AlaxalA

導入事例

CASE STUDY

高知工科大学 様

「サイバー攻撃自動防御ソリューション」の導入によりインシデントの初動対応を迅速化、リアルタイムに端末の接続場所を特定するトレーサビリティも向上

学内に多種多様な端末とユーザーを抱える高知工科大学では、学外からインシデント通知が寄せられた際に端末を特定するのが難しく、管理面で大きな負荷となっていた。そこで同大学は、ネットワークの更新に合わせてセキュリティの強化を決断。アラクサラネットワークス（以下、アラクサラ）のスイッチおよび「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、対象の端末と接続場所をリアルタイムで特定できるようになり、自動防御で二次被害を確実に防ぐことが可能になった。また、端末のトレーサビリティも向上し、過去のログをさかのぼって確認できるようになっている。

大学の機密情報を守るという意味からも、インシデントへの迅速・的確な対応が必要

――高知工科大学の特色を教えてください。

福本　1997年4月の開学以来、「大学のあるべき姿を常に追求し、世界一流の大学をめざす」という目標のもと、学群専攻制、クォータ制、早期卒業などの先進的な制度をいち早く採用するなど、よりよい教育システムの実現に取り組んできました。

現在は県内に2つのキャンパスを構えており、中でも塀のない香美キャンパスは「アメリカ景観建造物協会優秀賞」「公共建築賞優秀賞」を受賞するなど、美しいキャンパスとして知られています。研究機器・設備も充実しており、これらを学生たちが使って実験できるような環境が整えられています。また、24時間使用できる施設が多いことも特徴です。

――ネットワークの更新に至った理由についてお聞かせください。

福本　ちょうどネットワークの更新時期が近づいていたこともありましたが、一番の目的はセキュリティを強化し、管理面での負荷を軽減したいという思いがあったからです。かつて本学ではセキュリティ対策を研究室単位で実施していたのですが、それでは管理に支障を来すようになっていたのです。

福冨　たとえば、年に数回ほど外部機関からインシデント通知が対象のIP情報とともに寄せられることがあります。こうした通知に対しては調査報告を行わなくてはならないのですが、いざ調べようとしてもIPアドレスだけでは端末を特定するのが困難で、担当者に大きな負担がかかっていたのです。

福本　本学では学内外をさまざまな通信が流れています。また、BYODを認めているため、ネットワークに接続する端末は教職員、学生のものを合わせて1万台以上になります。さらに、高知県立大学との法人統合により、2大学3キャンパス体制となり、VLANが一気に増加。一部サービスも共有するようになりました。このようにシステムや運用の環境が変化していく中、機密情報を守るという意味からも、インシデントに迅速・的確な対応ができるような環境を整備することが不可欠と考えました。そこで、ネットワークの更新に合わせ、セキュリティソリューションの導入を検討することにしたのです。

自動防御ソリューションおよび端末トレーサビリティ機能を高く評価

――製品の選定から導入までの流れを教えてください。

福冨　2016年末より5、6社の製品について情報を収集、検討を行いました。特に重視した点は、充実したセキュリティ機能を持つこと、インシデント時に対象の端末を容易に特定できることです。

福本　そして2018年に複数のベンダーから提案を受け、プロポーザル方式による入札を実施。その中からアラクサラ製品を核とした提案を採用しました。

福冨　構築の作業は夏期一斉休業（8月10日～20日）に合わせて実施しました。一応、予備日も設けていたのですが、それを使うこともなく、実質1週間かからずに作業を完了しています。

