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

～トレンドマイクロ編～

初版

資料 No. NTS-17-R-003

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 トレンドマイクロ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 ユーザーズガイド
  (http://www.alaxala.com/jp/techinfo/guide/index.html)
- トレンドマイクロ
  (http://www.trendmicro.co.jp/jp/index.html)

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、ユーザー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. 1.0.A
- トレンドマイクロ製品
  Trend Micro Policy Manager™
  Deep Discovery™ Inspector

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。
- 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。
- 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 サーバとの通信許可、特定のサーバ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について、サーバ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。

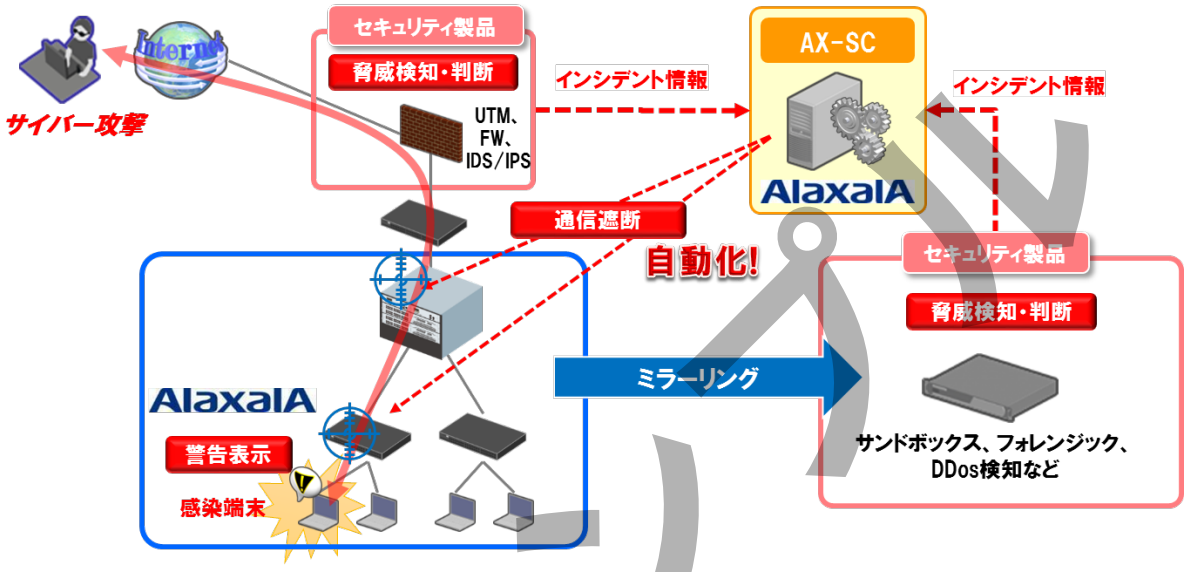


図 1-2　ソリューションの概要

2. トレンドマイクロ社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 と連携するトレンドマイクロ社のセキュリティ装置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。

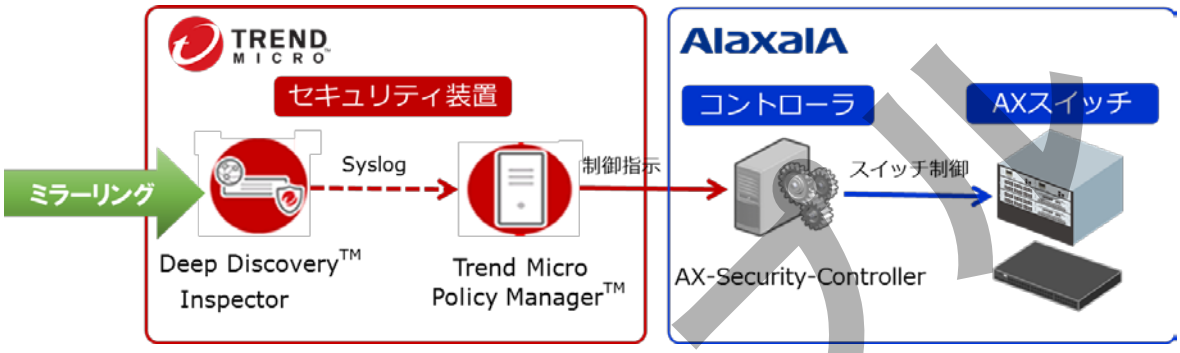


図 2-1　システム要件

◆ トレンドマイクロ セキュリティ装置

・ **Deep Discovery™ Inspector (DDI)**

Deep Discovery Inspector(以下 DDI)は、気付くことが難しい標的型攻撃やゼロデイ攻撃をネットワーク上の振る舞いから見つけ出し、早期に対処し被害の深刻化を防ぐための対策製品です。攻撃の初期段階から内部の拡散、外部への通信に至るあらゆる攻撃フェーズにおいて、不正なファイルや通信の検知に加え、管理ツールを悪用した攻撃まで発見します。

