CLOUDFLAREのセキュリティインサイト

Cloudflareのセキュリティインサイト：2022年第1四半期におけるDDoS攻撃の傾向

03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com

目次

概要

本レポートには、2022年1月から3月にかけてCloudflareグローバルネットワークで観測された、アプリケーション層とネットワーク層の両方における新しいデータポイントやインサイトが含まれています。

2022年第1四半期は、アプリケーション層DDoS攻撃の大幅な急増が見られましたが、ネットワーク層全体のDDoS攻撃の総数は減少しました。減少したものの、ボリューム型DDoS攻撃は前四半期比最大645%と急増し、そして私たちは、増幅率2200億%の新たなゼロデイリフレクション攻撃を緩和しました。

ロシアとウクライナのサイバースペースにおいて、最も標的にされた産業はオンラインメディアと放送メディアでした。アゼルバイジャンとパレスチナのCloudflareデータセンターではDDoSの活動が急増しており、これは内部から操作されるボットネットの存在を示しています。

要点

ロシアおよびウクライナのサイバースペース

- 第1四半期にロシア国内で最も標的にされた産業は、ロシアのオンラインメディア企業でした。次いで標的とされたのはインターネット業界、暗号通貨、小売業の順となっています。ロシアの暗号通貨企業を狙った攻撃の多くは、ウクライナや米国を発生源としていましたが、もう一つの主要な攻撃源はロシア国内そのものからでした。
- ロシアの企業を標的としたHTTPDDoS攻撃の大半は、ドイツ、米国、シンガポール、フィンランド、インド、オランダ、ウクライナから発信されたものでした。ここで重要なのは、サイバー攻撃のトラフィックの発信元を特定できることと、攻撃者の所在を特定できることは別物であることに留意することです。
- ウクライナへの攻撃は放送メディアや出版社のウェブサイトが標的とされ、より多くの国が発信源となり、より拡散されたものと見られます。これは、国際的にボットネットが使用されていることを示している可能性があります。しかし、攻撃トラフィックのほとんどは、米国、ロシア、ドイツ、中国、英国、およびタイから発信されたものです。

オープンインターネットのロシアへの流入を続けるため、攻撃を防ぐためにCloudflareが行っていることをご覧ください。

ランサムDDoS攻撃

- 2022年1月、攻撃を受けている回答者の17%以上が、ランサムDDoS攻撃の標的にされた、または事前に脅迫を受けたと回答しています。
- この数値は2月には6%、3月には3%へと急激に低下しました。
- これまでの四半期と比較すると、第1四半期にランサムDDoS攻撃を報告した回答者は全体の10%に過ぎず、前年同期比で28%減、前四半期比で52%減となっていることがわかります。

要点（続き）

アプリケーション層DDoS攻撃

- 2022年第1四半期は、アプリケーション層への攻撃が過去12ヶ月で最も活発な四半期となりました。HTTPレイヤーのDDoS攻撃は、前年同期比164%増、前四半期比135%増となりました。
- 四半期をさらに詳しく見ると、2022年3月には、第4四半期（および第3四半期、第1四半期）の総数を上回るHTTP DDoS攻撃がありました。
- HTTP DDoS攻撃の発生源は、4四半期連続で中国がトップでしたが、今四半期は米国がトップに躍り出ました。米国を発生源とするHTTP DDoS攻撃は、前四半期比6,777%、前年同期比2,225%という驚異的な増加率を示しています。

ネットワーク層DDoS攻撃

- 第1四半期のネットワーク層攻撃は、前年同期比で71%増となりましたが、前四半期比では58%減となりました。
- ネットワーク層DDoS攻撃で最も標的とされたのは電気通信業界、次いでゲーム・ギャンブル会社、情報技術・サービス業界でした。
- 帯域幅消費型攻撃は第1四半期に増加しました。10Mpps（百万パケット/秒）を超える攻撃は前四半期比300%以上増、100Gbpsを超える攻撃は前四半期比645%増となりました。

本レポートは、CloudflareのDDoS攻撃対策システムによって自動的に検知・軽減されたDDoS攻撃に基づいています。この仕組みの詳細については、こちらの深堀りしたブログ記事をご覧ください。

当社のネットワーク上で観測されたDDoS攻撃の測定方法に関するメモ

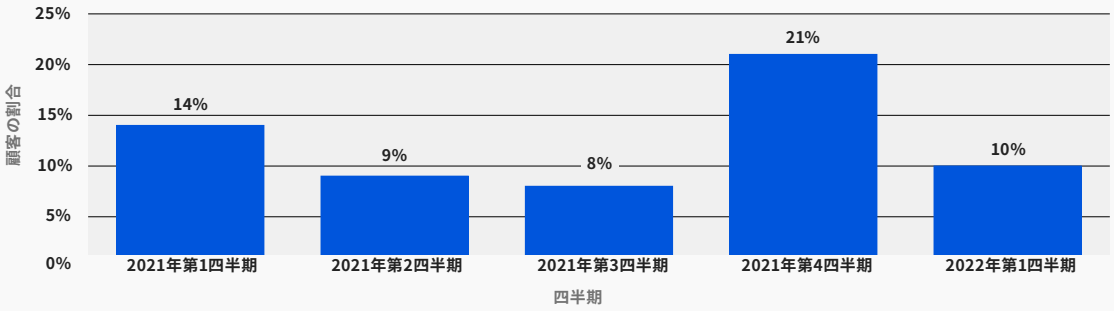
攻撃の傾向を分析するために、当社のグローバルネットワーク、特定の場所、または特定のカテゴリ（業界や請求先の国など）で観測された総トラフィック（攻撃＋クリーン）に占める攻撃トラフィックの割合である「DDosの活動」レートを計算します。割合を測定することで、データポイントを正規化し、例えば総トラフィックが多く、攻撃回数も多いと思われるCloudflareデータセンターに対しての絶対数に反映される数値が偏ることを回避できます。

ランサム攻撃

当社のシステムはトラフィックを常時分析し、DDoS攻撃を検知すると自動的に被害軽減措置を適用するシステムです。DDoSの被害に遭われたお客様には、攻撃の性質や軽減措置の効果をよりよく理解するために、自動化されたアンケートをお願いしています。

Cloudflareでは、2年以上前から攻撃を受けたお客様を対象にアンケート調査を実施しています。アンケートの質問の1つに、DDoS攻撃を止める代わりに支払いを要求する脅迫や身代金請求書を受け取ったかどうかというものがあります。前四半期の2021年第4四半期には、記録的なレベル（お客様の5人に1人）のランサムDDoS攻撃が報告されました。今期ではランサムDDoS攻撃が減少し、ランサムDDoS攻撃の報告者は回答者の10人に1人までになっており、前年同期比28%減、前四半期比52%減となりました。

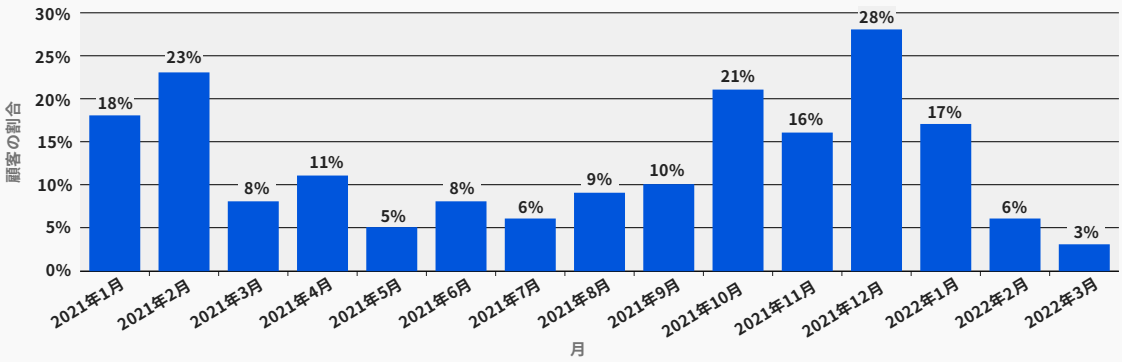
ランサムDDoS攻撃と脅威<四半期別>[1]
ランサムDDoS攻撃の標的になったと報告した回答者の割合



