DEOS協会 オープンシンポジウム

IoT時代の セーフティ＆セキュリティ

2016年6月8日

高田 広章

名古屋大学 未来社会創造機構 教授
名古屋大学 大学院情報科学研究科 教授
附属組込みシステム研究センター長
APTJ株式会社 代表取締役会長・CTO
Email: hiro@ertl.jp　URL: http://www.ertl.jp/~hiro/

自己紹介

本務

- 名古屋大学 未来社会創造機構 教授
- 名古屋大学 大学院情報科学研究科 情報システム学専攻 教授／附属組込みシステム研究センター長

その他の役職（主なもの）

- TOPPERSプロジェクト 会長
- APTJ株式会社 代表取締役会長・CTO
- 車載組込みシステムフォーラム（ASIF）会長
- 情報処理学会 組込みシステム研究会 元（初代）主査

研究分野

- （組込みシステム向け）リアルタイムOS
- リアルタイム性解析とスケジューリング理論
- 機能安全技術，消費エネルギー最適化技術
- 車載組込みシステムと車載ネットワーク，ダイナミックマップ

TOPPERSプロジェクトとは?

- ITRON仕様の技術開発成果を出発点として，組込みシステム構築の基盤となる各種の高品質なオープンソースソフトウェアを開発するとともに，その利用技術を提供

組込みシステム分野において，*Linux*のように広く使われるオープンソースOSの構築を目指す!

プロジェクトの狙い

- 決定版のITRON仕様OSの開発 ← ほぼ完了
- 次世代のリアルタイムOS技術の開発
- 組込みシステム開発技術と開発支援ツールの開発
- 組込みシステム技術者の育成への貢献

プロジェクトの推進主体

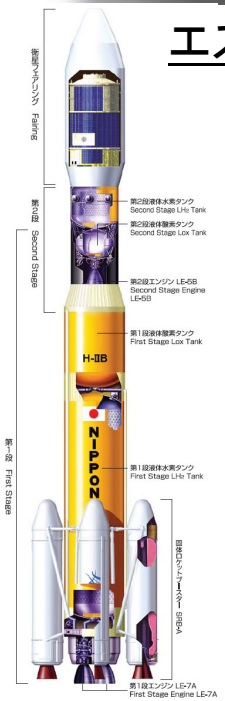
- 産学官の団体と個人が参加する産学官民連携プロジェクト
- 2003年9月にNPO法人として組織化

開発成果物の主な利用事例

エスクード（スズキ）

スカイラインハイブリッド（日産）

IPSiO GX e3300（リコー）



H-IIB（JAXA）

提供：JAXA，イラスト：池下章裕

ひとみ（ASTRO-H）（JAXA）

OSP-P300（オークマ）

SoftBank 945SH（シャープ）

UA-101（Roland）

PM-A970(エプソン)

名古屋大学 組込みシステム研究センター (NCES)

設立目的

☞ http://www.nces.is.nagoya-u.ac.jp/

- 組込みシステム分野の技術と人材に対する産業界からの要求にこたえるために，*組込みシステム技術に関する研究・教育の拠点*を，名古屋大学に形成

活動領域（スコープ）

- 大学の技術シーズを実現/実用化することを指向した研究
- プロトタイプとなるソフトウェアの開発
- 組込みシステム技術者の教育/人材育成

研究プロジェクトの例

- 車載制御システム向けSPF（AUTOSAR仕様ベース）
- 車載データ統合アーキテクチャとLDMへの適用
- 宇宙機向けソフトウェアプラットフォーム（スペースワイヤOS）
- 車載組込みシステムのセキュリティ強化技術

APコンソーシアム

※ AP = Automotive Platform

正式名称

- 車載制御システム向け高品質プラットフォームに関するコンソーシアム型共同研究

コンソーシアム型共同研究とは？

- 名古屋大学 大学院情報科学研究科 附属組込みシステム研究センター（NCES）が設定した研究開発テーマに，複数の企業の参加を得て研究・開発を進める共同研究

実施内容

- AUTOSAR仕様をベースとして，高品質な車載制御システム向けソフトウェアプラットフォーム（SPF，広い意味でのOS）に関する研究開発を行う
- 過去の成果をベースに，品質向上・開発範囲拡大を行う

