JPCERT/CC インターネット定点観測レポート

2022 年 4 月 1 日 ～ 2022 年 6 月 30 日

一般社団法人 JPCERT コーディネーションセンター

2022 年 7 月 28 日

目次

1. 概況

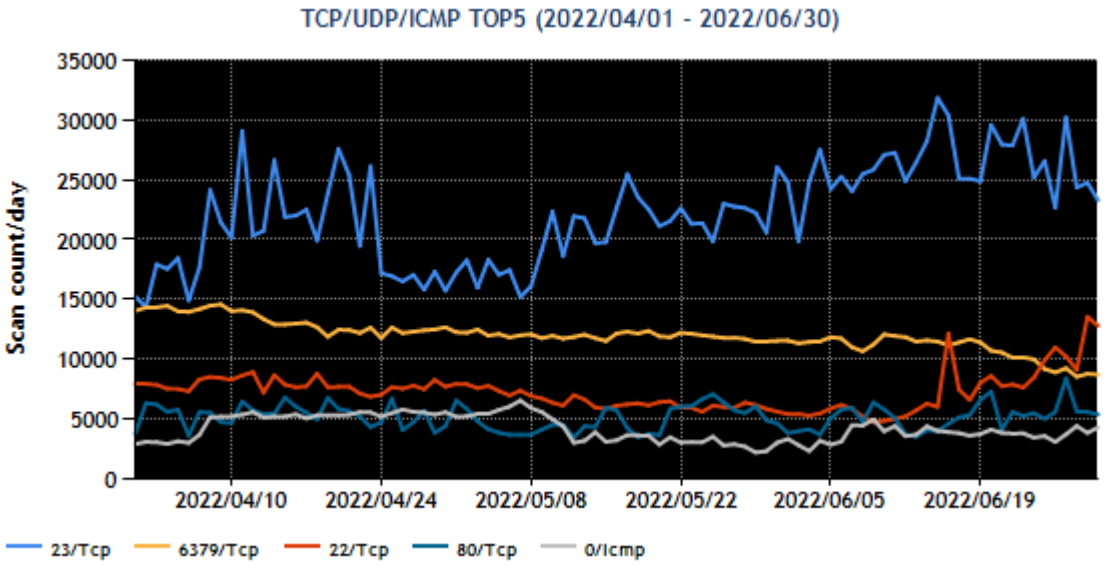
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点からの多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し、観測網に参加してもらう活動を行っています。
各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT などに情報を提供し、状況の改善を依頼しています。また、日本国内固有の問題については、JPCERT/CC の日々の活動の中で対処しています。
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）	2
2	6379/TCP（redis）	1
3	22/TCP（ssh）	4
4	80/TCP (http)	6
5	Icmp	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 1：2022 年 4～6 月のポート番号宛のパケット観測数トップ 5 の推移］

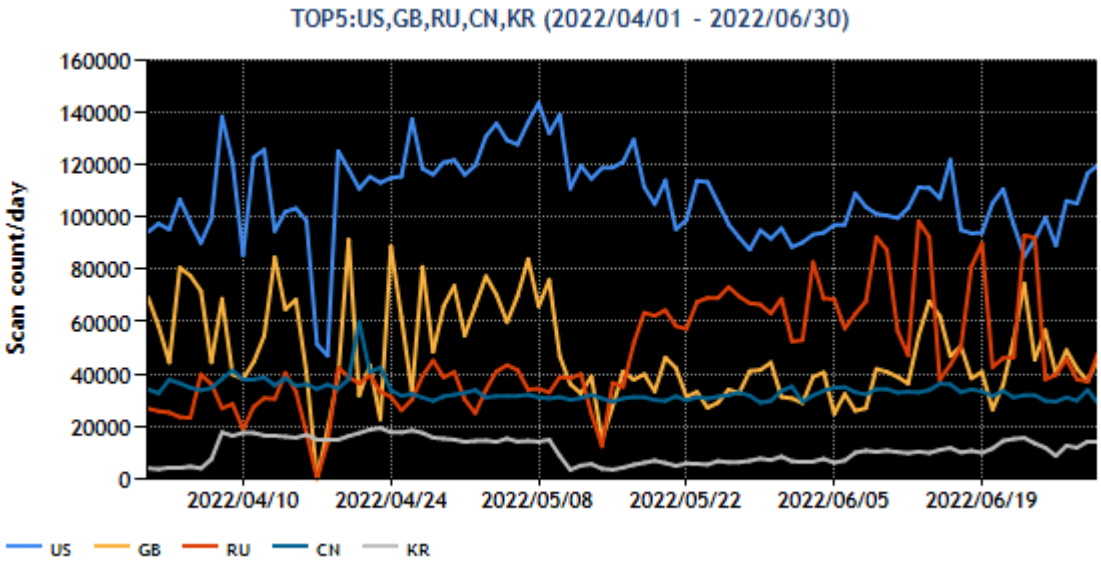
最も多く観測されたパケットは、23/TCP（telnet）宛の通信でした。4 月から 5 月にかけて短期間での増減が何度も発生していました。5 月 8 日頃からは、短期的な増減を繰り返しながらも、7 日間平均でみたパケット数の増加が続きました。一方、6379/TCP 宛のパケットは本四半期において緩やかに減少しているように見えます。

