レポート

平成 31年3月 28 日

ウェブメールクライアント「Internet Messaging Program」の脆弱性を有する機器に対するアクセスの増加等について

- ウェブメールクライアント「Internet Messaging Program」の脆弱性を有する機器に対するアクセスの増加
- 宛先ポート 8080/TCP 等を利用した SYN/ACK リフレクター攻撃とみられるアクセスの観測
- 宛先ポート 123/UDP に対する NTP リフレクタースキャンとみられるアクセスの増加

1 ウェブメールクライアント「Internet Messaging Program」の脆弱性を有する機器に対するアクセスの増加

警察庁のインターネット定点観測において、平成 31年1月 17 日以降、ウェブメールクライアント「Internet Messaging Program」(以下「IMP」という。)の脆弱性を有する機器に対するアクセスを観測しました(図1)。

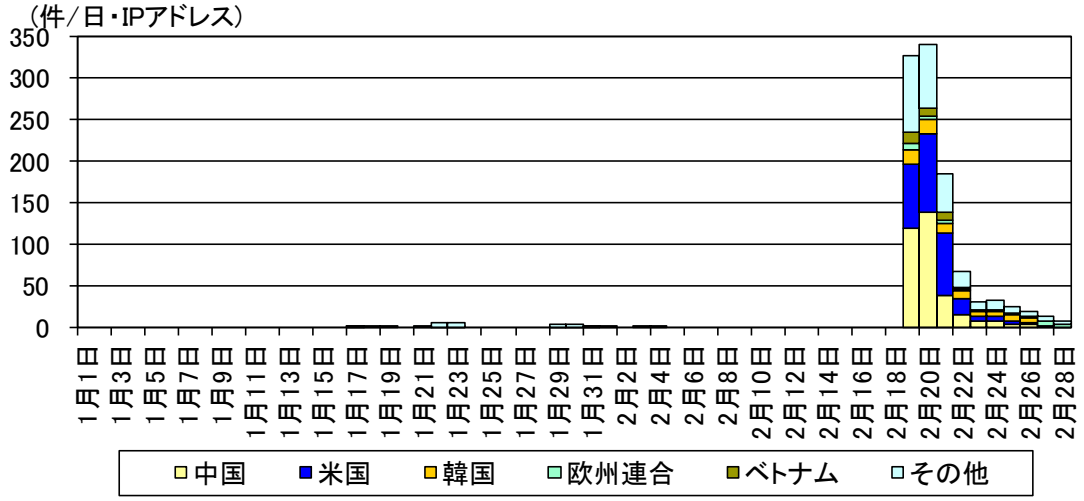

図1 IMP に対するアクセス件数の推移(着信元国・地域別 [i] H31.1.1～2.28)

IMP は The Horde Project が開発した IMAP [ii] に対応するウェブメールクライアントであり、グループウェア「Horde」のメール機能として使用され、フリーソフトとしても配布されています。

[i] 着信元国・地域については、判明した着信元(送信元)IP アドレスが当該国・地域に割り当てられていることを指しており、踏み台となっているなどにより、送信者の所在と一致していない場合があります。以降も同様の表記です。
[ii] Internet Message Access Protocol の略。メールサーバからメールを受信するための規約。POP と異なり、メールサーバにデータを保存したままメールの内容を確認することができる。

PHP には、IMAP サーバに接続する際の処理に実装不備があることが海外のセキュリティコミュニティにおいて指摘されており、平成 30 年 11 月 25 日に脆弱性（CVE-2018-19518）が公表[i] されました。

IMP には、CVE-2018-19518 に起因する脆弱性があり、当該脆弱性が悪用された場合、第三者により遠隔から任意の OS コマンドを実行される可能性があります。

