Project Summary

The Cross-ministerial Strategic Innovation Promotion Program (SIP)
Large-scale Field Operational Test for Automated Driving Systems:
- Information security field operational test -

Deloitte Tohmatsu Risk Services Co., Ltd.
February 2018

Contents

Aims and purposes of the field operational test

An FOT will be conducted to establish a method for evaluating network-based attacks on vehicles

Objectives for Research and development of the SIP Automated Driving System

1. Reduce the amount of traffic accidents, etc. and, achieving national goals
2. Realize and popularize the automated driving system
3. Develop the system in cooperation with the Tokyo Metropolitan Government, with the 2020 Tokyo Olympic and Paralympic Games as a milestone

From "Cross-ministerial Strategic Innovation Promotion Program (SIP), Automated Driving System Research & Development Plan" (April 1, 2017)

A large-scale field operation test (FOT) for accelerating implementation of the automated driving system

- **Identifying specific problems** in the fields of technology, operations, and systems
- **Promoting international cooperation and coordination**
- **Promoting accurate public understanding and engendering social acceptance** of automated driving systems, etc.

Five sectors of technology	1. Dynamic Maps 2. Human Machine Interface (HMI) **3. Information security** 4. Pedestrian Accidents Reduction 5. Next-generation Urban Transportation

The information security FOT, a part of the large-scale FOT of the Cross-ministerial Strategic Innovation Promotion Program (SIP) Automated Driving System **(below: "the project")**

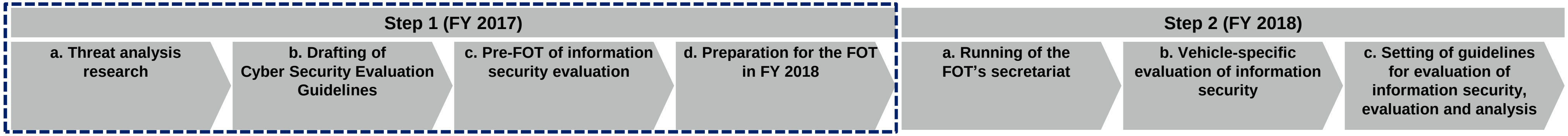
Purpose of the project

Through **research and analysis of security threats** in the field of automated driving, **the development of security evaluation methods and protocols** for the vehicle and component levels with a view to establishing international standards, and the use of vehicles provided by those participating in the **FOT** to undertake a black box experiment testing resistance to hacking, the project aims to achieve the following:

1. **Establish a method for evaluating network-based attacks on vehicles**
2. **Organize the full range of threats, including V2X-related and other external attacks**
3. **Build consensus about autonomous vehicle security**
4. **Develop human resources and accumulate knowhow related to autonomous vehicle security in Japan**

From "Application guidelines related to the 'information security FOT' part of the 'large-scale FOT of the Cross-ministerial Strategic Innovation Promotion Program (SIP) Automated Driving System'" (July 2017)

(Relation of each task to the aims of the project)


Step 1 (FY 2017)
a. Threat analysis research
b. Drafting of Cyber Security Evaluation Guidelines
c. Pre-FOT of information security evaluation
d. Preparation for the FOT in FY 2018
Step 2 (FY 2018)
a. Running of the FOT's secretariat
b. Vehicle-specific evaluation of information security
c. Setting of guidelines for evaluation of information security, evaluation and analysis

(Tasks pursued in this phase)

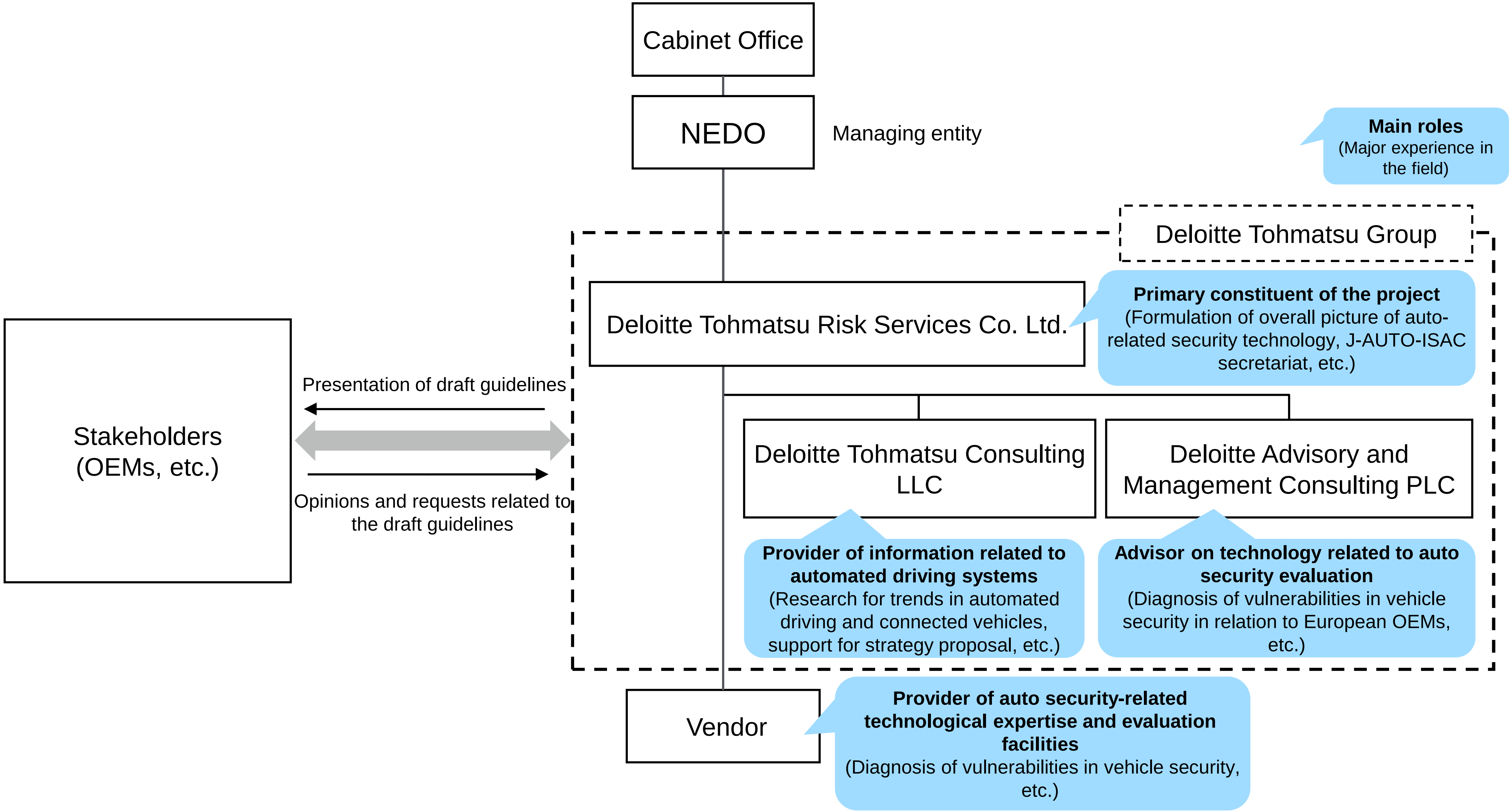
Overall schedule

XXX

	October 2017	November	December	January 2018	February
a. Threat analysis research	Research for the structure of existing automated driving systems	Organize of the types of automated driving systems Analysis of the security of system types	Analysis of the impact of threat items	Overall threat perspective	
b. Drafting of Cyber Security Evaluation Guidelines	Hearings with stakeholders	Organization and analysis of evaluation methods Drafting of first version of guidelines	Collection of opinions on first version (public comment for related parties)	Finalization of draft guidelines	
c. Pre-FOT of information security evaluation		Preparation of vehicles, systems, etc. to be evaluated	Evaluation based on draft guidelines		Evaluation report
d. Preparation for the FOT in FY 2018		Proposal of a plan for the FOT	Preparation for running the FOT's secretariat		

Implementation structure

The project has been conducted in cooperation with the Deloitte Tohmatsu Group's consultant teams including an overseas member firm with technological expertise and proven track records



Cabinet Office

NEDO

Managing entity

Main roles
(Major experience in the field)

Deloitte Tohmatsu Group

Deloitte Tohmatsu Risk Services Co. Ltd.

Primary constituent of the project
(Formulation of overall picture of auto-related security technology, J-AUTO-ISAC secretariat, etc.)

Stakeholders (OEMs, etc.)

Presentation of draft guidelines

Opinions and requests related to the draft guidelines

Deloitte Tohmatsu Consulting LLC

Deloitte Advisory and Management Consulting PLC

Provider of information related to automated driving systems
(Research for trends in automated driving and connected vehicles, support for strategy proposal, etc.)

Advisor on technology related to auto security evaluation
(Diagnosis of vulnerabilities in vehicle security in relation to European OEMs, etc.)

Vendor

Provider of auto security-related technological expertise and evaluation facilities
(Diagnosis of vulnerabilities in vehicle security, etc.)

Threat analysis research

Approaching the threat analysis research

In order to identify the overall perspective of cyber threats to automated driving systems, we will conduct a research for the components of such systems and analyze expected threats to them

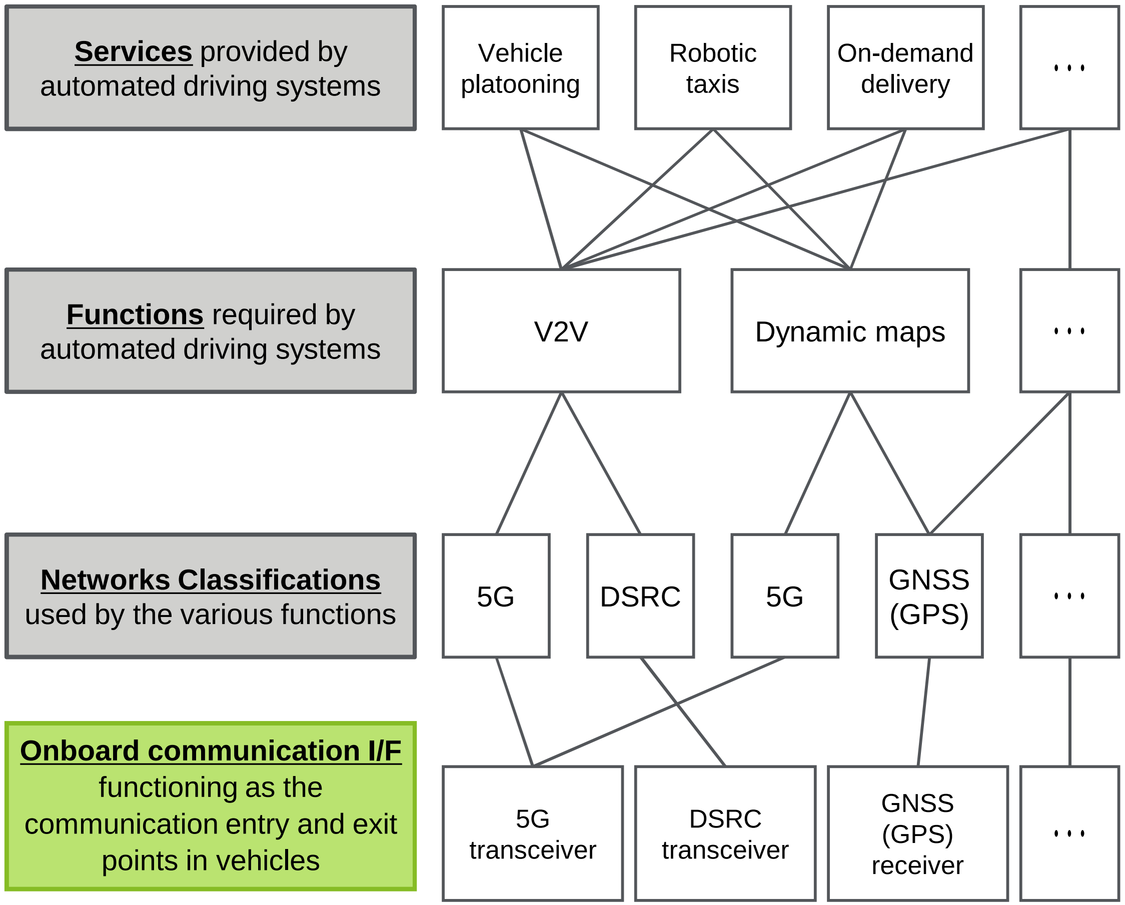
	Modeling and researching for components of automated driving systems	Threat analysis
Steps to be implemented	• Modeling of automated driving systems • Research for services and functions constituting automated driving systems • Organize network types and onboard communication I/F	• Development of scenarios for wireless network-based external attacks on autonomous vehicles • Evaluation of threat levels • Classification of threats • Organize the overall threat perspective for automated driving systems
Main outcomes	• Results of the service research • Results of the functions research • Results of the Networks Classifications research • Results of the research for onboard communication I/F	• List of threat scenarios • Threat evaluation index • Results of threat evaluation • Overall threat perspective

