください。
3	選択した端末はすべてセキュリティフィルタが適用されていません	選択した端末はすべてセキュリティフィルタが適用されていません。選択した個別選択チェックボックスを見直してください。
4	要求パラメータに間違があります	要求のパラメータに間違いがあります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
5	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (2) エイリアス

図 6-4 エイリアス一覧画面

図 6-4 エイリアス一覧画面のスクリーンショットです。画面には、IPアドレス、用途（OA）、端末名（OA端末1～OA端末18）が表示されるリストがあります。各リスト行には「編集」（青いボタン）と「削除」（赤いボタン）の操作ボタンがあります。また、画面下部にはページナビゲーション用のボタン群があります。

IP	用途	端末名	操作
IP:198.51.100.1	OA	OA端末1	編集 削除
IP:198.51.100.10	OA	OA端末10	編集 削除
IP:198.51.100.11	OA	OA端末11	編集 削除
IP:198.51.100.12	OA	OA端末12	編集 削除
IP:198.51.100.13	OA	OA端末13	編集 削除
IP:198.51.100.14	OA	OA端末14	編集 削除
IP:198.51.100.15	OA	OA端末15	編集 削除
IP:198.51.100.16	OA	OA端末16	編集 削除
IP:198.51.100.17	OA	OA端末17	編集 削除
IP:198.51.100.18	OA	OA端末18	編集 削除

表 6-9 エイリアス一覧に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	エイリアス追加ボタン	新規にエイリアスを追加します。ボタンを押下すると「(a) エイリアス追加」に移動します。
③	CSV形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「hosts_alias.csv」となります。
④	CSV形式からのエイリアス追加ボタン	CSV 形式のファイルから 1 個以上のエイリアスを追加、または置き換えることができます。ボタンを押下すると「(b) CSV 形式からのエイリアス追加」に移動します。

項目番号	内容	説明
⑤	エイリアス未登録端末一覧を CSV 形式で保存ボタン	ボタンを押下すると現在のエイリアス未登録の端末一覧を CSV 形式でダウンロードできます。ファイル名は「hosts_alias_unregistered.csv」となります。 本ボタンは、下記いずれかの端末接続のエイリアス未登録接続を有効にした場合だけ、エイリアス未登録端末の端末一覧を格納します。 <ul style="list-style-type: none"> <li>・Syslog サーバ            「6.1.8(2)(a) Syslog サーバ追加」            「6.1.8(2)(c) Syslog サーバ編集」</li> <li>・E-mail 通知先            「6.1.8(2)(d) E-mail 通知先追加」            「6.1.8(2)(f) E-mail 通知先編集」</li> </ul>
⑥	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑦	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑧	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑨	エイリアス情報	エイリアス情報の一覧を表示します。 表示項目は、条件/エイリアスです。 エイリアスは、複数のタイトルカラムに展開して表示します。各エントリのタイトルがタイトルカラムに存在しない場合、値には None を表示します。
⑩	エイリアスの編集ボタン	操作として、エイリアスの編集をおこないます。ボタンを押下すると、「(c) エイリアス編集」に移動します。
⑪	エイリアスの削除ボタン	操作として、エイリアスの削除をおこないます。ボタンを押下すると、  エイリアス <条件> を削除します  の確認ダイアログを表示します。了承した場合、エイリアスを削除します。削除が失敗すると、「表 6-10 エイリアス一覧の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑫	ページ切替ボタン	ボタンを押下すると指定のページを表示します。

表 6-10 エイリアス一覧の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	指定したエイリアスが存在しません	指定したエイリアスが存在しません。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) エイリアス追加

図 6-5 エイリアス追加画面

表 6-11 エイリアス追加に表示する項目

項目番号	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	条件	IP アドレス	エイリアスに対応する IPv4 アドレスまたは IPv6 アドレスを入力します。 空白, 0.0.0.0~255.255.255.255, または::~ffff:ffff:ffff:ffff:ffff:ffff を入力してください。ただし, IPv6 リンクローカルアドレスは入力できません。

項目番	内容		説明
③		MAC アドレス	エイリアスに対応する MAC アドレスを入力します。 空白、または 0000.0000.0000～ffff.ffff.ffff を入力してください。
④	項目	タイトル	エイリアスを示すタイトルを入力します。 最大 256 文字登録可能です。
⑤		値	タイトルに対応する値を入力します。最大 256 文字登録可能です。
⑥		+ボタン	+ボタンを押下すると、タイトルと値の組み合わせを追加することができます。最大 16 個の組み合わせを追加することができます。
⑦		-ボタン	-ボタンを押下するとタイトルと値の組み合わせを削除します。 タイトルと値の組み合わせが 1 つの場合、-ボタンを押下することはできません。
⑧	追加ボタン		エイリアス追加を反映します。 ボタンを押下し、同一条件のエイリアスが存在しなく反映が成功すると、「(2) エイリアス」に移動します。 同一条件のエイリアスが存在すると  既に追加済みのエイリアス条件です。上書きしますか  の確認ダイアログを表示します。了承し反映が成功すると、「(2) エイリアス」に移動します。 反映が失敗すると、「表 6-12 エイリアス追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑨	キャンセルボタン		エイリアス追加をキャンセルします。ボタンを押下すると、「(2) エイリアス」に移動します。

表 6-12 エイリアス追加の反映失敗時のダイアログ一覧

項目番	内容	説明
1	IP アドレスまたは MAC アドレスを入力してください	IP アドレス、および MAC アドレスが空白です。IP アドレス、または MAC アドレスを入力、または IP アドレスと MAC アドレス両方を入力してください。
2	IP アドレスのフォーマットが間違っています	IP アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
3	IPv6 グローバルアドレスを入力してください	IPv6 リンクローカルアドレスが入力されています。IPv6 グローバルアドレスを入力してください。

項目番号	内容	説明
4	MAC アドレスのフォーマットが間違っています	MAC アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
5	タイトルを入力するかタイトルが空の行を削除してください	エイリアスのタイトルを入力するか、タイトルが空の行を削除してください。
6	タイトルが重複しています	エイリアスのタイトルが重複しています
7	タイトルに[IP アドレス]および[MAC アドレス]は使用できません	エイリアスのタイトルに IP アドレスと MAC アドレスは使用できません。
8	エイリアスの値をひとつ以上入力してください	エイリアスの値は、1つ以上入力してください。
9	要求のパラメータに間違いがあります	要求のパラメータに間違があります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
10	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (b) CSV 形式からのエイリアス追加

図 6-6 CSV 形式からのエイリアス追加画面

CSV形式からのエイリアス追加

ファイル選択

② ファイルを選択 選択されていません

③ ④ 内容確認

表 6-13 CSV 形式からのエイリアス追加に表示する項目

項目番	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ファイル選択	ファイルを選択ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上のエイリアスを追加、または置き換えることができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
③		更新反映/置き換えラジオボタン	選択したファイルについて、更新反映をおこなうか、置き換えをおこなうかを選択します。 更新反映を選択した場合、AX-Security-Controller で管理しているエイリアス情報の上書きをおこない、かつ CSV ファイルだけに存在するエイリアスを追加します。 置き換えを選択した場合、AX-Security-Controller で管理しているエイリアス一覧を、CSV ファイルの内容に置き換えます。 CSV ファイル内に AX-Security-Controller で管理しているエイリアス情報がない場合、当該エイリアスは削除されます。
④		内容確認ボタン	更新反映ラジオボタン、または置き換えラジオボタンに従い、AX-Security-Controller で管理しているエイリアス一覧と、CSV ファイルの内容を比較・確認します。ボタンを押下すると、「図 6-7 CSV 形式からのエイリアス追加画面(適用内容含む)」を表示します。表示する項目は、「表 6-14 CSV 形式からのエイリアス追加(適用内容含む)に表示する項目」を参照ください。

図 6-7 CSV 形式からのエイリアス追加画面(適用内容含む)

The screenshot shows the 'CSV形式からのエイリアス追加' (Add Alias from CSV) page. At the top, there is a breadcrumb navigation: トップ > 共通 > エイリアス一覧 > CSV形式からのエイリアス追加. A red box labeled ① surrounds this area. Below the breadcrumb is a title 'CSV形式からのエイリアス追加'. The main area has a 'ファイル選択' (File Selection) section with a red box ② around the 'ファイルを選択' button and the file name 'hosts\_alias.csv'. There are two radio buttons: '更新反映' (Update Reflect) and '置き換え' (Replace), with '更新反映' selected. A red box ③ surrounds these buttons. To the right is a blue '内容確認' (Content Confirmation) button. The next section is '適用内容' (Applied Content) with a red box ④ around it. It contains a '表示カラム切替' (Column Switch) button ⑤, a dropdown for '件表示' (Number of items displayed) set to 25 ⑥, a '検索' (Search) input field ⑦, and a table showing applied content. The table has three rows: 'IP:203.0.113.1' (変更なし) ⑧, 'IP:203.0.113.2' (変更あり) ⑨, and 'IP:203.0.113.3' (追加). A red box ⑩ surrounds the search and table areas. At the bottom are '前のページ' (Previous page), '1' (Current page), and '次のページ' (Next page). The final row at the bottom has '適用' (Apply) and 'キャンセル' (Cancel) buttons, with a red box ⑪ around '適用' and another red box ⑫ around 'キャンセル'.

表 6-14 CSV 形式からのエイリアス追加(適用内容含む)に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ファイル選択	「表 6-13 CSV 形式からのエイリアス追加に表示する項目」を参照ください。
③	更新反映/置き換えラジオボタン	「表 6-13 CSV 形式からのエイリアス追加に表示する項目」を参照ください。
④	内容確認ボタン	「表 6-13 CSV 形式からのエイリアス追加に表示する項目」を参照ください。
⑤	適用内容	表示カラム切替ボタン
⑥		一覧から不要なカラムを非表示することができます。
	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。

項目番号	内容	説明
⑦	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑧	適用内容情報一覧	適用内容情報一覧を表示します。表示項目は、条件/適用内容です。適用内容は以下のいずれかです。 <ul style="list-style-type: none"><li>・追加</li><li>・変更あり</li><li>・変更なし</li><li>・削除</li></ul>
⑨	操作	操作は、差分表示ボタンが表示されます。差分表示ボタンを押下すると、更新反映ラジオボタン、または置き換えラジオボタンに従って CSV ファイル反映による適用前と適用後の変更箇所一覧をダイアログで表示します。 変更箇所一覧のダイアログの例を「図 6-8 変更箇所一覧画面」に示します。
⑩	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。
⑪	適用ボタン	更新反映ラジオボタン、または置き換えラジオボタンに従い、エイリアス追加を反映します。ボタンを押下し、反映をおこなうと、「(2) エイリアス」に移動します。
⑫	キャンセルボタン	エイリアス追加をキャンセルします。ボタンを押下すると、「(2) エイリアス」に移動します。

図 6-8 変更箇所一覧画面

変更箇所一覧		
項目	適用前	適用後
IPアドレス	203.0.113.2	203.0.113.2
MACアドレス		
端末名		OA端末2
用途	OA	OA

## (c) エイリアス編集

図 6-9 エイリアス編集画面

表 6-15 エイリアス編集画面に表示する項目

項目番号	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	条件	IP アドレス /MAC アドレス	追加済みのエイリアスに対応する IP アドレス/MAC アドレスを表示します。
③	項目	タイトル	エイリアスを示すタイトルを入力します。最大 256 文字登録可能です。
		値	タイトルに対応する値を入力します。最大 256 文字登録可能です。

項目番号	内容		説明
⑤		+ボタン	+ボタンを押下すると、タイトルと値の組み合わせを追加することができます。最大16個の組み合わせを追加することができます。
⑥		-ボタン	-ボタンを押下するとタイトルと値の組み合わせを削除します。 タイトルと値の組み合わせが1つの場合、-ボタンを押下することはできません。
⑦	更新ボタン		エイリアス編集を反映します。ボタンを押下し、反映が成功すると、「(2) エイリアス」に移動します。反映が失敗すると、「表 6-16 エイリアス編集の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑧	キャンセルボタン		エイリアス編集をキャンセルします。ボタンを押下すると、「(2) エイリアス」に移動します。

表 6-16 エイリアス編集の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	タイトルを入力するかタイトルが空の行を削除してください	エイリアスのタイトルを入力するか、タイトルが空の行を削除してください。
2	タイトルが重複しています	エイリアスのタイトルが重複しています
3	タイトルに[IP アドレス]および[MAC アドレス]は使用できません	エイリアスのタイトルに IP アドレスと MAC アドレスは使用できません。
4	エイリアスの値をひとつ以上入力してください	エイリアスの値は、1つ以上入力してください。
5	要求のパラメータに間違があります	要求のパラメータに間違があります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
6	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## 6.1.4 装置

### (1) 装置一覧

図 6-10 装置一覧画面

The screenshot shows the 'Device List' (装置一覧) page. At the top, there is a breadcrumb navigation: 'トップ > 共通 > 装置一覧'. Below it is a header with several buttons: '装置追加' (②), '装置検索' (③), 'CSV形式で保存' (④), 'CSV形式からの装置追加' (⑤), and '事前コンフィグ設定確認結果一括出力' (⑥). Further down are buttons for '表示カラム切替' (⑦), '件表示' (⑧), and a search field '検索:' (⑨). The main content area displays a table of device information:

装置情報	IPアドレス	モデル	状態	端末接続数	遮断端末数	コンフィグ空き容量	コメント	マップ
エッジスイッチ1	198.51.100.141	AX260A	正常 (⑩)	20	0	-		<button>表示 (⑪)</button>

Below the table, it says '1件中 1 から 1 まで表示'. At the bottom right, there are buttons for '前のページ' (Previous Page), '1' (Page 1), and '次のページ' (Next Page) (⑫).

表 6-17 装置一覧画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	装置追加ボタン	新規に管理対象装置を追加します。ボタンを押下すると「(a) 装置追加」に移動します。
③	装置検索ボタン	新規に管理対象装置を追加するための、管理対象装置の検索をおこないます。ボタンを押下すると「(f) 装置検索」に移動します。
④	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「nodes.csv」となります。
⑤	CSV 形式からの装置追加ボタン	CSV 形式のファイルから 1 個以上の装置を追加、または置き換えることができます。ボタンを押下すると「(c) CSV 形式からの装置追加」に移動します。

項目番	内容	説明
⑥	事前コンフィグ設定確認結果一括出力ボタン	<p>ボタンを押下すると、事前コンフィグ設定の確認結果を出力します。確認結果の出力が完了するまで時間がかかる、または対象装置からのコンフィグ取得に失敗する場合があります。</p> <p>の確認ダイアログを表示します。了承した場合、すべての管理対象装置に設定されたコンフィグレーションの取得をおこない、事前に必要なコンフィグレーションが設定されているかを確認し、結果を ZIP 形式でダウンロードできます。ファイル名は「nodes_configcheck.zip」となります。ZIP 形式のファイルを展開すると、下記のファイルを出力します。</p> <ul style="list-style-type: none"> <li>• nodes_configcheck_filelist.txt 装置名称と、後述の管理対象装置ごとの事前設定コンフィグレーション例ファイルの対応を示す一覧表ファイル。</li> <li>• nodes_configcheck_&lt;id&gt;_&lt;装置モデル&gt;_&lt;IP アドレス&gt;.txt 管理対象装置ごとの事前設定コンフィグレーション例ファイル。</li> <li>• nodes_configcheck_error.txt コンフィグレーションの取得に失敗した装置の一覧表ファイル(装置名,IP アドレス,装置モデル)。1 台以上、取得に失敗した場合だけ出力します。</li> </ul>
⑦	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑧	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑨	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑩	装置情報	<p>装置情報の一覧を表示します。 表示項目は、装置情報/IP アドレス/状態/装置モデル/端末接続数/遮断端末数/コンフィグ空き容量/コメントです。 状態*： 正常/削除待ち/ライセンス無効/メンテナンス実施/ 状態不明 ※：管理対象装置からの MIB 取得において、 lexicographically order で応答を返さない場合、状態の後に [OID not increasing] を表示します。 コンフィグ空き容量： -/未確認/&lt;空き容量&gt;%/状態不明 装置のエントリを押下すると、「(b) 装置詳細」に移動します。</p>

項目番	内容	説明
⑪	表示ボタン	管理対象装置が所属するマップを定義している場合に表示します。ボタンを押下すると、「6.1.7(1)(b)マップ」に移動し、該当する装置のアイコンに影を付与して明示します（表示例：  ）。
⑫	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

## (a) 装置追加

図 6-11 装置追加画面 (1/2)



The screenshot shows the 'Device Addition' (装置追加) page. At the top, there is a breadcrumb navigation: トップ > 共通 > 装置一覧 > 装置追加. A red box labeled ① surrounds this area. Below it is a title '装置追加'. The main form is divided into two sections: '装置情報' (Device Information) and '収集情報' (Collection Information). The '装置情報' section contains the following fields, each with a red box and a number from ② to ⑦: ② 装置名称 (Device Name: AX36605\_CoreSW), ③ IPアドレス (IP Address: 198.51.100.152), ④ 装置モデル (Device Model: AX3660S), ⑤ 装置MACアドレス (Device MAC Address: empty), ⑥ メンテナンスモード (Maintenance Mode: 有効 (Enabled) is selected), ⑦ コメント (Comment: コアスイッチ). The '収集情報' section contains checkboxes for collection protocols: ⑧ ARP, NDP, MACアドレス (Address), LLDP, and WLC. The 'MACアドレス' checkbox is selected.

図 6-12 装置追加画面 (2/2)

**SNMPアクセス情報**

- ⑨ コミュニティ: public アクセス確認
- ⑩ MIBオブジェクト(ARP/NDP): ⑪
- ⑫ MIBオブジェクト(MACアドレス): ⑬
- ⑬ MIBオブジェクト(LLDP):  LLDP-MIB  LLDP-V2-  
MIB ⑭
- ⑭ MIBオブジェクト(WLC): ⑮
- ⑮ VLANリスト: VLAN取得 ⑯

**SSHログイン情報**

- ⑰ ログインユーザ名: axsc ⑲ ログイン確認
- ⑱ パスワード: ..... ⑳

**装置管理情報**

- ㉑ 装置管理者モードのパスワード: ..... ㉒ 認証確認 ㉓

**特定端末へのWeb通信不可表示**

- ㉔ 有効/無効:  有効  無効
- ㉕ ポート番号: 80

追加 キャンセル ㉖ ㉗

表 6-18 装置追加画面に表示する項目

項目番	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	装置情報	装置名称	装置情報として、装置名称を示す文字列です。最大 256 文字登録可能です。

項目番	内容	説明
③	IP アドレス	装置情報として、管理対象装置の IP アドレスを入力します。 0.0.0.0～255.255.255.255 を入力してください。
④	装置モデル プルダウン	装置情報として、管理対象装置の装置モデルを選択します。以下のいずれかです。 <ul style="list-style-type: none"> <li>• AX2100S</li> <li>• AX2500S</li> <li>• AX2500S(スタック構成)</li> <li>• AX260A</li> <li>• AX3660S</li> <li>• AX8300S</li> <li>• AX8600S</li> <li>• AX2200S</li> <li>• AX3640S</li> <li>• AX3650S</li> <li>• AX3800S</li> <li>• AX4600S</li> <li>• AXprimoM210</li> <li>• AX620R</li> <li>• 標準 MIB 対応装置</li> <li>• 標準 MIB 対応装置(VLAN 每コミュニティ)</li> <li>• ワイヤレス LAN コントローラ</li> </ul>
⑤	装置 MAC アドレス	装置情報として、装置 MAC アドレスを入力します。装置モデルが下記の場合に入力します。 <ul style="list-style-type: none"> <li>• 標準 MIB 対応装置</li> <li>• 標準 MIB 対応装置(VLAN 每コミュニティ)</li> <li>• ワイヤレス LAN コントローラ</li> </ul> 装置 MAC アドレスが不明な場合、管理対象装置を識別する一意となる MAC アドレスを入力してください。
⑥	メンテナンスモード選択ボタン	装置情報として、管理対象装置への情報収集有無を選択するボタンです。一時的に情報収集をおこなわなくする場合、有効を選択してください。
⑦	コメント	装置情報として、管理対象装置の説明を記載する文字列です。0～256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。

項目番	内容	説明
⑧	収集情報	<p>装置情報として、管理対象装置の収集情報種別を選択します。以下を複数選択できます。</p> <ul style="list-style-type: none"> <li>• ARP</li> <li>• NDP</li> <li>• MAC アドレス</li> <li>• LLDP</li> <li>• WLC</li> </ul> <p>装置モデルが下記の場合、ARP を選択できません。</p> <ul style="list-style-type: none"> <li>• ワイヤレス LAN コントローラ</li> </ul> <p>装置モデルが下記の場合、NDP を選択できません。</p> <ul style="list-style-type: none"> <li>• AX2200S</li> <li>• AX2100S</li> <li>• AXprimoM210</li> <li>• ワイヤレス LAN コントローラ</li> </ul> <p>装置モデルが下記の場合、MAC アドレスを選択できません。</p> <ul style="list-style-type: none"> <li>• AX620R</li> <li>• ワイヤレス LAN コントローラ</li> </ul> <p>装置モデルが下記の場合、LLDP を選択できません。</p> <ul style="list-style-type: none"> <li>• AX620R</li> <li>• ワイヤレス LAN コントローラ</li> </ul> <p>装置モデルが下記の場合だけ、WLC を選択できます。</p> <ul style="list-style-type: none"> <li>• ワイヤレス LAN コントローラ</li> </ul>
⑨	SNMP アクセス情報	<p>SNMP アクセス情報として、管理対象装置の SNMP コミュニティ名称を入力します。256 文字登録可能です。</p>
⑩	アクセス確認ボタン	<p>SNMP アクセス情報として、管理対象装置への SNMP アクセスが可能か確認することができます。ボタンを押下すると、アクセス確認をおこない、以下のいずれかを表示します。</p> <p>[SNMP アクセス成功時] SNMP アクセスのチェックに成功しました</p> <p>[SNMP アクセス失敗時] SNMP アクセスのチェックに失敗しました</p>

項目番	内容	説明
⑪	MIB オブジェクト(ARP/NDP)プルダウン	装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 毎コミュニティ)の場合に、管理対象装置の ARP/NDP 情報収集時に取得する MIB オブジェクトを選択します。装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 毎コミュニティ)でない場合は選択できません。 収集情報として以下のどちらかを選択します。 <ul style="list-style-type: none"><li>• ipNetToMediaPhysAddress/ipv6NetToMediaPhysAddress</li><li>• ipNetToPhysicalPhysAddress</li></ul>
⑫	MIB オブジェクト(MAC アドレス)プルダウン	装置モデルが標準 MIB 対応装置の場合に、管理対象装置の MAC アドレス情報収集時に取得する MIB オブジェクトを選択します。装置モデルが標準 MIB 対応装置でない場合は選択できません。 収集情報として以下のどちらかを選択します。 <ul style="list-style-type: none"><li>• dot1dTpFdbPort</li><li>• dot1qTpFdbPort</li></ul>
⑬	MIB オブジェクト(LLDP)チェックボックス	装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 毎コミュニティ)の場合に、管理対象装置の LLDP 情報収集時に取得する MIB オブジェクトを選択します。装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 毎コミュニティ)でない場合は選択できません。以下を複数選択できます。 <ul style="list-style-type: none"><li>• LLDP-MIB</li><li>• LLDP-V2-MIB</li><li>• axslldp</li></ul>
⑭	MIB オブジェクト(WLC)プルダウン	装置モデルがワイヤレス LAN コントローラの場合に、管理対象装置の WLC 情報収集時に取得する MIB オブジェクトを選択します。装置モデルがワイヤレス LAN コントローラでない場合は選択できません。 以下から選択します。 <ul style="list-style-type: none"><li>• Aruba-1-wlsxUserAllInfoGroup/wlsxWlanAccessPointInfoGroup</li><li>• Cisco-1-bsnEss/bsnAP</li><li>• Fortinet-1-mwConfigAp/mwConfigStation</li></ul>
⑮	VLAN リスト	装置モデルが標準 MIB 対応装置(VLAN 毎コミュニティ)の場合に、管理対象装置の MAC アドレス情報収集時に使用する VLAN リスト*を入力します。 「VLAN 取得」ボタンにより管理対象装置から VLAN リストを収集するか、直接入力します。 VLAN リストとして使用可能な文字は、数値、ハイフン (-)、コンマ (,) です。(例: 10, 50-52)

項目番	内容		説明
⑯			<p>VLAN 取得ボタン</p> <p>管理対象装置の VLAN リストを取得します。ボタンを押下すると、VLAN リストの取得を試み、以下のいずれかを表示します。</p> <p>[SNMP アクセス成功時] VLAN の取得に成功しました</p> <p>[SNMP アクセス失敗時] VLAN の取得に失敗しました</p> <p>なお VLAN リストが空文字列でない場合にボタンを押下すると</p> <p>VLAN リストの内容を上書きします</p> <p>の確認ダイアログを表示します。了承した場合、VLAN リストの取得を試みます。</p>
⑰	SSH ログイン情報	ログインユーザ名	<p>SSH ログイン情報として、管理対象装置のログインユーザ名を入力します。256 文字登録可能です。なおコロン(:)文字は使用しないでください。</p> <p>AX620R の場合、ログインユーザ名には administrator 権限のあるユーザを指定してください。</p> <p>装置モデルが下記の場合、入力できません。</p> <ul style="list-style-type: none"> <li>・標準 MIB 対応装置</li> <li>・標準 MIB 対応装置(VLAN 毎コミュニティ)</li> <li>・ワイヤレス LAN コントローラ</li> </ul>
⑱		パスワード	<p>SSH ログイン情報として、管理対象装置のログインパスワードを入力します。256 文字登録可能です。</p> <p>装置モデルが下記の場合、入力できません。</p> <ul style="list-style-type: none"> <li>・標準 MIB 対応装置</li> <li>・標準 MIB 対応装置(VLAN 毎コミュニティ)</li> <li>・ワイヤレス LAN コントローラ</li> </ul>
⑲		パスワード可視化オンオフボタン	<p>SSH ログイン情報として、ログインパスワードの可視化のオンオフをおこないます。入力したログインパスワードの文字列を確認したい場合に押下してください。再度押下すると、文字列を隠します。</p>
⑳		ログイン確認ボタン	<p>SSH ログイン情報として、管理対象装置への SSH ログインが可能か確認することができます。ボタンを押下すると、ログイン確認をおこない、以下のいずれかを表示します。</p> <p>[SSH ログイン成功時] 装置ログインのチェックに成功しました</p> <p>[SSH ログイン失敗時] 装置ログインのチェックに失敗しました</p>

項目番	内容	説明
⑪	装置管理情報	装置管理情報として、管理対象装置の装置管理者モードのパスワードを入力します。0~256 文字登録可能です。 装置モデルが下記の場合、入力できません。 <ul style="list-style-type: none"><li>・AX620R</li><li>・標準 MIB 対応装置</li><li>・標準 MIB 対応装置(VLAN 毎コミュニティ)</li><li>・ワイヤレス LAN コントローラ</li></ul>
⑫	パスワード可視化オンオフボタン	装置管理情報として、装置管理者モードのパスワードの可視化のオンオフをおこないます。入力した装置管理者モードのパスワードの文字列を確認したい場合に押下してください。再度押下すると、文字列を隠します。
⑬	認証確認ボタン	装置管理情報として、管理対象装置への装置管理者モードへのコマンド入力モードの変更が可能か確認することができます。ボタンを押下すると、認証確認をおこない、以下のいずれかを表示します。  [装置管理者モードへのコマンド入力モード変更成功時] 装置管理者モードのチェックに成功しました [装置管理者モードへのコマンド入力モード変更失敗時] 装置管理者モードのチェックに失敗しました
⑭	特定端末への Web 通信不可表示	特定端末への Web 通信不可表示として、特定端末への Web 通信不可表示機能の有効、または無効を選択します。 特定端末への Web 通信不可表示機能を有効にする場合、有効を選択してください。 装置モデルが下記の場合、選択できません。 <ul style="list-style-type: none"><li>・AXprimoM210</li><li>・AX620R</li><li>・標準 MIB 対応装置</li><li>・標準 MIB 対応装置(VLAN 毎コミュニティ)</li><li>・ワイヤレス LAN コントローラ</li></ul>
⑮	ポート番号	特定端末への Web 通信不可表示として、TCP ポート番号を入力します。0~65535 の値を入力してください。起動パラメータ「--accesslist-mode v4-v6」を設定している場合、IPv4 アドレスと IPv6 アドレスで同一のポート番号に対するフィルタを設定します。 装置モデルが下記の場合、入力できません。 <ul style="list-style-type: none"><li>・AXprimoM210</li><li>・AX620R</li><li>・標準 MIB 対応装置</li><li>・標準 MIB 対応装置(VLAN 毎コミュニティ)</li><li>・ワイヤレス LAN コントローラ</li></ul>

項目番号	内容		説明
②⑥	追加ボタン		装置追加を反映します。ボタンを押下し、反映が成功すると、「(1) 装置一覧」に移動します。反映が失敗すると、「表 6-19 装置追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
	キャンセルボタン		装置追加をキャンセルします。ボタンを押下すると、「(1) 装置一覧」に移動します。

注※：VLAN リストは、フレームの送受信をおこなっている運用中の VLAN ID だけとしてください。運用中でない VLAN ID を登録すると、管理対象装置から定期的に収集する情報に時間がかかる場合があります。

表 6-19 装置追加の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	装置名称が入力されていません	装置名称が空白です。1 文字以上の文字列を入力してください。
2	装置モデルが入力されていません	装置モデルを選択していません。装置モデルを選択してください。
3	IP アドレスが入力されていません	IP アドレスが入力されていません。IP アドレスを入力してください。
4	MIB オブジェクト(ARP/NDP)が入力されていません	MIB オブジェクト(ARP/NDP)を選択していません。装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 每コミュニティ)の場合、MIB オブジェクトを選択してください。
5	MIB オブジェクト(MAC アドレス)が入力されていません	MIB オブジェクト(MAC アドレス)を選択していません。装置モデルが標準 MIB 対応装置の場合、MIB オブジェクトを選択してください。
6	MIB オブジェクト(WLC)が入力されていません	MIB オブジェクト(WLC)を選択していません。装置モデルがワイヤレス LAN コントローラの場合、MIB オブジェクトを選択してください。
7	IP アドレスのフォーマットが間違っています	IP アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
8	MAC アドレスのフォーマットが間違っています	MAC アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
9	重複した装置名称です	装置名称は既に登録済みです。別の装置名称を使用して登録してください。
10	範囲外のポート番号です	特定端末への Web 通信不可表示の TCP ポート番号が範囲外です。0~65535 の範囲で入力してください。
11	既に登録済みの装置名称です	装置名称は既に登録済みです。別の装置名称を使用して登録してください。
12	要求のパラメータに間違いがあります	要求のパラメータに間違があります。「6.1.8(6) メンテナンス」により保守情報を収集してください。

項目番号	内容	説明
13	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (b) 装置詳細

図 6-13 装置詳細画面 (1/3)

The screenshot shows the 'Device Detail' page of the AX-Security-Controller(Manager) web interface. The top navigation bar is highlighted with red boxes and numbered ① through ⑤. The main content area is divided into two sections: 'Device Information' and 'Connected Device List'.

**Device Information Section:**

- ① Navigation Bar:** Top navigation path: トップ > 共通 > 装置一覧 > エッジスイッチ1 (IP:198.51.100.141).
- ② Title:** The title 'エッジスイッチ1 (IP:198.51.100.141)' is highlighted with a red box.
- ③ Action Buttons:** Top right buttons: 事前コンフィグ設定確認 (Pre-configuration setting confirmation), 設定変更 (Change settings), and 装置削除 (Delete device).
- ④ Sub-Buttons:** Three small blue buttons below the main action buttons: ④ (blue), ⑤ (blue), and ⑥ (blue).
- ⑥ Device Information Table:** A large red box highlights the table containing device details. It includes fields like System Information, Host Name, MAC Address, LLDP Information, Comments, Status, Collection Date, and Configuration Space.

**Connected Device List Section:**

- ⑦ Filter Buttons:** Buttons for '表示カラム切替' (Change display column) and '件表示' (Number of items displayed) set to 25.
- ⑧ Sort Options:** Buttons for '接続先装置名称' (Connected device name) and '接続先シャーシID' (Connected chassis ID).
- ⑨ Search:** A search input field labeled '検索:'.
- ⑩ Data Table:** A table showing a single connected device entry: 'コアスイッチ' (Core Switch) with IP '0012.e258.9e0c[ALAXALA Networks Corporation]'.
- ⑪ Pagination:** Page navigation buttons: '前のページ' (Previous page), '1' (Page 1), and '次のページ' (Next page).

## 6 AX-Security-Controller(Manager)の Web インタフェース

図 6-14 装置詳細画面 (2/3)

接続端末一覧

IPアドレス	MACアドレス	ペンタ	用途	端末名	ポート番号	ポートエイリ	VLAN ID	操作
198.51.100.54	0000.5e00.5354	ICANN, IANA Department	OA	OA端末54	0/9	1Fフロア-1	100	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.55	0000.5e00.5355	ICANN, IANA Department	OA	OA端末55	0/9	1Fフロア-1	100	<span style="background-color: green; color: white;">通信遮断解除</span> <span style="background-color: orange; color: white;">セキュリティフィルタ解除</span>
198.51.100.56	0000.5e00.5356	ICANN, IANA Department	OA	OA端末56	0/9	1Fフロア-1	100	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.57	0000.5e00.5357	ICANN, IANA Department	OA	OA端末57	0/9	1Fフロア-1	100	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.58	0000.5e00.5358	ICANN, IANA Department	OA	OA端末58	0/9	1Fフロア-1	100	<span style="background-color: red; color: white;">通信遮断</span>
	0000.5e00.5359	ICANN, IANA Department	None	None	0/9	1Fフロア-1	100	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.60	0000.5e00.5360	ICANN, IANA Department	ファイバ	サーバ: F0	0/10	None	100	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.61	0000.5e00.5361	ICANN, IANA Department	None	サーバ: F1	0/10	None	100	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.62	0000.5e00.5362	ICANN, IANA Department	None	サーバ: F2	0/10	None	100	<span style="background-color: red; color: white;">通信遮断</span>
198.51.100.63	0000.5e00.5363	ICANN, IANA Department	None	サーバ: F3	0/10	None	100	<span style="background-color: red; color: white;">通信遮断</span>

20 件中 1 から 10 まで表示

前のページ 1 2 次のページ

(16)

図 6-15 装置詳細画面 (3/3)

ARP/NDPテーブル一覧 表示 ⑯  
 ⑯ 表示カラム切替 ⑰ 10 件表示 ⑯ 検索:  
 IPアドレス ^ MACアドレス  
 198.51.100.54 0000.5e00.5354  
 198.51.100.55 0000.5e00.5355  
 198.51.100.56 0000.5e00.5356  
 198.51.100.57 0000.5e00.5357 ⑯  
 198.51.100.58 0000.5e00.5358  
 198.51.100.60 0000.5e00.5360  
 198.51.100.61 0000.5e00.5361  
 198.51.100.62 0000.5e00.5362  
 198.51.100.63 0000.5e00.5363  
 198.51.100.64 0000.5e00.5364  
 12 件中 1 から 10 まで表示  
 前のページ 1 2 次のページ ⑯

MACアドレステーブル一覧 表示 ⑯  
 ⑯ 表示カラム切替 ⑰ 10 件表示 ⑯ 検索:  
 MACアドレス ^ ポート VLAN ID  
 0000.5e00.5354 0/9 100  
 0000.5e00.5355 0/9 100  
 0000.5e00.5356 0/9 100  
 0000.5e00.5357 0/9 100 ⑯  
 0000.5e00.5358 0/9 100  
 0000.5e00.5359 0/9 100  
 0000.5e00.5360 0/10 100  
 0000.5e00.5361 0/10 100  
 0000.5e00.5362 0/10 100  
 0000.5e00.5363 0/10 100  
 20 件中 1 から 10 まで表示  
 前のページ 1 2 次のページ ⑯

WLC情報テーブル一覧 表示 ⑯  
 ⑯ 表示カラム切替 ⑰ 25 件表示 ⑯ 検索:  
 AP-MACアドレス ^ 接続先AP 端末MACアドレス 端末IPアドレス 端末VLAN ID  
 データがありません  
 0 件中 0 から 0 まで表示  
 前のページ 次のページ ⑯

図 6-16 装置詳細画面(コンフィグ空き容量確認)

The screenshot shows a 'Device Information' section with the following details:

- System Information:** ALAXALA AX3640S AX-3640-245W-A [AX3640S-245W] Switching software Ver. 11.14.L [OS-L3A]
- Host Name:** AX3640S-1
- Device MAC Address:** 0012.e258.9e0c [ALAXALA Networks Corporation]
- Ports:**
  - LLDP Shaper: LLDP-MIB
  - SSID: LLDP-V2-MIB
  - axslldp: -
- Comment:**
- Device Status:** 正常 (Normal)
- Information Collection Date/Time:** 2019/07/19 10:49:45 JST
- Configuration Space Utilization:** 97.67% (2019/07/19 10:49:03 JST). A red 'Capacity Confirmation' button is visible next to it.

表 6-20 装置詳細画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	装置名称	管理対象装置の装置名称と IP アドレスを表示します。
③	事前コンフィグ設定確認ボタン	管理対象装置に設定されたコンフィグレーションを取得し、事前に必要なコンフィグレーションが設定されているかを確認します。ボタンを押下すると、「(d) 事前コンフィグ設定確認結果」に移動します。
④	設定変更ボタン	管理対象装置の設定を変更します。ボタンを押下すると、「(e) 装置編集」に移動します。
⑤	装置削除ボタン	管理対象装置を削除します。ボタンを押下すると、 装置 <装置名称> を削除します  の確認ダイアログを表示します。 了承した場合、管理対象装置を削除し、「(1) 装置一覧」に移動します。削除が失敗すると、「表 6-21 装置詳細の反映失敗時のダイアログ一覧」に示すダイアログを表示します。

項目番号	内容	説明
⑥	装置情報	<p>装置情報(システム情報/ホスト名/装置 MAC アドレス/LLDP シャーシ ID/コメント/装置状態/情報収集日時/コンフィグ空き容量)を表示します。システム情報/ホスト名/装置 MAC アドレスは、管理対象装置から情報を収集するまで、表示しません。</p> <p>MAC アドレスベンダが表示可能な場合、[]に装置 MAC アドレスベンダを表示します。</p> <p>LLDP シャーシ ID は、装置モデルが下記の場合に、管理対象装置から情報収集後、LLDP-MIB、LLDP-V2-MIB、および axslldp に関するシャーシ ID とシャーシ種別を表示します。</p> <ul style="list-style-type: none"> <li>・標準 MIB 対応装置</li> <li>・標準 MIB 対応装置(VLAN 每コミュニティ)</li> </ul> <p>コンフィグ空き容量は、装置モデルが下記の場合に、最後に確認したコンフィグ空き容量を表示します。</p> <ul style="list-style-type: none"> <li>・AX8600S</li> <li>・AX8300S</li> <li>・AX4600S</li> <li>・AX3800S</li> <li>・AX3660S</li> <li>・AX3650S</li> <li>・AX3640S</li> </ul> <p>容量確認ボタンにより、最新のコンフィグ空き容量を確認することができます。容量確認ボタンを押下すると、コンフィグ空き容量の取得をおこない、以下のいずれかを表示します。</p> <p>[コンフィグ空き容量確認成功時] コンフィグ容量確認に成功しました</p> <p>[コンフィグ空き容量確認失敗時] コンフィグ容量確認に失敗しました</p>
⑦	隣接装置一覧	表示カラム切替ボタン
⑧		ページあたり表示件数切替 プルダウン
⑨		検索テキストボックス
⑩		隣接装置情報
⑪		ページ切替ボタン
⑫	接続端末一覧	表示カラム切替ボタン

項目番号	内容	説明
⑯	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑰	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑱	接続端末情報	接続端末情報の一覧を表示します。 接続端末情報表示項目は、「表 6-3 端末一覧に表示する項目」の端末一覧を参照してください。
⑲	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。
⑳	ARP/NDP テーブル一覧	表示ボタン ボタンを押下すると、ARP/NDP テーブルのエントリー一覧を展開表示します。 もう一度ボタンを押下すると、ARP/NDP テーブルのエントリー一覧表示を折りたたみます。
㉑		表示カラム切替ボタン 一覧から不要なカラムを非表示にすることができます。
㉒		ページあたり表示件数切替プルダウン 1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
㉓		検索テキストボックス テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
㉔	ARP/NDP エントリー一覧	ARP/NDP エントリの一覧を表示します。 表示項目は、IP アドレス/MAC アドレスです。
㉕		ページ切替ボタン ボタンを押下すると、指定のページを表示します。
㉖		表示ボタン ボタンを押下すると、MAC アドレステーブルのエントリー一覧を展開表示します。 もう一度ボタンを押下すると、MAC アドレステーブルのエントリー一覧表示を折りたたみます。
㉗		表示カラム切替ボタン 一覧から不要なカラムを非表示にすることができます。
㉘	MAC アドレステーブル一覧	ページあたり表示件数切替プルダウン 1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
㉙		検索テキストボックス テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
㉚		MAC アドレスエントリー一覧 MAC アドレスエントリの一覧を表示します。 表示項目は、MAC アドレス/ポート/VLAN ID *1 です。
㉛		ページ切替ボタン ボタンを押下すると、指定のページを表示します。
㉕	WLC 情報テーブル一覧	表示ボタン ボタンを押下すると、WLC 情報テーブルのエントリー一覧を展開表示します。 もう一度ボタンを押下すると、WLC 情報テーブルのエントリー一覧表示を折りたたみます。
㉖		表示カラム切替ボタン 一覧から不要なカラムを非表示にすることができます。

項目番号	内容	説明
⑩	ページあたり表示件数切替 プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑪		検索テキストボックス
⑫		WLC 情報エンタリ一覧
⑬		ページ切替ボタン

注※1

下記管理対象装置で学習した端末の VLAN は、VLAN ID を表示しません。

- 標準 MIB 対応装置

MIB オブジェクト(MAC アドレス)が「dot1dTpFdbPort」の場合、「空白("")」になります。

MIB オブジェクト(MAC アドレス)が「dot1qTpFdbPort」の場合、「dot1qTpFdbPort で収集した dot1qFdbId の値」になります。

表 6-21 装置詳細の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みの装置です	既に削除済みの装置です。
2	指定した装置は存在しません	指定した装置は存在しません。
3	要求のパラメータに間違があります	要求のパラメータに間違があります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
4	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (c) CSV 形式からの装置追加

図 6-17 CSV 形式からの装置追加画面



表 6-22 CSV 形式からの装置追加に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ファイルを選択ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上の装置を追加、または置き換えることができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
③	更新反映/置き換えラジオボタン	選択したファイルについて、更新反映をおこなうか、置き換えをおこなうかを選択します。 更新反映を選択した場合、AX-Security-Controller で管理している装置情報の上書きをおこない、かつ CSV ファイルだけに存在する装置を追加します。 置き換えを選択した場合、AX-Security-Controller で管理している装置一覧を、CSV ファイルの内容に置き換えます。CSV ファイル内に AX-Security-Controller で管理している装置情報がない場合、当該装置は削除されます。
④	内容確認ボタン	更新反映ラジオボタン、または置き換えラジオボタンに従い、AX-Security-Controller で管理している装置一覧と、CSV ファイルの内容を比較・確認します。ボタンを押下すると、「図 6-18 CSV 形式からの装置追加画面(適用内容含む)」を表示します。表示する項目は、「表 6-23 CSV 形式からの装置追加(適用内容含む)に表示する項目」を参照ください。

図 6-18 CSV 形式からの装置追加画面(適用内容含む)

① リンク: トップ > 共通 > 装置一覧 > CSV形式からの装置追加

② ファイルを選択: nodes.csv

③ ラジオボタン: 更新反映 (選択済み) / 置き換え

④ 内容確認 ボタン

⑤ 表示カラム切替 ボタン

⑥ 件表示 ダropdown: 25

⑦ 検索 フィールド

⑧ テーブルセル: コアスイッチ (変更あり)

⑨ ボタン: 差分表示

⑩ ボタン: 差分表示

⑪ ボタン: 前のページ

⑫ ボタン: 次のページ

⑬ 項目名: 装置名称

⑭ 項目名: 変更内容

⑯ ボタン: 適用

⑰ ボタン: キャンセル

表 6-23 CSV 形式からの装置追加(適用内容含む)に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ファイル選択 更新反映/置き換えラジオボタン 内容確認ボタン	「表 6-22 CSV 形式からの装置追加に表示する項目」を参照ください。
③		「表 6-22 CSV 形式からの装置追加に表示する項目」を参照ください。
④		「表 6-22 CSV 形式からの装置追加に表示する項目」を参照ください。
⑤	適用内容 表示カラム切替ボタン	一覧から不要なカラムを非表示することができます。
⑥	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。

項目番号	内容	説明
⑦	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑧	適用内容情報一覧	適用内容情報一覧を表示します。 表示項目は、装置名称/適用内容です。 適用内容は以下のいずれかです。 <ul style="list-style-type: none"><li>・追加</li><li>・変更あり</li><li>・変更なし</li><li>・削除</li></ul>
⑨	操作	操作は、差分表示ボタンが表示されます。 差分表示ボタンを押下すると、更新反映ラジオボタン、または置き換えラジオボタンに従って、CSV ファイル反映による適用前と適用後の変更箇所一覧をダイアログで表示します。 変更箇所一覧のダイアログの例を「図 6-19 変更箇所一覧画面」に示します。
⑩	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。
⑪	適用ボタン	更新反映ラジオボタン、または置き換えラジオボタンに従い、装置追加を反映します。ボタンを押下し、反映をおこなうと、「(1) 装置一覧」に移動します。
⑫	キャンセルボタン	装置追加をキャンセルします。ボタンを押下すると、「(1) 装置一覧」に移動します。

図 6-19 変更箇所一覧画面

変更箇所一覧		
項目	適用前	適用後
装置名称	コアスイッチ	コアスイッチ
IPアドレス	198.51.100.1	198.51.100.1
装置モデル	AX3660S	AX3660S
装置MACアドレス		
メンテナンスマード	有効	無効
コメント		
SNMPコミュニティ	public	public
ログインユーザ名	axsc	axsc
パスワード	*****	*****
装置管理者モードのパスワード	*****	*****
特定端末へのWeb通信不可表示		
ポート番号	80	80
収集情報(ARP)	有効	有効
収集情報(NDP)	有効	有効
収集情報(MACアドレス)	有効	有効
収集情報(LLDP)	有効	有効
収集情報(WLC)		
MIBオブジェクト(ARP/NDP)		
MIBオブジェクト(MACアドレス)		
IBオブジェクト(LLDP)		
MIBオブジェクト(WLC)		
VLANリスト		

## (d) 事前コンフィグ設定確認結果

図 6-20 事前コンフィグ設定確認結果画面

① 階層リンク  
② 事前コンフィグ設定確認結果出力  
③ 表示カラム切替  
④ ページあたり表示件数切替プルダウン  
⑤ 検索:  
⑥ 装置  
⑦ 端末接続ポート/装置接続ポート  
⑧ 設定済み  
⑨ 未設定(LLDP/アクセスリスト)  
⑩ ポート種別  
状態  
⑪ コンフィグ  
⑫ 11 件中 1 から 11 まで表示  
⑬ 前のページ  
⑭ 次のページ

表 6-24 事前コンフィグ設定確認結果に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	事前コンフィグ設定確認結果出力ボタン	ボタンを押下すると、事前に設定するコンフィグレーション例をテキスト形式でダウンロードできます。ファイル名は「nodes_configcheck_<id>_<装置モデル>_<IP アドレス>.txt」になります。
③	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
④	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。

項目番号	内容	説明
⑤	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑥	設定対象	装置、またはポート番号を表示します。
⑦	ポート種別	<p>下記のいずれかを表示します。</p> <ul style="list-style-type: none"> <li>・装置接続ポート</li> <li>・端末接続ポート</li> <li>・WAN 接続ポート</li> <li>・永続設定ポート(受信側)</li> <li>・永続設定ポート(送信側)</li> <li>・ミラー先ポート</li> </ul> <p>AX-Security-Controller に、当該ポートをミラー先ポートで設定している場合、WAN 接続ポートとして設定していたとしても、ミラー先ポートとして判断します。</p> <p>設定対象が装置の場合、空白となります。</p>
⑧	状態	<p>設定状態を表示します。</p> <ul style="list-style-type: none"> <li>・設定済み</li> <li>・未設定(&lt;未設定コンフィグ&gt;)</li> </ul> <p>未設定コンフィグには、下記を 1 つ以上表示します。</p> <ul style="list-style-type: none"> <li>・LLDP</li> <li>・アクセスリスト</li> <li>・特定端末への Web 通信不可表示</li> </ul>
⑨	コンフィグ	<p>設定済みのコンフィグレーションを表示します。</p> <p>未設定のコンフィグレーションがある場合、赤色で表示します。</p> <p>不要なコンフィグレーションがある場合、灰色で表示します。</p> <p>表示内容により、ネットワーク構成にあわせて管理対象装置へのコンフィグレーション設定を検討ください。</p>
⑩	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

## (e) 装置編集

図 6-21 装置編集画面 (1/2)

図 6-21 装置編集画面 (1/2) のスクリーンショットです。この画面は、AX-Security-Controller(Manager)のWebインターフェースで、装置の編集を行なうためのものです。

ヘッダーには、ナビゲーションメニューが表示されています：「トップ」>「共通」>「装置一覧」>「AX3660S\_CoreSW (IP:198.51.100.152)」>「装置編集」。右側に赤い数字で1から6が付いた注釈があります。

「装置情報」セクションには、以下のフィールドがあります：

- 「装置名称」: AX3660S\_CoreSW (①)
- 「IPアドレス」: 198.51.100.152 (②)
- 「装置モデル」: AX3660S (③)
- 「装置MACアドレス」: (④)
- 「メンテナンスマード」: 有効 (⑤)
- 「コメント」: コアスイッチ (⑥)

「収集情報」セクションには、以下のチェックボックスがあります：

- ARP (⑦)
- NDP (⑧)
- MACアドレス (⑨)
- LLDP (⑩)
- WLC (⑪)

図 6-22 装置編集画面 (2/2)

The screenshot shows the second page of a device configuration interface. It consists of four main sections:

- SNMPアクセス情報** (SNMP Access Information):
  - ⑦ コミュニティ: public
  - ⑧ アクセス確認 (Access Confirmation) button
  - ⑨ MIBオブジェクト(ARP/NDP)
  - ⑩ MIBオブジェクト(MACアドレス)
  - ⑪ MIBオブジェクト(LLDP):
    - LLDP-MIB
    - LLDP-V2-
    - axlldp
    - MIB
  - ⑫ MIBオブジェクト(WLC)
  - ⑬ VLANリスト
  - ⑭ VLAN取得 (VLAN Acquisition) button
- SSHログイン情報** (SSH Login Information):
  - ⑮ ログインユーザ名: axsc
  - ⑯ パスワード: ..... (password field)
  - ⑰ ログイン確認 (Login Confirmation) button
  - ⑱ (empty box)
- 装置管理情報** (Device Management Information):
  - ⑲ 装置管理者モードのパスワード: ..... (password field)
  - ⑳ 認証確認 (Authentication Confirmation) button
  - ㉑ (empty box)
- 特定端末へのWeb通信不可表示** (Hide Web Communication from Specific Endpoints):
  - 有効/無効: 有効 (radio button selected)
  - 無効 (radio button)
  - ポート番号: 80
  - ㉒ (empty box)

At the bottom right are two buttons: **更新** (Update) and **キャンセル** (Cancel), numbered ㉓ and ㉔ respectively.

