JPCERT Coordination Center



# JPCERT/CC インターネット定点観測レポート

## 2025 年 1 月 1 日 ～ 2025 年 3 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 6 月 6 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

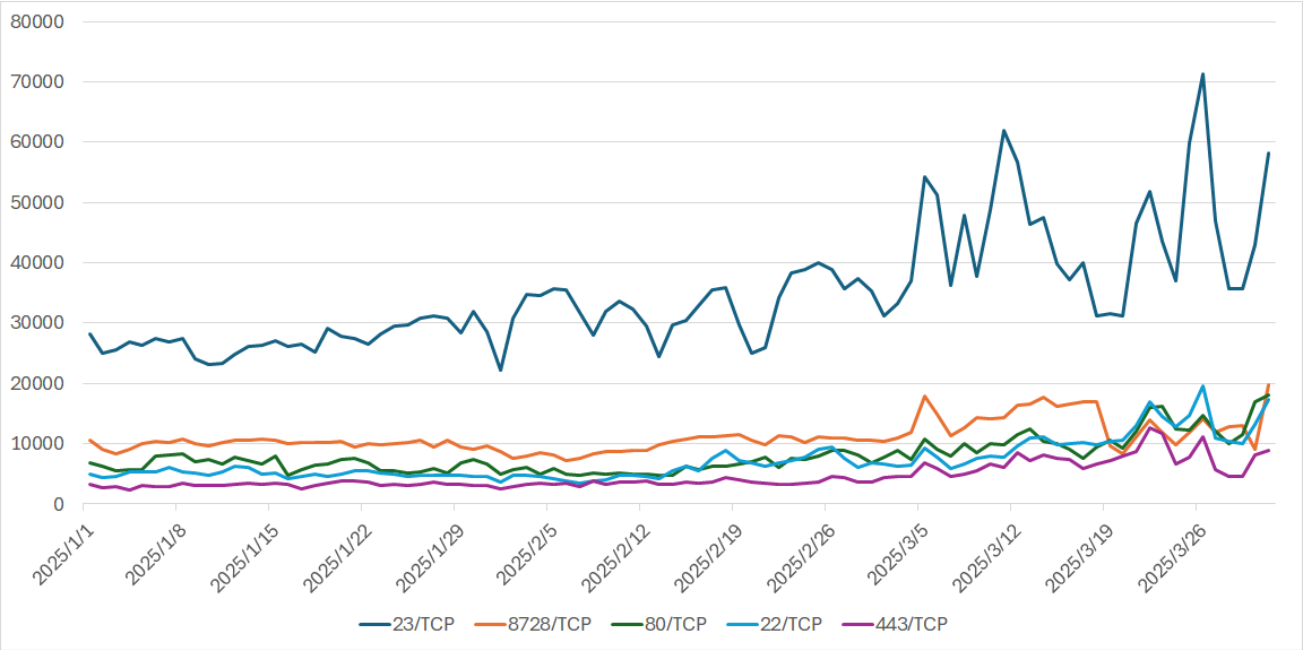
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、 一定の IP アドレス帯に向けて網羅的に発信されるパケットを観測しています。こうしたパケットの発信はそれぞれ特定の機器や特定のサービス機能を探索するために行われていると考えられます。JPCERT/CC では、センサーで観測されたパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。センサーから収集したデータを分析し、攻撃対象となっている問題や攻撃に利用されている問題が見つかれば、解決でき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） | 4 |
| 5 | https（443/TCP） | 6 |

