サイバーセキュリティ通信　【第6号】

平成28年12月
大分県警察本部　生活安全部
生活環境課　サイバー犯罪対策室

IoT機器のボット化に注意を！！

1　ボット(bot)とは

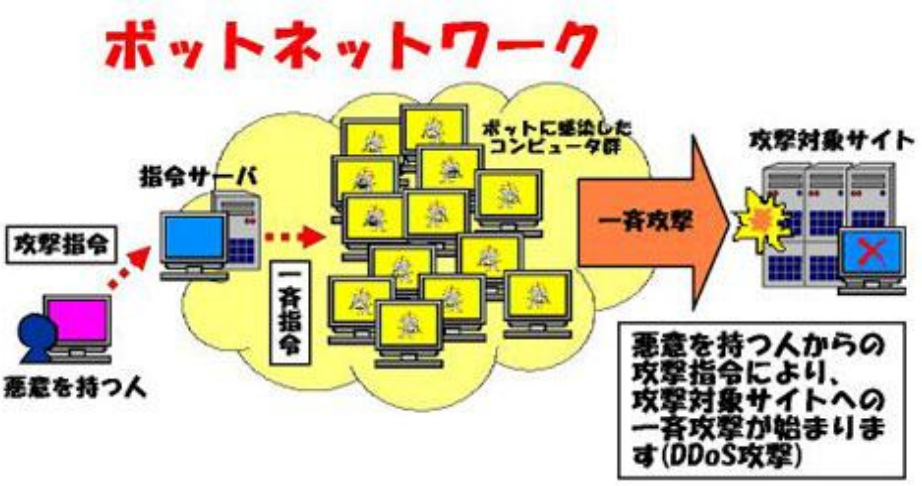
ボットとは、コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータをネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラムです。

感染すると、外部からの指示を受け、その指示に従って処理を実行します。この動作がロボットに似ていることから、ボットと呼ばれています。

2　ボットに感染した影響

ボットに感染したコンピュータは、悪意を持つ者がある特定の対象に一斉攻撃の指令を出すことの出来る「ボットネットワーク」に組み込まれてしまう場合があります。

しかも利用者は、自分のコンピュータが感染していることを知らないのです。

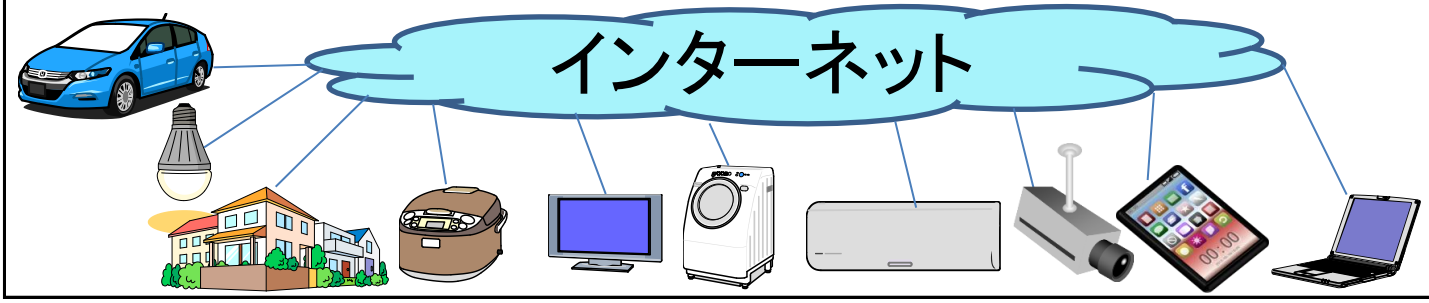


※独立行政法人情報処理推進機構提供

3　IoT機器を標的とした攻撃

(1)　IoT機器

IoT機器とは、パソコンやスマートフォンだけでなく、例えば、テレビ、ビデオレコーダー、防犯カメラ(ネットワークカメラ)、オフィスの複合機などがインターネットに接続されることで、モノとモノがインターネットで繋がっていることを言います。インターネットに繋がっていることで、外部からアクセスして、例えば、カメラ画像をスマートフォンでも確認することができるのです。



（2）ウイルス「Mirai（ミライ）」の感染拡大

「Mirai」は、Webカメラ、ルーター、ビデオレコーダーなどのIoT機器に感染して、ボットネットワークを形成してしまうマルウェアのひとつです。

平成28年9～10月にかけて、この「Mirai」が日本を含めて世界中で猛威を振るっており、現在も感染は拡大しているものと思われます。

感染拡大の最大の要因は、IoT機器のログイン情報が初期設定のまま無防備の状態になっていることです。

IoT機器を設置する際に、初期設定のままのユーザー名やパスワード（ログイン情報）を変更せずに、そのままにしていると、悪意のある者に侵入され「Mirai」に感染してしまうのです。

そして、「Mirai」に感染したIoT機器が、他の感染先を探したり、他の機器を攻撃するようになってしまうのです。

つまり、自分が持つIoT機器がウイルス感染拡大の手助けをしてしまうことになるの

4　防止対策

①　IoT機器の認証情報を変更する

IoT機器のログイン情報（認証情報）が初期設定のままだと、ウイルスに狙われる可能性が高くなります。

設定を変更するだけで、感染のリスクが低減されます。

②　パスワード＋1

利用しているパソコン、ルータやIoT機器等の今あるパスワードに「1文字」の数字かアルファベットを付け加えて下さい。

「1文字」付け加えるだけで、数字とアルファベット（大文字・小文字）の組み合わせで、62倍にセキュリティが向上します。

今あるパスワードに「＋1」のパスワードをお願いします。

③　OS、ソフトウェアを最新の状態にする

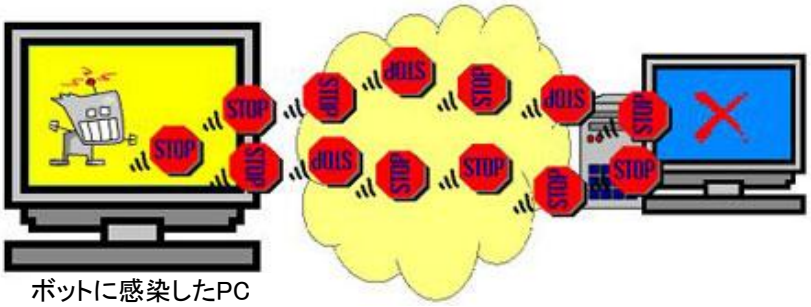
ウイルスは、パソコンのOSやインストールされている各ソフトのぜい弱な部分を狙って侵入します。

パソコンだけでなく、IoT機器の中にはOSが搭載されているものもあります。

OSやソフトウェアは、常に最新の状態に更新しましょう。

④　ウイルス対策ソフトを導入し、常に最新の状態にする

インターネットにアクセスするパソコンには、必ずウイルス対策ソフトを導入し、パターンファイルを常に最新の状態に更新しましょう。



ボットに感染したPC

あなたの会社や団体で研修の一環として、サイバーセキュリティカレッジを開催しませんか？
小学生から大人まで幅広く対応できます。下記の連絡先にご相談下さい。

大分県警察本部生活安全部生活環境課サイバー犯罪対策室
サイバーセキュリティ係　　Tel:097－534－2048