平成30年度成果報告書

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
情報セキュリティ実証実験

平成 31 年 2 月

国立研究開発法人新エネルギー・産業技術総合開発機構

委託先　PwC コンサルティング合同会社

要約（和文）

自動走行システムの基盤となる高度な地図情報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は、主に外部ネットワークから取得することが想定されている。こうして得られた情報は、自動走行システムによる車両制御に活用する目的で、車両の制御系／情報系の機器に送られるが、このような状況は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。

このような課題を解決するため、「戦略的イノベーション創造プログラム　自動走行システム／大規模実証実験　情報セキュリティ実証実験」では、自動走行におけるセキュリティ脅威の調査／分析、国際標準化も見据えた車両レベルでのセキュリティ評価手法・プロトコルの策定、および、本実証実験を通して募る参加者の実車両システムを用いた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の実施が計画されている。

本年度の事業においては、「実証験事務局の運営」、「情報セキュリティ評価の実施」、「情報セキュリティ評価ガイドラインの最終化」を行い、活動結果としてまとめた。

「実証験事務局の運営」については、昨年度の活動である実証実験の事前準備の内容に基づき、実証実験参加社募集の実施、実証実験参加社との各種手続き、契約締結、参加社から借用する評価対象システム等の管理、および、情報セキュリティ管理を行った。

「情報セキュリティ評価の実施」については、実証実験への参加依頼を受け参加いただいた車両OEM4 社の協力のもと、昨年度策定した情報セキュリティ評価ガイドラインドラフト版を元にした評価作業を実施した。評価にあたり、昨年度の試行調査の結果を受け判明した情報セキュリティ評価における実施課題を踏まえ、評価プロセスを整備するとともに、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ライテリアを明確化・定義した。

「情報セキュリティ評価ガイドラインの最終化」については、情報セキュリティ実証実験の実施結果をもとにした情報セキュリティ評価ガイドラインの最終化を行った。実証実験成果として、次の４項目についてまとめた。

１．情報セキュリティ評価ガイドラインの妥当性検証の結果。妥当性検証では参加社からのアンケートや自己点検結果をまとめた。２．実証実験実施を通した評価プロセス整理結果。評価プロセスの整理結果では、事前に整理した評価プロセスや評価条件について実証実験での実施結果を踏まえて再整理し、本ガイドラインで記載する情報セキュリティ評価におけるペネトレーションテストの評価プロセスについてはまとめた。３．実証実験実施を通した評価ガイドライン評価項目改善結果。評価ガイドライン評価項目改善結果では、昨年度策定した情報セキュリティ評価ガイドラインドラフト版の評価項目について、実証実験の実施を通じて評価項目として内容に不足が見られた項目については、改善・追加した項目についてまとめた。４．昨年度実証実験の他社検討結果を参考にした改善結果。昨年度他社検討結果について、本年度の実証実験の実施に向けて見直しを行い、弊社の取り組みとして参考にすべき項目を洗い出し、取り組みとして取り込んだ。具体的には、評価プロセスにおけるリスク分析の取り組みについて、昨年度他社検討結果を参考にまとめた。

要約（英文）

The basis of automated driving systems, information such as high definition map data, data of vehicles, pedestrians, road infrastructure etc., are expected to be obtained primarily from external vehicular networks. Such information will be transferred to vehicle control/information devices to be used for vehicle control in the automated driving system. This could lead to cause cybersecurity issues that did not exist before, in the time of conventional non-connected cars.

"Cross-ministerial Strategic Innovation Promotion Program (SIP) Automated Driving System, Large Scale Field Operational Test: Information Security Field Operational Test (FOT)" aims to provide solution for ever growing challenges related to cybersecurity of automated driving systems through; research and analysis of security threats related to automated driving, establish security evaluation method/protocol at vehicular level towards international standardization, and operate FOT for the vehicle hacking-resistance evaluation (black-box testing) using actual vehicle systems provided by the automakers participating in the FOT.

The FY18 FOT covered and summarized results for the project activities; "FOT management office activities", "FOT operation" and "Finalizing Information Security Evaluation Guideline (the Guideline)".

"FOT management office activities" utilized outcome preparation activities from FY17 and covered; recruitment of FOT participants, coordination of FOT participation conditions, contract arrangements related to FOT participation, management of vehicle systems and components provided by the participants, and information security management during the FOT.

"FOT operation" covered; security evaluation of vehicle systems provided by four participating automakers using the draft of the Guideline, establishment of evaluation process considering FY17 trial research results, definition of evaluation conditions and criteria to ensure reproducibility of the evaluation.

"Finalizing Information Security Evaluation Guideline" covered; updating the Guideline based on the FOT results. Following four topics were summarized as the result and the final report of the FOT;

1. Guideline validation through the FOT: Summarized results of the questionnaires answered by the participants, self-verification conducted by PwC.
2. Evaluation process establishment through the FOT: Summarized evaluation process of the penetration test in the information security evaluation and documented into the Guideline. The process was initially organized based on FY17 trial research results, then refined through and based on the result of FY18 FOT.
3. Improvements in the Guideline through the FOT: Based on the draft of the Guideline, the evaluation items were added, updated and reviewed reflecting any deficiencies or room for improvements identified during the FOT. Such changes or updates were summarized in the final report.
4. Improvements using other outcomes of FY17 FOT: Outcome of other contractors in FY17 FOT were reviewed and improvements were reflected to FY18 activities. Specifically, activities related to risk analysis was incorporated into the evaluation process referencing FY17 FOT outcome of other contractors.

まえがき

本報告書は、「戦略的イノベーション創造プログラム　自動走行システム／大規模実証実験　情報セキュリティ実証実験」として、国内 OEM を対象とした実証実験への参加募集および参加各社との調整、参加各社から提供を受けた車両システムに対する昨年度策定した評価ガイドライン(ドラフト)を用いてのセキュリティ評価を実施、および、評価結果の分析・改善点を反映することによる評価ガイドラインの最終化についてまとめたものである。

目次

1　事業概要

自動走行システムの基盤となる高度な地図情報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は、主に外部ネットワークから取得することが想定されている。こうして得られた情報は、自動走行システムによる車両制御に活用する目的で、車両の制御系/情報系の機器に送られるが、このような状況は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。

このような課題を解決するため、「戦略的イノベーション創造プログラム　自動走行システム／大規模実証実験　情報セキュリティ実証実験」においては、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レベルでのセキュリティ評価手法・プロトコルを策定し、本実証実験を通して募る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を行うことによる技術調査を行うことが計画されている。

