SOTI

第 10 巻、第 4 号

10 YEARS
OF SECURITY INSIGHT

包囲されるデジタル要塞

現代アプリケーションアーキテクチャを狙う脅威

Akamai

インターネットの現状／セキュリティ

目次

はじめに

過去 20 年間にわたり、Web アプリケーションは数と機能の両面で飛躍的に成長を遂げており、リアルタイムのコミュニケーション、データ分析、プロセス自動化などの機能を通じて業務処理を効率化し、顧客体験を向上させ、成長を促進してきました。API はアプリケーション間通信の基盤として浸透し、今や指数関数的に増加しようとしています。

それを後押ししたのは、マイクロサービスやクラウドコンピューティングの普及、システムやサービス間の連携の必要性、そして、近年の人工知能（AI）機能の急速な普及です。現在では、アプリケーションと API のセキュリティは、あらゆる戦略的防御の要となっています。

しかし、このような戦略的な要件を満たそうとすると、事が複雑化しがちです。

アプリケーションは、ビジネスのほぼあらゆる側面で実行され、何兆もの接続を容易にします。しかし、同時に攻撃に対する脆弱性も増します。このような何兆もの接続を保護するためには、ネットワークやビジネスのどの部分に、誰がアクセスできるようにしているのか、サーバー間のワークフローがどのようにアクセスされ、検証されているのかに注意を払う必要があります。インターネットトラフィックの大勢を占めるボットやボットネットも、優先的に注意する必要があります。その多くが、安全性が疑われる用途に使用されているためです。

そこで私たちは、この「インターネットの現状（SOTI）」脅威インテリジェンスレポートのテーマを Web アプリケーション戦略にすることにしました。当社のデータ分析は、皆様の組織のアプリケーションセキュリティ戦略にとって価値のある羅針盤になることを目指しています。現行のアプローチが何であれ、将来的なセキュリティ制御を戦略的に優先付け、実装するうえで当社の知見が何らかの参考になればと考えています。

このレポートに記載している指針は、デジタルイノベーションの重要なプロセスを阻害することなく、保護を強化することを目的としたものです。両方のバランスを取ることができれば、急速に進化している今日のデジタル情勢にあって競争力の維持に必要なアジリティを維持しながら、アプリケーションのセキュリティを向上させることができます。

本レポートの主要な知見

アプリケーションと API に対する Web 攻撃は、2023 年第 1 四半期から 2024 年第 1 四半期にかけて 49% 急増しました。需要が一気に増加したアプリケーションと API は、セキュリティギャップを悪用し、標的の貴重なデータに対するアクセス権限を不正に得ようとしている攻撃者にとって利益の出やすい標的となります。

108B 攻撃

2023 年 1 月から 2024 年 6 月にかけて 1,080 億件の API 攻撃が記録されました。組織にとって目に見えないゲートウェイとして機能するこの重要なデジタルインターフェースに対して執拗に攻撃を受けると、データ窃取、ブランドの評判の低下、規制当局の罰金につながる可能性があり、高額な金銭的損失が発生しかねません。

データやサービスへのアクセスを API に頼っている企業にとって、API の悪用は大きな懸念事項になっており、それは、データ漏えい、不正アクセス、分散型サービス妨害（DDoS）攻撃など、さまざまな形で現われます。

コマース業界は Web アプリケーションおよび API 攻撃の被害を最も多く受けており、攻撃数は他のどの業界と比べて 2 倍以上多くなっています。

DDoS 攻撃は、レイヤー 3 および 4 とレイヤー 7 のあらゆるポートとプロトコルのトラフィックを妨害します。これには、ドメイン・ネーム・システム（DNS）も含まれます。Akamai の研究者によると、過去 18 か月のレイヤー 3 および 4 DDoS 攻撃イベントの 60% を DNS が占めていました。

11T 攻撃

Akamai の研究者によると、アプリケーションレイヤー DDoS 攻撃の上位 3 位の業界はハイテク、商業、ソーシャルメディアであり、わずか 18 か月の間に 11 兆件以上（攻撃の 75%）の攻撃が発生しました。

絡み合う脆弱性：アプリケーションと API のセキュリティリスクを深く掘り下げる

2023 年には複層的な Web 攻撃で API と Web アプリケーションが標的となりました。サイバー犯罪者が、この急成長している API エコノミーを新しい攻撃手法として悪用したためです。ある米国の通信会社のデータ漏えい事件では、API の認可の脆弱性を攻撃者に悪用された結果、3,700 万件の顧客記録データが流出しました。新しい攻撃手法をいち早く採用する CL0P のようなランサムウェア集団は、Web アプリケーションの脆弱性も組織への攻撃に悪用します。

本レポートの対象期間（2023 年 1 月から 2024 年 6 月まで）に、Web アプリケーションおよび API を標的にした Web 攻撃の頻度が大幅に増加していることが Akamai の調査で判明しています。2023 年初めに検知した攻撃数は月間 140 億件ほどでしたが、2024 年 6 月には月間 260 億件以上にまで攻撃数が増加しています（図 1）。つまり、2023 年第 1 四半期から 2024 年第 1 四半期にかけて、Web 攻撃数が 49% 増加したことになります。

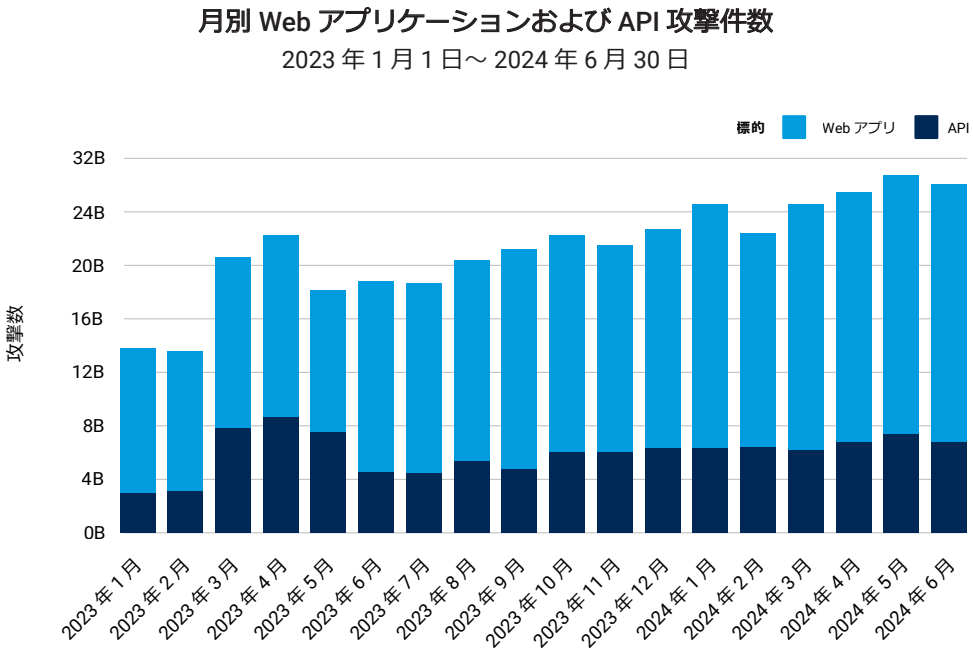
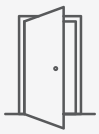


図 *1*：*Web* アプリケーションおよび *API* を標的にして、従来形の *Web* 攻撃を行う攻撃者数の増加が、前年比 *49%* 増という数値に表れている

メディアの関心の中心は引き続きゼロデイ攻撃ですが、攻撃者がネットワークに侵入する手段はそれだけではありません。パッチの未適用による脆弱性は、数年前から放置されているものもあり、依然として攻撃者の侵入口となります。2024 年 6 月には、Akamai の研究者により、CVE-2018-20062 および CVE-2019-9082 という脆弱性を持つ ThinkPHP アプリケーションを標的にしたキャンペーンが発見されました。この脆弱性は少なくとも 2018 年から野放しになっており、組織によってはパッチを適用していないため、今でも攻撃活動が続いています。

直近数か月に発生して注目を集めたいくつかのデータ漏えいには、API の悪用または API の脆弱性の悪用が関係しています。このことは、この必要不可欠なデジタルインターフェースがますます攻撃者の標的になりつつあることを示しています。

サイバーセキュリティ組織が発する主なアドバイスはパッチ管理の優先化ですが、いまだにパッチ管理手順の実施に悪戦苦闘している企業は多くあります。アプリケーションおよび API 保護ソリューションとマイクロセグメンテーションを使用すれば、パッチを適用できるようになるまでの間、悪用しようとする動きと、組織がその影響を受ける可能性を大幅に緩和することができます。このようなソリューションを使用すると、すぐにパッチを適用できなくても、重要な役割を担う防御層で脆弱なシステムを囲い込むことで、悪性のトラフィックから守ることができます。



パッチの未適用による脆弱性（中には数年前から放置されているものもある） は、 攻撃者にとっては依然として侵入口となります。

LFI、XSS：攻撃者が好む攻撃方法

当社のデータによると、ローカル・ファイル・インクルージョン（LFI）、クロスサイトスクリプティング（XSS）、SQL インジェクション（SQLi）、コマンドインジェクション（CMDi）、サーバーサイド・リクエスト・フォージェリー（SSRF）攻撃は、ビジネスアプリケーションと API を標的とするベクトルとして依然よく見られます。これらの攻撃手法は、Web アプリケーションや API によく見られる脆弱性を悪用するうえで効果的であるため、根強く残っています。このような脆弱性は、入力値の検証が不十分だったり、セキュリティ設定が不適切だったりする場合によく発生します。たとえば、LFI は、2023 年第 1 四半期から 2024 年第 1 四半期にかけて 120% 増加しています（図 2）。同様に、SQLi 攻撃と CMDi 攻撃も 25% 増と大きく増加しています。これらが攻撃ベクトルとして広く利用されているのは確かですが、重要なことを指摘しておくと、サイバー犯罪者の変わり続ける手口に対応するために Akamai も脅威検知機能を継続的に進化させています。

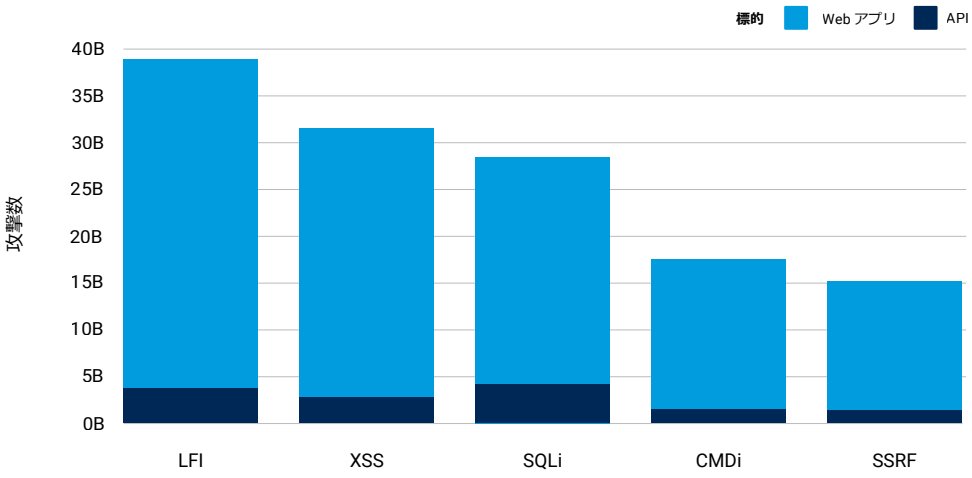


図 2：*LFI*、*XSS*、*SQLi* の各ベクトルが従来の *Web* 攻撃の増大を後押し

LFI、XSS、SQLi の各攻撃は、Web アプリケーションの設計や開発の慣行にある根本的な弱点を突くため、長年にわたって成功してきました。このような脆弱性に対する認識は高まっているにもかかわらず、開発サイクルの短期化、レガシーなコードメンテナンス、不十分なセキュリティテストなどが原因で、新しいアプリケーションにも依然としてこのような脆弱性が生まれ続けています。

それに加えて、最新の Web アプリケーションは複雑化し、API が幅広く使用されるようになっているため、アタックサーフェスが拡大し、このような定番の手口を攻撃者が活用できる機会が増えています。

2024 年 2 月に、ResumeLooters という名前の攻撃グループが、SQLi と XSS の脆弱性を悪用し、莫大な数の小売企業や求人情報の Web サイトを標的に攻撃を仕掛けました。その攻撃の影響を受けたのは主にアジア太平洋地域のユーザーです。報告によると、このキャンペーンで、200 万以上の E メールアドレスと 210 万以上のユーザーデータの記録が流出しています。さらに、攻撃者は盗んだ情報を Telegram チャネル経由で売りつけようとしました。

組織がクラウドサービスやマイクロサービスアーキテクチャへの依存度を高めるにつれ、SSRF のような新しい攻撃ベクトルが目立つようになっています。このような攻撃は、社内システム間の信頼関係を悪用し、従来のセキュリティ制御を迂回するため、現代の分散環境では特に危険です。

ここ最近の Web アプリケーションは複雑化し、 API が幅広く使用されるようになったため、 アタックサーフェスが拡大し、 このような定番の手口を攻撃者が活用できる機会が増えています。

業界動向：コマース業界における Web 攻撃の着実な増加

2023 年度 SOTI レポート「セキュリティギャップのすり抜け ： 組織を狙うアプリケーションおよび API 攻撃の増加」の主旨と一致する現象が起きており、2023 年 1 月から 2024 年 6 月にかけて、コマース業界の組織は、最大件数の Web 攻撃（1,640 億件）を受けています。これは、ハイテク業界（590 億件）の 2 倍以上の攻撃です（図 3）。

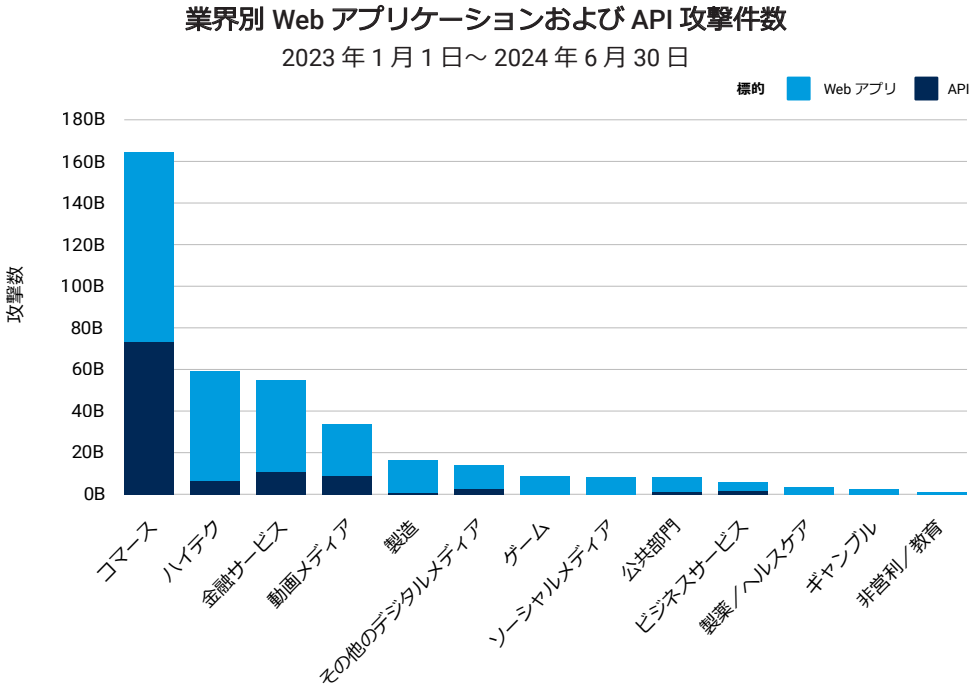


図 *3*：*Web* アプリケーションおよび *API* 攻撃の影響を受ける業種の上位はコマース、ハイテク、金融サービス

コマース業界の攻撃件数が最上位になり続けている要因として、次の 2 つが考えられます。まず、この業界の組織が、Web アプリケーションや API に大きく依存していることです。次に、市場投入のスピードが要求されるため、コマース組織によっては、新しい Web アプリケーションの導入時に、十分な保護ソリューションを準備できないところがあることです。この 2 つの要因が重なって、コマース業界はサイバー犯罪者にとって確実性が高く、利益の出やすい標的になり続けているのです。

