2025

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

NICTER 観測レポート

NICTER Observation Report https://www.nicter.jp/

ダークネット観測統計

年間総観測パケット数 / 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

IoTボット感染ホスト数の推移 / RapperBotの活動変化とシンクホールによる観測結果
MountBot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

NICTER Observation Report https://www.nicter.jp/

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 2025

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]および各種ハニーポット[*3]の観測結果に基づき，2025 年に確認されたサイバー攻撃関連事象について報告するものです．

2025 年も引き続き，NICTER の各種センサでは多岐にわたる事象が観測されました．本レポートでは，その中から主な観測結果を取りまとめて報告します．

- **ダークネット観測統計（2 章）：** 2025 年の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 250 万パケットとなり，2024 年から約 7 万 7 千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 55.0% を占め，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 宛パケットの割合は，前年の 17.9% から 14.4% へ減少し，多様なポート番号宛の攻撃が増加しました．
- **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．国内では，デジタルビデオレコーダー（DVR）や家庭用無線 LAN ルータへの感染継続して確認されました．また，RapperBot の活動が 2025 年中頃に終息した一方で，新たな IoT ボットである MountBot が出現し，感染手法の移行が観測されました．
- **DRDoS 攻撃の観測状況（4 章）：** DDoS 攻撃[*4]の一種である DRDoS 攻撃の観測においては，2025 年は全世界で約 8,285 万件，日本国内で約 90 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，NTP を悪用した攻撃件数の減少が観測されました．

2. ダークネット観測統計

2.1. 年間観測パケット数

NICTER ダークネット観測で過去 10 年間に観測された

- 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 アドレス数の影響を受けるため，本レポートでは，表の右端に示す「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把握するための指標として用います．

2025 年は，1 IP アドレスあたり年間約 250 万のパケットが観測され，観測開始以降で最多となり，増加傾向が引き続き確認されました．その主な要因としては，2018 年

*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．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で，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. 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（2025 年は年末にセンサのメンテナンスがあったため，12 月 26 日の 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
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
2025	約 7,010 億	284,305	2,504,680

頃から継続して観測されている海外組織による調査目的のスキャンパケットが，2025 年においても多く観測されたことが挙げられます．

大量のパケットを送信する IP アドレスについては，例年同様，DNS の逆引き，Whois 情報，AS 情報，Censys [1] のバナー情報等に加え，セキュリティ関連組織が公開する情報 [2, 3] を参照し，送信元組織の調査を行いました．

その結果，大学や調査機関等による調査・研究目的のスキャンであり，かつ送信元の IP アドレスが公開されている，または逆引き等により送信元組織を確認できたものを，「既知組織の調査スキャン」と判定しました．2025 年には，17,348 の IP アドレスから送信された約 2,413 億パケット (全観測パケットの約 34.4%) がこれに該当しました．

一方，送信元の組織を特定できないものの，調査目的と考えられるスキャンも 2018 年以降継続して観測されています．これらは攻撃傾向の分析においてノイズとなるため，本レポートでは昨年までと同様に一定の判定ルール*7を設け，「未知組織の調査スキャン」として判定および除去を行いました．その結果，2025 年には，2,490 の IP アドレスから送信された約 1,445 億パケット（全観測パケットの約 20.6%）がこれに該当しました．

既知組織および未知組織の調査スキャンを合計すると，調査目的のスキャンパケット数は約 3,858 億パケットとなり，2025 年に観測された全パケット数の約 55.0% を占めました．これは，2024 年の約 60.2% からやや減少しています．

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)」，および「攻撃関連パケット（non-scanner）」に分類して集計した結果を図 1 に示します．

12 月末には観測パケット数が全体的に減少していますが，これはセンサのメンテナンスによるものです．一方，攻撃関連パケット数（non-scanner）は年間を通じて概ね横ばいで推移しました．

8 月中旬には，未知組織の調査スキャンパケット (unknown scanner) が一時的に急増しました．この事象は，1 つの AS（アゼルバイジャン，AS19318 Interserver, Inc）に所属する数十の IP アドレスによるもので，Masscan ツール [6] を用いて，1 IP アドレスあたり数千ポート宛てのスキャンが行われていました．

なお，攻撃関連パケット（non-scanner）に含まれる 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，2025 年に約 58 億パケット観測されました（2024 年は約 54 億パケット）．

また，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 32 万ホスト/日（2024 年は約 37 万ホスト/日），UDP パケットが約 18 万ホスト/日（2024 年は約 22 万ホスト/日）で，いずれも 2024 年から減少しました．2025 年のホスト数の増減の詳細については，NICTER Blog の NICTER 観測統計 -第 1 四半期～第

*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、かつ
- 総パケット数が 30 万以上

の条件を共に満たす場合，当該 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．2025 年も昨年と同様に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 [4, 5] を参照して下さい．

