Addressing Supply Chain Security Risks through Security Transparency

Atsuhiro Goto and Yoshiaki Nakajima

Abstract

NTT has launched the Security Transparency Consortium to promote research and development of technologies for reducing supply chain security risks based on the key concept of *security transparency* and work with various companies forming the supply chain to mitigate such risks. In this article, we will introduce international trends related to supply chain security risks, relevant technologies, and an overview of the consortium.

Keywords: supply chain security, SBOM, security transparency

1. Emergence of unprecedented risks targeting supply chains

Cyber attacks have become a significant common threat to humanity, impacting the Internet, which supports economic activities and daily life and serves as a critical social infrastructure for health and life. Among the new risks related to cyber attacks, supply chain security risks are gaining global attention.

The services, systems, and products that people use are supported by diverse supply chains, from the design and development stage to the introduction and operation stage. If one of the suppliers in this supply chain is compromised, the impact propagates throughout the downstream of the supply chain. As services, systems, and products become more sophisticated and complex, the supply chain grows larger, and the scope of impact expands rapidly. It is also not uncommon for the downstream side of the supply chain where the impact propagates to be unaware of the existence of the supply chain, let alone understand it, making it difficult to avoid or reduce the impact. The risk arising from this is supply chain security risk, which has become significant and already caused harm.

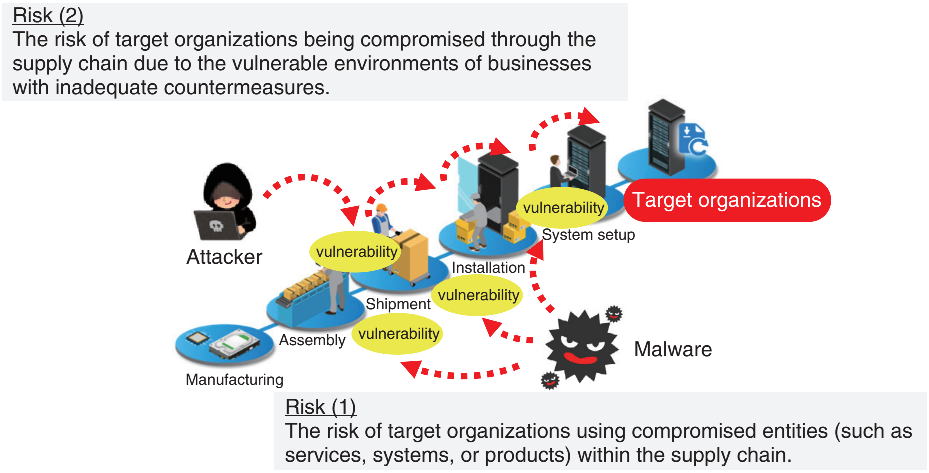
In this context, NTT Social Informatics Laboratories considers that the main cause of supply chain security risks is the *invisibility* of the supply chain and its objects, such as services, systems, and products. Therefore, we are conducting research and development to fundamentally reduce these risks by using *transparency* as a key concept, enabling users to verify the components, such as software elements, included in these objects. Recognizing that cooperation among the various entities forming the supply chain is essential for reducing these risks, the Security Transparency Consortium was established in September 2023 as a platform for such collaborative efforts. The consortium's chairperson is Dr. Atsuhiro Goto, president of the Institute of Information Security, who is also an author of this article [1].

The next section explains supply chain security risks and introduce the initiatives led by the consortium to reduce these risks.

2. Risk classification and incident cases

As the integration of cyberspace and physical space advances, supply chains are diversifying and expanding. It is practically difficult to fully understand the entire supply chain and prepare for risks, making cyber attacks on the supply chain highly threatening. These risks can be classified as shown in **Fig. 1**.

Risk (1) refers to the risk that entities such as services, systems, products, etc., transferred in a supply chain will be compromised, and downstream business operators who trust upstream business operators use them without knowing the fact of compromise; as



Risk (2)
The risk of target organizations being compromised through the supply chain due to the vulnerable environments of businesses with inadequate countermeasures.

Risk (1)
The risk of target organizations using compromised entities (such as services, systems, or products) within the supply chain.

Fig. 1. Classification of supply chain security risks.

Table 1. Incident examples related to supply chain security risks.

