第８回 成長戦略ワーキング・グループにおけるヒアリング

車両サイバーセキュリティ対応

Japan Automotive Software Platform and Architecture

目次

一般社団法人JASPAR
情報セキュリティ推進WG

TOYOTA	飯山(主査)・河井・平林
HONDA	根本(副主査)
NISSAN	宮下(副主査)
MAZDA	柏島
SUBARU	関口
DENSO	林

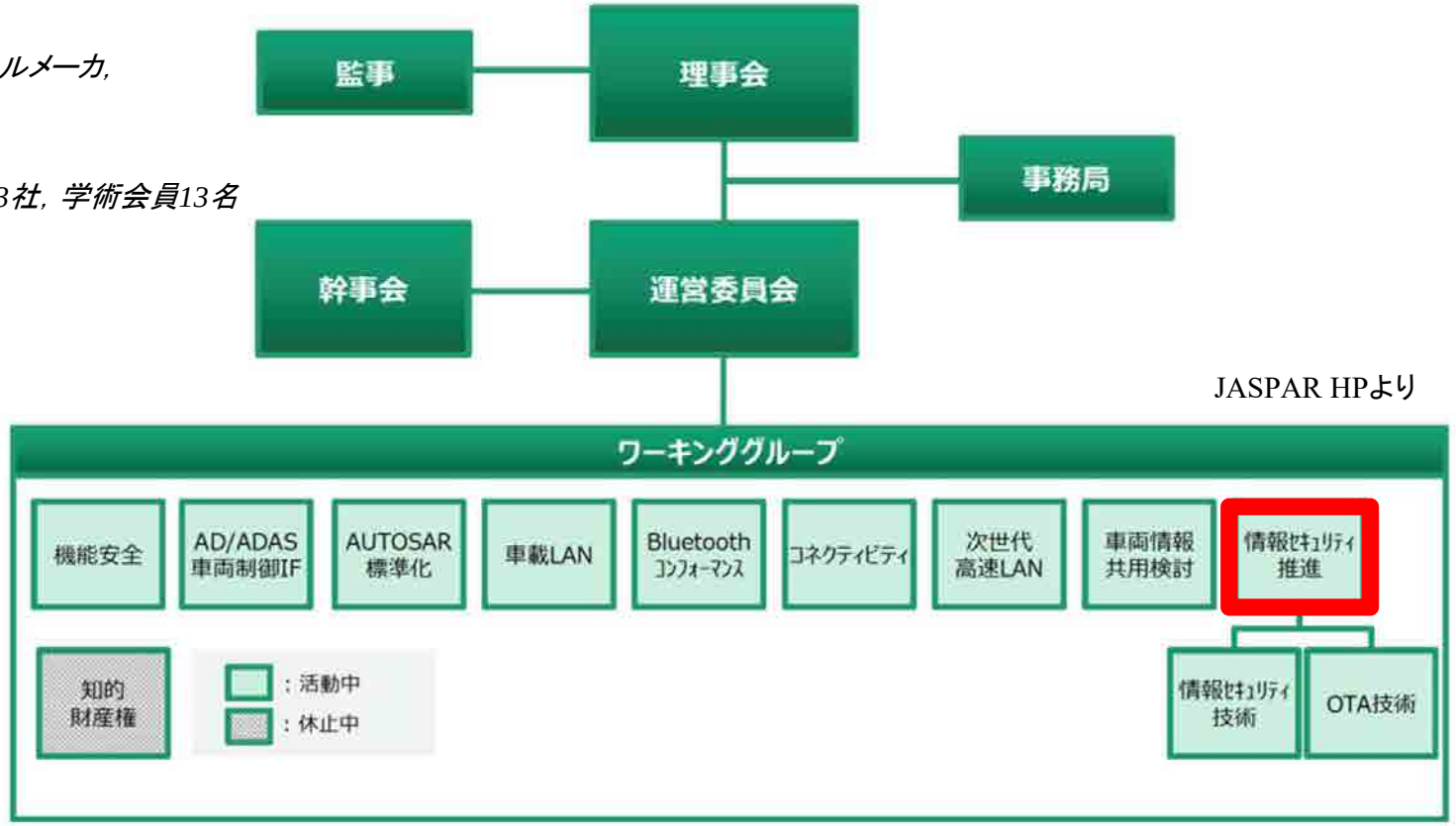
※本資料はJASPAR標準化になっていない一般的な技術紹介と
JASPAR標準技術の一部を組合わせた内容で構成しています