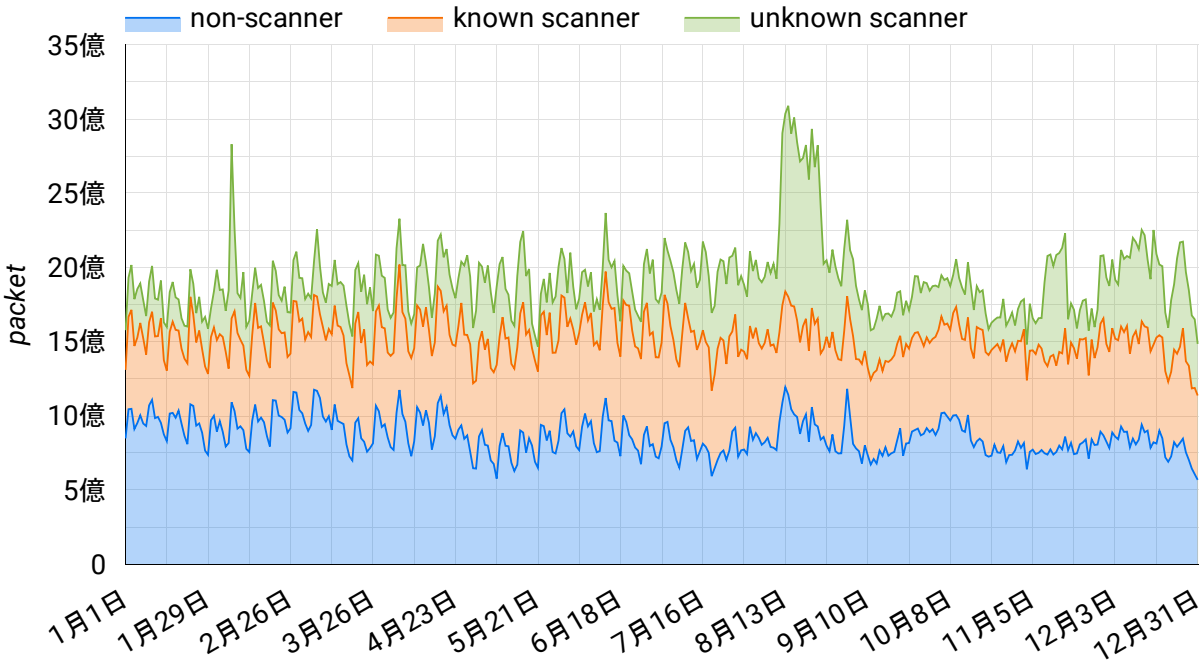

図1: ダークネットにおける日ごとの観測パケット数の推移（積み上げグラフ）

4 四半期をご参照ください [7] [8] [9] [10].

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 および UDP のパケットについて，宛先ポート別にパケット数を集計し，上位 10 種類のポート番号とその他の割合を円グラフとして図 2 に示します．図の左側は調査目的のスキャンを含む総観測パケット，右側は攻撃関連パケットを対象とした結果です．また，凡例中の青色の点線は主に IoT 機器で利用されるポート番号，橙色の実線は Windows で主に利用されているポート番号を示しています．右側の円グラフに示される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 2025 年の主な攻撃対象であると考えられます．

観測パケット数が最も多かった宛先ポートは，昨年に引き続き Telnet サービスで使用される 23/TCP でした．ただし，23/TCP 宛のパケット数の全体に対する割合は 14.4% で，2024 年の 17.9%，2023 年の 27.1% 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たことにより，昨年と同様に 2 番目に多く観測されました．

これに続いて，IoT 機器の Web インターフェイスが動作する 80/TCP（前年 4 位），サーバ等の遠隔操作で使用される SSH の 22/TCP（前年 3 位），および 443/TCP（前年 9 位）が多く観測されました．また，SSH サービスで 22/TCP の代替として利用される 2222/TCP が 10 番目に多く観測され（前年 8 位），SSH サービスを狙った攻撃が昨年に引き続き多く観測されました．

7 番目に多く観測された 34567/TCP は，Xiongmai 製 DVR の API が動作するポートで，ハニーポットでは該当製品の脆弱性 (CVE-2024-3765) [11] を悪用した攻撃が観測されました（前年 29 位）．

一方，Windows で主に利用されているポートは上位 10 位内には含まれていませんでした．最も上位のポートは Windows Remote Desktop サービスで使用される 3389/TCP で，12 番目でした（前年 6 位）．

2025 年は Rapperbot（23/TCP のほか 30 種類以上のポートを対象とするスキャンを行う）や，Mountbot (80/TCP，81/TCP，82/TCP，83/TCP，85/TCP を対象とするスキャンを行う）といった，多数の宛先ポートにスキャンを行う IoT マルウェアの活動が確認されました．その結果，多様な IoT 機器で利用されるポート宛ての攻撃が増加し，上位 10 種類以外の「その他」のポート宛ての割合は，前年 61.2% から 65.8% へと増加しました．

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数は増加傾向にあり，2025 年においても観測された全パ

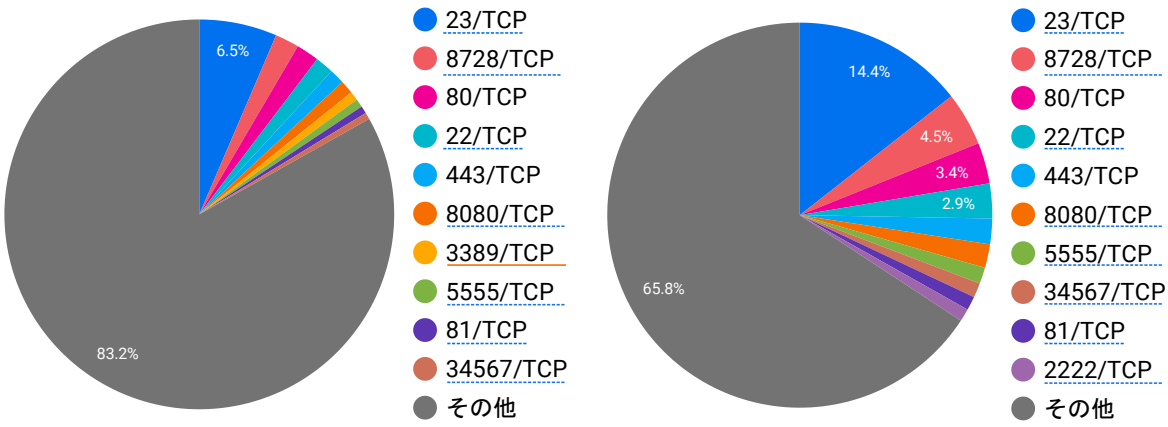

図2: 宛先ポート別の年間観測パケット数の割合

ケット数の約 55.0% を占めました．本節では，「既知組織の調査スキャン」と「未知組織の調査スキャン」について，それぞれの観測状況を整理します．

2.4.1 既知組織の調査スキャンの分析

2025 年に確認された調査目的スキャンについて，送信元組織数および対応する IP アドレス数を四半期ごとに整理した結果を以下に示します．

- 第 1 四半期：62 組織，10,492 IP
- 第 2 四半期：75 組織，11,205 IP
- 第 3 四半期：78 組織，12,216 IP
- 第 4 四半期：71 組織，13,827 IP

2025 年に確認された調査目的スキャンの送信元組織数は，四半期ごとに一部重複があるため，年間累計では 87 組織となりました．対応する IP アドレス数は 17,348 となり，期間ごとに調査組織の入れ替わりが確認されました．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 2,413 億パケットでした．

観測パケット数の多い上位 10 組織 [*8] について，組織の属性およびスキャン活動の特徴を整理した結果を表 2 に示します．なお，本調査で特定した全 87 組織の一覧は GitHub に公開しています [12] .

