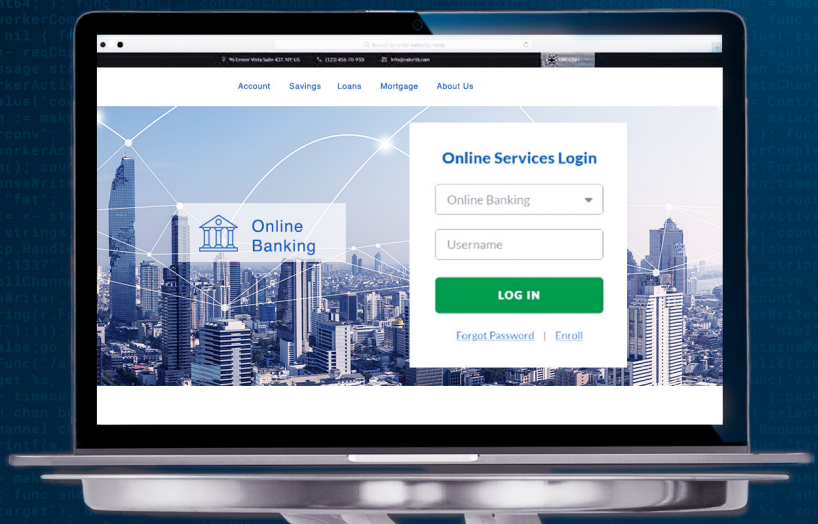
インターネットの現状
第 9 巻 | 第 5 号



イノベーションに潜む高いリスク

金融サービス業界の攻撃トレンド

目次

FS-ISAC ゲストコラム：
金融サービスにおけるサプライチェーンリスク

世界の金融サービス業が直面している主要な脅威ベクトルの 1 つは、サプライチェーンのリスクです。Akamai の調査によると、サードパーティーの API やスクリプトを介した攻撃、脆弱性の悪用が大幅に増加しているため、企業はシステムやサードパーティーのリスク管理をより幅広く強化するというアプローチをより積極的に採用する必要があります。私たちは、予防、検知、保証に関する制御を統合し、さらにシステムが侵害を受けた場合に代替システムにスムーズに移行するための堅牢な耐障害性計画を盛り込んだ多層防御アプローチをお勧めします。

このアプローチに含まれる制御としては、アタックサーフェスの縮小、コーディングのセキュリティ確保、パッチ／隔離／サンドボックスアプリケーション、Web アプリケーションファイアウォールの運用、ネットワークのセグメント化による迅速な封じ込め、保管データへの暗号化の適用、サーバーの強化とともに、許可されたアクティビティの実行時に最小限の権限を適用するアクセス管理などの機能があります。

また、金融企業は、セキュリティ検証とサプライヤーのガバナンスにも引き続き活発に取り組む必要があります。定期的なセキュリティ調査を実施し、リスク管理と規制の両面からサプライヤーのセキュリティ体制を評価するだけでは、もはや不十分です。

Critical Providers Program を通じて 2023 年初頭に実施した Akamai との共同調査によると、分散型サービス妨害（DDoS）攻撃は、以前よりはるかに大きな障害となっており、特に金融業界は、今や全業種の中で最もこの攻撃の標的になっています。DDoS は、社内業務やデータ損失には本質的に影響しませんが、Web サイトが数秒間でも利用不可になると、（この間、攻撃者は停止した Web サイトのスクリーンショットをソーシャルメディアで拡散するため、）企業の評判や顧客の信頼を大いに損ねる可能性があります。また、DDoS を「おとり」としてリソースを拡散させ、その間に攻撃者がマルウェアやランサムウェアなどの別種の攻撃を仕掛ける場合もあります。

また、金融企業は、セキュリティ検証とサプライヤーのガバナンスにも引き続き活発に取り組む必要があります。

多くの金融企業は強力な DDoS 防御を導入してはいますが、攻撃者はツールとテクニックを絶えずアップデートしているため、アップタイムを継続するためにはリソースをさらに増強するしかありません。DDoS がヨーロッパ・中東・アフリカ地域に集中しているという事実から、特にロシア・ウクライナ紛争に関連して、政治活動、ハクティビズム、サイバー戦争で DDoS がツールとして使用されていることがわかります。金融分野は全世界の今後の地政学的な紛争でも引き続き標的になる可能性があるため、脅威インテリジェンスプログラムでは地域的な情勢や分析を考慮する必要があります。

この脅威ベクトルへの耐障害性を常に確保するために、金融企業はこうしたシナリオでのインシデント対応の訓練を実施すべきです。Akamai の綿密な調査を参照することで、訓練計画者は、現在の脅威状況を踏まえたリアルなシナリオを構築し、実際に使用されている新たなツール、テクニック、手法に継続的に対応できます。

Teresa Walsh 氏
Global Head of Intelligence、FS-ISAC

FS-ISAC について

FS-ISAC は、会員主導の非営利組織です。グローバル金融システムにおけるサイバーセキュリティと耐障害性を強化し、金融機関とその顧客を保護しています。1999 年に設立された同組織のリアルタイム情報共有ネットワークは、会員が有するインテリジェンス、知識、実践を広め、金融業界全体のセキュリティと防御に役立っています。加入する金融企業は、75 か国で 100 兆米ドルの資産を保有しています。

イノベーションとリスクの岐路

現代は、前例のないデジタルトランスフォーメーションが進む特徴的な時代です。その中で、金融サービス業界はイノベーションとリスクの岐路に立たされています。テクノロジーは金融取引の環境を刷新すると同時に、経済の安定性を担う中核を狙った、新たなサイバー脅威の時代も招いています。今回の「インターネットの現状（SOTI）」レポートでは、既存のサイバー攻撃（分散型サービス拒否（DDoS）やフィッシングなど）の拡大する脅威とともに、金融サービス業界に対する新たなサイバー攻撃（Web アプリケーションの脆弱性など、拡大する攻撃ベクトルを含む）を考察しています。

特に、アプリケーション・プログラミング・インターフェース（API）に着目しています。API の脆弱性は、Open Web Application Security Project が公開した最新版の OWASP API Security Top 10 リリースで纏められており、これは API セキュリティにおける極めて重大な一歩と言えます。Akamai は、API 特有の複雑な脆弱性を検証し、不適切なセキュリティ対策が予期しない結果をもたらす可能性を指摘し、これらの重要なインターフェースを保護するための予防的なソリューションを提供しています。DDoS 攻撃の復活にも注目しています。金融機関は、他のどの業種よりもこの攻撃の標的になっており、特に世界の特定の地域で顕著です。また、このレポートでは、金融機関に対する Web アプリケーション攻撃数と他の一般的な標的への攻撃数を比較・評価し、攻撃者が好んで使用する攻撃ベクトルを詳しく検証しています。レポートで侵入手法の傾向を明らかにすることで、金融機関が防御を効果的に強化するためのヒントを提供するという狙いもあります。

さらに、金融機関と金融データアグリゲーターの共生関係についても取り上げ、こうした仲介者を通じてサイバー犯罪者が悪用する脆弱性に注目します。悪性ボットへの対応戦略を考察し、デジタルインタラクションのセキュリティを確保するための知見を提供します。このレポートでは、進化する脅威状況を明らかにし、金融機関に実用的な知見を提示することで、情報共有を改善し、世界経済のバックボーンを強化する包括的な取り組みをサポートしたいと考えています。

上位 5 つの知見

1. 金融サービス業界における Web アプリケーションおよび API 攻撃は、2022 年第 2 四半期と 2023 年第 2 四半期を比較すると 65% 増加しており、18 か月で 90 億回の攻撃がありました。その要因の 1 つは、サイバー犯罪者グループがゼロデイおよびワンデイの脆弱性を最初の侵入経路として積極的に追求したことでした。

2. 金融サービス業界ではレイヤー 3 およびレイヤー 4 の DDoS 攻撃が増加し続けており、ゲーム業界を上回って最も攻撃の多い業界となっています。このような増加の原因は、仮想マシンベースのボットネットの力が急激に増大したことや、ロシアとウクライナの戦争によって親ロシアのハクティビズムが活発化したことであると考えられます。

3. レイヤー 3 およびレイヤー 4 の DDoS イベントの 63.52% を欧州・中東・アフリカ（EMEA）地域のアカウントが占めており、昨年の「地域シフト」の傾向が続いています。この地域に対する攻撃の数は、次に多い地域のほぼ 2 倍でした。この原因は攻撃者グループが欧州の銀行に対して金融政策上の動機を持っていることであると、Akamai は推測しています。さらに、攻撃者が攻撃の矛先をすばやく容易に切り替えられるという事実も読み取れます。

4. 金融サービス業界では、他の業界よりもサードパーティースクリプトの利用数が少ない（30%）ものの、そのようなスクリプトは Web スキミングのような攻撃の標的になりやすいと言えます。金融サービス組織は、Payment Card Industry Data Security Standard（PCI DSS）v4.0 の新しい要件に準拠するためのソリューションの採用に積極的に取り組んでいます。

5. 悪性ボットからの要求は 69% 増（1.1 兆件）と急増し、アカウント乗っ取りや金融アグリゲーターによるリスクなど、金融サービス利用者とそのデータに対する攻撃が続いていることを示しています。

高度化と大規模化が進む Web アプリケーションの脆弱性

最新のデータと昨年の金融サービスレポート「差し迫る敵：金融サービスに対する攻撃の分析」を比較すると、金融機関に対する攻撃がどのように進化しているか、また業界はどういったセキュリティリスクや課題に引き続き直面しているかについて、極めて重要な視点を得ることができます。特に、Web アプリケーションおよび API 攻撃は引き続き被害を及ぼしています。Akamai のリサーチチームは、金融サービスに対するこうした攻撃が高度化・大規模化し続けていることを確認しています。オープンバンキング、拡大する組込型金融市場、Banking as a Service (BaaS) など、API が不可欠となる業界のデジタルイニシアチブによってアタックサーフェスが拡大しています。

18 か月間のレポート対象期間（2022 年 1 月～ 2023 年 1 月）において、金融サービス業界の攻撃数は大幅に増加しています。この増加傾向は、2022 年第 2 四半期から 2023 年第 2 四半期の 1 年間で Web アプリケーションおよび API 攻撃が前年比 65% 増となっていることからも明らかです。金融サービスは、引き続き Web 攻撃が 3 番目に多い業界となり（図 1）、その攻撃数は 90 億件に達しています。これは、広く一般に公開され、すぐに悪用できる Web アプリケーションの脆弱性が爆発的に増えたことも一因です。Akamai のレポート「セキュリティギャップのすり抜け」では、2022 年が Web アプリケーションおよび API 攻撃の記録的な年だったことがわかります。これは ProxyNotShell の脆弱性（CVE-2022−41040）などの重大なセキュリティの欠陥が発覚したことが原因です。

Web アプリと API への攻撃が多い上位の業種

2022 年 1 月 1 日～ 2023 年 6 月 30 日

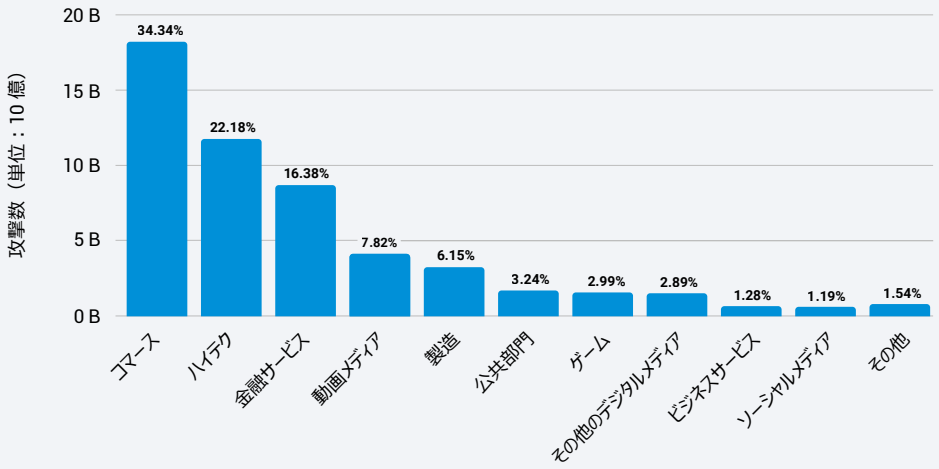


図 *1*：金融サービスは、調査期間における *Web* アプリケーションおよび API 攻撃数で *3* 位となっています。これは業界のデジタル化が進み、*Web* アプリケーションの脆弱性を悪用した攻撃が警戒すべき速さで増加しているためです。

金融サービスにおける Web アプリケーションおよび API 攻撃の詳細な調査（図 2）では、銀行が Web 攻撃の矛先となっており（58%）、金融サービス会社（フィンテック、資本市場、損害保険、決済会社、貸付会社など）がそれに続いている（28%）ことが明らかになっています。保険会社は、金融サービスの業種の中で Web アプリケーションおよび API トラフィック攻撃の 14% を占めています。

