SIP

戦略的イノベーション創造プログラム

「The second phase of SIP- Automated Driving for Universal Services/ Research on New Cyber-attacks and Countermeasures Against New Cyber-Attacks」

FY2021 Interim Report
Summary version

PwC Consulting LLC

2022 Mar.

Project Background and Objectives

New cyber-attacks against vehicles have been continuously reported at BlackHat and other international conferences. The intrusion detection system (hereinafter referred to as "IDS") is regarded as an effective countermeasure against such cyber-attacks.

In FY2019, a research was conducted on technological trend and basic assessment of vehicle IDS to confirm its necessity and effectiveness in countering new cyber-attacks. Moreover, it was confirmed that there is a need for a comprehensive method to evaluate the detection performance as well as the implementation and operation of IDS.

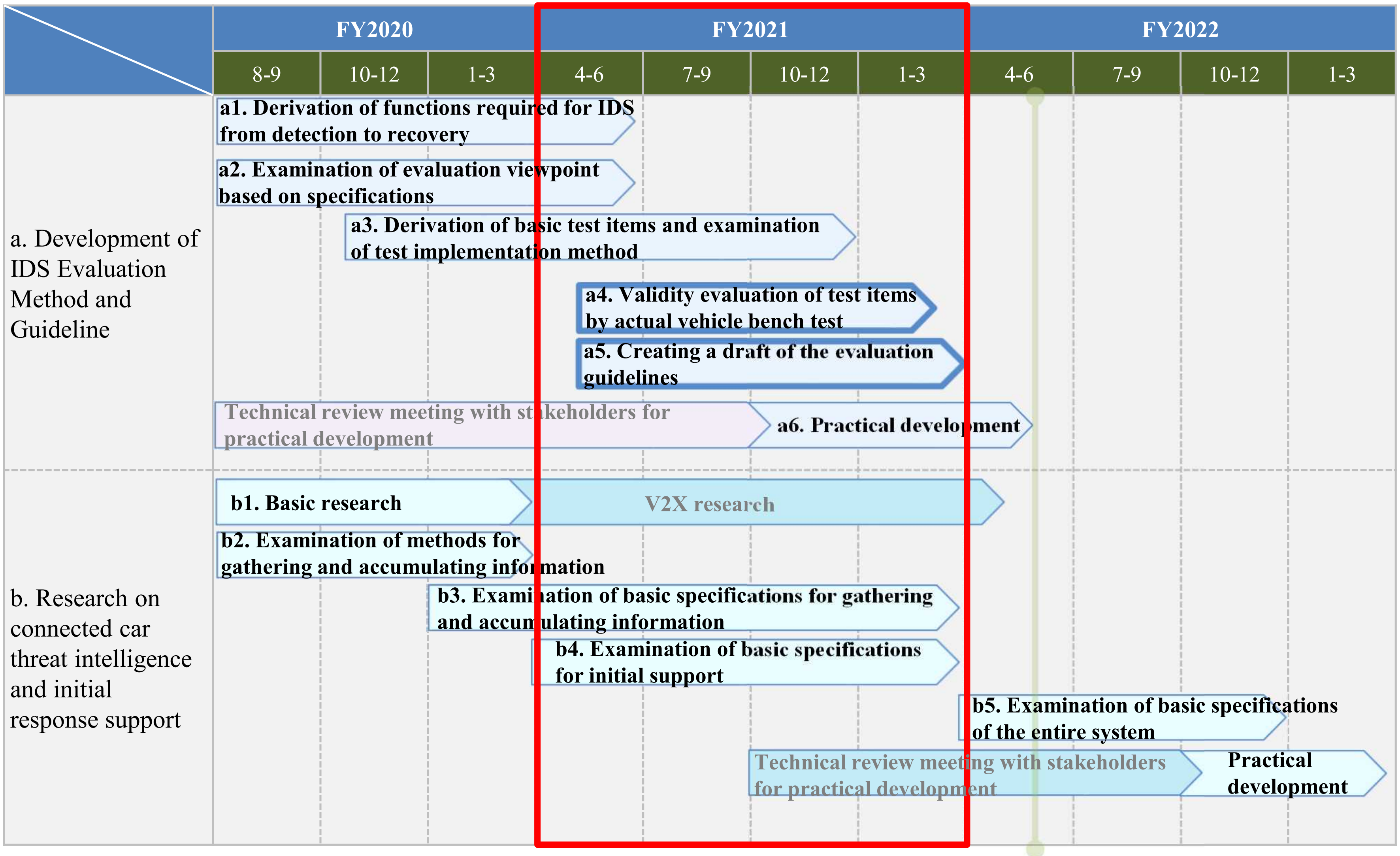
From FY2020 onwards, following researches are conducted;
a. Development of IDS evaluation method and guideline
b. Research on connected car threat intelligence and initial response support

Research Objectives and Activities Overview (a, b)

#	Objectives overview set by SIP	Project objectives
a	**“Development of IDS Evaluation Method and Guideline"** Summarize evaluation items, methods, procedures, and environments for in-vehicle IDS evaluation methods, examine evaluation criteria and document as a guideline. Transfer the guideline to related industry groups to relate to the practical development and operation of these guidelines to the automotive industry.	• The final goal is to transfer the IDS evaluation method guideline to industry groups at the end of FY2021. • By the end of 2021, component investigations of basic functions of various IDSs and experiments using test beds and actual vehicles, or actual vehicles benches will be conducted, and the outcomes will be used as inputs to the document. • In FY2020, the information such as latest cyber-attack cases which are necessary for the experiment will be collected and the contents of the experiment will be studied to create the outline of the guide. • Based on the activities of FY2019, hearings and coordination with industry stakeholders will be conducted as appropriate, enabling practical development and smooth transfer of operations to industry organizations.
b	**"Research on connected car threat intelligence and initial response support"** Consider the method of collecting and accumulating threat intelligence, conduct demonstration tests of attack monitoring using honeypots, develop basic specifications of systems for initial response support, and transfer to relevant industry groups to support collaborative development in the automotive industry.	• The ultimate goal is to transfer the operation of the basic system specifications to provide initial support for incident response to industry groups in 2023. • In initial support for incident response, assuming that sharing of threat information within the industry through the "Information Sharing System" is useful, the basic specifications for collecting and accumulating threat information and initial support using them will be formulated by the end of fiscal 2021. • The basic specifications of the entire system are examined when these elements are operated as a system.

Overall Schedule

Overall schedule of the project is as follows.



FY2020 | FY2021 | FY2022

8-9 | 10-12 | 1-3 | 4-6 | 7-9 | 10-12 | 1-3 | 4-6 | 7-9 | 10-12 | 1-3

a. Development of IDS Evaluation Method and Guideline

a1. Derivation of functions required for IDS from detection to recovery

a2. Examination of evaluation viewpoint based on specifications

a3. Derivation of basic test items and examination of test implementation method

a4. Validity evaluation of test items by actual vehicle bench test

a5. Creating a draft of the evaluation guidelines

Technical review meeting with stakeholders for practical development

a6. Practical development

b. Research on connected car threat intelligence and initial response support

b1. Basic research

V2X research

b2. Examination of methods for gathering and accumulating information

b3. Examination of basic specifications for gathering and accumulating information

b4. Examination of basic specifications for initial support

b5. Examination of basic specifications of the entire system

Technical review meeting with stakeholders for practical development

Practical development

This report describes the activities that were carried out in FY2021 (the red frame period in the above figure).
Changes may occur depending on future coordination with industry groups. For the final content, please see the final report for the next year.

a. Development of IDS Evaluation Method and Guideline

Research Objectives (Repeat)

The guideline for the evaluation method of in-vehicle IDS, including judgment criteria, will be formulated, and operation will be transferred to the industry organizations in 2022.

#	Objectives overview set by SIP	Project objectives
a	**“Development of IDS Evaluation Method and Guideline"** Summarize evaluation items, methods, procedures, and environments for in-vehicle IDS evaluation methods, examine evaluation criteria and document as a guideline. Transfer the guideline to related industry groups to relate to the practical development and operation of these guidelines to the automotive industry.	• The final goal is to transfer the IDS evaluation method guideline to industry groups at the end of FY2021. • By the end of 2021, component investigations of basic functions of various IDSs and experiments using test beds and actual vehicles, or actual vehicles benches will be conducted, and the outcomes will be used as inputs to the document. • In FY2020, the information such as latest cyber-attack cases which are necessary for the experiment will be collected and the contents of the experiment will be studied to create the outline of the guide. • Based on the activities of FY2019, hearings and coordination with industry stakeholders will be conducted as appropriate, enabling practical development and smooth transfer of operations to industry organizations.

Purpose of the IDS evaluation guideline

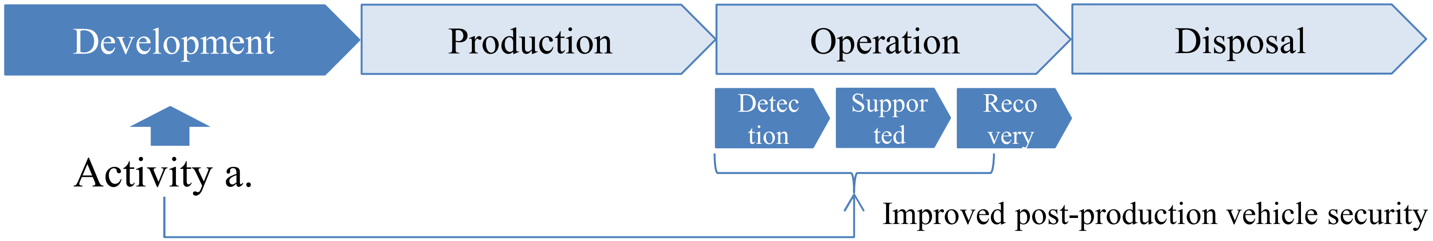
Conduct research on evaluation method for on-board IDS and develop IDS evaluation guideline which can be used during product development to contributes to the entire automotive industry in improving after production vehicle security.

Background related to post-production cybersecurity

Regulations	Industry Practices
WP29 UN-R155 sets requirements for the manufacturers to enable the vehicles to detect and respond to cyber-attacks.	Each manufacturer should specify the scope of attack to be detected as there are no existing regulations nor guidelines in this regard.

Activity a. Objectives and directions

Research IDS evaluation method for “Cyber-attack detection and vehicle recovery” and document as a “IDS evaluation guideline” to contribute to the improved cybersecurity for <u>automotive industry</u>.



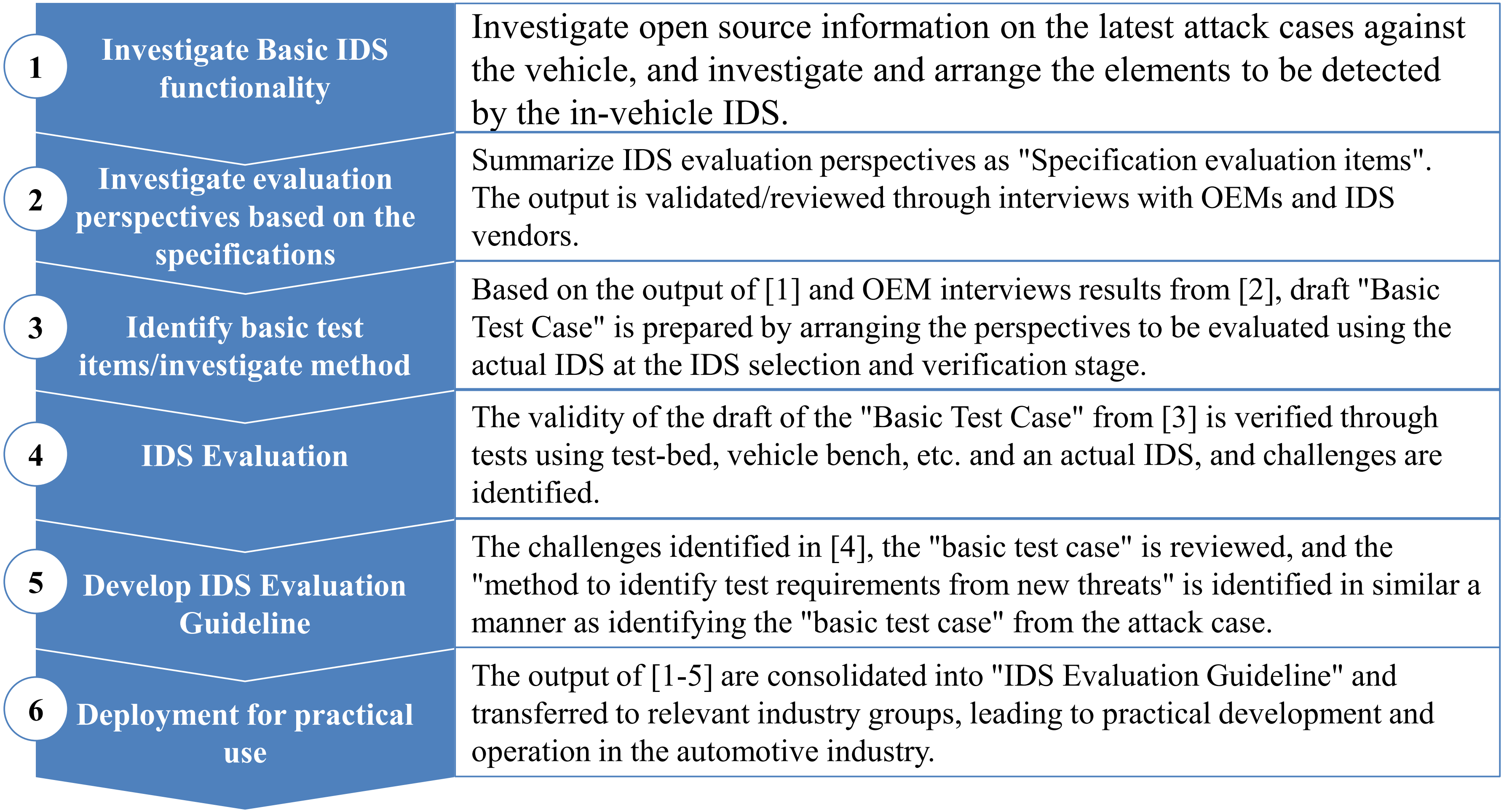
Activity Policy: Scope of the IDS evaluation guidelines

As a precondition, the content of the Guideline is a requirement and assessment perspective to be considered by OEMs/ suppliers, and does not imply that the requirements listed in the Guideline must be met, and that testing must be done in the way of the Guideline.

