2024

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研究室 / サイバーセキュリティネクサス

CYNEX
CYBERSECURITY NEXUS

NICTER 観測レポート

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 / 宛先ポート別のパケット数 / 調査スキャン組織

観測事象の分析

Mirai感染ホスト数の推移 / 国内におけるIoTボット感染ホスト数の推移
国内におけるInfectedSlursの感染活動 / 国内におけるLTEルータへのIoTボットの感染
RapperBotの観測事例

DRDoS攻撃の観測状況

DRDoS 攻撃の観測結果／ DRDoS 攻撃の観測事例

NICT 国立研究開発法人 情報通信研究機構

NICTER 観測レポート 2024

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研究室 / 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 2024 年のサイバー攻撃関連事象を報告するものです．

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 2024 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）：** 2024 年におけるダークネット観測では，1 IP アドレスあたりの年間総観測パケット数が約 243 万パケットとなり，2023 年の約 226 万パケットから約 17 万パケット増加しました．観測された全パケットのうち，調査目的と推測されるスキャンパケット数は約 60.2% を占めており，依然として高い割合が続いています．また，最も多く観測された 23/TCP 宛のパケットの割合は，前年の 27.1% から 17.9% へ減少しました．
- **観測事象の分析（3 章）：** Mirai の特徴を持たない IoT ボットの感染活動が活発化し，Mirai 感染ホスト数を上回る様子が観測されました．特に日本国内では，2023 年に続きデジタルビデオレコーダー（DVR）への感染が継続したほか，家庭用ブロードバンドルータや IoT 向け LTE ルータへの感染も確認されました．
- **DRDoS 攻撃の観測状況（4 章）：** DDoS 攻撃[*4]の一種である DRDoS 攻撃の観測においては，2024 年は全世界で約 3,095 万件，日本国内で約 8.5 万件の攻撃が観測されました．また，継続的に発生している絨毯爆撃型の DRDoS 攻撃のほか，複数の手法を組み合わせた日本の組織を標的とする攻撃事例も観測されました．

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．

2024 年は 1 IP アドレスあたりで約 243 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，観測パケット数の増加傾向が続いています．2024 年のパケット数増加の要因としては，2018 年頃から観測さ

*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
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
2024	約 6,862 億	284,445	2,427,977

れている海外組織からの調査目的のスキャンパケットが多く観測されたことと，海外のある IP アドレスから観測網のある IP アドレスに対して原因不明の大量のパケットが観測されたこと等が挙げられます．

大量のパケットを送信する IP アドレスについては例年通り，DNS の逆引き，Whois 情報，AS 情報等に加えて，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を参照しつつ，その送信元の組織を調査しました．大学や調査機関等，調査や研究を目的としてスキャンを行っていることが明らかで，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 アドレスからのパケットを調査目的のスキャン（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，2024 年は 1.5 万の IP アドレスからの約 2,029 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 2024 年に観測された全パケット数の約 29.6% にあたります．

さらに，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，4,570 の IP アドレスからの約 2,102 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 2024 年に観測された全パケット数の約 30.6% にあたります．

これらの調査スキャンのパケット数は，合計で約 4,131 億パケットに達しました．これは 2024 年に観測された全パケット数の約 60.2% にあたり，2023 年の約 63.8% からやや減少しました．

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 2024 年 7 月頃からやや増加傾向で推移しました．これは Mirai 亜種に感染した主に中国の IP アドレスからのパケット数が増加したためです．また，7 月初旬からは 1 週間の周期で 2.5 億パケット程度の増減を繰り返すように推移するようになりました．この周期的な増減はアメリカの IP アドレスからのパケット数の増減によるものでした．7 月末と 8 月中旬の急増は，前述の海外のある IP アドレスから観測網のある IP アドレスのハイポート番号宛に届いた大量のパケットによるものでした．

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 年間で約 54 億パケット観測されました（2023 年は約 31 億パケット）．2 月中旬にはロシアの約 58 万の IP アドレスから，約 2400 万パケットのバックスキャッタが観測されました [5]．送信元の IP アドレスは複数の AS（Autonomous System）に帰属し

*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．2024 年は四半期毎に調査目的のパケットの送信元の調査を実施しました．詳細は [3, 4] を参照して下さい．

