



METI

Ministry of Economy, Trade and Industry

OSS Security Initiatives

23rd August 2022

Cybersecurity Division

Ministry of Economy, Trade and Industry

10 Major Threats to Cybersecurity in 2022

Rank	Threats for Organizations
1	Damage caused by Ransomware
2	Confidential information theft by APT
3	Attacks exploiting supply chain weaknesses
4	Attacks on New Normal work styles such as remote-working
5	Information leakage by internal fraud
6	Increase of exploiting the released information of vulnerability countermeasures
7	Zero-day attacks
8	Financial loss by Business E-mail Compromise (BEC)
9	Business outages due to unexpected IT infrastructure failures
10	Damage by information leakage due to carelessness

<Source : Information-technology Promotion Agency, Japan (IPA) January 27, 2022 >

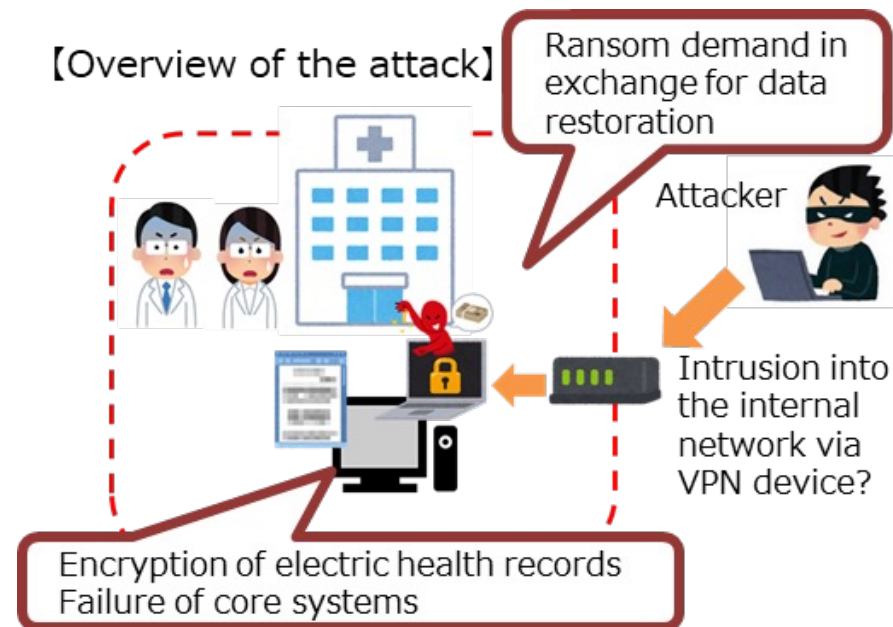
Overseas Case

- According to a U.S. specialized agency, **about 10% of cyberattacks on U.S. critical infrastructure providers affected ICSs.**
- In May 2021, the ransomware attack on a U.S. oil pipeline company resulted in **the suspension of its all pipelines** and the declaration of the state-of-emergency by the U.S. Department of Transportation.



Domestic Case

- At the end of October 2021, **a Japanese public hospital suffered ransomware attacks** and **it stopped accepting new patients** because its electric health records got encrypted and its core systems for medical fee calculations became not available.
- **The hospital didn't respond to the blackmail.** It restored the server on December 29, and resumed regular operation on January 4, 2022.



Surveys by the Osaka Chamber of Commerce

1. Results of network traffic analysis of SMEs systems (July 2019) Conducted with Kobe Uni. and Tokyo Marine Co.Ltd.

- Six months from Sept. 2018 - Jan. 2019
- Collected and analyzed communication data on networks at 30 SMEs
- **All 30 companies surveyed recorded suspicious communications that might be caused by cyber attacks.**
- At least 5 companies had infection with computer viruses or had information leak to outside.
 - Sophisticated attacks on **vulnerabilities** such as HeartBleed
 - Backdoor-type **malware** detected

2. Results of survey on cyber security measures of suppliers in the supply chain (May 2019)

- Feb. – Mar. 2018
- 118 large and midsize companies with over 100 employees via mail, fax, email, web & meeting to questionnaire
- **30 (25%) of the companies surveyed had experienced a cyber attack on a business partner that affected their company.**
- **"SMEs themselves should defend themselves"** said the **60%** of respondents

Cybersecurity policy directions

1. Policy deployment linked with industrial policies

- ① **Enhancing measures for CIIP**
 - Improving information sharing system, etc.
- ② **Enhancing measures for supply chain security as IoT development**
 - Promoting studies, R&Ds and demonstrations in the fields of industries such as defense, automotive, utilities, smart home and others
- ③ **Strengthening measures for SMEs**

