The Guaranteed Network
いちばん近くで、もっと先へ。

AlaxalA

サイバー攻撃自動防御ソリューション
～パロアルトネットワークス連携～

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

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

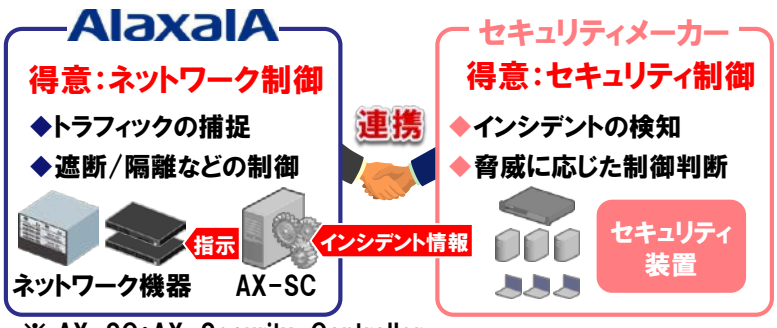
Interop BEST OF SHOW AWARD 2017 特別賞
セキュリティソリューション部門
審査員特別賞

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

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

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

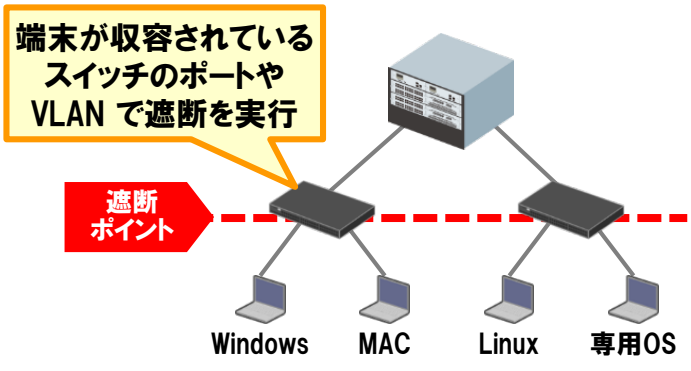
マルウェアに感染した疑いがあるため、この端末をネットワークから切り離しました！

遮断中のユーザ

◆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



ソリューション概要　パロアルトネットワークスとの連携

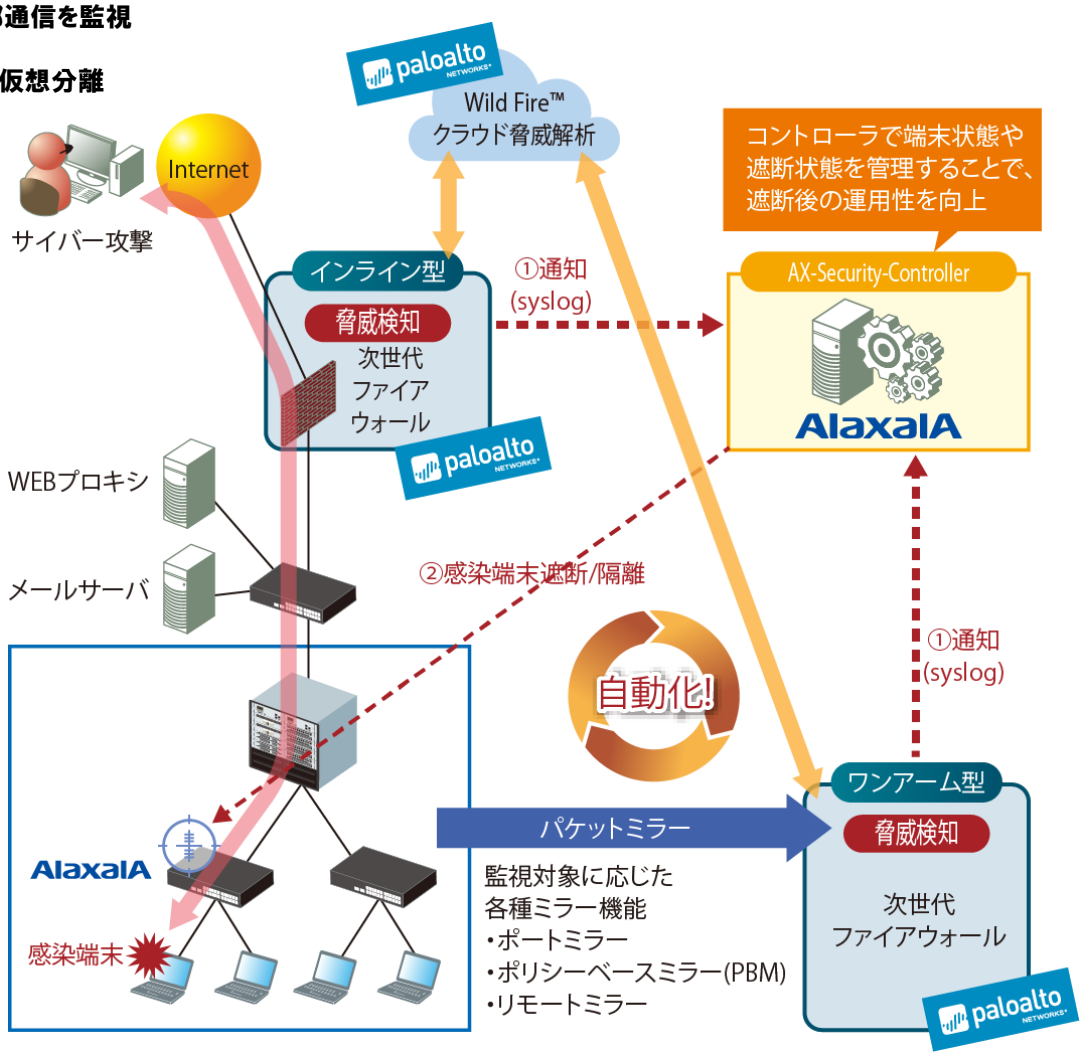
次世代ファイアウォールがサイバー攻撃に関わる通信を検知し、その情報を元にスイッチが該当端末をネットワークから遮断

ニーズに応じてインライン型とワンアーム型の構成を選択可能

- インライン型（入口/出口対策）
  - FWの位置に設置し、外部との通信を監視
  - AXだけでなく、FW 位置での遮断も可能
- ワンアーム型（内部対策）
  - ミラーを受信して（主に）内部通信を監視
  - 遮断はAXでのみ実施
- 次世代ファイアウォールのリソースを仮想分離することで、入口/出口対策と内部対策の両方を同一筐体に同居させることも可能
- いずれの構成においても、未知の脅威に対しても クラウド型の脅威解析を提供する WildFire™ サービスを利用可能

セキュリティ脅威の検知・特定から初動対応までを、企業ごとの運用ポリシーで自動化（ポリシーは AX-SC で管理）

- syslog のフィールド情報を組み合わせることで、セキュリティポリシーを設定（細かくポリシーを設定することができる）



サイバー攻撃自動防御ソリューション　パロアルトネットワークス連携　システム要件概要

アラクサラ	コントローラ	AX-Security-Controller Ver1.1 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、セキュリティポリシー管理）
	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*1
パロアルト ネットワークス	セキュリティ装置	①次世代ファイアウォール（必須：インシデントの検知）

*1：自動遮断は未対応、ARP情報がMIBで収集可能であること　*2：AX3630Sは未サポート

⚠ 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

201710