資料6－2

CCDSの取組紹介

2017年6月29日（木）

一般社団法人
重要生活機器連携セキュリティ協議会
Connected Consumer Device Security Council （CCDS）

CCDSのご紹介

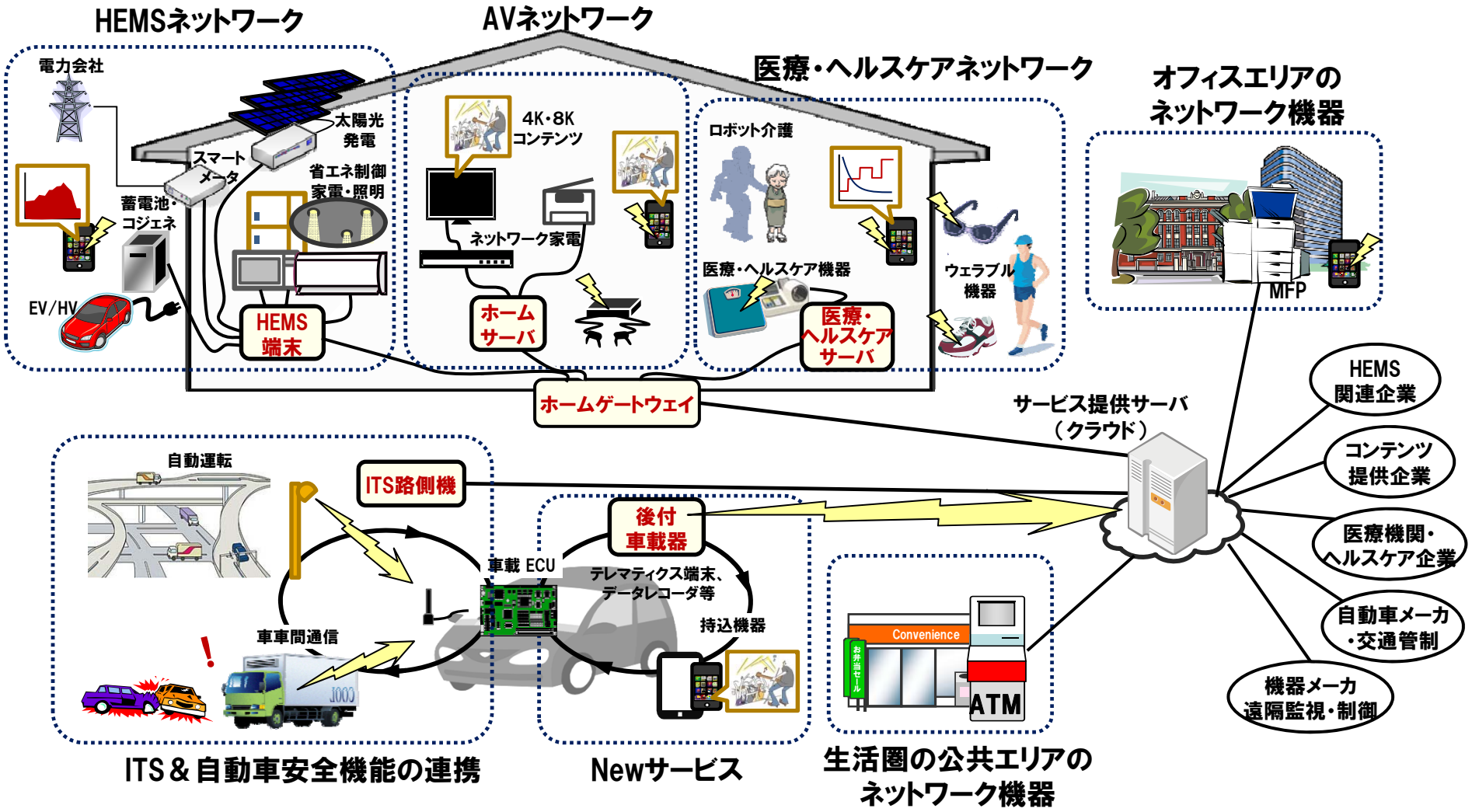
- 名称：一般社団法人 重要生活機器連携セキュリティ協議会
  - 英名：Connected Consumer Device Security council (CCDS)
- 設立：2014年10月6日
- 会長：徳田英幸（情報通信技術研究機構(NICT)理事長
- 慶應義塾大学 客員教授）
- 代表理事：荻野 司（京都大学特任教授）
- 専務理事・事務局長：伊藤 公祐（ゼロワン研究所）
- 理事：後藤厚宏（情報セキュリティ大学院大学教授）
  長谷川勝敏（イーソル（株）代表取締役社長）
  服部博行（（株）ヴィッツ　代表取締役社長）
- 会員数：143（正会員以上：44, 一般会員：72, 学術系：16, 提携団体：11）