2. International harmonization

- ① **Developing mutual recognition systems among Japan, the US and Europe**
- ② **Preventing spreads of unique rules that distort industry activities**

3. Support for creation of cybersecurity business

- ① **Exploring overseas markets of ICS security**
- ② **Introducing a service qualification system, utilizing government procurements**


4. Development of fundamentals

- ① **Raising security awareness of C-levels**
- ② **Capacity buildings at various levels**
- ③ **Dismissing underinvestments in cybersecurity**

Japan's Cybersecurity Strategy 2022 (Overview)

[https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022-gaiyou \(in Japanese\).pdf](https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022-gaiyou%20(in%20Japanese).pdf)

1. Major changes in circumstances surrounding cyberspace and the current situation

- Spread of the "new normal" triggered by the pandemic
 - Advancement of digital transformation (DX)
 - Growing cyber risks due to changes in international affairs
- 
- Various incidents occurring in Japan
 - ✓ Increasing damage caused by ransomware
 - ✓ Increasing damage caused by Emotet

2. Policy issues emerging in the wake of changing circumstances

- (1) **Prevention of incidents** to address growing threats in cyberspace
- (2) **Security enhancement and support for local companies, SMEs, etc. and strengthening measures against cyber crimes** to counter the spread of risks as a result of positioning cyberspace as a public space, and ensure the overall safety and security
- (3) **Strengthening international cooperation and collaboration** amid increasingly harsh national security environment

3. Measures of particular focus for ensuring "a free, fair and secure cyberspace"

- 1) **An all-Japan implementation framework for public-private collaboration (enhancement of national CERT/CSIRT functions)**
Increase information collection and analysis capabilities and strengthen information sharing systems between the public and private sectors to help prevent incidents
- 2) **Enhancement of cybersecurity in the private sector, including critical infrastructure operators**
Advance initiatives based on the "The Cybersecurity Policy for Critical Infrastructure Protection," ensure resilience of cyber infrastructure, etc.
- 3) **Cybersecurity measures tailored to the integration of cyberspace and physical space** *SBOM: software bill of materials
Advance initiatives designed to facilitate the adoption of software bill of materials (SBOM*) for managing vulnerabilities in software, etc.
- 4) **Cybersecurity measures by local companies and SMEs**
Raise awareness of business managers, promote activities of regional security communities (regional SECURITY) advancing local mutual-help initiatives, and promote "cybersecurity supporters services" for SMEs
- 5) **Advancement of public-private and international collaboration through the establishment of the Cyber Affairs Bureau and the National Cyber Unit**
Properly address the increasingly serious threats in cyberspace to ensure safety and security
- 6) **Advancement of capacity building support in the Indo-Pacific region**
Further advance capacity building support in the Indo-Pacific region through exercises, etc. for the government agencies of ASEAN member states

Realize "a free, fair and secure cyberspace" set forth in the Cybersecurity Strategy (approved by the Cabinet on September 28, 2021)

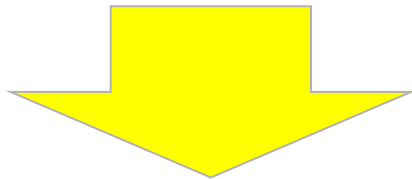
Initiatives in QUAD

May 2002, “The Quad Cybersecurity Partnership” launched at the Quad Summit

“Quad Cybersecurity Partnership: Joint Principles”

Cooperate in the following fields ;

- Critical infrastructure cybersecurity
- Supply chain risk management
- **Software security**
- Capacity building



Regarding software security, following cooperation will be taken;

- To ensure the implementation of baseline standards for software security domestically and internationally, and to promote harmonization
- To jointly align the development of a software security framework in government software procurement

Study Group on Industrial Cybersecurity

Members

As of Apr, 2022

Izumisawa, Seiji

-President & CEO, Mitsubishi Heavy Industries, Ltd.

Endo, Nobuhiro

-Chairman of the Board, NEC Corporation

-Chairman, Committee on Cyber Security, Keidanren

Obayashi, Takeo

-Chairman, Japan Users Association of Information Systems

-Chairman of the Board, Obayashi Corporation

Sakurada, Kengo

-Chairman, Japan Association of Corporate Executives

-Group CEO, President and Representative Executive Officer, SOMPO Holdings

Shinohara, Hiromichi

-Chairman & CEO, Nippon Telegraph and Telephone Corporation

Higashihara, Toshiaki

-Chairman & CEO, Hitachi, Ltd.

