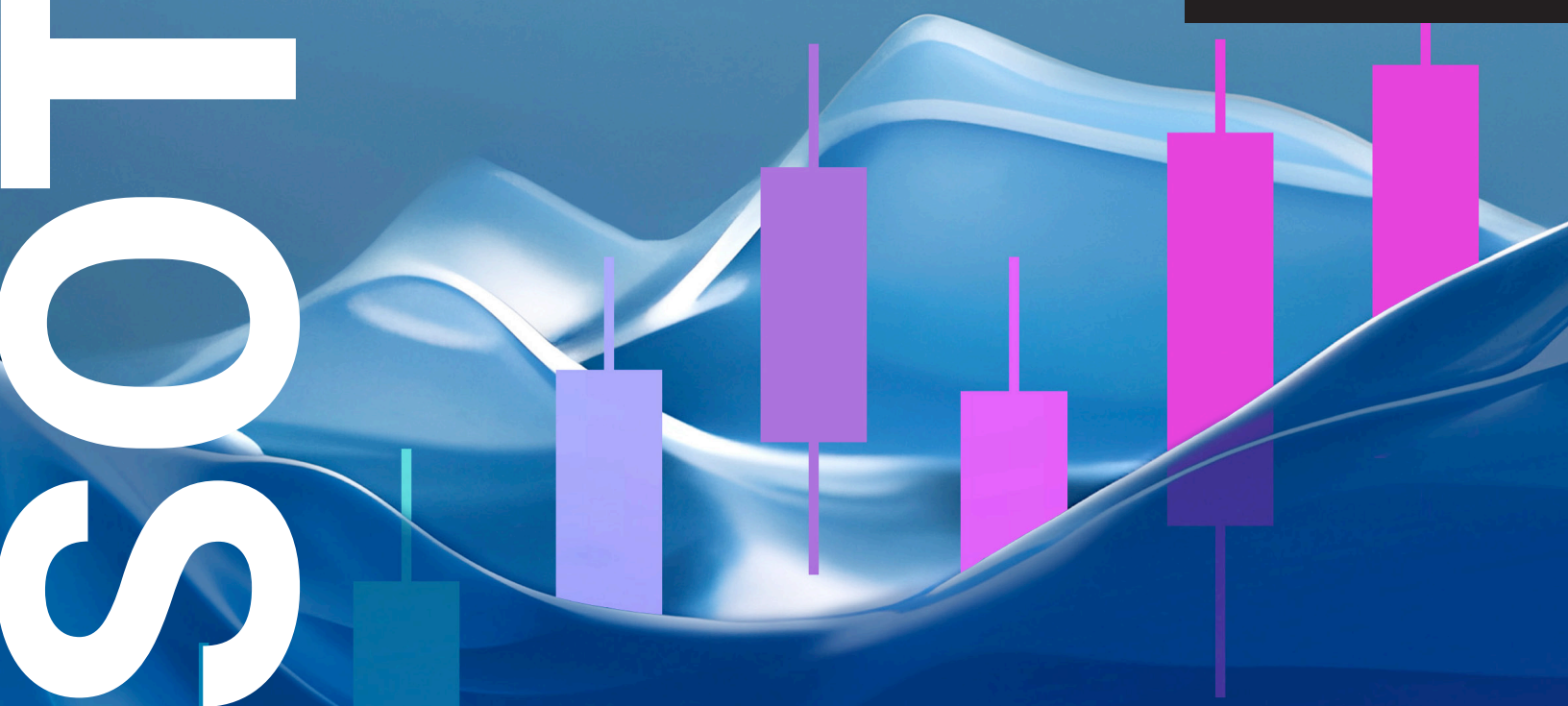
SOTI

第 10 巻、第 5 号

10 YEARS
OF SECURITY INSIGHT



高まる波を乗りこなす

金融サービス業界の攻撃トレンド

Akamai

インターネットの現状／セキュリティ

目次

はじめに

金融サービス業界はグローバル経済の基盤であるだけでなく、経済の成長と発展の生命線でもあります。商業銀行、決済処理業者、資産運用会社、投資銀行、保険会社など、多様な業種を網羅する金融サービス業界は、常に進化しています。

テクノロジーの進歩により、金融サービス業界の状況は変化し続けており、デジタル銀行、ロボアドバイザー、暗号資産など、金融テクノロジー（フィンテック）のイノベーションが生まれています。フィンテック企業の数は世界的に急増しており、米国と中国がそれを牽引しています。2024 年 1 月時点で、大手フィンテック企業 10 社のうち 8 社がこの 2 か国を拠点としています。このテクノロジーの変化は、キャッシュレス取引の拡大にも表れています。キャッシュレス取引は、特に金融サービスへのアクセスが限られている地域で大きく増加すると予想されます。しかし、イノベーションには脆弱性が付き物です。

サイバー犯罪者は絶えず金融機関を標的としており、攻撃の影響は財務的損失に留まりません。事業の中断、評判の失墜、深刻な規制上の罰則により、金融サービス業界を支えている信頼という土台が崩壊する可能性があります。デジタルトランスフォーメーションに匹敵するスピードでサイバー脅威が巧妙化している時代に、金融機関はどうすれば効果的な防御を確立できるでしょうか？

この「インターネットの現状」レポートは、世界中の金融サービスのプロフェッショナル（Akamai のクライアント、サイバーセキュリティ研究者、業界リーダー）が、ますます複雑化する脅威の状況を把握するための支援をすることを目的として作成されています。サイバー犯罪者の主要な標的である金融サービス業界は、重要なインフラの保護、企業と顧客の保護、金融市場の安定性の確保、経済的な混乱の防止のために協力する必要があります。このレポートで紹介されている調査結果は、攻撃者の一歩先を行き、業界の重要な資産を強化し、グローバルな金銭的関係を支える継続的な信頼と信用を確保したいと考えている人にとって必読です。

コンプライアンス、事業の回復力、サイバーセキュリティによって金融サービスを強化

今日のグローバル金融セクターが直面している極めて重要な課題の 1 つは、コンプライアンスと事業の回復力の強化が不可欠となっていることです。規制環境が変化するなか、金融機関はこうした新たな要求にプロアクティブに適応する必要があります。例えば、デジタル・オペレーショナル・レジリエンス法（DORA）の制定は、情報通信テクノロジー（ICT）に関連する混乱に耐えられる堅牢なフレームワークの必要性を明確に示しています。DORA は 2025 年 1 月に発効する予定であり、金融機関とその ICT サードパーティプロバイダーは包括的な回復力強化戦略を義務付けられます。そのため、企業はセキュリティとインシデントへの対応能力の向上を強いられています。

米国証券取引委員会の最新のガイドラインでは、包括的なサイバーセキュリティアプローチの必要性についてさらに詳しく説明されています。金融機関は現在、事業の回復力強化と災害復旧を戦略に組み込むことを求められており、サイバーリスクの重要性が極めて重視されています。これには、重大な脅威やインシデントが財務的安定と事業にどのような影響を及ぼすかを徹底的に把握することが含まれます。重大なサイバーセキュリティインシデントを迅速に開示する義務と、年次レポートにリスク管理戦略について詳細に記述する義務が課されることは、規制の期待事項にパラダイムシフトが起こっていることを表しています。この規制環境に対応するために、金融機関は最先端のセキュリティソリューションと可視性を提供する企業と提携する必要があります。この調査からわかるとおり、Akamai の専門知識は、金融サービス組織がコンプライアンスを達成するだけでなく、厳しい規制要件の中で事業の完全性を維持するためにも役立ちます。

これらの変化を考慮して、金融機関はコンプライアンスと事業の回復力の確保という複雑な課題に対処するための包括的なアプローチを取り入れる必要があります。これには、投資家の意思決定プロセスに大きく影響する可能性のある重大なリスクを特定し、優先順位を付けることが含まれます。金融機関はそのような重大なリスクをリスク管理フレームワークに組み込み、堅固なインシデント対応計画を確実に策定しなければなりません。効果的な事業の回復力を確保するためには、多層防御戦略を導入する必要があります。これには、ネットワークのセグメンテーションとマイクロセグメンテーションによるアタックサーフェスの縮小、保存されているデータの暗号化の実行、サーバーの強化、Web アプリケーションファイアウォールと高度な脅威検知システムの併用などが含まれます。リスクを迅速に特定して緩和するためには、継続的な監視と定期的なセキュリティ評価が極めて重要です。

金融機関は、最新の脅威インテリジェンスや Akamai のインターネットの現状（SOTI）レポートなどの調査に基づくインシデント対応計画を実践することが不可欠です。それを実践することは説得力のあるシナリオの構築に役立ち、金融機関は新しいツール、手法、手順が登場したときにそれらに適応できるようになります。このようなプロアクティブな姿勢は、脅威の状況がますます不安定になる中で事業の回復力を確保し、顧客の信頼を維持するために重要です。金融サービス業界が発展するにつれ、今後もコンプライアンス、事業の回復力強化、サイバーセキュリティが組み合わさり、業界の未来を形成していくこととなります。高度なセキュリティ対策を導入し、可視性を高めることで、金融機関は複雑な規制に対応し、事業を保護して、ビジネスに必要不可欠である信頼を維持することができます。

Teresa Walsh 氏
Global Head of Intelligence、FS-ISAC

重要な知見

34%

金融サービス機関で発生したレイヤー 3 および 4 の DDoS 攻撃イベントの割合

金融サービスは依然として、レイヤー 3 および 4 の分散型サービス妨害（DDoS）攻撃イベントが最も頻繁に発生している業界です。ゲーム業界（18%）とハイテク業界（15%）がそれに続きます。この脅威が蔓延している原因は、継続的な地政学的緊張関係（特にイスラエル・ハマス紛争とロシア・ウクライナ戦争）により、世界各地でハクティビストの活動が急増したことであると考えられます。

API の増加が、レイヤー 7 DDoS 攻撃の増加を招く

Web アプリケーションは従来、サイバー攻撃の主要な標的となってきましたが、この調査期間中に API に対するレイヤー 7 DDoS 攻撃が著しく増加しました。これは主に、変化するコンプライアンス要件と規制要件を満たすために、金融サービスで API の導入が拡大していることに起因します。組織が API への依存を強めているのに合わせて、攻撃者は戦術を適応させているため、API セキュリティは現代の企業にとって極めて重要な優先事項となっています。

トラフィックの急増は、DDoS を頻度と規模で評価する必要があることを示す

金融サービスに対する DDoS 攻撃から、重要な知見が得られます。それは、イベントの頻度と攻撃の強度が必ずしも相関するとは限らないということです。攻撃がほとんど見られなかった期間が数か月ありましたが、その期間の Gbps データはトラフィックの急増を示しています。これは、DDoS 攻撃の影響を評価する際には攻撃の頻度と規模の両方を考慮する必要があることを強調しています。

36%

金融機関を標的とする疑わしいドメインの割合

金融サービスの顧客を標的とするフィッシング攻撃が増加しており、アイデンティティの窃取やアカウントの乗っ取りのリスクが増大しています。この攻撃トレンドにより、金融機関は規制当局からより厳しい目で見られるようになり、侵害が発生すれば顧客は信頼性に懸念を抱くこととなります。

30%

フィッシングサイトやブランドなりすましサイトに誘導されたページ訪問の割合

攻撃者は正規の金融サービス Web サイトやアプリを模倣し、トラフィックを不正なサイトへ誘導します。金融サービス機関が保有する膨大な量の機微な情報を取得するために、攻撃者は金融機関を標的としたフィッシングを行い続けています。

