

「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

平成30年度 成果概要説明書

PwCコンサルティング合同会社

平成31年2月28日

実証実験の取り組み概要

「情報セキュリティ」実証実験を通じて、自動車メーカー、サプライヤで広く活用できる、車両セキュリティ評価ガイドラインの策定を進めた

自動走行システムを取り巻く環境

- 自動走行システムの基盤となる様々な情報は、主に外部ネットワークから取得されることが想定されている。
(e.g. 高度な地図データや地図上にマッピングされる自動車、人、インフラ設備等の情報等)
- こうして得た情報が自動走行システムにおける車両制御に活用されることで、従来の自動車にはなかったサイバーセキュリティ問題を引き起こす要因にもなっている。

「情報セキュリティ」実証実験の目的と取り組み概要

自動走行におけるセキュリティ脅威の調査/分析を行い、国際標準化も見据えて、車両・コンポーネントレベルでのセキュリティ評価手法・プロトコル(評価ガイドライン)を策定し、本実証実験参加者の実車両システムを用いて対ハッキング性能検証のためのブラックボックステストによる技術調査を行うことで以下を実現する:

1. 車両への通信を用いた攻撃に対する評価手法の確立
2. V2X等車外からの攻撃を含む脅威の全体像の整理
3. 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
4. 日本における自動走行車両セキュリティに関わる人材育成及びノウハウ蓄積

実証実験の全体計画と今年度計画

H30年度は、H29年度に策定した評価ガイドライン(ドラフト版)を用いて、複数の車両システムに対するブラックボックステストを行い、その結果を反映することで評価ガイドラインを最終化する

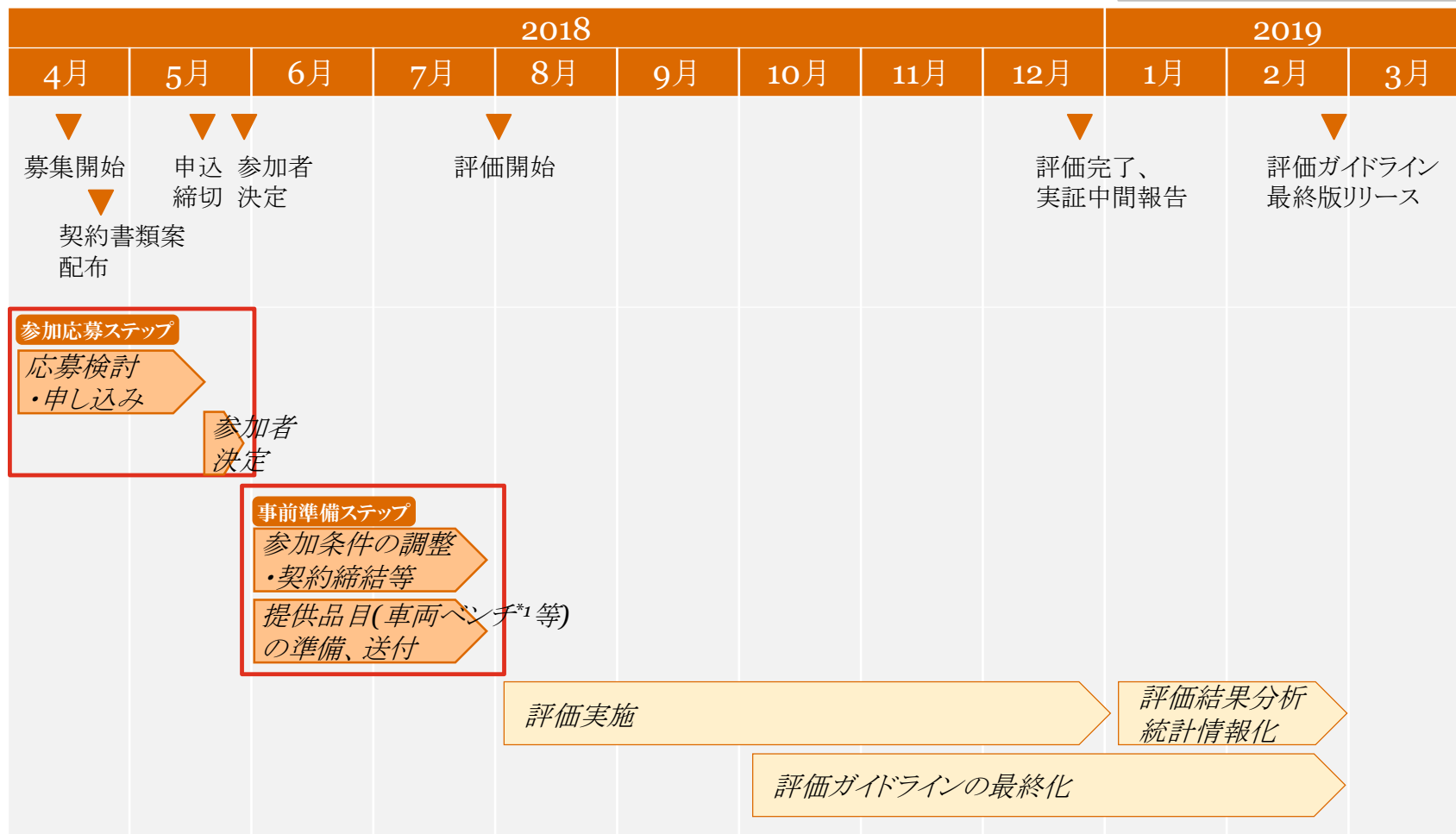
事業フェーズ	実施項目	実施内容	期間
H29年度 実証前調査 (Step1)	自動走行システムにおけるセキュリティ脅威の分析	<ul style="list-style-type: none"> 車両とインフラを含む自動走行システムに対するセキュリティ脅威の全体像を調査・分析・整理 	H29年9月 ～ H30年2月
	情報セキュリティ評価ガイドラインドラフト版の作成	<ul style="list-style-type: none"> 既知のインシデント・脆弱性やセキュリティ評価手法の整理に基づき、ガイドラインのドラフト初版を作成 ガイドラインのドラフト初版を用いた、セキュリティ評価の試行調査を実施 	
	情報セキュリティ評価の試行調査	<ul style="list-style-type: none"> 実施結果を踏まえ、評価ガイドライン(ドラフト版)を完成 	
H30年度 実証実験 (Step2)	実証実験事務局の運営	<ul style="list-style-type: none"> 国内OEMを対象に、実証実験への参加を募集 参加各社との、セキュリティ評価の対象(車両システム)、評価場所、評価時期等の調整 	H30年4月 ～ H30年7月
	情報セキュリティ評価の実施	<ul style="list-style-type: none"> 参加各社から提供を受ける車両システムに対し、STEP 1で策定した評価ガイドライン(ドラフト)を用いてセキュリティ評価を実施 	H30年8月 ～ H31年2月
	情報セキュリティ評価ガイドラインの最終化	<ul style="list-style-type: none"> 評価結果の分析を通じて改善点を明確化し、反映することで評価ガイドラインを最終化 	

実証実験スケジュール(計画時)

凡例

参加者

PwC



*1 車両ベンチ: 台上で検証することを想定し、駆動部品を持たず、Wi-Fi、BT、Cellular等の無線通信が動作可能な機器で構成されたコンポーネント

実証実験参加応募ステップ

実証実験への参加応募に向けて、以下のステップで活動した

	申し込み検討					申し込み
	採択結果 掲載	参加依頼 受領	説明会 参加	参加検討	参加契約 書類案 受領	参加 申し込み
	4/16(月)	4/17(火)	4/17(火)～申し込み期限(5/23)まで		4/26(木)	～5/23(水)
参加者 (OEM)	-	<ul style="list-style-type: none"> 参加依頼の受領・確認 内容に関する説明会への参加要否検討 	<ul style="list-style-type: none"> 説明会参加(希望者のみ) 	<ul style="list-style-type: none"> 本説明資料の内容を確認し、社内で検討 不明点を問い合わせ 	<ul style="list-style-type: none"> 契約書類案受領 	<ul style="list-style-type: none"> 参加申込書の提出
受託者 (PwC)	-	<ul style="list-style-type: none"> 候補各社への参加依頼連絡 関連資料の送付 	<ul style="list-style-type: none"> 説明会開催(依頼のあった各社向けに個別説明会を開催) 	<ul style="list-style-type: none"> 問い合わせ受付・回答 	<ul style="list-style-type: none"> 契約書類案の送付 	<ul style="list-style-type: none"> 申し込み受付 受付結果を事務局へ連絡
事務局 (NEDO)	<ul style="list-style-type: none"> 本事業の採択結果をHPに掲載 	-	<ul style="list-style-type: none"> 説明会実施実績受領 	<ul style="list-style-type: none"> 問い合わせ受付・回答 	-	<ul style="list-style-type: none"> 申し込み結果受領

実証実験事前準備ステップ

参加者決定後は、以下のステップで評価実施に向けてご準備頂いた
各社の評価実施時期は、提供頂く品目や準備状況に応じて調整・決定された

	参加者決定		実証実験準備			
	参加者決定	参加決定通知受領	参加条件調整	契約類締結	車両・機材提供準備	評価実施
	5/23(水)~5月末	5月末	~7月末			8月初~*
参加者 (OEM)	-	<ul style="list-style-type: none"> 参加者決定結果の受領 	<ul style="list-style-type: none"> 提供品目の調整、詳細情報を受託者に連絡 	<ul style="list-style-type: none"> 各契約書類の締結に向けた社内調整 契約締結 	<ul style="list-style-type: none"> 提供品目の準備・送付手配 提供品目の搬入・設置に関する詳細情報の提供 	<ul style="list-style-type: none"> 技術サポート窓口(担当者)の設定
受託者 (PwC)	-	<ul style="list-style-type: none"> 参加者決定結果の把握 	<ul style="list-style-type: none"> 各社の評価実施時期・環境の調整、決定 	<ul style="list-style-type: none"> 契約内容の参加者との調整 	<ul style="list-style-type: none"> 評価実施環境の準備 	<ul style="list-style-type: none"> 品目の受け入れ 評価実施
事務局 (NEDO)	<ul style="list-style-type: none"> 参加者の決定 	<ul style="list-style-type: none"> 参加者決定結果の通知 	<ul style="list-style-type: none"> 進捗状況の把握 必要に応じて参加者・受託者間の調整を支援 			