表 6-25 装置編集画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。

項目番	内容		説明
②	装置情報	装置名称/IPアドレス/装置モデル	装置情報として、登録済みの装置名称/IPアドレス/装置モデルを表示します。
③		装置 MAC アドレス	装置情報として、装置 MAC アドレスを入力します。装置モデルが下記の場合に入力します。 <ul style="list-style-type: none"><li>・標準 MIB 対応装置</li><li>・標準 MIB 対応装置(VLAN 毎コミュニティ)</li><li>・ワイヤレス LAN コントローラ</li></ul>
④		メンテナンスモード選択ボタン	装置情報として、管理対象装置への情報収集有無を選択するボタンです。一時的に情報集をおこなわなくする場合、有効を選択してください。
⑤		コメント	装置情報として、管理対象装置の説明を記載する文字列です。0~256 文字登録可能です。なおアポストロフィー('')文字は使用しないでください。
⑥	収集情報		<p>装置情報として、管理対象装置の収集情報種別を選択します。以下を複数選択できます。</p> <ul style="list-style-type: none"><li>・ ARP</li><li>・ NDP</li><li>・ MAC アドレス</li><li>・ LLDP</li><li>・ WLC</li></ul> <p>装置モデルが下記の場合、ARP を選択できません。</p> <ul style="list-style-type: none"><li>・ ワイヤレス LAN コントローラ</li></ul> <p>装置モデルが下記の場合、NDP を選択できません。</p> <ul style="list-style-type: none"><li>・ AX2200S</li><li>・ AX2100S</li><li>・ AXprimoM210</li><li>・ ワイヤレス LAN コントローラ</li></ul> <p>装置モデルが下記の場合、MAC アドレスを選択できません。</p> <ul style="list-style-type: none"><li>・ AX620R</li><li>・ ワイヤレス LAN コントローラ</li></ul> <p>装置モデルが下記の場合、LLDP を選択できません。</p> <ul style="list-style-type: none"><li>・ AX620R</li><li>・ ワイヤレス LAN コントローラ</li></ul> <p>装置モデルが下記の場合だけ、WLC を選択できます。</p> <ul style="list-style-type: none"><li>・ ワイヤレス LAN コントローラ</li></ul>
⑦	SNMP アクセス情報	コミュニティ	SNMP アクセス情報として、管理対象装置の SNMP コミュニティ名称を入力します。256 文字登録可能です。

項目番	内容	説明
⑧	アクセス確認ボタン	SNMP アクセス情報として、管理対象装置への SNMP アクセスが可能か確認することができます。ボタンを押下すると、アクセス確認をおこない、以下のいずれかを表示します。  [SNMP アクセス成功時] SNMP アクセスのチェックに成功しました [SNMP アクセス失敗時] SNMP アクセスのチェックに失敗しました
⑨	MIB オブジェクト(ARP/NDP)プルダウン	装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 每コミュニティ)の場合に、管理対象装置の ARP/NDP 情報収集時に取得する MIB オブジェクトを選択します。装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 每コミュニティ)でない場合は選択できません。 収集情報として以下のどちらかを選択します。 • ipNetToMediaPhysAddress/ ipv6NetToMediaPhysAddress • ipNetToPhysicalPhysAddress
⑩	MIB オブジェクト(MAC アドレス)プルダウン	装置モデルが標準 MIB 対応装置の場合に、管理対象装置の MAC アドレス情報収集時に取得する MIB オブジェクトを選択します。装置モデルが標準 MIB 対応装置でない場合は選択できません。 収集情報として以下のどちらかを選択します。 • dot1dTpFdbPort • dot1qTpFdbPort
⑪	MIB オブジェクト(LLDP)チェックボックス	装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 每コミュニティ)の場合に、管理対象装置の LLDP 情報収集時に取得する MIB オブジェクトを選択します。装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 每コミュニティ)でない場合は選択できません。以下を複数選択できます。 • LLDP-MIB • LLDP-V2-MIB • axslldp
⑫	MIB オブジェクト(WLC)プルダウン	装置モデルがワイヤレス LAN コントローラの場合に、管理対象装置の WLC 情報収集時に取得する MIB オブジェクトを選択します。装置モデルがワイヤレス LAN コントローラでない場合は選択できません。 以下から選択します。 • Aruba-1-wlsxUserAllInfoGroup/wlsxWlanAccessPointInfoGroup • Cisco-1-bsnEss/bsnAP • Fortinet-1-mwConfigAp/mwConfigStation

項目番	内容	説明
⑬	VLAN リスト	装置モデルが標準 MIB 対応装置(VLAN 每コミュニティ)の場合に、管理対象装置の MAC アドレス情報収集時に使用する VLAN リスト※を入力します。 「VLAN 取得」ボタンにより管理対象装置から VLAN リストを収集するか、直接入力します。VLAN リストとして使用可能な文字は、数値、ハイフン (-)、コンマ (,) です。(例: 10, 50-52)
⑭	VLAN 取得ボタン	管理対象装置の VLAN リストを取得します。ボタンを押下すると、VLAN リストの取得を試み、以下のいずれかを表示します。 [SNMP アクセス成功時] VLAN の取得に成功しました [SNMP アクセス失敗時] VLAN の取得に失敗しました  なお VLAN リストが空文字列でない場合にボタンを押下すると  VLAN リストの内容を上書きします  の確認ダイアログを表示します。了承した場合、VLAN リストの取得を試みます。
⑮	SSH ログインユーザ名情報	SSH ログイン情報として、管理対象装置のログインユーザ名を入力します。256 文字登録可能です。なおコロン(:)文字は使用しないでください。 AX620R の場合、ログインユーザ名には administrator 権限のあるユーザを指定してください。 装置モデルが下記の場合、入力できません。 <ul style="list-style-type: none"><li>・標準 MIB 対応装置</li><li>・標準 MIB 対応装置(VLAN 每コミュニティ)</li><li>・ワイヤレス LAN コントローラ</li></ul>
⑯	パスワード	SSH ログイン情報として、管理対象装置のログインパスワードを入力します。256 文字登録可能です。 装置モデルが下記の場合、入力できません。 <ul style="list-style-type: none"><li>・標準 MIB 対応装置</li><li>・標準 MIB 対応装置(VLAN 每コミュニティ)</li><li>・ワイヤレス LAN コントローラ</li></ul>
⑰	パスワード可視化オンオフボタン	SSH ログイン情報として、ログインパスワードの可視化のオンオフをおこないます。入力したログインパスワードの文字列を確認したい場合に押下してください。再度押下すると、文字列を隠します。

項目番	内容		説明
⑯		ログイン確認ボタン	SSH ログイン情報として、管理対象装置への SSH ログインが可能か確認することができます。ボタンを押下すると、ログイン確認をおこない、以下のいずれかを表示します。  [SSH ログイン成功時] 装置ログインのチェックに成功しました [SSH ログイン失敗時] 装置ログインのチェックに失敗しました
⑰	装置管理情報	装置管理者モードのパスワード	装置管理情報として、管理対象装置の装置管理者モードのパスワードを入力します。0~256 文字登録可能です。 装置モデルが下記の場合、入力できません。 <ul style="list-style-type: none"> <li>・AX620R</li> <li>・標準 MIB 対応装置</li> <li>・標準 MIB 対応装置(VLAN 毎コミュニティ)</li> <li>・ワイヤレス LAN コントローラ</li> </ul>
⑱		パスワード可視化オンオフボタン	装置管理情報として、装置管理者モードのパスワードの可視化のオンオフをおこないます。入力した装置管理者モードのパスワードの文字列を確認したい場合に押下してください。再度押下すると、文字列を隠します。
⑲		認証確認ボタン	装置管理情報として、管理対象装置への装置管理者モードへのコマンド入力モードの変更が可能か確認することができます。ボタンを押下すると、認証確認をおこない、以下のいずれかを表示します。  [装置管理者モードへのコマンド入力モード変更成功時] 装置管理者モードのチェックに成功しました [装置管理者モードへのコマンド入力モード変更失敗時] 装置管理者モードのチェックに失敗しました
⑳	特定端末への Web 通信不可表示	有効/無効/ポート番号	特定端末への Web 通信不可表示として、有効/無効、および TCP ポート番号を表示します。
㉑	—	更新ボタン	装置編集を反映します。ボタンを押下し、反映が成功すると、「(1) 装置一覧」に移動します。反映が失敗すると、「表 6-26 装置編集の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
㉒	キャンセルボタン		装置編集をキャンセルします。ボタンを押下すると、「(1) 装置一覧」に移動します。

注※：VLAN リストは、フレームの送受信をおこなっている運用中の VLAN ID だけとしてください。運用中でない VLAN ID を登録すると、管理対象装置から定期的に

収集する情報に時間がかかる場合があります。

表 6-26 装置編集の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	MIB オブジェクト(ARP/NDP)が入力されていません	MIB オブジェクト(ARP/NDP)を選択していません。装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 每コミュニティ)の場合、MIB オブジェクトを選択してください。
2	MIB オブジェクト(MAC アドレス)が入力されていません	MIB オブジェクトを選択していません。装置モデルが標準 MIB 対応装置の場合、MIB オブジェクトを選択してください。
3	MIB オブジェクト(WLC)が入力されていません	MIB オブジェクト(WLC)を選択していません。装置モデルがワイヤレス LAN コントローラの場合、MIB オブジェクトを選択してください。
4	要求のパラメータに間違いがあるか、指定した装置が存在しません	要求のパラメータに間違いがあるか、指定した装置が存在しません。「6.1.8(6) メンテナンス」により保守情報を収集してください。
5	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

### (f) 装置検索

図 6-23 装置検索画面

表 6-27 装置検索画面に表示する項目

項目番	内容	説明	
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。	
②	検索装置情報	IP アドレス	<p>検索する際の IP アドレスとして、下記のパターンが入力可能です。</p> <ul style="list-style-type: none"> <li>・ &lt;IPv4 プレフィックス&gt;/&lt;IPv4 プレフィックス長&gt;</li> <li>・ &lt;IPv4 アドレス&gt;[, &lt;IPv4 アドレス&gt;, ...]</li> </ul> <p>IPv4 プレフィックスは、0.0.0.0～255.255.255.255 を入力してください。      IPv4 プレフィックス長は、24～32 を入力してください。      IPv4 アドレスは、0.0.0.0～255.255.255.255 を入力してください。IPv4 アドレスを複数入力する場合、コンマ(,)で区切って入力し、最大 256 個入力可能です。</p>
③		SNMP のコミュニティ	検索する際の SNMP アクセス情報として、管理対象装置の SNMP コミュニティ名称を入力します。256 文字入力可能です。
④	—	検索ボタン	入力した IP アドレスと SNMP コミュニティにより、管理対象装置の候補を検索します。 ボタンを押下すると「(g) 装置検索一覧」に移動します。
⑤		キャンセルボタン	装置検索をキャンセルします。ボタンを押下すると、「(1) 装置一覧」に移動します。

## (g) 装置検索一覧

図 6-24 装置検索一覧画面 (1/5)

The screenshot shows the 'Device Search List' page. At the top, there is a breadcrumb navigation: トップ > 共通 > 装置一覧 > 装置検索 > 装置検索一覧. A red box labeled ① encloses this area. Below it, a button labeled '装置検索画面表示' is highlighted with a red box and labeled ②. Further down, two buttons are shown: '装置追加' (highlighted with a red box and labeled ③) and 'ユーザ名/パスワード認証確認' (labeled ④). To the right of these buttons is a search input field labeled '検索:' with a red box around it and labeled ⑤. On the left side of the table, there is a vertical column of checkboxes labeled ⑥. The table has columns: 状態 (Status), 装置名称 (Device Name), IPアドレス (IP Address), 装置モデル (Device Model), システム名称 (System Name), and 装置MACアドレス (Device MAC Address). The first row contains the following data: 状態 (unchecked), 装置名称 (AX3640S-1), IPアドレス (198.51.100.137), 装置モデル (AX3640S), システム名称 (ALAXALA AX3640S AX-3640-24SW-A [AX3640S-24SW] Switching software Ver. 11.14.L [OS-L3A]), and 装置MACアドレス (empty). The second row contains similar data for another device. Red boxes labeled ⑦, ⑧, and ⑨ highlight the status checkboxes, device name input field, and IP address input field respectively. A red box labeled ⑩ highlights the system name column for the second device.

状態	装置名称	IPアドレス	装置モデル	システム名称	装置MACアドレス
<input type="checkbox"/>	AX3640S-1	198.51.100.137	AX3640S	ALAXALA AX3640S AX-3640- 24SW-A [AX3640S- 24SW] Switching software Ver. 11.14.L [OS-L3A]	
<input type="checkbox"/>	AX3640S-1_0001	198.51.100.255	AX3640S	ALAXALA AX3640S AX-3640- 24SW-A [AX3640S- 24SW] Switching software Ver. 11.14.L [OS-L3A]	

2 件表示

図 6-25 装置検索一覧画面 (2/5)

トップ > 共通 > 装置一覧 > 装置検索 > 装置検索一覧

装置検索画面表示

装置検索一覧

装置追加 ユーザ名/パスワード認証確認

検索: [ ]

装置MACアドレス	メンテナンスマード	コメント	⑫ 情報収集 (ARP)	⑬ 情報収集 (NDP)	⑭ 情報収集 (MACアドレス)	⑮ 情報収集 (LLDP)
⑯	⑰	⑱	⑲	⑳	㉑	㉒

2 件表示

⑪: メンテナンスマード  
⑫: 情報収集 (ARP)  
⑬: 情報収集 (NDP)  
⑭: 情報収集 (MACアドレス)  
⑮: 情報収集 (LLDP)  
⑯: 装置MACアドレス  
⑰: コメント  
⑱: 検索欄  
⑲: 検索ボタン  
⑳: ページナビゲーション  
㉑: ページナビゲーション  
㉒: ページナビゲーション

図 6-26 装置検索一覧画面 (3/5)

トップ > 共通 > 装置一覧 > 装置検索 > 装置検索一覧

装置検索画面表示

### 装置検索一覧

装置追加 ユーザ名/パスワード認証確認

検索:

②③ ■情報収集(WLC)	SNMP コミュニティ ユニティ	MIBオブジェクト エクト (ARP/NDP)	MIBオブジェクト (MACアドレス)	②④ ■MIBオブジエクト (LLDP-MIB)	②⑤ ■MIBオブジエクト (LLDP-V2-MIB)	②⑥ ■MIBオブジェクト (axslldp)	MIBオブジェクト (WLC) VLANリスト
②⑦	public	②⑨	②⑩	②⑪	②⑫	②⑬	
②⑮	public	②⑯	②⑰	②⑱	②⑲	②⑳	

2 件表示

図 6-27 装置検索一覧画面 (4/5)

トップ > 共通 > 装置一覧 > 装置検索 > 装置検索一覧

装置検索画面表示

装置検索一覧

装置追加 ユーザ名/パスワード認証確認

検索:

VLANリスト	ログインユーザ名	パスワード	装置管理者モード
③⁵	③⁶	③⁷	③⁸

2 件表示

図 6-28 装置検索一覧画面 (5/5)

トップ > 共通 > 装置一覧 > 装置検索 > 装置検索一覧

装置検索画面表示

装置検索一覧

[装置追加](#) [ユーザ名/パスワード認証確認](#)

検索:

(39)

特定端末へのWeb通信不可表示

パスワード

装置管理者モードのパスワード

ポート番号

(40)

(41)

(42)

(43)

<input type="text"/>	<input type="text"/>	<input type="button" value="③"/>
----------------------	----------------------	----------------------------------

<input type="text"/>	<input type="button" value="④"/>
----------------------	----------------------------------

<input type="checkbox"/>
--------------------------

80
----

<input type="text"/>	<input type="text"/>	<input type="button" value="⑤"/>
----------------------	----------------------	----------------------------------

<input type="text"/>	<input type="button" value="⑥"/>
----------------------	----------------------------------

<input type="checkbox"/>
--------------------------

80
----

2 件表示

表 6-28 装置検索一覧画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	装置検索画面表示ボタン	ボタンを押下すると、装置検索をおこなう IP アドレスと SNMP のコミュニティの編集をおこないます。もう一度ボタンを押下すると、装置検索画面表示を折りたたみます。
③	装置追加ボタン	ボタンを押下すると、個別選択チェックボックスで選択した装置を追加します。
④	ユーザ名/パスワード認証確認ボタン	ボタンを押下すると、「(h) ユーザ名/パスワード認証確認」のダイアログを表示します。 押下する際は、個別選択チェックボックスを 1 つ以上選択してください。
⑤	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑥	全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての装置を追加、またはユーザ名/パスワード認証確認対象とします。もう一度選択すると、すべての装置を追加、またはユーザ名/パスワード認証確認対象から外します。
⑦	状態	[追加ボタン押下後の追加失敗時] 下記に表示内容と理由を記載します。 <ul style="list-style-type: none"> <li>・ 装置名称不正：装置名称が入力されていない場合</li> <li>・ 装置名称重複不正：装置名称が重複している場合</li> <li>・ MAC アドレス不正：装置 MAC アドレスのフォーマットが間違っている場合</li> <li>・ VLAN リスト不正：VLAN リストの文字列のフォーマットが誤っている場合</li> <li>・ ポート番号不正：特定端末への Web 通信不可表示のポート番号が範囲外の場合</li> <li>・ 要求パラメータ不正：要求のパラメータに間違いがある場合</li> <li>・ データベースアクセス不正：データベースのアクセスに失敗した場合</li> </ul> [ユーザ名/パスワード認証確認の認証確認ボタン押下後の認証失敗時] 下記に表示内容と理由を記載します。 <ul style="list-style-type: none"> <li>・ 認証失敗：認証が失敗した場合</li> </ul>
⑧	個別選択チェックボックス	選択した装置を追加、またはユーザ名/パスワード認証確認対象とします。もう一度選択すると、追加、またはユーザ名/パスワード認証確認対象から外します。

項目番号	内容	説明
⑨	装置名称	装置検索で取得した sysName.0 の値を表示します。重複した名称がある場合、_<4桁の数字>を付与して表示します。 (例: AX3660S_0001)
⑩	IP アドレス/装置モデル/システム名称	装置検索で検出した IP アドレス/装置モデル/システム名称を表示します。 ブロードキャストアドレスに応答する装置がある場合、一覧に表示します。この場合、管理対象装置として登録をおこなわないでください。
⑪	メンテナンスマード全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての装置をメンテナンスマード有効対象とします。もう一度選択すると、すべての装置をメンテナンスマード有効対象から外します。
⑫	情報収集(ARP)全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての装置について ARP の情報収集を有効対象とします。もう一度選択すると、すべての装置から ARP の情報収集を有効対象から外します。
⑬	情報収集(NDP)全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての装置について NDP の情報収集を有効対象とします。もう一度選択すると、すべての装置から NDP の情報収集を有効対象から外します。
⑭	情報収集(MAC アドレス)全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての装置について MAC アドレスの情報収集を有効対象とします。もう一度選択すると、すべての装置から MAC アドレスの情報収集を有効対象から外します。
⑮	情報収集(LLDP)全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての装置について LLDP の情報収集を有効対象とします。もう一度選択すると、すべての装置から LLDP の情報収集を有効対象から外します。
⑯	装置 MAC アドレス	装置モデルが下記の場合、装置検索で取得した dot1dBaseBridgeAddress.0 の値を表示します。 取得できなかった場合、管理対象装置の識別として、一意となる MAC アドレスを入力してください。 <ul style="list-style-type: none"><li>・標準 MIB 対応装置</li><li>・標準 MIB 対応装置(VLAN 每コミュニティ)</li><li>・ワイヤレス LAN コントローラ</li></ul>
⑰	メンテナンスマード個別選択チェックボックス	情報収集有無を選択するボタンです。一時的に情報収集をおこなわなくする場合、有効を選択してください。
⑱	コメント	説明を記載する文字列です。0~256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。
⑲	情報収集(ARP)個別選択チェックボックス	ARP の情報収集を有効とします。 装置モデルが下記の場合、選択できません。 <ul style="list-style-type: none"><li>・ワイヤレス LAN コントローラ</li></ul>

項目番号	内容	説明
⑩	情報収集(NDP)個別選択チェックボックス	NDP の情報収集を有効とします。 装置モデルが下記の場合、選択できません。 ・AX2200S ・AX2100S ・AXprimoM210 ・ワイヤレス LAN コントローラ
⑪	情報収集(MAC アドレス)個別選択チェックボックス	MAC アドレスの情報収集を有効とします。 装置モデルが下記の場合、選択できません。 ・AX620R ・ワイヤレス LAN コントローラ
⑫	情報収集(LLDP)個別選択チェックボックス	LLDP の情報収集を有効とします。 装置モデルが下記の場合、選択できません。 ・AX620R ・ワイヤレス LAN コントローラ
⑬	情報収集(WLC)全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての装置について WLC の情報収集を有効対象とします。もう一度選択すると、すべての装置から WLC の情報収集を有効対象から外します。
⑭	MIB オブジェクト(LLDP-MIB)全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての装置について LLDP-MIB の情報収集を有効とします。もう一度選択すると、すべての装置から LLDP-MIB の情報収集を有効対象から外します。
⑮	MIB オブジェクト(LLDP-V2-MIB)全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての装置について LLDP-V2-MIB の情報収集を有効とします。もう一度選択すると、すべての装置から LLDP-V2-MIB の情報収集を有効対象から外します。
⑯	MIB オブジェクト(axslldp)全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての装置について axslldp の情報収集を有効とします。もう一度選択すると、すべての装置から axslldp の情報収集を有効対象から外します。
⑰	情報収集(WLC)個別選択チェックボックス	WLC の情報収集を有効とします。 装置モデルが下記でない場合、選択できません。 ・ワイヤレス LAN コントローラ
⑱	SNMP コミュニティ	装置検索画面で入力した SNMP コミュニティ名を表示します。
⑲	MIB オブジェクト(ARP/NDP)プルダウン	収集情報として以下のどちらかを選択します。 ・ipNetToMediaPhysAddress/ ipv6NetToMediaPhysAddress ・ipNetToPhysicalPhysAddress  装置モデルが下記でない場合、選択できません。 ・標準 MIB 対応装置 ・標準 MIB 対応装置(VLAN 每コミュニティ)

項目番号	内容	説明
⑩	MIB オブジェクト (MAC アドレス)プルダウン	収集情報として以下のどちらかを選択します。 <ul style="list-style-type: none"> <li>• dot1dTpFdbPort</li> <li>• dot1qTpFdbPort</li> </ul> <p>装置モデルが下記でない場合、選択できません。  <ul style="list-style-type: none"> <li>• 標準 MIB 対応装置</li> </ul> </p>
⑪	MIB オブジェクト (LLDP-MIB)個別選択チェックボックス	LLDP-MIB の情報収集を有効とします。 <p>装置モデルが下記でない場合、選択できません。  <ul style="list-style-type: none"> <li>• 標準 MIB 対応装置</li> <li>• 標準 MIB 対応装置(VLAN 每コミュニティ)</li> </ul> </p>
⑫	MIB オブジェクト (LLDP-V2-MIB)個別選択チェックボックス	LLDP-V2-MIB の情報収集を有効とします。 <p>装置モデルが下記でない場合、選択できません。  <ul style="list-style-type: none"> <li>• 標準 MIB 対応装置</li> <li>• 標準 MIB 対応装置(VLAN 每コミュニティ)</li> </ul> </p>
⑬	MIB オブジェクト (axslldp)個別選択チェックボックス	axslldp の情報収集を有効とします。 <p>装置モデルが下記でない場合、選択できません。  <ul style="list-style-type: none"> <li>• 標準 MIB 対応装置</li> <li>• 標準 MIB 対応装置(VLAN 每コミュニティ)</li> </ul> </p>
⑭	MIB オブジェクト (WLC)個別選択プルダウン	収集情報として以下から選択します。 <ul style="list-style-type: none"> <li>• Aruba-1-wlsxUserAllInfoGroup/wlsxWlanAccessPointInfoGroup</li> <li>• Cisco-1-bsnEss/bsnAP</li> <li>• Fortinet-1-mwConfigAp/mwConfigStation</li> </ul> <p>装置モデルが下記でない場合、選択できません。  <ul style="list-style-type: none"> <li>• ワイヤレス LAN コントローラ</li> </ul> </p>
⑮	VLAN リスト	管理対象装置の MAC アドレス情報収集時に使用する VLAN リストを入力します。 <p>VLAN リストとして使用可能な文字は、数値、ハイフン (-)、コンマ (,) です。(例: 10, 50-52)</p> <p>装置モデルが下記でない場合、入力できません。  <ul style="list-style-type: none"> <li>• 標準 MIB 対応装置(VLAN 每コミュニティ)</li> </ul> </p>
⑯	ログインユーザ名	ログインユーザ名を入力します。256 文字登録可能です。なおコロン(:)文字は使用しないでください。
⑰	パスワード	装置モデルが下記の場合、入力できません。 <ul style="list-style-type: none"> <li>• 標準 MIB 対応装置</li> <li>• 標準 MIB 対応装置(VLAN 每コミュニティ)</li> <li>• ワイヤレス LAN コントローラ</li> </ul> <p>装置モデルが下記の場合、入力できます。  <ul style="list-style-type: none"> <li>• 標準 MIB 対応装置</li> <li>• 標準 MIB 対応装置(VLAN 每コミュニティ)</li> <li>• ワイヤレス LAN コントローラ</li> </ul> </p>

項目番号	内容	説明
③⁸	パスワード可視化オンオフボタン	ログインパスワードの可視化のオンオフをおこないます。入力したログインパスワードの文字列を確認したい場合に押下してください。再度押下すると、文字列を隠します。
③⁹	特定端末への Web 通信不可表示個別選択チェックボックス	特定端末への Web 通信不可表示機能の有効、または無効を選択します。 特定端末への Web 通信不可表示機能を有効にする場合、有効を選択してください。  装置モデルが下記の場合、選択できません。 ・AXprimoM210 ・AX620R ・標準 MIB 対応装置 ・標準 MIB 対応装置(VLAN 毎コミュニティ) ・ワイヤレス LAN コントローラ
④⁰	装置管理者モードのパスワード	装置管理者モードのパスワードを入力します。0～256 文字登録可能です。  装置モデルが下記の場合、入力できません。 ・AX620R ・標準 MIB 対応装置 ・標準 MIB 対応装置(VLAN 毎コミュニティ) ・ワイヤレス LAN コントローラ
④¹	装置管理者モードのパスワード可視化オンオフボタン	装置管理者モードのパスワードの可視化のオンオフをおこないます。入力した装置管理者モードのパスワードの文字列を確認したい場合に押下してください。再度押下すると、文字列を隠します。
④²	特定端末への Web 通信不可表示全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての装置について特定端末への Web 通信不可表示機能を有効対象とします。もう一度選択すると、すべての装置から特定端末への Web 通信不可表示機能を有効対象から外します。
④³	ポート番号	特定端末への Web 通信不可表示として、TCP ポート番号を入力します。0～65535 の値を入力してください。  装置モデルが下記の場合、選択できません。 ・AXprimoM210 ・AX620R ・標準 MIB 対応装置 ・標準 MIB 対応装置(VLAN 毎コミュニティ) ・ワイヤレス LAN コントローラ

表 6-29 装置検索一覧の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	追加対象装置が選択されていません	装置が選択されていません。個別選択チェックボックスを 1 つ以上選択してください。

図 6-29 装置検索画面表示中画面



(h) ユーザ名/パスワード認証確認

図 6-30 ユーザ名/パスワード認証確認画面



表 6-30 ユーザ名/パスワード認証確認画面に表示する項目

項目番号	内容	説明	
①	ユーザ名/パスワード認証確認	SSH ログインユーザ名	検索対象である管理対象装置の SSH ログインユーザ名を入力します。0~256 文字を入力可能です。
②		SSH パスワード	検索対象である管理対象装置の SSH パスワードを入力します。0~256 文字を入力可能です。
③		SSH パスワード可視化ボタン	SSH パスワードの可視化のオンオフをおこないます。入力したパスワードの文字列を確認したい場合に押下してください。再度押下すると、文字列を隠します。
④		装置管理者モードのパスワード	検索対象である管理対象装置の装置管理者モードのパスワードを入力します。0~256 文字を入力可能です。
⑤		装置管理者モードのパスワード可視化ボタン	装置管理者モードのパスワードの可視化のオンオフをおこないます。入力したパスワードの文字列を確認したい場合に押下してください。再度押下すると、文字列を隠します。
⑥		認証確認ボタン	ボタンを押下すると、「(g) 装置検索一覧」に移動します。SSH ログインユーザ名 / SSH パスワード / 装置管理者モードのパスワードの認証確認をおこない、認証に失敗した場合、「表 6-28 装置検索一覧画面に表示する項目」の状態に結果を表示します。
⑦		閉じるボタン	装置編集をキャンセルします。ボタンを押下すると、「(g) 装置検索一覧」に移動します。

表 6-31 ユーザ名/パスワード認証確認の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	追加対象装置が選択されていません	追加対象装置が選択されていません。個別選択チェックボックスを 1 つ以上選択してください。

## (2) 接続情報設定

図 6-31 接続情報設定画面



表 6-32 接続情報設定画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	接続情報追加ボタン	新規に接続情報を追加します。ボタンを押下すると「(a) 接続情報追加」に移動します。
③	接続情報検索ボタン	新規に接続情報を追加するための、接続情報の検索をおこないます。ボタンを押下すると「(b) 接続情報検索結果」に移動します。
④	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「nodes_link.csv」となります。
⑤	CSV 形式からの接続情報追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上の接続情報を追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑥	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑦	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑧	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑨	接続情報一覧	接続情報一覧を表示します。 表示項目は、装置 A 名称/装置 A ポート番号/装置 A アクセスリスト拡張ポート/装置 B 名称/装置 B ポート番号/装置 B アクセスリスト拡張ポートです。

項目番号	内容	説明
⑩	削除ボタン	<p>操作として、接続情報を削除します。ボタン押下時、</p> <p>接続情報 装置 A:&lt;装置 A 名称&gt; 装置 A ポート番号:&lt;装置 A ポート番号&gt; 装置 B:&lt;装置 B 名称&gt; 装置 B ポート番号:&lt;装置 B ポート番号&gt; を削除します</p> <p>の確認ダイアログを表示します。了承した場合、接続情報を削除します。削除が失敗すると、「表 6-33 接続情報削除の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p>
⑪	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-33 接続情報削除の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	指定した接続情報が存在しません	指定した接続情報が存在しません。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) 接続情報追加

図 6-32 接続情報追加画面

① ブラウザアドレスバーに表示される階層リンク (トップ > 共通 > 接続情報設定 > 接続情報追加)

② 装置 A の名前 (AX3660S)

③ 装置 A のポート番号 (1/0/1)

④ 装置 A のアクセスリスト (有効)

⑤ 装置 B の名前 (AX2500S)

⑥ 装置 B のポート番号 (0/1)

⑦ 装置 B のアクセスリスト (有効)

⑧ 「追加」ボタン (赤い枠で囲まれて表示)

⑨ 「キャンセル」ボタン

表 6-34 接続情報追加画面に表示する項目

項目番	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	装置 A	名称	隣接する管理対象装置(装置 A-装置 B)の装置 A の名称を入力します。 「(1)(a) 装置追加」で登録した装置名称を入力してください。
③		ポート番号	装置 A の接続ポートを入力してください。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>, <switch no.>/<nif no.>/<port no.>となります。 装置 A の装置モデルが 標準 MIB 対応装置、または 標準 MIB 対応装置(VLAN 每コミュニティ)の場合、 「(1)(b) 装置詳細」の MAC アドレステーブル一覧に表示されるポートを入力してください。 装置 A の装置モデルが AX620R の場合、トンネルインターフェース、またはサブインターフェースの名称を入力してください。 装置 A の装置モデルがワイヤレス LAN コントローラの場合、装置 A で一意となるポートの名称を入力してください。

項目番号	内容		説明
④		アクセスリスト拡張ポート	<p>装置 A のアクセスリスト拡張ポートの有効、または無効を選択します(1.6.7(2)を参照)。</p> <p>装置 A の装置モデルと装置 B の装置モデルの組み合わせが下記の場合、必要に応じて、有効を設定してください。</p> <p>装置 A の装置モデルが下記でない場合：</p> <ul style="list-style-type: none"> <li>・標準 MIB 対応装置</li> <li>・標準 MIB 対応装置(VLAN 每コミュニティ)</li> <li>・ワイヤレス LAN コントローラ</li> </ul> <p>装置 B の装置モデルが下記の場合：</p> <ul style="list-style-type: none"> <li>・標準 MIB 対応装置</li> <li>・標準 MIB 対応装置(VLAN 每コミュニティ)</li> <li>・ワイヤレス LAN コントローラ</li> </ul>
⑤	装置 B	名称	<p>隣接する管理対象装置(装置 A-装置 B)の装置 B の名称を入力します。</p> <p>「(1)(a) 装置追加」で登録した装置名称を入力してください。</p>
⑥		ポート番号	<p>装置 B の接続ポートを入力してください。</p> <p>入力形式は、装置モデルに応じて、&lt;nif no.&gt;/&lt;port no.&gt;, &lt;switch no.&gt;/&lt;nif no.&gt;/&lt;port no.&gt;となります。</p> <p>装置 B の装置モデルが 標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 每コミュニティ)の場合、「(1)(b) 装置詳細」の MAC アドレステーブル一覧に表示されるポートを入力してください。</p> <p>装置 B の装置モデルが AX620R の場合、トンネルインターフェース、またはサブインターフェースの名称を入力してください。</p> <p>装置 B の装置モデルがワイヤレス LAN コントローラの場合、装置 B で一意となるポートの名称を入力してください。</p>
⑦		アクセスリスト拡張ポート	<p>装置 B のアクセスリスト拡張ポートの有効、または無効を選択します(1.6.7(2)を参照)。</p> <p>装置 A の装置モデルと装置 B の装置モデルの組み合わせが下記の場合、必要に応じて、有効を設定してください。</p> <p>装置 A の装置モデルが下記の場合：</p> <ul style="list-style-type: none"> <li>・標準 MIB 対応装置</li> <li>・標準 MIB 対応装置(VLAN 每コミュニティ)</li> <li>・ワイヤレス LAN コントローラ</li> </ul> <p>装置 B の装置モデルが下記でない場合：</p> <ul style="list-style-type: none"> <li>・標準 MIB 対応装置</li> <li>・標準 MIB 対応装置(VLAN 每コミュニティ)</li> <li>・ワイヤレス LAN コントローラ</li> </ul>
⑧		追加ボタン	<p>接続情報を追加します。ボタンを押下し、追加が成功すると、「(2) 接続情報設定」に移動します。反映が失敗すると、「表 6-35 接続情報追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p>
⑨		キャンセルボタン	<p>接続情報追加をキャンセルします。ボタンを押下すると、「(2) 接続情報設定」に移動します。</p>

表 6-35 接続情報追加の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	装置 A の装置名称を入力してください	装置 A の装置名称が空白です。「(1)(a) 装置追加」で登録した装置名称を入力してください。
2	装置 B の装置名称を入力してください	装置 B の装置名称が空白です。「(1)(a) 装置追加」で登録した装置名称を入力してください。
3	装置 A のポートを入力してください	装置 A のポートが空白です。装置 A のポートを入力してください。
4	装置 B のポートを入力してください	装置 B のポートが空白です。装置 B のポートを入力してください。
5	装置 A が存在しない装置名称です	装置 A の装置名称は登録されていません。「(1)(a) 装置追加」で登録した装置名称を入力してください。
6	装置 B が存在しない装置名称です	装置 B の装置名称は登録されていません。「(1)(a) 装置追加」で登録した装置名称を入力してください。
7	要求のパラメータに間違いがあるか、削除中の装置です	要求のパラメータに間違いがあるか、削除中の装置です。「6.1.8(6) メンテナンス」により保守情報を収集してください。
8	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (b) 接続情報検索結果

図 6-33 接続情報検索結果画面

The screenshot shows the 'Connection Information Search Result' page. At the top, there is a breadcrumb navigation: トップ > 共通 > 接続情報設定 > 接続情報検索結果. A red box labeled ① surrounds this area. Below the breadcrumb, the title '接続情報検索結果' is displayed. On the left, there is a 'Select Connection Information to Add' button (②). To its right are buttons for 'Display Column Switch' (③), 'ALL' (④), and a search input field (⑤). Further down, there are checkboxes for 'Device A Accessory Expansion Port' (⑦) and 'Device B Accessory Expansion Port' (⑧). The main content area shows a table with four rows of data. The first row contains: Device A Name (AX3660S-48T4XW-057\_0001), Date (1/0/13), and Device B Name (AX3640). The second row contains: Device A Name (AX3660S-48T4XW-057\_0001), Date (1/0/13), and Device B Name (AX3640). The third row contains: Device A Name (AX3660S-48T4XW-057\_0001), Date (1/0/14), and Device B Name (AX3640). The fourth row contains: Device A Name (AX3660S-48T4XW-057\_0001), Date (1/0/14), and Device B Name (AX3640). Each row has a checkbox in the first column (⑨, ⑩, ⑪, ⑫) and a checkbox in the last column (⑬, ⑭). At the bottom, it says '4 件中 1 から 4 まで表示' and a navigation bar with '前のページ' (⑯), '1' (highlighted with a red box), and '次のページ'.