観測パケット数が最も多かった組織は Palo Alto Networks (Cortex-Xpanse)（前年 2 位）で，986 の IP アドレスから合計約 516 億パケットを観測しました．前年の 993 IP アドレス，約 418 億パケットと比較すると，IP アドレス数は同程度でしたが，送信元 IP アドレスあたりのパケット数は増加しました．

次に多く観測された組織は Censys（前年 1 位）で，882 の IP アドレスから合計約 493 億パケットを観測しました．前年の 1,002 IP アドレス，約 508 億パケットからは IP アドレス数が大きく減少しましたが，送信元 IP アドレスあたりのパケット数は増加しました．

上位 10 組織のうち 6 組織が 365 日間継続してスキャンを行っていました．全ポート番号宛てにスキャンを行っていた組織は，全 87 組織のうち，Censys（昨年同様）と driftnet（昨年は 65,556 ポート）でした．パケット数が最も多かった Palo Alto Networks (Cortex-Xpanse) のスキャン対象ポート数は 65,582 ポートで，前年の 41,094 ポートから大きく増加しました．また，他の多くの組織においても，スキャン対象ポート数が増加している傾向が確認されました．

調査目的のスキャンを実施する組織は，スキャンの目的や Opt-out の方法などを自身の Web サイト等で公開することが推奨されています [13] . しかし，これまでの我々の調査では，多くの組織においてスキャンに関する詳細な記述を確認することができませんでした．

一方，2025 年には新たに 8 組織で，スキャンの目的，スキャンの方法，頻度，Opt-out の方法などが公開されていることを確認しました．これらの組織では，スキャン

*8. 観測パケット数の多い上位 10 組織の Web サイト
https://www.paloaltonetworks.com/cortex/cortex-xpanse
https://censys.io/
https://www.shadowserver.org/
https://stretchoid.com/
https://internet-measurement.com/
https://www.modat.io/scanning
https://www.shodan.io/
https://academyforinternetresearch.org/
https://www.criminalip.io/
https://cypex.ai/

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
Palo Alto Networks (Cortex-Xpanse)	脅威情報提供サービス	約 516 億	65,465	117	365
Censys	脅威情報提供サービス	約 493 億	65,535	65,535	365
Shadowserver	脅威情報提供サービス	約 245 億	305	44	365
Stretchoid	不明	約 215 億	306	64	316
driftnet (internet-measurement.com)	脅威情報提供サービス	約 141 億	65,535	65,535	365
Modat	脅威情報提供サービス	約 133 億	13,531	6	363
Shodan	脅威情報提供サービス	約 100 億	4,141	82	365
Academy for internet research	不明	約 80 億	1,492	1	360
CriminalIP	脅威情報提供サービス	約 76 億	9,221	331	365
CYPEX	脅威情報提供サービス	約 72 億	952	3	274

[a] 調査で特定できた全 87 組織の一覧は GitHub で公開しています [12] .
[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．

倫理が一定程度考慮されていると考えられます．

2.4.2 未知組織の調査スキャンの分析

2025 年に未知組織の調査スキャンと判定された IP アドレス数は 2,503，観測パケット数は約 1,445 億でした．これは 2024 年の 4,570 IP アドレス，約 2,102 億パケットと比較して，大きく減少しています．本節では，これらのスキャンについて，送信元 IP アドレスが属する AS（Autonomous System）別の分析を行います．

AS 情報の推定には，MaxMind 社の GeoIP データベースを用いました．観測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，および IP アドレス数を整理した結果を表 3 に示します．

2025 年に最も多くのパケットが観測された AS は，昨年 2 位だった「AS50360 Tamatiya EOOD」で，65 の IP アドレスから約 216 億パケットを観測しました．昨年まで 1 位だった「AS396982 GOOGLE-CLOUD-PLATFORM」は大きく減少し，約 8 億パケットでした（28 位）．2 位以降の AS は「AS19318 Interserver, Inc（前年 3 位）」，「AS49581 Tube-Hosting（前年 6 位）」，「AS63949 Akamai Connected Cloud（前年 9 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．昨年と同様に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傾向が続きました．

IP アドレス単位で見ると，1 年で最も多くのパケットを観測したのは「AS50360 Tamatiya EOOD」に属する IP アドレスでした．当該 IP アドレスからは，1 日あたり数千から最大 1 億パケットが合計 144 日間にわたり断続的に観測され，年間では約 28 億パケットに達しました．

3. 観測事象の分析

本章では，前章で示した統計的傾向を踏まえ，2025 年にダークネットおよび各種ハニーポットを用いて観測・分析した事象の中から，特に特徴的であった次の 3 つの事例を報告します．

- IoT ボット感染ホスト数の推移（3.1 節）
- RapperBot の活動変化とシンクホールによる観測結果 (3.2 節)
- MountBot の観測結果 (3.3 節)

3.1. IoT ボット感染ホスト数の推移

3.1.1 感染ホストの判定

脆弱な IoT 機器に感染するマルウェア（IoT ボット）は，現在も継続的に観測されています．IoT ボットとして広く知られている「Mirai」およびその亜種は，スキャン時に生成する TCP の SYN パケットに固有の特徴を持つことが知られています[*9]．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で，Mirai（およびその亜種）に感染したホスト数を推計することが可能です．

