ガイドラインラッシュから国際標準の動向

2018年2月26日（月）

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　伊藤 公祐

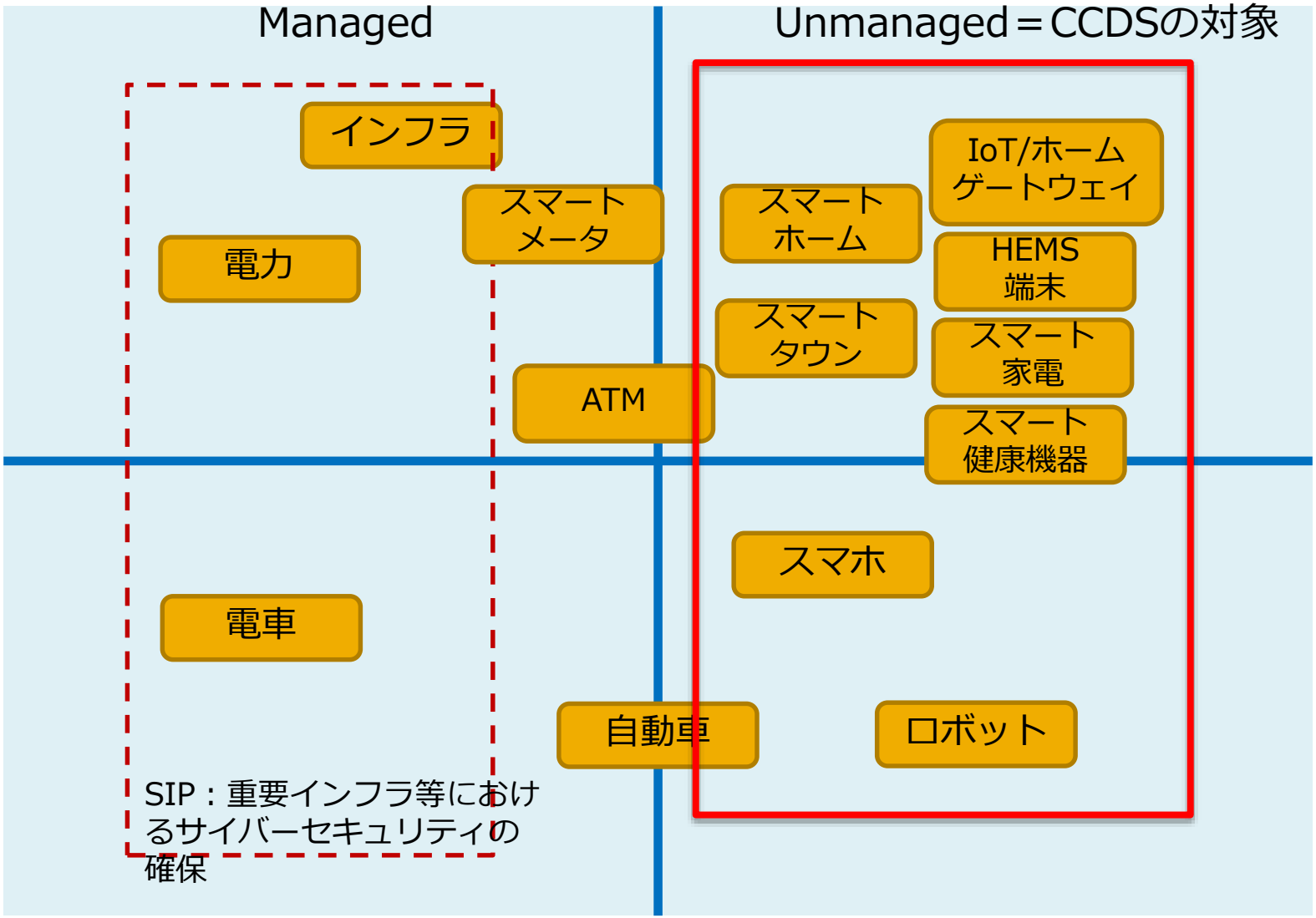
CCDSの概要

- 名称：一般社団法人 重要生活機器連携セキュリティ協議会
  - 英名：Connected Consumer Device Security council (CCDS)
- 設立：2014年10月6日
- 会長：徳田英幸（情報通信研究機構　理事長、慶應大学 教授）
- 代表理事：荻野 司（京都大学 特任教授）
- 専務理事・事務局長：伊藤 公祐（ゼロワン研究所）
- 理事：後藤厚宏（情報セキュリティ大学院大学 教授、SIP：PD）
  長谷川勝敏（イーソル㈱ 代表取締役社長）
  服部博行（株式会社ヴィッツ 代表取締役社長）

- 会員数：163（正会員以上：44、一般会員：90、学術系：16、協賛:13）(2018年1月)

- 主な事業：
  1. 生活機器の各分野におけるセキュリティに関する国内外の動向調査、内外諸団体との交流・協力
  2. 生活機器の安全と安心を両立するセキュリティ技術の開発
  3. セキュリティ設計プロセスの開発や検証方法のガイドラインの開発、策定および国際標準化の推進
  4. 生活機器の検証環境の整備・運用管理及び検証事業、セキュリティに関する人材育成や広報・普及啓発活動等

