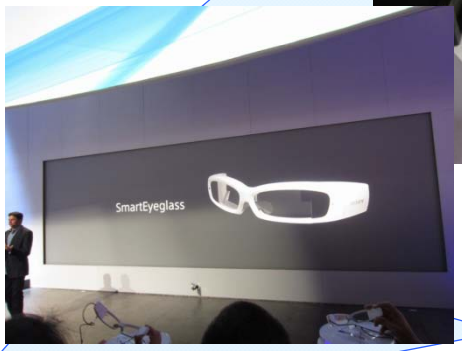
IoTのセキュリティ
～脅威と対策の方向は？～

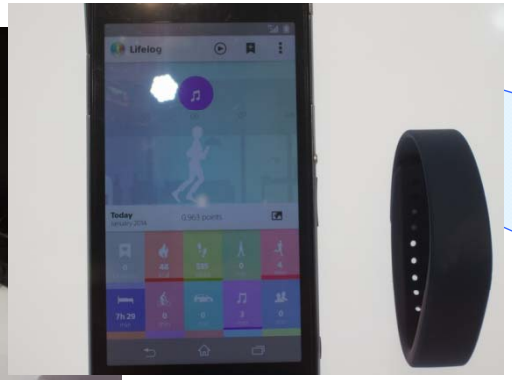
2015年7月27日

㈱ユビテック　ユビキタス研究所　所長
　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

繋がるIoTの世界へ！

（2014年1月7日－10日：CES）





ウェアラブル
&
自動走行

繋がる！　連携する！

- スマートライフ　　－＞　豊かさ
- ICT　　－＞　「アシスト」

- ウエアラブルの発展で、「人」と「機器」が連携
- 「人」のデータが、クラウド＝サーバ　に蓄積

- ビッグデータが身近に！

繋がる、連携する、ICTが人をアシストする

新産業にむけて世界が動いている！

---- Indutry 4.0 , Smart Home , IoT ----

OPEN
INTERCONNECT
CONSORTIUM℠

industrial internet®
CONSORTIUM

ALLSEEN
ALLIANCE

Internet of Things Consortium

THREAD

脅威の事例

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

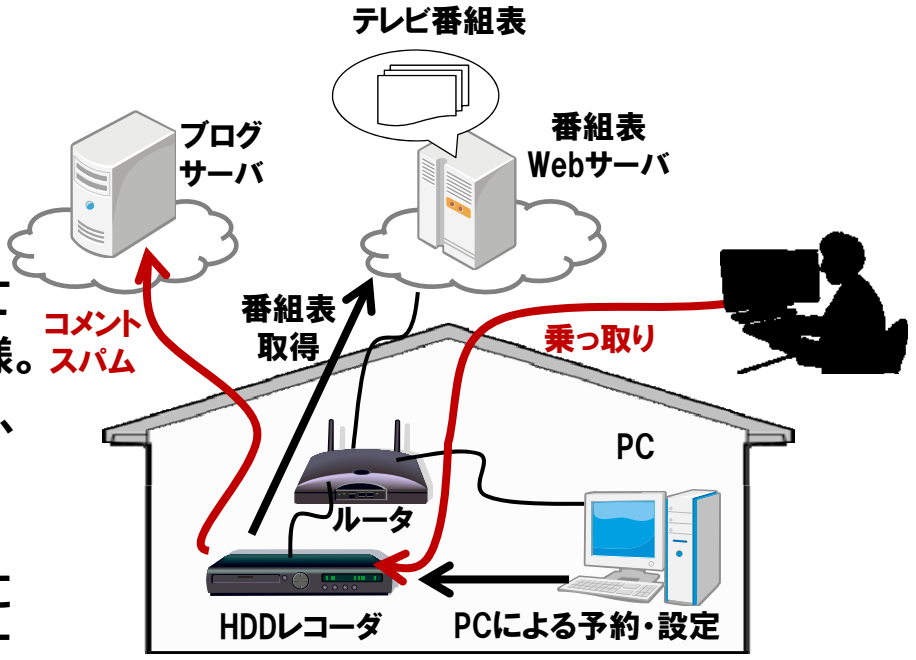
発見者のブログ投稿　（2013/9/12） http://nlogn.ath.cx/archives/000288.html
インターネットウォッチ（2013/10/06）
http://internet.watch.impress.co.jp/cda/news/2004/10/06/4882.html

脅威

セキュリティ設定が無効になっていたHDDレコーダが攻撃の踏み台にされる

概　要

- 情報家電に対する初期の攻撃事例。
- 本機器は、PCからの予約受付のためのWebサーバ機能、テレビ番組表取得のための外部サーバアクセス機能を有していたため、踏み台として利用された模様。
- ID・パスワードによるアクセス制御は、装備されていたものの出荷時には無効となっていた。
- あるブログライターが、自分のブログに国内から大量のコメントスパムが届いていることを不審に思い、分析し、発見。



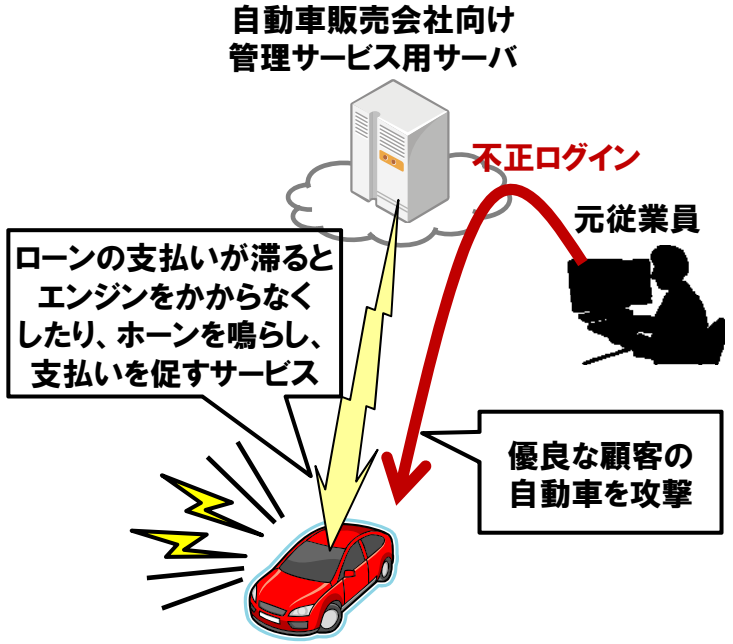
（Web上の情報を基に作成）

遠隔イモビライザーの不正利用（2010）

分　類	攻撃実例	分野	自動車	時期	2010/03	国名	米国
情報源	WIRED記事（2010/03/11） http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/						
脅威	遠隔イモビライザーの管理サーバへの不正ログインにより、自動車のエンジンがかからない、ホーンが鳴らされる等の被害が発生						