本節では，まずこの手法に基づき，世界全体および日本国内における Mirai 感染ホスト数の推移を分析します．また，昨年に引き続き，Mirai の特徴的な TCP ヘッダを持たないパケットを用いてスキャンを行う IoT ボットの活動についても報告します．

本年は，Mirai の特徴を持たない IoT ボット感染ホストについて，感染拡大時の挙動に着目し，以下の条件に基づ

*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 以上となる特徴．

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
AS50360	Tamatiya EOOD	約 216 億	65
AS51396	Pfcloud UG (haftungsbeschrankt)	約 170 億	80
AS19318	Interserver, Inc	約 132 億	49
AS211736	FOP Dmytro Nedilskyi	約 50 億	45
AS214295	Skynet Network Ltd	約 48 億	73
AS208949	Hbing Limited	約 44 億	14
AS49581	Tube-Hosting	約 39 億	11
AS63949	Akamai Connected Cloud	約 30 億	13
AS36352	HostPapa	約 29 億	63
AS201814	MEVSPACE sp. z o.o.	約 29 億	61

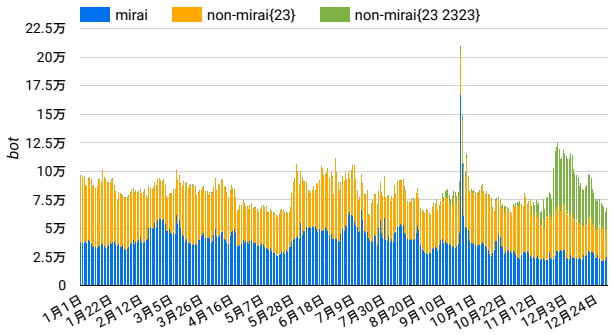

図3: IoT ボット感染ホスト数の推移（世界）

いて判定を行いました．

- IoT 機器への感染拡大に広く用いられている Telnet（23/TCP）のみ，もしくは Telnet（23/TCP）および 2323/TCP を対象にスキャンを行っていること
- スキャンにおいて Mirai 特有の TCP ヘッダの特徴を持たないこと

これらの条件に基づき，本節では，Mirai 感染ホスト，Mirai の特徴を持たず 23/TCP のみをスキャンする IoT ボット感染ホスト，および Mirai の特徴を持たず 23/TCP および 2323/TCP をスキャンする IoT ボット感染ホストの 3 つの分類について，それぞれの推移を報告します．

3.1.2 世界全体

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 の青色で示します．2025 年における 1 日あたりの Mirai 感染ホスト数は，概ね約 2 万〜約 6 万台の範囲で推移しており，年間を通じて比較的安定した状況が観測されました．

一方，9 月下旬には一時的な急増が観測され，最大で約 16.6 万台に達しました．送信元国別に集計した結果，特にブラジルでは前日比で約 31 倍（1,204 台から 37,744 台）と顕著な増加が見られたほか，アルゼンチンおよび米国においても，それぞれ約 6 倍，約 5 倍の増加が確認されました．急増が顕著であった送信元国とそのホスト数を図 4に示します．なお，送信元に関する調査結果については，NICTER ブログ [9] にて報告しています．

この急増は短期間で収束しており，2025 年 10 月以降は Mirai 感染ホスト数が全体として減少傾向を示しました．2024 年における最小値（約 2.7 万台）を下回る水準で推移する状況も観測されました．

また，Mirai の特徴を持たず 23/TCP のみをスキャンする IoT ボット感染ホスト数（図 3 の橙色）は，1 日あたり概ね約 2 万台〜約 6 万台の範囲で推移しており，年間を通じて大きな変動は見られませんでした．一方，Mirai の特徴を持たず 23/TCP および 2323/TCP をスキャンする IoT ボット感染ホスト数（図 3 の緑色）は，2025 年 11 月下旬以降に増加傾向を示しました．この増加は，Mirai 感染ホスト数や Mirai の特徴を持たず 23/TCP のみをスキャンする IoT ボット感染ホスト数が概ね維持された状況下で観測されており，現時点ではその要因を明確に特定することはできていません．

3.1.3 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 5 に青色で示します．2025 年における 1 日あたりの Mirai 感染ホスト数は，約 170〜約 1,470 ホストの範囲で推移しており，平均は約 542 ホストでした．日本国内の Mirai 感染ホスト数は，昨年と同様に全体として減少傾向を示しています．

一方で，Mirai の特徴を持たないパケットによるスキャンを行う IoT ボット感染ホスト（図中の橙色および緑色）は，昨年と比べて増加しました．特に，Mirai の特徴を持