3 番目に Web 攻撃が多い業界は金融サービス業であり、レポート対象期間の間に 550 億件の Web 攻撃が記録されています。この分野の企業は攻撃を受けると、利用者の口座情報の漏えいにつながる可能性があるため、組織にとっても顧客にとっても特に大問題になる傾向があります。このことで、Credential Stuffing やその他の形態の不正利用が発生する可能性が組織のアプリケーション全体に広がっています。

製造業も Web アプリケーションおよび API 攻撃の被害を受けており、今年の順位は第 5 位になっています。製造業は、コマース業界と異なり、あまり顧客と接することはありませんが、モノのインターネット（IoT）の利用やデータ共有が増えているため、このような攻撃の格好の標的となります。

API における攻撃トレンド

2024 年 3 月に Akamai の研究者は、攻撃者が API を標的にする際に使用する攻撃タイプを分析したレポートを発表しました。このレポートでは、ランタイムとポスチャの課題を特定し、安全性を向上させるために組織が API セキュリティのどの部分に力を入れるべきかを示しています。

データを調査したところ、懸念となる傾向が明らかになりました。それは、API が標的になる頻度が高くなっていることです。攻撃数が一貫して増え続けていることがそれを如実に表しています（図 4）。2024 年の上半期だけで、Akamai は 400 億件の API 攻撃（前年同期は 350 億件）を観測しています。API が侵害されると、機密性の高い情報への不正なアクセスが可能になり、さまざまな影響を与える恐れがあります。その代表的な例がデータ窃取や詐欺です。しかし、API 攻撃が成功した場合の影響はデータ損失にとどまりません。顧客からの信頼の失墜、ブランドや評判の低下、さらにコンプライアンスの問題にまで発展する可能性があります。

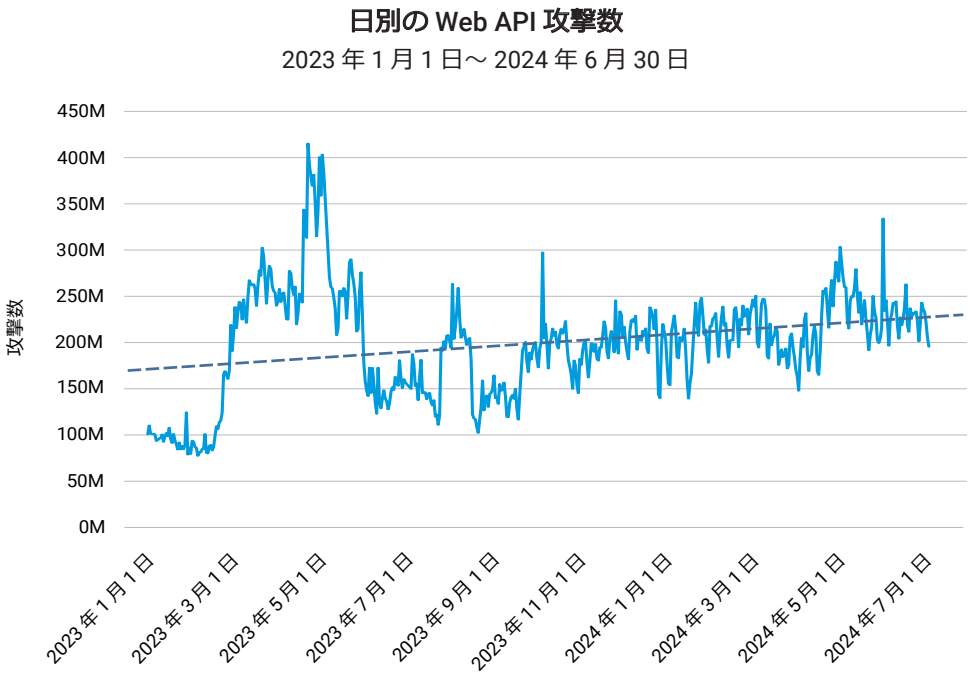


図 *4*：レポート対象期間全体で見ると、過去 *12* か月にわたって *API* 攻撃は数度の顕著な急増を繰り返しながら、着実に増加

API が侵害されると、 機密性の高い情報への不正なアクセスが可能になり、 さまざまな影響を与える恐れがあります。その代表的な例がデータ窃取や詐欺です。

API 攻撃に対する防御が困難な理由としては、次の 2 つの要因が考えられます。

1. 市場投入までの時間の短縮を求めるプレッシャーにより、開発リソースとセキュリティリソースの両方に過度の負担がかかります。それにより、導入後のアプリケーションの保護に必要なセキュリティプロセス、プロセス手順、ソリューションが見過ごされがちです。適切なセキュリティ対策が施されていないアプリケーションは、弱点を常に見張っている攻撃者にすぐに見つかり、悪用されます。それに加えて、安全でないコーディングから脆弱性が生まれる可能性があり、これもサイバー犯罪者の格好の標的になります。

2. 多くの組織のセキュリティチームは、API 環境の規模、スピード、複雑さに特有の課題に直面します。多くの企業は、API フットプリントを組織横断的に可視化できていないため、全体的なセキュリティの状況を完全には把握できていません。侵入者をネットワークに侵入させないためには、すべてのアタックサーフェスを網羅的に把握することと、そのアタックサーフェスを保護するためにセキュリティ対策を講じることの両方が非常に重要になります。特に配慮すべき事項は、文書化されていない API やシャドウ API を把握することと、機微な情報を外に出すアプリケーションの特定と優先付けを行うことです。

ビジネスロジック悪用への対抗策

API のセキュリティ確保には、設計上の欠陥を修正するだけでない包括的なアプローチが必要であり、Web アプリケーションも含めて社内システムと社外システムの両方をカバーする必要があります。ビジネスロジックの悪用は、検知と防止が特に困難です。このタイプの攻撃では、正当なアクセスを悪用して API に侵害することが多いためです。API の悪用では、承認された接続や認証情報を利用するユーザーや処理が起点となるため、攻撃がさまざまな形を採り得ることに注意する必要があります。

ロジックの悪用に対抗するためには、組織は API を継続的に監視し、API のふるまいの変わり方を継続的に学習し、それに適応できるようにする必要があります。それが可能になったら、次のような包括的なセキュリティ戦略を実施する必要があります。

- ビジネスロジックとアプリケーションのワークフローを事細かく把握する
- 悪用され得るケースを特定するために脅威のモデリングを徹底的に行う
- 強固な API セキュリティ対策を講じ、シャドウ API を含むすべての API の可視性を維持する
- ふるまい分析と AI を使用してビジネスロジックの悪用を検知し防止する高度なセキュリティソリューションを導入する

強固な包括的な API セキュリティ対策を講じる

強固な API セキュリティを確保するためには、多面的なアプローチが不可欠です。まず、不正な API やシャドウ API の増加を最小限に抑えるために、包括的なインベントリ管理と検知メカニズムを実装することが必要です。次に、Open Web Application Security Project （OWASP） Top 10 API セキュリティリスク （リンク先英語のみ） に関連するリスクを緩和するために、厳格なコーディング標準を確立、徹底させることが重要です。

このようなセキュリティ対策の検証は、脆弱性評価ツールとセキュリティ対策テストツールを使用して実施するべきです。業務システムについては、潜在的な脅威の検知と対応を専門とするチームに任せることをお勧めします。そのチームには、LFI や SQLi などの従来の攻撃ベクトルだけでなく、認証の不備、機密性の高い業務フローに対する制限なしのアクセスのような API 特有の脆弱性にも対応できる能力が必要です。

特に、悪用される可能性がある API を特定するためにユーザーアクティビティの監視を実施することが非常に重要です。このようなセキュリティ対策はすべて、セキュリティインシデントが発生したときに備えて、速やかな緩和戦略と効率的な報告メカニズムで補う必要があります。最後に、すべての環境にわたってアタックサーフェスを最小限に抑えるプロアクティブなアプローチを採用し、API インフラの全体的なリスクを減らすことが極めて重要です。

セキュリティの注目点：
モバイルアプリの細則はざっとではなく、よく読んで確認すること

モバイルアプリのユーザー契約では、ほとんどの場合、ユーザーはよく内容を確認せずに契約に同意します。しかし、アプリによっては、アプリが提供するサービスと引き換えに、ユーザーが自分のデバイスがモバイル・プロキシ・ネットワークの一部になることに同意する旨を細則に掲載しているものもあります。モバイルプロキシとは、モバイルデータを使用してプロキシサーバー経由でインターネットに接続するための携帯端末（スマートフォンやタブレットなど）のことです。

プロキシサービスのインストールは任意であり、モバイルアプリのユーザーの中には、自分のデバイスをそのようなネットワークに登録して帯域幅と引き換えに金銭的な見返りを受けている人もいます。

しかし、一部のアプリは、ユーザーが知らないうちに、モバイルデバイスやその他の住宅用 IoT デバイスを自動的に、プロキシネットワークのノードに変換します。これは、アプリ開発者がアプリケーションのもともとの機能の一部として組み込んだ場合もあれば、攻撃者が悪意を持ってインストールしたマルウェアが引き起こしている場合もあります。悪意のある変換が行われた場合、攻撃者がユーザーから帯域幅や機密性の高い情報を盗む可能性があります。

自社のモバイルソフトウェア開発キット（SDK）をゲームアプリケーションに組み込むようゲーム開発者にインセンティブを提供しているデータ抽出企業もあります。SDK とは、モバイルアプリの開発、更新を支援するツールの集合体のことです。この SDK により、ゲームスタジオは、アプリの実行時にデバイスをプロキシネットワークに登録するのと引き換えに、広告なしのゲーム体験やプレミアムなゲーム体験をユーザーに提供できるようになります。ユーザーが Web データの収集に自分のデバイスを参加させることに同意すると、SDK がアプリのバックグラウンドで実行されていたとしても、デバイスはプロキシとしてアクティブなままになる可能性があります。

モバイルアプリのユーザーにとって、アプリをよく調べ、そのアプリに関連する契約をよく理解することは極めて重要です。幸い、ほとんどの正規アプリは、ユーザーの認識も同意もない状態でデバイスをプロキシとして使用することはありません。さらに、アプリが安全かどうかを確かめるにはいくつかの方法があります。その方法には、次のようなものがあります。

- **アプリのプライバシーラベルを確認する：** Apple と Google Play は、デベロッパーにデータ収集方法を開示するように求めています。その中にはプロキシ使用に関する具体的な言及はありませんが、アプリがネットワーク接続をどのように処理しているかの手掛かりにはなります。
- **アプリの説明を読む：** 一部のアプリ、特にネットワークテストや VPN サービスを目的としているものは、その説明の中でプロキシ関連の機能について言及していることがあります。
- **ユーザーの意見を確認する：** 評価やレビューのセクションに、予期しないネットワークのふるまいやプロキシの使用に関する言及がないか確認します。
- **セキュリティ機能を確認する：** 証明書のピン留めなどのセキュリティ対策を実装しているアプリは、プロキシ接続を許可する可能性は低いと考えられます。このような対策で中間者攻撃を検知し、防ぐことができるからです。

いかなる場合でも、ユーザー契約に同意する前によく読むことが賢明な対策です。

アプリケーションとその支えとなっているインフラの防御

アプリケーションのインフラの防御に関して、セキュリティチームはファイアウォール、パッチ管理、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を考慮する必要があります。

DDoS はサイバー犯罪者が好んで使用する攻撃タイプの 1 つです。DDoS 攻撃は、ファイアウォール、ネットワーク、サーバーを標的とし、インフラやアプリケーション自体の脆弱性に付け入ろうとします。この攻撃は、DNS のような、レイヤー 3、4 および 7 のポートやプロトコルを介してトラフィックを送り込もうとするため、このレイヤーに適切な保護対策を講じることが不可欠になります。

アプリケーションに影響を与える DDoS 攻撃を大きく分けると、インフラ型とアプリケーション型の 2 つに分かれます。

1. インフラ型の DDoS 攻撃は、オープンシステム相互接続（OSI）モデルのネットワーク（レイヤー 3）レイヤーとトランスポート（レイヤー 4）レイヤーのプロトコル（伝送制御プロトコル（TCP）や User Datagram Protocol（UDP）トラフィックを含む）に狙いを絞った最も歴史の長い攻撃です。レイヤー 3 と 4 の攻撃は、ボリューム型の DDoS 攻撃になることが多く、その攻撃としては、SYN フラッド攻撃、スマーフ DDoS 攻撃、DNS 増幅攻撃またはリフレクション攻撃、UDP フラッド攻撃、ICMP フラッド攻撃などがあります。標的がさまざまな場所に跨る、複雑で巧妙な手口の DDoS 攻撃を仕掛けるために、攻撃者が複数の攻撃タイプや攻撃ベクトルを組み合わせるパターンが増えています。そのため、自動化と機械学習を使用して損害を未然に防げるよう、堅牢で包括的な DDoS 防御プラットフォームを用意する必要があります。

2. アプリケーションレイヤー（HTTP レイヤー／ Web トラフィックレイヤー）型の DDoS 攻撃も増加傾向にあり、攻撃者がよく使う手口になっています。中には、レイヤー 7 に使用されているプロトコルのロジックを悪用するものもあります。2023 年に見つかった HTTP/2 ロジックの脆弱性は、攻撃者が、一見して問題なさそうに見えるロジックを悪用して、いくつものリクエストを 1 つのストリームの中に束ね、記録上、レイヤー 7 DDoS 攻撃のうち最大のものとなった例です。DDoS 攻撃者にとってアプリケーションレイヤーが付け込みやすい理由の 1 つは、攻撃に必要な帯域幅、パケット、デバイスの量がさほど多くなく、規模が小さくて済むところです（ほとんどの場合は 1 Gbps 以下）。このタイプの攻撃は通常、ステルス性と深刻度が高く、アプリをクラッシュさせるために攻撃者が送信するリクエストは正当なものと勘違いされることがよくあります。また、アプリケーションの負荷の多い部分を集中的に攻撃し、ユーザーのアクセスを出来なくします。

DNS に対する DDoS 攻撃も、増加傾向にある一般的な手口です。組織の DNS がダウンすると、その組織のオンライン上でのプレゼンスが失われます。したがって、サイバー犯罪者から見ると、非常に大きなインパクトを与えることができる利益の出やすい標的となります。DNS DDoS 攻撃のタイプによっては、レイヤー 7 だけでなく、ネットワークのレイヤー 3 とレイヤー 4 にも影響を与えるものもあります。Akamai の内部データによると、過去 18 か月間に発生したレイヤー 3 とレイヤー 4 の DDoS 攻撃イベントの 60% に DNS コンポーネントが存在していました。このカテゴリでは、DNS リソース枯渇攻撃（NXDOMAIN 攻撃、擬似ランダムサブドメイン攻撃、DNS 水責め攻撃とも言われる）が、レイヤー 3 とレイヤー 4 の DNS DDoS 攻撃の 50% を占めています。今日のデジタルファーストの世界では、DNS DDoS 攻撃は、スポーツベッティング企業や重要なショッピングシーズン中のオンラインコマース企業など、対人関係の多い企業のオンラインパフォーマンスを低下させるために、サイバー犯罪者によって日和見的に使用されることもあります。