概要

・ローンで販売された自動車の支払いが滞った際にエンジンのイグニッションを無効にしたり、ホーンを鳴らして督促するサービスが悪用され、自動車を利用できなくなったり、真夜中にホーンが鳴らされた。
・販売会社には電話が殺到し、当初原因も分からず、
解除も走行もできなかったため、バッテリーを外してレッカーで工場に移動するしかなかったとのこと。
・逮捕された犯人は、前の月に販売会社に人員整理された元従業員で、他の従業員のID/パスワードで不正ログインしていた。



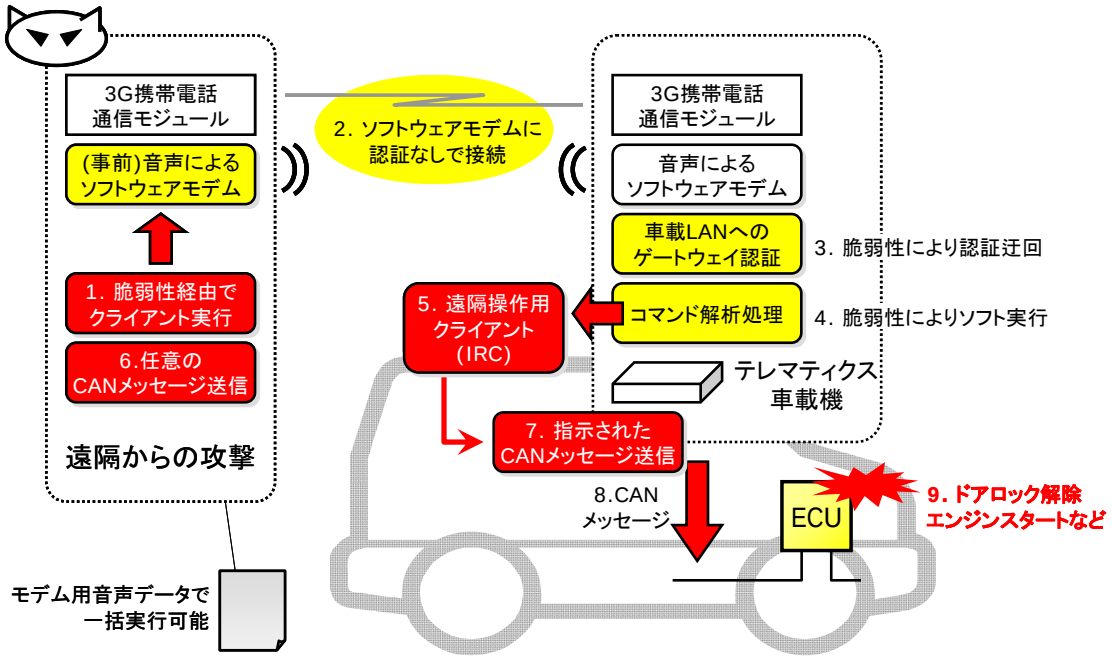
（Web上の情報を基に作成）

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=bHfOziIwXic						
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							

- 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、テレマティクスユニットの乗っ取り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の入手についてデモを実施。

遠隔からの攻撃のイメージ



2011 年度自動車の情報セキュリティ動向に関する調査より

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）

PC接続による自動車の不正操作（2013）

分　類	研究	分野	自動車	時期	2013/09	地域	米国

情報源

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

脅威

特定の自動車の車載ネットワークにPCを接続し、不正操作

概要

- PCを車載ネットワーク（CAN）に接続し、ECU（電子制御ユニット）にコマンドを送り、自動車を操作。
- 時速約130kmで走行中に急ブレーキをかけたり、運転手の意思とは関係なくハンドルを動かしたり、走行中にブレーキを利かなくすることが可能。
- またパネルに誤った数値（例えば時速300km超の速度）を表示させることも可能。
- ビデオでは、ダッシュボードを外していたが、床のシートをはがすことでCANに接続できる車種も多い。

（CCDS事務局作成）

Black Hat2014プログラムより

- ハッカー集団会議でも、組込みシステムを対象としたテーマが増加し注目される
  - Cellular Exploitation（携帯網の制御プロトコルの探索）
  - Survey of Remote Automotive Attack surfaces（自動車の遠隔攻撃界面の調査）
  - My Google Glass Sees your Password（Googleグラスによるパスワードハッキング）
  - Researching Android Device Security with the help of a Droid Army（ドロイドを活用したAndroidデバイスセキュリティの研究）
  - Home Insecurity: No Alarms, False Alarms（ホームセキュリティは安心できない、無線センサー信号の盗聴）
  - Stealing data from point-of-sale devices（POSデータの盗聴）
  - Hacking mobile providers‘ control code（モバイルキャリアの制御信号の解読）
  - 組込みデバイス会談（これから組込みはどこに向かうか）
  - BAD USB（USBメモリスティックなりすまし）

  などなど

脅威の動向： BadUSB

- 別クラスのUSBデバイスになりすまし
  能動的に攻撃
- 問題
  - USB I/F経由でFWを更新可能
  - ほかのUSBデバイスに感染させる
  - 別のタイプ(Class)機器になりすまし
  - 勝手にキーボード操作を実行する
- 今後の対策の可能性
  - 機器接続時の製造者認証
  - USB機器の脆弱性テスト
  - 実行中の復帰処理

(イメージ画像)

日経コンピュータ: 記者は「BadUSB」を試してみた、そして凍りついた, 2014-11-12
http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/110700106/

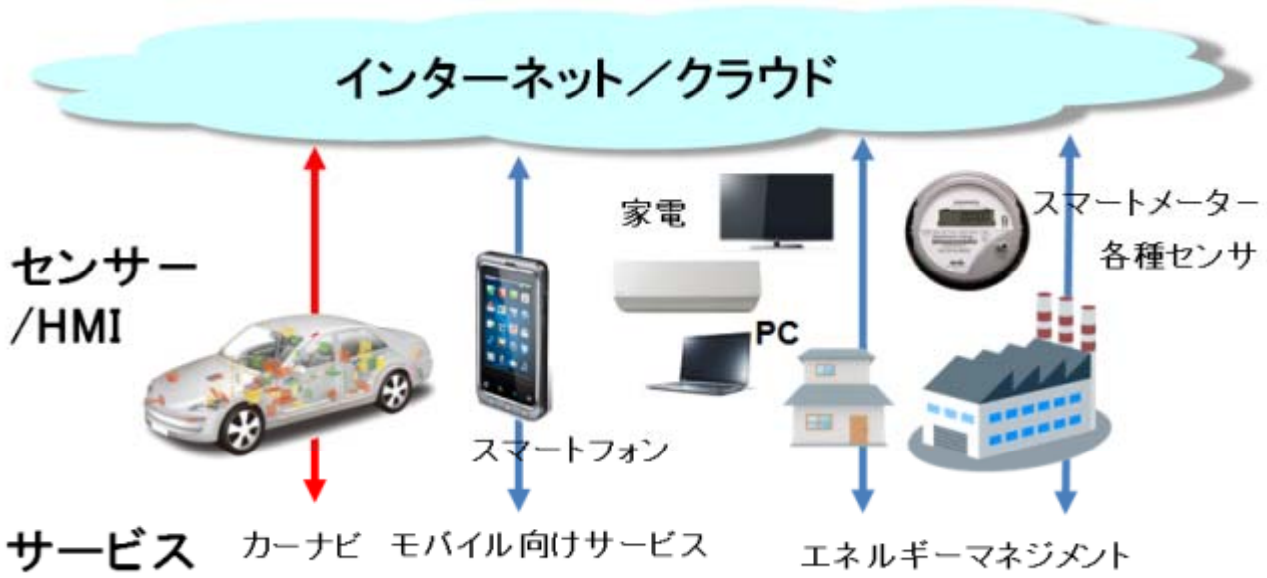
Black Hatの発表者はハッキングコードは公開しなかったが、DurbyConの発表者はコードを公開した上で、悪用法としてUSBメモリを装ったデバイスでユーザーのUSBキーボードをハックして好きにキーを入力するデモを実施。

