Akamai

ホワイトペーパー

ソフトウェアベースのセグメンテーションでサイバーセキュリティの障壁を突破

Akamai Guardicore Segmentation が、ヨーロッパの金融セクターにおけるセキュリティのアクセス改善とサイバーリスクのコスト削減をサポート

概要

金融業界は EU 経済の重要な部分であり、一部の欧州政府や規制当局の間では金融システムは重要なインフラとみなされています。金融サービス組織が提供する製品やサービスは、可用性の高い IT システムと、複数のチャネルや関係者を介して提供される情報へのタイムリーなアクセスに大きく依存します。

しかし、ランサムウェアや暗号通貨マイニングの攻撃は、こうした重要インフラをすぐさま、数日間、時には数週間も無効化することができ、接続されているサードパーティーやピアーに拡散している可能性もあります。

競争力、顧客獲得、維持を追求するためには、ヨーロッパの金融機関は最先端のデジタル機能を積極的に活用していくことが不可欠です。しかし、セキュリティ制御やレポート作成に関する規制要件が増加しているため、クラウド採用率の伸びは著しく低下しています。たとえば、EU 一般データ保護規則（GDPR）により、顧客を保護できない企業に対して、罰金として世界全体の売上高の最大 4% が科せられる場合があります。[1]

さらに、国際銀行間金融通信協会のカスタマーセキュリティプログラム（SWIFT CSP）や欧州中央銀行のサイバーレジリエンス監視の期待（ECB CROE）などの最近の規制では、よりきめ細かなネットワークセグメンテーションが求められています。

従来のセグメンテーションアプローチや関連する手動での手順は、テクノロジーイノベーションのペース、セキュリティリスクの増大、規制の厳重化に対応するためのアプローチとして現実的ではありません。

組織は新しいツールを導入するだけでなく、セキュリティやセグメンテーションプロセスを根本的に変え、シンプル化、透明性、自動化を実現する必要もあります。

本書では、以下の内容を説明してます。

- 欧州の金融業界が現在直面している主なサイバーセキュリティ問題
- 銀行や金融機関が、コスト効率が高く、複雑さのないセグメンテーションアプローチで、こうしたリスクに対処する方法
- Akamai Guardicore Segmentation のアプローチで、企業がセキュリティプロセスをシンプル化し、コストの大幅な削減や、コンプライアンスの促進を実現する方法

今日のサイバーセキュリティは、対処が複雑でコストがかかる

欧州の銀行や金融機関は、組織のセキュリティ確保や顧客のデータ保護に取り組んでいますが、リスク、サードパーティーのアクセスニーズ、コンプライアンス要件が変化する今、セキュリティ体制の強化を図る取り組みは容易なことではありません。

サイバーリスクの増加は、金銭的損失の増加

サイバー犯罪関連のリスクは、金融機関にとって特に深刻です。金融業界はすでに、攻撃の阻止に注力している業界の中で 2 番目に支出が大きい業界となり、データ漏えい 1 件あたりの平均コストは 572 万ドルに上ります。[2]

しかし、強力なセキュリティ体制を確立するためには、コストもかかります。セキュリティ制御による保護には、複数のプラットフォームだけでなく、ビジネスサービスの提供に不可欠なサードパーティーアクセスも含まれ、制御の実行は複雑なタスクと言えます。インフラや人員にかかるコストが大幅に増加することになります。

コンプライアンスによる、さらなるコスト増

欧州の金融サービス組織では、コンプライアンスの準備や検証に必要なコスト、時間、全体的なリソースが著しく増加しています。規制は金融業界の安定性の確保に役立ちますが、新たなサイバーセキュリティ要件が次々と導入されると、デジタルトランスフォーメーションが減速し、多額の投資が必要になり、収益性や成長に支障をきたします。

GDPR から始まり、その後 Network and Information Systems（NIS）のセキュリティに関する指令、ECB CROE ガイダンス、そして最近の EU サイバーセキュリティ法と、ポリシー運用の厳重化への圧力が高まっています。これに SWIFT CSP などのベンダー要件が加わり、今日のコンプライアンスを達成するためには、膨大な数のレポート要件や技術要件への対応が求められることになります。

そのため、テクノロジーのアップグレードに伴い、銀行や金融機関は管理をシンプル化し、サイバーセキュリティやコンプライアンス関連の運用コストを削減する方法も模索しなければなりません。

