IPA Better Life with IT

情報セキュリティ10大脅威2018

～1章 情報セキュリティ対策の基本　IoT機器（情報家電）編～

～引き続き行われるサイバー攻撃、あなたは守りきれますか？～

独立行政法人情報処理推進機構（IPA）
技術本部 セキュリティセンター
2018年4月

Copyright © 2018　独立行政法人情報処理推進機構

情報セキュリティ10大脅威 2018

- 10大脅威とは？
  - 2006年よりIPAが毎年発行している資料
  - 「10大脅威選考会」の投票により、
    情報システムを取巻く脅威を順位付けして解説


情報セキュリティ
10 大脅威 2018
～引き続き行われるサイバー攻撃、あなたは守りきれますか？～
IPA 独立行政法人情報処理推進機構 セキュリティセンター
2018 年 3 月


1.2. マニュアルの熟読
電源OFF
IoT家電 ご使用 マニュアル
IoT 機器には、マニュアル（取扱い説明書）が付属されている。マニュアルの中には、操作方法に加えて、利用時の注意事項やセキュリティ機能の設定方法等も書かれている。IoT 機器を安全に利用するためには事前に熟読し、内容を理解した上で利用する必要がある。
◆ IoT 機器を箱から出したらマニュアルを読む
購入した IoT 機器を箱から出したら、IoT 機器にケーブルを接続したり、電源を入れる前に、マニュアルを読む。IoT 機器はネットワークにつないで使用するものであり、接続する前に知っておくべきことがある。まずはマニュアルを熟読してから使用開始する。
なお、紙のマニュアルが付属されていない場合は、購入した IoT 機器メーカーや販売代理店のウェブサイト（ホームページ）等で公開されているオンラインマニュアルを熟読する。
◆ マニュアルには大切なことが記載されている
マニュアルには、操作方法に加えて、利用時の注意事項やセキュリティ機能の設定方法等も書かれている。利用時の注意事項を守らないとサイバー攻撃の被害に遭うおそれがある。また、セキュリティ機能は工場出荷時に初期設定されているが、初期設定でセキュリティ機能が無効化されている場合もある。そのため、マニュアルを熟読し、セキュリティ機能の初期設定や設定の変更方法を確認しておく。
◆ 簡易なセットアップガイドだけを読んで満足するのは NG
購入した IoT 機器によっては、購入者がすぐに利用できるように 1~2 ページ程度の簡易なセットアップガイド等が付属している場合がある。セットアップガイドは、必要最低限の手順で IoT 機器を利用できるようになるため便利だが、IoT 機器をより安全に利用するためには、ひと手間かかるが、マニュアルも読むことが望ましい。
6


個人ランク外
3位 ビジネスメール詐欺による被害
～偽の振込・送金依頼に注意～
銀行
「ビジネスメール詐欺」（Business E-mail Compromise：BEC）は巧妙に細工したメールのやりとりにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口である。詐欺行為の準備としてウイルス等を悪用し、企業内の従業員の情報が窃取されることもある。以前は主に海外の組織が被害に遭ってきたが、2016 年以降、国内企業でも被害が確認されている。
＜攻撃者＞
● 犯罪グループ
＜被害者＞
● 組織（企業、金銭の決裁権限を持つ責任者、金銭を取り扱う担当者）
＜脅威と影響＞
組織においてメールの利用がビジネスツールとして定着している中、海外の取引先や経営者等を装い企業の財務担当者等を騙して送金させる、ビジネスメール詐欺による被害が確認されている。
ビジネスメール詐欺で使用されるメールは、巧妙な騙しの手口が使われており、通常の取引のメールと見分けづらいように作成されている。また、取引先のメールアドレスを模したメールアドレスや本物のメールアドレスを使っている場合もあり、受信者は攻撃者からの偽のメールを本物のメールとして取り扱ってしまう。その結果、攻撃者に重要な情報を渡したり、攻撃者が用意した口座へ送金してしまう。ビジネスメール詐欺は組織間での取引のため金銭被害が高額になる傾向があり、組織にとって被害に遭った際の影響が大きい。
＜攻撃手口＞
◆ 取引先との請求書の偽装
取引先と請求にまつわるやりとりをメール等で行っている際に、攻撃者が取引先になりすまし、攻撃者の用意した口座を記入した偽の請求書等を送りつけ、振り込ませる。なお、攻撃者は取引のやりとりをなんらかの方法により盗み見し、取引や請求に関する情報や、関係している従業員の情報を入手した上で攻撃を行なっている。
◆ 経営者等へのなりすまし
企業の経営者等になりすまし、従業員に攻撃者の用意した口座へ振り込ませる。このとき、攻撃者は事前に入手した経営者や関係している従業員等の情報を利用している。
◆ 窃取メールアカウントの悪用
従業員のメールアカウントを窃取し、アカウントを乗っ取った上で、その従業員の取引実績のある別の企業の担当者へ、攻撃者の用意した口座を記入した偽の請求書等を送りつけ、振り込ませる。メール本文は
45