⇒個社でのセキュリティ対応は大変

標準化の動向

M2Mアプリケーションの垂直構造

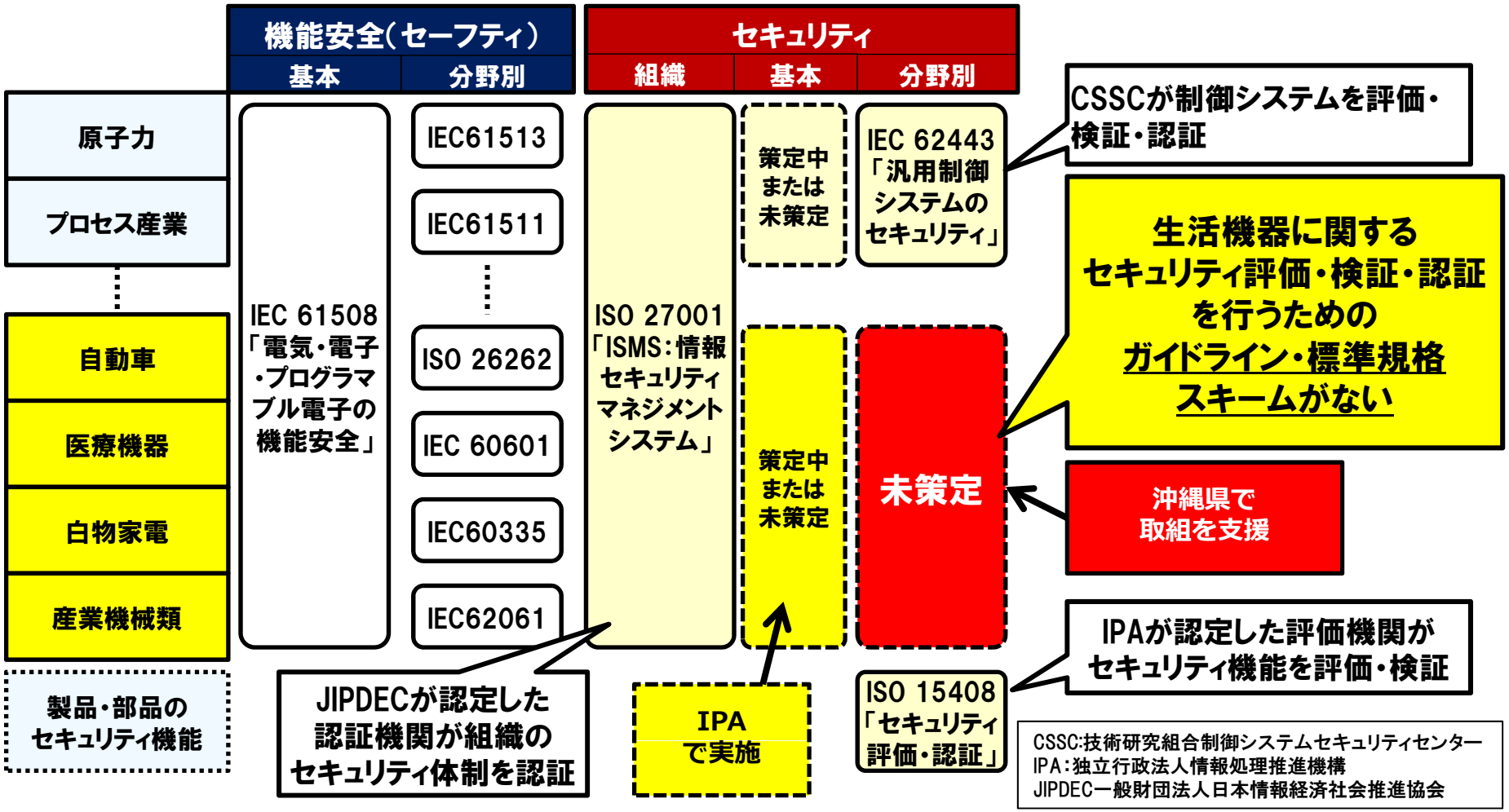
- クラウドによって相互接続する構造
  - ITU, oneM2Mが前提にしている



