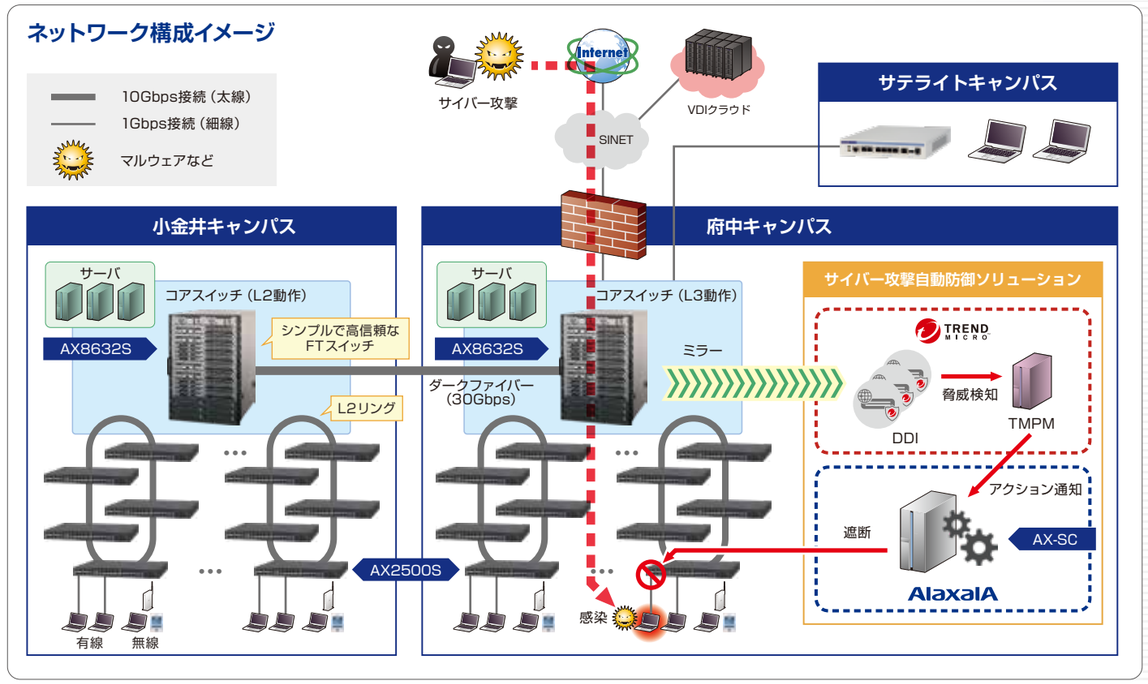
導入事例

国立大学法人 東京農工大学様



萩原　システム管理者の負担も軽減される見込みです。これまではひとたびインシデントが発生すると、感染の拡大を防ぐための対策や復旧作業に多くの時間が割かれていました。しかし、今回の「サイバー攻撃自動防御ソリューション」は検知後の初動対応を自動化してくれるため、落ち着いて事後の対処ができます。また、そのぶんのリソースをユーザへの啓発活動や脆弱性の分析など、今まで対応できなかったことに振り分けることも可能になりました。

さらには、トラブル対応を依頼していた保守ベンダーの負担も減りますので、原因の分析に時間を割いてもらえるようになりそうです。その他の効果としては、コアスイッチの集約により設置スペースが削減できたこと、スイッチの台数が減ったことで故障や障害発生による運用負荷が軽減できたことも挙げられます。

――今後の展望とアラクサラに対する期待についてお聞かせください。

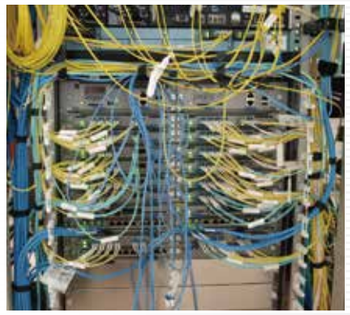
櫻田　他のベンダーのセキュリティ製品も加えた「多層防御」を検討しています。今は各社からいろいろと面白い製品がリリースされていますので、これらとうまく連携し、パケットの深いレベルまで可視化できるようなセキュリティ体制を整えられればと考えています。

