プレスリリース
2026 年 2 月 5 日
国立研究開発法人情報通信研究機構

NICTER 観測レポート 2025 の公開

【ポイント】

- 2025 年のサイバー攻撃に関連する通信がダークネット観測開始以降で過去最多を記録
- IoT 機器を狙う攻撃では、Mirai 以外の IoT ボットの感染が増加し、ボットの多様化が進行
- DRDoS 攻撃は絨毯爆撃型の攻撃が頻発し、攻撃件数が増加傾向

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 2025 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 2025 年に観測されたサイバー攻撃関連通信[*3] は約 7,010 億パケットに達しました（2024 年から約 2.2%増加）。観測規模がほぼ同じ 2024 年と比較すると、1 IP アドレス当たりの年間観測パケット数は約 7 万パケットの増加にとどまるものの、インターネット上での探索活動や攻撃準備行動は高い水準で常態化しています。IoT ボット[*4] の感染動向では、Mirai[*5] の特徴を持たない IoT ボット感染ホスト数が Mirai 感染を上回る状況が世界的に観測されたほか、DRDoS 攻撃[*6] の観測では、絨毯爆撃型[*7]の攻撃が頻発したことを受け、攻撃件数が前年から大幅に増加しました。

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[*8] 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 2025 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 2025」https://csl.nict.go.jp/report/NICTER_report_2025.pdf 参照）。主な観測結果は次のとおりです。

■ ダークネット観測統計：探索活動の常態化と多様化

NICTER のダークネット観測網（約 28 万 IP アドレス）において 2025 年に観測されたサイバー攻撃関連通信は、合計 7,010 億パケットに上り、1 IP アドレス当たり約 250 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
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**	**2,504,679**

注: ダークネット IP アドレス数（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、2025 年は 12 月 26 日のアドレス数です。

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るため、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。図 1 に示すとおり、1 IP アドレス当たりの年間総観測パケット数は、前年の 2024 年から微増し、インターネット上を飛び交う探索活動が高い水準で常態化していることが数字から読み取れます。なお、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。

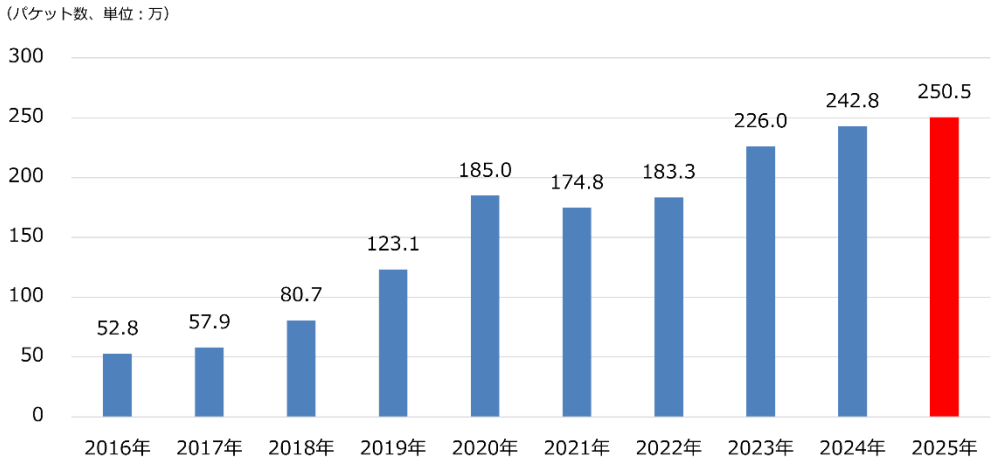
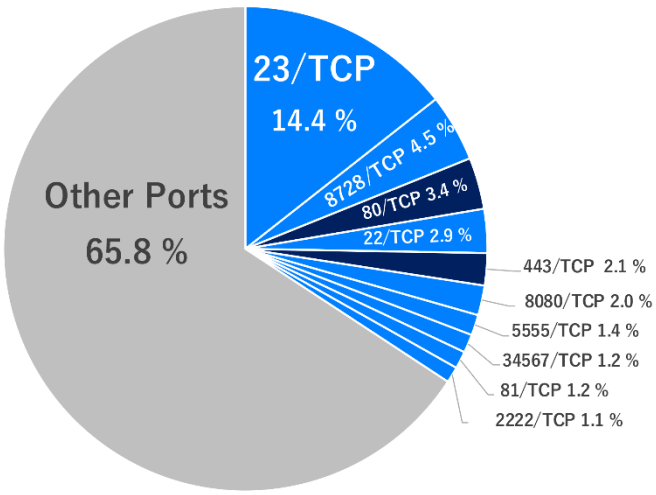


図 1 1 IP アドレス当たりの年間総観測パケット数（過去 10 年間）

また、2025 年に観測されたパケットのうち、調査目的と推定されるスキャン通信は全体の約 55%を占めました。前年（約 60%）から割合はやや減少したものの、依然として全体の半数以上を占める状況が継続しています。