DDoS 攻撃は、分かりやすくなるようにレイヤー 3、4、7 攻撃として、または DNS 攻撃として区分されることもありますが、攻撃者は、被害者のアプリケーションやその基盤とするインフラに過大な負荷をかけるために複数のレイヤーとプロトコルを標的とする攻撃ベクトルを使用する傾向が強いことに注意する必要があります。強固で効果的な DDoS 多層防御戦略には、攻撃者からすべてのレイヤー、ポート、プロトコル、コンポーネントを保護できる包括的な基盤となるソリューションを含める必要があります。

レイヤー 7 DDoS の標的になっている業界トップ 3：ハイテク、コマース、ソーシャルメディア

当社の調査によると、レイヤー 7 DDoS 攻撃は、世界的に見てハイテク、コマース、ソーシャルメディアの各業界がよく受けている攻撃です。

ハイテク

ハイテク業界を標的とした攻撃の数は、全業界の中でも群を抜いて多く、2023 年第 1 四半期から 2024 年 6 月までの攻撃件数は 5 兆件以上です（図 5）。

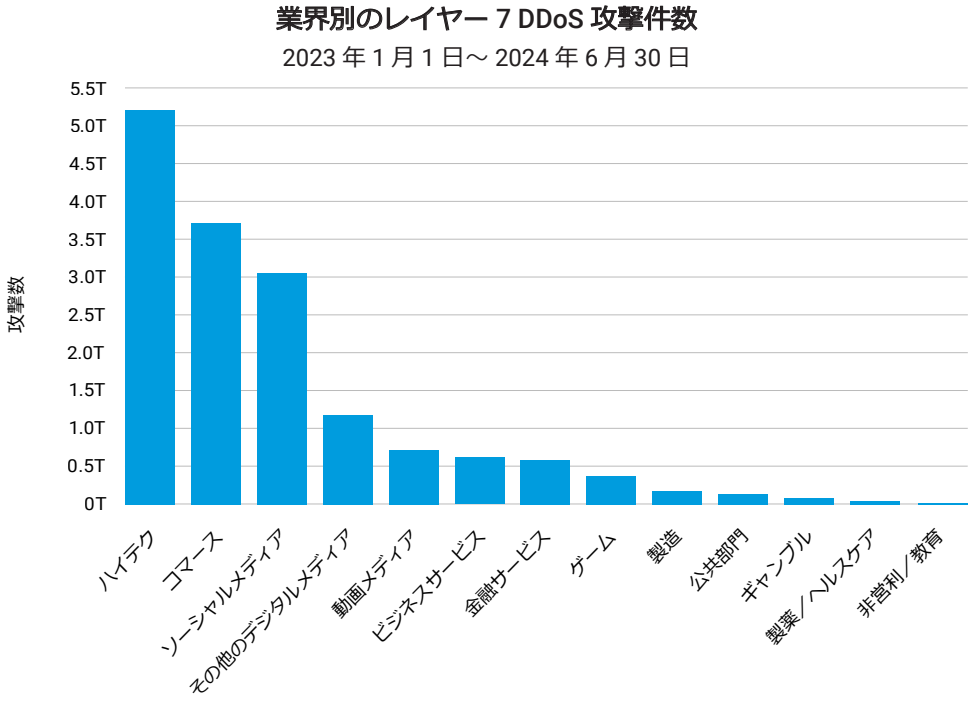
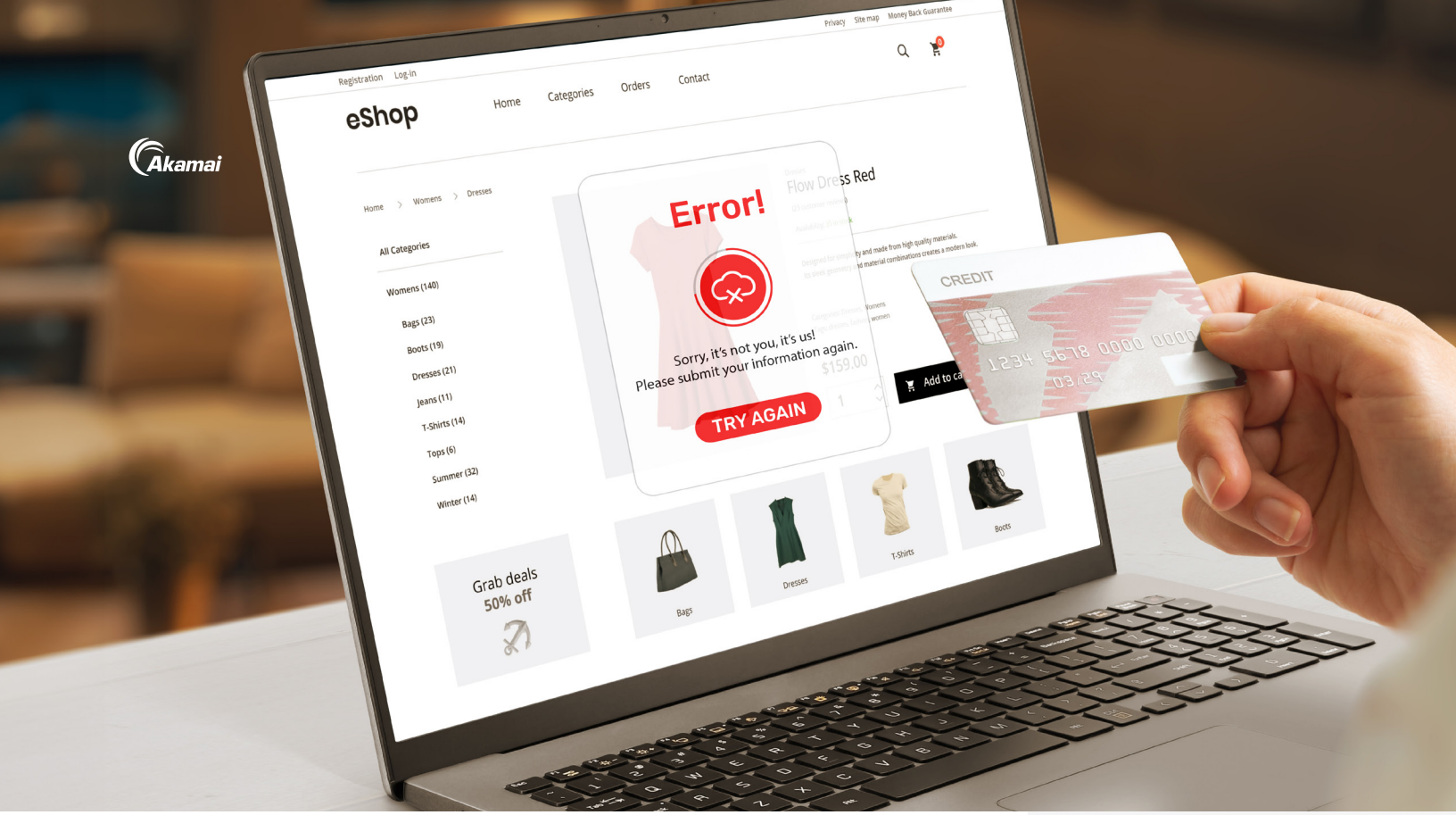


図 *5*：ハイテク、コマース、ソーシャルメディア業界のアプリケーションレイヤー *DDoS* 攻撃件数は他の業界の *2* 倍以上

ハイテク業界は、オンラインサービスに依存する企業で構成されています。当社が監視している DDoS 攻撃トラフィックには、クラウドサービスやブロックチェーンテクノロジーが含まれていることがあり、どちらもレイヤー 7 DDoS 攻撃の影響を強く受けています。

クラウドコンピューティングは、もはや DDoS 攻撃とは無関係ではなくなっています。セキュリティ担当者は、クラウドに接続されたビジネスを標的とした攻撃や、DDoS 攻撃を仕掛ける簡単な方法としてクラウド自体を攻撃者が使用している様子を見ています。つまり、クラウドコンピューティングは、そのような攻撃の火付け役であり、同時に標的でもあるのです。コマース、金融、ヘルスケアなど、どの業界であっても、クラウド対応 Web アプリケーションを使用している組織は、レイヤー 7 DDoS 攻撃に対して脆弱にならざるを得ません。そのうえ、クラウド環境の場合は、攻撃経路の選択肢が無数にあるため、このようなアプリケーションレイヤー DDoS 攻撃を特定することは至難の業になります。



ブロックチェーンネットワークにおける DDoS 攻撃の数は、ここ最近、顕著に増えています。ブロックチェーンは設計上、分散型であるにもかかわらず、攻撃者は従来のネットワークフラッディングとは異なる DDoS 攻撃手法を使用しています。当社が見たところ、サイバー犯罪者は、大量のスパムトランザクションをブロックチェーンに送り付け、正当なトランザクションの処理を遅延させています。さらに、ブロックチェーンに対する DDoS 攻撃には HTTP フラッド攻撃が見られ、ブロックチェーン内のスマートコントラクト・ネットワークも DDoS 攻撃の影響を受けやすくなっています。このタイプの攻撃でブロックチェーンネットワークに発生するリスクは、主にトランスポートレイヤーのプロトコルに生じます。

コマース

最近の EMEA SOTI レポートから分かるように、その地域ではレイヤー 7 DDoS 攻撃の件数が最も多かったものの、世界的に見ると第 2 位でした。レイヤー 7 DDoS 攻撃がコマース分野でこれほどまで多くなった理由は、このタイプの攻撃が攻撃者にとって収益に大きなダメージを与える機会になるからです。このタイプの攻撃は、オンラインストアや予約システムを利用できない状態に陥れ、被害企業に大きな収益損失をもたらすため、特にコマース組織には致命的なダメージとなります。同時に、このタイプの攻撃は、相手の注意をそらすための手口として利用されることもあります。インシデント対応のリソースを消費させながら、攻撃者が標的企業のネットワークのさまざまな場所から利益の出やすい顧客データ（決済カード情報など）を盗みます。

コマースは、 EMEA 地域でレイヤー 7 DDoS 攻撃を最も受けた業種であり、 世界規模で見ると第 2 位になります。

ソーシャルメディア

レイヤー 7 DDoS 攻撃は、2023 年に世界的に増加しており、6 月に急増しました（図 6）。ソーシャルメディアでもこの全体的な増加傾向に沿って攻撃が増加しましたが、この業界では、世界的な急増より丸 2 か月早い 2023 年 4 月からの 10 か月間でレイヤー 7 DDoS 攻撃が非常に早いペースで増加しました（図 7）。

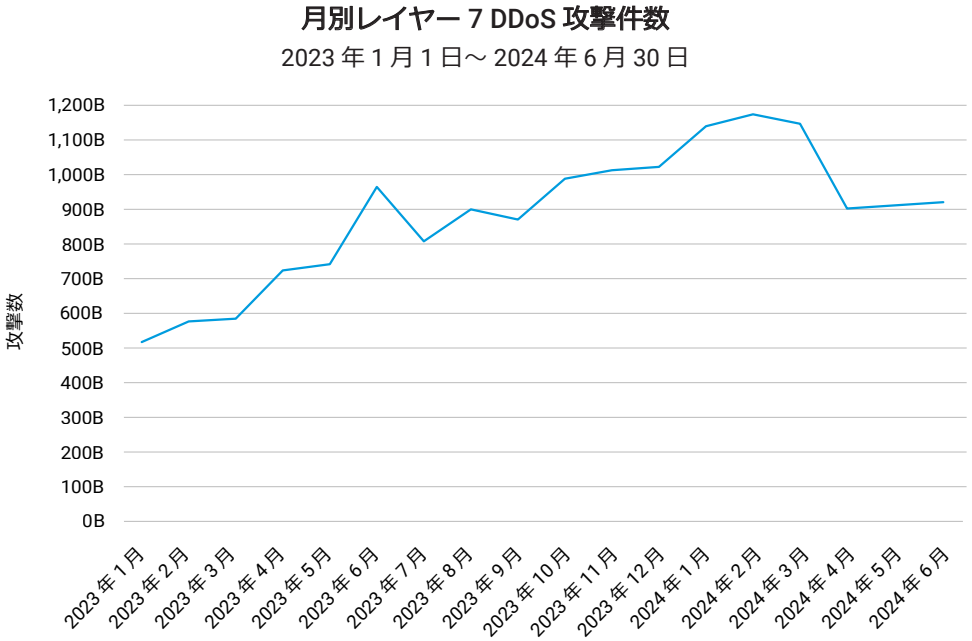


図 *6*：この期間の間にレイヤー *7 DDoS* 攻撃が全般的に増加しており、*2023* 年 *6* 月から急増傾向を示しています

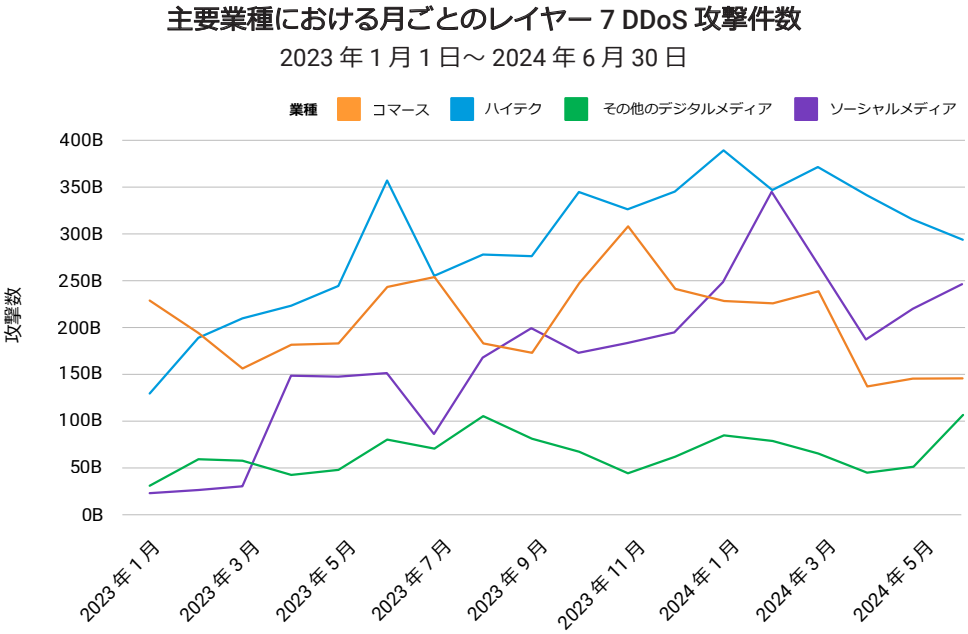


図 7：ソーシャルメディア分野は、レイヤー *7 DDoS* 攻撃の影響を顕著に受けている

ソーシャルメディア業界におけるこのレイヤー 7 DDoS 攻撃は、現在起きている地政学的な出来事と圧力に関係しています。

まず、2024 年に、複数のメディアが政治的な分断を煽るために、親ロシア派の詐欺的なソーシャル・メディア・アカウントやニュースサイトのなりすましの急増に関する報道を流すようになりました。このようなロシア側の世論工作は、世界中の幅広い視聴者やトピックに狙いを定めていますが、一貫してウクライナへの支持を低下させ、民主的な制度や指導者への信用を失墜させ、現存する政治的な分裂を利用することを目的としています。

