平成 28 年7月 29 日

インターネット観測結果等

（平成 28 年6月期）

- DNS ルートサーバに対する DoS 攻撃の跳ね返りパケット[i]を観測
- Linux 組込機器を発信元とした宛先ポート 23/TCP に対するアクセスが増加
- Netis 社製ルータに対する攻撃を企図したアクセスが増加

1 DNS ルートサーバに対する DoS 攻撃の跳ね返りパケットを観測

DNS ルートサーバは、インターネットで利用される DNS においてツリー構造の起点となるサーバで、A～M の英字で区別される 13 のサーバ[ii]がルートサーバとして DNS に登録されています。

これらの DNS ルートサーバにおける特異なトラフィックの観測結果について、平成 28 年6月下旬に、Root Server Technical Operations Association が報告書を公表[iii]しています。

同報告書では、日本標準時の6月 26 日6時 45 分から同日9時 41 分の間に、すべての DNS ルートサーバにおいて1秒間に最大約 1,000 万パケット（17Gbps）のトラフィックを観測しましたが、一般ユーザのインターネット利用に顕在的な影響は無かったとしています。また、同トラフィックは、広範囲かつ一様に分布した複数の IP アドレスを発信元とした TCP SYN パケット及び ICMP パケットであった点が特徴的であると分析しています。

警察庁の定点観測システムでは、DNS ルートサーバに割り当てられた IP アドレスを発信元とする発信元ポート 53/TCP からの跳ね返りパケットを観測しました（図1及び図2）。同パケットは、複数のセンサーに均一的な頻度で到達しており、前述の報告書のトラフィックと符合した特徴が見られることから、DNS ルートサーバに対して発信元 IP アドレスを詐称した SYN flood 攻撃が実施されたものと考えられます。

---

[i] 跳ね返りパケットは、「back scatter」と呼ばれることもあります。

[ii] DNS 上にルートサーバとして登録されたエントリであり、実際の物理的なサーバの数が 13 台ということではありません。

[iii] Root Server Technical Operations Association（平成 28 年6月 29 日）
http://root-servers.org/news/events-of-20160625.txt