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	英国	2
3	ロシア	4
4	中国	3
5	韓国	6

［表 2］の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。



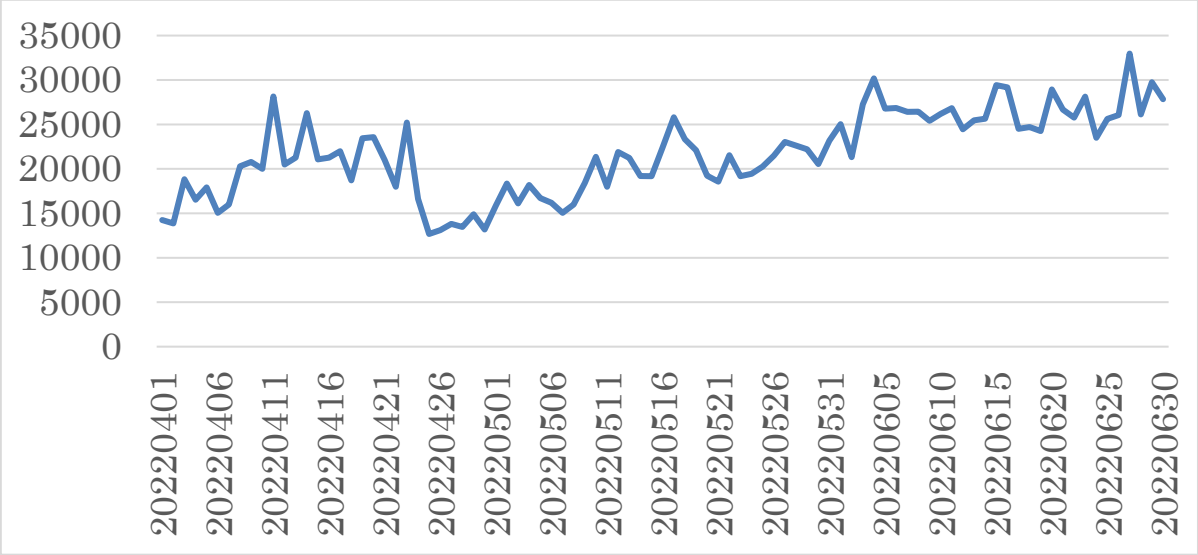
［図 2：2022 年 4～6 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

ロシアからのパケットが 5 月 18 日ごろより増加し中国と順位が入れ替わりました。また、韓国からのパケットが 4 月～5 月 6 日頃にかけて一時的に増加しました。その後いったん減少したものの 6 月下旬にかけて少しずつ増加し、通期では 5 番目になりました。

