成果概要説明書

「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」

デロイト トーマツ リスクサービス株式会社

2018年2月

目次

実証実験の「ねらい」と「目的」

車両への通信を用いた攻撃に対する評価手法確立のために実証実験を行います

「SIP自動走行システム」研究開発のねらい

①交通事故低減等　国家目標の達成
②自動走行システムの実現と普及
③2020年東京オリンピック・パラリンピック競技大会を一里塚として東京都と連携し開発

（「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　研究開発計画」（2017年4月1日）より）

自動走行システム実用化の加速に向けた「大規模実証実験」

- 技術面、運用面、制度面等での**具体的課題抽出**
- **国際連携・協調の推進**
- 自動走行システムに対する一般の方々の正確な**理解促進と社会受容性の醸成**、等

5つの技術領域
①ダイナミックマップ
②HMI
③情報セキュリティ
④歩行者事故低減
⑤次世代都市交通

「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」
（以下「本事業」）

本事業の目的

自動走行における**セキュリティ脅威の調査及び分析**を行い、国際標準化も見据えて車両レベル・コンポーネントレベルでの**セキュリティ評価手法・プロトコルを策定**し、本**実証実験**を通して募る参加者の車両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で、下記を実現する

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. **我が国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**

（『「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」に係る公募要領』（平成29年7月）より）

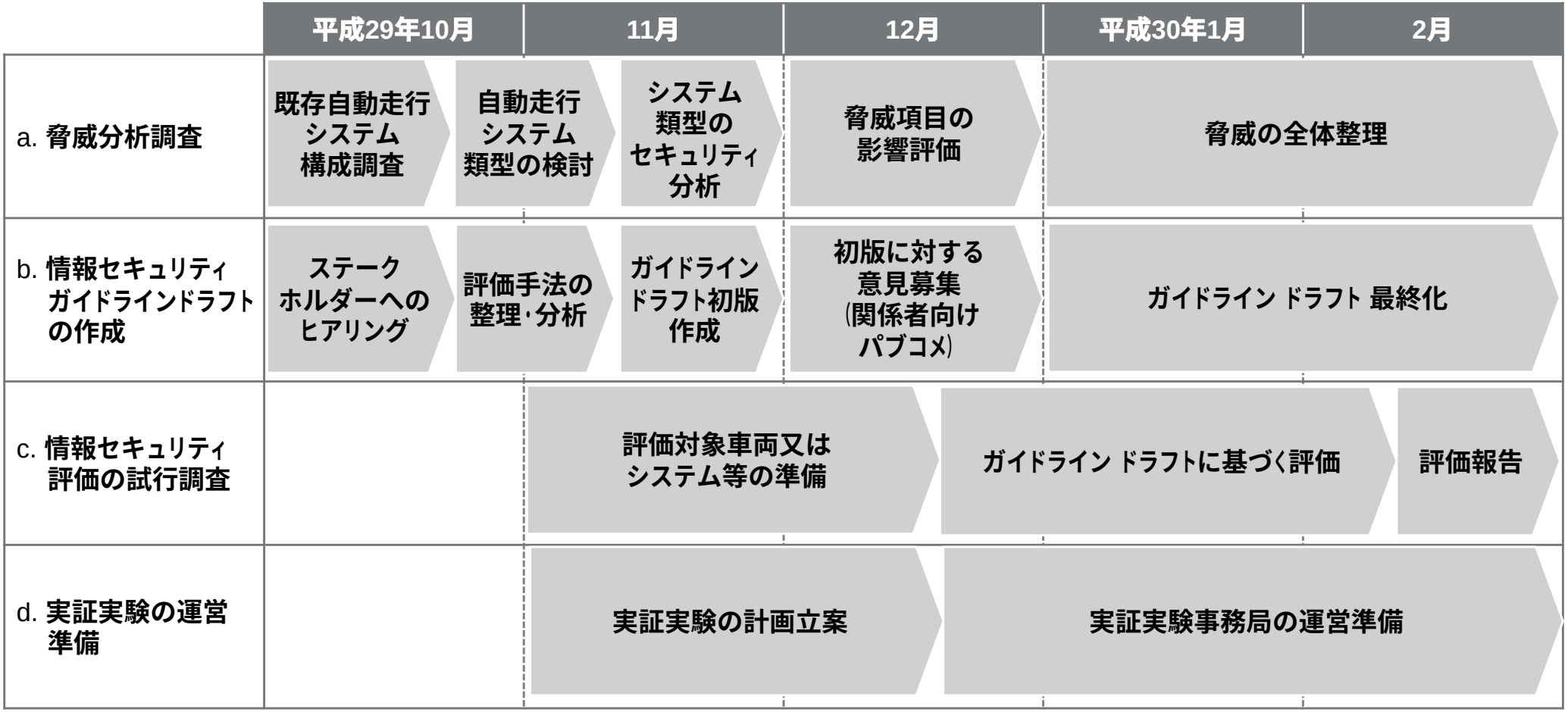
（本事業の目的と各業務との関係）

STEP1（平成29年度）				STEP2（平成30年度）		
a. 脅威分析調査	b. 情報セキュリティ評価ガイドラインドラフトの作成	c. 情報セキュリティ評価の試行調査	d. 実証実験の運営準備	a. 実証実験事務局の運営	b. 車両毎の情報セキュリティ評価の実施	c. 情報セキュリティ評価ガイドライン作成と評価分析

