

2026 年の アプリ、API、 および DDoS

コンバージェンスの危機に備える：
API、AI、DDoS のリスクの緩和



目次

03	概要
04	エキスパートの知見 : 現代のインターネット攻撃の経済性 (寄稿者: Brent Maynard)
06	本レポートの主な知見
07	API セキュリティ
12	エキスパートの知見 : エージェント型 AI がもたらす新たな脅威からの防御 (寄稿者: Steve Winterfeld)
14	DDoS 攻撃
18	セキュリティの注目点 : ソフトウェアおよび SaaS 業界に対する DDoS の影響
26	Web アプリケーション攻撃
29	地域別のトレンド
29	APAC のスナップショット
29	エキスパートの知見 : AI、API、デジタル化が Web 攻撃や DDoS 攻撃をどのように再形成しているか (寄稿者: Reuben Koh)
33	EMEA のスナップショット
33	エキスパートの知見 : 攻撃の増加に伴い CISO が優先するレジリエンス (寄稿者: Richard Meeus)
40	緩和戦略
41	結論
42	調査手法
43	寄稿者
44	クレジット

概要

2026 年、最大の注目点は、脅威の状況がもはや派手な新しい攻撃手法によって変化しているのではなく、産業化が進んでいる、という点です。かつてはトレンドとして始まった、Web アプリケーション、API、分散型サービス妨害 (DDoS) 攻撃のコンバージェンス (融合) は、現在では常套手段となっています。変化したのは、これらのサイバー犯罪キャンペーンのスピード、精度、コスト効率です。

今年最初の「インターネットの現状 (SOTI)」セキュリティ調査レポートでは、このコンバージェンスの危機について検証します。2025 年を通じての、アプリケーションセキュリティ、API への脅威、DDoS 攻撃について振り返り、特に人工知能 (AI) が、これらの新たな産業化された攻撃手法に潜む脆弱性を加速させたかに焦点を当てます。数字がすべてを物語っています。Web アプリケーション攻撃は 2 桁増加し続け、DDoS 攻撃は爆発的な進化を続け (レイヤー 7 DDoS 攻撃は 104% 急増)、API の悪用は、技術的な頭痛の種から、真の事業継続上の危機へと発展しました。

セキュリティのリーダーと実務担当者が注視すべき 3 つの変化が明らかになっています。



攻撃の経済性が根本的に変化しました。

自動化により、かつては膨大なリソースと本格的な技術力を必要とした高度なキャンペーンを、タダ同然で大規模に開始できるようになり、攻撃のタイムラインが数週間から数時間に短縮されました。AI を活用した偵察、適応型ペイロード、Botnet as a Service プラットフォームにより、脅威が加速しただけでなく、不備が許される余地が全く無くなりました。



アプリケーションと API のセキュリティは密接に結び付いています。

組織は依然としてこれらを個別の問題として扱っているため、攻撃者が悪用するのに理想的な可視性のギャップが生じています。最新のアプリとその API は切り離すことができません。脅威アクターはシームレスにそれらの間を移動し、最も楽な侵入経路を探します。



損害が以前とは様変わりしました。

2025 年に観測された最も有害な攻撃の中には、大規模な機能停止が発生しなかったものもありました。その代わりに、パフォーマンスの低下、予想外のインフラコスト、コンバージョンの喪失、セキュリティチームへの負荷を招きました。このようなビジネス上の問題は多くの場合、損害が積み重なるまで気付かれません。組織がインターネットのセキュリティ対策に注力しなければ、よく言われるように「ドアを全開したまま」の、攻撃者が容易に侵入できるような状態になってしまいます。

今年のレポートでは、セキュリティ担当者やビジネスリーダーに、こうした動向が世界的にどのように展開しているかを理解するための、データに基づいた知見を提供します。結論としては、アクセス制御、レート適用、不正利用防止、レジリエンスなどの基本事項を徹底している組織は、AI に特化した限定的な修正だけを追求している組織を常に上回る成果を出しています。

攻撃の勢いは衰える気配がありません。さっそく、今日のサイバーセキュリティ戦略が、攻撃の実際の手口という現実に対応できているかどうかを見ていきましょう。

現代のインターネット攻撃の経済性

北米では、攻撃のトレンドが革新から産業化に変わり、セキュリティ戦略のさまざまな側面に影響が生じています。企業のビジネス運営の最適化に使用される機能は、攻撃を最適化するメカニズムとして使用されると、両刃の剣となります。企業の経営幹部のレベルでは、次のようなパターン、その影響、そして相互に関連するリスクを理解し、戦略を現実と整合させることに焦点が当てられています。

兆候の解読

Akamai の調査では、いくつかのパターンが明らかになりましたが、それらはいずれも単独では存在するものではありません。それには次のようなものがあります。

 **コンバージェンスは新たなトレンドから運用モデルへと変化しています。** Web アプリケーション攻撃、API の悪用、ボットアクティビティ、DDoS は、同じキャンペーンの一部として現れることが増えています。攻撃は自動化から始まり、API を経由して進行し、抵抗に遭うと可用性やコストに対する圧力へと発展します。これらを別々の問題として扱うと、攻撃者の実際の動きが見えにくくなり、何年も続く可視性のギャップが生じます。

 **攻撃の経済性は進化し続けています。** 攻撃は低コストで実行でき、簡単に繰り返すことができ、帰属を特定するのは困難です。攻撃は、自分が何者であるかを知らせず、正当なトラフィックに紛れ込むように設計されています。このような環境では、手動による検知や応答モデルでは苦戦します。特に、目的が即時の中断ではなく、機能低下とその持続である場合はなおさらです。

 **可用性とコストは依然として最も影響を受ける指標です。** 観測された極めて損害の大きい DDoS 攻撃の多くは、明白な機能停止を引き起こすだけではありません。それに加え、パフォーマンスの低下、イベントの強制的なスケールアップ、インフラコストの増大、運用チームへの負荷を招きます。API 攻撃では、このような障害は、セキュリティの問題として認識されるずっと前に、信頼性やビジネス上の問題として表面化することがよくあります。

 **AI は独立したリスクカテゴリーではなく、戦力を増強させるものであることが証明されています。** Web アプリケーション、API、DDoS 攻撃のいずれにおいても、AI 駆動型のアクティビティは、全く新しい弱点を生み出すのではなく、既存の弱点をさらに深刻化させます。AI に特化した限定的な対策だけでは、根本的な対策が提供する全体像と同等の価値を必ずしも実現できるとは限りません。

今や従来の攻撃が、目立たない形でマシンスピードで実行される

Web アプリケーション攻撃は増加し続けていますが、その性質は変化しています。最も重要な変化は、あからさまな脆弱性の悪用から、アプリケーションロジックとワークフローの悪用への移行です。攻撃者は認証済みの経路を介し、自動化技術を用いて正当なユーザーになりすまして、長期間活動し続けることが増えています。

ボットとスクリプト化されたクライアントがこのアクティビティの要です。ヘッドレスブラウザと自動化フレームワークにより、攻撃者は状態を維持し、ふるまいを適応させ、通常のパターンに紛れ込むことができます。そのため、主にシグネチャーや静的な指標に依存する防御策では、ボリュームから意図のある攻撃を区別することが困難です。

AI は、タイムラインを圧縮することで、このトレンドを加速させます。エンドポイントの探索は高速化し、パラメーターの調査はより効率的に実行され、ペイロードは継続的に調整されます。基本的な手法はよく知られているものの、実行速度が速くなると、設定や防御の不備が許されなくなり、対応するための時間が限られてしまいます。

Web アプリケーション攻撃によるビジネスへの影響は、ますます間接的に現れるようになっていきます。多くの場合、パフォーマンスの低下、コンバージョンの喪失、アラート疲れは、侵害の明確な兆候よりも先に現れます。壊滅的なイベントではない場合でも、時間が経つにつれてこれらの影響によって信頼が損なわれ、運用コストが増加します。

API と AI により拡大するアタックサーフェス

API は依然として、最も優れた投資対効果をもたらすとサイバー犯罪者が考えているアタックサーフェスです。API により、コア・ビジネス・ロジックが公開され、自動化が可能になり、データや機能へ直接アクセスできるようになります。従来の Web 攻撃と比較して、API の悪用は多くの場合、目立たず、検知が困難であり、成功した場合には損害がより大きくなります。

開発速度がインベントリやガバナンスの整備を上回っているため、シャドウ API やゾンビ API が依然として根深い問題となっています。管理が行き届いていないエンドポイント、一貫性のない認可モデル、安全に利用されているという思い込みにより、当然悪用の可能性が生じます。ほとんどの場合、これらの問題は高度なものではなく、構造的なものです。

AI の導入が加速するにつれて、ある現実がますます明確になりつつあります。それは、AI エンドポイントは API であるということです。入力を受け入れ、ロジックを呼び出し、出力を返します。インターフェースは新しいものかもしれませんが、セキュリティの原則はそうではありません。プロンプト入力はあくまでも入力です。検証、制約、コンテキスト化が行われていない場合、システムは意図しないかたちで動作します。出力処理も同様に重要です。管理されていない応答は、機微な情報を漏えいし、内部の状態を公開し、あるいは信頼できる入力として他の場所で再利用される可能性があります。

AI 駆動型のシステムの拡大により、API インタラクションの量と速度の両方が増加しました。モデルエンドポイント、エージェントワークフロー、ツール統合はすべて、自律的な使用や無制限の使用を想定して設計されていないことの多い API アクセスに依存しています。攻撃者はこの依存関係を直接たどり、API を使用して機能を列挙し、ロジックの欠陥を悪用し、過剰消費やコストベースの悪用を推進します。

単独では成り立たない API セキュリティ

このデータによって補強された最も重要な教訓の 1 つは、API セキュリティは単独では成り立たないということです。API の問題は、Web アプリケーション、アイデンティティシステム、可用性制御に連鎖します。API を個別の問題領域として扱ってしまうと、攻撃者がすぐに悪用できる可視性のギャップが確実に発生します。

2026 年において、効果的な API セキュリティとは、新しい制御を発見することではなく、アクセス、レート、意図に規律を適用することです。API は副次的なアタックサーフェスではありません。主要なアタックサーフェスなのです。



Brent Maynard

Akamai, Senior Director for Cybersecurity Strategy

本レポートの主な知見



API は現代の企業の主要なアタックサーフェスとなっており、1日あたりの API 攻撃数は前年比で 113% 増加しています。

- 2025 年に発生した API 攻撃の約 61% が不正なワークフローと異常なアクティビティに関連しており、2024 年の 30% から増加しました。この変化は、攻撃者が従来の Web 攻撃からふるまいベースの脅威へと移行していることを示しています。
- 顧客 1 社あたり平均 3,000 件の API に機微な情報が含まれており、12% がセキュリティ上の脆弱性を示しました。それらの問題の 24% は機微な情報の漏えいに関連しています。エージェント型 AI の成長によってこのトレンドが増幅し、AI のセキュリティ確保はすなわち API のセキュリティ確保を意味すると裏付ける結果になりました。



Web 攻撃 (API エンドポイントと Web アプリケーションを標的とする攻撃を含む) は、2023 年から 2025 年の間に 73% 増加しました。これは、進化する今日の脅威の状況において、強力なサイバーハイジーンとセキュリティの基本が依然として重要であることを示しています。



過去 2 年間 (2023~2025 年) で、**レイヤー 7 の DDoS 攻撃は 104% 増加しました。**



Aisuru や Kimwolf (TurboMirai の亜種) などのスーパーボットネットにより、DDoS がサービスとして手軽に利用できるようになり、誰もが高度な攻撃を実行できるようになっています。



AI は戦力増強剤です。

- AI は新しいカテゴリーを生み出すのではなく、既存の弱点をさらに際立たせます。AI に特化した限定的な修正だけを追求する組織は、基本を見落としています。AI 支援コード生成 (パイプコーディング) により、新しい脆弱性や不適切な設定が発生するようになり、多くがテストされずに本番環境に導入されます。
- エージェント型 AI の脆弱性が現代のアタックサーフェスを拡大しているのです。新しい Open Worldwide Application Security Project (OWASP) フレームワークは、自律的な意思決定を行う AI エージェントに特有の 10 の脅威を特定しています (ゴールハイジャック、ツールの悪用、記憶の汚染など)。

API セキュリティ

このセクションの API 攻撃のトレンドに関するデータは、Web ベースとふるまいベースの両方の API 攻撃を検知する Akamai API Security プラットフォームから取得したものです。

API は現代の組織にとって、デジタル体験を推進し、アプリケーション、顧客、パートナー間のリアルタイムデータ交換を可能にする「結合組織」のような存在です。しかし、この相互接続により、巨大なアタックサーフェスが生じ、API はエンタープライズ環境で最も攻撃を受けやすい侵入経路の 1 つとなっています。API を標的とする従来の Web 攻撃とは異なり、ふるまいベースの API 攻撃はより目立たず、検知が困難で、見過ごされるとより大きな危険をもたらす傾向があります。

Akamai の「2026 年の API セキュリティの影響に関する調査」では、調査回答者の 87% が 2025 年に API 関連のセキュリティインシデントを経験したと報告しています。また、Akamai のテレメトリーデータは、API がどれほどの規模で拡大しているかをさらに明確に示しています。前年比で急増しており、2025 年の 1 社あたりの平均 API 攻撃数は 258 件で、2024 年の 121 件から 113% 増加しました (表 1)。

1 社あたりの日間平均 API 攻撃数

月	1 日あたりの平均攻撃数	
	2024	2025
1 月	75	205
2 月	70	230
3 月	55	215
4 月	74	275
5 月	107	286
6 月	74	310
7 月	114	343
8 月	153	332
9 月	197	257
10 月	189	221
11 月	176	211
12 月	169	214

表 1: API は現在、各企業が経験する平均攻撃数が大幅に増加していることから分かるように、悪用の主な標的となっています

これらの数字の元には、さらに厄介な現実があります。専用の API セキュリティソリューションを導入していない企業は多くの場合、こうした脅威が迫っていることに気が付きません。可視化ツールや検知ツールを導入していないと、攻撃が気付かれずにすり抜け、データの漏えいやサービスの中断を引き起こす可能性があります。

一般的な API の露出

「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」レポートでは、セキュリティアラートのサブセットを、MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) や OWASP などのフレームワークに加え、一般データ保護規則 (GDPR) や Payment Card Industry Data Security Standard (PCI DSS) などの規制基準にマッピングしました。一方、このレポートでは、今日の脅威の状況を定義している上位の OWASP API セキュリティリスク (2023 年) を調査し、2025 年を形作った脆弱性と攻撃パターンを詳細に調査しました (表 2)。

Top 5 の API 脆弱性

OWASP Top API セキュリティリスク	観測された問題の量
API8 : 2023 – 不適切なセキュリティ設定	39.61%
API3 : 2023 – オブジェクト・プロパティ・レベルの認可の不備	35.11%
API2 : 2023 – 認証の不備	18.56%
API5 : 2023 – 機能レベルの認可の不備	3.70%
API9 : 2023 – 不適切なインベントリ管理	1.55%

