JPCERT/CC インターネット定点観測レポート

2024 年 10 月 1 日 ～ 2024 年 12 月 31 日

一般社団法人 JPCERT コーディネーションセンター

2025 年 2 月 28 日

JPCERT CC®

目次

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索す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、問題が見つかれば、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。

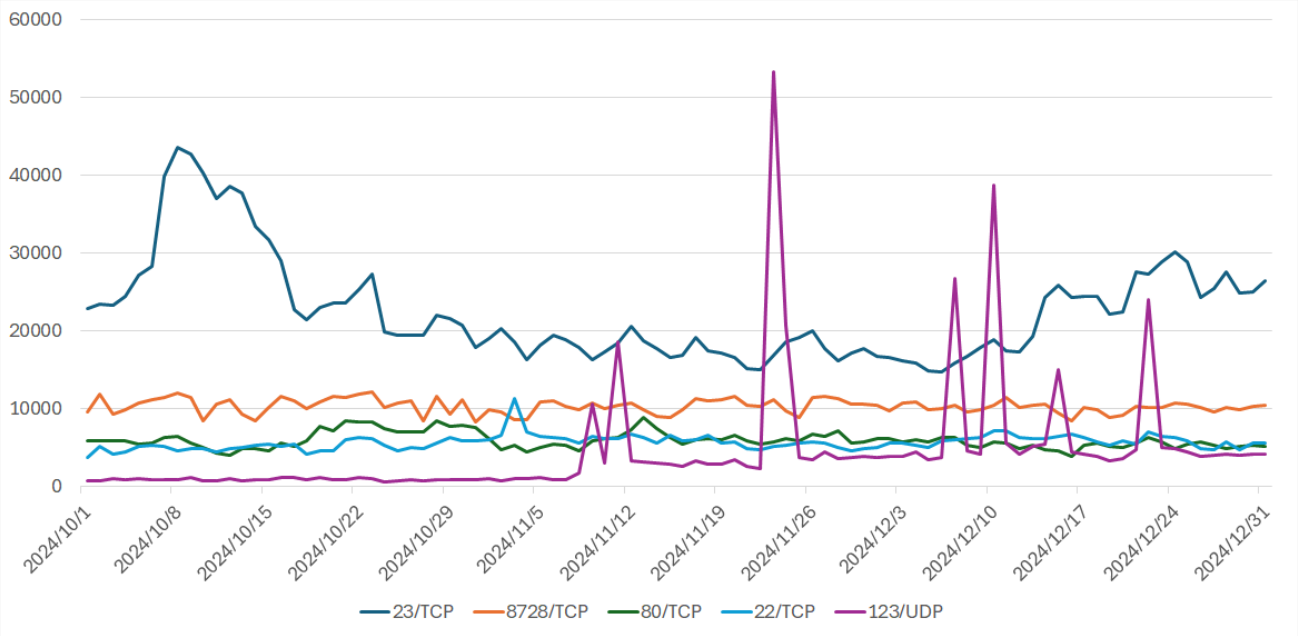
本四半期に探索された国内のサービスのトップ 5 は［表 1］に示すとおりでした。

［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）	3
4	ssh（22/TCP）	5
5	ntp（123/UDP）	TOP10 外