実施期間

- 2014年度に開始．3年程度の継続実施を予定

APコンソーシアムの参加企業（28社，2015年度）

- アイシンコムクルーズ（株）
- イーソル（株）
- （株）ヴィッツ
- （株）永和システムマネジメント†
- SCSK（株）
- APTJ（株）
- （株）OTSL†
- オムロン オートモーティブエレクトロニクス（株）†
- 京セラ（株）†
- （株）サニー技研
- （株）ジェイテクト
- スズキ（株）
- （株）デンソー *
- 東海ソフト（株）†
- （株）東海理化電機製作所 *
- （株）東芝
- （株）豊田自動織機
- （株）豊通エレクトロニクス†
- 日本電気通信システム（株）
- パナソニック（株）†
- パナソニック アドバンストテクノロジー（株）
- 富士通テン（株）
- 富士ソフト（株）
- マツダ（株）
- ルネサス エレクトロニクス（株）
- 矢崎総業（株）
- ヤマハ発動機（株）†
- 菱電商事（株）†

*は部分参加

†はオブザーバ参加

APTJ株式会社

APTJの活動と位置付け

- APコンソーシアムなどの研究開発成果を活用して，車載制御システム向けのSPFを開発・販売
  - 自動車メーカ／自動車部品メーカと共同でSPFを開発
  - 最新のAUTOSAR仕様をベースとする
  - 技術的な強みは，機能安全規格，サイバーセキュリティ対策，マルチコアプロセッサに効率的に対応できること
- パートナーソフトウェア企業と協力
- 名古屋大学発ベンチャー企業として設立

取締役

- 代表取締役会長・CTO（非常勤）：高田広章
- 代表取締役社長：高嶋博之
- 取締役（非常勤／社外）：浅野真弘，三木誠一郎

目次

組込みシステムの
セーフティ＆セキュリティ

安全性と機能安全

システム安全性（safety）

- システムが規定された条件のもとで，人の生命，健康，財産またはその環境を危険にさらす状態に移行しない期待度合い（JIS X 0134）
- 信頼性（機能単位が，要求された機能を与えられた条件のもとで，与えられた期間実行する能力（JIS X 0014））とは明確に異なる概念

機能安全（functional safety）

- 機能的な工夫（安全を確保する機能）により極力安全を確保する（NECA 技術委員会報告 第3の波「機能安全」の概要）

  例）踏切の警報機や遮断機
- 安全を確保するための機能を，安全機能と呼ぶ
- 本質安全と対比される考え方

情報セキュリティ

情報セキュリティ（information security）

- 情報の機密性，完全性および可用性の維持（JIS X 5080）
- さらに，真正性，責任追跡性，否認防止，信頼性などの特性の維持を含める場合も（ISO/IEC 27001）

機密性（confidentiality）

- アクセスを認可された者だけが情報にアクセスできることを確実にすること

完全性（integrity）

- 情報及び処理方法が，正確であること及び完全であることを保護すること

可用性（availability）

- 認可された利用者が，必要なときに，情報及び関連する資産にアクセスできることを確実にすること

安全性と情報セキュリティの関係

守るべき資産の違い

- 情報セキュリティは，（文字通り）情報を守ること
  - 情報セキュリティの3要素（CIA）は，いずれも情報に着目した性質
- 安全性が対象にしている「人の生命，健康，財産またはその環境」の内，財産（の一部）以外は情報に該当しない

対象とする事象の違い

- 「セキュリティ」という用語は，主に，故意による攻撃からの防衛を意味している場合が多い
  - national security ＝ 安全保障
  - home security ＝ 防犯
- 従来の安全技術は，主に，自然に発生する故障や，（故意でない）人為的なミスに対応することを主眼としてきた

組込みシステムのセキュリティ上のリスク

サイバー攻撃によるシステムの誤動作 ← まずはこれが重大

- システムの脆弱性を利用して，システムを誤動作・機能喪失させる
  - ソフトウェアを不正に書き換えて誤動作させることも
- 制御系組込みシステムでは，システムの*安全性*が損なわれる事態につながる可能性
- 安全機能を実現するシステムやセキュリティ機器（例：電子キー）の場合には，その機能喪失は大きいリスクに