金融サービスは依然としてレイヤー 3 および 4 の DDoS 攻撃の最大の標的

レイヤー 3 およびレイヤー 4 の分散型サービス妨害（DDoS）攻撃は、ネットワークレイヤーとトランスポートレイヤーを標的とし、ネットワークインフラを過負荷状態にして、サーバーリソースと帯域幅を枯渇させます。この攻撃は膨大な量のトラフィックを送信して、ネットワークキャパシティを消費し、正規ユーザーのパフォーマンスを低下させることを目的としています。金融サービス業界は全業界の中で最もレイヤー 3 および 4 の DDoS 攻撃の標的となっています（図 1）。このトレンドは、複数の要因が絡み合い、攻撃者にとって理想的な脆弱性と機会が生まれたことに起因しています。

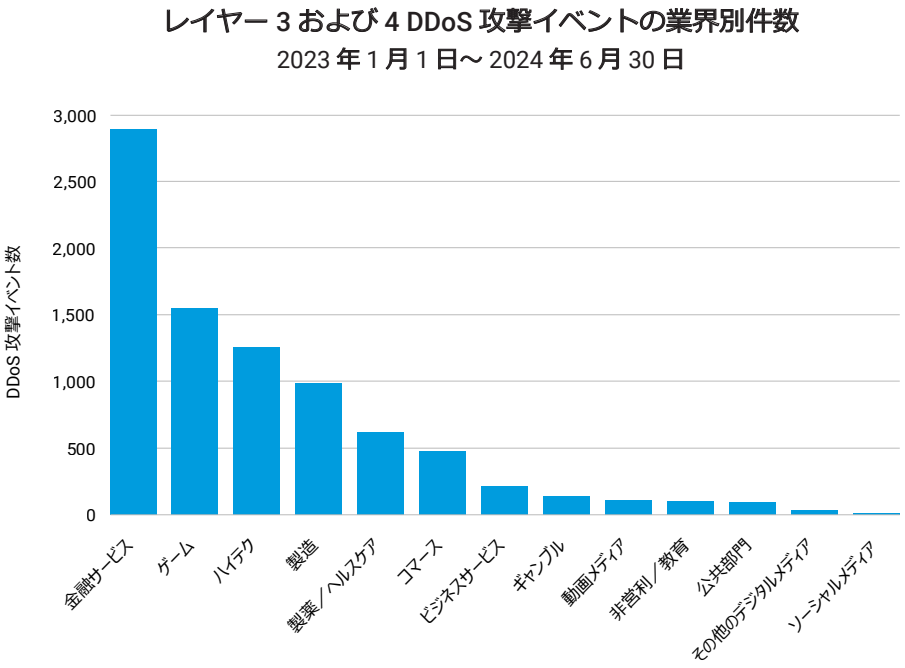


図 *1*：金融サービス業界は、レイヤー *3* および *4* の *DDoS* 攻撃イベントの件数で他の業界を圧倒的に上回っている

金融機関に対する DDoS 攻撃の増加には、地政学的な緊張関係が大きく関わっています。現在進行中のロシア・ウクライナ戦争とイスラエル・ハマス紛争と同時に、ロシア支持派とパレスチナ支持派のハクティビズムが著しく増加しました。これらの紛争により、特にウクライナと関係のある欧州の銀行を標的とする DDoS 攻撃が急増しました。このような攻撃は政治的な動機で行われているため、脅威の状況をさらに複雑化させます。

得られる見返りが大きいため、金融機関は DDoS 攻撃者にとって特に魅力的な標的となっています。事業が中断すると、深刻な財務的影響、評判の失墜、世界の金融システムに対する信頼の喪失につながる可能性があります。広範な影響が生じる可能性があるため、金融サービスは大規模な混乱や政治的声明を目的とした攻撃者の主要な標的となっています。

テクノロジーの進歩により、DDoS 攻撃者の力と能力が劇的に向上しました。攻撃者は今や、仮想マシン（VM）ボットネットを展開して、多数の VM や IoT デバイスでコンピューティングリソースを活用することにより、攻撃をより効率的に実行できるようになりました。このアプローチでは、分散されているというクラウドサービスの性質が悪用されるため、攻撃の緩和と追跡がより困難になります。攻撃者は高い帯域幅の可用性と膨大なコンピューティングリソースを活用できるため、適応性のある強力でコスト効率の高い DDoS 攻撃をさまざまな戦略で実行できます。

金融サービス業界でアタックサーフェスが拡大していることも、DDoS 攻撃の増加に寄与しています。デジタルサービスと API の使用が増加しているため、攻撃者にとってのエントリーポイントが増えています。この変化により、金融システムがさらに複雑化し、攻撃者が悪用する可能性のある多数の脆弱性がもたらされました。ドキュメント化されていないシャドウ API は、情報セキュリティチームが存在を認識していないため、保護されていないことが多く、特に問題となっています。攻撃者はこのような API を悪用して、データを窃取したり、認証制御を回避したり、破壊的な行為を実行したりする可能性があります。

攻撃者は高い帯域幅の可用性と膨大なコンピューティングリソースを活用できるため、適応性のある強力でコスト効率の高い DDoS 攻撃をさまざまな戦略で実行できます。

規制の圧力により、DDoS 攻撃に対する金融機関の脆弱性が意図せず増大しています。欧州連合が導入した Payment Services Directive 2（PSD2）などの要件により、銀行は API を使用し、フィンテック企業などのサードパーティプロバイダーに対してシステムをオープンにすることを義務付けられています。そうすることで、銀行はフィンテック、モバイルアプリ、その他のプラットフォームと統合して、高まる顧客の期待に応えることができますが、同時にセキュリティリスクが増大し、アタックサーフェスも拡大します。これらのさまざまなエンティティ間で API の使用が増えると、攻撃者が標的とする可能性のある障害点がさらに増加します。

これらの要因が総合的に影響し、金融サービス業界はレイヤー 3 および 4 の DDoS 攻撃の最大の標的となり続けています。地政学的な動機、標的としての価値の高さ、テクノロジーの進歩、拡大するデジタルフットプリント、規制の圧力が組み合わさり、金融機関に対する DDoS 攻撃がより頻繁に発生するだけでなく、かつてないほど大きな損害をもたらす可能性のある環境が生み出されています。金融サービス業界は発展し続けているため、ますます高度化する絶え間ない脅威に対する防御も発展させる必要があります。

レイヤー 3 および 4 の DDoS 攻撃イベント件数の急激な変動

金融サービス業界は、レイヤー 3 およびレイヤー 4 の DDoS 攻撃イベントの発生頻度が最も高いですが、この攻撃の発生率は年間を通して変動します（図 2）。

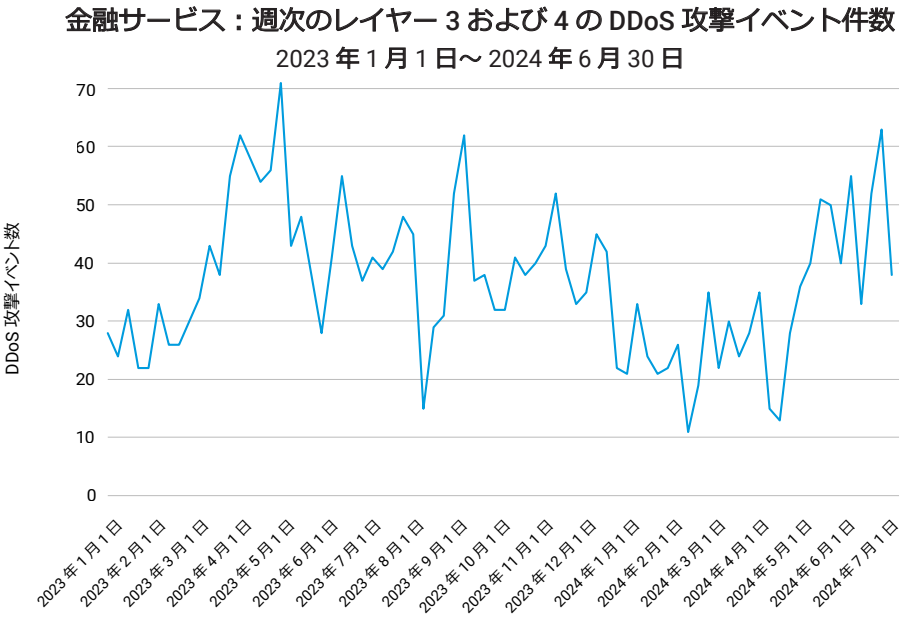


図 *2*：金融サービス業界におけるレイヤー *3* および *4* の *DDoS* 攻撃イベント件数の増減パターン

2023 年 3 ～ 4 月、2023 年 8 ～ 9 月、および 2024 年 4 ～ 5 月に発生した金融サービス業界に対するレイヤー 3 およびレイヤー 4 の DDoS 攻撃は、いくつかの特定の要因に起因します。

春（3 ～ 4 月）は米国で所得税の申告が活発に行われる時期であり、DDoS 攻撃者にとって魅力的な機会です。4 月 16 日から都市銀行や地方銀行でアカウントの悪用が著しく増加しましたが、これは多くの銀行が第 1 四半期決算を発表したタイミングと一致しています。この期間には、Okta や Cisco などのアイデンティティアクセス管理（IAM）プロバイダーやネットワークプロバイダーも、オンラインサービスを標的とした Credential Stuffing 攻撃が増加し、かなりの量の攻撃が発生したことを報告しています。

特に、2023 年 4 月には Service Location Protocol（SLP）に関する重大度の高い脆弱性（CVE-2023-29552）が発見されたことが、攻撃活動の急増に寄与した可能性があります。この脆弱性はネットワーク層とアプリケーション層の両方で DDoS 攻撃を増幅する可能性があり、世界中の 2,000 以上の組織やインターネット上の 54,000 以上の SLP インスタンスに影響を及ぼしたと報告されています。この脆弱性を悪用することにより、攻撃者は侵害されたインスタンスを使用して大規模な DDoS 増幅攻撃を開始することができました。増幅率は最大 2,200 倍で、この脆弱性によってこれまでに記録された中で最大規模の増幅攻撃が可能になりました。

2023 年 8 ～ 9 月の期間について調べたところ、重要なイベントが特定されました。2023 年 9 月 5 日、Akamai は米国の金融機関に対してこれまでに記録された中で最大の DDoS 攻撃が行われたことを観測し、これを阻止しました。この攻撃は ACK、PUSH、RESET、および SYN フラッドの手法を組み合わせたものであり、ピーク強度は 633.7 ギガビット毎秒（Gbps）、5,510 万パケット毎秒（Mpps）に達しました。攻撃の強度は高いものの、持続時間は短く、2 分未満でした。

セキュリティの注目点

レイヤー 3 および 4 の DDoS 攻撃の強度：イベント件数と Gbps の比較

DDoS 攻撃によって金融サービス業界にもたらされる脅威を十分に把握するためには、その真の複雑さと規模を理解することが重要です。これらは単純な個別のインシデントではありません。各攻撃には複数の大規模な試行が含まれ、何 Gbps ものデータや何 Mpps ものパケットによってネットワークが過負荷状態になることがよくあります。攻撃の巧妙さ、強度、長さが増しており、攻撃者はより多様な手法を使用しているため、金融機関にとってのリスクが高まっています（図 3）。