Model for threat analysis of automated driving systems and research/organize procedures

By modeling automated driving systems, and researching and organizing the components of each of their layers, we can identify the onboard communication I/F that function as entry and exit points in vehicles for wireless communications

Model for threat analysis of automated driving systems and their components

Threat analysis model | **Components (example)**



Services provided by automated driving systems

Vehicle platooning | Robotic taxis | On-demand delivery | ・・・

Functions required by automated driving systems

V2V | Dynamic maps | ・・・

Networks Classifications used by the various functions

5G | DSRC | 5G | GNSS (GPS) | ・・・

Onboard communication I/F functioning as the communication entry and exit points in vehicles

5G transceiver | DSRC transceiver | GNSS (GPS) receiver | ・・・

Research/organize procedures

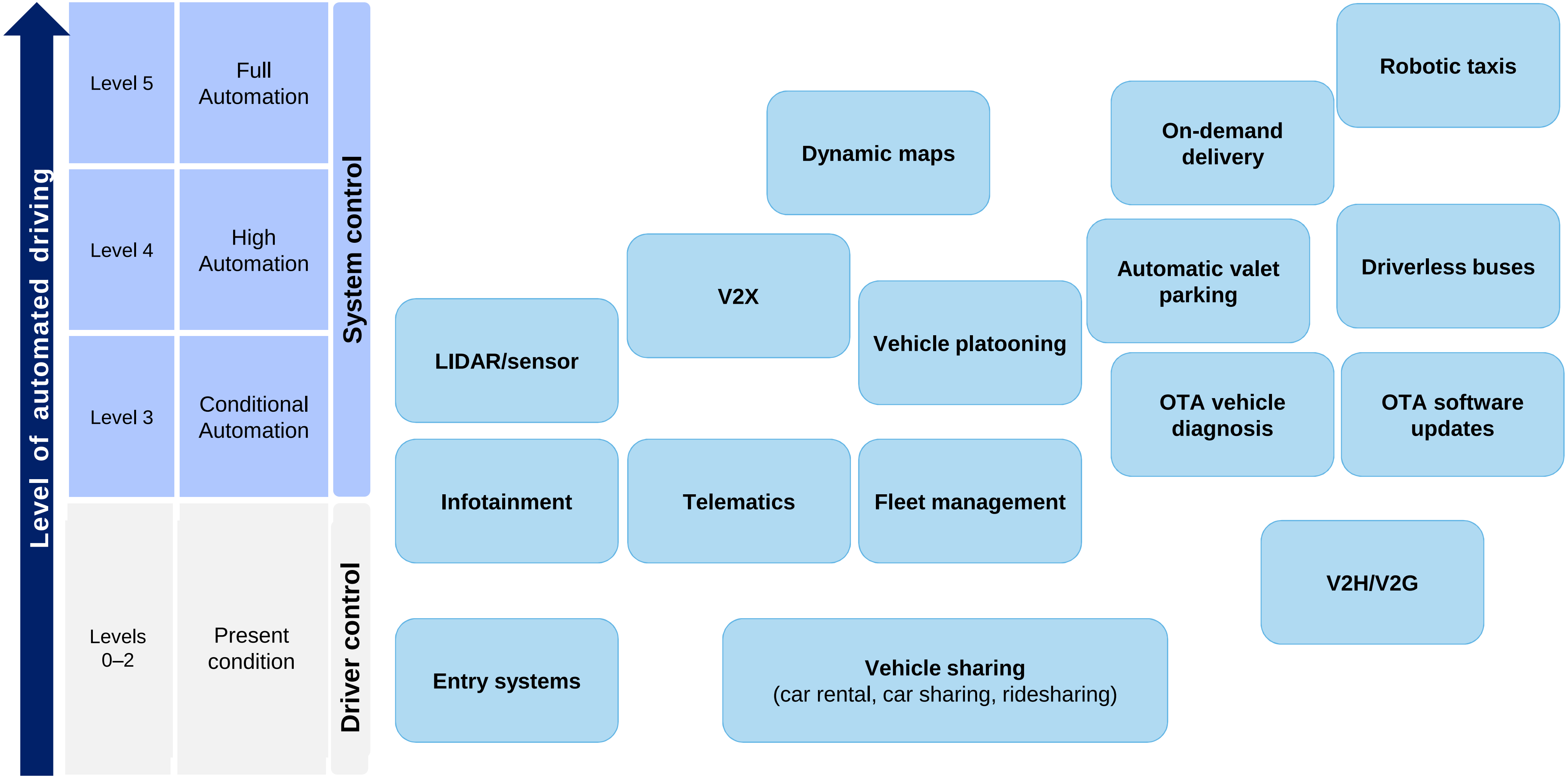
1 Research for auto manufacturers and suppliers' undertakings, FOTs, etc.

2 Listing of the functions that make up each service

3 Since networks used in each functions varies, identifying specific networks required to each function is necessary.

Services provided by automated driving systems (including some functions)

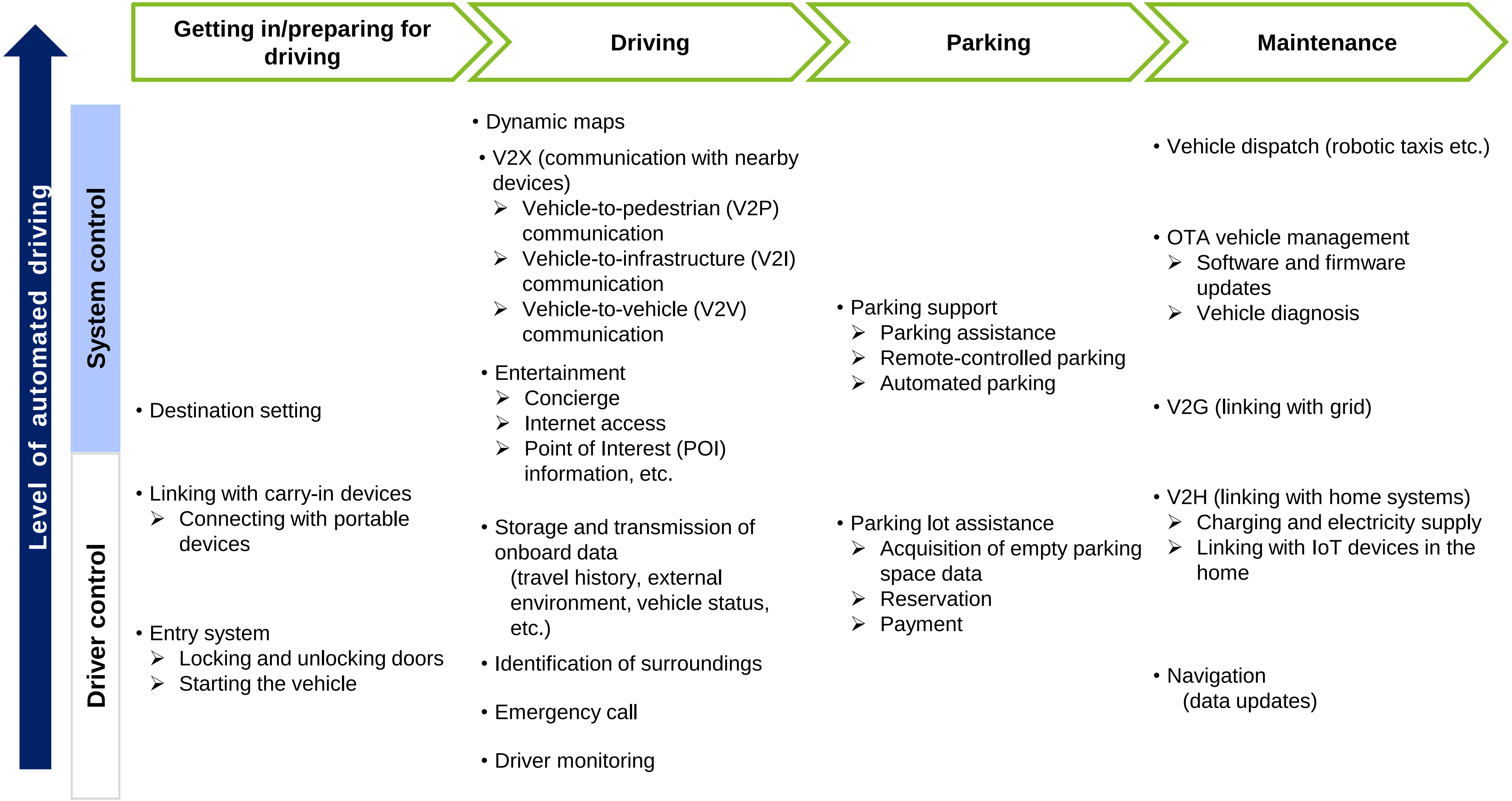
By comprehensively researching and organizing the services provided by automated driving systems, the overall perspective of cyber threats becomes identified



Services and functions are commodified as automated driving systems evolve

Results of the automated driving systems functions research

The functions included in automated driving systems can be summarized as follows



Getting in/preparing for driving

- Destination setting
- Linking with carry-in devices
  - Connecting with portable devices
- Entry system
  - Locking and unlocking doors
  - Starting the vehicle

Driving

- Dynamic maps
- V2X (communication with nearby devices)
  - Vehicle-to-pedestrian (V2P) communication
  - Vehicle-to-infrastructure (V2I) communication
  - Vehicle-to-vehicle (V2V) communication
- Entertainment
  - Concierge
  - Internet access
  - Point of Interest (POI) information, etc.
- Storage and transmission of onboard data (travel history, external environment, vehicle status, etc.)
- Identification of surroundings
- Emergency call
- Driver monitoring

Parking

- Parking support
  - Parking assistance
  - Remote-controlled parking
  - Automated parking
- Parking lot assistance
  - Acquisition of empty parking space data
  - Reservation
  - Payment

Maintenance

- Vehicle dispatch (robotic taxis etc.)
- OTA vehicle management
  - Software and firmware updates
  - Vehicle diagnosis
- V2G (linking with grid)
- V2H (linking with home systems)
  - Charging and electricity supply
  - Linking with IoT devices in the home
- Navigation (data updates)

See Appendix B for a structure chart of the above functions

Results of the organize of wireless and communication I/F

Summary of the types of networks and onboard communication I/F used by automated driving systems

