安心して自動走行車を利用するためには、外部からの攻撃に対するセキュリティを確保することが非常に重要です。

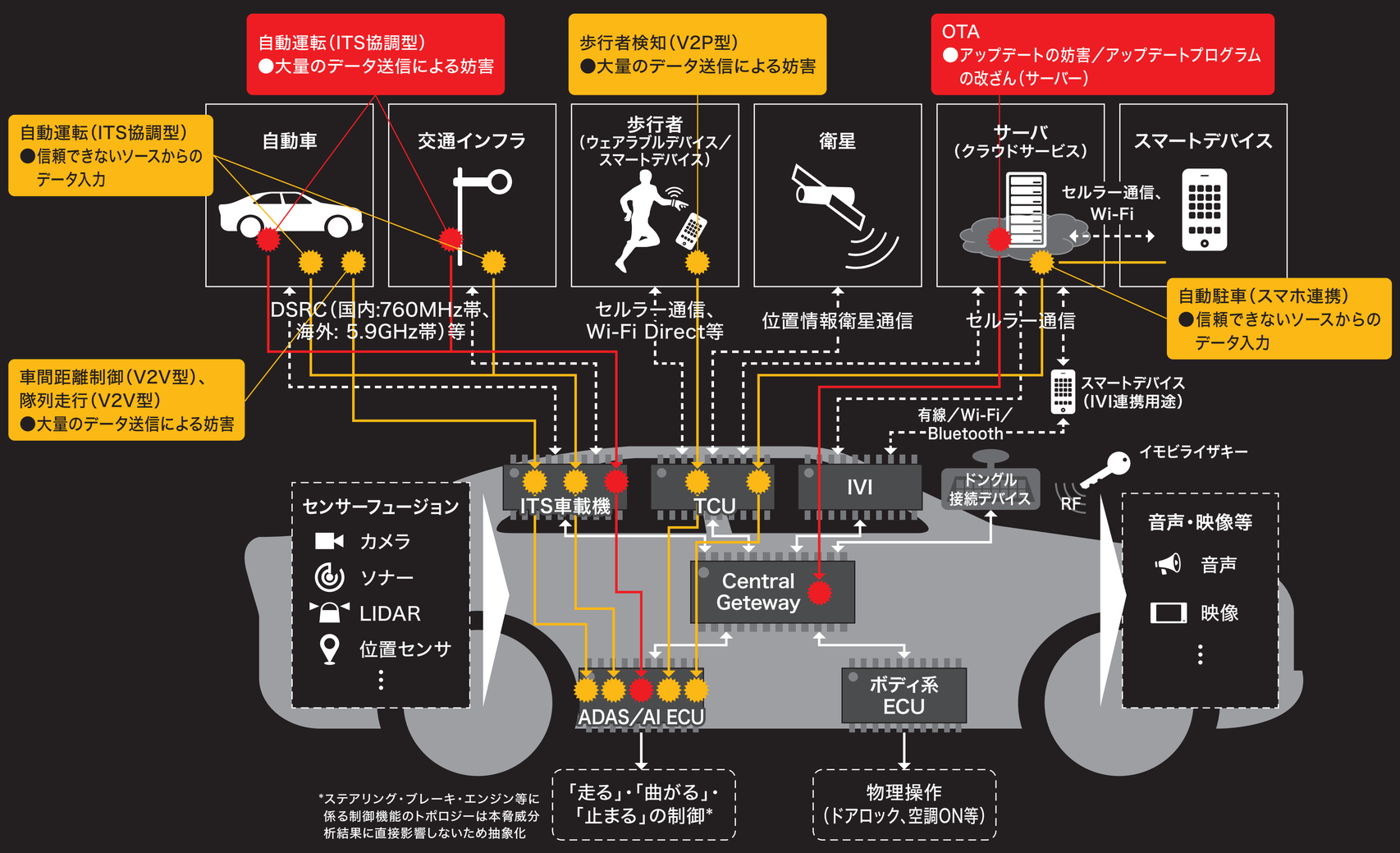
車両通信による攻撃に対するセキュリティ評価手法の確立

常時、車外情報と通信でつながる自動走行車は、ハッキングや乗っ取り等の外部からの攻撃を受ける可能性があります。これらの攻撃に対するセキュリティ機能を備えた自動走行車であれば、だれもが安心して利用することができます。

車両セキュリティ評価方法の確立

pwc

■包括的脅威モデルの策定　自動走行システム共通モデルの脅威の全体像



アプローチ

●自動運転システムに関連するサービスと機能を搭載する

共通モデルの定義

●共通モデルに対する脅威のリスト化

●脅威の重要度を評価するためのフレームワークを開発

■評価方法の確立　脅威モデルに基づいて、実際の攻撃プロセスに基づく確立された評価方法

実施プロセス

脅威分析

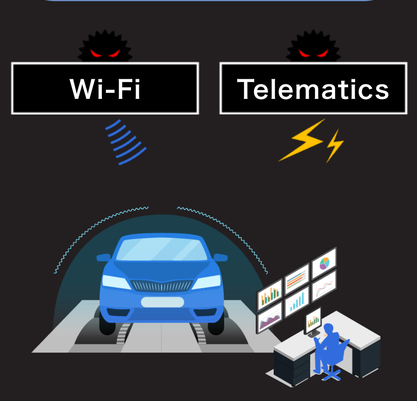
●世界の自動運転実証等のシステム構成を調査

●既知脆弱性やインシデント調査

●リスク／インパクト分析

セキュリティ評価ガイドライン策定

国内OEMとの実証実験による検証



有力セキュリティベンダ3社で競争的にガイドライン策定 → 最も目的に適したガイドライン選定して実証

2017/7-9	10-12	2018/1-3	4-6	7-9	10-12	2019/1-3

公募 → A社 / B社 / PwCコンサルティング

ステージゲート審査　OEM等と協議し3社から1社に絞り込み

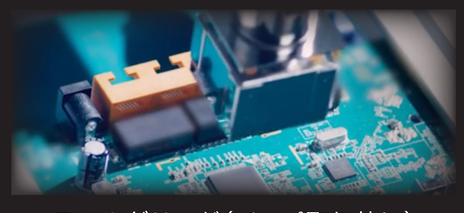
PwCコンサルティング：参加者募集 → 参加条件・各種契約調整 → 車両システム評価 → ガイドライン更新

策定評価手法のポイント

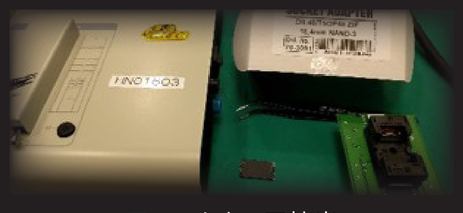
ポイント1　実際のハッカー（攻撃者）の視点からの外部I/Fからの侵入

1. 偵察	1.1 HW調査 / 1.2 SW調査
2. 侵入	2.1 ユーザー介在型の受動的攻撃 / 2.2 ユーザー非介在型の受動的攻撃 / 2.3 脆弱性を利用した能動的攻撃 / 2.4 通信傍受した情報を用いた能動的攻撃
3. 権限昇格	3.1 保護機能の解除 / 3.2 高権限の奪取
4. 目的の実行	4.1 情報漏えい / 4.2 サービス停止 / 4.3 不正操作（制御系） / 4.4 不正操作（制御系以外）

ポイント2　実際の攻撃を受けたHWセキュリティ機能を評価する



デソルダリング（チップ取り外し）



ファームウェア抽出

内閣府　NEDO

SIP 戦略的イノベーション創造プログラム　自動運転のある未来ショーケース