SWEST17
組込みシステム技術に関するサマーワークショップ

車載セキュリティにおける課題

Renesas Electronics Corporation
Automotive Information Business Department
Daisuke Oshida

2015/7/23 Rev. 0.00

自己紹介

- 1997年～2001年 （株）MCシステムにてコピーの営業に従事
- 1999年～2001年 （株）中勢ゴムにてドアゴム製造業務に従事
- 2001年～2004年 （株）APROより派遣にてCCDの開発
- 2005年 NEC Electronics（株）に中途入社
  - 2005年～2010年 プロセス開発・デバイスインテグに従事
    - 2005年～2010年　65nm～28nmの配線技術の研究開発
  - 2011年2月末より、技術営業職に職種転換
    - 2011年～2013年　PUFを用いたセキュリティソリューション検討
ISO/IEC 15118, IEC 61980標準化委員
    - 2013年～　V2X向けセキュリティソリューションの開発

- 大まかな人物像
  - 通勤往復6時間超（山梨～東京）
  - 酒好き
  - タバコがやめられない
  - 趣味：ダイエット（32kg減/2年間）
  - 特技：リバウンド（現在1年間で24Kgリバウンド中）
  - 海釣り全般が趣味だったが、結婚と同時に諦め

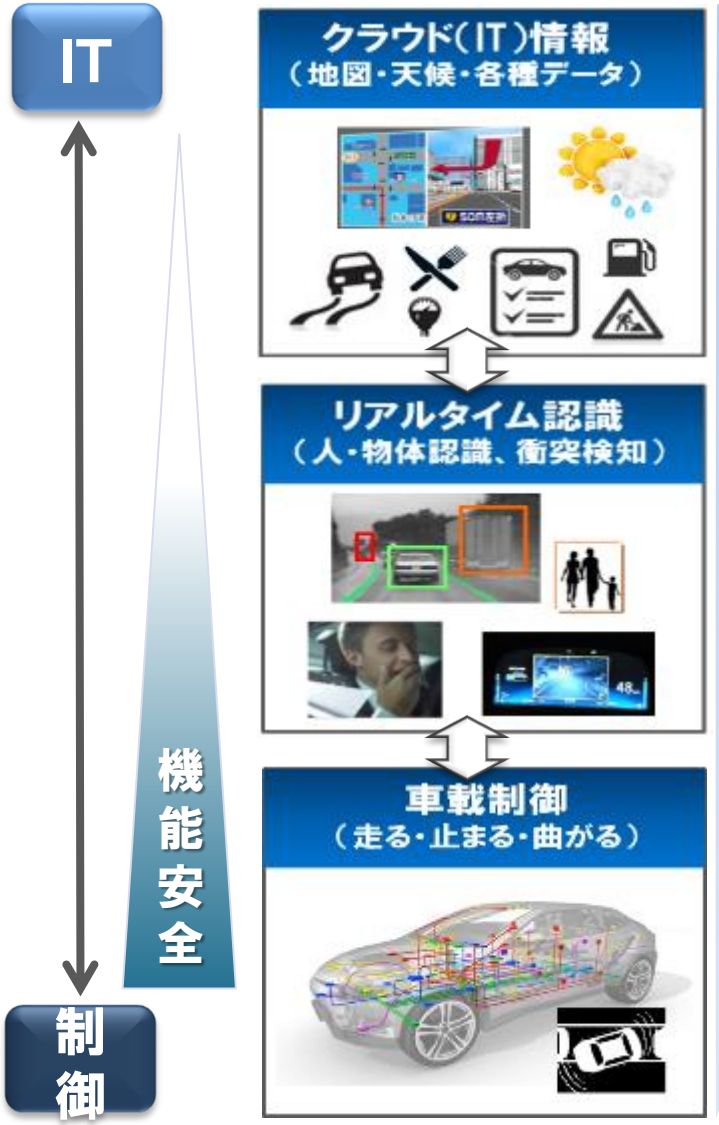
104cm（当時）

地図的にココらへん
ほったらかしの湯

ほうとうガチバトル
３連覇の歩成

これからの自動車
～走る・曲がる・止まる　から　賢い車　へ

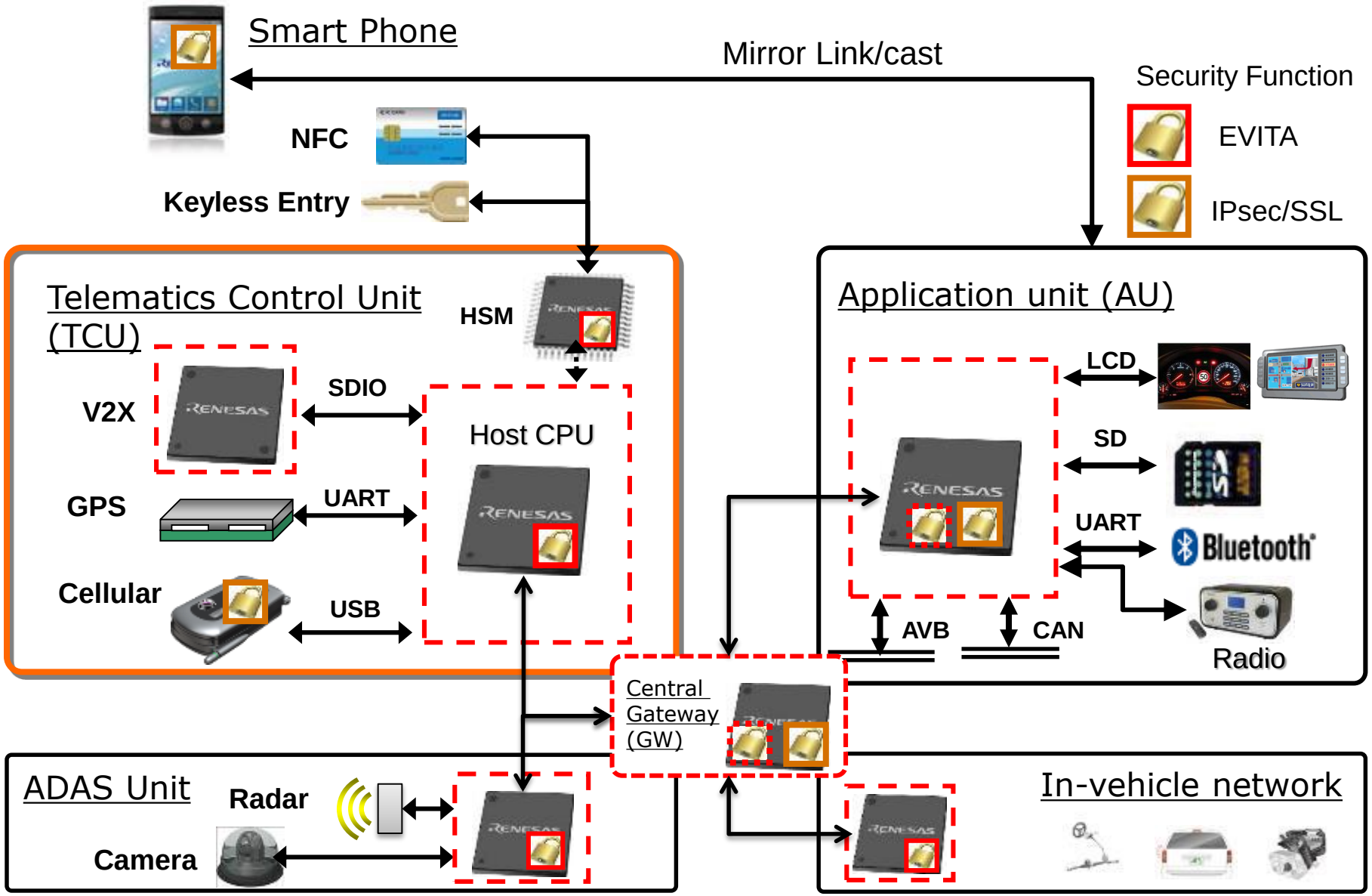
スマート社会における「賢いクルマ」



クラウド(IT)情報 ・リアルタイム認識・車両制御の連動が賢さの秘訣

**安全・安心・快適な
これからのクルマ社会を実現する。**

