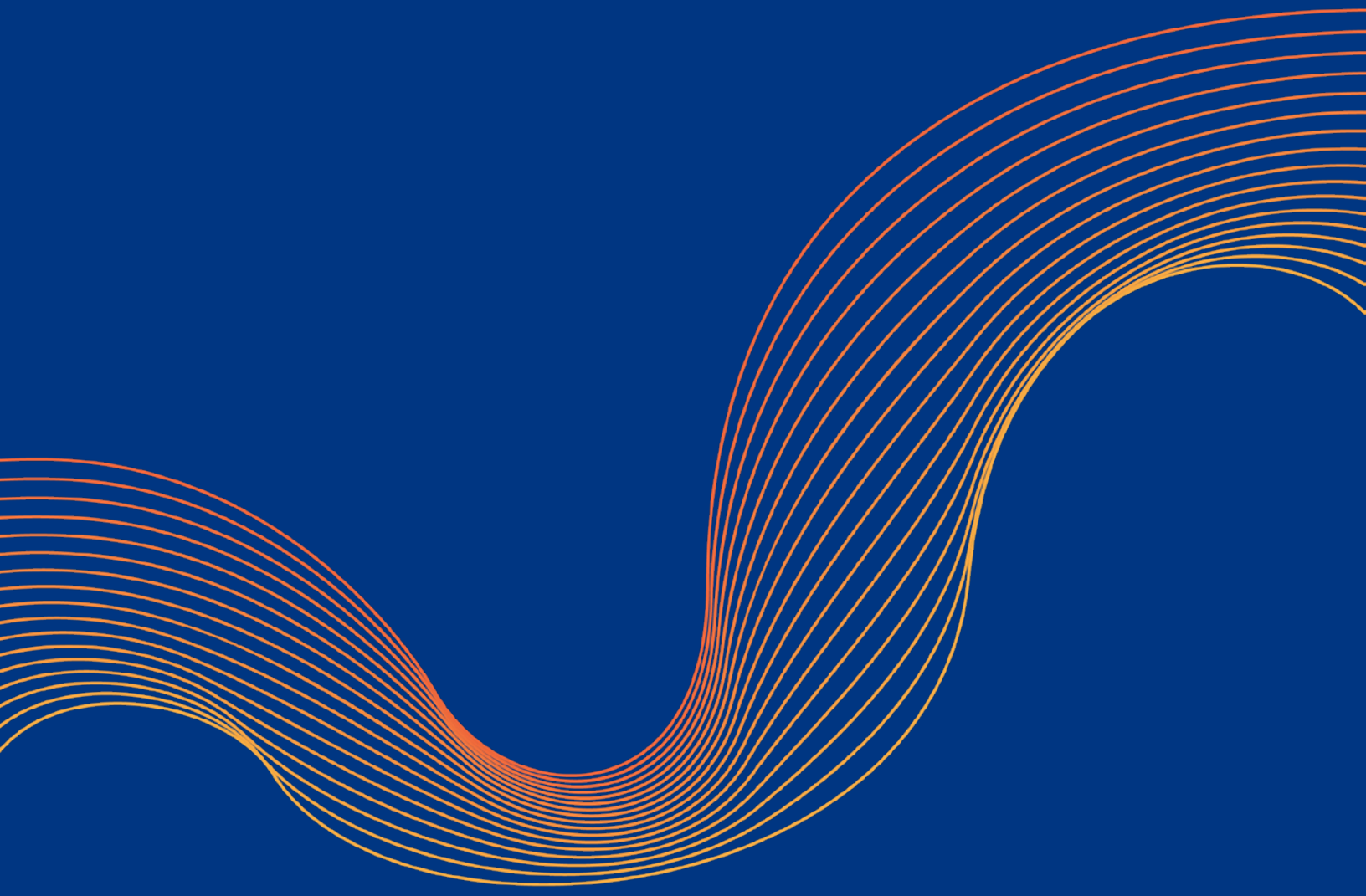
CLOUDFLARE

効果的なアプリケーションセキュリティには、包括的で迅速かつ継続的な保護が必要



03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com/ja-jp/

目次

はじめに

アプリケーションセキュリティの脅威は常に存在しています。2020 年に米国国家脆弱性データベース（NVD）が 18,000 件を超える脆弱性を報告し、それまでの記録を更新しました。恐ろしいことに、そのうちの 10,000 件以上が「致命的」または「極めて深刻な」脆弱性と評価されています。

また、攻撃者はよく知られた脆弱性を悪用し続けています。米国のサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）、連邦捜査局（FBI）、英国の国家サイバーセキュリティセンター（NCSC）、オーストラリアサイバーセキュリティセンター（ACSC）による共同調査で、2020 年（から 2021 年にかけて）攻撃者に最も悪用された脆弱性の上位 30 件はよく知られた脆弱性で、そのすべてに利用可能なパッチがあったことがわかっています。

