

本リリースは2024年1月24日に本社 G-Core Labs S.A により発表されたリリースの抄訳です。
末尾に当該テーマに関する日本国内向けのセッションに関する情報を追記しています。

Gcore Radar Report で解説する DDoS 攻撃動向 2023 年下半期にピーク時ボリュームが 2 倍に増加

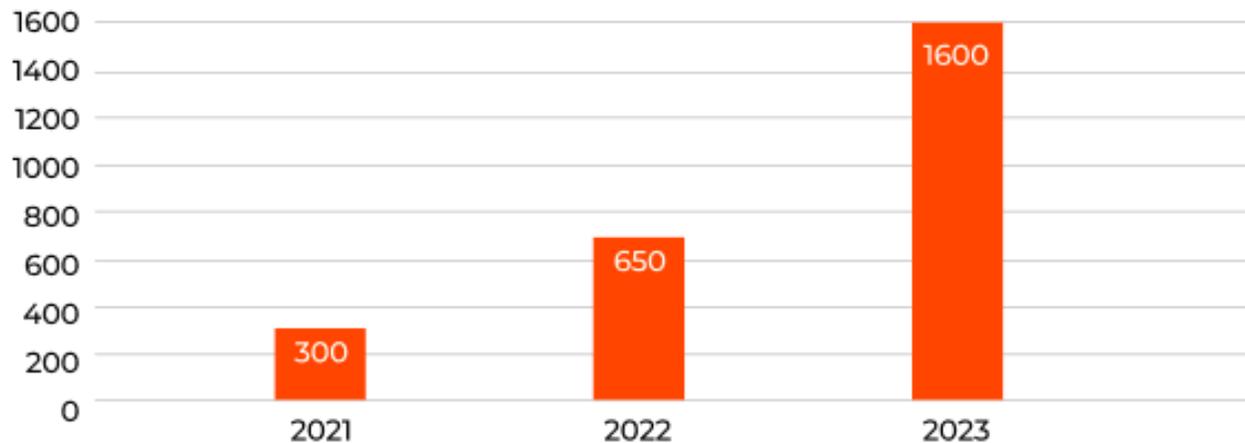
ボリューム急増に伴い、サイバーセキュリティ業界での測定指標単位が テラビット に更新される事態に

ルクセンブルク：2024年1月24日 – クラウドおよびエッジソリューションのグローバルプロバイダである Gcore は、2023 年下半期版 Gcore Radar Report を発行しました。このレポートで、DDoS プロテクション市場とサイバーセキュリティ動向について解説と洞察を提示し、2023 年下半期の特筆すべき動向として、サイバー脅威がその規模と巧妙さにおいて従来を凌ぐ展開に言及しています。

