GCORE

WHITE PAPER

Gcore Radar

DDoS アタックトレンド

2024年 第1・第2四半期

2024年8月 | gcore.com

DDoS アタックトレンド 2024年第1・第2四半期

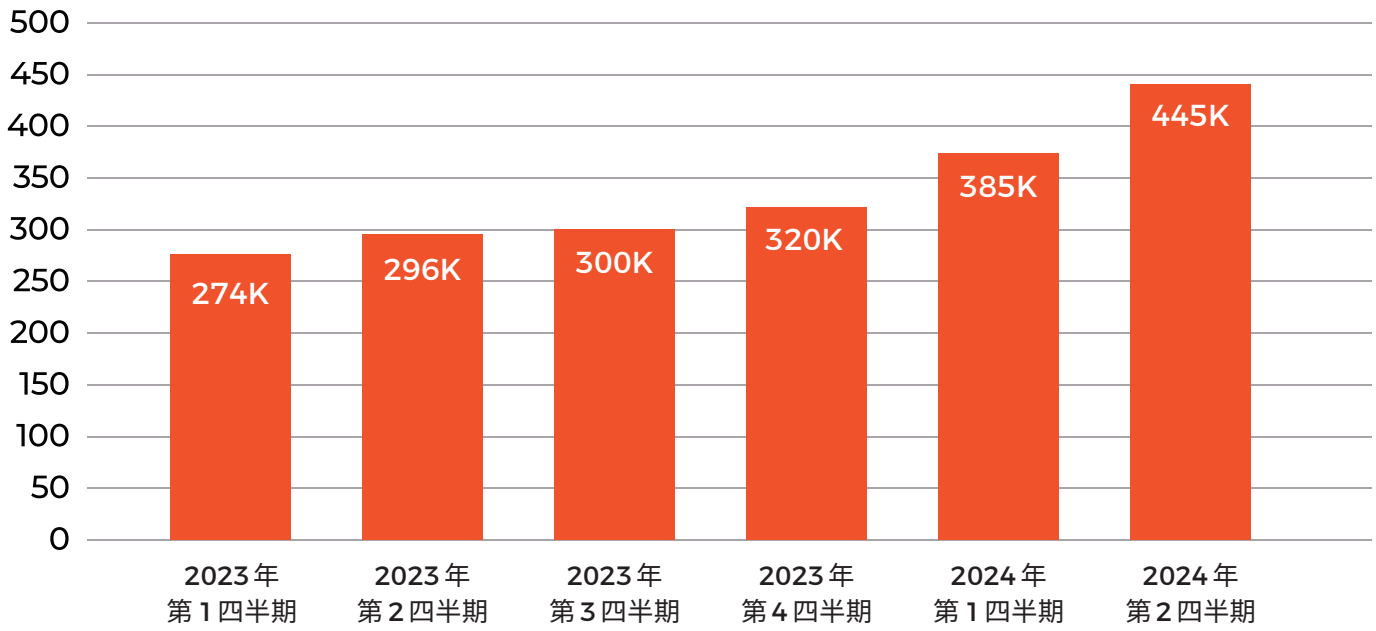
DDoS トレンドを追い続けることで、新興が止まない脅威に先行し、適格な防御戦略を採択することが可能だ。年2回の Gcore Radar Report で 過去半年間の DDoS 攻撃データを精査確認し、Gcore ネットワーク上で観測された攻撃者の行動の変遷と俯瞰で捉える攻撃の変化を可視化して把握する。

このレポートでは、業界別の分析で、どの業界が攻撃標的とされたか、どの 最多数を占めたのはどの DdoS 攻撃かについて詳細を提示。2024年上半期のデータと過去のデータを照合し、同行と攻撃パターンの方向性を抽出。