表 2: 2025 年に Akamai の顧客が遭遇した脆弱性の上位 3 つは、不適切な設定、オブジェクト・プロパティ・レベルの認可の不備、認証の不備です

2025 年には、不適切なセキュリティ設定、オブジェクト・プロパティ・レベルの認可の不備 (BOPLA)、認証の不備が最も一般的な脆弱性として浮上しました。不適切な設定が 1 位で、観測された問題の平均の 40% 近くを占めています。本来なら大部分は防止可能であるにもかかわらず、DevOps 環境に典型的に見られる迅速な展開サイクルでは多くの場合、適切なセキュリティ強化の時間がほとんど確保できず、その結果、攻撃者の侵入経路が生まれてしまいます。

影響を受けた Akamai の顧客の間では、BOPLA と認証の不備が 2 位と 3 位にランクインし、それぞれ発見された脆弱性の約 35% と 19% を占めています。BOPLA の欠陥が悪用されると、機微な情報への不正アクセスが可能になり、プライバシーやコンプライアンスのリスクが生じます。一方、認証制御が不十分である場合、API は総当たり攻撃や Credential Stuffing 攻撃に対して脆弱になります。

全体として、攻撃者はこれらの問題 (不適切な設定、安全でない認可、認証の不備) をシステム上の弱点としてますます悪用するようになっていきます。特に不適切な設定は、自動化と AI の普及が拡大するにつれて、組織が直面するリスクを大幅に高める可能性があります。また、AI 支援型コード生成 (バンプコーディングと呼ばれることもある) の増加に伴い、開発者はより高速に大量のコードを生成できるようになっています。しかし、このような AI 生成コードの急増により、エラーが生じることが多くなり、組織のアタックサーフェスが拡大しています。

上位の API インシデント

また、Akamai は独自の信頼度スコアに基づいて、疑わしいと記録された API インシデントや攻撃試行を分析しました。これにより、顧客が調査（して発生したことを確認）すべき悪性のアクティビティや異常なふるまいについてプロアクティブに警告することができます。表 3 は、Akamai のテレメトリデータに基づき、影響を受けた顧客 1 社あたり約 35% のインシデントが API の安全でない使用に関連していたことを示しています。さらに、影響を受けた顧客 1 社あたり 21% 以上のインシデントが認証の不備によるもので、それに続いて機能レベルの認可の不備が 17% 強でした。

Top 5 の API インシデント

OWASP Top API セキュリティリスク	影響を受けた顧客あたりのインシデント数
API10 : 2023 – API の安全でない使用	35.32%
API2 : 2023 – 認証の不備	21.33%
API5 : 2023 – 機能レベルの認可の不備	17.34%
API3 : 2023 – オブジェクト・プロパティ・レベルの認可の不備	16.58%
API7 : 2023 – サーバーサイド・リクエスト・フォージェリ	3.68%

表 3: 顧客 1 社あたり 3 分の 1 以上の API インシデントが、API の安全でない使用に起因しています

認証の問題は組織にとって課題となり続けています。オブジェクトレベルの認可の不備 (BOLA) や BOPLA などの脆弱性は、従来のシグネチャーベースのツールでは依然として検知が困難です。これらの欠陥に対処するためには、API のふるまいを分析し、異常なアクティビティをリアルタイムで特定できるソリューションが必要です。注目すべき例として、[2025 年に発生した Tea アプリの侵害](#)があり、この事例では 110 万件以上のプライベートメッセージが漏えいしました。API はますます攻撃者の主要な侵入経路になりつつあるため、セキュリティはデフォルトでアプリケーション開発のあらゆる側面に組み込まれる必要があり、もはやオプションではありません。

データ漏えいのリスク

アクセス制御が不適切に設定されている場合や不完全である場合、API は個人情報 (PII)、保護対象保健情報 (PHI)、認証情報、ユーザーのオンラインアクティビティ (閲覧履歴)、財務データなど、機微な情報を大量に漏えいすることがよくあります。この問題は多くの場合、BOPLA や BOLA などの脆弱性に起因します。これらの脆弱性により、アクセスされてはならないデータを不正ユーザーが表示または操作できるようになります。また、このリスクは、アクティブであるが通常のガバナンス外で動作するシャドウ API (文書化されていない API) やゾンビ API (非推奨の API) によって悪化します。これらの API は監視されていないため、攻撃者の標的になりやすくなります。

エージェント型 AI のブームに伴い、API 内の機微な情報が漏えいするリスクが高まっています。AI は統合とデータ交換を API に依存しているため、このインターフェースを通過する機微な情報の量は飛躍的に増加しています。今日の AI 駆動型の環境では、AI のセキュリティ確保はまさに API のセキュリティ確保から始まります。

影響は広範囲に及びます。API データの漏えいにより、アイデンティティの窃取、詐欺、プライバシー違反、規制違反が発生します。2025 年には、顧客 1 社あたり機微な情報を含む API を平均 3,000 件所有していることがわかりました。これらの API の約 12% がセキュリティ上の脆弱性を示しており、その脆弱性の 24% は API 入力検証攻撃や Lightweight Directory Access Protocol (LDAP) インジェクションなどの機微な情報の漏えいの調査結果に関連しています。さらに懸念すべきことに、機微な情報と機微な情報に関連する知見を公開する API の数は増加し続けており、2024 年には顧客 1 社あたりの平均数は 71 件でしたが、2025 年には 86 件に増加しました。

多くの組織には API の完全なインベントリがなく、完全なインベントリを持っている組織でも機微な情報を公開する API を把握していないことがよくあります。Akamai の「2026 年の API セキュリティの影響に関する調査」によると、回答者の 77% が API の完全なインベントリを持っていると回答していますが、そのうち機微な情報を返す API を把握しているのは 23% に過ぎません。これは、2 つの面で懸念されます。まず、このようなありがちな可視性のギャップにより、API が返すことのできる機微な情報についての理解が継続的に欠如します。不適切な設定や見落とされた API エンドポイントが 1 つでもあれば、攻撃者は貴重なデータにアクセスできます。次に、前述の 77% という数字は、セキュリティチームが把握している API のみを表しています。多くのチームは、管理されていない API を検知できないツールを使用しています。つまり、API 資産の大部分が検知されずに存続していることを意味します。

コンプライアンスの考慮事項

各種の規制のフレームワークでは、機微な情報のデータフローを守るための保護がますます求められるようになっているため、API はセキュリティリスクの域を超えて重要なコンプライアンス要素となります。1 つのエンドポイントが侵害されると、クレジットカードや銀行の詳細情報から、個人の病歴、保険情報、専有ビジネス資産まで、数百万件のレコードが漏えいする可能性があります。API キーやトークンが盗まれると、不正なシステムアクセスが可能になり、影響を受ける組織に損害が生じる可能性があります。このようなインシデントが規制要件に反すると、企業は多額の罰金が科されるリスク、法的リスク、顧客からの信頼が低下するリスクにさらされます。

多くの規制は API について明示的に言及していませんが、API に要件が適用されることは明らかです。たとえば、[EU の GDPR](#) では、個人データ (API を含む) を処理するシステムに対して、不正アクセス、損失、または悪用を防止するための「適切な技術的かつ組織的な対策」を講じることが求められています。データの最小化、アクセス制御、データ主体の権利という原則はすべて、API による個人データの扱い方や保護の仕方に影響を与えます。

PCI DSS 4.0 標準は、API セキュリティを明示的に規定し、API ライフサイクル全体における可視性、継続的な監視、安全な開発プラクティスを重視しています。包括的な API インベントリを維持し、API のアクティビティとふるまいを継続的に監視して、異常や悪用を検知することを強調しています。同様に、[米国国立標準技術研究所 \(NIST\)](#) の安全なソフトウェア開発フレームワーク (SSDF) も、安全なソフトウェアを構築し、ライフサイクル全体を通じて保護し続け、脆弱性が発生した場合に対処するためのガイダンスを提供しています。また、API はソフトウェア開発の中核を担っています。

多層防御戦略の事例

2025 年に観測された大きな変化の 1 つは、API エンドポイントに対する従来の Web 攻撃よりも、ビジネスロジックの悪用などのふるまい攻撃が増加したことです。Akamai のテレメトリデータによると、2025 年の API 攻撃の 61.18% に不正なワークフローと異常なアクティビティが含まれていました。これは 2024 年の 30.01% から大幅に増加しています (表 4)。このトレンドは、攻撃者が Structured Query Language インジェクション (SQLi) などの慣れ親しんだ攻撃から、API のビジネスプロセス処理方法をロジックベースで悪用することへ移行していることを示しています。

API 攻撃の種類

攻撃タイプ	2024	2025
ふるまいの脅威	30.01%	61.18%
Web 攻撃	69.99%	38.82%

表 4: API 攻撃の最も重要なトレンドの 1 つは、従来の Web 攻撃から、よりふるまいベースの戦術へ移行していることです

Web アプリケーションファイアウォール (WAF) などの従来の防御は、主にシグネチャーベースの脅威を検知するように設計されているため、これらの攻撃には対応できないことがよくあります。組織は、WAF と専用に設計された API 保護ソリューション技術を組み合わせた多層防御戦略を採用することを強く推奨します。これらのソリューションは、従来の Web 攻撃だけでなく、ビジネスロジックの悪用や過剰なデータ漏えいといった攻撃特有のふるまいリスクに対しても、可視性と検出機能を提供します。同様に重要なのは、API テストとランタイム監視です。これらは、セキュリティチームが API のデータ処理方法のギャップを特定し、認証と認可を実行するために役立ちます。

エキスパートの知見

エージェント型 AI がもたらす新たな脅威からの防御

Akamai は大規模言語モデル (LLM) と生成 AI (GenAI) についてたくさん論じてきましたが、今日のビジネスの主な焦点は**エージェント型 AI** に移行しており、脅威アクターもそれに追従しています。簡単に言えば、エージェント型 AI は質問に答えるだけでなく、従業員や顧客に代わって意思決定を行う AI です。これにより、アタックサーフェスが拡大し、脅威プロファイルが変化します。

今こそ、OWASP が提供する業界の中核的なベストプラクティスを活用し、脆弱性の緩和の優先順位を決定する方法を理解するときです。OWASP は 2025 年 2 月に「**Agentic AI – Threats and Mitigations**」というホワイトペーパーを公開しており、12 月にはより有名な **Top 10** 形式に合わせて内容を更新しています。これは、サイバーリーダーがエージェント型 AI 機能を評価し、リスクのある箇所を判断するのに役立ちます。

これらのホワイトペーパーの大きな特徴は、脅威モデリングです。これは、その 2 つのドキュメントを結びつける要素の 1 つとなっています。エージェントをアプリケーションとしてではなく、記憶、アイデンティティ、権限を持つ意思決定エンティティとしてモデル化する方法を示し、推論パス、状態の永続性、アクションチェーンに従う方法を説明します。情報セキュリティチームは脅威をカテゴリーにマッピングして、カバレッジ、一貫性、残留リスクを評価し、Top 10 という文言で調査結果を追跡し、リーダーに伝えることができます。これらのホワイトペーパーを組み合わせると、脅威モデリングは「何がシステムを悪用する可能性があるか」から「何がエージェントを誤った方向へ誘導する可能性があるか」へと変化します。それは自律型 AI の決定的なリスクです。

ガイドライン、ロードマップ、業界標準の分類法

たとえば、「エージェント・ゴール・ハイジャック」のような攻撃ベクトルを考えてみましょう。攻撃者は、Web ページやドキュメントに埋め込まれたペイロードを介したプロンプトインジェクションなどの手法を使用してエージェントの目的を操作し、システムをリダイレクトして機微な情報の窃取や接続されたツールの悪用を行います。OWASP は、AI ファイアウォールやランタイム検証からレッドチームやインサイダー脅威プログラムまで、一連の緩和ガイドラインを提供しています。この各脅威手法の詳細なガイドは、優れたベースラインとなります。また、マッピングマトリクスが含まれているため、レビューを単純化することができます。

Top 10 は優先順位を定めたロードマップを提供するのに最適ですが、元のホワイトペーパーには 6 つのプレイブックが用意されているという点も重要です。これらは Top 10 に完全に対応しているわけではありませんが、プレイブック形式を好むチームにとっては、より広範な概念を活用するための絶好の出発点となります。

最後に、これらのドキュメントでは、より成熟したポリシードキュメントを持つ大規模企業にとって最適な業界標準の分類法を紹介しています。「ツールの悪用」などの概念を定義しているため、サイバーセキュリティチーム内だけでなく、法務、コンプライアンス、ベンダー管理、IT 部門とより適切に連携できるようになります。

Top 10 の緩和策

参考までに、こちらが 2026 年のエージェント型アプリケーションの脅威ベクトルに関する OWASP Top 10 です。

ASI01:	エージェント・ゴール・ハイジャック
ASI02:	ツールの悪用と窃取
ASI03:	アイデンティティと権限の悪用
ASI04:	エージェント型・サプライチェーンの脆弱性
ASI05:	予期しないコード実行 (RCE)
ASI06:	記憶とコンテキストの汚染
ASI07:	安全でないエージェント間通信
ASI08:	連鎖的な障害
ASI09:	人間とエージェント間の信頼の悪用
ASI10:	未認可のエージェント

緩和には、ベンダーの管理、コーディング、ベストプラクティスの使用が必要です。多くの場合、現在のセキュリティ制御はこれらの問題に対処していますが、堅実なプランとして、組織のセキュリティベースラインを検証するために業界のフレームワークをレビューすることをお勧めします。これらの課題に対処するためには、プロセスと技術的な制御を組み合わせる必要があります。生成 AI エージェントが自律的に意思決定を行うことで複雑さが増すため、Web/API やランタイム強制制御などの制御をマッピングするのは簡単ではあり

ません。技術面では、AI ファイアウォール、API 保護、ボット管理、ランタイム防御、DDoS 防御などの基本をゼロトラストベースのマイクロセグメンテーションなどの原則によって強化し、潜在的な影響を最小限に抑える必要があります。



Steve Winterfeld
Akamai, Advisory Chief Information Security Officer

DDoS 攻撃

今日の DDoS 環境

DDoS 攻撃は、依然としてサイバー犯罪者が最も頻繁に使用する最も破壊的な戦術の 1 つです。増幅攻撃や強力な単一サーバーからの直接大量フラッドに加え、[Kimwolf](#) や [Aisuru](#) などのボットネットは破壊的な大量 DDoS フラッドを実行するために広く使用されています。しかし、DDoS キャンペーンは、単純な大量フラッドの域を超えて進化し続けており、ファイアウォール、API、アプリケーションサーバーも標的にしています。多くの場合、悪用された脆弱性や不適切な設定を利用してこれを行います。さらに、ボットネットは、侵害されたコンシューマー IoT デバイス、クラウドインスタンス、プロキシネットワークで構成されることが多いため、こうした攻撃はより大規模になり、検知が困難になります。

DDoS リスクのレイヤーを理解する

最新の DDoS 攻撃は、開放型システム間相互接続 (OSI) モデルの複数のレイヤーにわたってポートやプロトコルを介してトラフィックを脅かすハイブリッド攻撃を仕掛けます。

大量フラッドは、UDP、SYN、ICMP、または増幅された DNS/NTP リフレクションフラッドを介して、ネットワークレイヤーとトランスポートレイヤー (レイヤー 3 および 4) で発生します。アプリケーションレイヤー (レイヤー 7) キャンペーンは、HTTP GET/POST フラッドやその他の Web プロトコルの悪用に重点を置き、標的となるサーバー、API、生成 AI サービス、または Web サイトの CPU とメモリを枯渇させます。

