Security Transparency Consortium

Achievements

Visualization Data Utilization to Ensure Security Transparency

-Vulnerability Management Edition-

October 21, 2024

Security Transparency Consortium

Table of Contents

1 Introduction

1.1 Background

As products, systems, and services become more sophisticated, supply chains become more complex, deeper, and wider. As a result, security risks that arise in the supply chain are easily overlooked. Risks in the supply chain are difficult to properly capture and assess, and supply chain security risk measures have become a critical management issue for all businesses participating in supply chains.

To address this issue, efforts to improve transparency of security in products, etc., are attracting attention.[1] In Europe and the U.S., there is a growing movement to require each business operator in a supply chain to create and provide "Visualization Data" on the software configuration of products, etc., in the SBOM format (a standard data format for listing software components). Against this backdrop, the Ministry of Economy, Trade and Industry (METI) in Japan published "Guidance on Introduction of Software Bill of Materials (SBOM) for Software Management ver 2.0"[2] ("Introduction Guidance") on August 29, 2024, and is working to promote the introduction of SBOM.

1.2 Activity Vision of the Consortium

Product suppliers, etc., typically play the role of "creators" of Visualization Data through SBOM, etc. However, for this purpose, Visualization Data needs to be effectively utilized at a level commensurate with the cost of creating and providing Visualization Data. Conversely, the clearer the effective use of Visualization Data by the "users" of Visualization Data (e.g., service providers), the more they will be encouraged to create and provide more Visualization Data, leading to a virtuous cycle of increased use.

In addition, not only the security division but also the divisions involved in the procurement of target products, business owners, and other related parties must be involved from their respective standpoints when considering how to utilize Visualization Data, and the entire organization as a whole must work in a unified manner. Since the supply chain affects the entire organization in various ways, issues need to be dealt

---

[1] NTT Technology Journal, September 2024, Feature Article, " Reducing Security Risks in Supply Chains by Improving and Utilizing Security Transparency" https://journal.ntt.co.jp/article/29301

[2] A Guide to Implementing the Software Bill of Materials (SBOM) for Software Management ver 2.0, https://www.meti.go.jp/press/2024/08/20240829001/20240829001-1r.pdf

with from various viewpoints with awareness of the problems and issues, which will lead to the development of a wide range of valuable utilization methods for Visualization Data.

In February 2024, the Consortium published its activity vision[3], which sets forth the activity policy of the Consortium toward the realization of measures to deal with the issues and issues faced by the users of Visualization Data on the basis of the above approach.

1.3 Purpose of this Document

This document summarizes the results (knowledge) of joint studies conducted by member companies on the basis of the above-mentioned activity vision, and particularly targets "scenes where Visualization Data such as SBOM is utilized in vulnerability management."

On the basis of the activity vision, the Consortium will continue to work on expanding the number of participating businesses that are not bound to a specific business or industry and materialize more attractive ways of utilizing Visualization Data.

1.4 Structure of this Document

Chapter 1 describes the background and objectives of this document. Chapter 2 describes the value that can be brought to each actor by utilizing Visualization Data for vulnerability management. Chapter 3 presents an analysis of knowledge useful for vulnerability management in response to the eight problems and issues raised in the activity vision. Chapter 4 describes the specific implementation of each type of knowledge.

1.5 (Reference) Relationship between this Document and the "Introduction Guide" Issued by the Ministry of Economy, Trade and Industry

The Introduction Guide formulated by METI provides a framework for software suppliers to consider the benefits of SBOM, points to be recognized and implemented in the actual implementation, and the appropriate scope of SBOM implementation in consideration of the benefits and costs of SBOM implementation. This document also provides a broad overview of the matters (requirements, responsibilities, cost burdens,

[3] Security Transparency Consortium Activity Vision "Improving and Utilizing Security Transparency" https://www.st-consortium.org/?page_id=1066

rights, etc.) that should be stipulated for SBOM in contracts and other agreements with contractors.

In addition, the "Embodiment of Vulnerability Management Processes," which is a set of specific procedures and concepts for effectively utilizing SBOM in a series of processes to manage software vulnerabilities, is included for vulnerability management operations and in this document, to provide an overall picture of vulnerability management using SBOM. The "Embodiment of the Vulnerability Management Process" outlines specific procedures and concepts for effectively utilizing SBOM.

As mentioned above, this document also targets situations where Visualization Data is used for vulnerability management. Therefore, this document was prepared with reference to the Introduction Guide and reviewed so that both documents can be utilized complementarily in vulnerability management practice.

2 The Value of Using Visualization Data in Vulnerability Management

Products, systems, and services are provided through diverse software supply chains, and there are cases where vulnerabilities go unnoticed and are attacked. Under such circumstances, Visualization Data, which visualizes the contents of components, is considered to facilitate the clarification of vulnerabilities and other risks and to reduce the residual risk of vulnerabilities. In this document, we focus on vulnerability management, which is currently expected as a use case for utilizing this Visualization Data.2.1Section 2.1 describes the process of vulnerability management using Visualization Data and its actors, and Section 2.2 describes the value of the Visualization Data to each actor, the users of the data.

2.1 Actors and Processes in Vulnerability Management using Visualization Data

This document also considers the presence of multiple entities involved in the supply chain of one product or multiple products. This document employs the main actors in the vulnerability management process using Visualization Data (Figure 1).

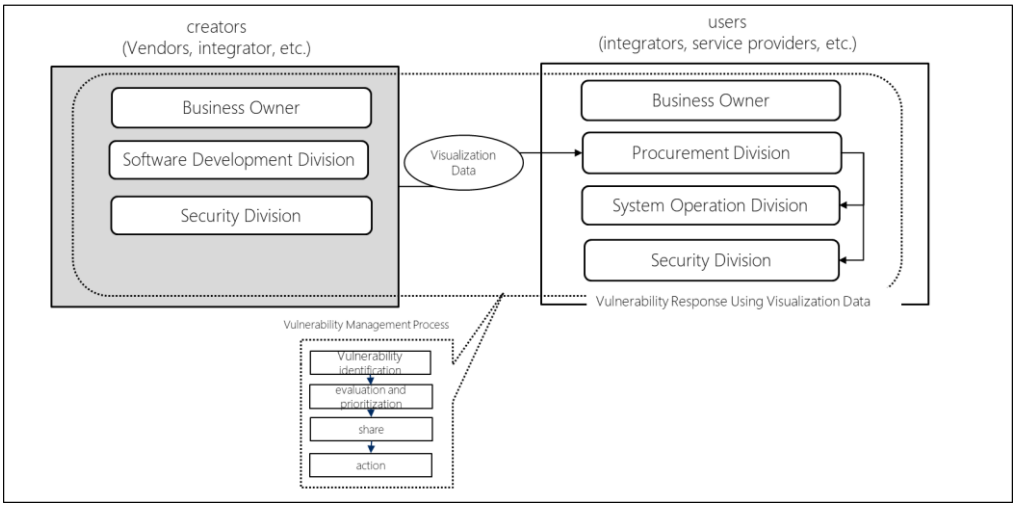

Figure 1 Main actors and processes in vulnerability management using Visualization Data

