JPCERT/CC インターネット定点観測レポート

2019 年 10 月 1 日 ～ 2019 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

2020 年 1 月 29 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、マルウエ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 等に情報を提供し、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、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。

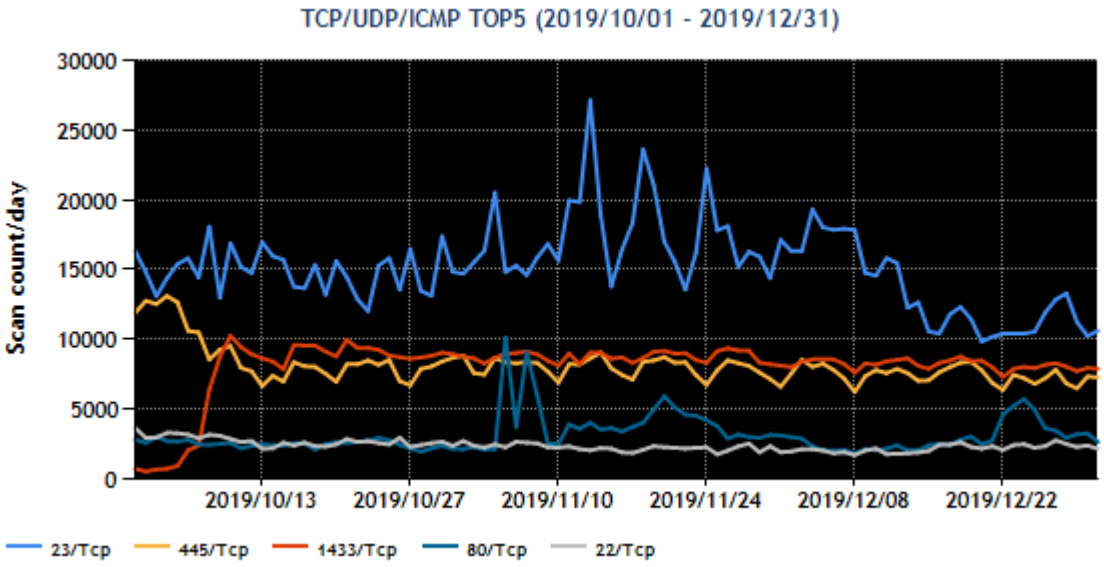
本四半期に国内で観測されたパケットの宛先ポート番号をパケットが多かった順に並べるとトップ 5 は［表 1］に示すとおりでした。

［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	23/TCP (telnet)	1
2	445/TCP (microsoft-ds)	2
3	1433/TCP (ms-sql)	TOP10 外
4	80/Tcp(http)	5
5	22/TCP	3

※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則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もつパケット観測数の推移を［図 1］に示します。



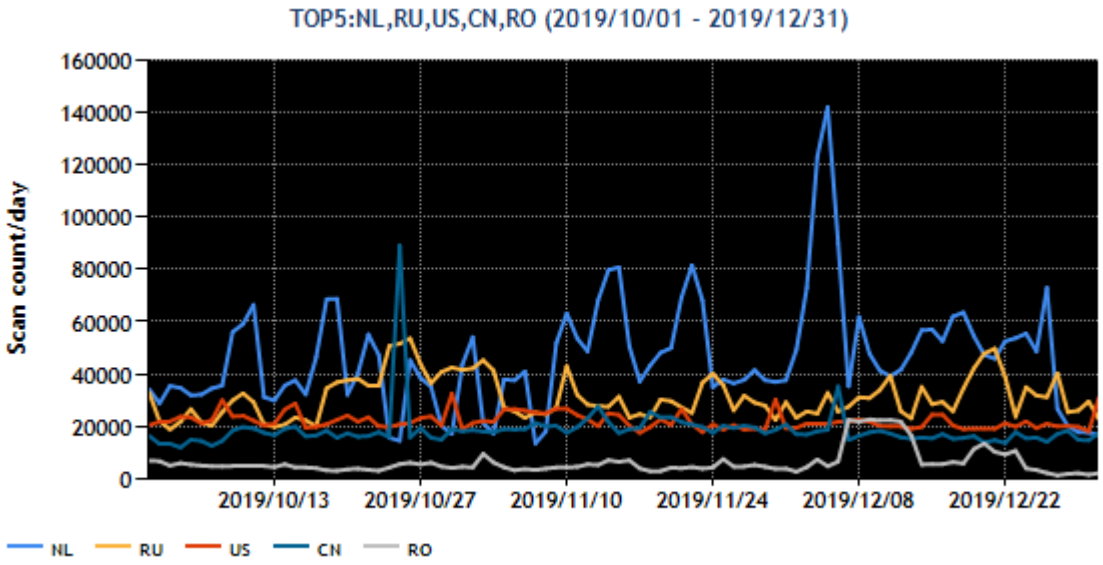
［図 1：2019 年 10～12 月の宛先ポート番号別パケット観測数トップ 5 の推移］

