The Guaranteed Network
いちばん近くで、もっと先へ。

サイバー攻撃自動防御ソリューション システム構築ガイド

～パロアルト編～

初版

資料 No. NTS-17-R-004

アラクサラネットワークス株式会社

はじめに

サイバー攻撃自動防御ソリューションは、セキュリティ製品との連携によりマルウェアに感染した端末を検出し、感染端末の通信を自動的に遮断するソリューションです。本ガイドは、サイバー攻撃の早期発見を可能にするパロアルトネットワークス株式会社のセキュリティ製品とアラクサラ製品の連携で実現する サイバー攻撃自動防御ソリューションの一例を紹介し、システムの構築の一助となることを目的としています。

関連資料

- アラクサラ AX シリーズ製品マニュアル
  (http://www.alaxala.com/jp/techinfo/manual/index.html)
- アラクサラ AX-Security-Controller ユーザズガイド
  (http://www.alaxala.com/jp/techinfo/guide/index.html)
- パロアルトネットワークス
  (https://www.paloaltonetworks.jp/)

本資料使用上の注意事項

本資料に記載の内容は、弊社が特定の環境において基本動作を確認したものであり、機能・性能・信頼性についてあらゆる環境条件すべてにおいて保証するものではありません。また製品マニュアル、ユーザズガイドの補助資料としてご利用いただけますようお願いいたします。

なお本資料作成時の OS ソフトウェアバージョンは特記の無い限り以下となっております。

- アラクサラ スイッチ
  AX3660S　Ver. 12.1
  AX2530S　Ver. 4.7
- アラクサラ セキュリティコントローラ
  AX-Security-Controller　Ver. 1.2
- パロアルトネットワークス 次世代ファイアウォール
  PAN-OS 8.0

本資料の内容は、改良のため予告なく変更する場合があります。

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。

商標一覧

- アラクサラの名称およびロゴマークは、アラクサラネットワークス株式会社の商標および登録商標です。
- 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。
- Ethernet は，富士ゼロックス株式会社の登録商標です。
- イーサネットは，富士ゼロックス株式会社の登録商標です。
- 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もしくは登録商標です。

目次

1. サイバー攻撃自動防御ソリューションとは

1.1　サイバー攻撃対策の課題

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。このため、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となっています。この課題への対策として、ネットワーク上のトラフィックの振る舞いから標的型攻撃の早期発見を可能にするセキュリティ製品の導入が有効です。セキュリティ製品を導入した上で、インシデントが発見された場合は、迅速に感染端末の物理的な位置を特定し、端末をネットワークから遮断することが重要となります。

また、標的型攻撃の兆候をより確実に捉えるためには、セキュリティ製品が監視するネットワークの範囲も課題になります。従来のソリューションでは、セキュリティ製品が直接接続するスイッチ上のトラフィックのみを監視対象としているため、遠隔のスイッチ上で折り返される端末間等の通信が監視できず、攻撃を見逃している可能性があります。監視範囲をネットワーク全体に広げることも重要となります。

さらに、システムの運用を考慮すると、次のようなことへの対応も必要です。

- 無線 LAN 環境などにおいて、遮断したはずの端末が、別の LAN へ移動して通信再開することを防止するため、端末が移動しても追従して遮断を行うこと。
- 端末の使用者に対して遮断された理由を知らせること。

1.2　サイバー攻撃自動防御ソリューションの特徴

本ソリューションは、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　セキュリティ製品との連携

アラクサラのサイバー攻撃自動防御ソリューションは、以下のような特徴があります。

- **感染端末を自動的に遮断**
  セキュリティ製品との連携により マルウェアに感染した端末を検出し、感染端末の通信を自動的に遮断することができます。遮断は 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 サーバーとの通信許可、特定のサーバーとの通信遮断が可能です。また、セキュリティ装置が検出した攻撃サーバーについて、サーバー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。

- **エッジスイッチ上の端末間通信を監視**
  リモートミラーリング機能により セキュリティ製品が直接接続しない、エッジスイッチ上の端末間通信の監視ができます。これにより 感染端末からの隣接端末やサーバー等への探索や感染拡大の活動も監視でき、セキュリティ製品での検知率の向上が期待できます。

- **端末移動追従**
  端末の位置をトポロ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、追従して通信遮断を提供します。

