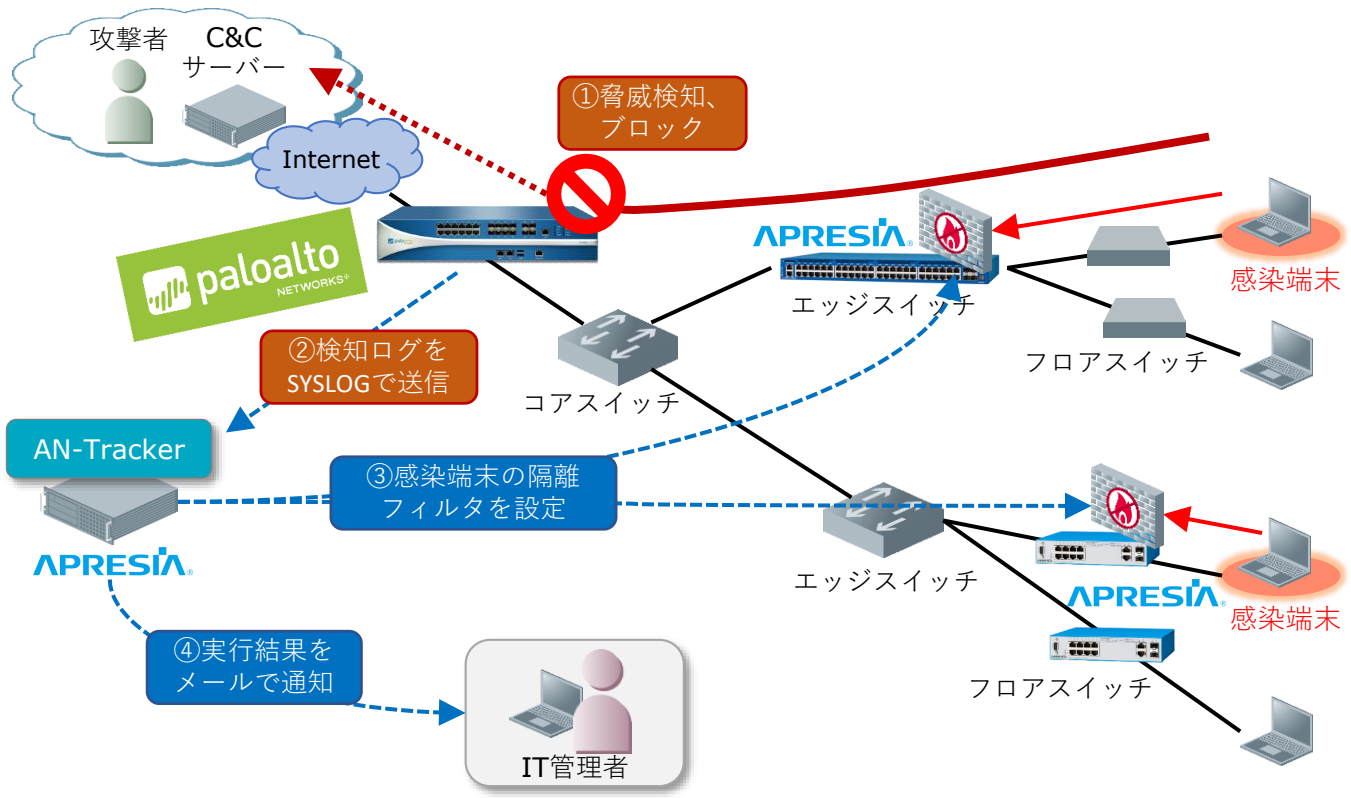
セキュリティ・オートメーションにより IT管理者の負荷を大幅に軽減します!!

～パロアルトネットワークスの次世代ファイアウォールと連携～

セキュリティ装置とネットワークの製品連携による インシデント対応の効率的な解決策!!

- ✓ *サイバー攻撃の脅威検知から封じ込めまでの初動対応を自動化します*
- ✓ *迅速に感染端末を隔離し、内部感染拡大や二次被害のリスクを最小化します*

連携ソリューションイメージ



連携ソリューションの概要

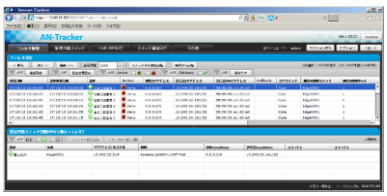
- **次世代ファイアウォールがC&Cサーバーなど外部との不正な通信を検出し、ブロックします。またその検知ログをSyslogでAN-Trackerへ送信します。**
- **AN-Trackerは、受信した検知ログ(Syslog)から感染端末のIPアドレスを抽出し、またネットワーク上からデバイス情報(MACアドレス、接続されているエッジスイッチ/フロアスイッチおよびポート番号)を検索します。デバイス特定後に感染端末からの通信を遮断するフィルタを各エッジスイッチ/フロアスイッチに設定します。**
- **AN-Trackerは、実行結果をIT管理者へメールで通知します。フィルタ内容および実行結果、また隔離のトリガーとなった次世代ファイアウォールの検知ログ情報をメールで送信します。**

AN-Tracker製品紹介

■ セキュリティ連携用ソフトウェア AN-Tracker 製品概要

- セキュリティ装置の脅威検知と連動し、感染端末を自動隔離
- ネットワーク上に配置されたエッジスイッチ/フロアスイッチを制御し、アクセス制御を行うため、**エージェントレス**で動作
- インシデントの深刻度やお客様の運用ポリシーに応じて、各種アクセス制御(**感染端末の全通信遮断/ブラックリスト・ホワイトリストによる通信制限**)を自動化
- アクセス制御は**MACアドレスベース**のため、エッジスイッチの配下にスイッチングハブ/無線アクセスポイントが接続されている環境、DHCP環境にも対応 (*ApresiaLightシリーズはIPアドレスベースでアクセス制御)
- 従来のネットワーク技術を使用するため、**インストール済みのAPRESIA**をそのまま活用することも可能
- 管理画面にて、**隔離フィルタの一覧、感染端末情報**(IPアドレス、MACアドレス、接続されているエッジスイッチ/ポート番号)の可視化が可能

■ 動作環境、ライセンス



AN-Tracker　動作環境、ライセンス	
OS	RedHat Enterprise Linux 7.x (x86_64)
CPU	x86 アーキテクチャの64bit CPU 2Core以上 （4Core以上推奨）
RAM	2GB以上 （4GB以上推奨）
HDD	100GB以上
クライアントPC（GUIへのアクセス）	Windows系OS上のInternetExplorer (IE11で動作確認済み) Abobe Flash Player Ver.24 以上
ソフトウェアライセンス（*）	50台、100台、200台、1000台

(*) 管理対象として登録するコアスイッチ、エッジスイッチの総数

■ 対応スイッチ

- コアスイッチ：感染端末のARP情報がSNMPで取得可能な機器
  RFC 3418 MIB(ipNetToMediaPhysAddress)に対応していること
- エッジスイッチ（Big EnterpriseからSmall Business向けまで幅広くラインナップ）

企業/DC向けイーサネットスイッチ

Apresiaシリーズ

ApresiaNPシリーズ(*)

SMB向けイーサネットスイッチ

ApresiaLightシリーズ

(*) スタックを使用している場合は、サポート対象外

APRESIA Systems 株式会社

〒104-0045 中央区築地二丁目3番4号 築地第1長岡ビル8階
お問い合わせ： https://www.apresia.jp/form/inquiry.php?type=1