「戦略的イノベーション創造プログラム（SIP）自動走行システム／大規模実証実験」のうち「情報セキュリティ実証実験」に係る公募

成果物概要説明書

PwCコンサルティング合同会社

平成30年2月28日

pwc

本年度事業の位置付け

事業フェーズ	主な取り組み	主な成果物	期間
STEP1 実証前調査	*脅威分析調査*	• *将来の自動走行モデルの全体像* • *上記に対する脅威の全体像*	2017/9/28 - 2018/2/28
	評価ガイドラインドラフトの作成	• *評価ガイドラインドラフト（初版および第2版）*	
	情報セキュリティ評価の試行調査		
	実証実験（STEP2）の運営準備	• *実証実験実施計画（スケジュール）* • *実証実験参加プロトコル（フローチャート等）* • *参加者募集要領（要領、規約、申請書、契約書類）* • *参加者募集説明実施要領、説明資料* • *実証実験情報管理手法、体制案*	
STEP2 実証実験	*実証実験の実施と評価ガイドラインのブラッシュアップ*	• *評価ガイドラインドラフト（最終版）*	2018/4 - 2019/2

本年度事業範囲

脅威分析調査の目的とスコープ

目的:

自動走行に係るV2X 等車外からの攻撃を含む脅威の全体像の整理し、自動走行車両セキュリティに関するコンセンサスの醸成を支援すること

スコープ:

I. 脅威分析調査	自動走行システム共通モデル調査	• 自動車メーカ、部品サプライヤ、IT企業などの自動運転・コネクテッドカーに係る取り組みをファクトベースで調査し、整理・類型化することで自動走行システム共通モデルを導出する
	脅威の全体像調査	• 自動走行システム共通モデルに係る、V2X等車外からの攻撃を含む脅威項目を抽出する • 脅威項目ごとに影響度評価を実施し、特に重大な脅威については、対策状況を調査し、必要に応じて別途作成する評価ガイドラインに反映する

自動走行システム共通モデル調査アプローチ

自動走行システム共通モデル調査	• 自動車メーカ、部品サプライヤ、IT企業などの自動運転・コネクテッドカーに係る取り組みをファクトベースで調査し、整理・類型化することで自動走行システム共通モデルを導出する
脅威の全体像調査	• 自動走行システム共通モデルに関し、[redacted]等の脅威を含む脅威を洗い出し、脅威の全体像の整理する • 自動走行システム共通モデルに含まれる脅威に対して脅威分析を実施し、特に重大な脅威については、評価ガイドラインに対策を盛りこむ

赤字: 本調査の主要な成果物

1 自動走行関連サービスと機能の一覧

- 自動車メーカ、自動車部品メーカ、およびIT企業等の公開情報を調査し、自動走行システム・コネクテッドカーに関するサービスを調査し、それを実現する機能を整理

調査対象

- 自動車メーカ（16社）
- 自動車部品メーカ（4社）
- IT企業（23社）

サービス・機能の一覧

	サービス	機能
1	運転・駐車支援	車間距離制御 車線維持制御 車間距離制御（ITS協調型） 隊列走行 自動運転（ITS協調型） 自動運転（自律型） 駐車周辺映像表示 自動駐車 自動駐車（スマホ連携）
2	…	…

【インプット】
- 自動車メーカ（16社）、自動車部品メーカ（3社）、IT企業（23社）の公開情報（HPなどを参照）

【アウトプット】
- サービス・機能の一覧

2 機能別のシステム構成想定

- 自動車メーカ、IT企業の公開情報をもとに調査し、機能を実現するシステム構成を検討
  ＊業界の有識者へのインタビュー結果も考慮

機能の想定システム構成

	サービス	機能
1	運転・駐車支援	車間距離制御 車線維持制御 車間距離制御（ITS協調型） 隊列走行 自動運転（ITS協調型） 自動運転（自律型） 駐車周辺映像表示 自動駐車 自動駐車（スマホ連携）
2	…	…

HP等

システム構成特定

車間距離制御（システム構成図）

【インプット】
- サービス・機能の一覧
- 主要な自動車メーカ・IT企業が公開する機能に関する公開情報
- 有識者インタビューにおけるご意見

【アウトプット】
- 機能別の想定システム構成

3 自動走行システム共通モデルの特定

- 機能別の想定システム構成をすべて勘案し本脅威分析調査における自動走行システム共通モデルを特定
  ＊業界の有識者へのインタビュー結果も考慮

機能別の想定システム構成

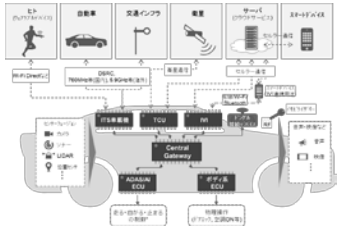
車間距離制御

自動運転（自律型）

自動運転（ITS協調型）…

有識者のご意見

自動走行システム共通モデル

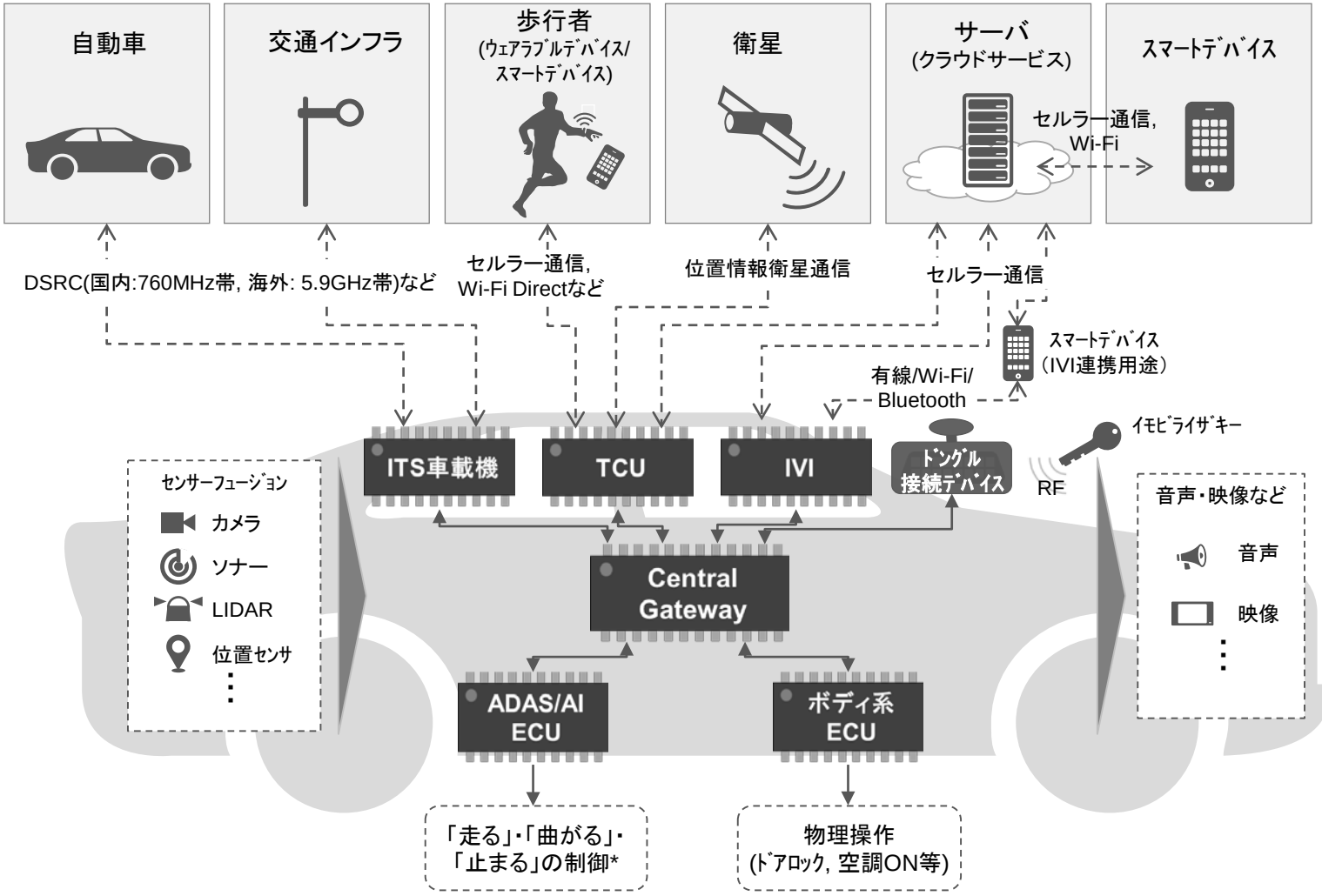


【インプット】
- 機能別の想定システム構成
- 有識者インタビューにおけるご意見

【アウトプット】
- 本脅威分析調査における自動走行システム共通モデル

自動走行システム共通モデル(2020年代前半)

