JPCERT Coordination Center

JPCERT/CC インターネット定点観測レポート

2020 年 10 月 1 日 ～ 2020 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

2021 年 2 月 4 日

JPCERT CC®

目次

1. 概況

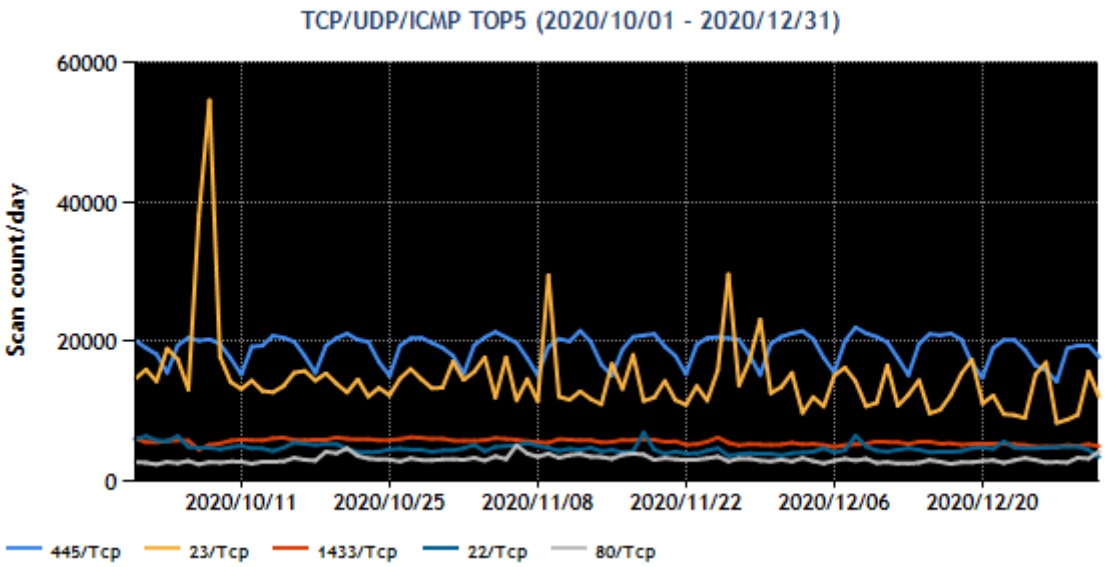
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点による多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し観測網に参加してもらう活動を行っています。
各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT などに情報を提供し、状況の改善を依頼しています。また、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、国内に設置されたセンサー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るとトップ 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	445/TCP (microsoft-ds)	1
2	23/TCP (telnet)	2
3	1433/TCP (ms-sql)	3
4	22/TCP (ssh)	4
5	80/TCP(http)	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。



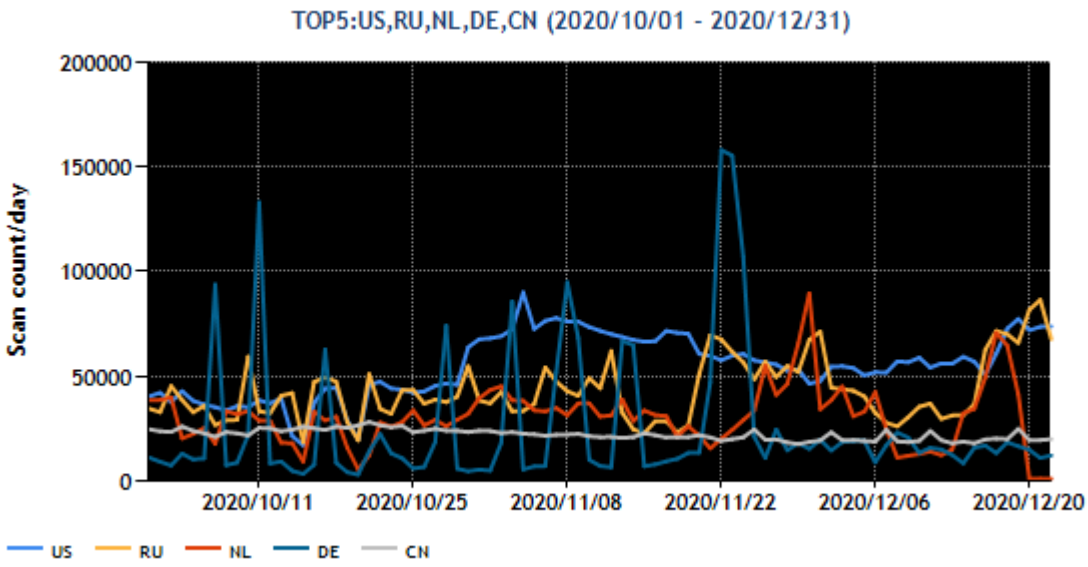
［図 1：2020 年 10～12 月の宛先ポート番号別パケット観測数トップ 5 の推移］