Funabashi, Yoichi

-Co-founder and Chairman, Asia Pacific Initiative

Murai, Jun (Chair)

-Professor, Keio University

Watanabe, Yoshihide

-Special Advisor, the Japan Chamber of Commerce and Industry

-Chairman and CEO, Osaki Electric Co., Ltd.

Observers

NISC, NPA, FSA, MIC, MOFA, MEXT, MHLW, MAFF, MLIT, MOD, Digital Agency

WG 1 (Rules, Technology, Standards)

1. Supply chain security package

WG 2 (Mgmt, HRs, International strategy)

2. Cybersecurity management package

3. Human resource development and awareness raising package

WG 3 (Cybersecurity business)

4. Business ecosystem creation package



Guiding principles for accelerating industrial cybersecurity

1. Leading 『Global』

2. Creating 『Value of Trust』 ~Proven in Japan~

3. Expanding to 『SMEs & Local』

Message to industry sector on cybersecurity measures

《Study Group on Industrial Cybersecurity, 11 Apr. 2022》

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20220411 (in Japanese).pdf

- Recent increases of damages by cyberattacks such as ransomware and Emotet
- Companies and organizations are requested to strengthen measures and response appropriately by taking the following measures under the leadership of C-levels

1. Thoroughly implement cybersecurity measures and establish sustainable system.
2. Timely report, consult and respond in case infection is confirmed.
3. Utilize cybersecurity services for SMEs, such as “Cybersecurity Supporters Service”
4. Have responsibilities for security of products/services in IT services

- Implement security measures for products and services in order to protect the information assets and privacy of their customers. Take measures such as contacting their customers in case serious vulnerabilities of products and services are announced.
- Develop software in an environment that can only be used by authorized developers.
- Check known and potential vulnerabilities during the development process and before shipping by conducting source code reviews and using error checking tools. Check the providing community, bugs, security-related information and support information related to the open source software used.

The Cyber Physical Security Framework (CPSF) ~for value creation process in Society5.0's supply-chain ~

https://www.meti.go.jp/english/press/2019/0418_001.html

- “**Society 5.0**”, where cyber and physical spaces are highly integrated, **enables rather dynamic and flexible creation of supply chain** while facing and coping with **new risks** as followings:

Distribution/linkage of large amounts of data in cyberspace

⇒ **Increased importance of managing data according to its nature**

Convergence of Physical and Cyber Space

⇒ **Cyber-attacks reach physical space**

Complex inter-company supply chains

⇒ **Increased scope of impacts**

- **Published “Cyber-Physical Security Framework (CPSF) Ver1.0” on 18 April 2019**
 - ✓ Drew the overall picture of security measures against new risks in "Society 5.0"
 - ✓ Compile examples of security measures that can be utilized for industrial countermeasures

Industry sector specifications & cross-sectoral studies

- Established seven industry-specific sub working groups (SWG), and developing CPSF based security guidelines.
- Established three cross-sectoral task-forces (TF) for common challenges.

Study Group on Industrial Cybersecurity WG 1

Standard Model (CPSF)

Industry by Industry discussion

Building SWG

- Developed a guideline ver. 1.0

Electric Utility SWG

- Developed a guideline

Defense SWG

- Revising the existing guideline

Automotive SWG

- Developed a guideline ver. 2.0

Smart Home SWG

- Developed a guideline ver. 1.0

Space Industry SWG

- Launched in January 2021

Factory SWG

- Launched in January 2022

...

Cross-sectoral SWG

『3rd layer』 TF : TF for ensuring the trustworthiness of 『Connection in cyber space』

- Developed “**Data Management Framework for collaborative data utilization**” (April 8, 2022)

Software TF : TF for software management to ensure cyber-physical-security

- Developed a **practice collection for OSS management** (April 2021)
- Conducting proof of concept for promoting the use of SBOM