IoT環境で対象とするシステム



慶應義塾大学教授/CCDS会長 徳田英幸氏「IoTセキュリティの課題」
CCDSにて修正（ATM、スマートメータ部）

CCDSが取り組む事業分野

検証基盤構築

・検証業務をサポートする共通基盤開発
－組込み機器評価・検証基盤システム

・セキュリティ検証ツール開発
－車載、IoT-GW、ATM、POS分野

・テストベット検討

標準化推進

・セキュリティガイドライン策定
－セキュリティガイドラインWG
（車載、IoT-GW、ATM、POS-SWG）

・IoTセキュリティ対策技術の体系化
－デバイスセキュリティ技術SWG
－ユーザビリティWG

・ガイドライン国際標準化検討

人材育成

・オープンセミナーの開催
－セキュリティシンポジウム
－検証技術セミナー
－CCDSガイドライン勉強会　.etc

・ワークショップの開催
－検証ツールハンズオン講習会
－IoTセキュリティ評価検証
技術講習会

CCDS

動向調査・研究

・国内外のガイドライン、標準化動向

・検証手法、検証ツールの調査・研究

・脅威事例の収集、ハッキング技術調査

・認証制度の実現に向けた調査

普及啓発

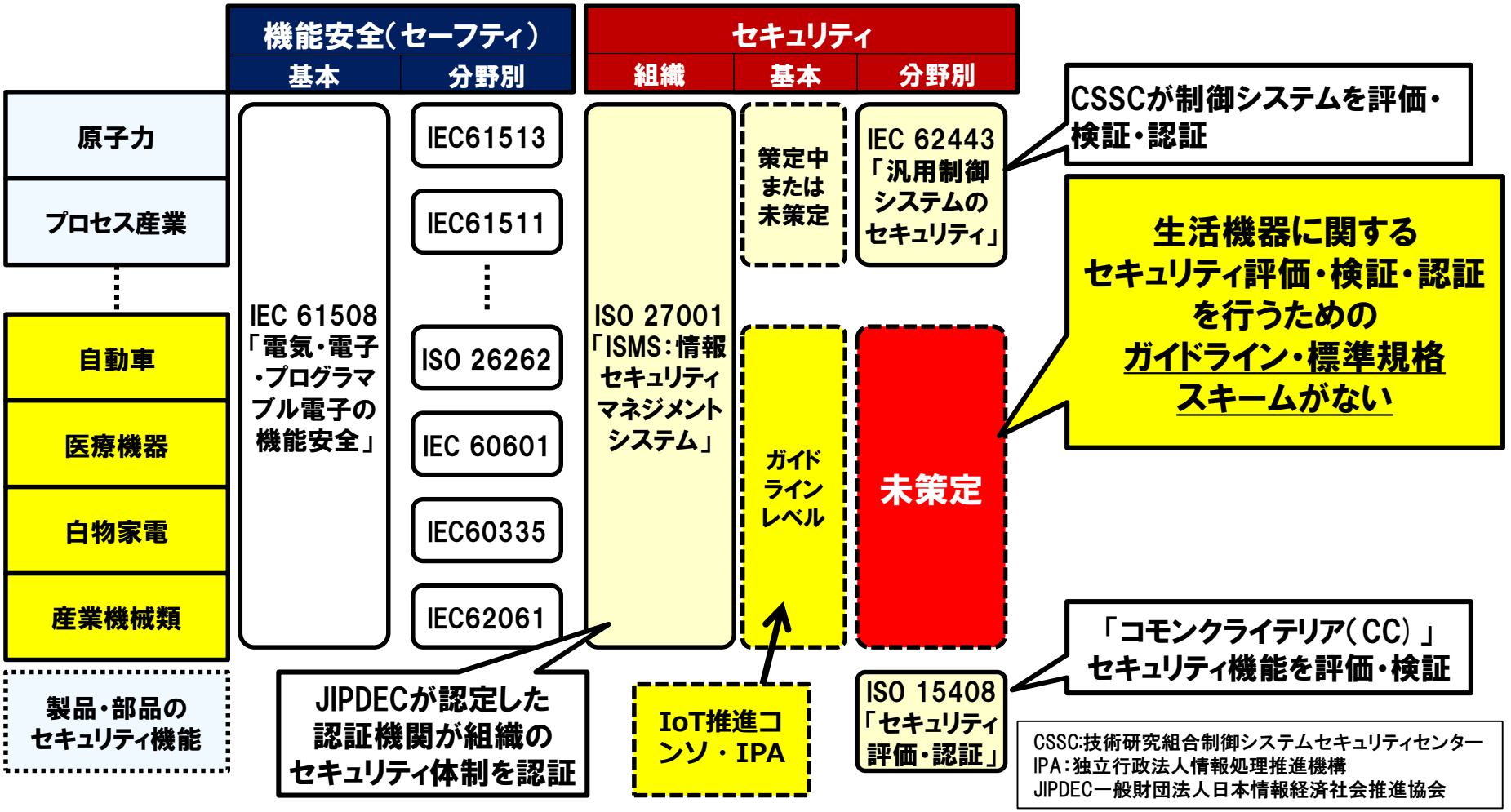
・シンポジウム、セミナーの主催

・調査資料、ガイドラインの公開

・提携団体での講演活動

CCDS発足当初の状況

- 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セキュリティガイドラインの例（海外）

- Dept. of Homeland Security
  - STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)
- oneM2M:
  - Security Solutions v2.4.1 (TTCより日本語版あり)
  - Security v2.0 (TR analysis)
  - End-to-End Security and Group Authentication v2.0
- CSA:
  - Security Guidance for Early Adopters of the Internet of Things (IoT)
  - Identity and Access Management for the Internet of Things – Summary Guidance
  - Security Guidance for Smart Health, for Smart Cities, for Smart Retails
  - Analysis of Hardware Security Options for the IoT
  - Checklist for Secure IoT Device Development
  - Internet of Things (IoT)インシデントの影響評価に関する考察 (CSAジャパンより日本語版あり)
  - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products（同上）
- OWASP
  - IoT Security Guidance (Draft)
    - https://www.owasp.org/index.php/IoT_Security_Guidance
- GSMA:
  - IoT Security Guidelines (Overview, for Service Eco-Systems, for End Point Eco-Systems, and for Network Operators)
  - IoT Security Self-Assessment
- SAE:
  - J3061（Cybersecurity Guidebook for Cyber-Physical Vehicle)
- Continua Health Alliance
  - End-to-End Security for Personal Telehealth

他にもいっぱいあると思います…

IoTセキュリティガイドラインの例（国内）

- NISC（内閣サイバーセキュリティセンター）
  - 「IoTセキュリティ一般的枠組み」
    - http://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf
- IoT推進コンソーシアム（IoTセキュリティWG）・総務省・経済産業省
  - 「IoTセキュリティガイドライン」
    - http://www.iotac.jp/wg/security/
- IPA
  - 「つながる世界の開発指針」
    - https://www.ipa.go.jp/files/000051411.pdf
  - 「つながる世界の開発指針の実践に向けた手引き＜高信頼化機能編＞
    - https://www.ipa.go.jp/files/000059278.pdf
- JNSA（IoTセキュリティWG）
  - 「コンシューマー向けIoTセキュリティガイド」
    - http://www.jnsa.org/result/iot/data/IoTSecurityWG_Report_Ver1.pdf
- CCDS
  - 「分野別セキュリティガイドライン」
    車載器編、IoT-GW編、オープンPOS編、ATM編
    - CCDSホームページ「公開資料」コーナーで一般公開中！
    - https://www.ccds.or.jp/public_document/

他にもあるかも…

2016年は国内外で
ガイドラインラッシュ

分野別セキュリティガイドライン

沖縄県 生活機器セキュリティ基盤形成促進事業

CCDS

・分野別ガイドラインv1：2016年6月リリース
・同英語版：2017年4月リリース
・分野別ガイドラインv2：2017年5月リリース

IPA「つながる世界の開発指針」やIoT推進コンソーシアム/総務省/経済産業省「IoTセキュリティガイドライン」を上位概念として、製品分野ごとに対策すべき脅威が異なることから、各分野ごとの視点でセキュリティの取組みを整理し、各業界にセキュリティ・バイ・デザインの考え方を理解しやすくする。

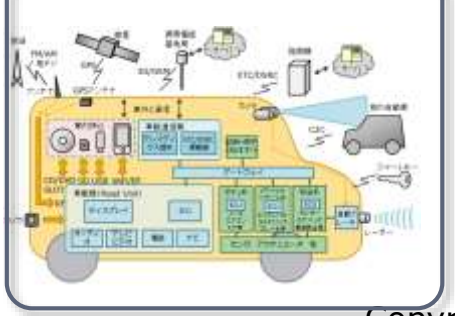
対象分野

・車載器　　・ATM（金融端末）
・IoT-GW　　・POS（決済端末）

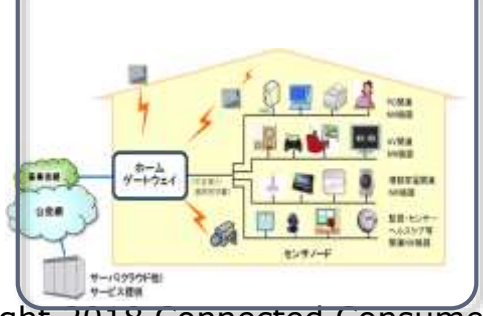
ガイドラインの主な内容と改良点

・対象とするシステム構成
・想定されるセキュリティ上の脅威
・製品ライフサイクルの各フェーズにおけるセキュリティの取組み
（IPA「つながる世界の開発指針」やIoT推進コンソーシアム「IoTセキュリティガイドライン」との相関表）
・脅威分析・リスク評価の方法
・製品全体およびセキュリティ対策機能の第三者セキュリティ評価
・別冊読本の追加
（実践的ケーススタディ、べからず集など）