まず、2024年の第1四半期と第2四半期の顕著な動向について。

主要動向

増加する攻撃と回数



DDoS 攻撃回数は対前年同期（2023年上半期）比46%上昇。対前6ヶ月（2023年下半期）比34%上昇。

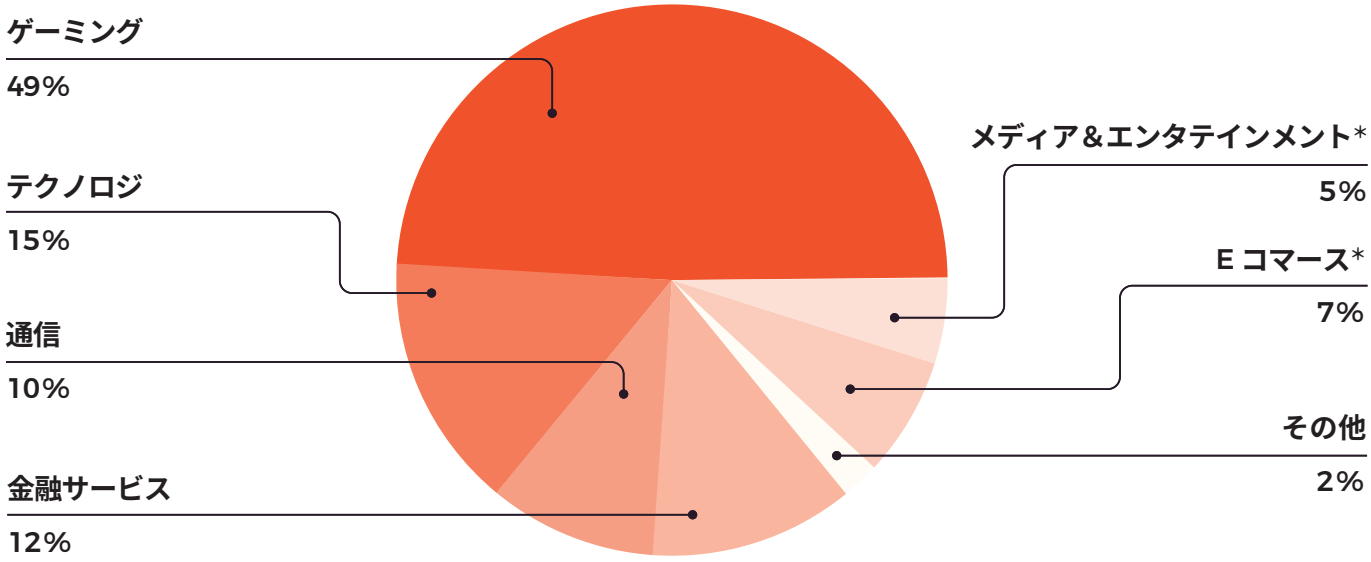
DDoS ピーク時攻撃力は依然急伸傾向

2023年下半期にはピーク時攻撃力が秒単位でギガビット（Gbps）からテラビット（Tbps）へと急増した。2024年下上半期の最強攻撃は1.7Tbps に達し、2023年下半期の1.6Tbps を上回った。2024年上半期での攻撃力増は0.1Tbps に留まったものの、ネットワーク、アプリケーション、デジタルサービスへの圧迫能力として判断すると、攻撃者側の力が増強している事実に他ならない。サービス完全停止、クリティカルなアプリケーションの破壊、財政上および企業評価への深刻な損害を与える脅威を有するのがテラビット級の攻撃だ。

攻撃対象とされた上位業界

攻撃対象の業界分布

＊2023 年第 3 四半期・第 4 四半期で
”その他” に分類されていた業界



ゲーミングが依然として最多攻撃対象

ゲーミングが標的最多業界で 2023 年下半期の 46%から 49%に上昇。オンラインゲーミングの競合指向性が、トーナメントや試合で競争相手に対する優位性を得ようとするプレイヤー、グループ、競合による DDoS 攻撃始動の誘発材料の一つとなってしまう。ゲームのマネタイズが、プレイヤーのゲーム内購入やサブ スクリプションで関与継続に依存するという側面も一因となる。ダウンタイムは収益に直接的な影響を及ぼすため、DDoS 攻撃側を潤わせるこの業界が格好の標的とされるのだ。