第二に、媒体を使った大規模な選挙イベントや国の指導者に関する疑問が引き金になって、さまざまな地域で政治的な動機に基づくサイバー攻撃（DDoS 攻撃など）が発生する傾向もあります。これは、攻撃者が政治的雰囲気の高まりを自分たちの目的のために利用しようとしているからです。

第三に、ロシアとウクライナ間の戦争やイスラエルとハマス間の戦争に絡んでハクティビズム （英語版のみ） が広がっており、これも攻撃の増加に加担していると見られます。

攻撃者は今後も、誤った情報や偽の情報を広範囲にわたって早く拡散させるために、ソーシャル・メディア・プラットフォームを利用していくでしょう。AI ツールの普及に伴い、本物らしく見せかけた偽コンテンツの作成と拡散が容易になり、その対策の難易度が上がっています。2024 年はアジア太平洋・日本（APJ）地域と米国の選挙の年に当たるため、AI が生成する政治的な偽情報の影響を受ける可能性に対する懸念が高まっています。

ソーシャルメディア企業は、誤った情報に対抗するためにさまざまな方針を立てていますが、その効果ははっきりしていません。偽情報戦術が進化し、AI 技術が急速に進歩しているため、2024 年が進むにつれ、ソーシャル・メディア・プラットフォームを介して偽情報がますます広がりを見せていますが、それに対抗することは非常に困難になっています。

Web アプリケーションのレイヤー 7 DDoS 攻撃は API 攻撃よりも一般的だが、API 攻撃は休日に急増する

スマートな DNS 解決サービスや CDN を使った健全なセキュリティアーキテクチャなど、Web アプリケーションファイアウォールやその他のセキュリティソリューションは、多くの場合、Web アプリケーションとそのインフラを DDoS 攻撃から保護するうえで役に立ちます。しかし、Web アプリケーションと API は依然として広く標的になっており、実際、それぞれについて取り上げた、OWASP セキュリティリスクのリストがあります。脅威の状況に関しては、Web アプリケーションおよび API のレイヤー 7 DDoS 攻撃の件数が各地域で大きな割合を占めています（図 8）。北米の後に続く地域を見ると、Web アプリケーションでは APJ が続き、API ではヨーロッパ、中東、アフリカ（EMEA）が続きます。

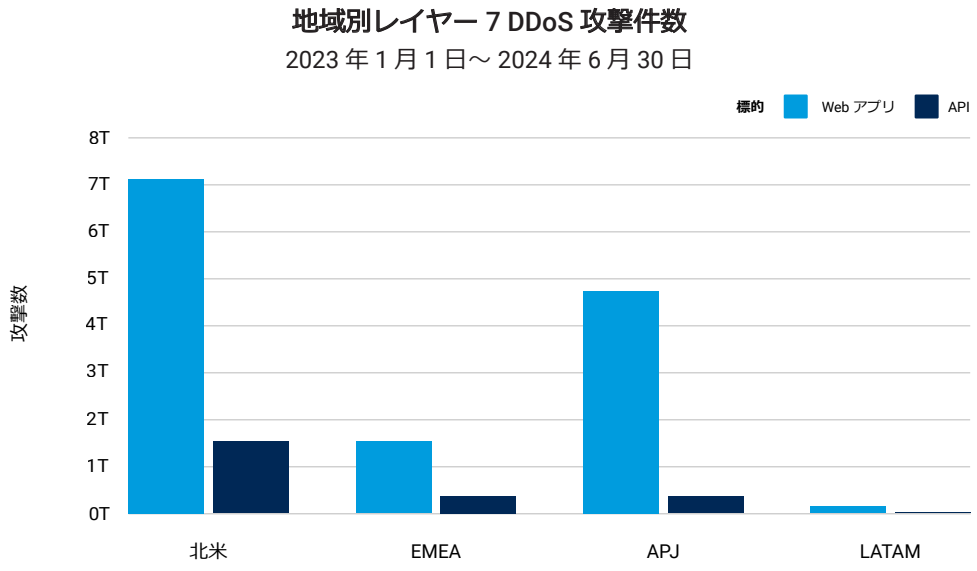


図 *8*：世界的に見ると、レイヤー *7 DDoS* 攻撃の標的は *API* よりも *Web* アプリケーションの方が多く、地域別に見ると北米が *Web* アプリケーションと *API* の両方で最も多くなっている

DDoS 攻撃のように大量のリクエストで過負荷をかけると、（アプリケーションと同様に）API もクラッシュする可能性があります。Akamai は、企業や組織が防御すべきセキュリティリスクの上位 5 位に DDoS 攻撃を挙げています。2023 年第 4 四半期に API に対するレイヤー 7 DDoS 攻撃が増加していることは注目に値します（図 9）。

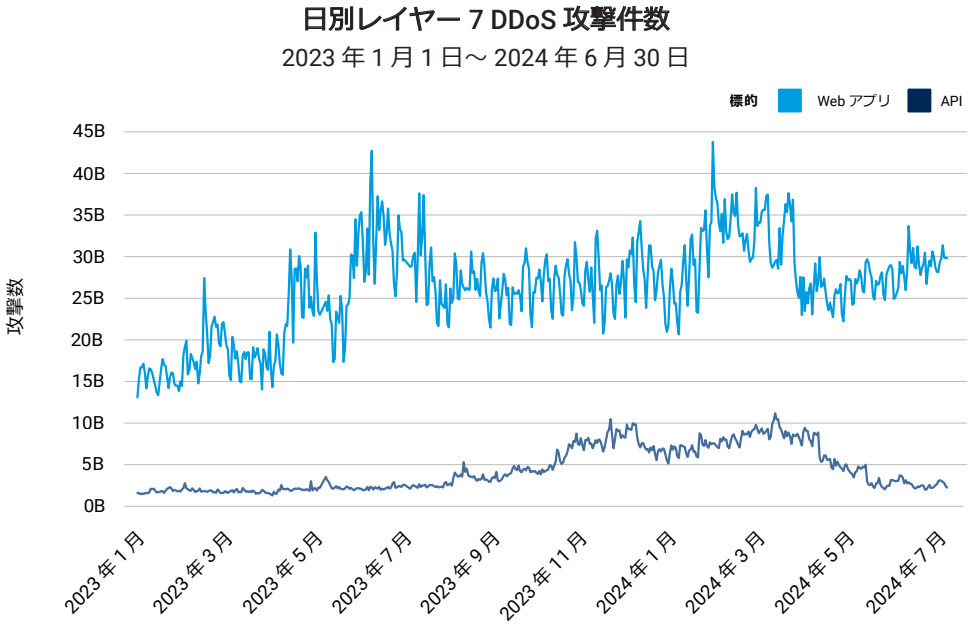


図 *9*：*API* に対するレイヤー *7 DDoS* 攻撃は、*2023* 年第 *4* 四半期に大幅に増加し、*2024* 年第 *1* 四半期までその傾向が継続

ホリデーシーズンと、攻撃者が企業の収益に大きな悪影響を与えようとする時期が重なる年末にかけて、攻撃件数が増加する傾向があります。Akamai の調査によると、冬季のホリデーシーズンとサイバー攻撃件数の増加との間には直接的な相関関係 （リンク先英語のみ） があります。特にコマース分野では、脅威に対応するセキュリティ担当者やインシデント対応リソースが少なくなるこの時期に、このような攻撃の件数が非常に多くなります。

レイヤー 7 DDoS ランサムウェア集団

攻撃の複雑化に伴い脅威が拡大しており、ランサムウェア集団は、攻撃の手口、技術、手順（TTP）の継続的な進歩に大きく貢献しています。高度な TTP の例としては、ランサム DDoS（RDDoS）とも呼ばれている三重の脅迫攻撃があります。RDDoS の場合は、DDoS が攻撃に上乗せされ、攻撃対象の業務を妨害するとともに、攻撃対象のデータを暗号化し、盗み出し、支払いに応じなければデータをさらすと脅迫します。RDDoS を使用する大手ランサムウェア集団としては、Killnet、DarkSide、Lazarus があります。

Lazarus ランサムウェア集団は一般的に、標的の Web プロパティに大量のレイヤー 7 の HTTP リクエストや HTTPS リクエストを送り付け、その攻撃キャンペーン全体を通して、50 Gbps ～ 300 Gbps、150 Kpps ～ 150 Mpps の攻撃ボリュームを監視します。Lazarus は、最大 2 Tbps クラスの DDoS 攻撃能力があると主張していますが、幸いなことに、それほどの大規模な攻撃はまだ発生していません。Killnet ランサムウェア集団も、レイヤー 7 に対して DDoS 攻撃（大量の POST ／ GET リクエスト）を仕掛け、リソースの枯渇やシステム障害を引き起こします。これらの例は、レイヤー 7 DDoS 攻撃を通じて組織に損害を与えることに重点を置いている多くの攻撃者の一例に過ぎません。

レイヤー 3 および 4 DDoS 攻撃トラフィック

アプリケーションレイヤーだけでなく、DDoS 攻撃イベントはインフラにも大きな影響を与えています。当社の継続的な観測によると、レイヤー 3 および 4 DDoS 攻撃の件数は、イベントが同時発生するという性質上、攻撃活動に増減があるため、波状になります（図 10）。過去 6 か月にわたって、EMEA と北米は交互に最も攻撃の標的にされた地域になっています。EMEA 地域では、過去 7 か月のうち 5 か月で、レイヤー 3 および 4 DDoS 攻撃イベントが北米よりも多くなっています。金融サービス業界は、依然としてレイヤー 3 と 4 の DDoS 攻撃イベントが世界的に最も多く、一定期間、一貫してトップの座にいたため、今後もしばらくはトップの座に居続けると推測できます。

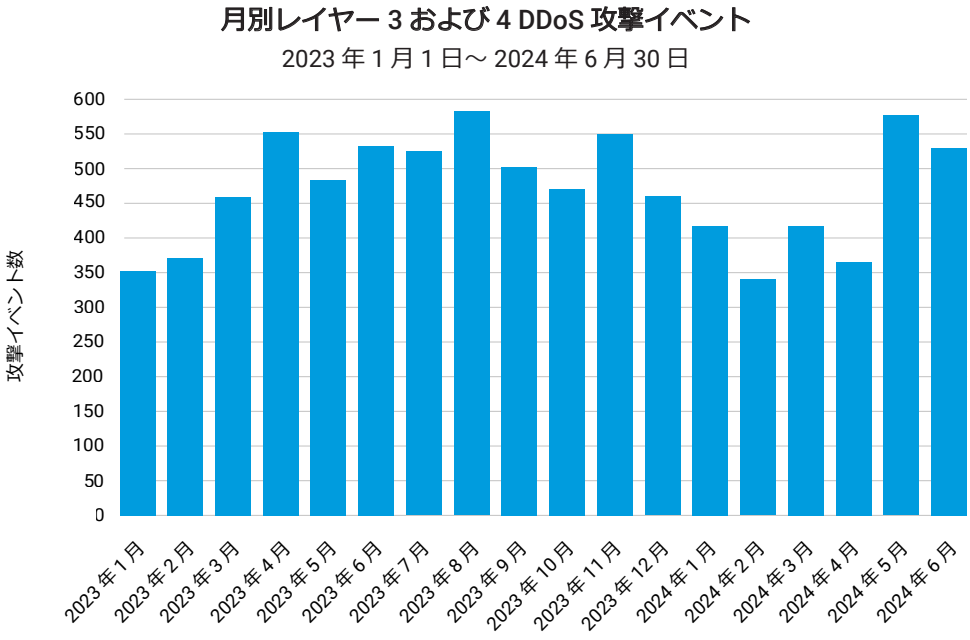
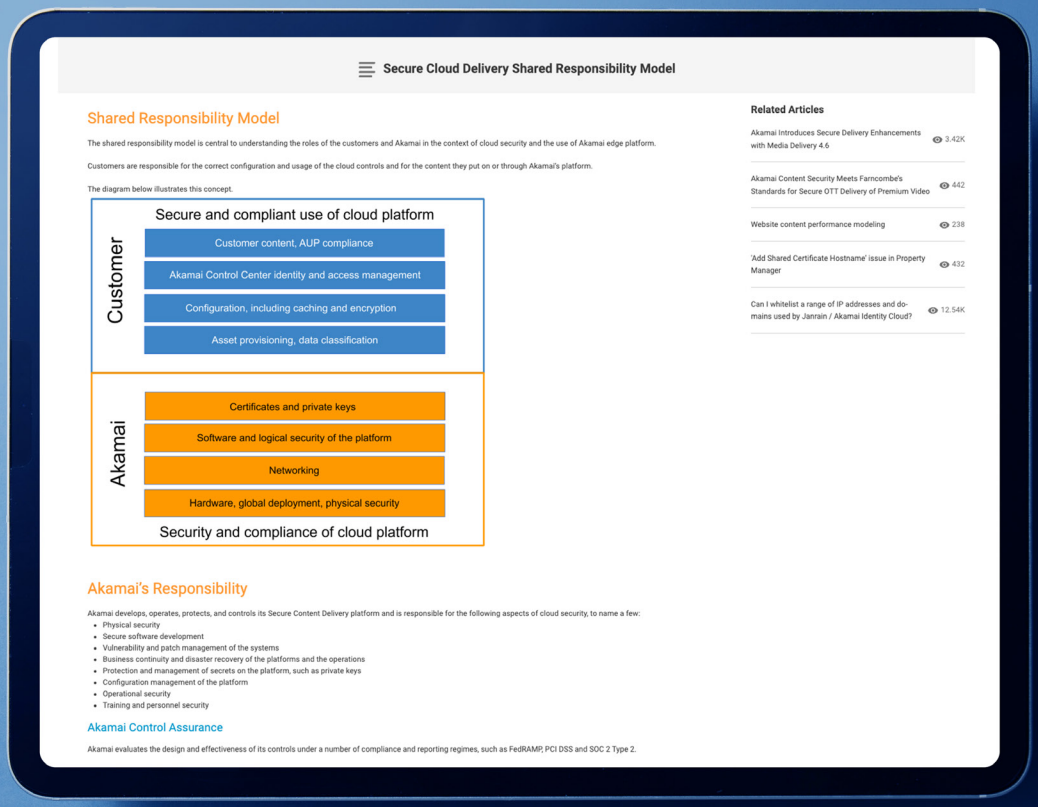


図 *10*：レイヤー *3* と *4* の *DDoS* 攻撃は増減を繰り返しており、過去 *18* か月間の攻撃イベントの件数には *200* 以上の差があることが観測されている



図：Akamai／セキュアクラウド配信の責任共有モデル

攻撃者の標的はアプリケーションワークロード

ゼロトラスト戦略は、ともすればネットワークセキュリティとの関係性という観点で考えられがちです。組織がゼロトラストの考え方を導入する際に、Web アプリケーションが見過ごされることがありますが、これを含めることは全体的な対策の有効性を最大限に高めるうえで非常に重要です。レイヤー 7 ではアタックサーフェスが異なる可能性がありますが、レイヤー 3 と 4 に影響を与える脅威から影響を受けないとは言えません。事実、安全性の低い Web アプリケーションは、ネットワークへの侵入口を増やす可能性があるため、ラテラルムーブメント（横方向の移動）や権限昇格の攻撃を受ける可能性があります。