宛先ポート番号ごとに観測されたパケット数の順位（トップ 5）は、前四半期から変動がありませんでした。最も多く観測されたパケットは、445/TCP（microsoft-ds）宛の通信でした。本四半期を通じて一週間単位での周期的な増減を観測しています。
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	2
3	オランダ	4
4	中国	3
5	ドイツ	5

［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。



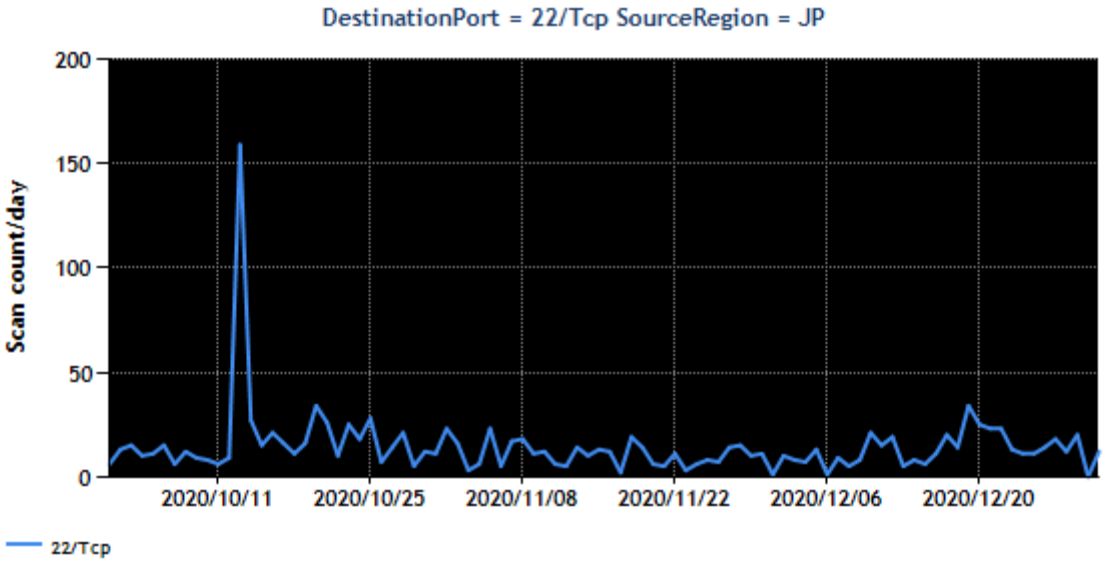
［図 2：2020 年 10～12 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期に受信したパケットの送信元地域として、最も多く見られたのは米国でした。米国は 10 月 30 日頃よりパケット数が増加しました。中国を送信元地域としたパケットはゆるやかに減少しており、ドイツと順位が入れ替わりました。オランダは 12 月 20 日からパケットが大きく減少しました。12 月 20 日以前はオランダが送信元であるとされていたパケットの送信元 IP アドレスの大半が、12 月 20 日以後にはオランダ以外の地域に割り当てられていることが確認できました。このような現象の妥当性や理由についてオランダの CSIRT に問い合わせるなどして調査中です。

