Cross-ministerial Strategic Innovation Promotion Program(SIP) Automated Driving System Large Scale Field Operational Test: - Information Security Field Operational Test -

Project Summary

PwC Consulting LLC

February 28, 2019

pwc

Project Activities Overview

In this project, "Vehicle Security Evaluation Guideline" was developed through "Information Security Field Operational Test" to benefit automakers and suppliers.

Environment around Automated Driving System

- It is expected that **<u>various information will be obtained from external vehicular networks to realize automated driving system</u>**
  (e.g. High definition map data, vehicle/pedestrian/road infrastructure information)
- Such situation could lead to cause **<u>cybersecurity issues that did not exist in the time of conventional non-connected cars</u>**

Overview & Project Goal

The project aims to realize the following goals through; **<u>research & analysis for security threats</u>**, **<u>establish security evaluation method/protocol at vehicle/component level</u>** towards international standardization, **<u>conduct technical research to verify security endurance</u>** by black-box testing of vehicle systems provided by the participants

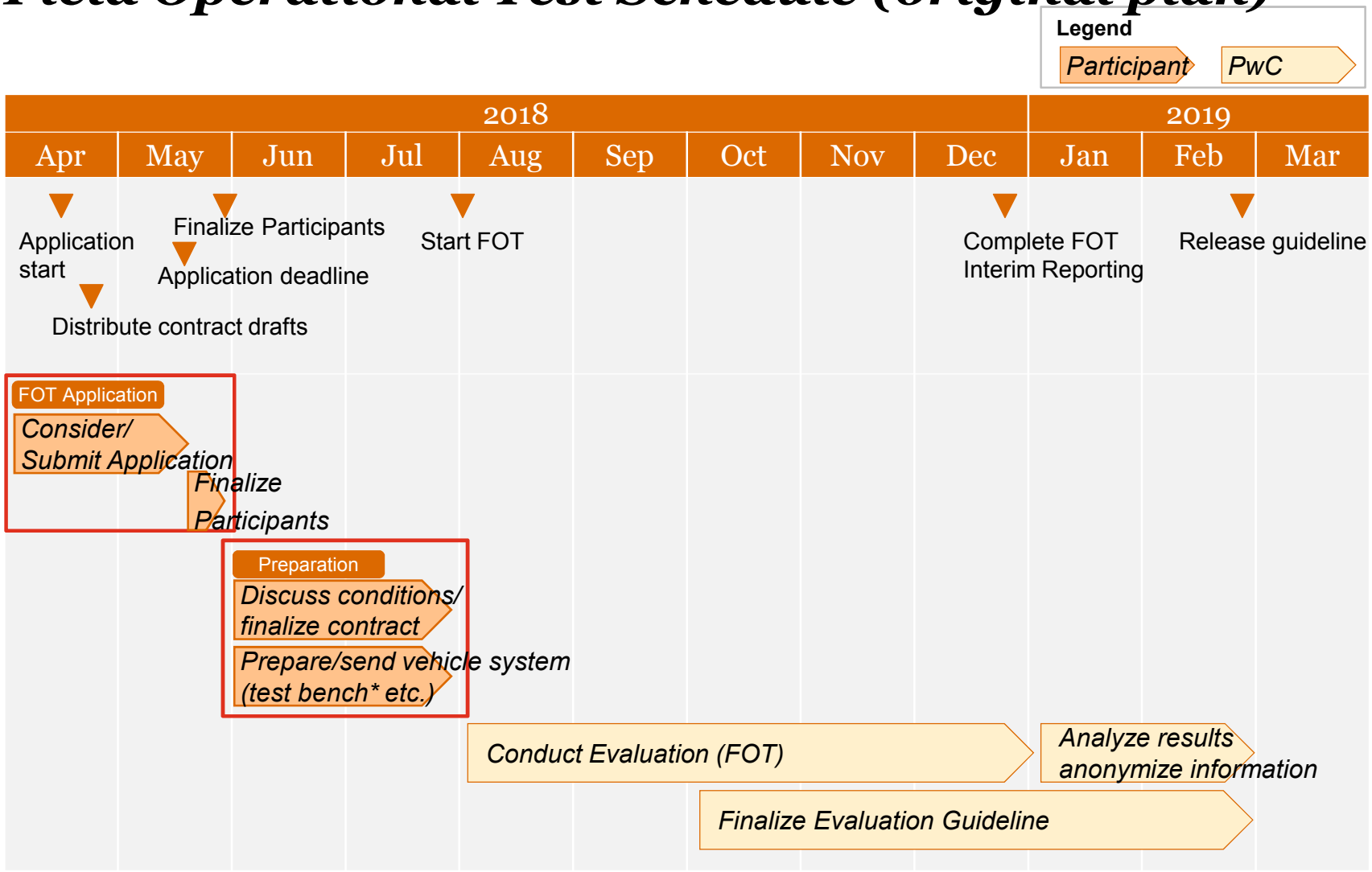
1. Establish an evaluation method against external-vehicular attacks
2. Establish comprehensive threats model for external vehicular attacks including V2X etc.
3. Build consensus on cybersecurity of automated driving vehicles
4. Develop human resources and accumulate knowhow related to automated vehicle cybersecurity in Japan

Project Overall Schedule & FY18 Schedule

In FY18, black-box tests were conducted on multiple vehicle systems using the draft of the "Information Security Evaluation Guideline (the Guideline)" developed in FY17 to finalize the Guideline by reflecting the test results.

Project Phase	Items	Details	Period
FY17 Trial Research (Step1)	Threat analysis for automated driving system	• Research/analyze comprehensive picture of threats against the automated driving system	2017/9 ～ 2018/2
	Develop draft of Information Security Evaluation Guideline	• Develop guideline (draft) based on known security incidents, vulnerabilities and/or evaluation methods • Conduct trial research/evaluation using the guideline (draft) • Finalize the guideline (draft) based on the results	
	Trial research for Information Security Evaluation		
FY18 FOT (Step2)	Preparation for the field operation al test	• Recruit JOEMs to participate in the FOT • Make necessary arrangements with the participants including evaluation subject, environment, period etc.	2018/4 ～ 2019/7
	Information Security Evaluation (Field Operational Test)	• Conduct multiple security evaluation on the vehicle systems provided by the participants using the guideline (draft)	2018/8 ～ 2019/2
	Finalize Information Security Evaluation Guideline	• Finalize the guideline by analyzing the evaluation results to clarify improvement points and reflect them to the guideline.	

Field Operational Test Schedule (original plan)



* Test bench: A group of components/part of a vehicle system that consists of the devices that enable Wi-Fi/BT/Cellular wireless communication

FOT application steps

Following shows application steps to participate in the FOT.

	Review Application					Submit Application
	Announce-ment	Request application	Briefing Session	Review	Review draft contracts	Application
	4/16	4/17	4/17～until deadline (5/23)		4/26	~5/23
Participant (OEM)	-	• Confirm application request	• Attend briefing session (voluntary)	• Review application internally • Queries	• Receive draft contracts	• Submit application form
PwC	-	• Request application to candidates • Send documents	• Arrange briefing session	• Receive & reply queries	• Send draft contracts	• Receive application • Inform secretariat
Secretariat (NEDO)	• Announce project	-	• Confirm briefing session results	• Receive & reply queries	-	• Receive application results

FOT preparation steps

Following shows preparation steps towards the FOT. Evaluation period/timing was coordinated within the project period based on each participants' situation.

