プレスリリース
2025 年 2 月 13 日
国立研究開発法人情報通信研究機構

# NICTER 観測レポート 2024 の公開

【ポイント】

- NICTER プロジェクトにおける 2024 年のサイバー攻撃関連通信の観測・分析結果を公開
- IoT ボットの感染活動や調査機関等によるスキャンパケットが増加し、過去最高の観測パケット数を記録
- 国内の IoT ボット感染ホスト数は約 730～11,500 で推移

国立研究開発法人情報通信研究機構（ＮＩＣＴ、理事長: 徳田 英幸）サイバーセキュリティネクサス[*1] は、NICTER[*2] 観測レポート 2024 を公開しました。NICTER プロジェクトの大規模サイバー攻撃観測網で 2024 年に観測されたサイバー攻撃関連通信[*3] は、2023 年と比べて 11%増加しました。また、調査目的とみられるスキャンパケットの割合は 60.2%（2023 年は 63.8%）と、依然として全体の 6 割以上を占めており、インターネット上の IoT 機器や脆弱性を狙った調査が活発に行われていることが分かります。日本国内では、1 日当たり約 730～11,500 ホストが IoT ボットに感染していることが確認され、平均すると 1 日当たり約 2,600 台が感染している状況です。個別の観測事象として、2023 年に引き続き、DVR 製品への IoT ボット感染が活発に発生し、IoT 向け LTE ルータ[*4] の感染も顕著でした。一方で、DRDoS 攻撃[*5] の観測件数は減少傾向を示しました。さらに、日本の IP アドレスを標的とした攻撃は累計 17 万件に達しました。

NICT は、日本のサイバーセキュリティ向上に向けて、NICTER の観測・分析結果の更なる利活用を進めるとともに、セキュリティ対策の研究開発を進めていきます。

## 【背景】

NICT は、NICTER プロジェクトにおいて大規模サイバー攻撃観測網（ダークネット[*6] 観測網）を構築し、2005 年からサイバー攻撃関連通信の観測を続けてきました。2021 年 4 月 1 日（木）に、サイバーセキュリティ分野の産学官の『結節点』となることを目指した新組織サイバーセキュリティネクサス（Cybersecurity Nexus: CYNEX）が発足し、そのサブプロジェクトの一つである Co-Nexus S においてサイバーセキュリティ関連の情報発信を行っています。

## 【今回の成果】

CYNEX は、NICTER プロジェクトの 2024 年の観測・分析結果を公開しました（詳細は、「NICTER 観測レポート 2024」https://csl.nict.go.jp/report/NICTER_report_2024.pdf 参照）。

NICTER のダークネット観測網（約 29 万 IP アドレス）において 2024 年に観測されたサイバー攻撃関連通信は、合計 6,862 億パケットに上り、1 IP アドレス当たり約 242 万パケットが 1 年間に届いた計算になります（表 1 参照）。

表 1 NICTER ダークネット観測統計（過去 10 年間）

| 年 | 年間総観測パケット数 | ダークネットIPアドレス数 | 1 IPアドレス当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** |

注: 年間総観測パケット数は、レポート作成時点のデータベースの値に基づきますが、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、あくまで NICTER で観測しているダークネットの範囲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。
ダークネット IP アドレス数は、当該年 12 月 31 日にパケットを受信したアクティブセンサ数を示します。アクティブなセンサの数は、年間を通じて一定ではなく変化することがあります。

表 1 のうち年間総観測パケット数は観測 IP アドレス数に大きく影響を受けますので、1 つの IP アドレスを 1 年間観測したときに届くパケット数がインターネット上のスキャン活動の活発さを測るには適しています。この値の過去 10 年間の推移を示したのが図 1 です。2024 年は 2023 年とほぼ同じダークネット観測規模（ダークネット IP アドレス数）で観測を行いましたが、1 IP アドレス当たりの年間総観測パケット数は前年の 2023 年から更に増加しており、インターネット上を飛び交う探索活動が更に活発化していることが数字から読み取れます。

