オートモーティブワールド　２０１７

セコムIS研究所
Intelligent Systems Laboratory

OTA時代の自動車のサイバーセキュリティ

2017年1月20日

セコム（株）ＩＳ研究所　松本　泰

松本の自己紹介

セコム（株）IS研究所　ディビジョンマネージャー

セコムIS研究所 Intelligent Systems Laboratory

- 1984年　UNIX上のビデオテックス・パソコン通信システムの開発
- 1994年　各種インターネットサービスの設計、開発、運用に従事
- 1999年　サイバーセキュリティ事業の立ち上げに従事
- 2003年-2007年　工学院大学「セキュアシステム設計技術[illegible]の育成」プログラム客員教授
- 2007年　経済産業省 商務情報政策局長表彰「情報セキュリティ促[illegible]
- 2007年-2012年
  - 情報処理推進機構 情報セキュリティ分析ラボラトリー 非常勤研究員
- 2011年-2012年
  - 社会保障・税に関わる番号制度　情報連携基盤技術WG　構成[illegible]
  - 社会保障・税に関わる番号制度　社会保障分野サブWG　構成[illegible]
- 2013年-2014年
  - 内閣官房　パーソナルデータに関する検討委員会・技術検討WG　[illegible]成員
- 2017年1月現在
  - 日本ネットワークセキュリティ協会　PKI相互運用技術WG　リーダー
  - 暗号技術検討会（CRYPTREC）構成員、暗号技術評価委員会　委員
  - 暗号技術検討会（CRYPTREC）重要課題検討タスクフォース　委員
  - 電子署名法研究会　構成員
  - 保健医療福祉情報システム工業会　セキュアトークンWG　構成員
  - 日本データセンター協会　セキュリティWG　リーダー
  - JST/RISTEX　公私領域アドバイザー

サービスのためのネットワーク・セキュリティ

PKI、認証サービス、IDSサービス等の立ち上げ

サイバー・セキュリティに関する様々な活動

OTA時代の自動車のサイバーセキュリティ

セコムIS研究所
Intelligent Systems Laboratory

- 自動運転等の車のセーフティのためには、ECUのソフトウェアや３次元地図等は、常に最新のソフトウェアやデータであることが要求される。そのため Over the Air(OTA)によるソフトウェア更新等は、非常に重要な役割を果たす。
- ソフトウェアの脆弱性対応のためにも必要となるOTAであるが、安易なOTAの実装は、新たなバックドアを生む可能性もあり、車のセーフティをも脅かすサイバー攻撃の元凶にもなり得る。
- 本講演では、OTA時代における自動車へのサイバー攻撃のシナリオを示すとともに、セキュアなOTAを実現するために必要不可欠となる「暗号技術によるトラスト」を中心に自動車のセキュリティの方向性について説明する。

セコムIS研究所
Intelligent Systems Laboratory

OTA時代の自動車のサイバーセキュリティ

- (1) 自動車のサイバーセキュリティ
- (2) 暗号技術によるトラスト
- (3) まとめ

- 参考文献
- 付録

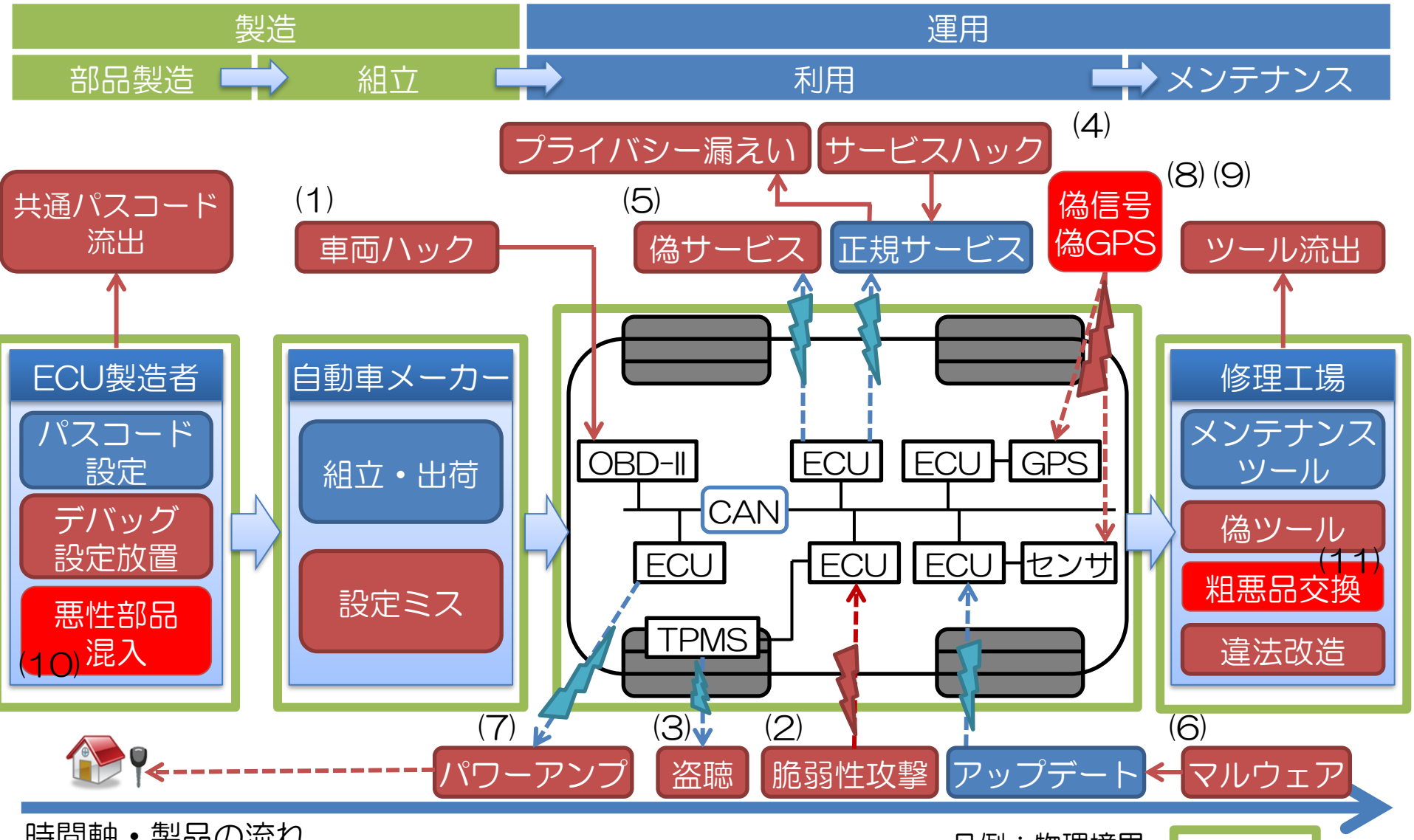
セコムIS研究所
Intelligent Systems Laboratory

自動車のサイバーセキュリティ

- 自動車へのサイバー攻撃のシナリオ
- OTAに関係する事例
- OTAに対して想定される脅威
- サイバーセキュリティの対応

車へのサイバー攻撃のシナリオ(概観)

セコムIS研究所
Intelligent Systems Laboratory



TPMS : Tire Pressure Monitoring System

自動車へのサイバー攻撃のシナリオ(現状)

