本調査結果は、総務省の「令和5年度 重要IoT機器のセキュリティ対策に係る調査の請負」事業（受託者：株式会社三菱総合研究所）により作成したものを、総務省で公表するものです。

本資料に関するお問合せ等は総務省サイバーセキュリティ統括官室までお願いいたします。

メールアドレス:notice@ml.soumu.go.jp

DDoS攻撃の傾向と対策について

三菱総合研究所

先進技術・セキュリティ事業本部

2024年3月

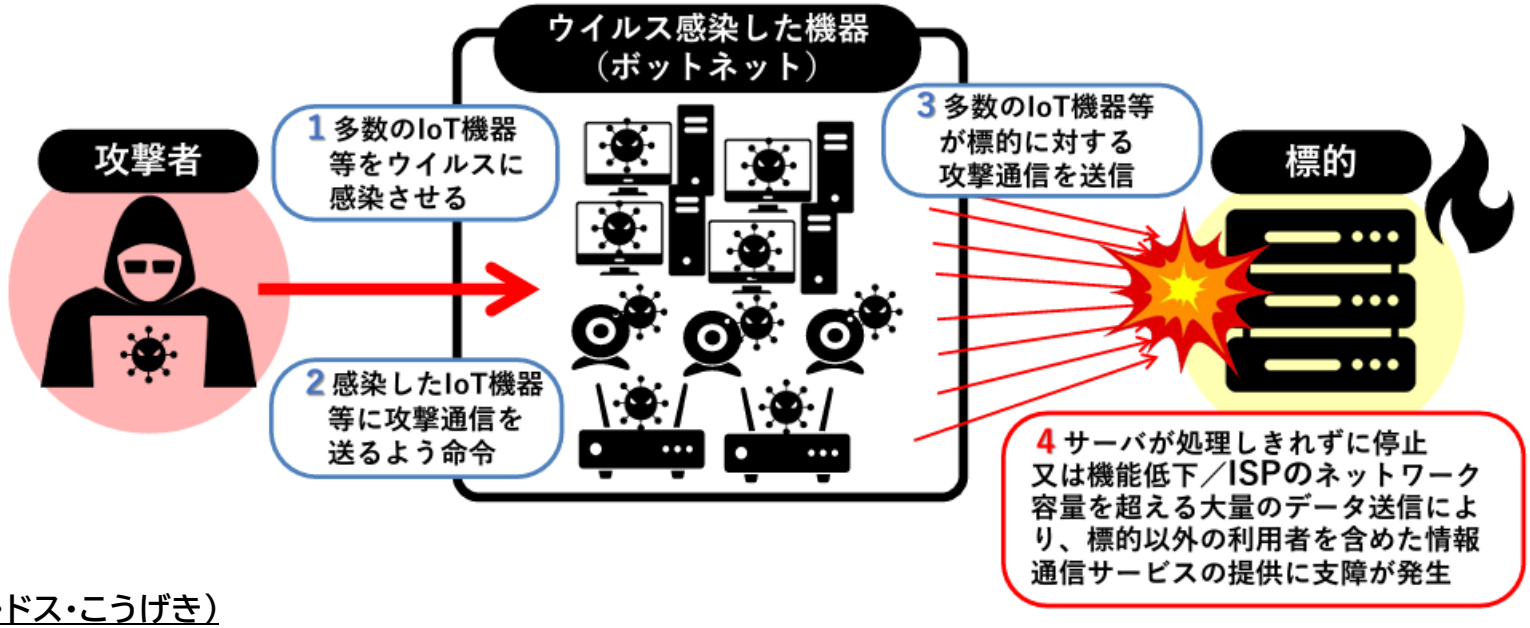
＊本資料は、総務省事業「令和5年度DDoS攻撃の俯瞰的な把握に関する調査請負」の成果を基に作成しました。

本資料について

DDoS（分散型サービス妨害）攻撃は、オンラインサービスやウェブサイトに対する重大な脅威です。効果的なDDoS対策を構築するためには、最近の攻撃傾向や影響を理解し、それに対する適切な対策を講じることが重要です。本資料はステークホルダでDDoS対策を検討するうえで参考となる情報を提供します。

DDoS攻撃の定義と概要

- インターネットは、今やあらゆる社会経済活動を支える基盤であり、インターネットの利用により経済活動や国民生活の利便性の向上が期待されています。一方で、このようなインターネット利用の普及に伴って、企業、個人、政府組織を狙ったサイバー攻撃が顕在化するとともに、情報通信技術の発展も相まって、DDoS攻撃やマルウェアの感染活動等、サイバー攻撃の手法そのものも巧妙化、複雑化している状況にあります。



DDoS攻撃（ディー・ドス・こうげき）
Distributed Denial of Service attack（ディストリビューテッド・デナイアル・オブ・サービス・アタック）。分散サービス拒否攻撃のこと。Webサーバやメールサーバなどに対して、複数のコンピュータから大量のサービス要求のパケットを送りつけることで、相手のサーバやネットワークに過大な負荷をかけ、使用不能にします。同様の攻撃方法であるDoS攻撃は1台のコンピュータから実行するものですが、DDoS攻撃の場合は、例えば第三者のコンピュータをボットに感染させておくなどして、攻撃者の指示によって複数のコンピュータ（ボット）が一斉に攻撃します。

出所）国民のためのサイバーセキュリティサイト ｜ 用語辞典（英字）｜ 国民のためのサイバーセキュリティサイト
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/glossary/glossary_11.html#DDoS%E6%94%BB%E6%92%83%EF%BC%88%E3%83%87%E3%82%A3%E3%83%BC%E3%83%BB%E3%83%89%E3%82%B9%E3%83%BB%E3%81%93%E3%81%86%E3%81%92%E3%81%8D%EF%BC%89

DDoS攻撃の影響と被害

- DDoS攻撃は、複数のコンピュータから同時に攻撃を仕掛けることによって、ウェブサーバーの機能を停止するサイバー攻撃です。以下に、DDoS攻撃がもたらす主な影響と被害について説明します。

サービスの中断

- DDoS攻撃により、ウェブサイトやオンラインサービスが利用できなくなる可能性があります。これは、特にオンラインショッピングサイトなどを運営している場合、営業ができないことによって売上の低下などの被害が発生します。

信用の喪失

- サービスの停止期間が長引けば、会社の信用の喪失に繋がります。ウェブでのビジネスでは信頼度の高さがそのまま売上にも直結するため、信用低下による経済的損失は想像以上に大きくなります。

復旧費用

- DDoS攻撃を受けると、サーバーの復旧作業が必要となります。これには、人的・金銭的・時間的リソースが割かれることになります。

他のシステムへの踏み台

- 攻撃者によってボットウイルスを送り込まれ、自分がボットネットの一員となってしまうというものです。ボットネットとは、攻撃者によって制御を奪われたコンピュータの集まりで、数千～数十万というネットワークから構成されていることもあります。攻撃者はボットに一斉に指令を送り、外部の他の組織に対して大規模なDDoS攻撃を行ったり、スパムメールを送信したりすることもあります。

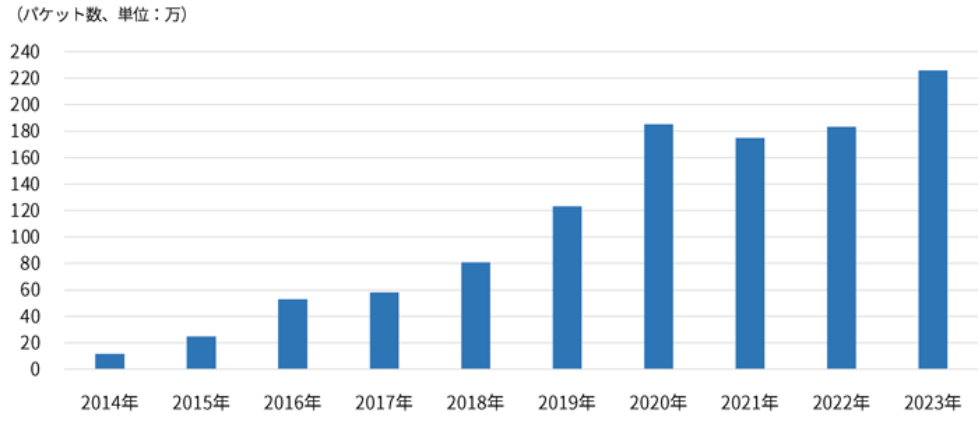
2023年に観測されているパケットの傾向

- 1 IPアドレス当たりの年間総観測パケット数は、前年の2022年から更に増加しており、インターネット上を飛び交う探索活動が更に活発化していることが、数字から読み取れます。
- 総観測パケットに占める海外組織からの調査目的と見られるスキャンの割合は、2022年の54.9%から更に増加し、63.8%を占めました。調査機関によるスキャンパケットが半数以上を占める傾向は、2019年以降継続していますが、その割合は年々増加する傾向が続いています。

NICTERダークネット観測統計(過去10年間)

年	年間総観測パケット数	ダークネットIPアドレス数	1IPアドレス当たりの年間総観測パケット数
2014	約241.0億	212,878	115,335
2015	約631.6億	270,973	245,540
2016	約1,440億	274,872	527,888
2017	約1,559億	253,086	578,750
2018	約2,169億	273,292	806,877
2019	約3,756億	309,769	1,231,331
2020	約5,705億	307,985	1,849,817
2021	約5,180億	289,946	1,747,685
2022	約5,226億	288,042	1,833,012
2023	**約6,197億**	**289,686**	**2,260,132**

IPアドレス当たりの年間総観測パケット数(過去10年間)

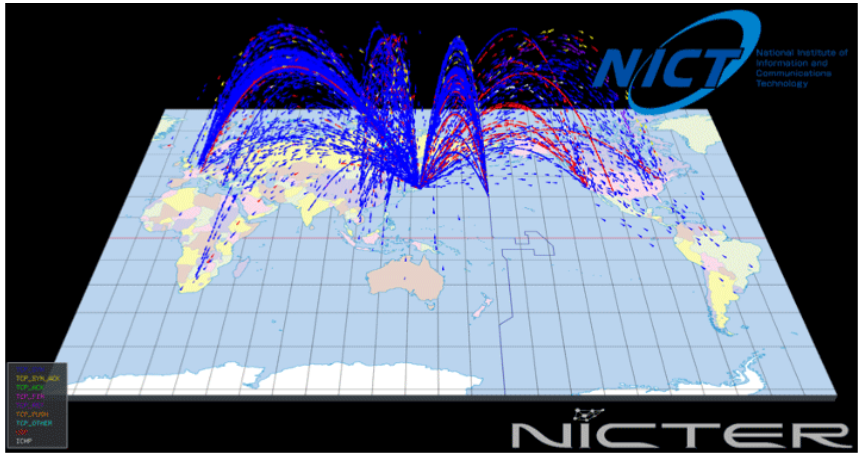


出所)NICTER観測レポート2023の公開 | 2024年 | NICT-情報通信研究機構 https://www.nict.go.jp/press/2024/02/13-1.html