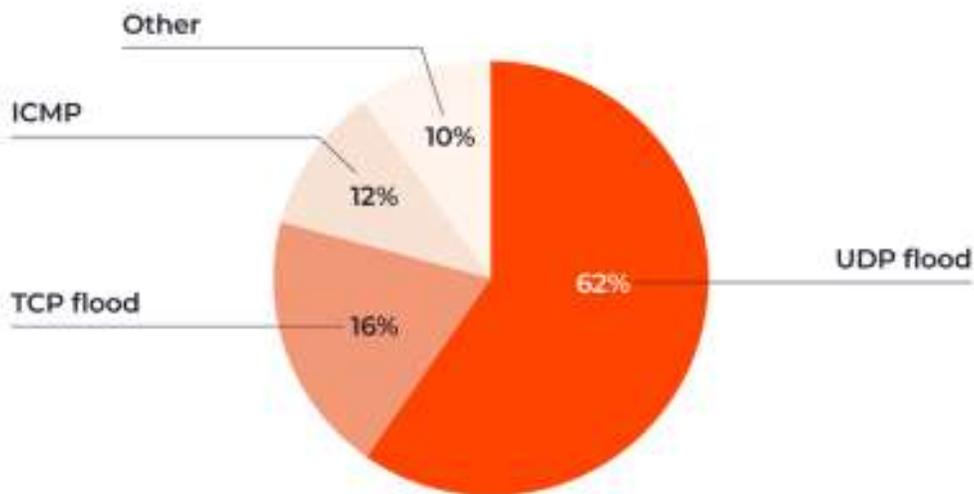
2023 年下半期（第 3 四半期～第 4 四半期）の主要動向

- 最大アタック威力が 1.6 Tbps へと急騰。（参考記事 [Gcore Thwarts 1.1 Tbps DDoS Attack](#)）
- 2021 年は 300 Gbps、2022 年は [650 Gbps](#)、2023 年上半期は [800 Gbps](#) に達していた。過去 3 年間の増加は年率 100%を超えた。また、この上昇傾向は 2024 年にも継続すると Gcore では予測している。2023 年下半期のこの急増に伴い、サイバーセキュリティ業界での測定単位を Terabit に切り替えることを余儀なくされた。
- UDP フラッドが DDoS アタックの 62%と、上半期と同様の最多を占めた。TCP フラッドは 16%、ICMP アタックは 12%、SYN、SYN+ACK と RST フラッドの合計が 10%に着地し、SYN フラッドは低位に下落した。2023 年上半期の分布は、UDP 52%、TCP 19%、SYN 24%、その他が 5%であった。
- 攻撃標的のビジネスセクタはゲーミング（46%）、ファイナンス（銀行・ギャンブルサービスを含む）（22%）、テレコム（18%）の順。2023 年上半期はそれぞれ、30.1%、28.4%、24.7%であった。
- 攻撃継続時間の最長は 9 時間であった。2023 年上半期の結果は最長 16 時間 22 分。
- 攻撃継続時間の平均は約 1 時間であった。2023 年上半期の結果は平均 4 時間以内。