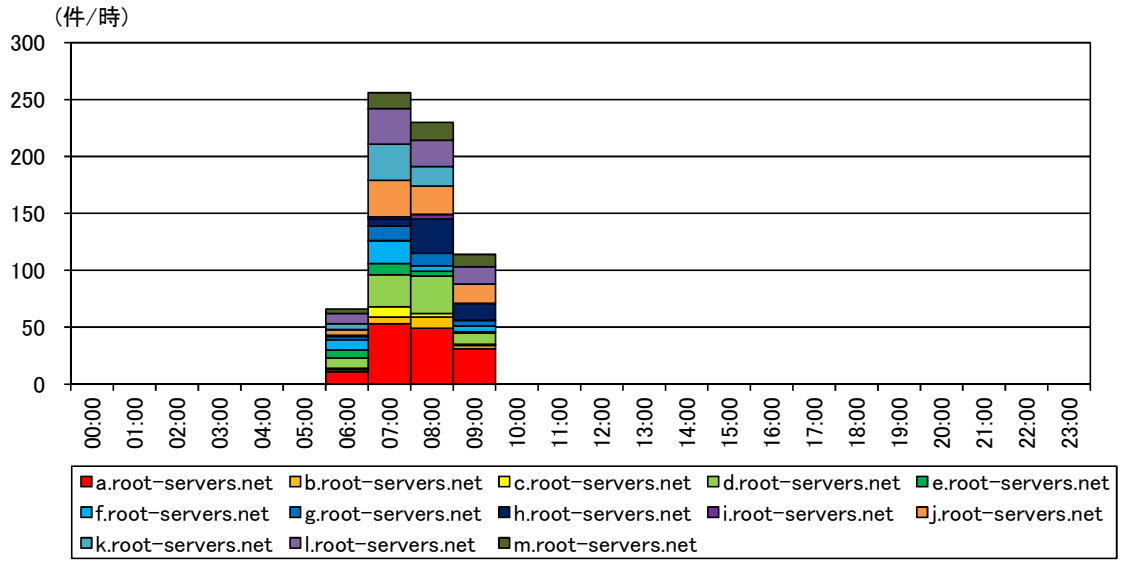

図1　DNS ルートサーバからの跳ね返りパケット件数の推移（発信元 IP アドレス[i]別）
（H28.6.26、1時間当たりのパケット数）

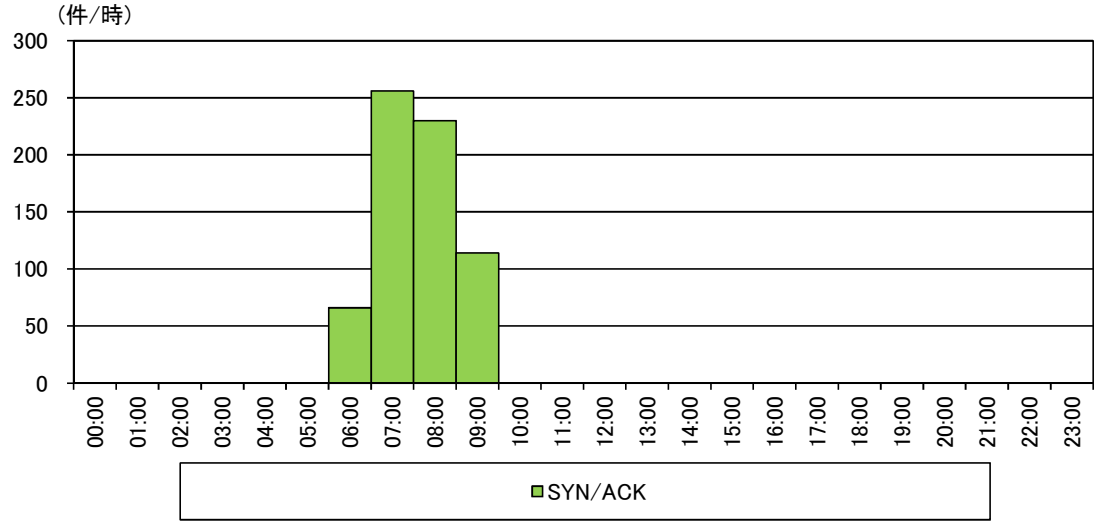

図2　DNS ルートサーバからの跳ね返りパケット件数の推移（TCP フラグ別）
（H28.6.26、1時間当たりのパケット数）

[i] 発信元 IP アドレスについては、DNS ルートサーバに割り当てられた IP アドレスを指しています。

今回は DNS ルートサーバに対する攻撃でしたが、日本国内の企業や組織等に対する同種の攻撃が多発する可能性も十分に考えられます。そのため、企業や組織等の管理者は攻撃の発生に備えて、以下の点に日頃から注意しておくことを推奨します。

- 日頃から管理するサーバの稼働状況を把握し、攻撃発生を迅速に把握できる体制を構築しておくことを推奨します。
- 他の事業者が提供し、複数の顧客が共用するサービスを利用している場合、自身が管理するドメインが攻撃対象とはならなくても、同一サービスを利用する他のドメインが攻撃被害を受けた場合には、その影響を受ける可能性があることに留意しておく必要があります。
- 攻撃により正常な運用が妨害された場合の代替措置の必要性や具体的な手順について、平常時から検討を実施しておくことを推奨します。