侵害された IoT デバイス、クラウドインスタンス、プロキシネットワークで構成されるボットネットにより、その運用はさらに大規模になり、検知が困難になります。

「[アプリと API セキュリティの現状 2025](#)」レポートで指摘されているように、攻撃者はますます AI と自動化を取り入れ、戦術をリアルタイムで適応させることで、より正確な標的設定、迅速なスケーリングを実現し、従来の防御を楽に回避しています。これに対応するために、防御側は AI 駆動型のふるまい分析、異常検知、自動緩和を展開し、これらの高度な攻撃を特定して無効化しています。2026 年においてもこのような進化を続ける DDoS 脅威を緩和するためには、多層的な適応型防御アプローチによるレイヤー 3、4、7 の堅牢な保護が依然として不可欠です。

世界の DDoS 攻撃のトレンド

レイヤー 7 の DDoS 攻撃の発生頻度は過去 2 年間で一貫して急増しており、2023 年から 2025 年の間に累計で 104% 増加しました。2024 年から 2025 年の前年比増加率は 61% でした (図 1)。その主な理由は、このタイプの攻撃は[ボットネット](#) (特に AI テクノロジー) を利用してより簡単に開始し、API や Web アプリを標的にできるからです。

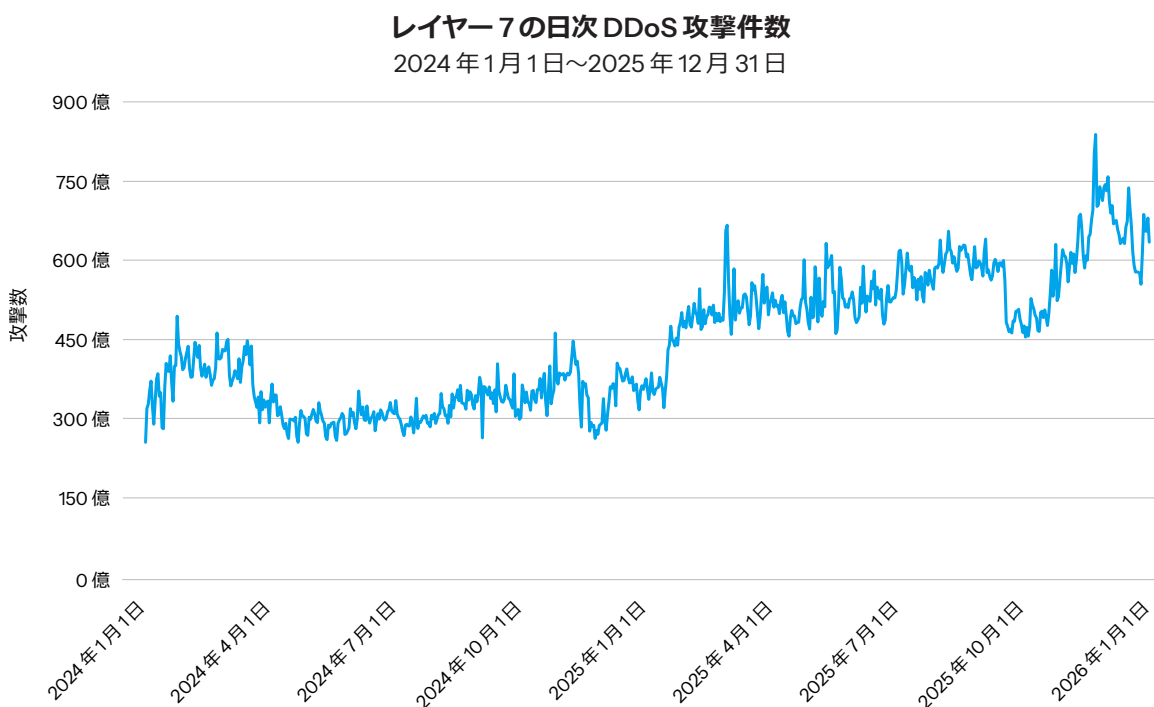


図 1: レイヤー 7 の DDoS 攻撃の発生率は、時間の経過とともに一貫して増加しており、前年比 61% 増加しています

時間の経過とともに着実に増加しているこの傾向は、一見すると劇的な変化には見えませんが、積み重なると大きな差となり、一部の急増は、ネットワークに大きな影響を与える可能性があります。組織が DDoS 防御ソリューションを見直す際には、一般的な持続的攻撃と記録的なピークの両方のレベルを追跡することが重要です。

図 2 は、レイヤー 3 およびレイヤー 4 の DDoS 攻撃の数はゆっくり増加していますが、規模は非常に大きくなっている（数テラビット）ことを示しています。また、Akamai の研究者は、レイヤー 3 および 4 の DDoS 攻撃がさらに大規模になっていると同時に、そのような大規模なボリューム型攻撃の頻度も高まっていることを確認しています（図 3）。

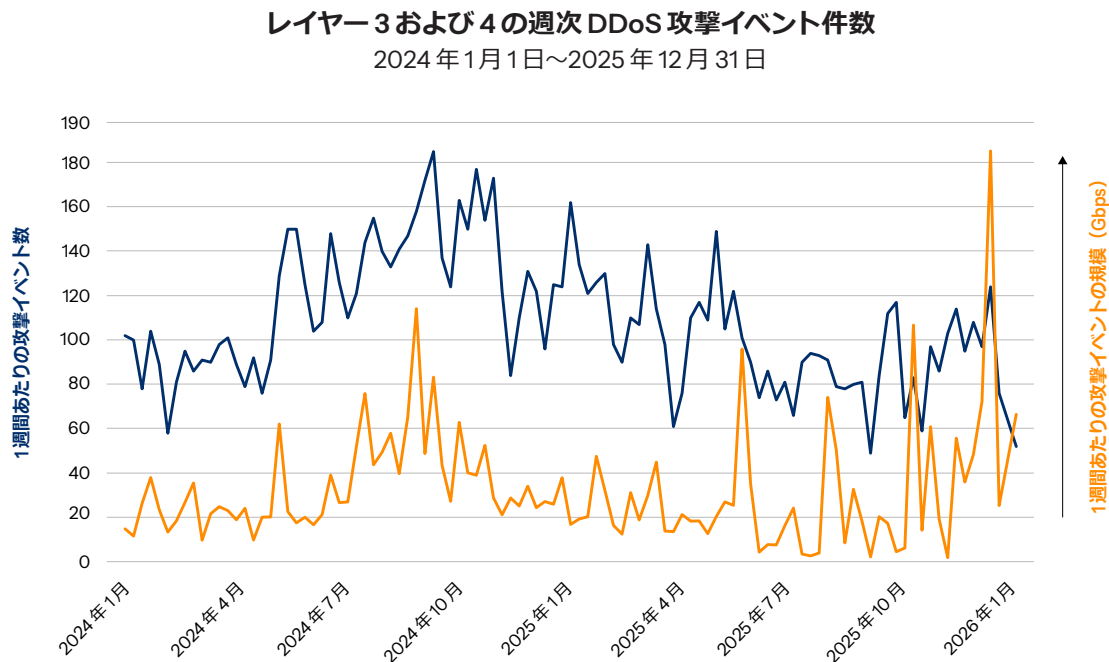


図 2: レイヤー 3 およびレイヤー 4 の DDoS 攻撃イベントの数は時間の経過とともにわずかに減少していますが、攻撃の規模は増大しています

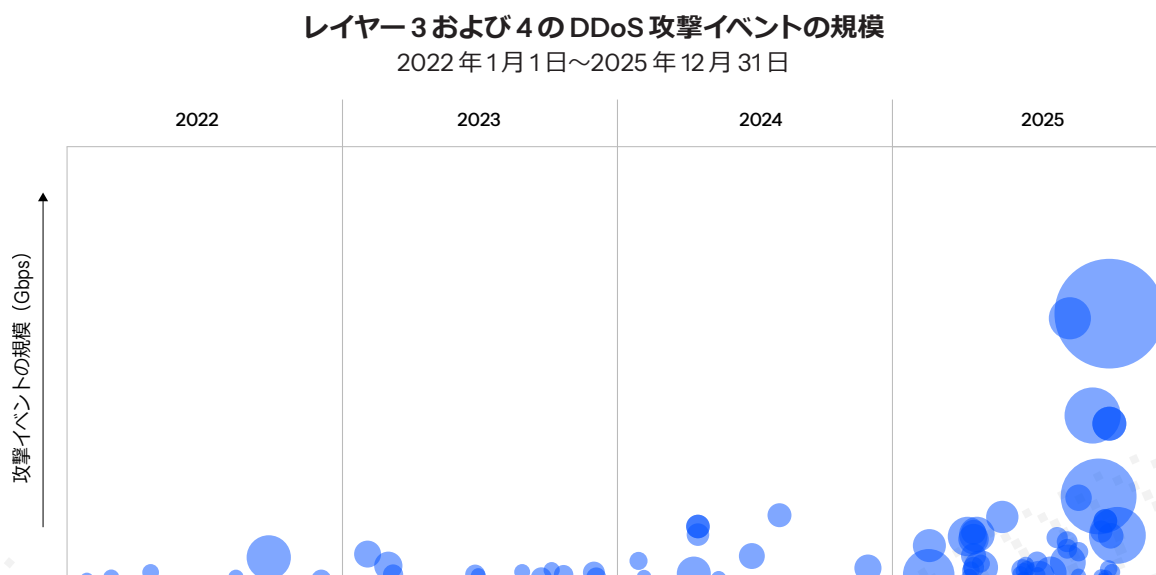


図 3: 過去 4 年間でレイヤー 3 および 4 の大規模 DDoS の頻度が劇的に増加したことを示すユースケースのスナップショット

レイヤー 7 とは異なり、レイヤー 3 および 4 の DDoS 攻撃は、**ネットワーク帯域幅**全体を過負荷状態にすることで、広範かつ即座に機能停止を引き起こす可能性があります。さらに、レイヤー 7 DDoS 攻撃は多くの場合、事前の綿密な偵察やカスタマイズされたリクエストパターンを用いずに、安価で基本的なボットが HTTP リクエストを送信するものもあり、その中には影響の少ないものもあります。そのため、レイヤー 7 攻撃の中には、リクエストしやすいに関わらず、レイヤー 3 やレイヤー 4 の攻撃ほど脅威ではない、より基本的なものも存在する可能性があります。

マルチレイヤー DDoS 攻撃

DDoS 攻撃は、攻撃手法もますます巧妙化しています。図 4 は、レイヤー 3、4 とレイヤー 7 の間でシフトした TurboMirai の亜種を利用した動的な攻撃を経験した顧客のスナップショットです。

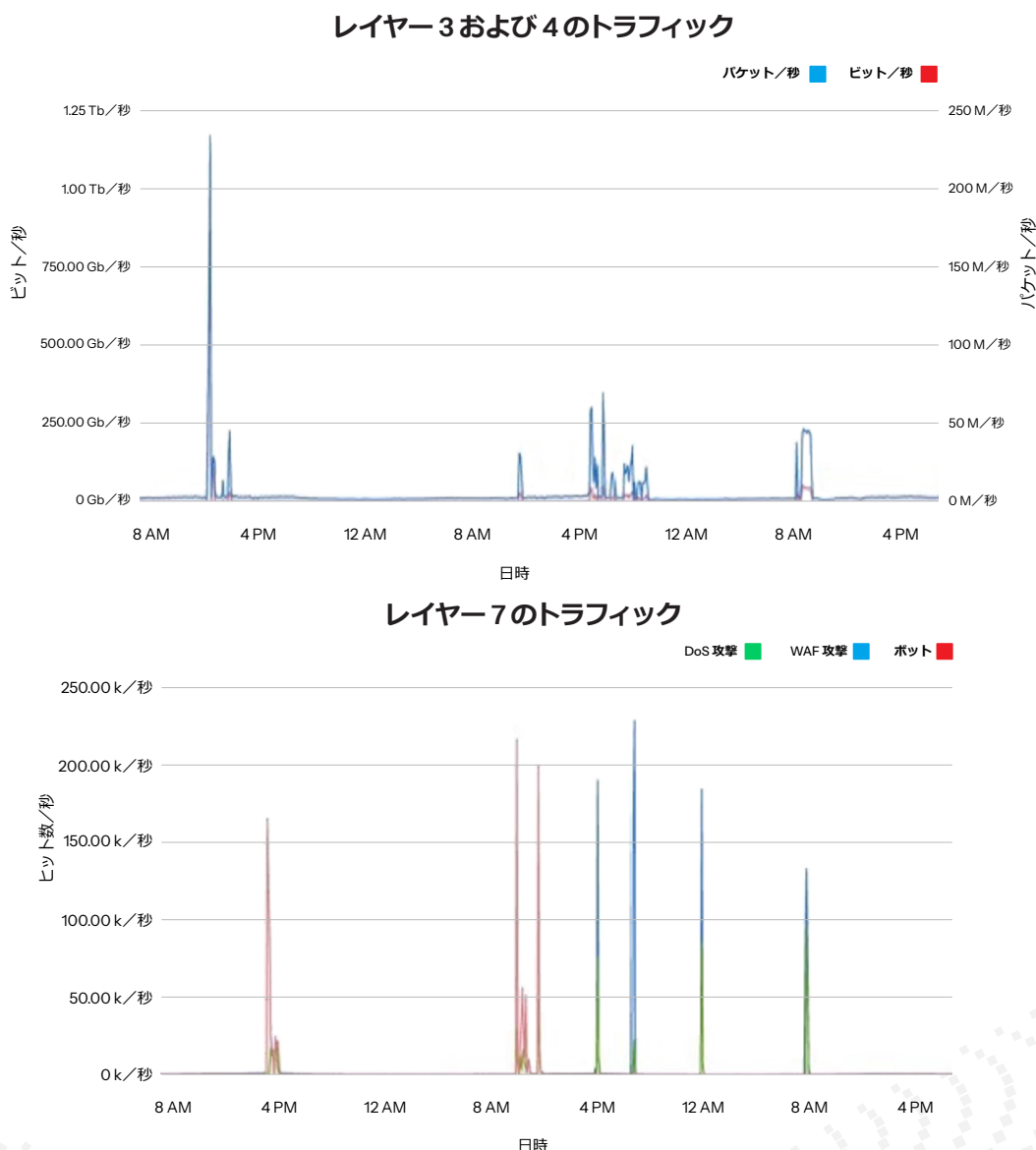


図 4: 最近発生した、TurboMirai の亜種を利用したスーパーボットネットによるマルチレイヤー攻撃

攻撃者は柔軟性が高く、システム間で迅速にシフトし、複数のベクトルにわたって脆弱性を悪用することができます。現代の攻撃者は、単一のツールやプラットフォームを使用して、環境から環境へとジャンプして複雑な多層攻撃を調整し、得られた結果に基づいてリアルタイムで障害を引き起こすことができます。このような適応性により、攻撃者はさまざまなシステムの弱点を探り、手法を臨機応変に調整できるため、企業は保護のために専用の DDoS 緩和サービスに頼らざるを得なくなっています。