辻澤　「サイバー攻撃自動防御ソリューション」を導入してから時間がたっていないこともあり、現在はセキュリティの検知レベルを厳しめに設定し、多くの脅威を検出しています。しかし、影響の少ない軽微な脅威を理由に止めてしまうと、警告が頻発しユーザの利便性が低下するばかりか、管理者の運用負荷も増えてしまいます。そこで、今後はどの程度の脅威までを自動的に止めればよいのか、最適なしきい値を探っていく予定です。そのためにも、アラクサラには他の大学に向けて積極的に「サイバー攻撃自動防御ソリューション」を広めてもらい、そこで蓄積した運用に関するノウハウを大学間で共有できるようになるとありがたいですね。

――ありがとうございました。

（※1）リングプロトコル：スイッチをリング状に接続することで、柔軟かつスケーラブルなシンプルネットワークを構築するアラクサラ独自のプロトコル。

（※2）フォールト・トレラント・アーキテクチャ：障害発生時に最小限の切替時間で運転を継続するための仕組み。



サイバー攻撃自動防御ソリューションを支えるAX8632S

アラクサラ ネットワークス株式会社
〒212-0058
神奈川県川崎市幸区鹿島田1丁目1番2号 新川崎三井ビル西棟13階
URL：http://www.alaxala.com/

CASE STUDY

導入事例

AlaxalA

国立大学法人 東京農工大学 様

ウイルスに感染した端末を自動的に隔離する「サイバー攻撃自動防御ソリューション」により全学規模でネットワークのセキュリティを強化、管理者の負担も軽減

東京農工大学は、標的型攻撃やマルウェアなど増大する脅威に対応するため、ネットワークの更新に合わせてセキュリティ強化を決断。アラクサラの「サイバー攻撃自動防御ソリューション」を導入した。これにより、学内のネットワークを利用するPC、タブレット、スマートフォンなどあらゆる端末のウイルス感染を素早く特定・隔離することが可能になり、セキュアなネットワーク環境が実現。また、インシデント発生時の対応も自動化されたため、システム管理者の負荷も軽減され、そのぶんのリソースをユーザへの啓発活動や脆弱性の分析などに振り分けることが可能になった。

情報漏えいや乗っ取りのリスクを考えればネットワークのセキュリティ対策は急務

――東京農工大学の概要および特色を教えてください。

辻澤　産業の根幹である「農学」と「工学」の2分野に特化した国立大学法人です。学部生と大学院生併せて約6,000名の学生が在籍。両学部とも大学院生が多く、工学部は約8割、農学部は約6割が進学します。農学部が府中市、工学部が小金井市にキャンパスを持ち、それぞれが我が国でもトップレベルの教育・研究を推進しています。

萩原　私たちが所属する総合情報メディアセンターは、1967年に電子計算機室として発足。1985年に情報処理センターに改編され、2002年より現在のかたちになりました。主なミッションとしては、当初は学内ネットワークの設計・管理・運用、メインフレームの調達・運用・ユーザ支援でしたが、現在はこれらに加え、研究組織として情報基盤と応用分野の研究を行いつつ、学内の総合情報支援、将来構想の検討などを行っています。当大学には新しいものを積極的に採り入れていくフットワークの軽さがあり、情報システムについても、学生のPC持ち込み（BYOD）対応を全学で推進するなど、さまざまなチャレンジに取り組んでいます。