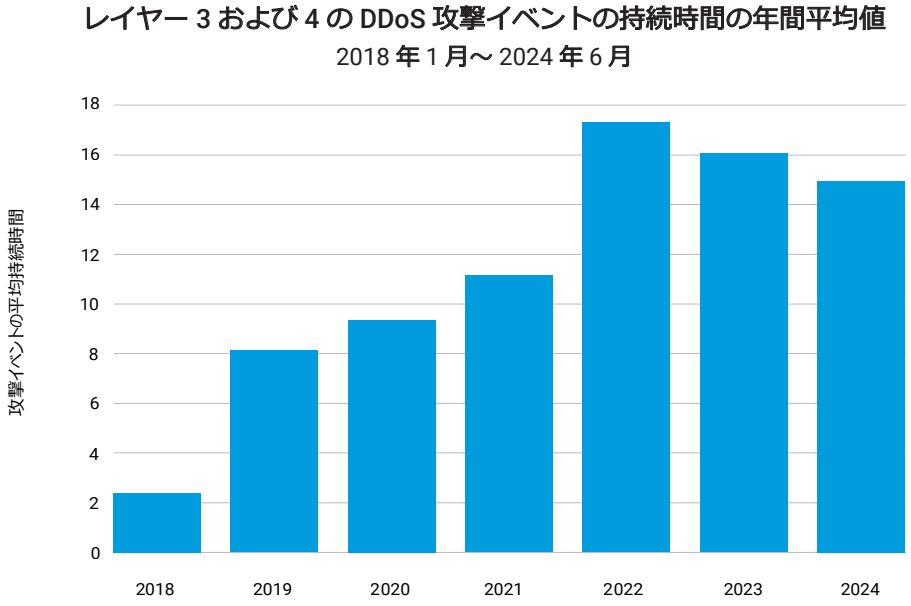


図 *3*：レイヤー *3* および *4* の *DDoS* 攻撃の持続時間は世界的に増加傾向にある

さらに、金融サービス業界におけるレイヤー 3 および 4 の DDoS 攻撃イベント件数のグラフを当該 DDoS の Gbps データと比較すると、大きな違いがあることがわかります（図 4）。Gbps グラフの急激な上昇が、攻撃イベント件数のグラフには表れていません。この不一致は重要なことを示しています。それは、攻撃イベント件数が比較的少ない月でも、Gbps の観点では極めて大量の DDoS トラフィックが発生する可能性があるということです。

セキュリティの注目点

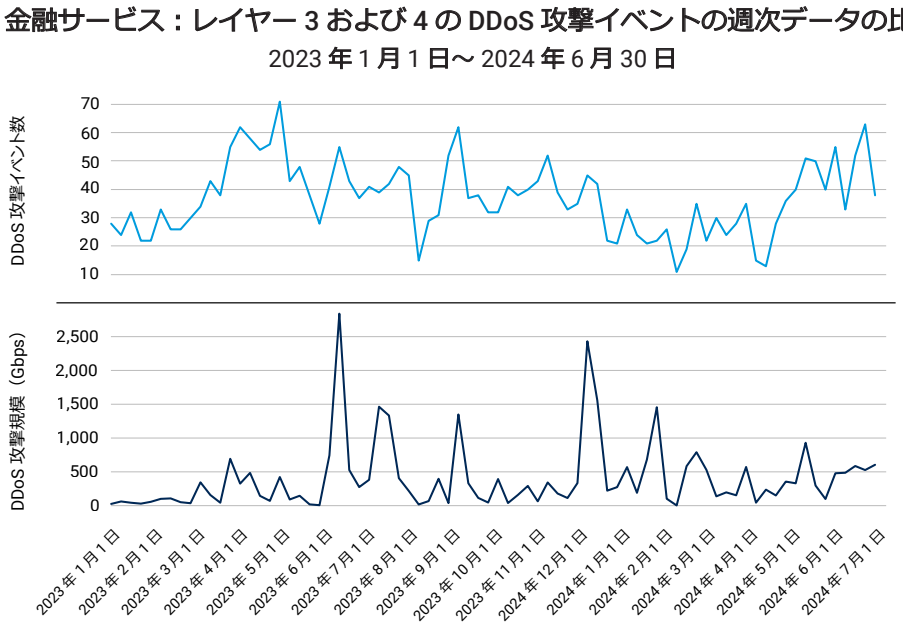


図 *4*：金融サービス業界におけるレイヤー *3* および *4* の *DDoS* 攻撃イベントの件数と測定値（*Gbps* 単位）の比較

この観測結果の重要なポイントは、攻撃イベントの頻度のみを重視すると、真の脅威を著しく過小評価してしまうということです。各攻撃のトラフィックの量と強度の両方を考慮することが不可欠です。強度の高い DDoS 攻撃は件数が少なくても、件数の多い小規模なイベントよりもはるかに大きな損害を与える可能性があるため、各脅威の全容を評価する必要があります。

単一化の傾向：金融サービスにおけるレイヤー 3 および 4 の単一ベクトル DDoS 攻撃

アプリケーションまたはネットワークに対するマルチベクトル攻撃は、システムの破壊や不正アクセスを試みるサイバー犯罪者がよく使用する戦略です。しかし、金融サービス業界にフォーカスしている攻撃者は、レイヤー 3 および 4 の DDoS で単一ベクトル攻撃を試みることが多いようです（図 5）。

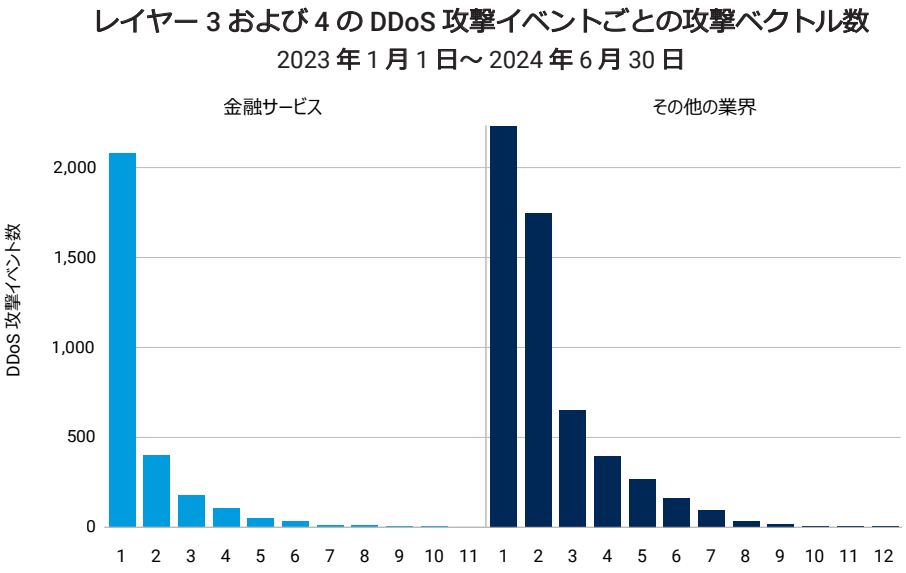


図 *5*：金融サービス業界におけるレイヤー *3* および *4* の *DDoS* 攻撃には、単一ベクトル攻撃がより広く使用されている

レイヤー 3 および 4 を標的とした単一ベクトル DDoS 攻撃は少ないリソースで実行でき、単独でも非常に効果的である可能性があります。特に、より複雑な攻撃に対して強力な防御を備えている可能性のある金融機関に対しては効果的です。一般的にマルチベクトル攻撃よりも実行が容易で、必要な調整が少なくて済みます。また、金融機関はレイヤー 3 および 4 に既知の脆弱性を抱えている場合があり、攻撃者はセキュリティによって検知される可能性のある他の攻撃ベクトルを試みるリスクを負うことなく、単一ベクトル攻撃でその脆弱性を効果的に悪用できる可能性があります。

金融サービス業界で単一ベクトル攻撃が好まれていることは、サイバーセキュリティチームにとって特有の課題となっています。複雑なマルチベクトル攻撃に対する警戒を緩めてはなりませんが、レイヤー 3 および 4 に対する集中的な単一ベクトル攻撃に耐えられる防御を確立することも極めて重要です。

API に対するレイヤー 7 DDoS 攻撃の増加

HTTP または Web トラフィックレイヤー攻撃とも呼ばれるアプリケーション層（レイヤー 7）の DDoS 攻撃がますます広まっており、金融サービス業界を標的とする攻撃者にとって好ましい手法となっています。この攻撃は、特にリソースを大量に消費するアプリケーションコンポーネントに照準を合わせて、正規ユーザーのアクセスを効果的に妨害します。レイヤー 3 および 4 の DDoS 攻撃はファイアウォールやネットワーク保護によって緩和されることが多いのに対し、レイヤー 7 攻撃はアプリケーションサーバーを過負荷状態にすることを目的とし、特定のアプリケーションページや検索機能を標的とする際に正当なリクエストになりすますことで、そのような防御を回避します。

金融サービス業界の Web アプリケーションは一般的に API よりも頻繁に標的にされていますが、Akamai は特に API を標的とするレイヤー 7 DDoS 攻撃の急増を観測しました（図 6）。それらの急激な増加は、他の業界の全体的な API 攻撃のパターンと比較して極めて顕著であり、変化に富んでいます。

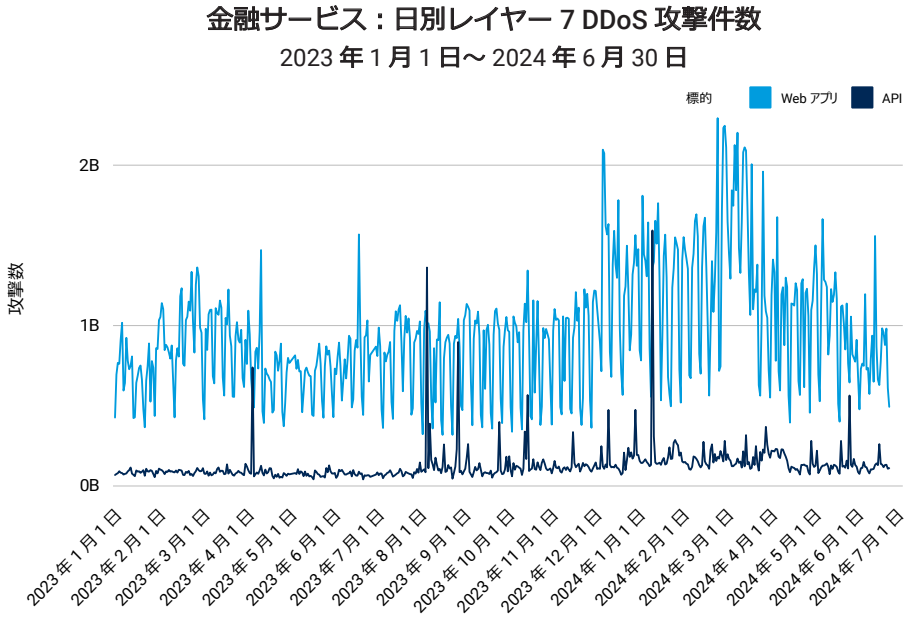


図 *6*：金融サービス業界に対するレイヤー *7 DDoS* 攻撃のパターンは、標的が *Web* アプリケーションであるか *API* であるかによって大きく異なる

これらの急激な増加は、特に 2023 年 4 月、2023 年 8 月、2024 年 1 月に発生しました。その原因は、レイヤー 3 およびレイヤー 4 の攻撃に寄与しているのと同様の要因だけでなく、レイヤー 7 固有の要因もあると Akamai は考えています。

攻撃者は悪用できる新しい脆弱性を常に探しており、そのような弱点が見つかると攻撃頻度が急激に増加する可能性があります。例えば、2023 年 8 月に初めて特定された HTTP/2 Rapid Reset の脆弱性（CVE-2023-44487）により、非常に効果的なレイヤー 7 DDoS 攻撃が可能になりました。この脆弱性により、攻撃者は一見無害に見えるロジックを悪用し、複数のリクエストをバンドルしてストリームを作成し、サーバーやアプリケーションを過負荷状態にできるようになりました。その結果、これまでに記録された中で最大のレイヤー 7 DDoS 攻撃が発生しました。