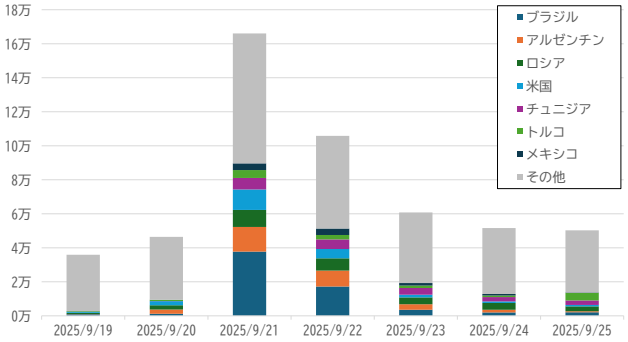

図4: 2025 年 9 月のホスト数急増の詳細

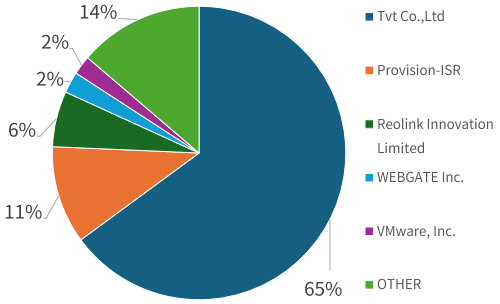

図6: RapperBot 感染機器の OUI 別ベンダー内訳

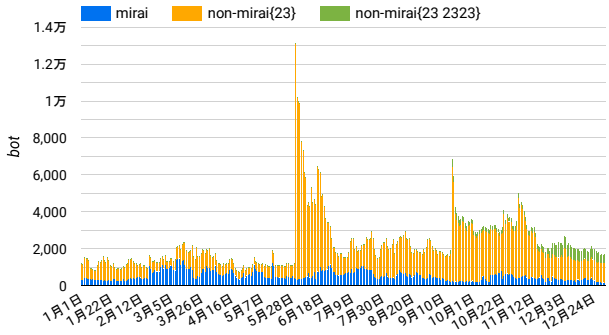

図5: IoT ボット感染ホスト数の推移（日本）

たず 23/TCP のみをスキャンするホスト数は，急増期を除くと概ね約 400〜約 2,000 ホストの範囲で推移しました．5 月末から 6 月上旬にかけては一時的な急増が確認され，最大で 1 日に約 12,700 ホストが観測されました．しかし，NICTER において一定時刻の直前 10 分間に観測されたホストを対象としたスキャンバック分析によると，新規に確認された ITX 社製 DVR は約 600 台にとどまっており，この急増については，IP アドレス変動の影響により，見かけ上多くのホストが観測された可能性が高いと考えられます [8]．また，これらの ITX 社製 DVR の一部では， 3.3節で紹介する MountBot による感染活動が確認されており，当該急増との関連が示唆されます．さらに，23/TCP および 2323/TCP の双方をスキャンするホスト（図中の緑色）は，主に 9 月以降に継続して観測されており，国内においても Mirai の特徴を持たない IoT ボットの活動が一定期間続いていることが確認されました．

3.2. RapperBot の活動変化とシンクホールによる観測結果

NICTER 観測レポート 2024 では，RapperBot と呼ばれる IoT ボット*10が 2024 年 10 月以降に勢力を拡大していることを報告しました．本節では，その後の継続観測および分析により 2025 年に確認された RapperBot の活動の変化について報告します．

まず，2025 年 5 月頃を境として，一部メーカー製 DVR 機器は，RapperBot による攻撃対象から外れ， 3.3節で紹介する MountBot による感染活動の対象となったことが確認されました．

また，RapperBot の C2 通信を調査した結果，C2 サーバ探索先として未登録のドメイン名が設定されていることを確認しました．そこで当該ドメインを取得し，2025 年 6 月にシンクホールを実施しました．シンクホールにより取得された約 6 万ホストのログをもとに分析を行い，MAC アドレスの重複を除外したうえで，OUI からベンダー名が特定可能であった約 5 万件を対象として感染機器の実態を整理しました（図 6）．

分析の結果，RapperBot に感染したとみられる機器は特定のベンダーに大きく偏っており，Tvt Co., Ltd. 製の機器が全体の約 65% を占めていました．また，日本国内においても DVR 機器が大半を占め，Tvt Co., Ltd. 製および WEBGATE Inc. 製の機器で全体の約 94% を占めていることが確認されました．なお，一部の機器については，OUI 情報と実際のベンダーが一致しない可能性がある点に留意が必要です．

さらに，C2 サーバとの通信可否に関する監視を継続した結果，2025 年 8 月 7 日をもって，RapperBot の C2 サーバとの通信が行われなくなったことを確認しました（図 7）．この時期は，米国司法省が RapperBot ボットネットの運用者に対する起訴を公表した時期と一致しており，当該起訴が RapperBot の C2 通信停止および攻撃活動の終息に影響を与えた可能性が高いと考えられます．

なお，RapperBot に関する感染対象探索手法や C2 通信アルゴリズムの詳細は，国際会議や学術論文において既に報告しているため [14, 15, 16]，本稿では割愛します．

*10. 検体内に特定の YouTube の URL が含まれるもの

図7: C2 サーバとの最終通信ログ（2025 年 8 月 7 日）

```
mount('/proc/1', '/proc/self', 0, MS_BIND, 0);
```

図8: MountBot のプロセス隠ぺい処理

3.3. MountBot の観測結果

2025 年 2 月頃より，Mirai の特徴を持たず 23/TCP 宛にスキャン活動を行う送信元の調査を進めた結果，AiCloud 機能が有効化された ASUS 製ルータが多数確認されました．ASUS 製 WiFi ルータの AiCloud 機能に関する脆弱性や感染規模の詳細は，NICTER ブログで紹介しています [17, 18]．

この結果を受けて，ASUS 製ルータの実機を用いた詳細な攻撃観測を行いました．取得したマルウェアを解析したところ，検体内にプロセスを隠ぺいするための特徴的な処理が含まれていることを確認しました（図 8）．本レポートでは，この特徴を持つ IoT ボットを MountBot と呼びます．MountBot の機能や感染後の挙動に関する解析結果は，NICTER ブログで報告しています [19]．

当初，NICTER の観測結果から，MountBot は ASUS 製ルータを主な感染対象としていると判断していました．しかし，その後の観測により，RapperBot の攻撃対象であった ITX などの DVR 機器に対しても同様の特徴を持つマルウェアによる感染活動が確認されました．

さらに，MountBot では感染機器ごとにマルウェアのスキャン挙動が異なっていた可能性があり，NICT では，スキャンを行わない，23/TCP のみにスキャンを行う，および 80, 81, 82, 83, 85/TCP 宛にスキャンを行う検体の 3 種類を確認しています．

最後に，NICTER において観測された，80, 81, 82, 83, 85/TCP 宛にスキャンを行うホスト数の推移を図 9に示します．2025 年 4 月以降，当該ポートセットをスキャンするホスト数は一定期間増加した後，8 月末をもって観測されなくなりました．一方で，同一の IP アドレスが 9 月中旬以降に Mirai の特徴を持たず 23/TCP をスキャンするようになったことから、攻撃者がスキャン挙動を切り替えた可能性があります．

