CLOUDFLARE

2024年APIセキュリティおよび管理レポート

目次

セクションをクリックすると該当するページにジャンプします

概要

インターネットはコンピューター間で行われる絶え間ない対話の流れです。これらの対話は、多くの場合アプリケーションプログラミングインターフェース（API）を使用して行われます。APIにより、ソフトウェアやアプリケーションと新しい方法での対話が可能になります。たとえば、OpenAIのChatGPT APIによって、Slackがチャットベースのワークフローを合理化したり、Booking.comがよりパーソナライズされた旅行計画体験を提供したりすることが可能になります。

現在では、APIは他のインターネットトラフィックを凌駕しており、昨年Cloudflare[1]が処理した**動的な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。**

しかし、この**2024年のAPIセキュリティと管理に関する報告書で言及されているように**、APIの管理と悪用からの保護はますます複雑になっています。

例えば、多くの組織では自社APIを正確に把握しきれていません。Cloudflareは、機械学習ベースの検索を使用して、組織の自己申告数と比較して30.7%多いAPIエンドポイントを発見しました。[2]

30.7%

その他のAPIエンドポイント

残念ながら、組織は目に見えないものを適切に守ることはできません。

APIの状況を正確かつリアルタイムに把握することなくAPIセキュリティを実装した場合、**意図せず、正当なトラフィックをブロックしてしまう可能性があります。**

例えば、2023年にCloudflareが軽減した**API[クライアントエラー](#)カテゴリーの中で「リクエストが多すぎます」（429）エラーコードが、カテゴリーの中で最も頻発したエラーコードでした。**429エラーコードは、必ずしも攻撃者からのリクエストが多すぎることを意味するわけではありません。例えば、エラーの原因となったレート制限が、DDoS（分散型サービス拒否攻撃）攻撃のために設置されたものである場合、過度に広範で不正確なレート制限を課すことは、正当なユーザーですらブロックしてしまう可能性があります。Cloudflareのクライアントにとって、**DDoS攻撃対策がAPI軽減方法の第1位でした。**

本レポートの目的は、組織がAPIエンドポイント管理の健全性を**総合的に評価するための貴重なベンチマークを提供することです。**結局のところ、APIセキュリティは可視性、パフォーマンス、リスクを管理するためのデータも組み込まなければなりません。

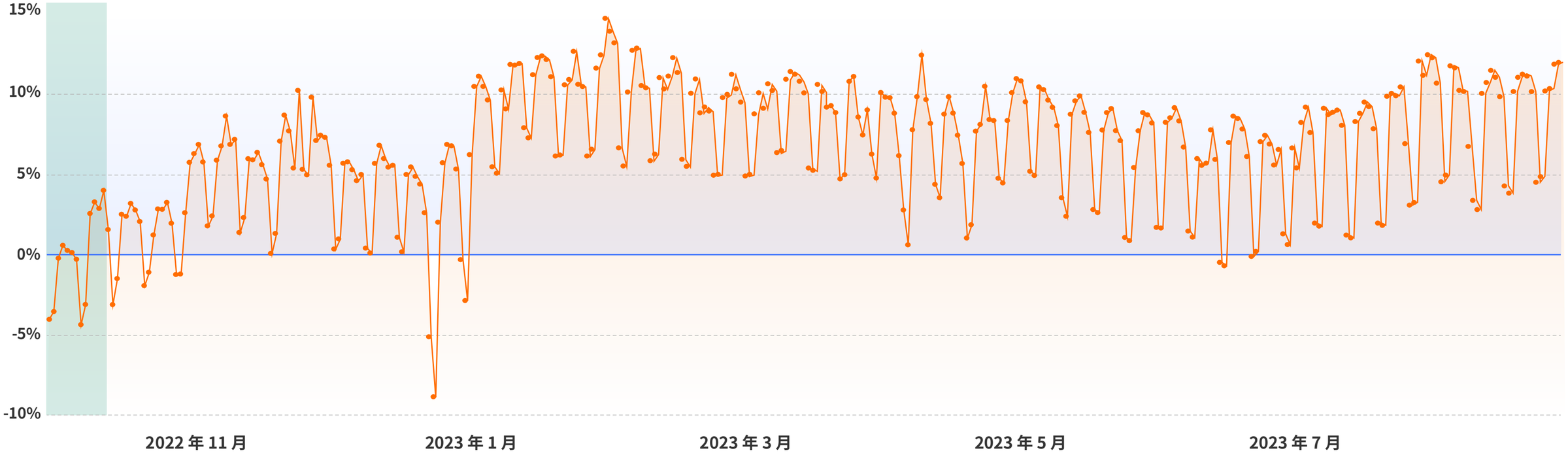
調査手法

この調査結果は、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。Cloudflareは毎秒平均5,000万件以上のHTTPリクエストを処理し、毎日平均1,700億件のサイバー脅威をブロックしています。

スナップショット：世界のAPI関連トラフィック

APIトラフィックの世界的な成長

ベースラインはハイライト表示、レスポンスコードは200、ダイナミックキャッシュのみ



2022年10月1日から2023年8月31日までの間、Cloudflareの動的HTTPトラフィックにおいて、成功応答（ステータスコード200）を示すAPIトラフィックは、53.1%から60.1%の範囲でした。動的コンテンツとは、訪問時間、場所、デバイスなど、ユーザー固有の要因に基づいて変化するコンテンツのことです。

主な調査結果

APIが他のインターネットトラフィックを凌ぐ

Cloudflareが処理したインターネットトラフィック（動的HTTPトラフィック）のうち、**成功したAPI呼び出しは57%**を占めました。[1]

未知の攻撃対象領域

機械学習モデルは、組織が自己報告したAPIエンドポイント数よりも**約3分の1（30.7%）多いAPIエンドポイント**を発見しました。[2]

No1エラー：リクエストが多すぎます

APIエラー率の半数以上（51.6%）が、「リクエストが多すぎます」（429エラー）でした。[3]

No1軽減方法：DDoS攻撃対策

APIに対する軽減策のうち、3分の1**（33%）は分散型サービス拒否（DDoS）攻撃のブロックでした。**[4]

業界のバリエーション

APIトラフィックの最も多いシェアを有する産業には、**IoTプラットフォーム、鉄道/バス/タクシー、法務サービス、マルチメディア/ゲーム、およびロジスティクス/サプライチェーンなどが含まれていました。**[5]

地域差

APIトラフィックは、**アフリカとアジア**で最もシェアされました。APIトラフィック**の変動が最も大きかったのは中東でした。**[6]

目次

隠れた攻撃対象領域

APIは、企業により優れたビジネスインテリジェンス、迅速なクラウド展開、新しいAI機能の統合などの競争上の優位性を生み出します。しかし、APIを最適化するための第一歩は、インターネット側にさらされているホスト名とすべてのAPIエンドポイントの完全なインベントリを保有することです。

組織がAPIの存在を知らなければ、APIを管理・保護することはできません。**そして結局のところ、多くの組織はAPIの完全なインベントリを保有していません。**

- **クライアントが提供したセッション識別子を介して発見したAPI RESTエンドポイントよりも、Cloudflareは機械学習によって、**約31%多くのエンドポイントを発見しました。[2]
- ***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。[7]

「シャドウ」APIとして知られる組織によって管理または保護されていないAPIは通常、特定のビジネス機能を実行するために開発者や個々のユーザーによって導入されます。

これらのシャドウAPIは本質的に悪意のあるものではありませんが、**シャドウAPIは本質的に保護されていない攻撃対象領域であり、新たなリスクをもたらします。**

シャドウAPIが悪用された場合、データの暴露、パッチ未適用の脆弱性、データコンプライアンス違反、ラテラルムーブメント、その他の脅威につながる可能性があります。

可視性の確認

現在、APIをどのように発見し、カタログ化していますか？

組織や開発者のAPIのインベントリは、APIスキーマ（有効なAPIリクエストとレスポンスの仕様を定義するメタデータ）を通じて把握されます。APIスキーマは、有効なAPI呼び出しとレスポンスの仕様を定義するメタデータです。これらAPIスキーマ（多くの場合、OpenAPI仕様で文書化されている）には、APIホスト、HTTPメソッド、パス、開発者が確立したその他の要件（パスやクエリ変数など）が記載されています。

目次

シャドウAPIのリスク

Cloudflareのよく見かけるものに、API管理を始めたばかりの組織が「メールで問い合わせる」方法があります。これにより、特定の時点でのインベントリが作成されますが、次のコードリリースで変更される可能性があります。しかし、この手作業によるアプローチは通常、グループ内独自の知識に頼ったもので、手作業によるミスが起こりやすくなります。

ある医療機関のITチームが、APIによってベンダーが特定のシステムにアクセスできることを知らなかったとします。ベンダーが侵害された場合、攻撃者はAPIを悪用して患者データを流出させる可能性があります。

例えば、2019年に発生したQuest Diagnostics社のデータ漏洩では、不正ユーザーが請求ベンダーに情報を送信するAPIにアクセスしたことで、約1200万人の患者のデータが流出しました。