Actors who are the "creators" of Visualization Data such as SBOM include business owners, the software development divisions that develop software to be incorporated into products, and the security divisions that improve the security of developed products and respond to incidents. On the other hand, the actors who are

the "users" of Visualization Data include, in addition to the business owner, the procurement division that procures products, the system operation division that operates the procured products, and the security division that handles vulnerabilities.

Next, let us look at the vulnerability management process. The Visualization Data created by the creators is shared with the system operation division and security division via the procurement division of the users. When vulnerability management is performed by the user actors using the Visualization Data, the process consists of "vulnerability identification," "evaluation and prioritization," "sharing," and "action." In general, the security division is expected to take the lead in each process, but it is also expected to collaborate with the procurement division in the vulnerability identification process and with the system operation division in the evaluation and prioritization process. In the sharing and action processes, the procurement division will collaborate with the system operation division. In addition, all processes may involve collaboration with software development division and security division on not only the user side but also the creator side.

The vulnerability management process described above is also based on the "Key Steps and Procedures of the Vulnerability Management Process Using SBOM" described in the Introduction Guide developed by METI.

2.2 Value Brought Using Visualization Data

The following section describes the problems in vulnerability management and the value of utilizing Visualization Data from each actor's perspective on the "users": business owners, procurement division, system operation division, and security division.

- ✓ Business owners
  - ➢ For business owners, vulnerability management does not directly generate profits, so they often want to keep the measures and systems as low cost and minimal as possible. On the other hand, the loss when an incident occurs is often so enormous that the return on investment of measures is difficult to judge properly. Business owners often refer to industry and legal systems or measures taken by their competitors, but this is not a sufficient basis for making a judgment.
  - ➢ Visualization Data increases the transparency of products, systems, services, etc., provided by the company and its supply chain, and increases the accuracy of understanding the risk of vulnerability, thereby increasing the possibility of reducing the risk of damage from narrowing the amount of investment and the

deterioration of revenue and expenditures from excessive investment. This enables security expenses to be optimized for the entire enterprise and enables management to make appropriate judgments on security risks to their business required as part of their role, such as decisions on implementation of risk management measures at the minimum necessary and best cost. In addition, by explaining to stakeholders that business judgments are based on accurate information based on Visualization Data, the company management can assert that it is fulfilling its responsibility. The "Cyber Security Management Guideline Ver 3.0" [4] also requires management to "promote collection, sharing and disclosure of cyber security information," and Visualization Data is expected to be used.

- ✓ Procurement Division
  - ➢ For the procurement division, the safety of products procured from vendors is a primary concern. However, as the supply chain for products becomes more complex, there are difficulties in easily determining whether products are safe. There is also the concern of not collaborating with vendors to resolve issues when responding to incidents quickly.
  - ➢ Visualization Data increases the transparency of the products to be procured, thus increasing the likelihood that it will be easier to understand the objects to be protected and to confirm the vulnerabilities and other risks that may lie there.

- ✓ Security Division
  - ➢ For the security division, understanding the residual risk of vulnerabilities is extremely important, and security assessments are an essential part of this process. However, as the residual risk of vulnerabilities becomes more complex, the procedures for conducting security assessments also become more complicated, which is a problem that can lead to a tight operating schedule. However, as the residual risk of vulnerabilities becomes more complex, the procedures for conducting security assessments also become more complicated, which can lead to operational pressures.
  - ➢ Utilizing Visualization Data for security assessments increases the transparency of the software being used, making security assessments more efficient and

[4] Ministry of Economy, Trade and Industry Information-technology Promotion Agency, Japan "Cyber Security Management Guideline Ver 3.0
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

improving reliability.

- ✓ System Operation Division
  - ➢ One concern of the system operation division is to prevent incidents such as important information leaking due to the exploitation of vulnerabilities in the system they are not aware of. Furthermore, another concern is that the time required to deal with the incident will be too long and that the damage will spread during that time. There is the problem of wanting to avoid the impact on business operations while not being able to establish a concrete method for dealing with the situation.
  - ➢ The use of Visualization Data will increase the transparency of operational systems, facilitate the identification of vulnerabilities, and improve the efficiency of vulnerability response by sharing the data among the necessary organizations in the supply chain.

3 Issues Faced by "Users" of Visualization Data in Vulnerability Management

The Consortium published its activity vision "Towards Increased Security Transparency and Utilization" in February 2024. As shown inFigure 2, the Visualization Data includes not only information that can be handled by the SBOM but also software and hardware configuration information, status information indicating actual usage, and risk information such as vulnerability information.

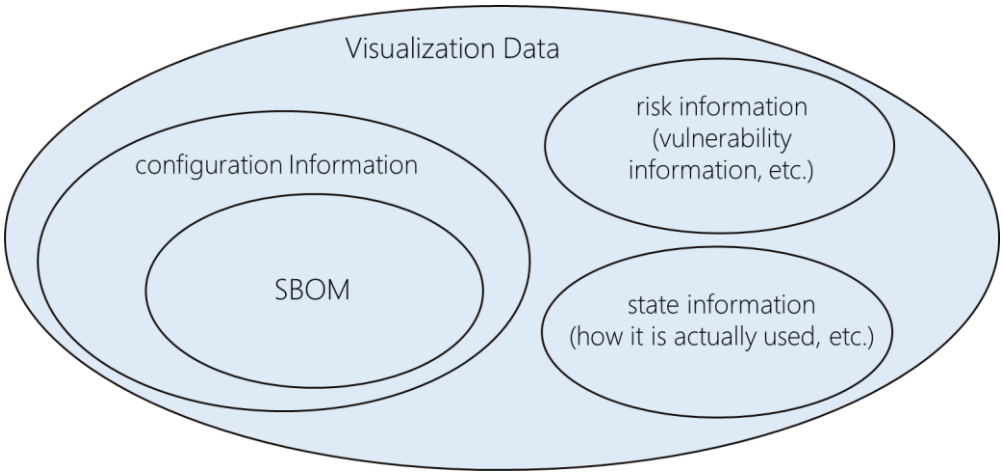

Figure 2 Visualization Data Classification

Examples of Visualization Data to be used in vulnerability management include software configuration information (including SBOM), network configuration information, source code, binary code, development documents, etc., which fall under configuration information, status information such as external access availability information and system configuration information, and risk information such as vulnerability information.