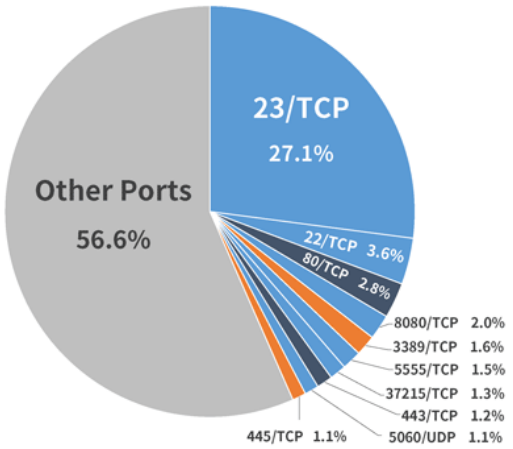
攻撃対象の上位10位の傾向

- 2023年にNICTERで観測した主な攻撃対象（宛先ポート番号）の上位10位までを表したものが右図です。円グラフの水色の部分が、**Webカメラやホームルータなどの**IoT機器**に関連したサイバー攻撃関連通信**です。
- 上位10位までのポートが全体に占める割合は、2022年とほぼ同じでしたが、**IoT機器が使用する特徴的なポート**番号宛ての通信が上位に多く観測される傾向が継続しました。

NICTER Atlasによるダークネットで観測された通信の可視化



宛先ポート番号別パケット数分布（調査目的のスキャンパケットを除く）



宛先ポート	攻撃対象
23/TCP	Telnet（ルータ，Webカメラ等）
22/TCP	SSH（サーバ，ルータ等）
80/TCP	HTTP（Webサーバ）
8080/TCP	HTTP（Web管理画面）
3389/TCP	Remote Desktop
5555/TCP	ADB（Android）
37215/TCP	Huawei 製ルータ
443/TCP	HTTPS（Webサーバ）
5060/UDP	SIP
445/TCP	Windows SMB

宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

- 個別の観測事象に目を転じると、2021年以降継続して観測されている**韓国製DVR製品のMiraiへの感染**に加え、モバイル回線に接続された複数のLTEルータがMiraiに感染し、**DDoS攻撃の踏み台として悪用**される事象が観測されました。
- DRDoS攻撃の観測では、**絨毯爆撃型DRDoS攻撃が頻繁に発生**したため、年間の攻撃件数が2022年の3,465万件から5,561万件へと大幅に増加しました。不適切な設定で外部に公開されている**IoT機器のサービスを悪用したDoS攻撃が観測**されました。

出所）NICTER観測レポート2023の公開｜2024年｜NICT-情報通信研究機構　https://www.nict.go.jp/press/2024/02/13-1.html

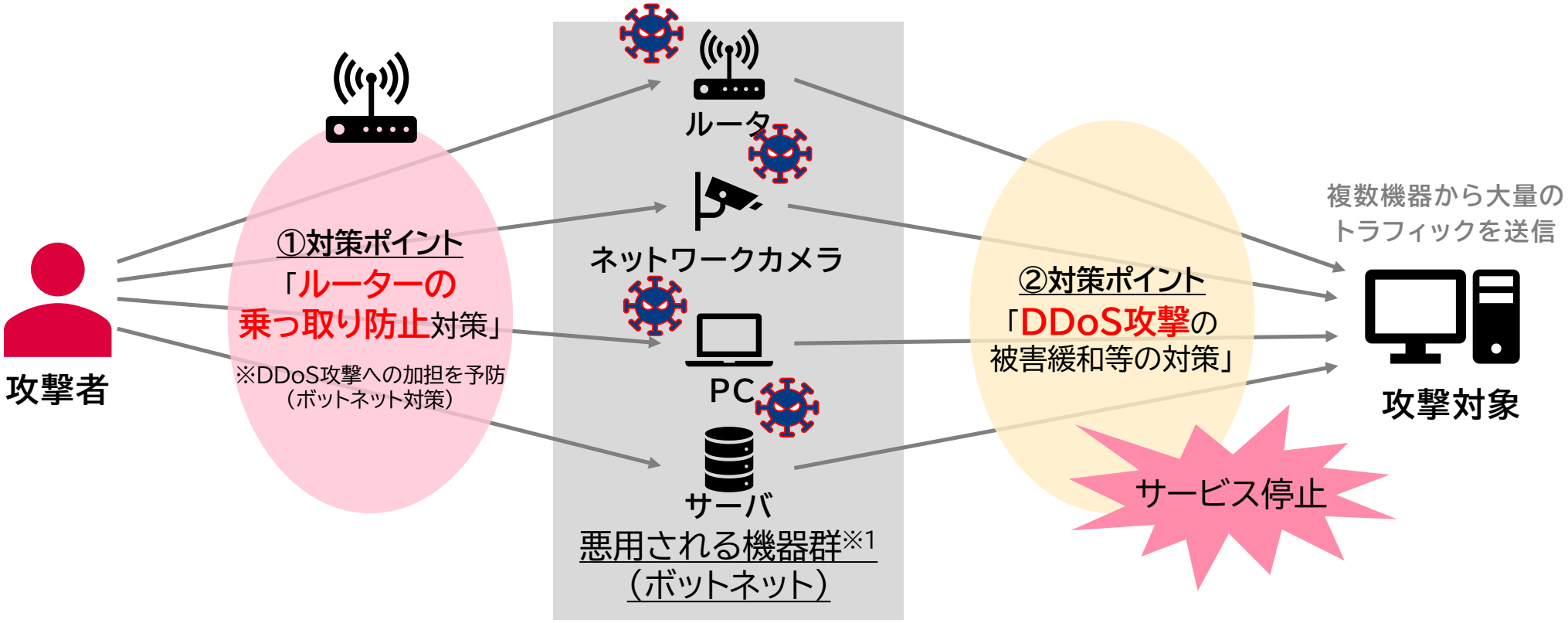
近年のDDoS攻撃の事例（2022年～2023年）

- 近年においても世界各地でDDoS攻撃に起因する具体的な被害が発生しています。Google Cloudの事例やENISA、Akamai、Cloudflareなどの調査によると、攻撃規模は拡大し、攻撃手法も巧妙化しています。2023年もDDoS攻撃の脅威は依然として高く、企業や組織は十分な対策を講じる必要があります。

情報源	発生時期	内容	URL
Google Cloud	2023年8月	・Google Cloudのインフラ やGoogleサービスを標的とした、**過去最大規模（398Mrps）**のDDoS攻撃。 ・アプリケーション攻撃のうち、新たな手法である**HTTP/2ラピッドリセット攻撃**が行われたと考えられている。	[1]
ENISA	2023年8月	・ポーランドの鉄道システムを標的とした無線によるDoS攻撃。 ・攻撃者は、無線通信に暗号化がなされていないことを利用して、列車の停止信号を送信し停止させた。	[2]
ニュースサイト	2023年6月	・Microsoftのサービス（Azure、OneDrive、Outlook）を標的とした**アプリケーション攻撃（具体的には、HTTP（S）flood 攻撃、キャッシュバイパス、Slowlorisなど）**であり、これらのサービスにおいて**一時的な障害が発生**した。 ・Microsoftによれば、Killnetとつながりがあるとされるロシア系グループであるStorm-1359により、**ボットネット等を介して、複数のクラウドサービスと公開プロキシから**DDoS攻撃が行われた。	[3]
Akamai	2023年2月	・Akamaiで保護されているサイトを標的とした、アジア最大規模（ピーク時に**900Gbps、158Mpps**）のDDoS攻撃。 ・発信元の国別内訳は上位から、香港、**東京**、サンパウロ、シンガポール、**大阪**であった。**ボットネットが用いられた**とされる。	[4]
Cloudflare	2023年2月	・Cloudflareで保護されているHTTP/2ベースのWebサイトを標的とした、**過去最大規模（71Mrps）**のDDoS攻撃。2022年6月にGoogleに対するDDoS攻撃で**46Mrps**が記録されている。 ・**発信元は多数のクラウドサービスプロバイダ**であり、3万を超えるIPアドレスから発信された。	[5]
FISC（FISAC）	2022年9月	・主に中国を標的とした、国内の**IoTボットネット（Fodcha**と推定）による大規模なDDoS攻撃であり、国内の特定の通信事業者で9月20日から9月28日にかけて**全国的な通信障害**が発生した。 ・この事業者の特定のWiFi ルータがボットに感染し、DDoS 攻撃のトラフィックを発生させた結果、上位の通信回線の停止や速度制限が行われた。	[6]
ニュースサイト	2022年9月	・e-Gov等の政府サイト等にDDoS攻撃による閲覧障害が発生。ハッカー集団「キルネット」が犯行声明。 ・一連の攻撃は最大100Gbpsで、発信元のIPアドレスは数万件に上り、ほとんどが海外からと考えられている。	[7]
ニュースサイト	2022年7月	・親ロシアのハクティビスト集団であるkillnetのDDoS攻撃により、リトアニアの**Secure National Data Transfer Network等の一部で接続障害**が発生。	[8]
FISC（FISAC）	2022年3月	・2021年12月頃から確認され、国内でも**監視カメラ等 IoT機器に広く感染しているボットであるRapprbot**による、DDoS 攻撃トラフィック（主に国内発、海外宛）が大規模化した。 ・ロシアによるウクライナ侵攻以降はロシア向けの攻撃が増加した。	[9]
ニュースサイト	2022年3月	・ウクライナの大手通信事業者Ukrtelecomに対するDDoS攻撃で、**15時間の接続サービス停止**が発生。 ・攻撃の詳細は不明ながら、**WordpressのPingbackを利用したアンプ攻撃**が用いられたとの報道が一部でなされている。	[10]

ルーター等の乗っ取り防止・DDoS攻撃の被害緩和

- DDoS攻撃とは、IoT機器等の複数機器から分散的にDoS（サービス拒否）攻撃を仕掛ける手法です。
- 対策すべきポイントは①ルーターの乗っ取り防止対策し、DDoS攻撃への加担を予防（ボットネット対策）
- ② DDoS攻撃の被害緩和等の対策があります。



※1：攻撃者に悪用されるパターンとしては、「マルウェアを利用し、機器を乗っ取り後、DDoS攻撃を行うケース」及び「偽装したIPアドレスを利用、リフレクション攻撃を行うケース」がある。
本章では、双方のケースを想定したうえで、対策を以降のスライドへ整理する。

下記を基に筆者作成
・NTT Communications、「DDoS攻撃とは？ 意味と読み方、対策方法」、https://www.ntt.com/business/services/network/internet-connect/ocn-business/bocn/knowledge/archive_18.html
・CYBER SECURITY CLOUD、「DoS攻撃・DDoS攻撃とは？意味と対策方法をわかりやすく解説」、 https://www.shadan-kun.com/waf_websecurity/dos_ddos_attack/

ウェブカメラやルータが乗っ取られないための対策

- 家庭のネットワークに侵入し、IoT機器を不正に操作しようとするサイバー攻撃を防ぎ、安心して安全にIoT機器を利用するために、日ごろから次のような対策を講じましょう。

ソフトウェアは常に最新のものにする
ソフトウェア（ファームウェア）は定期的にアップデートしましょう。自動更新機能がある場合は有効化しておくと、常に最新の状態にすることができます。

パスワードは複雑なものに変更する
初期設定の簡単なパスワードのまま使わず、複雑なパスワードに変更しましょう。また、設定を見直し、使わない機能は無効化しましょう。

使用していないIoT機器はインターネットに接続しない（電源を切る）
インターネットの接続を必要な場合に限ることでマルウェアの感染活動に対する影響を最低限に抑えることができます。また、マルウェアによっては電源を切ることでリセットされ駆除される場合があります。

