全学情報セキュリティを強化する ネットワークサイバー攻撃自動防御システム

萩原洋一*1・三島和宏*1・櫻田武嗣*2・辻澤隆彦*1
Email: hagi@cc.tuat.ac.jp

*1: 東京農工大学総合情報メディアセンター
*2: 情報医学研究所

◎Key Words サイバー攻撃，キャンパス情報ネットワーク，自動遮断

1. はじめに

大学は、先端研究情報や研究者・学生の個人情報（メールアドレス等）を多量に保有し、さらに情報セキュリティ対策がなされていない端末やサーバが存在する。大学に対する標的型攻撃やマルウェアなどによるサイバー攻撃が増加しており、サイバー攻撃に対する情報セキュリティ対策が急務である。一方、本学での情報環境として次のような特色がある。①グローバル教育を推進し海外留学生など多様な学生や研究者が在籍（東南アジア、中南米、中近東など）、②オープンな教育・研究環境を目的にBYODを推進した結果、個人の各種デバイス（PC、スマートフォン、タブレットなど）がキャンパス全域での活発利用、③キャンパス全域に講義室や実験実習室が分散、④FSセンターを中核とした野外フィールドワークのエリアが多い。これらの環境条件におけるキャンパス情報ネットワークを従来から提供してきたが、これまでの検疫対策のみでは十分な情報セキュリティの確保が難しくなった。

そこで高度に連携した「サイバー攻撃自動防御ソリューション」を導入し、セキュリティ対策の強化を図った。この結果インシデント発生時に従来必要であった感染拡大防止のための初動作業が人手を介さずに自動化、管理者の負担軽減を図る。

2. キャンパス情報ネットワーク

2.1 構成

本学のキャンパス情報ネットワーク（図１参照）は、2017年9月に更新し、ATnet6として第六世代となる。二つのキャンパス間は10Gbps×3回線のWDMによる接続で、自動防御ソリューションを導入したことによるトラフィックの増大に十分に耐える構成とした。大きな建物は、各階のエッジスイッチをリング構成とし、小さな建物は、複数建物でリング構成としている。約200台のレイヤ２エッジスイッチと約320台の無線LANアクセスポイントを配備し有線接続と合わせて１日あたり約8,000～10,000台の接続がある。原則IEEE802.1x認証による接続形態である。

2.2 導入理由

①OSの自動検疫チェックやセキュリティ対策ソフトのパターンファイルアップデートだけでは防御しきれなくなってきた、②研究室で利用が進んでいる家庭用ブロードバンドルータでのセキュリティ脆弱性を突かれるケースが散見されていた、③人手を介さず24時間対応が可能であること、④パケットの中身を管理者が見る必要がなくなること。