Also, as shown in**Figure** 3, the activity vision raised eight problems and issues faced by the users of these Visualization Data.

(1) Social Penetration and Recognition Inability to understand the value of Visualization Data in concrete terms, therefore lacking awareness of how to use it.	(5) Continuous Use It is necessary to continuously obtain the correct Visualization Data when updating software, etc.
(2) Format and Data In order to handle Visualization Data in a uniform manner, it is necessary to establish usage policies, etc.	(6) Coordination in a Supply Chain A mechanism of mutual sharing between creators and users in a multi-stage supply chain is necessary.
(3) Technology and Tools Automation is necessary to handle large amounts of Visualization Data.	(7) Impact of Visualization Data As security transparency increases due to the penetration of Visualization Data, it becomes necessary to deal with events that were previously invisible and could not be dealt with.
(4) Utilization Cost To respond to changes in operations brought about by the introduction of Visualization Data, it is necessary to efficiently educate personnel and familiarize them with related tools.	(8) Others As the use of Visualization Data is not included in conventional business, it is necessary to revise the business structure.

Figure 3 Eight problems and issues in the use of Visualization Data

Since these eight issues/problems do not represent a specific use of Visualization Data, we have organized them as issues when used for vulnerability management and analyzed the knowledge that we believe is necessary to address them. The results are presented below.

- (1) Social Penetration and Recognition

  The value of Visualization Data has not fully penetrated the market, especially for the users, and it is necessary to consider increasing the number of usage scenarios for the users without being restricted to vulnerability management. By communicating the value of using Visualization Data as a leading use case for vulnerability management, Visualization Data is expected to expand to use cases other than vulnerability management. Since we believe that this will lead to social penetration, we will prioritize addressing issues from (2) onward.

- (2) Format and Data

  There are multiple standard specifications for SBOM depending on the application, and even if the SBOM data format is the same, there may be variations in the output contents of SBOM generation tools. In vulnerability management, failure to correctly evaluate the quality of Visualization Data used to identify vulnerabilities may result in actions that were not originally necessary. In addition, there is a very serious situation at the practical level, such as whether vulnerabilities that should have been addressed have not been found. Indicators

for evaluating Visualization Data are explained エラー! 参照元が見つかりません。 ”Visualization Data Quality Indicators.” We believe that this knowledge will be useful in the vulnerability identification process of vulnerability management.

- (3) Technology and Tools

  In vulnerability management, collecting excessive Visualization Data from a wide variety of operators is critical for vulnerability identification. Although various technologies and tools are already available to handle Visualization Data, they may not be sufficient for some use cases. In vulnerability management, a serious issue is whether users of Visualization Data can make good use of it, and knowledge to deal with this issue needs to be created. How to use Visualization Data in vulnerability management is explained in 4.2 “Use of Visualization Data in Vulnerability Management” to deal with issues. We believe that this knowledge will be useful in the vulnerability identification process of vulnerability management.

- (4) Utilization Cost

  When Visualization Data is used for vulnerability management, the people in the security operation division, who are the users of the data, will have to deal with unprecedented changes in their work. Specifically, they will need to understand the Visualization Data correctly in decision-making and communication among the parties concerned. The kind of education necessary for users to understand the Visualization Data itself and to use it to respond to vulnerabilities is explained in 4.3 “Education for using Visualization Data."

- (5) Continuous Use

  In many cases, vulnerability management is done before utilizing Visualization Data, and depending on the product, service, or system used, it may be necessary to utilize Visualization Data in stages. 4.4 “Migration from Existing Operations" explains how to utilize Visualization Data for vulnerability management in a phased manner.

- (6) Coordination in a Supply Chain

  The supply chain of products, services, and systems often consists of multiple tiers, and when vulnerabilities occur, cooperation is required not only within an organization but also across organizations. For example, service providers, who

are the users of Visualization Data, need to stipulate necessary items in their contractual relationships with integrators, who are the creators. Also, it is assumed that some software provided by integrators used by service providers may not provide Visualization Data. Thus, knowledge of consensus building is very important in the supply chain. The knowledge on cooperation and total formation among organizations is explained in エラー! 参照元が見つかりません。 "Establishment of a System for Smooth Operation of Visualization Data."

- (7) Impact of Visualization Data

  As Visualization Data becomes more pervasive and security transparency increases, many vulnerabilities will be detected by collating vulnerability information databases, and more and more decisions will be required to address even those events that previously did not require action. Therefore, knowledge is required to evaluate and prioritize the detected vulnerabilities properly. The knowledge of evaluation and prioritization indicators and the ways to use them efficiently are explained in 4.6 “Vulnerability Response Prioritization Indicators." We believe that this knowledge will benefit the vulnerability management evaluation and prioritization process.

- (8) Others

  Visualization Data is not part of conventional operations, and the work system needs to be reviewed considering automation using various tools and continuous data updating. In vulnerability management, the users face various issues, and the work system may change depending on how these issues are addressed. Therefore, we will first prioritize the knowledge creation to address issues up to (7), but the knowledge in 4.3, 4.4, and 4.5 will also be useful when the business system is reviewed.

4 Knowledge to Deal with Issues

In Chapter 3, we discussed the issues faced by the users of Visualization Data in vulnerability management. In the <Background> section, we provided the assumptions and other information necessary to explain the knowledge of the consortium activities. We also provided specific details on the implementation of the knowledge, such as the implementation of the knowledge given in the <Contents> section.

4.1 Visualization Data Quality Indicators

✓ <Background>

If Visualization Data quality is low, vulnerability management based on that Visualization Data will result in unreliable results. We will introduce some issues related to Visualization Data quality and consider what can be done about them.

