SOTI

第 10 巻、第 1 号

10 YEARS
OF SECURITY INSIGHT

影に潜む脅威

攻撃トレンドで API の脅威を解き明かす

Akamai

インターネットの現状／セキュリティ

目次

可視性が重要である理由

今年は、Akamai が 「インターネットの現状 （SOTI） レポート」 でセキュリティ調査を共有し始めてから 10 年目になります。レポートのテーマは年を追うごとに変化し、運用／脅威エコシステムとともに進化しています。2024 年から、Web アプリケーションおよび API 攻撃をひとつの分野として捉えず、新たなデータセットを用いて Akamai の調査担当者が 2 種類の攻撃として区別するようになりました。このレポートでは、API を標的とする Web 攻撃の割合に注目します（詳しくは、「手法」セクションを参照してください）。その割合から、攻撃者がどのように API を攻撃しているか理解を深めて、より効果的な緩和戦略を提示できます。

API は、企業で近年推進されている多くの変化の基盤となっており、従業員体験と顧客体験の両方を改善してきました。しかし残念ながら、このデジタルイノベーションと API エコノミーの急速な拡大は、サイバー犯罪者に新たな悪用の機会を与えることになってしまいました。そのため、API のセキュリティを確保するための可視性が重要になっています。シャドー API やローグ（野良）API などの盲点が明らかになれば、セキュリティチームはそれまで認識していなかった脆弱性に取り掛かることができます。

この 2024 年最初の SOTI レポートでは、従来の Web 攻撃を含む API を標的としたさまざまな攻撃に注目します。データから可視性を得るとともに、ポスチャに関する課題やランタイム（実際の運用時）の課題など、一般的な問題分野を通じて API が悪用される危険を解き明かします。さらに、業界や地域ごとに危険を明らかにすることで、各企業に対するリスクをより正確に評価できるようになります。また、実際のケーススタディをいくつか紹介し、コンプライアンス要件の強化についても触れ、規制トレンドに応じてセキュリティ戦略がどのように変化するのかを解き明かします。最後に、API の状況を可視化するために、全体的なセキュリティポスチャの強化につながるいくつかのステップを提示しています。

本レポートの主な知見

- この 12 か月間（2023 年 1 月～ 12 月）では、全体で 29% の Web 攻撃が API を標的にしており、API はサイバー犯罪者の重点領域となっています。
- API に対する攻撃には、「Open Web Application Security Project（OWASP）API Security Top 10」 お よ び「OWASP Top 10 Web Application Security Risks」で挙げられているリスクが含まれます。攻撃者は、SQL 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）など、効果が実証されている手法を用いて、標的への侵入を果たしています。
- API のふるまいのベースラインを確立せずに異常な API アクティビティを検知することは困難であるため、ビジネスロジックの悪用が重大な懸念事項となっています。API アクティビティの異常を監視するソリューションを持たない組織は、データスクレイピング（認可された API を使用して内部からデータをゆっくりとスクレイピングする、新しいデータ漏えいベクトル）などのランタイム攻撃のリスクにさらされています。
- API は現在、ほとんどのデジタルトランスフォーメーションの中核となっています。そのため、ロイヤルティ詐欺、悪用、認可、カーディング攻撃など、業界の動向や関連するユースケースを把握することが非常に重要です。
- 組織は、再設計を避けるために、セキュリティ戦略プロセスの初期段階で、コンプライアンス要件や新たな法規制を考慮する必要があります。

API：大きな攻撃ベクトル

本質的に、API はデータを仲介するものです。そのため、脆弱性やビジネスロジックに対する攻撃で不正アクセスを許すと、攻撃者にデータがさらされることになります。2021 年に、Gartner® は、API の悪用とデータ漏えいが 2024 年までに倍増すると予測しました。そして今、大規模な API インシデントはかつてないほど一般的になっています。実際に、昨年、セキュリティリスクのトップ 10 ランキングで知られる非営利団体の Open Web Application Security Project（OWASP）は、API 特有のリスクに着目したリストとして分けた OWASP API Security Top 10 を公開し、API がもたらす固有の脅威を明らかにしました。

Akamai リサーチは、API が従来型の攻撃と API 特有の攻撃テクニックの標的になっている事実を確認し、複合的な保護対策の必要性を指摘しています。実際、2023 年 1 月から 12 月にかけて Web 攻撃全体の約 30% が API を標的にしていました（図 1）。API に対する需要が拡大する中で、組織が API を適切に保護したり、組織内のすべての API を把握しない限り、こうした攻撃は今後ますます増加すると考えられます。アタックサーフェス全体を把握するためには、まず API の包括的かつ正確なインベントリーを確立する必要があります。

月別の Web 攻撃数

2023 年 1 月 1 日～ 2023 年 12 月 31 日

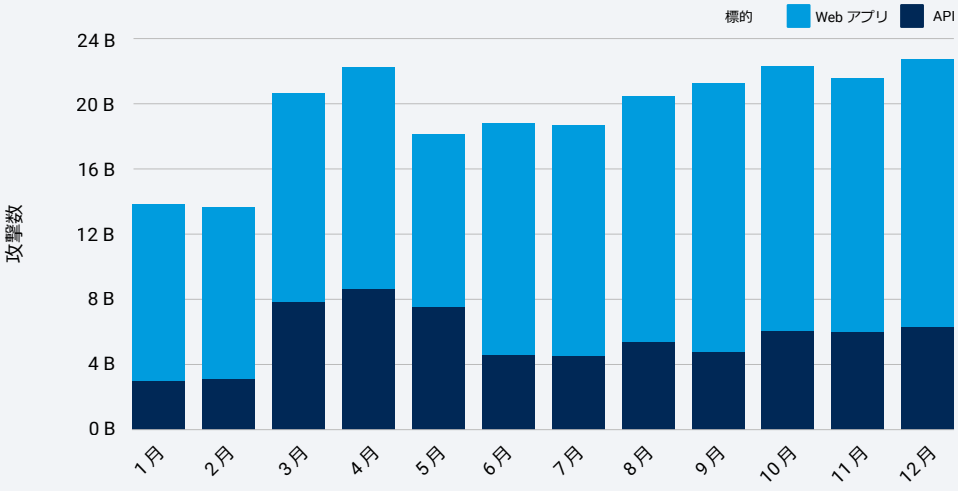


図 1 ： API に対する Web 攻撃の割合は、 2023 年 1 月の 22% から 12 月には 28% に増加しており、 3 月から 5 月にかけて多少の変動が見られた

また、世界各地で興味深い動向も確認しています。ヨーロッパ・中東・アフリカ（EMEA）地域では、API を標的とする Web 攻撃の割合が最も高く（47.5%）、北米（27.1%）とアジア太平洋・日本（APJ）地域（15%）がそれに続きました。国レベルでは、スペイン（94.8%）、ポルトガル（84.5%）、オランダ（71.9%）、イスラエル（67.1%）が上位となっています。これに対して、米国では、API を標的とする Web 攻撃の割合は 27.6% にとどまりました。

このように地域ごとに攻撃の差が生じるのは、規制環境、地理的な緊張、インフラの種類、アクセスと教育の違い、ビジネスモデル、社会的な要因など、多くの理由があります。しかし、重要な点として、サイバー攻撃は 1 つの地域や業界で発生した後、他の地域や業界に伝播していく傾向があります。そのため、幅広いトレンドを追跡すると有益です。地域ごとの動向の詳細については、このレポート内の APJ スナップショットと EMEA スナップショットを参照してください。

攻撃を受ける API

攻撃者が企業の API をどのように標的にし、どのような手法を頻繁に使用しているかを調査することで、重視すべき防御分野が明らかになります。過去 12 か月で、攻撃者は HTTP プロトコル（HTTP）、SQL インジェクション（SQLi）、データハーベスティング攻撃を好んで使用していました（図 2）。HTTP 攻撃では、攻撃者はさまざまなプロトコルの脆弱性を悪用し、機微な情報の読み取りやクライアントまたはサーバーのスプーフィングなど、悪意のある活動を仕掛けています。その他の一般的な手法にアクティブセッションがあります。疑わしいトラフィックにはフラグを立ててセッションの間ブロックされます。一方、データハーベスティングは、名前から想像できるように、情報の収集に関連する攻撃です。攻撃者は収集した情報をその後の別の攻撃に利用できます（このレポートの最後にある付録で、すべての攻撃ベクトルの定義のリストをご覧ください）。

当社が持つ最新のデータセットを用いると、API に対するその他の攻撃ベクトルも監視できるようになります。その良い例として、サーバーサイド・リクエスト・フォージェリ（SSRF）は、昨年の SOTI「セキュリティギャップのすり抜け」で紹介した最新ベクトルの 1 つであり、機密情報の取得やコマンドの実行のために使用されます。

