SIP
戦略的イノベーション創造プログラム

「Cross-ministerial Strategic Innovation Promotion Program (SIP)/ Automated Driving (Expansion of Systems and Services)/ Research on New Cyber-attacks and Countermeasures Against New Cyber-Attacks

FY2020 Interim Report
Summary version

PwC Consulting LLC

2021 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.

a. Development of IDS Evaluation Method and Guideline

Research Objectives

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 the industry organizations in 2023.

#	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

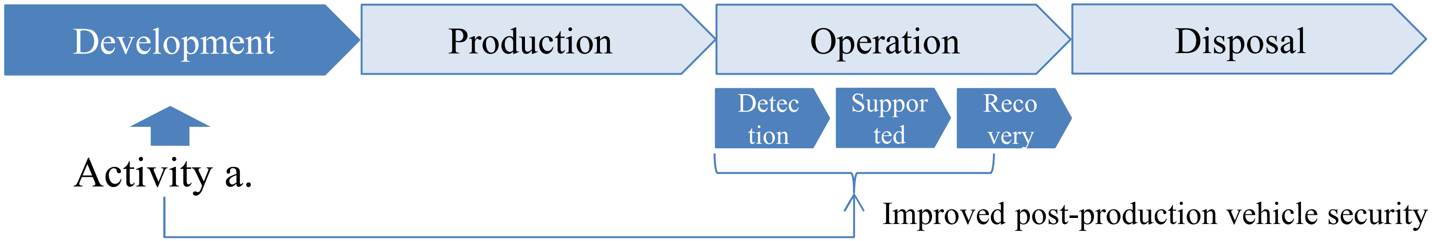
WP29 UN-R155 sets requirements for the manufacturers to enable the vehicles to detect and respond to cyber-attacks.

Industry Practices

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>.



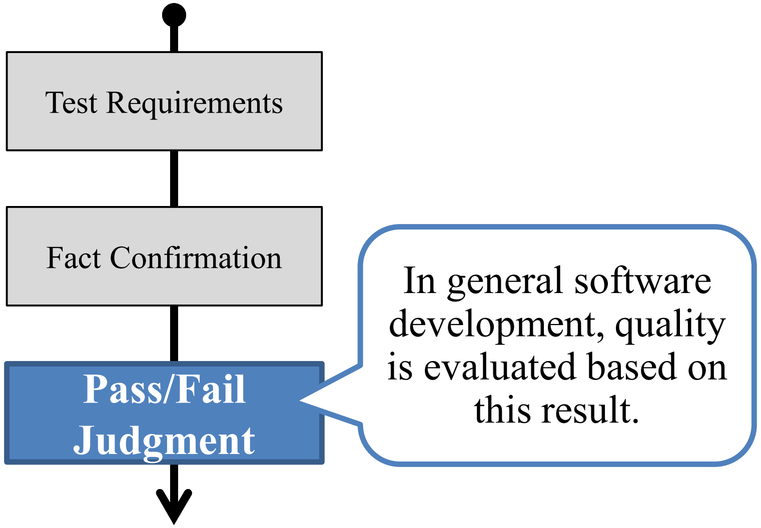
Definitions of “Testing" and “Evaluation"

In the guideline, terms “Testing/Test” and “Evaluation” are used separately as per following definitions.

Testing

Testing confirms that the test target operates as expected, the actual software and hardware shall be utilized, and the work shall be carried out according to the predefined method, and the pass/fail judgment shall be carried out according to the criterion whether the test requirement is satisfied or not.

The information necessary for pass/fail judgment (test requirements, work details, pass/fail judgment criteria, etc.) shall be referred to as "test cases".



Test Requirements

Fact Confirmation

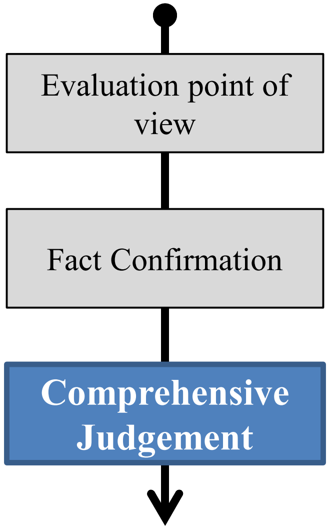
Pass/Fail Judgment

In general software development, quality is evaluated based on this result.

Evaluation

Evaluation comprehensively assesses whether the target of assessment is suitable for a specific environment or purpose.

Evaluation items includes considerations for cost, usability, availability of functions, performance, etc.



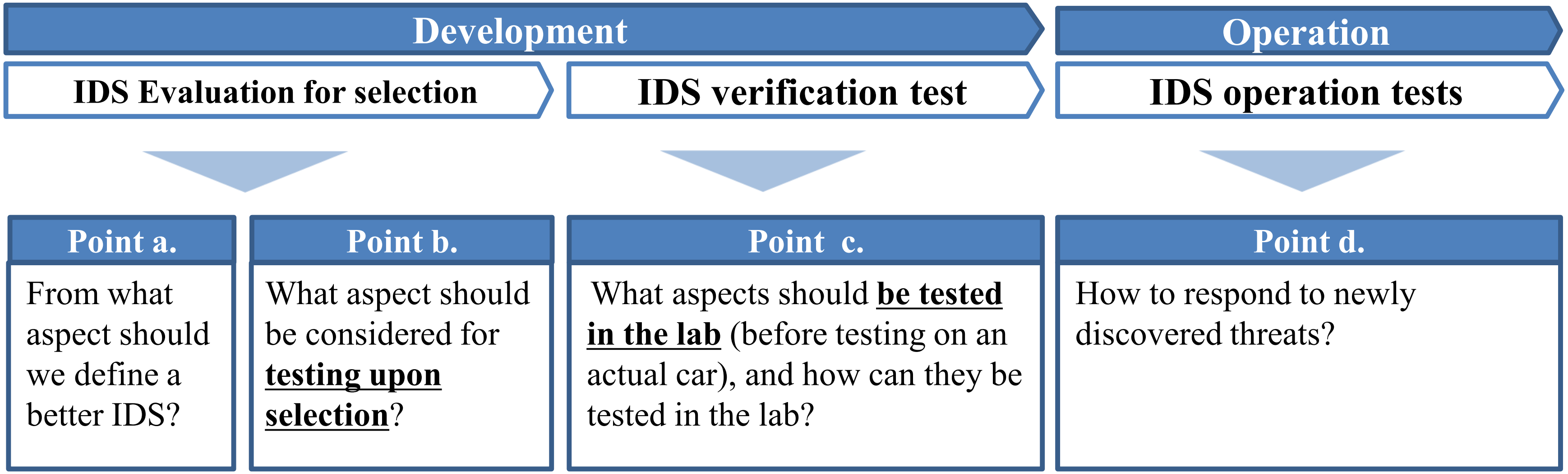
Evaluation point of view

Fact Confirmation

Comprehensive Judgement

Scope of the IDS evaluation guidelines

Following activities 1~3 are performed to contribute to IDS selection, in-lab IDS behavior verification, defect identification and respond to new threats /maintain vehicle operation.



Development

Operation

IDS Evaluation for selection

IDS verification test

IDS operation tests

Point a.

From what aspect should we define a better IDS?

Point b.

What aspect should be considered for **testing upon selection**?

Point c.

What aspects should **be tested in the lab** (before testing on an actual car), and how can they be tested in the lab?

Point d.

How to respond to newly discovered threats?

Scope of the project's activities

#	Activity	Point
1	Examine the evaluation perspectives based on the specifications	a
2	Examine basic test cases (test requirements, prerequisites, test environment, test procedures, etc.)	a, b, c
3	Examine methods to identify the detection function required for IDS from attack cases	d

Consideration regarding expected activity outcomes

By documenting the activity results as a guideline to be used upon IDS implementation, it is expected to establish industry-common perspective for evaluation/analysis as well as contribute to cost reduction for industry stakeholders.

Activity	Expected output (contents of the guideline)	Expected outcome (Hypothesis)
1. Examine the evaluation perspectives based on the specifications	**Specification evaluation items** List the perspectives to be checked when evaluating IDS product specifications on a desktop.	• Provide important evaluation points at the time of IDS selection. • IDS from different suppliers can be compared from common perspective • Reduce the cost of preparing the specification evaluation items using the guideline.
2. Examine basic test cases	**Basic test case** Lists the test requirements required to evaluate the operation of the IDS real machine, and provides examples of test environments, test procedures, etc. for testing in the laboratory prior to the actual vehicle test.	• It is possible to confirm that there are no fatal problems in the detection function of IDS at the time of IDS selection and the initial stage of IDS verification. • By showing requirements including environment, etc., the preparation and implementation cost of the test can be reduced. • Reduce the cost of creating test cases using the guideline.
3. Examine methods to identify the detection function required for IDS from attack cases	**Method to identify test requirements from new threats** Establish a method to identify how a new threat can be detected by the installed IDS	• If new threats are discovered for the vehicles on the road, IDS can be tested in a logically descriptive manner.