2021.4.8

JASPAR紹介

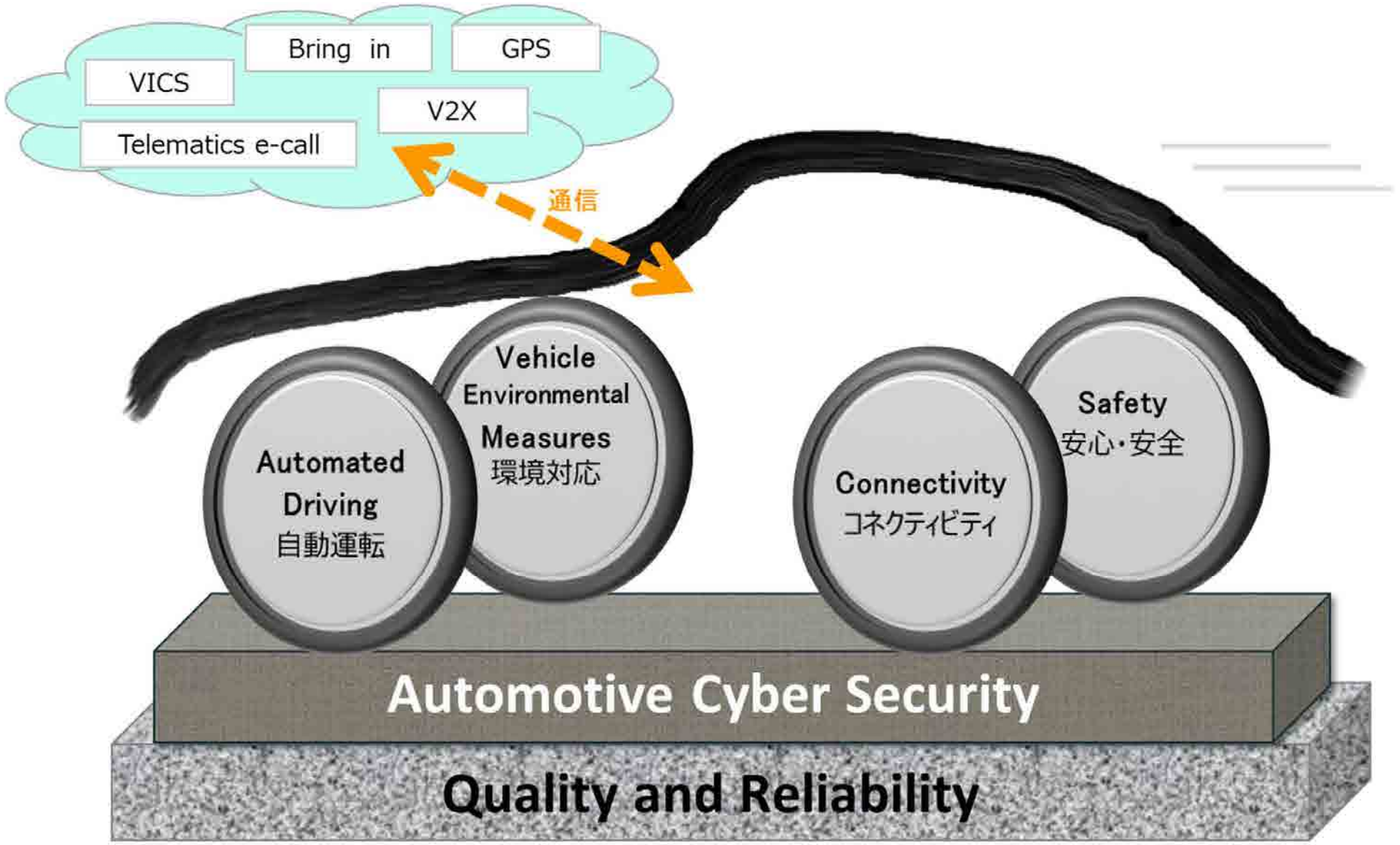
一般社団法人JASPAR(Japan Automotive Software Platform and Architecture)

