資料２－４

IoTのセキュリティ向上に向けて

吉岡克成（横浜国立大学）

サイバーセキュリティタスクフォース（2017/3/8）

アジェンダ

- IoTセキュリティの現状
- IoT機器と脆弱性のカテゴリ
- 対策について

IoTセキュリティの現状

- **多種多様な機器のマルウェア感染**
  - 218か国、500種類以上、130万IPアドレス/月の感染IoT機器からの攻撃を観測（横浜国大）
  - Telnet等の脆弱なサービスが原因
  - 1Tbpsを超えるDDoS攻撃 [1]

- **重要IoT機器のセキュリティ設定・機能不備**
  - 病院等重要施設の水処理プラントの管理画面がだれでも閲覧可能な状態 [2]
  - 重要機器の類似事例を多数確認（横浜国大）

[1] http://securityaffairs.co/wordpress/51640/cyber-crime/tbps-ddos-attack.html
[2] http://www9.nhk.or.jp/kabun-blog/200/259546.html

事例紹介：誰でも管理画面にアクセス可能な水処理プラント

- 水処理プラントの管理画面がインターネット側からアクセス可能なまま運用.
- 水処理プラントが設置されている具体的な施設名（病院、大規模商業施設、ホテル等）やプラントの動作状況が閲覧可能

- 指摘により施設名の匿名化、トップページでの認証等の対応を実施

2016/12/21
NHKニュース7
ニュースウォッチ9

IoT機器と脆弱性カテゴリ

- 脆弱性
  - 脆弱性カテゴリ1：マルウェアに感染し、攻撃者に制御を乗っ取られる（例：Telnet辞書攻撃，CWMP脆弱性，WebUI脆弱性など）
  - 脆弱性カテゴリ2：管理画面から機器の設定変更をしたり、機器に関する情報にアクセス可能（例：管理用WebUIの認証がない、または、脆弱な機器）
  - 脆弱性カテゴリ3：機器の存在、種別が遠隔から把握できる（例：管理用WebUIが外部からアクセス可能な機器）
- 機器重要度
  - 重要度カテゴリ1：利用者の生活や生命に直接影響を及ぼす可能性がある重要な機器（工業制御システム，重要インフラ，HEMSなど）
  - 重要度カテゴリ2：重要機器以外

＃数字が低いほど深刻

	脆弱性カテゴリ1（マルウェア感染・乗っ取り）	脆弱性カテゴリ2（設定変更・情報アクセス）	脆弱性カテゴリ3（機器存在露見）
重要度カテゴリ1：重要機器	非常に深刻	深刻	場合によって深刻（DoSの対象になるなど）
重要度カテゴリ2：重要機器以外	深刻	場合によって深刻	深刻ではない（ただし脆弱性カテゴリ1や2にエスカレートする可能性）

アジェンダ

- IoTセキュリティの現状
- IoT機器と脆弱性のカテゴリ
- **対策について**

IoTのセキュリティ向上（国内向け）

状況把握（定常的に実施）

- サイバー攻撃観測網（NICTER, ハニーポット等）による感染機器把握
- 能動的観測機構（日本版Shodan/Censys）による機器状況の把握
- 機器情報、脆弱性情報の集約（メーカ、運用者、研究者窓口）

緊急性高

短期的対策

- ISPによる通知、ブロック、切り離しなど
- メーカ、運用者、所持者への情報提供、対策の促し

中長期的対策

- ガイドライン・認証制度（検証環境構築）
- セキュアなプラットフォーム（セキュリティバイデザイン）
- IoTセキュリティゲートウェイ

IoTのセキュリティ向上（国内向け）