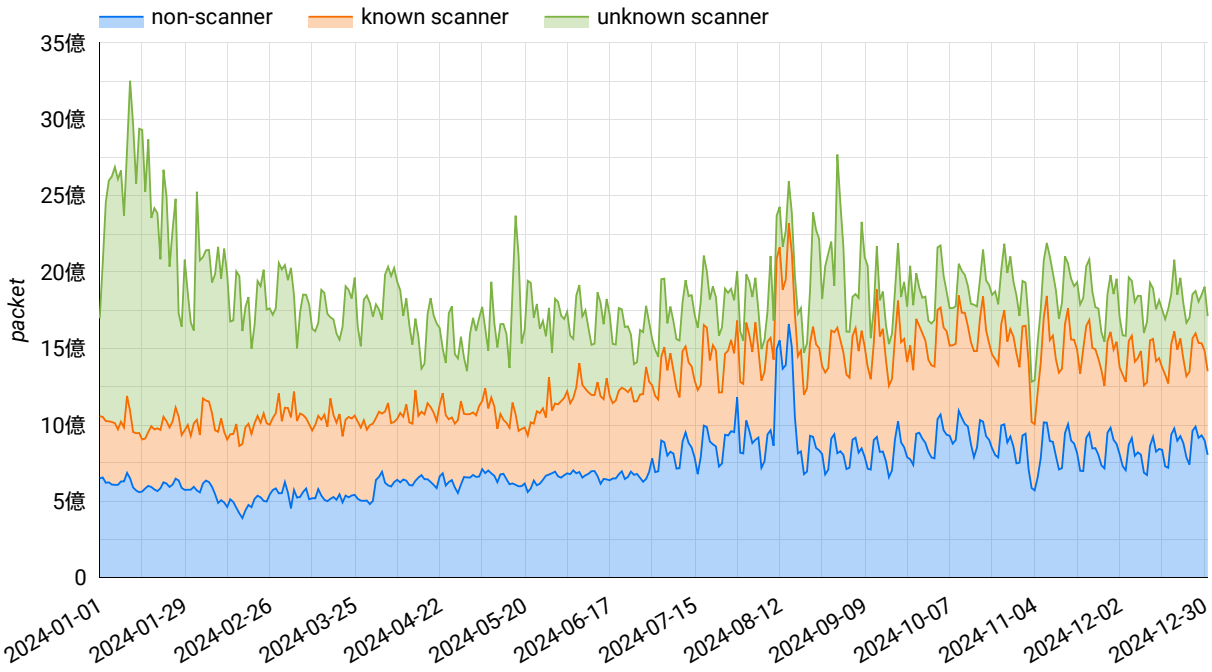


図1: ダークネットにおける日ごとの観測パケット数の推移（積み上げグラフ）

ており，その多くで SSH，SMTP，RDP，Web 等のサーバが実際に動作していることが確認されました．1 IP アドレスあたりの受信パケット数には，数百パケットから数万パケットとばらつきがありました．

1 日あたりに観測されたホスト数（IP アドレス数）は，TCP パケットが約 37 万ホスト/日（2023 年は約 37 万ホスト/日），UDP パケットが約 22 万ホスト/日（2023 年は約 16 万ホスト/日）で，TCP パケットは 2023 年と変わらず，UDP パケットは 2023 年から増加しました．2024 年のホスト数増減の詳細については，NICTER Blog の NICTER 観測統計 -第 1 四半期～第 4 四半期をご参照ください [5] [6] [7] [8].

2.3. 宛先ポート別のパケット数

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 2024 年の主な攻撃対象であると言えます．

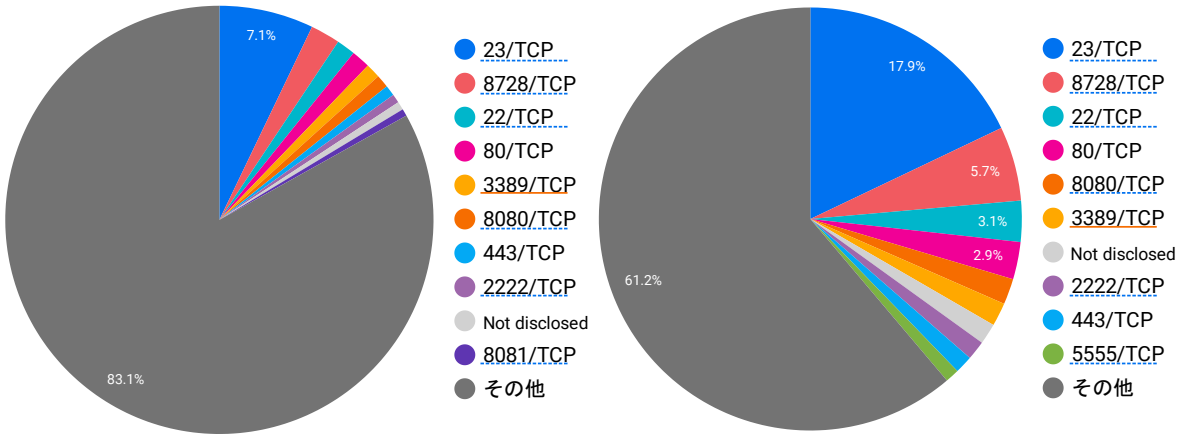
観測パケット数の最も多い宛先ポートは，昨年に引き続き Telnet サービスで使用される 23/TCP でした．しかし，2024 年の 23/TCP 宛のパケット数の全体に対する割合は 17.9% で，2023 年の 27.1%，2022 年の 23.0% と比較して減少傾向にあります．

Mikrotik Router OS の WinBox API が動作する 8728/TCP 宛のパケットは，複数のクラウドサーバの IP アドレス群からの集中的なスキャンが継続して観測された結果，2024 年は 2 番目に多いパケット数となりました（2023 年の 22 位）．サーバ等の遠隔操作で使用される SSH（Secure Shell）の 22/TCP（前年 2 位），IoT 機器の Web インターフェイスが動作する 80/TCP（前年 3 位），8080/TCP（前年 4 位）がこれに続きました．また，22/TCP の代わりに SSH サービスで使われる 2222/TCP が 8 番目に多く観測され（前年 17 位），SSH サービスを狙った攻撃が増加したことがわかります．

Windows で主に利用されているポートは上位 10 位内に 1 ポートのみで，Windows Remote Desktop サービスで使用される 3389/TCP が 6 番目に多く観測されました（前年 5 位）．

上位 10 種類以外の「その他」のポート宛ての割合は，2024 年は 61.2%（前年 56.6%）へ増加しました．

7 番目に多く観測されたポートは UDP のハイポートで，海外のある IP アドレスから観測網の特定の IP アドレスのハイポート宛に集中的なパケットが観測されたことにより上位にランクインしました．観測網秘匿のため，



(1) 調査目的のスキャンパケットを含む　　(2) 調査目的のスキャンパケットを除く

図2: 宛先ポート別の年間観測パケット数の割合

ポート番号は「Not disclosed」と表記しています．また，同様の事象は他のハイポート宛でも観測されました．

2.4. 調査スキャン組織

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．2024 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 60.2% を占めており，2023 年の 63.8% からはやや減少したものの引き続き多い状況が続いています．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，ダークネットにおけるそれぞれの観測状況を報告します．

2.4.1 既知組織の調査スキャンの分析

2024 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：69 組織，8,150 IP
- 第 2 四半期：61 組織，7,931 IP
- 第 3 四半期：60 組織，8,896 IP
- 第 4 四半期：59 組織，9,004 IP

2024 年 1 年間に確認された組織数は累計で 78，IP アドレス数はちょうど 15,000 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 2,029 億パケットでした．

特定した 78 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・観測パケット数・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をまとめた結果を表 2 に示します．なお，本調査で特定した全 78 組織をまとめたリストは GitHub で公開しています [19] .