JARI・「IT・CE技術のITSにおける利活用の研究」より
http://www.jari.or.jp/tabid/113/Default.aspx

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。



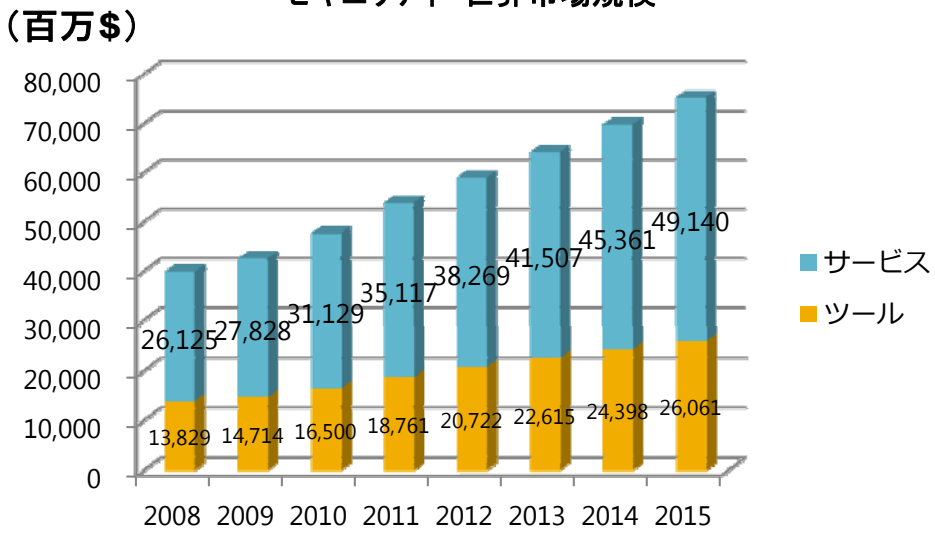
成長するセキュリティ市場！

1. セキュリティ市場予測

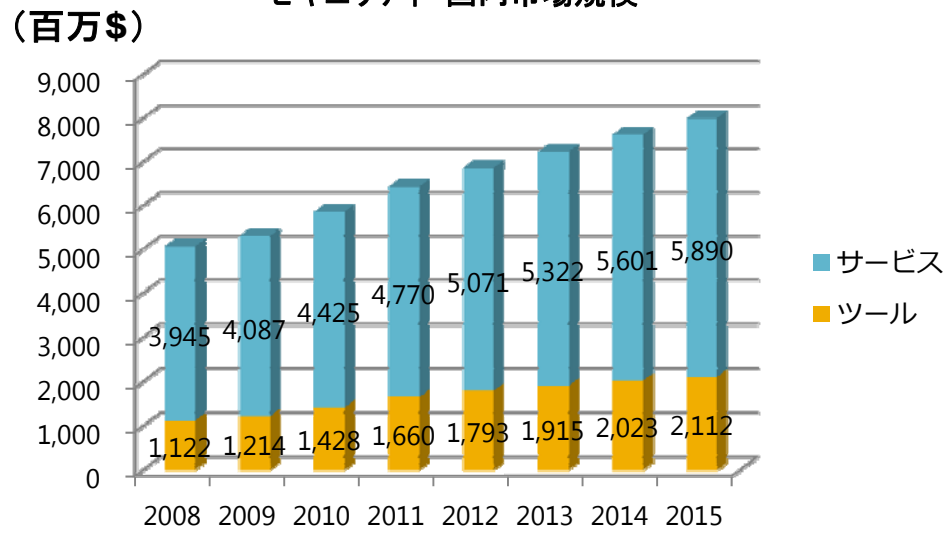
（※ ガートナー 平成23年度企業・個人セキュリティ対策促進事業　調査報告書から）

2015年 7兆6,705億（世界市場）、8,162億（日本市場）

セキュリティ　世界市場規模



セキュリティ　国内市場規模



2. セキュリティ　雇用創出

（※ 新たなICT戦略に関する提言　デジタル・ニッポン2013　－ICTで日本を取り戻す－　から）

高度サイバーセキュリティ産業を創出して10万人の新規雇用増を創出すること

第1グループ：　高度な専門管理者　　3,000人
第2グループ：　専門管理者　　17,000人
第3グループ：　開発／販売　　80,000人

現状、情報セキュリティ従事者　約26.5万人（うち 質的不足　約１６万人）さらに量的不足　約８万人

（※ 情報セキュリティ政策会議第38回会合資料　内閣官房セキュリティセンター（NISC）　から）

日本の現状

- 2014年７月　NISCセキュリティ研究開発戦略改正版

「様々な形でつながる自動車や家電、医療・ヘルスケア機器などの生活機器のセキュリティ」が重要と位置づけ

ー＞当協議会のパブリックコメントが反映！

NISC National Information Security Center

…また、様々なメーカーから提供される、自動車、HEMSや家電等の生活機器についても、ネットワーク接続が進みつつあるが、生活機器は、連携対象が多種多様であることや、操作する者が一般消費者であるという特性があることから、この分野において、分野横断的な情報セキュリティ技術の研究開発や国際標準化等の対応についても検討していく。

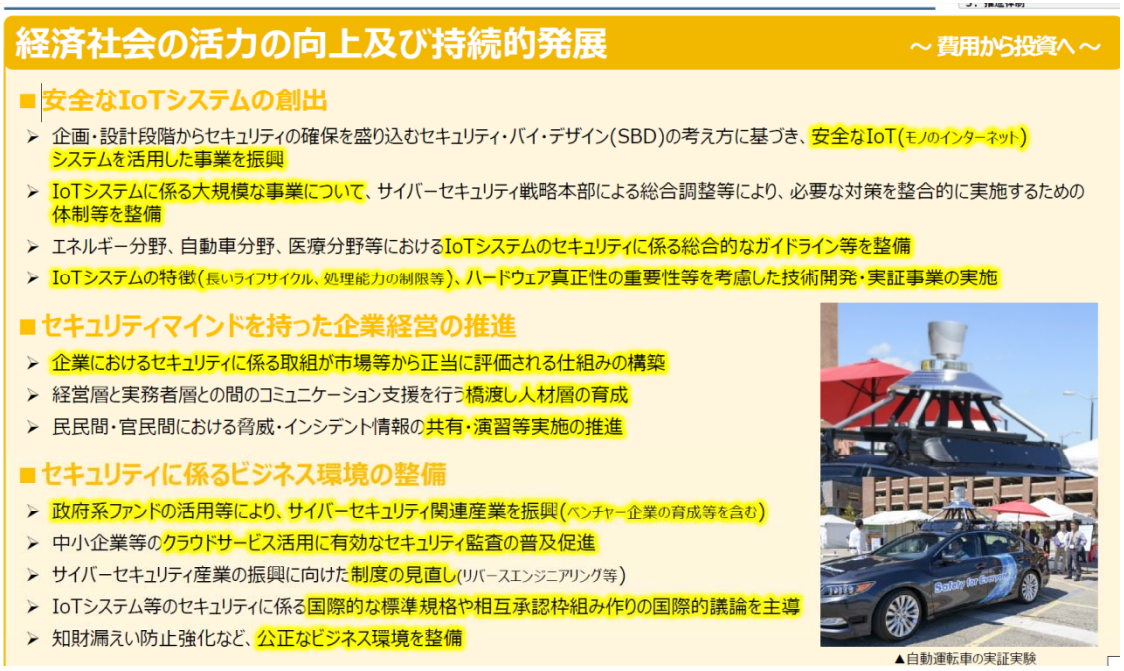
2014年10月　一般社団法人　CCDSを立ち上げ！

NISC:経済社会の活力の向上及び持続的発展

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)

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

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



経済社会の活力の向上及び持続的発展 ～費用から投資へ～

■安全なIoTシステムの創出

- 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)の考え方に基づき、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
- エネルギー分野、自動車分野、医療分野等における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
- 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

■セキュリティマインドを持った企業経営の推進

- 企業におけるセキュリティに係る取組が市場等から正当に評価される仕組みの構築
- 経営層と実務者層との間のコミュニケーション支援を行う橋渡し人材層の育成
- 民民間・官民間における脅威・インシデント情報の共有・演習等実施の推進

■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 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（慶應大学教授、内閣セキュリティ補佐官）
- 代表理事：荻野 司（京都大学特任教授）
- 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㈱代表取締役社長）
  服部博行（株式会社ヴィッツ常務取締役）
- 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

