

フォ の

第11巻、第2号

アプリとAPIセキュリティ の現状 2025

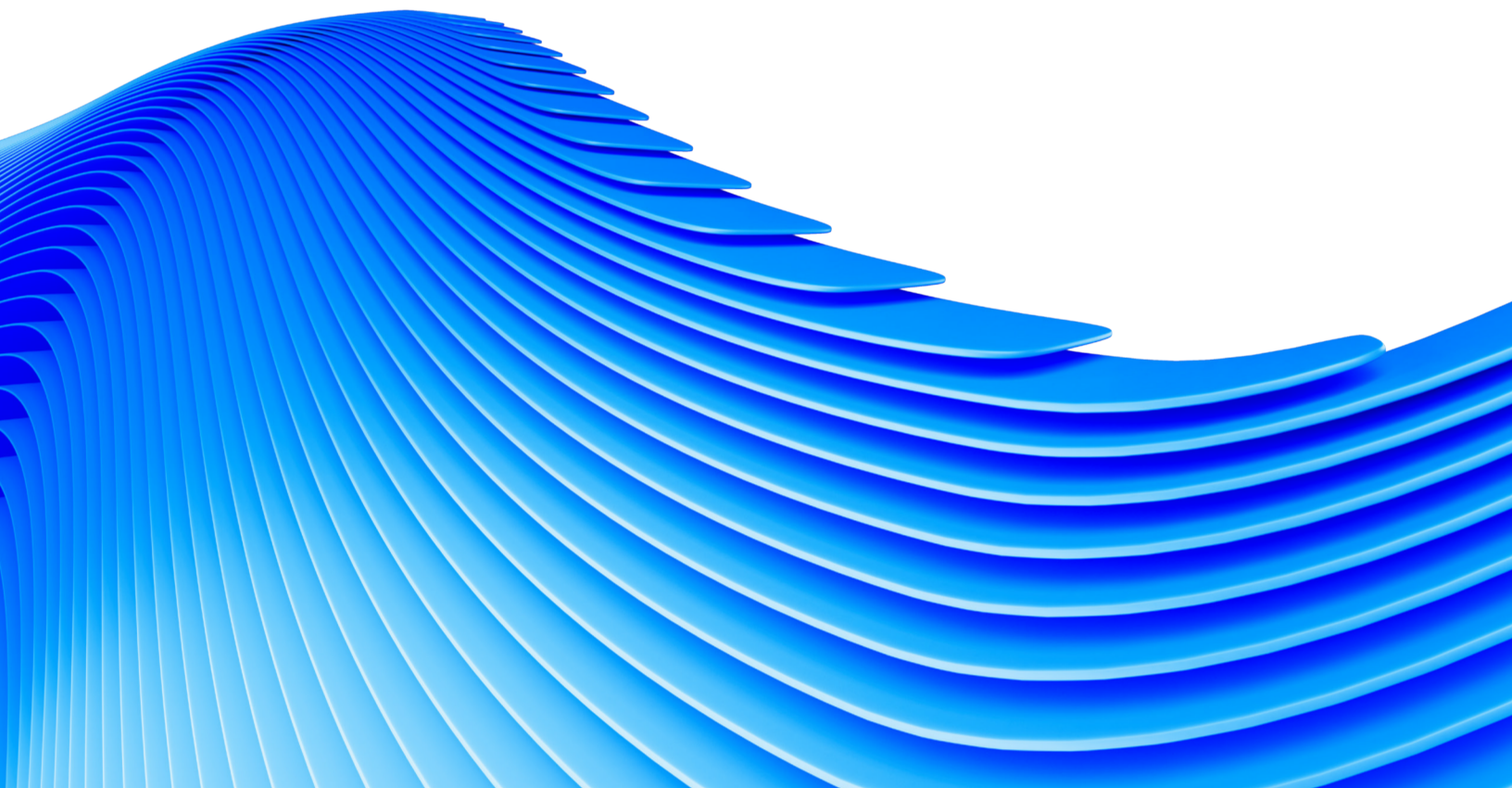
AIはデジタル領域をどうシフトさせるか



インターネット／セキュリティの現状

目次

02	はじめに
04	本レポートの主要な知見
06	Akamai の API 脅威インテリジェンスの進化
13	Web 攻撃 : 前年との比較とトレンド
17	レイヤー 7 DDoS 攻撃 : 前年との比較とトレンド
21	業界別のトレンド
27	地域別のトレンド
39	コンプライアンス
44	緩和策
46	手法
47	クレジット



はじめに

2025 年初頭の Web アプリケーションセキュリティの情勢には、脅威ベクトルのかつてない複雑さと高度化が表れています。組織は Web アプリケーションを標的とする攻撃の著しい増加に直面しています。Akamai が観測した Web アプリケーションおよび API 攻撃の件数は、2024 年だけで 3,110 億件を超え、前年比 33% の増加となりました。この急増は、クラウドサービス、マイクロサービスアーキテクチャ、人工知能（AI）を利用したアプリケーションの急速な導入に直接関連しています。このような情勢は地政学的な要因によってさらに激化しており、レイヤー 7（アプリケーションレイヤー）分散型サービス妨害（DDoS）攻撃の大部分はハイテク業界、コマース業界、ソーシャルメディア業界で発生しています。注目すべきは、脅威アクターが現在、AI で生成されたキルチェーンを展開し、攻撃ライフサイクル全体を自動化していることです。

同時に、API が主な標的となっており、Akamai は 2023 年 1 月～2024 年 12 月に 1,500 億件を超える API 攻撃を確認しています。AI 主導の SaaS（Software as a Service）ツールと API を介したコアプラットフォームの統合により、アタックサーフェスが大幅に拡大しました。財務面での影響は深刻です。API セキュリティの問題により、現在、組織では年間約 870 億ドルのコストが発生しています。また、適切な介入がなければ、この数字は 2026 年までに 1,000 億ドルを超える可能性があると予測されています。シャドウ API やゾンビ API は特に、ますます複雑化する API エコシステムにおいて脆弱な攻撃ベクトルを発生させています。



Web アプリケーションと API のセキュリティにおける AI の役割

AI による脅威検知機能と対応機能の強化により、Web アプリケーションと API のセキュリティ環境が変化しています。その一方、AI による新たなセキュリティ課題も発生しています。Web アプリケーションでは、AI を使用して、脅威検知の自動化、潜在的な侵害の予測、インシデント対応時間の改善が行われています。しかし、AI は、攻撃者が AI 主導のマルウェアや高度な Web スクレイピングを生成し、動的な攻撃手法で攻撃ライフサイクルを自動化することも可能にします。

API の場合、AI は膨大な数の API インタラクションを管理および保護する上で重要な役割を果たします。AI ベースのツールは、異常の検知、誤用パターンの特特定、脅威への対応の自動化をリアルタイムで行うために不可欠です。AI 主導の API 管理は、予測分析と自動化されたセキュリティ対策を統合することで、ますます高度化する攻撃を防ぐため進化を続けています。こうした進歩にもかかわらず、API に対する AI ベースの攻撃（Credential Stuffing やビジネスロジックの悪用など）は依然として大きな懸念事項であり、こうした脅威に効果的に対処するために堅牢なセキュリティフレームワークが必要となります。

同一ではないが、連動する：Web アプリケーション攻撃戦略と API 攻撃戦略

Web アプリケーション攻撃と API 攻撃は関連していますが、アプリケーションのインフラの異なる側面を標的とします。

 **Web アプリケーション攻撃**は、公開されているログインページなどの Web アプリケーションのユーザー向けコンポーネントを標的としており、通常は比較的単純な手法を使用します。

 **API 攻撃**は、アプリケーションの API エンドポイントやバックエンドロジックの脆弱性を悪用することに重点を置いており、API の構造とふるまいをより深く理解する必要があります。

主な違いは、アタックサーフェスと複雑さにあります。Web アプリケーション攻撃は通常、アプリケーションの可視部分を標的にしますが、API 攻撃はさまざまなソフトウェアコンポーネント間の通信チャネルを悪用します。ただし、どちらも、成功すると機微な情報やシステムリソースに不正アクセスできるようになります。

現代のアプリケーションでは API を使用した機能が増えているため、Web アプリケーション攻撃と API 攻撃の両方に対するサイバーセキュリティ対策を同時に理解することが極めて重要です。組織の多くは 2 年以内に Web アプリケーションが 39% 増加すると予想しており、Web と API のセキュリティの相互依存性がより顕著になっています。いずれかの側面をおろそかにすると、組織はアプリケーションのフロントエンドとバックエンドの両方の弱点を悪用する高度なマルチベクトル攻撃に対して脆弱になる可能性があります。

Akamai 独自の視点：脅威パターンの解明

この複雑さを分析するにあたり、Akamai は全世界の Web トラフィックの 3 分の 1 以上を処理する自社のネットワークインフラを活用することにより、脅威のパターンの可視化を、他に類を見ないレベルで提供しています。このような視点と、自社の研究チームやデータ・サイエンス・チームの知見を組み合わせることで、Akamai は包括かつ実用的なインテリジェンスを提供できます。その調査結果は、セキュリティリーダーがリスクを軽減し、セキュリティ投資の ROI を最大化する領域を決定するために必要な戦略的知見をもたらします。

本レポートの主要な知見

AI ベースの API は、そうでない API に比べて安全性が低い。

人工知能（AI）を利用する API の大部分は外部からアクセス可能で、多くの場合、脆弱な認証メカニズムに依存しています。そのような API を標的とする AI 主導の攻撃が増加しているため、この脆弱性は深刻化しています。

AI は脅威アクターの技術的進歩を促進する。

これには、AI 主導のマルウェア、脆弱性スキャン、AI 統合システムへの攻撃、高度な Web スクレイピング機能などの技術的進化が含まれます。

32%

OWASP API Security Top 10 関連のインシデントの増加率

API セキュリティインシデントが増加している中、Open Worldwide Application Security Project（OWASP）API Security Top 10 の問題により、機微な情報と機能を公開する認証および認可の欠陥が明らかになっています。

30%

MITRE セキュリティフレームワーク に関連するセキュリティアラートの 増加率

攻撃者は自動化や AI などの高度な手法を使用して API を悪用しています。MITRE フレームワークは、防御側がそのような攻撃を迅速かつ正確に特定するために役立ちます。

33%

グローバルな Web 攻撃の前年比 増加率

攻撃の急増は、クラウドサービス、マイクロサービス、AI アプリケーションの急速な普及と直接関係しており、それらによってアタックサーフェスが拡大し、新たなセキュリティ上の課題が生じています。

2,300 億件以上

コマース組織を対象とした Web 攻撃の数

コマース業界は最も影響を受けた業界であり、ハイテク業界（2 番目に多くの攻撃を受けた業界）の 3 倍近くの数の攻撃を受けました。

73%

アジア太平洋・日本（APJ）
地域における Web 攻撃の増加率

2023 年には 290 億件でしたが、
2024 年には 510 億件に増加しま
した。

37%

欧州・中東・アフリカ（EMEA）
地域で発生した Web 攻撃のうち、
API を標的とした攻撃の割合

EMEA は、全地域のうちこの種の
攻撃の割合が最も大きかった
地域です。

94%

四半期ごとのレイヤー 7 分散サービ
ス妨害（DDoS）攻撃の増加率

（2023 年第 1 四半期～2024 年
第 4 四半期）。

11.9 兆

北米を標的としたレイヤー 7 DDoS
攻撃の件数

（2023 年第 1 四半期～2024 年
第 4 四半期の 2 年間）。

7 兆

ハイテク業界を標的としたレイヤー 7 DDoS 攻撃の件数

（2023 年 1 月～2024 年 12 月）。これにより、ハイテク業界は最も影響を受けた
業界となりました。

7.4 兆

アジア太平洋・日本地域を標的とした
レイヤー 7 DDoS 攻撃の件数

（2023 年第 1 四半期～2024 年
第 4 四半期の 2 年間）。

20%

EMEA 地域を標的としたレイヤー
7 DDoS API 関連攻撃の割合。

EMEA は、全地域のうちこの攻撃
タイプの割合が最も大きかった
地域です。

Akamai の API 脅威インテリジェンスの進化

Akamai と Noname Security の統合により、API の脅威に関する調査機能とレポート機能が大幅に強化され、API 固有のリスクに対する新たな視点がもたらされました。Akamai は、この新しいデータセット（まだデータ統合の初期段階）を使用して、既存の脅威インテリジェンスを強化し、API セキュリティの問題に対する幅広い見解を提供しています。

アラートをセキュリティフレームワークにマッピング

この新しいデータセットは徐々に、セキュリティアラートの詳細を次のような重要なサイバーセキュリティフレームワークやコンプライアンス基準にマッピングします。

- MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
- 一般データ保護規則 (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO)
- Open Worldwide Application Security Project (OWASP)

こうした機能強化により、クライアントに堅牢な保護を提供する Akamai の能力が大幅に強化されます。これらのフレームワークに合わせることで、組織は自社のセキュリティポスチャをより明確に把握し、規制要件を満たし、セキュリティの取り組みに効果的に優先順位を付けることができます。この包括的なアプローチにより、組織はリソースを戦略的に割り当て、API と機微な情報を保護するための対象を絞った戦略を策定できます。

30 日間のデータサンプルの分析

本レポートの作成にあたり、Akamai は 30 日間のデータサンプルを分析して、各サイバーセキュリティフレームワークとコンプライアンス基準にまたがる脅威アクターの一般的なアクティビティを明らかにしました（図 1）。また、MITRE アラートや OWASP アラートに関する深い視点を提供します。さらに、これらのリスクとセキュリティインシデントがコンプライアンス基準にどのように影響するかについても検討します。

	30 日間のアクティビティ件数	毎月の増加率
OWASP	5,907,000	32%
MITRE	2,817,000	30%
ISO	832,000	22%
GDPR	669,000	21%
PCI DSS	881,000	16%

図 1: セキュリティフレームワークおよびコンプライアンス基準ごとのセキュリティアラートの内訳

MITRE アラート

30 日間で、Akamai は自社の顧客の間で MITRE 手法に関連するインシデントが 30% 増加したことを観測しました。特に、攻撃者は T1078（有効なアカウント）を頻繁に使用し、正当な認証情報を利用してシステムやネットワークに不正にアクセスしていました。API はトークンを利用して認可することが多いため、このトークンを取得した攻撃者は検知されることなく機微な情報にアクセスできます。

また、Akamai は T1566（フィッシング）も特定しました。この手法では、攻撃者がフィッシングキャンペーンを開始して、将来の攻撃に利用するために API トークンや認証情報を窃取します。API によりアタックサーフェスが拡大しているため、脅威アクターが API を悪用して侵入するケースが増大しています。さらに、T1190（公開アプリケーションの悪用）に関連するアラートにより、アプリケーションの欠陥を利用してネットワークに侵入する攻撃者がいることが明らかになりました。その他の観測された手法として、T1580（クラウドインフラ探索）があげられます。この手法では、攻撃者は API コールを介して、公開されているクラウドエンドポイントを調査するために API を利用していました。

MITRE には専用の API セキュリティマトリックスはありませんが、API を標的とする攻撃者の手法に関する知見を求めるセキュリティチームや組織にとって、MITRE のフレームワークは依然として重要です。攻撃者の戦術を API 固有のふるまいにマッピングすることで、セキュリティチームは攻撃の段階とそれに関連する戦術、手法、手順を特定し、インシデント対応と脅威検知を強化できます。このアプローチにより、防御者はより効果的にリスクを緩和できるようになります。

OWASP アラート

OWASP API Security Top 10 は、脆弱性の影響と重大度に関する実用的な知見を提供する重要なリソースです。急速に進化する脅威情勢との関連性を維持するように情報がアップデートされるため、開発者やセキュリティチームは効果的に取り組みの優先順位を付けることができます。

Akamai の分析では、30 日間のサンプル期間中に OWASP 関連のインシデントが 32% 増加したことが明らかになりました。特に、Broken Object Property Level Authorization（BOPLA）、Broken Function Level Authorization、Broken Authentication などの脆弱性は、機微な情報や重要な機能を攻撃者に直接公開してしまいます。認可メカニズムが不十分であれば、攻撃者は権限の昇格、アカウントの乗っ取り、機密情報へのアクセスを行えるようになるため、そのような認証メカニズムは API を標的とする極めて危険な攻撃ベクトルです。

