平成 27 年 1月 13 日

インターネット観測結果等

(平成 26 年 12 月期)

- **宛先ポート 8080/TCP に対するアクセスが増加**
- **宛先ポート 23/TCP に対するアクセスが高水準で推移**
- **脆弱性が公表されたルータを対象とするアクセスを観測**
- **脆弱性が公表された CMS[i]を対象とするアクセスを観測**

1 宛先ポート 8080/TCP に対するアクセスが増加

今期は、宛先ポート 8080/TCP に対するアクセスが大きく増加しました（図1）。

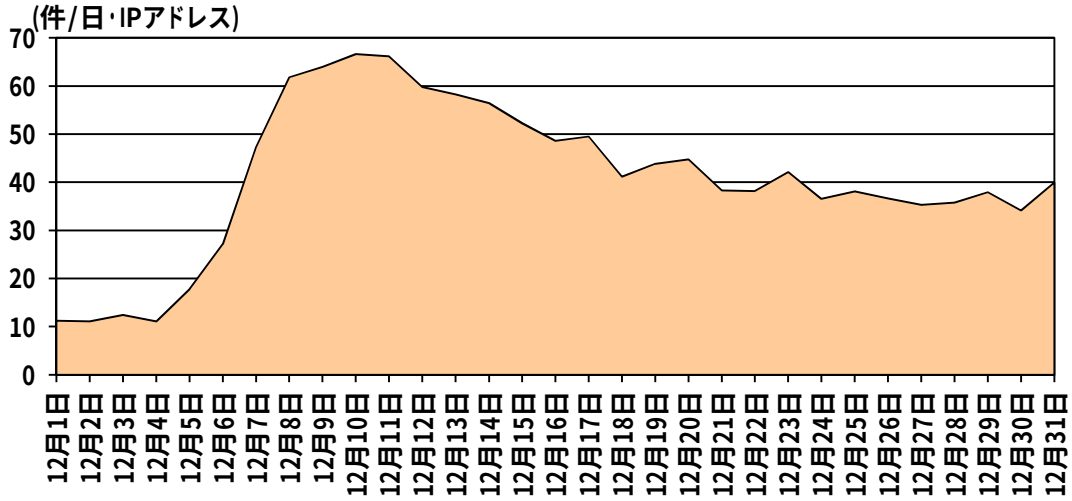

図1 宛先ポート 8080/TCP に対するアクセス件数の推移

これは、特定の NAS 製品に対する Bash の脆弱性を標的としたアクセスが、増加したことが原因であると考えられます[ii]。被害に遭った NAS 製品は、同様の脆弱性がある NAS 製品に対する探索・侵入行為を 8080/TCP ポートに対して行うため、観測したアクセスは、被害に遭った NAS 製品からのものが多いと考えられます。

---

i Contents Management System の略。ウェブサイトのコンテンツを管理するためのシステムで、専門的な知識が無くても比較的簡単にウェブサイトのコンテンツ管理が可能です。

ii 「Bash の脆弱性を標的としたアクセスの観測について（第3報）」（平成 26 年 12 月9日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141209-2.pdf