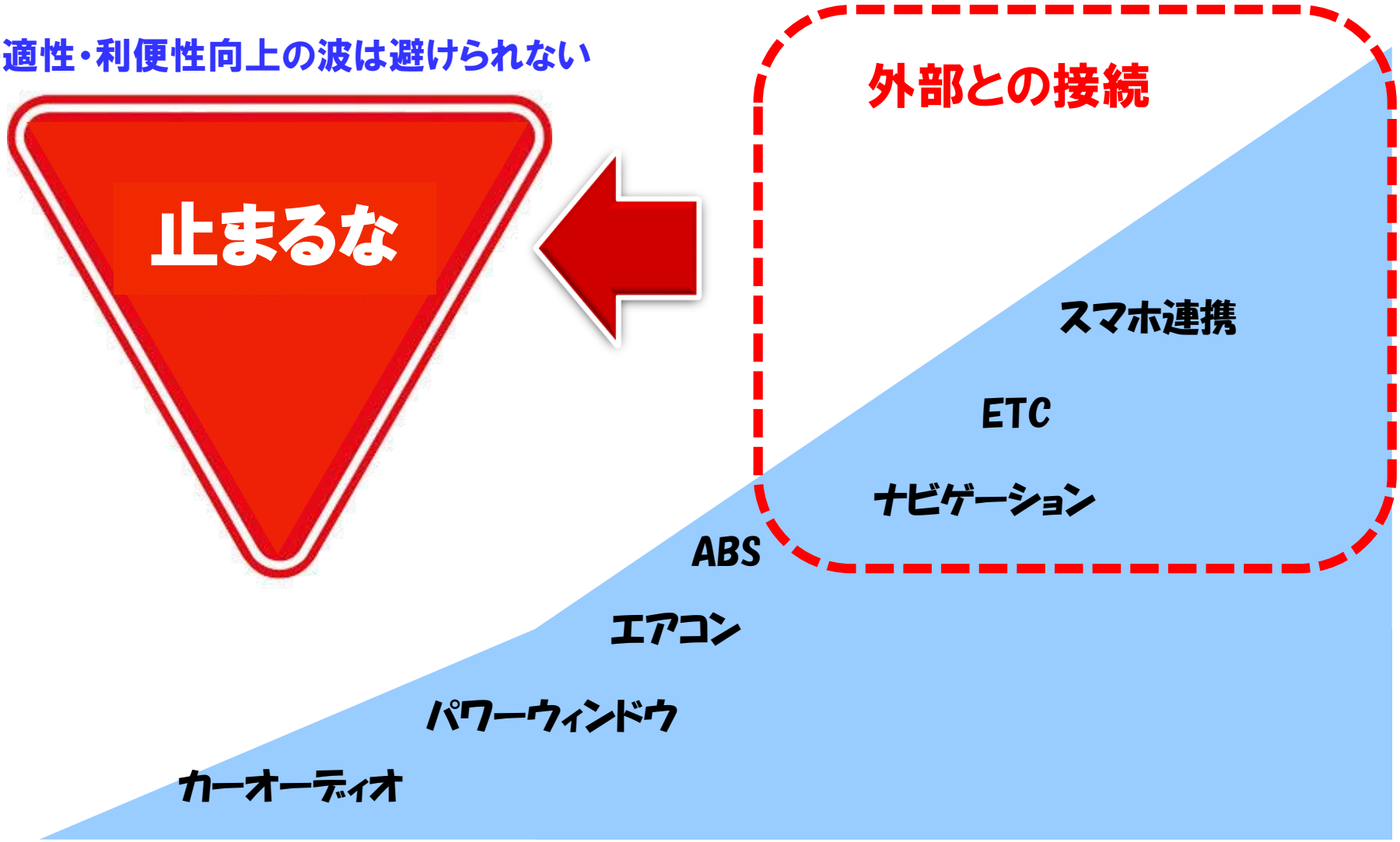
Connectivity System in Automotive



自動車にセキュリティは必要か？

快適性・利便性への要求

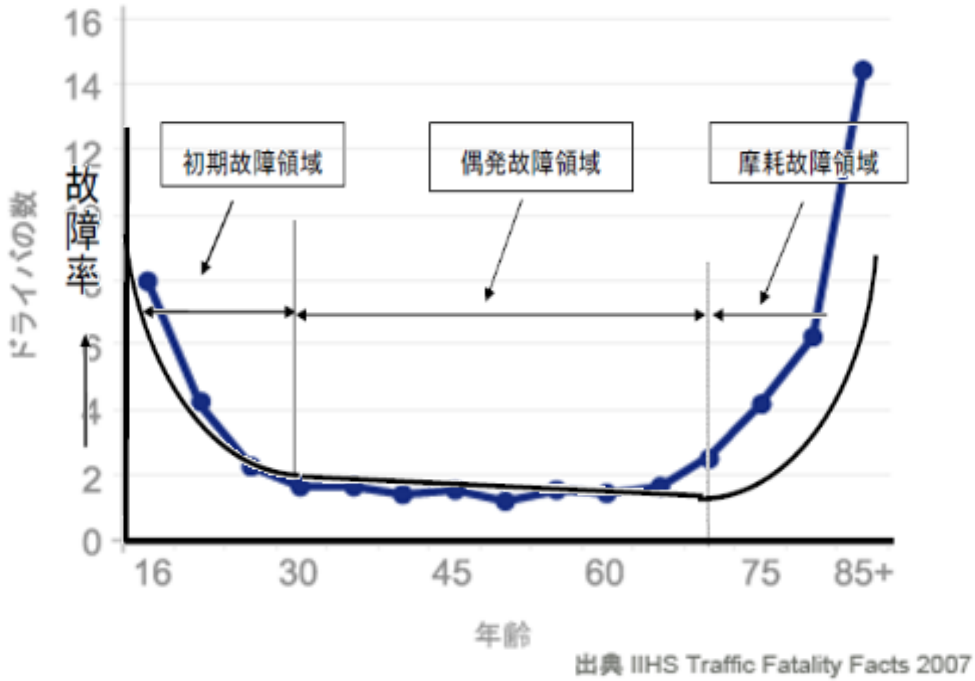
快適性・利便性向上の波は避けられない



安全性への要求

半導体の経年劣化

100,000 マイル当たりの死亡事故に関与するドライバの数（米国）



出典 IIHS Traffic Fatality Facts 2007

“しわ”の増加 ＝ 運転能力の劣化

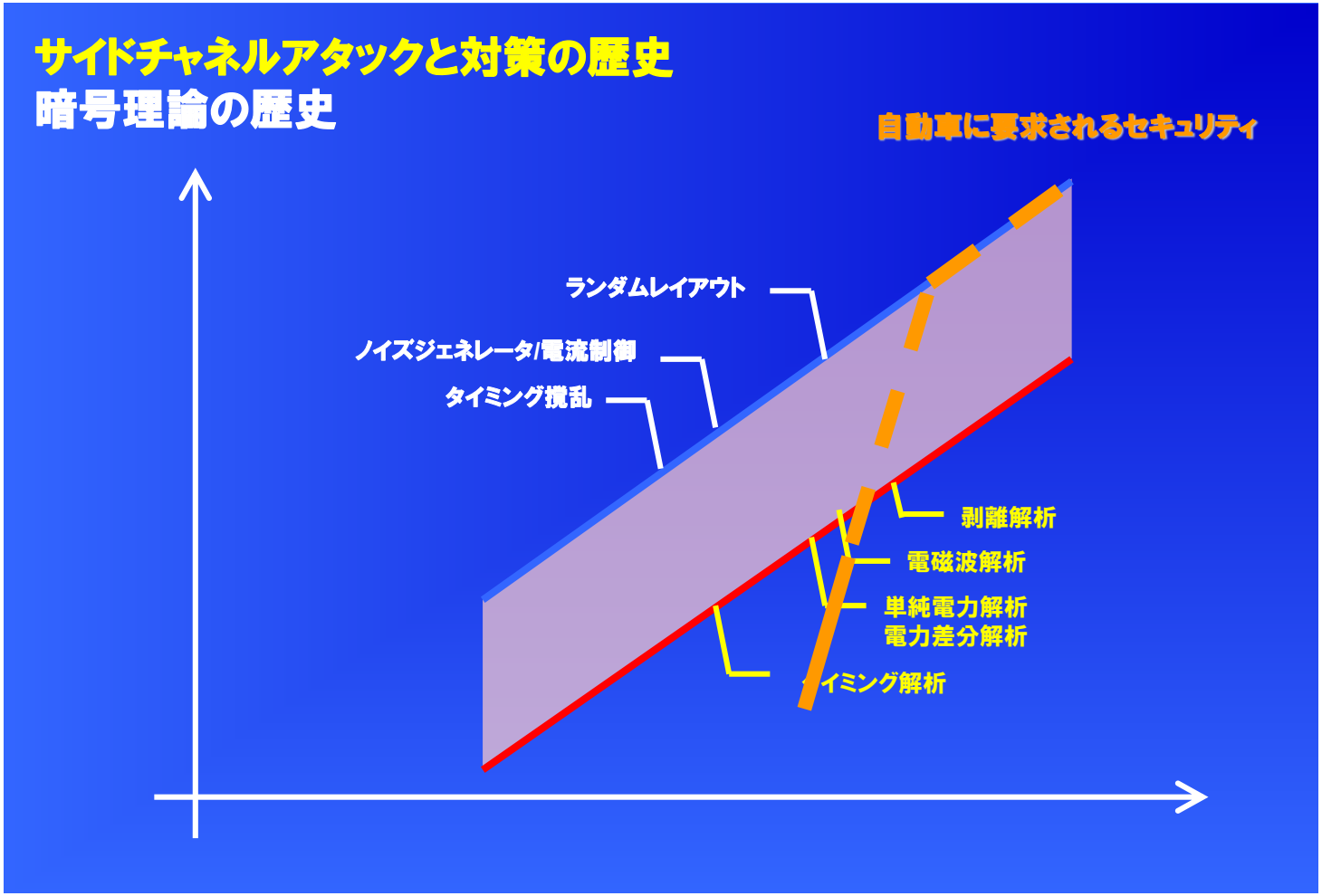
安全への要求の高まり⇒自動走行の流れ

自動車で守るべき資産の推移

情報所有者	資産分類	例	PC	1980年代	2000年代	2010年代
エンドユーザー	安全(走行性能)に関わる情報	コンピュータプログラム(エンジン・ブレーキ等)	—	○	○	○
	証拠情報(改竄されてはいけない情報)	運転履歴、事故時の情報(車速・ブレーキ等)	—	—	○	○
	著作権情報(ユーザー・第三者)	音楽・DVDデータ等	○	—	—	○
	プライバシー情報	氏名・住所・電話番号・運転履歴・事故時の情報(車速・ブレーキ等)	○	—	—	○
	個人情報	クレジットカード情報等	○	—	○※	○
	盗難に関わる情報・便利機能に関わる情報	ドアロック制御情報・エンジン制御情報(始動)・マルチメディアが使用する情報・シート位置補正情報等	—	—	○	○
エンドユーザー/自動車会社	品質・性能情報	ウォーニング、ダイアグ等	○	—	○	○
自動車会社	知的財産(車両メーカー)	各種コンピュータープログラム・各種データ	○	—	○	○

自動車内部にある守るべき資産は増加傾向にあり、PCと同等に近づきつつある

セキュリティ技術のトレンド



自動車市場で要求されるセキュリティ技術は、ネットワークの技術に比べて後発である
しかし、攻撃手段が確立しているので、ネットワークと同等のセキュリティ技術が必要である