――「サイバー攻撃自動防御ソリューション」を導入するに至った背景についてお聞かせください。

櫻田　実は10年ちょっと前の2005年ごろからセキュリティ対策として自動防御の導入を検討していました。しかしシステムを試作し導入してはみたものの、ハードウェアの処理性能が追いつかないなどの問題があり、残念ながら途中で断念しています。その代わりというわけではありませんが、2011年に行われたネットワークの更改の際に検疫システムを新たに導入しました。この検疫システムは、学生や職員が学内ネットワークにアクセスする際、端末にWindows/MacOSのパッチが適用されているか、アンチウイルスソフトのパターンファイルが最新状態に更新されているかを高速でチェックし、NGの場合はネットワークへの接続を禁止。その旨をユーザに通知するものです。これにより、ユーザのセキュ

企業概要

東京農工大学

About　国立大学法人 東京農工大学

1874年に内務省勧業寮内藤新宿出張所へ設置された農事修学場と蚕業試験掛が前身。1949年の新学制施行とともに東京農工大学として改編される。産業の根幹をなす農学と工学を中心に、これらの融合分野まで含めた教育・研究を推進している。現在は第3期中期目標期間（2016 ～ 2021年）の学長ビジョンとして「世界が認知する研究大学へ―世界に向けて日本を牽引する大学としての役割を果たす―」を掲げ、「世界と競える先端研究力の強化」「国際社会との対話力を持った教育研究の推進」「日本の産業界を国際社会に向けて牽引「高度なイノベーションリーダーの養成」の4つの機能強化戦略に取り組んでいる。
https://www.tuat.ac.jp/

「従来の検疫システムでは対処できなかった自動防御が実現しセキュリティレベルは確実に向上しました」

国立大学法人 東京農工大学
総合情報メディアセンター
教授 博士（工学）
辻澤 隆彦 氏

国立大学法人 東京農工大学
総合情報メディアセンター
教授 博士（工学）
萩原 洋一 氏

国立大学法人 東京農工大学
総合情報メディアセンター
講師 博士（工学）
櫻田 武嗣 氏

リティ意識は向上しました。

ところがWindows 10が登場した2015年あたりから、検疫システムがOSのアップデートのタイミングと合わないことがあり、運用が難しくなってきました。さらに、2016年に仮想デスクトップを導入しBYODを全学で推進した結果、持ち込みのノートPCやタブレット、スマートフォンが増えてOSが多様化し、検疫システムに対応しない機器の持ち込みが増加してきたのです。また、無線LANからの接続も検疫システムの仕様から対象外としていたため、無線LANのセキュリティ強化も課題となっていました。

辻澤　論文の中で研究者や学生のメールアドレスがオープンにされていることもあり、大学は標的型攻撃のターゲットになりやすい傾向があります。また、世界各国の大学・研究機関と姉妹校協定を締結し、グローバル教育を推進している本学の場合、海外からの留学生も多いため、日本語への理解が今ひとつの方も多く、検疫システムだけで統制を効かせることは困難です。実際、過去には留学生が海外から届いた怪しいメールを開いてしまい、不正なWebサイトにアクセス。ウイルスに感染してしまったこともありました。

萩原　端末がウイルスに感染すると、最先端の研究情報や、研究者・学生・職員の個人情報が外部に流出してしまう可能性があります。それ以上に注意しないといけないのは、本学の端末が乗っ取られて踏み台として利用され、他の大学や産学連携している企業、外部の公的機関に攻撃を仕掛けてしまうリスクです。農学、工学、理学などの融合分野を研究している本学は、連携している各種機関の数も多いため、本学が原因のセキュリティインシデントはあってはなりません。