Policy 1	Evaluate the outline at a level of detail that is comprehensive and comparable to IDS
Policy 2	Evaluate whether or not a hypothetical attack equivalent to that of a past attack can be detected and analyzed
Policy 3	Perform IDS actual machine tests in a test environment that can be easily prepared

Activity Policy: IDS Evaluation Guideline Development

Following approach will be taken to develop IDS evaluation guidelines and transfer to the industry groups.



1	**Investigate Basic IDS functionality**	Investigate open source information on the latest attack cases against the vehicle, and investigate and arrange the elements to be detected by the in-vehicle IDS.
2	**Investigate evaluation perspectives based on the specifications**	Summarize IDS evaluation perspectives as "Specification evaluation items". The output is validated/reviewed through interviews with OEMs and IDS vendors.
3	**Identify basic test items/investigate method**	Based on the output of [1] and OEM interviews results from [2], draft "Basic Test Case" is prepared by arranging the perspectives to be evaluated using the actual IDS at the IDS selection and verification stage.
4	**IDS Evaluation**	The validity of the draft of the "Basic Test Case" from [3] is verified through tests using test-bed, vehicle bench, etc. and an actual IDS, and challenges are identified.
5	**Develop IDS Evaluation Guideline**	The challenges identified in [4], the "basic test case" is reviewed, and the "method to identify test requirements from new threats" is identified in similar a manner as identifying the "basic test case" from the attack case.
6	**Deployment for practical use**	The output of [1-5] are consolidated into "IDS Evaluation Guideline" and transferred to relevant industry groups, leading to practical development and operation in the automotive industry.

Activity a. Approach (1/3)

Develop drafts of "Specification evaluation items" and "Basic test cases" based on attack information and papers on past cars, public information survey on IDS products, etc. and conduct interviews with OEMs and IDS vendors, and conduct IDS actual machine surveys to verify the validity.

1

Identify basic test items/investigate test method

Investigate open source information on the latest attack cases against the vehicle, and investigate and arrange the elements to be detected by the in-vehicle IDS.

INPUT

- Web attack information, papers
- Results of FY2019 Attack Scenario Survey and Analysis

OUTPUT

- Detection function required by IDS (security event)

2

Investigate evaluation perspectives based on the specifications

Summarize IDS evaluation perspectives as "Specification evaluation items". The output is validated/reviewed through interviews with OEMs and IDS vendors

INTPUT

- Detection function required by IDS (security event)
- Disclosure of IDS information (including results in fiscal 2019)
- OEM, IDS vendor interview

OUTPUT

- List of Specification Evaluation Items

Activity a Approach (2/3)

Develop drafts of "Specification evaluation items" and "Basic test cases" based on attack information and papers on past cars, public information survey on IDS products, etc. and conduct interviews with OEMs and IDS vendors, and conduct IDS actual machine surveys to verify the validity.

3 Identify basic test items/investigate test method

Based on the output of [1] and OEM interviews results from [2], draft "Basic Test Case" is prepared by arranging the perspectives to be evaluated using the actual IDS at the IDS selection and verification stage.

INPUT

- Papers and guidelines (NIST SP800-94, etc.)
- Detection function required by IDS (security event)

OUTPUT

- Basic Test Case (Draft)
- Outcomes of examining the test environment

4 IDS Evaluation

The validity of the draft of the "Basic Test Case" from [3] is verified through tests using test-bed, vehicle bench, etc. and an actual IDS, and challenges are identified.

INTPUT

- Basic Test Case (Draft)

OUTPUT

- Basic test case

Activity a Approach (3/3)

Develop drafts of "Specification evaluation items" and "Basic test cases" based on attack information and papers on past cars, public information survey on IDS products, etc. and conduct interviews with OEMs and IDS vendors, and conduct IDS actual machine surveys to verify the validity.

5

Develop IDS Evaluation Guideline

The challenges identified in [4], the "basic test case" is reviewed, and the "method to identify test requirements from new threats" is identified in similar a manner as identifying the "basic test case" from the attack case.

INPUT

- Basic test cases (including derivation methods)
- Specification evaluation items

OUTPUT

- IDS evaluation guideline (draft)

6

Deployment for practical use

The output of [1-5] are consolidated into "IDS Evaluation Guideline" and transferred to relevant industry groups, leading to practical development and operation in the automotive industry.

INTPUT

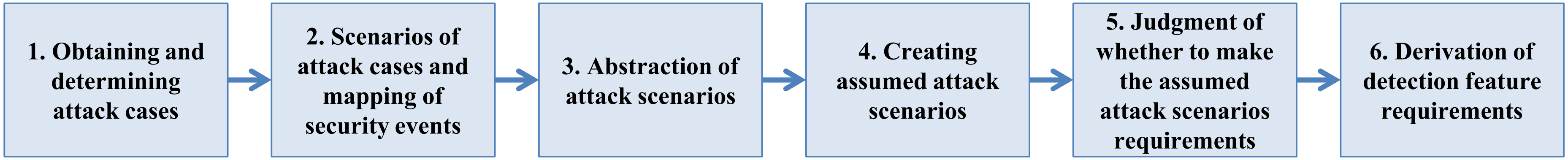
- IDS evaluation guideline (draft)

OUTPUT

- IDS evaluation guideline (First issue)

Criteria method of detect function

The method to derive the detection criterion from a certain past case was examined on 「policy 2: Evaluate whether or not a hypothetical attack equivalent to that of a priors attack can be detected and analyzed」 shown in the activity policy.



1. Obtaining and determining attack cases → **2. Scenarios of attack cases and mapping of security events** → **3. Abstraction of attack scenarios** → **4. Creating assumed attack scenarios** → **5. Judgment of whether to make the assumed attack scenarios requirements** → **6. Derivation of detection feature requirements**

#	Overview
1	Select attack cases to be detected by obtaining attack cases.
2	Attack cases are decomposed into attack procedures for each vehicle component, requirements and objectives for establishing attacks are added, attack scenarios are created, and security events that may occur in each attack procedure are mapped.
3	Abstract attack scenarios to derive attack scenarios that are "equivalent" to attack cases.
4	Taking into account the specifications of IDS-equipped vehicles and the possibility of vulnerability, the abstraction attack scenario will be implemented in IDS-equipped vehicles, and the attack scenario that may be established in IDS-equipped vehicles will be created.
5	Consider specific actions according to the risk assessment methods and response methods defined by OEM/ supplier for the assumption attack scenario.
6	Of the security events that may occur in the in-vehicle network due to an attack, those that should be detected by IDS are selected and derived as a requirement.

Research on fundamental IDS functions (1/3)

The security conference web information and vulnerability information held by 2020 were examined, and 12 cases directly related to the vehicle were analyzed, and the security event was derived.

	Cases	Cases analyzed in detail
Web information and vulnerability information	1329	6
Research Paper	1062	6
Total	**2391**	**12**

Scope	Event	Security Event Examples
Network	Behavior of context conflicts on in-vehicle NWs	Sending control messages that do not affect basic operation at timings inconsistent with the running state, and sending valid diagnostic messages at timings inconsistent with the running state
	Attacks on the UDS protocol	Attacks on the UDS protocol
	Physical connection of fraudulent devices to the on-board NW	Connecting External Devices to OBD I/F
	Fuzzing attacks on in-vehicle NWs	Fuzzing attacks from OBD I/F
Host	Fraudulent behavior	Invoking a system call library from an unspecified process
	Illegal external communication	Communication with a source/destination outside the car that is not permitted
	Invalid file system operation	Changing Attributes of Important Files (Permissions, etc.)
	Fraudulent app installation	Installation of regulation apps
	Invalid log	Invalid system logs, application logs
	Unspecified frequency of errors	Request Processing Errors to External Public Services More Than a Certain Number of Times per Hour
	High load	High CPU and memory load conditions
	Changing the Firmware	Changing the Firmware

Research on fundamental IDS functions (2/3)

The 12 cases covered are as follows.

Information source	Attack Case Overview
USENIX Security '20 Technical Sessions	In BT/WiFi where the authentication function is defective, OBD dongle was connected, and the message which disables the remote lock was injected into the in-vehicle network, and the vehicle could be stolen. [Haohuang Wen, 2020]
Blackhat USA 2015	In FCA Jeep Cherokee, the vehicle can be remotely accessed from any terminal on the NW of Sprint, the host (OMAP) of HU/TCU can be accessed by SSH to the exposed 6667, and the FW of the CAN controller (V850) can be rewritten, and any CAN message (steering, braking, etc.) can be transmitted through the SPI. [Dr. Charlie Miller, 2015]
Vulnerability information	The buffer overflow vulnerability of the BT module of the DCU (Display Control Unit) such as Toyota Lexus is used to automatically connect to an external WiFi AP, and the firmware of the CAN controller is tampered with to override the message filtering function, and diagnostic messages can be sent to the CAN bus by connecting WiFi to the vehicle from the outside. [Lab, 2020]
Blackhat USA 2019	A command can be sent to a service waiting on the TCP port through OBD I/F or USB I/F of the HU of the BMW, a CAN message can be sent to K-CAN using TOCTOU vulnerabilities, and an ECU can be reset or a seats can be moved back and forth through the UDS message. [Zhiqiang Cai, 2019]
Blackhat USA 2019	By inserting the update management file of the crafted navigation from USB I/F of HU of BMW, and utilizing the vulnerability of the process to analyze the update management file, it was possible to reset an ECU can be reset or a seats can be moved back and forth through the UDS message. [Zhiqiang Cai, 2019]
Blackhat USA 2019	A bogus base station was installed, and the response of BMW ConnectedDrive service was rewritten, and the attacker's web server was accessed, and an ECU can be reset or a seats can be moved back and forth through the UDS message by utilizing the vulnerability of the browser, etc. [Zhiqiang Cai, 2019]
Blackhat USA 2019	A bogus base station sent a NGTP (BMW Remote Service) message for ConnectedDrive over SMS, allowing for unauthorized use of functions for remote services (such as opening doors, horns, lights, etc.). [Zhiqiang Cai, 2019]
Blackhat USA 2019	With BMW's vehicle, MITM attacks for communication between false base stations and vehicles are performed, signatures for Provisioning data are tampered with, and the buffer overflow vulnerability of TCU is utilized to reset ECU and move seat back and forth through UDS messages. [Zhiqiang Cai, 2019]
Web information	In Viper's smart alarms, a vulnerability in the servers' APIs could impersonate legitimate users and track vehicles, or shut down engines. [PARTNERS, 2019]
Vulnerability information	In Daimler Mercedes-Benz Me App, after stealing access token used between the application and the server, it can impersonate the legitimate user, log in to the server, vehicle functions (such as locking/unlocking the door that can be used through the application) can be used. [NVD, CVE-2018-18071 Detail, 2018]
Vulnerability information	Since there were only 256 combinations for Security Access, the attacker could calculate the keys and bloat the airbags. [NVD, CVE-2017-14937 Detail, 2017]

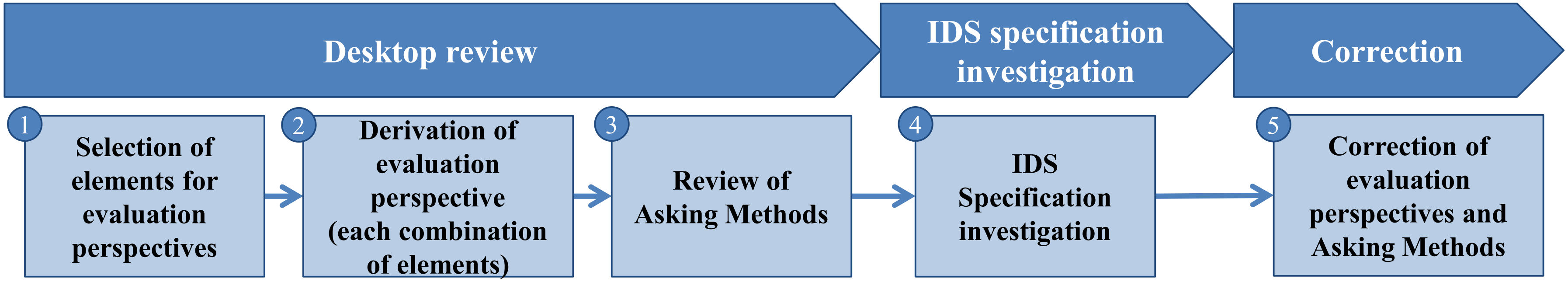
Research on fundamental IDS functions (3/3)

The IDS basic requirements derived from the analysis results of the cases are as follows.
※The specific basic requirements is stated only in the guidelines.