CCDS会員一覧（2015年5月時点）

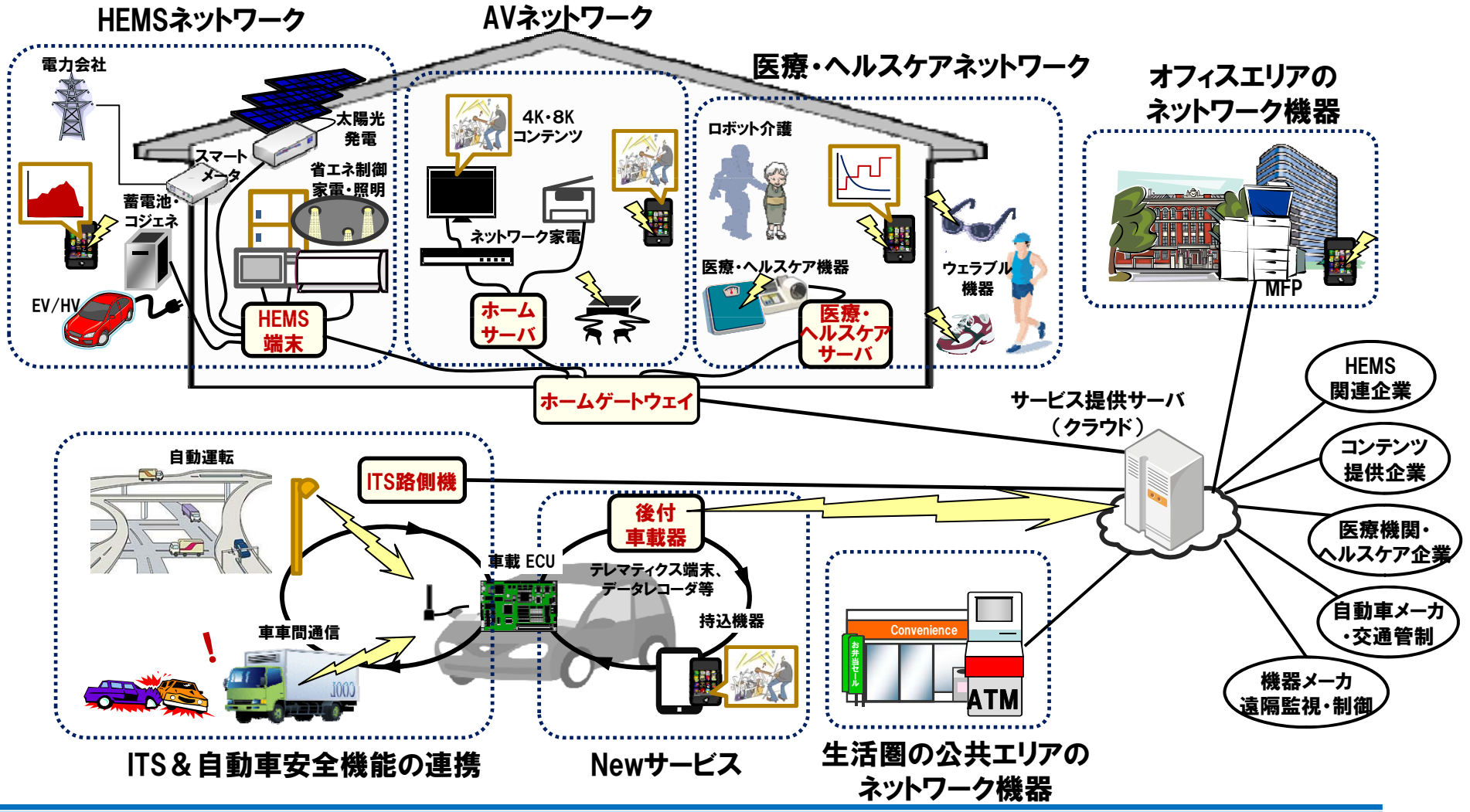
＊:沖縄県内企業

- 幹事会員（２２）
  - イーソル株式会社
  - 株式会社エイブリッジ（沖縄支社）＊
  - 株式会社ヴィッツ
  - 株式会社エイチアイ
  - 株式会社エヌジェーケー
  - オムロンソフトウェア株式会社
  - 沖縄フォーサイト株式会社＊
  - 沖縄日立ネットワークシステムズ株式会社＊
  - 株式会社システムビット（沖縄支社）＊
  - 株式会社シー・アール・シー（沖縄支店）＊
  - 株式会社ジーエヌエー＊
  - 株式会社ジービーエー＊
  - 株式会社JVCケンウッド
  - 日立オムロンターミナルソリューションズ株式会社
  - 株式会社日立製作所
  - 株式会社プラスナレッジ＊
  - 株式会社ブロードバンドタワー
  - 株式会社プロトデータセンター＊
  - ユーマーク株式会社＊
  - 株式会社ユビテック
  - 株式会社リコー
  - 株式会社ルクレ（沖縄支店）＊
- 正会員（２）
  - アイシン・コムクルーズ株式会社
  - パナソニックアドバンストテクノロジー株式会社
- 学術会員（１０）
  - 慶應義塾大学 徳田研究室
  - 情報セキュリティ大学院大学　大久保研究室
  - 情報セキュリティ大学院大学　後藤研究室
  - 情報セキュリティ大学院大学　佐藤研究室
  - 名古屋大学　高倉・嶋田研究室
  - 名古屋大学　高田研究室
  - 広島市立大学　インターネット工学研究室
  - 北陸先端科学技術大学院大学　丹研究室
  - 横浜国立大学 松本勉研究室
  - 独立行政法人産業技術総合研究所
- 一般会員（個人参加を含む）（２６）
  - アルパイン株式会社
  - アルプス電気株式会社
  - インヴァスト証券株式会社
  - インヴェンティット株式会社
  - インターネットITS協議会
  - 株式会社インテック
  - 株式会社エイチアイ
  - 株式会社ＦＦＲＩ
  - ＮＴＴコミュニケーションズ株式会社
  - ＮＴＴコムエンジニアリング株式会社
  - ガイオ・テクノロジー株式会社
  - 株式会社カスペルスキー
  - キャッツ株式会社
  - クラリオン株式会社
  - 株式会社ＫＤＤＩ研究所
  - ソシオメディア株式会社
  - 株式会社ソリトンシステムズ
  - 大日本印刷株式会社
  - 株式会社電脳商会
  - 株式会社東京海上研究所
  - 東芝ソリューション株式会社
  - 株式会社豊通エレクトロニクス
  - トレンドマイクロ株式会社
  - 日本電気株式会社
  - 株式会社U'eyes Design
  - ユニアデックス株式会社