ランサムDDoS攻撃の標的になった、
または事前に攻撃の脅迫を受けたと報告した回答者の割合です。

月別に見ると、2022年1月の第1四半期に最も多くの回答者が身代金要求の文書を受け取ったと報告していることが分かります。これは、ほぼ5人に1人（17%）のお客様です。

ランサムDDoS攻撃と脅威<月別>[1]
ランサムDDoS攻撃の脅威にさらされた、または標的になったと報告した回答者の割合

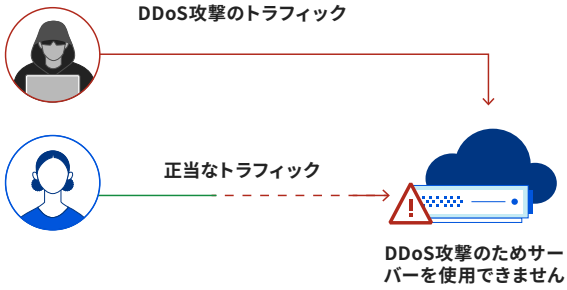


1. 出典： https://radar.cloudflare.com/notebooks/ddos-2022-q1

アプリケーション層DDoS攻撃

アプリケーション層DDoS攻撃（具体的にはHTTP DDoS攻撃）は通常、正当なユーザーリクエストを処理できないようにしてWebサーバーを停止させることを目的とします。

処理能力を超えるリクエストが殺到すると、サーバーは正当なリクエストをドロップするか、場合によってはクラッシュし、その結果、正当なユーザーに対するパフォーマンスの低下や障害に繋がります。



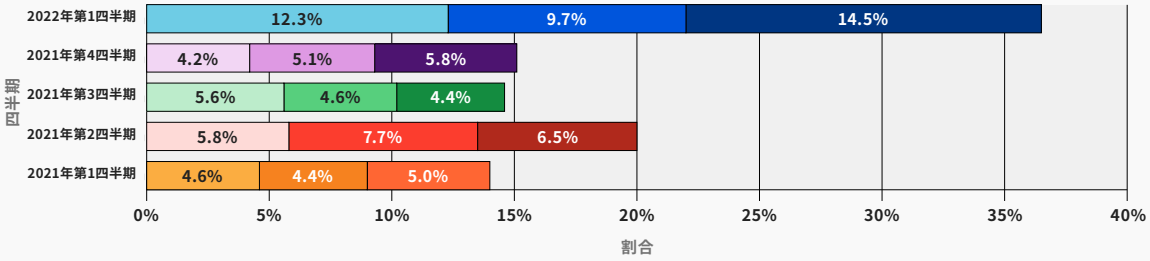
アプリケーション層DDoS攻撃の月別推移

第1四半期は、アプリケーション層DDoS攻撃が前年同期比164%増、前四半期比135%増と急増し、過去1年間で最も多発した四半期となりました。

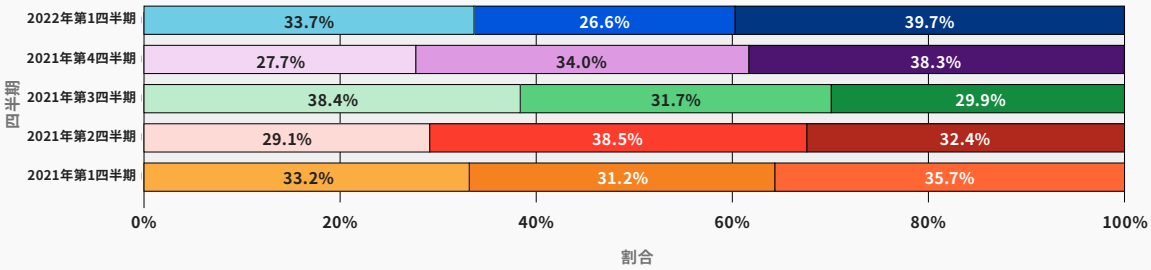
アプリケーション層DDoS攻撃は、2022年の第1四半期にかつてないほど増加しました。

3月だけで、2021年第4四半期の総数（および第3四半期、第1四半期）を上回るHTTP DDoS攻撃が発生しています。

月別年間分布[1]
過去15ヶ月のアプリケーション層DDoS攻撃の月別年間分布



月別四半期分布[1]
過去15ヶ月のアプリケーション層DDoS攻撃の月別四半期分布



1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

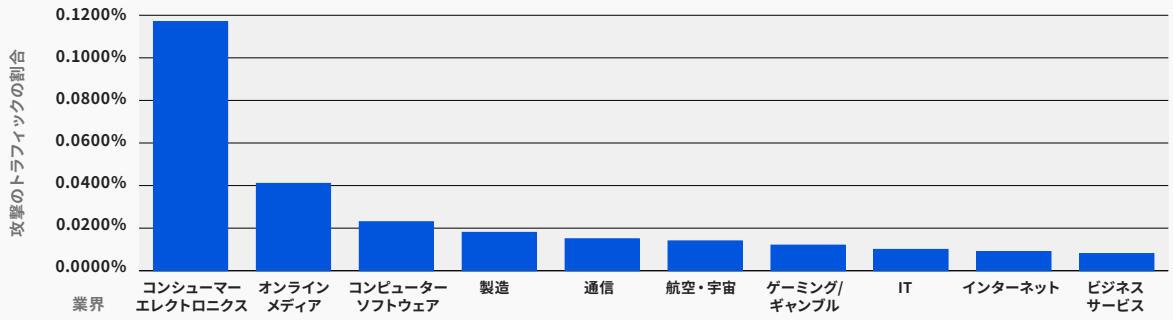
アプリケーション層DDoS攻撃＜業界別＞

第1四半期に最も標的とされた業界は、家電業界でした。

世界的には、家電業界が最も攻撃され、前四半期比5,086%増となりました。第2位はオンラインメディア産業で、攻撃件数は前四半期比2,131%増となりました。第3位はコンピュータ・ソフトウェア企業で、前四半期比76%増、前年同期比1,472%増となりました。

業界別分布[1]