本脅威分析調査における自動走行システム共通モデル



*ステアリング・ブレーキ・エンジン等に係る制御機能のトポロジーは本脅威分析結果に直接影響しないため抽象化

a 脅威分析調査

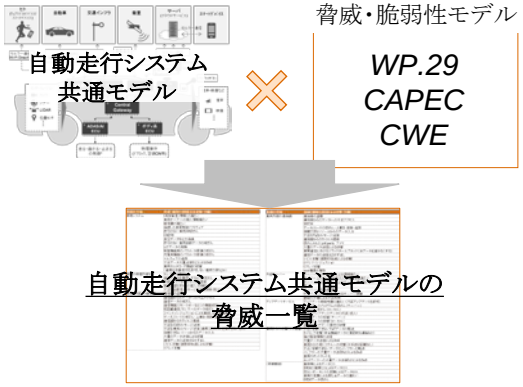
脅威の全体像調査アプローチ

自動走行システム共通モデル調査	• 自動車メーカ、部品サプライヤ、IT企業などの自動運転・コネクテッドカーに係る取り組みをファクトベースで調査し、整理・類型化することで自動走行システム共通モデルを導出する
脅威の全体像調査	• 自動走行システム共通モデルに係る、V2X等車外からの攻撃を含む脅威を洗い出し、脅威の全体像の整理する • 自動走行システム共通モデルに含まれる脅威に対して脅威分析を実施し、特に重大な脅威については、評価ガイドラインに対策を盛りこむ

赤字: 本調査の主要な成果物

4 自動走行システム共通モデルの脅威の一覧化

- 自動走行システム共通モデルに対して、WP.29のThreat Matrixと各種脅威・脆弱性モデルを適用することで、自動走行システム共通モデルの脅威の一覧を整理

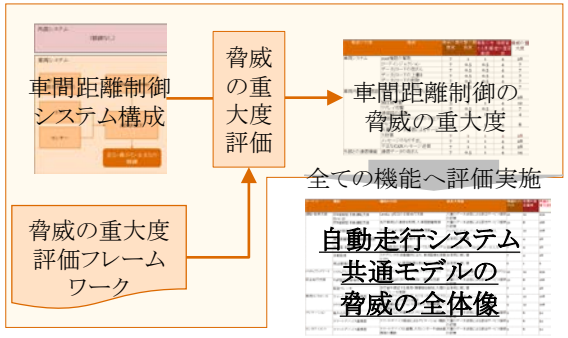


【インプット】
- 自動走行システム共通モデル
- 脅威モデル(WP.29 Threat Matrix, CAPEC)
- 脆弱性モデル(CWE)

【アウトプット】
- 自動走行システム共通モデルの脅威一覧

5 自動走行システム共通モデルの脅威の全体像特定

- 自動走行システム共通モデルの脅威一覧と脅威の重大度の評価指標と組み合わせ、脅威の重大度を評価するフレームワークを策定
- 機能を実現するシステムに対して、上記フレームワークを適用し、機能の脅威の重大度を評価
- 全ての機能に対してこれを実施し、自動走行システム共通モデルの重大の全体像を特定

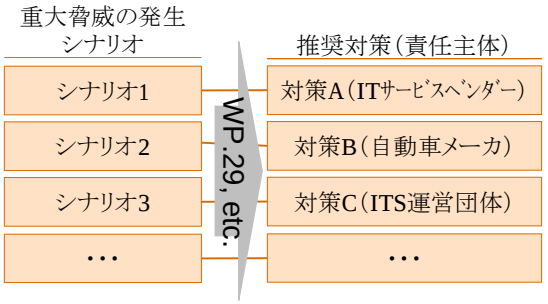


【インプット】
- 脅威の一覧
- 脅威の重大度の評価指標(WP.29, CRSS)
- 機能別の想定システム構成図

【アウトプット】
- 自動走行システム共通モデルの脅威の全体像

6 重大脅威に対する対策状況調査

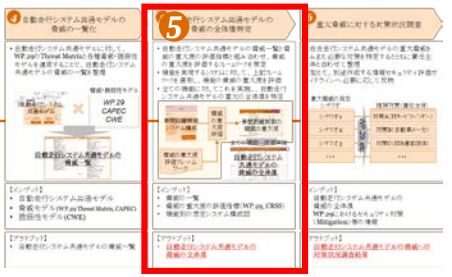
- 自走走行システム共通モデルの重大脅威をふまえ必要な対策を特定するとともに責任主体と合わせて整理
- 加えて、別途作成する情報セキュリティ評価ガイドラインへ必要に応じて反映



【インプット】
- 自動走行システム共通モデルの脅威の全体像
- WP.29におけるセキュリティ対策(Mitigation)等の情報

【アウトプット】
- 自動走行システム共通モデルの脅威への対策状況調査結果

自動走行システム共通モデルの脅威の全体像



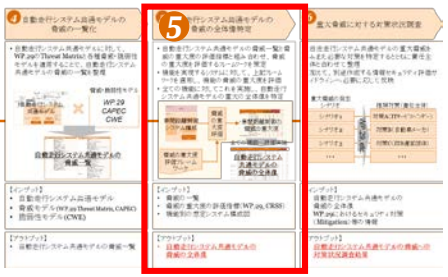
自動走行システム共通モデルに内在する脅威のうち、脅威の重大度スコアがレベルII以上のものを抽出し、以下に示す。

脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

自動走行システム共通モデルの脅威の全体像

サービス		機能			脅威	脅威の大きさ	攻撃の発生確率	脅威の重大度
名称		名称		内容				
1	運転・駐車支援	1-3	車間距離制御（V2V型）	ITSと協調し先行車両との車間距離を制御する機能	信頼できないソースからのデータ入力	2.8	1.6	4.4
					大量のデータ送信による妨害	4.2	1.6	6.7
		1-4	隊列走行（V2V型）	先頭車両と通信を行うことで後続車が無人で先頭車両を追従する機能（トラックなど商用車向け）	信頼できないソースからのデータ入力	2.8	1.6	4.4
					大量のデータ送信による妨害	4.2	1.6	6.7
		1-5	自動運転（ITS協調型）	ITSと協調することで人間に代わりあらゆる運転タスクを実施する機能	信頼できないソースからのデータ入力	2.8	2.4	6.7
					大量のデータ送信による妨害	4.2	2.4	10.0
		1-9	自動駐車（スマホ連携）	スマートフォンにインストールされたアプリケーション経由で車両の操作指示を行うことで、遠隔からの車両の自動駐車を実施する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
					信頼できないソースからのデータ入力	2.8	2.4	6.7
2	安全走行支援	2-2	歩行者検知（V2P型）	歩行者の所有するスマートデバイスと連携し、車両の近くにいる歩行者を検知することで、必要に応じて車両を制御し歩行者との衝突を回避する機能	信頼できないソースからのデータ入力	2.8	1.6	4.4
					大量のデータ送信による妨害	4.2	1.6	6.7
4	ｿﾌﾄｳｪｱｱｯﾌﾟﾃﾞｰﾄ	4-1	OTA	無線通信を利用した電子制御システムのソフトウェア更新サービス	アップデートの妨害/アップデートプログラムの改ざん（サーバー）	4.2	2.4	10.0
					正当なアップデート実行の妨害	3.6	1.2	4.3

自動走行システム共通モデルの脅威の全体像



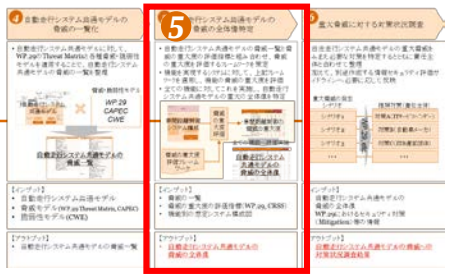
自動走行システム共通モデルに内在する脅威のうち、脅威の重大度スコアがレベルII以上のものを抽出し、以下に示す。