Broken Object Level Authorization (BOLA) は依然として API セキュリティ上の重要な脆弱性ですが、ビジネスロジックの欠陥を利用するため、検知が困難です。そのため、報告数が過小であったり、検知率が低かったりすることがよくあります。この問題に対処するために、組織はユーザーとユーザーが通常アクセスするリソースの間の明確な関係を確立する API セキュリティソリューションを使用する必要があります。それには、異常なアクセスパターンを認識できる高度な機械学習アルゴリズムを使用して、ふるまいのベースラインを設定する必要があります。

BOPLA は、API に存在するフィールドレベルのアクセスに関する細かい問題を悪用します。そのような問題は、セキュリティテスト中に見落とされることがよくあります。BOPLA 攻撃は、オブジェクト ID 全体を変更する必要がある BOLA とは異なり、オブジェクト内の特定のプロパティを標的とします。たとえば、応答内で機密性の高い個人を特定できる情報 (PII) を公開する DELETE API コールは、BOPLA の脆弱性を構成します。この微妙な違いにより、BOPLA の問題は BOLA 攻撃よりも頻繁に発生します。

実際の例として、電子メールアドレスのみを使用した登録解除要求があります。この場合、API 応答にユーザーのフルネームとアドレスが意図せずに含まれることがあります。このように機微な情報が不正な当事者にさらされる原因は、セキュリティテストでは通常、個々のプロパティではなくオブジェクト全体に重点が置かれることにあります。この見落としにより、API セキュリティ評価で BOPLA の脆弱性が検知されることが多くなっています。

もう 1 つの重大な脆弱性として、Unrestricted Resource Consumption があげられます。攻撃者はこの脆弱性を悪用して、リソースの枯渇や DDoS のような攻撃によってサービスの中断を引き起こす可能性があります。この脆弱性は、クラウドリソースの過剰使用による運用コストの増加や総当たり攻撃のリスクの増大など、サービスへの影響を超えたリスクをもたらします。適切なレート制限が行われていなければ、攻撃者は API を迅速に調べられるため、セキュリティが損なわれる可能性があります。さらに、このような攻撃はトラフィックを大量に生成するため、組織のコストが大幅に増加します。

API の安全でない使用も重要な脅威ベクトルであり、これは不適切な検証、データのフィルタリング、サードパーティ API 統合時のセキュリティメカニズムの欠如に起因します。デジタルトランスフォーメーションのために、組織によるサードパーティの API への依存度が上がっているため、この問題に対する懸念が高まっています。[最近の調査](#)によると、調査対象の組織の 80% 以上がサードパーティ API の問題に直面しており、ゼロトラスト・セキュリティ・モデルを採用することの重要性が浮き彫りになりました。この脆弱性だけではすぐには致命的にならないかもしれませんが、不十分な検証や安全でない依存関係など、他の弱点と組み合わせると、セキュリティ上の大きな脅威になる可能性があります。たとえば、検証されていないサードパーティトランザクションを財務 API が信頼すると、セキュリティ侵害につながるおそれがあります。



PCI DSS と GDPR に
関連するセキュリティ
アラートの増加率はそ
れぞれ 16% と 21% で、
ISO 27001に関連する
アラートの増加率は
22% でした。

API コンプライアンスの確保

API コンプライアンスを確保するためのベストプラクティスには、違反している特定のコンプライアンス基準や規制基準を各アラートにタグ付けすることが含まれます。これにより、組織は重要なコンプライアンスの問題について即座に知見を得て、それらに対処するための実践的なガイダンスを得られます。このプロアクティブなアプローチは組織が規制コンプライアンスを維持するために役立ち、規制上の罰金や法的な影響、財務上の大きな損失につながる可能性のある評判の失墜のリスクが軽減されます。たとえば、API の脆弱性により 400,000 人の顧客のデータが流出した後、[ある航空会社は 2,000 万ポンドの罰金を科されました](#)。このことから、GDPR のもとで API セキュリティが不十分である場合、深刻な結果につながる事が明らかになりました。

コンプライアンス基準は、機微な情報を保護し、顧客を守り、法的義務や規制上の義務を果たすために不可欠なガードレールです。PCI DSS、GDPR、Health Insurance Portability and Accountability Act（医療保険の携行性と責任に関する法律、HIPAA）などの基準では、決済データや PII などの機微な情報を安全に取り扱うことが求められます。Akamai のデータ分析によると、PCI DSS と GDPR に関連するセキュリティアラートの増加率はそれぞれ 16% と 21% で、ISO 27001 に関連するアラートの増加率は 22% でした。

GDPR

GDPR は、API ライフサイクル全体を通してデータ保護と顧客のプライバシーを統合することを重視しています。これには、安全な設計、強力な認証と認可、レート制限、定期的な脆弱性テスト、暗号化、開発の初期段階からの継続的なリスク評価が含まれます。これらの対策により、データの機密性、完全性、可用性が確保されます。

PCI DSS

同様に、[PCI DSS](#) は、設計、コーディング、テスト段階にセキュリティを組み込むことで、決済カードデータを処理する API のセキュリティを確保することを重視しています。セキュリティ上の欠陥を特定して対処するために、Web の脆弱性からの保護と定期的なテストを義務付けています。

具体的には、要件 10 と 11 により、リクエスト、応答、認証試行、システム変更などの API アクティビティの包括的なロギングと監視が求められます。ログは少なくとも 12 か月間保持する必要があり、直近の 3 か月分は容易にアクセスして分析できる状態でなければなりません。また、大幅な変更後には外部の脆弱性スキャンを実行することを推奨しています。PCI コンプライアンスを確保するために、組織はレート制限、ロギング、役割ベースのアクセス制御（RBAC）、セッション管理などの厳格な制御を実装し、API が脅威やリスクに対する回復力を備えるようにしなければなりません。



ISO 27001

ISO 27001 標準は、情報セキュリティリスクの効果的な管理、組織のセキュリティポスチャの改善、同業他社や顧客との信頼構築のための強固なフレームワークを提供します。推奨プラクティスには次のようなものがあります。

- ユーザーアイデンティティを検証するためにアクセス制御（API キーなど）を実装する
- エンドツーエンドのデータ暗号化を使用する
- 異常なふるまいを見つけるために API を監視する
- 潜在的な API の脆弱性を特定するために徹底的なリスク評価を実施する

これらのコンプライアンス要件は、API セキュリティと規制フレームワークの重要なつながりを明らかにしています。適切に実施することで、機微な情報を保護できるだけでなく、複数のコンプライアンス要件を同時に満たすことができます。既存のグローバル基準や新しいグローバル基準について、詳しくは本レポートの「[コンプライアンス](#)」のセクションをご覧ください。

API 可視性のギャップ：データへの隠し通路

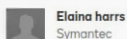
API の悪用

2024 年 11 月、電子署名ソリューションプロバイダーに対する重大な攻撃について、[Bleeping Computer](#) が報告しました。脅威アクターは、プロバイダーのドキュメント管理および追跡 API のコアコンポーネントを悪用し、多数の潜在的な被害者に不正な請求書を送信できるようにしました。受信者がこの文書にうっかり署名すると、攻撃者はさまざまな組織から支払いを得ることができます。

このインシデントは、API の悪用によって生じる有害な影響を浮き彫りにしています。攻撃者は、設計意図とは異なる方法で API を悪用し、API を意図しない攻撃ルートに変換する可能性があります。生成 AI の出現により、脆弱性の探索とレート制限の回避が自動化され、より迅速で高度な攻撃を容易に行えるようになったため、このようなリスクがさらに高まりました。

出典：bleepingcomputer / Wallarm

Please Review & Act on These Documents



Norton
Receipts & Invoice
[View More](#)

Norton
Internet Security
Powered by docusign

Please review the documents below.

CONTINUE

OTHER ACTIONS ▾

Signature
 Initial
 Stamp
 Date Signed

Name
 First Name
 Last Name
 Email Address
 Company
 Title

- Comprehensive protection against viruses and malware
- Identity theft protection
- Performance optimization tools
- 24/7 customer support

DETAILS:

PRODUCT	TENURE	AMOUNT
Norton LifeLock 360	2 Users/1 Year	249.00 USD
	Activation Charges	49.00 USD
TOTAL:		298.00 USD

POLICY:

We understand that circumstances can change and you may need to cancel your subscription. We

APIの悪用の検知に関する課題

セキュリティチームは、APIの悪用を検知する上で大きな障害に直面しています。その主な理由は、通常のふるまいと疑わしいふるまいのベースラインを確立する必要があることです。この課題は、リアルタイムのふるまい監視が、異常や脅威を事前に検知するために不可欠であることを明確に示しています。

Akamaiの「[2024年のAPIセキュリティの影響に関する調査](#)」では、次のような懸念されるトレンドが明らかになっています。調査対象の組織のうち、毎日APIのテストを行っている組織の割合はわずか13%で、2023年の37%から大幅に減少しました。現在のセキュリティ情勢を考慮すると、この減少は特に気がかりです。日々のAPIテストが急激に減少すると、急速に進化する脅威を検知して対応する能力が大幅に低下し、重大な脆弱性が長期にわたって解決されずに放置される可能性があるため、組織のセキュリティリスクが高まります。

自動化されたテストを開発サイクル中に頻繁に行うことで、組織は問題を早期に特定して対処できるため、本番環境でのコストのかかる修復を回避できます。自動化された検知しやすい手法でAPIが悪用されることが増えている時代では、プロアクティブなテストがリスク緩和において重要な役割を果たします。

管理されていないAPI：ゾンビAPIとシャドウAPI

API資産の可視化は依然として組織にとって重要な課題であり、これには正式なAPIの追跡と機微な情報の特定の両方が含まれます。「[2024年のAPIセキュリティの影響に関する調査](#)」では、次のような大きなギャップが明らかになりました。AppSecチームの47%は、APIの完全なインベントリを維持していますが、機微な情報を処理するAPIを特定できていません。シニア・セキュリティ・プロフェッショナルも同様の制約があることを報告しており、42%がこの監視に関する問題に直面しています。さらに懸念されることに、APIの完全なインベントリと機微な情報の流出に関する知識を有する企業の割合は、2023年には40%でしたが、2024年には27%に減少しました。また、この「セキュリティの影響に関する調査」では、ゾンビAPIとシャドウAPIをAPIセキュリティインシデントの主な原因のとして取り上げています。

不完全なインベントリは、主にゾンビAPIとシャドウAPIを捕捉できません。ゾンビAPI（不完全な廃止やスタッフの離職などの理由によりアクティブなままになっている古いインターフェース）は、脆弱な攻撃ベクトルを生み出します。シャドウAPI（標準の承認プロセスを経ずに迅速なソリューションとして開発されたAPI）も、同等の脅威をもたらします。[調査](#)によると、悪性のAPIトランザクションの3分の1がシャドウAPIを標的としています。

Webアプリケーションファイアウォール（WAF）などの従来のセキュリティ対策では、これらの脅威に対して不十分であることが分かっています。脆弱なエンドポイントを効果的に特定するためには、高度なAPI探索ソリューションと監視ソリューションが必要です。

包括的なAPIインベントリは効果的なセキュリティ戦略の基盤となり、組織は使用パターンの監視、バージョン履歴の追跡、脆弱性の特定、コンプライアンス要件や規制要件の遵守を実現できるようになります。この戦略的アプローチにより、組織のデジタルインフラが明確に可視化されるため、最終的にリスク管理を強化し、全体的なセキュリティポスチャを強化できます。

セキュリティの注目点

2025 年第 1 四半期に、Akamai は API の悪用による E コマース企業への攻撃を特定しました。同社の SMS 送信 API には適切な認証がなかったため、攻撃者は 200 を超える異なる IP アドレス、単一の認証トークン、多数のランダムな携帯電話番号（正当なものと偽りのものの両方）を使用してその API を悪用することができました。

この攻撃戦略は単純ですが、効果的でした。複数の携帯電話番号を登録し、不正な番号に SMS メッセージを送信して金銭的損害を直接引き起こすことで、企業に多大な損害を与えます。攻撃を受けたこの企業は、アプリケーションとモバイルデバイス間のテキストメッセージの送受信を円滑にする SMS ゲートウェイサービスに料金を支払っており、攻撃者が携帯電話番号を登録したことで、ブランドや評判を損なう可能性のある予期しない費用を負担することになりました。複数のセキュリティ対策を取り入れた多層防御戦略を実行すれば、このような攻撃に対抗し、関連するリスクを大幅に緩和できます。

Akamai のアラートによると、脅威アクターはこの攻撃中に 11,057 件の POST リクエストを実行し、成功の応答は 5,659 件でした（図 2）。

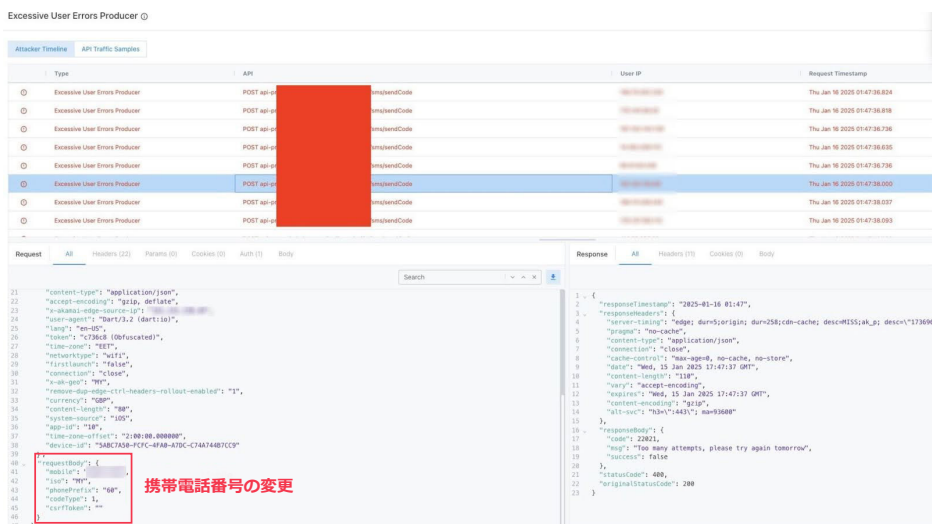


図 2：脅威アクターはセキュリティが確保されていない API に大量のリクエストを送信する

これらの自動化されたリクエストは、以下の重要なパラメーターを除いて同一でした。

ボディパラメーター **mobile**：次のパターンが検知されました - **<number>**

このようなリクエストは、サーバーに過剰な負荷をかけてサービス妨害を引き起こす可能性があります。また、API への不正アクセスが成功したことを示す可能性があります。従来の WAF には、この高度な攻撃を検知する機能がありませんでした。しかし、通常の API のふるまいのベースラインを作成する高度な API セキュリティソリューションは、ふるまい分析によってこのような攻撃を特定し、リスクをプロアクティブに緩和し、攻撃者による被害の拡大を防止することができます。

Web 攻撃：前年との比較とトレンド

Akamai の調査によると、2023 年 1 月から 2024 年 12 月までのレポート対象期間に Web アプリケーションと API を標的とした Web 攻撃が大幅に増加しました（図 3）。月別の攻撃数は、2023 年の初めには約 140 億件でしたが、2024 年 10 月までに 290 億件以上に増加しました。これは、2023 年第 1 四半期から 2024 年第 4 四半期にかけて、Web 攻撃が 65% 増加したことを意味します。

