生活機器セキュリティの状況

2015年2月2日

(一社)重要生活機器連携セキュリティ協議会　専務理事
（株）ユビテック　顧問
京都大学　宇宙総合学研究ユニット　特任教授

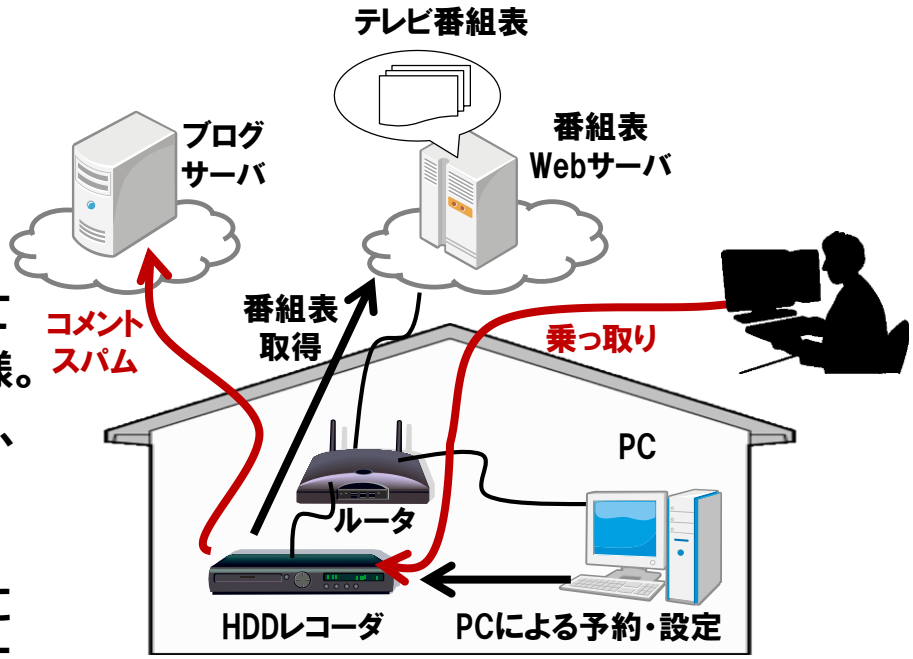
荻野　司

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）

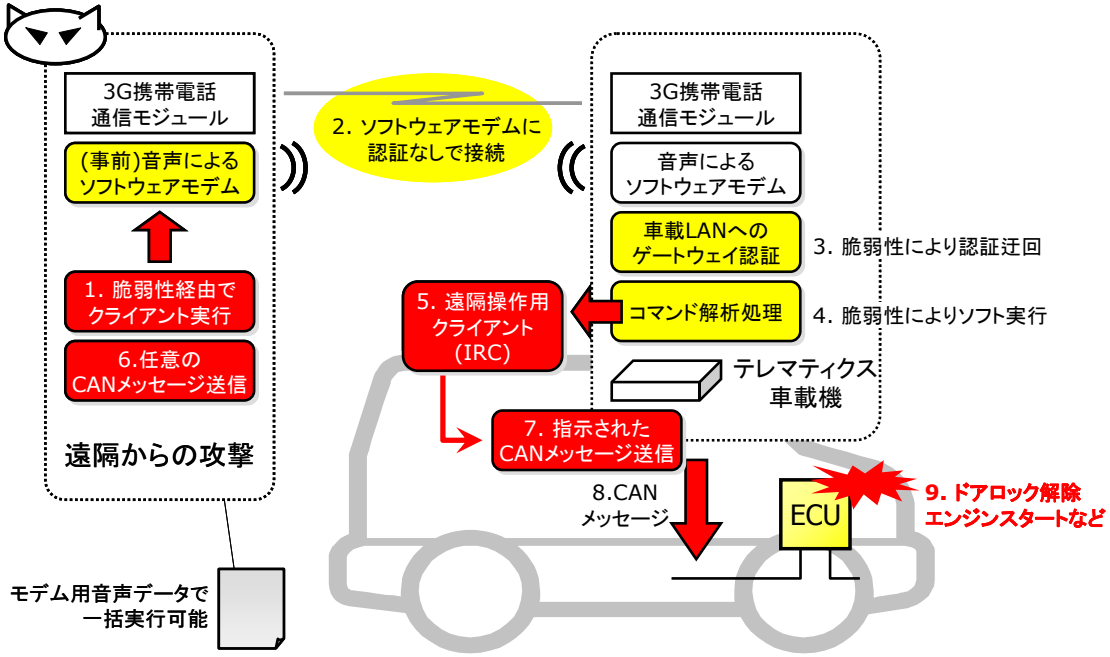
外部から車載LANへの侵入実験（2010）

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

- 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

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

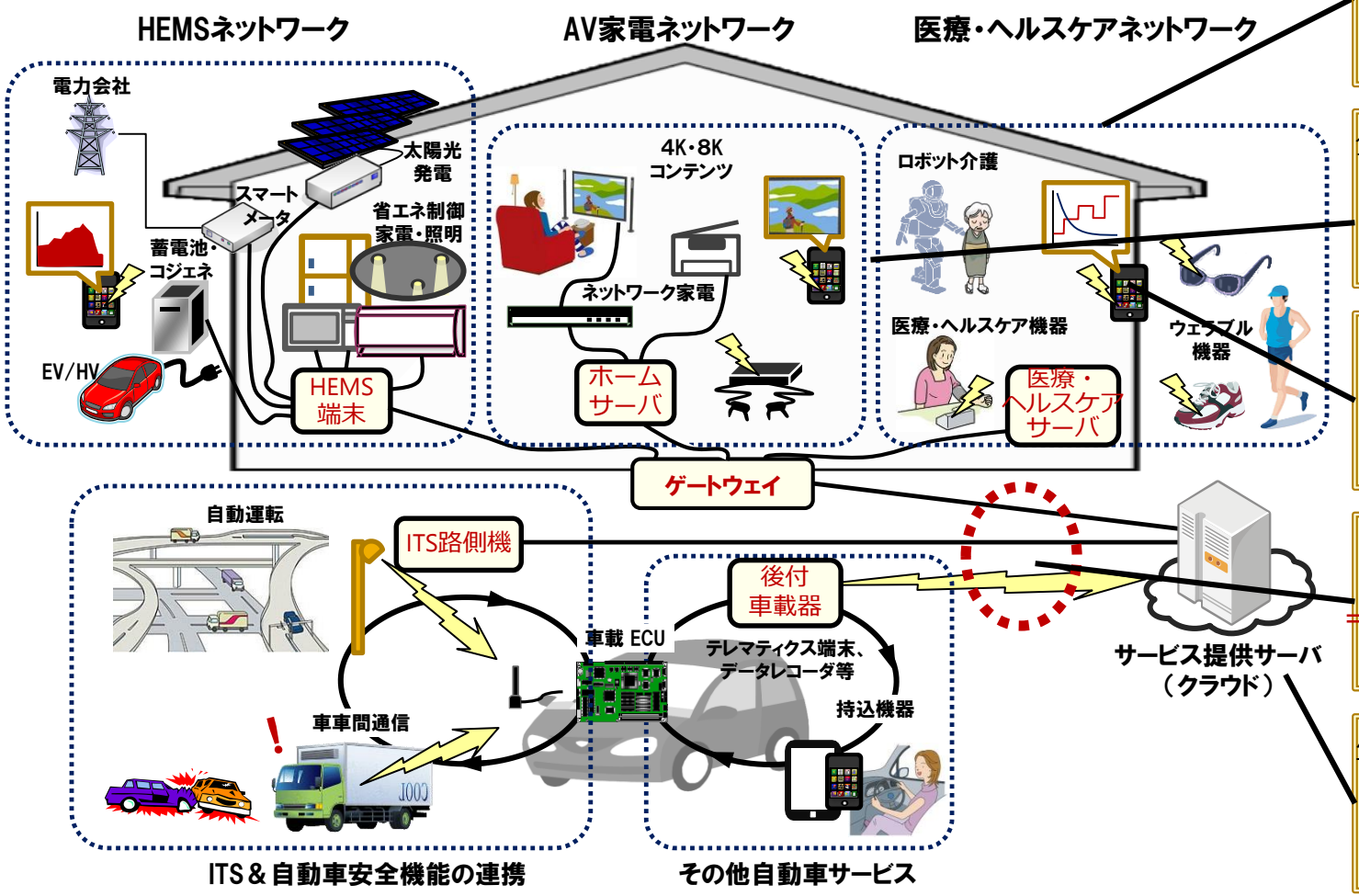
「BAD USB」

- USBのハッキング「BAD USB」（BlackHat2014より）
  - USBのファームウェアに検出不能な状態でマルウェアを送り込める致命的な脆弱性が報告された
    - ファームウェアを改変すれば、例えばUSBメモリにマルウェアをこっそり送り込んだり、USBストレージのデータを改竄したり、USBキーボードを無断で操作が可能
  - 設計上の問題で、修正は不可能。対策には新設計が必要。
- 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

2020年における脅威の想定

- 既に顕在化し始めた組込みシステムへの脅威が「つながる」世界でさらに拡大、深刻化すると想定される。



