平成 28 年 12 月 21 日

海外製ルータの脆弱性を標的としたアクセスの急増等について

（平成 28 年 11 月期）

- 海外製ルータの脆弱性を標的としたアクセスの急増
- 宛先ポート 27015/UDP に対するアクセスの増加
- SSDP に使用される宛先ポート 1900/UDP に対するアクセスの急増
- ntpd の脆弱性（CVE-2016-7434）を標的としたアクセスの観測

1 海外製ルータの脆弱性を標的としたアクセスの急増

インターネット定点観測システムでは、11 月 26 日 22 時頃から宛先ポート 7547/TCP に対するアクセスの急増を観測しました（図1）。

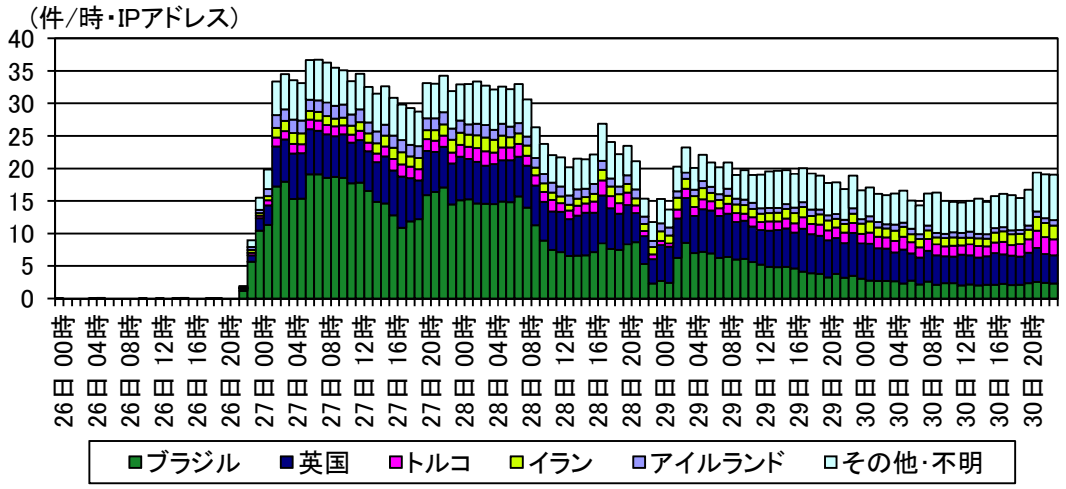

図1 宛先ポート 7547/TCP に対するアクセス件数の発信元国・地域別[i]推移
（H28.11.26～H28.11.30）

7547/TCP は遠隔で通信機器を管理する CWMP[ii]で使用されるポートです。当該ポートに対する脆弱性については、平成 28 年 11 月7日に、海外のセキュリティ研究者が特定のルータにおいてインターネットから実行することができるコマンドインジェクションの脆弱性が存在することを公開しており、同時に当該脆弱性に対する PoC[iii]も公開されています。

[i] 発信元国・地域別については、当該国・地域に割り当てられた IP アドレスを指しています。以降も同様の表記です。
[ii] CPE WAN Management Protocol の略。遠隔でルータ等の通信機器を管理するために使用されるプロトコル。
[iii] Proof of Concept の略。脆弱性を利用した攻撃が可能であることを示すための検証用プログラム。

海外のセキュリティ機関の SANS ISC（Internet Storm Center）から、11 月 29 日に当該脆弱性を悪用した攻撃について公開[i]されています。これによると、ダウンロードされる不正プログラムのコードは「Mirai」ボットに由来するとされています。また、12 月 2 日には、セキュリティ対策企業から、「Mirai」ボットの新たな亜種による 7547/TCP への攻撃を確認したことが公表[ii]されています。

観測したアクセスは、前述の PoC に記述されたコードに類似しており、これらのアクセスには外部のサーバからファイルをダウンロードし実行を試みるコマンドが含まれていました（図2）。