（今フェーズでの推進業務）

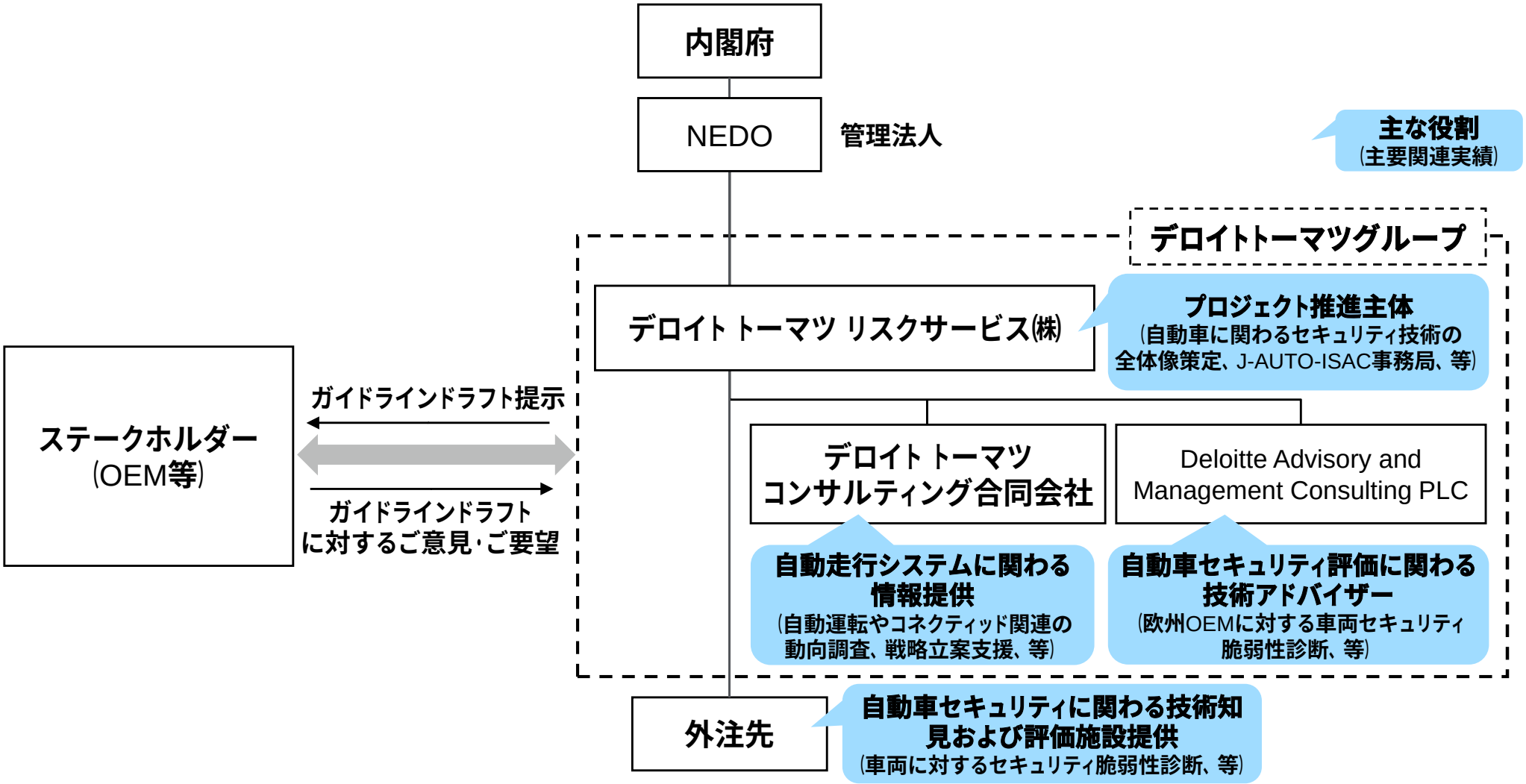
全体スケジュール

本プロジェクトにおける各タスク毎のプロセス



実施体制図

デロイトトーマツグループのコンサルティング部隊および技術的知見や実績を有する海外法人と連携し事業を推進



脅威分析調査

脅威分析調査のアプローチ

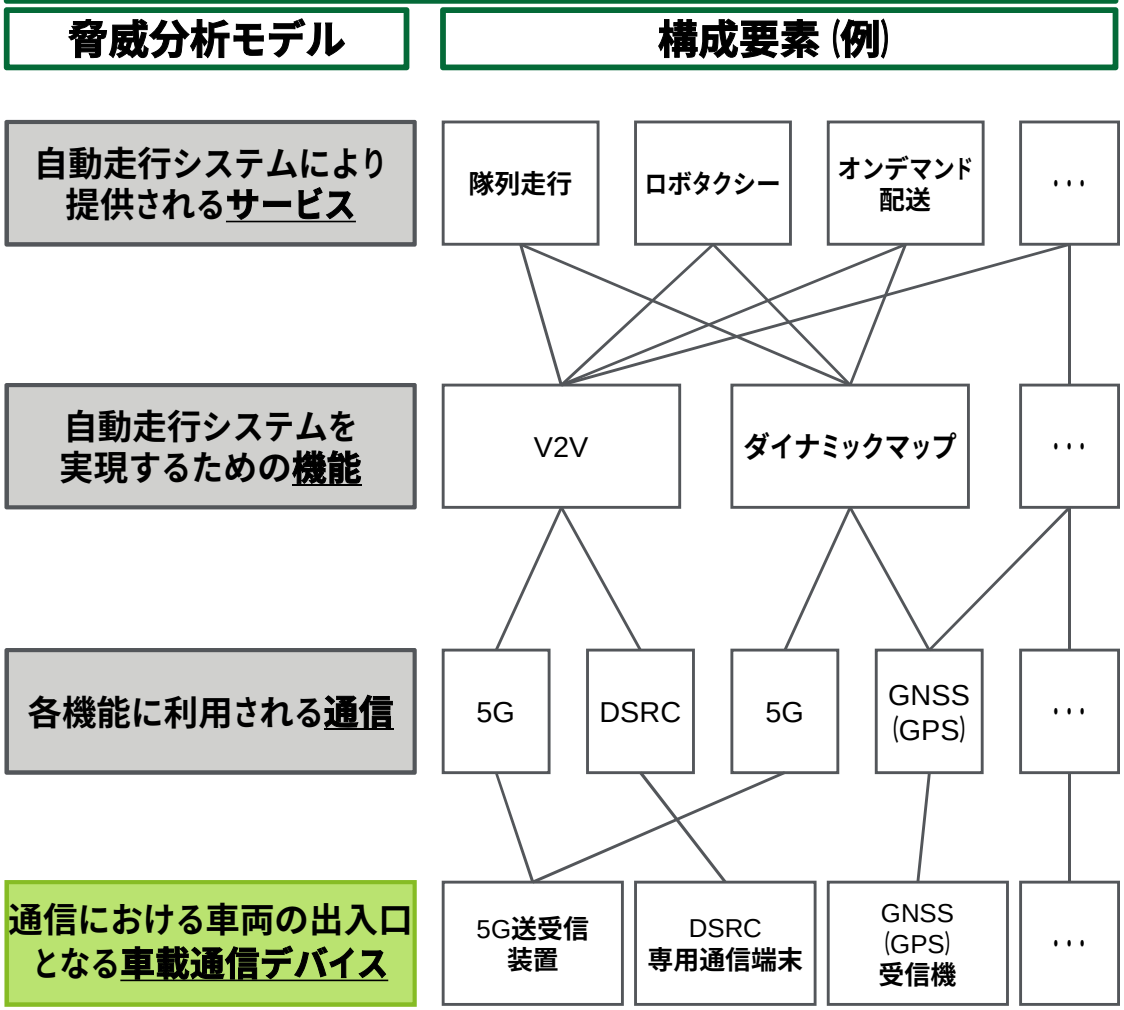
自動走行システムに対するサイバー脅威の全体像を導出するため、自動走行システムの構成要素を調査し、想定される脅威の分析を実施

	自動走行システムのモデル化・構成調査	脅威の分析
実施事項	・自動走行システムのモデル化 ・自動走行システムを構成するサービス及び機能の調査 ・通信の種類及び車載通信デバイスの整理	・自動走行車両に対する通信経由での外部攻撃のシナリオ化 ・脅威のレベルを評価 ・脅威の分類 ・自動走行システムに係る脅威の全体像を整理
主要成果	・サービス調査結果 ・機能調査結果 ・通信調査結果 ・車載通信デバイス調査結果	・脅威シナリオ一覧 ・脅威評価指標 ・脅威評価結果 ・脅威全体像

自動走行システムの脅威分析モデルと調査・整理手順

自動走行システムをモデル化し、各層の構成要素を調査・整理することで、通信における車両の出入り口となる車載通信デバイスを導出

自動走行システムの脅威分析モデルと構成要素



調査・整理手順

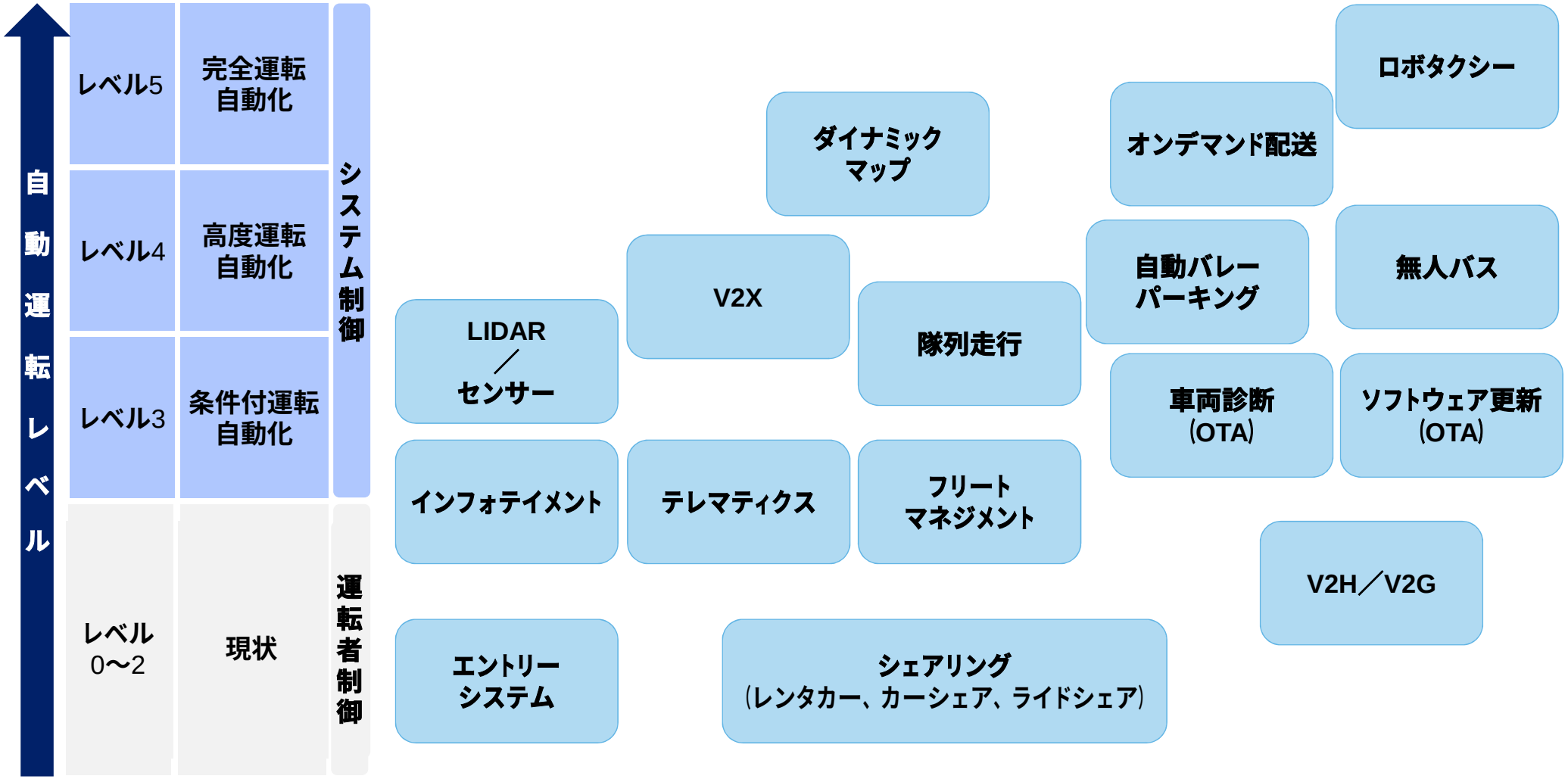
1 自動車メーカー・サプライヤー等の取組みや実証実験等を調査する

2 各サービスを構成する機能を洗い出す

3 機能毎に利用される通信が異なるため、それぞれの機能で利用される通信を特定し、車載通信デバイスを整理する

自動走行システムにおいて展開されるサービス（一部機能を含む）

自動走行システムにおけるサービスを網羅的に調査・整理することで、サイバー脅威全体像の導出を実施



自動走行システムの進化に応じてコモディティ化するサービスや機能

自動走行システムの機能調査結果

自動走行システムに実装される機能を以下の様に集約

機能の詳細は「自動走行システム構成調査表.xlsx」参照

自動運転レベル

	乗車／走行準備	走行	駐車	メンテナンス
システム制御	• 目的地の設定	• ダイナミックマップ • V2X（周辺機器との通信） ➢ V2P（車歩行者間通信） ➢ V2I（路車間通信） ➢ V2V（車車間通信） • エンタテイメント ➢ コンシェルジュ ➢ インターネット接続 ➢ POI情報の取得、等 • 車載データの保管・送信（走行履歴、外部環境、車両状態、等） • 周辺環境の検知 • 緊急通報 • ドライバー監視	• 駐車支援 ➢ 駐車アシスト ➢ リモコン駐車 ➢ 自動駐車 • 駐車場の利用支援 ➢ 空車情報の取得 ➢ 予約 ➢ 決済	• 配車（ロボタクシー等） • 車両管理（OTA） ➢ ソフトウェア／ファームウェア更新 ➢ 車両診断 • V2G（グリッドとの連携） • V2H（ホームシステムとの連携） ➢ 充電・給電 ➢ 家庭内IoT機器との連携 • ナビゲーション（データ更新）
運転者制御	• 持込み機器との連携 ➢ ポータブル機器接続 • エントリーシステム ➢ ドア類の開錠・施錠 ➢ 車両の始動			