※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。



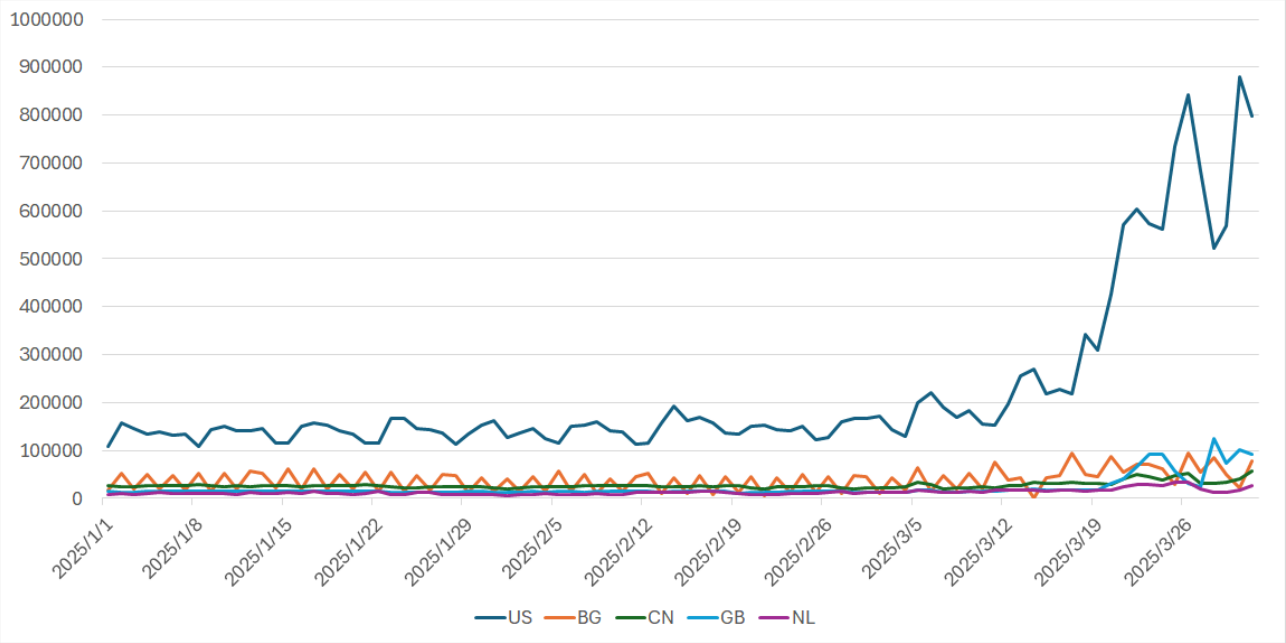

［図 1 探索頻度トップ 5 のサービス（宛先ポート番号）宛のパケット観測数の推移（2025 年 1～3 月）］

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。8728/TCP 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のための API に用いられており、それを探索していると推測しています。3 番目は http（80/TCP）、4 番目は ssh（22/TCP）でした。5 番目には 3 月に入ってから探索数が増えてきている https（443/TCP）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） | 4 |
| 5 | オランダ（NL） | 6 |