本年度の事業においては、「実証験事務局の運営」「情報セキュリティ評価の実施」「情報セキュリティ評価ガイドラインの最終化」を行い、活動結果としてまとめた。

2　本事業の構成

本事業の構成は以下のとおりである。

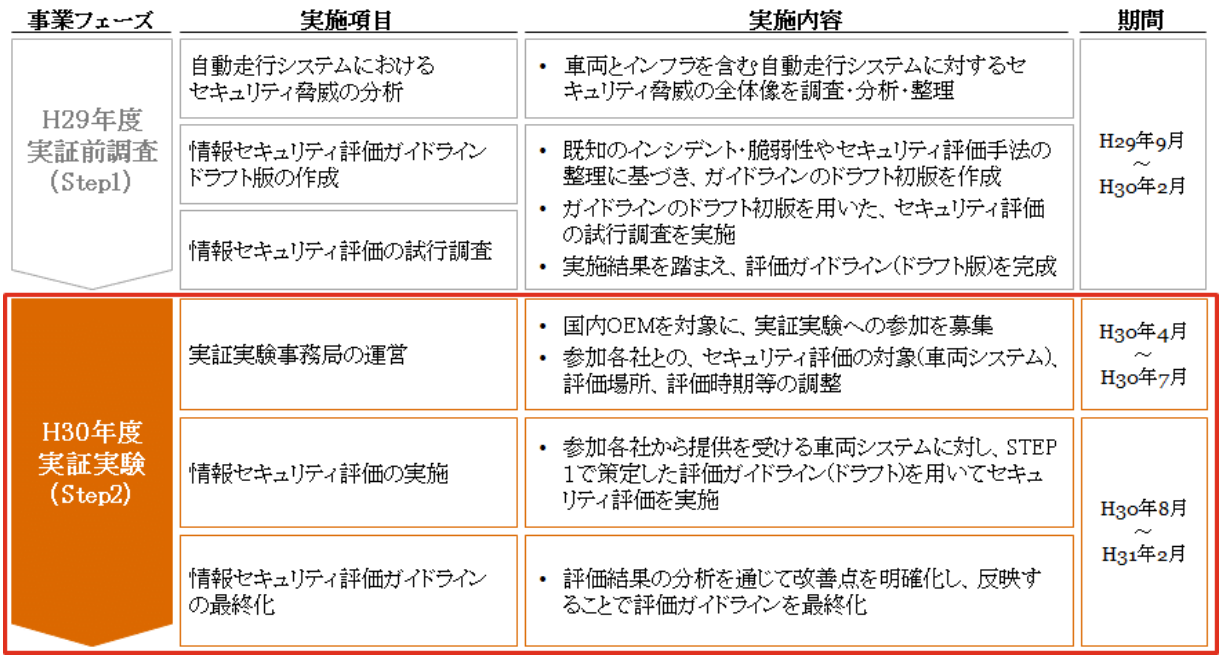


図 2-1　本事業の構成

第 3 章にて「実証実験事務局の運営」の活動である、国内 OEM に対する実証実験への応募および参加社への依頼等の取り組み結果をまとめる。第 4 章にて、「情報セキュリティ評価の実施」に関して、評価プロセスの整備を含む情報セキュリティ実証実験の評価作業の取り組みについてまとめる。第 5 章にて、「情報セキュリティ評価ガイドラインの最終化」に関して、情報セキュリティ評価実証実験から得られた評価ガイドラインの妥当性検証の結果および採取化した情報セキュリティ評価ガイドラインについて、昨年度策定の評価ガイドラインドラフト版からの変化点を主としてまとめる。なお、本報告書には策定したガイドライン自体は含まない。

3　実証実験事務局の運営

本章では、実証実験事務局運営に関する内容についてまとめる。実証実験事務局の活動については、「実証実験参加応募」および「実証実の事前準備」の項目からなる。

3.1.　実証実験参加社応募

3.1.1.　実証実験参加社募集ステップ

本活動では、平成 29 年度の活動である「実証実験の運営準備」で策定した参加者募集に係る各種文書を用いて、以下のステップで参加者を募集した。

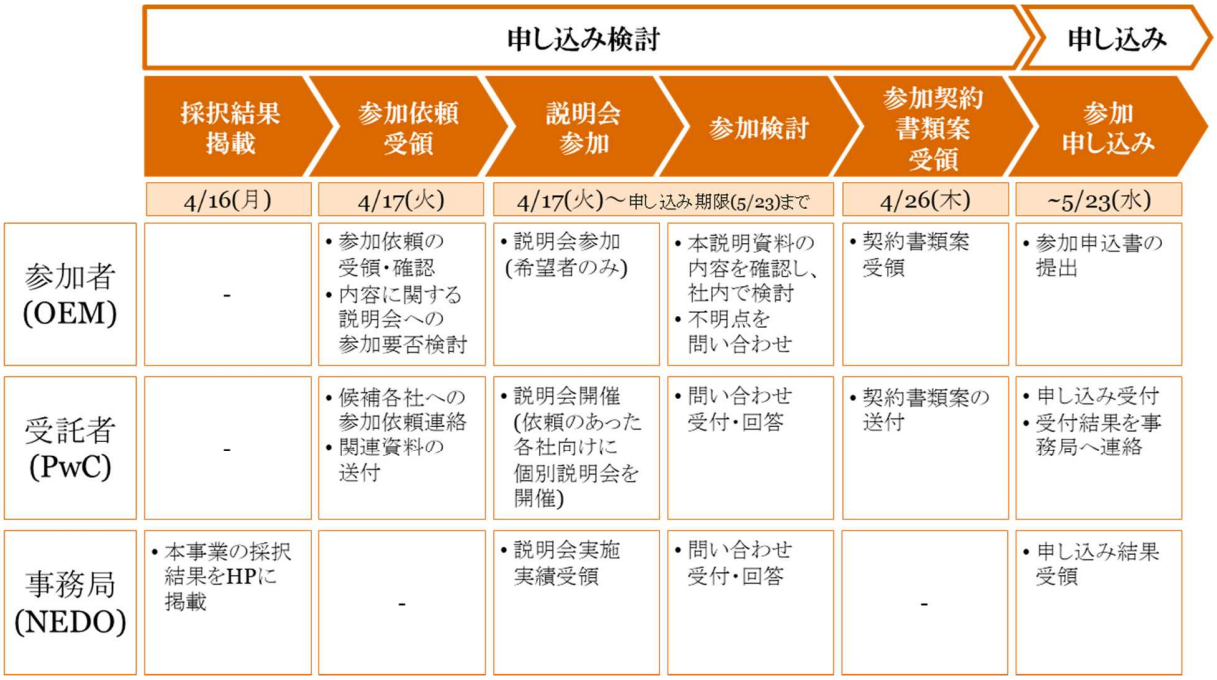


図 3-1　実証実験参加応募ステップ

3.1.2. 実証実験事前準備ステップ

参加社決定後は、以下のステップで評価実施に向けてご準備頂いた。また、実際の各社にご提供いただくシステムの評価実施時期は、提供頂く品目や準備状況に応じて調整・決定することとした。

＊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。

図 3-2　実証実験参加応募ステップ

3.1.3. 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。

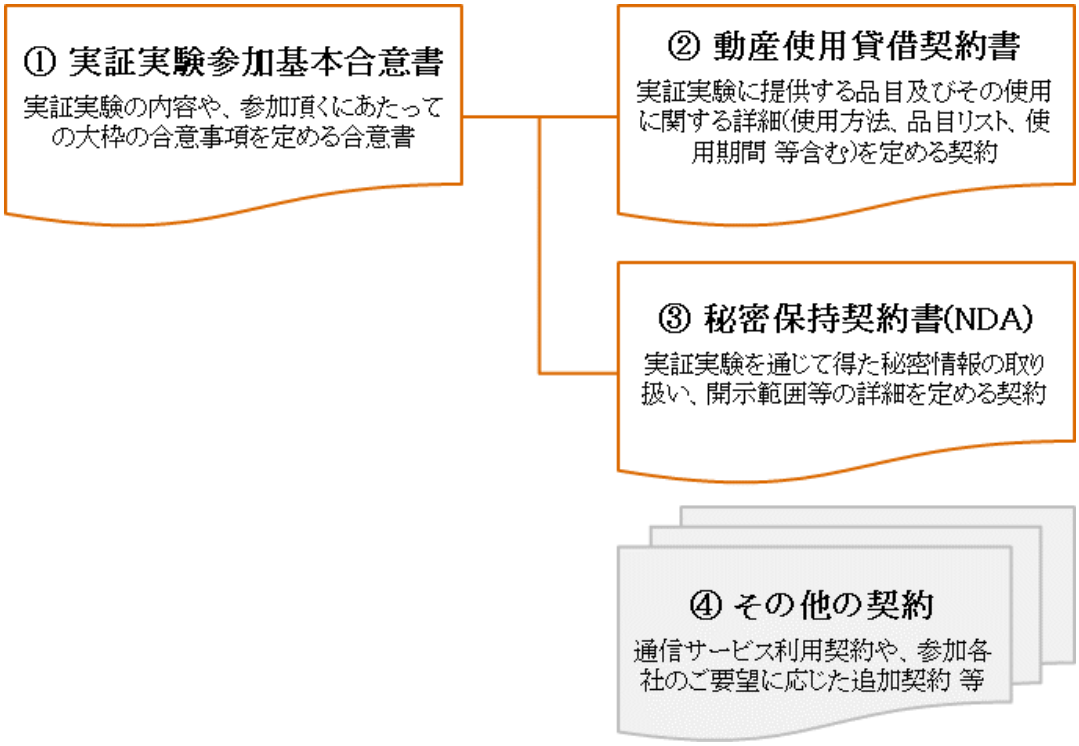


図 3-3　締結した契約書類の概要

3.2. 実証実験の事前準備

3.2.1. 参加各社にご支援頂く内容

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、参加各社に必要なご支援・ご協力を頂いた。以下に実施期間におけるご支援いただいた内容をまとめた。

