国立研究開発法人
情報通信研究機構

プレスリリース
2023 年 2 月 14 日
国立研究開発法人情報通信研究機構

NICTER 観測レポート 2022 の公開

【ポイント】

- NICTER プロジェクトにおける 2022 年のサイバー攻撃関連通信の観測・分析結果を公開
- Telnet（23/TCP）宛攻撃の割合が増加に転じたほか、IoT 機器のゼロデイ脆弱性を悪用した攻撃を観測
- DRDoS 攻撃観測では、攻撃件数の減少、攻撃時間の増加、攻撃に悪用されるサービスの種類の増加を観測

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 2022 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 2022 年に観測されたサイバー攻撃関連通信[*3] は、2021 年と比べ僅かに増加し、Telnet（23/TCP）を狙う攻撃の割合が増加しました。個別の観測事象としては、複数の DVR 製品への Mirai[*4] の感染が観測されましたが、NICTER プロジェクトでは製品ベンダの協力の下、脆弱性の調査や実機を使った攻撃観測を実施し、ゼロデイ脆弱性[*5] を悪用する攻撃が脆弱な機器に対してピンポイントで行われている実態を明らかにしました。DRDoS 攻撃[*6] の観測では、大規模な絨毯爆撃型[*7] の DRDoS 攻撃の規模の縮小による DRDoS 攻撃件数の減少、攻撃の継続時間の長時間化、及び攻撃に悪用されるサービスの種類の増加といった傾向の変化が見られました。

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 2022 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 2022」https://www.nict.go.jp/cyber/report/NICTER_report_2022.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 2022 年に観測されたサイバー攻撃関連通信は、合計 5,226 億パケットに上り、1 IP アドレス当たり約 183 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
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**

注: 年間総観測パケット数は、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。

図 1 は、1 IP アドレス当たりの年間総観測パケット数を 2013 年からグラフ化したものです。2022 年の 1 IP アドレス当たりの年間総観測パケット数は、前年の 2021 年から僅かな増加を見せたものの、ほぼ同じ水準で推移しました。

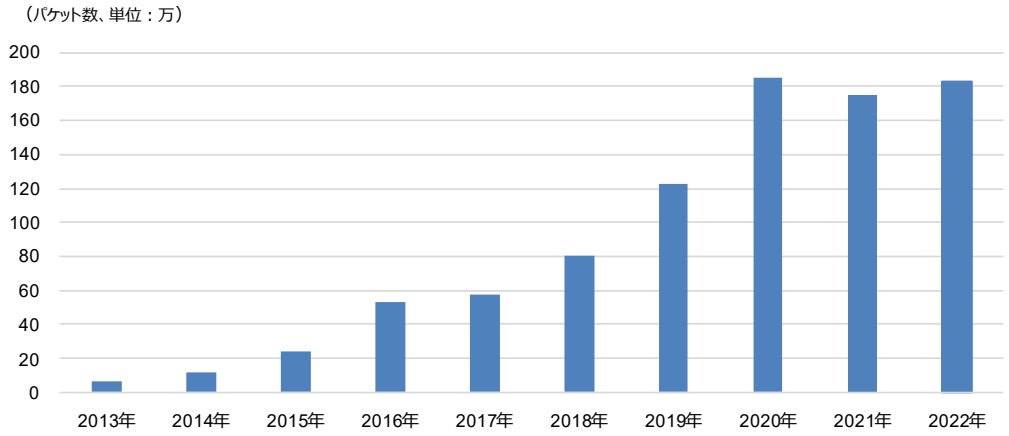
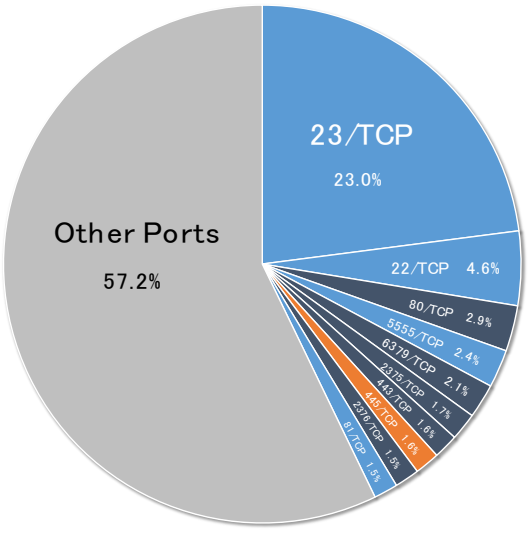


図 1. 1 IP アドレス当たりの年間総観測パケット数（過去 10 年間）

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みられるスキャンの割合は約 54.9%と半数以上を占めました。2019 年以降、半数以上を占める傾向が続いています。

このような調査目的のスキャンパケットを除いた上で、2022 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。