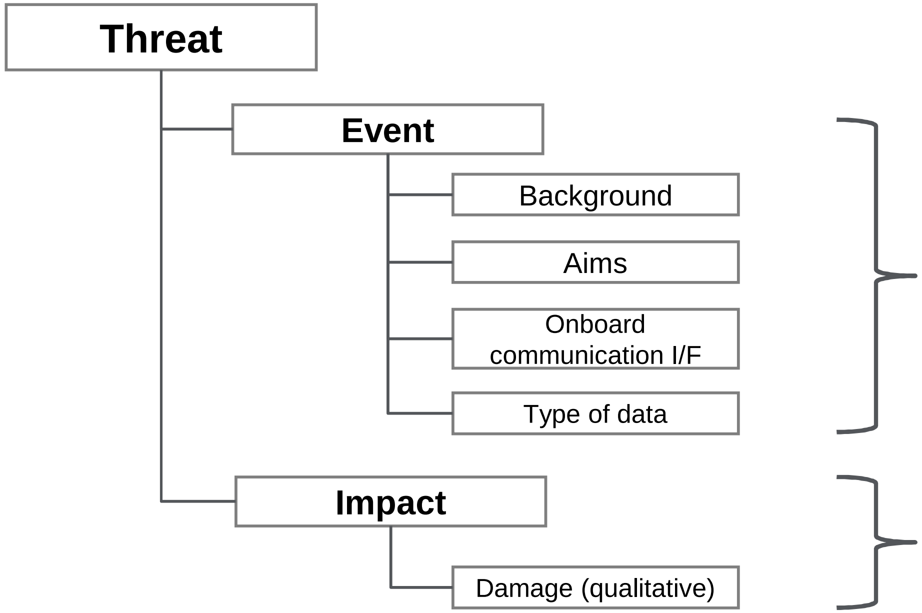
Types of Networks	Networks Classifications	Onboard communication I/F	Point(s) of connection from the vehicle	Examples of information communicated
Public network	5G	5G transceiver	Nearby vehicles, cellphone carriers' base stations, service providers' servers	Cruise control data, dynamic map data, etc.
	3G/4G	3G/4G transceiver	Cellphone carriers' base stations, service providers' servers	Software updates, traffic information, infotainment
Wi-Fi	Wi-Fi	Wi-Fi transceiver	Wi-Fi hotspots, service providers' servers	Software management data, vehicle location data, traffic information, infotainment
V2X communication	Cellular V2X	Cellular V2X transceiver	Nearby vehicles, infrastructure, etc.	Traffic information, cruise control data, etc.
	DSRC	DSRC transceiver device (V2X)	Nearby vehicles, infrastructure, etc.	
Device-to-device communication	Bluetooth (for VCK and portable devices)	Bluetooth transceiver	Smartphones and other portable devices	Identification data used by the entry system, information on linked portable devices, etc.
	Bluetooth (for OBD-II)	OBD-II dongle	Wi-Fi hotspots, service providers' servers	Software management data, diagnostics
	ZigBee	Wireless ZigBee module	Power grid, homes	Vehicle body control data
Remote sensing	Millimeter-wave radar (77/79GHz)	Millimeter-wave radar transceiver	Nearby vehicles, pedestrians, obstacles	Cruise control data
	Quasi-millimeter-wave radar			
	LIDAR	LIDAR transceiver		
	Ultrasonic sensor	Ultrasonic sensor transceiver		
	Biometric sensor	Biometric sensor	Passengers (fingerprints, irises, expressions, etc.)	Biometric data
Satellite transmission	GNSS (GPS)	GNSS (GPS) receiver	GPS satellites	Vehicle location data
Data provision (VICS etc.)	Quasi-microwave	Quasi-microwave terminal	Roadside devices (radio beacons)	Traffic information (congestion, accidents, etc.)
	Infrared	Infrared terminal	Roadside devices (infrared beacons)	
	DSRC	DSRC transceiver device (VICS/ETC)	Roadside devices (radio beacons), nearby vehicles	Traffic information, cruise control data, asset data
Entry system	NFC	NFC reader/writer device	Contactless IC cards, smartphones	Asset data
	RF/LF (RFID)	RF/LF (RFID) reader/writer	Smart keys	Vehicle body control data

Structure of threat scenarios

To make threat scenarios understandable, organized by events and impact

Premises

- ■ Threat scenarios are developed for each type of Onboard communication I/F
- ■ Threat scenarios are based on uniform structural rules to prevent variation in interpretations
- ■ Work is done to develop, evaluate, and organize threat scenarios going forward with following the rules below



On developing threat scenarios

- ◆ Clearly define factors such as the attack's background, aims, and type of relevant data
- ◆ On the level of the device in question, express what type of security breach (information disclosure, tampering, etc.) has occurred by clarifying the "event" (what has happened) and "impact" (what will happen) in the scenario
- ◆ Use as few technical terms as possible, making your scenario understandable for a broad audience
- ◆ Reinforce the concreteness of your scenario by telling a qualitative story about the effects that the event could cause

Example of threat scenario

Tampering

[Event]
Authentication data exchanged between a Bluetooth-equipped vehicle and a VCK (smartphone) is encrypted with ransomware
[Impact]
The vehicle becomes unusable, the attackers demand money

Developing STRIDE-based threat scenarios for each type of Onboard communication I/F

Develop STRIDE-based threat scenarios based on the "event" and "impact" structure in order to prevent issues such as variation in and insufficiency of threats

Classification of threats	Examples of threat scenarios
Spoofing	Event: By interfering with communications between the vehicle and GNSS (GPS) and transmitting a disguised signal, the attacker poses as a GPS satellite Impact: Location data cannot be acquired, making it impossible to set destinations and routes for the vehicle
Tampering	Event: By remotely tampering the software update data on communications, the attacker causes abnormalities in cruise control-related software Impact: As the attacker intended, abnormal limitations on vehicle control occur while driving, impacting driving safety
Repudiation	Event: Communication between an onboard ETC device and the ETC system at a tollgate is repudiated, resulting in the denial of fee payment Impact: Economic loss occurs as a result of this act of fraud
Information disclosure	Event: An attacker providing a fake hotspot or fraudulent free Wi-Fi access point approaches the target vehicle and, once the vehicle connects to this access point, steals the communication data Impact: The vehicle's destination, route, user ID, password, and other details are stolen
Denial of service	Event: A large quantity of packets are transmitted to a specific vehicle, bringing telematics services to a standstill Impact: The vehicle's network communication functions are stopped and no network-based services can be used
Elevation of privilege	Event: The attacker remotely inputs unauthorized codes and commands, seizing administrator rights for a 4G transceiver and using it to access other devices connected to the onboard network Impact: The attacker's use of devices and functions other than the 4G transceiver result in an intended malfunction of the accident evasion system, impacting driving safety

Evaluating threat scenarios

The level of a threat included in a scenario is evaluated by actualization rate and level of impact

Actualization rate

Analyzed separately from each viewpoint and then evaluated comprehensively, this refers **to how easy it is for an attacker to successfully carry out the threat**, irrespective of the characteristics and structure of the vehicle

Viewpoint		Evaluation method
1	Ease	Ease with which the attack can be carried out
2	Devices/tools	Need for special tools and devices
3	Preparation time	Preparation time required to carry out the attack (concealment etc.)
4	Number of attackers	Number of people required to carry out the attack
5	Vehicle status	Status of the vehicle being attacked (driving or parked)

+

Level of impact

Comprehensive evaluation of the **safety impacts and consequences** to the attacked vehicle and its surrounding environment

Viewpoint		Evaluation method
1	Level of lost functions	Impact on driving (driving, turning, stopping)
2	Level of damage	Safety impact on passengers
3	Scope of damage	Impact on the infrastructure, other vehicles, and pedestrians near the attacked vehicle

On evaluation

Evaluate the threat level of each threat by assigning a number to both the likelihood of actualization and the level of impact the actualized threat would have

Threat level

Level of impact			
3	4	5	6
2	3	4	5
1	2	3	4
	1	2	3
	Actualization rate		

Overall threat perspective

Threat tendencies calculated by actualization rate and level of impact on driving safety

Scores in the chart are averages of the threat level for each communication I/F by STRIDE classification. See slide 14 for how to calculate threat level.

— ; No applicable scenario

Types of Networks	Onboard communication I/F	Classification of threats					
		Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Public network	5G transceiver	5	6	4	4	5	5
	3G/4G transceiver*	5	6	4	3	4	3
Wi-Fi	Wi-Fi transceiver	5	4.5	—	4	4	5
V2X communication	Cellular V2X transceiver	5	5	3	4	5	4
	DSR transceiver (V2X)	5	5	5	3	5	3
Device-to-device communication	Bluetooth transceiver (for VCKs and other portable devices)	4	3	4	4	4	3
	Bluetooth transceiver (for OBD-II)	6	4.5	—	4	6	5
Satellite transmission	GNSS (GPS) receiver	4	4	—	—	4	—
Data provision (VICS etc.)	Quasi-microwave terminal	3.5	3	—	—	3	—
	Infrared terminal	3	4	—	—	3	—
	DSRC transceiver (VICS/ETC)	3	2	2	3	3	—
Entry system	NFC reader/writer device	3	4	4	4	4	4
	RF/LF (RFID) reader/writer	4	3	—	3	3.5	—

*As scenarios were developed for both 3G and 4G, the one with the higher threat level score is displayed here

The analysis shows that threat levels tend to be high for onboard communication I/F which communicate information necessary for driving safety

How to proceed going forward

Applying the results of the threat analysis to the security guidelines

Threat analysis results	Cyberattacks on the following kinds of onboard communication I/F have a significant impact on automated driving systems

Onboard communication I/F with high threat levels

Public networks	5G transceivers
	3G/4G transceivers
Wi-Fi	Wi-Fi transceivers
Device-to-device communication	Bluetooth transceivers

Part of security guidelines to be evaluated

- ➢ Cyber Security Evaluation Guidelines - DRAFT - (Practical Manual - IP Network)
- ➢ Cyber Security Evaluation Guidelines - DRAFT - (Practical Manual - Wi-Fi)
- ➢ Cyber Security Evaluation Guidelines - DRAFT - (Practical Manual - Bluetooth)

V2X communication	Cellular V2X transceivers
	DSRC transceiver

V2X communication is at the experimental stage with a view to practical realization in the future. As its specifications have yet to be standardized (as of January 2018), it will need to be revisited later