- **警告表示機能**
  感染端末の使用者が、ウェブブラウザで通信を試みると、ブラウザ画面上に警告を表示します。

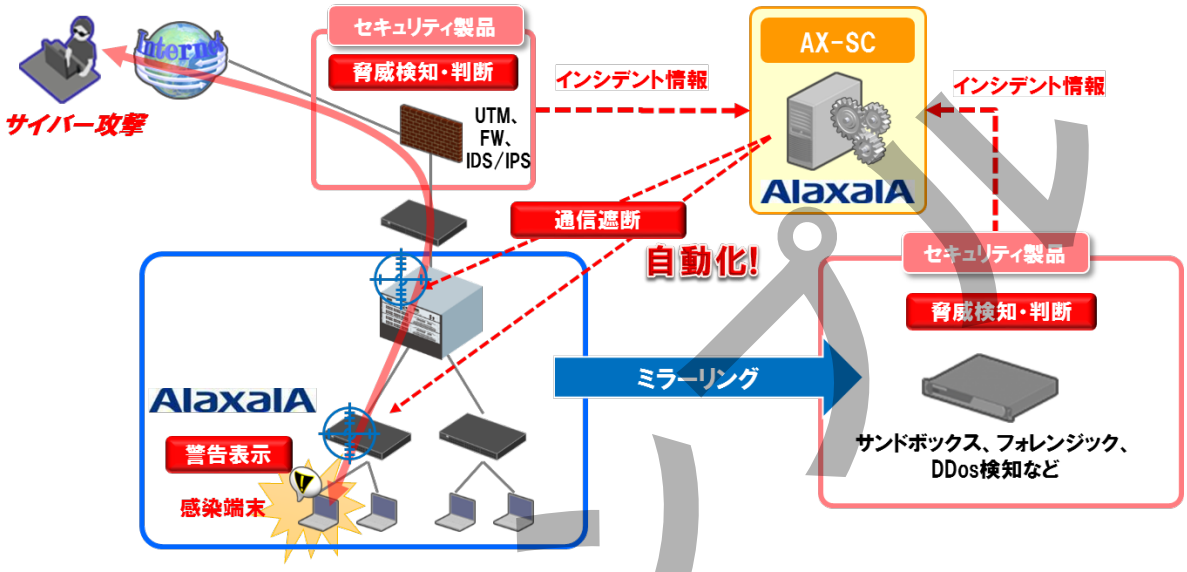


図 1-2　ソリューションの概要

2. パロアルトネットワークスとのソリューション連携

2.1　ソリューションのシステム要件

アラクサラのサイバー攻撃自動防御ソリューションのシステム要件について説明します。本ソリューションは、AX-Security-Controller および AX-Security-Controller と連携する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アラクサラの管理対象装置によって実現します。以下にそれぞれの製品の概要を示します。

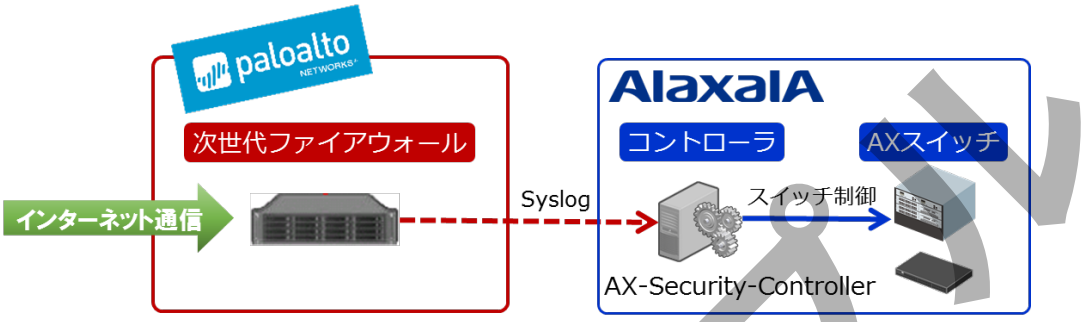


図 2-1　システム要件

(1) パロアルトネットワークス 次世代ファイアウォール

パロアルトネットワークスの次世代ファイアウォールは、アプリケーション、ユーザ、コンテンツに基づいて、あらゆるネットワークトラフィックを識別し、さらに侵入防御(IPS)やアンチウィルス、アンチスパイウェア等からなる脅威防御の機能を備え、組織内部と外部間の通信を監視して、マルウェアの活動の検知が可能です。

(2) AX-Security-Controller (AX-SC)

AX-Security-Controller(以下 AX-SC)は、ネットワーク上の端末位置情報を管理するトポロジ管理をおこないます。次世代ファイアウォールがインシデントを検出した場合、トポロジ管理と連携させ、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-SC を管理することができます。

AX-SC は次世代ファイアウォールと連携することにより、以下の機能を提供します。

(a) 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

(b) 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、セキュリティ装置からの指示および AX-SC が抽出したインシデントと連携して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
- 端末と攻撃サーバー(C&C サーバー等)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 や手動で感染端末の IP アドレスが変更されても、追従して遮断