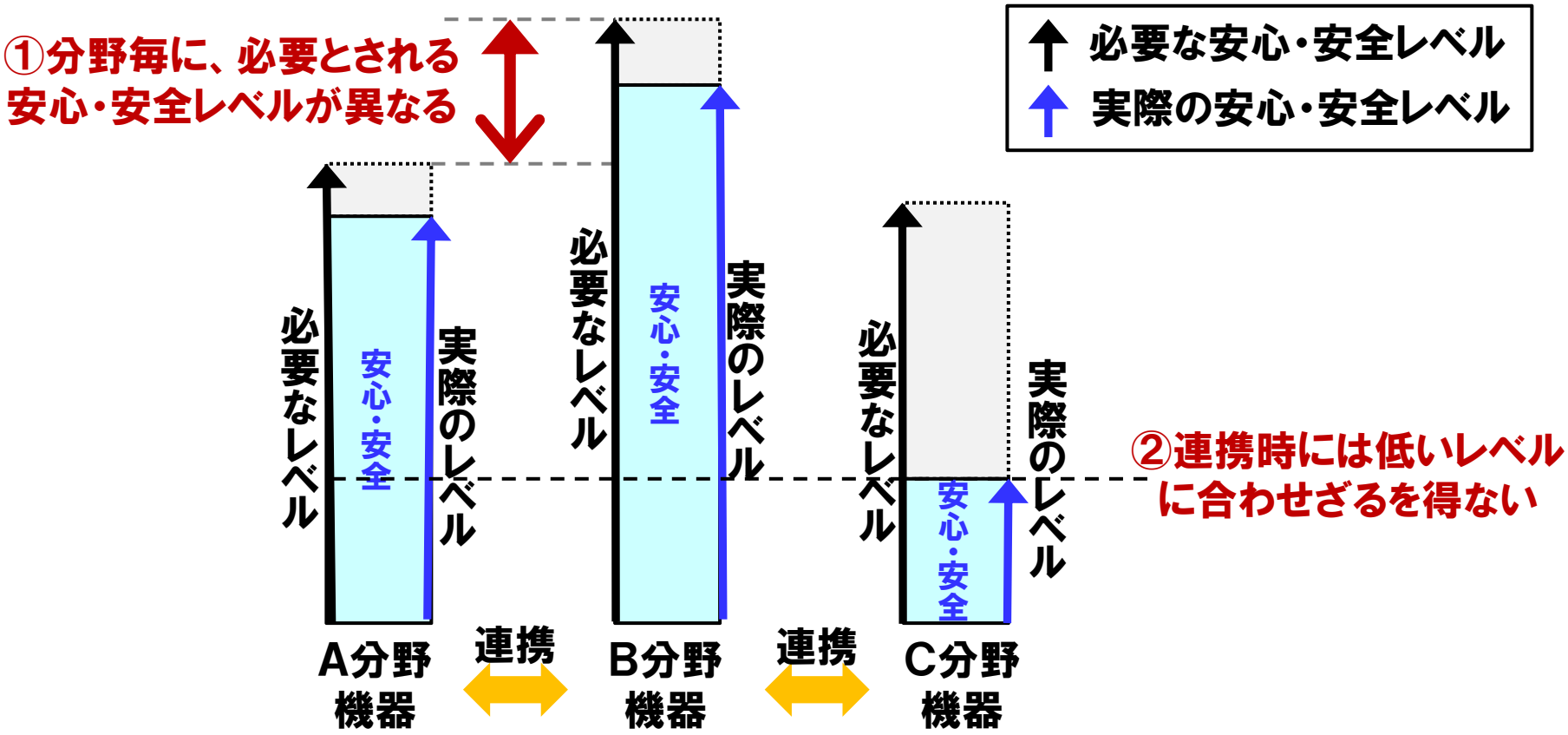
CCDSとは：
重要生活機器におけるセキュリティ事業の創生

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



分野で異なる安心・安全レベル

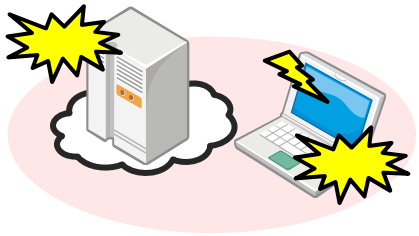


2020年に向けた取り組みのイメージ

CCDS

現状の脅威

サーバやＰＣへの攻撃



2020年の脅威

生活機器がネットワーク連携することで脅威が拡大

何がつながっているか、何が起こっているかが、分からない

今からセキュリティ対策を開始することが必要

業界団体

・業界共通対策の検討、セキュリティ標準・認証スキーム策定等

検討成果の提供

企業

・セキュアな開発・運用体制、人材育成等

業界連携

業界横断

・業界横断的な検討の場の設置、機器間の信頼性確認基盤検討等

製品提供・サポート

ユーザ

・セキュリティリテラシー・意識の向上
・ユーザへの共通的なセキュリティ情報提供

啓発・支援

行政

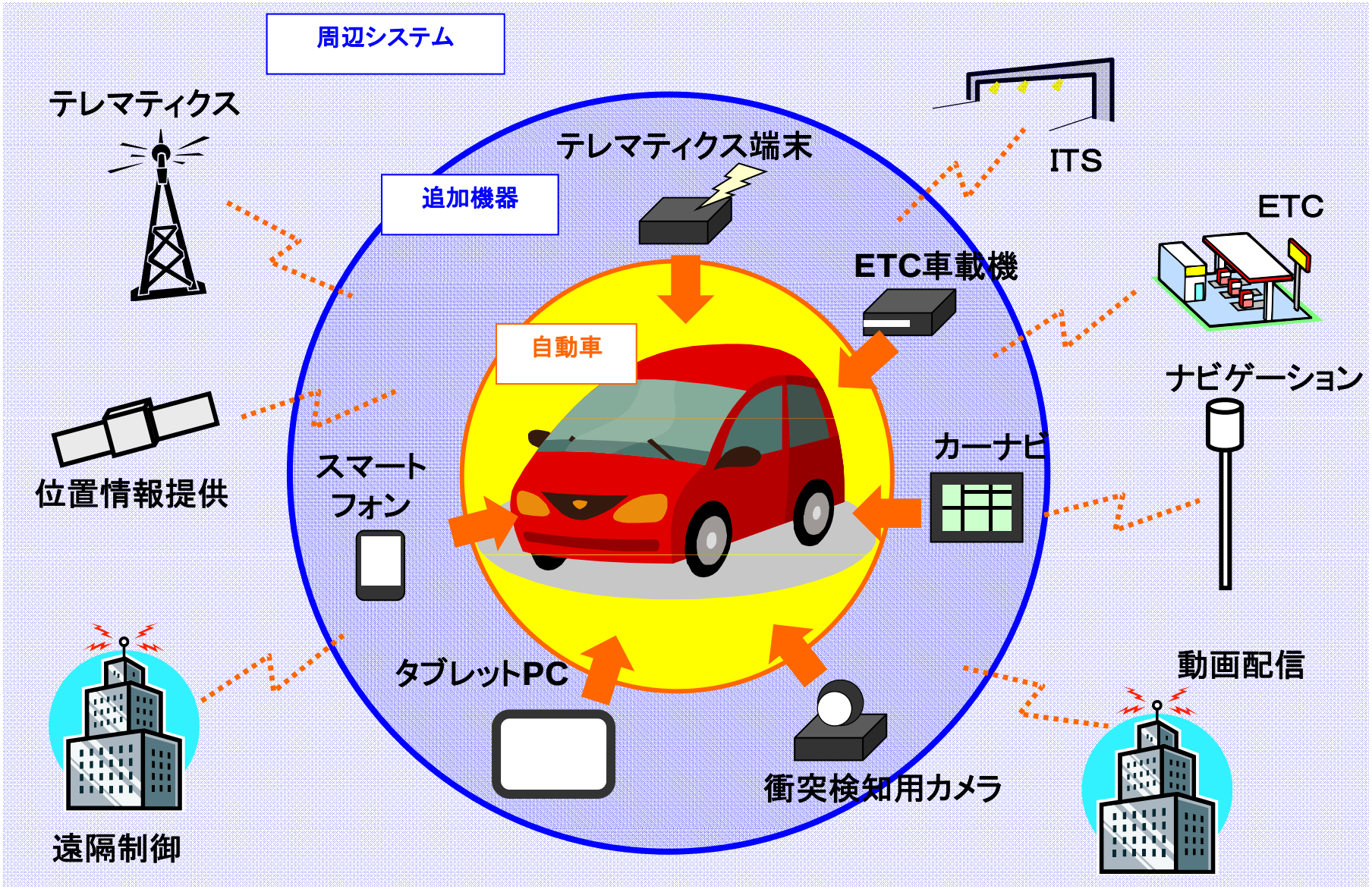
・セキュリティ技術開発、人材育成等の支援、
・ユーザの意識啓発、セキュリティ119番等