2. 注目された現象

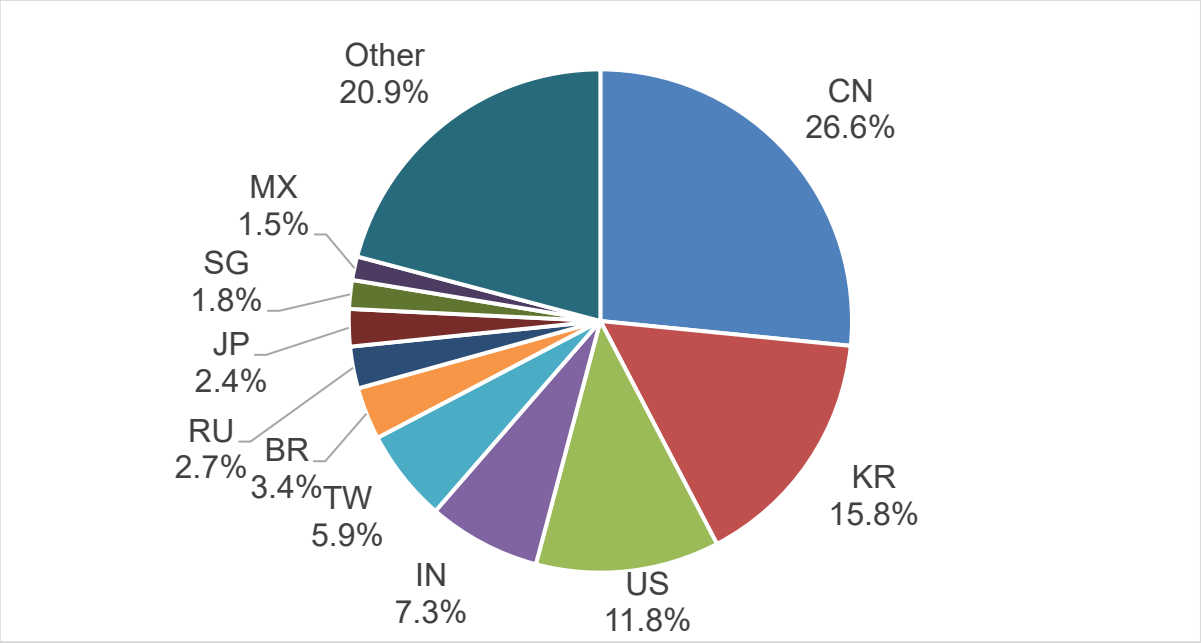
2.1. IoT 機器から送信されたとみられる Mirai の特徴をもつパケットの増加について

4 月頭から 25 日頃にかけて Mirai の特徴 （Initial Sequence Number = Destination IP address）をもつパケット（以下、Mirai 型パケット）が一時的に増加しました、その後 5 月 8 日から 6 月末にかけてパケット数の漸増を観測しています。［図 3］