* 8月から評価を開始する場合の一例。8~1月の間で各社提供機材に対し、2カ月程度の期間で評価を実施。

実証実験に係る契約書類

実証実験開始に向け、参加者・PwCの2社間で協議の上、以下の契約書類を締結した

① 実証実験参加基本合意書

実証実験の内容や、参加にあたっての大枠の合意事項を定める合意書

② 動産使用貸借契約書

実証実験に提供する品目及びその使用に関する詳細(使用方法、品目リスト、使用期間 等含む)を定める契約

③ 秘密保持契約書(NDA)

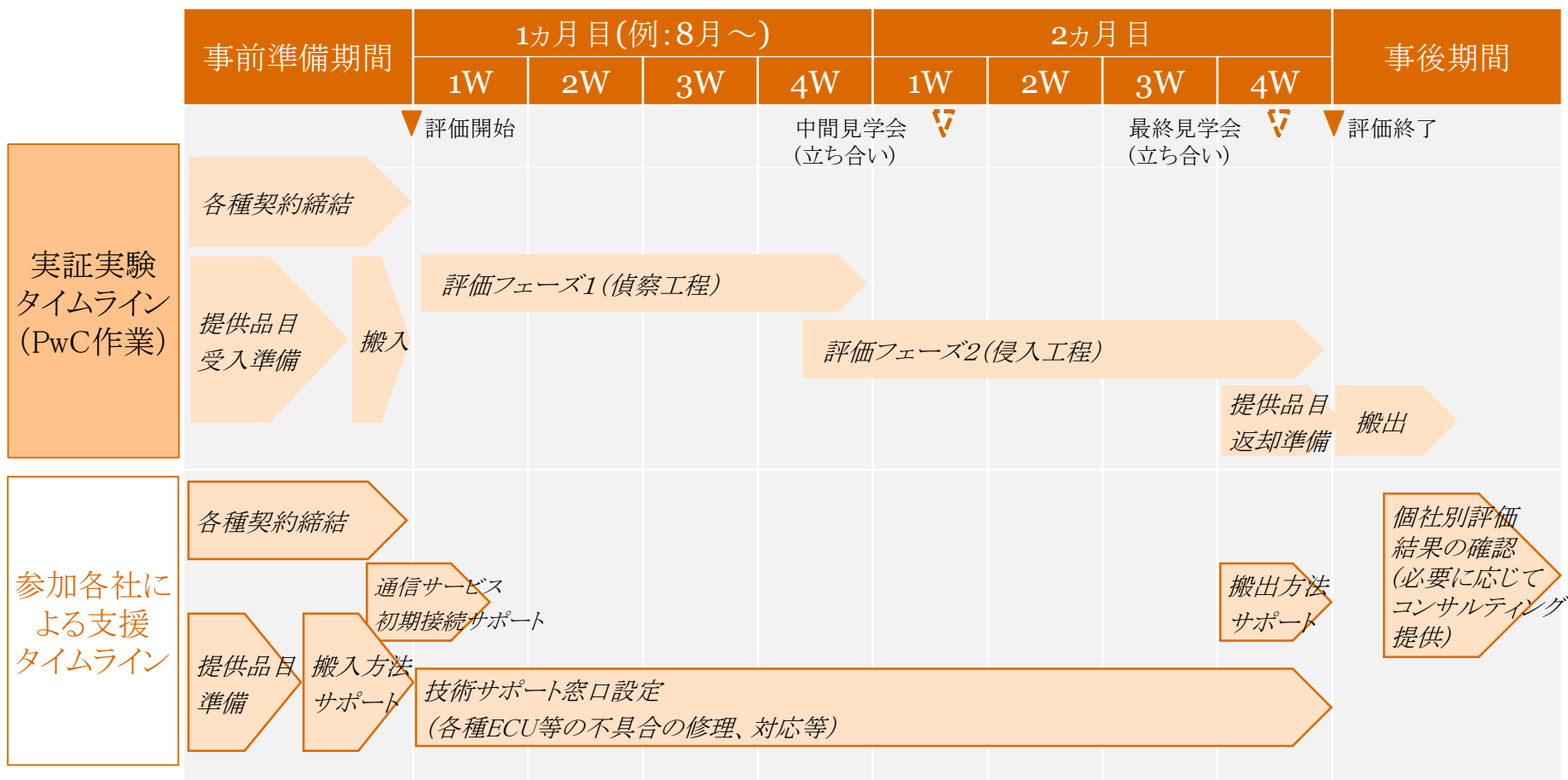
実証実験を通じて得た秘密情報の取り扱い、開示範囲等の詳細を定める契約

④ その他の契約

通信サービス利用契約や、参加各社の要望に応じた追加契約 等




参加各社による支援内容・タイムライン

実証実験に係る契約類締結後、実証実験のタイムラインに沿って、参加各社から必要な支援・協力を得た



参加各社から提供を受ける品目(1/2)

実証実験期間において、以下品目の提供を依頼した

No.	必須	品名	個数	必要条件	詳細条件
1	○	車両ベンチ*1	1台	<ul style="list-style-type: none"> 情報系ECUとGatewayECU*2が通信可能な状態で接続された構成であること 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) 一般ユーザが車内で利用するインターフェイスが付与されているもの (ディスプレイ、マイク、USBポート、タッチパッド等) GPS、Cellular等の通信アンテナが付与されているもの 	完成車が具備するWi-Fi、BT、Cellular等の無線通信を利用する機能が動作可能な状態で提供頂きます。テレマティクスサービスは必須ではございませんが多くのテストケースで必要となります。
2	○	情報系ECU	3セット	<ul style="list-style-type: none"> 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 Wi-Fi、BT、Cellular等の機能を持つ通信コンポーネント含む 	Wi-Fi、BT、Cellular等の機能を持つ通信コンポーネントが別ECU (TCU、DCM等)に存在していれば、そのECUも対象となります。
3	○	GatewayECU		<p>接続形態に応じたGatewayの提供(赤枠)</p> <p>例1: セントラルGatewayが存在する場合</p>  <pre> graph LR TCU[TCU] --- GW[GW] AVN[AVN] --- GW Control[制御系] --- GW style GW stroke:#f00,stroke-width:2px </pre> <p>例2: 複数GWが存在する場合</p>  <pre> graph LR TCU[TCU] --- AVN[AVN] AVN --- GW1[GW] GW1 --- GW2[GW] GW2 --- Power[Power系] Body[Body系] --- GW1 style GW1 stroke:#f00,stroke-width:2px style GW2 stroke:#f00,stroke-width:2px </pre> <p>例3: 情報系と制御系が直結している場合</p>  <pre> graph LR TCU[TCU] --- AVN[AVN] AVN --- Control[制御系] style AVN stroke:#f00,stroke-width:2px style Control stroke:#f00,stroke-width:2px </pre>	<p>本評価ガイドラインは制御系への任意の攻撃が可能となるポイントとしてGatewayのファームウェア改ざんを最終到達点としており、GatewayECUの提供をお願いしております(例1のケース)</p> <p>例2、3の接続形態の場合は、提供機材および評価方法について協議します</p>

*1 開発中の車両システムの場合は、より適切な評価結果を得るため、開発時のみに適用される仕様・設定等がある場合は、その内容および商用化時に想定される仕様・設定について情報提供することが望ましい。

*2 GatewayECUについては、No.3で記載の条件を考慮。

参加各社から提供を受ける品目(2/2)

No.	必須	品名	個数	必要条件	詳細条件
4		テレマティクスサービスアカウント	4個 (最低限2個)	<ul style="list-style-type: none"> 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) 	情報系ECUとアカウントが紐付いていることを想定して4個(車両ベンチ+部品3セット)用意いただきます。アカウントとECUが紐付かず自由に変更可能な場合であっても、複数アカウントからテレマティクスサービスを利用するテストを予定しているため、最低限2個ご提供いただきます。
5		テレマティクスサービスサーバ	—	<ul style="list-style-type: none"> 上記アカウントで、ご提供いただいた車両ベンチ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 	<p>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:</p> <ol style="list-style-type: none"> 一般ユーザが利用可能なサービスの利用 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) <p>上記2点を実施可能なサーバをご用意ください。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ません。</p>
6		検証用スマートフォンアプリ	1個	<ul style="list-style-type: none"> 検証用テレマティクスサービスにアクセス可能なスマートフォンアプリ(Android) 	「偵察(情報収集)」工程の一つとしてスマートフォンアプリからの通信傍受を行います。検証用サーバへ接続するアプリケーションは通常GooglePlayに公開されていないため、参加者様からバイナリファイルをご提供いただきます。iPhoneはJailbreakが必要で利用できるOSバージョンに制限があるため、Androidアプリをご提供いただきます。
7		各種マニュアル	各1部	<ul style="list-style-type: none"> 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 	
8	○	配線図	1セット	<ul style="list-style-type: none"> 情報系ECUおよびGatewayECUの各コネクタごとにどのPINが電源で何V必要なか判別できるもの 	ECU単体で電源を投入して評価する可能性があるため、電源コネクタの位置を予め把握しておく必要があるため、ご提供いただきます。