- 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時代における新産業が大きく進展

一般民生機器など あらゆるモノが繋がる “モノのインターネット”

HEMS、AV家電、医療・ヘルスケア、自動車関連機器（ナビ、AV機器等）製品・サービス



IoT活用ー＞セキュリティリスクの増大

サイバー空間における脅威がモノへ

HDDレコーダーの踏み台化（2004）

分類	攻撃実例	分野	HDDレコーダ	時期	2004/10	国名	日本
情報源	発見者のブログ投稿　（2013/9/12） http://nlogn.ath.cx/archives/000288.html 3/10/06） da/news/2004/10/06/4882.html						
概要	ていたHDDレコーダが攻撃の踏み台にされる						

遠隔イモビライザーの不正利用（2010）

分類		分野	自動車	時期	2010/03	国名	米国

外部から車載LANへの侵入実験（2010）

分類	攻撃研究	分野	自動車	時期	2010/06	国名	米国
情報源	ワシントン大学Kohno氏ら論文 http://www.autosec.org/pubs/cars-usenixsec2011.pdf デモビデオ http://www.youtube.com/watch?v=bHfOzilwXic						
脅威	遠隔から車載ネットワークに進入する方法を研究発表、デモも実施						
概要	遠隔からの攻撃のイメージ						

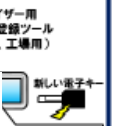
・3G携帯電話（自動車との通信はBluetooth経由）、CDによるメディアプレーヤーのアップデートなどを含め広範囲の侵入経路を検証。

・遠隔操作によるドア解錠、テマティクスユニットの乗っ取による特定の自動車内の音声ビデオ・位置等の記録データ入手についてデモを実施。

組込みシステム開発技術展

イモビカッターによる自動車窃盗（2010）

分類	実例	分野	自動車	時期	2010/11	地域	日本
情報源	「高級車窃盗団、修理道具悪用し電子ロック解除」 asahi.com（現在はリンク切れ）						
脅威	自動車のイモビライザーの鍵を入れ替えるメンテナンス用ツールが悪用され、「イモビカッター」として自動車窃盗に利用						
概要	・イモビライザーは、電子キーのIDと自動車のIDを照合する方式となっており、電子キー紛失時には						



心臓ペースメーカーを不正操作（2013）

分類	攻撃研究	分野	医療機器	時期	2013/08	国名	米国
情報源	米国議会の調査部門である米会計検査院(GAO)のレポート（2012） http://www.gao.gov/assets/650/647767.pdf 19～20P 上記を受けた米国食品医薬品局（FDA)のアナウンス（2013） http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm						
脅威	無線通信で遠隔から埋込み型医療機器を不正に操作できる						
概要							

・埋込み型医療機器の電池寿命は5～10年と長く、利用中に設定変更を行うための無線通信機能が内蔵されているが、保護が不充分。
・米会計検査院（GAO）は、ペースメーカーやインシュリンポンプを遠隔から不正に設定変更する研究（2008～2011年）を基に米国食品医薬品局（FDA)に検討を促した。
・FDAは上記を受け、リスクを医療機器メーカに警告。

（Web上の情報を基に作成）

組込みシステム開発技術展　© Connected Consumer Device Security Council Proprietary

PC接続による自動車の不正操作（2013）

研究	分野	自動車	時期	2013/09	地域	米国

イター記事 http://jp.reuters.com/article/topNews/idJPTYE96S04820130729
RS Technica 記事 http://arstechnica.com/security/2013/07/disabling-a-cars-brakes-and-speed-by-cking-its-computers-a-new-how-to/
正操作ビデオ http://wired.jp/2013/09/05/hack-a-car/