テクノロジ業界への攻撃増加

2023 年下半期から 2024 年上半期の差異の特徴として挙げられるのがテクノロジ業界への攻撃が大幅拡大したことだ。2023 年下半期の 7％から 2024 年上半期には 2 倍以上の 15％に達した。テクノロジプロバイダはビジネス企業向けに、サーバ、ストレージ、ネットワークリソースを含むクリティカルなインフラストラクチャをホストする業務を担う。このサービスを破壊することは、サービスを利用している多数の組織に甚大な影響を及ぼすことにつながる。つまり、破壊の広範な拡大を企図する攻撃者にとってテクノロジ業界を標的とすることが有効であり、その度合いが増しつつあることを示唆している。

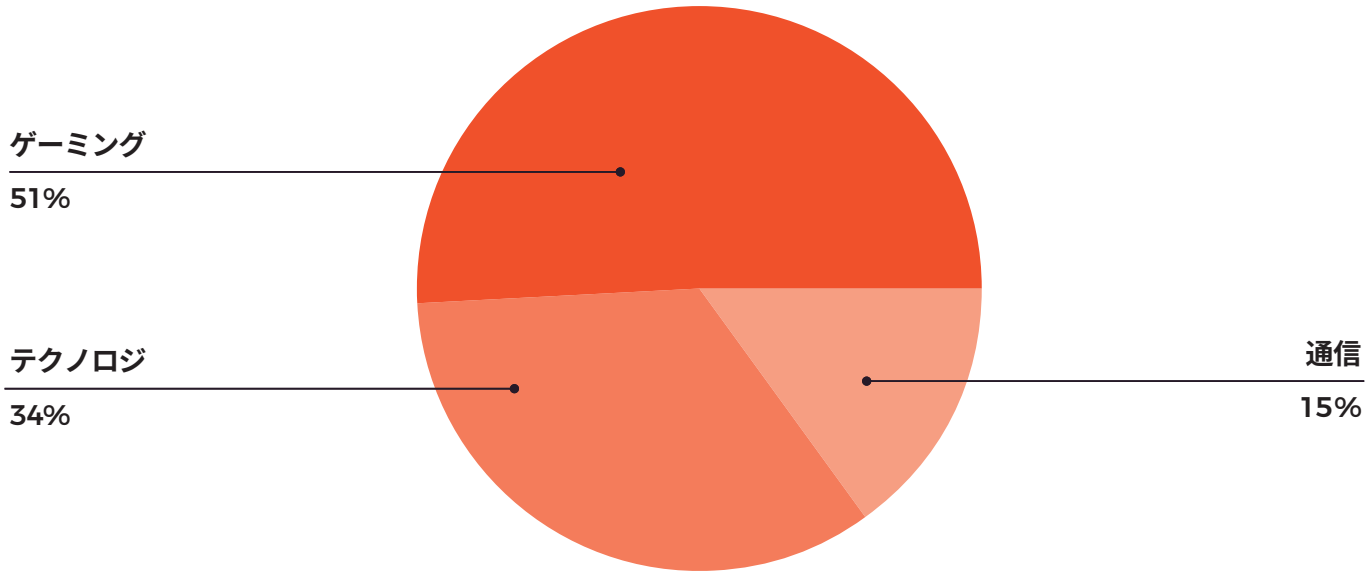
テクノロジプラットフォームを標的とする攻撃が蔓延しつつある理由のもう一つには、この業界の環境そのものがコンピュテーショナルリソースを実質的に包合しているという事実が挙げられ、この環境が DDoS 攻撃がこれらリソースを駆使して攻撃の増幅やマリシャス動作の促進の有効な土壌として使われる傾向にあるということだ。

上記以外で多数の標的とされた業界は、金融サービス (12%)、テレコム (10%)、E コマース (7%) だ。これらセクタへの攻撃が成功すれば財政面の見返りが高いということからすると何ら驚くことはない。

