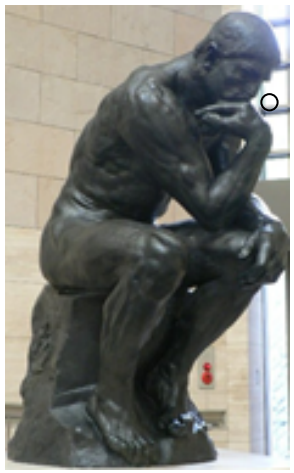
セキュアエレメントを基点とした車載制御システムの保護
–要素技術の整理と考察–

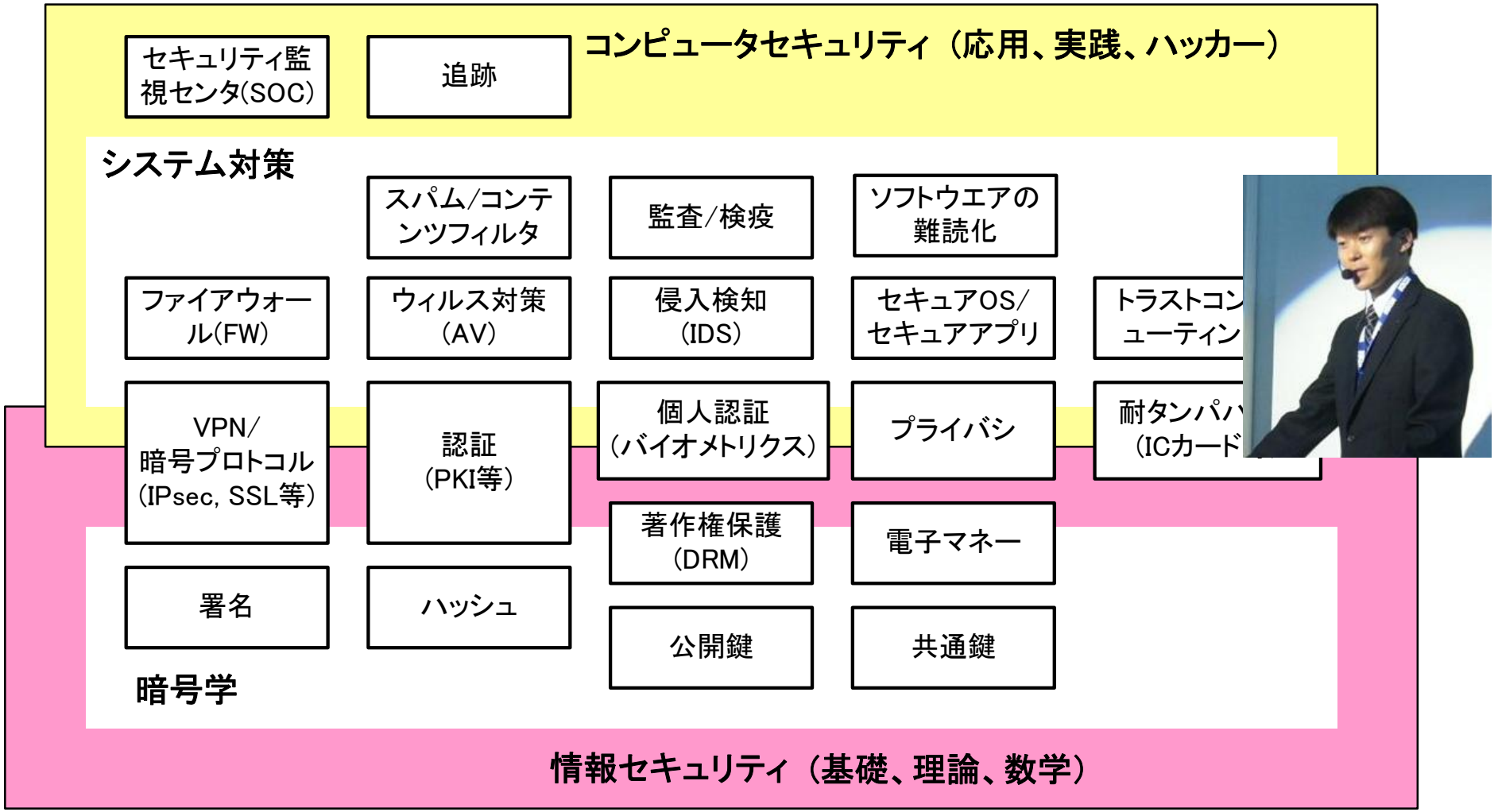
KDDI研究所　竹森敬祐



ハッカー視点で狙いどころを考え、セキュアエレメントの導入で、根本解決を目指す。

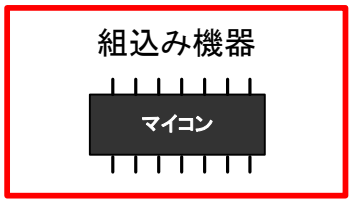
- ◆ セキュリティとは
- ◆ インシデントの収集・分析
- ◆ 対策に関する基礎技術
- ◆ 鍵管理の一例
- ◆ CANパケット認証、ECUのセキュアブート
- ◆ リモートリプログラミング

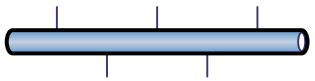
セキュリティの全体像 2006年作成図

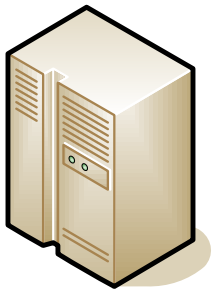


注）セキュリティの全てのテーマを包含しきれていない。分野の名称も定まっていないものもあります

システムの狙いどころ：2面ある対策技術







④近距離通信　　⑤インターネット通信

②連携機器／アプリ　　①組込み機器　　③クラウド／サーバ

① 組込み機器	コード／メモリ／漏洩電磁波などを解析する。
② 連携機器／アプリ	コード／メモリ／ログ／通信などを解析する。
③ クラウド／サーバ	通信／認証サービス／OS・サービスを解析する。
④ 近距離通信	電波／バスを流れるパケットを解析する。
⑤ インターネット通信	機器から発信されるパケットを解析する。

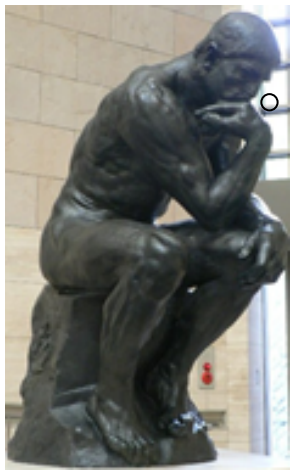
適切な技術を、適切に組み上げる必要がある。

情報セキュリティ　　コンピュータセキュリティ

KDDI R&D LABS

セキュアエレメントを基点とした車載制御システムの保護
–要素技術の整理と考察–

KDDI研究所　竹森敬祐



ハッカー視点で狙いどころを考え、セキュアエレメントの導入で、根本解決を目指す。

- セキュリティとは
- **インシデントの収集・分析**
- 対策に関する基礎技術
- 鍵管理の一例
- CANパケット認証、ECUのセキュアブート
- リモートリプログラミング

車載システムへのローカル攻撃

- 車載システムの不正改造(2013/8 DEFCON)
  - PCを制御システムに接続して、不正な制御を行っている。
    ⇒ ブレーキ、ハンドル、速度メータ、ガソリンメータ

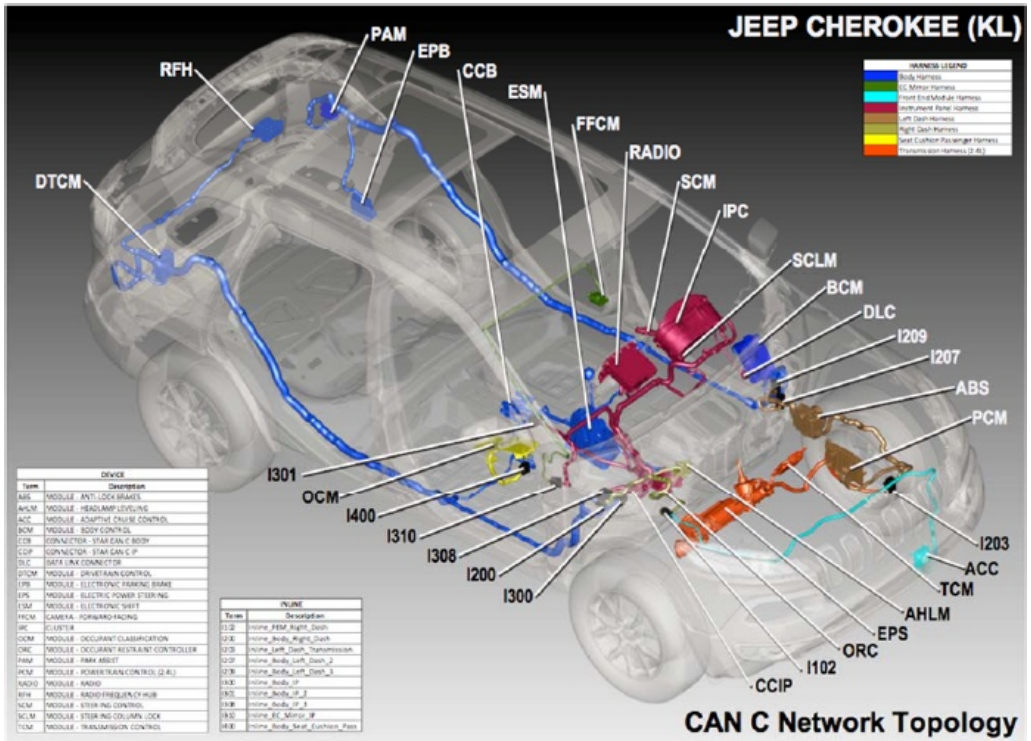
http://drive-love.jp/drivpedia/2013/08/post-19.html

KDDI R&D LABS

車載システムへのリモート攻撃／システム構成

- A Survey of Remote Automotive Attack Surface
  - 車載システムに対するリモート攻撃の可能性を解析。
  - 車載システムのネットワーク構成を車メーカ毎に解析・公開。

+ 脆弱
- 堅牢



Car	Attack Surface	Network Architecture	Cyber Physical
2014 Audi A8	++	--	+
2014 Honda Accord LX	-	+	+
2014 Infiniti Q50	++	+	+
2010 Infiniti G37	-	++	+
2014 Jeep Cherokee	++	++	++
2014 Dodge Ram 3500	++	++	--
2014 Chrysler 300	++	-	++
2014 Dodge Viper	++	-	--
2015 Cadillac Escalade	++	+	+
2006 Ford Fusion	--	--	--
2014 Ford Fusion	++	-	++
2014 BMW 3 series	++	--	+
2014 BMW X3	++	--	++
2014 BMW i12	++	--	+
2014 Range Rover Evoque	++	-	++
2010 Range Rover Sport	-	--	-
2006 Range Rover Sport	-	--	-
2014 Toyota Prius	+	+	++
2010 Toyota Prius	+	+	++
2006 Toyota Prius	-	--	--

http://ja.scribd.com/doc/236073361/Survey-of-Remote-Attack-Surfaces

KDDI R&D LABS

ドアのリモート解除 2015年2月

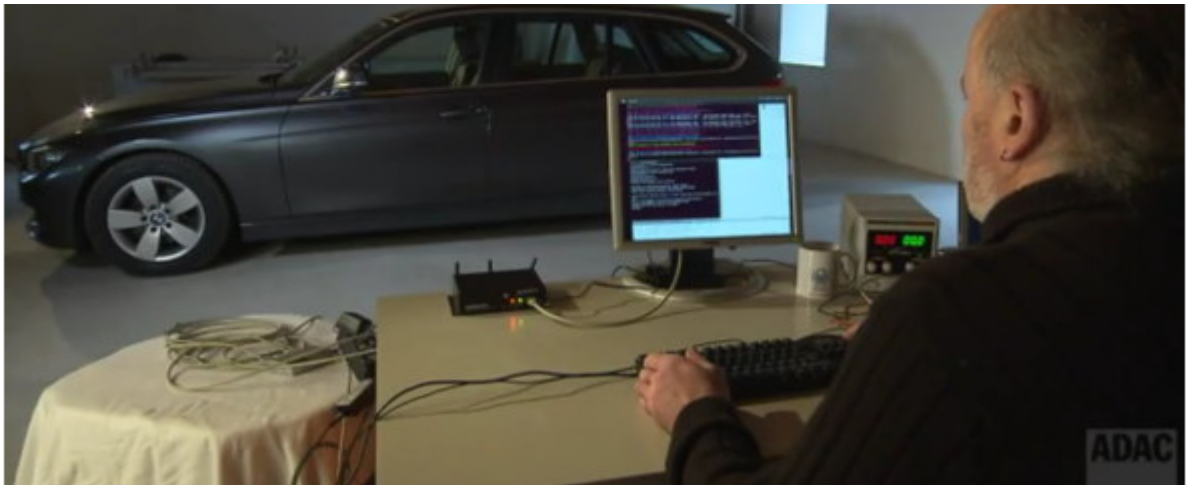
- 脆弱性：スマホからドアロック解除機能に脆弱性があり、第三者が開錠できる。
- 問題点：スマホ・車載機間が平文通信(http)のため、セッションハイジャックされる。

独BMW車に標準装備されているオンラインサービスに、ドアロック解除などの操作を他人ができてしまう脆弱性が見つかり、BMW Groupは設定を変更してこの問題に対処したことを明らかにした。

http://www.itmedia.co.jp/enterprise/articles/1502/03/news042.html

ドイツ自動車協会（ADAC）やBMWによると、この問題は、スマートフォンを使ってドアロックやエアコンなどの操作ができるオンライン機能の「コネクテッド・ドライブ」に存在していた。ADACの専門家が検証した結果、携帯電話ネットワークを通じてデータを転送する仕組みに脆弱性があり、スマートフォンを使って他人が痕跡を残さずに車のドアロックを解除できてしまうことが分かったという。

BMWは、HTTPS接続を使って車との通信を暗号化することによってこの問題に対処し、1月30日までにコネクテッド・ドライブ経由で修正を済ませたと説明。実際に問題が悪用されたり、悪用しようとしたりする動きは確認されていないとしている。



KDDI R&D LABS

リモートからCANへの不正パケットの注入 2015年7月

- 攻撃の概要
  - リモートからインフォ端末へ侵入し、CANへ不正パケットを注入する。
- 問題点
  - インフォ端末がインターネットからアクセス可能なグローバルIPを持つこと。
  - 外部からアクセス可能な通信サービス（Port）が開いていること。
  - インフォ端末からCANへパケットWriteできること。

車の遠隔操作防止 米で１４０万台リコール

7月25日 5時31分

NHKニュース

http://www.itmedia.co.jp/enterprise/articles/1507/22/news060.html
http://www3.nhk.or.jp/news/html/20150725/k10010165561000.html

クライスラーのブランドで知られるアメリカの自動車メーカーＦＣＡＵＳはハッカーの攻撃で車が遠隔操作されるおそれがあるとして１４０万台をリコールすると発表しました。自動車メーカーがハッカー対策でリコールを行うのは初めてです。

これはクライスラーのブランドで知られるアメリカの自動車メーカー、ＦＣＡＵＳが２４日発表したものです。それによりますとハッカーによる遠隔操作を防ぐためソフトウェアをアップデートする必要があるとしてアメリカ国内でジープなど１４０万台をリコールするとしています。メーカー

車載システムの脆弱性による米国でのリコール、USBメモリーで更新プログラムを配布

http://security.srad.jp/story/15/07/25/1731206/

ウイルス感染メモリ?
USBの形をしたｷｰﾎﾞｰﾄﾞ?

理由

USBメモリでプログラムを配る!

禁じ手

ローカル攻撃／リモート攻撃

■ ローカル攻撃
- ◆ 攻撃者は所有者自身である場合、手元環境で何でもできる。
- ◆ 過失でウイルスに手動感染した場合、デバイスを遠隔制御される。

⇒ 影響は、攻撃を受けた機器に限定される。

⇒ 自己責任

⇒「実験室による解析が成功」⇒記事化リスクを受容できるか?!