定の自動車の車載ネットワークにPCを接続し、不正操作

ネットワーク（CAN）に接続し、ECU
制ユニット）にコマンドを送り、自動

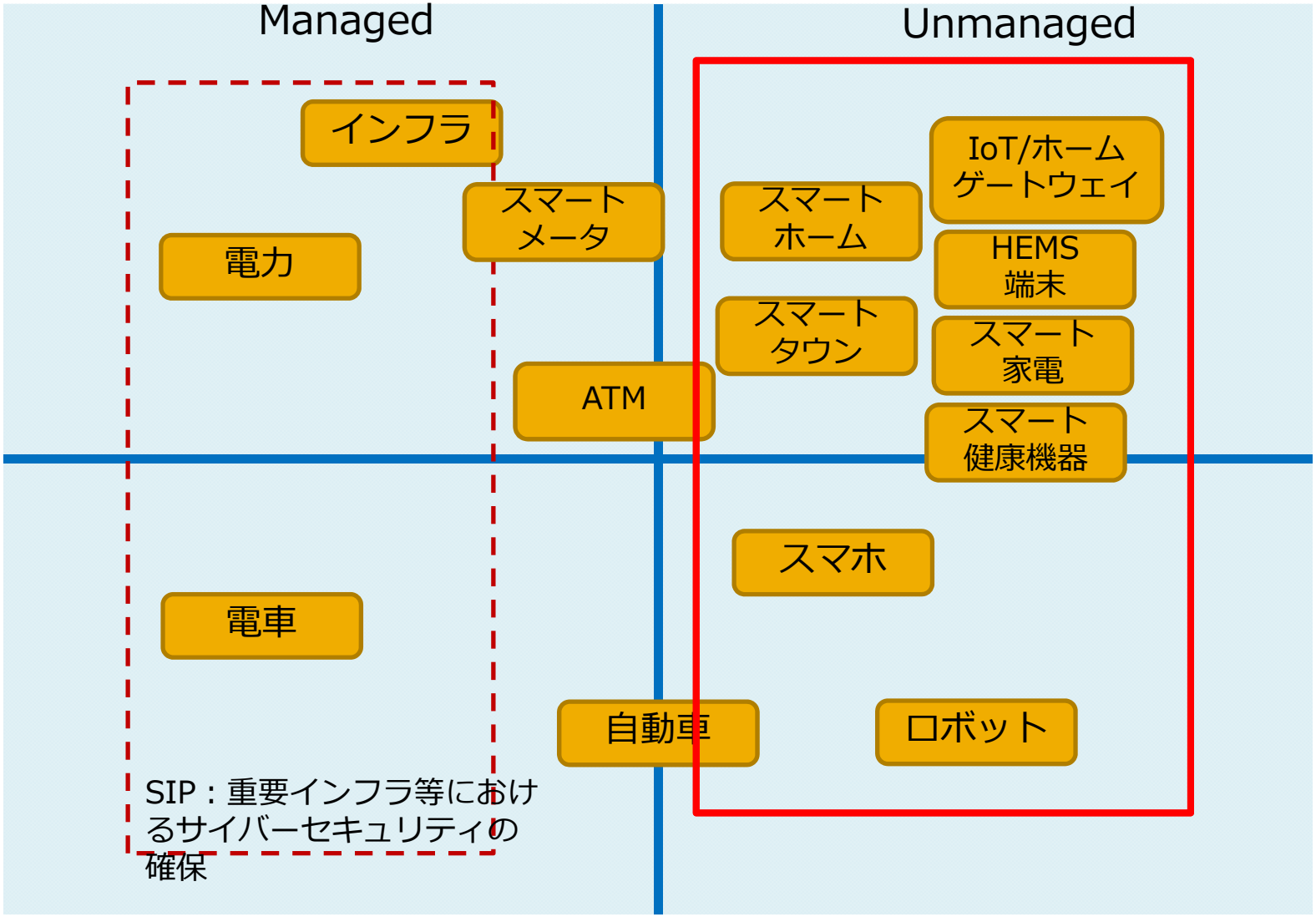
0kmで走行中に急ブレーキをかけたり、
運転思とは関係なくハンドルを動かした
中にブレーキを利かなくすることが可