セコムIS研究所 Intelligent Systems Laboratory

研究者による発表事例の多くは、リバースエンジニアリング

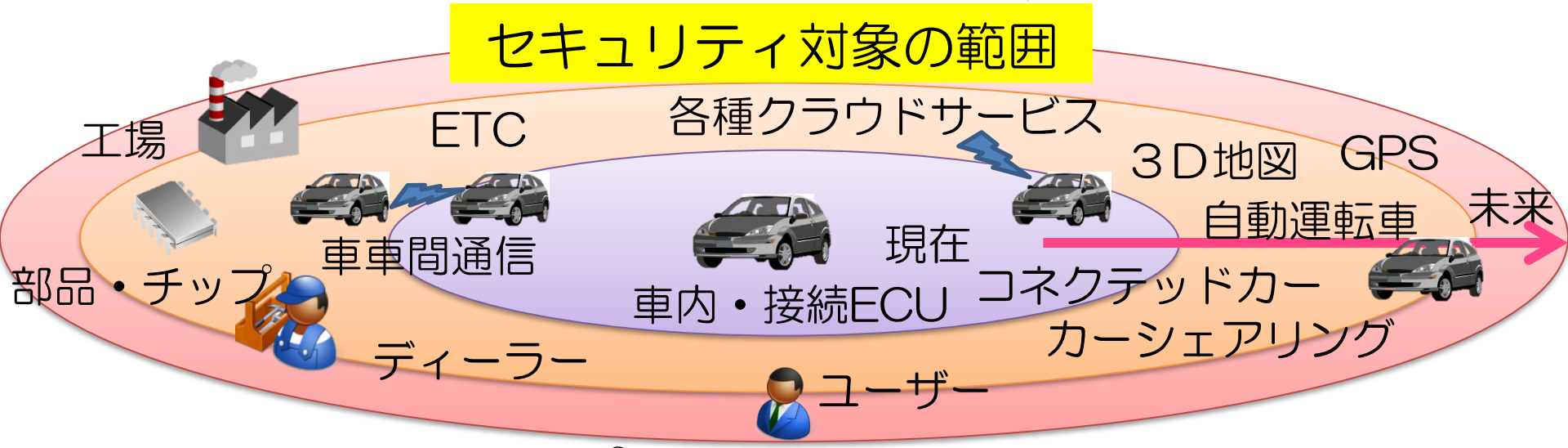
- (1) OBD-IIポートからCANへの直接通信
  - 安価な通信モジュール（USB-CAN）の普及
- (2) ECUの脆弱性をついた攻撃
  - 脆弱性・実証コードのネット公開
- (3) 自動車から発信される無線通信の盗聴・追跡
  - 標準通信プロトコルの採用
- (4) 自動車に接続されるサービス自体へのハッキング
  - グローバルなWebサービス
- (5) 自動車に接続されるサービスのなりすまし
  - 偽サービス中間者攻撃
- (6) アップデートでのマルウェア混入・ソフトウェア更新
  - ソフトウェアー・トロージャン
  - 情報の外部送信
- (7) 自動車との無線信号の増幅
  - リモートロック解除のパワーアンプ

自動車へのサイバー攻撃のシナリオ(将来/妄想)

セコムIS研究所 Intelligent Systems Laboratory

- (8) 無線のなりすましによる攻撃
  - ソフトウェア無線(SDR)の低価格化
- (9) GPS信号のなりすましによる攻撃
  - ソフトウェア無線(SDR)の低価格化
  - SDRのソフトのオープンソース化
- (10) ECU製造工場での悪性部品混入
  - ハードウェアー・トロージャン等
  - ECUの暗号鍵の漏えい
- (11) 修理工場で粗悪な部品への置き換え

自動運転等の車を起点としたイノベーションが広がる程に、検討するべきサイバーセキュリティの範囲は広がっていく



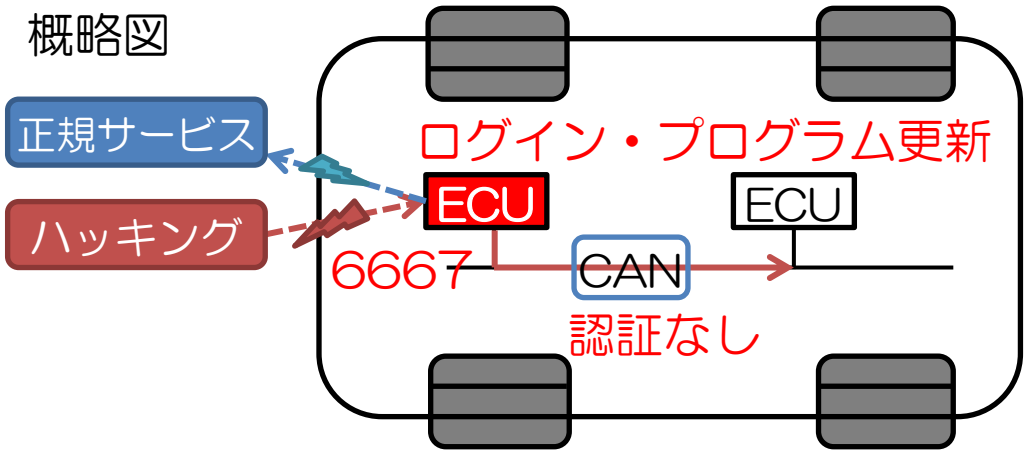
OTAに関係する事例　その１
研究者によるJeepへのハッキング（プログラムの改ざん）

セコムIS研究所
Intelligent Systems Laboratory

通信サービス(uconnect)に使われるECUに以下の脆弱性

- 特定ポート(6667)が常時アクセス可能であった
- ECUのOSへのログインがツールを使った総当たりで可能だった
- ログイン後root権限が取得できた
- ECUの制御系マイコンへの通信が簡単にできた。
- プログラム更新での認証・署名検証がなかった
- CANの脆弱性

概略図



設計の秘密による安全性

- コストは一見安いが、長期的維持は困難
- 秘密のデバッグ手段がバックドアーに
- 安全性の検証が不十分な場合がある

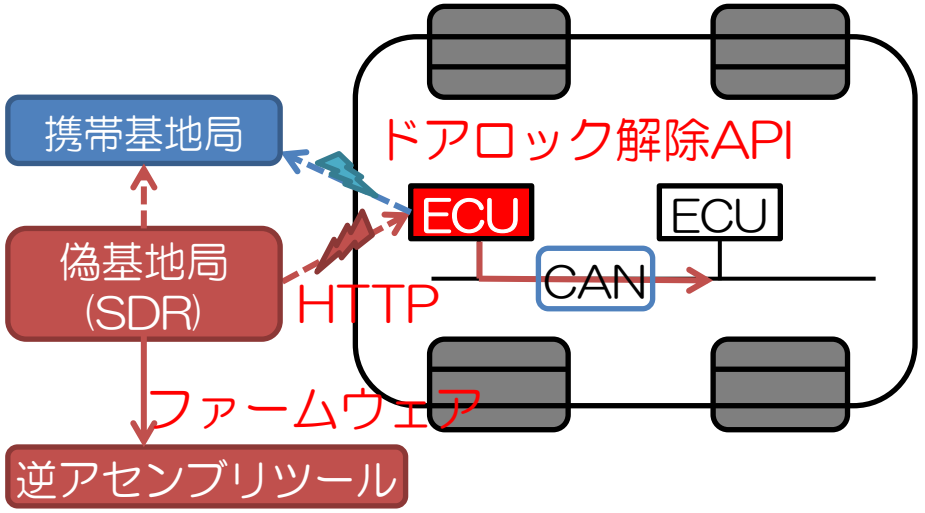
暗号技術によるトラスト

- 導入コストはかかる。長期維持にも課題あり
- 秘匿対象を設計全体から鍵データに極小化
- 技術的な安全性は検証されている

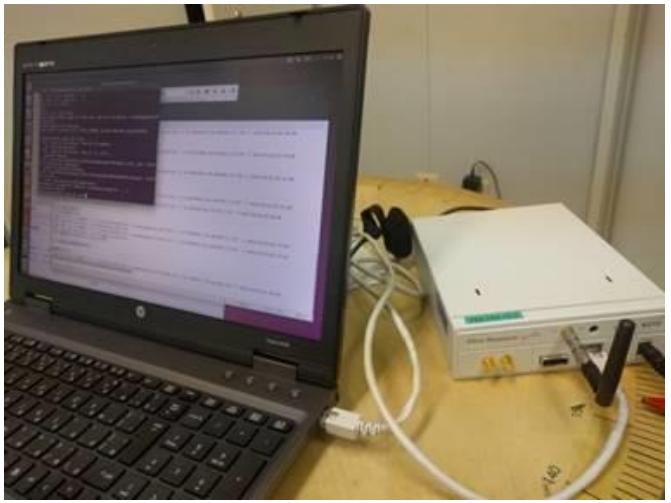
OTAに関係する事例　その2
ドイツ自動車連盟によるBMWの調査
（携帯基地局へのなりすまし）

セコムIS研究所
Intelligent Systems Laboratory

- ソフトウェア無線(SDR)と専用ライブラリ(OpenBSC)でGSMの基地局になりすます
- テレマティクスサービス(ConnectedDrive)への接続が偽基地局に接続
- HTTP通信を利用していたため中間者攻撃で通信内容観測
- さらに逆アセンブリツール(IDA Pro)を使ってファームウェアを解析
- 車両ドアのロック解除APIを発見しロック解除が遠隔から可能に