自動車のセキュリティ上の脅威

たくさんある自動車における脅威

・なりすましサーバからマルウェア/不正データ受信

・不正V2X通信データ受信

Navi

V2X com

Dashboard

Gateway

OBD2

EPS

Engine

Brake

ADAS

・記録媒体、情報端末を通じたマルウェアの混入

・不正CANデータ混入
・リプログラミング

・シリアルライタによるチューニング
・ソフト読出し

・センサ情報改竄
・ECUの置き換え

・従来からある脅威

・ITと制御の融合で生じる脅威

自動車におけるセキュリティの重要性

善良な一般市民を自称する作者が考えても、
これだけの悪事が挙げられる！

偽チップ（複製）または、ソフトウェアの改竄

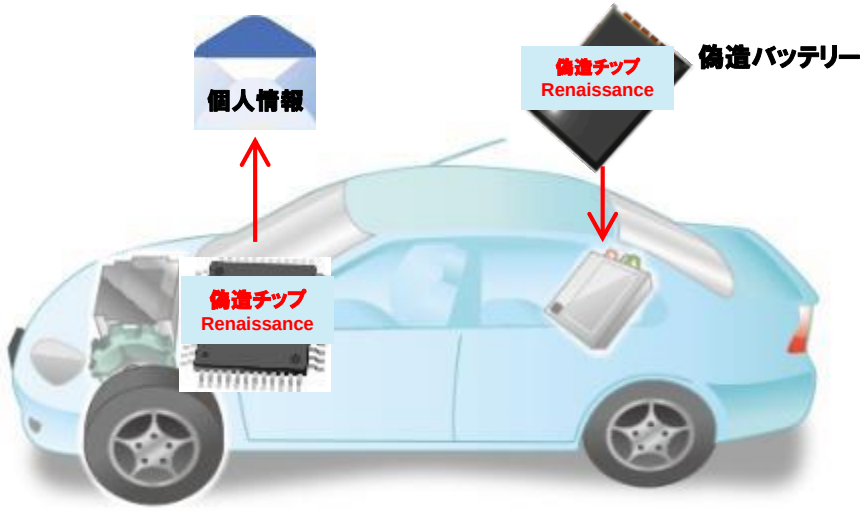
⇒純正と偽った商品の流通

（EV/PHV用バッテリー、電源ケーブル等）

保証されていないバッテリーの使用
最悪は燃えるケースも

⇒バックドアを使った個人情報の流出

クレジットカード情報、個人住所などの悪用
被害金額が膨大になる。



ECUの改竄

⇒ECU内部の設定変更（リミッターカット等）

リミッターカット、燃料費調整など
⇒重大事故への発展。車の寿命も短くなる。

⇒走行距離の偽造

タコメーターの初期化
⇒中古車市場における不正な金額での取引
最悪はカーメーカーの信用を落とすことも

⇒自動車の盗難（イモビライザーへのアタック等）

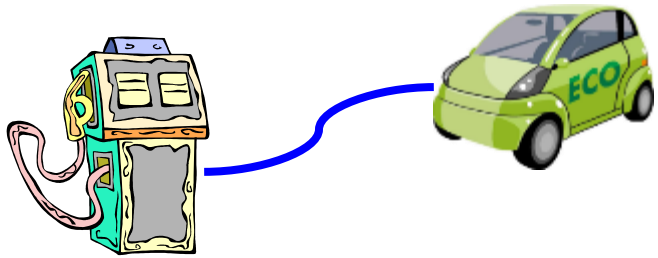
イモビライザーを攻撃
⇒鍵が無くても車を盗難可能

自動車のセキュリティ上のニーズ

自動車社会におけるセキュリティニーズ

- IEC 61851
- ISO/IEC 15118/12139
- IEC 61980
- SAE J2836/J2847/J2931

＜EV/PHV充電＞
- 家⇔自動車認証
- 充電スポット⇔自動車認証

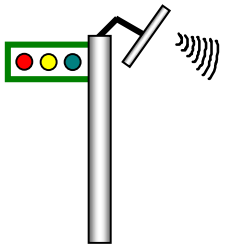


※路側機経由か、
3G等のキャリアを使うか
まだ明確になっていない

自動車メーカ・サーバ
ITSサービス

- ISO 20077/20078/20080

＜ITS/車間通信＞
- Diagnosis
- 挙動を利用したサービス
- 故障予知検出
- etc



＜路車間通信＞
- 道路/地域情報
- 課金(ETC等)
- etc

- C2CCC Protection Profile
- ETSI 103 097 etc…
- CAMP

＜内部情報＞
- 完全性/可用性/機密性
- 自社ノウハウ
- プライバシー情報
- etc

- EVITA
- SHE

＜車車間通信＞
- 衝突防止
- 交通渋滞緩和
- 自動走行
- etc

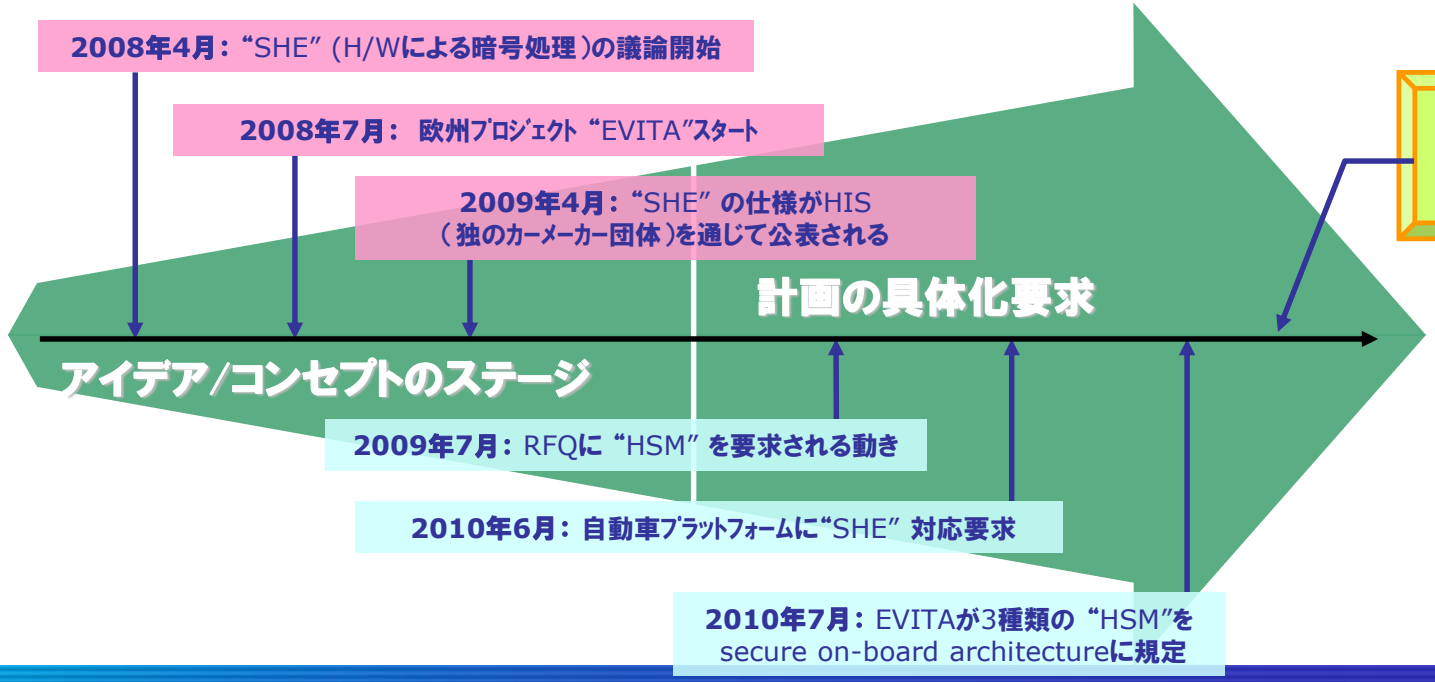
- C2CCC Protection Profile
- ETSI 103 097 etc…
- CAMP

欧州自動車市場でのセキュリティに関する標準化動向

欧州を中心とした、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

OEM: ⇒多タイプに及ぶ、SHE互換MCUの要求（Gateway、イモビなど）
⇒Mid/High-endの暗号エンジン搭載MCUの要求

Tier1: ⇒自動車プラットフォーム向けHSM（Hardware Security Module）の要求
⇒EVITA互換のRSA内蔵次世代HSMの要求



2011年12月に耐タンパを含めた議論（PRESERVE）が欧州でスタート

世界規模で広範囲の車載用途に対して、セキュリティ機能搭載が展開されていく方向

要求されるセキュリティ機能

- Authentication
  - End to End**の機器認証**
  - **自動車システム内部の機器認証**
- **通信経路の暗号化**
- **耐タンパ性**
  - Secure storage
    - **内蔵**Flash**メモリ**
    - **外部接続**Flash**メモリ**
  - Secure Boot
  - Side channel attack**耐性**
  - **外部モニター機能（温度/電圧等のモニター）**

暗号とは

- ここで知っておいて欲しいコト
  - 暗号って何？
  - 何を守るの？
  - 暗号方式の種類と特徴
  - 一方向性関数（HASH）って何？
  - HASHって何に使うの？
  - 乱数って何に使うの？
  - MACの重要性

暗号理論における暗号方式と鍵の関係

プログラム（平文）

暗号方式

る	ね	さ	す

これが“鍵”！！

50音表で○文字分だけ後ろにずらす。
ただし、行をはみ出たら同じ行の“あ”段に戻る。

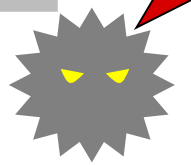
復号方式

ろ	な	す	そ

50音表で○文字分だけ前にずらす。
ただし、行をはみ出たら同じ行の“お”段に戻る。

2文字ずらす

何文字ずらす？



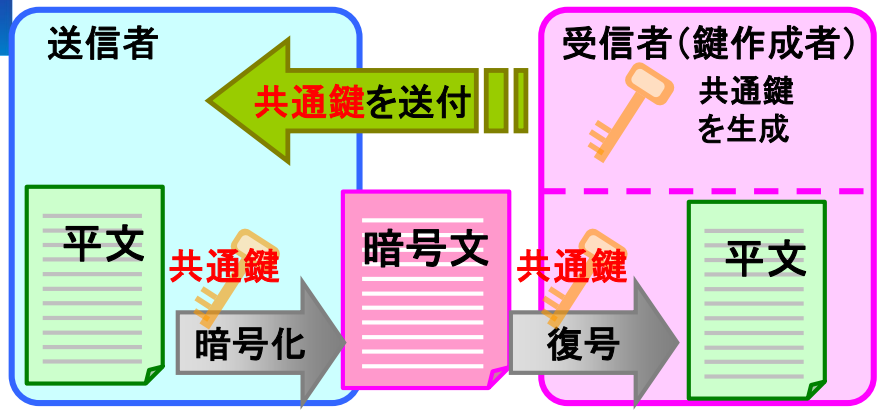
る	ね	さ	す

暗号方式と鍵の両方を使って、
元の文章に戻す

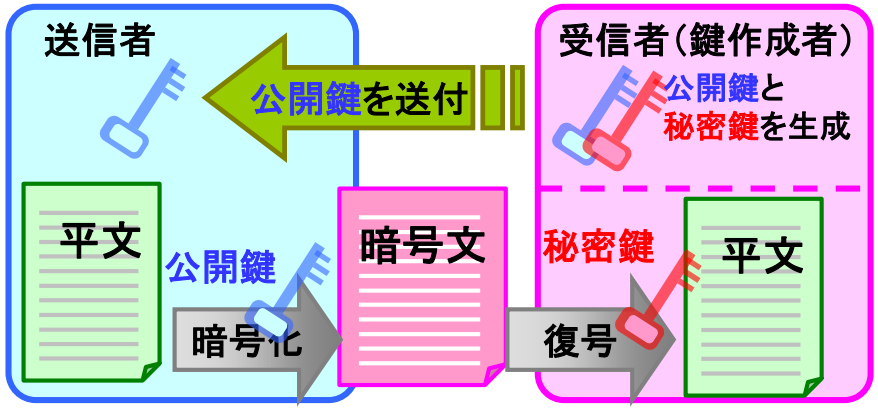
？	？	？	？

暗号方式だけで鍵が解らないと、
元の文章には戻せない

現代暗号方式の概要 （教科書ベース）



共通鍵暗号方式



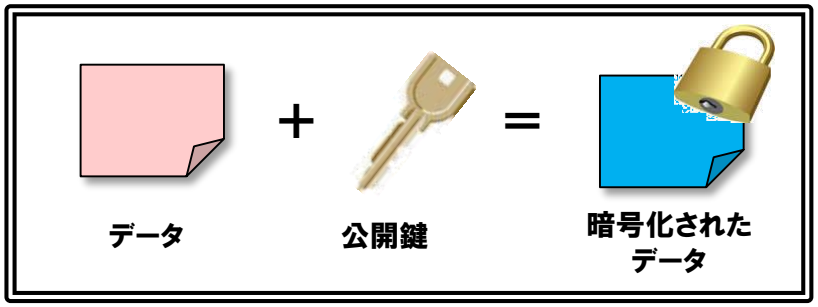
公開鍵暗号方式

	共通鍵暗号方式	公開鍵暗号方式
特徴	暗号/復号時、同じ鍵を使う	暗号/復号時、それぞれ別の鍵を使う
鍵の管理	共通鍵の管理が必要	秘密鍵のみ管理が必要 *公開鍵の管理は不要*
鍵の送付	共通鍵の送付	公開鍵のみ送付
鍵の送付時の危険性	共通鍵を送付する必要がある為、 盗聴に注意が必要	公開鍵を送付するだけなので、 改竄のみ注意が必要
処理時間	短い	長い（共通鍵暗号方式の数百～数千倍）
認証	認証には適していない	第三者に証明できる
暗号方式例	DES，AES	RSA，ECC

