JPCERT/CC インターネット定点観測レポート

2022 年 7 月 1 日 ～ 2022 年 9 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 10 月 26 日

JPCERT CC®

目次

1. 概況

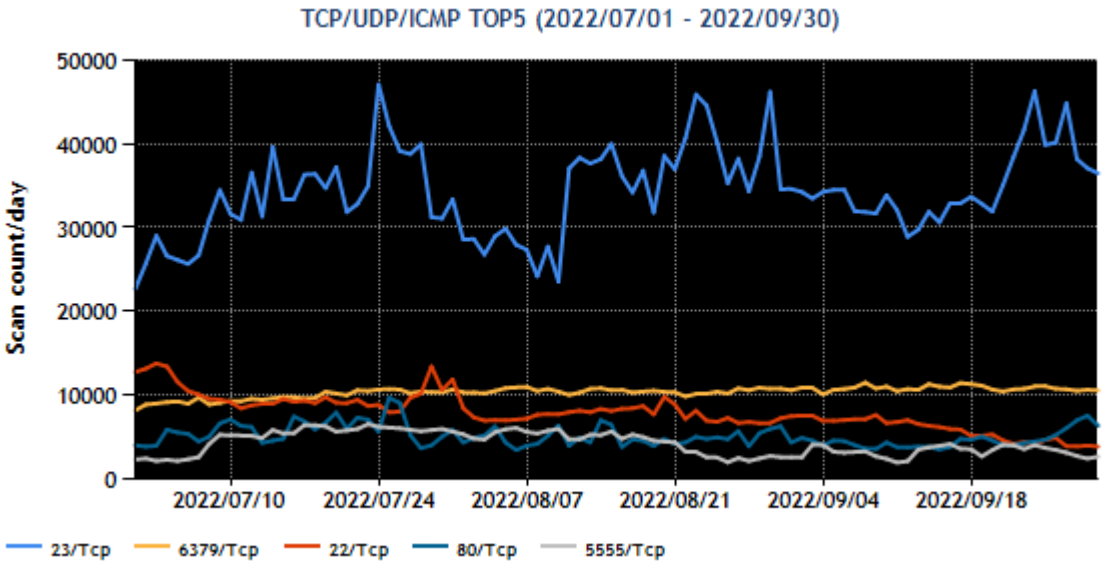
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点からの多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し、観測網に参加してもらう活動を行っています。
各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT などに情報を提供し、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）	1
2	6379/TCP（redis）	2
3	22/TCP（ssh）	3
4	80/TCP （http)	4
5	5555/TCP	8

※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。



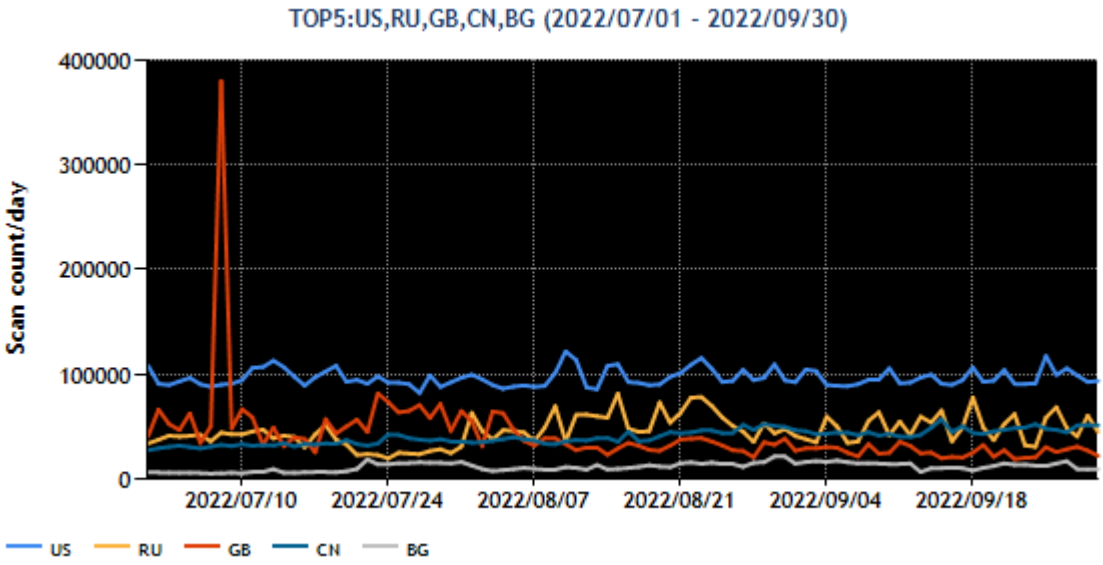
［図 1：2022 年 7～9 月のポート番号宛のパケット観測数トップ 5 の推移］

