JPCERT CC®

Japan Computer Emergency Response Team Coordination Center



JPCERT-IA-2014-03
発行日 : 2014-10-28

# JPCERT/CC インターネット定点観測レポート
# [2014 年 7 月 1 日～9 月 30 日]

## 1 概況

JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウエアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。なお、本レポートでは、本四半期に観測された日本宛のパケットを中心に分析した結果について述べます。

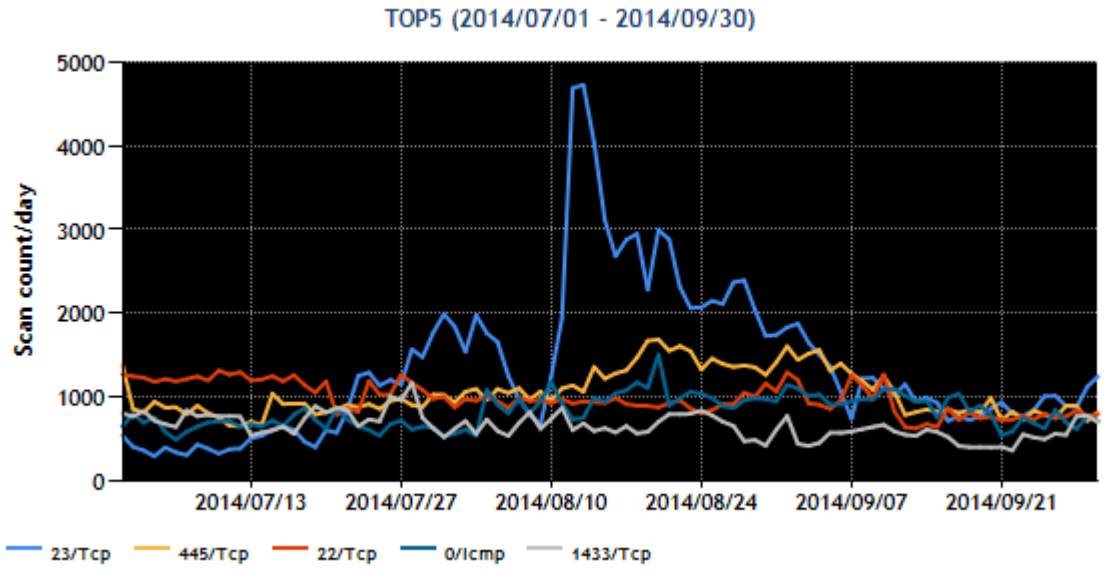
宛先ポート番号別パケット観測数のトップ 5 を [表 1]に示します。

[表 1 : 宛先ポート番号トップ 5]

| 宛先ポート番号 | 本四半期順位 | 前四半期順位 |
|---|---|---|
| 23/TCP (telnet) | 1 | 3 |
| 445/TCP (microsoft-ds) | 2 | 1 |
| 22/TCP(ssh) | 3 | 2 |
| 0/ICMP | 4 | 4 |
| 1433/TCP (ms-sql-s) | 5 | 5 |

※ポート番号とサービスの対応の詳細は、IANA の文書(*1)を参照してください。なお、サービス名は IANA の情報をもとに記載していますが、必ずしも各サービスプロトコルに則ったパケットが受信されているとは限りません。