さらに、季節に応じた DDoS 攻撃は金融機関を標的としたサイバー犯罪者に依然として人気のある戦術であり、確定申告の季節や休暇期間中に著しい急増が見られます。忙しいホリデー・ショッピング・シーズンの後、2024 年 1 月に大幅な増加が発生したことは、オンライン取引活動が活発になっている間に攻撃者が攻撃を準備していたことを示唆しています。

金融サービスにおけるランサムウェアとハクティビズム

金融サービス業界はよく、ランサムウェアグループなどの非常に高度な攻撃者から標的とされます。このようなグループはさまざまな手法を駆使して、金融機関に侵入し、機微な情報を窃取し、多大な身代金を要求します。攻撃の主な目的は金銭ですが、政治的な結びつきがある可能性のある金融機関が標的とされ、地政学的な事情も関与している場合があります。REvil（別名 Sodinokibi）と呼ばれる、ロシアを拠点とするランサムウェアグループのケースが、これに該当します。BlackCat（ALPHV）もそのように利用されており、実際に大手銀行に対する攻撃が行われました。

金融機関を含む大規模な組織に対する攻撃で知られる LockBit は依然として、最もアクティブなランサムウェアグループの 1 つです。最近、同グループに対する法執行活動が行われていますが、状況は変わりません。Operation Cronos では、欧州刑事警察機構（Europol）と欧州司法機構（Eurojust）が協力して初の国際的なタスクフォースを組織しましたが、LockBit が構築した新しいインフラによって打破されました。法執行活動によって 2024 年 2 月にサーバーが押収されてからわずか数日後に、このランサムウェアグループは新しいインフラとダーク Web リークサイトをひっさげて復活しました。また、LockBit は、Operation Cronos への対応として、行政ネットワークへの攻撃を増やして反撃すると声明を出しました。

ランサムウェアグループ CL0P も引き続き活動的であり、金融機関を含む組織で広く使用されているファイル転送ソフトウェアの脆弱性を悪用していることで特に知られています。注目すべき例の 1 つとして、MOVEit Transfer ソフトウェアに影響を及ぼした CVE-2023-34362 が挙げられます。このゼロデイ脆弱性では、初めに SQL インジェクションが行われ、MOVEit Transfer Web アプリケーションへの侵入が試みられました。この MOVEit の脆弱性の結果として、15 以上の銀行と信用組合でのデータ漏えいが確認されました。また、CL0P はフィッシングなどの他の手法によって初期アクセスを確立し、Ransomware-as-a-Service（RaaS）モデルで活動し続けています。最近、同グループは戦術を進化させ、金融機関などの標的に対する四重脅迫を取り入れました。三重脅迫に含まれる手法に加えて、四重脅迫ではビジネスパートナー、従業員、顧客、上級経営幹部、メディアにメッセージが送信され、組織がハッキングされたことが知らされます。この戦術は、身代金の平均支払額の増加につながりました。

ランサムウェアグループには分類されないものの、金融機関を標的としているハクティビスト攻撃者として、Anonymous Sudan、KillNet、NoName057(16) が挙げられます。これらはすべて、ロシア・ウクライナ戦争に関連した活動で知られており、さらに Anonymous Sudan はイスラエル・ハマス紛争に応じたサイバー攻撃に関与したと主張しています。昨年、他の多数の攻撃者グループに加えて、これらのグループもロシア・ウクライナ戦争によってもたらされた混乱に乗じ、重要な銀行インフラに矛先を向けました。

ランサムウェアグループに分類されないものの、金融サービス業界を標的としていることで知られている攻撃者は、たくさん存在します。例えば、Lazarus Group、MoneyTaker、Carbanak ／ FIN7、Cobalt、APT41 などです。

これらの攻撃者によってもたらされている脅威を考慮すると、金融機関は現在の脅威の状況を認識し、より効果的な防御戦略を考案するために攻撃者の動機と手法に対する理解を深めることが極めて重要です。推奨される安全対策については、このレポートの後半にある緩和のセクションをご覧ください。

中東の金融機関における昨今の DDoS ハクティビズムの流行

中東の金融サービス業界では最近、地政学的な緊張関係が原因で、高度で持続的な DDoS 攻撃が急増しています。このトレンドは特にヨーロッパ・中東・アフリカ（EMEA）地域で見られ、金融機関に対する政治的な動機による DDoS 攻撃の脅威が増大していることをよく表しています。

このトレンドの顕著な例は、親パレスチナのハクティビストグループである BlackMeta（別名 DarkMeta）が今年の初めにアラブ首長国連邦（UAE）の金融機関に対して実行した、6 日間にわたるレイヤー 7 DDoS 攻撃です。この攻撃は DDoS 請負サービスである InfraShutdown の手助けを受けて実行されたものであり、この攻撃ツールが利用しやすくなっていることを示しています。2023 年 11 月から活動している BlackMeta には、イスラエル、UAE、米国の組織を標的としてきた歴史があります。

UAE の金融機関に対する攻撃は、持続時間と強度の両方で際立っていました。この攻撃は約 100 時間に及び、Web リクエストが 4 ～ 20 時間にわたって押し寄せ、1 秒あたりの平均リクエスト件数は 450 万件でした。同銀行が攻撃にさらされていた時間はその間の 70% であり、サービスに大きな影響が生じました。同銀行に対する BlackMeta のキャンペーンは、パレスチナ人やイスラム教徒に対する不当と見なされている行為への幅広い抗議活動の一環であり、Anonymous Sudan が取り入れたのと同様の戦術が実行されました。

幸いにも、金融機関の緩和活動により、大きな混乱は回避されました。しかし、このインシデントは、政治的な動機によるサイバー攻撃が増加傾向にあることを明確に示しています。また、DDoS 請負サービスが利用しやすくなり、ハクティビストグループが大規模な攻撃を実行する際の障壁が低くなっていることが浮き彫りになりました。このような状況の変化は、大規模かつ持続的な脅威から保護するための強固なサイバーセキュリティ対策が必要であることを表しています。

最近ではその他にも、2024 年 7 月 15 日に政治的な動機によるものと思われる DDoS 攻撃が発生し、イスラエルの大手金融サービス会社が標的となりました。この大規模な攻撃はグローバルに分散されたボットネットから発生して、24 時間近く続き、ピーク時には 798 Gbps に達しました。レイヤー 3 および 4 に対するこの DDoS 攻撃には、DNS リフレクションや UDP フラッドなどのさまざまなベクトルが含まれていましたが、Akamai はこれをうまく緩和しました。

この攻撃中、3 時間の集中的なフェーズがあり、Akamai はその間に約 389 テラバイトの悪性トラフィックをブロックしました。攻撃の持続時間全体でブロックしたトラフィックの合計は約 419 テラバイトに達しました。イスラエルの金融機関では同日に他にも障害が発生しました。これは、組織的な攻撃であることを示唆しており、高度な DDoS 攻撃による脅威が増大していることがさらに明確になりました。

注目すべきは、このような豊富なリソースを持つ攻撃者が、その前の 90 日間に 27 回、同じ金融サービス会社を標的としていたことです。この企業は、2023 年第 4 四半期以降、イスラエル・ハマス紛争の勃発と時を同じくして、何度も DDoS 攻撃の標的とされていました。Akamai 社内の DDoS 脅威インテリジェンスグループの報告によると、イスラエルの機関や企業は 2024 年にかつてないほどの数の DDoS 攻撃を受けています。この持続的かつ積極的なキャンペーンは、このような脅威の規模と強度が増大していることを示しており、攻撃者がますますしつこく、多様な手段を駆使するようになっていることが明らかになりました。

認知度の高さを利用した攻撃：金融サービスにおけるブランドの悪用

金融サービスが顧客体験、業務効率、イノベーション、全体的な収益、可視性を向上させるためにデジタルファーストのアプローチを取り入れているなか、サイバー攻撃者は、ブランドなりすましスキームによって組織とその顧客の間に内在する信頼関係を悪用しています。図 7 は、既知の金融機関を模倣した不正なサイトの例です。フィッシングやブランドなりすましはよく使用される手口ですが、詐欺的な Web サイトの恐ろしいほどの多さと、元のサイトがオフラインになった後に攻撃者が新しいドメインを作成するスピードが特に懸念されます。この急速な広まりにより、金融サービスセクターにおいて厄介な脅威が増大しています。

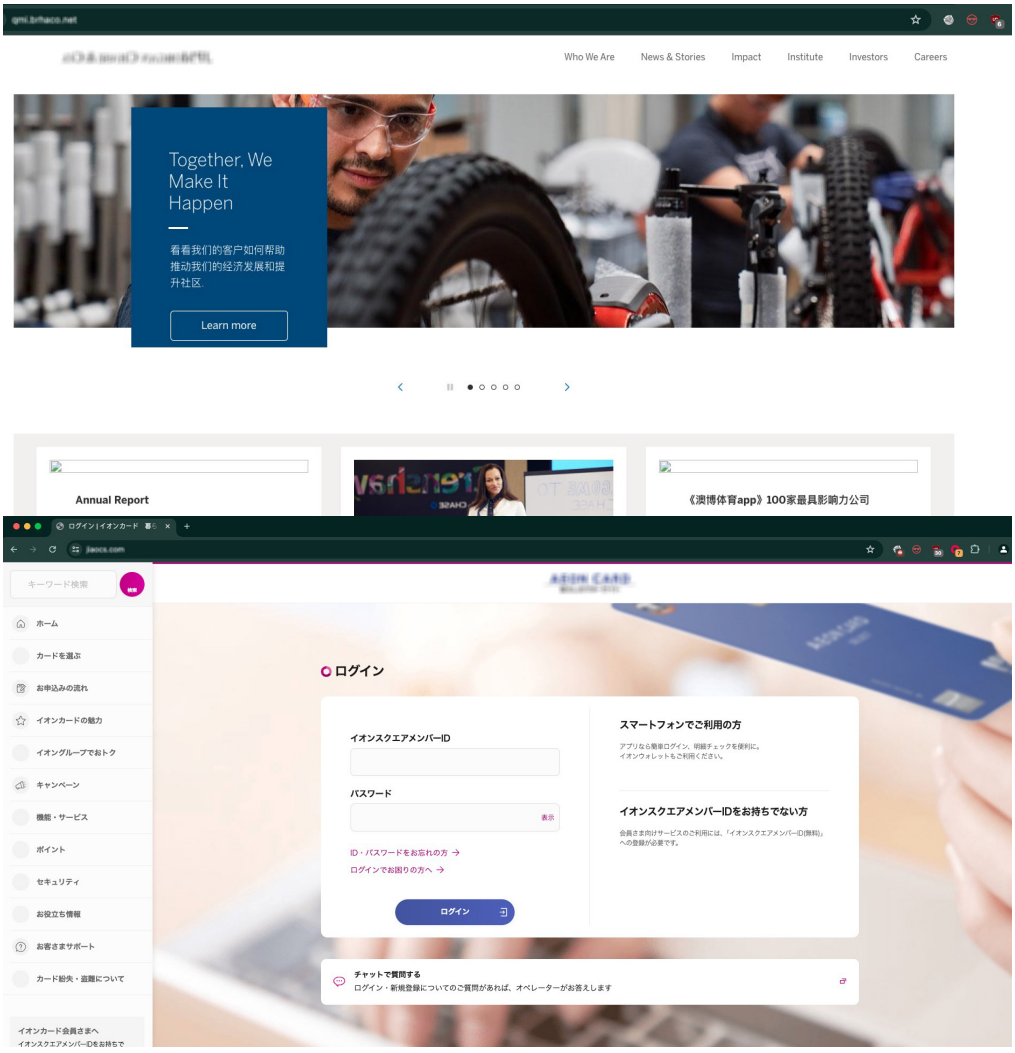


図 7：既知の金融機関を模倣した不正なフィッシングサイトの例

ブランドの悪用の状況は、Phishing-as-a-Service プラットフォームやツールキットの出現によって大きく変化しました。これらのリソースにより、サイバー犯罪者が参入する際の障壁が低くなり、金融サービスやその顧客に対するフィッシング攻撃の規模と深刻さが劇的に変化しました。この点に目を向けてみると、Anti-Phishing Working Group は 2023 年に約 500 万件のフィッシング攻撃を記録し、2023 年を「過去最悪のフィッシングの年」としています。

