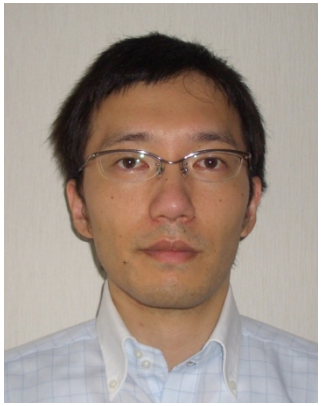
NAGOYA UNIVERSITY NCES 広島市立大学 Hiroshima City University

SWEST18 s2a,s3a@朝陽の間（舞台側）
組込み／自動車セキュリティ研究の最前線

講師

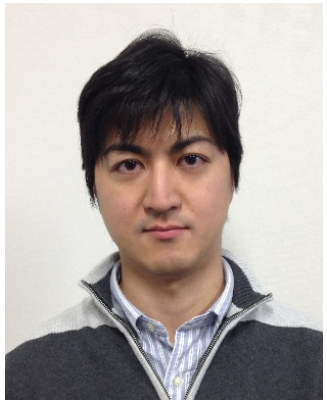
井上博之
広島市立大学／CCDS

倉地亮
名古屋大学



コーディネータ

松原豊
名古屋大学



[s2a] 8/26(金)9:00～10:10 チュートリアル編

- 最近，自動車，航空機，医療機器，制御システムなどの組込みシステムに対するセキュリティの脅威，脆弱性が多数報告されています
- 本セッションでは，まず，来るIoT時代に備えて，国内・海外の動向を紹介します
- さらに，国内の大学で研究を進めるお二人の先生方を交えて，主に，車載制御システムに関する研究を解説＆紹介頂きます

１時間で，最新情報を獲得できます！

[s3a] 8/26(金)10:30～11:40 パネル編

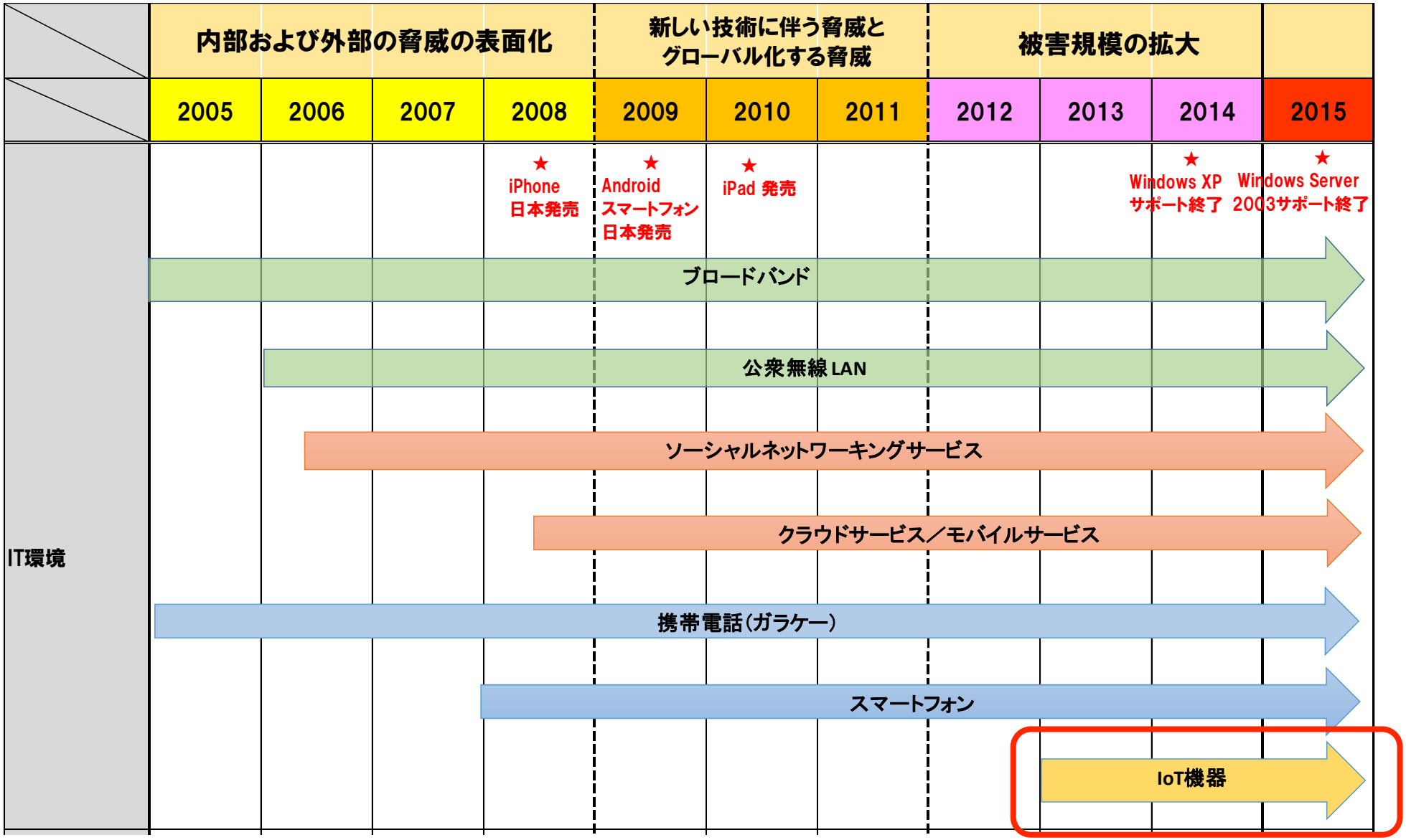
- s2a「組込み／自動車セキュリティ研究の最前線–チュートリアル編」を基に，会場の参加者を交えてパネル形式で議論します
- 主に，以下のテーマを議論する予定です
  - 最近，気になったセキュリティの話題は？
  - 世界的に見た日本の研究動向の位置付け，方向性の違いは？
  - 組込み／自動車セキュリティ人材の育成，スキルアップの方法は？
  - 公開された○○セキュリティガイドラインで足りないことは？

※時間の都合，参加者を交えた議論の状況に応じて，テーマを変更する可能性があります

参加者からの質問・提案を歓迎します！

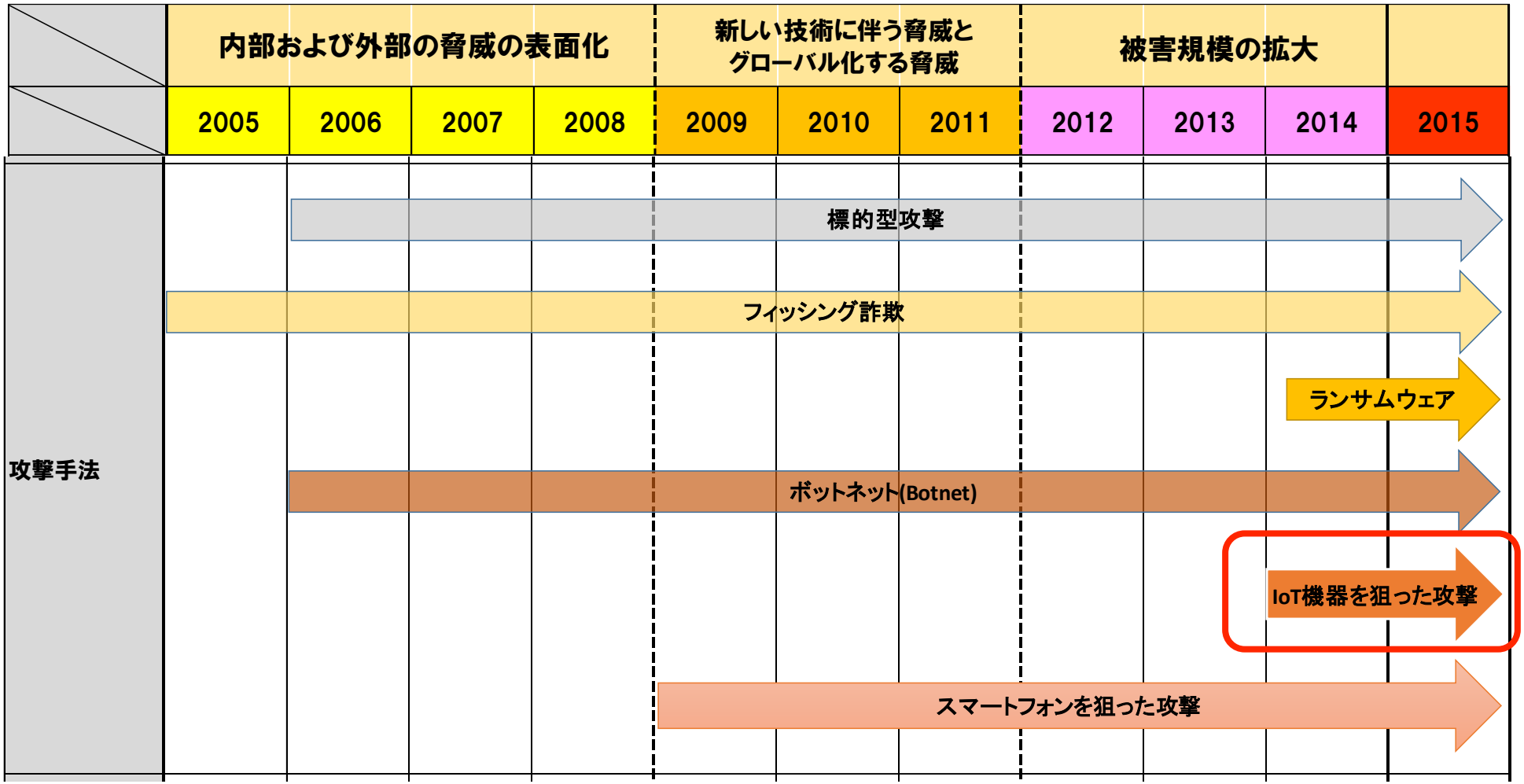
組込みセキュリティの基礎
組込みシステムのセキュリティの現状・事例

サイバーセキュリティの脅威の変遷（対象）



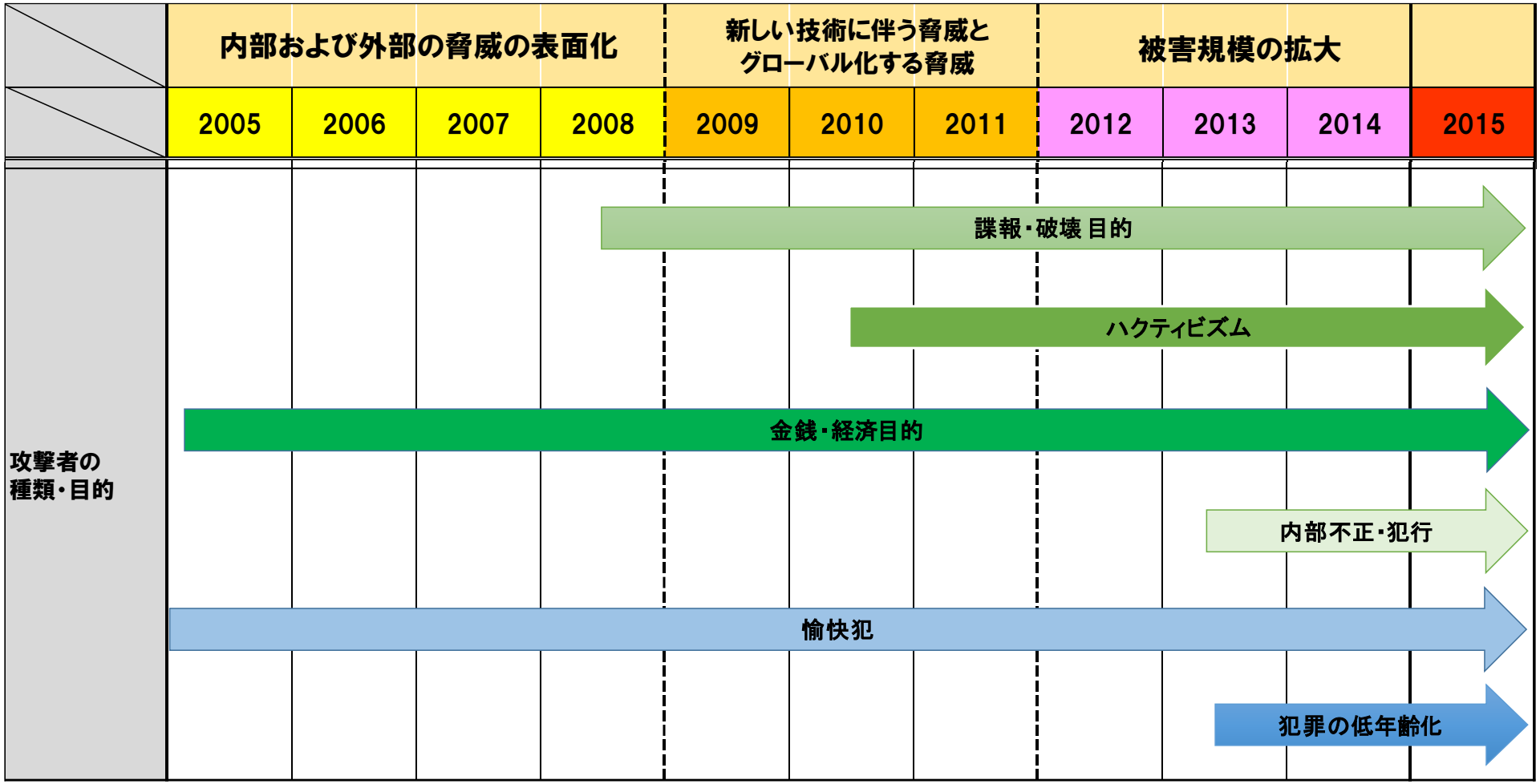
引用：「情報セキュリティ10大脅威 2016」https://www.ipa.go.jp/security/vuln/10threats2016.html

サイバーセキュリティの脅威の変遷（攻撃手法）



引用：「情報セキュリティ10大脅威 2016」https://www.ipa.go.jp/security/vuln/10threats2016.html

サイバーセキュリティの脅威の変遷（種類・目的）



引用：「情報セキュリティ10大脅威 2016」https://www.ipa.go.jp/security/vuln/10threats2016.html

組込み／IoTセキュリティが注目されている背景

組込みシステムの高機能化・ネットワーク化

- 製品，サービスの多様化により，ネットワークに繋がる組込みシステムが増加
- 独自開発ではなく既存技術の転用が増加
  - OS，TCP/IPスタック，USBスタックなど

→セキュリティの脅威が及ぶ

セキュリティの問題が安全性にも影響

- 安全性を確保する活動が浸透し，機能安全国際規格も広く普及しつつある
- 人命に関わる制御システムの安全性を確保するためには，故障の影響だけでなく，セキュリティの脅威を想定することが必要

→安全性とセキュリティの両立への要求が高まる

組込みシステムに対するセキュリティの脅威

情報家電

http://www.insurancejournal.com/news/international/2014/07/18/335214.htm

医療機器

http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack

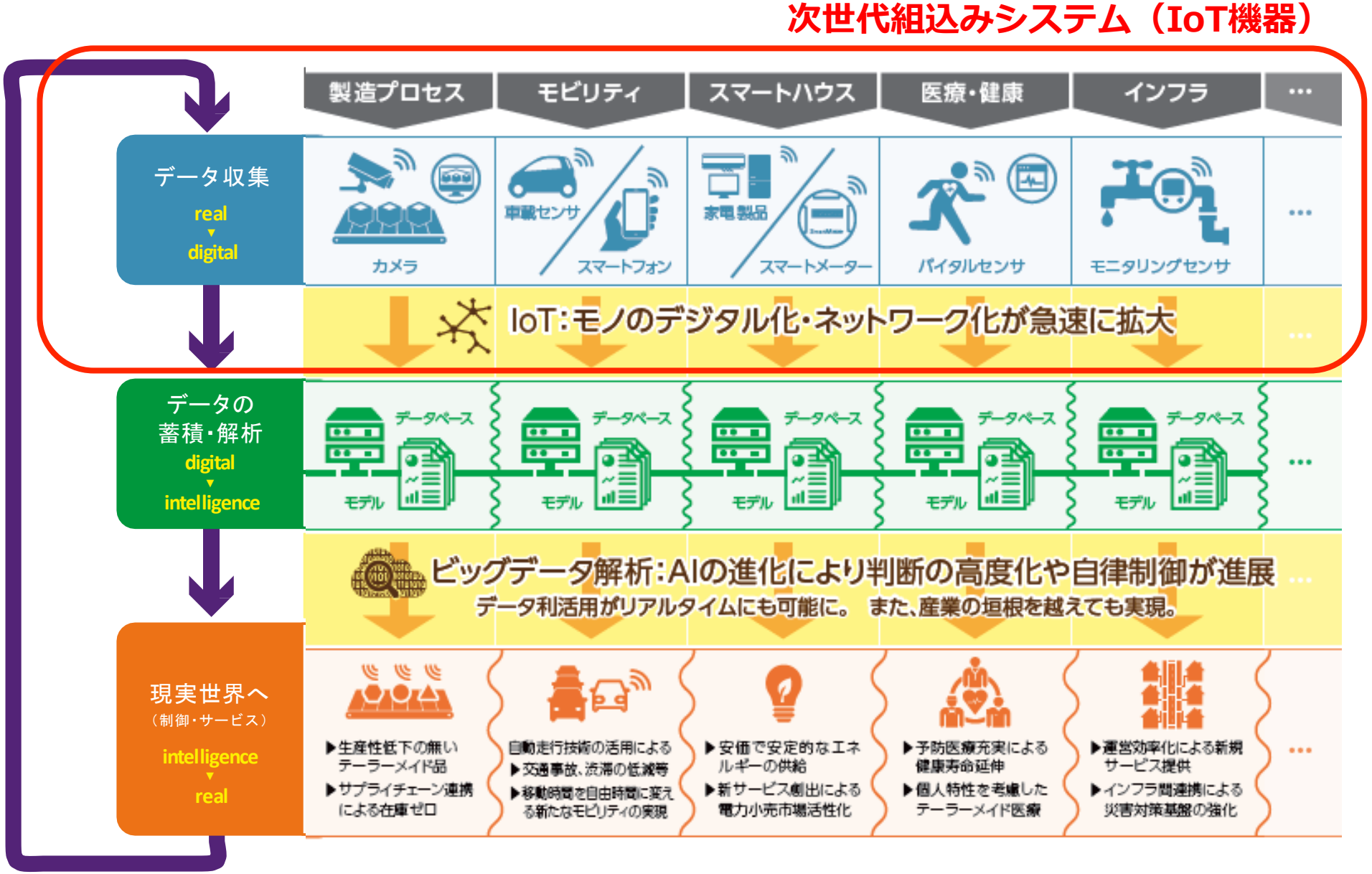
自動車

http://www.autoblog.com/2014/07/18/auto-industry-deals-with-hacking-cyber-threats/