表 6-36 接続情報検索結果画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	選択接続情報追加ボタン	ボタンを押下すると、選択した接続情報を追加します(<個別選択チェックボックスの選択済み数>件)の確認ダイアログを表示します。了承し、選択した個別選択チェックボックス※の追加の反映が成功すると、「(2) 接続情報設定」に移動します。反映が失敗すると、「表 6-37 接続情報検索結果の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
③	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。

項目番号	内容	説明
④	ページあたり表示件数 切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑤	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑥	全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての接続情報を追加対象とします。もう一度選択すると、すべての接続情報を追加対象から外します。
⑦	装置 A アクセスリスト 拡張ポート全選択 チェックボックス	検索テキストボックスにより絞り込んだ、すべての接続情報について、装置 A アクセスリスト拡張ポートを有効とします。もう一度選択すると、すべての接続情報から装置 A アクセスリスト拡張ポートを無効とします。
⑧	装置 B アクセスリスト 拡張ポート全選択 チェックボックス	検索テキストボックスにより絞り込んだ、すべての接続情報について、装置 B アクセスリスト拡張ポートを有効とします。もう一度選択すると、すべての接続情報から装置 B アクセスリスト拡張ポートを無効とします。
⑨	個別選択チェックボックス	選択した接続情報を追加対象とします。もう一度選択すると、追加対象から外します。
⑩	装置 A	装置 A 接続情報
⑪		装置 A アクセスリスト拡張ポート個別選択チェックボックス
⑫	装置 B	装置 B 接続情報
⑬		装置 B アクセスリスト拡張ポート個別選択チェックボックス
⑭	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

## 注※

任意の個別選択チェックボックスが選択された状態で、検索テキストボックスまたはカラムごと検索テキストボックスで絞り込みをおこない、接続情報が表示されない場合でも、接続情報は追加対象のままでです。この状態でボタンを押下すると、接続情報の追加が実施されることに注意してください。

表 6-37 接続情報検索結果の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	接続情報が選択されていません	接続情報が選択されていません。
2	要求のパラメータに間違があるか、削除中の装置です	要求のパラメータに間違があるか、削除中の装置です。「6.1.8(6) メンテナンス」により保守情報を収集してください。
3	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (3) ポートエイリアス

図 6-34 ポートエイリアス一覧画面

表 6-38 ポートエイリアス一覧画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ポートエイリアス追加ボタン	新規にポートエイリアスを追加します。ボタンを押下すると「(a) ポートエイリアス追加」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「nodes_portalias.csv」となります。

項目番号	内容	説明
④	CSV 形式からのポートエイリアス追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上のポートエイリアスを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑤	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑥	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑦	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑧	ポートエイリアス情報	ポートエイリアス情報の一覧を表示します。表示項目は、ポートエイリアス/条件/操作です。
⑨	ポートエイリアスの編集ボタン	操作として、ポートエイリアスの編集をおこないます。ボタンを押下すると、「(b) ポートエイリアス編集」に移動します。
⑩	ポートエイリアスの削除ボタン	操作として、ポートエイリアスの削除をおこないます。ボタンを押下すると、  ポートエイリアス <ポートエイリアス> を削除します  の確認ダイアログを表示します。了承した場合、ポートエイリアスを削除します。削除が失敗すると、「表 6-39 ポートエイリアス一覧の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑪	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-39 ポートエイリアス一覧の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	指定したポートエイリアスが存在しません	指定したポートエイリアスが存在しません。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) ポートエイリアス追加

図 6-35 ポートエイリアス追加画面

表 6-40 ポートエイリアス追加に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ポートエイリアス	ポートエイリアスを示す文字列を入力します。最大256 文字登録可能です。なおアポストロフィー('')文字は使用しないでください。「空白("")」は入力しないでください。
③	装置名称	ポートエイリアスに対応する装置の名称を入力します。 「(1)(a) 装置追加」で登録した装置名称を入力してください。
④	ポート番号	ポートエイリアスに対応するポート番号を入力します。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>, <switch no.>/<nif no.>/<port no.>となります。 装置の装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 每コミュニティ)の場合、 「(1)(b) 装置詳細」の MAC アドレステーブル一覧に表示されるポートを入力してください。
⑤	追加ボタン	ポートエイリアス追加を反映します。ボタンを押下し、反映が成功すると、「(3) ポートエイリアス」に移動します。反映が失敗すると、「表 6-41 ポートエイリアス追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑥	キャンセルボタン	ポートエイリアス追加をキャンセルします。ボタンを押下すると、「(3) ポートエイリアス」に移動します。

表 6-41 ポートエイリアス追加の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	ポートエイリアスを入力してください	ポートエイリアスが空白です。1文字以上の文字列を入力してください。
2	装置名称を入力してください	装置名称を入力してください。
3	ポート番号を入力してください	ポート番号を入力してください。
4	存在しない装置名称です	存在しない装置名称です。
5	要求のパラメータに間違があります	要求のパラメータに間違いがあります。「6.1.8(6)メンテナンス」により保守情報を収集してください。
6	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (b) ポートエイリアス編集

図 6-36 ポートエイリアス編集画面

表 6-42 ポートエイリアス編集画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ポートエイリアス	追加済みのポートエイリアスを示す文字列。
③	装置名称	追加済みのポートエイリアスに対応する装置の名称を入力します。 「(1)(a) 装置追加」で登録した装置名称を入力してください。

項番	内容	説明
④	ポート番号	追加済みのポートエイリアスに対応するポート番号を入力します。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>, <switch no.>/<nif no.>/<port no.>となります。 装置の装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 每コミュニティ)の場合、「(1)(b) 装置詳細」の MAC アドレステーブル一覧に表示されるポートを入力してください。
⑤	更新ボタン	ポートエイリアス編集を反映します。ボタンを押下し、反映が成功すると、「(3) ポートエイリアス」に移動します。反映が失敗すると、「表 6-43 ポートエイリアス編集の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑥	キャンセルボタン	ポートエイリアス編集をキャンセルします。ボタンを押下すると、「(3) ポートエイリアス」に移動します。

表 6-43 ポートエイリアス編集の反映失敗時のダイアログ一覧

項番	内容	説明
1	存在しない装置名称です	存在しない装置名称です。
2	装置名称を入力してください	装置名称を入力してください。
3	ポート番号を入力してください	ポート番号を入力してください。
4	要求のパラメータに間違があります	要求のパラメータに間違があります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
5	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (4) 管理対象外ポート

図 6-37 管理対象外ポート一覧画面



表 6-44 管理対象外ポート一覧画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	管理対象外ポート追加ボタン	新規に管理対象外ポートを追加します。ボタンを押下すると「(a) 管理対象外ポート追加」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「nodes_excludedport.csv」となります。
④	CSV 形式からの管理対象外ポート追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上の管理対象外ポートを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑤	選択管理対象外ポート削除ボタン	ボタンを押下すると、選択した管理対象外ポートを削除します(<個別選択チェックボックスの選択済み管理対象外ポート数>件)の確認ダイアログを表示します。了承した場合、選択した個別選択チェックボックスの管理対象外ポートを削除します。反映が失敗すると、「表 6-45 管理対象外ポート一覧の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑥	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。

項目番号	内容	説明
⑦	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑧	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑨	全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべての管理対象外ポートを削除対象とします。もう一度選択すると、すべての管理対象外ポートを削除対象から外します。
⑩	個別選択チェックボックス	選択した管理対象外ポートを削除対象とします。もう一度選択すると、削除対象から外します。
⑪	管理対象外ポート情報	管理対象外ポート情報の一覧を表示します。表示項目は、装置名称/ポート番号です。
⑫	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-45 管理対象外ポート一覧の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	管理対象外ポートが選択されていません	管理対象外ポートが選択されていません。個別選択チェックボックスを 1 つ以上選択してください。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) 管理対象外ポート追加

図 6-38 管理対象外ポート追加画面

①

②

③

④

⑤

表 6-46 管理対象外ポート追加に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	装置名称	「(1)(a) 装置追加」で登録した装置名称を入力してください。
③	ポート番号	管理対象外ポートを入力します。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>, <switch no.>/<nif no.>/<port no.>となります。 装置の装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 毎コミュニティ)の場合、「(1)(b) 装置詳細」の MAC アドレステーブル一覧に表示されるポートを入力してください。 装置の装置モデルがワイヤレス LAN コントローラの場合、当該装置で一意となるポートの名称を入力してください。
④	追加ボタン	ボタンを押下すると、 管理対象外ポートを追加します 管理対象外ポートに設定されているアクセリストがある場合、トポロジ管理で保持している端末情報がエージアウトすると削除されます  の確認ダイアログを表示します。了承し、管理対象外ポート追加の反映が成功すると、「(4) 管理対象外ポート」に移動します。反映が失敗すると、「表 6-47 管理対象外ポート追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑤	キャンセルボタン	管理対象外ポート追加をキャンセルします。ボタンを押下すると、「(4) 管理対象外ポート」に移動します。

表 6-47 管理対象外ポート追加の反映失敗時のダイアログ一覧

項目番	内容	説明
1	装置名称を入力してください	装置名称を入力してください。
2	ポート番号を入力してください	ポート番号を入力してください。
3	存在しない装置名称です	存在しない装置名称です。
4	既に登録済みの装置とポート番号の組み合わせです	既に登録済みの装置とポート番号の組み合わせです。
5	要求のパラメータに間違があるか、削除中の装置です。「6.1.8(6) メンテナンス」により保守情報を収集してください。	要求のパラメータに間違があるか、削除中の装置です。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## 6 AX-Security-Controller(Manager)の Web インタフェース

項目番号	内容	説明
6	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## 6.1.5 セグメント

### (1) セグメント一覧

6-39 セグメント一覧画面

The screenshot shows the 'Segment List' page. At the top, there are navigation links: 'トップ' (Top), '共通' (Common), and 'セグメント一覧' (Segment List). Below these are several buttons: 'セグメント追加' (Add Segment) (②), 'CSV形式で保存' (Save as CSV) (③), and 'CSV形式からのセグメント追加' (Add Segment from CSV) (④). There is also a '表示カラム切替' (Column Switch) button (⑤), a dropdown for '件表示' (Number of items per page) set to 25 (⑥), a search input field (⑦), and a '検索' (Search) button. The main area displays a table of segments:

セグメント名	優先度	状態	端末接続数	遮断端末数	コメント	操作
信頼済みセグメント	1	設定済み	0	0		<span>削除</span> (⑨)
セグメント1	2001 (⑧)	設定済み	0	0		
無所属セグメント	10000	設定済み	0	0		

Below the table, it says '3件中 1 から 3 まで表示' (Showing 1 to 3 of 3). At the bottom right are '前のページ' (Previous page), '1' (Page 1), and '次のページ' (Next page).

表 6-48 セグメント一覧画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	セグメント追加ボタン	新規にセグメントを追加します。ボタンを押下すると「(a) セグメント追加」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「segments.csv」となります。
④	CSV 形式からのセグメント追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上のセグメントを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑤	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑥	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑦	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑧	セグメント情報	セグメント情報の一覧を表示します。 表示項目は、セグメント名称/優先度/状態/端末接続数/遮断端末数/コメントです。 セグメントのエントリを押下すると、「(b) セグメント設定」に移動します。

項番	内容	説明
⑨	削除ボタン	<p>操作として、セグメントの削除を行います。ボタンを押下すると、</p> <p>セグメント &lt;セグメント名称&gt; を削除します</p> <p>の確認ダイアログを表示します。了承した場合、セグメントを削除します。削除が失敗すると、「表 6-49 セグメント一覧の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p> <p>なお、信頼済みセグメントと、無所属セグメントは削除することができません。</p>
⑩	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-49 セグメント一覧の反映失敗時のダイアログ一覧

項番	内容	説明
1	既に削除済みのセグメントです	既に削除済みのセグメントです。
2	指定したセグメントが存在しません	指定したセグメントが存在しません。
3	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) セグメント追加

図 6-40 セグメント追加画面

表 6-50 セグメント追加画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	セグメント名称	セグメント情報としてセグメントの名称を示す文字列です。最大 256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。
③	優先度	セグメント間の優先度を 1001~9000 までの数値で指定します。
④	コメント	セグメント情報として、セグメントの説明を記載する文字列です。0~256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。
⑤	無所属セグメントのルールコピー	有効を選択して反映すると、無所属セグメントに設定されたルールをコピーします。
⑥	追加ボタン	セグメント追加を反映します。ボタンを押下し、反映が成功すると、「(1) セグメント一覧」に移動します。反映が失敗すると、「表 6-51 セグメント追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。

項番	内容	説明
⑦	キャンセルボタン	セグメント追加をキャンセルします。ボタンを押下すると、「(1) セグメント一覧」に移動します。

表 6-51 セグメント追加の反映失敗時のダイアログ一覧

項番	内容	説明
1	セグメント名称が入力されていません	セグメント名称が入力されていません。セグメント名称を入力してください。
2	優先度が入力されていません	優先度が入力されていません。優先度を入力してください。
3	範囲外の優先度です	範囲外の優先度です。正しい優先度の値で入力してください。
4	重複したセグメント名称です	セグメント名称は既に登録済みです。別のセグメント名称を使用して登録してください。
5	既に登録済みのセグメント名称または優先度です	セグメント名称、または優先度は既に登録済みです。別のセグメント名称か、優先度を使用して登録してください。
6	要求パラメータに間違いがあります	要求のパラメータに間違いがあります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
7	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (b) セグメント設定

図 6-41 セグメント設定画面 (1/2)

図 6-41 セグメント設定画面 (1/2) のスクリーンショットです。この画面は、セグメントの定義とルールの管理を行なうためのものです。

**セグメント情報**

- セグメント名: セグメント1 (②)
- 優先度: 2001 (③)
- コメント: (④)

**セグメント定義**

- 操作ボタン: セグメント定義追加 (⑥), CSV形式で保存 (⑦), CSV形式からのセグメント定義追加 (⑧)
- 表示カラム切替 (⑨), 件数表示 (25) (⑩)
- 検索 (⑪)
- 操作ボタン: 削除 (⑬)
- 条件: IPサブネット (IP:192.168.10.0/24) (⑫)

**ルール**

- 操作ボタン: ルール追加 (⑯), CSV形式で保存 (⑰), CSV形式からのルール追加 (⑱)
- 表示カラム切替 (⑲), 件数表示 (25) (⑳)
- 検索 (㉑)
- ルール一覧表 (㉒)
 

クラ	優	条件1種	条件	条件2	条件3種	条件4種	条件5種	条件6種	条件7種	送信元	送信先
イア	先	条件1種	条件	条件2	条件3種	条件4種	条件5種	条件6種	条件7種	指定	指定
ント	度	別	1値	種別	条件2値	条件3値	条件4値	条件5値	条件6値	条件7値	条件7値
Syslog	10	Signature	virus	Name	THREAT	Severity	5	5	5	5	5
クラ	ID										
イア											
ント7											

図 6-42 セグメント設定画面 (2/2)

The screenshot displays three panels of the segment setting interface:

- 永続設定ポート(受信側)**: Shows a table with one entry: "エッジスイッチ1" (Port Number 0/5). Buttons include "表示カラム切替" (24), "件表示" (25), "検索" (26), "操作" (27), "削除" (28), and navigation buttons "前のページ" (29), "1", and "次のページ".
- 永続設定ポート(送信側)**: Shows a table with one entry: "コアスイッチ1" (Port Number 0/6). Buttons include "表示カラム切替" (31), "件表示" (32), "検索" (33), "操作" (34), "削除" (35), and navigation buttons "前のページ" (36), "1", and "次のページ".
- セキュリティフィルタ自動解除スケジュール**: Shows a table with one entry: "毎月1日00:10" (Release Date 2019/03/01 00:10:00 JST). Buttons include "自動解除スケジュール追加" (37), "操作" (38), and "削除" (39).

表 6-52 セグメント設定画面に表示する項目

項目番号	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	セグメント情報	セグメント名	セグメント情報として、登録済みのセグメント名称を表示します。
③		優先度	セグメント間の優先度を 1001~9000 までの数値で指定します。
④		コメント	セグメント情報として、セグメントの説明を記載する文字列です。0~256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。
⑤	—	更新ボタン	セグメント情報の変更を反映します。
⑥	セグメント定義	セグメント定義追加ボタン	新規にセグメント定義を追加します。ボタンを押下すると、「(c) セグメント定義追加」に移動します。

項目番号	内容	説明	
⑦	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「segments_definition.csv」となります。	
⑧	CSV 形式からのセグメント定義追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上のセグメント定義を追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。	
⑨	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。	
⑩	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。	
⑪	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。	
⑫	セグメント定義情報	セグメント定義情報の一覧を表示します。表示項目は、種別/条件です。	
⑬	削除ボタン	操作として、セグメント定義情報を削除します。ボタン押下時、  セグメント定義 <種別><条件> を削除します  の確認ダイアログを表示します。了承した場合、セグメント定義情報を削除します。削除が失敗すると、「表 6-53 セグメント設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。	
⑭	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。	
⑮	ルール	ルール追加ボタン	新規にルールを追加します。ボタンを押下すると「6.1.6(8)(a) ルール追加」に移動します。
⑯	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「segments_rule.csv」となります。	
⑰	CSV 形式からのルール追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上のルールを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。	
⑱	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。	
⑲	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。	

項目番号	内容	説明
⑩	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑪	ルール情報/操作	<p>ルール情報の一覧を表示します。 表示項目は、クライアント/優先度/条件1種別/条件1値/条件2種別/条件2値/条件3種別/条件3値/条件4種別/条件4値/条件5種別/条件5値/条件6種別/条件6値/送信元指定/宛先指定/アクションです。 操作には各種ボタンを表示し、以下に示す動作をします。</p> <ul style="list-style-type: none"> <li>「削除」ボタンを押下すると、ルールの削除を行います。ボタンを押下すると、 ルール クライアント:&lt;クライアント名称&gt; 優先度 &lt;優先度&gt; を削除します。</li> </ul> <p>の確認ダイアログを表示します。了承した場合、ルールを削除します。削除が失敗すると、「表 6-53 セグメント設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p> <ul style="list-style-type: none"> <li>「全セグメントコピー」ボタンを押下すると、ルール情報を、すべての個別セグメントと無所属セグメントにコピーします。 ボタンを押下すると、 ルール クライアント:&lt;クライアント名称&gt; 優先度 &lt;優先度&gt; を全セグメントに適用します</li> </ul> <p>の確認ダイアログを表示します。了承した場合、ルールをコピーします。削除が失敗すると、「表 6-53 セグメント設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p>
⑫	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。
⑬	永続設定ポート(受信側)	永続設定ポート(受信側)追加ボタン 新規に永続設定ポート(受信側)を追加します。「6.1.8(1)(b) 永続設定ポート(受信側)追加」を参照してください。
⑭		表示カラム切替ボタン 一覧から不要なカラムを非表示にすることができます。
⑮		ページあたり表示件数切替プルダウン 1ページあたりに表示する件数を切り替えることができます。件数のパターンは10/25/50/100/全ての5パターンです。

項目番号	内容	説明
⑯	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑰	永続設定ポート(受信側)情報	追加済みの永続設定ポート(受信側)情報(装置名称, ポート番号)を表示します。
⑱	削除ボタン	永続設定ポート(受信側)情報を削除します。ボタン押下時,  永続設定ポート(受信側) 装置:<装置名称> ポート:<ポート番号> を削除します  の確認ダイアログを表示します。了承した場合, 永続設定ポート(受信側)情報を削除します。削除が失敗すると, 「表 6-123 共通設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑲	ページ切替ボタン	ボタンを押下すると, 指定のページを表示します。
⑳	永続設定ポート(送信側)	永続設定ポート(送信側)追加ボタン 新規に永続設定ポート(送信側)を追加します。「6.1.8(1)(c) 永続設定ポート(送信側)追加」を参照してください。
㉑		表示カラム切替ボタン 一覧から不要なカラムを非表示にすることができます。
㉒		ページあたり表示件数切替プルダウン 1ページあたりに表示する件数を切り替えることができます。件数のパターンは10/25/50/100/全ての5パターンです。
㉓		検索テキストボックス テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
㉔	永続設定ポート(送信側)情報	追加済みの永続設定ポート(送信側)情報(装置名称, ポート番号)を表示します。
㉕	削除ボタン	永続設定ポート(送信側)情報を削除します。ボタン押下時,  永続設定ポート(送信側) 装置:<装置名称> ポート:<ポート番号> を削除します  の確認ダイアログを表示します。了承した場合, 永続設定ポート(送信側)情報を削除します。削除が失敗すると, 「表 6-123 共通設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
㉖	ページ切替ボタン	ボタンを押下すると, 指定のページを表示します。

項目番号	内容	説明
③⑦	セキュリティフィルタ自動解除スケジュール	新規に自動解除スケジュールを追加します。「6.1.8(1)(e) セキュリティフィルタ自動解除スケジュール追加」を参照してください。
③⑧		追加済みの自動解除スケジュール(解除スケジュール、解除予定日時)を表示します。解除予定日時は、次回、自動解除スケジュールが動作する予定の日時を表示します。
③⑨		対象の自動解除スケジュールを削除します。ボタンを押下すると、 セキュリティフィルタ自動解除スケジュール <スケジュール単位><自動解除時刻> を削除します  の確認ダイアログを表示します。 了承した場合、自動解除スケジュールを削除します。削除が失敗すると、「表 6-123 共通設定の反映失敗時のダイアログ一覧」 に示すダイアログを表示します。

表 6-53 セグメント設定の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	優先度が入力されていません	優先度が入力されていません。優先度を入力してください。
2	範囲外の優先度です	範囲外の優先度です。正しい優先度の値で入力してください。
3	重複した優先度です	重複した優先度です。別の優先度で入力してください。
4	指定したセグメント定義が存在しません	指定したセグメント定義が存在しません。
5	既に削除済みのルールです	既に削除済みのルールです。
6	他セグメントのルールと重複した優先度です	他セグメントのルールと重複した優先度です。
7	既に削除済みの装置とポート番号の組み合わせです	既に削除済みの装置とポート番号の組み合わせです。
8	指定した永続設定ポート(受信側)が存在しません	指定した永続設定ポート(受信側)が存在しません。

項目番号	内容	説明
9	指定した永続設定ポート(送信側)が存在しません。	指定した永続設定ポート(送信側)が存在しません。
10	指定したスケジュールが存在しません	指定したスケジュールが存在しません。
11	要求パラメータに間違いがあります	要求のパラメータに間違いがあります。「6.1.8(6)メンテナンス」により保守情報を収集してください。
12	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

### (c) セグメント定義追加

図 6-43 セグメント定義追加画面

① トップ > 共通 > セグメント一覧 > セグメント設定(セグメント1) > セグメント定義追加

② セグメント種別: IPサブネット

③ IPアドレス/マスク: 192.168.10.0/24

④ MACアドレス: [空]

⑤ 装置名称: [空]

⑥ ポート番号: <nif>/<port> or <switch>/<nif>/<port>

⑦ 追加 (Blue button)

⑧ キャンセル (Red button)

表 6-54 セグメント定義追加画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。

項目番	内容		説明
②	セグメント定義	セグメント種別	セグメント定義として、セグメント種別を選択します。以下のいずれかです。 <ul style="list-style-type: none"><li>・IP サブネット</li><li>・MAC アドレス</li><li>・端末収容ポート</li></ul>
③		IP アドレス/マスク	セグメント種別が IP サブネットの場合に、セグメントに属する IP アドレス/マスクを入力します。 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をスラッシュ(/)文字で連結して入力します。 IPv4 アドレスは 0.0.0.0～255.255.255.255、マスクは 0～32 を入力してください。 IPv6 アドレスは::～ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff、プレフィックス長は 0～128 を入力してください。
④		MAC アドレス	セグメント種別が MAC アドレスの場合に、セグメントに属する MAC アドレスを入力します。 0000.0000.0000～ffff.ffff.ffff を入力してください。
⑤		装置名称	セグメント種別が端末収容ポートの場合に、セグメントに属する装置名称を入力します。 「6.1.4(1)(a) 装置追加」で登録した装置名称を入力してください。
⑥		ポート番号	セグメント種別が端末収容ポートの場合に、セグメントに属するポート番号を入力します。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>, <switch no.>/<nif no.>/<port no.>となります。 装置モデルが AX620R の場合、トンネルインターフェース、またはサブインターフェースの名称を入力してください。
⑦	—	追加ボタン	セグメント定義追加を反映します。ボタンを押下し、反映が成功すると、「(b) セグメント設定」に移動します。反映が失敗すると、「表 6-55 セグメント定義追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑧		キャンセルボタン	セグメント定義追加をキャンセルします。ボタンを押下すると、「(b) セグメント設定」に移動します。

表 6-55 セグメント定義追加の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	セグメント種別が入力されていません	セグメント種別が入力されていません。セグメント種別を選択してください。
2	IP アドレス/マスクが入力されていません	IP アドレス/マスクが入力されていません。IP アドレス/マスクを入力してください。
3	IP アドレス/マスクのフォーマットが間違っています	IP アドレス/マスクのフォーマットが間違っています。正しいフォーマットで入力してください。
4	IPv6 グローバルアドレスを入力してください	IPv6 アドレスに IPv6 リンクローカルアドレスが入力されています。IPv6 グローバルアドレスを入力してください。
5	MAC アドレスが入力されていません	MAC アドレスが入力されていません。MAC アドレスを入力してください。
6	MAC アドレスのフォーマットが間違っています	MAC アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
7	装置名称を入力してください	装置名称を入力してください。
8	存在しない装置名称です	存在しない装置名称です。
9	ポート番号を入力してください	ポート番号を入力してください。
10	既に削除済みのセグメントです	既に削除済みのセグメントです。
11	要求のパラメータに間違いがあるか、削除中の装置またはセグメントです	要求のパラメータに間違いがあるか、削除中の装置またはセグメントです。「6.1.8(6) メンテナンス」により保守情報を収集してください。
12	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (2) セグメント詳細

図 6-44 セグメント詳細画面

図 6-44 セグメント詳細画面は、AX-Security-Controller(Manager)のWebインターフェースで表示されるセグメント詳細画面です。以下の各部が赤い枠で示されています。

- ① パンくじ:** トップ > 共通 > セグメント詳細 (セグメント1)
- ② セグメント情報:**

優先度	2001
状態	設定済み
コメント	
- ③ セグメント定義:**

表示カラム切替	25 ▼ 件表示	④	⑤ 検索
種別 ^		条件	
IPサブネット		IP:192.168.10.0/24	
- ⑥ ページナビゲーション:** 前のページ | 1 | 次のページ
- ⑦ 端末一覧:**

表示カラム切替	25 ▼ 件表示	⑨	⑩ 検索					
IPアドレス	MACアドレス	ペンダ	接続先 装置	ポート 番号	ポート エイリ アス	VLAN ID	操作	セキュ リティ フィル タ適用 状態
192.168.10.1	0000.5e00.5351	ICANN, IANA Department	エッジ スイッ チ1	0/7	None	200	通信遮断	
- ⑧ ページナビゲーション:** 前のページ | 1 | 次のページ
- ⑨ ルール一覧:**

表示	⑬															
表示カラム切替	25 ▼ 件表示	⑮	⑯ 検索													
クラ イア ント ^	優 先 度	条件1種 別	条件 1値	条件2 種別	条件2値	条件3種 別	条件3 値	条件4 種別	条件4 値	条件5 種別	条件5 値	条件6 種別	条件6 値	条件7 種別	条件7 値	送 信元 指定
Syslog	10	Signature	virus	Name	THREAT	Severity	5									
- ⑭ ページナビゲーション:** 前のページ | 1 | 次のページ
- ⑮ ルール一覧:**

表示	⑬															
表示カラム切替	25 ▼ 件表示	⑮	⑯ 検索													
クラ イア ント ^	優 先 度	条件1種 別	条件 1値	条件2 種別	条件2 値	条件3種 別	条件3 値	条件4 種別	条件4 値	条件5 種別	条件5 値	条件6 種別	条件6 値	条件7 種別	条件7 値	送 信元 指定
Syslog	10	Signature	virus	Name	THREAT	Severity	5									
- ⑯ ページナビゲーション:** 前のページ | 1 | 次のページ
- ⑰ ルール一覧:**

表示	⑬															
表示カラム切替	25 ▼ 件表示	⑮	⑯ 検索													
クラ イア ント ^	優 先 度	条件1種 別	条件 1値	条件2 種別	条件2 値	条件3種 別	条件3 値	条件4 種別	条件4 値	条件5 種別	条件5 値	条件6 種別	条件6 値	条件7 種別	条件7 値	送 信元 指定
Syslog	10	Signature	virus	Name	THREAT	Severity	5									
- ⑱ ページナビゲーション:** 前のページ | 1 | 次のページ

表 6-56 セグメント詳細画面に表示する項目

項目番号	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	セグメント情報	優先度/状態/コメント	セグメント情報として、登録済みの優先度/状態/コメントを表示します。
③	セグメント定義	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
④		ページあたり表示件数切替 プルダウン	1ページあたりに表示する件数を切り替えることができます。件数のパターンは10/25/50/100/全ての5パターンです。
⑤		検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑥		セグメント定義情報	セグメント定義情報の一覧を表示します。表示項目は、種別/条件です。
⑦		ページ切替ボタン	ボタンを押下すると、指定のページを表示します。
⑧	端末一覧	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑨		ページあたり表示件数切替 プルダウン	1ページあたりに表示する件数を切り替えることができます。件数のパターンは10/25/50/100/全ての5パターンです。
⑩		検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑪	端末一覧	収集した情報から端末の一覧を表示します。表示項目は、端末のIPアドレス/MACアドレス/ベンダ/エイリアス*/接続先装置/ポート番号/ポートエイリアス/VLAN ID/操作/セキュリティフィルタ適用状態/接続先APです。 接続先装置の装置モデルが標準MIB対応装置かつMIBオブジェクト(MACアドレス)がdot1dTpFdbPortの場合、VLAN IDは空文字列です。 操作は、通信遮断、または通信遮断解除・セキュリティフィルタ解除ボタンが表示され、以下に示す動作をおこないます。なお、信頼済みセグメントに所属している場合、ボタンを押下することはできません。	

項目番号	内容	説明
		<ul style="list-style-type: none"> <li>「通信遮断」ボタンを押下すると、 端末 MAC アドレス &lt;MAC アドレス&gt; を通信遮断します</li> </ul> <p>の確認ダイアログを表示します。了承した場合、セキュリティフィルタの通信遮断を適用します。反映が失敗すると、「表 6-4 通信遮断の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p> <ul style="list-style-type: none"> <li>「通信遮断解除」ボタンを押下すると、 端末 MAC アドレス &lt;MAC アドレス&gt; のセキュリティフィルタの通信遮断を解除します</li> </ul> <p>の確認ダイアログを表示します。了承した場合、該当する端末に適用しているすべてのセキュリティフィルタの通信遮断を解除します。 反映が失敗すると、「表 6-5 通信遮断解除の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p> <ul style="list-style-type: none"> <li>「セキュリティフィルタ解除」ボタンを押下すると、 端末 MAC アドレス &lt;MAC アドレス&gt; のセキュリティフィルタを一括解除します</li> </ul> <p>の確認ダイアログを表示します。了承した場合、該当する端末に適用しているすべてのセキュリティフィルタを解除します。 反映が失敗すると、「表 6-6 セキュリティフィルタ解除の反映失敗時のダイアログ一覧」に示すダイアログを表示します。 セキュリティフィルタ適用状態は、該当する端末に適用しているセキュリティフィルタの一覧をボタンで表示します。ボタンを押下すると、「6.1.6(2) セキュリティフィルタ詳細」に移動します。</p>
⑫	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。
⑬	ルール	表示ボタン ボタンを押下すると、ルールのエントリー一覧を展開表示します。 もう一度ボタンを押下すると、ルールのエントリー一覧の表示を折りたたみます。
⑭		表示カラム切替ボタン 一覧から不要なカラムを非表示にすることができます。

項目番号	内容	説明
⑯	ページあたり表示件数切替 プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑰	検索テキスト ボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑱	ルール情報	ルール情報の一覧を表示します。 表示項目は、優先度/条件 1 種別/条件 1 値/ 条件 2 種別/条件 2 値/条件 3 種別/条件 3 値/ 条件 4 種別/条件 4 値/条件 5 種別/条件 5 値/条件 6 種別/条件 6 値/送信元指定/宛先 指定/アクションです。
⑲	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

注※

「6.1.3(2)(a), 6.1.3(2)(c)」で 1 つ以上のエイリアスの設定をおこなった場合、複数のタイトルカラムに展開して表示します。タイトルカラムと、端末に対応する「6.1.3(2) エイリアス」のタイトルが一致しない場合、値には None を表示します。

## 6.1.6 セキュリティ装置連携

### (1) セキュリティフィルター一覧

図 6-45 セキュリティフィルター一覧画面

The screenshot shows the 'セキュリティフィルター一覧' (Security Filter List) page. The interface includes:

- Header:** ブラウザのアドレスバーに「トップ > 共通 > セキュリティフィルター一覧」が表示されている。(1)
- Buttons:** 「セキュリティフィルタ追加」(2), 「CSV形式で保存」(3), 「CSV形式からのセキュリティフィルタ追加」(4), 「選択セキュリティフィルタの解除」(5).
- Search and Filters:** 「表示カラム切替」(6), 「件表示」(7) (25件), 「検索」(8).
- Table:** テーブルには以下のデータが表示されています。(9) チェックボックス, (10) 登録日時, 種別, セキュリティフィルタ条件, 状態, 連携機能.
 

登録日時	種別	セキュリティフィルタ条件	状態	連携機能
2018/11/05 18:42:53 JST	詳細ミラー	送信元:198.51.100.62/32宛 先:0.0.0.0/0	設定済み	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
2018/11/05 18:41:45 JST	通信遮断	送信元:198.51.100.61/32宛 先:0.0.0.0/0	設定済み	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
2018/11/05 18:33:47 JST	通信遮断	送信元:198.51.100.54/32宛 先:0.0.0.0/0	設定済み	TMPM連携
2018/11/05 18:33:07 JST	通信遮断	送信元:198.51.100.53/32宛 先:198.51.100.202/32	設定済み	TMPM連携
2018/11/05 18:31:38 JST	例外通信許可	送信元:198.51.100.52/32宛 先:198.51.100.201/32	設定済み	TMPM連携
2018/11/05 18:29:17 JST	詳細ミラー	送信元:198.51.100.51/32宛 先:0.0.0.0/0	設定済み	TMPM連携
- Pagination:** 「6件中 1 から 6 まで表示」, 「前のページ」(12), 「次のページ」.

表 6-57 セキュリティフィルター一覧画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	セキュリティフィルタ追加ボタン	新規にセキュリティフィルタを追加します。ボタンを押下すると「(a) セキュリティフィルタ追加」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「actions.csv」となります。
④	CSV 形式からのセキュリティフィルタ追加	ボタンを押下すると、CSV 形式のファイルから 1 個以上のセキュリティフィルタを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。

項目番号	内容	説明
⑤	選択セキュリティフィルタの解除ボタン	ボタンを押下すると、選択したセキュリティフィルタを解除します(<チェック数>件)。セキュリティフィルタが解除されるまで時間がかかる場合があります。の確認ダイアログを表示します。了承した場合、実行する場合は YES と入力してください。の確認ダイアログを表示します。YES を入力して了承した場合、選択した個別選択チェックボックスのセキュリティフィルタ*について、セキュリティフィルタを解除します。反映が失敗すると、「表 6-58 選択セキュリティフィルタ解除の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑥	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑦	ページあたり表示件数切替プルダウントラッパー	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑧	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑨	全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべてのセキュリティフィルタをセキュリティフィルタ解除対象とします。もう一度選択すると、すべてのセキュリティフィルタ解除対象から外します。
⑩	個別選択チェックボックス	選択したセキュリティフィルタをセキュリティフィルタ解除対象とします。もう一度選択すると、セキュリティフィルタ解除対象から外します。
⑪	セキュリティフィルタ情報	セキュリティフィルタ情報の一覧を表示します。表示項目は、登録日時/種別/セキュリティフィルタ条件/状態/連携機能/遮断理由/要求元 IP アドレスです。 種別： 「表 1-29 種別」参照 状態： 「表 1-30 設定状態」参照 セキュリティフィルタのエントリを押下すると、「(2) セキュリティフィルタ詳細」に移動します。
⑫	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

## 注※

任意のセキュリティフィルタの個別選択チェックボックスが選択された状態で、検索テキストボックスで絞り込みをおこない、該当セキュリティフィルタが表示されない場合でも、該当セキュリティフィルタはセキュリティフィルタ解除対象のままです。この状態でボタンを押下すると、該当セキュリティフィルタのセ

セキュリティフィルタ解除が実施されることに注意してください。

個別選択チェックボックスの選択は、検索テキストボックスで絞り込みをおこなった後におこなうようにしてください。

表 6-58 選択セキュリティフィルタ解除の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	セキュリティフィルタが選択されていません	セキュリティフィルタが選択されていません。個別選択チェックボックスを1つ以上選択してください。
2	選択可能なセキュリティフィルタは最大50000件です	選択可能なセキュリティフィルタは最大50000件です。選択した個別選択チェックボックスを見直してください。
3	要求パラメータに間違があります	要求のパラメータに間違があります。「6.1.8(6)メンテナンス」により保守情報を収集してください。
4	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

### (a) セキュリティフィルタ追加

図 6-46 セキュリティフィルタ追加画面

表 6-59 セキュリティフィルタ追加画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。

項目番号	内容	説明
②	送信元	<p>セキュリティフィルタの条件として、送信元を入力します。入力パターンは以下のいずれかとなります。</p> <ul style="list-style-type: none"> <li>送信元 IPv4 アドレスとマスクをスラッシュ(/)文字で連結</li> <li>送信元 IPv6 アドレスとプレフィックス長をスラッシュ(/)文字で連結</li> <li>送信元 MAC アドレス</li> </ul> <p>送信元 IPv4 アドレスは 0.0.0.0～255.255.255.255、マスクは 0～32 を入力してください。</p> <p>送信元 IPv6 アドレスは::～ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff、プレフィックス長は 0～128 を入力してください。</p> <p>送信元 MAC アドレスは 0000.0000.0000～ffff.ffff.ffff を入力してください。</p>
③	宛先	<p>セキュリティフィルタの条件として、宛先を入力します。入力パターンは以下のいずれかとなります。</p> <ul style="list-style-type: none"> <li>送信元が IPv4 アドレスの場合、宛先 IPv4 アドレスとマスクをスラッシュ(/)文字で連結</li> <li>送信元が IPv6 アドレスの場合、宛先 IPv6 アドレスとプレフィックス長をスラッシュ(/)文字で連結</li> </ul> <p>宛先 IPv4 アドレスは 0.0.0.0～255.255.255.255、マスクは 0～32 を入力してください。</p> <p>宛先 IPv6 アドレスは::～ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff、プレフィックス長は 0～128 を入力してください。</p>
④	種類プルダウン	セキュリティフィルタの種別を選択します。以下のいずれかです。
⑤	追加ボタン	セキュリティフィルタ追加を反映します。ボタンを押下し、反映が成功すると、「(1) セキュリティフィルター一覧」に移動します。反映が失敗すると、「表 6-60 セキュリティフィルタ追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑥	キャンセルボタン	セキュリティフィルタ追加をキャンセルします。ボタンを押下すると、「(1) セキュリティフィルター一覧」に移動します。

表 6-60 セキュリティフィルタ追加の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	送信元 IP アドレス/マスクまたは送信元 MAC アドレスが入力されていません	送信元 IP アドレス/マスク、または送信元 MAC アドレスが入力されていません。送信元 IP アドレス/マスク、または送信元 MAC アドレスを入力してください。

項目番号	内容	説明
2	送信元 IP アドレス/マスクまたは送信元 MAC アドレスのフォーマットが間違っています	送信元 IP アドレス/マスク、または送信元 MAC アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
3	送信元 IPv6 アドレスに IPv6 グローバルアドレスを入力してください	送信元 IPv6 アドレスに IPv6 リンクローカルアドレスが入力されています。IPv6 グローバルアドレスを入力してください。
4	宛先 IP アドレス/マスクが入力されていません	宛先 IP アドレス/マスクが入力されていません。宛先 IP アドレス/マスクを入力してください。
5	宛先 IP アドレス/マスクのフォーマットが間違っています	宛先 IP アドレス/マスクのフォーマットが間違っています。正しいフォーマットで入力してください。
6	宛先 IPv6 アドレスに IPv6 グローバルアドレスを入力してください	宛先 IPv6 アドレスに IPv6 リンクローカルアドレスが入力されています。IPv6 グローバルアドレスを入力してください。
7	要求パラメータに間違いがあります	要求のパラメータに間違いがあります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
8	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (2) セキュリティフィルタ詳細

図 6-47 セキュリティフィルタ詳細画面

① 頭部ナビゲーション: トップ > 共通 > セキュリティフィルタ一覧 > 送信元IP:10.0.10.53/32宛先IP:0.0.0.0/0通信遮断

② ヘッダー: セキュリティフィルタ詳細

③ フィルタ情報欄: 登録日時 2018/05/15 11:36:05 JST、状態 設定済み、連携機能 バロアルトネットワークス 次世代ファイアウォール連携、遮断理由 場所元IPアドレス 172.17.0.100、セキュリティフィルタ条件 送信元IP:10.0.10.53/32宛先IP:0.0.0.0/0、種別 通信遮断(スケジュール解除 有効)、無効化ボタン

④ フィルタ条件欄: 送信元IP:10.0.10.53/32宛先IP:0.0.0.0/0

⑤ 端末情報欄: 端末MACアドレス 0000.5e00.5353[ICANN, IANA Department]

⑥ コンフィグ内容: 表示カラム切替、件数表示 (25)、件数表示 (7)

⑦ 検索欄: 検索: [入力欄]

⑧ テーブルヘッダー: 設定対象 (ドロップダウン)、ポート番号、装置名、検出方向、シーケンス番号、検出条件、追加状態、要因、登録日時、適用日時、コンフィグ要因、削除要因、削除日時

設定対象	ポート番号	装置名	検出方向	シーケンス番号	検出条件	追加状態	要因	登録日時	適用日時	コンフィグ要因	削除要因	削除日時
端末接続ポート	10.0.10.53	エンドツイジスポート	受信側	300000	deny ip host any	設定済み	セキュリティ	2018/05/15 11:36:07	2018/05/15 11:36:19	テイフイルタ追加		

⑨ テーブル内: 1件中 1 から 1 まで表示

⑩ ページナビゲーション: 前のページ、1、次のページ

表 6-61 セキュリティフィルタ詳細画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。

項目番	内容	説明
②	セキュリティフィルタ削除ボタン	<p>セキュリティフィルタを削除します。ボタンを押下すると、IP アドレス指定のセキュリティフィルタの場合</p> <p>セキュリティフィルタ &lt;送信元 IP アドレス/マスク&gt;&lt;宛先 IP アドレス/マスク&gt;&lt;種別&gt; を削除します</p> <p>の確認ダイアログを表示します。 MAC アドレス指定のセキュリティフィルタの場合</p> <p>セキュリティフィルタ &lt;送信元 MAC アドレス&gt;&lt;種別&gt; を削除します</p> <p>の確認ダイアログを表示します。 了承した場合、セキュリティフィルタを削除し、「(1) セキュリティフィルター一覧」に移動します。削除が失敗すると、「表 6-62 セキュリティフィルタ詳細の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p>
③	セキュリティフィルタ情報	<p>セキュリティフィルタ情報として、登録日時/状態/連携機能/遮断理由/要求元 IP アドレス/セキュリティフィルタ条件/種別を表示します。</p> <p>種別が通信遮断(スケジュール解除)、または詳細ミラー(スケジュール解除)の場合、状態により以下を表示します。</p> <ul style="list-style-type: none"> <li>・状態有効時： 通信遮断(スケジュール解除 有効) 詳細ミラー(スケジュール解除 有効)</li> <li>・状態無効時： 通信遮断(スケジュール解除 無効) 詳細ミラー(スケジュール解除 無効)</li> </ul>

項目番号	内容	説明
④	無効化ボタン/有効化ボタン	<p>種別が通信遮断(スケジュール解除), または詳細ミラー(スケジュール解除)の場合に表示します。スケジュール解除の状態が有効時は無効化ボタンを表示し, 状態が無効時は有効化ボタンを表示します。</p> <p>無効化ボタンを押下すると, IP アドレス指定のセキュリティフィルタの場合</p> <p>セキュリティフィルタ &lt;送信元 IP アドレス/マスク&gt;&lt;宛先 IP アドレス/マスク&gt;&lt;種別&gt; のスケジュール解除を無効にします</p> <p>の確認ダイアログを表示します。 MAC アドレス指定のセキュリティフィルタの場合</p> <p>セキュリティフィルタ &lt;送信元 MAC アドレス&gt;&lt;種別&gt; のスケジュール解除を無効にします</p> <p>の確認ダイアログを表示します。 了承した場合, スケジュール解除の状態を無効にします。スケジュール解除の無効化が失敗すると, 「表 6-63 セキュリティフィルタ詳細のスケジュール解除無効反映失敗時のダイアログ一覧」に示すダイアログを表示します。 有効化ボタンを押下すると, IP アドレス指定のセキュリティフィルタの場合</p> <p>セキュリティフィルタ &lt;送信元 IP アドレス/マスク&gt;&lt;宛先 IP アドレス/マスク&gt;&lt;種別&gt; のスケジュール解除を有効にします</p> <p>の確認ダイアログを表示します。 MAC アドレス指定のセキュリティフィルタの場合</p> <p>セキュリティフィルタ &lt;送信元 MAC アドレス&gt;&lt;種別&gt; のスケジュール解除を有効にします</p> <p>の確認ダイアログを表示します。 了承した場合, スケジュール解除の状態を有効にします。スケジュール解除の有効化が失敗すると, 「表 6-64 セキュリティフィルタ詳細のスケジュール解除有効反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p>