何がつながっているか分からない
＝脆弱な生活機器が攻撃の入口に

分野ネットワーク間の連携ができていない
＝他分野の生活機器の思わぬ動作が影響

いたる所で生活機器とモバイルデバイスが接続
＝モバイルデバイスが脅威の運び役に

多くの生活機器がサーバと通信
＝プライベートに係る情報の漏えい、改ざんの危険性

生活機器を遠隔から監視、操作するサービスが増加
＝遠隔サーバの乗っ取りによる生活機器への攻撃も

CCDSとは

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

会長：慶應大学　徳田教授

CCDS創設の目的：

消費者が日常生活で利用する機器の中で、予期せぬ動作が発生すると利用者の身体や生命および財産に影響を及ぼす可能性があるもの(以下、「重要生活機器」)をネットワーク接続したり他の機器と連携しても安全・安心に利用できる環境を実現する

各分野・業界の企業・団体からセキュリティに関する取組みの参照先となって、セキュリティ意識の向上を図る

一般社団化の狙い：

特定の企業や分野・業界に偏らず、総務省や経産省などの公的プロジェクトにも中立的に携われるような体制とするため

⇒重要生活機器におけるセキュリティ事業の創生をめざす

重要生活機器連携セキュリティとは？

- 重要生活機器とは？
  - 車載器、在宅ヘルスケア機器、スマート家電、HEMS、ATMなど利用者個人の生命や健康、財産、プライバシのリスクに直結するネット型組込みシステム機器類
- 連携セキュリティとは？
  - スマホや携帯網を通じてクラウドサービスと連携し、繋がる形で高機能化する組込みシステム自体の機能安全や脆弱性による機能悪用という脅威に対するセキュリティ

Safety

故障・不具合や操作ミスからの防御

&

Security

悪意のある攻撃者からの防御