ソフトウェア無線(SDR)

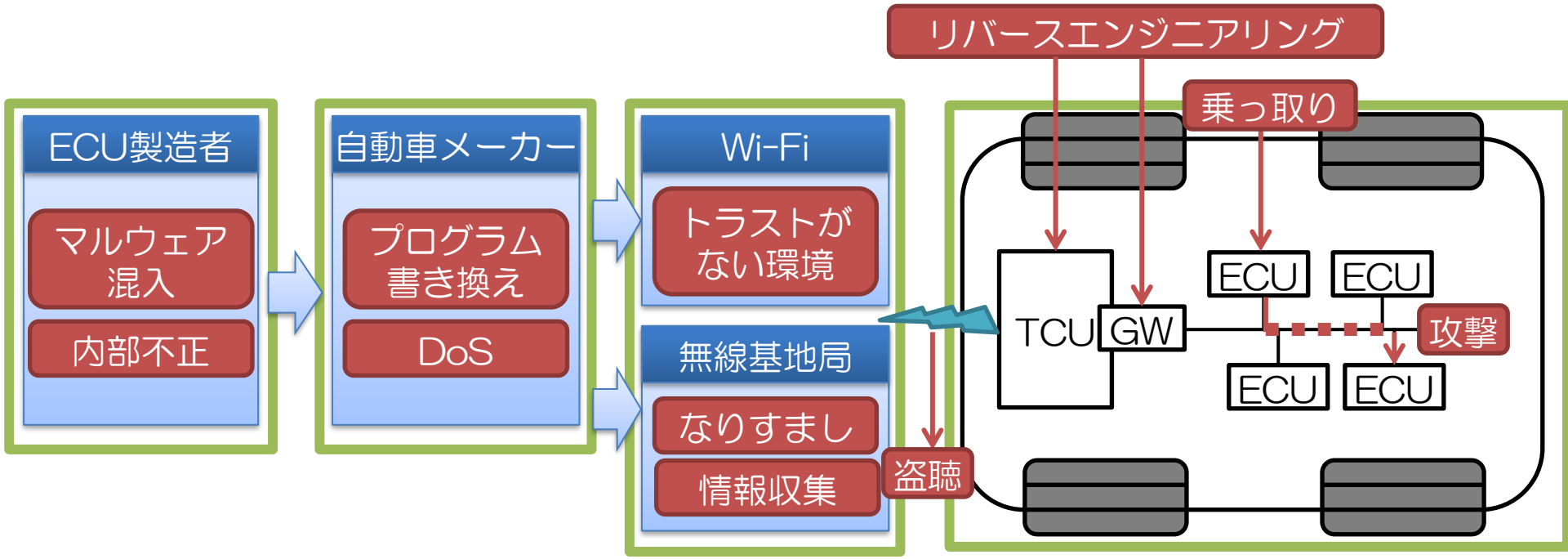


出典：http://www.sbdjapan.co.jp/bmw_connecteddrive_news/

OpenBSC:　SDRを使いGSMネットワークを構築できるオープンソース(プロジェクト)

OTAに対して想定される脅威

(1) サプライチェーン上における様々な脅威
(2) ECU間でのプログラム更新等の権限付与による脅威



プログラム作成者 (ECU製造者)

OTA事業者 (自動車メーカー)

