国立研究開発法人
情報通信研究機構

プレスリリース
2020年2月10日
国立研究開発法人情報通信研究機構

NICTER 観測レポート 2019 の公開

【ポイント】

- NICTER プロジェクトにおける 2019 年のサイバー攻撃関連通信の観測・分析結果を公開
- サイバー攻撃関連通信は、調査目的のスキャン活動が 2018 年より活発化し、全体の過半数に
- IoT 機器を狙う攻撃の傾向は 2018 年とほぼ同じで、Telnet(23/TCP)宛が僅かに増加

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研究所は、NICTER[*1] 観測レポート 2019 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 2019 年に観測されたサイバー攻撃関連通信[*2]は、2018 年と比べて約 1.5 倍と昨年以上の増加傾向にあります。内訳としては、海外組織からの調査目的とみられるスキャンの増加が著しく、総観測パケットの 53%を占めました。IoT 機器を狙った通信の傾向は 2018 年とほぼ同じで、最も多い Telnet(23/TCP)[*3] を狙う攻撃が占める割合は僅かに増加しました。その他、Windows のリモートデスクトップの脆弱性公表の影響などもあり、昨年より多くの Windows 関連ポートが上位を占める傾向がみられました。

NICT では、日本の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、IoT 機器のセキュリティ対策の研究開発を進めていきます。

【背景】

NICT サイバーセキュリティ研究所では、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[*4]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。

【今回の成果】

NICT は、NICTER プロジェクトの 2019 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 2019」https://www.nict.go.jp/cyber/report/NICTER_report_2019.pdf 参照)。

NICTER のダークネット観測網(約 30 万 IP アドレス)において 2019 年に観測されたサイバー攻撃関連通信は、合計 3,279 億パケットに上り、1 IP アドレス当たり約 120 万パケットが 1 年間に届いた計算になります(図 1 参照)。

年	年間 総観測パケット数	観測IPアドレス数	1 IPアドレス当たりの 年間総観測パケット数
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1,281億	約30万	469,104
2017	約1,504億	約30万	559,125
2018	約2,121億	約30万	789,876
2019	**約3,279億**	**約30万**	1,209,112

図 1. NICTER ダークネット観測統計(過去 10 年間)

注: 年間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であり、これは日本全体や政府機関への攻撃件数ではありません。

図 2 は、1 IP アドレス当たりの年間総観測パケット数を 2010 年からグラフ化したものです。2019 年の総観測パケット数は、2018 年から約 1,160 億増加しましたが、この増分は、海外組織からの調査目的とみられるスキャンが昨年以上に増加したことに起因します。調査スキャンが総パケットに占める割合は、2017 年の 6.8%、2018 年の 35%から更に増加し、2019 年は 1,750 億パケット（総パケットの 53%）にも及ぶことが判明しました。

