



# DDoS 攻撃は ゼロ秒 で阻止できるでしょうか？

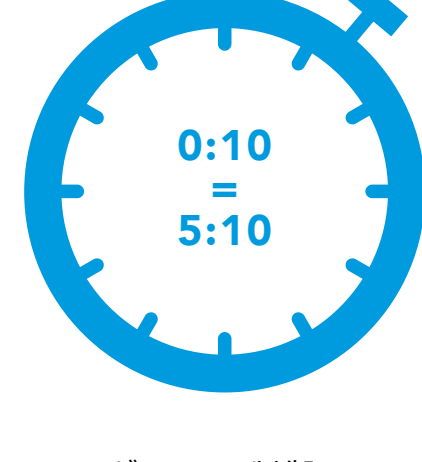
**緩和所要時間 (TTM) とは何かを明確にすることが重要です。**

TTMの意味は限定されるべきではないでしょうか？つまり、DDoS 攻撃が開始してから、アセットやアプリケーションが保護されるまでに要する時間です。

しかし実際には、ベンダーのサービスレベル契約 (SLA) では、そうなってはいません。時間の測定がいつ開始して停止するかを正確に理解する必要があります。

## 一般的なベンダーのシナリオ例

### ベンダー A



ベンダー A の制御では、DDoS 攻撃であることが確定するまで、トラフィックの急増を 5 分以上分析する必要があります。

10 秒の TTM SLA は、攻撃だと確定した後で開始されます。

### ベンダー B



ベンダー B の契約条件では、緩和制御の導入までの時間 (応答) として緩和所要時間 (TTM) を定義しています。

攻撃阻止を確約する SLA はありません。

### ベンダー C



ベンダー C は、TTM SLA において自動での検知と緩和を確約しています。

高度な攻撃を阻止するための手動によるカスタマイズされた防御手法は、その SLA には含まれません。

## 契約条件についての理解

次のような言葉にご注意ください。

... 応答時間...

... 検知後...

持続的な DDoS 攻撃の場合 ...

## AKAMAI の緩和所要時間



## ゼロとはゼロ秒を意味します

Akamai の事前対応型の緩和制御は、お客様が攻撃を受けていることに気付く前に、DDoS 攻撃を破棄するように設計されています。それが Akamai Intelligent Edge Platform の威力です。

攻撃検知までの時間 + 緩和制御適用までの時間 + 攻撃阻止までの時間 = 業界トップクラスの緩和所要時間

## 8 つの DDOS 緩和ステップ

Akamai は、脅威リサーチャー、インシデントマネージャー、セキュリティアーキテクト、最先端の防御テクノロジーの強力な組み合わせにより、業界で最速の TTM を実現しています。Akamai の Security Operations Command Center (SOCC) は、次のステップを実行します。

- Always-on の DDoS 監視により、攻撃を早期に検知します。
- 確立されたランブックを使用してお客様に警告します。
- Always-on のスムーズなルーティングでお客様のトラフィックを管理します。
- トラフィックを分析し、緩和を適用するベクトルを特定します。
- 適用された緩和策を微調整して、フォールス・ポジティブ (誤検知) とフォールス・ネガティブ (検知漏れ) のバランスを最適化します。
- 新しい攻撃ベクトルを特定します。
- トラフィックを分析して新たなベクトルを特定し、継続して緩和策を適用します。
- 適用される緩和策を最適化して、変化する攻撃を無効化します。