Time of occurrence	Outline of incident	Category
December 2020	The update program for the system provided by SolarWinds was compromised, affecting approximately 18,000 customers through the supply chain.	Risk (1)
July 2021	The update program for the IT management system provided by Kaseya was compromised, impacting around 36,000 customers through the supply chain.	Risk (1)
October 2022	In a domestic medical institution, a catering contractor was compromised, and ransomware spread through the system integration between the two parties, infecting a large number of servers and devices (about 1,300 units) within the hospital.	Risk (2)
December 2022	A severe vulnerability discovered in the “Apache Log4j,” a de facto standard for log output libraries, exposed many systems to attack risks. The issue was exacerbated by the difficulty in identifying software using the affected version of Log4j within the supply chain.	Risk (1)

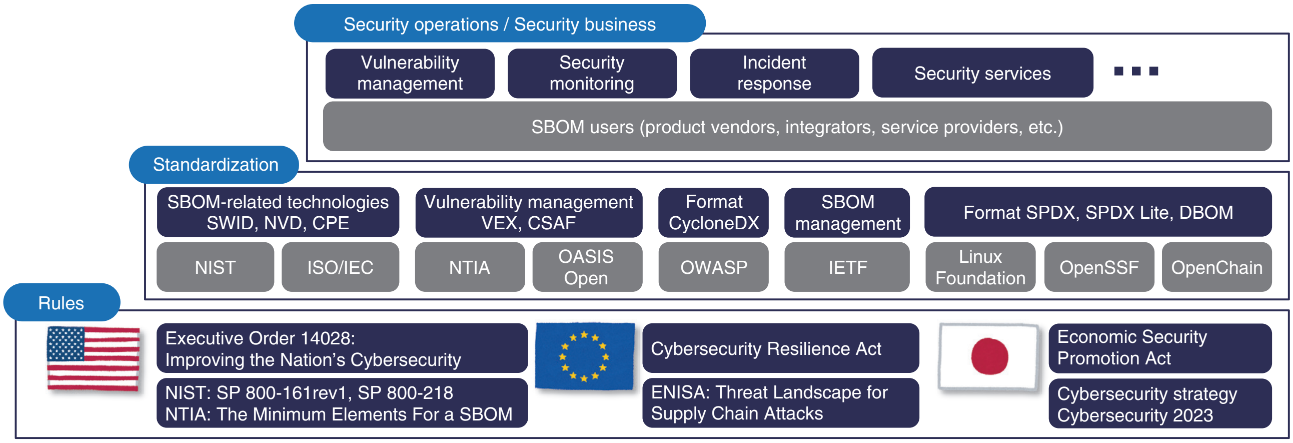
a result, they will be compromised. For example, there may be cases in which the software installed in the product is mixed with malicious software such as malware. It is also possible that vulnerabilities or unauthorized software might be introduced not only at the time of product introduction but also during software updates that are in operation.

In risk (2), the information technology (IT) environment of business operators that form a supply chain is compromised by cyber attacks, e.g., malware infection of company facilities, and hijacking of employee accounts, and various interactions with business partners, such as system linkage and email communication between business operators, are exposed to threats such as falsification, forgery, and malware infection.

There has been a series of incidents worldwide that have made us realize the emergence of such supply chain security risks. **Table 1** shows typical incident cases for each of the above categories.

3. National and industry trends in risk management

The occurrence of actual incidents has prompted governments, including the Japanese government, to recognize the importance and complexity of addressing supply chain security risks. Consequently, they are advancing various policies and regulations aimed at enhancing security. Related activities, such as standardization, are being promoted by industry groups, and it is expected that the security operations and security businesses of each business operator will be improved and developed on the basis of these activities. **Figure 2** shows an overview of the above.


Security operations / Security business
Vulnerability management
Security monitoring
Incident response
Security services
■ ■ ■
SBOM users (product vendors, integrators, service providers, etc.)
Standardization
SBOM-related technologies SWID, NVD, CPE
Vulnerability management VEX, CSAF
Format CycloneDX
SBOM management
Format SPDX, SPDX Lite, DBOM
NIST
ISO/IEC
NTIA
OASIS Open
OWASP
IETF
Linux Foundation
OpenSSF
OpenChain
Rules
Executive Order 14028: Improving the Nation's Cybersecurity
NIST: SP 800-161rev1, SP 800-218
NTIA: The Minimum Elements For a SBOM
Cybersecurity Resilience Act
ENISA: Threat Landscape for Supply Chain Attacks
Economic Security Promotion Act
Cybersecurity strategy
Cybersecurity 2023

CPE: Common Platform Enumeration
CSAF: Common Security Advisory Framework
DBOM: delivery software bill of materials
ENISA: European Union Agency for Cybersecurity
IETF: Internet Engineering Task Force
ISO/IEC: International Organization for Standardization/
International Electrotechnical Commission
NVD: National Vulnerability Database
OWASP: Open Web Application Security Project
SPDX: Software Package Data Exchange
SWID: Software ID
VEX: Vulnerability Exploitability eXchange

Fig. 2. Overview of trends related to supply chain security risks.

