多様化する IoT のセキュリティ脅威とその対策

多様化する IoT のセキュリティ脅威

- IoT機器に感染するウイルスの多様化
  - IoT機器のMirai等の感染に対抗する「Hajime」
    感染した機器のポートを閉じて、他のウイルスの感染を防御。善意の警告メッセージ
  - IoT機器を破壊する「BrickerBot」
    機器に致命的な改変を与えて最終的に使用不能に。全世界で1,000万台以上が被害
  - 続々と登場する「Mirai」の亜種：PERSIRAI, Reaper (IoTroop, IoT reaper), Satori/Okiru
    特定のIoT機器固有の脆弱性を突いて感染、初期パスワードから変更しても防御不能
  - 仮想通貨マイニングへの悪用
- 脆弱性を有するIoT機器の散在、国内に広がる感染被害
  - 利用者に対する脅威（映像・音声漏えい、情報漏えい、不正遠隔操作）
  - 第三者に対する脅威（IoTボットネットによる大規模DDoS攻撃）

開発者・製造者の対策

- 設計段階からセキュリティを考慮（セキュリティ・バイ・デザイン）
  - システムの全体構成の明確化
  - 保護すべき情報・機能・資産の明確化
  - 「脅威分析」　保護対象に対する脅威の明確化
  - 「対策検討」　対策候補の洗い出し、
    脅威・被害・コスト等を考慮した選定
- セキュリティ対策の継続的サポート
  （脆弱性対応、S/W更新）

☞ 「IoT開発におけるセキュリティ設計の手引き」

☞ 「IoT製品・サービス脆弱性対応ガイド」

利用者・運用者の対策

- 購入前／導入前の事前調査
- 使用開始前の説明書の確認
- 適切な機器設定（パスワード変更、不要管理機能停止等）
- ネットワーク接続における対策（ルータ経由での接続等）
- アップデートの実施（更新ソフトウェアの適用）
- 廃棄時のデータ消去

☞ 「増加するインターネット接続機器の不適切な情報公開とその対策」

☞ 「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

IoT 開発におけるセキュリティ設計の手引き
https://www.ipa.go.jp/security/iot/iotguide.html

IoT 製品・サービス脆弱性対応ガイド
https://www.ipa.go.jp/security/fy29/reports/vuln_handling/index.html#L3

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

増加するインターネット接続機器の不適切な情報公開とその対策
https://www.ipa.go.jp/security/technicalwatch/20160531.html

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