JPNIC総会 講演資料

IoTのセキュリティ
～ハッカーによる攻撃の現状と対策ポイント～

2015年12月11日

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. Security By Designに向けて
   - セキュリティ基準・標準化動向
   - セキュリティ対策ポイント

3. まとめ

つながるIoTの世界

（CES2014-2015）

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℠

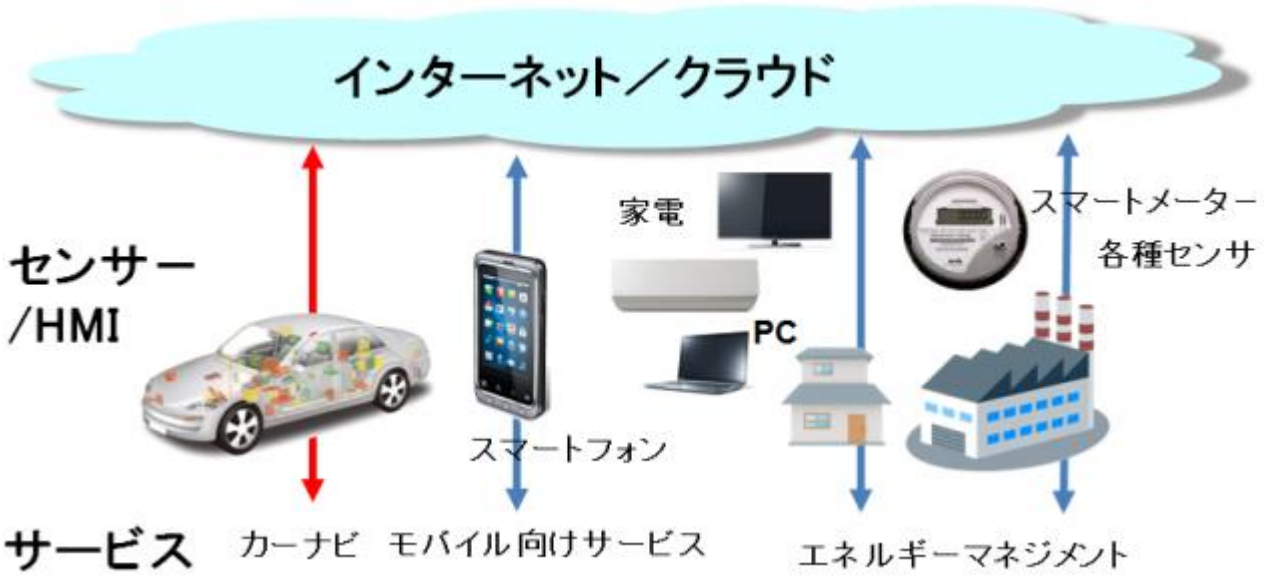
ALLSEEN
ALLIANCE

Internet of Things Consortium

THREAD

新産業にむけた活動が加速！

- サービス革新、新規プレーヤの登場
  - IoTデータをコンテキスト活用



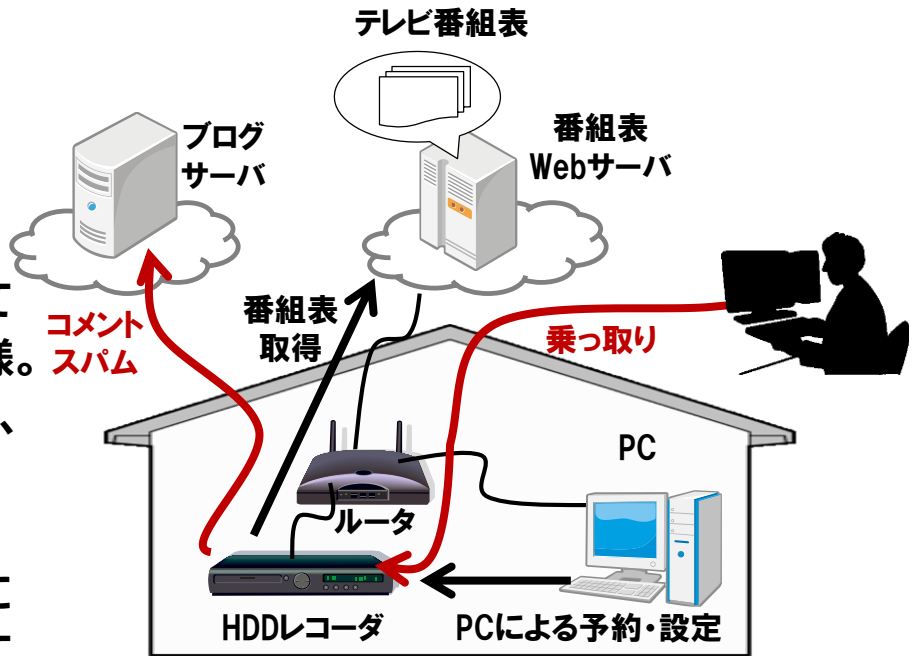
JARI・「IT・CE技術のITSにおける利活用の研究」より
http://www.jari.or.jp/tabid/113/Default.aspx

IoTシステムへの脅威事例

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）

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）

遠隔から車載LANへの侵入

分　類	研究	分野	自動車	時期	2010/06 2015/07	地域	米国

情報源

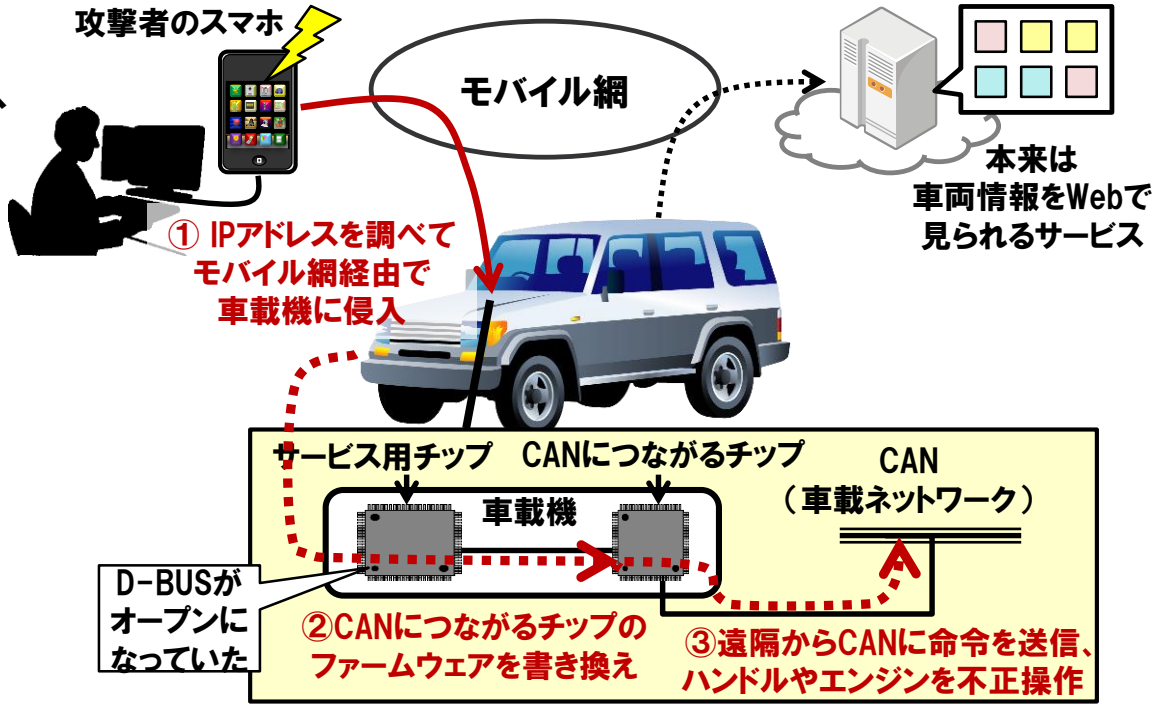
2010研究：ワシントン大学Kohno氏ら論文　http://www.autosec.org/pubs/cars-usenixsec2011.pdf
デモビデオ　http://www.youtube.com/watch?v=bHfOzilwXic
2015研究：http://wired.jp/2015/07/23/connected-car-bug/, http://illmatics.com/Remote_Car_Hacking.pdf

脅威

遠隔から車載LANに侵入する実験の発表、デモ

概要

- 2010年研究では、3G携帯電話、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車両の音声・ビデオ・位置等の記録データの入手についてデモを実施。
- 2015年には全米で47万台に普及しているサービス経由で走行中の車両を攻撃するデモが公開。



（研究論文を基に作成）

ATMのハッキング

分　類	実例	分野	ATM	時期	2014	地域	北米
情報源	14歳の少年2人がATMをハッキング（記事）http://www.edmontonsun.com/2014/06/09/14-year-olds-hack-bmo-bank-machine-staff-doesnt-believe-them スマートフォンでATMをハッキング（記事） http://www.itmedia.co.jp/enterprise/articles/1403/26/news037.html						
脅威	スマホでATMから現金を引き出すウイルス、14歳少年がATMの管理モードに入り表示画面を書き換えなど						

概要

- 14歳の少年2人が、インターネット上で発見したマニュアルを基にATMの管理モードに侵入することに成功。表示画面のメッセージを書き換えた。
  ログイン用のパスワードが初期設定のままだった。
- Symantecは、携帯メールを送信するだけでATMから現金を引き出せるマルウェアが出回っていると警鐘。研究室で実際のATMにPloutusを感染させて、攻撃を再現できたとのこと。

（記事を参考にCCDS事務局が作成）

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

Black hat USA 2015概要

- 会場：Mandalay Bay Convention Center
- 参加者数：約１万人（推定）
  - 主に社会人
- ブリーフィングカテゴリ
  - カテゴリ：暗号、**HW/組込み**、ネットワーク、モバイル、**IoT**、生体認証、OS/ホスト、セキュリティ開発ライフサイクル、防衛策、**スマートグリッド/インダストリ**、企業、バーチャリゼーション、探索技術、マルウェア、リバースエンジニアリング、Webアプリ、フォレンジックス/インシデントレスポンス、リスクマネージメント/コンプライアンス
- 解析ツール紹介
  - アーセナル
    - 解析・モニタリングツール（HW、SW様々）の紹介コーナー
  - スポンサーセッション・ワークショップ（8/6-7）
    - セキュリティベンダーのツール紹介や活用ワークショップ

Jeepを走行中に遠隔操作する研究発表

- Jeepを車載のインフォテイメントシステムを経由してインターネットから操作する研究が発表された
  - 元記事(英文) http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ ※動画あり
  - 要約記事 http://www.itmedia.co.jp/enterprise/articles/1507/22/news060.html
- Chryslerのコネクテッドカーシステム「UConnect」の脆弱性を利用
  - エンタメシステムのチップセットのファームウェアを更新
  - エアコン、ワイパー、ブレーキ、変速、ステアリングに干渉
  - バック中にはハンドル操作も奪取
  - ファームウェアの更新なしでもネットワーク内の他の自動車の情報も取得可能
- Chryslerではパッチ提供して対応（USBまたは整備工場での更新）
- 研究者は2013年にトヨタプリウス、フォードエスケープを自動車内で操作可能であることを示したCharlie MillerとChris Valasek

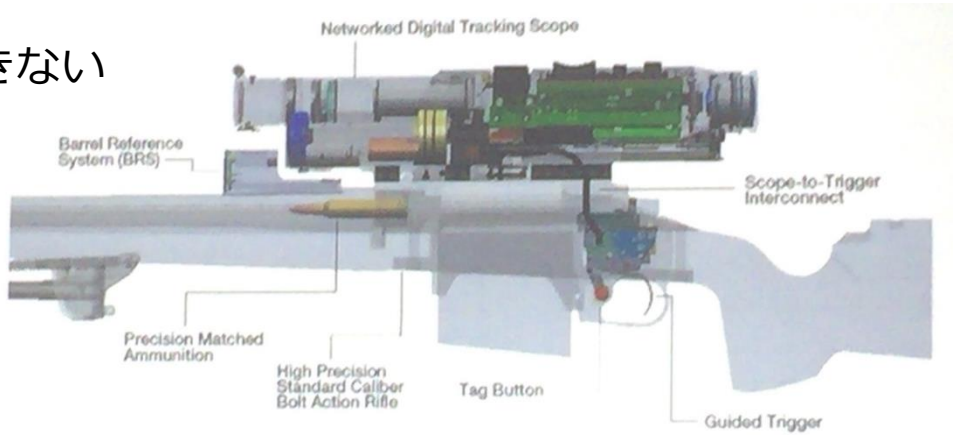
リモート操作で溝におちるJEEP
(出典:wired)