産業ロボット

http://www.iec.ch/etech/2014/etech_0614/ca-1.htm

IoT(Internet of Things)による新たなサービス



資料：経済産業省作成

引用：2015年度版ものづくり白書

IoTサービス／システムのレベル分け

レベル１：モノのデジタル化・ネットワーク化

- モノの組込みシステム化 →まずはここから対応！
  - センサ，コンピュータ，アクチュエータなどを搭載
- 組込みシステムのネットワーク化
  - 今までつながっていなかったモノがつながる

レベル２：データの収集・解析とシステム間の連携

- モノやセンサの情報を大量に収集し，高性能コンピュータで解析（ビッグデータ）
  - 解析結果を人間が活用
- 複数のシステム間で互いの情報を交換

レベル３：モノの自律制御

- 収集した情報，解析結果を使って，モノを自律的に制御
  - 意思決定や状況判断にAIを活用する場面も

レベル１のIoTシステムの例

スマート電源

http://www.belkin.com/us/p/F7C029fc/

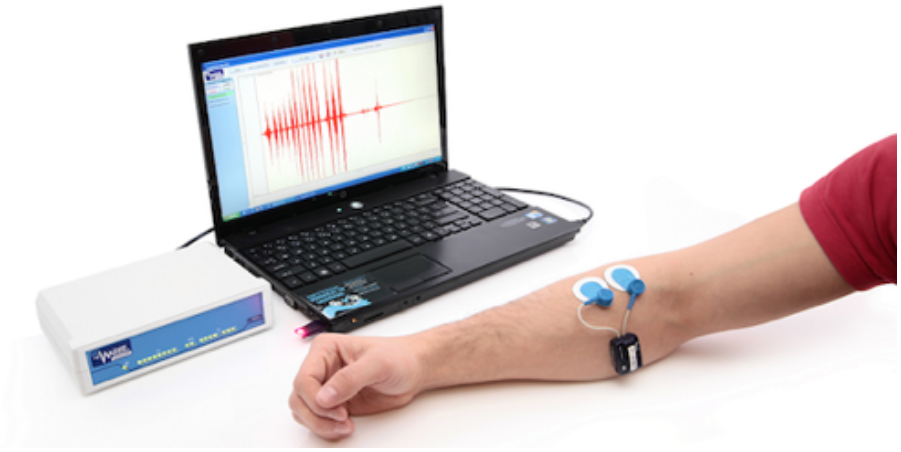
スマートキー

http://photosynth.co.jp

スマートマグカップ

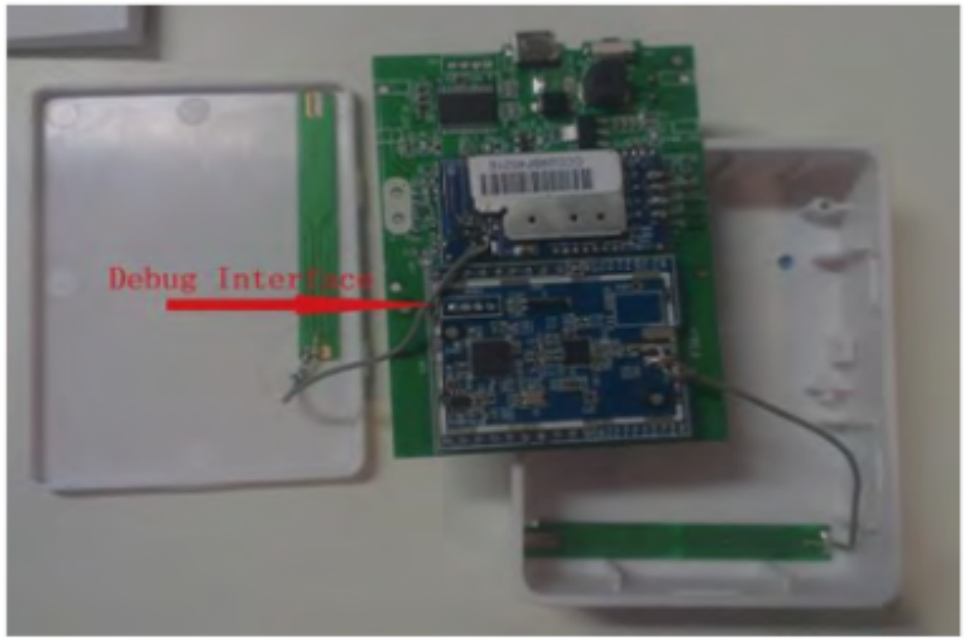
http://www.muggino.com/

ワイヤレス医療機器



IoT ゲートウェイに対する物理的攻撃

- LI Jun, YANG Qing：I’M A NEWBIE YET I CAN HACK ZIGBEE, DEF CON 23, 2015年
- WifiとZigbeeを利用した家電制御システムを対象に，家電（デモではZigbee搭載の電気バルブ）を不正に操作
  - 家電の中央管理システム（ゲートウェイ）を攻撃
  - ファームウェアのバイナリをリバースエンジニアリングし，Zigbeeデバイス認証用秘密鍵を特定
  - 秘密鍵を用いて，攻撃者の任意のデバイスから，Zigbeeデバイスを操作，攻撃可能に



Zigbeeデバイス自身をいきなり攻撃せずに，秘密鍵が格納されたゲートウェイを攻撃した後で，繋がっている家電を操作可能としたところがポイント
→車載機器やECUにも同様の脅威

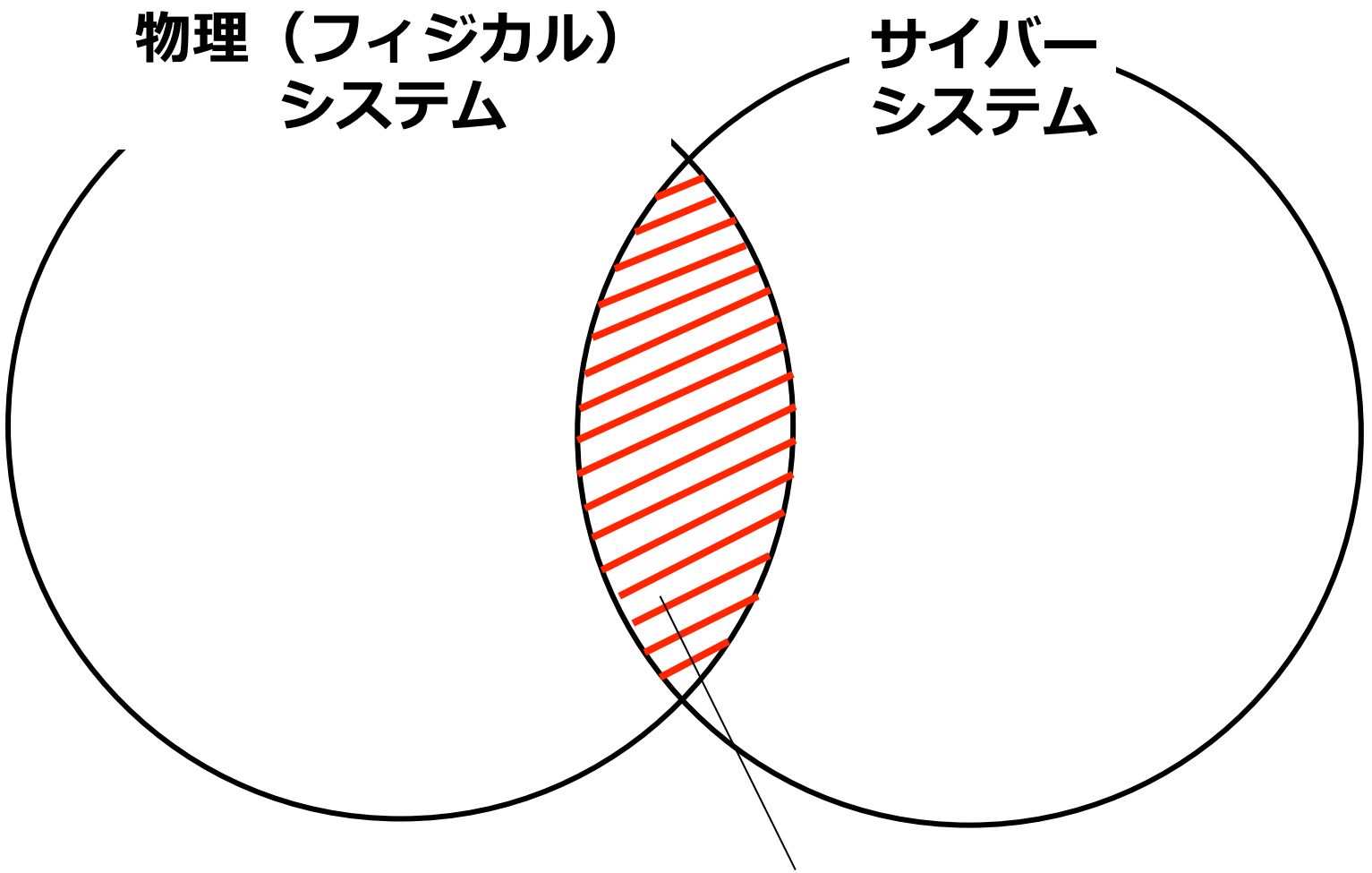
IoTデバイスに対するマルウェア

Familly name	Sample ID	File Name	Hash(md5)	Architecuture	Date of Capture	Existance in VirusTotal	Detection Ratio in VirusTotal
ZORRO	Bin 1	wb.arm	e94f48285ec44e739505889c922def55	ARM	2015/01	yes	0 / 56
	Bin 2	telnet.arm	4101d096094fa7f3b35a14cee8c5d6bb	ARM	2015/04	no	
	Bin 3	telnet.m68k	2d4c6238ad43bfcc4668467ef6846196	M68K	2015/04	no	
	Bin 4	telnet.mp	5c091a1c1311aa37443027a315b663f5	MIPS	2015/04	no	
	Bin 5	telnet.mps	acb79b0810aeb8e1db298cd678b33840	MIPSEL	2015/04	no	
	Bin 6	telnet.ppc	8e654a673d4bdd8ac16c39f7a4654e1b	Power PC	2015/04	no	
	Bin 7	telnet.sh4	60ee95389061b1c8ce0cf8b6f748c8a6	SH4	2015/04	no	
	Bin 8	telnet.sparc	9918dba3e5737d25424b05b9f10b16c0	SPARC	2015/04	no	
	Bin 9	telnet.x86	792d38b6fdd89d65d35d1b01cd1c2ba7	x86	2015/04	no	
Bashlite	Bin 10	arm	f73da5e1e33762f09d74e2d3d16c5c50	ARM	2014/11	yes	7 / 57
	Bin 11	i586	66113dc9a53866702ec0ca68a9a546b8	i586	2014/11	no	
	Bin 12	i686	6d9f7123e8692087bdb2822e44854eef	x86	2014/11	no	
	Bin 13	mips	c58e25360794355fc77c18b1688d4d01	MIPS	2014/11	yes	6 / 57
	Bin 14	mipsel	a265bab2443e0635a4adfe7f47e06974	MIPSEL	2014/11	no	
	Bin 15	sparc	738db9f6b9debd08976eaa91bbf16117	SPARC	2014/11	no	
	Bin 16	superh	a12e7f584177fb5d229707c5c7f7fa72	Super H	2014/11	no	
	Bin 17	arm	06b2fbee4e7ae5c1370753543b7d2e21	ARM	2015/04	no	
	Bin 18	i586	b7b299fdffbbaabd184ab4d8e69a4d98	x86	2015/04	no	
	Bin 19	i686	4061432ae8b37171af033d5185b31659	x86	2015/04	no	
	Bin 20	mips	3fc4bdb902e086e3e5681798036207e7	MIPS	2015/04	no	
	Bin 21	mips64	feb53f2aec98e96c1321a6811ac05a18	MIPS64	2015/04	no	
	Bin 22	mipsel	94b2e00fc4c11abd77fb76fd5815d1dc	MIPSEL	2015/04	no	
	Bin 23	ppc	06940d099751304c704f7a31c2459fb8	Power PC	2015/04	no	
	Bin 24	sparc	d76cf4f0f37395906df4d2c0defcd923	Super H	2015/04	no	
	Bin 25	arm	1549aed9b818b6a994dc5fb6c4a57fa2	ARM	2015/04	no	
	Bin 26	i586	daab490a0a0a0a2b2528b18dacbf66ed	x86	2015/04	no	
	Bin 27	i686	8a2b06d4ba8b88cab092801fbcbfd8b4	x86	2015/04	no	
	Bin 28	mips	61f32f7a0d4b7643fb03da75cf5a1329	MIPS	2015/04	no	
	Bin 29	mips64	ee7d764767c25d4c54be44f18a5aa47d	MIPS64	2015/04	no	
	Bin 30	mipsel	490968447a603c3664186164c99c14be	MIPSEL	2015/04	no	
	Bin 31	ppc	2695e6d6930fc3e5b3345f8cd811d693	Power PC	2015/04	no	
	Bin 32	sparc	132c5605752c9cfcc3f746b8451c7fe6	Super H	2015/04	no	
	Bin 33	arm	032ec8869e235bfa8a8dfe7b125a02b6	ARM	2015/05	no	
	Bin 34	i586	86f9fc4e914d358d05bd5d1d93a0d673	x86	2015/05	no	
	Bin 35	i686	c1ef1dd4232e14c45661e0a8a976867e	x86	2015/05	no	
	Bin 36	mips	a41867fbf8e2358ba5551509907b288c	MIPS	2015/05	no	
	Bin 37	mips32	77b73b0fe4a79dfc284fce55bf3cbe8b	MIPS32	2015/05	no	
	Bin 38	mips64	d31261199d16b7ad82e0f87094de6e07	MIPS64	2015/05	no	
	Bin 39	mipsel	c652fe5e53cba8c450ee6f7307408c8c	MIPSEL	2015/05	no	
	Bin 40	ppc	52f9bd74d63888182fbab15443b70898	Power PC	2015/05	no	
	Bin 41	sparc	be35cd9d4c6047e940e6c58a96fbf0b8	SPARC	2015/05	no	
nttpd	Bin 42	nttpd	bbf1327c1a5213b41a4d22c4b4806f7c	MIPSEL	2015/05	yes	0 / 57
KOS	Bin 43	1225.8196	ec381bb5fb83b160fb1eb493817081c1	MIPS	2015/05	no	

IoTPOT: A Novel Honeypot for Revealing Current IoT Threats (Preprint)
Yin Minn Pa,Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, 情報処理学会論文誌, Vol.57, No.4, pp.- (2016-04-15)

組込みセキュリティの基礎
組込みセキュリティの位置付けと課題

組込みシステムの位置付け



サイバー・フィジカルシステム

物理システムとサイバーシステムの両方の特徴を持つ

→組込み／IoTシステムや自動車はここに関係する場合が多い

組込みシステムのセキュリティの位置付け

	物理セキュリティ	サイバーフィジカル セキュリティ （組込み）	サイバー セキュリティ
資産	物理的資産（人，物，環境など）	**両方の資産が対象に！**	主にコンピュータが保持する情報
攻撃系経路	資産に対して，直接的，間接的に影響を与える，物理的なインタフェース	**攻撃方法，経路が多種多様に！** ↓ **攻撃者にとって，最も簡単で安く，攻撃リスクが低いところが狙われる**	主に，コンピュータへの入力装置，インターネットや無線通信などの通信インタフェース
攻撃コスト	低い～高い（多様）		比較的低い
攻撃者の特定確率	高い		低い
セキュリティ対策	• 資産所有者自身による対策 • 防犯サービス会社 • 国（法律，警察，特殊機関）	**資産所有者・企業，サービス提供企業，国が連携した対策が必要**	• セキュリティ対策機器，ソフトウェア • サイバーセキュリティサービス会社 • 国（法律，警察，特殊機関）

組込み／IoTシステムにおける セーフティとセキュリティの違い

	セーフティ（安全性）	セキュリティ
対象範囲	• 開発対象のシステムのみ • 安全系システムの系統的・物理的な故障への対策 • 非安全系から安全系へ影響防止	• 開発対象のシステム**＋つながるシステム** • 脆弱性の放置，意図的な攻撃への対策
前提	• 利用者，開発者，第三者は信用できる（可能な限り，リスクを低減するよう行動する）	• 利用者，開発者，第三者は**何らかの意図と持って行動する**（脅威となる）場合がある
実現するための基本的な考え方	• システムを安全状態に遷移，維持する • フェールセーフが有効でない場合には，冗長系で信頼性を高める	• システムのセキュア状態は存在しない • 脅威はなくならない．むしろ，**時代とともに増加する**と考えるべき
対策への要求レベル指標	• SIL(Safety Integrity Level)	• SAL(Security Assurance Level) • TAL(Trust Assurance Level)
国際規格	• グループ規格に加えて分野ごとの規格が整いつつある	• 情報セキュリティに関しては普及段階にある（例えばCCがある） • **組込み／IoTセキュリティに関しては，ガイドラインが各所から発行されている（乱立状態）**

組込みセキュリティが難しい理由

1. 脅威や脆弱性の網羅的な分析が困難
   - 複数のシステムやサービスが連携する複雑な分散システムの横断的，多角的な分析が必要
2. 製品の利用期間が長く，利用範囲が広い
   - 将来の脅威，脆弱性の発見に備える仕組み
   - セキュリティを改善する統一的な仕組み
     - OTAFU(Over-the-Air Firmware Upgrade)の活用
3. リソース，コスト制約が厳しい
   - セキュリティ対策によるコスト増をどこまで許容できるかの判断（経営的な判断にも影響？）
4. 規格，業界標準がない
   - 誰が何をどこまでやれば良いか（責任の所在）
   - システムによって異なる資産の明確化

組込み／IoTシステムのセキュリティ対応の現状

セキュリティ専門家，技術者不足

- 組込みシステム技術，安全に関する技術者・知見者は，（他業界に比べると）多いと思われるが，セキュリティの技術者はまだ少ない
- 組込みシステムの知識を持つセキュリティ専門家が少ない（特に日本）
  - 情報セキュリティ，特定の技術（暗号，チップ等）の研究者，専門家は多いが…

国際規格整備の遅れ

- 安全性，情報セキュリティの国際規格は，すでに普及段階にある
  - 特定分野を対象に，官公庁や関連団体が主導してガイドラインをまとめる動きも出始めている
- 組込みシステムのセキュリティ，安全性＋セキュリティの規格は，議論・検討段階

今後は、人材の育成と、ガイドライン運用がより重要に！

井上博之先生の資料は非公開です

自動車の制御システムに対する セキュリティ強化の取り組み

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
倉地　亮

kurachi@nces.is.nagoya-u.ac.jp

最終更新日: 2016年8月20日

アジェンダ

- 1. 自動車のセキュリティの課題
  - 車載制御システムの進展と脅威
- 2. 我々の取り組み事例
  - 自動車に適したセキュリティ技術の提案例を紹介
- 3. 最後に
  - まとめと今後の展開