サードパーティーや金融市場との相互関係におけるセキュリティの脆弱性

ユーザーの利便性と透明性の向上を目的とした、EU の改訂版決済サービス指令（PSD2）により、サードパーティーのアクセスや個人データ侵害のリスクが増大しました。また、金融サービスの同業社や規制当局からも、ビジネスやテクノロジーのプロセスにおける効率性や透明性に対する圧力が高まっています。

セキュリティ、モビリティ、新しいサービスに関する顧客からの要求が増えたことにより、サードパーティーの情報通信テクノロジーのインフラ、アウトソーシングプロバイダー、サプライチェーンへの依存度が高まっています。

環境の接続がこれまで以上に増加したため、銀行間取引や銀行内取引の自動化など、あらゆるタイプの通信を保護するために大量のリソースが使用されます。

今では、1 つのデータセンターで 1 回侵害が起きると、連鎖的に影響が広がる恐れがあります。攻撃者はたった 1 つの資産を悪用すれば、相互に接続された関係者（同業者の金融機関や金融市場など）間を水平移動し、欧州の金融サービスエコシステム全体のセキュリティや事業継続性をリスクに晒すことができるからです。

ハイブリッドクラウドには新しいセキュリティアプローチが必要

コンプライアンス要件と欧州銀行監督機構[3]のガイドラインは、金融業界におけるクラウド導入の傾向を方向付けています。欧州ではクラウドの導入が増加していますが、規制により、オンプレミスシステムのクラウドへの移行が複雑化しています。

そのため、欧州企業では、すべてをクラウド環境にするのではなく、コア機能をオンプレミスで維持してハイブリッドクラウド環境を採用する傾向があります。また、多くの銀行では複数のクラウド・サービス・プロバイダーを使用する方向に進んだため、マルチクラウドインフラが実現しています。

しかし、組織はセキュリティの向上だけではなく、それ以上のものを求めるのが一般的です。また、プロセスを変更することでコストを削減し、運用効率を向上させることも求めています。自動化とプロセスのモダナイズが成功の鍵となります。

ネットワークの可視性とセグメンテーションで、サイバーセキュリティの主な問題に対処

これらの問題に共通しているのは、重要なアプリケーションやワークロードを安全に分離するニーズで、これは一般にセグメンテーションと呼ばれています。これにより、金融機関は、ビジネスニーズに応じて大規模にセキュリティを実現し、リスクベースのアプローチが規制要件に沿っていることを実証できるようになります。

レガシーファイアウォールでは解決できない

欧州の銀行や金融機関では、セグメンテーションがあまり広く受け入れられておらず、導入もされていません。これには、いくつかの理由があります。

保守やリソースの負担：多くのセキュリティおよび IT 専門家は、時間がかかりすぎることや複数のチームやリソースが必要になることを理由に、セグメンテーションイニシアチブを進めることに抵抗を感じています。従来の方法は複雑で時間がかかる傾向があるため、このように抵抗を感じるのは無理もありません。たとえば、複数の場所や環境に VLAN、ACL、ファイアウォールを設定するのは手間や時間がかかりがちで、エラーが発生しやすいプロセスです。また、従来の方法は、IP などの信頼性の低い ID データに大きく依存します。しかし、頻繁に変更される可能性があるものなので、あまり意味がありません。

可視性の欠如：組織は、水平方向（East/West）のトラフィックを把握できないことでさらに行き詰まるため、セグメント間の依存関係を特定したり、セグメンテーションのルールを作成して重要なコンポーネントを破損しないようにしたりすることが困難になります。トラフィックタップや同様のテクノロジーを使用している場合でも、結果のビューで、IP とポート間で必要なコンテキストや高度な変換が欠けることも少なくありません。Platform as a Service（PaaS）などの動的な環境では、それはほぼ不可能です。

インフラの依存関係：ワークロードのクラウドへの拡張はますます進んでいますが、それに伴い、プロセスはさらに複雑になります。ハードウェアファイアウォールを各データのエグレス（出方向の通信）ポイントに配置すると、コストが非常に高くなります。ネットワークの設定も複雑化し、さらなる管理の問題が生じます。これらの設定は、クラウドやコンテナに加えて、仮想資産レガシー資産を有する多様な環境でのニーズに対応するために必要になります。

> **「一部の地域では、規制制度によりテクノロジーイノベーションのペースを維持することはもとより、企業のリスク管理や制御のフレームワークを取得することも困難になります」**
>
> —「Financial Markets Regulatory Outlook 2023（2023 年金融市場規制の見通し）」、Deloitte、EMEA Centre for Regulatory Strategy