2　Linux 組込機器を発信元とした宛先ポート 23/TCP に対するアクセスが増加

平成 28 年6月期（以下「今期」という。）は、23/TCP を宛先ポートとするアクセスの増加を観測しました（図4）。

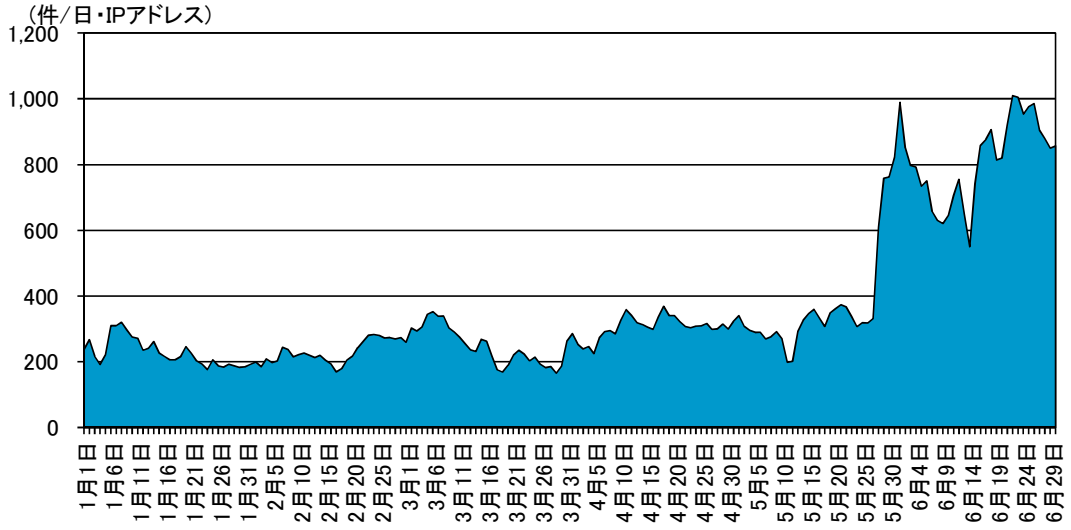

図4　宛先ポート 23/TCP に対するアクセス件数の推移（H28.1.1～6.30）

23/TCP は、Telnet で使用されるポートであり、これらのアクセスは、Telnet でログイン可能なコンピュータやネットワーク機器の探索を目的としているものと考えられます。また、これらのアクセスを確認したところ、センサー到達時の TTL 値が 64 未満のものが 98.7%を占めていました（図5）。

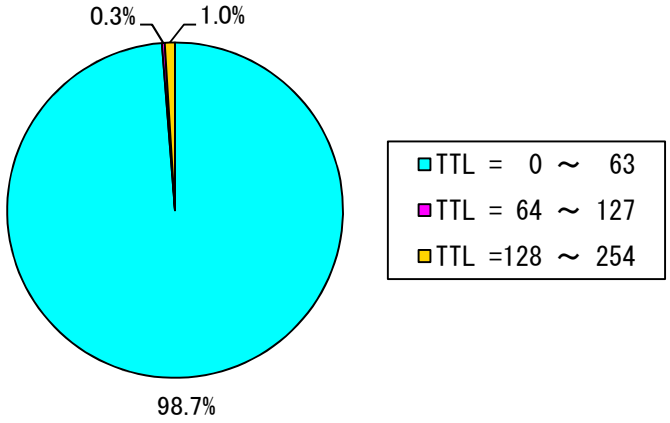

図5　宛先ポート 23/TCP に対するアクセスにおける TTL 値の内訳

TTL 値は OS により初期値が異なり、Linux 系 OS や MacOS の場合は 64、Windows の場合は 128、Solaris や Unix の場合は 255 となっていることから、当該アクセスの発信元は Linux 系の OS が組み込まれた機器である可能性が高いと考えられます。

Linux は組み込み OS の分野において過半数のシェアを占め、スマートフォン、ネットワーク機器、

デジタル家庭電化製品といったIoT(Internet of Things : モノのインターネット)機器のOSとして広く普及[i]しています。

当該アクセスの発信元を調査したところ、デジタルビデオレコーダー、ウェブカメラ、ルータ等の特徴が見られるものが多いことから、IoT機器が攻撃者に乗っ取られ、攻撃者の命令に基づいて動作するボットとして動作しており、ボットの感染拡大を目的としてTelnet探索を行っている可能性があります。また、過去には、これらIoT機器がビットコインのマイニングに悪用された事例も報告[ii]されています(図6)。

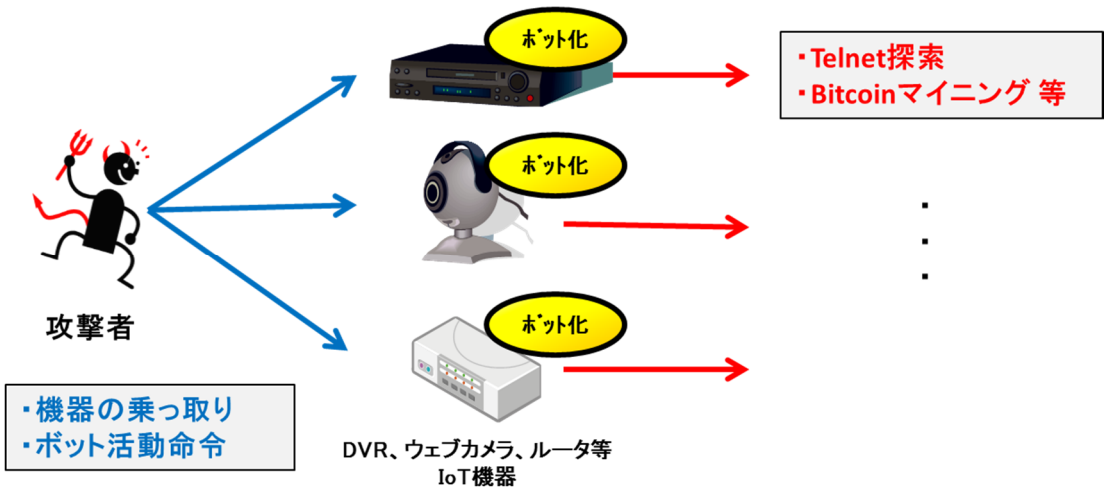

図6 IoT機器のボット化

[i] 「Embedded Linux Keeps Growing Amid IoT Disruption, Says Study」(平成27年3月20日)
http://www.linux.com/news/embedded-mobile/mobile-linux/818011-embedded-linux-keeps-growing-amid-iot-disruption-says-study