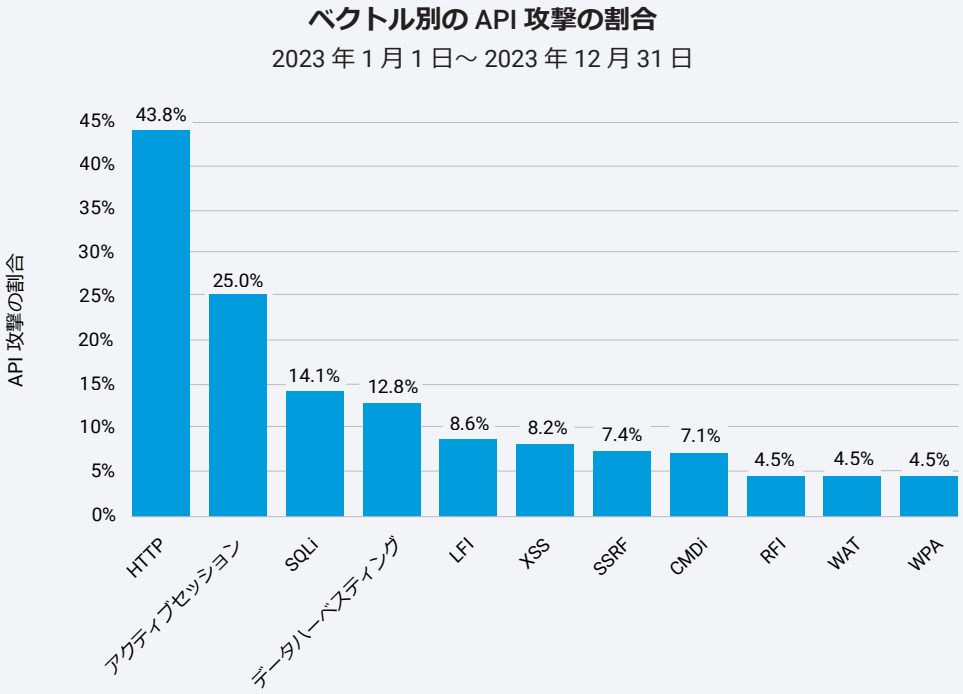


図 2：ローカル・ファイル・インクルージョン（LFI）は API の上位ベクトルではないが、意図した標的への侵入に使用されるため、依然として考慮すべき領域である。Web アプリケーションと API に対する攻撃の分布を詳しく見ると、LFI が攻撃ベクトルで依然として上位であることがわかる

当社の調査から、ボットリクエストにも懸念があることがわかりました。Akamai のデータによると、2023 年には、全世界で約 3 分の 1 の不審なボットリクエストが API を標的にしていました。すべてが悪性とは限りませんが、こうしたボットリクエストは、情報の窃取を目的とした Credential Stuffing 攻撃やデータスクレイピングに利用されます。

私たちはこれらの攻撃タイプに注目し、企業が追跡して侵入テストチームやレッドチームに検証させるべき直接攻撃が、OWASP API Security Top 10 におけるアクセスに対する攻撃やデータ悪用／スクレイピング、設定ミスに留まらず、依然として多発していることを突き止めました。

API セキュリティの実環境での教訓

Akamai は、世界中のエンタープライズと協力して API の使用に関する詳細な情報を収集し、高度なふるまい分析を実施して、セキュリティ脆弱性と API の悪用を示す指標を導き出しています。こうした API 活動を分析した結果、ポスチャに関する問題とランタイムの問題という特徴の異なる 2 つの問題があることを確認しました。

1. **ポスチャの問題**とは、企業の API の実装上の欠陥に関することです。ポスチャに関する問題を警告するアラートにより、セキュリティチームは、優先度の高い脆弱性を攻撃者に悪用される前に特定して対処できます。

2. **ランタイムの問題**とは、緊急対応を要するアクティブな脅威やふるまいのことです。本質的に重要なこれらのアラートは（より明確なインフラ侵害の試みとは異なり）API の悪用という形を取るため、その他のセキュリティアラートよりも繊細な内容になります。

最も一般的なポスチャに関する問題

私たちが確認した最も一般的なポスチャに関する問題を以下にまとめます。これらの問題を放置した場合に企業に起こり得る影響についても簡単に説明しています。

シャドーエンドポイント

シャドーエンドポイントとは、廃止または文書化されていない古くなった API や以前のバージョンの API のことです。ゾンビ、ローグ、またはレガシー API とも呼ばれ、組織の標準的なセキュリティ制御や対策の対象から外れているため、悪用されるリスクが高くなります。

未認可のリソースへのアクセス

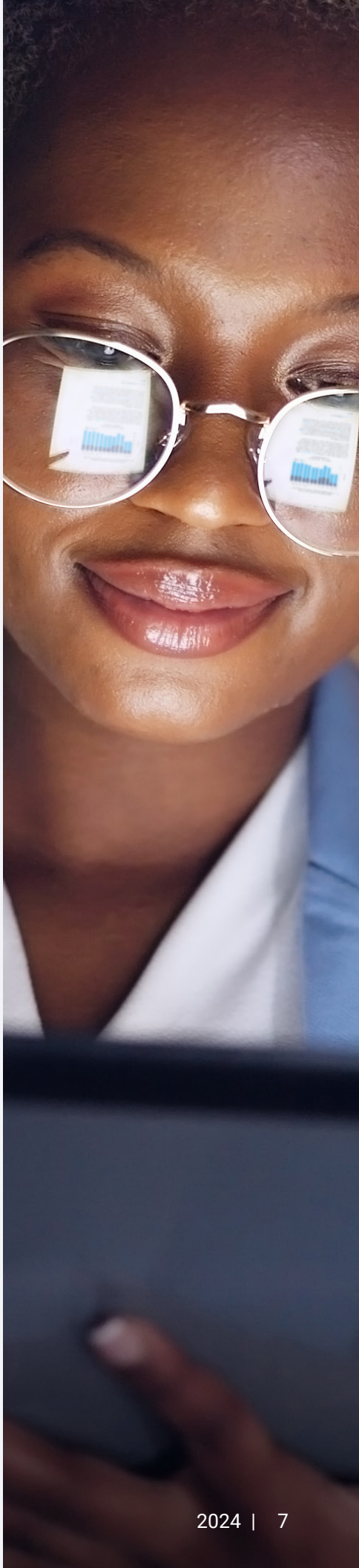
未認可のリソースへのアクセスは、ユーザーやシステムがいかなる形式でも認証を一切提供しないまま API リソースにアクセスできる状況のことです。多くの場合、API の導入や設定の結果が原因で発生します。多くの未認可リソースは、隠ぺいのために非表示になっていますが、そのリソースを発見した攻撃者が悪用し、機微な情報やアプリケーション機能にアクセスする可能性があります。

URL 内の機微な情報

時として、パスワード、認証トークン、クレジットカードの詳細、個人を特定できる情報（PII）などの機微な情報が API リクエストの URL に記載される場合があります。URL 内のデータは、攻撃者がアクセスできる場所（ログやキャッシュなど）に保存されることもあり、機微な情報の漏えいやコンプライアンス問題に発展する重大なリスクが生じます。

寛容な CORS ポリシー

寛容なクロスオリジン・リソース・シェアリング（CORS）ポリシーは、API が必要以上に幅広いオリジン（プロトコル、ドメイン、ポートなど）からのリクエストを許容する状況です。ポリシーが寛容すぎると、信頼されていないソースから攻撃者が機微なリソースに容易にアクセスしたり、クロスサイトスクリプティング（XSS）などの攻撃を容易に仕掛けられるようになります。



過剰なクライアントエラー
異常に多数の API リソースリクエストの失敗が観測される場合、過剰なクライアント・エラー・アラートが生成されます。クライアントサイドエラーの多くは設定ミスや悪意のないエラーが原因ですが、過剰なクライアント・エラー・アラートは、攻撃者が API 導入環境の脆弱性を探索していることを示す可能性があります。

最も一般的なランタイム問題

観測したランタイムアラートでも同様の分析を行った結果、以下のようなアクティブな脅威の可能性を示す一般的な API セキュリティ問題が明らかになりました。

未認可のリソースへのアクセス試行
これは、前述した認可されていないリソースアクセスのポスチャアラートの、より緊急性の高い派生型です。適切な認証なしで機微な API リソースへの具体的なアクセスの試行がみられます。たとえその試行が失敗したとしても、API の脆弱性を発見して悪用しようとするアクティブな活動であったことを示しており、即座に介入しないと、いずれ成功する可能性もあります。

異常な JSON プロパティ
予期しないデータタイプ、異常なサイズ、過度に複雑な構成など、異常な JSON ペイロードを使用する API 活動は、API の脆弱性を悪用しようとするアクティブな活動を示しています。この活動は、インジェクション攻撃、サービス妨害、データ窃取、API ロジック欠陥の悪用など、さまざまな悪性の行為を実行する試みと捉えることができます。

パス・パラメーター・ファジングの試み
パス・パラメーター・ファジングは、API リクエストの一部として予期しないまたは不正なデータを故意に送信するもう 1 つの例です。RESTful API が特定のリソースや操作を指定するために使用する URL の一部が主に対象となります。攻撃者が偵察として脆弱な API を探索し、データ窃取やサービスの混乱を仕掛けるためのテクニックと言えます。

不可能なタイムトラベル
API 活動を分析する際に、タイムスタンプ、ジオロケーション、API コールのシーケンスが論理的になっていない場合があります。これは、攻撃者が何らかの方法でそれらを操作しようとした兆候と考えられます。さらに、こうしたふるまいは、不正行為の一部であるデータ操作など、複数の脅威を示す場合もあります。