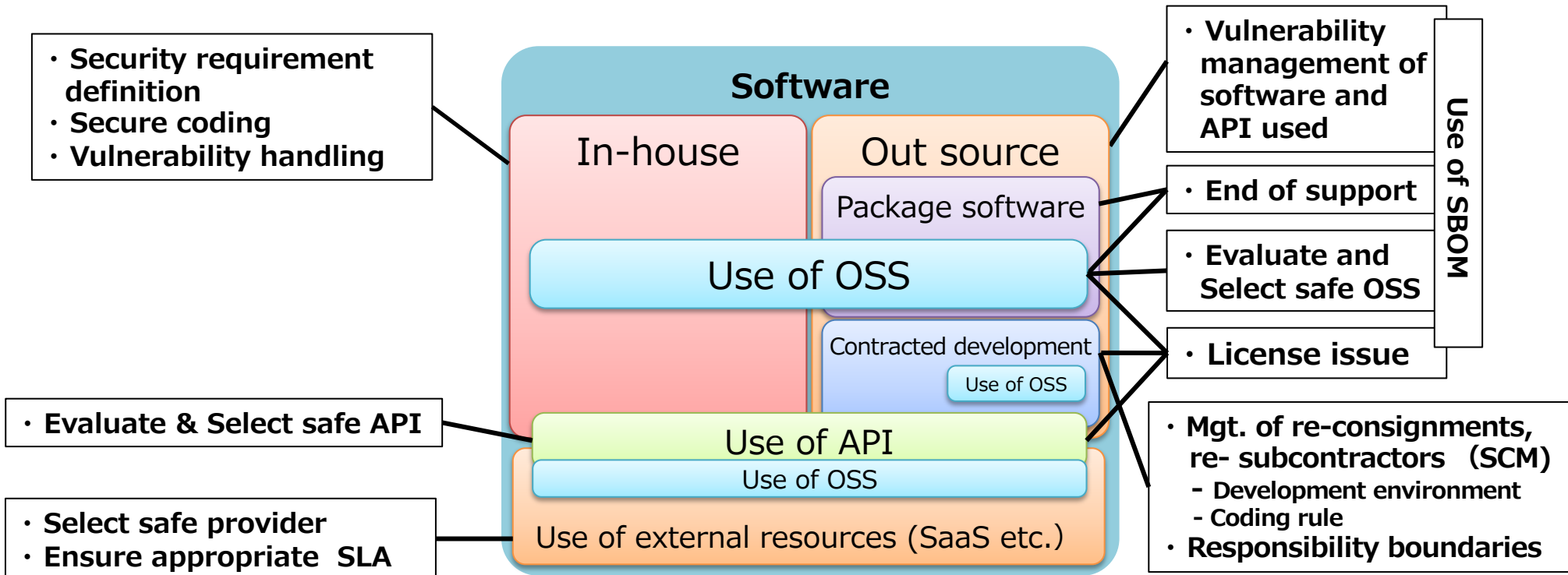
『2nd layer』 TF : TF for ensuring the trustworthiness of 『Connection between cyber and physical』

- Developed “**IoT Security Safety Framework**” for ensuring the trustworthiness between cyber space and physical space
- Collecting use cases of this framework for easy to use

[Software TF] Requirements for Software Management

- Increased reliance on software technologies including OSS, such as advances in virtualization technologies. Increased importance of software management methods, vulnerability handling and license support.
- In 2018, the U.S. NTIA advocates “Software Component Transparency”. It promotes discussion on the utilization of the SBoM, which is a software component composition table.
- This TF discusses appropriate management methods, vulnerability handling and license support for software (especially OSS).

Illustration of issues concerning software



Practices collection for OSS management

- Promote appropriate OSS use considering points
 - ✓ Points to be considered when companies use OSS
 - ✓ Reference cases for each point through individual company hearings, etc.
 - ✓ Promotion of OSS use by removing barriers to the use of OSS by companies
 - ✓ Improvement of industrial competitiveness getting the benefits of OSS use

OSS issues (ex.)