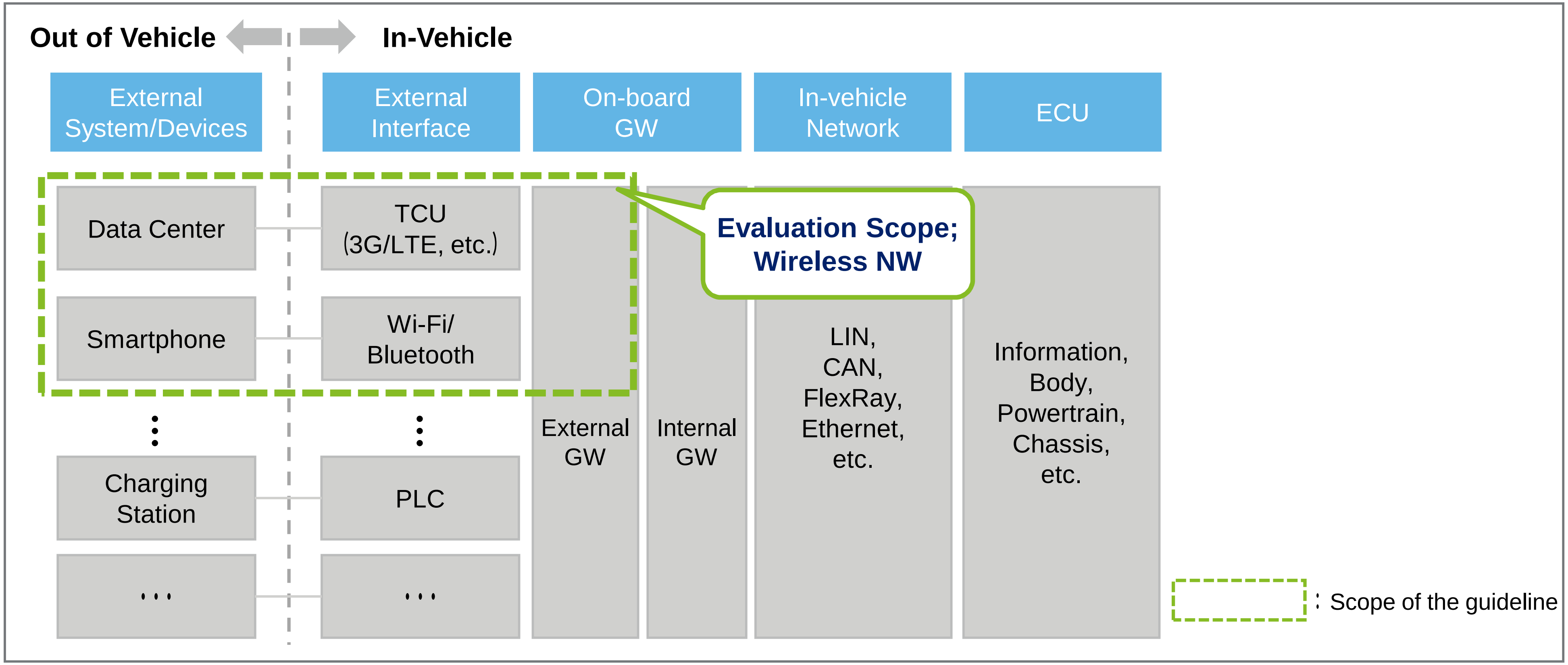
Security guidelines for onboard communication I/F used for commodified networks with high threat level should preferentially be developed

Drafting of Cyber Security Evaluation Guidelines

Scope of Cyber Security Evaluation Guidelines - DRAFT -

Evaluation Scope: Wireless Network Path

Scope	■ Cyber attacks on vehicles through wireless network from external system/devices to external GW ■ Drafted Guidelines as "Methodology" to cover the testing framework and "Practical Manual" to cover specific evaluation approaches for each communication protocol



Characteristics of Cyber Security Evaluation Guidelines - DRAFT -

Seven Advantages

1 Usability

- Providing testing methods applicable to not only vehicle integration testing and commercially available vehicles but also system design phase
- Clarifying use cases and penetration test conductors during V-model process

2 Efficiency

- Providing test approach for effective use of test resources (e.g. time, manpower, cost)

3 Reproducibility

- Ensuring reproducibility and objectivity by eliminating individual judgement in evaluation procedure

4 Effectiveness

- Applied methodologies to penetration test project for European OEMs
- Including knowhow derived from past penetration test project
- Ensuring effectiveness with cooperation with stakeholders through development process

5 Sufficiency

- Ensuring sufficiency with considering known vulnerabilities to both automotive and IT system
- Possible to add OEM specific evaluation items using the methodology provided in the Guideline

6 Specific

- Introducing detailed description of commands and execution results in Practical Manuals
- Understandable description for penetration testers

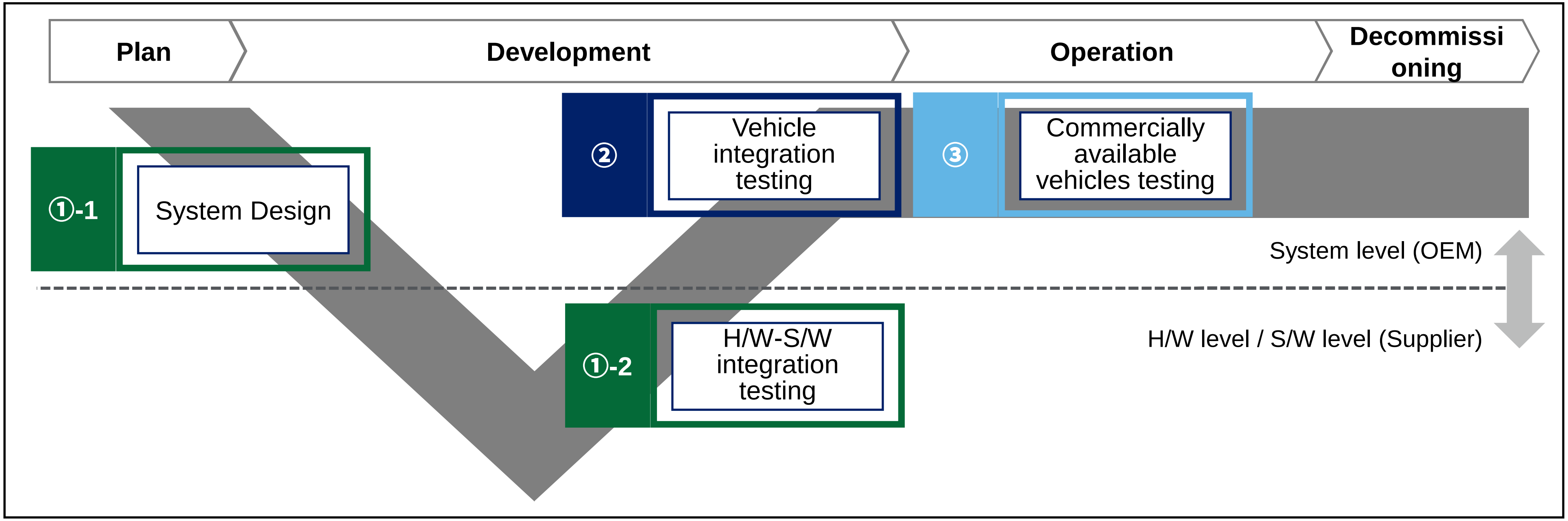
7 Expandability

- Easy to expand the scope to in-vehicle network level by adding new practical manuals

Key Points of Drafting Evaluation Guideline (1/7)

Usable Guideline through Development Process

1	Usability	■ Method applicable to not only vehicle integration testing and sold vehicle testing but also system design phase ■ Clarifying use cases and penetration teste conductors during V-model process



Plan

Development

Operation

Decommissioning

①-1 System Design

② Vehicle integration testing

③ Commercially available vehicles testing

System level (OEM)

H/W level / S/W level (Supplier)

①-2 H/W-S/W integration testing

①-1	Available to make penetration test plans in earlier stage using this guideline
①-2	Possible to execute penetration test in advance at H/W-S/W integration testing phase
②	Guideline applicable to vehicle integration testing phase before product released in to market
③	Guideline applicable to sold vehicle already in market

Key Points of Drafting Evaluation Guideline (2/7)

Efficient and Effective Resource Allocation

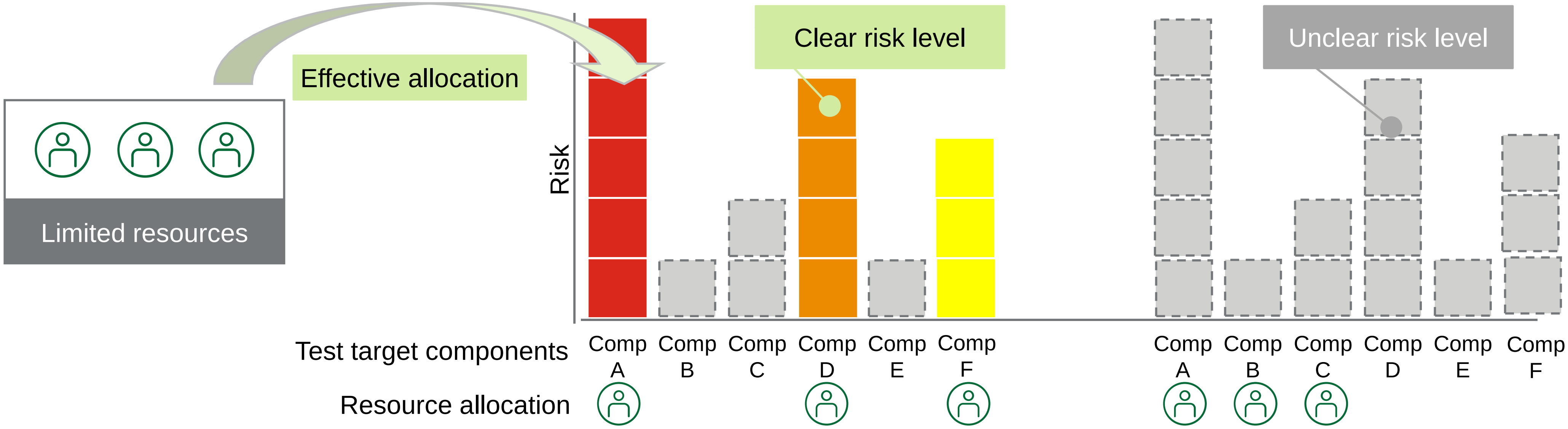
2	Efficiency	■ Providing test approach for effective use of test resources (e.g. time, manpower, cost) ■ Risk analysis with attacker view enables efficient penetration test by focusing on high risk level component

Penetration test focusing on high risk level component

Cyber Security Evaluation Guideline

Risk analysis makes it possible to allocate resources effectively and conduct efficient testing

Unable to allocate proper resources if component risk level were not evaluated

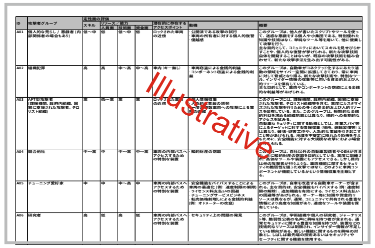


Key Points of Drafting Evaluation Guideline (3/7)

Templates for Risk Analysis and Penetration Test

3	Reproducibility	■ Ensuring reproducibility and objectivity with using prepared templates ■ Eliminating individual judgement in the evaluation procedure to maintain objectivity