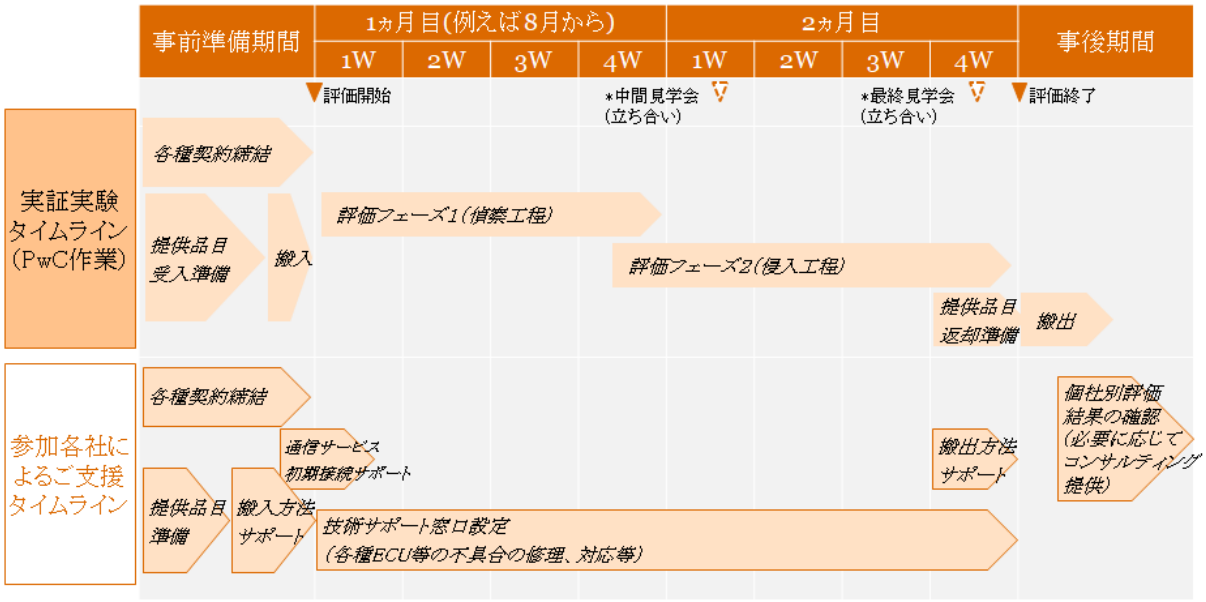


図 3-4　実証実験のタイムライン

3.2.2. 参加各社にご準備いただく品目

実証実験期間において、参加社には実証実験情報セキュリティ評価作業に必要となる、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台	• 情報系ECUとGatewayECU*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 ＊ GatewayECUについては、No.3で記載の条件を考慮。	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	• 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		接続形態に応じたGatewayの提供（赤枠） 例1：セントラルGatewayが存在する場合  例2：複数GWが存在する場合  例3：情報系と制御系が直結している場合  	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） 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
4		テレマティクスサービスアカウント	4個（最低限2個）	• 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	ー	• 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	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） 上記2点を実施可能なサーバーをご用意ください。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。
6		検証用スマートフォンアプリ	1個	• 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	• 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	・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必要なのか判別できるもの	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。

表 3-1　参加社にご準備いただいた品目一覧

*GatewayECU については、No. 3 で記載の条件を考慮

3.2.3. 参加各社にご支援（サポート）頂いた内容

実証実験期間において、参加社には実証実験情報セキュリティ評価作業の実施支援として、以下作業のご協力をお願いした。

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 ・実証実験基本合意書 － 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)

表 3-2　参加社にご協力いただいた作業項目一覧

3.2.4. 施行区分および費用負担

実証実験に用いる品目は参加各社のご負担により手配頂いた。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	参加社
1	評価対象品目の提供 (車両ベンチ・各種ECU等)	車両ベンチ(又は完成車)・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	○	-

表 3-3　施行区分および費用負担一覧

3.2.5. 見学会/実証実験評価作業立ち合い

実証実験の各参加社に対して、評価実施の中間進捗、最終結果について、ご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。各見学会の主な内容は以下のとおり。

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)	•個社別評価中間結果(進捗)ご報告 •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)	•個社別評価レポートご報告 •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)

3.3. 実証実験に関する情報セキュリティ管理

3.3.1. 実証実験で取り扱う機密情報と開示範囲

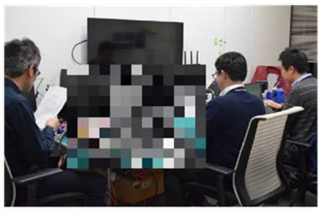
実証実験の実施にあたり参加各社からご提供をお願いする情報・機材、および、PwC よりご提示する機密情報に関して、開示範囲を以下の通り制限した。

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	○	○	○	○

*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。

3.3.2. 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、基本的には車両ベンチを提供いただき、弊社 HW ハッキングラボにて評価を実施した。弊社 HW ハッキングラボの概要は以下のとおり。

項目		PwC HWハッキングラボ
概要		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   
場所		東京都千代田区大手町1-1-3 大手センタービル19F
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
セキュリティ	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

4　情報セキュリティ評価の実施

4.1.　実証実験　評価前事前準備

4.1.1.　平成 30 年度実証実験参加社募集の流れ

平成 30 年度実証実験においては、国内 OEM10 社に参加を依頼した。依頼した参加社に対しては 3 章で記載した実証実験参加社募集ステップや実証実験の事前準備に関する内容を資料としてまとめ検討いただいた。結果、参加を依頼した OEM10 社のうち 4 社より参加応募をいただき、事前の準備をへて、提供いただいた機材を用いて実証実験を実施した。

参加依頼から評価実施までの実際流れを以下にまとめた。

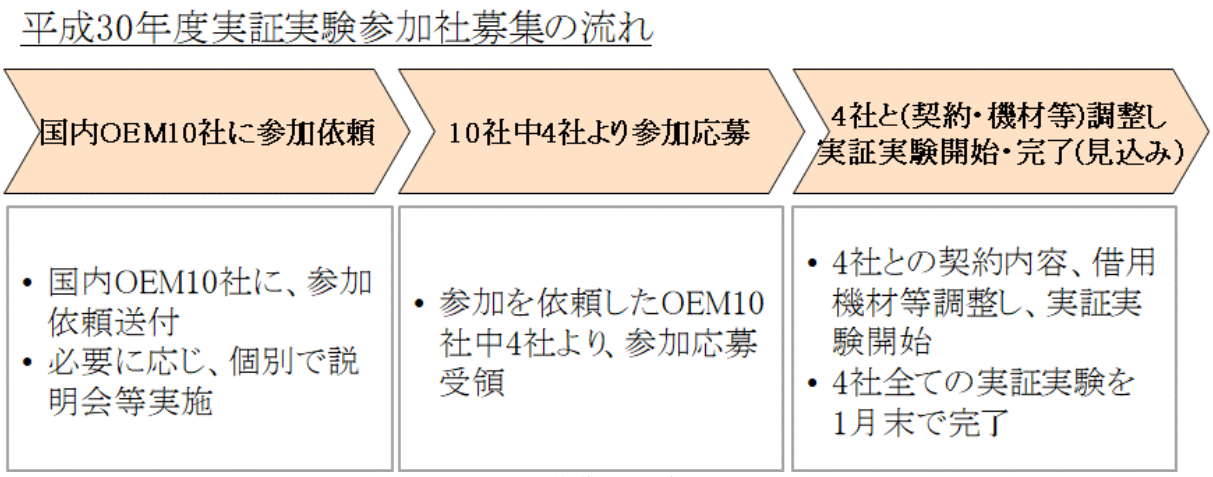


図 4-1 参加社募集・実施までの流れ

4.1.2. 評価実施前後のフロー

参加者確定後、参加社には 3 章で説明した内容について、実際のご対応いただいた。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。