License management

Vulnerability handling

Supply chain management

In-house structure for OSS use

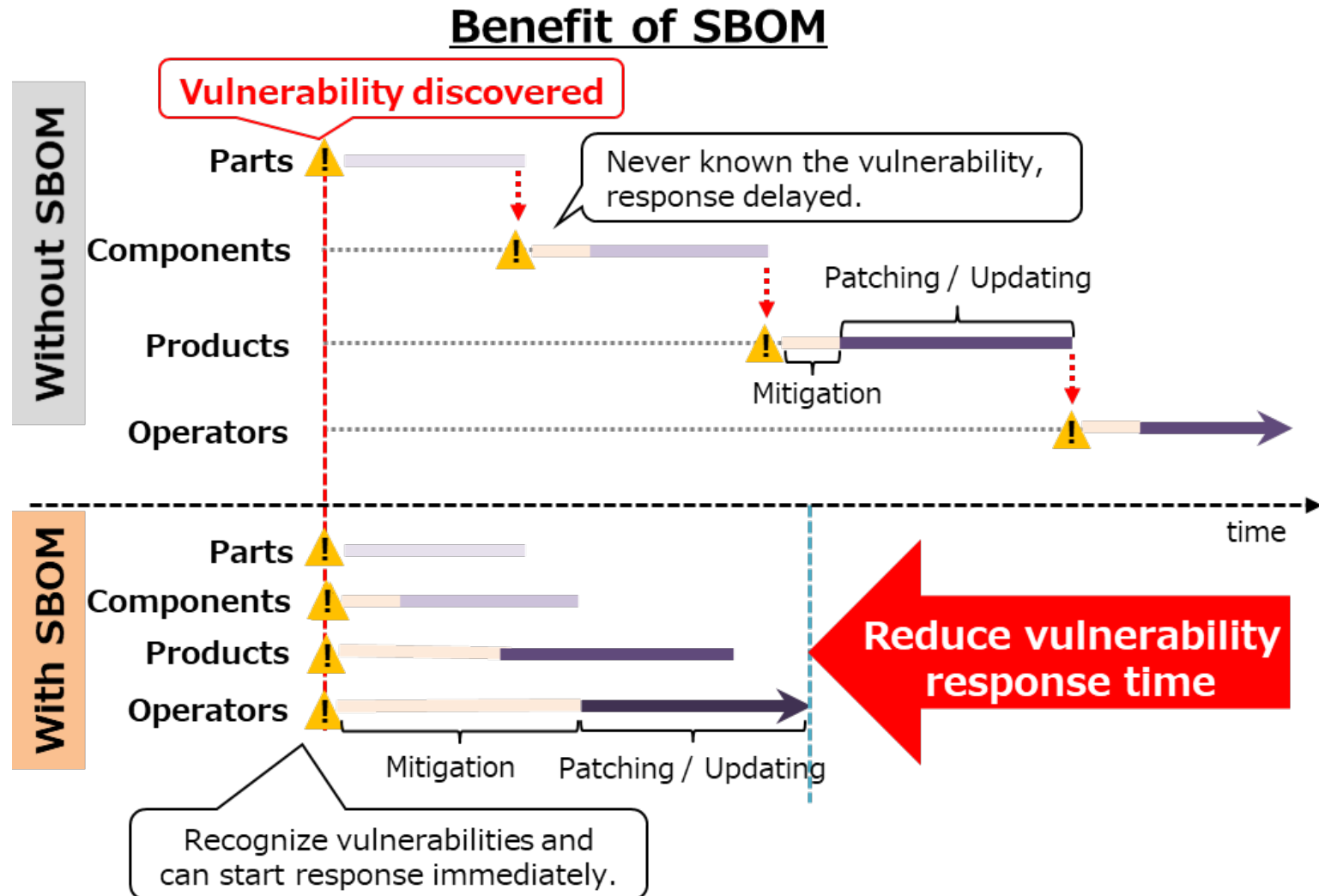
OSS community activities

Sample of good practices in the Practices collection

- Create SBOM using scanning tools
- Conduct sure risk management for vulnerabilities, licenses, etc.
- Establish a system to register/use OSS confirmed as safe, and to create a radar chart of evaluation results to select good OSS
- Provide written confirmation when suppliers deliver parts & software
- Promote understanding among suppliers by dispatching information through OpenChain Japan WG
- Agree with customers in advance on the risk of end-of-life support, costs associated with vulnerability management for long-term use and update support
- Establish company-wide rules for the process of OSS use, and execute by top-down instructions
- Increase projects using OSS for highly effective results
- Allow employees to develop OSS during working time
- Convert in-house developing software to OSS for improving performance through the OSS community-based development

Efforts related to SBOM

- Software Bill of Materials (SBOM) is a list of software components.
- METI has been conducting proof-of-concept projects considering the industrial structure and business practices in Japan.



Challenges in Introducing and Utilizing SBOM

- While the benefits of using SBOM are expected, **implementation of SBOM has not progressed in Japan as a whole due to barriers such as the cost of introduction.**
- In our PoC, METI will try to **find the good way to utilize SBOM for increasing the effectiveness by its introduction, and the one to lead its widespread use.**

- **Cost of SBOM implementation**

- Not enough information to decide the budget against the effective SBOM
- Manual management of a large number of SBOM would result in huge costs, so automation tools for component management is considered, but the following issues exist
 - ✓ New costs to implement and manage SBOM such as tool installation and its running
 - ✓ Lack of uniformity in software IDs and SBOM formats

- **Strong resistance by suppliers to SBOM preparation and information disclosure**

Details of the SBOM PoC Project for FY2021

Set up conditions for SBOM preparation means, preparers, etc., and compare effectiveness and costs, and organize future considerations.