本四半期の期間中、毎週ほぼ一定数の 445/TCP 宛のパケットや 23/TCP 宛のパケットが観測されました。1433/TCP 宛のパケットは、10 月 4 日から増加し 3 番目に多くパケットを観測しています。この事象については、「2.1 1433/TCP 宛のパケットの動向」で述べます。
続いて、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	オランダ	1
2	ロシア	2
3	米国	3
4	中国	4
5	ルーマニア	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。



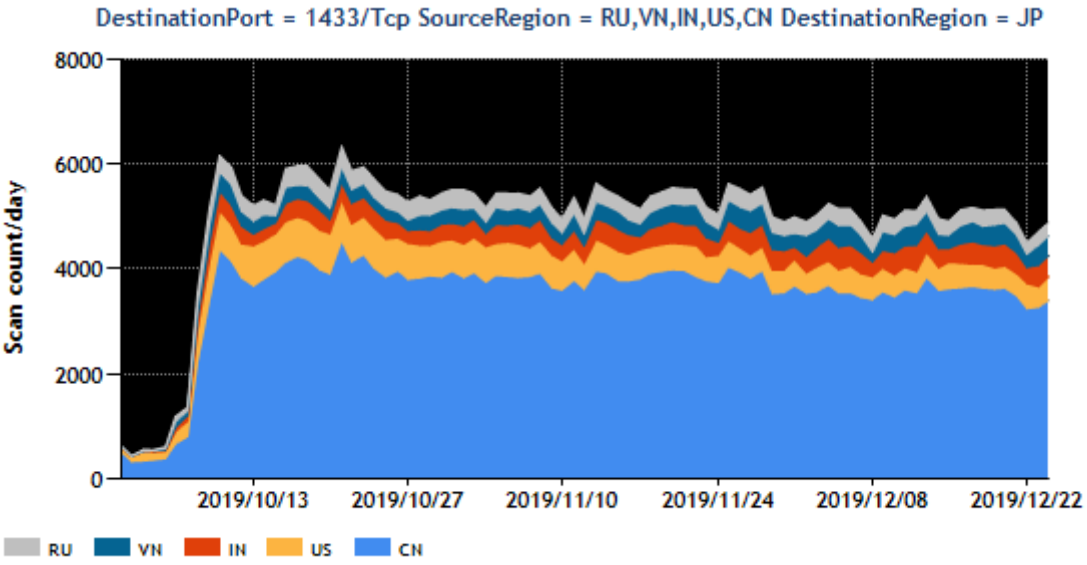
［図 2：2019 年 10～12 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期に受信したパケット数について、前四半期に引き続き送信元地域として一番多い状態が続いているオランダについて調査をおこないました。その結果、パケットの送信元の一部で Web サーバが稼働しており、開きポートの調査を目的としたスキャンを行っている旨を記載した Web ページが見つかりました。これに関連したものか否かでパケットを仕分けしたところ、パケットの 8 割近くがスキャン調査のために送信されていると推測されることが分かりました。スキャナの活動によるパケット数の変化がグラフに大きく表れる結果となりました。5 位のルーマニアについては、12 月 7 日から約一週間通常の約 3～4 倍のパケット数が観測された期間があったため、四半期の総数でも順位が変化しています。その他の地域については、順位に変化はありません。