（CCDS事務局作成）

レに誤った数値（例えば時速300km超
を表示させることも可能。
は、ダッシュボードを外していたが、床のシート
ことでCANに接続できる車種も多い。

組込みシステム開発技術展　© Connected Consumer Device Security Council Proprietary

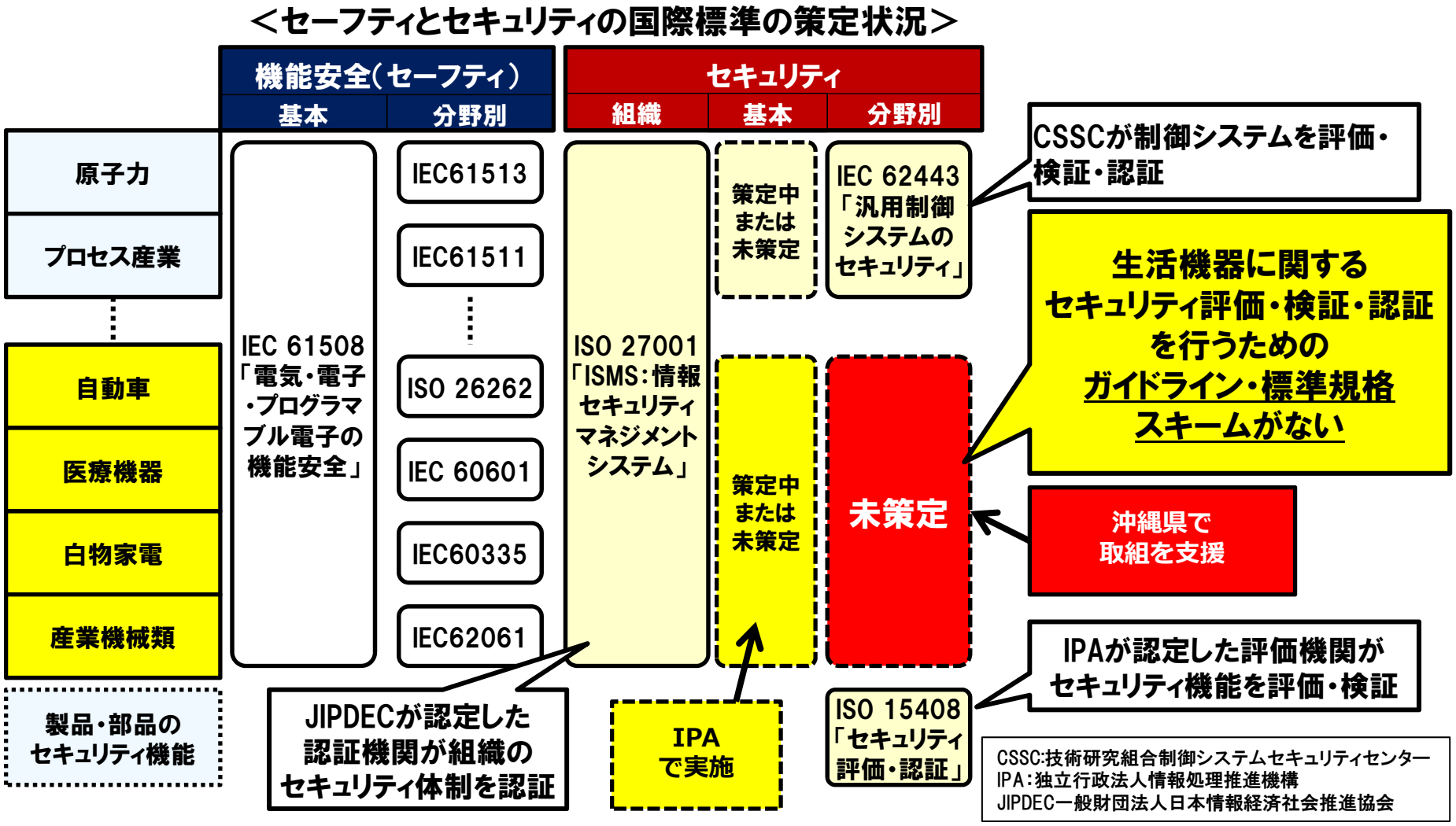
IoT環境で対象とするシステム



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）

国際標準は、セーフティーからセキュリティへ

自動車、医療機器、家電などの生活機器に関してはセキュリティ規格もなく、対応に遅れ



2013年 研究会時代の提言～セキュアライフ2020～
「つながるIT社会の安心・安全の確保に向けて」

１）つながる生活機器のセキュリティに目を向けよう

ユーザやサービス事業者が生活機器を自由に連携させて利用するシーンを想定し、セキュリティを検討する。

２）ユーザを巻き込んだセキュリティ対策を考えよう

ユーザのリテラシー向上、生活機器のセキュリティレベルや状態の通知、セキュリティ119番の設置など、ユーザを巻き込んだセキュリティ対策を検討する。

３）業界横断的な検討の場を設けよう

業界横断的なセキュリティ対策を検討する場の設置、対策技術の共同開発、セキュリティ用語の統一等により、効率的・効果的にセキュリティの実現を図る必要がある。

４）世界の安心・安全に貢献しよう

各業界における共通のセキュリティ対策やガイドラインの検討を進めるとともに、国際標準及び評価検証制度の制定を進める必要がある。

５）世界に誇れるセキュアなものづくりを進めよう