Copyright © 2018 独立行政法人情報処理推進機構

情報セキュリティ10大脅威 2018

- 章構成
  - 1章.情報セキュリティ対策の基本 IoT機器(情報家電)編
    - IoT機器(情報家電)におけるセキュリティ対策の基本を解説
  - 2章.情報セキュリティ10大脅威 2018
    - 脅威の概要と対策について解説
    - 個人と組織の2つの立場で解説
  - 3章.注目すべき脅威や懸念
    - 知っておくべき脅威や懸念を解説

Copyright © 2018 独立行政法人情報処理推進機構

1章. 情報セキュリティ対策の基本
IoT機器（情報家電）編

Copyright © 2018 独立行政法人情報処理推進機構

IoT機器とは

IPA

IoT(Internet of Things):モノのインターネット

IoT機器:インターネットに接続された機器

例えば情報家電であれば・・・

- **生活支援機器**

  冷蔵庫・洗濯機・エアコン・電子レンジ・炊飯器・ロボット掃除機

- **エンターテイメント機器**

  スマートテレビ・DVD/Blu-ray/HDDレコーダー・ビデオカメラ・オーディオコンポ・ゲーム

- **ヘルスケア機器**

  体組成計・血圧計・活動量計

- **ネットワーク機器**

  ホームルータ・モバイルルータ・ネットワークカメラ・スマートリモコン・スマートスピーカー

Copyright © 2018 独立行政法人情報処理推進機構

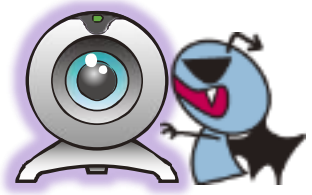
IoT機器を狙った脅威

- 初期設定のまま利用しているIoT機器に感染するウイルスの存在
  - 初期設定のまま利用しているIoT機器がMiraiと呼ばれるウイルスに感染
  - 遠隔操作され、TwitterやAmazon.com等のサービスが一時利用不能

- IoT機器の脆弱性を悪用して感染するウイルスの登場
（Miraiの亜種）

- IoT機器を破壊するウイルスの登場（BrickerBot）

- ウイルスに感染し、ネットワークカメラを覗き見される場合も



Copyright © 2018 独立行政法人情報処理推進機構

被害に遭う要因

利用者がネットワークにつながるメリットのみを理解し、デメリットとしてネットワーク越しに攻撃される可能性があることを理解していない

- IoT機器をほぼ初期設定のまま使っている
- 攻撃に対するセキュリティ対策が不十分
- セキュリティ機能の設定が難しい、面倒だ等の理由により、適切に設定されていない

IoT機器の利用者は

IoT機器はネットワークにつながる機器であり、ネットワークの外部にいる悪意を持った攻撃者から攻撃されるおそれがあるという認識を持って、IoT機器を適切に利用する。

Copyright © 2018 独立行政法人情報処理推進機構

被害に遭わないための対策

■ ライフサイクルを意識した対策が必要

IoT機器の購入前
- 事前調査

ネットワーク接続前
- マニュアルの熟読
- パスワードの変更
- 設定の見直し

ネットワーク接続後
- アップデートの実施
- 使用しないときは電源オフ

IoT機器の廃棄時
- 廃棄・譲渡前の初期化

■ その他の対策

- IoT機器対応セキュリティ機器の導入検討
- 既存のIoT機器の見直し

Copyright © 2018 独立行政法人情報処理推進機構

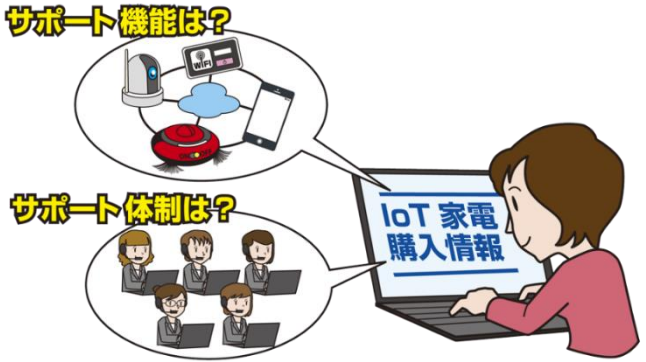
事前調査

セキュリティ機能の確認

- IoT機器の持つセキュリティ機能を使って攻撃を防げる可能性有
- 購入前にIoT機器に十分な機能があるかを確認
  - IoT機器と通信可能な端末（PCやスマートフォン等）を制限する機能
  - IoT機器の利用時やIoT機器との通信時の認証（ログイン）機能
  - 認証の際に利用するパスワード等を変更する機能
  - 自動アップデート機能
  - 個人情報や設定の初期化機能