企業はソフトウェアにパッチをあてようと試みるでしょうが、こうした既知の脆弱性によるセキュリティリスクは後を絶ちません。さらに悪いことに、不正利用される前に企業が脆弱性にパッチの適用を試みるとしても平均で 16 日かかります。この間、アプリケーションは攻撃にさらされたままです。

残念ながら、アプリケーションの所有者が抱えるセキュリティ関係の懸念材料は、ネイティブな脆弱性だけではありません。API が独自のリスクをもたらします。Cloudflare ネットワークのデータから、リクエストの 50% は API に関係することがわかっています。しかも、ボットはインターネットトラフィックの 40% を占め、ボット攻撃対策が極めて重要になっています。さらに、多くのサイトが依存するサードパーティコードを通じて、アプリケーションがサプライチェーン攻撃にさらされるのです。

可能性のあるすべての攻撃からアプリケーションを保護するために、複数の製品やソリューションが利用できますが、それらを個別に採用すると、アプリケーションセキュリティはたちまち断片化され、複雑化してしまいます。そこで有用なのが、包括的なアプリケーションセキュリティ戦略の実装です。効果的なアプリケーションセキュリティ戦略は、数多くのリスクから包括的かつ迅速に、継続的に保護するものでなくてはなりません。

アプリケーションセキュリティの問題についての概観

アプリケーションの所有者が早急に対処すべきセキュリティ問題：

アプリケーションの脆弱性

アプリケーション内の脆弱性は非常によくあることです。Veracode による最近のソフトウェアセキュリティレポートによると、83% のアプリケーションに少なくとも 1 つのセキュリティの欠陥があり、複数の欠陥があるアプリケーションも数多いことがわかっています。さらに、この調査の対象となったアプリケーションの 20% 以上に、少なくとも 1 つの重大な欠陥が見つかっています。

API 攻撃

アプリケーションの機能は、アプリケーションプログラミングインターフェース（API）にますます依存するようになっています。Gartner の最近の見通しでは、「低頻度の攻撃ベクトルだった API の悪用が、2022 年までに最も高頻度の攻撃ベクトルになり、その結果、エンタープライズ Web アプリケーションのデータ漏えいが発生する[1]」としています。

[1] Gartner は、「低頻度の攻撃ベクトルだった API の悪用が、2022 年までに最も高頻度の攻撃ベクトルになり、その結果、エンタープライズ Web アプリケーションのデータ漏えいが発生する」と予測しています。出典：Gartner「API セキュリティ：API を保護するために必要な対策」、報告者：Mark O'Neill、Dioniso Zumerle、Jeremy D'Hoinne、2021 年 3 月 1 日（閲覧には Gartner のサブスクリプションが必要です）

ボット攻撃

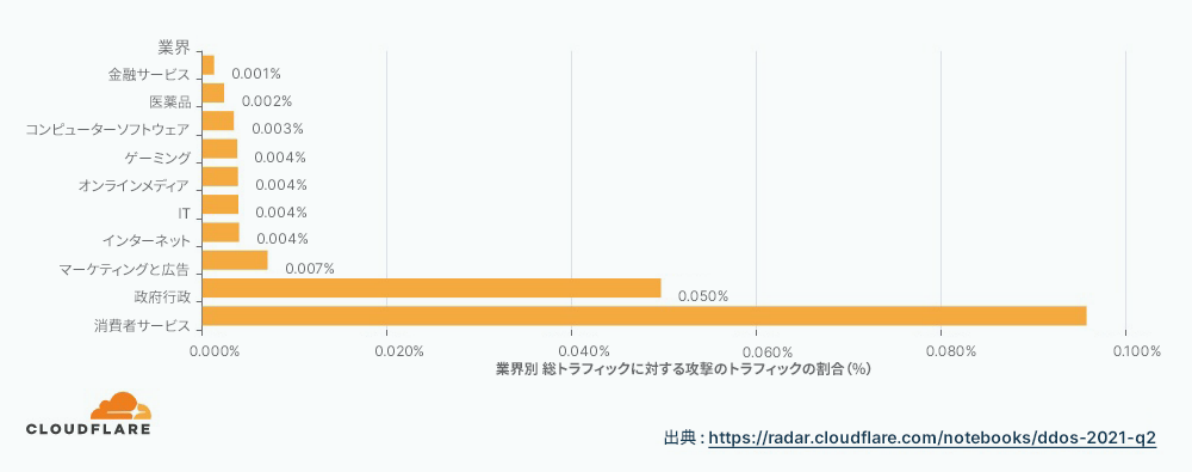
ボット攻撃もよく発生しています。攻撃者はボットネットと呼ばれる感染したデバイスのネットワークを使用して、悪意を持ってさまざまな行動をとります。その一例がクレデンシャルスタッフィングがあり、何百、何千という数の盗まれた資格情報をボットがログインページに「詰め込み」、アカウントへのアクセス権を得ようとします。ボットはコンテンツスクレイピング攻撃にも使われます。この攻撃では、ボットはサイトのコンテンツをダウンロードして複製し、検索エンジン最適化（SEO）の利点を盗もうとします。