Overview of IDS Evaluation Guideline Development

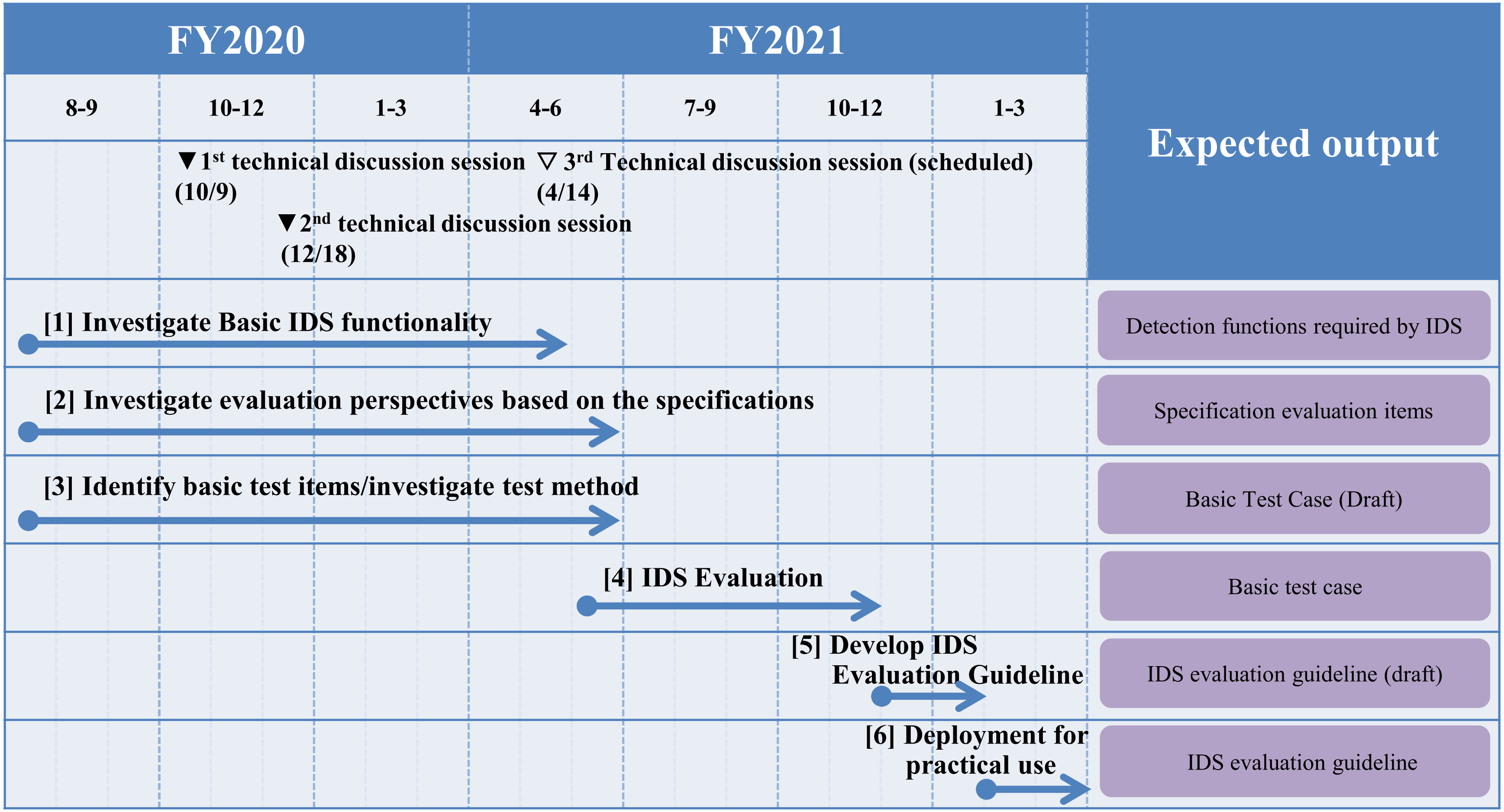
Following approach will be taken to develop IDS evaluation guidelines and transfer to the industry groups.

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. Overall schedule

Target for each year will be determined to complete transfer of the output to the industry groups by the end of March 2022

●⟶ : Working Period, ▼:Milestones (Fixed), ▽: Milestones (planned), Expected OUTPUT



FY2020 | **FY2021** | **Expected output**

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

▼1st technical discussion session (10/9)

▼2nd technical discussion session (12/18)

▽ 3rd Technical discussion session (scheduled) (4/14)

Activity	Expected output
[1] Investigate Basic IDS functionality	Detection functions required by IDS
[2] Investigate evaluation perspectives based on the specifications	Specification evaluation items
[3] Identify basic test items/investigate test method	Basic Test Case (Draft)
[4] IDS Evaluation	Basic test case
[5] Develop IDS Evaluation Guideline	IDS evaluation guideline (draft)
[6] Deployment for practical use	IDS evaluation guideline

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)

Research on vehicle cyber-attack cases

In order to identify the security events that should be detected by the IDS, the conference held in 2020, Web information, and vulnerability information were analyzed. 12 cases were analyzed in detail as a cyber-attack against a vehicle.

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

[Reference] Examples of attacks analysis

- **Examples of Attacks against Tesla Model S/X**

Exploited the bufferoverflow vulnerability of Wi-Fi connectivity in Marvell’s Wi-fi Module (88W8688), which was built into Tesla Model S/X manufactured before March 2018, to connect the HU to the attacker’s Wi-Fi AP and to use TCP23 number port service.

- **Examples of Attacks against Mercedes-Bentz E Classes**

The TCU (HERMES/Linux/ARM) eSIM can be connected to a back-end server through an attacker’s 4G router, and Mercedes ME functions (such as door locking/unlocking) can be utilized for other people’s cars.

Security events to be detected identified from the cases

The probable events for on-board network and ECU were identified through analyzing the vehicle cyber-attack cases.

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

Specification evaluation items (draft)

Upon IDS selection, the specification evaluation items(draft) and corresponding questions was prepared intended for use by the OEM as basis for questions asked to IDS vendors regarding specifications.

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-Car 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)

Specification Evaluation Items (Draft)-Questions and Options (Some Excerpts)

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()

Validation Results and Considerations of Specification Evaluation Items

The validity of the draft was verified using questionnaires on the specification evaluation items from three IDS vendors (covering six products),

Summary of Questionnaire Results for Specification Evaluation Items

- Basic detection functions are generally supported for the security events to be detected, and there was no significant difference at the specification level※1.
- There were differences in some specifications, such as whether CAN TP･AVB/TSN was supported, signature-based detection, and detection of external device connections.
- The logging or notification output items were either supported by each company or customized.
- For Security Operation Center (SOCs) requirement for analyzing the detection results, there were differences in the status of support, such as provision by in-house provision/collaboration/response by OEM.

Considerations for Questionnaire Results

- From the questionnaire, **it was possible to easily grasp whether necessary functions and characteristics are provided, and to compare multiple IDS products**.
- **For the security event to be detected, it is difficult to judge or to identify the difference between each product regarding the product conformity for vehicle implementation.**
- **Differences in some specifications** such as supported protocols, detection algorithms, presence or absence of detection functions for external device connections, and correspondence status of SOC can be **easily identified**.
- Since the output items of logging or notification are basically customized, it is difficult to identify differences **regarding logging and notification items**.

※1. Some products do not support the connection of unknown external devices. In addition, there were differences in the response status of contextual security events for Ethernet compliant products.

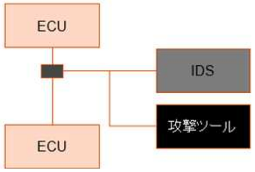
Basic Test Cases

The following table describes the test requirements and test methods for the basic test cases from the perspective that must be tested at the minimum in the software unit test when IDS is selected or verified.

Item		Description
Test Requirements		Description of the expected value of the test to clarify the perspective to be confirm in the test
Test method	**Prerequisites**	Conditions to be met prior to the implementation of the test
	Test environment	Equipment used for the test and how to connect them
	Test Procedure	Test procedure
	Example of Pass/Fail Judgment Method	A method for determining acceptance or rejection of a test item. Determine the indicators against the standards.