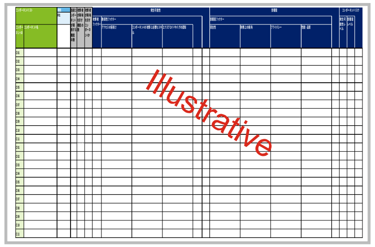
Templates for risk analysis



Illustrative

ID	攻撃者グループ	定性面の評価				潜在的に存在するアクセスポイント	動機	概要
		スキル	リソース／能力					
			人員面	技術面	資金面			
A01	個人的な荒らし／悪戯者（内部関係者の場合もあり）	低～中	低	低～中	低	ロックされた車両の近傍	・公開済である攻撃の試行 ・車両の所有者に対する個人的復讐 ・優越感	このグループは、他人が書いたスクリプトやツールを使って、迷惑な悪戯をする個人や小集団である。特別優れた知識や技術はなく、単純なツール等を用いて、他に便乗して攻撃を行う。 主な目的として、コミュニティにおいてスキルを見せびらかすことや、個人的な復讐が挙げられる。新たな攻撃技術自体を開発することはないが、既存の攻撃技術を組み合わせて、新たな攻撃手法を生み出す可能性がある。
A02	組織犯罪	高	高	中～高	中～高	車内（キー無し）	・車両窃盗による金銭的利益 ・コンポーネント窃盗による金銭的利益	このグループは、自動車がコネクテッド化するにあたり活動の領域をサイバー空間に拡張してきており、常に車両に対して脅威となり得る。新たな攻撃技術や、特別なツール、インサイダー情報の収集等に用いる資金的および人的リソースを保有している。 主な目的として、車両やコンポーネントの窃盗による金銭的な利益等があげられる。
A03	APT型攻撃者 （諜報機関、政府内組織、国家に支援された攻撃者、テロリスト組織）	高	低～高	高	高	ロックされた車両の近傍	・個人情報収集 ・人為的な事故の誘発 ・一度の多数車両への攻撃による[illegible]	このグループには、諜報機関、政府内組織、国家に支援された攻撃者、テロリスト組織等を含む。高度にカスタマイズされた攻撃を行うための多くの資金的および人的リソースを保有している。また、このグループは、短期的な金銭的利益を求める組織犯罪とは異なり、標的への長期的なアクセスを試みる。 自動車セキュリティに関する動機としては、産業スパイ等によるターゲットに対する情報収集（場所、運転習慣等）とは異なり、破壊・妨害工作や、人為的な事故を引き起こすこと等があげられる。地域を不安定に陥れたり恐怖を与えるために、安全機能に対する大規模な攻撃におよぶ場合[illegible]られる。
A04	競合他社	中～高	中	中～高	中～高	車両の内部バスへアクセスするための特別な装置	・知的財産の窃取	この[illegible]ループは、自社以外の自動車製造者やOEMが含まれ、[illegible]に知的財産の窃取を目的としている。高度に訓練され、高価なツールや装置にもアクセスできる。しかし目的は他の攻撃者が行うような、車両機能に関するセキュリティの脆弱性を狙った攻撃ではなく、どのように車両コンポーネントが機能しているかという情報収集を主眼とする。
A05	チューニング愛好家	中	中	中～高	中	車両の内部バスへアクセスするための特別な装置	・安全機能をバイパスすることによる車両の最適化（例：速度制限の解除） ・ライセンス料支払いの回避 ・チューニングサービスビジネス ・転売価格割増しによる金銭的利益（例：オドメーターの改竄）	このグループは、自車を改造する自動車オーナーが含まれる。主な目的は、安全機能をバイパスする（例：速度制限の解除）、追加機能を有効にする、ライセンス料支払いの回避等があげられる。オーナー毎に知識や資金的リソースは異なるが、通常、コミュニティで共有される豊富な情報により高度な知識があり、適度なツールや装置を保有している。
A06	研究者	高	低	高	低	車両の内部バスへアクセスするための特別な装置	・セキュリティ上の問題の発見	このグループは、学術組織や個人の研究者、ジャーナリスト等、脆弱性公表の名声に興味を持つ者が含まれる。通常セキュリティに関する豊富な知識を持つが、装置などの技術的なリソースは制限され、インサイダー情報が不足している傾向がある。新しい機能に関するものを興味の対象とし、しばしば最先端の技術あるいはセキュリティやセーフティに関する機能を使用する。

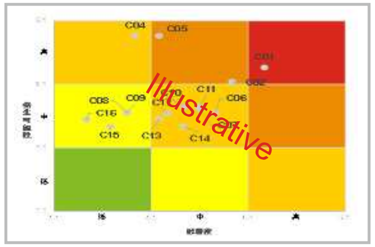
Attacker profiles



Illustrative

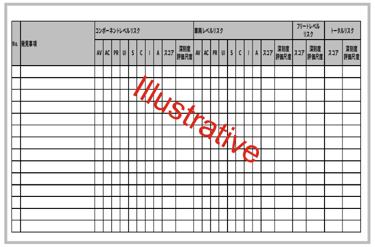
コンポーネントリスト		機能				発生可能性				影響度				コンポーネントリスク	
						攻撃者ファクター	脆弱性ファクター			影響度ファクター					
コンポーネントID	コンポーネント名						アクセスの容易さ	コンポーネントの攻撃に必要なスキル	エクスプロイトやバグの認知	安全性	財務上の損失	プライバシー	性能・品質	発生可能性レベル	影響度レベル

Risk analysis



Risk heat map

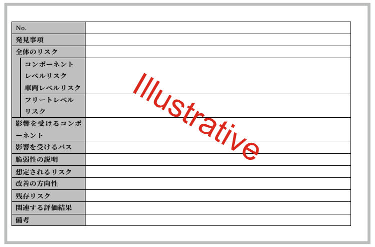
Templates for findings and evaluation result



Illustrative

No.	発見事項	コンポーネントレベルリスク										車両レベルリスク										フリートレベルリスク		トータルリスク	
		AV	AC	PR	UI	S	C	I	A	スコア	深刻度評価尺度	AV	AC	PR	UI	S	C	I	A	スコア	深刻度評価尺度	スコア	深刻度評価尺度	スコア	深刻度評価尺度

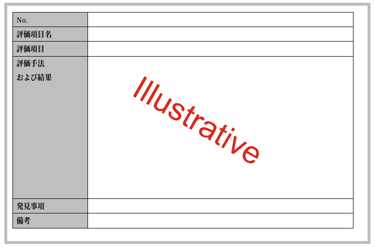
Risk evaluation for identified vulnerabilities



Illustrative

No.	
発見事項	
全体のリスク	
コンポーネントレベルリスク 車両レベルリスク	
フリートレベルリスク	
影響を受けるコンポーネント	
影響を受けるバス	
脆弱性の説明	
想定されるリスク	
改善の方向性	
残存リスク	
関連する評価結果	
備考	

Findings from evaluation



Illustrative

No.	
評価項目名	
評価項目	
評価手法 および結果	
発見事項	
備考	

Evaluation results

Key Points of Drafting Evaluation Guideline (4/7)

Best Practices and Public Comments

4	Effectiveness	
		■ Referring the guidelines accepted as practical standard in IT system field ■ Previously applied method to penetration test projects for EU OEMs ■ Including know-how derived from past penetration test projects. ■ Ensuring effectiveness incorporating public comments from stakeholders

Best practices of IT system

Considering practical guidelines and methodologies in IT system area

Guideline
NIST
Technical Guide to Information Security Testing and Assessment

Guideline
PCI Security Standards Council
Penetration Testing Guidance

Guideline
OWASP
Risk Rating Methodology

Proven methodology for Automotive

Applied methodologies to EU OEMs and verified through penetration projects

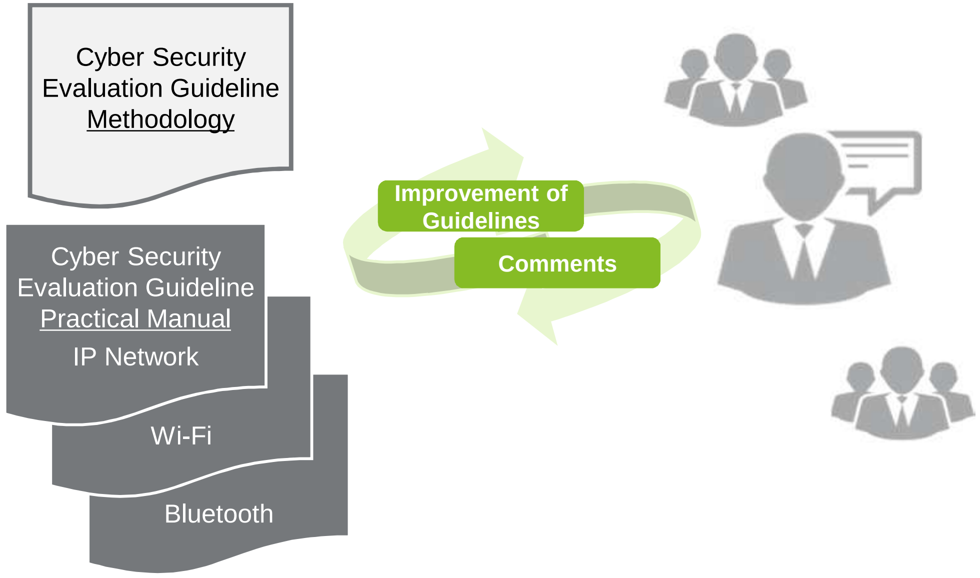
Methodology
Deloitte
Automotive Cyber Security Pentest Methodology

Public comments from stakeholders

Ensuring effectiveness by public comment from several stakeholders

Cyber Security Evaluation Guideline - DRAFT -

Stakeholders


Cyber Security Evaluation Guideline Methodology
Cyber Security Evaluation Guideline Practical Manual
IP Network
Wi-Fi
Bluetooth
Improvement of Guidelines
Comments

Key Points of Drafting Evaluation Guideline (5/7)

General Evaluation Items considering sufficient vulnerabilities

5	Sufficiency	■ Evaluation items for vulnerabilities known in automobile and vulnerabilities known in IT systems applicable to automobile are listed in Guideline (Methodology) ■ Possible to add specific evaluation items using the methodology provided in the Guideline(Methodology)

Vulnerability Category		Vulnerabilities to be considered	Points of Developing Evaluation Items
Known in Automobile		■ Example of Incidents Cases ➢ Vulnerability in In-Vehicle Infotainment System ➢ Vulnerability in Connected Services ➢ Vulnerability in Wireless LAN ➢ Vulnerability in Mobile Application, etc.	■ Referring to security research reports, in addition to past incident and attacks on vehicles
Unknown in Automobile	Known in IT System	■ Applicable to automobile among known vulnerabilities in IT system ➢ Vulnerability in Connected Server ➢ Vulnerability in Web Application ➢ Vulnerability in Mobile Application, etc.	■ Organized known vulnerabilities based on CWE ■ Referring to SANS Top 25 and OWASP TOP to study vulnerabilities applicable to automobile ■ Referring to CAPEC, etc. to develop evaluation items
	Others	Out of scope ※ Appropriate update is needed based on newly disclosed vulnerability of automotive and IT system area	

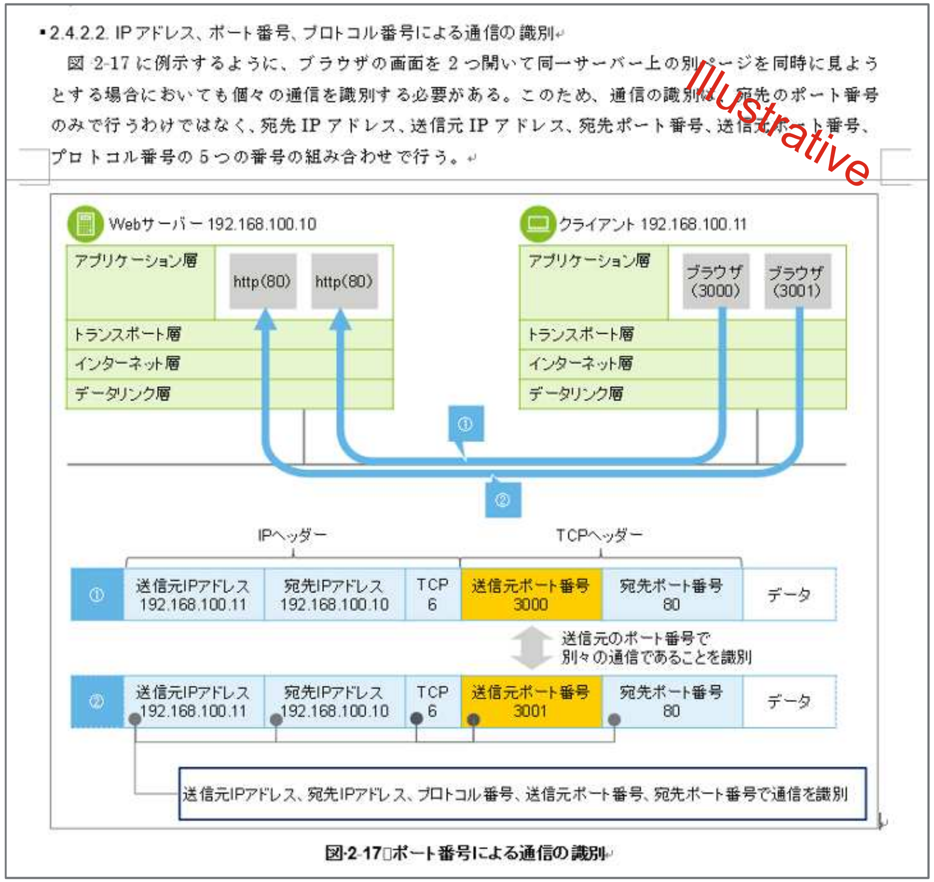
□ : Vulnerabilities considered in the general evaluation item list in the guideline (Methodology) Annex