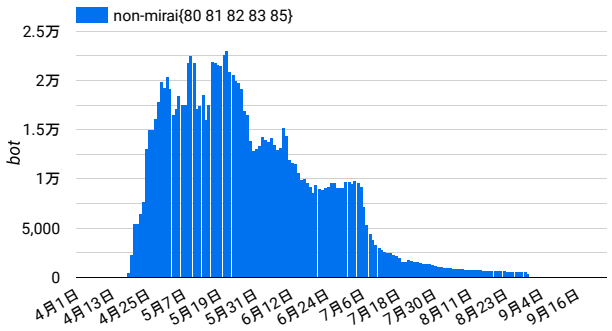

図9: 80,81,82,83,85/TCP でスキャンを行うホストの推移 (世界)

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 [20, 21] 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 2025 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：2025 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

*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 [20, 22] を参照して下さい．

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

2025 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．2025 年の 1 年間に，AmpPot は累計で約 8,285 万件（2024 年は約 3,095 万件，2023 年は約 5,561 万件），1 日平均で約 23 万件（2024 年は約 8.5 万件，2023 年は約 15 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 90 万件（2024 年は 17 万件，2023 年は約 896 万件），1 日平均で約 2500 件（2024 年は約 467 件，2023 年は約 2.4 万件）でした．

日ごとの攻撃件数の推移を見ると，攻撃件数が急増している期間が多数あります．これらの期間には，絨毯爆撃型[*12]の DRDoS 攻撃が観測されています．本レポートでは，攻撃件数を IP アドレス単位で集計しているため，絨毯爆撃型の攻撃が発生すると，見かけ上の攻撃件数が大幅に急増します．そのため攻撃件数の単純な比較は困難ですが，2025 年においても DRDoS 攻撃は依然として多く観測されました．

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 11 に示します[*13]．被攻撃件数の多い上位 5 カ国のみで攻撃件数全体の 3/4 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，昨年に引き続き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 58%，1 分〜10 分未満の攻撃が全体の約 18% 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，2025 年に観測された継続時間の最も長い攻撃はイギリスに割り当てられた IP アドレスを狙った攻撃で，約 25 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，2021 年は 38 種類，2022 年は 151 種類[*14]，2023 年は 31 種類，2024 年は 18 種類と推移してきましたが，2025 年は 16 種類へと減少しました．

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	24,102,175
53/UDP	DNS	7,492,977
11211/UDP	Memcached	3,271,303
19/UDP	CharGen	1,040,038
161/UDP	SNMP	257,161
1900/UDP	SSDP	117,048
17/UDP	QotD	4,750

(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
389/UDP	CLDAP	31,926,706
123/UDP	NTP	4,267,386
3702/UDP	WSD	2,139,524
53/UDP	DNS	1,808,548
37020/UDP	Hikvision SADP	1,699,090
3478/UDP	STUN	1,293,056
3283/UDP	ARMS	1,128,914
5683/UDP	CoAP	990,656
19/UDP	CharGen	627,505
1434/UDP	MSSQL	381,555

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 86% 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 14%（2024 年は約 23%）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 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，攻撃対象の組織を把握するには，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，

*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標的にした 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 年のサービス数の急増は，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．

