GCORE

High Performer
Mid-Market
SPRING 2023

Gcore Radar: DDoS アタックトレンド

2023年第3・第4四半期

2024年1月 | gcore.com

要旨

DDoS アタックの追跡結果および Gcore 社内の分析結果を Gcore Rader レポートとして年2回の頻度で公開しています。当資料は2023年下半期版です。Gcore ではグローバルに分散展開するスクラビングセンターネットワークを介し、攻撃傾向の経時追跡を行っています。2023年下半期の DDoS 攻撃の傾向は、大規模かつ高度なサイバー脅威の顕著な増加、これに対する警戒強化の必要性が浮上しています。ピーク時攻撃威力は前回調査比から倍増しTbps単位、特定の業界を狙った攻撃戦略、攻撃発信元のグロー バル化の傾向など、DDoS を取り巻く環境や状況の大きな変化が検知されました。

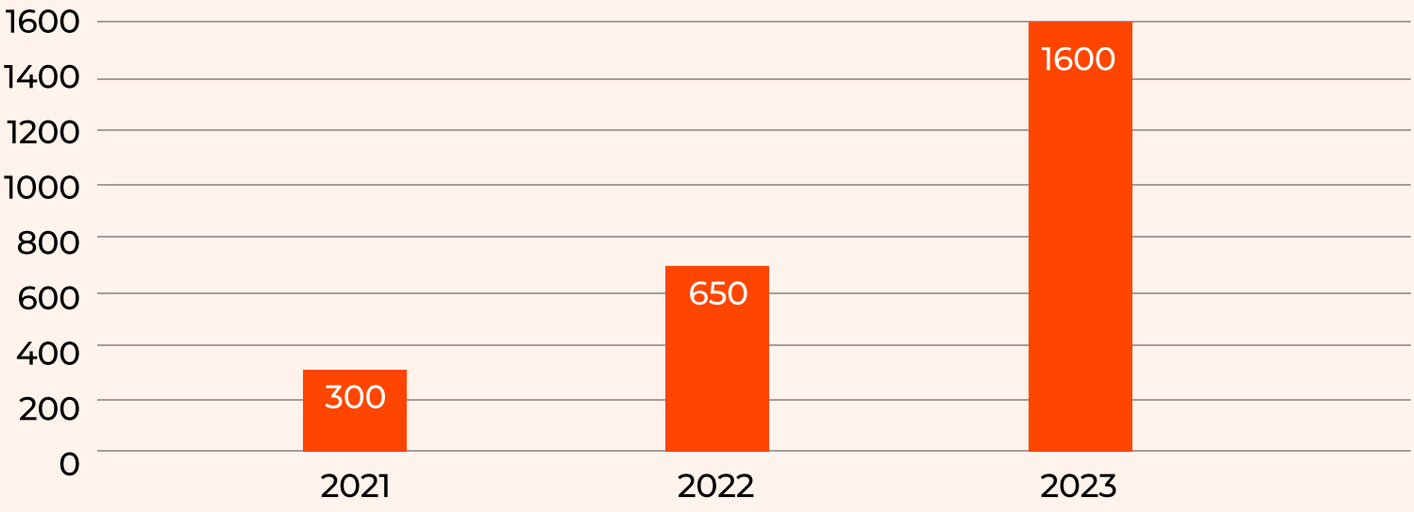
前例のない攻撃力

DDoSのピーク時（記録された中で最大）の攻撃ボリュームは過去3年間にわたり毎年100%超増加しています。

- **•2021年：300Gbps**
- **•2022年：650Gbpsに増加**
- **•2023年上半期：800Gbpsに増加**
- **•2023年下半期：1600Gbps（1.6Tbps）に急増**