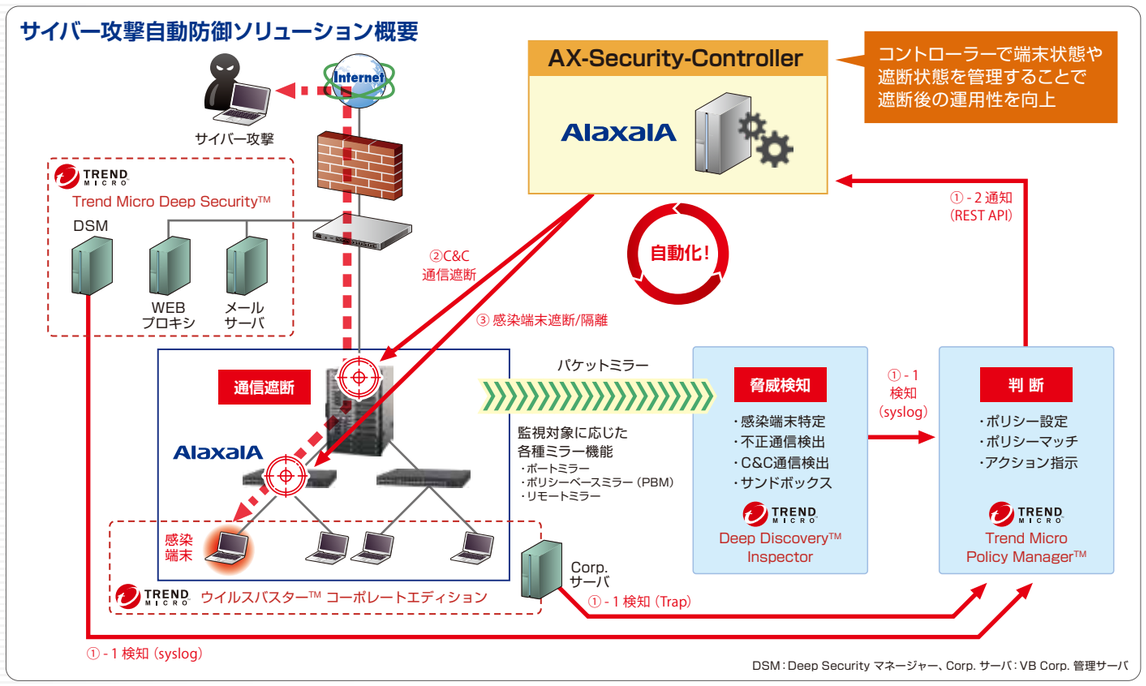
櫻田　近年、標的型攻撃やマルウェアなどの脅威が一段と増大していることを考えれば、ネットワークのセキュリティ対策は急務といえます。とはいえ、あまりガチガチに統制を固めてしまうとユーザの利便性は落ちますし、システム管理者の負担も大きくなってしまいます。そこで、ネットワークの更新を機に、オープンな環境をできる限り維持しつつ、セキュリティを強化できるようなしくみができないか検討することになったのです。

トレンドマイクロのセキュリティ製品と連携した自動防御ソリューションを採用

――「サイバー攻撃自動防御ソリューション」を導入した経緯をお聞かせください。

櫻田　2016年10月、学内に委員会を立ち上げて本格的な検討に着手し、自動防御を前提としたネットワークの仕様書を作成しました。具体的な要件としては、IPv6とIPv4のデュアルスタックで動いている端末が多くあったことから、IPv6対応というのがまずひとつ。さらに、複数のOSや外部から持ち込まれた端末にも対応できるようエージェントレスで利用できること、ネットワーク認証（ダイナミックVLANとIEEE 802.1x）やMACアドレス認証に対応していること、既存の検疫システムと遜色ないセキュリティレベルが維持できること、自動防御のポリシー設定が可能なことなどの点を盛り込みました。

これらの要件をもとに入札を実施したところ、アラクサラのスイッチとトレンドマイクロのネットワーク監視製品「Deep Discovery™ Inspector（以下、DDI）」およびネットワーク連携セキュリティ対策製品「Trend Micro Policy Manager™（以下、TMPM）」を組み合わせた「サイバー攻撃自動防御ソリューション」に決定しました。



アラクサラ製品のリングプロトコルおよび高耐久性を評価

――アラクサラ製品についてはどの点を評価されましたか。

櫻田　第一にコアスイッチの光ファイバの収容率の高さです。本学の場合、広大なキャンパスの中に講義棟や研究棟が散在しています。そのため、建屋間の光ファイバの敷設がネックとなるのですが、アラクサラのスイッチはリングプロトコル（※1）で冗長化できるため、少ない本数で多くの収容数を確保できるのはコスト削減という意味で大きいですね。