サプライチェーン攻撃

サプライチェーン攻撃では、攻撃者は外部ソース（信頼するベンダーのソフトウェア、サードパーティ Web サイトとの依存関係、サプライヤーなど）を通じてエントリーポイントを見つけます。2015 年には、Magecart と呼ばれるグループが一連の攻撃を仕掛け、標的サイトとサードパーティとの依存関係を悪意のあるコードでウィルス感染させ、e コマース Web サイトから支払い情報を盗み出しました。感染した依存関係を含むページをエンドユーザーのブラウザが読み込む際に、攻撃者が Web ページから情報を盗み、販売するのです。つまり、サードパーティとの連携は、それがベンダーであろうと Web サイトの依存関係であろうと、攻撃対象領域を大きく広げることになりかねないということです。

DDoS 攻撃

DDoS 攻撃では、攻撃者は大量のジャンクトラフィックを使って、アプリケーションをオフラインに陥れようとします。厄介なことに、DDoS 攻撃は絶えず規模やベクトルなどを変化させており、DDoS 攻撃は衰えることを知りません。Cloudflare ネットワークのデータから、2021 年第 2 四半期に米国の組織に向けて送信された HTTP リクエストは、200 件につき 1 件の割合で、DDoS 攻撃の一部であったことがわかっています。



パス上（On-Path）攻撃

アプリケーションは、パス上 (On-Path) 攻撃の餌食にもなります。攻撃者は、（ブラウザとサーバーのような）2 者間のコミュニケーションを悪意ある目的のために傍受します。攻撃者は当事者のどちらかになりすまし、コミュニケーション内容を改ざんしたり、機密情報を集めたりします。パス上攻撃はいろいろな形をとります。たとえば、Domain Name System（DNS）サーバーや、メールサーバーを攻撃対象にしたりします。DNS パス上攻撃では、攻撃者は DNS ルックアッププロセスを傍受し、ユーザーを別の（通常は不正な）Web サイトにアクセスさせます。同様に、メールハイジャックでは、攻撃者はメールサーバーと Web の接続を傍受し、メールを読んでメールコミュニケーションを妨害します。

Web アプリケーションの脅威から保護するためのベストプラクティス

こういったタイプの攻撃に対する防御を、各企業のアプリケーションセキュリティ戦略に組み込むべきです。ただし、どう防御するかも重要で、高度なアプリケーションセキュリティ戦略は以下のような性質を持っています。

- **クラウドエッジネットワークベース：**かつては、Web アプリケーションへの脅威に対してはオンプレミスの保護対策が標準でしたが、このアプローチは拡張が困難です。たとえば、アプリケーションがハードウェアベースの WAF で保護されている場合、保護を拡張するには追加のハードウェアを購入するしか方法がありません。ハードウェアベースの保護を増強するには長期間を要する可能性があり、その間アプリケーションは脆弱なままです。クラウドベースのソリューションならこの問題はありません。容量をいつでも増やせるため、保護の拡張にも制限がありません。

  容量の制約に加えて、オンプレミスの保護には、購入や維持に高額な費用がかかるという難点があります。ハードウェアは経年劣化が比較的速く、修理や交換の費用がかさみます。加えて、ハードウェアを管理するために訓練されたスタッフを雇うと、総所有コストがさらに高額になります。一方、クラウドベースのソリューションを使えば、所有コストを大幅に削減できます。

  クラウド配信ソリューションのもう 1 つの利点は、簡単に高頻度で自動更新できることです。これは Web アプリケーションファイアウォール（WAF）などのソリューションに特に有用です。クラウド配信であれば、ルールや軽減メカニズム、基盤となるソフトウェアを迅速に更新できるためです。一方、オンプレミスプロバイダーはソリューションの更新をリモートで行うことができますが、プロセスが複雑で、一般的には頻度も少なくなります。

  クラウドエッジネットワークは、これらの利点をさらに活かしたものです。クラウドエッジネットワークでは、地理的に分散されたサーバーグループで同じサービスを実行しています。エッジから保護することにより、組織はスケーラビリティというクラウドの利点を活かしつつ、集中型モデルにはないパフォーマンス面の優位も享受できます。

