

## AKAMAI お客様事例

# 東京医科歯科大学

東京医科歯科大学、Secure Internet Access Enterprise を活用してセキュリティ体制を強化

## Akamai の支援により、大学内外からのセキュリティアラートが大幅に減少

組織が大規模なネットワーク変革プロジェクトに着手する際は、新しい環境でインフラのセキュリティを確保し、ユーザーを保護する方法を慎重に考慮する必要があります。2017年にネットワークをアップグレードした後、東京医科歯科大学（TMDU）の情報推進課が直面したのは、まさにそんな状況でした。このチームは、湯島、駿河台、国府台にあるキャンパスをカバーするネットワークの運用と管理を担当しています。また、大学全体の共有スペースのゲスト用 Wi-Fi を管理し、6,000 人を超えるユーザーを監督しています。

当初このチームは、ファイアウォール、URL フィルタリング、電子メールフィルタリングなどの機能を備えた統合脅威管理アプライアンスを導入すれば、新しい環境に必要なレベルの保護を確保できると考えていました。

### ファイアウォールベースの保護の限界

大学のセキュリティアーキテクチャをアップグレードしたにも関わらず、ユーザーの受信ボックスに届く標的型の悪性メールの数は爆発的に増加しました。

「ユーザーに ID やパスワードを変更するように求める通常のフィッシングメールや、宅配便業者になりましたメールの他にも、本学の IT サポートチームになりました標的型のメールもありました」と、統合情報機構事務部長で情報推進課の長である佐藤和也氏は言います。

これらのメールの大部分には、受信者をフィッシングサイトへリダイレクトする URL が含まれていたため、ファイアウォールで複数のアラートが発生していました。さらに、学生やスタッフから、疑わしいメールに関する報告が毎日殺到しました。IT チームは、毎月数百にも及ぶセキュリティアラートに対応しながら調査を行いました。



東京医科歯科大学  
東京（日本）  
www.tmd.ac.jp

業種  
公共部門

ソリューション  
Secure Internet Access Enterprise

### 主な効果

- ・保護レイヤーを追加して既存のセキュリティソリューションを補完し、セキュリティ体制を全体的に強化
- ・大学内外からのセキュリティアラートを削減
- ・標的型のフィッシング攻撃を事前に識別してブロック



「その頃の私たちは、ファイアウォールで悪性の IP アドレスを簡単にブロックできると考えていたのです。しかし、昨今の標的型メールに対処するのは予想外に困難でした。メールに埋め込まれた URL の IP アドレスが動的に変化するからです」と、東京医科歯科大学教授で統合情報機構 IT セキュリティ部門長の高瀬浩造氏は言います。「IP アドレスが変わると、保護が失われる可能性があります。つまり、脅威がファイアウォールを通り抜けるという大きなリスクがあったのです。それに、IP アドレスが変わる頻度も把握できていませんでした」

既存のセキュリティ体制にはギャップがあると考えた情報推進課は、保護レイヤーを追加するプロジェクトに着手しました。導入可能なソリューションを調べていたチームは、DNS をセキュリティ制御ポイントとして使用して、キャッシュ DNS クエリーを調べるというアプローチでセキュリティを確保する方法を知りました。

「ファイアウォールでは、このような悪性のトランザクションを阻止できないため、キルチェーンにおけるもう 1 つ前の段階において、DNS レベルでブロックする方法は合理的だと考えました。この方法が論理的に正しいことは確認できましたが、実際に効果的に機能するだろうかという疑問が残りました。それを確認するためには、実際に試してみるしかありませんでした」と、高瀬氏は言います。

また、DNS を制御ポイントとして使用すれば、大学はファイアウォール内でトラフィックを復号するという複雑なプロセスを経ずに、Web の HTTPS トラフィックを調べて制御できるようになります。

## 概念実証による効果の証明

情報推進課は、Akamai Secure Internet Access Enterprise を含めたいくつかのソリューションを検討することにしました。Akamai は、チームが選択肢を選考していたときに、無料の概念実証（POC）サービスを試してみることを提案しました。

