IoT時代のセキュリティについて考える

KDDI研究所　溝口　誠一郎

今回のテーマ

IoT進展に伴う

様々なセキュリティ面の問題点

こういったレポートがあります

http://www.jnsa.org/seminar/nsf/2015/data/A1_kabuomori.pdf

JNSA

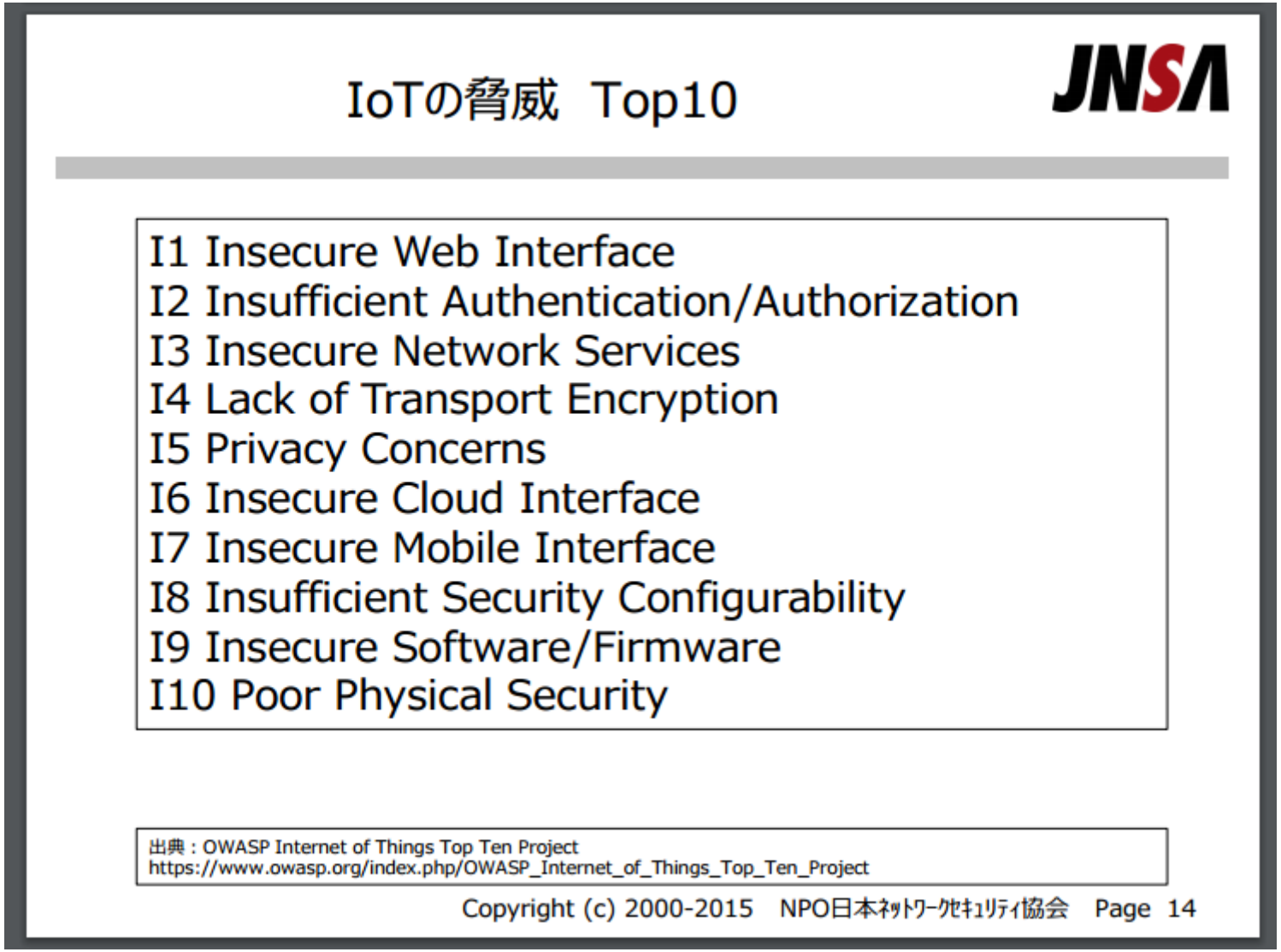
NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

IoTのセキュリティ脅威と今後の動向

NPO日本ネットワークセキュリティ協会　IoTセキュリティWG
株式会社シマンテック セキュリティソリューションSE部
兜森　清忠

Copyright (c) 2000-2015　NPO日本ネットワークセキュリティ協会　Page 1

お役御免なのでは（汗

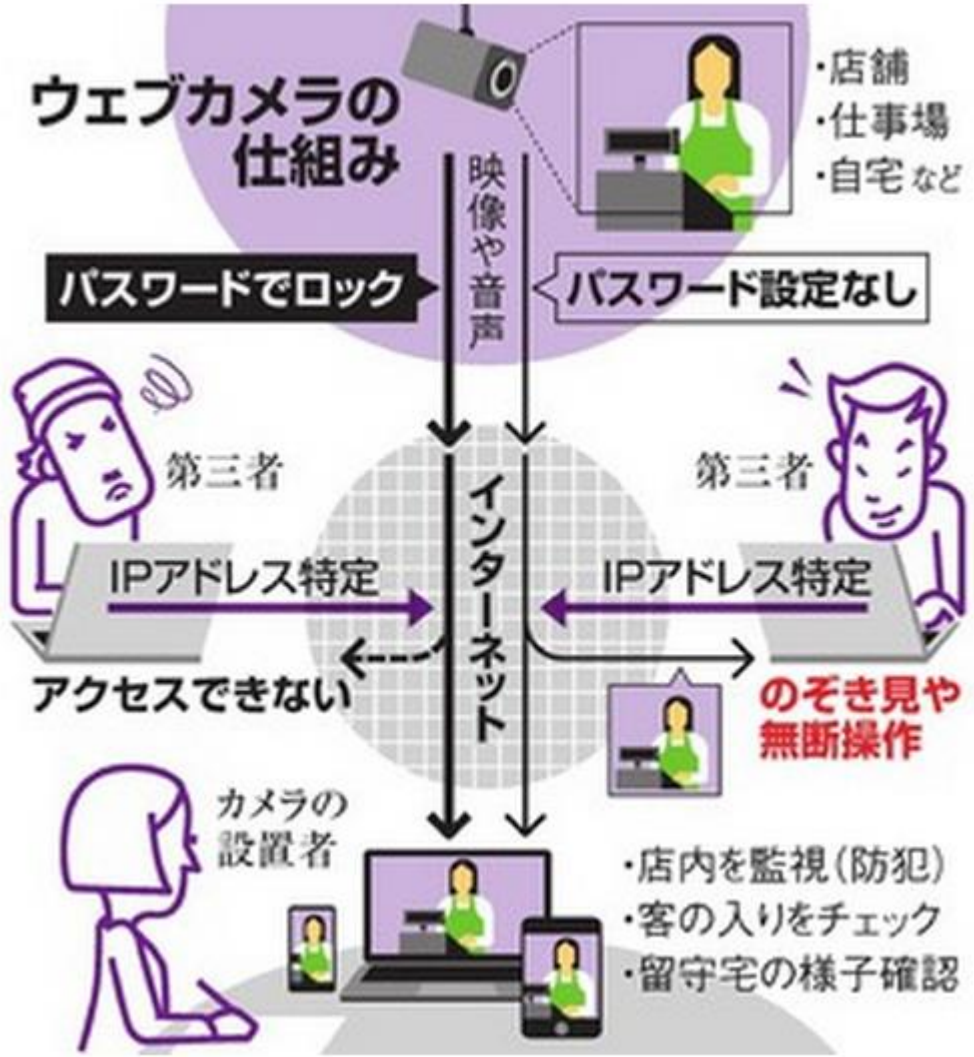

IoTの脅威 Top10
JNSA
I1 Insecure Web Interface
I2 Insufficient Authentication/Authorization
I3 Insecure Network Services
I4 Lack of Transport Encryption
I5 Privacy Concerns
I6 Insecure Cloud Interface
I7 Insecure Mobile Interface
I8 Insufficient Security Configurability
I9 Insecure Software/Firmware
I10 Poor Physical Security
出典：OWASP Internet of Things Top Ten Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project
Copyright (c) 2000-2015 NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会 Page 14

事例紹介

監視カメラへの不正アクセス

http://www.asahi.com/articles/ASH3654C1H36PTIL00W.html

2015年3月の記事



９千万以上ある。朝日新聞は昨秋以降、これらのＩＰアドレスを無作為にたどる方法で調べ、約１２５万のアドレスを抽出。先月末時点で２１６３台の ウェブカメラ がネットに接続されていることを確認した。

769台はパスワードを設定せず

先週のニュース

http://www3.nhk.or.jp/news/html/20160121/k10010380631000.html

トップページ > 社会ニュース一覧 > News Up ネットで丸見え？ 防犯カメラ

ニュース詳細

News Up ネットで丸見え？ 防犯カメラ

1月21日 18時57分

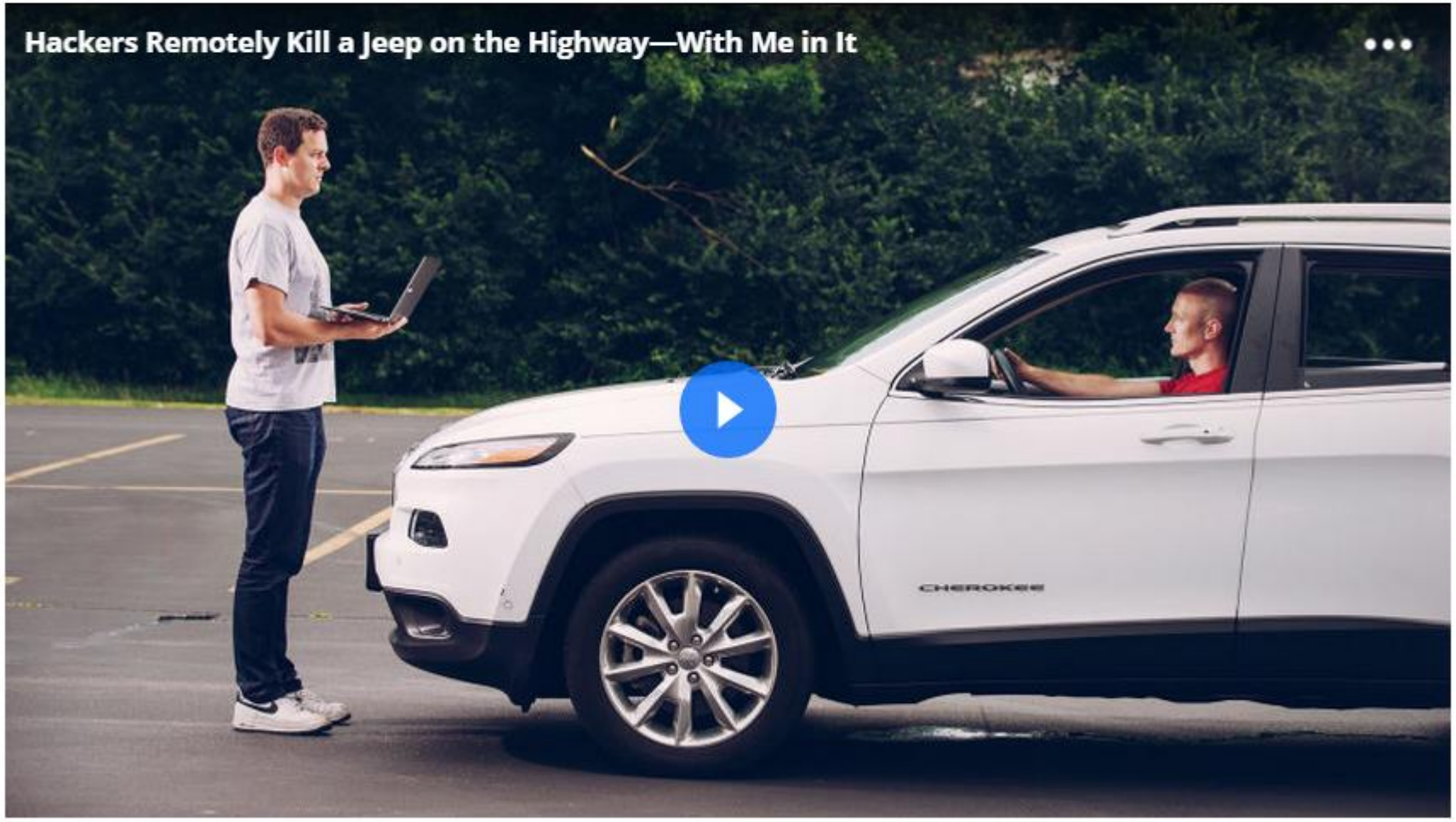
街頭や屋内のさまざまな場所に設置されている防犯カメラ。その映像がインターネットの海外のサイトで、いつでも閲覧可能になっていることが分かりました。その数は日本国内のものだけで、およそ６０００。世界全体ではおよそ２万８０００か所に及びます。なぜこのような事態が起きているのでしょうか。

パスワードが初期設定のまま

日本国内６０００か所も

街頭、オフィス、飲食店内・・・。さまざまな防犯カメラの中継映像が、海外のサイトで、いつでものぞき見ができる状態に。閲覧が可能になっているのは、世界各地の街頭や屋内に設置されているおよそ２万８０００か所の映像です。日本国内でもおよそ

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

これまで

http://wired.jp/2013/09/05/hack-a-car/

この時点では
クルマの制御システムに
物理的にアクセスする
必要があった

2013.9.5 THU

クルマの運転操作をハッキングしてみた：動画

ふたりの腕利きのハッカーが、ぞっとするデモを行った。クルマをハッキングして、ステアリング操作をすることができるというものだ。いまのところは車内からのみだが、将来は遠隔操作も可能になるかもしれない。

TEXT BY LORENZO LONGHITANO
TRANSLATION BY TAKESHI OTOSHI

WIRED NEWS(ITALIA)

しかし今回

http://wired.jp/2015/07/23/connected-car-bug/

この2人の研究者は、2013年に米国防高等研究計画局（DARPA）の資金提供を受けて自動車のセキュリティの研究を行い、多くの自動車メーカーの車両に利用しうる脆弱性があることを証明している。だが、その研究での「攻撃」は、車両への直接的な接続が必要だった。これに対して、Uconnectの脆弱性の最大の特徴は、[redacted]社の携帯電話ネットワークへの接続を利用して、事実上どこからでも車両への攻撃ができるという点にある。

もはや壁はない

やりたい放題だぜ

NEWS

2015.7.23 THU

走行中のクルマ乗っ取りに成功：「コネクテッドカー」のバグ（動画あり）

フィアット クライスラーの車載インターネット接続システムの脆弱性を利用して、ハッカーが事実上どこからでも、走行中の車両を「乗っ取れる」ことが実証された。実験の様子を動画で紹介。

いいね！ 543　ツイート 707　+1 47　B! 36

PHOTOGRAPH BY ANDY GREENBERG/WIRED
TEXT BY SEAN GALLAGHER
TRANSLATION BY KENJI MIZUGAKI/GALILEO

ARS TECHNICA (US)

http://www.bravesoft.co.jp/blog/archives/766
ニャンダフルなITプロダクト3選 & 猫向けデバイスの未来より

Internet of Thingsと私たち

OK Google

モノの**インターネット**（**Internet of Things**、**IoT**）は、一意に識別可能な「もの」が**インターネット**/クラウドに接続され、情報交換することにより相互に制御する仕組みである。「**Internet of** Everything」や「Smart Everything」、「サービスのモノ化」ともいう。「**Internet of Things**」という用語は、1999年にケビン・アシュトン（英語版）（Kevin Ashton）が初めて使った用語である。

モノのインターネット - Wikipedia
https://ja.wikipedia.org/wiki/モノの**インターネット**

フィードバック

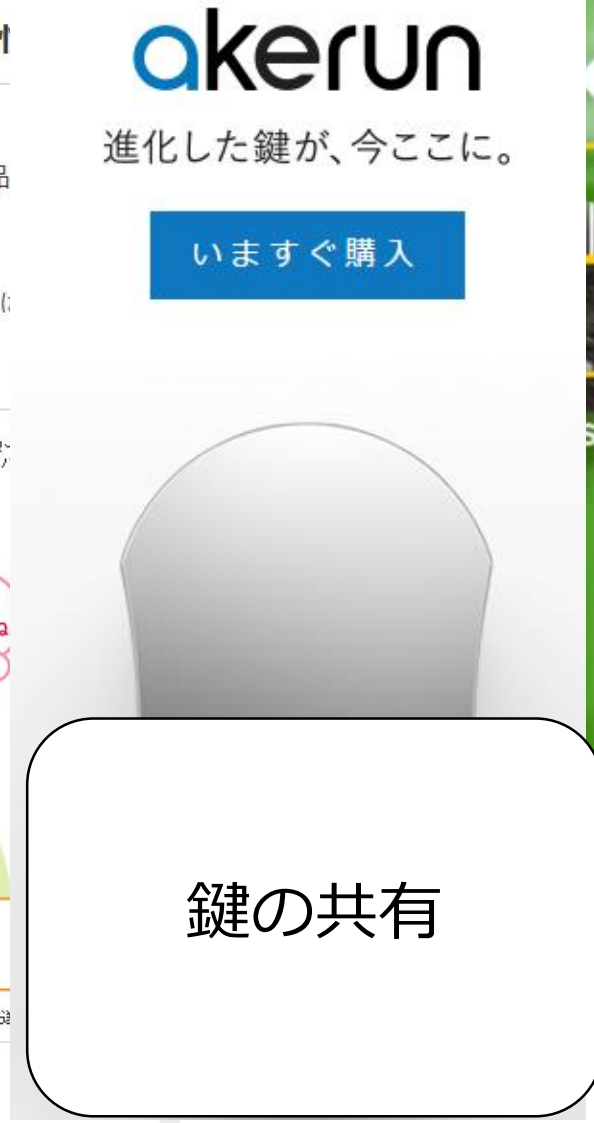
ビジネスインパクト

ガートナー	● 2020年までに300億個以上のデバイスが繋がる ● 1兆9000億ドルの経済価値
インテル	● 2020年までに500億個以上のデバイスが繋がる
シスコ	● 2020年までに500億個以上のデバイスが繋がる ● 14.4兆ドルの経済価値 ● デバイスの9割は繋がっていない