Major class	Small classification	ID
Detection Function	**No false positives**	SD-FP-1
		SD-FP-2
	Error in the data of a single message	SD-TP-1-1
		SD-TP-1-2
		SD-TP-1-3
	Transmission cycle error	SD-TP-2-1
		SD-TP-2-2
	Error in relation to previous/next message	SD-TP-3-1
		SD-TP-3-2
	Context error	SD-TP-4-1
		SD-TP-4-2
		SD-TP-4-3
		SD-TP-4-4
	Status error of in-vehicle NW	SD-TP-5-1
	Attacks on diagnostic protocols	SD-TP-6-1
		SD-TP-6-2
		SD-TP-6-3
		SD-TP-6-4
		SD-TP-6-5
		SD-TP-6-6
		SD-TP-6-7
		SD-TP-6-8
Logging Function		SL-1-1
		SL-1-2
		SL-1-3
Notification Function		SN-1-1

IDS Specification Evaluation Perspectives (1/9)

Based on "Policy 1: Evaluate the outline at a level of detail that is compprehensive and comparable to IDS“, a specification evaluation perspective was derived using the following flow.


Desktop review
IDS specification investigation
Correction
1
Selection of elements for evaluation perspectives
2
Derivation of evaluation perspective (each combination of elements)
3
Review of Asking Methods
4
IDS Specification investigation
5
Correction of evaluation perspectives and Asking Methods

#	Overview
1	The quality characteristics of ISO/IEC 25010 System/Software Product Quality Model, which organizes IDS's product life cycle and software quality, are selected as the perspective of evaluation.
2	Consideration an evaluation perspective on the characteristics referenced and used in each phase of the product lifecycle so that you can fully evaluate 1.
3	Create a list of questions to IDS vendors to assess whether the assessment perspective discussed in 2 is a degree of detail that can compare IDS.
4	Based on the created questions list, interviews with IDS vendors (Panasonic Corporation (Japan), ETAS Corporation (Germany), and Arilou Information Security Technologies (Israel)) are conducted to verify the validity of the specification evaluation perspectives and the content of the questions.
5	Finalization of the specification evaluation perspectives based on verification results, JASPAR, and feedback from OEMs who are assumption readers.

IDS Specification Evaluation Perspectives (2/9)

The questions to IDS vendors are as follows.

Security Function Classification	Function	Item
Basic Specifications	Form of provision	Form of offering a commercial version
		IDS provided for PoC
		Supported platforms (for SW provide)
		Product Type
	Protocol	Supported In-vehicle Network Protocols
		Supported Top CAN Protocols
		Supported Top Ethernet Protocols
	Other	Detection method
		Amount of used memory
		SOC linkage
		Communication function outside the car
Detection	Detection Settings	Necessity of DBC file
		Information required in addition to the DBC file
		Availability of setting tool
		Threshold specification parameter
	Detection	Security events to be detected
		How IDS vendors adjust detection parameters
Supported	Logging/Notification Setting Method	Logging/Notification Setting Method
	Logging	Steady-state logging items
		Logging items at detection
	Notification	Notification Items on Detection
	Detailed analysis	Availability of log analysis support tool
Recovery	Update	Update target (Physical port used)
		Update target (using OTA)

Question	Option
Select the security event to be detected.	Load condition error of in-vehicle network
	Connecting unknown external devices or sending messages
	Communication protocol error
	Operation outside the specifications of the vehicle (transmission cycle, data threshold)
	Operation that differs from the normal state of the vehicle defined in the rule (e.g., an error such as a threshold value for a change in the value)
	Operation impossible as a vehicle condition (door open during high-speed running, etc.)
	Operations that cannot be considered as the driving environment recognized by the sensor (left turn steering operation in the right curve, etc.)
	Deviation from rules for source and destination (IP, port-based)
	Others()

※ Abbreviation for Proof of Concept. Verification the feasibility of new ideas and concepts and the effects that can be obtained from them.

IDS Specification Evaluation Perspectives (3/9)

A consideration of the answers to the question list, for the three IDS vendors (six products), is as follows.

1. Security events

Since the results of the answers were generally same for each company, each company supports the basic detection function, and it is difficult to make a big difference in the nominal specifications, so it is not possible to make a comparative evaluation of each company based on this item alone. On the other hand, part of the functional specifications, such as the type of protocol supported and the detection function of external device connection, are vendor-specific.

2. Logging/notification method

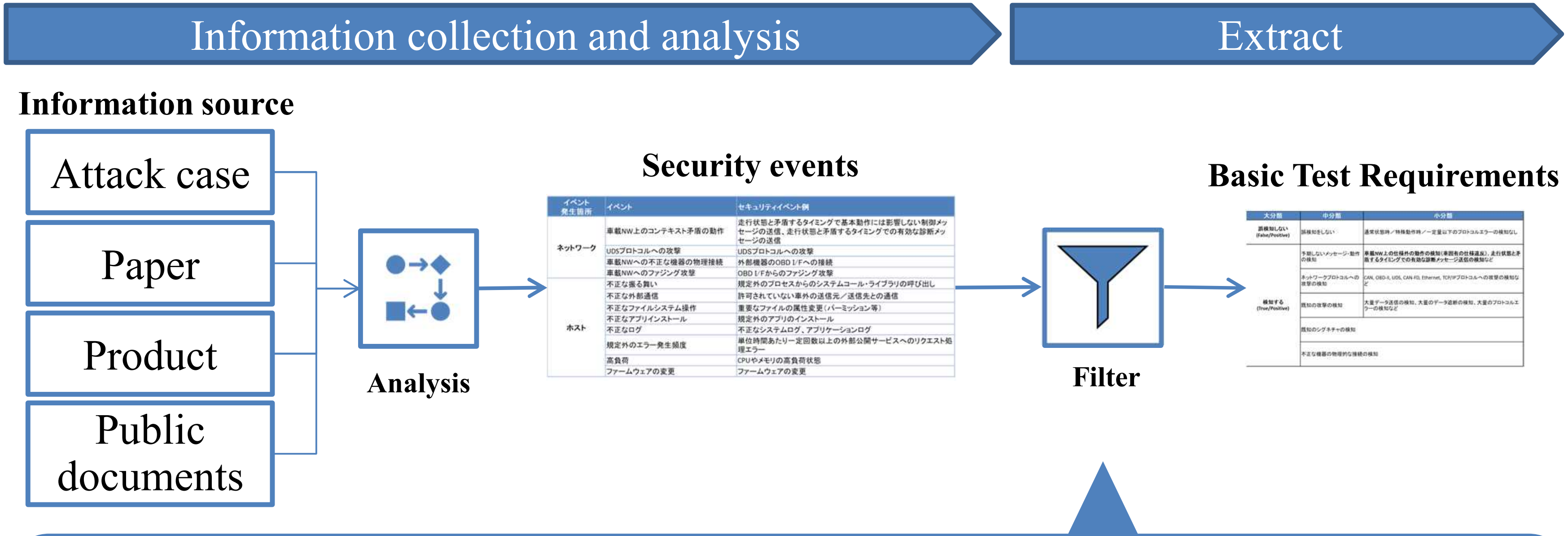
It is a prerequisite that each company is supported or can be customized, and basically customized based on OEM requirements. Therefore, by knowing the gap between the functionality required for IDS as OEM and the flexibility of the customization function, it is considered that the comparison of IDS is possible to some extent.

3. V-SOC operation services

As there are differences between vendors that exist as service menus and vendors that do not, this item is considered useful for comparison and examinations when analyzing IDS monitoring, analysis after detection, and support for response and recovery as needed are included.

Basic Test Case (4/9)

The Security events identified from the attack cases that meet certain conditions are defined as basic test requirements.



Security events

イベント発生箇所	イベント	セキュリティイベント例
ネットワーク	車載NW上のコンテキスト矛盾の動作	走行状態と矛盾するタイミングで基本動作には影響しない制御メッセージの送信、走行状態と矛盾するタイミングでの有効な診断メッセージの送信
	UDSプロトコルへの攻撃	UDSプロトコルへの攻撃
	車載NWへの不正な機器の物理接続	外部機器のOBD I/Fへの接続
	車載NWへのファジング攻撃	OBD I/Fからのファジング攻撃
ホスト	不正な振る舞い	規定外のプロセスからのシステムコール･ライブラリの呼び出し
	不正な外部通信	許可されていない車外の送信元／送信先との通信
	不正なファイルシステム操作	重要なファイルの属性変更（パーミッション等）
	不正なアプリインストール	規定外のアプリのインストール
	不正なログ	不正なシステムログ、アプリケーションログ
	規定外のエラー発生頻度	単位時間あたり一定回数以上の外部公開サービスへのリクエスト処理エラー
	高負荷	CPUやメモリの高負荷状態
	ファームウェアの変更	ファームウェアの変更

Basic Test Requirements

大分類	中分類	小分類
誤検知しない (False/Positive)	誤検知をしない	通常状態時／特殊動作時／一定量以下のプロトコルエラーの検知なし
検知する (True/Positive)	予期しないメッセージ・動作の検知	車載NW上の仕様外の動作の検知（車固有の仕様違反）、走行状態と矛盾するタイミングでの有効な診断メッセージ送信の検知など
	ネットワークプロトコルへの攻撃の検知	CAN, OBD-II, UDS, CAN-FD, Ethernet, TCP/IPプロトコルへの攻撃の検知など
	既知の攻撃の検知	大量データ送信の検知、大量のデータ途絶の検知、大量のプロトコルエラーの検知など
	既知のシグネチャの検知	
	不正な機器の物理的な接続の検知	

Filter conditions

1. Published in the past (2019-2021) ※1 , occurring in attacks against ※2 vehicle to which any IDS should respond, and/or;
2. It affects the basic operation (driving, steering, and braking) of the car.

※1. To take advantage of cases that have occurred in the past (see WP29 UN-R155 7 2.2.2 (f))

※2. Attacks that are considered applicable to other vehicles rather than attacks using vulnerabilities of special specifications of vehicles

Basic Test Case (5/9)

The basic test case summarizes the minimum points to be tested in the software unit test when IDS is selected or verified. The sections to be described are as follows.

Category	Item	Description
Test points	Test Case ID	Describe the ID
	Test Case Name	Describe the name of the test case
	Purpose	Describe the purpose of the test case
	SEv to be detected	Describe the SEv to be detected
	Type of attack msg to be injected	Type of attack msg injected for testing
	Prerequisites	Describe the running condition of the vehicle
	Derived Source Attack Case	Attack Case Derived from a Test Case
Test methods	Test environment	Describe either the simulation environment or the test bed environment.
	Prerequisite specifications of in-vehicle NW	Describe the specifications of vehicles equipped with IDS (vehicles equipped with IDS).
	Test Procedure	Describe the test procedure after building the test environment. Add sequential numbers (1., 2., and so on) to each viewpoint.
	Expected value	Describe the expected value of the test result <Hope Detection Test Case (SD-FT-*, SD-TP-*)> The guideline specifies that these information will be output to the IDS detection log. Number of detection: Number of detected Detection bus: bus detected by IDS as SEv (see next slide) Detection Type: Detection Type (see next slide) Reason for detection: Reason for detection (see next slide) Message to be detected
Remarks		Describe the precautions for implementation of the evaluation.

Basic Test Case (6/9)

The definitions of the expected values (detection bus, type, and reason) of the basic test case items listed on all slides are as follows.

Detection bus definition

Possible Values	Description
I	Information bus
C	Control bus
D	Diagnostic bus

Detection Type Definition

Detection Type	Description
Specific	Detect specific messages
Range	Detect specific time intervals

Detection reason definition

Reason for detection	Description
Incorrect ID	Invalid ID
Range	Range of incorrect data
Cycle	Illegal transmission cycle
Variation	Amount of change in incorrect data
Order	Fraudulent transmission order
Amount	Amount of fraudulent messages
Diag UDS	UDS protocol violation
Diag OBD	OBD protocol violation
Diag DoCAN	DoCAN protocol violation
Diag Err	Receiving error responses (including negative responses)

Basic Test Case (7/9)

An example of a fundamental test case is shown below.

Category	Item	Content
Test points	**Test Case ID**	SD-TP-1-2
	Test Case Name	Detecting the extent of illegal data by injecting the PT/chassis msg, body system msg
	Purpose	Verify that messages that violate a defined range of signal values are detected.
	SEv to be detected	Range of incorrect data
	Type of attack msg to be injected	PT/Chassis msg, Body System msg
	Prerequisites	Driving condition: Constant velocity driving
	Derived Source Attack Case	OBD2dongle/Wen(USENIX'20)-2 Jeep Cherokee(BH USA 2015)
Test methods	**Test environment**	Simulation environment
	Prerequisite specifications of in-vehicle NW	Vehicle speeds should not exceed between 0 km/h and 140 km/h.
	Test Procedure	1. The logging data of the control system bus of the actual vehicle is injected into the control system bus of CANoe from [Replay Block]. 2. A total of three messages of 141, 142, and 143 Km/h in <Vehicle Speed> are injected to CANoe control system bus at any timing, one message at a time from [i-Generator] (by pressing the key set at the injection timing). 3. Confirming that the log as expected is output in the IDS detection log.
	Expected value	Number of detection messages: 3 Detection bus: C Detection Type: Specific Reason for detection: Range Detection messages: {attack msg}
Remarks		

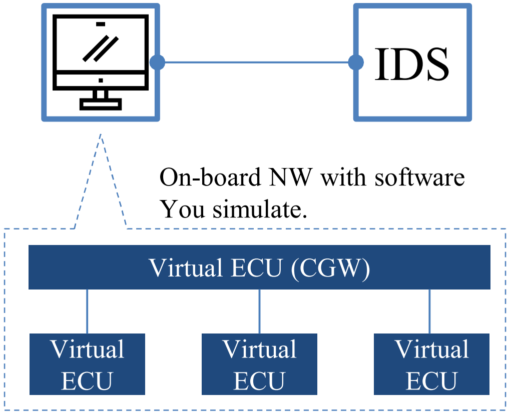
Basic Test Case (8/9)

Assumption test environments can be broadly divided into the following three categories. Among them, since the cost of the vehicle (bench) environment is larger than the simulation environment and the test bed environment in the test environment construction, this paper examines it on the assumption that it is carried out in either of the latter two.

