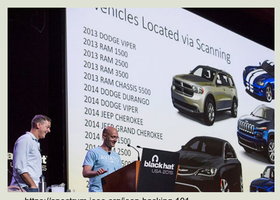
自動車のサイバーセキュリティ強化技術

名古屋大学大学院情報学研究科附属組込みシステム研究センター　倉地　亮

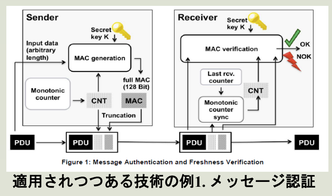
Center for Embedded Computing Systems, Graduate School of Informatics, Nagoya University

1.車載制御システムとセキュリティ

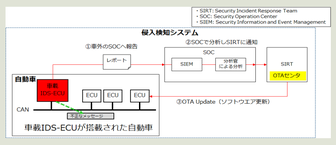
・現状，様々な機能を搭載すべく車載電子制御システムが発展
・今後は外部の機器と連携するアプリケーションが想定
・2010年以降，車載制御システムに対する脅威事例が報告
　→ プリウス (2013)，Jeep(2015)，BMW(2020)など
・2019年以降，セキュリティ強化がなされつつある.
・現在では一部の車両の型式認証にサイバーセキュリティ強化が必須



https://spectrum.ieee.org/jeep-hacking-101



適用されつつある技術の例1. メッセージ認証



適用されつつある技術の例2. 侵入検知システム

国際基準　UN-R155
（サイバーセキュリティ）

国際基準　UN-R156
（ソフトウェアアップデート）

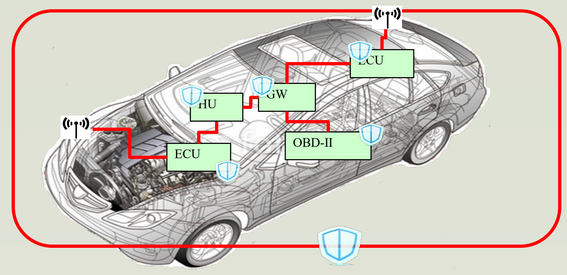
脅威事例
（2010～）
→ セキュリティ強化
(2019～)
→ 国際基準と法制度化
（2022～）

2.自動車のセキュリティ強化の課題

・ミッションクリティカルな制御システムの保護が重要
・車載特有の要件や制約が多数存在
・**民生技術をベースに，車載要件を満たすセキュリティ対策が必要**

セキュアな通信が必要な理由

分散制御システムの安全性
→　メッセージ認証技術
→　ECUと呼ばれるコンピュータの認証
ECUはクリティカルな信号を交換
→　ブレーキ，トルク，シフトポジション
悪意のある情報/信号が安全性を脅かす



セキュリティゴール

車両安全
→　運転者や乗員の安全性を確保
クリティカルな機能の保護
→　制御のための信号や通信メッセージの保護
知的財産権の保護
→　ユーザー/OEM/サプライヤの知財権

※現状，攻撃を検出することが最優先

車載制御ネットワークの制約

コスト要件
→　狭帯域，低い処理コスト，省メモリ性
リアルタイム性
→　暗号/復号によるジッタの増減が懸念
マイグレーション可能性
→　既存ECU/アプリケーションの実現性
→　特にHWの変更規模が少ないこと

3.セキュリティ強化技術の位置付け

・国際基準では，自動車のライフサイクルに合わせたプロセス全体のサイバーセキュリティ活動が要求
　– 導出されたリスクが十分に低減できていることの論証が必要
　– テスト工程では，要求が確かに実装され，論証が不十分な点が検証されていること