	Finalize Participants		Preparation for FOT			
	Finalize participants	Announce participants	Coordinate conditions	Finalize contracts	Prepare systems	Conduct FOT
	5/23~5/end	5/end	~7/end			8/1~*
Participant (OEM)	-	• Receive participation acceptance	• Coordinate subject system. Inform details to PwC	• Coordinate internally towards contract • Sign contract	• Prepare/send subject system • Provide necessary logistics/setup information	• Setup technical support window
PwC	-	• Confirm participants	• Coordinate evaluation period, environment etc.	• Coordinate contract details	• Prepare evaluation environment	• Receive subject system • Conduct Evaluation
Secretariat (NEDO)	• Finalize participants	• Inform participants	• Monitor project progress • Support coordination between PwC and participants as necessary			

* Evaluation to be conducted for two months for each participant in between August-2018 and January-2019.

FOT Contract Structure

Following shows the contracts discussed and agreed between PwC and the participants.

① MOU for FOT

Includes overview of the FOT, general conditions/agreements in participation the FOT

② Property Lease Agreement

Includes details related to the items(system) provided for the FOT (period, use conditions etc.)

③ Non Disclosure Agreement

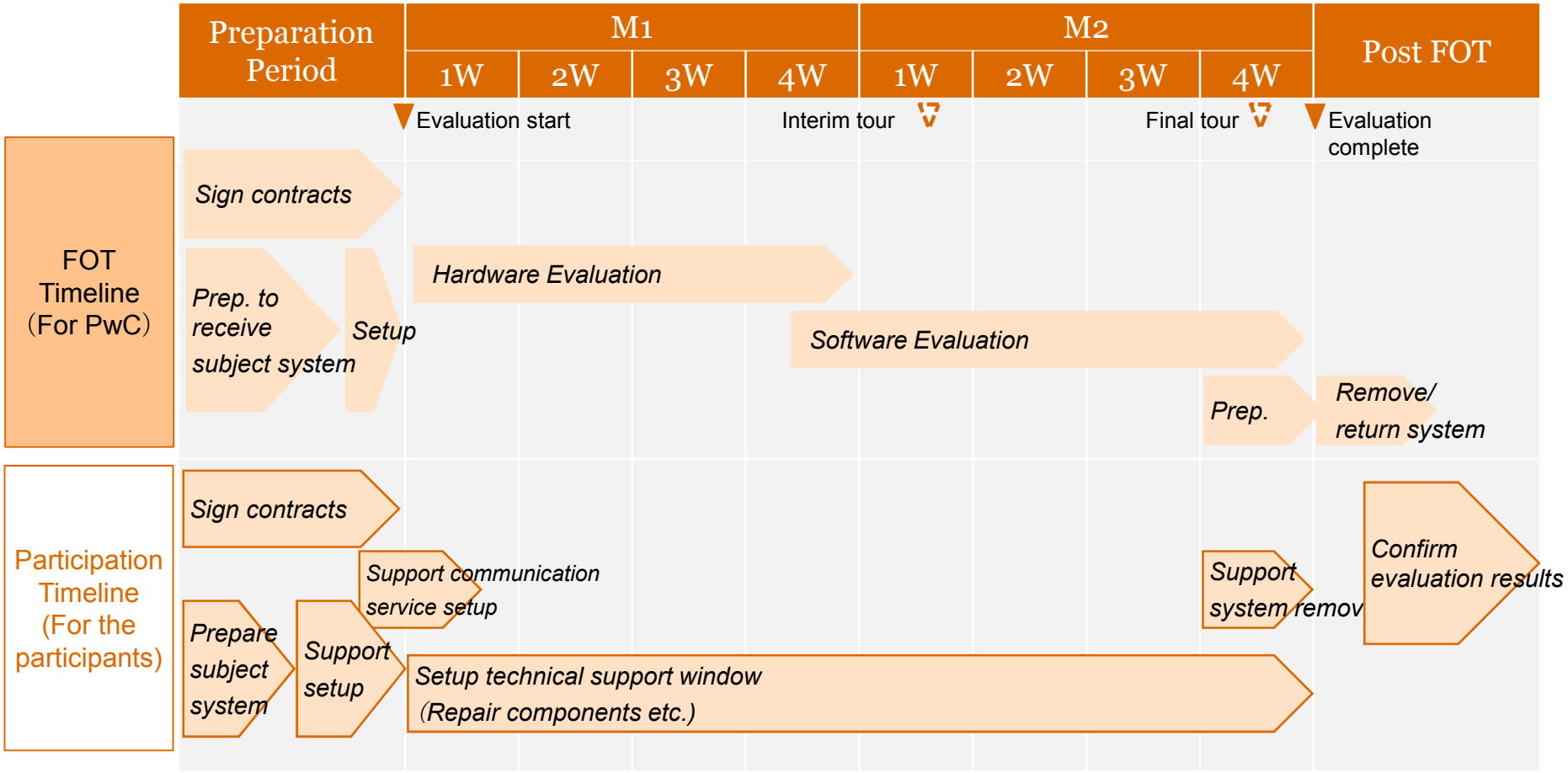
Includes handling and scope of disclosure for the information obtained/generated through the FOT

④ Other contracts

Contracts for communication service usage, other specific needs from the participants etc.

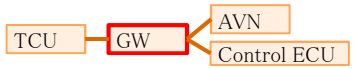
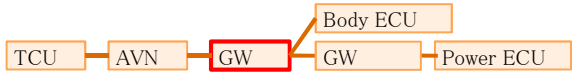
Details/Timeline for participation

After the contract, participants provided necessary support based on the FOT timeline.



Items provided for the FOT(1/2)

Participants were requested to provide following items during the FOT period.

No.	Mandatory	Item	Qty	Conditions	Remarks
1	○	Vehicle test bench*1	1	• Information ECU and Gateway ECU* are connected and communicable • Capable of connecting to telematics service (including test services) • Possesses in-vehicle interfaces accessible by general users. (Display, microphone, USB port, touchpad etc.) • Possesses communication antennas for GPS, Cellular etc.	The test bench needs to have wireless communication functions of an actual vehicle, such as Wi-Fi, BT, cellular. Connectivity to telematics services are not mandatory but required in most test cases.
2	○	Information ECU	3 sets	• Capable of connecting to telematics service server (including test server) • Possesses communication components such as TCU, AVN • Possesses communication components such as Wi-Fi, BT, Cellular etc.	In case another ECUs (TCU, DCM etc.) has wireless communication function, such ECUs also needs to be provided.
3	○	Gateway ECU		• Gateway (marked as red) Ptn1: Central Gateway  Ptn2: Multiple Gateways  Ptn3: No gateway 	In the Guideline, access and/or falsification of the gateway firmware is considered a point when attacks to the control systems can be successful. (as shown in Ptn.1) Investigation required for Ptn2 & 3 on application of the evaluation method in the Guideline.

*1 In case of vehicle under development, it is preferred that information regarding setting/specification etc. only applicable during development phase as well as expected setting/specification at the time of commercial phase are provided in order to obtain reasonable evaluation results.