Simulated environment

A test environment that does not use an actual ECU. The in-vehicle network is reproduced on the software.

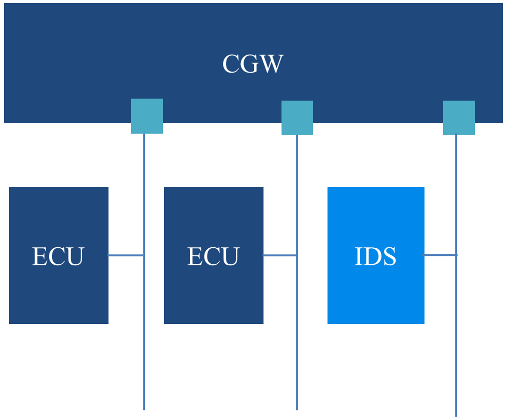
While simulating the on-board NW,
To meet testing requirements (attacks)
You enter a message in IDS.



On-board NW with software
You simulate.

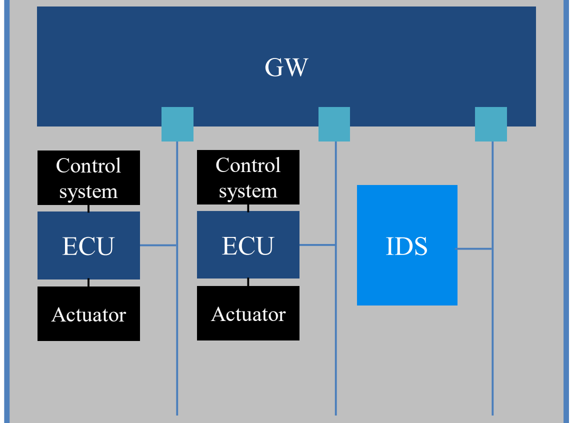
Test bed environment

An environment constructed with the minimum necessary hardware that meets the test requirements.



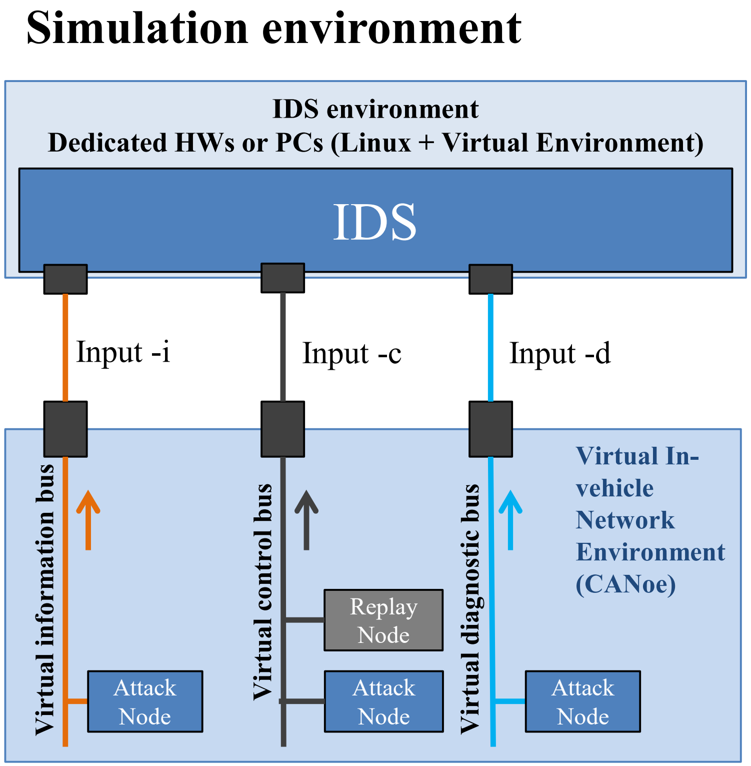
Vehicle (bench) environment

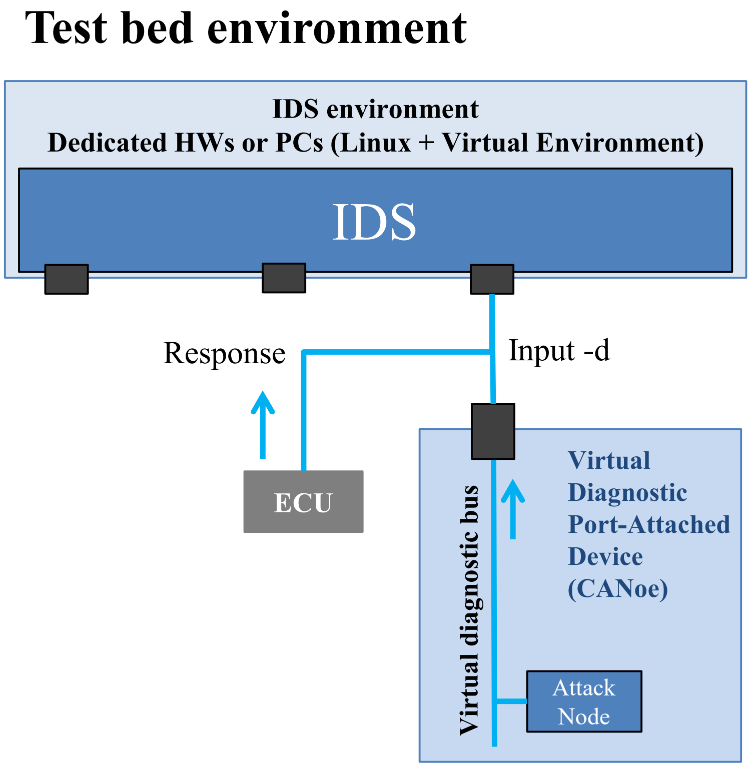
An environment in which an input device equivalent to an actual vehicle, an ECU, and an actuator are connected.



Basic Test Case (9/9)

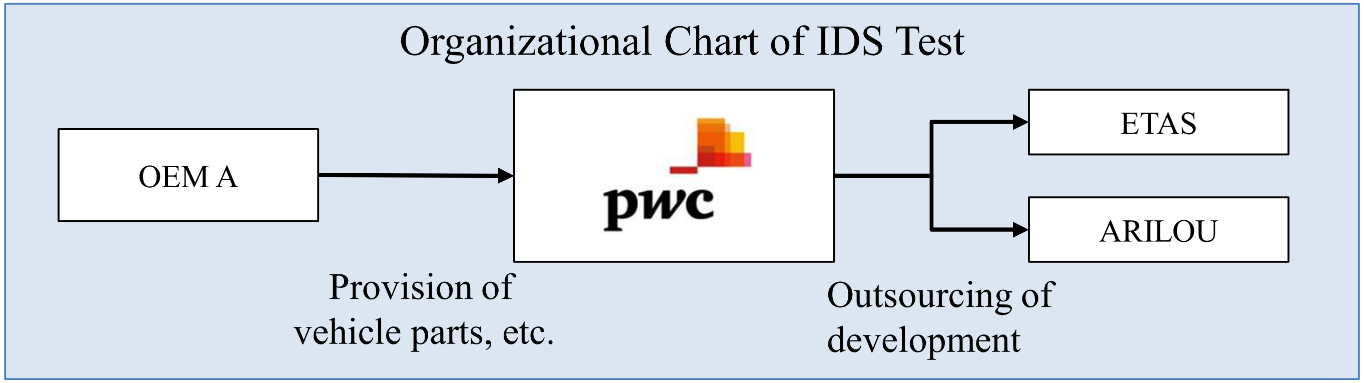
The basic configuration assuming the basic test case is as follows.




Test bed environment
IDS environment
Dedicated HWs or PCs (Linux + Virtual Environment)
IDS
Response
Input -d
ECU
Virtual diagnostic bus
Attack Node
Virtual Diagnostic Port-Attached Device (CANoe)

Verifying Test Cases with IDS Actual Machine Test (1/5)

The IDS actual machine test is not intended to evaluate IDS, but to verify the validity of the basic test case. The implementation system and contract form of the actual machine test are shown below.


Organizational Chart of IDS Test
OEM A
pwc
ETAS
ARILOU
Provision of vehicle parts, etc.
Outsourcing of development

#	Name of Contract	Main Sections to be Agreed	Contracting entity
1	Letter of intent of participation in IDS actual machine test	• Basic items: Function of IDS actual machine test, participants in implementation, mutual cooperation of PwC, etc. • Loan for Use of Equipment: Contract of a separate "Loan Agreement for Use of Movables" • Expiration date of the contract: Expiration date of the contract associated with the operation • Discontinuation of the test on the actual IDS unit: Terms under which the demonstration experiment will be discontinued • Ownership of Intellectual Property: Reservation of Intellectual Property Rights, etc. • Confidentiality: Definition, handling, scope of disclosure, etc. of the following information	OEM, IDS vendor, PwC
2	Lease Agreement for Use of Movable property	• Usage/Function: Purpose, description of use by provider, unavailability other than this activity • Delivery/Refund: Location of Delivery/Return, Installation Method, Due Date for Return, etc. • Cost sharing classification: Participant/PwC implementation classification, cost sharing classification • Items to be provided (list): Informations of the types of systems, parts, etc. to be provided for IDS actual machine tests, and the tasks to be supported in relation to the provision of quantities, etc.	OEM、PwC
3	Outsourcing agreement	• Contract Description: Developed Items, Technical Support • Cost: Outsourcing Cost • Delivery Date: Delivery Date, Acceptance Date, Due Date	PwC, IDS vendor

Verifying Test Cases with IDS Actual Machine Test (2/5)

The basic test case is a baseline from the evaluation point of view, and some of the test methods and expected values need to be adjusted according to the specifications of the target vehicle (ECU) and IDS. In the actual machine test, the test method and the required specifications for IDS were adjusted based on the specifications of the ECU and IDS provided.

Contents of the test method adjusted based on the vehicle (ECU) specifications

1. Threshold of the signal value to be used in the test
2. Preconditions for permitting specific values of the signal values used in the test (definition of the context in which a specific signal value is permitted)
3. Maximum allowable periodic disruption of messages used in the test (10%)
4. Maximum bus load for each bus (95%)

Policy for coordinating and implementing test methods based on IDS specifications

a. Test cases that can be tested with reference to other test cases are excluded.

b. Test cases related to functions (remote functions, etc.) that are not used in the vehicle in the actual machine test are excluded.

c. Functions that are considered not difficult to implement (they can be developed as required at a cost that is not too high), such as the output of the cumulative number of detection occurrences, are excluded.

d. If the base IDS is able to detect SEv, but it does not detect the expected value of the test case (detection count, detection reason), and if it requires more than a certain cost to detect it as expected, it should be excluded or IDS requirements should be adjusted (whether it actually operates as expected when PoC are used with OEM, or when it is mounted on a mass-production vehicle depends on the coordination with the IDS vendor).

Verifying Test Cases with IDS Actual Machine Test (3/5)

Among the target items excluded, *a to c are test cases that are excluded based on the adjustment and implementation policy of the test method based on the IDS specification defined in the previous slide. *1-3 are test cases that are excluded based on the specifications of the Base IDS and discussions with vendors. The reasons for this are described on the following slide.

Major class	Small classification	Test Case ID	ETAS	ARILOU
Detection function	No false positives	SD-FP-1	○	○
		SD-FP-2	Not applicable (*a)	Not applicable (*a)
	1. Error in the data of a single message	SD-TP-1-1	○	○
		SD-TP-1-2	Adjustment (specification of msg)	Not applicable (*1)
		SD-TP-1-3	Adjustment (prerequisites)	Adjustment (Detection target msg is output only to the payload.)
	2. Transmission cycle error	SD-TP-2-1	○	Adjustment (detection count)
		SD-TP-2-2	○	Adjustment (detection count)
	3. Error in relation to previous/next message	SD-TP-3-1	Adjustment (specification of msg)	Not applicable (*1)
		SD-TP-3-2	Not applicable (*a)	Not applicable (*a)
	4. Context error	SD-TP-4-1	Adjustment (detection target msg)	○
		SD-TP-4-2	○	Adjustment (detection target msg)
		SD-TP-4-3	Not applicable (*b)	Not applicable (*b)
		SD-TP-4-4	Adjustment (prerequisites)	○
	5. Status error of in-vehicle NW	SD-TP-5-1	○	○
	6. Attacks on diagnostic protocols	SD-TP-6-1	Adjustment (prerequisites)	○
		SD-TP-6-2	Adjustment (prerequisites)	Adjustment (Detection reason)
		SD-TP-6-3	Not applicable (*2)	Adjustment (Detection reason)
		SD-TP-6-4	○	○
		SD-TP-6-5	Not applicable (*a)	Not applicable (*a)
		SD-TP-6-6	○	○
		SD-TP-6-7	○	○
		SD-TP-6-8	○	○
Logging Function		SL-1-1	○	○
		SL-1-2	Not applicable (*c)	Not applicable (*c)
		SL-1-3	Not applicable (*c)	Not applicable (*c)
Notification function		SN-1-1	○	Not applicable (*3)

Verifying Test Cases with IDS Actual Machine Test (4/5)

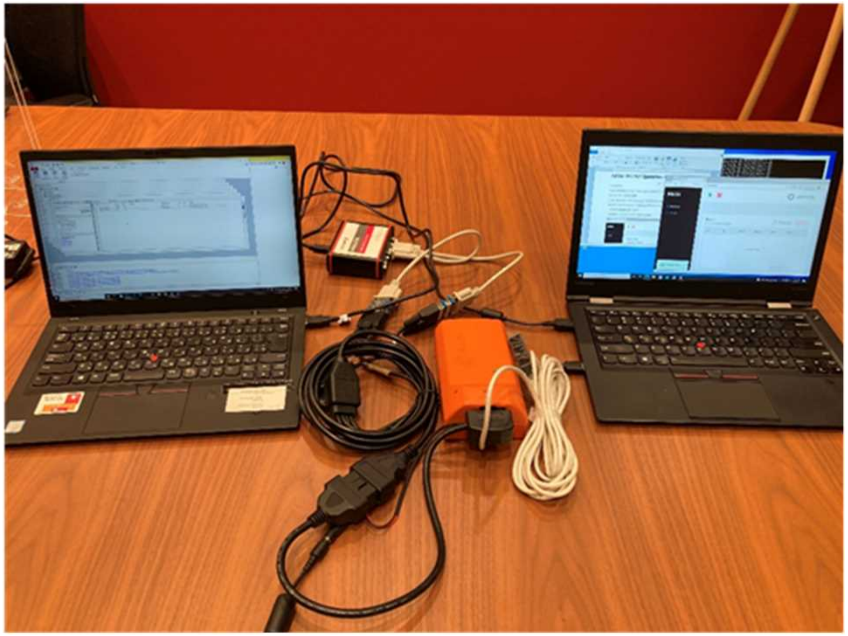
Reasons for exclusion from the Base IDS specification (previous slide*1 to 3) are shown below.