すべてのレイヤーで DDoS 攻撃が発生すると、ビジネスコストがますます増加します。特にレイヤー 7 の脅威の場合、アプリケーションレイヤーでの長期的な検知と緩和の取り組みにより、コストが増大します。このような攻撃は気付きにくく（典型的な Web トラフィックパターン内で動作する）、通常のリクエストと区別するのが困難である場合があるため、標準的なファイアウォールや基本的なボリューム型 DDoS 防御ツールをすり抜けてしまう可能性があります。その結果、組織は高度な分析と手作業による調査により多くの費用をかけざるを得なくなります。さらに、AI テクノロジーの統合により、攻撃者は悪性トラフィックを正当なトラフィックに紛れさせることができるようになるため、こうした脅威への対処コストはさらに高くなり、封じ込めもより困難になります。（これとは対照的に、レイヤー 3 および 4 の攻撃はその膨大な量によって、膨大な帯域幅コストを発生させ、広範かつ即座のネットワーク停止を引き起こします。）そのため、DDoS 攻撃の種類に関係なく、企業はコストの増加に直面しており、自社の事業を標的とする特定の脅威に合わせて防御と予算を調整する必要があることが浮き彫りになっています。

セキュリティの注目点

ソフトウェアおよび SaaS 業界に対する DDoS の影響

Akamai のデータによると、DDoS 攻撃の複雑さと規模はさまざまな業界で増大し続けています。注目すべきは、ソフトウェアと SaaS (Software as a Service) がレイヤー 7 攻撃とレイヤー 3 および 4 攻撃の両方で最も標的とされている業界のトップ 5 に入ったことです (表 5)。

レイヤー 7 攻撃とレイヤー 3 および 4 攻撃イベントで最も標的となっている業界

レイヤー 7 の攻撃	レイヤー 3 および 4 の DDoS 攻撃イベント
1. メディア	1. 金融サービス
2. コマース	2. ゲーム
3. ゲーム	3. 製造
4. ソフトウェアおよび SaaS	4. ソフトウェアおよび SaaS
5. 通信 ISP および MNO	5. コマース

表 5: ソフトウェアと SaaS は、レイヤー 7 攻撃とレイヤー 3 および 4 攻撃の両方で最も標的とされている世界トップ 5 の業界の 1 つです

これは DDoS の標的の従来のランキングが大きく変化したことを示しており、ソフトウェアプロバイダーや SaaS プロバイダーが直面する脅威の状況が拡大していることを示しています。次に、この変化を推進している要因と、それによって DDoS 脅威にさらされる業界の状況がどのように再形成されているかについて詳しく見ていきます。

事業運営のバックボーン:ソフトウェアおよび SaaS

ソフトウェアおよび SaaS 業界の攻撃サーフェスは、クラウドベースモデルの利用拡大、これらのプラットフォームが管理するデータの膨大な価値、そしてこれらのプラットフォームが事業継続性において果たす極めて重要な役割により、拡大を続けています。ソフトウェアおよび SaaS 企業は、もはや単なるサービスプロバイダーではなく、重要な営業、IT、ビジネス機能をサポートする現代企業のバックボーンとして、重要な事業運営のハブとなっています。顧客やパートナーはその持続的なアップタイムを頼りにしているため、短時間のサービス中断でもエコシステム全体に波及し、事業を停止させ、多大な経済的損失を招く可能性があります。

このような強い依存関係と相互接続性により、SaaS 環境は事業運営の広範な混乱、身代金の要求、評判の悪化を狙う攻撃者にとって DDoS の主要な標的となっています。言うまでもなく、SaaS プロバイダーが保有する高価値の情報が集中しているほど、サイバー犯罪者にとってその影響力と収益性の強化につながります。

DDoS 攻撃は業界の垣根を越えた直接的な影響を及ぼすことを理解することが極めて重要です。その一例が、ボリューム型 DDoS の標的となっている金融サービス業界です。多くの SaaS 企業が金融機関にサービスを提供しているため、銀行に対する攻撃によって SaaS の可用性が直接妨げられ、顧客ポータル、API、Web アプリがオフラインになる可能性があります。そのため、攻撃が成功した場合、1 つの企業に影響が生じるだけでなく、数千もの下流のクライアントが同時に混乱し、問題を増幅し注目を集める可能性があります。そのため、組織のリーダー（CISO、IT ディレクター、事業継続性責任者など）は、DDoS に対するレジリエンスを SaaS セキュリティの最優先事項と考えています。なお、多くの企業は長期的なサービス停止が発生して初めて自社の事業運営上の依存度の高さを認識すると言われています。このことは、プロアクティブな DDoS 防御と緩和の重要性を高めています。

手頃な DDoSaaS を実現する上での大規模ボットネットの役割

DDoS as a Service (DDoSaaS) 攻撃トラフィックはボットネットによって生成されますが、そのボットネットの力は単一の攻撃者が使用する私的資産のみにとどまらず、商用化され、他の攻撃者に貸し出されています。技術的にスキルの高い攻撃者が大規模なボットネットを構築またはレンタルし、固定価格のさまざまな DDoS パッケージ（さまざまな攻撃期間、帯域幅レベル、攻撃タイプなど）を宣伝する Web プラットフォームを作成します。通常、匿名性を維持するために、支払いは暗号資産（仮想通貨）で行われます。顧客が特定の DDoS 攻撃のタイプと期間のプランを選択し、標的の IP アドレスまたはドメインを提供して支払いを完了するだけで、指定された標的に対して数分以内にボットネット主導の攻撃が自動的に開始されます。



Mirai と呼ばれるマルウェアは、IoT 主導の大規模な DDoS ボットネットの典型的な例であり、DDoS 請負や DDoSaaS の運営に大きな影響を与え、それらを可能にしています。Akamai の Senior Director of Security Operations である Domingo Ponce は、Mirai について、「何年経っても（このボットネットが）まだ存在し、攻撃者がいまだにそのボットネットを使用する新たな手法を見出しているのは驚くべきことです」と述べています。このマルウェアは、数十万台の IoT デバイス（IP カメラ、DVR、家庭用ルーターなど）に感染し、それらを連携させて史上最大規模の DDoS 攻撃を仕掛けました。

Mirai のソースコードが公開された後、多数の亜種や模倣ボットネットが出現し、一部は明らかに商用の DDoS サービスとして運用されていました。Aisuru は、DDoS 攻撃を強化する大規模なボットネットの代表例です。Mirai の高度な進化版である「TurboMirai」の亜種に分類されます。また、Kimwolf と呼ばれる DDoS ボットネットは、Aisuru の後継である TurboMirai/Aisuru ファミリーの 1 つであり、Mirai スタイルの DDoS 構造を再利用しながら、プロキシネットワークを介して主に Android TV を標的にしています。Aisuru と Kimwolf はどちらも、数百万台の IoT デバイスと Android デバイスに感染し、記録的なフラッシングを引き起こしています。これらの亜種は、Mirai が大規模な DDoS ボットネットであり、手頃な DDoSaaS モデルであることを示しています。

Akamai Security Intelligence and Response Team (SIRT) は、Mirai の新たな亜種とキャンペーンを継続的に発見しています。2025 年 6 月、Akamai は Wazuh サーバーのリモートコード実行の脆弱性を悪用している 2 つの Mirai ボットネットについて報告しました。そのブログ記事では、API リクエストに含まれるサニタイズされていない JSON により、攻撃者が任意のコマンドを実行し、公開されているサーバーを乗っ取り、それらを DDoS 攻撃可能なボットネットに組み込むことができた経緯を説明しています。このボットネットは、リモートのコマンド & コントロールインフラから指示を受けて DDoS 攻撃を開始し新しい脆弱なシステムのスキャンを行います。そのようなキャンペーンの 1 つである「Resbot」では、イタリアをテーマにしたドメインが使用されており、特定の地域を標的としている可能性が示唆されています。その記事では、手頃な DDoSaaS を実現する上での大規模なボットネットの役割を直接説明してはいませんが、攻撃者が、実証済みのボットネットアーキテクチャ（Mirai）を迅速に適応させて、（その後 DDoSaaS 攻撃に使用される可能性のある）新たな脆弱性を悪用する仕組みについての知見を提供しています。攻撃者はボットネットを IoT デバイスだけでなく Wazuh などのサーバーにまで拡大し、その規模を DDoS 攻撃に利用します。

Mirai に侵害された IoT デバイスは引き続き懸念事項となっています。Mirai ベースの攻撃は、TurboMirai のようなより高度なスーパーボットネットへと進化し、規模と巧妙さを増幅させ続けているからです。これらのスーパーボットネットは Mirai の直系です。Mirai のオープン・ソース・コードを基盤として、破壊的な DDoS キャンペーンのためのより大規模でレジリエントなネットワークを構築します。そして多くの場合、AI 駆動型の自動化によって強化されます。AI テクノロジーは、自動化された脆弱性探索を強化し、ポリモーフィック型マルウェアの亜種を生成して検知を回避し、トラフィック増幅などの攻撃戦略を最適化して DDoS キャンペーンを効率化することで、これらの脅威を強化します。

DDoSaaS は、競合相手をオフラインにするために使用されることが多いですが、**脅迫**にも一般的に使用されます。ランサムウェア DDoS (RDDoS) 攻撃は、サービスの中断を招く DDoS 攻撃の防止または停止に対する支払いを要求するためにランサムウェアグループが実行します。DDoSaaS ボットネットを利用することが多い RDDoS は持続的な脅威であり、スタンドアロンの脅迫戦術として行われることや、**三重または四重脅迫**のようにランサムウェア手法を多層的に使用して被害者への圧力を増幅することが一般的です。三重脅迫の場合、DDoS を他のランサムウェア (暗号化、データ窃取など) と組み合わせて被害者に支払いを促します。また、四重脅迫の場合、サードパーティへの嫌がらせも行われます (図 5)。



図 5: ランサムウェアグループは、エスカレートするランサムウェア脅迫戦術を利用して、被害者に支払いを強要します

さらに、DDoS 能力を備えた Ransomware as a Service (RaaS) グループもトレンドになっています。たとえば、Agenda としても知られる [Qilin](#) は、2022 年に初めて観測されたロシアと関係のある RaaS グループであり、最近では脅迫ツールキットを強化して **DDoS 攻撃機能**を組み込んだと報告されています。2025 年第 2 四半期、[RansomHub](#) の崩壊後に多くの RansomHub アフィリエイトが Qilin に加わったとき、Qilin は米国を標的とするランサムウェア脅威のトップに躍り出ました。

DDoS とハクティビスト

今日の DDoS 脅威アクターは、金銭的利益や競争の混乱から、政治的または思想的なアジェンダまで、さまざまな動機を持っています。Akamai はこれらの悪性攻撃の背後にあるさまざまな動機を調査してきましたが、**ハクティビズム**は現代の DDoS 環境を形成する最も不安定で予測不可能な力の 1 つとして際立っています。ハクティビストの活動の多くは、イデオロギー、国家への忠誠心、社会的な目的によって推進され、多くの場合、実際の地政学的事象に反応して行われます。このような政治的に緊迫した環境により、[NoName057\(16\)](#)、[DieNet](#)、[CARR](#) などの攻撃的なグループが生まれ、大規模な破壊キャンペーンを実施し、アクティビズムとサイバー戦争の境界をあいまいにし続けています。

ハクティビスト主導の DDoS アクティビティは急増し続けています。これは、政治的な動機を持つ脅威アクターが、変化する世界情勢の緊張感に適応していることを示しています。欧州やベネズエラなどの地域で不安定性が高まる中、草の根のハクティビズムが復活する可能性が出てきており、分散型のグループが社会的および政治的な目的の下に結集しています。同時に、サイバー犯罪者とハクティビストの境界はますますあいまいになってきています。どちらのグループも共有インフラと大容量ボットネットを悪用して、特定の主張を拡散し、データを抽出し、重要なサービスを妨害しているからです。

欧州は依然として DDoS 関連のハクティビストの主張の主な焦点となっています。また、2025 年上半期にはイスラエル、米国、ウクライナも最大の標的となりました。このようなハクティビストグループの中で、NoName057(16) はその支配的地位を維持しており、永続的な破壊ではなくメディアの注目を集めることを目的とした、確立された高頻度攻撃パターンを継続しています。国家の支援を受けたハッカーグループに関連する地政学的イベントのトレンドは今後も続く予想されます。これにより、関係国や、これらのイベントの一方の側を支援していると考えられる国の重要インフラに巻き添え被害が発生します。

ハクティビストグループのリソースは一層充実しつつあり、顕著な技術的向上と持続性を示しています。DDoS 攻撃はほとんど脅威をもたらさないという従来の考えは時代遅れであり、近年、ハクティビストグループは劇的に進化した DDoS 環境を活用しています。これらのキャンペーンは、地政学的な紛争の中で信頼を揺るがして政府を不安定化させる取り組みが増加していることに伴い、激化しています。そのようなハクティビスト DDoS 攻撃は、手頃でレンタル可能なボットネットによって容易に実行可能であり、イデオロギー的な動機と専門化された DDoSaaS 事業の間でコンバージェンスが進んでいることを示しています。

優先順位付け、テスト、検証のベストプラクティス

DDoSaaS により、高度で大規模な攻撃をほぼ誰もが利用できるようになるため、組織は防御を堅牢で、十分に調整され、厳格にテストされたものにする必要があります。効果的な保護には、社内チーム、サービスプロバイダー、ベンダー全体の連携に加え、多様な攻撃ベクトルを緩和できる多層的なセキュリティ戦略が必要です。

優先すべき主なプロセス領域 3 つ

1. 関係者の連携 — 社内では、チーム（セキュリティ・オペレーション・センター、IT、インシデント対応、危機管理）がシームレスに連携して脅威を検知し、緩和するようにします。社外的には、ベンダーの SLA が迅速な対応のための明確なエスカレーションパスを定めていることを確認します。
2. インシデントへの備え — 明確に定められたプレイブックを確立し、攻撃中のあいまいさを排除します。このプレイブックには次の内容を含める必要があります。
 - あらゆるレベルの指定意思決定者と連絡先（最新の連絡先リストを含む）
 - さまざまな攻撃シナリオに対するステップバイステップの対応手順

3. 多層防御 — すべての潜在的なベクトルからの保護:

- インフラセキュリティ (レイヤー 3 および 4)
 - i. 可能な限り、レイヤー 4 制御ルールを DDoS 保護サービスを提供するプロバイダーにプッシュして、アタックサーフェスを小さく保つ
 - ii. インターネットに対してオープンにする必要のあるポートとプロトコルについて、実証済みの戦略を備える
 - 単一または複数のクラウドプロバイダーを使用して、DNS のレジリエンスを確保する
- アプリケーションレイヤー (レイヤー 7)
 - i. 組織の重要なホスト名はすべて CDN に解決されるべきであり、さらに、毎秒数百万件のリクエストをオリジンサーバーに漏れいさせることなく処理できる [Web アプリケーションおよび API 保護 \(WAAP\)](#) ソリューションも必要となる
- DNS
 - i. ドメイン・ネーム・システム・セキュリティ拡張機能 (DNSSEC) の実装
 - ii. DNS ポスチャ管理、ファイアウォール、フィルタリングの実装

テストと検証

-  プレイブックを定期的にテストし (少なくとも年 2 回)、妥当性と有効性を確認します。
-  DDoS シミュレーションを実施して、実際の条件下で防御を検証し、緩和戦略が期待どおりに機能することを確認します。
-  DDoS プロバイダーを擦り抜ける可能性のあるゼロデイ攻撃に対処するために、内部システムのストレステストを行います。