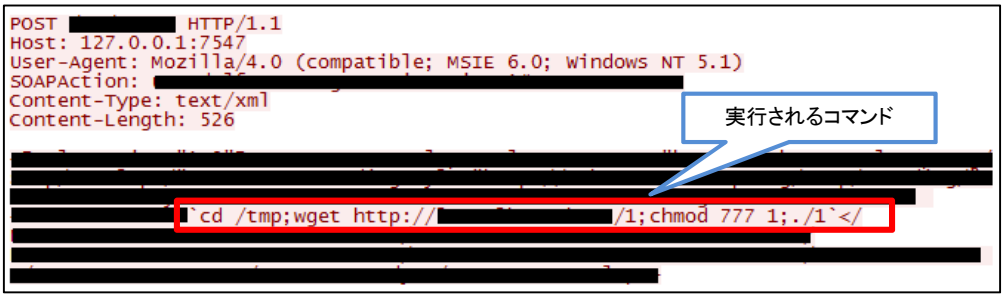

図2　実行されるコマンドの例（一部マスキングを実施）

また、11 月 27 日 18 時頃から宛先ポート 5555/TCP に対するアクセスの急増を観測しました（図3）。アクセスの内容を確認したところ、宛先ポート 7547/TCP に対するアクセスと同様に当該脆弱性を悪用するコマンドが含まれていました。

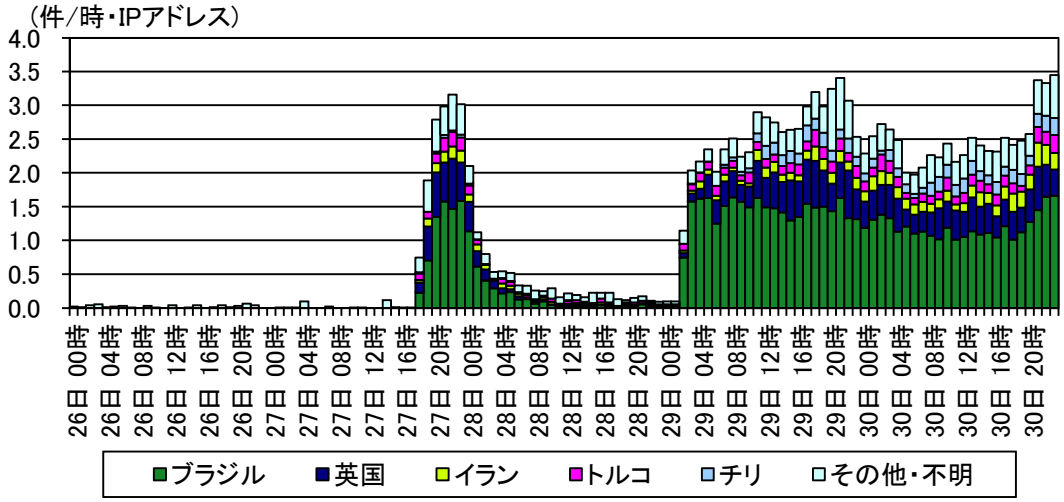

図3　宛先ポート 5555/TCP に対するアクセス件数の発信元国・地域別推移
（H28.11.26～H28.11.30）

[i] 「TR-069 NewNTPServer Exploits: What we know so far」
https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763/

[ii] 「新しい「Mirai」、ルータを狙うポート 7547 への攻撃が示す今後の脅威」（トレンドマイクロ）
http://blog.trendmicro.co.jp/archives/14108