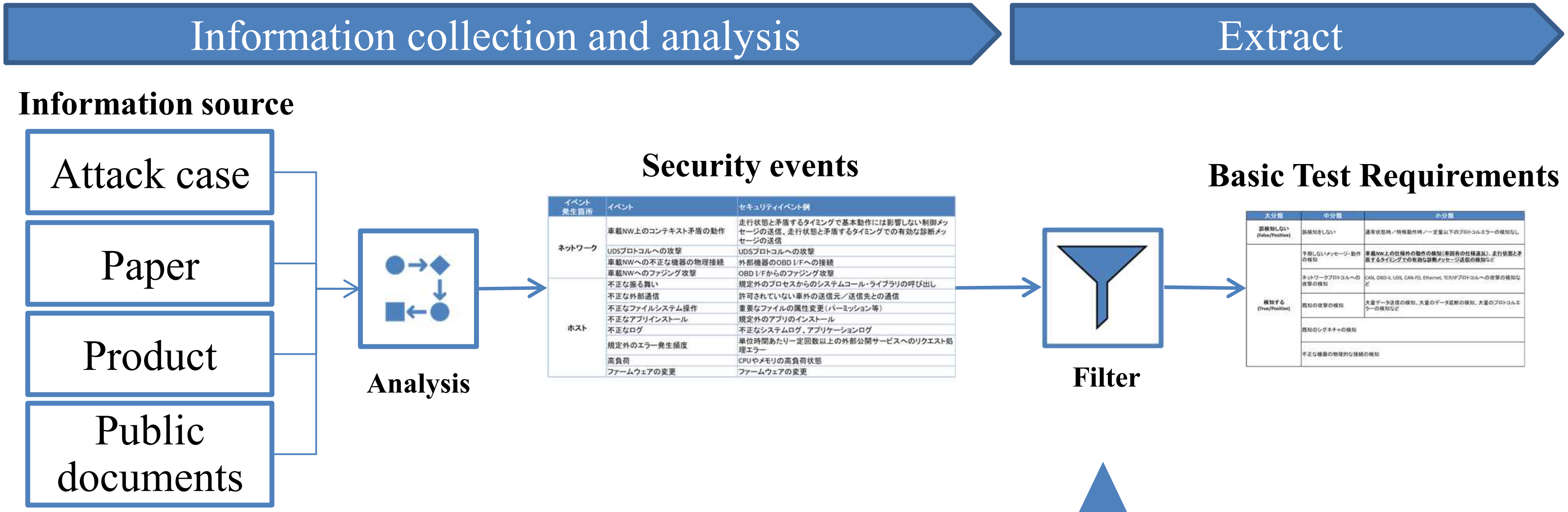
[Reference] Fundamental Test Case Image

The following is an example of a test case for detecting an unspecified transmission cycle for periodically send messages.

Item		Content
Test Requirements		Detects out-of-specification send intervals for periodically transmitted messages.
Test method	**Prerequisites**	• CAN ID = xx message transmits the vehicle speed from ECU X at 100msec intervals. • No MAC is set for the message. • The message is not encrypted.
	Test environment	
	Test Procedure	1. Connect the device as shown in the figure in the test environment. 2. Turning on the power 3. 10msec after receiving a message with the legitimate CAN ID = xx from the attacking tool, a message with the same content is transmitted on the same CAN bus once a second, and 10 messages are transmitted. 4. Retrieve IDS detection log. 5. Refer to the IDS log to confirm that all messages sent from the attack tool have been entered. 6. Refer to the IDS log to check the security event detection status.
	Example of Pass/Fail Judgment Method	Pass condition: Of the 10 messages sent from the attack tool, 10 messages were detected as cyclic anomalies.

Identification of basic test requirements (tentative)

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



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

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、大量のデータ遮断の検知、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 condition

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

List of Test Requirements for Basic Test Cases (Draft)

A summary of the testing requirements for NIDS is provided below. This paper adds "detection of operations outside the specifications on the on-board NW" and "detection of effective control and diagnostic messages at timing inconsistent with the running condition" from the examples.

Major classification	Medium classification	Small classification
No false positives (False/Positive)	Prevent false positives	No detection of protocol errors in normal state, special operation, or less than a certain amount
Detect (True/Positive)	Detecting Unexpected Message Behavior	Detection of operations outside the specifications of the on-board NW (breach of car-specific specifications), detection of effective diagnostic message transmission at timing inconsistent with the running status, etc.
	Detecting Attacks on Network Protocols	Detection of attacks on CANs, OBD-II, UDSs, and CAN-FD, Ethernet, TCP/IP protocols
	Detection of known attacks	Detection of large-volume data transmissions, detection of large-volume data interruptions, detection of large-volume protocol errors, etc.
	Detecting Known Signatures	
	Detecting the Physical Connection of Illegal Equipment	

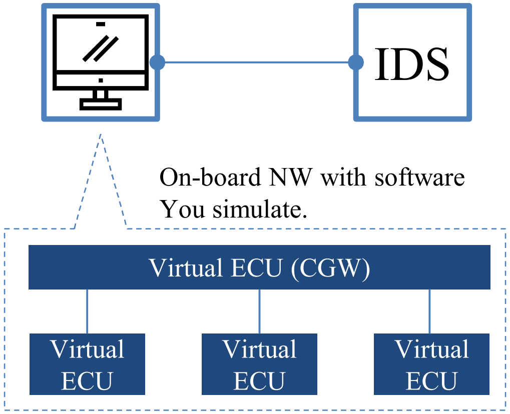
[Reference] IDS Test Environment Types and Considerations

The drafted IDS Fundamental Test Case runtime environment includes the following options:
In the future, the test case will be verified based on either or combination of these.

Simulated environment

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

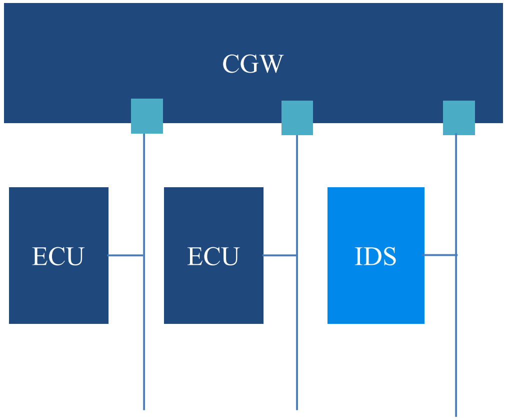
While simulating the on-board NW,
To meet testing requirements (attacks)
You enter a message in IDS.



On-board NW with software
You simulate.

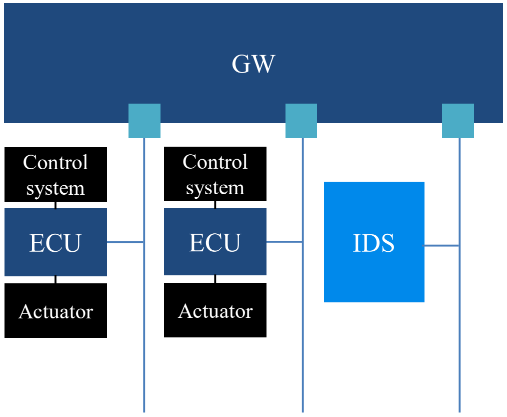
Test bed environment

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.