[ii] 「More Device Malware: This is why your DVR attacked my Synology Disk Station (and now with Bitcoin Miner!)(SANS)」(平成26年3月31日)
https://isc.sans.edu/forums/diary/More+Device+Malware+This+is+why+your+DVR+attacked+my+Synology+Disk+Station+and+now+with+Bitcoin+Miner/17879

3 Netis 社製ルータに対する攻撃を企図したアクセスが増加

今期は、53413/UDP を宛先ポートとするアクセスの増加を観測しました（図7）。

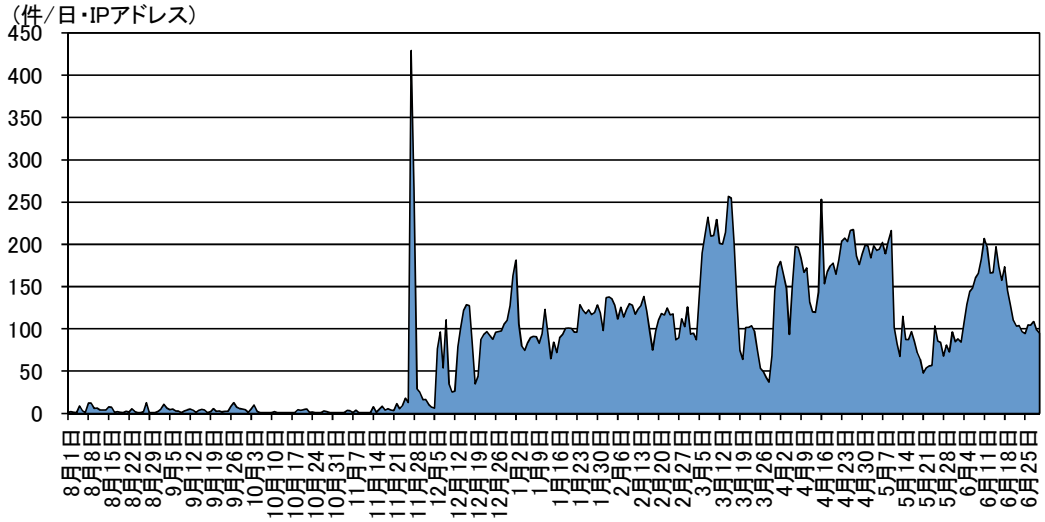

図7　宛先ポート 53413/UDP に対するアクセス件数の推移（H27.8.1～H28.6.30）

53413/UDP は Netis[i]社製のルータで使用されるポートで、平成 26 年8月には外部から容易にアクセスできる脆弱性をセキュリティ対策企業が公表[ii]しました。定点観測システムでも、同年8月 27 日にアクセスの急増を確認[iii]して以降、継続的に同アクセスを観測しており、平成 27 年8月のアクセス増加[iv]、11 月下旬の顕著な増加後からの継続的なアクセスを観測[v]しています。また、アクセスの中には当該ルータに対して不正プログラムのダウンロード及び実行を試みていると思われるものも確認しており、平成 27 年 12 月 15 日に注意喚起を実施[vi]しています。

今期は、Netis 社製ルータの探索行為が更に活発化した可能性があります。平成 28 年6月4日から当該ルータに対するログインの試行と思われるアクセスが増加し、さらに6月 26 日からは不正プログラムのダウンロード及び実行を試みていると思われるアクセスが増加（図8）しており、平成 28 年5月期と比較して目的が明確なアクセスの割合が増加（図9）しています。

---

[i] 2000 年に設立されたネットワーク機器メーカで、中国深圳市に本社を置く Netcore 社のグループ企業のひとつ。
http://www.netis-systems.com/

[ii] 「UDP ポートを開放した状態にする Netis 製ルータに存在する不具合を確認」（平成 26 年8月 27 日）
http://blog.trendmicro.co.jp/archives/9725

[iii] 「インターネット観測結果等（平成 26 年8月期）」（平成 26 年 10 月7日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141007_2.pdf

[iv] 「インターネット観測結果等（平成 27年8月期）」（平成 27 年9月 25 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=16942

[v] 「インターネット観測結果等（平成 27年 12 月期）」（平成 28 年1月 25 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=17624

[vi] 「IoT 機器を標的とした攻撃について」（平成 27 年 12 月 15 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=17323

