

JPCERT/CC インターネット定点観測レポート

2024年4月1日 ~ 2024年6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8月9日

目次

1. 概況	3
2. 日本国内を送信元 IP アドレスとし特定の TCP のパラメーターを持つ Telnet の探索数の推移に ついて	6
3. JPCERT/CC からのお願い	7
4. 参考文献	8

本活動は、経済産業省より委託を受け、「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]

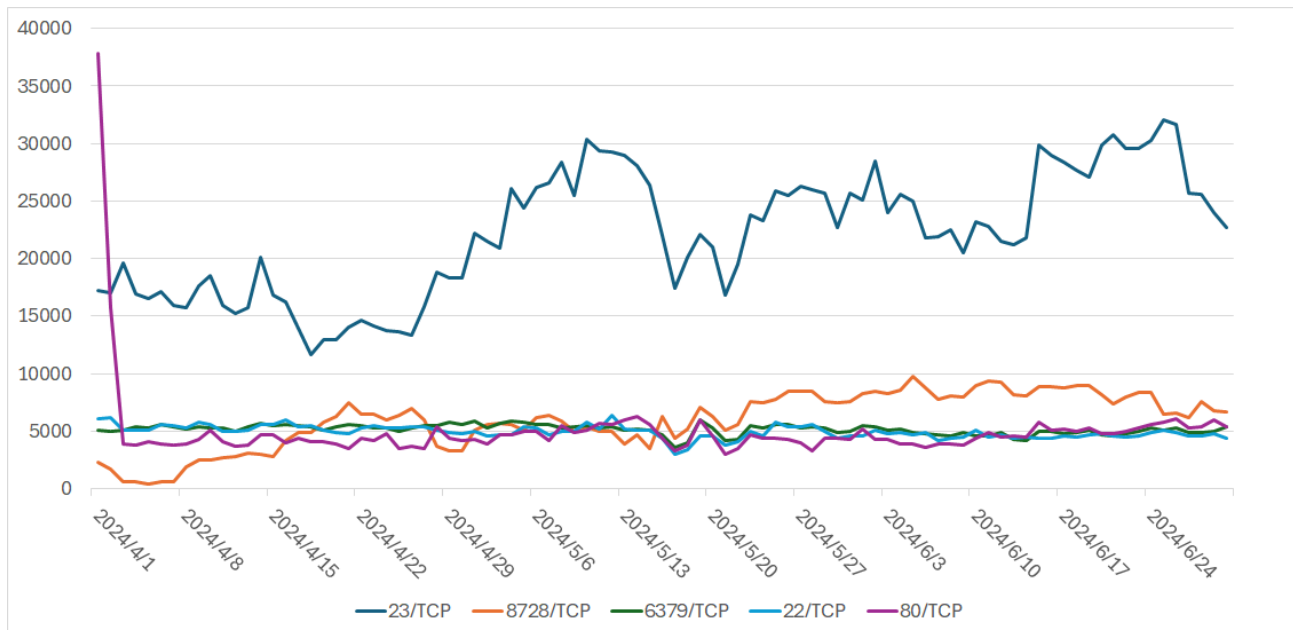
順位	宛先ポート番号	前四半期の順位
1	telnet (23/TCP)	1
2	8728/TCP	9
3	redis (6379/TCP)	2
4	http (80/TCP)	4
5	ssh (22/TCP)	3

※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] に示した探索されたサービスのトップ5 に対するパケット観測数の推移を [図 1] に示します。



[図1 2024年4～6月のポート番号宛のパケット観測数トップ5の推移]