2. 注目された現象

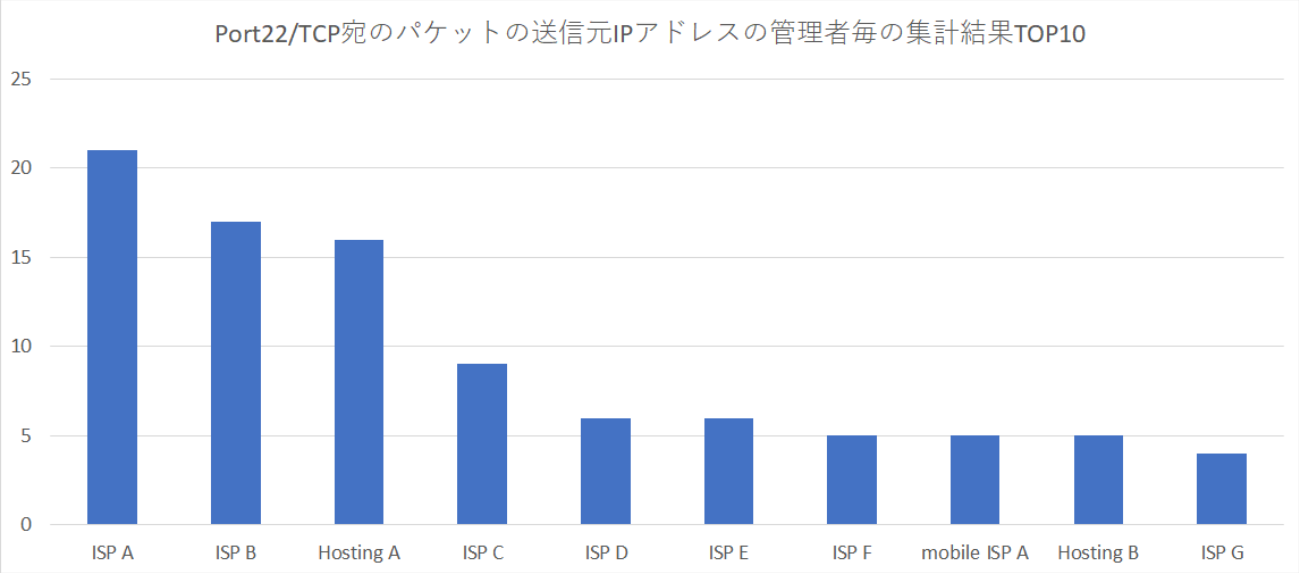
2.1. 送信元が日本となっている Port22/TCP 宛のパケット数の増加

本四半期をとおして、送信元が日本となっている Port22/TCP（ssh）宛のパケットを観測しています（図 3）。



［図 3：Port22/TCP 宛のパケット観測数の推移（送信元日本）］

Port22/TCP 宛のパケットの送信元自身も SSH を待ち受けていたケースが多くありました。Port22/TCP 宛のパケットの送信元の IP アドレスの管理者に調査を依頼したところ、ホストが侵害を受けマルウェアに感染していたという返事をこれまで複数受け取っています。今回のパケットを送ってきた送信元が同様の侵害を受けている可能性も推測できます。本四半期に観測された Port22/TCP 宛のパケットの送信元の共通性を見つけ出すための試みとして、WHOIS での管理者に基づいて集計した結果（管理者名は匿名化）を（図 4）に示します。