IoTの例

電気ポットの先にいる
「人」を見ている

http://ec-cube.ec-orange.jp/blogs/?p=6457



鍵の共有

https://akerun.com/

センサーの先にいる
「畑」を見ている

https://edyn.com/

IoTの例

サービスのモノ化
&
モノが通信モジュールを持ち、通信を介して制御される

電気ポットの先にいる
「人」を見ている

鍵の共有

センサーの先にいる
「畑」を見ている

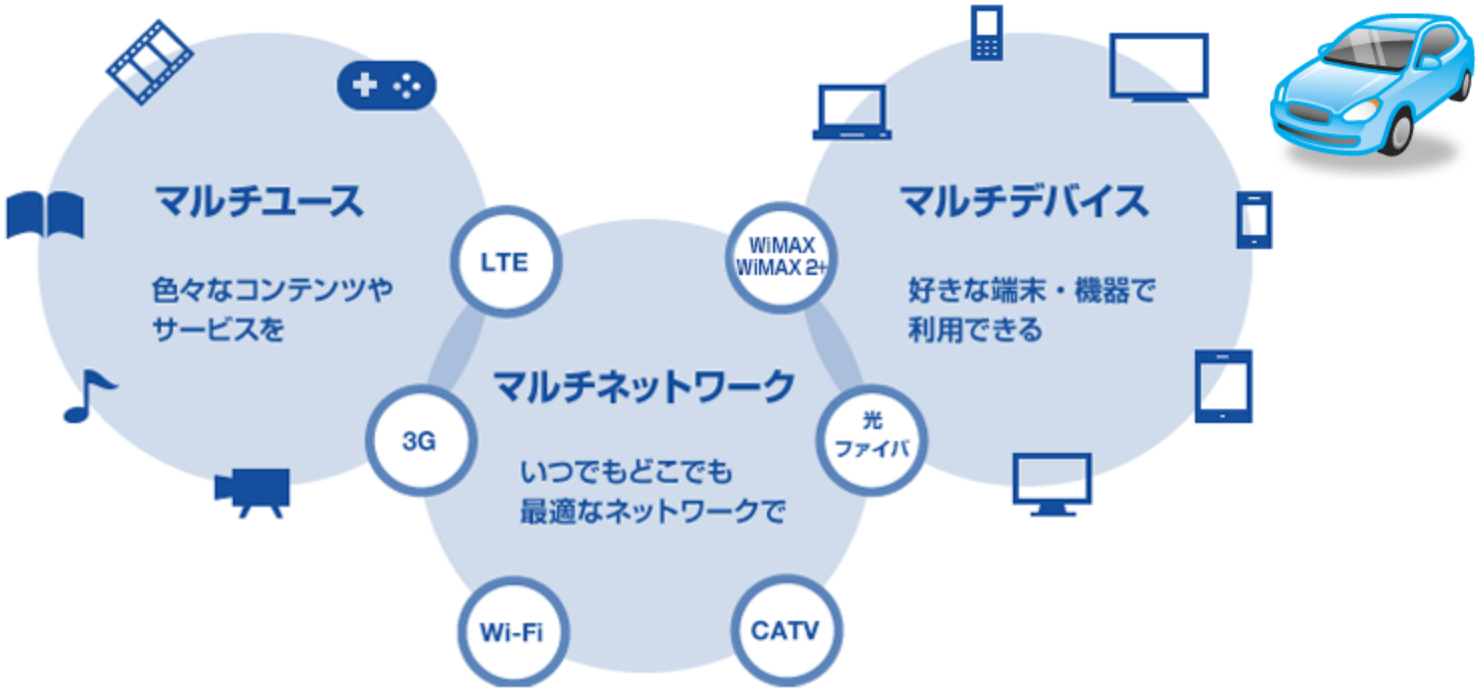
http://ec-cube.ec-orange.jp/blogs/?p=6457

https://akerun.com/

https://edyn.com/

弊社1/2

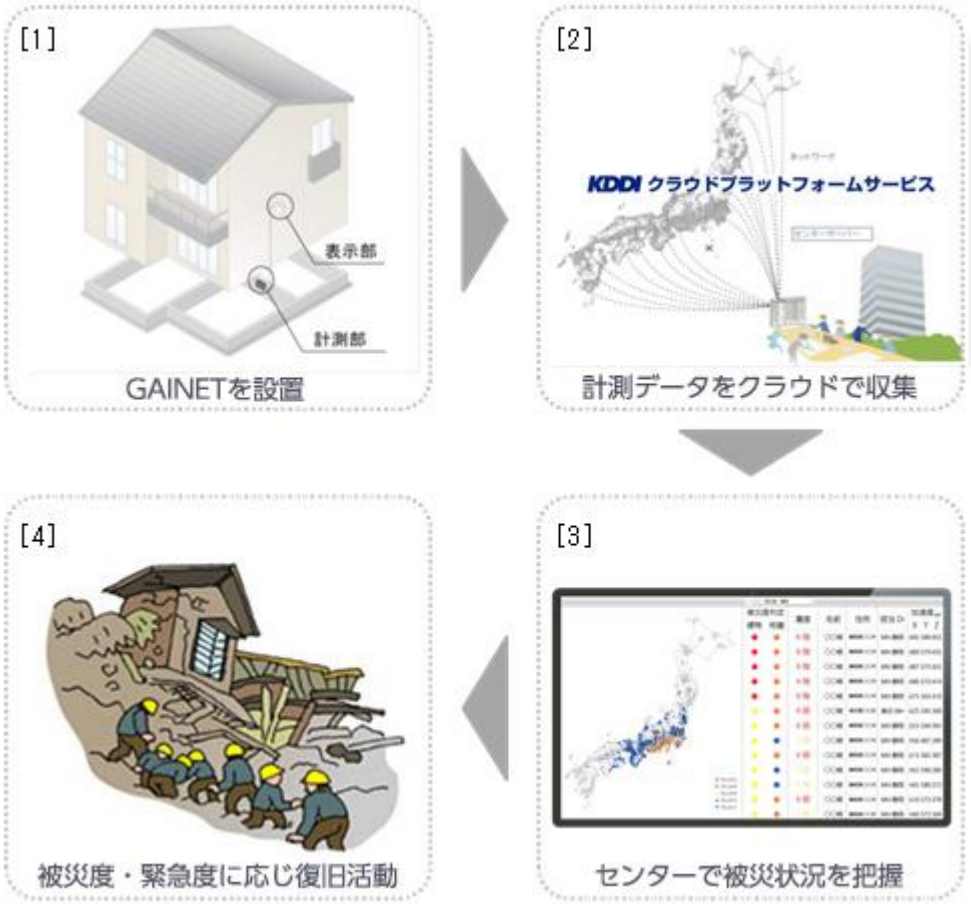
3M戦略



http://www.kddi.com/corporate/ir/individual/future/

弊社2/2

Raspberry Pi用
通信モジュール



自分で作って繋げる楽しさを
提供します

http://k-tai.impress.co.jp/docs/news/20150416_698149.html

家の安全を提供

http://news.kddi.com/kddi/corporate/newsrelease/2015/04/22/besshi1092.html

IoTに対する攻撃事例

家電乗っ取り

スパムを吐く冷蔵庫

Russia: Hidden chips 'launch spam attacks from irons'

News from Elsewhere...
...as found by BBC Monitoring

28 October 2013 Share

How Russian TV covered the story about the chips, shown inset

スパムを吐くアイロン

2014年01月21日 11時17分01秒

75万通のスパムメールは冷蔵庫・テレビ・家庭用ルーターなどを利用していることが判明

by Katie'sCameraClicks

すかさず Symantecが否定

Symantec Official Blog

Despite the News, Your Refrigerator is Not Yet Sending Spam

By: Paul_Thomas SYMANTEC EMPLOYEE

Created 23 Jan 2014

0 Comments | Translations: 日本語 | Share

You may have seen media reports based on research by Proofpoint that hundreds of home devices such as entertainment syste refrigerator had been sending spam. We refer to this collection of networked devices as the Internet of Things (IoT). Originally, th provide any evidence so we were unable to validate the claim. However, additional details have now been made available and w your IoT devices, including your refrigerator, are not the source of this recent spam run.

こんなものまで

[redacted]のトイレ操作アプリに脆弱性 - 使用中に蓋の開閉やビデが行われる恐れ

http://news.mynavi.jp/news/2013/08/05/015/

米国のセキュリティ会社であるTrustwaveは8月1日[redacted]が提供するAndroid向けトイレ操作アプリ「My SATIS」にハードコード化されたBluetooth PINの脆弱性が見つかったと発表した。

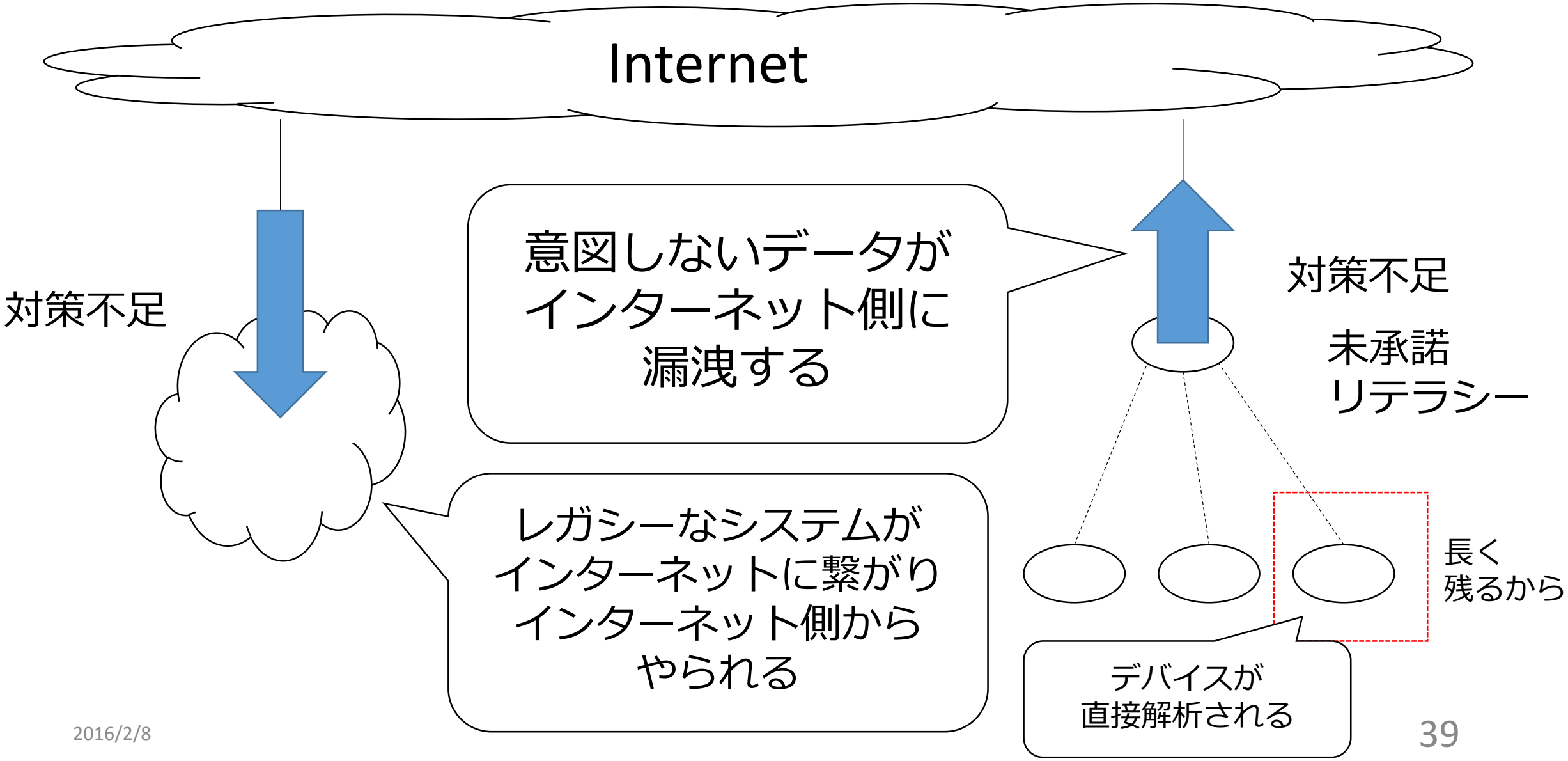
脆弱性は、同社が販売中のトイレ「SATIS」と連携を行うために利用されている
BluetoothのPINコードが「0000」固定で設定されているというもの。

この脆弱性を利用することにより、攻撃者は「My SATIS」をダウンロ
だけで、任意の「SATIS」トイレを制御できるようになる。

そのため攻撃者は、トイレ利用者が予期しないタイミングでトイレのフ
閉めすることができるほか、ビデや空気乾燥機能のオン/オフも可能とな
う。

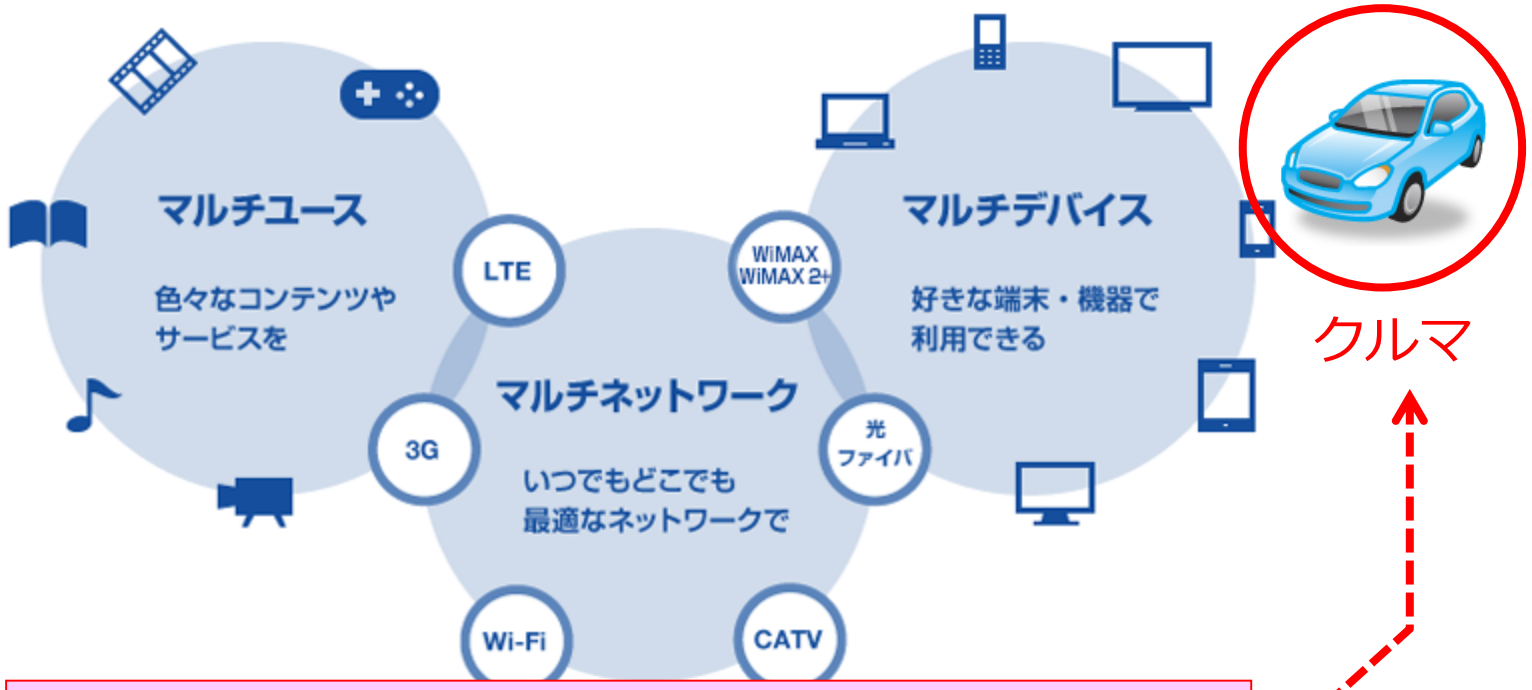
実際は、攻撃成功の条件がかなり厳しい

IoTにおける被害のパターン



繋がるクルマのセキュリティを考える

繋がるクルマについて

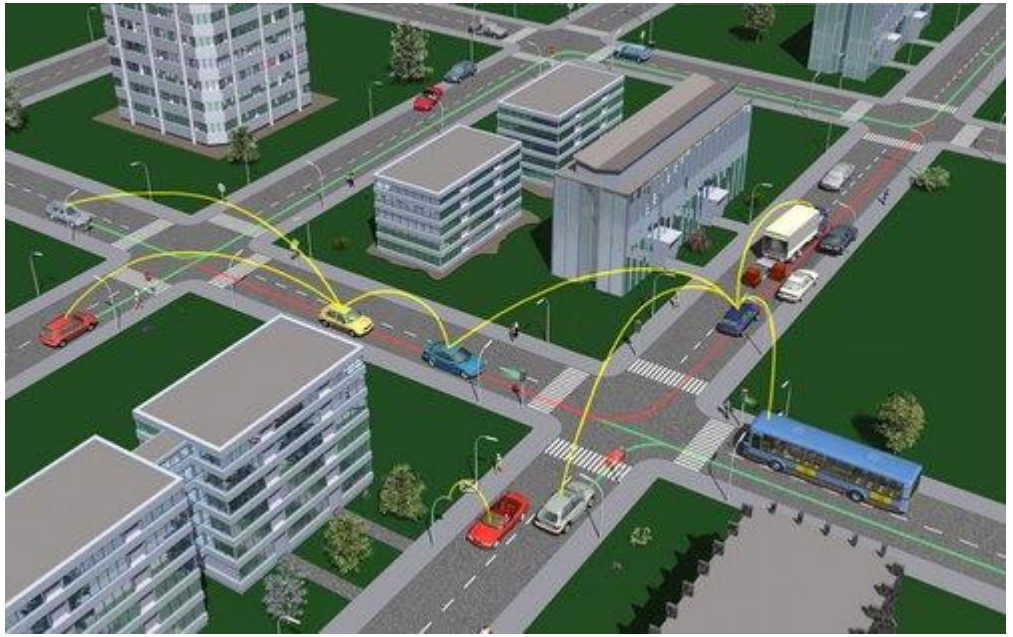


様々なモノがネットワークに繋がる
クルマも例外ではない！

コネクティッドカーの到来

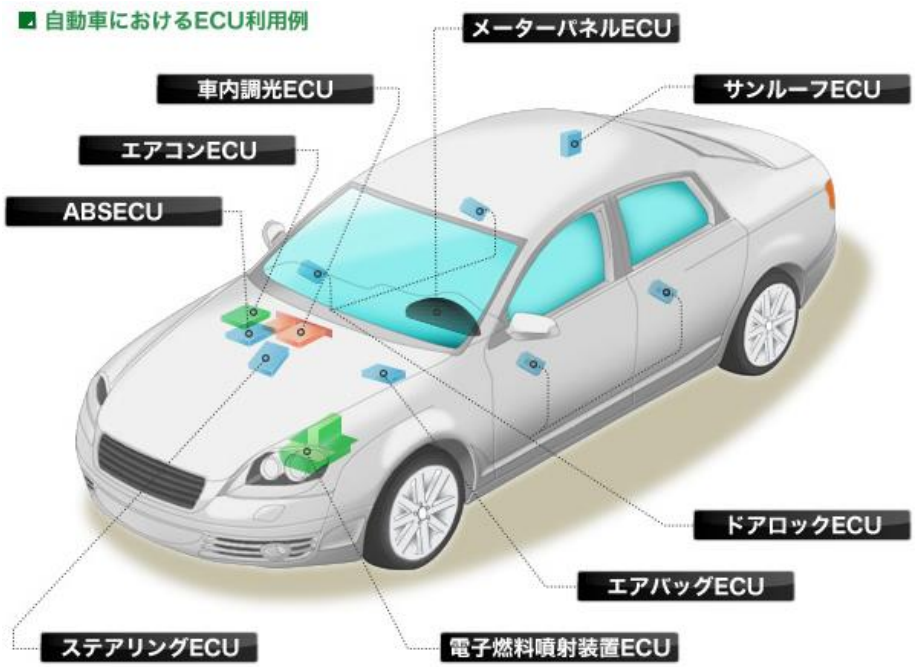
- 自動運転、先進運転支援システム（ADAS）
- V2X (Vehicle to X) ：「クルマ」と「何か」の通信