見過ごされた場合、Web アプリケーションは、アプリケーション間の内部ワークロードと同様に、外部にさらされる恐れがあります。Web アプリケーションの導入が起因となってアタックサーフェスが拡大すると、セキュリティチームが抱えている難しい仕事がさらに複雑化します。環境がクラウド、オンプレミス、ハイブリッドのいずれであっても、アプリケーションを機能させるためには、それぞれのワークロードがシームレスに動作しなくてはなりません。ワークロードはネットワーク内を移動しながら複数のセキュリティ管理範囲を通過します。新しい管理範囲を通過するたびに、侵入口となり得る箇所が増えていきます。ゼロトラストはテクノロジーの領域と考えられがちですが、人間同士の信頼関係もアプリケーションセキュリティに不可欠な要素になります。ワークロードの通り道のセキュリティを確立するためには、複数のベンダーが責任を共有 （参照先は英語版のみ）する必要があるためです。

適切なゼロトラスト・フレームワークの実装は、得てして組織にとって大きな負担になります。ハードウェア（従来のセグメンテーション）ベースで実施する場合は、特定の目標を前提において設計する必要があります。セキュリティ担当者にとってそれは、あらゆる面でリソースを大量に消費する「リップアンドリプレース（まるごと置き換え）」を意味します。アプリケーションセグメンテーションも似ていますが、依然として制御をレイヤー 4 に頼るとはいえ、一般に実装はやや容易になります。しかし、侵入者に対する防御策としては適切ではありません。

ソフトウェアベースのセグメンテーションであれば、数分で導入できるため、アプリケーションセキュリティに関わる負担が大幅に減り、そのうえ、インシデント対応の対策としても有効です。このアプローチは、熟練した開発者がセキュリティの負担を負うという状況を回避するという目的に適っており、組織への DevSecOps の効果的な導入を実現します。

真のゼロトラストを導入するのであれば、最低限、マイクロセグメンテーションが必要です。マイクロセグメンテーションがあれば、ランサムウェアやワークロード自体に対する攻撃から防御することができます。マイクロセグメンテーションにより、ネットワークを徹底的に可視化できます。また、危険にさらされたワークロードやコンテナを検知し緩和するために必要なガバナンスを非常にきめ細かく制御できます。認可されたアクティビティは、IP アドレスのスプーフィングや許可されたポートを使用した攻撃の影響を受けることがない、その活動に高度に特化したポリシーで制御することができます。

マイクロセグメンテーションにより、 ネットワークを徹底的に可視化できます。 また、 危険にさらされたワークロードやコンテナを検知し緩和するために必要なガバナンスを非常にきめ細かく制御できます。

このような強固な対策を講じなければ、攻撃者が攻撃の足がかりを得て、ランサムウェアを展開し、アプリケーションがどこにあろうとワークロードの処理をブロックしてくる可能性があります。そして、身代金の支払いに応じない限り、アプリケーションを使い物にならない状態にします。

ゼロトラストの適用方法

マシンと実行ファイルとの間の通信など、有効な通信には信頼が必要です。信頼は対人関係において望ましいものかもしれませんが、ことアクセスについては、ゼロトラスト（何も信頼しない）は、組織が一切の労力を惜しまずに実現すべきものです。ネットワークの内部では、ランサムウェアやその他の脅威がシステム内を移動するためにはラテラルムーブメントが必要です。そのため、1 つのドアをくぐるよりも、6 つのドアをくぐって侵入する方がはるかに困難になります。

このセクションでは、ゼロトラストを導入したエンタープライズ組織が、どのようにして全体的なセキュリティ対策に存在するギャップを埋め、強化しているかの実例として実際の現場のケーススタディを 2 つ紹介します。

ユースケース 1：ランサムウェアキルチェーンの切断

最近になって自社の環境にゼロトラスト・フレームワークを導入した米国のある通信インフラプロバイダーは、もし導入していなければ、ランサムウェア攻撃を受けて 100 万米ドルの損失を被る可能性がありました。このソリューションにより、きめ細かくイベントを監視できるため、セキュリティチームはブルートフォース攻撃について警告を受け、リモート・デスクトップ・プロトコル（RDP）を使用した大量のログイン試行の失敗が発生していることに気が付きました。調査を進めた結果、このプロバイダーは、有名なランサムウェア集団の標的になっていたことが分かりました。システムやデータが実際にダメージを受ける前に RDP を無効にする新しいポリシーを導入していたため、攻撃の試みを阻止できました。

ユースケース 2：インサイダーの脅威

インサイダーの脅威は、機密性の高い情報が盗まれ、不正な目的に使用される恐れがあるため、組織にとって重大な危険となります。業種に関わらず、インサイダーの脅威はあらゆる組織にとってリスクになるため、悪性の水平方向（East ／ West）のトラフィックを特定し、許可されていないラテラルムーブメントをブロックするソリューションが不可欠です。

アプリケーションやシステムの間の内部的な通信を可視化する必要があるため、米国のある教育機関では Active Directory や SQL Server などの重要なアセットを囲い込んで保護しています。この組織は、セグメンテーションを導入しており、アプリケーション間のデータフローを可視化し、不審なトラフィックを監視し、悪性と判断としたものをブロックすることができます。また、サードパーティベンダーから Web サーバーへの RDP アクセスをブロックすることもできます。

ネットワークの内部では、 ランサムウェアやその他の脅威がシステム内を移動するためにはラテラルムーブメントが必要です。 そのため、 1 つのドアをくぐるよりも、 6 つのドアをくぐって侵入する方がはるかに困難になります。

APJ スナップショット

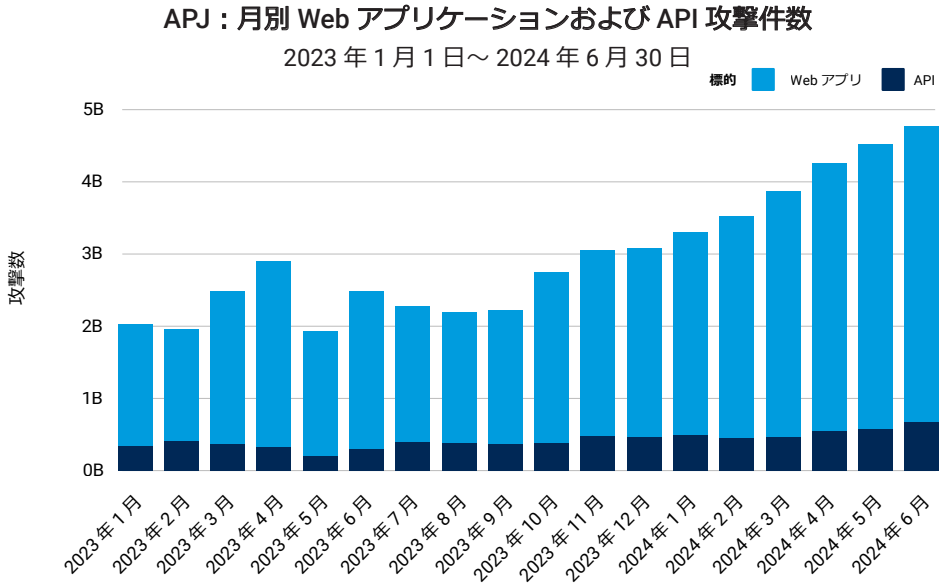
本 APJ スナップショットは、ランサムウェアに関する包括的なセキュアアプリ SOTI レポート「包囲されるデジタル要塞：現代アプリケーションアーキテクチャを狙う脅威」に付随するレポートです。拡大するアタックサーフェスを攻撃者がどのように悪用するのかの詳細な説明、組織を保護するための推奨事項、当社の調査方法に関する説明については、同レポートを参照してください。

Web アプリケーションと API：セキュリティリスクを生む原因が多数

組織が顧客体験の向上とビジネスの推進を図るためにアプリケーションの導入を急ぐなか、Web アプリケーション攻撃および API 攻撃が急増しています。拡大するアタックサーフェス（質の悪いコーディング、設計上の欠陥、数年前の古い脆弱性を抱えた Web アプリケーションなど）を攻撃者は悪用しようとしています。さらに、API 経済の急速な拡大を受けて、サイバー犯罪者は脆弱性の悪用やビジネスロジックの不正利用を行う機会をうかがっています。

数字で見る攻撃の傾向

Akamai の最初の 2024 年度版 SOTI レポートでは、Web アプリケーション攻撃全体から見たときの、2023 年における API 攻撃の傾向を調査しました。2023 年 1 月から 2024 年 6 月にかけての過去 18 か月を振り返り、Akamai の研究者が調査したところ、APJ の月間 Web アプリケーション攻撃および API 攻撃数が 18 か月目の 2024 年 6 月にピークを迎え、48 億件に達したことが明らかになっています。つまり、2023 年第 1 四半期から 2024 年第 1 四半期にかけて Web 攻撃数が 65% 増加し、その後の四半期も増加傾向が続いたことになります。API に対する攻撃はわずかに増加し、調査期間の終わりには 6 億 7,000 万件に達しています（APJ 図 1）。



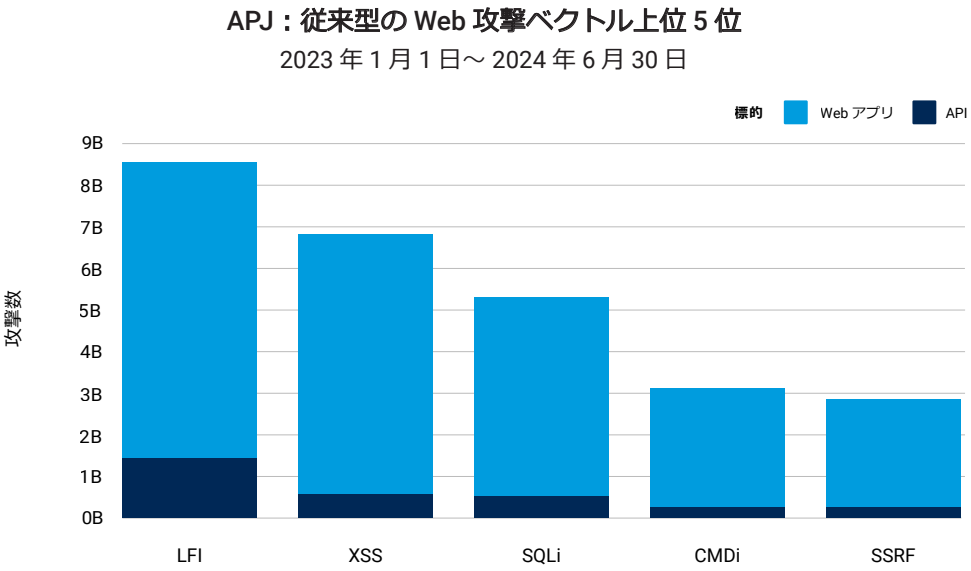
APJ 図 1：Web アプリケーションおよび API 攻撃件数が前年比で 65% 増加

Akamai の研究者の調査によると、 APJ における月別 Web アプリケーションおよび API 攻撃の件数は 18 か月目の 2024 年 6 月にピークを迎え、 48 億件にまで達しました。

APJ ではその期間、オーストラリア（146 億件）、インド（120 億件）、シンガポール（107 億件）が Web アプリケーションおよび API 攻撃を受け、中国（43 億件）、日本（40 億件）、ニュージーランド（21 億件）、韓国（16 億件）、香港特別行政区（15 億件）がこれに続きます。

Akamai は Web 攻撃ベクトルもいくつか追跡しています。このレポートでは従来のベクトルベースの攻撃手法の上位 5 位までに焦点を当てています。

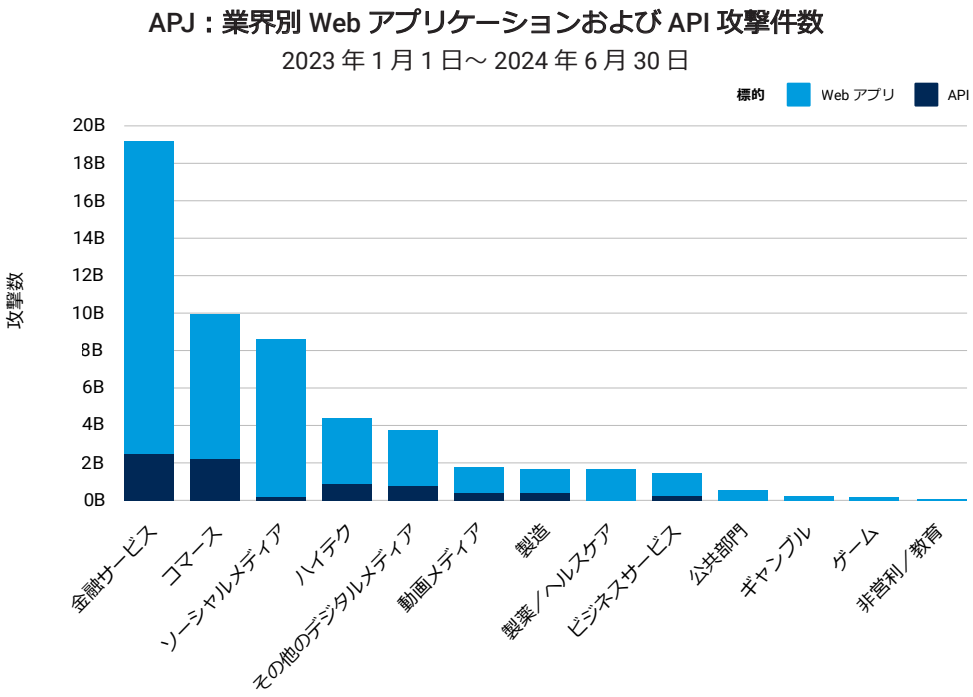
過去のレポートで説明した傾向と同じく、ローカル・ファイル・インクルージョン（LFI）は依然としてよく使われる攻撃ベクトルですが、クロスサイトスクリプティング（XSS）や SQL インジェクション（SQLi）などのその他のベクトルも引き続きリスクとなっています（APJ 図 2）。



APJ 図 2：LFI、XSS、SQLi が Web アプリケーションおよび API 攻撃の増加を後押し

攻撃者が LFI や XSS のような従来の手口を使って標的のデータにアクセスすることは珍しいことではありません。LFI が使用された場合、標的への足がかりが確保され、リモートコードの実行が可能になり、結果としてセキュリティが侵害されます。

業界別で見ると、Web アプリケーションおよび API 攻撃の影響を受けている上位 5 位の業界は、過去のレポートの内容と一致しており、金融サービスとコマースが大きな割合を占めています。API 攻撃を具体的に見ると、ゲーム分野の攻撃件数が大幅に低下しているため、API セキュリティ SOTI レポートの内容とは違った傾向を見せています（APJ 図 3）。とは言え、攻撃者がゲームに狙いを絞ってはいない、ということにはなりません。このレポートで後述するように、ゲームは、レイヤー 3 および 4 DDoS 攻撃で最も標的とされた業種の 1 つです。