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

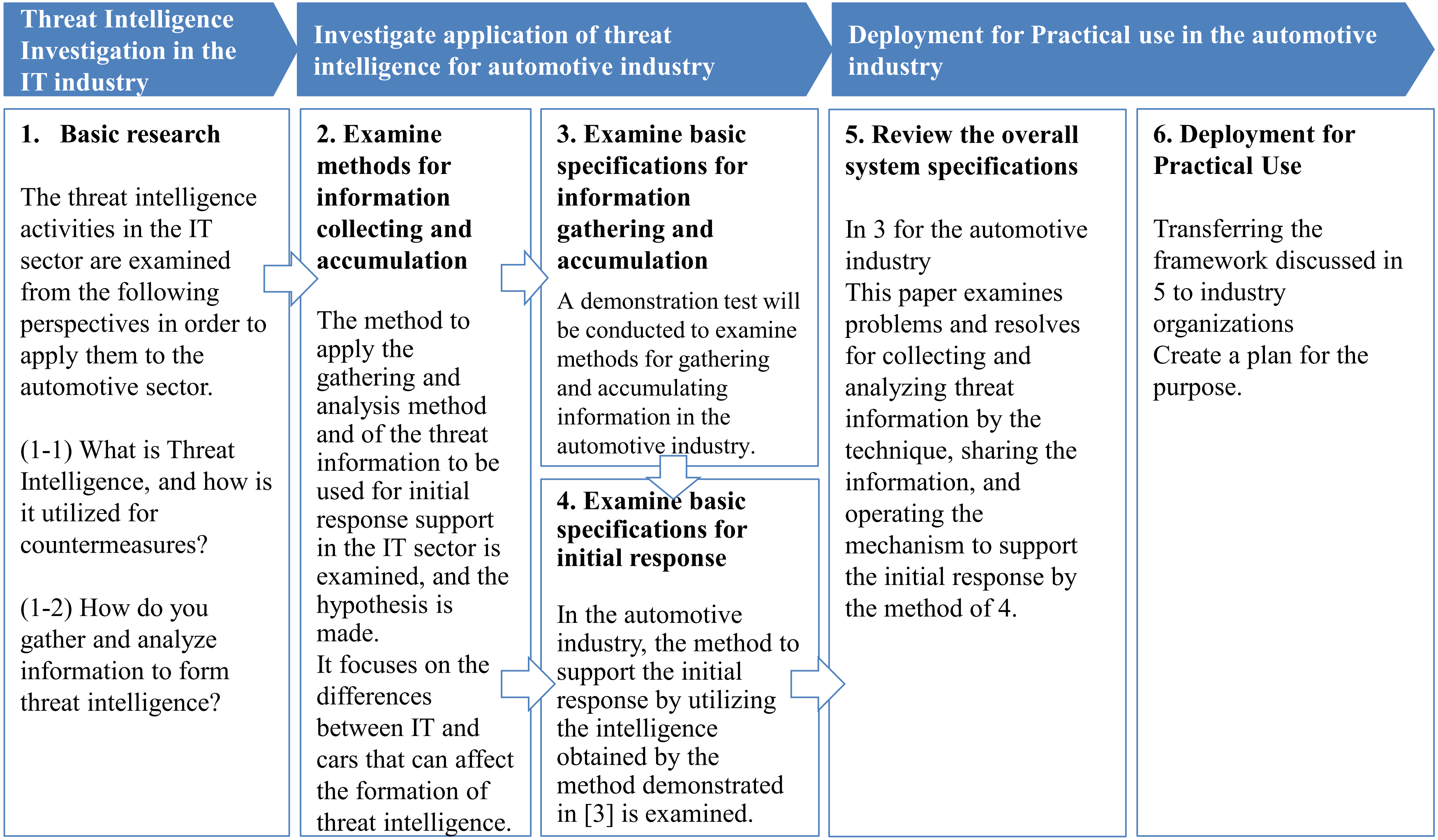
Research Objectives

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.

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.

Activity b Overall Schedule and Targets for Each Year

Target for each year will be determined to complete transfer of the output to the industry groups by the end of March 2023.

●⟶ : Working Period, ▼:Milestones (Fixed), ▽: Milestones (planned), Expected OUTPUT

FY2020			FY2021				FY2022				Expected output
7-9	10-12	1-3	4-6	7-9	10-12	1-3	4-6	7-9	10-12	1-3	
[1] Basic survey ●⟶	⟶	⟶									IT threats Intelligence
[2] Examine methods for information collecting and accumulation ●⟶	⟶	⟶	⟶								Hypothesis for information Gathering and analysis methodology
			[3] Examine basic specifications for information gathering and accumulation ●⟶	⟶							Test results Effectiveness of cyber-attack Capture and Gathering Methodology
					[4] Examine basic specifications for initial response ●⟶	⟶					Draft proposal for utilization of Threat intelligence for Initial Response support
						[5] Review the overall system specifications ●⟶	⟶	⟶			Draft operational design for the sharing of threat intelligence
									[6] Deployment for Practical Use ●⟶	⟶	Draft operation plan For threat intelligence sharing activities

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

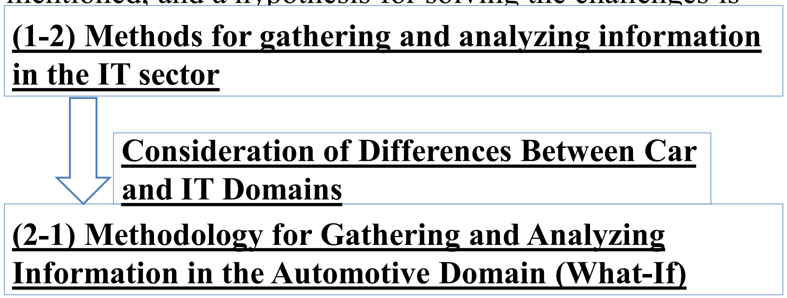
- IT threat intelligence activities

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



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

Consideration of Differences Between Car and IT Domains

(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

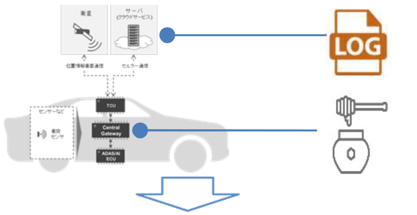
- **(2-1) Hypothesis on methods for gathering and analyzing information in the automotive sector**

Outline of Approach to Targets for Fiscal 2021

In fiscal 2021, demonstration tests will be conducted based on the assumptions created in the previous year. Consider the specifications of initial response support utilizing collected threat information.

3 Examine basic specifications for information gathering and accumulation

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



Analysis of implementation results and evaluation of effectiveness

INPUT

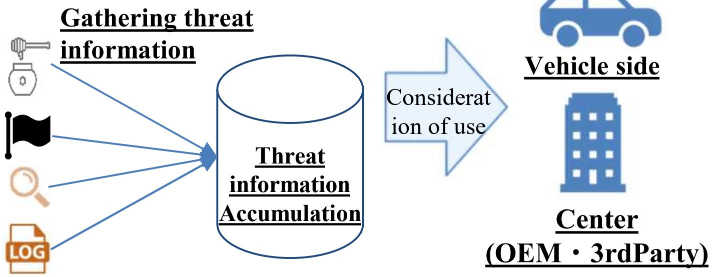
- Experimental Design for cyber-attack Capture and Gathering Methodology

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

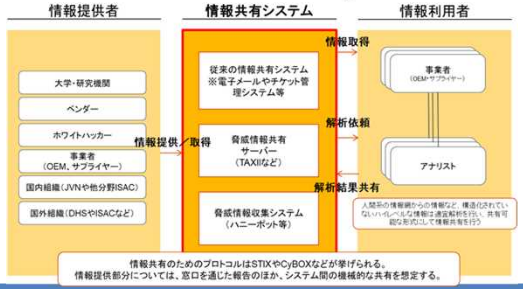
- **Draft use of threat information in response to initial responses in cars**

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.

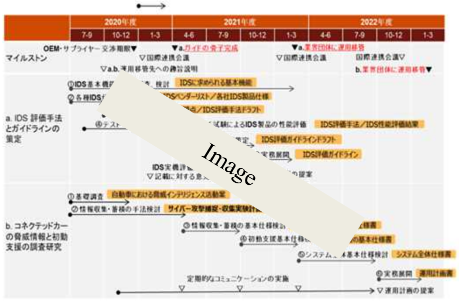

情報提供者
情報共有システム
情報利用者
大学・研究機関
ベンダー
ホワイトハッカー
事業者（OEM、サプライヤー）
国内組織（JVNや他分野ISAC）
国外組織（DHSやISACなど）
情報提供／取得
従来の情報共有システム ※電子メールやチケット管理システム等
脅威情報共有サーバー（TAXIIなど）
脅威情報収集システム（ハニーポット等）
情報取得
解析依頼
解析結果共有
事業者（OEM・サプライヤー）
アナリスト

人間系の情報網からの情報など、構造化されていないハイレベルな情報は適宜解析を行い、共有可能な形式にして情報共有を行う

情報共有のためのプロトコルはSTIXやCyBOXなどが挙げられる。
情報提供部分については、窓口を通じた報告のほか、システム間の機械的な共有を想定する。

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 Area
- Exchanging views with stakeholders