➡ セキュリティ強化技術として攻撃手法，設計手法，評価手法が要求

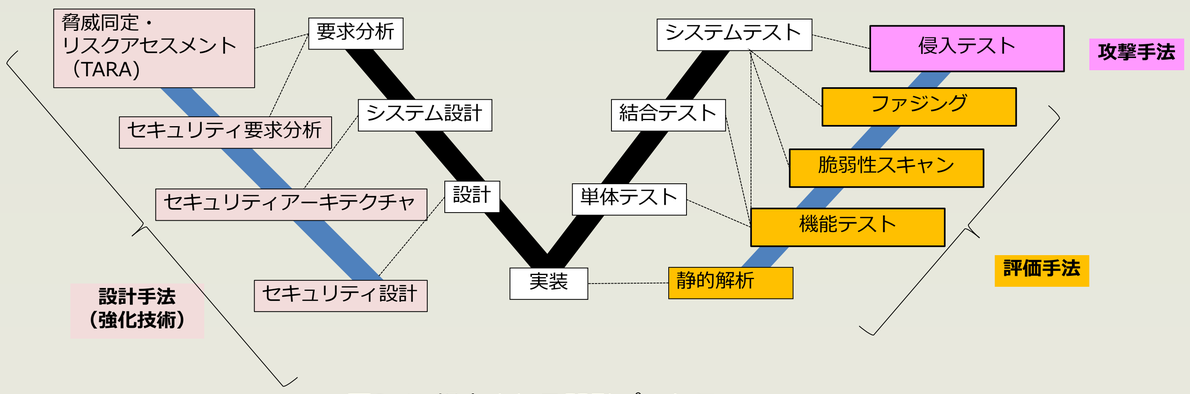


図3-1. 規定される開発プロセス

4.セキュリティ強化技術の例

•提案手法1) 集中型セキュリティ監視機構
　• Centralized Authentication System in CAN (CaCAN)
　　• 車載制御システム上での集中型セキュリティ監視機構
•提案手法2) マルウェア監視
　• ECU上でのマルウェアの閉じ込め手法
　• エラーフレーム監視: 車載制御システム上の異常監視技術

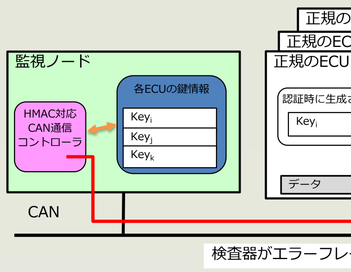


図4-1. CaCANの実装環境

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

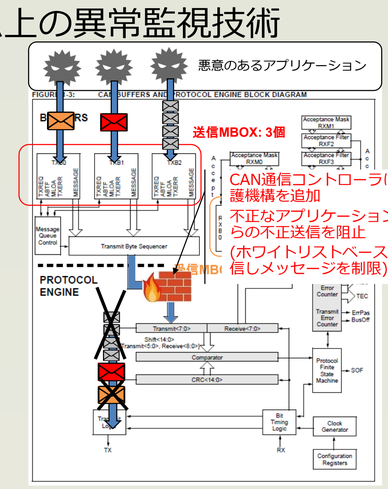


図4-2. CAN Disablerの例

Ryo Kurachi, T.David Pyun, Shinya Honda, Hiroaki Takada, Hiroshi Ueda, Satoshi Horihata, "CAN Disabler: Hardware-based Prevention method of Unauthorized Transmission in CAN and CAN-FD networks", Embedded Security in Cars Conference (escar US 2016), pp.1-7, Detroit, Jun 2016.

5. セキュリティ評価手法の例

•提案手法1) HILSを用いたセキュリティ評価手法
　• CANやCAN-FDに対する評価手法を検討
•提案手法2) 実車両の解析手法と評価手法
　• 実車両に対する評価手法についても検討(例: UDSなどの通信)
　• 出荷前の検査を効率的に行う方法を検討

図5-1. HILSを用いた評価環境

図5-2. HILSを用いた評価環境の実装例

藤倉俊幸，倉地亮，車載ネットワークセキュリティ検証環境の開発，自動車技術会2018年春季大会学術講演会，May 2018

図5-3. UDSのセキュリティアクセス評価の例

表 1:セキュリティアクセス機能 評価結果

		車両A	車両B	車両C
1. 評価対象 CAN ID数		21	41	22
2. 評価対象 セッションタイプ数		66	55	79
3. 評価対象 セキュリティアクセス機能総数		75 (19)	26 (16)	31 (17)
4. シード値の長さ	4-1. 3-4byte	53 (18)	8 (5)	12 (7)
	4-2. 1-2byte	1 (1)	3 (2)	1 (1)
5. シード値に規則性が存在	5-1. 毎回同じシード値	3 (1)	3 (1)	5 (3)
	5-2. 複数回同じシード値	20 (14)	0 (0)	7 (7)
	5-3. 規則性あり	9 (2)	8 (5)	0 (0)

表 2:ブルートフォース攻撃の成立までに要した平均所要時間及び試行回数

平均試行回数	2,841.2万回
平均所要時間	47.3時間
最短所要時間	0.5時間
最長所要時間	108.8時間

R. Kurachi *et al.*, "Evaluation of Security Access Service in Automotive Diagnostic Communication," *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 2019

6. 現在の取り組み

•1) 車載ECUのアクセス制御やデータセキュリティ(強化手法と評価手法)
•2) OTA Update技術
•3) セキュリティ強化を考慮したリアルタイム性保証手法

7.今後の計画

•将来システムにおけるセキュリティ強化手法/評価手法の提案
•直近の現実的な課題における解決手段の提案