1. 自動車のセキュリティの課題

車載電子制御システムの進展

- 多くの機器（センサやアクチュエータ）を制御することで機能を実現
- 機器によって定まる時間制約をもつリアルタイムシステム
- 時間制約を満たせない場合に重大な事態となりうる
- 昨今では，自動運転やアクティブセーフティと呼ばれる機能が拡充

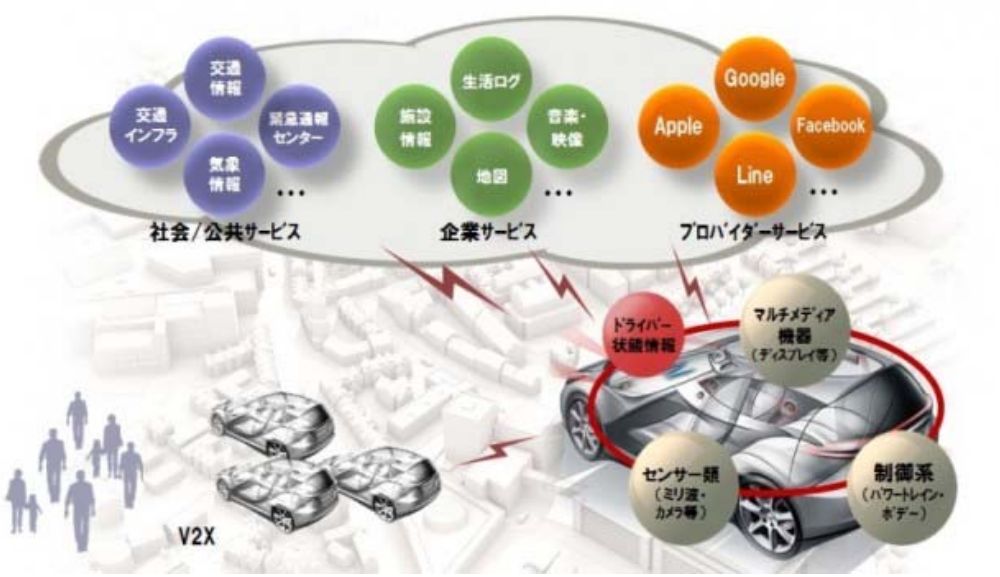
（例）VW Phaeton：

・11,136個の電子部品が搭載
・通信
  ・61個のECUが搭載
  ・外部からの診断のために31個のECUがシリアル通信
  ・35個のECUが4つのCANバスに接続
・通信データ
  ・2500個のシグナル
  ・250個のCANメッセージを使用

http://www.iestcfa.org/presentations/wfcs04/keynote_leohold.pdf

増える接続機器

○自動車/インフラ/サービス

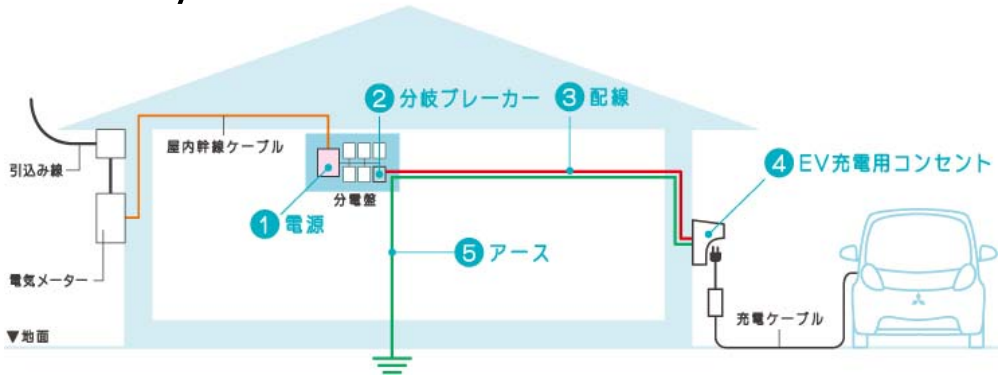


http://news.livedoor.com/article/detail/9378308/

○持ち込み機器(スマホ)

http://www.clarion.com/jp/ja/newsrelease/index_2012/120507_01/

○住宅/設備



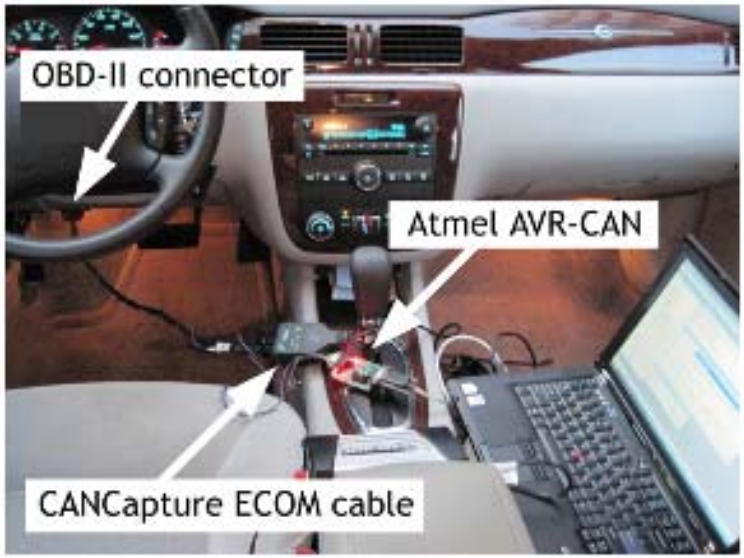
http://www.ev-life.com/charging/introduction.html

- 無線の接続経路が増加
- 新しい機器やインフラとの接続
- 先進運転支援機能も増加
  (例:自動ブレーキ, 追従走行)

自動車における攻撃事例 - 有名な事例

- 2010年頃から自動車の脆弱性をつく攻撃事例が登場
- 車載制御ネットワーク(CAN)になりすましメッセージを流すことで，意図しない制御を実現させる攻撃が存在
- 2015年には，脆弱性のある自動車がリコールされる事態に.

■事例1：Koscher (2010)



http://www.autosec.org/pubs/cars-oakland2010.pdf

■事例2：Miller - Prius (2013)

http://hackaday.com/2013/07/26/defcon-presenters-preview-hack-that-takes-prius-out-of-drivers-control/

■事例3：Valasek - Ford(2015)

http://japan.cnet.com/news/service/35067691/

自動車においても，セキュリティ対策が無視できない状況になりつつある

事例1. 自動車のCANネットワークに対する機器接続

- 実現した脅威
  - 急ブレーキ/ブレーキの無効化
  - 運転手の意思とは関係なくハンドルの操舵
  - ワイパー/ライト/ロックの意図しない動作/無効化，エンジンの停止･･･

K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, “Experimental Security Analysis of a Modern Automobile,”in 2010 IEEE Symposium on Security and Privacy (SP), May 2010

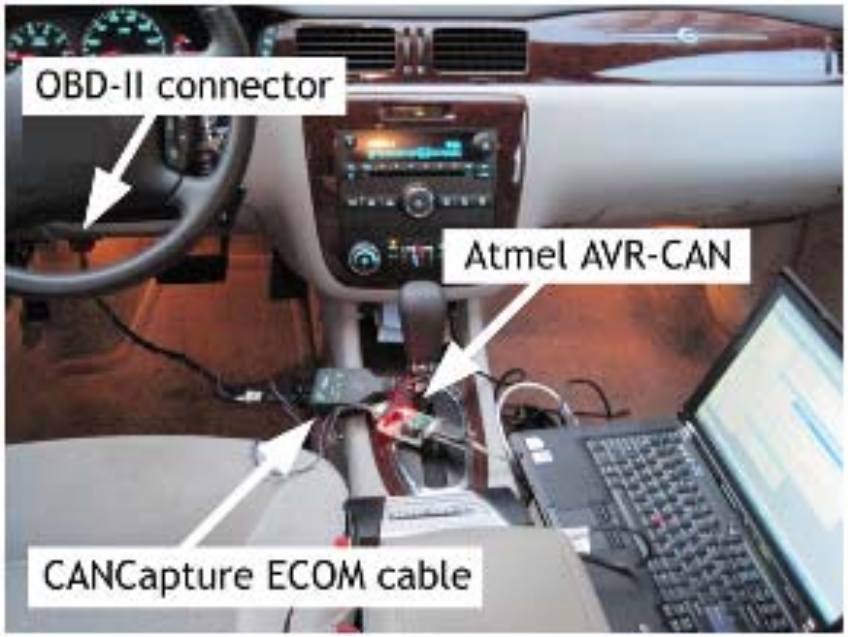


図1. 自動車内のOBD-IIポートから侵入

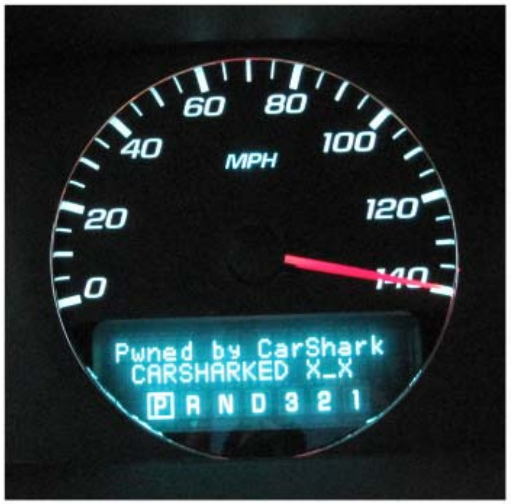


Figure 6. Displaying an arbitrary message and a false speedometer reading on the Driver Information Center. Note that the car is in Park.

特定の自動車でCANメッセージを注入し不正操作を実証

我々のモチベーションと研究課題

- 我々のモチベーション
  - まだ標準的な対策技術や評価技術が存在しないため，業界標準技術を目指す
- 研究課題とその目的
  - **1) 自動車の安全性を侵害する脅威への対策技術**
    - 情報セキュリティ技術をそのまま適用するとコスト高な自動車になる可能性がある
    - 適切なセキュリティ強度とコストの良いトレードオフ技術を探索する
  - **2) 自動車のセキュリティ評価技術**
    - システムあるいはプロトコル特有の評価手法やツールが存在しないため，効率の高い手法やシステムを実現する

2-1. 自動車の安全性を侵害する脅威への対策技術

自動車に適したセキュリティ技術の提案例を紹介する.

対策技術1: エラーフレーム監視

CAN/CAN-FDにおける攻撃検知技術の一例を紹介

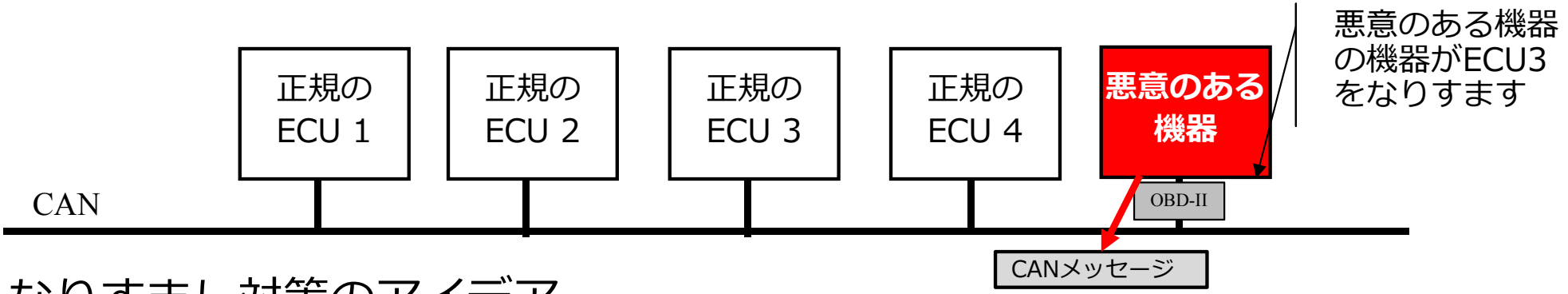
※公開資料からは内容を削除させていただいてます.

対策技術2: CaCAN

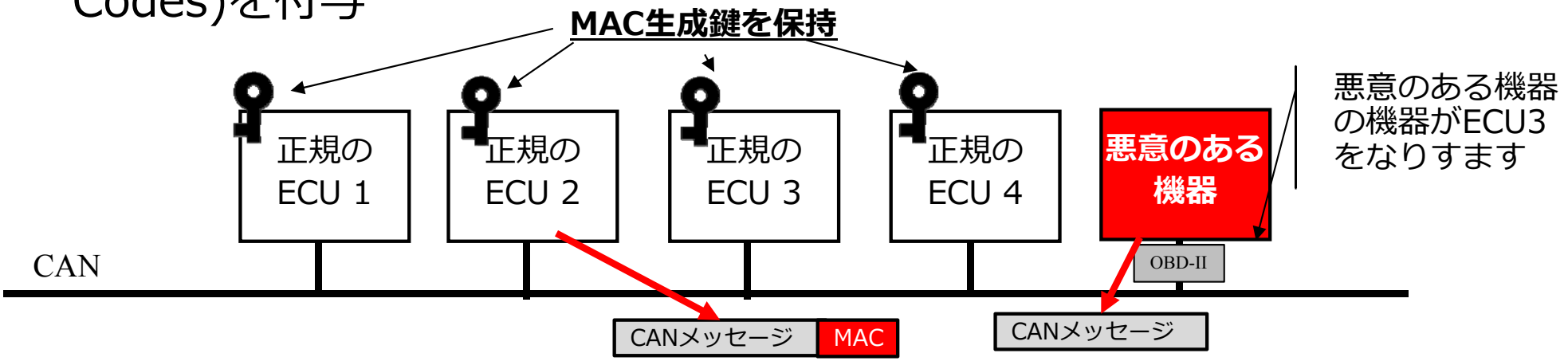
CAN/CAN-FDにおけるなりすまし防止機構を紹介

想定される脅威となりすまし対策のアイデア

- 脅威
  - OBD-IIポートなどに接続した悪意のある機器から不正なメッセージ(正規ECUが送信するCANメッセージのなりすまし)を注入



- なりすまし対策のアイデア
  - CANメッセージに認証情報(MAC: Message Authentication Codes)を付与



既存手法1: CANのメッセージ認証 in AUTOSAR

- PDUにメッセージ認証コード(MAC)の一部を付与
- すべてのノードでMACの計算に使用する共通鍵を保持

すべての受信ノードでMACを計算するには計算機リソースが不足

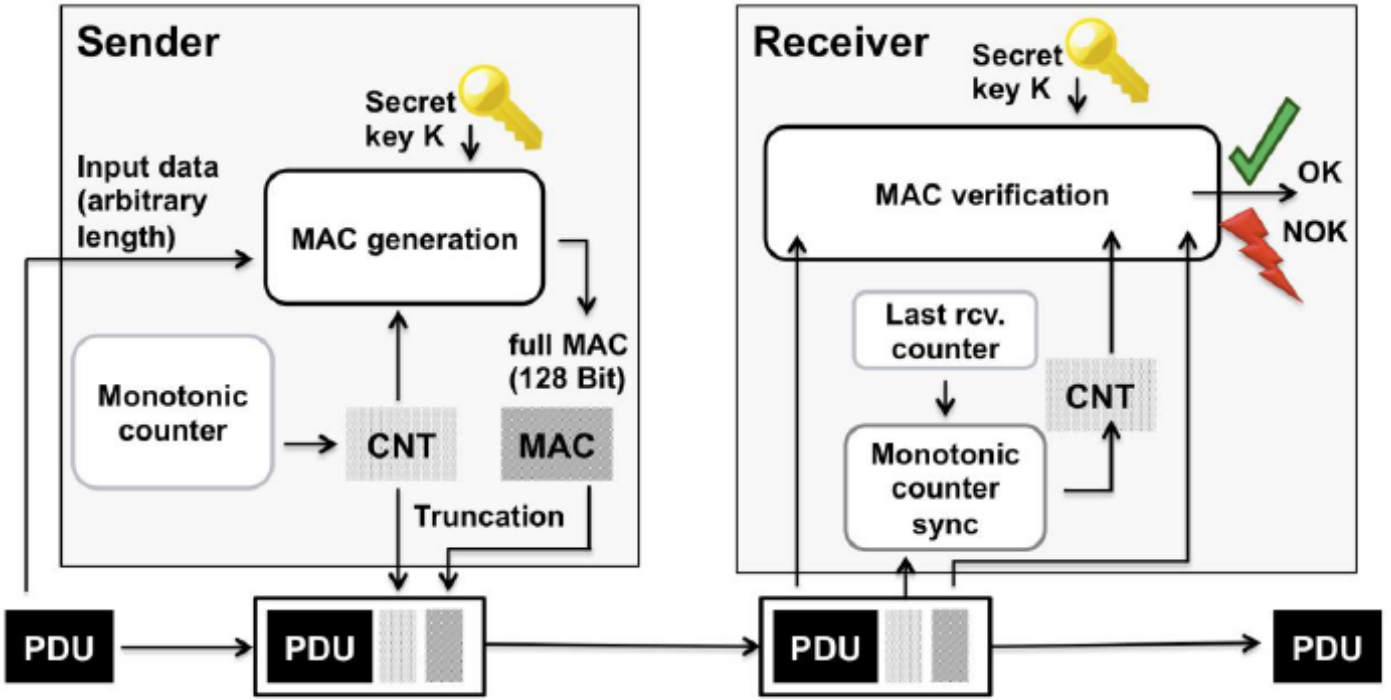
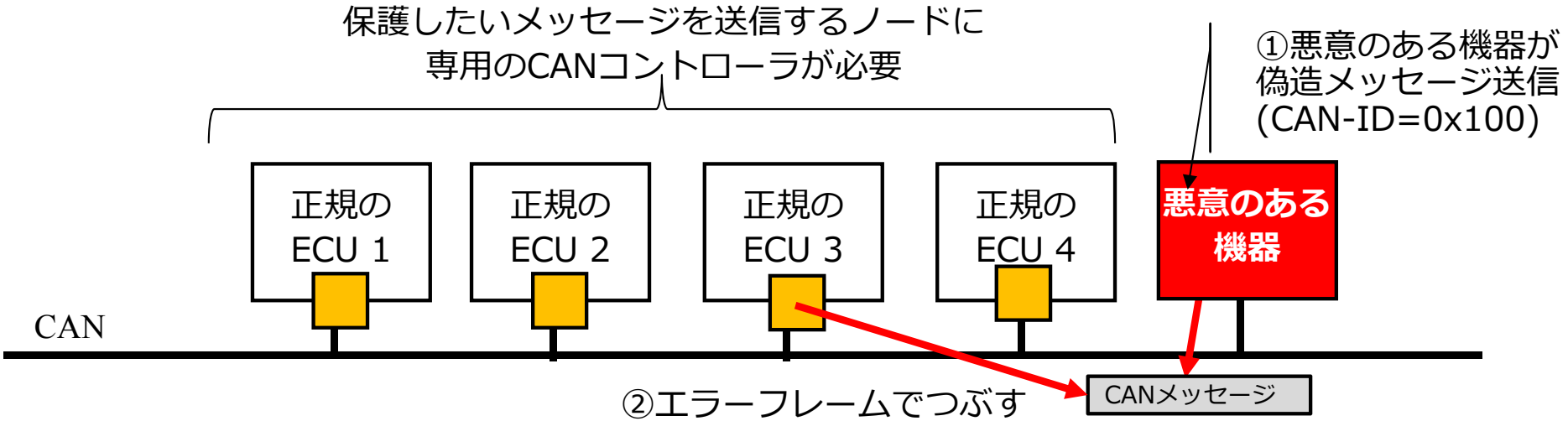


Figure 1: Message Authentication and Freshness Verification

Autosar version 4.2.1, Requirements on Module Secure Onboard Communication, AUTOSAR_SRS_SecureOnboardCommunication.pdf

既存手法2: CAN-IDによる不正メッセージの打ち落とし

- 特徴
  - 自身が送信するCANメッセージを他ノードから送信されたら，エラーフレームで打ち落とす
  - CAN-IDを用いて，不正メッセージを検出
- 良い点
  - CANメッセージのオーバーヘッドなし
  - ハードウェアの変更のみで良い
- 悪い点
  - 保護したいメッセージを送信するノードに専用コントローラが必要



Matsumoto, T., Hata, M., Tanabe, M., Yoshioka, K. et al.,“A Method of Preventing Unauthorized Data Transmission in Controller Area Network,” Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th, 2012.