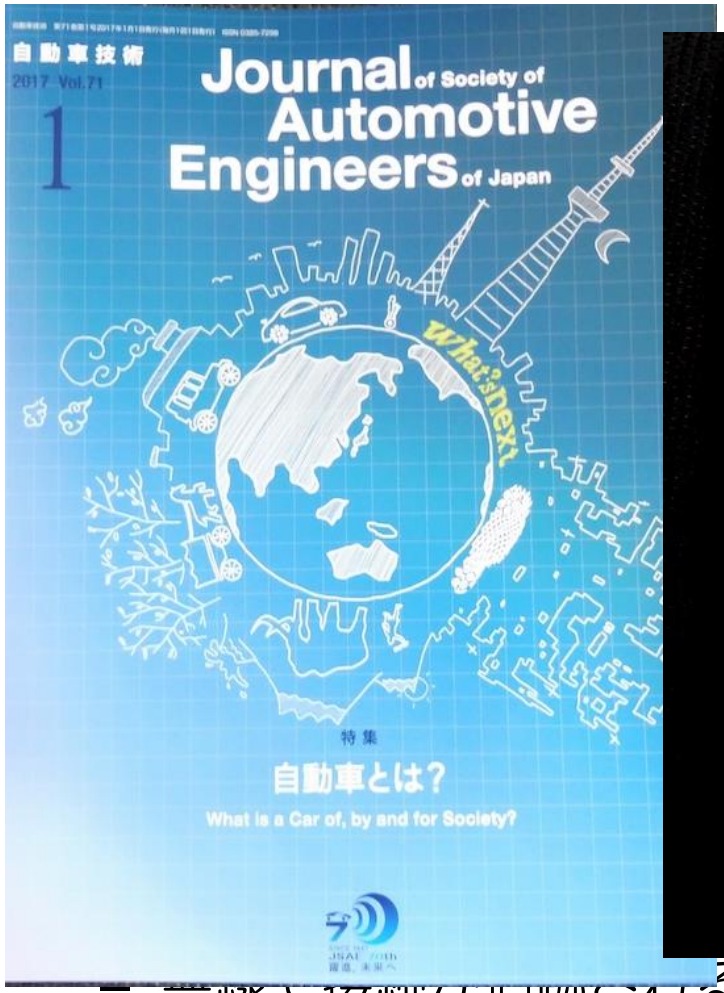
通信インフラ事業者

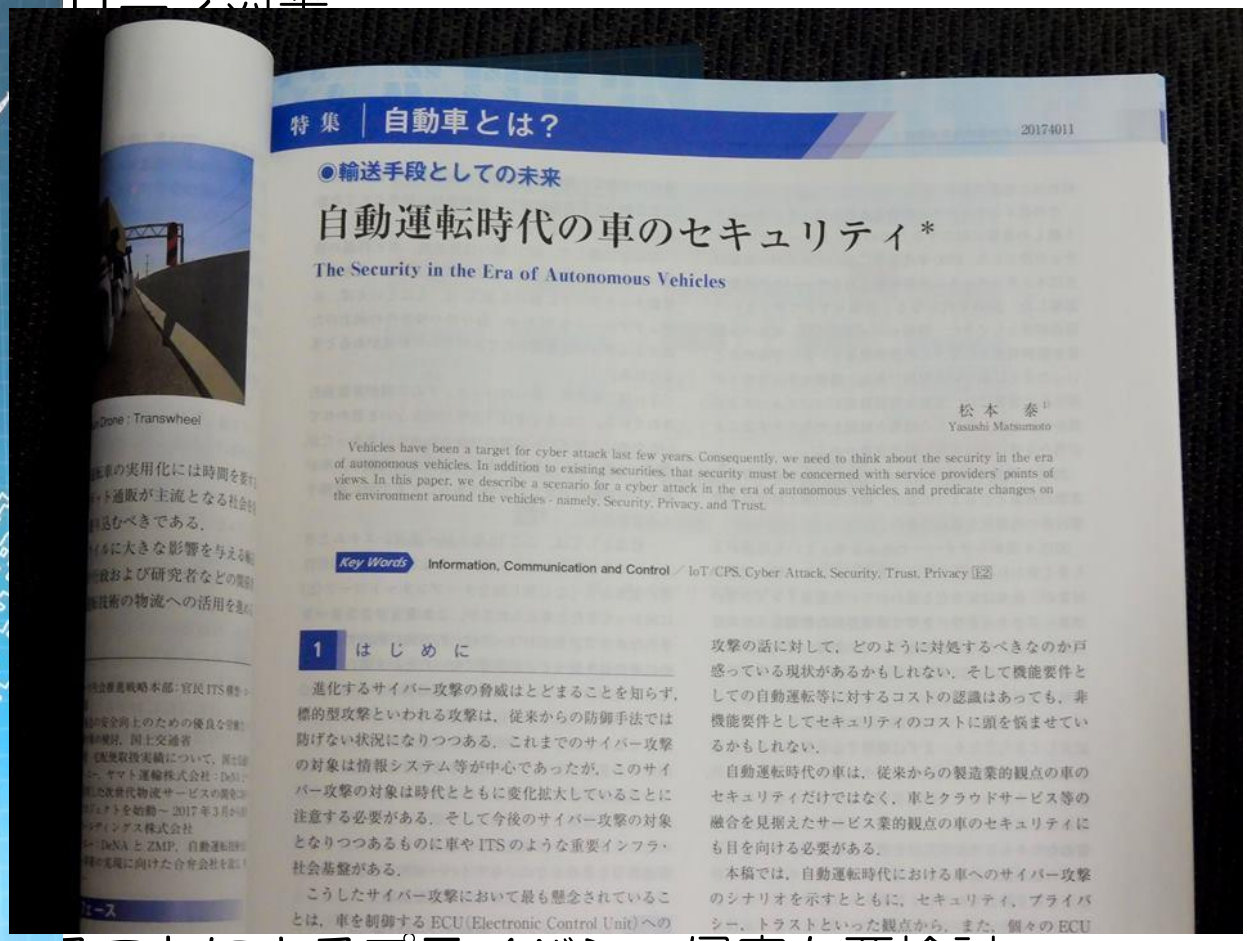
ユーザ

OTAにおけるソフトウェア・ファームウェアのサプライチェーン

自動車のサイバーセキュリティ対応

セコムIS研究所
Intelligent Systems Laboratory





- 無線で接続が追跡されることによるプライバシー侵害も要検討
- 暗号技術によるトラスト　→　次章へ

参考：自動車技術会・会誌「自動車技術」Vol71No1　2017年1月　「自動運転時代の車のセキュリティ」

セコムIS研究所
Intelligent Systems Laboratory

暗号技術によるトラスト

(1) なぜ暗号技術によるトラストが重要なのか？
(2) 暗号技術によるトラストとその役割
(3) マルチステークホルダーの暗号鍵管理（問題）
(4) 社会基盤・ロングタームセキュリティ（問題）

なぜ暗号技術によるトラストが重要なのか？

セコムIS研究所 Intelligent Systems Laboratory

- 設計の秘密の最小化・局所化
  - オープン化、コモディティ化の対応
    - 設計が知られてもセキュリティを確保する
  - バックドアーを防ぐ
    - 保守のための共通パスワードのような問題
- 物理的制約からの解放による（サービス）イノベーション
  - 物理的環境によるトラストから暗号技術によるトラストへ
    - 参考　→　付録　なぜ暗号技術によるトラストが重要なのか？
  - 車と外部のサービス間のトラスト
    - OTAの様な場所依存から場所に依存しないリモート保守
    - コネクテッドカー、スマートカー、クラウドサービスとの連携
      - 安全・安心・便利・快適
  - 車内のECU等の間のトラスト
    - 自動運転等に向けて、ECU間の高度な連携が求められる
      - Ex. ECUに格納された３次元地図を参照しながら自動走行

暗号技術によるトラストとその役割
暗号技術が提供する機能

セコム IS研究所 Intelligent Systems Laboratory

- 認証 – 機器の認証、サービスの認証等
  - CANに接続されたECU-ECU間の双方向の認証
    - 乗っ取られたECUから別の（無関係な）ECUへの攻撃を防ぐ
  - TCU(Telematics Control Unit) と外部サービス間の双方向の認証
- デジタル署名による証明、及び、証明書
  - コード署名 - プログラムコードの正当性の検証 – OTAでは非常に重要
  - 車のビジネスに係る様々なステークホルダー・エンティティ（人、組織、機器）の電子証明書と、そのエンティティによるデジタル署名による様々な証明 。サプライチェーンの電子証明によるトラストチェーン
    - ex. 正当な保守ツールの証明書、認定された修理工場の証明書、検査機関の証明書、検査機関により検査されたことの証明書、etc.
- 暗号化
  - TCUと外部のサービス間の暗号化
  - 車に格納されたプライバシー情報の暗号化

「暗号技術によるトラスト」 ≒ ビジネス的に要求される信頼関係を**暗号技術が提供する機能**により実現するもの

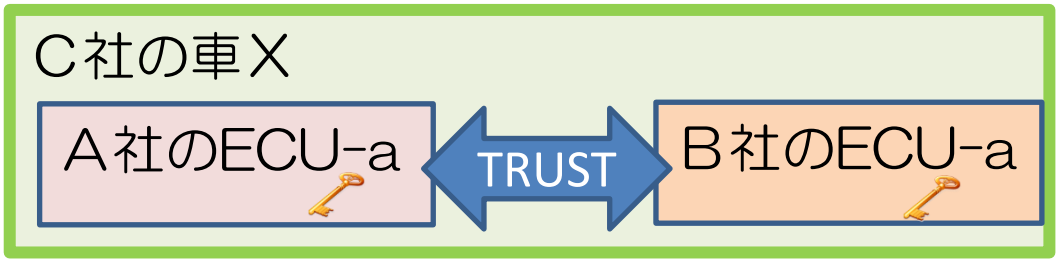
暗号技術によるトラストとその役割
暗号技術によるトラストの課題

セコムIS研究所
Intelligent Systems Laboratory

- 暗号技術の実装
  - リソース、コスト制約が厳しいECU等における暗号技術の実装
  - 暗号プロトコル等の複雑で脆弱性を生みやすい実装の問題
    - 暗号モジュールのブラックボックス化
- ハードウェアーセキュリティ（の重要性）
  - Root of Trust　– 設計の秘密の最小化のために必要な信頼の起点
    - 暗号鍵を起点としてトラストを構成する
    - 設計をオープンにしてもセキュリティを守るための仕組みの起点
- マルチステークホルダーの暗号鍵管理
  - マルチステークホルダー　– 車に関わる様々なステークホルダー
  - 暗号鍵管理　– 鍵生成、鍵配布、鍵更新、鍵の破棄まで
  - 自動運転時代の車関連ビジネスにおける様々なステークホルダー間のトラストの確立（非技術要件と技術要件の整合）
    - 車のサプライチェーンにおけるトラストチェーン・トラストモデル
- 社会基盤としてのロングタームセキュリティ
  - マルチステークホルダーでのトラストの確立　→　社会基盤そのもの

マルチステークホルダーの暗号鍵管理
なぜ暗号鍵管理が重要なのか？

セコムIS研究所
Intelligent Systems Laboratory



- 誰が、どういう権限でA社のECU-aの鍵を入れるのか
- C社の車のA社のECUは、全て同じ鍵なのか固有の鍵なのか？
- B社のECU-aをECU-bに交換した時、鍵はどうするのか？
- Etc……..

- 暗号鍵管理
  - 車に関わる様々なステークホルダー／エンティティが、固有（または共通）の鍵を持つ
- クレデンシャル管理
  - 車に関わる様々なステークホルダー／エンティティの証明
  - クレデンシャル管理の基礎が、暗号鍵管理になる
- 権限管理
  - 車に関わる様々なステークホルダー／エンティティの権限管理
  - ECU上のデータ／プログラム等の参照、書き換え等
  - 権限管理の基礎が、クレデンシャル管理になる。