定期的にテストされたプロアクティブなアプローチにより、システムが侵害されてダウンタイムが危機的な事態に発展する前に、最も重要な局面でレジリエンスを確保できます。

DNS がビジネスリスクになる場合

2025 年を通じて、[DNS](#) はリスクが静かに蓄積されている場所であるという認識が顧客の間で共有されました。業界を問わず、セキュリティチームは DNS について、インフラ、ベンダー、さらには事業部門全体よりも長く存続する可能性の最も高いレイヤーであると考えています。クラウド移行、SaaS の導入、開発者向けセルフサービス、サードパーティの統合により、DNS レコードの作成、変更、放棄の速度が高まりました。Akamai の顧客が必要としていたのは、アラートの強化ではなく、より優れた明示性でした。彼らは、インターネットに面したアイデンティティが実際に任意の時点でどのように見えているのか、そしてそれが現実を反映しているかどうかを把握したかったのです。

Akamai DNS Posture Management の調査と検証により、予想外の知見が明らかになり始めました。企業規模では、未解決の CNAME レコード、内部ネットワークデータの漏えい、レジストリロックの無効化など、基本的な DNS の設定ミスが依然として広く見られ、何千ものドメインが乗っ取りやハイジャックに対して脆弱な状態になっています。金融サービスなどの規制対象分野では、観測対象のドメインの 85% 以上が、権威の開始 (Start of Authority/ SOA) の完全性、認証局認可 (Certificate Authority Authorization/ CAA) の適用、DNSSEC などの基本的な DNS 対策を満たしておらず、半数近くが最新の電子メール認証を導入していませんでした。顧客は、こうした調査結果にしばしば驚いていましたが、それは問題が理論上知られていなかったからではなく、それ以外の点では成熟したセキュリティプログラムであるにもかかわらず、問題が気付かれずに放置されていたためです。いくつかの組織のセキュリティチームは、よく使われる業務上の略語を用いて、こう表現しました。「DNS じゃない。DNS のはずがない。.....やっぱり DNS だった...。」Akamai の調査では、新しいタイプの障害は確認されませんでした。ただ、未解決の DNS ドリフトが、他の場所で発見されたインシデントの背景に、どれほど頻繁に静かに潜んでいたかが明らかになりました。

これらのパターンは、彼らの組織の変化の最中に最も顕著になりました。合併や買収は、DNS リスク探索を促す要因として繰り返し機能しました。統合作業の過程で、顧客は、廃止されたクラウドインスタンス、廃止された CDN、古いマーケティングプラットフォーム、および以前のベンダーに関連する、大量の孤立した DNS レコードを発見しました。DNS エントリーは、基盤となる資産がなくなってからもずっと解決可能なままであり、サブドメインの乗っ取り、なりすまし、不正な証明書の発行といった現実的なリスクにさらされていました。これらの調査結果を実用的なものとしたのは、コンテキストでした。DNS Posture Management は、これらが個別の設定ミスではなく、企業の進化のスピードが、資産管理や廃止のプロセスを上回っていることに起因する、構造的な問題であることを示しました。

M&A 以外にも、顧客は進行中の近代化プロセスにおいて同様の不具合が発生していると述べています。クラウドの再構築により、古い CNAME が残されたままになっていました。メールの移行により、プロジェクトが完了したと見なされてからずっと後でも、SPF、DKIM、DMARC の整合性が損なわれていました。事業部門がキャンペーン用に作成したドメインが、一度も廃止されることなく放置されていました。ベンダーとの関係が終了した後も、DNS の信頼は継続していました。時間の経過とともに、チームは DNS ポスチャを組織的規律の指標として扱うようになりました。DNS ドリフトは、所有権、説明責任、変更管理の広範な崩壊の前兆となることがよくありました。

また、顧客は証明書と暗号化ポスチャを DNS に関連する新たなリスク領域として指摘しています。HTTPS の普及は進んでいますが、実際に観測された使用中の企業ドメインのうち量子耐性を持つドメインは 4% 未満であり、その大部分が将来的に暗号の破損にさらされる可能性があります。より差し迫った問題として、証明書のリスクは、まれに発生する障害ではなく規模の大きさに起因して引き起こされていました。Akamai が観測した証明書の 40% 近くはすでに期限切れになっているか、90 日以内に期限切れになる予定であり、信頼が少数の認証局にますます集中していました。

証明書の有効期間は 50 日未満へ短縮される動きが継続しているため、顧客は証明書管理がもはや定期的なハイジーン保守作業ではないことを認識しています。証明書管理は、継続的な可用性とセキュリティの要件です。DNS ポスチャが単なる技術的な懸念からビジネス上の問題へと昇格された理由は、不適切な設定の有無そのものではなく、その影響の大きさでした。DNS の障害は、サービス停止、E メール配信の途絶、なりすまし、あるいは顧客の信頼喪失といった形で表面化します。設定ミスが明らかになる頃には、そのコストはすでにビジネスに跳ね返っているのです。

知見を行動へ移すにあたり、多くの顧客が DNS のレジリエンスとセキュリティの実用的なリファレンスモデルを求めています。Web アプリケーションとは異なり、DNS は基本インフラであるにもかかわらず、これまで広く採用されている運用チェックリストが欠如していました。これに対応するため、セキュリティチームは、環境、プロバイダー、買収案件を問わず、DNS に起因するリスクを一貫して軽減する一連の中核的な対策にますます注力するようになりました。これらの実践から、運用上のレジリエンスのための新たな DNS ポスチャ管理対策 Top 10 が形成されました。

DNS ポスチャ管理 Top 10 リスト 2026

アップタイムと基本的なハイジーン

1. DDoS や地域的な障害に耐えるように設計された、分散型のクラウドホスティング DNS サービスを使用します。
2. 内部と外部の DNS 環境を分離し、期限切れのレコードや使用されていないレコードを定期的に削除します。
3. DNS インフラをアプリケーションや Web サイトのホスティングから独立させて、連鎖的な障害を防止します。
4. ロールベースのアクセス制御、多要素認証、監査ログ、変更管理、DNSSEC により、強力なアクセス制御を適用します。
5. TTL (Time to Live) の値を意図的に管理し、キャッシュ効率と迅速な復旧およびフェイルオーバーのバランスを取ります。

ポスチャ管理とコンプライアンス

6. すべてのクラウドとプロバイダーで DNS 資産の探索を自動化し、完全なインベントリを維持します。
7. 設定を継続的に分析し、ドリフト、不適切な設定、所有権のギャップを検知します。
8. 有効期限、脆弱性、ライフサイクルコンプライアンスを監視することで、証明書をプロアクティブに管理します。

新たなリスクと将来への備え

9. タイポスクワッシング、類似ドメイン、ブランドなりすましなどの DNS ベースの脅威を監視します。
10. 暗号のアジリティと標準に沿った計画を通じて、ポスト量子暗号 (PQC) への移行に備えます。

顧客は、このリストの価値は理論的な整合性ではなく、運用上の影響力にあると強調しました。このリストは、セキュリティチーム、インフラチーム、コンプライアンスチームに、DNS リスクに関する共通言語と、クラウド移行、ベンダーオフボーディング、合併および買収のワークフローにポスチャチェックを組み込む具体的な方法を提供します。これにより、経営陣は DNS インフラのサイバーリスクを総合的に把握することができます。

Web アプリケーション攻撃

このセクションの API および Web アプリケーション攻撃データは、主に Web 攻撃に重点を置いた Akamai App & API Protector から取得したものです。

Web 攻撃の件数は、2023 年の初めから 2025 年末までに 73% 増加しました。Web 攻撃の件数が持続的に増加傾向にあることは、こうした攻撃が衰えていないことの証です。攻撃者は、顧客向けの Web サイトからバックエンド API まで、企業環境を継続的に調査して、本格的な侵害につながる可能性のあるセキュリティギャップを探しています (図 6)。防御側にとって、これは新たな脅威に直面しながら、レガシーインフラ、パッチ適用の遅延、不適切な設定の見落としによるアタックサーフェスの拡大といった複合的なリスクに対処する必要があることを意味します。

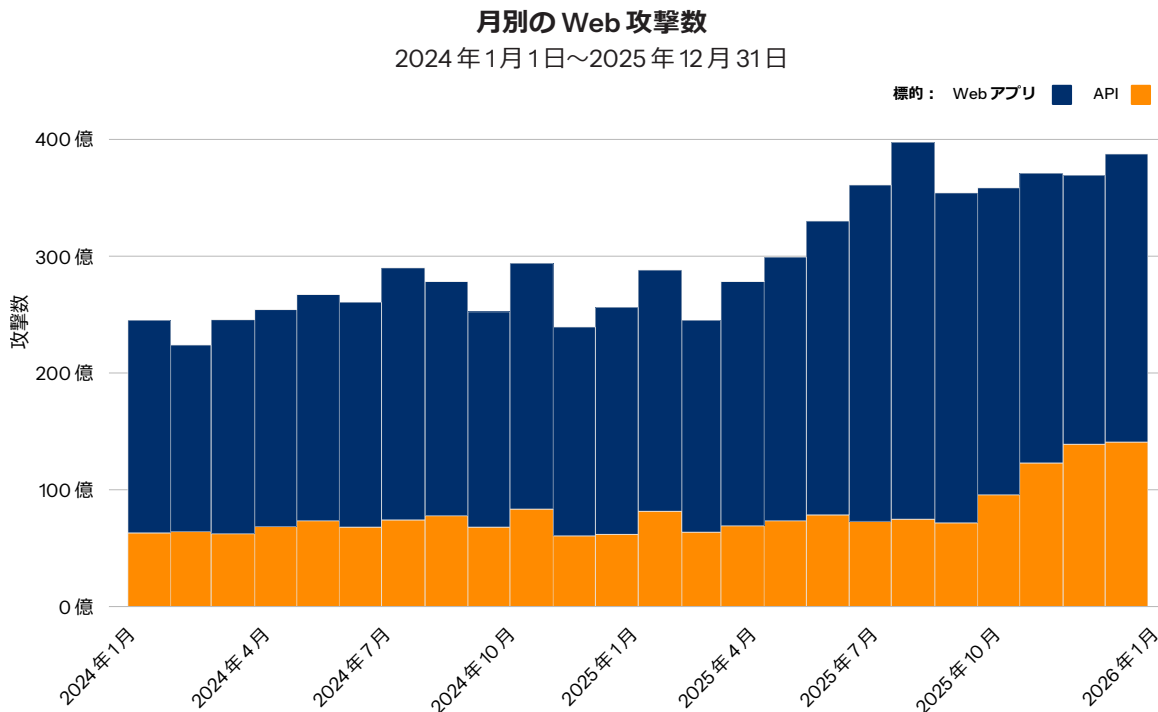


図 6: アプリと API に対する Web 攻撃の数は、2024 年 1 月から 2025 年 12 月まで増加傾向が続いており、組織にとっての大きな脅威として横行していることが分かります

侵害が検知される前によく見られるコンバージョン率の低下、アラート疲れ、パフォーマンスの低下などから明らかであるとおり、Web アプリケーション攻撃の副次的な影響は、顕著で本格的なインシデントよりも分かりづらい形で現れます。時間が経つにつれて、このような潜在的な影響により、大規模な侵害が発生しなくても、顧客の信頼が低下し、運用コストが増加します。

Web アプリケーションと API は、貴重なデータを公開し、デジタルビジネス事業において中心的な役割を担うため、依然として主要な標的となっています。さらに、Web 攻撃は、企業環境内に最初の足がかりを求めている脅威アクターにとって、実証済みで広く使用されている戦術です。

最新の OWASP Top 10 で強調されるセキュリティの基本の重要性

2025 年第 4 四半期、OWASP は最も重大な Web アプリケーション・セキュリティ・リスクの最新ランキングである [OWASP Top 10: 2025](#) を公開しました (図 7)。今回、OWASP はデータに基づいてカテゴリーをランク付けし、コミュニティ調査の回答に従って 2 つのカテゴリーをランクアップし、強調しました。このアップデートは、脅威の状況が大きく変化し、ソフトウェア・サプライ・チェーン攻撃の危険性が高まっていることを示しています。

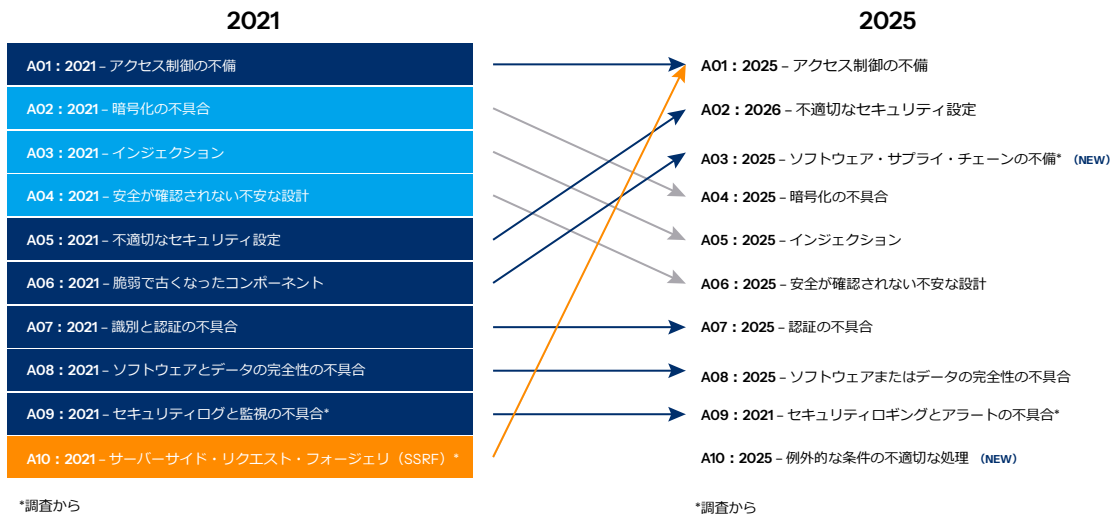


図 7: OWASP Web アプリケーション・セキュリティ・リスクの最新リストには、サプライチェーン攻撃の危険性に関する新しいカテゴリーが含まれています

このアップデートの中心は、「A03: 2025 - ソフトウェア・サプライ・チェーンの不備」です。これは、「A06: 2021 - 脆弱で古くなったコンポーネント」に代わる、再定義されたカテゴリーです。この変更は、最新の攻撃が従来のネットワーク境界をはるかに超えて拡大しており、相互接続されたベンダーエコシステム、サードパーティ製サービスへの依存、オープン・ソース・コンポーネントの普及に起因して脅威がますます発生するようになっていることを示しています。サプライチェーンの障害は、あらゆるカテゴリーの中で最も平均的な悪用可能性が高く、潜在的な影響が大きいため、組織が直面する最も重大なリスクの 1 つとなっています。Akamai のエキスパートは、[2025 年の年間レビューに関するブログ記事](#)で、2026 年にサードパーティのリスクがいかに重大になるかを上げました。

さらに、[2019 年の SolarWinds 侵害](#)や [2021 年の Log4Shell 悪用](#)から、React2Shell と呼ばれる最近のケースまで、注目度の高いインシデントはこの変化の緊急性を浮き彫りにしています。この [React Server コンポーネントと Next.js の重大な脆弱性](#)は、Flight リクエストの安全でないデシリアライゼーションを通じたリモートコード実行につながる可能性があります。これらのフレームワークが広く使用されていることを考えると、多数の Web サイトが影響を受ける可能性があります。これらの各インシデントは、深く根づいたサードパーティ依存における脆弱性がどのように攻撃ベクトルになり得るかを浮き彫りにしています。