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 2023 年と同じく Censys で，1,002 の IP アドレスから合計で約 508 億パケットが観測されました．一方，2023 年は 375 の IP アドレスから約 456 億パケットが観測されており，送信元 IP アドレスあたりのパケット数は減少しました．次に多く観測された組織は Palo Alto Networks (Cortex-Xpanse) で，993 の IP アドレスから約 418 億パケットが観測されました．前年の 488 IP アドレス，約 129 億パケットから大きく増加しました．

どちらの組織も 366 日間継続してスキャンを行っていましたが，スキャンしたポート番号の種類数は，Censys が前年同様に全ポート，Palo Alto Networks (Cortex-Xpanse) は 41,094 ポート（前年 1,521 ポート）と両者に違いが見られました．提供しているサービスによって，必要となるデータやその性質（リアルタイム性が必要かどうか，継続した調査が必要かどうかなど）が異なり，それが時間経過と共に変化もしていくためと考えられます．

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

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]	観測パケット数	TCP ポート数	UDP ポート数	観測日数
Censys [9]	脅威情報提供サービス	約 508 億	65,535	65,535	366
Palo Alto Networks (Cortex-Xpanse) [10]	脅威情報提供サービス	約 418 億	40,707	387	366
Stretchoid [11]	不明	約 191 億	463	64	341
Shadowserver [12]	脅威情報提供サービス	約 160 億	199	49	366
CriminalIP [13]	脅威情報提供サービス	約 138 億	10,770	1,728	348
The Recyber Project [14]	不明	約 135 億	65,536	0	366
driftnet (internet-measurement.com) [15]	脅威情報提供サービス	約 111 億	65,535	21	366
Academy for internet research [16]	不明	約 104 億	1,467	1	351
Shodan [17]	脅威情報提供サービス	約 48 億	2,330	88	366
Inspici [18]	調査・注意喚起	約 42 億	295	0	85

[a] 調査で特定できた全 78 組織の一覧は GitHub で公開しています [19] .
[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．

開することが推奨されていますが [20] ，我々の調査では 2024 年も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はできませんでした．

2.4.2 未知組織の調査スキャンの分析

2024 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 4,570 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 2,102 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*8，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．

2024 年は前年 2 位だった「AS396982 GOOGLE-CLOUD-PLATFORM」からのパケット数が最も多く，1,012 の IP アドレスから約 284 億パケットが観測されました．続いて多かったのは，前年 1 位だった「AS50360 Tamatiya EOOD」で，77 の IP アドレスから約 279 億パケットが観測されました．3 位以降の AS は「AS14061 DIGITALOCEAN-ASN（前年 9 位）」と「AS57523 Chang Way Technologies Co. Limited（前年 4 位）」以外は前年は上位 10 種類以内に含まれていませんでした．前年から継続してクラウドサービスの IP アドレスからのパケット数が多いことがわかります．

さらに，AS が判定できない IP アドレスが 234 あり，これらの IP アドレスからのパケット数の合計は約 260 億パケットでした．GeoIP データベースでは BG（ブルガリア）と RU（ロシア）と判定される IP アドレス群で，前年の未知組織の調査スキャンの判定時には「AS57523 Chang Way Technologies Co. Limited」や「AS204428 SS-Net」等の IP アドレスだったものが 42 個含まれていました．

IP アドレス単位で見ると，1 年で最も多くのパケットが観測されたのは「AS19318 IS-AS-1」の IP アドレスで，その IP アドレスからは 1 日に 2 億から 4 億パケットが約半月間継続して観測され，年間では約 61 億パケットが観測されました．

3. 観測事象の分析

本章では，2024 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 5 つの事例を報告します．

- Mirai 感染ホスト数の推移（3.1 節）
- 国内における IoT ボット感染ホスト数の推移（3.2節）
- 国内における InfectedSlurs の感染活動（3.3 節）
- 国内における LTE ルータへの IoT ボットの感染（3.4 節）
- RapperBot の観測事例 (3.5 節)

3.1. Mirai 感染ホスト数の推移

脆弱な IoT 機器に感染するマルウェア（IoT ボット）は依然として猛威を振るっています．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*9を持つため，ダークネット観測においてこの特徴を有するパケットの送信元 IP アドレスを集計することにより，Mirai（およびその亜種）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

*8. 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．

*9. 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．

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 10 AS）

AS 番号	AS 名	観測パケット数	IP アドレス数
AS396982	GOOGLE-CLOUD-PLATFORM	約 284 億	1,012
AS50360	Tamatiya EOOD	約 279 億	77
AS19318	IS-AS-1	約 138 億	41
AS16509	AMAZON-02	約 123 億	127
AS204428	SS-Net	約 66 億	34
AS49581	Tube-Hosting	約 52 億	17
AS14061	DIGITALOCEAN-ASN	約 49 億	640
AS57523	Chang Way Technologies Co. Limited	約 49 億	21
AS63949	Akamai Connected Cloud	約 45 億	206
AS209605	UAB Host Baltic	約 43 億	8

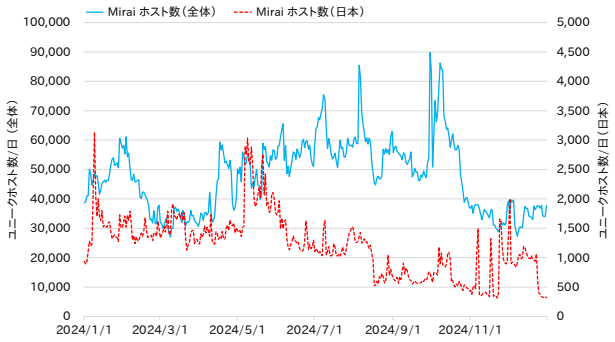
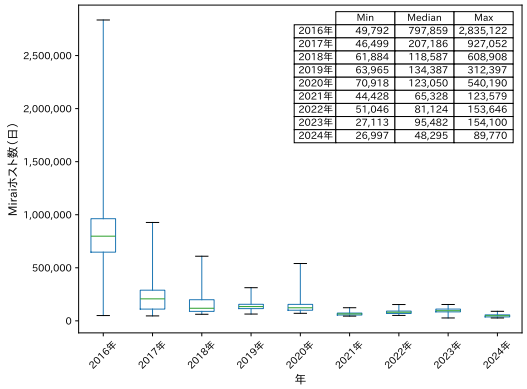
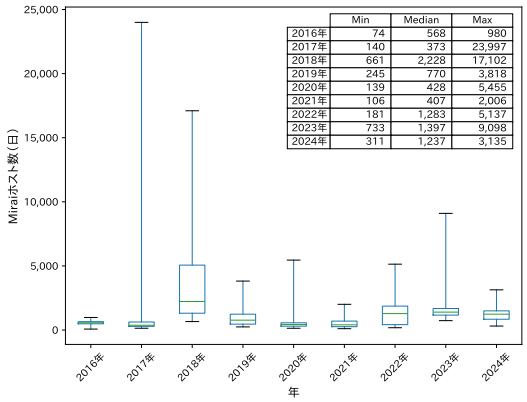