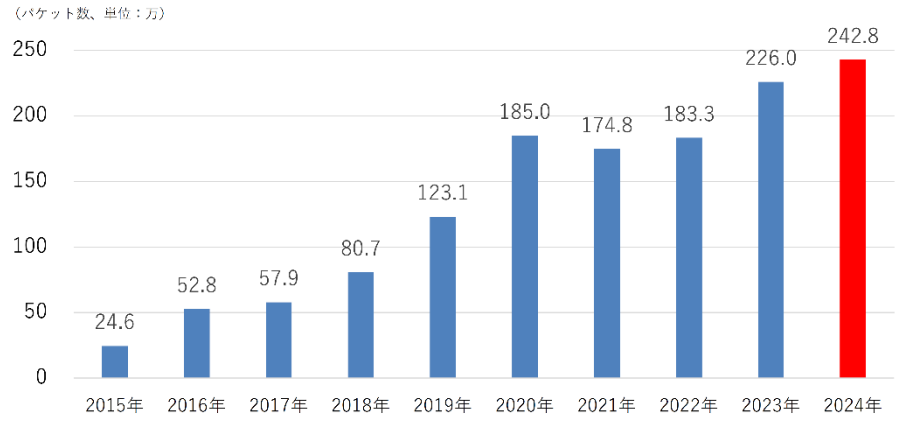
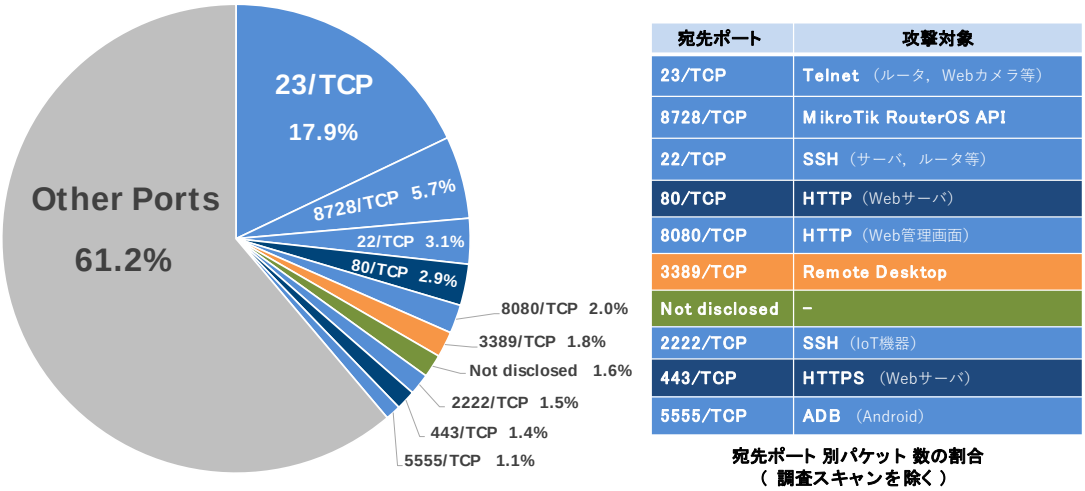



図 1 1 IP アドレス当たりの年間総観測パケット数（過去 10 年間）

また、総観測パケットに占める海外組織からの調査目的と見られるスキャンの割合は、2023 年の 63.8%からわずかに減少し、60.2%を占めました。調査機関によるスキャンパケットが半数以上を占める傾向は 2019 年以降継続しています。

このような調査目的のスキャンパケットを除いた上で、2024 年に NICTER で観測した主な攻撃対象（宛先ポート番号）の上位 10 位までを表したものが図 2 です。円グラフの水色の部分が、Web カメラやホームルータなどの IoT 機器に関連したサイバー攻撃関連通信です。




| 宛先ポート | 攻撃対象 |
|---|---|
| 23/TCP | Telnet （ルータ，Webカメラ等） |
| 8728/TCP | MikroTik RouterOS API |
| 22/TCP | SSH （サーバ，ルータ等） |
| 80/TCP | HTTP （Webサーバ） |
| 8080/TCP | HTTP （Web管理画面） |
| 3389/TCP | Remote Desktop |
| Not disclosed | – |
| 2222/TCP | SSH （IoT機器） |
| 443/TCP | HTTPS （Webサーバ） |
| 5555/TCP | ADB （Android） |