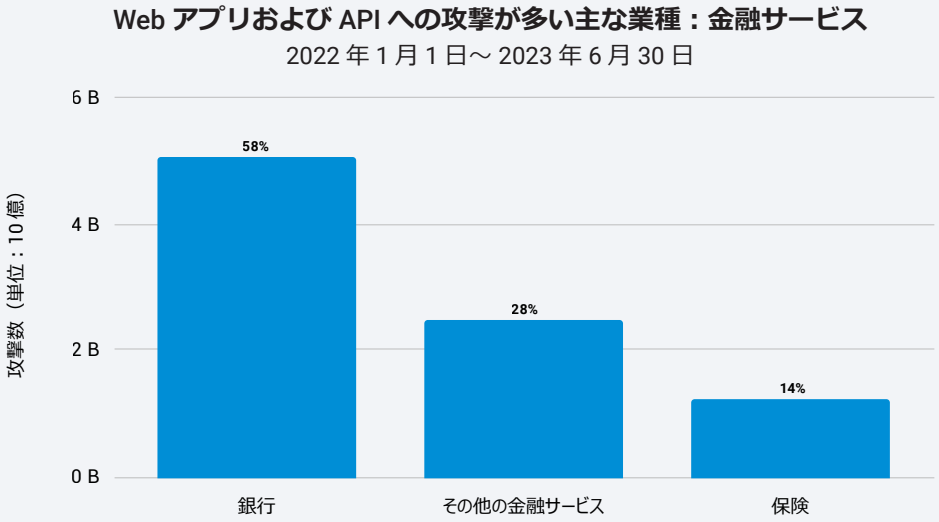


図 *2*：銀行は保有しているデータの種類が原因で *Web* 攻撃の影響を多大に受けていますが、フィンテックや資本市場などの他の金融サービス組織も大きな打撃を受けています

組織を標的とした今年の攻撃に共通しているのは、インターネットに面したアプリケーションのゼロデイとワンデイの脆弱性を積極的に狙い、標的組織への初期アクセスを得るという手口です。ランサムウェア攻撃では、こうした脆弱性は一般的な侵入手段になっており、初期侵害を果たす容易な経路として浸透しています。攻撃者が標的の防御を突破するために Web 脆弱性を利用するケースは増加の一途をたどっており、パッチの適用は時間との戦いになります。

ローカル・ファイル・インクルージョンは依然として Web 攻撃ベクトルの首位

ローカル・ファイル・インクルージョン（LFI）の脆弱性も、Web アプリケーションおよび API 攻撃の急増を後押ししています（図 3）。近年は、LFI が常に Web 攻撃ベクトルの首位となり、前年比 53% と急増しています。それに続くのが、クロスサイトスクリプティング（XSS）と SQL インジェクション（SQLi）です。攻撃者は、LFI を使用して、ディレクトリトラバーサル（パストラバーサルとも呼ばれる）攻撃を仕掛け、その攻撃が成功すると、機微な情報にアクセスできるようになり、そしてさらなる攻撃を仕掛けます。場合によっては、さまざまな目的で LFI を使用して不正を試みることがあります。たとえば、入力が有効であると Web アプリケーションを誤認させて Web サーバーのファイルや情報に不正にアクセスしたり、リモートコード実行（RCE）を試みたり、エンタープライズ企業のネットワーク侵入への足がかりを作ったりすることがあります。

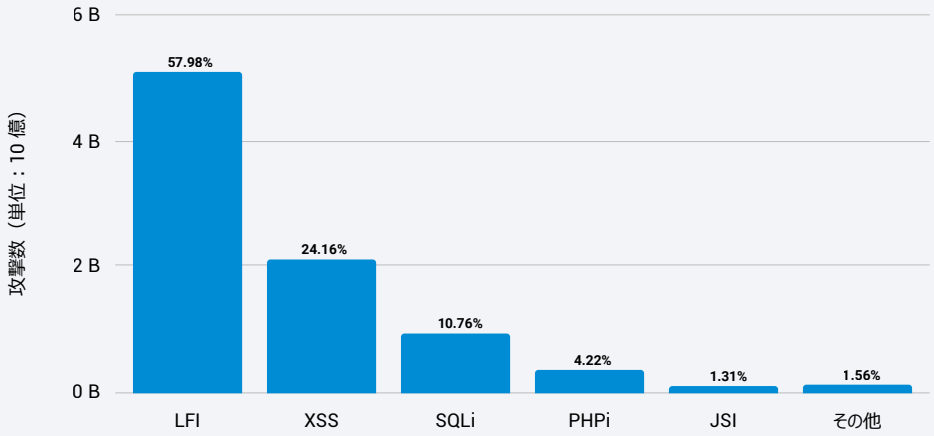


図 3：*LFI* は依然として *Web* 攻撃ベクトルの首位のままですが、*SQLi* などの他のベクトルも金融サービスに引き続きリスクをもたらしています

CL0P ランサムウェアが SQLi の危険を強調

昨年は、LFI が Web 攻撃タイプの首位となり、XSS と SQLi の件数は減少しています。これは、いくつかの要因が重なったことが原因と考えられます。Web アプリケーションファイアウォール（WAF）製品の XSS 攻撃や SQLi 攻撃の検知機能が改善され、攻撃者が別の攻撃手法に流れたことも一因でしょう。しかし、SQLi が減少したことで、金融サービスに対する潜在的な危険や影響が解消または軽減されるわけではありません。そのよい例として、2023 年 5 月、CL0P ランサムウェアの運営グループは、MOVEit Transfer の SQLi の脆弱性（CVE-2023-34362）を悪用し、多数の組織に攻撃を仕掛けました。Akamai の分析によると、攻撃者は、このセキュリティ欠陥を使用してファイル転送サーバーへのアクセスを獲得しました。目的は、そのサーバーから盗み出した機微な情報を利用して被害組織に身代金を要求することでした。金融機関は、この攻撃の影響を受ける注目度の高い組織と言えます。しかし、CL0P ランサムウェアがさまざまなマネージド型ファイル転送プラットフォームを悪用してきたやり口から考えると、このソフトウェア／プラットフォームを使用するあらゆる組織にランサムウェアの感染リスクがあります。他のランサムウェアグループがこの利益の出やすいビジネスモデルを模倣するかどうかは現時点ではわかりません。

攻撃者が標的の防御を突破するために Web 脆弱性を利用するケースは増加の一途をたどっており、パッチ適用は時間との戦いになります。

古い欠陥と、新しい Web スタック：金融サービス業界の攻撃ペイロード

組織は、脆弱なシステムをタイムリーに特定してパッチを適用することに困難を感じています。攻撃者はその弱点を把握し、古い脆弱性を標的への侵入ポイントとして引き続き悪用しています。さらに、ゼロデイ脆弱性を利用する攻撃者が増加しているという状況も、セキュリティギャップの問題をさらに悪化させています。金融サービスも例外ではありません。この業界に対する多くの攻撃を目の当たりにしてきた Akamai は、古い脆弱性を使った一般的なインジェクション攻撃だけでなく、新たな戦術を介して、より新しい、または最新の Web テクノロジースタックを標的とする攻撃も確認しています。

たとえば、PHP のテストフレームワークである PHPUnit の RCE 脆弱性（CVE-2017-9841）が発見されたのは 5 年前ですが、金融サービス業界ではいまだに活発に悪用されています（図 4）。

```
<?php print str_rot13('V pna erzbgryl rkrphgr CUC pbqr ba lbhe freire'); ?>
â€‹
```

図 *4*：このペイロードでは、攻撃者はアプリケーションに脆弱性がある場合に *RCE* の実行を試みます

ここに隠されたなテキストは「I can easily execute PHP code on your server（PHP コードをサーバーで容易に実行可能）」とデコードされます。このペイロードは、RCE が成功し、アプリケーションに脆弱性があることを示すために攻撃者によって使用されたものです。

次のペイロードは、より新しい Web テクノロジースタックへと攻撃者の関心が移行していることを示す例です（図 5）。この例では、Node.js（Web 開発者にとって一般的な JavaScript ベースのオープンソース・サーバーサイド環境）が使用されています。Akamai は、複数の金融サービス利用者を標的とするサーバーサイド・テンプレート・インジェクション（SSTI）攻撃を確認しました。Akamai は「App および API SOTI」レポートで、SSTI は単純な RCE 悪用に見えるが注意が必要な脅威の 1 つだと説明しています。SSTI を利用することで、攻撃者は悪性コードをテンプレートに注入し、そのコードがサーバー上で実行されると、攻撃者は機微な情報にアクセスし、サーバーを制御できるようになります。

図 5 は、「#{」で始まって「}」で終わるペイロードを示しています。これは文字列をコードとして評価するテンプレートエンジンの一般的なアノテーションです。波括弧の内側の記述内容は、Node.js の “child_process” パッケージをインポートしており、シェルスクリプトの実行を可能にします。

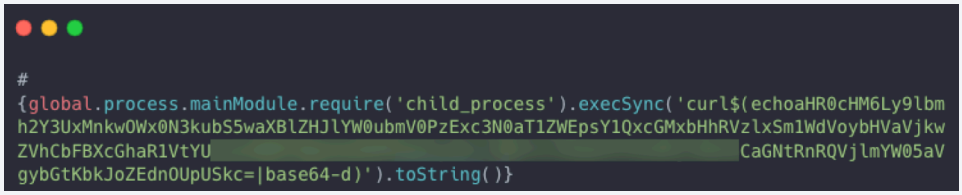


図 *5*：このペイロードはシェルコマンドの実行に使用されます

このシェルコマンドは、ほとんどの Linux 系オペレーティングシステムのデフォルトで実行できる「curl」です。さらに、呼び出される URL は Base64 でエンコードされ、組み込みの “base64” Linux コマンドでデコードされます（図 6）。このやり方は目新しいものではありません。最近確認したほとんどのコード・インジェクション・ペイロードは、Base64 エンコーディングで難読化されており、攻撃者が多用する手口となっているからです。

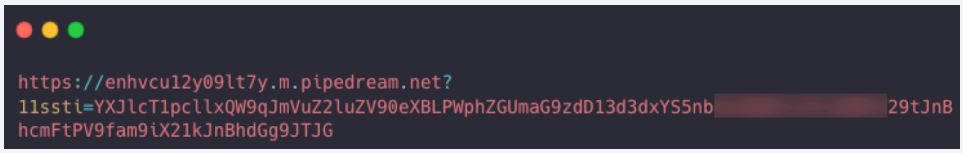


図 *6*：これは *Base64* エンコードストリングをデコードして取得した *URL* です

デコードされた URL は「pipedream.net」を示しています。これは Web 開発者が HTTP リクエストの受信とデバッグのために多用するサービスです。攻撃者は、このプラットフォームを使用して偵察アプローチを「隠ぺい」します。これもよくある手法であり、攻撃者はアウトオブバンドシグナリングを使用して脆弱性を検知します。基本的に、この pipedream.net が攻撃者のサーバーであり、受信接続を待機しています。攻撃者が標的に悪性コードを送信して接続が表示されると、サーバーに脆弱性があると判断して、さらなる攻撃を仕掛けます。この手法の詳細については、PortSwigger のブログをご覧ください。

現在の Web 開発者の間でテンプレートエンジンが普及する中、SSTI 攻撃は、あらゆる業種の組織にとって今後も重大な懸案事項になると予想されます。悪用テクニックとして広く出回っており、ペイロードのシンプルさもあって実際に悪用可能な脆弱性となっています。WAF も含めて、悪用を防ぐセキュリティ戦略を策定することをお勧めします。

現在の Web 開発者の間でテンプレートエンジンが普及する中、SSTI 攻撃は、あらゆる業種の組織にとって今後も重大な懸案事項になると予想されます。

API 攻撃と脆弱性

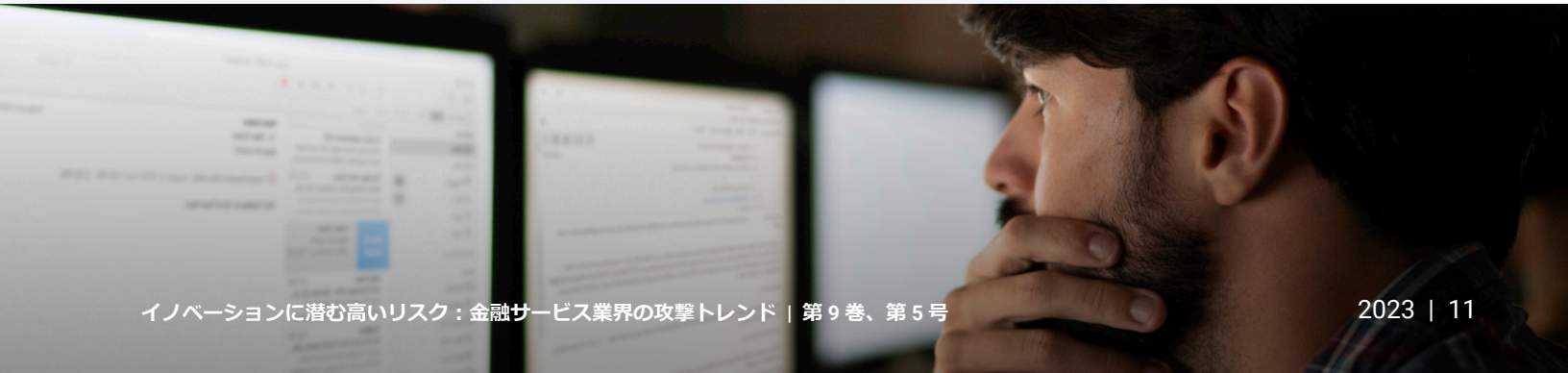
API は、結合繊維です。オープンバンキングなどで安全な情報交換を可能にし、組織におけるデジタルトランスフォーメーションを力強くサポートします。その成果として、さらなるビジネス成長とシームレスなユーザー体験をもたらし、顧客や銀行、金融サービスを提供する他社もメリットを得ることができます。金融サービスや他の業界で API が広く普及する中、ビジネスロジックの欠陥を悪用する攻撃者に対する懸念が高まっており、API セキュリティが注目されています。最新の OWASP Top 10 リリースでも、API セキュリティリスクが注目されています。このセクションでは、セキュリティ防御者と金融サービス組織が警戒すべきこのホットな脆弱性ベクトルについて詳しく考察し、攻撃が成功した場合の対応を明らかにします。