項目番号	内容		説明
⑤	端末情報		端末情報として、端末 MAC アドレスを表示します。MAC アドレスベンダが表示可能な場合、[]に MAC アドレスベンダを表示します。
⑥	コンフィグ 内容		一覧から不要なカラムを非表示にすることができます。
⑦	ページあたり表示件数 切替プルダウン		1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑧	検索テキストボックス		テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑨	コンフィグ 情報		<p>コンフィグ情報の一覧を表示します。          表示項目は、設定対象/端末 IP アドレス/装置名称/          ポート番号/アクセスリスト名称/検出方向/シーク          エンス番号/検出条件/コンフィグ設定状態/追加要因/          登録日時/コンフィグ適用日時/削除要因/コンフィ          グ解除日時です。</p> <p>設定対象：          端末接続ポート/WAN 接続ポート/ミラー先ポート/          永続設定ポート(受信側)/永続設定ポート(送信側)</p> <p>検出方向：          受信側/送信側</p> <p>コンフィグ設定状態：          「表 1-31 コンフィグ設定状態」参照</p> <p>追加要因：          セキュリティフィルタ追加/ポート移動/IP アド          レス変更/WAN 接続ポート追加/ミラー先ポート追          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/信頼済み</p> <p>削除要因：          セキュリティフィルタ削除/エージアウト/ポート          移動/WAN 接続ポート削除/ミラー先ポート削          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/未サポート種別/アクセスリスト適          用失敗/装置削除/ライセンス無効/メンテナンス          實施/セキュリティフィルタ追加失敗/WAN 接          続ポート削除失敗/ミラー先ポート削除失敗/永          続設定ポート(受信側)削除失敗/永續設定ポート          (送信側)削除失敗/信頼済みセグメント定義追加/          信頼済みセグメント定義削除</p>
⑩	ページ切替 ボタン		ボタンを押下すると、指定のページを表示します。

表 6-62 セキュリティフィルタ詳細の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みのセキュリティフィルタです。	既に削除済みのセキュリティフィルタです。
2	指定したセキュリティフィルタが存在しません。	指定したセキュリティフィルタが存在しません。
3	データベースのアクセスに失敗しました。	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

表 6-63 セキュリティフィルタ詳細のスケジュール解除無効反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みのセキュリティフィルタです。	既に削除済みのセキュリティフィルタです。
2	指定したセキュリティフィルタが存在しません。	指定したセキュリティフィルタが存在しません。
3	データベースのアクセスに失敗しました。	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

表 6-64 セキュリティフィルタ詳細のスケジュール解除有効反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みのセキュリティフィルタです。	既に削除済みのセキュリティフィルタです。
2	指定したセキュリティフィルタが存在しません。	指定したセキュリティフィルタが存在しません。
3	データベースのアクセスに失敗しました。	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (3) セキュリティフィルタ履歴

図 6-48 セキュリティフィルタ履歴画面

① 階層リンク  
② 履歴の削除  
③ CSV形式で保存  
④ 表示カラム切替  
⑤ ページあたり表示件数切替  
⑥ 検索  
⑦ セキュリティフィルタ情報  
⑧ ページ切替ボタン

登録日時	種別	セキュリティフィルタ条件	状態	連携機能	由	要件ID
2017/09/12 13:20:42 JST	通信遮断	送信元IP:10.0.10.101/32宛先 IP:0.0.0.0/0	設定削除済み	TMMP連携		10.200.0.250
2017/09/12 13:20:42 JST	通信遮断	送信元IP:0.0.0.0/0宛先 IP:198.51.100.222/32	設定削除済み	TMMP連携		10.200.0.250
2017/09/12 13:20:42 JST	例外通信許可	送信元IP:10.0.10.101/32宛先 IP:172.16.0.44/32	設定削除済み	TMMP連携		10.200.0.250
2017/09/12 13:20:42 JST	詳細ミラ一	送信元IP:10.0.10.102/32宛先 IP:0.0.0.0/0	設定削除済み	TMMP連携		10.200.0.250
2017/09/12 13:22:33 JST	通信遮断	送信元IP:10.0.10.108/32宛先 IP:0.0.0.0/0	設定削除済み	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		10.200.0.195

5件中1から5まで表示

表 6-65 セキュリティフィルタ履歴画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	履歴の削除ボタン	セキュリティフィルタ履歴を削除します。ボタンを押下すると「(a)セキュリティフィルタ履歴削除」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「actions_history.csv」になります。
④	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑤	ページあたり表示件数切替プルダウン	1ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑥	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑦	セキュリティフィルタ情報	セキュリティフィルタ情報を表示します。 表示項目は、「表 6-57 セキュリティフィルタ一覧画面に表示する項目」のセキュリティフィルタ情報を参照してください。 セキュリティフィルタのエントリを押下すると、「(4) セキュリティフィルタ詳細(履歴)」に移動します。
⑧	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

## (a) セキュリティフィルタ履歴削除

図 6-49 セキュリティフィルタ履歴削除画面

①

セキュリティフィルタ履歴削除

削除期間入力

開始日時

日	月	火	水	木	金	土
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

00 : 00

終了日時

日	月	火	水	木	金	土
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

23 : 59

削除 キャンセル

② ③ ④

表 6-66 セキュリティフィルタ履歴削除画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	削除期間	削除対象とする期間の開始日時と終了日時を指定します。本日の午前 0 時 0 分から午後 11 時 59 分までが自動で指定されています。

項番	内容	説明
③	削除ボタン	<p>セキュリティフィルタ履歴の削除を反映します。ボタンを押下すると、          &lt;開始日時&gt; から &lt;終了日時&gt; までの          セキュリティフィルタ履歴を削除します</p> <p>の確認ダイアログを表示します。          了承した場合、反映が成功すると、「(3)セキュリティフィルタ履歴」に移動します。反映が失敗すると、「表 6-67 セキュリティフィルタ履歴削除の反映失敗時のダイアログ一覧」に示すダイアログを表示します。履歴を削除すると元に戻せないため、セキュリティフィルタ履歴を CSV 形式で保存してからの実行をおすすめします。</p>
④	キャンセルボタン	履歴の削除をキャンセルします。ボタンを押下すると、「(3)セキュリティフィルタ履歴」に移動します。

表 6-67 セキュリティフィルタ履歴削除の反映失敗時のダイアログ一覧

項番	内容	説明
1	開始日または終了日が入力されていません。	開始日または終了日が入力されていません。
2	要求パラメータに間違이があります	開始日または終了日のフォーマットに間違いがあります。
3	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (4) セキュリティフィルタ詳細(履歴)

図 6-50 セキュリティフィルタ詳細画面

セキュリティフィルタ詳細

セキュリティフィルタ情報											
登録日時	2018/04/23 16:04:35 JST										
状態	設定削除済み										
連携機能	TPMP連携										
遮断理由											
要求元IPアドレス	10.215.217.148										
セキュリティフィルタ条件	送信元IP:10.0.10.53/32宛先IP:0.0.0.0/0通信遮断										
種別	通信遮断										
端末情報	0000.5e00.5353[ICANN, IANA Department]										

コンフィグ内容

表示カラム切替	④	25	件表示	⑤	⑥	検索:					
設定	ポ	検	シーケ	設定	追	削					
対象	装	出	ンス番	加	加	除					
端末IPア	一	方	号	要	用	要					
接続	ト	向	検出条件	態	日時	用					
ポート	番	号	受け取る	因	登録日時	日時					
	名	名	IPアドレス	登録	適用日時	解除日時					
	称	号	名称	日時		削除日時					
端末	10.0.10.53	工	AUTO_ACL_IPV4_IN_0_1	受	300000	deny ip	削除	セ	2018/04/23	2018/04/23	セ
接続	ツ	0/1		信		host	キ	16:04:37	16:04:49	キ	16:15:17
ポート	ジ			側		10.0.10.53	ユ	JST	JST	ユ	JST
	ス					any	リ			リ	
	イ						テ			テ	
	イ						フ			フ	
	チ						イ			イ	
							ル			ル	
							タ			タ	
							追			削	
							加			除	

1件中 1 から 1 まで表示

⑧ 前のページ 1 次のページ

表 6-68 セキュリティフィルタ詳細画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	セキュリティフィルタ情報	セキュリティフィルタ情報表示項目は、「表 6-61 セキュリティフィルタ詳細画面に表示する項目」のセキュリティフィルタ情報を参照してください。
③	端末情報	端末情報として、端末 MAC アドレスを表示します。および、[]内に MAC アドレスペンドラを表示します。
④	コンフィグ内容 表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。

項目番号	内容	説明
⑤	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑥	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑦	コンフィグ情報	<p>コンフィグ情報の一覧を表示します。          表示項目は、設定対象/端末 IP アドレス/装置名称/          ポート番号/アクセスリスト名称/検出方向/シーケ          ンス番号/検出条件/コンフィグ設定状態/追加要因/          登録日時/コンフィグ適用日時/削除要因/コンフィ          グ解除日時です。</p> <p>設定対象：          端末接続ポート/WAN 接続ポート/ミラー先ポート/          永続設定ポート(受信側)/永続設定ポート(送信側)</p> <p>検出方向：          受信側/送信側</p> <p>コンフィグ設定状態：          「表 1-31 コンフィグ設定状態」参照</p> <p>追加要因：          セキュリティフィルタ追加/ポート移動/IP アド          レス変更/WAN 接続ポート追加/ミラー先ポート          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</p> <p>削除要因：          セキュリティフィルタ削除/エージアウト/ポート          移動/WAN 接続ポート削除/ミラー先ポート          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/未サポート種別/アクセスリスト          適用失敗/装置削除/ライセンス無効/メンテナン          ス実施/セキュリティフィルタ追加失敗/WAN          接続ポート削除失敗/ミラー先ポート削除失敗/          永続設定ポート(受信側)削除失敗/永続設定ポート          (送信側)削除失敗</p>
⑧	ページ切替ボタン	ボタンを押下すると、指定のページを表示しま す。

## (5) ルールマッチ履歴

図 6-51 ルールマッチ履歴画面

① 階層リンク  
② 履歴の削除  
③ CSV形式で保存  
④ 表示カラム切替  
⑤ ページあたり表示件数切替プルダウン  
⑥ 検索  
⑦ ボタン  
⑧ ページナビゲーション

受信日時	クライアント名称	クライアント種別	優先度	アクション種別	送信元指定	宛先指定	セキュリティフィルタ条件	ログ	操作
2017/09/12 13:19:50 JST	ファイアウォール	パロアルトネットワークス 次世代ファイアウォール	60	手動選択				<a href="#">表示</a>	<a href="#">確認済み</a>
2017/09/12 13:19:53 JST	ファイアウォール	パロアルトネットワークス 次世代ファイアウォール	50	手動選択	<a href="#">セキュリティフィルタ詳細</a>	<a href="#">詳細ミラー確認済み</a>	<a href="#">確認済み解除</a>	<a href="#">表示</a>	<a href="#">詳細ミラー</a>
2017/09/12 13:19:55 JST	ファイアウォール	パロアルトネットワークス 次世代ファイアウォール	30	詳細ミラー	dst	送信元IP:10.0.10.109/32 宛先IP:0.0.0.0/0 詳細ミラー	<a href="#">セキュリティフィルタ詳細</a>	<a href="#">表示</a>	<a href="#">詳細ミラー解除</a>
2017/09/12 13:19:58 JST	ファイアウォール	パロアルトネットワークス 次世代ファイアウォール	10	通信遮断	dst	送信元IP:10.0.10.109/32 宛先IP:0.0.0.0/0 通信遮断	<a href="#">セキュリティフィルタ詳細</a>	<a href="#">表示</a>	<a href="#">通信遮断解除</a>
2017/09/12 13:22:12 JST	ファイアウォール	パロアルトネットワークス 次世代ファイアウォール	50	手動選択			<a href="#">セキュリティフィルタ詳細</a>	<a href="#">表示</a>	<a href="#">通信遮断解除済み</a>

表 6-69 ルールマッチ履歴画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	履歴の削除ボタン	ルールマッチ履歴を削除します。ボタンを押下すると「(c)ルールマッチ履歴削除」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「actions_match.csv」になります。
④	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑤	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑥	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。

項目番号	内容	説明
⑦	ルールマッチ情報	<p>ルールマッチ情報の一覧を表示します。 表示項目は、受信日時/クライアント名称/クライアント種別/優先度/送信元指定/宛先指定/セキュリティフィルタ条件/セキュリティフィルタ状態/ログ/操作です。</p> <p>「ログ」ボタンを押下すると、受信した Syslog メッセージを表示します。再度押下すると、Syslog メッセージの表示を隠します。</p> <p>操作には各種ボタンが表示され、以下に示す動作をします。</p> <ul style="list-style-type: none"> <li>・「通信遮断」ボタンを押下すると「(a) 通信遮断設定」に示すダイアログを表示します。</li> <li>・「詳細ミラー」ボタンを押下すると「(b) 詳細ミラー設定」に示すダイアログを表示します。</li> <li>・「セキュリティフィルタ詳細」ボタンを押下すると「(2) セキュリティフィルタ詳細」または「(4) セキュリティフィルタ詳細(履歴)」に移動します。</li> <li>・「通信遮断解除」または「詳細ミラー解除」ボタンを押下すると、セキュリティフィルタを削除します。反映が失敗すると、「表 6-70 ルールマッチ履歴の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</li> <li>・「確認済み」ボタンを押下すると、「通信遮断」、「詳細ミラー」ボタンを無効化します。反映が失敗すると、「表 6-70 ルールマッチ履歴の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</li> <li>・「セキュリティフィルタ設定エラー」ボタンは、該当フィールドが Syslog に含まれていない、またはセキュリティフィルタに設定できない IP アドレスが選択された場合に表示します。</li> </ul>
⑧	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-70 ルールマッチ履歴の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みのセキュリティフィルタです	既に削除済みのセキュリティフィルタです。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) 通信遮断設定

図 6-52 通信遮断設定画面

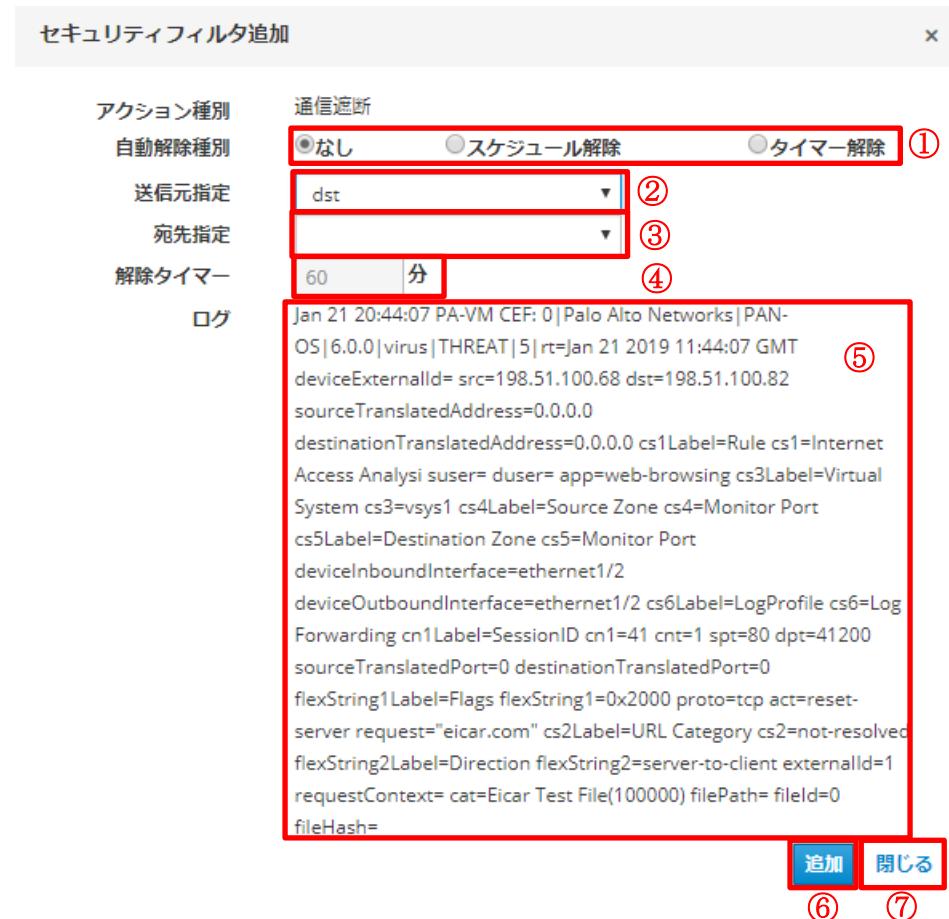


表 6-71 通信遮断設定画面に表示する項目

項目番	内容	説明
①	解除種別	解除種別を下記から選択します。 ・なし ・スケジュール解除 ・タイマー解除 スケジュール解除を選択してセキュリティフィルタを生成した場合、「6.1.8(1)(e) セキュリティフィルタ自動解除スケジュール追加」で設定した時刻にセキュリティフィルタが削除されます。 タイマー解除を選択してセキュリティフィルタを生成した場合、解除タイマーで設定した時間後にセキュリティフィルタが削除されます。

項目番号	内容	説明
②	送信元指定	通信遮断に使用する IP アドレス/MAC アドレスに、 Syslog の中の「src」, 「dst」, 「sourceTranslatedAddress」, 「destinationTranslatedAddress」, 「smac」, 「dmac」フィールドから選択して、送信元と宛先そ れぞれに指定します。
③	宛先指定	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、追加で 「PanOSXforwarderfor」フィールドも選択可能です。 および、ユーザ定義拡張フィールドとして、データ 型が「IPv4 Address」, 「IPv6 Address」, 「IPv4 Address or IPv6 Address」, または「MAC Address」で あるフィールドも選択可能です。 送信元指定にデータ型が「MAC Address」である フィールドを選択した場合、宛先指定は選択できま せん。
④	解除タイマー	解除種別がタイマー解除の場合、セキュリティフィ ルタ生成後に解除を実行するまでの時間(分)を指定しま す。 1~1440 が指定可能です。
⑤	ログ	受信した Syslog メッセージを表示します。
⑥	追加ボタン	通信遮断のセキュリティフィルタ追加を反映しま す。ボタンを押下し、反映が成功すると、「(5) ルー ルマッチ履歴」に移動します。反映が失敗すると、 「表 6-72 通信遮断設定の反映失敗時のダイアログ 一覧」に示すダイアログを表示します。
⑦	キャンセルボタン	セキュリティフィルタ追加をキャンセルします。ボ タンを押下すると、「(5) ルルマッチ履歴」に移動 します。

表 6-72 通信遮断設定の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	解除タイマーが入 力されていません	解除タイマーが入力されていません。
2	範囲外の解除タイ マーです	範囲外の解除タイマーです。
3	要求パラメータに 間違いがあります	指定されたフィールドがログに含まれていないか、 セキュリティフィルタを設定できない IP アドレス、 または MAC アドレスです。
4	データベースのア クセスに失敗しま した	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してくださ い。

## (b) 詳細ミラー設定

図 6-53 詳細ミラー設定画面



表 6-73 詳細ミラー設定画面に表示する項目

項目番号	内容	説明
①	解除種別	<p>解除種別を下記から選択します。</p> <ul style="list-style-type: none"> <li>・なし</li> <li>・スケジュール解除</li> <li>・タイマー解除</li> </ul> <p>スケジュール解除を選択してセキュリティフィルタを生成した場合、「6.1.8(1)(e) セキュリティフィルタ自動解除スケジュール追加」で設定した時刻にセキュリティフィルタが削除されます。</p> <p>タイマー解除を選択してセキュリティフィルタを生成した場合、解除タイマーで設定した時間後にセキュリティフィルタが削除されます。</p>

項目番号	内容	説明
②	送信元指定	詳細ミラーに使用する IP アドレス/MAC アドレスに、「Syslog」の中の「src」, 「dst」, 「sourceTranslatedAddress」, 「destinationTranslatedAddress」, 「smac」, 「dmac」フィールドから選択して、送信元に指定します。 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、追加で「PanOSXforwarderfor」フィールドも選択可能です。および、ユーザ定義拡張フィールドとして、データ型が「IPv4 Address」, 「IPv6 Address」, 「IPv4 Address or IPv6 Address」, または「MAC Address」であるフィールドも選択可能です。
③	解除タイマー	解除種別がタイマー解除の場合、セキュリティフィルタ生成後に解除を実行するまでの時間(分)を指定します。 1~1440 が指定可能です。
④	ログ	受信した Syslog メッセージを表示します。
⑤	追加ボタン	詳細ミラーのセキュリティフィルタ追加を反映します。ボタンを押下し、反映が成功すると、「(5) ルールマッチ履歴」に移動します。反映が失敗すると、「表 6-74 詳細ミラー設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑥	キャンセルボタン	セキュリティフィルタ追加をキャンセルします。ボタンを押下すると、「(5) ルールマッチ履歴」に移動します。

表 6-74 詳細ミラー設定の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	解除タイマーが入力されていません	解除タイマーが入力されていません。
2	範囲外の解除タイマーです	範囲外の解除タイマーです。
3	要求パラメータに間違があります	指定されたフィールドがログに含まれていないか、セキュリティフィルタを設定できない IP アドレス、または MAC アドレスです。
4	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (c) ルールマッチ履歴削除

図 6-54 ルールマッチ履歴削除画面

①

ルールマッチ履歴削除

削除期間入力

開始日時

日	月	火	水	木	金	土					
26	27	28	29	30	1	2					
3	4	5	6	7	8	9					
10	11	12	13	14	15	16					
17	18	19	20	21	22	23					
24	25	26	27	28	29	30					
31	1	2	3	4	5	6					

②

終了日時

日	月	火	水	木	金	土					
26	27	28	29	30	1	2					
3	4	5	6	7	8	9					
10	11	12	13	14	15	16					
17	18	19	20	21	22	23					
24	25	26	27	28	29	30					
31	1	2	3	4	5	6					

③ ④

削除 キャンセル

表 6-75 ルールマッチ履歴削除画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	削除期間	削除対象とする期間の開始日時と終了日時を指定します。本日の午前 0 時 0 分から午後 11 時 59 分までが自動で指定されています。

項目番号	内容	説明
③	削除ボタン	<p>ルールマッチ履歴の削除を反映します。ボタンを押下すると、      &lt;開始日時&gt; から &lt;終了日時&gt; までの      ルールマッチ履歴を削除します</p> <p>の確認ダイアログを表示します。      了承した場合、反映が成功すると、「(5)ルールマッチ履歴」に移動します。反映が失敗すると、「表      6-76 ルールマッチ履歴削除の反映失敗時のダイアログ一覧」に示すダイアログを表示します。履歴を      削除すると元に戻せないため、ルールマッチ履歴を CSV 形式で保存してからの実行をおすすめします。</p>
④	キャンセルボタン	履歴の削除をキャンセルします。ボタンを押下すると、「(5)ルールマッチ履歴」に移動します。

表 6-76 ルールマッチ履歴削除の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	開始日または終了日が入力されていません。	開始日または終了日が入力されていません。
2	要求パラメータに間違いがあります	開始日または終了日のフォーマットに間違いがあります。
3	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (6) Syslog 受信履歴

図 6-55 Syslog 受信履歴画面

① 階層のリンク

② 履歴の削除ボタン

③ CSV形式で保存ボタン

④ ページ数と件数表示

⑤ 検索入力欄

⑥ ログ詳細表示

⑦ ページナビゲーション

受信日時	内容
2017/09/12 13:19:50 JST	<15>CEF:0 Palo Alto Networks PAN-OS 7.1.0 virus THREAT 2 rt=Sep 12 2017 04:19:50 GMT deviceExternalId= src=198.51.100.111 dst=10.0.10.107 ア sourceTranslatedAddress=0.0.0.0 destinationTranslatedAddress=0.0.0.0 cs1Label=Rule user=Internet Access Analysis act=duser= app=web- イ browsing cs3Label=Virtual System cs3=vsys1 cs4Label=Source Zone cs4=Monitor Port cs5Label=Destination Zone cs5=Monitor Port ア deviceInboundInterface=ethernet1/2 deviceOutboundInterface=ethernet1/2 cs6Label=LogProfile cs6=Log Forwarding cn1Label=SessionID cn1=41 ウ cnt=1 spt=80 dpt=41200 sourceTranslatedPort=0 destinationTranslatedPort=0 flexString1Label=Flags flexString1=0x2000 proto=tcp act=reset-server オ request="eicar.com" cs2Label=URL Category flexString2Label=not-resolved act=Direction flexString2=server-to-client externalId=1 requestContext=cat=Eicar Test File(100000) filePath= fileId=0 fileHash= ル
2017/09/12 13:19:53 JST	<15>CEF:0 Palo Alto Networks PAN-OS 7.1.0 virus THREAT 3 rt=Sep 12 2017 04:19:53 GMT deviceExternalId= src=198.51.100.111 dst=10.0.10.108 ア sourceTranslatedAddress=0.0.0.0 destinationTranslatedAddress=0.0.0.0 cs1Label=Rule user=Internet Access Analysis act=duser= app=web- イ browsing cs3Label=Virtual System cs3=vsys1 cs4Label=Source Zone cs4=Monitor Port cs5Label=Destination Zone cs5=Monitor Port ア deviceInboundInterface=ethernet1/2 deviceOutboundInterface=ethernet1/2 cs6Label=LogProfile cs6=Log Forwarding cn1Label=SessionID cn1=41 ウ cnt=1 spt=80 dpt=41200 sourceTranslatedPort=0 destinationTranslatedPort=0 flexString1Label=Flags flexString1=0x2000 proto=tcp act=reset-server オ request="eicar.com" cs2Label=URL Category flexString2Label=not-resolved act=Direction flexString2=server-to-client externalId=1 requestContext=cat=Eicar Test File(100000) filePath= fileId=0 fileHash= ル
2017/09/12 13:19:55 JST	<15>CEF:0 Palo Alto Networks PAN-OS 7.1.0 virus THREAT 4 rt=Sep 12 2017 04:19:55 GMT deviceExternalId= src=198.51.100.111 dst=10.0.10.109 ア sourceTranslatedAddress=0.0.0.0 destinationTranslatedAddress=0.0.0.0 cs1Label=Rule user=Internet Access Analysis act=duser= app=web- イ browsing cs3Label=Virtual System cs3=vsys1 cs4Label=Source Zone cs4=Monitor Port cs5Label=Destination Zone cs5=Monitor Port ア deviceInboundInterface=ethernet1/2 deviceOutboundInterface=ethernet1/2 cs6Label=LogProfile cs6=Log Forwarding cn1Label=SessionID cn1=41 ウ cnt=1 spt=80 dpt=41200 sourceTranslatedPort=0 destinationTranslatedPort=0 flexString1Label=Flags flexString1=0x2000 proto=tcp act=reset-server オ request="eicar.com" cs2Label=URL Category flexString2Label=not-resolved act=Direction flexString2=server-to-client externalId=1 requestContext=cat=Eicar Test File(100000) filePath= fileId=0 fileHash= ル
2017/09/12 13:19:58 JST	<15>CEF:0 Palo Alto Networks PAN-OS 7.1.0 virus THREAT 5 rt=Sep 12 2017 04:19:58 GMT deviceExternalId= src=198.51.100.111 dst=10.0.10.109 ア sourceTranslatedAddress=0.0.0.0 destinationTranslatedAddress=0.0.0.0 cs1Label=Rule user=Internet Access Analysis act=duser= app=web- イ browsing cs3Label=Virtual System cs3=vsys1 cs4Label=Source Zone cs4=Monitor Port cs5Label=Destination Zone cs5=Monitor Port ア deviceInboundInterface=ethernet1/2 deviceOutboundInterface=ethernet1/2 cs6Label=LogProfile cs6=Log Forwarding cn1Label=SessionID cn1=41 ウ cnt=1 spt=80 dpt=41200 sourceTranslatedPort=0 destinationTranslatedPort=0 flexString1Label=Flags flexString1=0x2000 proto=tcp act=reset-server オ request="eicar.com" cs2Label=URL Category flexString2Label=not-resolved act=Direction flexString2=server-to-client externalId=1 requestContext=cat=Eicar Test File(100000) filePath= fileId=0 fileHash= ル
2017/09/12 13:22:12 JST	<15>CEF:0 Palo Alto Networks PAN-OS 7.1.0 virus THREAT 3 rt=Sep 12 2017 04:22:12 GMT deviceExternalId= src=198.51.100.111 dst=10.0.10.108 ア sourceTranslatedAddress=0.0.0.0 destinationTranslatedAddress=0.0.0.0 cs1Label=Rule user=Internet Access Analysis act=duser= app=web- イ browsing cs3Label=Virtual System cs3=vsys1 cs4Label=Source Zone cs4=Monitor Port cs5Label=Destination Zone cs5=Monitor Port ア deviceInboundInterface=ethernet1/2 deviceOutboundInterface=ethernet1/2 cs6Label=LogProfile cs6=Log Forwarding cn1Label=SessionID cn1=41 ウ cnt=1 spt=80 dpt=41200 sourceTranslatedPort=0 destinationTranslatedPort=0 flexString1Label=Flags flexString1=0x2000 proto=tcp act=reset-server オ request="eicar.com" cs2Label=URL Category flexString2Label=not-resolved act=Direction flexString2=server-to-client externalId=1 requestContext=cat=Eicar Test File(100000) filePath= fileId=0 fileHash= ル

5件中 1 から 5 まで表示

表 6-77 Syslog 受信履歴画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	履歴の削除ボタン	Syslog 受信履歴を削除します。ボタンを押下すると「(a)Syslog 受信履歴削除」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「syslogs.csv」となります。

項目番号	内容	説明
④	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑤	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑥	Syslog 情報	Syslog 情報の一覧を表示します。 表示項目は、受信日時/クライアント名称/ログです。
⑦	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

## (a) Syslog 受信履歴削除

図 6-56 Syslog 受信履歴削除画面

図 6-56 Syslog 受信履歴削除画面

①

②

③ 削除

④ キャンセル

表 6-78 Syslog 受信履歴削除画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	削除期間	削除対象とする期間の開始日時と終了日時を指定します。本日の午前 0 時 0 分から午後 11 時 59 分までが自動で指定されています。

項目番号	内容	説明
③	削除ボタン	Syslog 受信履歴の削除を反映します。ボタンを押下すると、 <開始日時> から <終了日時> までの Syslog 受信履歴を削除します  の確認ダイアログを表示します。 了承した場合、反映が成功すると、「(6)Syslog 受信 履歴」に移動します。反映が失敗すると、「表 6-79 Syslog 受信履歴削除の反映失敗時のダイアローグ 一覧」に示すダイアログを表示します。履歴を削除す ると元に戻せないため、Syslog 受信履歴を CSV 形式 で保存してからの実行をおすすめします。
④	キャンセルボタン	履歴の削除をキャンセルします。ボタンを押下する と、「(6)Syslog 受信履歴」に移動します。

表 6-79 Syslog 受信履歴削除の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	開始日または終了 日が入力されてい ません。	開始日または終了日が入力されていません。
2	要求パラメータに 間違いがあります	開始日または終了日のフォーマットに間違いがあ ります。
3	データベースのア クセスに失敗しま した	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してくださ い。

## (7) Syslog クライアント一覧

図 6-57 Syslog クライアント一覧画面

表 6-80 Syslog クライアント一覧画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	Syslog クライアント追加ボタン	新規に Syslog クライアントを追加します。ボタンを押下すると「(a)Syslog クライアント追加」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「actions_client.csv」となります。
④	CSV 形式からの Syslog クライアント追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上の Syslog クライアントを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑤	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑥	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑦	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑧	Syslog クライアント情報	Syslog クライアント情報の一覧を表示します。表示項目は、クライアント名称/IP アドレス/クライアント種別です。Syslog クライアントのエントリを押下すると、「(8)Syslog クライアント詳細」に移動します。
⑨	削除ボタン	操作として、Syslog クライアントの削除を行います。ボタンを押下すると、  Syslog クライアント <クライアント名称> を削除します  の確認ダイアログを表示します。了承した場合、 Syslog クライアントを削除します。削除が失敗すると、「表 6-81 Syslog クライアント一覧の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑩	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-81 Syslog クライアント一覧の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みの Syslog クライアントです	既に削除済みの Syslog クライアントです。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) Syslog クライアント追加

図 6-58 Syslog クライアント追加画面

表 6-82 Syslog クライアント追加画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	クライアント名称	クライアント情報としてクライアントの名称を示す文字列です。最大 256 文字登録可能です。なおアポストロフィ(')文字は使用しないでください。
③	IP アドレス	クライアントの IP アドレスを入力します。IP アドレスは 0.0.0.0～255.255.255.255 を入力してください。
④	クライアント種別	クライアントの種別を選択します。以下のいずれかが表示されますが、セキュリティ装置との連携ライセンスが有効な場合にのみ表示されます。 <ul style="list-style-type: none"> <li>・ パロアルトネットワークス 次世代ファイアウォール<sup>※1</sup></li> <li>・ Syslog 連携(CEF)</li> </ul>
⑤	追加ボタン	Syslog クライアント追加を反映します。ボタンを押下し、反映が成功すると、「(7)Syslog クライアント一覧」に移動します。反映が失敗すると、「表 6-83 Syslog クライアント追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑥	キャンセルボタン	Syslog クライアント追加をキャンセルします。ボタンを押下すると、「(7)Syslog クライアント一覧」に移動します。

表 6-83 Syslog クライアント追加の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	クライアント名称を入力してください	クライアント名称が入力されていません。クライアント名称を入力してください。
2	IP アドレスが入力されていません	IP アドレスが入力されていません。IP アドレスを入力してください。
3	IP アドレスのフォーマットが間違っています	IP アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
4	既に追加済みのクライアント名または IP アドレスです	既に追加済みのクライアント名または IP アドレスです。
5	Syslog クライアントが既に 10 個登録されています	Syslog クライアントが既に 10 個登録されています。
6	要求パラメータに間違いがあります	要求のパラメータに間違いがあります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
7	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

※1 :

クライアント種別「パロアルトネットワークス 次世代ファイアウォール」追加時、以下のルールを自動で設定します。

表 6-84 Syslog クライアント追加時に設定されるルール

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	THREAT	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	THREAT	手動選択	—	—
	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

## (8) Syslog クライアント詳細

図 6-59 Syslog クライアント詳細画面 (1/2)

セキュリティ装置 (IP:192.0.2.1)

クライアント情報

セグメント	偏先度	条件1種別	条件1値	条件2種別	条件2値	条件3種別	条件3値	送信元指定	アクション
無所属セグメント	5000	Name	CORRELATION					src	通信遮断
無所属セグメント	5100	Name	THREAT	Signature ID	spyware	flexString2	client-to-server	src	通信遮断
無所属セグメント	5200	Name	THREAT	Signature ID	spyware	flexString2	server-to-client	dst	通信遮断
無所属セグメント	5300	Name	THREAT	Signature ID	url	cs2	command-and-control	src	通信遮断
無所属セグメント	5400	Name	THREAT	Signature ID	wildfire	cs2	malicious		手動選択

操作: 削除 (11), 削除 (12), 削除 (13), 削除 (14), 削除 (15)

表示カラム切替 (7), 件表示 (8), 検索 (9)

ルール追加 (4), CSV形式で保存 (5), CSV形式からのルール追加 (6)

ナビゲーション: ページ数 (12), 前のページ, 次のページ

図 6-60 Syslog クライアント詳細画面 (2/2)

ユーザ定義拡張フィールド

ユーザ定義拡張フィールド追加 CSV形式で保存 CSV形式からのユーザ定義拡張フィールド追加

表示カラム切替 25 件表示 検索:

拡張フィールド名	データ型	操作
vendorSpecificKey1	String	<input type="button" value="削除"/> <input type="button" value="削除"/> <input type="button" value="削除"/>
vendorSpecificKey2	Integer	<input type="button" value="削除"/> <input type="button" value="削除"/> <input type="button" value="削除"/>
vendorSpecificKey3	IPv4 Address	<input type="button" value="削除"/> <input type="button" value="削除"/> <input type="button" value="削除"/>

3 件中 1 から 3 まで表示

前のページ 1 次のページ

表 6-85 Syslog クライアント詳細画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	クライアント情報	クライアント種別を表示します。
③	ルール	展開ボタン ボタンを押下すると、ルールのエントリ一覧表示を折りたたみます。 もう一度ボタンを押下すると、ルールのエントリ一覧を展開表示します。
④	ルール追加ボタン	新規にルールを追加します。ボタンを押下すると「(a)ルール追加」に移動します。
⑤	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「actions_client_rule.csv」となります。
⑥	CSV 形式からのルール追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上のルールを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑦	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑧	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑨	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。

項目番号	内容	説明
⑩	ルール情報	ルール情報の一覧を表示します。表示項目は、セグメント/優先度/条件 1 種別/条件 1 値/条件 2 種別/条件 2 値/条件 3 種別/条件 3 値/条件 4 種別/条件 4 値/条件 5 種別/条件 5 値/条件 6 種別/条件 6 値/送信元指定/宛先指定/アクション/解除タイマーです。
⑪		削除ボタン 操作として、ルールの削除を行います。ボタンを押下すると、 ルール <優先度> を削除します の確認ダイアログを表示します。了承した場合、ルールを削除します。削除が失敗すると、「表 6-86 ルールの削除反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑫		ページ切替ボタン ボタンを押下すると、指定のページを表示します。
⑬		ユーザ定義拡張フィールド 展開ボタン ボタンを押下すると、ユーザ定義拡張フィールドのエントリー一覧を展開表示します。 もう一度ボタンを押下すると、ユーザ定義拡張フィールドのエントリー一覧表示を折りたたみます。
⑭		ユーザ定義拡張フィールド 追加ボタン 新規にユーザ定義拡張フィールドを追加します。ボタンを押下すると「(b) ユーザ定義拡張フィールド追加」に移動します。
⑮		CSV 形式で保存ボタン ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「action_client_rule_extension.csv」となります。
⑯		CSV 形式からのユーザ定義拡張フィールド追加ボタン ボタンを押下すると、CSV 形式のファイルから 1 個以上のユーザ定義拡張フィールドを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑰		表示カラム切替ボタン 一覧から不要なカラムを非表示にすることができます。
⑱		ページあたり表示件数切替プルダウン 1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑲	検索テキストボックス テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。	

項目番号	内容	説明
⑩	ユーザ定義拡張フィールド情報	ユーザ定義拡張フィールド情報の一覧を表示します。 表示項目は、拡張フィールド名称/データ型です。
⑪	削除ボタン	操作として、ユーザ定義拡張フィールドの削除を行います。ボタンを押下すると、「表 1-18 インシデント抽出に指定可能なフィールド」および「表 1-19 インシデント抽出に追加で指定可能なフィールド (Syslog クライアントの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連携の場合)」に記載の拡張フィールド名称の場合、  ユーザ定義拡張フィールドを削除します  の確認ダイアログを表示します。「表 1-18 インシデント抽出に指定可能なフィールド」および「表 1-19 インシデント抽出に追加で指定可能なフィールド (Syslog クライアントの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連携の場合)」に記載の拡張フィールド名称でない場合、  ユーザ定義拡張フィールドを削除します 削除対象の条件を含むルールも削除されます  の確認ダイアログを表示します。了承した場合、ユーザ定義拡張フィールドを削除します。削除が失敗すると、「表 6-87 ユーザ定義拡張フィールドの削除反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑫	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-86 ルールの削除反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みのルールです。	既に削除済みのルールです。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

表 6-87 ユーザ定義拡張フィールドの削除反映失敗時のダイアログ一覧

項目番号	内容	説明
1	指定したユーザ定義拡張フィールドが存在しません。	指定したユーザ定義拡張フィールドが存在しません。
2	データベースのアクセスに失敗しました。	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) ルール追加

図 6-61 ルール追加画面

① トップ > 共通 > Syslogクライアント一覧 > ファイアウォール(IP:192.0.2.2) > ルール追加

**ルール追加**

Syslogクライアント

クライアント名称	ファイアウォール	②
----------	----------	---

ルール

優先度	10	③
条件1	Signature ID	virus
条件2	Name	THREAT
条件3	Severity	④ 5
条件4		
条件5		
条件6		

アクション種別	手動選択	⑤
送信元指定		⑥
宛先指定		⑦
解除タイマー	60	分 ⑧

セグメント

セグメント名称	無所属セグメント	⑨
---------	----------	---

追加 ⑩ キャンセル ⑪

表 6-88 ルール追加画面に表示する項目

項目番	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	Syslog クライアント Syslog クライアント	クライアント名称	クライアント名称を入力します。「(7)(a) Syslog クライアント追加」で登録したクライアント名称としてください。「(8) Syslog クライアント詳細」から移動した場合、クライアント名称は入力できません。
③	ルール	優先度	ルールの優先度を 1~10000 までの数値で指定します。 Syslog クライアントから受信した Syslog に対するルールを検索する際の優先度となります。値を昇順で検索し、ルールに一致した場合は対応するアクションを実行します。 ルールに一致した場合は、以降の検索は行いません。
④	条件(*)		プルダウンメニューにて、ルール化する Syslog メッセージのフィールド（種別）と、その値を指定します。 指定した条件のすべてがマッチした場合のみルールに一致したものとします。指定した条件のうち、いずれかがマッチしない場合は、ルールにマッチしていないものとします。 条件は、最大で 6 つを同時に設定することができます。 この例では、Signature ID が virus、Name が THREAT、Severity の値が 5 を条件とします。
⑤	アクション 種別(*)		条件に一致した場合のアクションを指定します。 以下のアクションから選択することができるです。 <ul style="list-style-type: none"><li>・手動選択</li><li>・通信遮断</li><li>・詳細ミラー</li><li>・通信遮断(スケジュール解除)</li><li>・詳細ミラー(スケジュール解除)</li><li>・通信遮断(タイマー解除)</li><li>・詳細ミラー(タイマー解除)</li><li>・なし</li></ul>

項目番号	内容	説明
⑥ ⑦	送信元指定 宛先指定	<p>アクション種別が下記の場合、送信元と宛先に使用する IP アドレス/MAC アドレスを、Syslog の中の「(未選択)」、「src」、「dst」、「sourceTranslatedAddress」、「destinationTranslatedAddress」、「smac」、「dmac」フィールドから選択します。</p> <ul style="list-style-type: none"> <li>・通信遮断</li> <li>・通信遮断(スケジュール解除)</li> <li>・通信遮断(タイマー解除)</li> <li>・詳細ミラー</li> <li>・詳細ミラー(スケジュール解除)</li> <li>・詳細ミラー(タイマー解除)</li> </ul> <p>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、追加で「PanOSXforwarderfor」フィールドも選択可能です。</p> <p>および、ユーザ定義拡張フィールドとして、データ型が「IPv4 Address」、「IPv6 Address」、「IPv4 Address or IPv6 Address」、または「MAC Address」であるフィールドも選択可能です。</p> <p>アクション種別が通信遮断(通信遮断(スケジュール解除))、通信遮断(タイマー解除)を含むで、送信元指定にデータ型が「MAC Address」であるフィールドを選択した場合、宛先指定は選択できません。</p> <p>アクション種別が詳細ミラー(詳細ミラー(スケジュール解除))、詳細ミラー(タイマー解除)含むの場合、宛先指定は選択できません。</p> <p>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において、端末を遮断する場合、端末の IP アドレスが flexString2 の値によって、どのフィールドに格納されているのかが異なります。例えば、flexString2=server-to-client の場合に、端末の IP アドレスは「dst」または「destinationTranslatedAddress」に格納されています。</p>
⑧	解除タイマー	アクション種別が通信遮断(タイマー解除)または詳細ミラー(タイマー解除)の場合、セキュリティフィルタ生成後に解除を実行するまでの時間(分)を指定します。 1~1440 が指定可能です。

項目番	内容		説明
⑨	セグメント 名称	セグメント 名称	セグメント名称を入力します。「6.1.5(1)(a) セグメント追加」で登録したセグメント名 称、または無所属セグメントとしてくだ さい。「6.1.5(1)(b) セグメント設定」から移動 した場合、セグメント名称は入力できま せん。
⑩	—	追加ボタン	ルール追加を反映します。ボタンを押下し、 反映が成功すると、「(8)Syslog クライアント 詳細」に移動します。反映が失敗すると、 「表 6-89 ルール追加の反映失敗時のダイ アログ一覧」に示すダイアログを表示しま す。
		キャンセル ボタン	ルール追加をキャンセルします。ボタンを押 下すると、「(8)Syslog クライアント詳細」に 移動します。

(\*) 指定する条件は、Name=THREAT、Severity=4 と 5 の値の指定を推奨します。アクション種別は手動選択を選択し運用者判断での通信遮断を推奨します。通信遮断や詳細ミラーを設定する場合は、十分に検証した上で設定を行って下さい。

表 6-89 ルール追加の反映失敗時のダイアログ一覧

項目番	内容	説明
1	優先度が入力され ていません	優先度が入力されていません。優先度を入力してく ださい。
2	送信元指定と宛先 指定のどちらかに 入力が必要です	アクション指定を通信遮断選択時、送信元指定と宛 先指定のどちらかも選択されていません。送信元指 定/宛先指定のどちらか、または両方を選択してく ださい。
3	送信元指定が入力 されていません	アクション指定を詳細ミラー選択時、送信元指定が 選択されていません。送信元指定を選択してく ださい。
4	存在しないセグメ ント名称です	存在しないセグメント名称です。
5	既に登録済みの優 先度です	既に登録済みの優先度です
6	既に削除済みの Syslog クライア ントです	既に削除済みの Syslog クライアントです。
7	解除タイマーが入 力されていません	解除タイマーが入力されていません。
8	範囲外の解除タイ マーです	範囲外の解除タイマーです。
9	要求パラメータに 間違があるか、削 除中のセグメン トです	要求パラメータに間違があるか、削除中のセグメ ントです。「6.1.8(6) メンテナンス」により保守情報 を収集してください。