宛先ポート 別パケット 数の割合
（ 調査スキャンを除く ）

図 2 宛先ポート別パケット数の割合（調査スキャンを除く）

注: 3 位の 22/TCP には、一般的なサーバ（認証サーバなど）へのスキャンパケットも含まれます。また、その他のポート番号（Other Ports）の中には IoT 機器を狙ったパケットが多数含まれます。

上位 10 位までのポートが全体に占める割合は、2023 年から減少しました。減少の要因としては、最も多い Telnet（23/TCP）を狙った攻撃が占める割合が、2023 年の 27.1%から 17.9%へと大きく減少したことが挙げられます。その他のポート番号宛ての通信については、2023 年と比べて多少の順位の入れ替わりはあるものの傾向の大きな変化

は見られず、IoT 機器が使用する特徴的なポート宛ての通信が上位に多く観測される傾向が継続しました。7 番目に多く観測されたポート宛のパケットは、海外の特定の IP アドレスからの局所的なスキャンによるものであったため、観測基盤の保護のため非公開（Not disclosed）としています。

個別の観測事象に目を向けると、2021 年以降継続して観測されている韓国製 DVR 製品の Mirai[*7] 感染に加え、家庭用 WiFi ルータやモバイル回線に接続された IoT 向け LTE ルータがボットに感染し、DDoS 攻撃の踏み台として悪用されるケースが確認されました。また、日本国内で IoT マルウェアに感染したいわゆる IoT ボットの数は、約 730～11,500 ホストの範囲で推移し、その半数以上が Mirai の特徴を持たない IoT マルウェアに感染したホストでした。NICTER プロジェクトでは、製品開発者や機器を設置したユーザーの協力の下、機器の脆弱性調査や実機をインターネットに接続した攻撃観測、感染機器のフォレンジック調査[*8] などを実施し、攻撃の実態把握及び製品開発者との観測結果の共有に努めました。

DRDoS 攻撃の観測では、年間の攻撃件数が 2023 年の 5,561 万件から 3,095 万件へと落ち込みました。ただし、これは 2023 年に絨毯爆撃型[*9]DRDoS 攻撃が頻繁に発生した影響によるもので、2022 年とほぼ同じ規模となっています。また、攻撃に悪用されたサービスの種類も減少しており、2023 年の 31 種類から 2024 年は 18 種類に減りました。

インターネットに公開された機器やサービスの脆弱性が悪用され、組織やユーザーが侵害される状況が続いています。 NICTER プロジェクトの観測でも、第三者による広域スキャンの増加傾向が確認されています。こうした状況を踏まえ、IT 資産の脆弱性管理の重要性を改めて認識することが不可欠です。特に、IoT 機器の感染のように、製品メーカーやユーザー自身が把握しづらい侵害の実態や、その対策方法について、関係者間で迅速に情報共有し、被害の拡大を防ぐための注意喚起を速やかに行うことがますます重要になっています。

**【今後の展望】**

NICT では、日本のサイバーセキュリティ向上のため、CYNEX が産学官の結節点となり、サイバーセキュリティ関連情報の発信力の更なる強化を行うとともに、セキュリティ対策の研究開発を進めていきます。

## ＜NICTER 観測レポート 2024（詳細版）＞

- NICTER 観測レポート 2024（Web 版）
  https://csl.nict.go.jp/nicter-report.html
- NICTER 観測レポート 2024（PDF 版）
  https://csl.nict.go.jp/report/NICTER_report_2024.pdf

---

＜ 本件に関する問合せ先 ＞
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 研究開発運用室
安田 真悟、久保 正樹
E-mail: nicter@ml.nict.go.jp

＜ 広報（取材受付）＞
広報部 報道室
E-mail: publicity@nict.go.jp

## ＜用語解説＞

***1 サイバーセキュリティネクサス**

2021 年 4 月 1 日（木）に、サイバーセキュリティ分野の産学官の『結節点』となることを目指して、NICT 内に発足した新組織サイバーセキュリティネクサス（Cybersecurity Nexus: CYNEX（サイネックス））は、4 つのサブプロジェクト Co-Nexus A/S/E/C から構成される。