Comment number	Reasons for Exclusion
(*1)	ETAS/ARILOU's IDS customizes the system for OEMs. However, in order to shorten the development period, the IDS actual machine test has a minimum specification that outputs only one high-priority detection reason (e.g. "illegal transmission period") when a periodic transmission message is injected. On the other hand, the original expected value was to output all the corresponding detection reasons for the attack message (e.g. "illegal transmission cycle" and "invalid data range" as detection reasons). This time, the test cases that had the above effects were excluded, and the attack message to be injected was set to "not periodically send" in the target of the detection rule, etc. were adjusted.
(*2)	ETAS's base IDS does not support sequencing or stateful detection rules, so some test cases were excluded.
(*3)	IDS of ARILOU can be output to other CAN buses for IdsR module of AUTOSAR, for example, but this time, the message transmission function to the on-board network was omitted in order to shorten the development man-hour. For this reason, test cases related to the notification function were excluded.

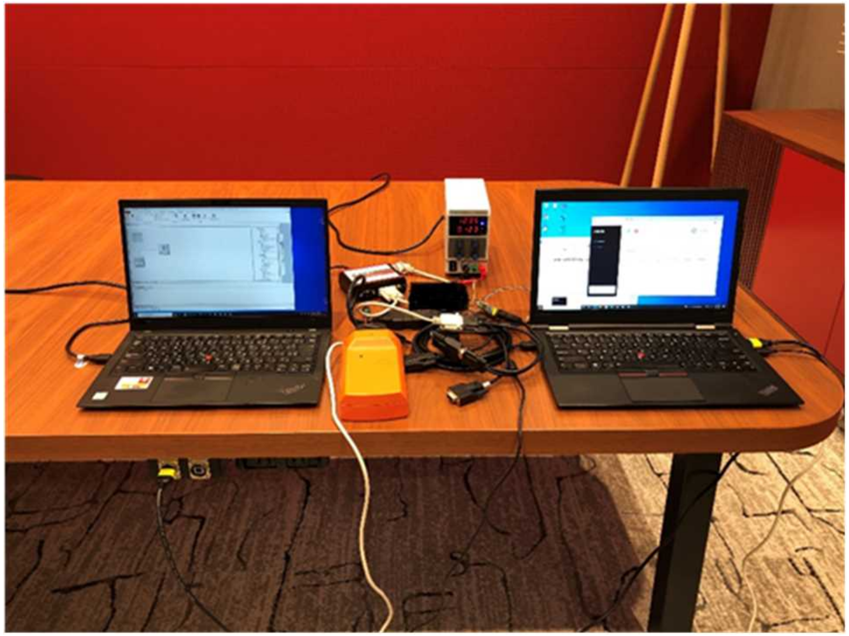
Verifying Test Cases with IDS Actual Machine Test (5/5)

The IDS actual machine test environment was constructed based on the basic configuration which was assumed when the basic test case was examined, and it was confirmed that the procedure shown in all test cases targeted for the test could be carried out as expected. The actual architecture of the IDS-based verification by "Arilou Information Security Technologies" is shown below.

Simulation environment



Test bed environment



Activities for Practical Deployment

For the transfer of the guideline, a total of eight technical discussion meetings were held, and JASPAR to which the guideline was transferred received comments and fed back. The hosting results are as follows.

Meeting Name	Date	Agenda
1st Technical Review Meeting	October 9, 2020	• Explanation of activity a.
2nd Technical Review Meeting	December 18, 2020	• Effectiveness of operations • Counseling regarding equipment provision
3rd Technical Review Meeting	April 14, 2021	• Usage Scenes of IDS Development Process Verification and Assumed Basic Test Cases • Scope of the fundamental test case
4th Technical Review Meeting	June 28, 2021	• Basic Test Case Test Perspective
5th Technical Review Meeting	July 29, 2021	• Basic Test Case Test Method
6th Technical Review Meeting	October 5, 2021	• Specification evaluation point of view
7th Technical Review Meeting	November 18, 2021	• Explanation of the purpose of activity a. (again)
8th Technical Review Meeting	February 10, 2022	• Explaining comments from OEMs that challenges in launching IDS development • Verifying schedule to transfer

Activities for Practical Deployment

Though the transfer of the guidelines has been accepted, the specific office procedures are planned for the end of May 2022. In addition, substantial research such as actual test and content study was completed at the end of March, but feedback from JASPAR will be handled until immediately before the transfer.

#	Work and Procedures	Working entity	Status
1	Finalization of the SIP version of the guidelines	Work: PwC Review: JASPAR, IDS Assessment Guideline Assumption Readers	Agreed with JASPAR and SIPs to fix by the end of May.
2	Determination of contract contents regarding transfer	NEDO, JASPAR	Adjusting
3	Transfer	PwC, NEDO, JASPAR	Scheduled for the end of May

b. Research on connected car threat intelligence and initial response support

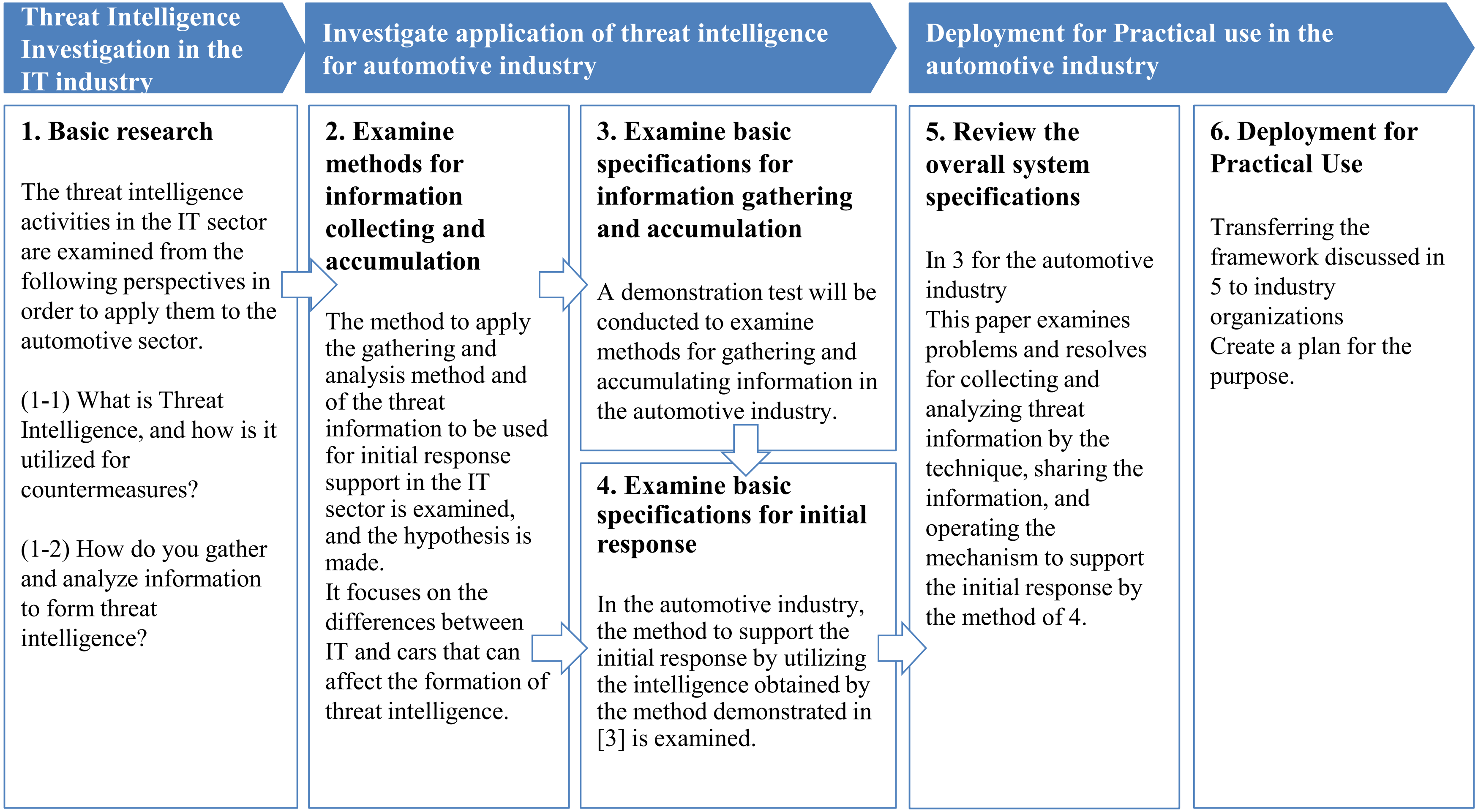
Research Objectives (Repeat)

The basic specifications for initial response support using Connected Car's method of gathering and accumulating threat information and threat intelligence will be formulated, and operation will be transferred to industry organizations in 2023.

#	Objectives overview set by SIP	Project objectives
b	**"Research on connected car threat intelligence and initial response support"** Consider the method of collecting and accumulating threat intelligence, conduct demonstration tests of attack monitoring using honeypots, develop basic specifications of systems for initial response support, and transfer to relevant industry groups to support collaborative development in the automotive industry.	• The ultimate goal is to transfer the operation of the basic system specifications to provide initial support for incident response to industry groups in 2023. • In initial support for incident response, assuming that sharing of threat information within the industry through the "Information Sharing System" is useful, the basic specifications for collecting and accumulating threat information and initial support using them will be formulated by the end of fiscal 2021. • The basic specifications of the entire system are examined when these elements are operated as a system, and the operation transfer to the industry group which is a practical development, and a final goal is completed in 2023.

Activity b Survey/Research Approach

Based on the threat intelligence activities in the IT industry that precede the incident response using threat intelligence, the application to the automotive sector is examined.



Threat Intelligence Investigation in the IT industry

Investigate application of threat intelligence for automotive industry

Deployment for Practical use in the automotive industry

1. Basic research

The threat intelligence activities in the IT sector are examined from the following perspectives in order to apply them to the automotive sector.

(1-1) What is Threat Intelligence, and how is it utilized for countermeasures?

(1-2) How do you gather and analyze information to form threat intelligence?

2. Examine methods for information collecting and accumulation

The method to apply the gathering and analysis method and of the threat information to be used for initial response support in the IT sector is examined, and the hypothesis is made.
It focuses on the differences between IT and cars that can affect the formation of threat intelligence.

3. Examine basic specifications for information gathering and accumulation

A demonstration test will be conducted to examine methods for gathering and accumulating information in the automotive industry.

4. Examine basic specifications for initial response

In the automotive industry, the method to support the initial response by utilizing the intelligence obtained by the method demonstrated in [3] is examined.

5. Review the overall system specifications

In 3 for the automotive industry
This paper examines problems and resolves for collecting and analyzing threat information by the technique, sharing the information, and operating the mechanism to support the initial response by the method of 4.

6. Deployment for Practical Use

Transferring the framework discussed in 5 to industry organizations
Create a plan for the purpose.

Approach overview towards FY2020 targets

In FY2020, the threat intelligence activity in the IT sector and the application to the automotive sector was examined. The hypothesis of the threat information gathering technique of the car was made.

1 Basic research

- Investigate threat intelligence activities in the IT sector from the viewpoint of information collection and analysis methods and initial response support.

(1-1) Threat intelligence in the IT sector

・Threat intelligence activities
・Examples of Threat Information Provided
・Use for initial response

(1-2) Threat Information Collection and Analysis Methodology

How do I collect information in (1-1)?
・Information gathering method
・Analysis point of view

INPUT

- IT threat intelligence activities

OUTPUT

- **(1-1) Example of IT area threat intelligence, initial response support using threat intelligence**
- **(1-2) Threat Information Collection and Analysis Methodology in the IT sector**

2 Examine methods for information collecting and accumulation

- Issues for applying information collection and analysis methods in the IT sector to the automotive sector are mentioned, and a hypothesis for solving the challenges is made.

(1-2) Methods for gathering and analyzing information in the IT sector

Consideration of Differences Between Car and IT Domain

(2-1) Methodology for Gathering and Analyzing Information in the Automotive Domain (What-If)

INTPUT

- (1-2) Methods for gathering and analyzing information in the IT sector
- Consideration of Differences Between IT and Car Domains

OUTPUT

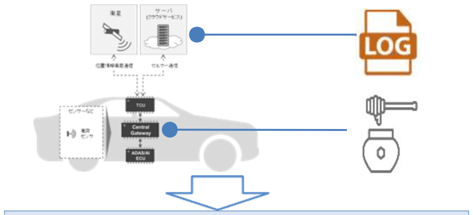
- **(2-1) Hypothesis on methods for gathering and analyzing information in the automotive sector**

Outline of Approach to Targets for Fiscal 2021

In fiscal 2021, a demonstration test was conducted based on a hypothesis created in the previous year. Specification of initial response support utilizing collected threat information was examined.