標準やガイドラインを基に企画段階からセキュリティを組み込んでいくこと、ソフトウェア開発工程のサプライチェーンにおいてセキュリティを考慮することが必要である。

NISC:経済社会の活力の向上及び持続的発展

経済社会の活力の向上及び持続的発展 ～費用から投資へ～

企画・設計段階からセキュリティの確保を盛り込む
セキュリティ・バイ・デザイン(SBD)

■安全なIo

- 企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン(SBD)の実践に基づく安全なIoT(モノのインターネット)システムを活用した事業を振興
- IoTシステムに係る大規模な事業について、サイバーセキュリティ戦略本部による総合調整等により、必要な対策を整合的に実施するための体制等を整備
- エネルギー分
- IoTシステムの特徴(長いライフサイクル、処理能力の制限等)、ハードウェア真正性の重要性等を考慮した技術開発・実証事業の実施

IoTシステムのセキュリティに係る総合的なガイドライン等を整備

■セキュリティマインドを持った企業経営の推進

- 企業におけ
- 経営層と実
- 民民間・官

IoTシステムの特徴(長いライフサイクル、処理能力の制限等)、
ハードウェア真正性の重要性等を考慮した技術開発・実証事業の実施

■セキュリティに係るビジネス環境の整備

- 政府系ファンドの活用等により、サイバーセキュリティ関連産業を振興(ベンチャー企業の育成等を含む)
- 中小企業等のクラウドサービス活用に有効なセキュリティ監査の普及促進
- サイバーセキュリティ産業の振興に向けた制度の見直し(リバースエンジニアリング等)
- IoTシステム等のセキュリティに係る国際的な標準規格や相互承認枠組み作りの国際的議論を主導
- 知財漏えい防止強化など、公正なビジネス環境を整備