暗号鍵管理モデル ＋ クレデンシャル管理モデル ＋ 権限管理モデル ≒ トラストモデル

マルチステークホルダーの暗号鍵管理
ECUに係るステークホルダーと権限管理

セコムIS研究所
Intelligent Systems Laboratory

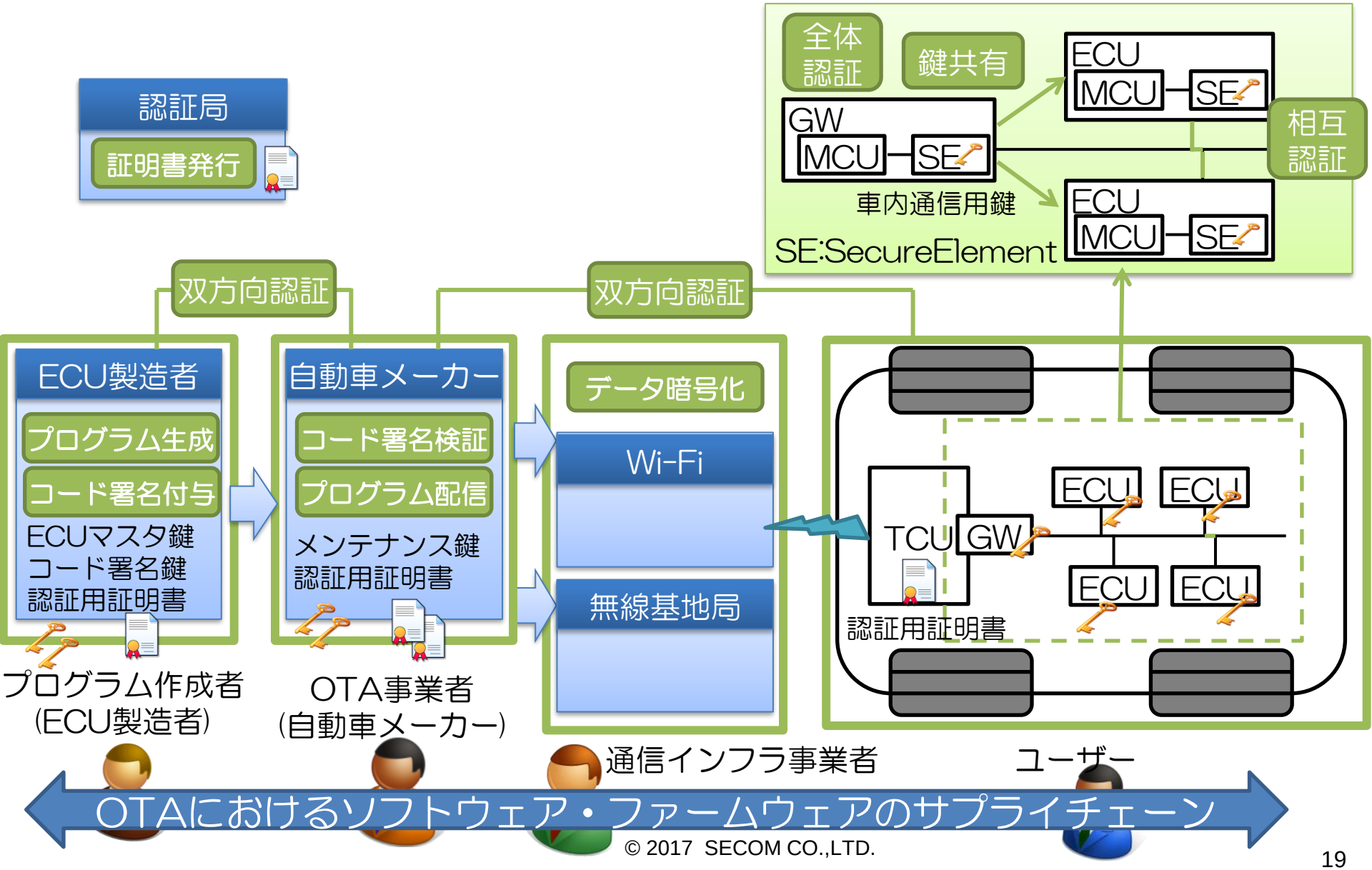
番号	ロール	権限レベル	権限
ユーザロール1	ECU製造者	高い	ECU自体へのアクセスとアップデート
ユーザロール2	自動車メーカー		各装置へのアクセスとアップデート
ユーザロール3	修理工場		自動車メーカーから配布されたツールをもとに各装置へのアクセスとアップデート
ユーザロール4	検査機関/警察		OBDポートから各装置の状態の読み込み
ユーザロール5	オーナー/運転手	低い	アクセス権なし

Horizon 2020 Program, SHARCS(Secure Hardware-Software Architectures for Robust Computing Systems), Deliverable D2.1, “SHARCS Applications and framework requirements for secure-by-design systems”から抜粋・訳

- こうした、マルチステークホルダーによる権限管理の理想モデルとして、PKI（公開鍵基盤）による各エンティティを証明する公開鍵証明書と、証明された各エンティティの権限を証明する属性証明書を使うモデルがある。
- しかし、すべてのECUにおいて公開鍵を扱うことは難しく、公開鍵と共通鍵のハイブリッドモデルを考える必要がある　→これが簡単ではない！！

マルチステークホルダーの暗号鍵管理
OTAを想定した鍵・証明書の配置の考え方の一例

セコムIS研究所
Intelligent Systems Laboratory

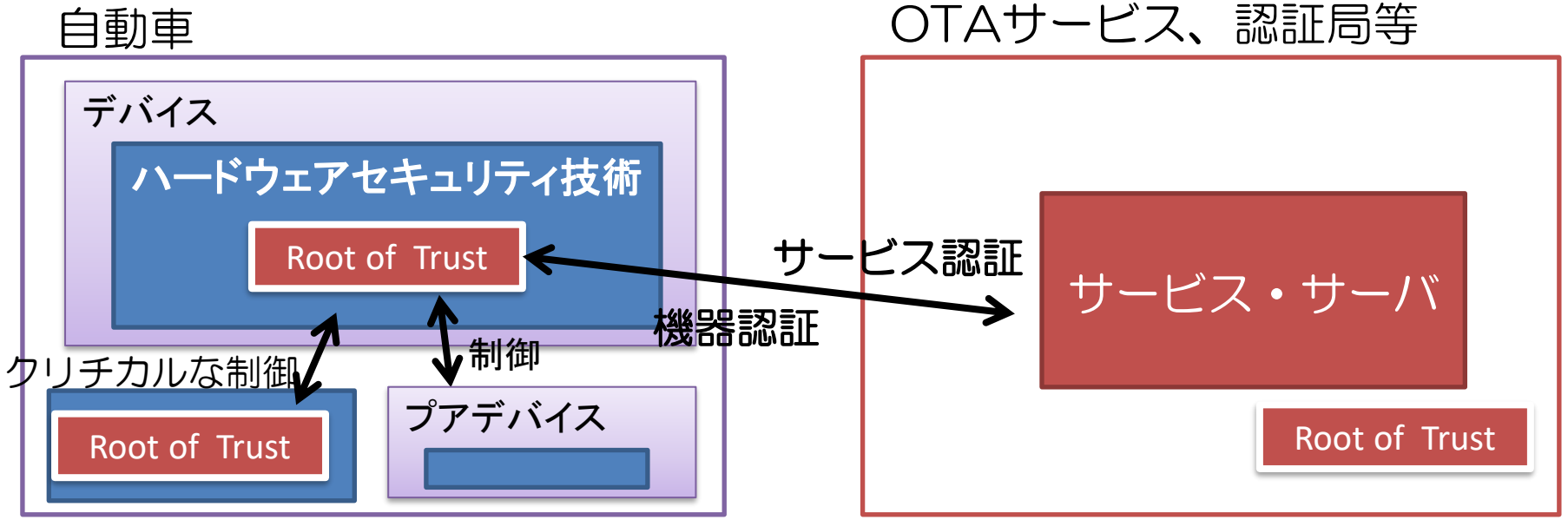


社会基盤・ロングタームセキュリティ（問題）

セコムIS研究所 Intelligent Systems Laboratory

- ロングタームセキュリティの対応
  - プログラムの脆弱性は、OTAで対応できるが、Root of trustとなる暗号鍵等は、車のライフサイクル以上に、長期的なセキュリティに対応する必要がある。
    - GW-ECU、各ECUの暗号鍵、外部のシステムの暗号鍵
  - 車/OTA等のシステム全体
    - 例えば、プログラムにコード署名する証明書の信頼点の鍵（ルート認証局の署名鍵）は、数十年に渡り守りきる必要がある
- 暗号システム全体の破たんに繋がる暗号危殆化に対する対応
  - 暗号アルゴリズムの危殆化の対応（ex. 暗号アルゴリズムの移行）
    - 暗号アルゴリズムの2010年問題(SSL/TLS証明書の場合）
  - 暗号鍵・暗号システムの危殆化
    - ex. BCASカード等　（ＢＣＡＳカードのバックドアーの発覚）
- 暗号アジリティの確保　（暗号アルゴリズムの移行性の確保）
  - 90年台にIETFにおいて設計された初期の暗号プロトコルは、仕様上の暗号アジリティが無いものが多かった
    - 固定長のプロトコル仕様、プロトコルと暗号アルゴリズムが一体化等
  - 初期の暗号技術の実装は、実装上の暗号アジリティが無かった
    - リソースの限られるECU等では？？