参加各社から支援(サポート)を受ける内容

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 <ul style="list-style-type: none"> • 実証実験基本合意書 <ul style="list-style-type: none"> - 提供品目に対するハッキング実施への承諾を含む • 動産使用貸借契約 • 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、社内調整等対応
2		実証実験提供品目の条件調整	-	• 提供する品目や搬入方法、通信サービス環境に係る条件調整等
3		提供品目の準備	-	• 実証実験に必要な条件を満たす評価対象品目の準備、送付手配等
4	実証実験 評価開始時	提供品目搬入方法サポート	-	• 各品目の搬入に係る、移動、設置方法等の連絡
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	• 提供品目の初期不良や、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対応等
7	実証実験 評価終了時	提供品目搬出方法サポート	-	• 各品目の搬出に係る、撤収、移動方法等の連絡
8		個社別評価レポートの確認・フィードバック	-	• 個社別評価レポートの確認と内容に関するフィードバック提供(任意)

施行区分および費用負担[役割分担]

実証実験に用いる品目は参加各社に費用負担・手配頂いた
その他詳細な費用負担については下表のとおり

No.	施行区分	想定される費用	費用負担区分	
			PwC	参加者
1	評価対象品目の提供 (車両ベンチ・各種ECU等)	車両ベンチ・各種ECU等の 貸与、輸送、設置等に係る費用	-	○
2	通信・テレマティクスサービスの提供	サーバの稼働、検証環境の用意に係る費用	-	○
3	評価実施用機材の準備	実証実験におけるセキュリティ評価実施のための 専門機材、ソフトウェア、PC等の購入・使用費	○	-
4	技術サポート窓口の設置	動作確認、初期不良等への対応に係る費用	-	○
5	実証実験環境(場所)の管理	実証環境の確保、安全管理、情報管理(セキュリ ティ)の実装に係る費用	○	-
6	実証実験中の資産管理	実証実験用に貸与された車両ベンチ・各種ECU 等の保守・管理に係る費用	○	-
7	実証実験見学会の実施	ご要望があり、実施する場合のHWハッキングの 見学会(立ち合い)に開催に係る費用	○	-
8	個社別評価レポートの作成	個社別の実証実験結果のレポート作成、説明	○	-
9	評価ガイドラインの策定	実証実験結果を反映した評価ガイドラインの策定	○	-

見学会/実証実験評価作業立ち合い(ご要望に応じて実施)

実証実験の中間進捗、最終結果について、要望に応じて実機を使用したデモンストレーションを実施した

見学会	時期	場所	内容例
中間見学会 (立ち合い)	実証実験 評価開始 4-5週間後	東京都大手町 (PwCオフィス)	<ul style="list-style-type: none"> • 個社別評価中間結果(進捗)報告 • 実機を使用したHWハッキングのデモンストレーションへの立ち合い
最終見学会 (立ち合い)	実証実験 評価終了前	東京都大手町 (PwCオフィス)	<ul style="list-style-type: none"> • 個社別評価レポート報告 • 実機を使用したHWハッキングのデモンストレーションへの立ち合い • セキュリティ対応等に関する簡易コンサルティング実施(評価結果により、必要に応じて)

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参加各社へ提供を依頼する情報・機材、および、PwCより提示する機密情報に関して、開示範囲を以下の通り制限した



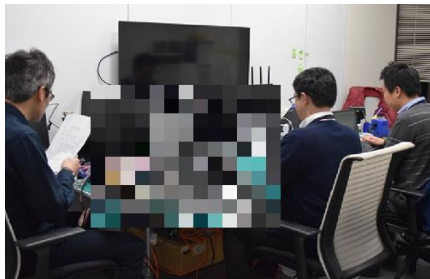
カテゴリ	項目	内容	作成・提供者	開示範囲			
				評価車両システムの提供者	OEM全体	NEDOを含むSIP-adus関係者(守秘義務あり)	制約なし(公知化)
プロジェクト進捗	1. 参加者募集状況*1	参加者募集に対する応募状況	PwC	○	✖	○	✖
	2. 個社名を匿名化した評価進捗報告	個社名を匿名化した評価実施状況	PwC	○	✖	○	✖
評価対象	3. 評価対象車両システム/部品	評価を行う対象の車両システムおよび車両部品	OEM各社	○ (PwC)	✖	✖	✖
評価手順	4. 参加社毎の評価手順	車両毎にシステムが異なるため、必要に応じて個別に評価手順を作成・まとめ共有する	PwC	○	✖	✖	✖
	5. 書類フォーマット	評価レポート等、評価車両システムを提供予定のOEMに提出、受領する書類フォーマット	PwC	○	○	✖	✖
	6. 評価ガイドライン(公開版)	実証実験の結果を反映した評価ガイドラインの公開版	PwC	○	○	○	○
評価結果	7. 評価報告書(個別)	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	○	✖	✖	✖
	8. 統計化した評価結果	公開できるように加工した実証実験結果(統計化など)	PwC	○	○	○	○

PwC

*1 参加者決定検討の必要から募集への応募情報はNEDO及びSIP関連会議体で共有される。ただし、個社名は一般公開されない。

実証実験環境 - 車両ベンチ・各種ECU 評価実施場所

実証実験は、参加各社との議論の結果を踏まえ、車両ベンチの提供を受け、PwCのHWハッキングラボにて評価を実施した

項目	PwC HWハッキングラボ
概要	<p>PwCオフィス内に設置した車両システムなど、IoT製品、組み込み機器の検査に特化した研究施設</p>   
場所	東京都千代田区大手町1-1-3 大手センタービル19F
セキュリティ	十分なセキュリティを備えている ※詳細は次頁
設備	HWハッキング機材(実証前試行実験で使用した機材一式)
収容台数	車両ベンチ4台
搬入	高さ200cm x 幅98cm以内の機材であれば搬入可

実証実験環境 - 車両ベンチ・各種ECU 評価実施場所のセキュリティ

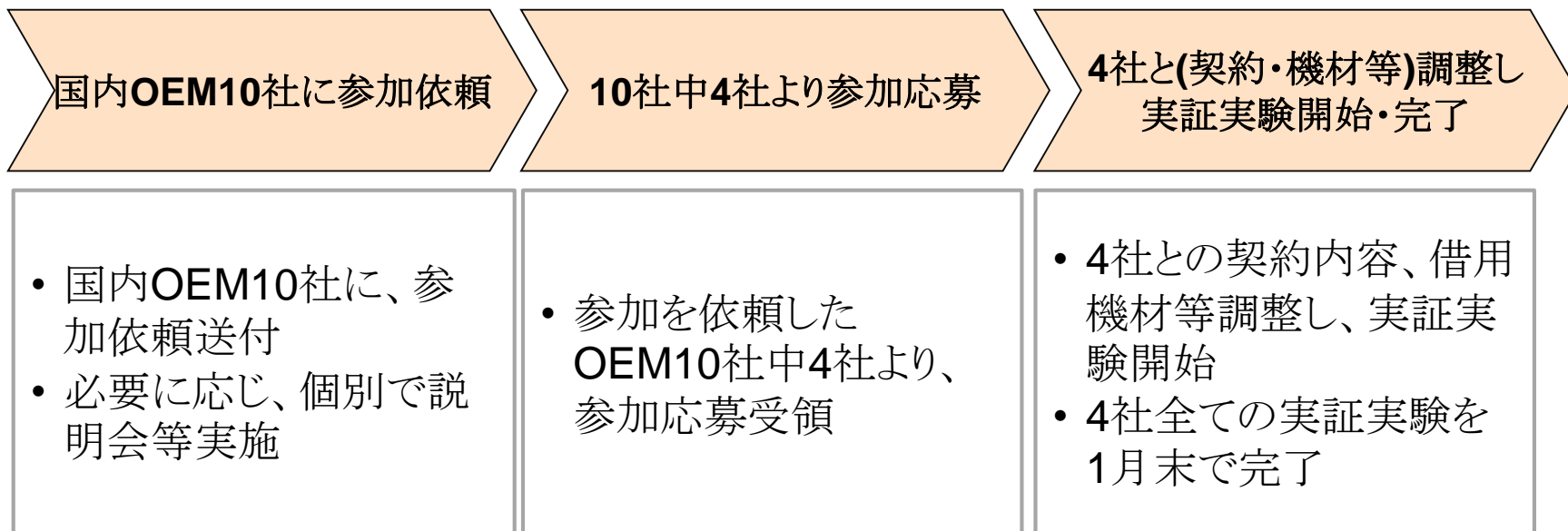
評価施設は以下のとおり本件を遂行する上で十分なセキュリティを備えている

セキュリティ設備	PwC HWハッキングラボ
入館チェック	警備員によるIDカード携帯チェック
	弊社標準のセキュリティ区画に応じた2重のID認証ドア
認証装置	ID認証ドア(評価担当者のみ入室可)
	指紋認証(評価担当者のみ入室可)
入退室記録	全ての入退室記録を管理
監視	監視カメラによる録画 直近3カ月の映像データは、ビデオレコーダにて録画し保存