▲自動運転車の実証実験

出典:NISC:サイバーセキュリティ戦略(案)より

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

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

分野別セキュリティガイドライン

・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。

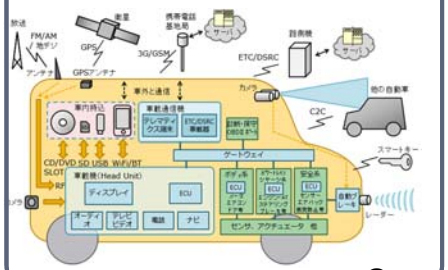
対象分野

・車載器　　・ATM（金融端末）
・IoT-GW　　・POS（決済端末）

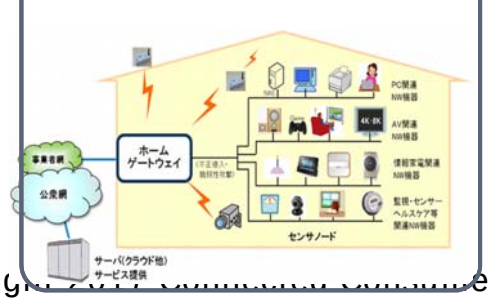
ガイドラインの主な内容と改良点

・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）

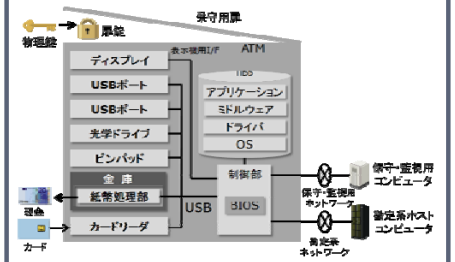
車載器システム構成



IoT-GW：ホームGWケース

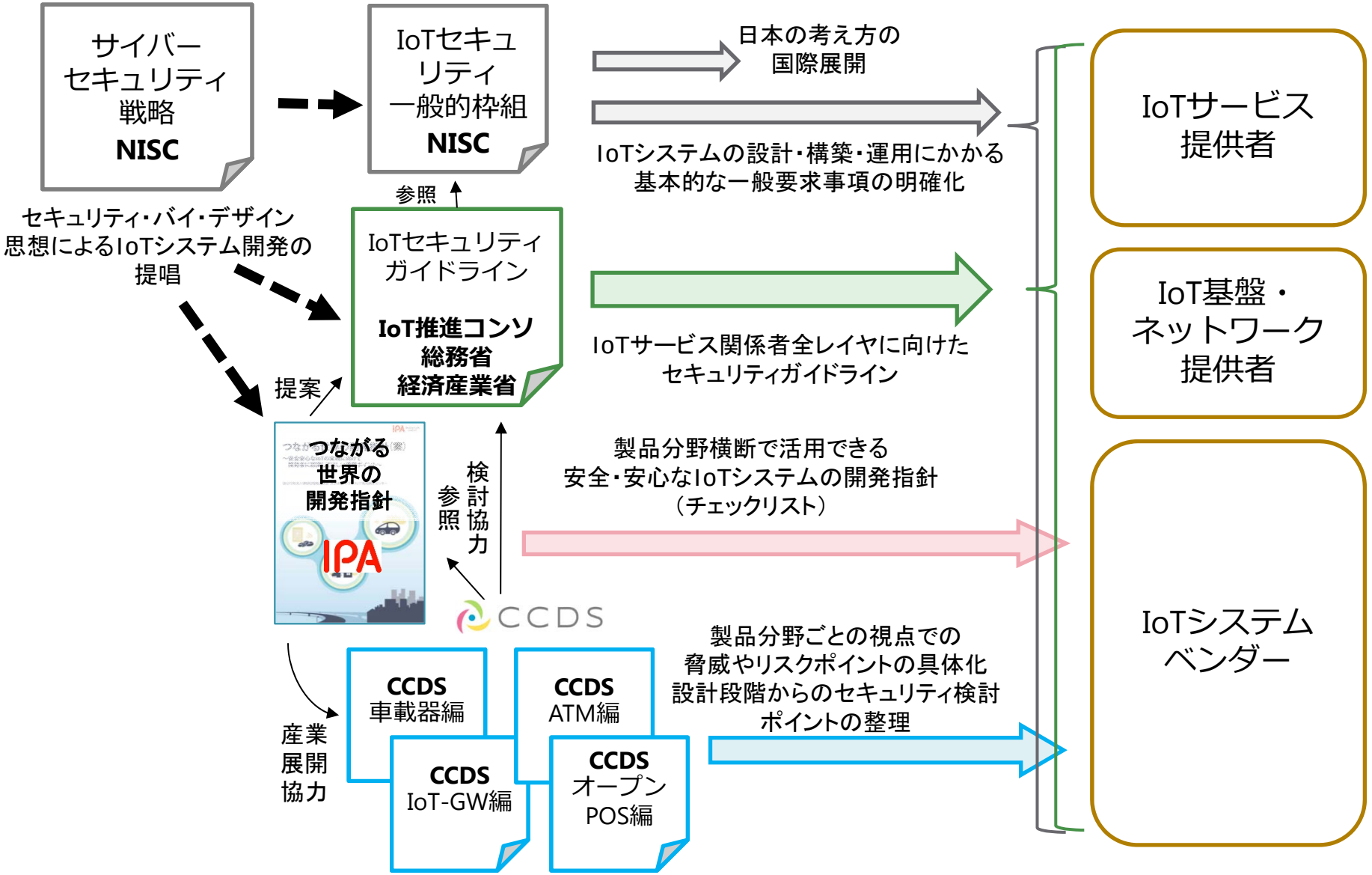


ATMシステム構成



POSシステム構成

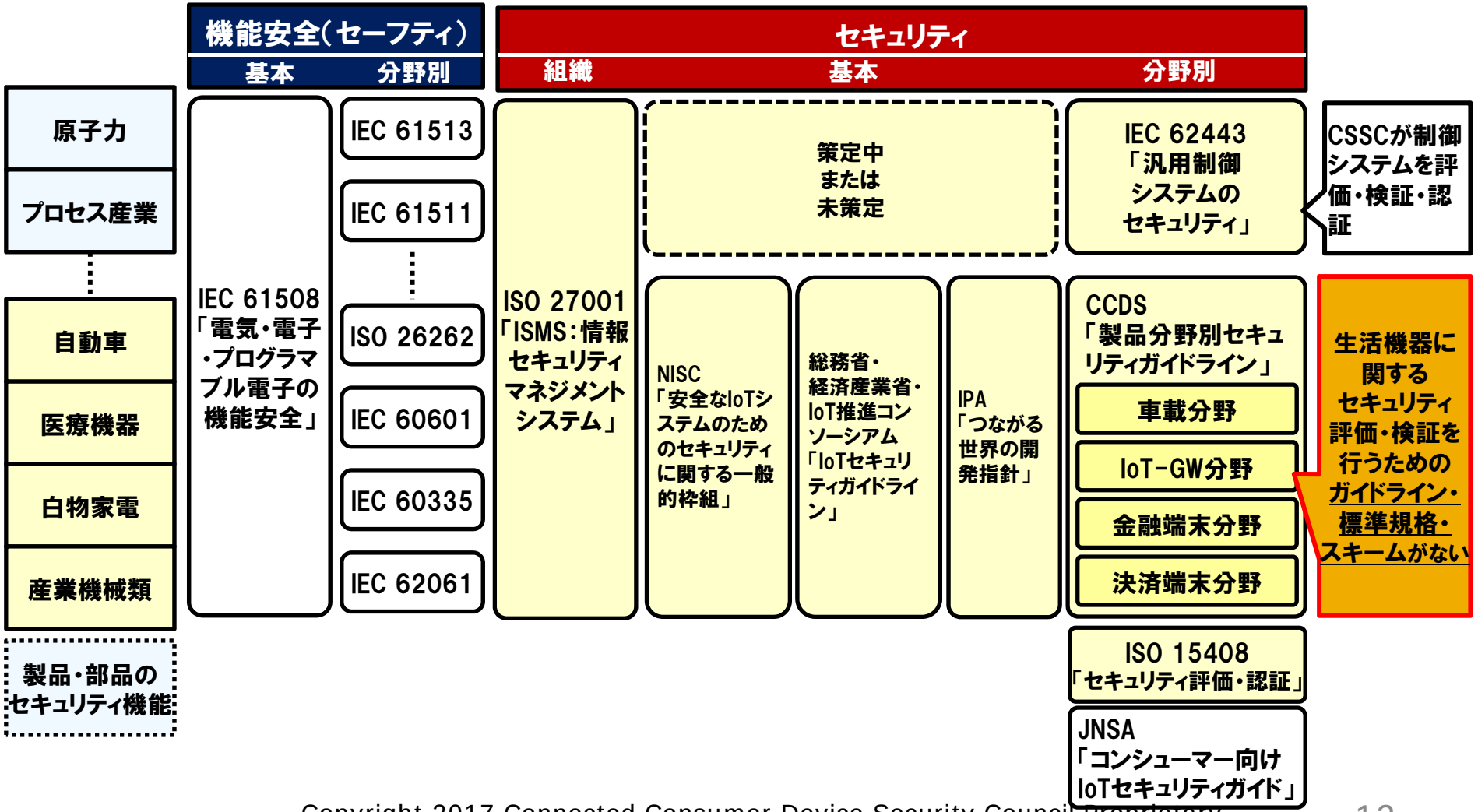
IoTセキュリティガイドラインの整備状況



規格・標準策定状況

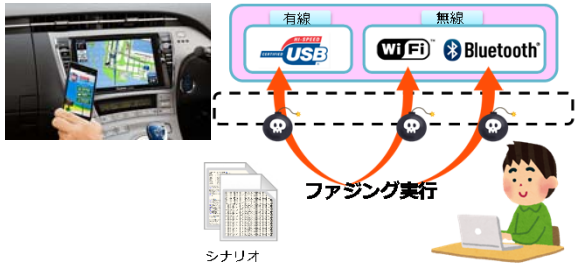
＜セーフティとセキュリティの国際規格の策定状況＞