受容しなければきりがない。但し、ｴﾊﾞﾝｼﾞｪﾘｽﾄを作り上げ安心を届ける体制を。

■ リモート攻撃
- ◆ 所有者の意図とは関係なく、攻撃が自動的に決まる。
- ◆ 機器に潜む共通な脆弱性を突き、遠隔からの攻撃を受ける。

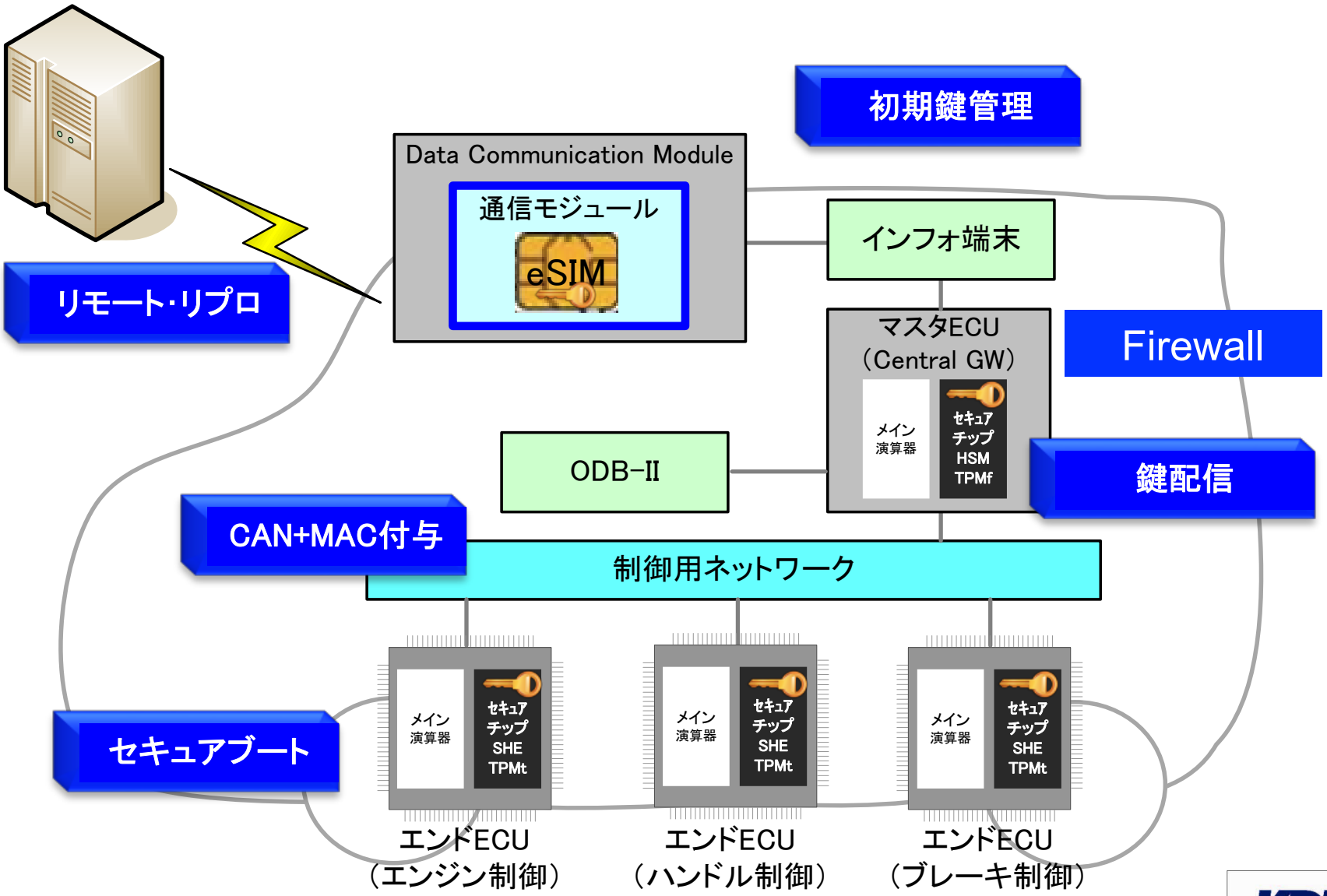
⇒ 影響は、他人の車（全車）に及ぶ。

⇒ 提供者責任（リコール）

Security by Designの考えで、抜け・漏れなく、根本解決を目指してください。

KDDI R&D LABS

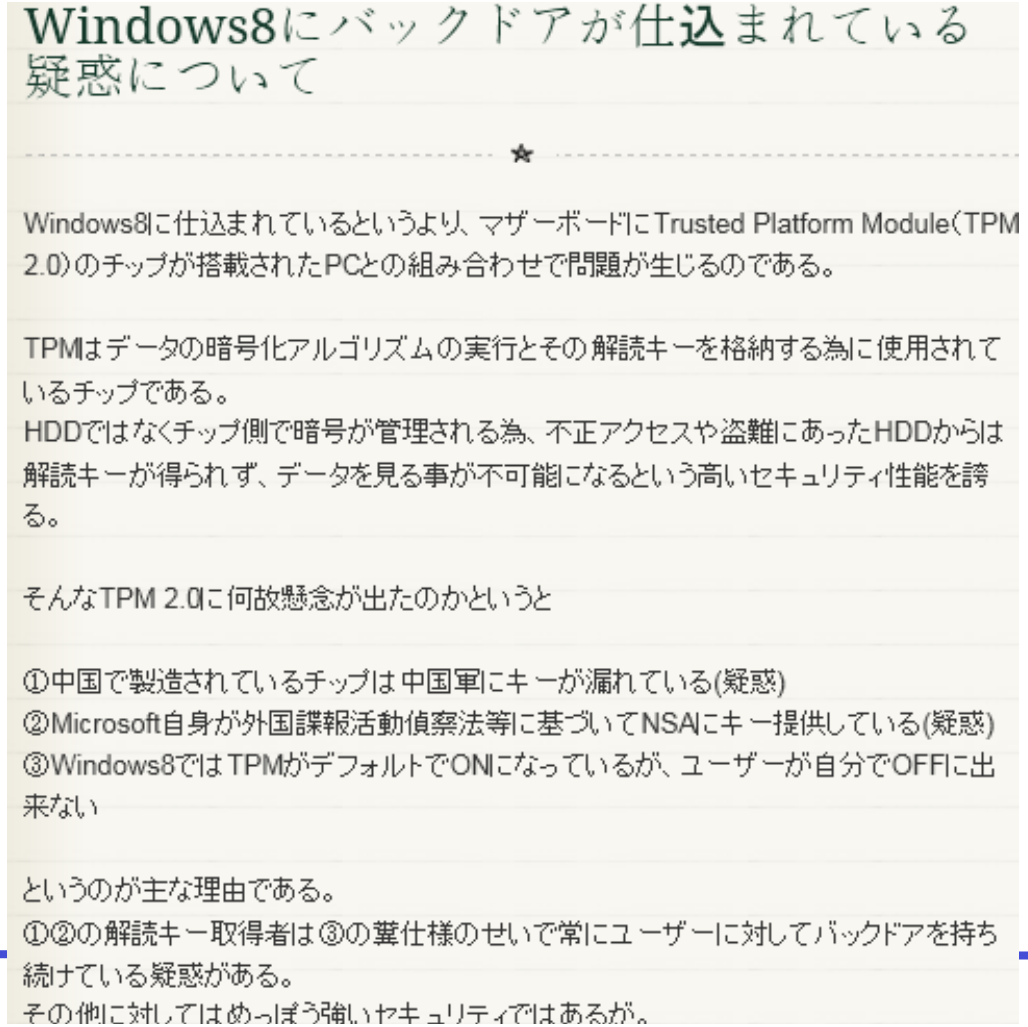
In-vehicle Network Securityの全体像（例）



都市伝説「TPMに隠された鍵疑惑」

- ドイツ政府「Windows 8にバックドアの可能性」
  http://pcscribblememo.blogspot.jp/p/windows8_14.html
  ⇒ PCディスクの暗号鍵を、外部の第三者がセットしていることへの気持ち悪さ。

「利用者関与の機会」
「透明性の確保」
が問われている。



Windows8にバックドアが仕込まれている疑惑について

★

Windows8に仕込まれているというより、マザーボードにTrusted Platform Module(TPM 2.0)のチップが搭載されたPCとの組み合わせで問題が生じるのである。

TPMはデータの暗号化アルゴリズムの実行とその解読キーを格納する為に使用されているチップである。
HDDではなくチップ側で暗号が管理される為、不正アクセスや盗難にあったHDDからは解読キーが得られず、データを見る事が不可能になるという高いセキュリティ性能を誇る。

そんなTPM 2.0に何故懸念が出たのかというと

①中国で製造されているチップは中国軍にキーが漏れている(疑惑)
②Microsoft自身が外国諜報活動偵察法等に基づいてNSAにキー提供している(疑惑)
③Windows8ではTPMがデフォルトでONになっているが、ユーザーが自分でOFFに出来ない

というのが主な理由である。
①②の解読キー取得者は③の糞仕様のせいで常にユーザーに対してバックドアを持ち続けている疑惑がある。
その他に対してはめっぽう強いセキュリティではあるが。

KDDI R&D LABS

組込みマイコンの解析「剥離攻撃」

- Trusted Platform Module (TPM)内データの奪取
  http://gcn.com/articles/2010/02/02/black-hat-chip-crack-020210.aspx

Engineer shows how to crack a 'secure' TPM chip

By William Jackson Feb 02, 2010

スライスして、穴を開け、タップしバスを流れる平文をモニタした。

A security engineer who reverse-engineered the family of chips from Infineon Technologies AG that includes its Trusted Platform Module implementation showed an audience at the Black Hat Federal Briefings how he cracked the chip and accessed its data.

Using an electron microscope to operate at the nanometer scale and Adobe Photoshop to plan his attack, Christopher Tarnovsky was able to sit on the chip's data bus and "listen" to unencrypted code.

"This takes you somewhere that Infineon says you can't go," said Tarnovsky, who runs Flylogic Engineering and specializes in analyzing semiconductor security. He demonstrated his technique Feb. 2 at the conference, in Washington, D.C.

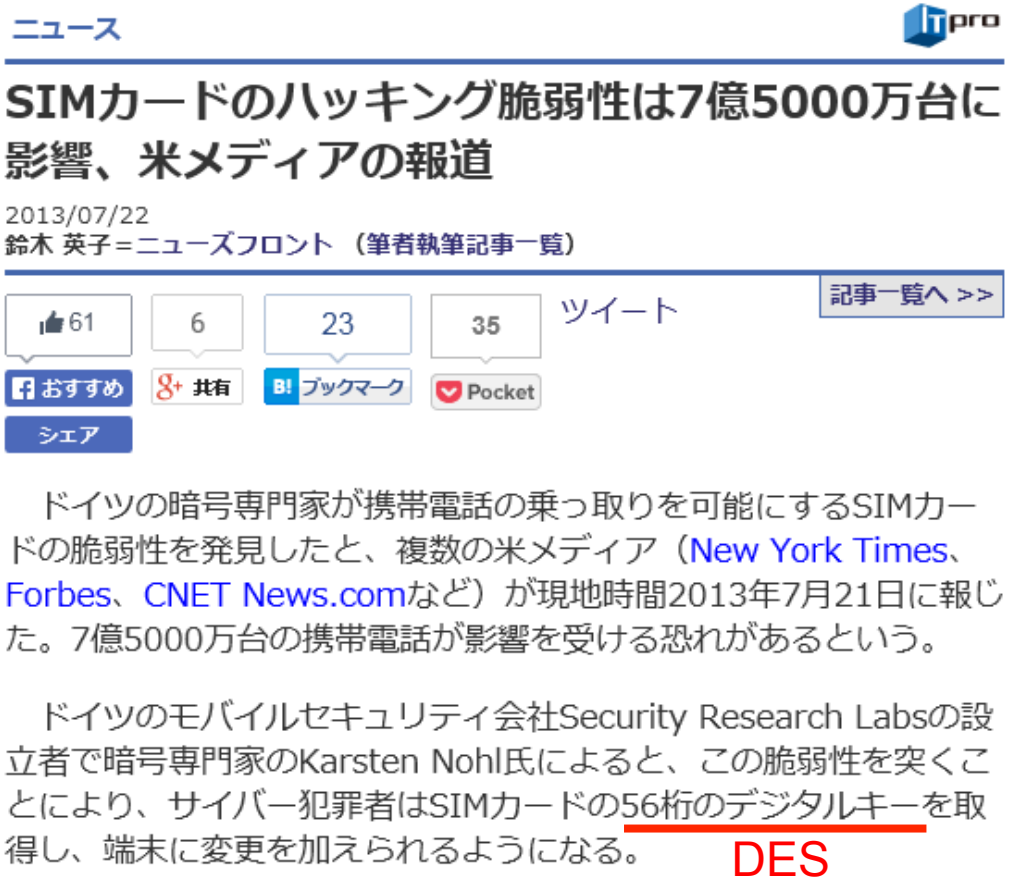
He began by buying chips in bulk for pennies apiece to experiment with and break. He stripped each layer off the chip to expose its topography, imaged the layers using optical and electron microscopes, and used Photoshop to layer the images so he could plan his attack through an intact chip.

剥離（物理）攻撃に対する耐性なし

KDDI R&D LABS

古いSIMのDESハック疑惑

http://pc.nikkeibp.co.jp/article/news/20130722/1098506/?set=relate#



ニュース

SIMカードのハッキング脆弱性は7億5000万台に影響、米メディアの報道

2013/07/22
鈴木 英子＝ニューズフロント （筆者執筆記事一覧）

61 6 23 35 ツイート 記事一覧へ >>

おすすめ 共有 ブックマーク Pocket シェア

ドイツの暗号専門家が携帯電話の乗っ取りを可能にするSIMカードの脆弱性を発見したと、複数の米メディア（New York Times、Forbes、CNET News.comなど）が現地時間2013年7月21日に報じた。7億5000万台の携帯電話が影響を受ける恐れがあるという。

ドイツのモバイルセキュリティ会社Security Research Labsの設立者で暗号専門家のKarsten Nohl氏によると、この脆弱性を突くことにより、サイバー犯罪者はSIMカードの56桁のデジタルキーを取得し、端末に変更を加えられるようになる。

DES

- 考察
  - ◆ DESという危殆化した暗号アルゴリズムが狙われた。
    - ⇒ SIMのアーキテクチャ自体が陥落した訳ではない。
    - ⇒ 時間の経過とともに危殆化するアルゴリズムの更新が重要。

注）日本の通信事業者は、当初から3DESを搭載。昨今は、AESを搭載。

人によるオペレーションの隙が突かれる

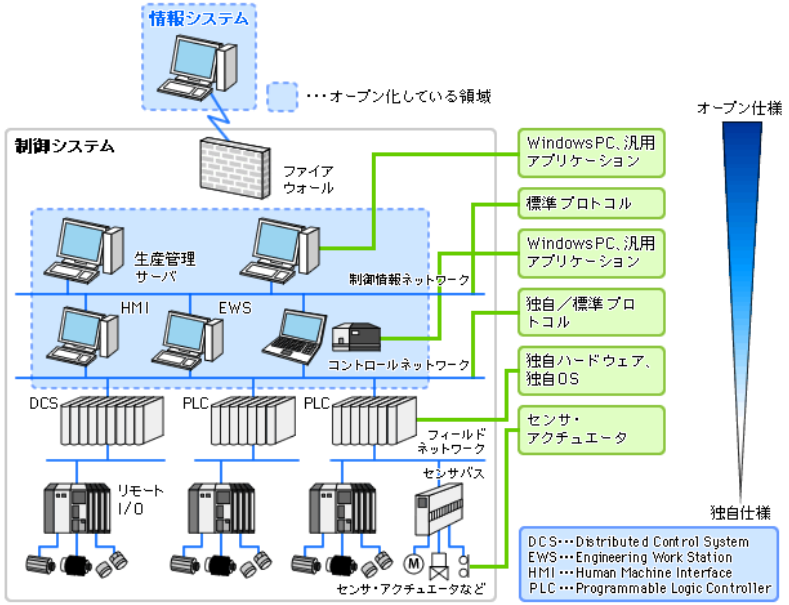
年金情報、流出は101万人　月内に謝罪文書を発送

2015年6月22日23時51分

情報持ち出し先PCのウイルス感染
（オペレーションの隙）

Stuxnet（スタックスネット）とは、複数の脆弱性を悪用しながらUSBメモリなどの外部メディア経由でWindows PCに感染し、原子力発電所の制御システムへ侵入して、その制御システム上にある装置に攻撃を加えるコンピュータウイルスのこと。Stuxnetは、独シーメンス社のPLC（プログラマブルロジックコントローラ）向けソフト「WinCC/Step7」の脆弱性を狙ってPLCに悪質なコードを書き込むことで、原子力発電所の制御システムに悪影響を及ぼすよう仕組まれている。

持込みUSBから汎用PCへの
ウイルス感染（オペレーションの隙）



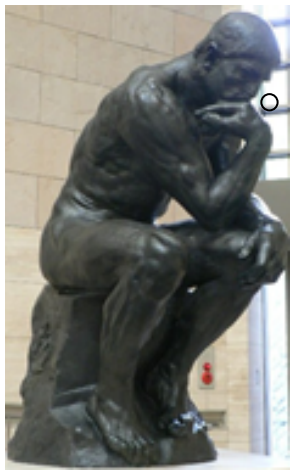
■ 考察

- ◆ システム／アルゴリズムの隙を突くより人が介在するオペレーションの隙を突く方が、攻撃は容易。
- ⇒ 適切なセキュリティ技術を適用し、人の介在を排除することで、そこそこ守れる。

鍵管理に人手による通常運用を挟まないこと。

セキュアエレメントを基点とした車載制御システムの保護
–要素技術の整理と考察–

KDDI研究所　竹森敬祐

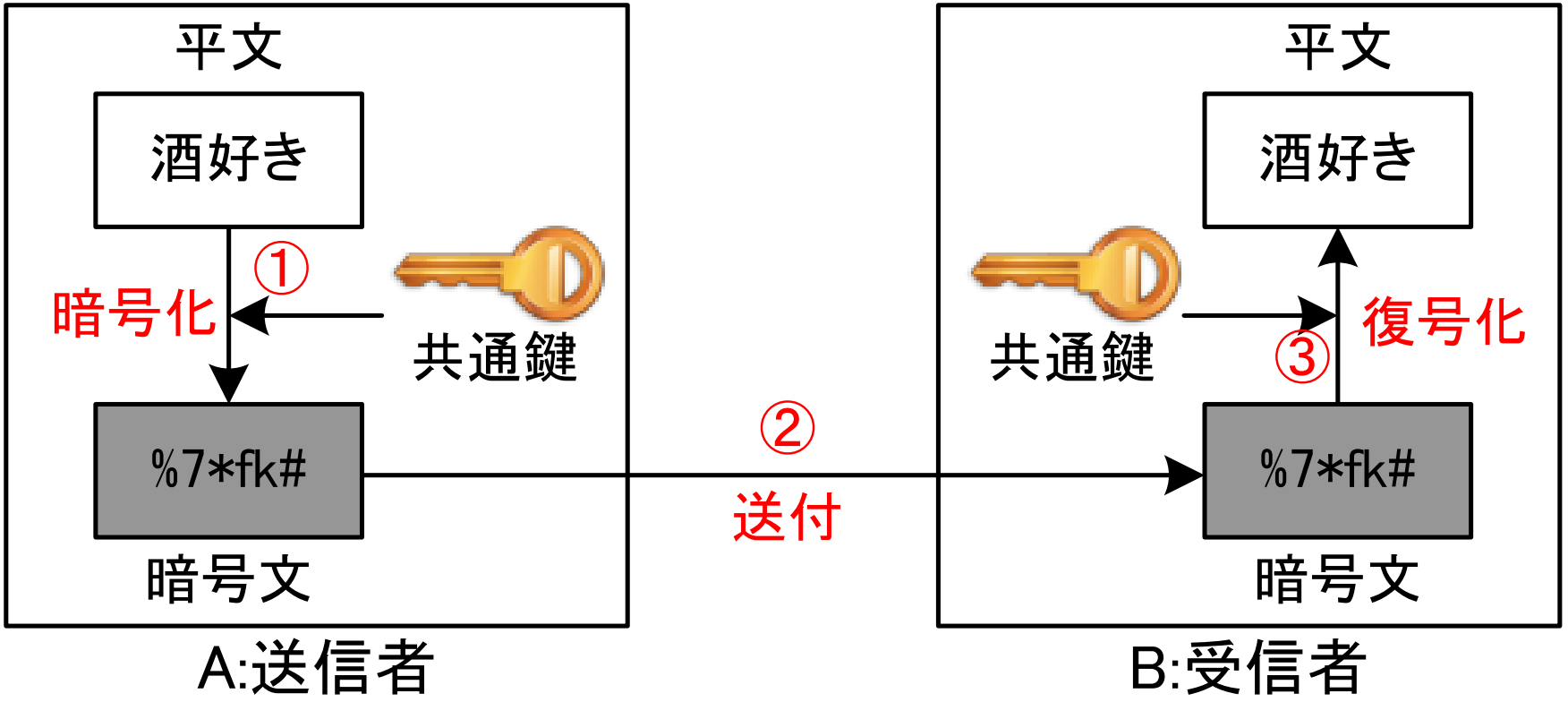


ハッカー視点で狙いどころを考え、セキュアエレメントの導入で、根本解決を目指す。

- セキュリティとは
- インシデントの収集・分析
- **対策に関する基礎技術**
- 鍵管理の一例
- CANパケット認証、ECUのセキュアブート
- リモートリプログラミング