Key Points of Drafting Evaluation Guideline (6/7)

Practical Description and Example

6	Specific	■ Introducing detail description of commands and execution results in the Guideline (Practical Manuals) ■ Understandable description for penetration testers

■ Graphical description



Illustrative

・2.4.2.2. IPアドレス、ポート番号、プロトコル番号による通信の識別

図 2-17 に例示するように、ブラウザの画面を 2 つ開いて同一サーバー上の別ページを同時に見ようとする場合においても個々の通信を識別する必要がある。このため、通信の識別は、宛先のポート番号のみで行うわけではなく、宛先 IP アドレス、送信元 IP アドレス、宛先ポート番号、送信元ポート番号、プロトコル番号の 5 つの番号の組み合わせで行う。

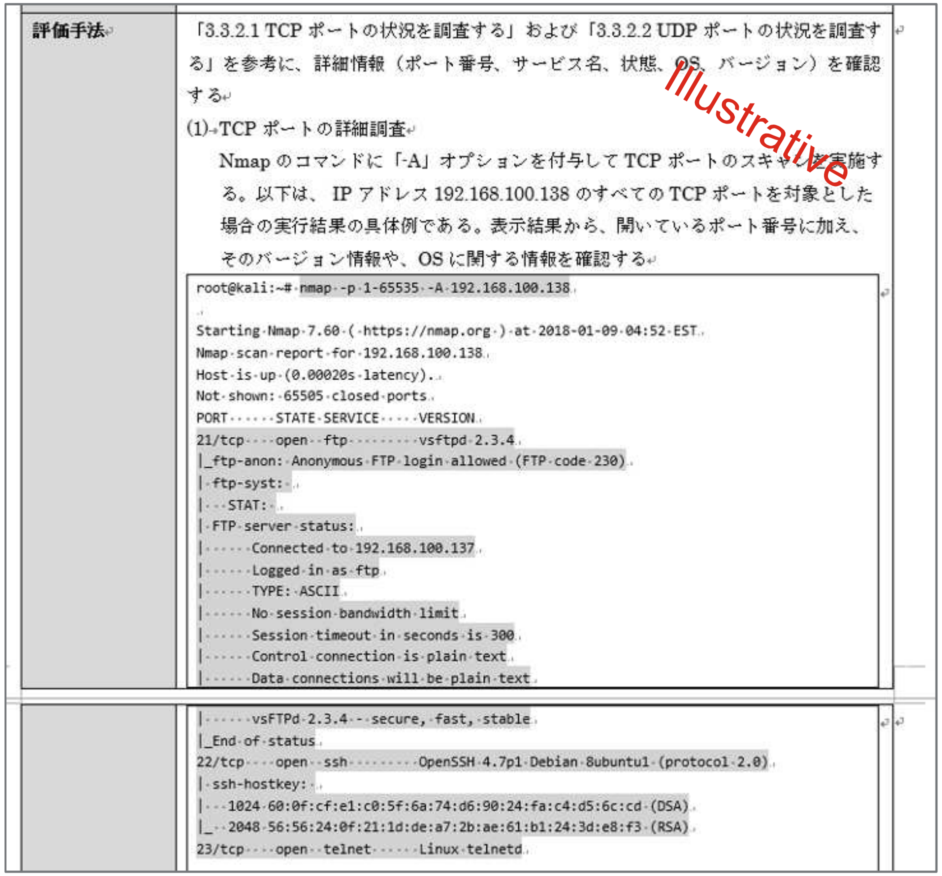
Webサーバー 192.168.100.10
アプリケーション層
http(80)
http(80)
トランスポート層
インターネット層
データリンク層
クライアント 192.168.100.11
アプリケーション層
ブラウザ (3000)
ブラウザ (3001)
トランスポート層
インターネット層
データリンク層
①
②
IPヘッダー
TCPヘッダー
送信元のポート番号で
別々の通信であることを識別

①	送信元IPアドレス 192.168.100.11	宛先IPアドレス 192.168.100.10	TCP 6	送信元ポート番号 3000	宛先ポート番号 80	データ
②	送信元IPアドレス 192.168.100.11	宛先IPアドレス 192.168.100.10	TCP 6	送信元ポート番号 3001	宛先ポート番号 80	データ

送信元IPアドレス、宛先IPアドレス、プロトコル番号、送信元ポート番号、宛先ポート番号で通信を識別

図-2-17□ポート番号による通信の識別

■ Detail description of commands and execution results



Illustrative

評価手法

「3.3.2.1 TCP ポートの状況を調査する」および「3.3.2.2 UDP ポートの状況を調査する」を参考に、詳細情報（ポート番号、サービス名、状態、OS、バージョン）を確認する

(1) TCP ポートの詳細調査

Nmap のコマンドに「-A」オプションを付与して TCP ポートのスキャンを実施する。以下は、 IP アドレス 192.168.100.138 のすべての TCP ポートを対象とした場合の実行結果の具体例である。表示結果から、開いているポート番号に加え、そのバージョン情報や、OS に関する情報を確認する

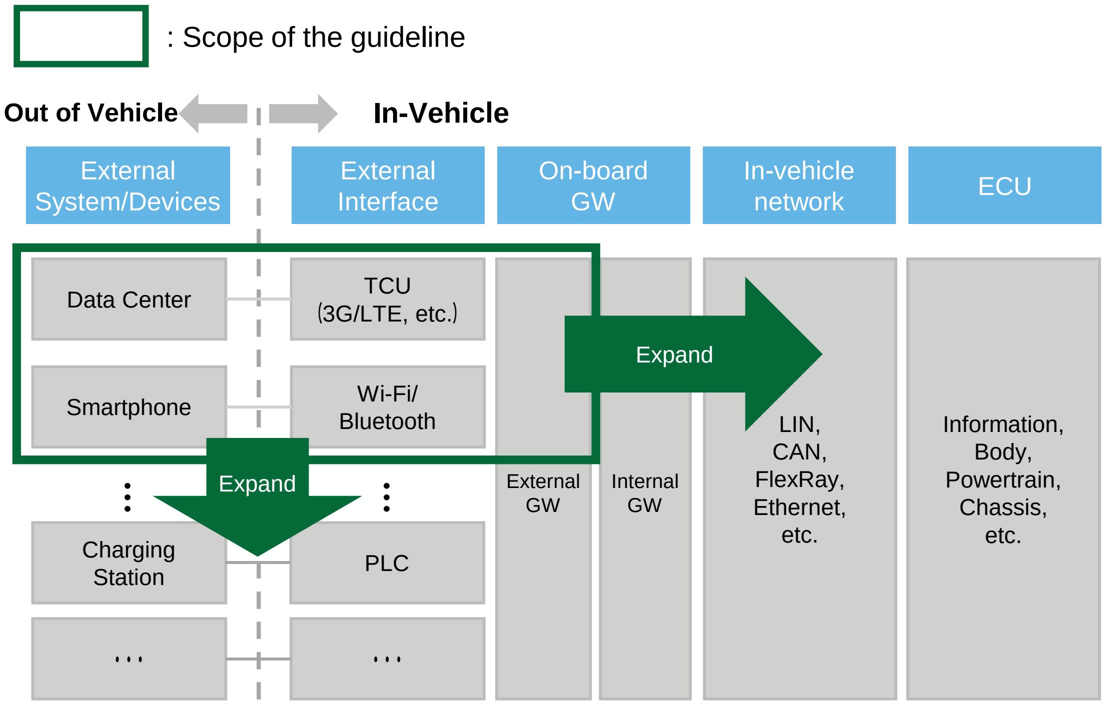
```
root@kali:~# nmap -p 1-65535 -A 192.168.100.138

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-09 04:52 EST
Nmap scan report for 192.168.100.138
Host is up (0.00020s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst: 
|   STAT: 
| FTP server status:
|      Connected to 192.168.100.137
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey: 
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
```

Key Points of Drafting Evaluation Guideline (7/7)

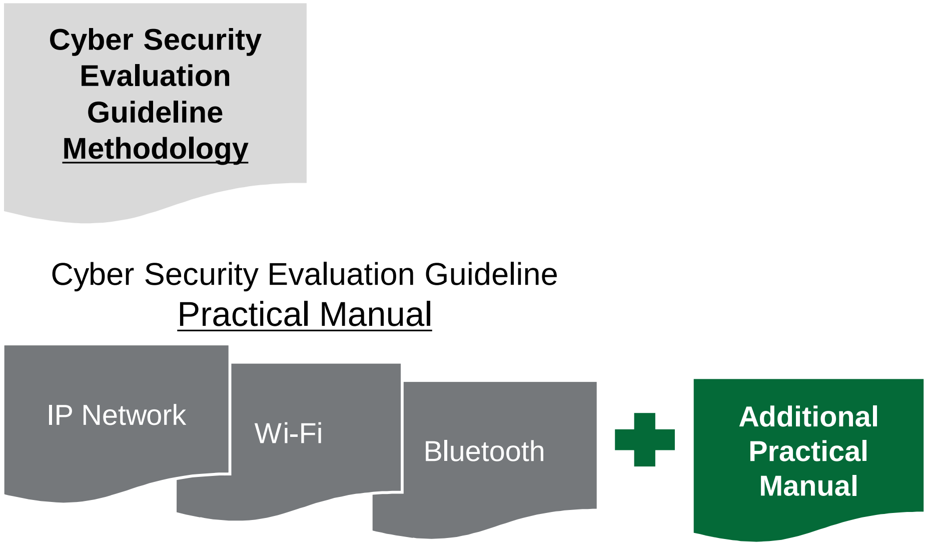
Ensuring Expandability of Guideline

7	Expandability	■ Able to expand the testing scope by adding “Practical Manual” of other communication protocol ■ Contents in "Methodology" cover the testing approaches and are not dependence on communication protocols



Expandability of evaluation scope

It is possible to expand the scope by adding practical manual of other protocol



Cyber Security Evaluation Guideline Methodology
Cyber Security Evaluation Guideline Practical Manual
IP Network
Wi-Fi
Bluetooth
Additional Practical Manual

Image of Cyber Security Evaluation Guidelines - DRAFT -

Developed Guidelines of "Methodology" and three "Practical Manual" more than total 500 pages

Cyber Security Evaluation Guidelines- DRAFT -
Methodology

< Outline >

- ■ Threat Perspective
- ■ Evaluation Process
- ■ Evaluation Report
- ■ Appendix1：Threat List
- ■ Appendix2：Evaluation Item List