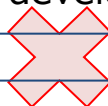
Items for comparison

● Benefit of SBOM

- Vulnerability Management: Man-hours for identification, Remediation time, Residual risk reduction
- License Management: Man-hours for identification, Residual risk reduction of license violations

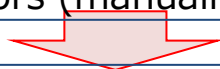
● Cost of SBOM

- Initial cost Organization building, tool environment building
- SBOM generation cost Man-hours for generation, Tool purchase or development
- SBOM utilization cost Man-hours for management(identification of the effect of vulnerabilities), Tool purchase or development



Conditions for comparison

- In the case of no efforts of software component management
- In the case of software components management other than SBOM
- In the case of generating SBOM by users
- In the case of generating SBOM by vendors (manually or automatically)

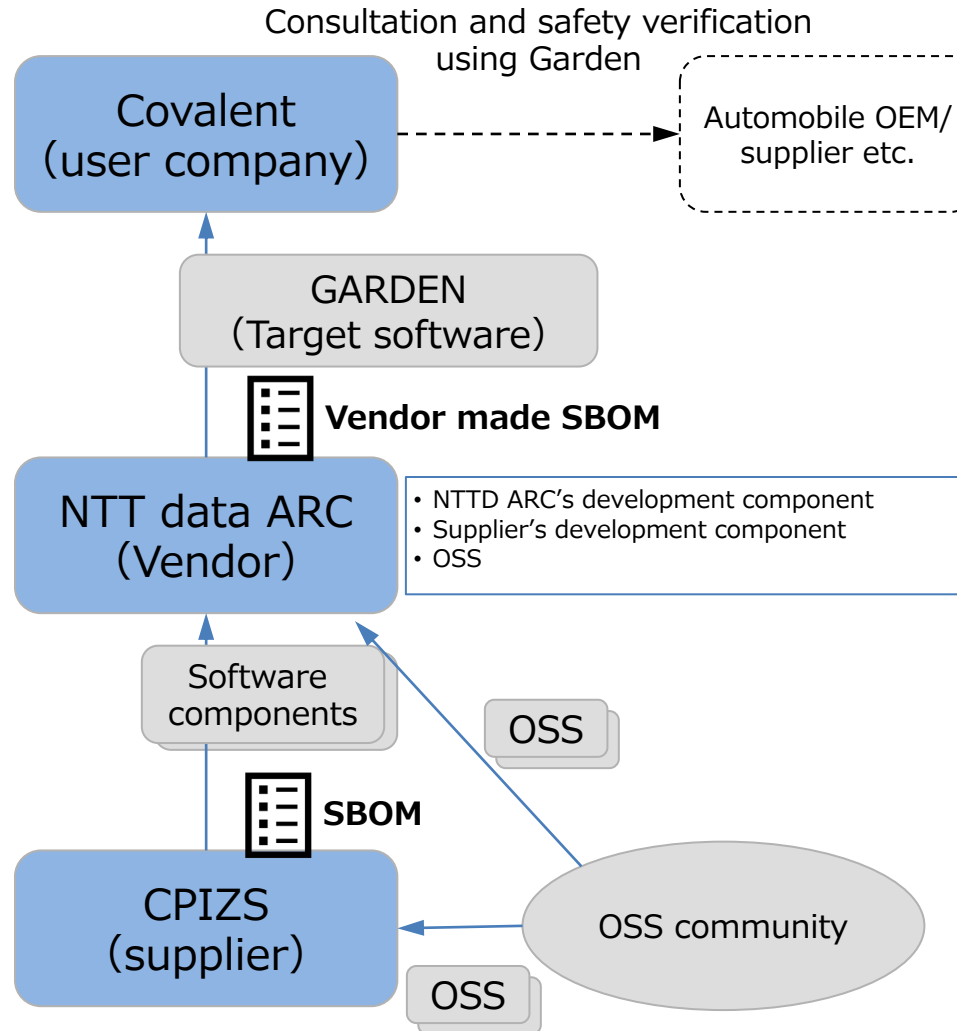


- Calculate the actual benefits and costs of SBOM through the PoC project
- Examine effective ways to utilize SBOM and organize future considerations as considering the progress of initiatives in other countries

The Software used for the PoC “GARDEN”

Name	GARDEN Scenario Platform
Vendor	NTT DATA Automobiligence Research Center, Ltd. (NTT Data ARC)
Software Overview	<ul style="list-style-type: none">• <u>Verification platform software for automated driving system development.</u>• <u>Provides a scenario generation function for functional operation simulation for safety evaluation</u> of automated driving software.<ul style="list-style-type: none">➤ Modeling, driving data classification, trajectory extraction road editing, scenario combination testing, and scenario execution• The source code is available to the public as open source.