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し続けました。
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	ロシア	3
3	英国	2
4	中国	4
5	ブルガリア	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。



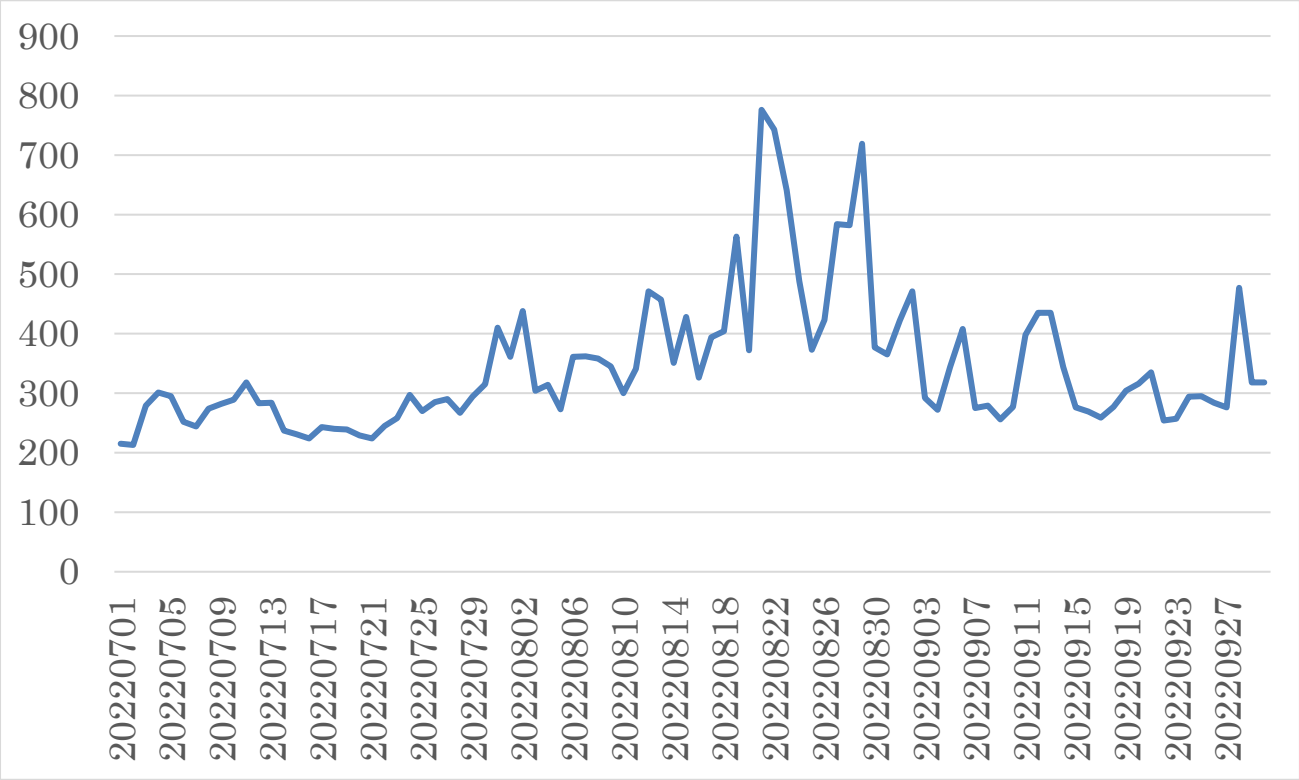
［図 2：2022 年 7～9 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

ロシアからのパケットが 8 月初めより増加し中国と順位が入れ替わりました。8 月 7 日頃から韓国からのパケットが減少しブルガリアと順位が入れ替わったため韓国は 6 番目になり、変動の少なかったブルガリアが 5 番目になりました。