2. 注目された現象

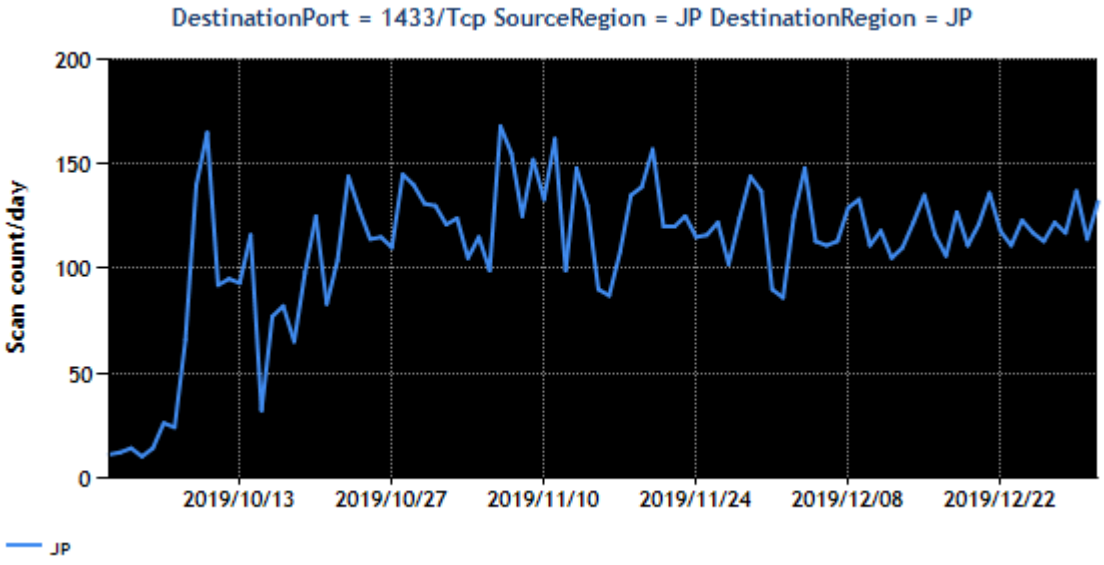
2.1. 1433/TCP 宛のパケットの動向

2019 年 10 月 4 日頃から 1433/TCP 宛の多数のパケットを観測[2]しています。［図 3］に示した地域別の積上げグラフに見られるように、主な送信元は中国で、それ以外は米国、インド、ベトナム、ロシア等の地域です。