共通鍵(対称鍵)暗号方式

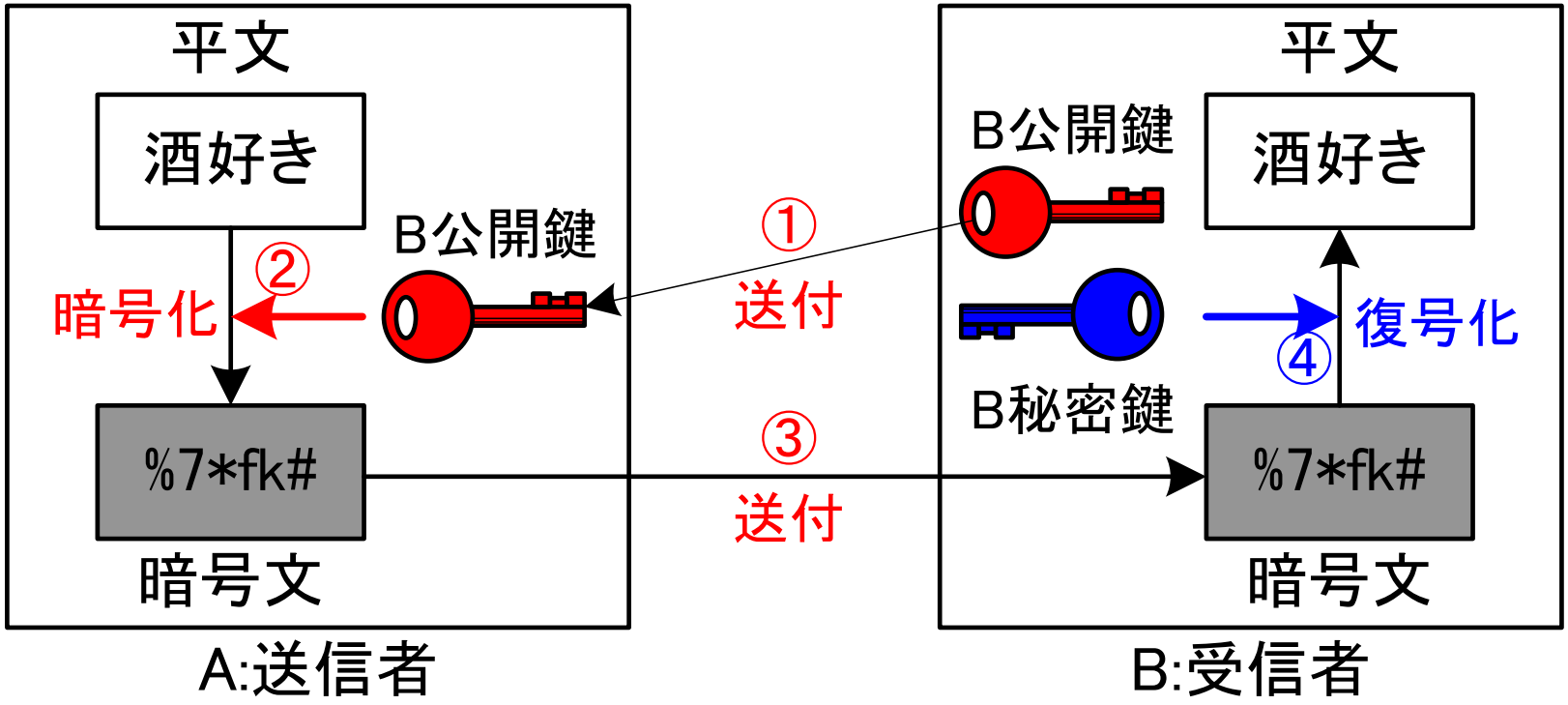
AESなど



■ 利点
- ◆ 処理が軽い(高速)。
- ◆ 鍵のサイズが小さい。

■ 課題
- ◆ 鍵の安全な配布。
- ◆ 鍵の秘匿管理。

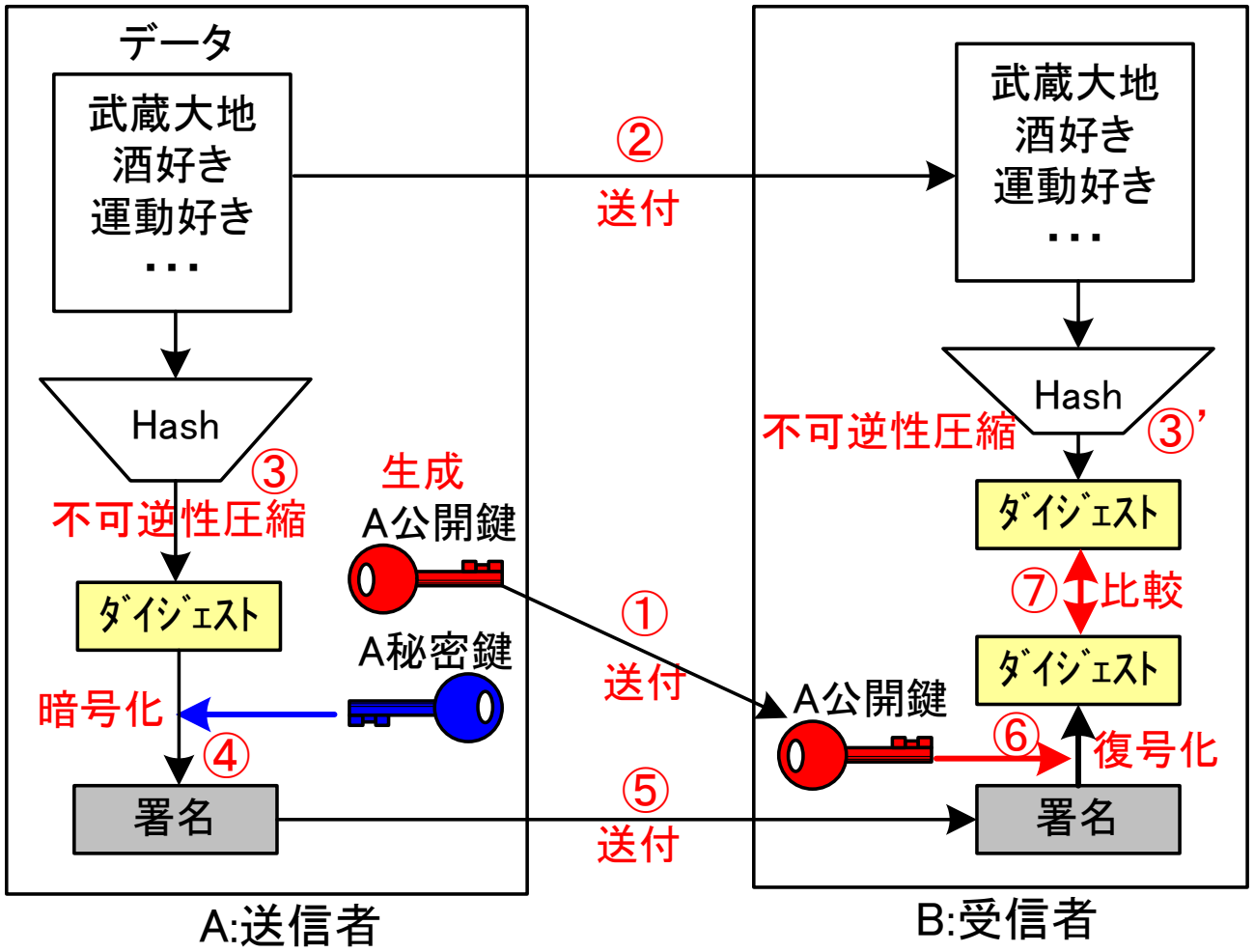
公開鍵(非対称鍵)暗号方式　RSA、ECCなど



■ 利点
- ◆ 鍵は通信時に渡せばよい。
- ◆ 暗号化と署名に利用できる。

■ 課題
- ◆ 処理が重い。
  (大きな情報の暗号化は不可)
- ◆ 本物の公開鍵の受け取り。
- ◆ 秘密鍵の秘匿管理。

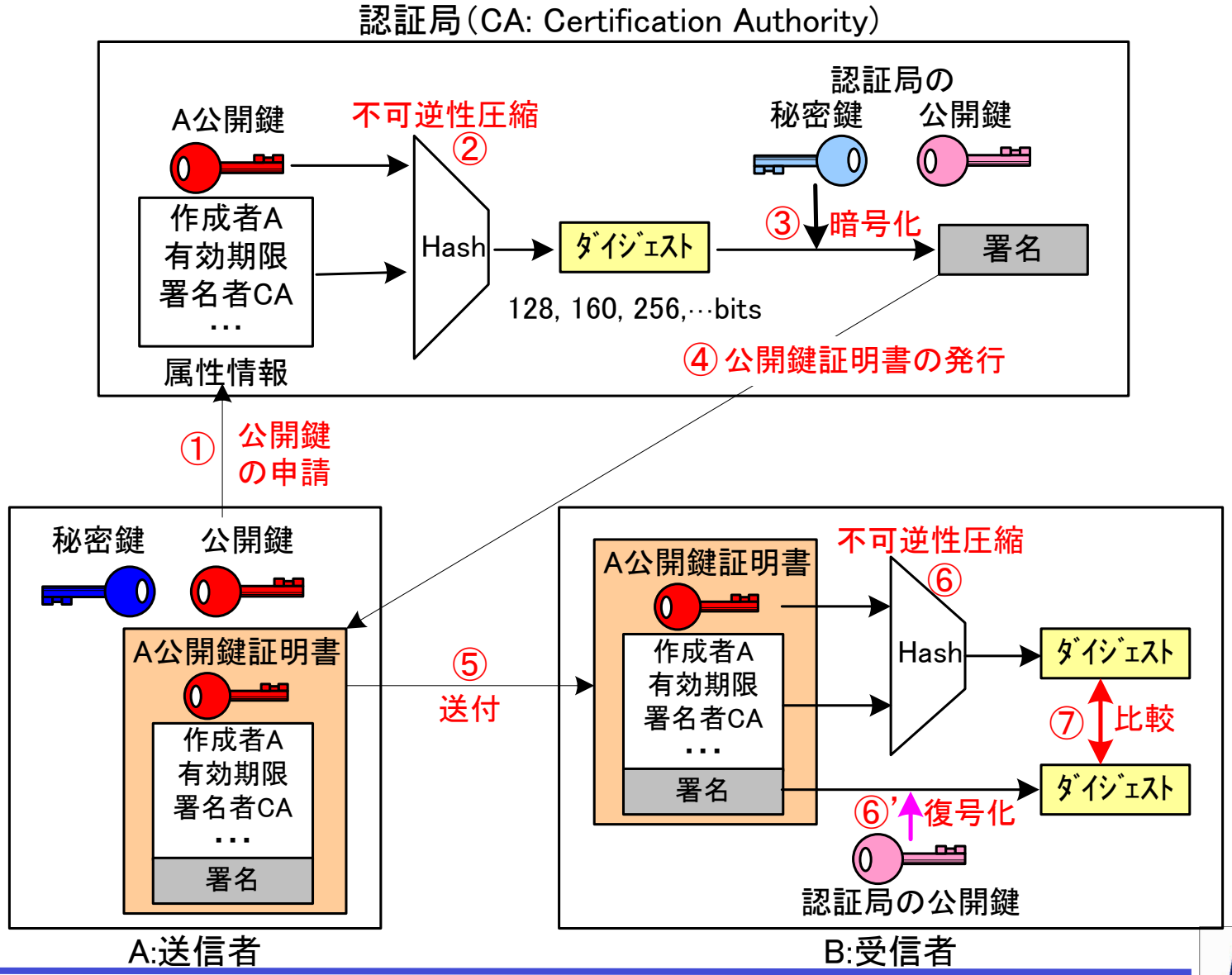
電子署名・検証



■ 利点
- ◆ データの完全性を検証可能。

■ 課題
- ◆ 公開鍵の正当性を要検証。

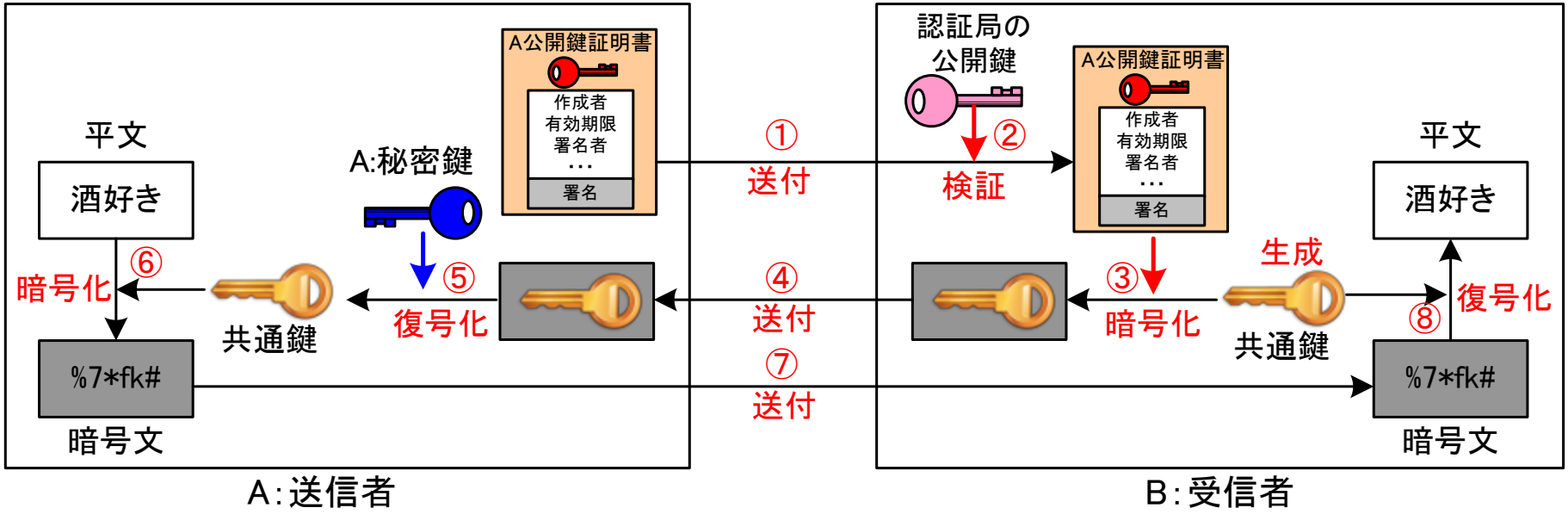
公開鍵証明書の発行・検証



KDDI R&D LABS

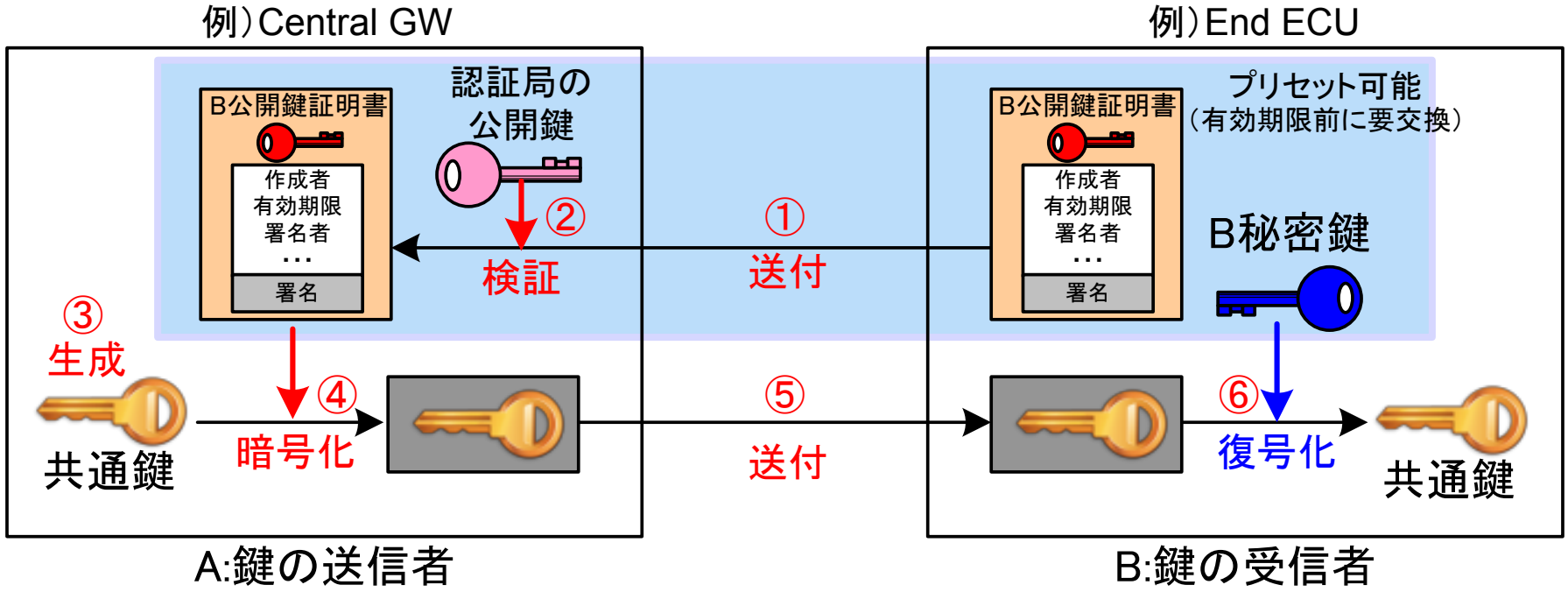
ハイブリッド暗号方式

HTTPSなど



- 利点
  - 鍵交換と高速な暗号通信を実現。
- 課題
  - 認証局の公開鍵の安全な管理。
  - A秘密鍵の秘匿管理。

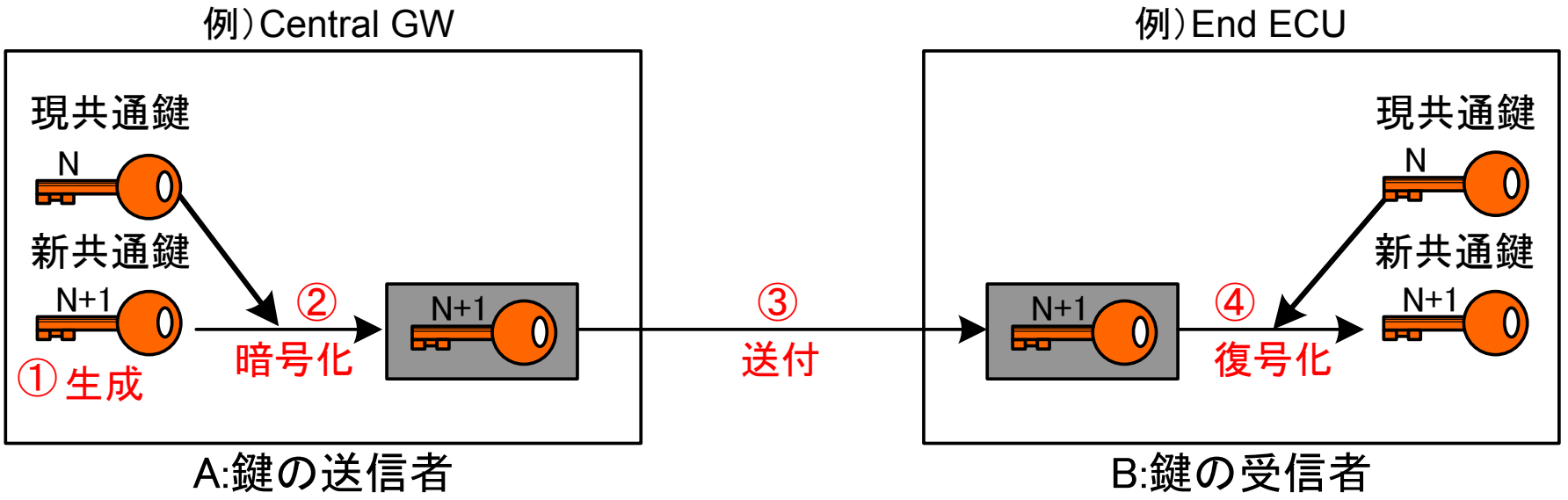
公開鍵ベースの鍵配信方式



■ 利点
- ◆ 知らない者間の暗号通信可能。

■ 課題
- ◆ 認証局の公開鍵の安全な管理。
- ◆ B秘密鍵の秘匿管理。
- ◆ 処理負荷（時間）が大きい。
  （ECU毎に公開鍵暗号の処理を行う）
- ◆ 公開鍵証明書サイズが大きい。