宛先ポート 7547/TCP 及び 5555/TCP に対するアクセスにおいては、多数の IP アドレスからのアクセスを確認しています（図4）。

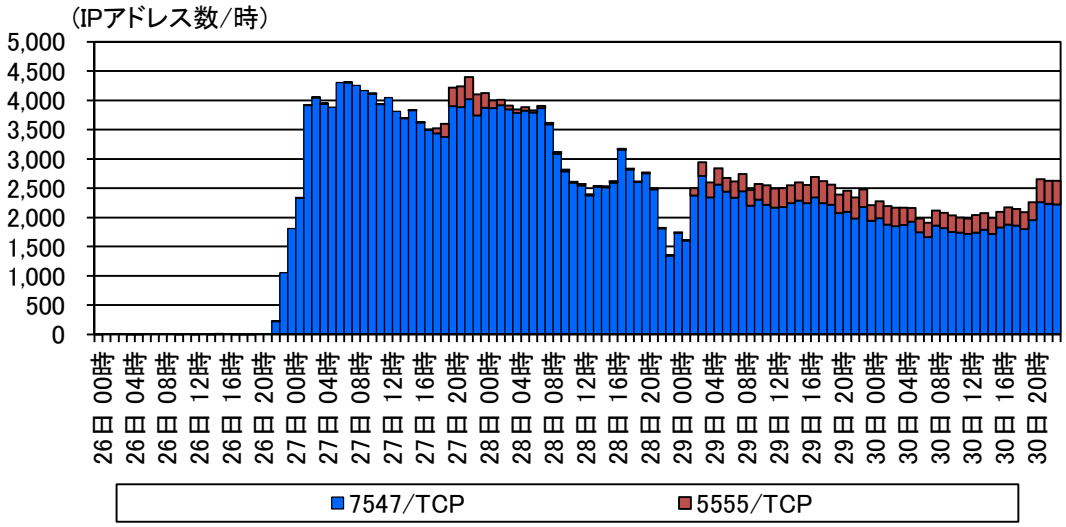

図4　宛先ポート 7547/TCP 及び 5555/TCP に対する発信元 IP アドレス数の推移
（H28.11.26～H28.11.30）

アクセスの発信元を調査したところ、ルータ等へのログイン画面が表示されるものが散見されました（図5）。

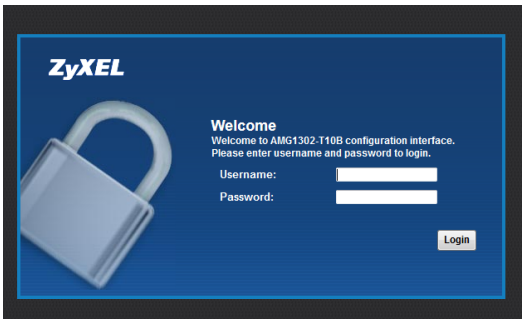

図5　発信元 IP アドレスにおいて確認できたログイン画面の例

これらのことから、ボットに感染した多数の機器が脆弱性の存在する特定のルータを標的として不正プログラムの感染を広げる活動を行っているものと考えられます（図6）。

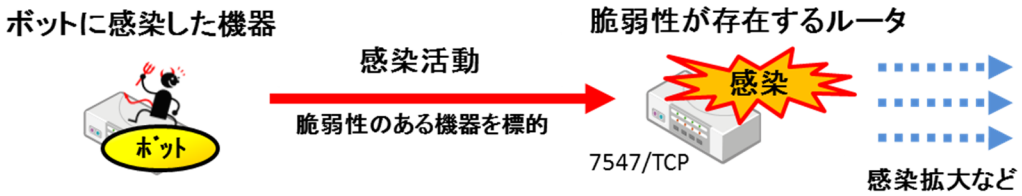

図6　不正プログラム感染活動のイメージ

ルータ等の機器がボットに感染すると、ボットに感染したルータ等は DoS 攻撃の踏み台となったり、感染拡大を狙ってさらなる探索を行ったりする可能性があります。そのため、ルータ等の利用者は、ボットへの感染を防止するため、以下のセキュリティ対策を推奨します。