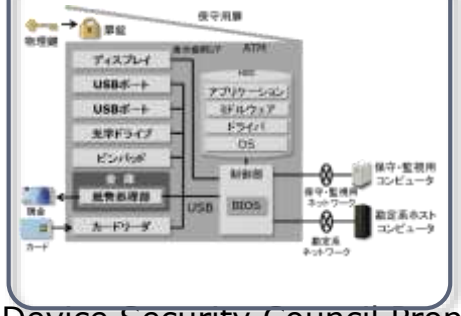
車載器システム構成



IoT-GW：ホームGWケース



ATMシステム構成



POSシステム構成

さらに、、、
IoTセキュリティ評価・検証ガイドライン

目的

製品分野別セキュリティガイドラインがIoT機器の開発者向けだったのに対し、IoT機器品質評価者向けに、セキュリティ評価に必要な基本プロセスと具体的な評価方法をガイドラインとして整理した※1

ガイドラインの特徴

- **ISO/IEC/IEEE 29119、NIST SP800-115といった国際標準を参考に策定**
- **スマートホーム分野での実例を交え、IoT機器全般を対象に、具体的なセキュリティの評価検証プロセスを体系的に整理**

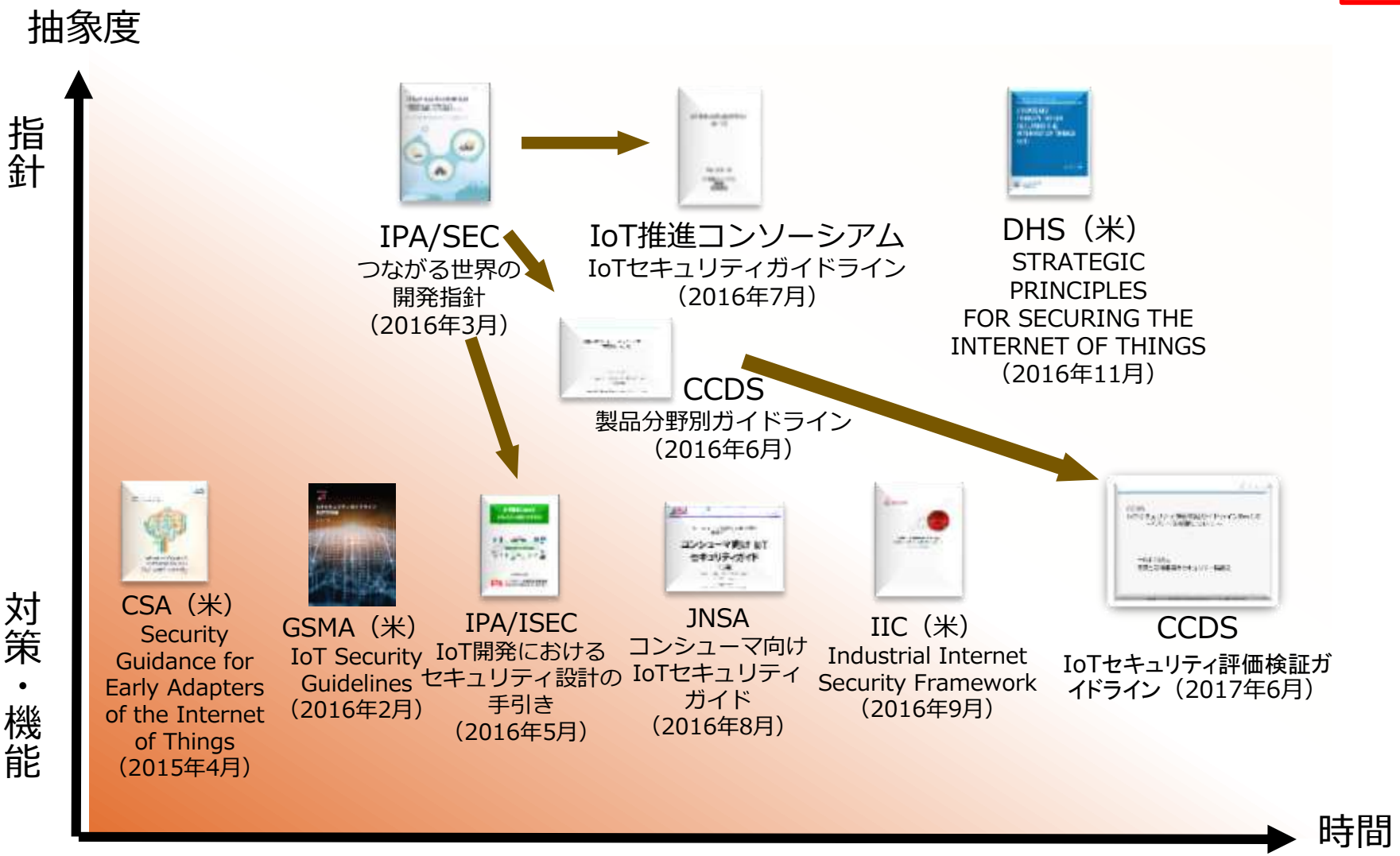
ガイドラインの主な内容

- **評価検証仕様書の策定手順の解説**
  - **リスク分析から対策の立案、評価検証ツールの選定方法、テストケース策定までを網羅**
  - **どこまで評価検証すべきか、評価検証（監査）レベルの定義事例を参考掲載**
- **検出されたインシデント（脆弱性）レポート記載要件の定義**
  - **IPA-ESBRガイドラインを基に記載要件を整理**
  - **深刻度指標のリスク評価手法の解説**
- **豊富な参考資料**
  - **脆弱性評価検証ツールリスト**
  - **スマートホーム脆弱性評価検証仕様書**
  - **リスク評価手法（CVSSv3他9種）**