「初めて Secure Internet Access Enterprise について聞いたときは、少しブラックボックスのような状態でした。そこで何が起きるのか、把握できていなかったのです。100 パーセント確信できないものを盲目的に実装したくはなかったので、まずその効果の証明が必要だと考えました」と、佐藤氏は言います。

## POC で数千もの脅威を検出

Secure Internet Access Enterprise を稼働させると、大学のネットワーク内から悪性の DNS リクエストが多数発信されていることがわかりました。

「私たちは毎日数千もの悪性のリクエストを確認しました」と、情報推進課の技術専門職である那須昌啓氏は言います。「正直なところ、驚きました。多くても、せいぜい数十とか数百ぐらいだろうと思っていたのです。」

最初、チームはフラグが付けられた悪性のリクエストの数に懐疑的でしたが、リクエストされたドメインを調べると、それらの大部分がフィッシングサイトやマルウェアのドロップサイトであることが明らかになりました。

情報推進課は Secure Internet Access Enterprise の信頼性を確信し、すぐに広く展開することを決断したのです。「リスクが迫っていることに気付くことができたため、Secure Internet Access Enterprise を導入するかどうかの議論は、もう必要ありませんでした。考えるべきことは、いつ導入するかだけでした」と高瀬氏は言います。



以前は退社した後でも、1 時間に 1 回は外部アラートが届いていないかチェックする必要がありました。今ではまったくそんな必要がなくなりました。

**那須昌啓氏**

技術専門職、東京医科歯科大学

## 結果

Secure Internet Access Enterprise を完全に導入してから、ファイアウォールでは識別できなかった悪性のトラフィックが検出され、安全にブロックされるようになりました。また、DNS レベルで脅威をシャットアウトすることによって、ファイアウォールからの脅威アラートの数も大幅に減少し、月に数回、通知が届くだけになりました。

さらに、Secure Internet Access Enterprise の導入前は、大学ネットワーク内に悪性のトラフィックが存在するという脅威について、外部の組織から何度も警告を受けていましたが、Secure Internet Access Enterprise の導入後は、まったく警告を受けることなく数か月が過ぎていきます。「以前は退社時間の後でも、1 時間に 1 回は外部アラートが届いていないかチェックする必要がありました。今ではまったくそんな必要がなくなりました。私たちの大きな目標は達成されました。この成果に満足しています」と那須氏は述べています。

大学の DNS トラフィックを Secure Internet Access Enterprise に切り替える作業には、若干の懸念もありましたが、Akamai Intelligent Edge Platform の規模、キャパシティ、耐障害性のおかげでシームレスに移行できました。

Akamai には大学向けの特別なライセンスがあるため、TMDU にとって Secure Internet Access Enterprise はコスト効率の良いソリューションでもあります。「また POC のおかげで、Secure Internet Access Enterprise が効果的に脅威をブロックし、セキュリティを強化できることを示せたので、導入に同意してもらうことも容易でした」と、佐藤氏は言います。

「私たちと同じような環境の大学は数多くありますが、どれほどリスクに晒されているか、まだ気付いていないだけなのです。Secure Internet Access Enterprise は迅速かつ簡単に導入できます。キャッシュ DNS を Akamai に変更するだけで完了します。他に何も変更する必要はありません。Secure Internet Access Enterprise には、既存のセキュリティ体制と重複する部分がほとんどないので、他の大学も Secure Internet Access Enterprise を検討すべきだと思います」と高瀬氏は結論づけています。



東京医科歯科大学は、1928 年 10 月に東京高等歯科医学校として設置されました。湯島昌平坂を神聖なる学びの場として医学と歯学の学部を合併した後、日本で唯一、医学と歯学の両方の大学院を備えた大学となりました。最先端の医療を追求し、知識と人間性を備えた専門家を育成しています。また、思いやりがあり、科学性を重んじる医師、歯科医師、看護師、医学者、歯科衛生士、歯科技工士を育成することを目的としています。卓越した医療スタッフと研究者を養成し、医学とライフサイエンスの分野で研究および教育システムを構築しながら、社会と人々に広く貢献するよう努力しています。<http://www.tmd.ac.jp/>