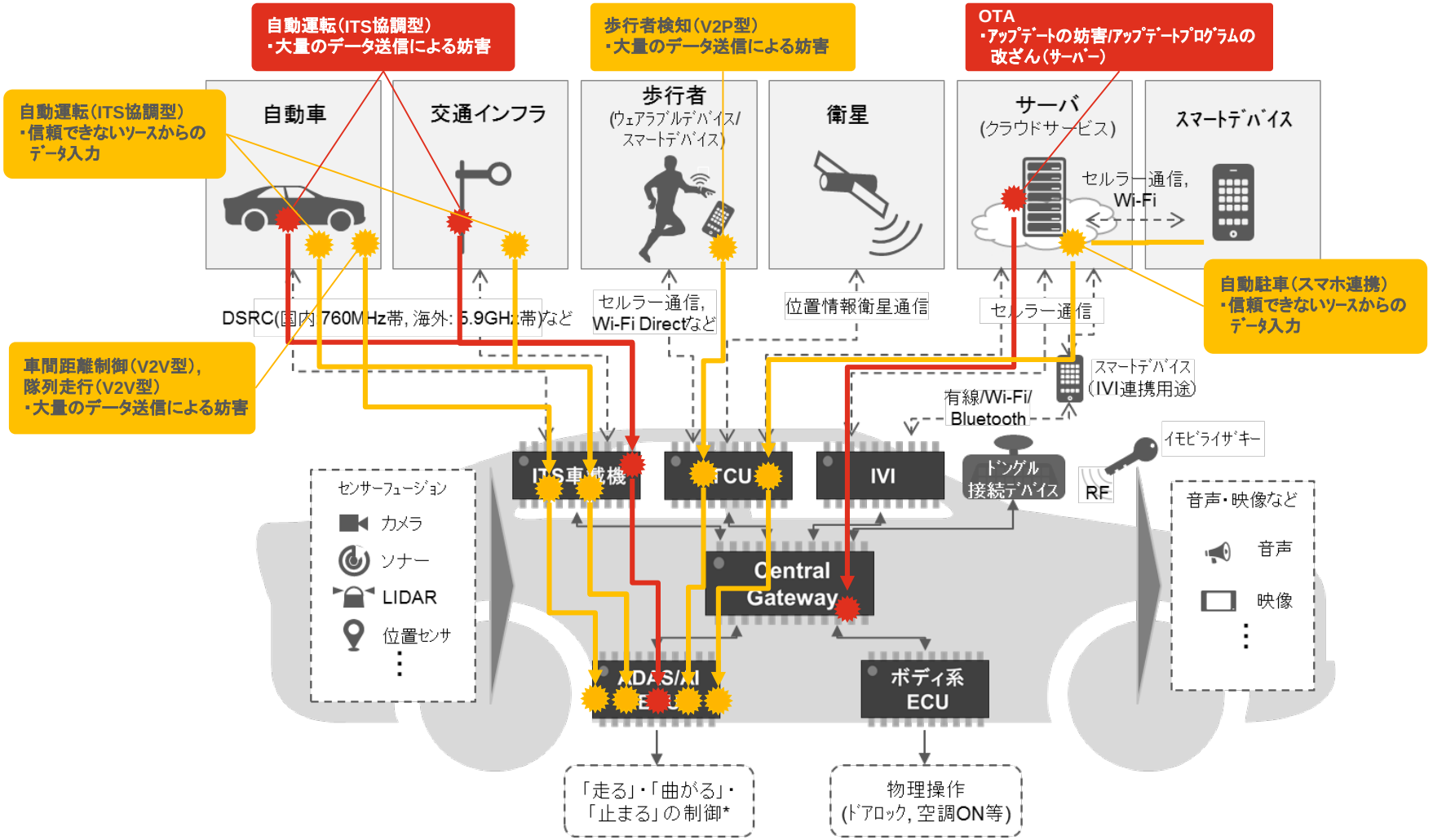
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

自動走行システム共通モデルの脅威の全体像

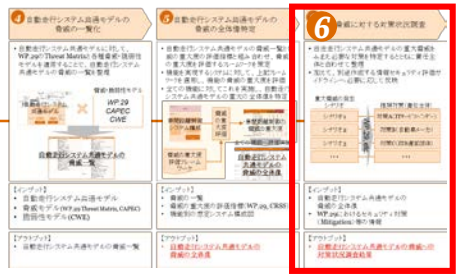
サービス		機能			脅威	脅威の大きさ	攻撃の発生確率	脅威の重大度
名称		名称		内容				
5	故障検知	5-1	故障検知	自動車に備わる自己診断機能を活用し、故障を予知・検知するサービス	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
8	車両遠隔操作	8-1	遠隔からのﾄﾞｱﾛｯｸ・ｱﾝﾛｯｸ	スマートデバイスなどと連携し、遠隔地より車両のドアのロック・アンロックを制御する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
		8-3	充電制御	スマートデバイスと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
		8-4	充電制御（音声認識AI連携）	音声認識AIエージェントと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
		8-5	エアコン制御	スマートデバイスと連携し、遠隔地よりエアコンのオン・オフを制御する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
		8-6	エアコン制御（ 音声認識AI連携）	音声認識AIエージェントと連携し、遠隔地よりエアコンのオン・オフを制御する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
		8-7	エンジン再駆動・ステアリングロック解除禁止	オーナーの要請に基づき、エンジンの再始動・ステアリングロックの解除の禁止を実施する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3

自動走行システム共通モデルの脅威の全体像
（スコアが6以上の脅威について図示）

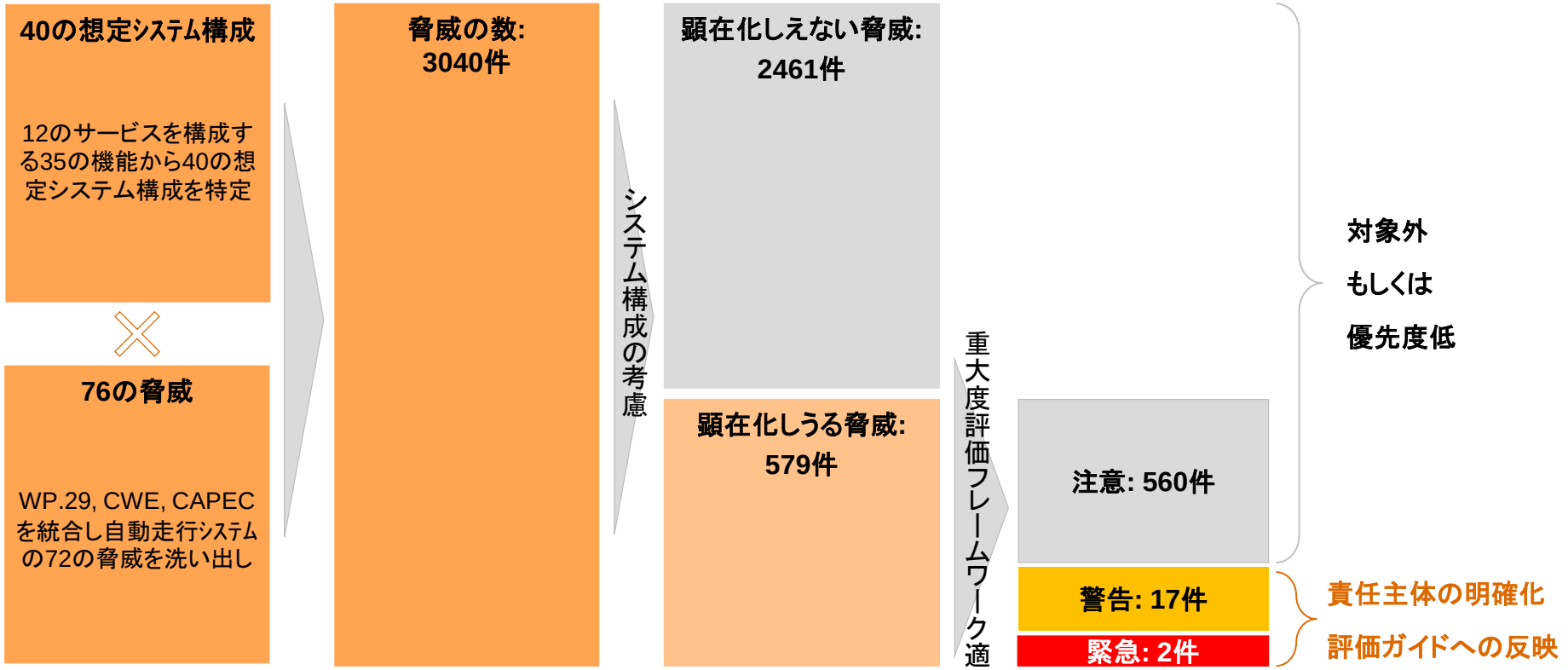




脅威の全体像調査のアプローチ（まとめ）



- 自動走行システムに係るすべてのシステム構成を踏まえ顕在化しうる脅威を抽出し、重大度評価フレームワークを適用することで優先して対応すべき脅威を特定
- 特定した脅威に対して、対策の責任主体を明確化するとともに、車両側での対策が必要な脅威は、評価ガイドへ反映



ステークホルダーが危惧すべき脅威と対策の提言

01 自動車メーカ

- 自動車メーカは、ITS 協調型の自動運転機能に対する「大量データ送信による妨害」などの脅威への対策が必要である
- 自動車メーカが主体的に対策すべき重大脅威については評価ガイドラインへ項目を追加しており、今後これらに基づき評価することで対策がなされることを期待している

02 IT サービス事業者

- IT サービス事業者は、OTA 機能に対する「アップデート妨害」などの脅威への対策が必要である
- これらは主にサーバ等の情報システムにおける対策が必要であり、本プロジェクトの検討範囲外である
- 一方で、SIP「重要インフラ等のけるサイバーセキュリティの確保」にて対応検討中であり、今後は協力した取り組みが重要となる

03 政府等

- 政府等は、自動車と協調する交通インフラに対する「大量データ送信による妨害」などの脅威への対策が必要である
- これらに対する自動走行システムと協調したセキュリティ対策は現状未検討の状態であり、今後の普及に向けて本格的なセキュリティ対策の検討が必要である

