平成 27 年 11 月 11 日

インターネット観測結果等

（平成 27 年 10 月期）

- PPTP サーバへの不正侵入が目的と考えられる 1723/TCP に対するアクセスが増加
- Portmap や RIPv1 を悪用するリフレクター攻撃の踏み台を探索するアクセスが高水準で推移
- 22/TCP 以外の宛先ポートに対する SSH サービスの探索が高水準で推移

1 PPTP サーバへの不正侵入が目的と考えられる 1723/TCP に対するアクセスが増加

今期は、宛先ポート 1723/TCP に対するアクセスの増加を観測しました（図1）。

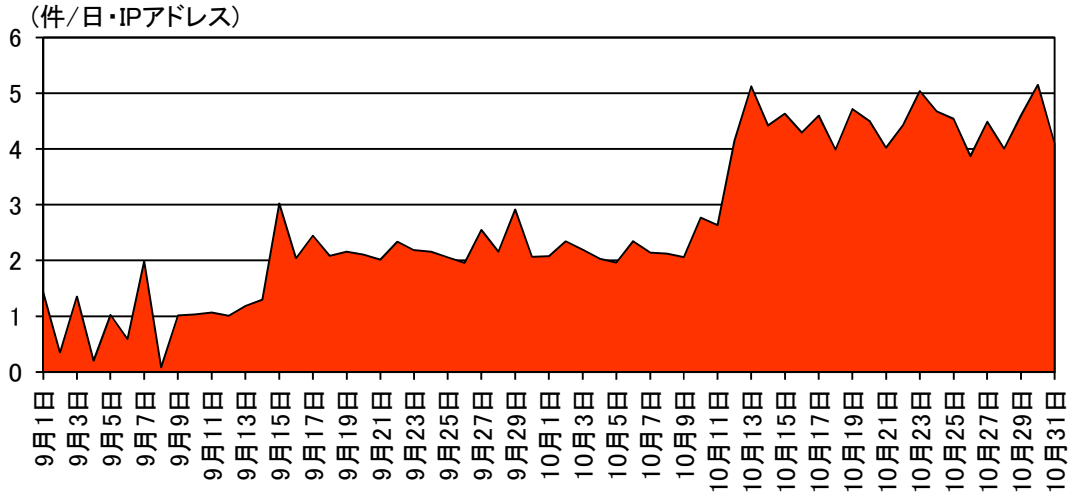

図1 宛先ポート 1723/TCP に対するアクセス件数の推移（H27.9.1～H27.10.31）

1723/TCP は PPTP（Point to Point Tunneling Protocol）で使用されるポートであり、PPTP サーバと PPTP クライアントとの間で VPN 接続を行う際に使用されます。

観測したアクセスの内容を確認したところ、その多くは PPTP サーバへの接続要求であったことから、攻撃者がインターネットに接続された PPTP サーバを探索し、セキュリティが脆弱なサーバに対して不正侵入を試みる目的があるものと考えられます。

VPN 内に不正侵入された場合、機密情報の窃取や新たな攻撃の踏み台として悪用されるおそれがあります。また、主に家庭や小規模な組織等で使用されるブロードバンドルータにおいても、PPTP サーバの機能が実装された製品が多数存在することから、PPTP は他の VPN プロトコルと比較すると、その利用範囲が比較的大きいものと考えられます。このため、ルータ等で PPTP サーバを運用する場合は、以下の対策を実施することを推奨します。

- PPTP での VPN 接続を許可する IP アドレスを限定できる場合には、発信元 IP アドレスによるアクセス制限を実施する。
- 接続に必要な ID・パスワードを推測されにくく、十分な強度があるものにする。また、他のサービスとの使い回しを避ける。
- PPTP 接続のログを定期的にチェックし、不正な接続が発生していないか点検を実施する。