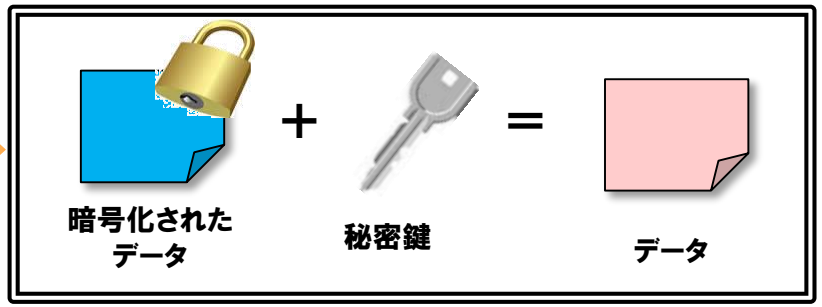
公開鍵暗号方式を少し深く見てみる

データを安全に送付する

送信者

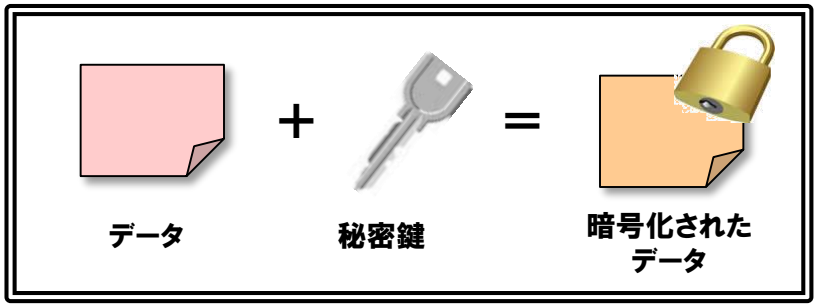


受信者
（鍵のオーナー）

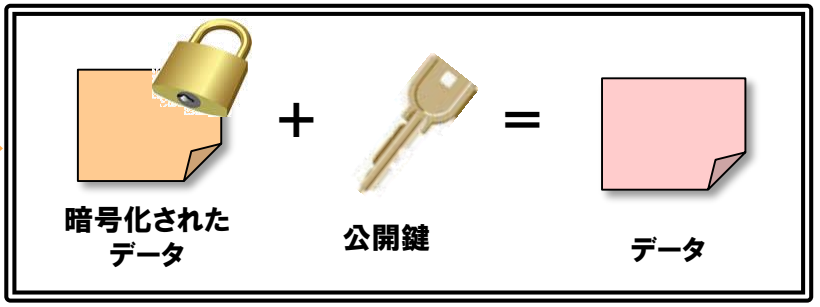


自分が送った事を証明する

送信者
（鍵のオーナー）

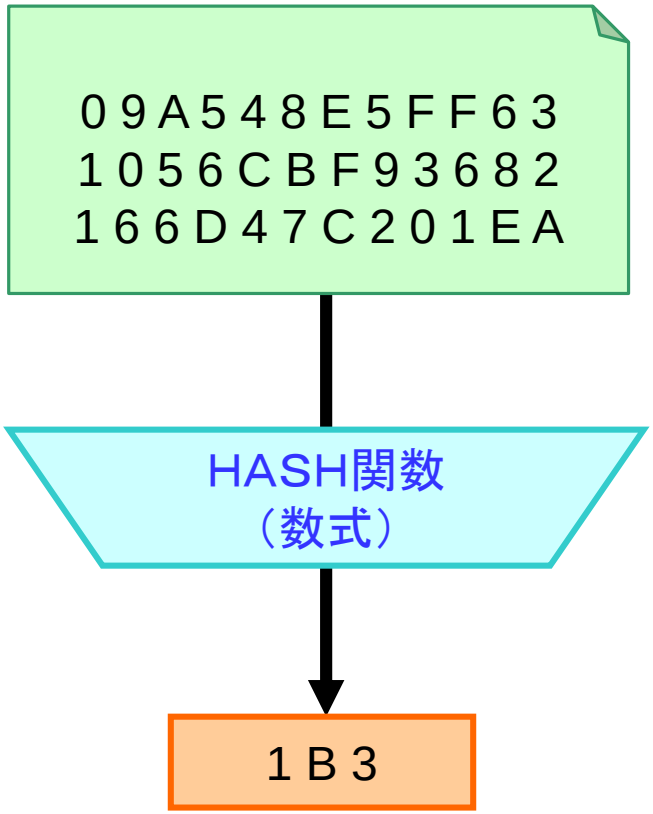


受信者



HASH関数とは

任意長の入力値を固定長に「不可逆圧縮」する関数



NIST(米)では、SHA1 / SHA2に対して
暗号移行ガイドが提示されている。
SHA1：署名生成は2013年以降、Disallowed
SHA2：2015年以降もAcceptable

HASH関数への要求事項

- Collision Resistance
  H(x)=H(x')となるx,x'を見つけるのが困難
- 2nd Preimage resistance
  xがある時、H(x)=H(x')となるx'を
  見つけるのが困難
- Preimage resistance
  y=H(x)となるようなxを見つけるのが困難

一方向性とランダム性を保証

・SHA1が現在のデファクトスタンダード。（ランダム性も保証されている）
・SHA1 / SHA2共に、現段階で問題は発見されていない。

乱数

- 全く無秩序に、しかも出現の確率が同じになるように並べられた数字の列。

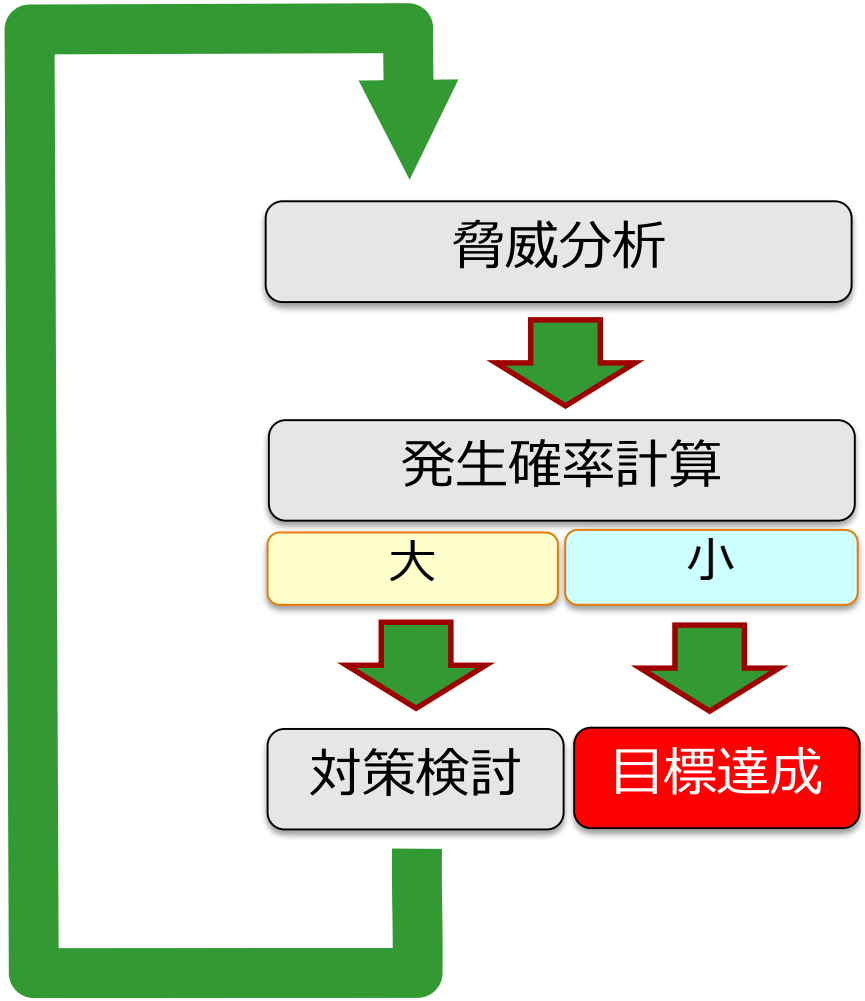
◆コピー(リプレイ)対策として用いる
- １回限りのチャレンジ＆レスポンス用データ
- １ Timeの暗号鍵 （使い捨ての鍵）
- その他

Media Authentication Code（MAC）

- メッセージを認証するための短い情報

車載セキュリティの課題

脅威分析の基本的な流れ

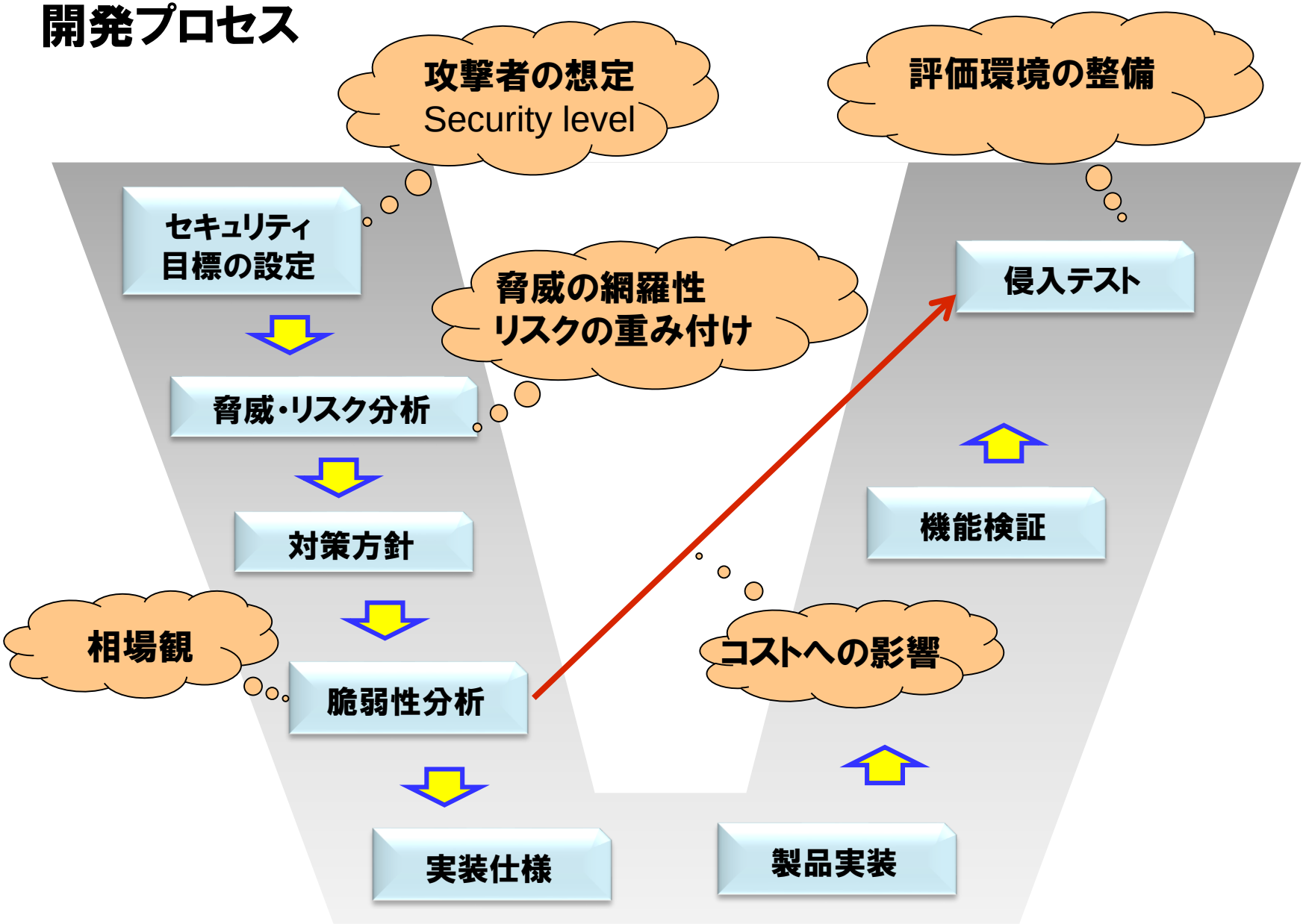


資産を整理し、脅威のシナリオをできるだけ多く所有する
(業界で共有するなど)