Google Self-Driving Car
https://plus.google.com/+GoogleSelfDrivingCars/about



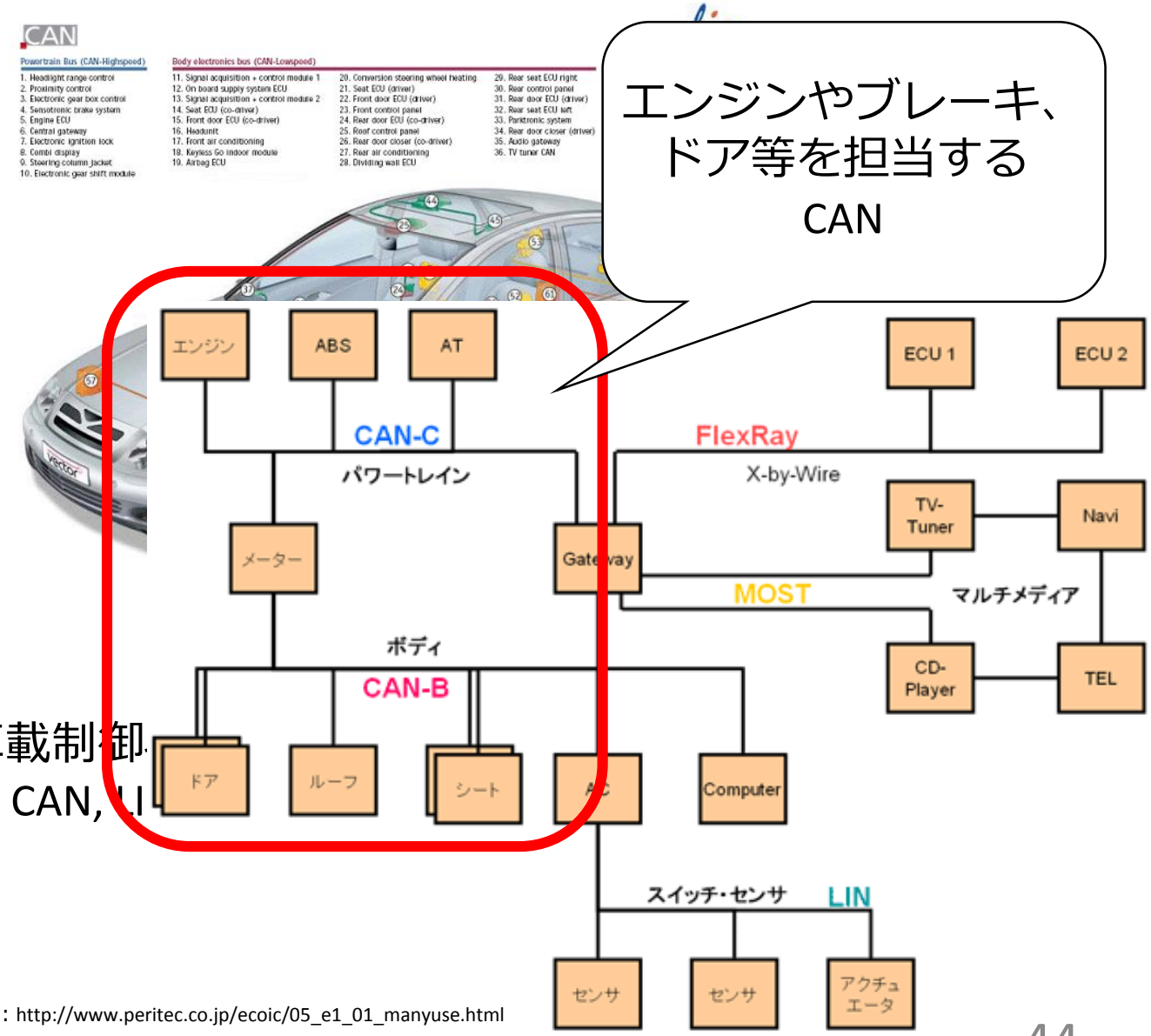
Car-2-Car Communication
https://www.car-2-car.org/index.php?id=5

コンピュータシステム化したクルマ



多数のECU (Electronic Control Unit) で構成

- 標準モデル　30～40個
- ハイエンド　100個以上



車載制御

- CAN, LI

引用：http://www.peritec.co.jp/ecoic/05_e1_01_manyuse.html

次々とアタックされる

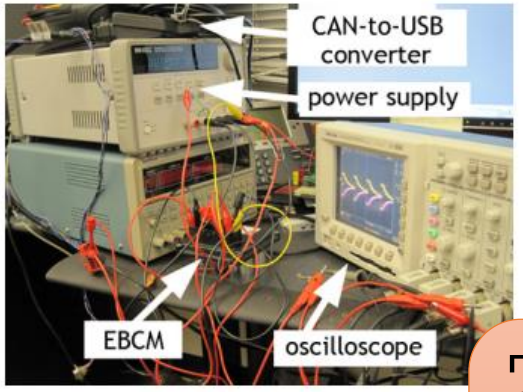
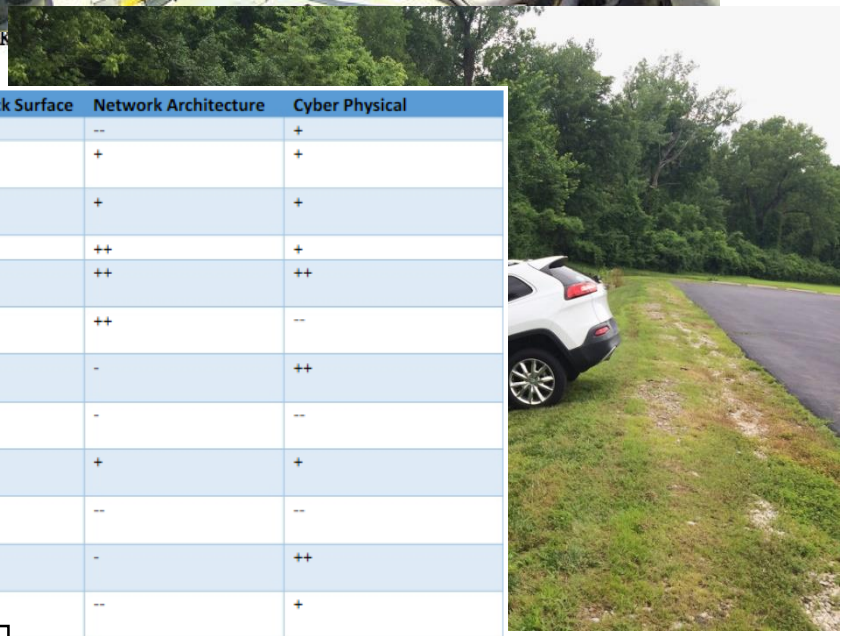
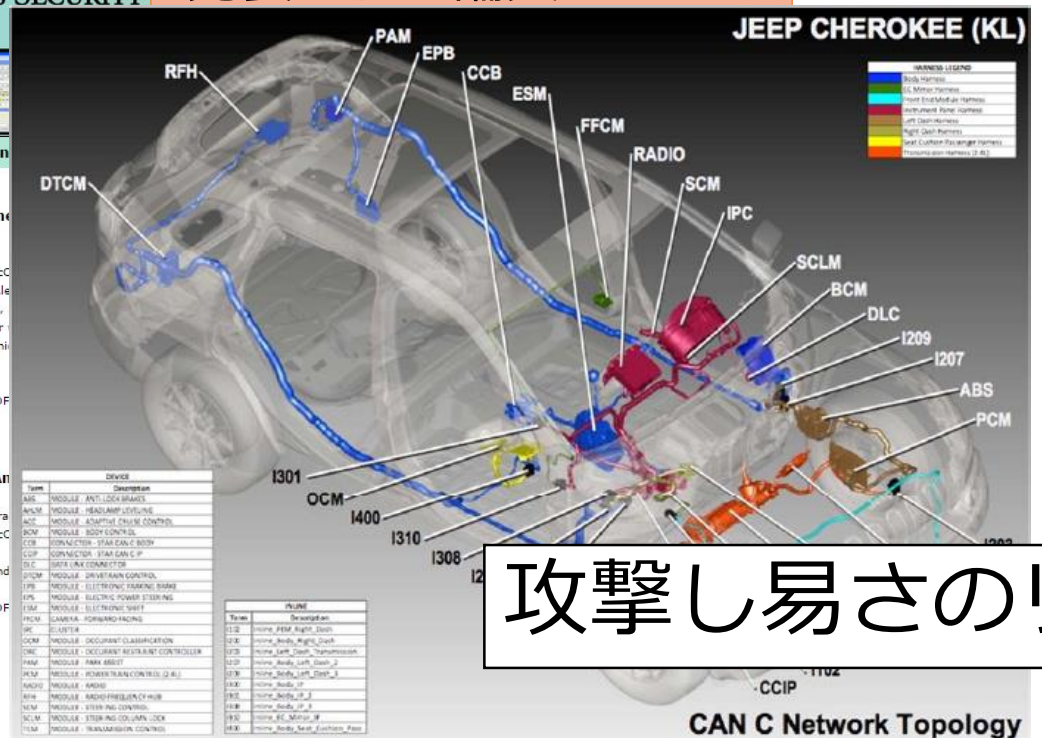


Figure 3. To test ECU behavior
controlled environment, we immobilize
car on jack stands while mounting attack

Defcon



ワシントン大学
Kohno准教授らによって
発表された論文

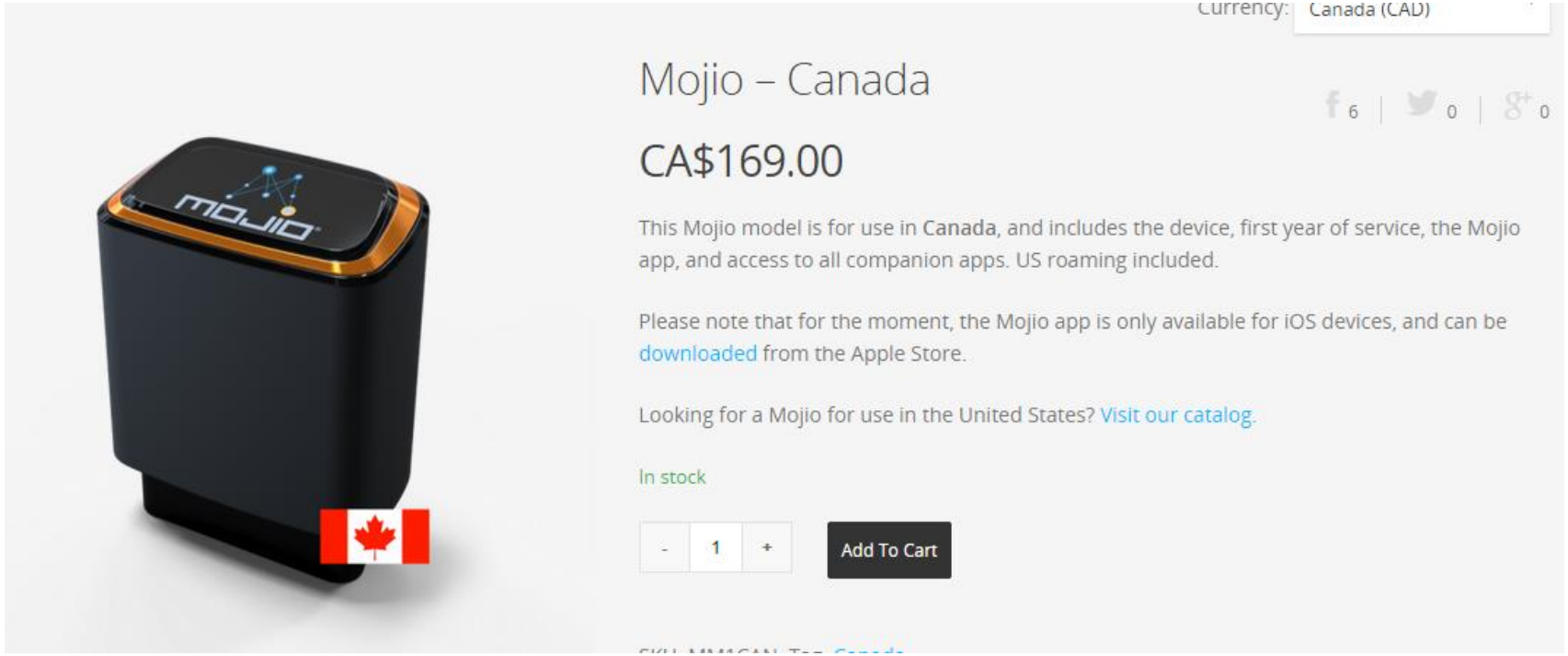


Car	Attack Surface	Network Architecture	Cyber Physical
2014 Audi A8	++	--	+
2014 Honda Accord LX	-	+	+
2014 Infiniti Q50	++	+	+
2010 Infiniti G37	-	++	+
2014 Jeep Cherokee	++	++	++
2014 Dodge Ram 3500	++	++	--
2014 Chrysler 300	++	-	++
2014 Dodge Viper	++	-	--
2015 Cadillac Escalade	++	+	+
2006 Ford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

攻撃し易さのリスト

（一方）勝手にコネクティッドしちゃう

- OBD-IIポートを活用したテレマティクス事業
  - On Board Diagnosis 2nd Generation: 自動車の自己診断機能のために用意されたポートにデバイスを接続
  - 携帯回線を使って情報をサーバにアップロード
  - 燃費、走行距離、駐車場所・時間等を記録する



OBD2デバイス

Yupiteru

SUPER CAT　レーダー探知機

■ＯＢＤ２接続時、待受表示項目は１７０項目以上！

■投稿ピン登録・投稿機能で取締り情報を登録・投稿できます。

http://www.autobacs.com/shop/g/g4968543107654

クルマの速度や回転数などをナビにわかりやすく表示

クルマから直接さまざまな車両情報を取得して、ナビゲーションにグラフィカルに表示します。

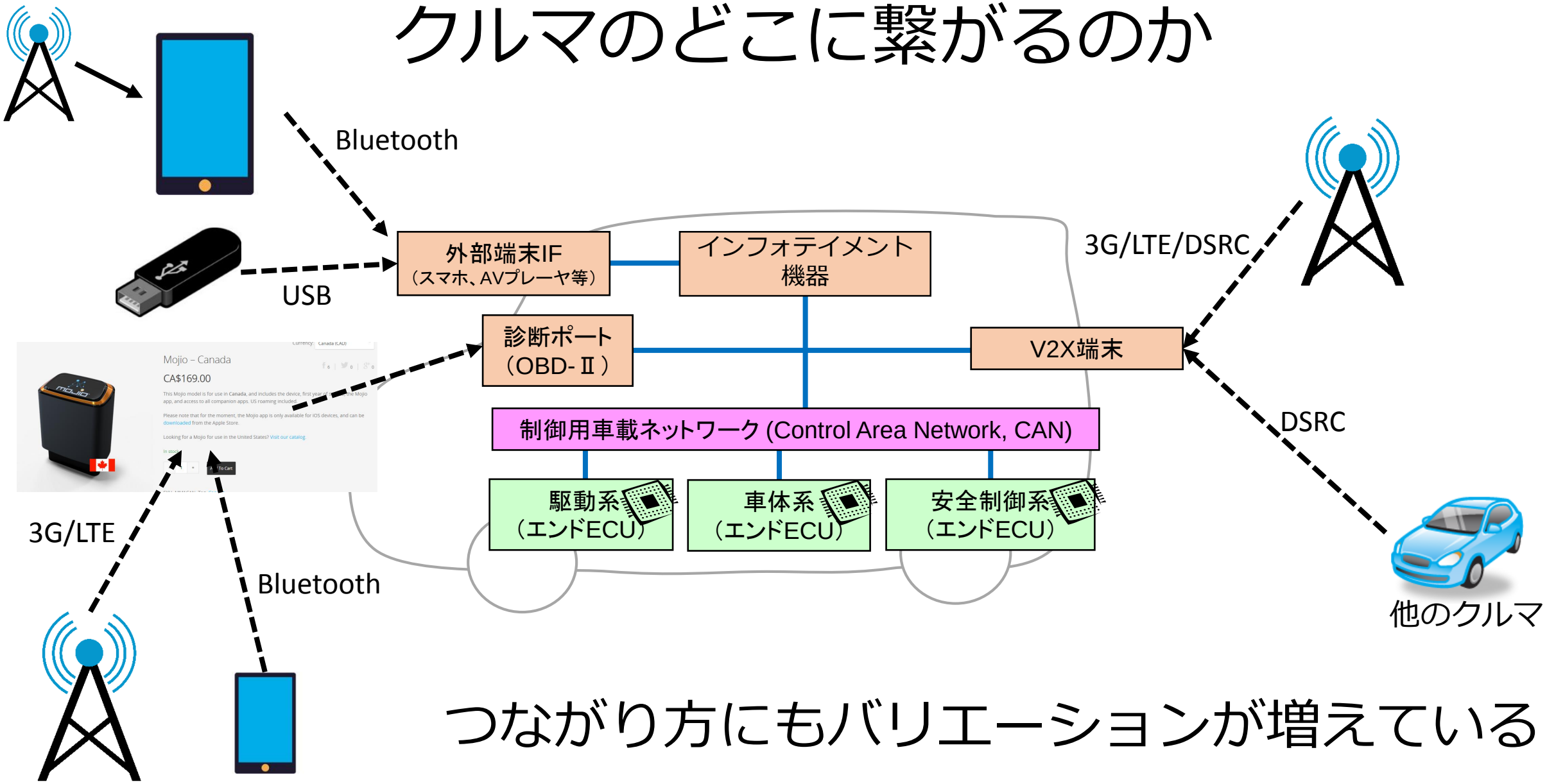
ナビに表示する車両情報

【1】MAF（吸入空気量）
【2】インテークマニホールドプレッシャー計
【3】エンジン負荷
【4】速度
【5】アクセル開度
【6】瞬間燃費
【7】平均燃費
【8】トリップメーター
【9】冷却水温計
【10】エンジン回転数
【11】電圧計
【12】時間別平均燃費グラフ

情報表示位置の確認

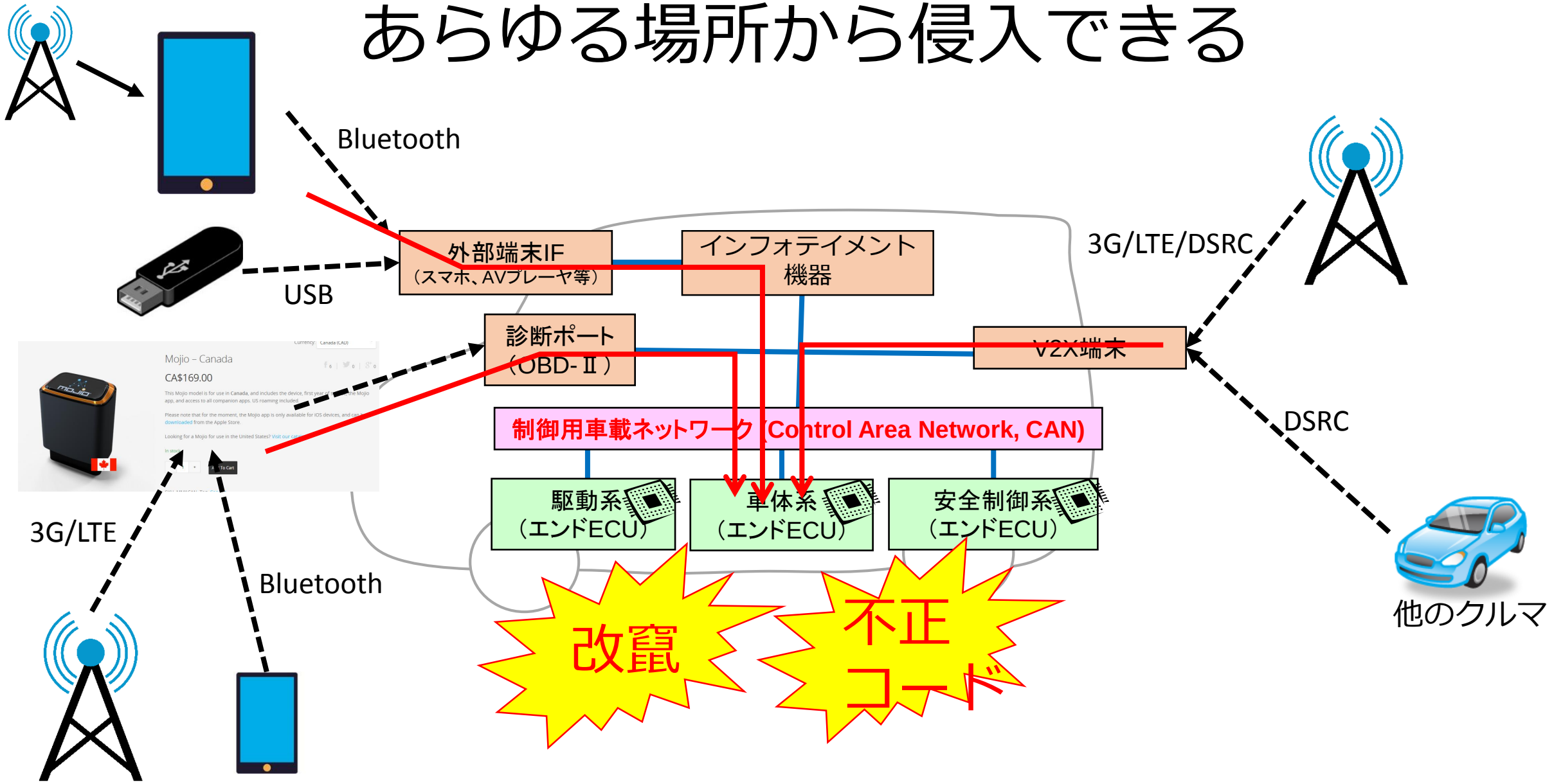
http://panasonic.jp/car/navi/products/cs10/

