CIAJ セキュリティ Information

# IoT 機器の不適切管理を狙うウィルスの脅威と対策について
## ～IoT 時代の加害者とならないために～

2017 年 3 月 24 日
CIAJ 通信ネットワーク機器セキュリティ分科会

### IoT 機器のサイバーセキュリティ

近年、サイバー攻撃の脅威が増しており、IoT 分野においても様々なセキュリティ要件が求められています。ところが、インターネットに繋がるカメラやモバイル・ルータといった IoT 機器については、セキュリティ対策が適切に施されていないケースも多く、一度、ウィルス感染が広がるとサービス停止を余儀なくされる等、被害者となる一方で、IoT 機器が特定のサーバに一斉にサービス妨害を行う攻撃(DDoS 攻撃)に知らない間に加担させられ、ウィルスを拡散する加害者にもなりかねません。

最近では、2016 年 9 月から急激に観測され始めたウィルス「Mirai」による被害が相次いでいます。そこで「Mirai」の現状と今後 IoT 機器に施すべき対策について紹介します。

### 不適切管理を狙う IoT ウィルス「Mirai」

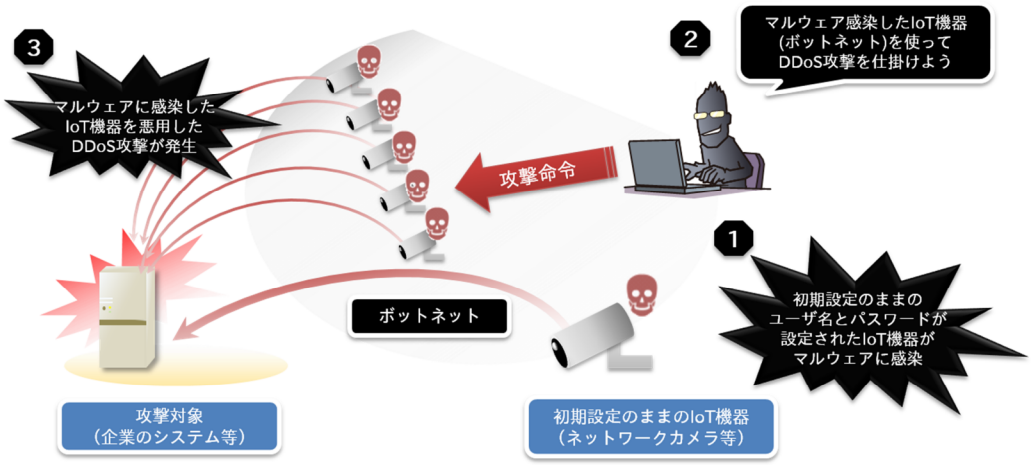
2016 年 10 月 21 日、DNS サービスを提供する米国 Dyn（ダイン）社の“Managed DNS”サービスに対し、大規模 DDoS が発生しました。攻撃は 10 月 21 日（UTC）11：10-17：45 まで継続し、“Twitter”、“ウォールストリートジャーナル”等の同社顧客がサービス停止に追い込まれました。攻撃は同社サービスである宛先ポート 53/TCP（DNS サービス）を狙い撃ちにしたものであり、同社ブログは“「Mirai」を使ったボットネットから発信されていたことを立証できる”と表明しました。

これに先立つ 9 月 20 日、元ワシントンポストのレポーターでもあり、高名なセキュリティジャーナリストである Brian Krebs 氏の運営するブログ“KrebsonSecurity.com”が最大で 623Gbps の DDoS 攻撃を受けました。攻撃は数日間に亘って継続し、後に「Mirai」の作者を名乗る人物から、38 万を超える IoT 機器を感染させた上で“Krebs on Security”に対する攻撃に使用したことが明かされました。

「Mirai」は 9 月下旬にオープンソースとして、ハッカーが集まるフォーラムでも公開されています。その機構は IoT 機器を無作為にスキャンして感染し、ボットネットに取り込む仕様です。特筆するべきは“ビジネスモデルを前提としたマルウェア設計”とその“簡素さ”でしょう。実際、「Mirai」が感染に用いるのは、ソースにハードコーディングされたユーザ名とパスワード（ログイン情報）であり、“root”、“password”といった汎用的な単語を初期設定としている機器を狙い、Port23/2323（Telnet サービス）をスキャンし、ログ

インを試み、プラットフォームに応じたマルウェアをダウンロードします。不正侵入に用いるログイン情報の組み合わせはソースによれば僅か 62 組であり、これだけで数十万台規模の IoT 機器が不正侵入を受けたことになります。

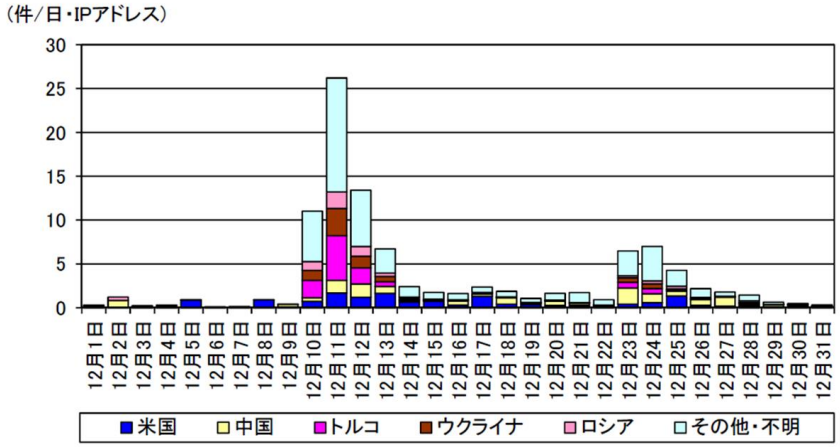
このように「Mirai」に感染した IoT 機器が大規模な DDoS 攻撃を引き起こした背景として、多くの IoT 機器でログイン情報が初期設定のまま利用されていたことが推察されます。