APJ 図 3：サイバー犯罪者は執拗に金融サービスに狙いを定め続けている

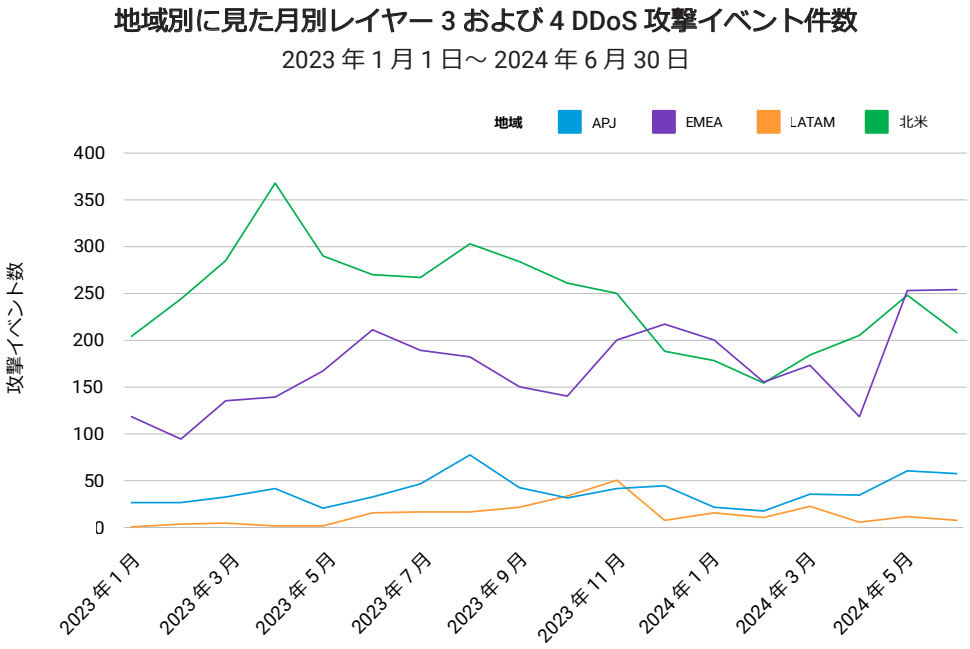
DDoS 攻撃がアプリケーションのアップタイムを脅かす

アタックサーフェスの継続的な拡大に伴い、アプリケーションに影響を与える DDoS 攻撃のタイプも増えています。グローバル SOTI レポートで詳しく説明したように、従来のレイヤー 3 （リンク先英語のみ） とレイヤー 4 の DDoS 攻撃は最も歴史が長く、ネットワークやアプリケーションサーバーのキャパシティをオーバーさせることを目的としています。アプリケーションレイヤー（レイヤー 7）DDoS 攻撃は、脆弱性を悪用し、アプリケーションレイヤーのビジネスロジックの抜け穴や欠陥を突きます。比較的少量の悪性トラフィックでも、大きな損害を与える能力を持っています。攻撃ベクトルが何であるかに関係なく、DDoS 攻撃が成功した場合に受ける被害は、アプリケーションのダウンタイムです。

当社の最新の調査によると、レイヤー 3 および 4 DDoS 攻撃とレイヤー 7 DDoS 攻撃の現在の脅威は、アプリケーション自体だけでなく、アプリケーションの基盤となっているインフラにも及んでいます。

インフラ DDoS 攻撃

2023 年 1 月から 2024 年 6 月にかけての 18 か月のレポート対象期間の間に、Akamai の研究者が調査したところによると、APJ が他の地域よりもレイヤー 3 および 4 DDoS 攻撃イベントの件数が少ないことが明らかになりました。しかし、2024 年 2 月以降には攻撃イベントは増加しています（APJ 図 4）。



APJ 図 4：APJ のレイヤー 3 および 4 DDoS 攻撃イベント件数は、他の地域よりも少なかったが、2024 年には増加

影響を受けた国は多い順に台湾（409 件）、オーストラリア（105 件）、パキスタン（51 件）、香港 SAR（49 件）、日本（38 件）、シンガポール（29 件）です。ここで説明したように、また、アプリケーションレイヤー攻撃に関する次のセクションで説明するように、DDoS 攻撃は APJ において選り抜きのサイバー兵器と化しています。その大きな要因は、地政学的な不安と緊張であり、国の支援を受けている活動家とハクティビストの両方がそれに深く関与しています。

業界別で見ると、レイヤー 3 および 4 DDoS 攻撃イベント件数は、コマース（207 件）業界とゲーム業界（158 件）が上位を占め、その後に金融サービス（120 件）、動画メディア（91 件）、ハイテク（63 件）が続きます。

アプリケーションレイヤー DDoS 攻撃

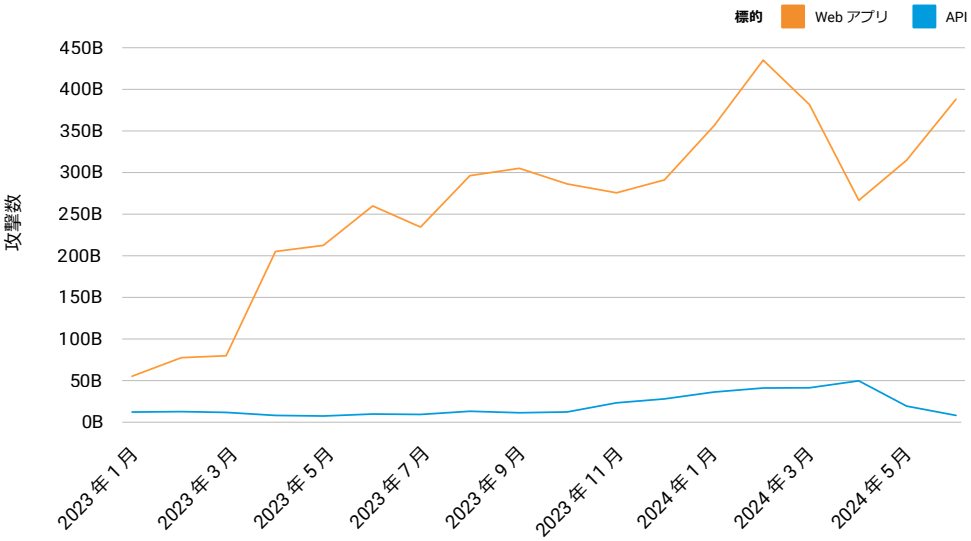
この地域は、レイヤー 3 および 4 DDoS 攻撃に加えて、アプリケーションレイヤー（レイヤー 7）DDoS 攻撃の標的にもなっていました。Akamai の研究者は、2023 年 1 月から 2024 年 6 月までの 18 か月のレポート対象期間の間に、レイヤー 7 DDoS 攻撃件数が北米の 8.7 兆件に対して APJ では 5.1 兆件という調査結果を得ました。

Akamai の研究者は、 2023 年 1 月から 2024 年 6 月までの 18 か月のレポート対象期間の間に、 レイヤー 7 DDoS 攻撃件数が北米の 8.7 兆件に対して APJ では 5.1 兆件という調査結果を得ました。

データを詳しく見ると、レイヤー 7 DDoS 攻撃の月別件数がレポート対象期間中に大幅に増加し、2023 年 1 月には 700 億件の攻撃から始まりましたが、2024 年 6 月には 5 倍以上に膨れ上がり、3,990 億件にまで増加したことが分かりました。それに加えて、APJ におけるレイヤー 7 DDoS 攻撃のうち API を標的としたものは 10% にも満たない件数でしたが（APJ 図 5）、リスクは増加傾向にありました。状況は刻一刻と変化しており、その地域における API の導入は増え続けているため、攻撃を受けるリスクも増えています。

APJ：月別レイヤー 7 DDoS 攻撃件数

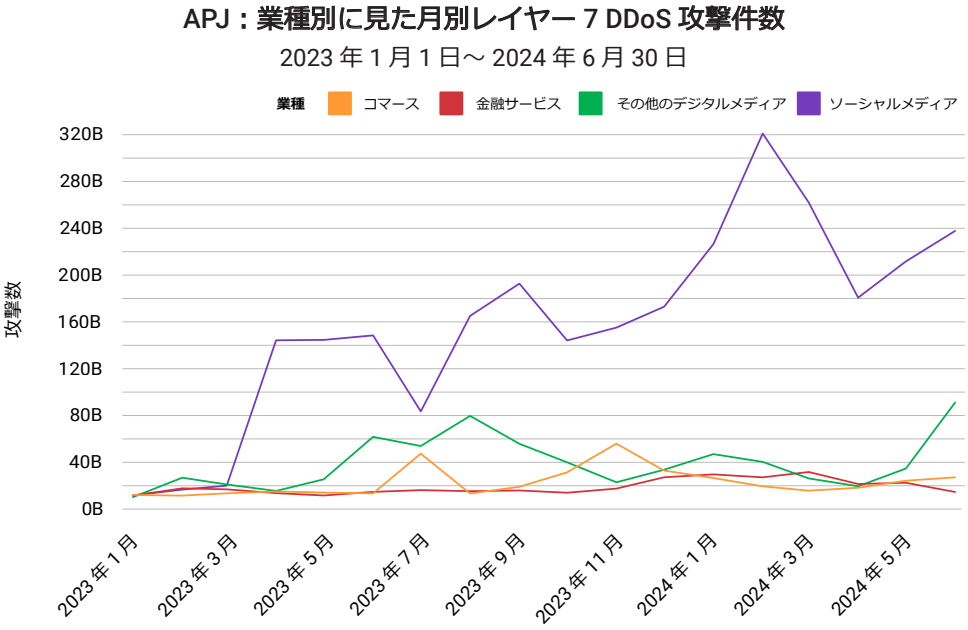
2023 年 1 月 1 日～ 2024 年 6 月 30 日



APJ 図 5：2023 年 1 月から 2024 年 6 月にかけてレイヤー 7 DDoS 攻撃が 5 倍に

その攻撃のうち、シンガポールが 2.9 兆件と最も攻撃が集中し、次いでインド（9,590 億件）、韓国（5,440 億件）、インドネシア（2,600 億件）、中国（1,880 億件）、日本（830 億件）、オーストラリア（740 億件）、台湾（500 億件）と続きます。

業種別に傾向を見ると、レイヤー 7 DDoS 攻撃活動の増加はほぼ、ソーシャルメディア業に対する攻撃の試みに集中しています（APJ 図 6）。



APJ 図 *6*：ソーシャルメディアに対する攻撃の増加は、より大きな世界的な傾向と一致しており、世界各地のより幅広い軍事紛争と、媒体を使った大規模な選挙イベントとの間に相関関係が認められます。

ソーシャル・メディア・プラットフォームは、地政学的な動乱に乗じて大量の攻撃トラフィックを受けることで知られており、APJ でもその例に漏れず攻撃が増加しました。グローバル SOTI で詳細に説明したように、このような活動には、政治的な対立を煽る、大量の新ロシア派による不正なソーシャル・メディア・アカウントやなりすましのニュースサイトも含まれています。このような攻撃は、世界各地で進行中の地政学的な動乱とも関係しています。媒体を使った大規模な選挙イベントや大統領／国の指導者に関する問題が引き金になって、さまざまな地域で政治的な動機に基づくサイバー攻撃（DDoS 攻撃など）が発生することもよくあります。これは、攻撃者が物議を醸すために政治的な雰囲気の高まりを利用しようと考えているからです。ロシアとウクライナ間の戦争やイスラエルとハマス間の戦争に絡んでハクティビズムが、攻撃の増加に加担していると見られます。

人工知能（AI）ツールが浸透し、本物を装う偽コンテンツの拡散が容易になりました。ソーシャル・メディア・プラットフォームはあらゆる種類のコンテンツを扱う巨大なコミュニケーションチャネルとなっているのです。2024 年は APJ と米国で選挙が重なる年でもあるため、攻撃者があらゆる地域でソーシャル・メディア・プラットフォームを標的にすることは今後も続くと考えられます。

このレポートで説明している攻撃傾向のデータから、攻撃者は混乱と金銭的な利益のために手段を選ばず、業界、地域、手口のいずれに焦点を合わせるか、すぐに切り替えることができることが分かります。したがって、どの組織も常に警戒を怠らず、あらゆるタイプの攻撃に対抗し得る防御策を講じ、アプリケーションのダウンタイムを回避できるようにする必要があります。

攻撃者の標的はアプリケーションワークロード

ゼロトラストは一般的に、ネットワークセキュリティの文脈で語られます。しかし、Web アプリケーションとその間にある内部ワークロードも、侵入口を求め、目的の標的に到達するまでの経路を探すランサムウェアのような脅威にさらされる可能性があります。

グローバルレポートで詳しく説明したように、環境がクラウド、オンプレミス、ハイブリッドのいずれであれ、アプリケーションを機能させるためには、各ワークロードがシームレスに動作できる必要があります。ワークロードがネットワーク内を移動するときに複数のセキュリティ管理範囲を通過しますが、新しい管理範囲を通過するたびに侵入口となり得る箇所を増やします。こうして拡大したアタックサーフェスを保護することは、セキュリティ対策を強化するうえで欠かせませんが、セキュリティチームがすでに抱えている難題をいっそう複雑化させます。

従来のハードウェアベースのアプローチに基づいてゼロトラスト・フレームワークを実装しようとすると、リソースと時間を大量に消費する作業になるため、ダウンタイムが必要になります。また、真のゼロトラストを実装するためには、マイクロセグメンテーションで、ランサムウェアやワークロード自体に対する攻撃から守る必要があります。

ソフトウェアベースのマイクロセグメンテーションであれば、実装と運用が迅速かつ容易になるため、実用的なインシデント対応策として機能させるだけでなく、規制コンプライアンスを支える重要なシステムを分離する制御としても機能させることができます。このようなメリットがあるため、変化の多いデータセンター環境、クラウド環境、ハイブリッドクラウド環境のワークロードやコンテナの危険を検知し、緩和するアプローチを採用する組織が増えています。

アプリケーションワークロードの保護の実例

このセクションでは、エンタープライズ組織がどのように重要なワークロードを保護し、ゼロトラストを推進しているのかを示す、アジア太平洋・日本地域における 2 つのケーススタディを紹介します。

APJ ケーススタディ 1:あるソーシャルネットワークは、メッセージングやゲーム、ソーシャルメディアなどのサービスや、金融サービスの購入機能を備えており、顧客との通信のセキュリティを確保する必要性がありました。ハッカーが顧客との通信にアクセスし、他のネットワークやデータベースに向かって横方向に移動するのを防ぐことは、最高情報セキュリティ責任者にとって最優先事項です。顧客はさまざまな種類のオペレーティングシステムやアプリケーションを使用しているため、どのデバイスが脆弱なのかを判断することは不可能です。同社が通信に必要な信頼性を維持するうえで、きめの細かいセグメンテーションポリシーを実装してデバイスとネットワークを分離することは基本的な手法です。

APJ ケーススタディ 2 : 世界的に事業を展開している、ある大手 IT ディストリビューターは、金融サービス分野の顧客に対して数々のサービスを提供しています。銀行の事業運営に必要不可欠な決済サーバーを保護することが最優先事項です。同社は、マイクロセグメンテーションに関する深い知識を備えており、ネットワークの可視化と非常にきめの細かいガバナンス制御を高度に複雑化した環境に大規模に導入し、運用しています。こうして、ビジネスの基盤となる顧客からの信頼とゼロトラスト能力の強みを背景に成長スピードを速めています。