クルマのどこに繋がるのか

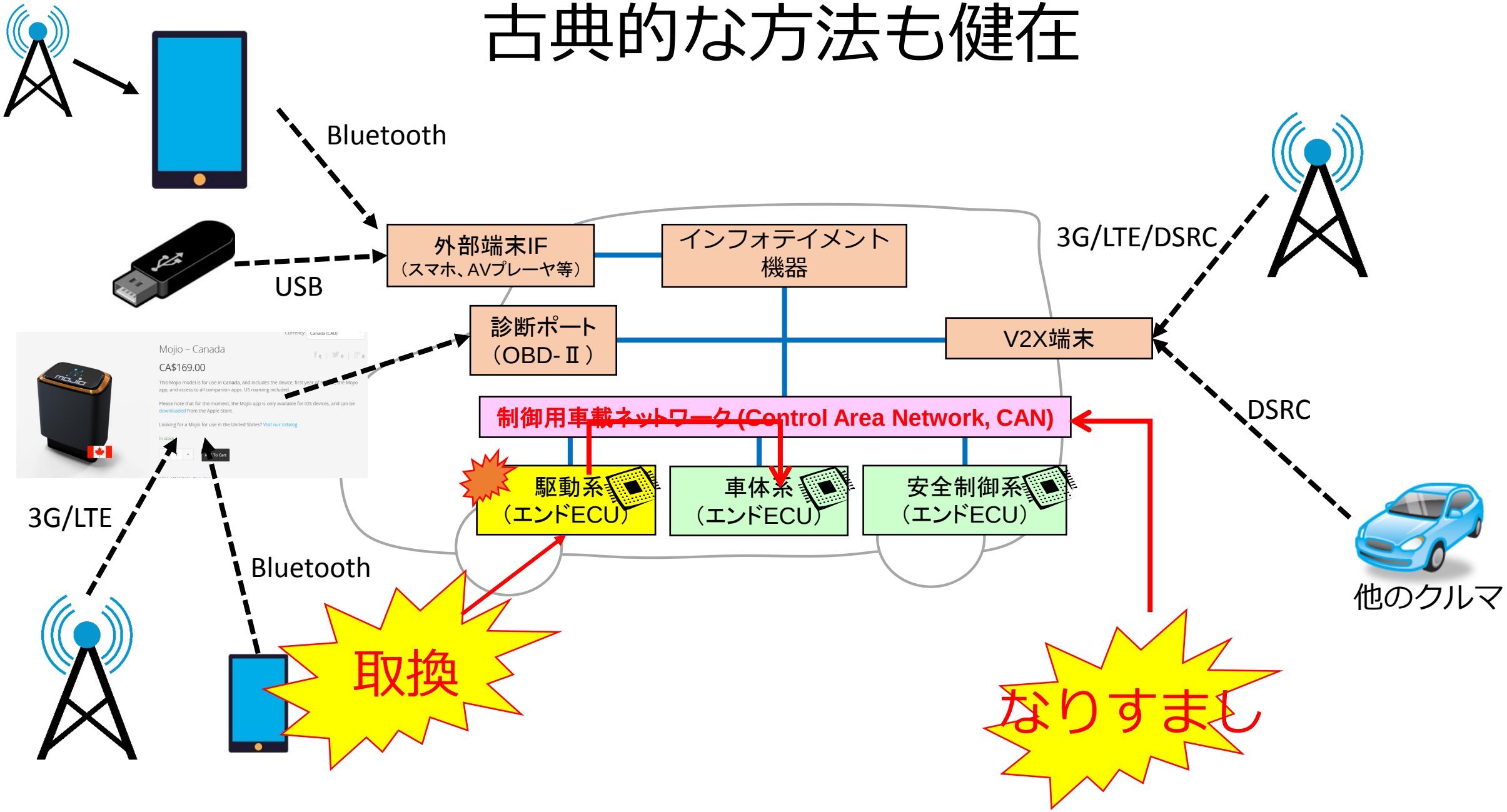


つながり方にもバリエーションが増えている

あらゆる場所から侵入できる



古典的な方法も健在


Bluetooth
USB
外部端末IF
（スマホ、AVプレーヤ等）
インフォテイメント
機器
3G/LTE/DSRC
診断ポート
（OBD-Ⅱ）
V2X端末
制御用車載ネットワーク(Control Area Network, CAN)
DSRC
駆動系
（エンドECU）
車体系
（エンドECU）
安全制御系
（エンドECU）
Mojio – Canada
CA$169.00
3G/LTE
Bluetooth
他のクルマ
取換
なりすまし

リスクへの提言

- IPA（国内）
  - 高田広章, 松本勉, “車載組込みシステムの情報セキュリティ強化に関する提言,” IPA, 2013年9月 [1]
    - 車載組込みシステムに対する攻撃リスクは3つ
- 車

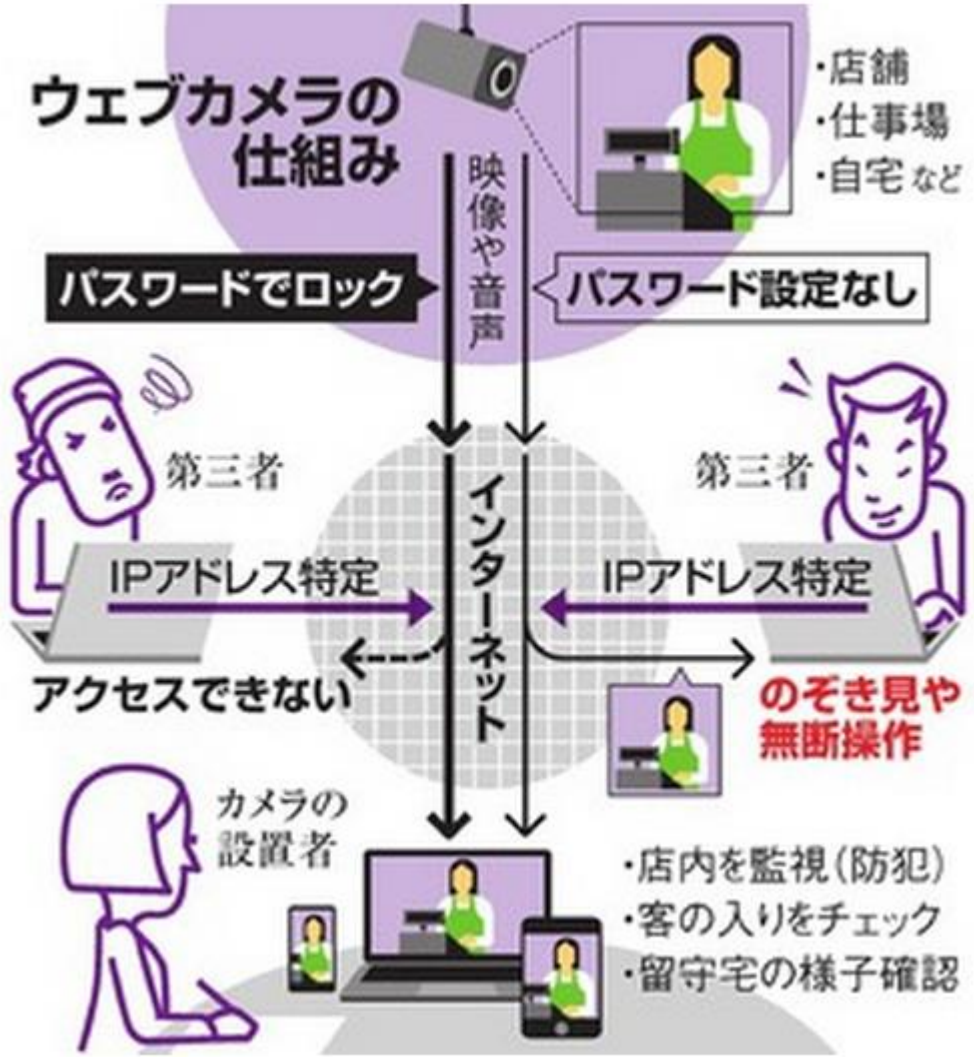
どこをどうやって守るかを整理する

[1] https://www.ipa.go.jp/files/000034668.pdf
[2] http://www.ipa.go.jp/files/000027273.pdf
[3] https://www.ccdssg.org/public/document/constitution/CCDSSG_2014Message.pdf