また、警察庁では、平成 31 年1月に海外の脆弱性投稿サイトにおいて当該脆弱性を悪用した攻撃ツールが公開されていることを確認しました。

同攻撃ツールは、HTTP GET リクエストにより IMP のテストページの取得に成功した場合に当該脆弱性を悪用して任意の OS コマンドを実行するものでした。

今回観測したアクセスにおいては、同攻撃ツールを起動した際にテストページのパスとして例示される「/horde/imp/test.php」に対する HTTP GET リクエストが含まれており（図2）、当該アクセスは IMP の稼働確認を行っているものと考えられます。また、IMP の稼働を確認した後に当該脆弱性を悪用し、攻撃を実施するものと推測されます。

```
GET /horde/imp/test.php HTTP/1.1
Host: [redacted]
Accept-Encoding: identity, deflate, compress, gzip
Accept: */*
User-Agent: python-requests/0.12.1
```

図2　観測したアクセスの例（一部マスキング）

宛先ポート別では、1月中旬以降に観測したアクセスは、全て宛先ポート 80/TCP に対して行われていましたが、2月 19 日以降、80/TCP を含む複数のポートでアクセスの急増を観測しました（図3）。このことから、宛先ポート 80/TCP 以外のポートで公開されているインターネット上の機器についても、当該脆弱性を有する IMP の稼働確認を広く行っているものと考えられます。

[i] https://nvd.nist.gov/vuln/detail/CVE-2018-19518

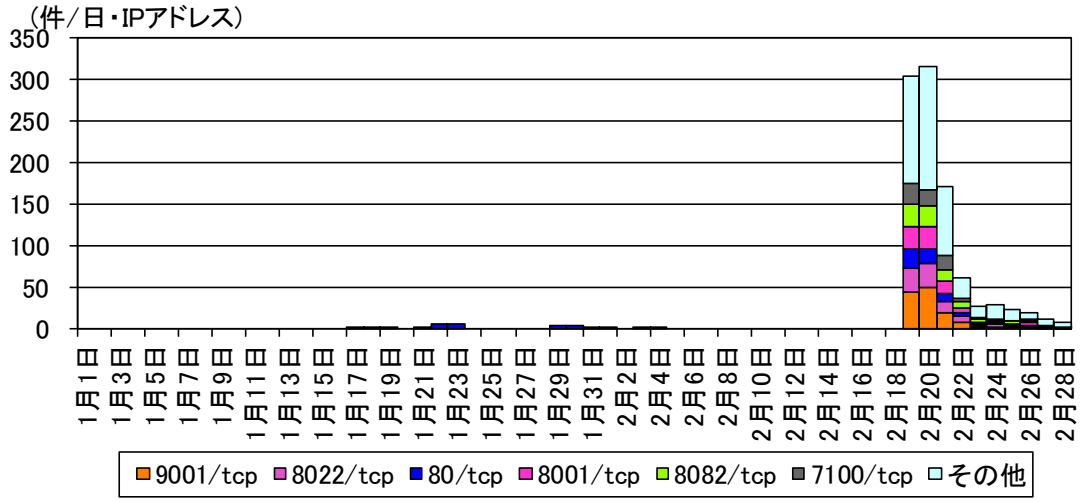

図3　IMP に対するアクセス件数の推移（宛先ポート別　H31.1.1～H31.2.28）

PHP 及び IMP の利用者は、以下の対策を参考に、セキュリティ対策を行うことを推奨します。

- PHP を最新バージョンにアップデートすることが有効です。ただし、OS（Linux）のディストリビューションによって影響を受けるバージョンが異なるため、各ディストリビューションのウェブページを参照[i]してください。
- PHP のアップデートが困難である場合、IMP のインストール後に必要な初期設定を行った後、テストページの削除又は外部からのテストページに対するアクセスの遮断等の制限を実施してください。
- 一般の利用者がアクセスする必要のないページについては、特定の IP アドレスからのみ許可するなどの適切なアクセス制限を実施してください。

