JPCERT/CC インターネット定点観測レポート

2023 年 10 月 1 日 ～ 2023 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

2024 年 2 月 15 日

JPCERT CC®

目次

1. 概況

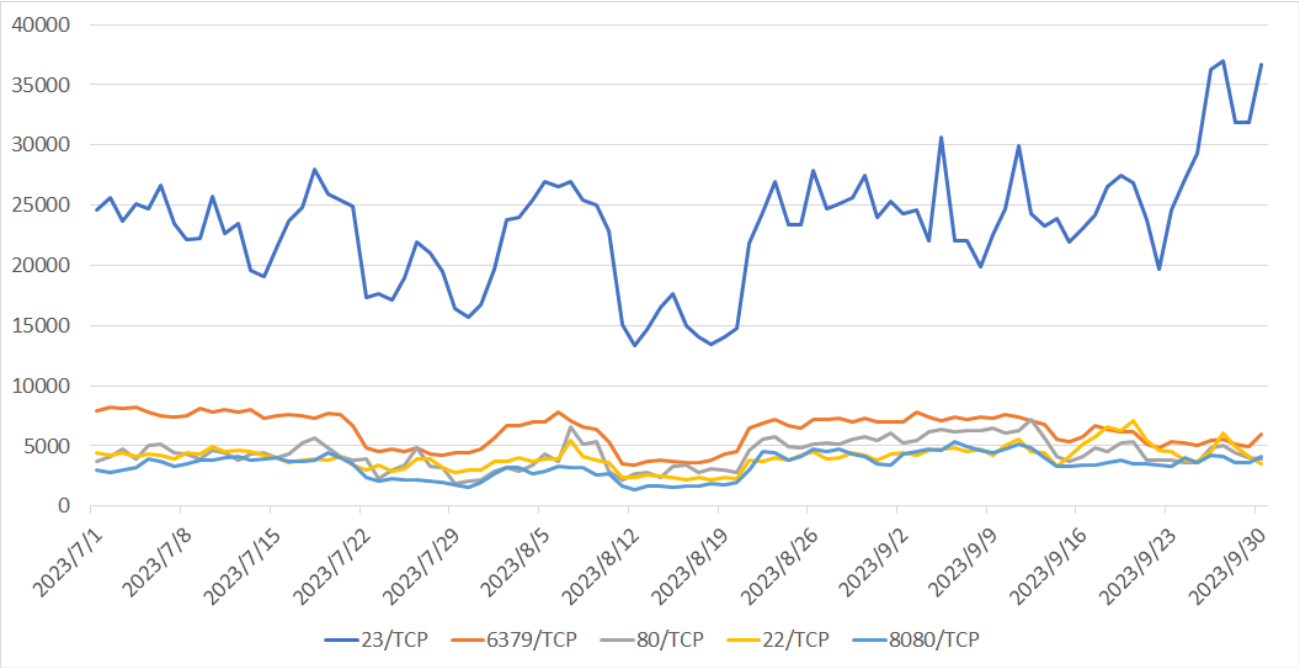
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、 一定の IP アドレス帯に向けて網羅的に発信されるパケットを観測しています。こうしたパケットの発信は特定の機器や特定のサービス機能を探索するために行われていると考えられます。JPCERT/CC では、センサーで観測されたパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。センサーから収集したデータを分析し、問題が見つかれば、解決できる可能性がある関係者に情報を提供し、対処を依頼しています。
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	ssh（22/TCP）	2
3	redis（6379/TCP）	5
4	http-alt（8080/TCP）	3
5	http （80/TCP）	10