加えて、スイッチの高耐久性も評価しています。アラクサラのスイッチは2011年のネットワーク更改から本格的に利用していますが、ほとんど故障したことがありません。これまで他社のスイッチがかなりの割合で故障・交換している環境での故障の少なさは驚くべきことだと思います。

――導入から稼働までの流れをお聞かせください。

萩原　2017年6月に本格的な導入プロジェクトがスタート。翌7月にスイッチが納品され、3カ月後の10月より新しいネットワークに切り替えました。構築の際にはアラクサラからも技術的なサポートが提供され、おおむねスムーズに進みました。「サイバー攻撃自動防御ソリューション」にとって本学はファーストユーザになるそうですが、検証および改善という意味でもお互い有意義なプロジェクトになったと思います。

「AX-Security-Controller」がウイルスに感染した端末の通信を自動的に隔離し画面上に警告を表示

――新しいネットワークの構成についてお聞かせください。

櫻田　コアスイッチのAX8632Sは、府中キャンパスと小金井キャンパスに1台ずつ設置しています。2つのキャンパス間は30Gbpsのダークファイバーで接続。府中キャンパスのAX8632SはL3で動作させ、小金井キャンパスのAX8632SはL2スイッチとして利用しています。これらのスイッチは1台の装置に2台分の機能を実装したフォールト・トレラント・アーキテクチャ（※2）により内部で2重化。以前のネットワークでは、府中キャンパスにマルチレイヤー対応のAX6708Sを2台、小金井キャンパスにAX6708Sを3台設置していましたので、各キャンパスのスイッチが1台に集約されたことになります。外部とは、学術情報ネットワーク「SINET5」で接続しています。

それぞれの足回りとなるL2スイッチにはAX2530Sを採用し、リングプロトコルでシンプルな冗長化を図りました。「サイバー攻撃自動防御ソリューション」で制御しているL2スイッチの台数は全部で約200台。その配下には有線で繋がった端末のほか、約300台の無線LANアクセスポイントを配備し、併せて1日1万台近い端末からのアクセスをコントロールしています。

――自動防御の流れについて教えてください。

櫻田　「サイバー攻撃自動防御ソリューション」では、アラクサラの制御ソフト「AX-Security-Controller（以下、AX-SC）」とトレンドマイクロのDDIとTMPMが連携し、ウイルスに感染した端末を自動的にネットワークから隔離します。具体的には、府中キャンパスと小金井キャンパスに設置されたコアスイッチ（AX8632S）はポリシーベースミラーリング機能によって監視対象となるトラフィックをDDIに転送していますが、DDIがマルウェアやスパイウェア、トラフィックの異常な振る舞いなどを検知すると、その情報を該当端末のIPアドレスなどと共にTMPMへ送信。TMPMは受信した脅威情報とポリシーとを照らし合わせ、該当するポリシーに合致していると判断した場合、「通信を遮断せよ」という指示と端末のIPアドレスをAX-SCに通知します。AX-SCはIPアドレスをもとに感染した端末の接続位置を特定し、端末が収容されているエッジスイッチで該当端末の通信のみを遮断。また、コアスイッチ側では攻撃者からのC&C通信の遮断も可能です。その際、感染した端末の画面には警告が表示され、ユーザに対処を促します。こうした端末は適切な対処を行うことで、再び接続できるようになります。

システム管理者の負担が軽減されユーザへの啓発活動や脆弱性の分析が可能に

――今回の導入で得られたメリットについてお聞かせください。

辻澤　従来の検疫システムでは対処できなかった端末や環境における自動防御が実現し、セキュリティレベルは確実に向上しました。SINET5でつながっている大学や研究機関に対しても、少なくとも本学が原因となるセキュリティインシデントで影響を与える可能性は低くなったため、本学への信頼度が高まることも期待されます。

CASE STUDY