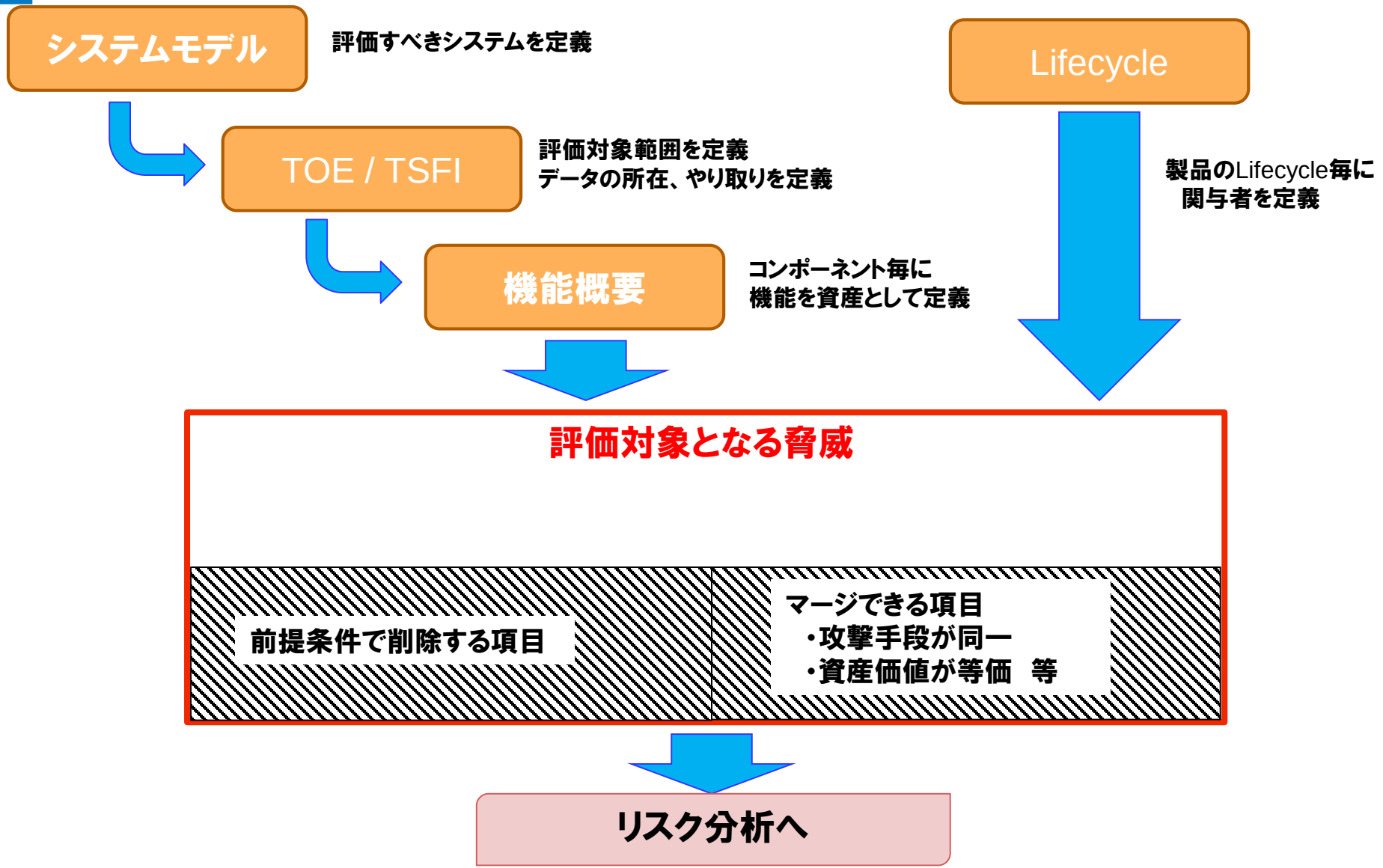
想定したシナリオの発生確率を計算する (専門家のコンサルも有効)
＊ リスクが小さい場合は対策不要
＊ リスクが大きい場合は対策を検討