項目番号	内容	説明
10	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (b) ユーザ定義拡張フィールド追加

図 6-62 ユーザ定義拡張フィールド追加画面

ユーザ定義拡張フィールド追加

ユーザ定義拡張フィールド

拡張フィールド名称	vendorSpecificKey1	②
データ型	String	③

追加 キャンセル ④ ⑤

表 6-90 ユーザ定義拡張フィールド追加画面に表示する項目

項目番号	内容	説明	
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。	
②	ユーザ定義 拡張フィー ルド	拡張フィー ルド名称	ユーザ定義拡張フィールドの名称を示す文字列です。最大 256 文字登録可能です。

項目番	内容	説明
③		データ型 データ型を選択します。以下のいずれかを選択してください。 <ul style="list-style-type: none"><li>• String</li><li>• Integer</li><li>• String or Integer</li><li>• IPv4 Address</li><li>• IPv6 Address</li><li>• IPv4 Address or IPv6 Address</li><li>• MAC Address</li><li>• Floating Point</li><li>• Double</li><li>• Long</li><li>• Time Stamp</li></ul>
④	—	追加ボタン ユーザ定義拡張フィールド追加を反映します。ボタンを押下し、反映が成功すると、「(8)Syslog クライアント詳細」に移動します。反映が失敗すると、「表 6-91 ユーザ定義拡張フィールド追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑤	キャンセルボタン	ユーザ定義拡張フィールド追加をキャンセルします。ボタンを押下すると、「(8)Syslog クライアント詳細」に移動します。

表 6-91 ユーザ定義拡張フィールド追加の反映失敗時のダイアログ一覧

項目番	内容	説明
1	拡張フィールド名称が入力されていません	拡張フィールド名称が入力されていません。拡張フィールド名称を入力してください。
2	データ型が選択されていません	データ型が選択されていません。データ型を選択してください。
3	既に登録済みのユーザ定義拡張フィールドです	既に登録済みのユーザ定義拡張フィールドです。
4	既に削除済みの Syslog クライアントです	既に削除済みの Syslog クライアントです。
5	要求パラメータに間違があります	要求パラメータに間違があります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
6	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

### 6.1.7 マップ

#### (1) マップ一覧

図 6-63 マップ一覧画面



表 6-92 マップ一覧に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	マップ追加ボタン	新規にマップを追加します。ボタンを押下すると「(a) マップ追加」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると、一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「map_list.csv」になります。
④	CSV 形式からのマップ追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上のマップを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑤	背景画像保存ボタン	ボタンを押下すると、一覧で表示した画像ファイルを ZIP 形式でダウンロードできます。ファイル名は「map_background_image.zip」になります。

項目番号	内容	説明
⑥	ZIP 形式からの一括背景画像追加ボタン	<p>ボタンを押下すると、ZIP 形式のファイルから 1 個以上の背景画像ファイルを追加することができます。背景画像追加に使用可能なファイルの条件を満たしたファイルを指定してください。</p> <p>背景画像追加に使用可能なファイルの条件は以下です。</p> <ul style="list-style-type: none"> <li>・背景画像が ZIP 形式で圧縮されていること。</li> <li>・ディレクトリ構造がないこと。</li> <li>・10MB 以下であること。10MB を超える場合は、複数のファイルに分けて、複数回おこなってください。</li> <li>・背景画像として使用可能な条件を満たしていること。</li> </ul> <p>背景画像として使用可能な条件は以下です。</p> <ul style="list-style-type: none"> <li>・背景画像のフォーマットは、JPEG, GIF, PNG であること。</li> <li>・背景画像のファイル名は、拡張子を含む最大 255 文字であること。ファイル名に使用できる文字は、1 バイト文字で、1 文字目が英数字で、2 文字目以降が英数字とハイフン (-) , アンダースコア (_) , ピリオド (.) であること。また、マップの背景画像として登録されたファイル名であること。</li> </ul>
⑦	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑧	ページあたり表示件数 切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑨	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑩	マップ情報	マップ情報の一覧を表示します。 表示項目は、マップ名/背景画像/背景画像ファイル名/コメントです。

項番	内容	説明
⑪	操作	<p>操作として、表示/編集/削除ボタンが表示され、以下に示す動作をおこないます。</p> <p>表示ボタンを押下すると、「(b) マップ」に移動します。</p> <p>編集ボタンを押下すると、「(c) マップ編集」に移動します。</p> <p>削除ボタンを押下すると、</p> <p>マップ &lt;マップ名&gt; を削除します</p> <p>の確認ダイアログを表示します。了承した場合、マップを削除します。削除が失敗すると、「表 6-93 マップ一覧の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p>
⑫	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-93 マップ一覧の反映失敗時のダイアログ一覧

項番	内容	説明
1	指定したマップは存在しません	指定したマップは存在しません。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) マップ追加

図 6-64 マップ追加画面

① 階層リンク  
② マップ名称  
③ 背景画像  
④ 新たに画像ファイルをアップロードする：  
⑤ 集線装置表示  
⑥ 表示エイリアス  
⑦ コメント  
⑧ 対象装置  
⑨ 件表示  
⑩ 検索  
⑪ チェックボックス  
⑫ チェックボックス  
⑬ 端末接続数  
⑭ 前のページ  
⑮ 次のページ  
⑯ 追加  
⑰ キャンセル  
⑱ フィルタ  
⑲ デバイス情報  
⑳ IPアドレス  
㉑ 装置モデル  
㉒ 状態  
㉓ 端末接続数  
㉔ 通信端末数  
㉕ コメント  
㉖ 所属マップ  
㉗ AX2130S\_Edge5W  
㉘ 192.0.2.3  
㉙ AX2100S  
㉚ 正常  
㉛ 8  
㉜ 0  
㉝ フロア1Fマップ  
㉞ AX3660S\_Core5W  
㉟ 192.0.2.2  
㉟ AX3660S  
㉟ 正常  
㉟ 1  
㉟ 0  
㉟ フロア1Fマップ

表 6-94 マップ追加に表示する項目

項目番	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	マップ情報	マップ名称	マップ情報としてマップの名称を示す文字列です。最大 256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。

項目番号	内容	説明	
③	背景画像： 別のマップで 使用している 背景画像から 選択する	AX-Security-Controller 上で管理している 背景画像一覧から、マップの背景画像を 設定します。背景画像を選択すると、選 択した背景画像が表示されます。背景画 像を指定しない場合は、「背景画像を使 用しない」を選択します。 ③と④両方で画像を選択した場合は、④ で選択した画像が優先されます。	
④	背景画像： 新たに画像 ファイルを アップロード する	ウェブブラウザが動作している環境で管 理している画像ファイルをアップロード し、マップの背景画像に設定します。 「ファイルを選択ボタン」、または、 「参照…ボタン」を押下し、ファイルを 選択します。選択したファイルを取り消 す場合は、「選択ファイルをクリア」ボ タンを押下します。 ③と④両方で画像を選択した場合は、④ で選択した画像が優先されます。 使用可能な背景画像のフォーマットは、 JPEG, GIF, PNG です。 使用可能な背景画像のファイル名は、拡 張子を含み最大 255 文字です。ファイル 名に使用できる文字は、1 バイト文字 で、1 文字目が英数字、2 文字目以降が英 数字とハイフン (-)、アンダースコア (_)、ピリオド (.) です。	
⑤	集線装置表示	マップでの集線装置表示有無を選択しま す。有効を選択すると、対象装置の同一 ポートに複数の端末が接続されている場 合に集線装置（ハブ）を表示します。こ の時、端末は集線装置に接続してい るよう表示します。	
⑥	表示エイリアス	マップで使用する端末のエイリアスのタ イトル（最大 256 文字）を指定する文字 列です。	
⑦	コメント	マップ情報として、マップの説明を記載 する文字列です。0~256 文字登録可能で す。なおアポストロフィー(')文字は使用 しないでください。	
⑧	対象装置	表示カラム切 替ボタン	一覧から不要なカラムを非表示にするこ とができます。 チェックボックスカラムを非表示にした まま追加を行うと、追加するマップの対 象装置になりません。
⑨	ページあたり 表示件数切替 プルダウン	1 ページあたりに表示する件数を切り替 えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。	
⑩	検索テキスト ボックス	テキストボックスに入力した文字列に該 当する行のみに一覧を絞り込むことがで きます。	

項目番号	内容	説明
⑪	全選択チェックボックス	チェックボックスを押下すると、すべての管理対象装置を、本マップの所属対象とします。もう一度押下すると、すべての管理対象装置を、本マップの所属対象から外します。 検索テキストボックスで絞り込みをおこなっている場合、チェックボックスを押下すると、絞り込みされた装置を対象に本マップの所属対象とします。もう一度押下すると、絞り込みされた装置を対象に、本マップの所属対象から外します。
⑫	チェックボックス	管理対象装置を、本マップの所属対象とします。もう一度押下すると、本マップの所属対象から外します。
⑬	対象装置情報	対象装置情報を表示します。 表示項目は、装置情報/IP アドレス/装置モデル/状態/端末接続数/遮断端末数/コメント/所属マップです。
⑭	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。
⑮	追加ボタン	マップ追加を反映します。ボタンを押し、反映が成功すると、「(1) マップ一覧」に移動します。反映前に注意喚起がある場合、または、反映が失敗すると、「表 6-95 マップ追加の注意喚起および反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑯	キャンセルボタン	マップ追加をキャンセルします。ボタンを押下すると、「(1) マップ一覧」に移動します。

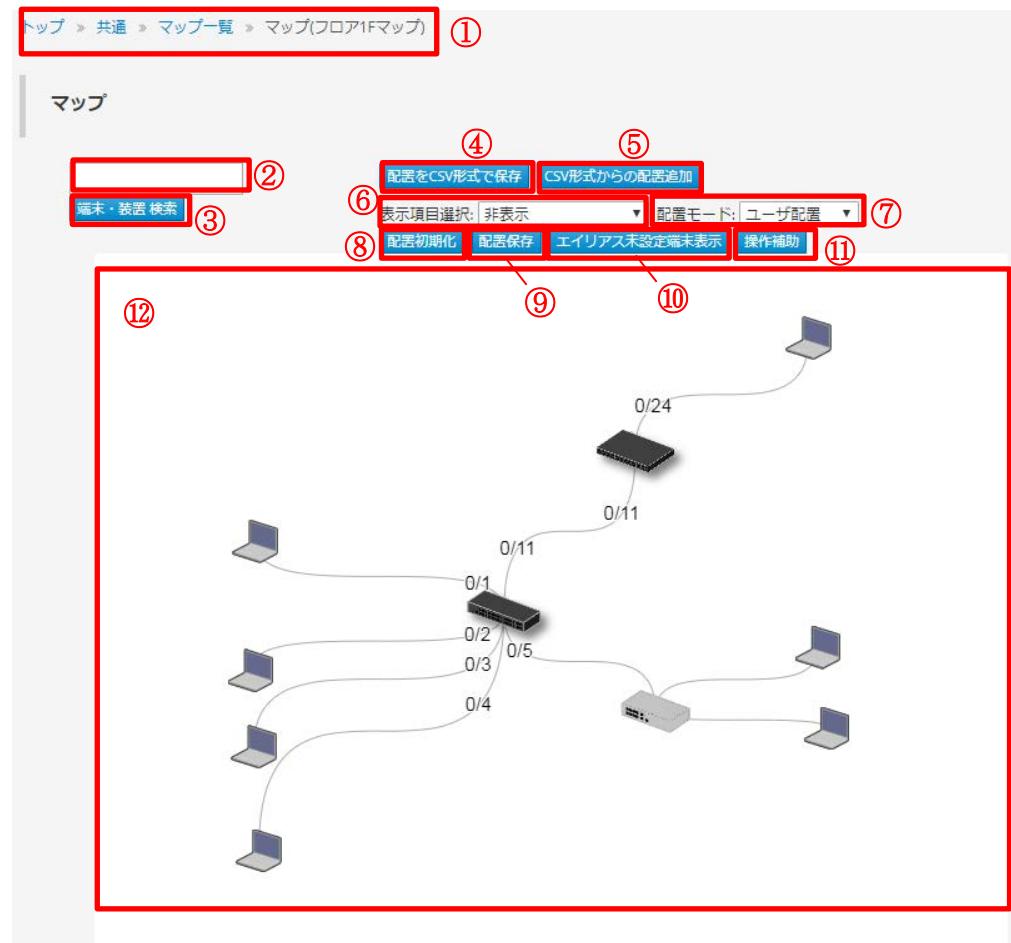
表 6-95 マップ追加の注意喚起および反映失敗時のダイアログ一覧

項目番号	内容	説明
1	マップの所属変更があります	別のマップに所属している装置を本マップに所属させます。
2	既に使用されているファイル名です	登録済みのマップの背景画像として使用されているファイル名です。選択した画像ファイルに置きかえられます。
3	既に登録済みのマップ名称です	既に登録済みのマップ名称です。
4	マップ名を入力してください	マップ名を入力してください。
5	既に 500 マップ登録されています	既に 500 マップ登録されています。

項番	内容	説明
6	背景画像のファイル名に使用できる文字は 1 文字目が英数字で 2 文字目以降が英数字とハイフン (-) , アンダースコア (_) , ピリオド (.) です。	背景画像ファイルのファイル名に使用できる文字は、1 バイト文字で、1 文字目が英数字、2 文字目以降が英数字とハイフン (-) , アンダースコア (_) , ピリオド (.) です。
7	指定可能なファイル形式は(JPG, GIF, PNG)です	背景画像ファイルの指定可能なファイル形式は(JPG, GIF, PNG)です。
8	指定可能なファイルサイズは最大 1MB です	背景画像ファイルの指定可能なファイルサイズは最大 1MB です。
9	ファイル名が長すぎます	背景画像ファイルのファイル名が長すぎます。
10	対象装置が存在しません	削除中の装置、または削除済みの装置です。
11	要求のパラメータに間違いがあります	要求のパラメータに間違があります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
12	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (b) マップ

図 6-65 マップ画面 (1/2)



## 6 AX-Security-Controller(Manager)の Web インタフェース

図 6-66 マップ画面 (2/2)

装置一覧⑬							マップ⑮
表示カラム切替		IPアドレス	装置モデル	状態	端末接続数	遮断端末数	コメント
AX2130S_EdgeSW	192.0.2.3	AX2100S	正常	6	0		<input type="button" value="表示"/>
AX3660S_CoreSW	192.0.2.2	AX3660S	正常	1	0		<input type="button" value="表示"/>

2件中1から2まで表示

端末一覧⑯							マップ⑰	
表示カラム切替		IPアドレス	MACアドレス	ペンドラ	エイリ アス	ポート 番号	ポートエイ リアス	VLAN ID
192.0.2.1	0000.5e00.53ff	ICANN, IANA Department	None	AX3660S_CoreSW	0/24	None	4093	<input type="button" value="表示"/>
198.51.100.101	0000.5e00.5301	ICANN, IANA Department	None	AX2130S_EdgeSW	0/1	None	3000	<input type="button" value="表示"/>
198.51.100.102	0000.5e00.5302	ICANN, IANA Department	None	AX2130S_EdgeSW	0/2	None	3000	<input type="button" value="表示"/>
198.51.100.103	0000.5e00.5303	ICANN, IANA Department	None	AX2130S_EdgeSW	0/3	None	3000	<input type="button" value="表示"/>
198.51.100.104	0000.5e00.5304	ICANN, IANA Department	None	AX2130S_EdgeSW	0/4	None	3000	<input type="button" value="表示"/>
198.51.100.105	0000.5e00.5305	ICANN, IANA Department	None	AX2130S_EdgeSW	0/5	None	3000	<input type="button" value="表示"/>
198.51.100.106	0000.5e00.5306	ICANN, IANA Department	None	AX2130S_EdgeSW	0/6	None	3000	<input type="button" value="表示"/>

/件中1から7まで表示

図 6-67 情報ウィンドウ画面(装置)



図 6-68 情報ウィンドウ画面(端末)

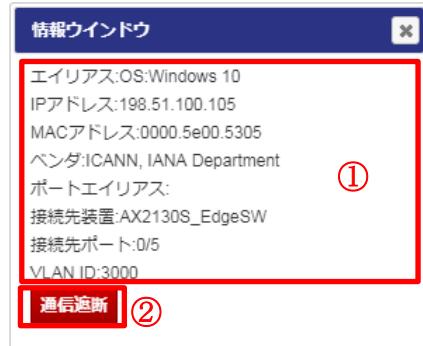


図 6-69 情報ウィンドウ画面(集線装置)



図 6-70 検索結果ウィンドウ画面



表 6-96 マップ画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	マップ操作領域	端末・装置検索ボタンを押下により、端末・装置検索テキストボックスに入力した文字列に該当する端末・装置の検索結果を「表 6-100 検索結果ウィンドウに表示する項目」に示す検索結果ウィンドウに表示します。
③		装置の検索対象とする項目は、装置名稱/IP アドレス/MAC アドレス/装置モデルです。 端末の検索対象とする項目は、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 です。

項目番号	内容	説明
④	配置を CSV 形式で保存ボタン	配置保存ボタンで保存したマップの配置情報を CSV 形式でダウンロードできます。ファイル名は「map_positions.csv」となります。
⑤	CSV 形式から配置追加ボタン	ボタンを押下すると、CSV 形式のファイルから配置情報を追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑥	装置・端末アイコン下表示項目選択プルダウンメニュー	マップ描画領域に表示する装置・端末アイコンの下に表示する項目を選択します。 <ul style="list-style-type: none"> <li>・非表示：表示しません。</li> <li>・装置名称/エイリアス：装置は装置名称、端末はエイリアスを表示します。それぞれ付与されていない場合は表示しません。</li> <li>・IP アドレス：IP アドレスを表示します。IP アドレスが付与されていない端末は表示しません。</li> <li>・MAC アドレス：MAC アドレスを表示します。</li> </ul>
⑦	配置モード選択プルダウンメニュー	マップ描画領域に表示する端末アイコンの配置モードを選択します。 <ul style="list-style-type: none"> <li>・ユーザ配置：端末アイコンを自由に配置できます。</li> <li>・端末自動配置：端末の接続先装置アイコンを中心に、端末アイコンが自動で配置されます。</li> </ul>
⑧	配置初期化ボタン	マップ描画領域の装置・端末・集線装置アイコンの配置と、マップ描画領域の表示中心位置および縮尺を初期化します。 ボタンを押下すると、 配置を初期化します の確認ダイアログを表示します。了承した場合、配置を初期化し、初期化が成功すると、 初期化が完了しました ダイアログを表示します。初期化が失敗すると、「表 6-101 配置初期化の反映失敗時のダイアログ一覧」に示すダイアログを表示します。

項目番号	内容	説明
⑨	配置保存ボタン	<p>マップ描画領域の装置・端末・集線装置アイコンの配置と、マップ描画領域の表示中心位置および縮尺を保存します。</p> <p>配置を保存するまでは、装置・端末・集線装置アイコンは自動配置になり、マップ描画領域の表示中心位置および縮尺は初期設定になります。配置を保存すると、マップ画面表示時に保存された配置で表示されます。</p> <p>ボタンを押下すると、</p> <p>配置を保存します</p> <p>の確認ダイアログを表示します。了承した場合、配置を保存し、保存が成功すると、</p> <p>保存が完了しました</p> <p>ダイアログを表示します。保存が失敗すると、「表 6-102 配置保存失敗時のダイアログ一覧」に示すダイアログを表示します。</p>
⑩	エイリアス未設定端末表示ボタン	ボタンを押下すると、マップ描画領域のエイリアス未設定の端末アイコンに影を付与して明示します (  )。もう一度押下すると、明示を終了します。
⑪	操作補助表示ボタン	ボタンの押下ごとに、マップ描画領域の操作補助ボタンの表示・非表示を切り替えます。

項目番号	内容	説明
⑫	マップ描画領域	<p>マップ表示位置の変更 マップ描画領域をドラッグすることで、マップの表示位置を変更できます。</p> <p>操作補助ボタンを表示し、方向ボタン (↑↓←→) を押下することでも、押下したボタンの方向にマップの表示位置を変更できます。</p> <p>マップ表示の縮尺変更 マップ描画領域で拡大・縮小操作 (マウスホイールの回転など) することでマップ表示の縮尺を変更できます。</p> <p>操作補助ボタンを表示し、拡大・縮小・全表示ボタンを押下することでも、マップ表示の縮尺を変更できます。</p> <p>拡大 (+) ボタンを押下することで表示範囲が狭くなり、装置や端末アイコンなどの表示が大きくなります。</p> <p>縮小 (-) : ボタンを押下することで表示範囲が広くなり、装置や端末アイコンなどの表示が小さくなります。</p> <p>全表示 (◎) : マップ内の装置と端末アイコンが全て画面内に表示されよう縮尺変更されます。</p>
	背景	<p><b>【表示】</b> マップに設定された背景画像を表示します。背景画像を設定しない場合は、あらかじめ用意された背景画像が表示されます。</p> <p><b>【操作】</b> なし</p>

項目番号	内容	説明
	装置	<p><b>【表示】</b>          マップの所属対象装置を表示します。アイコンは装置情報の装置モデル設定により、自動的に選択されます。          「(2)(a)装置アイコン設定」により、用意した画像を表示することもできます。          また、装置の状態をアイコンに影を付与して表示します。</p> <p><b>[表示例]</b></p> <ul style="list-style-type: none"> <li>メンテナンス実施：</li> <li>状態不明：</li> </ul> <p><b>【操作】</b>          装置のアイコンを選択すると、「表 6-97 情報ウィンドウ(装置)に表示する項目」に示す情報ウィンドウが表示されます。また、装置の接続回線および接続回線のポート番号が太表示になります。          装置のアイコンをドラッグ操作することで、自由に配置できます。</p>
	端末	<p><b>【表示】</b>          マップの所属対象装置に接続された端末を表示します。アイコンは「(2)(f)端末アイコン設定」により変更できます。また、端末の状態をアイコンに影を付与して表示します。</p> <p><b>[表示例]</b></p> <ul style="list-style-type: none"> <li>通信遮断中：</li> </ul> <p><b>【操作】</b>          端末のアイコンを選択すると、「表 6-98 情報ウィンドウ(端末)に表示する項目」に示す情報ウィンドウを表示します。また、端末の接続回線および接続回線のポート番号が太表示になります。          端末のアイコンをドラッグ操作することで、自由に配置できます。配置モードが端末自動配置の場合は、ドラッグ操作完了後、接続先装置アイコンを中心に、端末アイコンが自動で再配置されます。</p>

項目番号	内容	説明	
	集線装置 (ハブ)	<p><b>【表示】</b> 集線装置表示を有効に設定し、装置の同一ポートに複数の端末が接続されている場合に表示します。 アイコンは「(2)(c)集線装置アイコン設定」により変更できます。</p> <p><b>[表示例]</b> </p> <p><b>【操作】</b> 集線装置のアイコンを選択すると、「表 6-99 情報ウィンドウ(集線装置)に表示する項目」に示す情報ウィンドウが表示されます。 集線装置のアイコンを選択すると、集線装置の接続回線および接続回線のポート番号が太表示になります。 集線装置のアイコンをドラッグ操作することで、自由に配置できます。</p>	
	回線	<p><b>【表示】</b> マップの所属対象装置間、マップの所属対象装置と端末間の回線を表示します。集線装置表示が有効の場合は、装置と集線装置間、集線装置と端末間の回線を表示します。 マップの所属対象装置間の回線には両端のポート番号、マップの所属対象装置と端末、および集線装置間の回線には装置側のポート番号を表示します。 回線の表示は曲線のみです。</p> <p><b>【操作】</b> 回線を選択すると、選択した回線とポート番号が太表示になります。</p>	
(13)	装置一覧	表示カラム切替ボタン	一覧から不要なカラムを非表示することができます。
(14)		ページあたり表示件数切替プルダウン	1ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
(15)		検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
(16)		装置情報	装置の一覧を表示します。表示項目は、装置情報/IP アドレス/装置モデル/状態/端末接続数/遮断端末数/コメントです。 装置のエントリを押下すると、「6.1.4(1)(b)装置詳細」に移動します。

項目番号	内容	説明
(17)	端末一覧	表示ボタン ボタンを押下すると、マップ描画領域の該当する装置のアイコンに影を付与して明示します（表示例：  ）。アイコンの下に表示する項目がある場合は赤文字で表示します。
(18)		ページ切替ボタン ボタンを押下すると、指定のページを表示します。
(19)		表示カラム切替ボタン 一覧から不要なカラムを非表示することができます。
(20)		ページあたり表示件数切替プルダウン 1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
(21)		検索テキストボックス テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
(22)		端末情報 端末の一覧を表示します。表示項目は、IP アドレス/MAC アドレス/ベンダ/エイリアス*/接続先装置/ポート番号/ポートエイリアス/VLAN ID/接続先 AP です。
(23)		表示ボタン ボタンを押下すると、マップ描画領域の該当する端末のアイコンに影を付与して明示します（表示例：  ）。アイコンの下に表示する項目がある場合は、赤文字で表示します。
(24)		ページ切替ボタン ボタンを押下すると、指定のページを表示します。

## 注※

「6.1.3(2)(a), 6.1.3(2)(c)」で 1 つ以上のエイリアスの設定をおこなった場合、複数のタイトルカラムに展開して表示します。タイトルカラムと、「6.1.3(2)(a), 6.1.3(2)(c)」の項目のタイトルが一致しない場合、値には None を表示します。

表 6-97 情報ウィンドウ(装置)に表示する項目

項目番号	内容	説明
①	装置情報	装置情報を表示します。表示項目は、装置名称/IP アドレス/MAC アドレス/装置モデルです。
②	チェックボックス：配下端末の配置を固定する	情報ウィンドウを表示した装置に接続された端末を、ユーザが配置した場所に固定します。マップの配置モードを端末自動配置に設定しても、指定した装置に接続された端末は自動配置されません。

表 6-98 情報ウィンドウ(端末)に表示する項目

項目番号	内容	説明
①	端末情報	端末情報を表示します。表示項目は、マップ追加またはマップ編集画面で指定した表示エイリアスのタイトルと値/IP アドレス/MAC アドレス/ベンド/ポートエイリアス/接続先装置/接続先ポート/VLAN ID です。
②	操作	<p>操作として、通信遮断、または通信遮断解除ボタンが表示され、以下に示す動作をおこないます。</p> <p>通信遮断ボタンを押下すると</p> <p>端末 MAC アドレス &lt;MAC アドレス&gt; を通信遮断します</p> <p>の確認ダイアログを表示します。了承した場合、セキュリティフィルタの通信遮断を適用し、マップ画面を再読み込みします。</p> <p>通信遮断解除ボタンを押下すると</p> <p>端末 MAC アドレス &lt;MAC アドレス&gt; のセキュリティフィルタの通信遮断を解除します</p> <p>の確認ダイアログを表示します。了承した場合、該当する端末に適用しているすべてのセキュリティフィルタの通信遮断を解除し、マップ画面を再読み込みします。</p>

表 6-99 情報ウィンドウ(集線装置)に表示する項目

項目番号	内容	説明
①	装置情報	集線装置情報を表示します。表示項目は、ポートエイリアス/接続先装置/接続先ポート番号です。

表 6-100 検索結果ウィンドウに表示する項目

項目番号	内容	説明
①	装置・端末情報	端末・装置検索テキストボックスに入力した文字列に該当する装置・端末を表示します。 装置の表示項目は、IP アドレス/MAC アドレス/装置名称です。端末の表示項目は、IP アドレス/MAC アドレス/マップ追加またはマップ編集画面で指定した表示エイリアスの値です。

項番	内容	説明
②	マップ表示	表示ボタンを押下すると、マップ描画領域の該当する装置・端末のアイコンに影を付与して明示します（[表示例]装置：  ，端末：  ）。装置・端末アイコンの下に表示する項目がある場合は赤文字で表示します。

表 6-101 配置初期化の反映失敗時のダイアログ一覧

項番	内容	説明
1	マップが削除されました	指定したマップは存在しません。
2	要求のパラメータに間違이があります	要求のパラメータに間違いがあります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
3	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

表 6-102 配置保存失敗時のダイアログ一覧

項番	内容	説明
1	マップが削除されました	指定したマップは存在しません。
2	要求のパラメータに間違いがあります	要求のパラメータに間違いがあります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
3	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

表 6-103 通信遮断の反映失敗時のダイアログ一覧

項番	内容	説明
1	要求パラメータに間違いがあります	要求のパラメータに間違いがあります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

表 6-104 通信遮断解除の反映失敗時のダイアログ一覧

項番	内容	説明
1	要求パラメータに間違いがあります	要求のパラメータに間違いがあります。「6.1.8(6) メンテナンス」により保守情報を収集してください。

項目番号	内容	説明
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (c) マップ編集

図 6-71 マップ編集画面

IPアドレス	装置モデル	状態	端末接続数	遮断端末数	コメント	所属マップ
192.0.2.3	AX2100S	正常	8	0		フロア1Fマップ
192.0.2.2	AX3660S	正常	1	0		フロア1Fマップ

表 6-105 マップ編集画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。

項目番号	内容	説明
②	マップ情報	マップ名称 マップ情報としてマップの名称を示す文字列です。最大 256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。
③	背景画像： 別のマップで 使用している 背景画像から 選択する	AX-Security-Controller 上で管理している 背景画像一覧から、マップの背景画像を 設定します。背景画像を選択すると、選 択した背景画像が表示されます。背景画 像を指定しない場合は、「背景画像を使 用しない」を選択します。 ③と④両方で画像を選択した場合は、④ で選択した画像が優先されます。
④	背景画像： 新たに画像 ファイルを アップロード する	ウェブブラウザが動作している環境で管 理している画像ファイルをアップロード し、マップの背景画像に設定します。 「ファイルを選択ボタン」、または、 「参照…」ボタンを押下し、ファイルを 選択します。選択したファイルを取り消 す場合は、「選択ファイルをクリア」ボ タンを押下します。 使用可能な背景画像のフォーマットは、 JPEG, GIF, PNG です。 使用可能な背景画像のファイル名は、拡 張子を含み最大 255 文字です。ファイル 名に使用できる文字は、1 バイト文字 で、1 文字目が英数字、2 文字目以降が英 数字とハイフン (-)、アンダースコア (_)、ピリオド (.) です。
⑤	集線装置表示	マップでの集線装置表示有無を選択しま す。有効を選択すると、対象装置の同一 ポートに複数の端末が接続されている場 合に集線装置（ハブ）を表示します。こ の時、端末は集線装置に接続しているよ うに表示します。
⑥	表示エイリア ス	マップで使用する端末のエイリアスのタ イトル（最大 256 文字）を指定する文字 列です。
⑦	コメント	マップ情報として、マップの説明を記載 する文字列です。0~256 文字登録可能で す。なおアポストロフィー(')文字は使用 しないでください。
⑧	対象装置	表示カラム切 替ボタン 一覧から不要なカラムを非表示にするこ とができます。 チェックボックスカラムを非表示にした まま更新を行うと、更新するマップの対 象装置になりません。
⑨	ページあたり 表示件数切替 プルダウン	1 ページあたりに表示する件数を切り替 えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。

項目番号	内容	説明
⑩	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑪	全選択チェックボックス	チェックボックスを押下すると、すべての管理対象装置を、本マップの所属対象とします。もう一度押下すると、すべての管理対象装置を、本マップの所属対象から外します。 検索テキストボックスで絞り込みをおこなっている場合、チェックボックスを押下すると、絞り込みされた装置を対象に本マップの所属対象とします。もう一度押下すると、絞り込みされた装置を対象に、本マップの所属対象から外します。
⑫	チェックボックス	管理対象装置を、本マップの所属対象とします。もう一度押下すると、本マップの所属対象から外します。
⑬	対象装置情報	対象装置情報を表示します。 表示項目は、装置情報/IP アドレス/装置モデル/状態/端末接続数/遮断端末数/コメント/所属マップです。
⑭	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。
⑮	更新ボタン	マップ編集を反映します。ボタンを押下し、反映が成功すると、「(1) マップ一覧」に移動します。反映前に注意喚起がある場合、または、反映が失敗すると、「表 6-106 マップ編集の注意喚起および反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑯	キャンセルボタン	マップ編集をキャンセルします。ボタンを押下すると、「(1) マップ一覧」に移動します。

表 6-106 マップ編集の注意喚起および反映失敗時のダイアログ一覧

項目番号	内容	説明
1	マップの所属変更があります	別のマップに所属している装置を本マップに所属させます。
2	既に使用されているファイル名です	登録済みのマップの背景画像として使用されているファイル名です。選択した画像ファイルに置きかえられます。
3	既に登録済みのマップ名称です	既に登録済みのマップ名称です。
4	マップ名を入力してください	マップ名を入力してください。

項目番	内容	説明
5	背景画像のファイル名に使用できる文字は 1 文字目が英数字で 2 文字目以降が英数字とハイフン (-) , アンダースコア (_) , ピリオド (.) です。	背景画像ファイルのファイル名に使用できる文字は、1 バイト文字で、1 文字目が英数字、2 文字目以降が英数字とハイフン (-) , アンダースコア (_) , ピリオド (.) です。
6	指定可能なファイル形式は(JPG, GIF, PNG)です	背景画像ファイルの指定可能なファイル形式は(JPG, GIF, PNG)です。
7	指定可能なファイルサイズは最大 1MB です	背景画像ファイルの指定可能なファイルサイズは最大 1MB です。
8	ファイル名が長すぎます	背景画像ファイルのファイル名が長すぎます。
9	既にマップが削除されたか、対象装置が存在しません	既にマップが削除されたか、対象装置が存在しません。
10	要求のパラメータに間違いがあります	要求のパラメータに間違いがあります。「6.1.8(6) メンテナンス」により保守情報を収集してください。
11	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## (2) マップ設定

## (a) 装置アイコン設定

図 6-72 装置アイコン一覧画面

The screenshot shows the 'Device Icon List' page. At the top left is a breadcrumb navigation: トップ > 共通 > 装置アイコン一覧 (①). Below it is a header '装置アイコン一覧'. On the left, there are two buttons: 'CSV形式で保存' (②) and 'CSV形式からの装置アイコン追加' (③). To the right of these are '表示カラム切替' (④), a dropdown for '件表示' (⑤) set to 25, a '検索:' input field (⑥), and a search button. The main area displays a table with two rows of device icons. The first row contains an icon for 'AX3660S\_CoreSW' (IP: 198.51.100.60, Model: AX3660S, Pre-set), and the second row contains an icon for 'AX2100S\_EdgeSW' (IP: 198.51.100.163, Model: AX2100S, User setting). Each row has an 'Edit' button (⑦) and a 'Bulk Edit' button (⑧). At the bottom left is a message '2 件中 1 から 2 まで表示'. At the bottom right are navigation buttons: '前のページ' (⑨), '1', and '次のページ'.

表 6-107 装置アイコン一覧に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	CSV 形式で保存ボタン	ボタンを押下すると、一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「map_nodes_list.csv」になります。
③	CSV 形式からの装置アイコン追加ボタン	ボタンを押下すると、CSV 形式のファイルから装置アイコンを変更することができます。設定契機がユーザ設定の装置だけが反映されます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
④	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑤	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/500 の 5 パターンです。
⑥	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。

項目番号	内容	説明
⑦	装置アイコン情報	<p>装置アイコン情報の一覧を表示します。</p> <p>表示項目は、アイコン/装置情報/IP アドレス/装置モデル/設定契機です。</p> <p>設定契機：</p> <p>プリセット/ユーザ設定</p> <p>プリセット：AX-Security-Controller にあらかじめ用意された装置モデル毎の自動で表示されるアイコン（装置デフォルトアイコン）の場合。</p> <p>ユーザ設定：装置アイコン編集により、ユーザが装置デフォルトアイコン以外を選択した場合。</p>
⑧	操作	<p>操作として、編集ボタンが表示され、以下に示す動作をおこないます。</p> <p>編集ボタンを押下すると「(b) 装置アイコン編集」に移動します。</p>
⑨	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

## (b) 装置アイコン編集

図 6-73 装置アイコン編集画面

The screenshot shows the 'Device Icon Edit' screen. At the top, there is a breadcrumb navigation: トップ > 共通 > 装置アイコン一覧 > 装置アイコン編集 (①). Below it is a title '装置アイコン編集'. The main area is divided into two sections: '装置情報' and '装置アイコン'. In the '装置情報' section, there are three input fields: '装置名称' (AX2100S\_EdgeSW), 'IPアドレス' (198.51.100.163), and '装置モデル' (AX2100S). In the '装置アイコン' section, there is a dropdown menu for 'アイコン画像' with options '登録済み画像から選択する:' and '装置デフォルトイコン' (③). At the bottom right are '更新' (④) and 'キャンセル' (⑤) buttons.

表 6-108 装置アイコン編集に表示する項目

項目番	内容	説明	
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	装置情報	装置名称/ IP アドレ ス/装置モ デル	装置情報として、登録済みの装置名称/IP アド レス/装置モ デルを表示します。
③	装置アイコ ン	アイコン 画像	6.1.8(3)画像管理で管理している画像一覧から 画像を設定します。画像名称を選択すると、 選択した画像が表示されます。装置デフォル トイコンを選択すると、AX-Security- Controller にあらかじめ用意された装置モデル 毎のアイコンになります。

項目番号	内容	説明
④	更新ボタン	装置アイコン編集を反映します。ボタンを押し下し、反映が成功すると、「(a)装置アイコン設定」に移動します。反映が失敗すると、「表 6-109 装置アイコン編集の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑤	キャンセルボタン	装置アイコン編集をキャンセルします。ボタンを押下すると、「(a)装置アイコン設定」に移動します。

表 6-109 装置アイコン編集の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	画像が存在しません	指定した画像は存在しません。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (c) 集線装置アイコン設定

図 6-74 集線装置アイコン一覧画面

① トップ > 共通 > 集線装置アイコン一覧

② 集線装置アイコン一覧

③

④

⑤ 表示カラム切替

⑥ 25 件表示

⑦ 検索:

⑧ デフォルトアイコン

⑨ 編集

⑩ 削除

2 件中 1 から 2 まで表示

前のページ 1 次のページ

表 6-110 集線装置アイコン一覧に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	集線装置アイコン追加ボタン	新規に集線装置アイコンを追加します。ボタンを押下すると「(d)集線装置アイコン追加」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると、一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「maps_hubs_list.csv」になります。
④	CSV 形式からの集線装置アイコン追加ボタン	ボタンを押下すると、CSV 形式のファイルから集線装置アイコンを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑤	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑥	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/500 の 5 パターンです。
⑦	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑧	集線装置アイコン情報	集線装置アイコン情報の一覧を表示します。表示項目は、アイコン/条件/ポートエイリアスです。
⑨	操作	操作として、編集/削除ボタンが表示され、以下に示す動作をおこないます。 編集ボタンを押下すると「(d)集線装置アイコン追加」に移動します。 削除ボタンを押下すると、  集線装置アイコン 装置:<装置名称> ポート:<ポート番号> または、 ポートエイリアス:<ポートエイリアス> を削除します  の確認ダイアログを表示します。了承した場合、 集線装置を削除します。削除が失敗すると、「表 6-111 集線アイコン一覧の反映失敗時のダイア ログ一覧」に示すダイアログを表示します。
⑩	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-111 集線アイコン一覧の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	指定した集線装置アイコンは存在しません	指定した集線装置アイコンは存在しません。

項目番号	内容	説明
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (d) 集線装置アイコン追加

図 6-75 集線装置アイコン追加画面

① トップ > 共通 > 集線装置アイコン一覧 > 集線装置アイコン追加

② 接続先装置名称

③ 接続先ポート番号

④ ポートエイリアス

⑤ アイコン画像

⑥ 追加

⑦ キャンセル

表 6-112 集線アイコン追加に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。

項目番号	内容		説明
②	個別指定	接続先装置名称	集線装置アイコンに対応する装置の名称を入力します。 「6.1.4(1)(a)装置追加」で登録した装置名称を入力してください。 接続先ポート番号を同時に指定してください。 個別指定とエイリアス指定は同時に指定できません。
	接続先ポート番号		集線装置アイコンに対応するポート番号を入力します。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>, <switch no.>/<nif no.>/<port no.>となります。 装置の装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 每コミュニティ)の場合、「6.1.4(1)(b)装置詳細」の MAC アドレステーブル一覧に表示されるポートを入力してください。
④	エイリアス指定	ポートエイリアス	集線装置アイコンに対応するポートエイリアスを入力します。 「6.1.4(3)ポートエイリアス」で登録したポートエイリアスを入力してください。 エイリアス指定と個別指定は同時に指定できません。
⑤	集線装置アイコン	集線装置アイコン	6.1.8(3)画像管理で管理している画像一覧から画像を設定します。画像名称を選択すると、選択した画像が表示されます。
⑥	追加ボタン		集線装置アイコン追加を反映します。ボタンを押下し、反映が成功すると、「(c)集線装置アイコン設定」に移動します。反映が失敗すると、「表 6-113 集線アイコン追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑦	キャンセルボタン		集線装置アイコン追加をキャンセルします。ボタンを押下すると、「(c)集線装置アイコン設定」に移動します。

表 6-113 集線アイコン追加の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	いずれかのフィールドを入力してください	個別指定、またはエイリアス指定を行ってください。
2	存在しない装置名称です	存在しない装置名称です。
3	接続先装置名称を設定してください	装置名称を入力してください。

項目番	内容	説明
4	接続先ポート番号を設定してください	ポート番号を入力してください。
5	既に同じ条件が登録されています	指定した内容が重複しています。
6	画像が存在しません	指定した画像は存在しません。
7	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (e) 集線装置アイコン編集

図 6-76 集線装置アイコン編集画面

① トップ > 共通 > 集線装置アイコン一覧 > 集線装置アイコン編集

② 接続先装置名称: AX2100S\_EdgeSW

③ 接続先ポート番号: 0/21

④ ポートエイリアス

⑤ 登録済み画像から選択する: 集線装置アイコン(無線AP)

⑥ 更新

⑦ キャンセル

表 6-114 集線装置アイコン編集に表示する項目

項目番号	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	個別指定	接続先装置名称	追加済みの集線装置アイコンに対応する装置の名称を入力します。 「6.1.4(1)(a) 装置追加」で登録した装置名称を入力してください。 接続先ポート番号を同時に指定してください。 個別指定とエイリアス指定は同時に指定できません。
		接続先ポート番号	追加済みの集線装置アイコンに対応するポート番号を入力します。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>, <switch no.>/<nif no.>/<port no.>となります。 装置の装置モデルが標準 MIB 対応装置、または標準 MIB 対応装置(VLAN 每コミュニティ)の場合、「6.1.4(1)(b) 装置詳細」の MAC アドレステーブル一覧に表示されるポートを入力してください。
④	エイリアス指定	ポートエイリアス	追加済みの集線装置アイコンに対応するポートエイリアスを入力します。 「6.1.4(3)ポートエイリアス」で登録したポートエイリアスを入力してください。 エイリアス指定と個別指定は同時に指定できません。
⑤	集線装置アイコン	集線装置アイコン	6.1.8(3)画像管理で管理している画像一覧から画像を設定します。画像名称を選択すると、選択した画像が表示されます。
⑥	更新ボタン		集線装置アイコン編集を反映します。ボタンを押下し、反映が成功すると、「(c)集線装置アイコン設定」に移動します。反映が失敗すると、「表 6-115 集線装置アイコン編集の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑦	キャンセルボタン		集線装置アイコン編集をキャンセルします。ボタンを押下すると、「(c)集線装置アイコン設定」に移動します。

表 6-115 集線装置アイコン編集の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	いずれかのフィールドを入力してください。	個別指定、またはエイリアス指定を行ってください。

項目番号	内容	説明
2	存在しない装置名称です。	存在しない装置名称です。
3	接続先装置名称を設定してください	装置名称を入力してください。
4	接続先ポート番号を設定してください	ポート番号を入力してください。
5	既に同じ条件が登録されています	指定した内容が重複しています。
6	画像が存在しません	指定した画像は存在しません。
7	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (f) 端末アイコン設定

図 6-77 端末アイコン一覧画面

① ツップ > 共通 > 端末アイコン一覧

② 端末アイコン追加

③ CSV形式で保存

④ CSV形式からの端末アイコン追加

⑤ 表示カラム切替

⑥ 25 件表示

⑦ 検索:

⑧ デフォルトアイコン

⑨ 編集 削除

⑩ 前のページ 1 次のページ

表 6-116 端末アイコン一覧に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	端末アイコン追加ボタン	新規に端末アイコンを追加します。ボタンを押下すると「(g)端末アイコン追加」に移動します。