2. 注目された現象

2.1. 跳ね返りパケットの観測状況について

DDoS 攻撃を受けた際にみられる SYN と ACK フラグがセットされたものや、ACK と RST フラグ等がセットされたパケット（以下、跳ね返りパケット）の観測状況を［図 3］に示します。
こうした跳ね返りパケットは、DDoS 攻撃の手法の一つである Syn flood 攻撃に際し観測されます。このタイプの DDoS 攻撃では、SYN フラグをセットし、送信元アドレスをランダムに設定した攻撃用パケットが攻撃対象のサーバーに送られます。当該サーバーは SYN、ACK フラグをセットした応答パケットを送り返しますが、ランダムに設定された攻撃用パケット中の送信元の中にたまたま TSUMANE センサーの IP アドレスに一致したものがあったために、こうした応答パケットが観測されたと推測しています。



［図 3：跳ね返りパケットの特徴を持つパケットを送信した IP アドレス数の推移］

過去の定点観測レポートでは、「ウクライナを送信元地域とした跳ね返りパケット数の増加」として取り上げましたが、本四半期も特徴的な事象がありましたので、紹介したいと思います。

1. 日本からの 9 月 6 日頃の跳ね返りパケットについて
2. 台湾からの 8 月上旬頃の跳ね返りパケットについて

期間中の日本を送信元とした跳ね返りパケットの観測状況を表し、送信元組織が推定できたものが［表 3］です。9 月 6 日頃に跳ね返りパケットの送信元 IP アドレス数が一時的に増加しています。

［表 3：日本からの跳ね返りパケットの観測状況］

***送信元 IP アドレス：アドレスを保有する組織が提供するサービスを書き添えています**

送信元IPアドレス*											
	クラウド事業者A		○								
	政府系サイトA						○				
	ポータルサイトA						○				
	ポータルサイトB						○				
	ポータルサイトC						○				
	ポータルサイトD						○				
	ポータルサイトE						○				
	ポータルサイトF						○				
	ポータルサイトG						○				
	総合ショッピングモールA						○				
	動画配信サービスA						○	○			
	電力会社A							○			
	インターネットメディア事業A								○		
	インターネットメディア事業B								○		
		2022-09-01	2022-09-02	2022-09-03	2022-09-04	2022-09-05	2022-09-06	2022-09-07	2022-09-08	2022-09-09	2022-09-10

これらのパケットの送信元には、大手 EC サイト、大手ポータルサイト、インターネットメディアサイト、動画サービスサイト、重要インフラ事業者のサイト、政府系サイト等が含まれていました。ほぼすべてパケットの送信元ポート番号は 443/TCP となっており HTTPS が使用するポート宛の syn flood 攻撃が行われていたと考えられます。

同様のパケットは 8 月初頭に台湾で使用されている IP アドレスからも受信しました。期間中の日本を送信元とした跳ね返りパケットの観測状況を表し、送信元組織が推定できたものが［表 4］です。

［表 4：台湾からの跳ね返りパケットの観測状況］

***送信元 IP アドレス：アドレスを保有する組織が提供するサービスを書き添えています**

送信元IPアドレス*										
	CDN(政府・金融)A		○							
	CDN(政府・金融)B		○							
	通信事業者A		○							
	ECサイトA				○					
	政府系サイトA					○				
	CDN(政府・金融)C						○			
	セキュリティベンダーA							○		
	金融（銀行）A									○
	ECサイトB									○
	金融（保険）A									○
	情報通信A									○
	電力会社A									○
	金融（銀行）B									○
	金融（銀行）C									○
	金融（銀行）D									○
	金融（銀行）E									○
	金融（銀行）F									○
	金融（銀行）G									○
		2022-08-01	2022-08-02	2022-08-03	2022-08-04	2022-08-05	2022-08-06	2022-08-07	2022-08-08	2022-08-09	2022-08-10

送信元には、複数の金融機関や生命保険会社、CDN を使用している政府系サイトが含まれていました。送信元ポート番号は 443/TCP となっており、同様に HTTPS が使用するポート宛の syn flood 攻撃が行われていたと考えられます。

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

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。