3.1 United States

In the United States, Executive Order 14028: Improving the Nation's Cybersecurity, issued in May 2021, has been a starting point for efforts to strengthen the security of the software supply chain, improve the reliability of software, and strengthen cyber-incident reporting requirements. National Institute of Standards and Technology (NIST), National Telecommunications and Information Administration (NTIA), Cyber Security Infrastructure Agency (CISA) and others in the United States have published best practices and guidelines for implementing measures based on this Executive Order [2].

A key element in this effort is a software bill of materials (SBOM). An SBOM is a list of components included in a software product and their information (software version information, dependencies between software, etc.). This information is expected to enable proper recognition of the existence of software that constitutes services, systems, and products throughout the supply chain, which leads to rapid and effective identification of vulnerabilities, risk identification, and implementation of necessary measures.

Efforts by the United States to popularize SBOMs are accelerating. In addition to standardizing SBOMs and publishing best practices for its operation, efforts are underway to require companies and critical infrastructure operators that do business with the U.S. government to prepare and provide SBOMs.

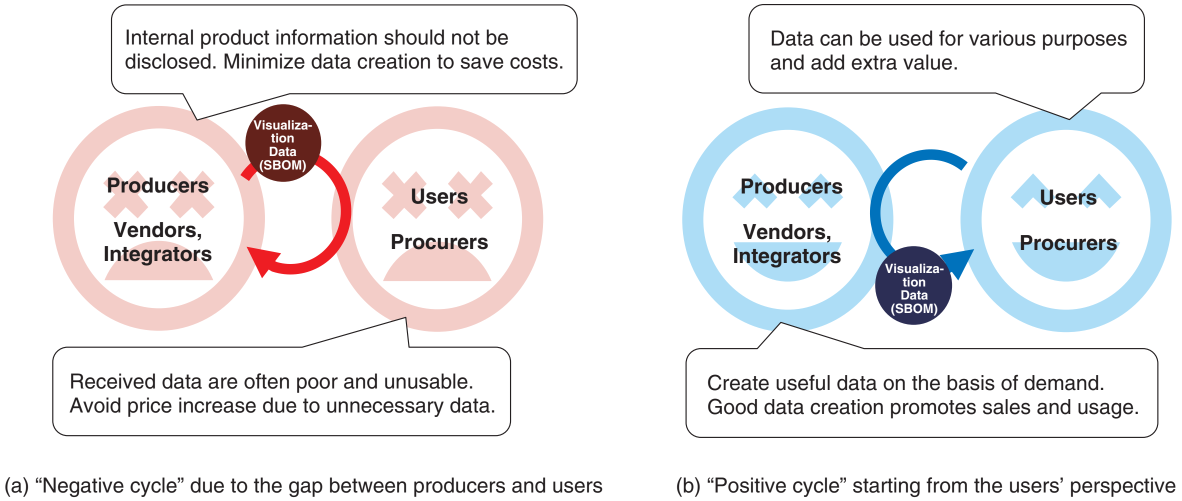
3.2 EU

The European Union (EU) is also promoting policies to address supply chain security risks. In particular, the Cyber Resilience Act (CRA) [3] published by the European Commission in September 2022 stipulates a variety of cyber-security-related regulations for products with digital elements, including supply chain security risks, and are scheduled to be enforced in 2024.

CRA is expected to clarify the responsibilities of the upstream (business operators) and the rights of the downstream (users) who form the supply chain and improve the environment for responding to risks throughout the supply chain. A business operator is obliged to provide information necessary to respond to cyber-security risks. As an SBOM is positioned as an important means to achieve this, it is expected that the creation of an SBOM will be widely sought in the EU as well as in the United States.

3.3 Japan

In the cyber-security strategy adopted by the Cabinet in 2021, the Japanese government has positioned the establishment of a foundation for ensuring supply chain reliability as key policy, and in its annual cyber security 2023 plan, the Japanese government states


Internal product information should not be disclosed. Minimize data creation to save costs.
Visualization Data (SBOM)
Producers
Vendors, Integrators
Users
Procurers
Received data are often poor and unusable. Avoid price increase due to unnecessary data.
Data can be used for various purposes and add extra value.
Producers
Vendors, Integrators
Visualization Data (SBOM)
Users
Procurers
Create useful data on the basis of demand. Good data creation promotes sales and usage.

(a) "Negative cycle" due to the gap between producers and users

(b) "Positive cycle" starting from the users' perspective

Fig. 3. "Negative cycle" and "positive cycle" related to visualization data.

that it will promote efforts to strengthen measures against supply chain security risks, including SBOMs.