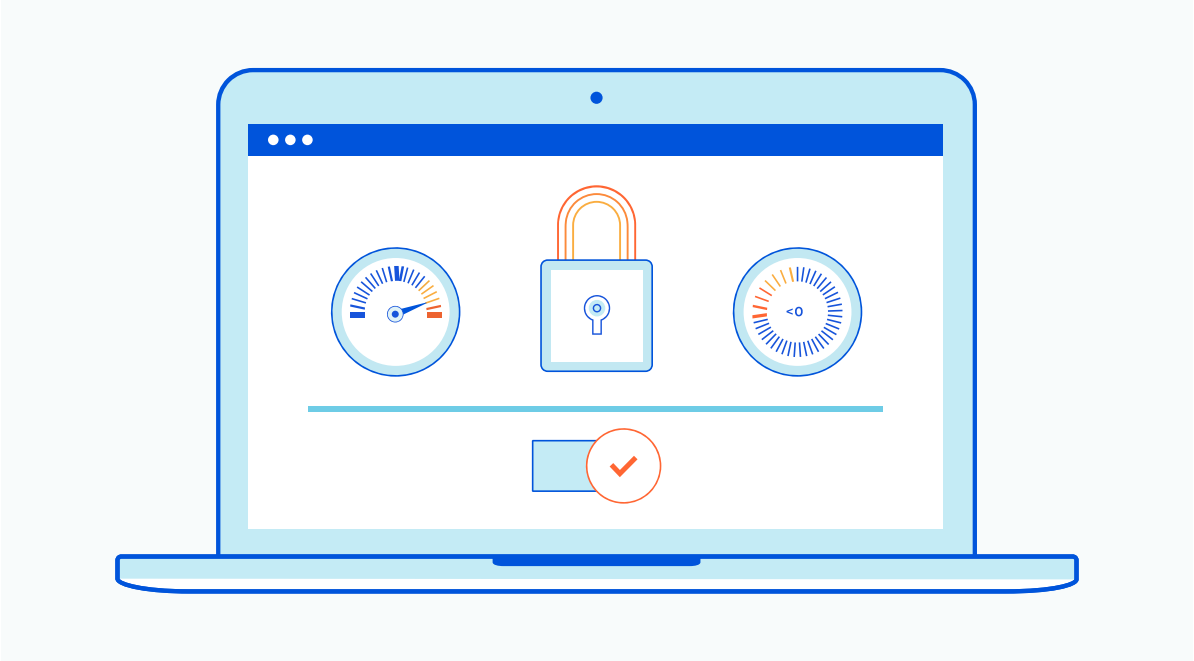
  クラウドエッジネットワークでは、エンドユーザーに可能な限り近い場所で保護を適用します。一方、集中型モデルでは、統合されたデータセンターで保護が適用され、世界中に分散するエンドユーザーからは遥かに遠くなります。セキュリティを提供するには、ユーザーの居場所にかかわらず、すべてのユーザートラフィックを、セキュリティ機器を備えた中央のデータセンターにバックホール（中継）しなければなりません。たとえば、データセンターがカリフォルニア州にあってエンドユーザーがニューヨークにいる場合、トラフィックはいったんカリフォルニアのデータセンターに送信され、そこからユーザーにバックホールする形になります。

- **統合型：**複数のツールで一貫性のある保護を適用しようとすると、エラーの余地が生まれます。そのため、攻撃から防御するには、1 つの統合システムを使う方が、複数のツールをつなぎ合わせて使うよりも良いのです。

  チームで別個のツールを使用すると、各人が別々のセキュリティ製品を管理することになり勝ちです。このため、重要な情報がより広く共有されずに、セキュリティのサイロ化（孤立化）が起こり、インフォメーションギャップが生じかねません。加えて、ツールすべてにそれぞれ設定・管理が必要なため、チームの負担が増え、余計に複雑になってしまいます。

  さらに、ツールが多すぎるとアラートすべてを解析することが困難になります。各ツールにはアラートの発動に関する独自のルールとロジックがあり、ツールの数が多いと、どのアラートが本当に重要なのかがわからなくなってしまいます。

  一方、統合型システムを使えば、チームの扱うツール数は少なくなり、アラートも集約化されるため、何に注意を払う必要があるのかを簡単に把握できます。統合型のツールは整合性のあるポリシーを参照することが多く、ポリシーをグローバルに適用しやすくなります。たとえば、アプリケーションの所有者が、データ損失防止（DLP）ルールを一度設定すれば、WAD、API、その他のアプリケーションツールに同じルールを自動的に適用することができます。