※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索するパケット観測数の推移を［図 1］に示します。



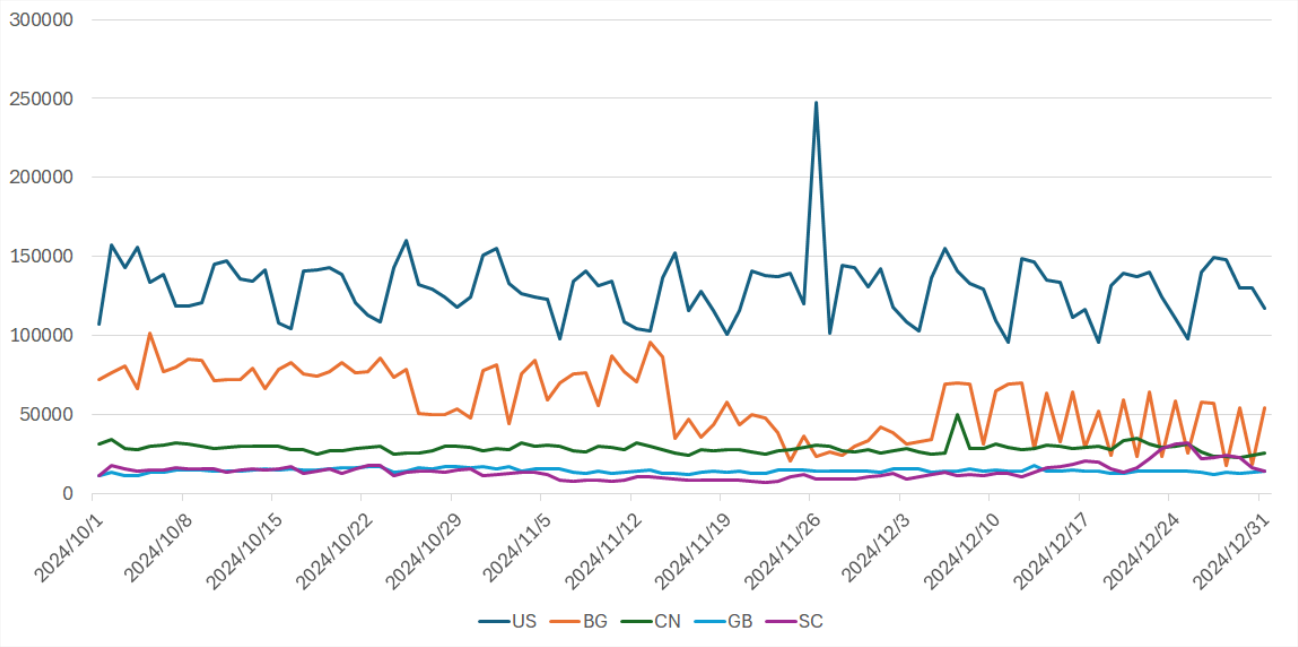
［図 1 探索頻度トップ 5 のサービス（宛先ポート番号）宛のパケット観測数の推移（2024 年 10～12 月）］

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に使われている API で待ち受けに使用されています。3 番目、4 番目は、http（80/TCP）と、ssh（22/TCP）でした。5 番目には何度か一時的な急増が見られた ntp（123/UDP）が入りました。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	イギリス（GB）	6
5	セーシェル（SC）	9