※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。



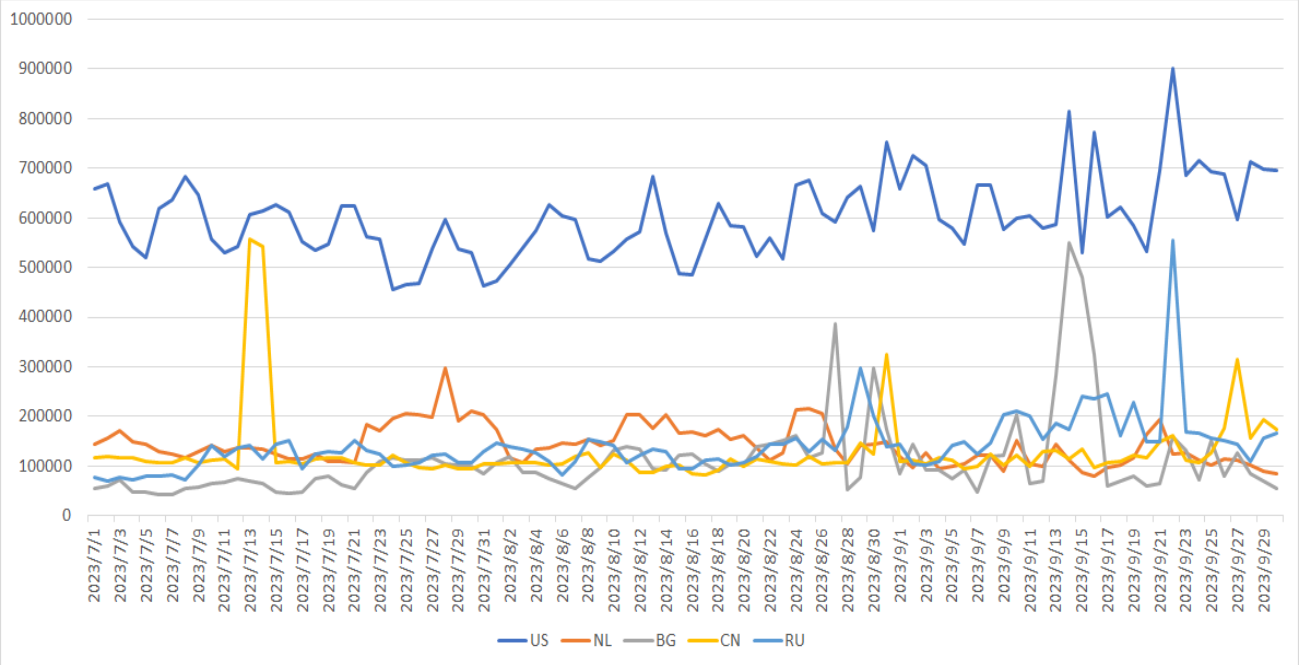
［図 1：2023 年 10～12 月のポート番号宛のパケット観測数トップ 5 の推移］

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。ssh（22/TCP）は 10 月 8 日から 11 月末にかけて探索される頻度が多くなり、3 番目の redis（6379/TCP）と入れ替わって 2 番目になりました。また、11 月下旬頃から http-alt（8080/TCP）と http（80/TCP）の探索頻度の順位が入れ替わり、http-alt 宛の探索数が http より定常的に多くなりました。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	1
2	中国	4
3	ドイツ	6
4	オランダ	2
5	ブルガリア	3

［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。

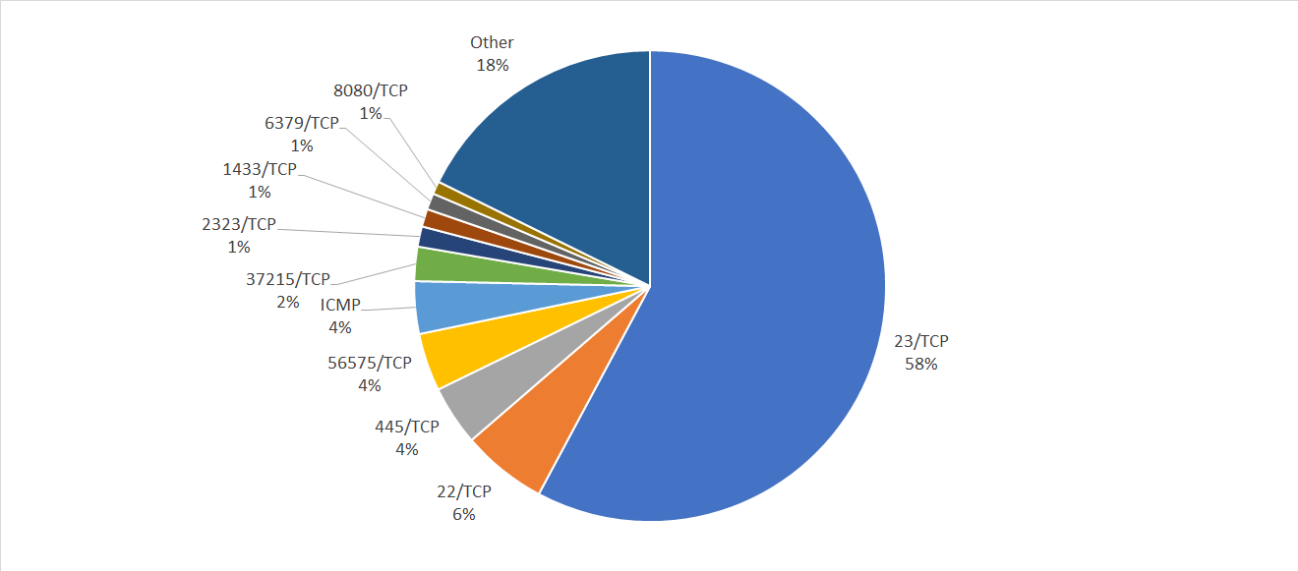


［図 2：2023 年 10～12 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

米国、中国の順位は変わりませんでしたが、10 月中旬から 11 月中旬にかけて頻度が増したドイツが 3 番目になりました。それ以外の地域については特筆すべき点がありません。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。