金融サービス企業が対処すべき主な脆弱性の 1 つが、シャドー API です。ほとんどの場合、シャドー API は、手順やプロトコルに従わずに作業した結果生じます（開発者が作業を文書化せずに緊急プロジェクトを急いで完了しなければならない場合など）。API が文書化されないと、追跡も管理もできず、セキュリティを確保できません。このように、API とそのアセットに対する可視性がない状態では、誰がどのようにそうした API を使用しているのか把握できないため、企業は問題の監視を余儀なくされます。

API で想定されるもう 1 つの問題が、機微な情報の漏えいです。この脆弱性は重大な懸念となり、経済的損失や評判の失墜も含めて、企業に多大な損害をもたらします。機微な情報が、個人を特定できる情報（ユーザー名、住所、メールアドレス、電話番号など）も含めて、ペイロードではなく その URL を介して不用意に受け渡される可能性があります。どんなデータ漏えいも壊滅的な被害をもたらしますが、金融機関で漏えいが発生すると、クライアントの銀行口座や資金に関わるため、被害はさらに甚大になります。米州機関で最近発生したデータ漏えいでは、不正なエンドポイントから脆弱なデータ（社会保障番号、住所、生年月日など）が流出しました。

90 億

金融サービスに対する Web アプリケーションおよび API 攻撃の数



API に対する現在のほとんどの攻撃は、2 つのメインカテゴリーに分類されます。1 つ目は、アクセス制御の回避です。ユーザー検証を導入すべきエンドポイントに対する攻撃が含まれます。適切な検証が導入されていないエンドポイントは、悪性アクティビティの温床となります。2 つ目のカテゴリーは、ここ数年連続して確認していますが、アカウントの乗っ取りです。オブジェクトレベルの認可の不備（BOLA）、総当たり攻撃、Credential Stuffing などが含まれます。こうした BOLA 攻撃は、他の攻撃よりも「伝統的」と思われがちですが、OWASP API Security Top 10 で数年にわたって首位にランクされています。

金融サービスによるサードパーティースクリプトへのプロアクティブなアプローチ

かつての金融サービス業界では、Web サイトに機能を追加するためにファーストパーティースクリプトに大きく依存していました。しかし、オンラインバンキングが普及するにつれて、金融機関はサードパーティースクリプトを追加で組み込むことで、全体的なユーザー体験を向上させています。コロナ禍に始まったサードパーティースクリプトの急速な導入により、多くのサービスや機能が生成され、新たなセキュリティリスクを招く可能性があります。攻撃者は、単純にクライアントサイドの脆弱性を侵入ポイントとして悪用したり、Web サイトの一部としてロードされるサードパーティーのスクリプトに悪性のコードを挿入したりする可能性があります。その結果、金融サービス企業は Magecart 型攻撃、Web スキミング、クリプトジャッキングのリスクにさらされ、顧客の情報が盗まれたり、不正なトランザクションで使用されたりする恐れがあります。組織のブランドや評判は失墜し、コンプライアンスの問題や、その過程で経済的損失を被る可能性もあります。サードパーティースクリプトの脆弱性を介した金融機関サービスに対する攻撃はまだ確認されていませんが、このアタックサーフェスを利用する攻撃者が現れるのは時間の問題です。そのため、Akamai Client-Side Protection & Compliance などのプロアクティブな保護で備えることが重要です。

Akamai のデータによると、金融サービスが使用しているスクリプトの 30% は、サードパーティーベンダーによるものです（図 7）。この割合は、他の業種（41%）を少しだけ下回っていますが、活動範囲を拡大している金融サービス業では、クライアントサイド攻撃に対して脆弱になります。幸い、金融サービス組織はこの潜在的なセキュリティ脅威を認識し、ソリューションの導入を進めています。さらに、Forrester の「The State Of Application Security（アプリケーションセキュリティの現状）」調査によると、PCI DSS v4.0 で注目された新たな要件により、16% の金融機関がクライアントサイドのコード保護を導入し、規制に準拠しています。金融サービス業界がデジタル化への取り組みと並行して、サードパーティースクリプトの組み込みを進めることで、この数字は今後さらに増加すると考えられます。

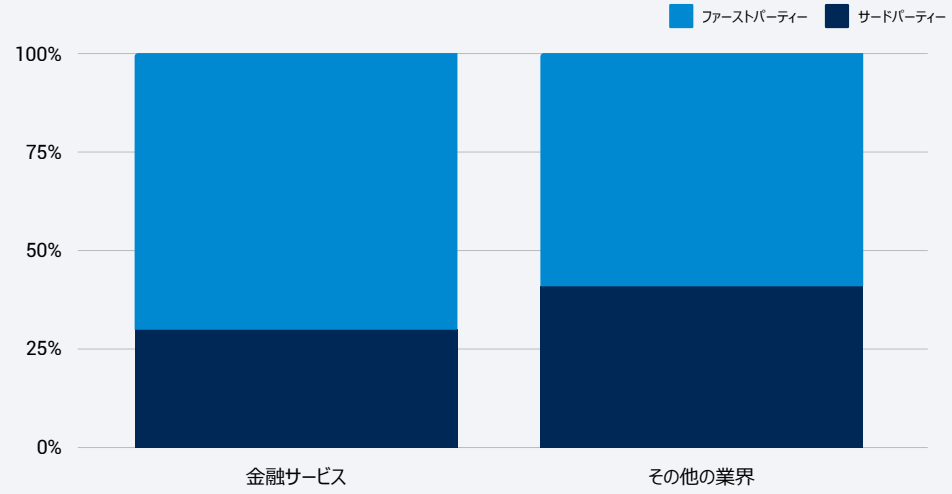


図 *7*：金融サービスで使用されるスクリプトの合計 *30%* は、サードパーティーベンダーによるものであり、他の業界は *41%* のスクリプトを使用しています

最近の CSO ／ Akamai の共同調査「悪性ボットから悪性スクリプトまで：特別な防御の有効性」では、疑わしいスクリプトのふるまいには共通点があると指摘しています。回答者全体の 10 人中 8 人（81%）は、直近の 12 か月間に疑わしいスクリプトのふるまいの標的になったと答えており、その割合は米国の回答者では 94%、ヨーロッパの回答者では 72% に達します。

コンプライアンスと脅威は、いずれも企業がスクリプト環境に関するリスクを評価するきっかけになっています。

DDoS 攻撃の業界および地域シフトが続く

金融サービス業界に対する DDoS 攻撃は、世界中で引き続き増加しています（レイヤー 3 およびレイヤー 4 攻撃に対する Akamai の DDoS 防御およびネットワーク・クラウド・ファイアウォール機能を通じて観測）。図 8 は、金融サービス業がゲーム業界を抜いて DDoS 攻撃対象の首位になったことを示しています。図 9A は、2022 年秋に全ての業種に対するレイヤー 3 およびレイヤー 4 DDoS 攻撃イベントが大幅に減少していることを示していますが、図 9B では、金融サービス業界に対する攻撃数が引き続き増加していることがわかります。

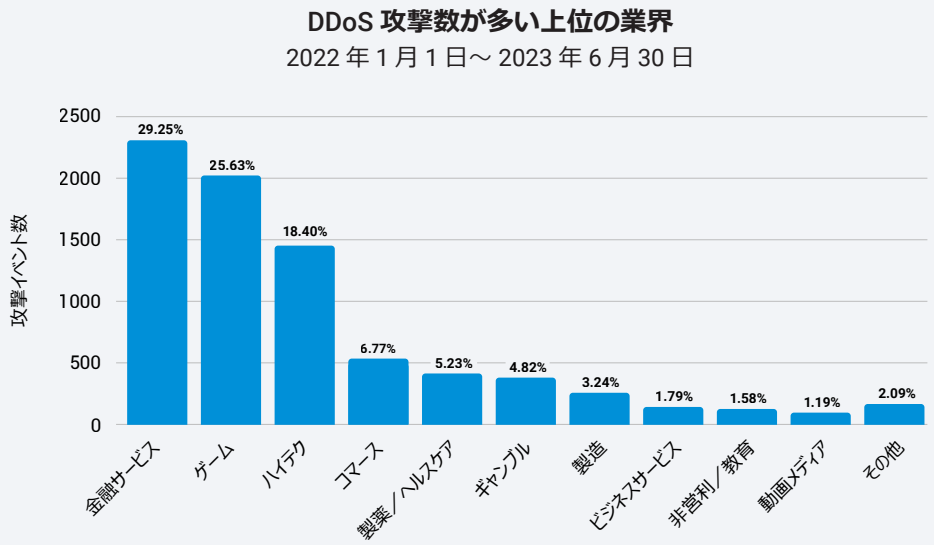


図 *8*：金融サービスはレイヤー *3* および *4 DDoS* 攻撃数で首位となり、金融サービス業界とゲーム業界だけで *DDoS* 攻撃数の 50% 以上を占めています

第 1 位

金融サービスは、最も多くの DDoS 攻撃を受けた業界であり、その数はゲーム業界を上回っています

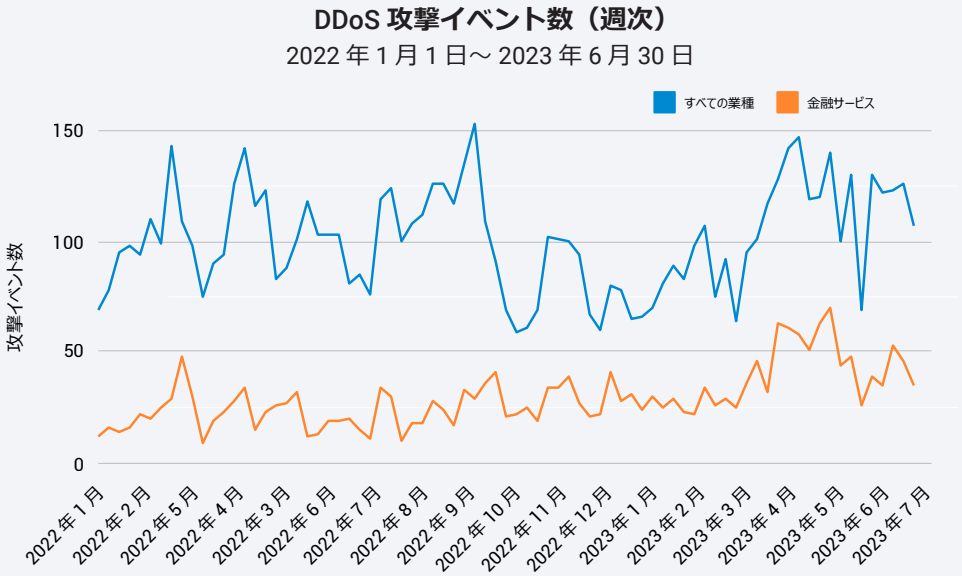


図 *9A*：すべての業界を合計したレイヤー *3* および *4 DDoS* 攻撃の数は *2022* 年 *8* 月末から *2022* 年 *12* 月初頭にかけて *3* 分の *1* 以上減少しています

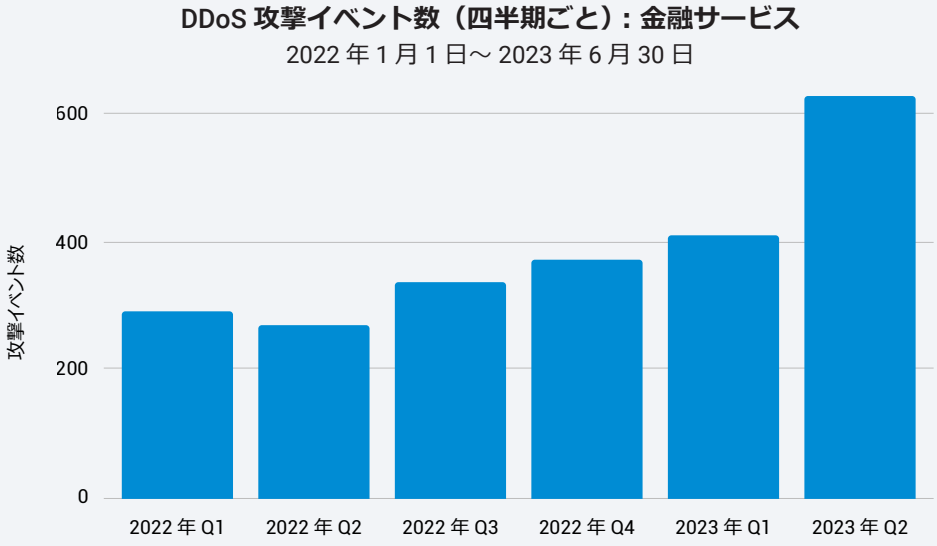


図 *9B*：*2022* 年第 *2* 四半期のわずかな減少を除き、金融サービス業界への攻撃は増加し続けています

DDoS 攻撃は、長年にわたってインターネットで最も強力な武器の一つだと考えられてきました。大規模なサービス中断と多額の経済的損失を招き、ネットワークのリソースや運用のあらゆる部分に影響を及ぼし、いつでも攻撃される可能性があります。銀行が DDoS 攻撃を受けると、サービスと Web サイトがオフラインになり、顧客は口座にアクセスできなくなり、業務が危機的状況に陥ります。その結果、多額の経済的損失が発生し、ブランドの評判は失墜します。

