News Release

2017年6月1日
アラクサラネットワークス株式会社

トレンドマイクロのセキュリティ製品との連動で、サイバー攻撃自動防御ソリューションを強化
～マルウェア感染端末を検出して、通信を自動遮断～

アラクサラネットワークス株式会社（本社： 神奈川県川崎市 代表取締役社長 南川育穂 以下アラクサラ）は、トレンドマイクロ株式会社（本社： 東京都渋谷区 代表取締役社長 エバ・チェン 以下、トレンドマイクロ）のセキュリティ製品「Trend Micro Policy Manager™（以下、TMPM）」、及び「Deep Discovery™ Inspector（以下、DDI）」との連携により、サイバー攻撃自動防御ソリューション（*1）の強化を行います。TMPM、DDIとの連携により、マルウェアに感染した端末を検出し、端末の通信を自動的に遮断することが可能になります。
アラクサラでは、この連携動作を可能とするために、スイッチ製品の制御を行うソフトウェア「AX-Security-Controller（以下、AX-SC）」を製品化します。

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ヒ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（TMPM、DDI等）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ヒ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。

アラクサラは、これらの課題を解決するため、サイバー攻撃自動防御ソリューションを強化して、次の特長を提供します。

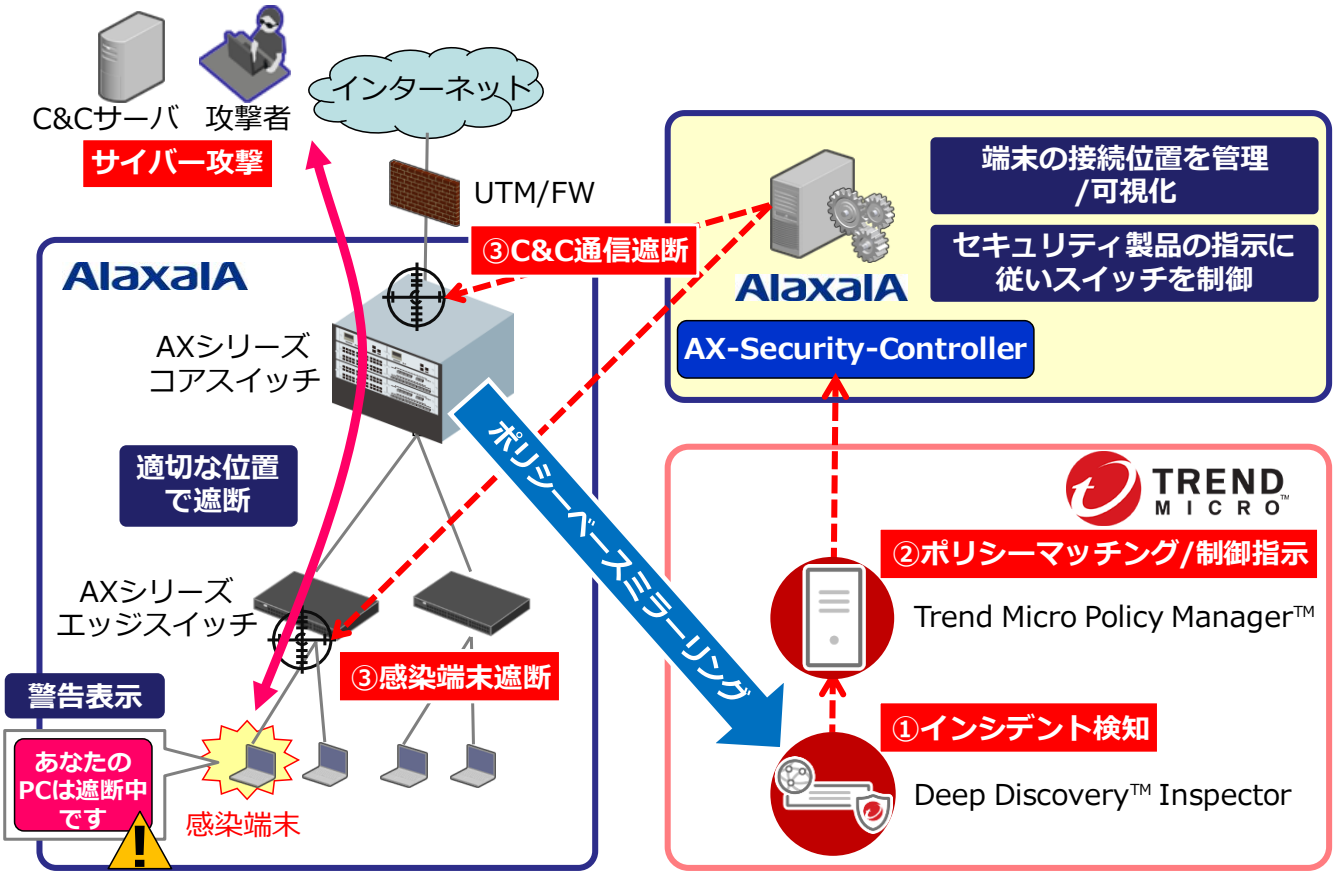
［特長］
- セキュリティ製品との連携によりマルウェアに感染した端末を検出し、感染端末の通信を自動的に遮断できます。
- リモートミラーリング機能（*2）により、セキュリティ製品が直接接続していない、エッジスイッチ上の端末間通信の監視ができます。これにより、感染端末からの隣接端末やサーバ等への探索や感染拡大の活動も監視でき、セキュリティ製品での検知率の向上が期待できます。
- 感染端末がネットワーク内を移動しても、追従して遮断します。また、DHCPを利用した環境において、感染端末のIPアドレスが変更されても、遮断を継続できます。
- 通信を遮断した感染端末のブラウザ画面上に警告表示を出し、端末の使用者へ通知することができます。端末に特別なソフトウェアのインストールは不要です。（*3）

