

感染端末を検出して、通信を自動遮断！ サイバー攻撃自動防御ソリューション

サイバー攻撃の検知から初動対処までを自動化し、
対応時間を短縮 & 拡散を防止するソリューション

お客様の課題

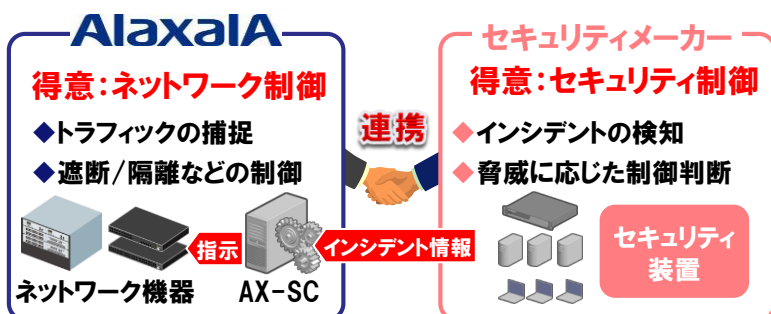
- ① インシデント時の初動対応を迅速化し、できれば自動化したい
- ② 感染端末の位置を容易に特定したい
- ③ 感染端末をネットワークから切り離した際、ユーザに警告メッセージを表示させたい
- ④ 全端末へのエージェントのインストールは難しい



セキュリティソリューション部門
審査員特別賞

解決① 初動対応の自動化

セキュリティ装置の通知に従い、マルウェアに感染した
端末の通信を自動遮断、感染端末がポートやスイッチ
間を移動しても、移動先へ追従して処理を継続



※ AX-SC: AX-Security-Controller

- ・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
- ・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

解決② 端末の位置情報管理

登録された装置 (スイッチ) から情報を自動収集し、
端末の接続位置を可視化することで、
マルウェアに感染した端末を簡単に発見できる

端末一覧

CSV形式で保存

表示カラム切替 25 件表示

検索:

端末にエイリアスを設定可能！
(例: 職員AのPC)

設置ロケーションを設定しても良い！
(例: A棟_集約SW_1)

端末が接続されている装置/ポート/VLANが一目瞭然！

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
10.10.20.30	0012.e228.9e63	None	AX36605	1/0/1	20	
10.20.0.1	d4c9.efd6.36bb	None	AX25305	0/1	100	
10.20.1.1	0012.e201.0001	端末1	AX25305	0/1	200	
10.20.1.10	0012.e201.0010	端末10	AX25305	0/1	200	
10.20.1.100	0012.e201.0100	端末100	AX25305	0/1	200	
10.20.1.101	0012.e201.0101	端末101	AX25305	0/1	200	
10.20.1.102	0012.e201.0102	端末102	AX25305	0/1	200	
10.20.1.103	0012.e201.0103	端末103	AX25305	0/1	200	
10.20.1.104	0012.e201.0104	端末104	AX25305	0/1	200	
10.20.1.105	0012.e201.0105	端末105	AX25305	0/1	200	

解決③ 警告メッセージ表示

通信遮断中のユーザには、
ブラウザを使って警告やメッセージを発信可能



遮断中のユーザ

マルウェアに感染した
疑いがあるため、
この端末をネットワークから
切り離しました！

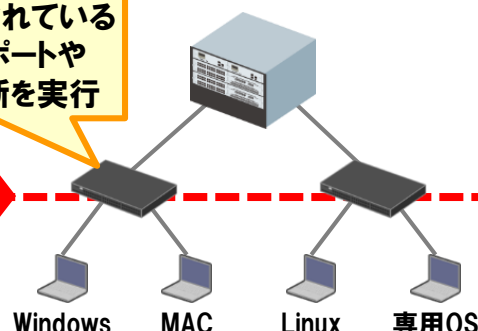
- ◆ アナウンス内容はカスタマイズ可能
- ◆ アクションの指示や問い合わせ先の表示などで利用者に適切な対応を促し、初動の迅速化を支援