2021年～2023年の攻撃の最大値 単位 Gbps



2023年下半期の主な攻撃タイプ

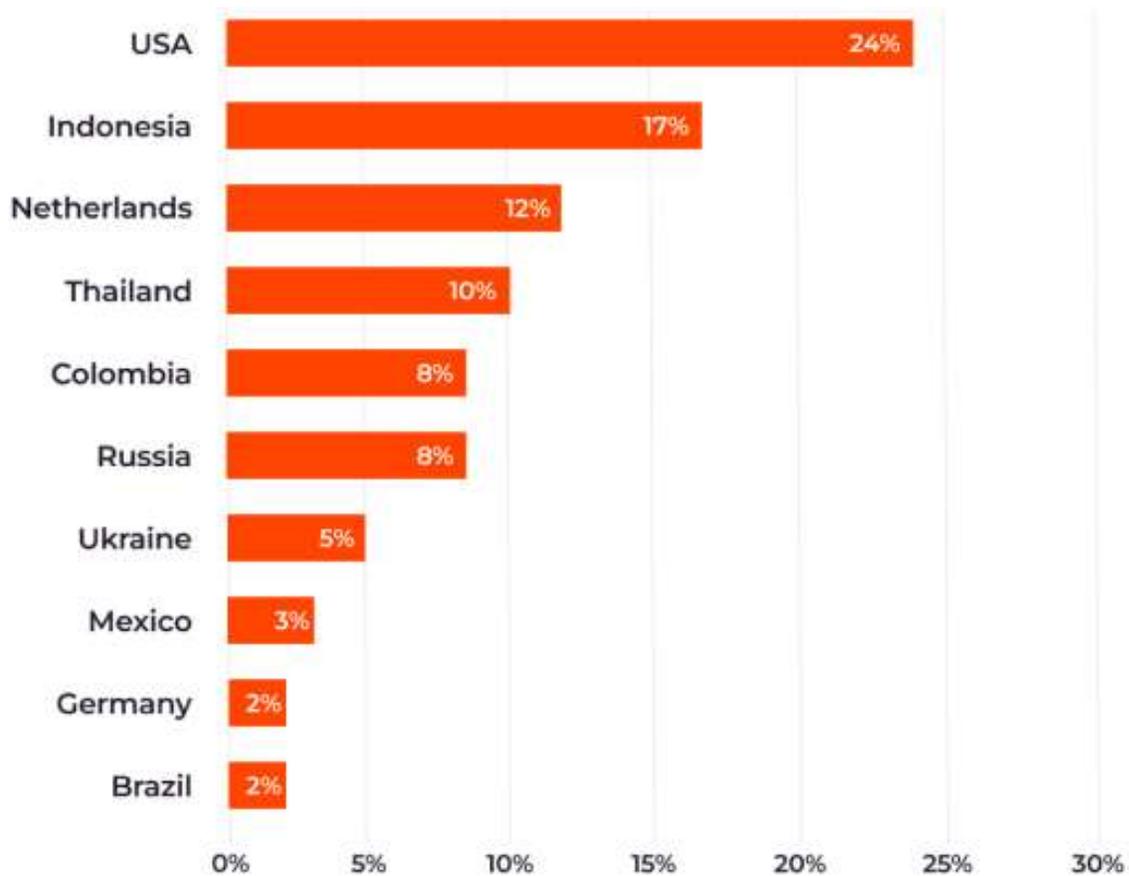


2023年後半の攻撃威力とパターン数が急増したことから、サイバーアタッカーの巧妙化が顕著となりました。企業や組織側での多面的な防御戦略を立て、広範囲に及ぶ DDoS 攻撃からの防御の必要性が一層増していると言えます。脅威はその進化を止めることなく、このような脅威に対する対応を誤ると、信用や名声の失墜、ユーザからの信頼喪失、セキュリティ違反等、混乱や風評被害を含む高コストリスクの温床となるでしょう。(Andrey Slastenov, Head of Security Department, Gcore)

地域別 DDoS アタック

脅威元となる国々は、全世界の広範囲にわたります。上位 3 国には米国、インドネシア、オランダ、下位 3 国にはメキシコ、ドイツ、ブラジルがランクされました。

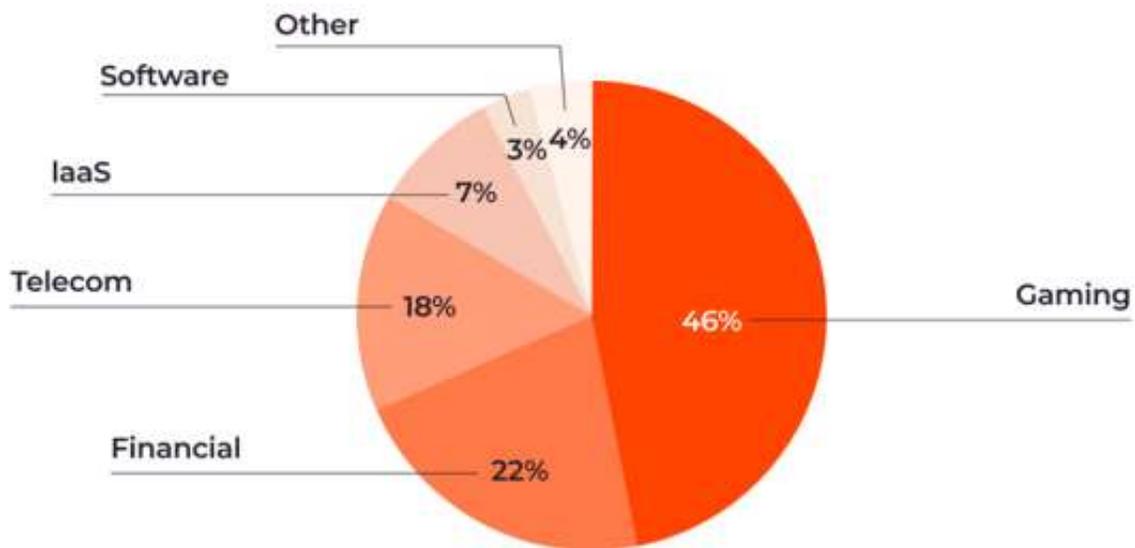
攻撃元の地域分散



ビジネスセクタ別 DDoS アタック

2023 年第 3～4 四半期で最も多く標的となったビジネスセクタはゲーミング、ファイナンスおよびテレコムでした。財務増収やユーザへの影響の大きさという側面がその要因となったと推測されます。そのため、サイバーセキュリティ標的への戦略的な対抗策や特定ゲーミングサーバを採用する必要性が浮上します。