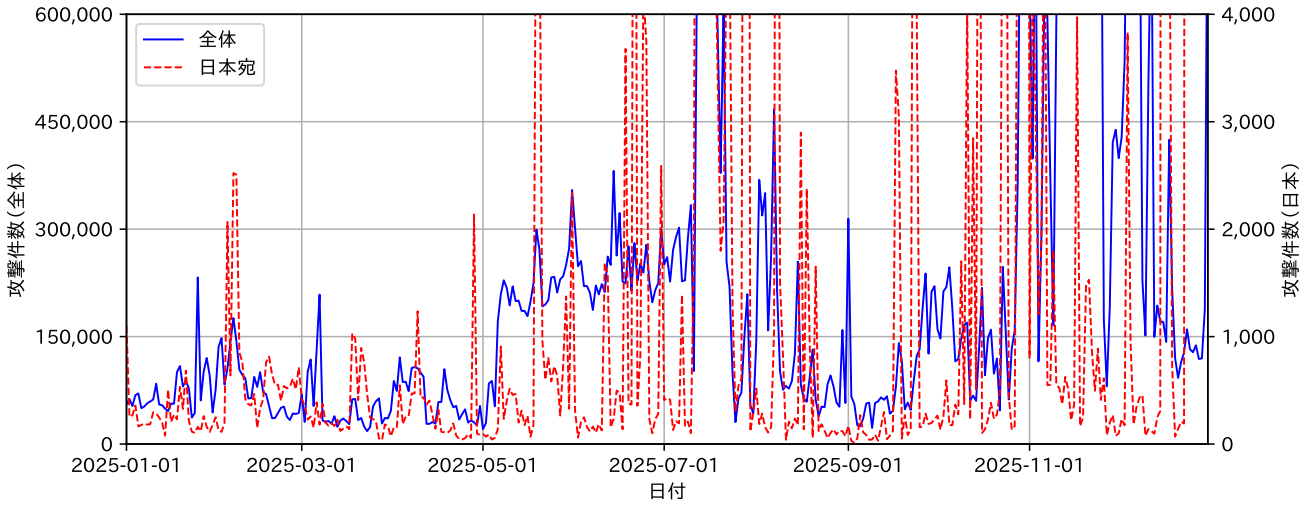

図10: 日ごとの DRDoS 攻撃件数の推移（左軸：全体，右軸：日本宛）

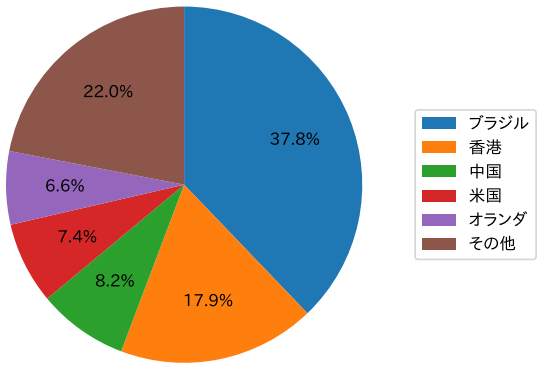

図11: 国・地域別の被攻撃件数

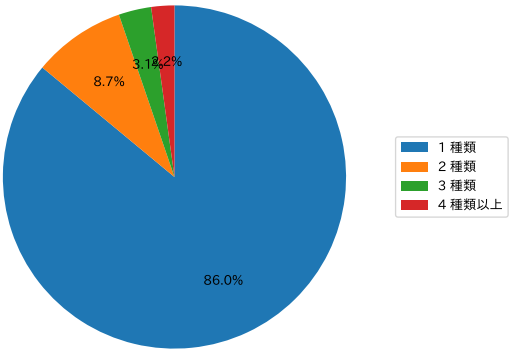

図13: 攻撃手法の種類数

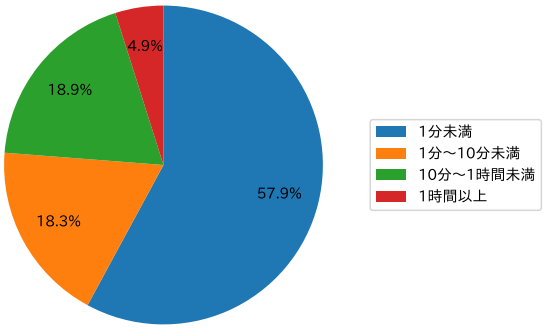

図12: 攻撃継続時間

クラウドサービス事業者のものや個人利用者が契約して使用している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．

2025 年の 1 年間に，日本の 29,583 個の IP アドレスに対して約 90 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（Autonomous System）・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 45 組織宛の攻撃を確認することができました[*15]．以下に，2025 年に観測された日本の組織を標的とした攻撃事例を報告します．

2025 年上半期に観測されたこの事例では，国内の企業で使用される 3 つの IP アドレスが標的になりました．この攻撃の時系列を表 5 に示します．全体を通して，ある 1 個の IP アドレス（IP-1）を中心に攻撃が観測されました．攻撃の継続時間はほとんどが 1～3 分程度で，NTP を

*15. 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5: 日本の組織を狙った DRDoS 攻撃の観測事例 （注: 紙面の都合上，10 分以下の攻撃は開始時刻のみを記載。）

時刻	攻撃対象	悪用されたサービス名
2025/04/11 22:48	IP-1	NTP
2025/04/12 05:12	IP-1	WSD
2025/04/13 11:52, 14:21	IP-1	DNS, NTP, WSD
2025/04/14 04:16, 04:20, 04:24	IP-1, IP-2	ARD, WSD, CoAP, Hikvision SADP
2025/05/08 19:13, 19:26, 19:54, 20:13, 22:18, 22:26, 22:29, 22:33, 22:43, 22:54, 22:57, 23:46	IP-1	NTP, Memcached
2025/05/08 19:46	IP-2	NTP
2025/05/09 00:17, 16:16, 16:27, 16:36	IP-1	NTP
2025/05/12 23:58	IP-1	NTP
2025/05/13 15:14, 15:34, 15:59, 16:11, 17:05	IP-1	NTP, Memcached
2025/05/16 20:59, 21:10	IP-1	NTP, SSDP
2025/06/06 17:45	IP-1	NTP
2025/06/14 17:21, 17:26	IP-3	ARD, STUN, WSD, CoAP

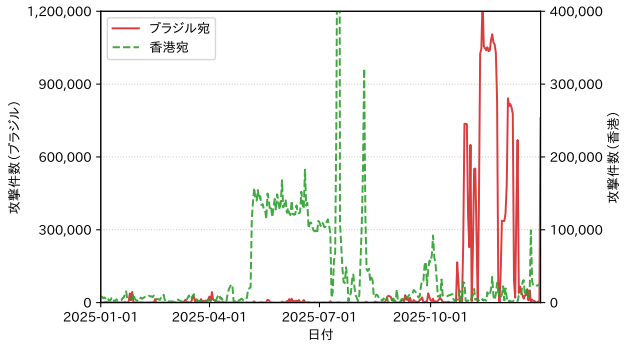

図14: ブラジル・香港宛の日ごとの攻撃件数の推移

中心に様々なサービスを悪用した攻撃が観測されました．特に，5 月 8 日には夕方以降，NTP と Memcached を悪用した断続的な攻撃が観測されました．このように短時間の攻撃を何度も執拗に繰り返す攻撃事例が観測されています．

4.2.2 ブラジル・香港宛の絨毯爆撃攻撃事例

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，2025 年に観測されたブラジル・香港宛の絨毯爆撃型 DRDoS 攻撃について報告します．

ブラジル宛の攻撃件数の推移を図 14 の赤色の実線（左軸）で示します．ブラジル宛の通常時の攻撃件数は多くありませんが，10 月後半から 12 月にかけて CLDAP を悪用した攻撃件数が急増しました．この時期に観測された IP アドレスを分析した結果，/24 の 256 の IP アドレスのうち 100 IP アドレス以上で攻撃が観測されたネットワークが 935 個存在しました．これらのネットワークが所属する AS 等に大きな偏りはなく，攻撃が急増したいずれの期間でも，類似したアドレス帯宛の攻撃が観測されました．これらの絨毯爆撃型の攻撃の標的は不明ですが，ブラジルのネットワークの広い範囲が攻撃されていたものと考えられます．

香港宛の攻撃件数の推移を図 14 の緑色の点線（右軸）で示します．通常時の香港宛の攻撃件数は 1 日数千件程度ですが，5 月前半から 7 月前半にかけて，1 日あたり約 10 万件の攻撃が継続して観測されました．この期間に標的となったのは，アメリカに本社を置く企業が運営する香港関連のネットワークでした．また，7 月 17 日には香港の 3 つの AS に対して 1 日で約 130 万件の香港宛の攻撃が観測されたほか，8 月前半には 2 つの AS に対して 1 日約 30 万件の攻撃が観測されました．これらの香港宛の絨毯爆撃型攻撃では，主に NTP が悪用されていました．