2022年にオーストラリアの通信プロバイダーであるOptus社が侵害された件については、報告によると、攻撃者が認証されていないAPIを介してクライアントデータベースにアクセスしたことが原因でした。

経済が成長するにつれて、APIの開発や管理、セキュリティにおける損失や管理、複雑さの問題も拡大しています。

セキュリティチェック

どのAPIが「書き込み」アクセスを許可されているか、どのように監視していますか？

アカウント全体のAPIを集計すると、Cloudflareは、組織のうち**59.2%が少なくとも半数のAPIに対して「書き込み」のアクセス権を付与していることを発見しました。**[8]

「読み取り専用」（GET）でアクセスするAPIは、システムから情報を引き出し、取り込みます。しかし、「書き込み」（POST、PUT、DELETE）でアクセスするAPIは、ユーザーや他のアプリがシステムの更新（変更）をプッシュすることも可能にしています。

多くのAPI侵害は寛容な権限付与が原因で発生しています。つまり、ユーザーが過剰な権限を付与されたり、他のユーザーのデータへのアクセスを許可されたりしているということです。APIが誤った人物に「書き込み」アクセスを提供した場合、本レポートで説明されているような攻撃につながる可能性があります。

一般的なAPIエラー

組織がAPIエンドポイントを正確に発見（その後、保存または削除）した場合、何がうまくいっているのか、そして何がうまくいっていないのかを知る必要があります。APIエラーはサイバー攻撃やアプリのパフォーマンスの問題を知らせる可能性があり、それが原因で正当なビジネス活動が妨げられることがあります。

HTTPステータスコードは、アプリが正常に動作しているか、エラーが発生しているかを示すために最も頻繁に使用される3桁のコードです。

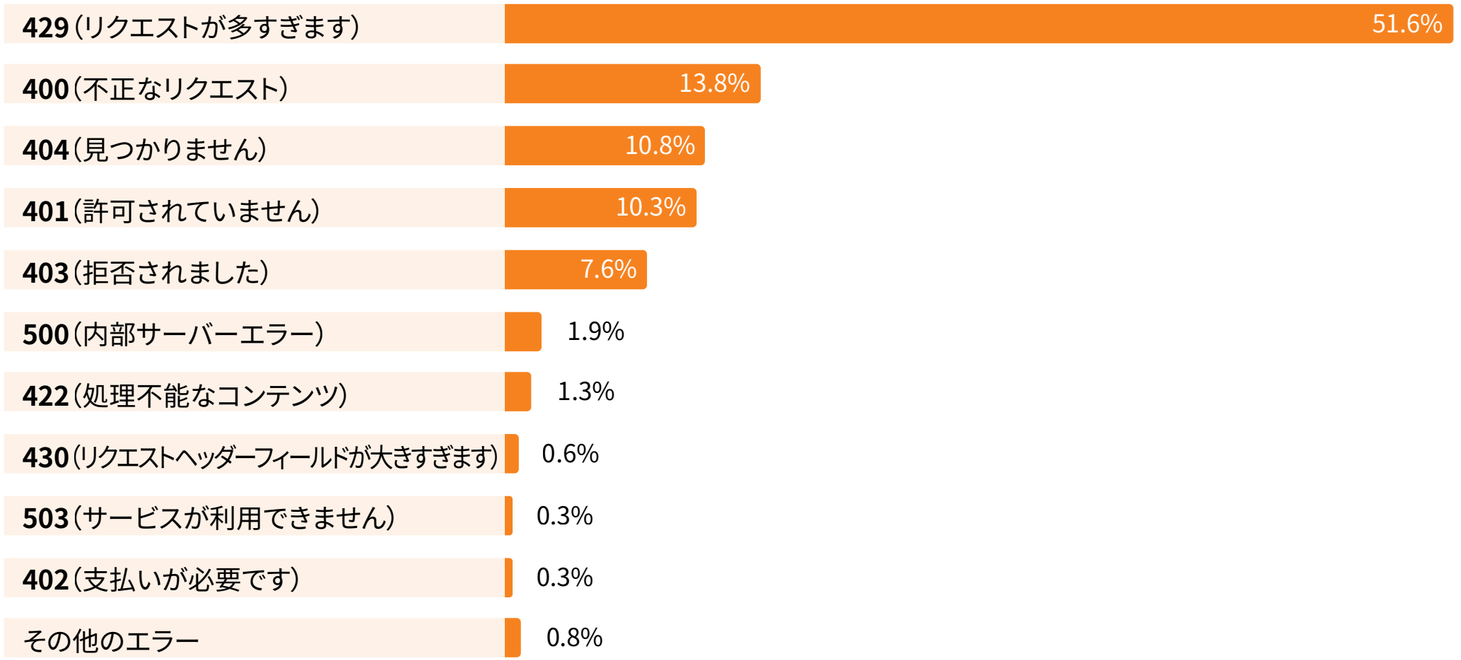
APIや他のHTTPリクエストにおいて、「2」で始まるステータスコード（2xxの成功コード）は、クライアントのアクションが受信され、理解され、受け入れられたことを示します（つまり、成功したことを示します）。

しかし、アプリ訪問者が意図した場所に到達できない場合、代わりにリダイレクトされたり（3xxリダイレクション）、4xxクライアントエラーや5xxサーバーサイドエラーが発生したりする場合もあります。

CloudflareはAPIの出典元から数兆のトラフィックエラーを観測し、**そのうち半数以上（51.6%）が「429」コードである「リクエストが多すぎます」から構成されていました。**[3]

「レート制限」としても知られる429エラーは、クライアントが一定の時間内にあまりにも多くのリクエストを送信した場合にサーバー側で発生します。

一般的なAPIエラー



エラーの説明については付録を参照してください

APIエラーを誤診するリスク

429エラー（前述の通り**最も頻出するAPIエラー**）は、特定のアクションが発生した場合にサーバーがAPIトラフィックを自動的に制限したことを意味します（例：特定のIPアドレスが特定のログインエンドポイントに対して1分あたりのリクエストを超えた場合など）。

しかし、組織が適応型のレート制限ではなく手動で設定されたレート制限を使用している場合、それらは即座に時代遅れとなる可能性があります。たとえば、ログインエンドポイントが通常よりも高いトラフィックを経験している場合はどうでしょうか。このシナリオでは、手動のレート制限は正当なトランザクションを妨げる可能性があります。

原因が「誤診断」されがちな別のエラーは、**401「非承認」エラー（CloudflareがAPIトラフィックで観測した中で4番目に多いエラー）です。**

401エラーは、ユーザーの資格情報が存在しないか、または要求されたリソースへの適切なアクセス権を含んでいなかったことを意味します。しかし、他のHTTPエラーコードと同様に、このコードは脅威（全体的なアカウント乗っ取りにつながる可能性のある「壊れたオブジェクトレベル認可」攻撃など）に起因する可能性があります。あるいは、単に正当なユーザーが誤った資格情報を入力した結果である可能性もあります。

APIトラフィックの「誤診断」の一例として、2023年初頭、GoogleはWebサイト所有者や一部のコンテンツデリバリーネットワークに対して、（正当な）Googlebotのクロール速度を制限するために、誤ったステータスエラーを使用しないよう警告しました。

Googleがユーザーに注意喚起したように、*「クライアントのエラーとは単にクライアントのリクエストに何らかの誤りがあったことを意味します。」*

パフォーマンスチェック

APIエラーをどのように監視、評価していますか？

すべてのAPIエラーが攻撃によって引き起こされるわけではありません。APIエラーの根本的な原因（およびそれらの問題の背後にある傾向）を理解するには、APIトラフィックの一貫したロギングと、長期的な傾向の分析が必要です。

どれだけのAPIトラフィックがレート制限を受けているかご存知ですか？不正な認証を理由に拒否されている件数は？エラーの原因が攻撃によるものであるか、認証情報の有効期限が切れた（あるいは入力が不正確など）ユーザーを起因とするものであるかを確認されていますか？

上位のAPIセキュリティの脆弱性

APIを悪用から守るのは困難です。他のWebアプリセキュリティサービスと比較して、より深いビジネスコンテキスト、発見方法、アクセス検証コントロールが必要となります。