無線通信および車載通信デバイス整理結果

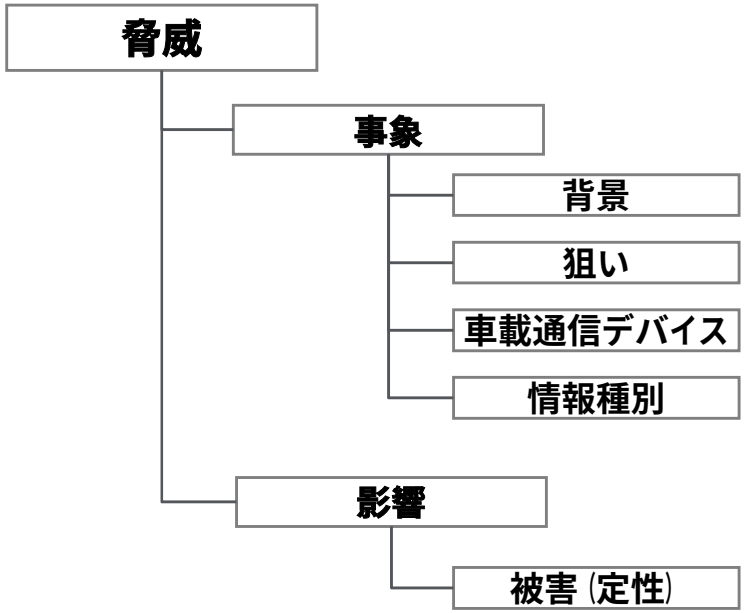
自動走行システムに利用される通信および車載通信デバイスを下表の通り集約

分類	通信の種類	車載通信デバイス	車両からの接続先	主な通信情報（例）
公衆回線	5G	5G送受信装置	周辺車両、携帯事業者の基地局、サービス事業者のサーバ	走行制御情報、ダイナミックマップ情報等
	3G/4G	3G/4G送受信装置	携帯事業者の基地局、サービス事業者のサーバ	ソフトウェア更新情報、交通情報、趣味・嗜好に関する情報（インフォテイメント）
Wi-Fi	Wi-Fi	Wi-Fi送受信機	Wi-Fiアクセスポイント、サービス事業者のサーバ	ソフトウェア管理情報、車両位置情報、交通情報、趣味・嗜好に関する情報
V2X通信	Cellular V2X	Cellular V2X送受信装置	周辺車両、インフラ等	交通情報、走行制御情報等
	DSRC	DSRC通信端末（V2X）	周辺車両、インフラ等	
デバイス間連携	Bluetooth（VCK、ポータブル機器用）	Bluetooth送受信装置	スマートフォン、ポータブル機器等	エントリーシステムに用いる認証情報、ポータブル機器との連携情報等
	Bluetooth（OBD-II用）	OBD-II／ドングル	Wi-Fiアクセスポイント、サービス事業者のサーバ	ソフトウェア管理情報、診断情報
	ZigBee	ZigBee無線モジュール	社会インフラの電力網、住宅	ボディ制御情報
センシング	ミリ波レーダ(77／79GHz)	ミリ波レーダ送受信装置	周辺車両、歩行者、障害物	走行制御情報
	準ミリ波レーダ			
	LIDAR	LIDAR送受信装置		
	超音波センサー	超音波センサー送受信装置		
	生体認証センサー	生体認証センサー	搭乗者（指紋、虹彩、表情など）	生体情報
衛星通信	GNSS(GPS)	GNSS（GPS）受信機	GPS衛星	車両位置情報
情報提供（VICS等）	準マイクロ波	準マイクロ波端子	路側機（電波ビーコン）	交通情報（渋滞、事故等）
	赤外線	赤外線端子	路側機（光ビーコン）	
	DSRC	DSRC通信端末（VICS/ETC）	路側機（電波ビーコン）、周辺車両	交通情報、走行制御情報、資産情報
エントリーシステム	NFC	NFCリーダ・ライタ端末	非接触ICカード、スマートフォン	資産情報
	RF/LF (RFID)	RF/LF (RFID)リーダ・ライタ	リモートキー	ボディ制御情報

脅威シナリオの構造

わかりやすさを重視し、「事象」と「影響」の構造でシナリオを整理

前提	■ 重要度評価結果に基づき、車載通信デバイス毎に脅威シナリオを作成 ■ 脅威シナリオは、解釈にバラツキが生じないように、構造上のルールを統一 ■ 以下のルールに沿って、以降の脅威シナリオの作成、評価、整理に至る一連の作業を推進



脅威シナリオの考え方

- ◆ 攻撃の背景・狙い、及び関係する情報種別等を明確にする
- ◆ 当該デバイス単位で、どのようなセキュリティ侵害（漏えい・改ざん等）が発生するかを、「事象」（何が起きて）と「影響」（どうなるか）の一連の流れのシナリオで表現する
- ◆ 専門的な表現は必要最低限に控え、多くの人がイメージできるように表現する
- ◆ 事象の結果起こり得る影響を、定性的なストーリーで整理することで、具体性を補強する

脅威シナリオ例 Tampering （改ざん）	【事象】 Bluetoothを利用した車両とスマホ間で授受される認証情報（VCK：ヴァーチャル・カー・キー）をランサムウェアで暗号化される 【影響】 車両の利用が出来なくなり、金銭が要求される

STRIDEを軸とした脅威シナリオ

各車載通信デバイスを毎に、STRIDEを軸として「事象」と「影響」の構造で脅威シナリオを作成

詳細は「脅威シナリオ一覧.xlsx」参照

脅威分類	脅威シナリオの例示
Spoofing (なりすまし)	【事象】 車両とGNSS(GPS) 衛星の通信を妨害し、偽装した電波を流し込むことで、攻撃者がGPS衛星になりすます 【影響】 位置情報取得が利用できず、車両の目的地や経路が決定できない
Tampering (改ざん)	【事象】 遠隔から通信上のソフトウェア更新情報を改ざんし、走行制御に関するソフトウェアを異常な状態とする 【影響】 攻撃者の意図に従って走行中に異常な走行機能制限が発生し、安全走行に支障が生じる
Repudiation (否認)	【事象】 車載ETC機と料金所ETCシステム間の通信を否認し、通行料の支払いを拒否する 【影響】 詐欺行為による経済的損失が発生する
Information Disclosure (情報漏えい)	【事象】 攻撃対象の車両に接近し、ホットスポットやフリーWi-Fiを模したアクセスポイントを提供し、これに接続した車両からのWi-Fi通信上の情報を窃取する 【影響】 車両の目的地や経路、ユーザーIDやパスワード等が漏えいする
Denial of Service (サービス妨害)	【事象】 特定車両に対して大量のパケットを送信し、テレマティックスサービスを停止させる 【影響】 車両の通信機能が停止し、通信機能を用いるすべてのサービスが提供できなくなる
Elevation of Privilege (権限の昇格)	【事象】 遠隔から不正なコードや命令を流し込み、4G送受信装置の管理者権限を奪取し、これを踏み台にして車載ネットワークで接続されている他のデバイスにアクセスする 【影響】 4G送受信装置以外のデバイスや機能が攻撃者に利用されることで、攻撃者の意図に従って事故回避行動を誤作動させられ、安全走行に支障が生じる

脅威シナリオの評価方法

シナリオ化した脅威を、「顕在化率」と「影響度」から脅威レベルを評価

顕在化率

各車両の特性・構成に依らず、攻撃者から見ていかに攻撃が**成功しやすいか**を各観点別に分析し、総合的に評価

観点		評価方法
①	容易性	攻撃を成功させるための容易度
②	機器・ツール	特殊なツールや機器の必要性
③	準備期間	攻撃を行うための準備期間（潜伏等）
④	実行人数	攻撃を行うために必要となる人数
⑤	運行状態	攻撃対象車両の状態（走行中／駐停車中）

＋

影響度

脅威が生じた車両や周辺環境への**安全面での影響**の度合いを総合的に評価

観点		評価方法
①	機能欠損の度合い	走行（走る、曲がる、止まる）に影響
②	被害の程度	乗車者に安全面での影響
③	被害の範囲	脅威が生じた車両周辺のインフラ、車両、歩行者に対する影響

評価の考え方

脅威が顕在化する可能性と、顕在化時の影響度を数値化し、各脅威の「脅威レベル」を評価

脅威レベル

影響度 ＼ 顕在化率	1	2	3
3	4	5	6
2	3	4	5
1	2	3	4

脅威の全体像整理

脅威の「顕在化率」と、安全走行への「影響度」で算出した脅威の傾向

【表中のスコア】各車載通信デバイスにおけるSTRIDE別の脅威レベル平均値。脅威レベルの算出方法はスライド14参照　「—」:該当シナリオなし

通信カテゴリ	車載通信デバイス	脅威の分類					
		Spoofing (なりすまし)	Tampering (改ざん)	Repudiation (否認)	Information Disclosure (情報漏えい)	Denial of Service (サービス妨害)	Elevation of Privilege (権限の昇格)
公衆回線	5G送受信装置	5	6	4	4	5	5
	3G/4G送受信装置※	5	6	4	3	4	5
Wi-Fi	Wi-Fi送受信装置	5	4.5	—	4	4	5
V2X通信	Cellular V2X送受信装置	5	5	3	4	5	4
	DSRC通信端末 (V2X)	5	5	5	3	5	3
デバイス間連携	Bluetooth送受信装置 (VCK、ポータブル機器用)	4	3	4	4	4	3
	Bluetooth送受信装置 (OBD-II用)	6	4.5	—	4	6	5
衛星通信	GNSS (GPS) 受信機	4	4	—	—	4	—
情報提供 (VICS等)	準マイクロ波端子	3.5	3	—	—	3	—
	赤外線端子	3	4	—	—	3	—
	DSRC通信端末 (VICS/ETC)	3	2	2	3	3	—
エントリーシステム	NFCリーダ・ライタ端末	3	4	4	4	4	4
	RF/LF (RFID)リーダ・ライタ	4	3	—	3	3.5	—