項目番号	内容	説明
③	CSV 形式で保存ボタン	ボタンを押下すると、一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「maps_hosts_list.csv」になります。
④	CSV 形式からの端末アイコン追加ボタン	ボタンを押下すると、CSV 形式のファイルから端末アイコンを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑤	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑥	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/500 の 5 パターンです。
⑦	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑧	端末アイコン情報	端末アイコン情報の一覧を表示します。 表示項目は、アイコン/条件です。
⑨	操作	<p>操作として、編集/削除ボタンが表示され、以下に示す動作をおこないます。</p> <p>編集ボタンを押下すると「(h)端末アイコン編集」に移動します。</p> <p>削除ボタンを押下すると、</p> <p>端末アイコン            IP アドレス:&lt;IP アドレス&gt; MAC アドレス:&lt;MAC アドレス&gt; または,            IP アドレス:&lt;IP アドレス&gt; または,            MAC アドレス:&lt;MAC アドレス&gt; または,            エイリアス:&lt;エイリアス&gt; または,            ベンダ:&lt;ベンダ&gt; または,            MAC アドレス:&lt;MAC アドレス&gt;/&lt;マスク&gt;            を削除します</p> <p>の確認ダイアログを表示します。了承した場合、端末アイコンを削除します。削除が失敗すると、「表 6-117 端末アイコン一覧の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p>
⑩	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-117 端末アイコン一覧の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	指定した端末アイコンは存在しません	指定した端末アイコンは存在しません。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (g) 端末アイコン追加

図 6-78 端末アイコン追加画面

① トップ > 共通 > 端末アイコン一覧 > 端末アイコン追加

② IPアドレス

③ MACアドレス

④ マップに表示するエイリアス

⑤ ペント

⑥ MACアドレス / マスク

⑦ アイコン画像 登録済み画像から選択する：  
デフォルト端末アイコン

⑧ 追加

⑨ キャンセル

表 6-118 端末アイコン追加に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	端末個別指定	IP アドレス 端末アイコンに対応する IPv4 アドレスまたは IPv6 アドレスを入力します。 空白, 0.0.0.0~255.255.255.255, または::~ffff:ffff:ffff:ffff:ffff:ffff を入力してください。ただし, IPv6 リンクローカルアドレスは入力できません。 エイリアス指定とベンダ指定は同時に指定できません。
		MAC アドレス 端末アイコンに対応する MAC アドレスを入力します。 空白, または 0000.0000.0000~ffff.ffff.ffff を入力してください。 エイリアス指定とベンダ指定は同時に指定できません。
④	エイリアス指定	マップに表示するエイリアス 端末アイコンに対応するエイリアスを入力します。 「6.1.3(2)エイリアス」で登録したエイリアスを入力してください。 端末個別指定とベンダ指定は同時に指定できません。
⑤	ベンダ指定	ベンダ 端末アイコンに対応するベンダを入力します。 「6.1.3(1)端末一覧」に表示されるベンダを入力してください。 端末個別指定, エイリアス指定は同時に指定できません。また, ⑥も同時に指定できません。
⑥		MAC アドレス/マスク 端末アイコンに対応する MAC アドレス/マスクを入力します。 MAC アドレスは, 空白, または 0000.0000.0000~ffff.ffff.ffff を入力してください。 マスクは, 24, 28, 36 から選択してください。 端末個別指定, エイリアス指定は同時に指定できません。また, ⑤も同時に指定できません。
⑦	端末アイコン	アイコン画像 6.1.8(3)画像管理で管理している画像一覧から画像を設定します。画像名称を選択すると、選択した画像が表示されます。

項番	内容	説明
⑧	追加ボタン	端末アイコン追加を反映します。ボタンを押し下し、反映が成功すると、「(f)端末アイコン設定」に移動します。反映が失敗すると、「表 6-119 端末アイコン追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑨	キャンセルボタン	端末アイコン追加をキャンセルします。ボタンを押下すると、「(f)端末アイコン設定」に移動します。

表 6-119 端末アイコン追加の反映失敗時のダイアログ一覧

項番	内容	説明
1	いずれかのフィールドを入力してください	個別指定、エイリアス指定、またはベンダ指定を行ってください。
2	IP アドレスのフォーマットが間違っています	IP アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
3	IPv6 グローバルアドレスを入力してください	IPv6 リンクローカルアドレスが入力されています。IPv6 グローバルアドレスを入力してください。
4	MAC アドレスのフォーマットが間違っています	MAC アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
5	既に同じ条件が登録されています	指定した内容が重複しています。
6	画像が存在しません	指定した画像は存在しません。
7	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (h) 端末アイコン編集

図 6-79 端末アイコン編集画面

① パンくじ  
② IPアドレス  
③ MACアドレス  
④ マップに表示するエイリアス  
⑤ ペンダ  
⑥ MACアドレス / マスク  
⑦ アイコン画像  
⑧ 更新  
⑨ キャンセル

表 6-120 端末アイコン編集に表示する項目

項目番号	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。

項目番号	内容		説明
②	端末個別指定	IP アドレス	追加済みの端末アイコンに対応する IPv4 アドレスまたは IPv6 アドレスを入力します。 空白, 0.0.0.0~255.255.255.255, または::~ffff:ffff:ffff:ffff:ffff:ffff を入力してください。ただし, IPv6 リンクローカルアドレスは入力できません。 エイリアス指定とベンダ指定は同時に指定できません。
	MAC アドレス	MAC アドレス	追加済みの端末アイコンに対応する MAC アドレスを入力します。 空白, または 0000.0000.0000~ffff.ffff.ffff を入力してください。 エイリアス指定とベンダ指定は同時に指定できません。
④	エイリアス指定	マップに表示するエイリアス	追加済みの端末アイコンに対応するエイリアスを入力します。 「6.1.3(2)エイリアス」で登録したエイリアスを入力してください。 端末個別指定とベンダ指定は同時に指定できません。
⑤	ベンダ指定	ベンダ	追加済みの端末アイコンに対応するベンダを入力します。 「6.1.3(1)端末一覧」に表示されるベンダを入力してください。 端末個別指定, エイリアス指定は同時に指定できません。
	MAC アドレス/マスク	MAC アドレス/マスク	追加済みの端末アイコンに対応する MAC アドレス/マスクを入力します。 MAC アドレスは, 空白, または 0000.0000.0000~ffff.ffff.ffff を入力してください。 マスクは, 24, 28, 36 から選択してください。 ベンダ指定, 端末個別指定, エイリアス指定は同時に指定できません。
⑦	端末アイコン	アイコン画像	6.1.8(3)画像管理で管理している画像一覧から画像を設定します。画像名称を選択すると、選択した画像が表示されます。
⑧	追加ボタン		端末アイコン編集を反映します。ボタンを押し下し, 反映が成功すると, 「(f)端末アイコン設定」に移動します。反映が失敗すると, 「表 6-121 端末アイコン編集の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑨	キャンセルボタン		端末アイコン編集をキャンセルします。ボタンを押下すると, 「(f)端末アイコン設定」に移動します。

表 6-121 端末アイコン編集の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	いずれかのフィールドを入力してください	個別指定、エイリアス指定、またはベンダ指定を行ってください。
2	IP アドレスのフォーマットが間違っています	IP アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
3	IPv6 グローバルアドレスを入力してください	IPv6 リンクローカルアドレスが入力されています。IPv6 グローバルアドレスを入力してください。
4	MAC アドレスのフォーマットが間違っています	MAC アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
5	既に同じ条件が登録されています	指定した内容が重複しています。
6	画像が存在しません	指定した画像は存在しません。
7	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## 6.1.8 管理

### (1) 共通設定

図 6-80 共通設定画面 (1/3)

① トップ > 共通 > 共通設定

② ベーシック認証  
有効  無効

③ ユーザ名  
axsc

④ パスワード  
.....

⑤ 通信遮断  
有効  無効

⑥ 見出し  
該当端末の利用者は情報システム部(XXX-YYYY)まで連絡してください。

⑦ OID not increasingマーク無視  
有効  無効

⑧ 更新

図 6-81 共通設定画面 (2/3)

WAN接続ポート			
<p><b>WAN接続ポート追加</b> ⑩</p> <p>⑪ 表示カラム切替 ⑫ 25 件表示 ⑬ 検索: [ ]</p> <p>装置名称 ^ ポート番号 操作</p> <p>コアスイッチ1 0/1 削除 ⑯ ⑮</p> <p>1 件中 1 から 1 まで表示 ⑭</p> <p>前のページ 1 次のページ ⑯</p>			
永続設定ポート(受信側)			
<p><b>永続設定ポート(受信側)追加</b> ⑰</p> <p>⑱ 表示カラム切替 ⑲ 25 件表示 ⑳ 検索: [ ]</p> <p>セグメント名称 ^ 装置名称 ポート番号 操作</p> <p>無所属セグメント エッジスイッチ1 0/4 削除 ㉒</p> <p>1 件中 1 から 1 まで表示 ㉑</p> <p>前のページ 1 次のページ ㉓</p>			
永続設定ポート(送信側)			
<p><b>永続設定ポート(送信側)追加</b> ㉔</p> <p>㉕ 表示カラム切替 ㉖ 25 件表示 ㉗ 検索: [ ]</p> <p>セグメント名称 ^ 装置名称 ポート番号 操作</p> <p>無所属セグメント コアスイッチ1 0/5 削除 ㉙</p> <p>1 件中 1 から 1 まで表示 ㉘</p> <p>前のページ 1 次のページ ㉚</p>			
Syslog連携(CEF)のミラー先ポート			
<p><b>ミラー先ポート追加</b> ㉛</p> <p>装置名称 ポート番号</p> <p>コアスイッチ1 0/8 削除 ㉚ ㉜</p>			

図 6-82 共通設定画面 (3/3)



表 6-122 共通設定画面に表示する項目

項目番	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ベーシック認証	ベーシック認証選択ボタン	ベーシック認証として、Basic 認証の有効/無効を選択するボタンです。
③		ユーザ名	ベーシック認証として、Basic 認証のユーザ名を入力します。最大 256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。
④		パスワード	ベーシック認証として、Basic 認証のパスワードを入力します。最大 256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。
⑤		パスワード可視化オンオフボタン	ベーシック認証として、Basic 認証のパスワードの可視化のオンオフをおこないます。入力した Basic 認証のパスワードの文字列を確認したい場合に押下してください。再度押下すると、文字列を隠します。
⑥	エイリアス未登録端末	通信遮断	<p>エイリアス未登録端末の通信遮断の有効/無効を選択するボタンです。</p> <p>本機能は、下記いずれかの端末接続のエイリアス未登録接続を有効にし、かつ本機能の通信遮断を有効にした場合だけ、通信遮断がおこなわれます。</p> <ul style="list-style-type: none"> <li>・ Syslog サーバ           <ul style="list-style-type: none"> <li>「(2)(a) Syslog サーバ追加」</li> <li>「(2)(c) Syslog サーバ編集」</li> </ul> </li> <li>・ E-mail 通知先           <ul style="list-style-type: none"> <li>「(2)(d) E-mail 通知先追加」</li> <li>「(2)(f) E-mail 通知先編集」</li> </ul> </li> </ul>

項目番号	内容	説明	
⑦	遮断端末一覧	見出し	遮断端末一覧として、AX-Security-Controller(Viewer)の画面に表示する見出します。最大 256 文字登録可能です。なおアポストロフィー(‘)文字は使用しないでください。
⑧	装置情報収集	OID not increasing エラー無視	管理対象装置からの MIB 収集において、OID not increasing エラーが発生している場合にエラー無視の有効/無効を選択するボタンです。 OID not increasing エラー発生有無は、「6.1.4(1) 装置一覧」で確認することができます。
⑨	—	更新ボタン	ベーシック認証、端末接続と、遮断端末一覧の変更を反映します。
⑩	WAN 接続ポート	WAN 接続ポート追加ボタン	新規に WAN 接続ポートを追加します。ボタンを押下すると、「(a) WAN 接続ポート追加」に移動します。
⑪		表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑫		ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑬		検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑭		WAN 接続ポート情報	追加済みの WAN 接続ポート情報(装置名称、ポート番号)を表示します。
⑮		削除ボタン	WAN 接続ポート情報を削除します。ボタン押下時、  WAN 接続ポート 装置:<装置名称> ポート:<ポート番号> を削除します  の確認ダイアログを表示します。了承した場合、WAN 接続ポート情報を削除します。削除が失敗すると、「表 6-123 共通設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑯		ページ切替ボタン	ボタンを押下すると、指定のページを表示します。
⑰	永続設定ポート(受信側)	永続設定ポート(受信側)追加ボタン	新規に永続設定ポート(受信側)を追加します。ボタンを押下すると、「(b) 永続設定ポート(受信側)追加」に移動します。
⑱		表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑲		ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。

項目番号	内容	説明
⑯	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑰		永続設定ポート(受信側)情報
⑱		削除ボタン
⑲		永続設定ポート(受信側)情報を削除します。ボタン押下時、 永続設定ポート(受信側) 装置:<装置名称> ポート:<ポート番号> を削除します  の確認ダイアログを表示します。了承した場合、永続設定ポート(受信側)情報を削除します。削除が失敗すると、「表 6-123 共通設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑳		ページ切替ボタン
㉑		永続設定ポート(送信側)追加ボタン
㉒		表示カラム切替ボタン
㉓		ページあたり表示件数切替プルダウン
㉔		検索テキストボックス
㉕		永続設定ポート(送信側)情報を削除します。ボタン押下時、 永続設定ポート(送信側) 装置:<装置名称> ポート:<ポート番号> を削除します  の確認ダイアログを表示します。了承した場合、永続設定ポート(送信側)情報を削除します。削除が失敗すると、「表 6-123 共通設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
㉖		ページ切替ボタン

項目番号	内容	説明	
③①	Syslog 連携(CEF)のミラー先ポート	ミラー先ポート追加ボタン	新規に Syslog 連携(CEF)の詳細ミラー用のミラー先ポートを追加します。ボタンを押下すると、「(d) Syslog 連携(CEF)のミラー先ポート追加」に移動します。 追加済みのミラー先ポート数が収容条件の値と同じ場合、ボタンは押下できません。
③②		ミラー先ポート情報	追加済みの Syslog 連携(CEF)のミラー先ポート情報(装置名称、ポート番号)を表示します。
③③		削除ボタン	対象の Syslog 連携(CEF)のミラー先ポートを削除します。ボタンを押下すると、  ミラー先ポート 装置:<装置名称> ポート:<ポート番号> を削除します  の確認ダイアログを表示します。 了承した場合、ミラー先ポートを削除します。削除が失敗すると、「表 6-123 共通設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
③④	セキュリティフィルタ自動解除スケジュール	自動解除スケジュール追加ボタン	新規に自動解除スケジュールを追加します。ボタンを押下すると、「(e) セキュリティフィルタ自動解除スケジュール追加」に移動します。
③⑤		表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
③⑥		ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
③⑦		検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
③⑧		自動解除スケジュール情報	追加済みの自動解除スケジュール(セグメント名称、解除スケジュール、解除予定期時)を表示します。解除予定期時は、次回、自動解除スケジュールが動作する予定の日時を表示します。

項目番号	内容	説明
⑨	削除ボタン	対象の自動解除スケジュールを削除します。ボタンを押下すると、セキュリティフィルタ自動解除スケジュール <スケジュール単位><自動解除時刻>を削除します
⑩	ページ切替ボタン	確認ダイアログを表示します。 了承した場合、自動解除スケジュールを削除します。削除が失敗すると、「表 6-123 共通設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。

表 6-123 共通設定の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みの装置とポート番号の組み合わせです	既に削除済みの装置とポート番号の組み合わせです。
2	指定した WAN 接続ポートが存在しません	指定した WAN 接続ポートが存在しません。
3	指定した永続設定ポート(受信側)が存在しません	指定した永続設定ポート(受信側)が存在しません。
4	指定した永続設定ポート(送信側)が存在しません	指定した永続設定ポート(送信側)が存在しません。
5	指定したミラー先ポートが存在しません	指定したミラー先ポートが存在しません。
6	指定したスケジュールが存在しません	指定したセキュリティフィルタ自動解除スケジュールが存在しません。
7	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (a) WAN 接続ポート追加

図 6-83 WAN 接続ポート追加画面

表 6-124 WAN 接続ポート追加画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	装置	「6.1.4(1)(a) 装置追加」で登録した装置名称を入力してください。
③	ポート	WAN 接続ポートを入力してください。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>、または<switch no.>/<nif no.>/<port no.>となります。 装置モデルが AX620R の場合、トンネルインターフェース、またはサブインターフェースの名称を入力してください。
④	追加ボタン	WAN 接続ポート追加を反映します。ボタンを押下し、反映が成功すると、「(1) 共通設定」に移動します。反映が失敗すると、「表 6-125 WAN 接続ポート追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑤	キャンセルボタン	WAN 接続ポート追加をキャンセルします。ボタンを押下すると、「(1) 共通設定」に移動します。

表 6-125 WAN 接続ポート追加の反映失敗時のダイアログ一覧

項目番	内容	説明
1	装置名称を入力してください	装置名称を入力してください。
2	ポートを入力してください	ポートを入力してください。
3	存在しない装置名称です	存在しない装置名称です。
4	ポートのフォーマットが不正です	ポートのフォーマットが不正です。

項目番号	内容	説明
5	既に登録済みの装置とポート番号の組み合わせです。	既に登録済みの装置とポート番号の組み合わせです。
6	要求のパラメータに間違いがあるか、削除中の装置です。	要求のパラメータに間違いがあるか、削除中の装置です。「(6) メンテナンス」により保守情報を収集してください。
7	データベースのアクセスに失敗しました。	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (b) 永続設定ポート(受信側)追加

図 6-84 永続設定ポート(受信側)追加画面

表 6-126 永続設定ポート(受信側)追加画面に表示する項目

項目番号	内容	説明	
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。	
②	永続設定 ポート(受信 側)	装置	「6.1.4(1)(a) 装置追加」で登録した装置名称を入力してください。

項番	内容		説明
③		ポート	永続設定ポート(受信側)を入力してください。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>、または<switch no.>/<nif no.>/<port no.>となります。 装置モデルが AX620R の場合、サブインターフェースの名称を入力してください。
④	セグメント	セグメント 名称	セグメント名称を入力します。「6.1.5(1)(a) セグメント追加」で登録したセグメント名称、または無所属セグメントとしてください。「6.1.5(1)(b) セグメント設定」から移動した場合、セグメント名称は入力できません。
⑤	-	追加ボタン	永続設定ポート(受信側)追加を反映します。ボタンを押下し、反映が成功すると、呼び出し元の「(1) 共通設定」または「6.1.5(1)(b) セグメント設定」に移動します。反映が失敗すると、「表 6-127 永続設定ポート(受信側)追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
		キャンセル ボタン	永続設定ポート(受信側)追加をキャンセルします。ボタンを押下すると、「(1) 共通設定」に移動します。

表 6-127 永続設定ポート(受信側)追加の反映失敗時のダイアログ一覧

項番	内容	説明
1	装置名称を入力してください	装置名称を入力してください。
2	ポートを入力してください	ポートを入力してください。
3	存在しない装置名称です	存在しない装置名称です。
4	ポートのフォーマットが不正です	ポートのフォーマットが不正です。
5	指定したセグメントに登録済みの装置とポート番号の組み合わせです	指定したセグメントに登録済みの装置とポート番号の組み合わせです。
6	要求のパラメータに間違があるか、削除中の装置またはセグメントです。「(6) メンテナンス」により保守情報を収集してください。	要求のパラメータに間違があるか、削除中の装置またはセグメントです。「(6) メンテナンス」により保守情報を収集してください。
7	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (c) 永続設定ポート(送信側)追加

図 6-85 永続設定ポート(送信側)追加画面

表 6-128 永続設定ポート(送信側)追加画面に表示する項目

項目番	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	永続設定ポート(送信側)	装置	「6.1.4(1)(a) 装置追加」で登録した装置名称を入力してください。
③		ポート	永続設定ポート(送信側)を入力してください。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>、または<switch no.>/<nif no.>/<port no.>となります。 装置モデルが AX620R の場合、トンネルインターフェース、またはサブインターフェースの名称を入力してください。
④	セグメント		セグメント名称を入力します。「6.1.5(1)(a) セグメント追加」で登録したセグメント名称、または無所属セグメントとしてください。「6.1.5(1)(b) セグメント設定」から移動した場合、セグメント名称は入力できません。

項番	内容		説明
(5)	-	追加ボタン	永続設定ポート(送信側)追加を反映します。ボタンを押下し、反映が成功すると、呼び出し元の「(1) 共通設定」または「6.1.5(1)(b) セグメント設定」に移動します。反映が失敗すると、「表 6-129 永続設定ポート(送信側)追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
		キャンセルボタン	永続設定ポート(送信側)追加をキャンセルします。ボタンを押下すると、「(1) 共通設定」に移動します。

表 6-129 永続設定ポート(送信側)追加の反映失敗時のダイアログ一覧

項番	内容	説明
1	装置名称を入力してください	装置名称を入力してください。
2	ポートを入力してください	ポートを入力してください。
3	存在しない装置名称です	存在しない装置名称です。
4	ポートのフォーマットが不正です	ポートのフォーマットが不正です。
5	指定したセグメントに登録済みの装置とポート番号の組み合わせです	指定したセグメントに登録済みの装置とポート番号の組み合わせです。
6	要求のパラメータに間違があるか、削除中の装置またはセグメントです。「(6) メンテナンス」により保守情報を収集してください。	要求のパラメータに間違があるか、削除中の装置またはセグメントです。「(6) メンテナンス」により保守情報を収集してください。
7	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (d) Syslog 連携(CEF)のミラー先ポート追加

図 6-86 Syslog 連携(CEF)のミラー先ポート追加画面



表 6-130 Syslog 連携(CEF)のミラー先ポート追加画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	装置	「6.1.4(1)(a) 装置追加」で登録した装置名称を入力してください。
③	ポート	Syslog 連携(CEF)の詳細ミラー用のミラー先ポートを入力してください。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>, または<switch no.>/<nif no.>/<port no.>となります。
④	追加ボタン	ミラー先ポート追加を反映します。ボタンを押下し, 反映が成功すると, 「(1) 共通設定」に移動します。反映が失敗すると, 「表 6-131 Syslog 連携(CEF)のミラー先ポート追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑤	キャンセルボタン	Syslog 連携(CEF)のミラー先ポート追加をキャンセルします。ボタンを押下すると, 「(1) 共通設定」に移動します。

表 6-131 Syslog 連携(CEF)のミラー先ポート追加の反映失敗時のダイアログ一覧

項目番	内容	説明
1	装置名称を入力してください	装置名称を入力してください。
2	ポートを入力してください	ポートを入力してください。
3	存在しない装置名称です	存在しない装置名称です。
4	ポートのフォーマットが不正です	ポートのフォーマットが不正です。

項目番号	内容	説明
5	既に登録済みの装置とポート番号の組み合わせです。	既に登録済みの装置とポート番号の組み合わせです。
6	ミラー先ポートが既に 5 ポート設定されています	ミラー先ポートが既に 5 ポート設定されています
7	要求のパラメータに間違いがあるか、削除中の装置です	要求のパラメータに間違いがあるか、削除中の装置です。「(6) メンテナンス」により保守情報を収集してください。
8	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (e) セキュリティフィルタ自動解除スケジュール追加

図 6-87 セキュリティフィルタ自動解除スケジュール追加画面

①

セキュリティフィルタ自動解除スケジュール追加

自動解除スケジュール

スケジュール単位 ② 毎日  
毎週 月 曜日  
毎月 1 日

自動解除時刻 ③ 00 : 10

セグメント

セグメント名称 ④ 無所属セグメント

⑤ 追加 ⑥ キャンセル

表 6-132 セキュリティフィルタ自動解除スケジュール追加画面に表示する項目

項目番	内容		説明	
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。	
②	自動解除スケジュール	スケジュール単位	スケジュール単位を以下より選択します。 ・毎日 ・毎週の指定曜日 ・毎月の指定日 毎週の指定曜日の場合、月～日のいずれかの曜日を選択してください。 毎月の指定日の場合、1～31 の範囲で選択、または入力してください。	
			自動解除時刻	
③	セグメント		自動解除を実施する日時を指定します。	
④	セグメント名		セグメント名称を入力します。「6.1.5(1)(a) セグメント追加」で登録したセグメント名称、または無所属セグメントとしてください。「6.1.5(1)(b) セグメント設定」から移動した場合、セグメント名称は入力できません。	
⑤	-	追加ボタン	自動解除スケジュールを反映します。ボタンを押下し、反映が成功すると、呼び出し元の「(1) 共通設定」または「6.1.5(1)(b) セグメント設定」に移動します。反映が失敗すると、「表 6-133 セキュリティフィルタ自動解除スケジュール追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。	
⑥		キャンセルボタン	自動解除スケジュールをキャンセルします。ボタンを押下すると、「(1) 共通設定」に移動します。	

表 6-133 セキュリティフィルタ自動解除スケジュール追加の反映失敗時のダイアログ一覧

項目番	内容	説明
1	日付が入力されていません	日付が入力されていません。1～31 の範囲で、選択、または入力してください。
2	範囲外の日付です	範囲外の日付です。1～31 の範囲で、選択、または入力してください。
3	指定セグメントにセキュリティフィルタ自動解除スケジュールが既に 1 スケジュール設定されています。	指定したセグメントにセキュリティフィルタ自動解除スケジュールが既に 1 スケジュール設定されています。

項目番号	内容	説明
4	要求のパラメータに間違いがあります	要求のパラメータに間違いがあります。「(6) メンテナンス」により保守情報を収集してください。
5	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (2) 通知設定

図 6-88 通知設定画面

通知設定

Syslog通知

② 表示カラム切替	③ 25 件表示	④ 検索:				
⑤ サーバ名	IPアドレス	ポート番号	通信種別	ファシリティ	通知	コメント
⑥ Syslogサーバ	198.51.100.250	514	UDP	local0	有効	

E-mail通知

⑩ 表示カラム切替	⑪ 25 件表示	⑫ 検索:			
⑬ 通知先名	サーバ情報	ポート番号	暗号化種別	通知	コメント
⑭ E-mailサーバ	smtp.example.com	587	TLS(SMTP STARTTLS)	有効	

表 6-134 通知設定画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	Syslog 通知 Syslog サーバ追加ボタン	新規に Syslog サーバを追加します。ボタンを押下すると「(a) Syslog サーバ追加」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「managements_notification_syslog.csv」となります。
④	CSV 形式からの Syslog サーバ追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上の Syslog サーバを追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑤	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑥	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑦	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑧	Syslog サーバ情報	Syslog サーバ情報の一覧を表示します。表示項目は、サーバ名称/IP アドレス/ポート番号/通信種別/ファシリティ/通知/コメントです。 Syslog サーバのエントリを押下すると、「(b) Syslog サーバ詳細」に移動します。
⑨	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。
⑩	E-mail 通知 E-mail 通知先追加ボタン	新規に E-mail 通知先を追加します。ボタンを押下すると「(d) E-mail 通知先追加」に移動します。
⑪	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「managements_notification_email.csv」となります。
⑫	CSV 形式からの E-mail 通知先追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上の E-mail 通知先を追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。
⑬	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。

項目番号	内容	説明
⑭	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑮	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑯	E-mail 通知先情報	E-mail 通知先情報の一覧を表示します。表示項目は、通知先名称/サーバ情報/ポート番号/暗号化種別/通知/コメントです。E-mail 通知先のエントリを押下すると、「(e) E-mail 通知先詳細」に移動します。
⑰	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

## (a) Syslog サーバ追加

図 6-89 Syslog サーバ追加画面

Syslog サーバ追加

Syslog サーバ情報

② サーバ名称	Syslog サーバ
③ IP アドレス	198.51.100.250
④ ポート番号	514
⑤ 通信種別	UDP
⑥ ファシリティ	local0
⑦ 通知	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
⑧ コメント	

syslog 通知種別

⑨ インシデント情報連携	<input checked="" type="checkbox"/> 手動選択 <input checked="" type="checkbox"/> 通信遮断 <input checked="" type="checkbox"/> 詳細ミラー
⑩ セキュリティファイアウォール接続	<input checked="" type="checkbox"/> 登録 <input checked="" type="checkbox"/> 設定完了 <input checked="" type="checkbox"/> 削除完了 <input checked="" type="checkbox"/> 端末毎設定 <input type="checkbox"/> 端末毎設定完了 <input checked="" type="checkbox"/> 端末毎設定失敗 <input type="checkbox"/> 端末毎削除要因 <input type="checkbox"/> 完了 <input type="checkbox"/> 失敗
⑪ 端末接続	<input type="checkbox"/> エイリアス未登録接続
⑫ 管理対象装置関連	<input type="checkbox"/> コンフィグ <input type="checkbox"/> 容量監視

⑬ 追加 ⑭ キャンセル

表 6-135 Syslog サーバ追加画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。

項目番号	内容	説明
②	サーバ名称	Syslog サーバ情報としてサーバの名称を示す文字列です。最大 256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。
③	IP アドレス	Syslog サーバの IP アドレスを入力します。IP アドレスは 0.0.0.0～255.255.255.255 を入力してください。
④	ポート番号	Syslog サーバのポート番号を入力します。ポート番号は、0～65535 を入力してください。
⑤	通信種別	Syslog 通知の通信種別を選択します。 ・ UDP
⑥	ファシリティ	Syslog 通知メッセージのファシリティの種別を選択します。以下のいずれかです。 ・ local0 ・ local1 ・ local2 ・ local3 ・ local4 ・ local5 ・ local6 ・ local7 ・ user
⑦	通知の有効/無効選択ボタン	Syslog サーバへの通知の有効/無効を選択するボタンです。
⑧	コメント	Syslog サーバ情報として、Syslog 出力先サーバの説明を記載する文字列です。0～256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。
⑨	インシデント情報連携	インシデント情報連携によりセキュリティフィルタが設定されたときに、Syslog 通知を行うインシデントの種別を選択します。以下を複数選択できます。 ・ 手動選択 ・ 通信遮断 ・ 詳細ミラー
⑩	セキュリティフィルタ関連	セキュリティフィルタの追加、更新、削除契機に、Syslog 通知を行うセキュリティフィルタ関連の種別を選択します。以下を複数選択できます。 ・ 登録 ・ 設定完了 ・ 削除完了 ・ 端末毎設定要因 ・ 端末毎設定完了 ・ 端末毎設定失敗 ・ 端末毎削除要因
⑪	端末接続	端末接続を契機に、Syslog 通知を行う端末関連の種別を選択します。以下を選択できます。 ・ エイリアス未登録接続
⑫	管理対象装置関連	管理対象装置に関する Syslog 通知の種別を選択します。以下を選択できます。 ・ コンフィグ容量監視

項目番号	内容	説明
⑯	追加ボタン	Syslog サーバ追加を反映します。ボタンを押下し、反映が成功すると、「(2) 通知設定」に移動します。反映が失敗すると、「表 6-136 Syslog サーバ追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑰	キャンセルボタン	Syslog サーバ追加をキャンセルします。ボタンを押下すると、「(2) 通知設定」に移動します。

表 6-136 Syslog サーバ追加の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	サーバ名称が入力されていません	サーバ名称が入力されていません。サーバ名称を入力してください。
2	IP アドレスが入力されていません	IP アドレスが入力されていません。IP アドレスを入力してください。
3	IP アドレスのフォーマットが間違っています	IP アドレスのフォーマットが間違っています。正しいフォーマットで入力してください。
4	ポート番号が入力されていません	ポート番号が入力されていません。ポート番号を入力してください。
5	範囲外のポート番号です	ポート番号が範囲外です。0~65535 の範囲で入力してください。
6	既に追加済みのサーバ名称です	既に追加済みのサーバ名称です。
7	Syslog サーバが既に 10 個登録されています	Syslog サーバが既に 10 個登録されています。
8	要求パラメータに間違いがあります	要求のパラメータに間違いがあります。「(6) メンテナンス」により保守情報を収集してください。
9	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (b) Syslog サーバ詳細

図 6-90 Syslog サーバ詳細画面



表 6-137 Syslog サーバ詳細画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	設定変更ボタン	Syslog サーバの設定を変更します。ボタンを押下すると「(c) Syslog サーバ編集」に移動します。
③	Syslog サーバ削除ボタン	操作として、Syslog サーバの削除を行います。ボタンを押下すると、 Syslog サーバ <サーバ名称> (IP:<IP アドレス>) を削除します  の確認ダイアログを表示します。了承した場合、 Syslog サーバを削除します。削除が失敗すると、 「表 6-138 Syslog サーバ詳細の反映失敗時の ダイアログ一覧」に示すダイアログを表示しま す。

項目番号	内容	説明
④	Syslog サーバ情報	Syslog サーバ情報を表示します。 表示項目は、サーバ名称/IP アドレス/ポート番号/ 通信種別/ファシリティ/通知/コメントです。
⑤	Syslog 通知種別	Syslog 通知種別を表示します。 表示項目は、インシデント情報連携/セキュリ ティフィルタ関連/端末接続/管理対象装置関連で す。

表 6-138 Syslog サーバ詳細の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	指定した Syslog サーバが存在しま せん	既に削除済みの Syslog サーバです。
2	データベースのア クセスに失敗しま した	データベースのアクセスに失敗しました。「(6) メン テナンス」により保守情報を収集してください。

## (c) Syslog サーバ編集

図 6-91 Syslog サーバ編集画面

**Syslog Server Information**

- ① ページヘッダー: トップ > 共通 > 通知設定 > Syslogサーバー(IP:198.51.100.250) > Syslogサーバー編集
- ② サーバ名: Syslogサーバー
- ③ IPアドレス: 198.51.100.250
- ④ ポート番号: 514
- ⑤ 通信種別: UDP
- ⑥ ファシリティ: local0
- ⑦ 通知: 有効 (選択済)
- ⑧ コメント: (空)

**syslog Notification Type**

- ⑨ インシデント情報連携: 手動選択 (選択済), 通信遮断 (選択済), 詳細ミラー (選択済)
- ⑩ セキュリティフィルタ関連: 登録 (選択済), 設定完了 (選択済), 削除完了 (選択済)  
要因: 端末毎設定 (選択済), 完了 (選択済), 失敗 (選択済)  
要因: 端末毎削除 (未選択), 要因 (未選択)
- ⑪ 端末接続: エイリアス (未選択), 未登録接続 (未選択)
- ⑫ 管理対象: コンフィグ (未選択)  
装置関連: 容量監視 (未選択)

ボタン: 更新 (青いボタン), キャンセル (赤いボタン)

表 6-139 Syslog サーバ編集画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。

項目番号	内容	説明
②	サーバ名/IP アドレス/ポート番号/通信種別/ファシリティ	Syslog サーバ情報として、登録済みのサーバ名/IP アドレス/ポート番号/通信種別/ファシリティを表示します。
③	通知の有効/無効選択ボタン	Syslog サーバへの通知の有効/無効を選択するボタンです。
④	コメント	Syslog サーバ情報として、Syslog サーバの説明を記載する文字列です。0~256 文字登録可能です。なおアポストロフィー('')文字は使用しないでください。
⑤	インシデント情報連携	インシデント情報連携によりセキュリティフィルタが設定されたときに、Syslog 通知を行うインシデントの種別を選択します。以下を複数選択できます。 ・手動選択 ・通信遮断 ・詳細ミラー
⑥	セキュリティフィルタ関連	セキュリティフィルタの追加、更新、削除契機に、Syslog 通知を行うセキュリティフィルタ関連の種別を選択します。以下を複数選択できます。 ・登録 ・設定完了 ・削除完了 ・端末毎設定要因 ・端末毎設定完了 ・端末毎設定失敗 ・端末毎削除要因
⑦	端末接続	端末接続を契機に、Syslog 通知を行う端末関連の種別を選択します。以下を選択できます。 ・エイリアス未登録接続
⑧	管理対象装置関連	管理対象装置に関する Syslog 通知の種別を選択します。以下を選択できます。 ・コンフィグ容量監視
⑨	更新ボタン	Syslog サーバ編集を反映します。ボタンを押下し、反映が成功すると、「(b) Syslog サーバ詳細」に移動します。反映が失敗すると、「表 6-140 Syslog サーバ編集の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑩	キャンセルボタン	Syslog サーバ編集をキャンセルします。ボタンを押下すると、「(b) Syslog サーバ詳細」に移動します。

表 6-140 Syslog サーバ編集の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	要求のパラメータに間違があるか、指定した Syslog サーバが存在しません	要求のパラメータに間違があるか、指定した Syslog サーバが存在しません。「(6) メンテナンス」により保守情報を収集してください。

項目番号	内容	説明
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (d) E-mail 通知先追加

図 6-92 E-mail 通知先追加画面 (1/2)

図 6-92 E-mail 通知先追加画面 (1/2)

E-mail通知先追加

E-mail通知先情報

② 通知先名称	E-mailサーバ
③ サーバ情報	smtp.example.com
④ ポート番号	
⑤ 暗号化種別	TLS(SMTP STARTTLS)
⑥ 認証	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
⑦ 認証ユーザ名	axsc
⑧ パスワード	..... <input type="button" value="目"/>
⑩ 通知	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
⑪ コメント	

メールアドレス情報

⑫ 宛先メールアドレス(To)	manager@example.com
⑬ 宛先メールアドレス(Cc)	
⑭ 宛先メールアドレス(Bcc)	
⑮ 差出人メールアドレス(From)	axsc@example.com
<input type="button" value="テストメール送信"/>	

図 6-93 E-mail 通知先追加画面 (2/2)

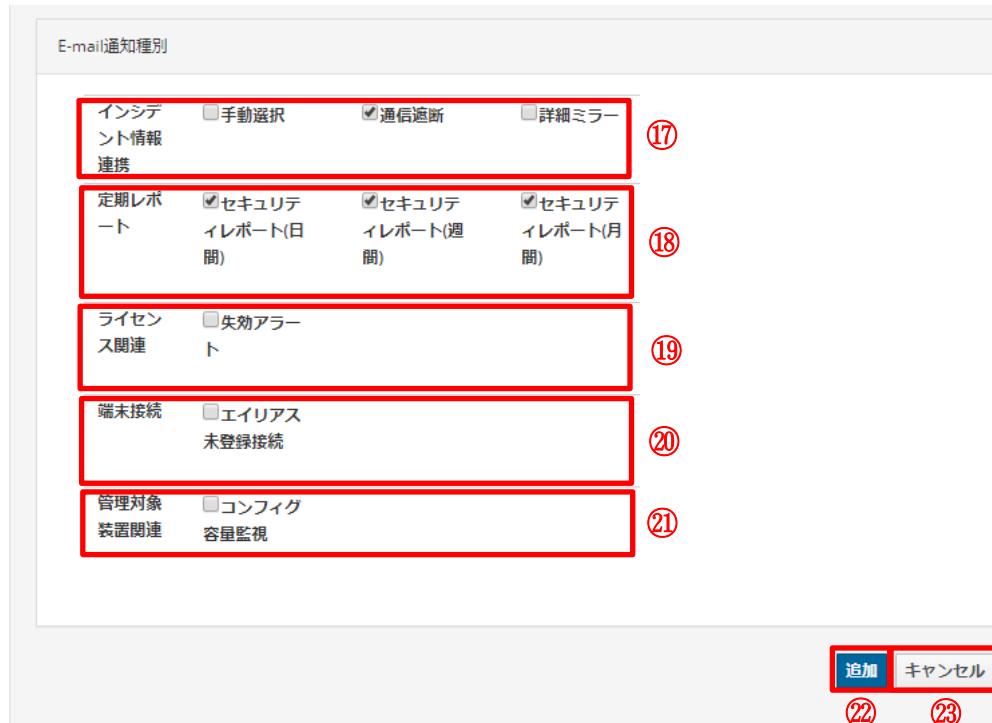


表 6-141 E-mail 通知先追加画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	E-mail 通知先情報	E-mail 通知先情報として通知先の名称を示す文字列です。最大 256 文字登録可能です。
③	サーバ情報	E-mail 通知先の FQDN を入力します。
④	ポート番号	E-mail 通知先のポート番号を入力します。 ポート番号は、0~65535 を入力してください。 ポート番号が未入力の場合、暗号化種別により、下記の値となります <ul style="list-style-type: none"> <li>なし(SMTP)の場合: 25</li> <li>TLS(SMTP STARTTLS)の場合: 587</li> <li>SSL(SMTPS)の場合: 465</li> </ul>
⑤	暗号化種別	E-mail 通知先の暗号化種別を選択します。 <ul style="list-style-type: none"> <li>なし(SMTP)</li> <li>TLS(SMTP STARTTLS)</li> <li>SSL(SMTPS)</li> </ul>
⑥	認証の有効/無効選択ボタン	E-mail 通知先の認証の有効/無効を選択するボタンです。

項目番号	内容	説明
⑦	認証ユーザ名	認証有効時、E-mail通知先の認証に使用するユーザ名を入力します。
⑧	パスワード	認証有効時、E-mail通知先の認証に使用するパスワードを入力します。
⑨	パスワード可視化オンオフボタン	パスワードの可視化のオンオフをおこないます。入力したパスワードの文字列を確認したい場合に押下してください。再度押下すると、文字列を隠します。
⑩	通知の有効/無効選択ボタン	E-mail通知先への通知の有効/無効を選択するボタンです。
⑪	コメント	E-mail通知先情報として、E-mail通知先の説明を記載する文字列です。0～256文字登録可能です。
⑫	メールアドレス情報	宛先メールアドレス(To) Toに使用する宛先メールアドレスを入力します。複数指定する際は、コンマ(,)で区切って入力してください。
⑬		宛先メールアドレス(Cc) Ccに使用する宛先メールアドレスを入力します。複数指定する際は、コンマ(,)で区切って入力してください。
⑭		宛先メールアドレス(Bcc) Bccに使用する宛先メールアドレスを入力します。複数指定する際は、コンマ(,)で区切って入力してください。
⑮	差出人メールアドレス(From)	Fromに使用する差出人メールアドレスを入力します。
⑯	テストメール送信ボタン	E-mail通知先へのアクセスが可能か確認することができます。 ボタンを押下すると、テストメールの送信をおこない、以下のいずれかを表示します。  [送信成功時] テストメールの送信に成功しました(<暗号化通信>) [送信失敗時] テストメールの送信に失敗しました(<失敗要因>)  <暗号化通信> ・暗号化通信無効 ・暗号化通信有効(SMTP STARTTLS) ・暗号化通信有効(SMTPS) <失敗要因> ・サーバ情報/ポート番号不正 ・サーバアクセス失敗 ・認証ユーザ名/パスワード不正 ・サーバ側送信処理失敗 ・メールアドレス不正 ・内部エラー

項目番号	内容	説明
⑯	E-mail 通知種別	インシデント情報連携によりセキュリティフィルタが設定されたときに、E-mail 通知を行うインシデントの種別を選択します。以下を複数選択できます。 ・手動選択 ・通信遮断 ・詳細ミラー
⑰	定期レポート	定期レポートの種別を選択します。以下を複数選択できます。 ・セキュリティレポート(日間) ・セキュリティレポート(週間) ・セキュリティレポート(月間)
⑱	ライセンス関連	ライセンス関連の種別を選択します。以下を選択できます。 ・失効アラート
⑲	端末接続	端末接続の種別を選択します。以下を選択できます。 ・エイリアス未登録接続
⑳	管理対象装置関連	管理対象装置関連の種別を選択します。以下を選択できます。 ・コンフィグ容量監視
㉑	追加ボタン	E-mail 通知先追加を反映します。ボタンを押下し、反映が成功すると、「(2) 通知設定」に移動します。反映が失敗すると、「表 6-142 E-mail 通知先追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
㉒	キャンセルボタン	E-mail 通知先追加をキャンセルします。ボタンを押下すると、「(2) 通知設定」に移動します。

表 6-142 E-mail 通知先追加の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	通知先名称が入力されていません	通知先名称が入力されていません。通知先名称を入力してください。
2	サーバ情報が入力されていません	サーバ情報が入力されていません。サーバ情報を入力してください。
3	範囲外のポート番号です	ポート番号が範囲外です。0~65535 の範囲で入力してください。
4	宛先メールアドレス(To)が入力されていません	宛先メールアドレス(To)が入力されていません。宛先メールアドレス(To)を入力してください。
5	差出人メールアドレス(From)が入力されていません	差出人メールアドレスが入力されていません。差出人メールアドレスを入力してください。
6	既に追加済みの通知先名称です	既に追加済みの通知先名称です。

項目番号	内容	説明
7	E-mail 通知先が既に 10 個登録されています	E-mail 通知先が既に 10 個登録されています。
8	要求パラメータに間違いがあるか、メールアドレス情報が不正です	要求のパラメータに間違いがあるか、メールアドレス情報が不正です。メールアドレス情報が不正でない場合、「(6) メンテナンス」により保守情報を収集してください。
9	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (e) E-mail 通知先詳細

図 6-94 E-mail 通知先詳細画面

① トップ > 共通 > 通知設定 > E-mailサーバ(サーバ:smtp.example.com)

② 設定変更

③ E-mail通知先削除

④

⑤

⑥

通知先名称	E-mailサーバ
サーバ情報	smtp.example.com
ポート番号	587
暗号化種別	TLS(SMTP STARTTLS)
認証	無効
通知	有効
コメント	

メールアドレス情報	
宛先メールアドレス(To)	manager@example.com
宛先メールアドレス(Cc)	
宛先メールアドレス(Bcc)	
差出人メールアドレス(From)	axsc@example.com