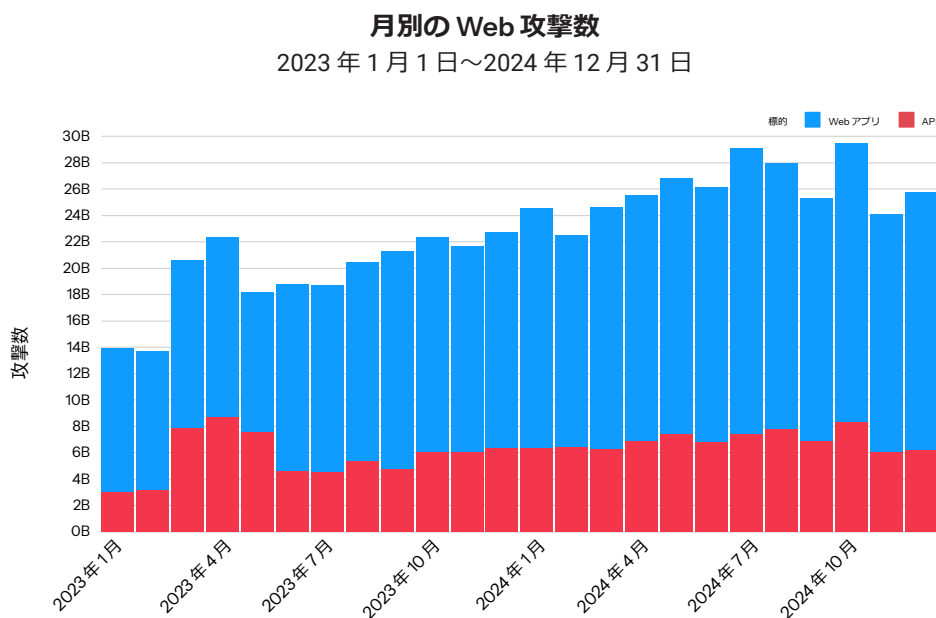


図 3：Web アプリケーションと API を標的とした従来の Web 攻撃が増加し続け、2023 年第 1 四半期から 2024 年第 4 四半期までに 65% 増加したことが示されている

主要な攻撃ベクトル：従来のふるまいベースのリスクと現代のふるまいベースのリスクの融合

サイバーセキュリティ専門家は、従来の Web 攻撃から、固有の脆弱性や誤設定を標的とする現代の攻撃まで、幅広い脅威から組織のデジタルインフラを保護するにあたり、増大する複雑さの課題に直面しています。

API リクエストの制約違反：増大する脅威

2年間にわたる API エンドポイントの包括的な分析により、API リクエストの制約違反が組織の懸念事項であることが明らかになりました（図 4）。このような違反は、リクエストまたは応答が事前に定められたパラメーターや確立された要件に準拠しない（レート制限の超過や無効なデータ入力の送信など）場合に発生します。

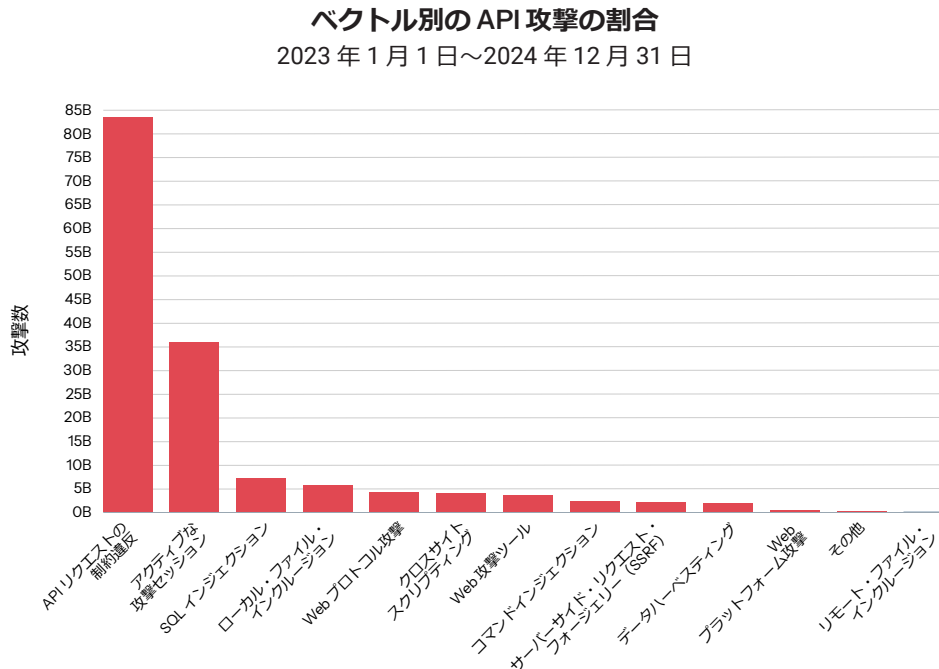


図 4：2年間で 830 億件以上のリクエスト制約違反が記録された

API リクエストの制約違反は、増大中の脅威であり、2年間で 830 億件以上の攻撃が記録されました。この攻撃ベクトルは 2023 年から 2024 年にかけて 24% も急増しており、API の悪用の危険性を明確に示しています。これらの違反の広範な発生は、潜在的な API の悪用を示す重要な指標であり、システムパフォーマンスの低下、サービスの中断、標的型攻撃に対する脆弱性の増大など連鎖的に悪影響を引き起こす可能性があります。

アクティブな攻撃セッション：創造的なソリューションを要する独自の攻撃

Akamai のソリューションは、API を標的とした攻撃によってもたらされる固有の課題に対処するために、革新的なセキュリティツールを採用しています。それらのソリューションの中核となるのは、アクティブな攻撃セッションを検知する独自のメカニズムであり、これは戦略的な防御ツールとして機能します。このシステムは、Akamai 独自の脅威インテリジェンスを使用して疑わしいふるまいを特定し、追跡します。これにより、組織は脅威が本格的な攻撃にエスカレートする前にアクティブに阻止できるようになります。

システムは脅威アクターにフラグを立て、「ペナルティボックス」のアプローチを実行します。現代の攻撃では、攻撃者は主に自動化を使用して偵察と攻撃を行います。Akamai はこれらの脆弱性スキャンセッションを迅速に特定し、クライアントを一時的にブロックすることによって対応し、それらをアクティブな攻撃セッションとしてラベル付けします。この戦略は、潜在的な脅威アクターが偵察を行ってネットワークの脆弱性を悪用することを効果的に阻止します。

攻撃者にとっての機会を制限することで、組織は API セキュリティポスチャを大幅に強化できます。このアプローチは、さまざまな潜在的な攻撃に対する堅牢な保護を提供し、全体的なサイバーセキュリティの回復力を大幅に向上させます。

この戦略の重要性は、Akamai のデータから明らかになっています。アクティブな攻撃セッションは、Web アプリケーションと API の両方で、全体的なランキングの第 1 位となりました（図 5）。2023 年には、これが原因で 690 億件以上の攻撃が発生しました。この数字は、2024 年に 1,130 億件以上に急増し、前年比で 63% の大幅な増加となりました。

攻撃ベクトル別の Web 攻撃数
2023 年 1 月 1 日～2024 年 12 月 31 日

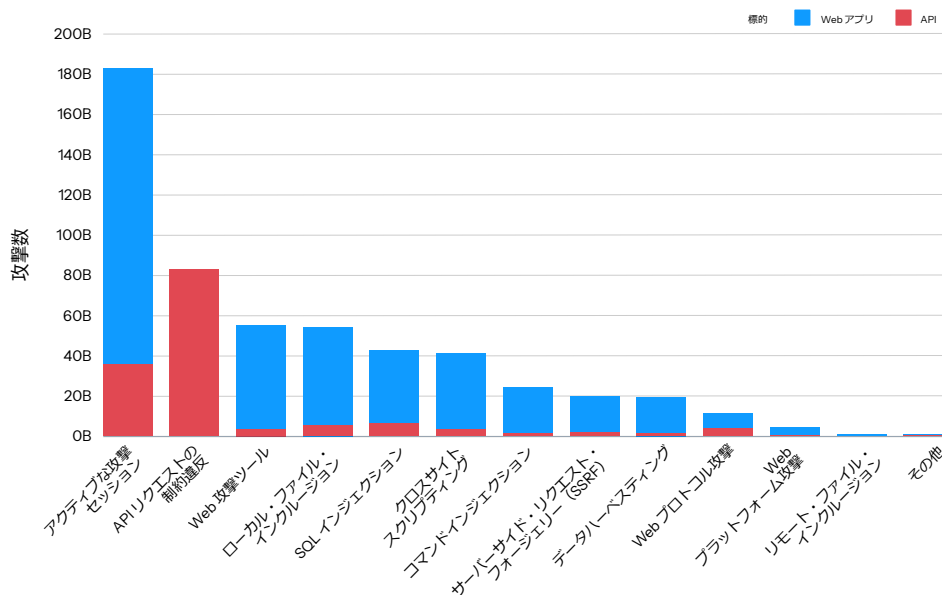


図 5：アクティブな攻撃セッションは Web アプリケーションと API の両方で他のすべてのベクトルを大きく上回っており、攻撃者は標的のネットワークに存在する脆弱性を執拗に追求していることを示している

現代のインフラに存在する従来の Web の脆弱性を無視できない理由

洗練されたふるまいベースの攻撃手法が出現し、従来の Web の脆弱性に対する認識が向上したにもかかわらず、インジェクション攻撃は引き続き高い有効性を示しています。2023 年 1 月から 2024 年 12 月までの Akamai のデータでは、攻撃数が大幅に増加していることが示されており、SQL インジェクション（SQLi）とコマンドインジェクションの前年比増加率はそれぞれ 60% と 34% でした。これらの脆弱性を悪用することにより、攻撃者は不正なコマンドを実行したり、システムの完全性を脅かしたり、適切な認証を行わずに機微な情報にアクセスしたりすることができます。これは、サイバーセキュリティ領域においてこれらの脆弱性が引き続き問題となることを示しています。

データストレージの信頼性とスケーラビリティに定評のある SQL データベースが持続的に普及していることが、このシステムがしつこく標的とされる原因になっています。特に、[最も広く使用されている 4 つのデータベース](#)に SQL ベースのアーキテクチャが使用されていることが、この攻撃ベクトルの深刻さをさらに際立たせています。

OWASP Top 10 API Security リストは更新されており、たとえば 2023 年の更新ではインジェクション攻撃がセキュリティの誤設定に置き換わりましたが、インジェクション攻撃に関連するリスクは依然として最も重要です。同時に、ローカル・ファイル・インクルージョン（LFI）やクロスサイトスクリプティング（XSS）などの他の確立された攻撃ベクトルも依然として高い頻度で発生しています。Akamai の「[Defenders' Guide 2025](#)」は、2024 年に観測された実際の攻撃事例を基に、リモート・リソース・インジェクション、クッキーの窃取、Web サイトの改ざん、セッションライディングなど、XSS 攻撃手法の巧妙さを明らかにしています。

これらの調査結果は、多層防御戦略を実行する必要があることを浮き彫りにしています。サイバーセキュリティ専門家は、適切な出力エンコーディング、堅牢なコンテンツ・セキュリティ・ポリシー、高度な WAF を組み合わせて、ますます巧妙化する攻撃に効果的に対処しなければなりません。

レイヤー 7 DDoS 攻撃：前年との比較とトレンド

Akamai の調査では、2023 年 1 月から 2024 年 12 月まで、Web アプリケーションと API に対するレイヤー 7（アプリケーションレイヤー）DDoS 攻撃が劇的に増加しました（図 6）。月間の攻撃件数は、2023 年の初めには 5,000 億件をわずかに上回る程度でしたが、2024 年 12 月には 1.1 兆件に急増しました。これは、2023 年第 1 四半期から 2024 年第 4 四半期にかけて、レイヤー 7 DDoS 攻撃が 94% 増加したことになります。

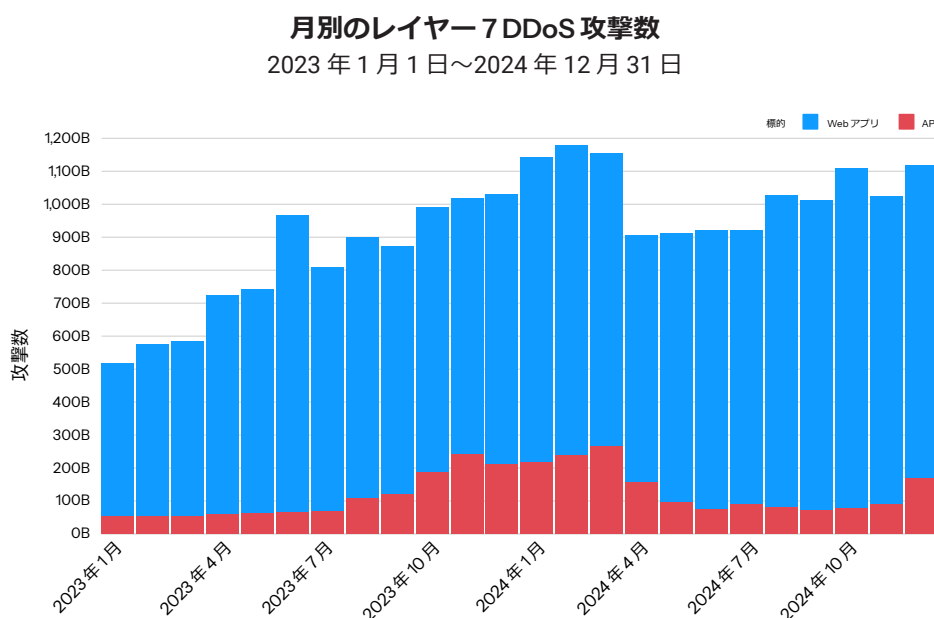


図 6：Web アプリケーションと API を標的としたレイヤー 7 DDoS 攻撃は増え続け、2023 年第 1 四半期から 2024 年第 4 四半期の間に 94% 増加した

アプリケーションと API に対するレイヤー 7 DDoS 攻撃

Web アプリケーションと API エンドポイントを標的とするレイヤー 7 DDoS 攻撃が継続的に進化している中、[HTTP フラッド](#)は主要な脅威ベクトルであり続けています。この攻撃は、リソースを大量に消費する運用を狙って、一見すると正当な要求を大量に送信することで、API リソースを過負荷状態にします。攻撃者は独自の手法を改良し、Web アプリケーションのロジックや API に存在する特定の脆弱性を悪用するレイヤー 7 DDoS 攻撃を作成して、検知と緩和を困難にしています。さらに、ボット主導型の攻撃がますます巧妙化しており、正当な API の使用を忠実に模倣するトラフィックパターンが生成されるようになりました。

攻撃者の AI トランスミッション：手動または自動で API の道を走行

生成 AI テクノロジーによって API を使用したビジネス統合に変革が起こり、API の普及と実用化が促進されています。AI API 市場は爆発的な成長が見込まれており、2025 年の 444.1 億ドルから、2030 年には 1,791.4 億ドルにまで達すると予想されています。この期間の年平均成長率は 32.2% に及びます。しかし、このように AI の導入が急増すると同時に、API に対する AI 主導の攻撃も大幅に増加しています。API の脆弱性が脅威にさらされることが増えている主な理由は、攻撃者が偵察と攻撃の両方のツールとして AI を手動でも自動でも活用していることです。

AI ベースの API 攻撃戦略

-  **戦略的ターゲティング**：攻撃者は AI ツールを使用して、標的とした API の特定のコンポーネントを特定、分析し、AI によって生成された悪性コードを使用して特定の脆弱性向けに攻撃をカスタマイズします。このアプローチにより、API の脆弱性に対する正確かつ効果的な攻撃が可能になります。
-  **自動攻撃**：攻撃プロセスを自動化することで、サイバー犯罪者は時間と労力を大幅に削減し、API セキュリティの脆弱性を迅速に特定して悪用します。この自動化には、多くの場合、企業と個人の両方に重大な脅威をもたらす AI ベースのボットが使用されます。
-  **ボリューム型攻撃**：攻撃者は AI を悪用し、トラフィックで API を過負荷状態にして膨大な量とスピードでセキュリティシステムをパンクさせます。自動化された DDoS 攻撃はこの戦略の典型例であり、AI ベースのボットが防御策に動的に適應しながら継続的に攻撃を実行します。
-  **ふるまいベースの攻撃**：AI はトラフィックパターンを分析し、一般的なアラートしきい値未満で動作して検知を回避する Low & Slow（少しずつ時間をかけた）攻撃を生み出します。このような攻撃は、多くの場合、BOLA や Broken Authentication などの一般的な API の脆弱性を標的とします。