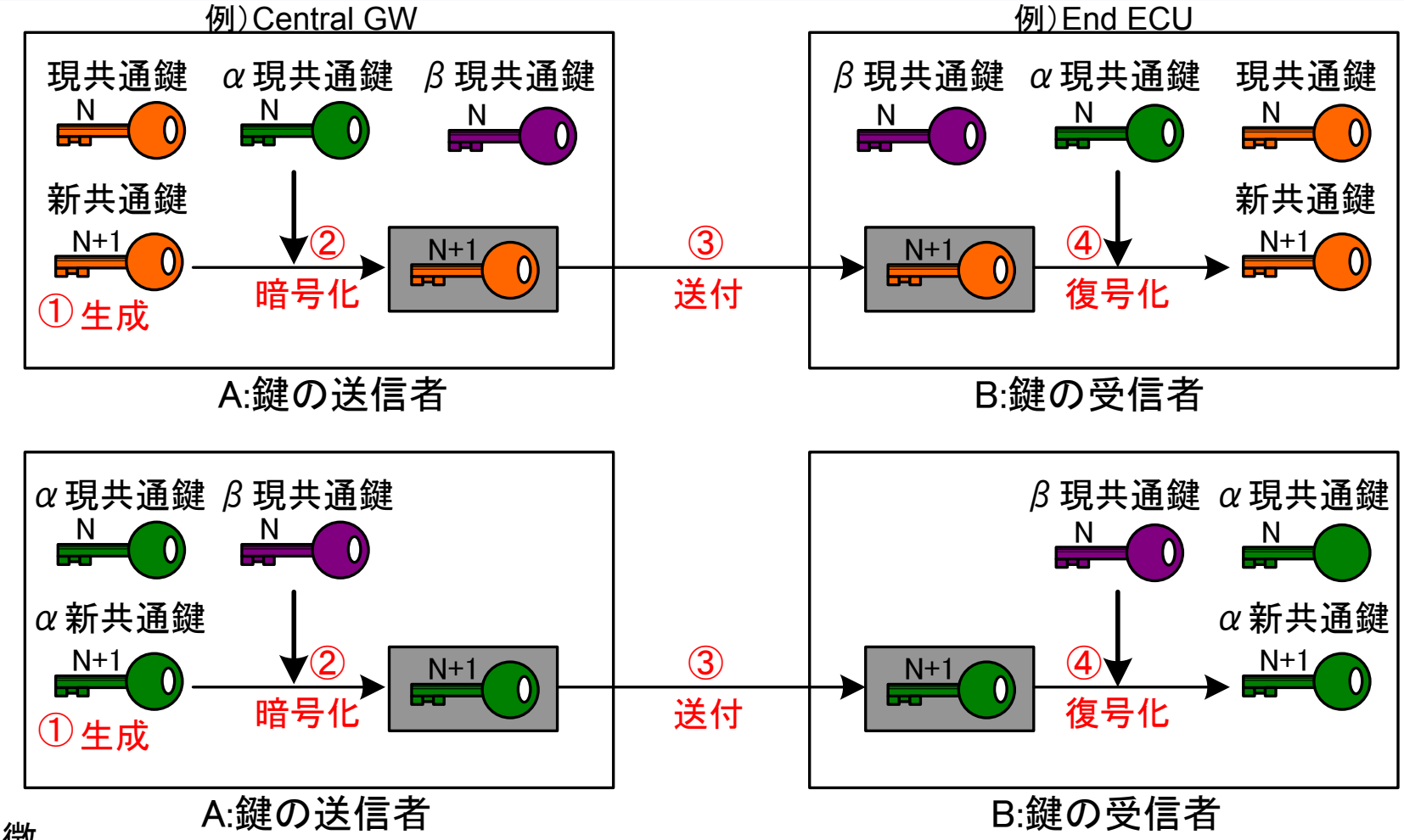
1層共通鍵ベースの鍵配信方式



■ 利点
- ◆ 処理が軽い（高速）。
- ◆ 鍵のサイズが小さい。

■ 課題
- ◆ 共通鍵を安全に共有すること。
  （一度漏洩すると、新鍵も漏洩する）

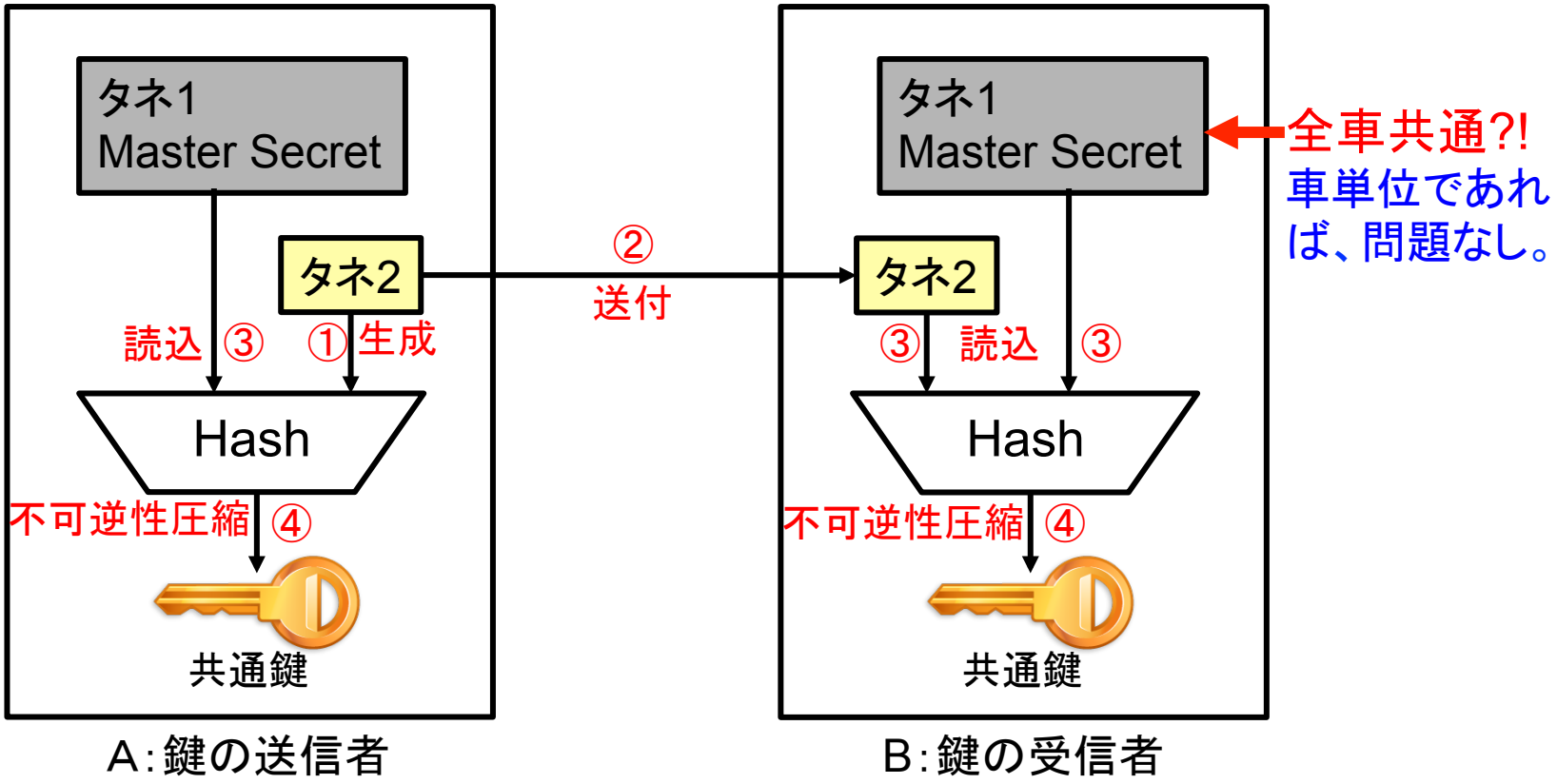
多層共通鍵ベースの鍵配信方式



■ 特徴

- ◆ 共通鍵を階層化することで、もし漏洩した場合でも、上層の共通鍵で新たな共通鍵を配布できる。
- ◆ 「認証局の公開鍵、B秘密鍵の安全な管理」の課題は、「上層の共通鍵の安全な管理」の課題と同じ。
  ⇒ 多層共通鍵ベースの鍵配信方式は、公開鍵ベースの鍵配信方式と、同じ安全性。

共通鍵の生成・共有



A:鍵の送信者　　B:鍵の受信者

■ 利点
- ◆ 処理が軽い(高速)。

■課題
- ◆ Master Secretの秘匿管理。
  - ⇒ 同じMaster Secretを何度も使うことになる。
  - ⇒ 多層共通鍵の配信方式が良さそう。
  - ⇒ SHEの鍵配信への問題提起。

KDDI R&D LABS

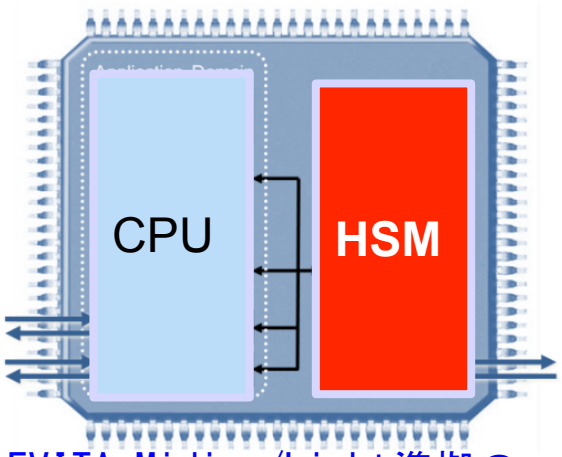
トラストアンカー（セキュアエレメント）の考察

	SHE	HSM （ICU-MB相当）	TPM （マイコン内包型）	SIM/eSIM
対タンパ性	△*1	△*1	？	○*2
高速性	○	○	○	×*3
暗号機能	△*4	○	○	○
アプリ実行環境	×	○	×	○
データ更新	○	○	○	○
デバイスコスト	○	△	△	×（○）*5

*1）メイン演算器から独立、インタフェース(IF)が限られているなど、直接的な攻撃への耐性はある。しかし、サイドチャネル攻撃などの間接的な攻撃への耐性は高くない。
*2）LSIレベルでEAL5+を取得済み。クレジットカード協会の基準をクリアしている。
*3）DCM内の通信モジュール内に組み込まれることでの複数IF経由の遅延が生じる。
*4）共通鍵ベースの暗号しかサポートしておらず、署名を車外と共有し難い。
*5）通信モジュール搭載車については、SIMの追加は不要。

KDDI R&D LABS

EVITA: Hardware Security Module（HSM） ～2010年7月～



EVITA Midium/Light準拠の
ルネサスRH850F1H/F1L

EVITA HSM http://www.evita-project.org/Publications/AEHR10.pdf

	Full EVITA HSM	Medium EVITA HSM	Light EVITA HSM
Internal RAM	✓ (e.g. 64 kByte)	✓ (e.g. 64 kByte)	optional
Internal NVM (Non-volatile memory)	✓ (e.g. 512 kByte)	✓ (e.g. 512 kByte)	optional
Symmetric Cryptographic Engine (e.g. AES-128 CCM, GCM f/AE)	✓	✓	✓
Asymmetric Cryptographic Engine (e.g. ECC-256-GF(p) NIST FIPS 186-2 prime field)	✓		
Hash engine (e.g. Whirlpool)	✓	セキュアブートの結果測定に必要	
Counters	✓ (e.g. 16 × 64-bit monotonic counter)	✓ (e.g. 16 × 64-bit monotonic counter)	optional
Random Number Generator	✓ (e.g. AES-PRNG with TRNG seed)	✓ (e.g. AES-PRNG with TRNG seed)	optional
Secure CPU (e.g. ARM Cortex-M3 32 bit, 50–250 MHz)	✓	✓	
Hardware Interface	✓	✓	✓

KDDI R&D LABS

考察：HSMへの追加要求

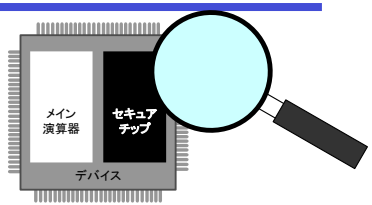
	Central GW		エンドECU
	Full EVITA HSM	Medium EVITA HSM	Light EVITA HSM
Internal RAM	✓ (e.g. 64 kByte)	✓ (e.g. 64 kByte)	○ (e.g. 64 kByte)
Internal NVM (Non-volatile memory)	✓ (e.g. 512 kByte)	✓ (e.g. 512 kByte)	○ (e.g. 512 kByte)
Symmetric Cryptographic Engine (e.g. AES-128 CCM, GCM f/AE)	✓	✓	✓
Asymmetric Cryptographic Engine (e.g. ECC-256-GF(p) NIST FIPS 186-2 prime field)	✓	不要（Secure CPUでS/W対応可能）	
Hash engine (e.g. Whirlpool)	✓	○	○
Counters	✓ (e.g. 16 × 64-bit monotonic counter)	✓ (e.g. 16 × 64-bit monotonic counter)	optional
Random Number Generator	✓ (e.g. AES-PRNG with TRNG seed)	✓ (e.g. AES-PRNG with TRNG seed)	optional
Secure CPU (e.g. ARM Cortex-M3 32 bit, 50–250 MHz)	✓	✓	
Hardware Interface	✓	✓	✓
サイドチャネル攻撃耐性	不要*1／必要*2		不要

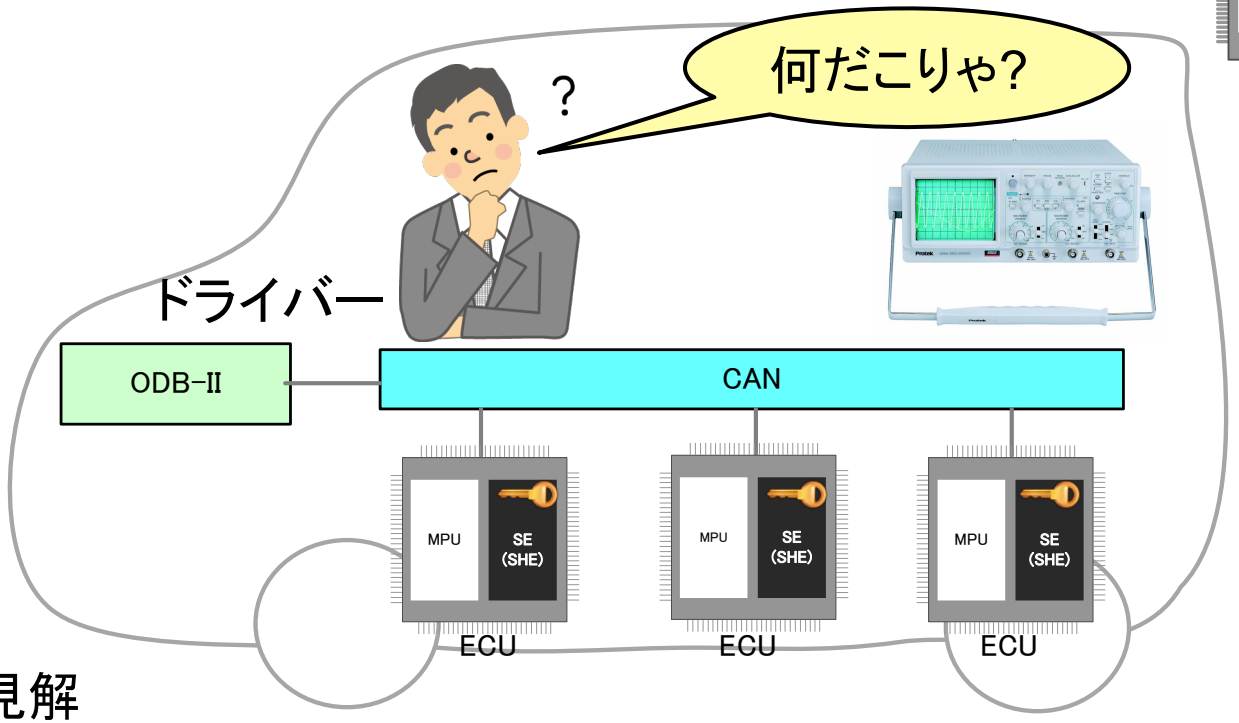
*1 他に頼れる耐性セキュアエレメントがある場合
*2 他に頼れる耐性セキュアエレメントがない場合

⇒高速性も問われるため、要求しない方が良い。

考察：ECUにサイドチャネル攻撃耐性は必要か？

ケース：車ごとに異なるセッション鍵を守る場合





出典
http://atex.pos.to/newpage26.htm

■ 個人的な見解

- ◆ 解析装置は大きく、車に取り付けられるとドライバーが気づく。
- ◆ 解析装置は高価なものであり、攻撃者が不利？　売り飛ばせば運転者が儲かる。
  ⇒ 普及する攻撃モデルとして成り立たない。

リスクの受容

ローカル（実験室）攻撃は成されて論文発表されるが、巷車に影響しない。

KDDI R&D LABS

サイドチャネル攻撃耐性を持つSEの例「SIM（ICカード）」

■ SIM（ICカード）のアプリ実行領域の活用
- ◆ トラストアンカー（信頼の基点）となりうる超重要な鍵を管理する。
- ◆ 処理速度は遅いため、超重要でない鍵の管理はCentral GWに任せる。