個人情報・価値のある情報の流出・改ざん

- 組込みシステムの中には，個人情報や機密情報（例：工場の稼働状況）を保持しているものも多い

踏み台として利用

- 組込みシステムをサイバー攻撃の踏み台に利用される

組込みシステムが守るべき資産

- 組込みシステムにおいては，本質的（最終的）に守りたいのは情報とは限らない
  - 人命，健康，金銭，物品，エネルギー，…
  - もちろん守りたい情報もある（個人情報等）
- 自動車の盗難防止は，情報セキュリティの範囲外？
  - 自動車は「情報」ではないため，直接的には範囲外
  - 盗難防止が，情報技術で実現されていれば（電子キーやイモビライザ），そこから先は「情報」セキュリティ
  - 類似例）電気自動車からの電気の盗難防止
  - 考える範囲を明確に切り分けられるか？

! まずは，扱っている範囲を明確にすることが重要

- 最近は「サイバーセキュリティ」という用語を使うようにしているが，まだ狭いかもしれない

機能安全技術とセキュリティ技術の類似性

セキュリティ技術は「機能セキュリティ」

- 「セキュリティ機能」によってセキュリティを確保する
- 「本質セキュリティ」もないわけではないが…

  例）外部のネットワークと接続しない

「安全機能」「セキュリティ機能」の決定が重要

- 機能安全においては，安全性を確保するために必要な安全機能が定義できれば，後は信頼性を確保すればよい
  - 安全性を確保するために取るべき手段（安全機能を含む）を抽出するための分析作業が，安全（要求）分析
- セキュリティにおいても同様
  - セキュリティ要求分析の技術が重要に
- 信頼性確保の部分は，安全性とセキュリティで大きい違いはなく，共通化が可能

安全性とセキュリティの両立の困難性

Clash of Cultures（Rainer Faller氏（exida社）の資料より）

- Safety
  - Precise targets because of well understood threats
- Security
  - Moving targets because of new threats from malicious people result in less practical guidance
  - Application engineers ask, however, for more practical guidelines

本質的な困難はリスク評価

- 機能安全規格は，厳密なリスク評価を要求する
- セキュリティに対するリスクを厳密に評価するのは難しい

Guarantee文化とBest Effort文化の衝突？

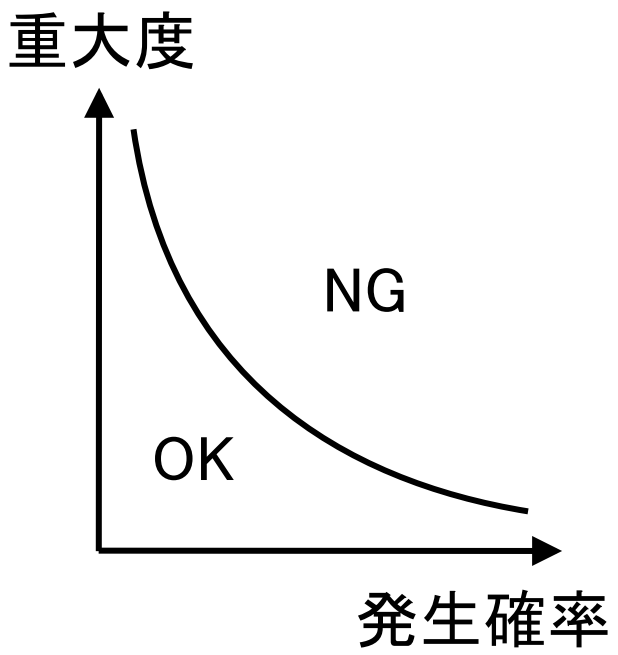
リスク（危険性）とは？

- ある事象生起の確からしさと，それによる負の結果の組合せ（JIS Z8115: 2000）

  重大度×発生確率

セキュリティに対するリスク

重大度×脆弱性×脅威



- 脆弱性（vulnerability）
  - セキュリティ上の問題を起こす可能性のあるシステムの弱点（欠陥や仕様上の問題）
  - セキュリティホール（セキュリティ上の問題を起こす可能性のあるシステムの欠陥）は脆弱性の一部
- 脅威（threat）
  - 脆弱性を利用してリスクを現実化させる手段