が対策急務!

NISC－情報セキュリティ研究開発戦略(改訂版)の概要

- **サイバーセキュリティ戦略**（2013年6月策定）　において示された、
  - **サイバー攻撃の検知・防御能力の向上**
  - 制御システム、ICチップなど**社会システム等を保護するためのセキュリティ技術の確立**
  - ビッグデータ（パーソナルデータ等）利活用等の**新サービスのための技術開発**　等を推進する観点から、**「情報セキュリティ研究開発戦略」を改定**
- 産業活性化につながる新サービス等におけるセキュリティ研究開発の中で、情報セキュリティ技術が求められる分野として、新たに一般利用者向けの生活機器が加えられた。

…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。

- ポイント
  - **生活機器分野での対応の重要性**
  - **Security By Designから日本製品の品質を高信頼化に**

    ステップアップさせる方針

CCDSの役割

世界に向けて強い組込み製品を目指そう！

「組込みセキュリティにおける。。。

１）情報収集、啓蒙活動　（日本の底上げ）
２）技術開発と人材育成　（追いつき、先行する）
３）ガイドライン・標準化（国際協調）
４）検証技術基盤の構築　（強い製品に向けてのツール）
５）検証新事業の創生　（差別化された技術を事業へ）

重要生活機器に対して取り組むべき事業ポイント

- 新規事業創造と強い産業の育成に向けて
  - 重要生活機器連携セキュリティ研究会でまとめた提言「セキュアライフ2020」に掲げる、「世界の安心・安全に貢献しよう」、「世界に誇れるセキュアなものづくりを進めよう」の基に、製品サービス提供側の環境整備として以下の４点の事業を相互に連携させ、同時並行的に推進する