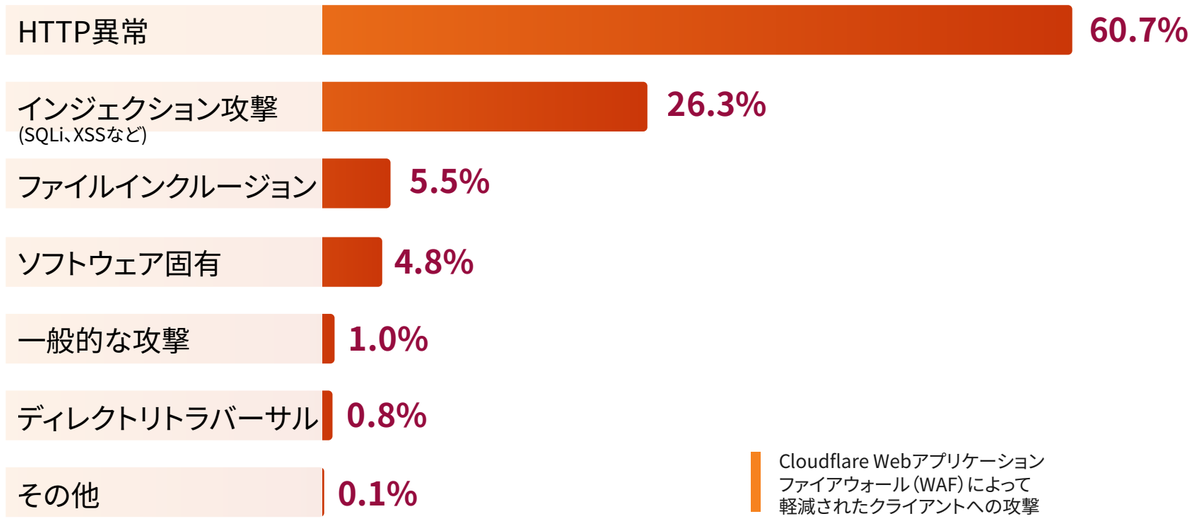
例えば、以下を考えてみましょう。

Webアプリケーション	API
エンドユーザーに**表示**される	アプリユーザーに**表示**される
Webブラウザ**を通してエンドユーザー**がアクセスする	**システムとアプリ**がデータを交換できるようにする
さまざまなユーザー側の操作を使用して、バックエンドからの**データを視覚化**します（HTML、CSS、およびJavaScriptを使用）。	サーバーとアプリケーションにアクセスし、定義済みフォーマット（最も一般的なRESTful JSON、gRPC、XML、GraphQL）を使用して、**データを転送します。**
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されます。	検証および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、より効果的に保護されます。

このような（そしてその他の）理由から、APIの定期的かつ自動化されたモニタリングは、セキュリティの脅威を迅速に特定し、対処するために極めて重要です。

以下は、2023年にCloudflareがクライアントのために軽減したAPIに対する最も頻度の高い脅威のスナップショットです[9]：

API脅威上位



これらの攻撃タイプのより詳細な説明は付録を参照してください。

MDM攻撃におけるAPIの脆弱性の役割

モバイルデバイス管理（MDM）は、企業が地理的に分散したすべてのデバイスを単一のプラットフォームで管理するのに役立ちます。MDMを使えば、ITチームはデバイスに内蔵されたAPIを使って、管理対象デバイス上にアプリを展開し、制御することができます。

しかし、MDMシステムの容易さと利便性は、リスクと天秤にかける必要があります：MDMシステムは、攻撃者が何千台ものモバイルデバイスに自由にアクセスできるため、格好の標的となります。

2023年8月、サイバーセキュリティおよびインフラストラクチャセキュリティ機関（CISA）とノルウェー国立サイバーセキュリティセンター（NCSC-NO）は、共同のサイバーセキュリティアドバイザリを発行しました。これは、2つの脆弱性を結びつけて攻撃者が**Ivanti社のエンドポイントマネージャーモバイル（EPMM、以前はMobileIron Coreとして知られていました）を攻撃する可能性があることを警告するものです。**

攻撃者は、次のチャートで概説されたMITRE ATT&CK®の技術など、複数の手法を使用しました。MITRE ATT&CKのようなフレームワークやOWASP API Security Top 10の準拠は、より強固なサイバーセキュリティの基盤を提供し、強化されたAPIディフェンスを含むものとなります。

例としてのテクニック （*詳細なリストはこちら*）	**使用内容**
アプリケーションの悪用	攻撃者は、少なくとも2023年4月以降、パブリック向けのIvanti EPMMアプライアンスでCVE-2023-35078を悪用していました。
コマンドおよびスクリプトインタープリター	攻撃者は、CVE-2023-35081を悪用してEPMMデバイス上にWebシェルをアップロードし、コマンドを実行した可能性があります。
アカウント検出：ドメインアカウント	攻撃者はCVE-2023-35078を悪用し、EPMMデバイスのユーザーと管理者の情報を収集しました。 **このシナリオでは、攻撃者はAPIパス** /mifs/aad/api/v2/authorized/users**を使用し、EPMMデバイス上のユーザーおよび管理者を一覧化しました。**
遠隔システムの検出	攻撃者はLDAPエンドポイントを取得しました。
サーバーソフトウェアコンポーネント：Webシェル	攻撃者は侵害されたインフラにWebシェルを埋め込みました。
プロキシ	攻撃者は、侵害されたSOHOルーターを利用して、プロキシ経由でインフラを侵害しました。

一般的なAPIの脆弱性を軽減する2つの方法

1. スキーマの検証

ユーザーエージェント（エンドユーザー向けにインターネットコンテンツを取得するソフトウェア）の欠落、不正なメソッド名、非標準ポートなどのHTTP異常は、悪意のあるリクエストの一般的な兆候です。また、前述の通り、Cloudflareが対処したAPIの脅威の大半は、この種のHTTP異常でした。

スキーマ検証は、各APIの「クリーン」なトラフィックだけをAPIサーバーに許可するために、HTTPの異常を特定する貴重な方法です。APIスキーマは、ターゲットエンドポイント、パスまたはクエリ変数フォーマット、HTTPメソッドなど、いくつかのリクエストプロパティに基づいて、どのAPI呼び出しが有効かを定義します。

2. 認証の抜け穴に挑む

API関連のデータ漏洩に関する過去のニュースの見出しにも表れるように、パブリックAPIにおける認証の欠如（または破損）も深刻な問題です。

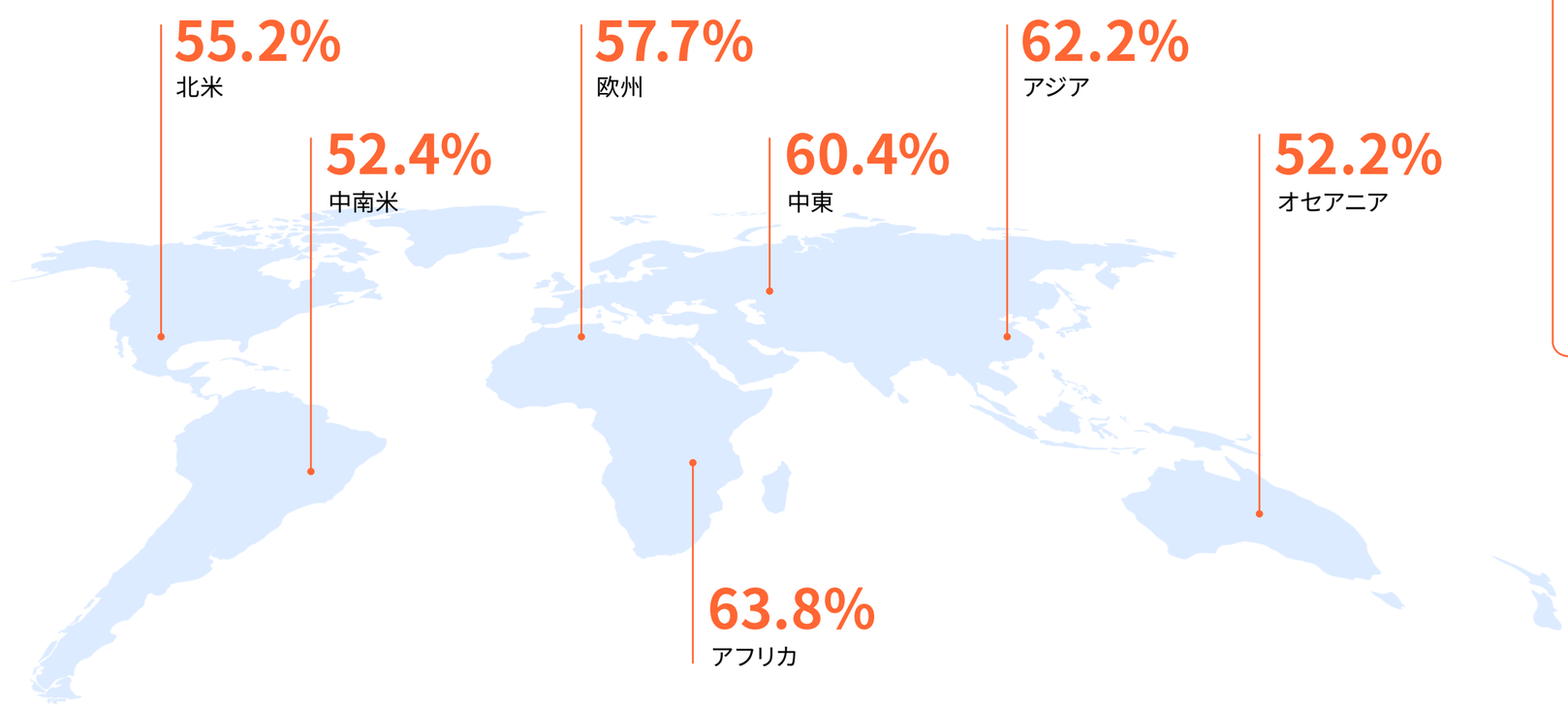
ここでは、APIを通じて機密データを暴露する可能性のある認証の抜け穴に対処する4つの方法を紹介します。