ネットワークレイヤ攻撃

ネットワークレイヤ DDoS 攻撃バイト数で47% を占めたゲーミング業界が最多対象となった。ゲーミング業界の高トラフィックボリューム、リアルタイム要件、競合ダイナミクス、金融および信用観点の膨大な利害関係（関与度合い？）が相互に作用しあうことがネットワークレイヤ DDoS 攻撃対象の最上位となる背景だ。攻撃者はこのセクタを有望視し続けるため、破壊・ダウンタイム・収益損失を回避するための DDoS 検知・緩和・プロテクションはゲーミング業界の最重要課題である。

ネットワークレイヤ（L3〜L4）攻撃対象上位３業界の対比分布



L3〜L4 レイヤでテクノロジは第２位、通信が第 3 位。テクノロジプラットフォームは多くの組織のビジネス上のクリティカル機能・サービスを支えるものだ。テクノロジ業界への破壊をしかけることで多数のビジネスとサービスへの影響を同時に及ぼし、その効果の余波の伝播が容易に可能になる。プロバイダにとどまらずその顧客にとっての甚大な経済損失につながる。この財政上の影響は、ランサムか容赦ないサボタージュかの攻撃手法を問わず攻撃者の動機となる。

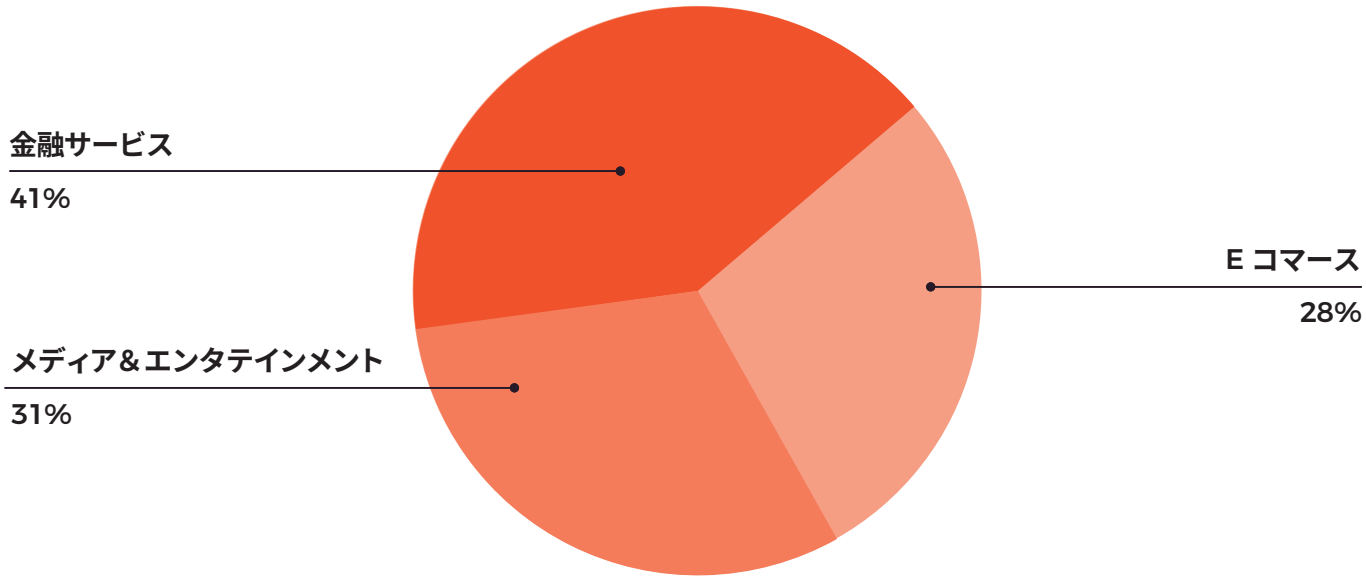
通信・テレコム企業はインターネット接続性と通信サービスの根幹部分を提供する。このサービスを破壊に伴う影響は多様かつ広範で、個々のユーザだけに留まらずビジネス企業体や組織機能の全体に影響を及ぼす。このプロバイダがサービスを提供する先は広範囲にわたり、個人コンシューマ、ビジネス企業、金融やヘルスケアのようなクリティカルなインフラストラクチャセクタを含み、この多様性に対し様々な攻撃者が様々な動機を持って攻撃をしかけるのだ。