- 2004年9月設立
- 目的
  - ***ソフトウエア標準化***，*共通利用による*
    - *車載電子制御システムの開発効率化*
    - *高信頼性確保*
    - *インタフェースのインターオペラビリティの確保*
- 参加メンバー
  - *自動車メーカ*
  - *電装品メーカ*
  - *半導体・電子部品，ソフトメーカ，ツールメーカ，*
  - *商社，キャリア*
  - *大学・研究機関など*
  - *幹事会社5社，正会員91社，準会員93社，学術会員13名*



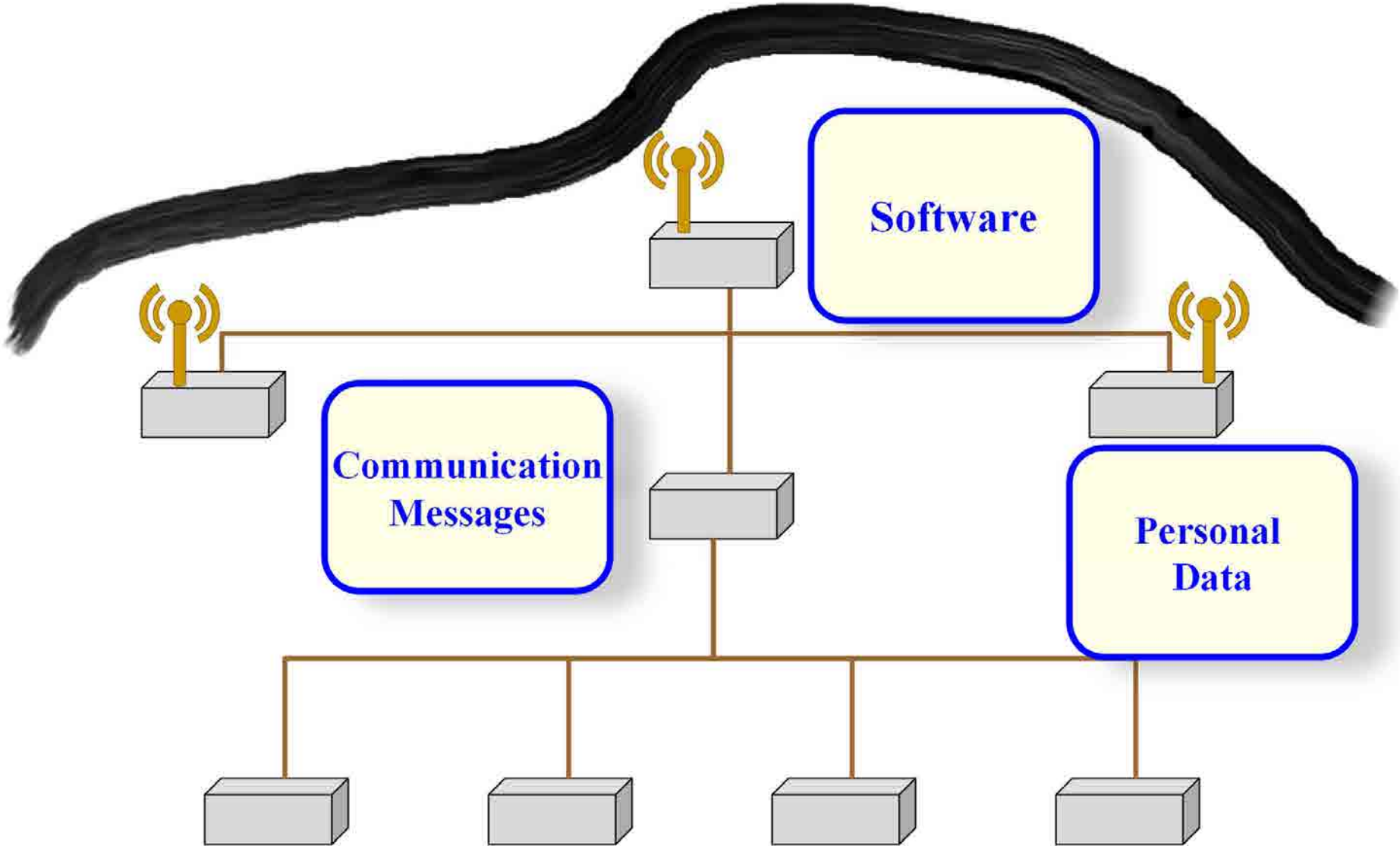
JASPAR HPより

車両を取り巻く環境



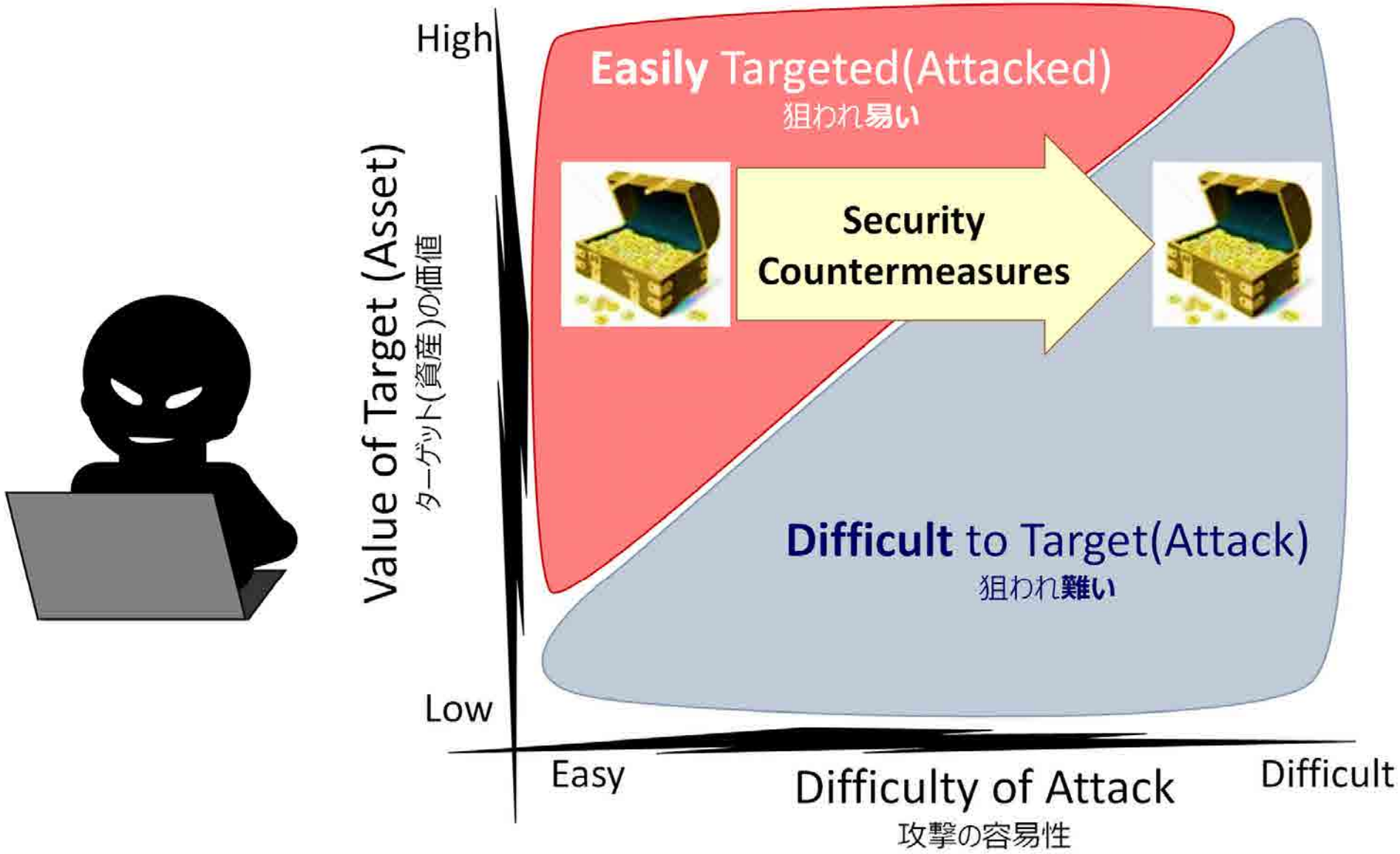
品質・信頼性同様、車両サイバーセキュリティ対応は必須

車両内の資産