Issue 1: Lack of minimum elements

The National Telecommunications and Information Administration (NTIA) in the United States defines the quality of SBOM, a type of Visualization Data, and the minimum, recommended, and additional elements of SBOM.

The minimum elements include the name of the software, the vendor, and the components that make up the software, which are the minimum data required to identify the software itself and its components. Currently, there are relatively many descriptions of the name, identifier, vendor, and version of the SBOM, which are information on the tools and components used to create the SBOM. Still, there are few descriptions of the creators of the SBOM or the time of creation. The status of descriptions for each element is as follows (detailed description ratios can be found in the reference (http://id.nii.ac.jp/1001/00228550/)).

Table1 Description Percentage of SBOM's minimum elements

Elements	Description Percentage
Names and identifiers for SBOM creation tools and components	About 90%
Vendors and versions	About 60%
Author of the SBOM	About 30%
SBOM creation time	About 10%

The SBOM creator and time of creation are also the minimum elements, and we expect that this information will be clearly stated from the perspective of the users in the future.

Issue 2: Inadequate representation of elements and distortion of notation

For example, if Apache is listed in the vendor field for the software httpd, we know that the developer is Apache. However, in some cases, the name of the software management manager, such as pip or maven, is listed, making it impossible to identify the developer. If the developer cannot be identified, it is impossible to verify the existence of problems, such as vulnerabilities or bugs in the software. Also, listing the branch name of the software repository in the version is not strictly accurate and may make it impossible to investigate a problem with the software accurately.

If the notation of elements is distorted, a user of Visualization Data can become confused. For example, a common variant of vendor or product names is the abbreviation and the full name. The distorted notation prevents mechanical matching with vulnerability databases and may result in undetected vulnerabilities.

As described above, technologies to check and verify whether the information described in Visualization Data is appropriately expressed and technologies to unify expressions and collate names will be necessary in the future.

Issue 3: Component comprehensiveness

Software components represented by Visualization Data can represent usage relationships (dependencies) between software. There are explicit and implicit dependencies.

Explicit dependencies are dependencies provided by software package information. For example, Linux distributions use packages to manage software, and the packages contain information about software dependencies (Depends, Build-Depends, etc.) and when the software is installed. By referring to the explicit dependencies listed in the package information, the components on which the software depends can be identified.

Implicit dependencies, on the other hand, are dependencies that do not appear in explicit dependencies. In other words, they are dependencies of software that are not noted in the package information and are caused by copy-pasting or partially reusing modified source code. If not discovered, vulnerabilities cannot be noticed during vulnerability management. Therefore, implicit dependencies need to be revealed by using technologies that detect and understand code base relationships and package information.

These three issues exist in the quality of Visualization Data.

✓ <Contents>

A mechanism is needed to evaluate software transparency through Visualization Data and reveal software with solid transparency, including the above three issues. We introduce several perspectives to assess the degree of software transparency on the basis of the abundance and accuracy of information about the software developers provide. Please refer to the reference (http://id.nii.ac.jp/1001/00228550/) for details of each point of view.

Table2 Evaluation Perspectives of Information on Software

Category	Point of view
Abundance of provided information	Has the software been sufficiently explained?
	Has the component been sufficiently explained?
Accuracy of provided information	Is there any additional information about the component?
	Is there any intentional deletion of component-related information?
	Are the components sufficiently visualized?
	Is the depth of dependencies sufficiently visualized?

“Abundance of provided information" refers to whether the software's purpose, operation, etc., are sufficiently explained. If the explanation is insufficient, software users will use the software without understanding its mechanism correctly and will be exposed to residual vulnerability risk. For example, if the users use the software without knowing that it has a function to transmit information externally, information may leak.

“Accuracy of provided information" refers to the accuracy of the information in the Visualization Data provided by the creator. The users need to understand whether component information is intentionally deleted and whether the number of software components and the depth of dependencies are sufficiently visualized. The depth of dependencies corresponds to the traceability of components, and it is an advantage for the users to visualize not only directly used components but also indirectly used components.

This way, software transparency can likely be evaluated on the basis of Visualization Data. In addition, evaluating whether the transparency of important components can be visualized will likely help the users select software.

4.2 Use of Visualization Data in Vulnerability Management

<Background>

As described in 2.1, vulnerability management using Visualization Data involves the processes of "vulnerability identification," "evaluation and prioritization," "share," and "action."

“Vulnerability identification" here refers to determining whether or not the software used by the organization is affected by the software vulnerability that has occurred.

In utilizing Visualization Data for vulnerability management, there are two perspectives: 1) to investigate and analyze the impact of vulnerabilities on the basis of Visualization Data and 2) to use Visualization Data itself for understanding vulnerability information. The former is based on the assumption that each process from vulnerability identification to software vulnerability management is performed using configuration information, which is one of the elements of Visualization Data, while the latter is based on the assumption that users collect information necessary for vulnerability identification by using the vulnerability information itself described in the Visualization Data. The latter is assumed to be the case where the users utilize the vulnerability information itself contained in the Visualization Data to collect information necessary for vulnerability identification.

In this section, we will summarize our knowledge on vulnerability identification and evaluation and prioritization in the software vulnerability management process from the perspective of "conducting vulnerability impact studies and analysis on the basis of Visualization Data" and partially touch on the perspective of "using Visualization Data to understand vulnerability information."

✓ <Contents>

“Vulnerability Identification" involves collecting information on the names of software affected by vulnerabilities and the versions of that software that are affected by vulnerabilities and investigating whether the software in question is used within the organization. When vulnerability identification is performed using Visualization Data, software configuration information such as SBOM, which is one of the elements of Visualization Data, can be used to match the collected vulnerability information. As an example, the following is an image of how vulnerability information and Visualization Data are matched.

Vulnerability Information

└ Name and version of software affected by the vulnerability

↕

■ Elements of Visualization Data (SBOM)

└ Name and version of software recorded as configuration information

An example of the use of these services is to construct a service or mechanism that mechanically checks the information on the SBOM by referring to services that provide vulnerability information, vulnerability databases, and various software vendor websites. By having the organization's security division manage the SBOM of software used and deployed within the organization, it is expected to reduce the man-hours required for vulnerability identification and the residual risk of vulnerabilities. (According to a study conducted by METI, vulnerability management using SBOM reduced the man-hours required for management by about 70% compared to conventional manual management.[2]) On the other hand, there are issues of notation distortion that occurs when performing mechanical matching and the cost of implementing SBOM in an organization, both of which will be discussed in future working group (WG) discussions to generate knowledge. In the evaluation and prioritization process, the urgency of the response to software vulnerabilities identified in the vulnerability identification process is assessed. Specific evaluation methods and indicators are introduced in 4.6.2.