アプリケーションレイヤ攻撃

金融業界はアプリケーションレイヤでの DDoS 攻撃の格好の標的となるが、その背景には破壊やダウンタイムに対する寛容度の低さと攻撃が成功した場合の高い報酬を見込めるためだ。

- 金融機関は極めて厳格な規制に準拠する必要がある。DDoS 攻撃に伴うダウンタイムやデータ侵害は深刻な規制違反につながる。
- アプリケーションレイヤでの DDoS 攻撃は IT スタッフを混乱に陥れ、フィッシング、不正取引、ハッキング他のマリシャス行為に気付かれない内に進行する結果を招く。

アプリケーションレイヤ（L7）攻撃対象上位３業界の対比分布



密な利害関係、取引の繊細性、規制要件、顧客からの信頼の維持の重大性が相互に作用するため、金融サービス＆銀行業界の L7 DDoS 攻撃への脆弱性と親和性は殊更高くなる。

次に標的となるのは E コマース業界で、アプリケーションレイヤ攻撃の28% を占める。E コマースは DDoS 攻撃にとっては魅力的な業界であるが、その理由は、ウェブサイトで頻繁に大容量トラフィックや大量取引が実行され、特にショッピングのピーク時には一層高まるからだ。このサービスを破壊することで財政損失と不利益を甚大なものにすることができる。

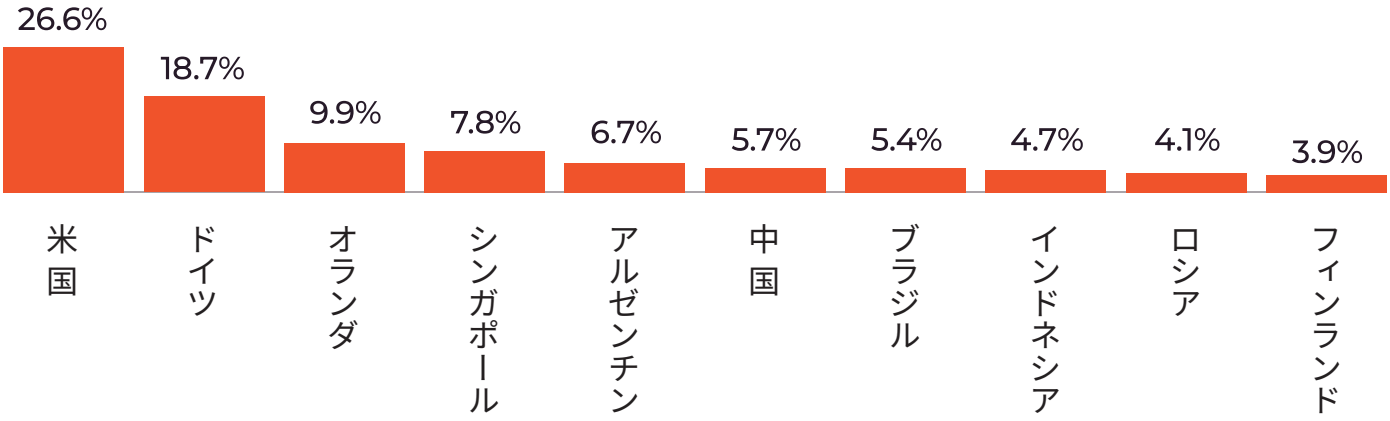
アプリケーションレイヤ（L7）での第３位にランクインしたのはメディア＆エンタテインメント業界で、その背景はこの業界の競合性に起因する破壊への寛容度の低さとカスタマからの期待値の高さだ。ストリーミングとコンテンツ配信を中断なく実施し続けるには、L7 プロテクション戦略の優先順位を高ることがメディア＆エンタテインメントサービスプロバイダに求められる。