- 製造元のウェブサイト等で脆弱性情報を確認し、脆弱性がある場合はファームウェアのアップデート等の適切な対策を行う。
- ユーザ名とパスワードを推測されにくいものに変更する。
- ファイアウォール等によって不必要な外部からのアクセスを遮断する、特定の IP アドレスのみにアクセスを許可するなどの適切なアクセス制限を実施する。

2 宛先ポート 27015/UDP に対するアクセスの増加

インターネット定点観測システムでは、11 月上旬にゲームサーバに使用される宛先ポート 27015/UDP に対するアクセスの一時的な増加を観測しました（図7）。

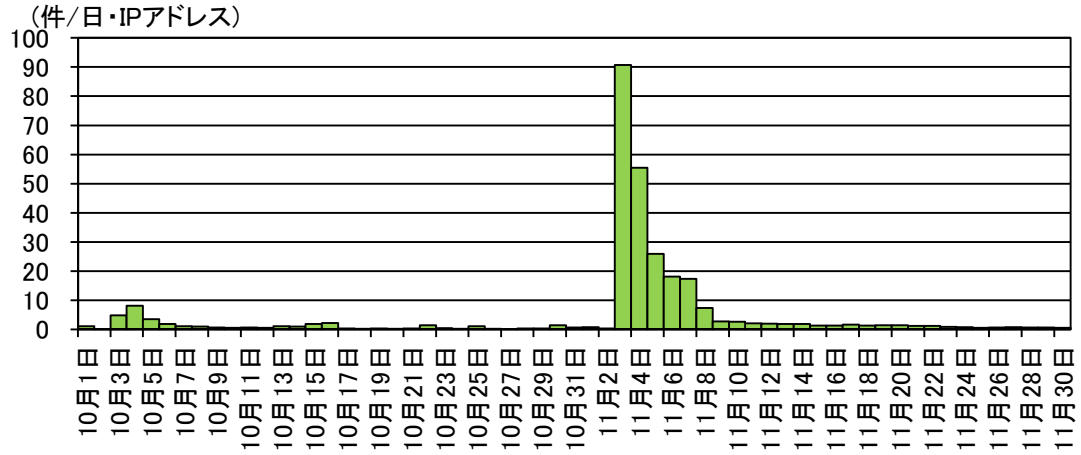

図7 宛先ポート 27015/UDP に対するアクセス件数の推移（H28.10.1～11.30）

観測したアクセスの多くは、「Source Engine Query」のリクエストでした。これは、Valve Corporation 製のゲームエンジン[i]である「Source Engine[ii]」で開発されたゲームが動作するサーバに対してサーバ名やゲームの稼働状況等の問い合わせを行うものです。

宛先ポート 27015/UDP に対するアクセスの発信元 IP アドレスのうち、宛先ポート 23/TCP に対してもアクセスしている IP アドレスが5割以上存在しており、観測したアクセスはボット等に感染した IoT 機器からのアクセスであると考えられます（図8）。

[i] ゲームの動作において共通で用いられるプログラム。
[ii] Valve Corporation によって開発されたゲームエンジン。数多くのオンラインゲーム等に利用されています。

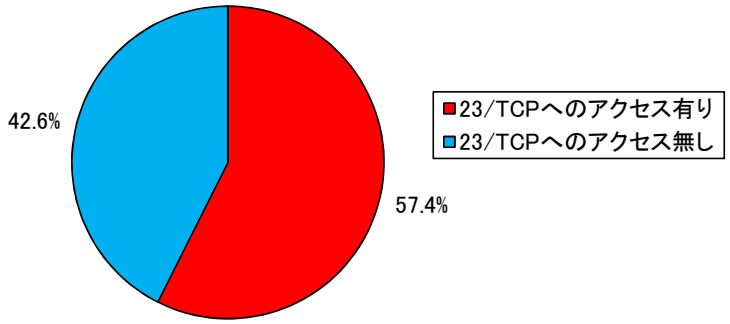

図8　宛先ポート 27015/UDP に対してアクセスのあった発信元 IP アドレスのうち、
宛先ポート 23/TCP に対するアクセス有無の比率（11 月１日～30 日観測分）