気にしているのは「真贋判定」

組みあがったクルマによくわからないECUが紛れ込まないようにしたい

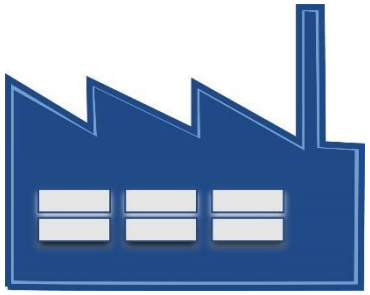
クルマだけではない



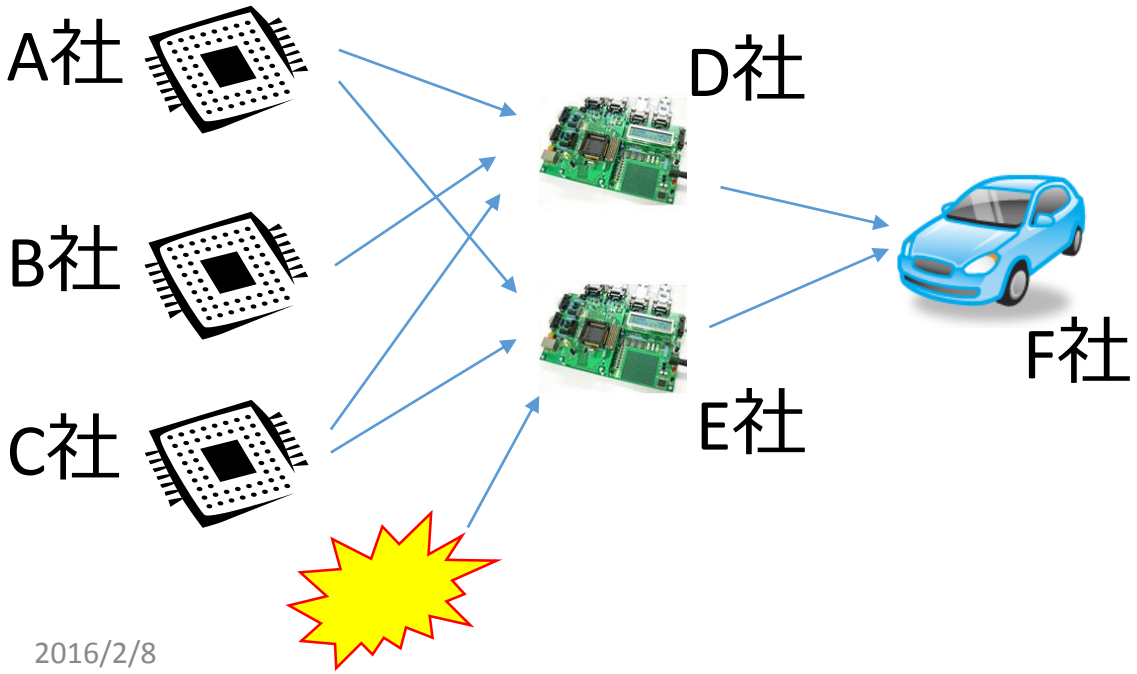
カメラがやられると
配信される動画が
正しいかわからなくなる

「証拠能力無し」

偽物が紛れ込むタイミング



工場での組立時に紛れ込む



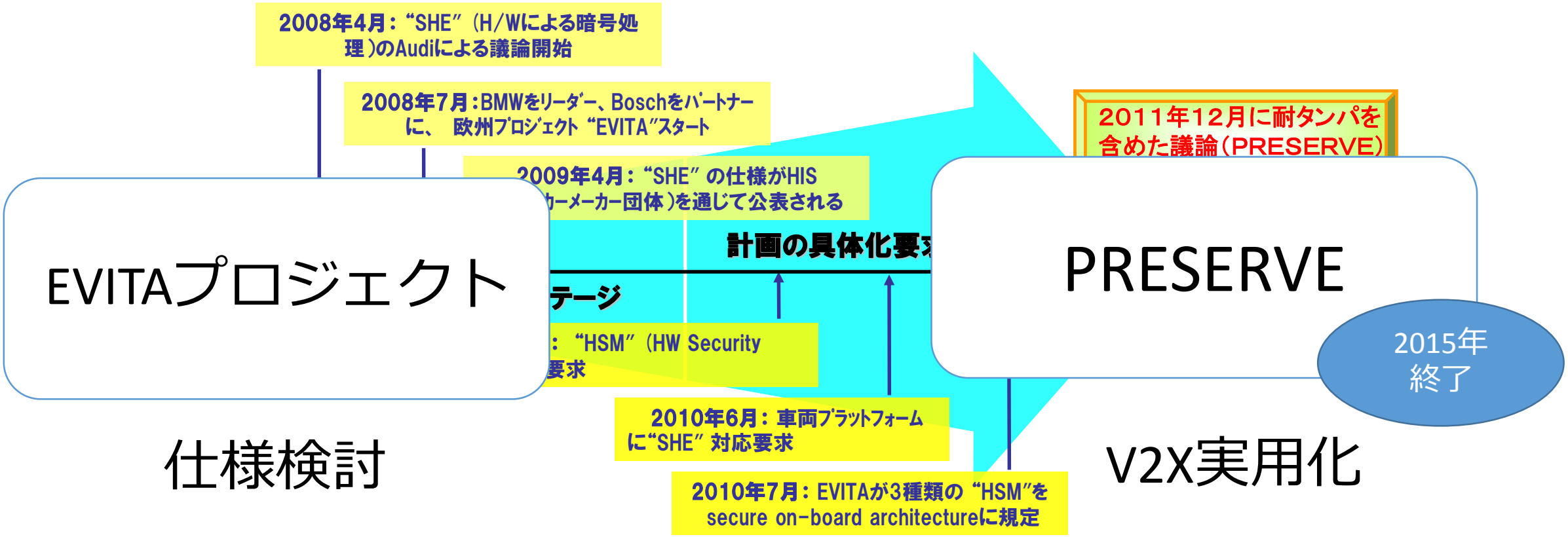
組立後

遠隔で改竄される

停車時に取り換えられる

欧州自動車市場でのセキュリティ要求

欧州を中心とする自動車へのセキュリティ実装のニーズ高まり
⇒　ECUの不正改竄防止・リプログラミングの保護
⇒　ECUの認証/データの暗号化が必須



EVITA仕様

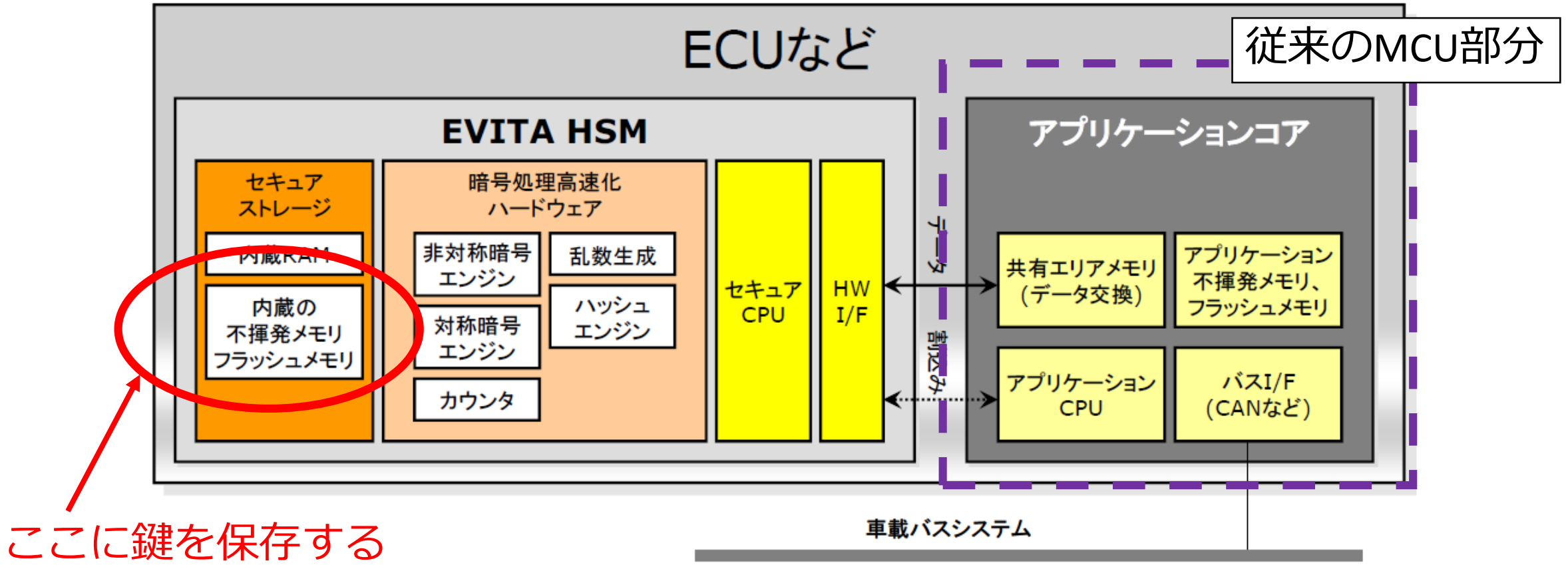


図 2-1 EVITA HSM のアーキテクチャの概要

（引用）2011年度自動車の情報セキュリティ動向に関する調査, IPA

TPM 2.0 Automotive

TPM (Trusted Platform Module) は TCG (Trusted Computing Group)が仕様を策定している

もともとはPC等に搭載

バージョン2.0から
クルマに特化した
Automotive仕様が出現

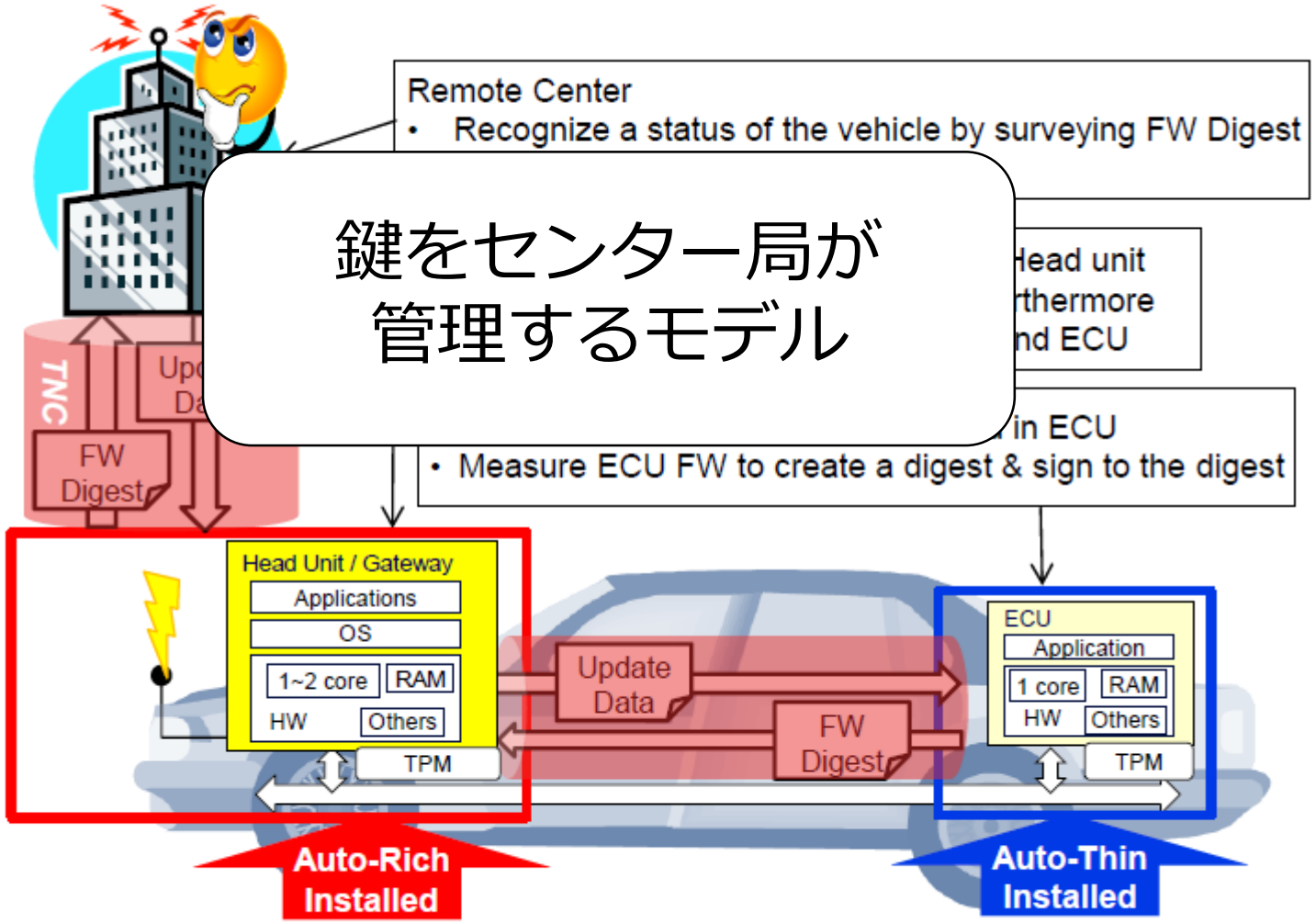


Figure 4: Message Flow for Remote Vehicle Maintenance

一方、組み込み機器全般で見ると

H/W（チップ）レベルでのセキュリティは
まだまだのように見える

これだけでは不足

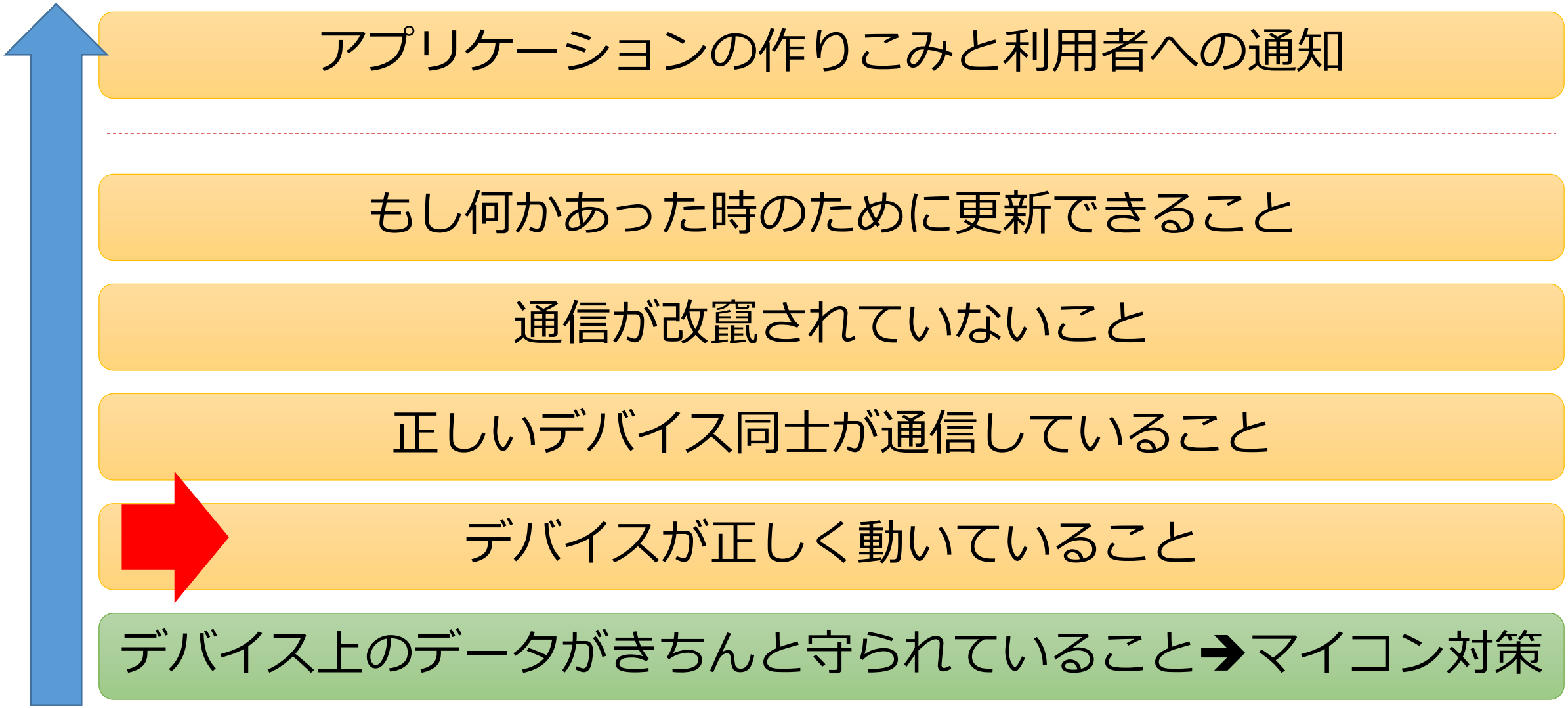
折角、正しいマイコンが
搭載されていても、

ソフトウェアに穴があってはやられてしまう

クルマのセキュリティとIoTへの展開

～KDDI研究所の取り組み～

信頼のモデル


アプリケーションの作りこみと利用者への通知
もし何かあった時のために更新できること
通信が改竄されていないこと
正しいデバイス同士が通信していること
デバイスが正しく動いていること
デバイス上のデータがきちんと守られていること➔マイコン対策

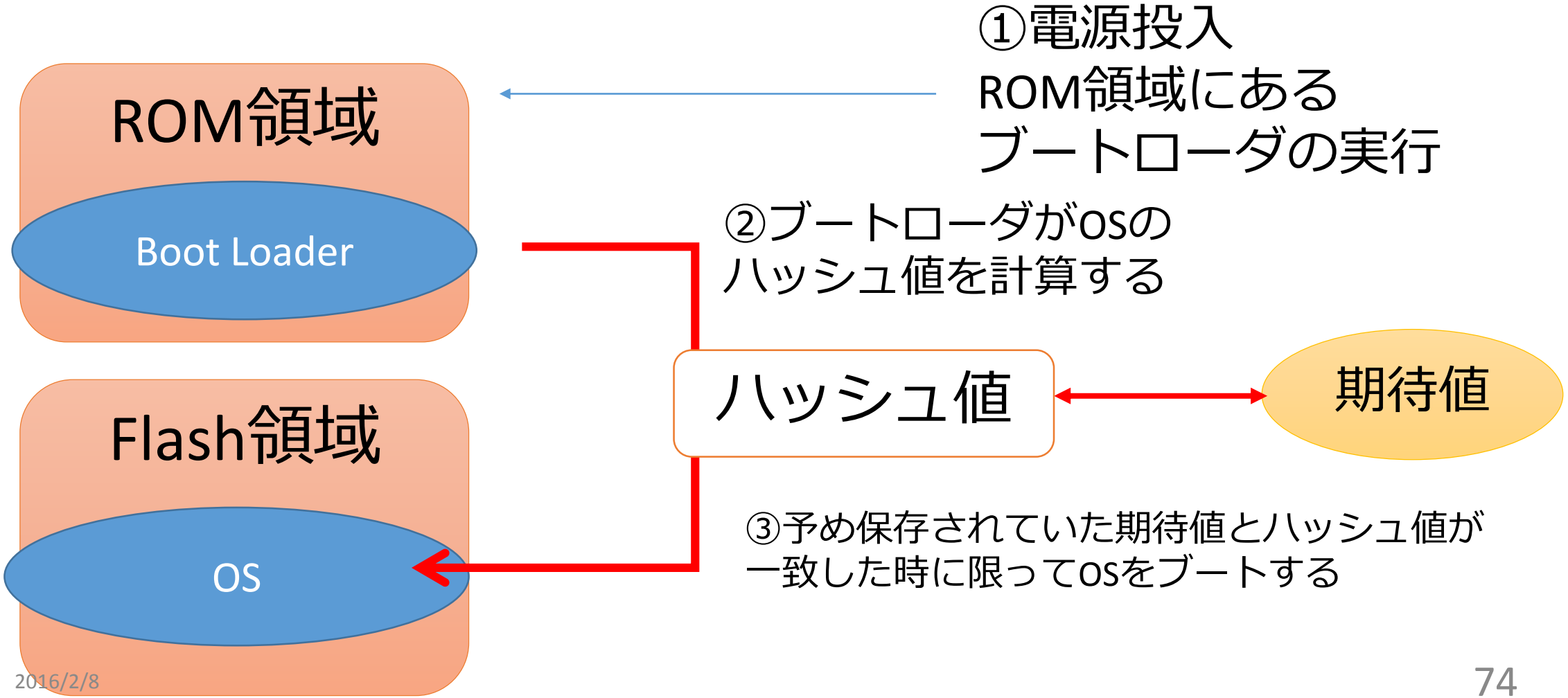
デバイスの信頼性の担保

- 正しいマイコンの上で、正しいソフトウェアが動作していることを保証する

セキュアブート

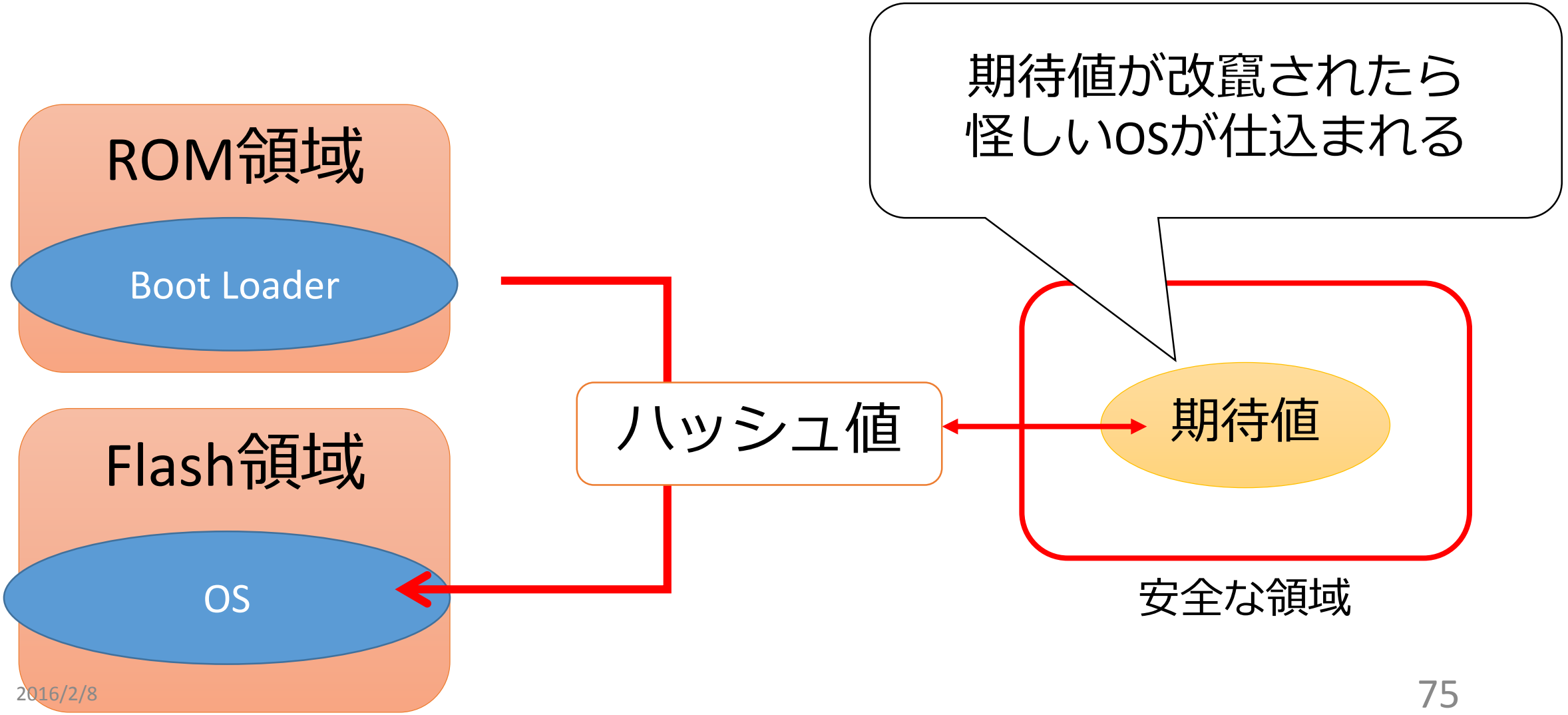
セキュアブートとは

OSのコードが改竄されていないことを
確認した上でOSを起動すること



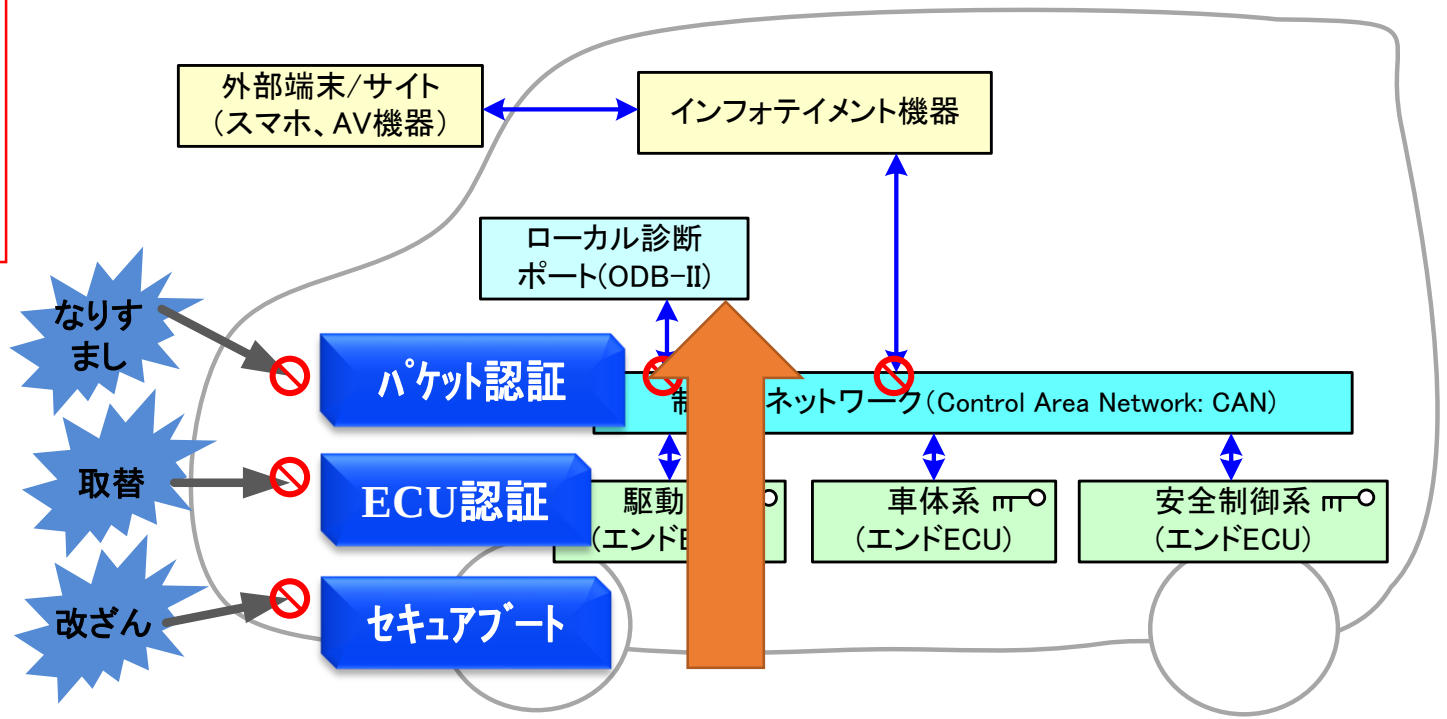
セキュアブートで大事なこと

期待値が安全に守られていること

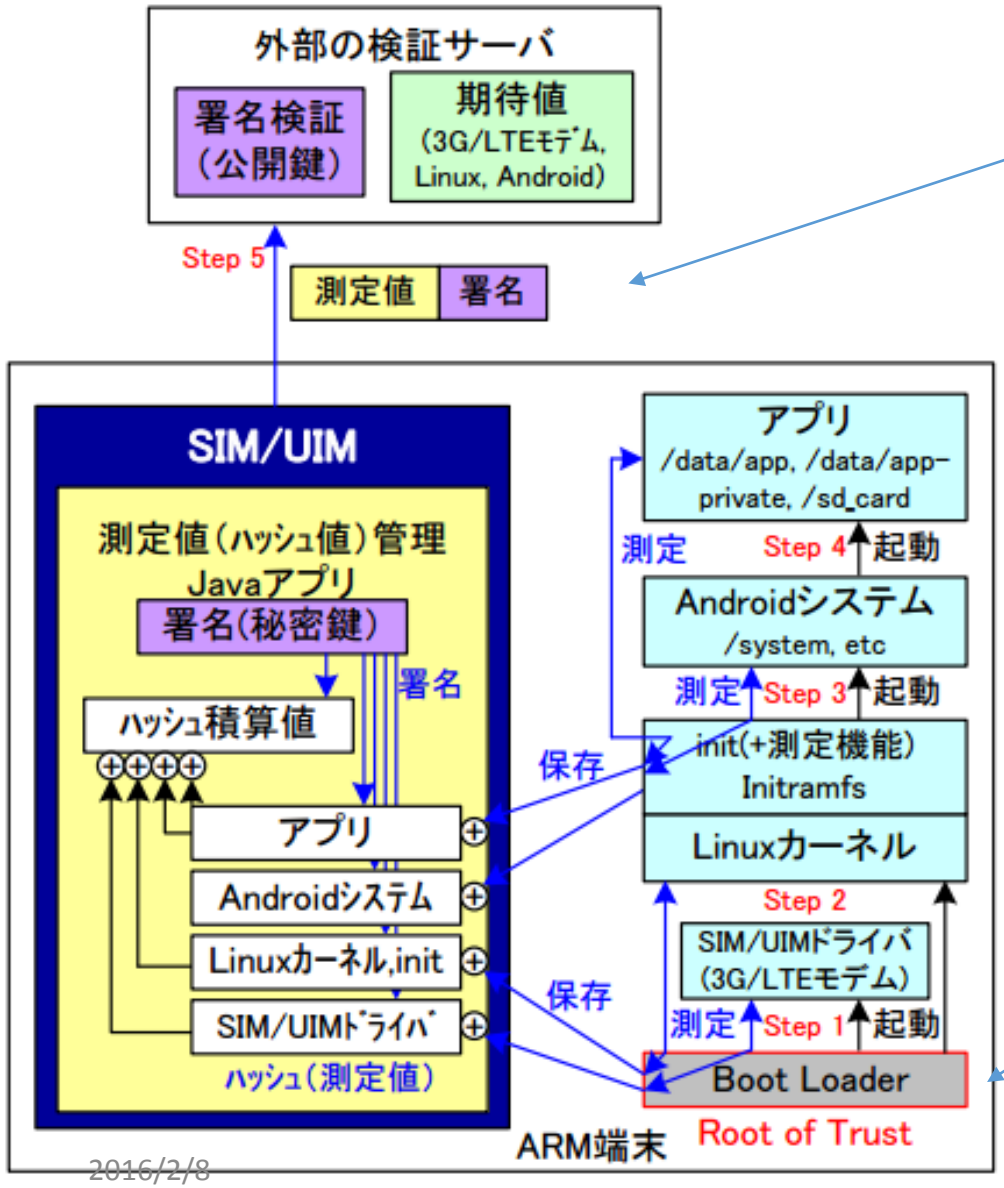


Trust Chain（信頼の連鎖）構築による車載セキュリティ向上

1. ECUのセキュアブート
   ECU自体を安全に起動する技術
   （ECUが改ざんされた場合、起動停止にする）
   ECUのHSMを活用した
   ECUファームウェアの改竄検知
2. ECU認証技術
   社内の複数のECU同士で相手ECUを認証する技術
   （不正なECUを検知する）
   事前にECUのHSMに格納された鍵を
   利用してのECUの相互認証
3. CANパケット認証
   MAC（Message Authenticate Code）を
   CANパケットに挿入することでの、
   なりすましパケット阻止



