サイバー攻撃自動防御ソリューション用ソフトウェア

AX-Security-Controller(AX-SC)

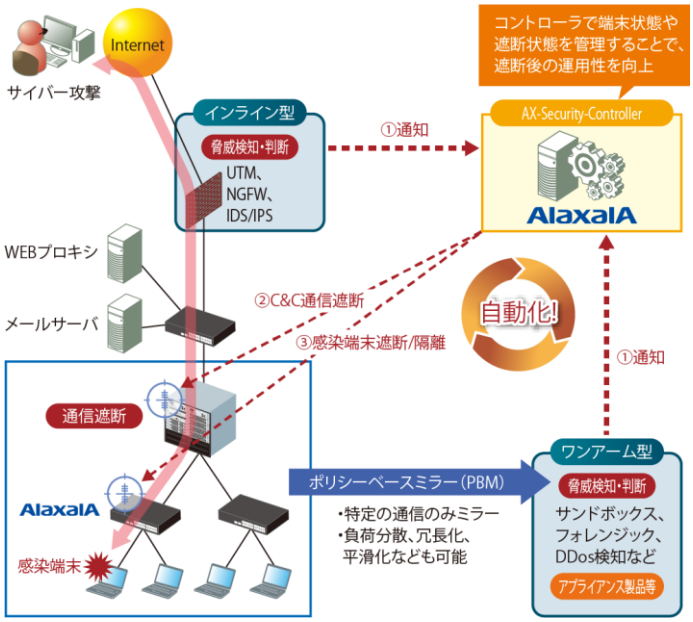
AlaxalA

セキュリティ装置からの通知に基づき、ネットワークを制御するセキュリティコントローラ

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(AX-SC)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。

セキュリティ装置からの通知に従い、ネットワーク機器に対して自動遮断などを設定



サイバー攻撃自動防御ソリューションを提供

- セキュリティベンダとのパートナーリングにより、サイバー攻撃をすばやく検知・判断し通信遮断の自動化を実現
  - トレンドマイクロとの連携:Trend Micro Policy Manager™ (TMPM) およびDeep Discovery™ Inspector (DDI)
  - パロアルトネットワークスとの連携:次世代ファイアウォール
  - フォーティネットとの連携:次世代ファイアウォールFortiGate
  - ファイア・アイとの連携:FireEye Network Security
  - 汎用連携インタフェース(CEF形式 syslog)のサポート:上記以外の多様なセキュリティ製品とも連携可能
- 汎用スイッチで導入環境を選ばず、スマートな制御でインシデントリスクを低減
- マルウェア感染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

ネットワーク機器の情報を収集し、端末の接続位置を管理/可視化

端末接続状況の画面

端末一覧

端末のエイリアス名は自由に設定可能

CSV形式で保存

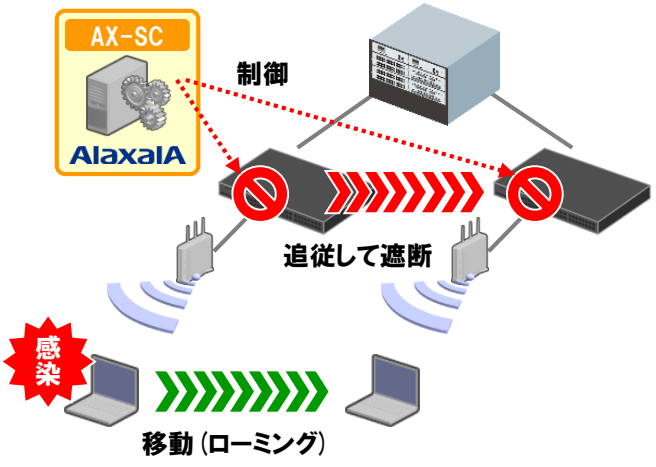
表示カラム切替　25 件表示　検索:

IPアドレス	MACアドレス	エイリアス	接続先装置	ポート番号	VLAN ID	セキュリティフィルタ適用状態
10.0.20.30	0012.e228.9e63	None	AX3660S	1/0/1	20	
10.20.0.1	d4c9.efd6.36bb	None	AX2530S	0/1	200	
10.20.1.1	0012.e201.0001	端末1	AX2530S	0/1	200	
10.20.1.10	0012.e201.0010	端末10	AX2530S	0/1	200	
10.20.1.100	0012.e201.0100	端末100	AX2530S	0/1	200	
10.20.1.101	0012.e201.0101	端末101	AX2530S	0/1	200	
10.20.1.102	0012.e201.0102	端末102	AX2530S	0/1	200	
10.20.1.103	0012.e201.0103	端末103	AX2530S	0/1	200	
10.20.1.104	0012.e201.0104	端末104	AX2530S	0/1	200	
10.20.1.105	0012.e201.0105	端末105	AX2530S	0/1	200	

端末管理ソフトとしての利用も可能

- 登録された装置(スイッチ)から情報を自動収集し、端末が接続されている装置/ポート/VLANを一覧で表示
- 端末に「エイリアス名」を設定したり、装置名として設置ロケーションを設定することで可読性を向上し、素早い状況確認が可能
  - IPアドレス/MACアドレス → 職員AのPC
  - AX3660S → A棟_集約SW_1

