

## AKAMAI お客様事例

# 東海大学（台湾）

東海大学、Akamai Secure Internet Access Enterprise  
の導入により、セキュリティを強化するとともにインシデント管理時間を短縮

## Akamai のサポートにより、セキュリティチームのリソースの解放 と外部からのセキュリティ通知を削減

攻撃者が、巧妙さの増した方法でセキュリティ防御を回避するようになり、現代の組織は複雑なサイバー脅威に直面しています。そうした攻撃に対する事前対応型の保護の必要性和、大規模な国際大学の学生の柔軟性と自由の必要性のバランスを取るにはどうすればよいか。

それが、東海大学のコンピューター・センター・チームが抱えていた課題でした。同校は、デジタル学習に対応しており、学生と職員に無料の高速ワイヤレス・インターネット・アクセスをキャンパス内外で提供する、スマートキャンパスを構築していました。学年の最初に、新入生が入学して各自のノート PC を同校のネットワークに接続します。

ただし、学生のデバイスにウイルス対策ソフトウェアをインストールすることを IT ポリシーで義務付けていなかったため、ノート PC の多くがマルウェアに感染していました。それらの感染したデバイスによって、キャンパス内外のネットワークで、クラッシュや過度の帯域幅使用、悪性のポットネットトラフィックが発生していました。さらに、マルウェアは横方向（ラテラル）に移動して大学の管理するコンピューターに感染し、東海大学のネットワークが攻撃され、ネットワークで異常な接続が行われたという通知を Taichung Network Regional Center から受信する事態に陥りました。

「コンピューターセンターは、情報セキュリティのトレーニングを実施し、学生と職員に対し、電子メールや Web サイトの怪しいリンクをクリックしないよう呼びかけました」と、Network Technology Director の Chien-Hui Ou 氏は述べています。「しかし、攻撃者は、本物かどうかすぐに分かりにくい、より巧妙化された手口を次々と繰り出したため、最終的にはユーザーが攻撃の犠牲になっていました」



東海大学（台湾）  
台中（台湾）  
eng.thu.edu.tw

業種  
公共部門

ソリューション  
Secure Internet Access Enterprise

### 主な効果

- ・セキュリティ体制の強化とセキュリティ管理  
およびインシデント解決時間の短縮
- ・感染したデバイスからのコマンド&コントロールサーバー（C2）のトラフィックの  
事前ブロックとラテラルムーブメント  
（横方向の移動）の削減
- ・外部へのセキュリティ通知量の削減
- ・CapEx から OpEx への投資の移行による  
セキュリティ予算の最適化



「悪性コードを分析し、特定する従来のウイルス対策ソフトウェアと情報セキュリティソリューションでは、対応が間に合いません。新種のマルウェアが出現し、ウイルス対策ベンダーがそのコードや更新されたシグネチャーを見つけ出していないと、マルウェアは検知されません」と、東海大学ネットワークグループの Kuang-Chin Chang 氏は言います。「ウェブトラフィックは暗号化される傾向があるため、攻撃者もそうした暗号化されたチャネルを使用して攻撃を開始しており、ゼロデイ攻撃を阻止するのがますます困難になっています」

## Akamai が疑わしい接続を効果的に阻止

同校のコンピューター・センター・チームは、既存のセキュリティ体制を強化する必要があると考え、セキュリティ制御ポイントとして DNS を活用した製品の検討を開始しました。同チームは、こうしたアプローチによって、学問の自由に影響を与えずに、大学全体のセキュリティを強化できると考えていました。

競合製品の評価プロセスを経て、同校は Akamai Secure Internet Access Enterprise を望ましいソリューションとして選択しました。Secure Internet Access Enterprise は、すべての DNS リクエストを分析することによって、ネットワークとユーザーに事前対応型の保護を提供するクラウドベースのサービスです。各クエリーを、Akamai の他に類を見ないインターネットトラフィックに対する可視性から得られたリアルタイムの脅威インテリジェンスと比較してから、リクエストされた Web コンテンツをブロックまたは配信します。

「Secure Internet Access Enterprise は、ランサムウェアや仮想通貨マイニングマルウェアなどの悪性コンテンツを配信したり、ユーザー情報を盗んだりするドメインに対する DNS リクエストを検知し、ブロックします」と、Kuang-Chin Chang 氏は言います。学生のコンピューターがキャンパス外での使用時にマルウェアに感染した場合でも、そのコンピューターをキャンパスネットワークに再接続した際に、マルウェアは外部の攻撃者のコマンド&コントロールサーバーに接続できません。