ケータイのセキュアブート



⑤**署名付き**測定値を検証サーバへ送付

確かにそのSIMであることを証明する

④任意のアプリを測定、
測定値を　　保存

ちゃんと起動したかを
外でチェックすることも可能

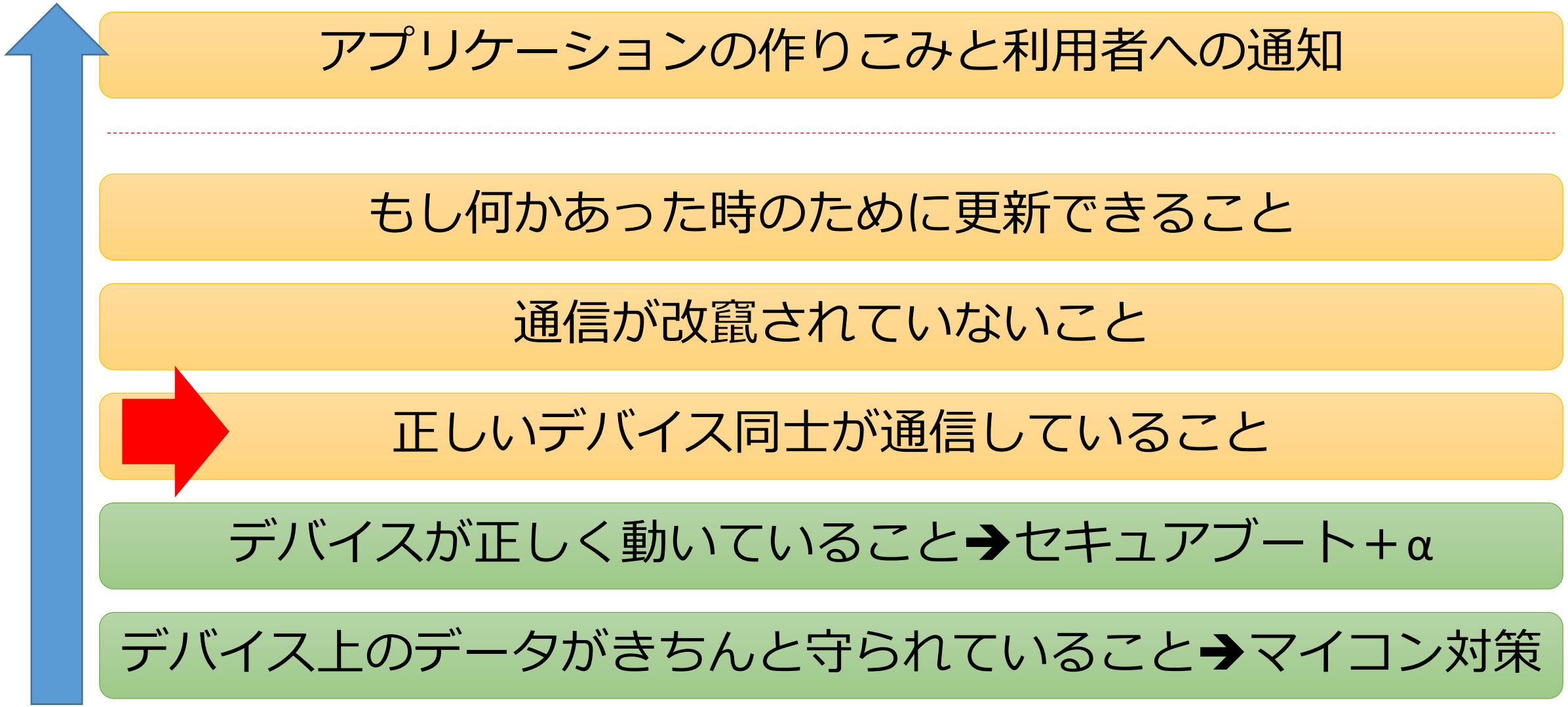
①SIM/UIMドライバを測定、
SIM/UIMを起動、測定値をSIMへ保存

ROM化されたBoot Loaderから測定

但し注意点がある

- セキュアブートは、『起動時』の正しさしか担保することができない
  - 『起動後』にやられる（ウィルス感染等）場合はメモリ保護技術等も併用しなければならない
    ➔パフォーマンスに影響する
- コーディングの時点で脆弱性を作りこまない努力が求められる

信頼のモデル


アプリケーションの作りこみと利用者への通知
もし何かあった時のために更新できること
通信が改竄されていないこと
正しいデバイス同士が通信していること
デバイスが正しく動いていること➔セキュアブート＋α
デバイス上のデータがきちんと守られていること➔マイコン対策

デバイス同士で認証しあう

- 自分が会話しようとする相手が、本当に信頼するに足るか

デバイス認証

信頼できる者同士で使われる合言葉

ご両親・身内の方が「振り込め詐欺」の被害にあわないために

■ 被害をなくすには、家族や社会が「振り込め詐欺」を許さない環境づくりが大切です。

最近、別居しているご両親や身内の方と話していますか？
「そういえば、最近あまり話をしていない。」という方は連絡をとり、近況だけでなく、振り込め詐欺の手口を話していただき、被害にあわないように注意を呼びかけてください。
そのときに「合言葉」を決めたり、「ATM利用限度額の引き下げ」を勧めてください。
いざというときに役に立ったり、被害を最小限にすることに効果があります。

合言葉

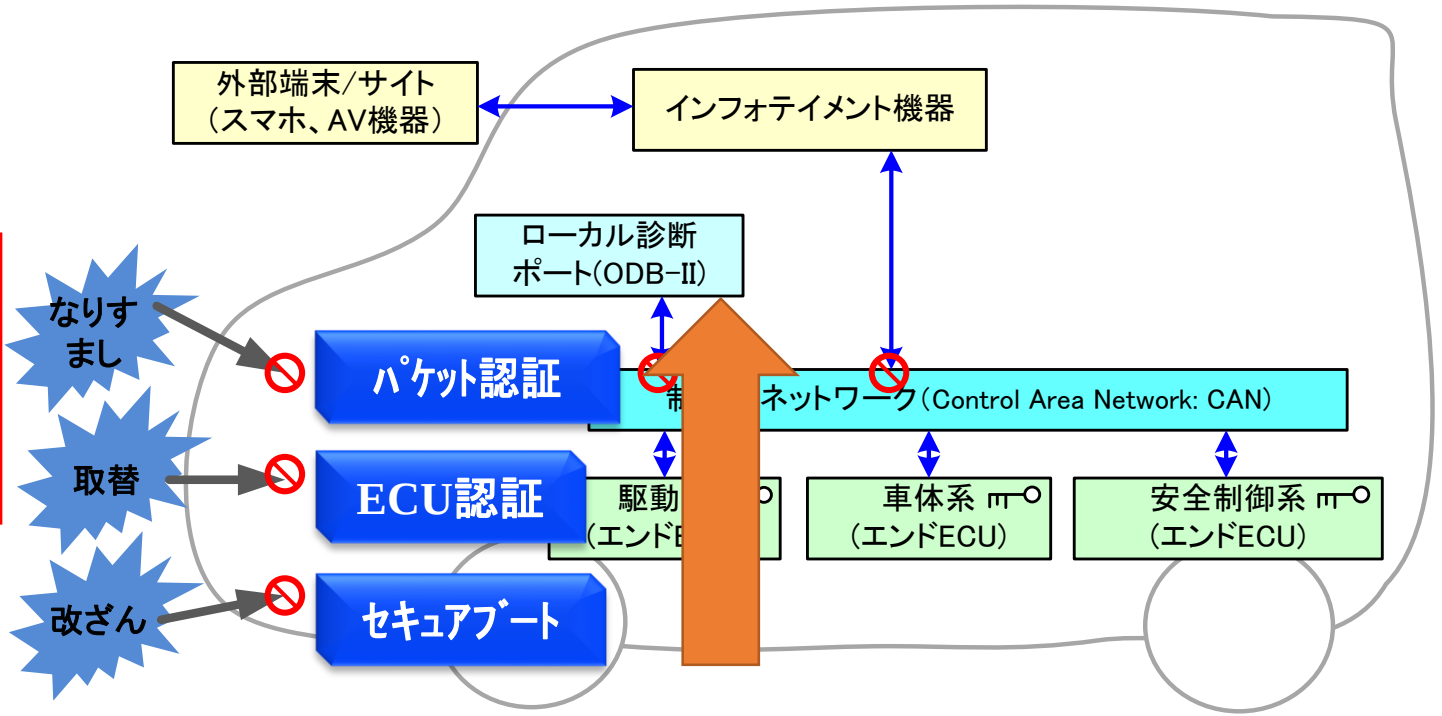
- 家族や身近な親戚しか知らない事実
- 慌てていても簡単に思い出せること
- 絶対に忘れない言葉、出来事

「慌てて忘れた」、「そんなことより」、「今、それどころではない」等と言って合言葉よりも、自分の言いたいことを優先させるときは、ためらわず電話を切りましょう。
それは、十中八九「振り込め詐欺」と考えてよいでしょう。
犯人は、同級生名簿等を入手して、住所や電話番号、家族の名前を知っている可能性があるので、そのような情報だけで信じることのないように

http://www.keishicho.metro.tokyo.jp/seian/koreisagi/koreisagi.htm

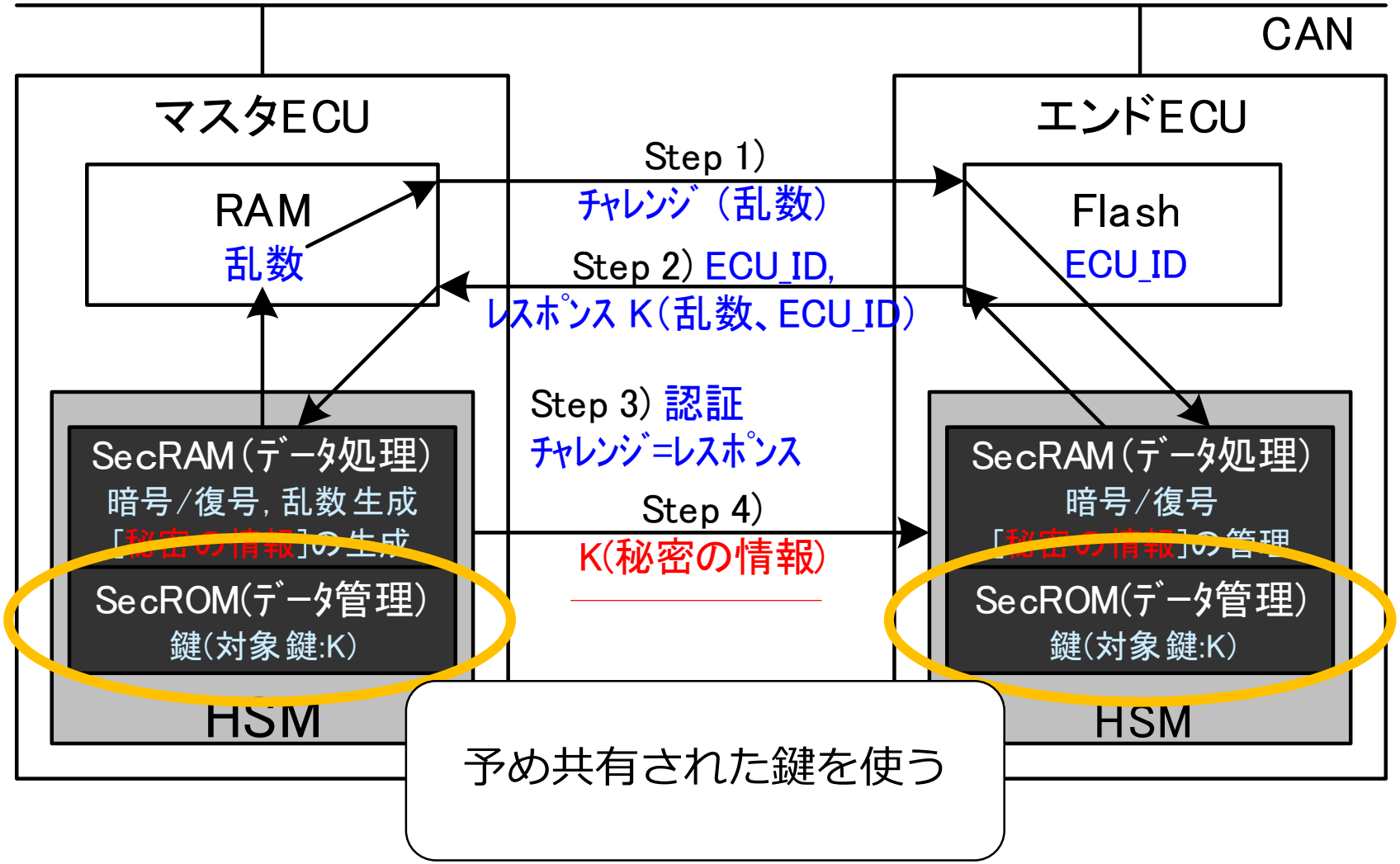
Trust Chain（信頼の連鎖）構築による車載セキュリティ向上

1. ECUのセキュアブート
   ECU自体を安全に起動する技術
   （ECUが改ざんされた場合、起動停止にする）
   ECUのHSMを活用した
   ECUファームウェアの改竄検知
2. ECU認証技術
   社内の複数のECU同士で相手ECUを認証する技術
   （不正なECUを検知する）
   事前にECUのHSMに格納された鍵を
   利用してのECUの相互認証
3. CANパケット認証
   MAC（Message Authenticate Code）を
   CANパケットに挿入することでの、
   なりすましパケット阻止

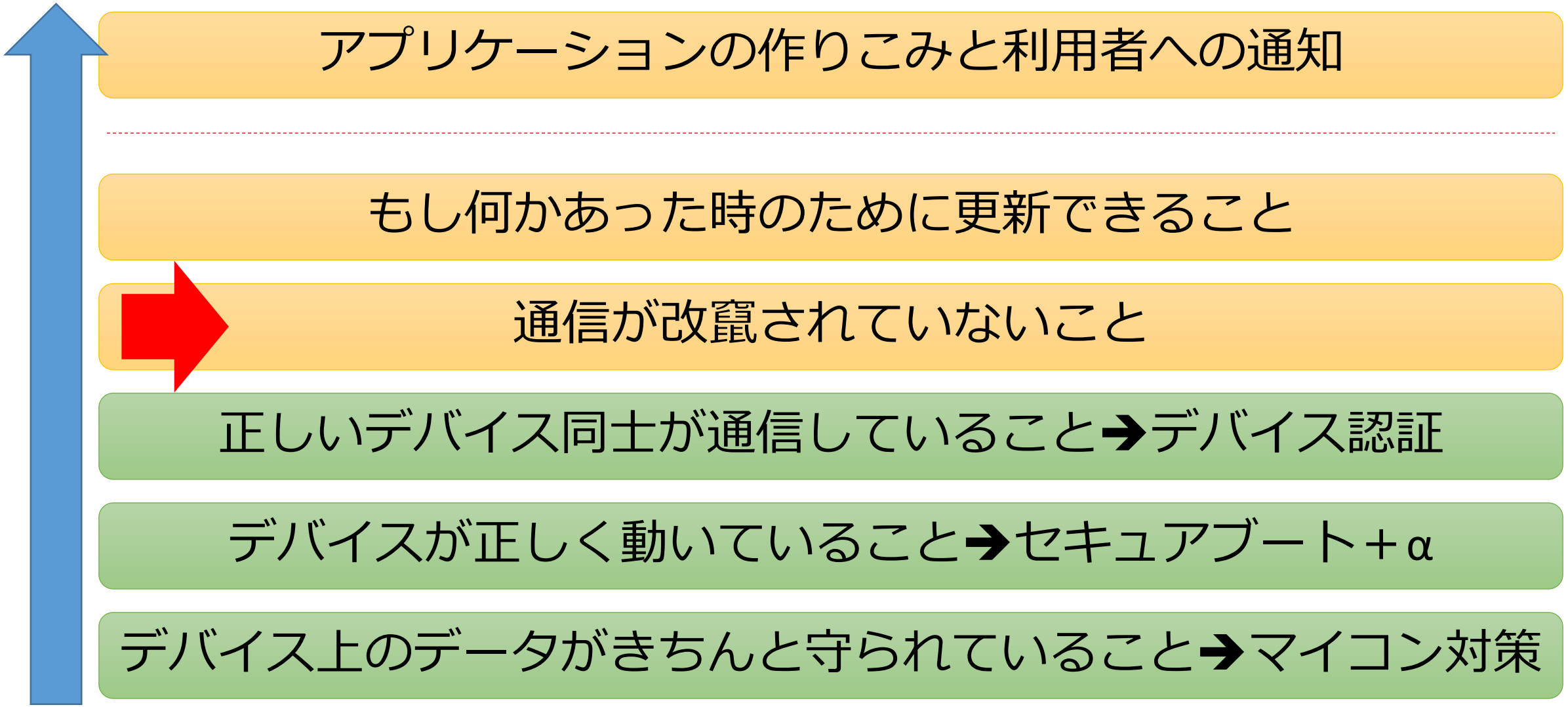


ECU認証

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で実装



信頼のモデル


アプリケーションの作りこみと利用者への通知
もし何かあった時のために更新できること
通信が改竄されていないこと
正しいデバイス同士が通信していること➔デバイス認証
デバイスが正しく動いていること➔セキュアブート＋α
デバイス上のデータがきちんと守られていること➔マイコン対策