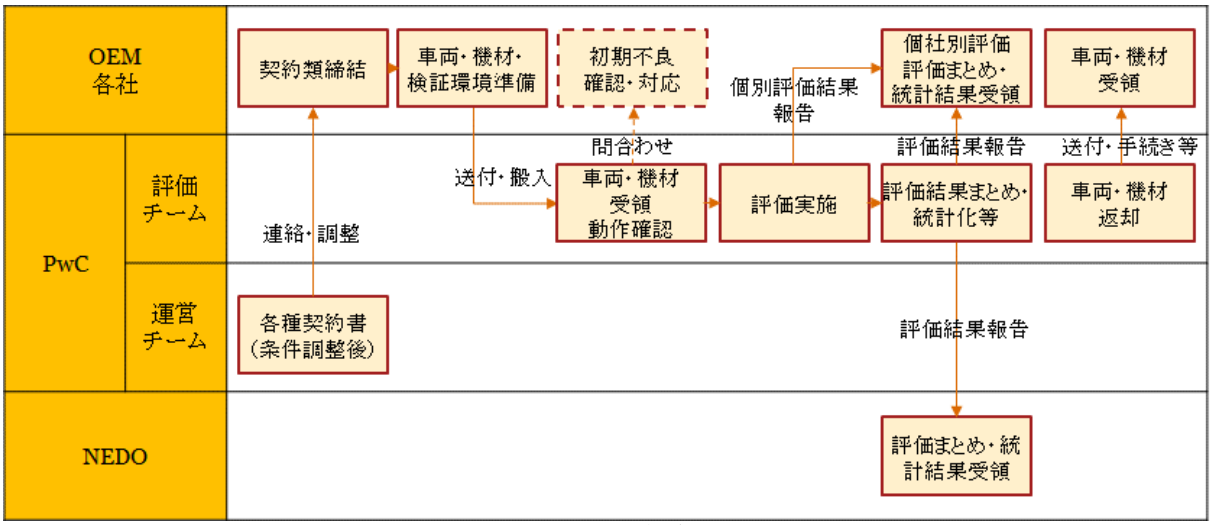


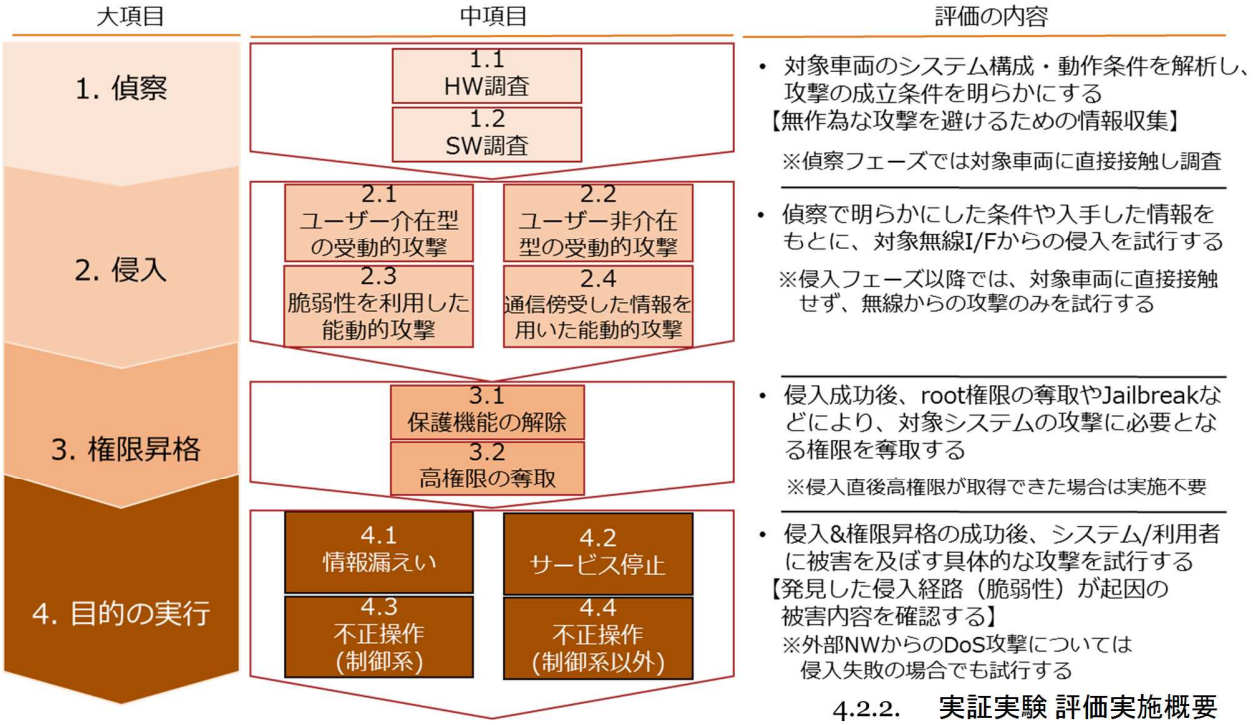
図 4-2　実証実験実施前後のフロー

4.2. 実証実験 評価実施内容

4.2.1. 情報セキュリティ評価ガイドラインドラフト版の評価項目

本年度実証実験では、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した。

昨年度策定した情報セキュリティ評価ガイドラインドラフト版の評価項目の項目概要は以下のとおり。



4.2.2. 実証実験 評価実施概要

図 4-3 情報セキュリティ評価ガイドラインドラフト版評価項目概要

本年度実証実験でのセキュリティ評価定は、ガイドラインに従った各工程の評価（攻撃）に対して、過去実績等から規定した一定期間での防御成否を元に行った。具体的な評価期間は以下のとおり。

- 「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（20 日稼働）
- 「侵入/権限昇格/目的の実行」工程 4 週間（20 日稼働）

図 4-4　評価期間

次項以降にて各評価工程の内容について説明する。

「偵察」工程の評価手法

「偵察」工程では、車両システムへの侵入のための情報収集に関して評価を行った。

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 週間で完遂できる工程とした。具体的には「図 4-5　偵察工程の評価作業フロー」に記載する専門業者によるファームウェア抽出の作業について、当該作業を専門とする業者に委託することで、本工程の作業品質および工数を均一化した。

