国立研究開発法人
情報通信研究機構

プレスリリース
2019年2月6日
国立研究開発法人情報通信研究機構

NICTER 観測レポート 2018 の公開

【ポイント】

- NICTER プロジェクトにおける 2018 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 2017 年よりも活発化、依然増加傾向に
- IoT 機器を狙う攻撃の傾向が変化し、仮想通貨の採掘や、Android 機器への攻撃拡大も

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 2018 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 2018 年に観測されたサイバー攻撃関連通信[*2]は、2017 年と比べて約 1.4 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見られるスキャンの増加が著しく、総観測パケット数の 35%を占めました。IoT 機器を狙った通信では、2017 年に 4 割近くを占めていた Telnet（23/TCP）を狙う攻撃が減少する一方、IoT 機器に固有の脆弱性を狙う攻撃が増加し、攻撃対象や攻撃手法が細分化している様子が観測されています。

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[*3]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 2018 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 2018」http://www.nict.go.jp/cyber/report/NICTER_report_2018.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 2018 年に観測されたサイバー攻撃関連通信は、合計 2,121 億パケットに上り、1 IP アドレス当たり約 79 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
2009	約35.7億	約12万	36,190
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**

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、これを日本全体や政府機関への攻撃件数と考えるのは適切ではありません。

図 2 は、1 IP アドレス当たりの年間総観測パケット数を 2009 年からグラフ化したものです。2018 年の総観測パケット数は、2017 年から約 600 億増加しましたが、この増分を分析した結果、海外組織からの調査目的と見られるスキャンが総パケットに占める割合が、2017 年の 6.8%から 2018 年は 35%へと大幅に増加し、753 億パケット（総パケットの 35%）にも及ぶことが判明しました。

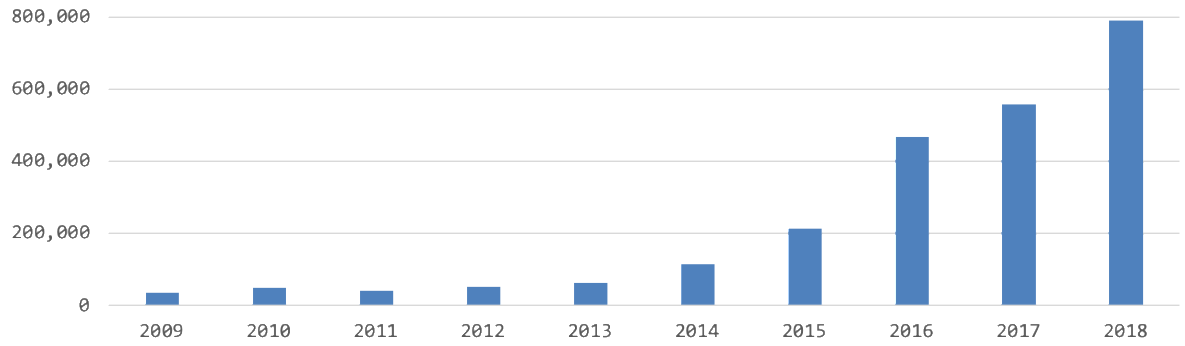
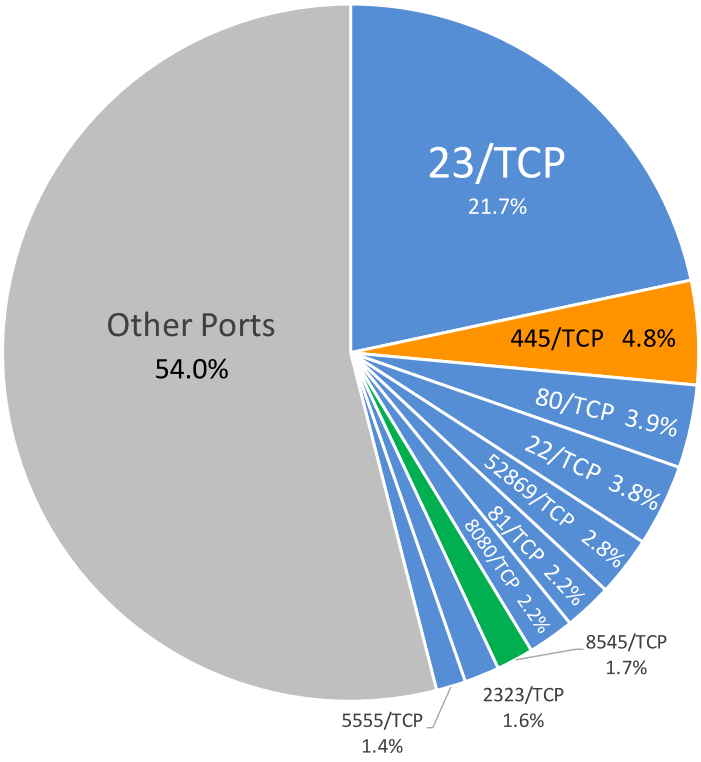


図 2. 1 IP アドレス当たりの年間総観測パケット数（過去 10 年間）

このような調査目的のスキャンパケットを除いた上で、2018 年に NICTER で観測した主な攻撃対象（宛先ポート番号）のトップ 10 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）
80/TCP	Webサーバ （HTTP） IoT機器 （Web管理画面）
22/TCP	IoT機器 （ルータ等） 認証サーバ （SSH）
52869/TCP	IoT機器 （ホームルータ等）
81/TCP	IoT機器 （ホームルータ等）
8080/TCP	IoT機器 （Webカメラ等）
8545/TCP	イーサリアム （仮想通貨）
2323/TCP	IoT機器 （Webカメラ等）
5555/TCP	Android 機器 （セットトップボックス等）

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: 4 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。Other Ports の占める割合は、全体の半数以上と目立ちますが、IoT 機器で使用されるポート（機器の Web 管理インターフェイス用ポートや 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。

2017 年には、これらトップ 10 のポートが全体の半数以上を占めていましたが、2018 年は、46%とおよそ半数に減少しています。減少の理由としては、Telnet（23/TCP）を狙った攻撃パケット数が 548 億パケットから 294 億パケット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（Other Ports）の占める割合は、全体の半数以上と目立ちますが、IoT 機器で使用されるポート（機器の Web 管理インターフェイス用ポートや 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。

2018 年に特徴的な観測事象としては、その他にも、IoT 機器が仮想通貨採掘を強要する悪性プログラムに大規模感染する事象や、Android OS を搭載する様々な IoT 機器を狙った感染活動も観測しています。NICTER で新たに発見した脆弱性やインシデントについては、関連組織への報告や情報共有を行いました。

IoT 機器の脆弱性が公開されると、その脆弱性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一般化しており、IoT 機器の脆弱性対策は、感染の未然防止や被害の拡大防止の観点で、ますます重要になってきていると考えられます。

【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 2018（詳細版）＞

- NICTER 観測レポート 2018（Web 版）
  http://www.nict.go.jp/cyber/report.html
- NICTER 観測レポート 2018（PDF 版）
  http://www.nict.go.jp/cyber/report/NICTER_report_2018.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 にて研究開発され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。

***2 サイバー攻撃関連通信**

ダークネット[*3]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 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。

＜ 本件に関する問い合わせ先 ＞
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 ＞
広報部 報道室
廣田 幸子
Tel: 042-327-6923
Fax: 042-327-7587
E-mail: publicity@nict.go.jp