As part of the above policies, the Ministry of Economy, Trade and Industry, the Ministry of Internal Affairs and Communications, and the Ministry of Health, Labour and Welfare are promoting various initiatives to popularize SBOMs, such as publishing guides on the introduction of SBOMs and vulnerability management using SBOMs. In the automotive industry, which is characterized by large-scale supply chains, there is a trend toward developing and adopting customized formats that take into account operational aspects, such as operational costs, of SBOMs.

4. What is required for risk management

Supply chain security risks, in which products, systems, and services are compromised through the supply chain, require countermeasures throughout the supply chain that extends throughout the world, including the suppliers of each component. SBOMs are being developed and studied by governments around the world and provide information (visualization data) to the supply chain that makes it easier to understand the content of objects to be protected and identify risks such as vulnerabilities hidden in them. SBOMs may increase the transparency of system configurations and reduce security risks. If visualization data can be shared throughout the supply chain from upstream to downstream and used for security measures, risks to the entire supply chain can be effectively reduced.

With the move toward making SBOMs mandatory, if efforts become more focused on the producer's perspective, such as the cost of generating visualization data, there is a risk that attention and efforts will be biased toward addressing problems on the producers. Therefore, as shown on the left of **Fig. 3(a)**, the goal may shift to producing visualization data within practical limits, potentially undermining the benefits that the visualization data were originally supposed to provide.

Therefore, we believe it is essential to also consider the user's perspective and approach the issue from both the user's and producer's viewpoints in a balanced manner, avoiding the above-mentioned bias. For example, identifying data conditions necessary for effective use of visualization data from the user's perspective enables producers to benefit from avoiding unnecessary generation of visualization data. If the creation of visualization data by the producers contributes to promoting product sales, it is expected that more resources to be allocated, further advancing the use of visualization data.

To truly address supply chain security risks, it is crucial for the diverse operators involved in the supply chain, both producers and users, to collaborate and tackle the issues from both perspectives.

5. The positive cycle of risk management the consortium aims for

Since the creation and provision of visualization

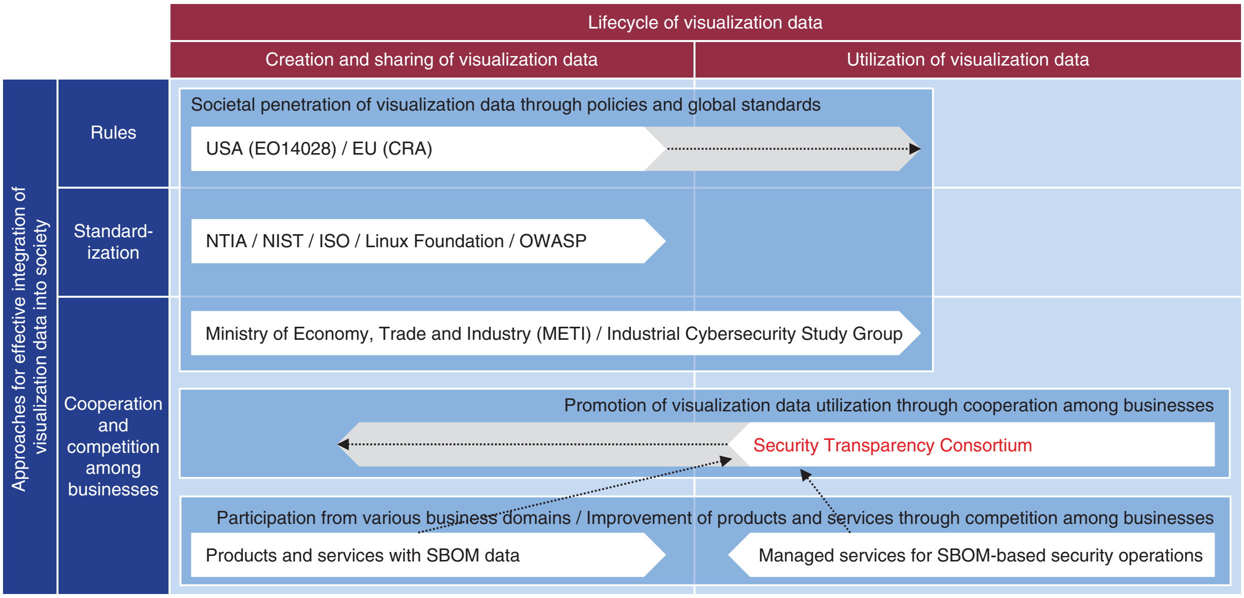

Lifecycle of visualization data
Creation and sharing of visualization data
Utilization of visualization data
Approaches for effective integration of visualization data into society
Rules
Standard-ization
Cooperation and competition among businesses
Societal penetration of visualization data through policies and global standards
USA (EO14028) / EU (CRA)
NTIA / NIST / ISO / Linux Foundation / OWASP
Ministry of Economy, Trade and Industry (METI) / Industrial Cybersecurity Study Group
Promotion of visualization data utilization through cooperation among businesses
Security Transparency Consortium
Participation from various business domains / Improvement of products and services through competition among businesses
Products and services with SBOM data
Managed services for SBOM-based security operations