[i] Ubuntu
https://people.canonical.com/~ubuntu-security/cve/2018/CVE-2018-19518.html
Debian
https://security-tracker.debian.org/tracker/CVE-2018-19518
Red Hat
https://access.redhat.com/security/cve/cve-2018-19518

2 宛先ポート 8080/TCP 等を利用した SYN/ACK リフレクターとみられるアクセスの観測

警察庁のインターネット定点観測において、平成 31 年1月 24 日頃から宛先ポート 8080/TCP 等に対するアクセスの増加を観測しました（図4）。警察庁では平成 30 年 9 月下旬頃以降、宛先ポート 80/TCP を利用した SYN/ACK リフレクター攻撃とみられるアクセス[i]を断続的に観測しており、今回観測したアクセスも当該攻撃に関連するものと考えられます。

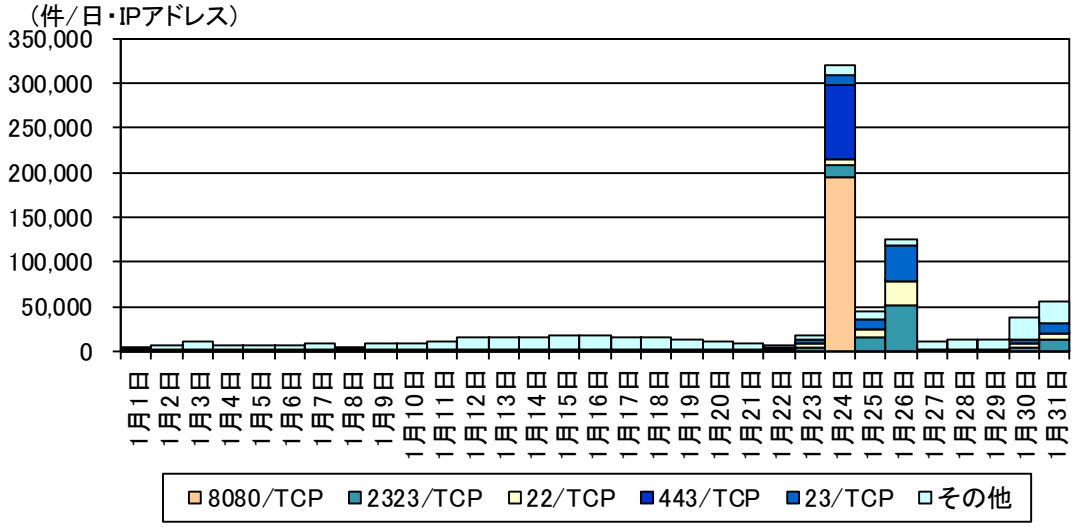

図4 宛先ポート 8080/TCP 等に対するアクセス件数の推移（宛先ポート別 H31.1.1～1.31）

1月 24 日に観測したアクセスでは、特定の IP アドレスから 8080/TCP 及び 443/TCP に対する大量の SYN パケットを3時間以上継続して観測しました（図5）。これまでの観測と同様に、これら SYN パケットは応答型センサー[ii]でのみ検知していることから、インターネット上で稼働するウェブサーバ等のサービスを事前に探索し、特定していたものと考えられます。また、このアクセスでは、それぞれの IP アドレスからのアクセスの変動は大きいものの、アクセスの総量を一定とするように送信している特徴がみられました（図6）。そのため、当該アクセスは何らかのツールを使用し、攻撃対象の IP アドレスを詐称して SYN パケットを送信していた可能性があります。

[i] 「宛先ポート 80/TCP を利用した SYN/ACK リフレクター攻撃とみられる観測等について」
https://www.npa.go.jp/cyberpolice/important/2018/201811301.html

[ii] TCP3ウェイハンドシェイクの TCP コネクション確立手順において、送信元からの SYN（開始要求）に対する SYN/ACK（確認応答）を送信するセンサー。