業界別 DDoS 攻撃



攻撃威力が 1.6 Tbps に増大したことは、企業や組織が高次レベルで対策を講じ、取り組むべき事態の到来を警告し提示するものです。アタック元凶となる国々の地域分散化が進んでおり、これらを総合すると、DDoS 脅威は深刻なグローバル問題で、国際間協力の実施、情報共有手法のインテリジェント化、破壊攻撃の可能性の回避と低減化への効率的な取り組みが求められています。（Andrey Slastenov, Head of Security Department, Gcore）

※Gcore Radar Report：進化し続ける脅威の全貌と効率的な対攻撃策に関する着眼点と、サイバーセキュリティ動向の最前線と洞察を提供する年 2 回の定期刊行。



Gcore は、3月21日（木）～3月22日（金）に開催される ITmedia 主催セミナー『ITmedia Tech Highlights 2024 冬～セキュリティ/開発/データ基盤編～』に協賛し、講演を行います。

当該レポートのデータと分析および Gcore セキュリティ専任として日々接する DDoS セキュリティ事案やその動向を様々な観点から紐解きつつ、これまで、今、そしてこれからについて企業・組織へのガイダンスをお届けするセッションに Gcore Head of Security が登壇します。

[『ITmedia Tech Highlights 2024 冬
～セキュリティ/開発/データ基盤編～』](#)

会期：2024年3月21日（木）～2024年3月22日（金）

主催：@IT 編集部

視聴登録（無料・事前登録制）は[こちら](#)から

Gcore セッション：セキュリティテーマ セッション 2-1

日時：2024年3月22日（金）午後1時50分～午後2時20分

タイトル：DDoS 脅威アップデート

概要：次々と繰り出されるサイバー攻撃。その手法やパターンが変遷し続ける一方で、デジタル領域におけるサイバーセキュリティリスク要因や潜在性の高まりも止まず、双方ともに深刻な懸念材料となっています。サイバーセキュリティ最新事情や事例、セキュリティレポート最新データ・分析とともに、攻撃への対抗策、防御や回避施策を提示・解説します。

Gcore について ～ Gcore は 2024 年 2 月に 10 周年を迎えました（参考英文記事；[Blog](#), [Linkedin Post](#)）。

Gcore はエッジ AI、クラウド、ネットワーク、セキュリティのグローバルソリューションプロバイダです。本社はルクセンブルク、600 超の従業員と世界各地に 10 の営業拠点を擁しています。Gcore の IT インフラストラクチャは自社運用、拠点は 6 大陸にまたがり、グローバル平均レスポンスタイムは 30ms、ヨーロッパ、アフリカ、LATAM における屈指のネットワークパフォーマンスを実現しています。ネットワークは Tier IV と Tier III のデータセンタに配備された世界各地の 160 超の PoP で構成され、110 超 Tbps の帯域を誇ります。

Web サイト www.gcore.com

ソーシャルメディア

<https://www.linkedin.com/company/g-core/>

<https://www.youtube.com/@GCoreOfficial>

<https://www.facebook.com/gcorelabscom>

https://x.com/gcore_official

<https://www.instagram.com/gcore.official/>

同件に関するお問い合わせ先

Gcore Japan 株式会社

Marketing Manager：白石

tel:03-4567-2817/email: keiko.shiraishi@gcore.com

共同ピーアール株式会社

担当：栗木、仙場、峰松

email: Gcore-pr@kyodo-pr.co.jp