DDoS 攻撃の主な発生源はどこか？

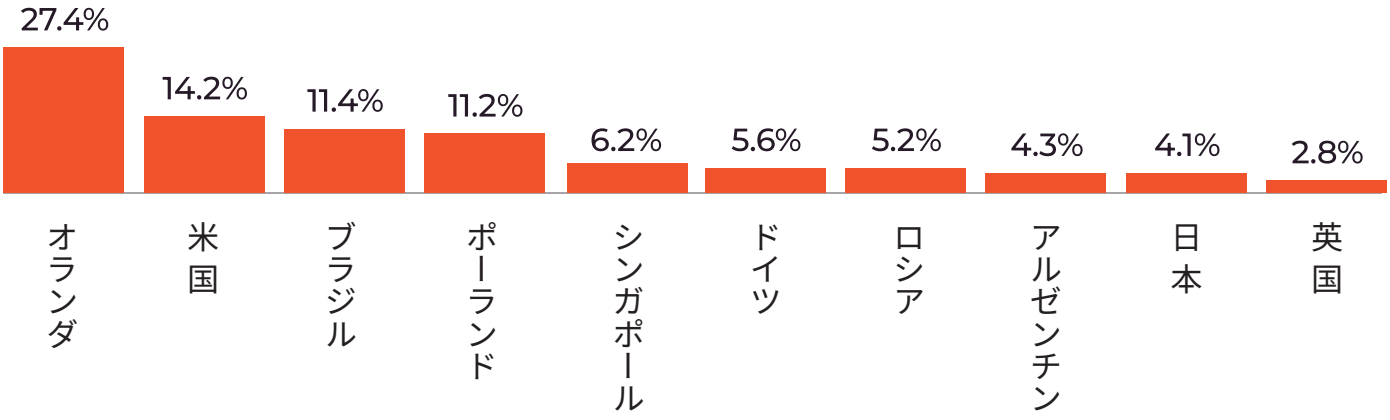
アプリケーションレイヤでの発生源の国の特定には攻撃者のIPアドレスを使用するが、これはIPアドレスは差し替えやごまかしが効かないからだ。ネットワークレイヤではソースIPアドレスが差し替えられてしまう。IPアドレスを辿って発生源を探るのではなく、攻撃パケットを受信したデータセンタ拠点を洗い出す手法を採用している。