データスクレイピング

データスクレイピングとは、API からデータを自動的に抽出する操作のことです。API の意図した用途やサービス規約と一致しない方法と規模で行われます。攻撃者はこのデータをゆっくりと収集することで、検知を回避し、知的財産を盗み出し、機微な顧客情報を収集し、何らかの利益を得ます。検知されない場合、この Low & Slow（少しずつ時間をかけた）のデータスクレイピングは、大規模なデータ漏えい攻撃に発展する可能性があります。

最後に、ポスチャに関する問題とランタイムの問題について検討する際は、一歩戻って、以下の API が直面する 3 つの一般的な課題を確認することをお勧めします。

1. **可視性** — すべての API をプログラムで確実に保護するためのプロセスと技術的な制御を備えていますか？これは重要な問題です。なぜなら、API は DX や新製品の部品として組み込まれるため、その多くは従来の Web プレゼンスと同じレベルの管理、保護、検証体制を維持できないからです。

2. **脆弱性** — API は開発のベストプラクティスに従っていますか？ OWASP の最も一般的なコーディング不良の問題を回避していますか？さらに、脆弱性を追跡／確認していますか？

3. **ビジネスロジックの悪用** — 想定されるトラフィックのベースラインがありますか？疑わしい行為のベースラインを確立していますか？

API の可視性を確保し、調査を実施できる体制を整えて、脅威を速やかに緩和するためのプロセスを確立することが重要です。これについては、顧客向けの API でも社内 API でも同様です。

業界動向がサプライチェーン攻撃の危険性を浮き彫りに

API は、組織におけるデジタルトランスフォーメーションの中心になっています。しかし、API の存在によって、ビジネスに対するリスクが高まり、大規模なセキュリティ課題に直面することになります。レポートの対象期間において、API を標的とした Web 攻撃の 44.2% がコマース業界に対するものであり、ビジネスサービス業界に対する攻撃が 31.8% で 2 位でした（図 3）。コマース業界が特に多いのは、複雑なエコシステム、API への依存度の高さ、大量の機微な顧客情報など、多くの要因が原因です。

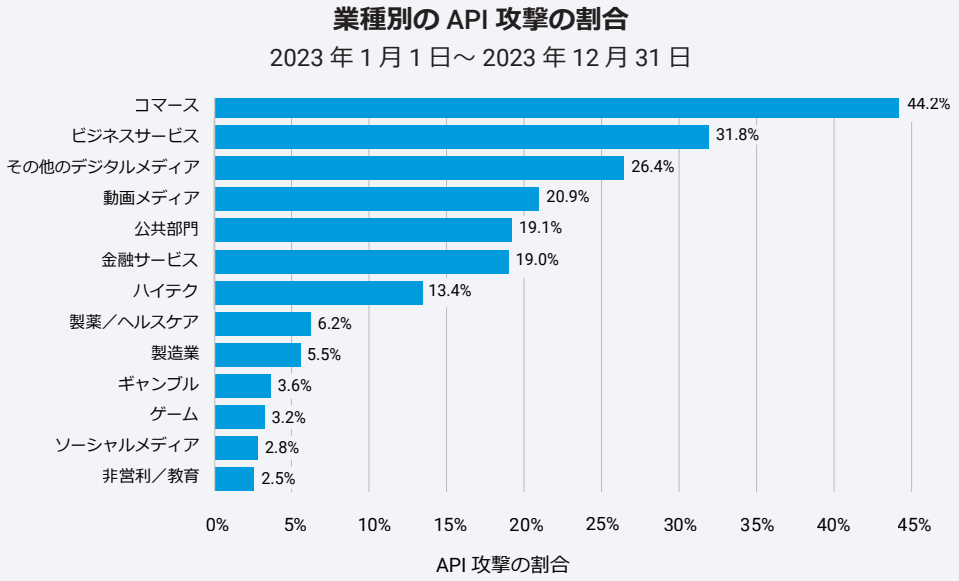


図 3：コマース業界とビジネスサービス業界は、2023 年に最も多くの API 攻撃を受けた。米国の金融サービスは、EMEA の金融サービス業界とは異なり、オープンバンキングを導入していないため、トップ 5 にも入っていない

ビジネスサービスが 2 位にランクしている事実は、サプライチェーン攻撃で想定される危険を考えると、憂慮すべき事態です。ビジネスサービスを提供するサードパーティ企業は、系列組織に関する機微な情報を保有しているか、その組織の環境にアクセスできる可能性があります。そのため、攻撃者が付加価値の高い標的への経路として利用することが考えられます。

データをさらに詳しく精査した結果、API 攻撃を回避できる業界はそもそも存在しないことがわかりました。たとえば、ヘルスケア業界では、医療業界におけるモノのインターネット（IoMT）が爆発的に普及し、データの相互運用性を確保するために API の使用が増加しています。ヘルスケア業界は大きなリスクにさらされており、ヘルスケアにおける API のセキュリティへの影響は、まだ完全には把握できていません。

ケーススタディ

さまざまな業界に対して、どのようなタイプの攻撃が実際に発生しているか確認してみましょう。実環境での組織と顧客に対する影響も含めて、複数のケーススタディを紹介します。

コマース業界でのロイヤルティ詐欺

攻撃者は、実世界の商品や現金に交換できるポイント、マイル、クレジットなど、価値のある通貨を扱うロイヤルティプログラムのアカウントを標的にしています。Akamai は、5 つ以上のロイヤルティアカウントにアクセスするユーザーの API のふるまいを検知しました。調査の結果、このふるまいがアカウント内の詐欺行為だと特定しました。ほとんどのアカウントは、承認された少数のユーザーしかアクセスしません。そのため、複数のアカウントにアクセスするユーザーは、不正行為に及んでいる可能性があります。詐欺を減らすには、通常のふるまいと不正なふるまいの違いを理解することが最善と言えます。

SaaS 通知サービスでの API の悪用

Akamai Hunt チームは、金融サービス企業による SaaS 型の通知システムで API が悪用されている事実を確認しました。ペイロード内の認可ヘッダーと署名が欠落しているため、企業はシステム内で誰がリクエストを行ったのかをチェックしたうえで通知を送信することができていませんでした。つまり、API にアクセスできるユーザーであれば、誰でも API を悪用し、企業の従業員や顧客にメッセージを送ることができます。

BOLA 攻撃の可能性

同チームは、ある航空会社でオブジェクトレベルの認可の不備（BOLA）攻撃の可能性を確認しました。約 200 個の IP を持つ認証済みのユーザーが {customer_id} パスパラメーターをファジングし、提供したパラメーターが有効であれば機微なユーザー情報が返されます（図 4）。この ID は単純な整数だったので、ファジングは非常に容易であり、顧客情報のデータ窃取に発展する可能性があるため、影響は甚大でした。API は、姓、名、ミドルネームとともに、政府機関の ID、国籍、居住国、生年月日など、機微な情報を返すために利用されました。

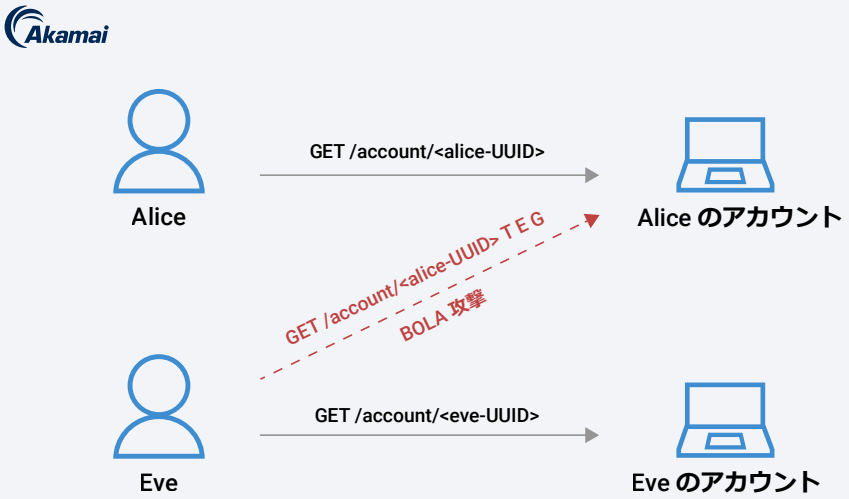


図 4：BOLA 攻撃が発生し、攻撃者はアクセス認証されていないリソースへのアクセスを試みて、機微な情報を盗み出そうとしている

日常に潜むカーディング攻撃

異常な API トラフィックからスタートし、カーディング攻撃に発展したケースを紹介しましょう。当初、影響を受けた組織は API トラフィックの急増に惑わされ、分散型サービス妨害（DDoS）攻撃だと考えました。その後、詳細な調査の結果、カスタマーシステムが正否を応答する（有効か否か）クレジットカードの有効性を確認する試みだと判明しました。カーディング攻撃では、攻撃者は盗難したクレジットカード番号をまず検証します。カードの正当性を確認できれば、攻撃者はダーク Web マーケットで売却するか、他の不正取引を悪用します。