図3: Mirai 感染ホスト数の推移



(a) 世界全体



(b) 日本

図4: 日ごとの Mirai 感染ホスト数の年ごとの分布（ヒゲの範囲を $1.5 \times IQR$ ルールではなく，データの最小値・最大値に設定してプロット）

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）

世界全体における Mirai 感染ホスト数の日ごとの推移を図 3 の青線で示します．1 日あたりの Mirai 感染ホスト数は約 2.7 万〜約 9 万で推移し，平均は約 4.8 万でした．

次に，2016 年から 2024 年までの世界全体の日ごとの Mirai 感染ホスト数を，年ごとにその分布をまとめた箱ひげ図を図 4a に示します．Mirai は 2016 年に大流行して以降，その感染ホスト数は減少傾向にあり，2024 年は過去最低の水準になりました．

3.1.2 Mirai 感染ホスト数の推移（日本）

日本国内における Mirai 感染ホスト数の日ごとの推移を図 3の赤線で示します．1 日あたりの Mirai 感染ホスト数は約 310〜約 3,100 で推移し，平均は約 1,200 ホストでした．日本国内の Mirai 感染ホスト数は減少傾向にありましたが，一方で Mirai の特徴を持たないパケットでスキャンするホストが増加しました（3.2 節参照）．

次に，2016 年から 2024 年までの日本国内の日ごとの Mirai 感染ホスト数を，年ごとにその分布をまとめた箱ひげ図を図 4a に示します．日本国内では 2017 年に Mirai が大流行した後，その流行は収束しましたが，一定数の感染が継続して観測されています．

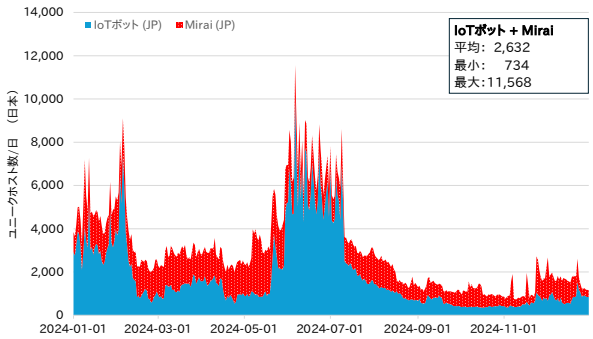


図5: 日本国内における IoT ボット感染ホスト数の推移（積み上げグラフ）

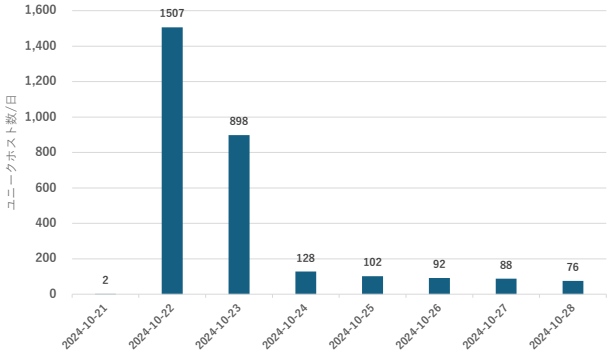


図6: ポートセット {80,81,82,8080}/TCP をスキャンするホスト数の推移

3.2. 国内における IoT ボット感染ホスト数の推移

近年，Mirai の特徴のないスキャンパケットを生成する IoT ボットが増加しており，Mirai 亜種の一部でも，この特徴を持たないパケットでスキャンする亜種が確認されています．本節では，日本国内において Mirai の特徴のないパケットでスキャンする IoT ボット感染ホスト数の推移を報告します．

本節では，日本国内における IoT ボット感染ホストを以下の条件で判定しました．

- IoT 機器への感染拡大に使われる Telnet（23/TCP）のみをスキャンする
- 送信元の IP アドレスが日本国内
- Telnet のスキャンパケットに Mirai の特徴が**ない**

これらの条件に基づいて判定した日本国内における IoT ボット感染ホスト数の推移を図 5 の青色で示します．IoT ボット感染ホスト数は約 730〜約 11,500 で推移しました．2 月と 6 月にホスト数が急増しましたが，これらは Hitron Systems 社の DVR/NVR 機器への感染が原因でした（3.3 節）．6 月 6 日のピーク時には 1 日に 1 万ホスト以上が観測されましたが，1 時間あたりの観測数は約 30〜約 800 ホスト程度であったことから，この急増は IP アドレスの変動による見かけ上の増加が原因と考えられます [21] .