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

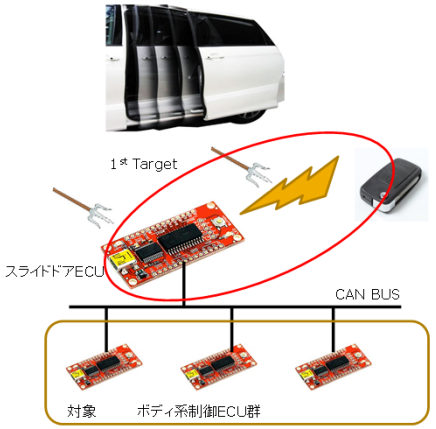


検証基盤構築：
IoT機器向け脆弱性検証ツール開発

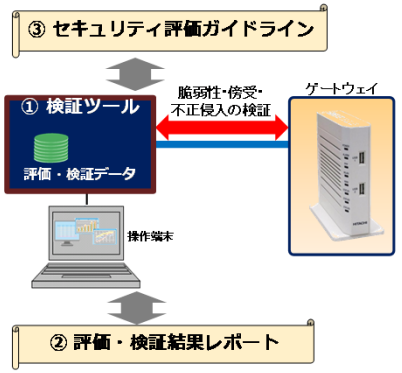
- WiFi-BTファジングツール
  - 主な対象：ナビなどの車載器
  - AIを活用した効率的検証用データ生成も研究中



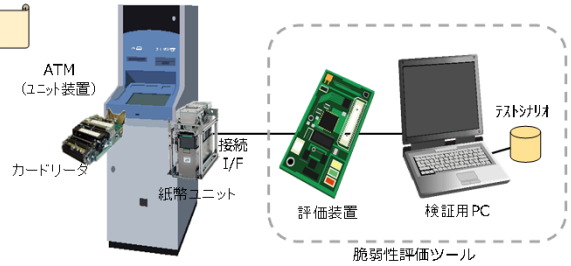
- 車載CAN向け静的解析ツール／動的検証ツール
  - 主な対象：ボディ系ECU



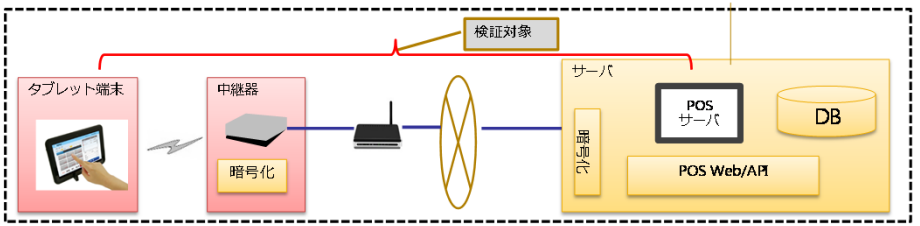
- ネットワークプロトコル脆弱性検証ツール
  - 主な対象：ホームルータなどIoT-GW類
  - ファジング、DoS攻撃、パスワード解析



- ATM向け脆弱性検証ツール
  - 主な対象：ATM
  - ATMのミドルウェアやUSB脆弱性検証など



- POS向け脆弱性検証ツール
  - 主な対象：オープン（タブレット型）POS
  - POSの無線ネットワーク脆弱性検証や残留個人データ検査など



- 検証業務基盤
  - クラウド型の検証業務効率化
  - テストシナリオやテスト結果などの作成、DB化機能

検証基盤構築：
IoTセキュリティ評価・検証ガイドライン

- 背景：
  - 開発向けの分野別セキュリティガイドラインに対し、品質評価部門向けガイドラインのニーズ