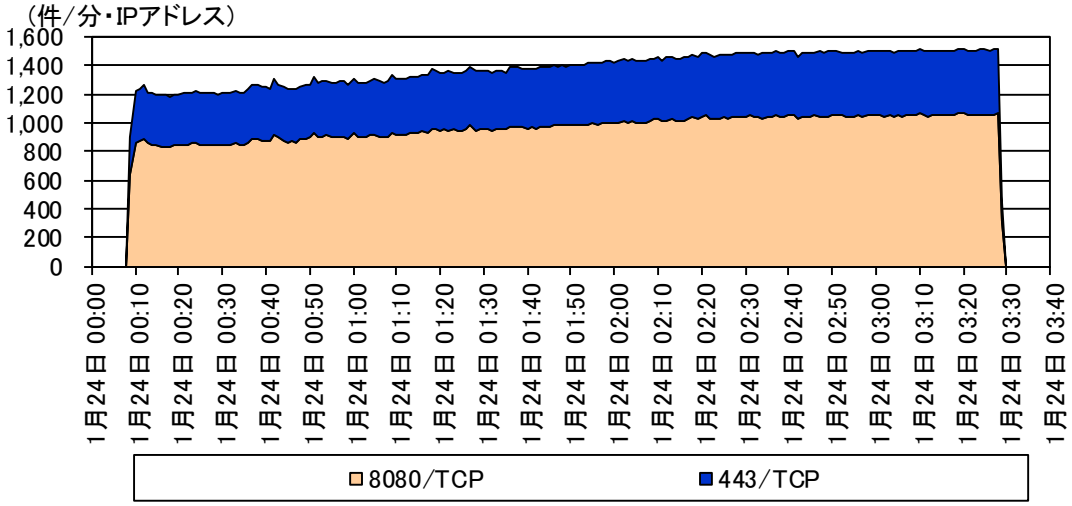

図5　特定 IP アドレスからの宛先ポート 8080/TCP 等に対するアクセス件数の推移
（宛先ポート別　H31.1.24 0:00～3:40）

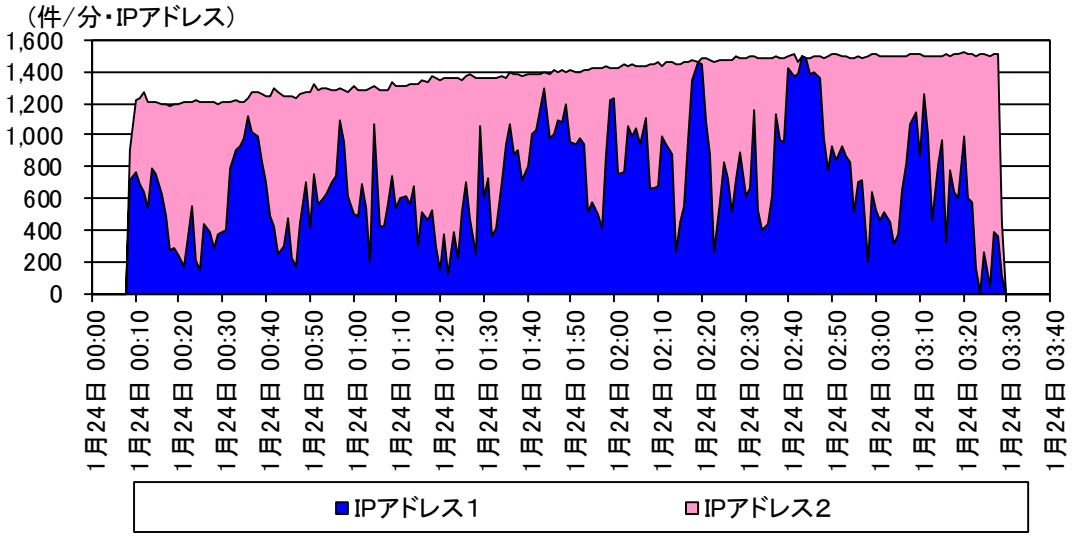

図6　特定 IP アドレスからの宛先ポート 8080/TCP 等に対するアクセス件数の推移
（IP アドレス別　H31.1.24 0:00～3:40）

さらに、1 月 25 日以降、Telnet で使用される 23/TCP や 2323/TCP に対しても SYN/ACK リフレクター攻撃とみられるアクセスを断続的に観測しています（図7）。これらのポートはデジタルビデオレコーダ等の IoT 機器においても広く使用されているものです。