「A01:2025 — アクセス制御の不備」はリストの首位を維持しており、現在は、サーバーサイド・リクエスト・フォージェリ（図 7 のオレンジ線）も含まれています。「A02:2025 — 不適切なセキュリティ設定」が 2 位に浮上したことは、安全なポスチャを維持する上で設定の健全性が依然として重要であることを示しています。インジェクションは 3 位から 5 位に低下しましたが、特にレガシーシステムやパッチ未適用のシステムでは、インジェクション攻撃は依然として広く悪用されやすい弱点となっています。Akamai のデータによると、2024 年から 2025 年までの期間に、SQLi とコマンドインジェクション (CMDi) が Web アプリケーション攻撃の 15% を占めていました（図 8）。

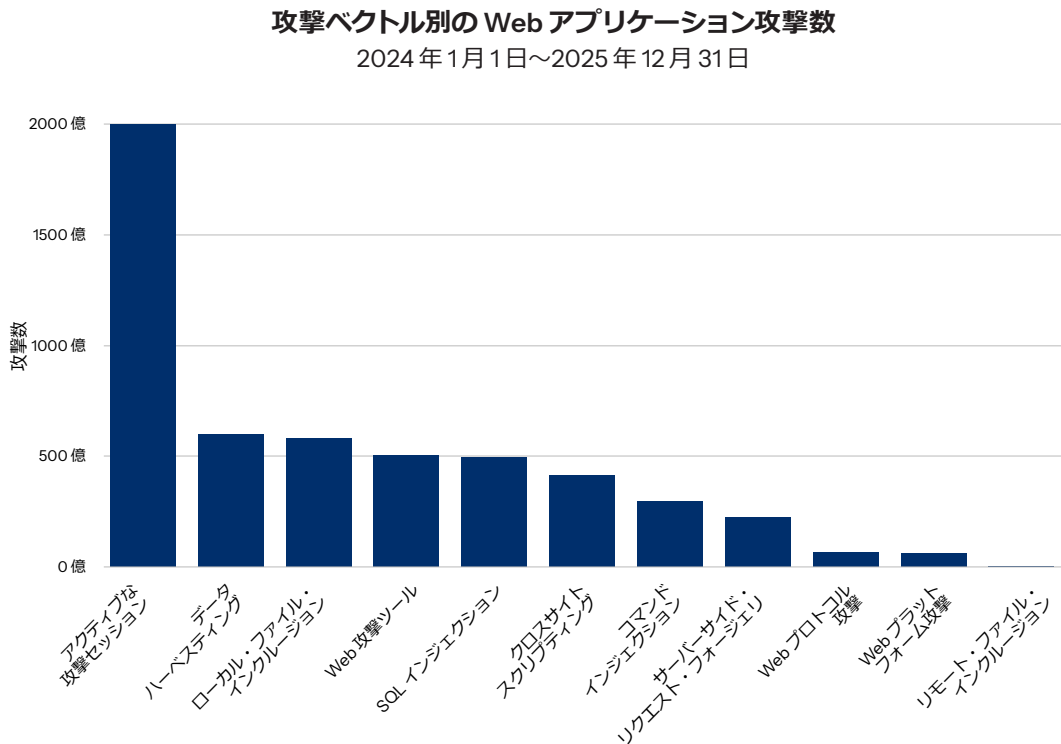


図 8: SQLi や CMDi などの実証済みの手法は、組織に大きな影響を与え続けています

全体的に、OWASP Top 10: 2025 は、よく知られているある真実を裏付けるものでした。それは、セキュリティの基本は依然として不可欠だ、ということです。サードパーティのガバナンスの強化（ソフトウェア・サプライチェーンの不備への対策）、最小権限アクセスの適用（アクセス制御の不備への対策）、開発の初期段階における設計上の欠陥への対処（安全でない設計への対策）など、こうした基本こそが引き続き重要であり、アプリケーションセキュリティのレジリエンスを決定付ける要素であり続けるのです。

地域別のトレンド

このセクションの API および Web アプリケーション攻撃データは、主に Web 攻撃に重点を置いた Akamai App & API Protector から取得したものです。

組織は、地理的な場所によって異なるサイバー犯罪の課題に直面しており、地域的な要因によって脅威の種類とセキュリティの優先事項の両方が決まります。以下の 2 つの地域別トレンドのセクションでは、アジア太平洋 (APAC) と欧州・中東・アフリカ (EMEA) のスナップショットを示し、各地域の CISO が最優先する攻撃タイプとトレンドについて、Akamai の各分野のエキスパートが見解を共有します。また、それに関連して、2024 年 1 月 1 日から 2025 年 12 月 31 日までのレポート期間中の Web 攻撃と DDoS 攻撃について、Akamai の研究者から得られたデータと知見を提供します。

APAC のスナップショット

エキスパートの知見

AI、API、デジタル化が Web 攻撃や DDoS 攻撃をどのように再形成しているか

2025 年、APAC 地域の経済的・業務上の実情により、CISO たちは、複雑で多面的なセキュリティ上の課題に直面しました。この地域における同年の主要な Web 攻撃と DDoS 攻撃のトレンドに関する知見は、技術的な成熟度が高いにもかかわらず、依然として非常に基本的なセキュリティ問題に対処し続けていることを示しています。

増幅する Web 攻撃

APAC で Web 攻撃が増加し続けている理由を完全に把握するには、CISO は、Web アプリケーションと API を単一の視点でとらえる必要があります。なぜなら、それらは切り離せないものとなっているからです。多くの CISO は、この拡大する開発エコシステムによって、次のような基本的な課題が生じていると述べています。

- シャドウ API
- バイブコーディング
- サイバーセキュリティスキルの地域差

シャドウ API: [Postman の「2025 State of the API report」](#)によると、APAC は他のどの地域よりも多くの API を定期的に量産しています。シャドウ API (つまり、未知で文書化されていない API) は当然の産物であり、組織にとって大きな問題です。開発チームは、本番環境向けの API の構築と展開で手一杯です。テストから文書化、実装まで、監視と説明責任が欠如していることが多く、シャドウ API につながる可能性があります。セキュリティチームと IT チームは、コンプライアンスチームと協力して、API の正確なインベントリと適切なセキュリティ制御を確保することに苦労しています。

パイプコーディング: 経済をデジタル化し、アプリと API を迅速に構築するために、チームは AI を使用して社内開発を加速するソフトウェア開発手法である「パイプコーディング」の採用を進めています。CISO は、AI 支援コーディングによってもたらされる生産性の向上を高く評価しています。しかし、パイプコーディングはミスがないわけではなく、脆弱性や不適切な設定によって組織の不意を突く可能性があります。API と同様に、このようなパイプコーディングによって作成されたアプリは、リスクを特定するための十分なテストなしで本番環境に移行することがよくあります。ゼロデイ攻撃を懸念する CISO は、2026 年にこの攻撃を緩和する最善の方法を継続的に模索する必要があります。

サイバーセキュリティスキルの地域差: APAC で特に顕著である、防御側にとってのもう 1 つの課題は、さまざまな経済圏の間でのサイバーセキュリティスキルの格差です。高度にデジタル化された経済圏では、最新テクノロジーへの投資をより効果的に保護するためのスキルセットが成熟していますが、発展途上国のサイバーセキュリティスキルは依然として非常に不足しています。技術力の低いチームが事業を迅速に拡大してデジタル化しようとする場合、セキュリティ体制が十分に整っていないまま、API や AI 要素を展開してしまう傾向があります。このミスマッチはリスクを悪化させます。イノベーションのペースを考えると、ギャップはさらに拡大する可能性があります。

攻撃者の視点から見ると、すべての Web アプリケーションには、機能や（場合によっては）データを公開する API が存在します。アプリや API が脆弱で、侵害が容易であるほど、脅威アクターは迅速に目標を達成できます。

現実世界とやり取りするために API を使用する AI エージェントの増加が、この問題を増幅させています。フライトの予約、乗り物の手配、送金のいずれにしても、組織には誰がなぜ API とやり取りしているのかを把握するための制御が必要です。重要な資産は通常、バックエンドのワークロードでセキュリティが確保されていますが、脆弱な API を介して直接漏えいするリスクがあります。この視点から見ると、Web 攻撃が拡大し続けている理由は明らかです。

依然として顕著な DDoS 攻撃

DDoS 攻撃は、レイヤー 7 またはレイヤー 3 および 4 のいずれを標的とする場合でも、次の 2 つの理由から、APAC 地域を標的とする脅威アクターにとって依然として好まれる攻撃手段となっています。

- 1. 複数の地政学的なホットスポット:** APAC 地域は、地政学的なホットスポットが複数ある地域です。地政学的な混乱が生じている時期には、重要インフラを機能不全に陥らせ、注目度の高いサービスを停止させ、標的となった地域の経済に打撃を与えることを目的とした DDoS 攻撃が急増します。さらに、ハクティビストが、政治的なアジェンダを推進するために、サイバー脅威環境でますます積極的な役割を果たすようになっています。レンタルボットネットやその他のツールをサービスとして利用することで、技術的な知識の乏しいグループでも簡単かつ低コストで DDoS 攻撃を開始できます。

2. デジタル化: APAC 地域の一部の成熟した経済圏はデジタル化し、金融、コマー、ヘルスケア、公共部門のサービスなどがオンラインで利用可能な状態を確保する必要があるため、魅力的な標的となっています。発展途上国がデジタルトランスフォーメーションを加速させるにつれ、同様に標的となりつつあり、DDoS 防御を管理体制に組み込む必要があります。Always-on のサービスには Always-on の保護が必要です。しかし、多くの組織はプロアクティブなリスク緩和のスタンスを取っておらず、DDoS 攻撃が発生している最中に保護を有効にするという対応をとっています。ISP またはクラウドハイパースケラーが提供する基本的な DDoS 緩和

サブスクリプションを追加する組織もありますが、大規模なマルチベクトル攻撃に対処するためには不十分かもしれません。平均的な ISP は、このような AI を活用した現代的な DDoS 攻撃の複雑さと規模の増大に対応する準備ができていません。

地域全体で微妙な違いのある課題が発生しているため、どこでもすべてを保護できる一貫した方法を見つけることはできません。組織には、投資を保護し、業務実態と経済的な実情に合致し、同時に成長を可能にするアプローチが必要です。



Reuben Koh

APJ 担当 Director of Security Technology

APAC のデータとトレンド

APAC 地域では、API と AI への依存の高まりに伴って Web 攻撃のアタックサーフェスが拡大し、Web 攻撃の試みが増加し続けています。2025 年では、Akamai の研究者は約 650 億件の Web アプリケーションおよび API 攻撃を APAC で確認しました。これは前年比 23% の増加です (図 9)。

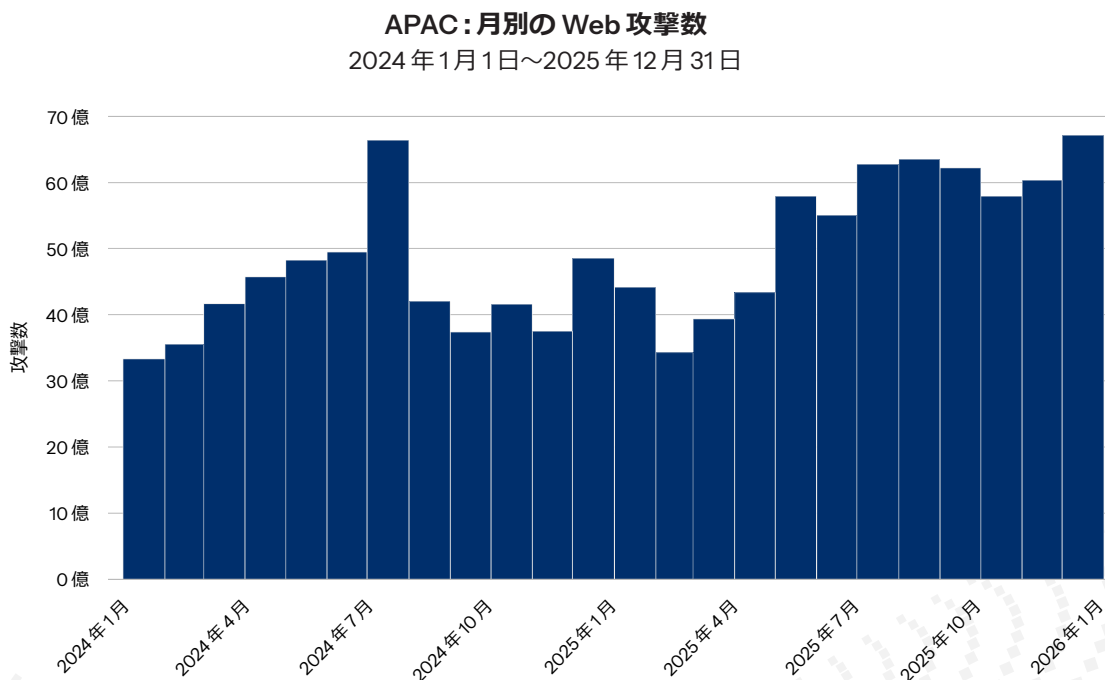


図 9 : APAC において、Web 攻撃は 2025 年により恒常的な脅威となり、2024 年の月平均 44 億件から月平均 54 億件に増加しました

この地域で進行中のデジタル化と、デジタルエコシステムのセキュリティ確保における課題が組み合わさり、APAC は Web 攻撃の格好の標的となりました。また、AI 支援ツールによって攻撃が加速しています。シャドウ API と AI 支援コーディングがもたらすリスクを管理するには、組織はライフサイクル全体を通じて API の探索、テスト、保護に役立つツールとプロセスを優先する必要があります。目的は、侵害を防止するだけでなく、運用上のレジリエンスを強化することです。

また、APAC における地政学的な緊張とイデオロギー的な不安の高まりを考慮すると、DDoS 攻撃は、重要かつ注目度の高いサービスを妨害する手段として日常的に使用されるため、引き続き懸念材料です。

自動化、AI、DDoSaaS によって攻撃ツールにアクセスしやすくなったため、2024 年と 2025 年に脅威アクターはこの地域の組織をレイヤー 7 の DDoS 攻撃の標的にしました (図 10)。