E-mail通知種別	
インシデント情報連携	通信遮断
定期レポート	セキュリティレポート(日間)/セキュリティレポート(週間)/セキュリティレポート(月間)
ライセンス関連	
端末接続	
管理対象装置関連	

表 6-143 E-mail 通知先詳細画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	設定変更ボタン	E-mail 通知先の設定を変更します。ボタンを押下すると「(f) E-mail 通知先編集」に移動します。
③	E-mail 通知先削除ボタン	操作として、E-mail 通知先の削除を行います。ボタンを押下すると、 E-mail 通知先 <通知先名称> (サーバ:<サーバ情報>) を削除します  の確認ダイアログを表示します。了承した場合、E-mail 通知先を削除します。削除が失敗すると、「表 6-144 E-mail 通知先詳細の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
④	E-mail 通知先情報	E-mail 通知先情報を表示します。 表示項目は、通知先名称/サーバ情報/ポート番号/暗号化種別/認証/通知/コメントです。
⑤	メールアドレス情報	メールアドレス情報を表示します。 表示項目は、宛先メールアドレス(To)/宛先メールアドレス(Cc)/宛先メールアドレス(Bcc)/差出人メールアドレスです。
⑥	E-mail 通知種別	E-mail 通知種別を表示します。 表示項目は、インシデント情報連携/定期レポート/ライセンス関連/端末接続/管理対象装置関連です。

表 6-144 E-mail 通知先詳細の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	指定した E-mail 通知先が存在しません	既に削除済みの E-mail 通知先です。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (f) E-mail 通知先編集

図 6-95 E-mail 通知先編集画面 (1/2)

**E-mail通知先情報**

② 通知先名称	E-mailサーバ
③ サーバ情報	smtp.example.com
④ ポート番号	587
⑤ 暗号化種別	TLS(SMTP STARTTLS)
⑥ 認証	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
⑦ 認証ユーザ名	axsc
⑧ パスワード	..... <span style="border: 1px solid black; padding: 2px;">⑨</span>
⑩ 通知	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
⑪ コメント	

**メールアドレス情報**

⑫ 宛先メールアドレス(To)	manager@example.com
⑬ 宛先メールアドレス(Cc)	
⑭ 宛先メールアドレス(Bcc)	
⑮ 差出人メールアドレス(From)	axsc@example.com <span style="border: 1px solid black; padding: 2px;">⑯ テストメール送信</span>

図 6-96 E-mail 通知先編集画面 (2/2)

E-mail通知種別

インシデント情報連携	<input type="checkbox"/> 手動選択	<input checked="" type="checkbox"/> 通信遮断	<input type="checkbox"/> 詳細ミラー	(17)
定期レポート	<input checked="" type="checkbox"/> セキュリティレポート(日間)	<input checked="" type="checkbox"/> セキュリティレポート(週間)	<input checked="" type="checkbox"/> セキュリティレポート(月間)	(18)
ライセンス関連	<input type="checkbox"/> 失効アラート			(19)
端末接続	<input type="checkbox"/> エイリアス未登録接続			(20)
管理対象装置関連	<input type="checkbox"/> コンフィグ容量監視			(21)

更新 (22) キャンセル (23)

表 6-145 E-mail 通知先編集画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	E-mail 通知先情報	E-mail 通知先情報として、登録済みの通知先の名称を表示します。
③		E-mail 通知先の FQDN を入力します。
④		E-mail 通知先のポート番号を入力します。 ポート番号は、0~65535 を入力してください。
⑤		E-mail 通知先の暗号化種別を選択します。 ・なし(SMTP) ・TLS(SMTP STARTTLS) ・SSL(SMTPS)
⑥	認証の有効/無効選択ボタン	E-mail 通知先の認証の有効/無効を選択するボタンです。
⑦	認証ユーザ名	認証有効時、E-mail 通知先の認証に使用するユーザ名を入力します。
⑧	パスワード	認証有効時、E-mail 通知先の認証に使用するパスワードを入力します。

項目番号	内容	説明
⑨	メールアドレス情報	パスワード可視化オンオフボタン パスワードの可視化のオンオフをおこないます。入力したパスワードの文字列を確認したい場合に押下してください。再度押下すると、文字列を隠します。
⑩		通知の有効/無効選択ボタン E-mail 通知先への通知の有効/無効を選択するボタンです。
⑪		コメント E-mail 通知先情報として、E-mail 通知先の説明を記載する文字列です。0～256 文字登録可能です。
⑫		宛先メールアドレス(To) To に使用する宛先メールアドレスを入力します。複数指定する際は、コンマ(,)で区切って入力してください。
⑬		宛先メールアドレス(Cc) Cc に使用する宛先メールアドレスを入力します。複数指定する際は、コンマ(,)で区切って入力してください。
⑭		宛先メールアドレス(Bcc) Bcc に使用する宛先メールアドレスを入力します。複数指定する際は、コンマ(,)で区切って入力してください。
⑮		差出人メールアドレス(From) From に使用する差出人メールアドレスを入力します。
⑯		テストメール送信ボタン E-mail 通知先へのアクセスが可能か確認することができます。 ボタンを押下すると、テストメールの送信をおこない、以下のいずれかを表示します。  [送信成功時] テストメールの送信に成功しました(<暗号化通信>) [送信失敗時] テストメールの送信に失敗しました(<失敗要因>)  <暗号化通信> ・暗号化通信無効 ・暗号化通信有効(SMTP STARTTLS) ・暗号化通信有効(SMTPS) <失敗要因> ・サーバ情報/ポート番号不正 ・サーバアクセス失敗 ・認証ユーザ名/パスワード不正 ・サーバ側送信処理失敗 ・メールアドレス不正 ・内部エラー

項目番号	内容	説明	
⑯	E-mail 通知種別	インシデント情報連携	インシデント情報連携によりセキュリティフィルタが設定されたときに、E-mail 通知を行うインシデントの種別を選択します。以下を複数選択できます。 ・手動選択 ・通信遮断 ・詳細ミラー
⑰	定期レポート	定期レポート	定期レポートの種別を選択します。以下を複数選択できます。 ・セキュリティレポート(日間) ・セキュリティレポート(週間) ・セキュリティレポート(月間)
⑱	ライセンス関連	ライセンス関連	ライセンス関連の種別を選択します。以下を選択できます。 ・失効アラート
⑲	端末接続	端末接続	端末接続の種別を選択します。以下を選択できます。 ・エイリアス未登録接続
⑳	管理対象装置関連	管理対象装置関連	管理対象装置関連の種別を選択します。以下を選択できます。 ・コンフィグ容量監視
㉑	—	更新ボタン	E-mail 通知先編集を反映します。ボタンを押下し、反映が成功すると、「(e) E-mail 通知先詳細」に移動します。反映が失敗すると、「表 6-146 E-mail 通知先編集の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
㉒	キャンセルボタン	キャンセルボタン	E-mail 通知先追加をキャンセルします。ボタンを押下すると、「(e) E-mail 通知先詳細」に移動します。

表 6-146 E-mail 通知先編集の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	サーバ情報が入力されていません	サーバ情報が入力されていません。サーバ情報を入力してください。
2	範囲外のポート番号です	ポート番号が範囲外です。0~65535 の範囲で入力してください。
3	宛先メールアドレス(To)が入力されていません	宛先メールアドレス(To)が入力されていません。宛先メールアドレス(To)を入力してください。
4	差出人メールアドレス(From)が入力されていません	差出人メールアドレスが入力されていません。差出人メールアドレスを入力してください。
5	指定した E-mail 通知先が存在しません	指定した E-mail 通知先が存在しません。

項目番号	内容	説明
6	要求のパラメータに間違いがあるか、メールアドレス情報が不正です	要求のパラメータに間違いがあるか、メールアドレス情報が不正です。メールアドレス情報が不正でない場合、「(6) メンテナンス」により保守情報を収集してください。
7	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

### (3) 画像管理

図 6-97 画像管理画面

The screenshot shows the 'Image Management' page with the following numbered elements:

- ① Top navigation bar: トップ > 共通 > 画像管理
- ② 'Image Management' title
- ③ 'Image Add' button
- ④ 'CSV Format Save' button
- ⑤ 'Image Import from CSV' button
- ⑥ 'Image Save' button
- ⑦ 'Column Switch' button
- ⑧ '件表示' (Item Display) dropdown set to 25
- ⑨ 'Search' input field
- ⑩ List of icons with details:
 

画像名称	画像	画像ファイル名	操作
ALAXALA		ALAXALA.jpg	<span>登録画像変更</span> <span>削除</span>
デフォルト端末アイコン		default_host_icon.png	
デフォルト集線装置アイコン		default_hub_icon.png	
端末アイコン(サーバ)		preset_host_server_icon.png	
端末アイコン(デスクトップPC)		preset_host_desktop_icon.png	
集線装置アイコン(無線AP)		preset_hub_icon.png	
- ⑪ 'Register Image Change' and 'Delete' buttons in the '操作' column
- ⑫ Page navigation: 前のページ [1] 次のページ

表 6-147 画像管理画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。

項目番号	内容	説明
②	画像追加ボタン	新規に画像を追加します。ボタンを押下すると「(a)画像追加」に移動します。
③	CSV 形式で保存ボタン	ボタンを押下すると、一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「managements_image_list.csv」になります。
④	CSV 形式からの画像追加ボタン	ボタンを押下すると、CSV 形式のファイルから 1 個以上の画像を追加することができます。指定するファイルは、「CSV 形式で保存」したファイルとしてください。 画像ファイルは⑥、または「(b)登録画像変更」から登録してください。
⑤	画像保存ボタン	ボタンを押下すると、一覧で表示した画像ファイルを ZIP 形式でダウンロードできます。ファイル名は「managements_images.zip」になります。
⑥	ZIP 形式からの一括画像追加ボタン	ボタンを押下すると、ZIP 形式のファイルから 1 個以上の画像ファイルを追加することができます。画像追加に使用可能なファイルの条件を満たしたファイルを指定してください。  画像追加に使用可能なファイルの条件は以下です。 <ul style="list-style-type: none"><li>・画像が ZIP 形式で圧縮されていること。</li><li>・ディレクトリ構造がないこと。</li><li>・10MB 以下であること。10MB を超える場合は、複数のファイルに分けて、複数回おこなってください。</li><li>・画像として使用可能な条件を満たしていること。</li></ul> 画像として使用可能な条件は以下です。 <ul style="list-style-type: none"><li>・画像のフォーマットは、JPEG, GIF, PNG であること。</li><li>・画像のファイル名は、拡張子を含む最大 255 文字であること。ファイル名に使用できる文字は、1 バイト文字で、1 文字目が英数字で、2 文字目以降が英数字とハイフン (-), アンダースコア (_) , ピリオド (.) であること。また、画像管理に登録されたファイル名であること。</li></ul>
⑦	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑧	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/500 の 5 パターンです。
⑨	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑩	画像情報	管理画像の一覧を表示します。 表示項目は、画像名称/画像/画像ファイル名です。

項番	内容	説明
⑪	操作	<p>操作として、登録画像変更/削除ボタンが表示され、以下に示す動作をおこないます。</p> <p>登録画像変更ボタンを押下すると「(b)登録画像変更」に移動します。</p> <p>削除ボタンを押下すると、</p> <p>画像 &lt;画像名称&gt; を削除します</p> <p>の確認ダイアログを表示します。了承した場合、画像を削除します。削除が失敗すると、「表 6-148 画像管理の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p>
⑫	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-148 画像管理の反映失敗時のダイアログ一覧

項番	内容	説明
1	指定した画像は存在しません	画像名称を入力してください。
2	指定した画像はアイコンとして使用されています。 削除する場合は、アイコンとしての使用をやめてから削除してください。	指定した画像はアイコンとして使用されています。 削除する場合は、アイコンとしての使用をやめてから削除してください。
3	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (a) 画像追加

図 6-98 画像追加画面

図 6-98 画像追加画面

表 6-149 画像追加画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	画像情報	画像の名称を示す文字列です。最大 256 文字登録可能です。なおアポストロフィー(')文字は使用しないでください。
③	画像：新たに画像ファイルをアップロードする	ウェブブラウザが動作している環境で管理している画像ファイルをアップロードし、アイコンとして使用する画像として追加します。 「ファイルを選択ボタン」、または、「参照…ボタン」を押下し、ファイルを選択します。選択したファイルを取り消す場合は、「選択ファイルをクリア」ボタンを押下します。 使用可能な画像のフォーマットは、JPEG, GIF, PNG です。 使用可能な画像のファイル名は、拡張子を含み最大 255 文字です。ファイル名に使用できる文字は、1 バイト文字で、1 文字目が英数字、2 文字目以降が英数字とハイフン (-)、アンダースコア (_)、ピリオド (.) です。
④	追加ボタン	画像追加を反映します。ボタンを押下し、反映が成功すると、「(3)画像管理」に移動します。反映が失敗すると、「表 6-150 画像追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。

項目番号	内容		説明
⑤	キャンセルボタン		画像追加をキャンセルします。ボタンを押下すると、「(3)画像管理」に移動します。

表 6-150 画像追加の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	画像を指定してください	画像を指定してください。
2	既に登録済みの画像名称です	既に登録済みの画像名称です。
3	画像名称を入力してください	画像名称を入力してください。
4	画像のファイル名に使用できる文字は1文字目が英数字で2文字目以降が英数字とハイフン(-), アンダースコア(_) , ピリオド(.) です	画像ファイルのファイル名に使用できる文字は1文字目が英数字で2文字目以降が英数字とハイフン(-), アンダースコア(_) , ピリオド(.) です
5	指定可能なファイル形式は(JPG, GIF, PNG)です	画像ファイルの指定可能なファイル形式は(JPG, GIF, PNG)です
6	指定可能なファイルサイズは最大500KBです	画像ファイルの指定可能なファイルサイズは最大500KBです。
7	ファイル名が長すぎます	画像ファイルのファイル名が長すぎます。
8	既に使用されているファイル名です	既に使用されているファイル名です。異なる画像ファイルの場合は、ファイル名を変更してください。
9	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (b) 登録画像変更

図 6-99 登録画像変更画面



表 6-151 登録画像変更画面に表示する項目

項目番	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	画像情報	画像名称	追加済みの画像の名称を示す文字列です。最大256文字登録可能です。なおアポストロフィー(')文字は使用しないでください。
③		画像	追加済みの画像を表示します。 ④で画像を選択した場合は、④で選択した画像が優先されます。

項番	内容	説明
④	画像：新たに画像ファイルをアップロードする	<p>ウェブブラウザが動作している環境で管理している画像ファイルをアップロードし、アイコンとして使用する画像として追加します。</p> <p>「ファイルを選択ボタン」、または、「参照…ボタン」を押下し、ファイルを選択します。選択したファイルを取り消す場合は、「選択ファイルをクリア」ボタンを押下します。</p> <p>使用可能な画像のフォーマットは、JPEG, GIF, PNG です。</p> <p>使用可能な画像のファイル名は、拡張子を含み最大 255 文字です。ファイル名に使用できる文字は、1 バイト文字で、1 文字目が英数字、2 文字目以降が英数字とハイフン (-)、アンダースコア (_)、ピリオド (.) です。</p>
⑤	更新ボタン	画像変更を反映します。ボタンを押下し、反映が成功すると、「(3)画像管理」に移動します。反映が失敗すると、「表 6-152 登録画像変更の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑥	キャンセルボタン	画像変更をキャンセルします。ボタンを押下すると、「(3)画像管理」に移動します。

表 6-152 登録画像変更の反映失敗時のダイアログ一覧

項番	内容	説明
1	画像を指定してください	画像を指定してください。
2	既に登録済みの画像名称です	既に登録済みの画像名称です。
3	画像名称を入力してください	画像名称を入力してください。
4	画像のファイル名に使用できる文字は1文字目が英数字で2文字目以降が英数字とハイフン (-)、アンダースコア (_)、ピリオド (.) です	画像ファイルのファイル名に使用できる文字は1文字目が英数字で2文字目以降が英数字とハイフン (-)、アンダースコア (_)、ピリオド (.) です
5	指定可能なファイル形式は(JPG, GIF, PNG)です	画像ファイルの指定可能なファイル形式は(JPG, GIF, PNG)です
6	指定可能なファイルサイズは最大 500KB です	画像ファイルの指定可能なファイルサイズは最大 500KB です。
7	ファイル名が長すぎます	画像ファイルのファイル名が長すぎます。

項目番号	内容	説明
8	既に使用されているファイル名です	既に使用されているファイル名です。異なる画像ファイルの場合は、ファイル名を変更してください。
9	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

#### (4) レポート

図 6-100 レポート画面(1/2)

The screenshot displays two stacked report pages from the AX-Security-Controller(Manager) web interface.

**Top Report (月間レポート):**

- ①:** Breadcrumbs: トップ > 共通 > レポート
- ②:** Section title: 月間レポート
- ③:** Button: 選択レポート削除
- ④:** Input: 表示カラム切替 (dropdown menu), 25 件表示
- ⑤:** Input: 検索
- ⑥:** Input: チェックボックス (checkboxes)
- ⑦:** Input: チェックボックス (checkboxes)
- ⑧:** Input: 期間 (date range: 2018/11/02 ~ 2018/11/30)
- ⑨:** Button: レポート出力
- ⑩:** Buttons: 前のページ, 1, 次のページ
- Text: 1 件中 1 から 1 まで表示

**Bottom Report (週間レポート):**

- ⑪:** Section title: 週間レポート
- ⑫:** Button: 選択レポート削除
- ⑬:** Input: 表示カラム切替 (dropdown menu), 25 件表示
- ⑭:** Input: 検索
- ⑮:** Input: チェックボックス (checkboxes)
- ⑯:** Input: チェックボックス (checkboxes)
- ⑰:** Table rows (8 items):
 

2018/10/29～2018/11/04	通知済み
2018/11/05～2018/11/11	通知済み
2018/11/12～2018/11/18	通知済み
2018/11/19～2018/11/25	通知済み
2018/11/26～2018/12/02	通知済み
2018/12/03～2018/12/09	通知済み
2018/12/10～2018/12/16	通知済み
2018/12/17～2018/12/23	通知済み
- ⑱:** Buttons: レポート出力 (repeated 8 times)
- ⑲:** Buttons: 前のページ, 1, 次のページ
- Text: 8 件中 1 から 8 まで表示

図 6-101 レポート画面 (2/2)

The screenshot shows a report list titled '日間レポート' (①). At the top right are buttons for '選択レポート削除' (②), '表示カラム切替' (③), '件表示' (④), and a search field '検索:' (⑤). Below these are columns for '期間' (Period), 'E-mail通知状態' (Email Notification Status), and '操作' (Operations). The main area displays a table with 10 rows, each containing a checkbox (⑥), a date (⑦), and a status (⑧). The last row is highlighted with a red box (⑨). To the right of the table is a vertical column of 'レポート出力' (Report Output) buttons (⑩). Navigation buttons at the bottom include '前のページ' (Previous Page) and '次のページ' (Next Page).

期間	E-mail通知状態	操作
2018/11/01	通知済み	レポート出力
2018/11/02	通知済み	レポート出力
2018/11/03	通知済み	レポート出力
2018/11/04	通知済み	レポート出力
2018/11/05	通知済み	レポート出力
2018/11/06	通知済み	レポート出力
2018/11/07	通知済み	レポート出力
2018/11/08	通知済み	レポート出力
2018/11/09	通知済み	レポート出力
2018/11/10	通知済み	レポート出力

表 6-153 E-mail 通知先編集画面に表示する項目

項目番	内容		説明
①	階層リンク		現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	月間レポート	選択レポート削除ボタン	個別選択チェックボックスで選択した月間レポート情報を削除します。ボタン押下時、 選択したレポートを削除します  の確認ダイアログを表示します。了承した場合、月間レポート情報を削除します。削除が失敗すると、「表 6-154 レポートの反映失敗時のダイアログ一覧」に示すダイアログを表示します。
③	表示カラム切替ボタン		一覧から不要なカラムを非表示にすることができます。

項目番号	内容	説明
④	ページあたり表示件数切替プルダウン 検索テキストボックス 全選択チェックボックス 個別選択チェックボックス 月間レポート情報 レポート出力ボタン ページ切替ボタン 週間レポート削除ボタン 表示カラム切替ボタン ページあたり表示件数切替プルダウン 検索テキストボックス	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑤		テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑥		すべての月間レポート情報を削除対象とします。もう一度選択すると、すべての月間レポート情報を削除対象から外します。
⑦		選択した月間レポート情報を削除対象とします。もう一度選択すると、削除対象から外します。
⑧		月間レポート情報を表示します。 表示項目は、期間/E-mail 通知状態です。 E-mail 通知状態： 未通知/通知済み/通知中/通知失敗
⑨		ボタンを押下すると、レポート内容をテキスト形式でダウンロードできます。ファイル名は「report_<期間 1>_<期間 2>.txt」となります。 <期間 1>, <期間 2>は YYYYMMDD の形式です。 YYYY : 4 術の西暦 MM : 2 術の月 DD : 2 術の日
⑩		ボタンを押下すると、指定のページを表示します。
⑪		個別選択チェックボックスで選択した週間レポート情報を削除します。ボタン押下時、  選択したレポートを削除します  の確認ダイアログを表示します。了承した場合、週間レポート情報を削除します。削除が失敗すると、「表 6-154 レポートの反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑫		一覧から不要なカラムを非表示することができます。
⑬		1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑭		テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。

項目番号	内容	説明
⑯	全選択チェックボックス	すべての週間レポート情報を削除対象とします。もう一度選択すると、すべての週間レポート情報を削除対象から外します。
⑰	個別選択チェックボックス	選択した週間レポート情報を削除対象とします。もう一度選択すると、削除対象から外します。
⑱	週間レポート情報	週間レポート情報を表示します。 表示項目は、期間/E-mail 通知状態です。 E-mail 通知状態： 未通知/通知済み/通知中/通知失敗
⑲	レポート出力ボタン	ボタンを押下すると、レポート内容をテキスト形式でダウンロードできます。ファイル名は「report_<期間 1>_<期間 2>.txt」となります。 <期間 1>, <期間 2>は YYYYMMDD の形式です。 YYYY : 4 術の西暦 MM : 2 術の月 DD : 2 術の日
⑳	日間レポート	選択レポート削除ボタン  個別選択チェックボックスで選択した日間レポート情報を削除します。ボタン押下時、  選択したレポートを削除します  の確認ダイアログを表示します。了承した場合、日間レポート情報を削除します。削除が失敗すると、「表 6-154 レポートの反映失敗時のダイアログ一覧」に示すダイアログを表示します。
㉑	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
㉒	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
㉓	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
㉔	全選択チェックボックス	すべての日間レポート情報を削除対象とします。もう一度選択すると、すべての日間レポート情報を削除対象から外します。
㉕	個別選択チェックボックス	選択した日間レポート情報を削除対象とします。もう一度選択すると、削除対象から外します。

項目番号	内容	説明
⑯	日間レポート情報	日間レポート情報を表示します。 表示項目は、期間/E-mail 通知状態です。 E-mail 通知状態： 未通知/通知済み/通知中/通知失敗
⑰	レポート出力ボタン	ボタンを押下すると、レポート内容をテキスト形式でダウンロードできます。ファイル名は「report_<期間>.txt」となります。 <期間>は YYYYMMDD の形式です。 YYYY : 4 術の西暦 MM : 2 術の月 DD : 2 術の日
⑱	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-154 レポートの反映失敗時のダイアログ一覧

項目番号	内容	説明
1	レポートが選択されていません	レポートが選択されていません。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (5) ライセンス

図 6-102 ライセンス画面

① リンク: トップ > 共通 > ライセンス

② テーブル: ライセンス情報

機能	基本部 Syslog連携(CEF)
最大装置管理数	130 台
最大ワイヤレス LAN コントローラ管理数	0 台

③ ボタン: 機能ライセンス追加

④ リスト: ライセンス種別

ライセンス種別	シリアル番号	有効期限
■ 基本部		2020/05/01 08:59:59 JST
■ 管理対象スイッチ拡張 + 20台		2020/05/01 08:59:59 JST
■ 管理対象スイッチ拡張 + 100台		2020/05/01 08:59:59 JST
■ Syslog連携(CEF)		2020/05/01 08:59:59 JST

⑤ ボタン: ベンダ編集

⑥ ボタン: 延長ライセンス追加

⑦ ボタン: 機能ライセンス削除

表 6-155 ライセンス画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ライセンス情報	<p>現在の有効なライセンス情報を表示します。</p> <ul style="list-style-type: none"> <li>機能           <ul style="list-style-type: none"> <li>基本部</li> <li>ワイヤレス LAN コントローラ</li> <li>トレンドマイクロ DDI/TMPM 連携</li> <li>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</li> <li>Syslog 連携(CEF)</li> </ul> </li> <li>最大装置管理数</li> <li>有効な最大装置管理数</li> <li>最大ワイヤレス LAN コントローラ管理数</li> <li>有効な最大ワイヤレス LAN コントローラ管理数</li> </ul>
③	機能ライセンス追加ボタン	機能ライセンスを追加します。ボタンを押下すると、「(a) 機能ライセンス追加」に移動します。

項目番号	内容	説明
④	機能ライセンス情報	機能ライセンス情報の一覧を表示します。 表示項目は、ライセンス種別/シリアル番号/有効期間です。
⑤	ベンダ編集ボタン	対象の外部連携ライセンスのベンダ情報を編集します。ボタンを押下すると、「0 ベンダ編集」に移動します。
⑥	延長ライセンス追加ボタン	対象の機能ライセンスの期間を延長します。ボタンを押下すると、「(b) 延長ライセンス追加」に移動します。
⑦	機能ライセンス削除ボタン	対象の機能ライセンスを削除します。ボタンを押下すると、  機能ライセンス <機能ライセンス> を削除します  の確認ダイアログを表示します。 了承した場合、機能ライセンスを削除します。削除が失敗すると、「表 6-156 ライセンスの反映失敗時のダイアログ一覧」に示すダイアログを表示します。

表 6-156 ライセンスの反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みのライセンスです	既に削除済みのライセンスです。
2	指定したライセンスが存在しません	指定したライセンスが存在しません。
3	要求のパラメータに間違があります	要求のパラメータに間違があります。「(6) メンテナンス」により保守情報を収集してください。
4	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (a) 機能ライセンス追加

図 6-103 機能ライセンス画面

トップ > 共通 > ライセンス > 機能ライセンス追加 ①

機能ライセンス

ライセンス追加

ライセンスキー ②

追加 ③ キャンセル ④

表 6-157 機能ライセンス画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ライセンスキー	ライセンスキーを入力します。 ライセンスキーは、0~9, a~f を4桁ごとにハイフン (-) で区切った形式の、39文字の文字列で構成されます。ただし、ハイフン (-) をすべて省略して、32文字の文字列としても入力できます。
③	追加ボタン	機能ライセンス追加を反映します。ボタンを押下すると  機能ライセンス を追加します  の確認ダイアログを表示します。了承し、反映が成功すると、「(5) ライセンス」に移動します。反映が失敗すると、「表 6-158 機能ライセンスの反映失敗時のダイアログ一覧」に示すダイアログを表示します。
④	キャンセルボタン	機能ライセンス追加をキャンセルします。ボタンを押下すると、「(5) ライセンス」に移動します。

表 6-158 機能ライセンスの反映失敗時のダイアログ一覧

項目番	内容	説明
1	ライセンスキーを入力してください。	ライセンスキーを入力してください。
2	既に登録済みのライセンスです。	既に登録済みのライセンスです。
3	要求のパラメータに間違いがあるか不正なライセンスキーです。	要求のパラメータに間違いがあるか不正なライセンスキーです。

項目番号	内容	説明
4	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (b) 延長ライセンス追加

図 6-104 延長ライセンス画面

① トップ > 共通 > ライセンス > 延長ライセンス追加

② ライセンス種別: 基本部  
シリアル番号: \*\*\*\*  
有効期限: 2019/09/01 08:59:59 JST

③ ライセンスキー (Red box highlights this table area)

④ 追加 (Add button)  
⑤ キャンセル (Cancel button)

表 6-159 延長ライセンス画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ライセンス種別/シリアル番号/有効期限	延長対象ライセンスとして、ライセンス種別/シリアル番号/有効期限を表示します。

項目番号	内容	説明
③	ライセンスキー	ライセンスキーを入力します。 ライセンスキーは、0~9, a~f を4桁ごとにハイフン (-) で区切った形式の、39文字の文字列で構成されます。ただし、ハイフン (-) をすべて省略して、32文字の文字列としても入力できます。 最大10個、入力することが可能です。
④	追加ボタン	延長ライセンス追加を反映します。ボタンを押下すると  機能ライセンス <機能ライセンス> に延長ライセンスを追加します  の確認ダイアログを表示します。了承し、反映が成功すると、「(5) ライセンス」に移動します。反映が失敗すると、「表 6-160 延長ライセンスの反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑤	キャンセルボタン	延長ライセンス追加をキャンセルします。ボタンを押下すると、「(5) ライセンス」に移動します。

表 6-160 延長ライセンスの反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に登録済みのライセンスです	既に登録済みのライセンスです。
2	要求のパラメータに間違があるか不正なライセンスキーです	要求のパラメータに間違があるか不正なライセンスキーです
3	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

## (c) ベンダ編集

図 6-105 ベンダ編集

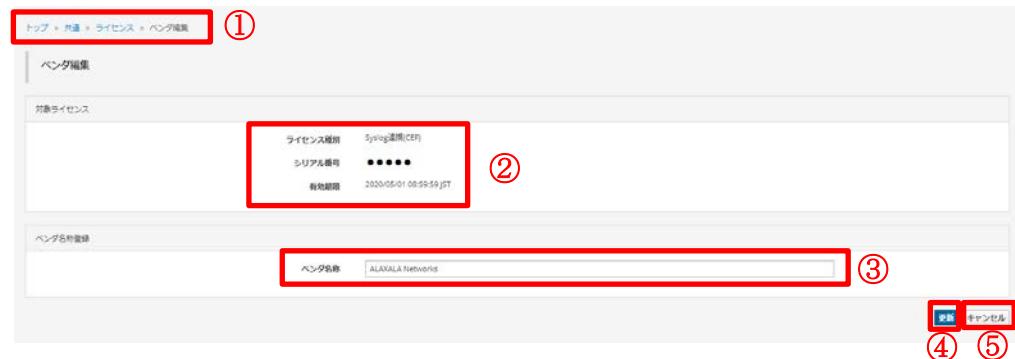


表 6-161 ベンダ編集画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ライセンス種別/シリアル番号/有効期限	対象ライセンスとして、ライセンス種別/シリアル番号/有効期限を表示します。
③	ベンダ名称	ベンダ名称を入力します。 ベンダ名称を示す文字列です。最大 256 文字登録可能です。連携対象装置が出力する Syslog の「Device Vendor」フィールドに設定される名称を設定します。なお、「ALAXALA Networks Corporation」は設定できません。
④	更新ボタン	ベンダ情報を反映します。ボタンを押下すると機能ライセンス <機能ライセンス> にベンダ情報を追加します  の確認ダイアログを表示します。了承し、反映が成功すると、「(5) ライセンス」に移動します。反映が失敗すると、「表 6-162 ベンダ編集の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑤	キャンセルボタン	ベンダ編集をキャンセルします。ボタンを押下すると、「(5) ライセンス」に移動します。

表 6-162 ベンダ編集の反映失敗時のダイアログ一覧

項目番	内容	説明
1	要求のパラメータに間違いがあります	ベンダ名称に誤りがあるか、要求のパラメータに間違いがあります。「(6) メンテナンス」により保守情報を収集してください。

項目番号	内容	説明
2	既に削除済みのライセンスです。	既に削除済みのライセンスです。
3	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「(6) メンテナンス」により保守情報を収集してください。

#### (d) ライセンス期限失効アラート

ライセンスが失効する3か月前に、画面上に失効アラートを表示します。失効するライセンスごとに表示します。

図 6-106 ライセンス期限失効アラート

The screenshot shows the 'ダッシュボード' (Dashboard) page of the AX-Security-Controller(Manager) web interface. At the top, two red-bordered alert boxes are displayed:

- ① 管理対象スイッチ拡張 +100台ライセンスが2017/12/01 08:59:59 JSTに失効します
- ① 基本部ライセンスが2017/12/01 08:59:59 JSTに失効します

Below the alerts, the dashboard summary is shown:

セグメント	状態	カウント
端末	⚠️	4
装置	⚠️	1
セキュリティ装置連携	✅	0

Each segment has a circular progress bar indicating the status distribution:

- 端末:** 11 (緑)
- 装置:** 4 (青)
- セキュリティ装置連携:** 5 (緑)

Legend for the status distribution bars:

- 緑: 正常
- オレンジ: 遅延中
- 青: メンテナンス中
- オレンジ: 状態不明
- 赤: ライセンス上限オーバー
- 緑: 設定済
- オレンジ: 設定中

Below the dashboard, a section titled 'セキュリティフィルタ実行情報 (最新10件)' (Security Filter Execution Information (Latest 10 items)) displays a table of recent security filter executions:

登録日時	種別	セキュリティフィルタ条件	状態	連携機能	遮断理由	要求元IPアドレス
2017/09/05 18:29:33 JST	通信遮断	送信元IP:10.0.10.106/32宛先IP:0.0.0.0/0	設定済み	Palo Alto Networks連携		10.200.0.10
2017/09/05 18:23:17 JST	詳細ミラード	送信元IP:10.0.10.106/32宛先IP:0.0.0.0/0	設定済み	Palo Alto Networks連携		10.200.0.10
2017/09/05 14:58:16 JST	通信遮断	送信元IP:10.0.10.100/32宛先IP:0.0.0.0/0	設定済み	手動追加		10.200.7.7
2017/09/04 17:11:30 JST	通信遮断	送信元IP:10.0.10.102/32宛先IP:0.0.0.0/0	設定済み	Palo Alto Networks連携		10.200.7.7
2017/09/04 17:11:16 JST	通信遮断	送信元IP:10.0.10.101/32宛先IP:0.0.0.0/0	設定済み	TMPM連携		10.200.7.7

表 6-163 ライセンス失効アラートに表示する項目

項目番	内容	説明
①	失効アラート表示	「<ライセンス名>が<時刻>に失効します」 <ライセンス名>が失効する<時刻>を表示します。  <ライセンス名>：ライセンス失効対象ライセンス名 <時刻>：ライセンス失効時刻

## (6) メンテナンス

図 6-107 メンテナンス画面

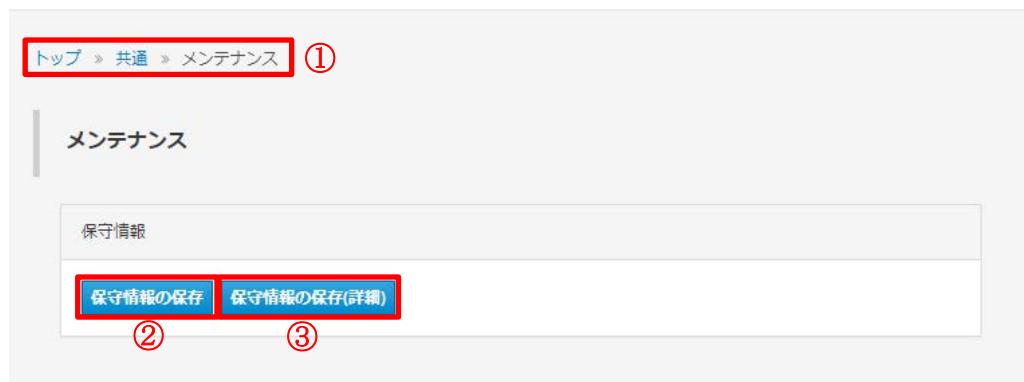


表 6-164 メンテナンス画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	保守情報の保存ボタン	ボタンを押下すると、保守情報をダウンロードします。ファイル名は「managements_showtech.zip」となります。
③	保守情報の保存(詳細)ボタン	ボタンを押下すると、保守情報(詳細)をダウンロードします。ファイル名は「managements_showtech_detail.zip」となります。保守情報(詳細)には、AX-Security-Controller で管理するエイリアス等の情報を含みます。

## (7) TMPM 連携

「6.2 TMPM 連携」を参照してください。

**(8) 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**

「6.3 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」を参照してください。

## 6.2 TMPM 連携

TMPM 連携の Web インタフェースを説明します。

ライセンス「外部連携トレンドマイクロ DDI/TMPM との連携」が有効な場合に、利用可能です。

### 6.2.1 ナビゲーションバー

図 6-108 ナビゲーションバー

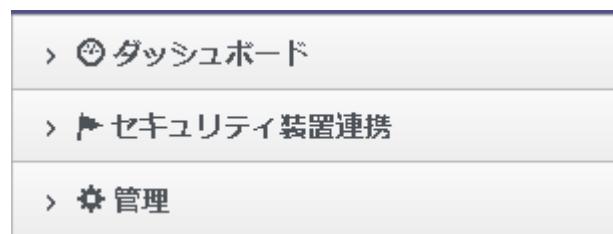


表 6-165 ナビゲーションバーより移動可能な機能の一覧

項目	機能	説明	参照先
ダッシュボード	—	最新 10 件のセキュリティフィルタを表示します。	6.2.2
セキュリティ装置連携	セキュリティフィルター一覧	セキュリティ装置から通知されたセキュリティフィルタの一覧を表示します。	6.2.3
管理	TMPM 連携設定	TMPM 連携の設定をおこないます。	6.2.4

### 6.2.2 ダッシュボード

図 6-109 ダッシュボード画面

ダッシュボード画面には、ナビゲーションメニュー、セキュリティフィルタ実行情報の一覧表示、操作ボタンがあります。各要素は赤枠で囲まれています。

- ナビゲーションメニュー: トップ > TMPM連携 > ダッシュボード (①)
- 操作ボタン: 更新 (②)
- セキュリティフィルタ実行情報 (最新10件): 表示 (③)

登録日時	種別	セキュリティフィルタ条件	状態	要求元IPアドレス
2017/09/04 17:11:16 JST	通信遮断	送信元IP:10.0.10.101/32宛先IP:0.0.0.0/0	設定済み	10.200.7.7

表 6-166 ダッシュボード画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	更新ボタン	ボタン押下で画面を更新します。
③	セキュリティフィルタ実行情報	最新 10 件のセキュリティフィルタを表示します。

### 6.2.3 セキュリティ装置連携

#### (1) セキュリティフィルター一覧

図 6-110 セキュリティフィルター一覧画面

The screenshot shows the 'Security Filter List' page. At the top, there's a breadcrumb navigation: 'トップ > TMPM連携 > セキュリティフィルター一覧'. Below it is a search bar labeled '検索:' with a red box around it. To the left of the search bar is a button labeled '選択セキュリティフィルタの解除' with a red box around it. Next to the search bar are buttons for '表示カラム切替' (red box), '件表示' (blue box), and a dropdown menu set to '25' (red box). On the right side of the search bar is a red box around the '検索:' input field.

登録日時	種別	セキュリティフィルタ条件	状態
2018/11/05 18:29:17 JST	詳細ミラー	送信元:198.51.100.51/32 宛先:0.0.0.0/0	設定済み
2018/11/05 18:31:38 JST	例外通信許可	送信元:198.51.100.52/32 宛先:198.51.100.201/32	設定済み
2018/11/05 18:33:07 JST	通信遮断	送信元:198.51.100.53/32 宛先:198.51.100.202/32	設定済み
2018/11/05 18:33:47 JST	通信遮断	送信元:198.51.100.54/32 宛先:0.0.0.0/0	設定済み

At the bottom, there's a message '4 件中 1 から 4 まで表示' and a navigation bar with buttons for '前のページ' (red box), '1' (blue box), and '次のページ' (red box).