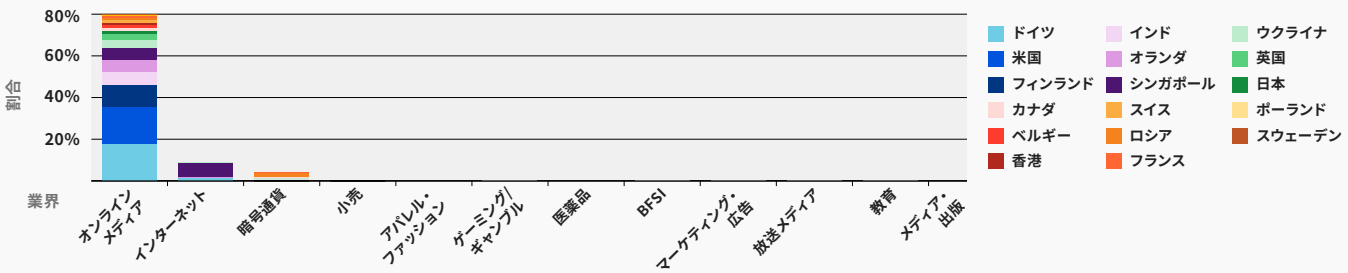
2022年第1四半期におけるHTTP DDoS攻撃の業界別分布



しかし、ウクライナとロシアだけに注目すると、放送メディア、オンラインメディア企業、インターネット企業が最も標的にされていることがわかります。詳しくは[オープンインターネットのロシアへの流入を続けるため、攻撃を防ぐためにCloudflareが行っていること]をご覧ください。

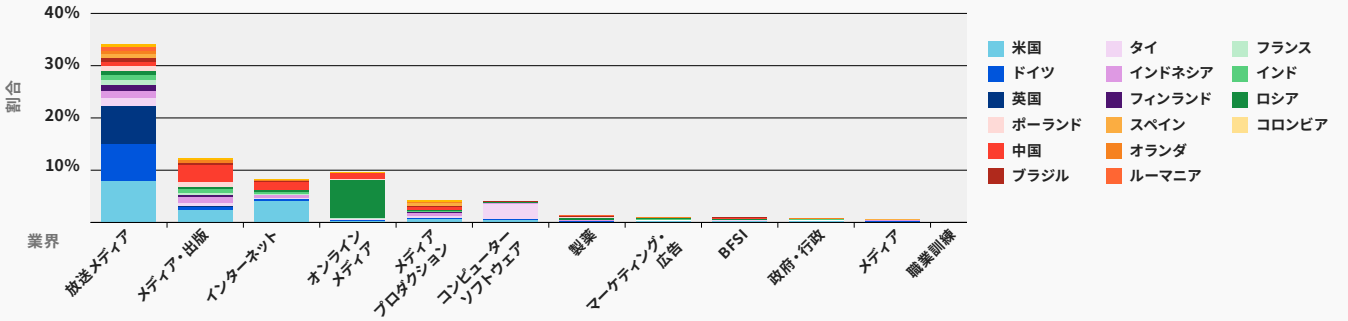
業界別・攻撃元の国別のロシアへの攻撃[1]

2022年第1四半期におけるロシア産業界へのHTTP DDoS攻撃の攻撃元の国別分布



業界別・攻撃元の国別のウクライナへの攻撃[1]

2022年第1四半期におけるウクライナ産業界へのHTTP DDoS攻撃の攻撃元の国別分布



1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

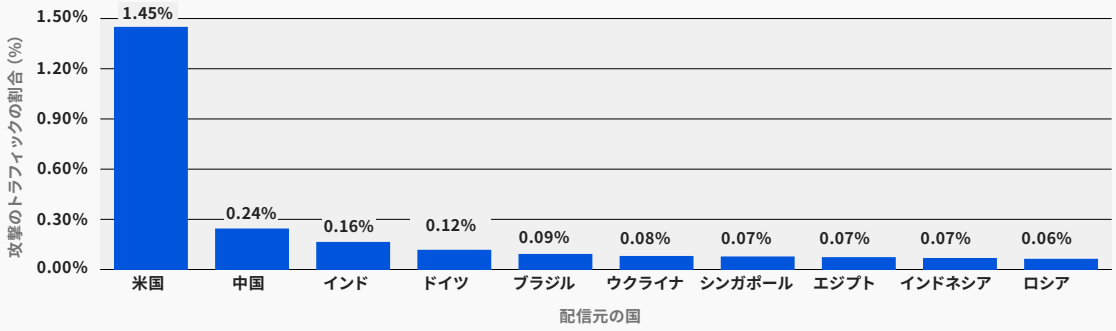
アプリケーション層DDoS攻撃＜攻撃元の国別＞

HTTP攻撃の発信元を理解するため、当社は攻撃のHTTPリクエストを生成したクライアントに属する送信元IPアドレスのジオロケーションを調べました。ネットワーク層攻撃とは異なり、HTTP攻撃では送信元IPアドレスのスプーフィングができません。ある国でのDDoS活動の割合が高い場合、通常、その国の国境内で活動するボットネットが存在することを示しています。

HTTP DDoS攻撃の発生源は、4四半期連続で中国がトップでしたが、今四半期は米国がトップに躍り出ました。米国を発生源とするHTTP　DDoS攻撃は、前四半期比6,777%、前年同期比2,225%という驚異的な増加率を示しています。2位の中国に次いで、インド、ドイツ、ブラジル、ウクライナとなっています。

攻撃元の国別分布[1]

2022年第1四半期におけるHTTP DDoS攻撃の攻撃元の国別分布



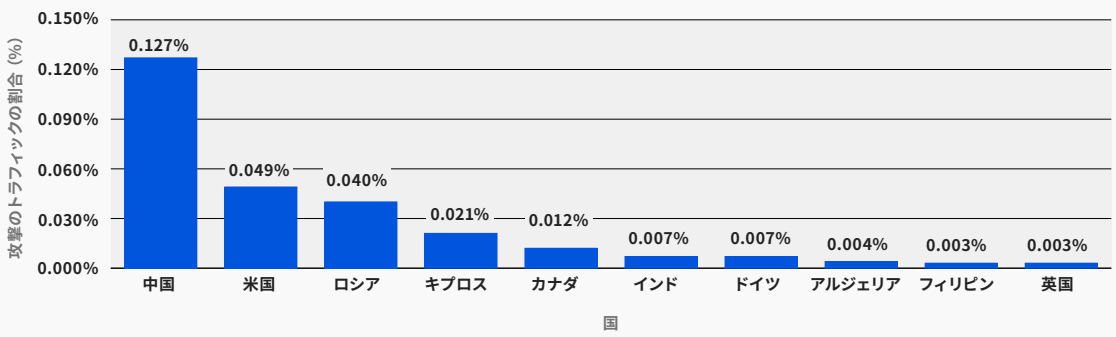
アプリケーション層DDoS攻撃＜標的国別＞

どの国が最もDDoS攻撃の対象となったのかを特定するために、お客様の請求先国別にDDoS攻撃をバケット化し、全DDoS攻撃に対する割合で表現しています。

米国は3四半期連続の1位から2位に後退しました。HTTP　DDoS攻撃で最も標的とされたのは中国の組織で、米国、ロシア、キプロスがそれに続く形となりました。

標的国別分布[1]

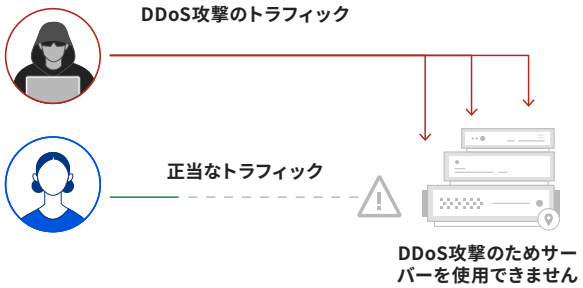
2022年第1四半期におけるHTTP DDoS攻撃の標的国別分布



1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

ネットワーク層DDoS攻撃

アプリケーション層攻撃は、エンドユーザーがアクセスしようとしているサービス（事例ではHTTP/S）を実行するアプリケーション（OSI参照モデルのレイヤー7）を狙うのに対し、ネットワーク層攻撃はネットワークインフラ（インラインルーターやサーバーなど）とインターネットリンクそのものを圧倒しようとします。