出所）ウェブカメラやルータが乗っ取られる？IoT機器のセキュリティ対策は万全ですか？ | 政府広報オンライン https://www.gov-online.go.jp/useful/article/202005/1.html

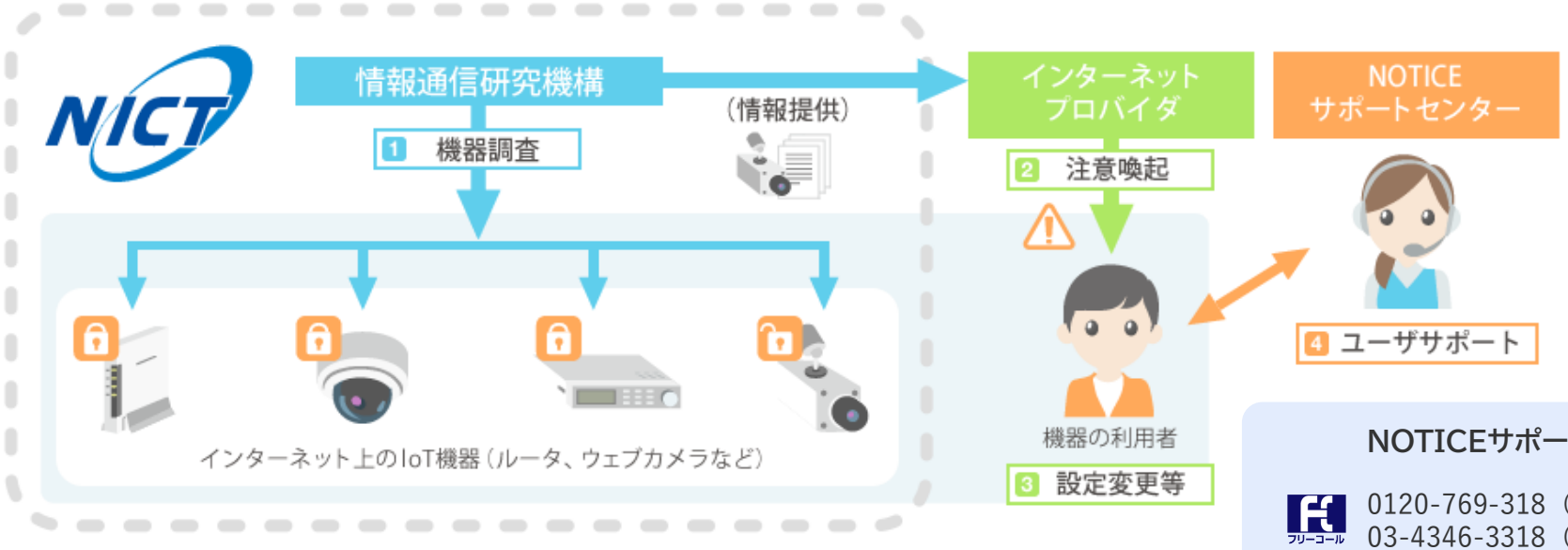
IoT機器の乗っ取りを対策するための「安全な管理方法」

- IoT機器やルーター等を安全に管理するためには、以下の対策が必要です。
  具体的な設定・確認方法は、「ルーター / ネットワークカメラの安全な管理方法」をご覧ください。
  https://notice.go.jp/safety

出所）ルーター / ネットワークカメラの安全な管理方法 | NOTICE　https://notice.go.jp/safety

サイバー攻撃に悪用されるおそれのある機器の注意喚起

- インターネットプロバイダは、NICTから受け取った情報を元に当該機器の利用者を特定し、電子メールや郵送などにより注意喚起を行います。
- 注意喚起を受けた利用者は、注意喚起の内容やNOTICEサポートセンターサイトの説明などに従い、パスワード設定の変更、ファームウェアの更新など適切なセキュリティ対策を行っていただくようお願いします。



NOTICEサポートセンター

フリーコール
0120-769-318（無料・固定電話のみ）
03-4346-3318（有料）
受付時間 10:00～18:00
年末年始（12/29～1/3）を除く
ウェブからのお問い合せは以下のページから
お問い合せフォーム

出所）NOTICE｜サイバー攻撃に悪用されるおそれのあるIoT機器の調査、注意喚起を行うプロジェクト　https://notice.go.jp/

IoT機器メーカー/ルーター・メーカーが利用者に提供すべき機能や情報

- 利用開始時や設置時だけではなく、利用中も含む機能・情報の提供が必要です。

項目	対策詳細
ルーター/IoT機器の乗っ取り防止対策	**1）安全性の高いIoT機器の選定** IoT機器へ事前に定めたセキュリティバイデザインの基準を適用する、及び要求を満たすIoT機器の利用・設定方法を利用者に提供・周知する
	2）ルータアクセス制御 ACL設定で特定のパケットを破棄する等の機能を提供し、設定方法を利用者に提供・周知する
	3）初期パスワードの変更 初期設定されているパスワードは必ず変更する機能を提供し、設定方法を利用者に提供・周知する
	4）不要なポート/サービスの停止 使わないポートやサービスを停止する情報を提供し、設定方法を利用者に提供・周知する
	5）未使用IoT機器の電源オフ 使わないIoT機器は、電源を切ることを利用者に周知する
	6）問合せ窓口の事前確認・サポート終了製品の買い替え検討 不具合発生時の問合せ窓口を利用者に周知する
	7）サポート終了製品の買い替え検討 サポートが終了した場合は買い替えを検討することを利用者に周知する
	8）設定の見直し パスワード、アカウント、アクセスやタイムアウト等を設定方法を利用者に提供・周知する

サーバー運用及び管理に求められる定常的な対策

- サーバーの運用・管理については、サーバー悪用されないために、定常的な対策が求められます。
  また、DDoS攻撃の被害緩和策として各種システムやサービスの導入・利用が求められます。

項目	対策詳細
乗っ取り・悪用防止対策	1）オープン・リゾルバ対策 外部の不特定のIPアドレスからの再帰的な問い合わせを許可しない
	2）DNSキャッシュでの検索拒否 DNSキャッシュサーバ上で攻撃用ドメインの検索を拒否する
	3）セキュリティパッチ適用・ファームウェア更新 OSやアプリケーションの脆弱性を解消するためのパッチを適用し、かつIoT機器のファームウェアを定期的に更新して最新の状態を保つ
	4）フィルタリングの設定（イングレスフィルタリング）※4 自組織から送信元IPアドレスを詐称したパケットの送信を許可しない
DDoS攻撃の被害緩和対策	5）CDNの導入 通信をキャッシュサーバへ転送し、DDoS攻撃による影響を抑止する
	6）WAFの導入 アプリケーションへの不正通信を検知・遮断し、DDoS攻撃による影響を抑止する
	7）DDoS対策サービスの導入 ベンダーが提供するDDoS対策サービスを導入し、DDoS攻撃による影響を抑止する
	8）サーバ設定の見直し 同一IPアドレスからのアクセス回数やタイムアウト等を設定する

各種の防止・影響緩和対策だけではなくユーザへの周知も重要

- ISPがルーターの乗っ取りとDDoS攻撃を防ぐための基本的な対策内容を示します。
（詳細は、本資料4章をご参考ください）
さらに、ユーザーのデバイスとネットワークのセキュリティの周知も求められます。

- **ルーターの乗っ取り防止対策**: ファームウェアの定期的な更新と脆弱性スキャン、セキュアな管理インタフェースの設定と強力なパスワードの推奨、不正なトラフィックを検出するための監視とアラート機能の実装。

- **DDoS攻撃の被害緩和対策**: ルーターでのトラフィックフィルタリングとブロッキング、DDoS攻撃のトラフィック分析などを含むシステムの導入、分散型のDDoS防御サービスとの提携。

- **セキュリティサービスの提供及び強化**: 法人向けまたはビジネスユーザーに対しては、上記に関するセキュリティ対策サービスの提供や強化及びベストプラクティスの提供。

- **ユーザーへの啓蒙**:セキュリティに関する情報提供を行い、ホームネットワークと含むコンシューマ/パーソナルユーザーに対しては、上記のセキュリティサービスの提供とともにのセキュリティ意識を高めることや、ルーターのパスワード管理やファームウェアアップデートなどの基本的なセキュリティ対策を周知する。

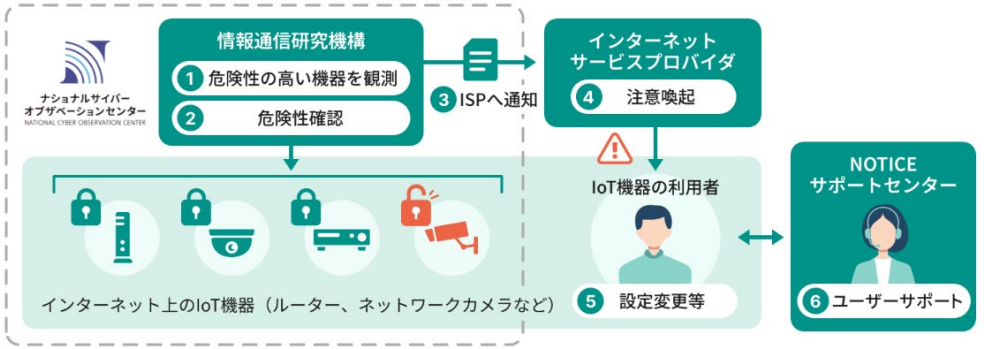
危険性が高いIoT機器の観測と利用者への注意喚起

- ISPが総務省NOTICE活動による危険性が高いIoT機器の利用者への注意喚起を行うことは、サイバーセキュリティ対策における重要な責務であると同時に、事業者としてのメリットがあります。

1. 早期発見・早期対策による被害の抑制
   - NOTICE活動により、脆弱なIoT機器が特定されると、ISPは自社ネットワーク上の該当機器を迅速に把握できます。これにより、ISPは利用者にすぐに注意喚起し、脆弱性対策を促すことができ、サイバー攻撃の被害を未然に防ぐことができます。

2. 信頼関係の構築と顧客満足度の向上
   - 利用者のIoT機器は意図せず攻撃に加担する可能性があります。ISPがNOTICE活動を通じて積極的に情報提供し、これらのリスクを共有することで、透明性と迅速な対応姿勢を示せます。これは利用者との信頼関係を築き、顧客満足度を向上させることにつながります。

3. 社会全体におけるサイバーセキュリティ強化
   - IoT機器がサイバー攻撃の標的となることが増えています。NOTICE活動は、ISPやメーカー、販売事業者、利用者が協力して、IoT機器のセキュリティ対策を推進する枠組みを提供します。この連携により、サイバーセキュリティが強化され、ISPは自社ネットワークのリスクを低減し、法令遵守や社会貢献を果たし、競争力を高めることができます。



出所）NOTICE｜サイバー攻撃に悪用されるおそれのあるIoT機器の調査、注意喚起を行うプロジェクト　https://notice.go.jp/

①DDoS攻撃への加担を予防(ボットネット対策)の詳細(1/2)