API 攻撃を理解することが重要である理由

ほとんどの API 環境に存在する一般的なビジネス問題には、プログラミングエラーや設定ミスがあり、API セキュリティプログラムの探索段階で検知されます。こうしたエラーの大部分は悪用されませんが、セキュリティ チームが API アセットと各 API で実行されているトラフィックを可視化すると、潜在的な被害が明らかになります。

API を利用するアプリケーションやビジネスプロセスを立ち上げて展開するスピードは、多くの場合、セキュリティチームがセキュリティポスチャを評価するスピードを上回ります。その結果、必然的に設定ミスや脆弱性が発生します。さらに、ほとんどの組織は API セキュリティの専門知識が不足しており、受け入れ難いセキュリティ方程式のすべての変数は流動的なままです。

> **API セキュリティのエラーが発生する条件**
>
> API を使用した、ビジネスクリティカルなプロセスの展開を急いでいる ＋ API の可視性が欠如している ＝ API の設定にミスがある、または API が脆弱

データ漏えいを防ぐためのベストプラクティス

API の未知の脆弱性は長期にわたって悪用され、多くの場合はプログラミングエラーと深く関連しています。現在、公開されている API に関するデータ漏えいは珍しくありません。これは、攻撃者が API エステートを悪用し、偵察によって悪用する API を選別していることを示します。このような偵察行為と、自動化されたデータスクレイピングの脅威により、API は新たなデータ漏えいベクトルになっています。このように攻撃が成功すると、ブランドや評判にダメージを受け、機微な情報の損失や顧客の信頼の喪失、さらに地域によっては、コンプライアンスや規制違反の対象となり、金銭的な損失につながる可能性もあります。そのため、API セキュリティがかつてないほど重要になっています。

API のデータ漏えいが発生する条件

本番環境で API の設定にミスがある、または API が脆弱	+	データスクレイピングによる自動化された脅威（ボット）	=	数週間、数か月間にわたる、少しずつ時間をかけたデータ漏えい

API の脆弱性によるデータ漏えいを阻止する最初の重要な一手は、正常な状態とどのデータがどの API にあるのかを正しく認識したうえで、環境に対する可視性を確保することです。これには、すべての API をセキュリティ制御の管理下におき、攻撃の緩和またはセキュリティオペレーションチームへのアラート通知のために自動応答を設定することが含まれます。次に、開発段階でシフトレフトテストを実施し、こうした脆弱性や弱点を攻撃者が悪用する前にいち早く解決します。最後に、防止策と危機対応の両方を検証するために、試験運用を行う必要があります。

Kong のアナリストが関わった **2023 年**の調査によると「API 攻撃による米国の被害額は…現時点で 106 億ドル、2030 年までに年間 1,980 億ドルに急増する」とされています。

コンプライアンスの考慮事項

従来のエンタープライズセキュリティとリスク管理の観点から、API の保護と、攻撃の新たなベクトルとなるこれらの侵入口の遮断が急務であることは明白です。加えて、セキュリティとデータ保護に関連する最近の法律や執行措置に関する傾向を見ると、API のセキュリティと可観測性の問題に対処しなければならない理由に説得力が増します。

セキュリティは世界各国のデータ保護法において、必ずその一部を担っています。優れたセキュリティなくして優れたプライバシーは得られないからです。たとえば、欧州連合の一般データ保護規則（GDPR）第 32 条では、PII を処理する事業者に対し「リスクに応じたセキュリティレベルを確保するために、 適切な技術的、 組織的対策を実施すること」を求めています。他の法律にも同様の要件が含まれており、たとえばカリフォルニア州プライバシー権法（CPRA）には「合理的なセキュリティ手続きと慣行」を実施し、PII の機密性、完全性、可用性を保護するために適切な措置を講じることが記載されています。

規制や執行措置にも、透明性と説明責任のレベルを上げる傾向が見られます。たとえば、米国証券取引委員会（SEC）は最近、公開企業を対象に重要なセキュリティインシデントのほか、リスク、セキュリティガバナンス、監視に関する詳しい情報の開示を義務付ける新しい規則を制定しました。

世界中で、PII の保護を怠った企業に罰金が科されるようになっています。たとえば、SEC は最近、既知のサイバーセキュリティリスクと脆弱性に関連して不正行為と内部統制の不備があったとして、SolarWinds の CISO を訴えました。この訴訟では、SolarWinds とその CISO がサイバーセキュリティの慣行を誇張し、既知のリスクを過小評価したり、開示しなかったりして投資家を欺いたと主張しています。

このように、API だけを対象にした法律や規制はほとんどありませんが、API について言及したり、企業にコンプライアンスを促したりする法律や規制は数多くあります。たとえば、欧州連合（EU）の改訂版決済サービス指令（PSD2）や米国の 21 世紀の治療に関する法律では、ヘルスケアプロバイダーが API を使用する際の透明性要件が厳格化されています。問題は、関連データが高度に規制されている一方でサイバー犯罪者に狙われやすいという点です。それを受けて、米国国家規格協会（ANSI）などの団体がガイドラインを策定し、国際標準化機構（ISO）と国際電気標準会議（IEC）が ISO/IEC 27001 を定めました。Payment Card Industry Data Security Standard（PCI DSS）v4.0 のような新しい規制にも、API に関する内容が含まれています。技術的な側面については、OWASP（Open Web Application Security Project）がトレーニング資料として優れています。まとめると、探索、監視、調査、修復が可能なシステムを構築すれば、コンプライアンス要件にマッピングできるようになるということです。

こうした法的措置の流れによってサイバーセキュリティプログラムの水準が上がる中、透明性と説明責任も進化を続ける必要があります。企業の API 領域における可視性の欠如と、それに付随するセキュリティポスチャの穴（見えないものは守れない）は、深刻な法的および規制上の問題を引き起こす可能性があります。

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 API 攻撃の動向に関する詳細については、次のセクションの地域別レポートをご覧ください。

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 API セキュリティ SOTI レポート「影に潜む脅威：攻撃トレンドで API の脅威を解き明かす」（英語版のみ）の姉妹編です。今回のスナップショットで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、当社の調査方法と新しいデータセットに関する説明については、同レポートをご参照ください。

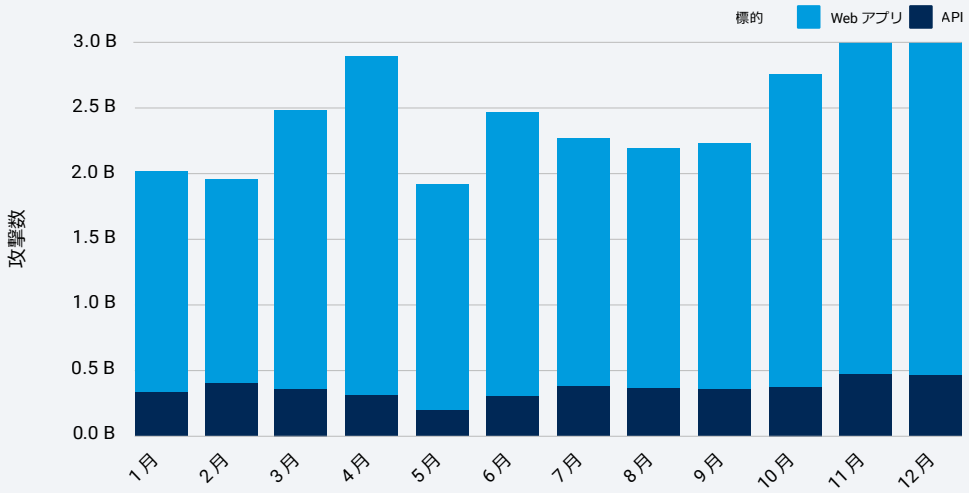
APJ における注目すべき API 攻撃

API 攻撃のトラフィックを追跡する新たなデータセットを Akamai の調査に活用したところ、アジア太平洋・日本（APJ）地域の Web 攻撃すべてのうち 15.0% が API を標的にしていたことが判明しました。世界規模で見ると、アジア太平洋・日本（APJ）地域は API 攻撃の割合が 3 番目に高く、これは、ヨーロッパ・中東・アフリカ（EMEA）地域の 47.5% と北米の 27.1% に次いで高い数値です。