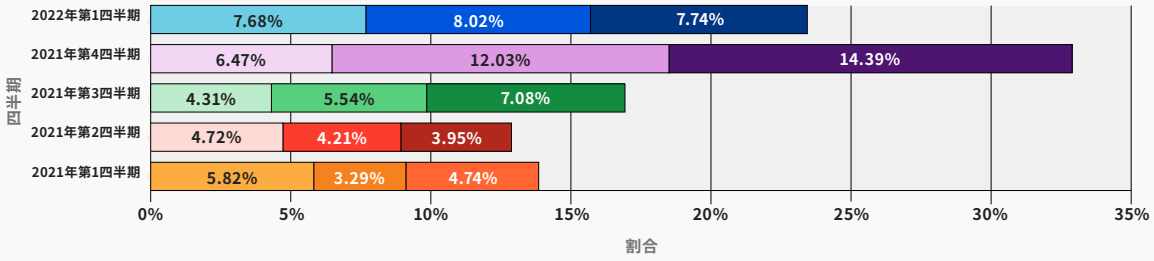


ネットワーク層DDoS攻撃＜月別＞

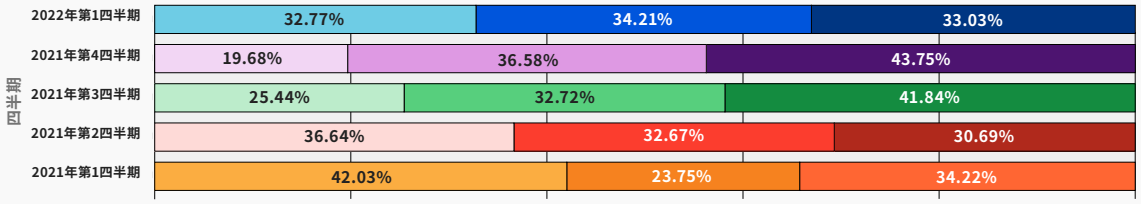
第1四半期にはHTTP DDoS攻撃が急増したものの、ネットワーク層DDoS攻撃は実際には前四半期比で58%減となりました。しかし前年同期比では71%増となっています。

第1四半期をさらに詳しく見ると、ネットワーク層DDoS攻撃の量は四半期を通じてほぼ一定であり、毎四半期に約3分の1の攻撃が発生していることがわかります。

月別年間分布[1]
過去15ヶ月のネットワーク層DDoS攻撃の月別年間分布



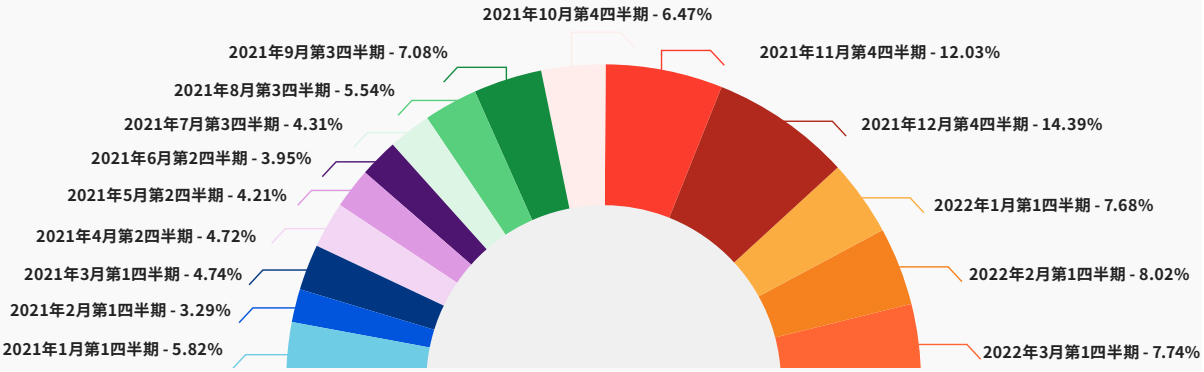
月別四半期分布[1]
過去15ヶ月のネットワーク層DDoS攻撃の月別四半期分布



1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

ネットワーク層DDoS攻撃＜月別＞（続き）

過去15ヶ月[1]
過去15ヶ月のネットワーク層DDoS攻撃の分布



Cloudflare、ゼロデイDDoSアンプ攻撃を緩和

これらのネットワーク層DDoS攻撃の中には、Cloudflareが自動的に検知し緩和したゼロデイDDoS攻撃も含まれています。

3月初旬、Cloudflareの研究者らが、企業の電話システム「Mitel」に存在するゼロデイ脆弱性の調査と公開に協力しました。この脆弱性を利用すると、攻撃者は他の悪用の可能性もありますが、DDoSアンプ攻撃を行うこともできます。この種の攻撃は、トラフィックを脆弱性のあるMitelサーバーから被害者へ反射させ、その過程で送信されるトラフィック量を増幅（この特定のケースでは**増幅率2200倍**）させます。これについての詳細は、最新のブログ記事をご覧ください。

当社では、このような攻撃を当社のネットワーク上でいくつか観測しました。そのうちの1つは、Cloudflare Magic Transitサービスを利用している北米のクラウドプロバイダーを標的としたものでした。この攻撃は、主に米国、英国、カナダ、オランダ、オーストラリア、その他約20カ国からの100のソースIPを発信源としていました。ピーク時には50Mpps（～22Gbps）を超えましたが、Cloudflareのシステムによって自動的に検出、軽減されました。

1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

業種別ネットワーク層DDoS攻撃

ネットワーク層DDoS攻撃の多くは、CloudflareのIP範囲を直接ターゲットにしています。これらのIP範囲は、WAF/CDNのお客様、Cloudflareの権威DNS、CloudflareのパブリックDNSリゾルバー1.1.1.1、Cloudflare Zero Trust製品、および企業オフィスなどに提供されています。また、Spectrum製品を介してお客様に専用IPアドレスを割り当てたり、Magic Transit、Magic WAN、Magic Firewall製品を介して他社のIPプレフィックスをアドバタイズしてL3/4 DDoS攻撃対策にも使用しています。

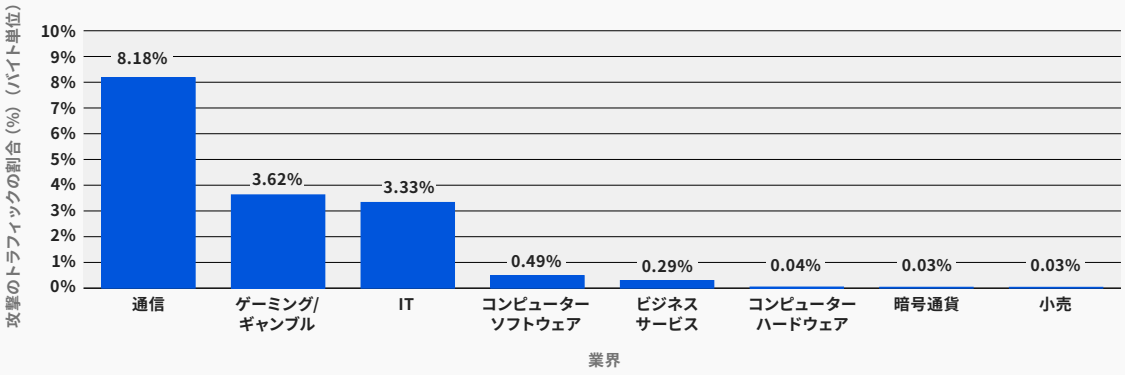
本レポートでは、SpectrumとMagic製品をご利用いただいているお客様の業界別に、初めてネットワーク層DDoS攻撃を分類するようにしました。このように分類することで、ネットワーク層DDoS攻撃によって最も標的とされている業界を把握することができます。