［表 2］に掲げた 2025 年 1～3 月の探索元地域からのパケット数の傾向を［図 2］に示します。

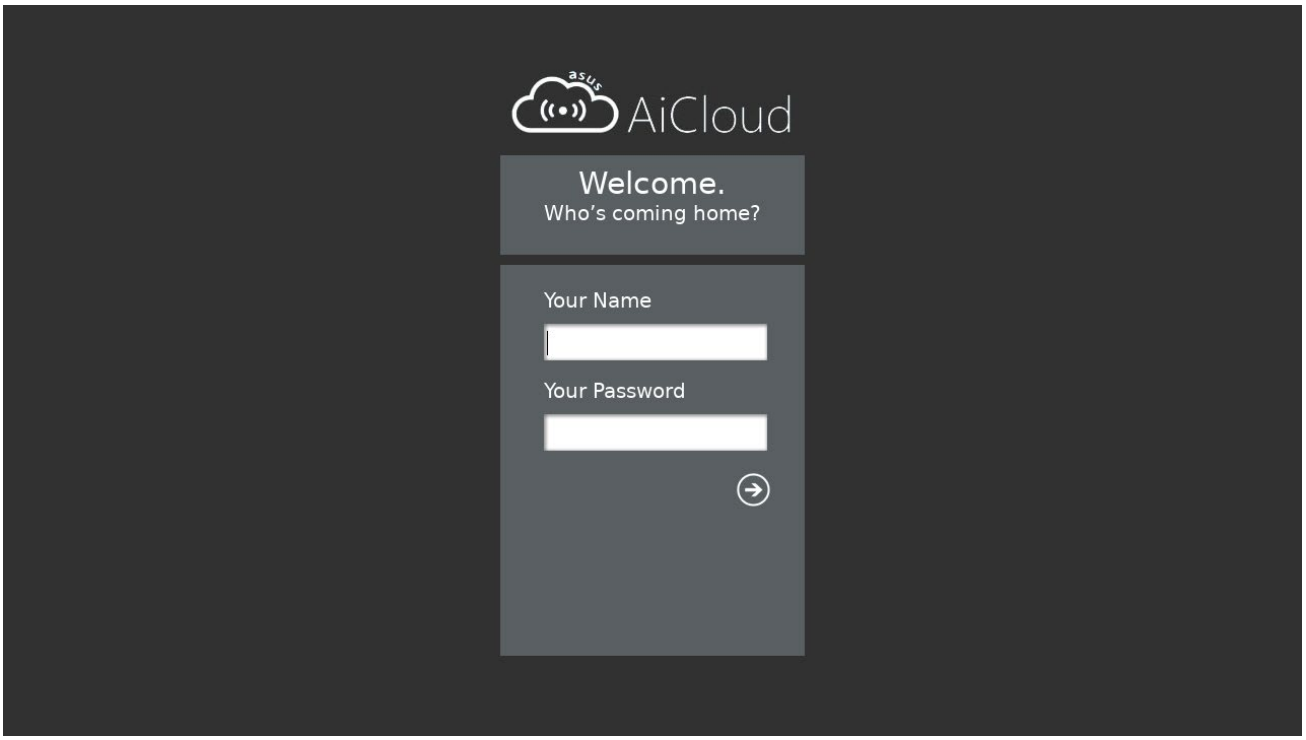



［図 2 送信元地域ごとのパケット数の推移（2025 年 1～3 月）］

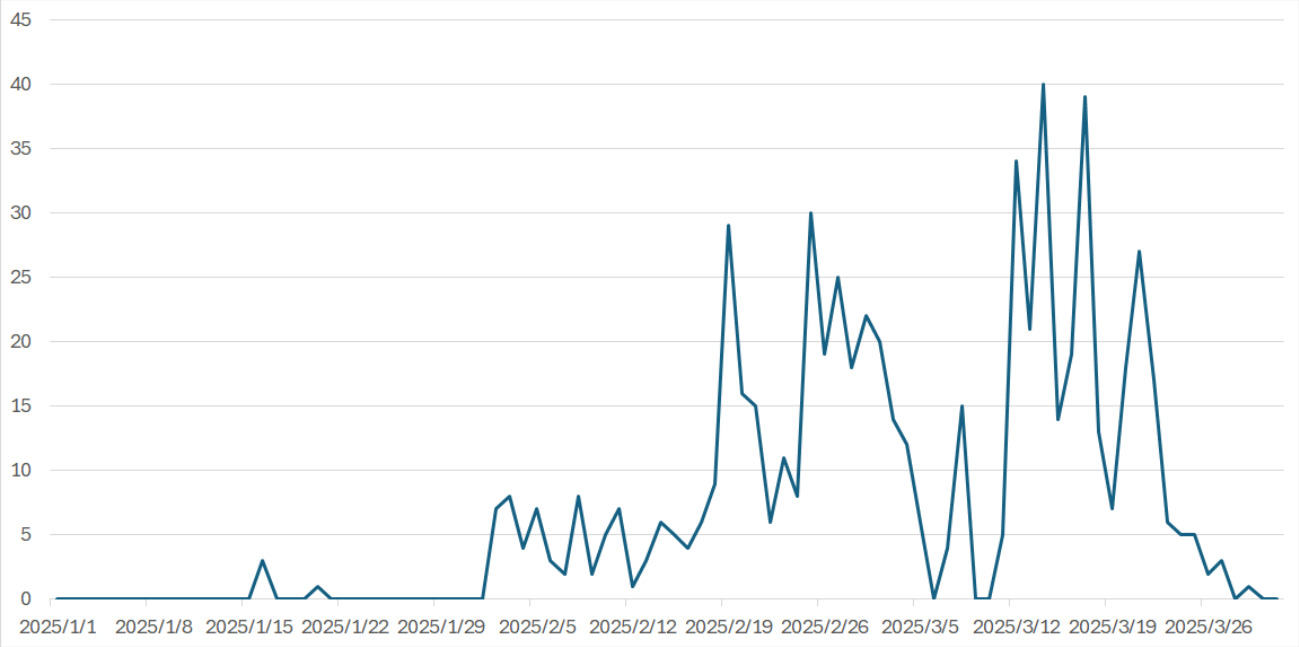
トップの米国から 4 番目までは前四半期と同じでした。特に米国については 3 月 18 日ごろから米国のクラウド事業者を送信元とするパケットが増加しました。2 番目から 4 番目については特に大きな変化はなく、5 番目には前回 6 番目だったオランダが入りました。なお、TSUBAME では RIR（Regional Internet Registry）による割り当て情報を用いて個々の IP アドレスの地域を判断しています。

