AKAMAI お客様事例

金融機関がサイバー犯罪者に対する強固な防御を展開

Daiwa Capital Markets Europe が Akamai Guardicore Segmentation を使用して、重要な取引システムと決済システムを保護

規制コンプライアンスに対応

ランサムウェア攻撃から防御

100%
クラウド移行ロードマップをサポート

サイバー犯罪者からビジネスを保護

大手投資銀行の Daiwa Capital Markets Europe は、取引システムや決済システムなどの重要システムを保護するために、IT インフラ全体に Akamai Guardicore Segmentation を導入しました。これにより、セキュリティ侵害を隔離し、横方向の拡散を抑え、悪性ソフトウェアが組織全体に広がるのを防止できます。また、セキュリティ監査をシンプル化して、最新の金融規制にも準拠できるようになりました。

サイバー犯罪者をブロックし、規制に遵守

Daiwa Capital Markets Europe にとって、セキュリティは最優先事項です。顧客を獲得して維持するためには、主要事業分野である投資銀行業務（株式、債券、グローバル転換社債など）に関連する機微な情報やシステムを保護しなければなりません。さらに、最新の法律に従ってビジネスを適切に保護していることを証明しなければ、英国や欧州の規制当局から多額の罰金が科されるリスクがあります。

システムを保護し、サイバー犯罪者の一歩先を行くために、同社はテクノロジーインフラのセキュリティを定期的に見直しています。Daiwa の Chief Information Security Officer（CISO）の Dave Wigley 氏は次のように述べています。「この見直しでは、あらゆる側面を綿密に調べて、当社のセキュリティ体制が、今日の厳しい規制環境において、当社の目標とレポート要件を満たしていることを確認しています」

同社のセキュリティ戦略は多岐にわたりますが、同氏が特に重視しているのがランサムウェア攻撃です。英国情報機関の GCHQ によると、ランサムウェア攻撃の発生件数は 2021 年に倍増しています。ランサムウェア攻撃とは、犯罪者が悪性ソフトウェアを使用してネットワークにアクセスし、ファイルやデータベースを暗号化して、暗号化を解除する条件として多額の金銭を要求する攻撃です。

Daiwa Capital Markets

Daiwa Capital Markets Europe Limited
英国、ロンドン
www.uk.daiwacm.com

業種
金融サービス

ソリューション
- Akamai Guardicore Segmentation

Akamai

「当社が懸念していたのは、1 台のワークステーションでセキュリティ侵害が発生した場合に、攻撃者がラテラルムーブメント（横方向の移動）を通じて組織内を動き回って権限を昇格させていき、システムを停止または暗号化できるだけのアクセス権を手に入れてしまうことです」と Wigley 氏は述べています。

ランサムウェアから防御

このような脅威に対抗するために、同氏はいくつかのアプローチを検討しました。その 1 つが、データセンター環境全体に安全なゾーンを構築するためのテクノロジーです。各アプリケーションワークロードの間に「リングフェンス（囲い）」を設けることで、1 つのアプリケーションワークロードが攻撃を受けても、それを隔離し、悪性ソフトウェアがネットワーク全体に広がるのを防止できます。

Daiwa のチームは、各種ソリューションを比較検討するにあたって、同社の比較的複雑な IT インフラをサポートするテクノロジーを提供しているプロバイダーを調査しました。同社は、Microsoft Windows、Unix、Solaris など、複数のオペレーティングシステムを実行しているためです。また、導入するソリューションは、同社の長期的な IT ロードマップ（クラウドへの移行など）をサポートするものでなければなりません。

「いくつかの候補がありましたが、スケーラビリティと幅広いオペレーティングシステムへの対応という点において、Akamai Guardicore Segmentation が際立っていました」と Wigley 氏は言います。「Akamai の概念実証には説得力があり、また、他社製品よりもずっと使いやすいことも決め手となりました」

Akamai Guardicore Segmentation は非常にシンプルです。異なるルールを持つ複数のファイアウォールをアプリケーションごとに構築する必要はありません。「Akamai Guardicore Segmentation により、レガシーファイアウォールのアップグレードにコストや時間をかけることなく、アタックサーフェスを大幅に削減できました」と同氏は言います。

疑わしいふるまいを即座に可視化

Akamai Guardicore Segmentation を導入したことで、Daiwa は複数の主要システム（ビジネスクリティカルな取引・決済プラットフォームなど）をリングフェンスで保護できるようになりました。これにより、Wigley 氏のチームはポリシーを設定して、最初のセキュリティ侵害を防止または阻止できます。たとえば、ポリシー違反を検知した際にリアルタイムのアラートを生成し、侵害アセットを起点としてネットワーク内の他の領域を攻撃する試みをブロックできます。

「重要なのは、セキュリティ上の弱点を理解して、それを管理することです」と Wigley 氏は語ります。「環境の可視化は、リスクを特定するうえで非常に役立ちます。レッドチームのアクティビティを監視することで、一般的な攻撃ベクトルをブロックするためのポリシーを速やかに作成できました」

コンプライアンスを徹底

Akamai は、Daiwa のコンプライアンス体制の強化も支援しています。規制対象のデータを含むインフラのセグメントを隔離すれば、規制に沿った使用を徹底させ、監査を大幅に簡素化できます。

Akamai Guardicore Segmentation により、システムに変更が加えられた際にセキュリティが正常に機能していることを証明できるため、セキュリティ制御の保証ポリシーにも対応できます。「当社には、本番環境の全体像を把握するためのデータソースがあるため、セキュリティ制御の場所も確認できます」と Wigley 氏は説明します。たとえば、Akamai Guardicore Segmentation が新しいワークステーションを認識した場合、そのワークステーションに同社のエンドポイント検知応答システムがインストールされていることを確認できます。

> 長年にわたって IT セキュリティに携わってきましたが、Akamai Guardicore Segmentation はこれまで使用した中で最高のシステムの 1 つです。極めて効果的で、迅速に展開でき、非常に直感的です。
>
> **Dave Wigley 氏**
> Chief Information Security Officer、Daiwa Capital Markets Europe

将来への投資

Wigley 氏のチームは、Akamai チームの継続的なサポートに感銘を受けています。ソリューション検討時の包括的な概念実証から、ソフトウェアの展開に至るまで、Akamai チームはすべての段階を通じてサポートしてきました。「Akamai チームは、日々の問い合わせにも非常に迅速に対応してくれました。当社システムのリングフェンスを支援してくれた Akamai チームは、製品に関する知識も豊富に備えており、すぐに稼働できるように支援してくれました」

今後に向けて、Wigley 氏は自社システムの保護に絶対的な自信を持ちながら、クラウド移行などに備えることができます。「長年にわたって IT セキュリティに携わってきましたが、Akamai Guardicore Segmentation はこれまで使用した中で最高のシステムの 1 つです。極めて効果的で、迅速に展開でき、非常に直感的です。最新のサイバー犯罪から新規制まで、Guardicore は当社の防御の要です」

> Akamai Guardicore Segmentation により、レガシーファイアウォールのアップグレードにコストや時間をかけることなく、アタックサーフェスを大幅に削減できました
>
> **Dave Wigley 氏**
> Chief Information Security Officer、Daiwa Capital Markets Europe

Daiwa Capital Markets

Daiwa Capital Markets Europe Limited は、日本最大級の証券・金融サービスグループである株式会社大和証券グループ本社が全額出資する投資銀行子会社です。主な事業分野は投資銀行業務、株式、債券、グローバル転換社債などです。uk.daiwacm.com