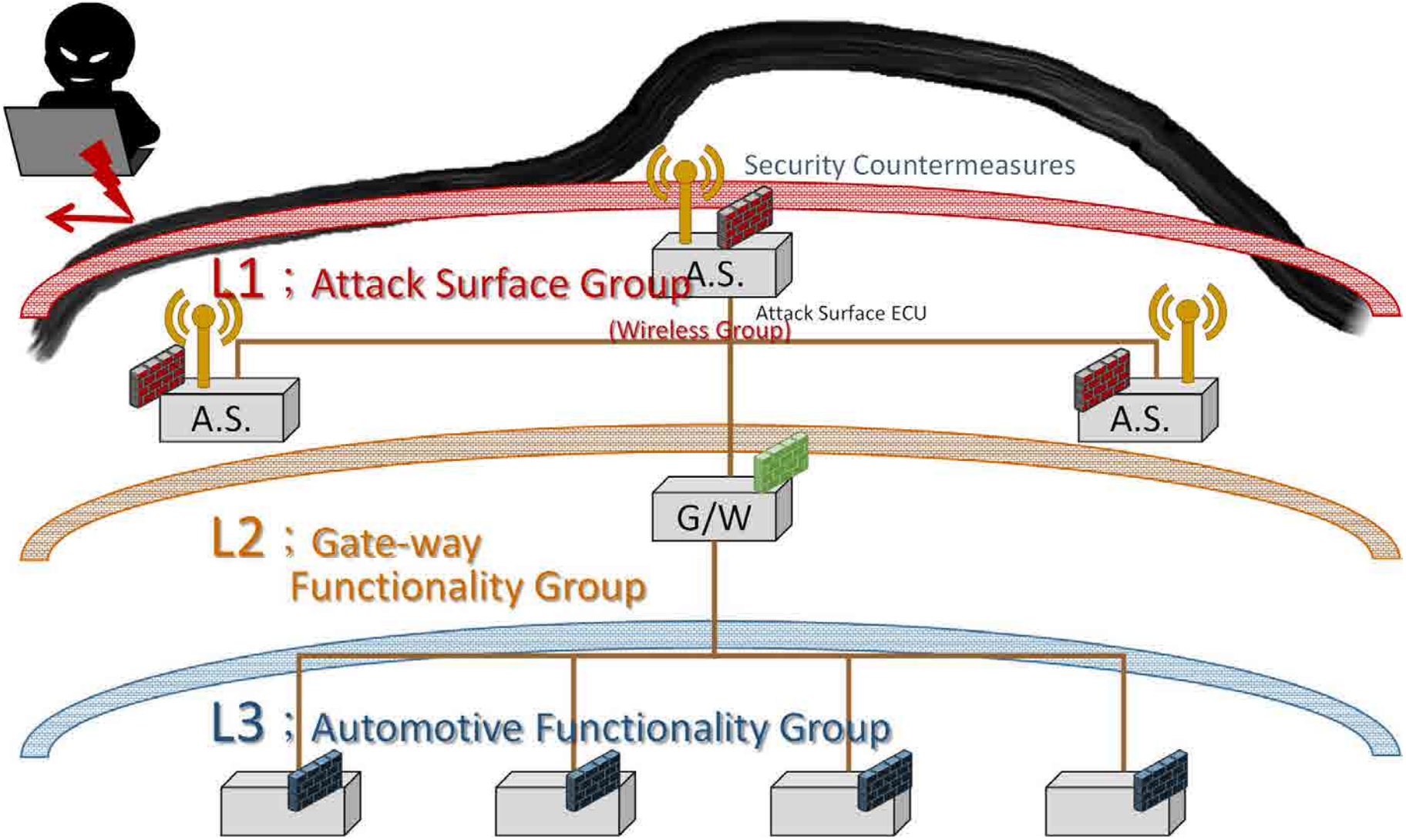
ソフトウェア、通信メッセージ、パーソナル情報を車両内資産に設定

セキュリティ対策の役割



セキュリティ対策でターゲット(資産)を狙われ難い領域に設置させる

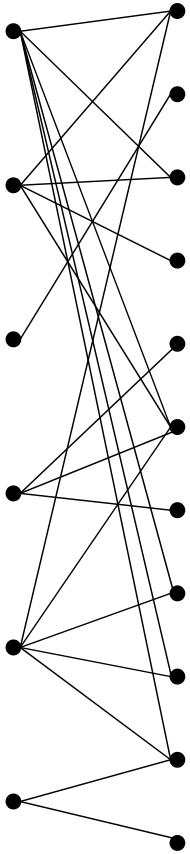
車両防御



制御ユニットを機能群別に階層配置し、複数壁を設ける多層防御アーキテクチャの適用が拡大