DDoS 攻撃は、長年にわたってインターネットで最も強力な武器の一つだと考えられてきました。

DDoS 攻撃は、ランサムウェアグループの戦術、技術、手順（TTP）の一部など、脅迫スキームの一部として発生します。2020 年 8 月の状況も同様でした。Akamai は、攻撃者がビットコインの身代金の支払いを要求し、従わないと DDoS 攻撃を仕掛けるという脅迫を検知しました。三重脅迫ランサムウェアまたはランサム DDoS（RDDoS）は、ビジネスにランサムウェアを侵入させ、身代金を支払わないと盗み出した顧客情報を流出させると脅します。さらに、DDoS 攻撃で被害組織の業務を混乱させ、身代金の支払いを迫ります。RDDoS はますます破壊的なサイバー脅迫となり、サイバー犯罪者から利益の出やすい手段として認知され、普及が進んでいます。BlackCat、AvosLocker、Killnet、DarkSide、Lazarus などのランサムウェアグループは、このように脅迫スキームで DDoS 攻撃を有効に活用しています。

DDoS 攻撃は、金融サービス業界でも増加しています。これは、仮想マシンベースのボットネットの力が大幅に増大し、ウクライナでの戦争によって親ロシアのハクティビズムが活発化したことが原因と考えられます。実際、親ロシアのハクティビズムグループは、2023 年 6 月初めに、ヨーロッパと米国の金融組織を標的とした「大規模」な組織的 DDoS 攻撃を仕掛けると表明しました。これらの攻撃グループには、Killnet、REvil、Anonymous Sudan が含まれます。この親ロシアのハクティビズムは、金融サービス業界における DDoS 攻撃の地域シフトを象徴していると言えるでしょう。EMEA での発生件数は北米のほぼ 2 倍に達しています（図 10）。

地域ごとの DDoS 攻撃イベント数：金融サービス

2022 年 1 月 1 日～ 2023 年 6 月 30 日

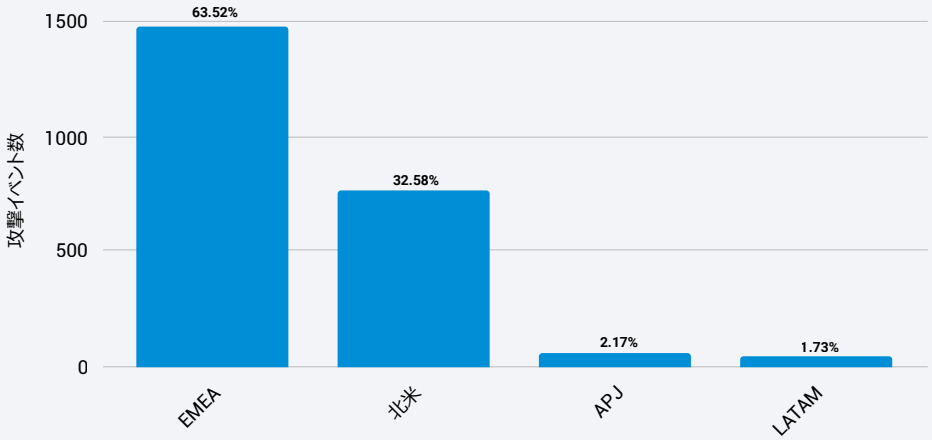


図 *10*：*EMEA* の金融サービス業界のレイヤー *3* およびレイヤー *4 DDoS* 攻撃数は、北米のほぼ *2* 倍に達しています

この地域シフトは、前回の金融サービスレポートから確認していました。ウクライナ側に賛同するヨーロッパの銀行に対する攻撃は、いまだ続くロシアのウクライナ侵攻の経済的・政治的な動機によるものであり、このシフトの主な原因だと推測されます。そして、攻撃者はその矛先をすばやく容易に切り替えられるという残念な事実も読み取ることができます。組織は、所在地や事業の種類にかかわらず、防御対策を導入しなければなりません。私たちは DDoS 攻撃と無縁な業界がないことをすでに把握しており、重要な他のインフラ（ヘルスケアなど）も数多く存在します。攻撃者からの人気が高く、金融サービスに対する DDoS 攻撃数が増加しているのも当然と言えるでしょう。EMEA における DDoS 増加の詳細については、このレポートの EMEA 地域のスナップショットセクションをご覧ください。

アプリケーション／ Web ページ（レイヤー 7）DDoS 攻撃

アプリケーション／ Web ページに対する攻撃数の増加も確認しており（レイヤー 7 DDoS 防御および WAF 機能で観測）、2023 年には、攻撃の量とスピードで多くの新記録を打ち立てています。アプリケーションレイヤー DDoS 攻撃は、依然として金融サービスとアプリケーションに対する最大の脅威の 1 つです。従来のレイヤー 3 またはレイヤー 4 DDoS 攻撃は、ネットワークやトランスポート・レイヤー・インフラに過度な負荷をかけることが狙いでしたが、アプリケーションレイヤー DDoS 攻撃は、特定のアプリケーション機能やアプリケーションサーバー自体を標的にします。悪性トラフィックの量が比較的少なくても、多大な損害を与えることができます。アプリケーションレイヤー DDoS 攻撃は、CPU やメモリーなど、アプリケーションレベルのリソースを標的にします。攻撃を受けたアプリケーションやサービスは、ネットワークを利用できたとしても速度が低下するか、完全に無反応になります。さらに、マルチベクトル攻撃に複雑さが加わり、アプリケーションレイヤーでのソフトウェアの欠陥や設定ミスなど、具体的な脆弱性を悪用する可能性もあります。モノのインターネットの進化により、インターネット接続デバイスの高度化が進み、その一方で防御しづらくなりました。すぐに利用できる DDoS 請負サービスと闇市場により、攻撃者は低コストで大規模な DDoS 攻撃を調達して仕掛けることができます。私たちはこの課題を認識しなければなりません。

金融アプリケーションに関しては、レイヤー 7 の DDoS 攻撃が引き続き問題になります。犯罪者は、より強力な防御に対抗するために、攻撃の作戦、ネットワーク、TTP を強化する取り組みを絶えず行っています。多くの大規模な DDoS 攻撃によく見られる特徴には、次のようなものがあります。

- IP ／サブネットおよび国の高度な分散
- 感染した／リースされたクラウド・サービス・プロバイダー、Tor 出口ノード、匿名／オープン・プロキシ・ノードなど、豊富な攻撃ソース
- GET フラッド
- ホームページ、ランダム URL、ログインエンドポイントなど、キャッシュできない URL
- 家庭用 ISP、モバイル・キャリア・ネットワーク、または大学ネットワークの背後にボットネットを作成する高度な攻撃者による IP スプーフィング
- 防御者の応答に基づいたダイナミックな適応型の攻撃

金融機関は、多層型の防御戦略を優先すべきです。たとえば、定期的なセキュリティ監査の実施、高度な検知と緩和の導入、コンテンツ・デリバリー・ネットワークを利用したトラフィック負荷の分散、境界セキュリティのインターネットエッジへの拡大などが考えられます。さらに、絶えず進化するこの脅威状況に対応するためには、事前対応型と適応型のサイバーセキュリティの実践を最優先すべきです。

攻撃を受ける金融サービス利用者

金融サービスの利用者は、機微な情報に対する猛攻に常にさらされています。金銭的な見返りを得られる可能性が高いため、当然とも言えます。攻撃者は、複雑で手間のかかるプロセスを経て金融サービス業界の厳重な境界防御を突破することなく、最小限の労力でユーザー情報を獲得できます。このセクションでは、2022 年のレポートで使用したデータセットの 1 つを更新し（図 11）、金融サービス業界で想定されるリスクを検証します。攻撃者が金融サービス組織とその顧客をどのように標的にしているのか理解を深めることで、こうした脅威に対する効果的な防御戦略を考案できます。

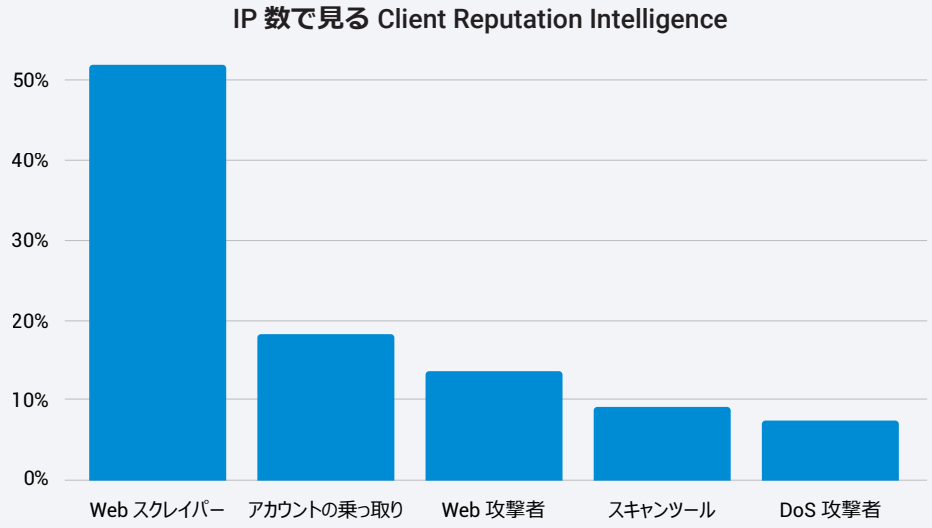


図 *11*：*Akamai Client Reputation* インテリジェンスの *IP* への配点は、*90* 日間の金融サービス業界全体を標的とした攻撃に基づいています

昨年はアカウントの乗っ取りが最も多かったのですが、今年は金融サービスをターゲットとする IP の 50% 以上が Web スクレイパーに関連していました。こうした自動化ツールは、Web サイトから情報を収集し、サイトの正確なレプリカを作成するために使用されます。そのレプリカをフィッシングに利用し、ユーザーをだまして機微な情報を入力するように仕向けます。

アカウントの乗っ取りや Web スクレイパーに関連する攻撃者の IP の存在は、金融サービスの利用者とそのデータが大きなリスクにさらされていることを意味します。

悪性ボットの増加により、ユーザーデータに対する脅威が悪化

金融サービス業界に影響する悪性ボットリクエストは、四半期ごとに増加の傾向を見せており、2023 年 7 月 1 日までの 18 か月間に 1.1 兆件のリクエストを確認しています（図 12）。特に、悪性ボットのリクエストは前年比 69% で急増し、金融機関とその顧客に対する脅威は引き続き拡大しています。悪性ボット数の増加は、詐欺行為や個人情報の窃取など、金融サービスの利用者が明らかにリスクにさらされていることを示しています。アカウントの詳細情報や個人の特定が可能な情報などの盗まれた情報は、ダーク Web で販売して現金化されたり、他の攻撃に利用されたりします。

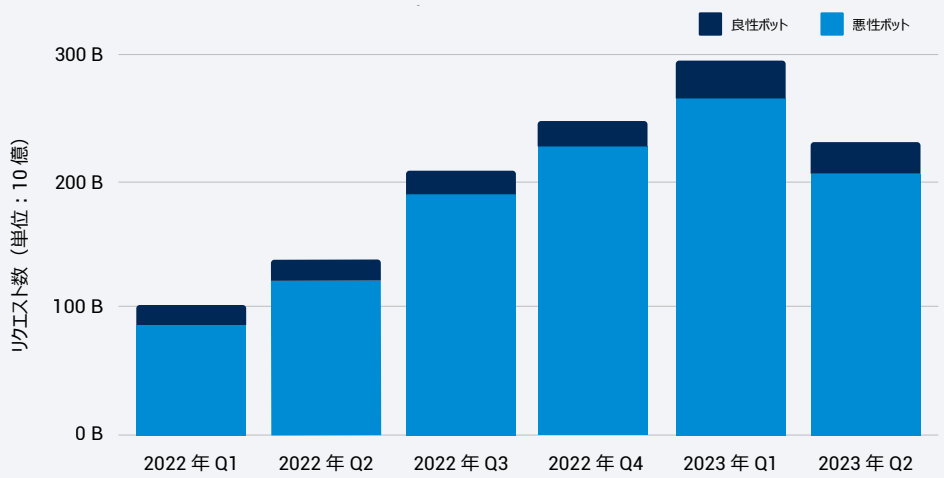


図 *12*：悪性ボットリクエストは *18* か月間で *1.1* 兆件に達し、金融サービス組織とその顧客にセキュリティ課題を引き続き突きつけています

ボットは幅広い用途で使用されます。たとえば、Web サイトコンテンツをスクレイプし、一見正当な金融サービスブランドに見えるフィッシング Web サイトを作成するケースもあります。2023 年第 2 四半期だけを見ても、フィッシング被害者の 50% 以上は金融サービス組織となっています（図 13）。Credential Stuffing 攻撃も顕著です。攻撃者はボットを使用してユーザー名とパスワードの組み合わせを自動的に取得し、アカウントの乗っ取りを達成します。さらに、アカウントの乗っ取り詐欺と Credential Stuffing を仕掛ける攻撃者は、パスワード認証が再利用される傾向を悪用しています。Okta の 2022 年度「State of Secure Identity Report（セキュアなアイデンティティの最新事情）」レポートによると、金融サービスのログイン行動の半数以上は Credential Stuffing 攻撃を受ける可能性があり、このセキュリティリスクが金融サービス業界にまん延していることは明白です。