事例：WiFiハッキングによるアタック

- WHEN IOT ATTACKS: HACKING A LINUX-POWERED RIFLE
  Linux搭載の照準装置に侵入し、照準を狂わす

TP750: WiFi接続したスマートフォンで環境に応じた発射タイミング
を割り出す

- SSID：シリアルNo.含む、変更できない
- WPA2 key：変更できない
- API ：un-authenticated
- API 設定は変更できる
  （モードロックと関係無し）



・ハード分解、中身を調査
・ソフト：Admin APIが無認証、無認証でコアシステム関数にアクセス
－＞DB内のGPGによる署名と暗号化ソフトをアップデートできる

メーカサイトにて：
「ハッカーが周囲約30mの範囲内に存在しないことが明らかな場合のみ、
WiFi機能を利用してください」

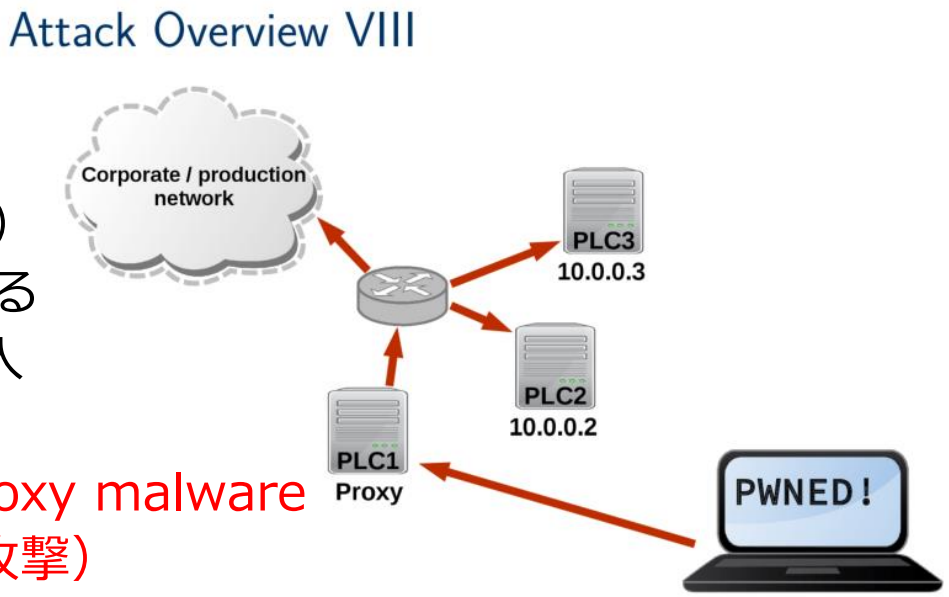
事例：制御システムへのアタック

- Internet-Facing PLCs - A New Back Orifice（シーメンス社製PLCへのアタック）
  イントラネットへの逆侵入

- STUXNET：シーメンス社製の制御機器を攻撃対象にしたマルウェア
- 一方、制御システムのインターネット接続が増加している

アタック手順：

1. PLCにインターネット経由で接続
2. ソフトウェアを注入（マルウェア）
3. ローカルネット上の装置を見つける
4. Proxy機能を最初の接続機器に注入



Connecting to PLCs through the proxy malware
（SOCKS5手順のProxy経由でPLCを攻撃）

DEF CON23概要

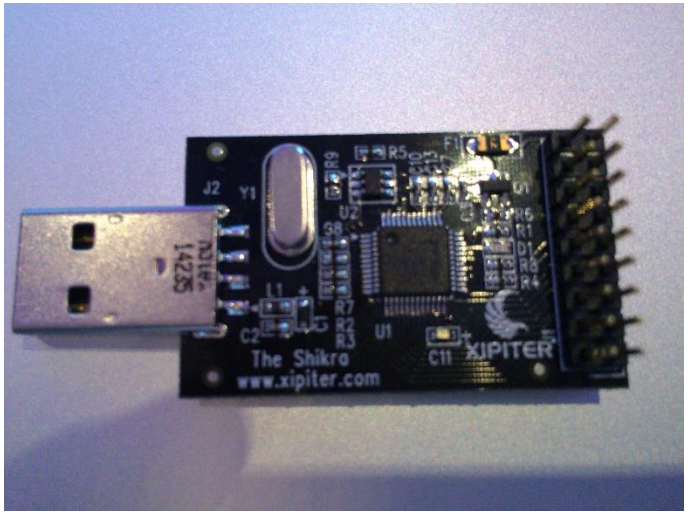
- 会場：Paris/Bally'sの会議室・ホール
- 参加者数：約1.5万人（推定）
  - 学生から社会人まで
- カバーされてる分野
  - 分野：
    バイオハッキング
    カーハッキング
    Crypto&Privacy
    ICS (Industrial Control System)
    IoT
    Lockpick
    Social Engineering
    Tamper Evident
    ワイヤレス
    データ
    パケットハッキングVill

IoT VILLAGE

DEFCON:CAR HACKING VILLAGE

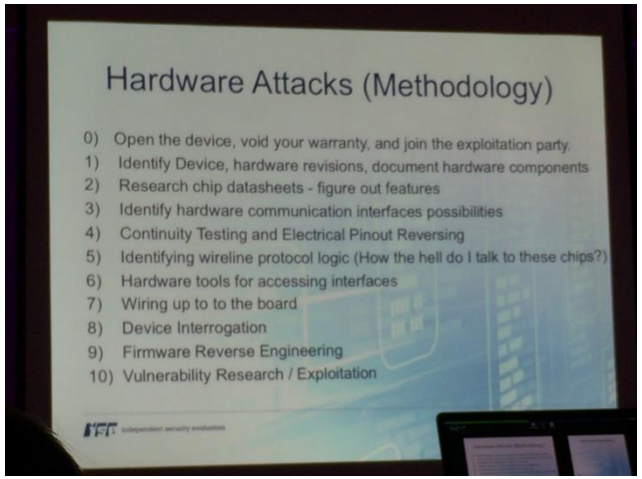
DEFCON:IoT Village

解析ツールの紹介



DEFCON:ハード解析チュートリアル

- IoTビレッジで照会された、IoT（ハードウェア）アタックの「いろは」とは？
  0. まず筐体を開ける！（製品保証は捨てろ）
  1. HWを構成するコンポーネントとリビジョンを把握する
  2. チップのデータシートを探せ（データシートは最良の友！）
  3. HW内の通信とI/Fをできる限り特定する
  4. ピン出力をリバースする
  5. Wire上のプロトコルを解析するチップは何を話してるか識別する
  6. I/Fとアクセスするハードウェアツールを用意する（探す、なければ作る）
  7. ボードに接続（wiring）する
  8. デバイスを調査する
  9. ファームウェア挙動をリバースする
  10. 脆弱性を調査・探索実施する



- ⇒「箱は開けられる前提で製品開発が必要」

IoTシステム攻撃者の視点

- ターゲットとなるのは、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）
  - ファームウェアアップデート機能を狙う！
- どういう仕組みで動いているか、まずは分解してみる
  - 破棄した基盤・パーツから情報収集
- 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…
  - コストパフォーマンス重視！

参考：組込み機器検索サイト「SHODAN」

- オフィス機器、家電、信号機、発電所などの機器を検索

http://www.shodanhq.com/

2．Security By Designに向けて

2-1　標準化の動向

oneM2M Security WG

項目	内容
組織の役割	• 世界の主要なSDO（標準化機関）が集まりM2Mの共通部分を切り出して標準を開発する
M2Mアプリ分野	• 幅広いM2Mアプリケーションを想定（モバイル、ホームネットワーク・家電、ヘルスケア、自動車）

セキュ検討状況	• oneM2M リリース1を標準化（2014年7月）事実上のドラフト
	• 内容は通信時の機器認証が中心。
	• リリース2の標準化を作業中:
	  • ホップバイホップではないE2Eのダイナミック認証
	  • サーバ側のセキュリティ機能を呼び出すAPI（common API for Security Function to call security service）

ITU-T JCA-IoT

項目	内容
組織の役割	• 国際電気通信連合（ITU-T）でIoT標準化団体の間で重なる部分を共有し調整を検討 • 作業部会（WG）のITU GSI （Global Standard Initiative）がJCA-IoTに動向を報告 • 参加組織はIEEE, IETF, W3C, OMA, oneM2M
M2Mアプリ分野	• 各標準化団体の調整機関で、幅広く情報収集
セキュ検討状況	• ITU-T SG17 Q6,7,11などで個別にIoT Securityの検討
その他	• IEEEにはIoT標準化中のP2413がありIoT全体のアーキテクチャをカバー • ISO/IECのJTC1はIoTアプリケーションをカバーする新しいPRJ. • ITU-T SG16はITS/eHealth/IoTアプリサービスをカバーしている

SAE TEVEES 1

項目	内容
組織の役割	• 自動車メーカーとサプライヤで構成される米国の自動車技術会（SAE）のセキュリティ委員会（TEVEES）は、米国自動車標準としてセキュリティガイドラインとハードウェアセキュリティ技術を調査検討
M2Mアプリ分野	• 自動車（駆動系を含むコア部分、車載機）
セキュ検討状況	• セキュリティガイドラインは2015年内にSAE内部に公開予定
その他	• 2013年の発表ではガイドライン、HW技術ともに2014年中ごろにSAE内部公開（予定）

ETSI ITS Security WG

項目	内容
組織の役割	• 欧州の標準化機関ETSIのITS標準化活動で、セキュリティ機能の標準化を行うWG。C2C-CCからの標準化案をETSI標準にするため、自動車メーカーとサプライヤも参加して関連する既存の標準との調和を図っている
M2Mアプリ分野	• 自動車（V2X通信車載機、路側器）
セキュ検討状況	• 保護仕様の中には脆弱性試験は含まれない。セキュリティ機能が動作することのみ • テスト方法はV2X機器メーカが自己テストする形。
その他	• ETSI ITS Rel1に準拠したV2X機器の相互接続テスト会（Plugfest）が2015年3月末に行う予定。このPlugfestではセキュリティ機能の相互接続テストも行われる見込み。

C2C-CC WG Security

項目	内容
組織の役割	• 欧州自動車メーカーとサプライヤがV2X（車車間・路車間）通信と機器の仕様を開発、提案する組織。提案は欧州標準化機関であるETSIが標準化する
M2Mアプリ分野	• 自動車（V2X通信車載機、路側器）
セキュ検討状況	• V2X通信プロトコルのセキュリティ機能を標準化: ETSI ITSリリース1（2014年2月発行済み） • 欧州と米国の間でセキュを含むV2X通信の相互運用性を標準化 • 欧州のV2X車載機のセキュを含む適合基準を開発中
その他	• C2C-CCではサービス用のインフラの一つとしてPKIが必須だが、サービス用PKIの提供は2016年後半になったためC2C-CC仕様のITSサービス開始も2016年後半以降に遅れる

IoTシステムのセキュリティに関連する標準の動向

- **要件が異なるため、分野ごとにセキュリティの対応レベルが異なる**
- **自動車は標準化と検討が幅広く進んでいる**

○ 標準あり
△ 検討中、一部
－ 標準見当たらず

特徴		共通	自動車*1	エネルギー	ヘルスケア	家電
要件	ユースケース	△	○	○	△	△
	脅威分析	－	○	○	△	－
	セキュリティ要求	－	○	△	△	△
対策	信用の担保	○	△	△	△	－
	アクセス制御	○	△	△	△	△
	機器認証*2	△	△	△	△	△
	アプリ認証	△	△	－	△	△
	メッセージ認証	－	○	－	△	△
	匿名化	－	△	－	△	－
	堅牢性	－	△	△	－	△
提示	セマンティック	－	△	－	△	△
	利用時品質提示	－	△	－	－	－

