本スライドは、当日のセミナー資料の一部を抜粋したものです。

つながるIoTシステムのセキュリティ確保にむけて
～ハッカーによる攻撃の現状と対策ポイント～

2015年11月
重要生活機器連携セキュリティ協議会　事務局長
伊藤 公祐

アジェンダ

1. IoTシステムとハッカーの視点
   – IoTシステムに対する脅威と攻撃事例

2. IoTシステムの標準化動向
   – 2-1　欧州/米国の動向
   – 2-2　日本の動向

3. IoTシステムのセキュリティ対策ポイント
   – 3-1　脆弱性を知る
   – 3-2　V字開発プロセスでのセキュリティ対応手法
   – 3-3. 具体的なセキュリティ検討方法
   – 3-4　CVSSにおける脅威分析手法

IoTシステム攻撃者の視点

- ターゲット
  ⇒コントロールを奪えると「高価値」なもの（人命、コンテンツ、社会的影響など）の自由を奪えるもの
  （= Return on Investmentの高いもの）

- どういう仕組みで動いているか、まずは分解してみる

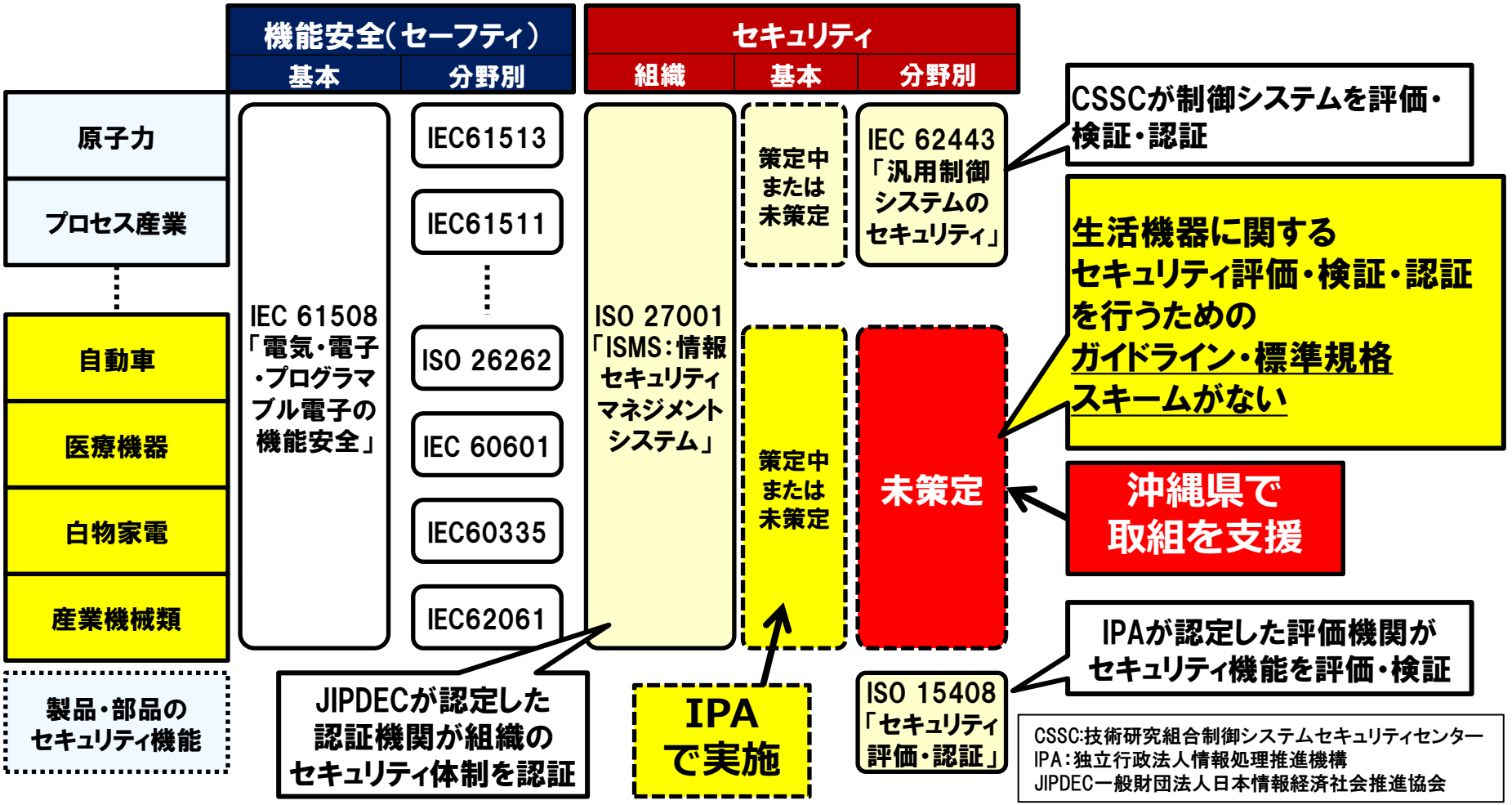
- 攻撃手法は基本的に組込み開発者のデバッグ手法と同じ

- IoT製品のコントロール（プロトコルメッセージやプログラム/FWアップデート）を奪える糸口を地道に探す
  （＝リバースエンジニアリングする）

- できるだけPC/インターネットサーバ、汎用I/Fのハッキング技術を流用する
  - USB、Ethernet、WiFI、BlueTooth、JTAG、GPIO、UART…

機能安全とセキュリティ

- IoT普及において、セキュリティ懸念が増しているが、IoT向け生活機器のセキュリティ標準が未整備。



IoTシステムの脅威分析の課題

コネクテッド	IoTデバイスはNW/SW/クラウドを総合して活用するため**脅威の対象が幅広い**
サイバーフィジカル	IoTデバイスは組込み機器の一つであり、**人や現実社会に直接影響する**製品がある
スマートシステム	IoTデバイスは最大1秒程度のリアルタイムに動作し、**人の介在なしで**自動化するため深刻になりやすい（コントローラビリティの喪失）
機械への依存	IoTデバイスへの依存度が高く、緊急時・災害時を含め**常に正常動作することが期待される**
複雑さ	IoTデバイスは多数の機器が分散するため**システムが非常に複雑**で脅威分析しにくい

IoTセキュリティ対策にむけて

- 課題
  - ET (Embedded Technology)とIT (Information Technology)の双方の技術知識が求められる
  - IoTサービスを構成するシステム全体の視点と構成要素ごとのセキュリティ対応の役割分担
  - システム更新機能の悪用対策
  - 新しい技術と脆弱性への対応
  - 攻撃者の一歩先で対応

- 対策
  - ステークホルダによる議論
  - 設計段階での脅威分析とリスク対策の取捨選択（コストバランス）
  - 自動化されたツールによる広範囲の脆弱性評価テスト
  - 第三者による（客観的な）セキュリティ評価