Items provided for the FOT(2/2)

No.	Mandatory	Item	Qty	Conditions	Remarks
4		Telematics service user account	4 (2 minimum)	• Accessible to all services provided to general users. (test service account is acceptable)	4 accounts in case an information ECU and accounts are associated 2 even in case a ECU and account are not associated as some test may require multiple accounts
5		Telematics service server (operating)	—	• Operate a server accessible from the vehicle test bench or other communication component using the account provided as per No.4 throughout the FOT period	Following may be performed during the evaluation process: 1. Use services accessible by general users 2. Investigate server information over the network (host name, certification, port number etc.) Anything that may disrupt the service will not be performed.
6		Smartphone application (test)	1	• Accessible to the telematics service (Android)	Interception of communication via smartphone application is performed during the “Reconnaissance” phase. An application accessible to test servers are not publically distributed so binary files needs to be provided from the participants. Require Android application as iPhone require jailbreak which restricts the OS versions.
7		Manuals	1 each	• Owner’s manual, service manual etc. that are publically accessible	-
8	○	Wiring diagram	1 set	• Provide information on required voltage etc. for each ECU connecters	In some cases, an ECU may be powered without connecting to other systems.

Support provided for the FOT

No.	Timing	Item	Period	Details
1	Before starting Evaluation (Assuming by end of July)	Sign contracts* • MOU for FOT - Includes acceptance for vehicle/component hacking** • Property Lease Contract • NDA • Other contracts (Communication service agreement etc.)	-	• Internal arrangements and preparations etc. towards contract signing.
2		Arrangement for conditions for items to be provided	-	• Discuss items to provide, deliver and other conditions necessary
3		Prepare vehicle/components	-	• Prepare vehicle/components and their delivery.
4	Upon starting Evaluation	Support for installing vehicle/components	-	• Provide necessary information for transportation, installation of the vehicle/components
5		Support for initial connection of communication service	1 week	• Provide support for connecting to communication service etc.
6	During Evaluation	Provide technical support	Approx. 2 months	• Provide support for repairing initial failure or failure unrelated to the test
7	After Evaluation	Support for returning vehicles/components	-	• Provide information regarding transportation, uninstallation of the vehicle/components
8		Confirm and provide feedback on Individual Evaluation Report	-	• Confirm individual vehicle evaluation report and provide feedback to PwC (optional)

Project work and cost distribution

Vehicle systems and related components required for the FOT were provided from the participants. Other cost distributions were as follows.

No.	Item category	Expected Cost	Cost Distribution	
			PwC	Participant
1	Provide vehicle systems, components	Cost related to leasing, logistics and setup of the vehicle system and components	-	○
2	Provide communication/telematics services	Server operation cost, other costs related to maintaining test environment	-	○
3	Prepare testing tools	Cost related to purchase, license of test tools, software and other devices required for the FOT	○	-
4	Provide technical support	Cost related to operation check, initial failure response etc.	-	○
5	Manage FOT environment (test lab.)	Cost related to maintaining the test lab. as well as its safety and information security implementation	○	-
6	Manage assets during the FOT	Cost related to maintenance, management of the vehicle system, components during the FOT	○	-
7	Arrange FOT tour (test lab. tour)	Cost related to arrangement of FOT tour, demonstration for the participants	○	-
8	Create individual report	Create individual report of evaluation results	○	-
9	Develop Information Security Evaluation Guideline	Updating the Guideline through FOT results	○	-

Laboratory Tour (not mandatory/request base)

Interim/final results were reported along with demonstration using the actual system.

Event	Timing	Location	Agenda (example)
Interim Tour (Lab tour)	4-5 weeks after the start of FOT	Otemachi, Tokyo (PwC HQ)	• Interim report on the evaluation progress • HW hacking demonstration
Final tour (Lab tour)	Before the end of the FOT	Otemachi, Tokyo (PwC HQ)	• Evaluation report • HW hacking demonstration • Brief security advisory session based on the evaluation results

FOT confidential information and disclosure scope

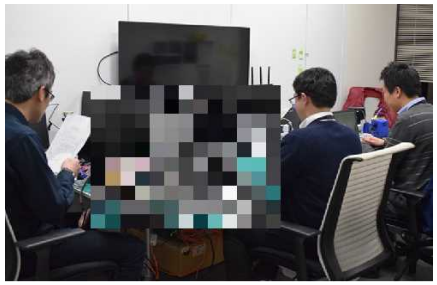
Scope of disclosure of the information, items provided by the participants, information presented from PwC were managed and restricted as follows.

Category	Item	Details	Owner	Scope of Disclosure			
				Individual Participant	All participants	SIP-adus related parties, NEDO*1	Public
Project phase	1. Application*2	Application submitted for the FOT	PwC	○	✖	○	✖
	2. FOT progress (anonymized)	Progress report of the FOT (anonymized)	PwC	○	✖	○	✖
Vehicle system	3. Vehicle system/ components	Information about vehicle systems and components provided for the FOT	Participant	○ (PwC)	✖	✖	✖
Evaluation procedure	4. Evaluation procedure for each participant	Evaluation procedures specific to each provided systems	PwC	○	✖	✖	✖
	5. Document format	Reporting format etc.	PwC	○	○	✖	✖
	6. Guideline (Public)	Guideline updated through the FOT	PwC	○	○	○	○
Evaluation results	7. Evaluation Result (Individual report)	Summary report of the results -Procedure including the techniques/tools used -Evaluation results (highly confidential)	PwC	○	✖	✖	✖
	8. Evaluation Results (anonymized)	Evaluation results anonymized for public disclosure	PwC	○	○	○	○

PwC *1 Confidentiality obligation
*2 Organization applied will be share to NEDO and SIP related parties for the purpose of finalizing participants. Name of the participants will not be publically disclosed.

FOT Site/Test Environment – Security of the Evaluation Facility

Evaluation work took place exclusively at PwC's "Hardware Hacking Lab."

Item	PwC Facility (Hardware Hacking Lab.)
Overview	PwC's research facility exclusively build for testing of IoT/embedded products including vehicle systems.   
Location	1-1-3, Otemachi, Chiyoda-ku, Tokyo Ote Center Building 19F
Security	Implemented * Details explained in the next page
Equipment	Hardware hacking equipment (Full sets used in FY7 trial research)
Capacity	Up to 4 vehicle systems (test bench)
Logistics	Able to bring in cargo size of up to H 200cm x W 98cm

FOT Site/Test Environment – Security of the Evaluation Facility

The faculty used for the FOT provides required information security for the FOT to handle confidential information.

Security Implementation	PwC Facility (Hardware Hacking Lab.)
Entrance Check	ID check by the security guard at the building entrance
	Two ID authentication doors based on PwC's area security management standard
Authentication Device	ID authentication on the lab. door (only registered evaluator can enter the lab.)
	Finger print authentication on the lab door. (only registered evaluator can enter the lab.)
Entry/Exit Control(record)	All entry/exit are recorded and managed
Security Monitoring/ Surveillance	Video recorded by the surveillance cameras. (The record preserved for three months.)