2 宛先ポート 23/TCP に対するアクセスが高水準で推移

今期も前期[i]に引き続き、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2）。

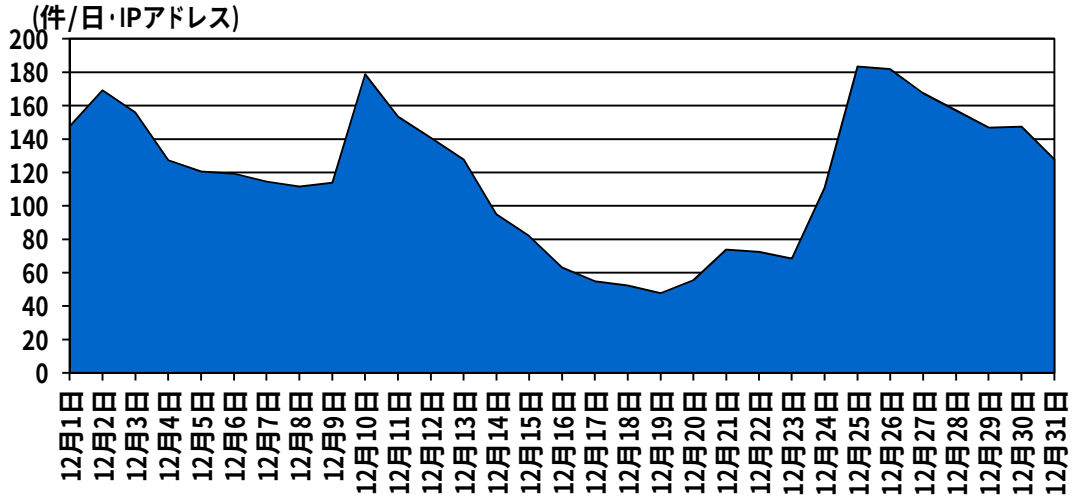

図2 宛先ポート 23/TCP に対するアクセス件数の推移

発信元 IP アドレスの中には、8080/TCP ポートにブラウザでアクセスすると、特定の NAS 製品の管理画面が表示されるものが存在することを確認しています。8080/TCP は、特定の NAS 製品に存在する Bash の脆弱性を標的としたアクセスにより増加しているポートであることから、Bash の脆弱性により侵入し、NAS 製品を踏み台として Telnet でログインできる機器を探索しているものと考えられます。

3 脆弱性が公表されたルータを対象とするアクセスを観測

平成 26 年 12 月に、多くのルータに、脆弱性が存在するファームウェアが実装されており、第三者に管理権限を取得される可能性があることが公表されました[ii]。この脆弱性は、2005 年に修正されている古いものですが、複数のルータでは、未だに古いバージョンのファームウェアが使用されており、全世界で 1,200 万台以上が攻撃可能となっていると指摘されています。この脆弱性は、「Misfourtune Cookie」と呼ばれています。

警察庁では、脆弱性が公表され以降の 12 月 23 日の短時間に、特定の IP アドレスから、脆弱性のあるルータを探索していると思われるアクセスを観測しました（図3）。このアクセスは、全て宛先ポート 80/TCP に対して行われていました。

---

i 「インターネット観測結果等（平成 26 年 11 月期）」（平成 26 年 12 月 18 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20141218.pdf

ii 「メディア・アラート：チェックポイント、一般家庭/小規模企業向けインターネット・ルータ数百万台の乗っ取りを可能にする深刻な脆弱性を発見」（平成 26 年 12 月 24 日）
https://www.checkpoint.co.jp/pr/2014/20141224_mediaalart_Misfortune_Cookie.html
「JVNVU#96446762 複数のブロードバンドルータに、脆弱性が存在するバージョンの Allegro RomPager を使用している問題」（平成 26 年 12 月 22 日）
https://jvn.jp/vu/JVNVU96446762/