Structure of the Supply-chain of “Garden”



Comparative cases in our SBOM PoC

- We have been **evaluating the cost & benefit of SBOM in comparative cases**, compared Non SBOM format (Vender-Specific) with using SBOM format.
- **We selected the tools from the list provided by the SPDX project※¹ and NTIA Formats and Tooling WG※²**, as it is considered to be highly compliant with the SBOM standard. We also **compared free tool and commercial tool** considering the promoting SBOM to SMEs.

Senario	Component list generation	Vuln. Identification	License info. Identification
① Non SBOM format (Vender-Specific)	Generated non SBOM format component list manually.	Evaluated searching vuln. Info. in NVD,etc. manually.	Evaluated searching license info. Manually.
②SBOM & Manual process	Generated SBOM manually.	Identified Vuln. info by automatic tool “Grype”.	Identified license info. by the tool “FOSSology”.
③SBOM & Automated tool (free tool)	SBOM generation by “Scancode-Toolkit”, “Syft”, “FOSSology” etc.		
④SBOM & Automated tool (commercial tool)	Generated SBOM, Identified Vuln. info and Identified license info. Seamlessly by the commercial tool “Black Duck”. User company Generated SBOM by the commercial tool “Black Duck” from Python virtual environment (contained source code, component file and OSS required for execution) vender provided.		

In this project, the definition of SBOM adopts the NTIA definition of "a formal record containing the details and supply chain relationships of various components used in building software. ", and it is distinguished from a specific record containing component list not premised on sharing between other companies.

※1 : <https://spdx.dev/spdx-tools/>

※2 : https://ntia.gov/files/ntia/publications/ntia_sbom_tooling_2021-q2-checkpoint.pdf

Results of SBOM PoC demonstration

Benefits of SBOM

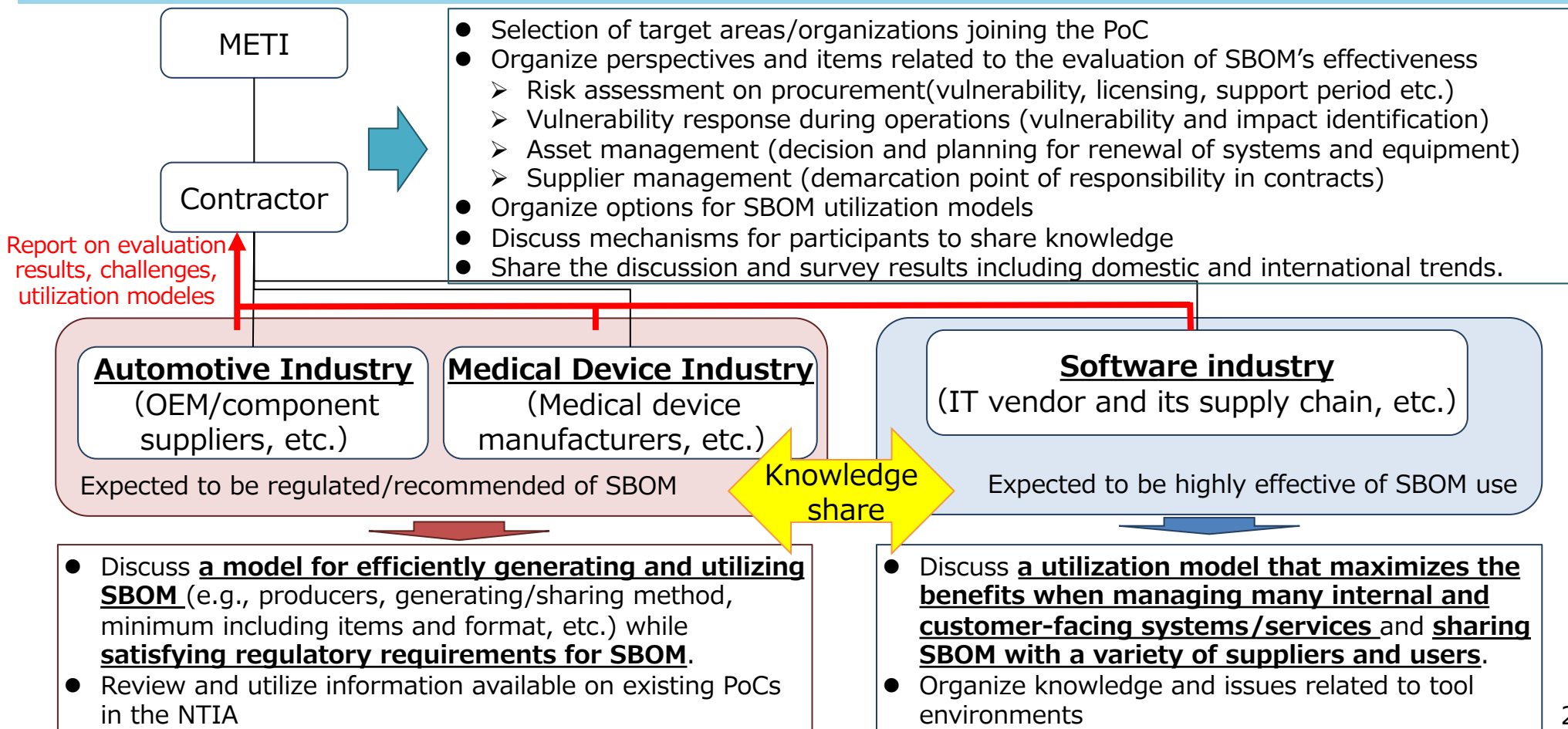
- Compared to conventional manual components management, **the use of tools has reduced the man-hours required for operations (SBOM generation and utilization).**
 - Confirmed that **SBOM using free OSS tools is less expensive than conventional manual components management when the number of components is 355 or more**, based on the effect of reducing the man-hours for vulnerability handling and license management per component.
 - In this PoC, **the tool-based SBOM was confirmed to be cost effective under the following conditions.**
 - ✓ 1 : Initial man-hours and costs for the SBOM tool are low enough.
 - ✓ 2 : Accuracy of tool-generated SBOMs is comparable to manual components management.
 - ✓ 3 : Components reused from third-party OSS components are NOT covered by SBOM.
※ if the conditions above are not met, SBOM does not always lead to cost reduction.
- **Shorten the lead time from vulnerability announcement to identification** in software by using SBOM (In case of manual work, it depends on frequency of vulnerability identification.)
- Paid tools can **detect reuse of other OSS in certain OSS by analyzing OSS dependencies.**
- **Linking SBOM tools with existing configuration management tools may reduce the man-hours required to identify the magnitude of vulnerability impact.**

