

# 州立大学が 24 のキャンパスで重要な建物運用テクノロジーを保護するために Akamai を採用



包括的ネットワークの可視性



セグメンテーションポリシー



脅威検知と対応力

## お客様

### 大規模な州立大学

24 のキャンパスに 1 万 7,000 名以上の教職員を擁しているこの大規模な州立大学は、10 万名以上の学生の高等教育ニーズに応えています。

## 課題

### 600 以上の建物のネットワークインフラ管理の一元化

この著名な州立大学は、州で展開されているスマート・キャンパス・プログラムの一環として、建物のオートメーションシステムを安全に導入したいと考えていました。大学の設備と OT システムを担当するチームは、デバイスやアプリケーションを保護するセグメンテーションがないことに不安を抱いていました。また、大学の IT ネットワークを今のエアギャップの状態から移行した場合の懸念もありました。そこで、担当チームは建物のオートメーションシステムを一元化し、セキュリティを強化するという意欲的な取り組みに乗り出すことにしました。

同大学のプロジェクトリーダーによると、「約 2 年前まで、個々のキャンパスはほぼ分離していました。メインのアプリケーションサーバーをホストしていましたが、個々のキャンパスのコントローラーは IT ネットワーク上に設置してあり、個々の VLAN とキャンパスのその他のトラフィック間がセグメント化されていないケースもありました」。

つまり、1 つの建物の制御システムへの攻撃が成功すると、キャンパスの IT ネットワーク全体に攻撃が容易に広がり、その逆も懸念される状態だったのです。

プロジェクトを進めた背景には、経済的な理由もありました。「大学はエネルギー管理を行ってコスト削減可能な部分を把握したいと考えていました」とプロジェクトリーダーは説明します。「しかし、すべてがスタンドアロンシステムだったため、キャンパスからデータを取得することはできませんでした」。

「それぞれを接続する必要を感じていましたが、それには安全性が求められました。リモートキャンパスからデータセンターに接続できるようにすると、ネットワークにバックドアが作られ、攻撃される恐れが生じます」。



業種  
教育

### ソリューション

[Akamai Guardicore Segmentation](#)

### 主な効果

- ・ラテラルムーブメント（横方向の移動）の阻止
- ・アプリケーションリングフェンシング



すべてを共有ネットワークインフラに組み込むという意欲的なプロジェクトで対象となっていたのは、24のキャンパスにある600以上の建物です。プロジェクトの実行には、学部の施設オートメーションチームが起用されました。

しかし、大学のオートメーションシステムは非常に複雑で、関与するベンダーの数が多いたことが大きな課題となりました。

「大学ではエレベーターシステム、空調、振動分析、照明、配電、電気メーターを管理しています。さらに、蒸気発生、配電、廃水処理などの主要なユーティリティ類もあります。こうしたシステムはさまざまな企業が管理しており、大学は260社以上もの業務委託先と契約しています」。これらのベンダーはネットワークにアクセスする必要があります。その際、リスクの発生や他の制御システムへの干渉を避けなくてはなりません。

## ソリューションの選択

### 求む:水平方向(East / West)のトラフィックの可視性と一元化ポリシー

遠隔地のキャンパスと大学の主要なデータセンターを結ぶ垂直方向(North / South)の接続に対応するために、スマート制御システムとIoT(モノのインターネット)ネットワークに特化したセキュリティプロバイダーであるTempered Networksが採用されました。その課題には対応することができましたが、データセンター内で稼働する300台以上のサーバーを侵害から保護するという課題は依然として残されていました。

「私たちは水平方向(East/West)のトラフィックを処理すると謳うソリューションを検討していましたが、いずれも私たちが望むほどクリーンでもシンプルでもありませんでした」と、大学のプロジェクトリーダーは振り返ります。

担当チームが初めてAkamaiの存在に気づいたのは、Akamaiの無料の違反・攻撃シミュレーションツールであるInfection Monkeyを知ったときでした。データセンターのオペレーターは、Infection Monkeyを使用して、セキュリティ侵害後に実行される攻撃やラテラルムーブメント(横方向の移動)に対する自社環境の耐障害性を評価することができます。

チームはそのツールをダウンロードして使用を開始した後、Akamai Guardicore SegmentationならInfection Monkeyの発見した問題を解決できることを知りました。