※脅威シナリオは3G, 4Gそれぞれで作成しているため、脅威レベルの高いスコアを採用

分析の結果、安全走行に影響する情報の通信に用いられる、車載通信デバイスへの脅威が大きい傾向にある

今後の対応方針

脅威分析結果のセキュリティガイドラインへの反映

脅威分析結果	下記の車載通信デバイスに対するサイバー攻撃が、自動走行システムに大きな影響を与える

脅威レベルの高い車載通信デバイス		セキュリティガイドラインでの評価対象
公衆回線	5G送受信装置	➢ 情報セキュリティ評価ガイドラインドラフト（実践手引き）IPネットワーク編 ➢ 情報セキュリティ評価ガイドラインドラフト（実践手引き）Wi-Fiネットワーク編 ➢ 情報セキュリティ評価ガイドラインドラフト（実践手引き）Bluetooth編
	3G/4G送受信装置	
Wi-Fi	Wi-Fi送受信装置	
デバイス間連携	Bluetooth送受信装置	
V2X通信	Cellular V2X送受信装置	V2X通信は、将来の実用化に向けた実証実験段階であり、仕様も確定していないため（2018年1月時点）、今後の検討事項とする
	DSRC専用通信端末	

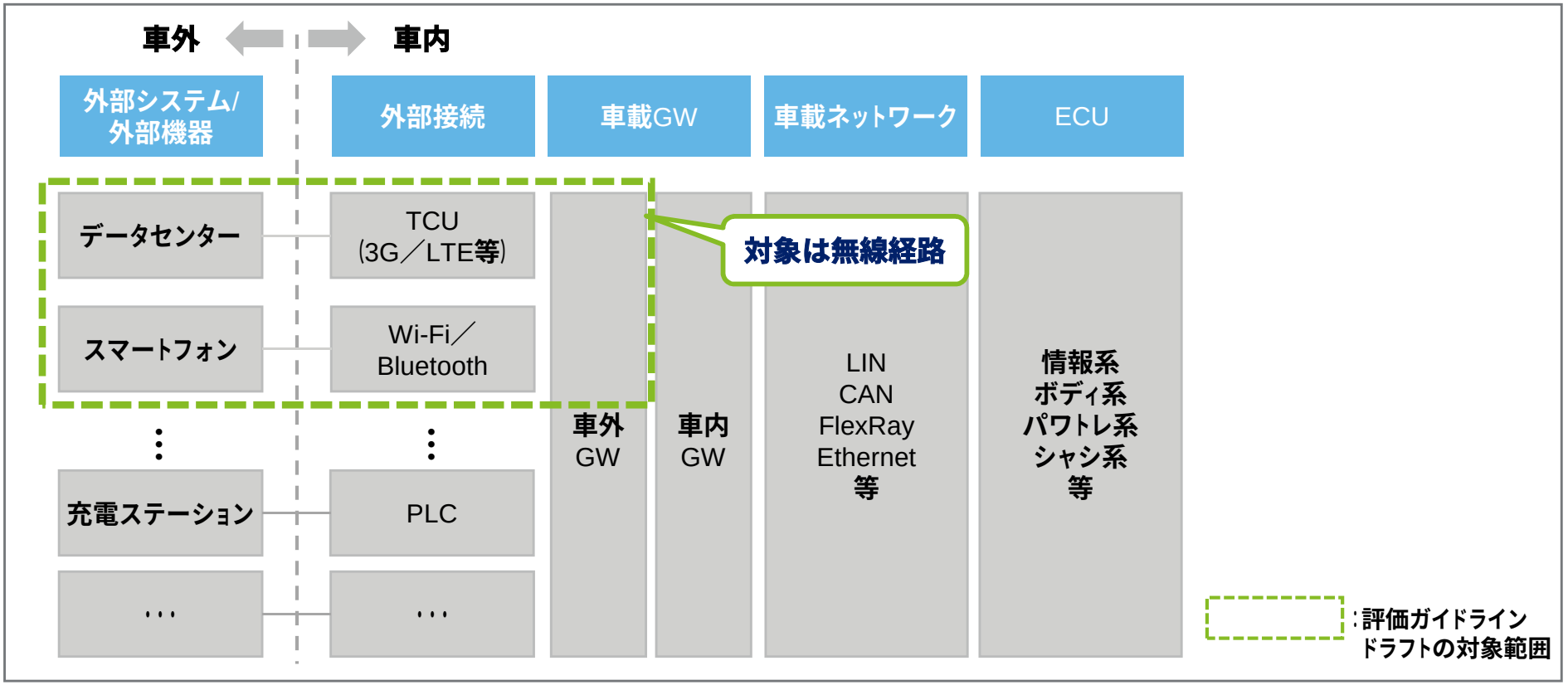
自動走行システムに対するサイバー脅威のレベルが高く、コモディティ化されているネットワークを利用する車載通信デバイスを対象にセキュリティガイドラインを策定

情報セキュリティ評価ガイドラインドラフトの作成

ガイドラインドラフトの対象範囲

評価ガイドラインドラフトの対象範囲を無線経路と定義

対象範囲	■ 車外との通信の入口となる車外GWまでを、無線経路から直接攻撃が及ぶ領域ととらえ、主に、3G／LTE等のセルラー通信やWi-Fi／Bluetooth等の無線経路による攻撃を想定し、車外から車外GWまでを本ガイドラインの対象と定義 ■ 評価ガイドラインドラフトは、評価の方法論を記載したプロトコルに依存しない「本編」と、各プロトコルにおける評価手法詳細を記載する「実践手引き編」より構成



評価ガイドラインドラフトの強み

評価ガイドラインドラフトにおける7つの強み

1 利便性

- 実車を用いる車両総合評価や市販車評価だけでなくシステム設計から活用可能
- V字プロセスの中での活用場面、実施者（OEM・サプライヤー等）を明確化

2 効率性

- ペネトレーションテスト実施にあたり、リソース（人・時間・費用）に制約がある中、効率的かつ効果的なテストを実施するためのアプローチを提供

3 再現性

- 評価プロセスから極力属人的な判断を排除し再現性と客観性を確保

4 実効性

- 欧州OEMに対する業務提供実績があり、過去の問題点や課題をノウハウとしてガイドラインに反映
- ステークホルダーとの会話やパブリックコメントを通じて、評価ガイドラインを見直し、実効性を確保

5 十分性

- 自動車での既知の脆弱性に加え、ITシステム分野での既知の脆弱性を考慮
- 評価項目の立案方法についても解説することで、OEM独自の観点を加えることも可能

6 具体性

- 実践手引きについては人材育成の観点からもOEMにおいて活用できるレベルで詳細な説明を記載
- 評価手法についてイメージが沸くように、実行すべきコマンドや、実行結果の具体例を記載

7 拡張性

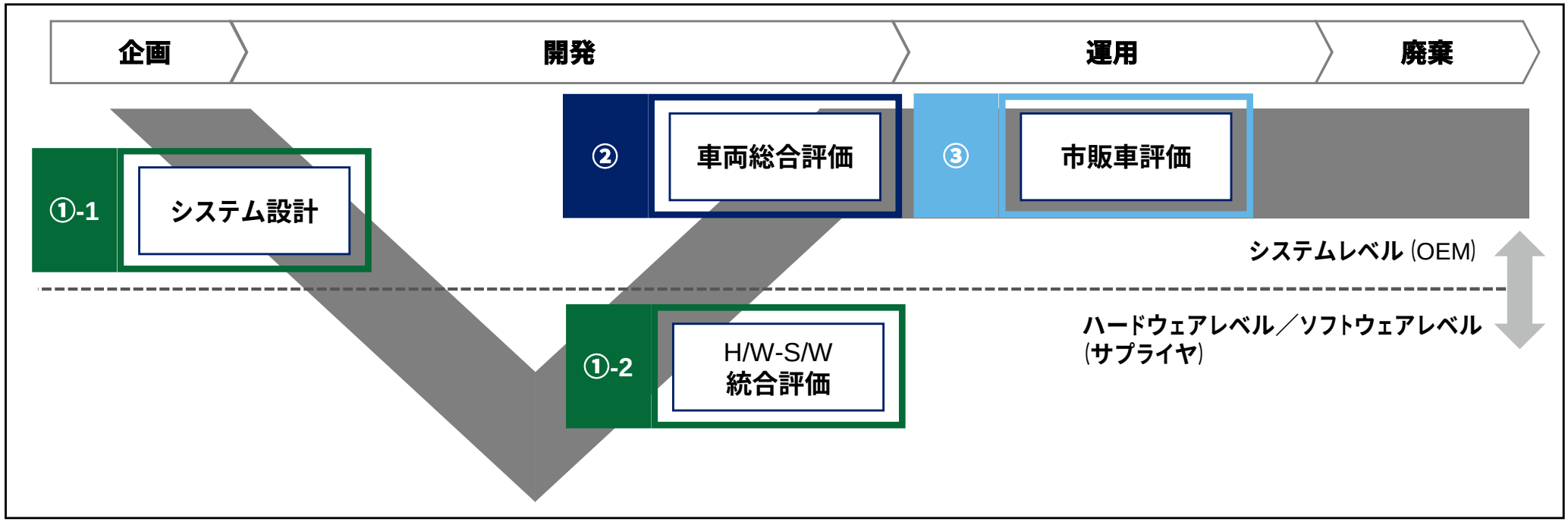
- ペネトレーションテスト全体のアプローチに加え、各通信プロトコルの技術的評価手法を個別に作成
- 今回のスコープである無線インターフェースに加え、車両内部も含めたスコープへの拡大も容易

評価ガイドラインドラフト作成のポイント(1/7)

実車を用いる評価のみならず、開発段階から活用可能な評価ガイドライン

1 利便性

- ■ 実車を用いる車両総合評価や市販車評価だけでなくシステム設計から活用可能
- ■ 評価におけるOEM･サプライヤーによる活用の場面を考慮



①-1	システム設計段階で、評価プロセスにおける評価計画の立案までを実施することで、車両総合評価で実施する評価項目の早期検討に活用可能
①-2	ハードウェアとソフトウェアの統合段階でセキュリティ要件の検証を行うことで、車両総合評価で実施する評価項目を前倒しで実施可能
②	製品リリース前の車両総合評価におけるペネトレーションテストガイドとして活用可能
③	市販車を対象とした運用時におけるペネトレーションテストガイドとして活用可能