ワークロードがネットワーク内を移動するときに複数のセキュリティ管理範囲を通過しますが、新しい管理範囲を通過するたびに侵入口となり得る箇所を増やします。

EMEA スナップショット

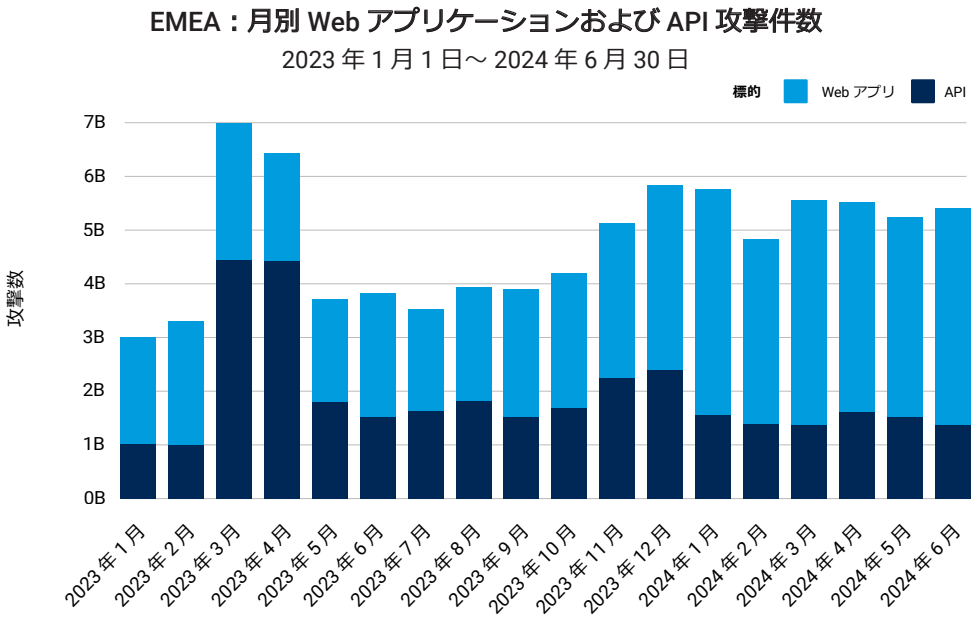
本 EMEA スナップショットは、ランサムウェアに関する包括的なセキュアアプリ SOTI レポート「包囲されるデジタル要塞：現代アプリケーションアーキテクチャを狙う脅威」に付随するレポートです。拡大するアタックサーフェスを攻撃者がどのように悪用するのかの詳細な説明、組織を保護するための推奨事項、当社の調査方法に関する説明については、同レポートを参照してください。

Web アプリケーションと API：セキュリティリスクを生む原因が多数

組織が顧客体験の向上とビジネスの推進を図るためにアプリケーションの導入を急ぐなか、Web アプリケーション攻撃および API 攻撃が急増しています。このような状況で生まれたアタックサーフェス（質の悪いコーディング、設計上の欠陥、数年前の古い脆弱性を抱えた Web アプリケーションなど）を攻撃者は悪用しようとしています。さらに、API 経済の急速な拡大を受けて、サイバー犯罪者は脆弱性の悪用やビジネスロジックの不正利用を行う機会をうかがっています。

数字で見る攻撃の傾向

Akamai の最初の 2024 年度版 SOTI レポートでは、Web アプリケーション攻撃全体から見たときの、2023 年における API 攻撃の傾向を調査しました。2023 年 1 月から 2024 年 6 月にかけての過去 18 か月を振り返り、Akamai の研究者が調査したところ、2023 年第 1 四半期から 2024 年第 1 四半期にかけて EMEA の月間 Web アプリケーションおよび API 攻撃活動が 21% 増加し、その後の 2024 年第 2 四半期でも増加傾向にあることが明らかになっています。API に対する攻撃は、活動がこのような水準で持続する要因となっており、調査期間中の月間 Web 攻撃件数のうち平均して 40% を占めています（EMEA 図 1）。

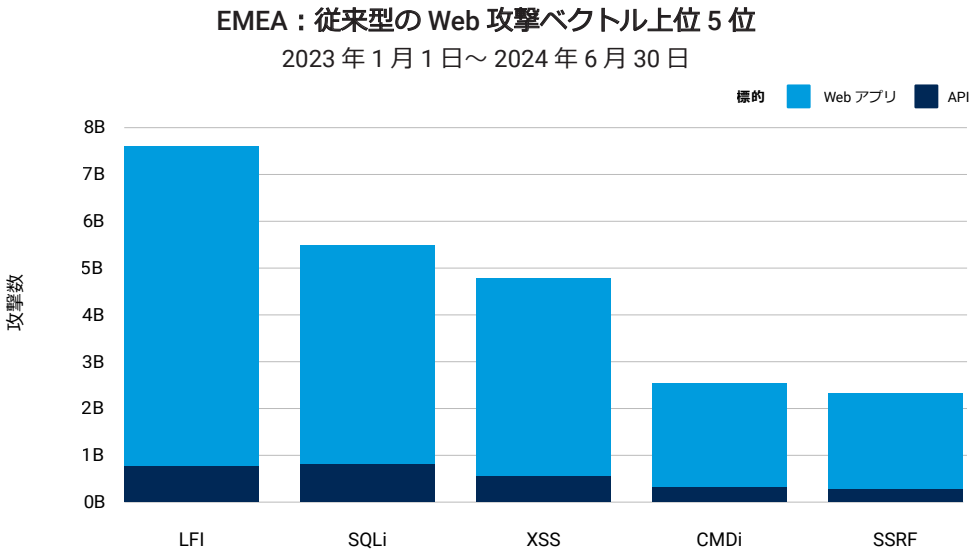


EMEA 図 *1*:*2024* 年度の月間 *Web* アプリケーションおよび *API* 攻撃件数は増加傾向（なお、API 攻撃の急増は、*API* に対して膨大な数の集中攻撃を受けているスペインのコマース分野の攻撃件数が反映されたもの）

EMEA における Web アプリケーションおよび API 攻撃を件数の多い順に見ると、英国（205 億件）、オランダ（156 億件）、スペイン（127 億件）となります。それに続く国を上位 10 位までを紹介すると、ドイツ（87 億件）、オーストリア（74 億件）、フランス（48 億件）、イスラエル（30 億件）、イタリア（27 億件）、スイス（25 億件）、ベルギー（23 億件）となります。

Akamai は Web 攻撃ベクトルもいくつか追跡しています。このレポートでは従来のベクトルベースの攻撃手法の上位 5 位までに焦点を当てています。

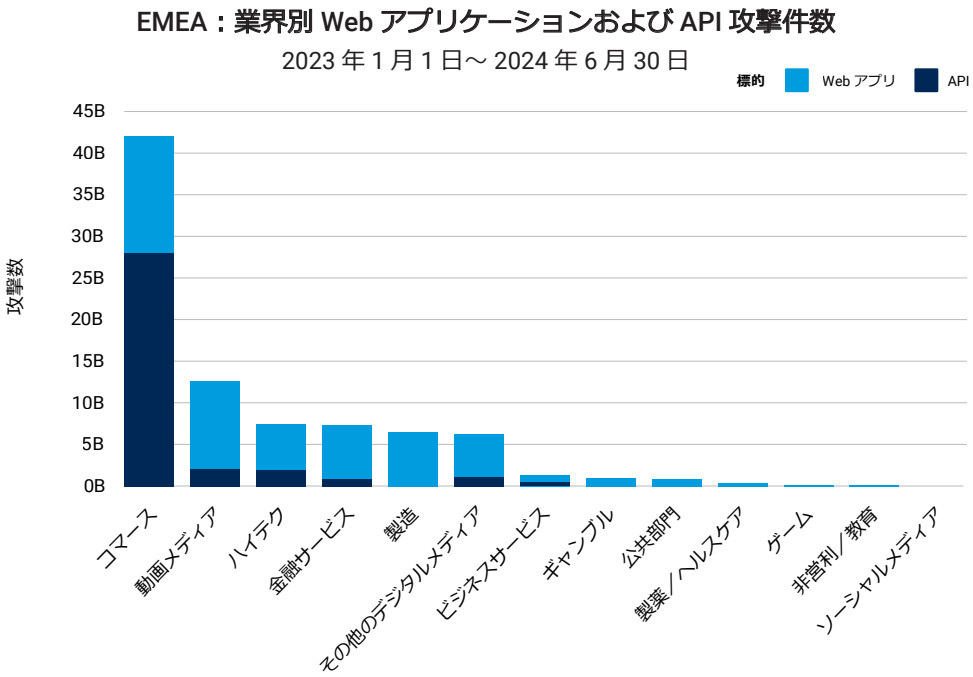
過去のレポートで説明した傾向と同じく、ローカル・ファイル・インクルージョン（LFI）は依然として好んで使われている攻撃ベクトルですが、SQL 言語インジェクション（SQLi）やクロスサイトスクリプティング（XSS）のようなその他のベクトルも懸念すべき攻撃です（EMEA 図 2）。



EMEA 図 2：LFI、SQLi、XSS が Web アプリケーションおよび API 攻撃の増加を後押し

攻撃者が LFI や SQLi のような従来の手口を使って標的のデータにアクセスすることは珍しいことではありません。LFI が使用された場合、標的への足がかりが確保され、リモートコードの実行が可能になり、そしてセキュリティが侵害されます。

過去のレポートで観察された傾向が継続しており、EMEA において Web アプリケーションおよび API 攻撃の影響を受けている業界のうちコマースと動画メディアが上位を占めています。さらに、API セキュリティ SOTI で説明しているように、コマース業は、この地域の他の業種と比較して、API 攻撃を受ける割合が引き続き最も高くなっています（EMEA 図 3）。



EMEA 図 *3*：*API* 攻撃の割合が非常に高いため、コマースは *Web* 攻撃の影響を最も受けた業種であり、その後に動画メディア、ハイテク、金融サービスが続きます。

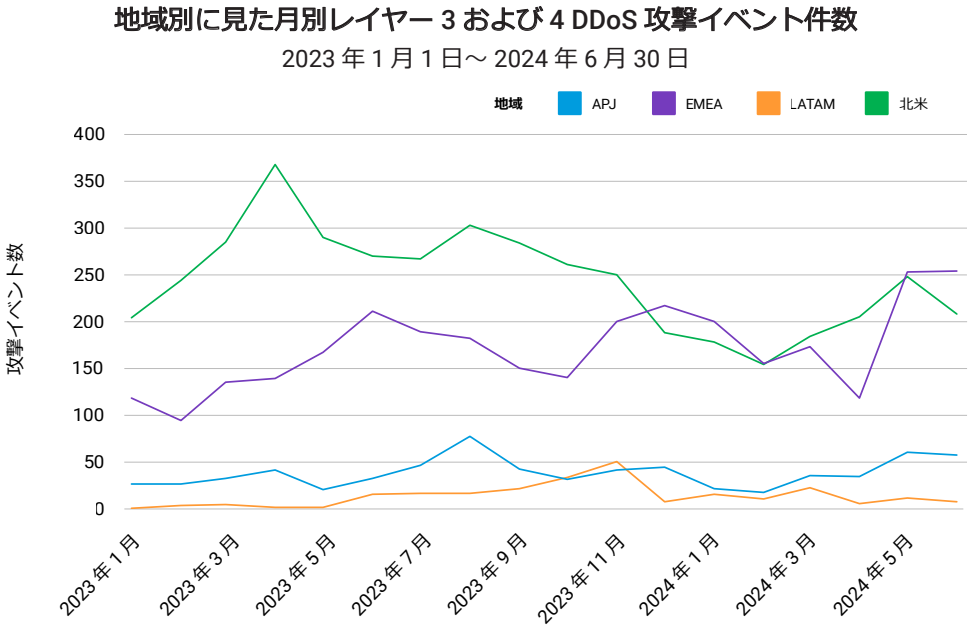
DDoS 攻撃がアプリケーションのアップタイムを脅かす

アタックサーフェスの継続的な拡大に伴い、アプリケーションに影響を与える DDoS 攻撃のタイプも増えています。グローバル SOTI レポートで詳しく説明したように、従来のインフラ（レイヤー 3（リンク先英語のみ）とレイヤー 4）への DDoS 攻撃は最も歴史が長く、ネットワークやアプリケーションサーバーのキャパシティをオーバーさせることを目的としています。アプリケーションレイヤー（レイヤー 7）DDoS 攻撃は、脆弱性を悪用し、アプリケーションレイヤーのビジネスロジックの抜け穴や欠陥を突きます。比較的な少量の悪性トラフィックでも、大きな損害を与える能力を持っています。攻撃ベクトルが何であるかに関係なく、DDoS 攻撃が成功した場合に受ける被害は、アプリケーションのダウンタイムです。

この地域における DDoS 攻撃の全般的な種類と傾向を最近の EMEA 2024 SOTI で詳しく調査しています。その中で言及していますが、最新データから、アプリケーション自体だけでなく、アプリケーションの基盤となっているインフラに対するレイヤー 3 および 4 DDoS の脅威とレイヤー 7 DDoS の脅威が継続して増加していることが分かっています。

インフラ DDoS 攻撃

Akamai の研究者の調査によると、2023 年 1 月から 2024 年 6 月までの 18 か月間にわたるレポート対象期間中において、レイヤー 3 および 4 DDoS 攻撃イベントの件数が EMEA で着実に伸びており、過去 7 か月のうち 5 か月間は北米の月間 DDoS 攻撃イベント件数を上回っていることが分かっています（EMEA 図 4）。



EMEA 図 4：EMEA における月別レイヤー 3 および 4 DDoS 攻撃イベント件数が、過去 7 か月間のうち 5 か月間は北米よりも上回っている

EMEA においてレイヤー 3 および 4 DDoS 攻撃イベントの影響を受けた国を多い順に挙げると、サウジアラビア（957 件）、英国（576 件）、スイス（240 件）、トルコ（205 件）、イタリア（203 件）、ドイツ（189 件）、ポーランド（115 件）となります。

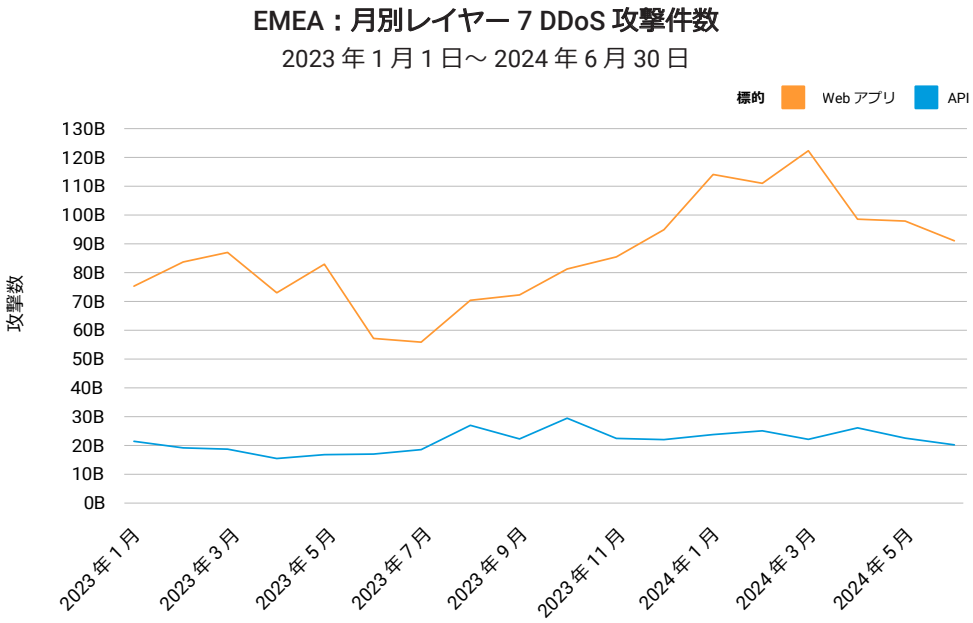
EMEA SOTI で説明したように、DDoS は、政治的な動機に基づくハクティビストや、国の後押しを受けている攻撃者がよく使う攻撃であり、ロシアとウクライナ間の戦争やイスラエルとハマス間の戦争に乗じて攻撃が増加しています。