APAC : 標的地域別のレイヤー 7 の DDoS 攻撃数

2024 年 1 月 1 日～2025 年 12 月 31 日

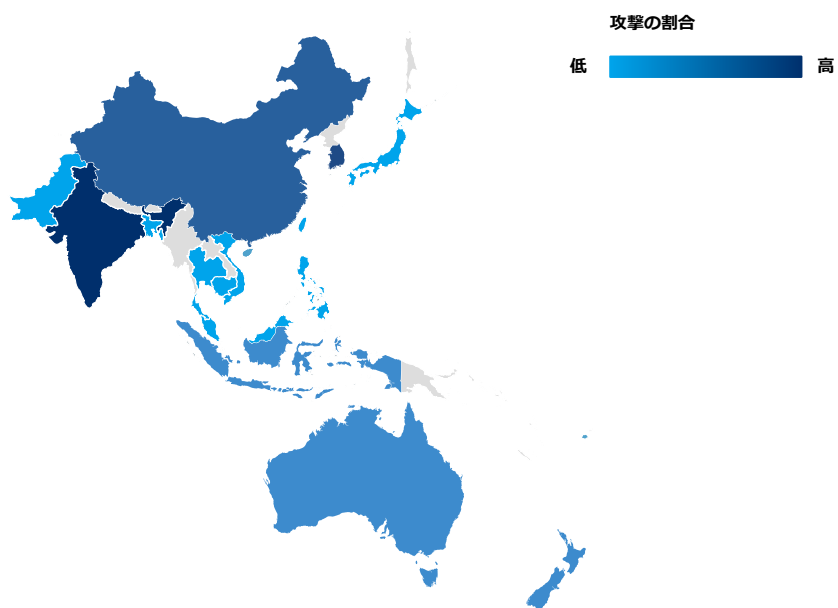


図 10 : APAC において、レイヤー 7 の DDoS 攻撃は地理的に広範囲に広がりました

さらに、複数のベクトルと大規模なボットネットをサービスとして使用することで、より大規模で長期間のレイヤー 3 および 4 DDoS 攻撃を簡単に開始できるようになりました (図 11)。

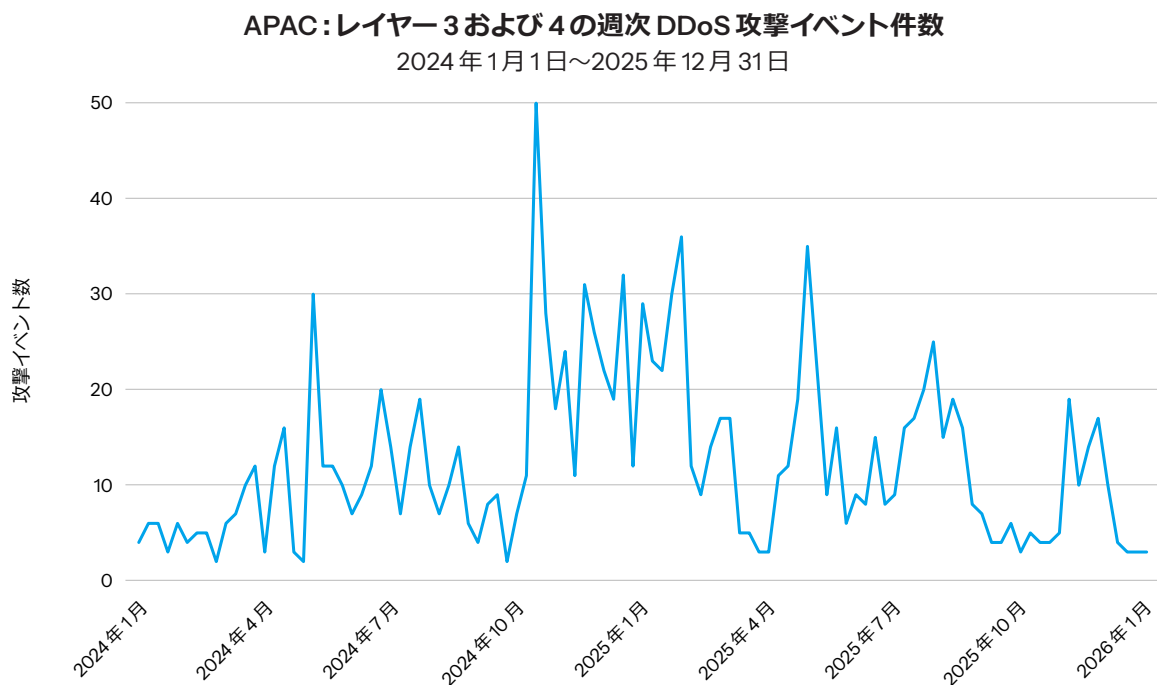


図 11: APAC において、ボリューム型のレイヤー 3 および 4 の DDoS 攻撃はより一般的になり、多くの場合、軍事演習の活発化、地政学的緊張、国境紛争と同時に発生しました

EMEA のスナップショット

エキスパートの知見

攻撃の増加に伴い CISO が優先するレジリエンス

セキュリティリーダーは、地政学的な緊張、ハクティビズム、金銭的利益の追求によって引き起こされる Web アプリケーション攻撃、API 攻撃、DDoS 攻撃が年々増加すると予想しています。EMEA 地域では、2025 年も例外ではありませんでした。そのため、CISO との対話では、数字や帰属に重点を置いていません。その代わりに、レジリエンスに重点を置きました。

それらのサイバー攻撃がサプライチェーンに与える影響を緩和する方法と、規制コンプライアンスを推進して運用上のレジリエンスを構築する方法は、EMEA の最も重要なトピックでした。

サプライチェーンに対する深刻な脅威

世界経済フォーラムの「Global Cybersecurity Outlook 2025」によると、調査に参加した大規模組織の 54% が、サイバーレジリエンスを達成するための最大の障壁として、サプライチェーンの課題（複雑化など）を挙げました。EMEA 地域の大手小売企業や一部の大手メーカーに対する顕著な攻撃により、サプライチェーンの存続を揺るがす危機が発生する極めて現実的な可能性が明らかになりました。CISO は次のように自問しています。

- 自社のレジリエンス計画はどの程度包括的か？
- 何か月も長引いて事業を停止させる大規模な攻撃が発生した場合でも、従業員、サプライヤー、顧客のニーズを満たし続けることができるか？
- 英国の国家サイバーセキュリティセンター (NCSC) が推奨しているように、デジタルシステムがダウンしても事業を維持するための書面計画はあるか？

大規模な複合企業が所有する大企業は、重大な攻撃による経済的影響を吸収できます。しかし、サプライチェーンへの影響は別問題であり、特に数百もの小規模サプライヤーに依存し、それらが組織の供給能力に不可欠な場合、「行き当たりばったり」の対応は賢明な戦略とは言えません。組織がサプライヤーへの支払いの手段を失い、手作業による計画ではサプライチェーンを維持することもできないために、それらのサプライヤーが破産した場合、組織は危機的な状況に陥ることになります。修復作業が数日から数週間、さらには数か月に及ぶ場合、システムが復元された後も、その企業を支える人材がいなくなっている可能性があります。

サプライチェーンの再構築を余儀なくされた企業は、かつてのような「通常業務」に戻れないかもしれません。

自社とパートナー企業の財務的存続がかかっているため、企業は、実績のあるセキュリティ制御でシステムを保護し、包括的なレジリエンス計画を通じて完全性を維持することで、サプライチェーンのリスクを緩和する方法に注力しています。

EMEA の複雑で進化する規制環境

英国と欧州連合 (EU) の規制機関は、サイバーセキュリティ規制の最前線に立っていることで知られており、運用上のレジリエンスの重要性を引き続き強く訴え続けています。

ネットワークおよび情報セキュリティ (NIS2) 指令は、組織がサイバー脅威からシステムとデータを保護するために設計された包括的なサイバーセキュリティ対策とリスク管理プラクティスを実施することを求めることにより、運用上のレジリエンスを強調しています。API と AI 駆動型の SaaS ツールの採用により、組織の攻撃サーフェスが拡大し、DDoS 攻撃が増大し続けているため、コンプライアンスの緊急性がますます高まっています。NIS2 は 2024 年 10 月までに EU 全体で国内法に置き換えられる予定でしたが、いくつかの加盟国では導入が困難であることが証明されており、置き換えの取り組みは依然として進行中です。

デジタル・オペレーショナル・レジリエンス法 (DORA) は、特に金融業界におけるサイバーセキュリティのレジリエンスに重点を置いています。影響を受ける組織は多大な労力を強いられませんが、規制フレームワークとしては NIS2 よりも導入が比較的容易であり、2025 年 1 月 17 日時点で EU 全体に適用されています。

EMEA の組織が遵守を計画しているその他の規制には、次のようなものがあります。

- **サイバーセキュリティおよびレジリエンス法案**：2025 年 11 月 12 日に提出された**サイバーセキュリティおよびレジリエンス法案**は、現在英国議会で審議中であり、人々が日々依存している不可欠なサービス（データセンター、重要な ICT サプライヤー、食品サプライチェーンなど）のレジリエンスと経済の安定性の向上に重点を置くために、既存の NIS 規制を見直します。
- **EU AI 法**：AI がサイバー攻撃の増加を促進するだけでなく、防御側にとっても価値があることを認識し、**EU AI 法**では AI 対応システムのセキュリティを確保するためのコンプライアンスフレームワークが導入されています。たとえば、ソーシャルエンジニアリングは、人間のサービスエージェントだけでなく、AI チャットボットを侵害するために使用されています。セキュリティチームは、コンプライアンスに準拠した制御を展開して、システムを適切にロックダウンする必要があります。

- **サイバーレジリエンス法**：**サイバーレジリエンス法 (CRA)** は、IoT デバイスのレジリエンスを強化することを目的としています。これには、**Mirai ボットネット**とその亜種が DDoS 攻撃を開始するために探索して悪用するハードコードされたパスワードなど、そのようなデバイスのセキュリティ上の弱点への対処が含まれます。

攻撃がますます破壊的に発展している中、EMEA のセキュリティリーダーは準備に重点を置いています。これは、レジリエンスが継続性と信頼性の基盤であることを示しています。



Richard Meeus
EMEA 担当 Senior Director of Security Technology & Strategy

EMEA のデータとトレンド

Akamai の調査によると、2024 年 1 月 1 日から 2025 年 12 月 31 日まで、EMEA では Web 攻撃が継続的な脅威でした。2025 年第 4 四半期には続けざまに 2 年間の最高値を記録しており、レジリエンスを優先する必要性が高まっています (図 12)。

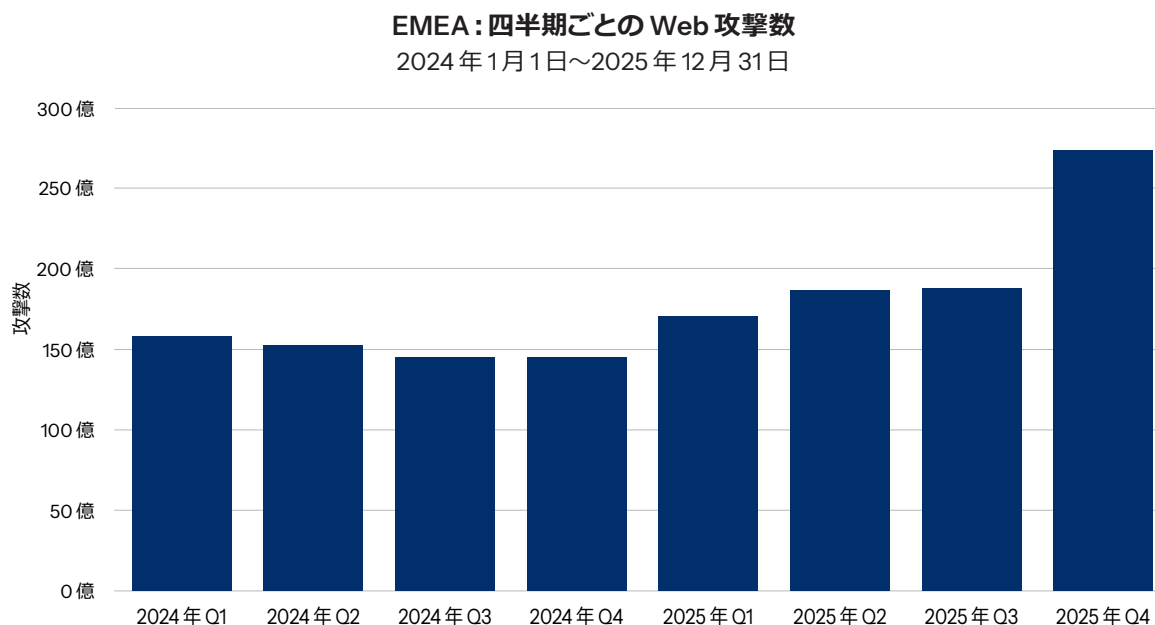
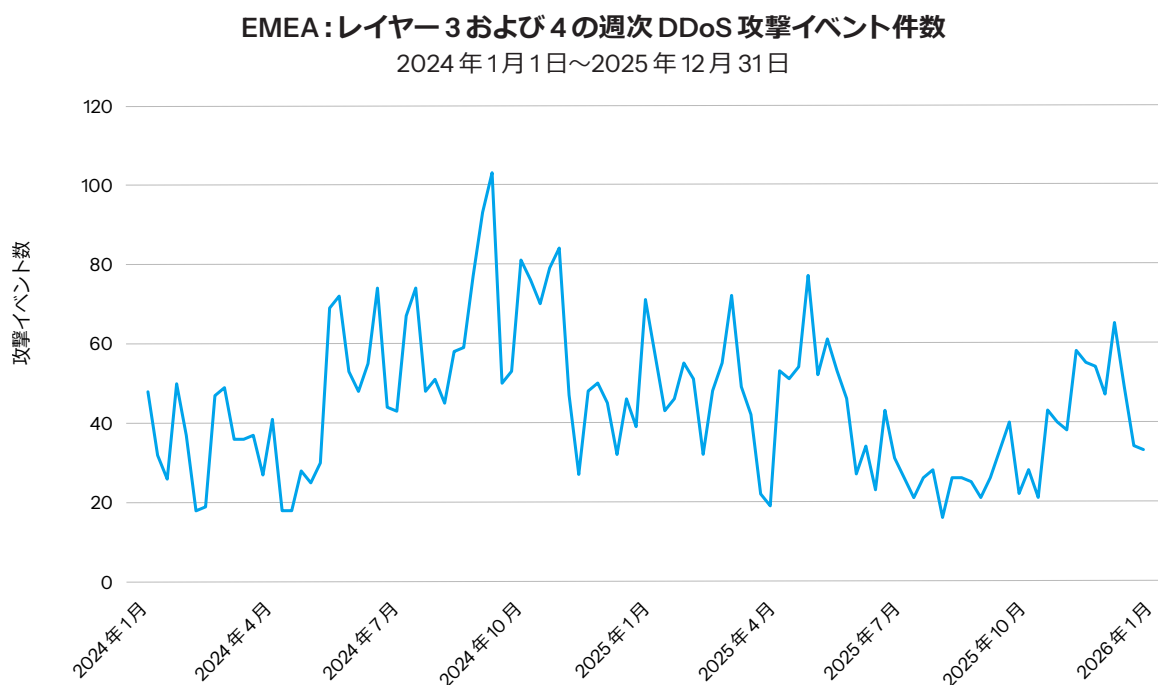


図 12 : EMEA では Web 攻撃の試みが増加し続け、2025 年第 4 四半期は過去 7 四半期のそれぞれより平均 69% 多く、前年比 36% 増となりました

この増加の原因の 1 つは、複雑でセキュリティ確保が困難なサプライチェーンへの依存度が高まっている組織に対する攻撃に重点が置かれていることです。たとえば、小売企業は 2025 年にこの地域で最も多く Web 攻撃の標的となっており (155 億件)、次いでメーカーは 2025 年に 120 億件の Web 攻撃試行を経験し、前年比 30% 増となりました。復旧には組織全体でさまざまなセキュリティ機能やリソースの連携が必要であるため、この混乱は即時的であるだけでなく、長期的でもあります。

