JPCERT CC®

JPCERT Coordination Center

JPCERT/CC インターネット定点観測レポート

2024 年 1 月 1 日 ～ 2024 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

2024 年 5 月 2 日

JPCERT CC®

目次

1. 概況

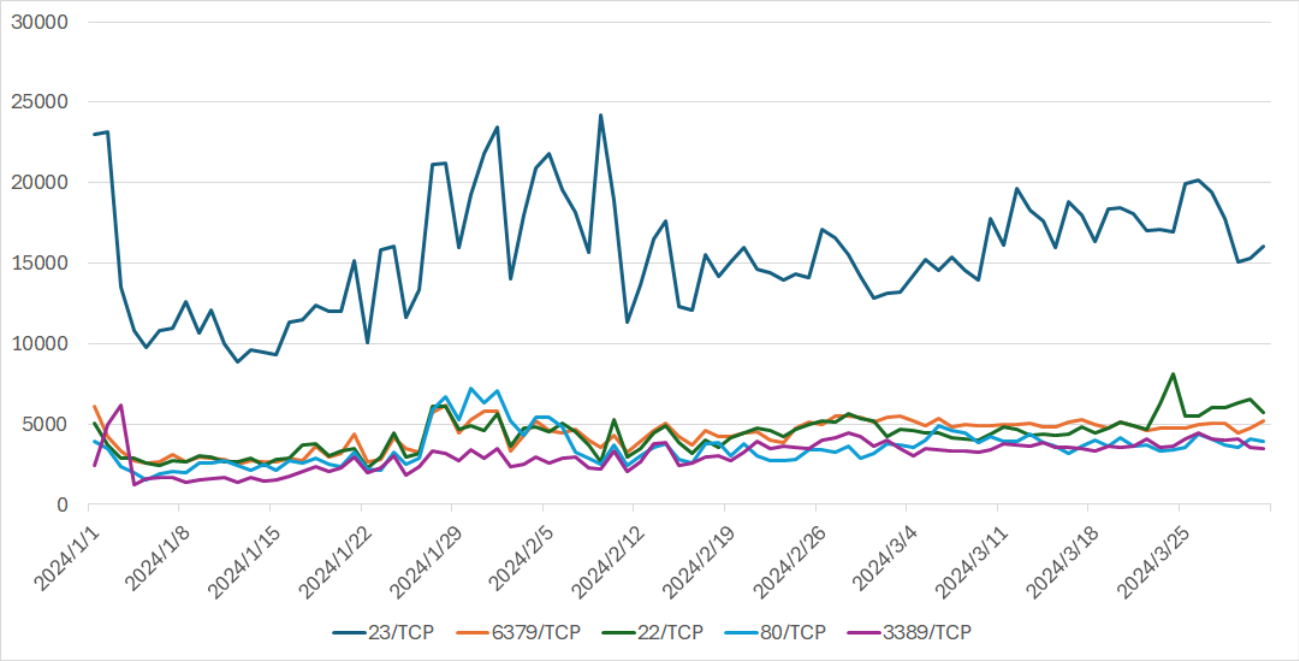
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、 一定の IP アドレス帯に向けて網羅的に発信されるパケットを観測しています。こうしたパケットの発信は特定の機器や特定のサービス機能を探索するために行われていると考えられます。JPCERT/CC では、センサーで観測されたパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。センサーから収集したデータを分析し、問題が見つかれば、解決できる可能性がある関係者に情報を提供し、対処を依頼しています。
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	redis（6379/TCP）	2
3	ssh（22/TCP）	3
4	http（80/TCP）	5
5	rdp （3389/TCP）	7