対策詳細	対象					
	IoT機器(ルーター、NWカメラ等)	サーバ※1	PC	ISP※2のネットワーク	CSP※3のプラットフォーム	ドメイン
1.1 オープン・リゾルバ対策 外部の不特定のIPアドレスからの再帰的な問い合わせを許可しない	●	●				
1.2 DNSキャッシュでの検索拒否 DNSキャッシュサーバ上で攻撃用ドメインの検索を拒否する	●	●				
1.3 セキュリティパッチ適用・ファームウェア更新 OSやアプリケーションの脆弱性を解消するためのパッチを適用し、かつIoT機器のファームウェアを定期的に更新して最新の状態を保つ	●	●	●			
1.4 フィルタリングの設定(イングレスフィルタリング)※4 自組織から送信元IPアドレスを詐称したパケットの送信を許可しない	●					
1.5 安全性の高いIoT機器の選定 IoT機器へ事前に定めたセキュリティバイデザインの共通基準を適用する、または要求を満たすIoT機器を選定する	●					
1.6 ルータアクセス制御 ACL設定で特定のパケットを破棄する	●					
1.7 初期パスワードの変更 初期設定されているパスワードは必ず変更する	●					

※1:CSPのIaaS上でユーザが構築したサーバも含む、※2:ISPは「インターネットサービスプロバイダ」、CSPは「クラウドサービスプロバイダ」を意味する、※3:CSPが主体となる対策範囲はユーザ及びCSPが連携する事業者との責任範囲の分担に基づき、決定される、※4:対策1.4は送信元IPアドレスを詐称することでアクセス制限を回避する「隠れオープンリゾルバ探索」にも有効である

以下および三菱総合研究所知見を基に三菱総合研究所が作成
- 警察庁、DDoS 攻撃への対策について、https://www.npa.go.jp/bureau/cyber/pdf/20230501.pdf
- 警視庁、ボットネット対策、https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/botnet.html
- 警視庁、家庭用ルーターの不正利用に関する注意喚起について、https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/router.html
- 総務省、クラウドサービス提供における情報セキュリティ対策ガイドライン(第3版)、https://www.soumu.go.jp/main content/000771515.pdf

①DDoS攻撃への加担を予防（ボットネット対策）の詳細（2/2）

対策詳細	対象					
	IoT機器（ルーター、NWカメラ等）	サーバ※1	PC	ISP※2のネットワーク	CSP※3のプラットフォーム	ドメイン
1.8 未使用IoT機器の電源オフ 使わないIoT機器は、電源を切る	●					
1.9 問合せ窓口の事前確認・サポート終了製品の買い替え検討 不具合発生時の問合せ窓口を事前確認し、サポートが終了した場合は買い替えを検討する	●					
1.10 設定内容の定期的な確認 見覚えのない設定変更がなされていないか定期的に確認する	●					
1.11 IP53B（Inbound Port 53 Blocking） ISP事業者が自社の動的IPアドレス宛てのUDP53ポートへのアクセスを予めブロックする				●		
1.12 ブラックホールルーティング 攻撃者が使用するC&Cサーバ等、特定IPアドレス宛てのトラフィックを全て破棄する				●		
1.13 Abuse対応 クラウド上の不適当な振る舞いへ対応する（Abuse窓口の用意、対応体制の構築等）				●	●	
1.14フロー情報分析によるC&Cサーバの検知及び共有（総務省による実証事業中） フロー情報の分析を通じて、サイバー攻撃の指令元であるC&Cサーバを検知する				●		

以下および三菱総合研究所知見を基に三菱総合研究所が作成
- 警察庁、DDoS 攻撃への対策について、https://www.npa.go.jp/bureau/cyber/pdf/20230501.pdf
- 警視庁、ボットネット対策、https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/botnet.html
- 警視庁、家庭用ルーターの不正利用に関する注意喚起について、https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/router.html
- 総務省、クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）、https://www.soumu.go.jp/main_content/000771515.pdf

②被害の予防・事後対応の詳細(1/2)

対策詳細	対象					
	IoT機器（ルーター、NWカメラ等）	サーバ	PC	ISPのネットワーク	CSPのプラットフォーム	ドメイン
被害の予防						
2.1 CDNの導入 通信をキャッシュサーバへ転送し、DDoS攻撃による影響を抑止する		●			●	
2.2 WAFの導入 アプリケーションへの不正通信を検知・遮断し、DDoS攻撃による影響を抑止する		●			●	
2.3 DDoS対策サービスの導入 ベンダーが提供するDDoS対策サービスを導入し、DDoS攻撃による影響を抑止する		●			●	
2.4 サーバ設定の見直し 同一IPアドレスからのアクセス回数やタイムアウト等を設定する		●				
2.5 可用性の規定・実現 サービスの稼働率を規定した上で、複数のリソースを事前準備することで、障害発生時もサービス継続を実現する					●	
2.6 悪性ドメイン解消 攻撃用の悪性ドメインをなくす						●

以下および弊社知見を基に筆者作成

- 警察庁、DDoS 攻撃への対策について、https://www.npa.go.jp/bureau/cyber/pdf/20230501.pdf
- 警視庁、ボットネット対策、https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/botnet.html
- 警視庁、家庭用ルーターの不正利用に関する注意喚起について、https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/router.html
- 総務省、クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）、https://www.soumu.go.jp/main_content/000771515.pdf

②被害の予防・事後対応の詳細(2/2)

対策詳細	対象					
	IoT機器 (ルータ、 NWカメラ等)	サーバ	PC	ISPのネットワーク	CSPのプラットフォーム	ドメイン
事後対応及びその準備						
2.6 ブラックホールルーティング DDoS攻撃対象となっているサーバ等、特定IPアドレス宛てのトラフィックを全て破棄する(正規ユーザの通信も破棄される恐れあり)				●		
2.7 ルータアクセス制御 ACL設定で特定のパケットを破棄する	●					
2.8 システムの重要度に基づく選別と分離 システムの重要性に応じて対応方針(ネットワーク分離等)を策定する		●				
2.9 稼働・障害監視 平常時から通信を監視し、異常通信発生時には組織内の担当者や利用者に通知する		●			●	
2.10 ソーリーページ等の設定 サービス提供が困難な場合、SNSでの通知や別サーバに準備したソーリーページの表示を行う		●			●	

以下および弊社知見を基に筆者作成

- 警察庁、DDoS 攻撃への対策について、https://www.npa.go.jp/bureau/cyber/pdf/20230501.pdf
- 警視庁、ボットネット対策、https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/botnet.html
- 警視庁、家庭用ルーターの不正利用に関する注意喚起について、https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/router.html
- 総務省、クラウドサービス提供における情報セキュリティ対策ガイドライン(第3版)、https://www.soumu.go.jp/main content/000771515.pdf

［参考情報］

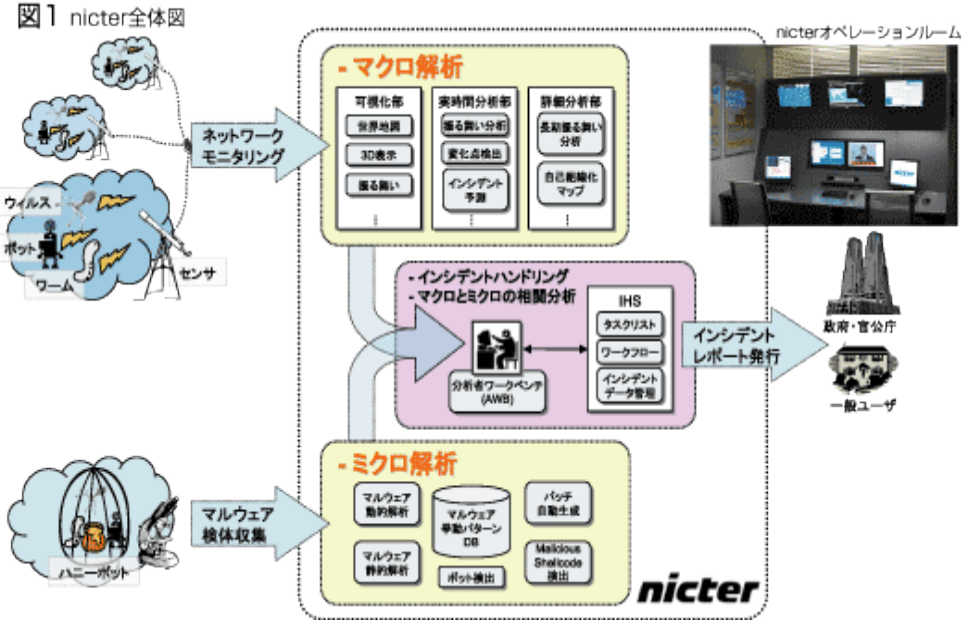
DDoS攻撃の傾向について

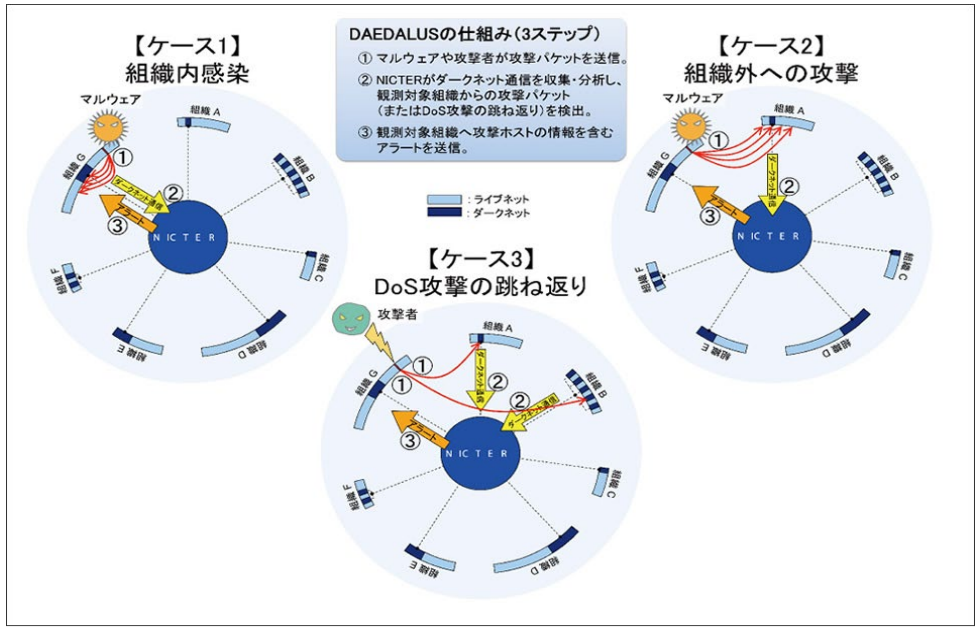
傾向 ・・・ DDoS関連の傾向を示す情報（2022年以降）

TOPIC ・・・ DDoS関連のTOPIC傾向を示す情報（2022年以降）

［観測システム］NICT:NICTER

- NICTはNICTERという無差別型サイバー攻撃の動向を把握するための観測システムを保有しており、ダークネットを大規模に観測している。
- また、アラートシステムのDAEDALUSも保有しており、対象の組織について組織内のマルウェアによる感染活動や、組織外への感染活動、組織外から受けているDDoS攻撃のバックキャストなどをNICTERが観測すると、当該組織へ迅速にアラートを出すことが可能である。
- NICTERの詳細な仕様は公開されていない。





