JPCERT Coordination Center

JPCERT/CC インターネット定点観測レポート

2023 年 1 月 1 日 ～ 2023 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

2023 年 4 月 27 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、不特定多数に向けて発信される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、解決を行うことができる適切な関係者に情報を提供し、善処を依頼しています。

本レポートでは、TSUBAME（インターネット定点観測システム）で本四半期に観測されたパケットを中心に分析した結果について述べます。

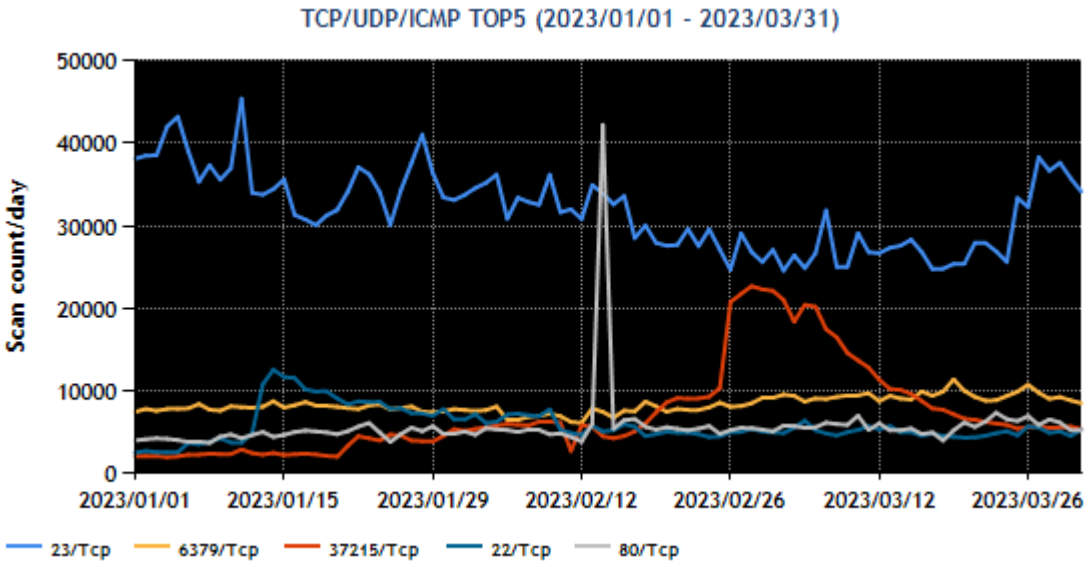
本四半期に国内で観測されたパケットの宛先ポート番号をパケットが多かった順に並べた時のトップ 5 は［表 1］に示すとおりでした。

［表 1：宛先ポート番号トップ 5］

順位	宛先ポート番号	前四半期の順位
1	23/TCP（telnet）	1
2	6379/TCP（redis）	2
3	37215/TCP	7
4	22/TCP（ssh）	4
5	80/TCP（Microsoft-ds）	5

※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］に示した各宛先ポート番号を持つパケット観測数の推移を［図 1］に示します。