・**Trend Micro Policy Manager™ (TMPM)**

Trend Micro Policy Manager(以下 TMPM)は、IT インフラ上の複数の監視ポイントでトレンドマイクロのセキュリティ製品が検知したイベントをトリガとし、ネットワークレイヤの制御コントローラとの連携により、企業の運用ポリシーに紐づいた動的なネットワーク制御を実行することが可能です。

トレンドマイクロの「DDI」をセキュリティセンサーとして使用し、センサーで検知したネットワーク上の振る舞い、不正プログラム感染などのインシデント情報に基づいて、「TMPM」が企業の運用ポリシーに沿ってコントローラやスイッチを介してネットワークを動的に制御します。

◆ 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。セキュリティ装置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 はセキュリティ装置と連携することにより、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(C&C サーバ等)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

◆ 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インターネットの外部通信やエッジスイッチ上の通信をセキュリティ装置に転送します。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。

- **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　ソリューションの基本動作

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。以下にその動作について説明します。

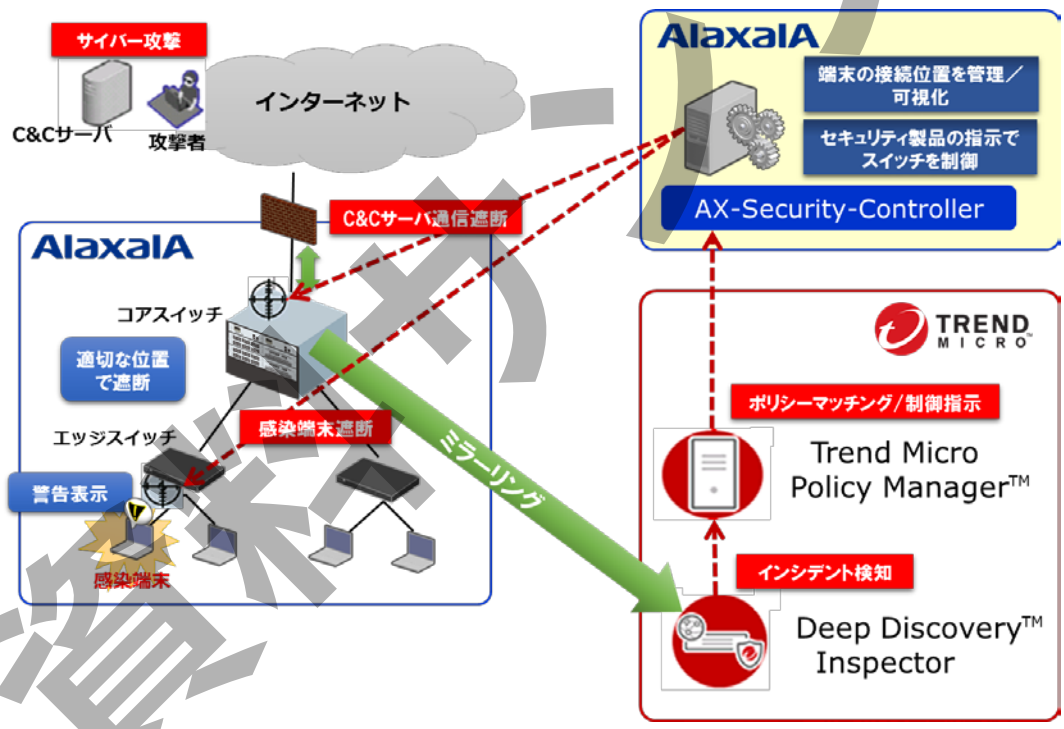


図 2-2　感染端末の通信の自動遮断動作

- 「AX-Security-Controller (以下 AX-SC)」は、端末がどのスイッチのどのポートに接続されているか自動的に把握します。
- アラクサラの AX シリーズ スイッチは、「ミラーリング機能」により、監視対象とするトラフィックを「Deep Discovery™ Inspector (以下 DDI)」へ転送します。
- 「DDI」 はトラフィックの振る舞いから脅威を検知すると、インシデント情報として、脅威種別や感染端末の IP アドレスを「Trend Micro Policy Manager™ (以下 TMPM)」へ通知します。
- 「TMPM」 は、通知された脅威情報が該当するポリシーにマッチした場合、制御指示（通信遮断等）と端末の IP アドレスを「AX-SC」へ通知します。
- 「AX-SC」 は、通知される IP アドレスからネットワーク上の感染端末の位置を特定し、該当端末が接続されているエッジスイッチへ通信遮断の設定を行います。
- 以後、感染端末の通信は事前に許可した通信を除いて全て遮断されます。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が表示されます。

2.3　トラフィックの監視方法

トラフィックを監視する方法として AX スイッチのミラーリング機能を使用します。ミラーリング機能には、以下に示す 3 つのパターンがあり、使用用途に合わせて選択可能です。

(1) ポートミラーリング

ポートミラーリングは、特定のポートで 送受信するパケットをコピーして 指定した物理ポートへ送信する機能です。インターネット通信のすべてのトラフィックを監視する場合などに使用します。