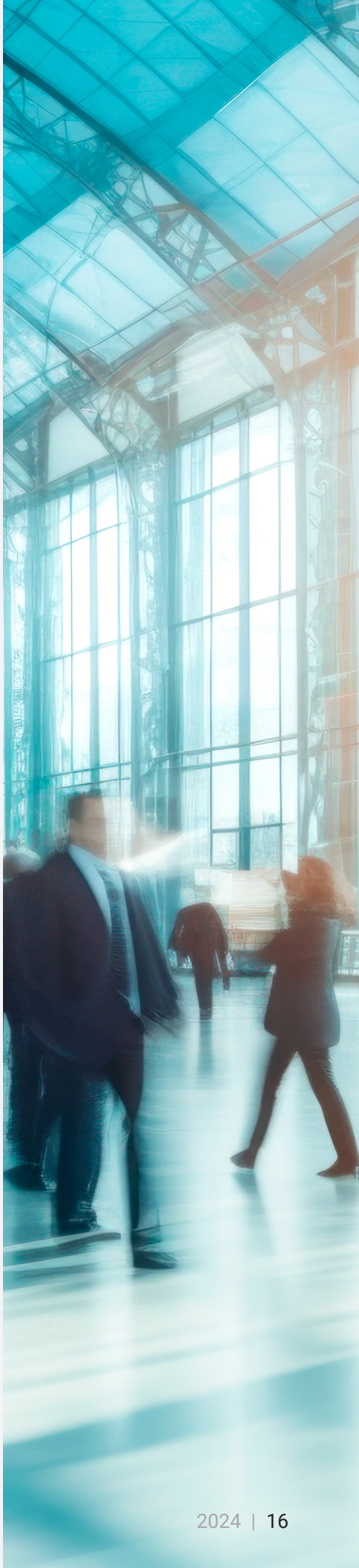
2023 年 1 月から 12 月までのレポートの期間中、API を標的とする Web 攻撃は、各月 11% から 21% の間で変動していました（APJ 図 1）。他の地域における攻撃の割合と比較してかなり低い理由の 1 つは、APJ ではオープン API の市場規模がヨーロッパおよび北米よりも比較的小さいため、API を保護対象にしている組織の割合が低いことにあるのかもしれません。

APJ：月別の Web 攻撃数

2023 年 1 月 1 日～ 2023 年 12 月 31 日



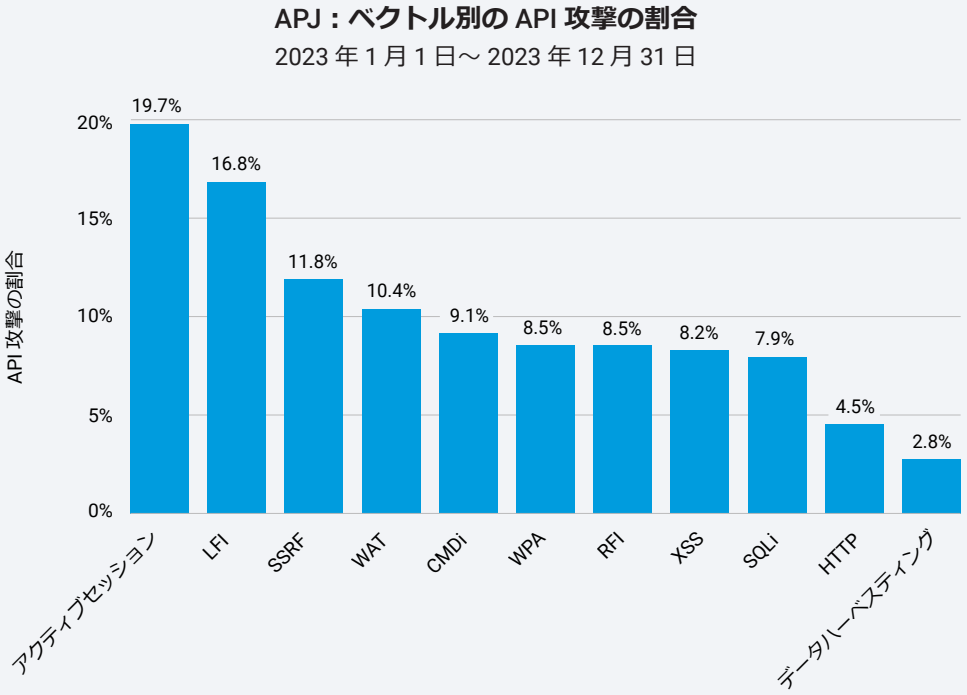
APJ 図 1：Web 攻撃全体が増加していても、API を標的にした攻撃の占める割合は平均 15.0%



APJ 内で API を標的とする Web 攻撃の割合が高い国は、韓国（47.9%）、インドネシア（39.6%）、香港（38.7%）、マレーシア（26.4%）、日本（23.4%）、インド（19.0%）、オーストラリア（15.6%）、シンガポール（5.8%）、フィリピン（5.5%）、ニュージーランド（4.8%）です。

攻撃を受ける API：トラフィックの分析

Web 攻撃全般を調査した以前のレポートと同様に、LFI は、依然として APJ に蔓延している API の攻撃ベクトルです。しかし、API 攻撃に絞って見ると、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）は下位にランク付けされます（APJ 図 2）。



APJ 図 2：LFI は依然として多く使用されている攻撃ベクトル。新しいデータセットから、その他によく使用されている API 攻撃の手法が判明した

当社は、新しいデータセットを活用することで、よく使用される API 攻撃ベクトルを見つけ出すことができます。たとえば、コマンドインジェクション（CMDi）は API 攻撃でよく使用される手法であり、サーバーサイド・リクエスト・フォージェリ（SSRF、2023 年のレポートに記載）も現在最も頻繁に使用されるベクトルです。注目すべきは、アクティブセッションがセッション中に不審なふるまいを示すことです。その結果、一時的にブロックされるようになりました（グローバルレポートの最後にある付録で、すべての攻撃ベクトルの定義のリストをご覧ください）。

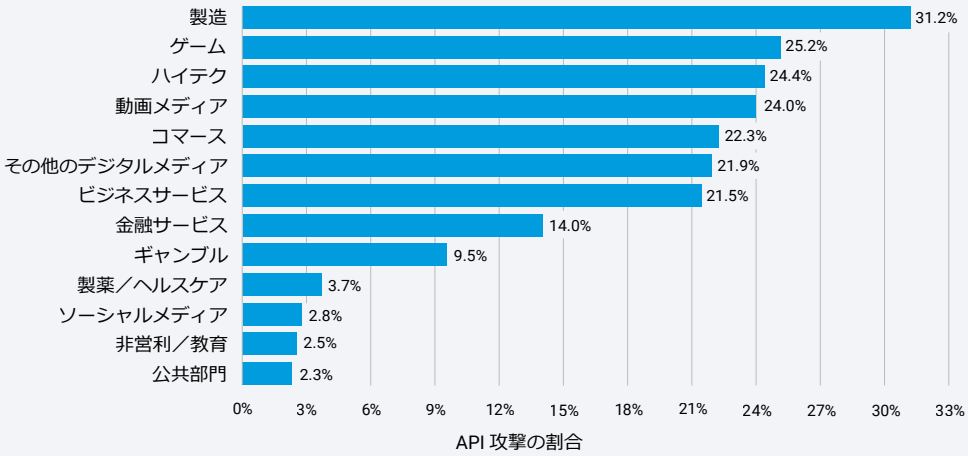
当社の調査から、ボットリクエストにも懸念があることがわかりました。12 か月間の同一レポート期間において、2 兆以上の不審なボットリクエストを検出しましたが、その 40% が、API を標的にしていました。

業界別の API 攻撃

Akamai の調査担当者の調査によると、同一レポート期間における割合の高い API 攻撃は、製造業（31.2%）、次いで、ゲーム（25.2%）、ハイテク（24.4%）、動画メディア（24.0%）、コマース（22.3%）となりました（APJ 図 3）。

APJ：業種別の API 攻撃の割合

2023 年 1 月 1 日～ 2023 年 12 月 31 日



APJ 図 3：API 攻撃の割合が最も高いのは製造業。その原因の 1 つとしては、重要なインフラであるこの業界において API を介した接続が増加していることや、サプライチェーンが混乱している可能性があることなどが考えられる

APJ スナップショットの結論

セキュリティとリスク管理の観点からすると、API の防御が必須であることは明らかです。既存の法規制や、脅威の状況に合わせてサイバーセキュリティ関連法規を維持するための新しい動きもまた、API の保護を不可欠にしています。

たとえば、インドでは IT 法を大幅に刷新する Digital India Bill を起草し、2023 年 8 月に Digital Personal Data Protection Act が議会を通過しました。オーストラリア政府は、2023 年 11 月 23 日に 2023-2030 Australian Cyber Security Strategy を発表しました。この戦略は、安全なテクノロジーを重視し、デジタル製品とソフトウェアの信頼を確保することを柱としています。今後施行される Payment Card Industry Data Security Standard(PCI DSS)v4.0 の Section 6 には、データ侵害リスクの低減を目的とする、システムやソフトウェアの開発と保守における API 使用方法に関する新しい基準が含まれています。

規制当局は、財務上の機密情報交換において API の使用が増加していることを受けて、サイバーセキュリティ基準を強化するための取り組みと指針を策定しています。可視性の向上、防御の強化、コンプライアンス要件へのマッピングを目的としたセキュリティプログラムに API を組み込むうえで、ベストプラクティスとガイドラインの理解は重要です。