- まず、ビジネス上承認された例外を除き、一般にアクセス可能な各APIに認証を強制します。
- サーバーへのAPI呼び出しの速度を制限し、潜在的な攻撃者の動きを鈍化させます。
- 異常な量の機密データの流出をブロックします。
- 攻撃者が正当なAPI呼び出しのシーケンスをスキップするのをブロックします。

API中心の世界

地域の動向

Cloudflareが保護する各地域において、APIトラフィックはその地域の動的HTTPトラフィックの半分以上を占めています[10]：



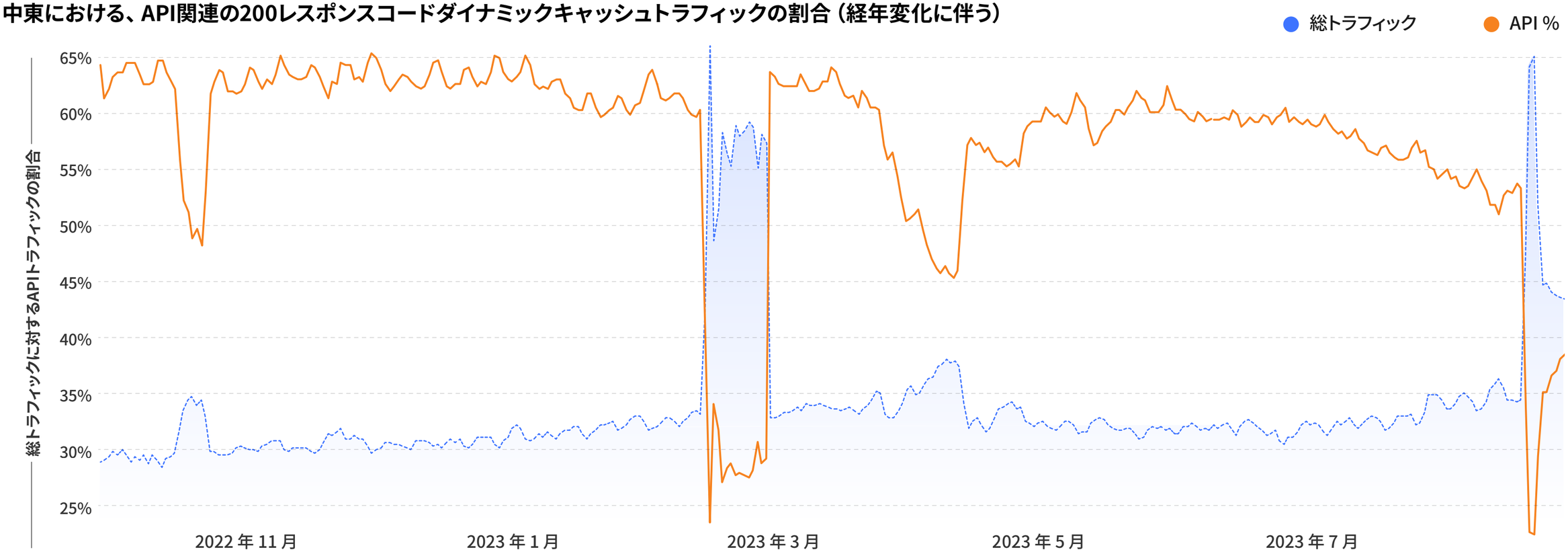
全体として、APIトラフィックの合計は、2023年を通して着実に増加しました。しかし、以下の地域では顕著な変動がありました。

- **中南米**では、APIトラフィックは動的HTTPトラフィックのうち**46.1%から58.6%**を占めていました。
- **オセアニア**では、APIトラフィックは動的HTTPトラフィックのうち**44.1%から57.4%**を占めていました。
- そして**中東**では、**APIトラフィックが最も変動したとされ、**それについては次のセクションで詳しく言及しています。

中東のトラフィックスパイク

中東でのAPIトラフィックの大きな変動は、ネットワークの制限の回避に使用する**匿名ツールへの突然の一時的な全体的なトラフィック**の急増した時期と一致していました。Cloudflareは、2023年のこの匿名ツールへのトラフィックの急増が、政府主導のインターネットシャットダウンの直後に発生したことを観察しました。

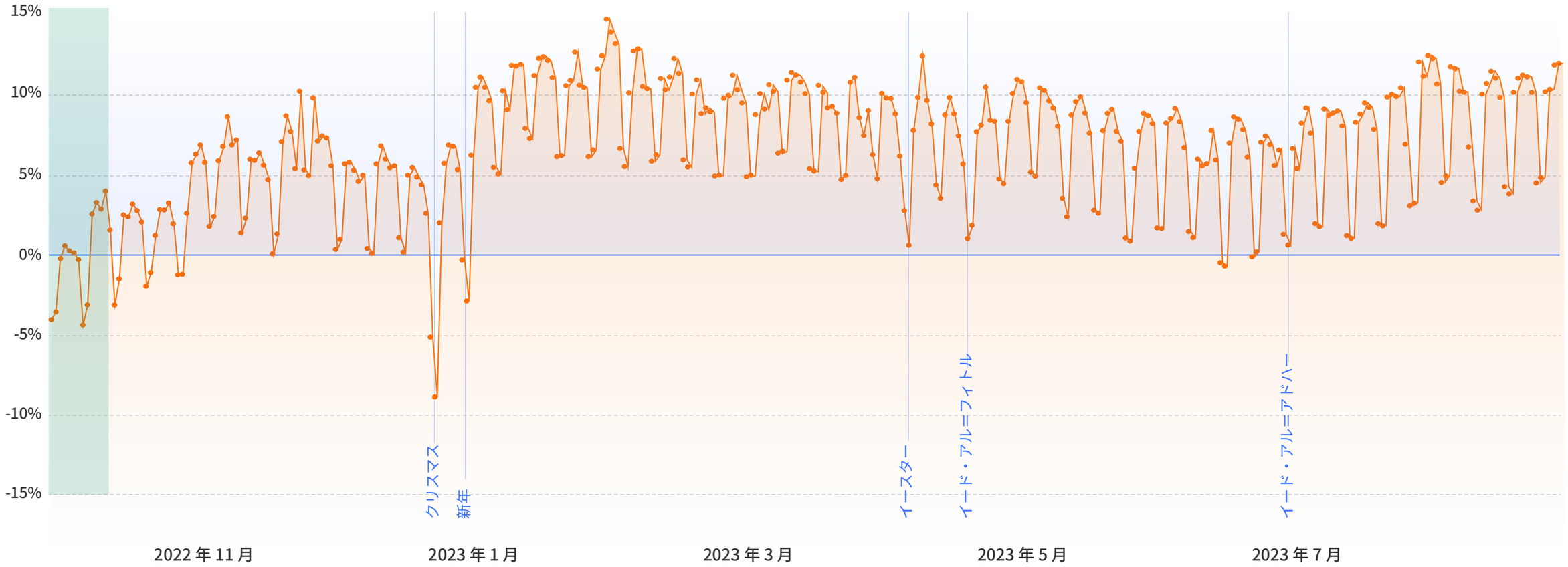
中東における、API関連の200レスポンスコードダイナミックキャッシュトラフィックの割合（経年変化に伴う）



APIのトラフィックは遅くなるのか？

APIトラフィックはボット間の会話と思われがちですが、Cloudflareのデータによると、APIトラフィックは年間を通して、特に大型連休の前後で、明らかに急増と急減を繰り返しています。