第1四半期の統計を見ると、Cloudflareのお客様に向けて発信された攻撃パケット数と攻撃バイト数から、電気通信業界が最も多く標的とされたことがわかります。Cloudflareが軽減した攻撃バイト数の全体の8%以上、攻撃パケット全体の10%が通信会社を標的としたものでした。

続く2位、3位に大きな違いは無く、「ゲーム／ギャンブル」「情報技術・サービス」となっています。

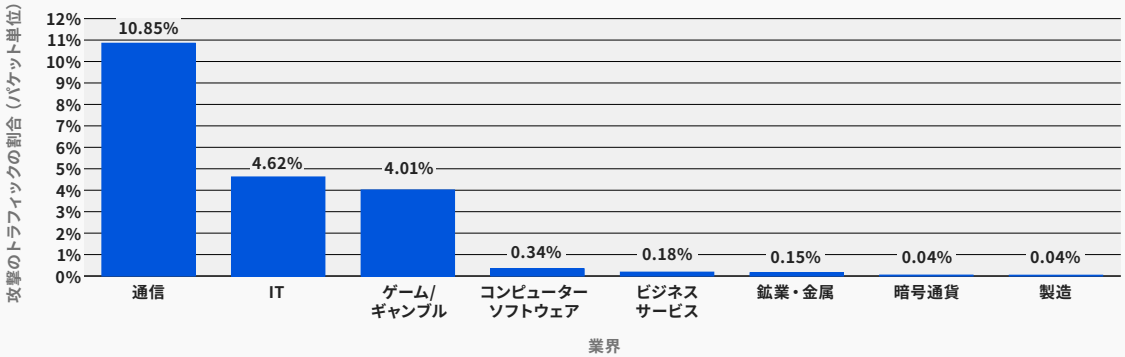
バイト数の業界別分布[1]

ネットワーク層DDoS攻撃のバイト数の業界別分布



パケット数の業界別分布[1]

ネットワーク層DDoS攻撃のパケット数の業界別分布



1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

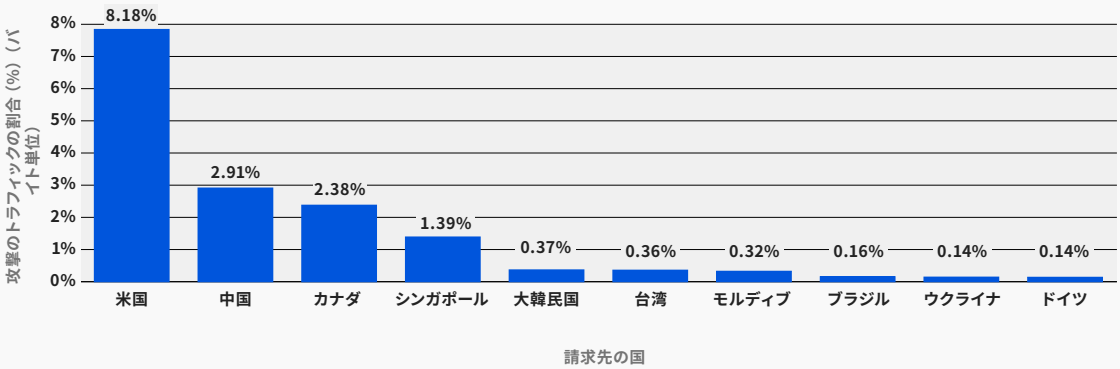
ネットワーク層DDoS攻撃＜標的国別＞

お客様の業種別の分類と同様に、アプリケーション層DDoS攻撃で行ったようにお客様の請求先国別に攻撃をバケット化して攻撃上位国を把握することも可能です。

第1四半期の数字を見ると、DDoS攻撃トラフィックのうち米国が最も高い割合で標的とされており、攻撃パケット全体の10%以上、攻撃バイト数の全体のほぼ8%を占めていることがわかります。米国に次いで、中国、カナダ、シンガポールとなっています。

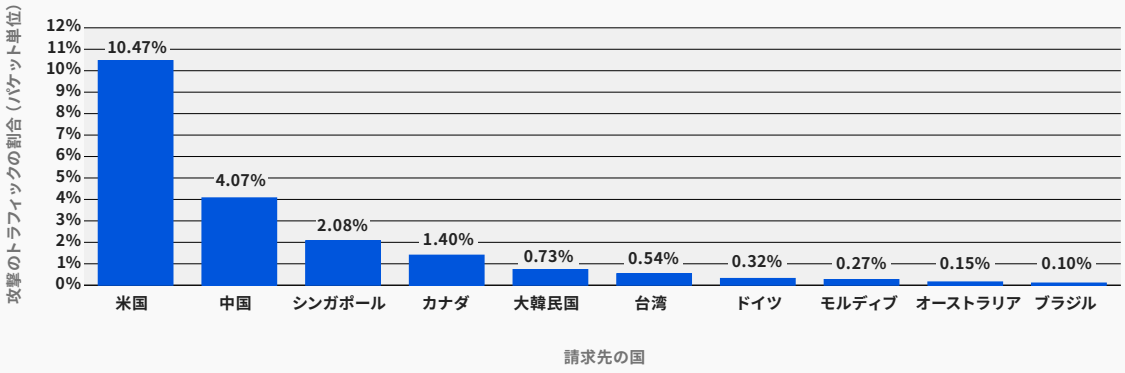
ターゲット国別のバイト数の分布[1]

ネットワーク層DDoS攻撃のバイト数の標的国別分布



ターゲット国別のパケット数の分布[1]

ネットワーク層DDoS攻撃のパケット数の標的国別分布



流入国別ネットワーク層DDoS攻撃

ネットワーク層DDoS攻撃の発生源を把握しようとする場合、アプリケーション層の攻撃解析と同じ方法は使えません。アプリケーション層DDoS攻撃を仕掛けるには、HTTP/S接続を確立するために、クライアントとサーバーの間でハンドシェイクを成功させる必要があります。ハンドシェイクを成功させるためには、攻撃者はその送信元IPアドレスをスプーフィングすることができません。攻撃者はボットネット、プロキシ、およびその他の方法を使用して身元を難読化することはできますが、攻撃側クライアントの送信元IPはアプリケーション層DDoS攻撃の発信源を正しく示すことになります。

1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

ネットワーク層DDoS攻撃＜流入国別＞（続き）

一方、ネットワーク層DDoS攻撃を仕掛けるには、ほとんどの場合ハンドシェイクは必要ありません。攻撃者は攻撃元を難読化し、攻撃特性にランダム性を導入するために、送信元IPアドレスをスプーフィングし、単純なDDoS防御システムでは攻撃をブロックしにくくすることができます。そのため、スプーフィングされた送信元IPに基づいて攻撃元の国を導き出した場合、「スプーフィングされた国」を得ることになります。