社会基盤・ロングタームセキュリティ（問題）
長期に渡る暗号鍵管理



- どの時点においても上記の関係が崩れない　＝　サービス継続性
  - サービス継続性は、可用性、BCPの観点だけでないことに注意する必要がある。
  - サービス側は、車単体のライフサイクルよりも、ずっと長期間に渡り、暗号システムの破たんを絶対に避ける暗号鍵管理が要求される。

社会基盤・ロングタームセキュリティ（問題）
暗号アルゴリズムの移行
TLS/SSLにおける暗号アルゴリズムの2010年問題

セコム IS研究所 Intelligent Systems Laboratory

レイヤー	関係者	一般的な世代交代の課題	TSL/SSLの場合
暗号アルゴリズム	CRYPTRECやNIST等の暗号アルゴリズムの評価機関	暗号アルゴリズムの脆弱化	NIST等の勧告
標準	IETF等の標準化団体	プロトコル等の暗号アルゴリズム移行性の確保	暗号アルゴリズムのダウングレード攻撃等に対応するプロトコル仕様へ変更
実装	様々な暗号モジュールの実装、オープンソース	暗号モジュールにおける暗号アルゴリズム移行性の確保	古い携帯電話が、RSA2048bitに対応できず2016年まで問題を引きずった
社会基盤トラスト	トラスト・ビジネスを形成する様々なステークホルダー	多数のステークホルダー間の調整	CA/Browser forum(CABF)等の合意形成の場

参考：　SSL証明書における暗号世代交代(暗号世代交代と社会的インパクト)

まとめ

セコムIS研究所
Intelligent Systems Laboratory

- Over the Airソフトウェア更新(OTA)は、リコール対応等のために、車にとって必須の機能になりつつあるが、今後の自動運転時代には、ソフトウェアの複雑化が進み、この複雑化に伴うソフトウェア脆弱等の対応のために、更にOTAが重要になることが予想される。
- その一方、 安易なOTAの仕組みは、新たなバックドアーを生む危険性もはらんでいる。安全なOTAを考えた場合、これまでの自動車にはなかった「暗号技術によるトラスト」の設計、実装、長期にわたる運用が、非常に大きな役割を果たす。
- 「暗号技術によるトラスト」設計、実装、運用では、暗号鍵の配置、配布、から破棄までの鍵管理の考え方が非常に重要になる。
- 「暗号技術によるトラスト」 は、OTAの基本的な機能を提供するだけではなく、今後のコネクテッドカー等と、様々な車にまつわるステークホルダー間との信頼関係を構築するベースの機能を提供することになる。
- 今後の自動車を起点としたイノベーション・新たなビジネスモデルも見据え「暗号技術によるトラスト」に取り組む必要がある。

参考文献

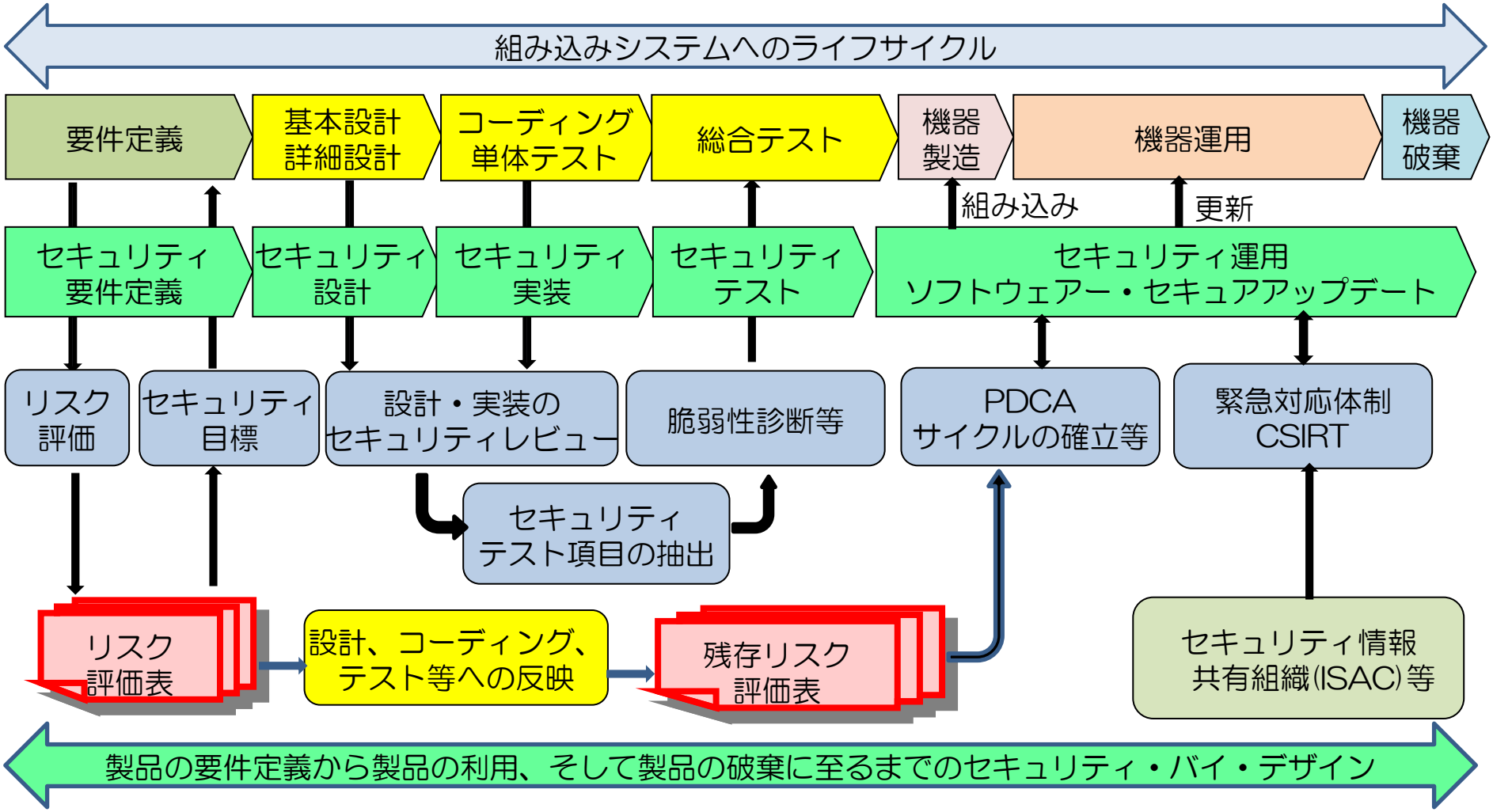
- 自動車技術会・会誌「自動車技術」Vol71No1　2017年1月　「自動運転時代の車のセキュリティ」
- IoTセキュリティを支える 「暗号技術によるトラスト」の重要性 http://www.jnsa.org/jnsapress/vol41/2_kikou_2.pdf
- 重要インフラ事業者が理解するべき サイバーセキュリティの動向 http://www.i-s-l.org/shupan/pdf/SE183_4_open.pdf
- SSL証明書における暗号世代交代(暗号世代交代と社会的インパクト) Transition of Cryptographic Algorithms in SSL Certificates
  - http://ci.nii.ac.jp/naid/110008762202

