平成 27 年 3 月 4 日

インターネット観測結果等

(平成 27 年1月期)

- 宛先ポート 8118/TCP に対するアクセスが増加
- Bash の脆弱性を悪用したアクセスが急激に増加
- 宛先ポート 23/TCP に対するアクセスが前期から高水準で推移

1 宛先ポート 8118/TCP に対するアクセスが増加

宛先ポート 8118/TCP に対するアクセスが平成 26 年 11 月中旬頃から観測され始め、12 月上旬頃から平成 27 年 1 月中旬頃までアクセスが増加しています（図1）。

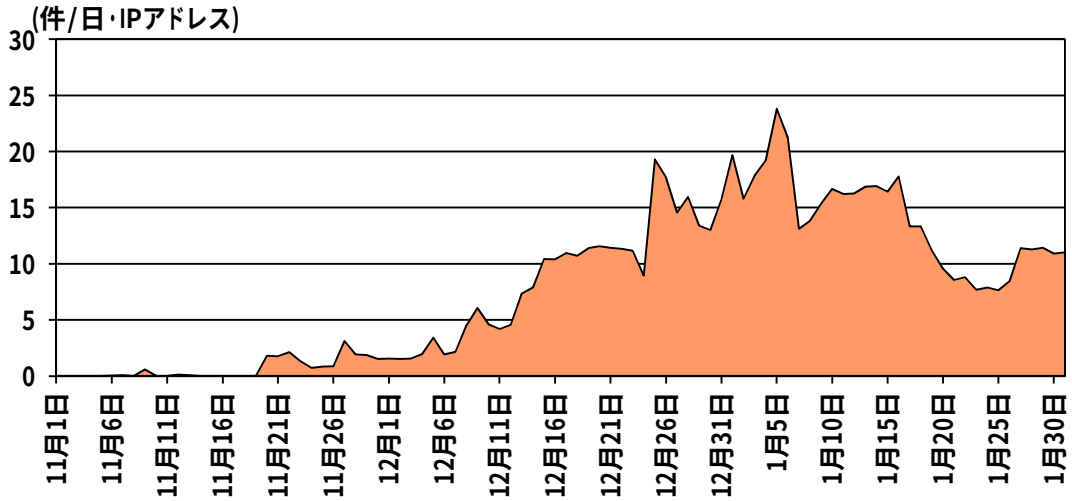

図1 宛先ポート 8118/TCP に対するアクセス件数の推移

8118/TCP は、「Privoxy」[i]が初期設定で使用するポートです。このポートに対するアクセスの内容を確認したところ、HTTP リクエストで特定の URL にアクセスを試みているものが多くを占めており、外部からの問合せに応答するプロキシサーバを探索しているものと考えられます。

[i] Privoxy はプライバシーを強化するための高度なフィルタリング機能を持つ非キャッシングプロキシ。
http://www.privoxy.org/

2　Bash の脆弱性を悪用したアクセスが急激に増加

宛先ポート 10000/TCP に対するアクセスを平成 26 年 12 月中旬頃から観測しはじめ、平成 27 年1月上旬頃から急激に増加しています（図2）。

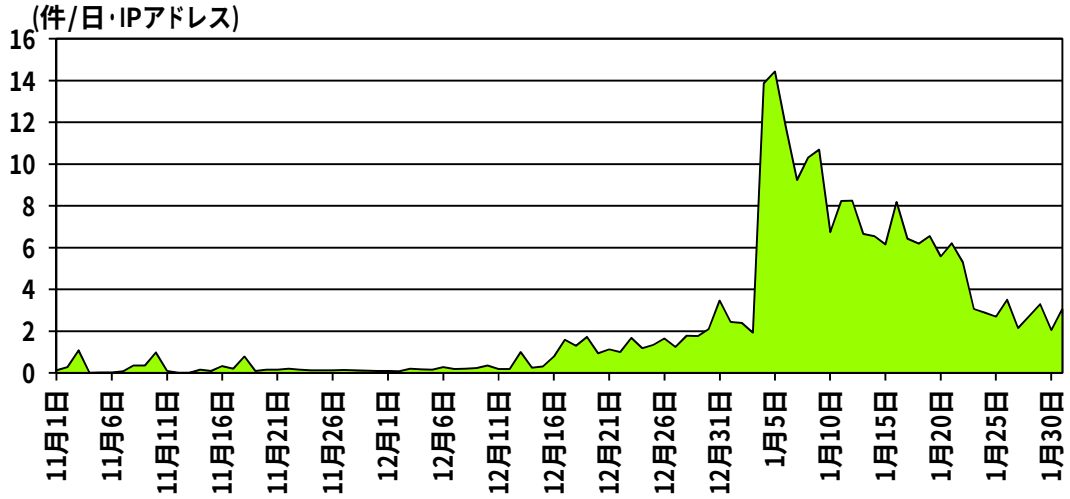

図2　宛先ポート 10000/TCP に対するアクセス件数の推移

10000/TCP は、サーバ管理ソフトウェア Webmin が初期設定で使用するポートですが、このポートに対するアクセスの内容を確認したところ、Bash の脆弱性がある国外の特定のメーカが製造する NAS 製品（以下「NAS 製品」という。）を標的としたと考えられるアクセスが多くを占めていました。