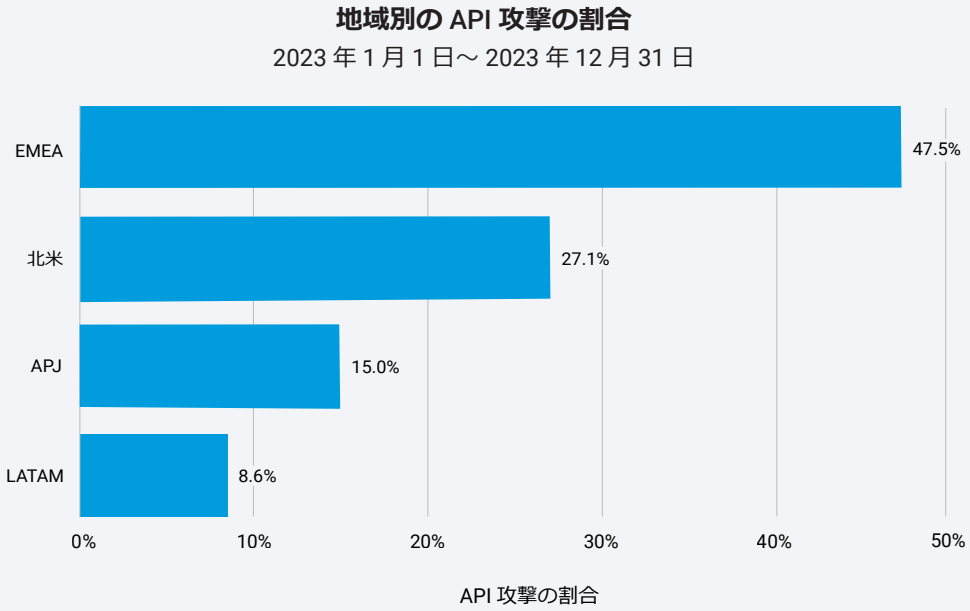
詳しくは、グローバルな SOTI レポート「影に潜む脅威：攻撃トレンドで API の脅威を解き明かす」をご覧ください。

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 API セキュリティ SOTI レポート「影に潜む脅威:攻撃トレンドで API の脅威を解き明かす」（英語版のみ）の姉妹編です。今回のスナップショットで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、当社の調査方法と新しいデータセットに関する説明については、同レポートをご参照ください。

EMEA で広まっている API 攻撃

Akamai が API 攻撃トラフィックに焦点を当てて追跡する新しいデータセットを活用して調査したところ、ヨーロッパ・中東・アフリカ（EMEA）地域では API 攻撃の割合が 47.5% と世界で最も高く、2 位の北米地域の 27.1% を大きく上回っていることが明らかになりました（EMEA 図 1）。この数値は各地域における Web 攻撃の総数に基づいており、EMEA では API が他の地域よりも危険にさらされていることを示しています。



EMEA 図 1：EMEA では他の地域よりも API を標的とする Web 攻撃が非常に多い

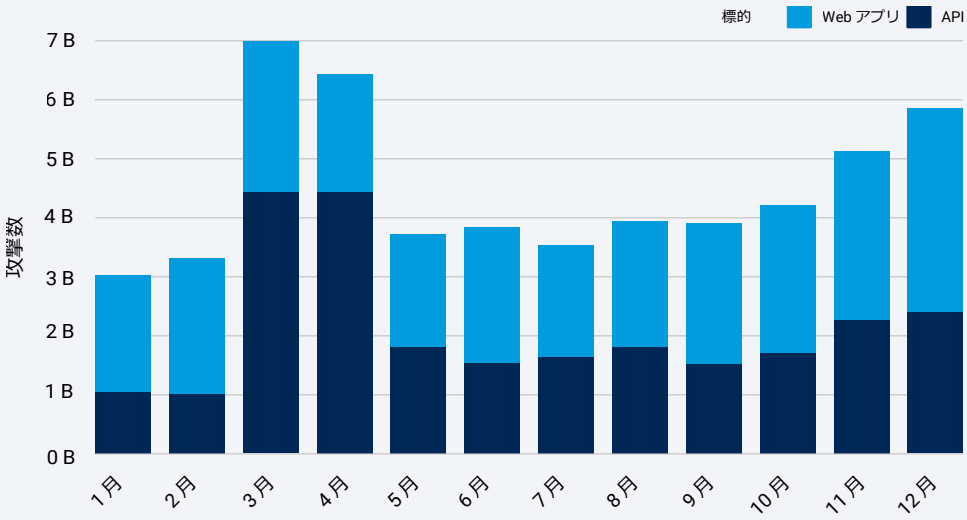
EMEA で攻撃の割合が（他の地域に対する攻撃の割合と比較して）高いのは、北米やアジア太平洋地域よりもオープン API の市場規模が大きい点、EMEA における API の導入率の高さに加え、オープンバンキングや Payment Card Industry Data Security Standard(PCI DSS)v4.0 が API の利用を促進していることが、グローバルレポートで取り上げたセキュリティリスクを引き起こしている可能性がある点が考えられます。

EMEA の中で、API を標的とした Web 攻撃の割合が特に高い国は、スペイン（94.8%）、ポルトガル（84.5%）、オランダ（71.9%）、イスラエル（67.1%）です。このことが示しているのは、これらの国は Web 攻撃全体の数が EMEA の他の国々よりも多いということではなく、むしろ攻撃者が API の攻撃ベクトルに焦点を当てているため、API の悪用をより集中的に受けるリスクを抱えているということです。

2023 年 1 月から 12 月までのレポート期間における月次動向を見ると、EMEA における API を標的とした Web 攻撃の割合は着実に増加しており、1 月には 34% だったのが、年末には 41% まで上昇しています（EMEA 図 2）。ただし、API 攻撃の急増が Akamai の調査担当者によって確認された 3 月と 4 月は例外で、この時期はすでに API 攻撃が集中していたスペインにおいてコマースセクターが大規模かつ集中的な攻撃を受けました。攻撃が急増したことは、攻撃者が地域間や業界間でいかに素早く攻撃対象を切り替えることができるかを示しており、より広範な傾向を追跡する価値が認められます。

EMEA：月別の Web 攻撃数

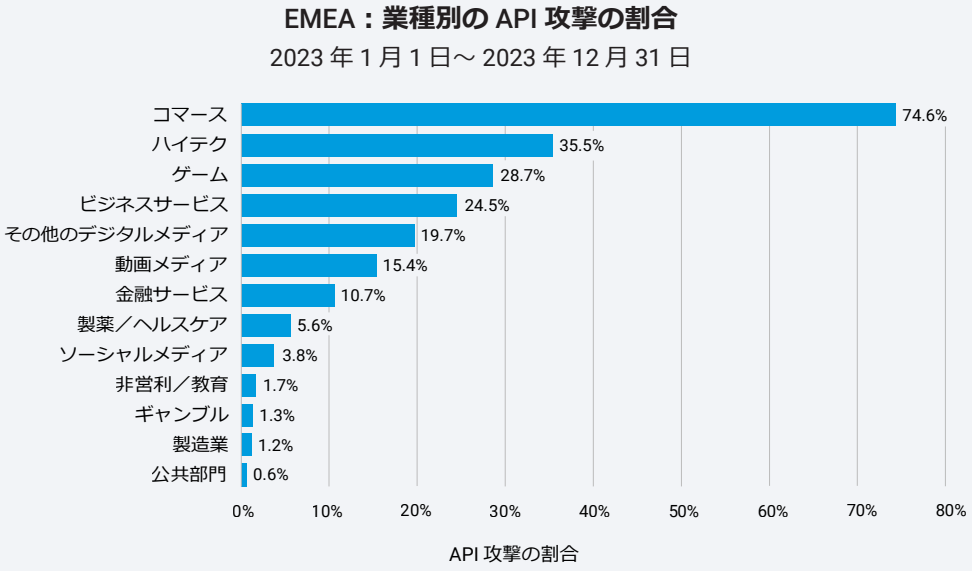
2023 年 1 月 1 日～ 2023 年 12 月 31 日



EMEA 図 2：API 攻撃は急増した 3 月と 4 月を除き、2023 年を通じて徐々に増加し、年末には全攻撃の 41% にまで上昇

業界別の API 攻撃

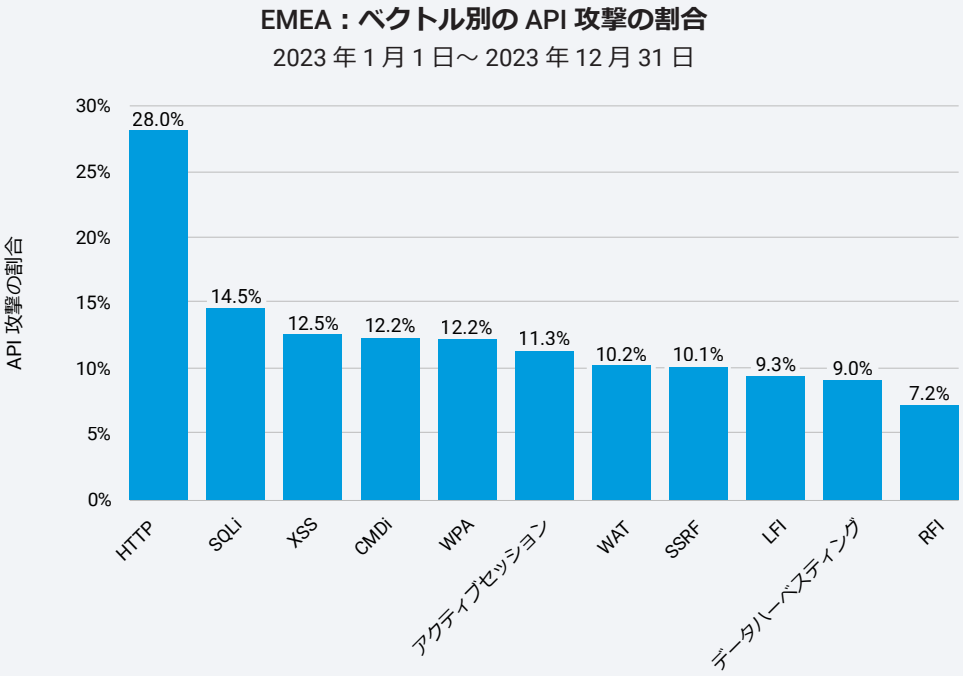
Akamai の調査結果によると、レポート期間中に発生した Web 攻撃全体のうち組織が影響を受けた API 攻撃の割合は、コマース業界が 74.6% と最も高く、2 位のハイテク業界（35.5%）の 2 倍以上となっています。次いで、ゲーム業界が 28.7%、ビジネスサービス業界が 24.5%、その他のデジタルメディア業界が 19.7% でした（EMEA 図 3）。