評価ガイドラインドラフト作成のポイント (2/7)

効率的かつ効果的なリソースの配分

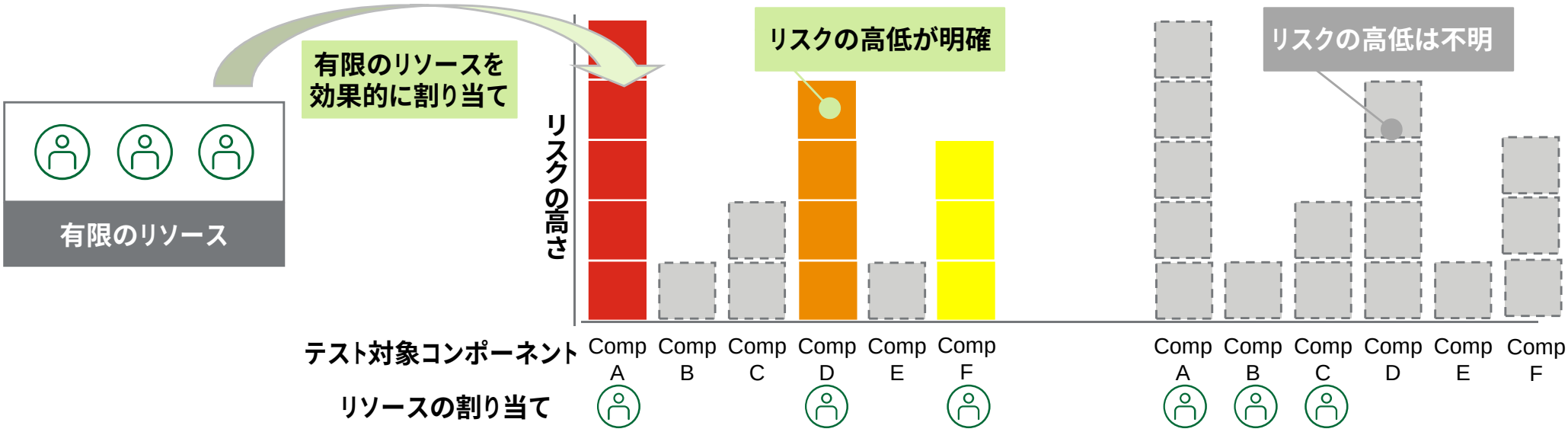
2	効率性	ペネトレーションテストにおいて**リソース (ヒト、モノ、カネ、時間) が有限**であり、評価実施の制約となるが、**攻撃者視点**でコンポーネント単位のリスク評価を行い、**リスクの高いコンポーネントに絞り込む**ことで効率的なテストが可能

絞り込んだ (高リスクの) コンポーネントを中心にテストを実施

【当社の評価ガイドラインドラフト】

リスク分析を行うことで、有限のリソースをリスクの高いコンポーネントに効果的に割り当てることで、効率的な評価が可能となる

リスクアプローチでないプロセスの場合は、リスクの高低がわからず、全方位的にリソースを割り当てることになる

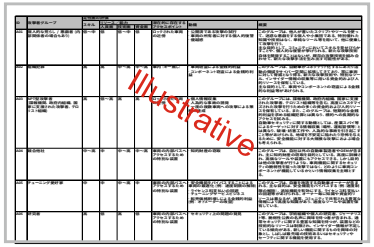


評価ガイドラインドラフト作成のポイント (3/7)

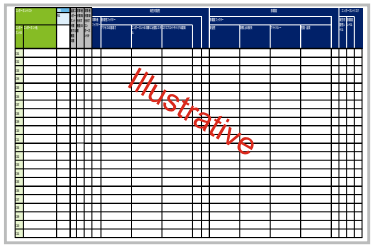
リスク分析および評価における各種テンプレートを整備

3	再現性	テンプレートを整備することで極力属人的な判断を排除し、再現性と客観性を確保

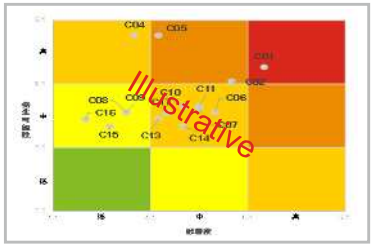
リスク分析における検討事項をテンプレート化



攻撃者プロファイルテンプレート

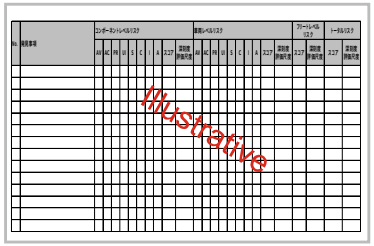


リスク分析テンプレート

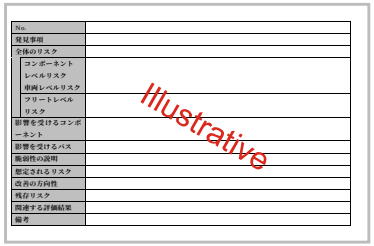


リスクヒートマップテンプレート

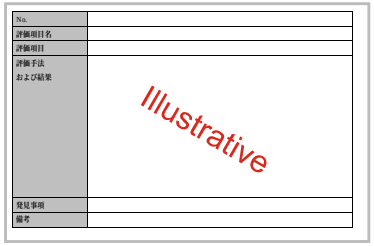
発見事項や評価結果においてまとめるべき項目をテンプレート化



発見された脆弱性に対するリスク評価テンプレート



個別発見事項テンプレート



個別評価結果テンプレート

評価ガイドラインドラフト作成のポイント (4/7)

ベストプラクティスやステークホルダーからの意見・要望を活用

4	実効性	■ ペネトレーションテストが浸透している情報システム分野において、実質的な業界標準として扱われているガイドラインを考慮 ■ 自動車のペネトレーションテストに係る当社の方法論を活用 ■ 実践的な評価ガイドラインとするため、ステークホルダーからのコメントを反映

ITシステム分野の各種ベストプラクティスの活用

ペネトレーションテストが浸透するITシステム分野において実質的な業界標準として扱われているガイドラインや方法論を考慮

ガイドライン	NIST Technical Guide to Information Security Testing and Assessment
ガイドライン	PCI Security Standards Council Penetration Testing Guidance
ガイドライン	OWASP Risk Rating Methodology

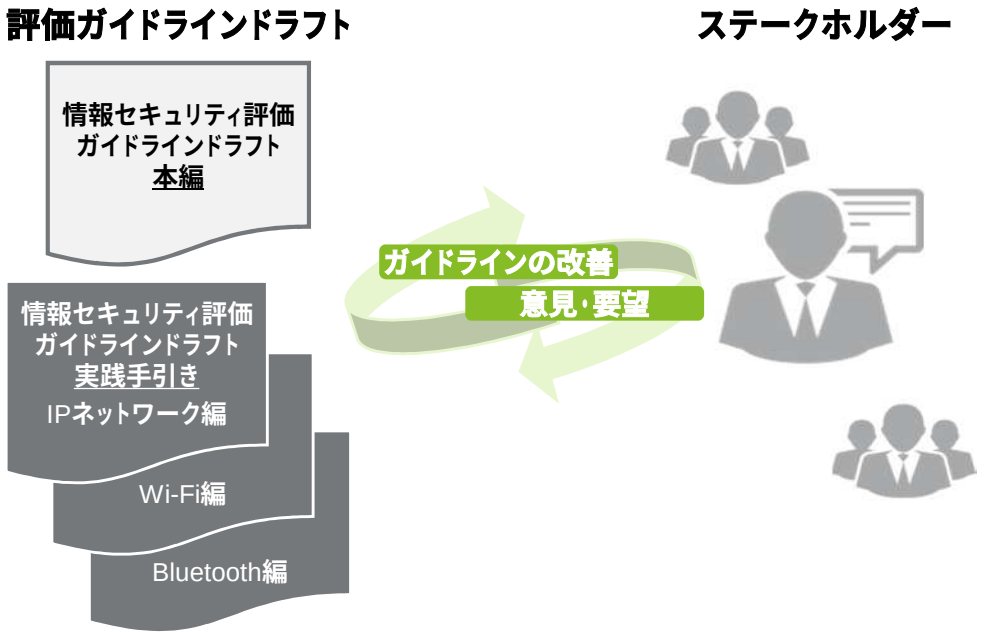
自動車分野で実績のある方法論の活用

欧州OEMでの採用実績もあり、セキュリティ評価における各種課題が実証済み

方法論	Deloitte Automotive Cyber Security Pentest Methodology

ステークホルダーとの定期的なディスカッション

ステークホルダーとの議論やパブリックコメントを通じて、評価ガイドラインドラフトを見直し、実効性を確保



評価ガイドラインドラフト作成のポイント (5/7)

評価対象となる脆弱性の十分性を考慮

5	十分性	■ 自動車の既知の脆弱性に対する評価項目ついては評価ガイドラインドラフト本編 (付録) として明確化 ■ ITシステム分野で既知の脆弱性に対する評価項目については自動車に適用可能な項目を評価ガイドラインドラフト (付録) として明確化するとともに、その整理の方法論についても本文中に明記

脆弱性の分類		考慮する脆弱性の内容	評価項目の作成のポイント
自動車分野で既知		過去のインシデント事例 ➢ 米国A社におけるIVIの脆弱性 ➢ 欧州B社におけるコネクテッドサービスの脆弱性 ➢ 米国C社の無線LAN脆弱性 ➢ 日本D社のモバイルアプリ脆弱性　等	• 過去のインシデント事例から、直接攻撃に係る事項以外にも、セキュリティ研究者によって実施・報告された関連事項も考慮
自動車分野で未知	ITシステム分野で既知	ITシステム分野における既知の脆弱性のうち、自動車に適用可能なもの ➢ コネクテッドサーバー側の脆弱性 ➢ Webアプリ・モバイルアプリの脆弱性　等	• CWEをベースに既知の脆弱性を整理 • 自動車に適用可能な脆弱性の抽出についてはSANS TOP 25やOWASP TOP 10を参照 • 脆弱性に対する評価項目の作成にあたってはCAPEC等の攻撃手法を参照
	上記以外	対象外 ※自動車およびITシステム分野で公表される情報を踏まえ、適時アップデートが必要	