INTPUT

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

OUTPUT

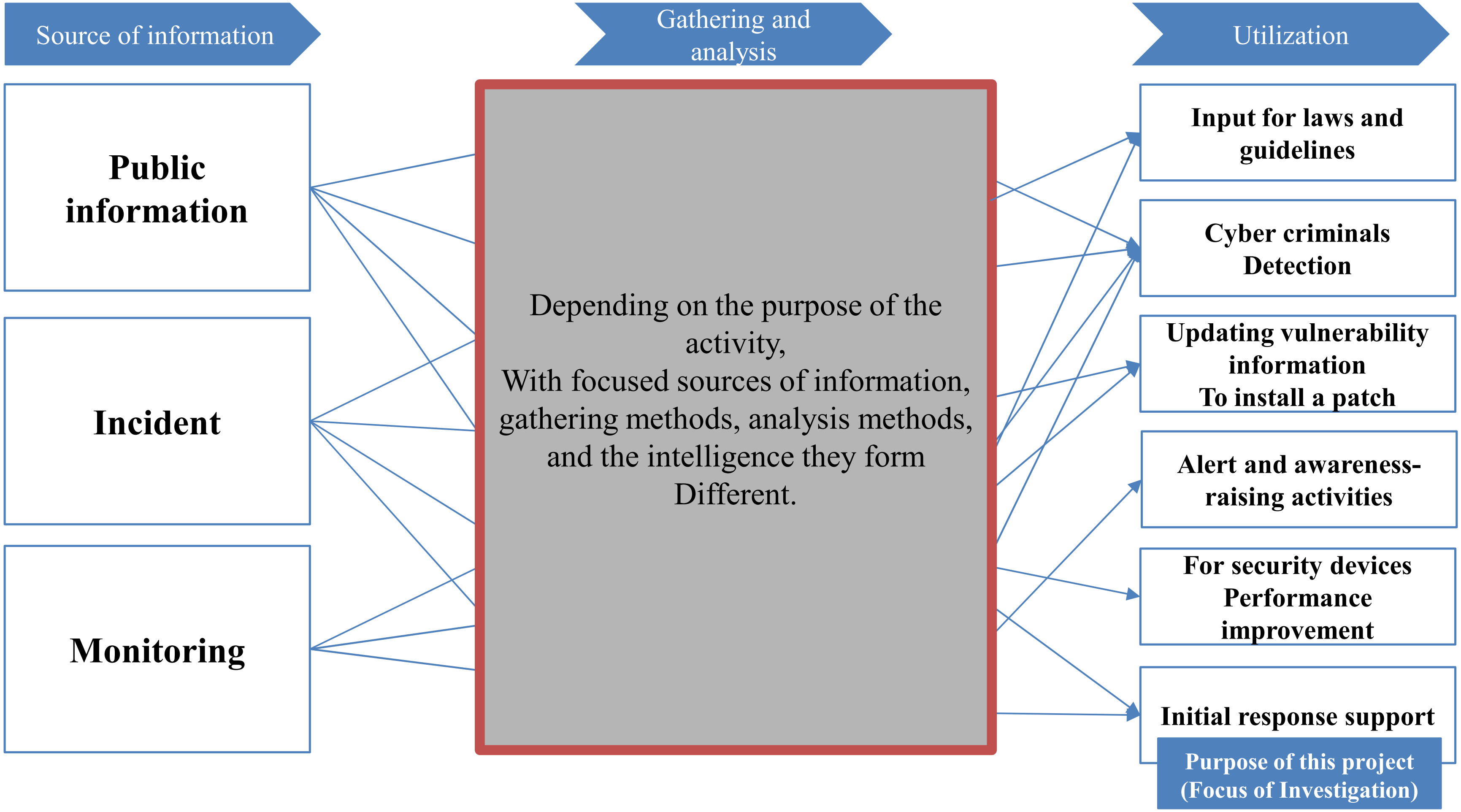
- **Draft operational design for the sharing of threat information on cars**

OUTPUT

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

Threat intelligence research directions

Threat intelligence activities in the IT sector are conducted for various purposes by organizations such as countries, industry groups, and private companies. This paper focuses on threat activities with the purpose similar to "initial response support" of this research, and investigates the information provided.



Source of information

Gathering and analysis

Utilization

Public information

Incident

Monitoring

Depending on the purpose of the activity,
With focused sources of information, gathering methods, analysis methods, and the intelligence they form
Different.

Input for laws and guidelines

Cyber criminals Detection

Updating vulnerability information To install a patch

Alert and awareness-raising activities

For security devices Performance improvement

Initial response support

Purpose of this project (Focus of Investigation)

Incident Response Using Threat Intelligence

Following are some examples of how the threat intelligence can be used to respond to incidents and how it can be used in various phases of NIST CSF.

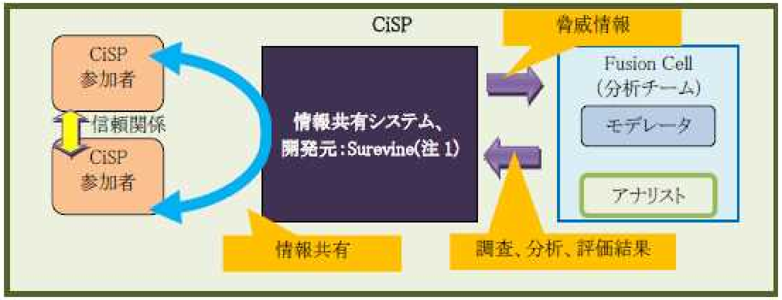
	Identification	Defense	Detection	Response and Recovery
①Indicator Specific events observed from cyber-attacks		Block used IP addresses, URLs, and domains in a blacklist in a cyber-attack.	Define and detect security events from events observed in a cyber-attack.	Verify traces of attacks such as IP addresses and hash values, judge whether they are cyber-attacks, and formulate responses and restorations.
②TTP (Tactics, Strategies, Procedures) An attacker's intention, behavior, and modus operandi are explained	Identify targetable information assets and systems and assess the impact of cyber-attacks.	Create attack scenarios and conduct response training.	Define behavior specific to TTP and detect suspicious behavior.	
③Security Alerts Vulnerability information and exploit information for the system	Assess vulnerability systems and their impact when they are exploited.	Apply a fix program to vulnerable systems.		
④Intelligence Report Document describing threat-related information that increases the status awareness of the organization	Identify threats related to your organization and assess their impact on your business.			
⑤Tool Configuration Setting of tools to support the use of information obtained from ①～ ④		In order to protect, detect, and recover from attacks, the security tool sets are defined from the information obtained from ① to ④ and delivered as a policy.		

Consideration on Threat Information Sharing Activity

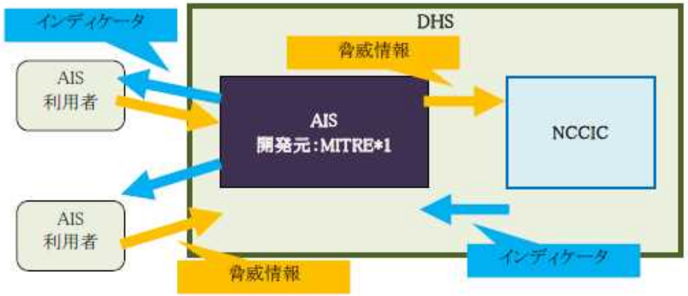
In some industries, common objectives are shared, such as preventing incidents from occurring and responding appropriately to initial responses, and shared threat information across companies.

Information sharing across industries

■Overview of CiSP (UK)

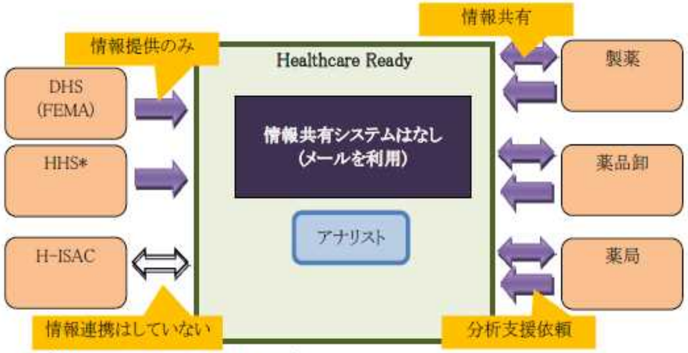


■Overview of DHS (US)



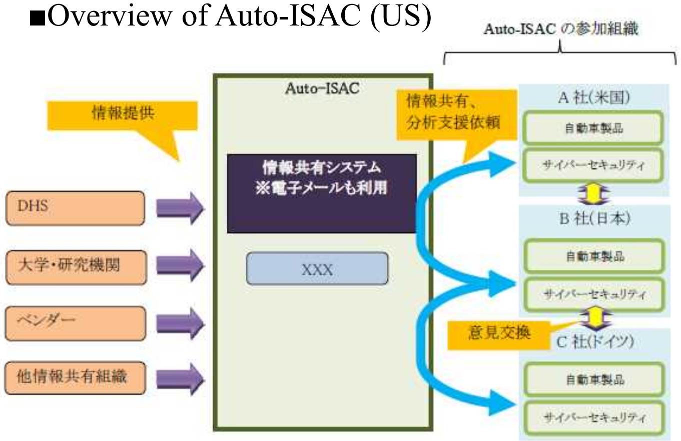
Sharing of information within the industry

■Overview of Healthcare Ready (US)



* (US National of Healthcare & human service)

■Overview of Auto-ISAC (US)



This project provides a mechanism to support the sharing of threat information across multiple companies and organizations.It is called an information sharing system.