Bluetooth

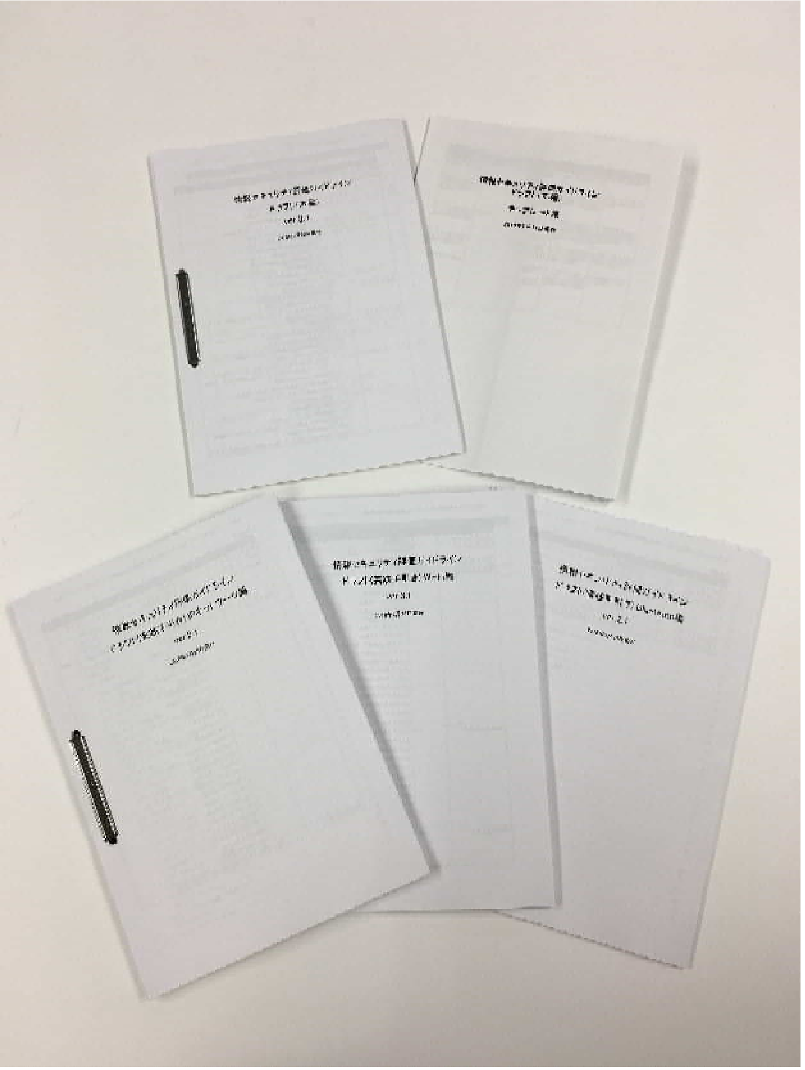
Wi-Fi

IP Network

Cyber Security Evaluation Guidelines- DRAFT -
Practical Manual

< Outline >

- ■ Protocol Overview
- ■ General Attack Methods
- ■ Testing Tools
- ■ General Evaluation Methods



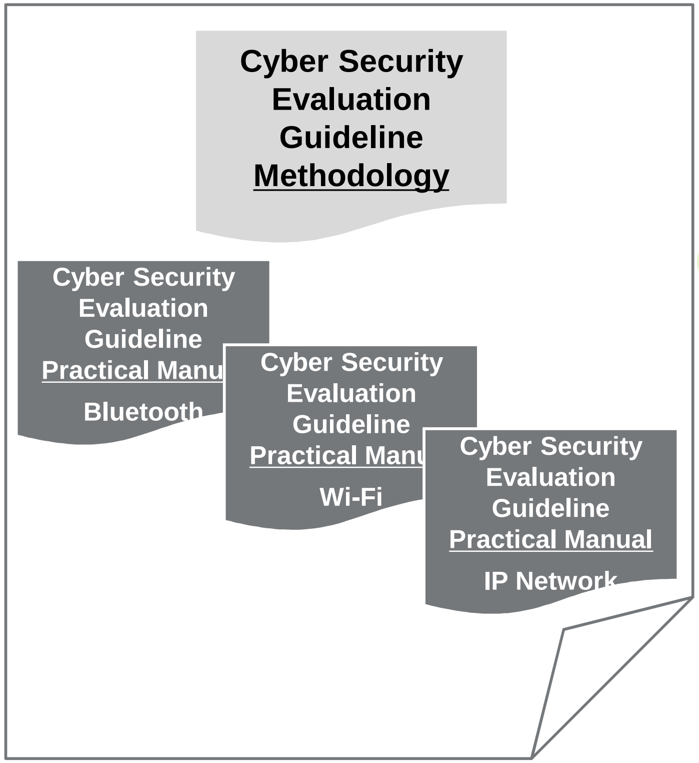
Pre-FOT of information security evaluation

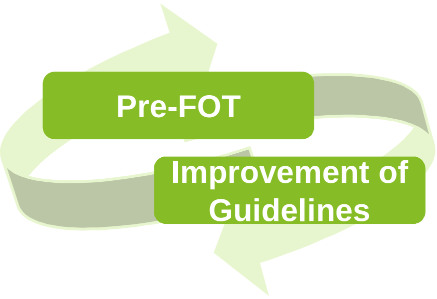
Purpose of Pre-FOT of information security evaluation

Improving effectiveness and usability of Cyber Security Evaluation Guidelines from pre-FOT

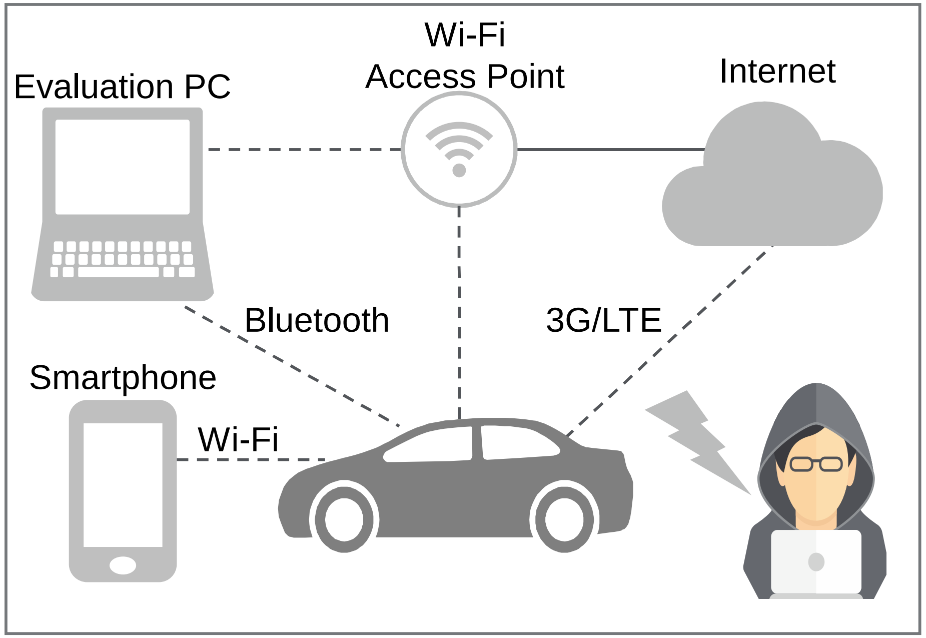
Purpose	■ To verify the validity of the drafted Cyber Security Evaluation Guidelines by conducting a penetration test on vehicle systems ■ To improve the Evaluation Guidelines from the pre-FOT

Evaluation Guideline - DRAFT -


Cyber Security Evaluation Guideline Methodology
Cyber Security Evaluation Guideline Practical Manu
Bluetooth
Cyber Security Evaluation Guideline Practical Manu
Wi-Fi
Cyber Security Evaluation Guideline Practical Manual
IP Network

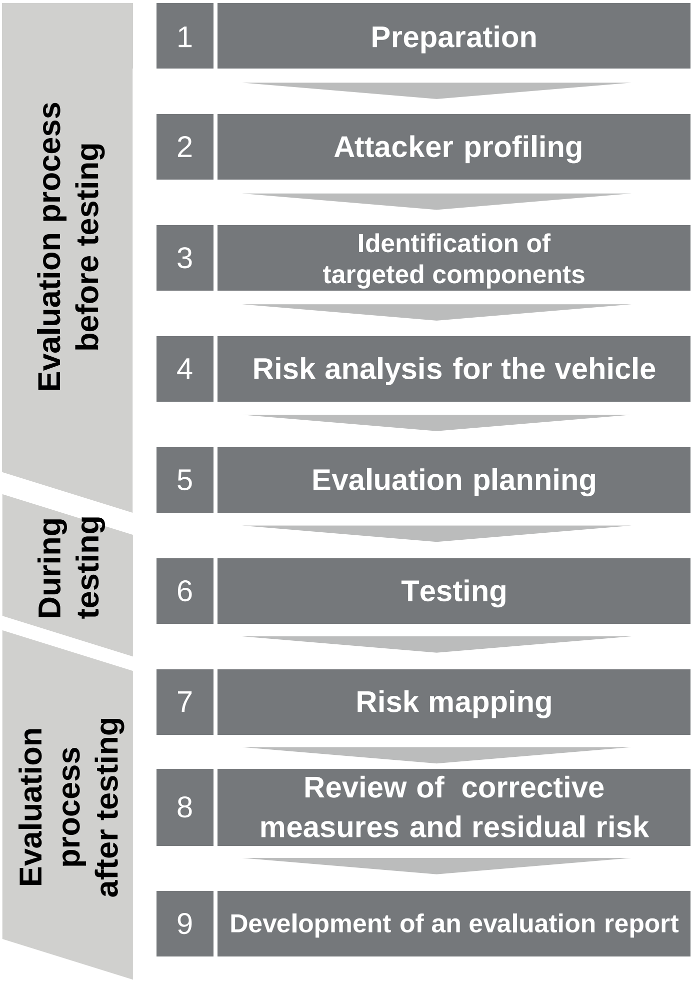


Execution of Pre-FOT in accordance with Evaluation Guideline - DRAFT -



Procedures of pre-FOT

The scope and efficacy of the draft evaluation guidelines are inspected by undertaking a pre-FOT based on the guidelines



		Evaluation flow	Outline
Evaluation process before testing	1	Preparation	➢ Coordinate with participating companies on the various terms to be agreed on
	2	Attacker profiling	➢ Define and profile possible attackers of the vehicles to be evaluated
	3	Identification of targeted components	➢ After specifying the functions (information) that could be targeted by the attackers, map the components of said functions and specify the components susceptible to attacks
	4	Risk analysis for the vehicle	➢ Evaluate component risk based on the threat agent, vulnerability, and impact factors
	5	Evaluation planning	➢ After scoping the testing target, conduct a detailed technical analysis of the relevant components and draw up an evaluation plan
During testing	6	Testing	➢ Conduct testing in accordance with the test plan
Evaluation process after testing	7	Risk mapping	➢ Conduct a risk evaluation of the vulnerabilities found during the testing process
	8	Review of corrective measures and residual risk	➢ Use the results of the risk evaluation to clarify the corrective measures required to each risk, and review residual risk after said measures have been taken
	9	Development of an evaluation report	➢ Explain and report the results of the evaluation to the relevant parties

The evaluation guidelines are to be improved based on the results of the pre-FOT

Confirmation of the validity of the drafted evaluation guidelines and pre-FOT reporting

Confirming the validity of the draft evaluation guidelines

Validity confirmation checklist

- Confirmation of validity is based on the seven strengths and advantages of the evaluation guidelines
  - Usability
    - Confirm that the guidelines can be applied to vehicles already on the market
  - Efficiency
    - Confirm that evaluation can be completed within a realistic timeframe
  - Reproducibility
    - By employing quantitative evaluation, confirm that the results of evaluation can be reproduced
  - Effectiveness
    - Secure the efficacy of the guidelines by providing feedback and making corrections based on issues identified during the evaluation process
  - Sufficiency
    - Confirm that the evaluation guidelines can detect vulnerabilities
  - Specificity
    - Confirm that the content of the guidelines can be understood by testers with a standard skill level
  - Expandability
    - Confirm that there is no repetition in the practical guide, and that the scope of the guidelines can be expanded by adding I/F protocols

Producing a pre-FOT report based on the drafted evaluation guidelines

Pre-FOT report on information security evaluation (excerpt of contents)