脅威に対して対策を検討する
対策を講じたシステムでもう一度分析する

開発プロセス

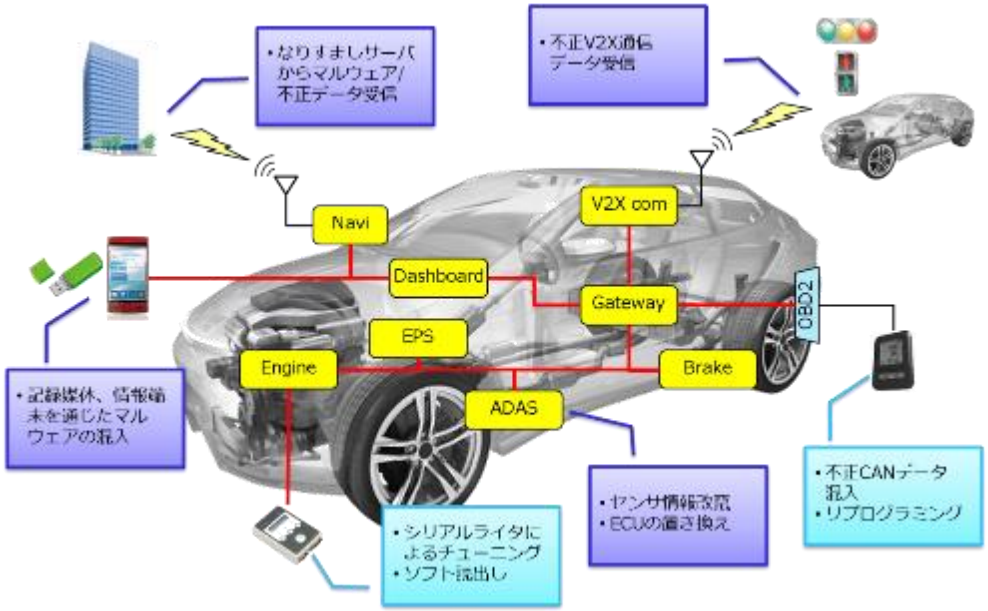


脅威分析



脅威の網羅性

これだけ考えれば十分なのか？



インシデント例が少ない
業界共通の自動車の被害データベースが必要

攻撃者の想定

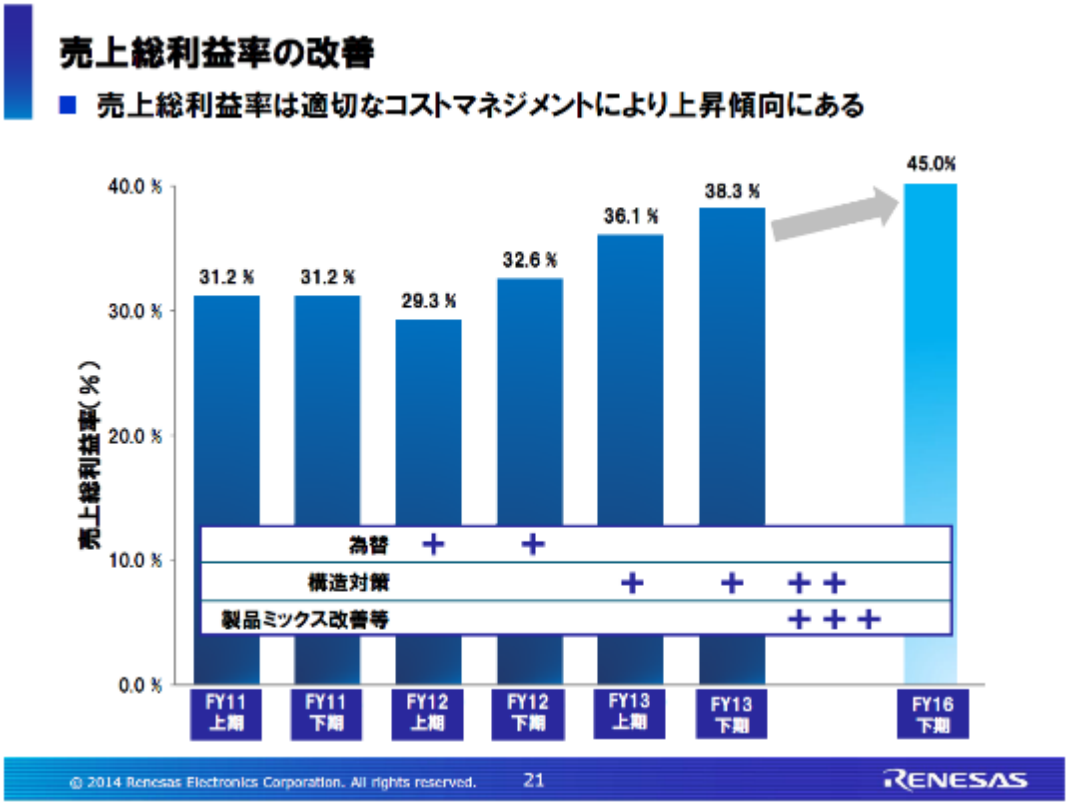
まさか、あの人が・・・

どのLifecycleで、誰が、どこに攻撃するのかを想定する

車検、レンタカー、カーシェア、友人への貸し出し、中古車・・・
様々なケースが存在する

セキュリティ目標の設定：セキュリティレベル

ルネサスエレクトロニクス（株）
第1四半期決算説明会（2014年8月6日）
さらなる利益成長に向けた取り組み



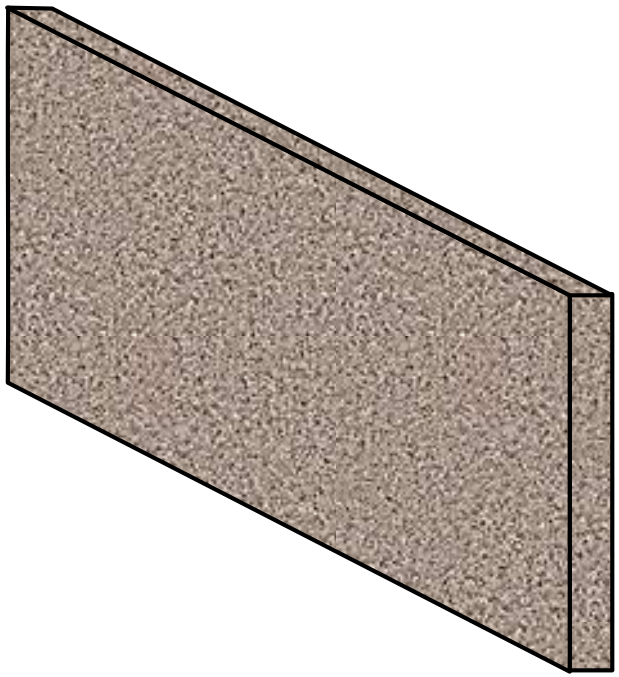
理想だけでは現実はついてこない

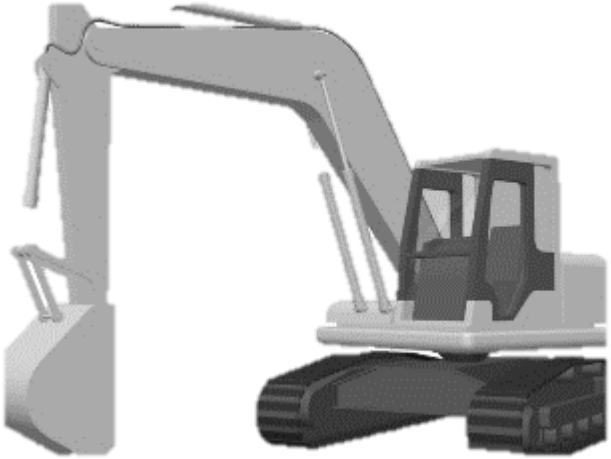
妥当な攻撃シナリオとは？

× セキュリティを突破する攻撃コストが高い

× 資産に対して対策コストが高い

× そもそも資産価値がそれほど高くない





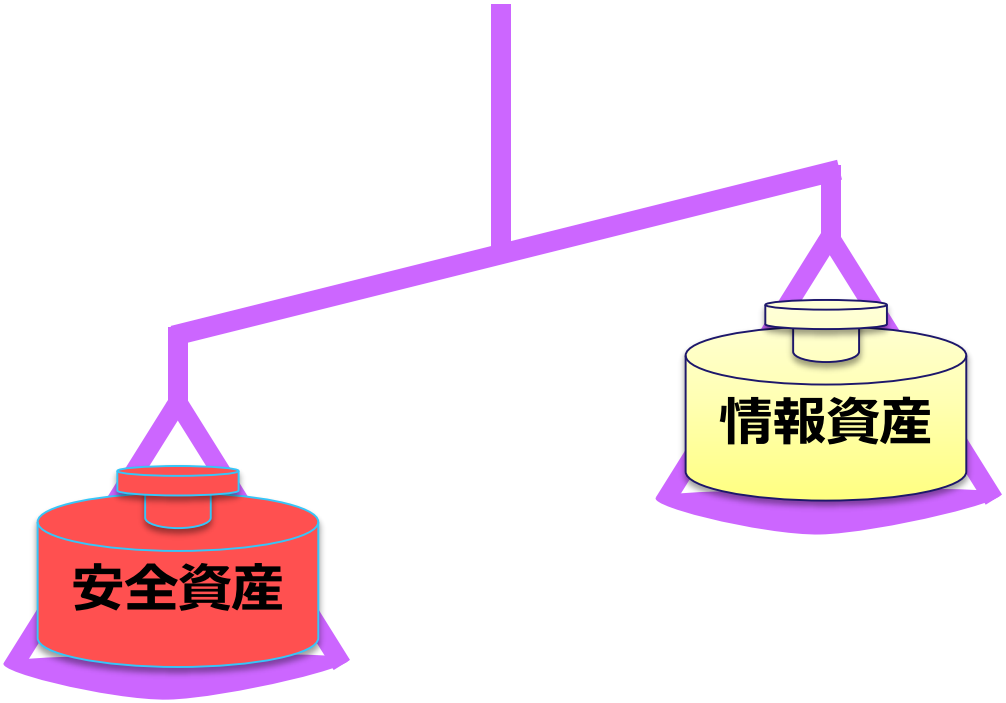
資産　対策　攻撃

リスクの重み付け

安全に、
- 走る
- 曲がる
- 止まる

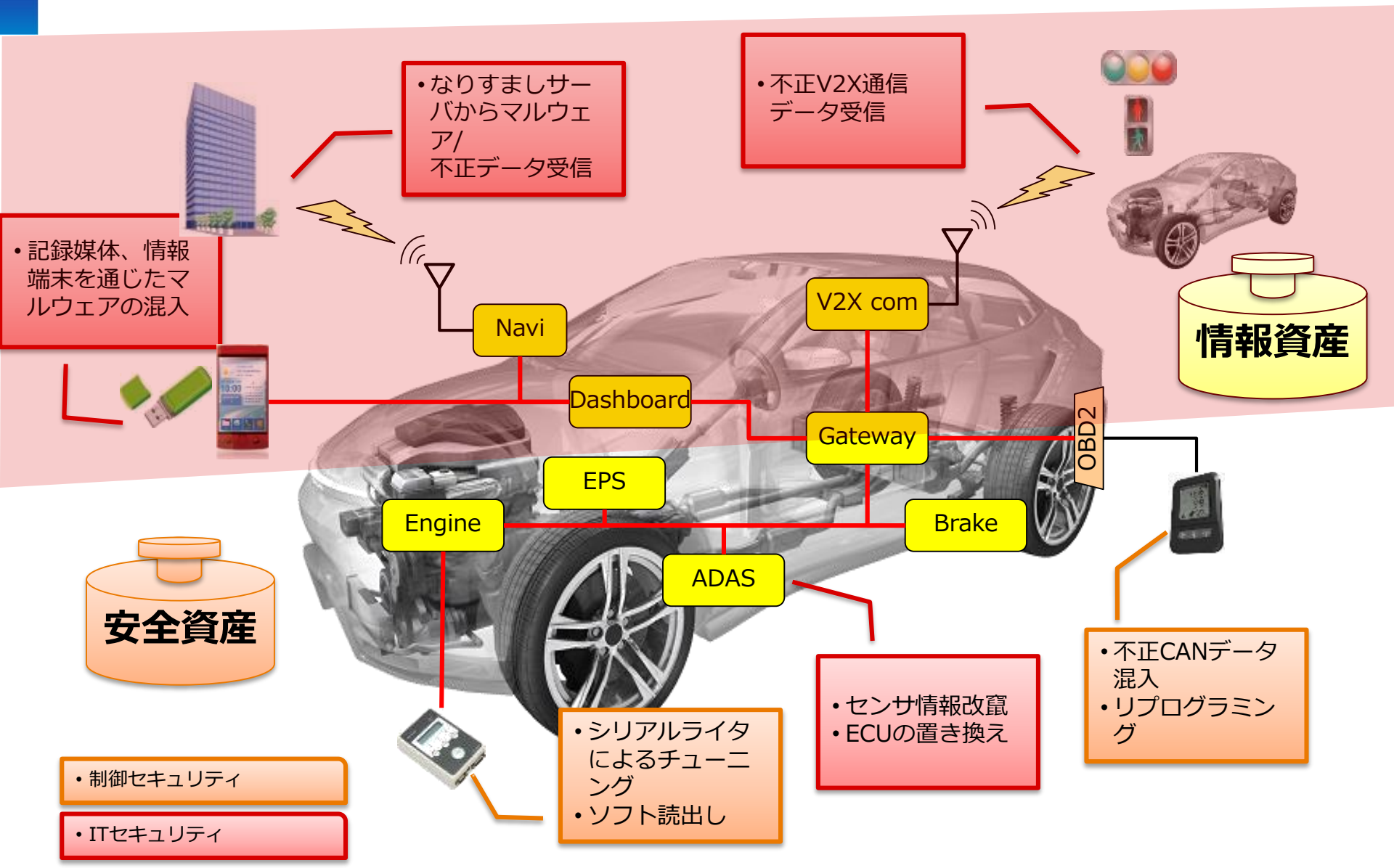
- 金銭情報
- 個人情報
- 著作権
- ・・・

直感的には・・・



安全資産と情報資産を分けて考える必要がある

GWがある場合制御系の脅威は絞られる



対策方針を考える

どのレベルで考えるのが合理的か

システムで考える
　　ECUへのアクセスのしやすさ

環境的セキュリティ

車内ネットワークで考える
　　LSIへのアクセスのしやすさ
　　DoS攻撃対策

ネットワーク
セキュリティ
★　脅威の中心

LSIレベルで考える
　　セキュアストレージへのアクセス制御
　　暗号機へのアクセス制御

LSIセキュリティ

資産

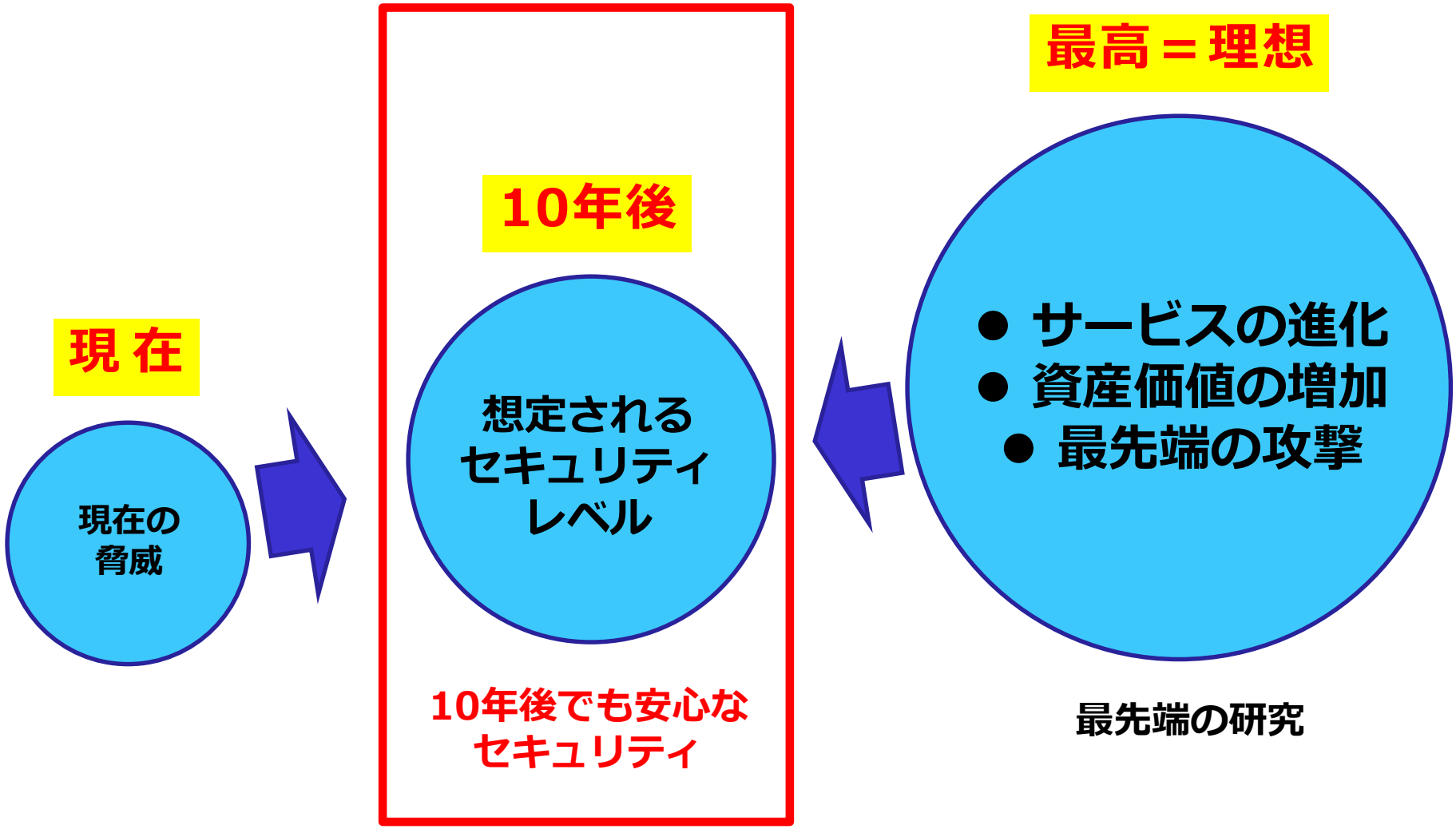
お金 → **金庫に入れる** → **家への侵入を防ぐ** → **地域の防犯**

脆弱性分析・侵入テスト

ボトムアップでの脅威の想定は実際のシステムの脅威に対して過剰に想定せざるを得ない

頑張り過ぎると、そのままコストに跳ね返ってくる

先を見据えた対応



車載セキュリティの課題のまとめ

- 全体開発フロー
  - 機能安全とセキュリティの融合
  - 認証の扱い
- 脅威分析
  - TOEの範囲
  - 脅威の網羅性（データベース化）
  - ライフサイクル（自動車独自のライフサイクルを考慮する）
- リスク分析
  - 保護資産の重み付け
  - 人に依存しないシステム化
- 対策方針
  - 機能安全を考慮した対策方針（エラーハンドリング）
  - 車のライフサイクルを考えたセキュリティ実装
- 脆弱性分析・侵入テスト
  - 開発期間/コストを考慮した最適な分析、テスト