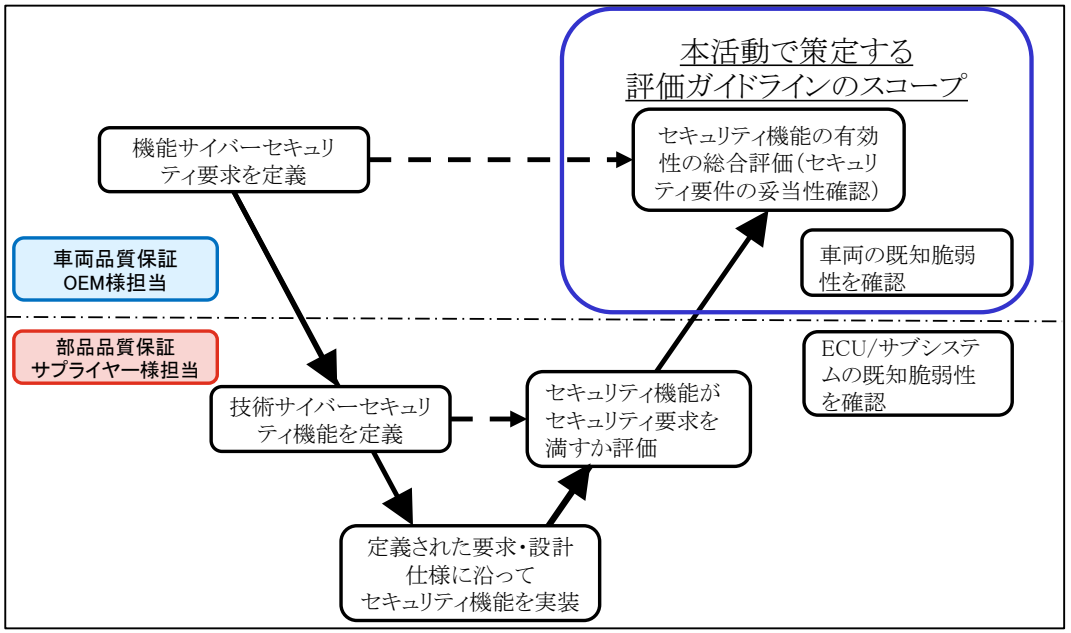
04 デバイス提供事業者

- デバイス提供事業者は、V2P 用途のウェアラブルデバイスやスマートデバイスに対する「信頼できないソースからのデータの入力」などの脅威への対策が必要である
- これらに対する自動走行システムと協調したセキュリティ対策は現状未検討の状態であり、今後の普及に向けて本格的なセキュリティ対策の検討が必要である

評価ガイドラインの概要 および スコープ

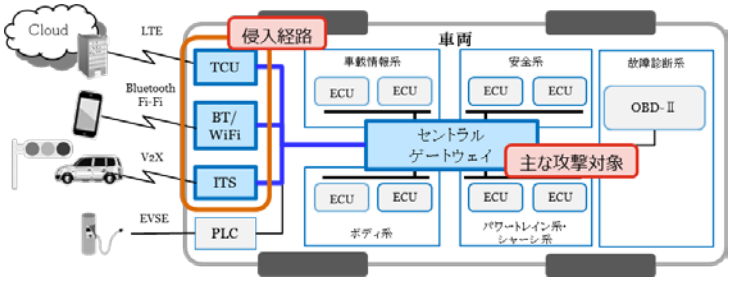
ガイドラインのスコープ

- 車両OEM各社、JasPar等のステークホルダとの議論の結果を踏まえまして、*車両開発のV字モデルにおける総合評価などで活用できるガイド*にする方針としました

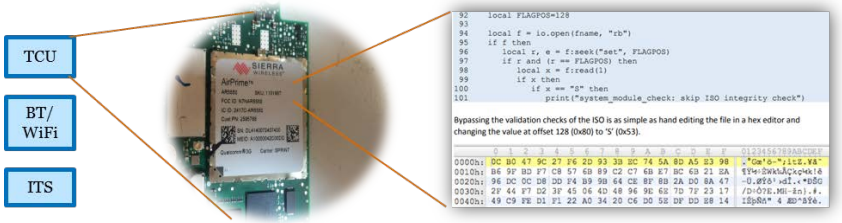


評価方法の特徴

1. 実際のハッカー（攻撃者）の視点で車両外部I/Fから侵入テストによる評価

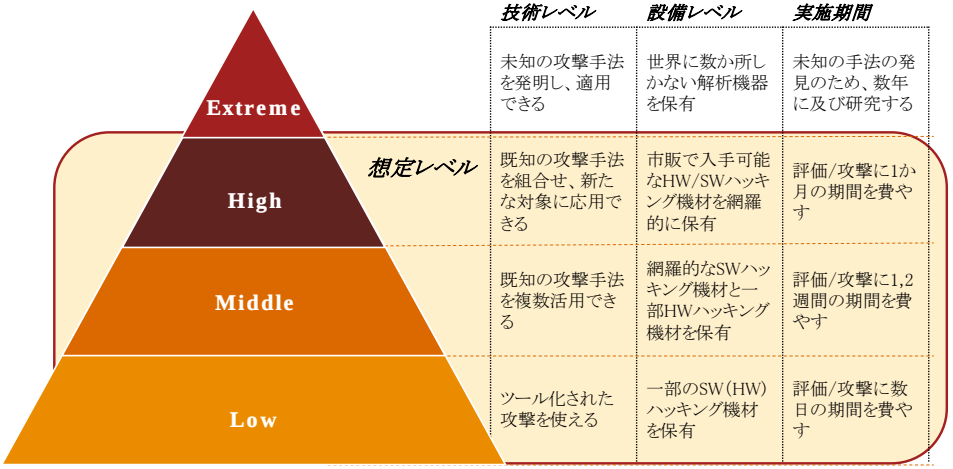


2. 現実の車両攻撃内容を考慮したHWセキュリティ対策も評価対象とする

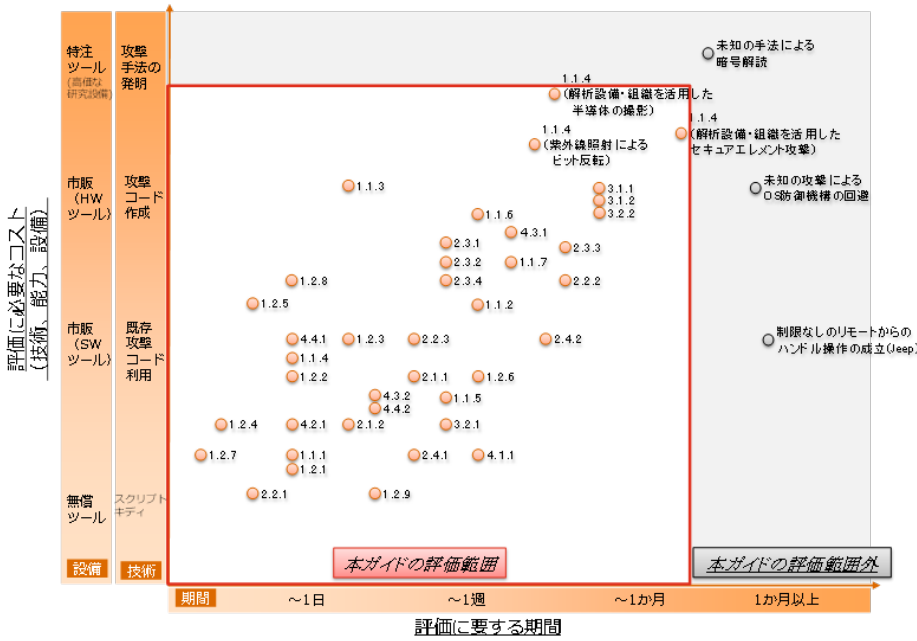


評価ガイドライン　評価内容

攻撃者のプロファイルを分析し、高度な技術レベルや設備を持つ場合をカバーする評価内容を策定。同評価の実施により、現実の車両セキュリティ被害を防止できる。



	技術レベル	設備レベル	実施期間
Extreme	未知の攻撃手法を発明し、適用できる	世界に数か所しかない解析機器を保有	未知の手法の発見のため、数年に及び研究する
High	既知の攻撃手法を組合せ、新たな対象に応用できる	市販で入手可能なHW/SWハッキング機材を網羅的に保有	評価/攻撃に1か月の期間を費やす
Middle	既知の攻撃手法を複数活用できる	網羅的なSWハッキング機材と一部HWハッキング機材を保有	評価/攻撃に1,2週間の期間を費やす
Low	ツール化された攻撃を使える	一部のSW(HW)ハッキング機材を保有	評価/攻撃に数日の期間を費やす