4.2.3 NTP を悪用した攻撃件数の減少

ntpd の monlist を悪用したアンプ攻撃はこれまで長期にわたって数多く観測されてきましたが，2025 年 9 月以降，その攻撃件数の減少が確認されました．

NTP を悪用した DRDoS 攻撃件数の推移を図 15 に示します．2025 年の前半には，1 日あたり約数万件の攻撃が観測されていました．5 月から 8 月にかけて見られる攻撃件数の急増は，4.2.2 節で述べた香港宛の絨毯爆撃型攻撃によるものです．その後，攻撃件数は急減し，9 月から 10 月頃に一旦は同程度の水準まで回復したものの，それ以降は 1 日数百件から数千件程度にまで減少しています．

過去に，DDoS 攻撃代行サービスの Booter/Stresser

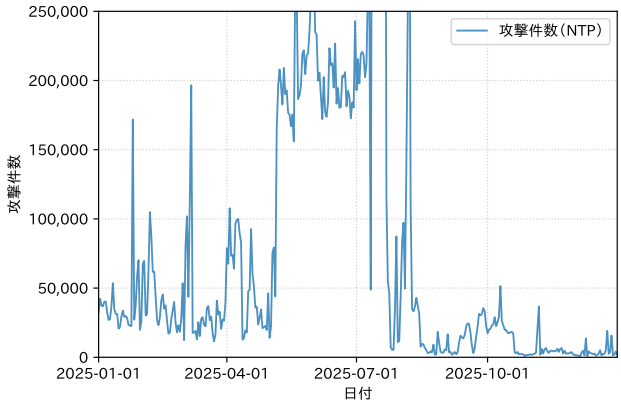

図15: NTP を悪用した攻撃件数の推移

がテイクダウンされた際に，特定のサービスを悪用する攻撃件数が著しく減少した事例はありました．しかし，現状ではそのような事象は確認されておらず，NTP を悪用した攻撃の減少の理由はわかっていません．

5. おわりに

本レポートでは，NICTER プロジェクトにおいてダークネットおよび各種ハニーポットを用いて実施した 2025 年のサイバー攻撃観測とその分析結果を報告しました．

2025 年においても，広域スキャンは観測された前パケット数の過半を占めました．これは，個別の脆弱性や攻撃手法といった特定の脅威に限らず，インターネット上に公開された機器やサービスが，常時第三者に探索される前提で運用されている現状を意味すると言えるでしょう．

IoT 機器を標的とする攻撃では，2016 年に登場した Mirai 以降に確立された IoT ボットの感染と拡大のパターンが，いまだに変化しながら繰り返されている現状が観測されました．本レポートで取り上げた RapperBot の事例では，Operation PowerOFF による法執行機関の介入という，社会的対応による脅威の排除が，実際に C2 通信の停止およびボットの活動終息として観測されましたが，一方で，感染ターゲットとなった脆弱な IoT 機器の多くは，依然として脆弱なまま放置されているのが現実です．

IoT 機器を巡る脅威は，利用者が被害に気付きにくいという特性から，社会的な把握が難しい課題です．NICT では，今後もダークネットやハニーポットを用いた継続的な観測と分析を通じて，攻撃の実態やその変化を明らかにするとともに，関係組織との情報共有や情報発信を通じて，実効性のあるサイバーセキュリティ対策の検討と向上に貢献していきます．

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，4 章 牧田，5 章 久保，全体統括 久保．

参考文献

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

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

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

[4] 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.

[5] 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.

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

[7] NICTER. NICTER 観測統計 - 2025 年 1 月〜3 月. https://blog.nicter.jp/2025/06/nicter_statistics_2025_1q/.

[8] NICTER. NICTER 観測統計 - 2025 年 4 月〜6 月. https://blog.nicter.jp/2025/09/nicter_statistics_2025_2q/.

[9] NICTER. NICTER 観測統計 - 2025 年 7 月〜9 月. https://blog.nicter.jp/2025/12/nicter_statistics_2025_3q/.

[10] NICTER. NICTER 観測統計 - 2025 年 10 月〜12 月. https://blog.nicter.jp/2026/02/nicter_statistics_2025_4q/.

[11] NIST. CVE-2024-3765. https://nvd.nist.gov/vuln/detail/CVE-2024-3765.

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

[13] 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 Sumposium, SEC '13, pages 605–620, 2013.

[14] Unveiling the DVR Ecosystem: A 3-Year Investigation into Global IoT Bot Recruitment Campaigns. https://www.botconf.eu/botconf-presentation-or-article/unveiling-the-dvr-ecosystem-a-3-year-investigation-into-global-iot-bot-recruitment-campaigns/.

[15] Yuki Umemura, Masaki Kubo, Yoshiki Mori, Hideyuki Furukawa, Kanta Okugawa, and Takahiro Kasama. Watchers compromised: The stealthy and persistent strategies of iot botnet. https://doi.org/10.1109/DSC65356.2025.11260869.

[16] RapperBot の C2 オペレーションと DDoS 攻撃の詳細. https://jsac.jpcert.or.jp/timetable.html.

[17] ASUS 製 WiFi ルーターの AiCloud 機能の脆弱性を悪用する攻撃に関する注意喚起. https://blog.nicter.jp/2025/04/asus_aicloud/.

[18] 修正された ASUS 製 WiFi ルーターの AiCloud 機能の脆弱性について. https://blog.nicter.jp/2026/01/aicloud_vulnerability/.

[19] プロセスを隠蔽する MountBot の出現. https://blog.nicter.jp/2025/08/mountbot_2025aug/.

[20] 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.

[21] 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/.

[22] 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.