Gcoreでは6大陸にわたるグローバル地域をカバーしており、地勢精度を持つ攻撃源の報告が可能だ。

ネットワークレイヤ攻撃 — 発生源の国別分布

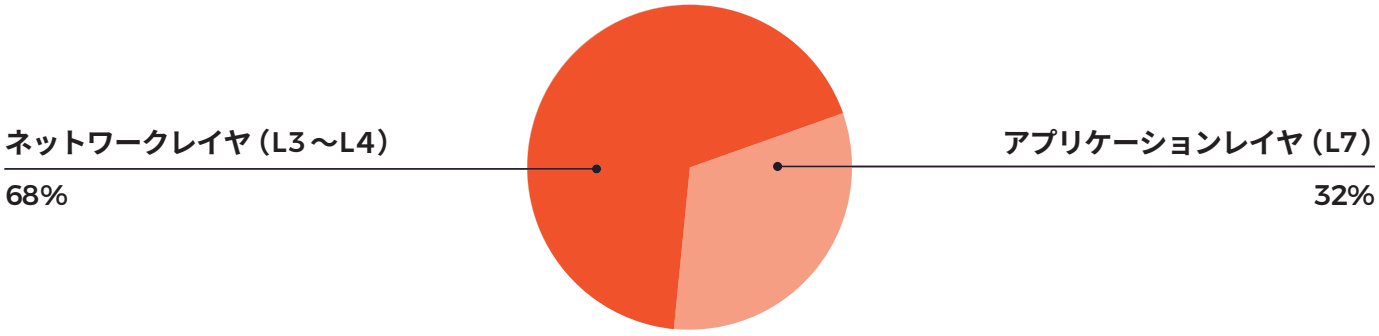


アプリケーションレイヤ攻撃 — 発生源の国別分布



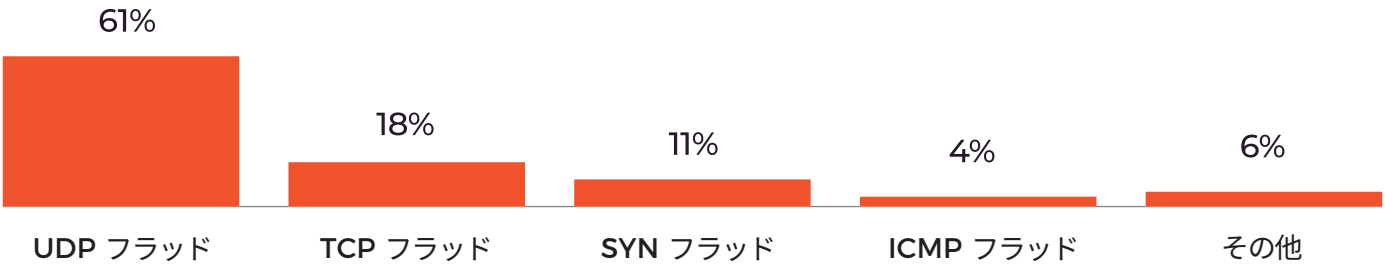
DDoS 攻撃タイプの分布

L3〜L4 と L7 の対比分布

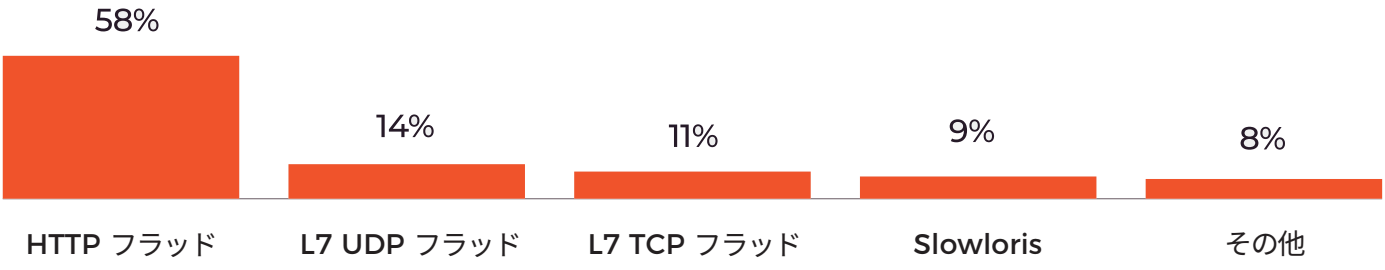


依然としてL3〜L4 レイヤ攻撃タイプの主流は UDP フラッドで、DDoS 攻撃の 61% を占めた。TCP および SYN フラッド攻撃も主流タイプであり、それぞれ全体の18% と11% を占めた。