Source: Strategic Innovation Creation Program (SIP) Securing Cyber Security in Critical Infrastructure (b2) Information Sharing Platform Technology "Information Sharing Design Guide Building", January 2020

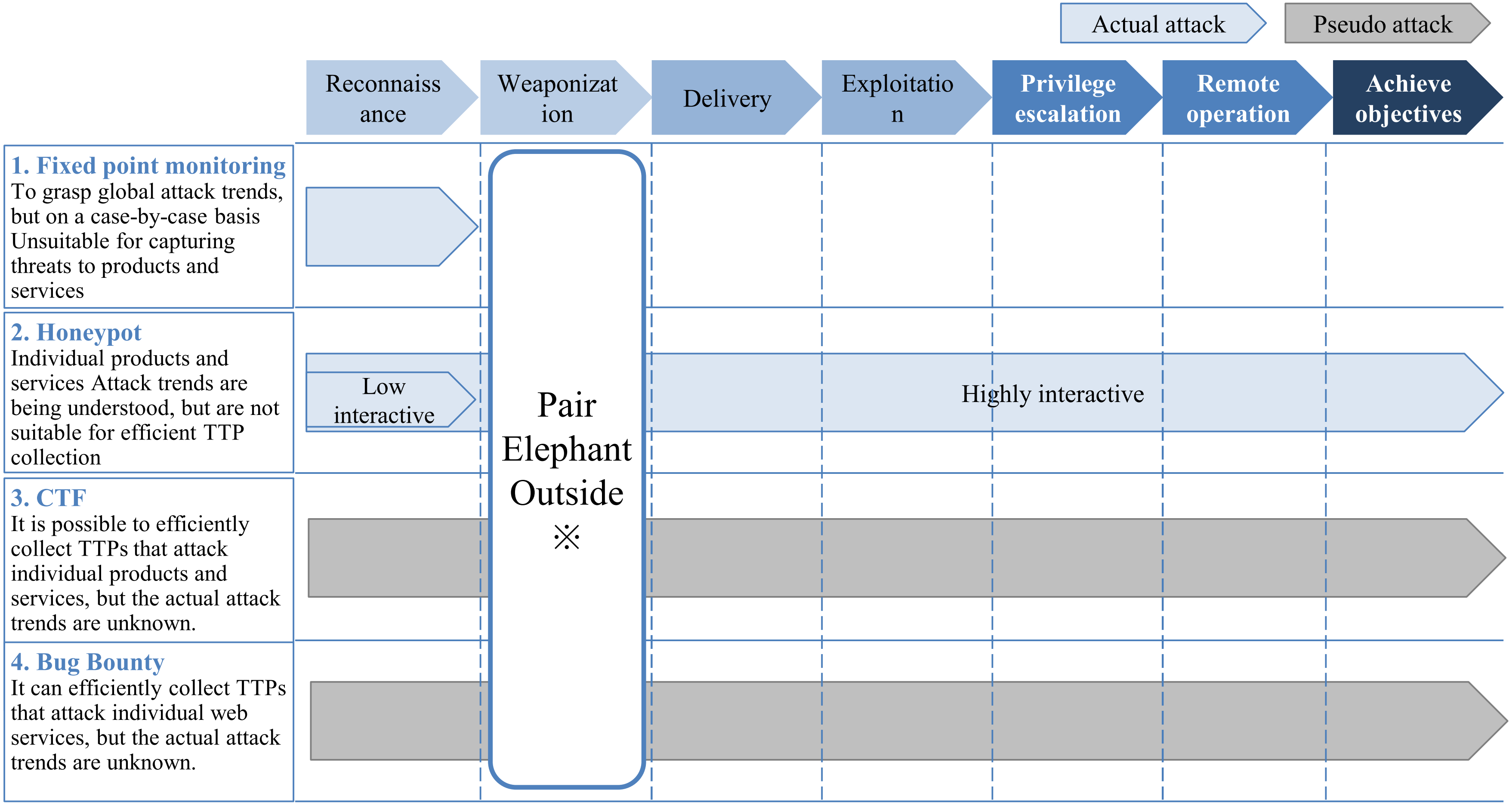
Threat Information Gathering Method in the IT sector

Threat information in the IT sector are mainly collected from the information sources such as public information, incidents, monitoring and experimentation. Following summarizes the outline of the collection technique and the viewpoint of data collection/analysis.

Methods	Overview	Examples
Internet Fixed point monitoring	A method of finding out the global trend of cyber-attacks by observing communications on the Internet at fixed points.	• NICTER(NICT) • TSUBAME(JP-CERT/CC)
Honeypot	A method of publishing a system intended to be attacked on the Internet and gathering attacker access information. It is sometimes used as a decoy that is subject to attack instead of protecting a real system.	• MITF (IIJ) • A IoT Malware Story(Kaspersky) • Connected Home Laboratory (Yokohama National University)
CTF	A way to get White Hacker to intentionally launch an attack and collect information in an environment that mimics the system. In addition to the (CTF) method of setting the objective (Flag) of the attack and contesting the score, there is also the method of providing a playground to test the pseudo-attack.	• DEFCON CTF • SECCON
Bugbounty program	A way to collect vulnerability information for actual systems in the filed by providing rewards to those who discover bugs.	• LINE's Bug Bounty Program • Servicing such as HackerOne and Sprout
OSINT	A method of gathering information from the Internet by hand or by mechanical means such as a web crawler or product or service. In addition to examples and reports, existing threats such as fake sites and fake apps may be discovered.	• (A large number of products and services are deployed).

Consideration of Threat Information Gathering Methodology

From the information collected by the above-mentioned method, the degree to which the attacker's modus can be captured was arranged along the cyberkill chain.



1. Fixed point monitoring
To grasp global attack trends, but on a case-by-case basis Unsuitable for capturing threats to products and services

2. Honeypot
Individual products and services Attack trends are being understood, but are not suitable for efficient TTP collection

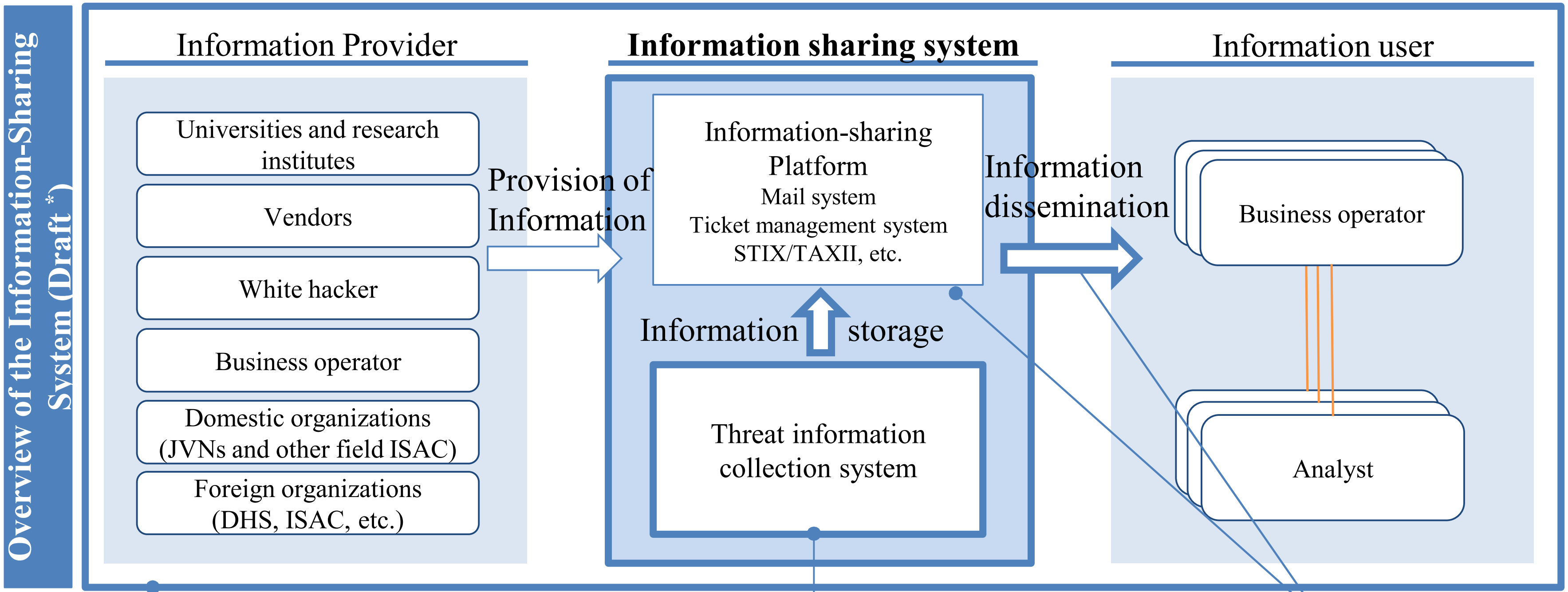
3. CTF
It is possible to efficiently collect TTPs that attack individual products and services, but the actual attack trends are unknown.