基本プロセスの変更を導入

数百台のサーバーを有する中規模の金融サービス組織でも、数千ものセグメンテーションポリシー項目が生成されます。これらを手動で管理することは効果的ではありません。特に、アプリケーション配信が自動化されている環境で、Jenkins や CI/CD サイクルなど、コンテキストが重要となるツールを使用しても役に立ちません。

これが、Akamai Guardicore Segmentation が一歩先を行っている理由です。組織がポリシー作成および更新のサイクルを手動プロセスから自動プロセスへと根本的に変えていけるようにサポートします。

Akamai Guardicore Segmentation では、アプリケーションのプロファイリングが自動化され、すべての依存関係がマッピングされると、ルール作成および更新が反復可能なプロセスに転換されます。このプロセスになると、関係者とアプリケーション所有者は自動生成されたポリシーを承認するだけで済むようになります。これにより、手作業による介入がほとんどなくなり、プロジェクトに大きなゆとりが生まれ、誤設定や人的ミスのリスクが軽減されます。

ルール作成が自動化されると、ルールの構造的な一貫性やポリシー自体の拡張性が保たれるようになり、ファイアウォールがさらに最適化されます。

IT 変革を促進して、真のゼロトラスト環境を構築

金融機関は、プロセスが手動であることやリソースが限られていることにより、大規模なセグメンテーションの実現が制約されることのないようにする必要があります。真のゼロトラストでは、適切なテクノロジーだけでなく、セキュリティポリシーの作成、変更、保守のプロセスを最新化することも必要です。

ホストベースまたはソフトウェアベースのファイアウォールは、アプリケーションレベルのセキュリティに対するシンプルかつコスト効率の高いアプローチとして生まれました。このアプローチにより、実装が大幅に迅速化し、継続的な保守がシンプル化され、最終的に脅威が効果的に緩和されるようになります。Akamai Guardicore Segmentation は基礎から新たに構築されているので、組織の規模を問わず、セグメンテーションのシンプル化、コスト効率化、迅速化が可能です。

さらに、データセンター内のすべてのアプリケーションや依存関係のビジュアルマップも提供します。セキュリティオペレーターは、ネットワークおよび個々のプロセスレベルのセキュリティポリシーを作成、適用し、重要なアプリケーションと資産を分離してセグメント化できます。ソフトウェア定義のオーバーレイアプローチでは、基盤となるインフラから独立して、オンプレミスのレガシーシステム、VM、コンテナ、クラウドなどにまたがるワークロードを保護します。ポリシーは、場所に関係なく、個別のアプリケーションや論理的にグループ化されたアプリケーションに対して作成することができます。これらのポリシーでは、相互に通信できるコンポーネントと通信できないコンポーネントを規定し、セキュリティに対するゼロトラストのアプローチの基盤を構築します。

サイバーリスクとコストを効率的に削減

Akamai Guardicore Segmentation を使用すると、金融機関は、最も差し迫ったセキュリティ問題のいくつかに対処しながら、短期間でコストを削減できます。

サイバーリスクのコストを削減。相互接続された環境がますます複雑化していく中、ネットワークセキュリティのウイルス予防策やベストプラクティスを適用します。

コンプライアンス管理をシンプル化。コンテキストのきめ細かい可視化とセグメンテーションを行います。これにより、コンプライアンス関連の資産やビジネスクリティカルなアプリケーションをすばやくマッピングして分離することができます。一元的な表示のアプローチで、金融機関は、重要資産の保護、不正リスクの緩和、顧客のプライバシー保護のための対策を講じていることを合理的に示すことができるようになります。

サードパーティーアクセスの保護。ID ベースのセグメンテーションでサードパーティーのトラフィック向けのルートを強制し、ネットワーク内を進むユーザーを隔離したり制限したりします。これにより、サードパーティーや金融市場との相互関係におけるセキュリティが強化され、他の感染したシステムを介して攻撃者が「入り込み、拡大する」のを阻止することができます。

一般的な IT 部門から送金システムと決済システムを分離。SWIFT など、電資金移動や決済システムの要件が満たすため、金融機関の一般的な IT 環境から SWIFT サービスを厳密に分離します。きめ細かいセグメンテーションにより、銀行の IT チームは、サービスプロバイダーの「ゾーン」の周囲にコンテキストベース（ユーザー、ドメイン）の境界を設定して、不正アクセスをさらに制限できるようになります。