AI ベースの API の皮肉

皮肉なことに、AI ベースの API は著しく安全性に欠けることが判明しています。AI ベースの API の多くは外部からアクセス可能であり、不十分な認証メカニズムに大部分を依存しているため、攻撃に対して脆弱になります。Akamai の「2024 年の API セキュリティの影響に関する調査」では、生成 AI ツールの API が、小売および E コマース業界のセキュリティチームによって報告された API インシデントの主な原因であることが明らかになりました。

進化する AI の脅威情勢

AI テクノロジーの進歩は、API の脅威情勢の進化に大きく寄与しています。過去 1 年間で AI 主導の API の脆弱性が記録的に増加したことが報告されており、米国のサイバーセキュリティ・社会基盤安全保障庁が記録したすべての悪用された脆弱性の過半数が API 関連のものだと指摘されています。

AI ベースの Web アプリケーション攻撃と防御戦略

新たな攻撃ベクトルと防御機能の登場により、AI が Web アプリケーションのセキュリティに及ぼす影響も大きくなっています。AI によって Web アプリケーション攻撃のサイバーセキュリティ情勢が大幅に変化した主な領域としては、AI 強化型マルウェア、AI ベースの脆弱性スキャン、AI を含むシステムへの攻撃、高度な Web スクレイピング、AI ベースの WAF システムなどがあげられます。

AI 強化型マルウェア

サイバーセキュリティ専門家は、AI を活用して Web アプリケーションを攻撃する高度なマルウェアを観測しました。フランスのユーザーを標的とした 2024 年の電子メールキャンペーンで、攻撃者は生成 AI の支援を受けて設計された可能性が高い悪性コードを展開し、[AsyncRAT マルウェア](#)を実行しました。この例は、AI を使用してマルウェアを作成し、展開するトレンドが拡大していることを示しており、これは Web アプリケーションセキュリティの専門家にとって新たな課題となっています。

AI ベースの脆弱性スキャン

AI により、Web アプリケーションの脆弱性スキャンに変革が起こり、有効利用または悪性利用を問わず、防御機能と攻撃機能の両方がもたらされました。現在では、このような AI 主導ツールにより、SQLi、XSS、クロスサイト・リクエスト・フォージェリー、サーバーサイド・リクエスト・フォージェリー（SSRF）などの一般的な脆弱性の検索が自動化されています。さらに、AI 主導で潜在的な影響の分析が行われ、修正手順に関する AI ベースの推奨事項が作成されます。

AI を含むシステムへの攻撃

AI、特に大規模言語モデル（LLM）を Web アプリケーションに統合したことにより、[新たなセキュリティ脆弱性](#)が生じました。プロンプトインジェクション攻撃は AI システムを標的とし、モデルの保護機能が無効化することを目的としています。注目すべき例としては、現在はパッチ適用済みである [Slack AI の脆弱性](#)があげられます。この脆弱性は、間接的なプロンプトインジェクションによるプライベートチャネルからのデータ収集を可能にしていました。データポイズニング攻撃は、ごく一部のデータセットを操作することで AI モデルのふるまいを破壊します。これにより、システムの整合性が損なわれる可能性があります。ジェイルブレイク手法は LLM 保護を回避し、攻撃者が制限を無効化して機微な情報を抽出し、有害な出力を生成できるようにします。このような新たな攻撃ベクトルに対しては、警戒の強化と新たな防御戦略が必要です。

高度な Web スクレイピング

AI によって Web スクレイピング機能が強化され、Web アプリケーションのセキュリティに新たな課題が生じています。現在、そのような AI ベースのスクレイピングツールによって、より効率的なデータ抽出方法がもたらされ、スクレイピング対策の回避が強化されています。2020 年代初頭から、[高度な Web スクレイピング](#)は AI を活用してデータを処理してきましたが、最近では LLM スクレイピングの頻度が大幅に増加しています。その多くはエージェントベースのクエリーが増えていることに起因するため、リアルタイム（非静的）データソースの需要が高まっています。

遺憾なことに、これらの要因により、平均的な Web アプリケーションリクエスト（リクエストの複雑さやホスティングインフラなどの要因による）は、1 件あたり 0.01~0.50 ドルのコストがかかるようになりました。当初、LLM スクレイピングの増加により最も影響を受けた業界はコマースでしたが、状況が変化し、現在では、他の業界（金融サービス、ギャンブル、デジタルメディア、動画メディアなど）がこの変化の最も大きな影響を受けています。

AI ベースの WAF システム

良い面として、高度な WAF システムは AI を活用して、ボット、DDoS 攻撃、スクレイパー、スキャナーなどのさまざまなサイバー脅威をより効果的に特定し、緩和できるようになっています。静的なルールセットを使用する従来の WAF ではゼロデイ脅威に対処できず、手動での更新が必要となるため、高度なサイバー攻撃に対処するためには [AI ベースの WAF システム](#)が役立ちます。

多層的な機械学習戦略により、パターン認識、アダプティブラーニング、異常検知を行い、応答時間を強化させることができます。AI ベースの WAF システムの目的は、日々発生する何十億件ものイベントを学習し、継続的な監視を伴う多層的なアプローチを採用することで、進化する脅威をプロアクティブに防止し、顧客を常に保護することです。

業界別のトレンド

全業界の中でも、コマース業界が他のすべての業界を大きく上回っており、2023 年第 1 四半期から 2024 年第 4 四半期の間に発生した Web 攻撃の件数はハイテク業界（攻撃数第 2 位の業界）の約 3 倍を記録しました（図 7）。さらに、同時期にコマース業界で発生した API 攻撃の件数は、上位 10 位以内の他の業界で発生した API 攻撃の総数を大幅に上回っています。

業界別の Web 攻撃数
2023 年 1 月 1 日～2024 年 12 月 31 日

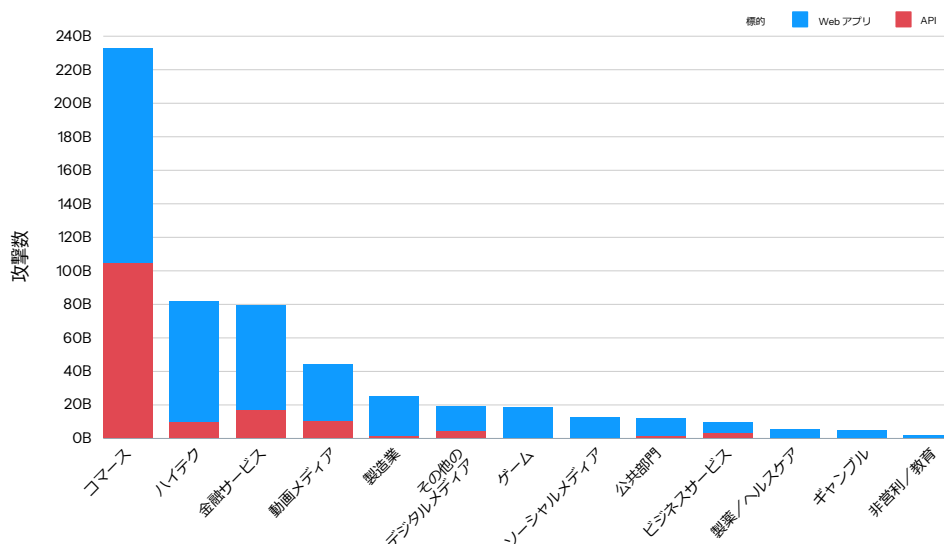


図 7 : Web 攻撃の標的となった業界のトップ 3 は、コマース、ハイテク、金融サービス

レイヤー 7（アプリケーションレイヤー）DDoS 攻撃全体では、ハイテク業界が他のどの業界よりも標的にされることが多く、2023 年第 1 四半期から 2024 年第 4 四半期の間に 7 兆件以上の攻撃が発生しました。ハイテク業界に次いで多かったのは、ソーシャルメディア業界とコマース業界でした（図 8）。しかし、同じ期間に発生した API を標的とするレイヤー 7 DDoS 攻撃の件数を見ると、コマース業界に対する攻撃数が、他のすべての業界に対する攻撃の合計を大幅に上回りました。

業界別のレイヤー7 DDoS 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日

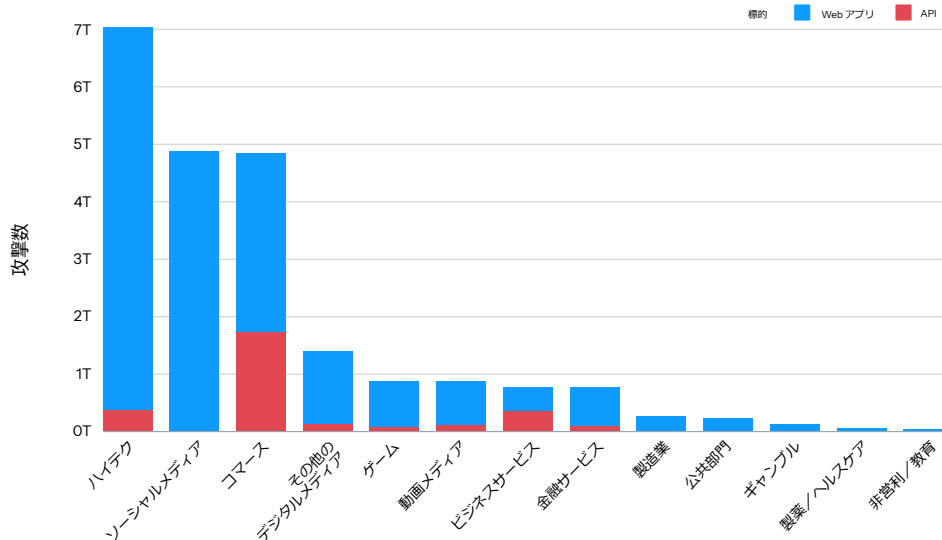


図 8：業界別のレイヤー7 DDoS 攻撃数

コマース

2023 年から 2024 年にかけてコマース業界は 2,300 億件以上の Web 攻撃（全 Web 攻撃の 40% 以上）を受けただけでなく、かつてない規模のレイヤー7 DDoS 攻撃に直面し、Akamai のデータによると 2023 年から 2024 年の攻撃数は 4.8 兆件を超えました。

この合計攻撃量は、Web アプリケーションが攻撃の約 64.25% を占め、API が残りの 35.75% を占めるという戦略的なターゲティングパターンを示しています。この分布は、攻撃者が 2 つの攻撃ベクトルを利用してコマースプラットフォームを侵害していることを表しており、現代の脅威情勢の多面性を明らかにしています。

コマース組織には機微な顧客情報、決済情報、金融取引が集中するため、特に利益の出やすい標的となっています。窃取された決済認証情報、侵害された顧客アカウント、機密性の高い PII を通じて直接的に収益を得られるため、脅威アクターに金銭に直結する動機を与えることとなります。侵害されたデータを金銭的利益に変えるためにはさらなる手順を踏む必要がある業界とは異なり、コマースプラットフォームは多くの場合、直接悪用できる資産を攻撃者に与えます。

主要な標的としての小売業

小売業は、広範なコマース業界において最も標的とされている業界セグメントであり、いくつかの際立った特徴が原因で、不相応なほど多くの攻撃に直面しています。

小売業では一般的に、さまざまなプラットフォームとシステムを組み込んだ複雑なデジタルエコシステムを維持します。その積極的なデジタルトランスフォーメーションの取り組みは、多くの場合、包括的なセキュリティよりも市場投入までの時間を優先するため、セキュリティギャップが生じます。オムニチャネル戦略を採用すると、意図せずアタックサーフェスの複雑さを増大させることになります。さらに、サードパーティサプライヤーへの依存度が高いため、数多くの潜在的な脆弱性を有する複雑なサプライチェーンが形成されます。

トラフィックパターンに季節性があるため、攻撃者が標的として大量のインシデントを発生させる期間を予測することができます。たとえば、FBI の Internet Crime Complaint Center（インターネット犯罪苦情センター）によると、冬のホリデーシーズンにはサイバー犯罪インシデントが **25~30%** 増加します。E コマースプラットフォームも脅威の高まりに直面しており、12 月には年間平均と比較してサイバー攻撃が **31%** 増加します。

Web アプリケーション攻撃の進化

Web アプリケーション攻撃は、テクノロジーの進歩と攻撃手法の変化により、大きな変革を遂げています。脅威アクターは、ますます高度化した手法を使用して Web アプリケーションの脆弱性を悪用し、進化するセキュリティ対策を回避するために戦略を適応させています。自動化された攻撃ツールの増加と機械学習アルゴリズムの統合が組み合わさることで、攻撃者は小売企業の Web アプリケーションに対してより正確に標的を定めたキャンペーンを実行できるようになりました。

さらに、マイクロサービスアーキテクチャと API 主導の開発への移行により、アタックサーフェスが拡大したため、従来のセキュリティパラダイムの再評価が必要になっています。このような進化にはサイバーセキュリティ専門家によるプロアクティブなアプローチが必要であり、継続的な監視、適応型防御メカニズム、Web アプリケーション環境における新たな攻撃ベクトルに対する深い理解が重視されています。

ボットの脅威情勢

特に攻撃者が生成 AI 機能を組み込むことで、ボットの脅威情勢はテクノロジーの進歩を通じて急速に進化しています。この進化により、高速のゼロデイ攻撃や、従来の防御を回避する高度な回避手法が生まれ、攻撃戦略が強化されました。小売企業に対する AI ベースのボット詐欺攻撃が 2022 年 8 月から 2024 年 4 月までの期間に一貫して**増加**し、2024 年 1 月には 137% の急増を記録しました。検知の課題により、これらの脅威がさらに悪化しています。通常、企業がボット攻撃を特定するには 4 か月を要し、その間に財務的な損害と評判の失墜に見舞われます。

ボットは現在、小売業のサイバー情勢において中心的なベクトルとなっており、これによってアカウントの乗っ取り、クレジットカード詐欺、ギフトカードの不正使用が促進されています。ボットは、侵害されたサイトから窃取されたデータを他のサイトに対する Credential Stuffing 攻撃に利用することで、より広範な攻撃キャンペーンを実現する手段として機能し、小売業界のエコシステム全体に悪影響を及ぼします。このアクティビティはオンライン詐欺の「産業化」に貢献しており、グローバルな犯罪集団が自動化されたツールを使用して、手動では到底及ばない規模でオペレーションを拡大しています。

小売事業の Web アプリケーションと API を AI やボット関連の攻撃からより適切に保護する方法については、「[緩和策](#)」のセクションに列挙されている推奨事項を参照してください。

金融サービス

金融サービス業界は Web 攻撃の主要な標的となっており、レイヤー 7 DDoS 攻撃が継続して発生しています。2023 年 1 月から 2024 年 12 月までの期間中、Web 攻撃は計 790 億件を超え、同期間に Web アプリケーションと API の両方に対するレイヤー 7 DDoS 攻撃は計 7,610 億件を超えました。

この前例のない規模は、この業界に脆弱性があり、脅威アクターにとって魅力的であることを示しています。急増の背景には、グローバル経済インフラにおける同業界の役割の重要性、財務データの価値の高さ、大きな[混乱](#)が生じる可能性などいくつかの要因があります

金融サービスのデジタル化

金融サービスのデジタル化により、サイバー犯罪者にとってのアタックサーフェスが拡大しました。AI 主導のパーソナライズ、BaaS（Banking as a Service）、組み込み金融ソリューションの導入は、新たな脆弱性を生み出しました。地政学的な対立、特にロシア・ウクライナ戦争により、金融機関を[標的](#)としたハクティビスト活動が活発化しました。暗号資産（仮想通貨）の増加や暗号資産を裏付けとした準備通貨の導入の可能性により、金融業界に対する脅威アクターの[関心](#)が高まっています。

Web アプリケーション攻撃は急速に変化しており、新しいテクノロジーに適応して、新たな脆弱性を悪用しています。攻撃者は今や高度な AI と機械学習アルゴリズムを活用して、従来のセキュリティ対策を回避し、より標的を絞った持続的な攻撃を行っています。サーバーレスアーキテクチャとマイクロサービスの増加により、新たな攻撃ベクトルが生まれると同時に、API の使用が増加して、攻撃者の潜在的なエントリーポイントが拡大しました。さらに、モバイルアプリケーションやクラウドベースのアプリケーションへの移行に伴い、データ保護やアクセス制御において独自の課題を抱えるこれらのプラットフォームに対応するため、セキュリティ戦略の見直しが不可欠となっています。