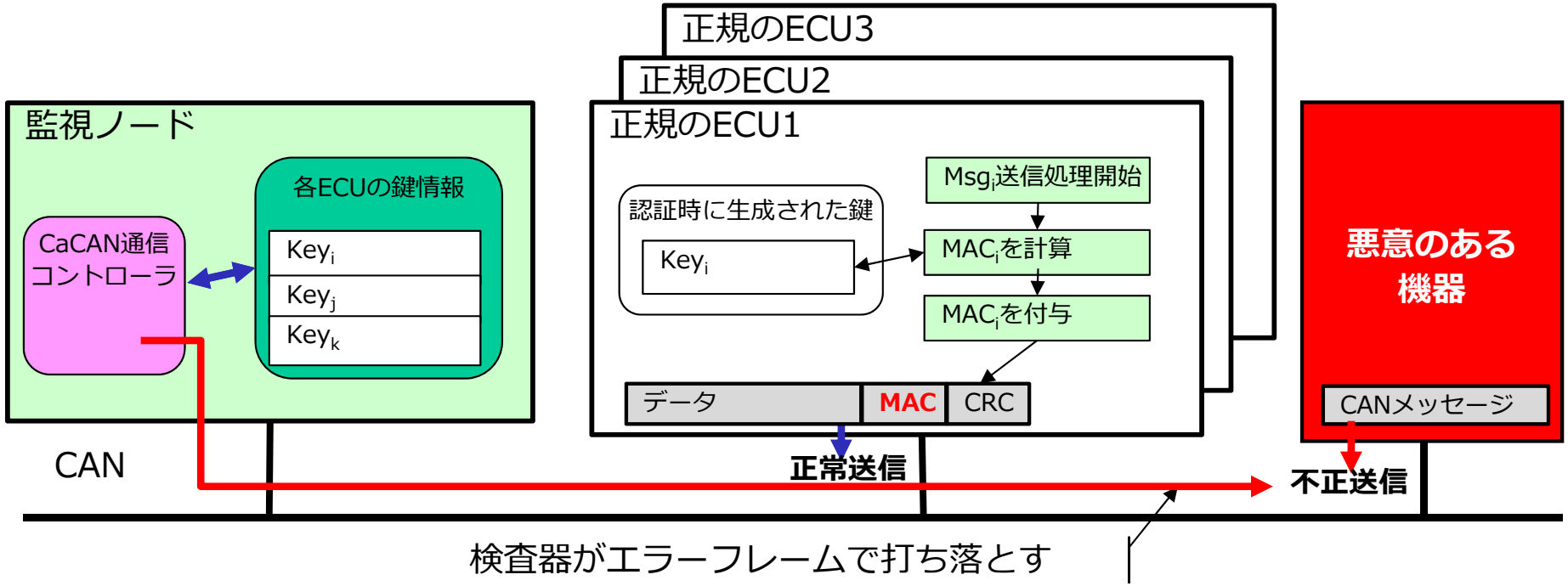
我々の提案– 集中型セキュリティ監視(CaCAN*) -

*Centralized Authentication system in CANの略

- アイデア
  - 監視ノードがなりすましメッセージをエラーフレームで打ち落とす

※松本先生らとの違いは，監視したいメッセージを送信するすべてのノードに改造されたCANコントローラを必要としないこと

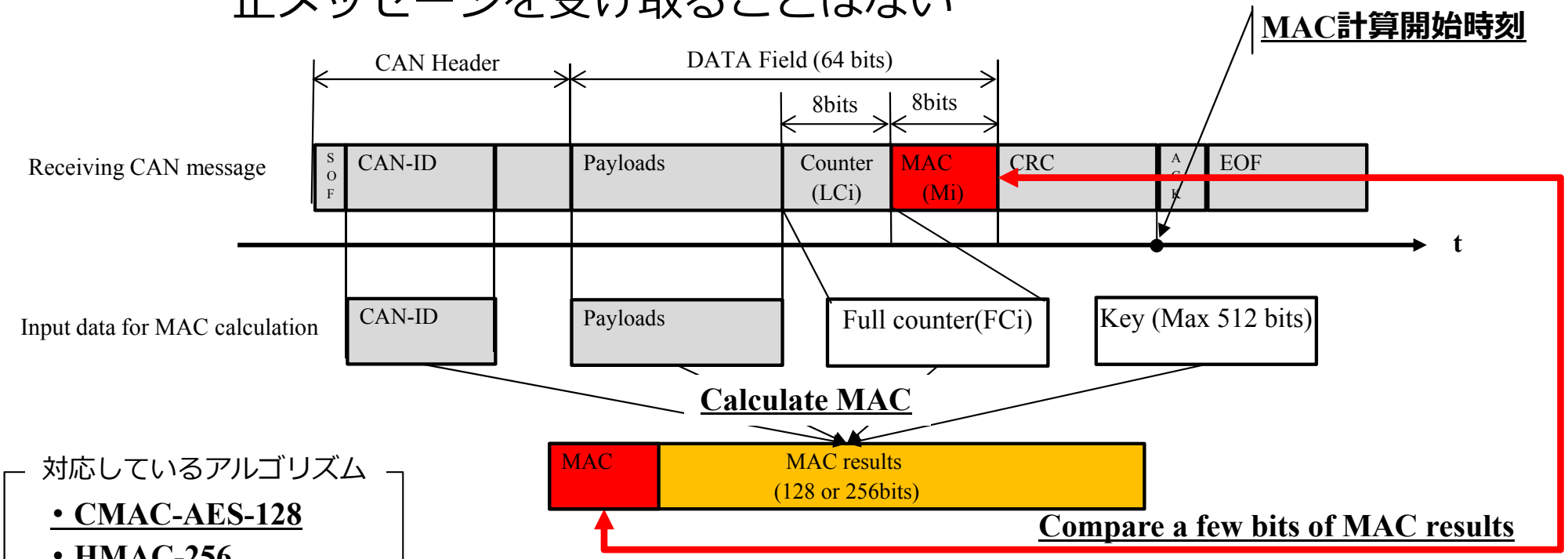
- 手段
  - 監視ノードが各ECUを認証し鍵を交換
  - 認証されたECUはMACを付与しCANメッセージを送信



Kurachi, R., Matsubara, Y., Takada, H., Adachi, N., Miyashita, Y., and Horihata, S., ”CaCAN - Centralized Authentication System in CAN”, Proceedings of the escar 2014 Europe Conference, Hamburg, Germany, Nov 2014

CaCANコントローラ

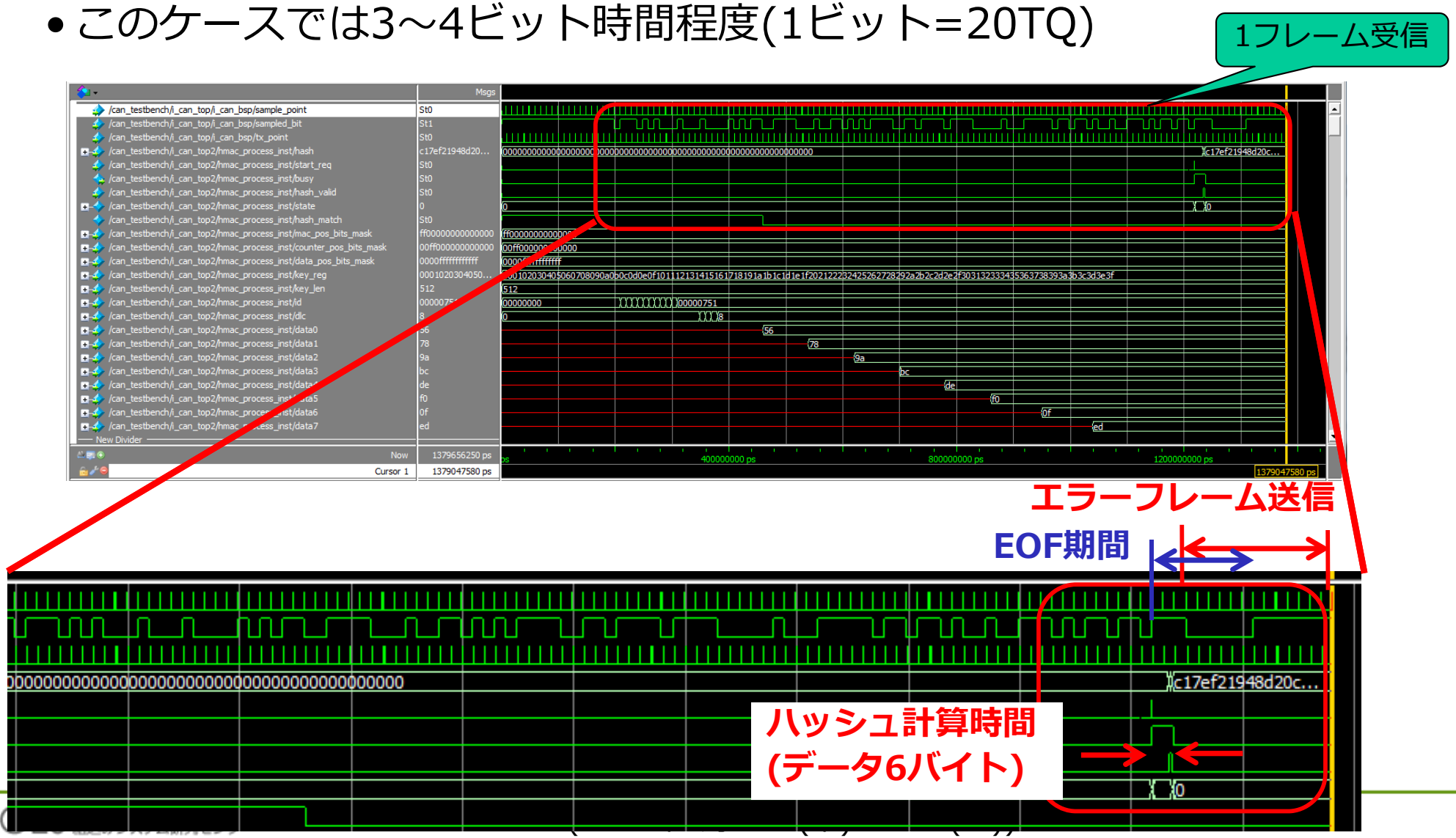
- CaCANコントローラの役割
  - 受信したメッセージに正しいMACが付与されているか検査
  - MACが異常となるメッセージをエラーフレームで打ち落とす
- CaCANコントローラの効果
  - 監視ノードがエラーフレームを送信した場合，他のノードも不正メッセージを受け取ることはない



対応しているアルゴリズム
- **CMAC-AES-128**
- **HMAC-256**

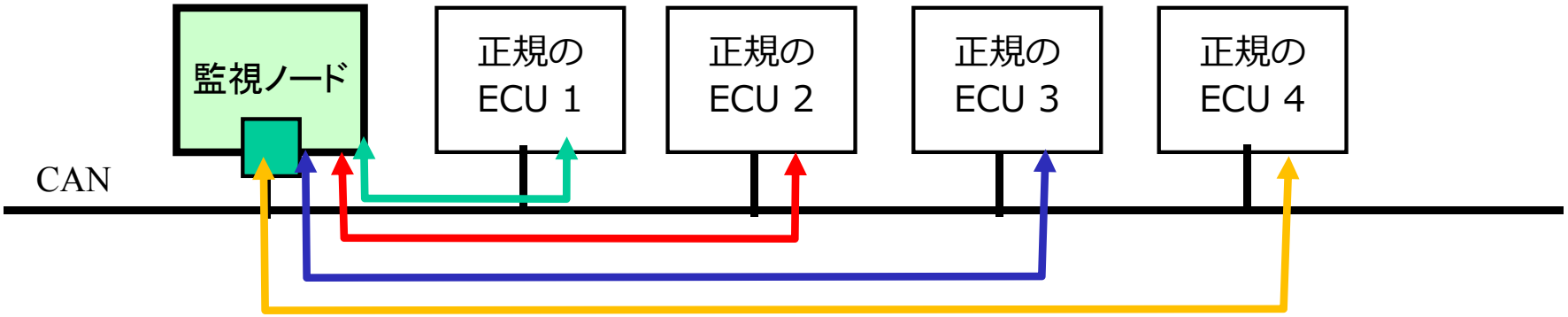
CaCANコントローラの実装

- CaCANコントローラの実現性を評価
  - MACの計算処理がEOF期間内に完了可能か？ ⇒ **CaCANは実現可能**
- このケースでは3～4ビット時間程度(1ビット=20TQ)

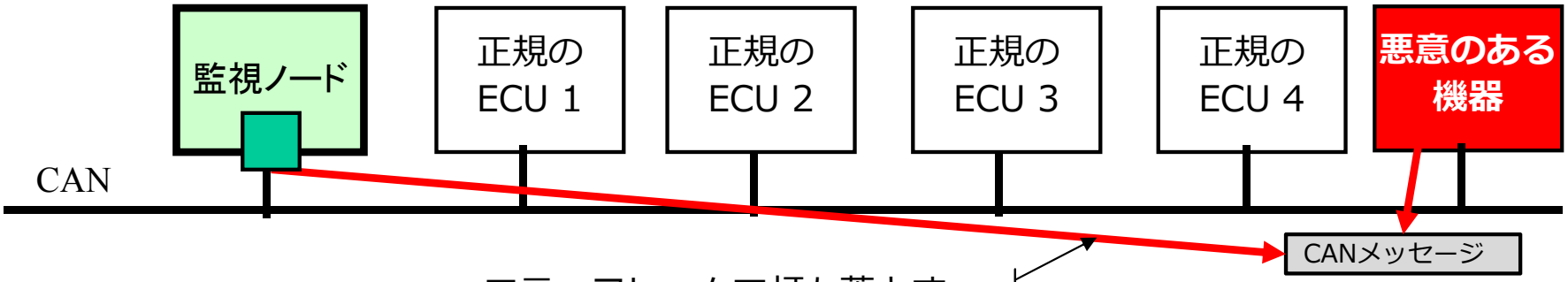


提案手法の強い点

- 監視ノードとの1対1の鍵交換のみでよい
  - 他の手法では，暗号化のためにM(送信):N(受信)で鍵交換
  - 通信オーバーヘッド最小．鍵漏えいのリスクも低い．



- ハードウェアの改造は1ノードのみで十分
  - 監視ノードからのエラーフレームで不正メッセージを潰せる
  - CANコントローラを改良せず，監視機能を外付けにしても良い

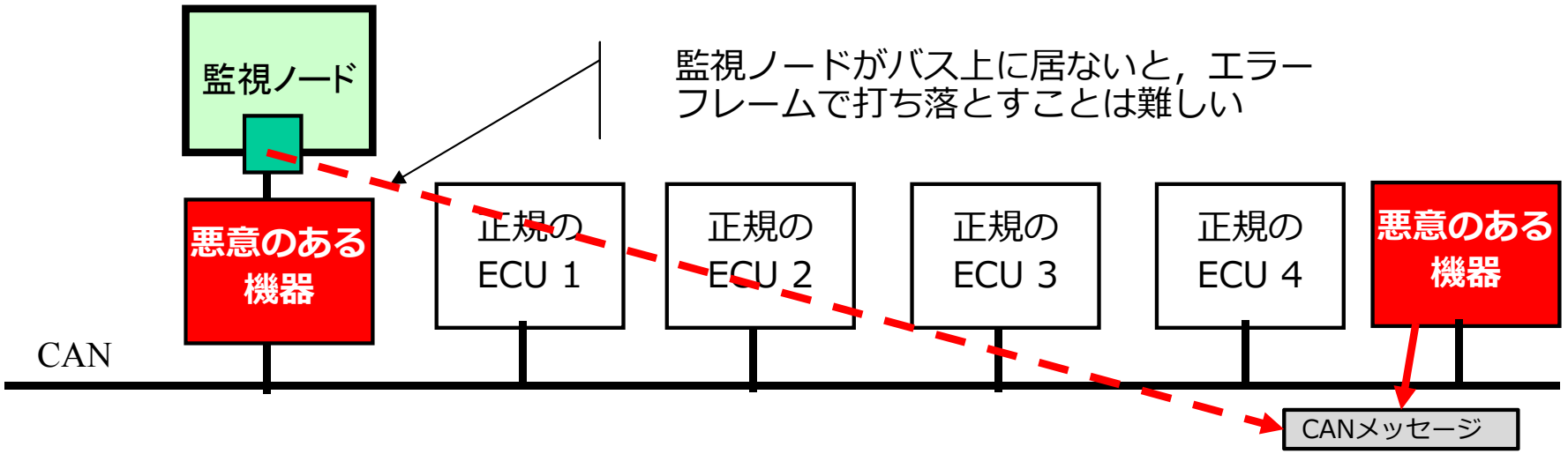


提案手法の弱い点

- 監視ノードが取りはずされる場合，監視機能が無効化
  - 機器取り外し攻撃: 監視ノードによる打ち落としが無効化

- 機器取り外し攻撃の対策方法
  - 機器が取り外されたことを検出できるコネクタの採用
  - 機器が取り外されると動作しないような重要なノードに監視機能を同居させたり，複数の監視ノードを配置することも可能

○中間者攻撃(監視ノードの無効化)の例



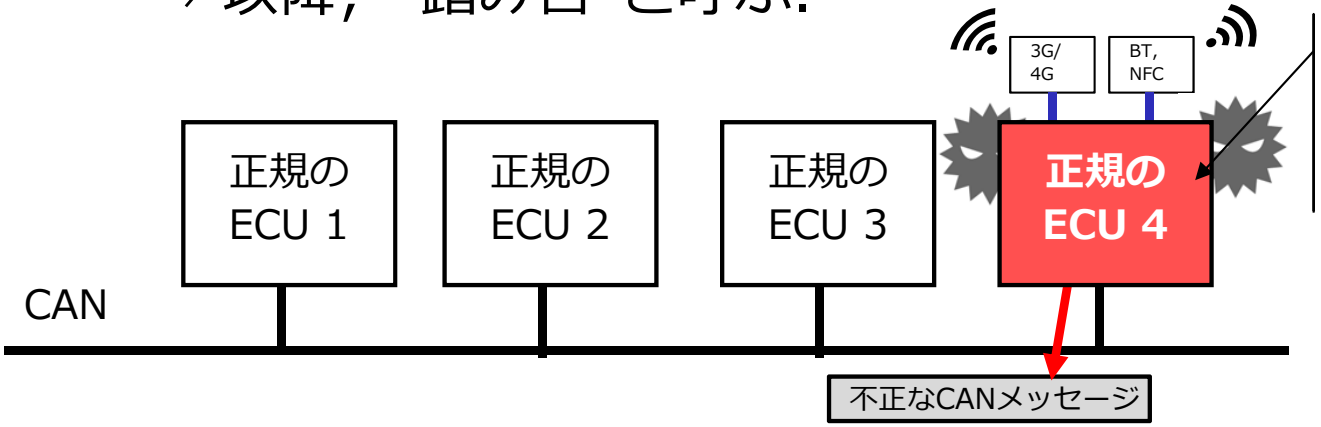
対策技術2: CAN Disabler

CAN/CAN-FDにおける不正送信防止機構の例を紹介

想定される脅威

- 脆弱性の事例より
  - 外部ネットワークに接続されるECUのプログラムが書き換えられる
  - プログラムが改ざんされたECUによる他のECUのなりすまし送信

    ⇒ 以降，“踏み台”と呼ぶ.