安全性とセキュリティの両立に向けて

セキュリティリスク分析手法の確立と支援技術

- セキュリティ分析の技術を確立する．中長期的には，形式手法や人工知能による分析支援が求められる

組込みシステムに向いたセキュリティ対策技術の開発

- 組込みシステムでは，限られたリソース下でのセキュリティ対策技術が求められる

システムのアーキテクチャからの考慮

- セキュリティ確保に重要な部分と，安全性確保に重要な部分を分離したアーキテクチャとする

セキュリティ対策に対する相場観の醸成と国際標準化

- セキュリティ対策に対する相場観を作ることが必要

変化する脅威に対応する仕組みの導入

- 変化する脅威に対応してシステムを更新する仕組み（制度面も含めて）を導入する（その必要性の認識を広める）

IoTのセキュリティに関する ガイドライン

IoTに関するセキュリティガイドラインの作成

IoT推進フォーラム／総務省／経済産業省

- 6月1日付けで「IoTセキュリティガイドライン（案）」を公表
- 6月14日まで意見募集中
  - 「IoTセキュリティガイドライン」で検索してください

情報処理推進機構（IPA）

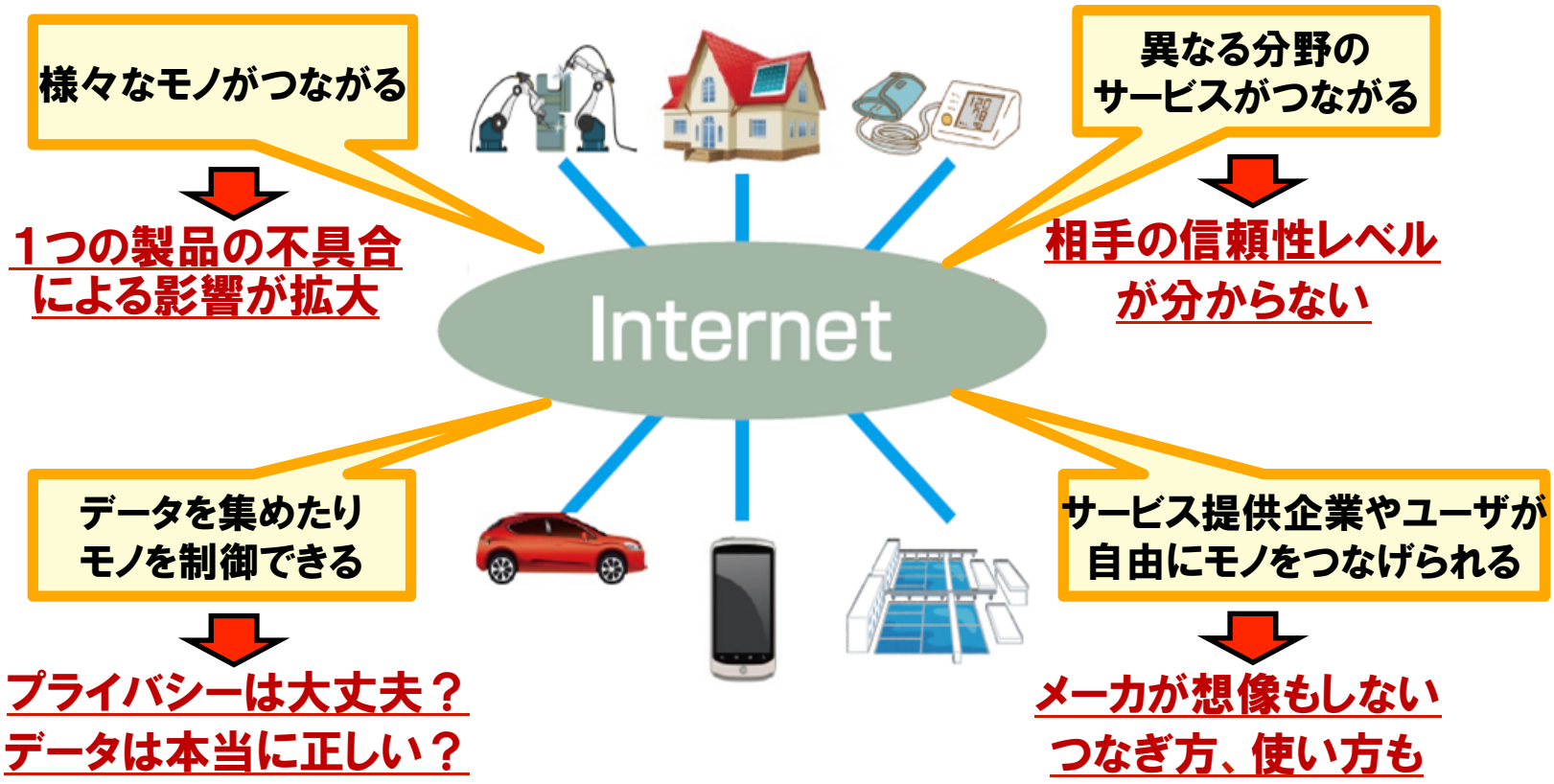
- 3月14日に「つながる世界の開発指針」を公開
  - 「IoTセキュリティガイドライン（案）」のベースの1つに
- IoT機器/システムの開発者が安全/安心の確保のために最低限検討して欲しい事項を，開発ライフサイクルに沿って17の指針として整理