※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。



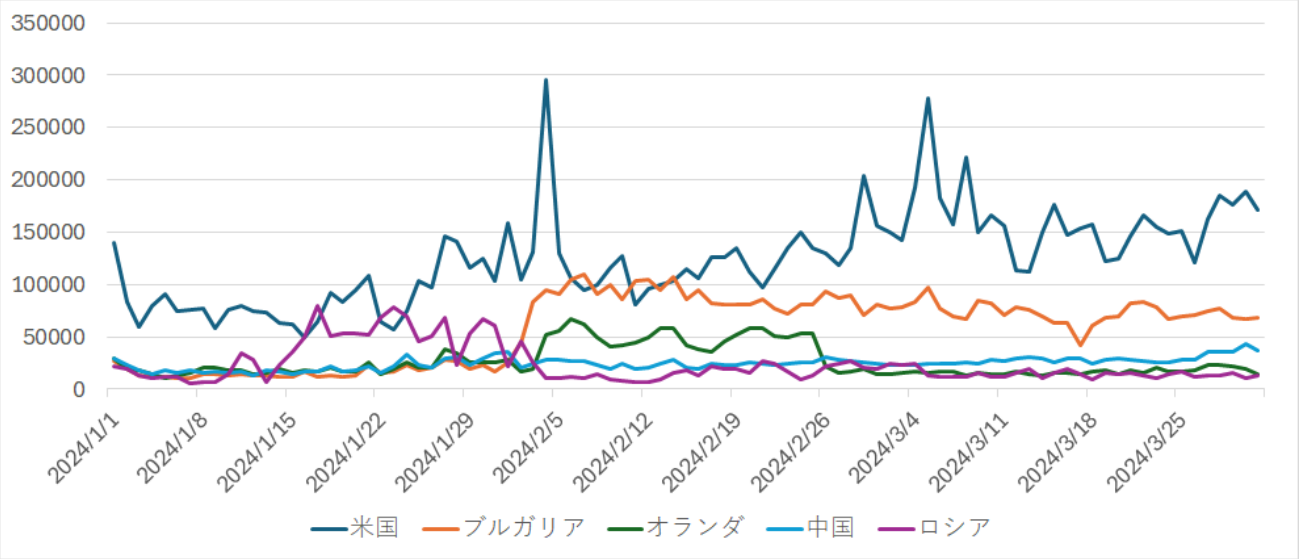
［図 1：2024 年 1～3 月のポート番号宛のパケット観測数トップ 5 の推移］

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、3 番目は変動がありませんでした。4 番目に http（80/TCP）、5 番目に rdp（3389/TCP）が入りました。この順位の変動は、http-alt（8080/TCP）と ICMP の探索が大きく減った影響であり、http と rdp の探索数は前四半期とほぼ同数でした。
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	ブルガリア	5
3	オランダ	4
4	中国	2
5	ロシア	6

［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。

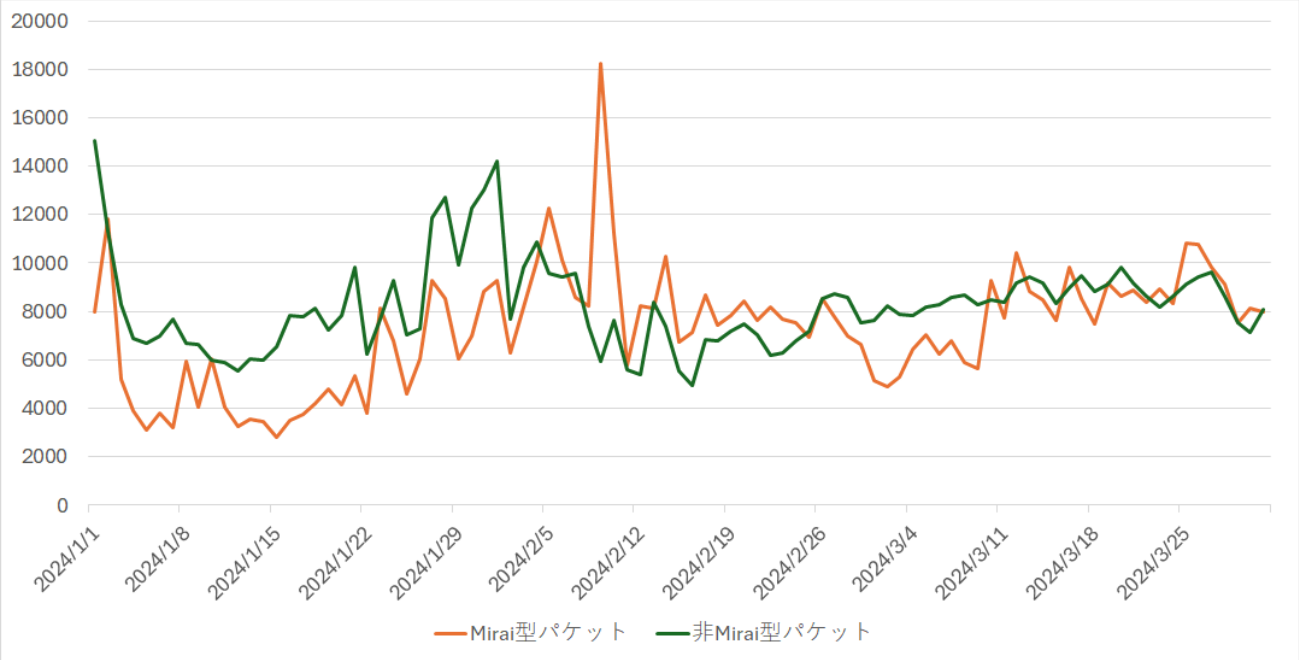


［図 2：2024 年 1～3 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

引き続き米国がトップでした。ブルガリアは 2 月上旬からパケット数が増加したため 2 番目になりました。また、オランダも 2 月上旬から下旬にかけて一時的に増加したため 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。

