## 重要な知見

**34%**

**金融サービス機関で発生したレイヤー 3 および 4 の DDoS 攻撃イベントの割合**

金融サービスは依然として、レイヤー 3 および 4 の分散型サービス妨害（DDoS）攻撃イベントが最も頻繁に発生している業界です。ゲーム業界（18%）とハイテク業界（15%）がそれに続きます。この脅威が蔓延している原因は、継続的な地政学的緊張関係（特にイスラエル・ハマス紛争とロシア・ウクライナ戦争）により、世界各地でハクティビストの活動が急増したことであると考えられます。

**API の増加が、レイヤー 7 DDoS 攻撃の増加を招く**

Web アプリケーションは従来、サイバー攻撃の主要な標的となってきましたが、この調査期間中に API に対するレイヤー 7 DDoS 攻撃が著しく増加しました。これは主に、変化するコンプライアンス要件と規制要件を満たすために、金融サービスで API の導入が拡大していることに起因します。組織が API への依存を強めているのに合わせて、攻撃者は戦術を適応させているため、API セキュリティは現代の企業にとって極めて重要な優先事項となっています。

**トラフィックの急増は、DDoS を頻度と規模で評価する必要があることを示す**

金融サービスに対する DDoS 攻撃から、重要な知見が得られます。それは、イベントの頻度と攻撃の強度が必ずしも相関するとは限らないということです。攻撃がほとんど見られなかった期間が数か月ありましたが、その期間の Gbps データはトラフィックの急増を示しています。これは、DDoS 攻撃の影響を評価する際には攻撃の頻度と規模の両方を考慮する必要があることを強調しています。

**36%**

**金融機関を標的とする疑わしいドメインの割合**

金融サービスの顧客を標的とするフィッシング攻撃が増加しており、アイデンティティの窃取やアカウントの乗っ取りのリスクが増大しています。この攻撃トレンドにより、金融機関は規制当局からより厳しい目で見られるようになり、侵害が発生すれば顧客は信頼性に懸念を抱くこととなります。

**30%**

**フィッシングサイトやブランドなりすましサイトに誘導されたページ訪問の割合**

攻撃者は正規の金融サービス Web サイトやアプリを模倣し、トラフィックを不正なサイトへ誘導します。金融サービス機関が保有する膨大な量の機微な情報を取得するために、攻撃者は金融機関を標的としたフィッシングを行い続けています。