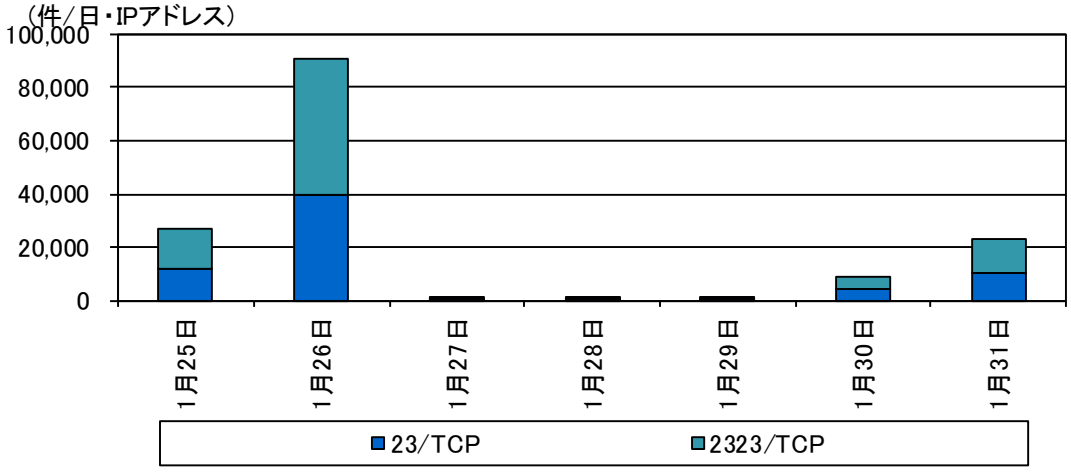

図7　宛先ポート 23/TCP、2323/TCP に対するアクセス件数の推移
（宛先ポート別　H31.1.25～1.31）

このことから、攻撃者はウェブサーバ以外にもインターネット上で多数稼働している踏み台として利用可能な IoT 機器等の稼働状況をあらかじめ探索した上で SYN/ACK リフレクター攻撃を行っていたと推測されます。

なお、SYN/ACK リフレクター攻撃は攻撃対象だけでなく当該攻撃の踏み台となった機器についても、SYN Flood 攻撃への対策が不十分であった場合、意図せずサービス不能に陥ることがあります。

そのため、ウェブサーバ等の管理者は、以下の対策を参考にセキュリティ対策を行うことを推奨します。

- 上位の通信事業者やサービスプロバイダが提供する DDoS 攻撃対策サービスの利用を検討してください。
- Syn Flood 攻撃に対応した OS やネットワーク IDS 製品の導入を検討してください。
- ファイアウォール等によって不必要な外部からのアクセスを遮断してください。

また、IoT 機器の利用者は、当該機器が SYN/ACK リフレクター攻撃の踏み台として悪用されないよう、以下の対策を行うことを推奨します。

- IoT 機器をインターネットに接続する場合には、直接インターネットに接続せずに、ルータ等を使用してください。
- 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 IP アドレスのみにアクセスを許可したり、VPN を用いて接続することも検討してください。

3 宛先ポート 123/UDP に対する NTP リフレクタースキャンとみられるアクセスの増加

警察庁のインターネット定点観測において、平成 31年2月 16 日以降、NTP [i] で使用される宛先ポート 123/UDP に対するアクセスの増加を観測しました（図8）。