*1: 自動車は制御システムと車車間通信の両方を含む
*2: マシン間での処理のため、人のユーザ認証は除外

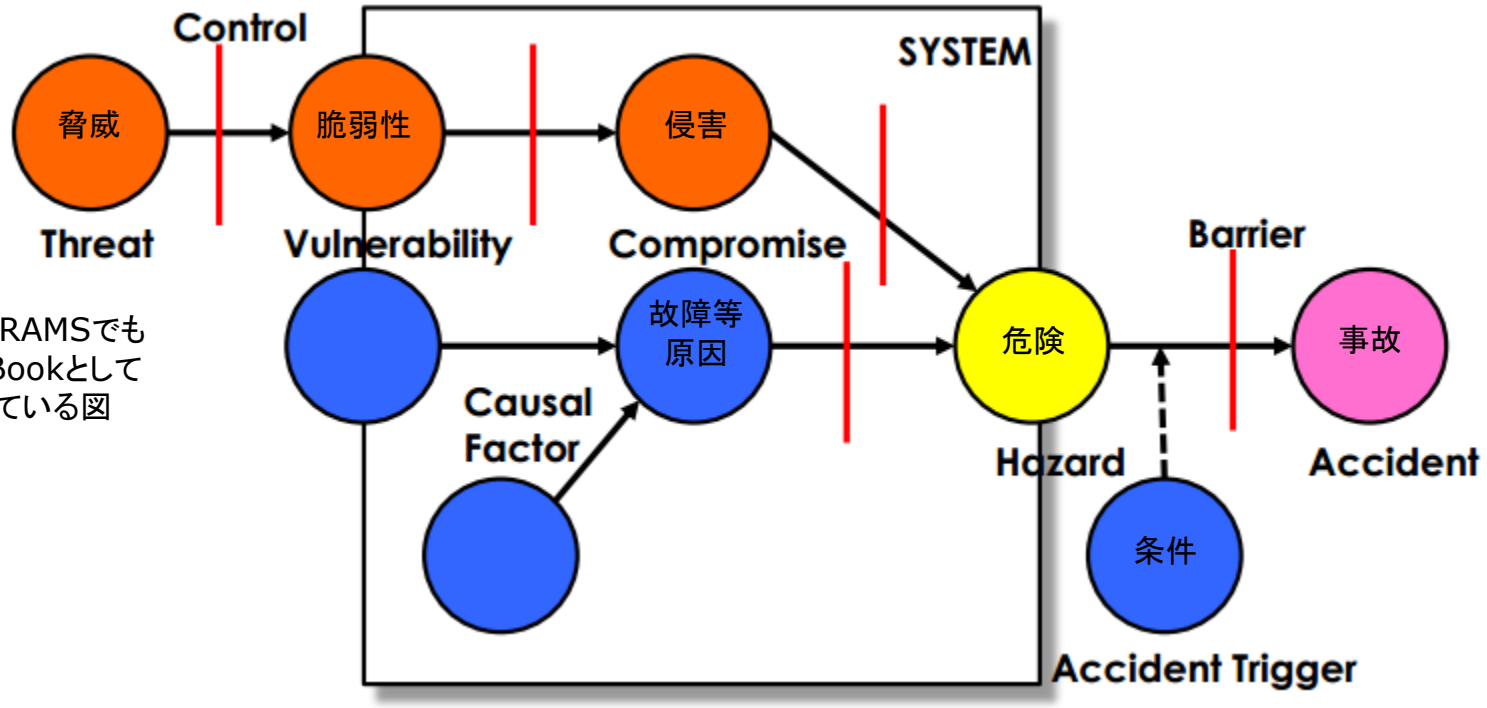
セーフティ標準で求められるセキュリティの例

- IEC 61508-1:2010, 1.2, K)
  - 工場・プラントなど制御システムの機能安全標準
  - “requires malevolent and unauthorised actions to be considered during hazard and risk analysis. […]”
  - その他2点: 7.4.2.3, 7.5.2.2
- draft EN 50126-5:2012
  - 鉄道分野の機能安全標準 (RAMS)
  - “The Safety Case shall demonstrate that […] misuse-based failures on external interfaces do not adversely impact on the safety integrity of the system”

http://sesamo-project.eu/sites/default/files/downloads/publications/02-isse14-sesamo.pdf

セーフティとセキュリティ分析の構造

上にセキュリティの
影響を図式化



下半分はRAMSでも
Yellow Bookとして
知られている図

http://sesamo-project.eu/sites/default/files/downloads/publications/02-isse14-sesamo.pdf

リスクの構成要因

	機械製品	情報システム
発生する原因(潜在)	欠陥(defect)	脆弱性(vulnerability)
発生のきっかけ	故障(failure)	脅威(threat)
発生する現象	ハザード(hazard)、事故	事象、現象
発生する確率	故障確率、制御性、…	攻撃能力、攻撃/発生機会、動機/利得/価値
リスクの影響	被害	被害

消費者安全調査委員会
http://www.caa.go.jp/csic/
リスク = 自然災害 x 脆弱性
http://www.jsnds.org/contents/shizen_saigai_back_number/ssk_31_3_169.pdf
外力(Hazard) x 脆弱性(Vulnerability) x 人・資産(Exposure)
http://www.jice.or.jp/international/nikkan/pdf/nikkan2010_02.pdf
被害＝ハザード×脆弱性
http://www.bousai.go.jp/kaigirep/hakusho/h16/BOUSAI_2004/html/honmon/hm150104.htm

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

NISC National Information Security Center

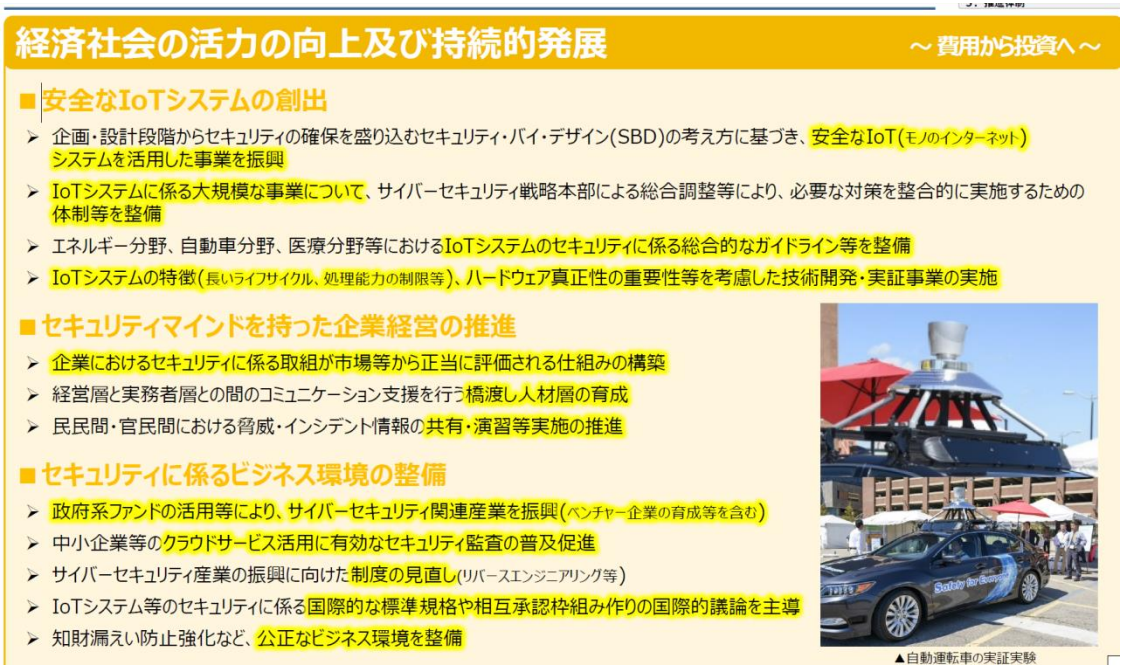
…また、様々なメーカーから提供される、自動車、HEMSや家電等の生活機器についても、ネットワーク接続が進みつつあるが、生活機器は、連携対象が多種多様であることや、操作する者が一般消費者であるという特性があることから、この分野において、分野横断的な情報セキュリティ技術の研究開発や国際標準化等の対応についても検討していく。

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

サイバーセキュリティ2015

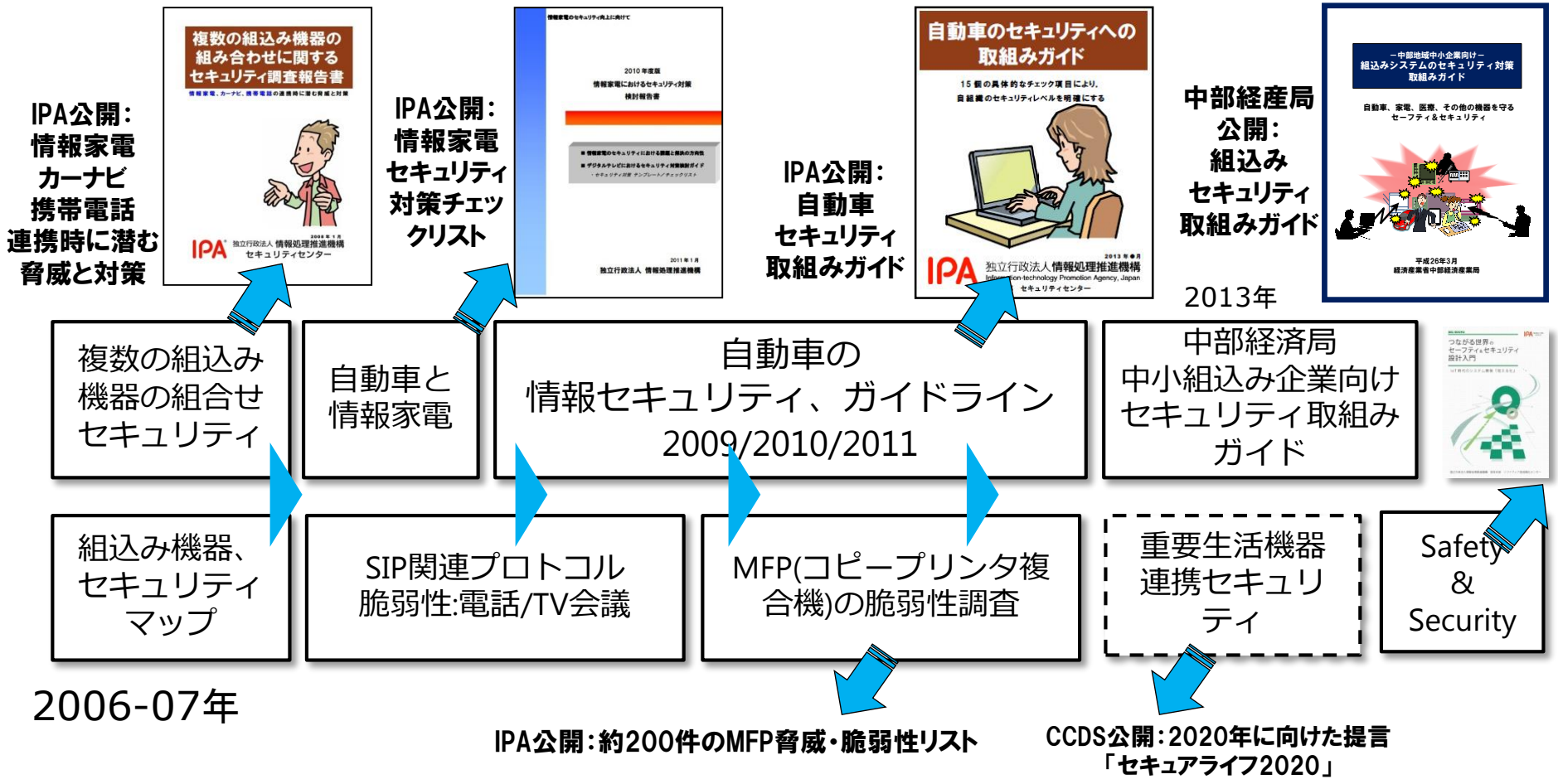
- NISCで2015年9月に発表
- IoTシステムにおけるセキュリティ方針
- 主なポイント
  - IoTシステムのセキュリティに係る**体系・体制の整備**
    - **セキュリティｂｙデザイン**の考え方を定着させる
  - IoTシステムのセキュリティに係る**制度の整備**
    - 各分野におけるガイドライン・セキュリティ基準、評価技術、脆弱性情報の集約
  - IoTシステムのセキュリティに係る**技術開発・実証**
    - 基礎研究、リスク評価、評価・認証制度
  - セキュリティマインドを持った企業経営の推進
    - 経営層の意識改革
    - セキュリティ人材の育成
  - セキュリティビジネス環境の整備
  - 安全・安心なサイバー空間の利用環境構築、利用者の取り組み推進
  - サイバー犯罪への対策、等々