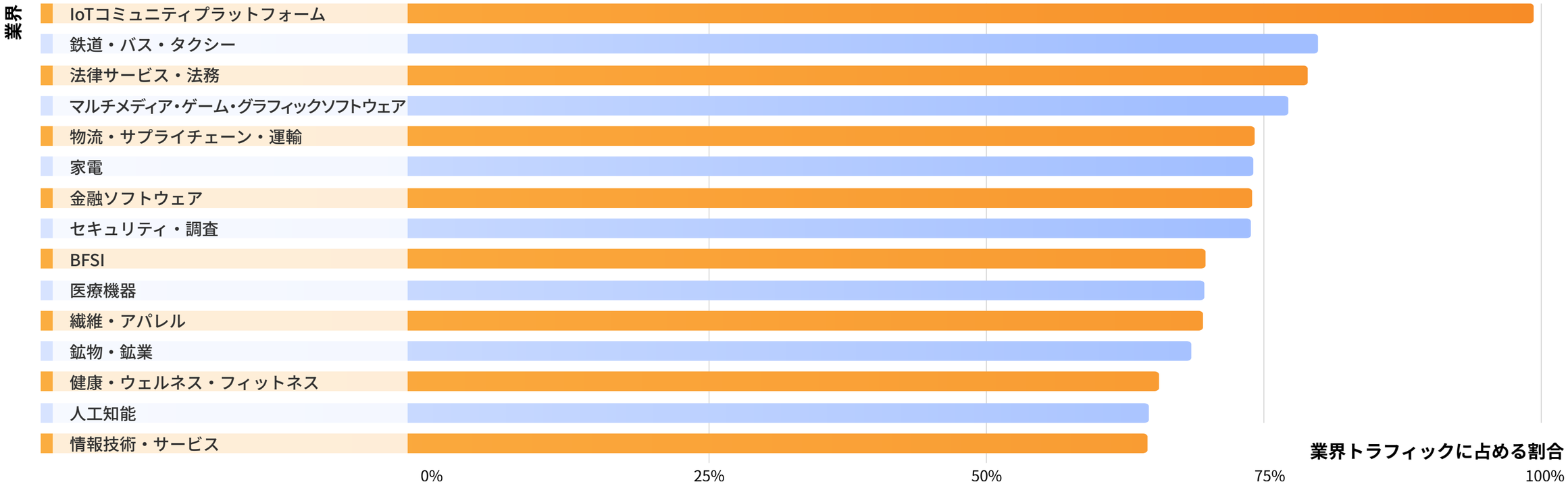
人々がオフラインである可能性が高いと思われる時期（たとえば、**12月25日（クリスマス）、4月9日（イースター）、または4月22日（イード・アル＝フィトル））には、APIトラフィックが顕著に減少するようです。**[11]



業界を超えたAPIトラフィック

特定の地理的な変動に加えて、**一部の産業は他の産業と比較して、APIトラフィックの割合が大きくなっていました。**

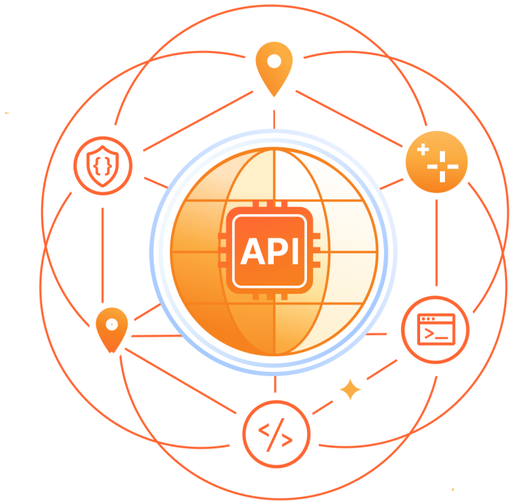
CloudflareがAPIによるトラフィック量が他の動的なHTTPトラフィックに比べて多いと観察した上位15の産業は以下の通りでした[12]：



業界のベンチマーク

アプリケーション、Webサイト、モバイルアプリは、ゼロから新しい機能を作る代わりに、APIを介して機能を追加することで、ユーザーエクスペリエンスを豊かにすることができます。

例えば、ライドシェアアプリは、独自の決済サービスをゼロから作るのではなく、決済会社のAPIを経由して決済を追加することができます。また、小売業のAPIは、バーチャル試着室、商品の推奨、注文状況など、クライアントの体験をパーソナライズする際に役立ちます。



APIは、あらゆる業界、あらゆる場所で役立ちます。

以下は、特定の地域全体で最も高いAPIトラフィックの割合を持つ産業です。[12]:

アフリカ

1. **施設サービス**
2. 鉱物・鉱業
3. 資本市場
4. 資金調達
5. クレジットカードおよびトランザクション処理

アジア

1. **IoTコミュニティプラットフォーム**
2. 鉱物・鉱業
3. 繊維・アパレル
4. 銀行、金融サービス、保険
5. 人工知能

欧州

1. **マルチメディア、ゲーム、グラフィックソフトウェア**
2. コンテンツ・コラボレーションソフトウェア
3. 医療機器
4. 繊維・アパレル
5. 法務サービス

中南米

1. **鉱物・鉱業**
2. 金融ソフトウェア
3. マルチメディア、ゲーム、グラフィックソフトウェア
4. 資本市場
5. 弁護士

中東

1. **資金調達**
2. 法務サービス
3. ワイヤレス
4. 資本市場
5. 運輸・トラック運送・鉄道

中東

1. **法務サービス**
2. 鉄道、バス、タクシー
3. コンシューマーエレクトロニクス
4. セキュリティと調査
5. 物流、サプライチェーン、運輸

北米

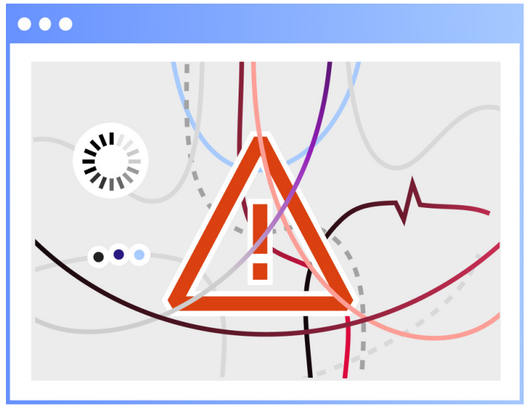
1. **鉱物・鉱業**
2. 繊維・アパレル
3. 資本市場
4. セキュリティと調査
5. 医薬品、バイオテクノロジー、健康

2024年以降の予測

消費者とエンドユーザーがより速く、よりダイナミックなWebとモバイルエクスペリエンスを求め続ける中、開発チームとAPIチームはより多くのAPIをデプロイし、維持する必要に迫られるでしょう。このような善意のアプリ開発者は、ときには、他のITやセキュリティの利害関係者に相談することなく、APIを迅速に展開し続けるでしょう。

このようなまとまりのないアプローチでは、企業は以下のような課題に直面し、困難な状況に追い込まれることになります。

1 コントロールの喪失と複雑性の増大



IT意思決定者たちは、「ITおよびセキュリティ環境のコントロールを失う要因の第1位は「アプリケーションの総数」であり、それに続いて「アプリケーションの場所の増加」である」と述べています。

しかし、ほとんどの組織では、これらのチームはサイロ化されたままです。

73% 開発者のうち、そのセキュリティチームが使用を要求する仕事やツールが「生産性とイノベーションに干渉している」と述べている人の割合。

87% CIOうち、ソフトウェアエンジニアと開発者が「新製品やサービスを迅速に市場に投入するためにセキュリティポリシーやコントロールを妥協している」と考えている人の割合。

<50% CISOのうち、開発者が「開発およびワークフローのツールのセキュリティリスクに非常に精通している」と感じている人の割合。

IT、セキュリティ、アプリ開発チームはすべて、何千ものAPIがサポートする資産を持つことに伴う膨大な攻撃対象領域を保護する責任を共有しています。

自動化されたAPI保護によってIT、セキュリティ、アプリ開発間の断絶を解決しない限り、**事業におけるAPIリスクと管理の複雑さが増すと予想されます**。

2 AIへのアクセスが容易になり、APIリスクが増大

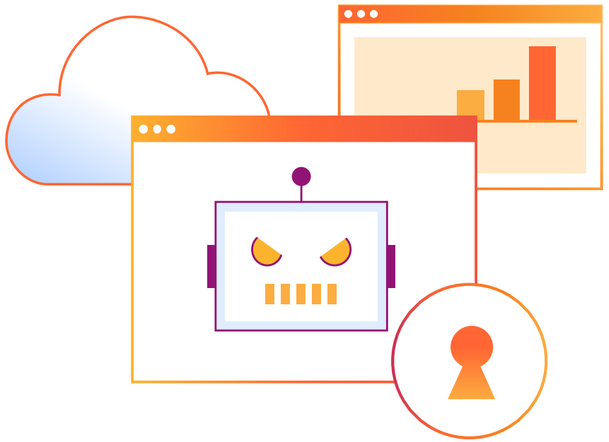
アナリストたちの予測によると、2026年までに80%以上の企業が生成的な人工知能（GenAI）APIやモデルを使用、またはGenAI対応のアプリケーション（例：ChatGPT）を実際の稼働環境で展開するとされています。

GenAIモデル（Webアプリのフロントエンドがない場合）は、一般的には内部機能として直接アクセスされるか、OpenAIのChatGPTやWhisper APIなどの公開APIを介して他のアプリやユーザーからアクセスされます。**GenAIの使用がAPIの使用を大幅に増加させるため、GenAIサービスはそのAPIに対するAPI関連の攻撃を引き寄せる可能性があります。**

例えば、競合他社や攻撃者が数百万回程度製品のAPIを呼び出してデータを抽出して盗み出す場合、被害者のインフラストラクチャには目をつぶることのできる程度の直接コストしかかかりません。しかし、攻撃者が対象の被害者の生成モデルをAPIを介して利用する場合、コストははるかに高くなります — 一呼び出しにつき数セント。攻撃者が人工知能アプリのAPIに何百万回も濫用的な呼び出しを行うと、即座に財務的な損失につながる可能性があります。

