

Cloudflareセキュリティサービス

Cloudflareセキュリティサービスは、サービス拒否攻撃、顧客データ侵害、不正なボットなどからインターネットアプリケーションを保護し、安全を確保します。



DDoS攻撃を軽減

ネットワーク層とアプリケーション層を対象とする悪意のあるトラフィックからインターネットアプリケーションを保護して可用性とパフォーマンスを維持し、その一方で営業費用を抑えます。

サービス

- エニーキャストネットワーク
- IPレピュテーションデータベース
- ヒューリスティックベースの緩和
- Webアプリケーションファイアウォール (WAF)
- Rate Limiting
- DNS
- Cloudflare Spectrum
- Argo Tunnel

DDoS攻撃

攻撃トラフィックが可用性やパフォーマンスに影響を及ぼす



顧客データ漏えいを防止

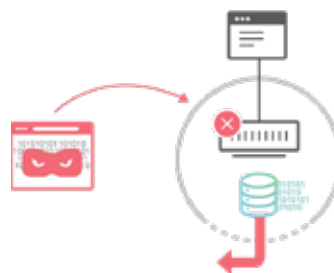
ユーザー資格情報、クレジットカード情報、およびその他の個人識別情報など、攻撃者が敏感な顧客データを侵害するのを防ぎます。

サービス

- Webアプリケーションファイアウォール (WAF)
- Rate Limiting
- DNS
- SSL / TLS 1.3
- Spectrum

データ窃盗試行

機密性の高い顧客データの侵害



悪意のあるボット乱用をブロック

コンテンツスクレイピング、不正なチェックアウト、アカウントの乗っ取りなど、悪質なボットによるインターネットの財産への被害を阻止する。

サービス

- IPレピュテーションデータベース
- Webアプリケーションファイアウォール (WAF)
- Rate Limiting

ボット

悪意のあるサイトまたはアプリケーションからボットが悪用されるのを防ぐ



Cloudflare セキュリティサービス



グローバルな エニーキャストネットワーク

Cloudflareのグローバルなエニーキャストネットワークは、正当なトラフィックスパイクや不正なトラフィックスパイクや攻撃を吸収して、Webサイト、アプリケーション、またはAPIの表面積を広げます。

ユースケース:
DDoS攻撃

IPレピュテーションデータベース

何百万ものIPを持つCloudflareのIPレピュテーションデータベースは、リアルタイムのフィードバックを伴うデータ主導のセキュリティ層と動的レピュテーションスコアリングを採用することで、効果的なセキュリティインテリジェンスを提供します。

ユースケース:
DDoS攻撃
悪意のあるボット乱用をブロック

DNS

Cloudflare DNSはドメイン解決のためのDDoS保護です。これは、サービス拒否攻撃から700万以上のインターネットプロパティを保護するのと同じ、30 Tbpsネットワークの背後に位置します。DNSSECは、認証を提供することによってDNSの上に信頼層を追加します。

ユースケース:
DDoS攻撃
顧客データ漏えいを防ぐ

Webアプリケーション ファイアウォール (WAF)

CloudflareのエンタープライズクラスのWebアプリケーションファイアウォール (WAF) は、OWASP Top 10、Cloudflare内蔵アプリケーション、カスタム作成されたルールセット、アプリケーション固有のルールセット、カスタムルールセットを適用して、Cloudflareネットワークエッジでアプリケーション層の一般的な脆弱性を検出し、ブロックします。

ユースケース:
DDoS攻撃
顧客データ漏えいを防ぐ
悪意のあるボット乱用をブロック

Rate Limiting

CloudflareのDDoSソリューションはネットワークやアプリケーションに対する帯域幅消費型攻撃から自動的に保護しますが、顧客によっては、容量が少ないものの悪意のあるトラフィックから自社のシステムを保護するためにコントロールを構成する必要があります。Rate Limitingは不審なリクエストレートの訪問者を微細なコントロールでブロックまたは識別し、重要なリソースを保護します。

ユースケース:
DDoS攻撃
顧客データ漏えいを防ぐ
悪意のあるボット乱用をブロック

SSL / TLS 1.3

Transport Security Layer (TLS) 暗号化は、訪問者と配信元サーバー間のHTTPS接続を確立し、中間者攻撃、パケットスニффリング、Webブラウザーに表示される信頼性の警告などを防止します。

ユースケース:
顧客データ漏えいを防ぐ

Argo Tunnel

Cloudflareはパブリック受信ポートを開かずに、最も近いデータセンターとアプリケーションの配信元サーバー間に暗号化されたトンネルを作成します。

ユースケース:
DDoS攻撃
顧客データ漏えいを防ぐ

Cloudflare Spectrum

SpectrumではCloudflareのエニーキャストネットワークを通るWebトラフィック以外のトラフィックにプロキシ処理を行うことにより、TCPアプリケーションおよびポートを帯域幅消費型DDoS攻撃やデータ窃盗から保護します。

ユースケース:
DDoS攻撃
顧客データ漏えいを防ぐ

Cloudflareの 利点



Cloudflareの180か所以上のデータセンターで結ばれ、30 Tbpsの容量を備えるエニーキャストネットワークでは、これまでに記録された最大のDDoS攻撃の15倍の帯域幅消費型攻撃を防御できます。Cloudflareは世界中のHTTPインターネットトラフィックの10%である、1日あたり300億件を超えるリクエストを監視して、自社のネットワークを利用する800万人の顧客を対象とした攻撃を学習することで、脅威に対する防御を積極的に行っています。



Cloudflareの設定は、わずか5分で完了します。使いやすいCloudflareを導入することで、企業はより多くの従業員にインターネットセキュリティポリシーの責任を広げ、新しいポリシーの展開時間を短縮し、複雑なアプリケーションのセキュリティに対する取り組みをタイムリーに調整できるようになります。



Cloudflareを使用すると、セキュリティのためにパフォーマンスを犠牲にする必要はなくなり、Cloudflareのセキュリティ機能は、トラフィック高速化と統合されたレイテンシーの短いセキュリティサービスであるため、パフォーマンスを低下させるのではなく、アプリケーションパフォーマンスを向上