DDoS 攻撃は EMEA でも増加し続けています。Akamai の調査によると、EMEA は過去 2 年間で最もレイヤー 3 および 4 の DDoS 攻撃の標的となった地域です (4,750 件)。さらに、トラフィックパターンは、[Akamai の Security Operations Command Center が観測した攻撃者のふるまい](#)と一致しています。熱心な攻撃者は、強力なインフラを持つ標的を狙って、非常に大規模な攻撃を仕掛け続けています (図 13)。



また、レイヤー 7 の DDoS 攻撃は前年比で 37% 増加しており、組織はレイヤー 7 の DDoS 攻撃に対する警戒を維持する必要があります (図 14)。

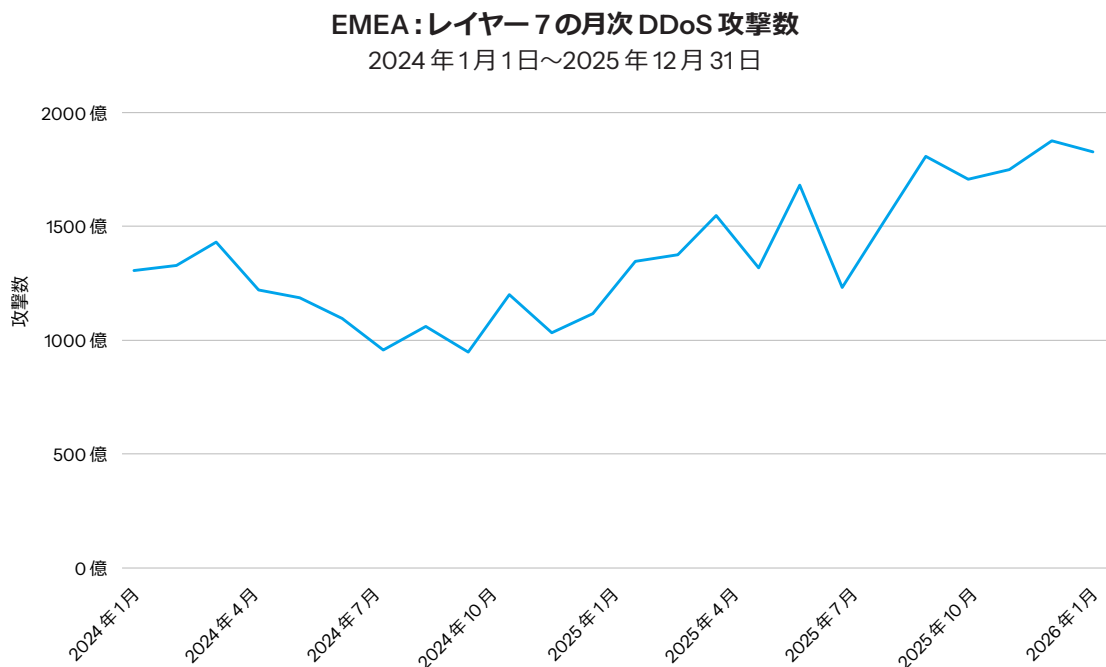


図 14: EMEA ではレイヤー 7 の DDoS 攻撃が増加傾向にあり、2025 年 11 月には最大 (1,880 億件) に達しました

ラテンアメリカのサイバーセキュリティの現状

ラテンアメリカの Akamai のエキスパートは、地域のセキュリティリーダーとの対話で常に軸となってきた 3 つのトピックを特定しました。それは、オンライン詐欺の脅威の増大、アタックサーフェスの拡大、ハクティビズムの脅威の高まりです。

-  **最優先事項:** 特に Credential Stuffing によるオンライン詐欺の脅威が増大していることが、ラテンアメリカにおける話題の中心になっています。この地域のサイバーセキュリティ専門家は、オンライン詐欺に加えて、前年比で 70% 増加した典型的な WAF 攻撃や API 攻撃への対応に追われています。
-  **重要なポイント:** 他の地域と同様に、アタックサーフェスも爆発的に拡大しています。API、モバイルアプリ、パートナー統合、AI エージェントが、混乱につながる新たな経路を生み出しています。一方、AI を活用したボットは Credential Stuffing 攻撃を加速させています。しかし、80/20 のルールはまだ生きています。組織は、可視性、アクセス制御、トレーニング、テスト、検証、パッチ適用などの基本的なギャップを修正することにより、最大のセキュリティ効果を得ることができます。
-  **今後の展望:** この地域全体で政治的混乱の可能性が高まっていることは、ハクティビズムの脅威の高まりにつながります。緊張が高まるにつれ、DDoS 攻撃の可能性も高まります。DDoS の監視と緩和を含む多層的なセキュリティ戦略を優先してこなかった組織はまもなく、この課題が後回しの状態から最優先事項へ急速に変化していることに気付くでしょう。

緩和戦略

このレポートでは、データ源である Akamai のプラットフォームの全機能に基づいて、さまざまな領域を取り上げました。この情報を使用して組織をより適切に保護する方法について説明します。

- **大まかに言えば、DDoS、アプリおよび API 攻撃、そして新たな AI 脅威を阻止するために組織にまず必要な最初の機能は、可視性です。**組織が環境の可視性を確保したら、次に、リーダーシップのリスク許容度に応じて調整できるセキュリティ制御の統合プラットフォームを展開する必要があります。最後に、組織はトレーニングと検証を通じて人材とプロセスに投資する必要があります。サイバーセキュリティはチームでの取り組みであり、開発者、IT、情報セキュリティ、ベンダー管理、法務の各チームが最新のベストプラクティスと規制ガイダンスに従っているという文化を持つことが重要です。
- **取締役会と話す場合も、情報セキュリティチームと話す場合も、業界のベストプラクティスを使用することは常に重要です。**OWASP は、トレーニングの優先順位付け、セキュリティ制御の展開、レッドチームとブルーチームの侵入テストの推進、脆弱性の分析に最適なリソースです。基本的な Web アプリケーションセキュリティの OWASP Top 10 は頻繁には更新されないため、定期的に確認する価値があります。さらに重要なのは、エージェント型 AI などの新たなトレンドを OWASP がカバーしていることです。これにより、組織は技術的負債を先読みし、展開の開発段階にセキュリティを組み込む機会を得ることができます。
- **最後に、脅威環境におけるアクティビティの多くは徐々に変化する傾向がありますが、このようなレポートを活用して、組織の対策が最新の攻撃に対処できるかどうかを検証することが重要です。**つまり、DDoS 緩和、WAF、API セキュリティ、ボットおよび不正利用防止、アイデンティティ認識型制御を個別のポイントソリューションとして扱うのではなく、それら全体で保護を連携させます。前年の想定ではなく、現在の脅威のふるまいが反映されるようにするために、定期的に制御を見直します。

これらのステップにより、セキュリティリーダーは事後対応型の制御更新から、データドリブンのプロアクティブなレジリエンスへと移行できます。

結論

今日の進化する DDoS 脅威の動向をみると、自動化の増幅、AI、そしてますます大規模化するボットネットによって、従来の帯域幅を圧迫する攻撃が、ますます複雑なものへと変化していることがわかります。過去 3 年間でレイヤー 7 の DDoS 攻撃の数は急増しました。主な要因は、DDoS 請負キャンペーンや AI 対応の攻撃スクリプトによるボットネットへのアクセスが可能になったことです。これにより、API や Web アプリケーションをこれまで以上に迅速かつ容易に標的にすることができます。一方、ボリウム型 DDoS 攻撃は、記録的な規模を達成し続けており、依然としてネットワーク全体を数秒以内に到達不能にすることができます。Mirai の基本アーキテクチャから進化した Aisuru や Kimwolf などのスーパーボットネットは、DDoSaaS エコシステムを維持し、サイバー犯罪者とハクティビストの両方のグループが高機能インフラをレンタルできるようにします。

クラウドベースのモデル、価値の高いデータ、ビジネス上の不可欠な依存関係が原因で、ソフトウェアおよび SaaS 業界に対する DDoS 攻撃が拡大しており、これらのプラットフォームは混乱、脅迫、評判の低下の最適な標的となっています。その影響は、直後のダウンタイムにとどまりません。顧客とパートナーはアップタイムの継続を頼りにしているため、短時間の中断でもエコシステム全体に連鎖し、事業を停止させ、重大な財務損失を招く可能性があります。攻撃者が自動化、AI、ハイブリッドマルチレイヤー戦術をますます展開する中、防御側は進化する DDoS 脅威に対するレジリエンスを維持するために、レイヤー 3、4、7 にわたる適応型かつインテリジェンス主導の保護戦略を採用する必要があります。

攻撃者が主要な侵入経路として API を使用するようになると、AI とのコンバージェンスにより、これらの脆弱性が組織の重大なリスクに変わる恐れがあります。コード作成（バインドコーディング）に生成 AI を使用することで、不適切な設定や安全でないデフォルト設定を通じて、意図せず多くの脆弱性が生じています。組織はこれまで以上に、API ライフサイクル全体にセキュリティを組み込み、本番環境に先立って保護を優先する必要があります。前述のように、API セキュリティは独立した領域としてではなく、より広範なアプリケーションエコシステムの一部として扱うべきです。このエコシステムでは、たった 1 つの脆弱性が相互接続されたシステム全体に波及する可能性があるからです。

一方、Web アプリケーション攻撃は着実に増加し続けています。これは、サイバーハイジーンの持続的な不備により、多くの組織が脆弱な状態になっていることに助長されています。OWASP の 2 つの最新リスト（主なアプリケーション・セキュリティ・リスクとエージェント型 AI の脆弱性を取り上げている）は、サードパーティ統合がどのように現代の攻撃サーフェスを拡大し、サプライチェーン攻撃の危険性を増幅させているかを示しています。

これらの課題は目新しいものではありませんが、組織が真に備えるためには、可視化とリスク緩和のための適切なツールを備えているかどうかを把握する必要性が、ますます高まっています。

調査手法

Web アプリケーションとレイヤー 7 の DDoS のデータ

このデータは、Akamai の App & API Protector 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 Akamai が検知した場合に、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 の 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します。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が、このレポートで分析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していません。

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。

レイヤー 3 および 4 の DDoS 攻撃のデータ

Akamai Prolexic Routed は、すべてのポートやプロトコルで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に到達する前に阻止することにより、DDoS 攻撃から組織を保護します。Akamai の Security Operations Command Center (SOCC) のエキスパートは、プロアクティブな緩和制御を展開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、さらに対応が必要かどうかを判断します。これらの緩和された攻撃は攻撃イベントに分類され、分析のために記録されます。

API データ

Akamai API Security は、Web ベースとふるまいベースの両方の脆弱性と攻撃の分析を含めることで、API 脅威リサーチおよびレポート機能を強化しました。本レポートを作成するために、Akamai は 2024 年と 2025 年のデータの日次スナップショットを取得し、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。

別段の記載がない限り、このレポートでは 2024 年 1 月 1 日～2025 年 12 月 31 日までの 24 か月間のデータを使用しています。

寄稿者



Brent Maynard
Senior Director for Cybersecurity Strategy

Brent Maynard は、Akamai の Senior Director for Cybersecurity Strategy です。サイバーセキュリティのイノベーションを推進してきた 17 年以上の経験があり、金融サービス業界や主要なクラウド・サービス・プロバイダーのチームを率いて、画期的なセキュリティソリューションを開発し、脅威の検知と対応に対する業界のアプローチを進化させてきました。Brent は、自動化されたセキュリティ調査の特許を保有し、Security Operations Command Center の体験を強化する革新的な製品を生み出しています。

インテリジェンスコミュニティと連邦法執行機関の信頼できるアドバイザーとして、注目度の高いサイバー調査を主導し、複雑なセキュリティ課題の解決策について協力してきました。



Steve Winterfeld
Advisory Chief Information Security Officer

Steve Winterfeld は Akamai の Advisory CISO です。業界の規制に準拠した運用セキュリティプログラムの構築に関して強力なバックグラウンドがあります。チームに加わる前は、Nordstrom Bank の CISO、Charles Schwab の Managing Director of Incident Response and Threat Intelligence、Northrop Grumman の Senior Technical Director Cybersecurity & Group CTO を歴任しました。民間企業で働く前は、米国陸軍の空挺レンジャーとして、南方軍のために地域初の緊急対応センター（現在はセキュリティ・オペレーション・センターと呼ばれている）を設立しました。

Steve は Akamai の顧客と協力し、顧客とその顧客を適切に保護できるようにすることに注力しています。また、Akamai がセキュリティプラットフォームの機能をどこに集中すべきかを判断する上でも貢献しています。サイバー戦争に関する書籍を出版したこともあります。また、CISSP、ITIL、PMP の認定を取得しています。



Richard Meeus
EMEA 担当 Senior Director of Security Technology & Strategy

Richard Meeus は、Akamai の欧州・中東・アフリカ (EMEA) 担当 Senior Director of Security Technology and Strategy を務めています。30 年以上の経験があり、世界で最も影響力のある組織の安全なソリューションの設計と構築を支援する責任を担っています。Akamai、Mirapoint、Prolexic への在籍中に、英国最大の企業メール実装の変革や、重要インフラや機微な情報を保護するための多国籍組織向けの DDoS ソリューションの展開など、さまざまなプロジェクトで戦略的役割を果たしました。

英国コンピュータ協会の公認会員であり、認定情報システム・セキュリティ・プロフェッショナルです。



Reuben Koh
APJ 担当 Director of Security Technology

Reuben Koh は、Akamai のアジア太平洋および日本 (APJ) 地域担当 Director of Security Technology and Strategy です。サイバーセキュリティ業界で 20 年以上リーダーシップを発揮しており、Akamai の戦略的セキュリティイニシアチブを推進し、組織が複雑なデジタルトランスフォーメーションに対応しながら、進化するサイバー脅威に対する堅牢な防御を維持できるよう支援する責任を担っています。

キャリアを通じて、特に金融およびエネルギー業界の大企業に対して、ゼロトラスト・アーキテクチャの実装、SecOps の最適化、さまざまな業界フレームワークに関する信頼できるアドバイザーとして貢献してきました。現在は、人工知能とサイバーセキュリティの交点、特にエージェント型 AI によってもたらされるリスクとインテリジェントなデジタル資産の保護に重点を置いて研究を行っています。

クレジット

Research director

Kimberly Gomez

執筆・編集

Charlotte Pelliccia

Badette Tribbey

Lance Rhodes

Maria Vlasak

校閲およびテーマ別寄稿者

Ryan Barnett

Stas Neyman

Roger Barranco

Menachem Perlman

Gabriel Bellas

Juan Carlos Rivera

Reuben Koh

Yariv Shivek

Brent Maynard

Rubens Waberski

Richard Meeus

Steve Winterfeld

データ分析

Galit Belkov

Chelsea Tuttle

販促資料

Ashley Linares

Ellen O'Brien

マーケティング・出版

Georgina Morales Hampe

Kimberly Gomez

インターネットの現状／セキュリティ

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](#)をご覧ください。今後のリリースをお待ちください。

Akamai の脅威リサーチ

[こちら](#)から、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ご確認いただけます。常に最新情報を把握するためにお役立てください。

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ください。

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はこちら](#)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 Security 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](#) と [LinkedIn](#) で Akamai Technologies をフォローしてください。公開日：2026 年 3 月。