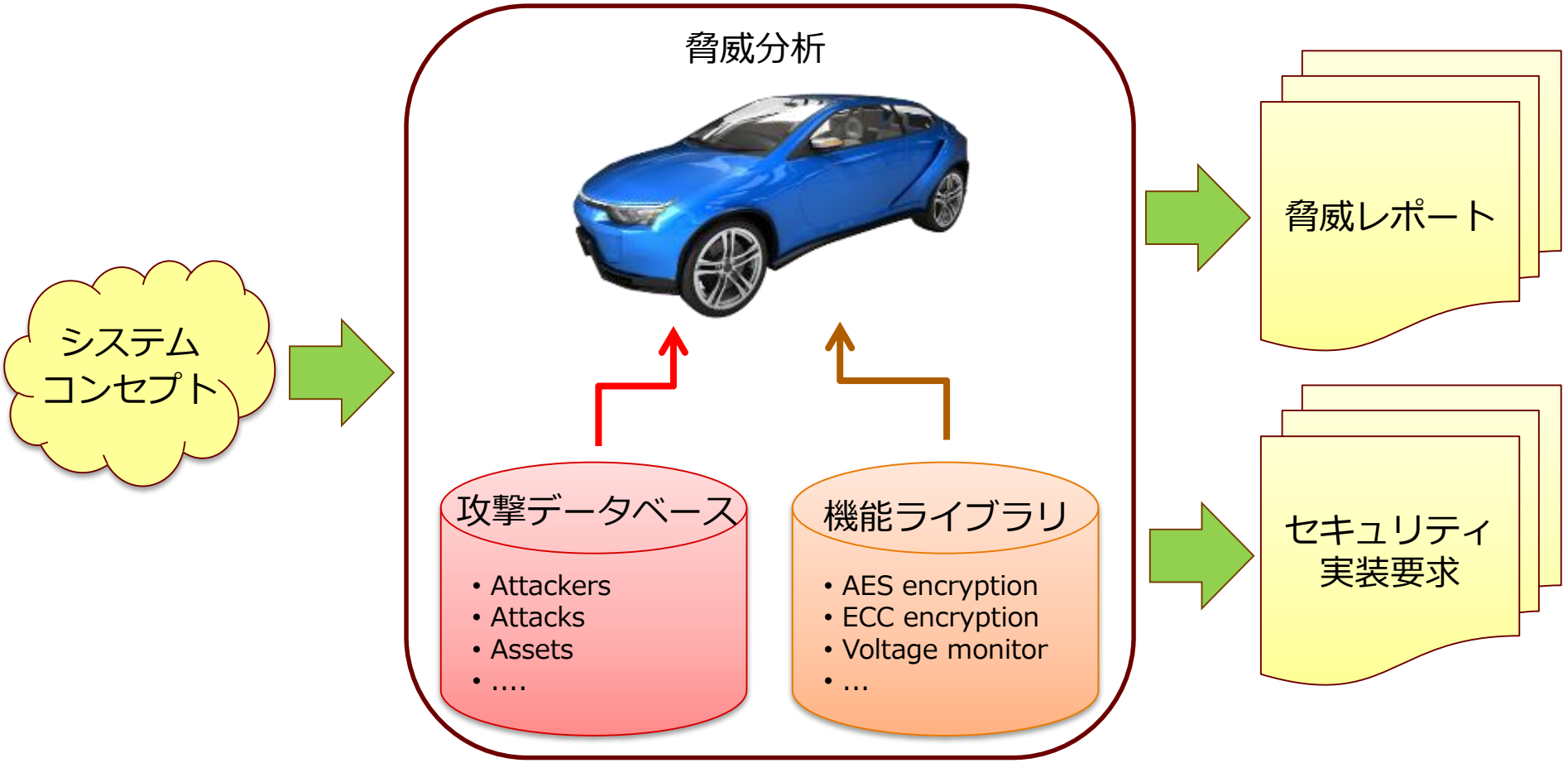
ここで、ちょっと演習

お題

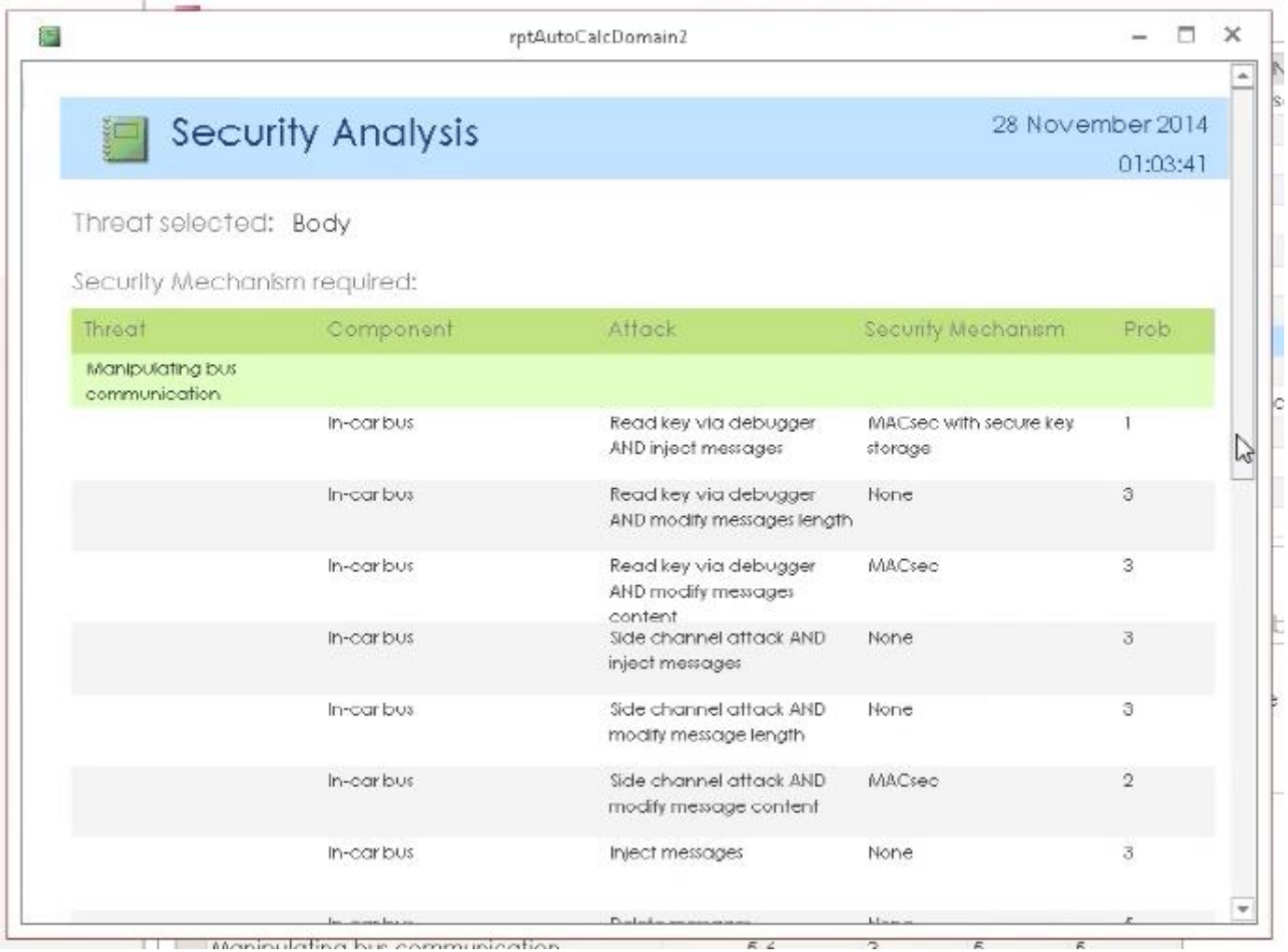
当日発表

やる事が多くて圧倒されてしまう

脅威分析をツールでサポート！



ツールイメージ



当社のセキュアマイコンとソリューション

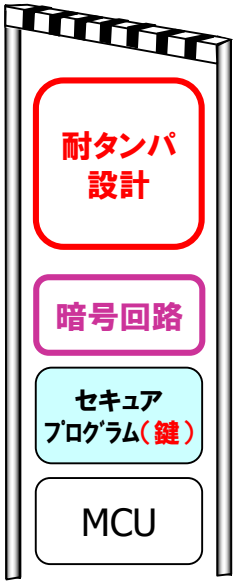
ルネサスのセキュリティ技術

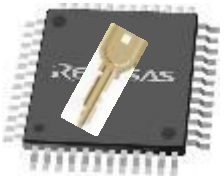
物理アタック

耐タンパ設計で更にセキュリティ向上

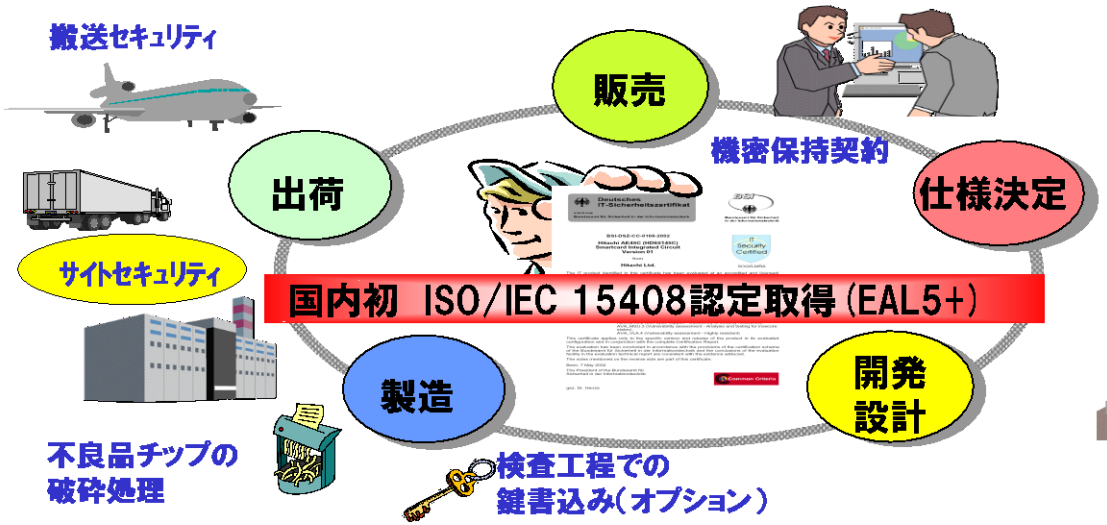
なりすまし
盗聴

暗号回路とセキュアプログラムで
セキュリティ向上



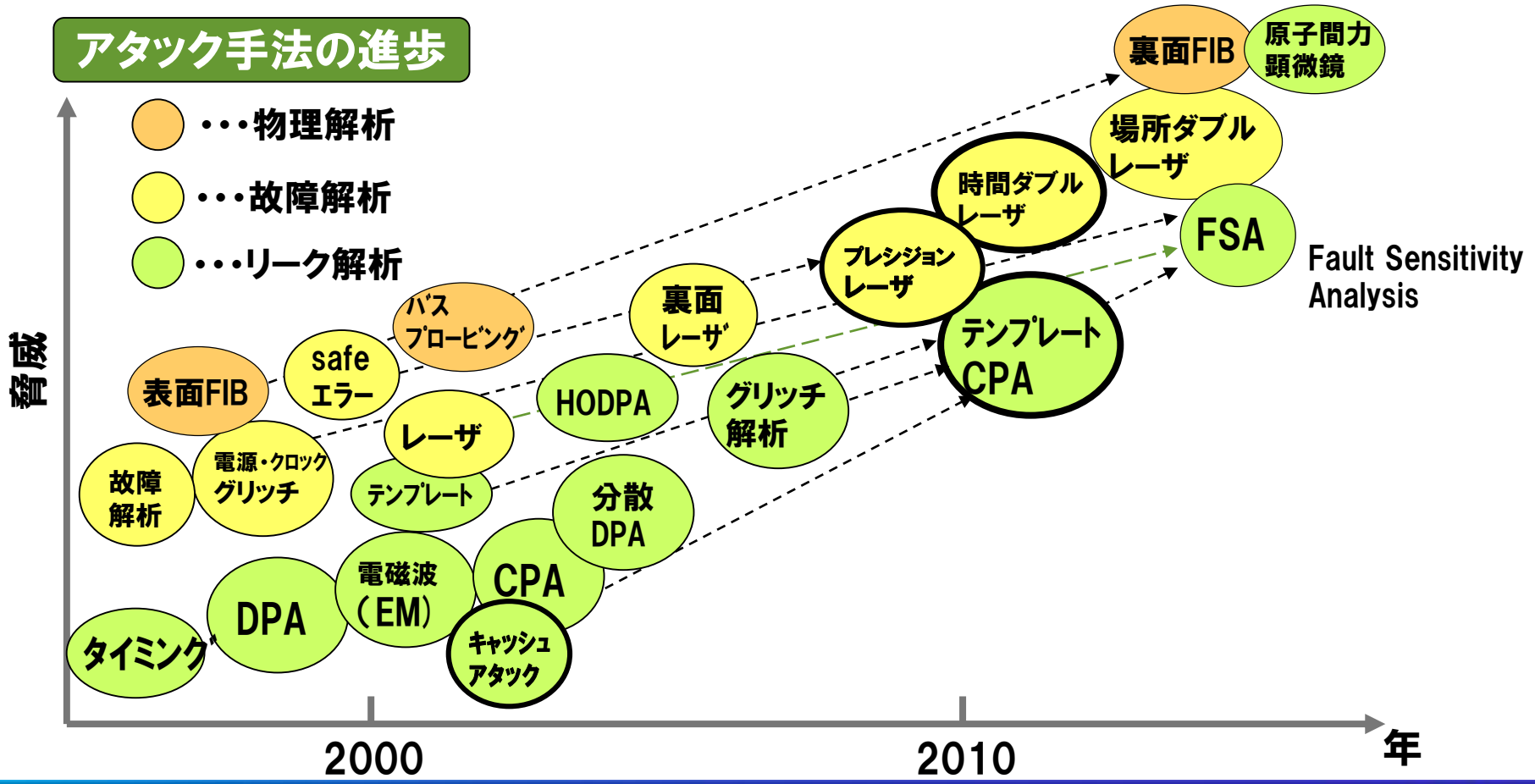


― 製品のライフサイクル全ててセキュリティを保証します ―



High Security Spec：アタック手法の進化に対応

- 既存アタックの組み合わせ、測定装置の性能向上によるアタックの高度化
- 新規モジュールの導入による、攻撃対象の増加
- アタックの進歩に遅れをとらない、ソフト・ハード対策技術の開発