プログラムが書き換えられた/
マルウェアが仕込まれたECUによる他のECUのなりすましメッセージ送信

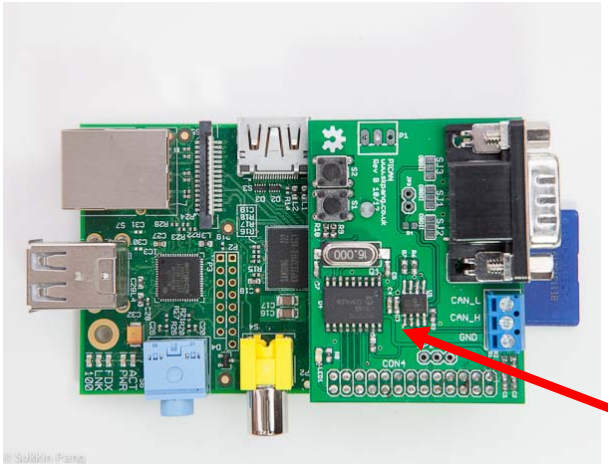
- 踏み台ECUによる攻撃例:
  - 1) なりすまし送信
  - 2) DoS攻撃

- 我々の研究のモチベーション

今後はFOTAによるECUのソフトウェア更新も要求されているため，
ECUのソフトウェアの対策だけではなくハードウェアでも対策できないか

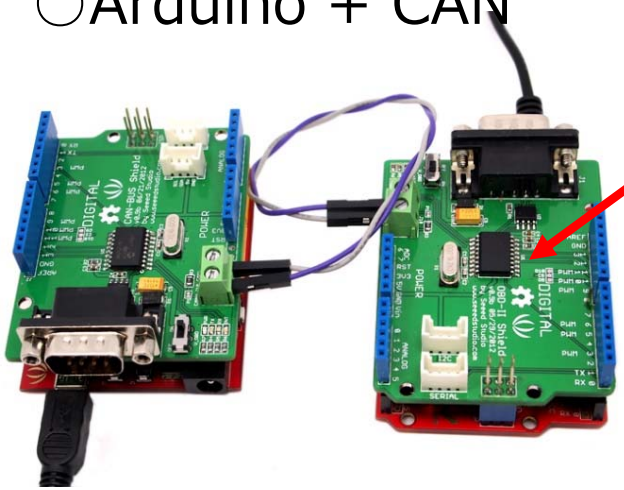
CAN Controller - Microchip MCP2515 -

○Raspberry pi + CAN

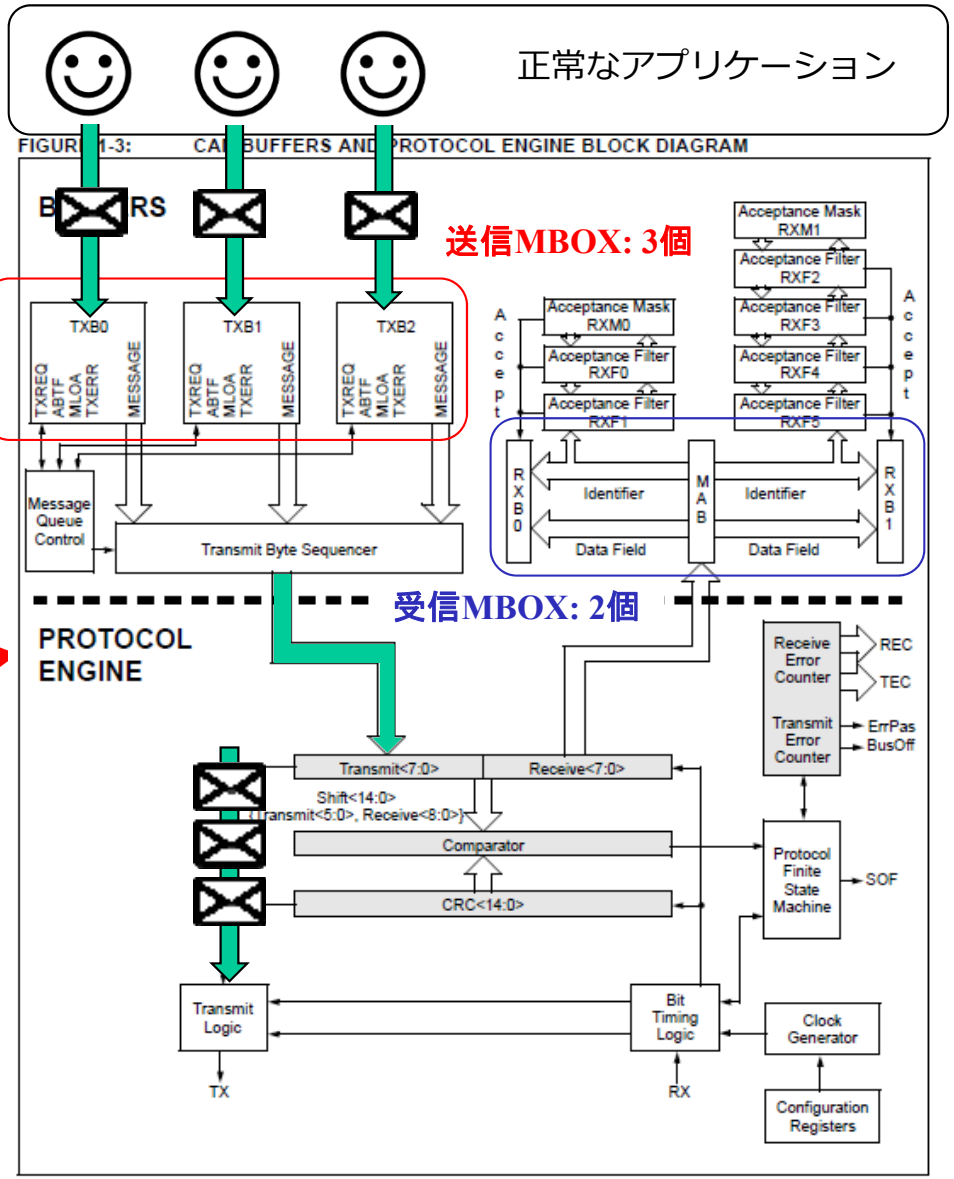


http://skpang.co.uk/catalog/pican-canbus-board-for-raspberry-pi-p-1196.html

○Arduino + CAN



http://www.seeedstudio.com/wiki/CAN-BUS_Shield

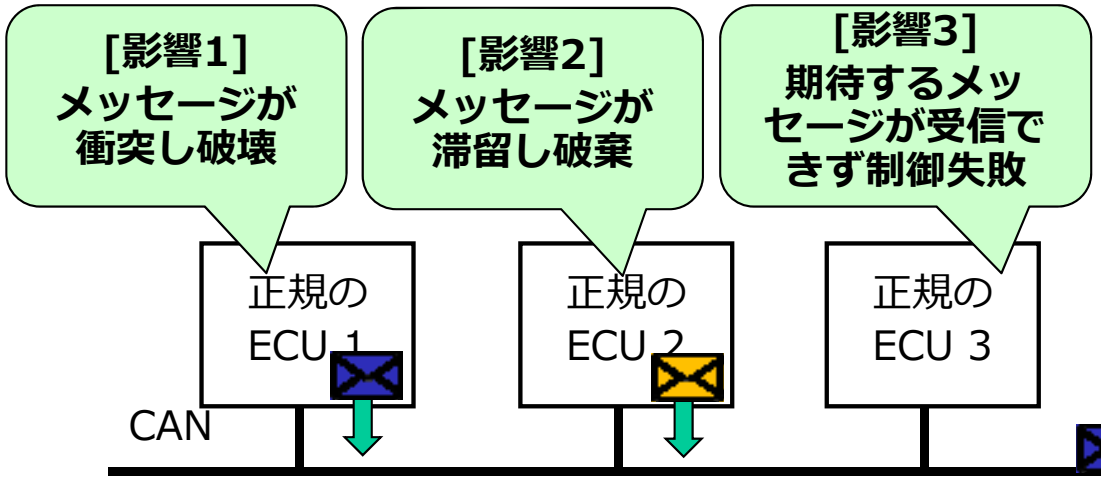


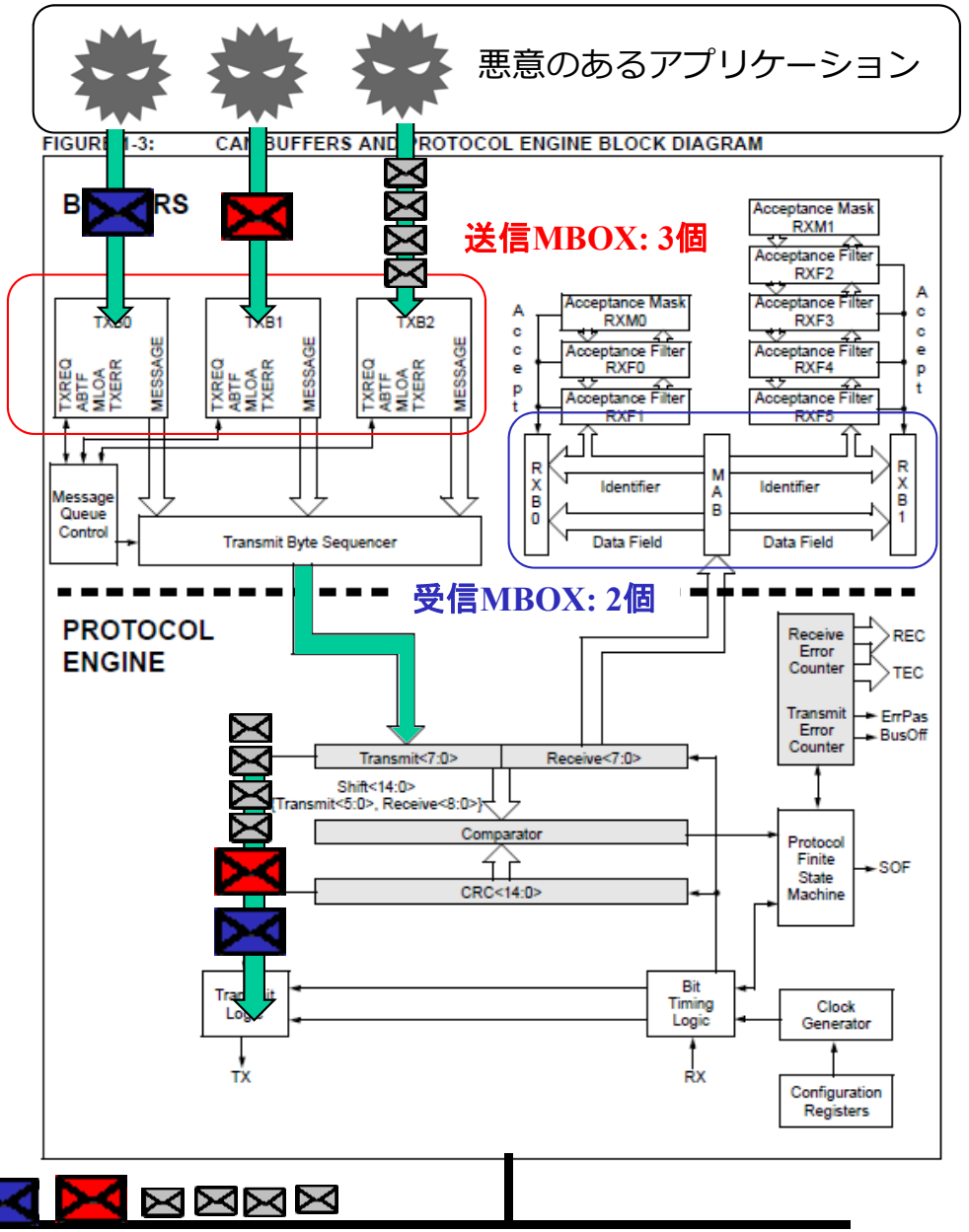
踏み台ECUの課題と影響

- **踏み台ECUの課題:**
  - 悪意のあるアプリケーション からのすべての送信要求を 許可してしまっている

踏み台ECUによる攻撃

- 他のECUのなりすましメッセージ
- 自ECUのなりすましメッセージ
- DoS攻撃

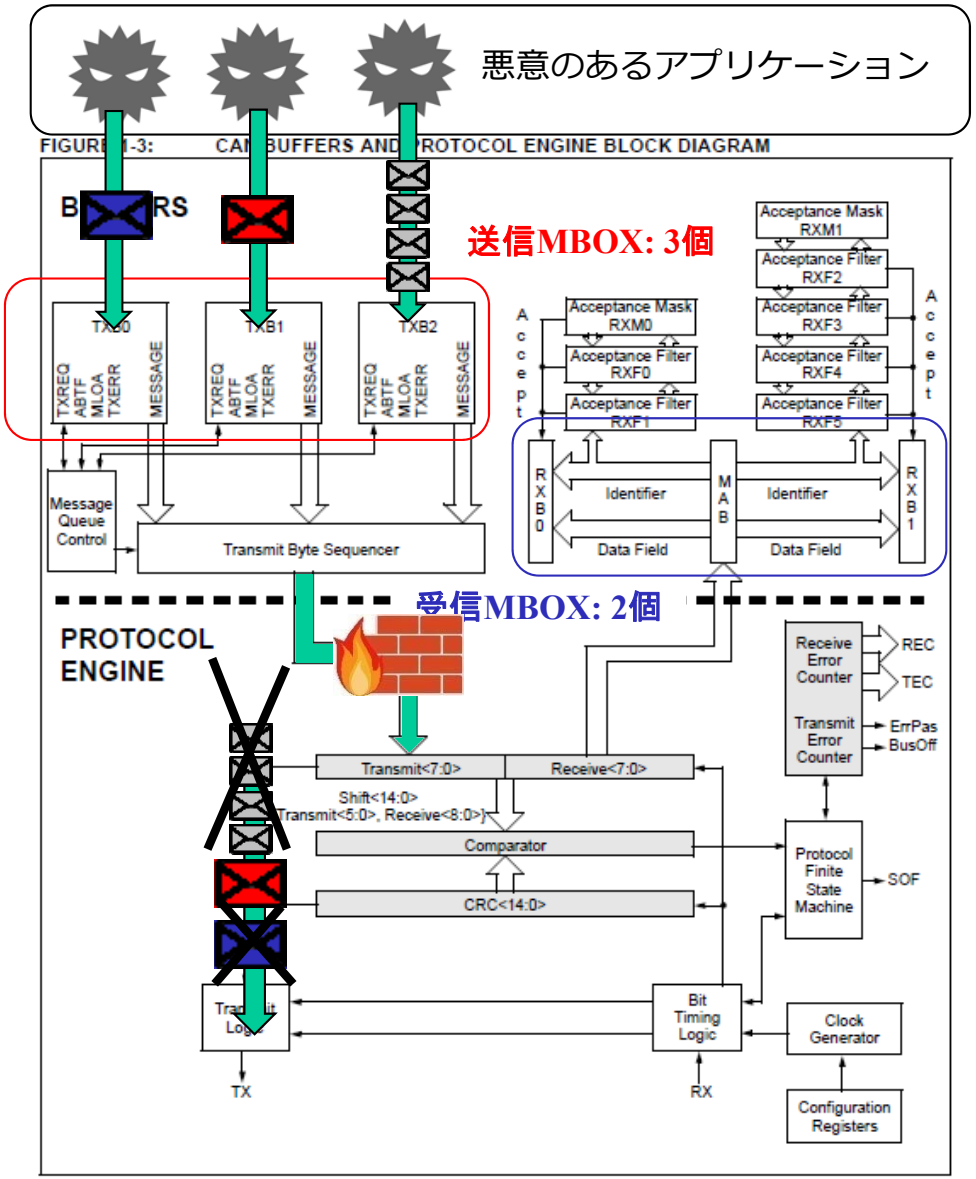




踏み台ECU対策のアイデア: CAN Disabler

- **送信前にゲートを設ける**
  - ホワイトリストベースで送信メッセージを制限
    (理由: 自動車では予め静的に各送信メッセージが仕様で規定)

- **制限内容とその効果:**
  - 1. 未使用MBOXの利用制限
    ⇒ 不正送信防止
  - 2. 送信メッセージIDを制限
    ⇒ 他のECUのなりすまし対策
  - 3. 送信頻度を制限
    ⇒ DoS対策