1. 生活機器セキュリティ認証

- 生活機器のセキュア開発・検証ガイドライン策定と国際標準化の検討
- セキュア開発・検証ガイドライン準拠認定スキームの検討
- 消費者の安全・安心を担保する一定のセキュリティ要件のあり方の検討（製品分野別）

2. セキュリティ技術開発

- 生活機器との連携におけるセキュリティ攻撃・防御・検知技術開発
- 攻撃技術・対策技術効果を実証するテストベッドの構築、など

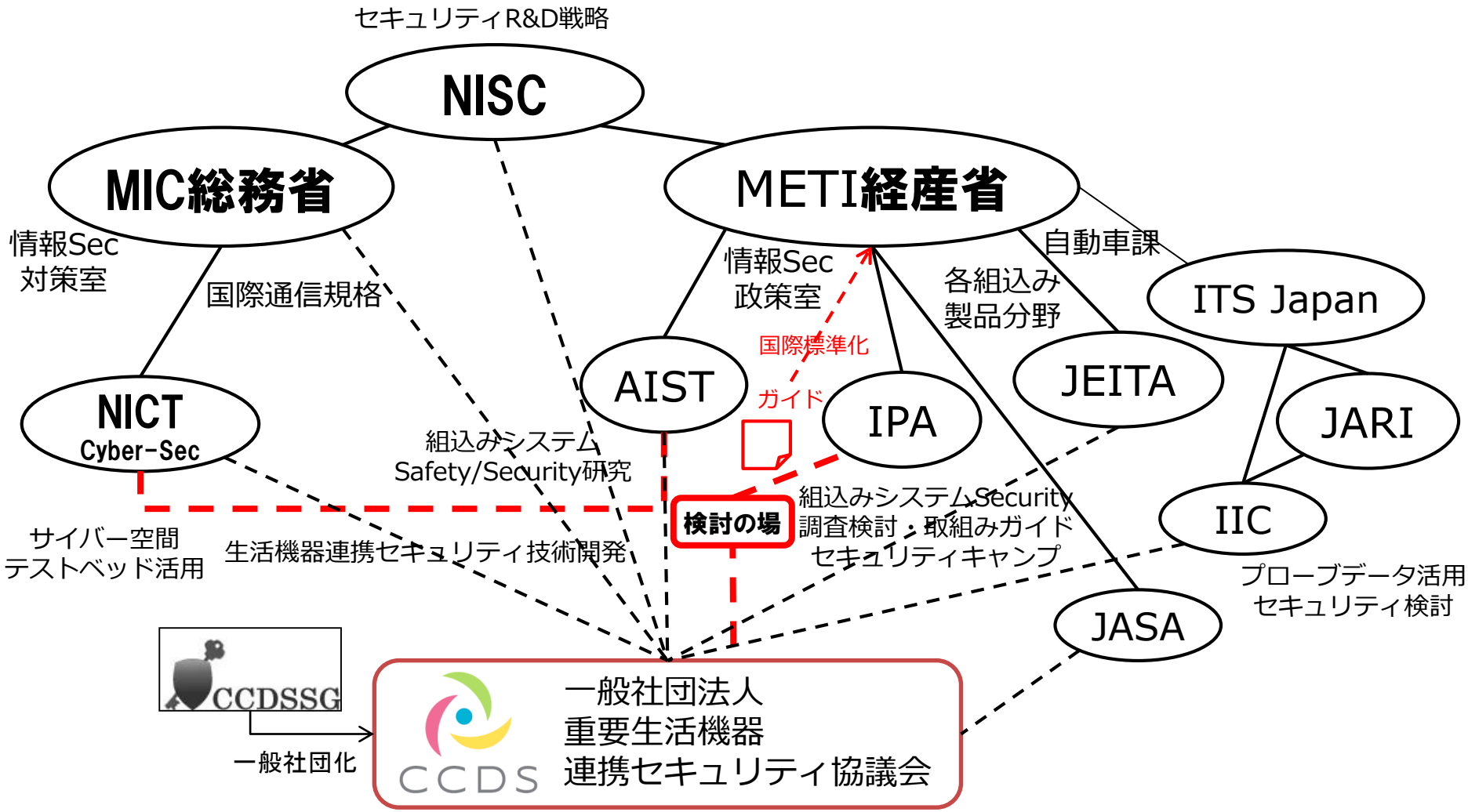
3. セキュリティ人材育成