付録

- セキュリティ・バイ・デザイン
- なぜ暗号技術によるトラストが重要なのか？
- 認証局における暗号鍵管理
- 暗号アルゴリズムの2010年問題

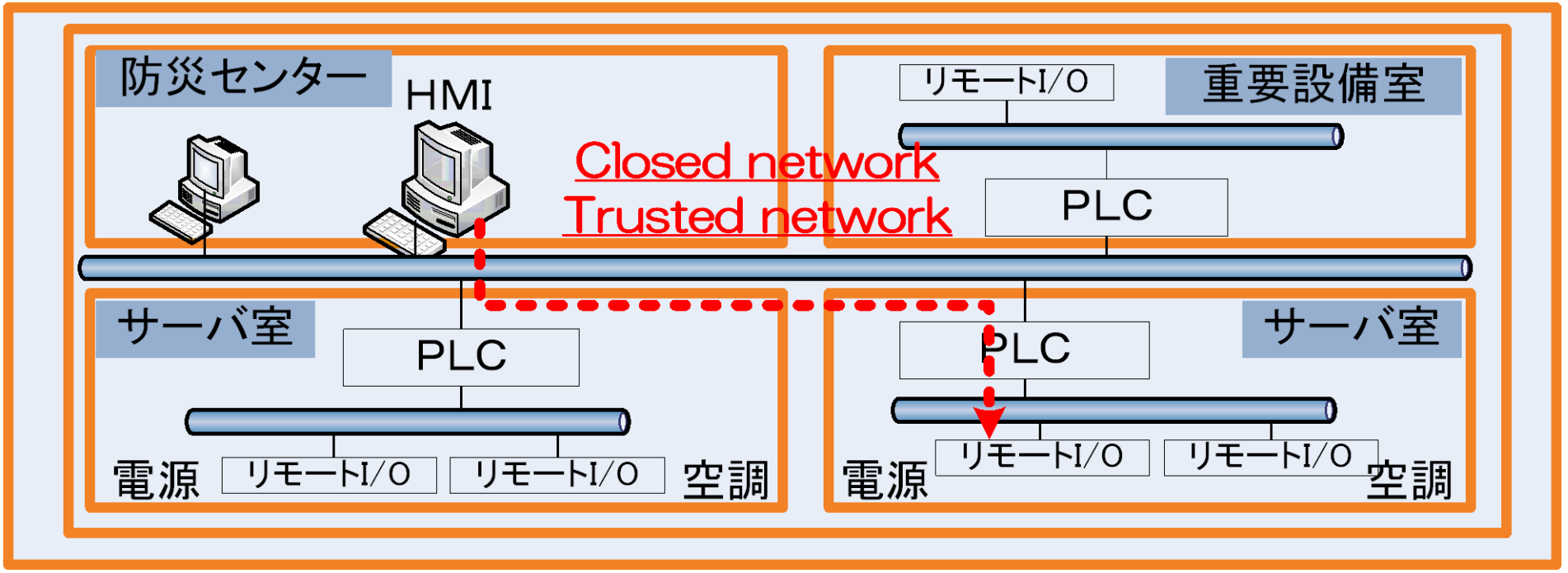
脆弱性対応としてのセキュリティ対策
セキュリティ・バイ・デザインの考え方

セコムIS研究所
Intelligent Systems Laboratory



なぜ暗号技術によるトラストが重要なのか？（１）
重要インフラ等におけるトラスト(Trusted Network)の仕組み

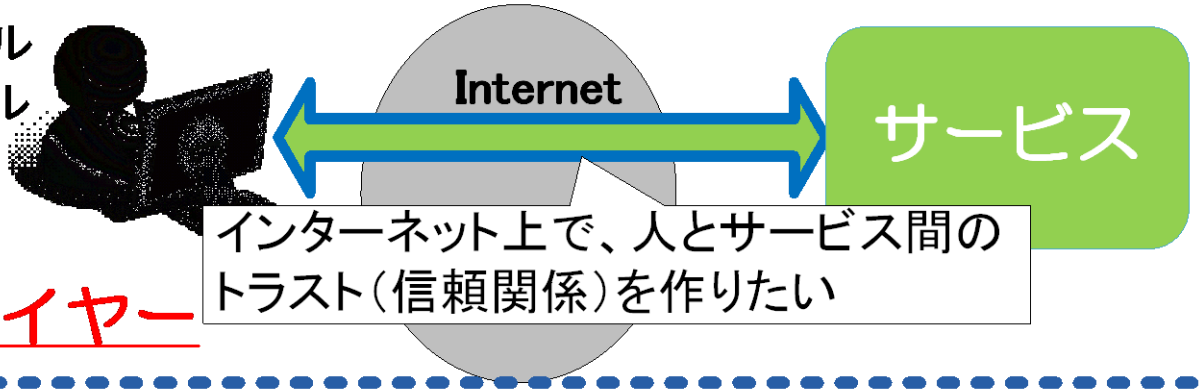
重要施設という物理的環境・物理的なゾーニングによるトラスト



HMI: Human Machine Interface　　PLC: Pogrammable Logic Controller

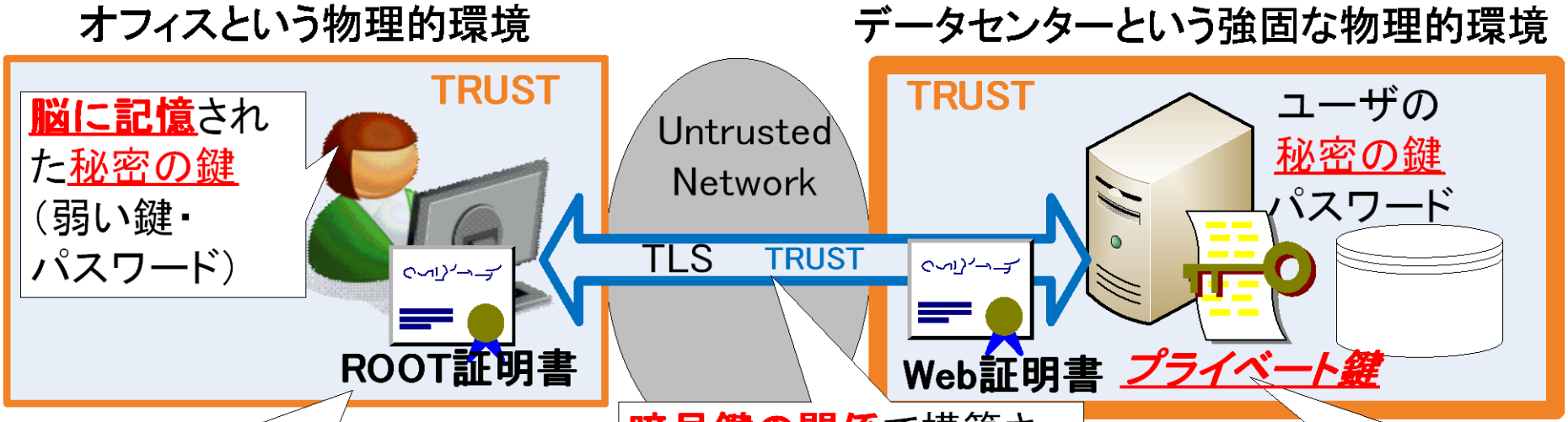
- ファシリティ系のネットワークではBACnet等のプロトコルが利用されるが、多くの場合、暗号技術によるトラスト(機器認証等)は実装されていない。