ブランドの悪用は、アイデンティティ窃取やアカウントの悪用などのリスクが増大するきっかけになり得ます。攻撃者は多くの場合、顧客情報をダーク Web で売ったり、アカウントの乗っ取りに使用したりします。セキュリティの観点からは、ブランド攻撃に早期に介入することが極めて重要です。攻撃ライフサイクルを早期に阻止することで、攻撃者が不正な目的で認証情報を収集するのを防ぐことができます。

ブランドの悪用の悪影響は、目の前のセキュリティ上の課題に留まらず拡大します。企業は、評判の失墜、コンプライアンスや法律上の問題、さらには偽造品への売上の流出などにより、多額の財務的損失を被る可能性があります。今日のデジタル環境では、ブランドなりすまし攻撃を早期に検知することが、顧客の信頼と事業継続性を維持する上で最も重要です。

詐欺が潜んでいるポイント：なりすまし攻撃の詳細

ブランドの悪用はさまざまなオンラインプラットフォームで発生する可能性があり、セキュリティチームはこれを防ぐという困難な課題に直面しています。ブランドの悪用によって正規ユーザーと攻撃者の両方がデジタル資産にアクセスできるようになると、保護が困難になります。攻撃者は多くの場合、オンライン・バンキング・ポータルのような公開されている資産のコンテンツをスクレイプして、独自のスプーフィングサイトを作成したり、スペルの異なるドメインを登録したりすることにより、無防備なユーザーを欺きます。さらに、サイバー攻撃者は、フィッシングメール、ソーシャルメディアへの投稿、その他のデジタルチャネルを使用したキャンペーンを実行し、潜在的な被害者を悪性のサイトや偽のアプリに誘導します。

このレポートを作成するために、Akamai はアクティブなドメインで過去 12 か月間に観測されたブランドなりすまし活動やフィッシング活動を分析し、特に金融サービスにフォーカスしながら、さまざまな業界におけるブランドなりすましの蔓延に関する知見を導き出しました。Akamai の包括的な可視性とプロプライエタリーソリューションを利用することで、次のことを行えるようになります。

- フィッシングサイトやブランドなりすましサイト（マーケットプレイスなど）のトラフィックの追跡
- アクティブな悪性ドメインの数の特定
- 悪性ドメインの重大度スコアの評価

金融サービスは、Akamai が監視しているすべての疑わしいサイトの中で最もなりすましの多い業界（36.25%）でした（図 8）。この調査結果は特に、金融サービス業界がブランドのなりすましや悪用に脆弱であることを示しています。第 2 位と第 3 位は、それぞれコマース業界（26.41%）、ビジネスサービス業界（18.90%）でした。

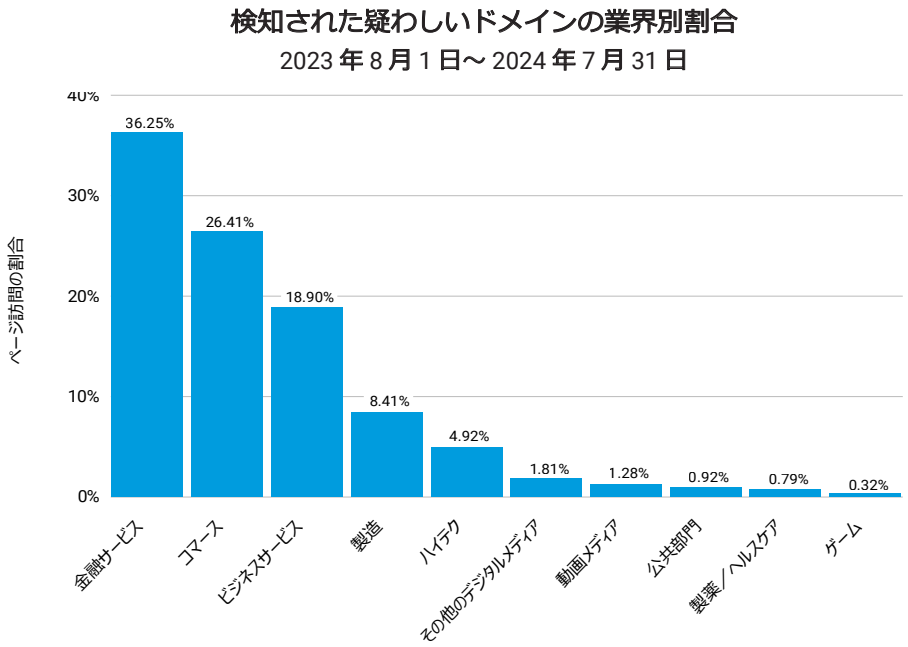


図 *8*：金融サービスはフィッシングドメインやブランドなりすましドメインの *36.3%* を占めている

金融サービス業界は、銀行の認証情報や個人識別用情報（PII）など、高価値の機微な情報を大量に保有しているため、ブランドなりすまし攻撃の主な標的となっています。偽造銀行サイトから入手した情報を利用することで、サイバー犯罪者は簡単に口座にアクセスして、資金を吸い上げることができます。同様に、電子ウォレットや暗号資産（仮想通貨）口座の認証情報など、その他の高価値の財務情報（ダーク Web での価格は 120 ～ 400 米ドル）を取得することで、攻撃者は口座にあるものを転送したり、ダークマーケットプレイスで情報を販売したりできます。このようなスキームは見返りが大きいため、金融サービスはブランドの悪用やフィッシング攻撃の主な標的となっています。

同様に、E コマースやオンラインショッピングが台頭し、認証情報やその他の個人情報を抜き取る機会がもたらされて以降、コマース組織を標的としたブランドの悪用は利益が出やすくなりました。製造企業や、サービスを提供するサードパーティベンダーも同様に、ブランドの悪用に対して脆弱です。デジタル化は全体的なビジネスの成長を促進しますが、多くの組織にとって弱点となっており、ブランドなりすまし攻撃の蔓延やフィッシング攻撃の増加につながっています。

ブランドなりすましスキームは見返りが大きいため、金融サービスはブランドの悪用やフィッシング攻撃の主な標的となっています。

この進化するデジタル環境において、組織はブランドと顧客の両方を保護するためのセキュリティ対策を徹底的に実施し続ける必要があります。これには、ブランドの悪用の継続的な監視、不正サイトの迅速なテイクダウン手続き、なりすましの可能性を認識するための顧客の教育などが含まれます。このような取り組みを重視することにより、組織はますます複雑化する脅威環境において、評判と顧客の信頼をより適切に守ることができます。

ブランドの悪用の標的となっている金融サービス

ブランドなりすましやフィッシングの影響を総合的に把握するために、Akamai は疑わしい Web サイトのページ訪問数も分析しました。調査結果によると、金融機関を装ったサイトが訪問数の 30%、コマース企業を装ったサイトが訪問数の 20% を占めていることが明らかになりました（図 9）。この調査結果では、リクエスト数で測定するかドメイン数で測定するかにかかわらず、金融サービス業界とコマース業界が一貫して上位に位置しています。この一貫した結果は、両業界がブランドの悪用となりすましの主な標的となっていることを明確に表しています。そして、それには相応の理由があります。

金融サービスでは、大手銀行から、セキュリティリソースの少ない小規模な機関まで、幅広い組織が標的とされており、それらすべてが大きなリスクにさらされています。また、コンプライアンス機関と執行サービス（Payment Card Industry Security Standards Council など）によって同様に監視されているコマース業界も、顧客情報を豊富に保有しているため、重大なリスクに直面しています。

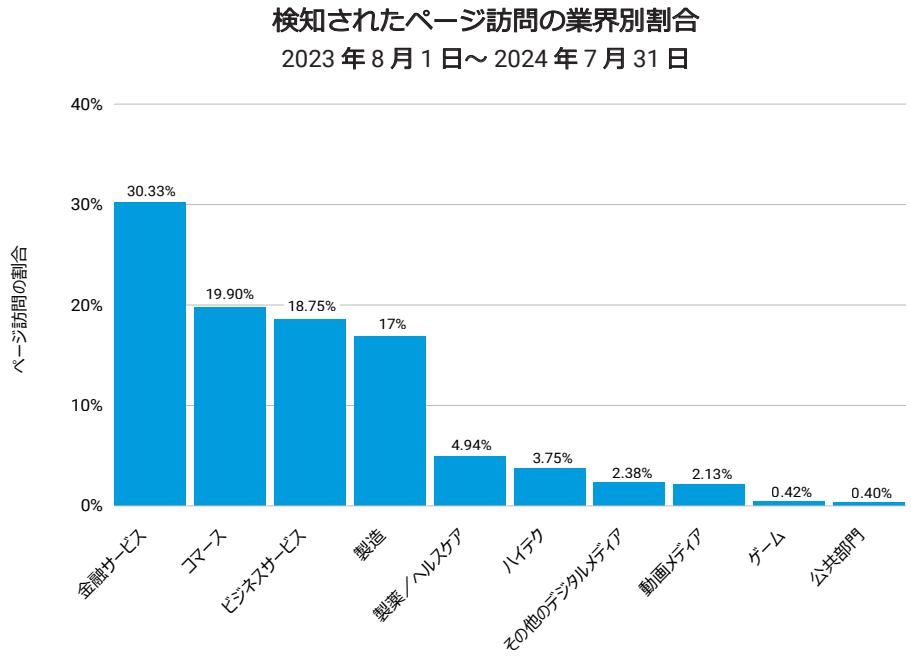


図 *9*：レポートの対象期間中（*2023* 年 *8* 月～ *2024* 年 *7* 月）のページ訪問の *30%* 以上が、正当な金融サービスサイトを装った疑わしいサイトへのアクセスである

興味深いことに、Akamai はさまざまな業界のドメインなりすましランキングと実際の訪問数の間にいくつかの相違点があることを確認しました。例えば、ハイテク業界はなりすましドメイン数では 5 位にランクインしていますが、実際の訪問数では 6 位です。同様に、製薬／ヘルスケア企業を装っているドメイン数は少ないですが、そのようなドメインへの訪問数は多くなっています。

認証情報のフィッシング

ブランドの悪用はさまざまな形で行われます。例えば、企業の正規のロゴとデザインを正確に再現した類似サイト、詐欺アプリ、公式の企業アカウントを装った偽のソーシャル・メディア・プロファイルなどです。この問題の程度を理解するために、Akamai は偽造ページを分析し、ブランドなりすまし、フィッシング、不正アプリ、偽のストア、ペイウォールバイパス、偽のソーシャルプロファイルやストアに分類しました。監視対象のページによっては、1 つの組織のドメインが複数のカテゴリーに分類される場合があることに注意してください。

分析結果によると、金融サービス機関を標的とする偽造ドメインのうち最も多いのはフィッシングであり、記録されたすべてのインスタンスの 68% を占めています（図 10）。第 2 位はブランドなりすましで、記録されたすべてのドメインの 24% を占めています。ユーザーが頻繁にアクセスするサイトでも、フィッシングとブランドなりすましがそれぞれ第 1 位と第 2 位です。金融機関では他の業界よりも、他の形式のブランドの悪用（偽のソーシャル・メディア・プロファイルやストアなど）の重要性が低くなっています。不正なアプリケーションを標的とする攻撃は少ないですが、攻撃者がリーチを広げるためにより創造的な方法を取り入れていることに注意する必要があります。