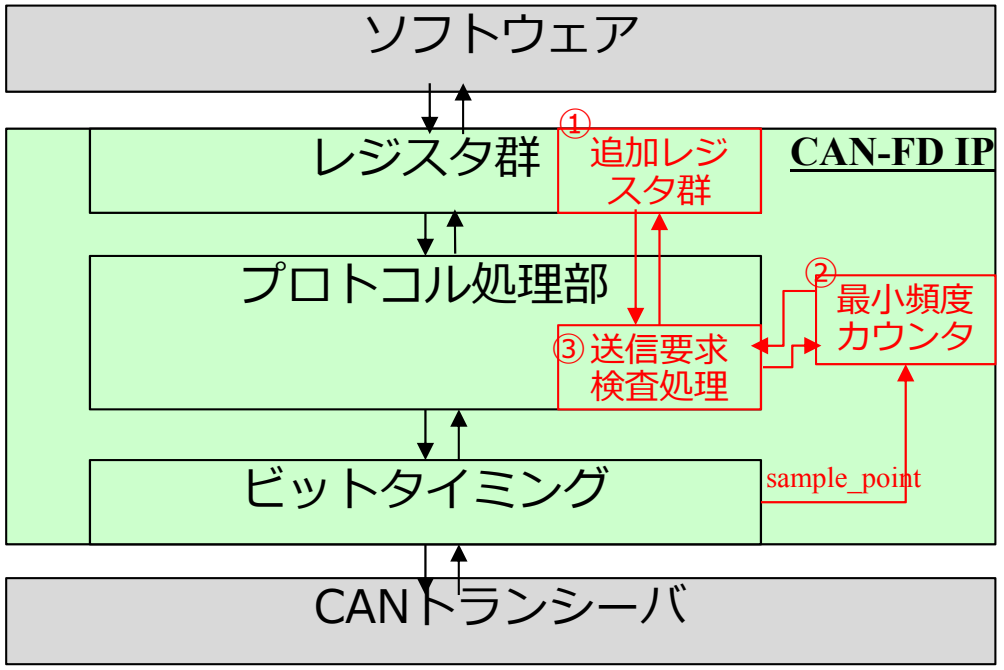


CAN Disablerの実装方法

- 既存するCAN-FDのIPに提案する**ゲート処理**と**ホワイトリスト**を追加
- ホワイトリスト(≒追加するレジスタ情報)

レジスタ名	用途
送信MBOX許可情報	各送信メールボックスに対して送信許可/禁止を設定
送信許可CAN-IDリスト	送信許可されるCAN-IDのリスト
最小送信頻度	各送信メールボックスに対して最小送信インターバル時間を設定

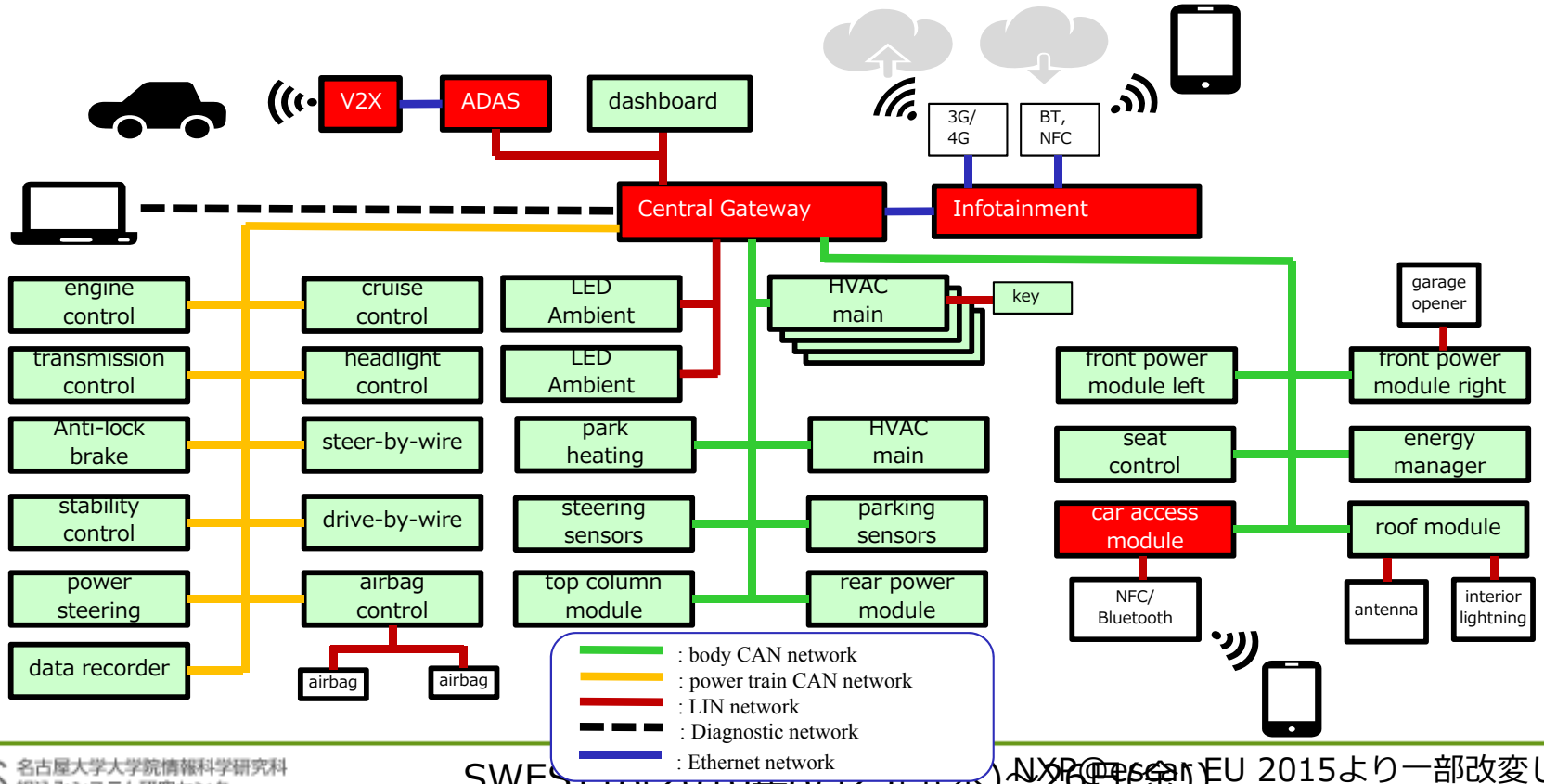
- CAN-FD IPブロックの修正箇所：
  - 1) レジスタ情報の追加
  - 2) 送信頻度カウンタ処理の追加
  - 3) ゲート処理の追加



実装上，CANとCAN-FDのいずれでもDisablerの処理は共通

CAN Disablerの適用対象ECU　※図中の背景が赤色のECU

適用例	ECU名	役割
外部ネットワークに接続するECU ⇒外部から内部への通信に適用	V2X	車車間通信用ECU
	Infortainment	ナビ/ディスプレイなどの車載情報端末
	Car access module	スマホなどと連携するECU
複数ネットワークにまたがるECU ⇒ネットワーク間の通信に適用	Central gateway	車載制御ネットワーク内のゲートウェイ
	ADAS	走行制御



NXP@escar EU 2015より一部改変して出典

2-2. 自動車のセキュリティ評価技術

自動車に適したセキュリティ技術の提案例を紹介する.

自動車のセキュリティ開発プロセス

- SAE-J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systemsでは，セキュリティのための開発プロセスが定義
  - ISO26262に適合するよう決められたプロセス全般を対象とするガイドライン
    - プロセス＝コンセプト，開発，運用を含む
  - 今後，北米自動車メーカへのECU納入時に対しては必須になると思われる

Requirements for Hardware-Protected Security for Ground Vehicle Applications

2015-06-03 WIP Standard

Define a common set of requirements for security to be implemented in hardware for ground vehicles to facilitate security enhanced applications, developing expectations for necessary functionality to achieve an ideal system for hardware protection for ground vehicle applications, including examples, but not explicitly detailing implementation requirements. **J3101**

Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

2014-01-14 WIP Standard

This recommended practice provides guidance on vehicle cybersecurity and was created based off of, and expanded on from, existing practices which are being implemented or reported in industry, government and conference papers. The best practices are intended to be flexible, pragmatic, and adaptable in their further application to the vehicle industry as well as to other cyber-physical vehicle systems (e.g., commercial and military vehicles, trucks, busses). Other proprietary cybersecurity development processes and standards may have been established to support a specific manufacturer's development processes, and may not be comprehensively represented in this document, however, information contained in this document may help refine existing in-house processes, methods, etc. This recommended practice establishes a set of high-level guiding principles for cybersecurity as it relates to cyber-physical vehicle systems. **J3061**

http://profiles.sae.org/tevees18/

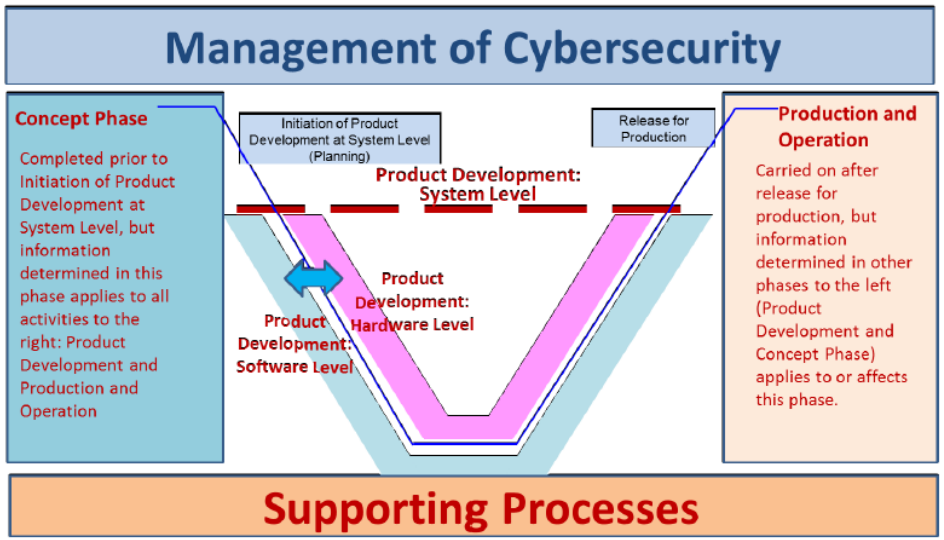


Figure 3 - Overall Cybersecurity process framework

上図はJ3061より出典

J3061におけるHW開発とSW開発

- 脆弱性分析や脆弱性テストが要求されている
  - ただし手法の詳細については言及していない

図はJ3061より出典

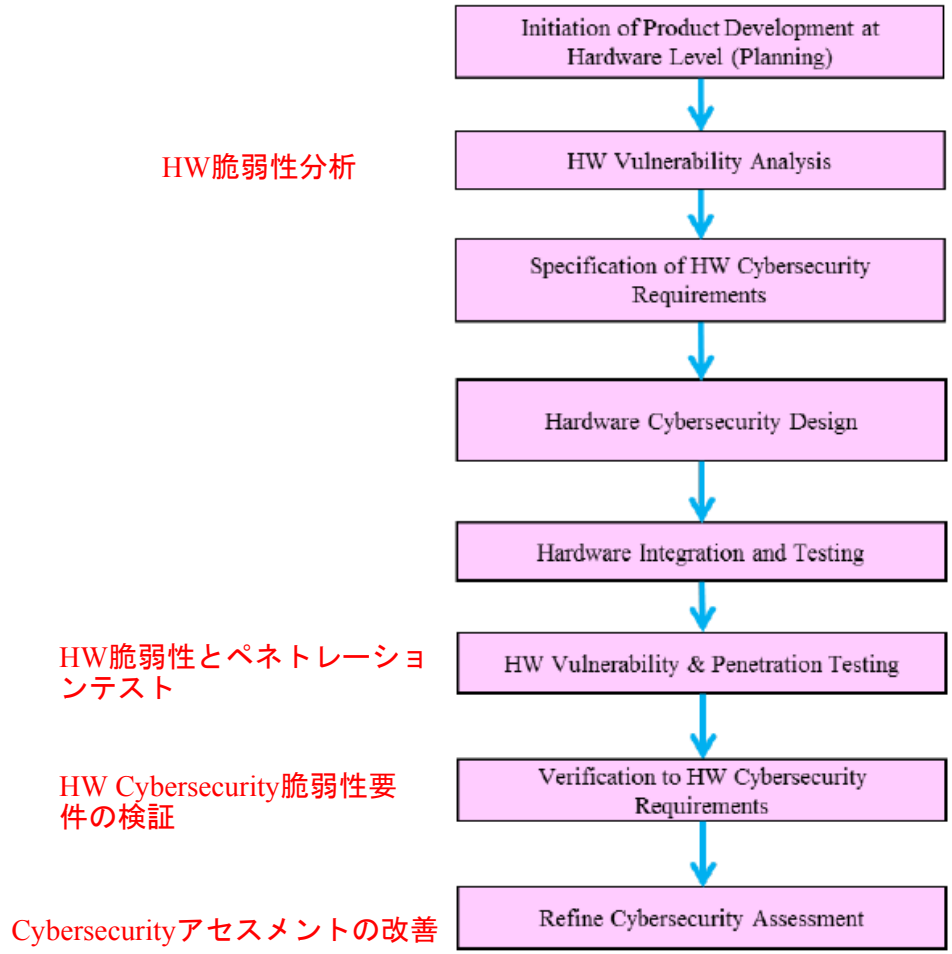


Figure 9 - Product development: hardware level

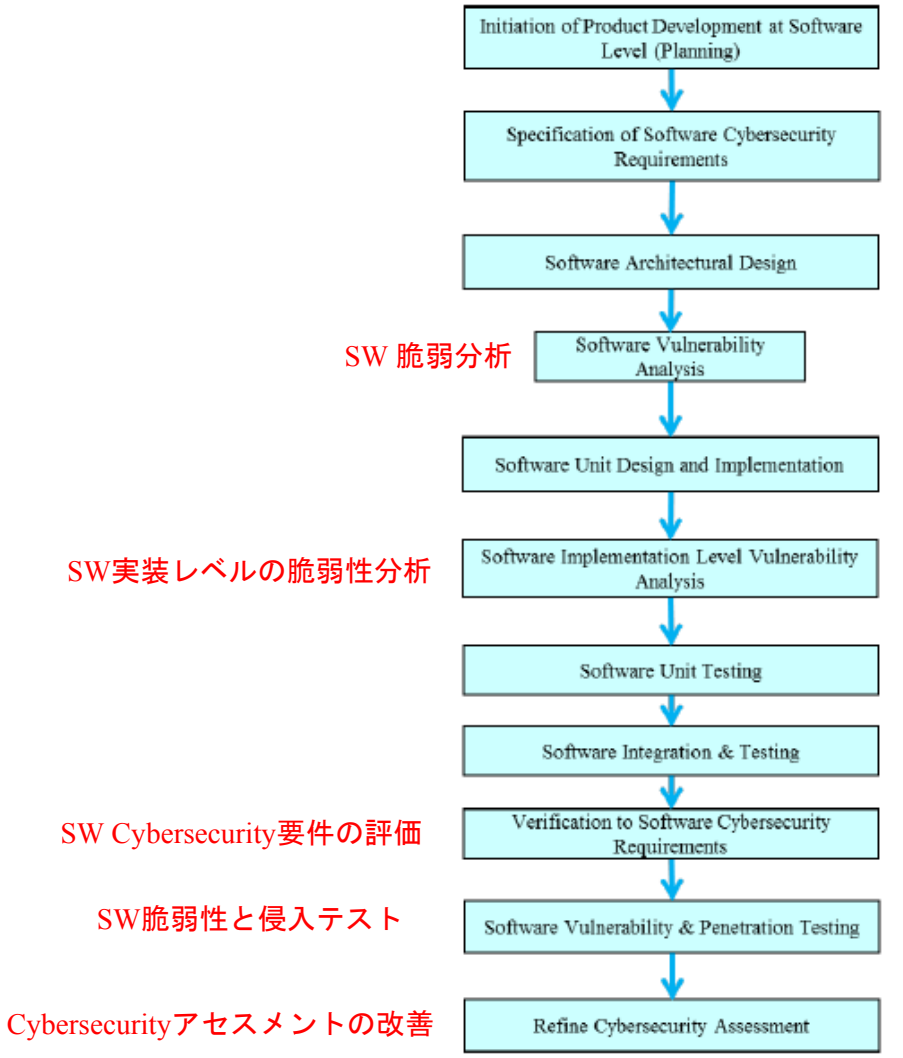


Figure 11 - Product development: software level

自動車のセキュリティ評価手法の研究

- 自動車業界でも情報セキュリティの評価手法をベースに議論
- 多くは情報セキュリティの手法が適用できると予想

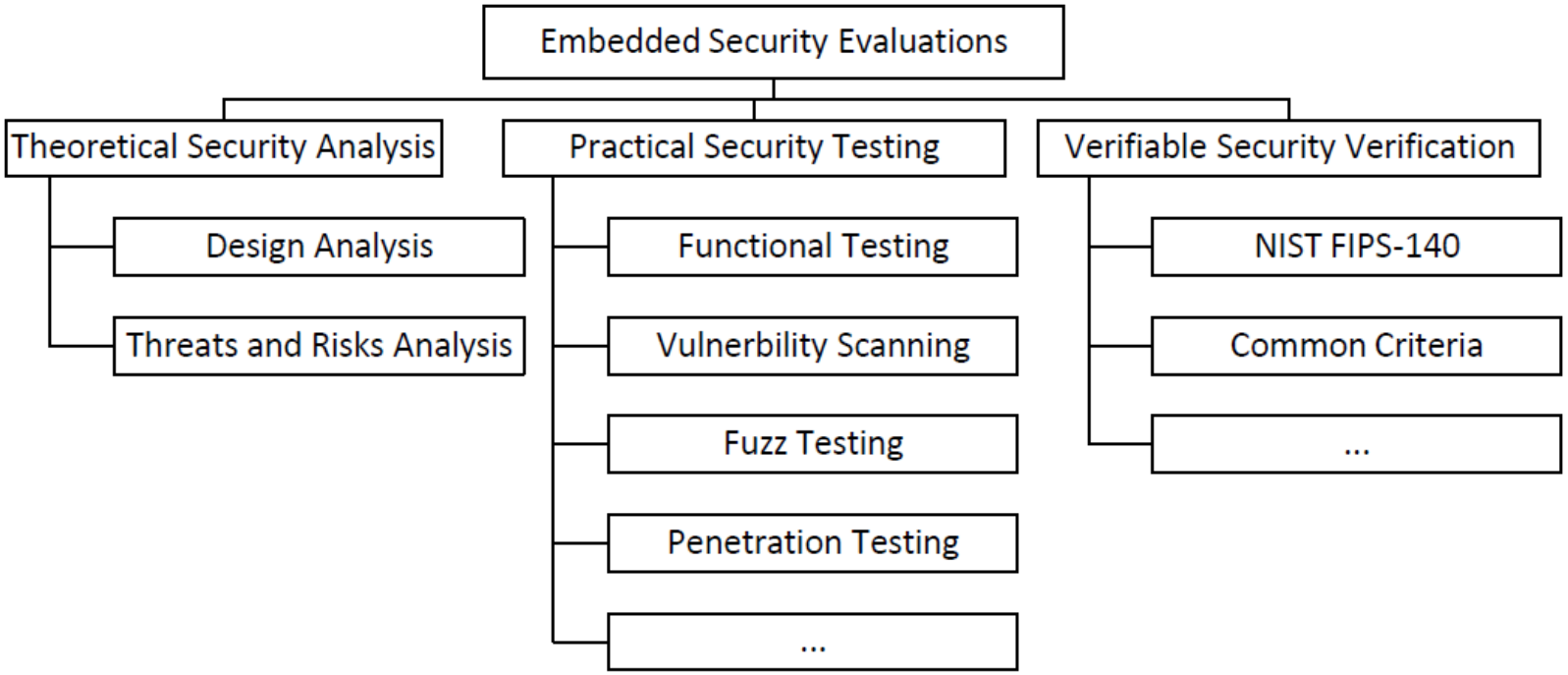


Figure 2: Overview of Embedded Security Evaluation Categories.