評価ガイドラインで想定する評価レベル

現実の攻撃者の技術・設備を考慮した内容で評価レベルを設定

評価レベルと評価項目の関係

HW評価など高レベルな攻撃（評価）を含む評価項目単位で外部委託するケースも考慮

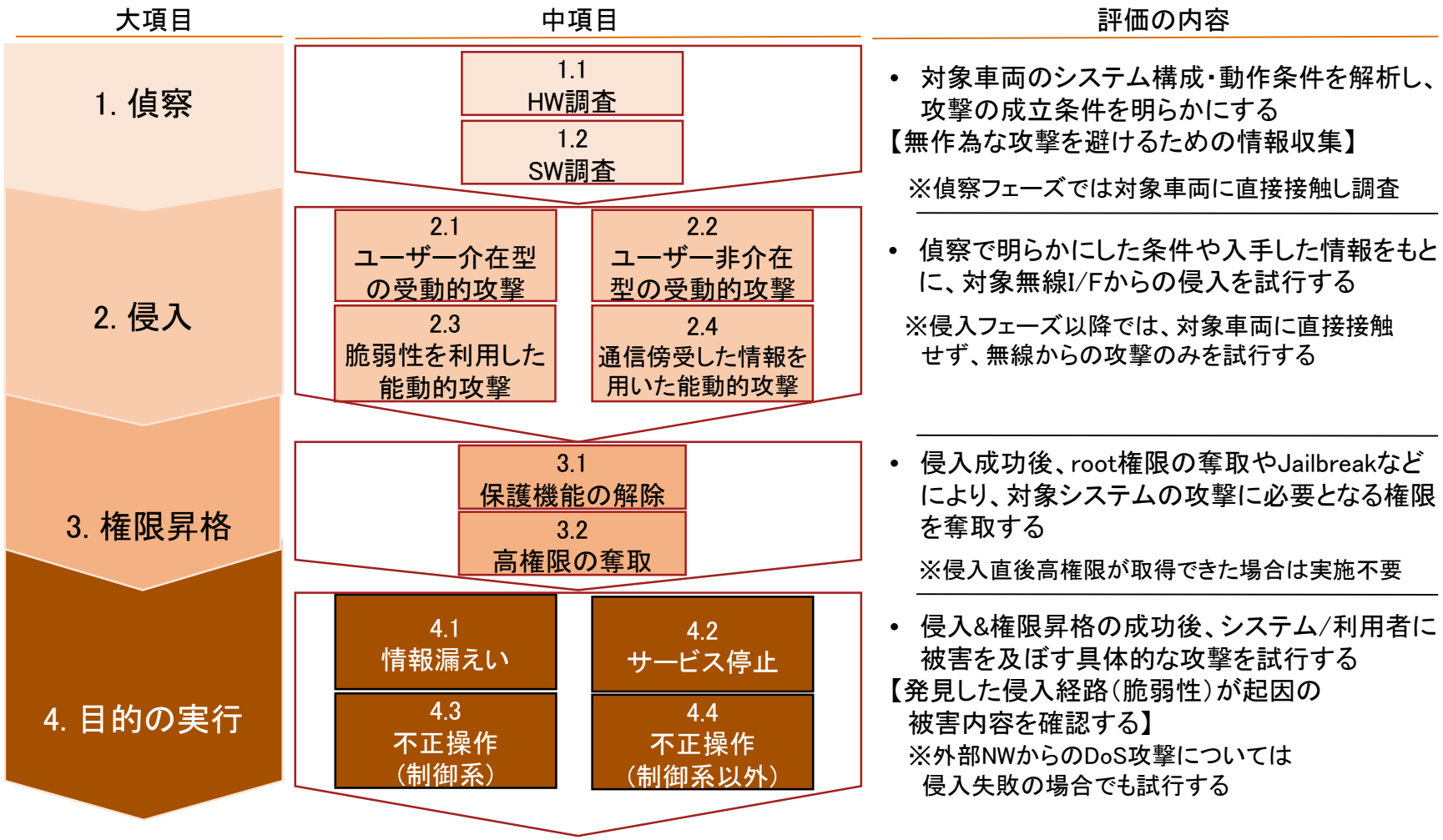
評価ガイドライン　評価範囲

本評価ガイドラインは下記に挙げる車両インシデント・脆弱性事例をプロファイルし、各インシデントで実施された攻撃を再現する手法を評価ガイドラインの評価項目として記載した。これにより、下記と同種の車両セキュリティインシデントの再発を防止します。

インシデント事例	インシデント概要
Jeep CherokeeのuConnect脆弱性	第３者により車両位置の特定やリモートで車両を操作される脆弱性。Cellular Network上の開放ポートから車載器に侵入し、CANコントローラのファームウェア改ざんすることで車両をリモート操作することが可能
BMWのConnectedDrive脆弱性	第３者により車両をリモート操作される可能性のある脆弱性。研究者の用意したテレマティクスサーバーから車両に対しドア解錠のコマンドを送ることでドアを解錠することが可能
Tesla ModelSの無線LAN脆弱性	第３者により車両をリモート操作される脆弱性。研究者は偽WiFiスポットを利用して攻撃サイトに誘導する方法を提示したが、Cellular Networkを介した攻撃も可能である。その場合、おとりメール等を用いて、ユーザーを攻撃サイトに誘導する。
三菱アウトランダーのモバイルアプリ脆弱性	第３者により空調設定等の環境設置をリモート操作される脆弱性。車内に設置されたWiFiスポットにアクセスすることで防犯装置の設定や空調操作をリモート操作することが可能
日産Nissan Connect EVの脆弱性	一般ユーザーが利用しない開発設定が残存しており、これを利用することでユーザーID,パスワード等の機密情報が外部に漏えいさせることが可能
日産リーフの脆弱性	認証方式に不備があり、スマートフォン⇔サーバーAPIに認証の仕組みが実装されておらず、VIN下5桁が判明すれば他の車両を制御することが可能 ※スマートフォンアプリの脆弱性であるが、車両⇔サーバー、あるいは車両⇔スマートフォンで同様の事象が発生しないか確認する
スバルStarLinkの脆弱性	スマートフォンのデバイス認証に使用されるセキュリティトークンには有効期限がなく、窃取された場合、第３者によりドアを解錠させることが可能 ※スマートフォンアプリの脆弱性であるが、車両⇔サーバー、あるいは車両⇔スマートフォンで同様の事象が発生しないか確認する
Continental AGのTCUの脆弱性	第３者によりTCUがリモート操作される可能性のある脆弱性
マツダのMazda Connectの脆弱性	車内のUSBポートから任意のコードを実行される脆弱性。AVNのカスタマイズに利用された ※ローカル攻撃であるが、リバースエンジニアリング耐性を図る評価ポイントとして採用
本田技研工業のHonda Connectの脆弱性	車内のUSBポートから任意のコードが実行される脆弱性。AVNのカスタマイズに利用された ※ローカル攻撃であるが、リバースエンジニアリング耐性を図る評価ポイントとして採用

情報セキュリティ評価ガイド　評価一覧（大・中項目）

ハッカーによる実際の攻撃フローを基に、評価手順、評価項目を体系化



国際標準化のプロセス

専門委員会 /分科委員会の積極参加メンバーと協力し、我が国の推奨する自動車に係る情報セキュリティ技術を確実にWD /CD /DISへ反映する必要があります。

幹事により任命された専門家によるWGにおけるWDの検討作成

定められた基準に従い承認活動を実施し、基準を満たす場合、最終国際規格案（FDIS）として登録

*投票による承認を実施

各加盟国期間、TC（専門委員会）/SC（分科委員会）の幹事などによる新たな規格の策定、現行規格の改定案の提案

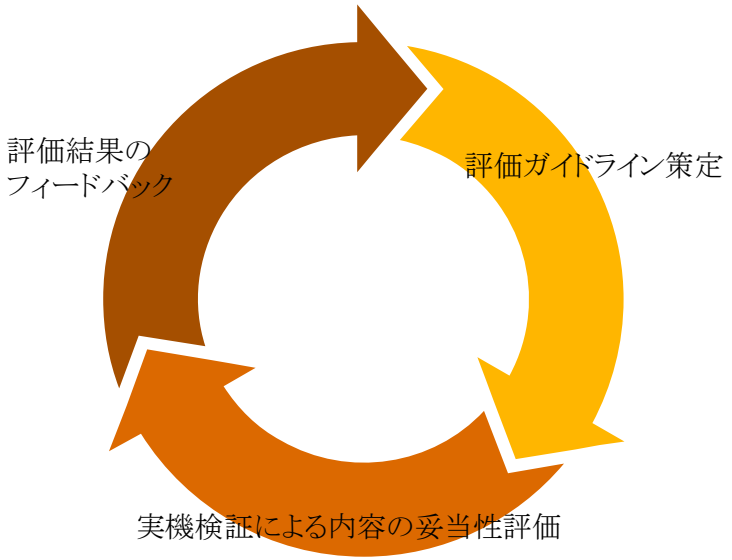
P（積極的参加）メンバーの意見を踏まえ幹事を中心にCD案を検討、必要に応じて修正
※委員会は技術的問題が解決できない場合、TSとして発行可能