企業概要

高知工科大学
KOCHI UNIVERSITY OF TECHNOLOGY

About　高知県公立大学法人 高知工科大学

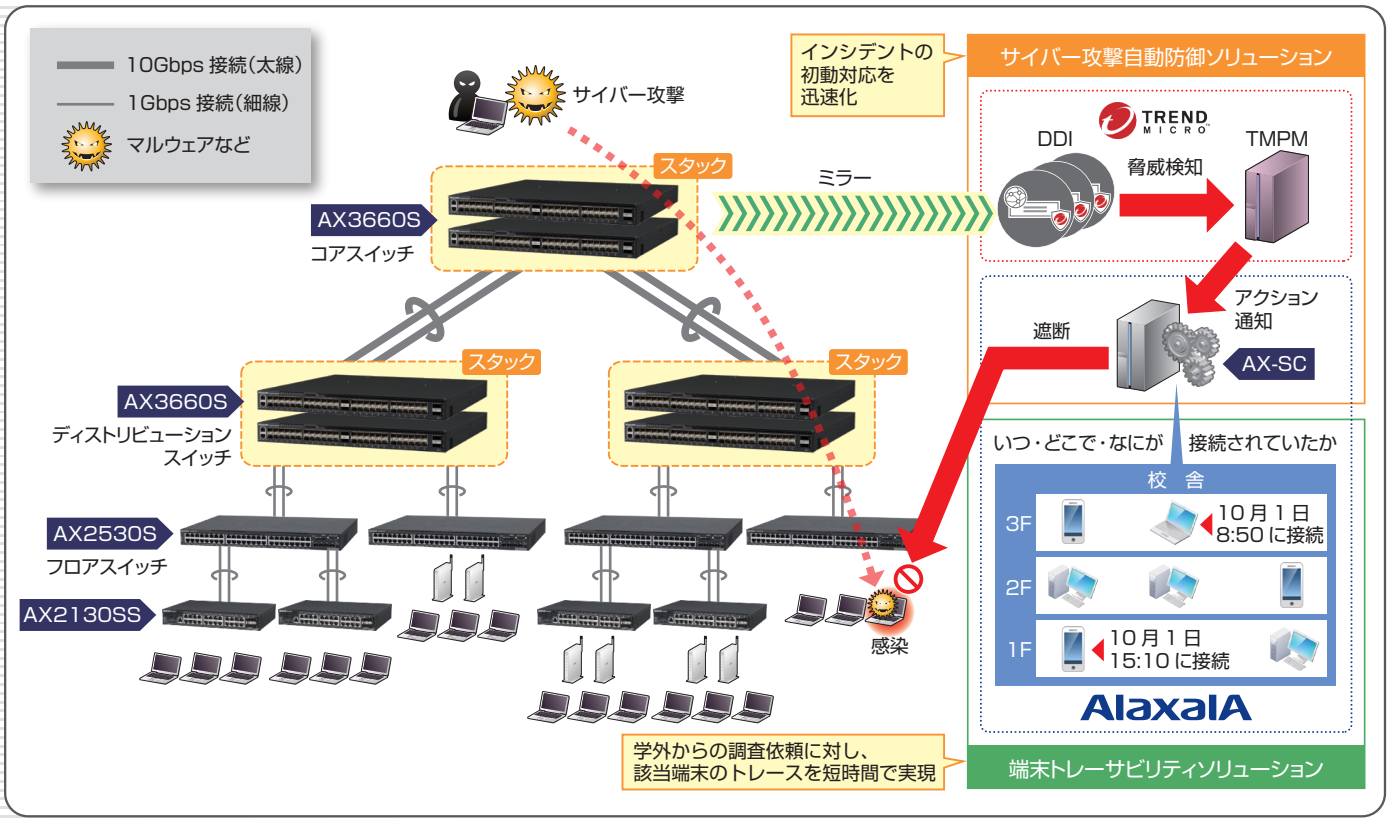
1997年4月に公設民営の学校法人として開学。2009年には日本初の私立大学から公立大学法人化、2015年には高知県公立大学法人と法人統合し、現在は、システム工学群、環境理工学群、情報学群、経済・マネジメント学群の理系・文系4学群および大学院を擁し、県内に2キャンパスを展開している。「大学のあるべき姿を常に追求し、世界一流の大学をめざす」という高い志のもと、優秀な学生が目標や希望に応じて自ら主体的に学びの好奇心を広げられるよう支援する「KUTアドバンストプログラム」を実施するなど、先進的な取り組みを進めている。
https://www.kochi-tech.ac.jp/