2023年下半期における著しい増加に伴い、サイバーセキュリティ業界での DDoS 攻撃測定単位がテラビットに改変される事態となりました。

2021～2023年の最大攻撃力（Gbps単位）

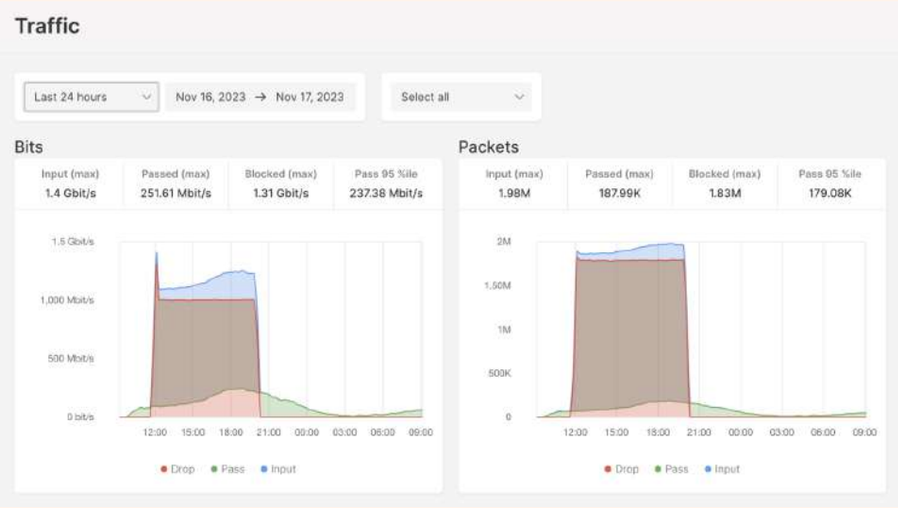


2021~2023年にかけて、ピーク時最大攻撃力が300、650、1600 Gbpsへと増大していく状況がグラフから見て取れます。

DDoS 攻撃による甚大かつ潜在的な被害が増加し続けていることが分かります。

攻撃時間

2023年下半期に記録された最長攻撃時間は9時間でした



攻撃継続時間は3分から9時間、平均約1時間であることが分かりました。通常、短時間攻撃は検知が難しくなる傾向があります。データ不足によりトラフィック分析が不可能となり、識別や回避が困難になることが一因です。

長時間攻撃では、取り組みにかかる負担が増加します。高い有効性を備えた回避策が必要になるためです。有効性が引き出せない場合、サーバ機能不全の状況が長引く結果につながってしまいます。

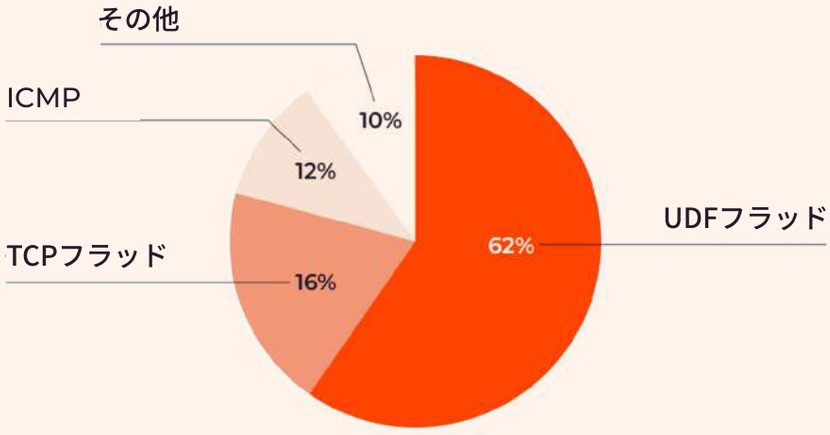
主流攻撃タイプ

依然として主流なのはUDPフラッドで、DDoS攻撃の62%を占めています。TCPフラッドとICMPはそれぞれ16%と12%と引き続き上位を占めています。

SYN、SYN+ACKフラッド、およびRSTフラッドを含むその他 DDoS 攻撃タイプは10%にどとまります。これらの高度な手法での攻撃パターンの可能性は払拭できませんが、主流は大量パケット送信によるサーバ攻撃です。