また，（Mirai の特徴を持たない）IoT ボット感染ホスト数を従来の Mirai 感染ホスト数（図 5 の赤色）と比較してみると，日本国内においては Mirai の特徴を持たない IoT ボットが従来の Mirai 亜種と同等あるいはそれ以上に規模を拡大していることがわかります．

3.3. 国内における InfectedSlurs の感染活動

InfectedSlurs は IoT 機器に感染するボットで，昨年の NICTER 観測レポートでもその観測状況を報告しました．本節では，InfectedSlurs の 2024 年における日本国内の観測状況を報告します．

2024 年に日本国内で InfectedSlurs への感染が確認された主な IoT 機器は以下のとおりです．

- Hitron Systems 社製造の一部 DVR/NVR 機器 [22]
- Buffalo 社の一部ブロードバンドルータ [23]

Hitron Systems 社の DVR/NVR 機器を狙った攻撃は 2023 年から確認されており，2024 年 1 月に修正ファームウェアが公開された [22] 後も，該当機器への攻撃が継続して観測されました．また，InfectedSlurs は，2024 年 5 月以降に Buffalo 社のブロードバンドルータへも感染を広げました．該当機種については修正されたファームウェアがすでに公開されており，ファームウェアの自動更新機能により脆弱性は自動で修正されます [23] . いずれの機器も，機器のパスワードが工場出荷時から変更されずに運用されていたことが感染の原因でした．

3.4. 国内における LTE ルータへの IoT ボットの感染

10 月 22 日以降，日本国内のモバイル回線で，これまで観測されていなかったポートセット {80, 81, 82, 8080}/TCP をスキャンする IoT ボットの活動が急増しました（図 6）．スキャンの送信元を調査した結果，IO-DATA 社製の LTE ルータが IoT ボットに感染していたことがわかりました．

調査の結果，該当機器は以下の流れで IoT ボットに感染することがわかりました．この LTE ルータには，工場出荷時の初期設定として，インターネット側からアクセスできない管理画面とゲストユーザアカウントが存在します．しかし，一部のユーザが遠隔管理を目的にインターネット側のアクセスを有効化したため，それにより攻撃

```
GET /gui/(redacted).cgi HTTP/1.1
Host: XXX.X.XXX.XXX:80
User-Agent: Go-http-client/1.1
Authorization: Digest username="guest", realm="Server Status",
nonce="5e60863f2f37feb5d479d9039cd461ae", uri="/gui/(redacted).cgi",
response="fcf47a147ed3e9315727040a80031ee5", cnonce="b6c96e1d70458925374e44e8b2d31ce4",
qop=auth, nc=00000001
Accept -Encoding: gzip
```

図7: ゲストアカウントを使って管理画面にログイン後，認証情報を詐取する攻撃ペイロード（一部マスクあり）

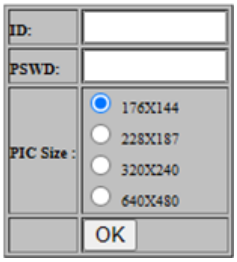


図8: DEEPLET 社製 DVR/NVR のログイン画面

者がゲストアカウントを使って管理画面の認証を突破できるようになりました．その結果，認証後のページに存在する脆弱性が悪用されて管理者の認証情報が窃取され (図 7)，ファイアウォール設定の書き換えや Telnet/SSH の有効化が行われ，最終的に機器が IoT ボットに感染しました．

我々は本脆弱性をベンダに報告し，現在は脆弱性アドバイザリとともに修正版ファームウェアが公開されています [24] .

3.5. RapperBot の観測事例

NICTER プロジェクトでは，Mirai 亜種をはじめとする IoT ボットの活動を実機を用いたハニーポットで分析しています．このハニーポットで取得した IoT ボットの検体を解析した結果，RapperBot [25] と呼ばれる IoT ボットが 2024 年 10 月以降に勢力を拡大していることが確認されました．そこで，本節では 2024 年 10 月以降に DVR 機器の実機ハニーポットから取得した 6 種類の RapperBot 検体と，それらのダークネットでの観測結果について報告します．なお，本節では，検体内に特定の YouTube の URL[*10]が含まれているものを RapperBot として分類しました．

RapperBot は 2022 年に確認された Mirai 亜種で，当初は SSH サーバへのブルートフォース攻撃を行うことで知られていました [25] . しかし，2024 年に我々が観測した 6 種類の RapperBot には，スキャン機能を持たない検体と，さまざまなポートをスキャンする検体の 2 種類が存在しました．分析した 6 検体について，取得時期，検体を取得したハニーポット（感染機器），検体がスキャンするポートセット等を一覧にまとめた表を表 4 に示します．

表 4 に示す RapperBot の検体 A および B にはスキャン機能が搭載されていませんでした．そのため，ボットは機器に感染してもインターネット上の無差別なアドレスへのスキャンを行わず，C2 サーバからのコマンドに従って DDoS 攻撃を実行します．また，ネットワークスキャンを行わないため，我々のダークネット観測ではこの RapperBot の感染状況を把握することができません．

表 4 に示す RapperBot の検体 C〜F には，それぞれ固有のポートセットを対象とするスキャン機能が搭載されていました．特に，RapperBot C は 67/TCP および 6700/TCP という特徴的なポートをスキャンしており，検体の解析結果から，これらのポートが DEEPLET 社製の DVR/NVR 機器を識別するためのものであることがわかりました．さらに，RapperBot D に感染したホストを調査したところ，台湾国内に 1500 以上の IP アドレスで DEEPLET 社製 DVR/NVR 機器のログイン画面（図 8）が確認されました．このことから，RapperBot C がネットワークスキャンを通じて DEEPLET 社製 DVR 機器を特定し，その後，攻撃者がこの DVR 機器を RapperBot D に感染させたと考えられます．

RapperBot C〜F のスキャンポートセットをもとに，各検体の日ごとの感染ホスト数の推移をダークネット観測で推計した結果を図 9 に示します．時期によって観測されるポートセットが変遷しており，RapperBot C〜F の累計では，最も多い時には世界全体で 5000 台規模のボットが形成されていたことが確認されました．なお，日本国内における感染ホスト数は，12 月 31 日時点で RapperBot C が 4 ホスト，RapperBot D が 3 ホスト，RapperBot E

*10. @2tallforfood - I Am Da Bag (Official Video): https://www.youtube.com/watch?v=4fm_ZZn5qaw