■ H/Wサポートする機能の一例
- ◆ RSA 2048
- ◆ ECC P256
- ◆ AES 128
- ◆ SHA-256
- ◆ HMAC

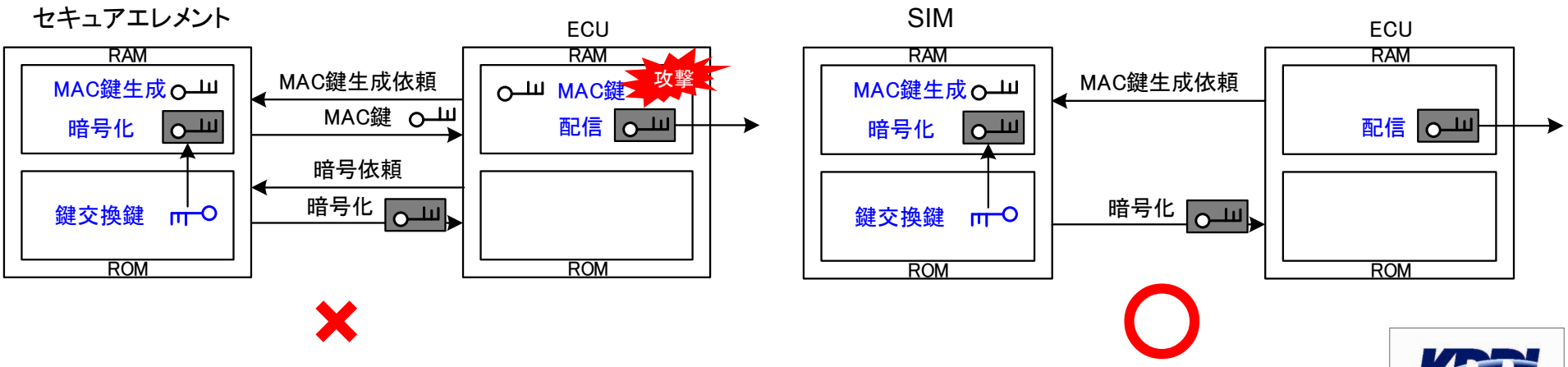
■ その他機能の一例
- ◆ ｱﾌﾟﾘ実行領域の空き：275KB程度（参考値）
- ◆ 書換えは100万回まで保証

■ アプリ領域の管理
- ◆ Over the Air (OTA)で書き換え可能。⇒ 未来の攻撃に対する耐性あり。
- ◆ アプリ実行領域は、通信事業者やOEM殿が書き換え主体になりえる。

KDDI R&D LABS

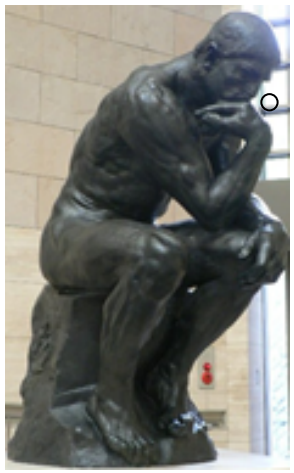
参考）SIM（ICカード）の特徴

- SIM（ICカード）の特徴
  - 通信モジュールが搭載されているクルマなら、H/W追加コストなし。
  - アーキテクチャに関する事故ゼロの実績。
    - ⇒ LSIとしてEAL5+を取得済み。
    - ⇒ クレジットカードブランドが定めるセキュリティ試験をパスしている。
  - Over the Air（OTA）で書き換え可能。
    - ⇒ 未来の攻撃に対応できる（危殆化した際のリカバリ可能）。
  - Javaアプリを組み込める。
    - ⇒ 処理をSIMの内部に閉じ込めることで、狙いどころが無い（実装セキュリティ）。



セキュアエレメントを基点とした車載制御システムの保護
–要素技術の整理と考察–

KDDI研究所　竹森敬祐

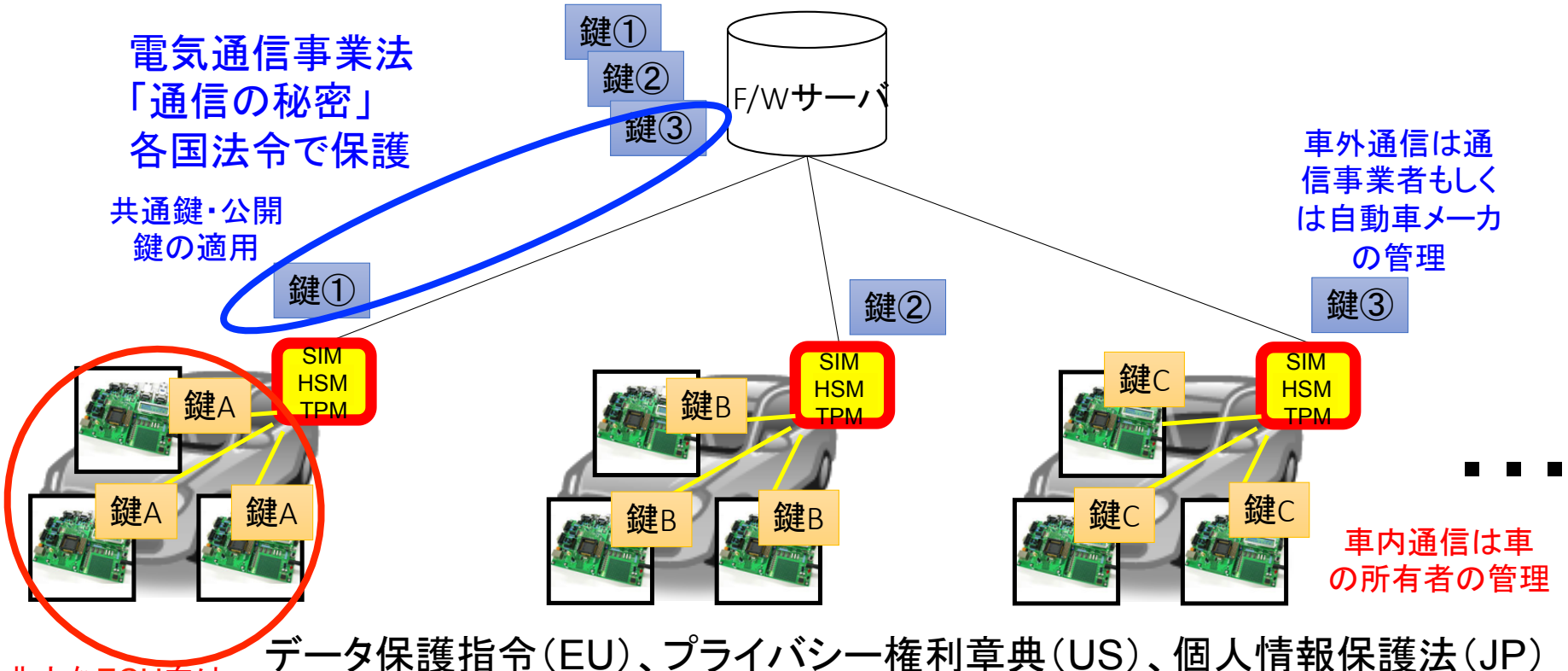


ハッカー視点で狙いどころを考え、セキュアエレメントの導入で、根本解決を目指す。

- セキュリティとは
- インシデントの収集・分析
- 対策に関する基礎技術
- **鍵管理**
- CANパケット認証、ECUのセキュアブート
- リモートリプログラミング

考え方）車外NWと車内NWの境界

- Privacy by Design（車内外の鍵を分ける）
  - 車内処理に関わる鍵を、外部者が関与することへのプライバシ不安を解消するために、車外と車内の鍵を分けて、SIM／HSM／TPMがプロキシ役を果たす。



データ保護指令（EU）、プライバシー権利章典（US）、個人情報保護法（JP）
「透明性の確保」と「利用者関与の機会」への配慮

車内鍵の管理単位の考察

単位	管理の容易性	漏洩時の影響
(1)車メーカ 車種	メーカ(車種)単位で鍵を管理する。	攻撃者は自身の車を解析することで、同一メーカ(車種)の全車を乗っ取れる。リコールに発展する可能性あり。 ⇒実験室解析が巷車に影響する。
(2)車	車単位で鍵を管理する。	漏洩した車のみに影響。攻撃者は個々の車を解析する必要がある。 ⇒実験室解析が巷車に影響しない。
(3)ECU	ECU毎に異なる鍵を持つ場合、各ECUは通信相手のECUの数だけ鍵を管理する必要がある。 ⇒ MAC検証時の鍵探索処理負荷が掛かる。	漏洩したECUのみに影響する。 ⇒実験室解析が巷車に影響しない。 個々のECUを解析することになるが、重要なECUに絞って攻撃すればよく、攻撃者の負担は(2)と同程度。

MAC鍵は、(2)車単位で生成・管理するのが良さそう。

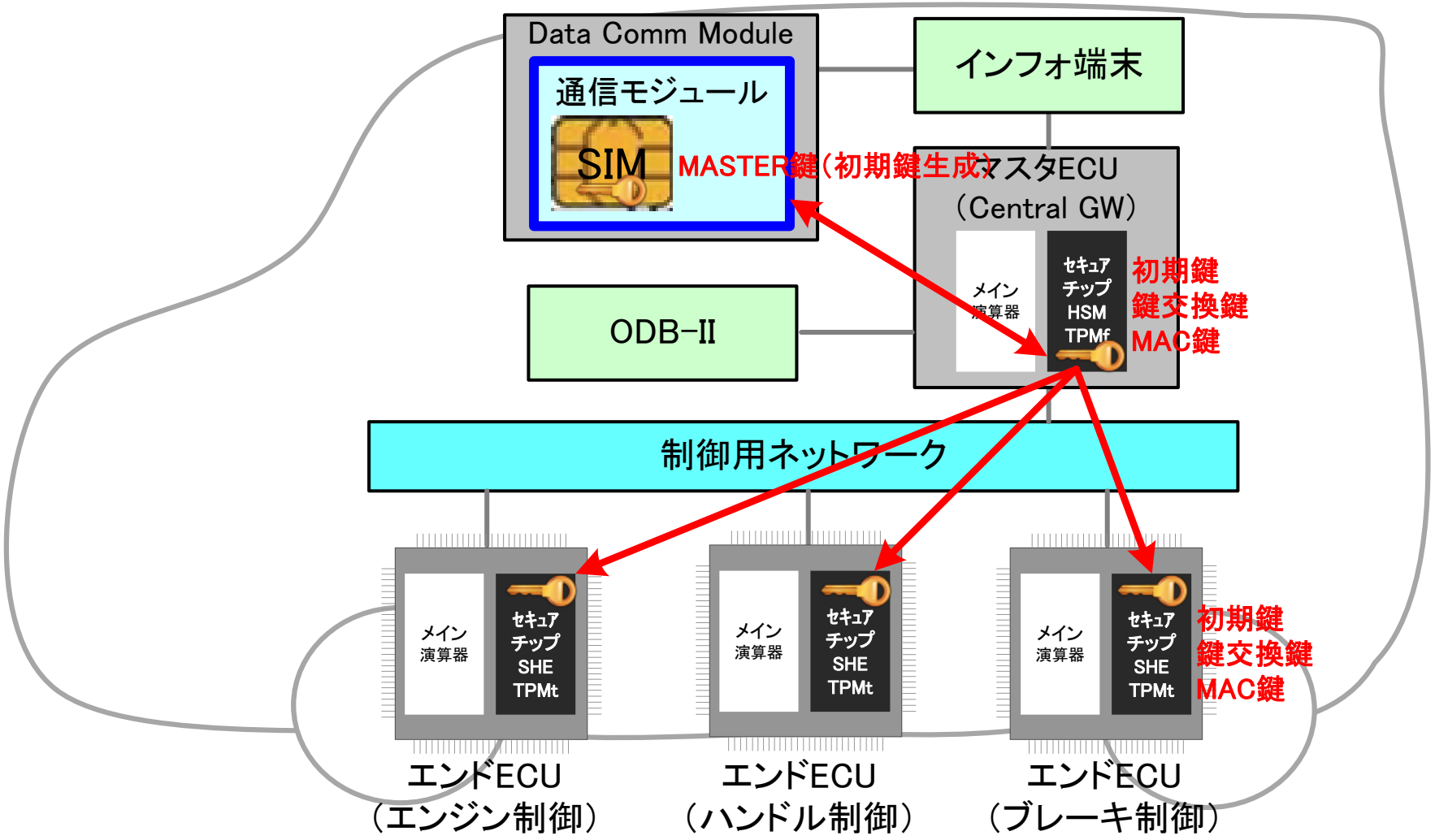
鍵の一例

	説明	要求 安全性	要求 高速性	適用先	対称鍵, 非対象鍵
Master Secret	初期鍵を生成する種。	◎	–	車内 車外	タネ
初期鍵	正規ECUを認証するための鍵。安全にプリセットしておく。初回のみ利用。	○	–	車内 車外	共通鍵
鍵交換鍵	セッション鍵を交換するための車ごとに異なる鍵。長周期で交換。	○	Yes	車内	共通鍵
セッション鍵	MAC生成や車内通信の暗号・復号のために、車ごとに異なる鍵。短周期で交換。	○	Yes	車内	共通鍵
Root証明書	コード署名鍵、ｾｷｭｱﾌﾞｰﾄ署名鍵、車外通信鍵などの正当性の検証に用いる鍵。	◎	–	車内 車外	公開鍵
コード署名鍵	コードの署名の検証に用いる鍵。	○	–	車内 車外	公開鍵
ｾｷｭｱﾌﾞｰﾄ署名鍵	FOTA後のｾｷｭｱﾌﾞｰﾄ測定値に対する署名鍵。車内はCMAC、車外はHMAC。	○	–	車内 車外	車内:共通鍵, 車外:公開鍵
期待値登録鍵 (Boot_MAC_Key)	ECUコードの期待値を算出するための鍵であり、コードのCMACを算出。	○	–	車内	共通鍵
車外通信鍵	車外サーバの認証や暗号化通信のための鍵。	○	–	車外	共通鍵＋ 公開鍵

◎全車共通
○車単位

KDDI R&D LABS

鍵管理モデルの一例

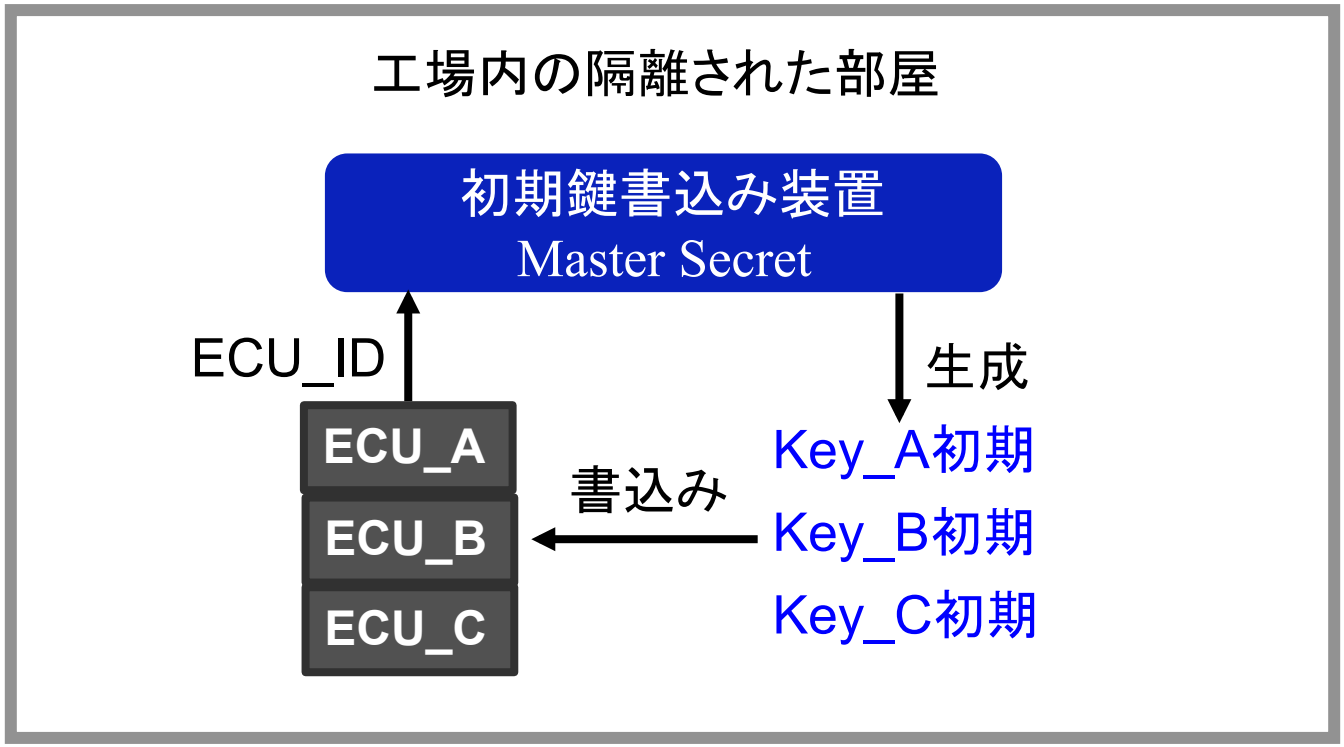


(1-1) ECU認証のための初期鍵の書き込み

■ 初期鍵の生成

◆ Master SecretとECU_IDを基に、ECUの初期鍵を生成する。

ECU初期鍵 ＝ ダイジェスト(ECU_ID + Master Secret)