***2 インシデント分析センター NICTER**

NICTER（Network Incident analysis Center for Tactical Emergency Response）は、NICT が研究開発している、コンピュータネットワーク上で発生する様々な情報セキュリティ上の脅威を広域で迅速に把握し、有効な対策を導出するための複合的なシステムである。サイバー攻撃の観測やマルウェアの収集などによって得られた情報を相関分析し、その原因を究明する機能を持つ。

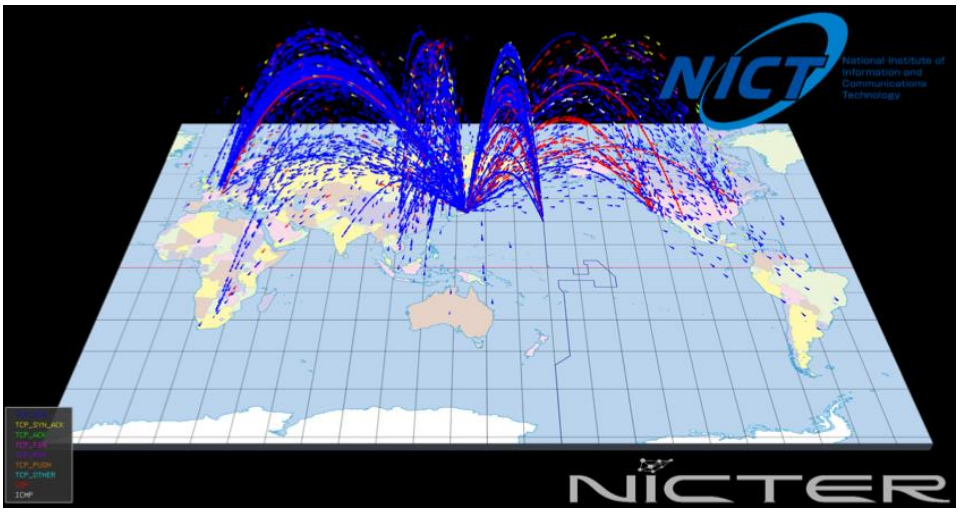



図 3 NICTER Atlas によるダークネットで観測された通信の可視化

***3 サイバー攻撃関連通信**

ダークネットに届くパケットの総称。マルウェアに感染した機器がインターネット上で次の感染先を探すためのスキャンパケットや、DoS 攻撃を受けているサーバからの跳ね返りパケット（バックスキャッタ）などが含まれる。

***4 LTE ルータ**

4G/LTE のモバイルネットワーク回線を使用してインターネットに接続するルータ。遠隔地や屋外等において安定的なインターネット接続を必要とする産業機器や各種センサに用いられることが多い。

***5 DRDoS 攻撃**

DRDoS 攻撃（Distributed Reflection Denial-of-Service Attack）とは、インターネット上の DNS や NTP 等のサーバを悪用して攻撃対象に大量のパケットを送付し、攻撃対象のネットワーク帯域を圧迫する DDoS 攻撃の一種のこと。

***6 ダークネット**

インターネット上で到達可能かつ未使用の IP アドレス空間のことを指す。未使用の IP アドレスに対しパケットが送信されることは、通常のインターネット利用の範囲においてはまれであるが、実際にダークネットを観測してみると、相当数のパケットが到着することが分かる。これらのパケットの多くは、マルウェアの感染活動など、インターネットで発生している何らかの不正な活動に起因している。そのため、ダークネットに到着するパケットを観測することで、インターネット上の不正な活動の傾向把握が可能になる。

***7 Mirai**

家庭用ルータやネットワークカメラといった IoT 機器に感染するマルウェアの一種。Mirai に感染した機器は DoS 攻撃の踏み台として悪用され、攻撃対象のホストに大量のパケットを送信させられる。

***8 フォレンジック調査**

フォレンジック調査（デジタル・フォレンジック）とは、サイバー攻撃の痕跡を、ログやファイル、メモリデータなどのデジタルデータから分析し、侵入経路や被害の範囲を特定するとともに、証拠を適切に保全する調査のこと。

***9 絨毯爆撃型**

単一の IP アドレスではなく主に同一ネットワーク内の広い範囲の IP アドレスに対して行われる攻撃。