

JPCERT/CC インターネット定点観測レポート

2024年7月1日 ~ 2024年9月30日



一般社団法人 JPCERT コーディネーションセンター

2024年11月12日

目次

1. 概況	3
2. 日本からの Telnet (23/TCP) を対象としたパケットの送信元 IP アドレス数の減少について	6
3. JPCERT/CC からのお願い	7
4. 参考文献	8

本活動は、経済産業省から委託を受け、「令和 6 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。

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、一定のIPアドレス帯に向けて網羅的に発信されるパケットを観測しています。こうしたパケットの発信は特定の機器や特定のサービス機能を探るために行われていると考えられます。JPCERT/CCでは、センサーで観測された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、マルウェ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。センサーから収集したデータを分析し、問題が見つければ、解決できる可能性がある関係者に情報を提供し、対処を依頼しています。

本レポートでは、本四半期にTSUBAME（インターネット定点観測システム）が観測した結果とその分析の概要を述べます。

本四半期に探索された国内のサービスのトップ5は〔表1〕に示すとおりでした。

〔表1 頻繁に探索された国内のサービスのトップ5〕

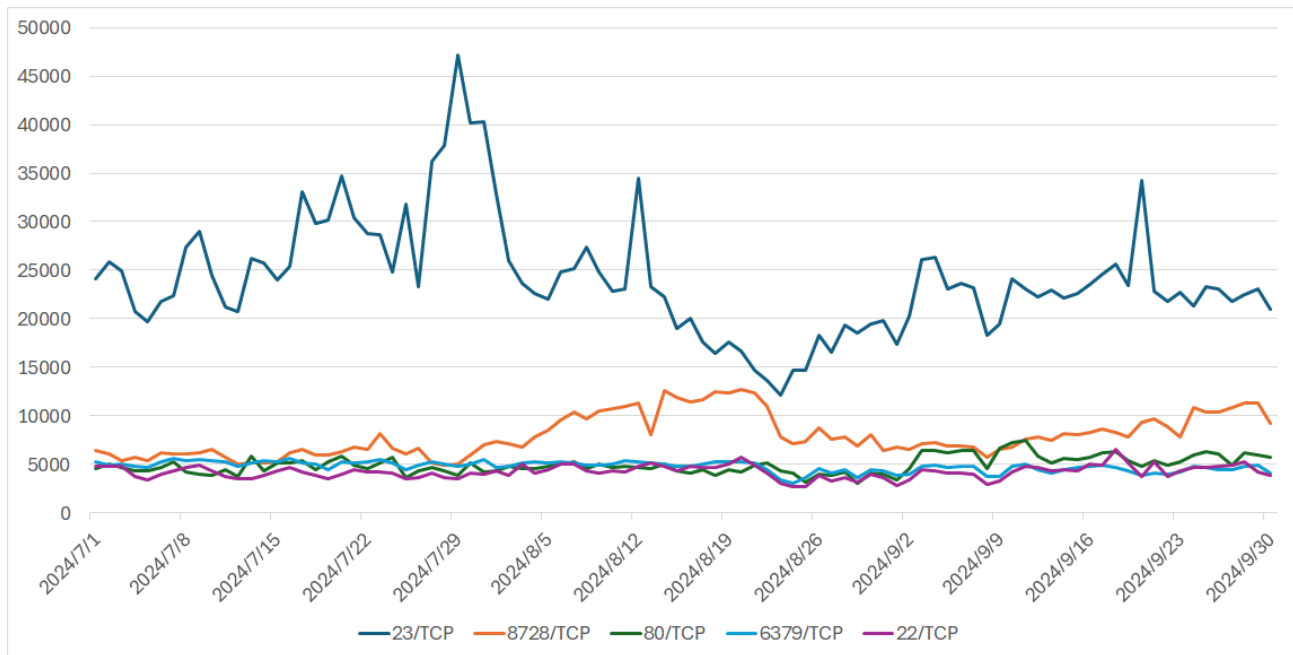
順位	宛先ポート番号	前四半期の順位
1	Telnet (23/TCP)	1
2	8728/TCP	2
3	http (80/TCP)	4
4	redis (6379/TCP)	3
5	ssh (22/TCP)	5