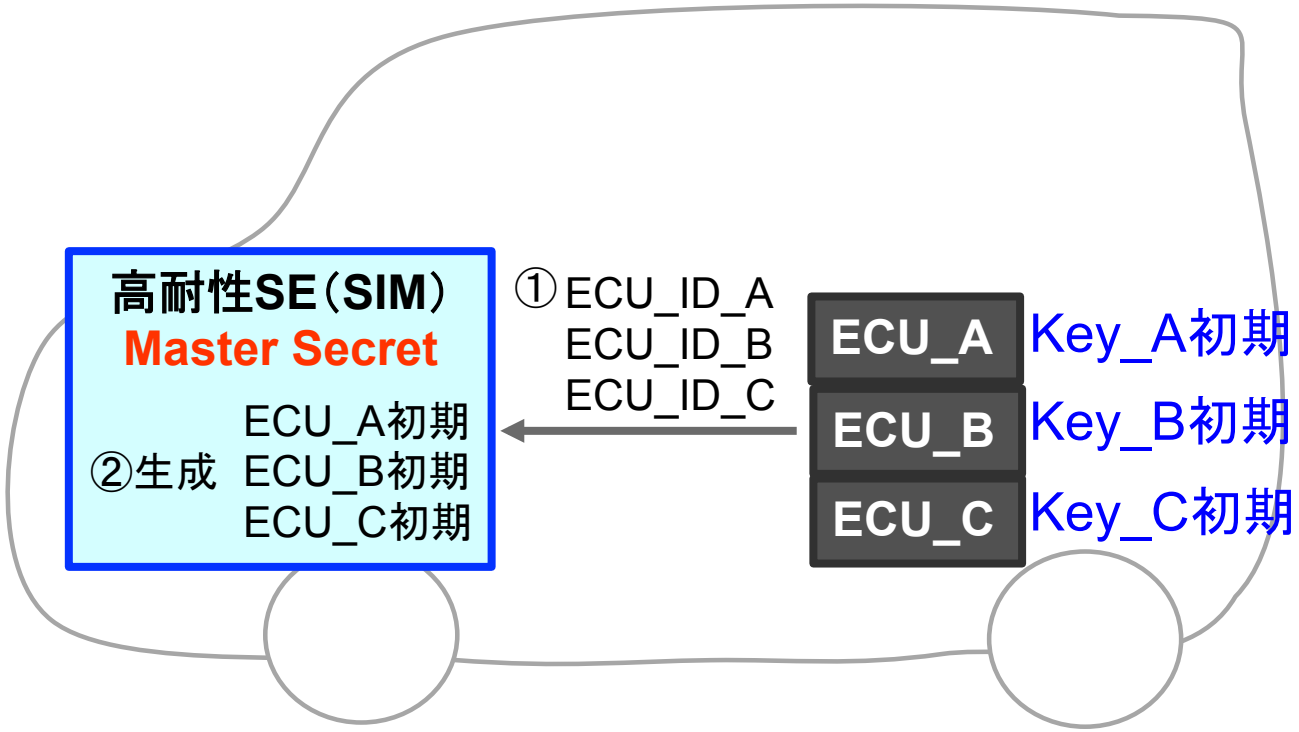
注）初期鍵は、マイコンベンダ、Tier1、OEMのいずれかが書き込む。

(1-2) SIMとの初期鍵の共有案

■ 仕組み

◆ 初めて電源が入ったときに、車内の高耐性SEにECU_IDを通知。

◆ ECU初期鍵 ＝ ダイジェスト(ECU_ID + Master Secret) で初期鍵を生成。



高耐久SEの未搭載車は、完成時や整備時にのみ、高耐久SEをODB-IIに接続すれば良い。

もしMaster Secretが漏洩した場合には、OTAで書き換えると良い。

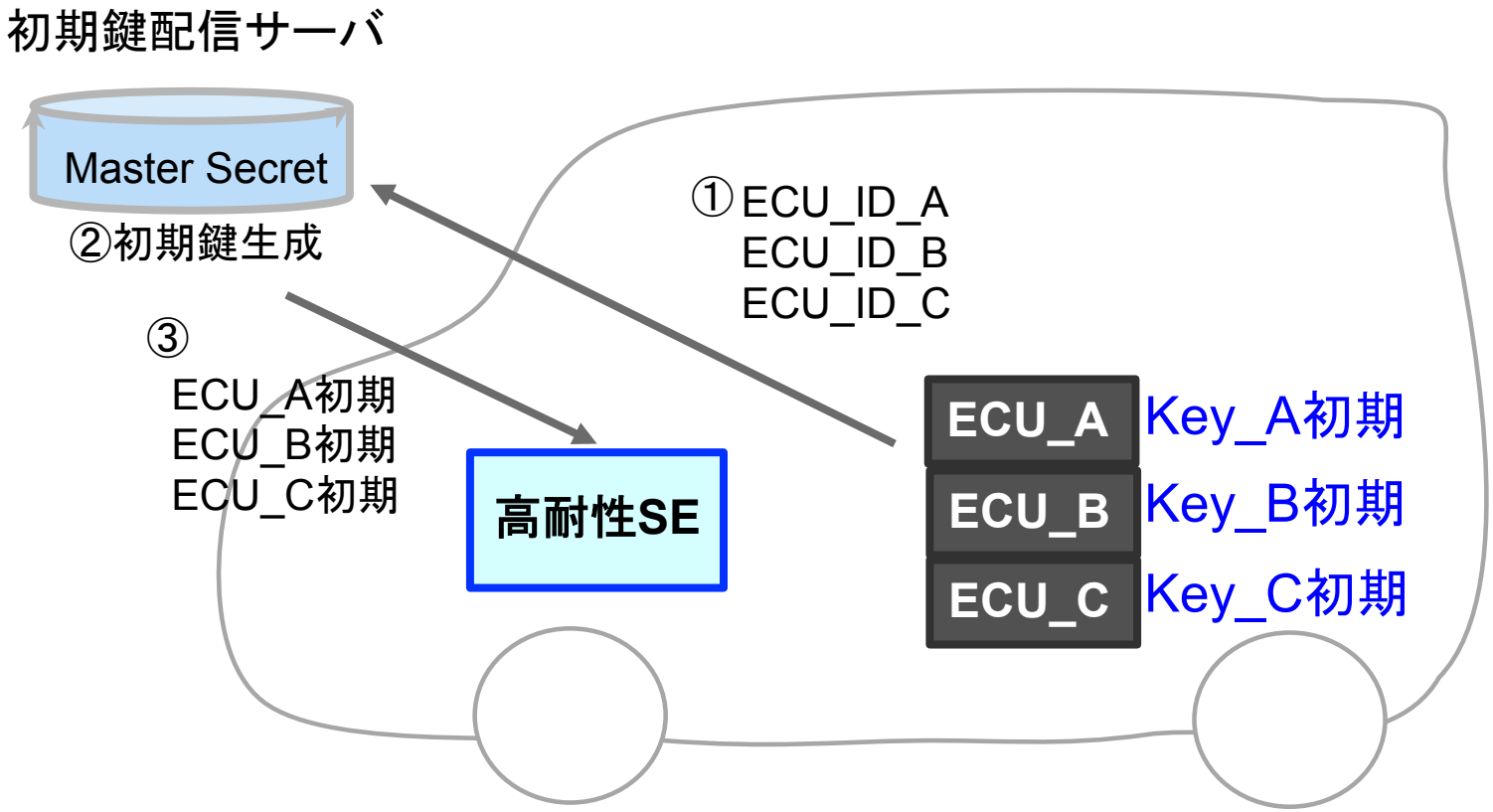
KDDI R&D LABS

(1-2') SIMとの初期鍵の共有案2

■ 仕組み

◆ 初めて電源が入ったときに、車外の初期鍵管理サーバにECU_IDを通知。

◆ ECU初期鍵 ＝ ダイジェスト(ECU_ID + Master Secret)の初期鍵を生成・返信。

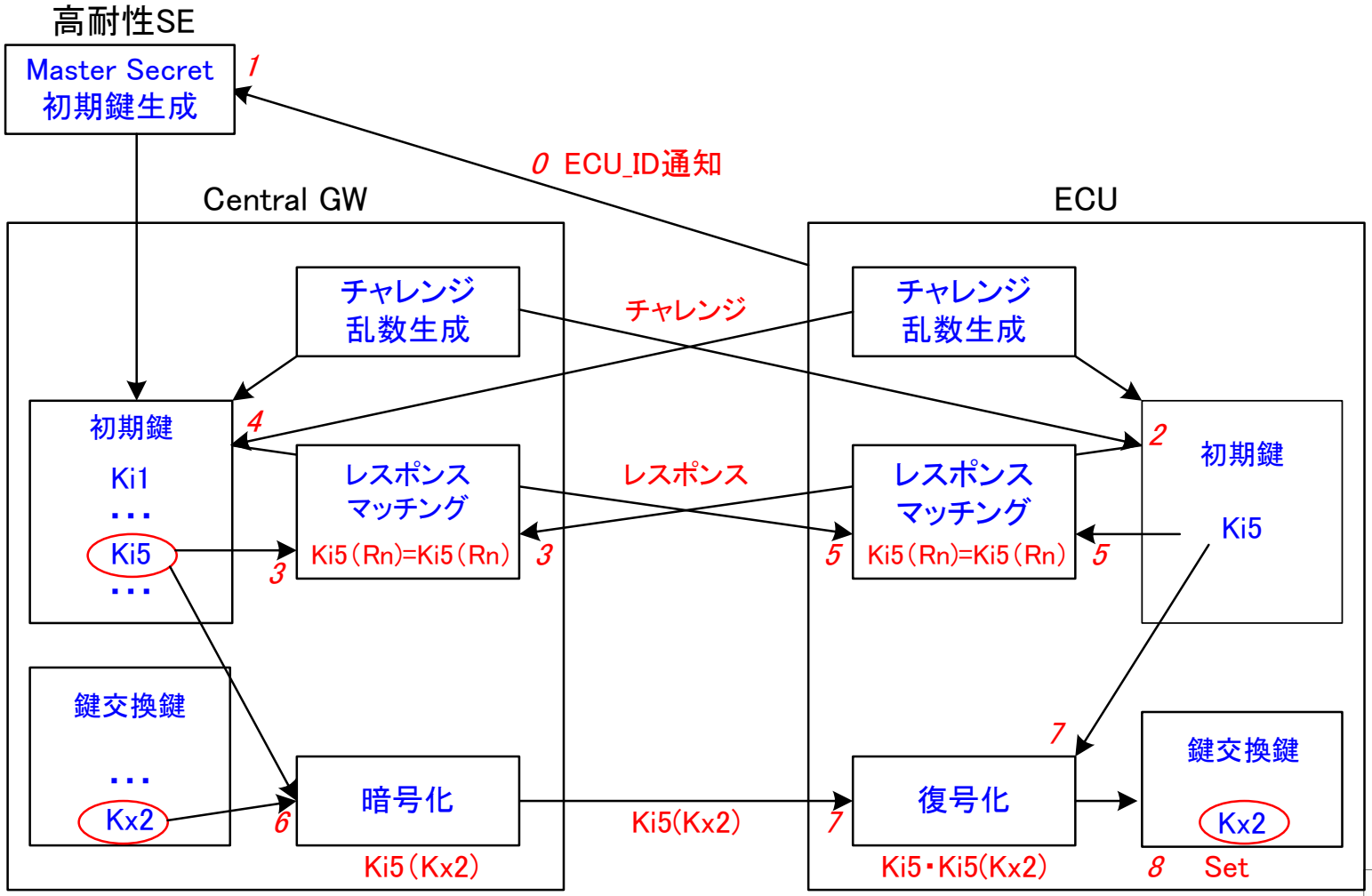


欠点：外部サーバに接続できる通信環境が必要。

KDDI R&D LABS

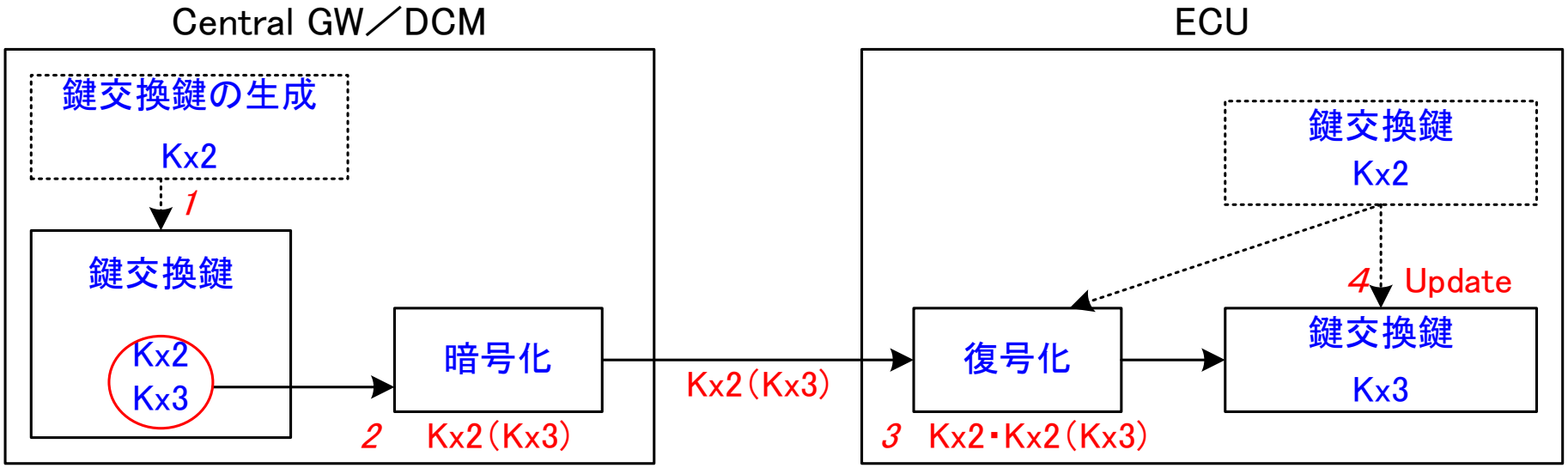
(2-1)鍵交換鍵の初期設定

- 新車、ECUの交換時は、初期鍵を用いて相互認証する。
- 認証に用いた初期鍵を用いて、鍵交換鍵を暗号・復号化して配信する。



(2-2)鍵交換鍵の更新

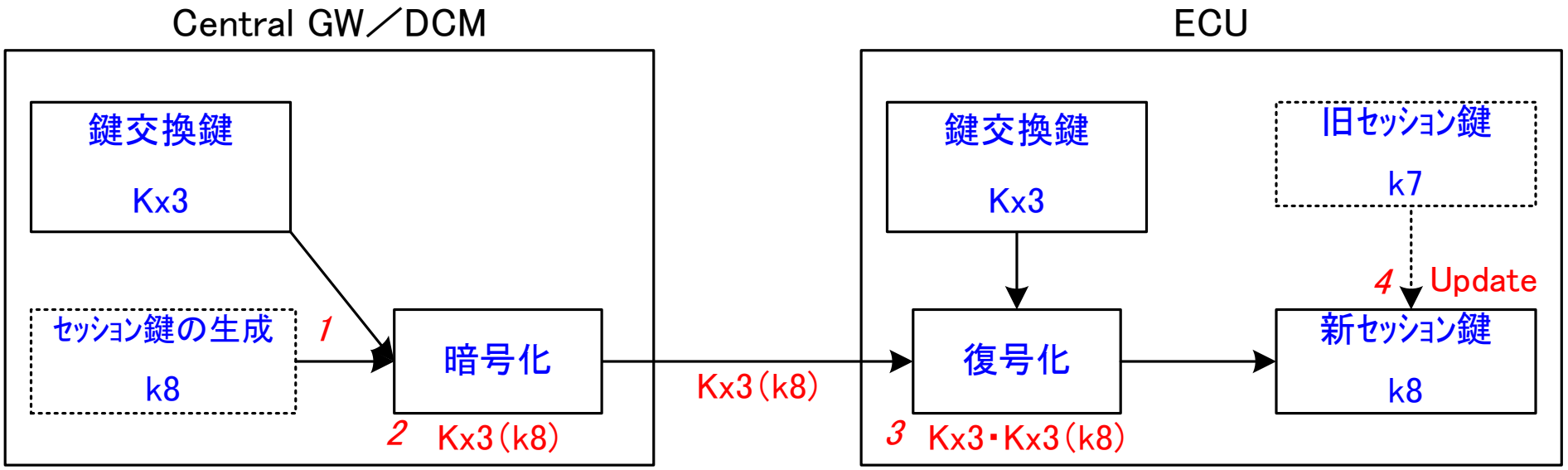
- Central GW／DCMは、一定の間隔で鍵交換鍵を生成する。
- Central GW／DCMは旧鍵交換鍵で、新鍵交換鍵を暗号化して、ECUへ配信。
- ECUは、旧鍵交換鍵で復号し、新鍵交換鍵を取り出す。



一度鍵交換鍵が漏洩すると、その後に生成される鍵交換鍵もモニタされる。
⇒ 鍵交換鍵を多層化しても良い。尚、セッション鍵とで2階層になっている。

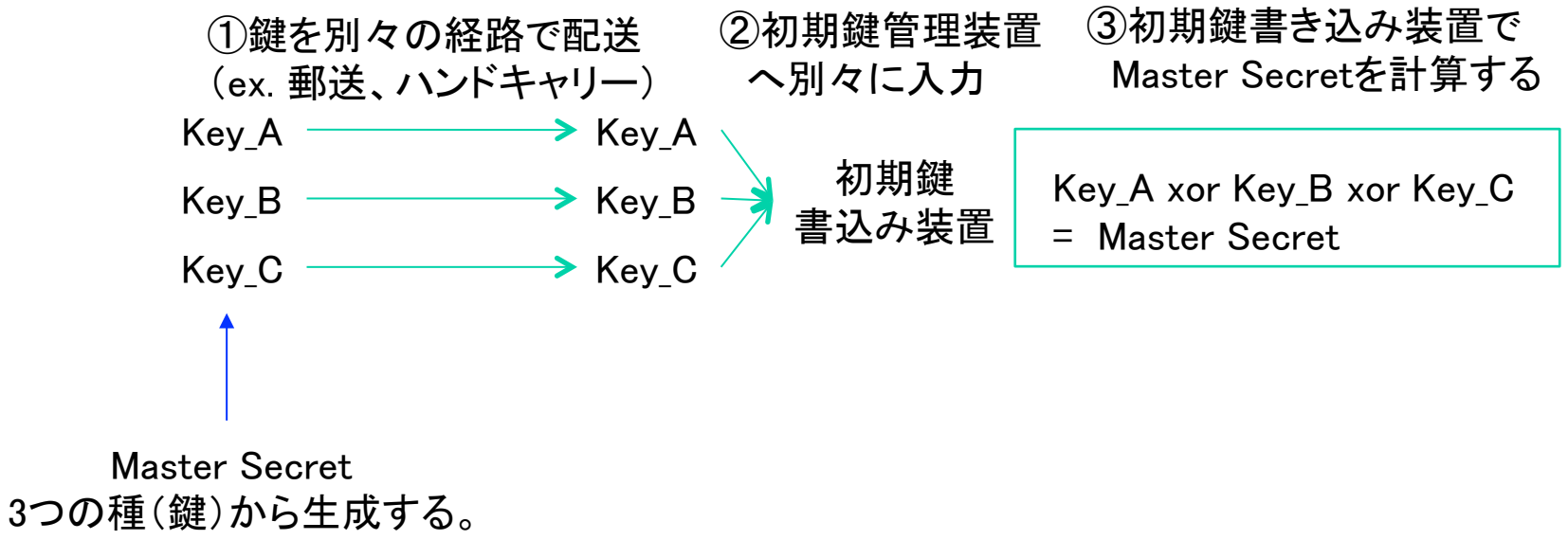
(3)セッション鍵の更新

- Central GW／SIMは、一定の間隔で セッション鍵を生成する。
- Central GW／SIMは鍵交換鍵で、セッション鍵を暗号化して、ECUへ配信。
- ECUは、鍵交換鍵で復号し、セッション鍵を取り出す。



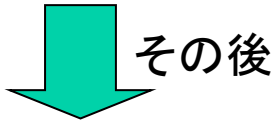
（4）Master Secretの安全な共有

- Master Secretの安全な共有の一例
  - 「初期鍵書込み装置」や「初期鍵管理サーバ」などとMaster Secretを安全に共有する手法を以下に示す。



（4）Master Secret漏洩時への対応

■ Master Secretの失効処理
- ◆ 車外サーバ管理モデル
  - ⇒ サーバ内のMaster Secretを更新する。
- ◆ 車内高耐久SE管理モデル
  - ⇒ 全てのクルマの高耐久SE内のMaster SecretをOver the Air（OTA）などで書き換える。



■ 初期鍵の更新
- ◆ 漏洩したMaster Secretで生成されたECUの初期鍵を更新する。
  - ⇒ ECU認証済：高耐久SEからECUへ新たな初期鍵を通知。
  - ⇒ ECU認証前：ECUを回収して、新初期鍵を埋め込む。

部品交換に関する考察

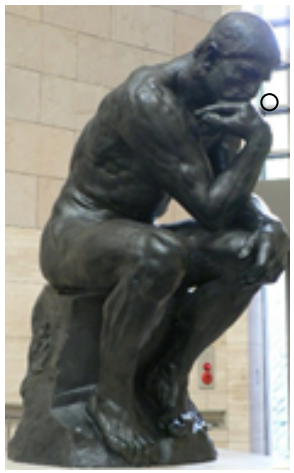
■ ECUの交換
- ◆ 新品ECUの鍵交換鍵を”0”値（未設定）にして、（1-2）から実施すれば良い。
- ◆ 廃車の中古ECUを再利用する際は、鍵交換鍵に何らかの値が入っている。
  - ⇒ ECU_IDを初期鍵配信サーバに問い合わせ*、盗難車のECUかを確認する。
    - ⇒ 正規の廃車からのECUであれば、（1-2）から実施すれば良い。