※1「総務省 身近なIoTプロジェクトに参画したゼロワン研究所の成果を基にCCDSのガイドラインとして整備
※2「CCDS製品分野別セキュリティガイドライン Ver.1.0」に準拠し「評価・検証」フェーズを詳細化

IoT関連の主なセキュリティガイドライン

参考



出典：CCDS沖縄セキュリティウィークパネルIPA田丸氏資料を改変

CCDS分野別ガイドラインの位置づけ

サイバーセキュリティ戦略
NISC

IoTセキュリティ一般的枠組
NISC

2016年7月リリース

日本の考え方の国際展開

IoTシステムの設計・構築・運用にかかる基本的な一般要求事項の明確化

セキュリティ・バイ・デザイン思想によるIoTシステム開発の提唱

参照

IoTセキュリティガイドライン

IoT推進コンソ
総務省
経済産業省

IoTサービス関係者全レイヤに向けたセキュリティガイドライン

提案

2016年3月リリース

検討協力
参照

製品分野横断で活用できる安全・安心なIoTシステムの開発指針（チェックリスト）

CCDS

産業展開協力

CCDS 車載器編

CCDS ATM編

CCDS IoT-GW編

CCDS オープンPOS編

製品分野ごとの視点での脅威やリスクポイントの具体化
設計段階からのセキュリティ検討ポイントの整理

2016年6月リリース

2017年5月末
改訂版リリース

IoTサービス提供者

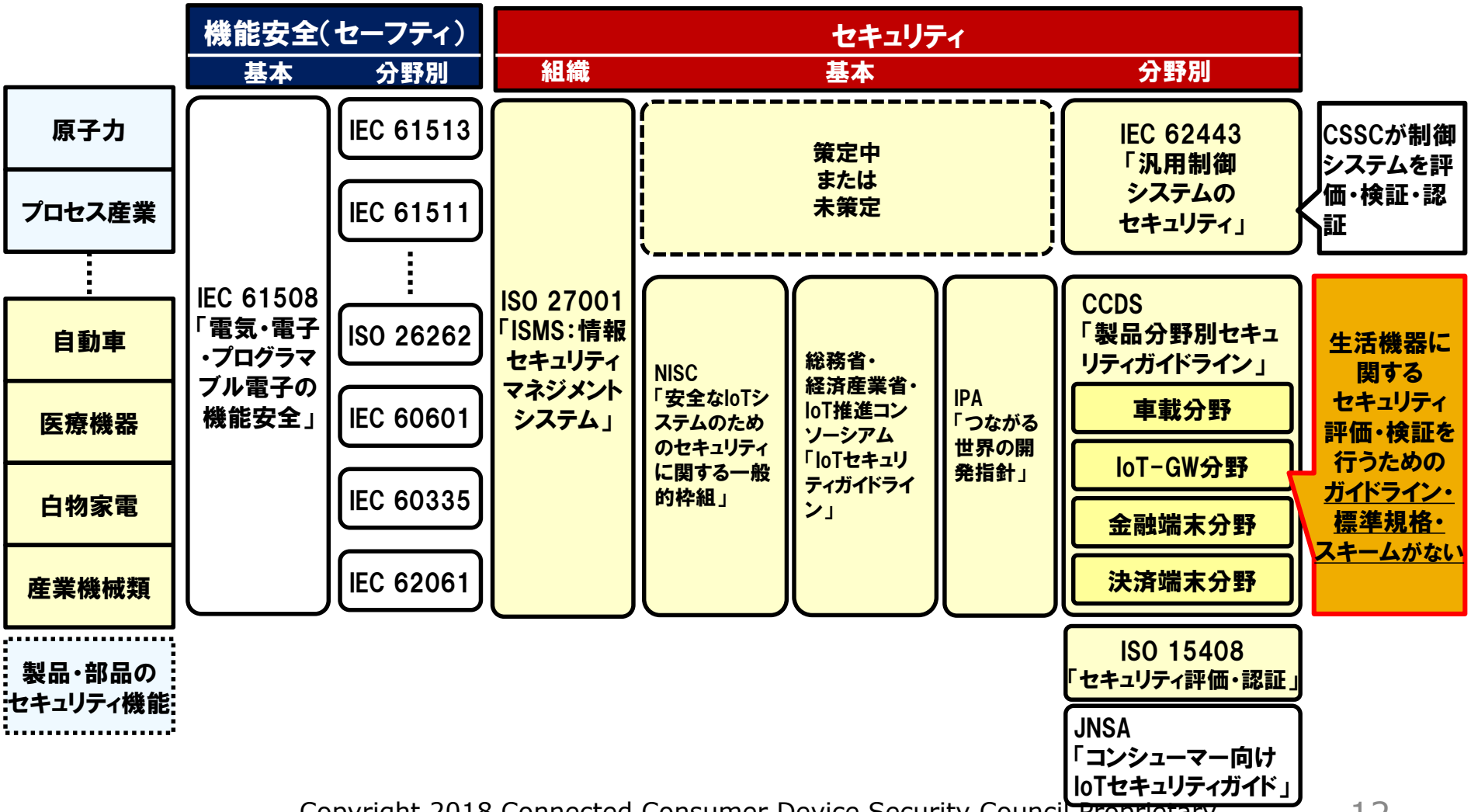
IoT基盤・ネットワーク提供者

IoTシステムベンダー

規格・標準策定状況

＜セーフティとセキュリティの国際規格の策定状況＞

NISC：内閣サイバーセキュリティセンター
CSSC:技術研究組合制御システムセキュリティセンター
IPA：独立行政法人情報処理推進機構
JIPDEC一般財団法人日本情報経済社会推進協会
JNSA：特定非営利活動法人 日本ネットワークセキュリティ協会



ガイドラインから国際標準化へ

- ISO/IEC JTC1 SC27/WG4およびSC41 国内委員会が始動
  - ISO/IEC JTC1 SC27/WG4：
    - 日本のIoTセキュリティガイドラインをベースに、米国CSAなどからの提案を加味した目次案を検討中。10月下旬のベルリン会合にてNew Work Item化。
  - ISO/IEC JTC1 SC41：
    - 「IoTを安全にするための一般的要求事項」として明文化することで文書の目的を検討中。IoTシステムの高信頼化（Trustworthiness）のための設計要求事項を導出する考え方とする方向。

ガイドラインから国際標準化へ

- ITU-T SG17
  - IoTセキュアアップデートスキームをNICT中心に提案中。
- IETF
  - IoTのソフトウェアアップデート手法の標準化を検討するWGが発足（SUIT）

ガイドラインから法制化

- 米国
- IoT Cybersecurity Improvement Act 2017　法案
  - IoTデバイスにセキュリティ機能の搭載を強制する法案が提出された（2017.08.04）
    - 検討の進展はなし？
  - 概要：