なぜ暗号技術によるトラストが重要なのか？（2）
既存の「物理的環境＋暗号技術」によるトラスト



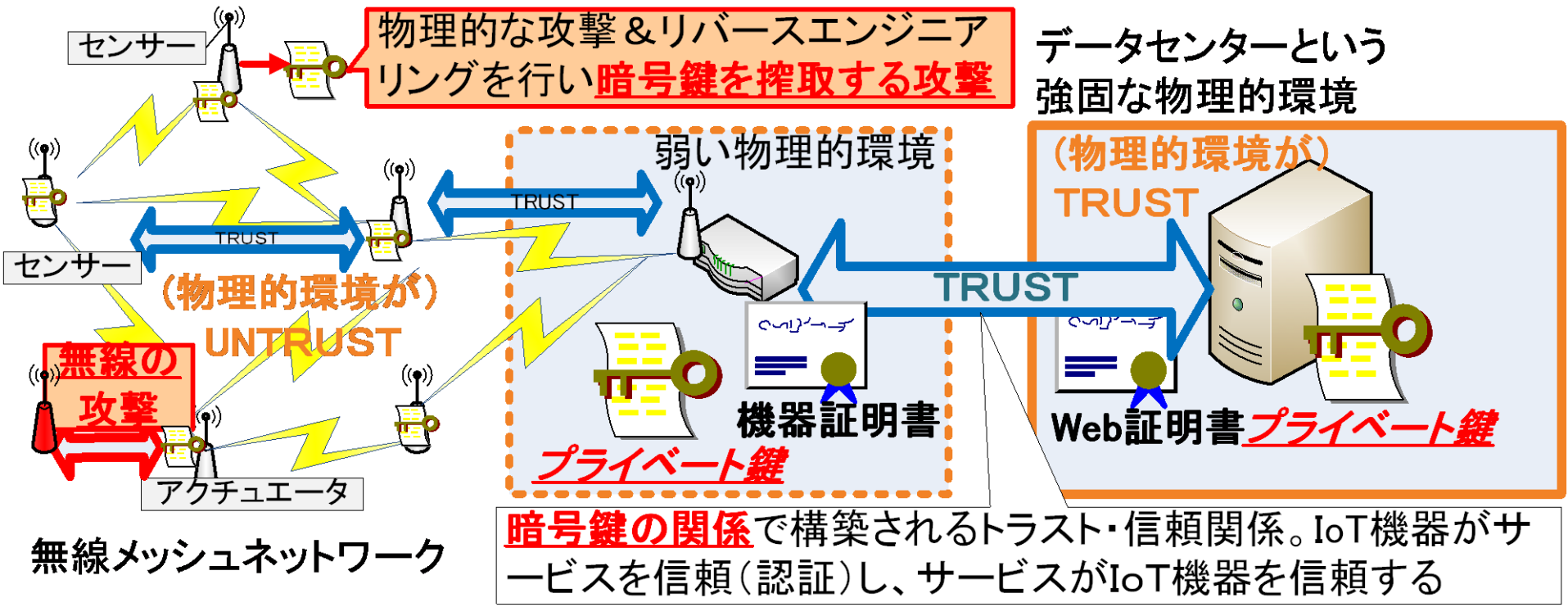
ビジネスレイヤー

実装レイヤー



なぜ暗号技術によるトラストが重要なのか？（3）

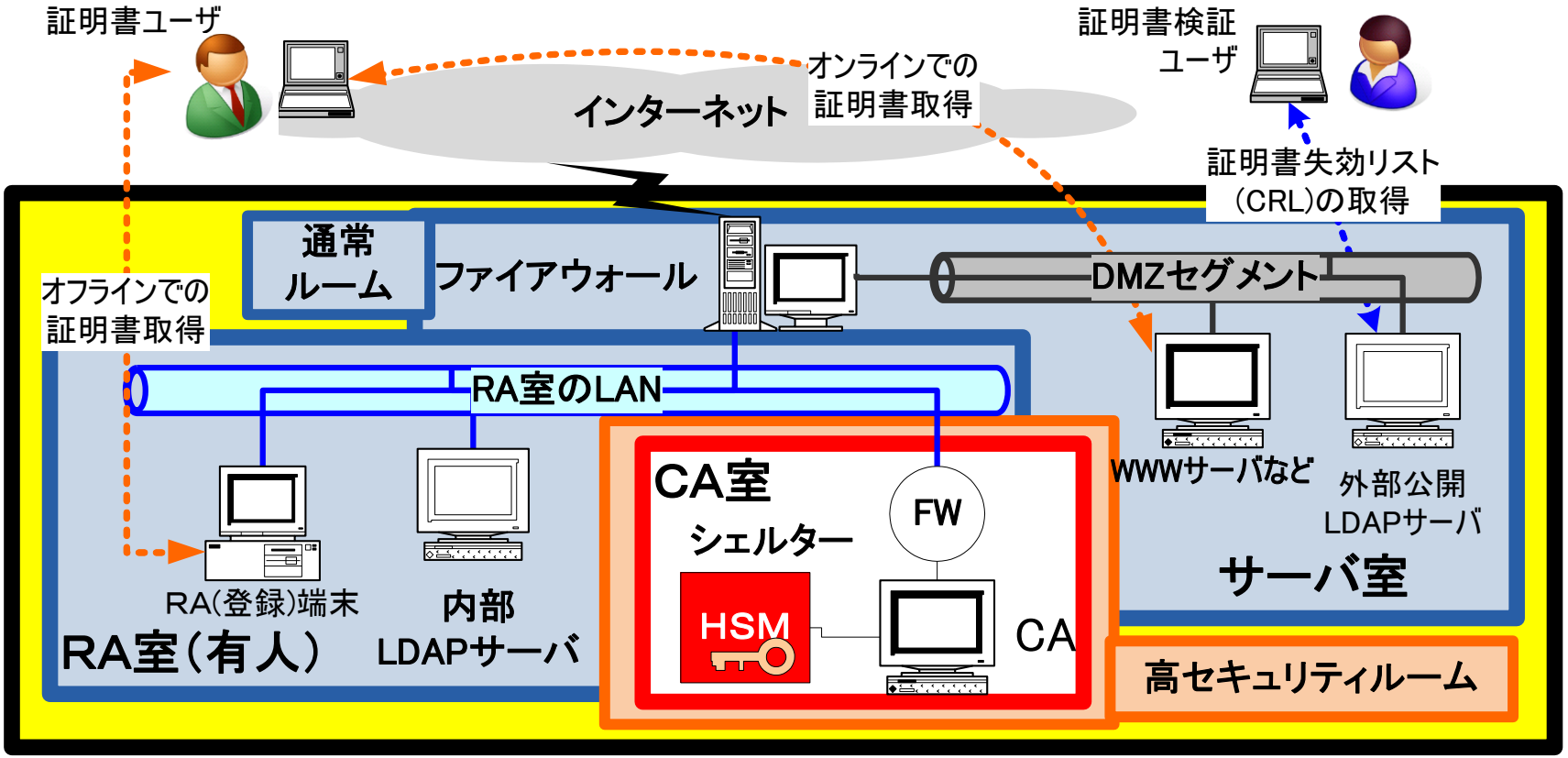
（物理的環境に依存しない）暗号技術によるトラスト
⇒　　IoT時代のトラスト



- IoT機器が、「弱い物理的環境」において多く利用されることが想定。
- 物理的環境による「暗号鍵」の保護に代わるIoT機器自身のハードウェアセキュリティの重要性
- 大量のIoT機器を接続するラストワンマイル、ラストワンメートル等での無線の要求　－　必然的に暗号技術によるトラストが重要になる

認証局における暗号鍵管理
機密性、完全性、可用性等の両立

セコムIS研究所
Intelligent Systems Laboratory



・「ＣＡ室」、「ＲＡ室（登録業務）」、「サーバ室」の３つの部屋を使い分け（物理セキュリティ）
　・入室権限が異なり権限が分離される。CIAの要件により部屋を使い分ける 。
・サーバ室はCIAのA(Availability)重視　（24時間ノンストップ）
　・Integrityを保証するために署名されたデータのみ扱う
・CA室は通常無人で運用されＣＩＡのＣ（Confidentiality）重視
　・CA(Certification Authority)は、Availabilityを要求しない技術的アーキテク

認証局における暗号鍵管理　－　セコム認証サービスの事例

- 基本的な運用ポリシーを公開
- 運用ポリシーに則り運用されているかを外部監査

セコムIS研究所 Intelligent Systems Laboratory

- セコムパスポート　for G-ID 認証運用規定　2016 年 7 月 29 日 Version 11.20
  - https://repository.secomtrust.net/PassportFor/G-ID/repository/CPS.pdf
- 6. 技術的セキュリティ管理
  - 6.1 鍵ペアの生成とインストール
    - 6.1.1 鍵ペア生成
    - (1) CA 秘密鍵生成
      - CA の秘密鍵は、CAサーバシステムを最初に立ち上げる際に生成される。本サービスでは CA の署名用鍵ペアを FIPS140-2 レベル3の認定を取得したハードウェアセキュリティモジュール(Hardware Security Module、以下、「HSM」という)上で生成する。CA の秘密鍵 の生成作業は、CA 室又は BC 認証設備室内でサービス運用管理者立会いのもと、複数名の CA 管理者が操作を行うことによって行われる。
  - 6.2 CA 秘密鍵の保護
    - 6.2.1 暗号モジュール
      - CA の秘密鍵の生成、保管、署名操作は、FIPS140-2 レベル3の認定を取得した HSM を用いて CA 室又は BC 認証設備室で行われる。
    - 6.2.2 秘密鍵の複数人コントロール
      - CA の秘密鍵の生成を完了するには、サービス運用管理者と複数名の CA 管理者を必要とする。生成後に発生する秘密鍵の更新等の秘密鍵管理についても同様である。

暗号アルゴリズムの2010年問題（移行問題）

競争の中でのトラストの維持

セコムIS研究所
Intelligent Systems Laboratory

モバイル
キャリア

メモリの関係から、よく使われるルート証明書だけを格納したい。

認証局

「全ての端末をサポート」して欲しいというお客様がいる限り古いルート証明書を使うしかない。

ブラウザベンダ

基準を満たしている限り、証明書リストに入れていくけど、暗号のことはどうしましょーね。
後、古いOSは、勘弁してね？

信頼できる証明書なんて分らないからブラウザを信頼するしかない

利用者

SSL

サーバ運営者

ともかくPCも携帯も全ての端末をサポートして欲しい