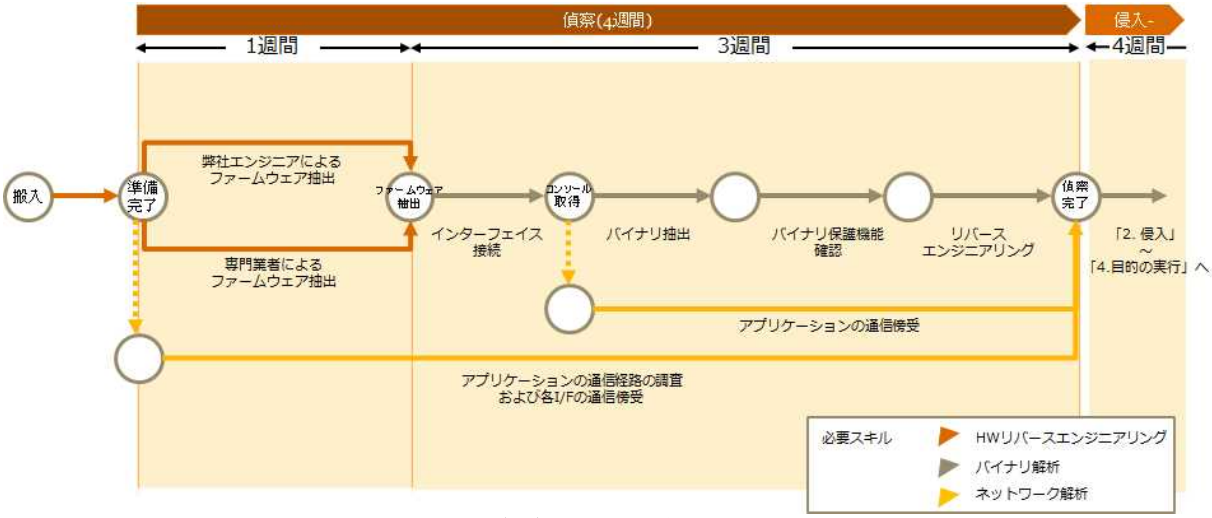
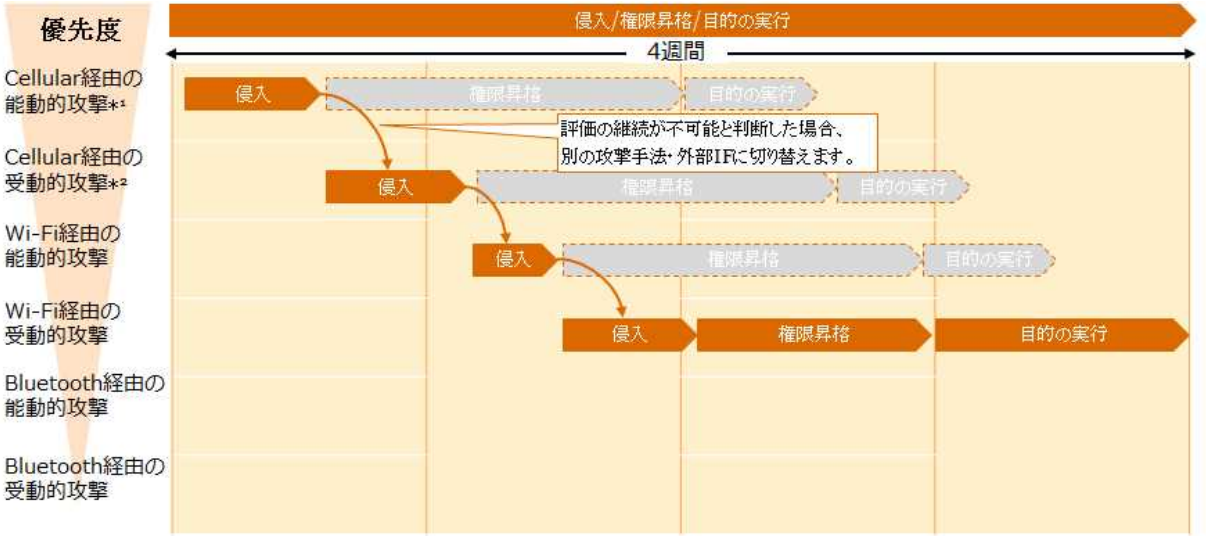


図 4-5　偵察工程の評価作業フロー

「侵入」/「権限昇格」/「目的の実行」工程の評価手法

「侵入」/「権限昇格」/「目的の実行」工程では、車両が持つ通信外部 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」まで深堀りする形で評価を実施した。



本実証実験においては、評価期間である 1 カ月で、すべての攻撃手法・通信外部 I/F への「侵入」を実施した。「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することとした。例えば、Wi-Fi 経由からの侵入が成功し、権限昇格以降の作業を実施した場合、その他の I/F からも侵入できたケースでは、Wi-Fi から侵入した結果を利用しみなし評価とした。

4.2.3. 実証実験による評価レポート（イメージ）

本実証実験の評価結果は、実証実験の参加個社に対して報告した。評価結果として、現実に発生し得る被害（リスク）と攻撃の再現手順をご報告した。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案した。

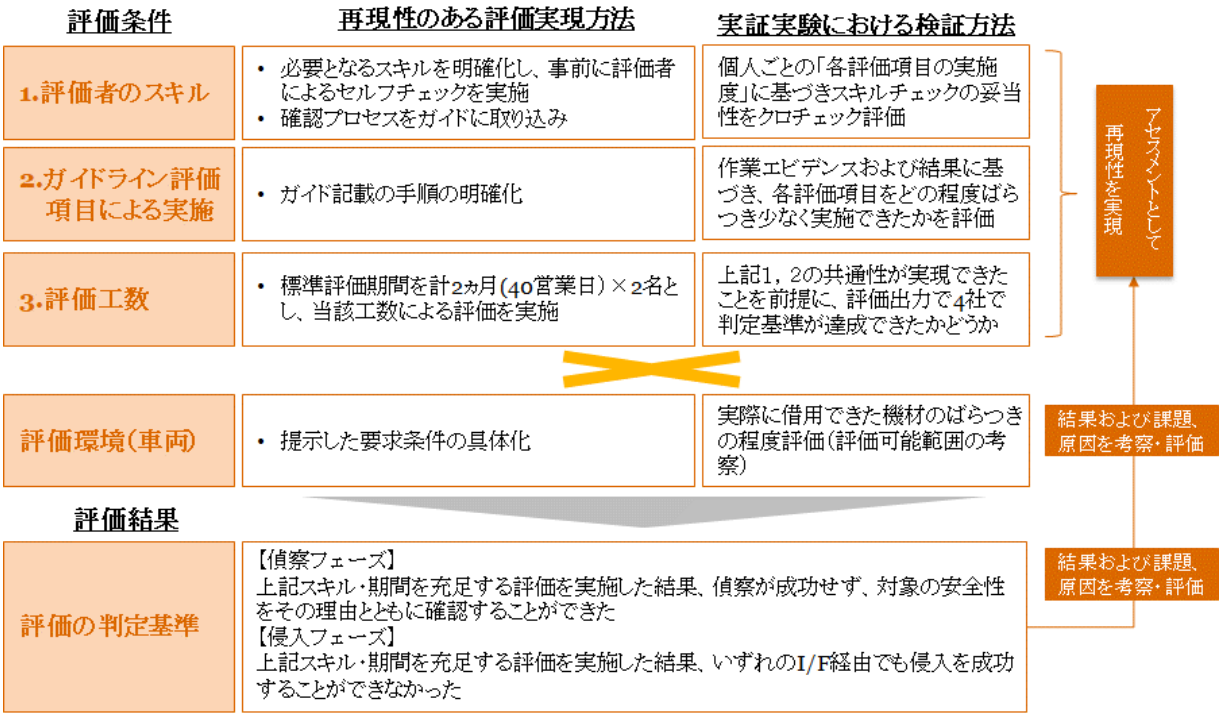
図 4-6　評価レポートのイメージ

4.2.4. 評価におけるクライテリアの明確化

昨年度試行調査の結果および車両業界におけるペネトレーションテストに共通する課題として、評価の妥当性判断や再現性があった。つまりペネトレーションテストの評価者のスキルや評価時間などに、評価結果が大きく依存し、車両業界がペネトレーションテストを実施・委託する際に、評価者ないし評価結果が妥当なものであるか判断することが課題となっていた。

この課題を受け、本年度実証実験では、ペネトレーションテストとしての評価条件を定め、評価クライテリアを明確化した。実証実験を通して各評価条件の妥当性を評価し、ガイドラインに反映することとした。

本年度実証実験で定めた評価条件と、各条件の検証方法は以下のとおり。



評価者のスキル

評価者のスキルについては、評価工程のフェーズ毎に以下のとおり条件項目を策定した。

- 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	プリント基板上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エ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

表 4-1　偵察工程評価者スキル表

- 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

表 4-2　侵入以降工程評価者スキル表

これら評価者スキルの条件項目に対して、以下のレベル分けで評価実施者のレベルを確認し、実際の評価でそのレベル確認およびレベル設定の妥当性を確認した。

評価スキルレベル	レベル内容
0	知識を有しておらず、実践することもできない（知らない）
1	Web・書籍等の公開情報に基づく知識は有しているが、実践することができない（できない）
2	Web・書籍等の公開情報に基づく知識を有しており、市販のツール・製品等を用いて実践することができる（できる/標準）
3	過去に複数の経験・実績を有しており、それらの経験・実績に基づいた実践をすることができる（できる/高度）

表 4-3　評価者スキルレベル表

ガイドライン評価項目

ガイドライン評価項目については、情報セキュリティ評価ガイドラインドラフト版の評価項目を基準とし、評価者によりばらつき無く評価が実施できたかで条件の妥当性を確認した。

評価工数

評価工数については、「4.2.2 実証実験 評価実施概要」で記載のとおり、昨年度試行調査の結果を受け、本実証実験での評価期間を8週間としたことを受け、これを具体化し、40日間（1日8時間）を評価期間として定め、実証実験を通じて妥当性を確認した。

