Akamai Webinar Report

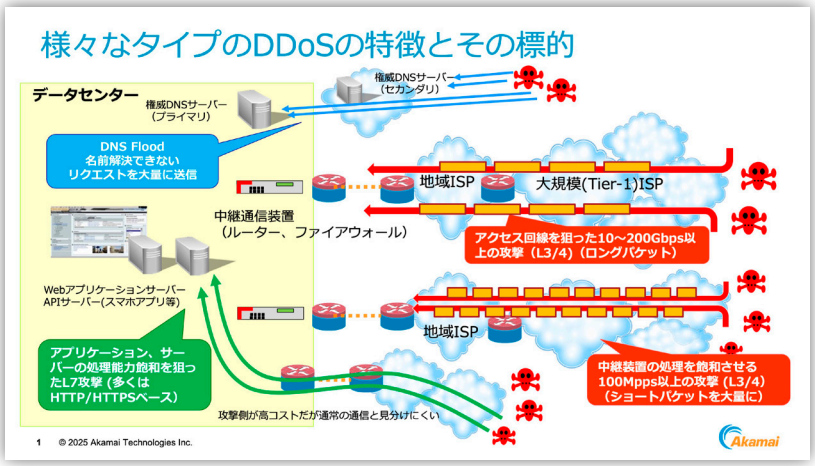
大規模化・複合化するDDoS攻撃

― 対策強化のベストプラクティス

既存の対策の隙を狙う複合型DDoS攻撃の拡大

2024年末から2025年初頭にかけて、日本国内では金融、交通、通信など社会基盤を支える重要インフラ事業者がDDoS攻撃の被害を受けました。これらの攻撃は単発的な愉快犯によるものではなく、継続的で組織的な攻撃の特徴があります。

近年のDDoS攻撃は多様化しており、主に3つのタイプに分類されます。1つは権威DNSサーバーを標的とするDNSフラッド攻撃、次にアクセス回線やネットワーク中継装置を狙った大量トラフィックによるレイヤー3/4攻撃、そしてWebサーバーやAPIサーバーの処理能力を枯渇させるレイヤー7攻撃です。Akamaiの観測によれば、今回の攻撃ではこれらの手法が複合的に用いられました。



攻撃者は、用意されたDDoS対策の隙を巧みに付こうと、レイヤー3/4DDoS（SYN/Ack/UDP/GRE Floodなど）とレイヤー7DDoS（HTTP/HTTPS）攻撃ベクトルを巧妙に変化させてきたため、自動的な緩和措置だけでは十分ではなく、専門家による追加的な緩和戦略が必要でした。攻撃規模は数十Gbpsから数百Gbpsに及び、国内事業者向けのDDoSとしては過去最大規模となりました。

注目すべきは、CDNの緩和策を回避するための、IPアドレス直打ちによるオリジンサーバーへの直接攻撃が頻発したことです。攻撃者はサブネットのIPを総当たりする手法も用い、システム構成情報を事前調査した形跡が見られました。攻撃ソースは世界中に分散していましたが、一部の攻撃に共通するTLS

Fingerprintパターンが観測されたため、同一の攻撃ツールが使用されていた可能性が高いと考えられます。

さらに2024年10月から12月にかけて、オーストラリア／ニュージーランド地域でも日本と類似の攻撃が発生しました。攻撃ベクトルの類似性や一部IPの一致など共通点が見られ、組織的で継続的な攻撃キャンペーンである可能性があります。

三層構造のDDoS対策強化で新たな脅威に備える

これら最新のDDoS攻撃が成功した主な要因としては、次の3つが挙げられます。1つ目はWAFやCDNによる保護のないWeb/APIサーバーが狙われたこと。2つ目は、Web/APIサーバー以外の公開システム（ファイアウォール、ルーター、ロードバランサーなど）が狙われたこと。3つ目は、既存のDDoS対策のしきい値以下で大規模な分散環境から攻撃を仕掛けられたことです。

このような複合的かつ高度なDDoS攻撃に対応するためには、多層防御アプローチが不可欠です。そこでAkamaiは、次のような三層構造からなるDDoS対策のベストプラクティスを提案しています。この手法を採用することで、自社のサービスひいてはビジネスを強固に保護できるようになります。

具体的には、まず権威DNSに対する水責めDDoSやランダムサブドメイン攻撃から保護する第一の防御層。次に、レイヤー3/4 DDoSおよびレイヤー7 DDoSに対処してオリジンへの負荷を軽減するCDNベースの第二の防御層。さらに第三の防御層で、CDNの緩和策を回避するIPアドレス直打ちによるオリジンへの攻撃に対しても有効な対策を講じます。

Akamaiを活用してビジネスを守る事前準備のポイント

すでに多くの日本企業が、Akamaiのサービスを積極的に活用し、ビジネスやブランドの保護に乗り出しています。たとえば全日本空輸（ANA）では、高度なリアルタイム性と信頼性が求められるシステムへのアクセスを保護し、旅客サービスの安定稼働を実現しています。重要なエネルギーインフラを担う関西電力では、企業システムと制御系ネットワークの境界を含む広範な領域において、ゼロダウンタイムを見据えたセキュリティ強化を進めています。

このような対策強化には、プロフェッショナルの視点が欠かせません。いずれのユーザー企業も「Akamaiの高品質なサポートが重要な役割を果たした」と評価しています。

大規模なサイバー攻撃は今後も継続すると予想されており、いっそう激しい攻撃に備えたリスク対策の強化が求められます。あらゆる日本企業がベストプラクティスに基づいた対策を進め、国内のDDoS対策レベルを底上げしていくことが必要です。

世界中で毎日DDoSを緩和しているAkamaiでは
そのノウハウを活かしてお客様ごとの環境を踏まえた
対策強化を提案できます。
こちらまでご相談ください。
https://www.akamai.com/ja/why-akamai/contact-us/contact-sales

2003年以来、Akamai は当社にとって非常に大切な存在です。長年にわたり当社のビジネスをサポートしていただいていることに感謝しています。

和田昭弘氏
全日本空輸 デジタル変革室
専門部長（サイバーセキュリティ）

Akamaiの丁寧なサポートを受けてセキュリティ強化を推進し、強力なWAF･DDoS対策を導入できました。運用を支援するサービスが充実しており、少人数での管理でも無理なく効果的な対策を講じられています。

江渕誠氏
関西電力株式会社
IT戦略室 サイバーセキュリティグループ　チーフマネジャー