国内OEMとの実証実験によるガイドライン検証

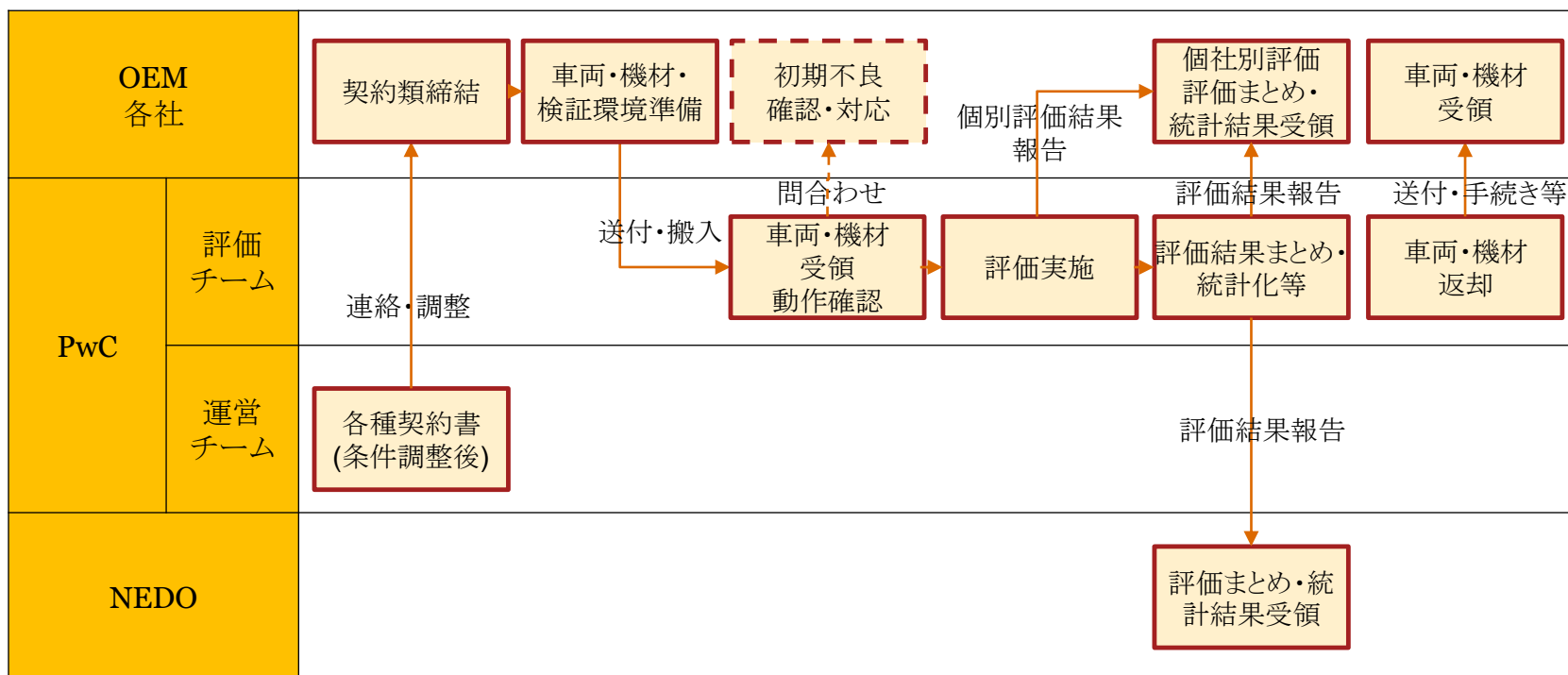
平成30年度は、**国内OEM4社の参加**を募り、提供を受けた機材を用いて実証実験を実施した

平成30年度実証実験参加社募集の流れ



評価実施のフロー

参加者確定後の実証実験準備から評価実施に関するフローは以下のとおり。
 実証実験として評価ガイドラインに従った侵入テストにより車両システムのセキュリティ性能評価を実施した。



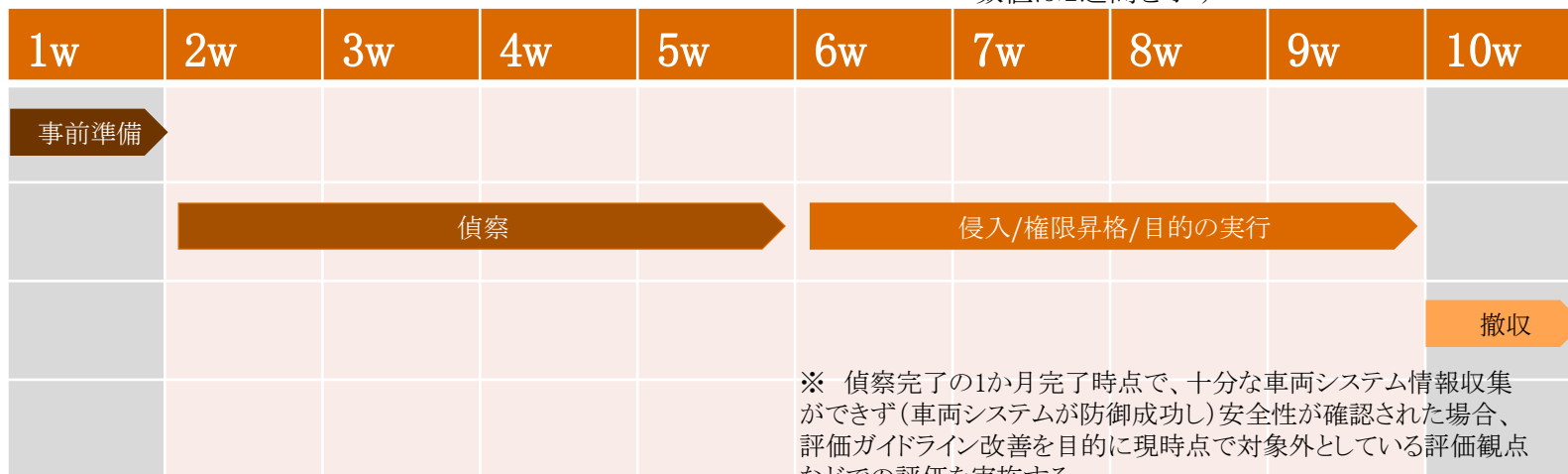
実証実験 評価実施概要

策定した評価ガイドラインに沿って評価(攻撃)を行い、車両システムの対サイバーセキュリティ防御性能を判定する

安全性判定は、ガイドラインに従った各工程の評価(攻撃)に対して一定期間(過去実績等から規定)での防御成否を元に行う

- ・「偵察」工程(主にHWハッキングによる攻撃のための情報収集)・・・4週間(1カ月)
 - ・本工程で防御成功(情報収集失敗)時は、後工程の攻撃ができないため安全性を判定できる。
- ・「侵入/権限昇格/目的の実行」工程・・・4週間(1カ月)