Guideline verification through FOT involving JOEMs

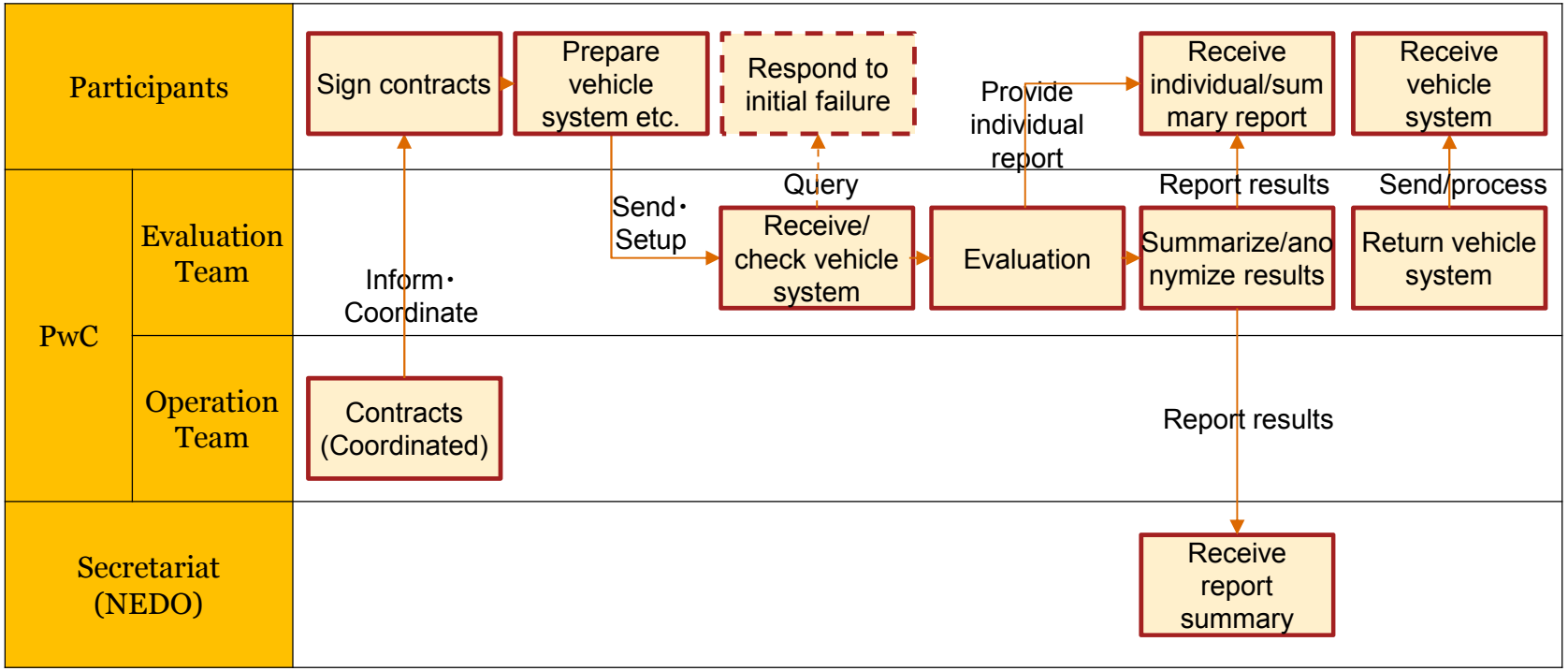
In FY18, FOT was conducted with **participation of 4 Japanese automakers** each providing their vehicle systems for the security evaluation.

FY18 FOT participation flow

Requested 10 JOEMS for participation	Application from 4 JOEMS	FOT completed with 4 JOEMS
• Requested 10 JOEMs to participate in the FOT • Briefing sessions conducted	• 4 OEMS applied to participate (submitted application)	• Coordinated contract conditions etc. to start FOT • Completed FOT for all 4 by the end of Jan-19

FOT Evaluation flow

Workflow from the FOT preparation to conducting FOT is as follows.
Penetration testing based on the evaluation guideline(draft) was conducted as FOT.



FOT Information Security Evaluation Overview

Evaluate cybersecurity performance of the vehicle systems through simulated attacks(evaluation) based on the Guideline.

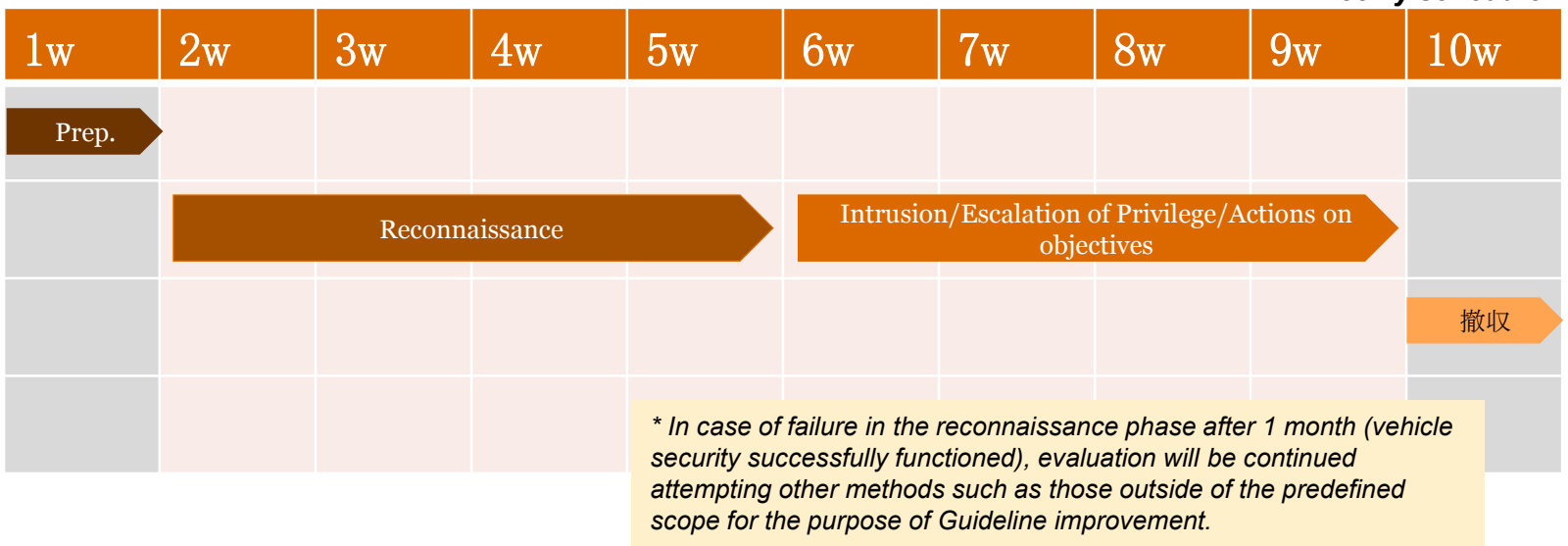
Assessment results are base on success of attempt(attack) in each evaluation phase conducted for predefined period of time (period based on existing cases)

・”Reconnaissance” phase (information collection for HW hacking) ・・・・ ***4 weeks***

・In case of failure in the Reconnaissance attempt (failure to collect information), security is confirmed as later phases of attacks cannot be performed.