業界別で見ると、レイヤー 3 および 4 DDoS 攻撃イベント件数は、金融サービス業（1,523 件）と製造業（890 件）が上位を占め、その後にゲーム（189 件）、コマース（151 件）、ギャンブル（105 件）、ハイテク（95 件）が続きます。

アプリケーションレイヤー DDoS 攻撃

この地域は、レイヤー 3 および 4 DDoS 攻撃に加えて、アプリケーションレイヤー（レイヤー 7）DDoS 攻撃の影響も受けていました。Akamai の研究者は、2023 年 1 月から 2024 年 6 月までの 18 か月のレポート対象期間の間、レイヤー 7 DDoS 攻撃件数が北米では 8.7 兆件、APJ では 5.1 兆件なのに対して EMEA では 1.9 兆件であり、受けた影響が 3 番目に多いという調査結果を得ました。

他の地域よりは低いものの、EMEA におけるレイヤー 7 DDoS 攻撃の件数が増加傾向にあることに注意が必要です。月別のレイヤー 7 DDoS 攻撃件数で見ると、2023 年 5 月に 740 億件にまでいったん落ち込んだ後、一転して大幅な増加傾向に転じ、2024 年 3 月にはほぼ倍増しており、2024 年第 2 四半期には Web アプリケーションおよび API を標的とした攻撃が月平均で 1,190 億件に達しています（EMEA 図 5）。

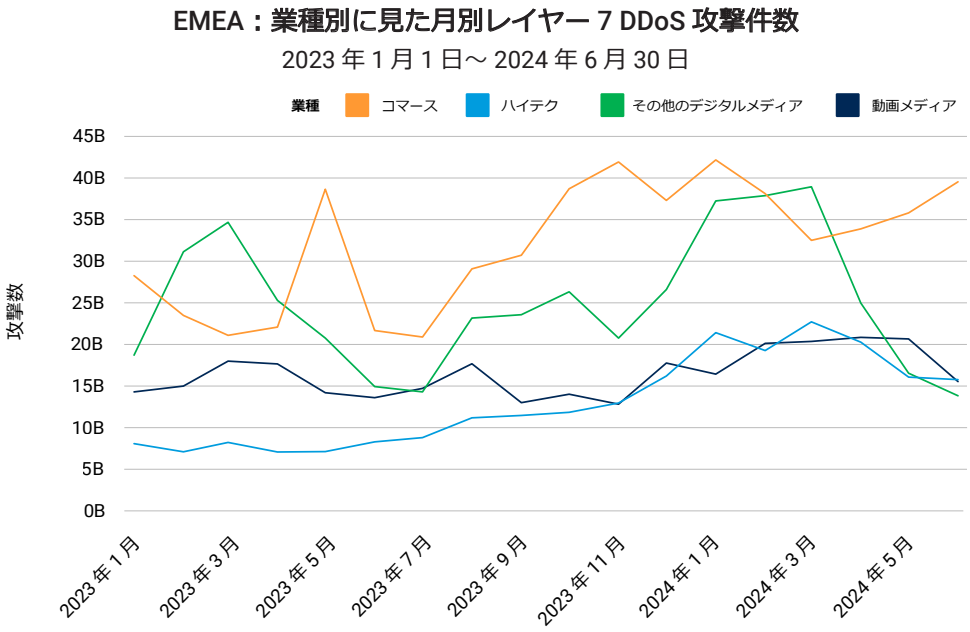


EMEA 図 5：レイヤー 7 DDoS 攻撃の件数は、2023 年 6 月以降大幅に増加し、2024 年第 2 四半期には月平均 1,190 億件に達している

この期間を通じて、API に対する DDoS 攻撃は常に一定の数を維持しており、この攻撃の 25% を占めています。したがって、Web アプリケーションおよび API 攻撃に関しては、行政からの指導、規制が API の使用を推進し続けている以上、前述した攻撃ベクトル（EMEA 図 2 を参照）に対する防御策に加えて、DDoS 攻撃からの API の保護が明らかに必須となります。

EMEA 地域の国をレイヤー 7 DDoS 攻撃件数が多い順に挙げると、ドイツ（4,610 億件）、英国（3,660 億件）、スウェーデン（1,670 億件）、イスラエル（1,510 億件）、イタリア（1,250 億件）、マルタ（1,130 億件）、スイス（1,120 億件）、フランス（900 億件）、オランダ（790 億件）、スペイン（770 億件）となります。

業種別に見たときに、レイヤー 7 DDoS 攻撃の影響を最も受けた業種は、終始一貫して総じてコマース業が多く、その後にデジタルメディア、動画メディア、ハイテクが続きます（EMEA 図 6）。



EMEA 図 6：レイヤー 7 DDoS 攻撃の影響を最も受けた業界はコマース業

攻撃者の標的はアプリケーションワークロード

ゼロトラストは一般的に、ネットワークセキュリティの文脈で語られます。しかし、Web アプリケーションとその間にある内部ワークロードも、侵入口を求め、目的の標的に到達するまでの経路を探すランサムウェアのような脅威にさらされる可能性があります。

グローバルレポートで詳しく説明したように、環境がクラウド、オンプレミス、ハイブリッドのいずれであれ、アプリケーションを機能させるためには、各ワークロードがシームレスに動作できる必要があります。ワークロードがネットワーク内を移動するときに複数のセキュリティ管理範囲を通過しますが、新しい管理範囲を通過するたびに侵入口となり得る箇所を増やします。こうして拡大したアタックサーフェスを保護することは、セキュリティ対策を強化するうえで欠かせませんが、セキュリティチームがすでに抱えている難題をいっそう複雑化させます。

従来のハードウェアベースのアプローチに基づいてゼロトラスト・フレームワークを実装しようとすると、リソースと時間を大量に消費する作業になるため、ダウンタイムが必要になります。また、真のゼロトラストを実装するためには、マイクロセグメンテーションで、ランサムウェアやワークロード自体に対する攻撃から守る必要があります。

ソフトウェアベースのマイクロセグメンテーションであれば、実装と運用が迅速かつ容易になるため、実用的なインシデント対応策として機能させるだけでなく、規制コンプライアンスを支える重要なシステムを分離する制御としても機能させることができます。ネットワークの徹底的な可視化や、きめ細かいガバナンス制御もできます。このようなメリットがあるため、変化の多いデータセンター環境、クラウド環境、ハイブリッドクラウド環境のワークロードやコンテナの危険を検知し、緩和するアプローチを採用する組織が増えています。

アプリケーションワークロードの保護の実例

このセクションでは、エンタープライズ組織がどのように重要なワークロードを保護し、ゼロトラストを推進しているのかを示す、EMEA 地域における 2 つのケーススタディを紹介します。

EMEA ケーススタディ 1:ある大手投資銀行の最高情報セキュリティ責任者（CISO）は、トレーディングや決済に関わる重要なシステムや機微な情報を保護するために、技術インフラのセキュリティを定期的に見直し、あらゆる領域のセキュリティ対策を強化するようにしています。各種のオペレーティングシステムやクラウド環境のスケーラビリティや網羅と同様に、ランサムウェア攻撃の阻止に重点を置いています。さらに、CISO は、古いファイアウォールのアップグレードに伴うコストと遅延を抑えつつ、アタックサーフェスを縮小することを望んでいました。データセンター環境全体を通して安全なゾーンを作るというソフトウェアベースのマイクロセグメンテーションのアプローチを導入することで、アプリケーションワークロード相互を囲うフェンスを設けるようにしました。したがって、ワークロードが攻撃を受けた場合に、そのワークロードを分離できるため、悪性のソフトウェアがネットワークを介して拡散することを防ぐことができます。

EMEA ケーススタディ 2 : あるメディア／ソフトウェアベンダーは、重要なワークロードと顧客データの保護を強化するために、ゼロトラスト・フレームワークの高度化を簡単にする必要がありました。この改善を実現するためには、精度の高いセグメンテーションポリシーを策定し、アイデンティティ管理システムやエンタープライズリソース計画システムのような価値の高いコンポーネントを互いに分離する必要がありました。目標は、何百台ものエンタープライズサーバーの送受信トラフィックを最小限に抑え、アクセスポリシーを厳格化することでした。それと同時に、エコシステムを大幅に変更したために、混乱が生じたり、セキュリティリスクが高まったりする事態は避けたいと考えていました。そこで、相互作用のパターンのきめ細かい可視化に加えて、アラートの機能を備えたソフトウェアベースのマイクロセグメンテーションのアプローチを採り、ネットワーク全体を通した悪性のラテラルムーブメントをチームが阻止できるようにしました。

緩和：アプリケーションと API を攻撃から守る

アプリケーションと API を保護することは、ほとんどの企業にとって大きな需要がありますが、さまざまな手口でアプリケーションが標的にされるため、至難の業に見えます。問題の核心は、それぞれの Web アプリケーションおよび API がアタックサーフェスになり得ることであり、また組織や機密性の高い情報への入口にもなり得ることです。

アプリケーションと API のセキュリティを確保するうえで、設計／構築段階から本番稼動後に至るまでの包括的なアプローチが不可欠です。アプリケーションのコーディングの質が悪いと脆弱性やセキュリティギャップを生み、アプリケーションが悪用されやすくなります。OWASP は、開発者の参考になるようにコードの望ましい書き方を実践するためのチェックリストを公開しています。このようなアプリケーションを放置しておくと、チームを守ることがセキュリティチームの責任範囲になり、API を正確に把握できなくなり、チームに死角を作ることになりかねません。知らぬ間に環境内でシャドウ API が放置されるようになり、悪用される可能性が生まれます。API 使用の規模と範囲が、脆弱性のタイムリーなテストにも影響を与える可能性がありますが、API のテスト機能を備えたソリューションがあれば、リスクが外に漏れ、悪用される可能性を最小限に抑えることができます。

Akamai は最近発表したとおり Noname Security を買収しました。その結果、API エステートの正確なインベントリを含む、API の可視化と（古い API、ゾンビ API などの）探索でもお役に立てるようになり、アタックサーフェスに対する理解を深めることができるようになりました。「把握できていないものは守れない」のです。

このレポートにおける主な知見の 1 つは、攻撃者が古い CVE を悪用して標的に侵入しようとし続けていることです。脆弱性のあるシステムやサーバーのアップデートは時間との闘いになりますが、中にはタイムリーにパッチを適用できない組織もあります。しかし、Adaptive Security Engine のようなソリューションがあれば、悪性トラフィックを拒否できるため、組織に対する攻撃の試みとその影響を受ける可能性を最小限に抑えることができます。

また、DDoS を使用したアプリケーションレイヤーに対する攻撃が顕著に増加しています。2024 年も半ばですが、レイヤー 7 DDoS 攻撃の標的にされている業界の上位 3 位までの攻撃件数がすでに 5 兆件を超えています。デジタルアセット、アプリケーション、インフラを DDoS 攻撃から守るための最善の防御策は、現状の把握と継続的な緩和の組み合わせに尽きます。つまり、パッチ管理、インシデント対応計画、緩和制御（DDoS 攻撃を受ける API アドレスや重要なサブネットを対象とした制御）、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を常に最新の状態に維持するということです。その他にも講じた方がよい事前対応型のソリューションがあります。たとえば、レート制限の設定、CDN におけるコンテンツのキャッシング、さらには DDoS の検知、 緩和、 保護を専門とする製品の使用などがあります。DNS インフラを保護するために、インバウンドの DNS トラフィックを継続的に監視、分析し、従来の DNS ファイアウォールの代わりにハイブリッド型のプラットフォームを使用するという方法も役に立ちます。

ランサムウェア攻撃とワークロードに対するその他のリスクに関しては、ゼロトラスト・ソリューションを導入すれば、水平方向（East ／ West）のトラフィックと垂直方向（North ／ South）のトラフィックの両方をブロックできるため、ネットワークのより深い部分にまで潜り込まれることを阻止できます。また、マイクロセグメンテーションを導入すれば、アプリケーション間のデータフローをきめ細かく可視化し、アクセス要求が信頼できるかどうか、許可できるかどうかを評価できるため、重要なアプリケーションの保護にも役立ちます。最後に、セキュリティチームは MITRE ATT&CK フレームワークを使用して、攻撃者がよく使う手口やテクニックに関する知見を獲得し、それに応じてプレイブックを更新することができます。

図 ： *MITRE ATT&CK® ／エンタープライズ向け ATT&CK マトリックス*

結論：説明を総括する

このレポートでは、攻撃者が多種多様な手口でアプリケーションや API を標的にしている事実を概説してきました。アプリケーションと API に対する需要が天文学的に増えているため、侵入口の数も爆発的に増えています。アプリケーションで実行されるビジネスの数が増えるにつれ、あらゆる面でアプリケーションを保護することが今まで以上に重要になっています。このレポートでは、デジタルトランスフォーメーションを安全に行ううえで重要になるセキュリティ上の考慮事項をまとめて説明してきました。必要不可欠な事前対応型の対策を大別すると次の 3 つになります。

1. **アプリケーションと API**
2. **アプリケーションワークロード**
3. **アプリケーションと API の背後にあるインフラ**

アプリケーションや API に対する攻撃が成功すると、収益や評判に影響を与えるだけでなく、最終的にはコンプライアンスや法規制への違反により高額の罰金を科される可能性もあります。このレポートの最初のセクションで、顧客（またはホームユーザー）に影響を与える攻撃について説明しました。Web 攻撃を受けたり、API を悪用されたりすると顧客の認証情報やその他の個人情報が盗まれ、詐欺の被害にあう可能性があります。次に、事業継続性を題材に、DDoS 攻撃の危険性について説明しました。そして最後に、アプリケーションワークロードに対する攻撃は、攻撃者が（フィッシングやランサムウェアの手口を使って）会社の従業員を標的にし、会社のネットワークに侵入するための足場作りに重点を置いていることを説明しました。

このレポートをお読みいただき、皆様がアプリケーションと API を保護、セキュリティ確保、防御するうえで何かの参考になればと願っています。

最新の脅威に関する情報はセキュリティ・リサーチ・ハブでご確認いただけます。

手法

Web アプリケーションおよびレイヤー 7 DDoS 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）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。保護されている Web サイト、アプリケーション、API 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。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、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作動されます。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。

データ更新について（2024 年版）

10 周年という節目を迎え、この機会に、当社のデータセットの更新について説明します。当社の Web アプリケーション攻撃データセットは数回にわたって更新されています。収集方法について、変更、合理化、最適化を行ってきました。知見の範囲と深さが広がりました。SSRF など、攻撃ベクトルの分類を追加してきました。API エンドポイントを標的にする攻撃の識別も各データシートに追加してきました。これらの改善点の一部は、本レポートでご紹介しました。今後もこの「SOTI ／セキュリティ」レポートを通じて、読者の方々に最新状況を引き続きお知らせしようと考えています。

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。

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。

クレジット

Research director

Mitch Mayne

共同執筆者

Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

校閲およびテーマ別寄稿者

Sven Dummer
Reuben Koh
Tony Lauro
Richard Meeus
Menacham Perlman
Sandeep Rath
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

アプリケーションおよび API 攻撃向けの Akamai ソリューションの詳細については、アプリケーション & API セキュリティページでご覧いただけます。

Akamai は、お客様が生み出すものすべてにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティ体制の適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。

公開日：2024 年 7 月。