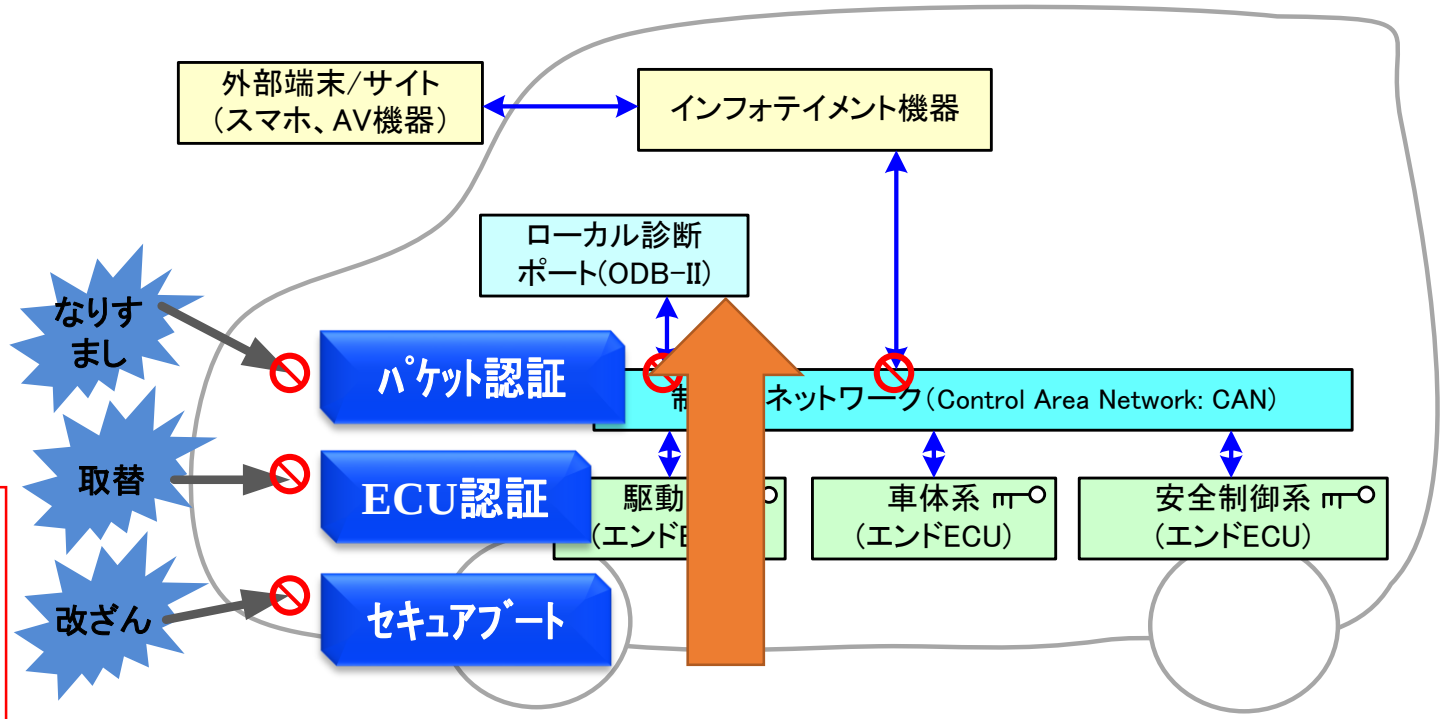
経路上のセキュリティ

- デバイスから送られてくるデータが、経路上で改竄されていないか
- 正しいデータが送られてきているか

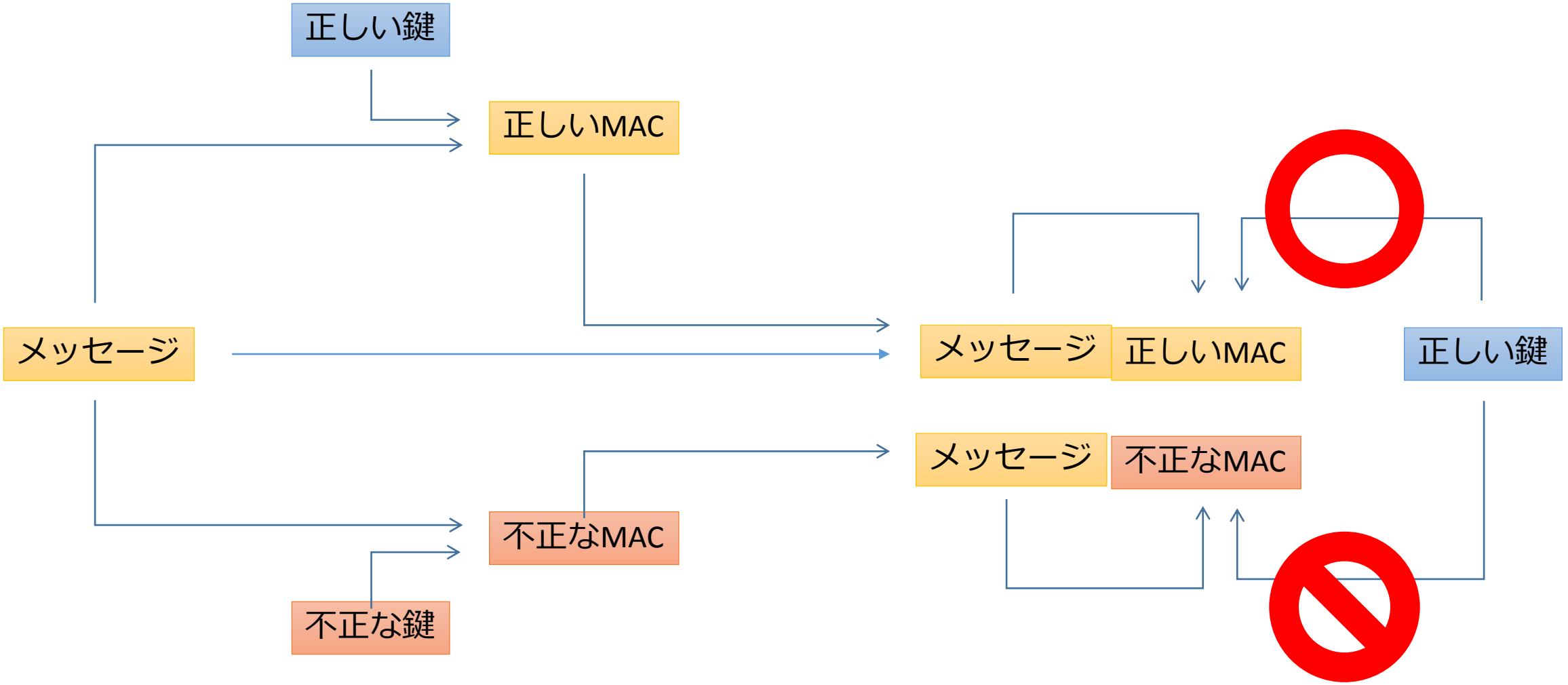
メッセージ認証

Trust Chain（信頼の連鎖）構築による車載セキュリティ向上

1. ECUのセキュアブート
   ECU自体を安全に起動する技術
   （ECUが改ざんされた場合、起動停止にする）
   ECUのHSMを活用した
   ECUファームウェアの改竄検知
2. ECU認証技術
   社内の複数のECU同士で相手ECUを認証する技術
   （不正なECUを検知する）
   事前にECUのHSMに格納された鍵を
   利用してのECUの相互認証
3. CANパケット認証
   MAC（Message Authenticate Code）を
   CANパケットに挿入することでの、
   なりすましパケット阻止



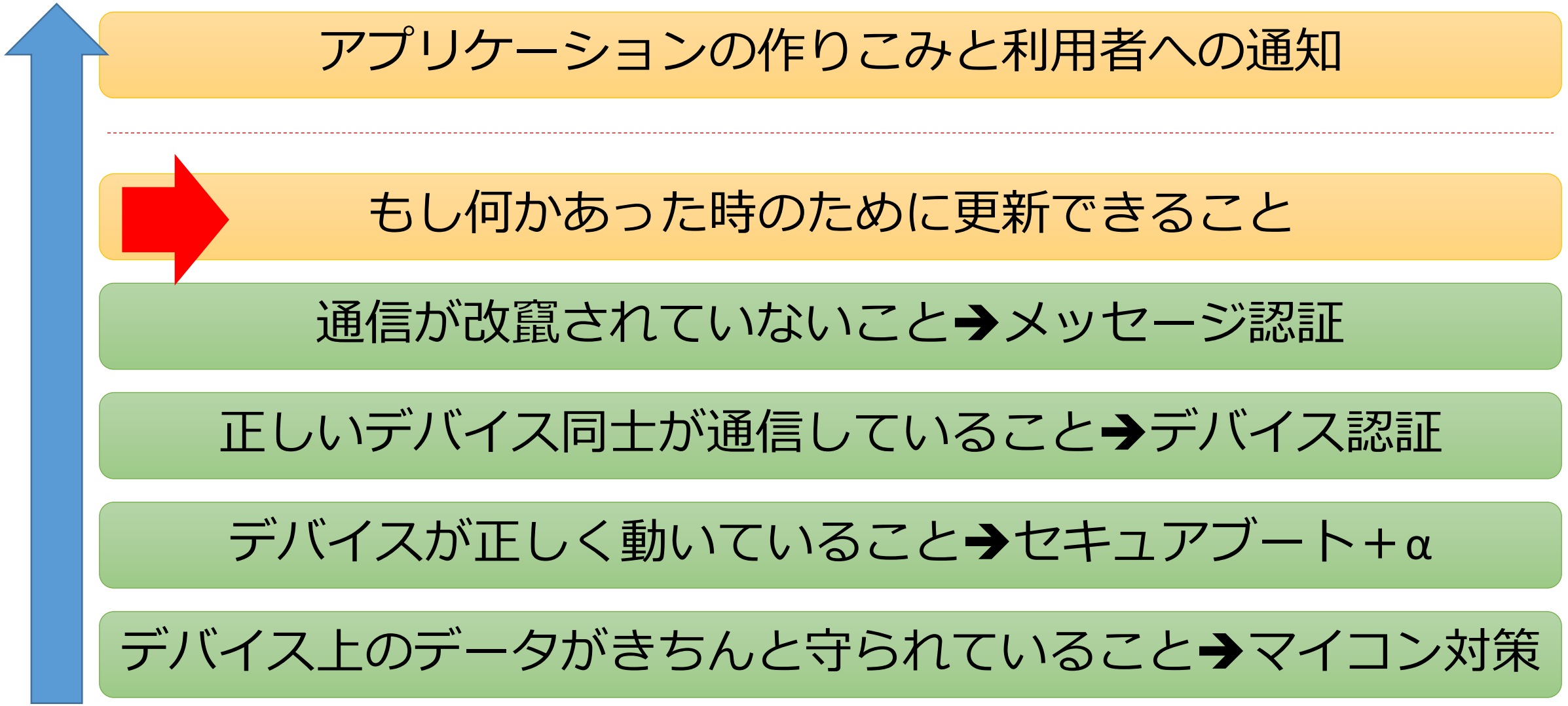
MAC付与によるCANパケット認証



送信側
（モーター制御ECU）

受信側
（モーター駆動ECU）

信頼のモデル

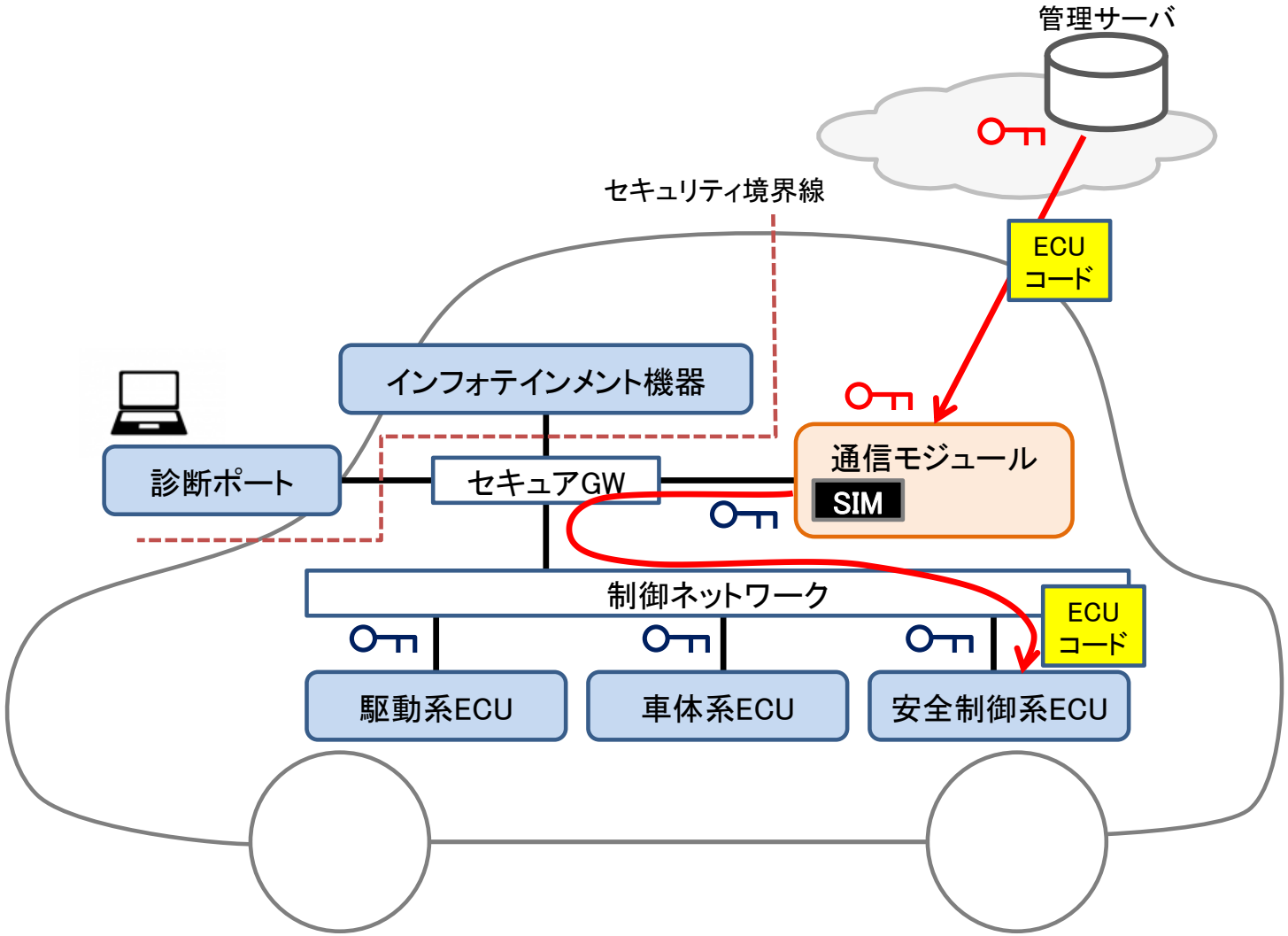

アプリケーションの作りこみと利用者への通知
もし何かあった時のために更新できること
通信が改竄されていないこと➔メッセージ認証
正しいデバイス同士が通信していること➔デバイス認証
デバイスが正しく動いていること➔セキュアブート＋α
デバイス上のデータがきちんと守られていること➔マイコン対策

更新の必要性

- IoTデバイスは、PCよりも長く運用される
- 脆弱性が見つかることも

セキュアなアップデート

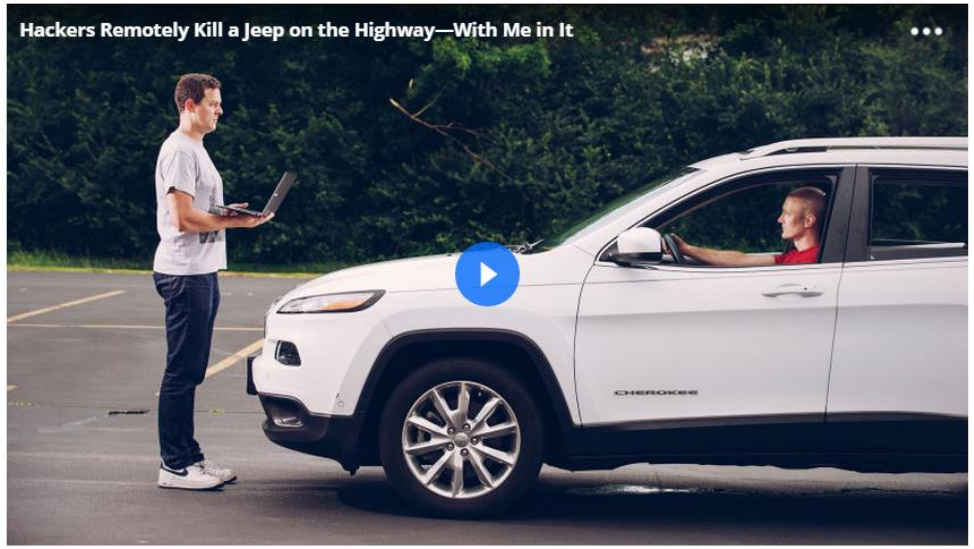
ファームウェア更新 Over the Air



クルマに搭載された通信モジュールを介して
制御系マイコンのファームウェア更新を行う

アップデート機能自体が攻撃対象になる

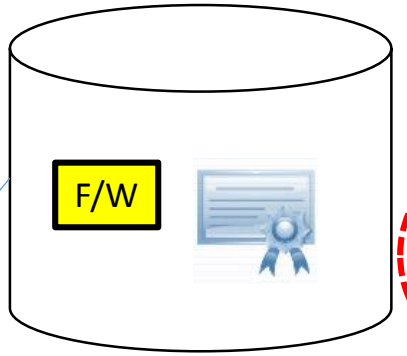
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