・”Intrusion/Escalation of Privilege/Actions on Objectives” phase ・・・ ***4 weeks***

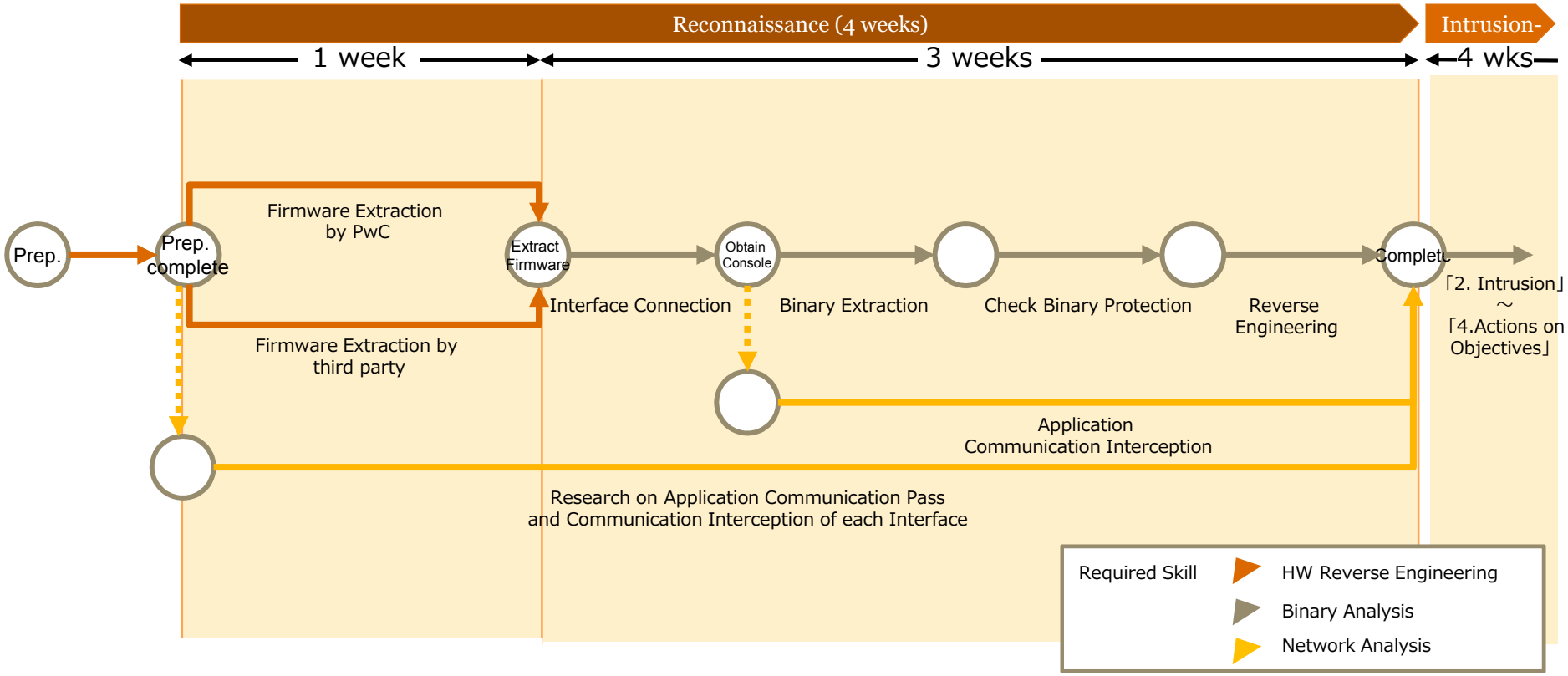
Weekly schedule



Evaluation method: Reconnaissance

Evaluation regarding information collection for vehicle system intrusion

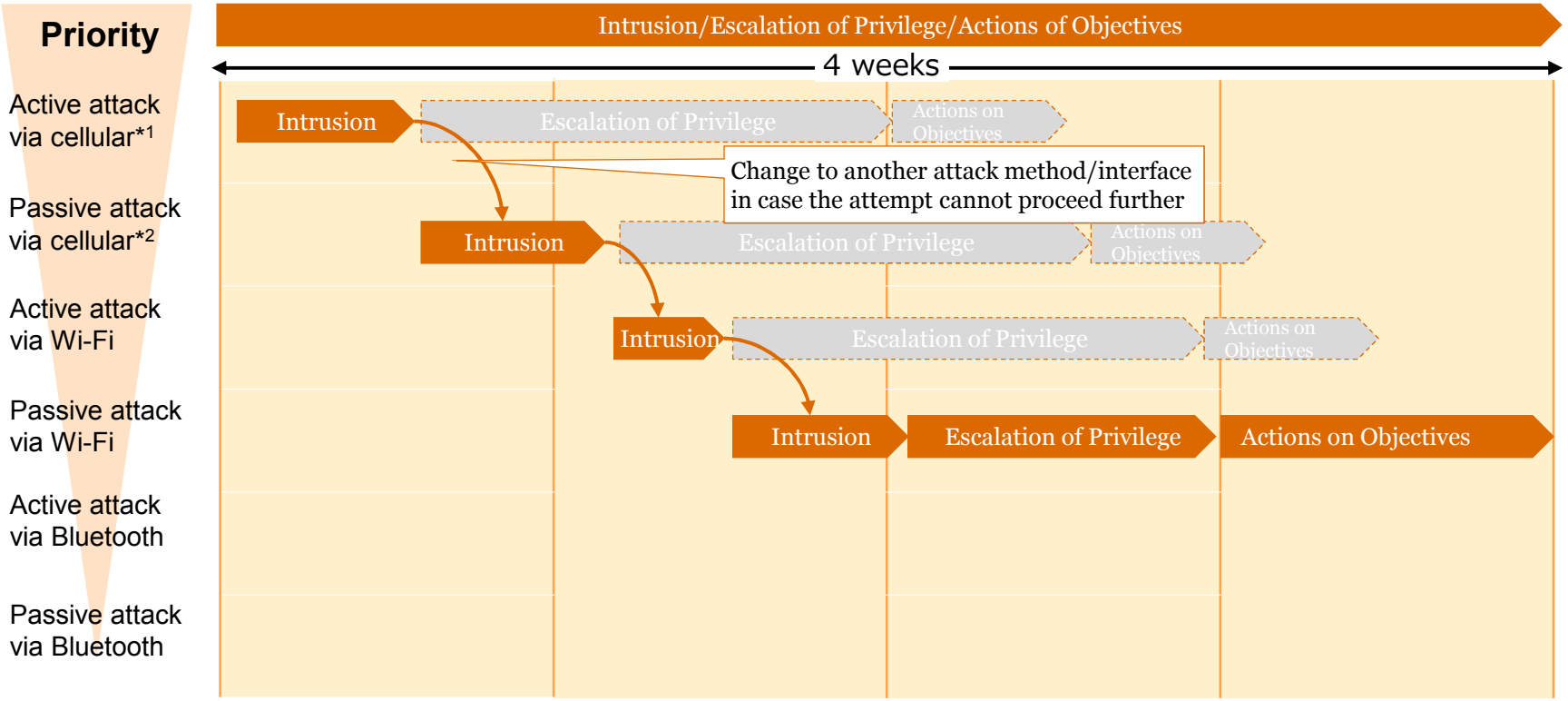
- Based on findings from FY17 results, HW reverse engineering is concentrated in the earlier phase, and part of the work is contracted to expert third party to complete all procedures within 4 weeks.
- Standard 4 weeks are set as standard period. The validity of the duration will also be verified through the FOT.



※1 Analysis of the hidden interfaces required extremely high level of reverse engineering skills as well as extended duration (2 month), therefore only check tamper-resistance at public document level.

Evaluation Method:
Intrusion/Escalation of Privilege/Actions of Objectives

Proceed from "Intrusion" to "Attack on Objectives" for each external communication interfaces based on the following priority. Within standard evaluation period of 1 month, attempt all attack methods and from all interfaces. For "Escalation of Privilege" and "Actions on Objectives", a successful attempt through one interface will be considered as the same results achieved from other interfaces.