端末の接続位置情報を定期更新することで、端末移動時の自動追従を実現



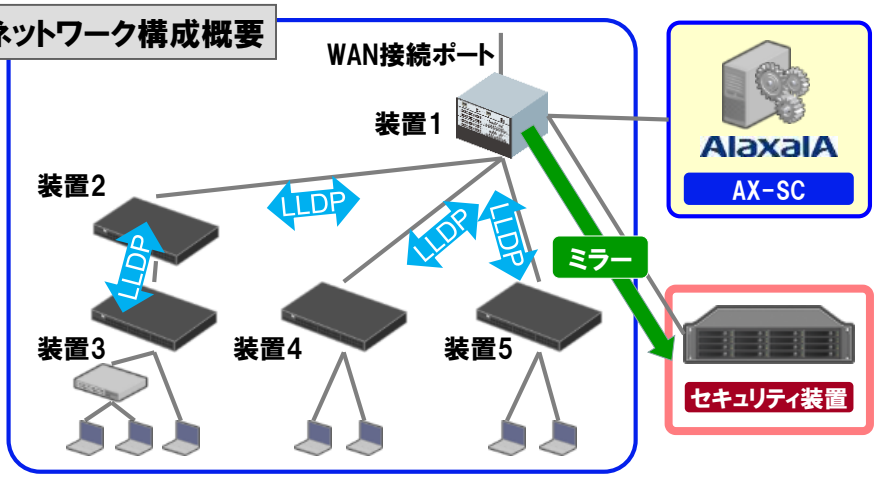
無線環境で課題となるローミングにも追従

- AX-SCでは端末の接続状況を常に把握
- 端末がポートやスイッチ間を移動しても、移動先のポート/スイッチへ追従して処理を継続

だから

- 感染端末がネットワーク内を移動しても、追従して遮断することが可能
- DHCP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

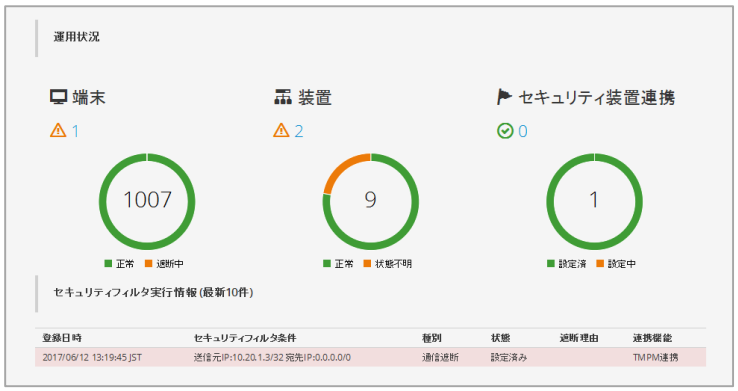
ネットワーク構成概要



AX-SC に管理対象装置として登録可能なスイッチは、「サポート機器（製品仕様を参照）」に含まれる製品

- ◆ 各装置は AX-SC から IP リーチャビリティがあること
- ◆ 最低1台はレイヤ3スイッチである必要があり、端末の ARP 情報を学習する（装置1）
- ◆ レイヤ3スイッチ（装置1）と端末間で NAT や Proxy などのアドレス変換がされていないこと
- ◆ 端末を収容するスイッチでは、端末のMACアドレス情報を学習する（装置3～5）
- ◆ 隣接する管理対象装置間では LLDP が有効であるあるか、
  AX-SCでスイッチ間の接続情報を事前登録すること（装置1-2/1-4/1-5/2-3間）

ダッシュボード



AX-SC が提供する機能のサマリーを表示（円内/円外）

- ◆ 端末：認識している端末数/遮断中の端末数
- ◆ 装置：登録装置数/通信不可等で状態不明な装置数
- ◆ 連携：セキュリティフィルタの登録数/設定中の数
- ◆ セキュリティフィルタ設定中は、実行情報を追加表示

装置管理（登録スイッチの一覧）

AX-SC の管理対象装置について以下の機能を提供

- ◆ 装置の追加・変更・削除
- ◆ 装置の詳細表示
  隣接装置の一覧と、接続端末の一覧を表示
- ◆ メンテナンスモード
  特定の装置を一時的に管理対象外とすることが可能

AX-Security-Controller 製品仕様

運用管理機能ソフトウェア名	AX-Security-Controller	AX-Security-Controller(端末移動履歴機能を利用する場合)
OS	Windows 10(64bit), Windows Server 2016, Linux CentOS 7(64bit), Red Hat Enterprise Linux 7	
必須ソフトウェア	python 3.5以上	
CPU	インテル Core i シリーズ以上（コア数4以上推奨）	
必須メモリ	4.0GB以上（8.0GB以上推奨）	8.0GB以上（32.0GB以上推奨）
ディスク容量	20GB以上	20GB以上＋端末移動履歴での必要分*3
サポート機器	AX8600S/AX8300S/AX6700S*1/AX6600S*1/AX6300S*1/AX4600S/AX3800S/AX3600S*2/ AX2500S/AX2200S/AX2100S/AX1200S*1/AXprimoM210/AX260A, AX8600R*1/AX620R*1, 他社L3/L2スイッチ*1	
管理最大機器数	1000台	

*1：自動遮断は未対応、ARP/FDB情報がMIBで収集可能であること *2：AX3630Sは未サポート *3：1エントリあたり1024byteとして必要な容量を確保してください

⚠ ご注意　正しく安全にお使いいただくために、ご使用の前に必ず「取扱説明書」、「使用上のご注意」などをよくお読み下さい。

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

201810