そして、GenAIが善意で活用されている場合であっても、多くの開発者にとっては未知の（つまり、リスクのある）領域です。Forresterは2024年に、適切な防御策がない場合、「少なくとも3つのデータ漏洩が、安全でないAI生成コードに起因するか、またはAI提案の依存関係にセキュリティの欠陥があるために公然と非難されるだろう」と予測しています。

3 ビジネスロジックに基づく詐欺攻撃の増加



2020年代には、ボットオペレーターがWebブラウザの計装版を使用してWebアプリをターゲットとし、洗練されたブラウザベースのボットを作成するようになりました。これと並行して、最近のアプリのほとんどは、アカウント作成、ログイン、フォーム入力、金銭取引ワークフローなどのユーザーアクションを完了するために、舞台裏でAPIを使用しています。

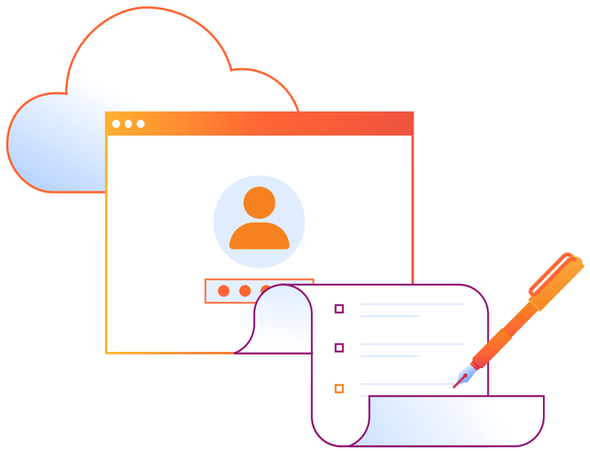
そのような攻撃はより効率的であり（APIはWebアプリのUIよりも頻繁に変更されない傾向があり）、（Webアプリと比較して）保護されていないため、2024年にはボットオペレーターがこれらのワークフローの背後にあるAPIを直接攻撃することが増えると予想されます。

スポーツベッティングやファンタジーリーグにおける偽アカウントの作成を例に挙げてみましょう。一人で複数のアカウントを持ち、異なるベットやチームラインナップを行うことで勝率が上がり、それがしばしば金銭的な報酬につながることあります。このように、大量に新しいアカウントを自動的に作成するインセンティブは、さらに利益をもたらすことがあります。

同様のインセンティブが、マルチファクタ認証が存在しないか簡単に回避できる状況でのクレデンシャルスタッフィング攻撃や限られた供給のアイテムの詐欺的な購入などで現れています。

このような場合、企業はAPIセキュリティツールに対して、ビジネスのロジックに基づくインテリジェンスを必要とします。例えば、攻撃者が不正行為を短時間で実行するために試みた、異常な数のシーケンスを特定します。また、API呼び出しが、そのAPIのベースラインのトランザクション量よりも速くトランザクションを完了しようとするなど、異常な動作特性を持つ場合を特定します。

4 高まる規制およびガバナンス



組織はまた、API関連のセキュリティとプライバシーに対する、**より強力なガバナンスと規制の取り組みが期待されるべきです**。

例えば、「PCI DSS（Payment Card Industry Data Security Standard）」は、カードホルダーのトランザクションおよび支払い認証データを管理するためのプロセスをビジネスに指南するフレームワークです。2024年3月31日に、**新しいPCI DSS v4.0の要件が発効され、これはAPIセキュリティに明示的に取り組む最初のバージョンとなります**。

PCI DSS v4.0のリリースに伴い、カード決済を送信または処理するすべての組織は、APIの脆弱性への対応、適切なAPI認証の確保などが求められます。PCI DSS 要件を遵守しない場合、高額な罰金やその他の罰則が科される可能性があります。

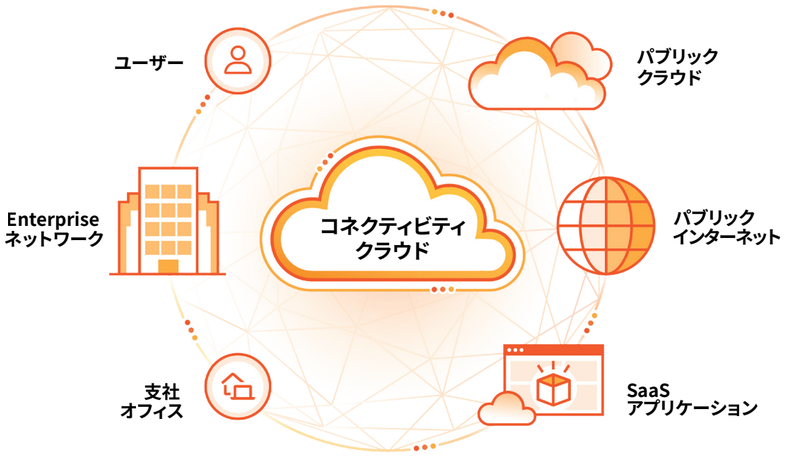
ヘルスケアは、システム間で電子的保護医療情報（ePHI）を伝送するAPIの能力により、APIをめぐる監視が厳しくなることが予想される、もう一つの規制の厳しい業界です。

2023年7月、米国連邦取引委員会（Federal Trade Commission）および保健福祉省の公民権事務所（Office for Civil Rights、OCR）は、健康アプリのプライバシーリスクに対する監視を強化し、個人の健康データの侵害を開示しない場合には金融制裁が科される可能性を警告しました。

推奨事項

どんなソフトウェアもそうですが、APIの脆弱性は起こり得ます。攻撃者がアプリケーションやAPIを破壊するために常に新しい戦術を試みることは誰も止められませんが、組織は以下のベストプラクティスを取り入れた全体的なアプローチでAPIを特定、保護および管理することができます。

1 コネクティビティクラウドでアプリ開発、可視化、パフォーマンス、セキュリティを一元管理



多くの企業では、独自のインフラ、独自のコンプライアンスニーズ、互換性が不十分なプロセスや構成によって、SaaSアプリ、Web アプリ、その他ITインフラを接続することが難しくなっています。これらの領域は単純に、容易・安全に連携できるように作られていません。

コネクティビティクラウドは、企業がデジタル環境をセキュアにし、接続するために必要な多くのサービスを提供する新しいアプローチです。これは、プログラマブルでクラウドネイティブなサービスのインテリジェントなプラットフォームであり、ネットワーク、クラウド環境、アプリ、ユーザー間の任意の接続を可能にします。

コネクティビティクラウドは、アプリのデプロイメントとAPI防御の綿密なサービスとの間の結合組織を提供します。

- 組織にAPIエステート（APIの状態や構成の全体像）の明確なインベントリをもたらす**自動化されたAPIディスカバリーと可視化**
- 最初から組み込まれた**現代の認証および認可**プロセス
- API駆動のドメインに対して遅延、エラーおよびエラーレート、および応答サイズなどのメトリクスをモニタリングする**APIエンドポイント管理**
- **API**アプリケーション層7（L7）**の保護、**拒否サービス攻撃に対する高度なレート制限やDDoS攻撃対策、ブルートフォースによるログイン試行、およびその他のAPIの悪用に対する保護など
- **zero-day**（新しい脆弱性で、パッチや修正がないソフトウェアで見つかる）の検出は、zero-day攻撃が発生する前にその脆弱性を検知することです。

2 APIゲートウェイによる「ポジティブセキュリティ」モデルへの移行

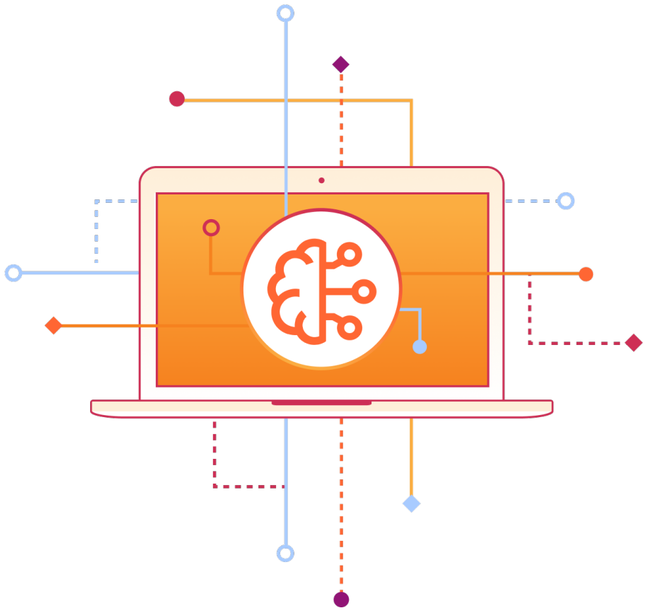
推定では、使用中のパブリックおよびプライベートAPIは約2億もあり、これは増加しています。ITおよびセキュリティのリーダーが各APIのパフォーマンス、挙動、およびリスクの露出を現実的に「追いつく」ことは困難です。