ポート番号	攻撃対象
23/TCP	Telnet （ルータ，Webカメラ等）
22/TCP	SSH （サーバ，ルータ等）
80/TCP	HTTP （Web管理画面）
5555/TCP	ADB (Android Debug Bridge)
6379/TCP	Redis
2375/TCP	Docker REST API
443/TCP	HTTPS (Webサーバ)
445/TCP	Windows SMB
2376/TCP	Docker REST API
81/TCP	HTTP （ホームルータ等）

宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

図 2. 宛先ポート番号別パケット数分布（調査目的のスキャンパケットを除く）

注: 2 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、2020 年以降減少傾向にありましたが 2022 年は増加に転じ、2021 年の 31.3%から 42.8%へと増えました。この増加の主な要因は、IoT 機器で依然として使用されている Telnet（23/TCP）を狙った攻撃が占める割合が、2021 年の 11.0%から 23.0%へと増加したことにあります。IoT 機器が使用する特徴的なポート番号はこれまでにもボットネットの攻撃対象として多く観測されていましたが、2022 年は特に 23/TCP を含むポートセット宛の攻撃が活発に観測されました。

Windows に関連するポートの観測は、上位 10 位中では 445/TCP（ファイル共有等で使われる）のみにとどまり、その順位も 2021 年 3 位から 8 位へと後退しました。NoSQL データベースの Redis で使われる 6379/TCP や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 REST API の 2375/TCP と 2376/TCP は上位に観測され、これらのサービスを狙う攻撃が 2021 年から継続しています。

そのほか、2022 年に特徴的な観測事象としては、日本国内において複数の DVR 製品が Mirai に感染し、DDoS 攻撃の踏み台として悪用される事象が発生しました。NICTER プロジェクトでは、製品開発者の協力の下、機器の脆弱性を調査し、製品開発者が存在を知らない未知の脆弱性が存在することを明らかにしたほか、この脆弱性を悪用する攻撃が対象となる機器のみに対してピンポイントで送られている実態を観測しました。

DRDoS 攻撃の観測では、2021 年に多く見られた絨毯爆撃型の DRDoS 攻撃の規模が縮小し、その結果、DRDoS 攻撃件数が減少して 2020 年の水準に戻ったほか、1 時間以上継続した攻撃の割合が前年の約 2.9%から約 16%へと増加し、攻撃に悪用されるサービスの種類についても前年の 38 種類から 151 種類に増加するといった傾向の変化が見られました。

インターネット全体を広範囲にスキャンすることで脆弱な IoT 機器やサーバ等を探索する活動は、引き続き活発に観測されている一方で、脆弱性を悪用する攻撃コードが攻撃対象の機器のみに対して送られている様子も観測されています。インシデントに関する情報を迅速に共有し、対策方法の検討や啓発、被害の拡大防止に向けた脆弱性対策を迅速に行うことが、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 2022（詳細版）＞

- NICTER 観測レポート 2022（Web 版）
  https://www.nict.go.jp/cyber/report.html
- NICTER 観測レポート 2022（PDF 版）
  https://www.nict.go.jp/cyber/report/NICTER_report_2022.pdf

＜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）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。

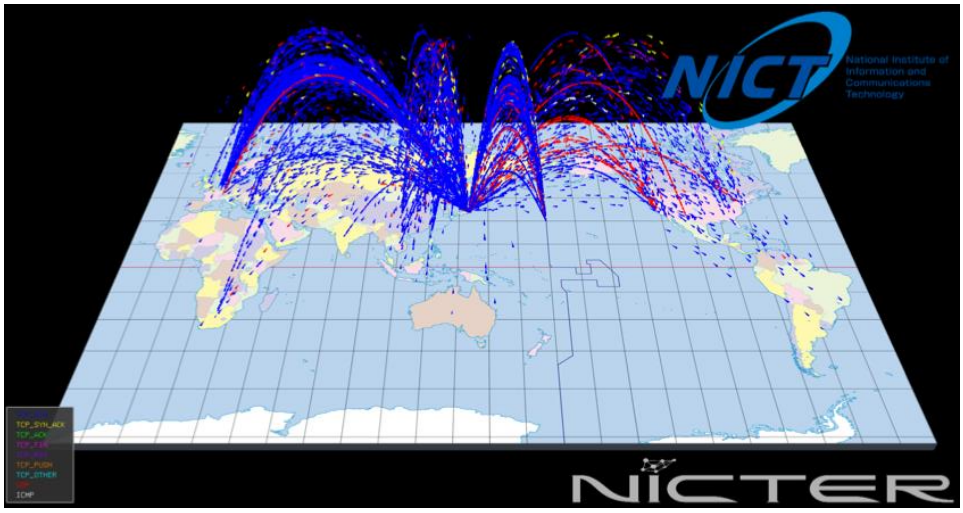


図 3. NICTER Atlas によるダークネットで観測された通信の可視化

***3 サイバー攻撃関連通信**

ダークネット[*8]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 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。

***5 ゼロデイ脆弱性**

ソフトウェア製品の脆弱性の中でも開発者がその存在を知らず、修正パッチ等の対策が提供されていないもの。

***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。

＜ 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
井上 大介、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