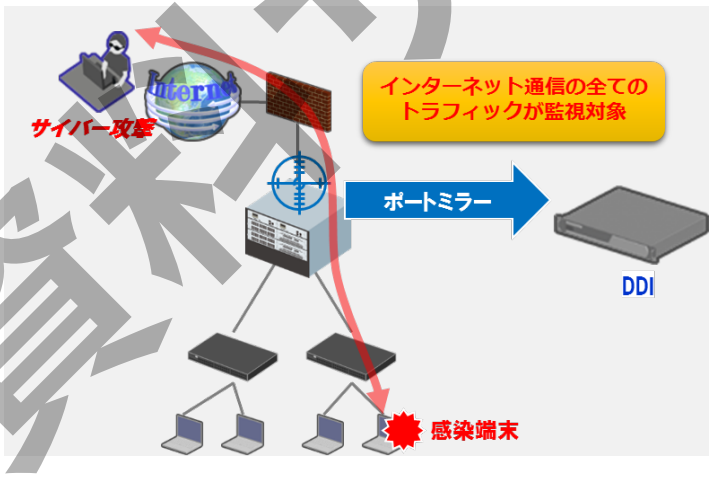


図 2-3　ポートミラーリング

(2) ポリシーベースミラーリング

ポリシーベースミラーリングは、スイッチを通過するパケットのうち 事前に設定したポリシーに従って、該当するパケットをコピーして、本来の転送先とは別のポートに出力する機能です。大量のトラフィックの中から、メールや Web 通信などに絞って 監視対象のトラフィックのみを監視することができます。

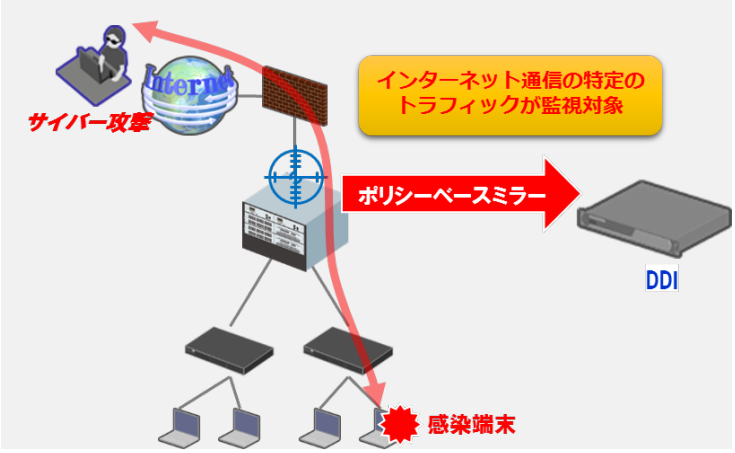


図 2-4　ポリシーベースミラーリング

(3) リモートミラーリング

リモートミラーリングは、エッジスイッチ上を通過する端末間のパケットをコピーして上流のスイッチに転送するミラー機能です。この機能を利用して、コピーしたパケットをコアスイッチおよびセキュリティ装置に向けてミラーし、トラフィックの監視や解析をおこないます。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。

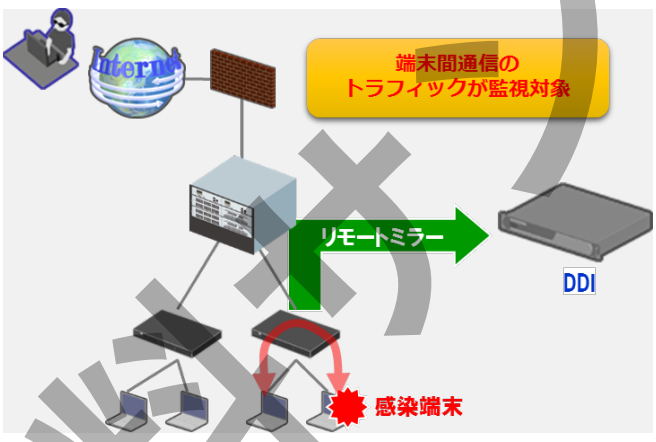


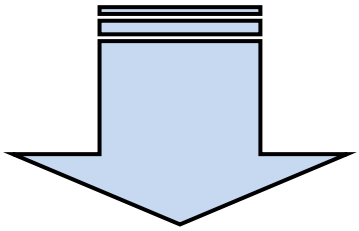
図 2-5　リモートミラーリング

また リモートミラーリングには、すべての端末間通信を監視する常時ミラーと 特定の端末通信のみを監視する詳細ミラーの 2 つの方式があります。

表 2-1　リモートミラーリングの方式

ミラー方式	特徴
常時ミラー	エッジスイッチ上を流れる端末間通信のミラーパケットをセキュリティ装置へ転送します。 端末間通信を常に監視する場合に使用します。
詳細ミラー	インシデント検出を契機に、特定の端末通信のミラーパケットをセキュリティ装置へ転送します。 インシデント検出時、マルウェア感染の被疑端末の通信のみを集中監視する場合に使用します。

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/