※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のっとった形式のパケットが受信されているとは限りません。

〔表1〕に示したサービスを探るパケット観測数の推移を〔図1〕に示します。



[図1 探索頻度トップ5のサービス（宛先ポート番号）宛のバケット観測数の推移（2024年7～9月）]

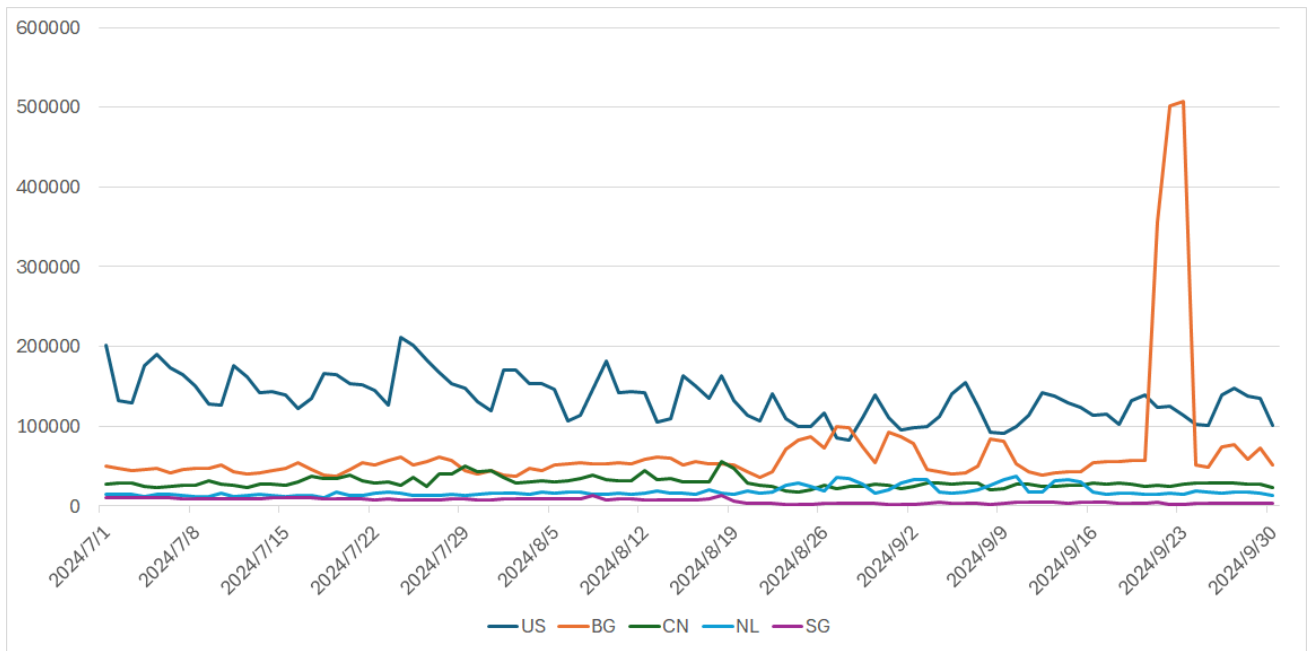
本四半期に最も頻繁に探索されたサービスは Telnet（23/TCP）、2番目は 8728/TCP でした。このポート番号は IANA のリストには記載されていませんが、MikroTik 社のルーターの管理で使われている API が待ち受けに使用するポート番号です。3番目から5番目には、http（80/TCP）と redis（6379/TCP）、ssh（22/TCP）が入りました。9月3日ごろから http への探索活動が活発になっていて、redis と順位が入れ替わりました。

次に、国内を対象とした探索活動の探索元地域を、本四半期において活動が活発だった順に並べたトップ5を [表2] に示します。

[表2 探索元地域トップ5]