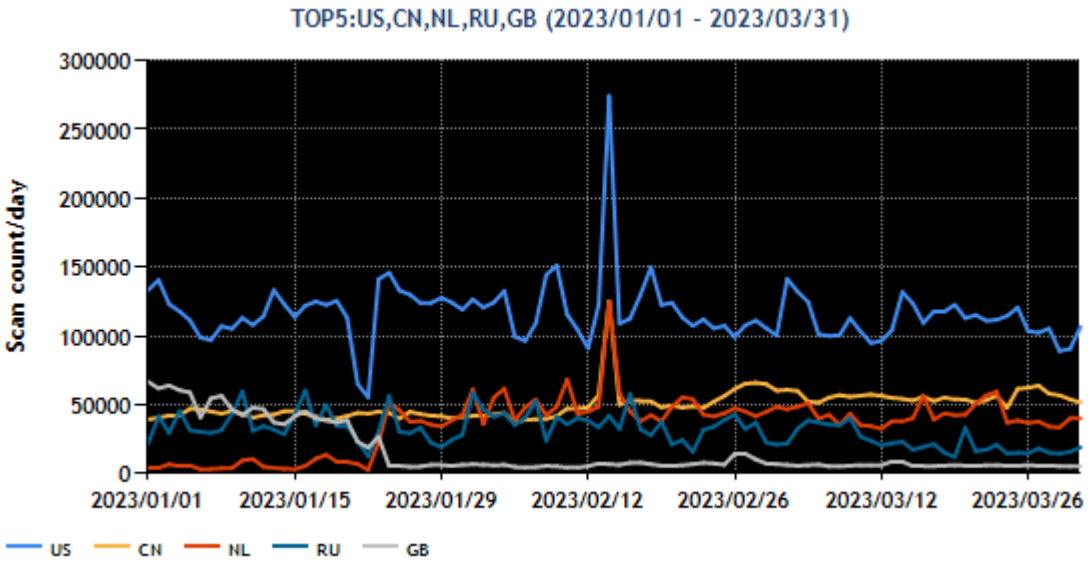
［図 1：2023 年 1～3 月のポート番号宛のパケット観測数トップ 5 の推移］

最も多く観測されたパケットは 23/TCP（telnet）宛で、期間中に増減を繰り返していました。6379/TCP 宛のパケットは本四半期を通じて微増傾向が続きました。37215/TCP 宛のパケットが、1 月 18 日頃から微増傾向 (2) が続いた後に、2 月 26 日頃からの約 10 日間には一段と増えて、順位も 3 番目に上がりました。パケットの送信元には日本国内の IP アドレスも含まれていました。この現象については「2.1. さまざまな地域を送信元とする 37215/TCP 宛のパケットの推移について」で取り上げます。次に、本四半期に国内で観測されたパケットについて、送信元 IP アドレスを地域ごとにまとめてパケットが多かった順に並べたトップ 5 を［表 2］に示します。

［表 2：送信元地域トップ 5］

順位	送信元地域	前四半期の順位
1	米国	1
2	中国	4
3	オランダ	TOP5 外
4	ロシア	2
5	英国	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。



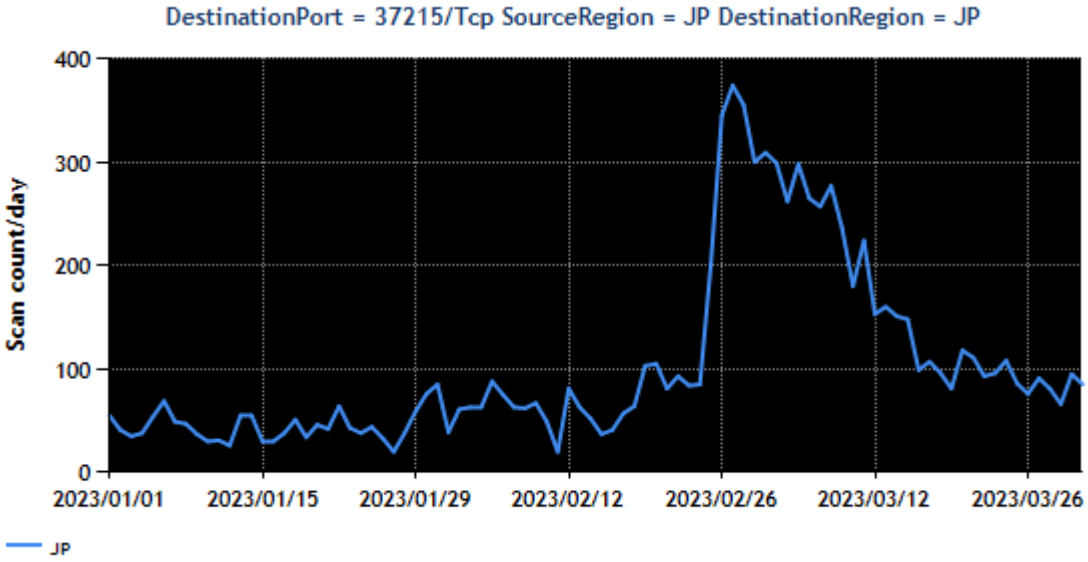
［図 2：2023 年 1～3 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