: 評価ガイドラインドラフト本編 (付録) の評価項目一覧で考慮される脆弱性

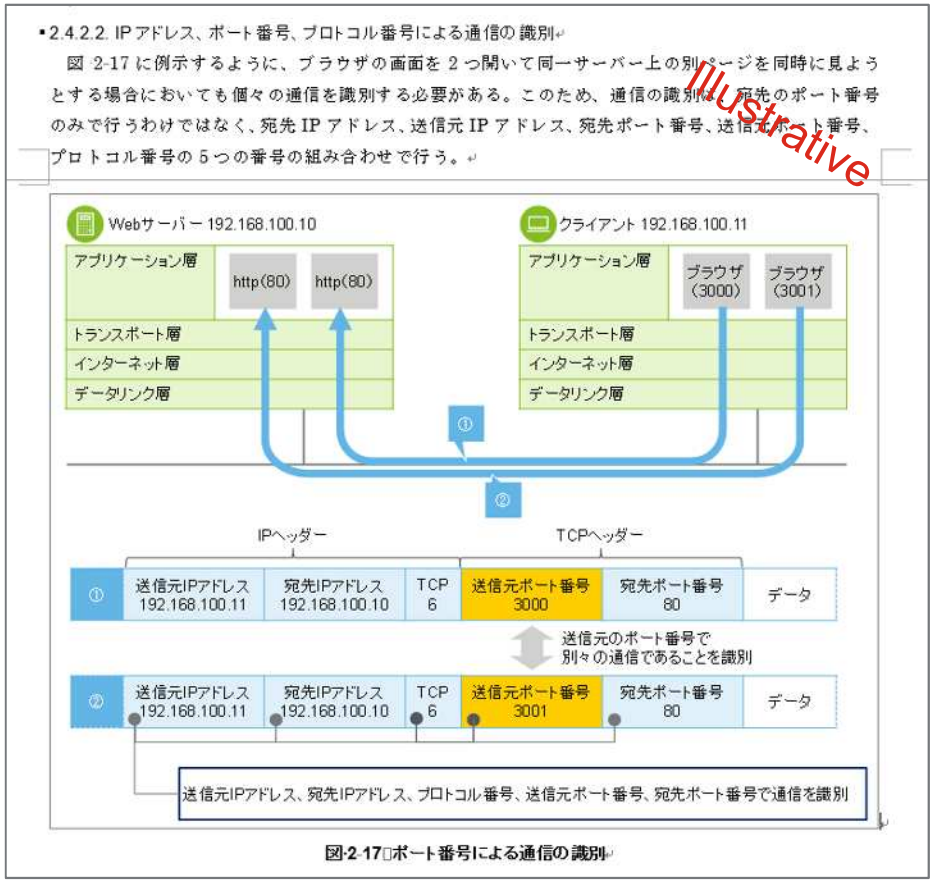
評価ガイドラインドラフト作成のポイント (6/7)

各技術要素の図表や実行すべきコマンド及びその実行結果を例示し、具体的でわかりやすい内容

6	具体性

■ セキュリティ人材育成の観点からもOEMにおいて活用できるレベルで各技術要素の詳細説明を記載
■ 評価実施者が評価手法についてイメージが沸くように、実行すべきコマンドや、実行結果の具体例を記載

■ 各技術要素について、図表を用いて詳細に説明



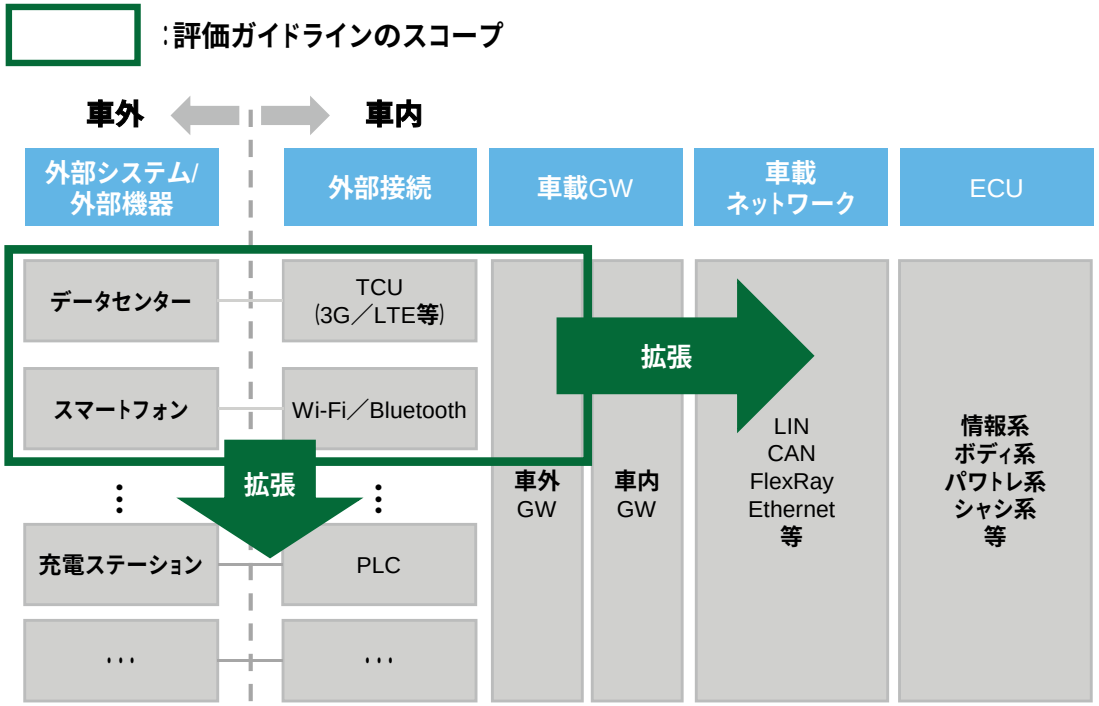
■ 評価手法について実行すべきコマンドや結果の具体例を記載

評価ガイドラインドラフト作成のポイント（7/7）

将来における評価対象の拡大に対応するため、評価ガイドラインの拡張性を確保

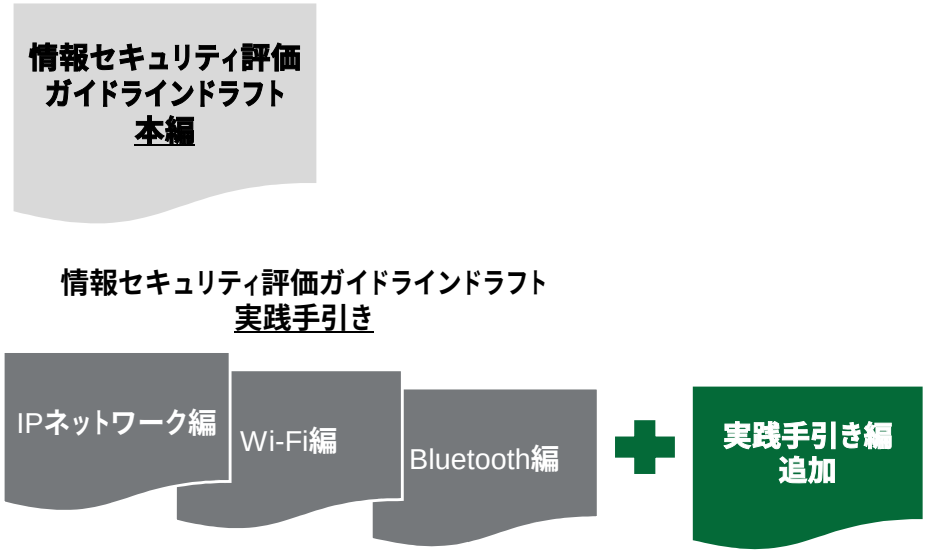
7	拡張性

- 評価ガイドライン（本編）は、プロトコルに依存しない内容のみを記載
- 評価ガイドラインのスコープの拡張にあたってはプロトコルに依存する評価ガイドライン（実践手引き編）を追加することで対応可能