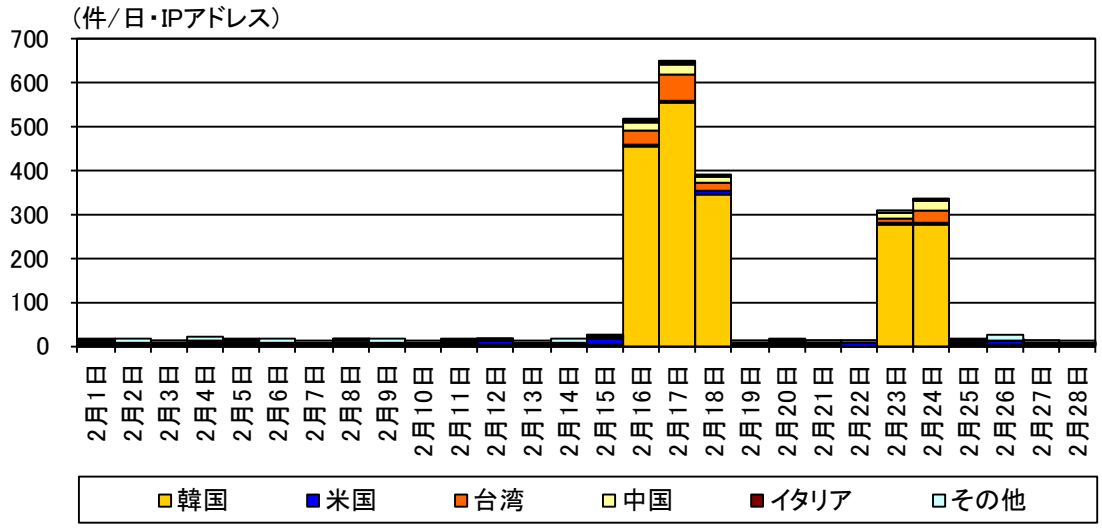

図8 宛先ポート 123/UDP に対するアクセス件数の推移（着信元国・地域別 H31.2.1～2.28）

警察庁では、平成 27 年 10 月 23 日、UDP を利用するプロトコルを悪用するリフレクター攻撃について注意喚起 [ii] しています。

攻撃者が、踏み台となる NTP サーバに対して着信元（送信元）を攻撃対象に偽装して問い合わせを行うと、踏み台となった NTP サーバは、偽装された問い合わせ元、つまり攻撃対象に対して問い合わせ結果を回答します（図9）。この際に、問い合わせのデータサイズと比較して、NTP サーバからの回答のサイズが大きくなり、攻撃者からの攻撃パケットが、あたかも NTP サーバで反射増幅されて攻撃対象に届くかのように動作します。

[i] NTP とは、「Network Time Protocl」の略であり、ネットワーク経由でコンピュータ等の時刻同期を行うプロトコルです。

[ii] UDP を利用するプロトコルを悪用するリフレクター攻撃の観測状況について
https://www.npa.go.jp/cyberpolice/detect/pdf/20151023.pdf

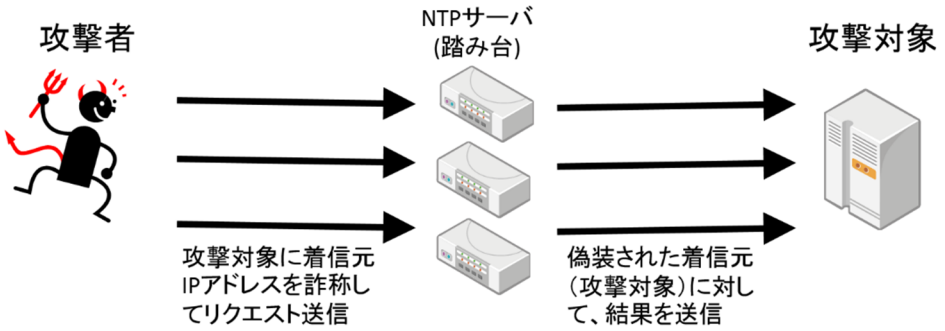

図9　NTP リフレクター攻撃の原理

今回観測したアクセスの急増は、当該パケットの送信元 IP アドレス及び宛先 IP アドレスに偏りが認められないことから、攻撃ではなく、攻撃で使用するための踏み台となるリフレクターのスキャンと考えられます。