*1 Active attack: An attack method which can be completed solely by attacker's actions (cf. FCA Jeep Cherokee hacking case)
*2 Passive attack: An attack method which require certain action by the driver/vehicle owner (cf. Tesla Model S hacking case)

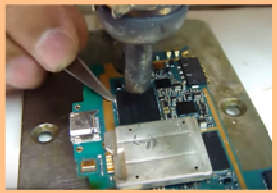
FOT Evaluation Report (image)

The report summarizes impact of the potential incident and reproduction procedure regarding the security issues identified through the evaluation. Advisory on the countermeasure will also be provided taking into account the impact, attack conditions/difficulty.

Evaluation Procedure(image)

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

Evaluation Report(image)

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

Evaluation Criteria Definition

Evaluation criteria are as follows. Each criteria were validated through the results of the FOT and necessary changes were reflected to the final guideline.

Evaluation Condition	Method to realize reproducible evaluation	Verification method in FOT
1. Evaluator Skill	• Identify necessary skills to be checked/rated by the managers in prior to the evaluation work. • Include the checking process in the guideline	Cross-check validity of the skill check based on the results of evaluation items covered by each tester
2. Evaluation items	• Identify procedures described in the guideline	Evaluate variation of the evaluation items covered based on work evidence and results
3. Evaluation Workload	• The FOT sets standard period of 2 months (40 working days) x 2 evaluators	On precondition that No.1 & 2 were met, confirm whether the results meet the criteria for the participants
Evaluation Subject (vehicle system)	• Specify requirements	Assess variation of the vehicle systems(test environment) to confirm evaluable scope

Realize Reproducible Evaluation

Study/evaluate results/issues/ causes

Study/evaluate results/issues/ causes

Evaluation Results

Assessment Criteria	【Reconnaissance Phase】 Attempt failed after fulfilling above set evaluator skills and workload, and confirmed security of the subject with sufficient reasons. 【Intrusion Phase】 Attempt failed after fulfilling above set evaluator skills and workload.(via all I/F)

FOT Results Reporting & Evaluation Guideline Finalization

FOT

Completed Information security Field Operational Test (penetration test) using the vehicle systems provided by 4 Japanese automakers

Outcome

Finalized "Information Security Evaluation Guideline" implementing necessary improvements through the results of FOT. * Confidential information of the participants are anonymized in the report

FOT Reporting Topics

1. Guideline validation through the FOT
2. Evaluation process establishment through FOT
3. Improvement of the guideline through the FOT
4. Improvement through the outcomes of FY17 project

FOT Reporting Topic 1: Guideline validation through the FOT

Manage and conduct FOT using the Guideline. Verify as well as implement necessary improvements to the Guideline through the results.

*Details of the improvements implemented are explained later

Verification Activity

01 Participants

- *Validate evaluation method/the Guideline through the results of the FOT/reporting. (Questionnaire answered by the participants)*

02 Evaluator /Self-assessment (PwC)

- *Through evaluating multiple vehicle systems using the Guideline, confirm validity and practicality of its contents and implement necessary additions and updates.*

03 Related Stakeholders

- *Explain the project activity and the Guideline to related stakeholders in public/private sector. Analyze their feedback towards the Guideline utilization in the industry.*

FOT Reporting Topic 1: Participants Feedback Summary

Feedback from the participants were collected through the questionnaire . Summary of the questionnaire replies is as follows*.

Questionnaire Item	Feedback Summary
Evaluation method establishment (The Guideline)	• Methods contribute to securing a certain level of security quality • Methods contribute to homogenizing penetration testing, which is generally dependent on individual skills
FOT using actual vehicle systems	• FOT contributes to verification of the Guideline • Verification using multiple vehicle systems is good.
Future expectations	• Quality of the advisory regarding countermeasures against the issues found in the evaluation is still dependent on the evaluators' individual skills, which leaves some room for improvement. • Look forward for a guideline that can also be used in the earlier stages of the product development, such as design phase.

 * The summary only reflects the feedback that were agreed to be disclosed by the participants at the time of creating this document.

FOT Reporting Topic 1: Evaluator/Self-assessment (PwC)

Following shows the summary of the self-assessment results on the FOT conducted by PwC.

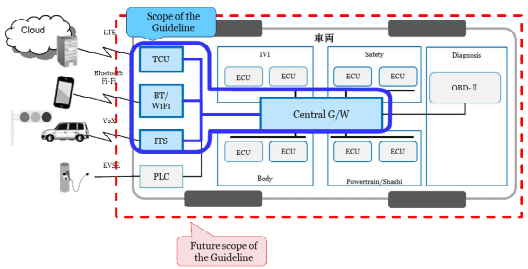
Assessment Item	Results Overview
Evaluation Process	• Evaluation process was organized through discussion with the stakeholders before the start of FOT • Evaluation process contributed to the uniformity of the evaluation work.
Evaluator Skill	• Definition of the evaluator skills contributed to the uniformity of the evaluation work • Based on the tendency observed during the FOT, reconfirmed that resources with adequate HW security evaluation are scarce.
Evaluation Period	• Complete all evaluation based on the Guideline within preset period of 2 months. • As success rate of intrusion using unknown vulnerabilities are trade off with elapsed time, it may be necessary to consider setting evaluation duration based on reconnaissance results.
Evaluation Items	• FOT conducted based on the Guideline draft developed in FY17 project. • Evaluation items were added to the Guideline as identified necessary through the FOT.
Subject System	• The vehicle systems provided for the FOT had different system architectures, which resulted in variation in applicable evaluation items • Established evaluation process considering such differences, and listed required system components.

FOT Reporting Topic 2：Evaluation process establishment through FOT

A standard process for vehicle system security evaluation (penetration test) was established as method applicable as an assessment.

Security Evaluation(Penetration test) Process

1. Evaluation Scope Definition
2. Evaluation Condition Definition
3. Evaluation Item Definition
4. Evaluation



Reconnaissance Skill

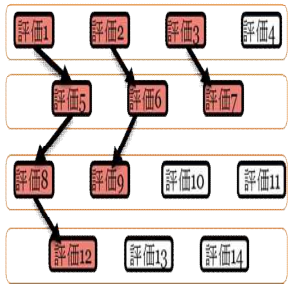
Category	Skill
Hardware analysis	Surficial analysis
	Processing
	Binary extraction from data input/output port
	Binary extraction from debug port
Binary analysis	File system analysis
	Software architecture analysis
	Binary code analysis
	Source code analysis
	Bypass safeguard
Network analysis	WiFi communication analysis
	BlueTooth / BlueTooth LE communication analysis
	Cellular communication analysis
	TCP/IP communication analysis
Management	Information transfer

1. Reconnaissance
2. Intrusion
3. Escalation of Privilege
4. Actions on Objectives

Intrusion Skills

Category	Skill
Intrusion	Threat Analysis
	Binary code analysis
	Identify/penetrate vulnerability
Escalation of privilege	Bypass security technique
	Bypass safety mechanism
	Bypass mandatory access control mechanism
	Bypass falsification detection mechanism
Actions on Objectives	Embedded network analysis
	CAN communication analysis
	Attack Demonstration/ Reproduction

Penetration Test Approach(image)