投票により国際規格としての承認を行う
（承認されなかった場合、修正原案の再提出、TSとして発行、取り消しのいずれかを選択）

36ヶ月以内

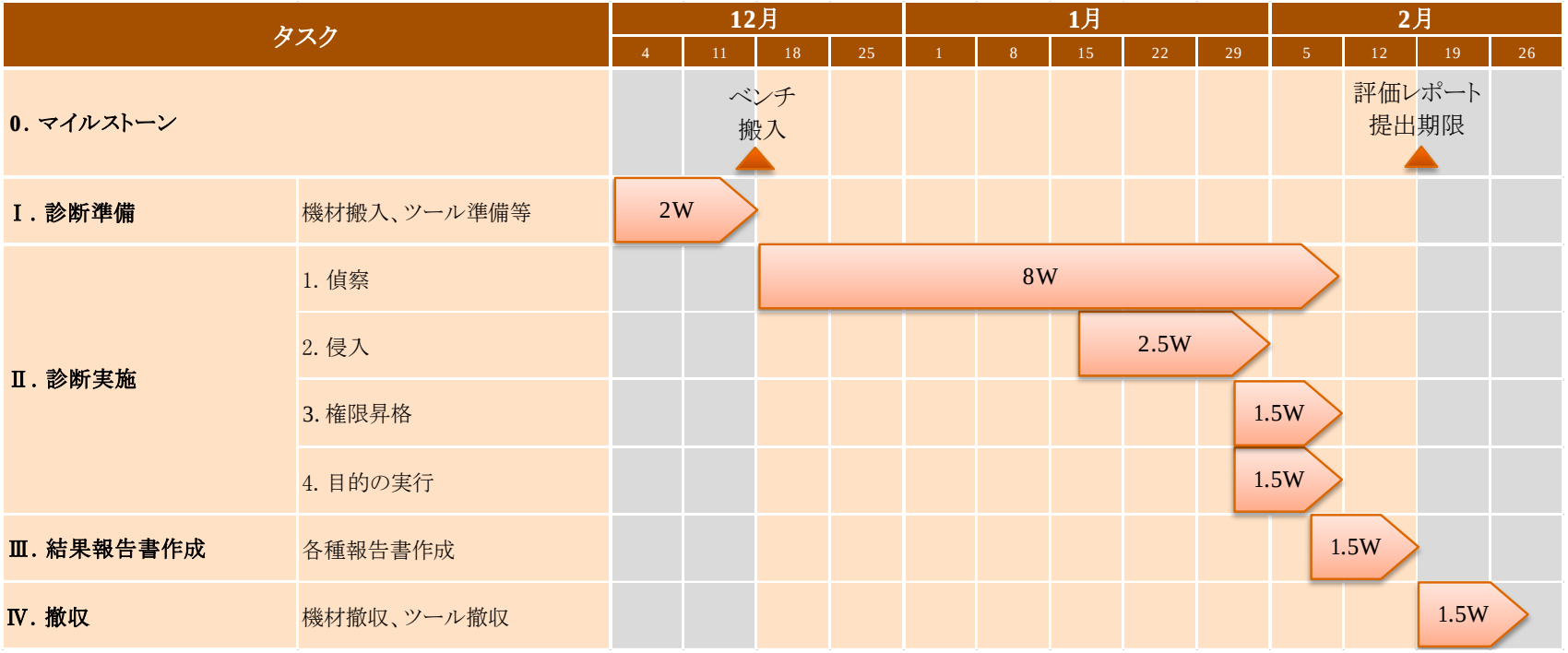
試行調査の目的

試行調査は、評価ガイドラインの妥当性評価の他、車両提供者（OEM)に対する改善事項のフィードバックを行うことを目的とする

評価ガイドラインの妥当性評価	車両提供者（OEM）へのフィードバック
評価ガイドラインの項目に従い、実車両に対し評価を試行することで、内容の妥当性を評価する。併せて評価結果を評価ガイドラインへ反映させることで、より実現可能性の高いものへ昇華させる  	攻撃者の立場から検証機に関わるセキュリティ脅威の顕在要因となりうる脆弱性を調査し、改善が必要とみられる事項を検出した場合は、OEMに対し改善の方向性について助言を行う OEMが得られるメリット 1. 高い技術力を持つ攻撃者によるHWおよびSWハッキングで、現実に発生し得る被害を明らかにする 2. 攻撃者が対象車両を攻撃する具体的な詳細手順をご提供し、OEM担当者による再現を可能にする 3. 現実の被害をベースとしたセキュリティ品質および、開発コストの両面で最良の対策の提供する

試行調査　実施スケジュール

ベンチシステム搬入から評価レポートの提出まで、年末年始を挟み、約8週間の評価期間であった。そのうち7週間を偵察フェーズにおけるファームウェア入手の作業に充てた。一方、時間的な制約の都合で権限昇格や目的の実行に関する作業は一部のみ実施した。



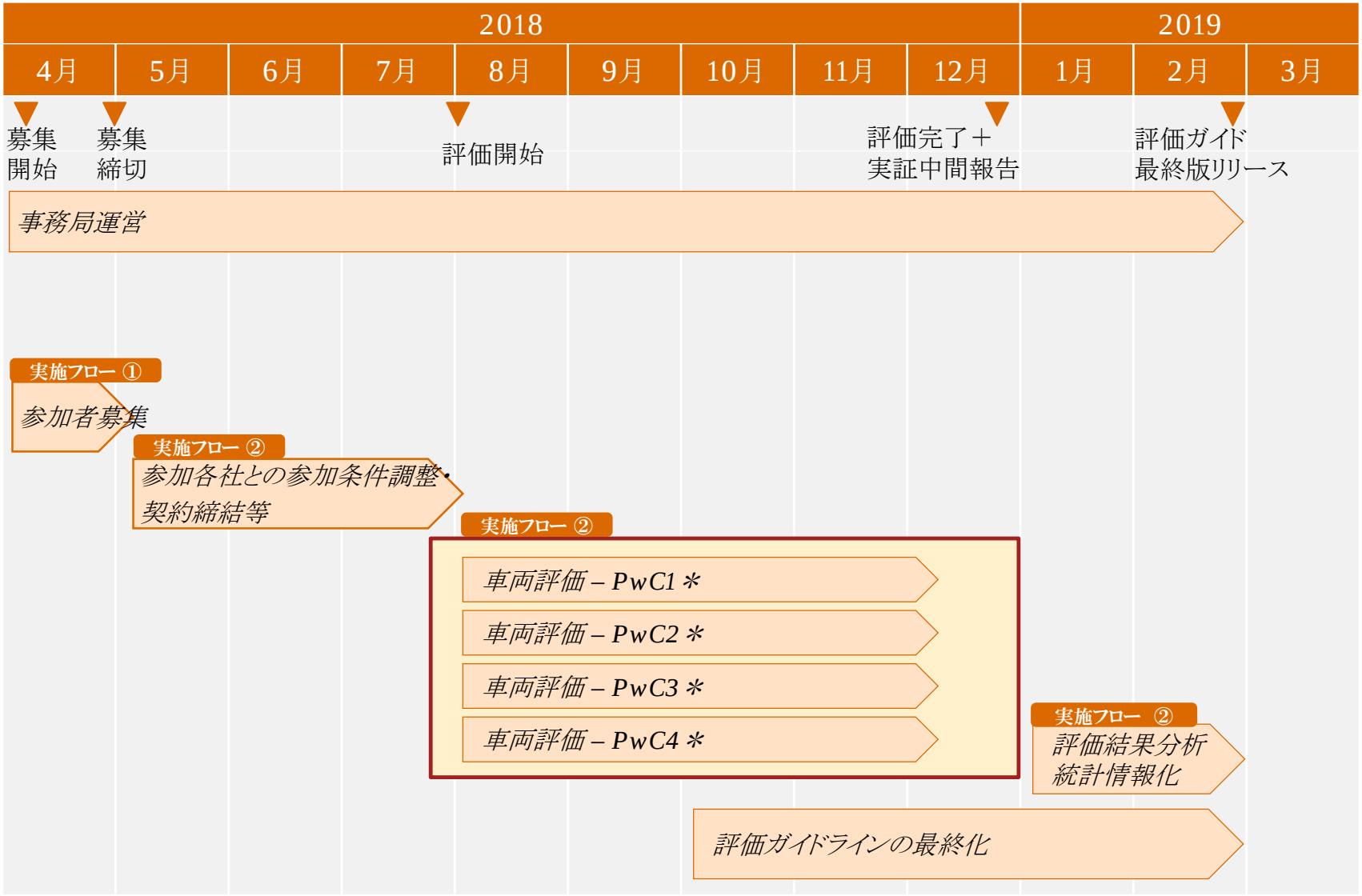
評価結果報告フォーマット

本試行調査の結果は下記の様式を用いて結果を報告した。

評価ガイドライン項番	（評価項目の対応する項番を記載）
評価結果	評価結果の内容を記載
危険度	右記の判定基準に沿って 項目の危険度を記載
評価内容	評価により確認する内容を記載
評価手順	具体的な評価実施手順を記載
想定されるリスク	問題が見つかった場合、想定されるリスク（被害）の内容を記載
攻撃成立条件	問題が見つかった場合、攻撃が成功するための前提条件を記載
改善案	問題が見つかった場合、攻撃を防ぐための改善案を記載