- 上記を通じたセキュリティ人材育成

4. 検証事業促進

- 開発標準やセキュリティ標準に沿った評価ツール・検証環境の開発支援

組織間連携プロジェクト化のイメージ

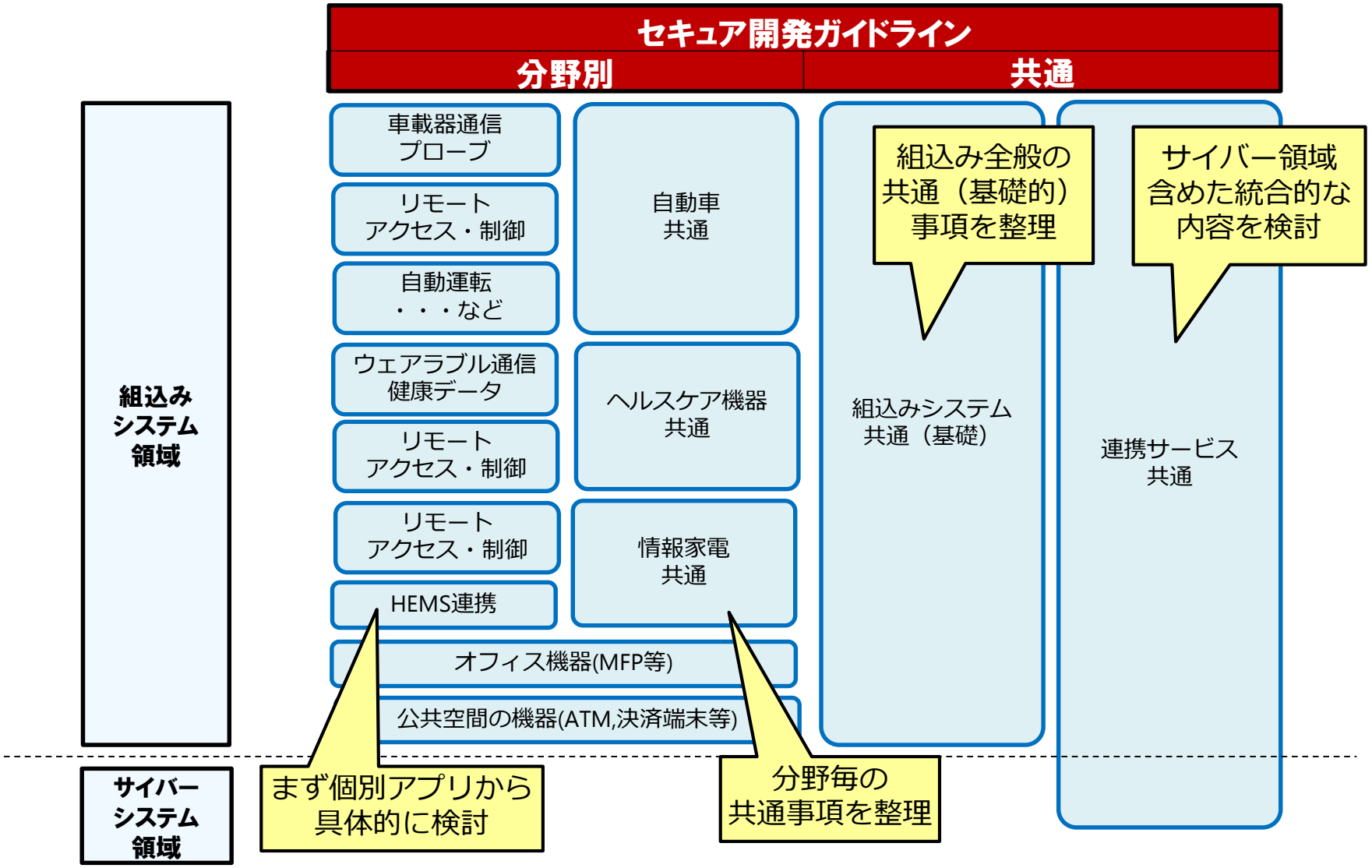


IT利活用セキュリティ総合戦略推進部会（山本前大臣主催）
「IT利活用セキュリティにおける総合的かつ戦略的な政策推進に係る提言
http://www.nisc.go.jp/active/kihon/pdf/ituse20140728.pdf