表 6-167 セキュリティフィルター一覧画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。

項目番号	内容	説明
②	選択セキュリティフィルタの解除ボタン	ボタンを押下すると、選択したセキュリティフィルタを解除します(<チェック数>件)。セキュリティフィルタが解除されるまで時間がかかる場合があります。の確認ダイアログを表示します。了承した場合、実行する場合は YES と入力してください。の確認ダイアログを表示します。YES を入力して了承した場合、選択した個別選択チェックボックスのセキュリティフィルタ*について、セキュリティフィルタを解除します。反映が失敗すると、「表 6-58 選択セキュリティフィルタ解除の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
③	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
④	ページあたり表示件数切替プルダウントラック	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑤	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑥	全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべてのセキュリティフィルタをセキュリティフィルタ解除対象とします。もう一度選択すると、すべてのセキュリティフィルタ解除対象から外します。
⑦	個別選択チェックボックス	選択したセキュリティフィルタをセキュリティフィルタ解除対象とします。もう一度選択すると、セキュリティフィルタ解除対象から外します。
⑧	セキュリティフィルタ情報	セキュリティフィルタ情報の一覧を表示します。表示項目は、登録日時/種別/セキュリティフィルタ条件/状態/要求元 IP アドレスです。セキュリティフィルタ情報を押下すると、「(2) セキュリティフィルタ詳細」画面に移動します。
⑨	ページ切替ボタン	ボタンを押下すると指定のページを表示します。

## 注※

任意のセキュリティフィルタの個別選択チェックボックスが選択された状態で、検索テキストボックスで絞り込みをおこない、該当セキュリティフィルタが表示されない場合でも、該当セキュリティフィルタはセキュリティフィルタ解除対象のままです。この状態でボタンを押下すると、該当セキュリティフィルタのセキュリティフィルタ解除が実施されることに注意してください。

個別選択チェックボックスの選択は、検索テキストボックスで絞り込みをおこなった後におこなうようにしてください。

## (2) セキュリティフィルタ詳細

図 6-111 セキュリティフィルタ詳細画面

① ページヘッダー: トップ > TMPM連携 > セキュリティフィルター観 > 送信元IP:10.0.10.53/32宛先IP:0.0.0.0/0通信遮断

② セキュリティフィルタ情報: 登録日時 2018/04/23 16:04:35 JST、状態 設定済み、要求元IPアドレス 172.17.0.254、セキュリティフィルタ条件 送信元IP:10.0.10.53/32宛先IP:0.0.0.0/0通信遮断、種別 過信遮断

③ 端末情報: 端末MACアドレス 0000.5e00.5353[ICANN, IANA Department]

④ 表示カラム切替ボタン

⑤ ページ数表示: 25件表示

⑥ 検索ボックス

⑦ テーブルヘッダー: 設定 対象 端末IPアドレス 装置番号 ポート番号 ポート番号 方向 アクセスリスト名称 検出シーケンス番号 検出条件 定状況 追加要因 コンフィグ定義登録日時 コンフィグ適用日時 削除原因 削除日時

設定	対象	端末IPアドレス	装置番号	ポート番号	ポート番号	方向	アクセスリスト名称	検出シーケンス番号	検出条件	定状況	追加要因	コンフィグ登録日時	コンフィグ適用日時	削除原因	削除日時
端末	接続	10.0.10.53	エジス	0/1	10.0.10.53	受信側	AUTO_ACL_IPV4_IN_0_1	300000	deny ip host any	設定済み	セキュリティフィルタ登録	2018/04/23 16:04:37	2018/04/23 16:04:49	JST	JST

1件中 1 から 1 まで表示

⑧ ページナビゲーション: 前のページ | 次のページ

表 6-168 セキュリティフィルタ詳細画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	セキュリティフィルタ情報	セキュリティフィルタ情報として、登録日時/状態/要求元IPアドレス/セキュリティフィルタ条件/種別を表示します。
③	端末情報	端末情報として、端末MACアドレスを表示します。および、[]内にMACアドレッサンプルを表示します。
④	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
⑤	ページあたり表示件数切替プルダウン	1ページあたりに表示する件数を切り替えることができます。件数のパターンは10/25/50/100/全ての5パターンです。
⑥	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。

項目番号	内容	説明
⑦	コンフィグ内容	コンフィグ内容の一覧を表示します。 表示項目は、「表 6-61 セキュリティフィルタ詳細画面に表示する項目」を参照してください。
⑧	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

## 6.2.4 管理

### (1) TMPM 連携

図 6-112 TMPM 連携設定画面



表 6-169 TMPM 連携設定画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ミラー先ポート追加ボタン	新規に詳細ミラー用のミラー先ポートを追加します。ボタンを押下すると、「(a) ミラー先ポート追加」に移動します。 追加済みのミラー先ポート数が収容条件の値と同じ場合、ボタンは押下できません。
③	ミラー先ポート情報	追加済みのミラー先ポート情報(装置名称、ポート番号)を表示します。

項目番号	内容	説明
④	削除ボタン	対象のミラー先ポートを削除します。ボタンを押下すると、 ミラー先ポート 装置:<装置名称> ポート:<ポート番号> を削除します  の確認ダイアログを表示します。 了承した場合、ミラー先ポートを削除します。削除が失敗すると、「表 6-170 TMPM 連携設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。

表 6-170 TMPM 連携設定の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みの装置とポート番号の組み合わせです	既に削除済みの装置とポート番号の組み合わせです
2	指定したミラー先ポートが存在しません	指定したミラー先ポートが存在しません。
3	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) ミラー先ポート追加

図 6-113 ミラー先ポート追加画面

表 6-171 ミラー先ポート追加画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	装置	「6.1.4(1)(a) 装置追加」で登録した装置名称を入力してください。
③	ポート	詳細ミラー用のミラー先ポートを入力してください。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>、または<switch no.>/<nif no.>/<port no.>となります。
④	追加ボタン	ミラー先ポート追加を反映します。ボタンを押下し、反映が成功すると、「(1) TPM 連携」に移動します。反映が失敗すると、「表 6-172 ミラー先ポート追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑤	キャンセルボタン	ミラー先ポート追加をキャンセルします。ボタンを押下すると、「(1) TPM 連携」に移動します。

表 6-172 ミラー先ポート追加の反映失敗時のダイアログ一覧

項目番	内容	説明
1	装置名称を入力してください	装置名称を入力してください。
2	ポートを入力してください	ポートを入力してください。
3	存在しない装置名称です	存在しない装置名称です。
4	ポートのフォーマットが不正です	ポートのフォーマットが不正です。
5	既に登録済みの装置とポート番号の組み合わせです	既に登録済みの装置とポート番号の組み合わせです。
6	ミラー先ポートが既に 5 ポート設定されています	ミラー先ポートが既に 5 ポート設定されています
7	要求のパラメータに間違があるか、削除中の装置です。「6.1.8(6)メンテナンス」により保守情報を収集してください。	要求のパラメータに間違があるか、削除中の装置です。「6.1.8(6)メンテナンス」により保守情報を収集してください。
8	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## 6.3 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

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の Web インタフェースを説明します。

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」が有効な場合に、利用可能です。

### 6.3.1 ナビゲーションバー

図 6-114 ナビゲーションバー

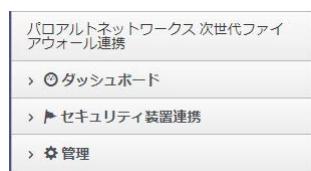


表 6-173 ナビゲーションバーより移動可能な機能の一覧

項目	機能	説明	参照先
ダッシュボード	—	最新 10 件のセキュリティファイルとルールマッチ履歴を表示します。	6.3.2
セキュリティ装置連携	セキュリティフィルター一覧	インシデント抽出ルールにより適用したセキュリティフィルターの一覧を表示します。	6.3.3(1)
	ルールマッチ履歴	受信した Syslog から、インシデント抽出ルールに従い抽出したルールマッチ履歴を表示します。	6.3.3(3)
管理	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設定	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の設定をおこないます。	6.3.4

### 6.3.2 ダッシュボード

図 6-115 ダッシュボード画面

セキュリティフィルタ実行情報 (最新10件)				
登録日時	種別	セキュリティフィルタ条件	状態	要求元IPアドレス
2018/11/05 18:42:53 JST	詳細ミラー	送信元:198.51.100.62/32宛先:0.0.0.0/0	設定済み	198.51.100.10
2018/11/05 18:41:45 JST	通信遮断	送信元:198.51.100.61/32宛先:0.0.0.0/0	設定済み	198.51.100.10

ルールマッチ履歴 (最新10件)							
セキュリティフィルタ名	アドレス	送信元	宛先	セキュリティフィルタ状態	ログ	操作	
受信日時	名称	偏先度	種別	指定	セキュリティフィルタ条件		
2018/11/05 18:42:53 JST	クライアントメント	無	1010	詳細	送信元:198.51.100.62/32宛先:0.0.0.0/0	設定済み	<a href="#">セキュリティフィルタ詳細</a> <a href="#">詳細ミラー解除</a>
2018/11/05 18:41:45 JST	クライアントメント	無	1000	通信遮断	送信元:198.51.100.61/32宛先:0.0.0.0/0	設定済み	<a href="#">セキュリティフィルタ詳細</a> <a href="#">通信遮断解除</a>

表 6-174 ダッシュボード画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	更新ボタン	ボタン押下で画面を更新します。
③	セキュリティフィルタ実行情報	最新 10 件のセキュリティフィルタを表示します。
④	ルールマッチ履歴	最新 10 件のルールマッチ履歴を表示します。 各項目の説明は、「表 6-177 ルールマッチ履歴画面に表示する項目」を参照してください。

### 6.3.3 セキュリティ装置連携

#### (1) セキュリティフィルター一覧

図 6-116 セキュリティフィルター一覧画面

登録日時	種別	セキュリティフィルタ条件	状態
2018/11/05 18:41:45 JST	通信遮断	送信元:198.51.100.61/32宛先:0.0.0.0/0	設定済み
2018/11/05 18:42:53 JST	詳細ミラー	送信元:198.51.100.62/32宛先:0.0.0.0/0	設定済み

表 6-175 セキュリティフィルター一覧画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	選択セキュリティフィルタの解除ボタン	<p>ボタンを押下すると、 選択したセキュリティフィルタを解除します(&lt;チェック数&gt;件) セキュリティフィルタが解除されるまで時間がかかる場合があります  の確認ダイアログを表示します。了承した場合、 実行する場合は YES と入力してください  の確認ダイアログを表示します。YES を入力して了承した場合、選択した個別選択チェックボックスのセキュリティフィルタ※について、セキュリティフィルタを解除します。反映が失敗すると、「表 6-58 選択セキュリティフィルタ解除の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</p>
③	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。

項目番号	内容	説明
④	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑤	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑥	全選択チェックボックス	検索テキストボックスにより絞り込んだ、すべてのセキュリティフィルタをセキュリティフィルタ解除対象とします。もう一度選択すると、すべてのセキュリティフィルタ解除対象から外します。
⑦	個別選択チェックボックス	選択したセキュリティフィルタをセキュリティフィルタ解除対象とします。もう一度選択すると、セキュリティフィルタ解除対象から外します。
⑧	セキュリティフィルタ情報	セキュリティフィルタ情報の一覧を表示します。表示項目は、登録日時/種別/セキュリティフィルタ条件/状態/要求元 IP アドレスです。 セキュリティフィルタ情報を押下すると、「(2) セキュリティフィルタ詳細」画面に移動します。
⑨	ページ切替ボタン	ボタンを押下すると指定のページを表示します。

## 注※

任意のセキュリティフィルタの個別選択チェックボックスが選択された状態で、検索テキストボックスで絞り込みをおこない、該当セキュリティフィルタが表示されない場合でも、該当セキュリティフィルタはセキュリティフィルタ解除対象のままです。この状態でボタンを押下すると、該当セキュリティフィルタのセキュリティフィルタ解除が実施されることに注意してください。

個別選択チェックボックスの選択は、検索テキストボックスで絞り込みをおこなった後におこなうようにしてください。

## (2) セキュリティフィルタ詳細

図 6-117 セキュリティフィルタ詳細画面

① 領域内リンク (Header breadcrumb)

② セキュリティフィルタ情報 (Security Filter Information)

③ 端末情報 (Endpoint Information)

④ 表示カラム切替 (Column Switch)

⑤ 件表示 (Number of items displayed)

⑥ 検索 (Search)

⑦ テーブルヘッダー (Table Header)

設定対象	端末IPアドレス	装置番号	ポート	検出方向	シーケンス番号	検出条件	設定状態	追加要因	コンフィグ	削除要因	解説	削除日時
------	----------	------	-----	------	---------	------	------	------	-------	------	----	------

⑧ ページナビゲーション (Page navigation)

表 6-176 セキュリティフィルタ詳細画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	セキュリティフィルタ情報	セキュリティフィルタ情報として、登録日時/状態/要求元 IP アドレス/セキュリティフィルタ条件/種別を表示します。
③	端末情報	端末情報として、端末 MAC アドレスを表示します。および、[]内に MAC アドレスペンドラを表示します。

項目番号	内容	説明
④	コンフィグ	表示カラム切替ボタン
⑤	内容	一覧から不要なカラムを非表示にすることができます。
⑥	ページあたり表示件数切替プルダウン	1ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑦	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑧	コンフィグ情報	コンフィグ情報の一覧を表示します。 表示項目は、「表 6-61 セキュリティフィルタ詳細画面に表示する項目」を参照してください。
⑨	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

### (3) ルールマッチ履歴

図 6-118 ルールマッチ履歴画面

受信日時	クライアント名	先度	アクション種別	送信元指定	宛先指定	セキュリティフィルタ条件	ログ	操作
2017/09/12 13:19:50 JST	ファイアウォール	60	手動選択				[表示]	[確認済み]
2017/09/12 13:19:53 JST	ファイアウォール	50	手動選択				[表示]	[通信遮断] [詳細ミラー] [確認済み]
2017/09/12 13:19:55 JST	ファイアウォール	30	詳細ミラー	dst		送信元IP:10.0.10.109/32宛先IP:0.0.0.0/0 詳細ミラー	[表示]	[セキュリティフィルタ詳細] [詳細ミラー解除]
2017/09/12 13:19:58 JST	ファイアウォール	10	通信遮断	dst		送信元IP:10.0.10.109/32宛先IP:0.0.0.0/0 通信遮断	[表示]	[セキュリティフィルタ詳細] [通信遮断解除]
2017/09/12 13:22:12 JST	ファイアウォール	50	手動選択				[表示]	[セキュリティフィルタ詳細] [通信遮断解除済み]

5 件中 1 から 5 まで表示

⑦ 前のページ | 1 | 次のページ

表 6-177 ルールマッチ履歴画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	CSV 形式で保存ボタン	ボタンを押下すると一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「pa_actions_match.csv」となります。
③	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。

項目番号	内容	説明
④	ページあたり表示件数切替プルダウン	1 ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑤	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑥	ルールマッチ情報	<p>ルールマッチ情報の一覧を表示します。 表示項目は、受信日時/クライアント名称/優先度/送信元指定/宛先指定/セキュリティフィルタ条件/セキュリティフィルタ状態/ログ/操作です。</p> <p>「ログ」ボタンを押下すると、受信した Syslog メッセージを表示します。再度押下すると、Syslog メッセージの表示を隠します。</p> <p>操作には各種ボタンが表示され、以下に示す動作をします。</p> <ul style="list-style-type: none"> <li>「通信遮断」ボタンを押下すると「(a) 通信遮断設定」に示すダイアログを表示します。</li> <li>「詳細ミラー」ボタンを押下すると「(b) 詳細ミラー設定」に示すダイアログを表示します。</li> <li>「セキュリティフィルタ詳細」ボタンを押下すると「(2) セキュリティフィルタ詳細」に移動します。</li> <li>「通信遮断解除」または「詳細ミラー解除」ボタンを押下すると、セキュリティフィルタを削除します。反映が失敗すると、「表 6-178 ルールマッチ履歴の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</li> <li>「確認済み」ボタンを押下すると、「通信遮断」、「詳細ミラー」ボタンを無効化します。反映が失敗すると、「表 6-178 ルールマッチ履歴の反映失敗時のダイアログ一覧」に示すダイアログを表示します。</li> <li>「セキュリティフィルタ設定エラー」ボタンは、該当フィールドが Syslog に含まれていない、またはセキュリティフィルタに設定できない IP アドレスが選択された場合に表示します。</li> </ul>
⑦	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

表 6-178 ルールマッチ履歴の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みのセキュリティフィルタです	既に削除済みのセキュリティフィルタです。
2	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) 通信遮断設定

図 6-119 通信遮断設定画面

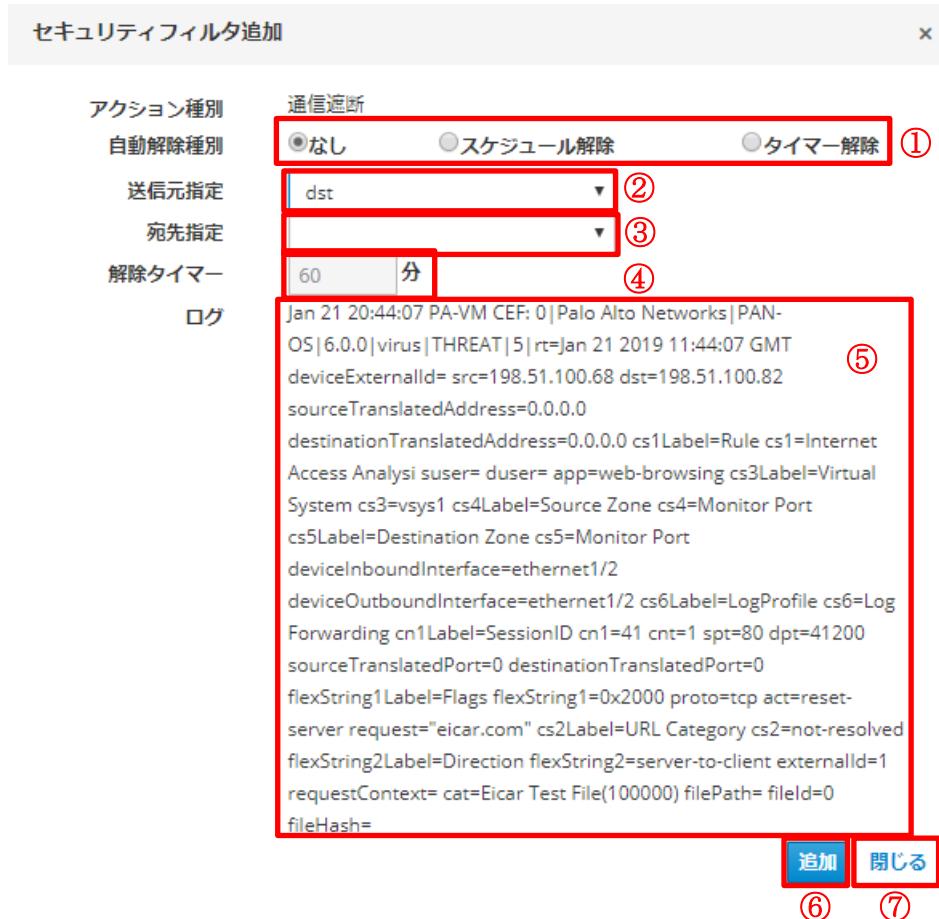


表 6-179 通信遮断設定画面に表示する項目

項目番号	内容	説明
①	解除種別	<p>解除種別を下記から選択します。</p> <ul style="list-style-type: none"> <li>・なし</li> <li>・スケジュール解除</li> <li>・タイマー解除</li> </ul> <p>スケジュール解除を選択してセキュリティフィルタを生成した場合、「6.1.8(1)(e) セキュリティフィルタ自動解除スケジュール追加」で設定した時刻にセキュリティフィルタが削除されます。</p> <p>タイマー解除を選択してセキュリティフィルタを生成した場合、解除タイマーで設定した時間後にセキュリティフィルタが削除されます。</p>

項目番号	内容	説明
②	送信元指定	通信遮断に使用する IP アドレス、または MAC アドレスに、 Syslog の中の「src」、「dst」、「sourceTranslatedAddress」、「destinationTranslatedAddress」、「PanOSXforwarderfor」、「smac」、「dmac」フィールドから選択して、送信元と宛先それぞれに指定します。
③	宛先指定	および、ユーザ定義拡張フィールドとして、データ型が「IPv4 Address」、「IPv6 Address」、「IPv4 Address or IPv6 Address」、または「MAC Address」であるフィールドも選択可能です。 送信元指定にデータ型が「MAC Address」であるフィールドを選択した場合、宛先指定は選択できません。
④	解除タイマー	解除種別がタイマー解除の場合、セキュリティフィルタ生成後に解除を実行するまでの時間(分)を指定します。 1~1440 が指定可能です。
⑤	ログ	受信した Syslog メッセージを表示します。
⑥	追加ボタン	通信遮断のセキュリティフィルタ追加を反映します。ボタンを押下し、反映が成功すると、「(3) ルールマッチ履歴」に移動します。反映が失敗すると、「表 6-180 通信遮断設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑦	キャンセルボタン	セキュリティフィルタ追加をキャンセルします。ボタンを押下すると、「(3) ルールマッチ履歴」に移動します。

表 6-180 通信遮断設定の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	解除タイマーが入力されていません	解除タイマーが入力されていません。
2	範囲外の解除タイマーです	範囲外の解除タイマーです。
3	要求パラメータに間違いがあります	指定されたフィールドがログに含まれていないか、セキュリティフィルタを設定できない IP アドレス、または MAC アドレスです。
4	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (b) 詳細ミラー設定

図 6-120 詳細ミラー設定画面



表 6-181 詳細ミラー設定画面に表示する項目

項目番	内容	説明
①	解除種別	<p>解除種別を下記から選択します。</p> <ul style="list-style-type: none"> <li>・なし</li> <li>・スケジュール解除</li> <li>・タイマー解除</li> </ul> <p>スケジュール解除を選択してセキュリティフィルタを生成した場合、「6.1.8(1)(e) セキュリティフィルタ自動解除スケジュール追加」で設定した時刻にセキュリティフィルタが削除されます。</p> <p>タイマー解除を選択してセキュリティフィルタを生成した場合、解除タイマーで設定した時間後にセキュリティフィルタが削除されます。</p>

項目番号	内容	説明
②	送信元指定	詳細ミラーに使用する IP アドレス、または MAC アドレスに、Syslog の中の「src」、「dst」、「sourceTranslatedAddress」、「destinationTranslatedAddress」、「PanOSXforwarderfor」、「smac」、「dmac」フィールドから選択して、送信元に指定します。および、ユーザ定義拡張フィールドとして、データ型が「IPv4 Address」、「IPv6 Address」、「IPv4 Address or IPv6 Address」、または「MAC Address」であるフィールドも選択できます。
③	解除タイマー	解除種別がタイマー解除の場合、セキュリティフィルタ生成後に解除を実行するまでの時間(分)を指定します。 1~1440 が指定可能です。
④	ログ	受信した Syslog メッセージを表示します。
⑤	追加ボタン	詳細ミラーのセキュリティフィルタ追加を反映します。ボタンを押下し、反映が成功すると、「(3) ルールマッチ履歴」に移動します。反映が失敗すると、「表 6-182 詳細ミラー設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。
⑥	キャンセルボタン	セキュリティフィルタ追加をキャンセルします。ボタンを押下すると、「(3) ルールマッチ履歴」に移動します。

表 6-182 詳細ミラー設定の反映失敗時のダイアログ一覧

項目番号	内容	説明
1	解除タイマーが入力されていません	解除タイマーが入力されていません。
2	範囲外の解除タイマーです	範囲外の解除タイマーです。
3	要求パラメータに間違があります	指定されたフィールドがログに含まれていないか、セキュリティフィルタを設定できない IP アドレス、または MAC アドレスです。
4	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

### 6.3.4 管理

#### (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

図 6-121 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設定画面



表 6-183 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設定画面に表示する項目

項目番	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	ミラー先ポート追加ボタン	新規に詳細ミラー用のミラー先ポートを追加します。ボタンを押下すると、「(a) ミラー先ポート追加」に移動します。 追加済みのミラー先ポート数が収容条件の値と同じ場合、ボタンは押下できません。
③	ミラー先ポート情報	追加済みのミラー先ポート情報(装置名称、ポート番号)を表示します。
④	削除ボタン	対象のミラー先ポートを削除します。ボタンを押下すると、  ミラー先ポート 装置:<装置名称> ポート:<ポート番号> を削除します  の確認ダイアログを表示します。 了承した場合、ミラー先ポートを削除します。削除が失敗すると、「表 6-184 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設定の反映失敗時のダイアログ一覧」に示すダイアログを表示します。

表 6-184 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設定の反映失敗

## 時のダイアログ一覧

項目番号	内容	説明
1	既に削除済みの装置とポート番号の組み合わせです	既に削除済みの装置とポート番号の組み合わせです
2	指定したミラー先ポートが存在しません	指定されたミラー先ポートが存在しません。
3	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6)メンテナンス」により保守情報を収集してください。

## (a) ミラー先ポート追加

図 6-122 ミラー先ポート追加画面

表 6-185 ミラー先ポート追加画面に表示する項目

項目番号	内容	説明
①	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
②	装置	「6.1.4(1)(a) 装置追加」で登録した装置名称を入力してください。
③	ポート	詳細ミラー用のミラー先ポートを入力してください。 入力形式は、装置モデルに応じて、<nif no.>/<port no.>、または<switch no.>/<nif no.>/<port no.>となります。
④	追加ボタン	ミラー先ポート追加を反映します。ボタンを押下し、反映が成功すると、「(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」に移動します。 反映が失敗すると、「表 6-186 ミラー先ポート追加の反映失敗時のダイアログ一覧」に示すダイアログを表示します。

項番	内容	説明
⑤	キャンセルボタン	ミラー先ポート追加をキャンセルします。ボタンを押下すると、「(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」に移動します。

表 6-186 ミラー先ポート追加の反映失敗時のダイアログ一覧

項番	内容	説明
1	装置名称を入力してください	装置名称を入力してください。
2	ポートを入力してください	ポートを入力してください。
3	存在しない装置名称です	存在しない装置名称です。
4	ポートのフォーマットが不正です	ポートのフォーマットが不正です。
5	既に登録済みの装置とポート番号の組み合わせです	既に登録済みの装置とポート番号の組み合わせです。
6	ミラー先ポートが既に 5 ポート設定されています	ミラー先ポートが既に 5 ポート設定されています
7	要求のパラメータに間違があるか、削除中の装置です。「6.1.8(6) メンテナンス」により保守情報を収集してください。	要求のパラメータに間違があるか、削除中の装置です。「6.1.8(6) メンテナンス」により保守情報を収集してください。
8	データベースのアクセスに失敗しました	データベースのアクセスに失敗しました。「6.1.8(6) メンテナンス」により保守情報を収集してください。

## 7. AX-Security-Controller(Viewer)の Web インタフェース

---

この章では、AX-Security-Controller(Viewer)の Web インタフェースについて説明します。

---

## 7.1 遮断端末表示機能

遮断中の端末の一覧を表示する Web インタフェースを説明します。

図 7-1 遮断端末一覧表示画面



表 7-1 遮断端末一覧表示画面に表示する項目

項目番	内容	説明
①	見出し	「6.1.8(1) 共通設定」により、遮断端末一覧の見出しを設定すると、設定した文章を画面に表示します。
②	遮断端末情報	遮断中の端末情報(IP アドレス/MAC アドレス/ベンダ)の一覧を表示します。

## 8. AX-Security-Controller(Tracker)の Web インタフェース

---

この章では、AX-Security-Controller(Tracker)の Web インタフェースについて説明します。

---

## 8.1 端末移動履歴機能

端末移動履歴の Web インタフェースを説明します。

### 8.1.1 ナビゲーションバー

図 8-1 ナビゲーションバー



表 8-1 ナビゲーションバーより移動可能な機能の一覧

項目	機能	説明	参照先
端末移動履歴	履歴検索	端末の移動履歴を検索し、その検索結果を表示します。	8.1.2

## 8.1.2 端末移動履歴

### (1) 履歴検索

図 8-2 履歴検索画面

履歴検索

検索条件

MACアドレス

IPアドレス

エイリアス

① 装置名称

検索期間

開始日時

日	月	火	水	木	金	土	▲	▲	
26	27	28	29	30	1	2	00	:	00
3	4	5	6	7	8	9			
10	11	12	13	14	15	16			
17	18	19	20	21	22	23			
24	25	26	27	28	29	30			
31	1	2	3	4	5	6			

② 終了日時

日	月	火	水	木	金	土	▲	▲	
26	27	28	29	30	1	2	23	:	59
3	4	5	6	7	8	9			
10	11	12	13	14	15	16			
17	18	19	20	21	22	23			
24	25	26	27	28	29	30			
31	1	2	3	4	5	6			

③

表 8-2 履歴検索に表示する項目

項目番	内容	説明
①	検索条件	<p>検索する端末の条件を入力します。指定できる条件は MAC アドレス、IP アドレス、エイリアス、装置名称です。複数の条件を入力した場合、それぞれの条件すべてに一致する端末のみが検索対象となります。</p> <p>なお、エイリアスと装置名称に入力した文字は大文字/小文字を区別しません。また、複数装置をまとめて検索するためにワイルドカード文字として一文字ならば「_」を、複数文字ならば「%」が使用可能です。</p> <p>および、エイリアスの場合、値だけでなくタイトルも検索対象となります。</p>
②	検索期間	検索対象とする期間の開始日時と終了日時を指定します。検索を実施する日の午前 0 時 0 分から午後 11 時 59 分までが自動で指定されています。
③	検索実行ボタン	端末の移動履歴を指定された条件で検索します。ボタンを押下すると、「(2)検索結果画面」画面に遷移します。

## (2) 検索結果画面

図 8-3 検索結果画面

The screenshot shows the search results page for the AX-Security-Controller (Tracker). The interface includes:

- Buttons:** '検索画面表示' (①), 'CSV形式で保存' (②), '表示カラム切替' (③), '件表示' (④), '検索:' (⑤), and a search input field.
- Table Headers:** 接続開始日時, 接続終了日時, 接続期間, MACアドレス (sorted by ⑥), IPアドレス, OA, 端末名, エッジスイッチ番号.
- Table Data:** A list of 10 connection logs. Each log includes date/time, duration, source MAC/IP, destination MAC/IP, port, device name, and edge switch number. The first log is highlighted with a red border.
- Pagination:** 表示件数 (10), and a page navigation bar at the bottom showing '前のページ' (7), '1', '2', '3', '4', '5', '次のページ'.

表 8-3 検索結果画面に表示する項目

項目番	内容	説明
①	検索画面表示	履歴検索画面を表示します。ボタンを押下すると、「図 8-4 検索結果画面(検索画面表示中)」の表示を展開します。
②	CSV 形式で保存ボタン	ボタンを押下すると、一覧で表示した内容を CSV 形式でダウンロードできます。ファイル名は「host_result.csv」になります。

項目番	内容	説明
③	表示カラム切替ボタン	一覧から不要なカラムを非表示にすることができます。
④	ページあたり表示件数切替プルダウン	1ページあたりに表示する件数を切り替えることができます。件数のパターンは 10/25/50/100/全ての 5 パターンです。
⑤	検索テキストボックス	テキストボックスに入力した文字列に該当する行のみに一覧を絞り込むことができます。
⑥	端末移動履歴情報	端末の移動履歴を表示します。 表示項目は、接続開始日時/接続終了日時/接続期間※/MAC アドレス/ベンダ/IP アドレス/エイリアス/接続先装置/ポート番号/ポートエイリアス/VLAN/接続先 AP です。
⑦	ページ切替ボタン	ボタンを押下すると、指定のページを表示します。

※AX-Security-Controller が動作するオペレーティングシステムの時刻を戻した場合、正しく接続期間が表示されない可能性があります。

図 8-4 検索結果画面(検索画面表示中)

**履歴検索**

**検索条件**

MACアドレス	0000.5e00.5351
IPアドレス	
エイリアス	
装置名称	エッジスイッチ2

**検索期間**

開始日時

4月 2018						
日	月	火	水	木	金	土
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

00 : 00

終了日時

4月 2018						
日	月	火	水	木	金	土
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

23 : 59

**履歴検索結果**

**CSV形式で保存**

表示カラム切替  検索:

接続開始日時	接続終了日時	接続期間	MACアドレス	ペンド	IPアドレス	エイリアス	接続先装置	ポート番号	ポートエイリアス	VLAN
2018/04/24 10:40:34 JST	接続中	0d0h0m24s	0000.5e00.5351	ICANN, IANA Department	10.0.10.51	端末1	エッジスイッチ2	0/1	None	100

1件中 1 から 1 まで表示



## 9. トラブルシューティング

---

この章では、発生する問題への対処方法について説明します。

---

---

## 9.1 手動バックアップ・リストア

ここでは、オペレーティングシステムの障害等により、AX-Security-Controller が内部で管理するデータベースが消失するといった事象を回避するため、手動によるバックアップ・リストア手段を説明いたします。

### 9.1.1 バックアップ

インストール先の axsc ディレクトリについて、ディレクトリごとコピーをおこなうことで、バックアップをおこなってください。

### 9.1.2 リストア

既にインストール済みのディレクトリ axsc を別名に退避後、バックアップ先のディレクトリ名を axsc に変更してください。

## 9.2 トラブル発生時の対応

AX-Security-Controller の操作中に発生するトラブルへの対処方法を解説します。

### 9.2.1 プログラム起動

表 9-1 現象と対応

項目番号	現象	原因	対応
1	HTTP Server: [Errno 98] Address already in use と表示されて起動できない。	オペレーティングシステム上の別プロセスがすでに指定した TCP ポート番号を使っていています。	--port オプションで別の TCP ポート番号を使用するか、該当 TCP ポート番号を使用しているプロセスを終了してください。
2	Syslog Server: [Errno 98] Address already in use と表示されて起動できない。	オペレーティングシステム上の別プロセスがすでに指定した UDP ポート番号を使っていています。	--syslog-udp-port オプションで別の UDP ポート番号を使用するか、該当 UDP ポート番号を使用しているプロセスを終了してください。
3	Failed DB initialization と表示されて起動できない。	AX-Security-Controller(Manager)が二重起動しています。	起動中の AX-Security-Controller(Manager)を終了してください。

### 9.2.2 Web インタフェースへのアクセス

表 9-2 現象と対応

項目番号	現象	原因	対応
1	ブラウザからのアクセスが失敗する。	Windows 10 / Windows Server 2016 上で動作している場合、別プロセスが同一の TCP ポート番号を使っていることが考えられます。	--port オプションで別の TCP ポート番号を使用するか、該当 TCP ポート番号を使用しているプロセスを終了してください。
2	SSL 通信で証明書のエラーが起きていることが考えられます。	起動パラメータで正しく証明書を指定しているか、または証明書の有効期限が切れていないか確認してください。	

項目番号	現象	原因	対応
3		<p>下記の履歴情報が大きくなつたことにより、アクセスできなくなつたことが考えられます。</p> <ul style="list-style-type: none"> <li>・ セキュリティ フィルタ履歴</li> <li>・ ルールマッチ履歴</li> <li>・ Syslog 受信履歴</li> </ul>	<p>各履歴情報削除画面より、過去の履歴情報を削除してください。</p> <ul style="list-style-type: none"> <li>・ 6.1.6(3)(a) セキュリティ フィルタ履歴削除</li> <li>・ 6.1.6(5)(c) ルールマッチ履歴削除</li> <li>・ 6.1.6(6)(a) Syslog 受信履歴削除</li> </ul> <p>各履歴情報削除画面にアクセスできない場合、下記パスの URL にアクセスしてください。</p> <ul style="list-style-type: none"> <li>・ セキュリティフィルタ履歴削除 <code>/api/v1/actions/history/delete</code></li> <li>・ ルールマッチ履歴削除 <code>/api/v1/actions/match/delete</code></li> <li>・ Syslog 受信履歴削除 <code>/api/v1/syslogs/delete</code></li> </ul>
4	AX-Security-Controller(Manager)へのアクセス時、Basic認証のユーザ名/パスワードを忘れた。	—	起動パラメータに <code>--reset-basic-auth</code> を追加して Basic 認証を一時的な無効状態で起動してください。起動後、共通設定画面からユーザ名/パスワードの再設定が可能です。

### 9.2.3 トポロジ管理

表 9-3 現象と対応

項目番号	現象	原因	対応
1	端末一覧画面に、接続しているはずの端末が表示されない。	<p>端末が接続されている管理対象装置への到達性がないことが考えられます。</p> <p>この原因により、管理対象装置の情報収集に失敗しました。</p>	管理対象装置への到達性を確認してください。到達性がない場合、到達性を確保してください。
2		<p>管理対象装置の装置モデルが誤っていることが考えられます。</p> <p>この原因により、管理対象装置の情報収集に失敗しました。</p>	管理対象装置の装置モデルを確認してください。異なる場合、一度該当装置を削除し、新規に装置を追加してください。

項目番号	現象	原因	対応
3		管理対象装置の SNMP アクセス情報のコミュニティが、管理対象装置上のコミュニティ名称と異なっていることが考えられます。 この原因により、管理対象装置の情報収集に失敗しました。	管理対象装置の SNMP アクセス情報のコミュニティを確認してください。異なる場合、正しいコミュニティ名称を設定してください。
4		管理対象装置の SSH ログイン情報のログインユーザ名、パスワードが、管理対象装置上のログインユーザ名、パスワードと異なっていることが考えられます。 この原因により、管理対象装置の情報収集に失敗しました。	管理対象装置の SSH ログイン情報のログインユーザ名、パスワードを確認してください。異なる場合、正しいログインユーザ名、パスワードを設定してください。
5		AX8600S・AX8300S、AX3660Sについて、未サポートソフトウェアのバージョンを使用していることが考えられます。 この原因により、管理対象装置の情報収集に失敗しました。	ソフトウェアのバージョンを確認し、サポートしているバージョンへとソフトウェアのアップデートをおこなってください。
6		AX8600S・AX8300Sにおいて、端末を接続しているイーサネットポートで、標準版 LLDP(IEEE Std 802.1AB-2009)の隣接情報を学習していることが考えられます。	標準版 LLDP(IEEE Std 802.1AB-2009)のアクセスを拒否する MAC フィルタを設定してください。 (「3.3 管理対象装置個別の事前準備」参照)

項目番号	現象	原因	対応
7		すべての管理対象装置で、LLDPが動作していない、または管理対象装置間の接続情報設定が未設定であることが考えられます。	<p>すべての管理対象装置について、下記をおこなってください。</p> <ul style="list-style-type: none"> <li>・ LLDPを動作させるようにしてください</li> <li>・ 管理対象装置でLLDPが動作しない場合、接続情報設定により、隣接する管理対象装置との接続情報を設定してください (「6.1.4(2) 接続情報設定」参照)</li> </ul>
8	端末一覧に、同じIPアドレスの端末が複数表示される。	隣接する管理対象装置において、管理対象装置間を接続するイーサネットポートで、LLDPが動作していないことが考えられます。	<p>管理対象装置において、隣接する管理対象装置と接続するイーサネットポートのLLDPを有効にするか、接続情報設定を設定してください。</p> <p>(「3.2.3 LLDP」参照) (「5.3.4 接続情報設定の設定」)</p>
9		AX8600S, AX8300SとAX260A, AX2500S間のイーサネットポートにおいて、標準版LLDP(IEEE Std 802.1AB-2009)によりLLDPの隣接情報を学習していることが考えられます。	AX260A・AX2500Sにおいて、イーサネットポートのLLDPバージョンにIEEE802.1AB/D6(2003年10月)を設定するようにしてください。
10		管理対象装置間のイーサネットポートをリンクアグリゲーションで構成し、任意のイーサネットポートがデータパケット送受信不可能状態(Down)であることが考えられます。	該当するイーサネットポートをデータパケット送受信不可能状態(Down)から復旧させてください。
11	装置の状態が状態不明のまま正常にならない。	端末が接続されている管理対象装置への到達性がないことが考えられます。 この原因により、管理対象装置の情報収集に失敗しました。	管理対象装置への到達性を確認してください。到達性がない場合、到達性を確保してください。

項目番号	現象	原因	対応
12		管理対象装置の装置モデルが誤っていることが考えられます。 この原因により、管理対象装置の情報収集に失敗しました。	管理対象装置の装置モデルを確認してください。異なる場合、一度該当装置を削除し、新規に装置を追加してください。
13		管理対象装置の SNMP アクセス情報のコミュニティが、管理対象装置上のコミュニティ名称と異なっていることが考えられます。 この原因により、管理対象装置の情報収集に失敗しました。	管理対象装置の SNMP アクセス情報のコミュニティを確認してください。異なる場合、正しいコミュニティ名称を設定してください。
14		管理対象装置の SSH ログイン情報のログインユーザ名、パスワードが、管理対象装置上のログインユーザ名、パスワードと異なっていることが考えられます。 この原因により、管理対象装置の情報収集に失敗しました。	管理対象装置の SSH ログイン情報のログインユーザ名、パスワードを確認してください。異なる場合、正しいログインユーザ名、パスワードを設定してください。
15		AX260A / AX2500S / AX2100Sにおいて、SSH ホスト鍵ペア(公開鍵・秘密鍵)が工場出荷時のままであることが考えられます。 この原因により、管理対象装置の情報収集に失敗しました。	SSH ホスト鍵ペアを変更してください。 (「3.3 管理対象装置個別の事前準備」参照)
16		管理対象装置からの MIB 収集において、OID not increasing エラーが発生していることが考えられます。この原因により、管理対象装置の情報収集に失敗しました。	管理対象装置で OID not increasing エラーが発生しているかを確認してください。 (「6.1.4(1) 装置一覧」参照) 発生している場合、OID not increasing エラー無視を有効にしてください。 (「6.1.8(1) 共通設定」参照)

## 9.2.4 セキュリティフィルタ

表 9-4 現象と対応

項目番号	現象	原因	対応
1	セキュリティフィルタが、設定中のままとなり、設定済み(または、再設定中のままであり、再設定済み)にならない。	端末が接続されている管理対象装置への到達性がないことが考えられます。 この原因により、管理対象装置の情報収集、またはコンフィグレーション設定に失敗しました。	管理対象装置への到達性を確認してください。到達性がない場合、到達性を確保してください。
2		管理対象装置の装置モデルが誤っていることが考えられます。 この原因により、管理対象装置の情報収集、またはコンフィグレーション設定に失敗しました。	管理対象装置の装置モデルを確認してください。異なる場合、一度該当装置を削除し、新規に装置を追加してください。
3		管理対象装置の SNMP アクセス情報のコミュニティが、管理対象装置上のコミュニティ名称と異なっていることが考えられます。 この原因により、管理対象装置の情報収集、またはコンフィグレーション設定に失敗しました。	管理対象装置の SNMP アクセス情報のコミュニティを確認してください。異なる場合、正しいコミュニティ名称を設定してください。
4		管理対象装置の SSH ログイン情報のログインユーザ名、パスワード、装置管理情報の装置管理者モードのパスワードが、管理対象装置上のログインユーザ名、パスワード、装置管理者モードのパスワードと異なっていることが考えられます。 この原因により、管理対象装置の情報収集、またはコンフィグレーション設定に失敗しました。	管理対象装置の SSH ログイン情報のログインユーザ名、パスワード、装置管理情報の装置管理者モードのパスワードを確認してください。異なる場合、正しいログインユーザ名、パスワード、装置管理情報の装置管理者モードのパスワードを設定してください。

項目番号	現象	原因	対応
5		管理対象装置のアクセリストの事前準備が完了していないことが考えられます。	アクセリストの事前準備を確認し、不足している場合、事前準備の設定をおこなってください。 (「3.2.4 アクセリスト」参照)
6		管理対象装置のフロー検出モードの設定値により、アクセリストの設定が完了していないことが考えられます。	管理対象装置のフロー検出モードを確認してください。
7		WAN 接続ポート、またはミラー先ポートまたは永続設定ポート(受信側/送信側)に、存在しないポートを設定していることが考えられます。	設定済みの WAN 接続ポート、またはミラー先ポートまたは永続設定ポート(受信側/送信側)が、管理対象装置に存在するか確認してください。存在しない場合、一度削除してください。その後、存在するポートを設定してください。
8		セキュリティフィルタの適用先の管理対象装置が AX8600S・AX8300S の場合、コンフィグレーションのコミットモードが手動コミットモードであることが考えられます。	コンフィグレーションのコミットモードを確認し、手動コミットモードの場合は逐次コミットモードにしてください。
9	アクセリストの追加と削除が繰り返される。	通常モードで運用し、管理対象装置のポート配下で IPv6 端末を直接収容している構成において、当該端末が通信遮断対象となる場合、当該装置への IPv6 アクセリストの追加と削除が繰り返されます。	ICMP の Neighbor discovery router advertisements(タイプ 134)、および Neighbor discovery router solicitations(タイプ 133)を許可するように、IPv6 アクセリストの設定を検討ください。

## 9.2.5 マップ

表 9-5 現象と対応

項目番号	現象	原因	対応
1	マップが表示されない	マップに背景画像を設定しているにもかかわらず、画像ファイルが AX-Security-Controller 上に存在しないことが考えられます。または CSV 形式からのマップ追加を実施後、背景画像を設定していないケースが考えられます。	マップ一覧から背景画像を登録してください。または、マップ編集画面で、背景画像を再設定してください。
2	ZIP 形式からの一括背景画像追加で画像が登録されない	背景画像ファイル名に対応するマップが登録されていないことが考えられます。	CSV 形式からのマップ追加を実施し、背景画像ファイル名に対応するマップを先に登録してください。
3	ZIP 形式からの一括画像追加で画像が登録されない	画像ファイル名に対応する画像名称が登録されていないことが考えられます。	CSV 形式からの画像追加を実施し、画像ファイル名に対応する画像名称を先に登録してください。

## 9.2.6 E-mail 通知

表 9-6 現象と対応

項目番号	現象	原因	対応
1	E-mail がメールサーバに届かない	メールサーバへの到達性がないことが考えられます。	メールサーバへの到達性を確認してください。到達性がない場合、到達性を確保してください。
2		メールサーバであるサーバ情報の名称を IP アドレスに変換できないことが考えられます。	AX-Security-Controller が動作している環境で、サーバ情報の名称が IP アドレスに変換できるか確認してください。 変換できない場合、DNS リゾルバ機能の設定を確認してください。
3		メールサーバの TCP ポート番号と Web インタフェースで設定したポート番号が異なることが考えられます。	メールサーバの TCP ポート番号と Web インタフェースで設定したポート番号を確認してください。 異なる場合、Web インタフェースでポート番号を変更してください。

項目番号	現象	原因	対応
4		メールサーバで使用可能なプロトコルと Web インタフェースで設定したプロトコルが異なることが考えられます。	メールサーバで使用可能なプロトコルと Web インタフェースで設定したプロトコルを確認してください。 異なる場合、Web インタフェースでプロトコルを変更してください。
5		メールサーバはユーザ認証が有効ですが、Web インタフェースのユーザ認証の設定が無効であると考えられます。	メールサーバのユーザ認証の有効・無効と Web インタフェースのユーザ認証の有効・無効を確認してください。 異なる場合、Web インタフェースでユーザ認証の有効・無効を変更してください。
6		認証を有効にしている場合、メールサーバの認証ユーザ名/パスワードと Web インタフェースで設定した認証ユーザ名/パスワードが異なることが考えられます。	メールサーバの認証ユーザ名/パスワードと Web インタフェースで設定した認証ユーザ名/パスワードを確認してください。 異なる場合、Web インタフェースで認証ユーザ名/パスワードを変更してください。
7		Web インタフェースで設定した下記の形式が誤っていることが考えられます。 ・ 宛先メールアドレス(To, Cc, Bcc) ・ 差出人メールアドレス(From)	Web インタフェースで設定した宛先メールアドレス(To, Cc, Bcc), 差出人メールアドレス(From)の形式を確認してください。 誤っている場合、Web インタフェースで宛先メールアドレス(To, Cc, Bcc), 差出人メールアドレス(From)を変更してください。



## 付録

---

---

## 謝辞 (Acknowledgments)

本製品で導入しているオープンソースソフトウェアは、下記になります。

### (1) Bootstrap

The MIT License (MIT)

Copyright (c) 2011–2019 Twitter, Inc.

Copyright (c) 2011–2019 The Bootstrap Authors

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### (2) C3

The MIT License (MIT)

Copyright (c) 2013 Masayuki Tanaka

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

**(3) D3**

Copyright 2010–2017 Mike Bostock  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* Neither the name of the author nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**(4) DataTables**

Copyright (c) 2008–2015 SpryMedia Limited  
<http://datatables.net>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

**(5) jQuery**

Copyright JS Foundation and other contributors, <https://js.foundation/>

This software consists of voluntary contributions made by many individuals. For exact contribution history, see the revision history available at <https://github.com/jquery/jquery>

The following license applies to all parts of this software except as documented below:

====

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

All files located in the node\_modules and external directories are externally maintained libraries used by this software which have their own licenses; we recommend you read them, as their terms may differ from the terms above.

## (6) jQuery UI

Copyright jQuery Foundation and other contributors, <https://jquery.org/>

This software consists of voluntary contributions made by many individuals. For exact contribution history, see the revision history available at <https://github.com/jquery/jquery-ui>

The following license applies to all parts of this software except as documented below:

====

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be

included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

Copyright and related rights for sample code are waived via CCO. Sample code is defined as all source code contained within the demos directory.

CCO: <http://creativecommons.org/publicdomain/zero/1.0/>

====

All files located in the node\_modules and external directories are externally maintained libraries used by this software which have their own licenses; we recommend you read them, as their terms may differ from the terms above.

## (7) PatternFly

Modifications to Bootstrap are copyright 2013 Red Hat, Inc. and licensed under the Apache License 2.0.

Version 2.0, January 2004  
<http://www.apache.org/licenses/>

### TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

#### 1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licenser for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licenser or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licenser for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licenser and any individual or Legal Entity on behalf of whom a Contribution has been received by Licenser and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses

granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
  - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
  - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
  - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
  - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

#### END OF TERMS AND CONDITIONS

#### APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "{}" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright {yyyy} {name of copyright owner}

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

## (8) Moment

Copyright (c) JS Foundation and other contributors

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## (9) Bootstrap 3 Date/Time Picker

The MIT License (MIT)

Copyright (c) 2015 Jonathan Peterson (@Eonasdan)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

(10) vis

The MIT License (MIT)

Copyright (c) 2014–2017 Almende B.V.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.