［図 3：Port1433/TCP 観測パケット数の主な送信元地域ごとの推移］

日本もパケットの送信元として例外ではなく、同時期から多数のパケットを観測しています。順位では 13 番目に多い状態となっています。

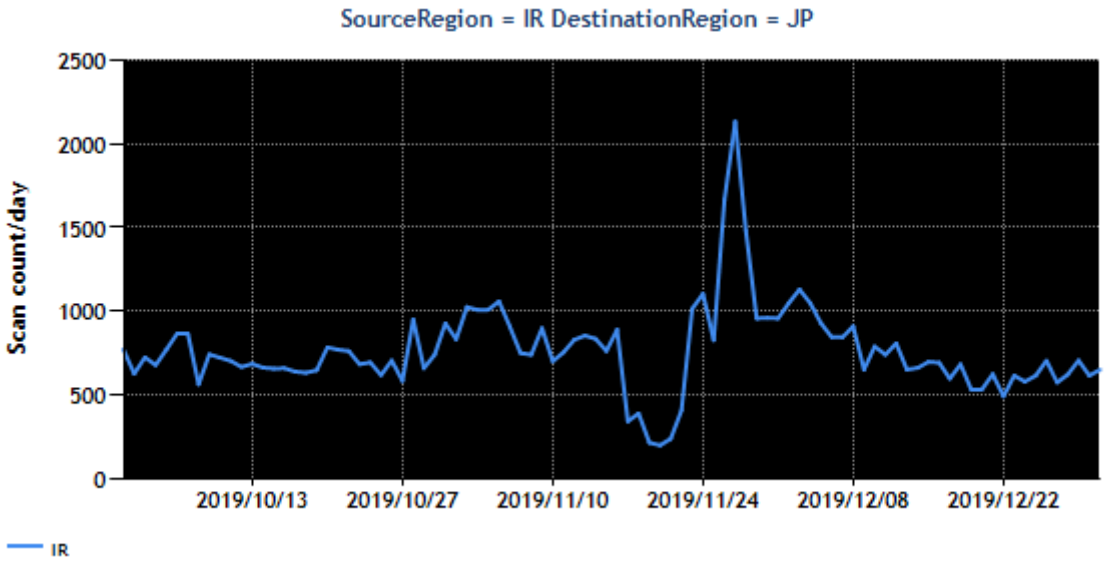


［図 4 ：日本から送信された Port1433/TCP 観測パケット数の推移］

TSUBAME のセンサーによる観測からは、スキャン後にどのような攻撃が意図されているのかは分かりません。そこで、ハニーポットを構築し 1433/TCP にどのようなリクエストが送られてくるのか確認したところ、SQL Server を対象とした認証試行が行われていることを確認しました。
次に、送信元について調査をしたところ、1433/TCP のほかにも 445/TCP のポートへのパケットの送信元の多くで IIS や SMB が動作しており Windows 環境であろうと推測されました。Windows のバージョンは特定のバージョンに偏っておらず、また SMB や RDP のポートは空いているものも閉じられているものも見られ、共通した特徴は確認できませんでした。これらのホストがどのようなマルウエアに感染してパケットを送信しているのかについてはまだ分かっていません。
SQL Server を稼働させているサーバに対する認証試行の攻撃が今後も続く可能性があります。適切なアクセス制御を行い、強固なパスワードを使用する等サーバを適切に保護することをお勧めします。