In the "evaluation and prioritization" process, vulnerability information itself is expected to be used in addition to the security settings of the system running the software and security control using access control devices such as firewalls (FWs). The perspective of "using the Visualization Data itself to understand vulnerability information" mentioned in the background is expected to be utilized in this process. One example is the inclusion of VEX (Vulnerability Exploitability eXchange) as one of the elements of the Visualization Data, which is a document that provides information from software vendors (“creators”) to user companies (“users”) on whether their products are affected by known vulnerabilities. It is expected to be used for evaluation and prioritization.[5]

[5] FY2022 Cyber Physical Security Measures Promotion Project: Report on Survey and Demonstration Project for Establishment of Supply Chain Model Introducing and Utilizing SBOM, https://www.meti.go.jp/meti_lib/report/2022FY/000372.pdf

4.3 Education for Using Visualization Data

✓ <Background>

To operate SBOM and other Visualization Data within a company, the personnel involved in the use of Visualization Data must understand and verify the information contained in the data and then use the data for decision-making and communication in their work.

In this regard, tools such as SBOM tools and vulnerability management tools have emerged with user interface(UI) that make it easy for humans to understand Visualization Data, and Visualization Data is being created and distributed in machine-readable formats. However, there are still situations in which Visualization Data needs to be read by humans. For example, when troubleshooting is necessary because a tool does not produce the intended result when inputting or outputting data, or when there is doubt about the displayed information, Visualization Data may need to be checked visually to ensure that there are no problems. In addition, there are Visualization Data such as SBOM in SPDX-Lite format, which are intended for manual operation in the first place.

In such cases, if the person in charge does not understand the types of Visualization Data, their purposes, contents, and formats, and the reference points and reading methods according to practical applications, quality problems with the Visualization Data may remain unidentified and unaddressed, or the lead-time for responding to vulnerabilities may increase due to confusion among the people in charge. This could lead to a situation where Visualization Data, which is originally intended to mitigate supply chain security risks, ends up increasing the risks.

✓ <Contents>

One measure to address the above issues is to implement educational programs to deepen the understanding of Visualization Data itself by those who are in charge of utilizing Visualization Data. Here, we will use SBOM as an example to illustrate the content of in-house education conducted by members of this consortium.

➢ (1) Growing cybersecurity risks in the software supply chain

As prerequisite knowledge for understanding the significance of SBOM, we explained the changes in the software development environment in our industry, the necessity of using open-source software (OSS)/commercial off-the-shelf and outsourcing software development as measures against the changes in the environment, and the possibility of introducing vulnerabilities due to

OSS/commercial off-the-shelf and outsourcing. As a response to the widespread use of automatic code generation by generative AI, it was also useful to mention the possibility of vulnerability introduction through OSS code snippet output of generative AI.

- (2) Significance of the SBOM

  While the company-wide and social significance of SBOM is important, it was also important for the internal training to mention the benefits to the participants in their work. For example, we appealed to those in charge of the security division to realize automatic vulnerability monitoring, while we appealed to users, software operation divisions, and software development divisions to visualize the components used to improve the efficiency of verification during development and to use it as evidence of whether or not they are responsible for responding to vulnerabilities when they occur. The appeal was made to users, software operation divisions, and software development divisions.

- (3) Composition of the SBOM and how to decipher it

  What is written where in the SBOM was explained with actual data from the SBOM, and the positioning and limitations of the SBOM standard were also explained here, which helped to spread knowledge and eliminate misunderstandings about the SBOM standard.

- (4) SBOM operating rules in your company

  We have indicated the tasks required to create and utilize the SBOM in the software supply chain and software lifecycle, and the corresponding relationship with a company's operations.

- (5) (as appropriate) How the SBOM tool operates

  In cases where SBOM tools have already been implemented, for participants to understand the procedures for implementing operations to create and utilize SBOM, the actual SBOM tools were displayed and operated while the procedures were explained, enabling participants to visualize the SBOM operations in concrete terms.

  In particular, it was effective to show actual SBOM data in the “SBOM structure and how to decipher it,” as some participants who did not understand the SBOM at an early stage could not visualize the SBOM itself, some confused it with a hardware BOM, and some equated the SBOM tool's output result screen with the SBOM. Therefore, by presenting a hypothetical case similar to the software developed by the company and showing examples of how they are represented in the SBOM standard SPDX format and CycloneDX format, we were able to

deepen participants' understanding of "what information is displayed in which item of the SBOM."

Figure4　Image of explanatory material of the structure and decoding method of SBOM (by Covalent Corporation).

The same approach is expected to apply to vulnerability databases such as NVD and machine-readable security advisories such as VEX, etc. The information that security division staff should refer to when responding to vulnerabilities (such as common vulnerability scoring system (CVSS), target versions, whether or not measures have been disclosed, and the results of impact assessment) can be easily extracted from the actual data. This will facilitate the extraction of necessary information from the vulnerability information and is expected to be effective in shortening the lead-time for vulnerability response.

We recognize that developing human resources able to utilize Visualization Data is an effective measure to reduce supply chain security risks for society as a whole. As a recommendation for the future, we expect that the definition of skill sets that organize the knowledge and skills required to effectively utilize Visualization Data and the establishment of a certification system that certifies sufficient skill sets will contribute to reducing supply chain security risks in society as a whole by equalizing the skill levels of human resources who utilize Visualization Data. This is expected to contribute to reducing supply chain security risks in society as a whole by equalizing the skill levels of personnel who utilize visual data.

4.4 Migration from Existing Operations

✓ <Background>

It is not realistic to proceed with vulnerability management using Visualization Data all at once. Since Visualization Data is relevant to a wide variety of suppliers, it is difficult to switch from an operation without Visualization Data to an entire operation with Visualization Data all at once. The spread of the system can be promoted by having it gradually and partially penetrate to the current vulnerability management.