3 Examine basic specifications for information gathering and accumulation

- Execute a demonstration test based on the project prepared in ② and evaluate the effectiveness of the capture method.



Analysis of implementation results and evaluation of effectiveness

INPUT

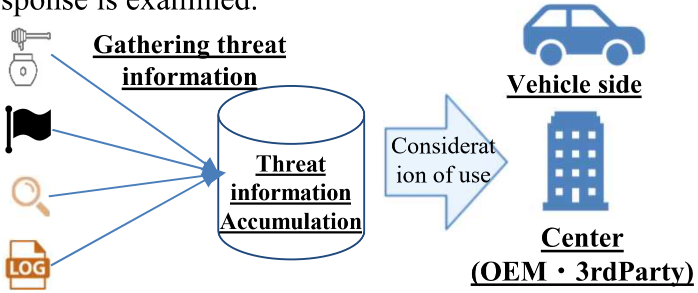
- Experimental Design for cyber-attack Capture and Gathering Methodology

OUTPUT

- **Test results**
- **Effectiveness of cyber-attack Capture and Gathering Methodology**

4 Examine basic specifications for initial response

- The method of utilizing the threat information collected and accumulated by the method examined in ③ for the initial response is examined.



Gathering threat information

Threat information Accumulation

Consideration of use

Vehicle side

Center (OEM・3rdParty)

INTPUT

- Effectiveness of cyber-attack Capture and Gathering Methodology
- Examples of Threat Information Utilization in the IT sector

OUTPUT

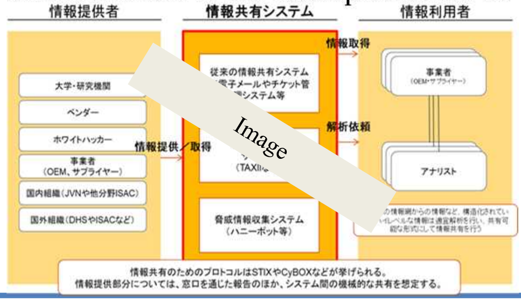
- **Draft use of threat information in response to initial responses in cars**

Outline of Approach to Targets for Fiscal 2022

In fiscal 2022, a mechanism to collect, analyze, and share threat information using threat information as an industry will be examined, and a plan for the transfer of practices to industry groups will be examined.

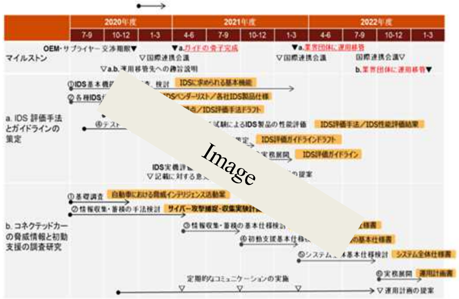
5 Review the overall system specifications

- In order to smoothly operate threat information gathering and sharing activities in the automotive industry, activities will be designed with reference to the examples in the IT industry.



6 Deployment for Practical Use

- Prepare a draft operation plan for practical development based on the destination of operation transfer and the exchange of opinions.



INPUT

- Examples of Threat Information Sharing in the IT Domain
- Exchanging views with stakeholders

OUTPUT

- **Draft operational design for the sharing of threat information on cars**

INTPUT

- Draft operational design for the sharing of threat information on cars
- Exchanges of views with operation transfer destination

OUTPUT

- **Draft operation plan for threat intelligence sharing activities**

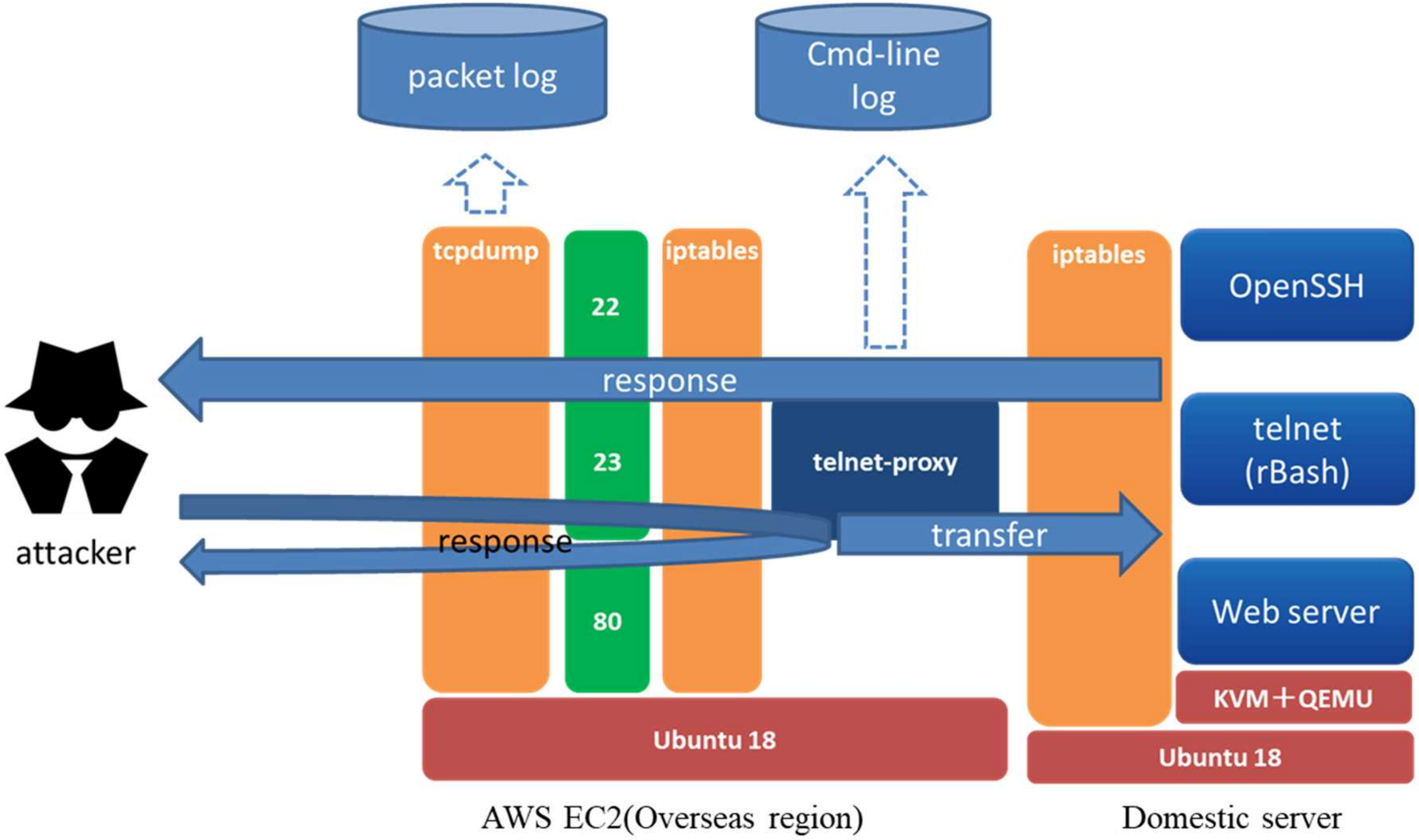
Threat Information Gathering Method

In order to establish gathering and accumulation method of threat information in the car domain, the threat information observation experiment is carried out referring to the case of implementation in the IT domain. In this activity, the research is carried out focusing on honeypots and CTFs.

Purpose	• Establishing methods for gathering and accumulation threat information in the car domain.
What-If	• In the IT field, various methods have been tested and operated to actively collect threat information on the trends of cyber attackers, attack methods, etc., and they are useful for the construction of cyber intelligence. • In the connected system, the threat information can be collected by the same technique, and cyber intelligence can be constructed. (Example) Fixed point observation | Honeypot | CTF | Bug Bounty | OSINT gathering
gathering information (Assumed)	• Cyber Attacker Properties (Indicators such as IP Address and URL) • Attack operandi (TTPs of attack codes, malware, etc. attempted)
Approach	• Attack patterns on connected systems are organized, and the possibility of collecting threat information in connected systems is evaluated through actual observation experiments using the threat information collection method in the IT field.

Honeypot demonstration

We surveyed aftermarket products that can be discovered by a wide area scan, developed a prototype of honeypots for those products, and began observational experiments on cyber attacks in late January 2021.



Devices that can be discovered from the Internet

Twelve devices such as on-board routers and gateways were discovered by the Internet wide area scan.

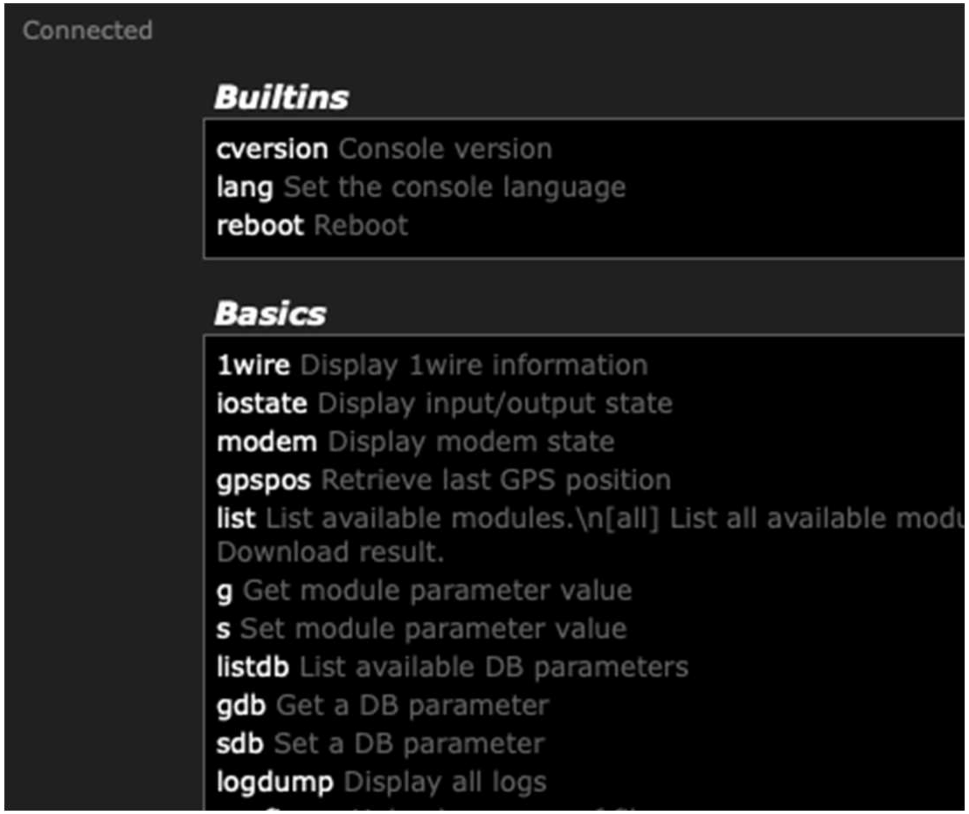
Device name	Web-base/Cluster-base	#devices	Discovered Countries	Open ports
Product A	Cluster-based	278	NL 26.0% SE 18.9% US 16.3%	22/tcp 80/tcp 8080/tcp
Product B	Cluster-based	391	ES 59% MA 20.3% DE 11.9%	22/tcp 23/tcp 80/tcp
Product C	Web-search-engine-based	821	US 96.5% BR 2.2%	8443/tcp 22/tcp 8080/tcp 80/tcp 443/tcp
Product D	Web-search-engine-based	186	IT 59.1% DE 40.0%	80/tcp or 81/tcp 21/tcp 22/tcp
Product E	Web-search-engine-based	88	DE 95.6%	80/tcp 22/tcp 23/tcp
Product F	Both	104	US 60.0% ES 11.8% AU 10.0%	2332/tcp 9191/tcp 9443/tcp
Product G	Web-search-engine-based	5	TW 100.0%	161/tcp
Product H	Web-search-engine-based	360	ES99.4%	80/tcp
Product I	Web-search-engine-based	3	DE 100%	21/tcp 80/tcp 443/tcp
Product J	Web-search-engine-based	67	US 51.5% FR 19.6% CN9.6%	2332/tcp 9191/tcp 9443/tcp
Product K	Web-search-engine-based	144	ES 99.9%	21/tcp 22/tcp 80/tcp 123/tcp
Product L	Web-search-engine-based	85	Us 84.3%	8443/tcp 22/tcp 8080/tcp 80/tcp 443/tcp

Example device that can be discovered from the Internet

For some of the devices discovered, some services, including without authentication Telnet, were published on the Internet.