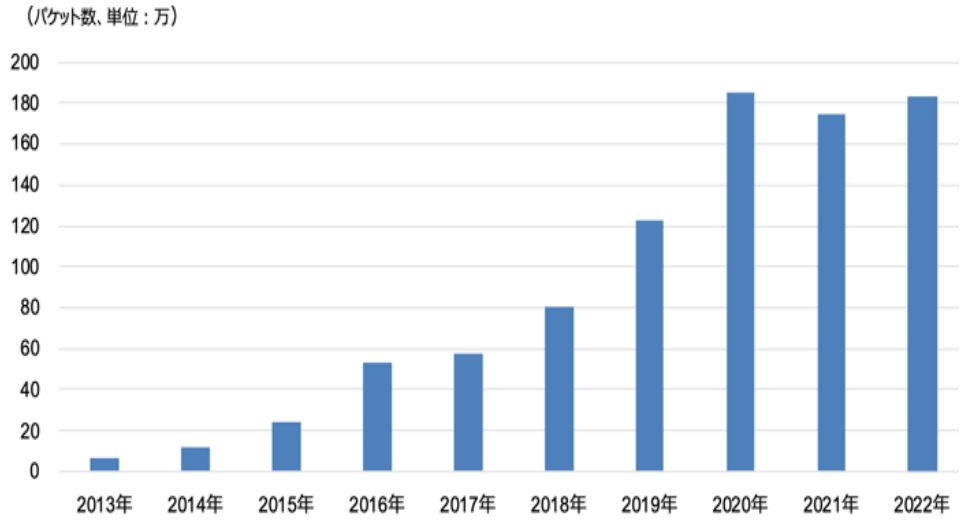
NICTER，NICT NEWS,https://www.nict.go.jp/publication/NICT-News/0607/research/index.html,プレスリリース ｜ 対サイバー攻撃アラートシステム“DAEDALUS”（ダイダロス）の外部展開を開始！ ｜ NICT-情報通信研究機構 https://www.nict.go.jp/press/2012/06/06-1.html，2023/11/14アクセス

傾向

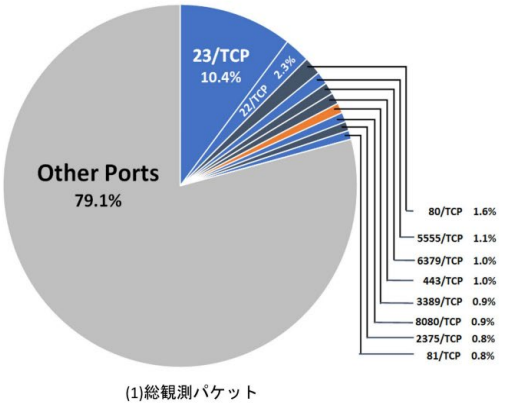
NICTER観測レポート2022　ダークネット観測

- NICTERのダークネット観測網にて2022年に観測されたサイバー攻撃関連通信は合計5,226億パケットで2021年とほぼ同じ水準で推移。
  - 観測したパケットのうち約54.9%が海外組織からの調査目的とみられるスキャンパケット。
  - 攻撃目的のパケットのうち23.0%がTelnet(23/TCP)パケットで、昨年度の11.0%から増加している。

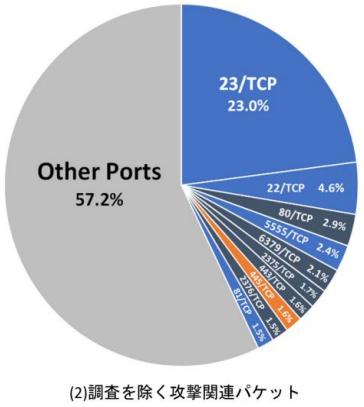
NICTERのダークネット観測網にて観測されたパケットの推移



観測されたパケットの分布



(1)総観測パケット



(2)調査を除く攻撃関連パケット

NICTER観測レポート2022の公開｜2023年｜NICT-情報通信研究機構 https://www.nict.go.jp/press/2023/02/14-1.html
https://csl.nict.go.jp/report/NICTER_report_2022.pdf

TOPIC

NICTER観測レポート2022　IoTボットの感染活動（DVR/NVR機器への感染）

- 日本国内におけるMirai感染ホスト数の日ごとの推移は、2022年の初めは1日当たり数百台程度で推移したが、4月24により増加し、それ以降、感染ホスト数は一日当たり1千から5千程度で推移。
  - 4月24日の増加を受けて5月12日にMirai感染ホストを調査したところ、確認された1,217台の感染ホストのう631台が韓国メーカ数社のDVR/NVR機器であった。
  - NICTはこれを受けて当該の韓国製DVR/NVR製品を調査し、確認された脆弱性をJVNに通知し、また当該機器を販売する日本国内の複数の販売代理店に連絡することで、ファームウェアの修正に協力した。

日本国内のMiraiの感染ホストの推移

NICTで調査した韓国製DVR/NVR機器の例

製造元	筐体（一例）	管理ログイン画面
FocusH&S		
Rifatron		
Pinetron		
CTRing		
ITX		

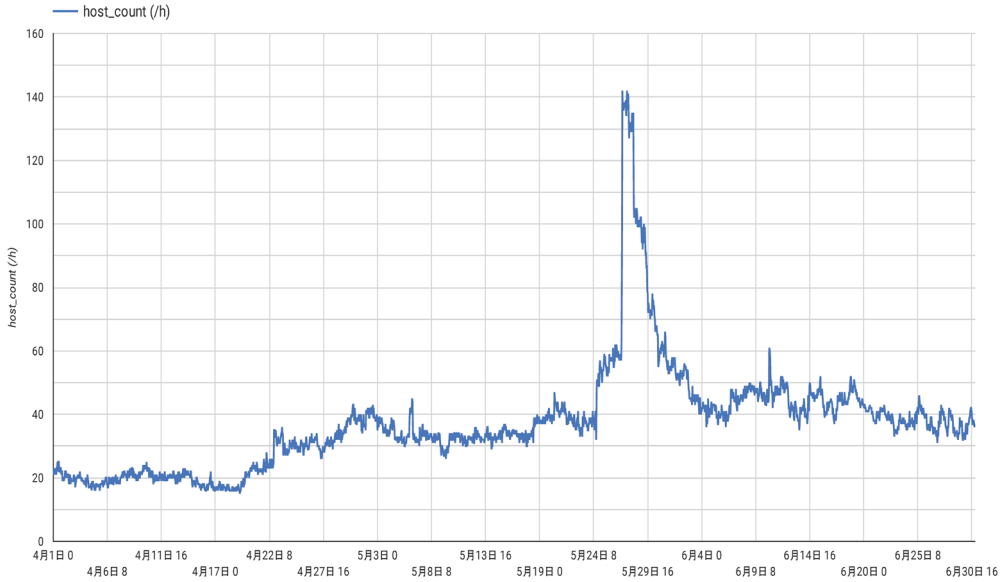
NICTER観測レポート2022の公開 | 2023年 | NICT-情報通信研究機構 https://www.nict.go.jp/press/2023/02/14-1.html
https://csl.nict.go.jp/report/NICTER_report_2022.pdf

TOPIC

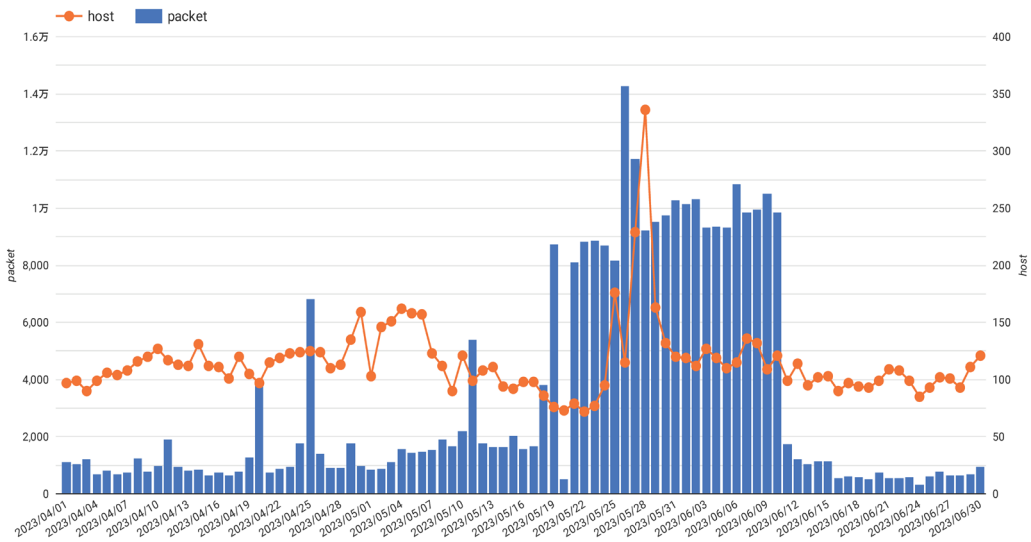
NICTER観測統計 - 2023年4 月～6月　台湾メーカ製 DVR機器へのMirai感染

- 2023年5月27日ごろから日本国内の特定の法人系のプロバイダにおいてMiraiの感染ホスト数の増加を観測。
  - 感染ホストについて調査をしたところ、台湾のDVR機器であった。
  - 同時期に、NICTERは51101/TCP宛のパケット数および送信元ホスト数の増加も観測。送信元ホストを調査すると5140/TCP, 51101/TCP から連番で複数のポートが開いており、5140/TCP にアクセスする際に index.php を指定すると、台湾の DVR ベンダ NUUO の 管理画面が表示された
  - DVR機器の設置業者もしくは管理者が当該DVR機器に脆弱なパスワードを設定していた、もしくは使いまわしていた可能性が考えられる。

プロバイダにおけるMiraiの感染ホスト数(/時)



51101/TCP宛送信元ホスト数とパケット数の推移(/日)



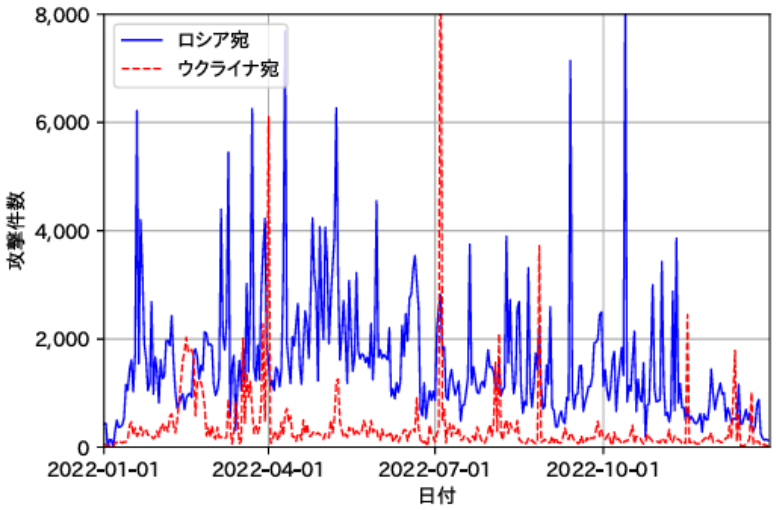
NICTER観測統計 - 2023年4 月～6月 - NICTER Blog
https://blog.nicter.jp/2023/08/nicter_statistics_2023_2q/