4. Bug Bounty
It can efficiently collect TTPs that attack individual web services, but the actual attack trends are unknown.

※ Since Weaponization refers to the process of developing malware and exploit kits, it cannot be supplemented by the methods 1-4 above.

Study on application of threat intelligence in the automotive sector

In the following phases ② to ⑤, a mechanism to support initial responses by collecting, analyzing, and accumulating information and sharing it with stakeholders was studied. Challenges to be examined in each phase were identified.



Overview of the Information-Sharing System (Draft *)

Information Provider

Universities and research institutes

Vendors

White hacker

Business operator

Domestic organizations (JVNs and other field ISAC)

Foreign organizations (DHS, ISAC, etc.)

Provision of Information

Information sharing system

Information-sharing Platform

Mail system

Ticket management system

STIX/TAXII, etc.

Information storage

Threat information collection system

Information dissemination

Information user

Business operator

Analyst

Challenge

How will the automotive industry build a mechanism for gathering threat information and providing initial response support? **(discussed in ⑤)**

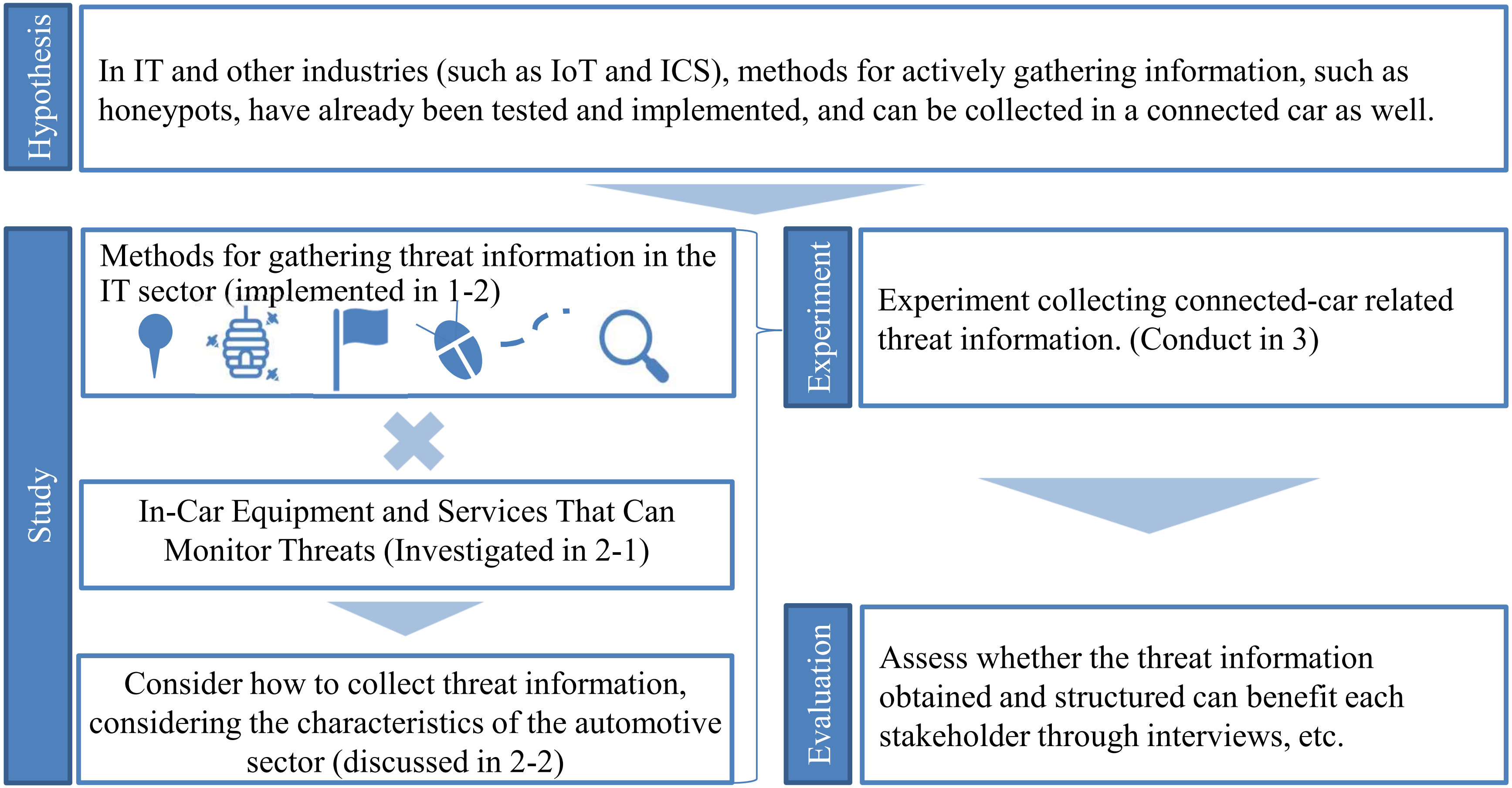
How to collect threat information for vehicles? **(Consider in ②③ basis on the results of the survey in 1-2.)**

How to accumulate and transmit collected information to support initial response? **(Consider in ④ basis on the results of the survey in 1-1.)**

(※) Draft based on the overview of UA Auto-ISAC. The overall picture of the Japanese automotive industry will be discussed in Phase ⑤.

Study on methods Information collection/accumulation

In this project, we will conduct a demonstration test on whether or not the threat information of the car can be collected by the gathering method as described above. In this phase, as the preparation, the on-board equipment in which the threat can be monitored was examined, as well as the applicable gathering technique.



Hypothesis

In IT and other industries (such as IoT and ICS), methods for actively gathering information, such as honeypots, have already been tested and implemented, and can be collected in a connected car as well.

Study

Methods for gathering threat information in the IT sector (implemented in 1-2)

In-Car Equipment and Services That Can Monitor Threats (Investigated in 2-1)

Consider how to collect threat information, considering the characteristics of the automotive sector (discussed in 2-2)

Experiment

Experiment collecting connected-car related threat information. (Conduct in 3)

Evaluation

Assess whether the threat information obtained and structured can benefit each stakeholder through interviews, etc.

Expectations for Threat Information Gathering Experiment

The purpose of the experiment is to evaluate whether it is applicable to collect threat information for vehicles and to establish preparation for practical application.