安全かつ迅速なクラウドへの移行。ワークロードをマッピングし、重要なアプリケーションや依存関係のインベントリをすべて取得してから移行します。リングフェンシングのポリシーでは、移行プロセス全体でワークロードを追跡する一貫したセキュリティの基盤としてこれらのマップを使用できます。このアプローチでは、アプリケーションやインフラの変更に関係なく、同じセキュリティ制御を維持しながら、より迅速で安全なクラウド移行を実現します。

効率的な侵害緩和で事業継続性を確保。攻撃者が金融データや顧客データを盗み出す前に、水平方向（East/West）のトラフィックや侵害の兆候を可視化し、異常な動向に対してアラートを出して攻撃者を阻止しします。

ラテラルムーブメントを制限してリスクを低減。現在、データセンターのトラフィックの大部分は、外部からデータセンターに入る（縦方向）のではなく、アプリケーション間で水平方向（横方向）に流れています。ビジネスクリティカルなアプリケーションやシステムをリングフェンシングして内部の境界を設定することで、アタックサーフェスを効果的に縮小し、攻撃が水平方向に広がるのを防ぎ、侵害が発生したときの損害が限定的で済むようにします。

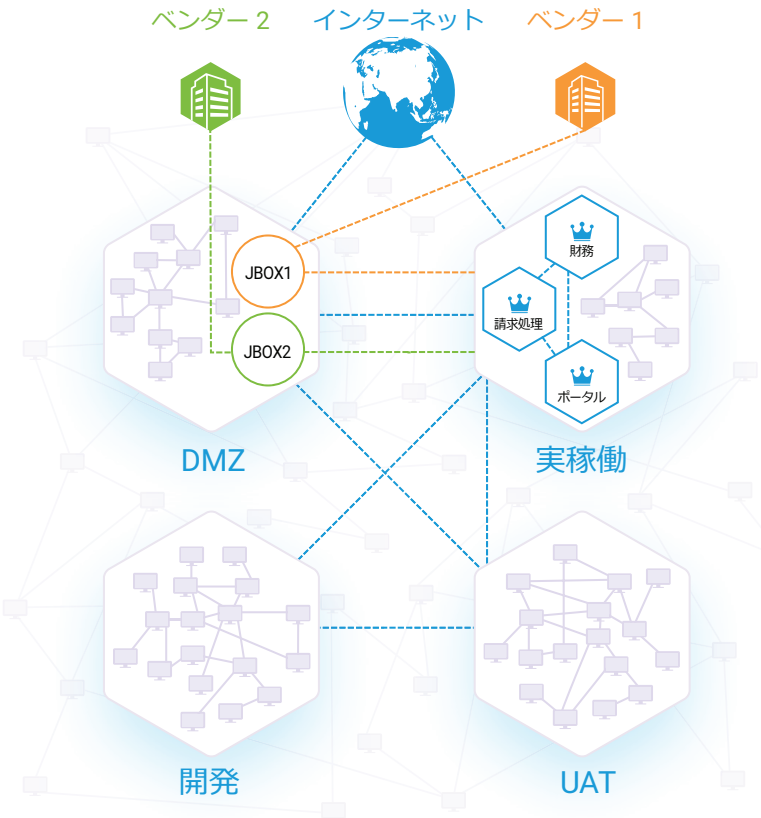
ケーススタディ：欧州の大手多国籍銀行におけるコンプライアンスのコスト削減

欧州のある大手銀行は、ニューヨーク連邦準備銀行（FRBNY）、シンガポール金融管理局（MAS）、ECB などの複数の規制機関からの技術要件を満たすために必要な、効率的な最新のネットワーク・セグメンテーション・アプローチを探していました。

銀行が使用している従来のセグメンテーションアプローチ、ファイアウォールルール、VLAN は効果がなく、毎年のコンプライアンス違反のコストが上昇していました。また、ポリシーの作成や更新に必要な実稼働環境のダウンタイムやリソースが大幅に増加し、IT 運用にも支障をきたしていました。

銀行のセグメンテーション目標を達成するためには、コスト効率が高く、実装が簡単なアプローチが必要でした。新しいソリューションの主な要件は、銀行のインフラやリソースへの影響を最小限に抑えながら、関連の規制に完全準拠することでした。

複数ベンダーとの比較を含む徹底的な評価プロセスを経て、同行のインフラチームと IT セキュリティチームの意思決定者は、最も迅速かつ簡単なマイクロセグメンテーション方法を提供したのは Akamai Guardicore Segmentation だった、とコメントしました。