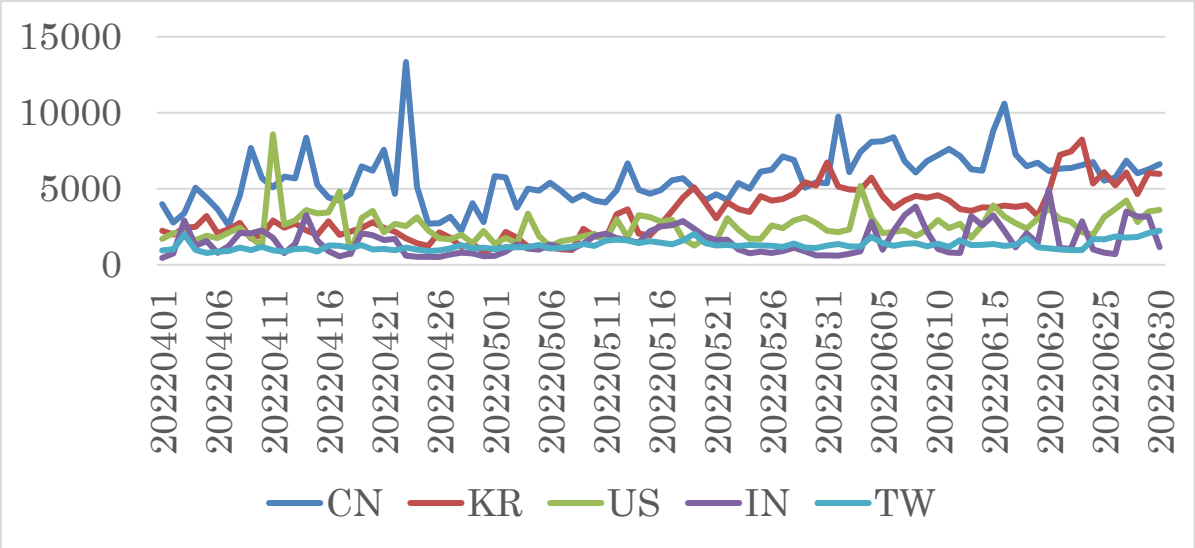
［図 3：Mirai 型のパケット数の推移］

本四半期中の Mirai 型パケットの送信元の地域別に集計したものを［図 4］に示します。



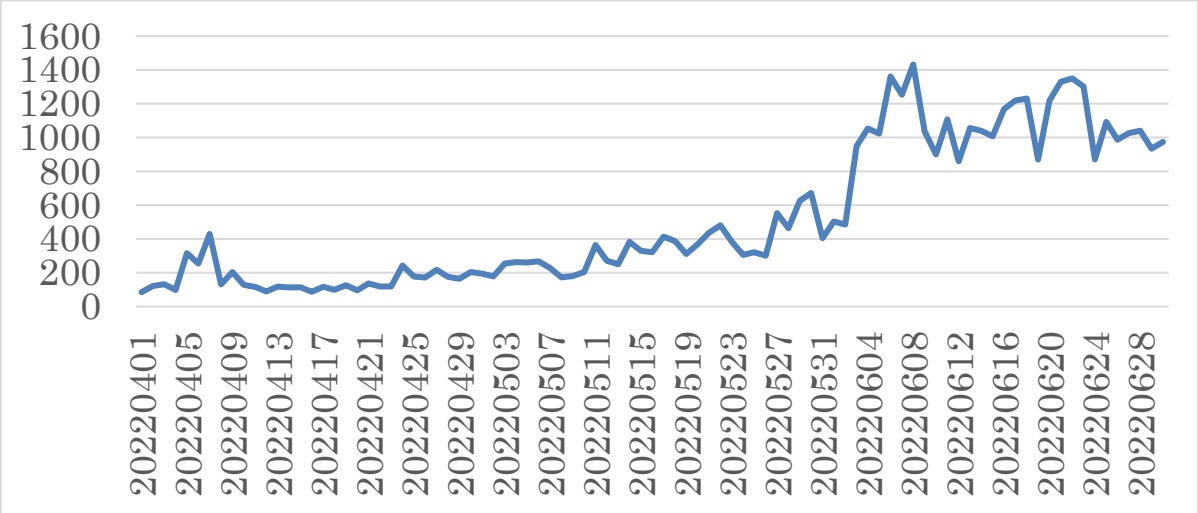
［図 4：Mirai 型のパケットの送信元アドレスの延べ数の割合］

Mirai 型パケットの送信元アドレスと観測された全パケットの送信元アドレスの延べ数を地域ごとに積算して比較すると、中国米国や韓国などともに上位になる地域がある一方で、後者だけが目立つインドや台湾等の地域もありました。日本は、前者では 8 番目、後者では 19 番目にランクされました。
Mirai 型パケットの観測数の日ごとの推移を送信元地域ごとに示したのが［図 5］です。地域ごとに増減のタイミングが異なっています。いくつか例をあげると、中国は 4 月頭から 25 日にかけて多くのパケットを観測しました。その後 5 月から 6 月中旬にかけて緩やかにパケット数が増加しています。韓国は 4 月の増減の幅はそれほど多くありませんでしたが、5 月 11 日頃から急激に増加しており 4 月頭と比較して 2 倍以上になりました。台湾は 6 月 26 日頃から大きく増加しました。



［図 5：送信元地域別のパケット数の推移（TOP5)］

次に送信元地域が日本となっている Mirai 型のパケットの動向を［図 6］に示します。



［図 6：送信元地域別のパケット数の推移（日本)］

4 月上旬に一時的な増加があった後は落ち着いていましたが、4 月 25 日頃から増加傾向 [2] がみられました。特に 6 月に入ってからは急激に増加 [3] し、4 月初頭と比較して約 5 倍のパケットを観測しました。これらのパケットの送信元上位 TOP5 の地域と日本について、送信元のノードに関する情報を SHODAN 等によって調べてみました。日本、韓国、台湾の送信元 IP アドレスについては防犯用カメラ映像記録装置が稼働しているとみられる IP アドレスが約 6 割含まれていることがわかりました。中国や米国は、大半が何らかの侵害をうけている Linux サーバなどで、防犯用カメラ映像記録装置の割合は多くありませんでした。

現時点では防犯用カメラ映像記録装置に対しどういった攻撃が行われた結果、マルウェアに感染しパケットを送ってきているのかについては複数のシナリオが推測されますが、いずれとも断定できておりません。

日本国内においては、Mirai の特徴を持つパケットの送信元となっている IP アドレスの管理者に対して情報提供を行うことで、機種や攻撃の流れなどに関する情報の入手を試みています。

また、発見された防犯用カメラ映像記録装置の販売や設置をしている日本国内の事業者に製品の利用に関するセキュリティ向上を目指し関係する団体との情報交換等を進めています。

これから新規に設置される機器については、公益社団法人日本防犯設備協会が防犯機器に必要とされる機器と性能の基準を策定し適合した RBSS（優良防犯機器認定制度）[4] 認定の防犯用カメラ映像記録装置等を使用することや、機器の初期パスワードの変更、ファームウェアの更新、アクセス制限などにも注意を払って運用してください。

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 Twitter 2022 年 7 月 8 日
https://twitter.com/nicter_jp/status/1545264938306146306

（3）NICTER 解析チーム Twitter 2022 年 6 月 9 日
https://twitter.com/nicter_jp/status/1534722508729229312

（4）日本防犯設備協会
https://www.ssaj.or.jp/rbss/index.html

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。