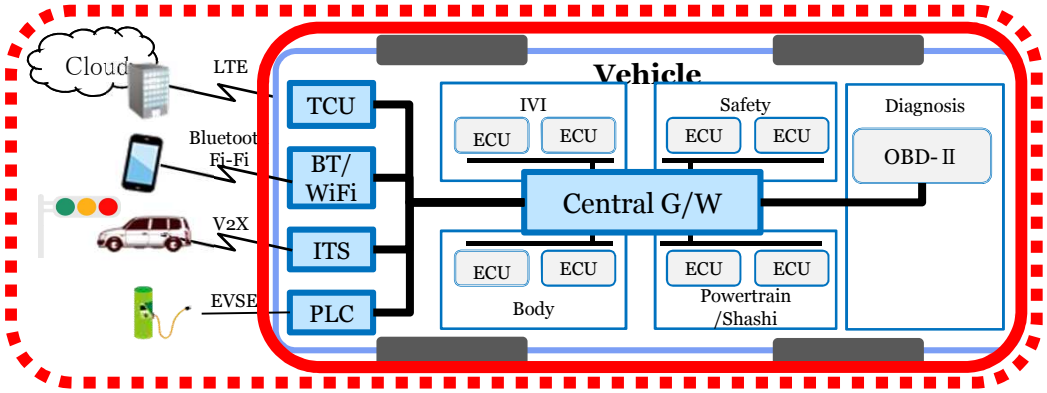


Evaluation Scope Definition : Definition Based on Risk analysis

Vehicle System Security Evaluation (Penetration Test) Procedure 1:
Conduct a risk analysis on the subject system as well as its surround systems to identify high risk interface, components to be define as the scope of the evaluation.

Likelihood × Impact = Component Risk

Likelihood		Impact	Component Risk	
Threat Agent Factors	Vulnerability Factor	Impact Factor	Likelihood and Impact Levels	
➢ Skill Level	➢ Ease of discovery	➢ Loss of confidentiality	0 to <3	LOW
➢ Motive	➢ Ease of exploit	➢ Loss of integrity	3 to <6	MEDIUM
➢ Opportunity	➢ Awareness	➢ Loss of availability	6 to 9	HIGH
➢ Size	➢ Intrusion detection	➢ Loss of accountability		



Evaluation Condition Definition: Clarify conditions regarding the evaluations

Vehicle System Security Evaluation (Penetration Test) Procedure 2:
To ensure reproductively of the evaluation, clarify and define conditions, criteria regarding the evaluation.

※Following are the criteria as explained in P20

Evaluation Condition	Condition Details
Evaluator Skill	• Identify necessary skills to be checked/rated by the managers in prior to the evaluation work.
Evaluation Workload	• The FOT sets standard period of 2 months(40 working days) x 2 evaluators
Environment (Vehicle system)	• Confirm subject system considering the items actually prepared

Evaluation Result

Assessment Criteria	【Reconnaissance Phase】 Attempt failed after fulfilling above set evaluator skills and workload, and confirmed security of the subject with sufficient reasons. 【Intrusion Phase】 Attempt failed after fulfilling above set evaluator skills and workload.(via all I/F)

Overview of "Evaluator Skill" by phase (1/2)

Reconnaissance Skill

Category	Skill	Skill explanation
Hardware analysis	Surficial analysis	Analyze PCB structure based on hardware knowledge to identify debug port and/or external communication port
	Processing	Process necessary work on the PCB including desoldering, resoldering of the flash memory from the PCB etc.
	Binary extraction from data input/output port	Extract data from the flash memory/external communication port
	Binary extraction from debug port	Extract data from the debug port identified
Binary analysis	File system analysis	Analyze and understand data structure of the file systems etc. from the data extracted from the flash memory
	Software architecture analysis	Analyze files extracted from the file system and analyze, understand software architecture including OS, library etc.
	Binary code analysis	Analyze and understand design and implementation of the program files etc. identified
	Source code analysis	Analyze and understand design and implementation at source code level through decompiling the binary codes using various tools
	Bypass safeguard	Analyze and bypass safeguard implemented in the software such as data encryption/obfuscation/encoding
Network analysis	WiFi communication analysis	Intercept and analyze WiFi communication
	BlueTooth / BlueTooth LE communication analysis	Intercept and analyze BlueTooth・BlueTooth LE communication
	Cellular communication analysis	Intercept and analyze cellular communication
	TCP/IP communication analysis	Intercept and analyze TCP/IP communication
Management	Information transfer	Manage information obtained and pass on to next phase of the evaluation

Overview of "Evaluator Skill" by phase (2/2)

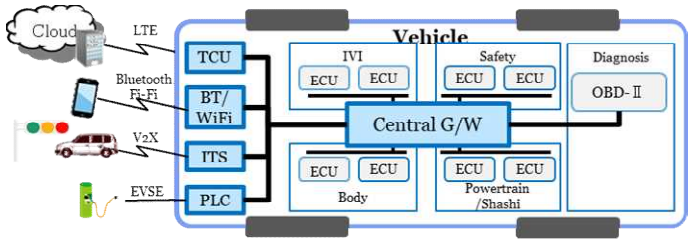
Intrusion Skills

Category	Skill	Skill explanation
Intrusion	Threat Analysis	Analyze and identify an attack surface for the intrusion based on the results on reconnaissance phase
	Binary code analysis	Analyze and understand design and implementation of the program files etc. which can be an attack surface based on threat analysis
	Identify/penetrate vulnerability	Identify vulnerability, produce attack code etc. based on or along with binary code analysis to succeed intrusion
Escalation of privilege	Bypass security technique	Analyze and bypass vulnerability mitigation technique such as data execution prevention, address space randomization
	Bypass safety mechanism	Analyze and bypass product specific safeguard (performance restriction etc.)
	Bypass mandatory access control mechanism	Analyze and bypass mandatory access control mechanism such as SELinux
	Bypass falsification detection mechanism	Analyze and bypass falsification detection, integrity verification mechanism such as secure boot
Actions on Objectives	Embedded network analysis	Analyze and understand embedded network structure (central gateway and each ECUs etc.)
	CAN communication analysis	Intercept, analyze, resend CAN communication based on network analysis results
	Attack Demonstration/ Reproduction	Demonstrate, reproduce attack using the vulnerabilities based on the result of all evaluation phases

Evaluation Item Definition: Decide evaluation items based on defined conditions

Vehicle System Security Evaluation (Penetration Test) Procedure 3:
Based on risk analysis results and defined conditions, identify evaluation items, to be applied as well as the order to perform them.

Evaluation Scope



Evaluation Conditions

- Environment (vehicle system)
- Evaluation Equipment
- Evaluator Skill
- Evaluation Period
- Assessment Criteria

Evaluation Items

1. Reconnaissance
   - 1.1 HW research
   - 1.2 SW research
2. Intrusion
   - 2.1 Passive attack with user intervention
   - 2.2 Passive attack without user intervention
   - 2.3 Active attack targeting vulnerabilities
   - 2.4 Active attack using information obtained through interception
3. Escalation of Privilege
   - 3.1 Remove protection
   - 3.2 Obtain higher privilege
4. Actions on Objectives
   - 4.1 Information breach
   - 4.2 Service interruption
   - 4.3 Unauthorized control (Control Systems)
   - 4.4 Unauthorized control (Other Systems)

Conduct Evaluation: Procedure and reporting

Vehicle System Security Evaluation (Penetration Test) Procedure 4:
Conduct evaluation based on defined evaluation items. Define operation and items to be reported as the result of the evaluation considering characteristics of the penetration test.