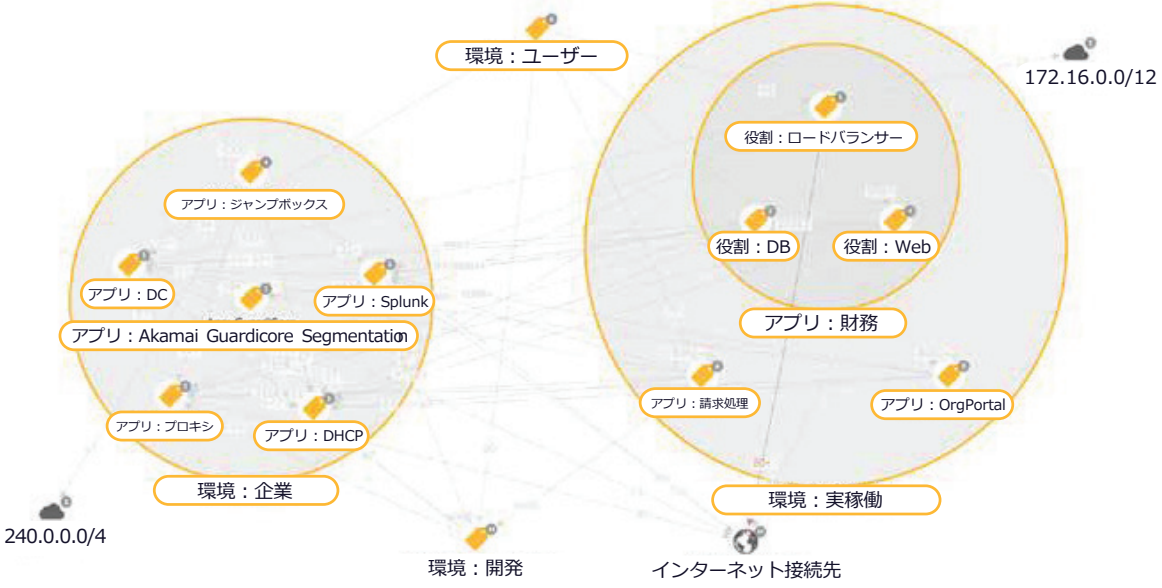
Akamai Guardicore Segmentation による環境セグメンテーションとサードパーティーのアクセス制御

セグメンテーションのシンプル化と加速

同行は、Akamai Guardicore Segmentation を複数の地域と IT インフラタイプ（コンテナを含む）に展開しました。アプリケーションに変更を加える必要がないため、実稼働環境でダウンタイムは不要でした。さらに、データセンターのワークロードを迅速かつ一元的に可視化して、実稼働環境、テスト環境、開発環境を分離できました。Akamai Guardicore Segmentation を使用することで、プリンター、IoT デバイス、不正ユーザーによるサーバーへのアクセスも制限できます。

プロジェクトは 3 か月未満で完了しました。従来型のセグメンテーション手法を用いた当初の予想より、10 倍速く導入できた計算です。環境を速やかにマッピングし、収集した情報に基づいてポリシーを策定することで、同行はセキュリティ対策を改善し、コンプライアンスに違反していた 10,000 を超える資産のコンプライアンス要件を満たすことができました。スピーディな展開により、リスクが軽減され、コストとリソースも大幅に節約できました。

Akamai のプロフェッショナル・サービス・チームのサポートにより、同行はセグメンテーションプロセスを完全に変革することができました。現在、資産のラベリングとセグメンテーションのポリシーは完全に自動化され、アプリケーション開発および展開プロセスに組み込まれています。ラベル作成、変更管理、セキュリティインシデント、サービスリクエストは、ServiceNow ワークフローに完全に統合されています。同行は、Akamai の高いスキルを備えた専任のテクニカル・サービス・チームとともに、プラットフォームの効果やプラットフォームがもたらした価値に心底満足しています。



Akamai Guardicore Segmentation の詳細については、akamai.com/guardicore をご覧ください。

1 「What are the GDPR Fines?（GDPR 罰金とは？）」、GDPR.EU、2019 年 2 月 13 日。

2 「Cost of a data breach 2022（2022 年データ漏えいのコスト）」、IBM

3 「A comprehensive guide to cloud adoption in Europe's banking sector（欧州銀行業界におけるクラウド採用総合ガイド）」、Techerati、2019 年 10 月 31 日。