評価環境（車両）

評価環境については、「3.2.2 参加各社にご準備いただく品目」で記載した要求事項を元に、実際に提供いただけた品目による実験環境の充足度に関する許容可能範囲を評価すること、および、その評価結果を踏まえ、評価環境（車両）としての妥当性を確認した。

5　情報セキュリティ評価ガイドラインの最終化

5.1.　実証実験結果

5.1.1.　実証実験結果報告項目

実証実験の実施を通じた各種の改善を経て、情報セキュリティ評価ガイドラインを最終化した。実証実験の成果としては以下の項目について記載する。

- 実証実験成果報告内容
  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 実証実験実施を通した評価プロセス整理結果
  ③ 実証実験実施を通し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

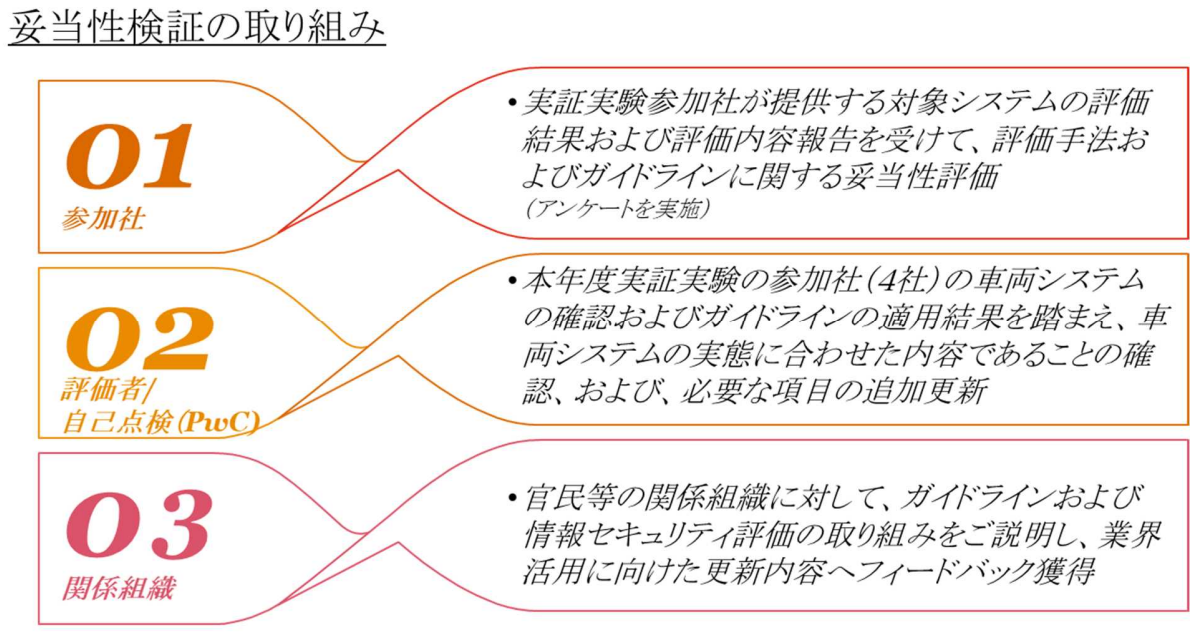
なお、参加社個社の機密情報に関わる情報については、「3.3.1 実証実験で取り扱う機密情報と開示範囲」に記載の通り、公開しないものとし、評価ガイドラインの最終化に関する情報としてのみ利用した。

5.2.　実証実験結果報告項目

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

一部事前に改善した情報セキュリティ評価の取り組みおよび情報セキュリティ評価ガイドラインドラフト版を用いた実証実験の実施結果を通じて、評価ガイドラインの妥当性を評価し、必要な改善を実施した。

妥当性評価については以下の３点で実施した。



5.2.1. 参加社の評価

実証実験参加社に対して、ガイドラインの活用・有効性に関する以下のアンケートを依頼した。

本取り組みに関して、ご意見をお聞かせください。 **(1) 実証実験は、業界の課題解決に資する取り組みだったと思いますか？** **(1. 非常にそう思う 2.そう思う 3. どちらでもない 4. あまりそう思わない 5. 全くそう思わない)**
(2) 評価ガイドラインの策定は、業界の課題解決に資する取り組みだったと思いますか？ **(1. 非常にそう思う 2.そう思う 3. どちらでもない 4. あまりそう思わない 5. 全くそう思わない)**
実証実験評価結果について、ご意見をお聞かせください。 **(1) 評価ガイドラインを用いた情報セキュリティ評価結果は有効だったと思いますか？** **(1. 非常にそう思う 2.そう思う 3. どちらでもない 4. あまりそう思わない 5. 全くそう思わない)**
(2) 評価ガイドラインは将来の車両開発に活用できると思いますか？ **(1. 非常にそう思う 2.そう思う 3. どちらでもない 4. あまりそう思わない 5. 全くそう思わない)**
評価ガイドラインを将来活用する上で、改善が必要だと思う点についてお聞かせください **（自由記述）**
その他、ご自由コメント

表 5-1 実証実験参加社アンケート項目

上記アンケート項目について、回答頂いたコメントの概要は以下のとおり。なお回答内容は個社情報が特定できないよう匿名化・概要レベルの記載とした。

アンケート項目	回答概要
実証実験について	・ 評価ガイドの妥当性検証に寄与する活動であった ・ 複数車両を用いた検証が良い取り組みであった
評価手法について （評価ガイド策定）	・ 一定レベルのセキュリティ品質確保に寄与する手法であった ・ 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であった
今後の改善点	・ 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がある ・ 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

※上記の回答概要は、本書作成時点で回答内容の開示に関して許諾頂けた参加社分のみ反映した
※各アンケート項目の回答数値は本書作成時点で未回答の参加者があるため未記載とした

5.2.2. 評価者/自己点検

実証実験の評価者自身の自己点検結果は、以下の項目および内容のとおり。

点検項目	結果
評価プロセス	・ 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した ・ 評価プロセスの整理により、OEM4 社の評価作業について同一の評価条件を確認、評価実施、評価結果のまとめを実施でき、作業レベルの均一化に寄与したと考える
評価者スキル	・ 設定した評価者スキルおよびレベルを確認した評価者の作業で、策定した情報セキュリティ評価ガイドラインの評価作業は実施することができ、かつ、問題の発見について均一化ができたと考える（後述の評価項目も参照） ・ 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（40 営業日）で情報セキュリティ評価ガイドラインに記載の評価項目を実施できた。 ・ 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 ・ 異なるシステムに対して別チームが評価を実施したが、評価試行手順が同様に進めることができ、前述の評価スキルを確認したことの効果もあり、評価項目毎のばらつきなくの実施できたと考える。 ・ ただし、実際の車両システムでの評価作業で、昨年度策定した情報セキュリティ評価ガイドラインの評価項目では不足する内容が見つかり、最終化の際には項目追加を行った
評価環境（対象システム）	・ 本実証実験では、参加いただいた OEM4 社毎に、ご用意いただけた車両システム構成に差分があり、結果として、評価実施可能な項目に差が発生した ・ 提供いただいた車両システムに沿って可能か評価は実施したが、ガイドラインの最終化においては、評価対象システムの実態を考慮して評価を判断するプロセスを追加整備した

表 5-2　自己点検結果

5.2.3. 関係団体

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 と、より広い活用に向けた協議を進めており、今後も継続議論することで合意した。

5.3. 実証実験実施を通した評価プロセス整理結果

「4.2.44.2.4 評価におけるクライテリアの明確化」で準備した評価条件や、実証実験を通じた評価実施手順を踏まえ、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、確立した。
評価プロセスの概要は以下のとおり。

以下、評価プロセスの各フェーズの内容について記載する。

5.3.1. 評価対象定義

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、ペネトレーションテストによる評価対象として選定・定義するフェーズ。

情報セキュリティ評価ガイドラインでは、リスク分析に関する評価手法そのものは規定せず、評価プロセスにおけるリスク分析作業工程とリスク分析の事例を記載した。リスク分析事例として 昨年度弊社にて実施した SIP 実証実験における脅威分析手法と OWASP（The Open Web Application Security Project）の OWASP Risk Rating Methodology について記載した。