また、Telnet（23/TCP）宛の通信の割合は年々減少傾向にある一方で（図 2 参照）、多数のポート番号を対象とするスキャンが増加しています。上位 10 ポート以外のその他を示す Other Ports の占める割合が増加傾向にあり、IoT 機器やネットワーク機器を幅広く探索する傾向が顕著になっています。



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
80/TCP	HTTP （Webサーバ）
22/TCP	SSH （サーバ、ルータ等）
443/TCP	HTTPS （Webサーバ）
8080/TCP	HTTP （Web管理画面）
5555/TCP	ADB （Android）
34567/TCP	Xiongmai DVR API
81/TCP	HTTP （Web管理画面）
2222/TCP	Telnet （ルータ，Webカメラ等）

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 80/TCP、5 位の 443/TCP には、一般的な Web サーバ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。

■ IoT 機器を狙う攻撃が高度化・多様化

従来主流だった Mirai 型とは異なる IoT ボットの感染活動が拡大し、家庭用ルータや監視カメラの録画機器など、利用者が感染に気付きにくい機器が引き続き標的となっています。

NICTER では、IoT 機器を標的とするボットの一つである RapperBot について、2025 年も継続的に観測と分析を行いました。その結果、世界全体で約 6 万台規模の IoT 機器が RapperBot に感染していた可能性を明らかにしました。また、感染が特定ベンダーの機器に偏っている状況も確認されています。

さらに、米国司法省による RapperBot 運営者の起訴が発表された 2025 年 8 月を境に、攻撃者の指令サーバからの通信が停止したことを確認しました。

一方で、感染後に機器内部で不正な動作を行っていることを利用者や管理者から見えにくくする仕組み（プロセス隠蔽[*9]）を備えた新たな IoT ボットが、家庭用ルータなど複数種の IoT 機器を標的として活動している状況も観測されました。

■ DRDoS 攻撃：再増加と攻撃手法の変化

DRDoS 攻撃については、2025 年に世界全体で約 8,285 万件、日本宛で約 90 万件を観測しました。攻撃件数は前年から大幅に増加しており（2024 年は世界全体で約 3,095 万件、日本宛は約 17 万件）、特に絨毯爆撃型の攻撃が頻発しています。一方で、攻撃に悪用されるサービスの種類は年々減少しており、攻撃手法の集約・効率化が進んでいる可能性が示唆されます。

【今後の展望】

インターネットに常時接続される IoT 機器の増加に伴い、広域スキャンや IoT ボット感染は今後も継続すると予想されます。NICT では、NICTER による継続的な観測・分析を通じて、攻撃の実態把握と注意喚起を行うとともに、産学官の連携拠点である CYNEX を通じた情報共有と研究開発を一層推進していきます。

＜NICTER 観測レポート 2025（詳細版）＞

- NICTER 観測レポート 2025（Web 版）
  https://csl.nict.go.jp/nicter-report.html
- NICTER 観測レポート 2025（PDF 版）
  https://csl.nict.go.jp/report/NICTER_report_2025.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。

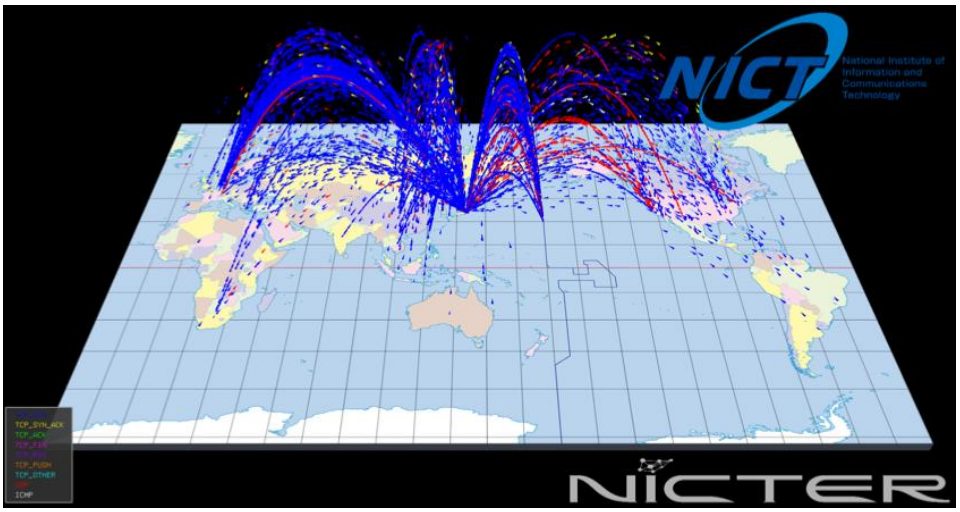


図 3 NICTER Atlas によるダークネットで観測された通信の可視化

***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 IoT ボット**

インターネットに接続された機器に侵入し、攻撃者の指示で不正な通信や攻撃を行うプログラム。

***5 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。

***6 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。

***7 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。

***8 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。

***9 プロセス隠蔽**

不正なプログラムが動作していることを、機器の利用者や管理者から分かりにくくする仕組み。