［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。

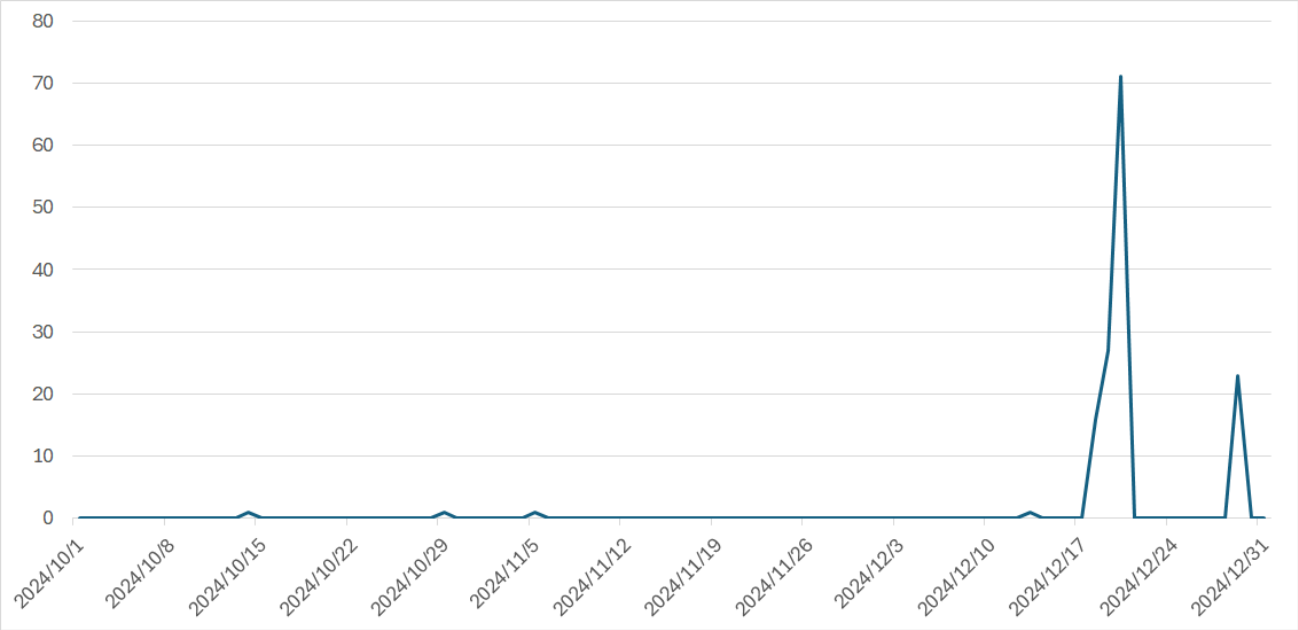


［図 2 送信元地域ごとのパケット数の推移（2024 年 10～12 月）］

トップの米国から 3 番目までは前四半期と同じでした。オランダからのパケットが 11 月 26 日ごろから徐々に減少して 6 位となり、代わりにイギリスが 4 位となりました。5 位になったセーシェルですが、複数の宛先ポート番号を対象としたパケットが一時的に増加する現象が見られました。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. オープンリゾルバーを踏み台に使用した攻撃パケットの観測について

本章では、12 月に国内のオープンリゾルバーを踏み台とした攻撃パケットの観測について取り上げます。攻撃パケットとして DNS が使用する 53/UDP が送信元ポート番号となっているのが特徴です。日本国内が送信元であった攻撃パケットの IP アドレス数の推移を示します（図 3）。



［図 3 日本国内から送信された DNS パケットの IP アドレス数（2024 年 10～12 月）］

期中を通じて攻撃パケットを観測しなかった日が大半ですが、12 月 18 日から 20 日、29 日に急激かつ一時的な増加が見られました。送信元となっていた IP アドレスについて SHODAN などを用いて確認すると、ほぼすべてがオープンリゾルバー状態であることが確認できました。それらのホストについて次のいずれかの特徴が見られました。

1. Linux や MacOS 等を用いたサーバーがリゾルバーとして動作しており、リゾルバーに対するアクセス制限が行われていない
2. SOHO・事業者向けルーター製品で、アクセス制限を設定していない
3. 一般向けルーター製品で、WAN ポートと LAN ポートとを取り違えて接続して利用している

機器やサーバーを適切に設定すること、特にインターネットからのアクセス（WAN ポートへのアクセス）に対するアクセス制限の確認をお願いします。多くのケースで、リゾルバーとして確認できるだけでなく、管理インタフェースや API ポートなどに WAN からアクセス可能な状態でした。意図していない設定や接続状態になっていないかを確認することも重要です。マニュアルやコンフィグ・設定を照らしあわせて、意図した設置になっていることを確認してください。JPCERT/CC では、オープンリゾルバーか

どうかの判定用のサービス [2] を提供しています。サーバーの構築後やネットワーク機器の設置後にぜひご利用ください。

今回観測したパケットは比較的サイズが大きくなりやすい DNSSEC を使うなどの特徴がありました。また、TSUBAME のセンサーは世界各地に設置していますが、特定のクラウド事業者のネットワークに設置したセンサーのみで観測しました。当該事業者の IP アドレスを詐称した、DNS クエリを送信することで、当該事業者への DDoS 攻撃を試みた活動の一部であった可能性があったため、今回のレポートでは本事象を取り上げました。

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

(2) JPCERT/CC

オープンリゾルバー確認サイト
https://www.jpcert.or.jp/magazine/security/openresolver.html

- 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-pgp.html

JPCERT/CC インターネット定点観測レポート［2024 年 10 月 1 日～2024 年 12 月 31 日］
- 2025 年 2 月 28 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/