2.2. イランで行われたインターネット遮断の影響について

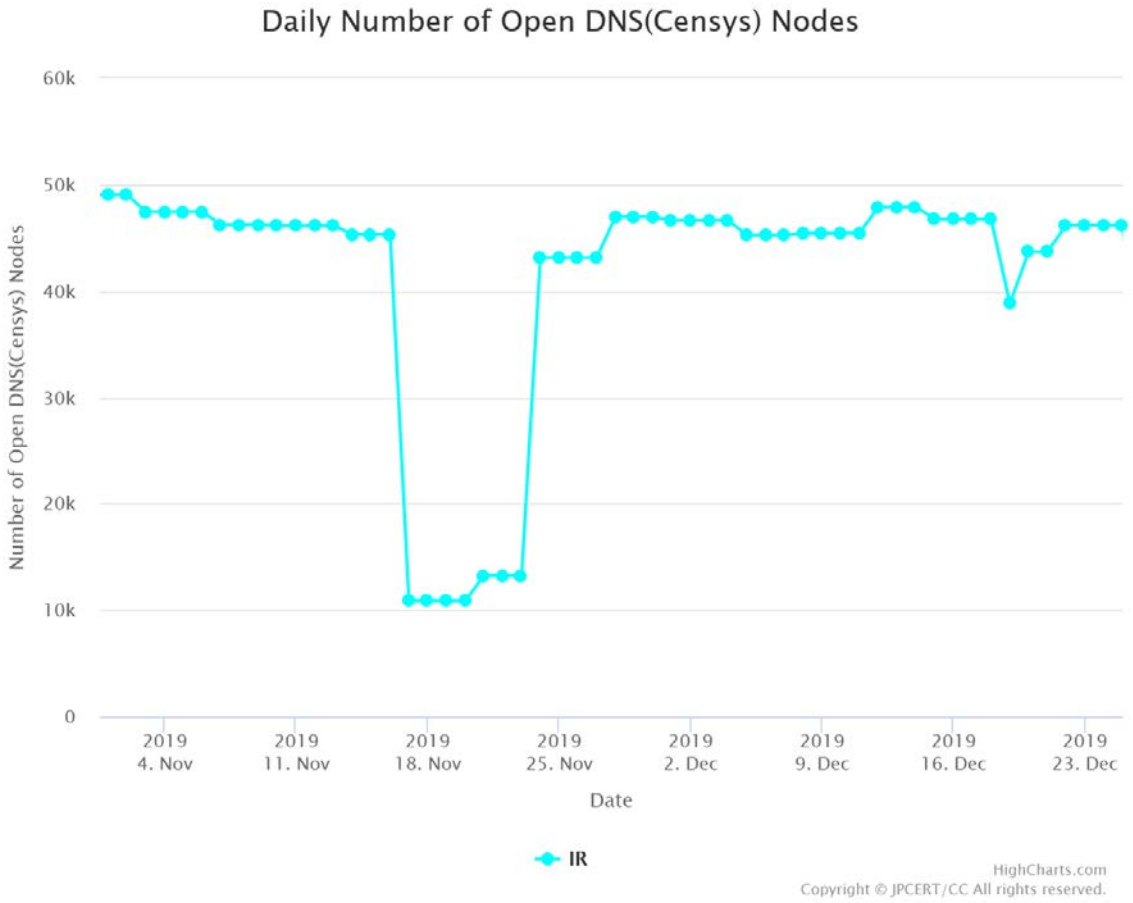
TSUBAME センサーに届くパケットは、送信元の状況だけでなく、パケットが通過する経路の状況の変化の影響も受けます。つまり、送信元の状況に大きな変化がなくとも、例えばパケットの通信経路が遮断ないし不安定になれば、観測されるパケット数が減少します。
2019 年 11 月 17 日から 23 日にかけて、送信元地域がイラン（IR）となっているパケットの観測数が減少しました。



［図 5：送信元がイランのパケット数の推移］

イランでは、11 月 15 日からガソリンの値段を引き上げたことに対する抗議デモ活動[3]が、テヘランを中心に各地で行われました。サイバーセキュリティとインターネットのガバナンスを監視する非政府組織の NetBlocks では、インターネットの遮断がこの期間中行われたと推測[4]しています。

JPCERT/CC がインターネットリスクの可視化を目的に行っている実証実験プロジェクト Mejiro[5]では、インターネット上のノードがオープンポートとなっている状況を公開していますが、オープンリゾルバの数が 11 月 17 日から 23 日にかけて減りました。



［図 6：イランの OpenResolver のノード数（Mejiro より）］

Tsubame および Mejiro による観測データに一時的な変動が見られた理由については、イラン内のボットネットの活動や、オープンリゾルバの状況の変化と考えるよりは通信制限による影響と見た方が合理的だと考えています。

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) PHP-FPM の脆弱性（CVE-2019-11043）を標的としたアクセスの観測等について
https://www.npa.go.jp/cyberpolice/important/2019/201911281.html

(3) Iran Reimposes Internet Blackout in Various Provinces, ILNA Says
https://www.bloomberg.com/news/articles/2019-12-25/iran-reimposes-internet-blackout-in-various-provinces-ilna-says

(4) NetBlocks.org (@netblocks)
https://twitter.com/netblocks/status/1196116024359366656

(5) 実証実験:インターネットリスク可視化サービス―Mejiro―
https://www.jpcert.or.jp/mejiro/

本活動は、経済産業省より委託を受け、「平成３１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。