米国からのパケットが期間を通して一番多く観測されました。中国からのパケットの観測数は、期間中に徐々に増えて、期初と比べて期末には（10 日間平均で）約 1.5 倍となりました。1 月 23 日頃を境として、英国とオランダを送信元とするパケット観測数に変化がありました(オランダが 10 日平均で約 8 倍)。これは、従来英国に割り当てられていた IP アドレス帯がオランダに割り当てられた影響と考えています。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. 注目された現象

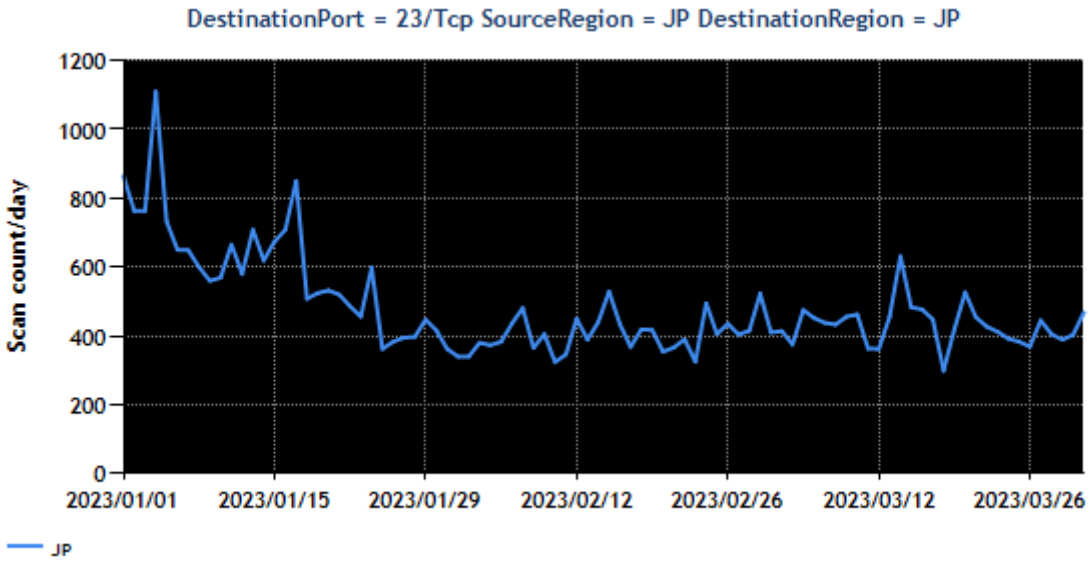
2.1. さまざまな地域を送信元とする 37215/TCP 宛のパケットの推移について

日本を送信元とする Mirai の特徴 （Initial Sequence Number と Destination IP address とが一致する；以下、Mirai 型パケットという）を持つ 37215/TCP 宛のパケットが 2 月中旬頃から 3 月中旬頃にかけて増加しました。2 月 19 日から 21 日に一時的な増加 [3] [4] がありました。2 月 25 日頃から再び増加に転じ、2 月 28 日には増加前の 2 月 18 日までの 10 日平均と比較して約 6 倍に達した後、3 月 18 日頃にかけてゆるやかに減少しました。（図 3）