    - IoT製品の政府調達条件として、メーカー側に既存(IoT)製品のソフトウェアアップデートと、その証明を要請し、修正がきかないハードコードのパスワードを用いることを禁ずるもの。
    - また、この法案はIoTデバイスを政府へ販売するベンダー側にも及ぶことになる。
  - 評価要件：
    - **既知の脆弱性はすべて排除**しておくこと
    - アップデートは、適切に認証され、信用できるものとすること
    - 通信・暗号・機器などとの相互接続には、業界標準技術を使用すること

ガイドラインから法制化

セキュリティに対する
メーカー責任が拡大

- 米国
  - FTCの動き
    - 台湾製のルーターに対する訴訟事例
      - 複数の脆弱性が発覚⇒メーカー対応が不十分（パッチ提供も解決せず）
      - 約1万3千ルータのクラウド接続サービスから不正アクセスインシデント

      ⇒和解：ただしメーカに対し、セキュリティ管理策の実施記録保持と20年間のセキュリティ監査（第三者による脆弱性診断）実施
  - FDA規制
    - Postmarket Management of Cybersecurity in Medical Devices (2016年12月施行)
    - 対象：稼働中のデバイス・システム
    - メーカへの要求事項：
      - 自社・他社製品の脆弱性についての情報収集
      - 自社製品の脆弱性について検証および影響を評価
      - 脆弱性発見時の、開発・生産管理チーム等との社内連携体制の構築
      - インシデントへの迅速な対応
      - 実際にサイバー攻撃を受けた時の縮退運転機能の明確化
      - アップデートやパッチの配布方法・脆弱性情報の公開基準について定義

ガイドラインから法制化

- 欧州：
- EU Cybersecurity Agencyによる認証制度「EU Framework for Cybersecurity Certification」
  - 2017/9/19リリース
    http://europa.eu/rapid/press-release_IP-17-3193_en.htm
  - 目的：IoTのTrustworthiness（信頼性）の確保
  - 対象は、EU圏におけるプロダクトとサービスの両方
    - EUのFood Label（食品安全表示）のようなイメージ
    - サイバー犯罪者に対する法的罰則も検討
  - 詳細は不明。考え方を示したレベル。

©Connected Consumer Device Security Council Proprietary

17

総務省 IoTセキュリティ総合対策

- 2017年10月にリリース
- 総務省サイバーセキュリティタスクフォース（座長：安田浩 東京電機大学学長、副座長：徳田英幸（慶應義塾大学教授）において、IoTに関するセキュリティ対策の総合的な推進に向けて取り組むべき課題を整理し、まとめたもの
- 主な構成：
  1. 脆弱性対策に係る体制の整備
     - 10施策の１つに「認証マークの付与及び比較サイト等を通じた推奨」
  2. 研究開発の推進
  3. 民間企業等におけるセキュリティ対策の促進
  4. 人材育成の強化
  5. 国際連携の推進