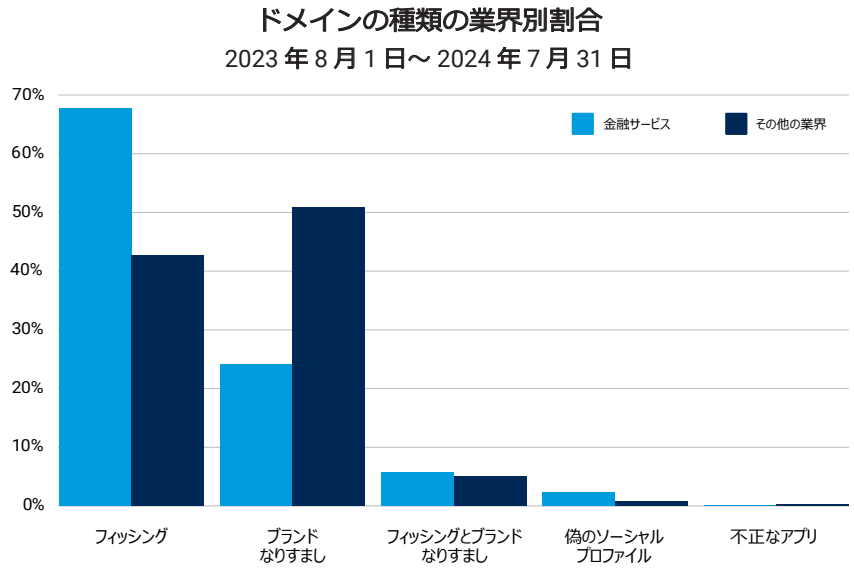


図 *10*：*Akamai* が記録した金融サービスを標的とするドメインの大多数はフィッシングサイトであり、他の全業界の合計を上回っている

金融機関は信頼性の高い組織とみなされているため、そのような信頼を悪用する詐欺師の主要な標的となっています。

フィッシングによってもたらされるリスクに対する意識は高まっていますが、人的要素も依然として重大なセキュリティギャップです。このギャップは、攻撃者が使用する高度な手法により悪化しており（詳しくはブランドの悪用の仕組みのセクションを参照）、訓練を受けていない人が偽のページを見抜くのは困難です。金融機関は信頼性の高い組織とみなされているため、そのような信頼を悪用する詐欺師の主要な標的となっています。攻撃者は金融機関になりすまして、ユーザーを欺き、自ら認証情報を渡すように誘導します。その際、金融機関の評判を利用して、詐欺の信憑性と効果を高めます。

組織とその顧客の両方を保護するためには、ブランドの不正使用（ドメイン名、モバイルアプリ、メール配信など）をプロアクティブに監視できるブランド監視機能を備えたセキュリティテクノロジーを使用することが極めて重要です。そのような不正使用が特定されたら、次のステップはテイクダウンを行い、ブランドの悪用やフィッシングによってもたらされる危険（データ窃取など）に顧客をさらすことになる可能性のあるトラフィックを阻止することです。

ケーススタディ：金融機関に対する Credential Stuffing 攻撃の高度化

ある米国のフィンテック企業は、2023 年から 2024 年にかけて、同社の顧客向けアプリケーションの 1 つを標的とした執拗な Credential Stuffing 攻撃に苦しめられました。この攻撃の規模は驚異的です。Akamai は 24 時間の間に、窃取された認証情報を使用してアカウントへの侵入を試みたさまざまな IP アドレスから 3,000 件以上のアラートを検知しました。また、単一の IP アドレスが少なくとも 115 組以上のユーザー名とパスワードを試行するのを観測しました。2024 年 7 月には、計 100,000 件以上のアラートを記録しました。

重大なリスクのある不正金融サービスサイト

Akamai のグローバルエッジから得られる独自のインテリジェンスと、サードパーティの脅威インテリジェンスからの追加のデータフィードを組み合わせれば、ブランドなりすましを検知する上で明らかな利点が得られます。Akamai はこの包括的なシステムを使用して、各ドメインを綿密に調査し、脅威スコアに基づいて分類します。

脅威スコアは、次の 3 つの重要な要素を使用して算出されます。

1. **信頼度 ― イベントがフィッシング攻撃であることの確実性**
2. **重大度 ― イベントに伴うリスクの程度（重大、高、中、低）**
3. **頻度 ― 特定の期間内における、サイトに関連するイベント／セッションの数**

Akamai のスコアリングシステムは、信頼度、重大度、頻度の 3 つの重要な要素のバランスをとっています。これらのスコアを組み合わせて、それぞれの疑わしいドメインの包括的な脅威スコアを算出し（上限は 99）、潜在的な脅威を総合的に評価します。

最新の分析では、金融サービスセクターの脅威スコアの中央値は 85 で、恐ろしいほど高く、同業界は重大なリスクに直面し続けていることが明らかになりました（図 11）。このようなスコアであるため、金融機関はサイバー犯罪者に真っ向から狙われており、金融機関が保有する膨大な量の機微な情報が絶えず標的とされています。

業界別の脅威スコア

業種	脅威スコアの中央値	業種	脅威スコアの中央値
公共部門	**95**	ゲーム	**65**
金融サービス	**85**	製造業	**64**
ビジネスサービス	**85**	その他のデジタルメディア	**62**
製薬／ヘルスケア	**85**	コマース	**61**
動画メディア	**71**	ハイテク	**60**

図 *11*：脅威スコアの中央値を計算した結果、金融サービスのスコアが極めて高いことがわかる

公共部門は機微な情報が豊富で、セキュリティリソースが限られているため、最も高い脅威スコアを記録しましたが、金融サービスも依然として同じくらい魅力的な標的であり、莫大な金銭的利益を得られる可能性があるため攻撃者が集まっています。ビジネスサービスや製薬／ヘルスケアなどのセクターも同程度のスコアであり、サイバー犯罪者の標的が多様化していることを示しています。しかし、金融機関は極めて重要なデータを保有しているため、依然として主要な標的となっています。

このように脅威レベルが高い場合、財務的損失や評判の失墜につながる前に、防御を強化し、進化する脅威を緩和するための措置を迅速に講じる必要があります。

ブランドの悪用の仕組み

フィッシングやなりすましのキャンペーンの規模は、フィッシングツールキットの存在によって悪化しています。

不正行為やブランドの悪用が成功するかどうかは詐欺やブランド悪用の成功は、ソーシャルエンジニアリングのルアー（釣り＝フィッシングの擬似餌）としてのブランドの力に大きく依存しています。消費者と既知のブランドの間には信頼が内在しています。攻撃者はその認知度と信頼を利用し、正当な Web サイトによく似た偽のサイトを作成します。コードを正確にコピーして、本物のサイトとほぼ同じ見た目の不正サイトを作成することもあります。詐欺師がスペルミスや文法ミスをなくすのに役立つ生成 AI ツールの登場により、消費者が本物のサイトと偽のサイトを区別することがさらに難しくなりました。

フィッシングやなりすましのキャンペーンの規模は、フィッシングツールキットの存在によって悪化しています。攻撃者は信憑性のあるフィッシングサイトを作成できるフィッシングツールキットをわずか 50 米ドルで購入できます。フィッシングツールキットの開発、構築、販売を行うサイバー犯罪エンタープライズは、フィッシングやなりすましのキャンペーンを実行する際の障壁を大幅に下げています。普及しているフィッシングルールキットの例として、Kr3pto と 16Shop が挙げられます。Kr3pto は二要素認証を回避して英国の銀行を標的とし、16Shop は特に PayPal や Amazon などの大手ブランドに照準を合わせました。2023 年 8 月には、国際的な法執行活動により、16Shop の作成者が逮捕されました。これらのケースにより、フィッシング攻撃が巧妙化していることと、サイバー犯罪に対抗するための協調的な取り組みが行われていることが明らかになりました。

過小評価されているが効果的：コンボスクワッティング

ブランドの悪用のもう 1 つの重要な側面として、正当な Web サイトによく似たドメイン名の使用が挙げられます。通常、攻撃者は独自のフィッシングサイトを購入または構築した後にドメインを登録します。その際、サイバースクワッティングやその各種バリアントなどの実績のある手法が重要な役割を果たします。よく使用される戦術の 1 つは、タイポスクワッティングです。攻撃者は、消費者がタイプミスをすることを期待し、会社名のスペルを少しだけ変えたドメインを登録します（例：acamai[.]com）。他にも、ドメイン名に「support」、「login」、「help」などのキーワードを追加するコンボスクワッティングという手法があります。この戦術は、正当な企業 Web サイトでよく見られるマイクロサイトを模倣します。

Akamai の調査結果によると、コンボスクワッティング（キーワードの追加）はあまり取り上げられていない戦術であるにもかかわらず、アクティブドメインの数でタイポスクワッティング（文字の追加、削除、置換）を上回っています。興味深いことに、「com」は詐欺サイトに追加されることの多いキーワードの 1 つでした。

配信メカニズム

偽造 Web サイトやフィッシング Web サイトは、さまざまなメカニズムを利用して配信され、広められます。その中でも主要なメカニズムは E メールです。このような E メールメッセージは、本物のロゴを使用して見た目の信憑性を確保しており、アカウント情報の更新要求などの緊急メッセージが含まれています。しかし、ブランドの悪用は Web サイトや E メールに限りません。攻撃者はソーシャルメディアを通じて脅威を拡散し、その範囲と詐欺戦術をさらに拡大しています。

見えているのに気付きづらいリンク

その他にも、消費者がなりすましサイトを特定するのを難しくし、攻撃の成功率を高めることができるさまざまな戦術が利用されているのが確認されています。例えば、短縮 URL、QR コード、画像ハイパーリンク、テキストリンクを SMS で使用すると、悪性のリンクが難読化されます。このような悪用を防止するスパムフィルター機能を備えた E メールとは異なり、テキスト詐欺はブロックされず、閲覧または開封される可能性が高くなります。

その他にも、 消費者がなりすましサイトを特定するのを難しくし、 攻撃の成功率を高めることができるさまざまな戦術が利用されているのが確認されています。

金融サービスにおける地域ごとのフィッシング攻撃とブランドなりすまし攻撃

ブランドの悪用は世界中の組織や消費者に影響を与えますが、一部の地域ではブランドなりすましサイトやフィッシングサイトへのトラフィックの集中によって不正行為や悪用に対する脆弱性が高まっています。Akamai の分析結果によると、EMEA 地域は過去 12 か月間に検知されたフィッシングサイトやなりすましサイトへのトラフィックが最も多く、北米を上回りました（図 12）。金融サービスとその他の業界の両方とも、この順位になっています。