*11. SHA256: 44f897e8afb6417e3597fe51e44b101040221354ae8542066401fd5e595a7f06

*12. SHA256: 7da3d4805795ca85be0e764d732cead98cd68b6a4ebde6b42cc56bb81979eb20

*13. SHA256: 06c4df579267477428e6feaf7d4484eac922c7a9d27ddaf415b759fff43904cb

*14. SHA256: 589c4fabe4d276a4672a8ffdc9fbcf3d6e8ebe1cfb2884415fb2da54e7e46907

*15. SHA256: b0b02df76a20beaf0ea3f0a13b6d12bb33c848b428ca9551ee7dddcffe6a7a93

*16. スキャン対象のポートとして，0 から 65535 の中からランダムに 1 つのポートが選ばれます．検体がそのポートを含むポートセットでネットワークスキャンを行い，機器を判定することまでは確認できましたが，攻撃者がスキャンポートの一つをランダムに決定する実装にした理由はわかっていません．

*17. SHA256: 7b9cda9a77caacb37cad7d9fb79fae04ef39cbb3b67a42c8e78c7e30991cb6b2

表4: 本稿で分析した RapperBot の検体別の特徴

	検体の取得時期	検体を取得した機器（感染機器）	スキャンするポートセット	Mirai の特徴
A[*11]	2024 年 10 月	ITX Security 社製 DVR/NVR	なし	-
B[*12]	2024 年 12 月	ITX Security 社製 DVR/NVR	なし	-
C[*13]	2024 年 10 月	Rifatron 社製 DVR	{67, 80, 6700, 8291, 50100}/TCP 等計 14 ポート	なし
D[*14]	2024 年 10 月	Rifatron 社製 DVR	{23, 80, 2051, 34567, 345678}/TCP 等計 16 ポート	なし
E[*15]	2024 年 12 月	Rifatron 社製 DVR	{23, 26, 254, 523, 1023}/TCP 等計 31 ポート ＋ランダムな 1 ポート[*16]	あり
F[*17]	2024 年 12 月	Rifatron 社製 DVR	{23, 67, 70, 79, 80, 6700}/TCP 等計 26 ポート	なし

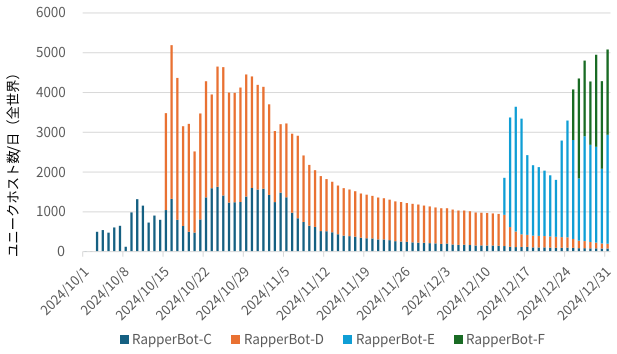


図9: RapperBot C〜F の感染ホスト数の推移

が 22 ホスト，RapperBot F が 174 ホストでした．

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 [26, 27] 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 2024 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：2024 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[*18]）

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

2024 年に AmpPot が観測した DRDoS 攻撃件数の日ごとの推移を図 10 に示します．2024 年の 1 年間に，AmpPot は累計で約 3,095 万件（2023 年は約 5,561 万件，2022 年は約 3,465 万件），1 日平均で約 8.5 万件（2023 年は約 15 万件，2022 年は約 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 17 万件（2023 年は約 896 万件，2022 年は約 61 万件），1 日平均で約 467 件（2023 年は約 2.4 万件，2022 年は約 1700 件）でした．

これらの攻撃件数には絨毯爆撃型[*19]の DRDoS 攻撃が含まれているため攻撃件数の単純な比較はできませんが，攻撃件数の傾向としては減少傾向にあります[*20]．

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 11 に示します[*21]．被攻撃件数の多い上位 5 カ国のみで攻撃件数全体の 2/3 を占めました．中国・米国宛の攻撃は定常的に多く観測されていますが，香港・ブラジル・ポーランドでは絨毯爆撃型の DRDoS 攻撃が頻繁に観測されており，その結果，