総務省資料より

IoTセキュリティ総合対策

脆弱性対策に係る体制の整備

（ライフサイクル全体を見通した対策）

- セキュリティ・バイ・デザイン等の意識啓発・支援の実施
- 認証マークの付与及び比較サイト等を通じた推奨
- IoTセキュアゲートウェイ
- セキュリティ検査の仕組み作り
- 簡易な脆弱性チェックソフトの開発等
- 利用者に対する意識啓発の実施や相談窓口等の設置

（脆弱性調査の実施）

- 重要なIoT機器に係る脆弱性調査
- サイバー攻撃の踏み台となるおそれがある機器に係る脆弱性調査
- 被害拡大を防止するための取組の推進
- IoT機器に関する脆弱性対策に関する実施体制の整備

研究開発の推進

- 基礎的・基盤的な研究開発等の推進
- 広域ネットワークスキャンの軽量化
- ハードウェア脆弱性への対応
- スマートシティのセキュリティ対策の強化
- 衛星通信におけるセキュリティ技術の研究開発
- AIを活用したサイバー攻撃検知・解析技術の研究開発

民間企業等におけるセキュリティ対策の促進

- 民間企業のセキュリティ投資等の促進
- セキュリティ対策に係る情報開示の促進
- 事業者間での情報共有を促進するための仕組みの構築
- 情報共有時の匿名化処理に関する検討
- 公衆無線LANのサイバーセキュリティ確保に関する検討

人材育成の強化

- 実践的サイバー防御演習（CYDER）の充実
- 2020年東京大会に向けたサイバー演習の実施
- 若手セキュリティ人材の育成の促進
- IoTセキュリティ人材の育成の促進

国際連携の推進

- ASEAN各国との連携
- 国際的なISAC間連携
- 国際標準化の推進
- サイバー空間における国際ルールを巡る議論への積極的参画

IoT推進コンソ／IoTセキュリティWGの再起動

- 2016年にIoTセキュリティガイドラインv1.0をリリースして一旦活動を休止
- 再開の目的：
  - IoTセキュリティガイドラインの普及啓発及び汎用的な IoT 機器 のセキュリティ確保策等を検討するため、本ワーキンググループを設置する
- 検討内容：
  - IoT セキュリティに係る諸外国の動向（EU、ドイツ、米国など）や、我が国の産業界の動向 等を踏まえて、同ガイドラインの普及や、ガイドラインの内容の IoT 機器への具体的な実装に向けた取組等を検討する
- 事務局：
  - 総務省情報流通行政局サイバーセキュリティ課
  - 経済産業省商務情報政策局サイバーセキュリティ課（一般財団法人日本情報経済社会推進協会（JIPDEC））

IoTセキュリティWG構成員

- 座長：佐々木良一（東京電機大学 教授）
- 委員：
  - 有村 浩一（JPCERT/CC）
  - 出雲 秀一（在日米国商工会議所サイバーセキュリティTF共同委員長）
  - 岩井 伸夫（一社 日本電機工業会JEMA スマートホーム委員会）
  - 鵜飼 裕司（株式会社ＦＦＲＩ 代表取締役社長）
  - 大矢 隆一郎（一社 ビジネス機械・情報システム産業協会JBMIA）
  - 小川 武史（青山学院大学 理工学部機械創造工学科 教授）
  - 荻野 司（一社 重要生活機器連携セキュリティ協議会CCDS 代表理事）
  - 川上 景一（一社 電子情報技術産業協会JEITA 常務理事）
  - 小山 覚（一社 ICT-ISAC ステアリングコミッティー 副委員長）
  - 四ノ宮 大輔（一社 情報通信ネットワーク産業協会CIAJ）
  - 新 誠一（電気通信大学 情報理工学研究科 教授、兼 技術研究組合制御システムセキュリティセンターCSSC 理事長）
  - 高田 広章（名古屋大学大学院情報学研究科 教授）
  - 塚原 哲史（ＮＴＴドコモ 情報セキュリティ部 部長）
  - 徳田 英幸（情報通信研究機構NICT 理事長）
  - 中尾 康二（情報通信研究機構NICT サイバーセキュリティ研究所 主管研究員）
  - 中野 利彦（日立製作所 制御プラットフォーム統括本部）
  - 向殿 政男（明治大学 名誉教授）
  - 森 亮二（英知法律事務所 弁護士）
  - 吉岡 克成（横浜国立大学 大学院環境情報研究院 准教授）

2017年度第1回の概要

- 経済産業省サイバーセキュリティ課奥家課長の司会進行
- 各方面からのプレゼン
  - 総務省より「IoTセキュリティ総合対策について」
    - 「脆弱性対策に係る体制の整備」の中で、「認証マークの付与」による「利用者が容易に認証取得の有無等を確認できる仕組み」の必要性について言及
    - 既に進めている「IoT機器に関する脆弱性調査等」といった取り組みの紹介
  - 経済産業省より「IoT機器に求められるセキュリティについて」
    - サプライチェーン全体でセキュリティを確保する海外の動きへの追従の必要性等に言及
    - 政策の方向性として４つの観点で進めていることの紹介
      1. 産業政策と連動した 政策展開（重要インフラの対策強化、サプライチェーン毎の対策強化、中小企業のサイバーセキュリティ対策強化）
      2. 国際ハーモナイゼーション
      3. サイバーセキュリティ ビジネスの創出支援（産業サイバーセキュリティシステムの海外展開、サービス認定創設、政府調達などの活用）
      4. 基盤の整備（経営者の喚起、人材育成など）