セキュアMCUのイメージ

四つの壁で秘密データを守ります。

フィジカルセキュリティ

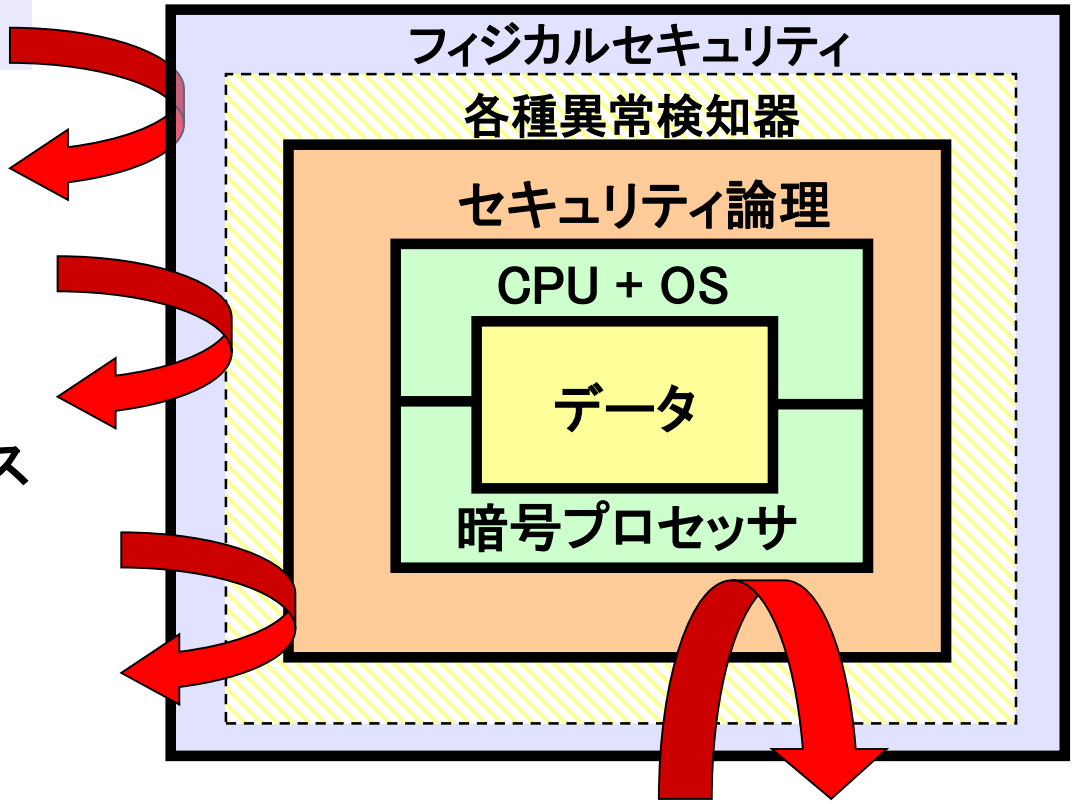
- メタルシールド
- ランダムレイアウト　…

各種異常検知器

- 電圧、周波数、など
- 未定義命令、未定義アドレス

セキュリティ論理

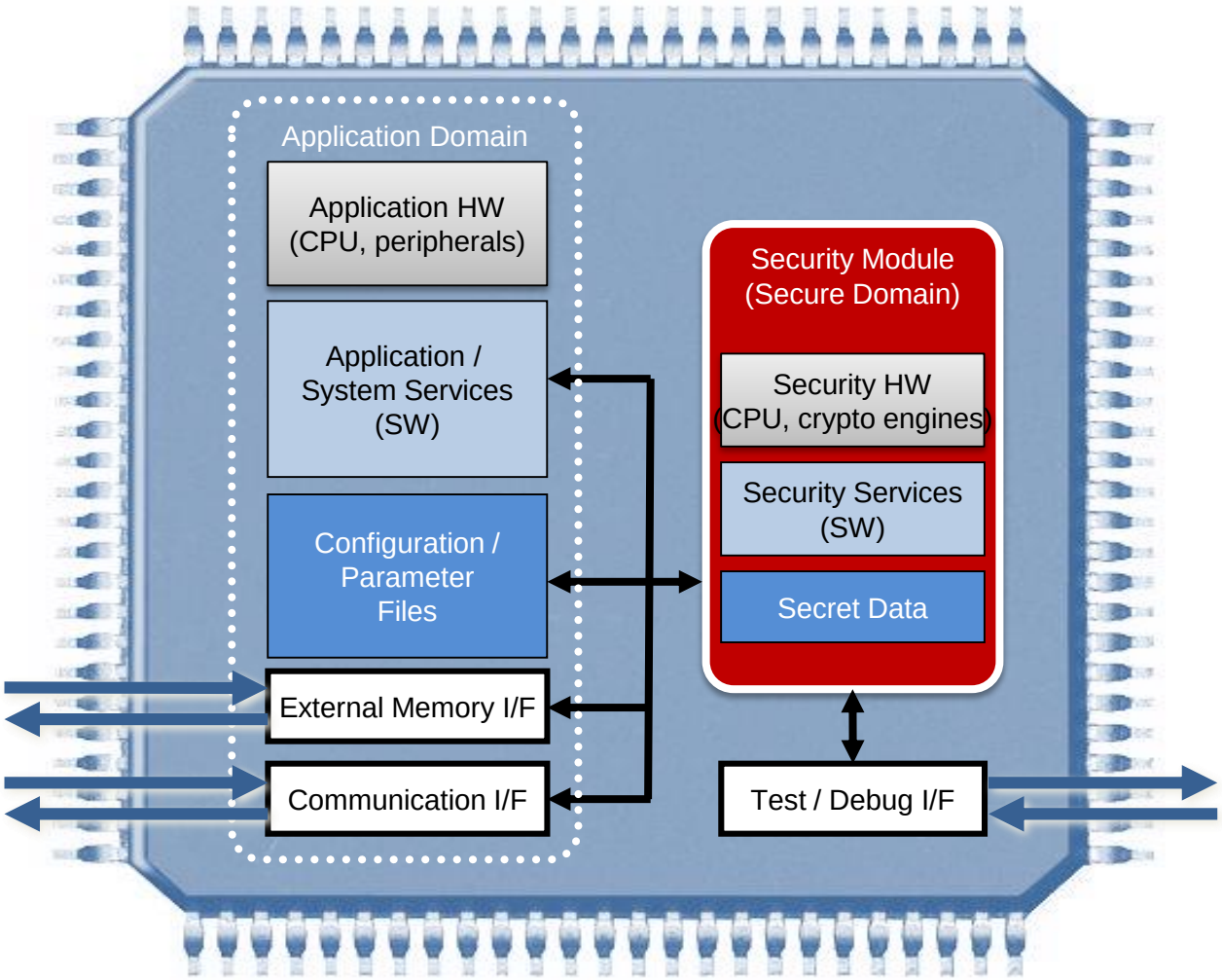
- ウオッチ・ドッグ・タイマ
- 乱数発生回路
- FMU（メモリマネージメント）
- 電流制御回路



暗号プロセッサ

- DES/AESコプロセッサ
- RSA/ECCコプロセッサ

セキュアIP搭載マイコンのイメージ図



Security Module (Secure Domain)

Isolation of secret data

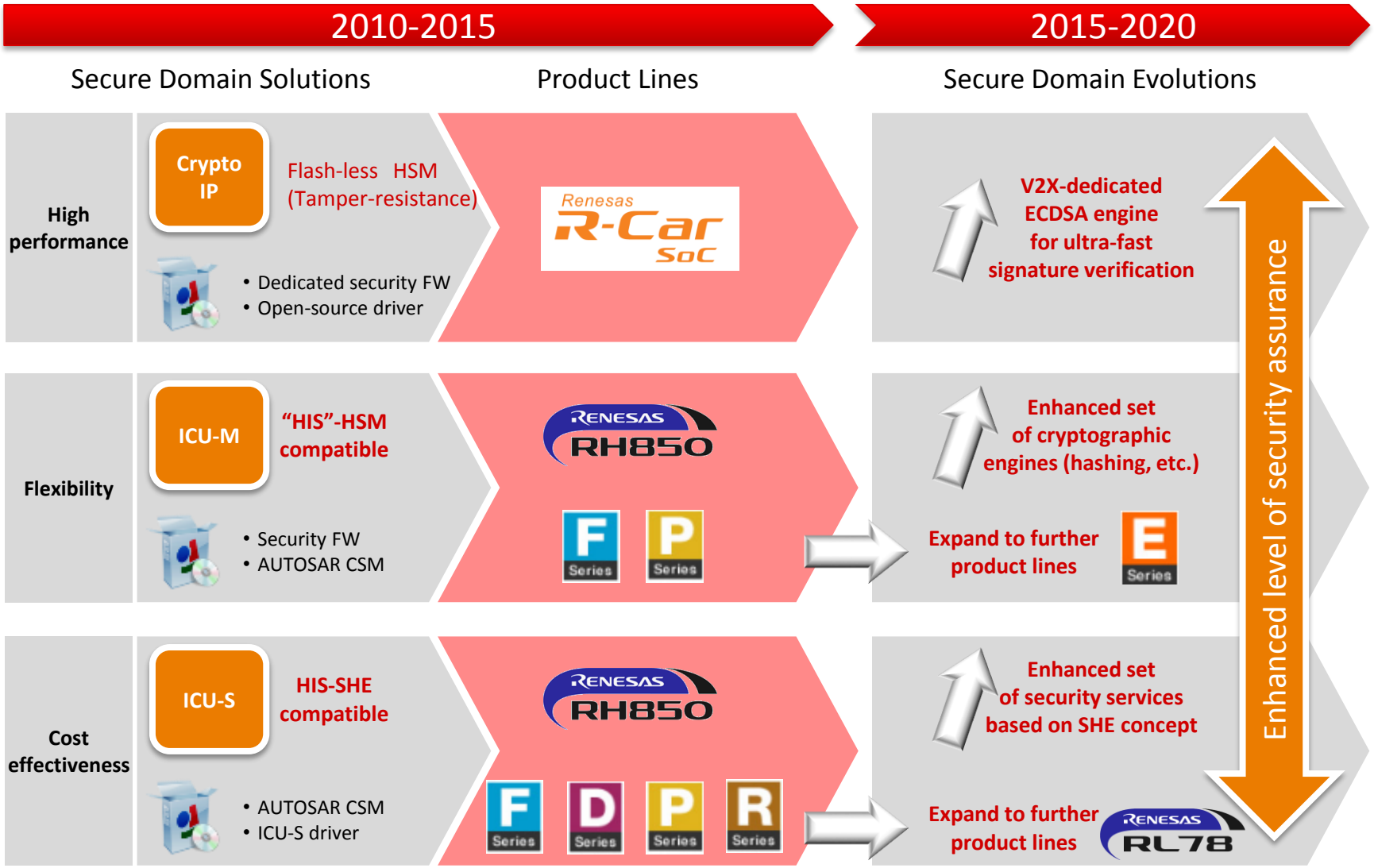
Dedicated HW for efficient cryptography

Parallel processing

Fixed（SHE type）or customized（Evita HSM type）security services

Renesas Secure Domain Solutions

Development strategy proposal



これからの車載セキュリティを一緒に考えましょう

ご清聴　ありがとうございました

Renesas Electronics Corporation