さらに、リリース済のポリシーベースミラーリング機能（*4）を併用することで、セキュリティ製品へ転送するトラヒックを選択的に抽出することができます。これにより、セキュリティ製品の処理能力を抑え、セキュリティ製品の投資効率を高めることができます。

この実現のため、トレンドマイクロのTMPM、DDIと連携し、ネットワークの制御を行うAX-SCを製品化します。AX-SC、TMPM、及びDDIは次のように動作します。

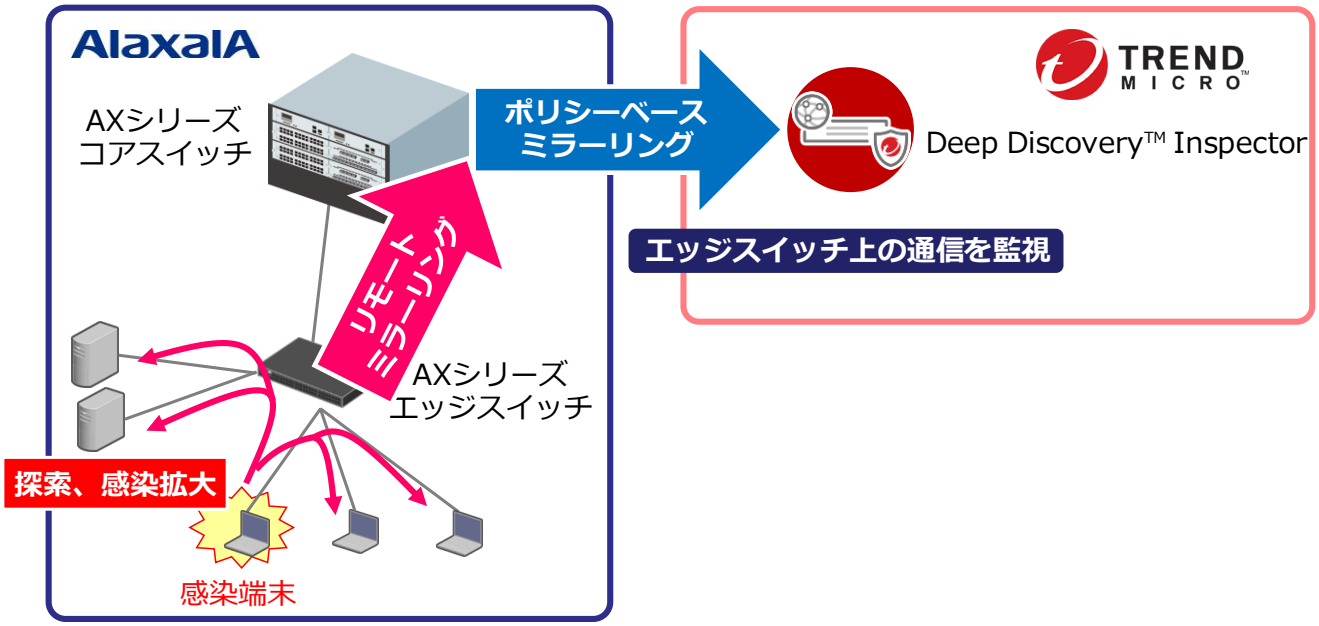
感染端末の通信の自動遮断

- 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、ポリシーベースミラーリング機能により、監視対象とするトラヒックのみをDDIへ転送します。
- DDIはトラヒ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、感染端末の通信は全て遮断されます。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。