順位	送信元地域	前四半期の順位
1	米国（US）	1
2	ブルガリア（BG）	2
3	中国（CN）	3
4	オランダ（NL）	4
5	シンガポール（SG）	6

[表2] に掲げた本四半期の送信元地域の傾向を [図2] に示します。



[図 2 2024 年 7～9 月の送信元地域の傾向]

引き続き米国がトップ、以下 4 番目まで順番に変更はありませんでした。ロシアを送信元としたパケットが 8 月 19 日ごろに減少し、シンガポールと入れ替わりました。それ以外の送信元地域の傾向について、特筆すべき点はありませんでした。なお、TSUBAME では RIR (Regional Internet Registry) による割り当て情報を用いて個々の IP アドレスの地域を判断しています。

2. 日本からの Telnet (23/TCP) を対象としたパケットの送信元 IP アドレス数の減少について

本章では、日本国内を送信元 IP アドレスとした特定のパラメーターを持つ Telnet の探索の動向について取り上げます。本四半期を通して、Telnet (23/TCP) を対象とした探索元の数が増減しました (図 3)。



[図 3 Telnet を対象としたパケットの日本国内 IP アドレス数の推移]

期中を通じて緩やかな減少傾向が見られ、9月最終週には7月一週目の約4割まで少なくなりました。送信元のIPアドレスも減ってきており、機器においてもすでに確認されているルーターやDVR機器のみで、新たなものは見られませんでした。

この背景には、IoT機器などに対するセキュリティ対策が進んだ可能性があります。攻撃者の興味は他に移った可能性や、攻撃者が使用するマルウェアが変化した第三者に対してむやみに探索を行わない挙動をとるようになった可能性も考えられます。

今後再び活発化する可能性も残っておりますので、ファームウェアの更新や攻撃に対する軽減策などについては継続して行ってください。なお、本件のような異常な探索活動が観測された場合には、「3. JPCERT/CCからのお願い」に記載したように、ISPに情報を提供しています。

3. JPCERT/CC からのお願い

JPCERT/CC では、不審なパケットの送信元 IP アドレスについて ISP を通じて当該 IP アドレスのユーザーに確認と対応をお願いすることがあります。このような依頼を受け取った際には、調査活動へのご理解をいただき、可能であれば、使用していた製品やファームウェアのバージョン、侵害の有無などの情報提供などのご協力をいただければ幸いです。本報告書で紹介したものを含め、不明な探索活動が複数あり、提供いただいた情報が解明の重要な糸口になり得ます。

4. 参考文献

(1) IANA (Internet Assigned Numbers Authority)

「Service Name and Transport Protocol Port Number Registry」

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

本文書を引用、転載する際には JPCERT/CC 広報 (pr@jpcert.or.jp) まで確認のご連絡をお願いします。
本文書に記載の社名、製品名は各社の商標または登録商標です。
最新情報については JPCERT/CC の Web サイトを参照してください。

- ・ JPCERT コーディネーションセンター (JPCERT/CC) : <https://www.jpcert.or.jp/>
- ・ インシデント情報の提供および対応依頼 : info@jpcert.or.jp, <https://www.jpcert.or.jp/form/>
- ・ 脆弱性情報ハンドリングに関するお問い合わせ : vultures@jpcert.or.jp
- ・ 制御システムセキュリティに関するお問い合わせ : icsr@jpcert.or.jp
- ・ セキュアコーディングセミナーのお問い合わせ : secure-coding@jpcert.or.jp
- ・ 公開資料の引用、講演依頼、その他のお問い合わせ : pr@jpcert.or.jp
- ・ PGP 公開鍵について : <https://www.jpcert.or.jp/jpcert-gpg.html>

JPCERT/CC インターネット定点観測レポート [2024年7月1日～2024年9月30日]

- ・ 2024年11月12日 初版発行
- ・ 発行
一般社団法人 JPCERT コーディネーションセンター
〒103-0023
東京都中央区日本橋本町 4-4-2 東山ビルディング 8 階
TEL 03-6271-8901 FAX 03-6271-8908
URL <https://www.jpcert.or.jp/>