攻撃の標的として突出している銀行セグメント

金融サービス業界内でも、銀行は最も Web 攻撃の標的として最も注目されている部門です（図 9）。コマース業界と同様に、銀行セグメントでも [Credential Stuffing](#) 攻撃が主要な脅威ベクトルとして台頭してきています。

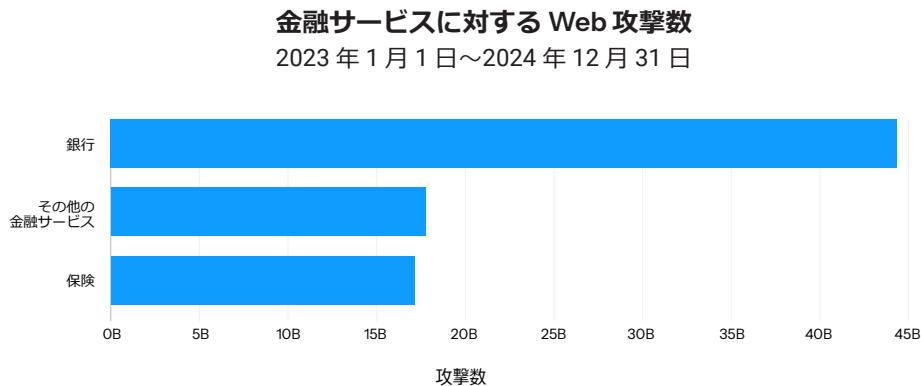


図 9：金融サービス業界の中で、最も Web 攻撃の標的とされているセグメントは銀行

オンライン・バンキング・サービスの普及とアカウントアクセスの重要性が、サイバー犯罪者を引き寄せています。攻撃が成功した場合の金銭的利益は莫大であり、少数のアカウントを侵害するだけでも大きな利益が生まれる可能性があります。銀行セグメントは、多要素認証など、ユーザー体験を損なう可能性のある厳格なセキュリティ対策を実施することに前向きではなく、それが意図せず脆弱性の一因となりました。

銀行部門が攻撃の標的として特に目を付けられていますが、その状況は複数の要因によりさらに悪化しています。脅威アクターはサービスの中断に関する懸念を悪用するため、ダウンタイムに対する敏感さは脅迫の機会を与えることになります。さらに、AI や機械学習を利用して検知を回避するなど、攻撃手法の高度化により、従来の防御メカニズムに大きな課題が突きつけられています。厳格なコンプライアンス要件が定められ、セキュリティ侵害が生じた場合に罰金を科される可能性のある規制環境では、銀行セグメントのサイバーセキュリティの課題が一層複雑化します。

ハイテク

ハイテク業界は依然として、Web 攻撃とレイヤー 7 DDoS 攻撃の主要な標的産業として、変わらず上位にランクインしています。本レポートにおけるハイテク業界には、通信、エンタープライズソフトウェアおよびハードウェア、コンシューマーソフトウェアおよびハードウェアの業界セグメントが含まれます。Akamai のデータによると、この業界は Web 攻撃の総数がコマースに次いで多く、2023～2024 年の期間に 817 億件を超える攻撃を受けました。また、ハイテク産業はレイヤー 7 DDoS 攻撃の標的となった産業として最も多く、2 年間で 7 兆件を超える攻撃を受けました。

ハイテク業界の Web アプリケーションは複雑なデータベースクエリーや動的コンテンツを使用することが多いため、攻撃者が悪用してサーバーを簡単に過負荷状態にできる脆弱性が生じます。このような脆弱性は、同業界が受けたレイヤー 7 DDoS 攻撃の大部分に寄与しています。特に、**ブロックチェーンネットワーク**に対する DDoS 攻撃が大幅に増加しており、ブロックチェーンは分散型アーキテクチャであるにもかかわらず、攻撃者は HTTP フラディングやスパムトランザクションなどの手法を使用して正当なトランザクションを妨害しています。ハイテク業界では運用ダウンタイムによって重大な財務的影響が生じることが、攻撃者が重要なサービスを機能不能にできる DDoS 攻撃を展開する動機となっています。現代のソフトウェア開発は API 中心のアーキテクチャに依存しているため、さらなるリスクが生じます。これは、攻撃者は HTTP フラッド攻撃において、コードの安全性が低いエンドポイントを悪用することが多いためです。

通信セグメントも同様の課題に直面

通信セグメントは大量の API 攻撃の影響を受けており、同様のサイバーセキュリティの課題に直面しています。このハイテク業界セグメントにおける Web アプリケーションおよび API の脅威には、データ漏えい、DDoS 攻撃、サプライチェーンの脆弱性が含まれます。これらの脆弱性により、複数の重大なデータ漏えいが発生しています。

たとえば、2025 年 1 月には、研究者が**大手通信ネットワーク**に重大な API の脆弱性を発見しました。この脆弱性により、3,000 社の企業がセキュリティリスクにさらされました。この調査では、顧客の本人確認 (Know Your Customer) プロセスの脆弱性や、内部システムへのアクセスを可能にするバックエンド API パストラバーサル脆弱性など、重大なセキュリティ上の欠陥が明らかになりました。

IoT (モノのインターネット) により、新たな攻撃ベクトルが発生

テクノロジーが急速に進歩している時代において、ハイテク業界は進化し続ける Web アプリケーションと API の脆弱性に対処し続けています。この進化には IoT (モノのインターネット) デバイスの普及が含まれており、多くのデバイスは堅牢なセキュリティ対策を備えていないため、新しい攻撃ベクトルが生まれています。マルチクラウドインフラが急速に導入されると、多くの場合、環境の構成が不適切になりやすく、攻撃に利用される可能性のあるエントリポイントが生じます。

セキュリティ対策が不十分な IoT デバイスやクラウドシステムの脆弱性が、高度な **AI 主導の攻撃**に悪用されるケースが急増しています。**SaaS プラットフォーム**はアタックサーフェスが広範であるため、API 攻撃のリスクが高まっています。AI ソリューションの普及とサードパーティ SaaS プラットフォームへの依存が上昇したことにより、ハイテク業界全体で API アタックサーフェスが大幅に拡大しました。組織がこれらのテクノロジーの導入を進める以上、攻撃を受ける可能性が高まるため、堅牢なセキュリティ対策と注意深い監視が必要になります。

地域別のトレンド

注：地域レポートの形式を変更して、読者がデータをより容易に閲覧できるよう改善しました。北米、アジア太平洋・日本（APJ）、欧州・中東・アフリカ（EMEA）、ラテンアメリカ（LATAM）の各地域における攻撃のトレンドを分かりやすく強調できるようになりました。また、本セクションで説明するデータを一目で確認できる表も用意しました（図10）。

地域	Web 攻撃数	レイヤー7 DDoS 攻撃数	主な Web 攻撃ベクトル	標的となった主なエリア	標的となった主な業界
APJ	800 億件、14% API	7.4 兆件、6% API	アクティブな攻撃セッション、LFI、XSS	オーストラリア（203 億件）、インド（173 億件）、シンガポール（159 億件）	金融サービス、コマース、ソーシャルメディア
				シンガポール（4.7 兆件）、インド（6,070 億件）、韓国（2,830 億件）	ソーシャルメディア、その他のデジタルメディア、コマース
EMEA	1,160 億件、37% API	2.6 兆件、20% API	アクティブな攻撃セッション、API リクエストの制約違反、LFI	英国（303 億件）、オランダ（195 億件）、スペイン（142 億件）、ドイツ（128 億件）	コマース、動画メディア、金融サービス
				ドイツ（5,690 億件）、英国（5,060 億件）	コマース、その他のデジタルメディア、動画メディア
LATAM	30 億件、12% API	2,580 億件、18% API	アクティブな攻撃セッション、WAT、SSRF	ブラジル（193 億件）、メキシコ（20 億件）	コマース、金融サービス
				ブラジル（1,750 億件）、メキシコ（390 億件）	コマース、金融サービス
北米	3,270 億件、29% API	11.9 兆件、16% API			

図10：一目で分かる地域別のトレンド、2023年1月～2024年12月（LFIはローカル・ファイル・インクルージョン、XSSはクロスサイトスクリプティング、WATはWeb攻撃ツール、SSRFはサーバーサイド・リクエスト・フォージェリー）



アプリケーションおよび API 攻撃の2つのトレンド

Akamai が 2023 年 1 月から 2024 年 12 月までの 24 か月間のレポート期間における Web アプリケーションおよび API 攻撃とレイヤー 7 DDoS 攻撃の地域別比較分析を行ったところ、2 つの大きなトレンドが明らかになりました（図 11）。

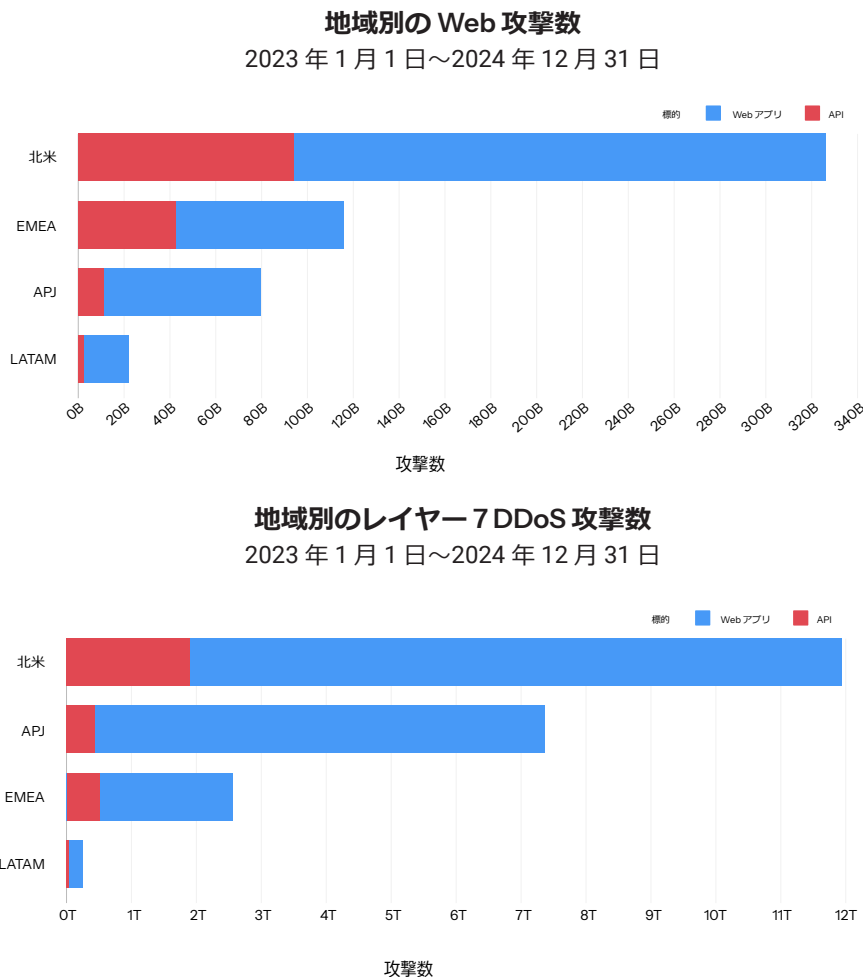


図 11：レポート期間中、全世界で、API 攻撃の割合が最も大きかったのは EMEA で、APJ はレイヤー 7 DDoS 攻撃の総数が 2 番目に多かった

攻撃のトレンド 1： API 攻撃は EMEA で広く発生しました。その原因は、[API の普及率が他の地域よりも高い](#)ことに加え、オープンバンキングや [PCI DSS v 4.0](#) によって API の使用が促進され、セキュリティリスクが生じる可能性があることであると考えられます。（API 固有のリスクに関する詳細な説明については、「[Akamai の API 脅威インテリジェンスの進化](#)」のセクションを参照してください）。

Akamai が [2023 年に初めて観測](#)したトレンドが継続しており、この 24 か月間で API に対する Web 攻撃の割合が最も大きかった地域は EMEA でした。この地域で発生した Web 攻撃の総数 1,160 億件のうち、37% が API を標的としたものでした。一方、北米で記録された Web 攻撃の総数は 3,270 億件で、そのうち 29% が API に対する攻撃でした。API を標的とした攻撃の割合は、APJ では 800 億件の Web 攻撃のうち 14%、次いで LATAM では 30 億件のうち 12% でした。

また、API を標的としたレイヤー 7 DDoS 攻撃の集中度が最も高かった地域は EMEA（20%）、次いで LATAM（18%）、北米（16%）、APJ（6%）でした。一般的に、各地域における API を対象としたレイヤー 7 DDoS 攻撃の試行回数は、Web 攻撃全体に占める割合としては比較的低い水準にとどまっています。この割合は、ボット主導型攻撃の高度化や API の脆弱性に対する AI 主導型攻撃の急増といったさまざまな理由で次第に増加すると予想されます。

攻撃のトレンド 2： APJ はレイヤー 7 DDoS 攻撃の件数が全世界で 2 番目に多く、7.4 兆件でした（北米では 11.9 兆件）。次いで EMEA は 2.6 兆件、LATAM は 2,580 億件でした。このトレンドは Akamai の [SOTI レポート「包囲されるデジタル要塞」](#) で最初に観測されたものであり、Akamai は引き続き、その原因は APJ がソーシャルメディアに対する攻撃の試みの割合が最も大きい地域であると考えています。

APJ、EMEA、LATAM の詳細な分析

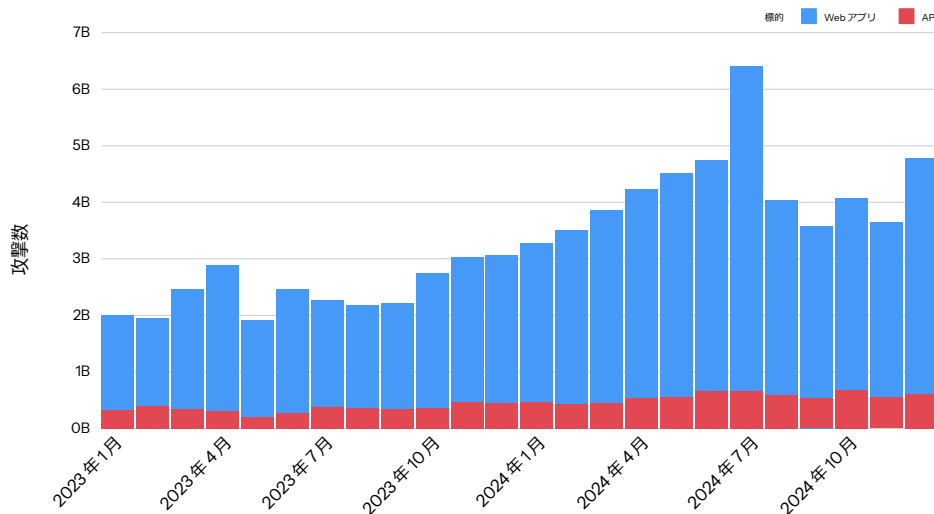
このセクションでは、APJ、EMEA、LATAM の主なトレンドについて説明します。また、これらの地域内の特定のエリアについて、Akamai が統計的に有意な知見を提供できる十分な攻撃イベントデータを保有している場合は、そのエリアに固有のデータも取り上げます。