http://www.ipa.go.jp/files/000051411.pdf

IPA「つながる世界の開発指針」

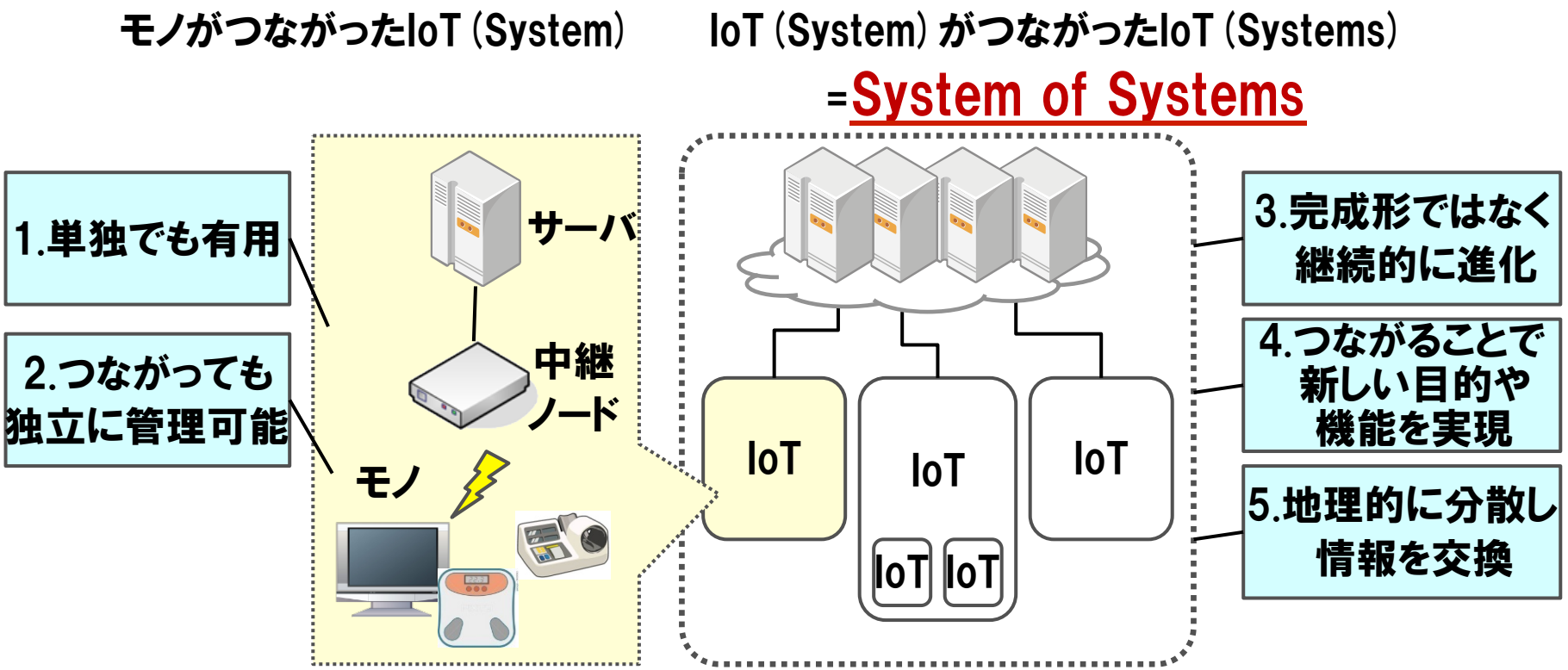
つながる世界の課題

- 想定外のつながりにより，利用者や製品の安全性・セキュリティを脅かすリスクの発生



System of Systems（SoS）としてのIoT

- モノがつながって，IoTを構成
- IoTとIoTがつながって，IoTを構成



⇒ 指針では，IoTの構成要素（コンポーネント）開発に着目

System of Systems（SoS）の主要特性

（1）構成要素の運用の独立性：個々のコンポーネントは独立かつそれ自体が役に立つように運用できる。

（2）構成要素のマネジメントの独立性：コンポーネントは，個別に調達され，インテグレートされるとともに，SoSの中で独立に運用が可能である。

（3）進化的開発：完成形ではなく，機能や目的が追加・削除・変更されながら進化する。

（4）創発的振る舞い：コンポーネント単独では実現できない目的や機能を果たす。

（5）地理的な分散：コンポーネントは広域に分散し，モノやエネルギーではなく，情報を交換する。

出典：Mark W. Maier: “Architecting Principles for Systems-of-Systems”（訳：IPA）

指針一覧

大項目		指針
方針	つながる世界の安全安心に企業として取り組む	指針1　安全安心の基本方針を策定する
		指針2　安全安心のための体制・人材を見直す
		指針3　内部不正やミスに備える
分析	つながる世界のリスクを認識する	指針4　守るべきものを特定する
		指針5　つながることによるリスクを想定する
		指針6　つながりで波及するリスクを想定する
		指針7　物理的なリスクを認識する
設計	守るべきものを守る設計を考える	指針8　個々でも全体でも守れる設計をする
		指針9　つながる相手に迷惑をかけない設計をする
		指針10 安全安心を実現する設計の整合性をとる