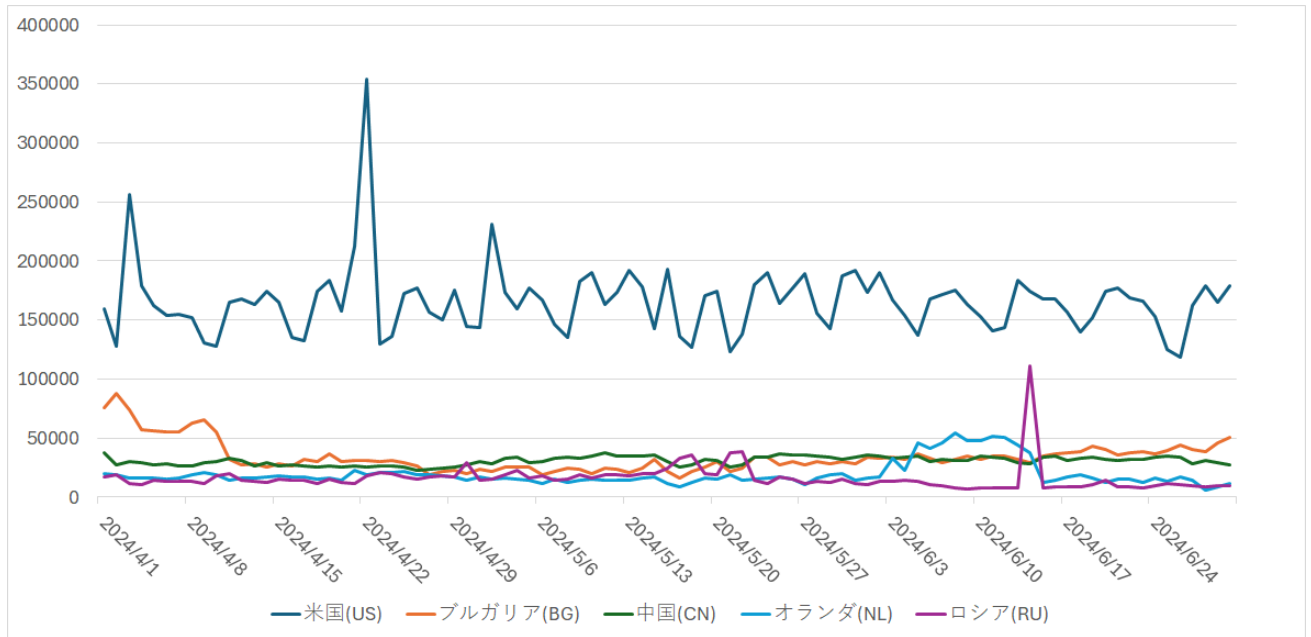
本四半期に最も頻繁に探索されたサービスは telnet (23/TCP) でした。2番目は 8728/TCP でした。このポート番号は iana のリストには記載されていませんが、MikroTik 社のルーターの管理で使われている API が待ち受けに使用するポート番号です。3番目から5番目には、redis (6379/TCP)、http (80/TCP)、ssh (22/TCP) が入りました。

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)	4
4	オランダ (NL)	3
5	ロシア (RU)	5