■ 高耐性SEの交換
- ◆ 新品高耐性SEの鍵交換鍵を”0”値（未設定）にして、（1-2）から実施すれば良い。
- ◆ 廃車の中古高耐性SEを再利用する際は、鍵交換鍵に何らかの値が入っている。
  - ⇒ 高耐性SE_IDを初期鍵配信サーバに問い合わせ*、盗難車かを確認する。
    - ⇒ 正規の廃車からの高耐性SEであれば、（1-2）から実施すれば良い。

＊その場での確認（1-2’）でも、ネットワーク接続されるタイミングでも構わない。

セキュアエレメントを基点とした車載制御システムの保護
–要素技術の整理と考察–

KDDI研究所　竹森敬祐

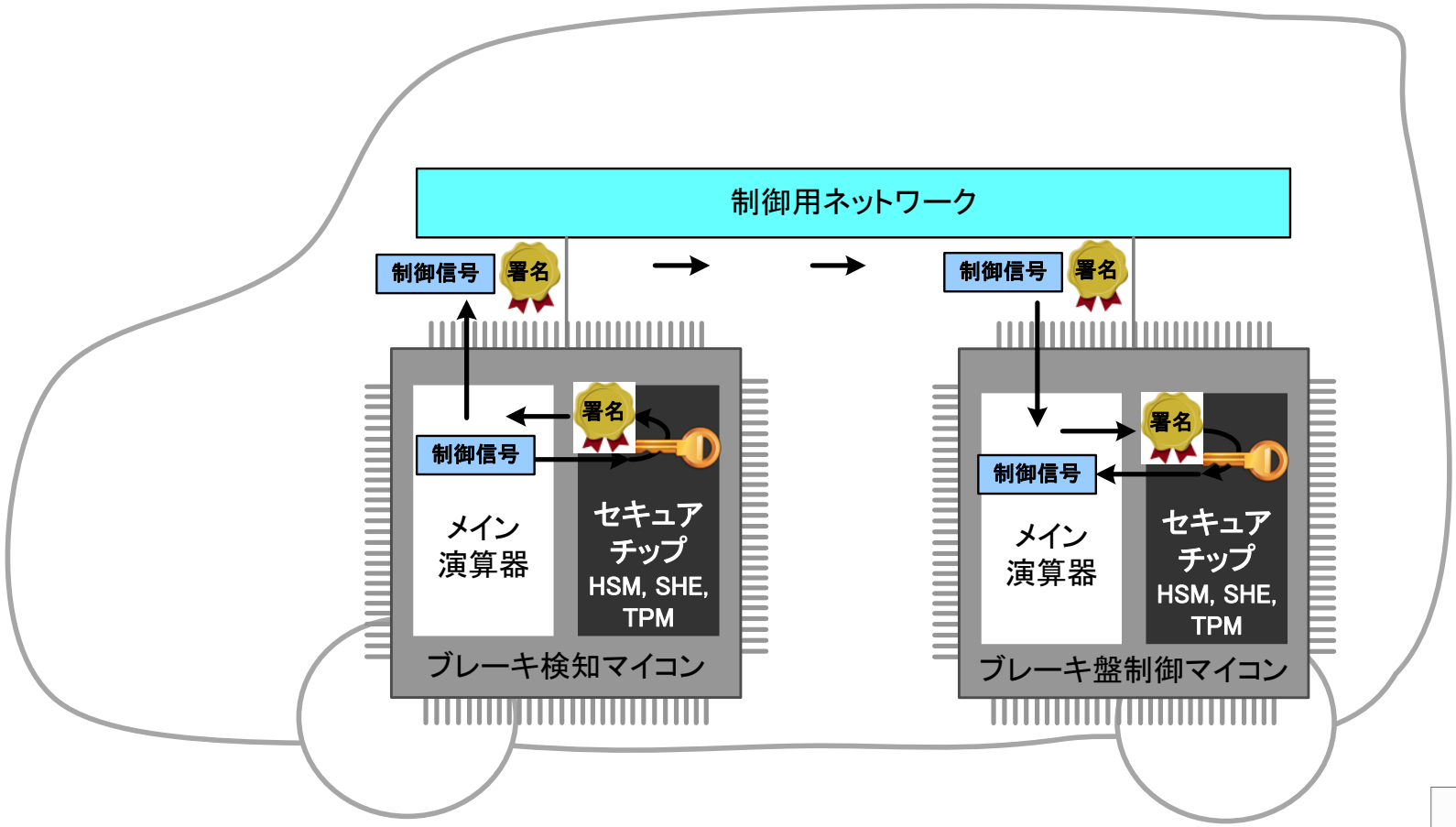


ハッカー視点で狙いどころを考え、セキュアエレメントの導入で、根本解決を目指す。

- セキュリティとは
- インシデントの収集・分析
- 対策に関する基礎技術
- 鍵管理の一例
- **CANパケット認証、ECUのセキュアブート**
- リモートリプログラミング

CANパケットへのMAC付与

- CMAC（データ、秘密の共有情報、パケットカウンタ）の付与
  - データの完全性、送信元の認証、リプレイ阻止を担保する。
  - HSM内で生成・検証することで、高速性と安全性を担保する。

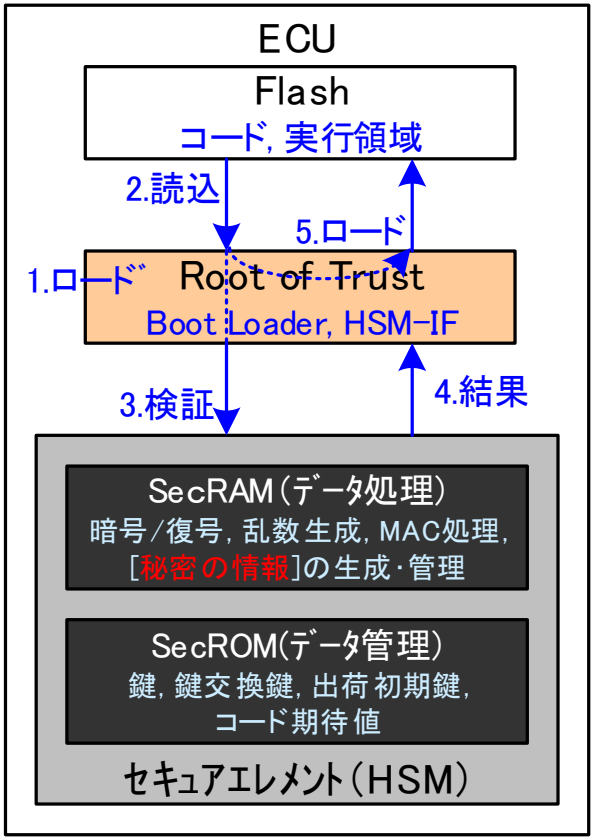


KDDI R&D LABS

（1）ECUのセキュアブート

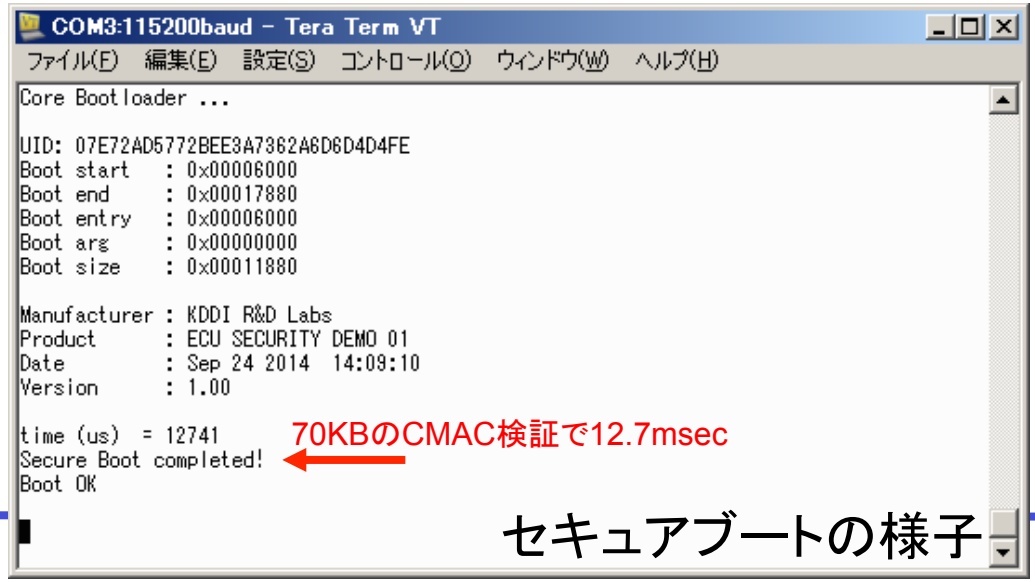
■ ECUの構成要件

- セキュアブートの基点となるRoot of Trustに、Boot Loaderを組み込む。
- 安全な情報管理領域（Secure ROM）と、安全な情報処理領域（Secure RAM）からなるHSM（セキュアエレメント）で、ハッシュ値（CMAC）比較を行う。



■ 署名検証方式のセキュアブートの流れ

Step 0) ROM化（Root of Trust）されたBoot Loaderを起動する。
Step 1) Boot Loaderは、Flashメモリから制御コードを読み込み、制御コードのハッシュ値（CMAC）を算出する。
Step 2) ハッシュ値とセキュアエレメント内のコード期待値と比較する。
Step 3) 一致した場合には、検証OKとして、Boot Loaderに通知する。
Step 4) Boot Loaderは、読み込んだ制御コードをRAMに展開する。



セキュアブートの様子

KDDI R&D LABS

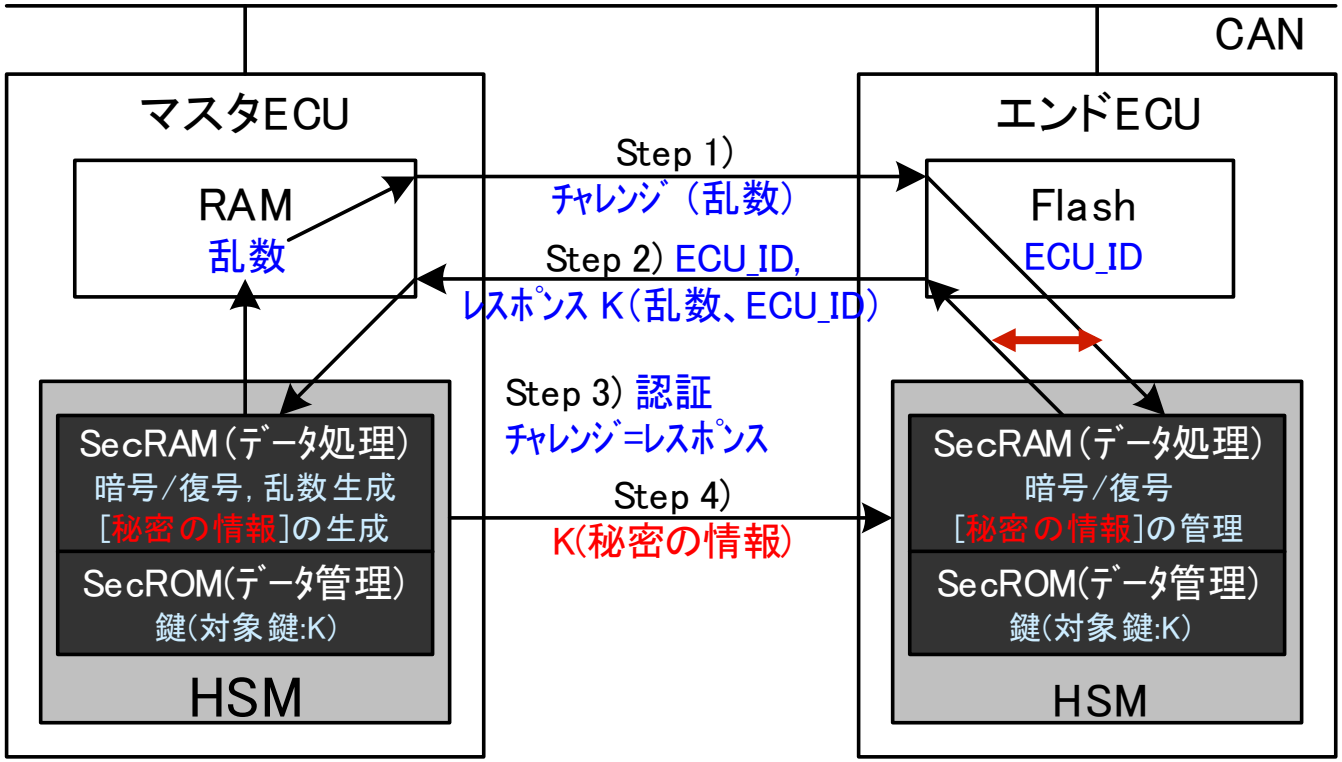
(2)マスタECUからエンドECUの認証

■ チャレンジレスポンスによるECU認証

◆ システム起動時に、マスタECUからエンドECUをチャレンジレスポンスで認証。

⇒ 認証用の鍵の管理、暗号・復号処理は、HSM(セキュアエレメント)で実施。

注) 実装では、エンドECU(RH850F1L)間の相互認証



【評価】

1 block (16 bytes)

AES128暗号処理

39.4 μs

AES128復号処理

39.7 μs

ラウンドトリップ遅延

2.4ms

KDDI R&D LABS

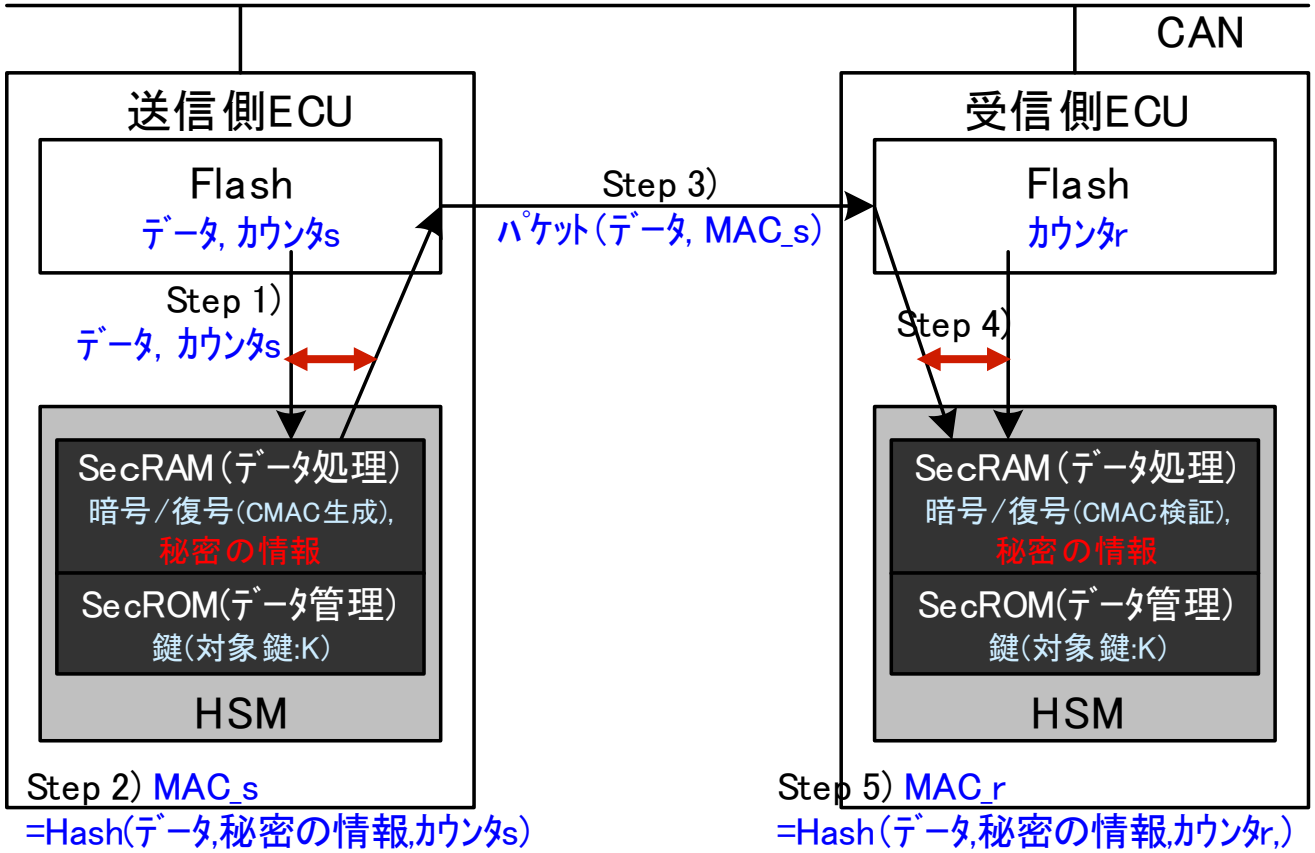
(3)MACによるCANパケット認証

■ CANパケット認証

◆ RAMでカウンタ値を管理しておき、セキュアエレメントに渡す。

◆ CMAC(データ、秘密の情報、パケットカウンタ)をHSMで算出する。

注) 実装では、セキュリティ要求の高いECU間でのみMAC付与すれば良い。



【評価】

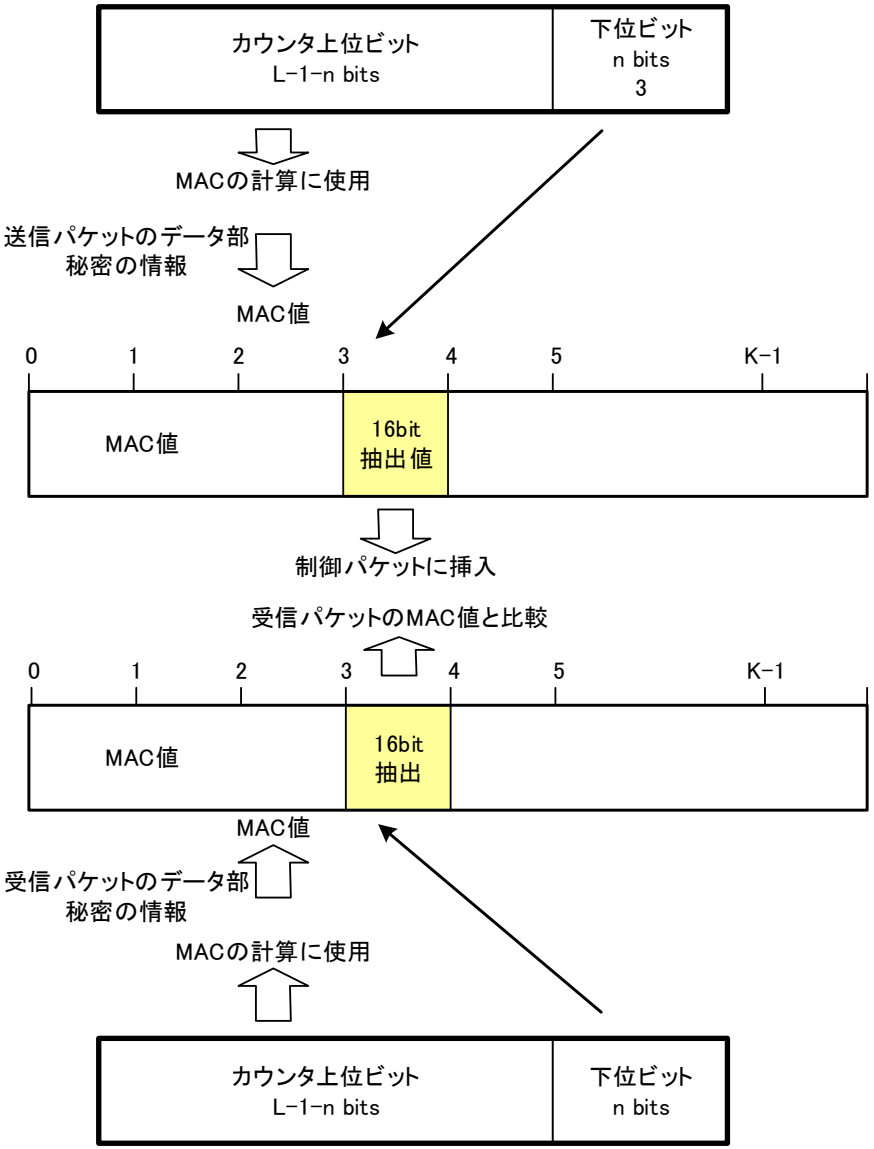
1 block (16 bytes)