		指針11　不特定の相手とつなげられても安全安心を確保できる設計をする
		指針12 安全安心を実現する設計の検証・評価を行う
保守	市場に出た後も守る設計を考える	指針13 自身がどのような状態かを把握し、記録する機能を設ける
		指針14 時間が経っても安全安心を維持する機能を設ける
運用	関係者と一緒に守る	指針15 出荷後もIoTリスクを把握し、情報発信する
		指針16 出荷後の関係事業者に守ってもらいたいことを伝える
		指針17 つながることによるリスクを一般利用者に知ってもらう

IoT時代の
セーフティ＆セキュリティの課題

IoT時代の課題（オープンシステムの課題）

従来の議論では…

- 組込みシステムのつながる先も含めて，1つのシステムとして設計していることを，暗黙に想定していた

IoT時代の組込みシステムは…

- 他の会社（契約関係にないもの）・他の業界で開発されたシステムとの接続が一般的に
  - それを許容しないと，魅力的なサービスの提供が困難
  - 例えば，HEMSには，家の中の電気を使う機器（多様な会社・業界が開発）はすべてつながる方向
- 設計時点で想定していないシステムとつながる可能性
  - 信頼性の低いHEMSに，ライフクリティカルな医療機器を接続するかもしれない…
- つながる相手が，どれだけ信用できるかが問題に

C2C-CCによる信用保証レベルの定義

概要

- Car 2 Car Communication Consortium（C2C-CC）が，車々間および路車間通信におけるセキュリティの扱いについて検討している
- その中で，信用保証レベル（Trust Assurance Level; TAL）を定義し，レベル毎のセキュリティ要件を定義しようとしている
- この定義のコンセプトが納得できるもので，今後注目すべき技術と考え，紹介する

参考文献

- S. Goetz and H. Seudié: “Operational Security”, Car2Car Forum 2012, 2012年11月.