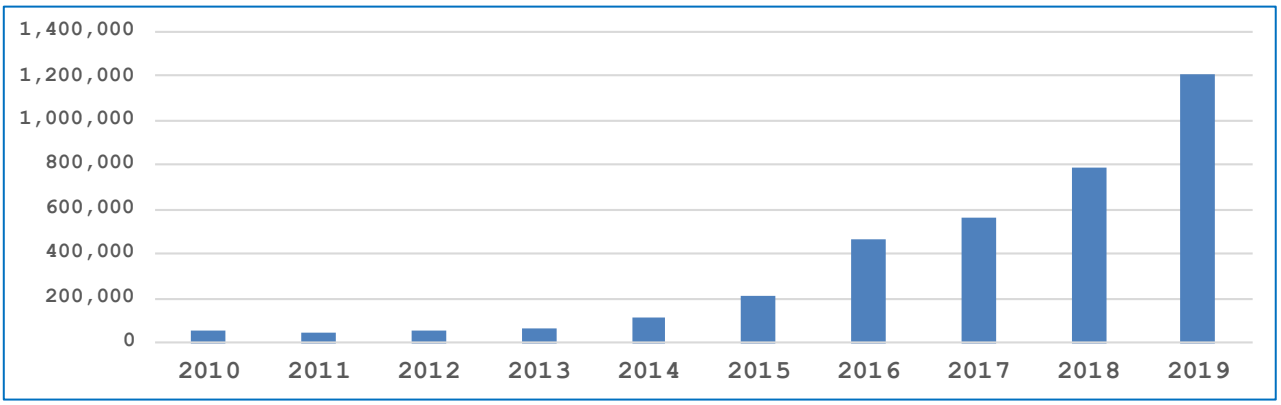
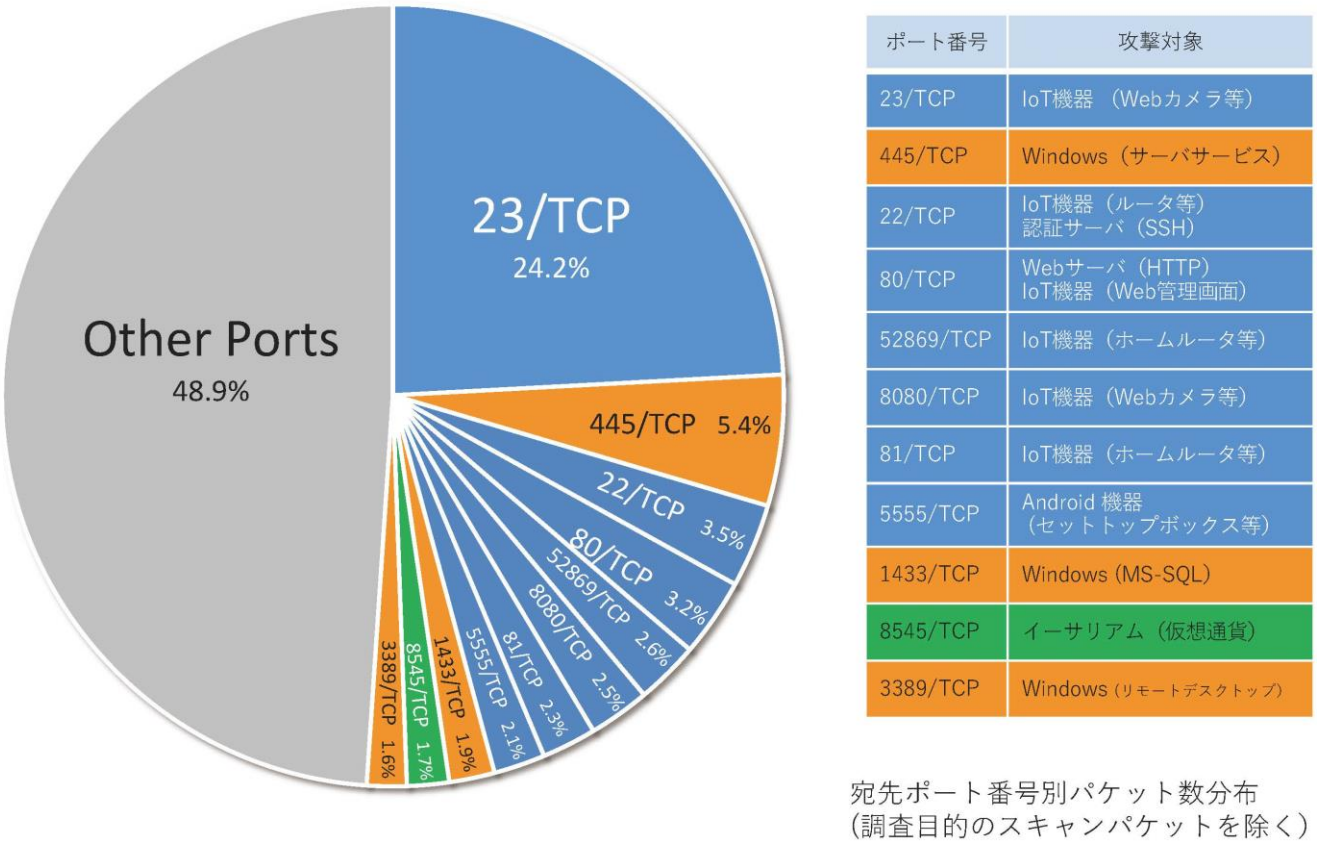


図 2. 1 IP アドレス当たりの年間総観測パケット数（過去 10 年間）

このような調査目的のスキャンパケットを除いた上で、2019 年に NICTER で観測した主な攻撃対象（宛先ポート番号）の上位 11 位までを表したものが図 3 です。円グラフの青色の部分が、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	IoT機器 （Webカメラ等）
445/TCP	Windows （サーバサービス）
22/TCP	IoT機器 （ルータ等） 認証サーバ （SSH）
80/TCP	Webサーバ （HTTP） IoT機器 （Web管理画面）
52869/TCP	IoT機器 （ホームルータ等）
8080/TCP	IoT機器 （Webカメラ等）
81/TCP	IoT機器 （ホームルータ等）
5555/TCP	Android 機器 （セットトップボックス等）
1433/TCP	Windows (MS-SQL)
8545/TCP	イーサリアム （仮想通貨）
3389/TCP	Windows (リモートデスクトップ)

図 3. 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: 3 位の 22/TCP には、一般的な認証サーバ（SSH）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も多数含まれます。

上位 10 位までのポートが全体に占める割合は、2018 年の 46%から 49%へと僅かに増加しました。増加の理由

としては、Telnet（23/TCP）を狙った攻撃パケット数が 294 億パケットから 364 億パケットへと僅かに増加したことが挙げられます。

その他のポート（Other Ports）の占める割合は全体の半数と目立ちますが、IoT 機器で使用されるポート（機器の Web 管理インターフェース用ポートや UPnP 関連ポート、機器に固有のサービス用ポートなど）が多数含まれており、それらのポートを合わせると、全体の約半数が IoT 機器で動作するサービスや脆弱性を狙った攻撃です。この傾向は、2018 年とほぼ同じ傾向です。