EMEA 図 3：API 攻撃の割合が最も高かったのはコマース業界。その原因の 1 つとして、エコシステムの複雑さ、API への依存度の高さ、組織が保有しているデータの価値の高さが挙げられる

攻撃を受ける API：トラフィックの分析

この 1 年間に攻撃者が API 攻撃をしかける主な方法として、EMEA では HTTP プロトコル攻撃（HTTP）と SQL インジェクション（SQLi）を使用しており、世界全体で同じ傾向が認められます。Web アプリケーション攻撃でよく使用されるローカル・ファイル・インクルージョン（Local File Inclusion：LFI）は、下位になっています（EMEA 図 4）。



EMEA 図 4：API 攻撃でよく使用されるベクトルは、HTTP、SQLi、XSS。LFI は API 攻撃ではあまり使用されていないが、Web アプリケーション攻撃では依然として使用されることが多い

EMEA では、API 攻撃に使用される手法としてクロスサイトスクリプティング（XSS）が依然として一般的であり、コマンドインジェクション（CMDi）も多く見受けられます。新しいデータセットを用いることで、API でのその他の攻撃ベクトルを監視できます。最近流行し始めたベクトルとしては、サーバーサイド・リクエスト・フォージェリ（SSRF：2023 年レポートで解説）が挙げられます（グローバルレポートの最後にある付録で、すべての攻撃ベクトルの定義をご覧ください）。

当社の調査から、ボットリクエストにも懸念があることがわかりました。12 か月間の同一レポート期間において、4 兆近くの不審なボットリクエストを検出しましたが、その 40% が、API を標的にしていました。

EMEA スナップショットの結論

セキュリティとリスク管理の観点からすると、API の防御が必須であることは明らかです。既存の法規制や、脅威の状況に合わせてサイバーセキュリティ関連法規を維持するための新しい動きもまた、API の保護を不可欠にしています。

たとえば欧州連合の一般データ保護規則（GDPR）では、個人データの保護に焦点が当てられており、API については現在、どのように使用および共有すべきか活発に議論されているところです。さらに、新しいネットワーク・情報システムの安全に関する指令（NIS2）では、特に強固な API セキュリティプログラムの確立が要求されています。EU 以外の各国、たとえばサウジアラビアなども、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。今後施行される Payment Card Industry Data Security Standard（PCI DSS） v4.0 の Section 6 には、データ侵害リスクの低減を目的とする、システムやソフトウェアの開発と保守における API 使用方法に関する新しい基準が含まれています。

規制当局が API に対するサイバーセキュリティ基準を強化する取り組みや方針を打ち出している現在、ベストプラクティスやガイドラインをしっかり理解し、セキュリティプログラムに API を組み込むことによる可視性の向上、防御力の強化、コンプライアンス要件のマッピングを図ることが重要です。

詳しくは、グローバルな SOTI レポート「影に潜む脅威：攻撃トレンドで API の脅威を解き明かす」をご覧ください。

可視性の向上：エンタープライズ API アセットの 1 年

レポートの冒頭で、API の可視性が欠如していることによる危険性を考察し、セキュリティアラートから組織が得るべき知見を挙げました。このセクションでは、下記のように強力な API セキュリティプログラムを採用することで、さまざまな観点から視認性が得られることを解説します。

- **探索** — 組織内の API アセットを可視化
- **リスク監査** — 探索して見つけた各 API のリスク対策を可視化
- **ふるまい検知** — 各 API でアクティブな脅威を確認するために、通常の使用と異常な不正使用を可視化。
- **調査と脅威ハンティング** — API アセット内に潜む脅威を精通した人間の脅威ハンターが発見し、可視化

このような観点は API に限定されたものではありません。しかし急速に導入された API の多くは、すでに定着している他の IT インフラに見られるような成熟したサイバーセキュリティを備えていないと考えられます。問題は、多くの API に含まれている機微な情報が悪用されるかもしれない点にあります。Akamai が支援している組織では、API フットプリントに対してより高度な API セキュリティを実践しており、API アクティビティについての知見が多く、ポスチャに関するアラートとランタイムアラートの両方を監視し始めるにつれて、共通のパターンが見られます。

1. **影に光を当てる**
   古い格言「見えないものは守れない」は、現代の API にも当てはまります。API アクティビティの可視性の向上に成功した多くのエンタープライズを驚かせたのは、環境内で誰にも知られることなく動作しているシャドウエンドポイントの多さでした。野良 API やゾンビ API を発見するとセキュリティチームは感謝します。なぜなら、これまで影になっていた場所に光が当たるからです。API セキュリティの成熟度を高める第一歩は、こうしたシャドー API を体系的に発見し、すべて廃止するか、正式に文書として記録して組織の API セキュリティ管理に組み込むことです。この方法は、API の予期せぬ不正使用やその他の脅威が発生するリスクを低減する上で即効性があります。一般的に、API セキュリティツールを導入した当初はアラートが急増しますが、やがて管理されていない API や未承認の API が見つかるごとにプロセス内の穴が明らかになってきます。

2. **整理する**

シャドー API への対応が終わっても、認可された API のインベントリーを合理化して整理する作業が残っています。具体的には、開発、テスト、本番などの大まかな分類によるセグメント化や、チームが API 関連のリスクを把握することを目的とした、セキュリティアラートと分析に適切なコンテキストを持たせた階層化が挙げられます。

次のステップとしてやるべきことは、各 API を文書化して可視性を向上させる作業です。文書化すると、セキュリティチームはポスチャに関するアラートに対してより効率的に対応できるようになります。なぜなら、アラートにコンテキストが付与され、アプリケーション、API、ビジネスプロセスに関する考え方とすり合わせることが可能になるためです。API のふるまいのベースラインを確立しない限り、どのアクティビティが疑わしいか判断するのは困難です。

3. **API ポスチャの強化**

初期にエンタープライズが受信するポスチャに関するアラートとランタイムアラートの多くは、API の実装に重要度の高い変更が加えられたことを伝えるものです。たとえば、セキュリティチームの業務として、一般的なアラートの種類を調べ、リスクを低減するための戦略と優先順位を特定するというものがあります。具体的には、API コードの欠陥の修正、設定ミスの修正、これまでの経験を踏まえて今後の脆弱性を防止するためのプロセスの導入などの組み合わせです。その後、侵入テスト検証計画の優先順位を設定し、将来的に脆弱性を回避するために必要なコーディングのベストプラクティスを経営陣に報告します。

4. **脅威の検知と対応の明確化**

これまで紹介した 3 つのステップを実行すると、API セキュリティアラートの件数が全体的に減少しますが、年間を通じて見ると時々急増するのが一般的です。このようにアラートが急増する原因としては、広範囲にわたるビジネスモデルの変更、新機能の付与、新たな脆弱性や不正なシステムを招き入れる API フットプリントの追加などの内部要因が考えられます。それ以外にも、犯罪者からの攻撃などの外部要因もあり得ます。最も効果的な組織ではこのような急増イベントに備えており、リスクとアラートの量を通常レベルに下げるために、事前に明確に定義された対応手順を実行します。また、アクティブな API 脅威への対応、調査、封鎖、復旧にかかる時間を継続的に短縮するための対策も講じています。そのためには、API 環境に応じた新しいスキルが必要になることもあります。

5. **より強力なオフェンスの開発**
   組織が防御的な API セキュリティ対策を改善する際の次の段階は、防御策を API 脅威の探索と緩和のためのオフェンス的なアプローチで補完することです。たとえば、後手に回る前に潜在的な脅威を早期に特定することを目的とした、正規化された API 脅威ハンティングの統制とサイクルの確立が挙げられます。非常に専門的なスキルを持つ人材と、割り込みタスクからリソースを切り離す能力が必要とされるため、これを実行するのは簡単ではありません。そのため一部のエンタープライズは、Akamai のように、この重要な機能を提供する専門のサードパーティ・サービス・プロバイダーを利用しています。