*18. 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 [26, 28] を参照して下さい．

*19. 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．

*20. 特に 2023 年は国内の IP アドレス宛に大規模な絨毯爆撃型の攻撃があったため，攻撃件数が見かけ上多く計上されました．

*21. 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．

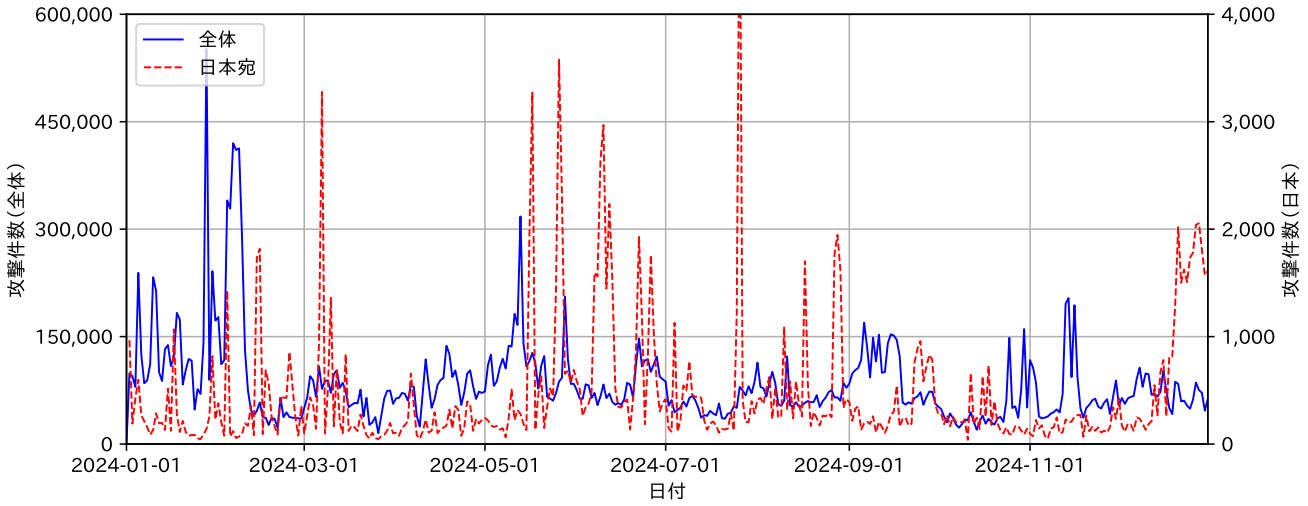


図10: 日ごとの DRDoS 攻撃件数の推移（左軸：全体，右軸：日本宛）

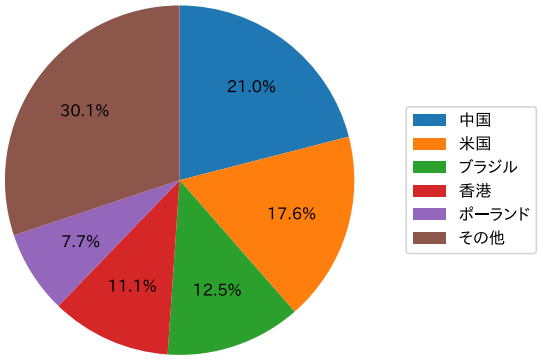


図11: 国・地域別の被攻撃件数

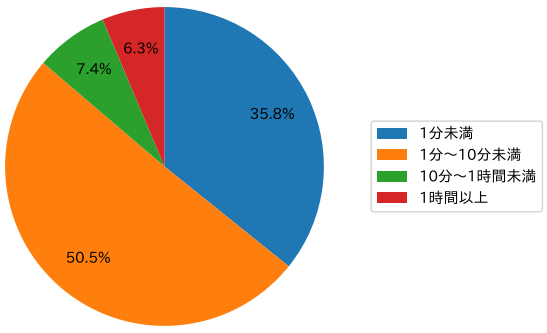


図12: 攻撃継続時間

累計の被攻撃件数が見かけ上増加しました．

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 12 に示します．1 分未満の攻撃が約 36%，1 分～10 分未満の攻撃が全体の約 51% で，例年通り継続時間の短い攻撃が大部分を占めました．また，2024 年に観測された継続時間の最も長い攻撃は香港に割り当てられた IP アドレスを狙った攻撃で，約 15 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 5 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[*22]，2023 年は 31 種類と推移してきましたが，2024 年は 18 種類と減少しました．

4.1.5 マルチベクタ型の攻撃

DRDoS 攻撃の中には，複数種類のサービスを組み合わせて悪用するマルチベクタ型の攻撃も存在します．AmpPot が観測した同一 IP アドレス宛の DRDoS 攻撃の種類数の割合を図 13 に示します．全体の約 77% は 1 種類のサービスのみを悪用した攻撃でしたが，残りの約 23%（2023 年は約 21%）は複数種類のサービスを悪用した攻撃でした．

4.2. DRDoS 攻撃の観測事例

4.2.1 ポーランドのある ISP 系企業を狙った絨毯爆撃型 DRDoS 攻撃

近年，ネットワークや AS を狙った絨毯爆撃型の DRDoS 攻撃が頻繁に観測されています．本レポートに記載する

*22. 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．

表5: 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	1,3456,137
161/UDP	SNMP	1,318,751
53/UDP	DNS	381,150
11211/UDP	Memcached	205,335
19/UDP	CharGen	112,333
1900/UDP	SSDP	49,513
17/UDP	QotD	28,898

(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
53/UDP	DNS	6,899,398
37020/UDP	Hikvision SADP	2,355,398
123/UDP	NTP	1,709,567
3702/UDP	WSD	930,619
3478/UDP	STUN	908,810
5683/UDP	CoAP	843,238
3283/UDP	ARMS	546,195
161/UDP	SNMP	313,865
1900/UDP	SSDP	307,558
389/UDP	CLDAP	292,570

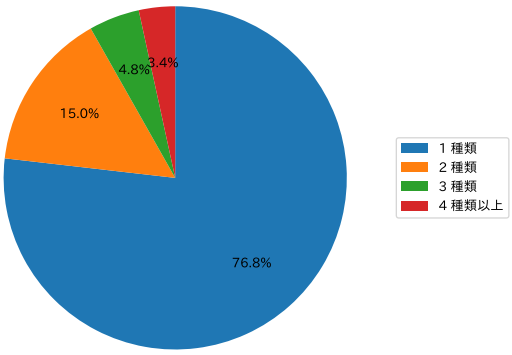


図13: 攻撃手法の種類数

攻撃件数は IP アドレス単位で集計しているため，絨毯爆撃型の DRDoS 攻撃が実行されると見かけ上の攻撃件数が急増します．本節では，2024 年に観測されたポーランドの企業を標的にした絨毯爆撃型の DRDoS 攻撃について報告します．

ポーランド宛の日ごとの攻撃件数の推移を図 14 に示します．通常時のポーランド宛の攻撃件数は 1 日数千件で推移していましたが，4 月後半から 5 月後半かけて攻撃

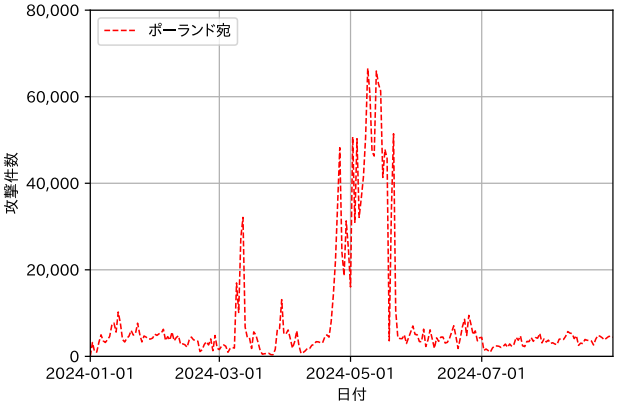


図14: ポーランド宛の日ごとの攻撃件数の推移

件数が 1 日数万件に達していたことがわかります．

この時期の急増は，ポーランドでインターネットサービスを提供する企業のネットワークを標的とした絨毯爆撃型の DRDoS 攻撃によるものでした．この企業は少なくとも連続する/16 のネットワークを保有しており，4 月 23 日から 5 月 14 日まではその中のある 1 つの/24 ネットワークが継続的に攻撃されていました．しかし，15〜16 日には攻撃対象が 6 つの/24 ネットワークに，20〜22 日には 8 つの/24 ネットワークに拡大し，このネットワークが執拗に攻撃される様子が観測されました．