**ログイン情報が初期設定のままの IoT 機器が狙われるイメージ（出展：IPA 安心相談窓口だより第 16-13-359 号）**

### 「Mirai」亜種の急増

その後、2016 年末には様々な亜種による攻撃が観測されるようになりました。“警察庁セキュリティポータルサイト@Police”によれば、12 月 10 日から海外製のデジタルビデオレコーダ等に使用される宛先ポート 37777/TCP に対するアクセスの急増が観測されています。「Mirai」亜種は海外製のデジタルビデオレコーダ等の脆弱性を突いて不正侵入を試み、管理ポートを開けて、マルウェアのダウンロードを行い、更なる感染活動を続けます。観測されたアクセスは、宛先ポート 23231/TCP を介して機器側の Telnet サービスにアクセスできるよう設定変更を試みるものであり、その後、あて先ポート 23231/TCP に対するアクセスの急増が観測されました。




**宛先ポート 37777/TCP に対するアクセス件数の発信元国・地域別推移**

**（出展：警察庁「Mirai」ボットの亜種等からの感染活動と見られるアクセスの急増について　平成 28 年 12 月期）**

更に攻撃手法だけでなく、ターゲットとなるプラットフォームも拡大しつつあります。当初、Linux のファームウェアを搭載した IoT 機器だけを対象としていましたが、Windows 固有のサービスも対象としたスキャンが行われるようになったほか、可能な限り脆弱な攻撃対象を探索し、パスワード・リストによる不正侵入を試みます。現在でも「Mirai」亜種は進化を続け、様々な感染活動が世界中で行われている状況です。

## IoT 機器に施すべき対策とは

IoT 機器 “利用者“が、「Mirai」のようなウィルスを拡散する加害者にならないためには、以下のような点に注意を払う必要があります。

(1) 不要な管理サービスのインターネット側への公開を停止
(2) 初期パスワードの変更と認証機能の有効化
(3) ファームウェアのアップデート

たとえベンダーから提供される最新のファームウェアを使用したとしても、IoT 機器の中には脆弱性を含むオープンソースが採用されているケースもあります。踏み台となり得る侵入ルートは極力閉じるべきで、不要なサービスはインターネット側への公開を行うべきではありません。更に初期パスワードの変更も行う必要があります。

また、IoT 機器によるサービスを提供する“事業者”の視点では、以下が重要です。

(1) IoT 機器の要塞化（ハードニング）やホワイトリストによる対策
(2)脆弱性診断の実施
(3)不要な通信の禁止とセキュリティログ監視

(1)のホワイトリストによる対策は対象となるプラットフォームが限定されることに注意が必要です。しかし、大変強力な仕組みであり、例え侵入されたとしてもその後の感染拡大や不正操作を防止することができるため、事後の防止策としても有効でしょう。(3)は IoT 機器の接続仕様を把握した上で“最小限のシステム接続”の原則を守ったインターネット接続を行います。外部から内部への通信（Ingress）だけでなく、内部から外部への通信（Egress）についても許可された通信相手“以外”はフィルタリングを行って、想定外の通信を行う際にはアラートとして通知を行うことで「Mirai」の加害者とならないようにします。

このように不正侵入を全て防ぐことは困難であることから、侵入を前提として、侵入後の不正操作を防止し、攻撃発生時にはアラートとして検知しつつ、的確かつ迅速・柔軟に“ダメージコントロール”の実施を考慮する必要があります。

**今後の課題**

「Mirai」の“進化“に見られるように、仮にどのような対策を採ったとしても、悪意のある攻撃者は更に新たな手法やマルウェアを用いて攻撃を仕掛けるため、サイバー攻撃は本質的に“想定外”となり、防御者の脆弱性を突きます。こうした“想定外の想定”や“有事の際の即応対応”を行うには、既存の組織の枠組みに縛られることなく、組織横断の PSIRT（製品セキュリティインシデント対応チーム）のようなサイバーセキュリティ体制の構築が課題となっています。外部攻撃を受け入れた前提で被害を極小化する“減災視点”での組織検討とその仕組みづくりが重要です。今後、業界を挙げた PSIRT の取り組みや施策にも注目していくと良いでしょう。

著者：平永　敬一郎（ひらなが　けいいちろう）　株式会社　東芝
プロフィール
株式会社　東芝　インダストリアル ICT ソリューション社
インダストリアル ICT セキュリティセンター
セキュリティ技術部　勤務
参事

**【参考文献】**

・IPA　安心相談窓口だより　第 16-13-359 号『ネットワークカメラや家庭用ルータ等の IoT 機器は利用前に必ずパスワードの変更を』
https://www.ipa.go.jp/security/anshin/mgdayori20161125.html
・警察庁セキュリティポータルサイト@Police『「Mirai」ボットの亜種等からの感染活動と見られるアクセスの急増について』
http://www.npa.go.jp/cyberpolice/important/2017/19824.html

・国際公共政策研究センター（CIPPS）「枠にとらわれないサイバーセキュリティ」
http://www.cipps.org/pdf/20140801.pdf
・国際公共政策研究センター（CIPPS）「サイバーセキュリティ政策 – シミュレーションと提言」
http://cipps.org/essay/pdf/report32.pdf#page=2

問い合わせ先
企画推進部
TEL:03-5403-9357　FAX：03-5403-9360