## TTM 遅延によるリスク

## ダウンタイムの影響はどのようなものですか？

**0:01**

1 秒で Web 上のアセットやアプリケーションが使用できなくなります。

**0:10**

10 秒でお客様のフリクションが高まり、従業員の生産性が低下します。

**5:00**

5 分でブランドの評判が傷つき、収益が失われます。

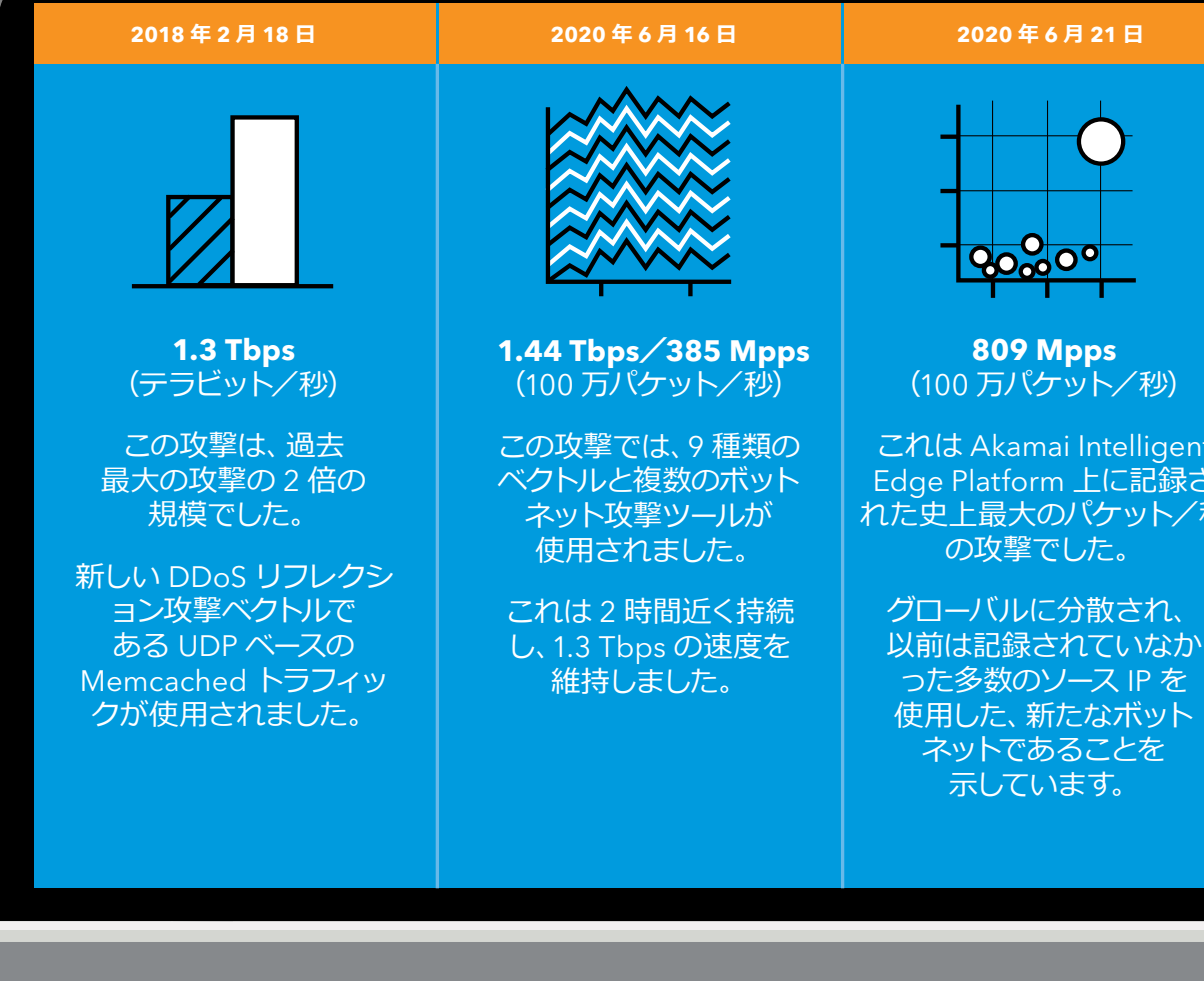
## 貴社の DDOS 対策を評価

- 貴社のベンダーは攻撃をどのくらい迅速に検知できますか？
- 貴社のクリティカルなアプリケーションの可用性は確保されますか？
- 巻き添え被害を受けますか？
- 正規ユーザーは影響を受けますか？
- 貴社のベンダーはどのくらい迅速に緩和対策を適用できますか？
- 貴社のベンダーはトラフィックの分析をどのくらい迅速に開始できますか？

## AKAMAI の脅威に関する知見

### ますます規模、複雑さ、危険性が增大

DDoS 攻撃が記録的な規模にまで増大しています。2020 年には、ますます大規模で複雑な DDoS アクティビティが観察され、攻撃ベクトルの数と組み合わせは過去最大となっています。



効果的な防御には、実績のあるプラットフォーム、経験豊富なスタッフ、洗練されたプロセスと手法の組み合わせが必要です。

緩和所要時間とは、正規のトラフィックやユーザーに影響を与えることなく、どれだけ迅速に悪性トラフィックを特定してブロックするかを意味します。

最終的には、ミッションクリティカルなアプリケーション、インフラ、ブランドの評判を保護することが真の成功の尺度となります。

## 今すぐ DDOS 防御を強化

Akamai がゼロ秒緩和を実現する方法をご確認ください。

[詳細はこちら](#)



Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範囲に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、ウェブ/モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比較のないカスタマーサービスと分拆、365 日/24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com、blogs.akamai.com および Twitter の @Akamai でご紹介しています。全事業所の連絡先情報は、www.akamai.com/locations をご覧ください。

公開日：2020 年 11 月