一般的な車両搭載コネクテッドサービスの紹介

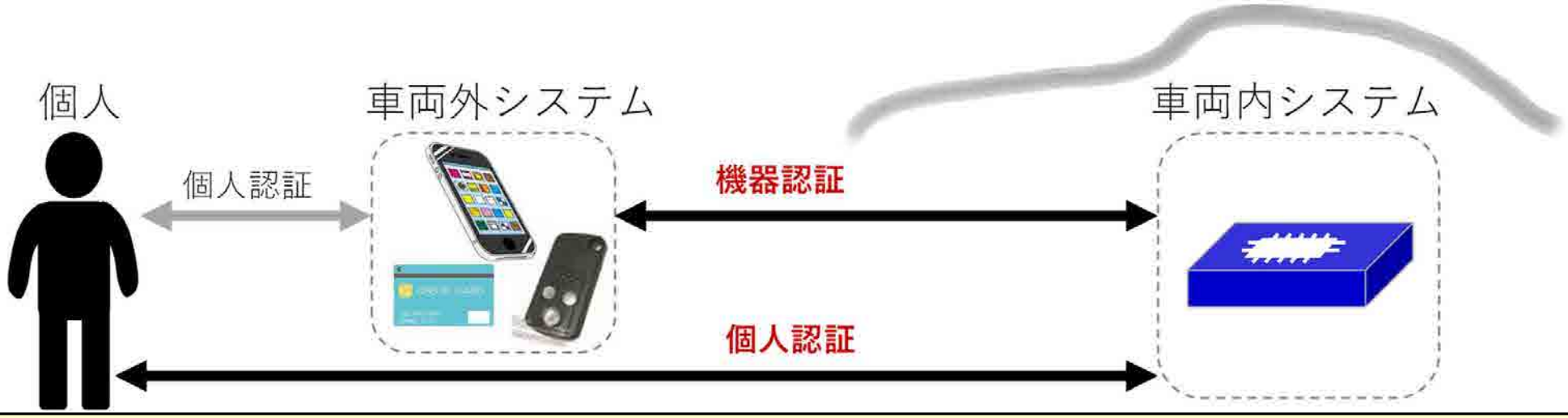
■コネクテッド技術
車両内搭載ユニットと車両外(非搭載)製品が無線で接続し通信する技術



無線通信
Wi-Fi
Bluetooth
Qi
RF (Radio Frequency)
Cellular
DSRC (Dedicated Short range Communication)