Web アプリケーションおよび API 攻撃：トラフィックの分析

月別の Web 攻撃のトレンドを地域間で比較すると、はっきりとした差異が見られます（図 12）。

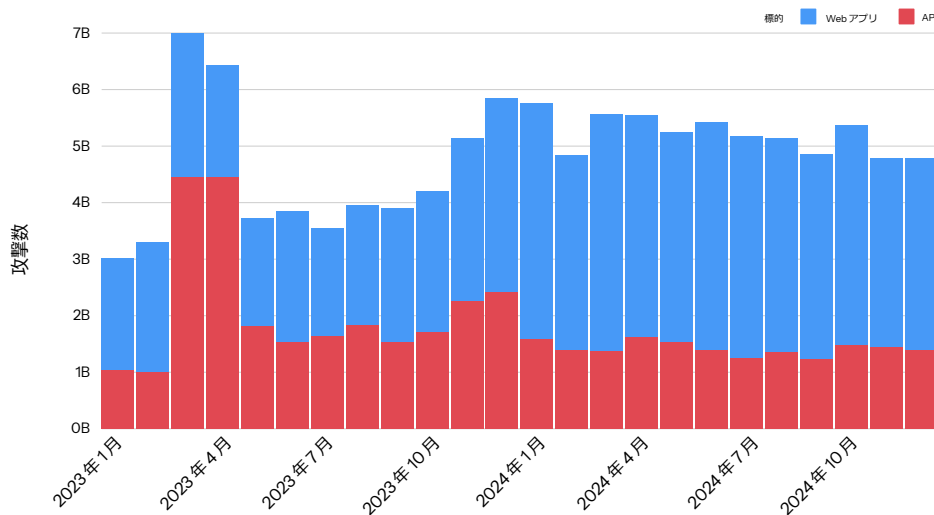
アジア太平洋・日本地域：月別の Web 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日



EMEA : 月別の Web 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日



南米 : 月別の Web 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日

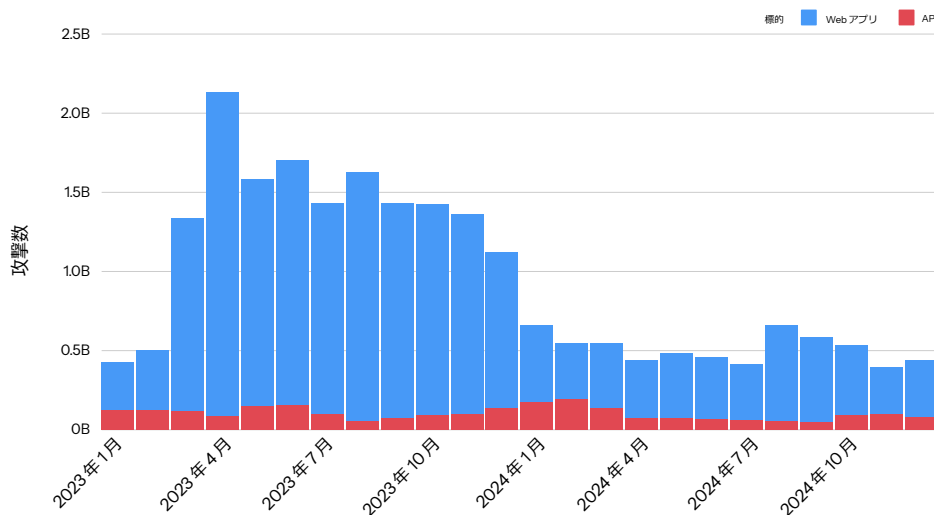


図 12 : Web アプリケーション攻撃アクティビティにより、APJ と EMEA では Web 攻撃の総数が増加したが、LATAM では急激に減少した

APJ で発生した Web 攻撃の総数は、2023 年には 290 億件でしたが、2024 年には 510 億件に増加し、前年比で 73% の大幅増となりました。EMEA では、前年比 16% の緩やかな増加（540 億件から 620 億件）でした。しかし、この小幅の増加は、データに異常値イベントが記録されていることの影響を受けたものであり、それを取り除くと、この数値は 33% 近くに上昇します。LATAM では、Web 攻撃の総数が 2023 年には 160 億件だったのに対し、2024 年には 600 万件に激減し、前年比で 61% の減少となりました。

特に APJ と LATAM では API 攻撃数が依然として低水準であるため、Web アプリケーション攻撃の増加に伴って Web 攻撃の総数が増加しているようです。

EMEA では、2023 年前半にスペインのコマース業界に対する大規模な集中攻撃に関連して API 攻撃が急増しましたが、その後は 2024 年を通じて低い水準にとどまりました。しかし、他の地域と比較すると、依然として高い水準にあります。

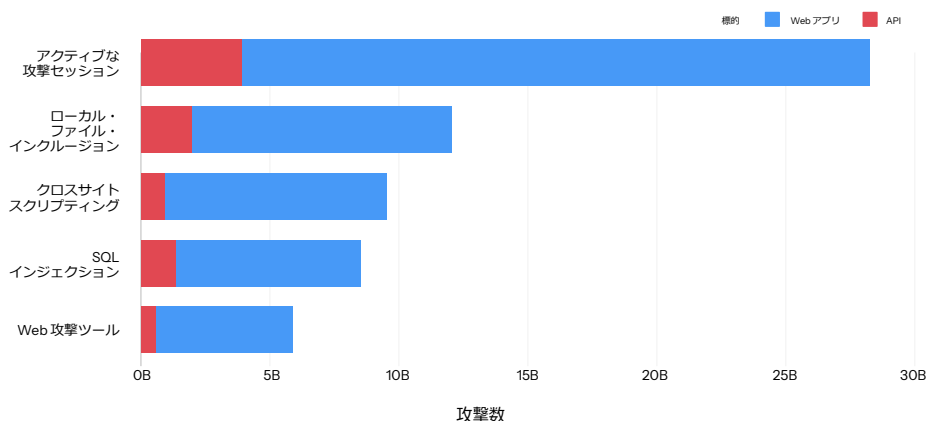
LATAM では、脅威アクターがコマース業界から他の業界（医薬品やビジネスサービスなど）に焦点を移し、攻撃のタイプについてもランサムウェアなどに重点を置くようになったため、Web 攻撃が減少しました。

Web アプリケーションおよび API 攻撃：戦術のトレンド

過去 2 年間にわたり、脅威アクターは従来の実証済みの手法に依存し続けていましたが、現代的なふるまいベースの Web 攻撃ベクトルが使用されることも多くなりました（図 13）。

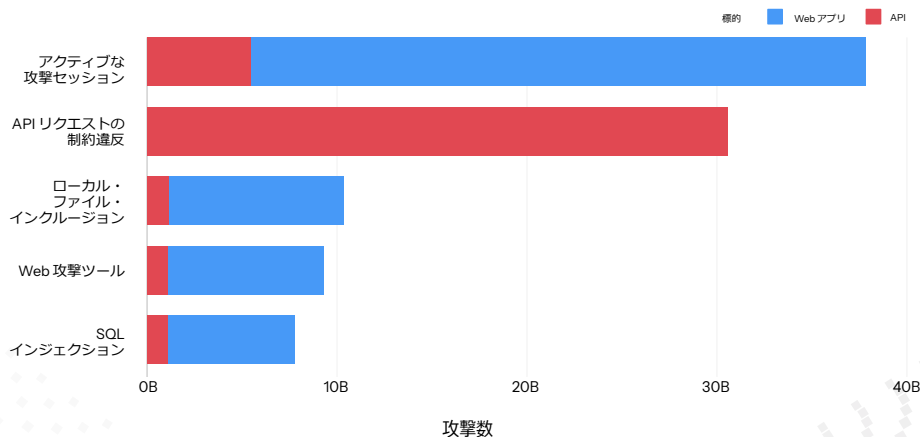
アジア太平洋・日本地域：攻撃ベクトル別の Web 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日



EMEA：攻撃ベクトル別の Web 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日



南米：攻撃ベクトル別の Web 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日

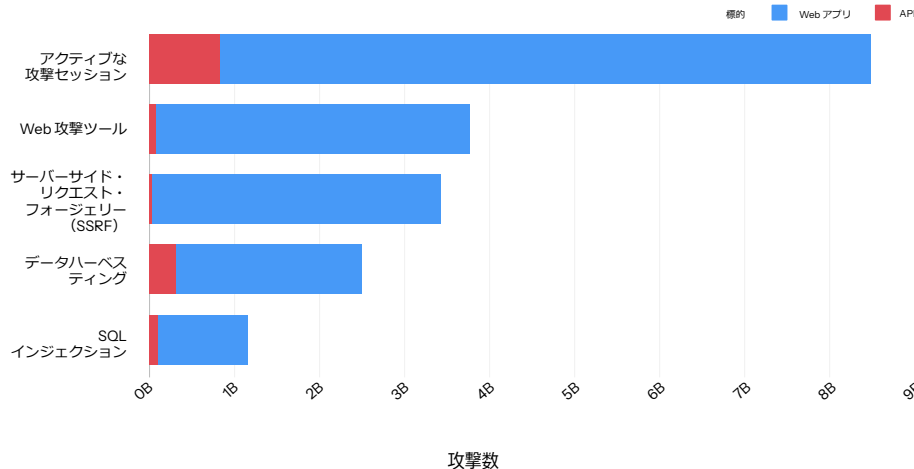


図 13：どの地域でも、上位の攻撃ベクトルには、従来の手法と、特に API の悪用を目的とした現代的なふるまいベースの手法が含まれていた

全世界のトレンドと同様に、各地域で LFI、SQLi、XSS などの従来の攻撃ベクトルが存続しており、LATAM では SSRF も観測されました。Akamai は「[Defenders' Guide 2025](#)」において、XSS は依然として強力な攻撃手法であり、従来の Web 脆弱性を防ぐ上で継続的な重要性を有することを強調しました。

この期間で変わったことは、脅威アクターが API の悪用にますます重点を置くようになっていたため、現代的なふるまいベースの攻撃ベクトルに関する問題が増加したことです。脅威アクターは、そのようなベクトルを使用して脆弱性を探索し、悪用します。そのようなベクトルを地域レベルで追跡したところ、Akamai の研究者は次のことを観測しました。

- 各地域で最も多い攻撃ベクトルは、アクティブな攻撃セッションでした。これに対しては、Akamai のインテリジェントな制御を使用して、既知の脅威アクターからのリクエストが長期間プロアクティブにブロックされています。
- API リクエストの制約違反は、API を狙った攻撃の割合が最も大きい地域である EMEA において 2 番目に多い攻撃ベクトルでした。攻撃者は、レート制限やデータ入力などの要件を回避して API を悪用しようとします。
- 各地域で Web 攻撃ツールは 5 位以内に入っていました。脅威アクターは、このベクトルを使用して標的を調査し、不正な目的で利用できるセキュリティ、設定、潜在的な脆弱性に関する情報を集めます。

これらの上位のベクトルについて、詳しくは「[Web 攻撃](#)」のセクションを参照してください。

Web アプリケーションおよび API 攻撃：主な標的

各地域内のどこに攻撃者が重点をおいているかを見てみると、API ではオーストラリア（203 億件）、インド（173 億件）、シンガポール（159 億件）に Web アプリケーション攻撃と API 攻撃の矛先が向けられており、日本（63 億件）、中国（62 億件）、韓国（49 億件）、ニュージーランド（29 億件）、香港特别行政区（22 億件）がそれに続きます。

EMEA で Web アプリケーション攻撃と API 攻撃の影響を最も受けた国は、英国（330 億件）、オランダ（195 億件）、スペイン（142 億件）、ドイツ（128 億件）でした。次いで、オーストラリア（82 億件）、フランス（75 億件）、イタリア（41 億件）、スイス（37 億件）、ベルギー（35 億件）、イスラエル（33 億件）となりました。

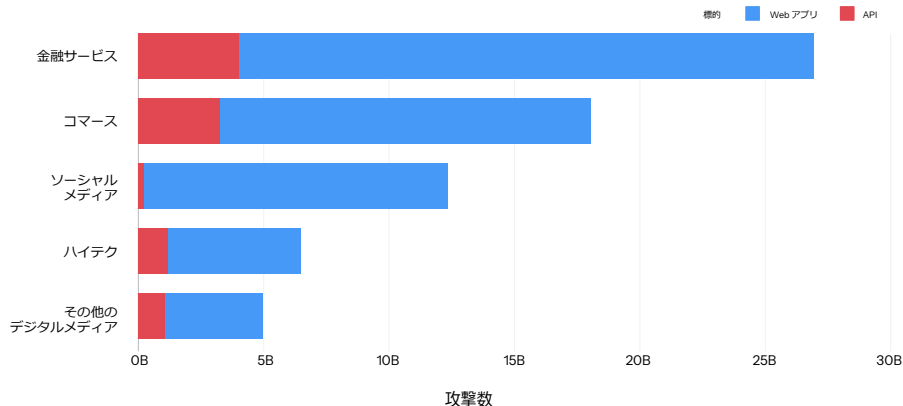
LATAM では、Web アプリケーションおよび API 攻撃はブラジル（193 億件）に集中しました。次いで多いのはメキシコ（20 億件）とチリ（4 億件）ですが、これらはこの地域で発生した攻撃のほんの一部に過ぎません。

標的となる業界

業界別のトレンドを分析したところ、APJ、EMEA、LATAM で、Web 攻撃の標的となっている業界の 3 位以内にコマースと金融サービスが一貫して含まれていることが分かりました（図 14）。

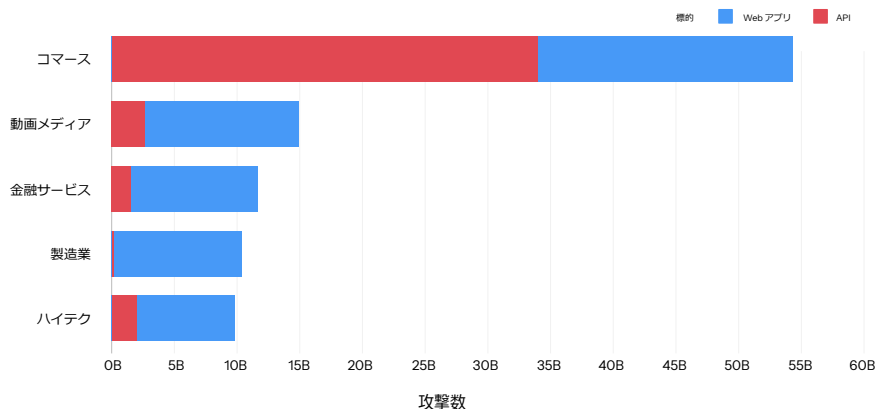
アジア太平洋・日本地域：業界別の Web 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日



EMEA：業界別の Web 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日



南米：業界別の Web 攻撃数 2023 年 1 月 1 日～2024 年 12 月 31 日

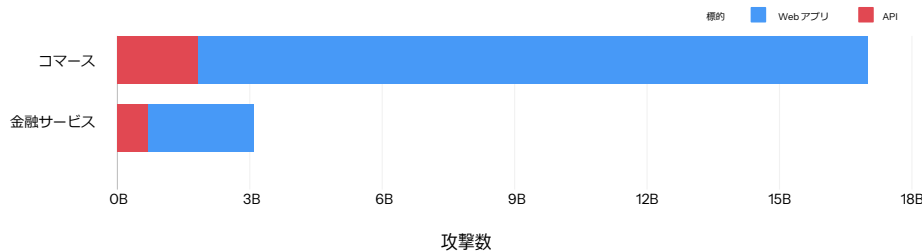


図 14：APJ、EMEA、LATAM 地域では、標的とされている業界の 3 位以内にコマースと金融サービスが含まれていた

APJ で Web 攻撃総数が最も多かった業界は金融サービス（270 億件）で、次いでコマース（180 億件）でした。これはそれぞれ、前年比で 52% と 161% の増加率です。API 攻撃の標的となった業界は、その他のデジタルメディア（22%）が最も多く、コマース（18%）と金融サービス（15%）がそれに続きました。

EMEA で最も Web 攻撃の影響を受けた業界はコマース（54 億件）で、第 2 位の業界の 3 倍以上の件数でした。このように大きな割合を占めているものの、コマース企業に対する Web 攻撃の総数は前年比で 10% 減少しています。これは、同地域では 2023 年の急増によってデータが歪められたためです。しかし、EMEA では、金融サービス（152%）や製造（96%）など、他の業界に対する攻撃の増加により、Web 攻撃の総数が前年比で 16% 増加しています。この地域における API を標的とした攻撃を詳しく見てみると、コマースに対する Web 攻撃全体の 63% が API を標的としていたことが分かります。

LATAM でも同様のトレンドが見られ、コマース業界に対する Web 攻撃の総数は 170 億件に達し、他の業界を大きく上回っていますが、コマース業界に対する攻撃は前年比で 76% 減少しました。一方、製薬業界とビジネスサービス業界は、それぞれ前年比 107% 増、129% 増となっています。さらに、コマースに対する攻撃の 11% は API を狙ったものでした。金融サービス業界では API を狙った攻撃の割合がさらに大きく、23% でした。