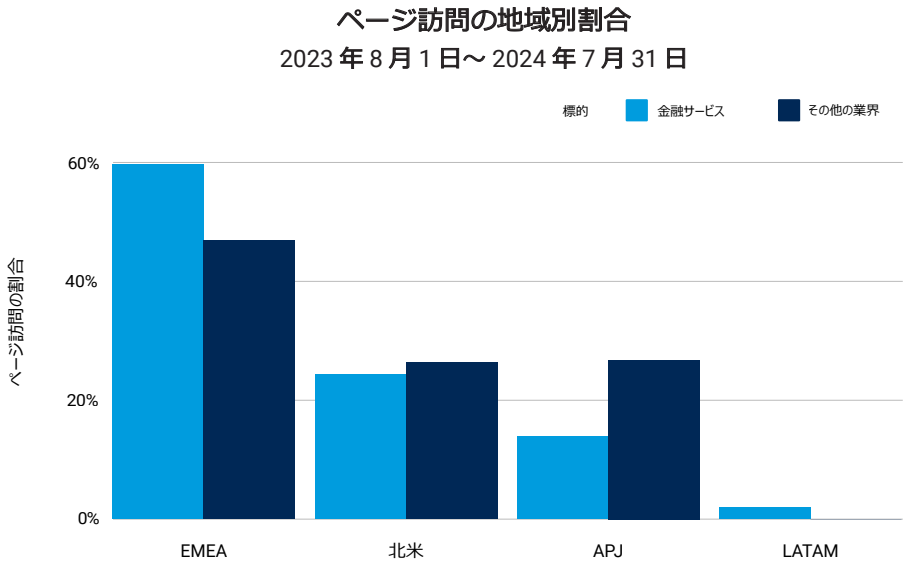


図 *12*：*EMEA* は北米を上回り、金融サービスにおけるフィッシングやブランドの悪用の影響を最も受けている地域となっている

ラテンアメリカとアジア太平洋・日本（APJ）地域はページ訪問数が比較的少ないですが、標的とされる頻度が少ないわけではありません。むしろ、この調査結果は、大規模な顧客基盤を持つグローバルブランドが北米と EMEA に集中していることの表れである可能性があります。つまり、攻撃者の潜在的な標的が大量に存在するということです。また、この調査結果は、2023 年以降に特に EU の銀行を標的とした V3B のようなフィッシングツールキットが登場したことにも起因するかもしれません。

EMEA は疑わしいドメイン数とページ訪問数でほとんどの地域を上回っていますが、脅威スコアの中央値は APJ が最も高く、97 でした。ラテンアメリカは、サイト訪問数が最も少ないにもかかわらず、驚くべきことに脅威スコアの中央値は 94 です。これは、ラテンアメリカと APJ の両地域の消費者が、Web サイトを訪問する際に銀行情報などの機微な情報を盗まれるリスクが高いことを示しています。

APJ で金融サービスに対するブランドの悪用の危険性が高まっている原因はいくつかあります。1 つ目は、APJ のほとんどの金融サービス機関は高度にデジタル化されており、実店舗を訪問せずにオンラインでほぼすべてのサービスを利用できることです。APJ はインターネット普及率とデジタル導入率が世界で最も高く、この地域はサイバー犯罪者にとって利用しやすい魅力的な標的となっています。2 つ目は、この地域には世界で最も活発にソーシャルメディアを利用している国々があることです。金融サービス機関は、そのようなプラットフォームを利用して顧客エンゲージメントを強化し、市場シェアを奪い合い、顧客ロイヤルティを向上させています。APJ 地域ではソーシャルメディアやメッセージングアプリが広く使用されているため、サイバー犯罪者がフィッシングやなりすまし攻撃を仕掛けるためのベクトルが増えており、プラットフォームに対する人々の信頼が悪用されることがよくあります。

コンプライアンスの進化：世界的なサイバーセキュリティ規制が金融機関に及ぼす影響

悪名高い銀行強盗の Willie Sutton が、なぜ銀行強盗をしたのかと聞かれ、「そこに金があるからだ」と答えたことは有名です。当然のことながら、Sutton の言葉は今日の金融機関に対するサイバー攻撃にも容易に当てはめることができます。しかし、金銭的利益という動機は、この話の一端にすぎません。金融機関は、政治的な懸念や地政学的戦略を動機とする攻撃者からますます攻撃を受けるようになっています。このような動機と、「金がある」という事実が相まって、金融機関は最も攻撃を受けている業界となり、最悪の状況に見舞われています。

これは驚くべきことではありません。金融業界は社会において常に重要かつ中心的な役割を果たし、重大な規制の対象となってきました。金融機関に対するこれまでの規制は、金融機関との取引において消費者を保護することに重点を置いていましたが、規制当局は現在、重要インフラと同様のセキュリティと回復力に関する規制を金融機関やサービス企業に適用しようとしています。この新しいトレンドには、金融機関自体だけでなく、情報通信テクノロジー（ICT）サプライヤーに対する要件も含まれています。

サイバーセキュリティと事業の回復力に関する規制の例はたくさんあります。欧州連合では、デジタル・オペレーショナル・レジリエンス法（DORA）により、金融機関とそのサプライヤーは堅牢な ICT リスク管理フレームワークを確立し、定期的なテストとインシデント報告を実施することが義務付けられています。米国では、証券取引委員会（SEC）がサイバーマテリアリティ規制を導入し、事業に重大な影響を及ぼす可能性のあるサイバーインシデントの情報開示を、金融機関を含む上場企業に義務付けました。オーストラリアでは、オーストラリア健全性規制庁（APRA）が、情報資産に対する脅威の規模と程度に応じた情報セキュリティ機能を維持することを組織に求める基準を定めました（規制 CPS 234）。これらの例は、金融セクターのサイバーセキュリティと事業の回復力を強化して、変化するリスクを防止し、金融の安定性を確保することが世界的なトレンドになっていることを示しています。

これらの規制を考慮すると、ICT サービスやセキュリティサービスを購買する際にデューデリジェンスを実施し、サプライヤーがこれらの厳格な基準を満たすようにすることは、金融機関の義務です。金融機関は、回復力に優れたサービスを提供するだけでなく、関連規制を理解し、進化する脅威を特定して緩和するために必要な可視性をもたらし、現行の事業にそのインテリジェンスを適用するための支援をするサプライヤーを選択する必要があります。

可視性は極めて重要です。なぜなら、保護すべきものがある（または保護すべきものに接続している）ことを認識していなければ、それを守ることはできず、脅威が存在していることを認識していなければ、それを防ぐことはできないからです。Akamai Guardicore Platform のようなサービスは、攻撃からの保護を提供するだけでなく、顧客がデータフローを把握し、異常を特定し、ネットワーク資産を適切にセグメント化して脅威を緩和するために役立ちます。同様に、Akamai の API セキュリティサービスは、シャドウ API を支援する API トラフィックを特定したり、API を介した潜在的な攻撃を察知したりするように設計されています。

おそらく、銀行は従来の CIA トライアド（機密性、完全性、可用性）に可視性を追加した、VCIA（可視性、機密性、完全性、可用性）という新たなトレンドを反映する必要があります。

James Casey
Akamai、Vice President、
Chief Privacy Officer

ゼロトラストによる防御の強化

信頼は、金融機関が評判を築くための土台となります。しかし、複雑な環境や機密データの保護という観点では、信頼は容易に大きな負担になり得ます。攻撃者は多くの場合、次のようなありとあらゆる方法で暗黙の信頼を利用します。

- 組織内の個人になりすましたフィッシング攻撃
- サードパーティサプライヤーのセキュリティの脆弱性を悪用して高価値の標的にアクセスする攻撃
- 不正な目的でアクセスを悪用するインサイダーの脅威

従来の境界ベースのセキュリティは、内部からのすべてのトラフィックを信頼できるものと見なします。攻撃の巧妙化により、このようなセキュリティでは不十分になりました。金融サービスが抱えている大きなリスクを考慮すれば回復力に優れたセキュリティ体制を維持することが極めて重要です。その際には、ゼロトラスト・フレームワークが不可欠です。このセキュリティアプローチは、いかなる接続要求、ユーザー、デバイスも有害である可能性があるという原則に基づいて機能します。継続的な検証を行い、暗黙の信頼を排除し、要求者が認証および許可されていない場合はデフォルトでリソースへのアクセスを拒否します。

ゼロトラストは規制対象のデータを処理するシステムのセキュリティを確保することにより、金融機関向けの変化する規制要件の遵守を強化します。これにより、組織は監査で不合格となり罰金を科されるのを回避できます。また、レガシーシステムの制御が強化されるため、きめ細かい可視性を確保し、許可されていないユーザーが重要なアプリケーションにアクセスしようとしているのを検知できます。

ゼロトラスト・モデルは、重要なシステムへのネットワークアクセスを制限し、ランサムウェアなどの脅威のラテラルムーブメント（横方向の移動）を防止することにより、水平方向（East ／ West）のトラフィックを制限します。この封じ込め戦略は、感染したシステムを隔離することで重要なデータと資産を保護します。金融サービスに対するランサムウェア攻撃の件数は大幅に増加しているため、機微な情報を保護する上でゼロトラストは言い表せないほど重要です。ゼロトラストはきめ細かい可視性をもたらすため、複雑な環境内の脅威を検知して無効化するために役立ちます。これは、ランサムウェアの拡散を防止し、重要な資産を保護するために不可欠です。

ゼロトラストのもう 1 つの重大な利点は、アプリケーション間のデータフローのセキュリティを確保できることです。これは、クラウドベースのアプリケーションを安全に展開するために不可欠です。これにより、近代化が促進されるだけでなく、脅威の状況が絶えず変化する中で機密情報が保護され、金融機関はセキュリティを犠牲にすることなくイノベーションを起こすことができます。ゼロトラスト・フレームワークを導入することで、セキュリティ体制が強化され、組織は進化する脅威から将来にわたって保護されます。

セグメンテーションは効果的。マイクロセグメンテーションはさらに効果的。

セグメンテーションとは、パフォーマンスとセキュリティを強化する目的で、ネットワークをより小さなセグメントに分割するアーキテクチャアプローチです。マイクロセグメンテーションとは、個々のワークロードのレベルまで、ネットワークを細かいセキュリティセグメントに論理的に分割するセキュリティ手法です。これにより、分割したセグメントごとにセキュリティ制御やサービスデリバリーを定義できます。

マイクロセグメンテーションは、ゼロトラストの要でもあります。最近の Akamai のレポートによると、金融サービス業界のサイバーセキュリティリーダーは、セグメンテーションプロジェクトを実施する主な理由として「ゼロトラストの推進」を挙げています。実際に、セグメンテーションを実施したほぼすべて（99%）のリーダーが、ゼロトラストのセキュリティフレームワークを導入中または導入済みだと回答しています。ただし、ゼロトラストのフレームワークが完成し定義され、成熟していると回答したリーダーは半数未満（47%）にとどまりました。

マイクロセグメンテーションは既存のシステムで機能し、ファイアウォールなどを用いる従来の方法よりも迅速に展開できます。このアプローチにより、ランサムウェアへの対応が最大 13 時間短縮され、すべての IT 環境で管理がシンプル化されます。また、正確なデータ制御によってコンプライアンスのニーズを満たすこともできます。

現代的なマイクロセグメンテーションの効果を示す実例を紹介します。あるプロジェクトでは実装にかかる時間が 2 年から 6 週間に短縮され、必要だったエンジニアの人数はたった 1 人で、コストが 85% 削減されました。このケースは、マイクロセグメンテーションによってどれほど組織の時間と資金を節約できるかを示しています。IT ディレクターはこの結果を現在のセキュリティコストや実装時間と比較するべきです。

サイバーセキュリティ体制を強化するために、金融機関は高度なセグメンテーション戦略の実装に優先的に取り組む必要があります。CISO は、セキュリティ対策を業界標準の変化に合わせるための取り組みを主導し、強固なゼロトラスト・アーキテクチャの土台としてマイクロセグメンテーションを統合するべきです。IT ディレクターは、高度なサイバー脅威に対する回復力を備えた防御を維持するために、定期的なセキュリティ監査と戦略のアップデートを確立しなければなりません。

このプロアクティブなアプローチは、既存の脆弱性を緩和するだけでなく、組織が新たなサイバーセキュリティの課題に効果的に対処できるようにするために役立ちます。このような対策を取り入れることで、金融機関は喫緊の懸念事項と長期的なリスク管理の両方に対処する包括的なセキュリティフレームワークを構築できます。