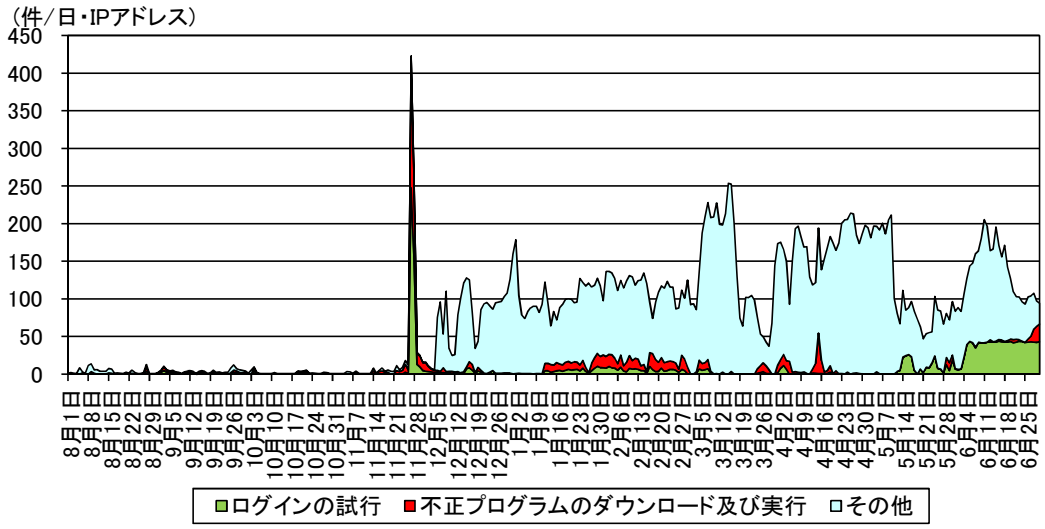

図8　宛先ポート 53413/UDP に対するアクセス件数の推移（目的別）
（H27.8.1～H28.6.30）

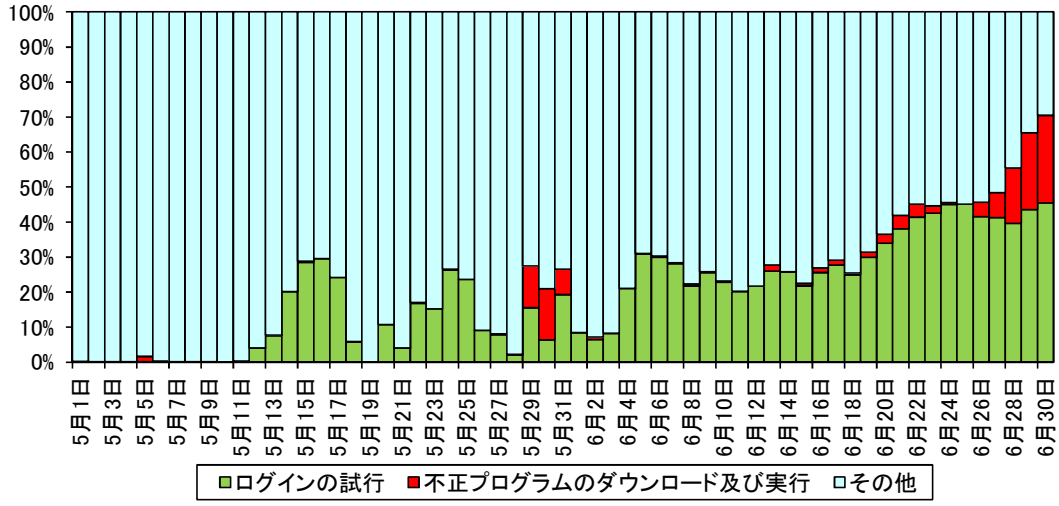

図9　宛先ポート 53413/UDP に対するアクセス件数の推移（目的別内訳）
（H27.5.1～H28.6.30）

これらのアクセスの発信元について調査したところ、宛先ポート 23/TCP に対するアクセスの発信元と同様の特徴があったことから、IoT 機器がボットの感染拡大に利用されているものと考えられます。当該ルータの脆弱性を放置したままの状態であれば、これらの発信元機器と同様に攻撃に悪用される可能性があります。このため、ルータについても、適切なセキュリティ対策を実施することが必要となります。

ルータのセキュリティ対策としては、以下のようなものがあります。

- 管理用のパスワードは、推測されにくいものに変更する。
- メーカ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対策を行う。
- 管理用のインターフェースに対するアクセス制限を適切に設定し、外部ネットワークからの不要なアクセスを遮断する。