従来、Webアプリケーションは「ネガティブセキュリティ」モデルによって保護されており、問題のあるIP、ASN、国、または問題のある署名（SQLi試行など）からのリクエストを除くすべてを許可する「Webアプリケーションファイアウォール（WAF）」が強制されています。これは、Webアプリケーションにはさまざまな方法でユーザーがアクセスしてやり取りできるためです。このモデルでは、WAFは「既知の悪意のある」トラフィックをブロックし、他のすべてのトラフィックを許可します。

これとは対照的に、API向けの「ポジティブセキュリティ」モデルは、APIがそれらとやり取りするための構造化された形式を持つため、より適しています。ネガティブセキュリティアプローチとは反対に、**「ポジティブセキュリティモデル」は「既知の適正な」動作とアイデンティティ（APIスキーマで定義された「適正」）のみを許可し、**それ以外のすべてを拒否します。

ポジティブセキュリティモデルを使用する組織は、そのスキーマに適合するトラフィックだけを受信することによって、APIを保護します。クレデンシャルスタッフィング攻撃や自動スキャンツールなど、不正なリクエストやHTTPの異常をより効果的にブロックすることができます。

3 機械学習を使用してリソースを解放し、コストを削減

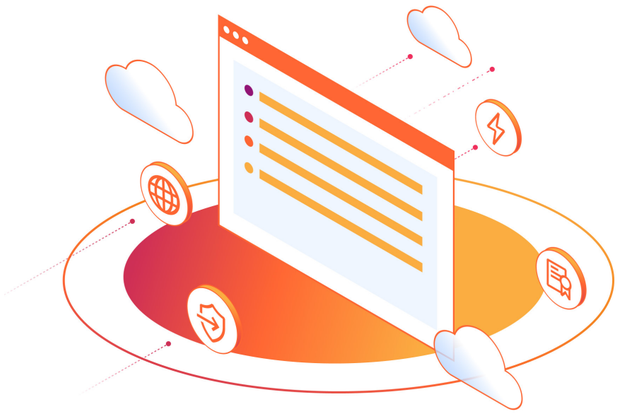


自動化や特定の目的のために作成されたAPIツールがなければ、ITとセキュリティの利害関係者はAPIチームに追いつくチャンスはありません。

一方で、組織は機械学習ベースのセキュリティサービスを利用することで、APIの可視化とセキュリティ管理をより効率的に行うことができます。例えば、機械学習は迅速な実施を可能にします。

- セッション識別子に基づくデータに関係なく、ドメインへのすべてのAPIトラフィック（非認証APIを含む）を**明らかにする**
- APIに対するRCE、XSS、およびSQLi攻撃の変種を**検知する**
- さまざまなトラフィックタイプとAPI攻撃ベクトルを区別するための分類器を**訓練する**
- アプリ利用者のトラフィックによる正当なスパイクと、潜在的に悪意のあるボットトラフィックからのスパイクを**区別する**

4 組織のAPI成熟度レベルを測定し、長期的に改善する



APIを保護するための最も包括的なアプローチは、総合的なWebアプリケーションおよびAPI保護（WAAP）プラットフォームを実装することです。ただし、APIの露出を認識し始めたばかりの組織は、これをすぐに実現できないかもしれません。

しかし、すべての進歩には始まりの地点が必要です。組織が保護すべきものを理解すれば、包括的なAPI管理とセキュリティに向けて前進することができます。

レベル1：可視性

企業はまず、シャドウAPIを含むすべてのAPIエンドポイントを追跡し、正式に管理する必要があります。しかし、多くの組織は、開発者がAPIを構築するほど迅速にAPIを見つけることはできません。また、APIを見つけたとしても、潜在的に数百あるAPIエンドポイントごとに、固有のスキーマを個別かつ正確に構築することは困難です。

API可視化サービスを使えば、組織はAPIエンドポイントを自動的に発見し、そのAPIが誰のもので、どのように使われるべきかを特定することができます。

レベル2：一般的なWeb攻撃対策

WebアプリケーションとAPIは、しばしば協力して動作します（例えば、eコマースのWebサイトが支払いを処理するためにAPIを使用するなど）。しかし、インターネットのグローバルな性質により、Webサイトやその他アプリケーションは、多くの場所、様々な規模や複雑さのレベルからの攻撃にさらされています。

以下は、「table stakes」サービスの例です（詳細についてはこちら）。これらのサービスは、Webアプリケーションとそれらの背後にあるAPIをDoSおよびDDoS攻撃、クレデンシャルスタッフィング、zero-dayの脆弱性、およびその他の脅威から直接保護します。

- **DDoS軽減サービス**は、サーバーと公共のインターネットの間に位置し、悪意のあるトラフィックの急増がサーバーを圧倒するのを防ぎます
- **Webアプリケーションファイアウォール（WAF）**は、Webアプリケーションの脆弱性を利用することが知られている、または疑われているトラフィックをフィルタリングします
- **暗号化証明書管理**は、SSL/TLS暗号化プロセスのキー要素を管理するのに役立ちます
- **高度なレート制限**は、正規ユーザーに影響を与えることなく、DoS攻撃、ブルートフォースによるログイン試行、およびその他のAPIトラフィックの急増からエンドポイントを保護します

レベル3 - API固有の攻撃対策

WAFやDDoSのようなツールは、Webセキュリティと（人間の）アプリユーザーのエクスペリエンスにとって重要ですが、これらのサービスはアプリケーションを保護するために設計されたものであり、APIに特化したものではありません。

組織がAPIを介してより多くのサービスを公開するようになれば、Webアプリケーションのセキュリティを、APIに特化したセキュリティと管理で補強する必要があります。

先進的なAPIセキュリティは、無監督の機械学習を使用して、各APIに対して独自のベースラインを開発し、API呼び出しの意図（正当または悪意のあるものか）をリアルタイムで予測することが可能です。

組織は、APIセキュリティがチームの多くにとって初めてのものであることを理解しています。セキュリティはそれ自体のために達成されるものではなく、ビジネスの成果を向上させ、より良くするために達成されるものです。これらの利点として、より迅速な製品提供、公開APIにおけるセキュリティの抜け穴の減少、より効率的なセキュリティチーム、そして最終的には、より生産的な開発者とAPIチームなどが挙げられます。

ビジネスの成長を促すAPIの保護

CloudflareのCloudflareコネクティビティクラウドによって強化されたWebアプリとAPI保護 (WAAP)ポートフォリオは、主要なアプリケーションセキュリティ機能を統合し、アプリケーションとAPIを安全かつ生産的に保ち、DDoS攻撃を阻止し、ボットをブロックするなどの機能を提供します。

詳細

CloudflareのAPIディスカバリー、OWASP API トップ 10リスクに対する保護、mutual TLS、イノベーションを損なうことなくAPIを保護することについて。

目次

APIセキュリティ用語集

APIコールまたはAPI呼び出し：APIにサービスや情報の提供を依頼するためにサーバーに送信されるメッセージです。

APIディスカバリー：APIディスカバリーは、組織内で使用されているすべての社内製およびサードパーティ製のAPIをカタログ化するプロセスです。

APIエンドポイント：APIリクエスト（またはAPI呼び出しとも呼ばれる）が届けられる場所です。APIエンドポイントはほとんどの場合、サーバー上にホスティングされています。

APIトラフィック：レスポンスのコンテンツタイプがXML、JSON、gRPC、またはそれに類似するすべてのHTTPリクエストです。軽減されたリクエストなど、レスポンスのコンテンツタイプが使用できない場合、代わりに同等のAcceptコンテンツタイプ（ユーザーエージェントによって指定される）が使用されます。後者の場合、APIトラフィックは完全には考慮されませんが、インサイトの面では引き続き役に立ちます。

ボットトラフィック/自動トラフィック：Cloudflareのボット管理システムにより、ボットによって生成されたと識別された任意のHTTPリクエストです。

壊れたオブジェクトレベル認可（BOLA）：BOLAは、1件のリクエストに含まれるオブジェクトIDの操作を意味するもので、機密データへ許可なくアクセスすることを目的としています。攻撃者はBOLAを使用して、IDを変更するだけでアクセス権を持たないオブジェクト（データ）にアクセスできます。

認証の不備：認証が正しく実装されていない場合、攻撃者はAPIユーザーになりすまし、機密データにアクセスできるようになる可能性があります。

クライアント：HTTPリクエストを行う側。通常はブラウザでサイトにアクセスするエンドユーザーですが、APIクライアントやサイトからリソースを要求する他の誰かも含まれる可能性があります。

ディレクトリトラバーサル：パストラバーサル攻撃としても知られ、ディレクトリトラバーサルは、Webルートフォルダーの外部に保存されているファイルやディレクトリにアクセスしようとします。