■IOT関連セキュリティ政策の重要性
■サイバーセキュリティ特区の創設

セキュア開発ガイドライン策定イメージ

- 検討するガイドラインのタイプ

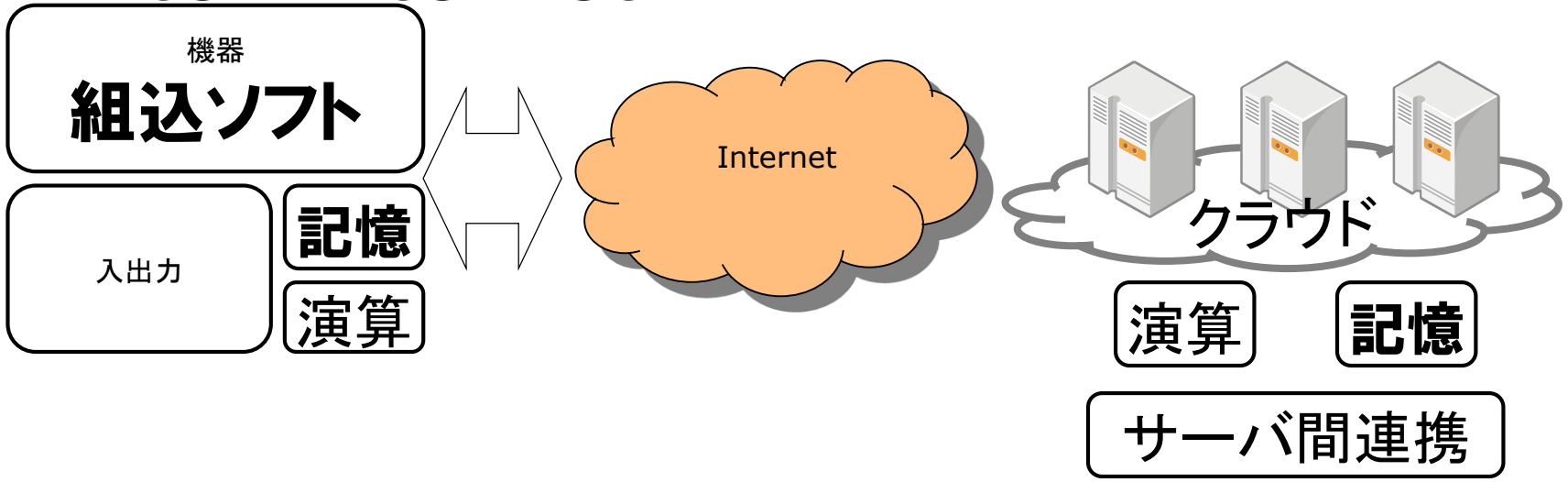


組込みシステムの今後

- Before Internet

1. 組込みソフトでの機能がクラウドへ
2. データ連携

- After Internet

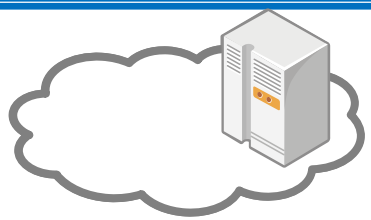


自動車セキュリティの考え方

CCDS

スマホ・ネット協調

基地局
路車間
車車間



クラウド連携

対象：持ち込まれたスマホ、タブレット
対象：エンタメ、グリッド連携、ソーシャル
対策：スマホ機器を車載機から認証
対策：スマホ・ネットの通信とコンテンツ保護

OBD2とボディ系車載バス

対象：ドアロック、ライト、ハンドブレーキ、
エアコン、クラクション、AV等の制御・監視
対策：OBD2の物理的保護(鍵つきコネクタ
対策：CANバスの監視と抑制/妨害、通報

対象：走る・曲がる・止まる
エンジン、トランスミッション、
ブレーキ、ステアリングの制御

対策：車載バス、制御システム保護

自動運転

高度安全システム

ハンブルグ空港