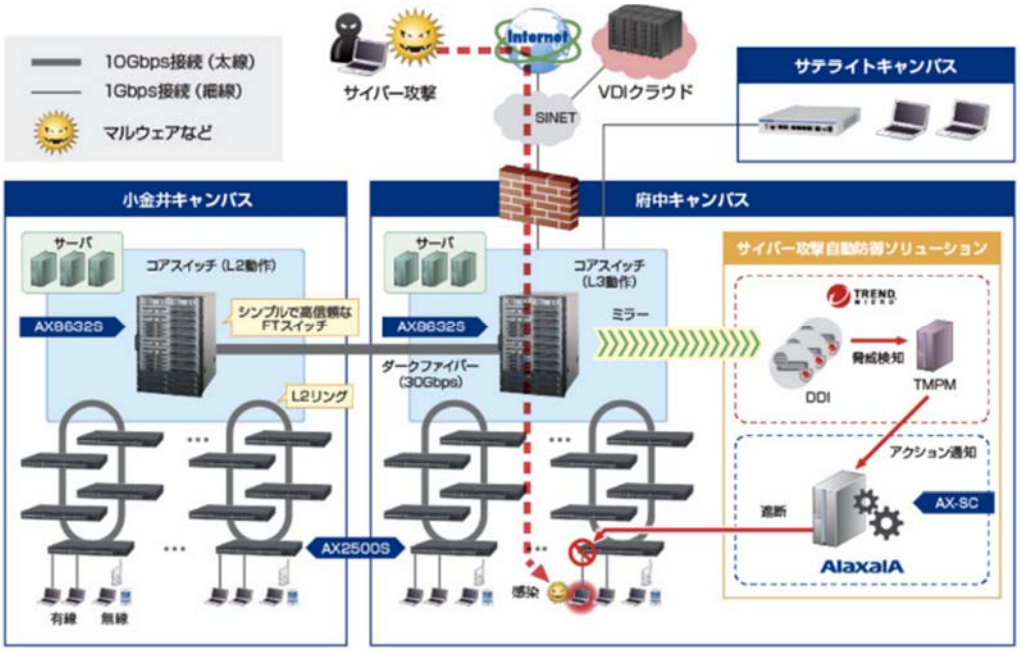

図１．概念図

出所：「アラクサラネットワークス(株)事例：国立大学法人東京農工大学」

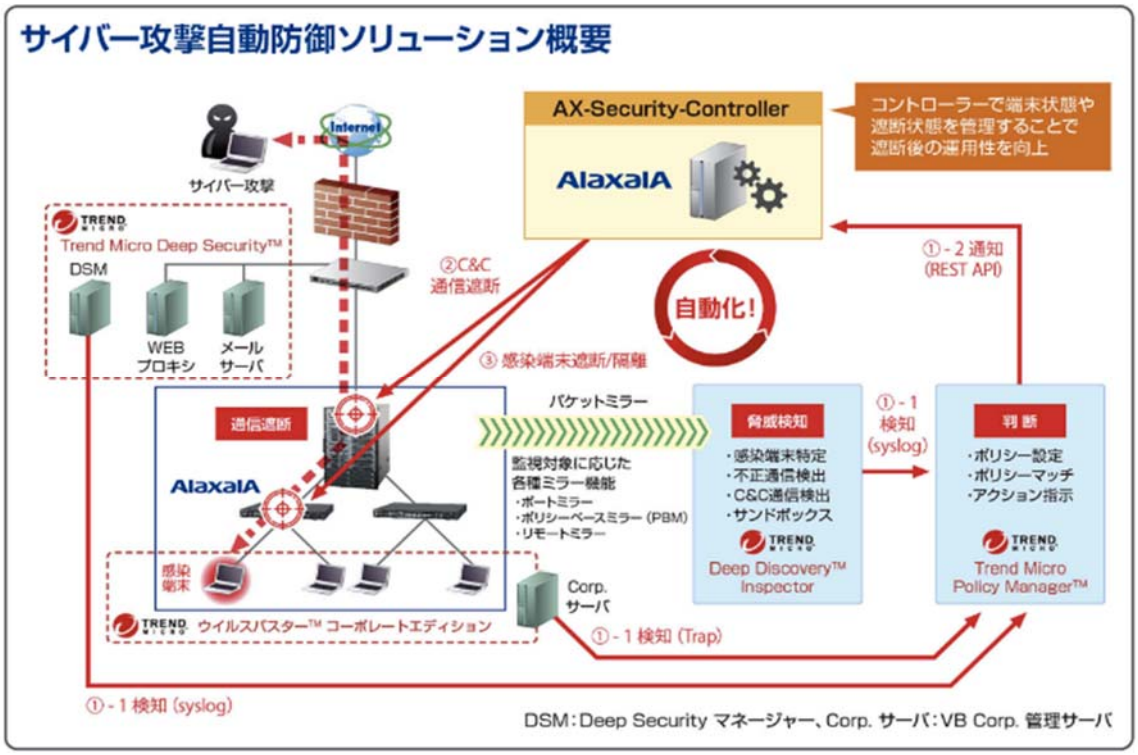

図２．動作概念図　出所:「アラクサラネットワークス(株)事例:国立大学法人東京農工大学」

3. 自動遮断

3.1 有線 LAN 端末

感染端末をキャンパス情報ネットワークから自動隔離するシステムの連携関係を図 2 に示す。コアスイッチに入る通信は全てミラーリングし、複数台で構成されるセキュリティ検知システム DDI（Deep Discovery Inspector）で脅威解析を行う。脅威が検出された場合、セキュリティポリシーを設定する TMPM（Trend Micro Policy Manager）において脅威レベルを判定、AX-SC（Alaxala Security Controller）へ連携して処理が行われる。

最も脅威が大きいものに関しては即時遮断を行うために、AX-SC から当該端末が接続されている場所に一番近いエッジスイッチの接続ポートにて当該端末をキャンパス情報ネットワークから切り離す隔離処理を行う。

経過観察を行う必要があると TMPM が判断した場合は、AX-SC がエッジスイッチのリモートミラーリングする設定を有効にして端末に近い箇所の通信を DDI に送信して脅威の判断を行う。

3.2 無線 LAN 端末

無線 LAN については、無線 LAN コントローラから出て来た通信を一度エッジスイッチ経由でルータへ転送する形とする。エッジスイッチのポートをミラーリングして DDI へ通信を送り脅威解析を行う。隔離遮断は有線 LAN と同じ仕組みである。

3.3 解除

遮断端末の情報は利用者に公開する。具体的には、MAC アドレスや IP アドレス、接続場所の情報などを G Suite（Google Apps）に掲示される。利用者は大学の Google 系サービス利用アカウント認証後にアクセス可能である。

端末が遮断されている場合は、OS 再インストールによるクリーン処理、または、アップデートやウィルス対策ソフトウェアの導入を行った後に解除申請を申し込む。一定時間後に自動的に遮断が解除される。ただし、脅威が残っていた場合には遮断が再び行われる。

4. おわりに

本稿では、全学情報セキュリティ対策のための、自動防御ソリューションについて述べた。現在は、脅威レベルの高いものに限定して自動隔離機能を動作させているが、今後どの程度の脅威レベルが適切なのかの判断材料を蓄積し、チューニングしつつ本ソリューションを導入する大学とノウハウ等の情報交換が行えればと考えている。

参考文献

(1) 櫻田武嗣, 辻澤隆彦, 萩原洋一, 三島和宏 : “不正端末検出のためのネットワークトラフィックモニタ型キャンパスネットワークの設計”, 情報処理学会インターネットと運用技術(IOT)研究報告, vol.2017-IOT-38, No.2, pp.1-3 (2017.6).

(2) アラクサラネットワークス(株) : “事例 : 国立大学法人東京農工大学様”, http://www.alaxala.com/jp/introduce/case36/（2018.3）.

(3) トレンドマイクロ(株) : “導入事例 : 国立大学法人東京農工大学”, https://www.trendmicro.com/ja_jp/about/customer-stories/2017/tuat-201711-01.html (2018.3).

(4) エイチ・シー・ネットワークス(株) : “導入事例 : 国立大学法人東京農工大学”, https://www.hcnet.co.jp/case/tat.html（2018.3）.

(5) 東京農工大学総合情報メディアセンター年報, 2017, https//web.tuat.ac.jp/~imc/ (2018.6)