平成 26 年 3 月 28 日

インターネット観測結果等
(平成 26 年 2 月期)

- **中国[1]を発信元とする宛先ポート 23/TCP に対するアクセスが増加**
- **53/UDP を発信元ポートとするパケットが増加**
- **宛先ポート 5000/TCP に対するアクセスが増加**

1 中国を発信元とする宛先ポート 23/TCP に対するアクセスが増加

中国を発信元とする宛先ポート 23/TCP に対するアクセスが増加しました（図1）。

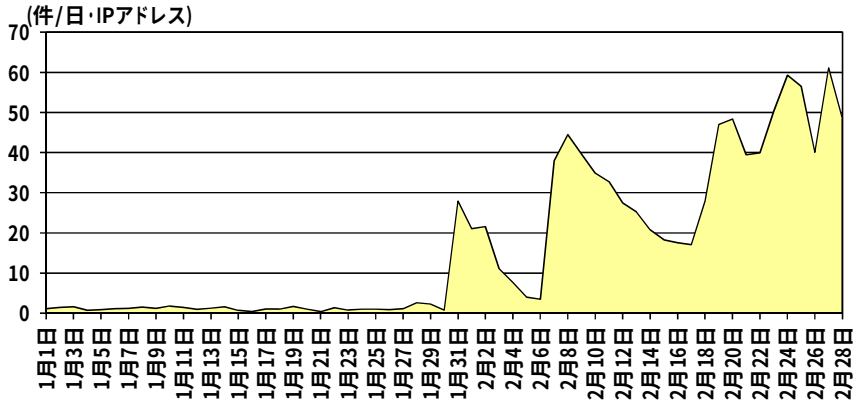

図1 中国を発信元とする宛先ポート 23/TCP に対するアクセス件数の推移（H26.1.1～H26.2.28）

23/TCP は、Telnet に使用されるポートであり、遠隔でネットワーク機器等に接続する際に使用されるものです。同アクセスの発信元 IP アドレスに対する調査を行ったところ、web カメラ等のログイン画面が確認できました。このことから、同アクセスはネットワーク機器を踏み台としたスキャン行為であると考えられます。

2 53/UDP を発信元ポートとするパケットが増加

53/UDP を発信元ポートとするパケットを多数観測しました（図2）。

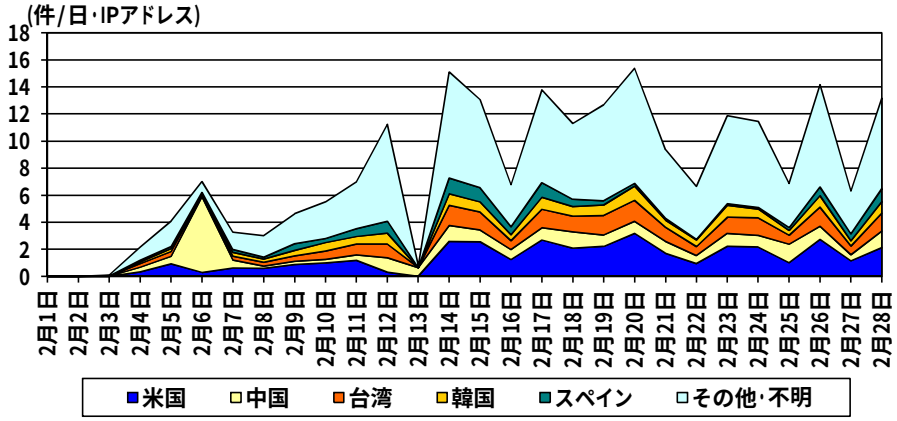

図2 53/UDP を発信元ポートとする発信元国･地域別アクセス件数の推移

[1] 発信元国･地域については、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。以降同様の表記。

同パケットの内容を確認すると、多くのものは DNS 問い合わせに対する応答パケットでした。何者かが発信元 IP アドレスを偽装した上で、当該 DNS サーバを踏み台とした DNS リフレクター攻撃の実行可否の調査を実施した可能性が考えられます。また、発信元となっている IP アドレスの多くが、外部からの問い合わせが可能なオープン・リゾルバであることが判明しています。

このことについては、平成 26 年2月に注意喚起[1]を実施しており、その後も継続して多数のパケットを観測している状態です。

3 宛先ポート 5000/TCP に対するアクセスが増加

宛先ポート5000/TCP に対するアクセスは、これまでほとんど観測されませんでしたが、2月 11 日以降観測され始めました。同アクセスは2月 27 日から更に増加傾向にあります（図3）。

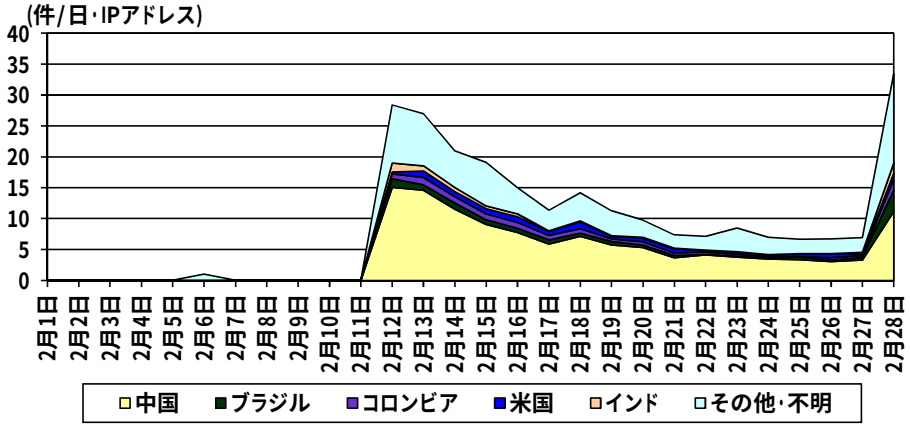

図3　宛先ポート 5000/TCP に対するアクセス件数の推移

同アクセスを分析した結果、5000/TCP は、Synology 社製の NAS のウェブ管理画面に使用されているポートであります。また、同製品にアクセスして、バージョン判定を実施したうえで、その結果に基づき脆弱性を持つ製品を狙った攻撃を実行する攻撃コードが公開されていることも確認しています。このことから、これらのアクセスは脆弱性を持つ同製品を狙った攻撃活動であると考えられます。

平成 26 年3月に注意喚起[2]を実施したので、対策等については、そちらを参考にして下さい。

[1] 発信元 IP アドレスを偽装したオープン・リゾルバの探索行為の増加について
http://www.npa.go.jp/cyberpolice/detect/pdf/20140217.pdf

[2] 脆弱性が存在する NAS の探索と考えられる宛先ポート 5000/TCP に対するアクセスの急増について
http://www.npa.go.jp/cyberpolice/detect/pdf/20140305.pdf