マイクロセグメンテーションは、 既存の脆弱性を緩和するだけでなく、 組織が新たなサイバーセキュリティの課題に効果的に対処できるようにするためにも役立ちます。

緩和

金融機関をさまざまなサイバー脅威から保護するためには、多面的なアプローチを取り入れる必要があります。ここでは、フィッシング、ブランドなりすまし、DDoS 攻撃、ランサムウェアに対する主な緩和戦略について説明します。

フィッシングとブランドなりすましからの保護

フィッシングやブランドなりすましから組織を保護するためには、サードパーティのブランド保護サービスを使用して、不正なコンテンツを迅速に検知し、テイクダウンすることを検討します。また、従業員や顧客の教育も重要です。従業員に対しては、フィッシングやなりすましの試みを見極める方法に関するセキュリティ意識向上トレーニングを定期的に実施します。組織からの正当な連絡を識別する方法について、明確なガイダンスを提供します。なりすましの試みに対する迅速な対応計画を策定します。これには、アイデンティティ詐欺についてパートナーや顧客に通知するプロセスが含まれます。

さらに、次の防御手法を導入します。

- 類似するドメイン名を登録してタイポスクワッティングを防止し、ドメイン監視サービスを使用して類似ドメインを検知します。
- 強力な固有のパスワードとパスワードマネージャーを使用して認証プロトコルを強化し、すべてのアカウントとシステムに堅牢な多要素認証（MFA）を導入します。
- Sender Policy Framework（SPF）、DomainKeys Identified Mail（DKIM）、Domain-based Message Authentication, Reporting and Conformance（DMARC）などの E メール認証プロトコルを展開し、E メールのスプーフィングを防止します。フィッシング対策ソリューションと高度な E メールフィルタリング機能を使用して、悪性の E メールを検知し、ブロックします。
- SSL 証明書を取得し、HTTPS を導入し、不正防止ツールを使用して Web サイトやモバイルアプリで疑わしい活動を検知することにより、Web サイトとデジタルチャネルのセキュリティを確保します。
- 安全なポータルを提供し、機密性の高い通信向けに暗号化されたメッセージングを導入することにより、通信チャネルを保護します。

DDoS 防御

金融機関を DDoS 攻撃から保護するためには、多層防御戦略が必要です。専用の DDoS 検知、緩和、保護製品の使用、レート制限の設定、CDN によるコンテンツのキャッシングなど、プロアクティブな戦略を実行します。さらに、パッチ管理、インシデント対応計画、DDoS 攻撃を受ける IP アドレスや重要なサブネットを対象とした緩和制御、アクセス制御ポリシー、ネットワークセグメンテーション、ファイアウォールなどの安全対策について、常に最新の情報を把握します。レート制限の設定、CDN によるコンテンツのキャッシング、専用の DDoS 検知、緩和、保護製品の使用など、プロアクティブな戦略を実行します。

DNS インフラを保護するために、インバウンド DNS トラフィックを継続的に監視および分析し、従来の DNS ファイアウォールではなくハイブリッドプラットフォームを選択します。攻撃者が使用する戦術、手法、手順を理解することで、DDoS 攻撃からの保護を強化できます。

ランサムウェア防御

前述のとおり、ネットワークセグメンテーション（特にマイクロセグメンテーション）によってゼロトラストを実現することは、金融機関全体へのランサムウェアの拡散を制限するために極めて重要です。そのような堅牢なサイバーセキュリティ対策を実行することで、ランサムウェア攻撃者が使用している高度な手法に対抗することができます。また、警戒を緩めず、MITRE ATT&CK フレームワークを使用して、攻撃者が使用する一般的な戦術や手法に関する知見を獲得し、それに応じてランサムウェアのキルチェーンを断ち切るための戦略を強化することが重要です。

防御の継続的なアップデートと従業員の教育を行い、潜在的な脅威を認識して効果的に対応できるようにします。強力な境界防御、エンドポイント保護、E メールフィルタリング、定期的なパッチ管理を取り入れます。ネットワークトラフィック、システムログ、ユーザーのふるまいを継続的に監視し、ランサムウェアの脅威をプロアクティブに特定するための脅威検知方法を実践します。

エアギャップ（物理的に隔離された）されたバックアップなど、定期的かつ安全なデータバックアップを実行して、ランサムウェア攻撃が発生した場合に重要な情報を迅速に復元できるようにします。すべてのユーザーアカウントに MFA を導入して、セキュリティレイヤーを追加します。

これらの包括的な緩和戦略を実行することで、金融機関はさまざまなサイバー脅威を防ぎ、事業継続性を確保し、評判を保護し、顧客の信頼を維持する能力を大幅に向上させることができます。

まとめ

金融機関が顧客体験、事業効率、競争上のポジショニングを強化するためにデジタルトランスフォーメーションを推進しているなか、セキュリティの課題が増大すると同時に、変化する規制環境に対応しなければならないというプレッシャーが高まっています。この SOTI レポートでは、金融サービス業界が直面している持続的な脅威と新たな脅威について考察し、セキュリティソリューションの継続的な評価と強化の必要性を明らかにしました。脅威が高度化しているため、防御を強化し、セキュリティ戦略を改善することにより、常に一歩先を行くことが極めて重要です。

現在では、長らく最大の標的と見なされていたゲーム業界に対する DDoS 攻撃を、金融機関に対する DDoS 攻撃が上回っています。この驚くべきトレンドは、リスクが増大していることを明確に示しています。ハクティビズムや地政学的情勢などの要因によって、金融サービスはかつてないほど脆弱になっています。同時に、金融機関を標的とするブランドなりすましサイトやフィッシングサイトによって生成されるトラフィックの規模と重大度、および最初のサイトがテイクダウンされた後に攻撃者が新しいドメインを生成する速度が際立っています。組織がこれらの活動を追跡するためには、多大なリソースが必要になる可能性があります。セキュリティチームは、テイクダウンサービス、脅威インテリジェンス、複数のデジタルチャネルでのブランドなりすましやフィッシングの検知などのソリューションを必要としています。

消費者や規制当局は、フィッシングやその他の詐欺の被害を受けた後、金融機関に直接的な過失がない場合でも、責任を負わせることがよくあります。さらに重要なのは、フィッシングやブランドなりすましは、より危険な攻撃の前兆であることが多いということです。そのため、攻撃サイクルを早期に断ち切ることが極めて重要です。断固たる行動をとることが、侵害を受けて翌日のトップニュースになるか、組織の評判と顧客の信頼を守るかを左右する可能性があります。

金融機関に対する攻撃が絶え間なく発生していることを考慮すると、機密情報を保護して詐欺や不正行為を防止することは、依然として困難な課題です。従業員を標的としたフィッシング攻撃を効果的に防ぎ、ネットワーク内でランサムウェアが拡散して重要な資産に到達するのを防止しつつ、既存のグローバル規制や新たなグローバル規制を遵守するためには、ゼロトラストなどのセキュリティフレームワークの導入が不可欠です。

このレポートは、金融サービス業界における最新の攻撃トレンドに関する実用的な知見を提供し、防御の強化を支援するものです。常に警戒し、このレポートに記載されている戦略を実行することで、増大する脅威から組織と顧客をより適切に保護することができます。

最新の Akamai リサーチをセキュリティ・リサーチ・ハブでご確認いただけます。

分析手法について

DDoS（レイヤー 7）

このデータは、Akamai の Web アプリケーションファイアウォール（WAF）を通じて観測されたアプリケーションレイヤーのアラートです。レイヤー 7 DDoS のアラートは、保護対象の Web サイト、アプリケーション、または API に対するリクエストの数に異常を検知した際に発せられます。このアラートは、悪性のリクエストと良性のリクエストのいずれによっても発動されます。通常、リクエスト自体は良性ですが、リクエスト数が大量になると、悪質な意図が疑われます。このアラートは、攻撃が成功したことを意味するものではありません。この製品では高度なカスタマイズが可能ですが、このレポートで提示されているデータは、保護対象のプロパティのカスタム設定を考慮せずに収集されています。

データは、Akamai Connected Cloud で検知されたセキュリティイベントを分析するための内部ツールから抽出されました。Akamai Connected Cloud とは、130 か国以上、1,300 近くのネットワーク上の 4,000 か所以上に配置された約 34 万台のサーバーからなるネットワークです。このデータは、ペタバイト／月の単位で測定され、Akamai セキュリティチームによる攻撃のリサーチ、悪性のふるまいの警告、Akamai ソリューションへのインテリジェンスの追加のために使用されます。

2023 年 1 月 1 日～ 2024 年 6 月 30 日までの 18 か月間のデータを使用しています。

DDoS（レイヤー 3 および 4）

Akamai Prolexic Routed は、DDoS 攻撃やその他の望ましくないトラフィック、悪性のトラフィックが、アプリケーション、データセンター、インターネットに面したパブリックまたはプライベートのクラウドインフラやハイブリッドインフラ（すべてのポートやプロトコルなど）に到達する前に、こうした脅威から組織を保護します。Akamai Security Operations Command Center（SOCC）のエキスパートは、事前対応型の緩和制御を調整して攻撃を即座に検知、阻止するとともに、残りのトラフィックのライブ分析を実施し、さらに緩和が必要かどうかを判断します。このように緩和された攻撃は、攻撃イベントに整理、グループ分けされ、それに関連するデータがすべて分析対象として SOCC によって記録されます。

別段の記載がない限り、このレポートでは *2023* 年 *1* 月 *1* 日～ *2024* 年 *6* 月 *30* 日までの *18* か月間のデータを使用しています。

ブランドなりすまし攻撃

Akamai Brand Protector は、フィッシング、偽造 Web サイト、偽のソーシャルアカウント、不正アプリケーションなどのブランドなりすまし攻撃から企業やその顧客を保護するために設計された不正防止ソリューションです。Akamai のグローバル・エッジ・ネットワークを利用して、毎日 900 TB 以上のデータを分析し、顧客に影響が及ぶ前に脅威を検知します。このインテリジェンスをパートナーからのサードパーティフィードによって強化し、さまざまなオンラインプラットフォームで潜在的な脅威を幅広く把握できるようにします。

また、検知された疑わしいドメインのさまざまな特性を分析して、リスクレベルを判定し、ドメインの脅威スコアの算出に寄与します。さらに、そのような疑わしいドメインを監視して、関連データを追跡し、影響を受ける顧客に対してブランドアイデンティティを悪用しようとする悪性のキャンペーンへの注意喚起を行います。

このレポートでは、*2023* 年 *8* 月 *1* 日～ *2024* 年 *7* 月 *31* 日までの *12* か月間に検知された疑わしいドメインのデータを使用しています。

クレジット

Research director

Mitch Mayne

共同執筆者

James Casey
Badette Tribbey
Lance Rhodes

校閲およびテーマ別寄稿者

Cheryl Chiodi
Gal Meiri
Ziv Eli
Richard Meeus
Reuben Koh
Steve Winterfeld

データ分析

Chelsea Tuttle

販促資料

Barney Beal

マーケティング・出版

Georgina Morales
Emily Spinks

その他の「インターネットの現状／セキュリティ」レポート

高い評価を受けている Akamai の「インターネットの現状／セキュリティ」レポートのバックナンバーおよび今後のリリースについては、akamai.com/soti をご覧ください。

その他の Akamai の脅威リサーチ

akamai.com/security-research では、最新の脅威インテリジェンス分析、セキュリティレポート、サイバーセキュリティリサーチを通じ、常に最新情報を把握できます。

このレポートに掲載されているデータ

このレポートに引用されているグラフや図のハイクオリティバージョンを以下のリンクからご覧いただけます。これらの画像は、出典元として Akamai を明記し、Akamai のロゴをそのまま残すことを条件に、利用および引用が可能です：akamai.com/sotidata

Akamai ソリューションの詳細

金融サービス業界を標的とする脅威に対する Akamai のソリューションについて、詳しくは金融サービスのページをご覧ください。