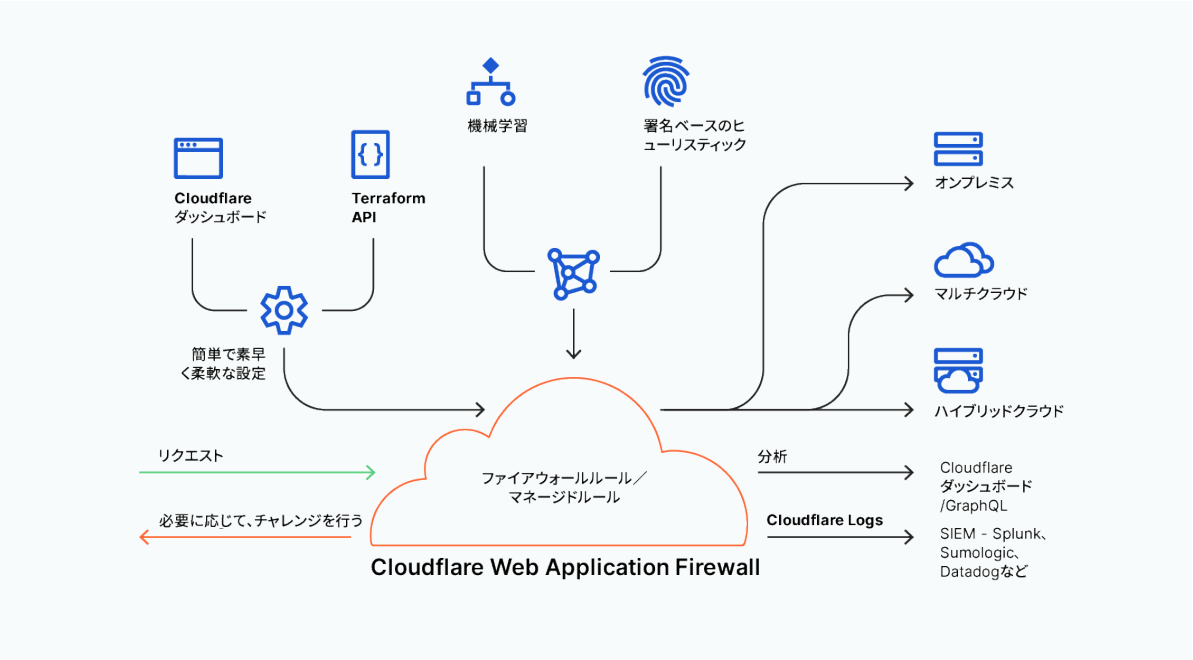


攻撃タイプごとに特化した戦略

アプリケーションが直面するセキュリティリスクは何種類にも及ぶため、保護にも複数の種類が必要です。以下では、アプリケーションの所有者が使える各攻撃タイプに特化した戦略をいくつか説明します。

アプリケーションの脆弱性

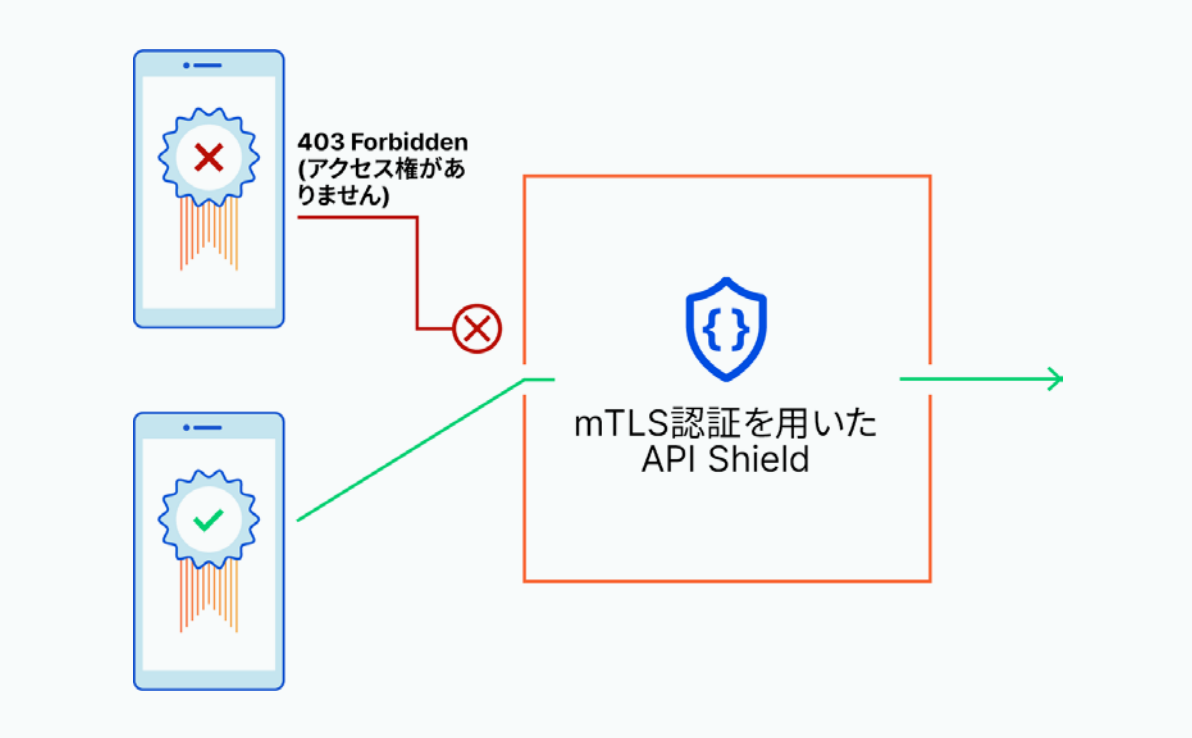
WAF：WAF はアプリケーションの脆弱性を悪用する攻撃を防止するのに最適な方法の 1 つです。WAF は既知の攻撃の手口に関するセキュリティルールセットを使って、悪意のあるトラフィックをフィルタリングし、攻撃を防止します。事前設定されたルールと、ルール変更をすばやくデプロイできるカスマタイズオプションがある WAF が、最も効果的です。これらの機能が多くの WAF が抱える二大問題（誤検知とルール変更のデプロイメントの遅さ）を軽減するためです。誤検知は、WAF ルールが意図せずに正当な Web トラフィックをブロックすることをいいます。一部の WAF では複雑なルール設定手順を踏む必要があるため、正確かつ最新のリストを維持し、正当なトラフィックのブロックを解除することが難しくなっています。マネージドルールやカスタムルールに加えて OWASP ルールセットを提供する WAF であれば、誤検知の頻度が減ります。しかし、これらの新ルールをデプロイするまでに長い時間を要すると、その間アプリケーションは攻撃に対して脆弱になります。