セキュリティ対応の動向（ISO TC204 WG16）

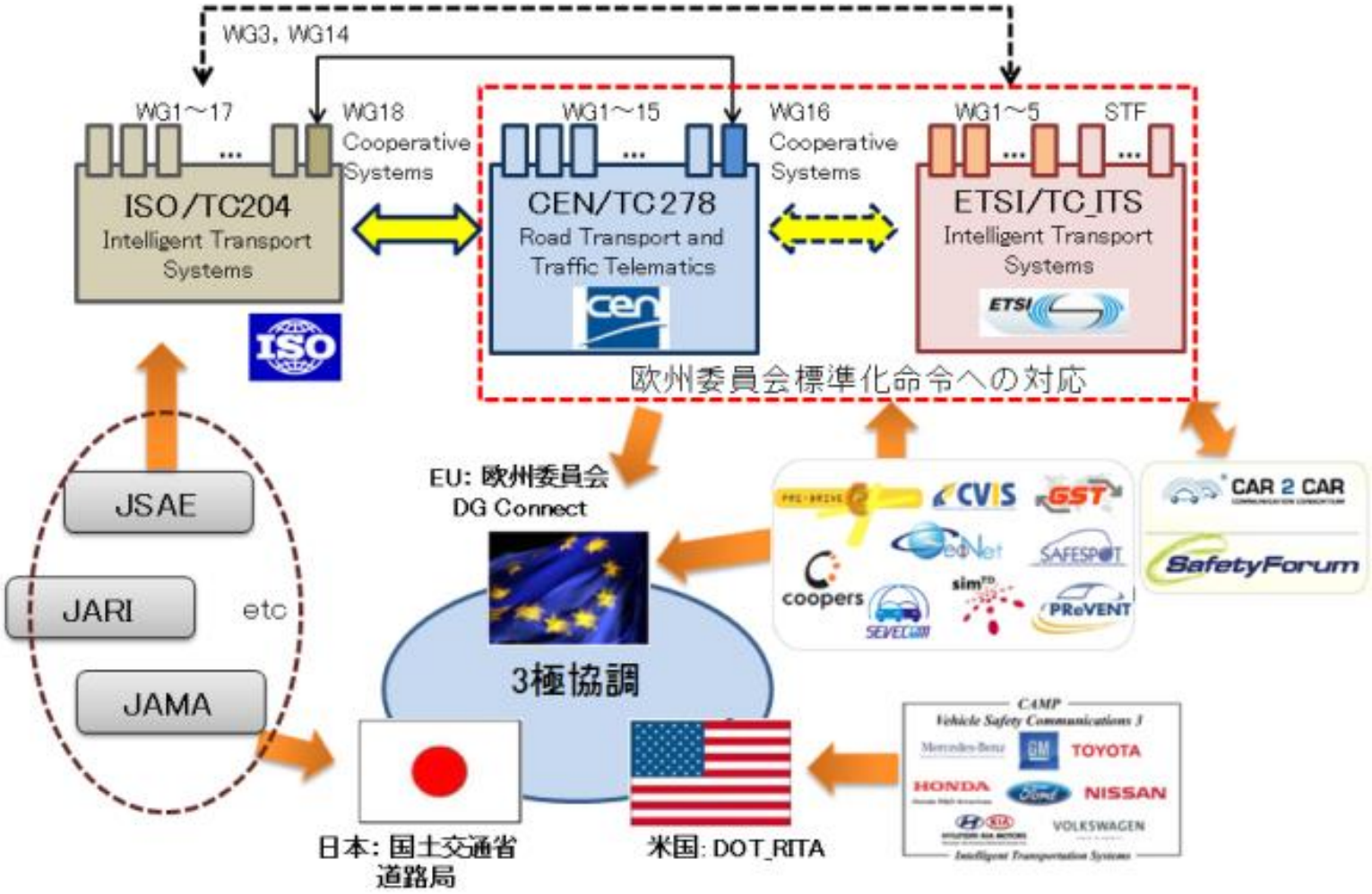
- ISO 24100 プローブ個人情報保護　(2010年)
  - プローブ情報サービスで取り扱われる個人情報
    - 「プロバイダなどとの契約登録情報
    - 「プローブ情報提供者の識別情報」
    - 「通信アドレス」、「認証用パスワード」、
    - 「通信ログ」、「プローブ情報自体に含まれる個人情報」等
  - プローブ情報提供者が安心して情報を提供するために、個人情報保護に関する法律の遵守に加えて、「関係者が守るべき事項（ガイドライン）の作成」、「その達成に必要な設計指針の標準化」を図っています
- ISO PWI 16461 プローブ情報システムにおける匿名性に関する要件整理と評価基準
  - プローブ情報のプライバシー評価基準を数値化、見える化
  - プローブ情報システム間の相互認識･接続について検討
  - 標準化作業中