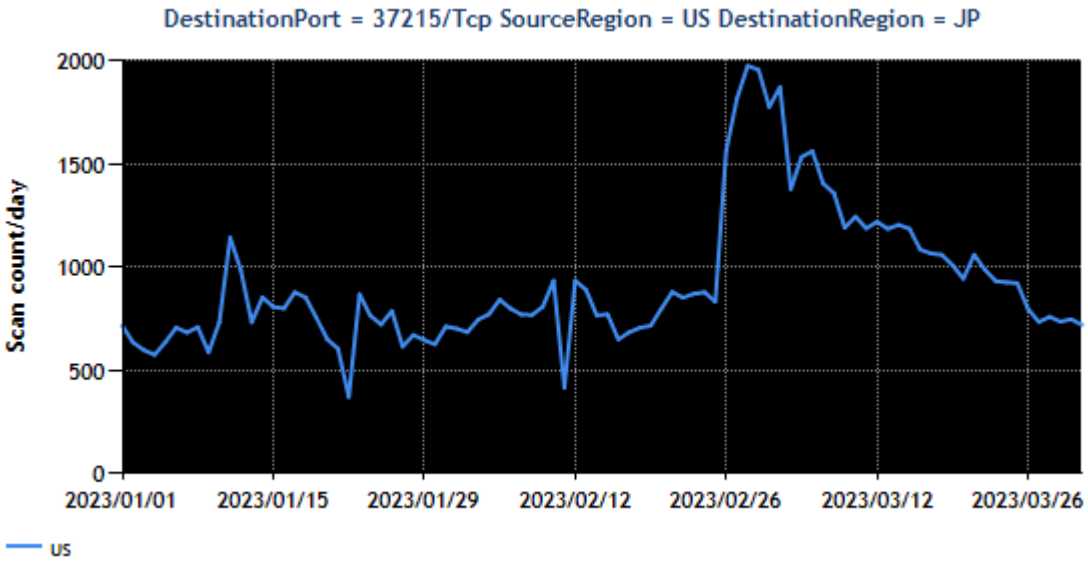
［図 3：日本を送信元とする 37215/TCP 宛のパケットの推移］

これらのパケットの送信元は 37215/TCP 宛だけでなく 23/TCP（telnet）宛のパケットも送信していました。図 4 に日本を送信元とする 23/TCP 宛のパケットの推移を示します。図 3 に示した増減と相関するような特徴的な変化を見出すことはできませんでした。