コネクテッド技術を使ったサービス代表例
アプリダウンロード/アプリ通信サービス(天気予報・音楽など) Wi-Fi テザリングサービス
無線充電サービス
カーファインダーサービス
デジタルキーサービス
キーレス(ドアロック/アンロック)
車両外からの操作機能(AC操作、エンジンスタータなど)
車両内情報表示(タイヤ空気圧など)
OTAによるソフトアップデートサービス
車両外から車両制御情報入手(高精度地図データ、規制情報など)
V2X(車々間通信、スマートグリッド(電力網)など)
ETCサービス

一般的な車両搭載コネクテッドの認証紹介



機器認証と個人認証に分類される

- 車載認証技術
  - 機器認証
    - 独自認証方式
    - 標準認証方式
  - 個人認証
    - 所有者を判断する知識&所有認証
    - 個人を特定する生体認証

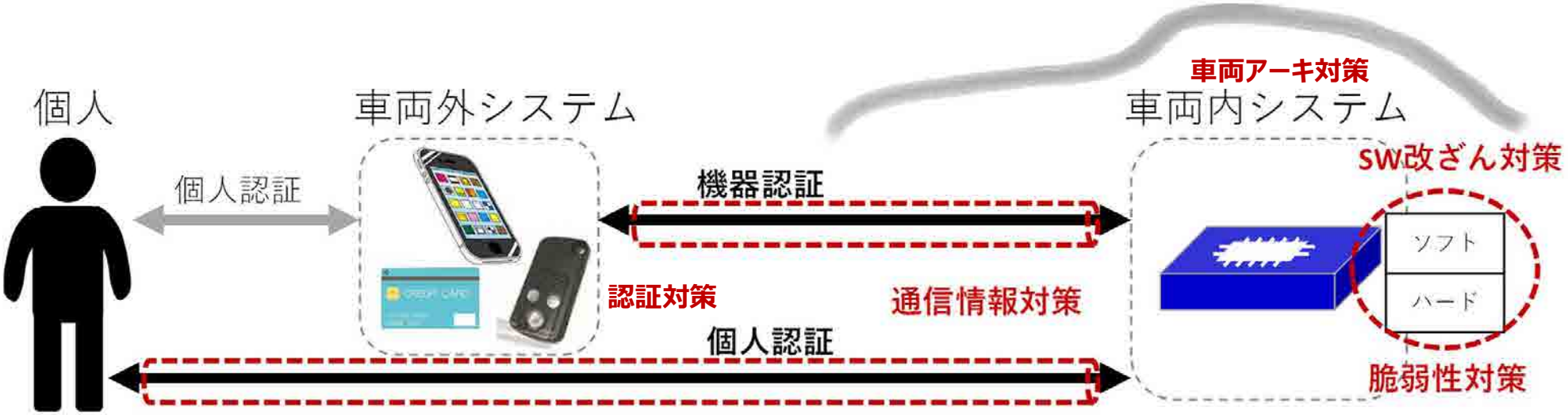
車両搭載コネクティドの認証は
自動車向けの固有技術
ではなくIT領域技術の応用

資産リスク、想定脅威に応じ適切な認証手法を選定する

個人認証の具体例

分類		概要	例	攻撃
知識		本人のみが記憶しているデータに基づいて利用者を認証する方法	パスワード、PIN、秘密の質問	なりすまし(複製含)
所有		本人のみが所持している物によって利用者を認証する方法	USBメモリ、ICカード、携帯電話	改ざん
生体	身体	本人の生体に基づくデータにより利用者を認証する方法	爪、顔	否認(利用妨害)
			指紋	
	行動		網膜、静脈	情報漏洩(盗聴)
			声紋、署名、歩き方	