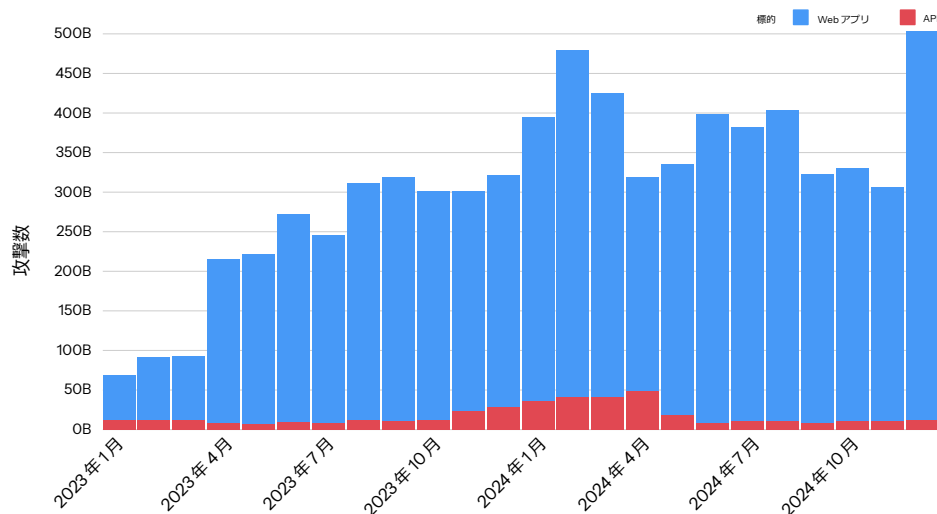
金融サービス業界とコマース業界には、Web アプリケーションおよび API 攻撃の標的として魅力的である共通の要因があります。それは、どちらの業界も複雑なエコシステム内で事業が運営されており、API への依存度が高く、貴重なデータを保有していることです。脅威アクターは、従来の攻撃手法と新たな攻撃手法を組み合わせ、目標を達成しようとしています。

レイヤー7 DDoS 攻撃：トラフィックの分析

各地域の月別のレイヤー7 DDoS 攻撃数のトレンドを比較すると、API がホットスポットであり、EMEA と LATAM では攻撃の増減が繰り返されました（図 15）。

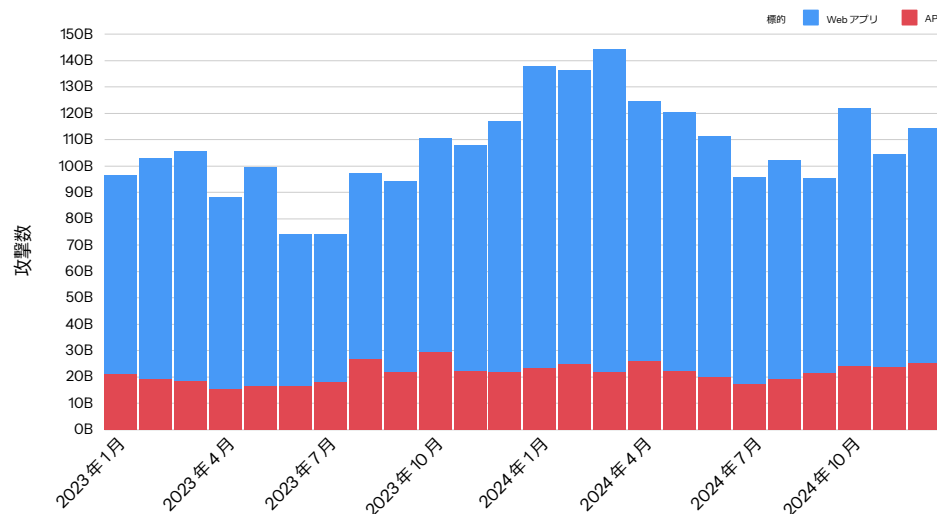
アジア太平洋・日本地域：月別のレイヤー7 DDoS 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日



EMEA：月別のレイヤー7 DDoS 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日



南米：月別のレイヤー7 DDoS 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日

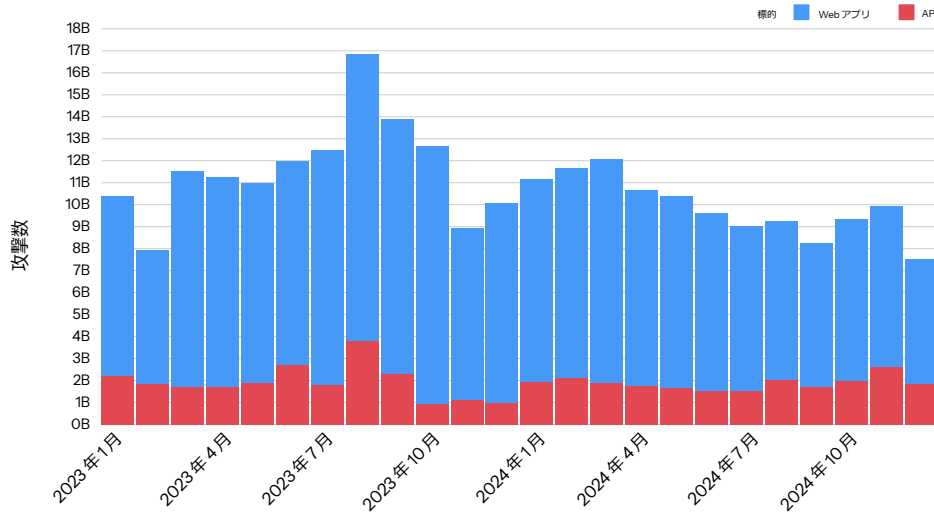


図 15：レイヤー 7 DDoS 攻撃は APJ と EMEA で増加したが、LATAM では 2024 年に減少した

APJ では、レイヤー 7 DDoS 攻撃が前年比で 66% 増加して、24 か月ぶりに最高値に達し、ピークは 2024 年 12 月の 5,040 億件でした。この増加は、主にソーシャルメディア業界を狙った攻撃が要因でした。

EMEA では、レイヤー 7 DDoS 攻撃が 2024 年 3 月に約 145 億件でピークに達しました。その後は減少して、再び増加し、前年比 20% の増加率を達成しました。その原因は、地政学的要因と技術的要因が重なったことであると考えられます。同地域で続いている緊張状態が、ハクティビストの活動に拍車をかけました。このトレンドは、AI によって強化されたツールと DDoS as a Service プラットフォームの台頭によってサイバー犯罪者の参入障壁が低くなったことにより、さらに悪化しています。

LATAM では、レポート期間の早い段階でレイヤー 7 DDoS 攻撃の試みが大幅に増加し、それと同時に API リソースを過負荷状態にすることを目的とした [HTTP フラッド攻撃](#) も増加しました（この攻撃ベクトルについては、「[レイヤー 7 DDoS 攻撃：前年との比較とトレンド](#)」のセクションで詳しく取り上げています）。攻撃は 2023 年 8 月に 168 億件でピークに達し、それ以降は減少を続けて 75 億件まで低下し、前年比 15% 減となりました。

レイヤー7 DDoS 攻撃：主な標的

Akamai の以前のレイヤー7 DDoS 攻撃分析と比較して、各地域内で脅威アクターが標的としたエリアや業界にほとんど変化は見られませんでした。

APJ では、シンガポールが 4.7 兆件と最も攻撃が集中し、次いでインド（1.1 兆件）、韓国（6,070 億件）、インドネシア（2,830 億件）、中国（2,460 億件）、日本（1,110 億件）、オーストラリア（1,080 億件）、台湾（810 億件）と続きます。

EMEA でレイヤー7 DDoS 攻撃が最も多く発生した国はドイツ（5,690 億）と英国（5,060 億）で、イスラエル（2,050 億）、スウェーデン（1,930 億）、マルタ（1,600 億）が続きました。これらに加え、イタリア（1,580 億）、スイス（1,470 億）、フランス（1,290 億）、オランダ（1,110 億）、スペイン（960 億）がトップ10 にランクインしました。

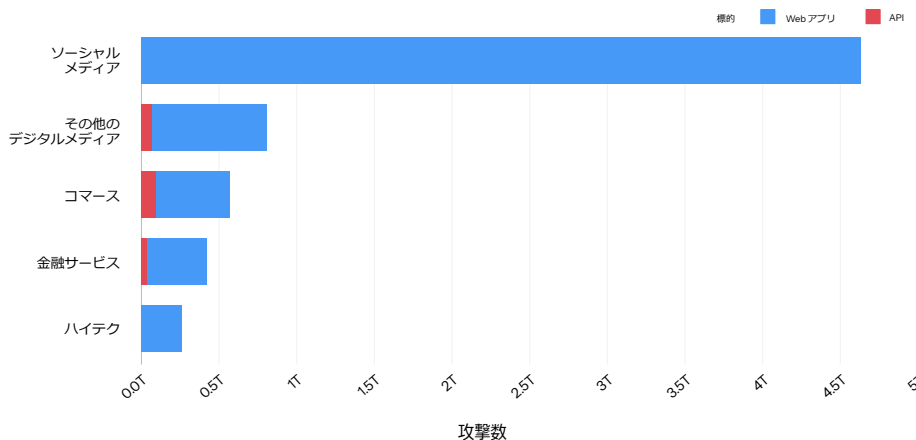
LATAM では、ブラジルが 1,750 億件で最もレイヤー7 DDoS 攻撃が集中し、メキシコ（390 億件）とコスタリカ（190 億件）がそれに続きました。

標的となる業界

APJ と EMEA でレイヤー7 DDoS 攻撃の影響を受けた主な業界（図 16）は、[アプリのセキュリティ確保に関する以前の SOTI レポート](#)から変わっていません。そのレポートで詳述したとおり、APJ におけるソーシャル・メディア・プラットフォームに対するレイヤー7 DDoS 攻撃は、広範な軍事衝突や世界中で大きく報じられた選挙イベントに連動して、2023 年 1 月から 2024 年 6 月まで急増しました。地政学的混乱の発生中にソーシャル・メディア・プラットフォームは大量のトラフィックを受信するため、これは驚くべきことではありません。予想通り、2024 年後半には APJ と米国の両方で選挙があったため、このトレンドが強まりました。これらの要因が寄与し、同業界への攻撃は前年比で 130% 増加しました。

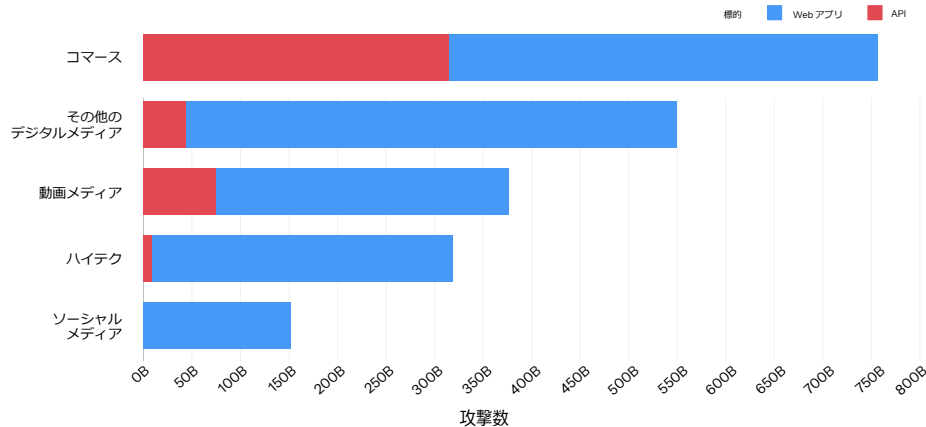
アジア太平洋・日本地域：業界別のレイヤー7 DDoS 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日



EMEA：業界別のレイヤー7 DDoS 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日



南米：業界別のレイヤー7 DDoS 攻撃数

2023 年 1 月 1 日～2024 年 12 月 31 日

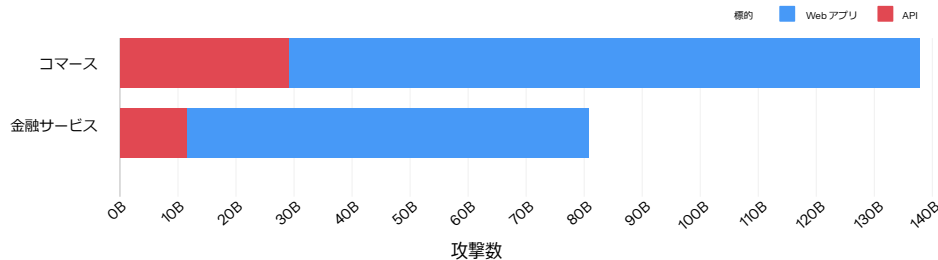


図 16：影響を受けた主な業界に関する各地域の分析結果は以前の分析以来変わっておらず、最も API に対するレイヤー 7 DDoS 攻撃の標的となった業界はコマースで一貫していた

EMEA では、レイヤー 7 DDoS 攻撃の影響を最も受けた業界は相変わらずコマースであり、他のデジタルメディアや動画メディアがそれに続きました。この攻撃の前年比増加率が最も大きかった業界は、ハイテク（70%）、ソーシャルメディア（23%）、コマース（14%）でした。この変化は、攻撃者が業界間や地域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、より広範なトレンドを追跡する価値があることを表しています。

LATAM でもコマースは最もレイヤー 7 DDoS 攻撃の標的となった業界であり、第 2 位は金融サービスでした。レポート期間中、レイヤー 7 DDoS 攻撃アクティビティの継続的水準は、業界全体でほぼ一貫していました。

全世界のトレンドとして、レイヤー 7 DDoS 攻撃の標的となることが多かった業界の中でも、各地域で API に対する攻撃の割合が最も大きかった業界はコマース業界でした。EMEA ではコマースに対する攻撃の 43% が API を標的としたものであり、この割合は LATAM では 21%、APJ では 16% でした。

地政学的な混乱が発生したことや、注目度の高いサービスが混乱に陥ると経済的影響が生じる可能性があることなどの複数の理由から、コマース、メディア、金融サービスは過去 2 年間、EMEA と LATAM におけるレイヤー 7 DDoS 攻撃の主な標的となりました。コマース業界や金融サービス業界に対する高水準の攻撃アクティビティの背後にある要因と手法について、詳しくは「[業界別のトレンド](#)」のセクションを参照してください。

コンプライアンス

全世界と北米の視点

2025 年の全世界のサイバーセキュリティ情勢の特徴は、かつてないほどの複雑さと不安定さです。地政学的な緊張、特にウクライナと中東で続いている紛争により、サイバー脅威や国家の支援を受けた攻撃が激化しました。とりわけ西側諸国を標的とする親ロシアグループによるハクティビズムの増加が原因で、脅威情勢はさらに複雑化しました。経済的には、さまざまな業界の急速なデジタルトランスフォーメーションによってアタックサーフェスが拡大しており、サイバー犯罪者は重要なインフラを標的にし、AI などの高度なテクノロジーを活用して能力を高めています。

これらの要因が、世界規模の経済的圧力と主要国における政治的な変化と相まって、世界中のサイバーセキュリティ専門家にとって最悪の事態を引き起こしました。Web アプリケーションと API の保護は、組織にとって重要な課題です。倫理的なハッカー、サイバーセキュリティ専門家、Akamai などの組織は、これらのエントリーポイントのセキュリティ確保という緊急の課題に対応する取り組みを推進し、増加するコンプライアンスに関する検討事項を補完します。

世界中の規制機関は、アプリケーションに対してより厳格なサイバーセキュリティコンプライアンス要件を施行しています。北米では、包括的なリスク管理戦略とインシデント報告義務に焦点が移りました。米国の [Cyber Incident Reporting for Critical Infrastructure Act \(重要インフラ向けサイバーインシデント報告法\)](#) は、2026 年に発効する予定であり、重要インフラ組織が情報システムのインベントリを作成し、サイバーリスクを分類し、サイバーセキュリティポスチャを年 1 回以上の頻度で評価することを義務付けます。この法律は、特にエネルギー、化学製造、情報テクノロジーなどの重要な業界で使用されているアプリケーションに堅牢なセキュリティ対策が必要であることを強調しています。