Issues identified

- **Initial man-hours required for SBOM introduction**
(e.g., tool introduction and other environmental improvements, learning how to use the tool, etc.).
- **Free tools lack manuals and know-how and are not sufficient in terms of functionality and accuracy**, such as inability to detect reused components, limited readable SBOM formats, and license detection failures.
 - Expected **the improvement of the accuracy and functionality of the tools themselves**, as well as **the development of Japanese-language documents that organize know-how to use the tools, points to keep in mind**, etc.
- **SBOM, which is generated by non-developers, increase the man-hours or make it difficult to examine the accuracy of SBOM** such as OSS reuse and source code modified components.
- **Management responsibility may become ambiguous** when components are detected that the developers themselves are not aware of.
 - **If developers (vendors and suppliers) themselves identify software components and share them in a standard SBOM format, it will lead to more efficient component management and clarification of responsibilities throughout the supply chain.**

Details and structure of the PoC in FY2022

- Select companies participating in the PoC and design its content based on "areas expected to be regulated or recommended" and "areas expected to be highly effective" as candidates of industry sector of SBOM use.
- Share the results of the PoC and the industry's know-how of SBOM use, and discuss actual utilization methods.



Upcoming Schedule

	Apr.2022~Mar.2023	Apr.2023~Mar.2024	Apr.2024~Mar.2025
①evaluation of costs and benefits and discussion of issues through PoC	Select target and implement PoC → linked	Implement PoC (necessity and target areas to be considered) -----→	
②Discuss effective utilization models for SBOM	Discuss utilization models from PoC results → applied	Discuss methods and processes to agree utilization models → linked	Discuss other areas -----→
③Consideration of transaction deals for SBOM sharing	linked Organize issues →	Discuss transaction agreement models sector by sector →	Discuss other areas, Utilize the PoC results -----→
④Know-how sharing on SBOM	Develop guiding documents →	Promote and update the documents -----→	
⑤Technical considerations for SBOM automation and sharing	Identify technical challenges →	Plan and discuss initiatives to support efforts solving the technical challenges →	Implement the initiatives →
⑥Institutional harmonization with other countries	Organize cooperation items → Plan & discuss initiatives →	Implement initiatives → Share the PoC results, etc.(at timely manner) →	