Akamai Guardicore Segmentationは、主にマイクロセグメンテーションに重点を当てた、市場でも数少ないソリューションの1つです。これによってオペレーターは、セキュリティポリシーの定義、作成、展開を行い、個々のアプリケーション間または論理的にグループ化されたアプリケーション間の通信を容易に管理できるようになります。

Akamaiチームは大学に対する初回のプレゼンテーションで、このプラットフォーム独自の視覚化機能を実演して見せました。Akamai Guardicore Segmentationを使用すると、データセンターのオペレーターは、環境内で実行されているすべてのアプリケーションと、それぞれの依存関係を示すグラフィックマップを見ることができます。

「それはすぐに機能しました。まさに私たちが求めているものだ実感しました」。

## Akamai Guardicore Segmentation

### Akamaiと内部ファイアウォールの比較

「一元的なファイアウォール管理では、ファイアウォールごとにルールを個別に設定する必要があります。Akamaiなら、アプリケーショングループを作成して、指定したシステム間で通信するように指示できます」。

ファイアウォールには、コスト、リソース、管理性の問題もあります。「ファイアウォールの管理は悪夢のようでした。システムを導入し、問題がないことを確認するためだけに、6人のスタッフが必要になるでしょう。その後も管理だけに2人以上の専任スタッフが必要になります」。



ファイアウォール管理システムはAkamaiには勝てません。

大学のプロジェクトリーダー

さらに、ファイアウォールは柔軟性がなく、アプリケーションレベルでポリシーの設定も変更もすることができません。「Akamai では、しばらくリッスンして、システム間で何が起きているのか、そのシステム間でなぜ通信する必要があるのかを理解することができます。ファイアウォールを使用する場合は、100% かゼロかの選択になります。ファイアウォールはポート間をブロックするだけです」。

## 一元管理が容易なマイクロセグメンテーション

チームメンバーがルールを作成して展開できるスピードと容易さも、大きなメリットとして挙げられています。

「起動した初日、私たちはいくつかの機器にインストールしてから、1つのベンダーを別のベンダーが表示できないようにするポリシーを作成しようとしていました。あっという間に最初のベンダーで成功しました。その出来事は、私たちの求めていた製品を手に入れたことの証でした」とプロジェクトリーダーは述べています。

Akamai のマイクロセグメンテーションツールと手法は専門家を必要としません。「チームの誰もが使えるほどシンプルであることが大きな魅力でした」。

## マイクロセグメンテーションからさらに踏み込む：検知と応答

Akamai での可視化により、データセンター内で運用上の異常を発見できるメリットも得られました。「私たちのネットワーク以外に接続している印刷スプールサービスが見つかりました」と、プロジェクトリーダーは振り返ります。「最終的に、それは誰かのリモート・デスクトップ・セッションであり、切断されたものの完全には終了しておらず、PC の印刷サーバーに通信を何度も再試行していたことが判明しました。もしその PC が侵害されれば、アプリケーションサーバーにも被害がおよぶ恐れがありました」。

現在、チームは積極的に Akamai を使用しており、大学は早くもそのソリューションを活用した一層のセキュリティ強化と効率化を構想しています。

「将来的には、インシデントが発生した場合に備え、ネットワークの多くの機能を自動化する予定です。たとえば、建物から不正な MAC アドレスやアクセスポイントを検知したら、Akamai Guardicore Segmentation を使用して、その建物をロックダウンするコマンドを Tempered Network のソリューションに送信し、オペレーターにアラートを送信して修正と現状の把握を行うことができます。これまではその検知機能がありませんでした」。

Akamai プラットフォームにより、大学の施設オートメーションチームは、予想以上に迅速かつ容易に目的のセキュリティ状態に到達できました。「すべてを常時監視するこのようなプロアクティブなツールは、今までありませんでした」と、プロジェクトリーダーは説明します。

Akamai が水平方向(East / West)のデータセンタートラフィックを監視しているため、チームはその作業を行う必要がありません。「私はチームメンバーに本来の仕事、つまり大学のエネルギーとコストの節減に専念してもらいたいと思っています。データセンターの状況に気をとられていると、仕事に集中できません」。

大学のチームは、シンプルなマイクロセグメンテーションソリューションを探しました。そして、それ以上の機能を持つ Akamai に出会ったのです。

「説明を受けた通りの働きをしています」。

その他の詳細については、[akamai.com/guardicore](https://akamai.com/guardicore) をご覧ください。



インストールが完了するとすぐに、導入、展開を終え、保護ルールを設定し、販売することができました。

大学のプロジェクトリーダー