アップデート機能の設計は重要

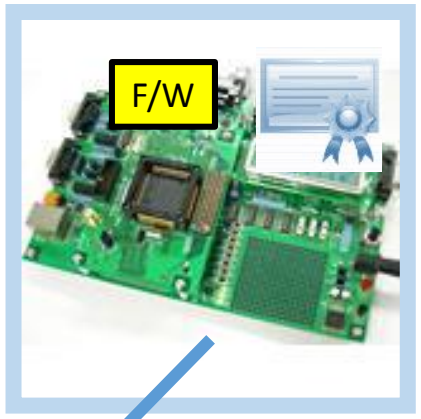
『セキュア』なファームウェア更新 Over the Air

安全が担保された
デバイス上で実施



署名鍵

検証したF/Wを安全にECUに配信するためには、
車内NWの堅牢化が必須である



署名検証

SIM

OK/NG

ECU認証鍵

署名検証鍵

FOTAの経路上でF/Wが改竄されていないことを証明するためには、
F/Wの署名検証が必要である。

SIM上の署名検証アプリを用いて
F/Wを検証する

ECU認証鍵

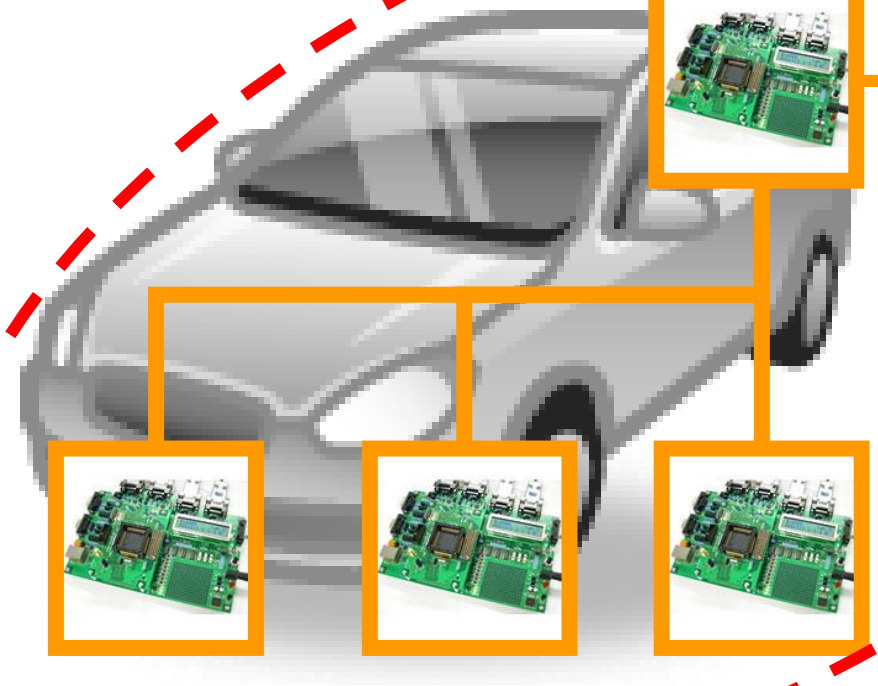
認証に必要な鍵・証明書

- デバイスに残す場合は適切な管理が必要

鍵管理

セキュアなデバイス管理

トラストアンカーとしてのSIM



SIM

通信モジュール

ECU
コード

ファームウェア
管理サーバ

ECU
コード

SIMを基点とした
外部NW通信の堅牢化

SIMを基点とした
車載制御NWの堅牢化

SIMカードの特徴

SIM（ICカード）＝Javaカード

使えるサービス：NFC（情報取得／リンク）

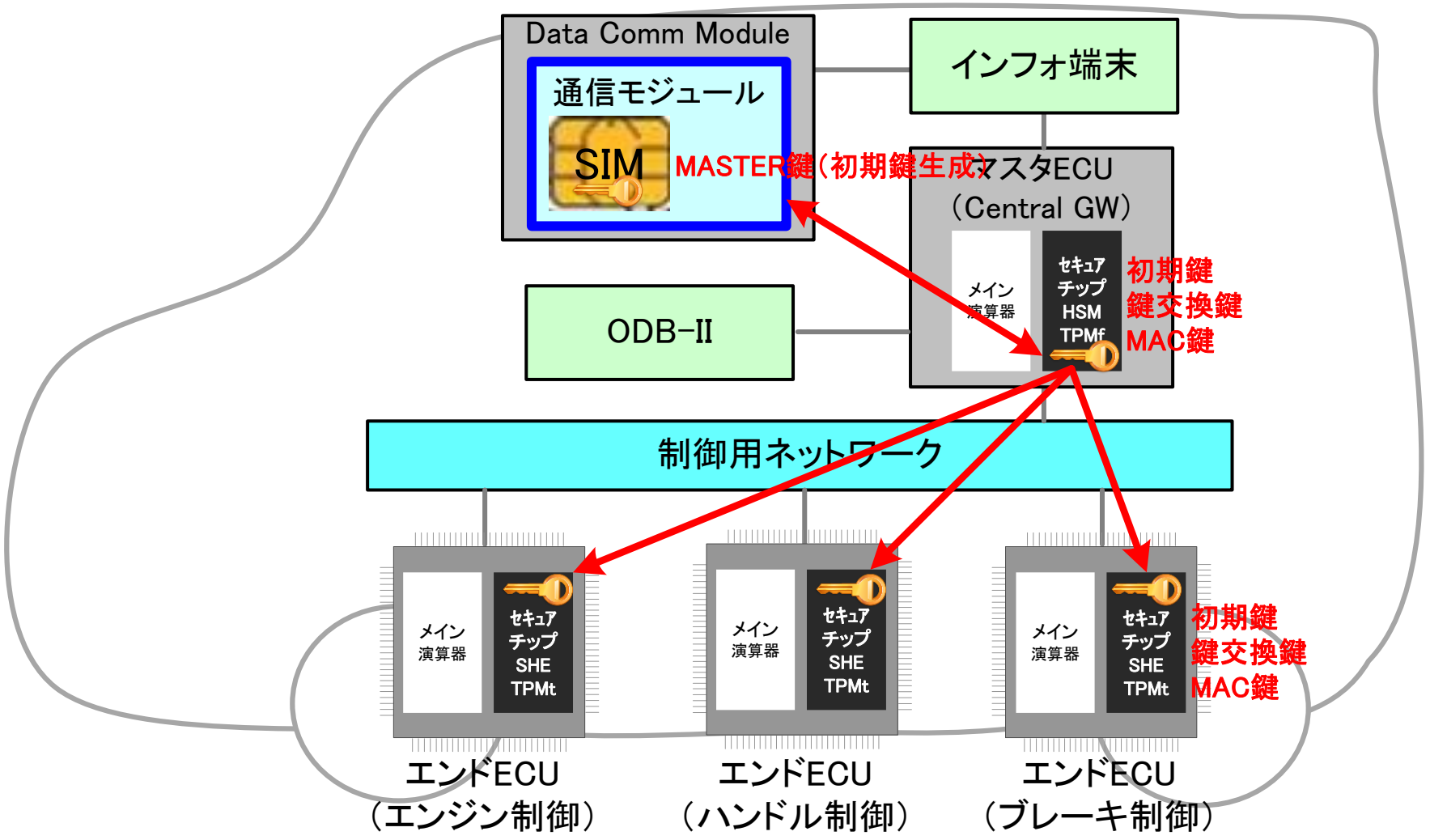
概要 | 使えるサービス | セキュリティ | 対応機種一覧

使えるサービス

JALタッチ&ゴー

JALのスマートフォンサービスに"らくらくカンタン"に飛行機へご搭乗いただける「JALタッチ&ゴー」アプリが登場!
サービス登録をいただくだけであなたのスマホが搭乗券になり、そのまま空港にてご利用いただけます。
アプリ一覧からはJALが提供するアプリがダウンロードできます。予約アプリだけでなく、エンタメアプリも充実。
まずは今すぐダウンロード!

鍵管理モデル

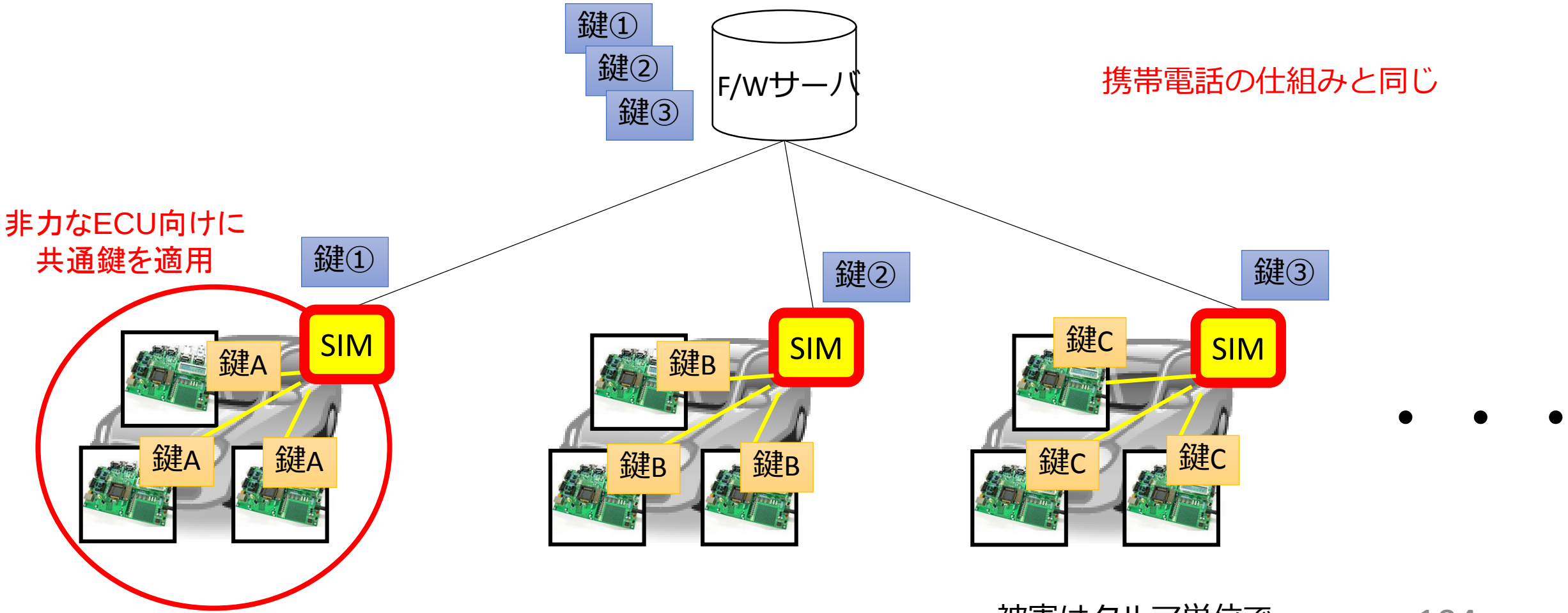


SIMがマスターとなって鍵を配布する

（考え方）鍵管理の境界

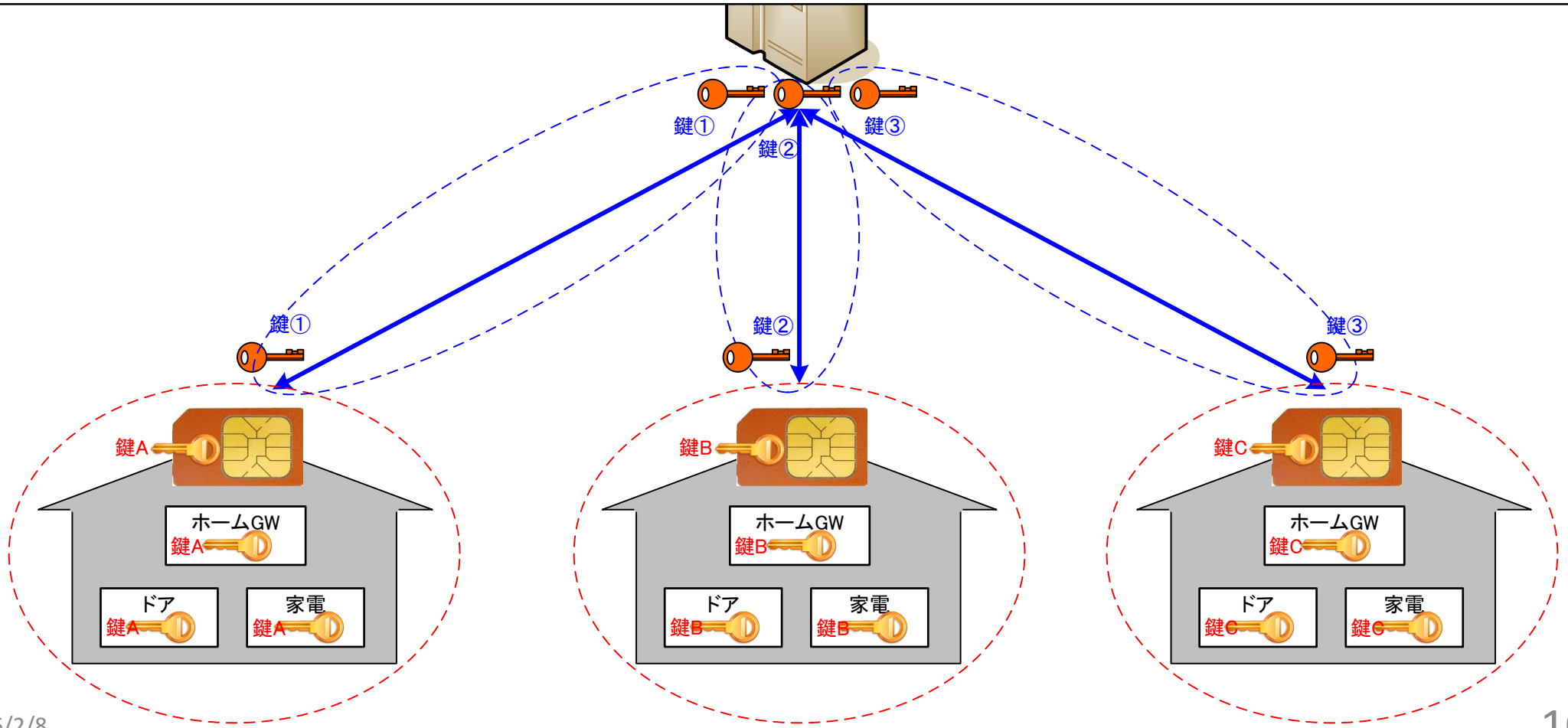
プライバシ境界のプロキシ役

◆ 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がプロキシ役を果たす

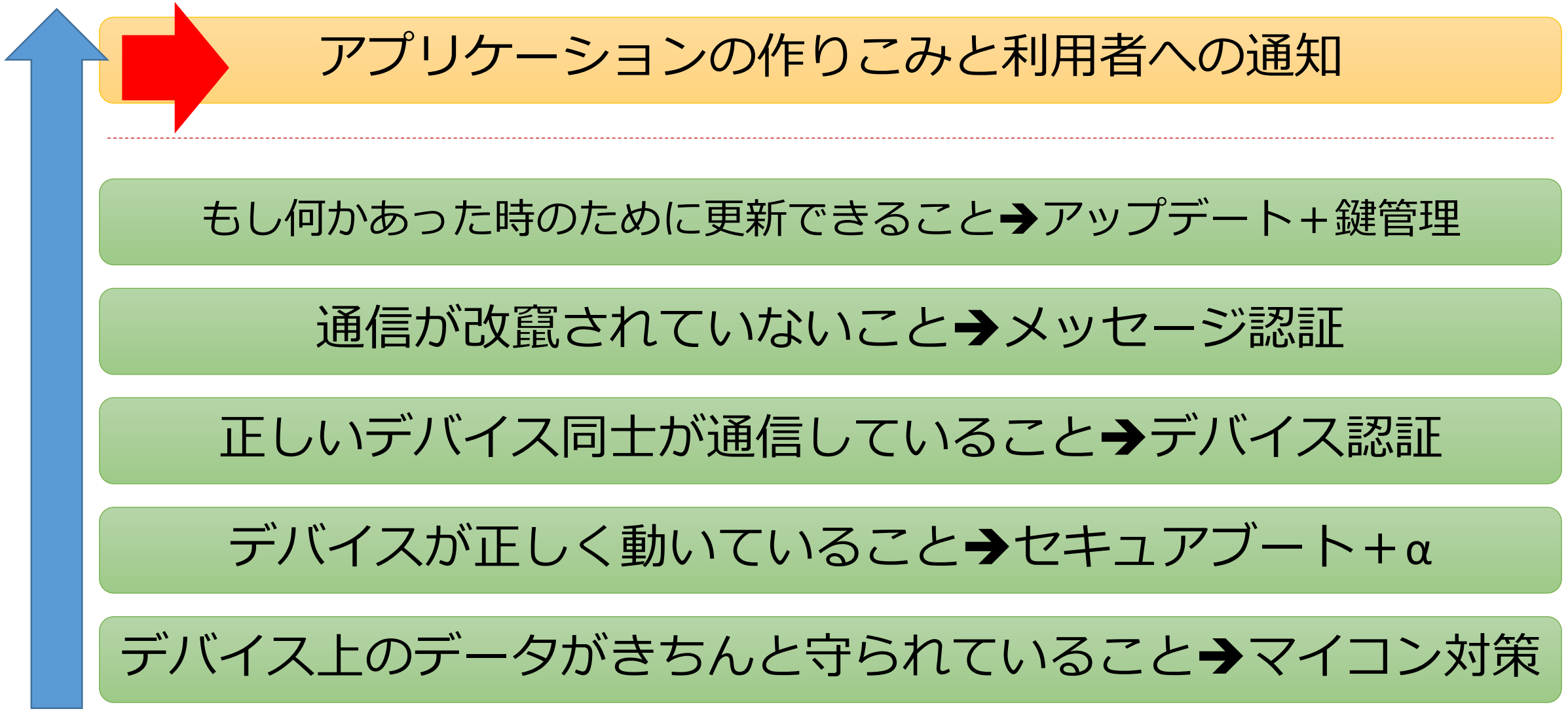


スマートハウスへの適用

データ保護指令（EU）、プライバシ権利章典（US）、個人情報保護法（JP）など、
「透明性の確保」と「利用者関与の機会」への配慮。
⇒ 宅内鍵を外部の第三者が扱わないよう、宅外鍵と分けること。



信頼のモデル

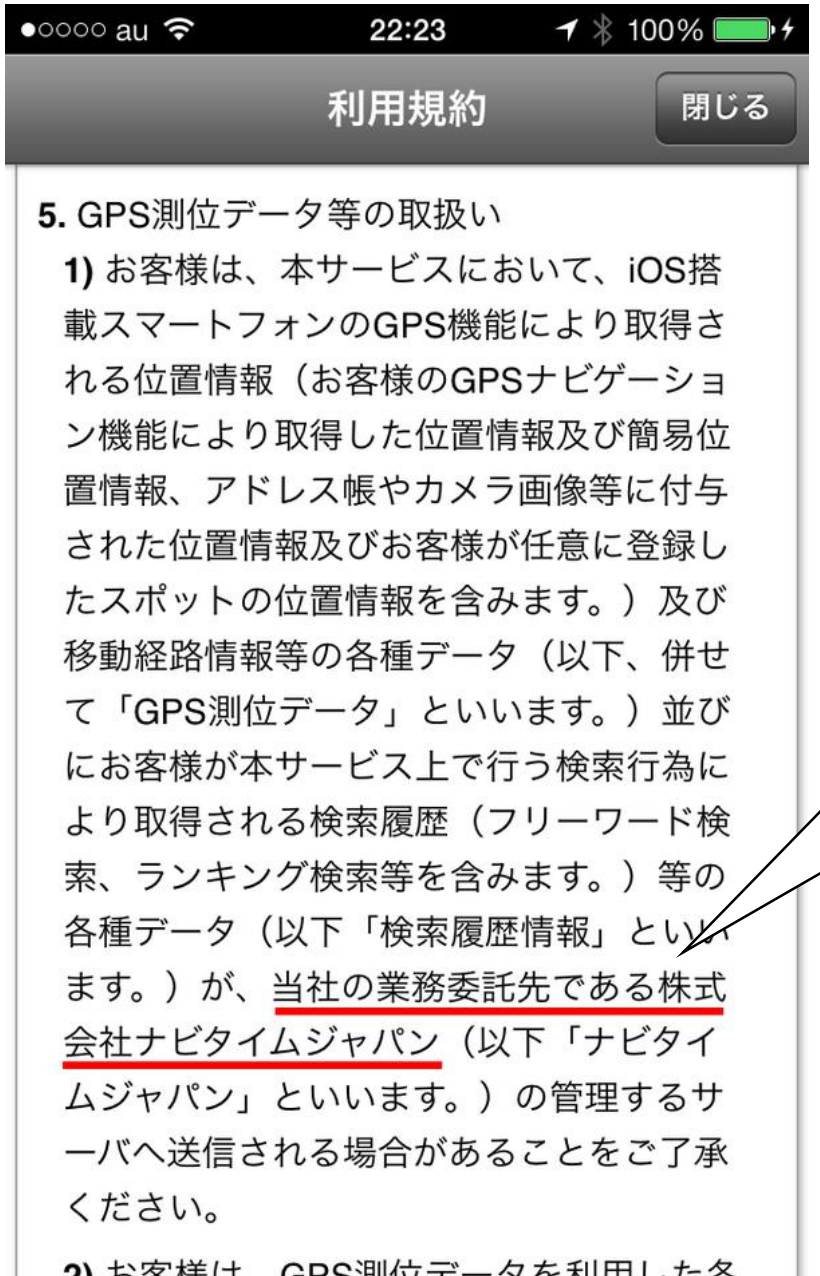

アプリケーションの作りこみと利用者への通知
もし何かあった時のために更新できること➔アップデート＋鍵管理
通信が改竄されていないこと➔メッセージ認証
正しいデバイス同士が通信していること➔デバイス認証
デバイスが正しく動いていること➔セキュアブート＋α
デバイス上のデータがきちんと守られていること➔マイコン対策

プライバシー

- 利用者が不安に思う前にきちんと説明すること

プライバシー情報の
利用承諾

プライバシーポリシー



その情報が何のために
誰に渡されるかを明記する
➔活用しないデータは集めない

それでも秘密裏に情報を集めようとする者は
どうすればいいのか➔課題

リスク分析

- IoTデバイスに対するセキュリティを適用していくうえで
  - ベンダーさんにどのように理解してもらうか
    - 場合によっては工場の設計に影響を及ぼすため、なぜそれにお金を掛けなければならないかを試算する必要がある

リスク分析

まとめ

- IoTの脅威Top10
- デバイスの信頼性の担保
- デバイス同士の認証
- データの信頼性
- 安全なアップデート
- 信頼の基点となるデータ＝鍵の保護
- プライバシー情報の利用許諾
- リスク分析

通信事業者のやること

『モノが繋がる世界』
IoT: Internet of Things

クルマ

家電

センサー

IoTを支えるインフラの構築
IoTにおけるサービスの実現

ココも
本職

みなさん共にがんばりましょう！