✓ <Contents>

Currently, service providers, who are the "users" of vulnerability information, apply patches after receiving notifications of vulnerability information from vendors, etc., who are the "creators" of the software. As a first step, we will add Visualization Data such as SBOM to this effort to visualize what patches have been applied so that the users can fulfill their management responsibility. First, we will start with visualization. Gradually, we will expand the scope of the visualization by providing more and more Visualization Data.

Once the Visualization Data (SBOM) has been prepared to some extent, vulnerability assessment using the Visualization Data is conducted as the second step, on the basis of the CVSS basic evaluation criteria. Since the evaluation is conducted for each device or system procured, the evaluation is easy to apply, starting with devices for which Visualization Data is available. The results should be sent to the service providers who are the "users" of the equipment. However, if the service provider does not provide Visualization Data (SBOM) or vulnerability information, the users can easily conduct the missing part of the evaluation. The service provider can automatically perform vulnerability assessments on the basis of the basic assessment criteria.

Once the vulnerability has spread to this level, it will become realistic to conduct vulnerability assessments corresponding to the CVSS environmental assessment criteria as the third step. Once the results of the basic assessment criteria are available for various devices and systems, it will be possible to conduct an assessment using environmental assessment criteria that incorporates environmental values in an integrated system, thereby minimizing the implementation of measures.

4.5 Establishment of a System for Smooth Operation of Visualization Data

✓ <Background>

If the software developed by the company includes the vendor's scope of development, the vendor's cooperation is required when a vulnerability occurs. For example, when the company confirms the vulnerability information, the software developer and vendor need to investigate and answer whether the vulnerability affects the vendor's development scope, and if so, the vendor is required to implement modifications. If Visualization Data of software components used in the software is not provided by the vendors ("creators"), the users of the software components cannot monitor or respond to the vulnerabilities of the components, and vulnerability management for the software as a whole will not be possible.

Unless the vendor is contractually obligated to take such measures in the event of a vulnerability and the financial burden is clearly defined, a smooth response is difficult to expect. Therefore, the users and vendor of the software component need to clearly stipulate and agree on the details of vulnerability handling, such as provision of Visualization Data and division of roles in vulnerability management, in the contract between them and in the RFP/quotation conditions at the preliminary stage. On the other hand, the status of the vulnerability response varies from company to company.

One factor hindering the implementation of clear statements is the difficulty in ensuring the comprehensiveness and specificity of the requirements to be clearly stated. In some cases, contractually required requirements are omitted or not specified in detail to an operational level, and this can lead to questions arising between the vendor and the contractor at the time of actual vulnerability response, preventing the vulnerability response from progressing smoothly. For example, the contract may not be clear on how to proceed with monitoring, reporting, and responding to vulnerabilities, the scope of vulnerabilities to be monitored and reported, the criteria for prioritizing vulnerabilities and whether they require response, and the communication plan. This is a situation that can lead to a lack of clarity in the communication plan. In some cases, the integrator or vendor unilaterally sets the terms and conditions for questions that are not fully reviewed at the time the contract is signed, resulting in problems related to the scope of the contract and financial obligations when a vulnerability occurs.

Another disincentive to clear statements is the difficulty in establishing a uniform model for vulnerability handling. The content that can be agreed upon with vendors when attempting to clearly define vulnerability responses depends on the vendor's

contractual structure, negotiation power, and other relationships with the user, as well as the vendor's corporate strength. Industry norms and practices related to software development and cybersecurity also affect vulnerability response, making it difficult to establish a uniform model. For example, in embedded software development, it tends to be customary to minimize information disclosure from the perspective of intellectual property protection. In addition, some companies are reluctant to share the list of parts used in the Visualization Data (SBOM) with other companies due to concerns that the list could be misused in cyber-attacks.

Differences in perception of cybersecurity and related norms on both sides of the contracting entity can also be cited as a disincentive for clarification. For example, there was a case in which a difference in interpretation of the statement in the EU Cyber Resilience Act (EU CRA) that "there should be no obligation to disclose the SBOM" resulted in a dispute with a vendor regarding whether to disclose the SBOM or not. The term "disclosure" in the CRA refers to making the SBOM available to unspecified third parties by posting it on the company's website, etc. However, this difference in interpretation is believed to arise from the desire to minimize information disclosure.

✓ <Contents>

To address the above issues, we recommend that the following actions be taken in preparation for negotiations with vendors to clarify vulnerability responses.

① Identification of requirements for vulnerability response clarification

② Coordination of requirements at each point of discussion through the arrangement of a reasonable and realistic scope of Visualization Data sharing by the vendor.

The following explains our knowledge in proceeding with (1) and (2).

① Identification of requirements for vulnerability response clarification

It is recommended to identify the requirements that should be clearly stated in the first place to ensure that the agreements necessary for vulnerability response operations are not omitted from the contract. In doing so, the omission of important clauses can be prevented by referring to various model contracts and vendor requirements published by other companies in the same industry.

In particular, examples of other companies in the same industry are expected to be effective as a basis for showing in contract negotiations with vendors that the requirements are expected to be in line with actual practice and that the requirements are reasonable in light of the market prices in the industry. Here, we

introduce an example of vulnerability handling requirements that a European automobile manufacturer requires vendors to meet when procuring software.

table 3　Contracts with Suppliers for Appropriate Vulnerability Response (Example)

category	Examples of Contracts with Suppliers
Response processes	・ Establishment of post-launch monitoring and response process for vulnerabilities ・ Feedback on development division after launch processes
Division of roles and responsibilities	・ The obligation of suppliers to monitor and respond to vulnerabilities in the deliverables of their business partners ・ Authority for automakers to set vulnerability response deadlines
Correspondence rule	・ Bi-weekly status management of product cybersecurity-related activities ・ Bi-weekly access rights management for configuration management tools
Deliverables	The name of the deliverable and required information items. Example below: ・ SBOM Required information items: Specify at least 10 items such as names of software components to be used, unique identifiers, etc. ・ Vulnerability Response Results Required information items: Description of the solution, Changes, Details of tests performed, etc.
System	・ Only persons who have received cyber security training will be involved in the project. ・ Unit of Responsible Person
Communication plan	・ Obligation to send acknowledgement of receipt of vulnerability response requests on the part of automobile manufacturers ・ Response deadline (set in business days)

② Coordination of requirements at each point of discussion through the arrangement of a reasonable and realistic scope of Visualization Data sharing by the vendor.