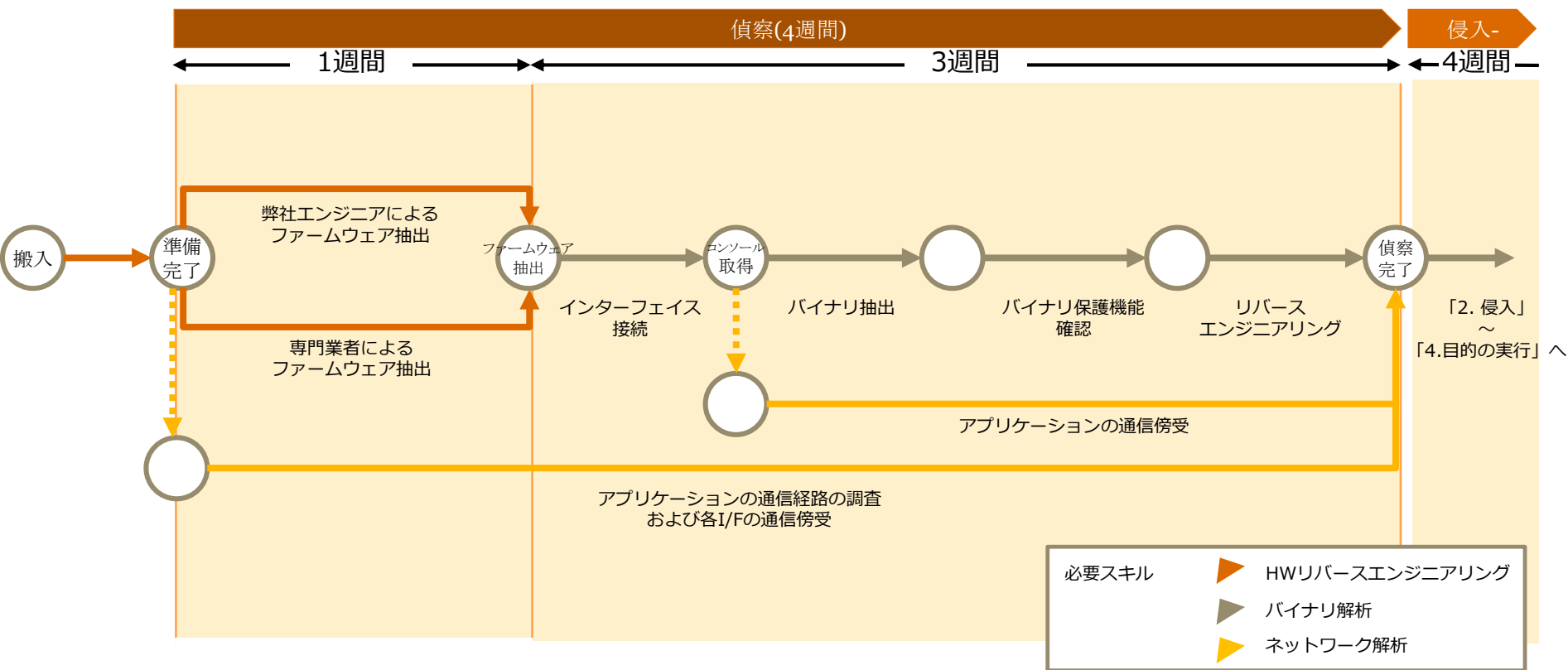
数値は1週間を示す



「偵察」の評価手法

車両システムへの侵入のための情報収集について評価を行う。

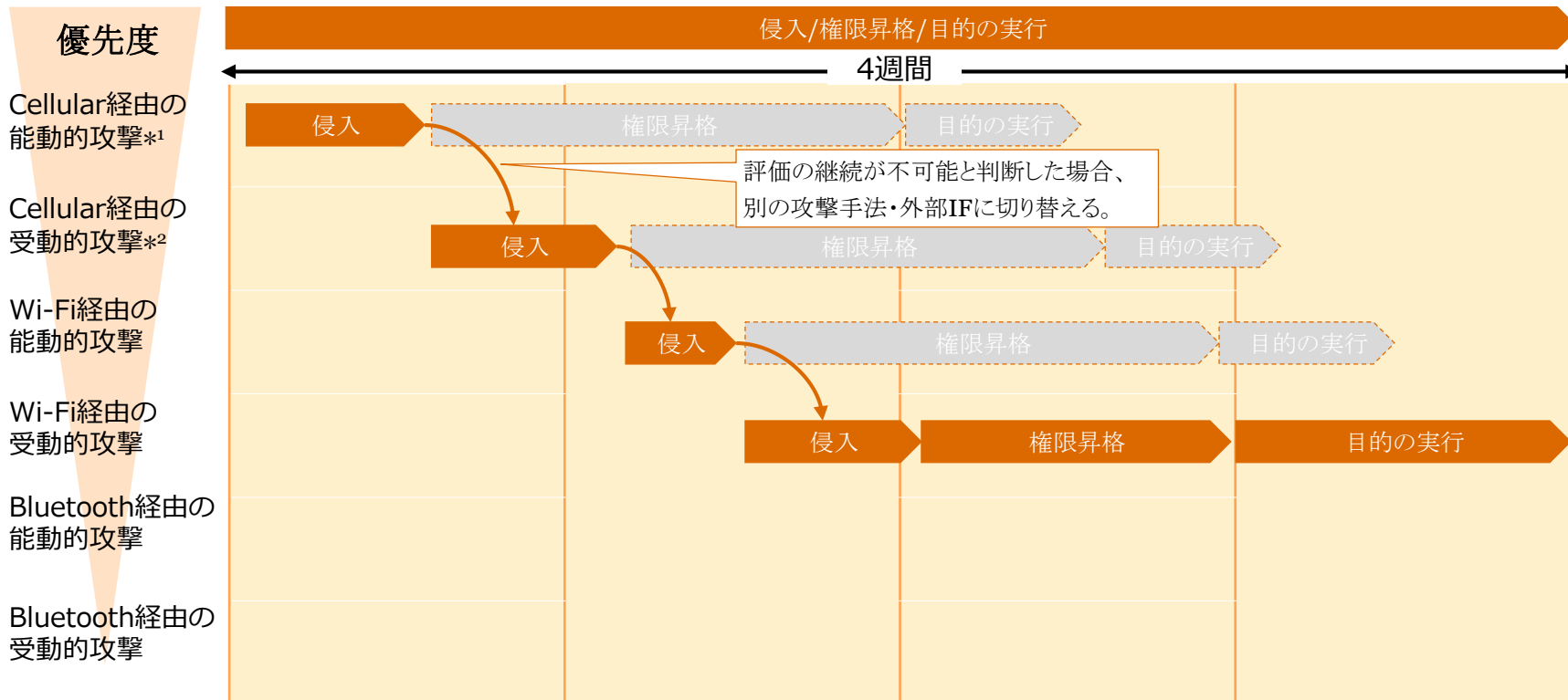
- 昨年度試行調査での結果を踏まえ、HWリバースエンジニアリング作業を初期に集約し、その一部を専門業者に依頼することで、4週間(1か月)で完遂できる工程とする。
- 4週間(1か月)を偵察の標準期間としますが、本実証実験を通じて本期間の妥当性についても検証する。



※1 隠れたインターフェイスの解析には非常に高度なHWリバースエンジニアリング技術と長期間(2か月以上)を要するため、公開文書レベルでのチップの耐タンパ性を評価する

「侵入」/「権限昇格」/「目的の実行」の評価手法

通信外部I/Fごとに、以下の図に記載の優先度に基づいて「侵入」から「目的の実行」まで深掘りする標準評価期間である1カ月の場合、すべての攻撃手法・通信外部I/Fに対する「侵入」を実施する
 なお、「権限昇格」「目的の実行」に関しては、車載システム侵入後の評価のため、いずれかの外部I/Fより「侵入」できたことをもって、別I/Fからの評価結果をみなし評価とする



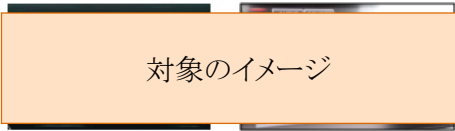
*1 能動的攻撃: 攻撃者の一方的な攻撃で成立する攻撃手法 (FCA Jeep Cherokeeのハッキング事例等)


*2 受動的攻撃: 搭乗者および車両オーナーの介入を必要とする攻撃手法 (Tesla Model Sのハッキング事例等)

実証実験による評価レポート(イメージ)

PwCホワイトハッカーチームが明らかにした、現実には発生し得る被害の内容と再現手順を報告した

また、これら実際の被害内容や攻撃条件・難易度を考慮した対策提案も併せて提供した

評価手順のイメージ		
評価ガイドライン項番	1.1.1	
作業員・知識レベル	PwC 太田尾 / 情報セキュリティ:A-1、車両セキュリティ:B-1	
総作業時間	0:30	
評価	○	
事前作業	項目	
	作業内容	ネットワーク設置情報および、ファームウェアのバージョン情報
	ツール・環境	Android Studio (Android SDK)
	作業結果	IP: 192.168.23.61 MAC: 34-E1-AD-67-68-E1 電話番号: 080-1234-5678 ISMI: 123121234567890 ファームウェアバージョン: 1.13-4b 
	作業時間	0:05
	評価	○
	作業内容	車載器の電源を遮断し、各車載器の背面パネル構成および
ツール・環境	Android Studio (Android SDK)	

評価レポートのイメージ	
評価ガイドライン項番	1.1.3
危険度	Middle
想定されるリスク	対象車両に物理的にアクセス可能な攻撃者がECUからファームウェアを抜き出すことが可能であるため、ファームウェアを解析することで、外部から対象車両を攻撃可能な脆弱性が発見される可能性がある。また、対象ECU内に貴社機密情報が含まれる場合、それら情報を抜き出される可能性もある。 ...
攻撃成立条件	対象車両のセキュリティ保護に関して、チップ取り外し後のデバックポートに関する防護機構が存在しないことを確認済み。
攻撃再現手順	攻撃者が対象車両に物理的にアクセス可能である。 手順1.対象ECUが搭載された基盤を車両より取り出す 手順2.取り出した基盤から対象ECUをとり剥がす(チップ剥し) (参考) 対象チップをとり剥がした際の様子 
改善の方向性	...
	デバックポートからのファームウェア抜き取りは、その後の攻撃可能を高めることから、以下のような対策実施を推奨します。 ... なお、デバックポート以外からのファームウェア抜き取りも理論上可能ですが、非常に高度な技術・施設が必要、かつ、これら対策はECUベンダーが実施する必要があります。そのため貴社においては、以下の確認の実施と、コンテンジェンシープランの策定を推奨します。 ...

評価におけるクライテリアの明確化

本評価の判定クライテリアと入力となる評価手法要素は以下のとおり
実証実験結果を通して各要素の妥当性を評価し、ガイドラインに反映する

評価条件	再現性のある評価実現方法	実証実験における検証方法	
1. 評価者のスキル	<ul style="list-style-type: none"> 必要となるスキルを明確化し、事前に評価者によるセルフチェックを実施 確認プロセスをガイドに取り込み 	個人ごとの「各評価項目の実施度」に基づきスキルチェックの妥当性をクロチェック評価	再現性を実現 アセスメントとして
2. ガイドライン評価項目による実施	<ul style="list-style-type: none"> ガイド記載の手順の明確化 	作業エビデンスおよび結果に基づき、各評価項目をどの程度ばらつき少なく実施できたかを評価	
3. 評価工数	<ul style="list-style-type: none"> 標準評価期間を計2ヵ月(40営業日)×2名とし、当該工数による評価を実施 	上記1, 2の共通性が実現できたことを前提に、評価出力で4社で判定基準が達成できたかどうか	
評価環境(車両)	<ul style="list-style-type: none"> 提示した要求条件の具体化 	実験環境(提供品目)の充足度に関する許容可能範囲の評価(各社毎の差異に基づき考察)	結果および課題、原因を考察・評価
評価結果	<p style="text-align: center;">評価結果</p>		
評価の判定基準	<p>【偵察フェーズ】 上記スキル・期間を充足する評価を実施した結果、偵察が成功せず、対象の安全性をその理由とともに確認することができた</p> <p>【侵入フェーズ】 上記スキル・期間を充足する評価を実施した結果、いずれのI/F経由でも侵入を成功することができなかった</p>		結果および課題、原因を考察・評価

実証実験結果報告／評価ガイド最終化

実証実験 実施

国内OEM4社の実際の車両システムを用いて、情報セキュリティ実証実験(セキュリティ・ペネトレーションテスト)を実施

成果

実証実験を通じた改善を経て、情報セキュリティ評価ガイドラインを最終化

※参加社個社の機密情報は匿名化(統計化)して開示

実証実験報告項目

- ① 実証実験実施を通じた評価ガイドライン妥当性検証結果
- ② 実証実験実施を通じた評価プロセス整理結果
- ③ 実証実験実施を通じた評価ガイドライン改善結果
- ④ 昨年度他社検討結果を参考にした改善結果