両手法では、リスク評価の観点として、「被害の深刻度」「攻撃の成立可能性」「攻撃（被害）の影響範囲」といった項目でシステムに対する脅威の程度を指標化し、定量的にリスク値を算定し、評価している。

以下に参考までに、昨年度弊社にて実施した SIP 実証実験における脅威分析手法の脅威の重大度算定式を記載する。

「脅威の重大度フレームワーク」における算定式は以下の通り：
脅威の重大度 ＝ **脅威の大きさ**（「脅威の重大度」×「攻撃の難易度」）
× **攻撃の発生確率**（「事象の与える影響範囲」×「情報資産の重要度」）

上記算定式における各要素のスコア表は以下の通り。

重要度	内容	スコア

Lv7	車両の安全性へ影響を与える	7
Lv6	車両機能の動作停止	6
Lv5	ソフトウェアの改ざん、パフォーマンスの変更	5
Lv4	ソフトウェアの変更 （ただし、操作上の影響なし）	4
Lv3	データの完全性侵害	3
Lv2	データの機密性侵害	2
Lv1	その他	1

表 5-3　脅威の重大度

難易度	内容	スコア
高	権限昇格や情報収集など攻撃に至るまでに複数の条件が必要となるもの	1
中	難易度がシステムに内在する脆弱性に依存する攻撃	2
低	攻撃が容易（難易度「高」に記載するような条件が不要な攻撃）	3

表 5-4　攻撃の難易度

影響範囲	内容	スコア
大	不特定多数の対象に影響を及ぼす	3
中	複数あるが周辺の対象のみに限定される	2
小	1 つの対象のみに限定される	1

表 5-5　事象の与える影響範囲

重要度	内容	スコア
特高	制御情報	4
高	金融資産に関する情報	3
中	プライバシー情報	2
低	上記以外の情報	1

表 5-6　情報資産の重大度

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

表 5-7　脅威の重大度

5.3.2. 評価条件定義

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ライテリアを明確化・定義するフェーズ。

情報セキュリティ評価の計画策定に必要な条件を、「評価品目」、「評価者スキル」、「評価設備」、「評価期間」、「判定基準」の 5 つの観点から定義する。

「評価品目」

評価対象として用意可能な車両システム、コンポーネント、サーバ、アプリおよび情報を含む評価品目を明確化する。

なお、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。

「評価者スキル」

評価者に必要なスキルを明確化する。

本実証実験においては「4.2.4 評価におけるクライテリアの明確化」に定める偵察工程と侵入以降工程で規定する内容が実施できる技術レベルを有する必要がある。この際、技術的知識のみならず、実際の評価手法が再現可能な技能の有無に判定基準を置く。

「評価設備」

評価実施に必要な評価設備を明確化し、それら設備が準備できることを条件とする。不足する機材がある場合、妥当な評価が実施できないものとする。

以下に、本評価ガイドラインで定める評価項目の実施に必要な機材を記載する。

機材名称	内容
Digital Microscope	プリント基板、ICチップの構成を確認するために使用する
Logical Analyzer	デジタル通信信号のモニタリング及びプロトコルのデコードを行うために使用する
HAKKO Soldering Iron station	プリント基板からICチップを剥がすために使用する
Hot-Air Gun	プリント基板からICチップを剥がすために使用する
Bus Pirate	HWインターフェース間で送受信されるデータの内容を確認するために使用する
Jtagulator	プリント基板のJTAGポート、UARTポートのピンレイアウトを診断するために使用する
RIFF BOX 2	JTAGポートからのファームウェアダンプおよびデバッグを実施するために使用する
BeeProg2C	フラッシュメモリからのバイナリファイルの抽出に使用する
Arduino UNO CANBUS Shield	CANプロトコルの解析を実施するために使用する

Ubertooth One	Bluetoothのパケットをキャプチャするために使用する
USRP N210	SMS解析時にFakeBTSソフトウェアを利用したModem Hackを実施するために使用する（3G/LTE）
Alfa Network AWUS036H	WiFiパケットをキャプチャするために使用する
IDA Pro（x86、ARM32、ARM64）	ファームウェアのリバースエンジニアリングを実施するために使用する
Burp Suite	Webアプリケーションの脆弱性テスト用ツール（本資料ではプロキシサーバーとして使用）
Nessus Vulnerability Scanner	脆弱性診断スキャナ
Metasploit	ペイロード、攻撃コードの作成、あるいは攻撃用Webサイトの作成時に使用する
FTK Imager	バイナリファイルからファイルを取得する際に使用する
enCase	バイナリファイルから機密情報を取得する際に使用する

「評価期間」

評価結果を判定するために必要な評価実施期間を明確かする。

本実証実験においては、「4.2.4 評価におけるクライテリアの明確化」に記載のとおり、評価項目を実行するに十分なスキルを有する評価者が以下の人日をもって評価実施することで十分な評価完了を可能と定義した。

・評価者数：　2名
・評価期間：　偵察フェーズ 140 時間（7 時間×20 日）、侵入フェーズ 140 時間（7 時間×20 日）

「判定基準」

情報セキュリティ評価の判定基準を明確化する。

本実証実験においては以下の内容で判定基準を定めた。

評価フェーズ	評価結果(安全性)の判定基準
偵察	本項で定義した偵察フェーズに係る評価スキル・期間を充足する評価を実施した結果、偵察が成功しなかった場合
侵入以降	本項で定義した侵入以降のフェーズに係る評価スキル・期間を充足する評価を実施した結果、いずれのインターフェースからも侵入が成功しなかった場合

表 5-8　情報セキュリティ評価の判定基準

5.3.3. 評価項目定義

5.4.　「5.1 評価対象定義」、「5.3.2 評価条件定義」、の結果に基づいて、情報セキュリティ評価において実施される評価項目を定義する。

本フェーズでは具体的に以下の作業を実施する。

実施対象となる評価項目の確認

5.7. 「5.1 評価対象定義」で定義されたコンポーネントやインターフェースに基づき、評価実施対象となる評価項目を確認する。

本実証実験および情報セキュリティ評価ガイドラインにおいては、以下の項目実施を判断する。

- 偵察フェーズ
  「1.1 HW 調査」、「1.2 SW 調査」の評価項目のうち、実施可能な項目を選定する。

- 侵入フェーズ
  評価対象として定義されたコンポーネントや I/F の性格に応じて、「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」から評価項目を選定する。

評価条件の反映

実施対象となる評価項目の確認」で定めた評価項目のうち、「5.3.2 評価条件定義」の結果を踏まえ、評価実施計画に含める評価項目を決定する。その際、以下の条件に考慮する。

・評価の目的
・評価品目
・評価設備
・評価者のスキルレベル、人数
・評価期間、評価開始期限、評価終了期限

組織の実情に応じて、効率化のため本項内容を「実施対象となる評価項目の確認」と並行して実施することも可能とする。

評価実施計画の策定

評価作業のリーダーは、実施する評価項目やその実施順序、実施パターン、実施担当者等を含む評価実施計画を立案し、評価管理者の承認を得る

評価計画の一部内容を以下に例示する。

図 5-1　実施計画：評価実施手順・担当表

5.9.1.　評価実施

前項までに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。

評価準備

評価開始前の準備として、評価チームは以下を実施する。

- 評価環境の構築：評価設備の購入・配置、電源・ネットワーク環境の設営、セキュリティ確保のために必要な設備の設置または必要な措置の実施
- 評価品目の準備：評価品目の評価環境への搬入、セットアップ、搬出時注意事項の確認など
- 関係者調整：　外注先を含む、評価実施に係る社内外関係者との連絡窓口の設定・各種調整など

評価実施

前段のプロセス実施結果に基づいて、情報セキュリティ評価を実施する。
評価チームの構成と役割は以下のとおり。

役割	担当業務
情報セキュリティ評価管理者	・　評価計画、評価実施計画の承認（兼務不可） ・　評価者スキルの判定（兼務不可） ・　評価費用に係る予算管理 ・　評価報告書のレビュー
情報セキュリティ評価リーダー	・　評価実施計画の立案、更新 ・　評価環境の構築 ・　外部委託先との調整 ・　評価報告書の作成
情報セキュリティ評価者	・　評価作業実施 ・　評価結果の記録