このように，絨毯爆撃型の DRDoS 攻撃の中には，攻撃規模を拡大しつつ長時間にわたり実行される事例が確認されています．

4.2.2 日本の組織を狙った攻撃観測事例

AmpPot で観測される攻撃通信に含まれる情報の中には，攻撃対象組織（被害組織）に関連するものは IP アドレスしかありません．そのため，攻撃対象の組織を特定するには，IP アドレスからその組織を特定する必要があります．しかしながら，観測される IP アドレスの中には，クラウドサービスやエンドユーザのものも多く含まれるため，IP アドレスのみからでは攻撃対象の組織を特定できるケースは多くありません．

2024 年の 6 月から 12 月に，日本の 7339 個の IP アドレスに対して約 11 万件の DRDoS 攻撃が観測されました．これらの IP アドレスについて，DNS の逆引き・Whois・AS・Passive DNS 等の情報から被害組織の特定を試みました．その結果，該当期間において，大学や企業，公的機関等，少なくとも 47 組織宛の攻撃を確認することができました[*23]．本節では，2024 年に観測された日

*23. 観測された複数の IP アドレスが同じ組織に紐づくこともあるため，組織数は IP アドレス数より大幅に少なくなります．

表6: 日本の組織を狙った DRDoS 攻撃の観測事例

時刻	攻撃対象	悪用されたサービス名
2024/0X/XX 15:27, 15:37, 16:30	IP-1	DNS, Memcached
2024/0X/XX 17:18〜21:08	IP-1	DNS, NTP, CoAP, Memcached, Hikvision SADP
2024/0X/XX 21:07〜21:14	IP-2	DNS, Memcached
2024/0X/XX 23:18〜23:20	IP-2	DNS, Memcached
2024/0X/XX 23:21〜23:27	IP-1	DNS, Memcached

本の組織を標的とした攻撃事例を報告します．

2024 年上半期に発生したこの事例では，国内の企業で使用される 2 つの IP アドレスが標的になりました．この攻撃事例のタイムラインを表 6 に示します（日付は一部マスクしています）．まず，1 つ目の IP アドレス（IP-1）に対して短時間の攻撃が複数回実行されました．その後，本攻撃と思われる攻撃が実行され，約 4 時間にわたって攻撃が観測されました．IP-1 への攻撃の後，同じネットワークに属する別の IP アドレス（IP-2）への攻撃も新たに観測され，それ以降数日にわたって不定期に IP-1 への攻撃が観測されました．このときの DRDoS 攻撃に悪用されたサービスは，DNS・NTP・CoAP・Memcache・Hikvision SADP など多岐にわたりました．また，この事例ではダークネット観測においてもバックスキャッタ（DDoS 攻撃の跳ね返りパケット）が同時刻に確認されたことから，攻撃者は複数の手法を組み合わせて攻撃を実行したと考えられます．

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やハニーポット等を活用したサイバー攻撃観測のうち，2024 年の 1 年間に得られた結果と，それに基づく調査・分析の結果を報告しました．

2018 年以降に顕著な増加が観測されたインターネット広域スキャンの増加は，2023 年に続き，2024 年も全体の 6 割以上を占める結果となりました．この傾向は今後も継続すると予想されます．VPN 装置をはじめとする企業のエッジデバイスの脆弱性を悪用したサイバー攻撃は広く認知され、対策の重要性が社会的に認識されつつありますが，一方で，コンシューマー向けの IoT 製品も同様に攻撃の被害を受けているものの，その実態は十分に共有されておらず，社会的な認知はまだまだ十分とはいえません．実際，2024 年には，これまで感染が確認されていなかった新たな製品が IoT ボットに感染していることが，観測結果から明らかになりました．

IoT ボットの問題は，ユーザー自身が感染に気づきにくいことも対策の普及を阻害する要因となっていると考えられ，効果的な対策を普及させるためには，製品メーカーによる具体的なセキュリティ強化策と併せて，この問題を社会全体が正しく理解し，認識を深めることが重要です．NICT では，今後も継続的な観測と分析を通じて実態を把握し，関係組織との情報共有，情報発信に努めていきます．

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，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 観測統計 - 2024 年 1 月〜3 月. https://blog.nicter.jp/2024/05/nicter_statistics_2024_1q/.

[6] NICTER. NICTER 観測統計 - 2024 年 4 月〜6 月. https://blog.nicter.jp/2024/09/nicter_statistics_2024_2q/.

[7] NICTER. NICTER 観測統計 - 2024 年 7 月〜9 月. https://blog.nicter.jp/2024/11/nicter_statistics_2024_3q/.

[8] NICTER. NICTER 観測統計 - 2024 年 10 月〜12 月. https://blog.nicter.jp/2025/02/nicter_statistics_2024_4q/.

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

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

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

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

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

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

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

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

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

[18] Inspici. https://inspici.com/.

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

[20] 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.

[21] PPPoE 環境におけるロジテック製ルータの IP アドレス変動事象について. https://blog.nicter.jp/2022/04/logitec_router_ip_churn/.

[22] 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/.

[23] バッファロー. NICTER の投稿に関する重要なお知らせ（7/19 更新）. https://www.buffalo.jp/news/detail/20240719-01.html.

[24] JVN#46615026: アイ・オー・データ製ルーター UD-LT1 および UD-LT1/EX における複数の脆弱性. https://jvn.jp/jp/JVN46615026/index.html.

[25] FortiGuard Labs Threat Research. So RapperBot, What Ya Bruting For? https://www.fortinet.com/blog/threat-research/rapperbot-malware-discovery.

[26] 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.

[27] 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/.

[28] 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.