多様化が進む攻撃方法や DDoS 技術からの保護、つまり、多面的な防御戦略が必要とされています。

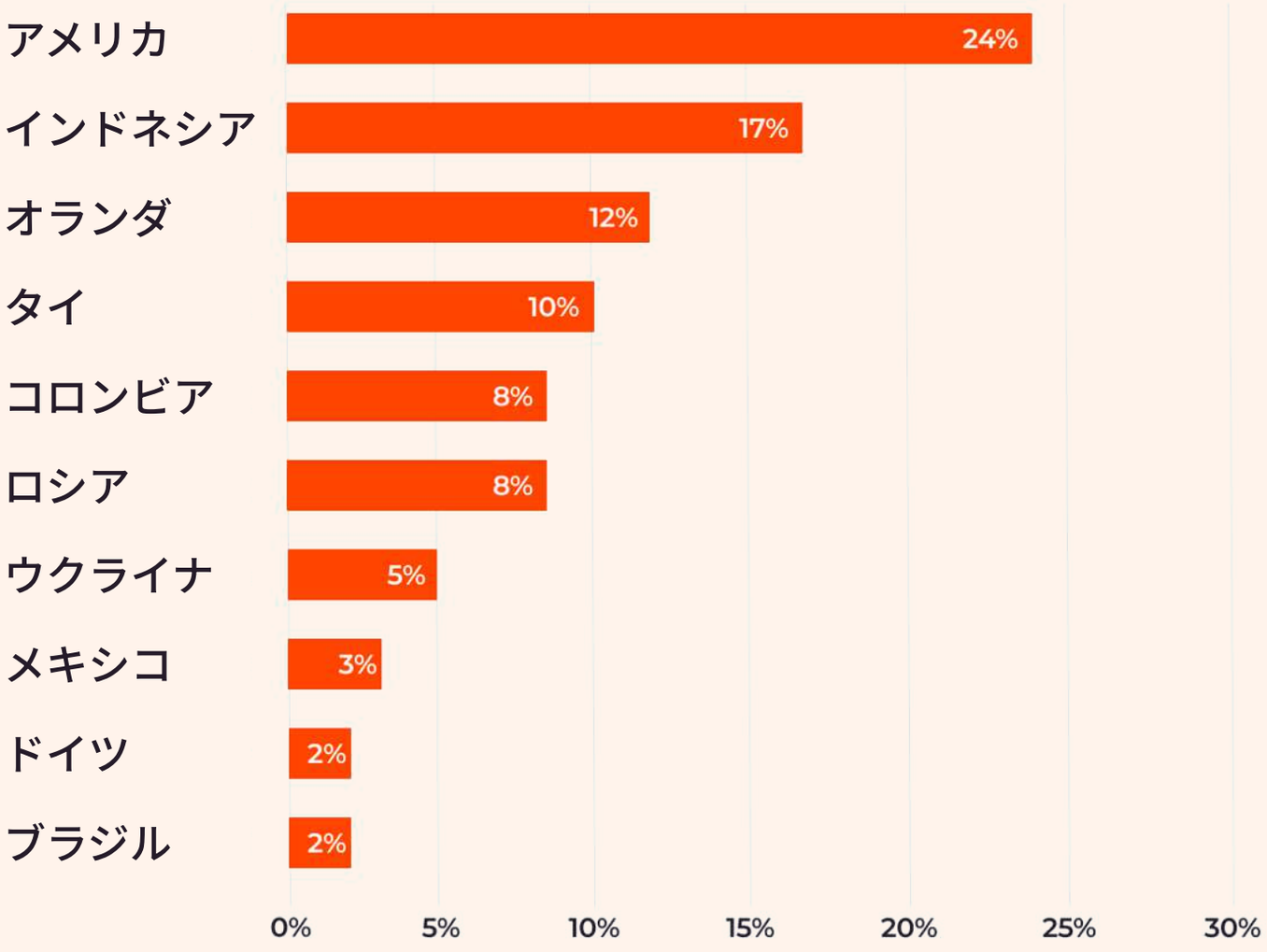
2023年下半期の主な攻撃の種類



世界の攻撃元

攻撃元が世界中への拡散は、サイバー脅威がボーダーレス化し攻撃者が国境を越えて活動していることを示しています。Gcore では2023年後半の攻撃元を複数検出しました。最多は米国で24%、 続くインドネシア(17%)、オランダ(12%)、タイ(10%)、コロンビア(8%)、ロシア (8%)、ウクライナ(5%)、メキシコ(3%)、ドイツ(2%)、およびブラジル(2%)で上位10カ国を占め、脅威の動向がグローバル拡散していることが分かります。