危険度	判定基準の定義
High	対象システムにおいて発見された脆弱性を修正対応しないことにより、高度な技術や高いコストをかけずに緊急性の高いセキュリティ侵害が発生し、事業運営に甚大な悪影響を及ぼす（リコールや業務停止等の）可能性がある。直ちに脆弱性の修正対応等の実施に着手すべきである。
Medium	対象システムにおいて発見された脆弱性を修正対応しないことにより、一定の技術やコストをかけた攻撃により緊急性のあるセキュリティ侵害が発生し、事業運営に多大な悪影響を及ぼす（業務パフォーマンスの著しい悪化等の）可能性がある。必要に応じて脆弱性の修正対応等の実施を推奨する。
Low	対象システムにおいて発見された事項において、直ちにセキュリティ上の影響があるわけではないが、対策を実施することにより一定のセキュリティの向上が見込まれる項目である。将来的に事項の対応等の実施を推奨する。
Info	対象システムにおいて発見された事項において、何らかの影響を及ぼす可能性がある項目である。対策の是非について検討を推奨する。

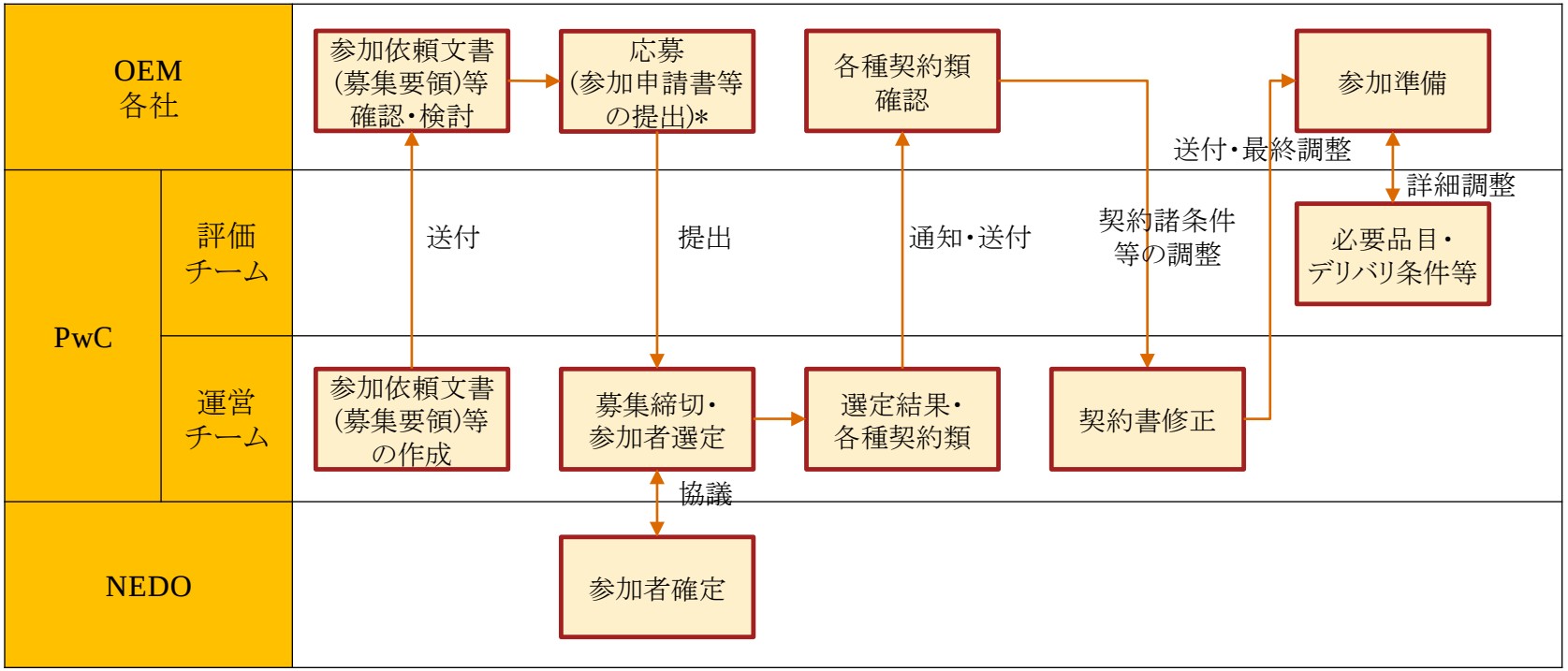
実証実験スケジュール概要



PwC　＊設定期間内で各参加者提供車両・機材のセキュリティ評価を2か月間実施します。実施時期は事前に調整させていただきます。

実施フロー①： 参加者募集

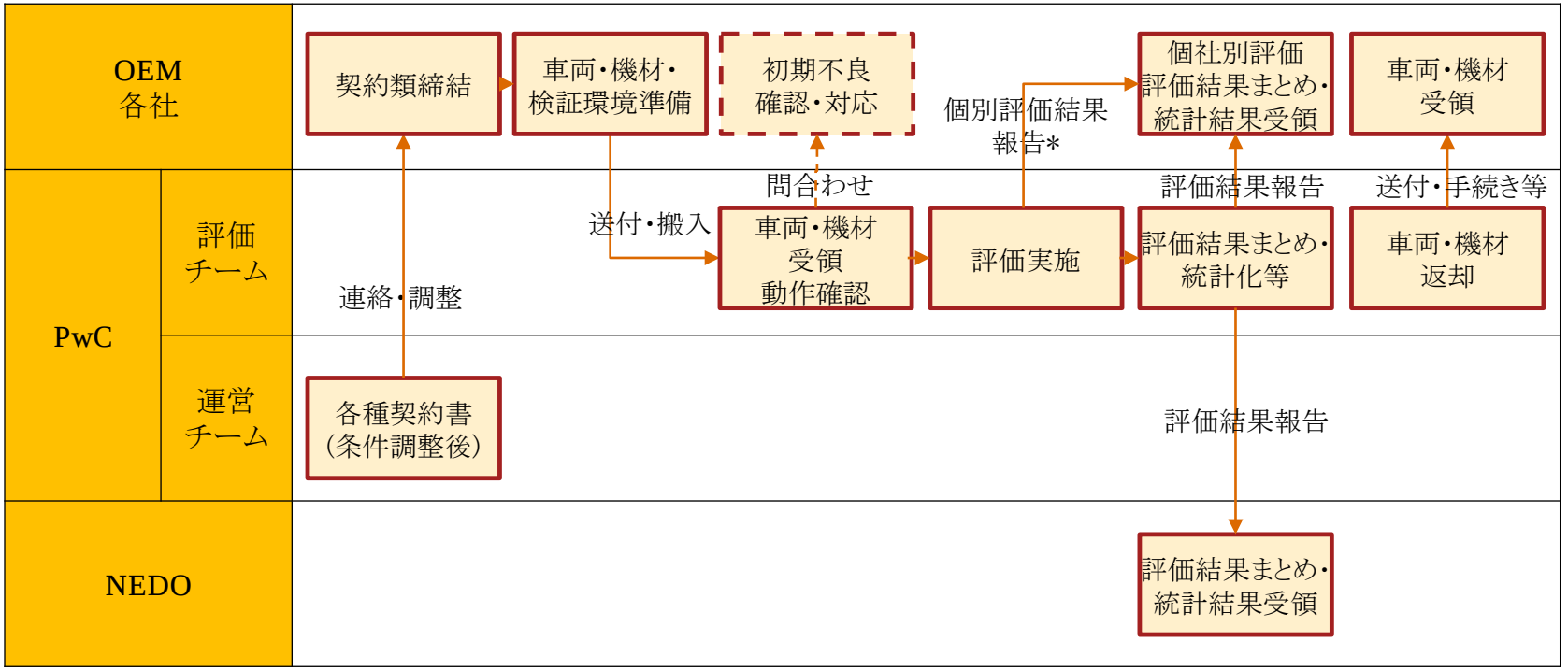
参加者募集及び諸条件の事前調整等に関するフローは以下を想定しています。



＊参加者からの要望に応じて参加説明会を実施いたします。

実施フロー②： 評価準備・実施及び評価結果まとめ

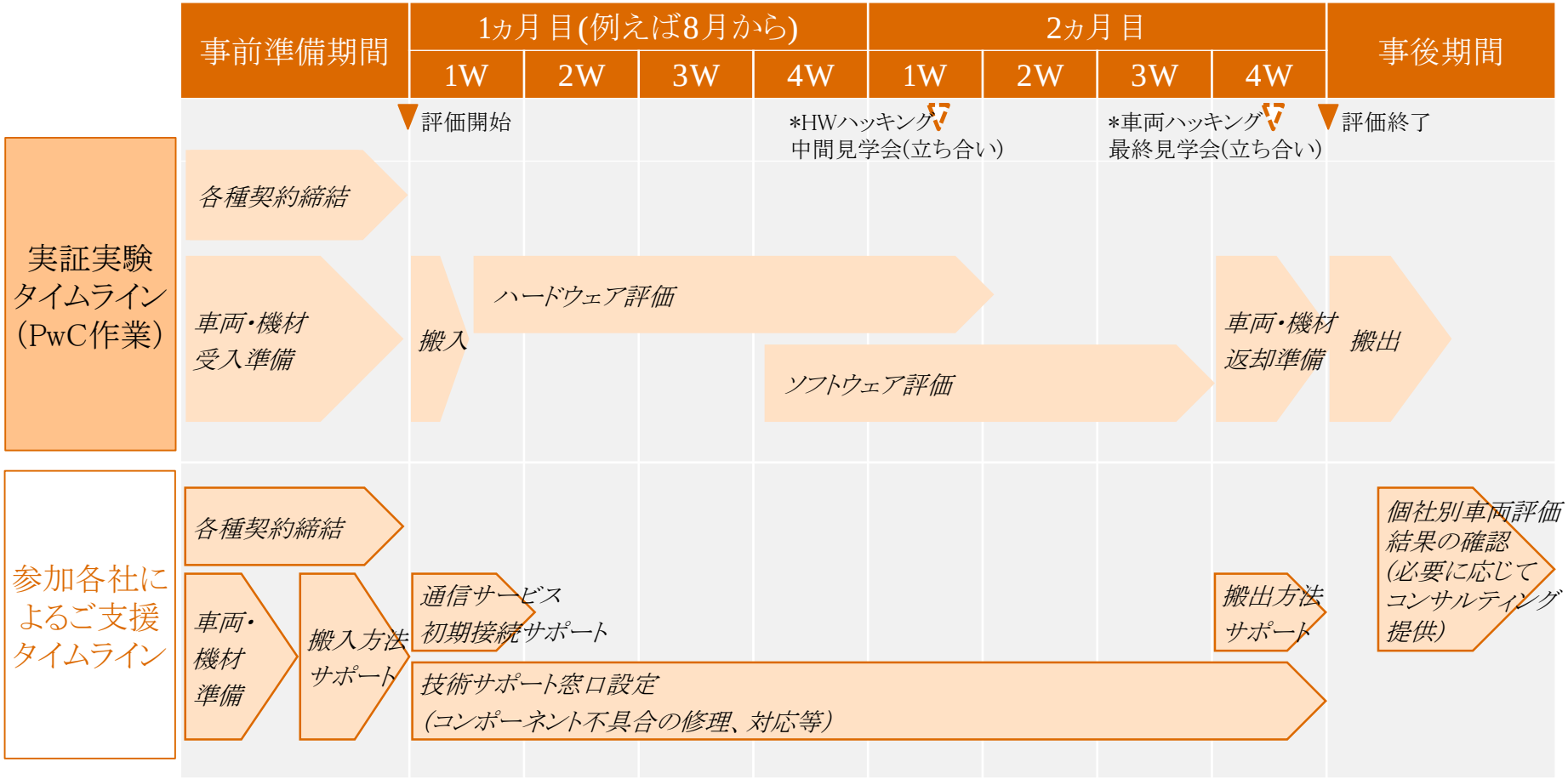
参加者確定後の実証実験準備から実施に関するフローは以下を想定しています。



＊参加者からの要望に応じて中間見学会(評価開始4-5週間後)、最終見学会(評価終了時)を実施いたします。

参加OEM各社にご支援頂く内容・タイムライン

実証実験に係る契約類締結後（18年8月頃～）より、実証実験のタイムラインに沿って、参加各社に必要なご支援・ご協力を頂きます。



＊中間、最終見学会(立ち合い)は予定しておりませんが、ご要望がある場合は、確認いただく内容や実施場所を各参加者と事前に調整し実施することも可能です。

参加OEM各社にご準備いただく品目(1/2)

実証実験期間(4カ月間を予定)において、以下の品目の提供をお願いいたします。

No.	品名	個数	必要条件・詳細	必須
1	実験車両* (商用車、開発車両も可)	1台	• 実験車両からテレマティクスサービスに接続可能な状態であること (検証用のテレマティクスサービスでも可) 【備考】車両は通信コンポーネントを使用した実証実験評価結果の中で、特に重要な内容に関する実車テストに使用します。	○
2	情報系ECU	3セット	• テレマティクスサービスに接続可能なもの (検証用のテレマティクスサービスでも可) • TCU、AVN等通信コンポーネントを含む • 携帯電話回線、Wi-Fi、BT等の機能を持つ通信コンポーネント含む	○
3	GatewayECU		• 情報系ECUと直接接続されるもの	○
4	通信アンテナ	1セット	• GPS、携帯電話回線等	○
5	車内インターフェース		• 一般ユーザが車内で利用するインターフェイス • (ディスプレイ、マイク、USBポート、タッチパッド等)	○
6	情報系ワイヤーハーネス		• 各終端にコネクタが付属したもの。加工していない状態でも可	○
7	各ECU毎の コネクタPIN構成	1セット	• どのPINが電源で何V必要なのか判別できるもの	○
8	配線図	1セット	• 各情報系ECUおよびGateWayECUを含むもの	○