IPAでの組込みセキュリティの取り組み

- これまで
  - IPAの組込みシステム・自動車セキュリティガイド策定や中部経産局のセキュリティガイド策定を通じた組込みセキュリティ普及



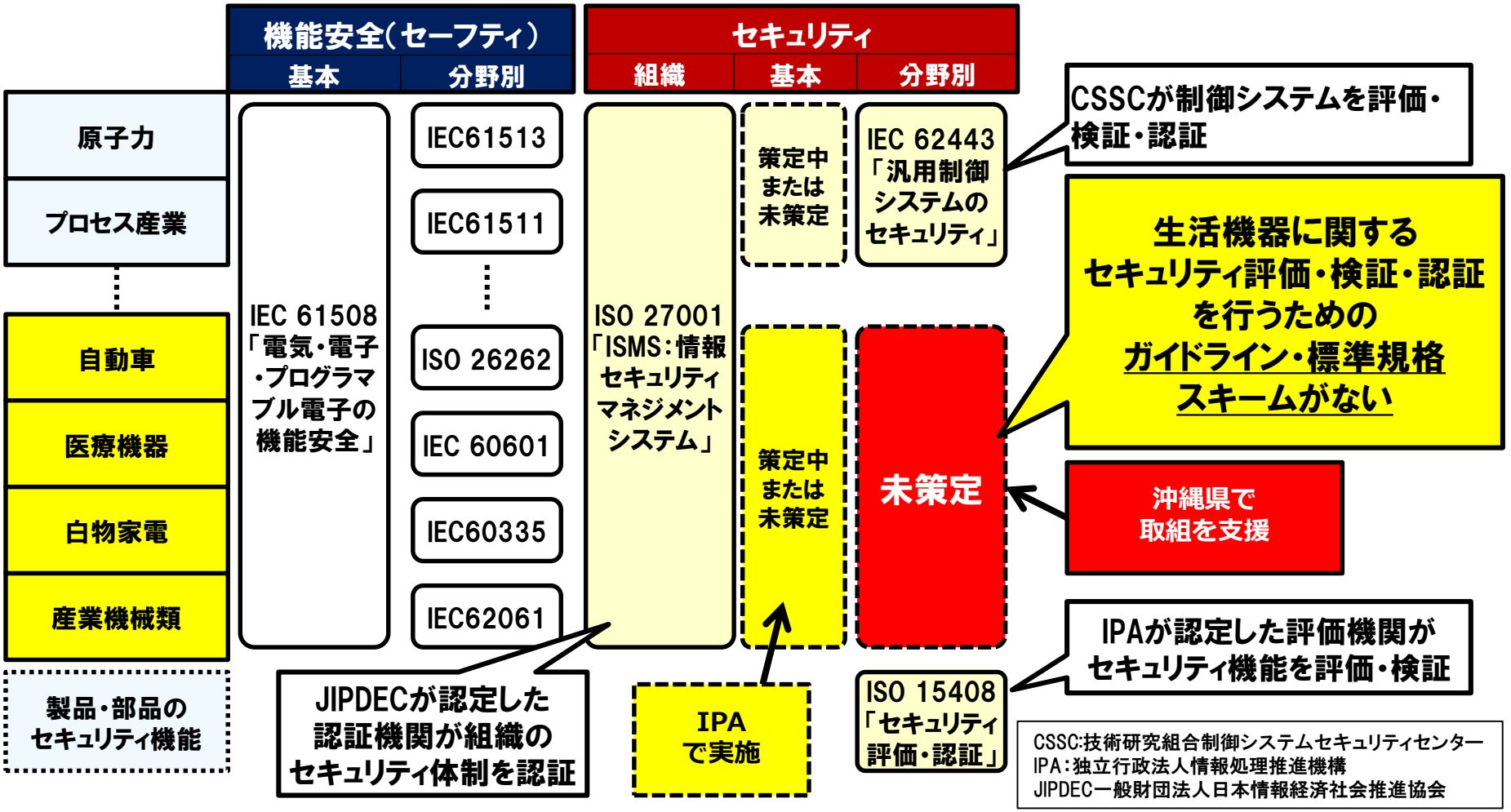
自動車の標準化の全体像



JARI・「ITSに関する国際的な標準化の取り組み」
http://www.jari.or.jp/tabid/113/Default.aspx

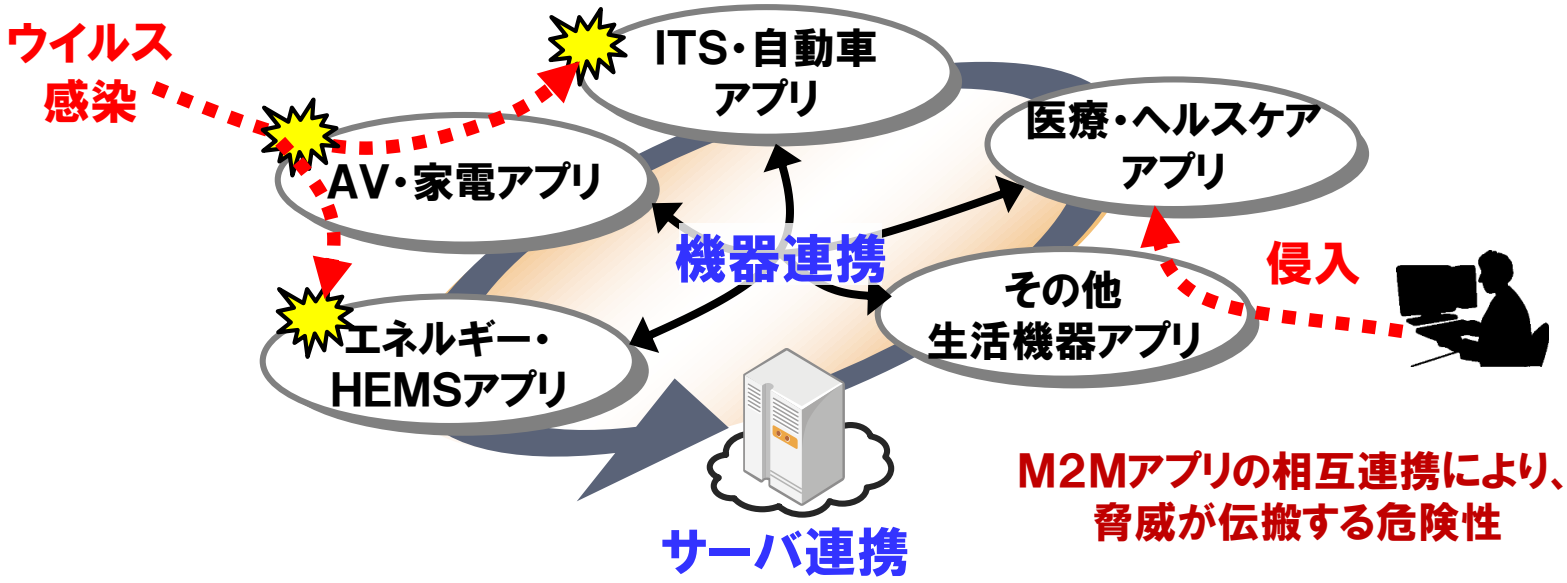
機能安全とセキュリティ

- 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。



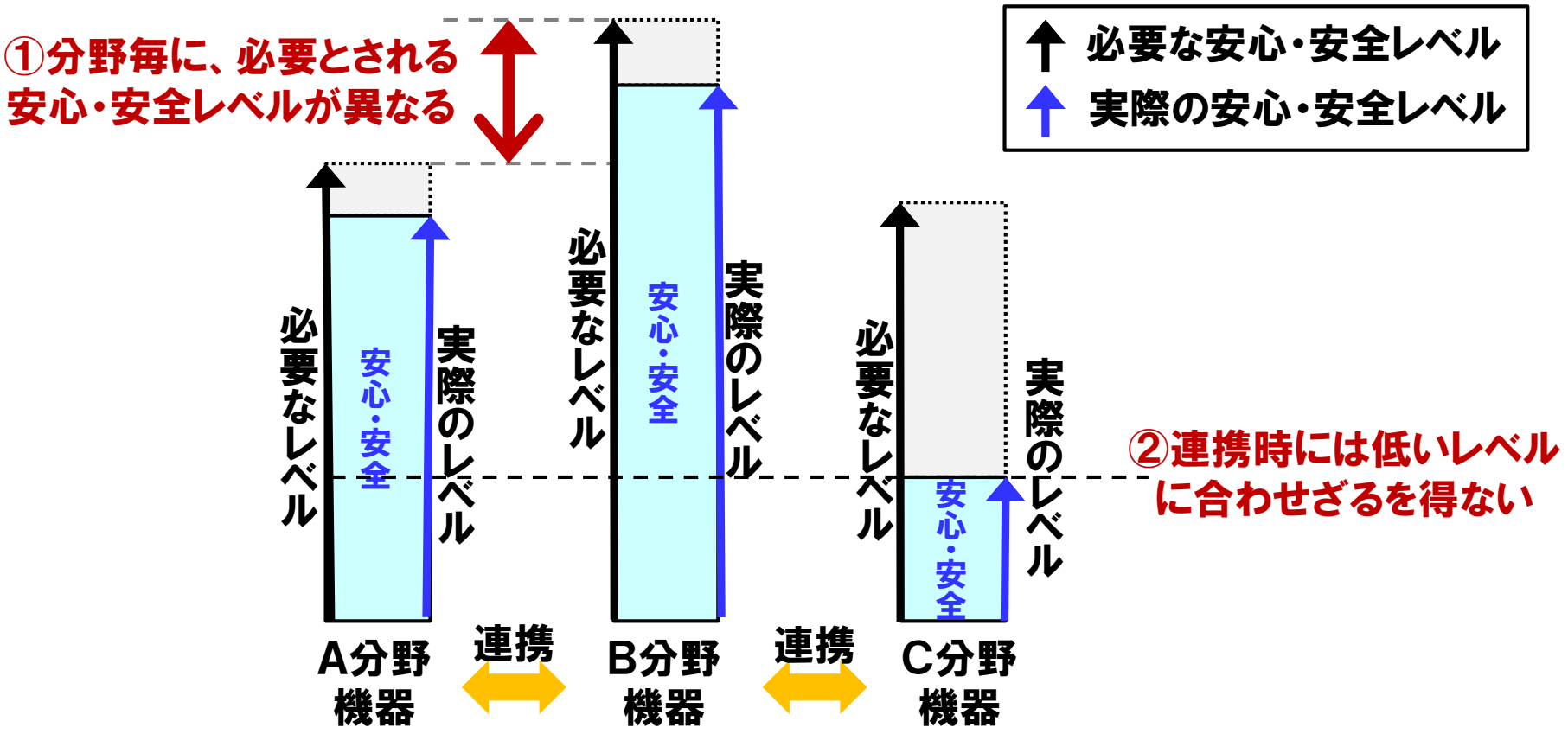
重要生活機器連携セキュリティ協議会

- 脆弱な生活機器を通じて他の生活機器にも侵入されたり、M2Mアプリケーションのネットワーク連携を通じてウイルスの感染が広まる脅威が想定される。



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

分野で異なる安心・安全レベル



外部団体との連携関係

CCDS ⇔ NISC 内閣サイバーセキュリティセンター National center of Incident readiness and Strategy for Cybersecurity

IoTセキュリティガイドライン策定 ⇔ IPA Better Life with IT 情報処理推進機構

つながる世界の開発指針検討WG

・開発プロセスガイドライン：**Security by Design**
・検証ガイドライン　　－＞国際標準化に向けて
安心、安全なサービス・製品開発を目指す！

IoT脆弱性検証基盤構築 ⇔ 沖縄県 OKINAWA PREFECTURE

・脆弱性検証ツール（業種毎）
・脆弱性検証シナリオの策定
セキュリティの観点を組み入れた脆弱性基盤を構築！

セキュリティと対策コストのバランス

製品・サービスの対価 ＞ 対策コスト

機能と構造

複雑になるとコスト増

セーフティ
ISO/IEC 61508 SIL 1～4
ISO 26262 ASIL QM, A～D

セキュリティ
ISO/IEC 15408/CC EAL 1～7
FIPS 140-2 Level 1～4
ETIS ITS/C2C-CC TAL 1～4

対策技術

使い方、構造による対策も

セーフティ等
重要要件

品質レベル

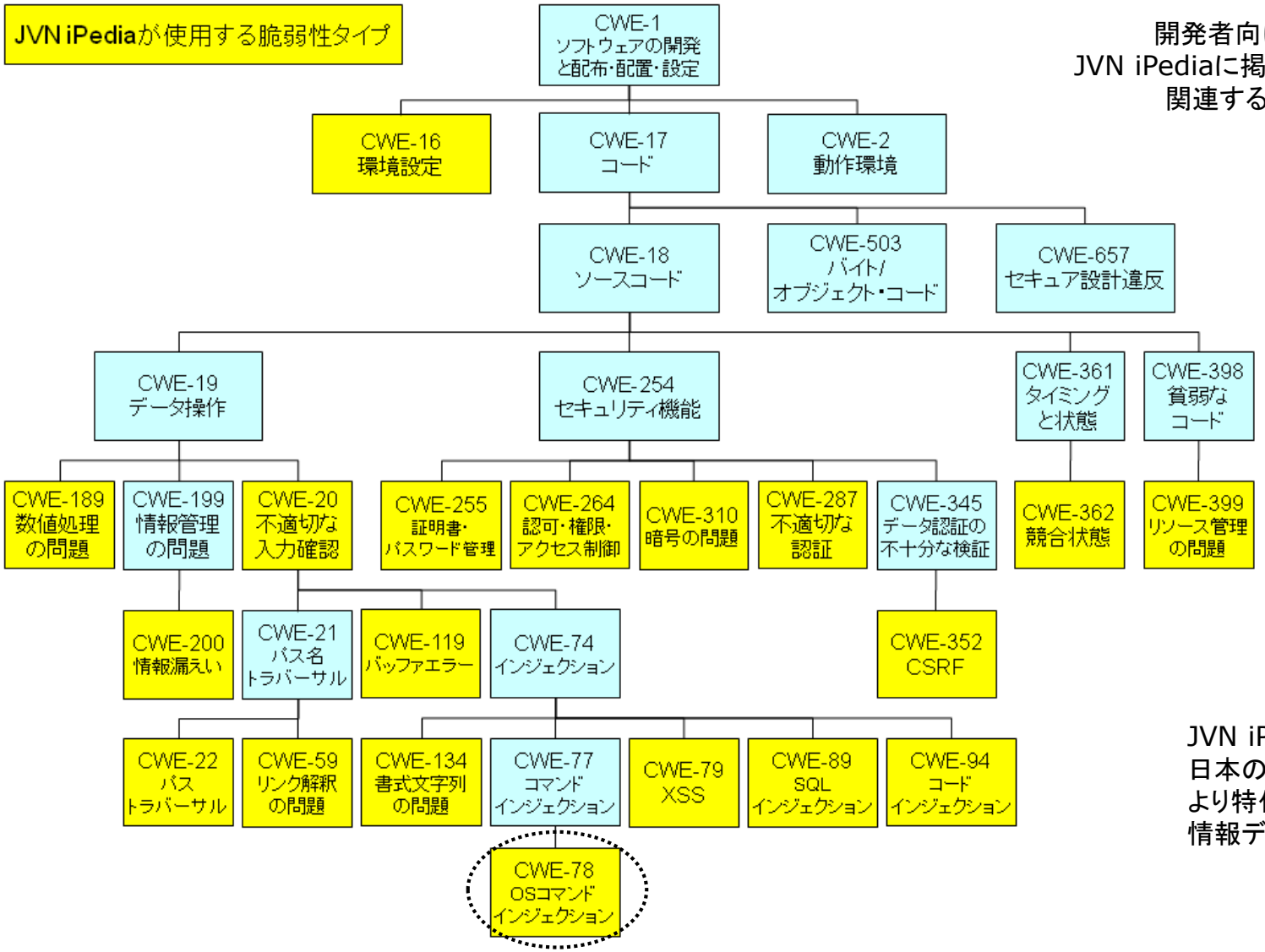
単機能のほうが品質上

業界ごとに異なる
考え方と基準がある

IoTシステムのセキュリティ対策ポイント

1　脆弱性を知る

脆弱性の例(JVN iPediaより)



開発者向けの階層構造図から、
JVN iPediaに掲載する脆弱性タイプに
関連するものを抜き出し(黄色)

JVN iPedia:
日本の製品について
より特化した脆弱性
情報データベース

共通脆弱性タイプ一覧CWE (Common Weakness Enumeration)概説, https://www.ipa.go.jp/security/vuln/CWE.html

脆弱性の例(OWASP Top10より)

順位	脆弱性(2013年版)
A1	インジェクション
A2	認証とセッション管理の不備
A3	クロスサイトスクリプティング(XSS)
A4	安全でないオブジェクト直接参照
A5	セキュリティ設定のミス
A6	機密データの露出
A7	機能レベルアクセス制御の欠落
A8	クロスサイトリクエストフォージェリ（CSRF）
A9	既知の脆弱性を持つコンポーネントの使用
A10	未検証のリダイレクトとフォワード

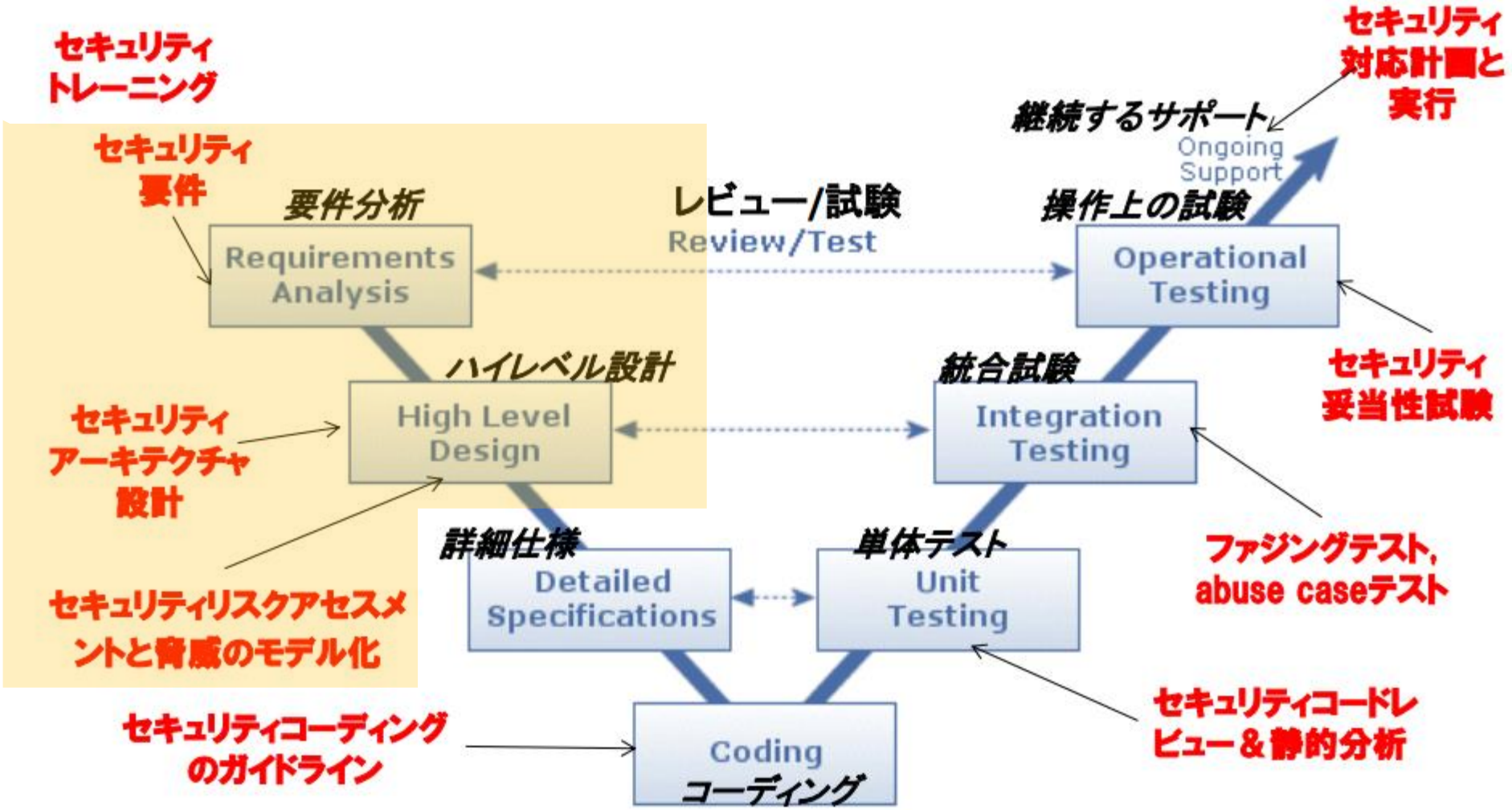
主にクラウド側の脆弱性**サーバー機能にも影響する**

OWASP:
Webアプリケーションのセキュリティ情報を共有する業界団体

「OWASP Top 10 for 2013」の日本語版を公開（OWASP）
http://scan.netsecurity.ne.jp/article/2013/10/24/32779.html