2017年度第1回の概要（つづき）

- 各方面からのプレゼン
  - 事務局（JIPDEC）より「海外のIoT機器の動向」
    - ENISA「IoTのベースラインセキュリティの推奨事項」、Cybersecurity Certification Framework提案の動きとパブコメによる意見の紹介
    - 米国「サイバーセキュリティに関する大統領令」、『Framework for improving Critical Infrastructure』改訂についての紹介
  - 各団体より、セキュリティに関する対応状況の紹介
    - （一社）電子情報技術産業協会 JEITA
    - （一社）ビジネス機械・情報システム産業協会 JBMIA
    - （一社）日本電機工業会 JEMA
    - （一社）情報通信ネットワーク産業協会 CIAJ
- 委員間の意見交換

パブコメ

- 経済産業省より
  「情報セキュリティサービス基準（案）に関する意見」
  - 意見募集：2017/12/25～2018/1/12

  目的：
  - 専門知識をもたない企業において情報セキュリティサービスを利用する際のサービス事業者選定時の品質を見極めることが難しいという課題に対し、「情報セキュリティサービスについて一定の品質が担保されていることを第三者が客観的に判断し、その結果を台帳等でとりまとめて公開することで、サービス利用者が調達時に参照できるような仕組み」（セキュリティサービス審査登録制度）の創設につながるもの

  脆弱性診断サービスの審査基準
  - 資格要件の他に、
    （イ）次の専門家コミュニティにおける講師又はリーダーの経験を有する者
    - a 特定非営利活動法人日本ネットワークセキュリティ協会
    - b 日本セキュリティオペレーション事業者協議会
    - c ＯＷＡＳＰ：The Open Web Application Security Project

パブコメ２

- 総務省より
  円滑なインターネット利用環境の確保に関する検討会対応の方向性（案）に対する意見募集
  - 意見募集：2017/12/27～2018/1/18

  目的：
  - 主に大規模なDDoS攻撃の対処の方策として、主として電気通信事業者が対応してきたが、悪質化・巧妙化する中、ネットワーク障害からの回復が困難になりつつある。そこで、
    １）攻撃の予防 に向けた対策を強化
    ２）関係者間で必要な情報を共有
    ３）ネットワークに接続される IoT 機器を含む端末設備に係るセキュリティ対策

パブコメ３

- The Interagency International Cybersecurity Standardization Working Group (IICS WG), NIST
- **NISTIR 8200 (DRAFT)**
  Status of International Cybersecurity Standardization for the Internet of Things (IoT)
  - 募集期間：Feb, 2018 – April, 2017
  - 目的：2017年4月にIICS WGを立ち上げ、様々な国や国際標準化機関でのサイバーセキュリティ標準に関する検討の動向を把握し、各産業セクターの民間企業や担当部局での標準化の方向性の検討に役立てるとともに、IoTサイバーセキュリティ国際標準化活動における米国政府の参加対象を調整していく。
  - 主な内容：
  - IoTの機能構成 (Section 4);
  - 代表的なIoTアプリケーションの概要 (Section 5);
    - Connected Vehicle, Consumer IoT, Health IoT & Medical Devices, Smart Building, Smart Manufacturing
  - セキュリティの核となるエリアと標準 (Section 6);
    - 暗号技術、インシデント管理、ハードウェアの保証、ID/アクセス管理、ISMS、ITシステムセキュリティ評価、 ネットワークセキュリティ、SACM（セキュリティ自動化、継続監視）、ソフトウェア保証、サプライチェーンリスク管理（SCRM）、システムセキュリティエンジニアリング
  - IoT cybersecurity objectives, risks, and threats (Section 7);
  - IoTセキュリティにおける標準化の外観 (Sections 8 and 9); and
  - IoT関連（核となるところ）の標準化状況マップ (Appendix D).

まとめ

- ガイドラインで自主的に始める段階は終わり
  - 国際標準で共通的考え方は進化
  - 分野別も必要だが、クルマを除いてまだ国際標準化の動きになっていない？
- 国際標準化、各国での法制化や認証マークの動向に注目
  - 調達要件への適用
    調達側は、セキュリティ要件を独自に明文化することに抵抗（自信もない）
- 「最低限のセキュリティ」は、まだまだ模索中
  - 「最低限」であって、「大丈夫」ではないことを利用者に理解させることの難しさ
  - 「最低限」やればいいのか？
  - メーカ責任は「最低限」で許される？

分野別セキュリティガイドラインなど
CCDSホームページ「公開資料」コーナーで
無料公開中！
https://www.ccds.or.jp/public_document/

本日はご清聴ありがとうございました

© Copyright 2018 Connected Consumer Device Security Council Proprietary