データ損失防止（DLP）：DLP はデータ流出（組織から許可なくデータが持ち出されること）を防止するための戦略です。DLP のツールやソリューションはアプリケーションや API 活動をモニタリングし、流出の可能性を特定して実際に流出が起こる前に阻止します。DLP は送信トラフィックを検査し、既知のデータタイプと比較して、ブロックすべきデータ流出かどうかを判断します。たとえば、DLP ツールは文字列をユーザー名として識別できます。組織が設定したルールに基づいて、アクティビティにフラグ付けしたり、アクティビティを阻止したり続行させたりすることができます。一部の DLP ツールは、ユーザータイプによってアクセスレベルを制限するロールベースアクセス制御（RBAC）と統合でき、組織内やアプリケーション内のデータ移動がさらに安全なものになります。

API のセキュリティリスク

スキーマ検証とポジティブセキュリティモデル：API スキーマは、API とやりとりを行う際に想定される動作を記述した取り決めです。スキーマは、API と連携する際にユーザーが行ってもよいことについて基本原則を設定しています。OpenAPI（Swagger）は、最も一般的なスキーマフォーマットです。スキーマは、ポジティブな API セキュリティを適用するのに適したテンプレートです。ポジティブセキュリティモデルは、スキーマと照合してリクエストを検証し、スキーマに準拠するリクエストだけを許可し、悪用や潜在的な攻撃を防止します。「ブロックせよと指示されたもの以外のリクエストはすべて許可する」がデフォルト設定になっているネガティブセキュリティモデルよりも厳格です。



認証と承認：認証（API リクエストが正当なものであることの確認）と承認（エンドポイントまたはクライアントがどのレベルのアクセス権を有するかの確認）も、API セキュリティの重要な側面です。API リクエストの認証方法や承認方法はたくさんあります。たとえば、相互トランスポートレイヤーセキュリティ（mTLS）では、クライアントとサーバーの両方が認証証明書を持ち、お互いの ID を検証するために使用します。

API ディスカバリ：「シャドー」API とは、セキュリティチームが気づいていない可能性のある API のことです。セキュリティチームが監視していないため、シャドー API はデータ漏えいにつながったり、コンプライアンス基準を満たしていないかもしれません。API ディスカバリツールは、より良い API 管理のために、エンドポイントを監視し、シャドー API を検出します。

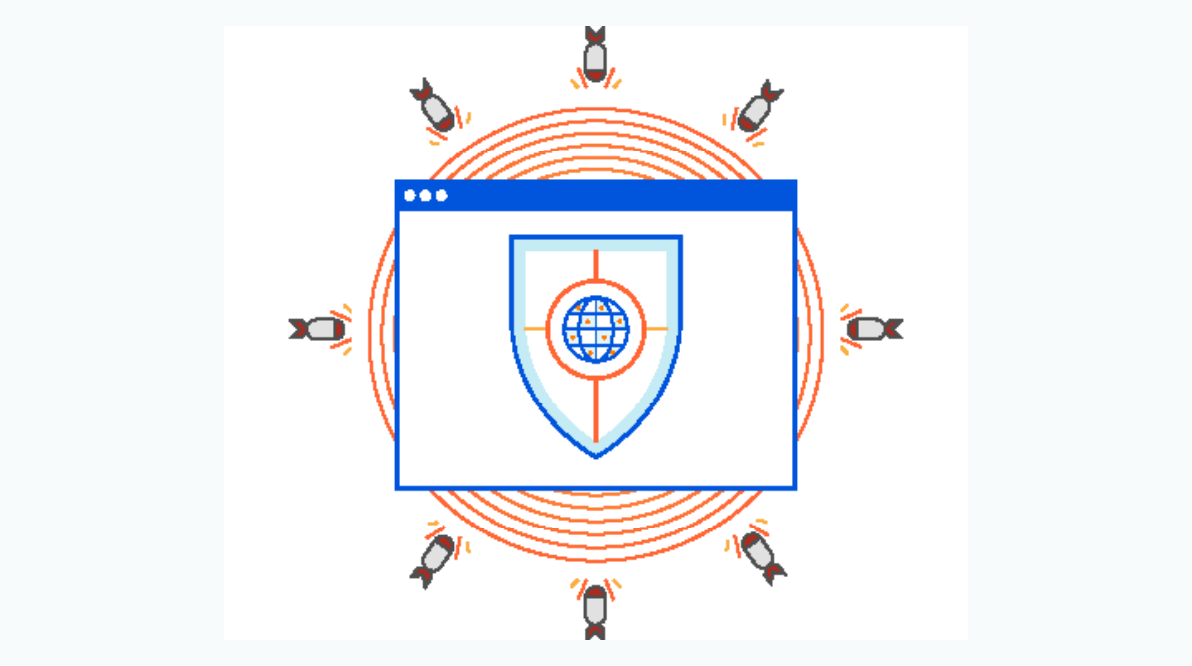
DLP：データの流出は、旧来型のアプリケーションだけでなく API でも起こり得ます。DLP ツールで API の送信トラフィックを監視し、API 応答の中に潜在的な機密データがあれば、検出・ブロックすることができます。