傾向

NICTER観測レポート2022の公開　DRDoS攻撃観測

- DRDoS攻撃観測では、攻撃件数の減少、攻撃時間の増加、攻撃に悪用されるサービスの種類の増加を観測。
  - DRDoS攻撃の観測では、大規模な絨毯爆撃型のDRDoS攻撃の規模の縮小によるDRDoS攻撃件数の減少、攻撃の継続時間の長時間化、及び攻撃に悪用されるサービスの種類の増加といった傾向の変化が見られた。
  - DRDoS攻撃の観測では、2021年に多く見られた絨毯爆撃型のDRDoS攻撃の規模が縮小し、その結果、DRDoS攻撃件数が減少して2020年の水準に戻ったほか、1時間以上継続した攻撃の割合が前年の約2.9%から約16%へと増加し、攻撃に悪用されるサービスの種類についても前年の38種類から151種類に増加するといった傾向の変化が見られた。

ロシア・ウクライナに関連するDRDoS攻撃の観測事例



KillnetによるDRDoS攻撃事例

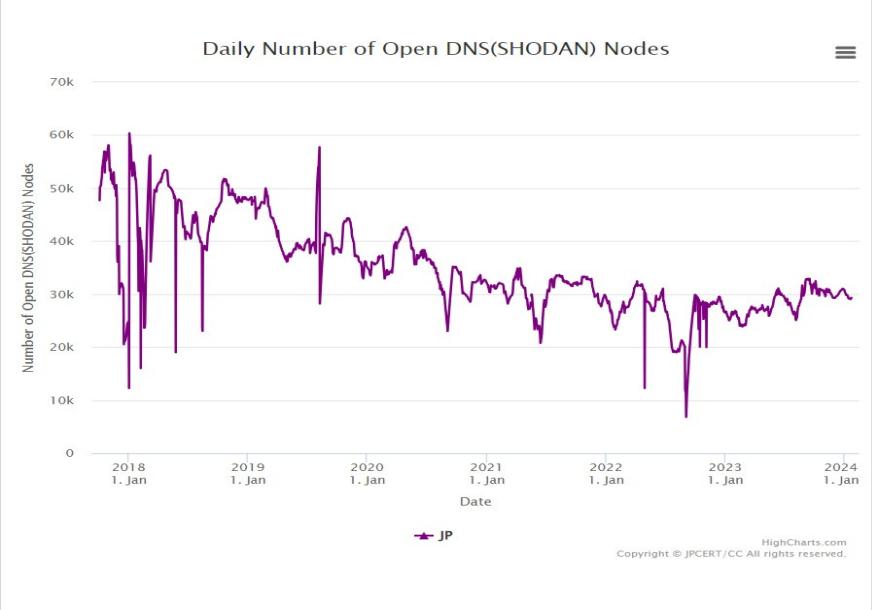
攻撃対象	悪用されたサービス	攻撃時刻（JST）
政府系サイト 1	DNS	2022-09-06 13:47～13:48 2022-09-06 16:32～17:32
政府系サイト 2	DNS	2022-09-06 13:48～13:49 2022-09-06 16:31～17:31
政府系サイト 3	DNS	2022-09-06 13:49～13:51
政府系サイト 4	DNS	2022-09-06 13:50～13:51
クレジットカード会社	DNS	2022-09-06 17:15～18:15
通販会社 1	DNS	2022-09-06 20:40～20:49
通販会社 1 の別サイト	DNS	2022-09-06 21:43～21:50
検索サイト	DNS	2022-09-06 20:55～21:24
無料通話アプリ	DNS	2022-09-06 21:52～21:54
無料通話アプリの API サーバ 1	DNS	2022-09-06 21:54～22:00
無料通話アプリの API サーバ 2	DNS	2022-09-06 21:55～22:00
管理組合サイト	DNS	2022-09-06 22:12～23:12
動画サイト	DNS SNMP	2022-09-06 23:51～09-07 00:42 2022-09-07 01:54～01:55
鉄道会社 1	SNMP	2022-09-07 19:17～19:20
鉄道会社 2	DNS	2022-09-07 21:07～22:08

NICTER観測レポート2022の公開｜2023年｜NICT-情報通信研究機構 https://www.nict.go.jp/press/2023/02/14-1.html
https://csl.nict.go.jp/report/NICTER_report_2022.pdf

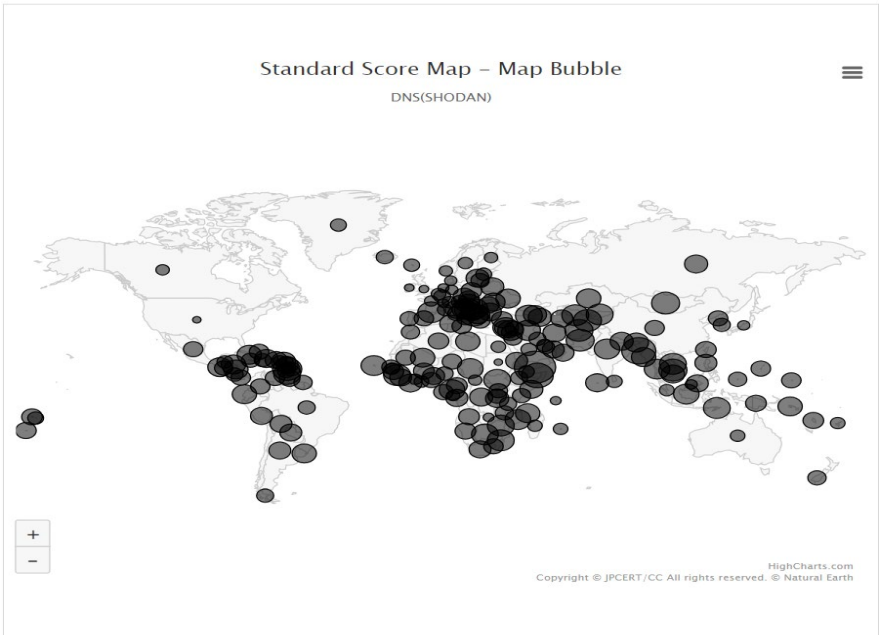
［観測システム］JPCERT/CC：インターネットリスク可視化サービス―Mejiro―

- インターネットリスク可視化サービス―Mejiroとは、インターネット上のリスク要因に関するデータを収集し、国・地域別の指標を計算して可視化するサービスである。
- 国・地域別のリスク要因の数と当該国・地域に割り当てられたIPアドレスの数を両対数グラフによる回帰直線からの乖離を偏差値として計算し、リスク指標としている。（Mejiro指標）
- ShodanやCensys等のスキャンサーバを使い、オープンな機器の状況を調べることで、国・地域別のリスク要因の数を調べている。

日本国内のオープンリゾルバー数の時系列推移



各国のオープンリゾルバー数のMejiro指標のバブルマップ



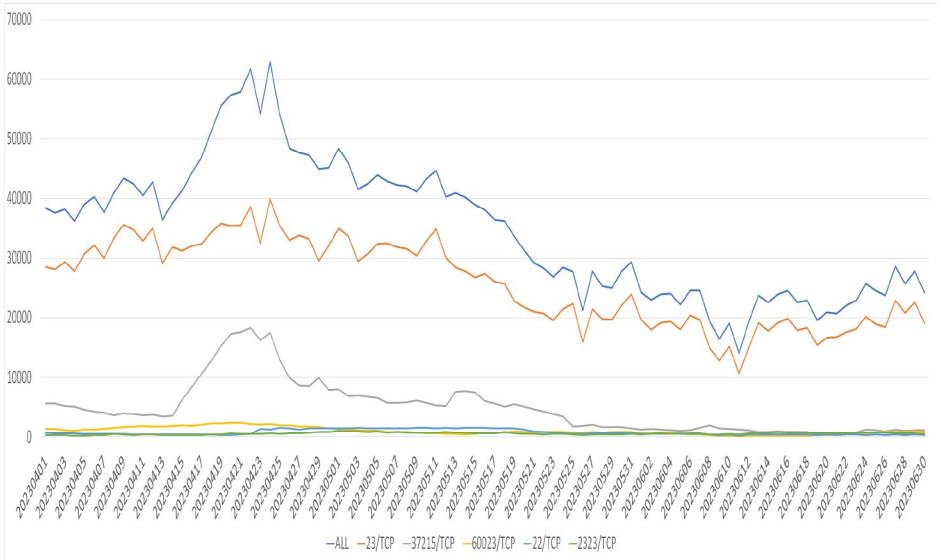
実証実験:インターネットリスク可視化サービス―Mejiro―
https://www.jpcert.or.jp/mejiro/#

TOPIC

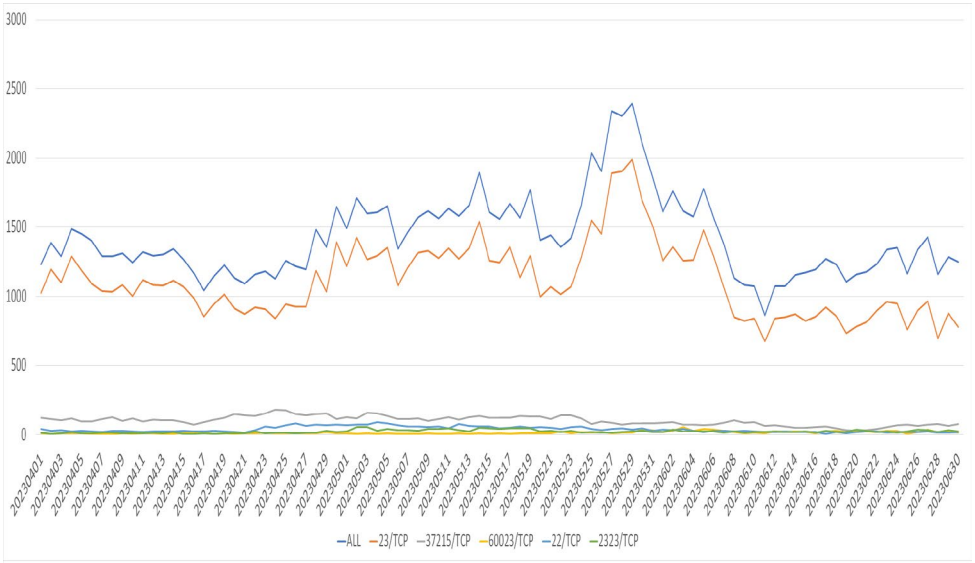
JPCERT/CC:インターネット定点観測レポート（2023年 4～6月）

- Miraiの感染活動との関連性が推測される特徴を持つパケットを継続的に観測
  - 海外からの37215/TCP宛のパケットは、4月14日頃から増え、4月20頃のピーク以降は減少。60023/TCP宛のパケットについても4月20日頃をピークにゆるやかに減少。
  - 探索元日本のパケットについて、37215/TCP宛は、国内からの探索が4月に僅かに増えたものの、海外からの探索程には目立った変化がなく、その後はいずれも徐々に減少。
  - 攻撃者が探索対象とする機器を変化させながら機器の探索や攻撃を行いマルウェアの感染をさせていると推測し探索対象のサービスの時間的な変化の分析を試みたが、その結果からは攻撃対象機器の変化を読み取ることはできなかった。