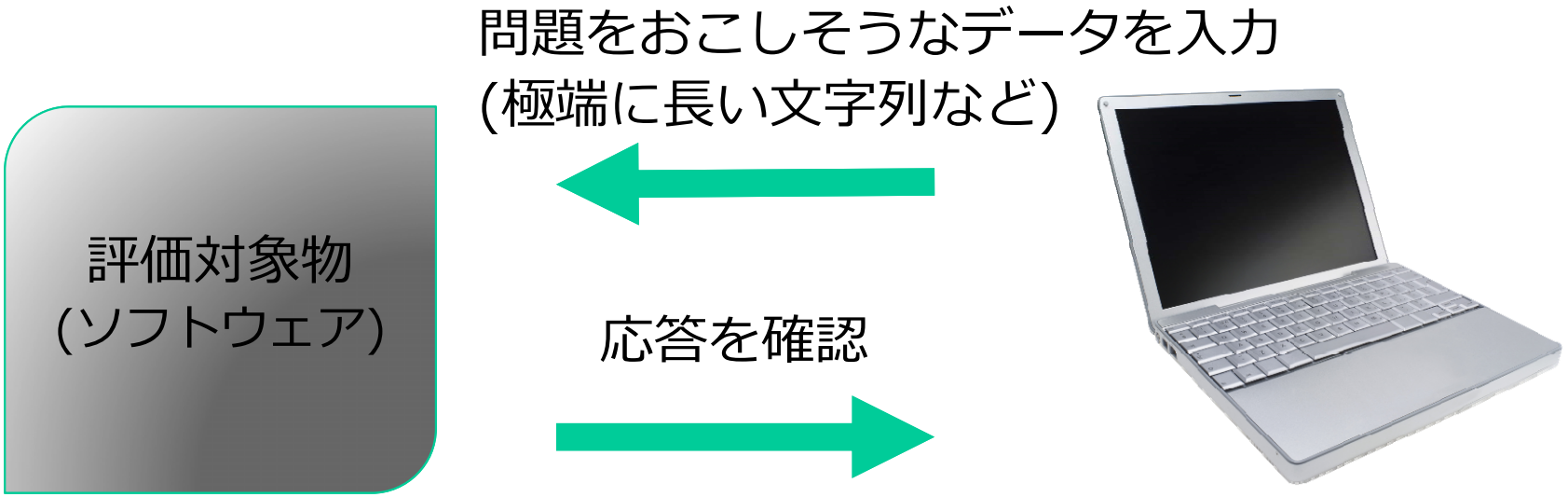
S. Bayer, T.Enderle, D.K. Oka, M. Wolf , “Security Crash Test - Practical Security Evaluations of Automotive Onboard IT Components", In Automotive - Safety & Security 2015, Stuttgart, Germany, April 21-22, 2015.

Practical Security Testingについてはシステム特有であるため,
Fuzzing Testingに着目

ファジングテストの概要

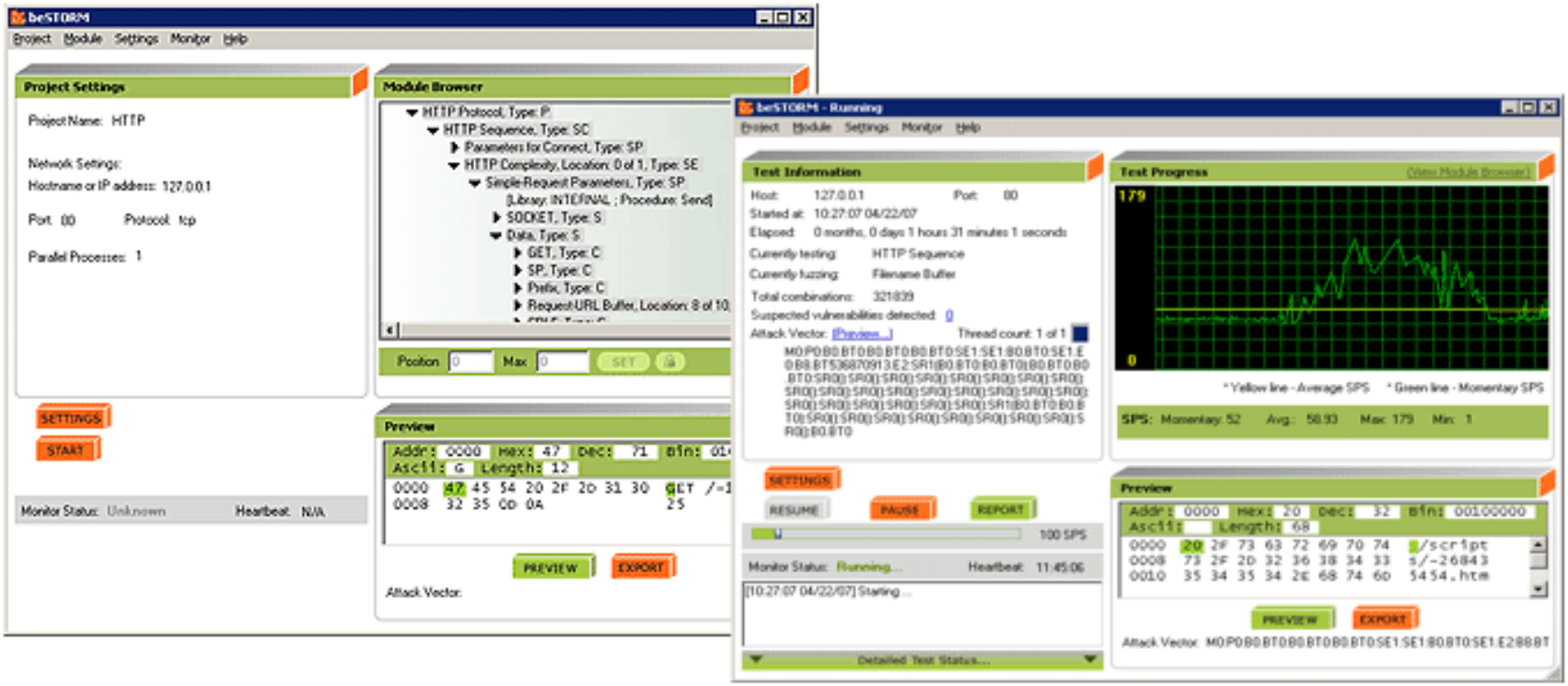
- ファジングテスト:
  - 1. 問題が起こりそうなデータ(ランダム/無効値/異常値)を入力
  - 2. 評価対象の挙動(クラッシュ/想定外の動作/異常な出力)を確認

- CAN/CAN-FDの実装上の以下の問題点を探索:
  - 無効なメッセージ長
  - 有効ではないペイロードの値やCANメッセージの送信
  - 制約されないタイミングや頻度での転送



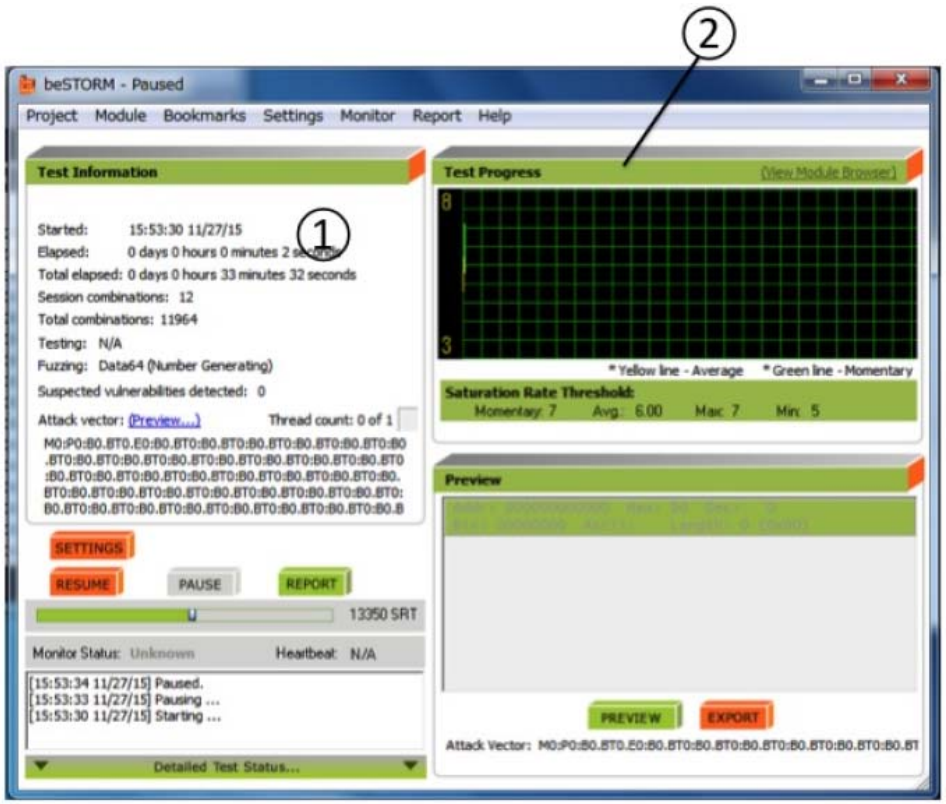
Beyond Security beSTORM

- Beyond Security社 (米国，CA, クパチーノ)
  - 日本の代理店は，アイユート社
  - CANのプロトコルにも対応可能だが，CANのインタフェース自体はユーザが作ることを想定
  - http://www.beyondsecurity.com/black-box-testing.html



beSTORMによるファジングテスト

- beSTORMはPCで動作するソフトウェア
- 実行釦を押下すると設定されたファジングデータを生成し転送
- その後，ファジングデータを全件送信し終わると結果をレポート

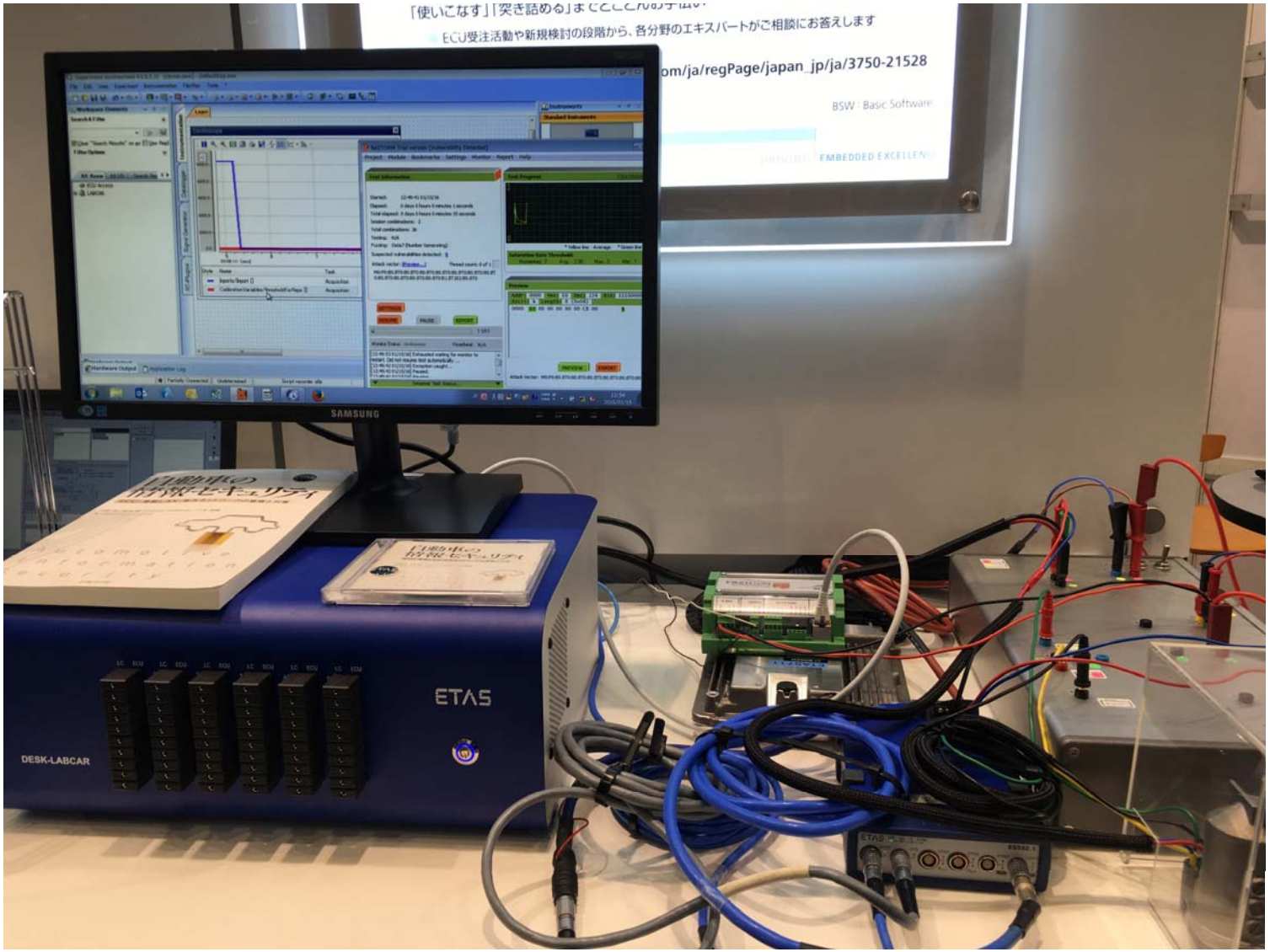


①: 全件実行時間の表示
②: 実行しているファジングの
スループットを表示

beSTORMを使えば，ファジングテストが容易に自動化できると判断

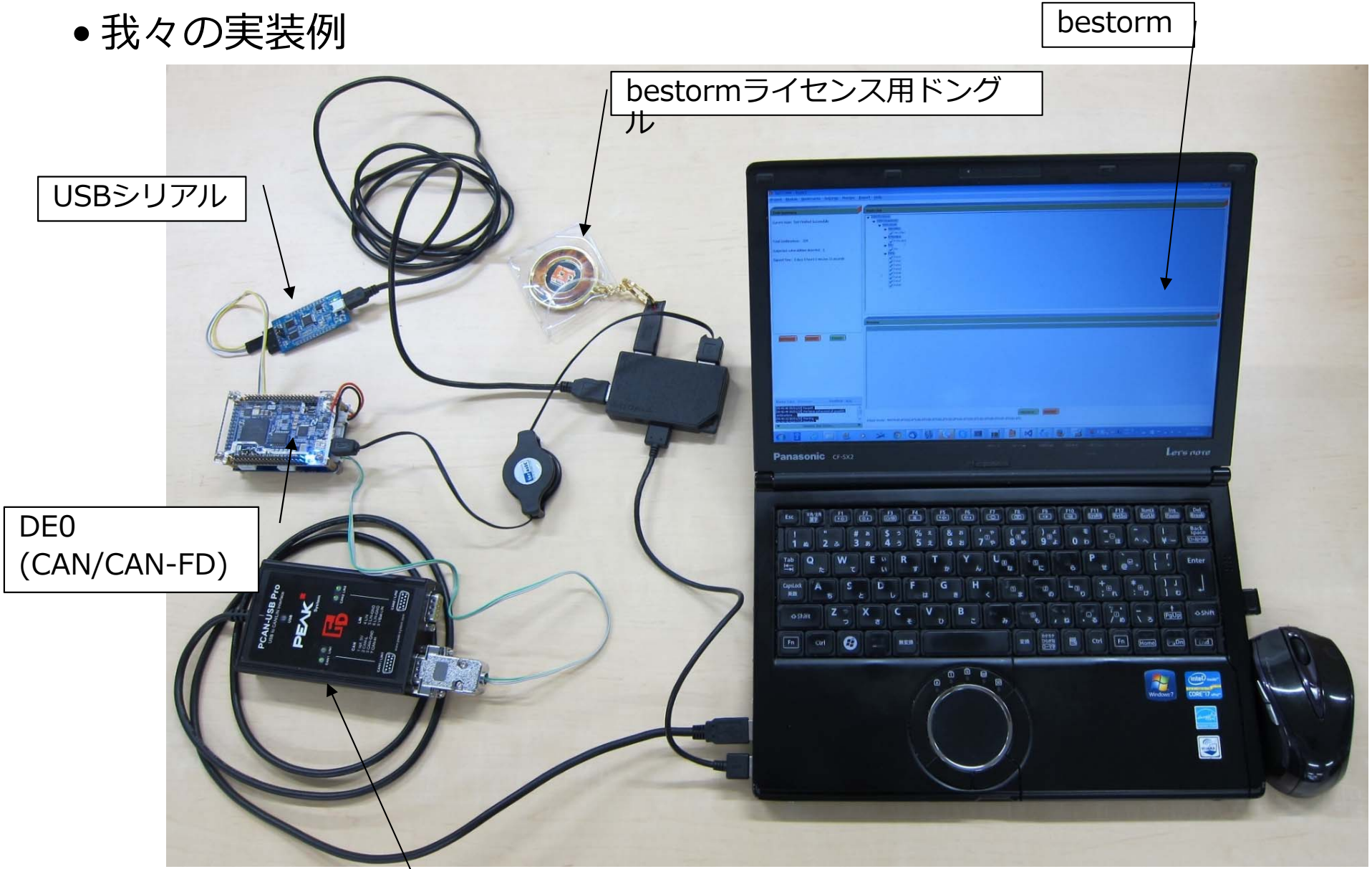
beSTORMを用いたファジングツールの実装例(1/2)

- カーエレ展2016(ETAS様)