悪性ボット数の増加は、詐欺行為や個人情報の窃取など、金融サービスの利用者が明らかにリスクにさらされていることを示しています。

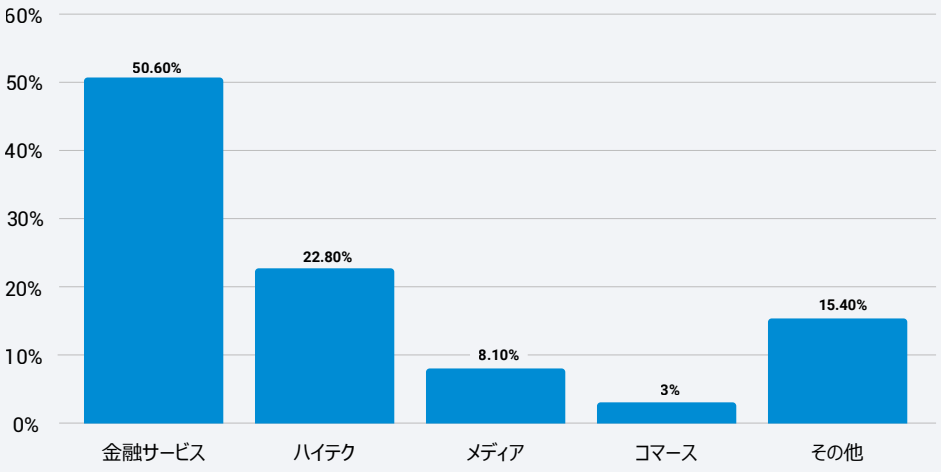


図 *13*：*2023* 年第 *2* 四半期の金融サービスにおけるフィッシング攻撃の被害者数は最多でした（*50.6%*）

CSO との共同調査で、ATO 攻撃もコマース業界の組織にとって大きな問題になっていることを確認しました。回答者の 4 分の 3 以上（79%）は、直近の 12 か月間にアカウント乗っ取り攻撃の標的になったと回答しています。米国ではさらに深刻で、実に 90% が攻撃の対象になったと回答しています。

アカウント乗っ取り詐欺がもたらす危険性は、複数のユーザーアカウントでログイン試行が成功し、攻撃者がアカウントを流出させるか、他のサイバー犯罪者にアクセス権や情報を転売する状況にあると言えるでしょう。しかし、金融機関にも弊害があります。問題解決を支援し、リソースを提供しなければなりません。アカウント乗っ取りは、金融サービスの利用者によるブランド意識と信頼の両方を失墜させます。

金融アグリゲーター：良い面、悪い面、醜い面

デジタルバンキングの登場により、消費者のアカウント情報やその他のバンキングデータを複数のソースから 1 つのダッシュボードやアプリに集約して操作できるようになりました。通常はフィンテックによって運営される金融アグリゲーターは、複数の金融機関から金融情報を集めて統合するサービスを提供します。消費者は、膨大な数のアカウント（銀行、クレジットカード、投資ポートフォリオ、ローンなど）を 1 か所で閲覧、管理できます。その結果、消費者はすべての金融データにリアルタイムでアクセスする機会と利便性を得られ、豊富な情報に基づいて財務全般の判断を下すことができます。こうしたアグリゲーターは、ターゲットとなる顧客、ビジネスモデル、集約する金融データの種類に応じて、以下のように分類できます。

- オープンバンキングコンプライアンス
- ペイメント
- パーソナルファイナンス
- 投資
- クレジットカードアグリゲーション
- ローンアグリゲーション
- 保険アグリゲーション

大きなメリットにはセキュリティ課題が付きもの

メリットがある反面、アグリゲーターには潜在的なアタックサーフェスがあり、詐欺行為やアイデンティティ盗難などのリスクを消費者にもたらします。アグリゲーターは、その性質と保有するデータ量から、サイバー犯罪者に利益の出やすい標的として目を付けられています。さらに、アグリゲーター間に存在するセキュリティギャップとデータ収集方法のギャップによっては、攻撃者にとって新たな悪用の手口を生み出す可能性もあります。銀行や他の金融組織は綿密に調査されますが、アグリゲーションサービスのサードパーティープロバイダーには同じ規制やコンプライアンス要件が適用されないケースがあり、大手銀行よりもリスクを犯してデータ窃取しやすいと判断される場合もあります。この事情を把握した攻撃者は、こうしたプラットフォームを機微なアカウントや銀行の認証情報を盗むのに最も抵抗の少ない経路とみなす可能性があります。攻撃者がこうしたプラットフォームに攻撃を仕掛けて機微なアカウントの宝庫にアクセスし、不正な取引に使用したり、オンラインのダーク Web 市場で売却したりするのも時間の問題でしょう。

アグリゲーターは、その性質と保有するデータ量から、サイバー犯罪者に利益の出やすい標的として目を付けられています。

こうしたアグリゲーターのほとんどは複数の外部ソースからデータを収集しているため、いったん侵害されると顧客データも筒抜けとなり、データソースにも影響が及びます。さらに、データが安全に処理・保管されていない場合は、プライバシーやセキュリティの課題も浮上します。同様に、外部ソースの構造や可用性に変化があると、アグリゲーターの機能にも影響します。以下のようなセキュリティリスクやアグリゲーターの基本的な脆弱性によっては、データ漏えいも発生します。

- **安全ではないデータ転送：**アグリゲーターがデータ転送に HTTPS などの安全なプロトコルを使用していない場合、データの横取りや操作の可能性があります。
- **不十分な入力検証：**アグリゲーターが検索クエリーや個人データなどのユーザー入力を適切な検証なしで受け入れる場合、SQLi や XSS などの攻撃に対して脆弱になります。
- **安全ではない API：**多くの Web アグリゲーターは、API を使用してさまざまなソースからデータを取得します。これらの API のセキュリティが適切に確保されない場合、データやサービスへの不正アクセスに利用されかねません。
- **認証と認可の欠如：**アグリゲーターが認証や認可を適切に導入していない場合、機微な情報や機能への不正アクセスに利用されかねません。
- **クロスサイト・リクエスト・フォージェリまたは他の WAF 攻撃：**適切な保護がない場合、攻撃者はユーザーをだまして同意のないままアクションを実行し、データ損失やアカウント侵害を招く可能性があります。

こうした潜在的なリスクを考慮し、企業は、トラフィックのソース、クライアントのアプリケーション内の転送先、リクエストの量と分散を含めたボット／ API トラフィックに対する可視性を提供することで、財務情報アグリゲーター向けのエッジベース･ガバナンスモデルを構築すべきです。この可視性を得ることで、クライアントは財務情報アグリゲーターに許可すべき適切なアクセスレベルを判断できます。この判断では、これらのアグリゲーターがもたらすリスクとともに、エンドユーザーの使い勝手を考慮する必要があります。この戦略的なアプローチにより、エンドユーザーのシームレスな体験を実現しながら、アグリゲーターから漏れる情報の量を制限できます。

最後に、個々の消費者は、アグリゲーターが収集する情報の種類を検証し、そのアグリゲーターが消費者への通知や同意なしで他のプロバイダーと情報を共有するかどうかも確認する必要があります。これらのプラットフォームのサービス契約を確認することで、消費者はプラットフォームの仕組みをより深く理解し、アグリゲーターによる情報の収集方法、セキュリティ対策、共有方法を容認できるかどうか判断できます。

1.1 兆

悪性ボットリクエストの数

コンプライアンスと規制

金融サービスは、最も厳しい規制が課せられている業界の 1 つです。そのため、セキュリティ戦略と現行および今後の法律／規制をすり合わせることが不可欠です。現在の機能やポリシーに関連して考慮すべき新たなコンプライアンス問題としては、耐障害性、身代金の要求に従うかどうか、JavaScript 環境などがあります。

まず、欧州連合（EU）の新たなサイバーセキュリティ規制は、耐障害性に重きを置いています。デジタル・オペレーショナル・レジリエンスに関する規制（DORA）は、包括的な EU 規制です。EU の金融セクターとその情報通信技術（ICT）サードパーティープロバイダーに対して、5 本柱の義務を規定します。

1. ICT リスク管理
2. ICT に関連するインシデントの管理、分類、報告
3. デジタル・オペレーショナル・レジリエンスに関するテスト
4. ICT サードパーティーリスクの管理
5. 情報共有に関する合意

DORA の目的は、EU 金融システムの運営上の耐障害性、パフォーマンス、安定性を脅かす ICT リスクに対処することです。一般データ保護規則（GDPR）と同様に、この規制は他の管轄区域にも影響を及ぼし、金融セクター向けのサイバー保護法の範囲が拡大する可能性があります。DORA は、2025 年 1 月に発効される予定です。注意すべき他の規制としては、ネットワークおよび情報セキュリティ指令（NIS2）の拡張や、サイバーレジリエンス法案などがあります。

次に、身代金要求（主にランサムウェアまたは DDoS 攻撃で発生）の報告と対応に関する要件が進化を続けています。2022 年の重要インフラに関する米国サイバーインシデント報告法により、米国サイバーセキュリティ・インフラセキュリティ庁 (CISA) は、報告要件を策定する要件を与えられています。ニューヨーク州金融サービス局は、72 時間から 24 時間への報告期限の変更案を提出しました。フロリダ州はノースカロライナ州に続く 2 番目の州として、州および地方自治体が身代金の要求に従うことを禁止しました。さらに多くの州も同様の法律の導入を検討しています。こうした規制や契約上の合意に確実に準拠し、これらを危機管理計画に盛り込む必要があります。

最後に、スクリプトに関する PCI DSS v4.0 要件の発効が迫っています。2025 年 3 月 31 日までに、組織は消費者のブラウザーに読み込まれ実行される支払いページの全スクリプトを管理する必要があります。さらに、対話型ログインで使用されるアプリケーションやシステムアカウントで、ファイルやスクリプトに組み込むパスワード／パスフレーズをハードコードしないという新しい要件があります。JavaScript 環境は動的な性質があり、サードパーティースクリプトが多数存在するため、スクリプト環境を理解し、インベントリ、検証、スクリプトのセキュリティを提供するセキュリティ制御の導入が不可欠です。攻撃を検知して緩和するための可視性を保つことも重要です。

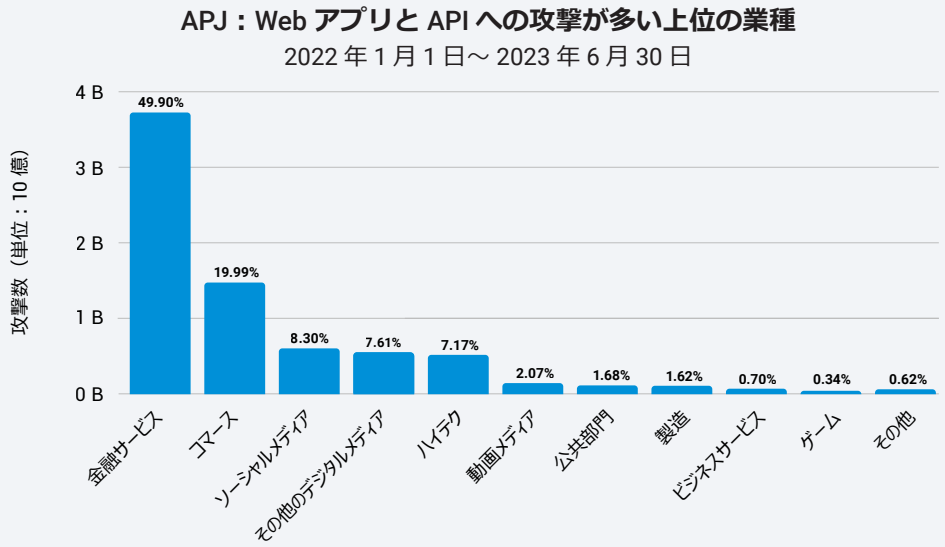
アジア太平洋・日本（APJ）地域とヨーロッパ・中東・アフリカ（EMEA）地域における金融サービス業界の動向の詳細については、各地域の以下のスナップショットをご覧ください。

金融サービス：APJ スナップショット

APJ スナップショットは、当社の大手金融サービスに関する SOTI レポート「イノベーションに潜む高いリスク：金融サービス業界の攻撃トレンド」（本編は英語版のみ）の姉妹編として作成されたものです。これから説明する攻撃ベクトルを攻撃者がどのように利用するのかの詳細な説明、組織を保護するための推奨事項、当社の調査方法に関する説明については、同レポートを参照してください。

サイバー犯罪者は Web アプリケーションおよび API 攻撃に狙いを絞っている

前回の金融サービスに関する SOTI レポートの調査結果で示唆したように、アジア太平洋・日本（APJ）地域で最も Web 攻撃の標的になっている業種は、依然として金融サービス業界であり、2022 年 1 月から 2023 年 6 月までの 18 か月の間に発生した Web アプリケーションと API への攻撃のうち、ほぼ 50% が APJ で発生しています（APJ 図 1）。これは、APJ の全業種が受けた Web 攻撃の総数 74 億件のうち 37 億件に相当し、その件数は 2022 年第 2 四半期と 2023 年第 2 四半期の前年同期比で 36% 増加しています。



APJ **図 *1*：*APJ* で攻撃の頻度が最も多い業種は依然として金融サービス**

世界的に見ると、金融サービス業に対する Web アプリケーションと API への攻撃の最も標的になっている国はオーストラリアで 36.6% を占め、米国の 34.4% よりもわずかに多くトップに立っています。APJ に絞って見ると、オーストラリア、シンガポール、日本が、標的にされる地域のトップ 3 となっており、この地域を合計すると、このタイプの攻撃の 4 分の 3 以上を占めることになります。