探索元海外のMiraiの特徴を持つパケットの推移



探索元日本のMiraiの特徴を持つパケットの推移

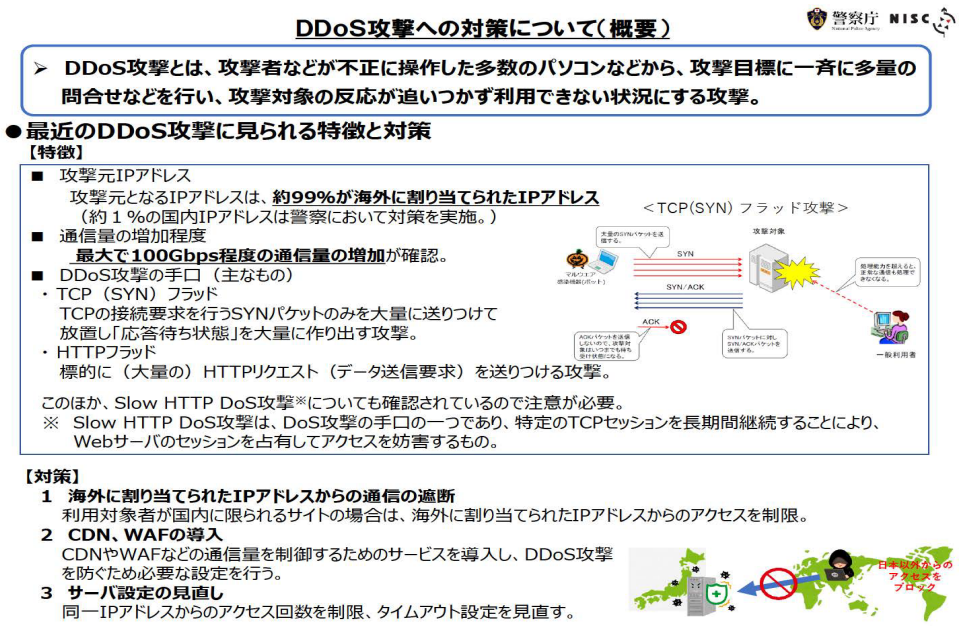


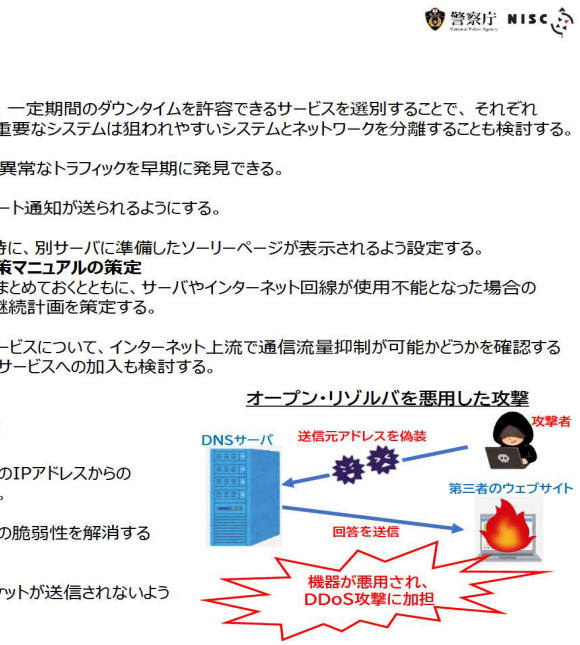
インターネット定点観測レポート（2023年 4～6月）
https://www.jpcert.or.jp/tsubame/report/report202304-06.html

TOPIC

警視庁：令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について

- **2023年上半期において、DDoS攻撃による被害とみられるウェブサイトの閲覧障害が複数発生した。**
  - 2月から3月にかけて、政府機関や重要インフラ事業者等を含む複数 の組織・団体等のウェブサイトにおいて閲覧障害が断続的に発生。同じ頃、SNS上に親ロシア派ハッカー集団からの犯行をほのめかす投稿が確認された。
  - 3月から6月にかけては、DNS権威サーバーを狙ったランダムサブドメイン攻撃によるとみられるウェブサイトの閲覧障害が断続的に発生した。
  - 5月、政府機関が運営するウェブサイトに閲覧障害が発生し、同じ頃、SNS上にハクティビストと思料されるアカウントからの犯行をほのめかす投稿が確認された。
- **2023年5月、警視庁はNISCと連名で重要インフラ事業者等のウェブサイトへDDoS攻撃に関する注意喚起を行った。**





令和5年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

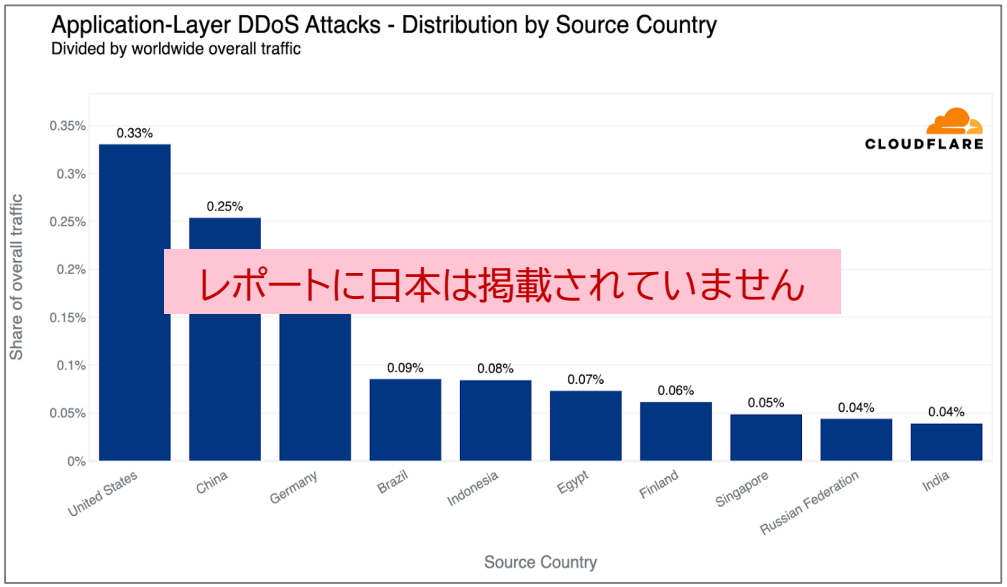
傾向

Cloudflare 2023年第2四半期DDoS脅威レポート

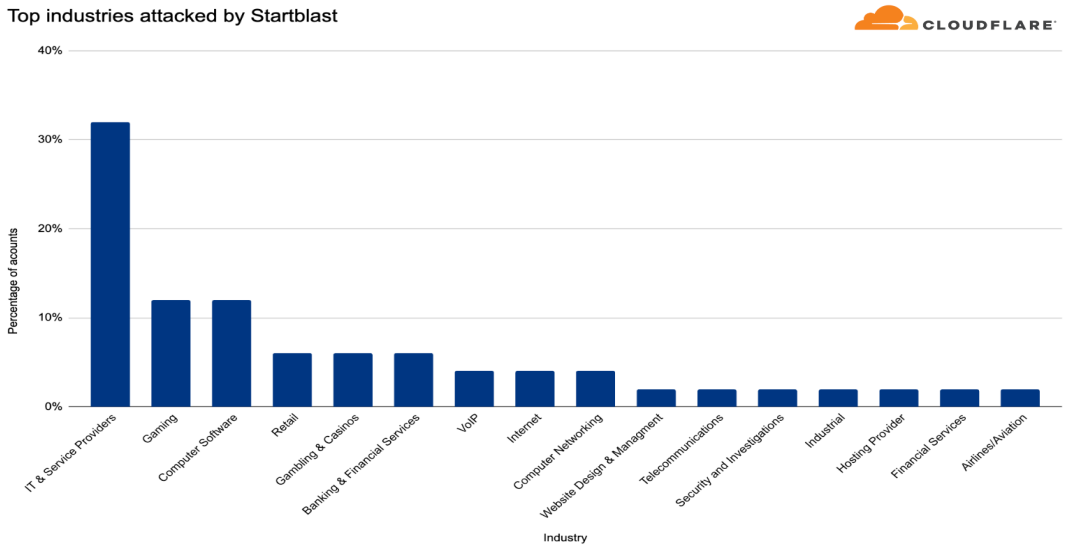
- 2023年第2四半期は、以下のDDoS攻撃が特徴となった。

1. 親ロシアのハクティビストグループであるREvil、Killnet、Anonymous Sudanが共謀した、欧米関連ウェブサイトに対する複数の DDoS攻撃。
2. Mitelの脆弱性（CVE-2022-26143）を悪用したDDoS攻撃が532%急増したのに加え、標的型DNS攻撃の増加。
3. 暗号通貨企業を標的とした攻撃が600%増加、HTTP DDoS 攻撃は15%増加

HTTP DDoS攻撃の発信元上位国



Mitelの脆弱性を悪用したDDoS攻撃の標的とされた業界上位



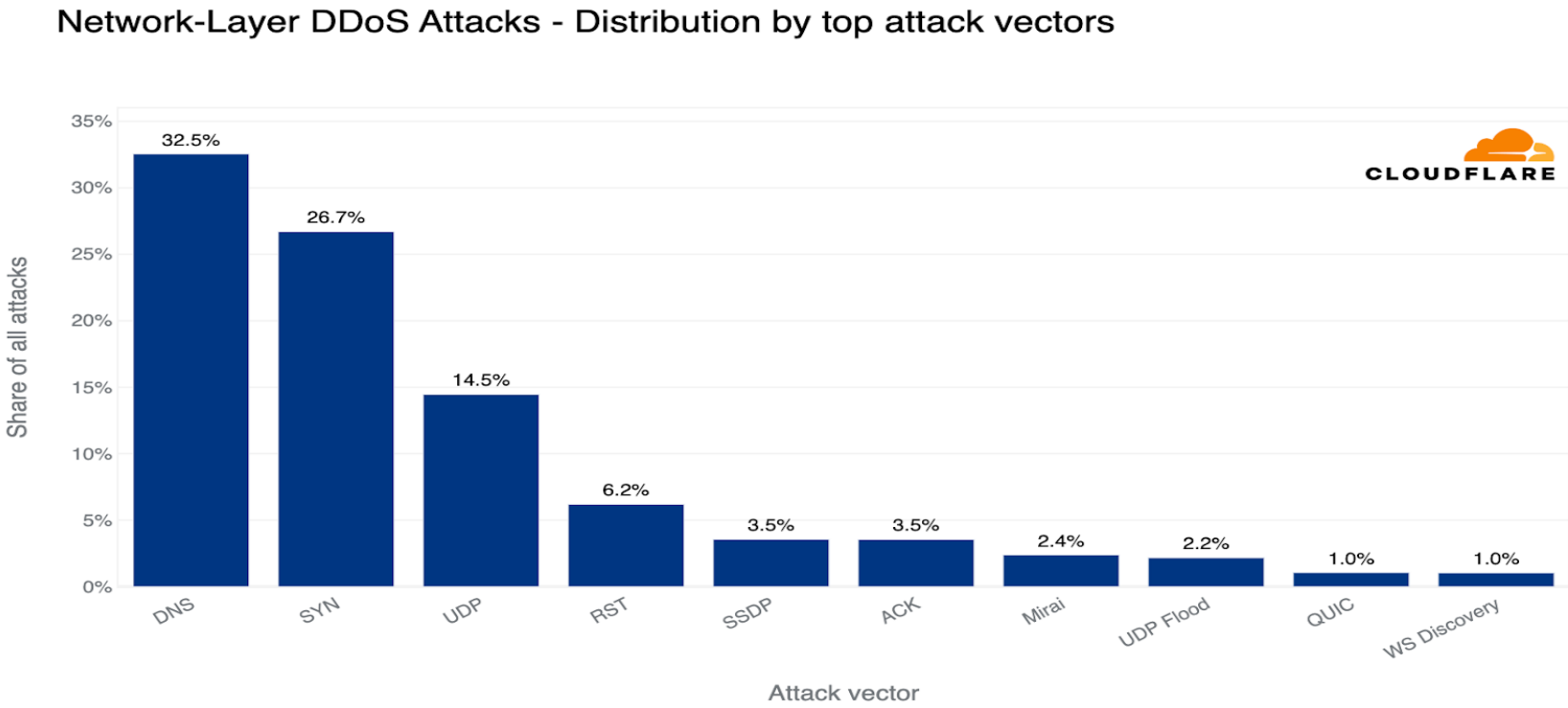
2023年第2四半期DDoS脅威レポート
https://blog.cloudflare.com/ja-jp/ddos-threat-report-2023-q2-ja-jp/