図 1 は、期間中のトップ 5 の宛先ポート番号ごとの日々のパケット観測数を示しています。



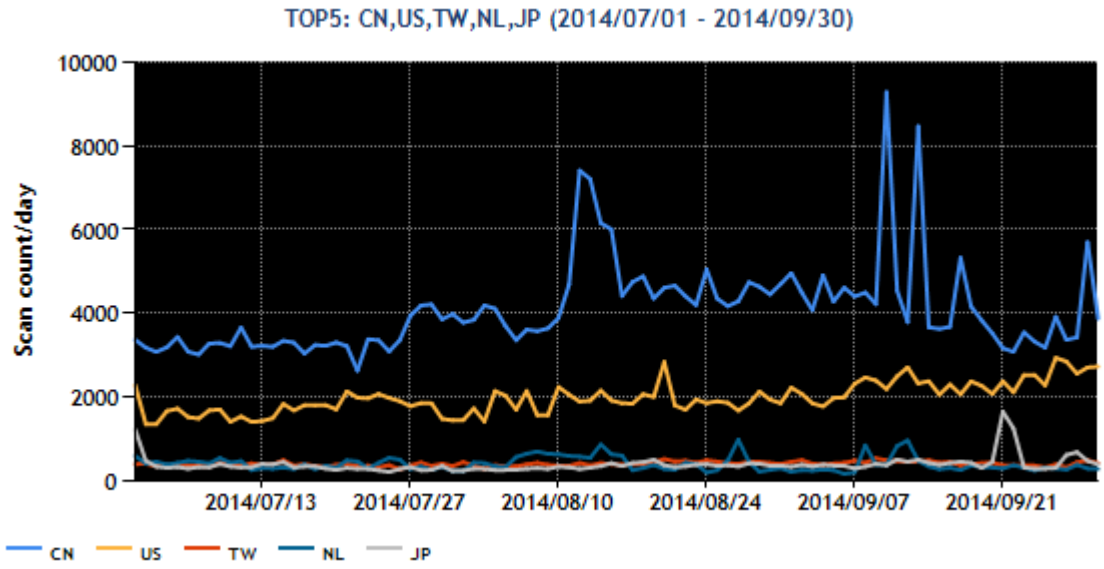

[図 1：2014 年 7~9 月の宛先ポート番号別パケット観測数トップ 5]

送信元地域のトップ 5 を [表 2]に示します。

[表 2：送信元地域トップ 5]

| 送信元地域 | 本四半期順位 | 前四半期順位 |
|---|---|---|
| 中国 | 1 | 1 |
| 米国 | 2 | 2 |
| 台湾 | 3 | 4 |
| オランダ | 4 | 3 |
| 日本 | 5 | 5 |

図 2 に期間中のトップ 5 のパケット送信元地域からの日々のパケット観測数を示します。



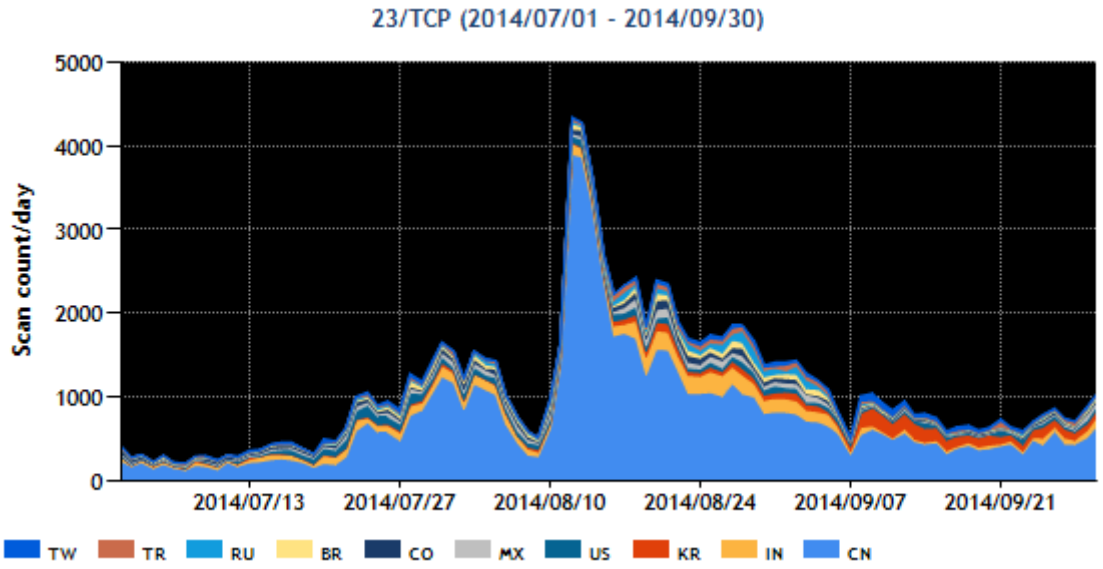

[図 2：2014 年 7~9 月の送信元地域別トップ 5 ごとのパケット観測数]

23/TCP 宛のパケット数が 8 月中旬に増加し、本四半期を通じた合計でも 1 位となりました。23/TCP の現象については、「2.1」で詳しく述べます。その他については、多少の増減はありますが、特筆すべき状況の変化は見られませんでした。