Fig. 4. Basic stance on consortium management.

data entails a cost burden on suppliers of products, it is essential to effectively use visualization data at a level commensurate with the cost. Effective utilization will encourage the creation and provision of visualization data, leading to a positive cycle that will further expand the use of visualization data (**Fig. 3(b)**).

We have established the Security Transparency Consortium to collaborate with various businesses that form the supply chain (product vendors, system integrators, security vendors, and businesses that use and operate services, systems, and products) and work on the *co-creation of knowledge* that contributes to the promotion of visualization data usage.

By promoting the creation and provision of visualization data and sharing the knowledge and expertise of each member, we aim to materialize and expand use cases. The three pillars of this consortium are as follows:

- We will work to materialize a wide range of use cases and methods for using visualization data. Specifically, we will analyze issues, examine solutions, and demonstrate the use of transparency enhanced by visualization data such as software configuration for security operations.
- With the participation of a variety of businesses, not limited to a specific industry or field, the study is conducted from a broad perspective that includes both the providers and users of the visualization data.
- With the aim of contributing to solving social issues, such as dealing with supply chain security risks, through the publication of the study results, we will also promote community activities that contribute to these efforts and cooperation with government agencies.

In advancing the above initiatives, ensuring ease of participation is particularly important to incorporate the insights of the diverse businesses that form the supply chain. Therefore, we operate the consortium with a clear definition of the collaborative domain and competitive domain. In our consortium, we define and publish the issues and challenges that members commonly face as the activity vision [4]. To address these issues, we discuss and co-create knowledge (such as insights on effectively using visualization data such as SBOMs) in the collaborative domain. During this process, each member refrains from bringing in their proprietary confidential information and operates solely using publicly available information. Members are expected to feed back the insights gained from the consortium activities into their own business (such as business or technology development) and strive for excellence in the competitive domain, thereby strengthening society's overall risk response capabilities. **Figure 4** summarizes the basic stance of consortium management as described above.

Through our consortium activities, we are dedicated to promoting greater societal penetration of security transparency. By embracing this key concept, we aim to tackle various social challenges and work toward their resolution.

References

[1] Press release issued by NTT, “Establishment of the Security Transparency Consortium to address supply chain security risks,” Oct. 11, 2023.
https://group.ntt/en/newsrelease/2023/10/11/231011a.html

[2] NIST, “Improving the Nation’s Cybersecurity: NIST’s Responsibilities Under the May 2021 Executive Order.”
https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

[3] EU Cyber Resilience Act,
https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[4] Press release issued by NTT, “Security Transparency Consortium Announces Activity Vision for Improving and Utilizing Security Transparency - Promoting comprehensive cybersecurity capabilities in the supply chain using SBOMs -,” Feb. 16, 2024.
https://group.ntt/en/newsrelease/2024/02/16/240216b.html

Atsuhiro Goto
President and Professor, Institute of Information Security (IISEC).
He received a Ph.D. from the University of Tokyo in 1984 and joined NTT Musashino Laboratories the same year. Since starting his career as a professor at IISEC in 2011, he worked for Cybersecurity R&D as the program director for the Cross-ministerial Strategic Innovation Promotion Program (SIP) from 2015 to 2022. He has been a member of Cybersecurity Strategic Headquarters, Government of Japan, as well as a member of professional associations such as the Association for Computing Machinery (ACM), the Institute of Electronics, Information and Communication Engineers (IEICE), and the Information Processing Society of Japan (IPSJ).

Yoshiaki Nakajima
Vice President, Head of NTT Social Informatics Laboratories.
He received a B.S. in information science and M.S. in mathematical and computing science from Tokyo Institute of Technology in 1995 and 1997. He joined NTT Information and Communication Systems Laboratories in 1997. He has been involved in the R&D of information and communication platforms, security platforms, and other areas. He has Certified Information Systems Security Professional (CISSP), Certified Cloud Security Professional (CCSP) and Registered Information Security Specialist (RISS) qualifications.