(3) AX スイッチ(管理対象装置)で利用する機能

サイバー攻撃自動防御ソリューションは、トラフィックを監視するためのミラーリング機能と通信を遮断された感染端末に注意を促す警告表示機能を利用します。 機能の詳細については、製品マニュアルを参照ください。

➢　**ミラーリング機能**

アラクサラの AX スイッチに実装するミラーリング機能を使用しておもにエッジスイッチ上の内部通信を次世代ファイアウォールに転送します。ミラーリング機能には、ポートミラーリング、ポリシーベースミラーリング、リモートミラーリングの 3 種類があります。ミラーリング機能については、「付録 2」を参照ください。

➢　**端末警告表示**

AX-SC により通信を遮断された端末のブラウザ上に、警告表示する機能。端末と接続するエッジスイッチが端末からの HTTP 通信を検出して、警告画面を表示します。

2.2　連携ソリューションの特徴

次世代ファイアウォールとの連携により マルウェアに感染した端末を検出し、感染端末の通信を自動的に遮断することができます。以下に本ソリューションの特徴について説明します。

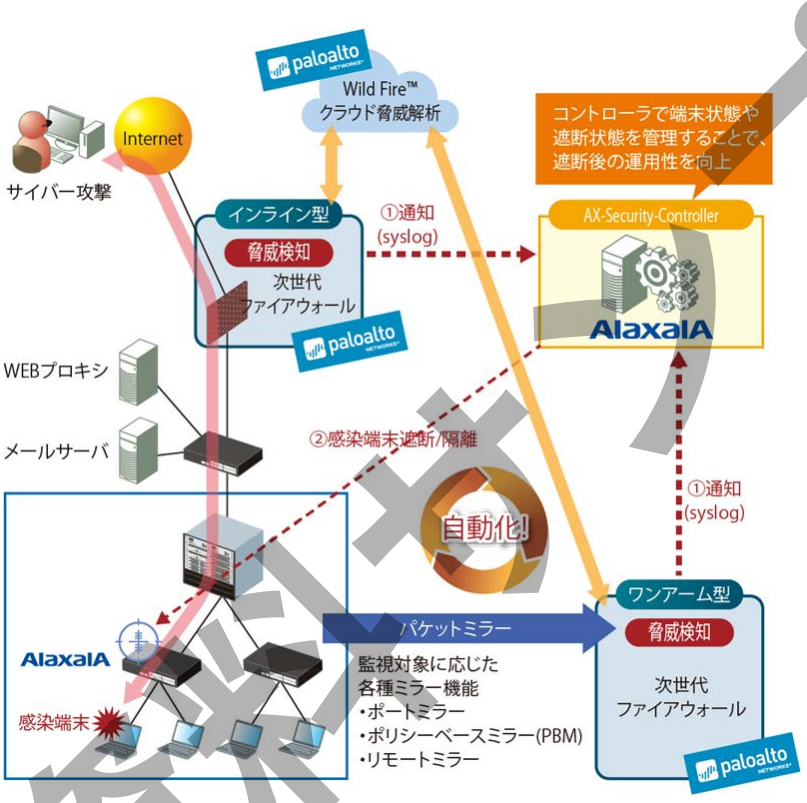


図 2-2　感染端末の通信の自動遮断

◆　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

(a)　インライン型（入口／出口対策）

ファイアウォールの位置に設置し外部との通信を監視します。通信遮断は AX スイッチだけでなく、ファイアウォール位置での遮断も可能となります。

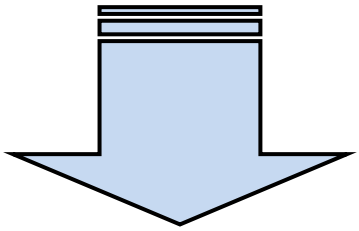
(b)　ワンアーム型（内部対策）

AX スイッチのミラーリング機能を利用して内部通信を監視し、通信遮断は AX スイッチのみで実施します。

◆　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

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します。細かくポリシーを設定することが可能です。

気になる続きは…



・アラクサラ　インテグレータ会員

または

・ビジネスパートナー様会員

にご登録いただければ、全てをご覧いただけます！

アラクサラ インテグレータ会員またはビジネスパートナー様会員へ登録することで、アラクサラ製品のご利用にあたり役立つ各種資料(システム構築ガイドなど)を全て閲覧することができます。ぜひこの機会にご登録下さい。

アラクサラネットワークス株式会社

〒212-0058
川崎市幸区鹿島田一丁目１番２号 新川崎三井ビル西棟
http://www.alaxala.com/