2 Portmap や RIPv1 を悪用するリフレクター攻撃の踏み台を探索するアクセスが高水準で推移

警察庁では、UDP を利用する各種プロトコルを悪用するリフレクター攻撃について注意喚起を実施[i]してきました。しかしながら、今までに注意喚起を実施してきたプロトコル以外においても、リフレクター攻撃への悪用が確認された事例が複数報告されています。特に平成 27 年に入ってからセキュリティ対策企業等から攻撃事例の報告が行われている Portmap 及び RIPv1 については、警察庁の定点観測システムにおいてもリフレクター攻撃の踏み台の探索と考えられるアクセスの顕著な増加があり、今期まで高い水準で観測件数が推移しています（図2）。また、これらのプロトコルの概要と、主な攻撃事例の報告は表1のとおりです。

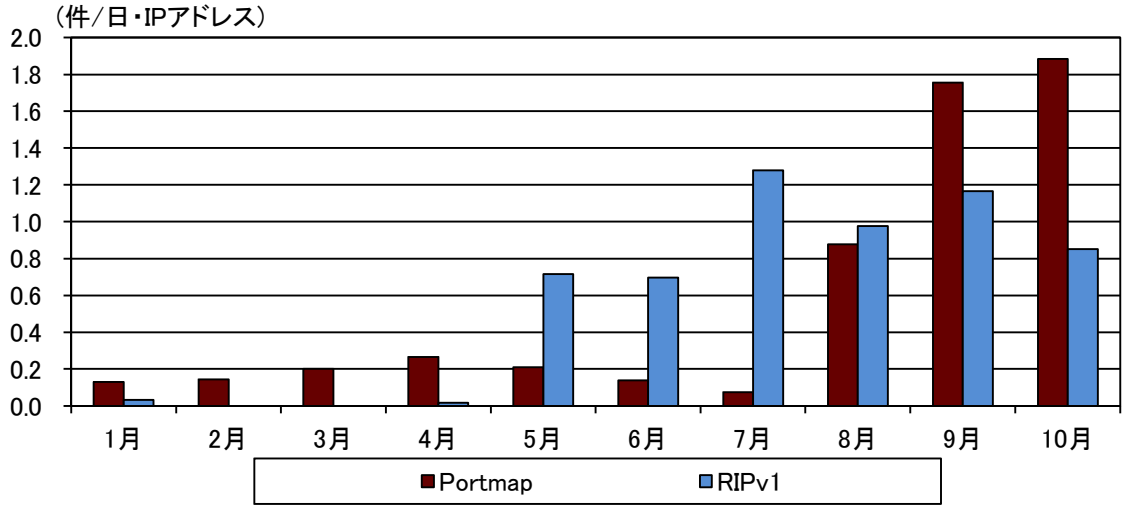

図2 リフレクター攻撃の踏み台の探索と考えられるアクセスの推移
（H27.1.1～10.31、月毎の1日当たりの平均値）

[i] 「DNS リフレクション攻撃に対する注意喚起について」（平成 25 年4月 11 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130411.pdf
「NTP サーバを踏み台としたリフレクター攻撃（NTP リフレクター攻撃）に対する注意喚起について」（平成 26 年1月 17 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140117.pdf
「情報技術解析平成 25 年報」（平成 26 年2月 27 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/H25_nenpo.pdf
「UDP を利用するプロトコルを悪用する各種リフレクター攻撃に対する注意喚起について」（平成 26 年7月 11 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140711.pdf
「UPnP に対応したネットワーク機器を踏み台とした SSDP リフレクター攻撃に対する注意喚起について」（平成 26 年 10 月 17 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141017.pdf
「SNMP リフレクター攻撃に対する注意喚起について」（平成 26 年 11 月 26 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141126.pdf
「情報技術解析平成 26 年報」（平成 27 年3月 12 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=15688
「UDP を利用するプロトコルを悪用するリフレクター攻撃の観測状況について」（平成 27 年 10 月 23 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=17080