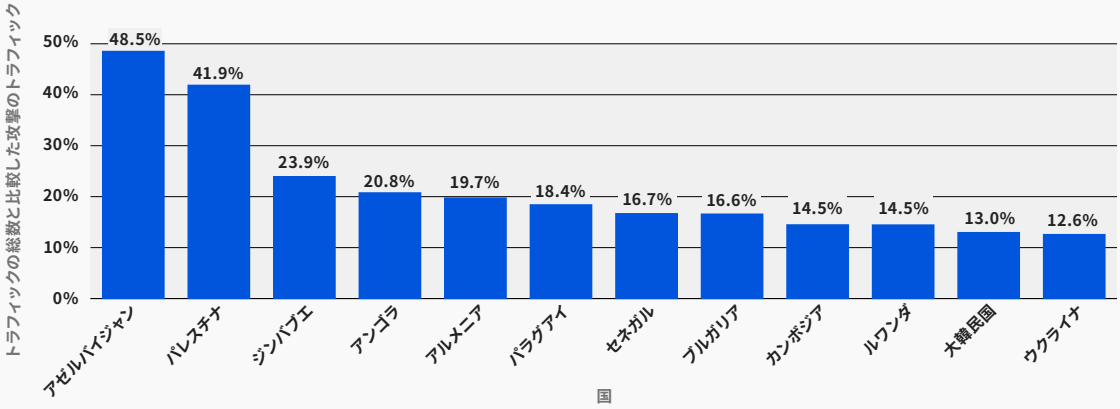
このため、ネットワーク層DDoS攻撃の発信源を分析する際には、攻撃の発信源を把握するためにスプーフィングされた（可能性のある）ソースIPではなく、トラフィックが取り込まれたCloudflareエッジデータセンターのロケーション別にバケットを構成します。世界270以上の都市にデータセンターがあるため、レポートで地理的な精度を実現できます。ただし、コスト削減から輻輳や障害管理まで、さまざまな理由でトラフィックがバックホールされ、さまざまなインターネットサービスプロバイダや国を経由してルーティングされる可能性があるため、この方法でも100%正確ではありません。

第1四半期において、アゼルバイジャンにあるCloudflareのデータセンターで検出された攻撃の割合は、前四半期比16,624%増、前年同期比96,900%増となり、ネットワーク層のDDoS活動の割合が最も高い国（48.5%）となっています。

アゼルバイジャンのデータセンターに続き、パレスチナのデータセンターでは、全トラフィックの41.9%という驚異的な割合でDDoSトラフィックが発生しています。これは、前四半期比110,120%増、前年同期比46,456%増となりました。

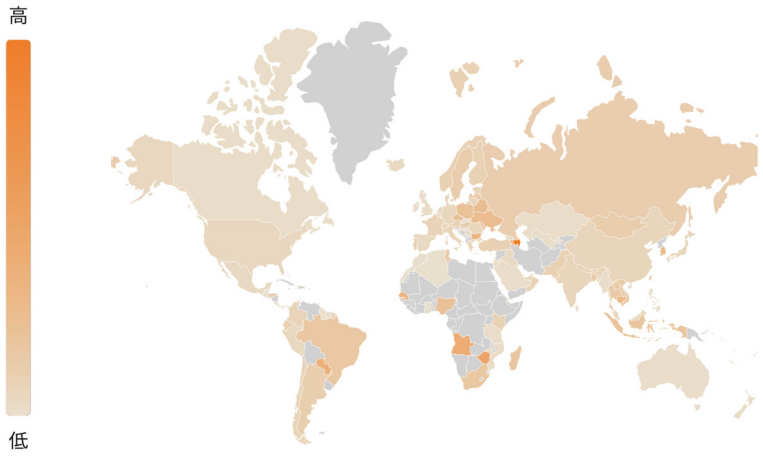
流入国別のバイト数の分布[1]

2022年第1四半期におけるネットワーク層DDoS攻撃の攻撃元の国別分布



1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

ネットワーク層DDoS攻撃＜流入国別＞（続き）



すべての地域と国を見るには、インタラクティブマップをご覧ください。

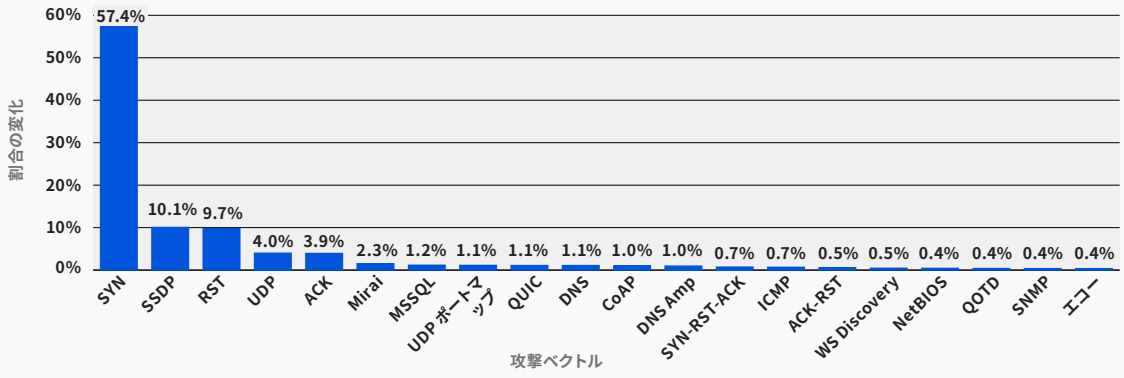
攻撃ベクトル

第1四半期では、一般的なUDPフラッドの使用が大幅に減少する一方で、SYNフラッドが依然として最も人気のあるDDoS攻撃ベクトルとなっています。

攻撃ベクトルとは、攻撃者がDDoS攻撃を行う際に用いる手法のことで、IPプロトコル、TCPフラグなどのパケット属性、フラッディング方法などの基準を示す言葉です。

第1四半期は、ネットワーク層へのDDoS攻撃全体の57%をSYNフラッドが占め、前四半期比69%増、前年同期比13%増となりました。2位はSSDPを使った攻撃で、前四半期比1,100%を超える急激な増加となりました。以下、RSTフラッドとUDPを使用した攻撃へと続きます。前四半期は汎用UDPフラッドが2位でしたが、今回は汎用UDP DDoS攻撃が前四半期の32%から87%減少し、わずか3.9%にとどまりました。

上位の攻撃ベクトル別の分布[1]
2022年第1四半期におけるネットワーク層DDoS攻撃の上位ベクトル



1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

新たな脅威

上位の攻撃ベクトルを特定することは、組織が脅威の状況を理解するのに役立ちます。そうすることで、これらの脅威から身を守るためにセキュリティ体制を強化することができます。同様に、まだ攻撃の大部分を占めていない新たな脅威について知ることは、それらが大きな力となる前に軽減するのに役立ちます。

第1四半期に新たに出現した攻撃ベクトルを見ると、Lantronix社のサービスのリフレクションDDoS攻撃（前四半期比971%増）やSSDPリフレクション攻撃（前四半期比724%増）が増加していることが確認できます。また、SYN-ACK攻撃は前四半期比437%増加し、ボットネット「Mirai」による攻撃は前四半期比321%増となりました。