サポート体制の確認

- IoT機器はメーカーや販売店の違いによりサポート体制が異なる
- 購入予定のIoT機器がどのようなサポート体制になっているかを確認
  - 脆弱性公開時のアップデートの提供頻度
  - 日本語問い合わせの可否
  - サポート終了時期



Copyright © 2018 独立行政法人情報処理推進機構

マニュアルの熟読

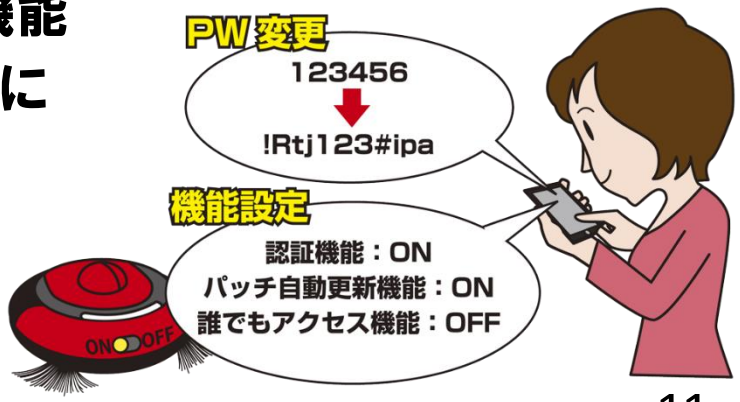
- **マニュアルには大切なことが記載**
  - マニュアルには利用時の注意事項やセキュリティ機能の設定方法が記載
  - 利用時の注意事項を守らないとサイバー攻撃の被害に遭うおそれ

- **箱から出したらマニュアルを読む**
  - IoT機器にケーブルを接続したり、電源を入れる前にマニュアルを読む
  - ただし、簡易なセットアップガイドだけを読んで満足するのはNG

Copyright © 2018 独立行政法人情報処理推進機構

パスワードの変更 / 設定の見直し

- IoT機器へのアクセスに使うパスワードを変更
  - 初期設定のパスワードからセキュアなパスワードに変更する
- IoT機器の設定を見直す
  - 使わない機能を無効化
  - 初期設定の見直し（必要な機能を有効化する等）
- セキュリティ機能を有効化
  - IoT機器と通信可能な端末を制限する機能
  - IoT機器の利用時やIoT機器との通信時にログイン（認証）を要求する機能
  - 自動アップデート機能



Copyright © 2018 独立行政法人情報処理推進機構

アップデートの実施

ネットワークに接続したらアップデート

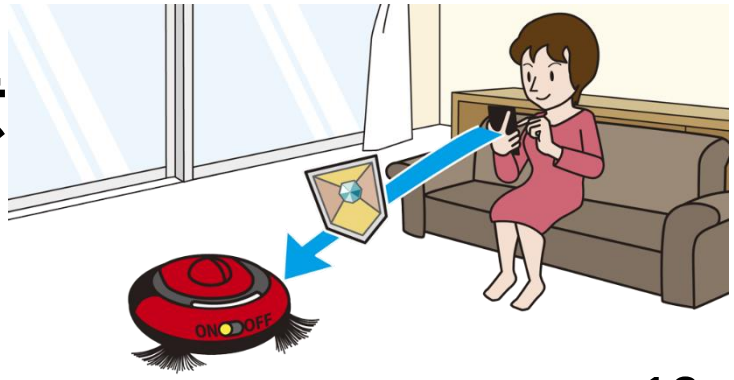
- 購入直後でも古いソフトウェアがインストールされている可能性有
- 最初にネットワークに接続した際に、アップデートを実施する

定期的にアップデート

- 利用開始後も新しいソフトウェアが公開される可能性有
- 定期的にソフトウェアの有無を確認し、公開されていたらアップデートする
- 自動更新機能がある場合は有効化する
- 管理用アプリがある場合は、そのアプリもアップデートする

サポート終了したIoT機器は注意

- 脆弱性等があっても新しいソフトウェアが公開されない
- IoT機器の利用を停止する



Copyright © 2018 独立行政法人情報処理推進機構

使用しないときは電源オフ

- IoT機器を使用しないときは電源オフ
  - 常時使わないIoT機器や使用しなくなったIoT機器は電源オフする
  - 電源オフすることでウイルス等を駆除できる可能性がある