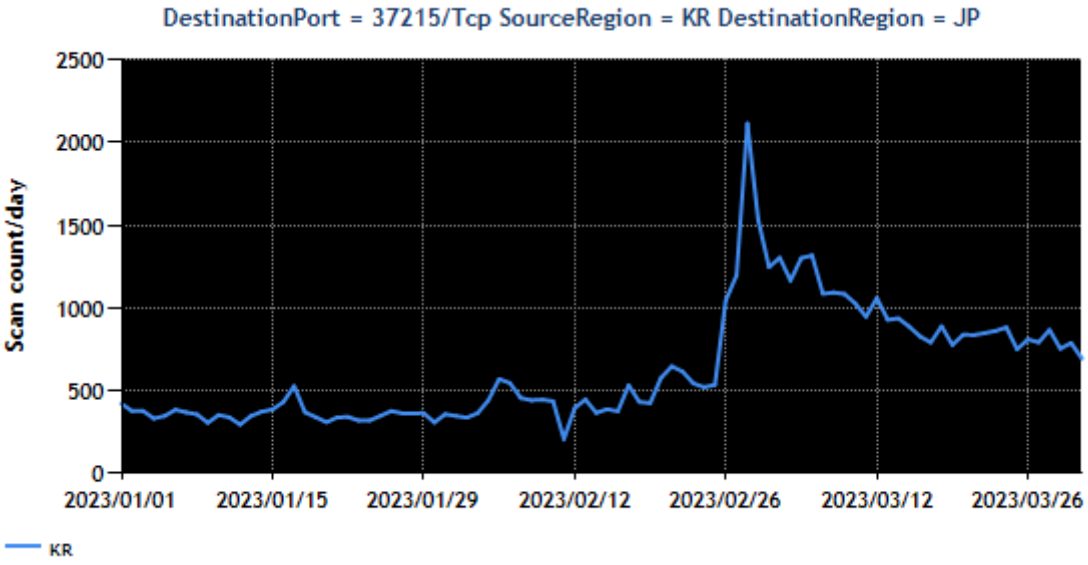


［図 4：日本を送信元とする 23/TCP 宛のパケットの推移］

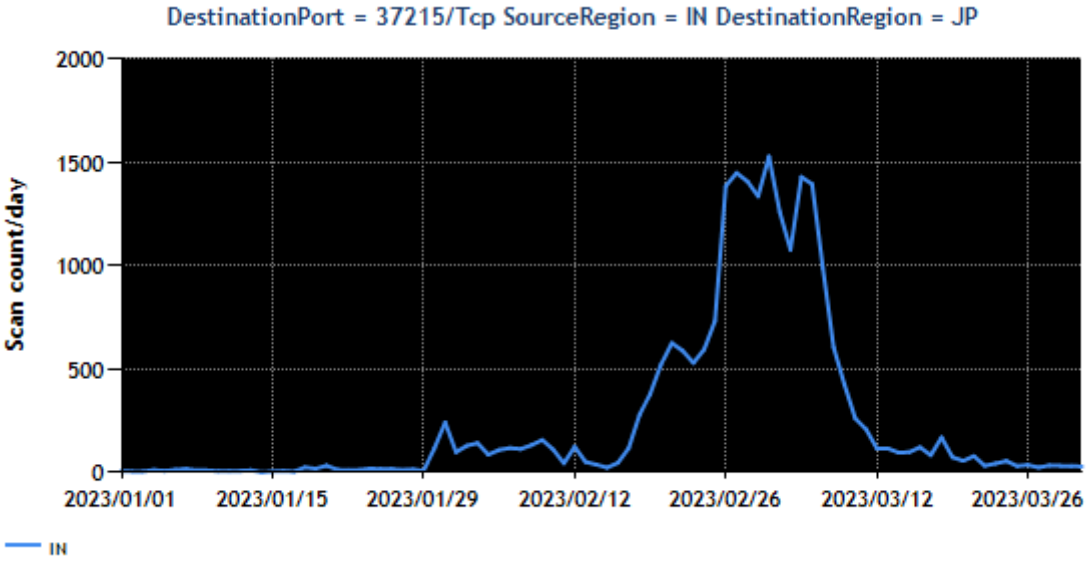
さまざまな地域から送信された 37215/TCP 宛のパケットで一時的な増加の現象が観測されました。一部地域について増加の様子を図 5 から図 11 に示します。