2　V字開発プロセスでの
セキュリティ対応手法

V字開発プロセスでのセキュリティ対応

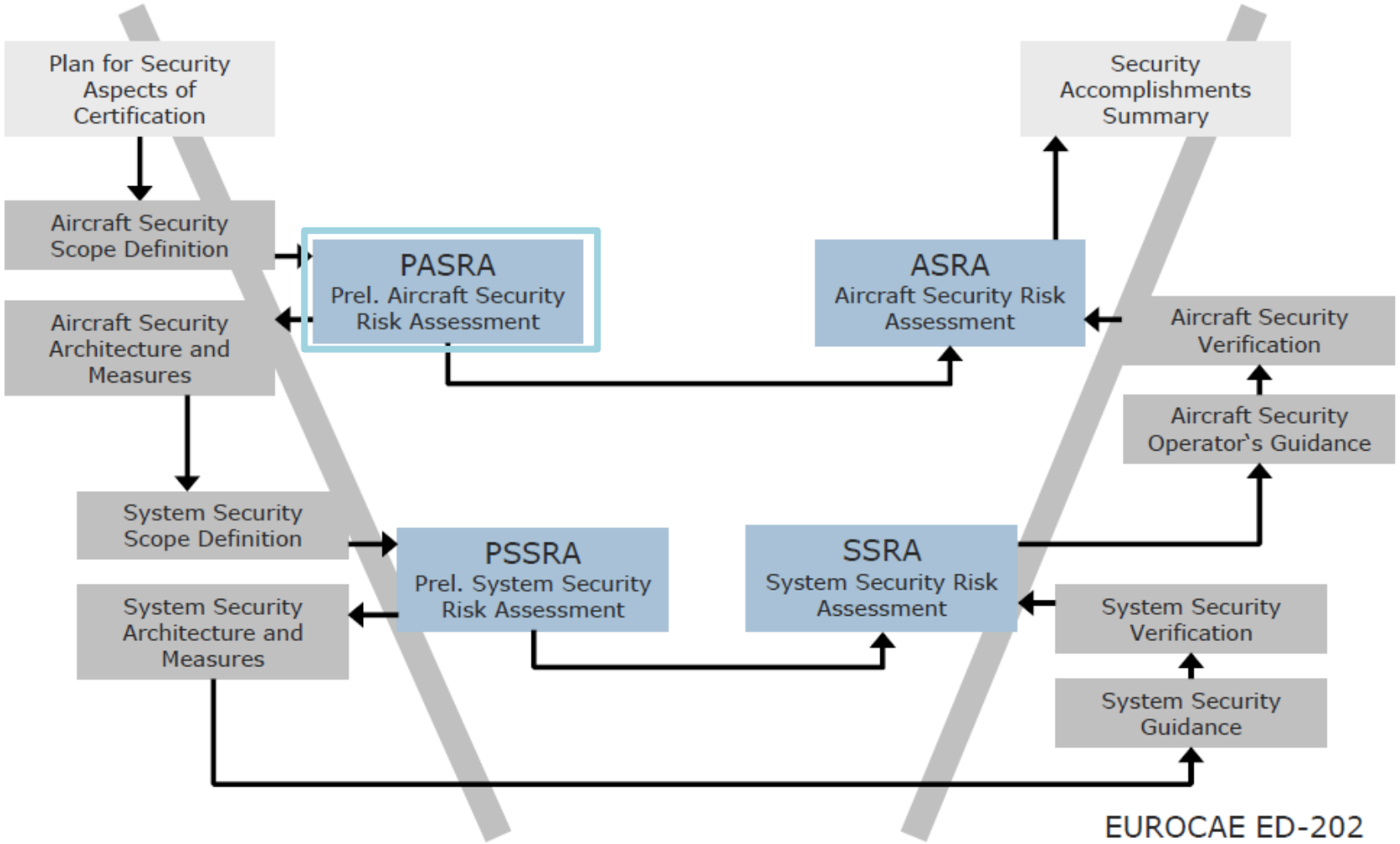


http://www.css-center.or.jp/sympo/2014/documents/sympo20140115_07_cssc_okumura.pdf

参考：航空宇宙Security開発プロセス

Aerospace Security Process

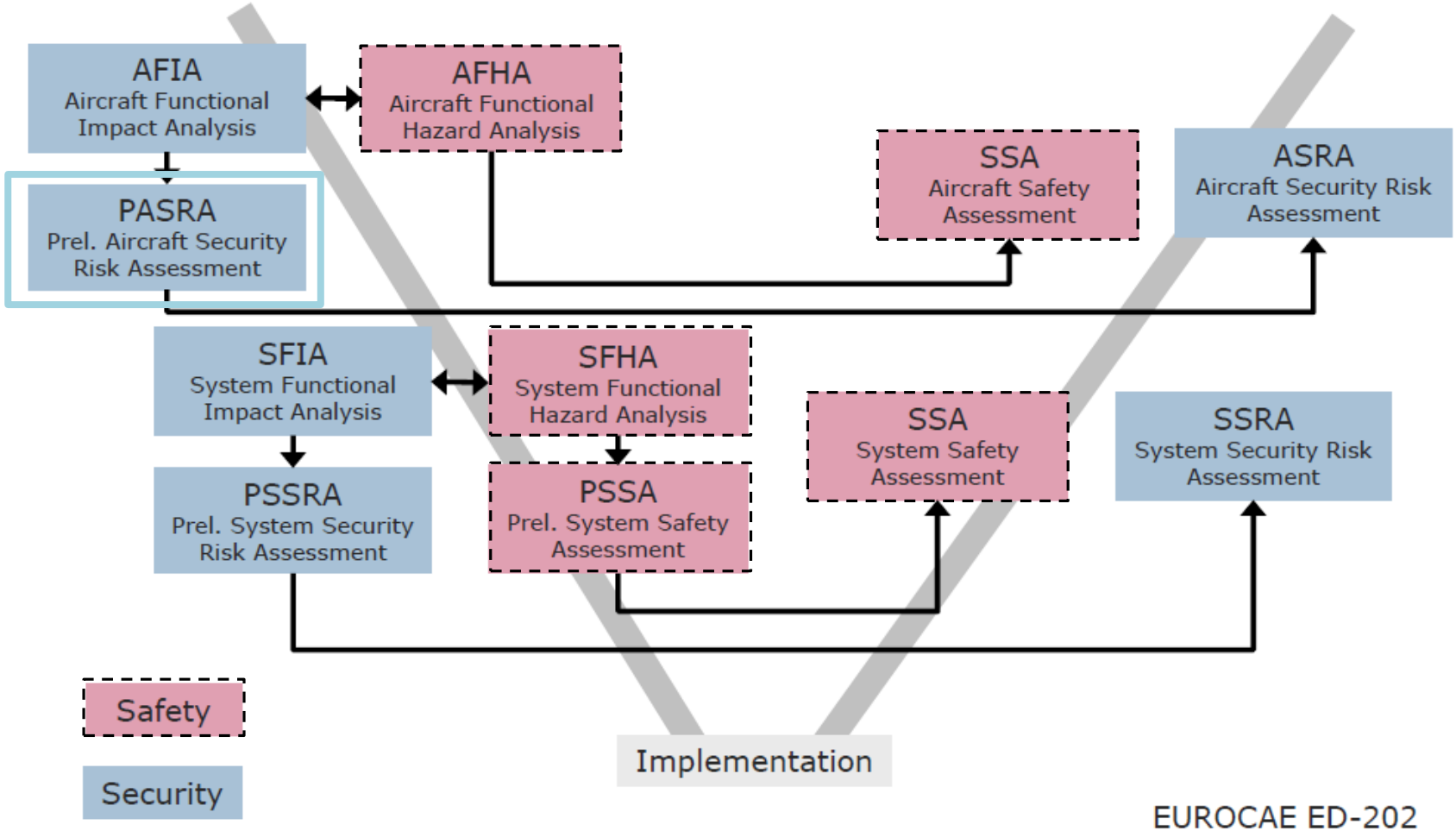
10_12th escar Europe_Insights from Aerospace Security.pdf