悪意のあるボット

ボットトラフィックの管理では、良性のボットをブロックしないで、悪性のボットを検出・ブロックすることが必要です。SEO サイトクローラーのような良性のボットは、重要なビジネス指標を把握するために必要です。一方、悪性ボットはアプリケーションにクレデンシャルスタッフィング、コンテンツスパム、その他の攻撃を仕掛け、大問題を引き起こしかねません。ボット管理ソリューションでは、トラフィックを分析して、ボット活動を検出し、良性 / 悪性を判断し、ブロックまたは許可します。効果的にボットを管理するためには、高度な検出方法と、ボット活動の傾向を時系列で分析・把握する能力、そして、そのデータに基づいてボットブロックのルールをカスタマイズするための柔軟性が必要です。

DDoS 攻撃

DDoS 攻撃に対する効果的な防御とは、軽減までの時間を最適化し、セキュリティのためにパフォーマンスを犠牲にしないことです。軽減までの時間を減らす方法の 1 つは、DDoS 攻撃対策をオンデマンドの発動ではなく常時稼働にしておくことです。オンデマンドの保護とは異なり、常時稼働の DDoS 軽減対策では、トラフィックが特定の閾値に到達するのを待って保護を開始するのではありません。すべてのトラフィックがフィルタリングされ、軽減がより迅速に行われます。エッジから DDoS 軽減を適用することで、アプリケーション所有者はパフォーマンスとセキュリティを享受できます。攻撃の発生場所を問わず、事前に決められた場所で対策を行う集中型の保護とは異なり、DDoS 軽減は攻撃の発生元にできるだけ近い場所で行うため、パフォーマンスが向上します。



サードパーティーの脆弱性

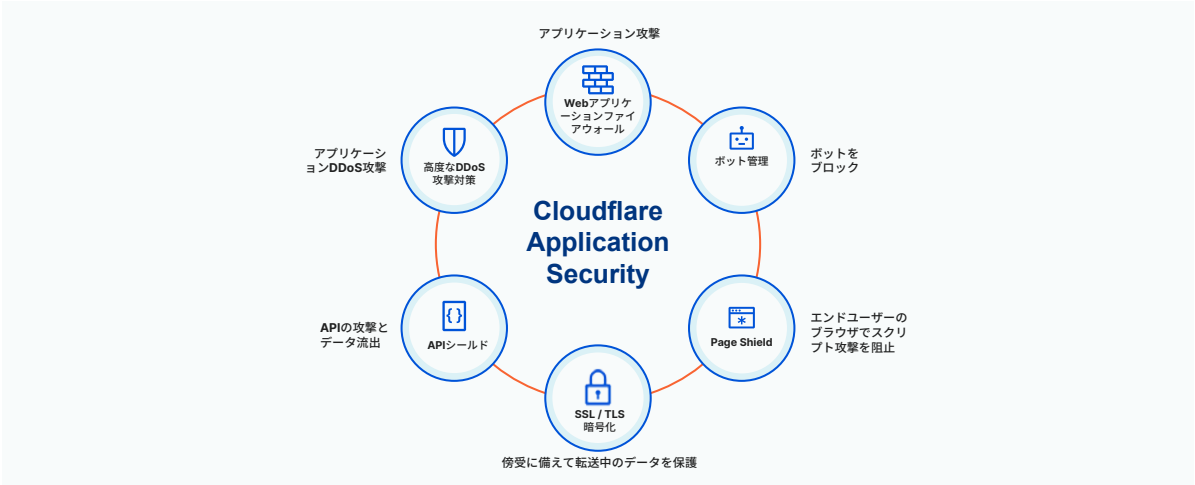
クライアント側のセキュリティソリューション：多くのサイトがサードパーティーに依存しているにも関わらず、その依存関係について頻繁に監視しないため、サプライチェーン攻撃に対して脆弱になり得ます。クライアント側のセキュリティでは、アクティビティはユーザー側（通常はブラウザ）で保護されます。クライアント側のセキュリティは、サードパーティとの依存関係の変化を監視し、コード変更の性質を調査することによって、サプライチェーン攻撃から保護します。たとえば、コンテンツセキュリティポリシー（CSP）技術は、承認されたリソースのリストを使って、リストに記載のないリソースの実行をすべてブロックします。しかし、CSP 技術の欠点は、動的ではないことです。許可リストに記載されているリソースの安全性が損なわれ、悪意のあるものに変わっても、CSP では感知してブロックすることができません。幸いなことに、クライアント側セキュリティサービスのなかには CSP のメリットを活かして構築されているものもあります。一部のツールは、新しい JavaScript の依存関係を追跡することができ、サイトオーナーに警告して調査を促すことができます。同様に、一部のサービスでは、サイト上で JavaScript を配信している既知の悪意ある URL を検出したり、検出したスクリプトの変更について調査するようサイトオーナーに警告することができます。