[表2] に掲げた送信元地域からのパケット観測数の推移を [図2] に示します。

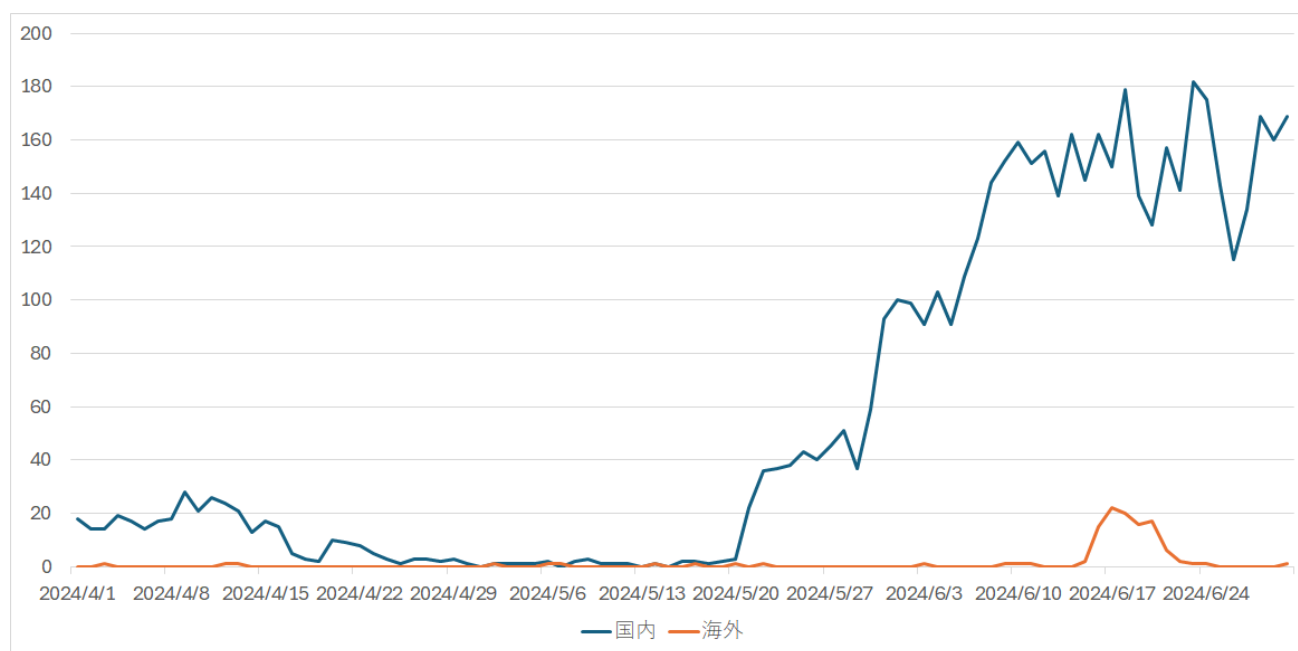


[図 2 2024 年 4～6 月の送信元地域別トップ 5 ごとのパケット観測数の推移]

引き続き米国がトップ、ブルガリアが 2 番目でした。オランダは 6 月中旬に一時的に増加がみられましたが、それ以外の時期は中国からのパケットが多く観測されたため、3 番目は中国になりました。それ以外の地域については特筆すべき変化がありませんでした。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. 日本国内を送信元 IP アドレスとし特定の TCP のパラメーターを持つ Telnet の探索数の推移について

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。5月20日ごろから、国内からの telnet (23/TCP) を対象とした探索元の数が増加しました。海外は6月17日ごろ一時的に観測されましたが、それ以外の期間は観測されていません(図3)。



[図3 window サイズ 5656 のパケットの送信元の推移]

これらの探索パケットは、Mirai に由来するパケットを示す特徴を持たず、TCP のパラメーターの一つの window サイズが 5656 であることが特徴です。

一方、探索元のほとんどで、http や https 等のアクセスによる機種の特特定が行えませんでした。これは、探索元の機器がマルウェアによる高負荷等で再起動を起こしたために、探索時と調査時点とで IP アドレスが変わり追跡できなかったと推測されます。

このように機器の特特定に至らないケースがほとんどでしたが、一部について、国内メーカー製ブロードバンドルーターが探索元であることがわかり、関与が疑われる製品とファームウェアのバージョンが複数見つかりました。同一 IP アドレスからの探索は 1~2 日程度しか続きませんが、機器が再起動して IP アドレスが付け替わっている影響と考えられます。

このことから、Mirai とは異なるマルウェアを使ったボットネットの活動が活発化しており、国内の特定のベンダー製のルーターを対象としているものと推測しています。詳細情報については伏せますが、本件に観測した探索については、「3. JPCERT/CC からのお願い」にも記載の通り、ISP や製品開発者らに対して情報提供を行っております。

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 4 月 1 日～2024 年 6 月 30 日]

- ・ 2024 年 8 月 9 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/>