傾向

Cloudflare 2023年第2四半期DDoS脅威レポート　ランダムサブドメイン攻撃①

- Cloudflareの観測によると、2023年第2四半期で最も多かったDDoS攻撃手法はDNSベースのもので、全DDoS攻撃の約32%がDNSプロトコル経由のものだった。
- その中で特に増加しているのがランダムサブドメイン攻撃であった。

手法別DDoS攻撃数



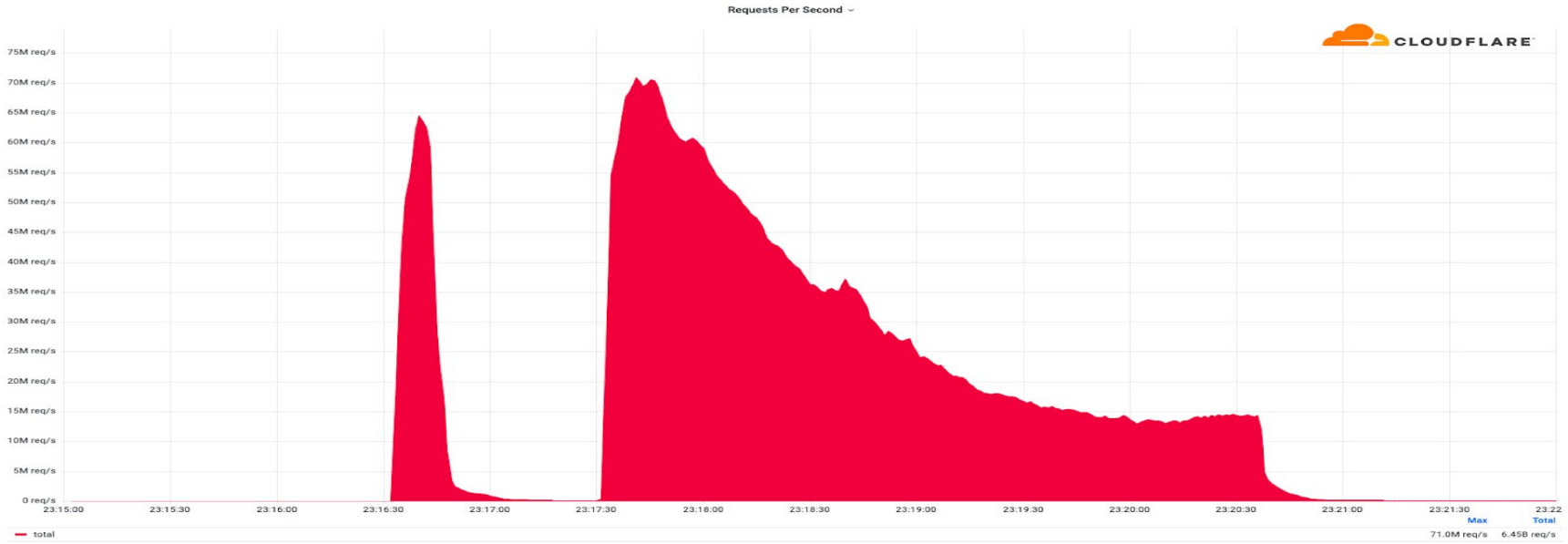
2023年第2四半期DDoS脅威レポート
https://blog.cloudflare.com/ja-jp/ddos-threat-report-2023-q2-ja-jp/

TOPIC

Cloudflare クラウドサービスを利用したボットネットによるDDoS攻撃の観測

- Cloudflareはピーク時に攻撃の大部分が5000万～7000万リクエスト/秒（rps）で、最大で7,100万rpsを超える大規模なHTTP DDoS攻撃を観測した。
- これは報告されたHTTP DDoS攻撃の中では過去最大のもので、HTTP/2ベースのWebサイトを標的としており、3万を超えるIPアドレスから発信されていた。
- この攻撃は多数のクラウドプロバイダーから発信されており、Cloudflareはクラウドプロバイダーらと協力してボットネットの取り締まりを強化している。

HTTP DDoS攻撃数の推移



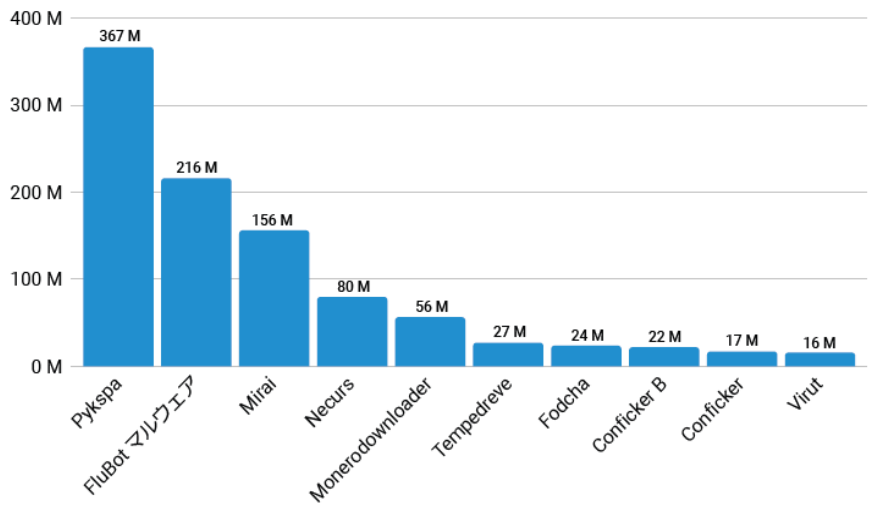
Cloudflareが1秒あたり7,100万件のリクエストを送信する記録的なDDoS攻撃を軽減
https://blog.cloudflare.com/ja-jp/cloudflare-mitigates-record-breaking-71-million-request-per-second-ddos-attack-ja-jp/

傾向

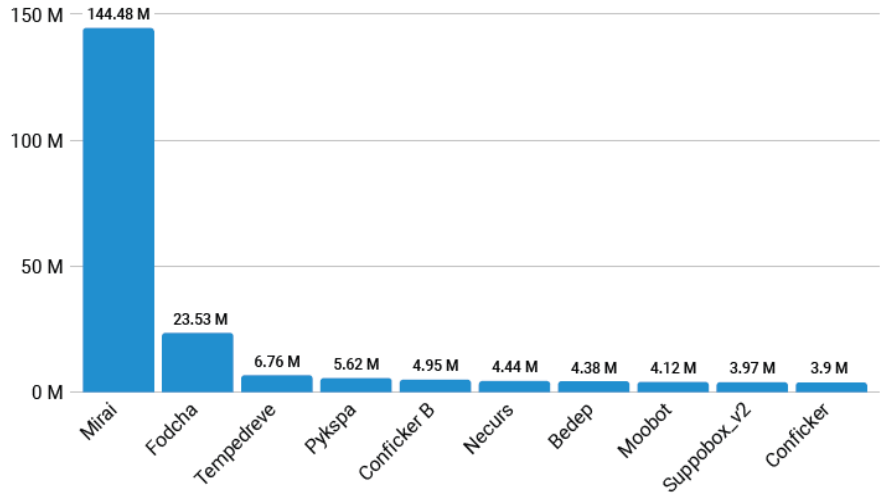
Akamai:「インターネットの現状」 攻撃の「高速道路」 悪性 DNS トラフィックの詳細な分析（2022）

- ホームユーザーのネットワークの悪性DNSトラフィックを調査するため、Akamaiは悪性のフラグが付けられた匿名サンプルを収集、分析した。
  - 2022年7月～2023年1月にて悪性DNSトラフィックのうちC2トラフィックをマルウェア別に分類したところ、トラフィック数上位はボットネットが関係していた。
  - 北米単位で同様に分類したところ、Mirai ボットネットに関連する 1億4400万件件以上のクエリーがホームネットワークで発生しており、マルウェア別でみるとトップのトラフィック数であった。
  - 北米の家庭内ではIoTデバイスの人気が高く利用の多いことが原因であるとAkamaiは推測している。

マルウェア別C2トラフィック数



北米におけるマルウェア別C2トラフィック数



攻撃の「高速道路」：悪性 DNS トラフィックの詳細な分析
https://www.akamai.com/site/ja/documents/state-of-the-internet/attack-superhighway-a-deep-dive-on-malicious-dns-traffic.pdf

参考情報

No	情報源	発生時期	URL
[1]	Google Cloud	2023年8月	https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps/?hl=en
[2]	ENISA	2023年8月	https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks https://www.wired.com/story/poland-train-radio-stop-attack/
[3]	ニュースサイト	2023年6月	https://www.computerweekly.com/news/366542252/Early-June-Microsoft-outages-were-result-of-large-scale-DDoS-hit https://msrc.microsoft.com/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks-ja/ https://www.itmedia.co.jp/enterprise/articles/2306/20/news040.html
[4]	Akamai	2023年2月	https://www.akamai.com/ja/blog/security/record-breaking-ddos-in-apac https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks
[5]	Cloudflare	2023年2月	https://blog.cloudflare.com/ja-jp/cloudflare-mitigates-record-breaking-71-million-request-per-second-ddos-attack-ja-jp/
[6]	FISC(FISAC)	2022年9月	https://www.fisc.or.jp/sysaud/pub/event/20221125 FISAC 01.pdf
[7]	ニュースサイト	2022年9月	https://www3.nhk.or.jp/news/html/20230501/k10014054791000.html https://www.nhk.or.jp/kaisetsu-blog/100/473659.html
[8]	ニュースサイト	2022年7月	https://threatpost.com/killnet-pummels-lithuania/180075/ https://www.hackread.com/russia-killnet-group-lithuania-sites-ddos-attacks/
[9]	FISC(FISAC)	2022年3月	https://www.fisc.or.jp/sysaud/pub/event/20221125 FISAC 01.pdf https://kcm.trellix.com/corporate/index?page=content&id=KB95505&locale=en US
[10]	ニュースサイト	2022年3月	https://www.datacenterdynamics.com/en/news/ukraine-ukrtelecom-hit-by-15-hour-outage-due-to-cyberattack/ https://www.forbes.com/sites/thomasbrewster/2022/03/28/huge-cyberattack-on-ukrtelecom-biggest-since-russian-invasion-crashes-ukraine-telecom/?sh=493bb7707dc2