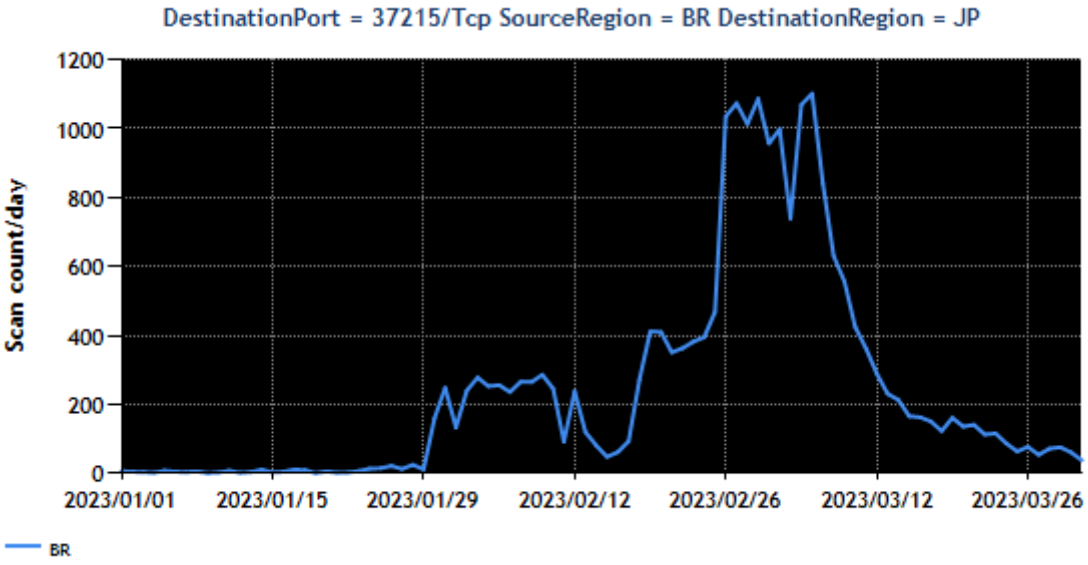
［図 5：米国を送信元とする 37215/TCP 宛のパケットの推移］



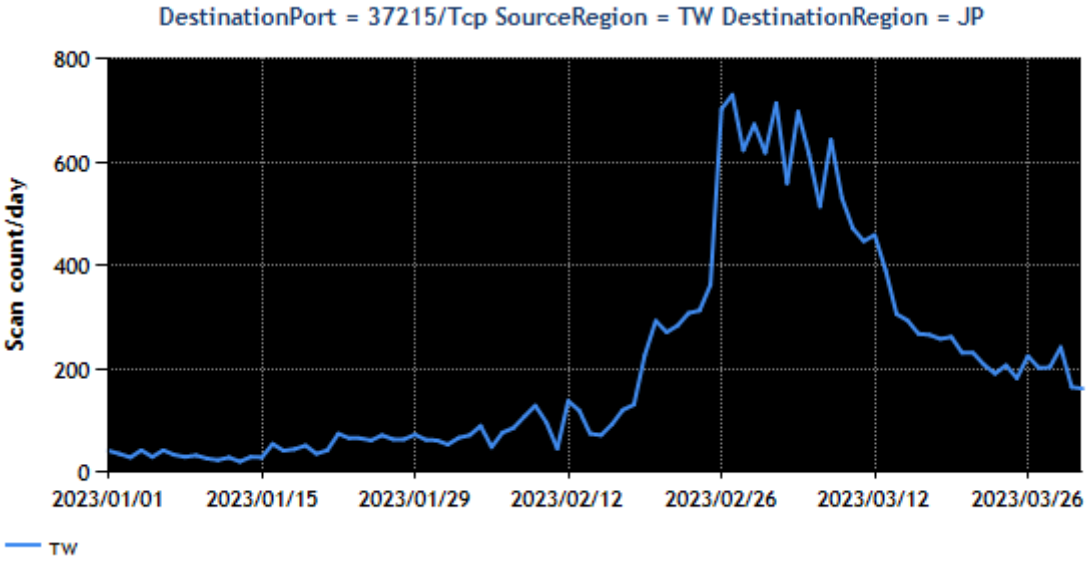
［図 6：韓国を送信元とする 37215/TCP 宛のパケットの推移］



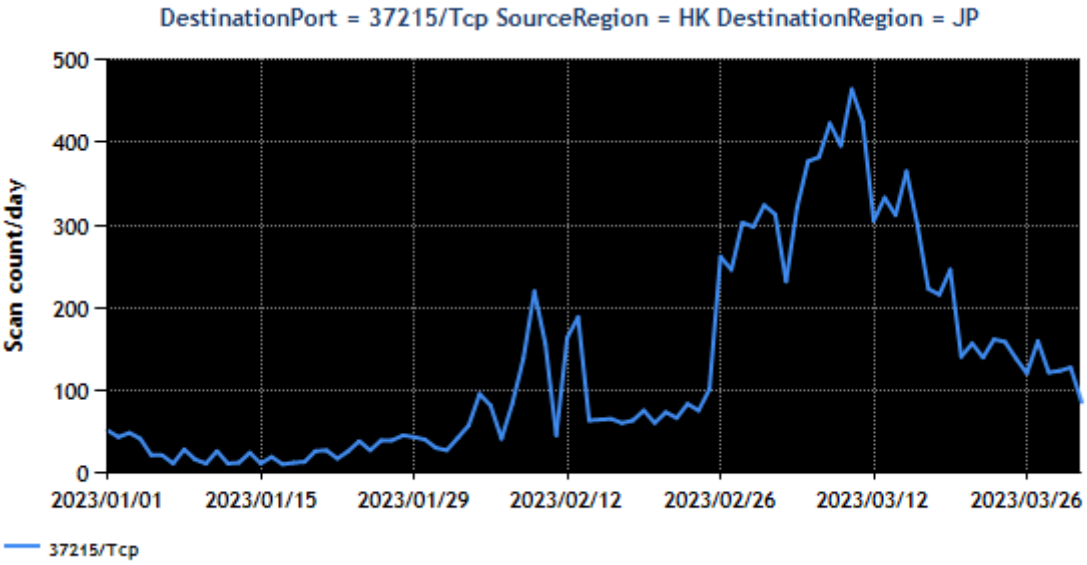
［図 7：インドを送信元とする 37215/TCP 宛のパケットの推移］



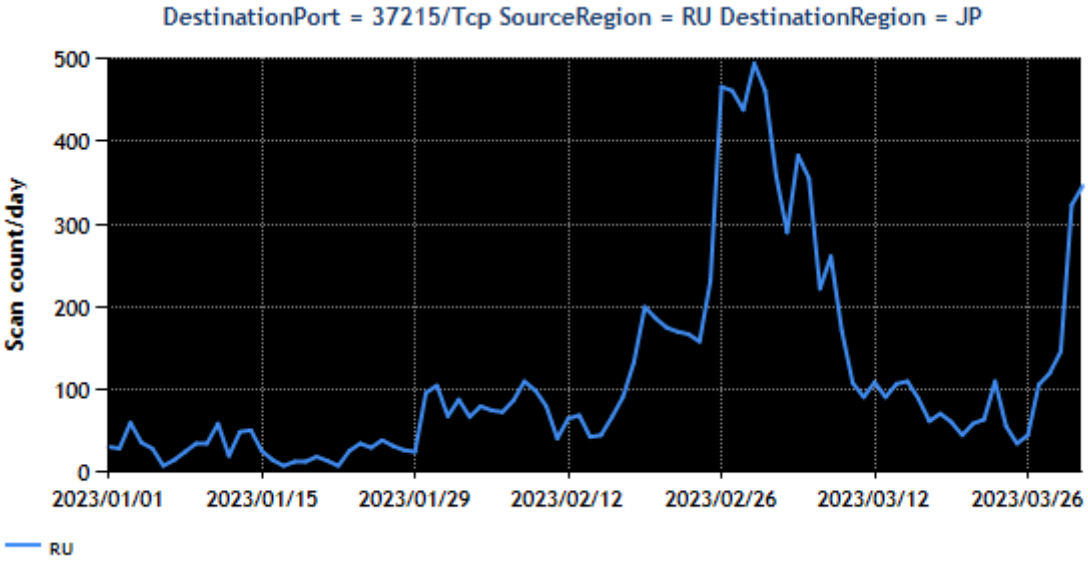
［図 8：ブラジルを送信元とする 37215/TCP 宛のパケットの推移］



［図 9：台湾を送信元とする 37215/TCP 宛のパケットの推移］



［図 10：香港を送信元とする 37215/TCP 宛のパケットの推移］



［図 11：ロシアを送信元とする 37215/TCP 宛のパケットの推移］

これらの地域以外からも、時期は異なるものの一時的な増加が見られました。図 1 の 37215/TCP の変化はこれらの一時的な増減が重なり合ったものと考えられます。

3. 参考文献

(1) Service Name and Transport Protocol Port Number Registry
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

(2) NICTER 解析チーム @nicter_jp
https://twitter.com/nicter_jp/status/1633309683778994181

(3) NICTER 解析チーム @nicter_jp
https://twitter.com/nicter_jp/status/1633310985074397184

(4) NICTER 解析チーム @nicter_jp
https://twitter.com/nicter_jp/status/1645981342499475457

本活動は、経済産業省より委託を受け、「令和 4 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。