また、Windows 関連の観測傾向としては、ファイルやプリンタの共有で使われる 445/TCP を狙った攻撃が昨年に引き続き目立つほか、リモートデスクトップサービスに使われる 3389/TCP が上位に入っています。

そのほか、2019 年に特徴的な観測事象としては、SSL-VPN 製品*5 の脆弱性公表後に、これを悪用する攻撃が世界的に観測されました。また、ボットに感染したホストが、これまでに観測されなかった新しいポートの組合せで攻撃する事象も観測されています。DRDoS 攻撃*6 の観測では、複数のサービスを同時に悪用するマルチベクタ型の攻撃が多く観測されたほか、単一の IP アドレスではなく、AS*7 全体を狙う攻撃も観測されています。

IoT 機器の脆弱性が公開されると、その脆弱性を保有するホストに関する調査スキャンやそれを悪用するマルウェアの攻撃通信が観測されるというパターンが定式化しており、感染の未然防止や被害の拡大防止に向け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、IoT 機器の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 2019（詳細版）＞

- NICTER 観測レポート 2019（Web 版）
  https://www.nict.go.jp/cyber/report.html
- NICTER 観測レポート 2019（PDF 版）
  https://www.nict.go.jp/cyber/report/NICTER_report_2019.pdf

＜用語解説＞

***1 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。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。

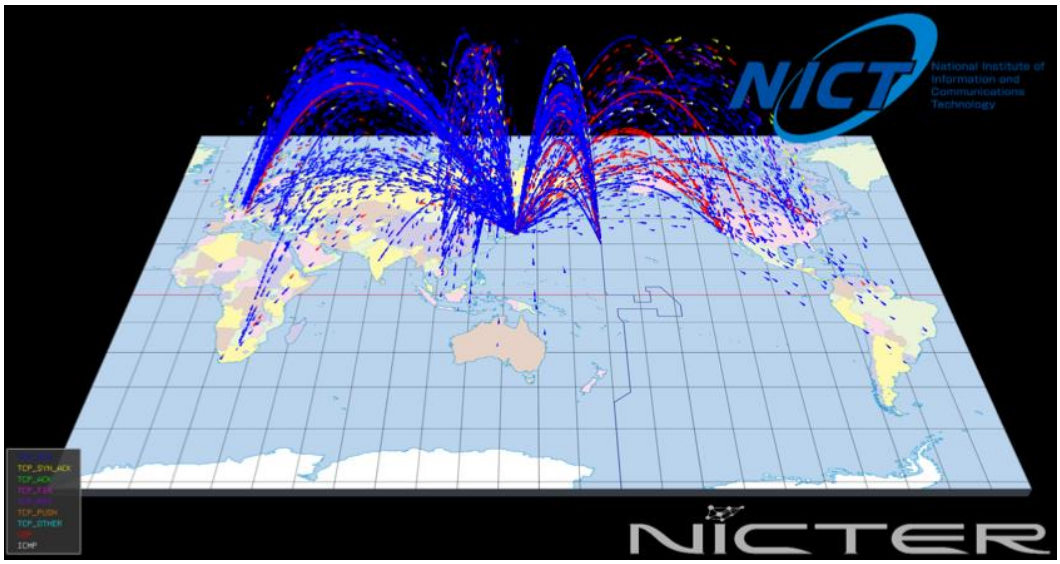


図 4. NICTER Atlas によるダークネットで観測された通信の可視化

***2 サイバー攻撃関連通信**

ダークネット[*4]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。

***3 Telnet（23/TCP）**

コンピュータを遠隔から操作するために用いられるプログラムで 23/TCP 番ポートが使われることが多い。設計が古く通信内容が暗号化されない等の問題があるが、現在でも一部の IoT 機器で使われている。ユーザ名とパスワードを入力してログインする仕組みであるが、IoT 機器等でよく使われるユーザ名とパスワードの組が攻撃者に知られており、IoT マルウェア「Mirai」の感染拡大に悪用された。

***4 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。

***5 SSL-VPN 製品**

遠隔から企業内ネットワークに VPN 接続するのに用いられる製品の一種。通常、VPN 接続には専用のクライアントソフトが用いられることが多いが、SSL-VPN ではウェブブラウザが用いられるため、汎用性が高く、規模の大きな組織で利用されている。

***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 AS**

「Autonomous System」の略。インターネット・サービス・プロバイダや大学など、決められたポリシーに従って運用されるネットワークの集まりを指す。個々の AS には番号が割り当てられ、これによりインターネット上で一意に識別される。

＜ 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研究室
井上 大介、久保 正樹
Tel: 042-327-6225
E-mail: nicter@ml.nict.go.jp

＜ 広報（取材受付） ＞
広報部 報道室
廣田 幸子
Tel: 042-327-6923
E-mail: publicity@nict.go.jp