警察庁では、平成 28 年9月中旬以降、「Mirai」ボットに感染した IoT 機器が発信元と考えられるアクセスの増加を観測[i]しています。「Mirai」ボットは様々な攻撃を実行することが可能ですが、その中には「Source Engine Query」のリクエストを使用する DoS 攻撃も存在します。

3　SSDP に使用される宛先ポート 1900/UDP に対するアクセスの急増

インターネット定点観測システムでは、平成 28 年8月中旬に SSDP[ii]で使用されるポートである 1900/UDP に対するアクセスの一時的な増加を観測[iii]しましたが、11 月下旬から韓国に割り当てられた IP アドレスからのアクセスの急増を再び観測しました（図9）。

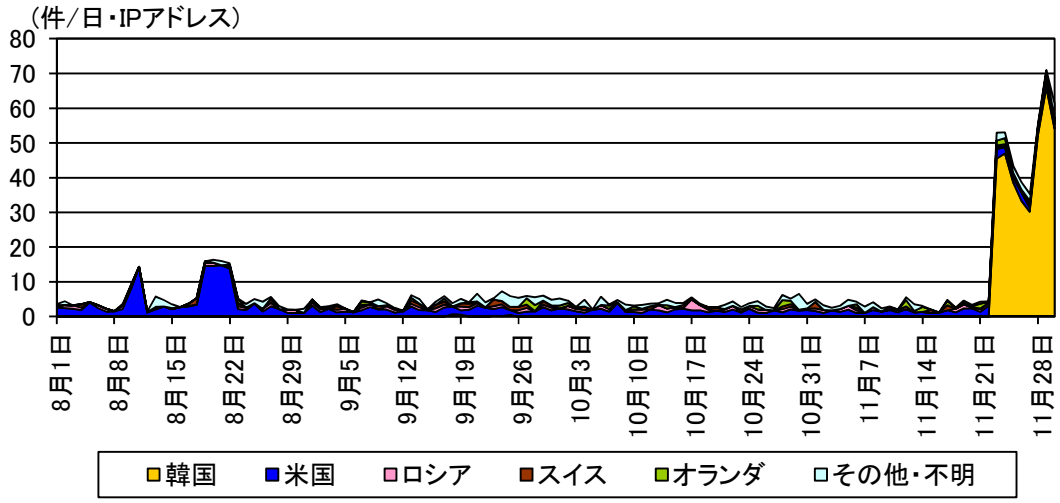

図9　宛先ポート 1900/UDP に対するアクセス件数の発信元国・地域別推移（H28.8.1～11.30）

[i] 「インターネット観測結果等(平成 28 年9月期)」（平成 28 年 10 月 20 日）
https://www.npa.go.jp/cyberpolice/topics/?seq=19361

[ii] SSDP（Simple Service Discovery Protocol）の略。ネットワーク機器同士の接続機能である UPnP（Universal Plug and Play）で使用されるプロトコル。

[iii] 「インターネット観測結果等(平成 28 年8月期)」（平成 28 年9月 30 日）
https://www.npa.go.jp/cyberpolice/topics/?seq=19259

急増した韓国からのアクセスの発信元を調査したところ、特定のメーカー製のネットワーク機器が多数確認されました（図 10）。

図 10　確認したネットワーク機器の例

観測したアクセスは、多数の IP アドレスを発信元としており、それぞれ複数のセンサーに対してアクセスを行っていることから、これらの機器がボット等の不正プログラムに感染し探索活動を行ったり、攻撃の踏み台となったりしている可能性があります。

観測したパケットのほとんどは内容が同一のものであり、機器情報の送信を要求する「M-SEARCH」メッセージでした。

外部からの「M-SEARCH」メッセージに応答するネットワーク機器が攻撃者に発見された場合、SSDP リフレクター攻撃の踏み台として悪用される危険性があります。

管理するネットワーク機器が SSDP リフレクター攻撃の踏み台として悪用されないために、外部からの SSDP プロトコルの通信（宛先ポート 1900/UDP へのパケット）を遮断したり、ネットワーク機器の UPnP 機能を停止したりするなどのセキュリティ対策を推奨します。