［図 4：Port22/TCP 宛のパケットの送信元 IP アドレスの管理者毎の集計結果 TOP10（送信元日本）］

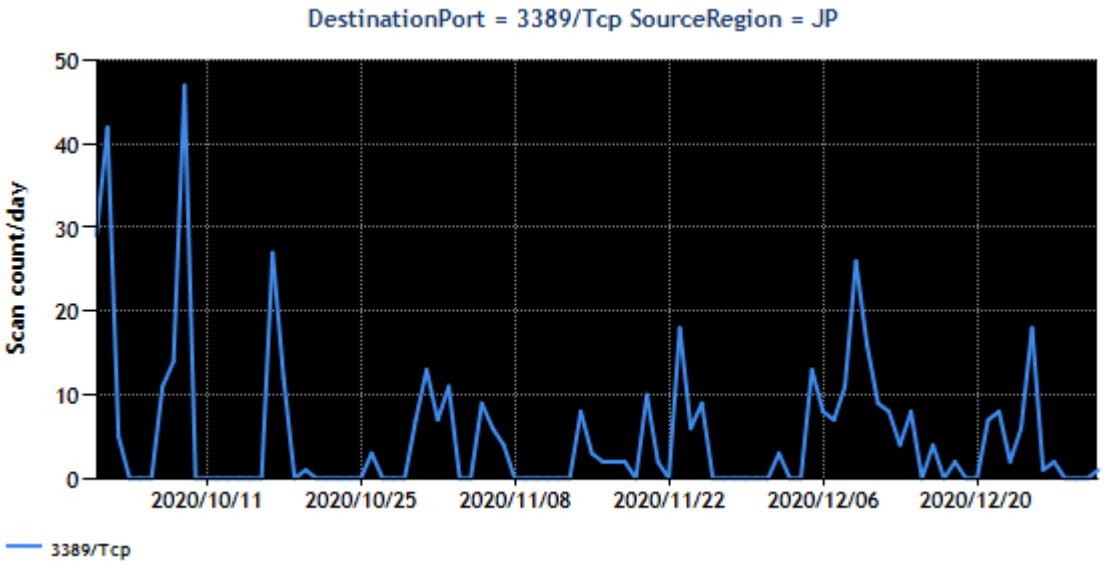
上位の 3 つの組織のうち ISP A、ISP B は動的 IP アドレスを配布する方式でサービスを行っている ISP です。Hosting A はサーバーなどを構築する際に使用されることが多い固定 IP アドレスを配布する方式でサービスを行っている事業者です。
観測されたパケットの送信元 IP アドレスのうち Hosting A が保有する範囲のものを SHODAN で検索して分析してみたところ、3 割程度が共通する特徴を持つサーバーのものであることがわかりました。一方で、ISP A と ISP B から届いたパケットの送信元に関しては、そういった特徴がみられませんでした。この特徴を持つサーバーが何らかの方法で悪用されている可能性が考えられるため、さらに分析を進めました。そうしたところ、このサーバーは箱庭ゲームでマルチプレイする際に利用されており、さらに特徴を調べてみたところ、次の点がわかりました。

- SSH がパスワードによる認証で接続可能であり、ユーザーが安易なパスワード設定を行なっていた場合、侵入を許してしまう恐れが考えられる。なお、初期の登録ユーザーは root のみである
- マルチプレイ用のゲームサービス以外のほとんどのサービスは立ち上がっていないが、UDP amp 攻撃が可能なサービスが稼働しており、ファイアウォール等により外部からのアクセス制限がなされていない

調査の結果、当該サービスはサービス提供者によってさまざまなセキュリティ上の問題に配慮して提供されていたにもかかわらず、サービス利用者による対策が不十分だったために、第三者による悪用を許容している可能性があることがわかりました。ゲーム目的のサーバーのため、利便性を優先し設定を変更しても構わないと考えるユーザーがいるのではないかと推測されますが、踏み台として他の重要なサーバーへの攻撃に利用される可能性を念頭に置いて、ゲーム目的であってもサーバーのメンテナンスを適切に行う必要があります。不要なサービスの停止やファイアウォールで必要な通信のみを許可するなどの設定を行い、管理者アカウントのパスワードを安易なものに変更することを避け、OS のアップデートを適用するなど、セキュアな環境を保つことがサーバーの管理では不可欠です。

2.2. 日本を送信元とした 3389/TCP 宛のパケットの観測事象について

本四半期中、3389/TCP（ms-wbt-server）宛のパケットの増減を観測しています（図 5）。



［図 5：Port3389/TCP 宛のパケット観測数の推移（送信元日本）］

送信元は SHODAN 等で調査すると、ほぼすべての送信元で 3389/TCP を待ち受けていることを確認できました。パケットの送信元 IP アドレスの管理者に連絡を取ったところ、サポートが終了したバージョンの Windows Server が侵害を受け、管理者が認識していないツールが設置されていたとの報告を受けました。
サポートが終了したバージョンの OS で稼働していないか、セキュリティ更新プログラムが適用されているかなどを、今一度確認することをおすすめします。

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２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。