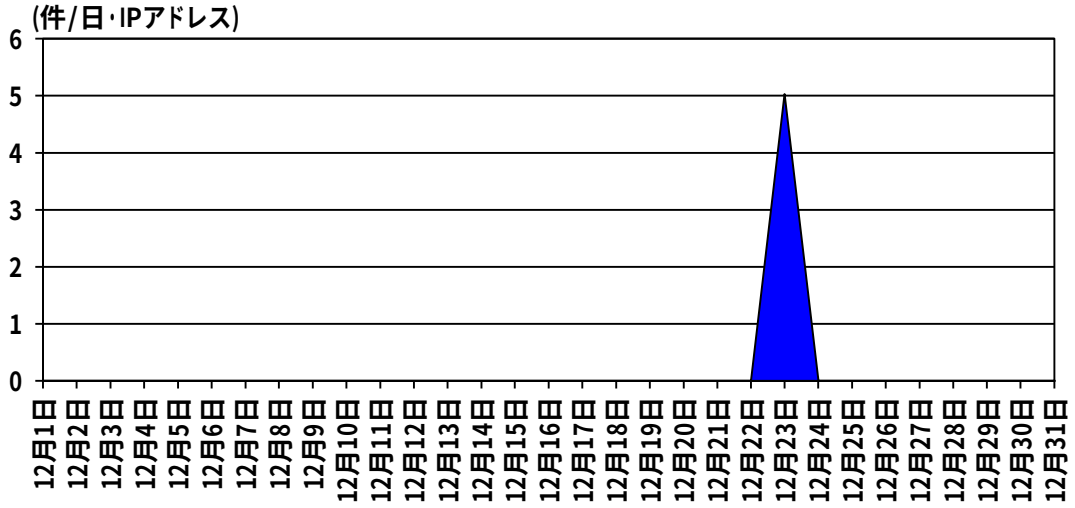

図3　脆弱性が公表されたルータを対象とするアクセス件数の推移

4　脆弱性が公表された CMS を対象とするアクセスを観測

平成 26 年 10 月に、CMS のひとつ Drupal[i]に SQL インジェクションの脆弱性が存在することが公表されました[ii]。この脆弱性が悪用されると、バックドアが作成されたり、ウェブサイトが改ざんされたりする可能性があります。

警察庁では、10 月及び 11 月には、この CMS を対象としたアクセスは観測されませんでしたが、12 月には、特定の IP アドレスからのアクセスを観測しています（図4）。このアクセスの宛先ポートは、全て SSL で使用されるポート 443/TCP でしたが、実際の通信内容は、暗号化されていない HTTP リクエストでした。脆弱性が存在する CMS が稼動しているウェブサイトの探索を行っているものと思われます。このように、脆弱性が公表された直後に、攻撃や探索行為が観測されなくても、ある程度の期間を空けて観測される場合もあるので、セキュリティ修正プログラムの適用を確実に行うなどのセキュリティ対策を実施することが重要です。

---

i PHP で記述されたオープンソースとして開発・配布が行われている CMS
http://drupal.jp/

ii 「JPCERT/CC Alert Drupal の脆弱性に関する注意喚起」（平成 26 年 10 月 21 日）
https://www.jpcert.or.jp/at/2014/at140042.html

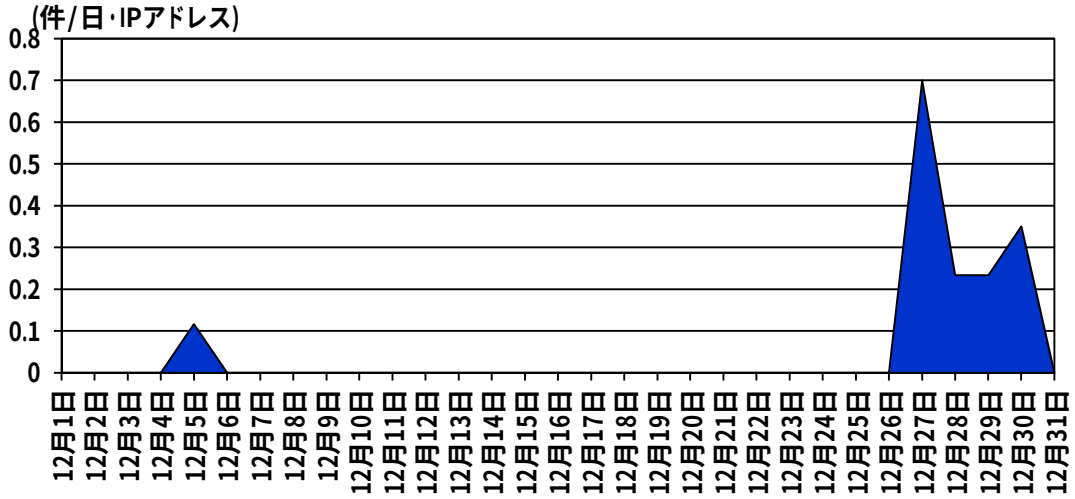

図4　脆弱性が公表された CMS（Drupal）を対象とするアクセス件数の推移