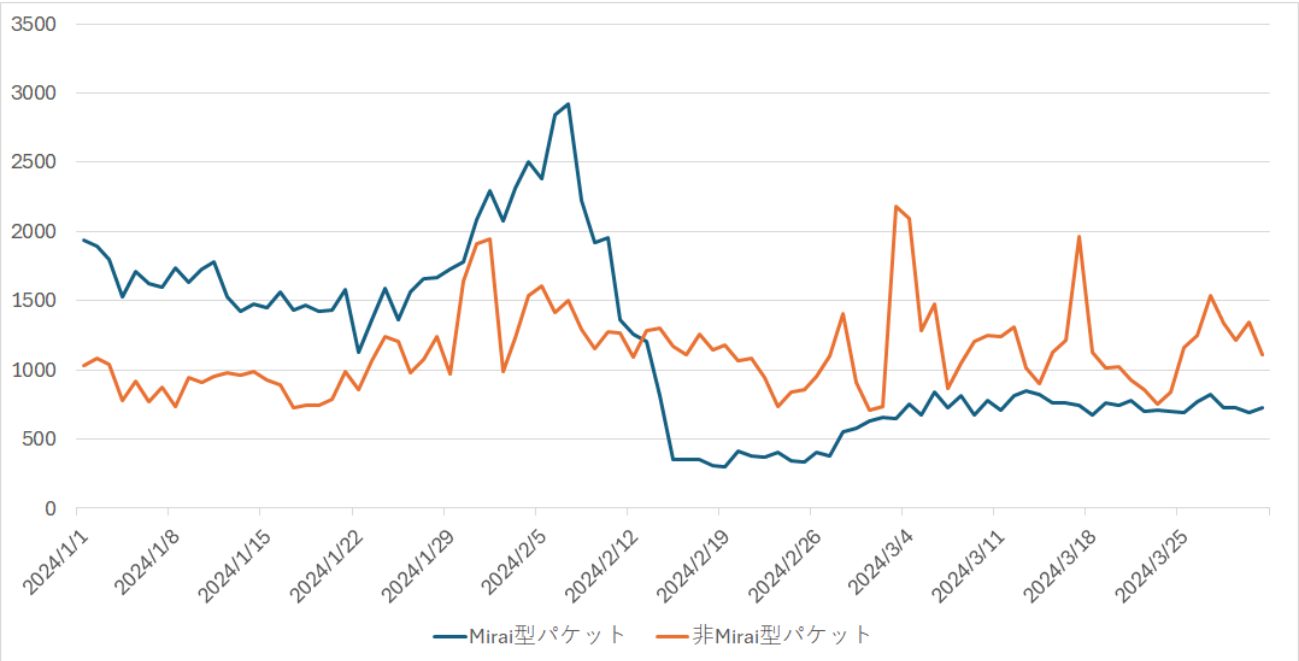
2. 日本国内からの探索パケットの観測状況について

本章では、最近の Telnet に対する探索の動向について取り上げます。Telnet に対する探索パケットの多くが Mirai に由来しています。Mirai に由来する探索パケット（以下、「Mirai 型パケット」という。）かどうかは、「2323/TCP など他のさまざまなサービスを探索する、同じ送信元からのパケットが同時に観測される」と「宛先 IP アドレス＝Sequence Number」の特徴を持っているかどうかで判定できます。最近、Mirai の特徴を持たない Telnet の探索パケット（以下、「非 Mirai 型パケット」という。）が頻繁に見られるようになりました。日本国内のセンサーで観測された Mirai 型パケットと非 Mirai 型パケットの双方について、まずは送信元が海外であるものの観測数を［図 3］に示します。



［図 3：2024 年 1～3 月の Telnet に対する探索の推移（送信元海外）］

Mirai 型パケットと非 Mirai 型パケットとの間で、変化のタイミングに若干のズレがあるものの、いずれも大局的には 1 月初めに一旦減少し、その後、1 月 16 日頃から 2 月の上旬にかけて増えました。3 月末に向けては大きな増減が見られなくなり、両者がほぼ同数となりました。減衰の兆候が見られないことから、どちらの感染活動も海外で続いていると考えられます。
次に国内が送信元となっている探索パケットの推移を［図 4］に示します。



［図 4：2024 年 1～3 月の Telnet に対する探索の推移（送信元国内）］

1 月に入った時点では、Mirai 型パケットが非 Mirai 型の 2 倍ほど観測されていました。2 月に入ってから一週間ほど増え続けた後、2 月末にかけて急減してから少し持ち直し、その後はほぼ一定の探索が続いています。
Mirai 型パケットと非 Mirai 型パケットの送信元を調査すると、時期によって製品に違いがありましたが、ルーターや DVR 等の IoT 製品であることが分かりました。Mirai とは異なるマルウェアが存在し、ボットネットを形成する活動が活性化していて、日本国内においては Mirai とは異なるマルウェアの感染活動が活発になっており、独自のボットネットを新たに形成しつつあると推測しています。

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。