高知工科大学
情報学群　教授
情報センター長
博士（工学）
福本 昌弘 氏

高知工科大学
情報部
情報システム課　主査
福冨 英次 氏

導入事例

高知県公立大学法人 高知工科大学様



トレンドマイクロ製品との連携により自動防御を実現 二次被害を確実に防止し 端末のトレーサビリティも向上

――新しいネットワークの構成についてお聞かせください。

福冨　コアスイッチとディストリビューション・スイッチの両方で「AX3660S」を採用。それぞれ2台でスタック構成をとっています。その配下のフロアスイッチには「AX2530S」と「AX2130S」を採用しました。

そして「サイバー攻撃自動防御ソリューション」では、ミラーリングによってトラフィックをコアスイッチからトレンドマイクロのセキュリティ製品へと転送します。トラフィックに異常な振る舞いなどが検知されると、「通信の遮断」などのアクション通知がアラクサラの制御ソフト「AX-Security-Controller(以下、AX-SC)」へ送られます。AX-SCは対象の端末の接続場所を特定し、端末とつながっているエッジスイッチが通信を遮断します。これにより、ウイルスの感染拡大や情報の漏洩などの二次被害を確実に防ぐことができるようになりました。

――アラクサラ製品についてはどのような点を評価していますか。

福本　「サイバー攻撃自動防御ソリューション」と、その機能の一つである「端末トレーサビリティ」ですね。ネットワークに接続した端末の情報を自動的に収集してくれるため、インシデントの際に対象の端末と接続場所をリアルタイムに特定できます。

また、アラクサラのスイッチには国産ならではの安心感があります。とにかく壊れない、信頼性が高いというイメージですね。実は前回の更新のときもアラクサラ製品を検討したのですが、当時は本学の環境に合った製品がなかったことから見送ったという経緯がありました。今回は幸いマッチした製品があったため、採用することができました。

――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。

福冨　3週間の試験運用を経て本稼働を開始しましたが、問題なく安定稼働しています。ユーザーはネットワークが一新されたことも気がつかなかったでしょう。セキュリティ面でいうと、9月はまだ学生が少ない時期でもあり、検知は少数でした。ところが10月になると一気に検知が増加、接続を遮断したケースもありました。ただ、実際には重大なインシデントではないものがほとんどでしたが。

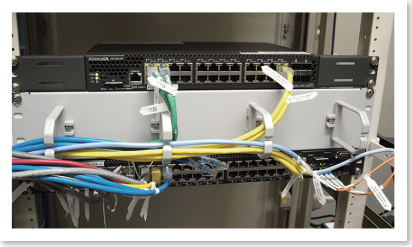
福本　従来と比べて端末のトレーサビリティが格段に向上したのは大きな成果です。おかげで担当者にかかる負荷も減りました。また、過去にさかのぼってログを参照することができるようになったのも嬉しいですね。端末情報はダッシュボード画面で確実に把握でき、わかりやすく可視化されているので、調査が必要なときは、どの端末が、いつ・どこで・何に接続されたか、素早くトレースすることができます。

――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。

福本　無線環境および永国寺キャンパスのネットワークについて整備を進めていく予定です。また、これまでインターネットへのアクセスはデータセンター経由でしたが、今後は外部へ直接アクセスできるような形態も検討したいと考えています。さらに、クラウドサービスの利用を拡大し、各種ITシステムについても、所有から利用へと転換していくことも考えています。ですから、アラクサラにはスイッチの先にあるソリューション、例えば、クラウドサービスを併用したハイブリッド環境などの提案を期待したいですね。

――ありがとうございました。

コアスイッチ・ディストリビューションスイッチ
AX3660S



フロアスイッチ・AX2130S・AX2530S

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