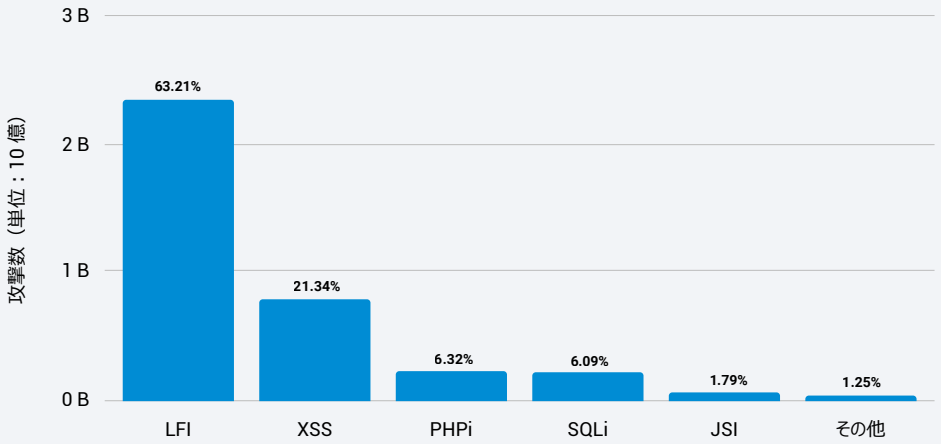
金融機関に対する Web アプリケーションおよび API 攻撃をさらに掘り下げて調べると、その攻撃の大部分（92.3%）を銀行業が占めており、保険業が 1.7%、その他の金融サービス企業（フィンテック、資本市場、損害保険、決済、融資など）が 6.0% を占めていることがわかりました。

LFI が依然として群を抜いて多い攻撃ベクトル

APJ の金融サービスは、2022 年に報告した傾向と、攻撃ベクトルという点で見たときの現在の世界的な金融サービスの傾向を反映しており、ローカル・ファイル・インクルージョン（LFI）が攻撃の 63.21% を占め、最も多い攻撃となっており、続いて、クロスサイトスクリプティング（XSS）が 21.34% を占め 2 位となっています（APJ 図 2）。

APJ：Web アプリケーションと API への上位の攻撃ベクトル：金融サービス

2022 年 1 月 1 日～ 2023 年 6 月 30 日

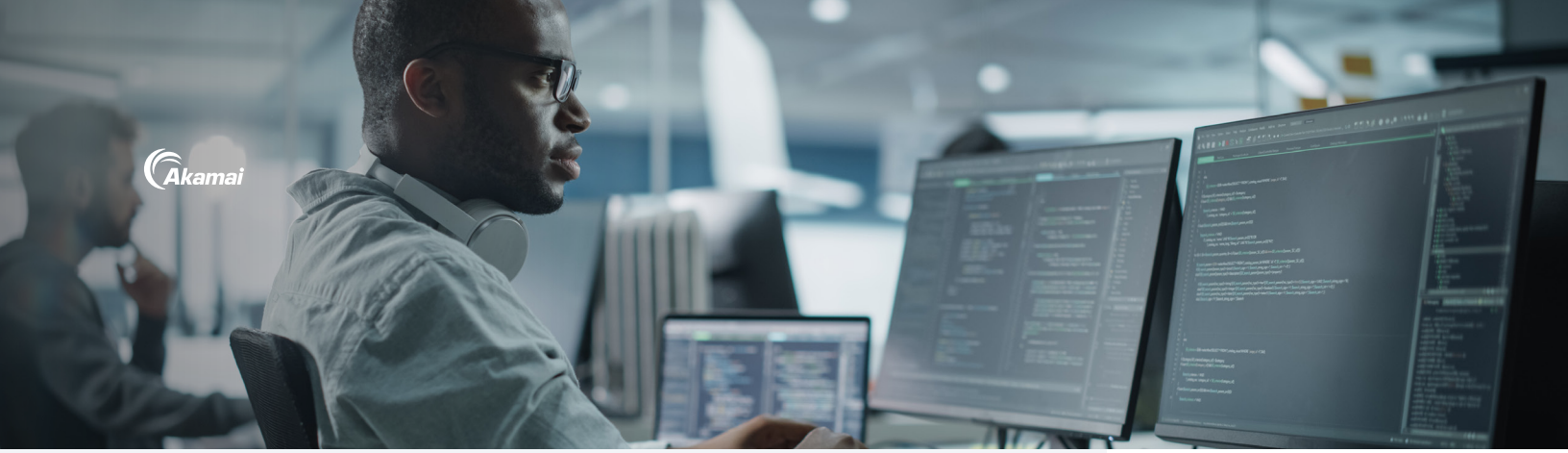


***APJ* 図 2：*APJ* の金融サービスに対する攻撃ベクトルの中では依然として *LFI* が群を抜いているが、*XSS*、*PHPi*、*SQLi* などの攻撃ベクトルのリスクも無視できない**

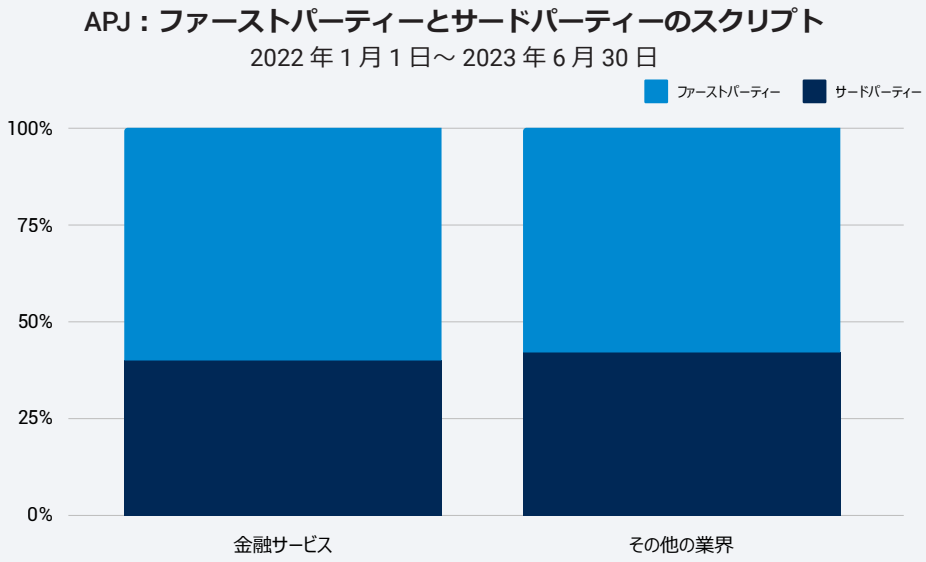
攻撃者は、何年にもわたって LFI を使用して、ディレクトリトラバーサル（パストラバーサルとも呼ばれる）攻撃を仕掛け、その攻撃が成功すると、機微な情報にアクセスできるようになり、そしてさらなる攻撃を仕掛けます。場合によっては、さまざまな目的で LFI を使用して不正を試みることがあります。たとえば、入力が有効であると Web アプリケーションを誤認させて Web サーバーのファイルや情報に不正にアクセスしたり、リモートコードを実行したり、エンタープライズ企業のネットワーク侵入への足がかりを作ったりすることがあります。

サードパーティースクリプト – リスクと被害

オンラインバンキングが普及するにつれて、金融サービス企業は、サードパーティースクリプトを使用して、新しいサービスや機能を手早く増やして全体的なユーザー体験を向上させています。しかし、これらのスクリプトは管理範囲外のため、金融サービス企業自身では、それらのコードの開発とテスト、および潜在的な脆弱性を把握できていません。それらの可視化ができていないと、攻撃者が悪性のスクリプトを使用して、ユーザーセッションへの介入、敵対的なコンテンツの挿入、データの奪取、ユーザーのブラウザーの乗っ取りを行う危険性があります。また、サードパーティースクリプトは他のサードパーティーのコードを使用する場合があり、それによって攻撃に悪用できる死角や経路が生まれる可能性があります。



当社のデータによると、APJ の金融サービス組織が使用しているスクリプトの 40% は、サードパーティーのスクリプトであり、これは、導入しているスクリプトの 42% がサードパーティーのものである他の業界とほぼ同じです（APJ 図 3）。サードパーティースクリプトは、その性格上、必ずしも悪意があるわけでも信頼性が低いわけでもありませんが、新しいセキュリティリスクを生む可能性があります。それに加えて、サードパーティースクリプトを使用していると、スクリプト管理に関する Payment Card Industry Data Security Standard（PCI DSS）v4.0 の要件を満たすうえでの課題が増える可能性もあります。

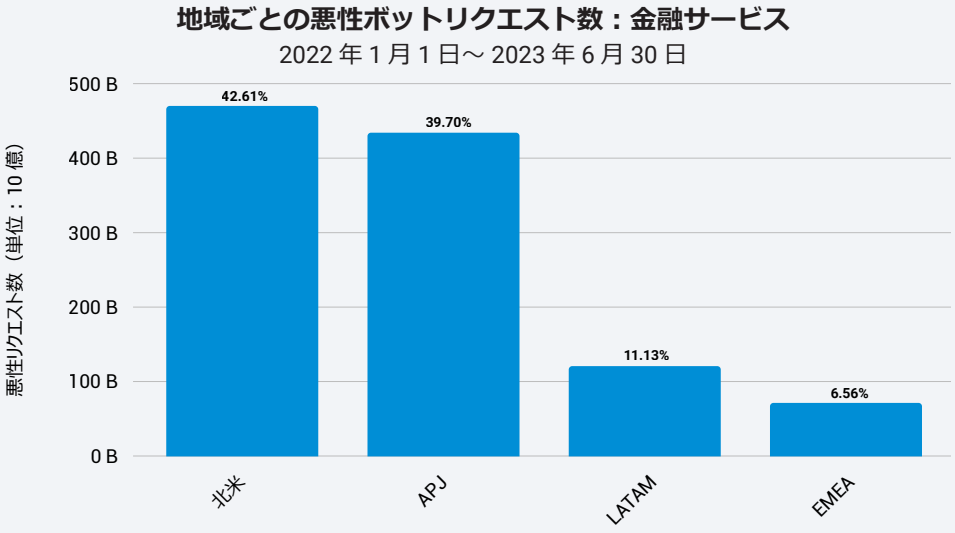


APJ **図 *3*：サードパーティースクリプトの利用率で見ると、金融サービス企業は他の業種とほぼ同等**

金融サービス業界に影響を与えている悪性ボットリクエストの件数を地域別に見ると、APJ は北米に次いでわずかな差で 2 位となっています。

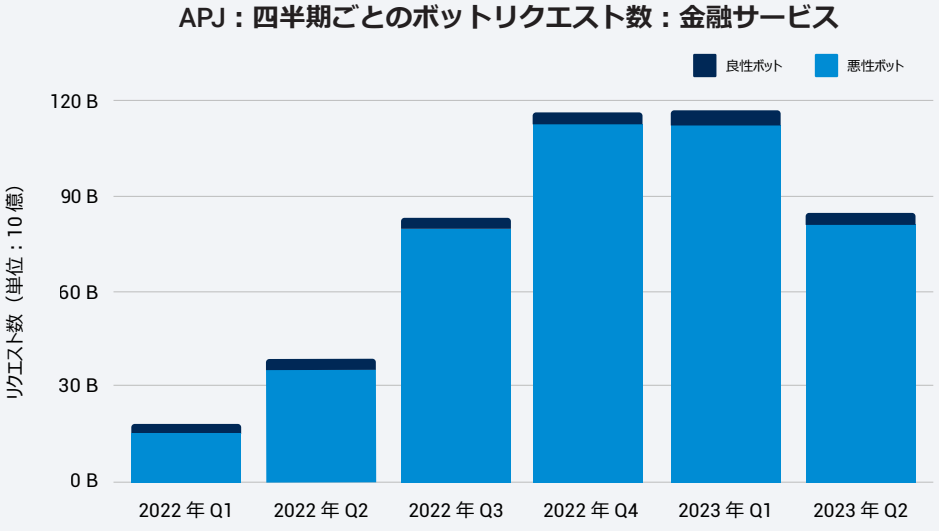
APJ では悪性ボットが多用されている

金融サービス業界に影響を与えている悪性ボットリクエストの件数を地域別に見ると、APJ は北米に次いでわずかな差で 2 位となっています（APJ 図 4）。悪性ボットは、攻撃者によって詐欺やなりすましなどの不正行為に使用されます。攻撃の例としては、金融サービス機関の Web サイトに似せたサイトでフィッシング詐欺を行う Web スクレイピングや、ユーザー名とパスワードを自動的に組み合わせてアカウントを乗っ取る Credential Stuffing などがあります。アカウントの詳細情報や個人の特定が可能な情報などの盗まれた情報は、ダーク Web で販売されたり、他の攻撃に利用されたりします。



APJ **図** *4*：APJ **は、***2* **番目に多く金融サービスに対する悪性ボットリクエストの標的にされている地域**

前回の金融サービスに関するレポートで報告した状況は依然として継続しており、現在の世界的な金融サービスのトレンドと一致しています。APJ では悪性ボットのトラフィックが 2022 年第 2 四半期と 2023 年第 2 四半期の前年同期比で 128% 増加しており、2022 年第 4 四半期に急増し、2023 年第 1 四半期に至るまでその状態が継続しています（APJ 図 5）。2022 年第 1 四半期から 2023 年第 2 四半期に至る 18 か月の間に、この地域で発生した悪性ボットリクエストの 13% が、金融サービスを標的にしたものでした。悪性ボットリクエストの標的となった地域のトップはフィリピンで 40.5%、次いで中国が 25.6%、オーストラリアが 10.2% となっています。



APJ **図** *5*：**悪性ボットリクエスト数は前年に比べて増加しており** *2022* **年下半期に急増**

APJ スナップショットの結論

金融サービスは、サイバー犯罪者の標的になることが最も多い業界の 1 つですが、同時に規制の厳しい業界でもあります。そのため、デジタルイノベーションと耐障害性を確保するための新しい法律、規制、ベストプラクティスに沿ったセキュリティ戦略を立てることが不可欠です。その分野固有の既存の規制に加えて、金融サービス業界は（オーストラリア、インド、シンガポールなどの管轄区域で見られるように）重要インフラに区分されることが次第に多くなっているため、規制当局の監督が厳しくなり、報告義務が増えています。