また、観測したパケットのほとんどは IP ヘッダの TTL[i] 値が 64 未満となっていることから、着信元（送信元）となっている機器の多くは Linux が動作していると推測されます（図 10）。

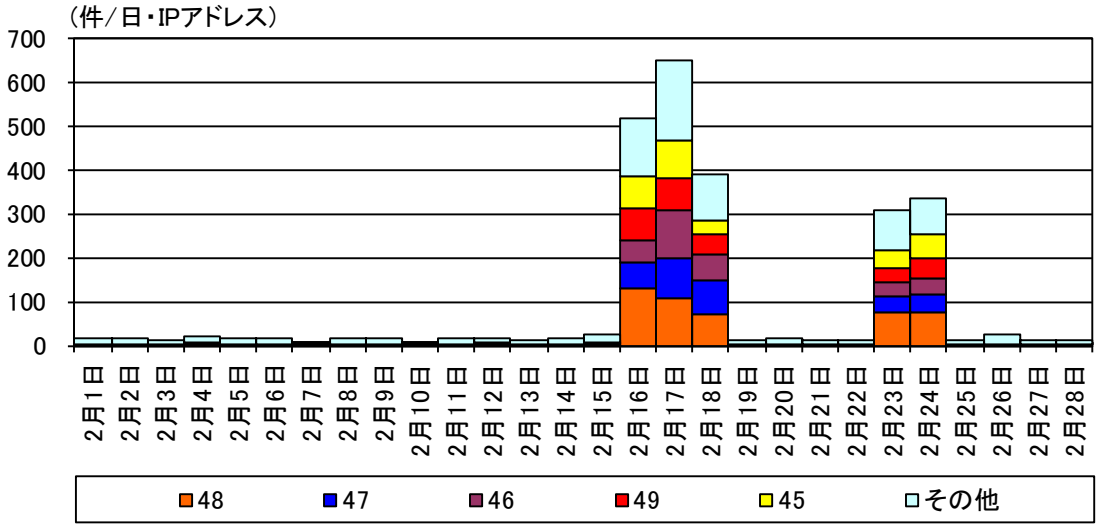

図 10　宛先ポート 123/UDP に対するアクセス件数の推移（TTL 別　H31.2.1～2.28）

管理する機器が、踏み台として悪用されないために、次の対策を実施することを推奨します。

- 使用していない不要なサービスは停止してください。サーバ等のコンピュータだけではなく、ネットワーク機器においても、意図せずに外部へ不要なサービスを公開していないか確認を実施してください。
- 外部に公開する必要がないサービスは、インターネットからの通信を遮断してください。

[i] TTL は Time to live の略。IP ヘッダの TTL 値は、ネットワーク転送の際にルータ等を経由する毎に値が減少します。パケット送出時の IP ヘッダの TTL 値は、Linux で 64、Microsoft Windows で 128、UNIX で 255 が初期値となっています。ただし、一部のバージョンの OS では、異なる値となっているものも存在します。

- 不特定多数に公開する必要がないサービスについては、適切なアクセス制限や認証を実施してください。
- 不特定多数に公開する必要があるサービスについては、リフレクター攻撃の踏み台として悪用されないように、適切な設定への変更を実施してください。
- ブロードバンドルータの製造元、貸与している ISP や回線事業者等が公開している最新バージョンのファームウェアや、攻撃の踏み台となることを回避する設定変更方法を確認してください。
- 最新バージョンのファームウェアが未適用であれば、適用を実施してください。
- 攻撃の踏み台となることを回避する設定がされていなければ、設定変更を実施する。