エッジスイッチ上の通信の監視

- エッジスイッチのリモートミラーリング機能により、スイッチ上を通過するパケットを、コアスイッチに向けてミラーします。
- コアスイッチのポリシーベースミラーリング機能により、エッジスイッチからミラーされてきたパケットの中から監視対象とするパケットを選択的に抽出してDDIへ転送します。
- DDIは、従来監視できていなかった、エッジスイッチ上のトラヒックも監視できるため、インシデント検知率の向上が期待できます。



トレンドマイクロ IoT 事業推進本部 ソリューション推進部 部長の津金英行氏は「アラクサラネットワークスが提供するスイッチ製品の制御ソフトウェアとトレンドマイクロのセキュリティ製品の連携を歓迎します。両社の製品連携により、企業ユーザが標的型攻撃に代表される昨今のサイバー攻撃を早期に検知し、迅速な初動対応を行うことでリスクを最小化できることを確信しています。」とコメントしています。

AX-SCは、2017年7月からの出荷を予定しております。
また、今後アラクサラは、サイバー攻撃自動防御ソリューションで連携するセキュリティ製品を順次拡大していく予定です。

なお、2017年6月7日から幕張メッセで開催される Interop Tokyo 2017 のアラクサラブースにおいて、本連携ソリューションのデモを行います。

製品一覧

ソフトウェア名	予定標準価格（税抜）
AX-Security-Controller	400,000円～

AX-Security-Controllerの動作環境

ソフトウェア名	AX-Security-Controller
OS	Windows 10, Linux CentOS 7
必須ソフトウェア	python 3.3以上
CPU/必要メモリ	Intel Core iシリーズ以上/4.0GB以上
ディスク容量	20GB以上
サポート機器	AX8600S/AX8300S/AX3660S/AX2530S/AX260A (※)
管理最大機器数	200台 (※)

(※)サポート機器、管理最大機器数は将来拡張予定

*1 2016年6月2日プレスリリース「ネットワークフォレンジックス／マルウェア検知の連携によるサイバー攻撃自動防御ソリューションを製品化」
http://www.alaxala.com/jp/news/press/2016/20160602.html

*2 リモートミラーリング機能
エッジスイッチ上を通過するパケットをコピーして指定のVLANに転送する機能。
リモートミラーリング機能をサポートする機種は以下となります。本機能は2017年7月にリリース予定です。
AX3660Sシリーズ、AX2500Sシリーズ、AX260Aシリーズ

*3 端末警告表示機能
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/HTTPS通信を検出して、警告画面を表示します。
端末警告表示機能をサポートする機種は以下となります。本機能は2017年7月にリリース予定です。
AX2500Sシリーズ、AX260Aシリーズ

*4 ポリシーベースミラーリング機能
スイッチを通過するパケットのうち、あらかじめ指定された選択条件に一致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。大量のデータトラヒックの中から、監視対象とするトラヒックのみを選択的に抽出することが可能になります。
ポリシーベースミラーリング機能をサポートする機種は以下となります。
AX8600Sシリーズ、AX8300Sシリーズ、AX4600Sシリーズ、AX3660Sシリーズ：リリース済。
AX2500Sシリーズ、AX260Aシリーズ：2017年7月にリリース予定です。

■ アラクサラネットワークス株式会社について

アラクサラネットワークス株式会社は、「快適で安心して使えるネットワークを世界の人々に提供し、豊かな情報通信社会の実現に貢献」を企業理念としています。情報ライフラインを支える概念としてギャランティード・ネットワークを提唱し、ネットワーク構築に必要な基幹系ルータおよびスイッチの開発から設計、製造、販売、保守のサービスを提供しています。

会社名	アラクサラネットワークス株式会社
設立日	2004 年 10 月 1 日
代表者	代表取締役社長 南川育穂
資本金	55 億円
所在地	神奈川県川崎市幸区鹿島田一丁目1番2号 新川崎三井ビル西棟
従業員数	約 210 名 （2017 年 3 月末現在）
URL	http://www.alaxala.com/

■ 商標名称等に関する表示

■ 製品に関するお問い合わせ先

アラクサラネットワークス株式会社 ネットワークシステム部
〒212-0058 神奈川県川崎市幸区鹿島田一丁目1番2号 新川崎三井ビル西棟
URL： http://www.alaxala.com/jp/contact/

■ 報道機関お問合わせ先

アラクサラネットワークス株式会社 広報担当 【担当： 新井】
〒212-0058 神奈川県川崎市幸区鹿島田一丁目1番2号 新川崎三井ビル西棟
電話：044-549-1706(ダイヤルイン)
URL： http://www.alaxala.com/jp/contact/