*車両については、完成車が具備するWi-Fi、BT、テレマティクス等の無線通信を利用する機能が動作可能であれば車両ベンチ(必要部品を接続したシステム)を提供頂くことでも構いません。

参加OEM各社にご準備いただく品目(2/2)

実証実験期間(4カ月間を予定)において、以下の品目の提供をお願いいたします。

No.	品名	個数	必要条件・詳細	必須
9	テレマティクス サービスアカウント	4個 (車両+部品合計セット数分)	• 一般ユーザが利用可能なテレマティクスサービスが全て利用可能であること (検証用のテレマティクスサービスのアカウントでも可)	○
10	テレマティクス サービスサーバ	ー	• 上記アカウントで、ご提供いただいた実験車両または通信コンポーネントから接続可能なサーバをご用意いただき、実証実験期間中に稼働していただく 【備考】 • 当該サーバは検証環境/本番環境を問いませんが、以下を実施します: 1.一般ユーザが利用可能なサービスの利用 2.外部から参照可能なサーバ情報の調査 (ホスト名、証明書、利用ポート番号等) • その他、テレマティクスサービスに影響を与える可能性のある行為は実施しない	○
11	各種マニュアル	各1部	• 車両マニュアル、サービスマニュアル等の一般入手可能なマニュアル類一式	

参加OEM各社にご支援（サポート）頂く内容

No.	タイミング	項目	期間	内容
1	実証実験 評価開始前 (7月末までを想定)	各種契約類締結* • 実証実験に係る契約(動産借用契約) – 車両・通信コンポーネントに対するハッキング実施承諾含む** • 秘密保持契約(NDA) • 通信サービス関連契約類、等	–	• 契約締結に向けた準備、社内調整等ご対応
2		実証実験提供物の条件調整	–	• 提供する品目（車両・機材）や搬入方法、通信サービス環境に係る条件調整等
3		車両・機材準備	–	• 実証実験に必要な条件を満たす車両・機材のご準備、送付手配等
4	実証実験 評価開始時	車両・機材搬入方法サポート	–	• 機材搬入に係る、移動、設置方法等のご教示
5		通信サービス初期接続サポート	1週間	• 通信サービス等への接続サポート
6	実証実験 評価実施中	技術サポート窓口設定	2カ月 程度	• コンポーネントの初期不良や、実証実験による分解等に係らない不具合の修理や問い合わせご対応等
7	実証実験 評価終了時	車両・機材搬出方法サポート	–	• 機材搬入に係る、撤収、移動方法等のご教示
8		個社別車両評価レポートの確認・フィードバック	–	• 個社別車両評価レポートのご確認と弊社へのフィードバック（任意）

＊ 契約の形態や契約内容の詳細については5月以降に調整させていただければと考えております。
また、各社様のひな型の活用等ご要望の際にはご相談ください。
** ハッキング実施承諾は参加規約等に含む場合もあります。

実証実験で取り扱う機密情報と開示範囲

実証実験の実施にあたりOEM各社からご提供をお願いする情報・機材、および、PwCよりご提示する機密情報に関して、開示範囲を以下の通り制限いたします。

カテゴリ	項目	内容	作成・提供者	開示範囲		
				評価車両の提供者	NEDO	制約なし（公知化）
評価対象	1. 評価対象車両/部品	評価を行う対象の車両および車両部品	OEM各社	○（PwC）	✖	✖
評価手順	2. 車両毎の評価手順	車両毎にシステムが異なるため、必要に応じて個別に評価手順を作成・まとめ共有する	PwC	○	✖	✖
	3. 評価ガイドライン（最終版）	実証実験の結果を反映した評価ガイドライン	PwC	○	○	○
評価結果	4. 車両評価報告書（個別）	車両評価の結果をまとめた報告書 -使用技術、機材を含む実施内容 -評価結果 （脆弱性情報を含むため機密度高）	PwC	○	✖	✖
	5. 統計化した車両評価結果	公開できるように加工した実証実験結果（統計化など）	PwC	○	○	○