解決④ エージェントレス

エージェントレスで動作するので、端末側に特別な
ソフトや設定は不要

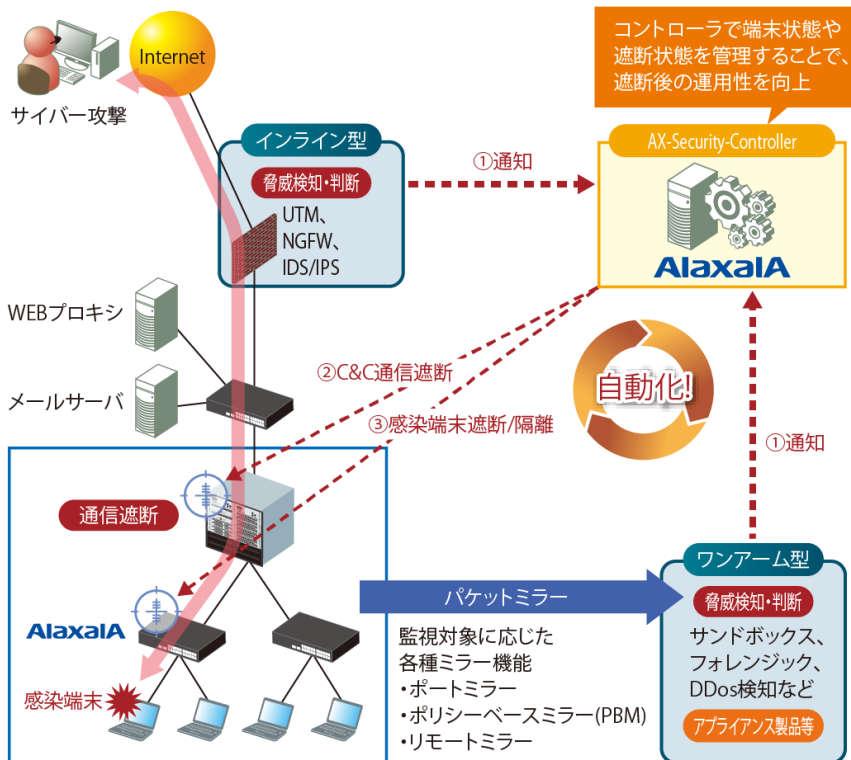
端末が収容されている
スイッチのポートや
VLAN で遮断を実行

遮断
ポイント



ソリューション概要

セキュリティメーカーのアプライアンス製品との連携により サイバー攻撃の脅威検知・判断 → 通信遮断を自動化

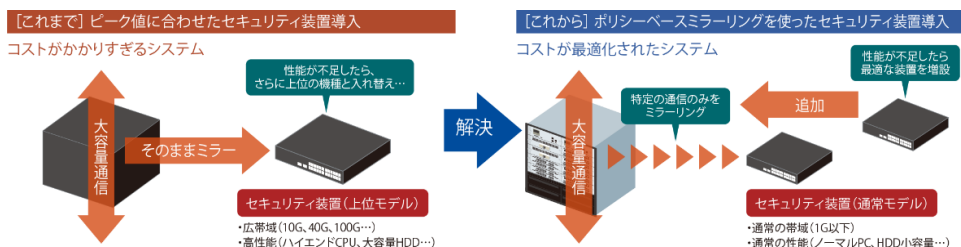


セキュリティメーカー各社との連携

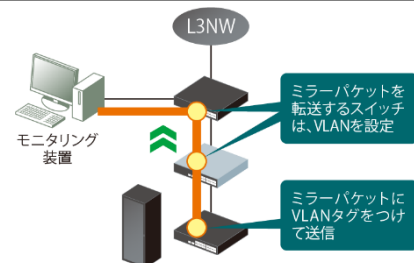


**汎用連携インターフェース (CEF形式syslog) をサポート、
上記以外のセキュリティ製品とも連携可能**

【ポリシーベースミラー】セキュリティ投資のコストを最適化



【リモートミラー】



サイバー攻撃自動防御ソリューション システム要件概要

アラクサラ	コントローラ	AX-Security-Controller Ver1.0 以上 (セキュリティ装置からの通知に従いネットワーク機器を制御)
	ネットワーク機器	AX8600S/AX8300S/AX6700S ^{*1} /AX6600S ^{*1} /AX6300S ^{*1} / AX4600S/AX3800S/AX3600S ^{*2} /AX2500S/AX2200S/AX2100S/AX260A、他社L3スイッチ/他社L2スイッチ ^{*1}
トレンド マイクロ	セキュリティ装置	①Trend Micro Policy Manager™ (必須: セキュリティポリシー管理、②～③製品からのインシデント通知を集約管理) ②Deep Discovery™ Inspector (選択: ネットワークセンサー[サンドボックス機能も実装]) ③Trend Micro Deep Security™ (選択: サーバの多層防御製品) ④ウイルスバスター™ コーポレートエディション (選択: 総合エンドポイントセキュリティ製品)
パロアルトネットワークス	セキュリティ装置	次世代ファイアウォール
フォーティネット	セキュリティ装置	FortiGate
ファイヤアイ	セキュリティ装置	FireEye Network Security
その他	セキュリティ装置	汎用連携インタフェース ^{*3} に対応した製品

*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: 業界標準のログメッセージフォーマットであるCommon Event Format(CEF)に対応したsyslogメッセージ

・TREND MICRO、Trend Micro Policy Manager、Deep Discovery、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
 ・その他記載の会社名、製品名はそれぞれの会社の商標または登録商標です



ご注意 正しく安全にお使いいただくために、ご使用前に必ず「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/ip/contact>

- 当カタログ記載の会社名/製品名は各社の商標もしくは登録商標です。
- 製品の外観、仕様は予告なく変更することがあります。
- 本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規制など外国の輸出関連法規をご確認の上、必要な手続きをおとりください。なお、不明な場合は、弊社担当営業にお問い合わせ下さい。
- カタログ上の名称及びロゴマークは、アラウカネネットワーク株式会社所有の商標及び登録商標です。