## 2　注目された現象

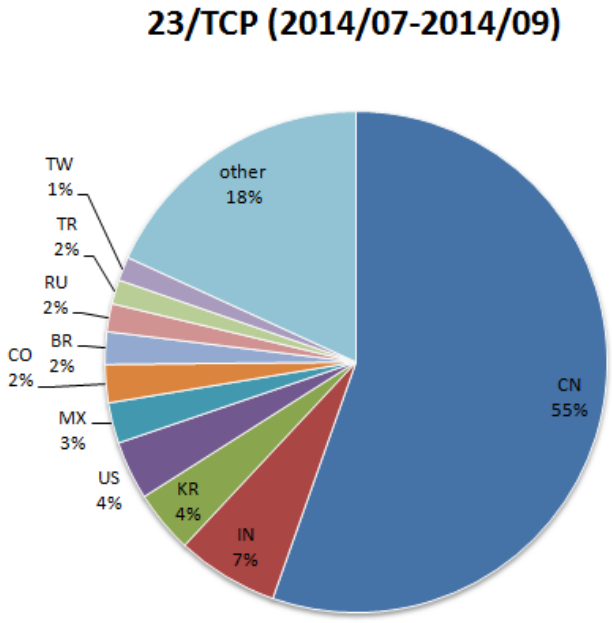
### 2.1　23/TCP 宛へのパケットの増加

図 3 が示すように、7 月中旬から 9 月上旬にかけて 23/TCP 宛へのパケット数が増加しました。telnet を待ち受けるサーバを搭載したネットワーク機器を対象とする探索活動については、過去の定点観測レポート [*2,3,4] でも紹介したことがありましたが、再び活発になっています。




[図 3：2014 年 7～9 月の 23/TCP 宛のパケット観測数]

図 4 が示すように本四半期に観測された 23/TCP 宛のパケットの送信元地域のトップは中国で、23/TCP 宛の全パケット数のうち約 5.5 割を占めました。図 1 および図 3 が示すように半数以上を占める中国を送信元としたパケットの増加の傾向が、そのまま本四半期の 23/TCP の傾向に表れています。また、2 位のインドと 3 位の韓国についても若干の増加が見られました。



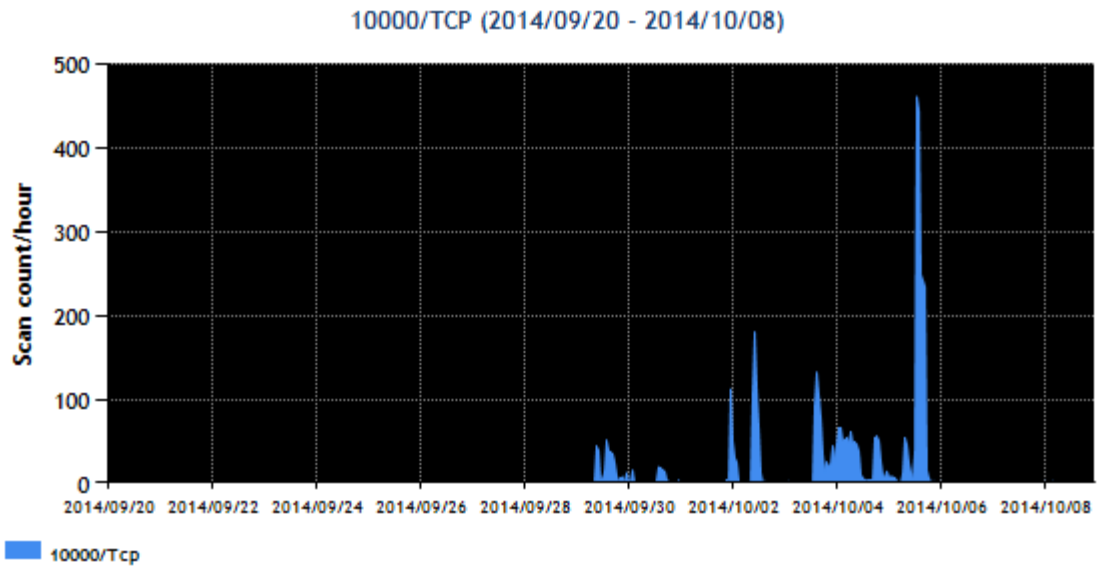

[図 4：2014 年 7～9 月の 23/TCP 宛の送信元地域割合]

23/TCP 宛パケットの送信元 IP アドレスについて調査したところ、インターネット定点観測レポート(2014 年 1～3 月) [*3]で紹介したネットワークカメラ製品および、国外で使用されている特定のブロードバンドルータ製品 が多数稼働していました。

本四半期の増加は、ネットワークカメラ製品やブロードバンドルータなどに Bot プログラムが設置され、それらの機器が複数のセンサーに対して頻繁にパケットを送ったことが原因と推測しています。

