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向けて
～IoTセキュリティを実践するための設計ポイント～

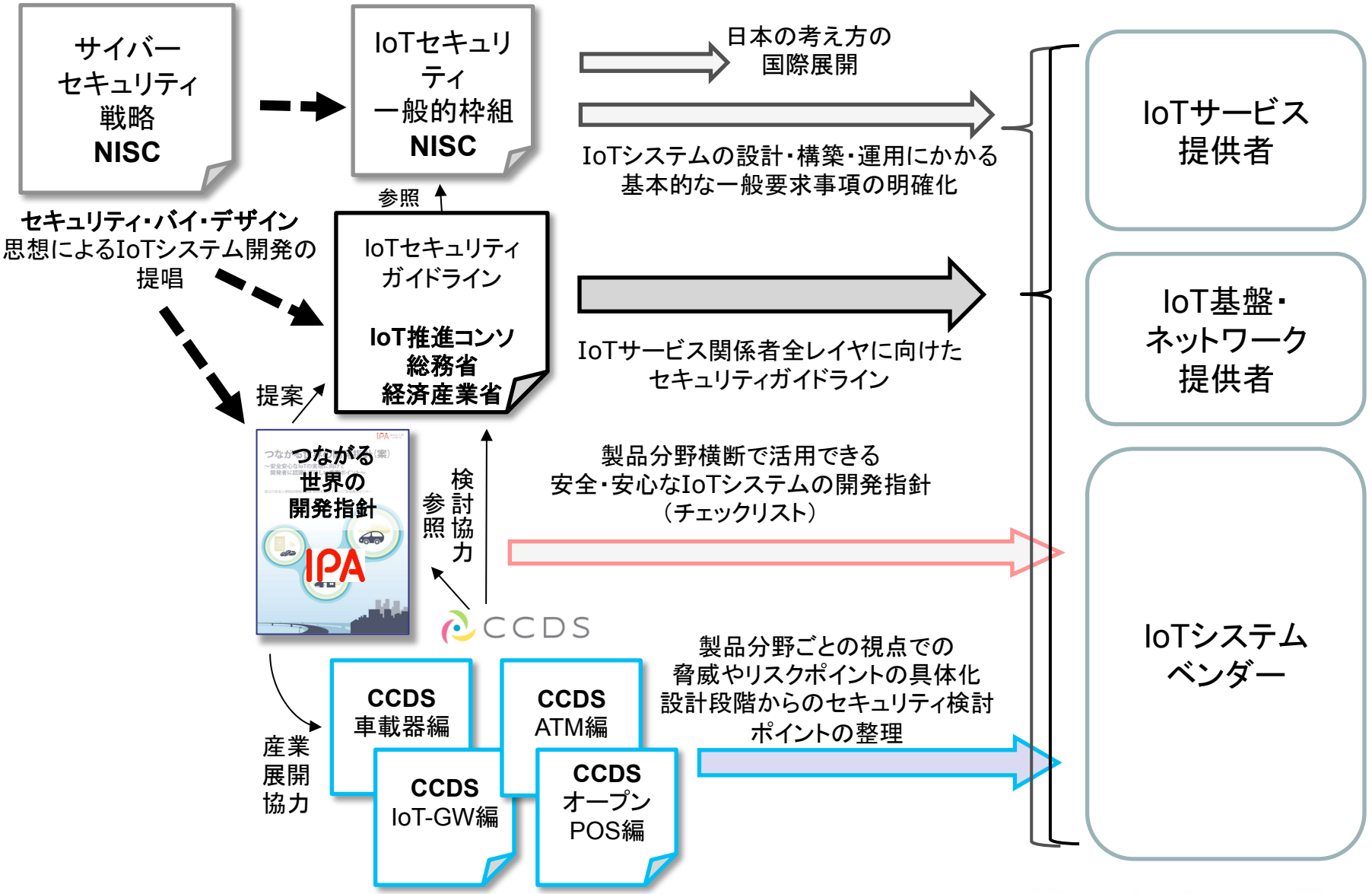
一般社団法人
重要生活機器連携セキュリティ協議会
（CCDS）
専務理事・事務局長　伊藤公祐

本日の内容

1. 昨年の簡単なおさらい
2. IoTをセキュアにするための関連ガイドライン
3. 脅威分析とリスク評価手法
4. 対策を打つべき脅威の見極め方
5. セキュアな製品かの検証方法の事例紹介
6. まとめ

主なガイドラインの関係

CCDS分野別ガイドラインの位置づけ(私見)



3．脅威分析とリスク評価手法（車載器編）

■リスク特性の項目

項番	項目	内容
1	対象機器	脅威に晒されている機器。
2	分野固有・共通	参照☞「（1）分野固有・共通」
3	脅威の分類	脅威の分類の事例をリストアップ。 参照☞「（2）脅威の分類」 その分類基準は以下の通り。 **①利用者の操作に起因するもの。** **⇒“設定ミス／ウィルス感染”** **②攻撃者による攻撃手段が明確なもの。** **⇒“盗聴／Dos攻撃／偽メッセージ／不正中継”** **③攻撃者による攻撃手段が不明確、もしくは上記に該当しないが被害を被った場合、以下に該当しているもの。** **⇒“不正設定／情報漏えい／ログ喪失”** **上記の①②に該当しない場合は、“不正利用”とする。**
4	接続I/F（侵入ルート）	参照☞「（3）接続I/F（侵入ルート）」
5	who 誰がつなげたか	参照☞「（4）who 誰がつなげたか」
6	whom 何が危害をうけたか	参照☞「（5）whom 何が危害をうけたか」
7	where どこで発生したか	参照☞「（6） where どこで発生したか 」

4. 対策を打つべき脅威の見極め方

- 対象システムの定義
  - システム構成、システムの連携先、システム設置時から運用中に関連するプレイヤー（登場人物）とそのプレイヤーの権限
- システム対する脅威の洗い出し
  - 前述の「脆弱性の例」やIPAなどから出されている資料（自動車の情報セキュリティ取組みガイド、IoTシステム開発手引きなど）、過去の攻撃事例を参考に実施
- 洗い出した脅威の発生ルートを想定し、リスク評価を実施
  - リスクを見落とさないためにも、複数手法での評価を推奨
- 赤・オレンジレベルになった脅威が優先的に対策を打つべきもの
  - 過去の脅威分析・リスク評価の経験値を積み上げて、過去の脅威分析に照らして、優先度の見極め速度を上げていく

5. セキュアな製品かの検証方法の事例紹介

◆セキュリティ検証の種類

①静的検証

・ソースコードを解析し脆弱性の有無を検査

ソースコード解析レビュー、コーディング規約検証

②動的検証

・アプリケーション動作状態でのアタック検査

・ネットワーク、サーバ設定を含めた検査

ファジング、脆弱性スキャン、ペネトレーション

セキュリティ検証での特徴