サイバーセキュリティに関する法規制を脅威の現況に合わせて最新の状態に維持できるように、多くの管轄区域で法改正が進められています。たとえば、インドでは、最近のデジタルの状況に合わせるために IT 法（2000 年に成立）を大幅に刷新する Digital India Bill を起草しているところです。この取り組みは、2023 年 8 月の Digital Personal Data Protection Act の可決が発端となって始まりました。オーストラリアでは、最新の脅威の状況に既存の法律では対応できないと政府がたびたび指摘しています。これに対処するために新しい法律の制定が重点的に検討されており、新しいサイバーセキュリティ法の導入、または既存の Security of Critical Infrastructure Act（重要インフラ保護法）の拡張が検討されています。これに加えて、近々リリースされる PCI DSS v4.0 では、2025 年 3 月 31 日までに、新しいスクリプト管理要件を満たすことも求められます。

規制当局が、サイバーセキュリティ基準を強化するためのイニシアチブとポリシーを打ち出す中、自社の地域における報告要件を把握して、プレイブックや危機管理計画にその要件を盛り込み、多層防御によってリスクを緩和する方法を認識することが重要です。

詳細については、世界的に金融サービスを調査した SOTI レポート「イノベーションに潜む高いリスク：金融サービス業界の攻撃トレンド」をご覧ください。

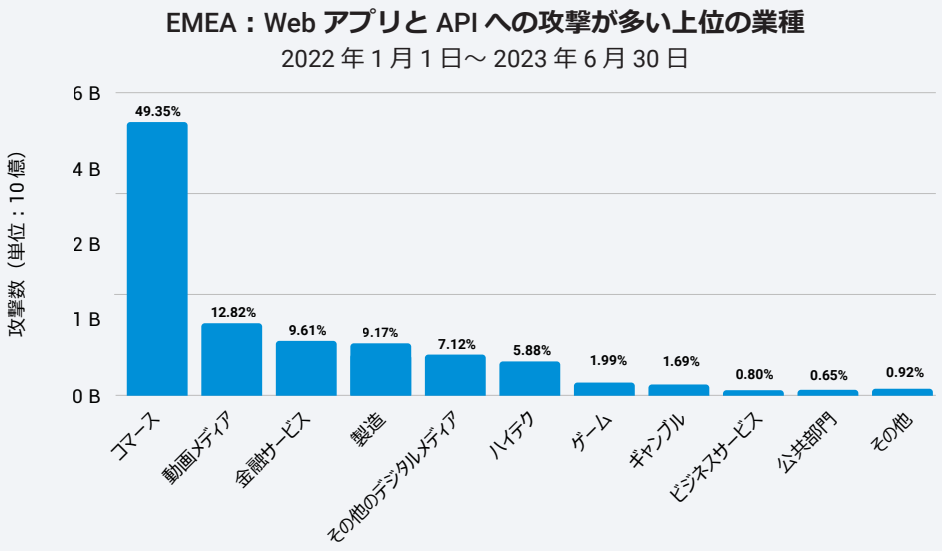
金融サービス業は重要インフラに区分されることが次第に増えており、規制当局による監督が厳しくなり、報告義務が増えています。

金融サービス：EMEA スナップショット

EMEA スナップショットは、当社の大手金融サービスに関する SOTI レポート「イノベーションに潜む高いリスク：金融サービス業界の攻撃トレンド」（本編は英語版のみ）の姉妹編として作成されたものです。これから説明する攻撃ベクトルを攻撃者がどのように利用するのかの詳細な説明、組織を保護するための推奨事項、当社の調査方法に関する説明については、同レポートを参照してください。

金融サービスに対する Web アプリケーションおよび API 攻撃は増加している

世界的な傾向に続き、金融サービス業界は、ヨーロッパ・中東・アフリカ（EMEA）地域で第 3 位の Web 攻撃の標的になっている業種は、依然として金融サービス業界であり、2022 年 1 月から 2023 年 6 月までの 18 か月の間に発生した Web アプリケーションと API への攻撃のうち、ほぼ 10% が EMEA で発生しています（EMEA 図 1）。これは、EMEA の全業種が受けた Web 攻撃の総数 11 億件のうち 10 億件に相当し、その件数は 2022 年第 2 四半期と 2023 年第 2 四半期の前年同期比で 119% も増加しています。



EMEA **図** *1* **：** *EMEA* **で攻撃の頻度が** *3* **番目に多かった業種は金融サービス**

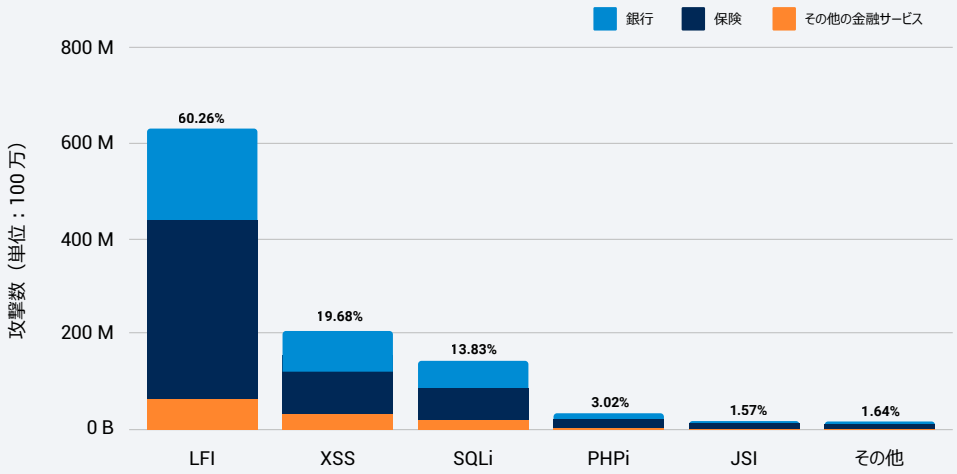
EMEA の金融サービス業界に対する Web アプリケーションと API 攻撃をさらに掘り下げて調べると、英国が 59.2% で最も多くの Web アプリケーション攻撃を受けています（昨年のレポートとも一致）。さらに、2022 年第 2 四半期と 2023 年第 3 四半期の前年比増加率を比較すると、英国がトップ（79%）となり、オランダ（16.2%）とドイツ（10.7%）が続いています。

上位の攻撃ベクトルと業種

前回の金融サービス SOTI レポートとともに、現在の世界的な金融サービスの傾向を見ると、ローカル・ファイル・インクルージョン（LFI）が EMEA の全業界における攻撃ベクトルの首位となっています（Web 攻撃の 60.26%、EMEA 図 2）。さらに、クロス・サイト・スクリプティング（XSS）が Web 攻撃の 19.66% で 2 位、SQL インジェクション（SQLi）が 13.83% で 3 位となっています。

EMEA：Web アプリケーションと API への上位の攻撃ベクトル：金融サービスの業種

2022 年 1 月 1 日～ 2023 年 6 月 30 日



EMEA **図 2：***LFI* **により、***EMEA* **の金融サービス業界で** *Web* **攻撃が急増していますが、***XSS* **や** *SQLi* **などの他のベクトルにもリスクがあります**

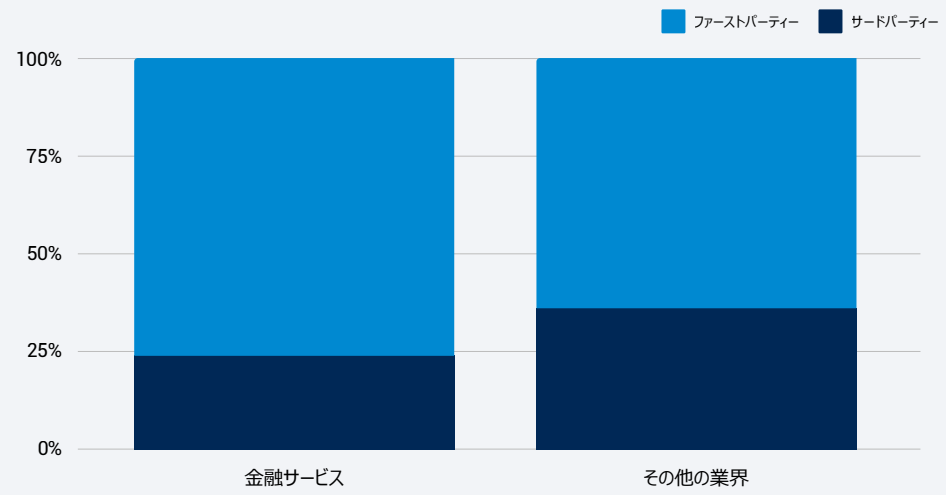
こうした攻撃ベクトルのランキングは EMEA 金融サービス業界全体でも一致しており、保険（全 Web 攻撃の 54.5%）と銀行（34.0%）に、他の金融サービス企業（フィンテック、資本市場、損害保険、決済会社および貸付会社など）が続いています（11.5%）。特に、2022 年第 2 四半期と 2023 年第 3 四半期を比較すると、保険業界の Web アプリケーションと API 攻撃数は 68% 増加しています。金融データを保有する銀行や他の金融サービス企業とは対照的に、保険会社は個人を特定できる情報を大量に収集するため、保険業は特に魅力的な標的となっています。こうした企業は、投資、債権、資本調達を通じて、さまざまな金融機関との豊富なつながりを持っています。最後に、地理的・政治的な情勢もこうしたリスクに影響します。国家規模の攻撃者は、ゼロデイ脆弱性の発見および悪用などのためにサイバー研究と開発にますますリソースを割くようになるでしょう。

保険業では、Web アプリケーションと API 攻撃数が前年比 68% 増となっています

サードパーティースクリプト – リスクと被害

オンラインバンキングが普及するにつれて、金融サービス企業は、サードパーティースクリプトを使用して、新しいサービスや機能を手早く増やして全体的なユーザー体験を向上させています。しかし、金融サービス企業はそのようなスクリプトをコントロールできないため、コードの開発やテスト、潜在的な脆弱性をほとんど可視化できません。また、サードパーティースクリプトは他のサードパーティーのコードを使用する場合があり、それによって攻撃に悪用できる死角や経路が生まれる可能性があります。

Akamai のデータによると、EMEA の金融サービス組織が使用するスクリプトの 24% はサードパーティー製であり、他業界と比較しても割合が低くなっています（36%、EMEA 図 3）。サードパーティースクリプトは、必ずしも悪意があるわけでも信頼性が低いわけでもありませんが、新しいセキュリティリスクを生む可能性があります。それに加えて、サードパーティースクリプトを使用していると、スクリプト管理に関する Payment Card Industry Data Security Standard（PCI DSS）v4.0 の要件を満たすうえでの課題が増える可能性もあります。サードパーティー製のスクリプトへの依存度が低い場合、金融機関のコンプライアンス負担が軽減されます。

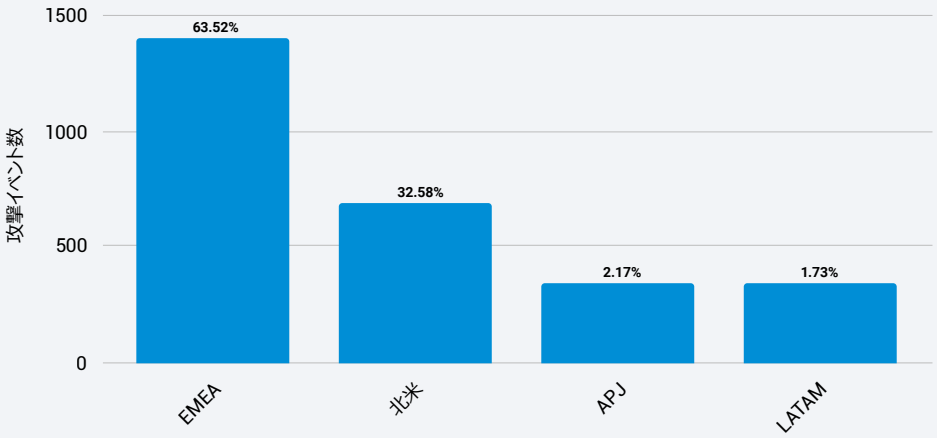


EMEA **図 *3*：金融サービス企業は他の業界よりもサードパーティースクリプトの使用数が少なくなっています**

EMEA は DDoS 攻撃の地域シフトの標的になっている

グローバルレポートで解説したように、金融機関は復活した分散型サービス妨害（DDoS）攻撃の矛先になっています。特に、EMEA で顕著です。地域として、EMEA は最多の DDoS 攻撃を受けており（63.52%）、その割合は 2 位の北米の約 2 倍となっています（32.58%、EMEA 図 4）。Akamai は、昨年のレポートでこの地域シフトについて検証を開始しました。その結果、米国に対する DDoS 攻撃が減少する一方で、EMEA に対する攻撃数は増加し、標的組織の全体数が少ないにもかかわらず、北米を上回っていることがわかりました。