地理的な攻撃元の分布



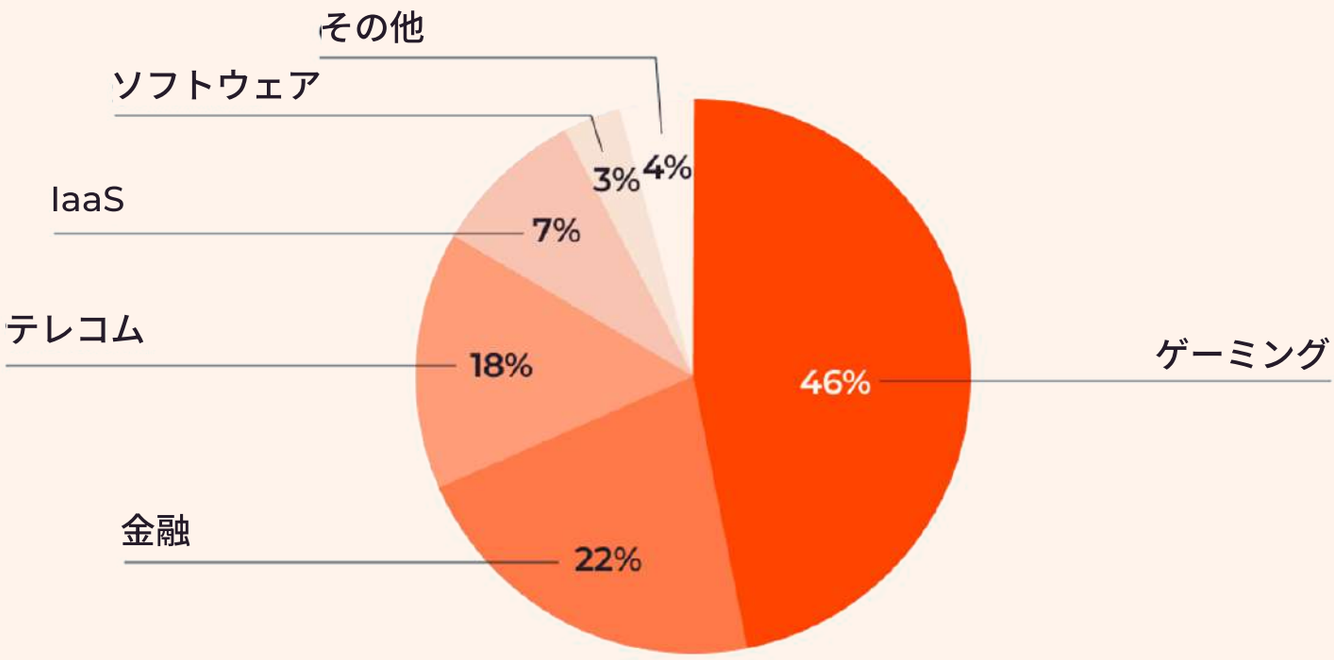
DDoS 攻撃元の地域分散が進んでいる事実から引き出せる情報は、照準を絞った防御戦略の策定や、サイバー犯罪への取り組みに向けた国際ポリシー策定に有効活用することができます。ただし、IPスプーフィングなどの手法や分散型ボットネットが関与することから、攻撃者の場所の特定は困難です。攻撃者に関しては、国家が背後で支援しているケースから個々のハッカーレベルまで多岐にわたるという背景も加わり、攻撃動機や攻撃能力の精査は困難を極めるざるをえません。

業界別標的

2023年下半期の業界別標的の分析から、DDoS 攻撃は幅広いセクタに及んでいることが分かります。

- ゲーミング業界が46%と最多
- 銀行やギャンブルを含む金融分野は22%で2位
- 電気通信(18%)、IaaS(Infrastructure as a Service)プロバイダ(7%)、およびコンピューターソフトウェア企業(3%)が続く

影響を受けた業界別のDDoS攻撃



攻撃対象は前回の Gcore Radar レポートから変化は見られません。ゲーミングおよび金融セクタは依然として攻撃標的です。財政面での利益およびユーザへの影響力の大きさが標的となる要因になっていると推測されます。この結果から、被害が甚大な業界においては、照準を定めたサイバーセキュリティ戦略が必須と言えます。特定ゲーミングサーバ向けの対策がその一例です。

分析

2023年下半期のデータから、DDoS 攻撃状況には懸念すべき傾向があることが分かります。攻撃力の1.6 Tbpsへの増大は特に警戒するべきで、レベルが更新された脅威に対し、組織側が対策を講じる必要があることを警告するものです。保護対策が取られていなければ、 300 Gbsの「小規模」レベルの攻撃であっても、サーバを無力化する能力を有しているのです。攻撃元の地理分布と併せて考慮すると、DDoS の脅威は深刻かつ世界的な課題であることは明白です。協力体制の構築とインテリジェンスの共有を国際規模で行い、潜在的な破壊攻撃を効果的に回避することが求められます。

攻撃時間に幅があることから、攻撃者がより戦略的になっており、特定の標的や目的に合致する手法を能動的に選択していることが見て取れます。

- **ゲーミングセクタ；**攻撃力と攻撃時間は比較的抑制的であるものの、その頻度は高く、特定のサーバへの破壊行為が繰り返し続き、その結果、ユーザ体験にダメージが及ぶことから競合企業のサーバへの移行が進んでしまうことになります。
- **金融およびテレコムセクタ；**経済的影響という即時効果が得られるため、様々な継続時間で大規模ボリューム攻撃が実行されます。

まとめ

このレポートは絶え間なく進化し続けるサイバー脅威についての情報をタイムリーにお伝えするものです。様々なセクタ組織による投資は、包括的かつ優れた対応力を備えたサイバーセキュリティ対策に向けられる必要があります。DDoS 脅威に先手を打つには、サイバー攻撃のパターンや戦略の変化に対する鋭敏かつ的確な理解を維持し続けなければなりません。

最強かつ長時間攻撃を撃退した実績を持つGcore DDoS プロテクションを活用して、2024年のDDoS 状況が及ぼす影響からのビジネス保護と推進を検討してください。