重要生活機器連携セキュリティ研究会（CCDSSG）

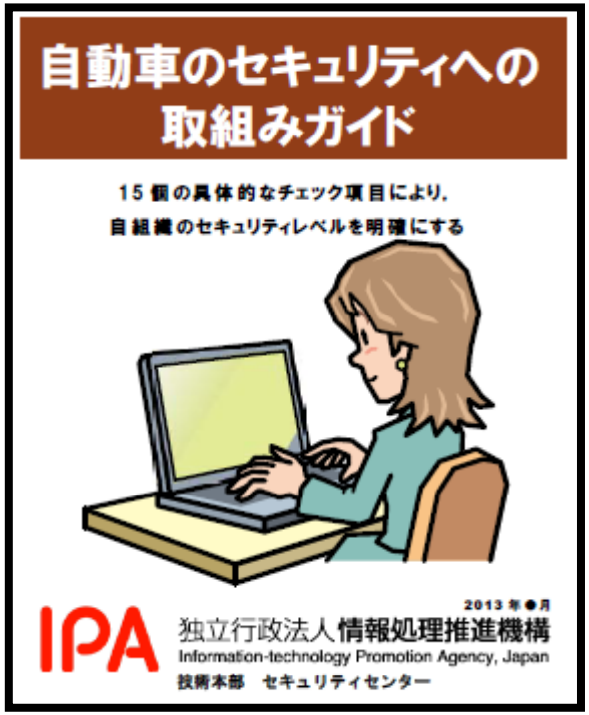
・連携セキュリティの研究成果の発信
・業界間連携の場の設立支援、協力
・2020年においても安全安心な生活の実現をサポート

Safty＆Security

自動車システムのモデル



自動車のセキュリティへの取り組みガイド



自動車セキュリティ報告書
（2009年～）

裏づけ

自動車特化

組込みシステムのセキュリティへの取組みガイド
（2009年策定・2010年改訂）

対象	**組込みシステム全般**
内容	開発時の「組織マネジメント」、企画・開発・運用・廃棄の各フェーズでの「**セキュリティの取り組み項目**」（４レベル）
使い方	組織の**セキュリティレベルアセスメント**とPDCAによる改善

マージ

情報家電におけるセキュリティ対策 検討報告書
（2010年策定）

対象	**情報家電（特にデジタルテレビ）**
内容	システムに存在する**脅威とセキュリティ対策の具体的提示**
使い方	企画・開発フェーズで搭載する**セキュリティ機能の検討・設計の際の参考**

「組込みシステムのセキュリティへの取組みガイド」の自動車版
「情報家電におけるセキュリティ対策検討報告書」脅威・対策分析をマージ

脅威分析手法　組込みシステムへの拡張

1. CVSSによる脆弱性の深刻度評価の手順
2. CVSS評価結果による判断の目安
3. CVSSのしくみ
4. CVSSの課題

カーナビ・サービス停止例の深刻度

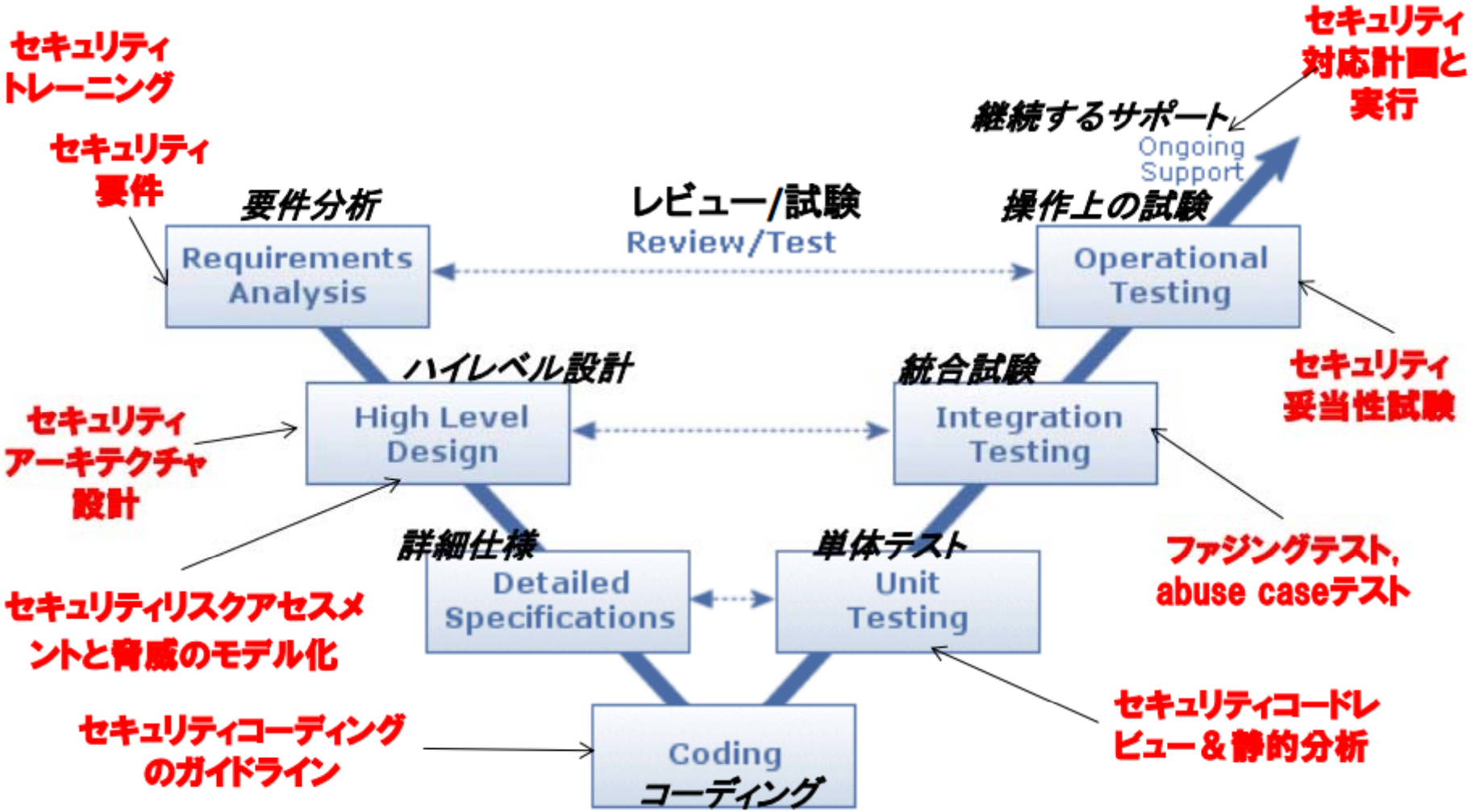
- AV:NWから攻撃可能、AC:複雑(高)、Au:複数認証
  C:なし、I:なし、A:全面的影響、CDP: 壊滅的、TD: 大規模
- 総合値: 4.6→7.3(危険)