  - CCDS会員ゼロワン研究所の総務省「身近なIoTプロジェクト」での成果「スマートホーム向け脆弱性検証ガイドライン」をCCDSにて一般IoT向けとして検討中
- 概要
  - スマートホーム分野での実例を取り入れつつ、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掘り下げた内容
  - ISO/IEC/IEEE 29119を参考に、「検証方針・計画策定」「検証設計」「検証実行」「報告、フィードバック」に分け、プロセス毎に詳細を解説

CCDSの主なWG活動

- セキュリティガイドラインWG
  - 分野別セキュリティガイドラインの検討
  - 海外や国内のIoTセキュリティガイドライン情報共有
  - 国際標準化や認証マークの在り方に関する検討
  - 国やIPA、各団体のガイドライン策定、国際標準化活動への参加
  - 主な成果：分野別セキュリティガイドラインv2、v1英語版など
- セキュリティ技術WG／デバイスセキュリティ技術SWG
  - IoT機器向けセキュリティ対策技術マップの検討
  - 主な成果：スマートホームやコネクテッドカーの脅威と対策手法の整理
- ユーザビリティWG
  - IoT機器類のUI等、デザインの観点からセキュアな設定、使い方を維持する端末の在り方の検討
  - 主な成果：セキュアな使い方を促すデザインケースの事例集

分野別セッキュリティガイドライン
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/