同様に、カナダとメキシコもデータ保護と重要インフラのセキュリティに重点を置き、国際基準に準拠した規制の整備を進めています。具体的な規制はさまざまですが、世界的なトレンドは、入力検証の強化、安全な開発手法、定期的なセキュリティ監査など、アプリケーションのセキュリティ要件の厳格化に向かっています。

API セキュリティ情勢にも同様の課題があり、API はサービス統合とデータ交換を可能にする上で重要な役割を果たすため、サイバー犯罪者の主要な標的になりつつあります。世界中の規制機関は、組織に堅牢な API セキュリティ対策を実施することを求める、[より厳格な規制](#)を導入して対処しています。

これには、継続的な API 探索、監視、進化する脅威からの保護が必須です。北米では、API エコシステムのリスク評価を徹底することに重点が置かれ、安全な開発手法、堅牢な認証メカニズム、リアルタイムの脅威検知機能が重視されています。AI 主導の SaaS ツールが急速に導入され、多くの場合 API を介して統合されているため、アタックサーフェスが大幅に拡大し、規制当局はより高度なセキュリティアプローチを要求するようになりました。

特に AI や機械学習アプリケーションの普及に伴って、API 環境の複雑さが増しているため、データ漏えい、不正アクセス、サービスの中断に関連するリスクを緩和するためにコンプライアンス要件が進化しています。APJ、LATAM、EMEA などの地域では独自の規制が整備されつつありますが、全世界のトレンドは、API セキュリティ標準の調和を図り、現代的なデジタルアーキテクチャの相互接続性に対処する方向に向かっています。

API の視点

アジア太平洋・日本地域では、さまざまな業界の組織に影響を与えている新たなコンプライアンス要件により、規制環境が大幅に変化しています。シンガポールでは最近、[サイバーセキュリティに関する法案](#)が修正され、クラウドプラットフォーム上でホストされているシステムや[海外](#)に置かれているシステムを含め、物理とバーチャルの両方の重要な情報インフラシステムを対象とするように範囲が拡大されました。日本では、[内閣サイバーセキュリティセンター](#)の法律が改正されました。インドでは、[Digital Personal Data Protection Bill（デジタル個人データ保護法）](#)の可決に伴い、IT 法が見直されました。オーストラリアは 2023-2030 Cyber Security Strategy（2023～2030 年サイバーセキュリティ戦略）を導入しました。これにより、同地域ではサイバーセキュリティ対策の強化にさらに重きが置かれることになりました。この戦略の一環として、2024 年後半に Australian Security of Critical Infrastructure Act（オーストラリア重要インフラ安全保障法）が改正され、新しい [Cyber Security Act 2024（2024 年サイバーセキュリティ法）](#)が成立しました。機微な情報を処理する IoT デバイス、アプリケーション、API などの二次資産も対象となります。これらの規制の変化により、組織は特に重要インフラと機微な情報の保護に重点を置いて、Web アプリケーションのセキュリティ慣行を再評価し、強化することを余儀なくされています。

[PCI DSS v4.0.1](#) は、決済カードデータを処理する組織に大きな影響を及ぼすことが予想されています。準拠期限は 2025 年 3 月 31 日です。この新バージョンでは、消費者のブラウザーで実行されるすべての支払いページスクリプトに制御を実装することや、自動化された技術ソリューションを使用して Web ベースの攻撃を継続的に検知し、防止することなど、Web アプリケーションに対するより厳格な要件が導入されます。現在、アジア太平洋・日本地域の組織は、徹底的なギャップ分析を実施し、セキュリティポリシーを更新し、強化されたセキュリティ標準を満たすために必要な技術的変更を Web アプリケーションに実装しなければなりません。

APIに関して、アジア太平洋・日本地域では、オープンバンキング構想の採用が増加していることもあり、APIセキュリティがますます重視されるようになっていきます。同地域ではまだ、EMEA 地域で見られるほど、オープンバンキング規制が完全に導入されていないものの、API 諸国にはAPI [セキュリティ上の懸念事項](#)にプロアクティブに対処する機会があります。2024 年 8 月に実施されたこの地域の API セキュリティに関する知見の[調査](#)では、内部 API が最も一般的に使用されていることが明らかになりましたが、API アクセス制御における最大の懸念は依然として外部ユーザーへのアクセスです。これは、強力な認証および認可プロトコル、データ暗号化、継続的な API 探索および監視など、堅牢な API セキュリティ対策を組織が実行する必要がありますを示しています。この地域は[オープンバンキング](#)指針への移行を進めているため、組織は API セキュリティを優先して、進化する規制へのコンプライアンスを確保し、新たな脅威を防ぐ必要があります。

EMEA の視点

EMEA 地域では、地政学的な緊張、テクノロジーの進歩、規制の変化が複雑に絡み合うことにより、サイバーセキュリティ情勢が大きく変化しています。この地域は、ウクライナと中東で起こっている紛争が原因でサイバー脅威や国家の支援を受けた攻撃が激化し、固有の課題に直面しています。さらに、特に欧州諸国を標的とする親ロシアグループによるハクティビズムの台頭により、同地域は政治的動機に基づくサイバー作戦の主要な標的となっています。

EMEA の API 情勢にも、同様の課題があります。API はサービス統合とデータ交換を可能にする上で重要な役割を果たすため、サイバー犯罪者の主要な標的となっています。AI 主導の SaaS ツールが急速に導入され、多くの場合 API を介して統合されているため、アタックサーフェスが大幅に拡大しました。

こうした脅威の深刻化に対応するため、欧州連合（EU）は包括的なサイバーセキュリティ規制を導入しました。2025 年 1 月に発効した改正版の [Network and Information Systems \(NIS2\) Directive](#)（[ネットワークおよび情報システムに関する指令](#)、NIS2 指令）は、その適用範囲を大幅に拡大して 18 の重要な業界を対象とし、中規模および大規模の組織に厳格なサイバーセキュリティ対策を義務付けています。

金融業界では、2025 年 1 月 17 日に施行された [Digital Operational Resilience Act](#)（[デジタル・オペレーショナル・レジリエンス法](#)、DORA）が NIS2 に代わって適用され、金融サービスで使用するアプリケーションには堅牢な情報通信テクノロジーリスク管理フレームワーク、インシデント報告メカニズム、デジタル・オペレーショナル・レジリエンスのテストプログラムの確立が求められます。さらに、2025 年 3 月 31 日に必須となった [PCI DSS v4.0.1](#) は、進化するセキュリティニーズ、継続的なセキュリティプロセス、柔軟な手法、強化された検証手順を中心とした新しいコンプライアンス要件を導入します。今後改正される [EU Payment Services Directive \(PSD3\)](#)（[EU 決済サービス指令 3](#)）は、データ共有メカニズムの強化、セキュリティ要件の強化、金融サービス業界の監督強化により、PSD2 の欠点を是正することを目的としています。

2024 年 12 月 10 日に施行された Cyber Resilience Act（サイバーレジリエンス法、CRA）は、欧州連合で販売されるデジタル要素を備えた製品に対する義務的なサイバーセキュリティ標準を導入するものであり、製造業者はコネクテッド製品のライフサイクル全体にわたってセキュリティ対策を実施する必要があります。アプリケーションの開発者とユーザーにとって重要なのは、CRA ではスマートフォンとタブレットが重大なリスクベクトルとされていることです。そのため、組織はモバイル端末を全体的なサイバーセキュリティ戦略の基本要素として扱い、アプリケーションのライフサイクル全体にわたって厳格なセキュリティ対策を実施する必要があります。

英国では、今後施行される見込みである [Cyber Security and Resilience Bill（サイバーセキュリティおよびレジリエンスに関する法案）](#) により、英国のサイバー防衛が強化され、重要な公共サービスが保護される予定です。この法案には従来の規制フレームワークの重要な更新が含まれており、より多くのデジタルサービスとサプライチェーンを保護するように対象を拡大して、法執行を強化し、報告要件を増やします。

LATAM の視点

LATAM のサイバーセキュリティ情勢は急速に変化しており、世界的なテクノロジートレンドと、地域特有の経済的および政治的課題の両方に影響を受けています。そうした中、中南米諸国全体での急速なデジタルトランスフォーメーションと、ますます相互に接続するようになったシステムの脆弱性が重なり、同地域はサイバー犯罪者にとっても国家の支援を受けた攻撃者にとっても魅力的な標的となっています。サイバー攻撃の主な標的として、コマース業界と金融サービス業界が浮上しています。オンライン小売企業、決済処理業者、銀行、保険会社、フィンテックスタートアップ、暗号資産（仮想通貨）取引所は、デジタルインフラ、中でも Web アプリケーションや API を標的とする脅威に対して特に脆弱です。

LATAM 諸国はこれらの課題を認識し、サイバーセキュリティ規制の開発と実施において大きな進歩を遂げており、Web アプリケーションと API のセキュリティに重点を置いた取り組みが進んでいます。ブラジルは、データ保護とセキュリティに関する厳格な要件を課す Lei Geral de Proteção de Dados Pessoais (LGPD) を施行し、主導的な役割を果たしてきました。LGPD は、Web アプリケーションや API に特化したものではありませんが、デジタルインターフェースのセキュリティを含めてサイバーセキュリティポスチャ全体を強化するよう組織を促しました。

同様に、チリでは、[Framework Law on Cybersecurity（サイバーセキュリティに関する枠組み法）](#) が制定され、2025 年 1 月 1 日に施行されました。この法律は、National Cybersecurity Agency（国家サイバーセキュリティ庁）の設立について定め、Web アプリケーションや API に大きく依存している業界を含むさまざまな業界においてサイバーセキュリティインシデントを防止、報告、解決するための包括的な対策の概要を示しています。また、アルゼンチンは、2025 年 1 月に[サイバー犯罪の防止とサイバーセキュリティの戦略的管理のための連邦計画（2025～2027 年）](#) を発表しました。

API に特化した規制に関しては、有望な進展が見られます。たとえば、メキシコでは、フィンテックを含む金融業界を対象とした法律が施行され、信用調査機関やクリアリングハウスに対して安全な API を開発するための詳細な要件を定めています。このアプローチは、現代的なデジタルエコシステムにおいて API が果たす重要な役割と、対象を絞ったセキュリティ対策の必要性が認識されるようになったことを表しています。さらに、メキシコは、[Federal Law on the Protection of Personal Data Held by Private Parties](#)（民間団体が保有する個人データの保護に関する連邦法）により、個人データの処理を規制し、企業および組織に対する義務を定めています。

また、コロンビアは規制の枠組みを強化し、公共機関向けのサイバーセキュリティに関する公共政策を発表して法律の範囲を拡大するとともに、さまざまなレベルのインシデント対応報告機能を備えたデジタル・セキュリティ・リスク管理システムを構築しています。これらの措置は API に特化したものではありませんが、組織内の API セキュリティ慣行に不可避免的に影響を及ぼします。

地域全体で、消費者データを保護するための API セキュリティ基準を設定するオープン・ファイナンス・フレームワークなど、業界固有の戦略を採用するトレンドが強まっています。このようなフレームワークは、金融業界で特に重要です。これは、金融業界では、金融取引の完全性を維持し、機微な顧客情報を保護するために、API のセキュリティが不可欠であるためです。LATAM 諸国はセキュリティの向上を優先し続け、サイバーセキュリティ規制を国際標準に合致させています。そのため、Web アプリケーションと API のセキュリティに関するより包括的で具体的なガイドラインが登場すると予想されます。

緩和策

脅威情勢が進化し、より高度な攻撃手法が増加しているため、Web アプリケーションと API の保護は組織にとって重要な課題です。Akamai が推奨する保護手法と緩和手法として、たとえば次のものがあげられます。

- **包括的な API セキュリティプランを確立する**：シフトレフトと DevSecOps のアプローチを導入し、API 設計から稼働後までセキュリティを統合します。継続的な探索を行って、可視性を確保し、隠れた API（シャドウ API、レガシー API、ゾンビ API）を含むアタックサーフェス全体を把握します。厳格な認証と認可（OAuth 2.0、mTLS、ロールベースのアクセス制御／属性ベースのアクセス制御）、レート制限、ボット緩和によってセキュリティを強化し、不正使用を防止します。リアルタイムの脅威検知、異常監視、ランタイム保護を実行し、攻撃が発生した場合にそれを特定して阻止します。DORA、GDPR、HIPAA、NIS2、PCI DSS などの規制へのコンプライアンスを確保すると同時に、API ガバナンスポリシーを適用し、大規模な環境でもセキュリティを維持します。
- **堅牢なサイバーセキュリティ対策を実行する**：継続的な監視を行ってリアルタイムで脅威に対応し、脅威インテリジェンスとランタイム保護を提供する適応型セキュリティエンジンを使用します。また、動的アプリケーション・セキュリティ・テスト（DAST）などの API テストツールを使用して、安全なアクセス、暗号化、認証などのセキュリティ要件を確実に満たします。
- **脅威に対してプロアクティブな防御を行う**：専用の DDoS 防御ツールを使用して、レート制限と CDN キャッシングを設定し、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などの対策を実行します。また、継続的なトラフィック監視とハイブリッドプラットフォームにより、DNS インフラを保護します。
- **API の脆弱性を緩和する**：OWASP が提供するガイドラインなど、既定のセキュリティガイドラインに従って、堅牢な API セキュリティを確保し、API アーキテクチャの不適切なコーディング方法や設定ミスリスクに対処します。これらのリスクは、ハッカーによる不正アクセスやデータ操作を可能にする、悪用可能な脆弱性をもたらすおそれがあります。

- **ランサムウェアの脅威を阻止する**：多層的なアプローチを使用して、ランサムウェアに対抗します。ゼロトラスト・ソリューションを導入して悪性のトラフィックをブロックし、マイクロセグメンテーションによって詳細な可視性と正確なアクセス制御を実現します。また、[MITRE ATT&CK フレームワーク](#)を活用して攻撃パターンを把握し、対応戦略を強化します。
- **AI に備える**：[ボット防御ソリューション](#)、AI ベースのセキュリティツール、専用のファイアウォール、プロアクティブな対策（継続的評価やゼロトラスト・モデルなど）を含む包括的な防御戦略を採用し、[AI の使用の拡大](#)によって生じる新たなセキュリティリスクに対処します。多面的なアプローチで AI システムのセキュリティを確保：モデルやデータセットを把握することにより、プロンプトインジェクションやデータポイズニングなど特定の脅威に対処し、プロアクティブな脆弱性テストを実行します。また、開発環境とランタイム環境の両方に統合されたふるまい監視、コンテンツ検証、自動攻撃応答などの強力な防御を使用します。

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、悪性の意図が疑われます。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。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 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 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 Recherche、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 12 月 31 日までの 24 か月間のデータを使用しています。

API セキュリティ攻撃データ

Noname Security との統合により、API の脅威に関する Akamai の調査機能とレポート機能が強化されました。このデータセットは、まだ統合と分析の初期段階にあります。本レポートを作成するために、Akamai は 2025 年第 1 四半期から 30 日間のデータサンプルを取得し、対応するセキュリティフレームワークとコンプライアンス基準に従って API セキュリティアラートの内訳を分析しました。このデータセットは今後も継続的に更新され、API セキュリティの問題に関する幅広い見解を提供していく予定です。



クレジット

Research director

Mitch Mayne

共同執筆者

Charlotte Pelliccia

Badette Tribbey

Lance Rhodes

Maria Vlasak

校閲およびテーマ別寄稿者

Tom Emmons

Stas Neyman

Reuben Koh

Steve Winterfeld

Richard Meeus

データ分析

Chelsea Tuttle

販促資料

Barney Beal

Ashley Linares

マーケティング・出版

Georgina Morales Hampe

Emily Spinks

インターネット／セキュリティの現状

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。

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（英語版のみ）

Akamai のセキュリティリサーチ

Akamai のセキュリティ・リサーチ・ブログでは、今日の最も重要な調査に関する迅速な回答の観点をご覧いただけます。

akamai.com/blog/security-research



Akamai セキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携して、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現することが可能になります。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）および [LinkedIn](#) で Akamai Technologies をフォローしてください。公開日：2025 年 4 月