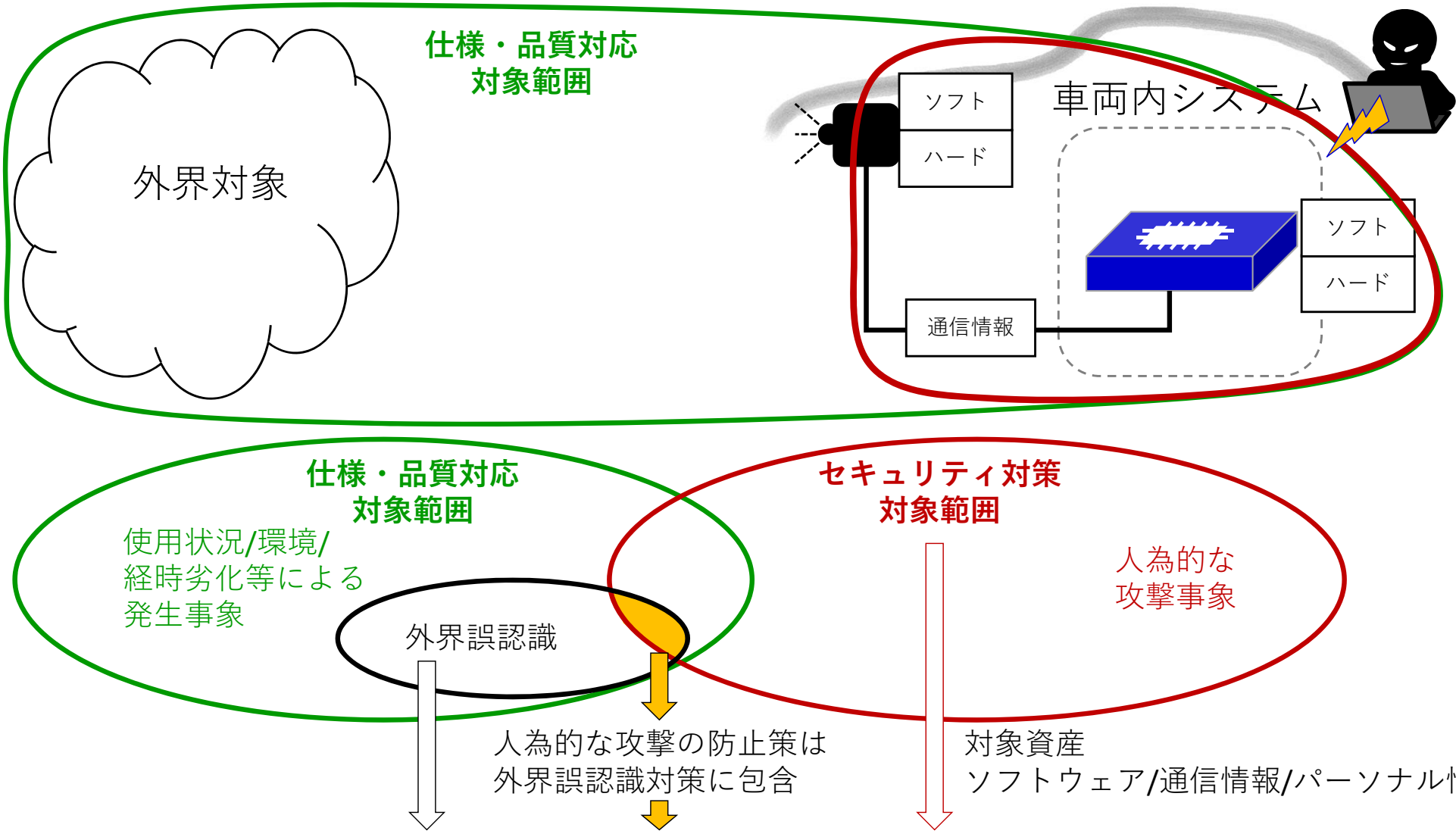
コネクテッドのセキュリティ対策概要



認証対策		通信情報対策	SW改ざん対策	脆弱性対策	車両アーキ対策
機器認証	個人認証	通信手段（プロトコル）	ソフトウェア アップデート	既知脆弱 (セキュアコーディング等)	車両内ネットワークの 多層防御
なりすまし/否認/改ざん/情報漏洩		盗聴/DOS/なりすまし			

【採用される対策技術】
■IT業界で採用されている対策技術
■車載標準化対策技術
⇒代表例；JASPAR標準化技術

外界認識システムのセキュリティ対策



認識ロジックで解決すべき課題であると想定
サイバーセキュリティとして扱うかは今後議論要

対象資産のセキュリティ対策標準化を推進

End of Presentation