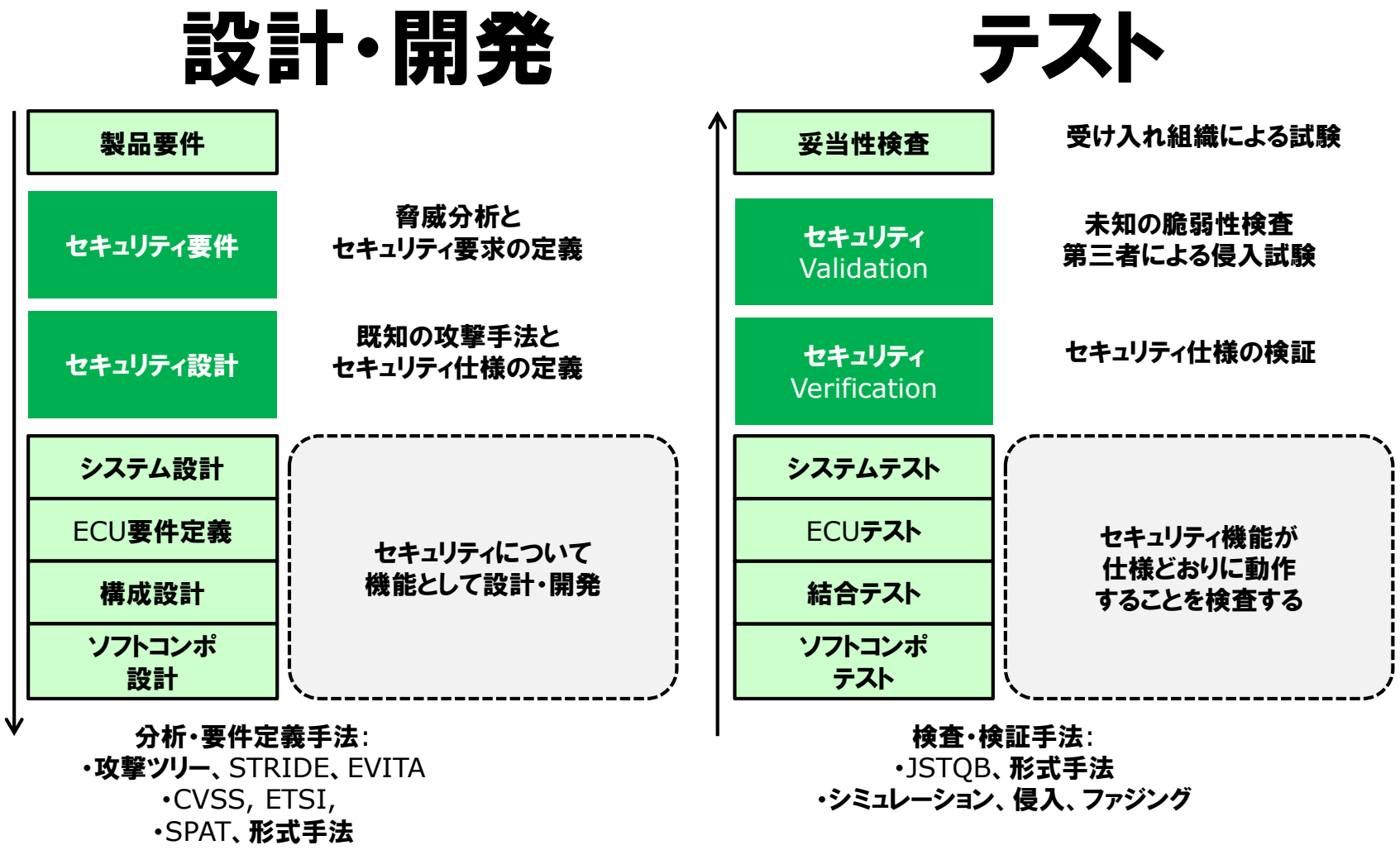
参考：航空宇宙Safety/Security開発プロセス

Aerospace Safety/Security Process Interface

10_12th escar Europe_Insights from Aerospace Security.pdf



セキュリティ設計開発プロセス
既存の品質保証開発プロセスからの差分



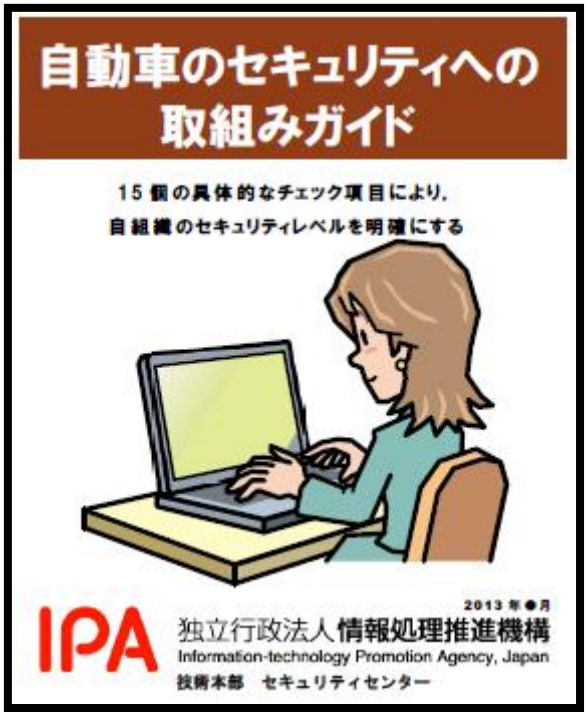
IPA: CC評価を理解するための開発者向け説明会資料
http://www.ipa.go.jp/security/jisec/seminar/documents/cc_eval_20120625.pdf

3. 具体的なセキュリティ検討方法

既存の情報システムでの脅威分析

- 脆弱性
  - 情報システムを構成するソフトウェア、運用手順、組織には部分的に欠陥を含むことがあり、「脆弱性」と呼ぶ
    - 脆弱性は開発プロセス内のいつでも混入するが、上流で対応したほうが開発コストが下がる
- 脅威分析
  - 脆弱性には類型と事例があり、設計時にある程度想定可能
  - 脅威分析では既知の脅威、脆弱性の類型などから脅威を想定するが、範囲が広いため適切な注力配分が必要
    - 注力配分は、ツリー分析による根源的な原因特定か、深刻度分類による優先度づけ方法がある
- 簡易な定量化の手法として、CVSSはIT業界で広く利用されている

自動車のセキュリティへの取り組みガイド



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**

裏づけ

自動車セキュリティ報告書
（2009年～）

「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

ガイドのねらい

想定読者

自動車業界（OEM、サプライヤ、その他サービス事業者 等）

企画・開発者、経営者、他（運用・サポート担当者、等）

ねらい

セキュリティ意識の啓蒙

セキュアな製品の実装・維持

レベルアセスメント
具体的な取組み項目

ポイント

1. **自動車セキュリティの考え方を整理**
   （セキュリティ検討に向けた車載システムの分析）
   概念の整理 モデル化
2. **自組織のレベルアセスメントの手段を提供**
   （セキュリティへの取組みレベルの一覧表）
   4レベルで「今」を評価
3. **具体的な脅威と対策の提示**
   （脅威と対策のマッピング表）
   何が起きる？ 対策は？
4. **具体的な取組み項目**
   （ライフサイクルの各フェーズでの取組み事項）
   いつ、何に取り組むか？