1. Executive summary

1.1. Objective

1.2. Scope

1.3. Execution

1.4. Risk evaluation

1.5. Key findings

1.6. Conclusion

2. Details of the evaluation

2.1. Evaluation environment

2.2. Evaluation team

2.3. Evaluation method

3. Evaluation results

3.1. Risk evaluation of vulnerabilities discovered in penetration test processes

3.2. Detailed findings

3.3. Evaluation activities

Appendix A: Hardware hacking and reverse engineering

Appendix B: Detailed evaluation activities

Preparation for the FOT in FY 2018

Background and aims of the field operational test

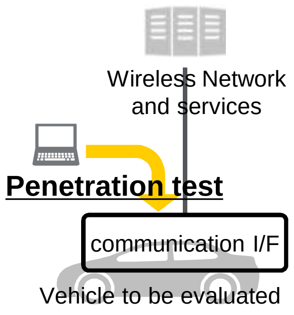
The FOT is conducted to establish a method for evaluating wireless network-based attacks on vehicles

Background

- Toward the 2020 Tokyo Olympic and Paralympic Games, it is important to accelerate the practical realization of automated driving systems
- Involving auto manufacturers and other parties, it is necessary to conduct a large-scale FOT focusing on five sectors of technology (dynamic maps, HMI, information security, reduction of pedestrian accidents, and next-generation urban transport) and, with a view to practical realization going forward, highlight specific issues in areas including technology, operations, and systems

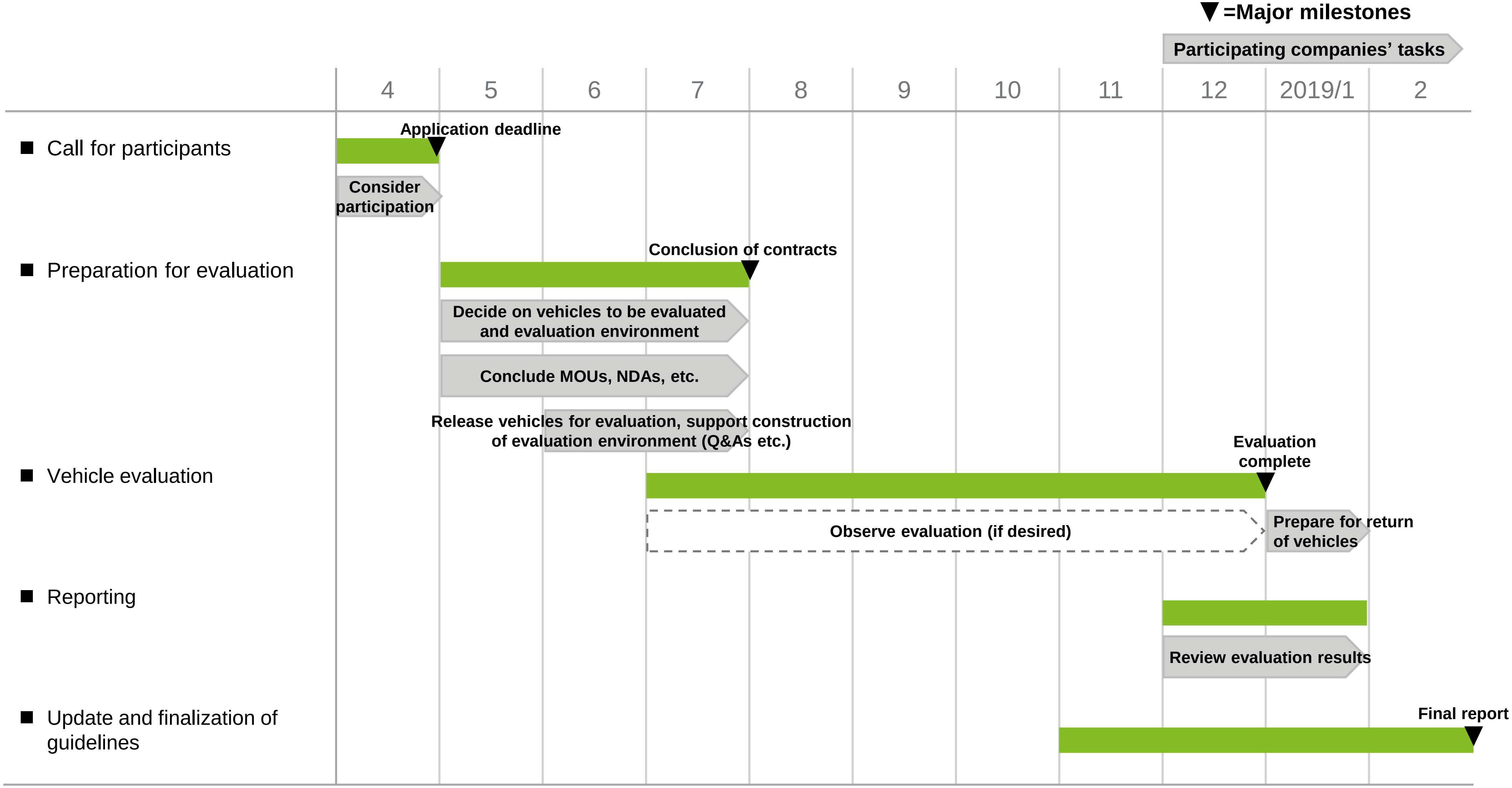
Aims

- By developing vehicle- and component-level security evaluation methods and protocols in the form of guidelines, and conducting black box experiments testing resistance to hacking by using vehicles provided by those participating in this FOT, establish **a method for evaluating wireless network-based attacks on vehicles**



Overall schedule for the field operational test

Recruitment of participating companies will be done in April, evaluation will begin in July after each company's preparations are complete, and the evaluation process is expected to be finished by the end of December



▼ =Major milestones

Participating companies' tasks

4 5 6 7 8 9 10 11 12 2019/1 2

- Call for participants
  - Application deadline
  - Consider participation
- Preparation for evaluation
  - Conclusion of contracts
  - Decide on vehicles to be evaluated and evaluation environment
  - Conclude MOUs, NDAs, etc.
  - Release vehicles for evaluation, support construction of evaluation environment (Q&As etc.)
- Vehicle evaluation
  - Evaluation complete
  - Observe evaluation (if desired)
  - Prepare for return of vehicles
- Reporting
  - Review evaluation results
- Update and finalization of guidelines
  - Final report

Note: The above schedule is based on assumption on the most effective progress, but actual tasks can be adjusted based on participants' needs

Requirements related to the vehicles to be evaluated and the evaluation environment (1/2)

Participating companies need to agree on various requirements related to the provision of vehicles for evaluation

The following is based on current assumptions, with details set to be adjusted with each company after entry into the project

■ On the provision of vehicles for evaluation

Vehicle requirements	Please prepare a system with at least one of the following wireless network functions: **Wi-Fi**, **Bluetooth**, **3G/4G/LTE**
Vehicle types	Vehicles to be evaluated are assumed to be either **development vehicles or commercially available vehicles**.
Form of vehicle provision	If it is difficult to provide an **actual vehicle**, a **test bench (parts system)** will be accepted. However, the system needs to fulfill the "Vehicle requirements" above and the wireless network communications needs to be testable.
Time of provision	We are looking at a **6-month period.** (The actual time of evaluation is expected to be 2-3 months per vehicle, but because multiple vehicles are being evaluated simultaneously, we would prefer the leeway afforded by a 6-month period. In case a shorter period is required, this can be adjusted individually.)
Spare parts	In addition to one vehicle for evaluation, please provide **spare parts (parts systems including the head unit required for evaluation)*** for the vehicle in question. *Please provide at least one unit. Provision of two or more units will allow for more in-depth evaluation.

Requirements related to the vehicles to be evaluated and the evaluation environment (2/2)

Participating companies need to agree on various requirements related to the provision of vehicles for evaluation

The following is based on current assumptions, with details set to be adjusted with each company after entry into the project

■ On the provision of vehicles for evaluation (continued)

Maintenance support	If problems occur during the construction of the evaluation environment or during evaluation, please be prepared to offer **maintenance support** for the vehicles being evaluated. (Concrete measures include the establishment of a point of contact and coordinating with the suppliers of relevant parts.)
Cost of vehicle provision	**Each participating company will be responsible for the costs of vehicle provision (assumed to include the vehicle itself, transport costs, and spare parts).** We will bear all other related costs (manuals etc.).
Status of vehicles at the time of return	Please be aware that vehicles may be damaged during the evaluation process, and that they will be returned as is.

■ On the preparation of the evaluation environment

External transmission environment	Please prepare the **network services and servers** necessary for telematics. The servers should be running a **test environment** for verification or similar purposes (please also prepare test accounts). In addition, we would appreciate the connections between the vehicles and servers having been tested before vehicle provision.
Information provision	We would appreciate provision of **user and service manuals** (with the same scope of information provided to general users) for the vehicles (we will bear the costs for these).
Consent	Consent for evaluation of vehicles and servers by way of simulated cyberattacks is earned by exchanging memorandums of understanding, non-disclosure agreements, and letters of confirmation (described later).

About information security management

As some of the information handled during the FOT is extremely sensitive, thorough measures must be taken to ensure security

Security measures for preventing information leaks when cooperating with overseas group companies

The below measures are to be taken to prevent leakage of classified information at oversea group companies.

1. Minimize the amount of information available to team members outside of Japan

The following measures are to be taken to minimize the amount of information related to the project available to team members outside of Japan:

- Evaluation is to be conducted only within Japan
- Team members outside of Japan are to take part only as advisors, and may not conduct actual evaluation work
  (Team members outside of Japan should only be given the information required in order for them to share their knowhow and knowledge)

In addition

2. Take contractual measures to prevent information leaks to external parties by team members outside of Japan

The security of classified information related to the project and available to team members of overseas group companies is to be guaranteed by including a confidentiality clause in the contract between the Japanese party and the group companies.

Securing evaluation-related information among participating companies

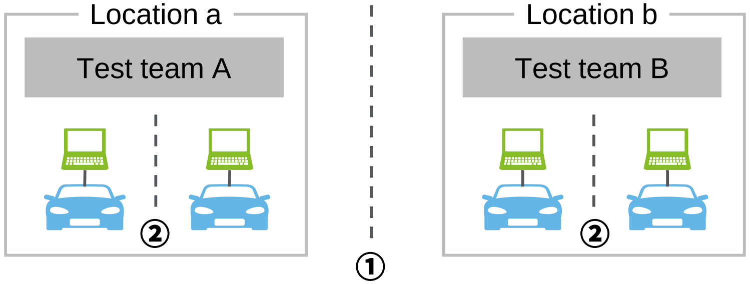
Security is to be ensured by physically dividing evaluation environments.

1. Physical separation of evaluation sites

Security between evaluation sites is to be ensured by conducting evaluation at two separate sites (each one with separate evaluation teams conducting the evaluation) and by not moving evaluation vehicles between the two sites.

2. Physical division of the testing environment

When several vehicles are being evaluated at the same site, the testing environments (including PCs used for evaluation and other equipment) are to be physically separated from each other to ensure security.



In addition to the above, as evidenced by having obtained the international ISO/IEC27001 information security management certificate, our information security management conforms to the international standard, and sufficient security measures will be taken with regard to this project

Scope of disclosing evaluation results

Vehicle-specific evaluation results, items, and procedures are to be disclosed only to the participating companies

- As stipulated in the non-disclosure agreement concluded between each participating company and NEDO, vehicle-specific evaluation results are to be disclosed only to the relevant participating company.

Legend O: Can be disclosed
X: Cannot be disclosed

Type of information		Scope of disclosure		
		Provider of evaluation vehicle (participating company)	Managing entity of the FOT (NEDO)	The public (in guidelines etc.)
1	Vehicle-specific evaluation results	○	×	×
2	Vehicle-specific evaluation items and procedures	○	△[2]	×
3	Statistical[1] evaluation results	○	○	○
4	Generalized evaluation items and procedures	○	○	○

[1] “Statistical” here refers to evaluation data for multiple vehicles which has been formatted to express qualities and tendencies in quantitative form, and which cannot be used to identify any of the participating companies.

[2] Disclosure within the limits consented to by the participating companies.