地域ごとの DDoS 攻撃イベント数：金融サービス
2022 年 1 月 1 日～ 2023 年 6 月 30 日

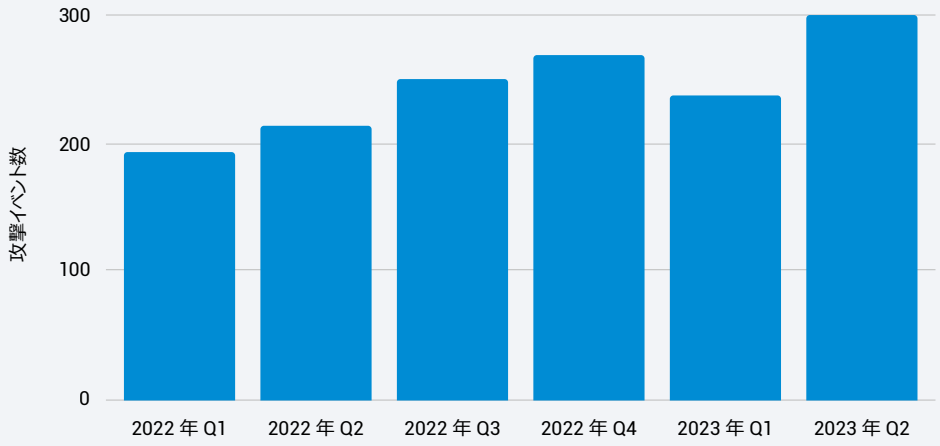


EMEA **図 4：*EMEA* は金融サービスに対する *DDoS* 攻撃が最も多い地域であり、*2* 位の地域のほぼ *2* 倍に達しています**

2022 年 1 月から 2023 年 6 月までの 18 か月間で、EMEA の金融サービス業界で発生した DDoS 攻撃数は増加傾向にあり、この地域の全攻撃の 57% が金融サービス業界を標的にしていました。これは、EMEA の全業種が受けた攻撃の総数 2,590 件のうち 1,466 件に相当し、2022 年第 2 四半期と 2023 年第 2 四半期で DDoS 攻撃数を比較すると、前年同期比で 40% 増加しています（EMEA 図 5）。

EMEA：DDoS 攻撃イベント数（四半期ごと）：金融サービス

2022 年 1 月 1 日～ 2023 年 6 月 30 日



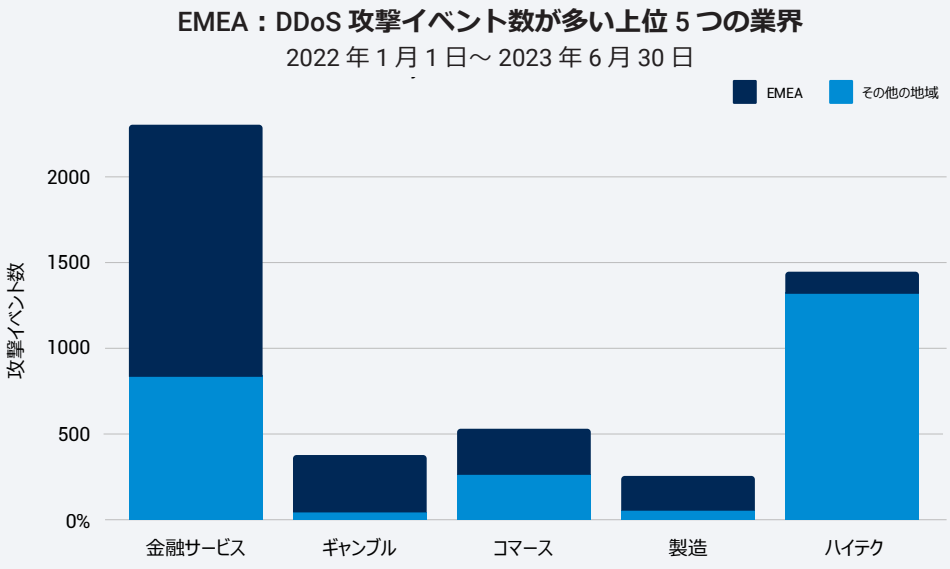
EMEA **図 *5*：金融サービスに対する *DDoS* 攻撃は増加傾向にあります**

この地域をさらに詳しく見ていくと、英国が DDoS 攻撃数の 29.2% で首位となり（前年比 154% 増）、ドイツが 15.1% で続いています。

ウクライナ側に賛同するヨーロッパの銀行を標的とした攻撃は、いまだ続くロシアのウクライナ侵攻の経済的・政治的な動機によるものであり、EMEA における攻撃数の増加の主な理由だと推測されます。たとえば、親ロシアのハクティビズムグループは、6 月初めにヨーロッパと米国の金融組織を標的とした「大規模」な組織的 DDoS 攻撃を仕掛けると発表しました。これらの攻撃グループには、Killnet、REvil、Anonymous Sudan が含まれます。

EMEA は金融サービスに対する DDoS 攻撃イベントが最も多い地域です

金融サービスに対する DDoS 攻撃の地域シフトは、攻撃者の標的の切り替えの速さを示しています。しかし、このコンテキストでは、この地域の他の業界への影響を考慮することも重要です。攻撃者は金融組織を主な標的にすると表明していますが、さらに分析を進めると、EMEA のギャンブル、コマース、製造業界に対する DDoS 攻撃も、他のすべての地域の合計数を超えていることが明らかになりました（EMEA 図 6）。



EMEA **図** *6*：*EMEA* **は** *4* **つの業界だけで他の地域の合計より多くの** *DDoS* **攻撃を受けています**

EMEA スナップショットの結論

金融サービスは、サイバー犯罪者の標的になることが最も多い業界の 1 つですが、同時に規制の厳しい業界でもあります。そのため、デジタルイノベーションと耐障害性を確保するための新しい法律と規制に沿ったセキュリティ戦略を立てることが不可欠です。EU の金融セクターは、2025 年 1 月 17 日に発効するデジタル・オペレーショナル・レジリエンス法（DORA）の準拠に備える必要があります。DORA は、金融セクターの企業および組織、ならびに情報・通信技術関連サービス（クラウドプラットフォームやデータ分析サービスなど）を金融セクター組織に提供する主要サードパーティーのネットワーク・情報システムのセキュリティに対する統一要件を設定するものです。これは、2024 年 10 月 17 日に発効する新しいネットワークおよび情報システム指令（NIS2）に続く法律です。EU 以外の各国、たとえばサウジアラビアなども、EU の一般データ保護規則（GDPR）に類似したデータ保護法を導入しており、金融機関による個人データの取り扱いを規制しています。これに加えて、近々リリースされる PCI DSS v4.0 では、2025 年 3 月 31 日までに、新しいスクリプト管理要件を満たすことも求められます。

規制当局が、サイバーセキュリティ基準を強化するためのイニシアチブとポリシーを打ち出す中、自社の地域における報告要件を把握して、プレイブックや危機管理計画にその要件を盛り込み、多層防御によってリスクを緩和する方法を認識することが重要です。

詳細については、世界的に金融サービスを調査した SOTI レポート「イノベーションに潜む高いリスク：金融サービス業界の攻撃トレンド」をご覧ください。

結論：実用的な知見で防御を強化

金融サービスは、常に最も攻撃を受けている業界の 1 つです。金融サービス業界は、引き続き Web アプリケーションおよび API 攻撃では 3 位、フィッシングでは 1 位にランクしていますが、今年は DDoS 攻撃でも 1 位になっています。この業界は、新旧のセキュリティ脅威の標的になっており、拡大するアタックサーフェスをいかに効果的に防御するかという課題に引き続き取り組んでいます。攻撃の範囲が拡大し、技術面の革新が進む中で、今年も金融サービス組織は顧客を確実に保護し続けています。

業界は革新を継続し、API をさらに活用した顧客アクセスを提供していますが、可視性の確保と緩和の自動化に注力する必要があります。シャドー API とアクセス制御回避攻撃が増加する一方で、管理されていない API（顧客に表示されるものと社内用の両方）をすばやく検知し、攻撃または悪用について監視し、インシデントの調査プロセスを確立し、緩和ポリシーを自動化しなければなりません。

アカウントの乗っ取り、金融アグリゲーター、Web スクレイピング、フィッシングなどについても、同様の方法で可視性を確保して対応することが推奨されます。こうしたエッジに面した問題は、OWASP Top 10 および MITRE ATT&CK フレームワークを活用した、レッドチーム／侵入テストグループ向けのトレーニングプログラム、成熟度ベースライン測定、テスト計画の作成に適した分野です。ATT&CK Navigator ツールを使用して、特定の脅威に基づいてパープルチームを結成することもできます。（パープルチームは、セキュリティを強化する目的で組織の境界内のセキュリティ上の弱点を見つけるために、シミュレーション攻撃を実行します）。

サイバー犯罪者と規制当局の両方から関心が高まっているもう 1 つの領域として、スクリプト環境があります。この領域はこれまでリスクレジスターの上位に位置付けられていませんでしたが、最近リリースされた PCI DSS v4.0 に準拠して危機を防ぐために、適切な制御を早めに導入する必要があります。また、法務部門と緊密に連携して、耐障害性などの領域に関する新たな規制に対応するポリシーを更新する必要もあります。

DDoS は依然として主要な脅威ベクトルであるため、レイヤー 3 ／ 4、ならびにレイヤー 7 攻撃に対する最新の計画を策定する必要があります。プレイブックの検証や、規模とスピードの両方に関する攻撃のトレンドの追跡を行い、現在の機能に基づいてリスクを評価します。また、技術演習を実施するきっかけを決めておくのも効果的です（通常は、過去 3 四半期に攻撃を受けたことがなければ、実戦的な演習を行います）。

顧客や Web サイトに関する情報を収集し、最終的にフィッシングサイトを開設する Web スクレイパーを検知して速やかに対応することが重要です。これを実現するためのツールとサービスは数多くあり、ソリューションを開発する際には不正防止チームと協力することが重要です。

このレポートは、Akamai が阻止する脅威トラフィックと、お客様から学んだベストプラクティスの両方に基づいています。それらの知見が ROI やリスクに関するパートナーとの話し合いに役立てられ、また、データに基づいた効果的かつ戦術的なアプローチによって企業と顧客が脅威から守られることを願っています。

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。

手法

Web アプリケーション攻撃とボット攻撃

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）とボット管理ツールを通じて観測されたトラフィックに関するアプリケーションレイヤーのアラートです。保護されている Web サイトやアプリケーションへのリクエスト内に悪性のペイロードを検知した場合に、Web アプリケーション攻撃アラートが作動します。保護されている Web サイトやアプリケーションへのリクエスト内にボットのペイロードを検知した場合に、ボットアラートが作動します。このボットアラートは、悪性ボットと良性ボットのいずれによっても作動されます。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。

2022 年 1 月 1 日～ 2023 年 6 月 30 日までの 18 か月間のデータを使用しています。2022 年 5 月に発生した大規模な攻撃は、ボリュームがあまりに膨大であるため、Web アプリケーション攻撃を可視化する際に除外されている場合があります。分析目的のすべてのデータセットには含まれています。

Client-Side Protection & Compliance に関するデータ

このデータは、Akamai Client-Side Protection & Compliance ツールで観測、分析したスクリプトに基づいています。Client-Side Protection & Compliance（旧 Page Integrity Manager）はブラウザー内で稼動し、保護対象の Web ページにある、ブラウザー内で実行されたあらゆるスクリプトを観測します。このツールは毎日、180 億以上のスクリプトを監視し、約 100 億の Web ページを保護しています。Akamai のセキュリティチームはこのデータを利用してスクリプトの脆弱性を調査し、悪性のふるまいを検知して、インテリジェンスを Akamai の他のセキュリティソリューションに取り入れます。

本レポートのために当社が分析した Client-Side Protection & Compliance のデータは、2023 年の第 2 四半期から第 3 四半期にかけて収集したデータの 90 日間分のサンプルです。

DDoS

Prolexic Routed は、Akamai スクラビングセンターを経由してネットワークトラフィックをリダイレクトし、クリーンなトラフィックのみを通すことで、DDoS から組織を守ります。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。

DDoS 攻撃イベントは、選択された展開モデル（Always-on またはオンデマンド）に応じて、SOCC または標的組織自体によって検知されますが、SOCC は緩和されたすべての攻撃のデータを記録します。Web アプリケーショントラフィックと同様、発信元は Akamai ネットワークに入る前の IP トラフィックの発信元から判断されます。

2022 年 1 月 1 日～ 2023 年 6 月 30 日までの 18 か月間のデータを使用しています。

Client Reputation

Akamai Client Reputation は、Akamai App & API Protector の一部であり、Akamai ネットワークのすべての IP について 10 段階でリスクスコアを計算します。リスクスコア 1 の場合は、そのクライアントによる将来的な攻撃の可能性が低いと予想されます。リスクスコア 10 の場合は、その IP アドレスが攻撃者に使用される可能性が高いと予想されます。

スコアをまとめる際に、Client Reputation は Akamai のすべてのフィードとデータを利用します。フィードやデータには、攻撃トラフィック、WAF トリガー、レートコントロール、ボット検知、通常（良性）トラフィックなどがあります。Client Reputation は、各顧客のコンテキストに合わせてスコアを IP に割り当てることができます。このスコアは顧客本人にしか表示されず、他者は見ることができません。Client Reputation は、スコアを顧客セグメント全体や、業界全体（金融サービスセグメントなど）に割り当てることもできます。この場合、スコアは顧客セグメント全体に表示されますが、他のセグメントに対しては非表示になります。

このレポートのデータは、2023 年 5 月 1 日から 2023 年 7 月 31 日の Client Reputation データで生成されており、以下のいずれかのコンテキストで絞り込んだ IP に割り当てられたスコアのみを取得しています。

- 金融サービスの利用者
- 金融サービスセグメント全体

このアプローチにより、金融サービスの利用者に対する明確な攻撃の構図を正確に把握できます。

クレジット

共同執筆者

Yossi Barkshtein
Cheryl Chiodi
Chen Doytshman
Ryan Gao
Karan Mankodi
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Steve Winterfeld

校閲およびテーマ別寄稿者

Tom Emmons
Or Katz
Reuben Koh
Emily Lyons
Gal Meiri
Richard Meeus
Matthew Payne
Maxim Zavodchik

データ分析

Chelsea Tuttle

マーケティング・出版

Georgina Morales Hampe
Shivangi Sahu
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 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

金融サービスをターゲットとする脅威に対抗する Akamai ソリューションの詳細については、**金融サービス CDN ページ**をご覧ください。