このアクセスの発信元 IP アドレスについて 8080/TCP ポートに接続して確認すると、当該 NAS 製品の管理画面が表示されるものが散見されたことから、当該 NAS 製品が踏み台となり Bash の脆弱性を標的とした攻撃を更に別の当該 NAS 製品に対して行っていると考えられます。

また、前期[i]に増加した 8080/TCP に対するアクセスも継続して高い水準で観測しています（図3）。

[i] 「インターネット観測結果等（平成 26 年 12 月期）」（平成 27 年1月 13 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20150113.pdf

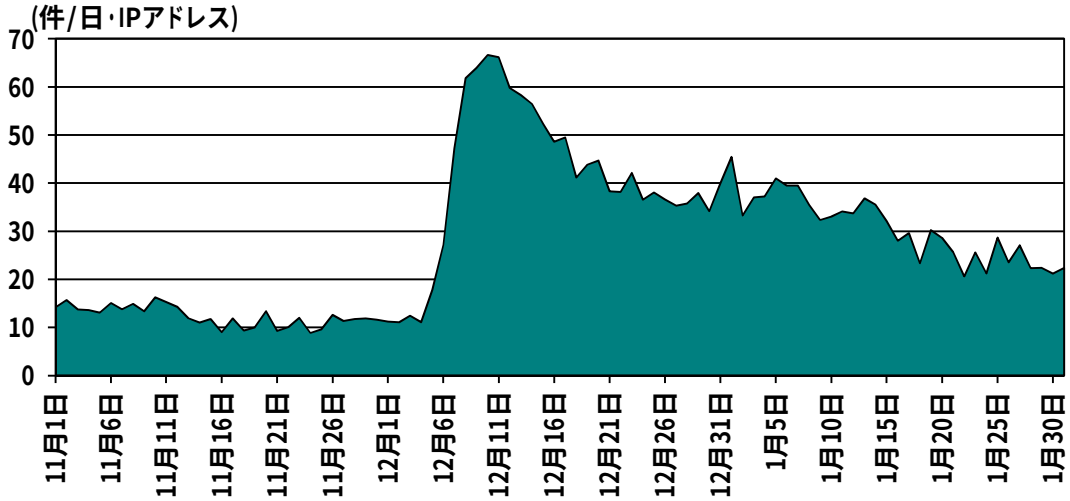

図3　宛先ポート 8080/TCP に対するアクセス件数の推移

3　宛先ポート 23/TCP に対するアクセスが前期から高水準で推移

前期に引き続き、Telnet において使用される宛先ポート 23/TCP に対するアクセスが、高水準で推移しました（図4）。

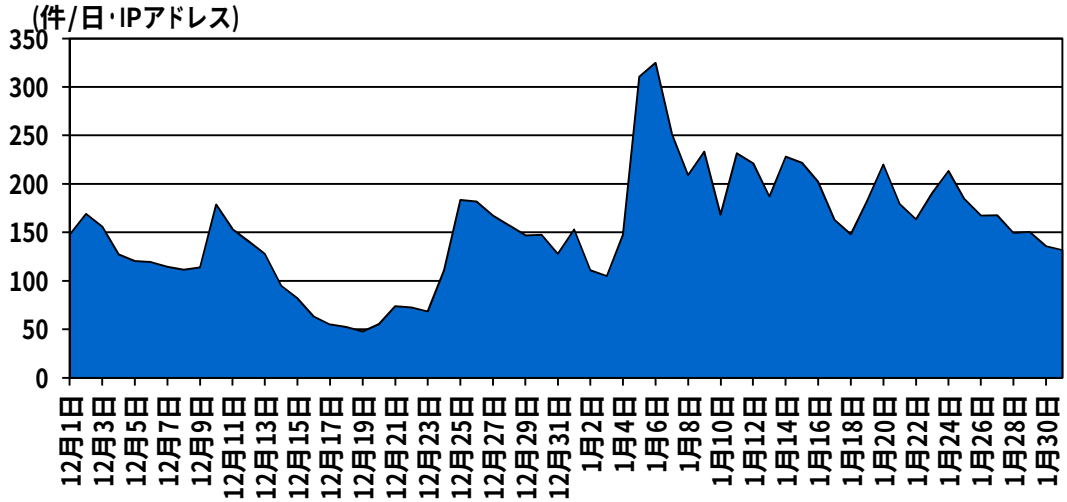

図4　宛先ポート 23/TCP に対するアクセス件数の推移

これらのアクセスの発信元の中には、NAS 製品の管理画面が表示されるものが存在しました。同 NAS 製品を踏み台として、リモートでログインできる機器を探索している行為が継続しているものと考えられます。