ネットワークレイヤ攻撃ベクタ（L3〜L4）

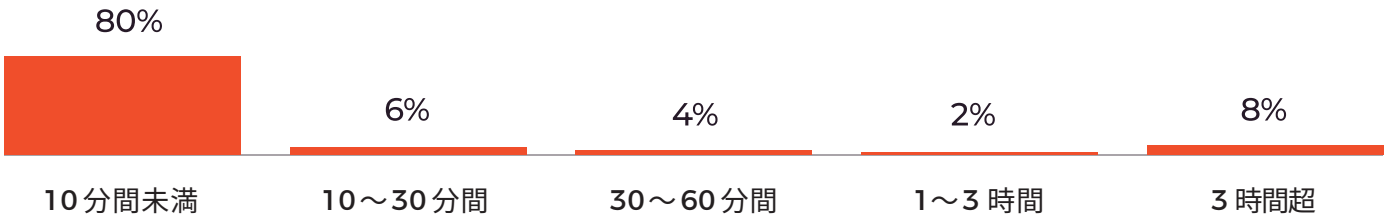


アプリケーションレイヤ攻撃ベクタ（L7）

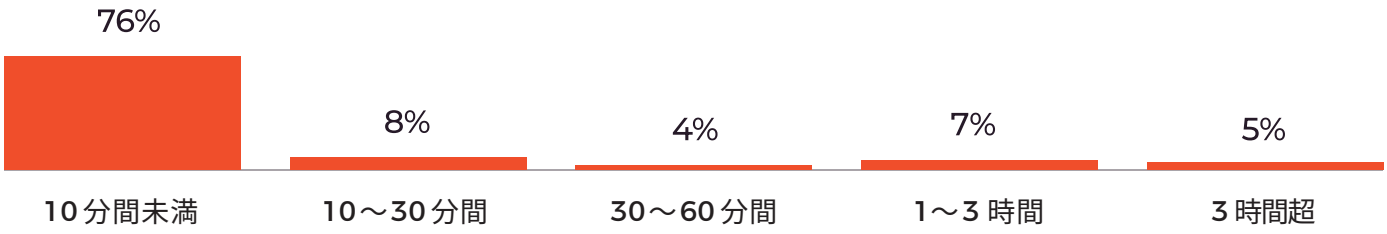


攻撃傾向は短時間かつ強大

ネットワークレイヤ攻撃持続時間



アプリケーションレイヤ攻撃持続時間



攻撃継続時間分析

2024年第1四半期・第２四半期の最長持続時間は16時間だが、上記グラフから見て取れるように平均的には攻撃時間は短い。ほとんどの攻撃は10分間以内－持続時間は分単位で測定－であるが、だからといって破壊力が抑制されるというものではない。

継続時間の如何に関わらず攻撃はユーザ体験とブランド評価に損害を与えるものであり、短時間であっても損害は相当高くつくのだ。

DDoS 攻撃は全世界共通の脅威、一方で攻撃のパーソナライズも進行

DDoS 攻撃はクリティカルなワールドワイド規模で頭痛の種であり、グローバル協働やインテリジェンスの交換共有で迅速な行動や攻撃が及ぼす影響の最小化が望まれる。

攻撃継続時間の変異性は犯人が戦術を高度化させていること、脆弱性と攻撃標的の優先順位に見合うよう手法のカスタマイズを行なっているということを示している。例えばゲーミング業界では、攻撃は一時的で、その威力も弱めではあるが、発生頻度がとてつもなく高い。この戦術は特定サーバでの継続障害で、ゲーミング体験を損ない、プレイヤーに競合他社サーバへの移行を強いることを目したものだ。これとは対照的に、金融サービスや通信事業セクタではーサービス破壊は極めて高い利害関係と収益への悪影響がより短絡的に起こるー攻撃は量の観点でより苛烈となり、持続時間の観点で多様性を帯びる。

ゲーミング、テクノロジ、金融サービス、通信業界に対しては依然として攻撃者側の注目度は高く、これは、攻撃者が恣意的な戦略を以て、破壊が経済面や経営・運営面で深刻な結果につながる標的を選択しているということを示している。

攻撃タイプ、サイズ、地域、持続時間に関わらず、ビジネスを守る Gcore

業界や地域全般で明確かつ一貫している事実がある：DdoS 攻撃がその矛先を緩めてはいないということだ。攻撃そのものと標的戦略とは複雑化しつつ膨張を続けている。業界や規模を問わず、組織にとっては今が行動を起こす時で、警戒を解かず、プロテクションと事前阻止戦略への投資を行うべきだ。

DDoS 脅威に先んじることはサイバー攻撃者が変え続ける実施パターンや戦略への深く的確な理解が欠かせない。Gcore DDoS Protection は最大規模級の威力の継続攻撃を撃破した実績がある。150 超 Tbps のフィルタリング総容量、6 大陸におよぶカバー、数百万のインターネット資産を配するグローバルネットワークを保持する Gcore で規模増強化と高度化が進む攻撃からの保護を。

Gcore DDoS Protection 詳細