攻撃者によるLantronix Discovery Serviceからのトラフィックの反射

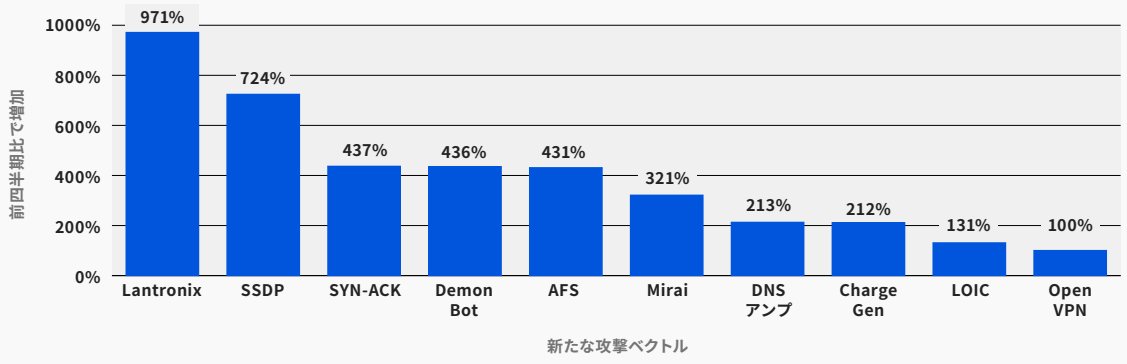
Lantronix社は、米国に拠点を置くソフトウェア／ハードウェア企業であり、Internet of Things（IoT）管理のためのソリューションを幅広く提供しています。同社がIoTコンポーネントを管理するために提供しているツールの1つが「Lantronix Discovery Protocol」です。これは、Lantronix社製のデバイスを検索して見つけるためのコマンドラインツールです。この検索ツールはUDPベースで動作するためハンドシェイクの必要がありません。

送信元IPはスプーフィング（なりすまし）が可能です。そのため、攻撃者はこのツールを使って、4バイトのリクエストで一般に公開されているLantronix社製のデバイスを検索することができ、その結果ポート30718から30バイトの応答が返されます。被害者の発信元IPをスプーフィングすることで、すべてのLantronix社製のデバイスは被害者をターゲットとした応答のリフレクション／アンプ攻撃をもたらします。

リフレクションDDoS攻撃に使用されるSimple Service Discovery Protocol

Simple Service Discovery Protocol（SSDP）プロトコルは、Lantronix Discoveryプロトコルと同様に動作しますが、ネットワーク接続されたプリンターなどのUniversal Plug and Play（UPnP）デバイスを対象としています。SSDPプロトコルを悪用することで、攻撃者はリフレクションベースのDDoS攻撃を発生させ、ターゲットのインフラストラクチャを過負荷状態にして、そのインターネットプロパティを停止させることができます。SSDPベースのDDoS攻撃についてはこちらをご覧ください。

上位の新たな脅威別の分布[1]
2022年第1四半期におけるネットワーク層DDoS攻撃の上位の新たな脅威



1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

ネットワーク層DDoS攻撃＜攻撃レート別＞

第1四半期には、パケットレートとビットレートの両方の観点から、ボリューム型DDoS攻撃が大幅に増加したことが確認されました。10Mppsを超える攻撃は前四半期比で300%以上増、100Gbpsを超える攻撃は前四半期比で645%増となりました。

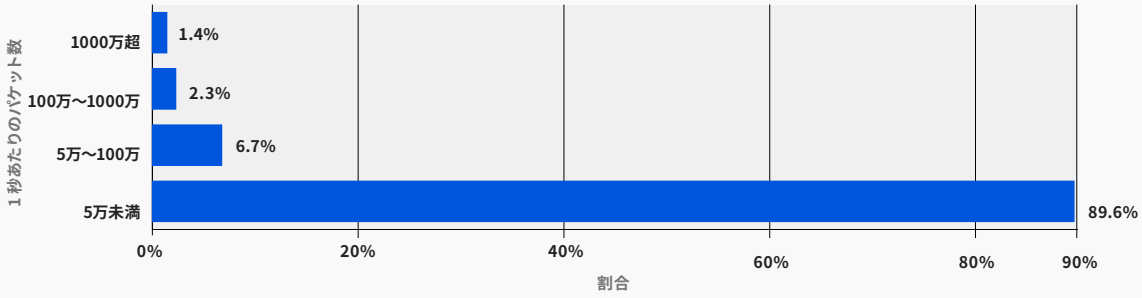
L3/4 DDoS攻撃の規模の測定には、さまざまな方法があります。1つは送信するトラフィックの量で、ビットレート（具体的にはテラビット/秒またはギガビット/秒）を使用して測定します。もう1つは送信するパケットの数で、パケットレート（具体的には、何百万パケット/秒）を使用して測定します。

ビットレートの高い攻撃は、インターネットリンクの閉塞を発生させることによってサービス妨害を起こそうとし、パケットレートの高い攻撃はサーバーやルーター、その他のインラインハードウェア機器を過負荷状態に陥れようとします。これらの機器は各パケットの処理に特定量のメモリと計算能力を割きます。そのため、多数のパケットが送り付けられると機器の処理リソースが枯渇してしまう可能性があります。その場合はパケットが「ドロップ」されます。つまり、機器がそれらを処理できない状態となるのです。ユーザーに対しては、サービスの中断や拒否になります。

パケットレート別分布

ネットワーク層DDoS攻撃の大半は、毎秒5万パケット以下にとどまっています。50kppsはCloudflareの規模では低い方ですが、それでも保護されていないインターネットのプロパティを簡単にダウンさせ、標準的なギガビットイーサネット接続でさえも輻湊させることができます。

パケットレート別分布[1]
2022年第1四半期におけるネットワーク層DDoS攻撃のパケットレート別分布

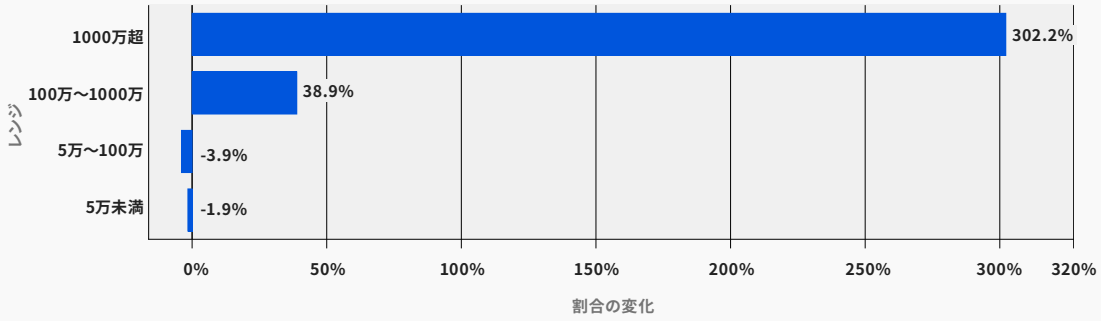


攻撃規模の推移を見ると、10Mppsを超える攻撃は前四半期比で300%以上増となっていることがわかります。同様に、1〜10Mppsの攻撃は前四半期比で40%近い増となっています。

1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

ネットワーク層DDoS攻撃＜攻撃レート別＞（続き）

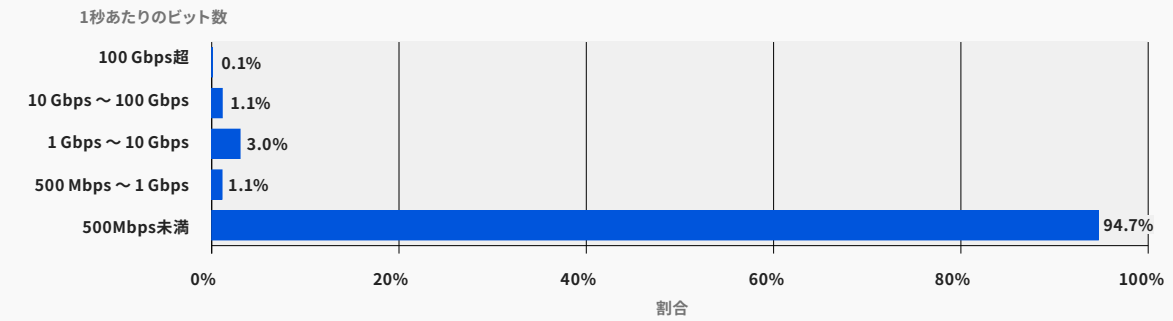
パケットレートの前四半期比[1]
ネットワーク層DDoS攻撃のパケットレート別分布の前四半期比の変化