Background:

- Currently, actual cyber-attacks targeting vehicles are rare
- In addition, large-scale cyber-attacks targeting vehicles (so-called campaigns) have not been observed so far

Expectation for Threat Information Observation Experiment:

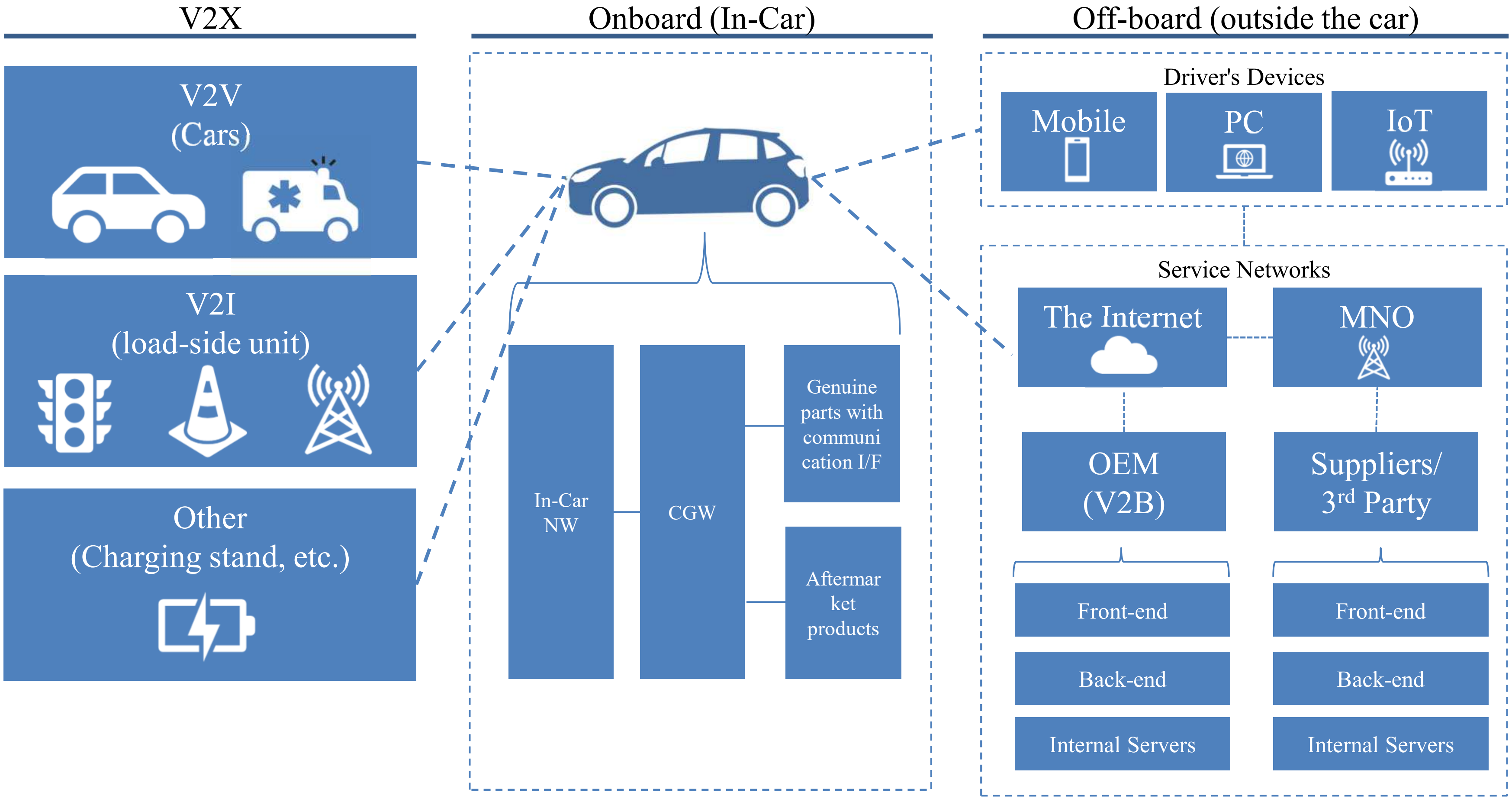
- Is there any car or in-vehicle device that can be accessed from the Internet in the first place?
- Are there cars or in-vehicle devices that are unintentionally exposed to the Internet?
- What methods are used by pseudo-attackers (CFT participants) to attack cars?
- How does an attacker attack a car?

Basic survey → **Examination of methods for collecting and accumulating information** → Collection/ accumulation of information Examining basic specifications

Investigating Services and Equipment exposed to threats

The following shows the market distribution volume of in-car equipment and the equipment which are expected to be realistic threats in the market, and examines the threat information gathering and storage technique of the vehicle based on the outcome of the basis research.

Research target(image)



Vehicle specific Characteristics- Attack Methodology

Differentiations in the attack method, difficulty of attack detection, frequency of attacks, and a suitable method for gathering information were identified in he categories shown on the previous slide.

Category	V2X	Onboard Area	Offboard Area
Communications protocols	RF/CAN, etc.	Vary BLE/Wi-Fi/ ZigBee/HTTPS/CAN	Mainly HTTPS
Attack method	Some social implements, such as DSSS and charging stations, are becoming increasingly popular, but there are many technologies in the demonstration stage and there are no specific threats.	For individual elements, there is some information in the IoT area, but there are not many car-specific information	Knowledge of attacks against general Web systems has already been collected
Attack detection difficulty	Need to consider a mechanism for detecting attacks	Need to consider a mechanism for detecting attacks	Can detect attacks on common products
Frequency of attacks	It is necessary to devise a way for an attacker to reach the target.	Attackers need to be devised to be able to reach the target	It can be accessed from the Internet, so the attack frequency is considered to be high. In addition, open OEM services are easily targeted for attack because they can be identified by DNS, etc.
Main challenge	• As part of the social infrastructure, it is necessary to collaborate not only with OEMs and suppliers, but also with infrastructure providers.	• Detection is difficult because it is a low-information attack method using a special protocol at present. • How to direct an attacker to the environment	• How to identify attacks against common web systems, especially those targeting telematics services • OEM collaboration is essential to observe attacks on existing services because the environment is maintained by OEM.

Hypothesis and Evaluation Policies for Threat Information Sharing in the automotive sector

Unlike IT systems, vehicles do not have common architecture for each OEM, so there is a high probability that a certain threat for a vehicle may not be applicable for another. On the other hand, analyzing the case may enable identifying threat that is commonly applicable.

Hypothesis

Vehicle control differs greatly from IT in terms of HW/SW and communication protocols depending on the type of vehicle, and other vehicles may not be exposed by a common threat in some cases when attention is paid only to cases of unauthorized vehicle control.

In general, **multiple attacks are combined to establish an attack case result in vehicle control.** (from case studies in FY 2019 and FY 2020 Activity a).

Therefore, **a case for certain vehicle may still be applicable for other vehicles.**

Research/Analyze

Image of Attack Case for a Vehicle (Method)

Decomposable by attacking flow (Tactics) and analyzing methods (Techniques)

Reconnaissance

- Known Vulnerability Investigations with Network Vulnerability Scans
- Unknown vulnerability investigation by fuzzing
- Firmware extraction (hardware hack, etc.)

Intrusion

- Logging in from I/F for Developers
- Insufficient strength password settings
- Get shell or promote authorities with known or zero-day vulnerabilities

Achieve Objectives

- Avoiding Authentication Processes During ECU Repro/Update
- Arbitrary control of the vehicle by input of an arbitrary CAN message

Evaluation

Assess whether the threat information analyzed can be used among multiple stakeholders rather than one OEM (assuming J-AUTO-ISAC as a point of contact).

Examining basic specifications for information gathering and accumulation

In collaboration with Yokohama National University, we have begun testing threat information gathering using Honeypot disguised as an aftermarket product. The honeypot was developed, and the observation experiment of the cyber-attack started in late January, 2021.

Current status

- Investigate in-vehicle products that can be identified by a wide area scan and development software that simulates the features of the product (as a result of the investigation, the product is not applicable to domestic products and is developed for products sold in the EU area)
- Subscribe to the cloud and obtain the IP address of the EU area. In response to a message received in the EU area by YNU, the transmission of product-specific commands has not been observed after operation. Only attacks that target IoT indiscriminately

Challenge

- Usually, the product is communicating using SIM, but because it cannot be contracted with EU carriers, it is unavoidable to operate in the cloud (there is a concern about the ability to collect attacks by operating in an IP address range that is different from the actual product group).

Future prospects

- Currently, the behavior of the product is reproduced by the software, but it will be replaced by the real product. In a honeypot using a real product, events on the host side are hard to observe, and events on the network side are mainly planned to be observed.
- cyber-attacks targeted at in-vehicle devices are not expected to be very popular, and there are various in-vehicle products. Because it is difficult to operate the honeypot for all in-vehicle products, it is considered to compile a framework for the operation of the honeypot with in-vehicle devices in the future.

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 kick off (Results/Future Prospects)

The outline of the research in Japan was introduced, and the proposal of the possibility of the collaboration was proposed for the following 3 themes.
Collaboration will be promoted by holding meetings in April 2021 and holding workshops in June of the same year.

#	Collaboration Candidate Name	Content
1	Vehicler attack database (Karlsruhe Institute of Technology)	• Taxonomy for establishing vehicle vulnerability database • The idea of taxonomy is helpful when analyzing threat-information observed and gathered by Honeypots and CTFs.
2	IDS management system(Autosar)	• A mechanism regarding threat information exchange among vehicle IDS and software update • It is possible to relate threat information gathering from the Japanese honeypot and threat collection from IDS in Germany.
3	IDS-vendor ESCRYPT	• Participated in #2 and may be able to collaborate on “Activity a. Development of IDS evaluation methods and guideline."

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