CMAC(AES128)計算

42.1 μs

KDDI R&D LABS

詳細）MACによるCANパケット認証



■ 送信側

◆ カウンタ上位｜下位　に分離。

⇒ 上位ビットでCMAC(AES128) を算出。

hash（送信データ、秘密の情報、上位ビット）

◆ カウンタ下位の値で分割位置を抽出。

⇒ 抽出された16ビットをCANに挿入

■ 受信側

◆ 同じアルゴリズムで、CMAC(AES128)を算出。

hash（抽出データ、秘密の情報、上位ビット）

◆ カウンタ下位の値で分割位置を抽出。

⇒ 抽出された16ビットを比較

詳細）MACによるCANパケット認証

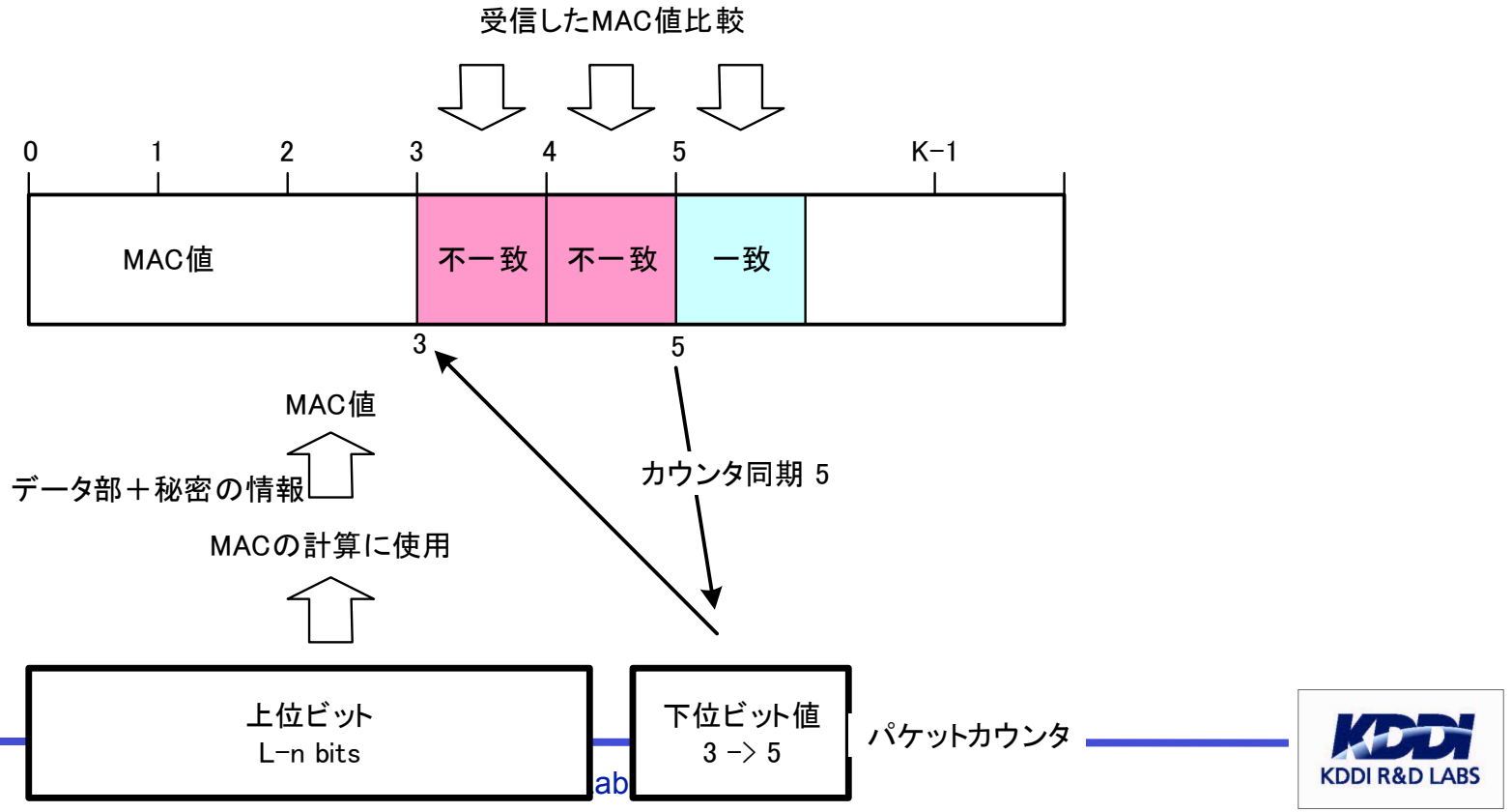
■ 16フレーム内同期外れの補正

◆ 受信側でMAC値が不一致だった場合、+1ずつフレームを比較していく。

◆ フレーム終端（K-1）まで比較して不一致だった場合、上位ビットを+1インクリメントしてCMACを再計算。そして、下位ビット値-1まのフレームまで比較。

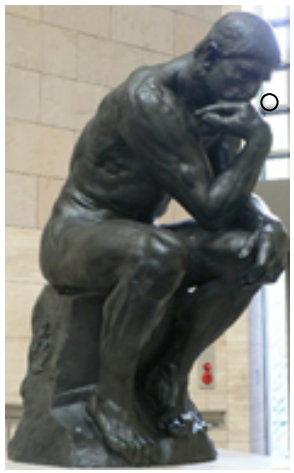
⇒ 一致フレームが有れば、カウンタ同期を図り、パケット受け入れ。

⇒ 一致フレームが無ければ、リプレイ攻撃／改竄の可能性があり、異常処理へ。



セキュアエレメントを基点とした車載制御システムの保護
–要素技術の整理と考察–

KDDI研究所　竹森敬祐



ハッカー視点で狙いどころを考え、セキュアエレメントの導入で、根本解決を目指す。

- セキュリティとは
- インシデントの収集・分析
- 対策に関する基礎技術
- 鍵管理の一例
- CANパケット認証、ECUのセキュアブート
- リモートリプログラミング

KDDI R&D LABS

2015/5/27 ワイヤレスジャパンでリモート・リプロ発表

■ 日経テクノロジーOnline
http://techon.nikkeibp.co.jp/article/NEWS/20150527/420381/?rt=nocnt

HOME > ニュース > クルマのセキュリティーはSIMにおまかせ、KDDI研が新技術

車載部品＆ネットワーク　クルマ

新産業
- Social Device
- デジタルヘルス
- 航空・宇宙
- ビッグデータ
- ロボット
- 3Dプリンター
- ウエアラブル
- リアル開発会議
- 5G

コンテンツ
- ニュース

ニュース　▸ニュース一覧へ

クルマのセキュリティーはSIMにおまかせ、KDDI研が新技術

中道 理　2015/05/27 20:38

いいね！ 2　ブックマーク　印刷

2015年5月27日、KDDI研究所は、悪意ある攻撃から自動車の制御系ネットワークを守る仕組みを開発したことを明らかにした。東京ビッグサイトで開催中の「ワイヤレスジャパン2015」の基調講演においてKDDI 商品・CS統括本部 プロダクト企画本部長の小林昌宏氏が明かした。

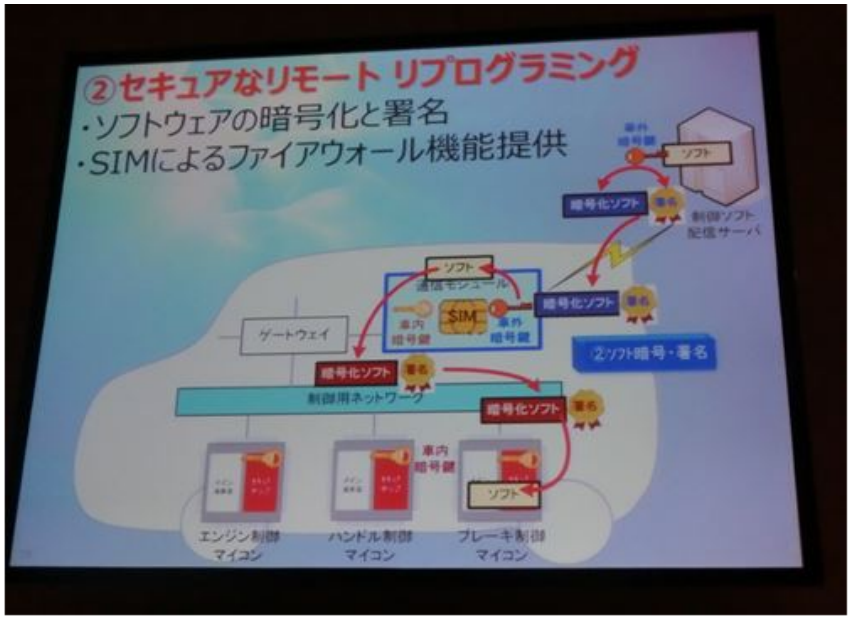


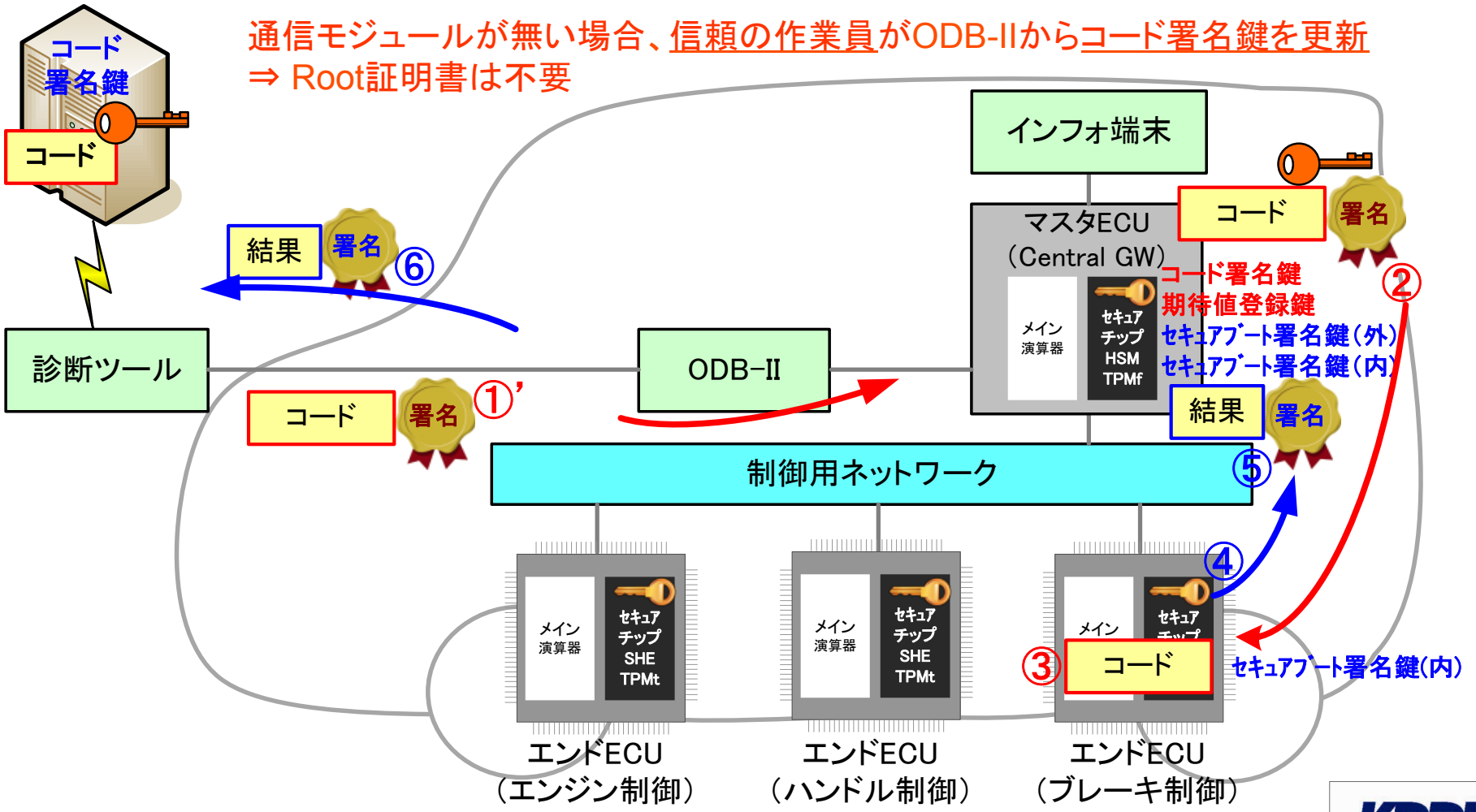
図5　セキュアなリモート リプログラミング
[画像のクリックで拡大表示]

「（自動車のネットワーク化を含めて）IoT時代にはプライバシーとセキュリティーがポイントとなる。今後、SIMを、さまざまなIoTデバイスのトラストアンカーとしたい」（小林氏）とした。なお、トラストアンカーとはセキュリティーを制御・統括する役割を指すようだ。今後は実証試験などを通じて、この仕組みが実環境で動作することなどを確認していきたいとしている。

KDDI R&D LABS

直近のリプロ

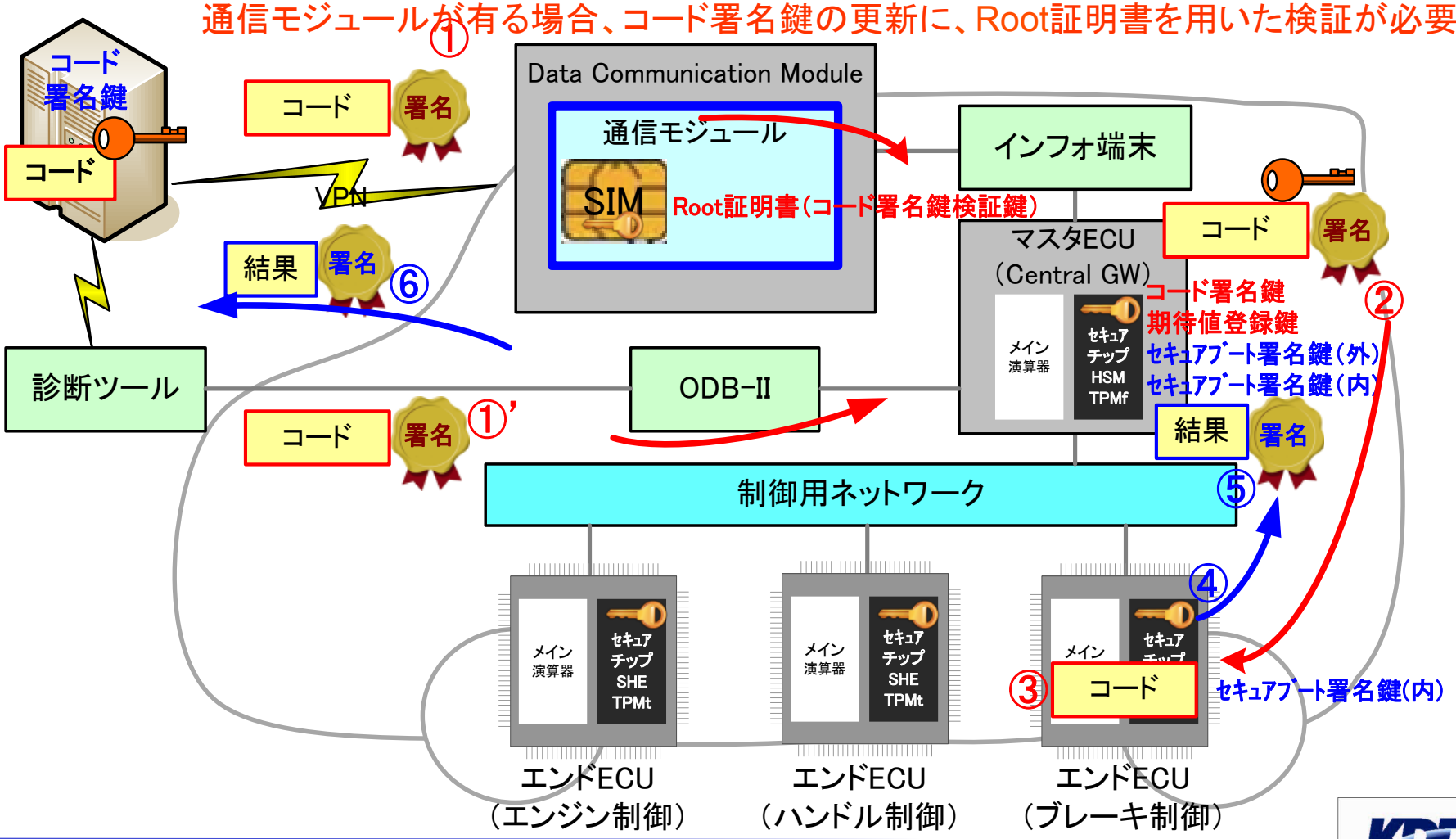
①～③ DCM経由 or ODB-II経由で、コードがCentral GWに届き、署名検証を行う。
④～⑥ コードと期待値を適用し、セキュアブート結果にCentral GWで署名を付し返信する。



中期　リモート・リプロ

①～③ DCM経由 or ODB-II経由で、コードがCentral GWに届き、署名検証を行う。
④～⑥ コードと期待値を適用し、セキュアブート結果にCentral GWで署名を付し返信する。

通信モジュールが有る場合、コード署名鍵の更新に、Root証明書を用いた検証が必要



デモ