4　ntpd の脆弱性（CVE-2016-7434）を標的としたアクセスの観測

インターネット定点観測システムでは、11 月 29 日9時頃から 13 時頃までの間、NTP[i]サーバのソフトウェアである ntpd の脆弱性を標的としたアクセスを観測しました（図 11）。

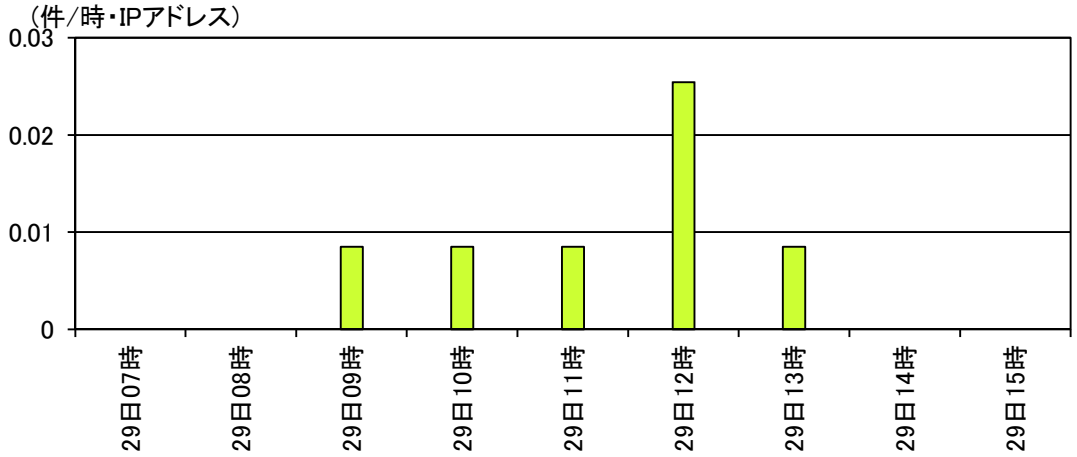

図 11　ntpd の脆弱性（CVE-2016-7434）を標的とするアクセス件数の推移
（11 月 29 日 07 時～15 時）

ntpd については、平成 28 年 11 月 22 日に複数の脆弱性[ii]が公表されており、当該脆弱性（CVE-2016-7434）を悪用する攻撃ツールもインターネット上に公開されています。

11 月 28 日には、国内の企業からも当該脆弱性を検証した結果が公開[iii]されています。このレポートによると、当該脆弱性は、細工された mrulist[iv]クエリを受信すると、ntpd の動作が停止してしまう場合があるとされています。

警察庁において確認した結果、観測したパケットは、当該攻撃ツールを動作させたときに送信されるパケットと同様のものでした。また、当該攻撃ツールを使用して細工したパケットを送信すると、脆弱性の影響を受けるバージョンの ntpd が動作停止することも確認されました。

NTP サーバを運用している管理者は、使用している NTP サーバが当該脆弱性の影響を受けるバージョンではないか確認し、当該脆弱性の影響を受けるバージョンであった場合は、対策済みの最新バージョンにアップデートすることを推奨します。

---

[i] Network Time Protocol の略。ネットワーク経由でコンピュータ等の時刻同期を行うプロトコル。

[ii] 「NTP.org の ntpd に複数の脆弱性」（JVN）
https://jvn.jp/vu/JVNVU99531229

[iii] 「CVE-2016-7434　脆弱性調査レポート」（ソフトバンク・テクノロジー）
https://www.softbanktech.jp/information/2016/20161128-01/

[iv] 最近時刻同期を行ったクライアント IP アドレス等のリスト。