## 2. マルウェアに感染した ASUS 社製ルーターと見られる機器からのパケットの観測について

TSUBAME で観測されるパケットの多くが、マルウェアに感染した機器から送信されていることがこれまでの観測で分かっています。どのような機器が関与しているのかを明らかにして対策などに結びつけるために、パケットの送信元にブラウザーでアクセスするなどして情報を収集することにしています。そのような活動において、以前も稀には確認されていた ASUS 社製ルーターのログイン画面（図 3）が、2025 年 2 月からほぼ連日確認されるようになりました（図 4）。本章では、その背景を探るために行った調査について述べます。




［図 3 ASUS 社製ルーターのログイン画面］




［図 4 ASUS 社製ルーターが動作しているとみられる IP アドレス数の推移］

図 3 のログイン画面は、ASUS 社製ルーターに搭載されている AiCloud という独自の機能が有効となっている場合に表示される画面です。AiCloud には、外出先などからインターネット経由でルーターに接続された USB ストレージデバイスを NAS のようにアクセスする、LAN 内の共有フォルダーにアクセスする、WoL で PC の電源を ON にすることができる機能などがあります。

一般的に、Mirai 等のルーターなど IoT 機器を対象とするマルウェアは感染した状態を保つ永続化する機能を持たないものがほとんどです。そのため、マルウェアによってルーターがスキャン活動を行うと負荷が高まる等の要因によって再起動等を起こし、マルウェアに感染していない状態となります。これは、同社製ルーターが動作していた IP アドレスからのパケットの約 9 割が 48 時間以内に観測されなくなったことからも推測されます。

しかし、2 月から 3 月と 2 カ月にわたって同社製ルーターのログイン画面が新たに発見され続けました。これは、同社製ルーターの脆弱性を悪用しマルウェアを感染させようとする攻撃活動がこの期間に継続して発生していたことによるものと推測されます。

ASUS 社製ルーターの脆弱性などを悪用する攻撃活動を観測したことは JPCERT/CC 以外の組織からも報告されており、NICT は文書 (2) を発行して注意を呼びかけています。JPCERT/CC は CyberNewsFlash (3) で観測状況や対策を公表し、2025 年 1 月 2 日に ASUS 社から公開された脆弱性への対応を呼びかけています。

インターネットに接続する機器は、利用者だけでなく攻撃者もアクセスを試みる可能性があります。最新のファームウェアを使用する、適切な認証や強固なパスワードの設定を施す、必要がなければサービスを無効にするなど、注意して運用してください。

## 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) NICT
「ASUS 製 WiFi ルーターの AiCloud 機能の脆弱性を悪用する攻撃に関する注意喚起」
https://blog.nicter.jp/2025/04/asus_aicloud/

(3) JPCERT/CC
「AiCloud が稼働する ASUS 製 WiFi ルーターからの通信の観測」
https://www.jpcert.or.jp/newsflash/2025041701.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［2025 年 1 月 1 日～2025 年 3 月 31 日］
- 2025 年 6 月 6 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/