表1　定点観測システムでアクセスが増加したリフレクター攻撃に悪用されるプロトコル

プロトコル ポート	プロトコルの概要	主な攻撃事例の報告
Portmap 111/UDP	Linux(UNIX)において、プログラムと使用するポートの管理を行う RPC portmap（portmapper、rpcbind 等とも呼ばれる。）で使用される。	8/17　A社[i]
RIPv1 520/UDP	RIPv1(Routing Information Protocol Version 1)は、小規模なネットワーク内で使用されるルーティングプロトコルである。	7/1　B社[ii]

これらのプロトコルの警察庁における今期までの観測件数は、これまでに注意喚起を実施してきた他のプロトコルと比較すると少ない状況です。また、インターネット上で攻撃の踏み台として悪用できる機器の台数も多くはないと考えられます。しかしながら、万が一にも管理する機器がリフレクター攻撃の踏み台として悪用されることがないように、一部再掲となりますが、以下の対策を実施することを推奨します。

- 使用していない不要なサービスは停止する。
- 外部に公開する必要がないサービスは、インターネットからの通信を遮断する。
- 不特定多数に公開する必要がないサービスについては、適切なアクセス制限や認証を実施する。
- RIPv1 を使用しているルータについては、RIPv2 に切り替えた上で認証を実施する。

[i] http://blog.level3.com/security/a-new-ddos-reflection-attack-portmapper-an-early-warning-to-the-industry/

[ii] http://www.akamai.co.jp/enja/html/about/press/releases/2015/press_jp.html?pr=070215
http://www.stateoftheinternet.com/ripv1-reflection-ddos

3 22/TCP 以外の宛先ポートに対する SSH サービスの探索が高水準で推移

サーバやネットワーク機器のコマンドラインによる遠隔制御等に利用される SSH（Secure SHell）では、通常は 22/TCP ポートが使用されます。しかしながら、SSH サービスを意図的に 22/TCP 以外のポートで運用することにより、攻撃を回避しようとする運用が実施される例があります。

定点観測システムでは、かねてから 22/TCP 以外の宛先ポートに対する SSH サービスの探索を継続して観測しています。今期には、22/TCP 以外の宛先ポートに対する探索を実施した発信元 IP アドレス数の一時的な増加が見られました（図3）。