実証実験報告項目①： 実証実験実施を通じた評価ガイドライン妥当性検証結果

改善したガイドラインを用いて実証実験を運営し、実施結果を通じて評価ガイドラインの妥当性を評価し、必要な改善を実施 ※具体的な改善項目は次項以降

妥当性検証の取り組み

01

参加社

- 実証実験参加社が提供する対象システムの評価結果および評価内容報告を受けて、評価手法およびガイドラインに関する妥当性評価（アンケートを実施）

02

評価者/
自己点検 (PwC)

- 本年度実証実験の参加社(4社)の車両システムの確認およびガイドラインの適用結果を踏まえ、車両システムの実態に合わせた内容であることの確認、および、必要な項目の追加更新

03

関係組織

- 官民等の関係組織に対して、ガイドラインおよび情報セキュリティ評価の取り組みをご説明し、業界活用に向けた更新内容へフィードバック獲得

実証実験報告項目①: 参加社アンケート結果

実証実験参加社に対して、ガイドラインの活用・有効性に関してアンケートを実施したアンケート回答結果*の概要は以下のとおり

アンケート項目	回答概要
評価手法の確立 (評価ガイド策定)	<ul style="list-style-type: none">• 一定レベルのセキュリティ品質確保に寄与する手法• 属人性の高いペネトレーションテストの均質性向上に寄与する手法
車両システムを用いた実証実験	<ul style="list-style-type: none">• 評価ガイドの妥当性検証に寄与する活動• 複数車両を用いた検証が良い取り組み
今後の取り組み	<ul style="list-style-type: none">• 発見された問題への対策検討などは依然、評価者依存である点は改善の余地ある• V字後期の総合評価だけでなく、設計等前工程でも活用できるガイド化を望む

実証実験報告項目①: 評価者/自己点検(PwC)

弊社による自己点検結果は以下のとおり

点検項目

点検結果概要

評価実施プロセス

- 実証実験開始前に関係者との協議で評価プロセスを整理
- 評価プロセスの整理は、作業レベルの均一化に寄与した

評価者スキル

- 評価者スキルの設定により、評価作業(問題の発見)について均一化に貢献した
- 実証実験での評価者スキルの傾向からHWセキュリティ評価スキルを有する人材が少ないことが確認できた

評価期間

- 設定した2カ月間でガイドに記載の評価項目を実施することはできた
- 一方で、未知脆弱性を使った侵入については、投入時間とのトレードオフとなるため、偵察の結果を受けて投入時間を設定する取組も必要と思われる

評価項目

- 本実証実験では昨年度策定した評価ガイドラインドラフト版の評価項目をもって評価を実施した
- 本年度実証実験の実施時に、いくつかの確認項目不足が見つかり、項目追加した

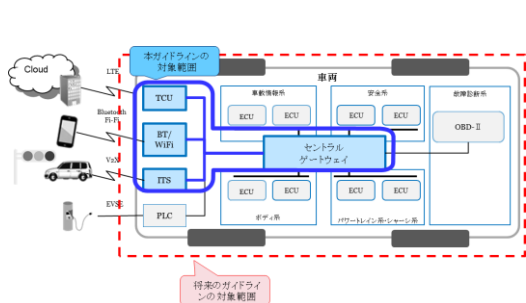
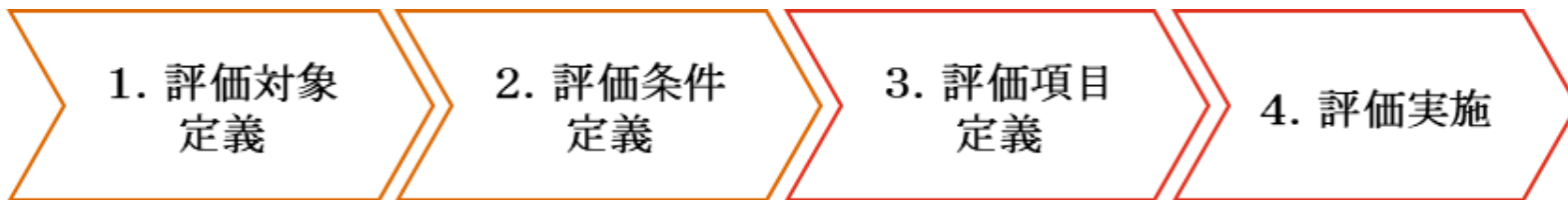
評価対象システム

- 本実証実験では、ご用意いただいた車両システム構成に差分があり、評価実施可能な項目に差が発生した
- 差分の有無を考慮したプロセス整備および必要品目の再整理を行った

実証実験報告項目②: 実証実験実施を通じた評価プロセスの整理結果

実証実験を通じて車両システムセキュリティ評価(ペネトレーションテスト)の標準的な評価プロセスを定め、アセスメントとして活用できる手法として確立

セキュリティ評価(ペネトレーションテスト)のプロセス



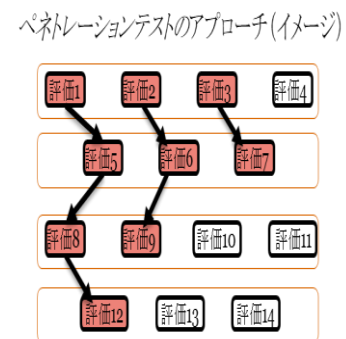
偵察スキル

カテゴリ	スキル内容
HWリバースエンジニアリング	MCU,ISP等HW基礎知識 UART/JTAG Pin Scanning技術 フラッシュメモリアダプ技術
バイナリ解析	リバースエンジニアリング ソースコード解析技術 ソフトウェア対策回避技術
ネットワーク解析	WiFi/Bluetooth解析 Bluetoothプロトコル解析 TCP/IPプロトコルスタック知識
管理	後続工程への情報提供



侵入スキル

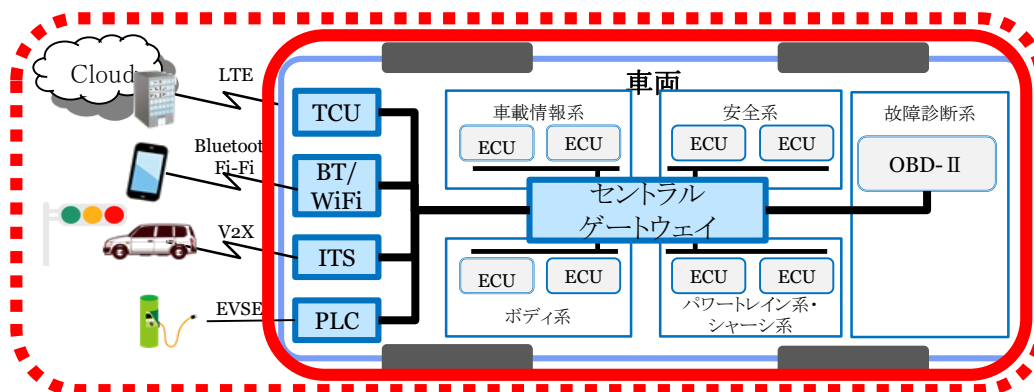
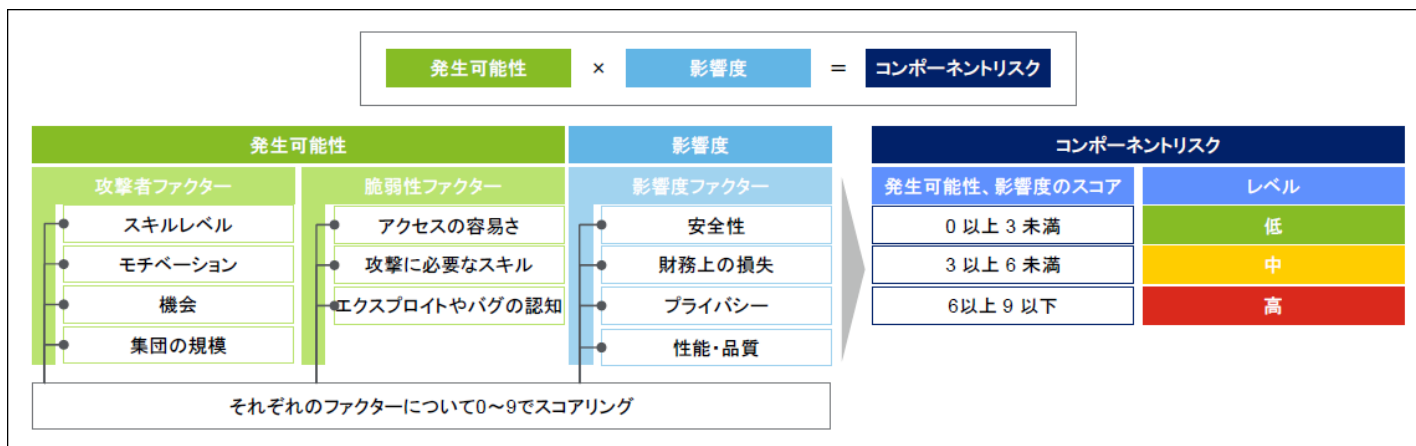
カテゴリ	スキル内容
侵入	リバースエンジニアリング 脆弱性特定・攻略 WiFi/Bluetooth/TCP/IPプロトコル解析
権限昇格	メモリセキュリティ(DEP,ASLR)および回避技術 MAC(強制アクセス制御)および回避技術 改ざん検知技術(セキュアブート等)および回避技術
目的の実行	CANプロトコル知識 DoSツール運用技術 HW構成の理解