22/tcp OpenSSH5.1
23/tcp telnet
80/tcp http

No-authentication

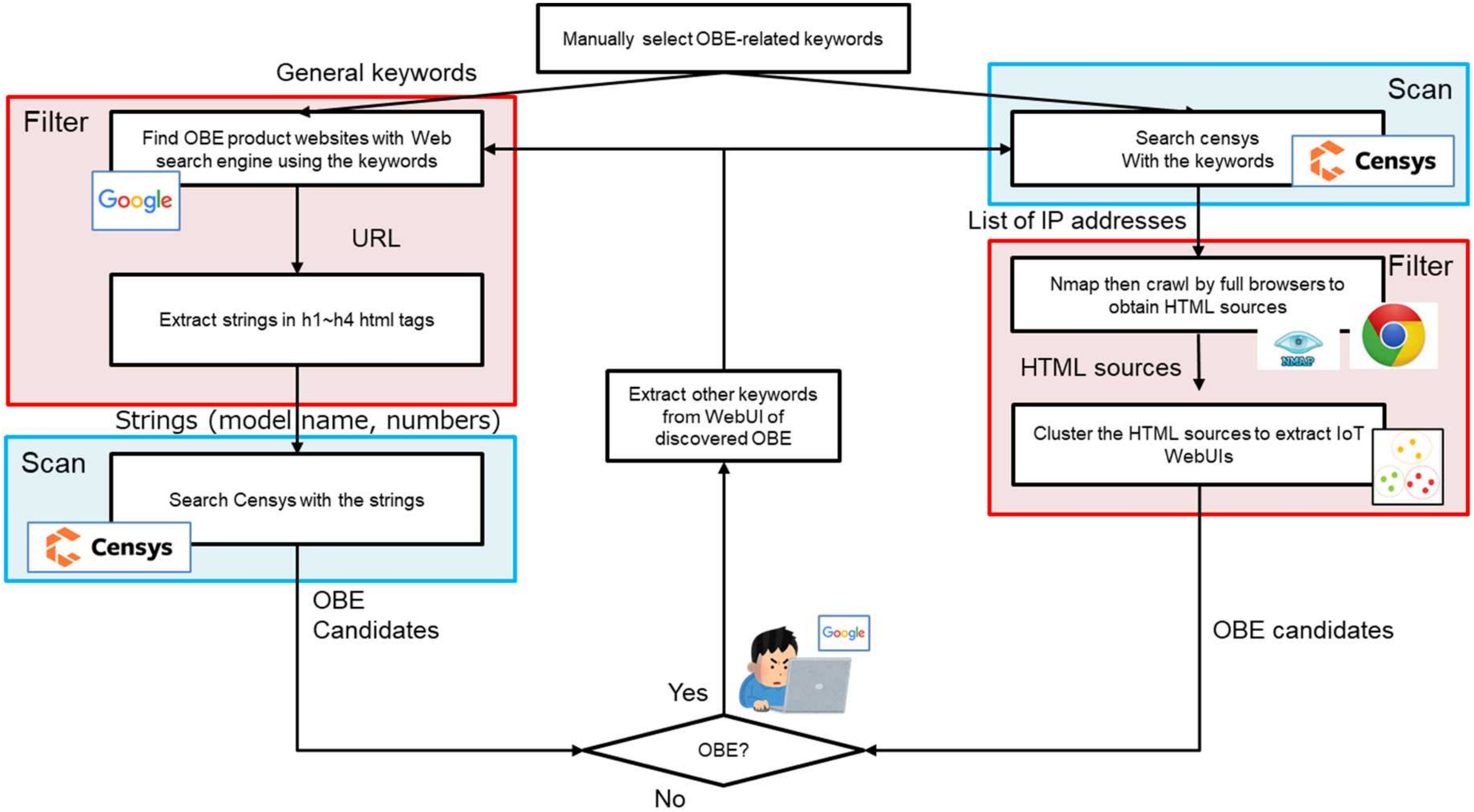


```
Connected

          Builtins
          cversion Console version
          lang Set the console language
          reboot Reboot

          Basics
          1wire Display 1wire information
          iostate Display input/output state
          modem Display modem state
          gpspos Retrieve last GPS position
          list List available modules.\n[all] List all available modu
          Download result.
          g Get module parameter value
          s Set module parameter value
          listdb List available DB parameters
          gdb Get a DB parameter
          sdb Set a DB parameter
          logdump Display all logs
```

Source: Jose Carlos Norte. Hacking industrial vehicles from the internet: http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html

About Device Search Methodology

In order to search in-vehicle devices efficiently, two approaches were implemented: an approach is to search the Web site of OBE products (keywords search using a Web search engine), and the other approach is to search Censys directly about keywords related to OBE products.

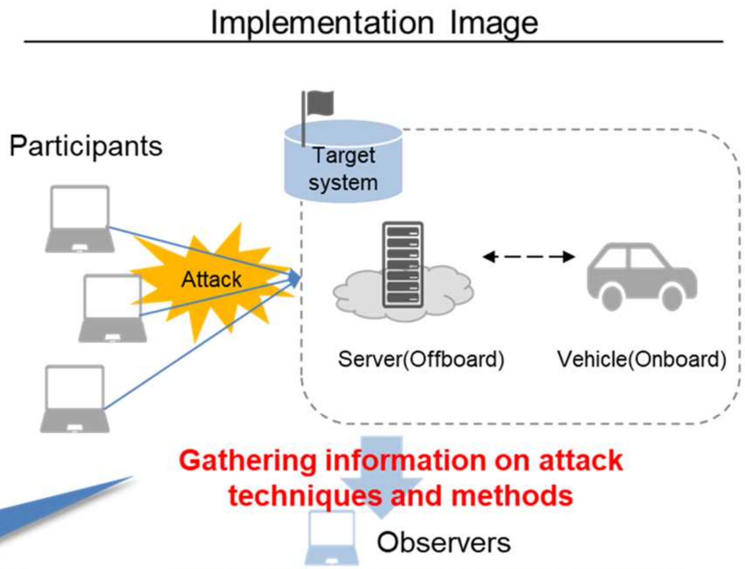

Manually select OBE-related keywords
General keywords
Filter
Find OBE product websites with Web search engine using the keywords
Google
URL
Extract strings in h1~h4 html tags
Strings (model name, numbers)
Scan
Search Censys with the strings
Censys
OBE Candidates
Extract other keywords from WebUI of discovered OBE
Google
Yes
OBE?
No
Scan
Search censys With the keywords
Censys
List of IP addresses
Filter
Nmap then crawl by full browsers to obtain HTML sources
NMAP
HTML sources
Cluster the HTML sources to extract IoT WebUIs
OBE candidates

About Implementation of Playground (CTF)

In the connected system, to know what attack is possible, a playground is carried out and the insights of the attack against the connected system is obtained from the behavior and attack method of the participant.

Purpose	• Investigate what kind of attacks can be made against the connected system of the car. • Consider the criteria for determining what kind of activity applicable to an "attack aimed at a vehicle".
Implementation Policy	• Participants attempt to attack the target system, targeting vehicle control and acquisition of vehicle information. • From the observation results of the attacker's attack technique and method, we will obtain knowledge for quickly detecting the attack.

Implementation Image



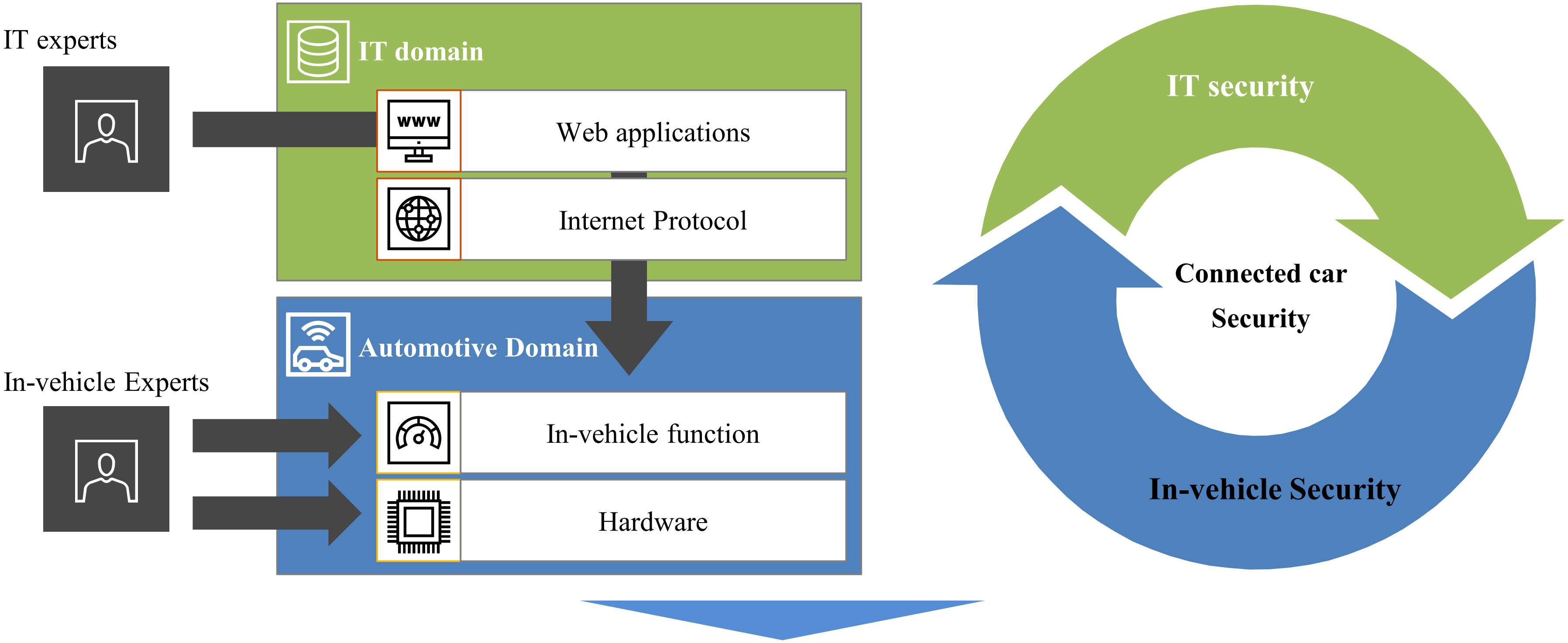
It will be used for developing in-vehicle device (automobile) honeypots and creating criteria when analyzing attacks during operation.

By holding CTF and operating Honeypot, it is expected that PwC will continue to obtain threat information and trends related to connected cars.

Threat Information Descriptions and Sharing Methods

In order to gather and share effectively threat information, the threat information to be handled must be structured at a certain level and the sharing methods must be formulated. Based on the richness of the information that can be described and the utilization status in the IT domain, this activity focused on STIX/TAXII.

BACKGROUND: With the connectivity and automation of vehicles, there has been an increasing number of links with existing Web and IT technologies.



The research will be conducted focusing on STIX/TAXII that are the most popular in the IT domain and have many types of information that can be described for efficiently utilizing threat information in a connected system that combines vehicle and IT systems.

(Reference) Information that can be written in STIX format

#	Classification*1	STIX information*2	Description
1	IOC (Breach Indicators)	Identity/Identifier	Information representing the actual individuals, organizations, groups, systems, industries, etc. targeted or potentially targeted by the attack.
2		Indicator	Information about technical logs or events that indicate the occurrence or doubt of an attack. Hash value, IP address, domain name, certificate, etc.
3		Location	Location information about attacks such as cyber attackers, attack platforms, and targets.
4		Observed Data	Information about cyber attacks such as files, systems, and network IP addresses. Unlike indicators and location information, it actually refers to (merely) information that has been observed more than once.
5	TTPs (Tactics/Techniques/Procedures)	Attack Pattern	Information that explains method (such as Spearphishing) a cyber attacker can use to attack a target.
6		Attack Infrastructure	Information about systems, software, physical/virtual resources, etc. for attack support functions. Describes the C2 server used at the time of attack, mobile devices that are part of the target system, servers, etc.
7		Intrusion Set	Information about attack patterns and groups (sets) of attack infrastructures with common properties that are considered to be created, coordinated, and implemented by a single cyber attacker.
8		Malware	Detailed information about how the attack program (malware) plugged into the target system works and does what.
9		Malware Analysis	Perform a specific analysis on a program suspected of being malware and show the results.
10		Tool	Information about legitimate software available to cyber attackers. Unlike malware, it refers to software that is legitimate software on the system and may be used by cyber attackers.
11	Security Alerts	Note	Provides information contexts by adding notes to existing STIX objects.
12		Opinion	Third-party evaluations of the accuracy of the data in STIX are called the Opinions. Five-step evaluation from strong consent to strong disagreement.
13		Vulnerability	Information on software and hardware requirements, design or implementation weaknesses / defects.
14	Intelligence Report	Campaign	Information on cyber attack operations (campaigns). Describes a series of of malicious activities or attacks that occur over a period of time against a specific set of targets. A campaign can be characterized by its purpose and the incidents that occur, the target person or resource, and the resources that it uses (infrastructure, intelligence, malware, tools, etc.).
15		Report	Information that summarizes cyber intelligence focused on one or more topics such as cyber attackers, malware, and attack methods.
16		Threat Actor	Information about individuals, groups, or organizations that are considered to be malicious. It is characterized by its motivation, capability, goals, skill, past activities, etc.
17	Tool configuration	Action (configuration) policy	Information about actions to take to prevent or respond to cyber-attacks. Information about patching, firewall reconfiguration, employee training, policy changes, and so on.

STIX's description of automotive threats

Threat-information from four studies was attempted to be described in STIX format using the following approach. Consequently, it was judged that the four threat-information data focused on using SITX could be described.

Report/Paper

Search for automobile attack cases and research reports.

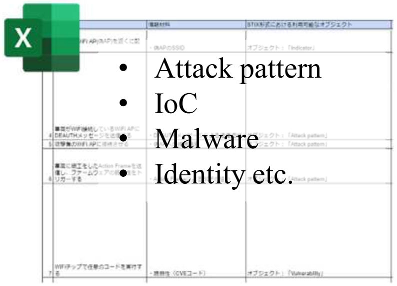
usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

SAE INTERNATIONAL

black hat

Obtained information

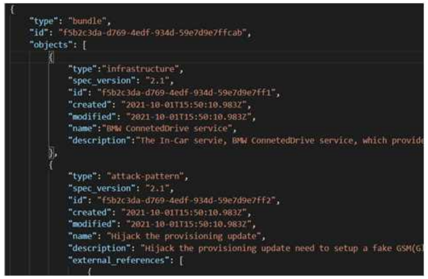
Analyze the reports to obtain threat information.