表 5-9　評価チームの役割表

5.9.2. 評価結果報告

実施した評価項目の評価結果を統合し、総合評価結果としての評価報告書を作成する。評価報告書には以下の内容を含む。

- 評価における試行作業の全体（侵入失敗フローを含む）
- 評価の実施手順・利用したツール・プログラム
- 発見された問題点
- 対策への提案（問題点の修正方法）

5.4. 実証実験実施を通した評価ガイドライン改善結果

本年度実証実験の実施結果を受け、情報セキュリティ評価ガイドラインの評価項目 19 件に関して改善した。具体的な改善項目と内容は以下のとおり。

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

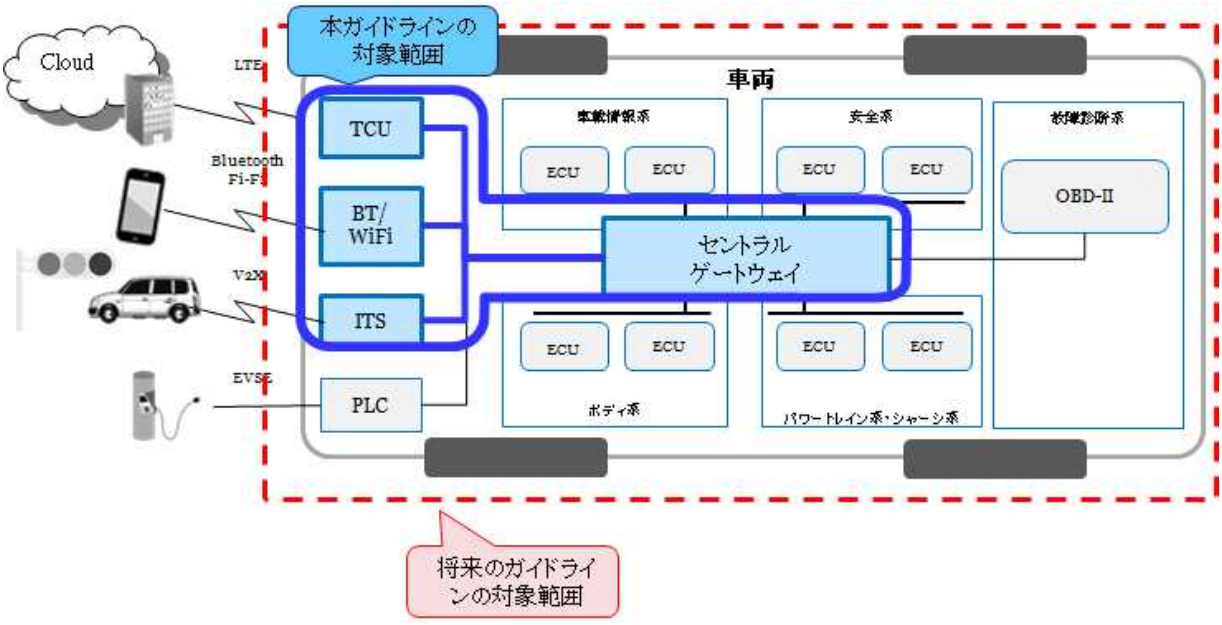
表 5-10　評価ガイドライン評価項目　改善項目一覧

なお、具体的な改善内容については実証実験参加社の影響を考慮し記載しないものとした。

5.5. 昨年度他社検討結果を参考にした改善結果

情報セキュリティ評価ガイドラインの最終化にあたり、昨年度 SIP 情報セキュリティ実証実験の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。

具体的には、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む際に、他社成果を活用した。



6 まとめ

6.1. 本事業の成果

本年度の事業においては、自動走行システム　情報セキュリティ実証実験として、「実証験事務局の運営」「情報セキュリティ評価の実施」「情報セキュリティ評価ガイドラインの最終化」の活動を行った。

「実証験事務局の運営」
昨年度の活動である実証実験の事前準備の内容に基づき、実証実験参加社募集の実施、実証実験参加社との各種手続き、契約締結、参加社から借用する評価対象システム等の管理、情報セキュリティ管理を行った。実証実験事務局の運営では、参加社である車両 OEM との事前調整や機材提供を通じて、情報セキュリティ評価の実施に必要な手続きが整理できた。一部機材提供においては、実証実験を通じた実態の把握により、情報セキュリティ評価の評価プロセスの評価条件定義にその内容を反映した。

「情報セキュリティ評価の実施」
実証実験参加社の参加依頼を受け参加いただいた車両 OEM4 社の協力のもと、昨年度策定した情報セキュリティ評価ガイドラインドラフト版を元にした評価作業を実施した。評価にあたり、昨年度の試行調査の結果を受け判明した情報セキュリティ評価における実施課題を踏まえ、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を明確化・定義した。評価条件の明確化では、昨年度の試行調査の結果を踏まえ、条件設定をするとともに、実証実験の運営および結果を通じて妥当性を検討した。

「情報セキュリティ評価ガイドラインの最終化」
情報セキュリティ実証実験の実施結果をもとにした情報セキュリティ評価ガイドラインの最終化を行った。実証実験実施結果としては、次の 4 項目について結果をまとめた。
１．情報セキュリティ評価ガイドラインの妥当性検証の結果。妥当性検証では参加社からのアンケートや自己点検結果をまとめた。参加社からのコメントとして、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であったこと、業界課題の解決に資する活動であるとの評価が得られた一方、今後の課題として開発設計等前工程でも活用できるガイドラインの策定について期待があることが明らかになった。
２．実証実験実施を通した評価プロセス整理結果。評価プロセスの整理結果では、事前に整理した評価プロセスや評価条件について実証実験での実施結果を踏まえて再整理し、本ガイドラインで記載する情報セキュリティ評価におけるペネトレーションテストの評価プロセスについてまとめた。ペネトレーションテストの評価プロセスは今後業界活用いただく可能性を考慮し継続検討いただくよう検討が進められている。
３．実証実験実施を通した評価ガイドライン評価項目改善結果。評価ガイドライン評価項目改善結果では、昨年度策定した情報セキュリティ評価ガイドラインドラフト版の評価項目について、実証実験の実施を通じて評価項目として内容に不足が見られた項目については、改善・追加した項目についてまとめた。
４．昨年度他社検討結果を参考にした改善結果。昨年度他社検討結果について、本年度の実証実験の実施に向けて見直しを行い、弊社の取り組みとして参考にすべき項目を洗い出し、取り組みとして取り込んだ。具体的には、評価プロセスにおけるリスク分析の取り組みについて、昨年度他社検討結果を参考にまとめた。

6.2. 総括

本実証実験では、昨年度策定した情報セキュリティ評価ガイドラインを使い、情報セキュリティ評価（ペネトレーションテスト）の取り組みについて、昨年度から規模を拡大して実証実験として実施することができた。規模が拡大されたことにより、昨年度と比して、情報セキュリティ評価ガイドラインの妥当性をより精緻に確認することができ、情報セキュリティ評価ガイドラインの改善ができたとともに、業界の課題の一つであるペネトレーションテストの標準化・均一化に資する評価プロセスを形作る一歩とすることができた。

本事業で策定した情報セキュリティ評価ガイドラインを元に、業界団体での検討を通じて、今後自動車業界でペネトレーションテストを実施する際により効果的・効率的に利用可能な評価ガイドラインに改善し、策定し、将来の自動走行システムに開発で実際に活用されることが求められる。

自動車のサイバーセキュリティの確保は、自動車の安全（セーフティ）にも影響を与えることも考えられるため、最低限満たすべきセキュリティ水準については日本の業界全体の協調領域とすることが適切であり、これにより開発効率の改善を図ることも可能となり、日本企業の国際的な競争力維持にもつながる。また、定められたセキュリティ対策は、国内の業界における共有にとどめるのではなく、昨今の自動車セキュリティ開発における国際標準・標準規格に提言するなどで、日本企業の強みとして活用できるよう、戦略的に標準化団体に働きかけることも重要である。

以上を踏まえ、自動走行システムに係る情報セキュリティ活動は、重要な役割を持つものであり、業界のセキュリティ活動の発展に寄与することを期待するものである。

以上

契約管理番号：18100331-0