Evaluation(Penetration Test) Operational Flow

Preparation

- Prepare necessary security testing tools based on evaluation subject and evaluation items.
- Establish evaluation team. Identify individual members and their skills.

Evaluation

- Identify team roles and conduct evaluation

【Roles】

✓ Evaluation Leader
Plan and decide strategy for penetration based on evaluation progress.

✓ Evaluator
Perform actual evaluation work

Reporting

- Report following items

✓ Every work performed during the evaluation (including failed attempts)
✓ Procedures, tools and programs used for evaluation (To enable reproduction)
✓ Advisory on the necessary countermeasures against identified issues.

FOT Reporting Topic 3: Improvements in the guideline through the FOT

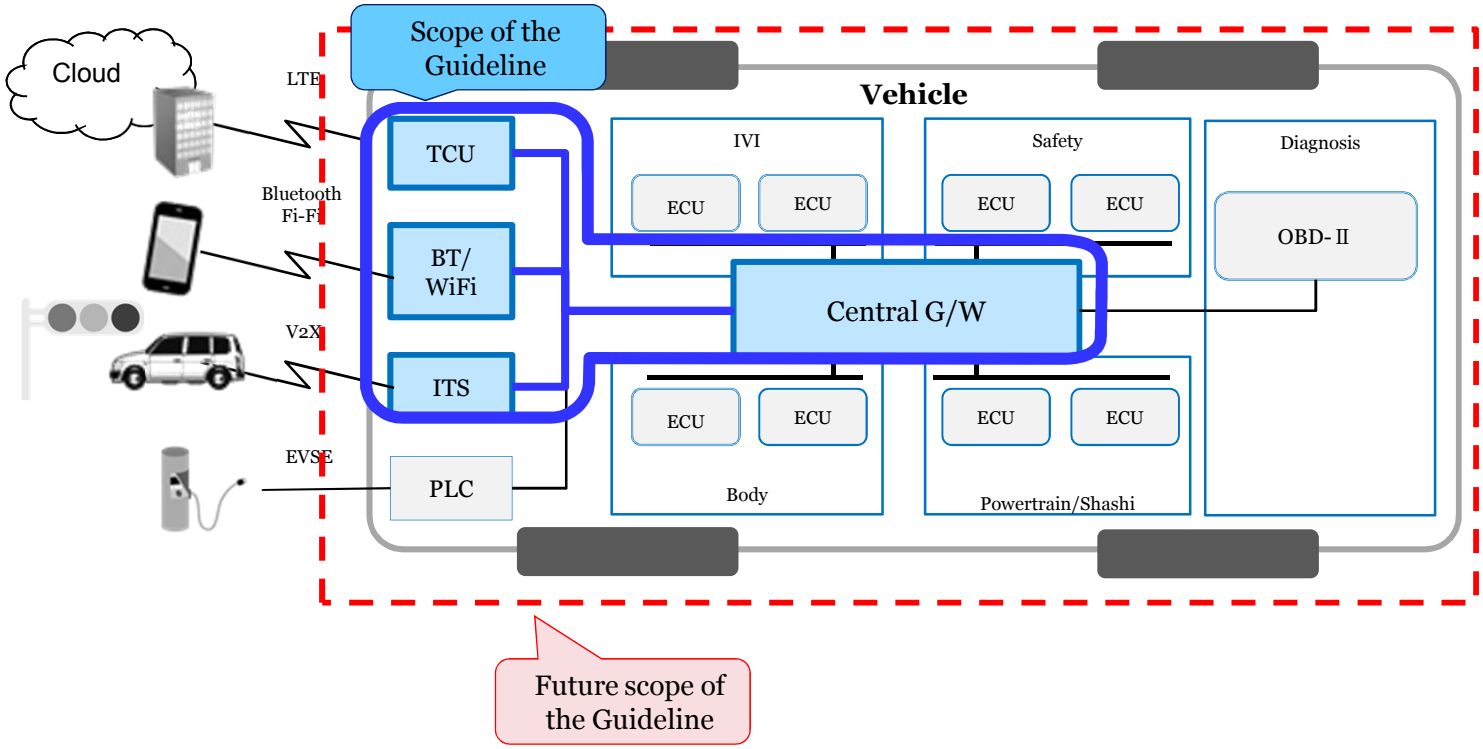
Following 19 items* were improved through the FOT

Item No	Change detail	Reason
1.1.1 I/F research before device extraction	Item updated「1.1.1.1 Check USB port connection」	Reviewed by the evaluator based on FOT results
	Item added「1.1.1.4 Check SD card」	Reviewed by the evaluator based on FOT results
1.1.3 I/F research after chip removal	Contents updated「1.1.3.2 Flash memory chip research」	Updated by the evaluator
1.1.5 Interface connection	Contents updated「1.1.5.5 Obtain console by binary falsification」	Updated by the evaluator
1.1.6 Binary extraction	Contents updated「1.1.6.1 Binary extraction from UART(OS active state)」	Updated by the evaluator
	Contents updated「1.1.6.3 Binary extraction from UART(BootLoader active state)」	Updated by the evaluator
	Contents updated「1.1.6.5　Binary extraction from flash memory」	Updated by the evaluator
1.1.7 Confirm binary safeguard	Item added「1.1.7.8 Obfuscation research」	Reflected FOT feedback
1.1.8 Reverse engineering	Item added「1.1.8.2 Target selection」	Reflected FOT feedback
1.2.6 TCU communication interception	Item updated「1.2.6.1 Modem research」	Reviewed by the evaluator based on FOT results
	Item added「1.2.6.2 TCU－IVI communication interception」	Reviewed by the evaluator based on FOT results
1.2.8 CAN message communication interception	Method updated「1.2.8.1 CAN message capturing tool setup」	Updated by the evaluator
2.3.4 Attack via WiFi(in-vehicle)	Method updated「2.3.4.1 Login from public port」	Updated by the evaluator
	Method updated「2.3.4.3 Analyze API source code」	Updated by the evaluator
3.1.2 Bypass DAC	Method updated「3.1.2.2 Bypass DAC confirmation」	Reviewed by the evaluator based on FOT results
3.1.3 Bypass safeguard	Added as Mid-level item	Reviewed by the evaluator based on FOT results
3.2.1 Bypass escalation of privilege prevention	Method updated「3.2.1.1 Check escalation of privilege prevention function」	Reviewed by the evaluator based on FOT results
	Method updated「3.2.2.2 Bypass mandatory access control」	Reviewed by the evaluator based on FOT results
3.3.1 Bypass SecureBoot	Added as Mid-level item	Reviewed by the evaluator based on FOT results

 * Minor adjustments were also applied to several items other than the above mentioned.

FOT Reporting Topic 4: Improvements through other outcomes from FY17

Outcome of FY17 project from other parties were referenced and reviewed to efficiently improve the Guideline.
Considering future expansion in the scope of vehicle security evaluation, implemented risk analysis as method to define priorities in the evaluation scope which would benefit the penetration tests which needs to be performed within a particular timeframe. (cf. P30)



Structure for Guideline standardization/update

With completion of SIP-adus(Ph1), discussions are ongoing towards future management as well as wider usage of the Guideline in the industry, after transferring the Guideline rights to JasPar, an organization responsible for technology standards related to vehicle security .