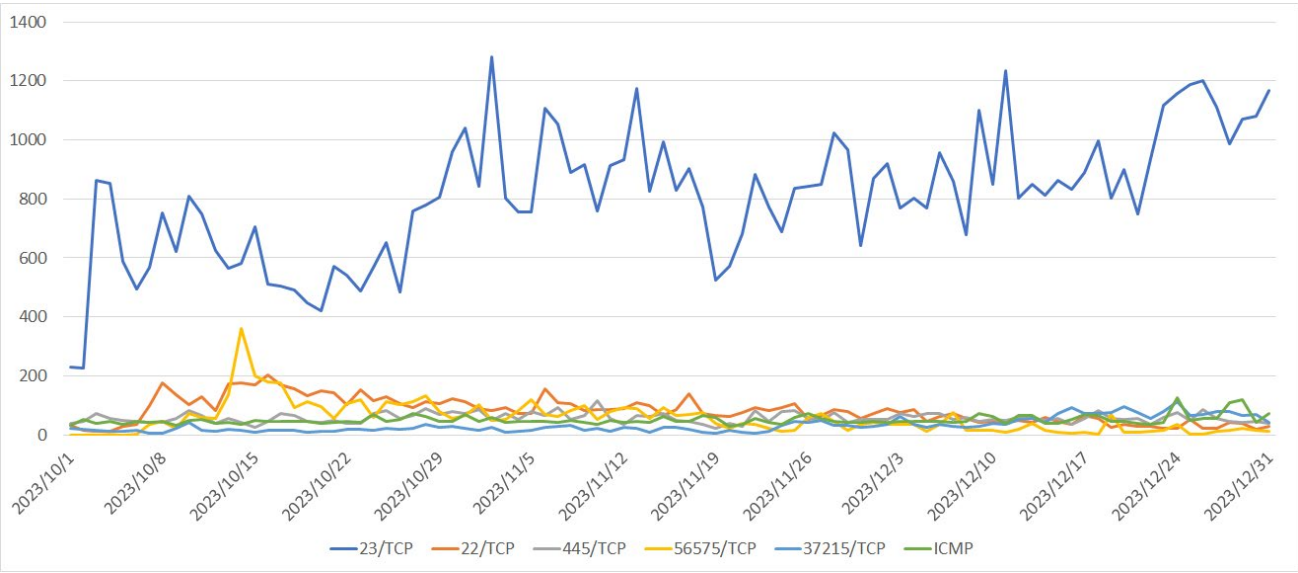
2. 日本国内からの探索パケットの観測状況について

本章では、概況では触れることができなかった国内の傾向について取り上げます。本四半期に国内から探索されたサービスの割合を［図 3］に示します。



［図 3：2023 年 10～12 月の国内から探索されたサービスの割合］

Telnet の探索の頻度が高まり約 6 割を占めました。2 番目の SSH までは表 1 の海外と同じでしたが、それ以降は、3 番目が Microsoft-ds（445/TCP）、4 番目が 56575/TCP、5 番目が 37215/TCP と異なっていました。トップ 5 の推移を［図 4］に示します。



［図 4：2023 年 10～12 月の国内から探索されたポート番号宛のパケット観測数トップ 5 の推移］

Telnet（23/TCP）は期中一定の頻度での探索が行われたのではなく、10 月初旬と比較して 12 月下旬には約 3 倍と変化しました。この探索の一部は NAS や無線 LAN ルーター、DVR などの機器が送信元となっていることが判明しました。一方、探索元が分からなかったものは、http や https 等のポートで動作していない機器、または、マルウェアの負荷等により機器が再起動したため調査時までに IP アドレスが変わり追跡できなかった機器と推測されます。
一方、56575/TCP の探索は 10 月 7 日頃から頻度が高まりました。56575/TCP の探索元が 22/TCP も探索することが多いため、［図 4］の両ポートのグラフに相互に似通った変化が見られました探索元の機器に Web ブラウザーでアクセスして表示されるページを確認し、ほぼすべての DVR が送信元となっていることを確認しました。これらの DVR では、インターネット経由で侵害を受けた結果、何らかのマルウェアが埋め込まれて動作していると推測されます。

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の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

本活動は、経済産業省より委託を受け、「令和 5 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。