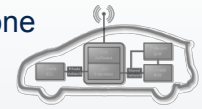
信用保証レベルの必要性

- 車々間/路車間通信で，他の自動車やロードサイドユニットから得られた情報を，どれだけ信じて使ってよいか？
  - 例えば，前を走る車からブレーキをかけているという情報が送られてきた時，それを信じて使ってよいか？
- 信じるためには…（2つの認証）
  - 自動車が要求されるセキュリティ基準を満たしていることを，その開発時に認証を得ておく
  - 情報の発信源（前を走る車）が，認証を得た自動車であることを確認する

PKIの利用

- 情報の発信源の認証には，PKI（公開鍵基盤）を用いる
  - 証明書の中に，TALも入れておく
- 証明書の有効期限を短くすることで，TALを動的に変更することも可能に

Trust Assurance Levels (TAL) and certification

Trust Ass. Level (TAL)	Requirements			Implications		
	Minimum Target of Evaluation (TOE)	Minimum Evaluation Assurance Level (EAL)	Minimum (Hardware) Security Functionality	Prevented (Internal) Attacker acc. to CC	Potential Security Implications	C2X Use Case Examples
0	None 	None	None	None	Not reliable against security attacks in general	Some limited,e.g. using trusted C2I infrastructures
1	+ ITS Station software 	EAL 3	Only software security mechanisms	Basic	Not reliable against simple hardware attacks (e.g., offline flash manipulation)	Non-safety, but most privacy relevant use cases
2	+ ITS Station hardware 	EAL 4	+ dedicated hardware security, i.e., secure memory & processing)	Enhanced Basic	Not reliable against more sophisticated hardware attacks (e.g., side-channel attacks)	C2C-CC day one use cases (e.g., passive warnings and helpers)
3	+ private network of ECUs 	EAL 4+ (AVA_VAN.4 vulnerability resistance)	+ basic tamper resistance	Moderate	C2X box secure as stand alone device, but without trustworthy in-vehicle inputs	Safety relevant relying not only on V2X inputs
4	+ relevant in-vehicle sensors and ECUs 	EAL 4+ (AVA_VAN.5 vulnerability resistance)	+ moderate – high tamper resistance	Moderate – High	C2X box is trustworthy also regarding all relevant in-vehicle inputs	All

Minimum Level

※ 参考文献より

補足

- TAL毎にProtection Profile（セキュリティ機能仕様のテンプレート）が作成されている模様だが，現時点では公開されておらず，詳細はわからない

注目すべき点

- 他社で開発されたシステムをどこまで信じてよいかに関して，1つの考え方を提案している（ただし，応用分野は限定）
- Common Criteriaのフレームワークに基づいており，認証のスキームは明確（ただし，既存の認証スキームを使うとは限らない）
- TAL 4になると，車載ネットワークやその先のECUまで評価対象（TOE）に含まれる
  - 車々間/路車間通信に限らず，1台の自動車単独に適用しても有益な可能性

課題：責任の所在

結局，誰が責任を取るか？

- いくらしっかり作られたシステムでも，セーフティ＆セキュリティ上の脆弱性／リスクはゼロにはならない
- 他のシステムから受け取った情報が誤っていた結果，事故が起こった場合の責任は？
  - 情報の出し元に責任を負わせると，誰も情報を出さなくなる（情報を出すメリットと釣り合えば別）

当面のソリューション

- 他のシステムから受け取った情報は，（少なくとも単独では）safety-criticalな目的には使用しない

本質的なソリューションは？

- 個別に契約？ 法律で縛る？ → SoSを飼い慣らす？
- 保険？（法律の援用も必要）

課題：個人情報の扱いと情報銀行

個人情報／パーソナルデータ保護は最大の課題

- 個人情報／パーソナルデータ保護が，IoTやビッグデータ活用に向けての最大の課題であることは言うまでもない
- 個人情報／パーソナルデータ保護と情報セキュリティは分けて考えたい
  - 個人情報／パーソナルデータ保護 … ポリシーの問題
  - 情報セキュリティ（アクセス制御） … 機能／機構の問題

有力なソリューションとしての情報銀行

- 「情報銀行」とは？
  - 個人情報／パーソナルデータのオーナーは誰か？
  - 個人情報／パーソナルデータを「信託する」
- 世界最先端IT国家創造宣言の最新版（2016年5月20日閣議決定）でも言及