- Attack pattern
- IoC
- Malware
- Identity etc.

STIX Object

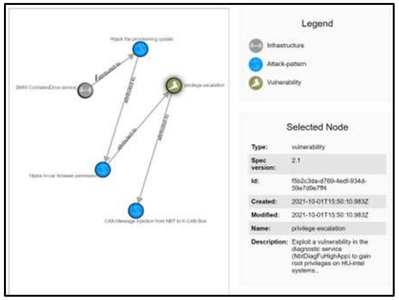
Make the threat information into STIX object.



```
{
    "type": "bundle",
    "id": "f5b2c3da-d769-4edf-934d-59e7d9e7ffcab",
    "objects": [
        {
            "type":"infrastructure",
            "spec_version": "2.1",
            "id": "f5b2c3da-d769-4edf-934d-59e7d9e7ff1",
            "created": "2021-10-01T15:50:10.983Z",
            "modified": "2021-10-01T15:50:10.983Z",
            "name":"BMW ConnetedDrive service",
            "description":"The In-Car servie, BMW ConnetedDrive service, which provide
        },
        {
            "type": "attack-pattern",
            "spec_version": "2.1",
            "id": "f5b2c3da-d769-4edf-934d-59e7d9e7ff2",
            "created": "2021-10-01T15:50:10.983Z",
            "modified": "2021-10-01T15:50:10.983Z",
            "name": "Hijack the provisioning update",
            "description": "Hijack the provisioning update need to setup a fake GSM(G
            "external_references": [
                {
```

Visualization

Visualizing STIX object using the OASIS STIX Visualizer(*)



Hijack the provisioning update
BMW ConnectedDrive service
privilege escalation
Hijack in-car browser permission
CAN Message injection from NBT to K-CAN Bus
Legend
Infrastructure
Attack-pattern
Vulnerability

Selected Node

Type:	vulnerability
Spec version:	2.1
Id:	f5b2c3da-d769-4edf-934d-59e7d9e7ff4
Created:	2021-10-01T15:50:10.983Z
Modified:	2021-10-01T15:50:10.983Z
Name:	privilege escalation
Description:	Exploit a vulnerability in the diagnostic service (NbtDiagFuHighApp) to gain root privileges on HU-intel systems..

https://oasis-open.github.io/cti-stix-visualization/(Link)

#	Target vehicle type	Overview
1	BMWs with Connected Drive (BMWs)	A bogus base station was installed, and the response of BMW ConnectedDrive service was rewritten, and the attacker ‘s web server was accessed, then the ECU was reset or seats were moved back and forth in utilizing the vulnerability of the browser, etc. (2020)
2	Model S/X (Tesla)	We exploited the bufferoverflow vulnerability of WiFi connectivity in Marvell's Wi-fi Module (88W8688), which is built into Tesla Model S/X, and used TCP23 number port-of-service. (2018)
3	E-Class (Mercedes-Bentz)	The TCU (HERMES/Linux/ARM) eSIM can be connected to a back-end server through an attacker's 4G router, and Mercedes ME functionalities (such as door locking/unlocking) can be utilized for other people's cars. (2020)
4	Cherokee (Jeep)	It is reported that the ECU firmware can be rewritten through the cellular telephone network, and BCM such as the vehicle's steering, air conditioner, stereo, etc. can be operated illegally for the driving vehicle. (2015)

Examination of basic specifications for initial response

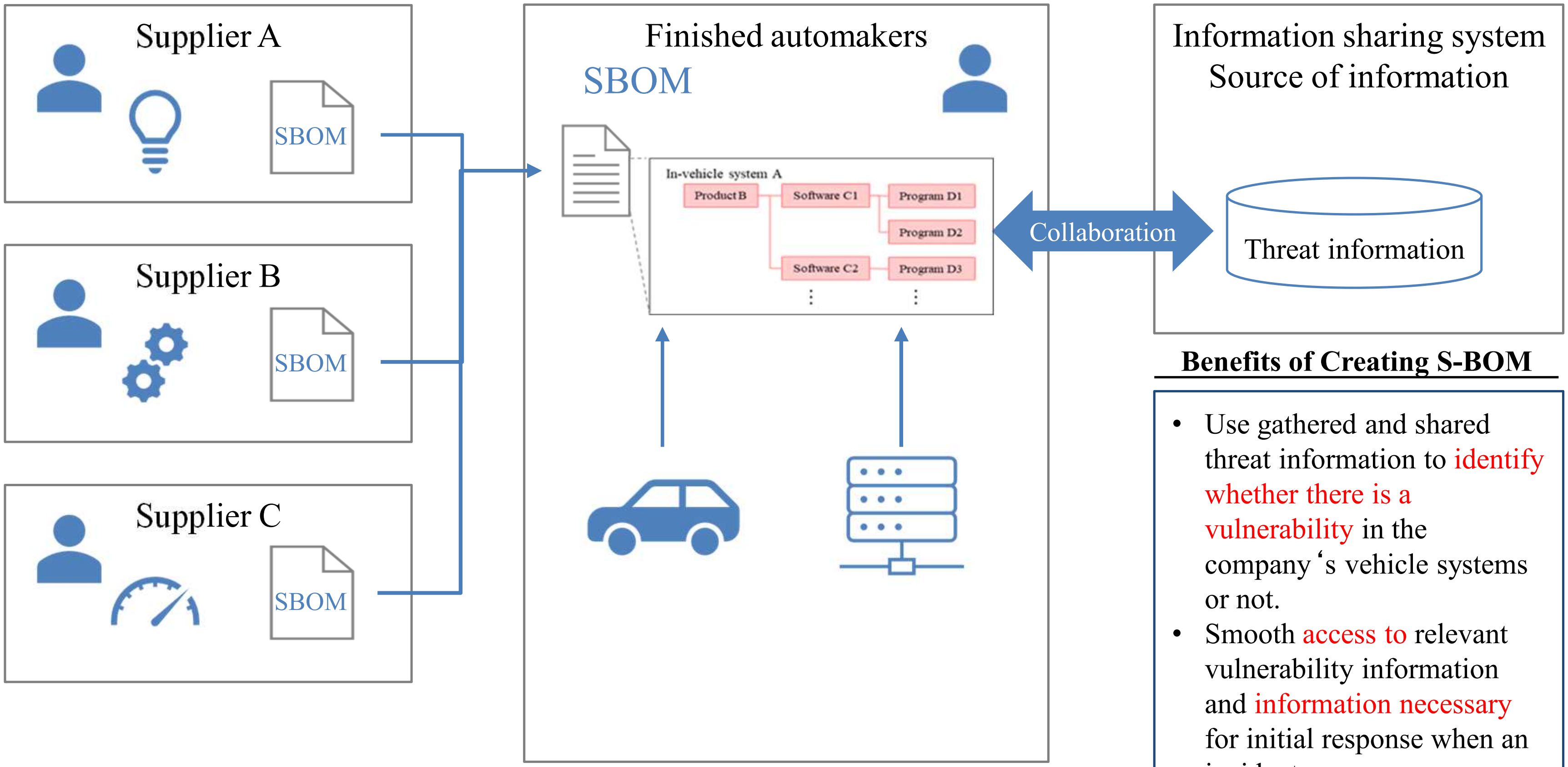
Initial response in this activity refers to activities that prevent incidents through information gathering during normal times and response activities after an incident occurs.

Phase		Description
Preventive measures	Identification	Identify threats and vulnerabilities related to owned cars and systems through information gathering
	Defense	Take appropriate security measures against identified threats and vulnerabilities
Countermeasures for incidents	Detection	Monitoring the vehicle system and detecting events
	Response	Respond to incidents that have occurred
	Recovery	Recover incidents that have occurred and take permanent measures

Scope of the Initial response in this project

Utilization of threat information for initial response

In order to facilitate the selection of threat information to be gathered and the determination of threat information gathered, a software list (S-BOM) within the company's products and systems must be created.



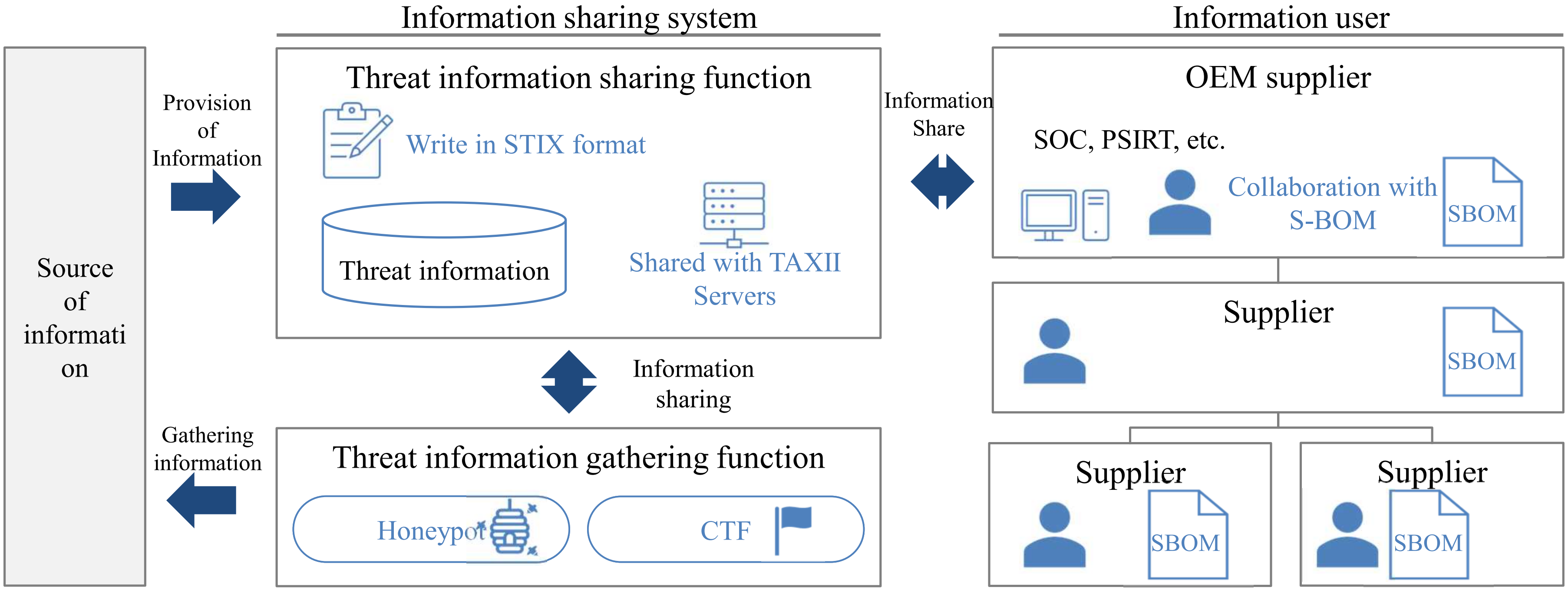
Benefits of Creating S-BOM

- Use gathered and shared threat information to identify whether there is a vulnerability in the company ‘s vehicle systems or not.
- Smooth access to relevant vulnerability information and information necessary for initial response when an incident occurs.

Examination of overall system specifications

The ideal image of the information sharing system is as follows.
By using each element technology in gathering, accumulating, and sharing information, threat information can be smoothly utilized for initial response.

Point of the information sharing system	- Shared System Functions: Threat-Info Description (STIX)/Shared (TAXII)/Gathering (Honeypot, CTF) - User Functions: S-BOM



Status of collaboration between Japan and Germany

Trends in Automated Driving Security Development Assistance in Germany

In Germany, the Federal Department of Education and Research (BMBF) is leading the security research and development support for connected cars (automated driving), and at least four projects are currently in progress. The projects are in collaboration with SecForCARs.

R&D support requirements in Germany

The following outcomes needs to be included at minimum:

- Methods for protecting vehicles and infrastructures from cyber-attacks
- Methods for verifying vehicle security

#	Project Name	Activity theme
1	SATiSFy (Implement of safety functions in an automated driving vehicle)	Evaluation of individual components (sensors, etc.) and their mutual interactions related to automated driving
2	**SecForCARs (Security of Connected Automated Vehicles)**	**Research and Evaluation of Methods and Tools for Securing Communication to Vehicles**
3	SecVI (Security Architecture of Communication Network for Vehicles)	Developing a Robust, low-complexity network architecture for vehicles
4	VITAF	Ensuring the reliability of the automated driving How cyber-attacks are Detected and Responded Immediately Developing a mechanism to avoid impacts on safe operation even in the event of cyber-attacks Vehicle data protection (e.g. masking)

https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/it-sicherheit-und-autonomes-fahren

Japan-Germany Collaboration Workshop

Five JAPAN-Germany collaboration workshops are planned, and as of April 2022, the third workshop has been held.

Time and location	Name of the meeting	Agenda
2021/7 Online	WS1	• Threat intelligence and Vehicular honeypots • Concept and demonstration for integrated OTA software update • IDS management concept for distributed IDS
2021/12 Online	WS2	• Threat intelligence and Vehicular honeypots • Security Composition for Automotive System of Systems • Platform and Hardware Security
2022/4 Online	WS3	• Threat information sharing system • Discovery of exposed automotive devices • Crypto Hardware security
Fall 2022 TBD	WS4	TBD
Fall 2023 TBD	WS5	TBD

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

This report documents the results of Cross-ministerial Strategic Innovation Promotion Program (SIP) 2nd Phase, Automated Driving for Universal Services (SIP-adus, NEDO management number: JPNP18012) that was implemented by the Cabinet Office and was served by the New Energy and Industrial Technology Development Organization (NEDO) as a secretariat.