Akamai の匿名エンタープライズ顧客を例として以上のようなパターンを示したのが図 5 です。年が始まって間もない 1 月と 2 月はシャドー API の排除と整理、API セキュリティポスチャへの初歩的な改善措置を講じたため、アラート数が減少しています。API アセットに変更が加えられると、ポスチャに関するアラートが急増することもあります。API を可視化することで、潜在的な脆弱性が残存するのを防ぎ、迅速に解消することができました。

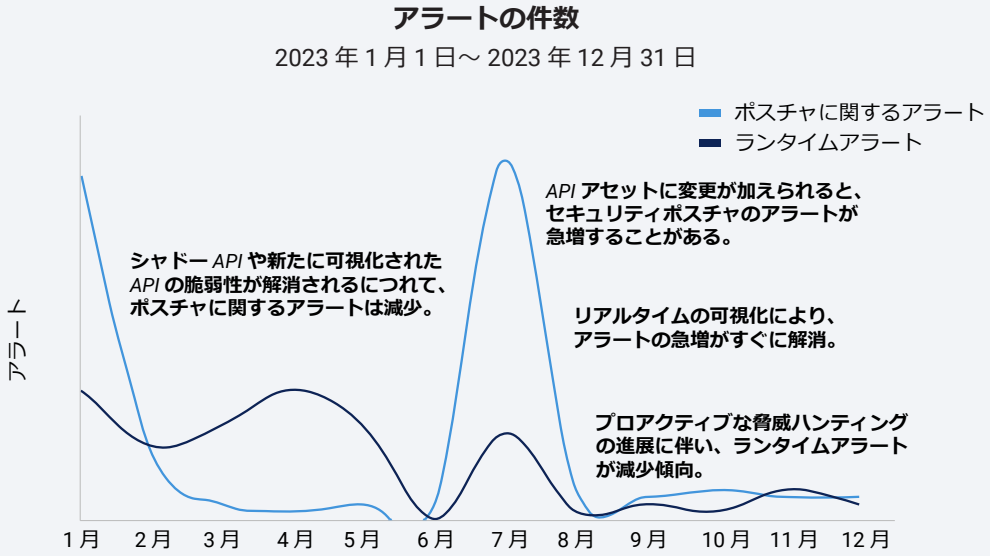


図 5：API の状況を可視化した後の API アセットの変動とアラートが大幅に減少

ランタイムアラートの件数は、外部要因によって左右されるため、予測は困難です。しかし、全体的なセキュリティポスチャを改善し、プロアクティブな脅威ハンティング能力を強化するにつれて、全般的な減少傾向が見られるようになります。

まとめると、IT チームのみで API の面倒を見続けるのは不可能だということです。API の潜在的なリスク状況はデータの機密性に依存し、それによって新しいツールとスキルが必要とされます。新しいツールを展開する際、API 防御に対してリーダーはスキルセットと人員配置の必要性を検討しなくてはならず、多くの場合、エンジニアリング時間の再配分やマネージドサービスへの移行が求められます。全体として、API をサポートするためのサイバーセキュリティの取り組みのレベルを追跡し、非効率な点がないか分析する必要があります。

API の世界を守る

API は、企業が構築する多くの新機能の基盤となっています。それにもかかわらず、API のセキュリティは計画プロセスの初期段階で十分に考慮されていない場合や、新しいテクノロジーの急速な展開に追いついていない場合がほとんどです。ここで、効果的なセキュリティプログラムの構築方法について、私たちが大好きな白髭のサイバーセキュリティ専門家、Bruce Schneier 氏が述べた言葉を紹介しましょう。「防御することは不可能だ。 前もって防ぐことも不可能だ。 唯一できることは、 察知して対応することだけだ」。この考え方は、的確な状況認識への原動力になるはずです。セキュリティプログラムにすべての API が組み込まれ、攻撃や脆弱性、悪用を積極的に監視するようにすべきです。侵入テストチームと攻撃者視点で検証するレッドチームは、認証や公開されたデータだけでなく、JSON プロパティやスクレイピングなどのランタイムについても体制を検証する必要があります。このテストはパープルチームの演習として構築すべきです。演習では、セキュリティ情報およびイベント管理チームとセキュリティ・オペレーション・センターが攻撃を検知し、その影響を緩和するための最新のプロセスを備えていることを検証します。本レポートではケーススタディ（ロイヤルティ詐欺やカーディング攻撃など）を紹介していますので、テンプレートとしてテスト計画に活用してください。

最も一般的な攻撃を防ぐためのコーディングプラクティスに関する OWASP のガイダンスがありますので、これを活用しましょう。こうした事前対応型のコントロールを用意し、探索、強化、検知、対応に役立つ強力なプロセスの開発に向けて働きかけることが、四半期ごとのアクションプランを構築する基盤になります。

コンプライアンスについても検討が必要です。現段階で API に関する法律や規制はそれほど多くありませんが、顧客の保護に向けて適切な行動を取るために、さまざまなベストプラクティスや基準を活用すべきです。API は GDPR をはじめとする現在の規制で言及されており、PCI DSS v4.0 などの新しい基準でも大きく取り上げられています。また、ANSI などの団体もガイドラインを発表しています。

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。また、当社は顧客との関わりの中で、より少ない（整理された）プラットフォームでセキュリティコントロールを統合する価値や、変革の目標を達成するための柔軟な人材配置ソリューションの必要性、意思決定やパフォーマンス評価における可視性の重要性をよく耳にします。本レポートのデータから得た知見と可視性が、お客様の顧客を保護するプログラムの更新とベストプラクティスの開発に役立つことを願っています。

最新の Akamai リサーチはセキュリティ・リサーチ・ハブでご覧いただけます。

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、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。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、4,000 か所以上のエッジポイントからなるグローバルネットワークです。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～ 2023 年 12 月 31 日までの 12 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。当社は、Web アプリケーションとボット攻撃のデータセットに関して、数回のアップグレードを実施してきました。それぞれの収集方法について、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「インターネットの現状／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。

Akamai API Security の知見

Akamai API Security Solution Engineering チームは、API Security のアラートに基づいた API のリスクとその潜在的な影響について、現実の知見を提供してくれました。その貢献に、非常に感謝しています。

付録

攻撃ベクトル	定義
アクティブセッション	セッション中に繰り返されるリクエスト。攻撃トラフィックにはクライアントに対してフラグが立てられ、ブロックされるようになっています。
コマンドインジェクション（CMDi）	もともとの意図とは異なる解釈を行い、攻撃者が選択したアクションを実行するように、攻撃者が新しい要素を既存のコマンドに注入すること
クロスサイトスクリプティング（XSS）	攻撃者が悪性のスクリプトをコンテンツに埋め込み、そのコンテンツが Web ブラウザーに表示されたときに、ユーザーの権限レベルを使用して標的ソフトウェアにそのスクリプトを実行させること
データハーベスティング	攻撃者が、標的およびその通信の設計や設定にある弱点を悪用し、意図されたものよりも多くの情報を得ようとすること。別の攻撃の準備用データを収集する目的で実行されることがよくありますが、情報にアクセスすることが攻撃者の最終目標である場合もあります。
HTTP プロトコル（HTTP）	攻撃者が、予期しないアクションを実行するために、クライアントとサーバーが通信するときに使用するプロトコルの弱点を悪用すること。悪用するプロトコルに応じて、攻撃の最終目標が異なります。
ローカル・ファイル・インクルージョン（LFI）	攻撃者が標的ソフトウェアの入力情報を操作して、アクセスされることを意図していなかったファイルシステムの領域にアクセスできるようにすること（おそらくその領域を変更することが目的）

攻撃ベクトル	定義
リモート・ファイル・インクルージョン（RFI）	攻撃者がリモートの任意のコードを読み込み、実行した後に、標的アプリケーションをハイジャックし、攻撃者の命令を強制的に実行させること
サーバーサイド・リクエスト・フォージェリ（SSRF）	攻撃者がサーバーの機能を悪用し、内部リソースを読み取るか、更新すること
SQL インジェクション（SQLi）	標的ソフトウェアがユーザーの入力に基づいて SQL ステートメントを作成することを前提にして入力文字列を作り、その結果、SQL ステートメントに攻撃者の意図したアクションを実行させること。インジェクションが成功すると、情報の開示やデータベース内のデータの追加や変更が可能になる場合があります。
Web 攻撃ツール（WAT）	攻撃者が、悪用可能な情報を得られるよう、標的を念入りに調査すること。調査の結果、攻撃者はセキュリティ、設定、あるいは潜在的な脆弱性に関する推測に役立つ情報を取得できます。
Web プラットフォーム攻撃（WPA）	別の攻撃グループには属さない、ソフトウェアプラットフォーム（クラウド、Web、アプリケーションレイヤー）に対する攻撃

クレジット

共同執筆者

Badette Tribbey – 編集責任者
Charlotte Pelliccia – 代表執筆者（地域）

論説寄稿者

James Casey
Edward Roberts
Steve Winterfeld

校閲およびテーマ別寄稿者

Tom Emmons
Reuben Koh
Rob Lester
Richard Meeus
Abigail Ojeda
Menachem Perlman
Yariv Shivek

データ分析

Chelsea Tuttle

マーケティング・出版

Georgina Morales Hampe
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

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 & 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 3 月。