MFP・サービス停止例の深刻度

- AV:隣接NWから、AC:攻撃条件単純、Au:単一認証
  C:なし、I:なし、A:部分的影響、CDP: 中程度、TD: 中規模
- 総合値: 2.7→3.7(注意)

V字開発プロセスでの
セキュリティ対応手法の検討

参考：制御システムのセキュリティ開発プロセス

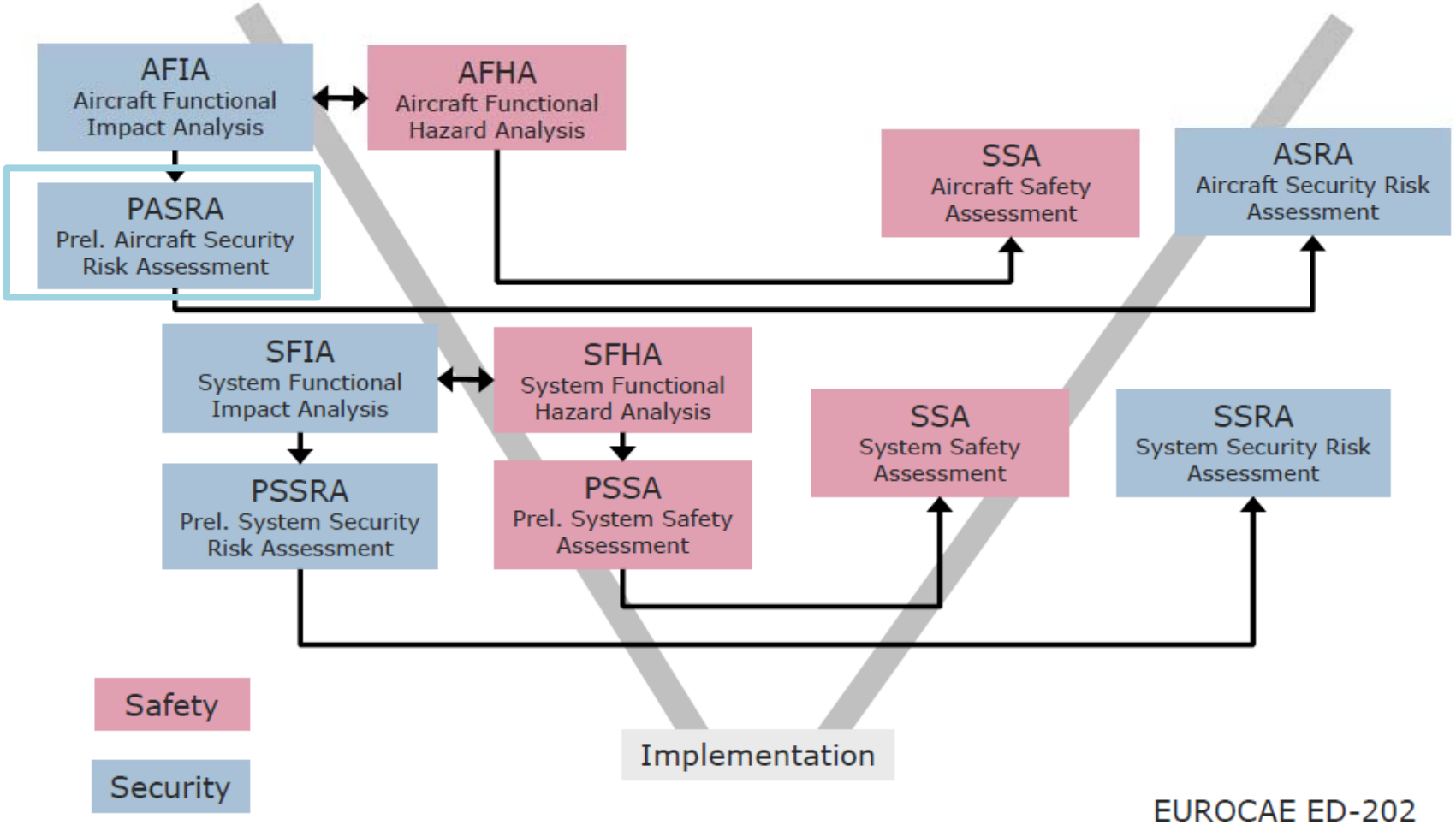


http://www.css-center.or.jp/sympo/2014/documents/sympo20140115_07_cssc_okumura.pdf

航空宇宙Safety/Security開発プロセス

Aerospace Safety/Security Process Interface

10_12th escar Europe_Insights from Aerospace Security.pdf



CCDS　組織体制

2015年度

会長：徳田英幸
　　慶應義塾大学教授
代表理事：荻野 司
　　京都大学特任教授
理事：後藤（情報セキュリティ大学院大学教授）
　　長谷川（eSol社長）
　　服部（ヴィッツ取締役）

社員総会
幹事・正会員

理事会
総会で選任

会員種別
幹事会員
正会員
学術会員
一般会員
賛助会員

総会員数３９（2015/3末）

事務局

幹事会
幹事会員
学術会員
理事

生活機器セキュリティガイドラインWG
幹事会員
正会員
学術会員

ユーザビリティWG
全会員
(当面)

セキュリティ技術WG
全会員

事業推進WG
幹事会員
正会員
学術会員

車載器 Sub WG (JVCK)

金融ATM Sub WG (HOTS)

決済端末 Sub WG (OSK)

ホームネット Sub WG (日立)

個別技術 WG （設置可能）

※クローズドなWGも設置可能。

今後

- 課題
  - 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
  - 脅威分析とリスクの取捨選択
  - 第三者によるセキュリティ評価
  - 自動化された広範囲の脆弱性テスト

2015年7月10日（金） CCDS中期戦略（2015年～2017年）
ー標準化戦略
ー脆弱性検証基盤