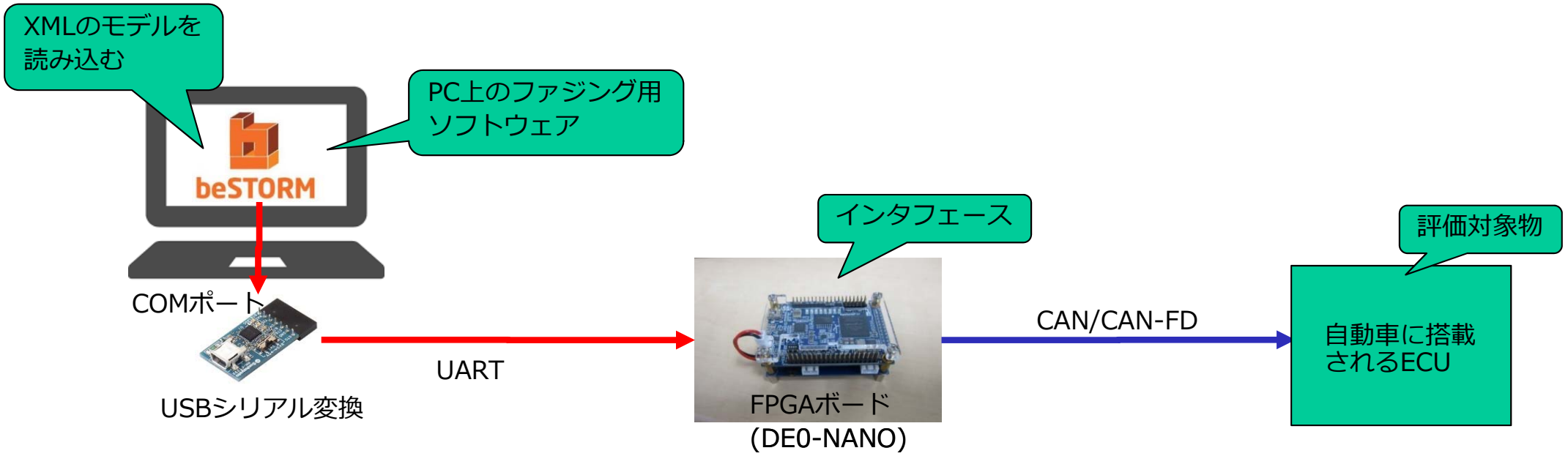
beSTORMを用いたファジングツールの実装例(2/2)

- 我々の実装例



ツールの構成

- 目的:
  - ファジングツールをCAN-FDに対応
- 構成要素と処理フロー:
  - 1. beSTORMで生成されたデータをCOMポート経由で転送(赤線部)
  - 2. インタフェースでは受信したデータをCAN/CAN-FDへ転送(青線部)
    - インタフェースにはFPGAボード”DE0-NANO”を使用し，CAN-FDのIPを実装

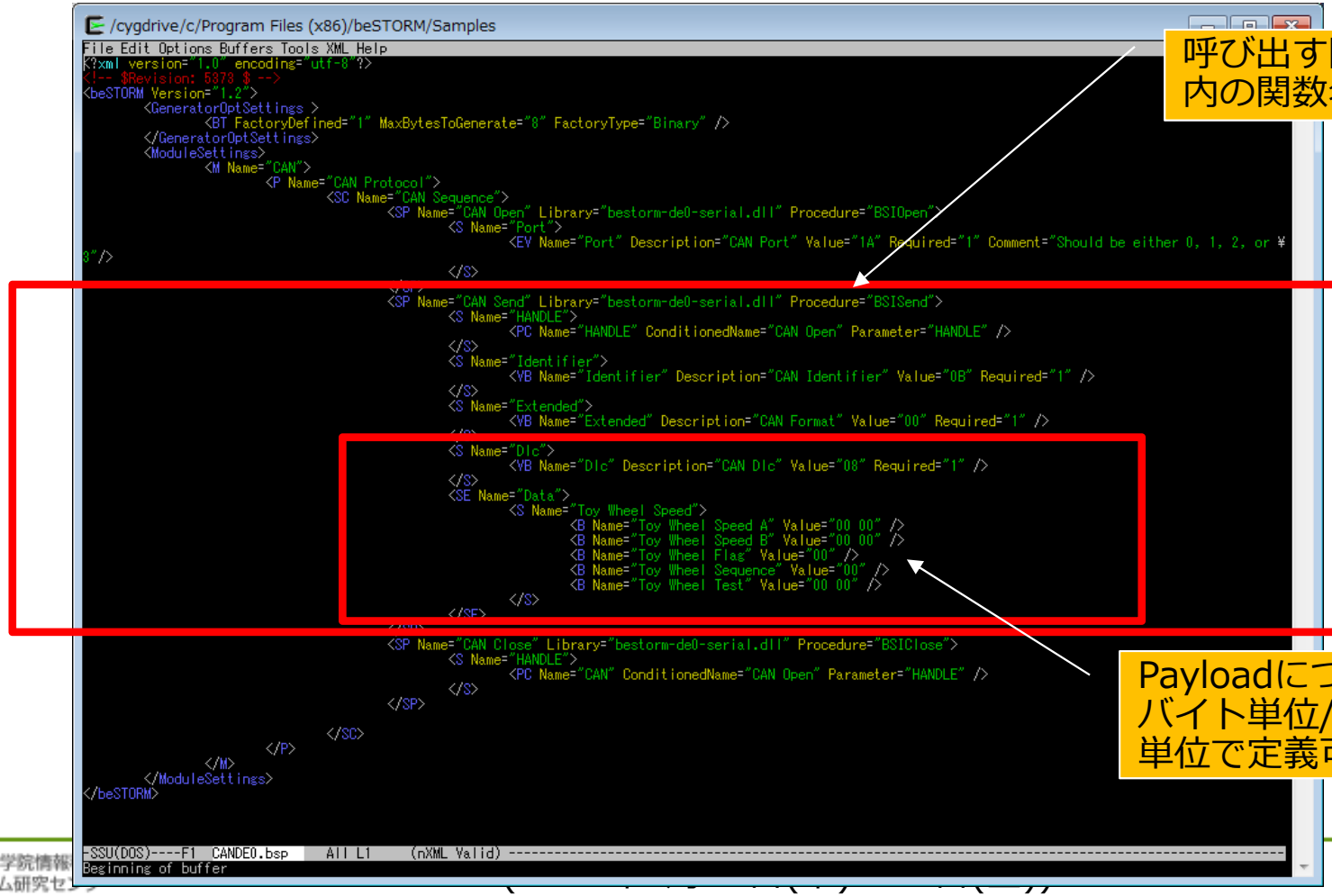


beSTORMが読み込むモデル(XML記述)

- **例) 1つのCANメッセージに対するモデル**

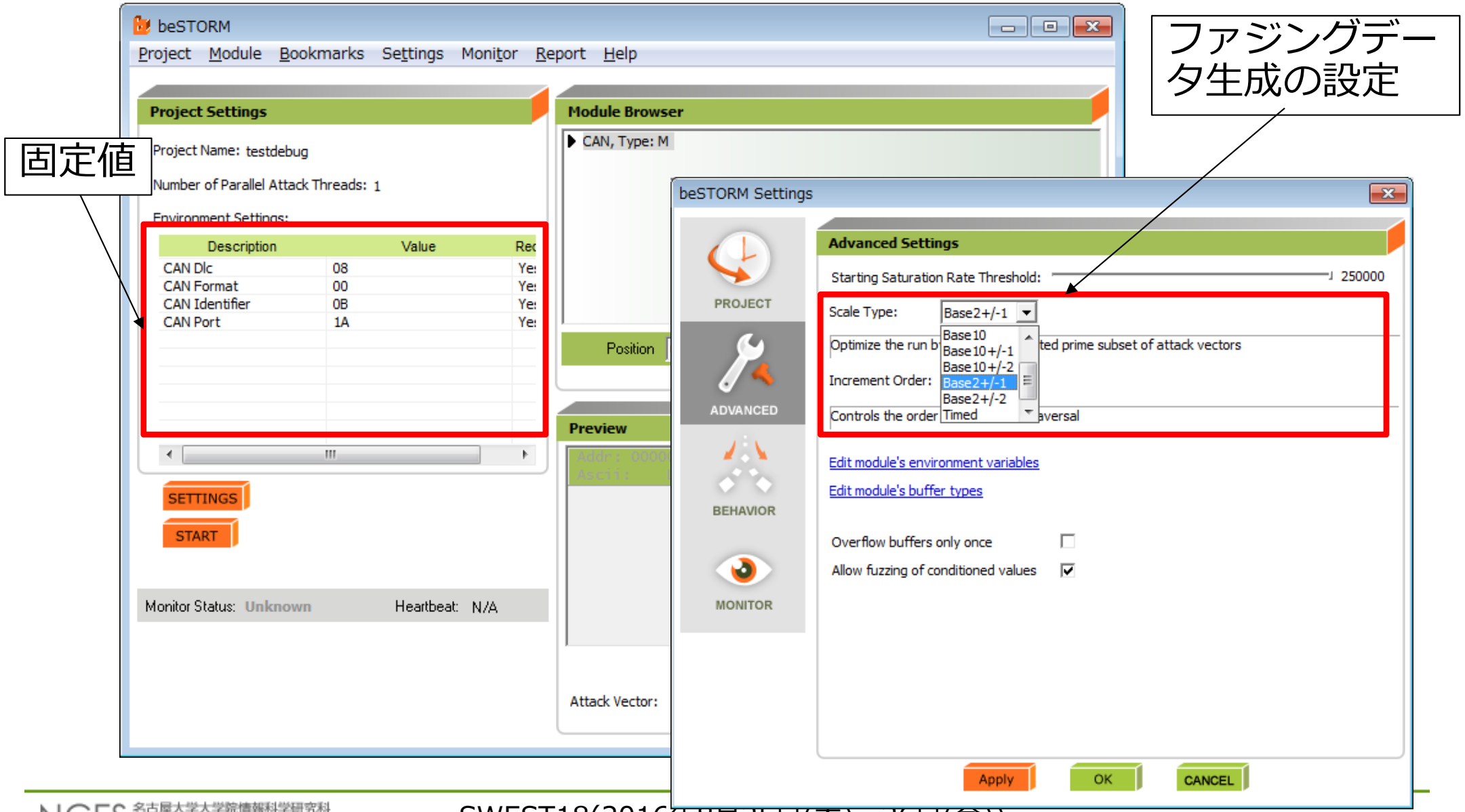
  (1)CAN-ID, (2)Dlc, (3) Extended, (4) Data(Payload)のタグを追加

  - (1)CAN-ID, (2)Dlc, (3) Extendedは，固定値として扱う
  - (4) Dataのみを任意のデータを生成させる



ファズデータ生成の設定

- 生成するデータについては，beSTORMの設定でステップ値(粒度)を変更可能



CAN-FD/CANで実行した結果

- beSTORMとDE0-NANOが連携し，CANメッセージの送信を確認
  - beSTORM実行後，生成したテストデータ数を表示
  - 異常が発生する場合には，エラーレポートが都度表示

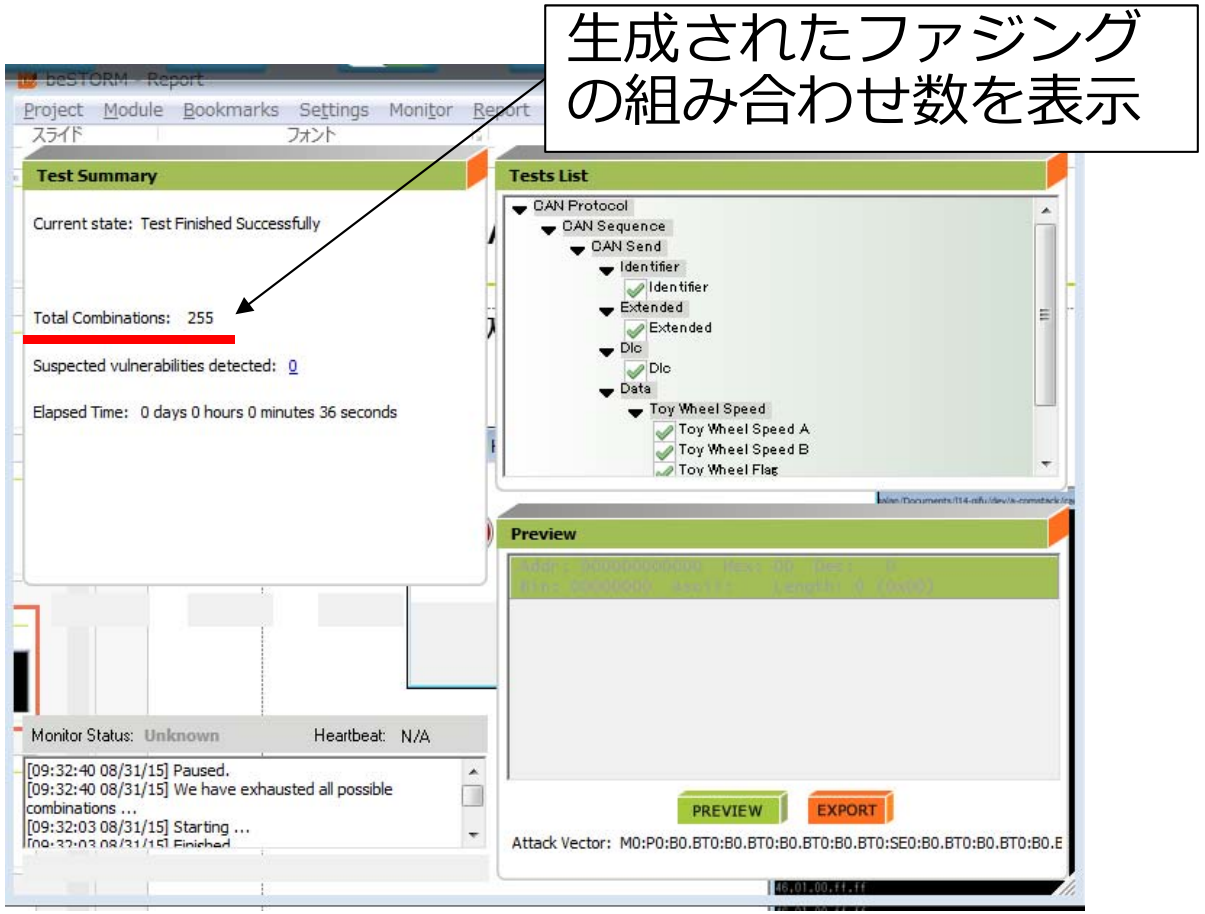
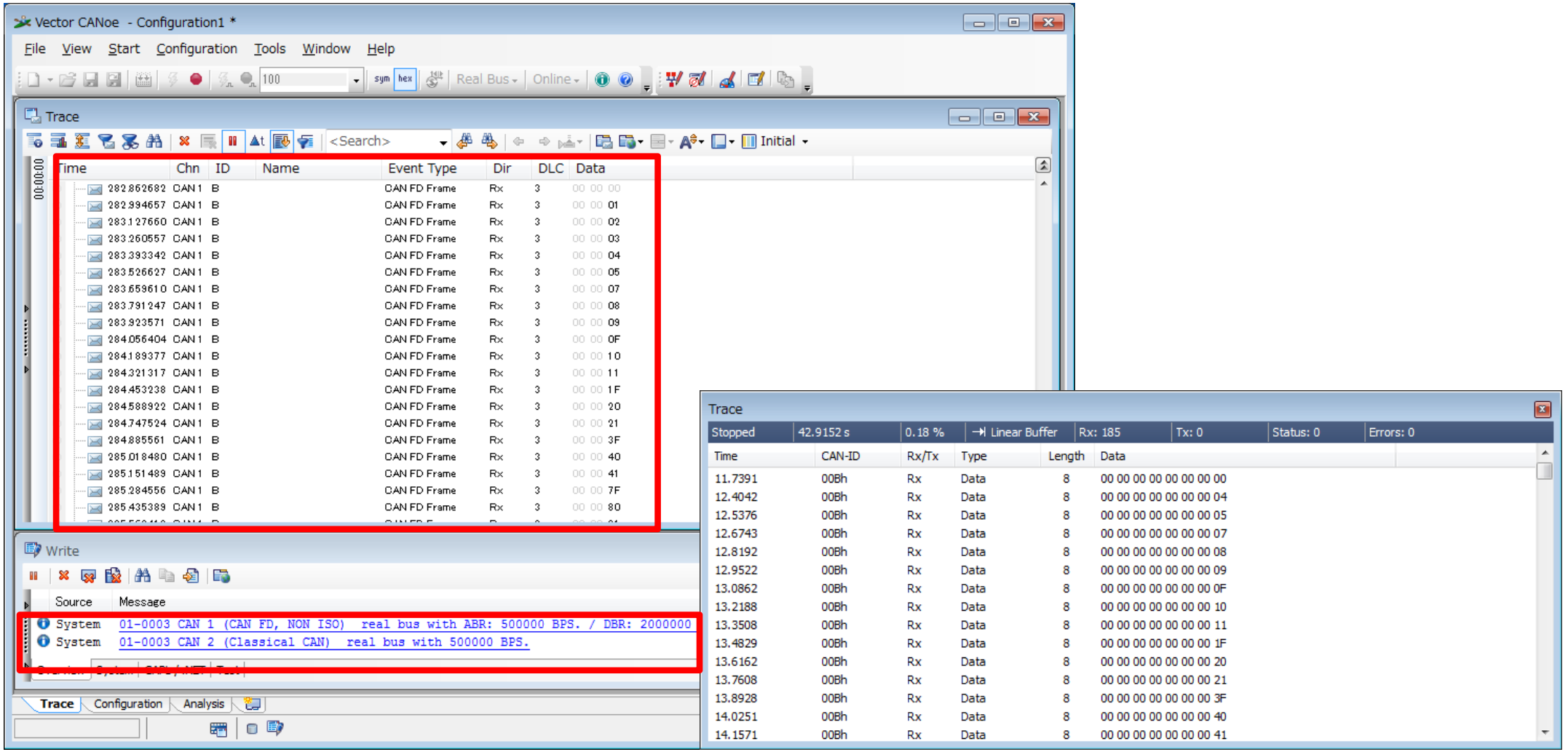


図. bestorm側の実行結果

CAN-FD/CANで実行した結果

- 左がCAN-FDの場合，右がCANの場合



3. 最後に

まとめと今後の展開

- まとめ
  - 自動車のセキュリティに対する脅威事例が増えている
  - 車載制御システムでは，安全性を侵害する脅威の対策が必要
    - 特に，車載制御ネットワークCANでのなりすましなど
  - 我々は，自動車のセキュリティ強化に対する対策技術の提案と評価手法の検討を実施
    - 特に，近い将来において実用可能となる技術を提案
  - 自動車の対策技術としては情報セキュリティとは異なるアプローチもありえるため，組込み技術者が優位に立てる場面も多いかも？
    - ただし，現在玉石混合しており，有益な活動や提案が求められていることも事実！

- 今後の展開
  - 対策技術の拡充
  - 評価手法の拡充