As mentioned earlier, what can be agreed upon with vendors depends on the relationship with the user, industry practices, etc. Therefore, it is necessary to adjust what to request from the vendor on each issue with an eye toward areas of possible agreement.

One axis useful for this adjustment is "reasonable and realistic scope of sharing Visualization Data by vendors." If the Visualization Data shared by the vendor is limited, then there will be restrictions on the measures that the company can take.

There are various possible patterns for "reasonable and realistic scope of sharing Visualization Data by vendors," but here is an illustrative image of the adjustment of requirements for cases (a) and (b) below.

(a) Example of a case where Visualization Data of software components to be used is provided by a vendor

If the vendor provides Visualization Data of the software components used, the users can monitor the vulnerabilities of the entire software, including the components in question.

However, the vendor's cooperation in providing information and modifying the software is necessary to address the vulnerabilities detected. Therefore, it is desirable to discuss and agree in advance and exchange documents on the provision of Visualization Data of software components used and the details of cooperation with vendors in responding to detected vulnerabilities.

(b) Example of a case where Visualization Data of software components to be used is not provided by vendors

If the vendor does not provide Visualization Data of the software component used, the users cannot monitor the vulnerability of the component. In this case, the vendor will monitor the vulnerability of the component and provide information and corrected software to the users when a vulnerability is detected. The users will also consider vulnerability management other than the information provided by the vendor for the relevant component as necessary. For example, there are tools available on the market that analyze source code and binary data to extract OSS in use, and these tools can be used.

Therefore, in this case, the vulnerability management of the target software is shared between the users and the vendor ("creators"). In this case as well, it is advisable to discuss and agree on the division of roles in vulnerability

management and the details of cooperation to be requested from the vendor in advance and to exchange documents.

Although additional man-hours will be required to revise and negotiate contracts on the basis of this knowledge, we recognize that this will enable smooth collaboration with vendors without contractual discussions when responding to vulnerabilities, thereby contributing to a reduction in man-hours and lead-time in responding to vulnerabilities and lowering security risks.

4.6 Vulnerability Response Prioritization Indicators

4.6.1 Ensure Traceability between SBOM and Development Deliverables

✓ <Background>

When the software developer and security division staff prioritize vulnerability responses on the basis of the impact of the vulnerability on the software to be addressed, they are required to make decisions on the following issues, for example

- Does the targeted vulnerability occur in the software you developed in the first place?
- If it occurs, where in the software does it occur and what is the extent of the residual risk of the vulnerability due to spillover?
- Which files need to be modified and which development documents need to be updated to reflect the results of the modifications?
- If the vendor's scope of development also needs to be modified, which vendor should be involved?

The above decisions are generally difficult to make solely on the basis of information in the SBOM, and it is necessary to refer to source code, configuration files, and development documents such as requirement definitions and specifications. In such cases, files and documents related to the vulnerability take time to locate, which increases the man-hours required to prioritize vulnerability responses. This can also be a factor that lengthens the vulnerability response lead-time and may increase the residual risk of the vulnerability. In the worst case, the quality of the vulnerability response can be negatively impacted by incorrectly prioritizing and implementing remediation due to inability to correctly identify the impacted area.

✓ <Contents>

As a countermeasure to the above issue, there are examples of reducing the man-hours required to locate files and deliverables related to vulnerabilities by ensuring traceability between components and development deliverables submitted to the SBOM.

In this case, the ideal situation is to specify a component for which vulnerability information has been issued from the components submitted to the SBOM and to automatically identify the files and development deliverables associated with the component, such as source code with dependencies on the component, design files

affecting the configuration, and other development documents that mention the component. The files and development deliverables associated with the component are automatically identified.

To achieve the above situation, we used a traceability management tool to manage related files and development documents in each component of the SBOM by linking them together at the development stage. When a vulnerability occurs, the related files and development documents can be called up immediately by specifying the target component on the traceability management tool.

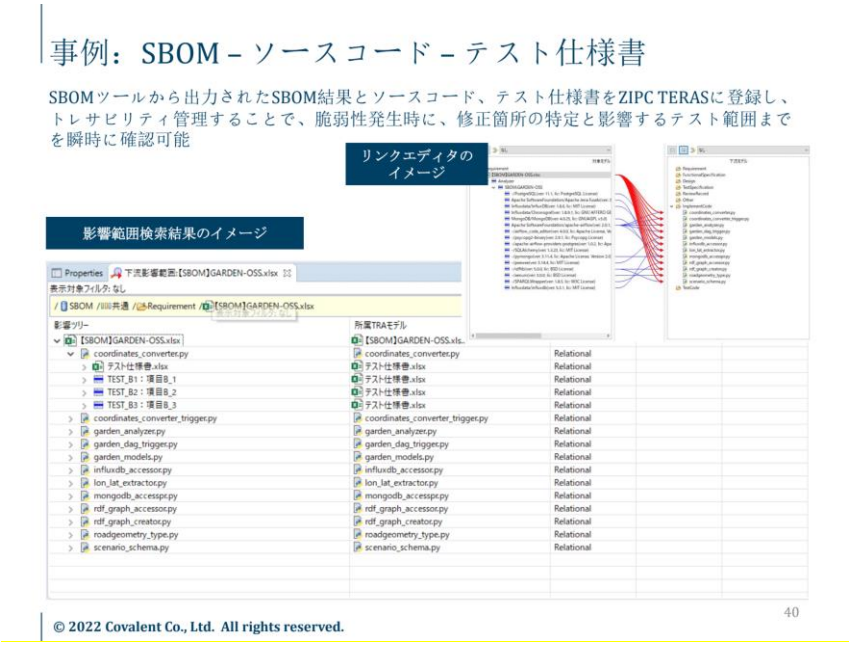

Figure5 Example of traceability management and influence range search for SBOM and development deliverables (by Covalent Corporation)

This case study also analyzed the effect of reducing the number of man-hours required to respond to vulnerabilities by ensuring traceability between the SBOM and development deliverables. In this case study, approximately 20% of the vulnerability management process from the identification of a vulnerability to the completion of the response was spent on the identification of the impacted area. This was necessary to identify the scope of modification required, the scope of retesting after modification, and other affected internal files in order to develop a plan for vulnerability response at a later stage. By using a traceability management tool to immediately call up relevant files and development documents in units of SBOM components, we were able to reduce the man-hours involved. In addition, the use of the traceability management tool prevented the omission of the identification of the impacted scope, suggesting the

possibility of preventing the increase in man-hours required for the subsequent modification and testing.