ビットレート別分布

第1四半期は、ネットワーク層DDoS攻撃の大半が500Mbps未満にとどまっています。これもCloudflareの規模ではわずかなものですが、保護されていないインターネットプロパティをより少ない容量で即座に停止させたり、標準的なギガビットイーサネット接続でさえも輻湊させたりできます。

ビットレート別分布[1]
2022年第1四半期におけるネットワーク層DDoS攻撃のビットレート別分布

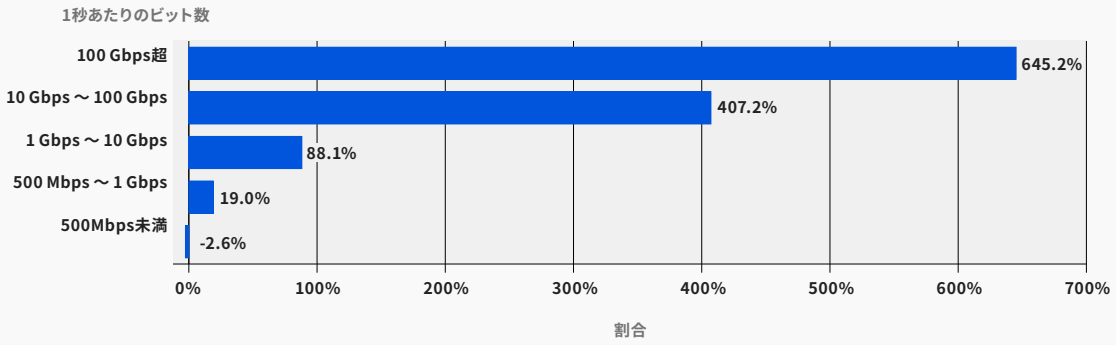


1秒あたりのパケット数の領域と同様に、ここでも大きな増加傾向が見られます。ピーク時に100Gbpsを超えるDDoS攻撃は前四半期比645%増、ピーク時の10Gbps～100Gbpsの攻撃は407%増、ピーク時の1Gbps～10Gbpsの攻撃は88%増、さらにピーク時の500Mbps～1Gbpsの攻撃は前四半期比で20%近い増となっています。

1. 出典： https://radar.cloudflare.com/notebooks/ddos-2022-q1

ネットワーク層DDoS攻撃＜攻撃レート別＞（続き）

ビットレートの前四半期比[1]
2022年第1四半期におけるネットワーク層DDoS攻撃のビットレート別分布



ネットワーク層DDoS攻撃＜継続時間別＞

ほとんどの攻撃は従来と同じく継続時間が1時間未満で、自動化されたDDoS軽減ソリューションを常にオンにしておく必要性を改めて感じます。

当社では、攻撃が当社のシステムによって最初に検出されたときと、特定のターゲットに向けた攻撃シグネチャを持つ最後のパケットを確認したときの差を記録することによって、攻撃の持続時間を測定しています。

以前のレポートでは、「1時間以内の攻撃」とそれ以上の時間範囲の内訳を示しました。しかし、多くの場合、90%以上の攻撃が1時間未満で終了しています。そこで、今回のレポートから、短時間の攻撃を分解し、より短い時間幅でグループ化することで、より粒度の高いレポートを提供するようにしました。

留意すべき重要な点は、たとえ数分間の攻撃であっても、それが成功すれば、その影響は最初の攻撃時間をはるかに超えて続く可能性があるということです。攻撃が成功した場合、対応するIT担当者はサービスの復旧に数時間から数日を費やすことがあります。

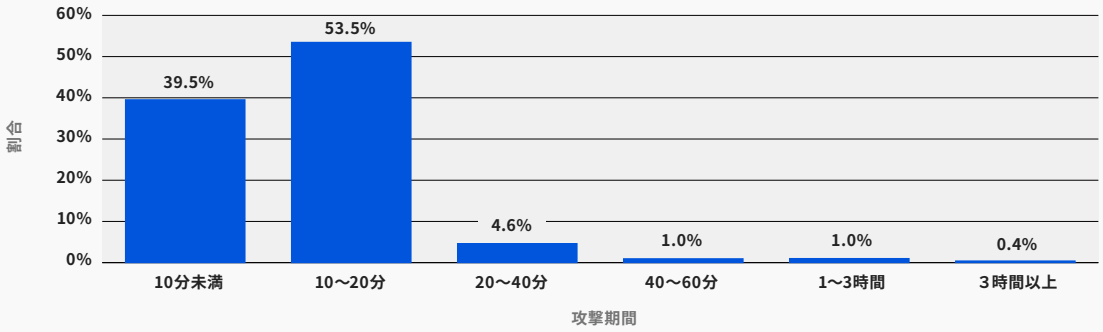
1. 出典：https://radar.cloudflare.com/notebooks/ddos-2022-q1

ネットワーク層DDoS攻撃＜継続時間別＞（続き）

2022年第1四半期では、半数以上が10～20分、約40%が10分以内に終了、さらに5%が20～40分、残りが40分以上続いています。

継続時間別分布[1]

2022年第1四半期におけるネットワーク層DDoS攻撃の継続時間別分布



特に、数秒間に大量のパケット、バイト、リクエストをターゲットに浴びせるバースト攻撃は、短時間の攻撃では容易に発見されない可能性があります。この場合、セキュリティ解析による手動での軽減に頼るDDoS攻撃対策サービスでは、攻撃の軽減措置が間に合いません。攻撃後の分析でそこから学び、攻撃固有のフィンガープリントをフィルタリングする新しいルールをデプロイし、次回の攻撃を捕らえることを期待するしかないのです。同様に、攻撃中にセキュリティチームがDDoSプロバイダーにトラフィックをリダイレクトする「オンデマンド」サービスの利用も、オンデマンドDDoSプロバイダーにトラフィックが転送される前に攻撃がすでに終了しているため、非効率的です。

企業は、トラフィックを分析し、短時間の攻撃をブロックするのに十分な速さでリアルタイムのフィンガープリントを適用する、自動化された常時稼働型のDDoS攻撃対策サービスを使用することが推奨されます。

1. 出典： https://radar.cloudflare.com/notebooks/ddos-2022-q1

まとめ

Cloudflareのミッションは、より良いインターネットの構築を支援することです。より良いインターネットとは、たとえDDoS攻撃に直面しても、誰にとっても、より安全で、より速く、より信頼できるインターネットです。ミッションの一環として、2017年以降、すべてのお客様に定額制で無制限のDDoS攻撃対策を無償で提供しています。ここ数年、攻撃者がDDoS攻撃を仕掛けることはますます容易になってきています。しかし、このように簡単になったからこそ、あらゆる規模の組織があらゆる種類のDDoS攻撃から身を守ることも、これまで以上に簡単かつ無料でできるようにしたいと考えています。

まだCloudflareをお使いでない方は、当社のFreeまたはProプランを使用したWebサイトの保護を今すぐ始めるか、Magic Transitを使用したお客様のネットワーク全体の包括的なDDos攻撃対策に関してお問い合わせください。

CLOUDFLAREのセキュリティインサイト