評価対象定義：リスク分析を元にした対象選定

車両システムセキュリティ評価（ペネトレーションテスト） 第1手順

車両システム全体および周辺システムを対象にリスク分析を実施し、リスクの高い攻撃I/Fおよびコンポーネントを選別し、本手法による評価対象として選定・定義する



評価条件定義：評価の実施方法等条件の明確化

車両システムセキュリティ評価（ペネトレーションテスト） 第2手順

セキュリティ評価を再現性のあるものとするため、評価における各種条件とそのクリテリアを明確化・定義する ※下記はP20で定めた本実証実験における具体的なクリテリア

評価条件	具体的な条件内容
評価者のスキル	<ul style="list-style-type: none">評価に必要となるスキルを明確化し、事前に評価者・管理者によるチェックを実施
評価工数	<ul style="list-style-type: none">（本実証実験では） 標準評価期間を計2ヵ月(40営業日)×2名とし、当該工数による評価を実施
評価環境(車両)	<ul style="list-style-type: none">実際に用意できた機材を踏まえた、可能な評価環境を確認
評価結果	
評価の判定基準	<p>【偵察フェーズ】 上記スキル・期間を充足する評価を実施した結果、偵察が成功せず、対象の安全性をその理由とともに確認することができた</p> <p>【侵入フェーズ】 上記スキル・期間を充足する評価を実施した結果、いずれのI/F経由でも侵入を成功することができなかった</p>

工程毎の「評価者のスキル」の概要 (1/2)



偵察スキル

カテゴリ	スキル内容	概要
H/W解析	表面解析	ハードウェアの知識に基づいてプリント基板構成を分析しデバックポートや外部通信ポートを探索、特定する
	加工処理	プリント基板にはんだ付けされたフラッシュメモリ等の剥離、再度はんだ付けを行う他、必要に応じてプリント基板に加工処理を施す
	データ入出力ポートからのバイナリ抽出	各種ツール等を用いてプリント基板から剥離したフラッシュメモリ、外部通信ポートからデータの抽出および書込みを行う
	デバッグポートからのバイナリ抽出	上記特定したデバッグポートからデータを抽出する
バイナリ解析	ファイルシステム解析	フラッシュメモリから抽出されたデータを解析し、ファイルシステム等のデータ構造を分析、把握する
	ソフトウェアアーキテクチャ解析	ファイルシステム上から抽出されたファイル群を解析し、OS、ライブラリ等のソフトウェアアーキテクチャを分析、把握する
	バイナリコード解析	特定されたプログラムファイル等の各ファイルを分析し、その設計・実装を分析、把握する
	ソースコード解析	各種ツールによりバイナリコードの逆コンパイルを行い、ソースコードレベルでの設計・実装を分析、把握する
	保護機能の回避	データの暗号化、難読化、エンコード等のソフトウェア的に実装された保護機能を分析、回避する
ネットワーク解析	WiFi通信解析	WiFi通信の傍受、解析を行う
	BlueTooth/BlueTooth LE通信解析	BlueToothおよびBlueTooth LE通信の傍受、解析を行う
	セルラー通信解析	セルラー通信の傍受、解析を行う
	TCP/IP通信解析	TCP/IP通信の傍受、解析を行う
管理	後続工程への情報提供	上記の偵察工程で分析・把握した情報を管理し、後続のフェーズへ提供、連携する

工程毎の「評価者のスキル」の概要 (2/2)



侵入スキル

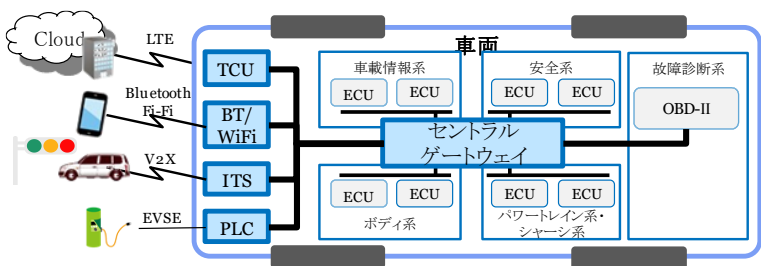
カテゴリ	スキル内容	概要
侵入	脅威分析	偵察フェーズの結果を踏まえて侵入の起点になると考えられるアタックサーフェイスを分析、特定する
	バイナリコード解析	脅威分析の結果に基づきアタックサーフェイスとなるプログラムファイル等の各ファイルを分析し、その設計・実装を分析、把握する
	脆弱性特定・攻略	バイナリコード解析と並行またはその結果を踏まえて侵入に利用可能な脆弱性を特定し攻撃コード等を作成することで攻略する
権限昇格	脆弱性緩和技術の回避	データ実行防止、アドレス空間ランダム化等の脆弱性緩和技術を分析、回避する
	安全機構の回避	製品特有の安全機構（動作条件の制限、性能制限等）を分析、回避する
	強制アクセス制御機構の回避	SELinuxに代表される強制アクセス制御機構を分析、回避する
	改竄検知機構の回避	セキュアブートに代表される改ざん検知、完全性検証機構を分析、回避する
目的の実行	車載ネットワーク分析	車載ネットワーク全体の構成（セントラルゲートウェイおよび各種EUCの配置等）を分析、把握する
	CAN通信解析	ネットワーク分析の結果を踏まえたCAN通信の傍受、分析、再送等を実施する
	攻撃検証・再現	上記の偵察および侵入工程の結果を踏まえて脆弱性を悪用した攻撃を検証・再現する