Note that to use a traceability management tool as in this case, related files and development documents for each SBOM component need to be linked at the development stage, and the man-hours required to do so are what is called an "initial investment." In this case study, it has not yet been demonstrated whether or not the man-hours required to do so can be recovered by the reduction in man-hours required to address subsequent vulnerabilities.

Although additional man-hours will be required for traceability management, this is expected to result in necessary information being promptly collected when responding to vulnerabilities, leading to a reduction in man-hours and lead-time for vulnerability response, and contributing to reducing the residual risk of vulnerabilities. In particular, if service level agreements (SLAs) between service providers and integrators, requirements for vulnerability response from integrators to vendors, or related laws and regulations such as the European Cyber Resilience Act stipulate strict lead-time requirements for vulnerability management processes, traceability management between SBOM and development deliverables is an important part of contract fulfillment and compliance. Traceability management between SBOM and development deliverables may be useful for contract performance and compliance.

4.6.2 Vulnerability Assessment Criteria

✓ <Background>

One type of the Visualization Data, SBOM, can be used to identify vulnerabilities in the relevant software. In general, since SBOM is assumed to be widely used in OSS, many engineers tend to discover a large number of vulnerabilities by verifying them. Therefore, it is important to determine the impact of vulnerabilities on the system and triage how and when to implement countermeasures against attacks to vulnerabilities to maximize return on investment.

✓ <Contents>

CVSS is an open, generic, and vendor-independent method of assessing vulnerabilities in information systems, providing a common, vendor-independent method of assessing vulnerabilities. CVSS allows for vulnerability severity to be quantitatively compared using the same criteria. In general, three evaluation criteria are defined

(1) Base Metrics

This criterion evaluates the characteristics of the vulnerability itself. The

confidentiality, integrity, and availability (CIA) are evaluated on the basis of criteria such as whether or not it can be attacked from the network, and the CVSS Base Score is calculated. This is the basis of SBOM's vulnerability assessment service.

(2) Temporal Metrics

This is a criterion to evaluate the current severity of vulnerabilities. It is evaluated on the basis of criteria such as whether attack code appears or not and whether countermeasure information is available, and the CVSS Status Value (Temporal Score) is calculated. Attack intelligence and countermeasure information are required.

(3) Environmental Metrics

This criterion is used to evaluate the severity of the vulnerability, including the usage environment of the product users. The CVSS Environmental Score is calculated on the basis of criteria such as the severity of secondary damage in the event of an attack and the usage of the target product in the organization. Although it requires environmental information and information on the expected damage, it provides an accurate assessment.

It is advisable to decide which of these criteria should be adopted, in accordance with the magnitude of the system's risk and the difficulty of the countermeasure.

Now, the overall cost can be reduced by sharing the vulnerability testing for triage between the "creators" (e.g., vendors) and the "users" (e.g., service providers). The most optimal method is for the creators to evaluate the system on the basis of the basic evaluation criteria, notify the results to the users, which are the customer, and for the users to evaluate the system on the basis of the environmental evaluation criteria in its own system. Note, however, that even if the creators discover a vulnerability, they may not create an update file because of a low CVSS score in the basic evaluation criteria. In such a case, the ideal communication is for the users to notify the results of the evaluation on the basis of their own environmental evaluation criteria and explain with numerical values that there is a large risk if no action is taken, thereby insisting on the necessity of creating an update file.

5 Conclusion

This document is a compilation of knowledge mainly for security divisions to address issues faced by "users" of Visualization Data (e.g., service providers) when utilizing Visualization Data for vulnerability management. In this consortium, various business operators from both "creators" (e.g., vendors) and users gather to discuss the issues. To promote the use of Visualization Data, we believe knowledge needs to be created not only for the security sector but also for management, and we aim to materialize and implement measures to create such knowledge. In addition, to ensure transparency in security, we will work on using Visualization Data for use cases other than vulnerability management.

We look forward to working with you to support this publication.
Please feel free to contact us at the following websites or the contact information.

- Security Transparency Consortium Website
  https://www.st-consortium.org/
- Security Transparency Consortium Secretariat
  stc-info@st-consortium.org

The Consortium's participating businesses as of September 30, 2024, are as follows

- ALAXALA Networks Corporation
- NRI SecureTechnologies, Ltd.
- Assured Inc.
- NTC Corporation
- NTT DATA Group Corporation
- FFRI Security, Inc.
- ZYYX Corporation
- LAC Co., Ltd.
- Contrast Security, Inc.
- Covalent Inc.
- Cybertrust Japan Co., Ltd.
- Cisco Systems G.K.
- Tokyo Electron Ltd.
- NEC Corporation

- NTT Corporation
- Hitachi, Ltd.
- Sumitomo Mitsui Trust Group, Inc.
- Mitsubishi Electric Corporation

Glossary

Term	Definition
Business Owner	The Owner of a business included in the supply chain or a business that uses products, systems, and services provided through the supply chain.
Security Division	The Division in charge of responding to vulnerabilities among businesses that comprise the supply chain or businesses that use products, systems, and services provided through the supply chain.
Procurement Division	The Division that procures products, systems, and services provided through the supply chain.
System Operation Division	The Division uses products, systems, and services provided through the supply chain.
SBOM	SBOM is a machine-processable inventory (list) that includes information on software components and their dependencies. It can be used for not only OSS but also proprietary software. In addition to being made widely available to the public, there are also methods of use that involve presenting SBOM only to those involved.
Visualization Data	Information that expresses the "configuration," "state," and "risk" of software and hardware in products, systems, services, etc. that are shared between businesses in the supply chain. Visualization Data includes SBOM, which is configuration information of software such as products.
Supply Chain	A linked set of resources and processes across multiple tiers of an organization, beginning with the procurement of products and services and extending throughout the lifecycle. [ISO 28001:2007, NIST SP 800-53 Rev. 5]
Cybersecurity risks throughout the supply chain	The potential for harm arising from the supply chain, its products, or its services to suppliers and beyond. Cybersecurity risks throughout the supply chain are threatened by threats that exploit, for example, vulnerabilities in products and services across the supply chain, as well as vulnerabilities in the supply chain itself. [NIST SP 800-161r1]
Vulnerability	A weakness in an asset or control measure that can be exploited by one or more threats. [JIS Q 27000:2014]