- IoT機器の安定稼働
  - 常時起動しているIoT機器であっても定期的に電源オフする
  - ウイルスを駆除したり、IoT機器の安定稼働につながる

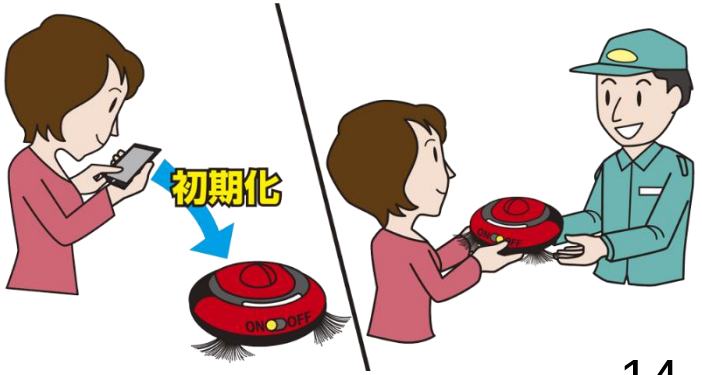
Copyright © 2018 独立行政法人情報処理推進機構

廃棄・譲渡前の初期化

- IoT機器内には重要情報が存在
  - ユーザー名(ID)やパスワード
  - GPS情報(自宅や個人の行動履歴)
  - クレジットカード情報

- IoT機器を廃棄・譲渡する前に初期化
  - 初期化機能がある場合は、初期化を実施する
  - 初期化機能がない場合は、物理的に破壊する
  - 専門の廃棄業者に依頼する等の適切な廃棄を実施する

- 管理用アプリのアンインストール
  - 管理用アプリがある場合は忘れずに
    スマートフォン等からアンインストール



Copyright © 2018 独立行政法人情報処理推進機構

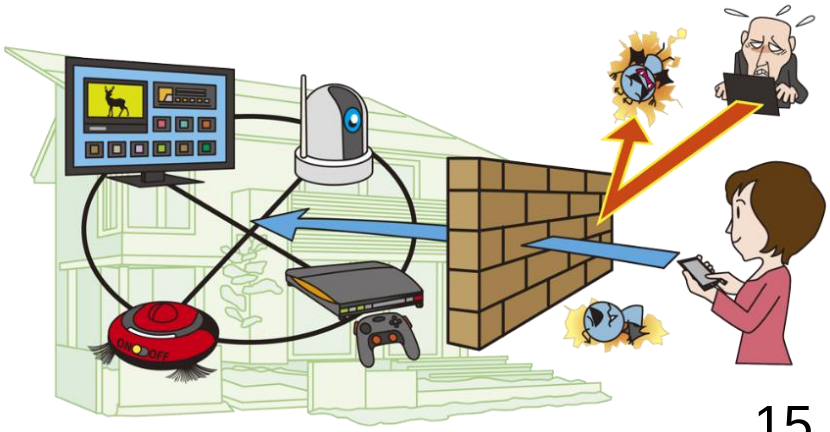
その他の対策

IoT機器対応セキュリティ機器の導入検討

- ルーター等に接続してセキュリティを保護するセキュリティ機器が存在
- 導入することで、ウイルス感染、不正遠隔操作や情報漏えいを防止する
- 1年毎等定期的な利用継続の更新が必要
- 費用対効果を考え、継続利用する場合は更新する

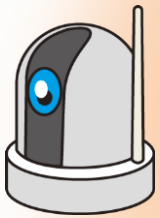
既存のIoT機器の見直し

- 新しく購入したIoT機器以外に既に使っているIoT機器がある場合、この機会にパスワードや設定等を見直す



Copyright © 2018 独立行政法人情報処理推進機構

付録：情報セキュリティ船中八策
IoT機器（情報家電）編



情報セキュリティ船中八策
―IoT機器（情報家電）編―

一、事前調査
～後悔先に立たず～

二、マニュアルの熟読
～初心忘れるべからず～

三、パスワードの変更
～敵に塩を送ることのなきように～

四、設定の見直し
～転ばぬ先の杖～

五、アップデートの実施
～善は急げ～

六、使用しないときは電源オフ
～火のないところに煙は立たぬ～

七、廃棄・譲渡前の初期化
～立つ鳥跡を濁さず～

八、IoT機器対応セキュリティ機器の導入検討
～予防は治療に勝る～

Copyright © 2018 独立行政法人情報処理推進機構

本資料に関する詳細な内容は

- 以下のページのPDF資料をご覧ください。

情報セキュリティ10大脅威 2018
https://www.ipa.go.jp/security/vuln/10threats2018.html

Copyright © 2018 独立行政法人情報処理推進機構

Copyright © 2018 独立行政法人情報処理推進機構