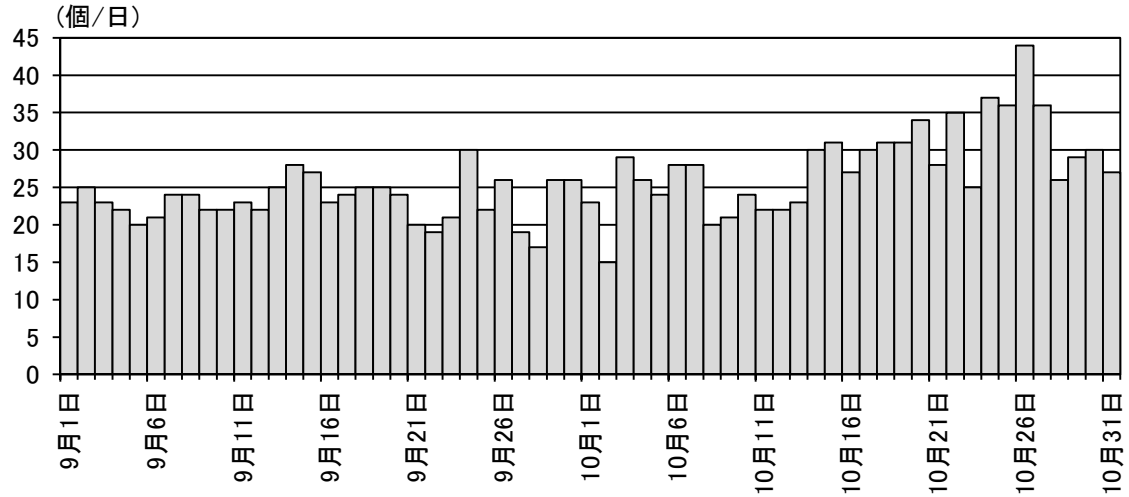

図3 22/TCP 以外の宛先ポートに対する SSH サービス探索の発信元 IP アドレス数の推移
（H27.9.1～10.31）

今期に観測した SSH サービスの探索を宛先ポート別に集計すると、23.0%が 22/TCP 以外のポートに対する探索でした。また 22/TCP 以外の宛先ポートでは、2222/TCP、8022/TCP 及び 222/TCP といった宛先ポートに対する探索が多数を占めました（図4）。今期には 22/TCP を含め計 196 種の宛先ポートで、SSH サービスの探索を観測しています。

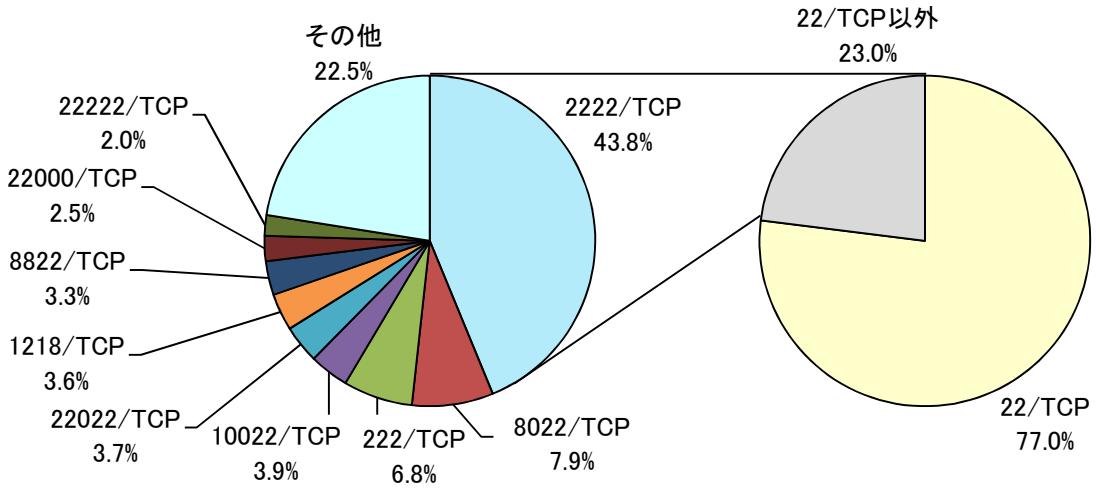

図4　SSH サービス探索の宛先ポート別割合

十分なセキュリティ対策を実施した上で、追加の対策としてポートを変更することは、22/TCP のみを対象とした攻撃を回避する効果があると考えられます。しかしながら、22/TCP 以外のポートで SSH サービスを運用していても、攻撃者がポートスキャンにより SSH サービスの稼動ポートを発見することは難しくありません。このため、ポート変更による攻撃回避の効果を過信して、基本的な対策がおろそかになることがないように留意する必要があります。SSH サービスにおけるセキュリティ対策[i]の代表的なものを以下に例示します。

- SSH サービスへのアクセスを許可する IP アドレスが限定できる場合には、当該 IP アドレスからの接続のみを許可する。
- パスワード認証を使用する場合には、アカウント名とパスワードには、容易に推測できない十分な強度を持ったものを使用する。また、アカウント名とパスワードは他のサービスとの使い回しは行わない。
- 公開鍵認証等のパスワード認証以外の認証方式が使用できる場合には、これを利用する。また、パスワード認証は無効とする。
- ログイン試行が可能な回数に制限を設ける。
- 一定回数のログイン失敗があった IP アドレスについては、アクセスを制限する。

[i] SSH サービスのセキュリティ対策については以下の資料が参考となります。
「SSH サーバセキュリティ設定ガイド Ver 1.0」（日本コンピュータセキュリティインシデント対応チーム協議会）
http://www.nca.gr.jp/imgs/nca_ssh_server_config_v01.pdf