### 2.2 10000/TCP 宛へのパケットの増加

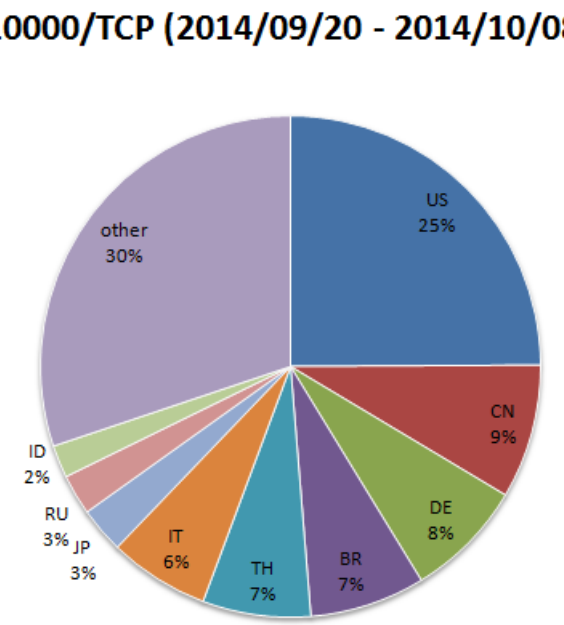
図 5 が示すように 9 月下旬から、10000/ TCP 宛へのパケット数が増加しました。[*5]




[図 5 : 2014 年 9 月 20 日から 10 月 9 日までの 10000/TCP 宛のパケット観測数]

2014 年 9 月 20 日から 10 月 9 日までに観測した 10000/TCP 宛のパケットの送信元地域別の内訳トップは米国ですが、米国以外は図 6 と図 7 が示すように日本を含む様々な地域に分散しています。


[図 6：2014 年 9 月 29 日の 10000/TCP 宛のパケット送信イメージ]




[図 7：2014 年 9 月 20 日から 10 月 9 日までの 10000/TCP 宛の送信元地域割合]

10000/TCP ポートは、ウェブベースのシステム管理ツールである Webmin の標準ポートとして利用されています。センサーに対して 10000/TCP 宛へのパケットを送信した IP アドレスについて調査したところ、Webmin が多数稼働 (図 8 は調査結果の一例) していることを確認しました (センサーに対して 10000/ TCP 宛のパケットを送信した IP アドレスを調査した限りでは、国内の IP アドレスは、他の地域よりも高い割合で Webmin が稼働していました)。


[図 8：送信元 IP アドレスで稼働する Webmin の一例]

Webmin で標準の shell として使われることが多い GNU bash に、深刻な脆弱性があったことが 9 月下旬に公表 (*6) されました。この脆弱性を悪用すると、Webmin を稼働させているユーザの権限で、任意のコードを実行することができます (JPCERT/CC では、Webmin 1.700 (RPM) と CVE-2014-6271 の影響を受けるバージョンの GNU bash を使用して検証し、任意のコードが実行できることを実際に確認しています) 。標準的なインストールをすると、Webmin は管理者 (root) 権限で稼働しますので、この脆弱性を悪用されれば管理者権限で任意のコードを実行され得ることになります。

今回観測している 10000/TCP 宛のパケットは、GNU bash の脆弱性を悪用できる Webmin を探索するものと推測されます。

インターネットからアクセス可能なサーバで Webmin がインストールされているかどうかを調査し、インストールされていた場合には、「TCP 10000 番ポートへのスキャンの増加に関する注意喚起」(*7)を参考に適切なセキュリティ対策 (パッチやアップデート、アクセス制御、セキュリティ設定の再確認など) を実施して、攻撃の踏み台に使用されないよう努めてください。

また、GNU bash の脆弱性については、cPanel や Parallels Plesk Panel などシステム管理ツールもの影響を受ける(*8,9)とのことですので、Webmin に準じた対策を検討してください。cPanel や Parallels Plesk Panel が使用する標準ポート (2082/TCP, 2083/TCP, 8443/TCP) 宛のパケット数は、以前から若干量が観測されてきたものの、9 月下旬の前後における変化はありません。

## 3 参考文献

(1) Service Name and Transport Protocol Port Number Registry
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
(2) JPCERT/CC インターネット定点観測レポート(2012 年 1～3 月)
https://www.jpcert.or.jp/tsubame/report/report201201-03.html
(3) JPCERT/CC インターネット定点観測レポート(2012 年 4～6 月)
https://www.jpcert.or.jp/tsubame/report/report201204-06.html
(4) JPCERT/CC インターネット定点観測レポート(2014 年 1～3 月)
https://www.jpcert.or.jp/tsubame/report/report201401-03.html
(5) @police 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）
https://www.npa.go.jp/cyberpolice/topics/?seq=14737
(6) GNU bash の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140037.html
(7) TCP 10000 番ポートへのスキャンの増加に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140038.html
(8) cPanel Security Team: Bash CVE-2014-6217 and CVE-2014-7169
http://cpanel.net/cpanel-security-team-bash-cve-2014-6217-and-cve-2014-7169/
(9) [Hub] 「Shellshock」脆弱性
http://kb.sp.parallels.com/jp/123006

本活動は、経済産業省より委託を受け、「平成２６年度サイバー攻撃等国際連携対応調整事業」として実施したものです。