評価項目定義：前項を踏まえた評価実施項目の決定

車両システムセキュリティ評価(ペネトレーションテスト) 第3手順

リスク評価、条件確認の結果を踏まえ、(既存の)セキュリティ評価項目から実際に実施すべき評価項目および実施順序を決定する

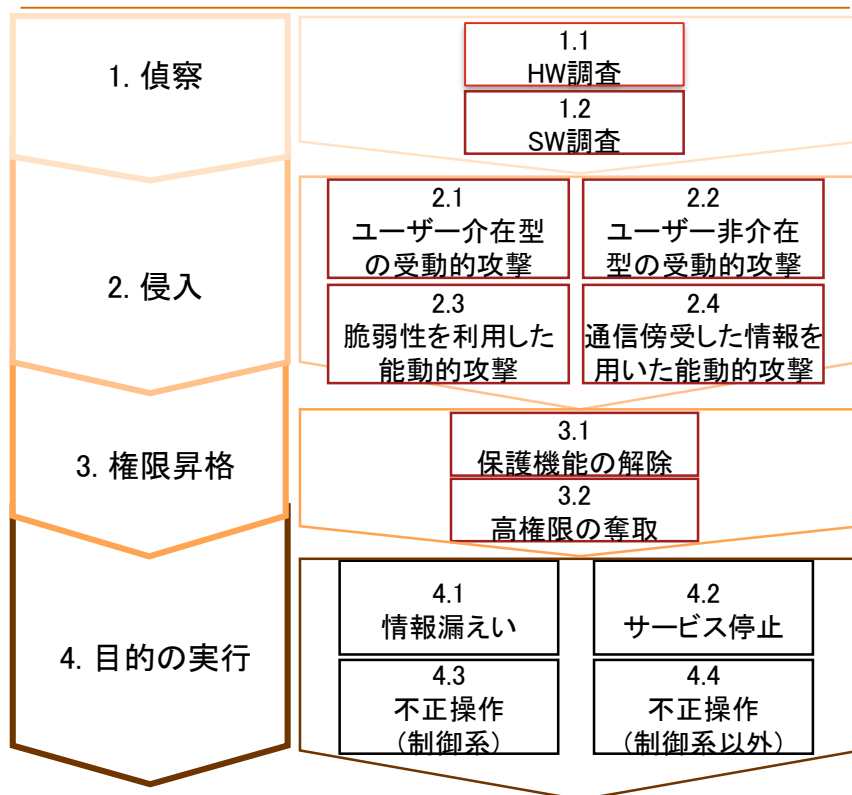
評価対象



評価条件



評価ガイドライン項目

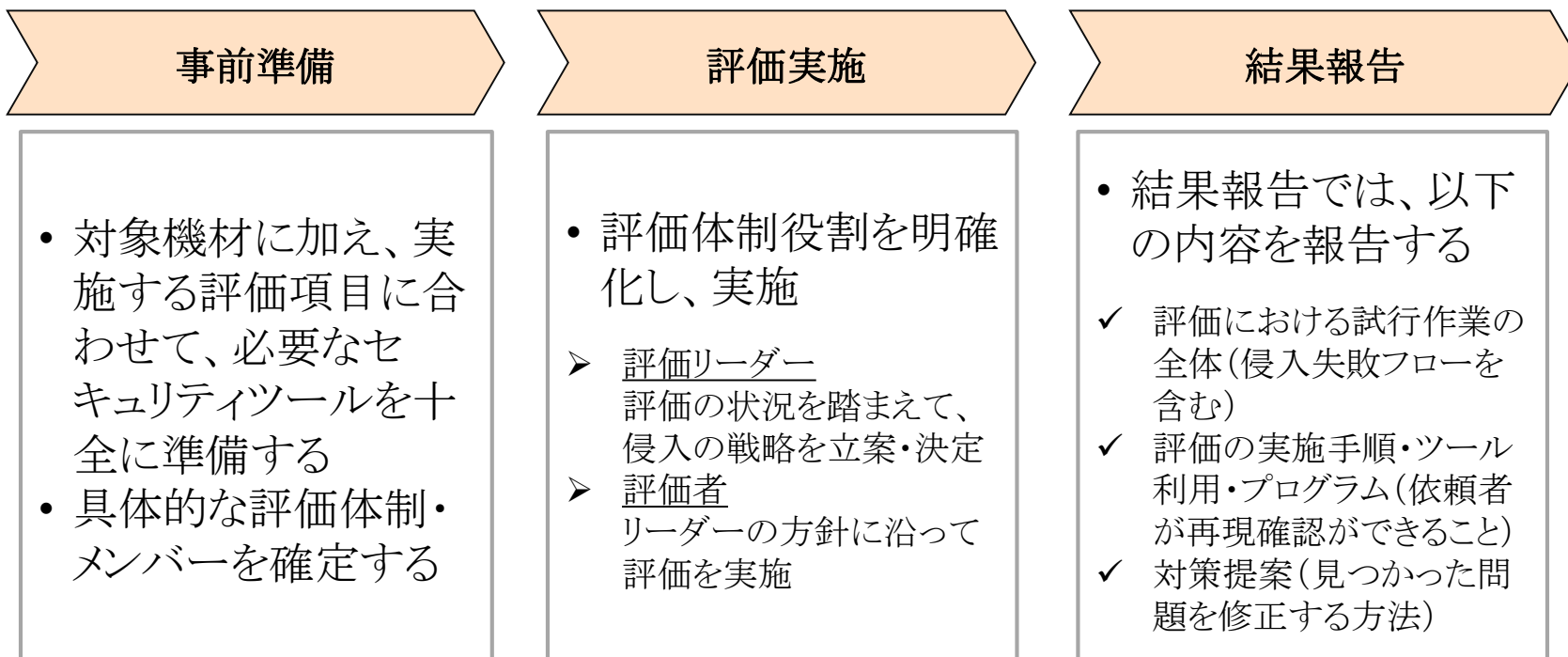


評価実施 : 評価推進方法および評価結果

車両システムセキュリティ評価(ペネトレーションテスト) 第4手順

定義した評価項目に沿って、評価を実施する。ペネトレーションテストの特性を踏まえた評価運営と評価結果に記載すべき項目について規定する

ペネトレーションテストの実施フロー



実証実験報告項目③： 実証実験実施を通じたガイドライン改善結果

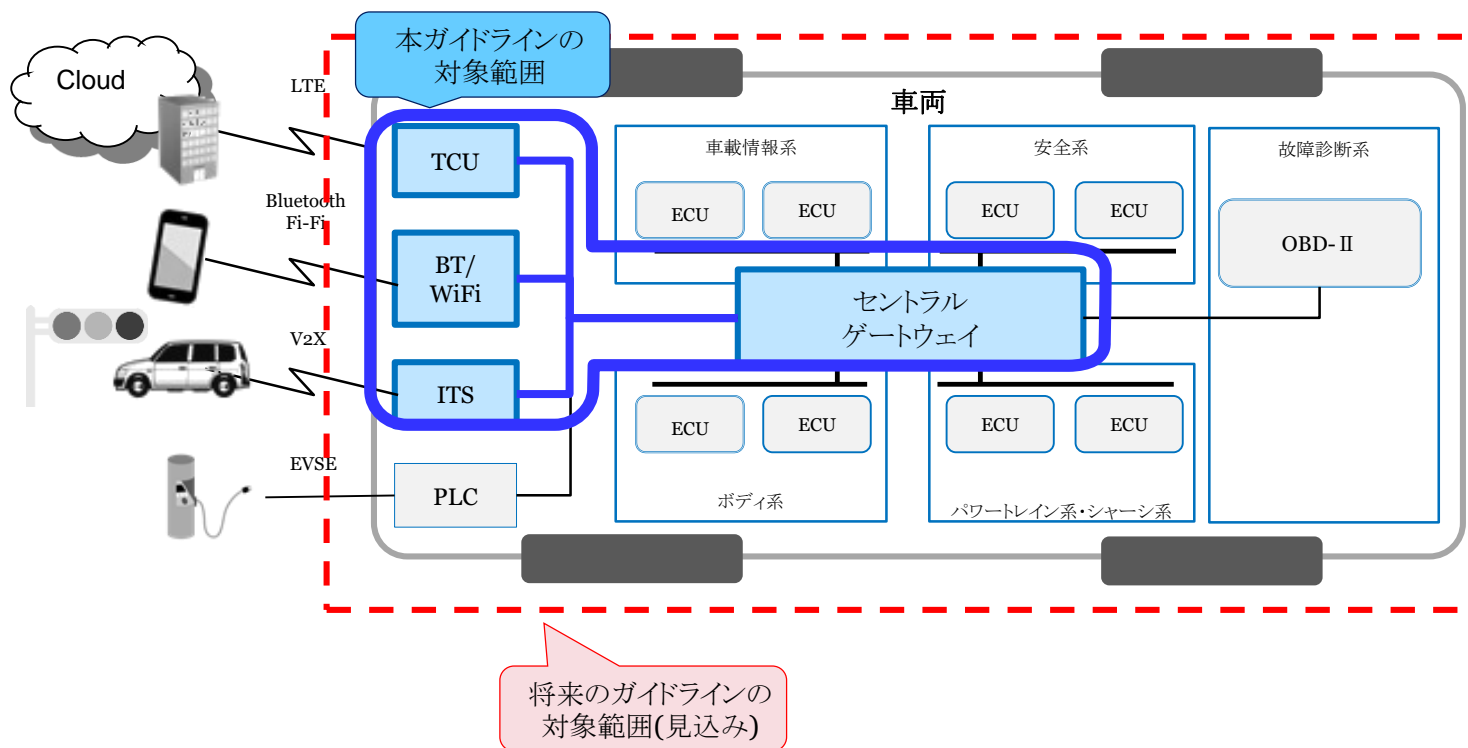
本年度実証実験により、評価項目19件*に関して改善した

ガイド項番	内容
1.1.1 デバイス取り出し前I/F調査	評価項目更新「1.1.1.1 USBポート接続確認」 評価項目追加「1.1.1.4 SDカードの確認」
1.1.3 チップ取り外し後I/F調査	評価内容更新「1.1.3.2 フラッシュメモリのチップ調査」
1.1.5 インターフェース接続	評価内容更新「1.1.5.5 バイナリ改ざんによるコンソールの取得」
1.1.6 バイナリ抽出	評価内容更新「1.1.6.1 UART(OS起動状態)からのバイナリ抽出」 評価内容更新「1.1.6.3 UART(BootLoader起動状態)からのバイナリ抽出」 評価内容更新「1.1.6.5 フラッシュメモリからのバイナリ抽出」
1.1.7 バイナリ保護機能確認	評価項目追加「1.1.7.8 難読化の調査」
1.1.8 リバースエンジニアリング	評価項目追加「1.1.8.2 ターゲットの選定」
1.2.6 TCUの通信傍受	評価項目更新「1.2.6.1 モデムの調査」 評価項目追加「1.2.6.2 TCU-IVI間の通信傍受」
1.2.8 CANメッセージ通信傍受	評価手法更新「1.2.8.1 CANメッセージキャプチャツールの設置」
2.3.4 WiFi(車両内部)経由の攻撃	評価手法更新「2.3.4.1 公開ポートからのログイン」 評価手法更新「2.3.4.3 APIソースコードの解析」
3.1.2 任意アクセス制御(DAC)の回避	評価手法更新「3.1.2.2 任意アクセス制御の確認の回避」
3.1.3 安全機能の回避	評価中項目追加
3.2.1 権限昇格防止機能の回避	評価手法更新「3.2.1.1 権限昇格防止機能の確認」 評価手法更新「3.2.2.2 強制アクセス制御の回避」
3.3.1 SecureBootの回避	評価中項目追加

実証実験報告項目④: 昨年度他社検討結果を参考にした改善結果

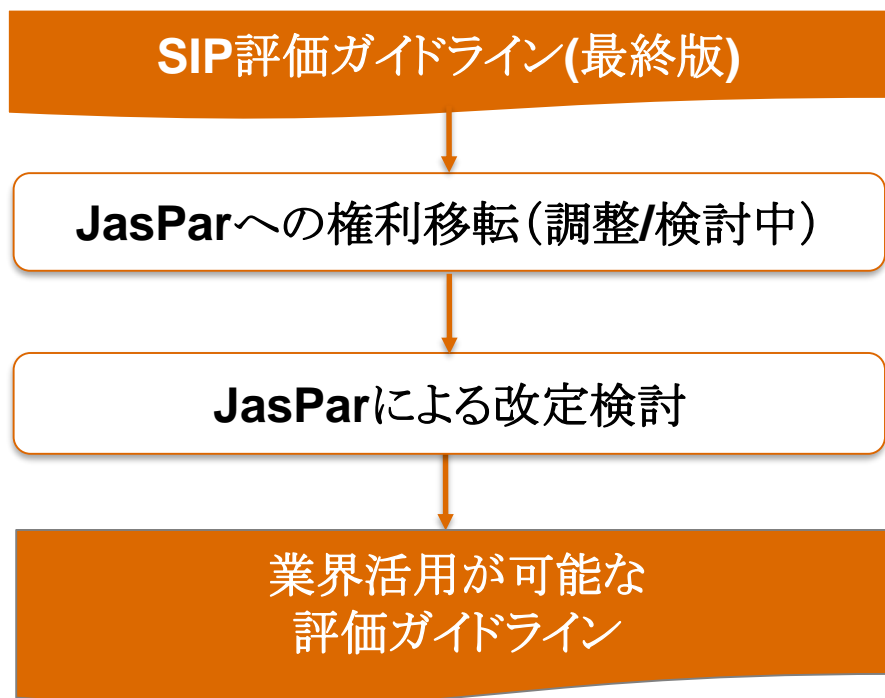
昨年度他社成果を参照することで効率的にガイドラインを改善した

制約時間内で実施するペネトレーションテスト手法において、今後対象範囲が拡大する事を見通し、脅威分析による優先順位付け手法を取り込み (P30参照)



ガイドラインの標準化・更新体制

SIP自動走行(第1期)の終了にあたり、本ガイドラインの自動車業界での活用と今後の管理を見据え、車両セキュリティに関する技術規格を策定するJasParへガイドライン権利移転を行ったうえでのより広い活用に向けた協議を進めている





© 2019 PwC Consulting LLC., PwC Cyber Services LLC. All rights reserved.

PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.