パス上（On-Path）攻撃

パス上攻撃に対する防御では暗号化が鍵になります。セキュアソケッツレイヤー（SSL）/ トランスポートレイヤーセキュリティ（TLS）の暗号化は、HTTP トラフィックを保護する最善の方法の 1 つです。TLS はデータを暗号化し、そのデータを交換する当事者を認証し、データが改ざんされていないことを検証します。このプロセスが Web サービスとエンドユーザーの交信を保護し、パス上攻撃を阻止します。しかし、中には SSL/TLS をかいくぐる攻撃者がいます。その際に役に立つのが、HTTP ストリクトトランスポートセキュリティ（HSTS）です。HSTS は攻撃者からの非セキュアな接続すべてをブロックし、パス上攻撃からのエンドユーザー保護を強化します。

Cloudflare でアプリケーションを外部の脅威から保護

Cloudflare で、外部の脅威からアプリケーションを保護できます。Cloudflare のエッジネットワークは 100 か国、200 都市以上に広がっており、何百万ものインターネットプロパティを、DDoS 攻撃、アプリケーションの脆弱性、悪意のあるボット、API の悪用などから保護しています。すべての Cloudflare セキュリティサービスが、Cloudflare ネットワークの全サーバー上で実行されており、すべて同一の優れたグローバル脅威インテリジェンスを利用しています。



Cloudflare のアプリケーションセキュリティサービスには以下のものが含まれます。

- **アプリケーションの脆弱性**
  - **WAF：**Cloudflare WAF は、階層化されたルールセットを提供します。これは、(1) 管理されたルールセット（最新の攻撃に反応して定期的に更新される）、(2) コアとなるルールセット（OWASP Top 10 に基づく）、(3) カスタムルール（お客様が数秒で設定・デプロイできる）から構成されています。Cloudflare WAF は、Cloudflare Bot Management や API Shield と同じ Rust ベースのルールエンジンで稼働し、一貫性のある保護を提供します。
- **API のリスク**
  - **API シールド：**Cloudflare API Shield は、クライアント証明書とスキーマベースの検証によって API を守ります。API Shield は、mTLS を使用して、API へのアクセスを試みるデバイスやクライアントを検証し、DLP に照らして送信トラフィックをスキャンしたりします。
    - **DLP：**Cloudflare では、API 向けの DLP 機能も提供しています。この機能を使用すると、API キーやクレジットカード情報などの機密データを含む応答を API でブロックすることができます。Cloudflare の DLP 機能は API だけでなく、たとえば、アプリケーションやデバイスも保護することができます。
- **サードパーティの脆弱性ーブラウザサプライチェーン攻撃**
  - **Page Shield：**Cloudflare Page Shield の一部である、Script Monitor では、サイトの JavaScript の依存関係を経時的に記録し、依存関係に変化があったり新しい依存関係が出現した際に、調査するよう組織に警告します。
- **ボット攻撃**
  - **ボット管理：**Cloudflare Bot Management は、機械学習、挙動分析、グローバルデータの活用によって、悪性ボットをブロックします。Bot Analytics を使ってトラフィックパターンを把握でき、カスタムルールと許可リストによってアクセスの詳細設定が可能です。
- **DDoS 攻撃**
  - **DDoS：**1 日あたり平均 870 億件の脅威をブロックする 90 Tbps のネットワークを活かし、Cloudflare DDoS 軽減は、エッジで最大規模の攻撃から保護します。
- **暗号化**
  - **Cloudflare Free SSL/TLS：**Cloudflare の無料 SSL/TLS を利用すると、Web トラフィックを暗号化してアプリケーションを保護することができます。Cloudflare SSL は HSTS プロトコルもサポートしており、防御をさらに強化することができます。

詳細については https://www.cloudflare.com/ja-jp/security/ をご覧ください。