分散型サービス妨害（DDoS）攻撃：DDoS攻撃は、標的もしくはその周りのインフラストラクチャに大量のインターネットトラフィックを与えることで、標的となるサーバー、サービス、ネットワークの通常トラフィックを妨害しようとする悪意のある行為です。

ファイルインクルージョン：この脆弱性は、攻撃者が対象のアプリケーションにファイルを組み込むことを可能にします。この脆弱性は、適切な検証なしにユーザー提供の入力を使用することに起因します。

HTTP異常：CloudflareのManaged WAF Rulesによって緩和される攻撃の一般的な指標として、HTTP異常があります。これには、不正なメソッド名、ヘッダー内のヌルバイト文字、標準でないポート、またはPOSTリクエストでのゼロのコンテンツ長などが含まれます。HTTP異常の例に関する詳細な説明は、Cloudflareのブログ（こちら）でご覧いただけます。

インジェクション攻撃**の種類は**以下の通りです。

- **コマンドインジェクション：**攻撃者が脆弱なアプリを介してホストオペレーティングシステムで任意のコマンドを実行する場合。
- **Cross-site scripting（XSS）：**XSSは、攻撃者がクライアント側のスクリプトをWebアプリに挿入して、重要な情報に直接アクセスしたり、ユーザーになりすましたり、ユーザーをだまして重要な情報を開示させたりできる脆弱性です。
- **SQLインジェクション（SQLi）：**SQLiは、攻撃者がデータベースが検索クエリを実行する方法の脆弱性を悪用する方法です。攻撃者はSQLiを使用して、不正に情報へのアクセスを取得したり、ユーザー権限を変更したり新たに作成したり、機密データを操作したり破壊したりします。

HTTPリクエスト：Webブラウザやアプリなどのインターネット通信プラットフォームが、リソースを読み込むために必要な情報を要求する方法です。

軽減されたトラフィック： Cloudflareプラットフォームによって「終了」とされた任意のHTTP*リクエスト。これには、BLOCK、CHALLENGE（キャプチャやJavaScriptベースのチャレンジなど）などのアクションが含まれます。これには、LOG、SKIP、ALLOWのアクションが適用されたリクエストは含まれません。

レート制限：コンピューターシステムでリクエストが処理される速度を制御するために使用される技術です。これはAPI攻撃を防ぐセキュリティ対策として、または配信元サーバーのリソース使用を制限するために使用できます。

リモートコード実行（RCE）：攻撃者が組織のコンピュータやネットワーク上で悪意のあるコードを実行することです。攻撃者が制御するコードの実行能力は、追加のマルウェアの展開や機密データの窃取など、さまざまな目的で使用される可能性があります。

スキーマの検証：API呼び出しがAPIのスキーマに従ったものでない場合、APIは機密情報を公開してしまうなど、予期しない方法で反応する可能性があります。スキーマの検証を有効にすることで、APIがそのようなリクエストを拒否することができます。

Zero-day脆弱性：アプリケーションのメーカーが把握していない脆弱性で、修正プログラムが存在しないものです。攻撃者は、これらの脆弱性をできるだけ素早く悪用しようとします。

目次

HTTPステータスコードの説明

以下のステータスコード例（セクション8で説明した最も一般的なAPIエラー）は、CloudflareがHTTPレスポンスコードのインターネット標準トラックプロトコルの解釈の仕方を詳しく示すものです。標準化の状態と、このプロトコルのステータスの最新版「インターネット公式プロトコル規格」(STD 1)を参照してください。

429は、**リクエストが多すぎることを意味します。**指定された時間内にクライアントがサーバーに対して送信したリクエストが多すぎるとされています。これは一般的に「レート制限」として知られています。サーバーは、要求者が特定の期間後に再試行できるようにする情報を含んで応答する場合があります。

400は**不正なリクエスト**を意味します。クライアントが正しいリクエストをサーバーに送信していない場合です。これはクライアントエラーであり、不正なリクエスト構文、無効なリクエスト、メッセージのフレーミング、または欺瞞的なリクエストのルーティングが原因です。

404は**見つからなかったこと**を意味します。配信元サーバーが要求されたリソースを見つけることができなかったか、または見つけることを拒否しました。通常、これはホストサーバーがAPIのURLを認識しなかったことを意味し、これはさまざまな理由による可能性があります。

401は**認証されていないこと**を意味します。ユーザーの資格情報が存在しなかったか、または要求されたリソースに対する適切なアクセスレベルを含んでいなかったことを示します。

403は**アクセスが拒否されたこと**を意味します。Cloudflareは、リクエストがすべてのorange-clouded Cloudflareドメインで有効になっているデフォルトのWAF管理ルール、または特定のゾーンで有効になっているWAF管理ルールのいずれかに違反している場合、403レスポンスを提供します。Cloudflareのブランドがない403エラーが表示される場合、これはCloudflareではなく、常に配信元のWebサーバーから直接返されます。

500は**処理できないコンテンツ**を意味します。サーバー側の予期せぬエラーに対する一般的なエラーメッセージ。

422は**処理できないコンテンツ**を意味します。リクエストには意味論的なエラーがありました。

503は**サービスが利用できないこと**を意味します。サーバーはメンテナンス中であるか、オリジンのWebサーバーが過負荷である可能性があります。

430は**リクエストヘッダーフィールドが大きすぎること**を意味します。このエラーコードは公式ではありませんが、Shopifyはリクエストが悪意がある可能性があり、Shopifyがそれを拒否してアプリを可能な攻撃から保護するために応答したことを意味します。

402は**支払いが必要なこと**を意味します。広く使用されていませんが、一部のプラットフォームでは、日々の制限が超えられた場合や支払いに問題があった場合に使用されることがあります。

巻末注

1. Cloudflareのグローバルネットワークは、平均で毎秒5,000万件のHTTPリクエストに対応しており、ピーク時には毎秒7,000万件以上のHTTPリクエストを処理しています。2022年10月1日から2023年8月31日までの間、Cloudflareの動的HTTPトラフィックにおいて、成功応答（ステータスコード200）を示すAPIトラフィックは、53.1%から60.1%の範囲でした。動的コンテンツとは、訪問時間、場所、デバイスなど、ユーザー固有の要因に基づいて変化するコンテンツのことです。
2. REST APIエンドポイントについては、CloudflareのAPI Discoveryは、アカウントごとに、すべてのクライアントのドメイン/ゾーンにわたって、クライアントから提供されたセッション識別子を通じて発見したエンドポイントよりも、機械学習を通じて発見したエンドポイントの方が中央値で30.7%多くなりました（260対199）。
3. 2022年10月1日から2023年8月31日までのAPI（ダイナミックキャッシュステータス）の全HTTPエラーに占める、最も一般的な2xx以外のHTTPステータスコード（4xxおよび5xxエラーを含む）の割合に基づきます。
4. 軽減されたAPIトラフィックを計算するために、CloudflareはCloudflare製品のソースごとに、軽減されたAPIトラフィックの日ごとの割合とを計算しました。また、Webアプリケーションファイアウォール（WAF）のルールカテゴリごとに、管理ルールによって軽減されたトラフィックの日ごとの割合を計算しました。
5. APIトラフィックが業界全体の動的HTTPトラフィックの70%以上を占める上位の業界（組織のSalesforce業界カテゴリごと）。
6. 北米、ヨーロッパ、中南米、オセアニア、アジア、アフリカ、中東のAPIトラフィックで、Cloudflareのネットワークで処理されたすべての動的HTTPトラフィックのうち、成功（200）レスポンスコードを返したトラフィックの割合に基づきます。
7. Cloudflareには、セッション識別子を含むトラフィックを調べる方法と、セッション識別子を必要としない機械学習ベースのディスカバリーエンジンを使用する方法の2つのAPIディスカバリー方法があります。機械学習によってのみ発見されたエンドポイントを持つアカウントは15,431件でした。
8. アカウントごとのAPI数を集計し、書き込みアクセス（PUT、POST、PATCH、DELETE）と「情報のみ」（GET）アクセスのエンドポイント別に分類しています。このレポートの目的のために、CloudflareはGET APIが各クライアントのAPI総数の少なくとも50%を占めるアカウントの割合を計算しました。
9. APIトラフィックに基づき、Cloudflare WAFマネージドルールカテゴリに従ってクライアント向けに軽減されます
10. クライアントの国地域内で200レスポンスコードとダイナミックキャッシュを返したAPI呼び出し数（ダイナミックキャッシュを持つ全200のレスポンスコードトラフィックのうち）から算出した、1日あたりのAPIパーセンテージの中央値に基づいています。
11. 全世界の1日あたりのAPIトラフィックのベースライン（平均）と比較した、1日あたりのAPIトラフィックの変化率に基づいています。
12. 他の業界と比較したその業界の総ダイナミックHTTPトラフィックに基づいています。ここでの"業界"は、クライアントアカウントのSalesforceの業界カテゴリによって定義されています。

メール：enterprise@cloudflare.com

訪問先：www.cloudflare.com/ja-jp/

REV:BDES-5122.2024年1月4日