評価対象の拡張性

現状のスコープは無線経路だが、将来的に実践手引き編を追加することで容易にスコープを拡張可能



評価ガイドラインドラフトの成果イメージ

本編・実践手引き編を合わせて4冊（約500ページ）の評価ガイドラインドラフトを作成

情報セキュリティ評価ガイドラインドラフト
本編

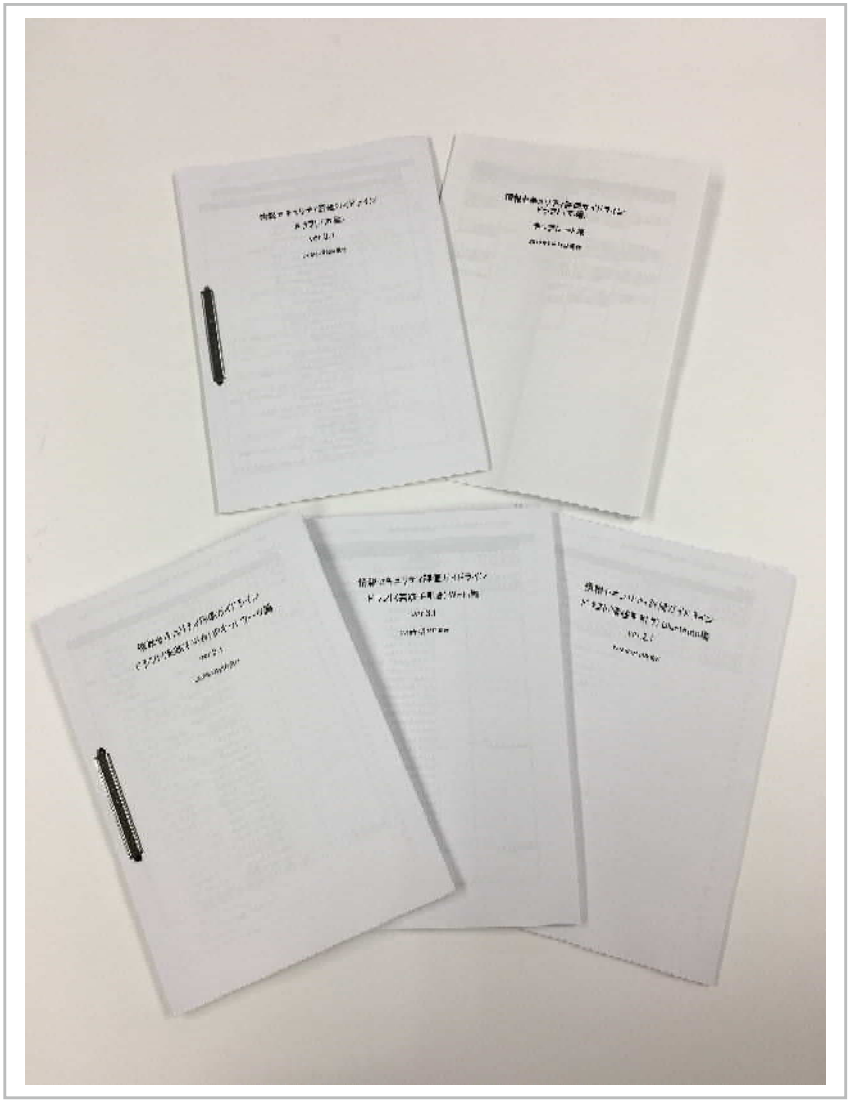
＜内容骨子＞
- 脅威の全体像の説明
- 評価プロセスの説明
- 評価レポートの説明
- 付録1：脅威一覧
- 付録2：評価項目一覧

【Bluetooth編】

【Wi-Fi編】

【IPネットワーク編】
情報セキュリティ評価ガイドラインドラフト
実践手引き

＜内容骨子＞
- プロトコル概要
- 一般的な攻撃手法
- 使用するツール紹介
- 一般的な評価手法



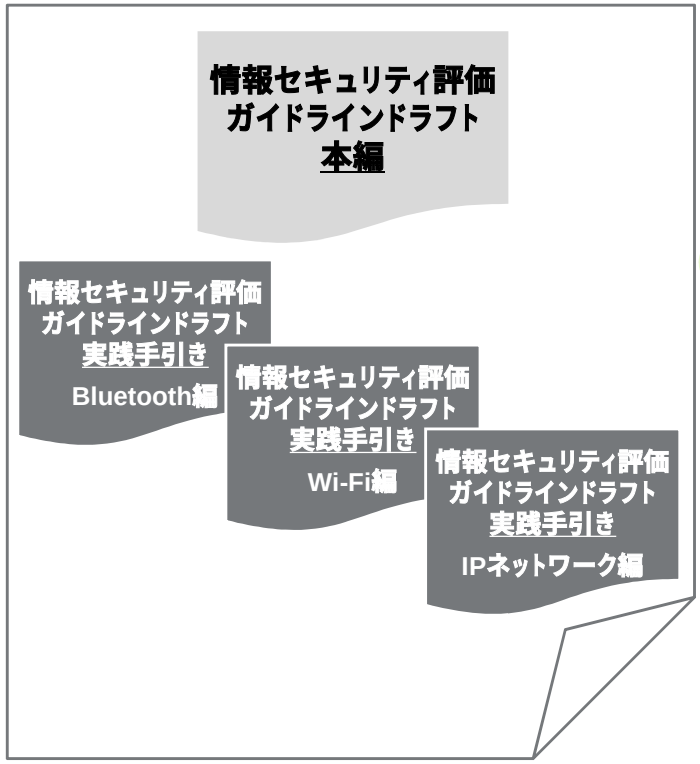
情報セキュリティ評価の試行調査

情報セキュリティ評価の試行調査の目的

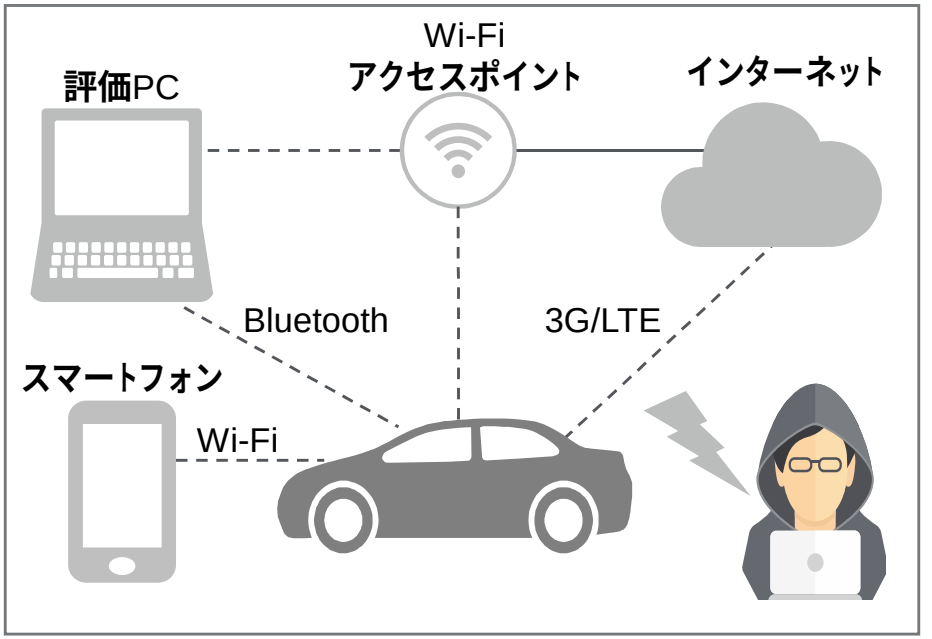
試行調査結果を評価ガイドラインドラフトに反映することで、実効性･利便性を向上

試行調査の目的	本プロジェクトで作成した評価ガイドラインドラフトを用いて、実際の車両を構成するシステムに対して評価を行い、評価ガイドラインドラフトの妥当性の検証を行うとともに、必要に応じて内容の修正を実施

評価ガイドラインドラフト



評価ガイドラインドラフトに基づいた試行調査の実施



試行調査の実施手順

評価ガイドラインドラフトに沿って試行調査を実施し、ガイドラインドラフトの内容の過不足や実効性を検証

	評価の流れ	概要
テスト実施前の評価プロセス	1 事前準備	➢ 参加企業様との間で各種取り決め事項を調整
	2 想定される攻撃者の整理	➢ 評価対象を攻撃する可能性のある攻撃者を推定し、攻撃者をプロファイル
	3 攻撃対象コンポーネントの特定	➢ 攻撃者の標的となり得る機能（情報）を特定のうえ、当該機能を構成するコンポーネントとマッピングし、攻撃者の標的となり得るコンポーネントを特定
	4 車両個別のリスク分析	➢ 攻撃者ファクター、脆弱性ファクター、影響度ファクターからコンポーネントリスクを評価
	5 評価計画の立案	➢ テスト対象範囲の決定のうえ、対象のコンポーネントに対する詳細な技術的分析を行い、評価計画を作成
テスト実施	6 テストの実施	➢ 評価計画に従いテストを実施
テスト実施後の評価プロセス	7 リスクマッピング	➢ テストで発見された脆弱性に対してリスク評価を実施
	8 改善案および残存リスクの整理	➢ リスク評価の結果から、リスクに対する対処を明確化し、対処実施後の残存リスクを整理
	9 評価レポートの作成	➢ 評価結果の説明、および関係者への報告

試行調査の結果得られた情報を基に、評価ガイドラインドラフトを改善

評価ガイドラインドラフトの妥当性の確認と試行調査報告書

評価ガイドラインドラフトの妥当性を確認

妥当性の確認ポイント

■ 当社の評価ガイドラインが持つ7つの強みから妥当性を確認

- ➢ 利便性
  - • 市場リリース後の車両に対する評価に適用可能であることを確認
- ➢ 効率性
  - • 想定する現実的時間内で評価が完了することを確認
- ➢ 再現性
  - • 定量化評価を活用することで再現性の確保が可能であることを確認
- ➢ 実効性
  - • 評価中に識別した課題は、評価ガイドラインへフィードバック･修正したことで実効性を確保
- ➢ 十分性
  - • 脆弱性を発見しうる評価ガイドラインであることを確認
- ➢ 具体性
  - • 標準的なスキルのテスターであれば理解できる内容であることを確認
- ➢ 拡張性
  - • 実践手引きの内容に重複はなく、スコープ拡大が生じても通信プロトコルの追加にて対応できることを確認

