CLOUDFLARE

APIの現状
セキュリティと管理

アプリケーションプログラミングインターフェイス（API）は、健康データの追跡からオンラインゲーミングのパーソナライズに至るまで、新しいアプリ体験を推進します。また、顧客分析、SaaS統合、生成AI機能など、数え切れないほどのビジネス上の利点も生み出します。

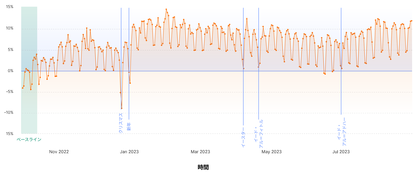
同時に、APIは管理が複雑で、常に攻撃にさらされる存在となります。APIトラフィックにおけるセキュリティと管理の傾向をご覧ください—APIトラフィックは現在、**全動的インターネットトラフィック**の**半分以上（57%）を占めています。**

30.7%

顧客提供のセッション識別子よりも機械学習によって検出されたAPI RESTエンドポイントの方が約31%多くなっていました

API中心の世界

全体として、世界中のAPIトラフィックの合計は、2023年を通して着実に増加しました。



Webトラフィック全体のうち、APIトラフィックのシェアが最も高い業界トップ10:

1. IoTコミュニティプラットフォーム
2. 鉄道、バスおよびタクシー
3. 法務サービス
4. マルチメディア、ゲームおよびグラフィックソフトウェア
5. 物流、サプライチェーンおよび輸送
6. 家庭用電化製品
7. 金融ソフトウェア
8. セキュリティおよび調査
9. 銀行、金融サービスおよび保険
10. 医療機器

保護されていないAPI

包括的なAPIインベントリを持たない組織は、本質的に隠れた攻撃対象領域である「シャドーAPI」を抱えるリスクがあります：

59.2%

APIの「書き込み」アクセス権を誤ったユーザーに提供すると、セキュリティリスクにつながる可能性があります。多くの組織（59.2%）が、少なくとも半数のAPIに対し、「書き込み」アクセス（更新をプッシュする機能）を許可しています。

15,000以上

15,000を超えるアカウントがCloudflareを使用しており、機械学習手法のみを用いてAPIエンドポイントが検出されました。

一般的なAPIの脆弱性

APIのセキュリティと管理に対する市場の需要は、APIトラフィック、エラー、および攻撃の増加と並行して急増しています。

APIに対する脅威 - 第1位
HTTP異常—APIに対する最も頻繁な脅威—は、悪意のあるAPI呼び出しの一般的なシグナルです。

APIトラフィックのエラー - 第1位
APIオリジンからのトラフィックエラーの半分以上（51.6%）は、**「リクエストが多すぎます」**というエラーコード**「429」を占めていました。**

軽減方法 - 第1位
APIに対する軽減策のうち、3分の1は分散型サービス拒否（DDoS）攻撃のブロックでした

APIとWebアプリの保護の課題の対比

対

Webアプリケーション

- エンドユーザーに**表示**
- **エンドユーザー**がWebブラウザを通してアクセス
- さまざまなユーザー操作を通じてバックエンドからのデータを視覚化（HTML、CSS、およびJavaScriptを使用）。
- 通常、既知の悪意のあるトラフィックをブロックする**「ネガティブセキュリティ」**モデルによって保護。

API

- アプリユーザーに**表示されない**
- **システムやアプリ**にデータを交換させる
- サーバーとアプリケーションにアクセスして、定義済みフォーマット（最も一般的なRESTful JSON、gRPC、XML、GraphQL）で**データを転送**。
- 検証済み、認証済みのトラフィックのみを許可する**「ポジティブセキュリティ」**モデルによって、より効果的に保護。

APIを防御する3つの主な方法

移行先としての「ポジティブセキュリティ」モデルと「ネガティブセキュリティ」の対比

ポジティブセキュリティモデルでは、「既知の正常な」APIトラフィックのみを受け入れます（APIスキーマで定義された通り）ポジティブセキュリティモデルの効果は、「既知の悪意のある」APIトラフィックを制限することに焦点を当てているネガティブセキュリティを上回ります。

機械学習を適用してリソースを解放し、コストを削減

機械学習は、APIトラフィックすべて（攻撃の変種を含む）を検出し、正当なトラフィックスパイクと悪意のあるボットトラフィックを区別し、他のリソース集約型のAPI管理タスクを処理することができます。

アプリの開発、可視性、パフォーマンス、セキュリティを統合

コネクティビティクラウドはアプリ開発とAPI多層防御サービスの間に重要なつなぎ目を提供し、ネットワーク、クラウド、アプリ、ユーザー間のAny-to-Any接続を可能にします。

CLOUDFLARE

もっと詳しく知りたいですか？

レポートを読む

Cloudflareの2024年APIセキュリティおよび管理レポート全文にアクセス

*このインフォグラフィック全体のデータ調査結果は、2022年10月1日から2023年8月31日までの間にCloudflareのグローバルネットワーク（CloudflareのWebアプリケーションファイアウォール、DDoS攻撃対策、ボット管理、APIゲートウェイサービスを含む）が観察した集約されたトラフィックパターンに基づいています。