Secure Internet Access Enterprise の導入前は、情報セキュリティインシデントを緩和することが困難でした。異常な接続が行われたという報告を受信すると、通常はネットワーク管理スタッフが IP アドレスを使用して感染したコンピューターを特定し、ログファイルから接続記録を見つけ出して、インシデントが発生したことを当事者に説明し、ウイルス駆除手順への協力を依頼していました。

「そのため、インシデントを解決するのに約 1 週間かかっていました。さらに、膨大なセキュリティリソースが必要でした」と、Kuang-Chin Chang 氏は述べています。「しかし、Secure Internet Access Enterprise の導入後、報告されるセキュリティインシデントの件数が激減し、リソースを解放して他のセキュリティプロジェクトに取り組むことができるようになりました」

さらに、同氏は言います。「システムを本稼働させる前にはまずネットワークから切断しテストを実行する必要のある従来のハードウェアとは異なり、Secure Internet Access Enterprise は、非常に簡単かつ迅速な展開と設定が可能です。Secure Internet Access Enterprise では、DNS トラフィックを Akamai プラットフォームに直接ルーティングするだけです。このプロセスは数分で完了します」

Director の Chien-Hui Ou 氏は次のように述べています。「Secure Internet Access Enterprise は詳細なインシデントレポートを自動的に提供するため、クライアントコンピューターがどのようなマルウェアに感染したかや、コンピューターが仮想通貨マイニングマルウェアに感染する前にどの Web リンクをクリックしたかを、セキュリティチームがすばやく把握できます。データは SIEM と統合されるため、レポートを見ればセキュリティチームが最近の異常なネットワークアクティビティを把握でき、事前に対応できます」



Secure Internet Access Enterprise の導入後、報告されるセキュリティインシデントの件数が激減し、リソースを解放して他のセキュリティプロジェクトに取り組むことができるようになりました。

Kuang-Chin Chang 氏  
東海大学ネットワークグループ

## 労力とコストの大幅な削減

東海大学の Electronic Computer Center の Director である Chao-Tung Yang 氏は、戦略的なメリットを強調します。「現在、情報セキュリティは重要であり、デジタルアプリケーションの普及によって、今後ますます重要になるでしょう。当校は常に IT アプリケーションと情報セキュリティの保護を優先しており、学長は情報セキュリティへの投資を支持しています」

Yang 氏は続けます。「一歩下がって、IT が現在どの方向に向かって成長しているのかに目を向ければ、クラウドベースのサービスが今後も定着し続けるのは明らかです。以前の防御システムは、ソフトウェアとハードウェアの組み合わせとして展開されており、それらの維持やパッチの更新などに、労力と時間がかかっていました」

Akamai のクラウドベースのサービスはこうした状況を変え、メンテナンスにかかる労力を削減できます。Yang 氏は、クラウドベースの情報セキュリティサービスの将来について楽観視しており、次のように述べています。「労力を削減するだけでなく、コンピュータールームの物理的なスペースの必要性も減らし、空調費と電力費も節約できます。これは、機器室に使用されるエネルギーコストを削減するという、コンピューターセンターの努力とも一致しています」

「コストの点では、クラウドベースのサービスを使用すれば、物理機器を購入するのとは異なり、多額の一時費用が不要になります」と、Yang 氏は言います。「Secure Internet Access Enterprise は年間リースのため、大学にとっても負担が少ないのです」

「情報セキュリティの作業に終わりはありません。ただし、Secure Internet Access Enterprise を使用すれば、インシデント管理作業の量を大幅に削減でき、ボットネット攻撃への防御の強化や、より包括的なアクティビティ分析に注力できます」と、Yang 氏は述べています。



システムを本稼働させる前にまずはネットワークから切断しテストを実行する必要のある従来のハードウェアとは異なり、Secure Internet Access Enterprise は、非常に簡単かつ迅速な展開と設定が可能です。

Kuang-Chin Chang 氏  
東海大学  
ネットワークグループ



東海大学は、1955年に創立された台湾初の私立大学です。同校は、幼稚園から博士号までの完全な教育プログラムを提供している、最初にして唯一の教育機関です。東海大学には、文学部、理学部、工学部、経営学部、社会科学部、農学部、芸術・クリエイティブデザイン学部、法学部、国際学部の9つの学部があり、約1万7千人の学生と約500人の教師が在籍しています。<http://eng.thu.edu.tw/>。