評価ガイドラインドラフトに則り試行調査報告書を作成

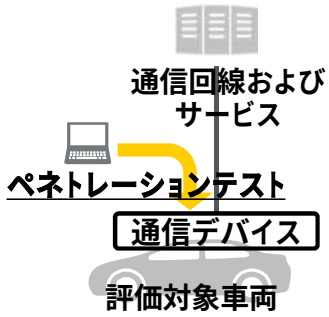
情報セキュリティ評価　試行調査報告書（目次抜粋）

実証実験の運営準備

実証実験の背景と目的

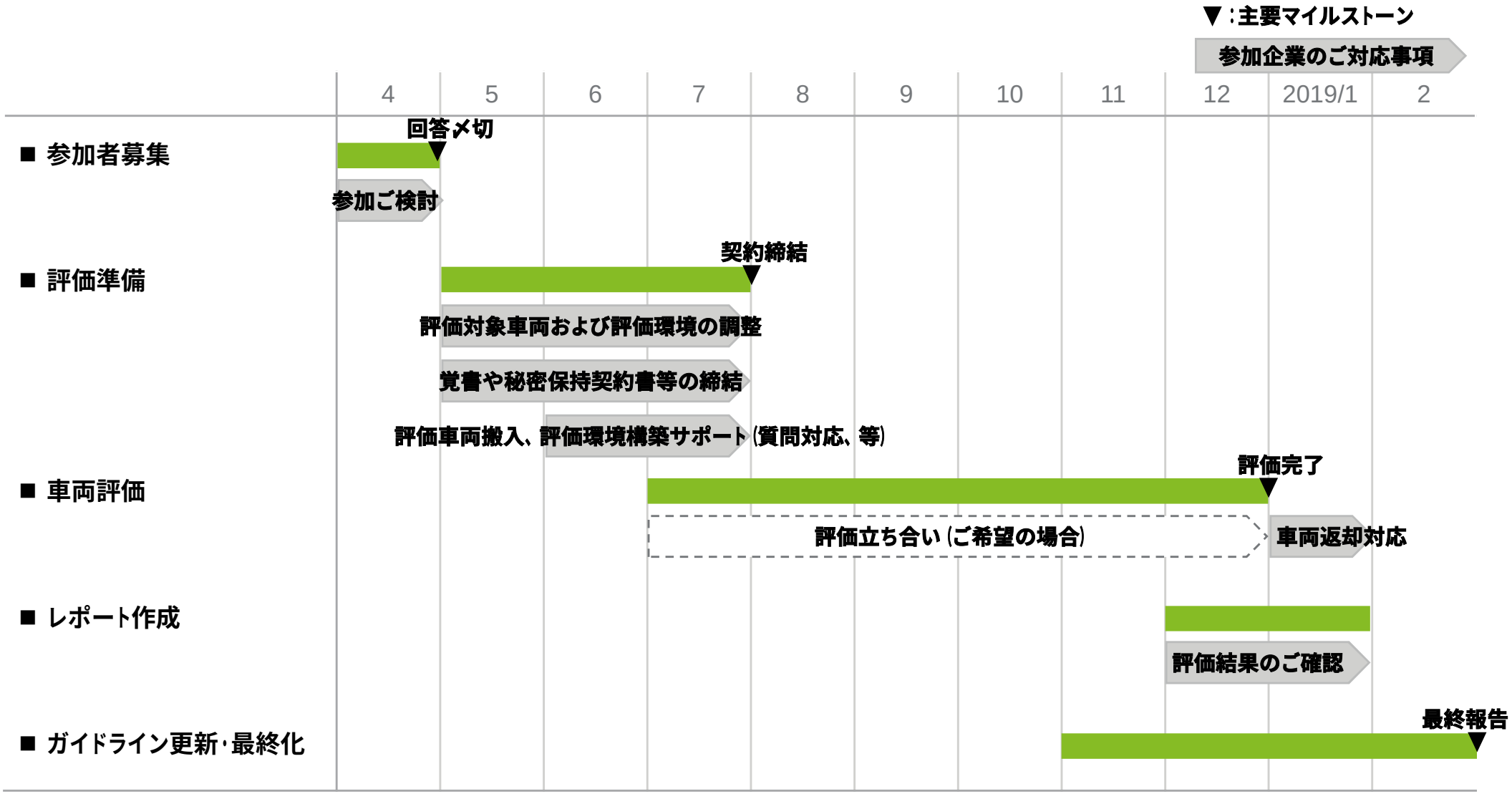
車両への通信を用いた攻撃に対する評価手法確立のために実証実験を実施

背景	■ 2020年の東京オリンピック・パラリンピックに向けて、自動走行システムの実用化の加速を図ることが重要となっています ■ 5つの技術領域（ダイナミックマップ、HMI、情報セキュリティ、歩行者事故低減、次世代都市交通）を中心に、自動車メーカー等の参加のもと大規模実証実験を行い、今後の実用化に向けた、技術面、運用面、制度面等での具体的課題抽出が必要です
目的	■ 車両レベル・コンポーネントレベルでのセキュリティ評価手法・プロトコルをガイドラインとして策定し、本実証実験を通して募る参加者の車両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で、**車両への通信を用いた攻撃に対する評価手法**を確立します



実証実験の全体スケジュール

4月中に参加企業の募集を行い、各社評価準備のうえ7月に評価を開始し、12月末までに評価を完了予定



※ 上記は最も効率的な進捗を想定したスケジュールであり、実際には個別に調整のうえ、各対応を進めます。

評価対象車両および評価環境に関わる要件 (1/2)

参加企業と、評価車両提供等に関わる各種要件への合意が必要

以下は現時点の想定であり、具体的な内容は各社エントリー後に個別に調整

■ 評価対象車両提供に関して

車両の要件	少なくとも以下のうちいずれかの外部通信機能を持つシステムをご準備ください。 Wi-Fi、 Bluetooth、 3G/4G/LTE
車両の種別	評価対象車両は**開発車または市販車**を想定しています。
車両の提供形態	**車両そのもの**の提供が難しい場合は、**車両ベンチ (部品システム)** でも構いません。 ただし、上記「車両の要件」を満たし、無線区間のテストができるシステムである必要があります。
提供期間	**6ヶ月間**を想定しています。 (評価作業そのものは評価対象1台あたり2～3か月程度を見込んでおりますが、複数の評価対象車両を並行して評価を進めるため、余裕を見て6ヶ月間ご提供頂きたく考えております。より短期間のご提供が必要な場合は、個別にご調整させて頂きます。)
予備部品	評価対象車両1台に加え、当該車両に関わる**予備部品 (評価に必要となるヘッドユニット等を含む部品システム) *のご用意をお願い致します。** * 少なくとも1台のご用意をお願いします。2台以上ご用意頂けるとより深い評価が可能になります。

評価対象車両および評価環境に関わる要件 (2/2)

参加企業と、評価車両提供等に関わる各種要件への合意が必要

以下は現時点の想定であり、具体的な内容は各社エントリー後に個別に調整

■ 評価対象車両提供に関して (続き)

保守サポート	評価環境構築時および評価実施中の評価車両に関する**問題発生時のサポート体制**をご準備願います (具体的には担当窓口の設置と、必要な部品サプライヤーとの連携、等を想定)。
車両提供に係る費用	**車両提供に係る費用 (車両そのものおよび運送費、予備部品を想定) は各参加企業様に負担して頂きます**。 その他関連費用 (マニュアル、等) については当社が負担致します。
車両返却時の状態	車両返却時には、評価により破損している恐れがありますのでご了承願います。

■ 評価環境の準備に関して

外部通信環境	テレマティクスで必要になる**通信サービスおよびサーバー側**のご用意をお願いします。 サーバーは検証用サーバー等の**テスト環境**でお願いします。(併せてテスト用アカウントをご用意願います) また、車両出荷前に車両との開通テストを済ませておいて頂けると助かります。
情報提供	車両に関する一般ユーザーが手に入る範囲の情報として、**ユーザーマニュアルやサービスマニュアル**もご用意頂けると助かります (費用は当社負担とします)。
承諾	覚書または秘密保持契約書、確認書等 (後述) の取り交わしを通じて、車両およびサーバーにサイバー攻撃による評価を実施することについてご承諾を頂きます。

情報セキュリティ管理体制について

実証実験において取り扱う情報に大変機微なものが含まれることを踏まえ、その機密管理を徹底

海外法人との連携時の情報の海外流出を防ぐ機密管理

下記により、海外メンバーからの機密情報の流出を防ぎます。

①海外のチームメンバーが知りうる情報の最小限化

下記にて、海外メンバーが本プロジェクトで知りうる情報は最小限に抑えます。

- 評価は日本国内でのみ実施する
- 海外メンバーは、アドバイザーとしての関与であり、評価作業を直接実施しない
  （海外メンバーへは、ノウハウや知見の提供に必要な情報のみを提供）

そのうえで

②契約により海外のチームメンバーからの対外情報流出を防止

海外メンバーが本プロジェクトで知り得た機密情報は、日本と当該海外法人との契約における秘密保持条項により、機密保持を担保します。

参加企業間の評価に関わる情報のセキュリティ確保

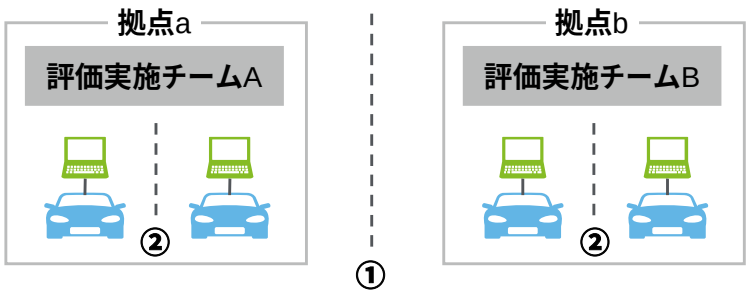
評価環境を物理的に分けることでセキュリティを確保します。

①評価拠点による物理的隔離

評価実施は2つの拠点（それぞれの別の評価実施チームが評価を実施する体制）とし、かつ拠点間の評価車両の移動は行わないことにより、拠点間でのセキュリティを確保

②テスト実施環境の物理的隔離

同一拠点で複数の評価車両を評価する場合において、テスト実施環境（評価で使用するPC等）を物理的に分けることでセキュリティを確保



上記に加え、当社では情報セキュリティ管理に関わる国際標準であるISO/IEC27001の認証を取得したうえで、当基準に則った情報管理を徹底しており、本プロジェクトにおいても十分な機密管理を行います。

評価結果の開示範囲

車両毎の評価結果および評価項目/手順の開示は、各参加企業様個社に限定

■ 車両固有の評価結果については、各参加企業様やNEDO様と締結する秘密保持契約に基づき各参加企業様に限定して開示します。

凡例 ○ ： 開示する
× ： 開示しない

情報分類		開示範囲		
		評価車両の提供者 (各参加企業様)	実証実験事務局 (NEDO)	公表 (ガイドライン等に記載)
1	車両毎の評価結果	○	×	×
2	車両毎の評価項目/手順	○	△*2	×
3	統計化*1した評価結果	○	○	○
4	汎用化した評価項目/手順	○	○	○

*1 「統計化」とは、複数の車両の評価データをその性質や傾向を数量的に把握するために整理することを言い、「統計化」によって作られたデータからは参加企業様が特定できないものとなります。

*2 参加企業様からの許諾を頂いた範囲内での開示となります。