一つ上のレベルへ

今後　新規事例・対策技術加筆により充実を図っていく想定

自動車の構成（IPAカー）

セキュリティ検討用自動車モデル

セキュリティ検討での重要度に基づく機能カテゴライズ
車載LANは最大限に抽象化

「走る」「止まる」「曲がる」

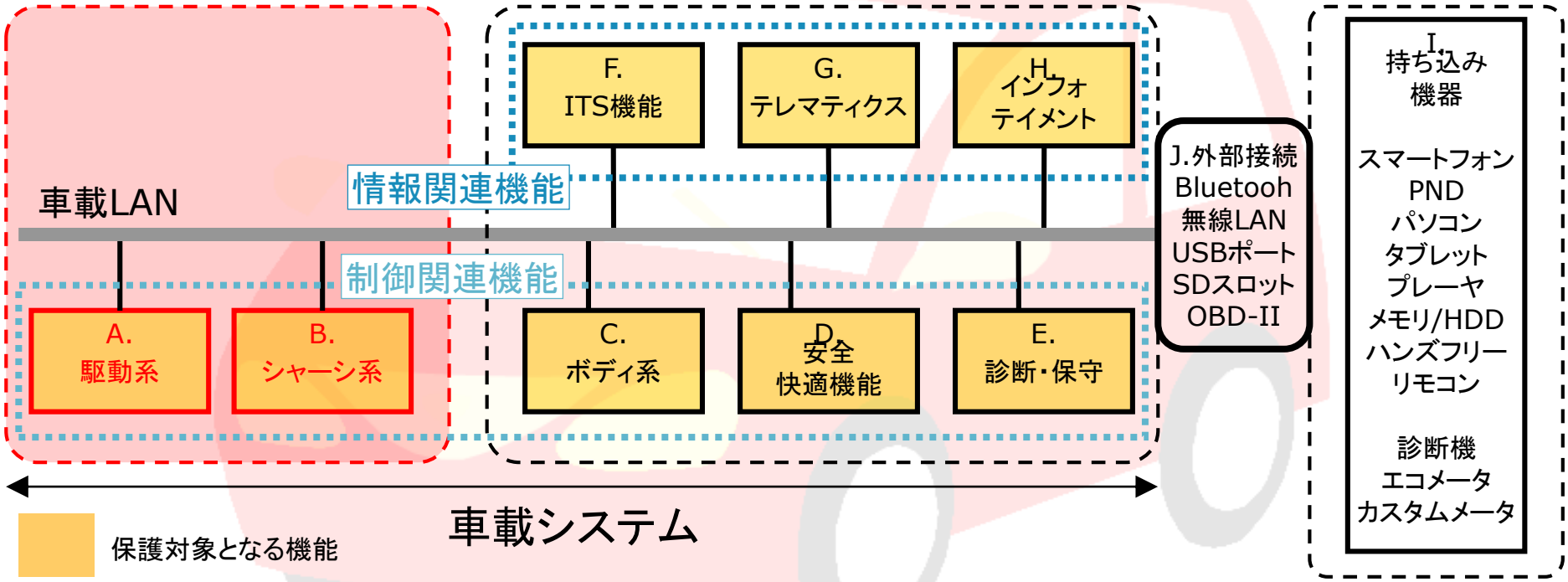
1. 基本制御機能

運転者の快適性・利便性向上

2. 拡張機能

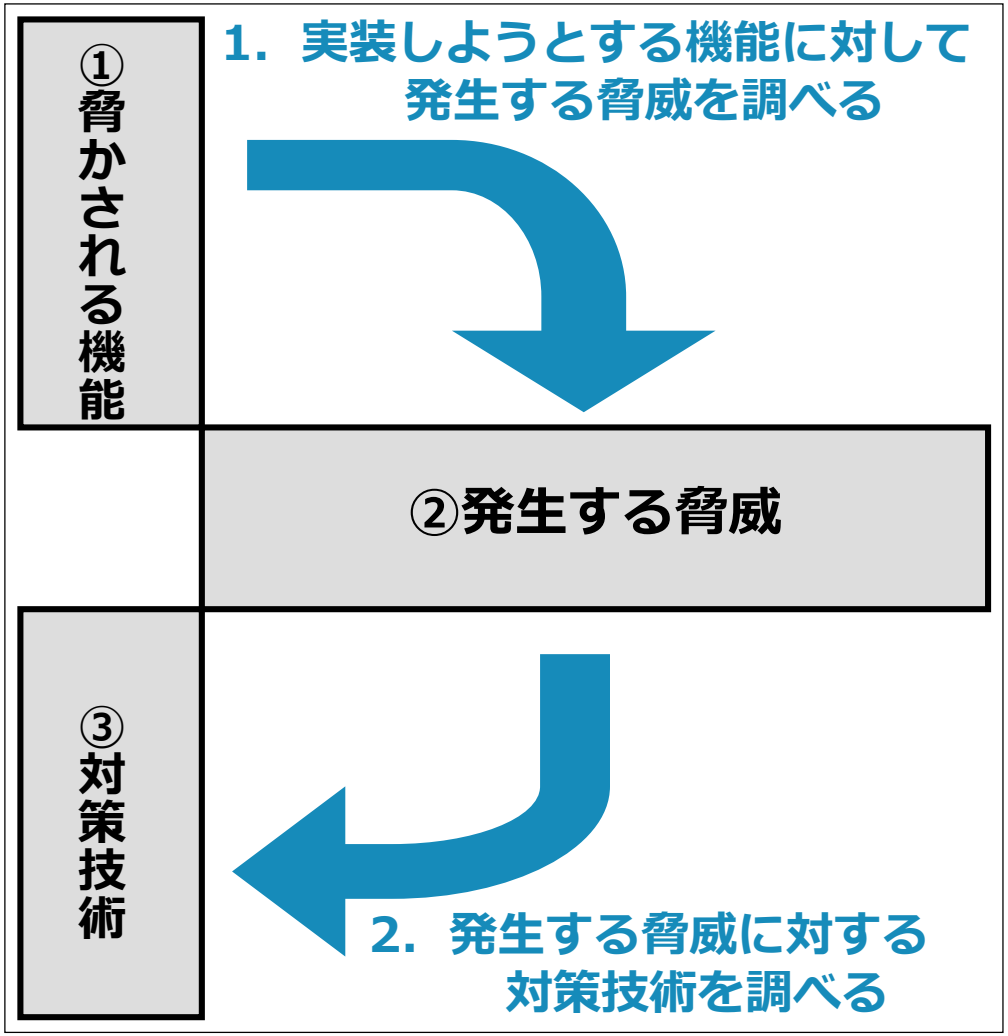
持込み機器での実現機能

3.一般的機能



赤字は特に重要な機能

脅威と対策のマッピング表



上半分　機能×脅威の対応表

●直接的な脅威
▲間接的な脅威

下半分　脅威×対策技術の対応表

○抜本的な対策として有効な技術
△抜本的ではないが効果のある技術

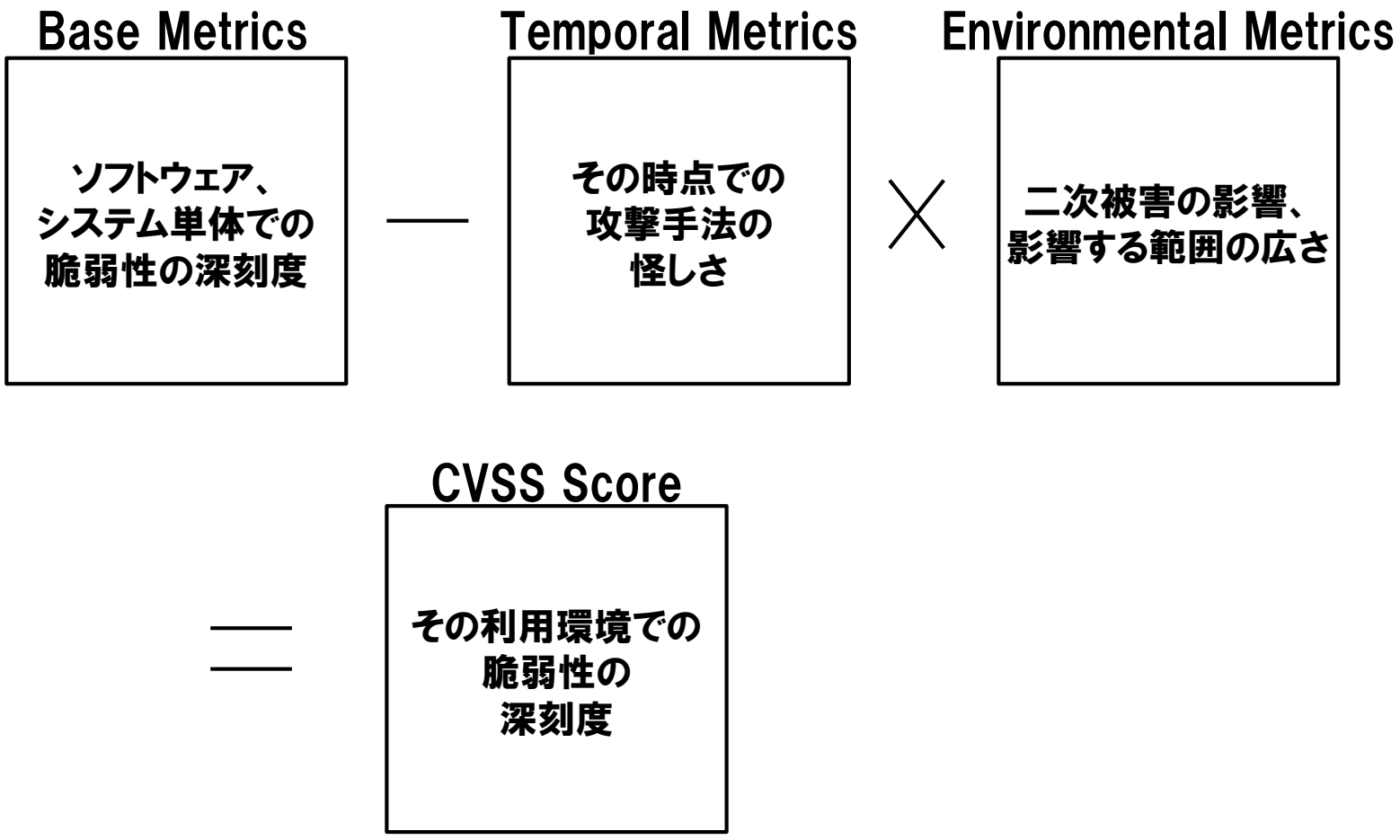
CVSSにおける脅威分析手法

・CVSSとは
・IoTシステムセキュリティ技術の評価
・CVSSによる脆弱性の深刻度評価の手順
・事例：自動車向けセキュリティ技術の評価例

CVSSとは

- ソフトウェアの脆弱性の深刻度を数値化する手法
  - 米国NISTが支援するFirst.orgが標準化している
  - 世界30以上の脆弱性情報提供機関で指標として利用中
  - SCAPというセキュリティ対策ツールの一部で
    脆弱性診断ツール、管理ツールも対応製品が複数あり
- 主な対象
  - 脆弱性の対応者が、対応する優先度を短時間に決めること
- 特長
  - 最終的に10点満点の数値1つで評価
  - 最終評価は「注意・警告・危険」の3段階レベルでシンプル
  - 簡潔なベクタ表現(Vector String)あり

CVSSのしくみ



CVSS評価結果による判断の目安

- 手短に見積もるため、基本値だけ評価してレベル分けする例から

- 基本値4.0以上は要対応＊
  - 脆弱性自体を解消するか
  - 被害が発生しにくくする対応や、被害が小さくなるようにするなど、リスクを低減させる

- 基本値3.9未満は一部の条件で対応が必要
  - 基本値3.9未満は再現しないか、まれに被害が起こる脆弱性など
  - ただし、大規模に普及したシステムや、被害が人命に関わるものは対応を要するため環境値まで評価して検討する

＜基本評価基準＞の目安

深刻度	基本値
レベルIII（危険）	7.0～10.0
レベルII（警告）	4.0～6.9
レベルI（注意）	0.0～3.9

＊参考: PCI DSS 2.0, Requirement: 6.2, 11.2.2.b, 11.2.3.b
https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

IoTシステムでのCVSS利用上の課題

- 人命への影響、セーフティについて明確な評価指標がない
  - 元来IT用で、セーフティ用途に使われていなかった
- 評価担当者や組織によって評価が異なることがある
  - 被害の発生後に対応の優先順位をつけるために使われていたため、現場での使いやすさのため相対評価項目が含まれる
- 今回は上記2つの課題の解決を検討、実施、評価する

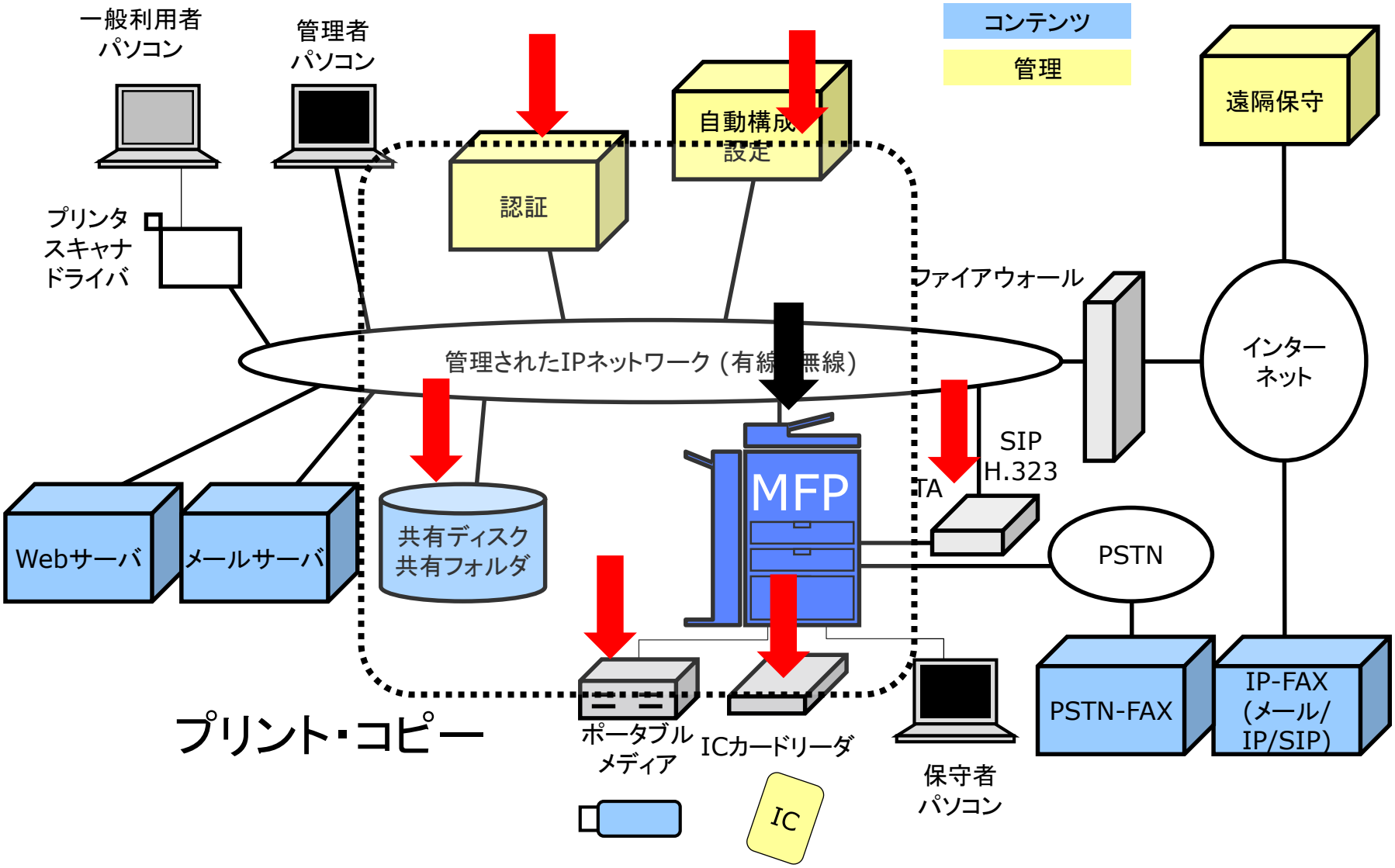
具体的な検討事例

サービス停止による被害の想定例

- MFP(コピープリンタ複合機)のサービス停止
  - 複数台のMFP停止により、1部署の50名が5営業日、書面対応が集中する時期にプリント・コピーをできなくなり、年間の売り上げの1%の損失を受ける

- カーナビのサービス停止
  - 携帯圏外の砂漠地帯でナビが停止し数日帰れなくなる

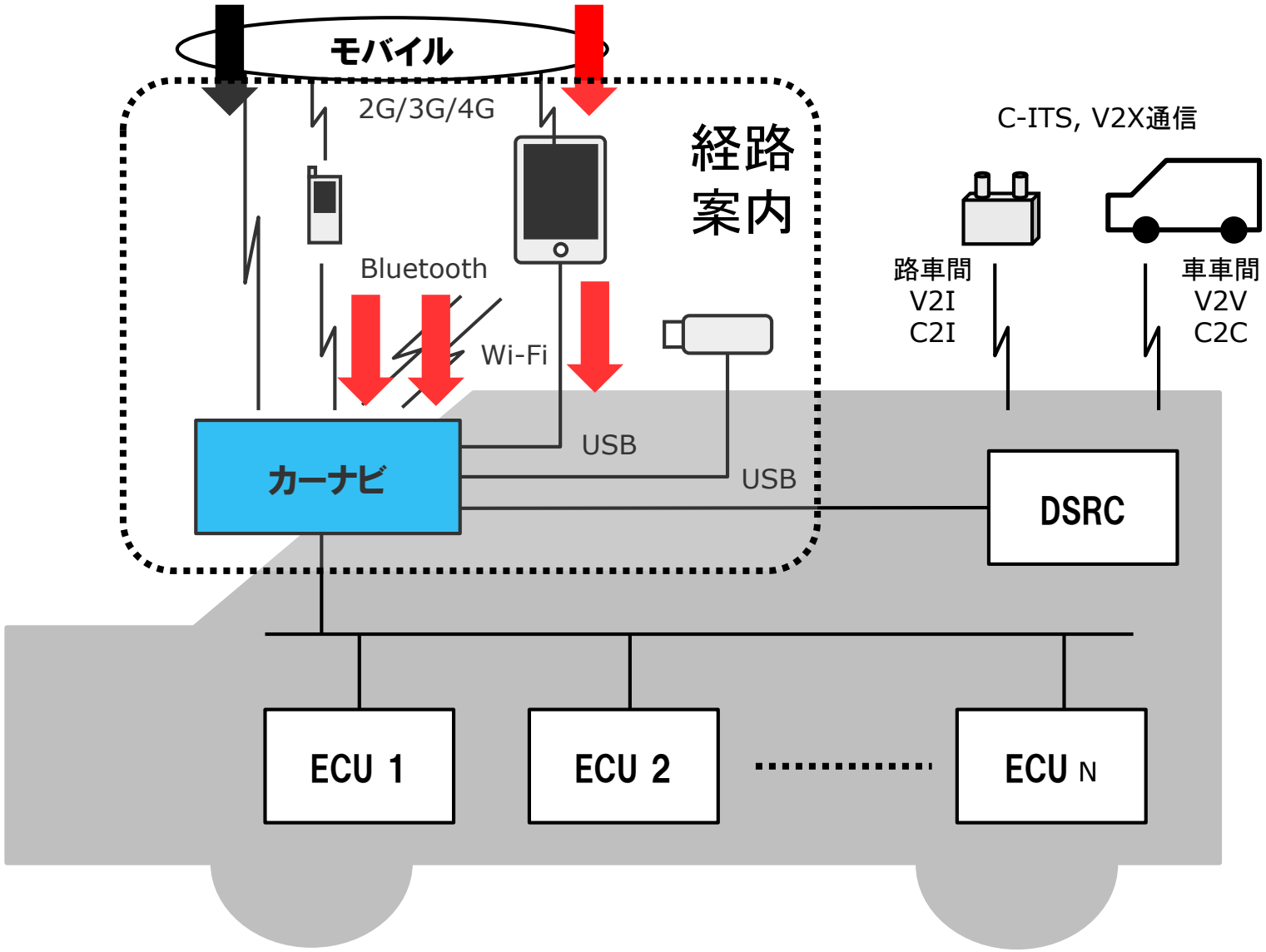
MFP・サービス停止の脅威例



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)

カーナビ・サービス停止の脅威例



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)

まとめ

- 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（攻撃手法の研究）

- 対策
  - IoTサービスに関わる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）
  - 第三者による（客観的な）セキュリティ評価
  - 自動化されたツールによる広範囲の脆弱性評価テストとテストノウハウの蓄積

ご静聴ありがとうございました。