(Press release)

October 21, 2024.

NTT Corporation
NEC Corporation
ALAXALA Networks Corporation
NRI SecureTechnologies, Ltd.
NTC Corporation
NTT DATA Group Corporation
ZYYX Inc.
LAC Co., Ltd.
Contrast Security, Inc.
Covalent Inc.
Cybertrust Japan Co., Ltd.
Tokyo Electron Ltd.
Sumitomo Mitsui Trust Group, Inc.
Mitsubishi Electric Corporation

Co-creation of knowledge for utilizing Visualization Data such as SBOM Visualization Data Utilization to Ensure Security Transparency -Vulnerability Management Edition- Security Transparency Consortium announces

～Improving the ability to deal with supply chain security risks through co-creation by diverse businesses ～

In a working group of the Security Transparency Consortium※1, chaired by Atsuhiro Goto, President and Professor, Graduate School of Information Security, Institute of Information Security, aiming at reducing supply chain security risks, 14 companies※2 consisting of diverse businesses, including NTT Corporation (NTT) and NEC Corporation (NEC) as the chief and vice chief have been working to solve problems and issues faced by users utilizing Visualization Data※3 such as SBOM※4 under the activity vision "Improving and Utilizing Security Transparency"※5 announced in February 2024.

As an example of the using Visualization Data for vulnerability management, the consortium co-creates knowledge to deal with the problems and issues faced by users utilizing Visualization Data, such as identifying and prioritizing vulnerabilities. The result of the Consortium's activities is the release of the "Visualization Data Utilization to Ensure Security Transparency – Vulnerability Management Edition-". This is the first released case study of vulnerability management utilization of Visualization Data in Japan and was co-created by diverse businesses including both the users (e.g., integrators, service providers) and creators (e.g., vendors, integrator) of Visualization Data. It

is expected to be useful for businesses in various industries that are considering using Visualization Data for vulnerability management.

1. Background and Objectives

To deal with supply chain security risks to products, systems, and services, Visualization Data such as SBOM, which ensures transparency of products, systems, and services, is attracting attention. On August 29, 2024, the Ministry of Economy, Trade and Industry (METI) released "Guidance on Introduction of Software Bill of Materials (SBOM) for Software Management ver 2.0" to promote the introduction of SBOM. Additionally, studies on how to utilize SBOM are underway, especially in the medical and automotive industries, and SBOM is expected to be used in various use cases in the future.

Under such circumstances, various problems and issues need to be solved to utilize Visualization Data, and knowledge based on specific use cases is strongly required. In February 2024, the Consortium also released an activity vision to organize and address the problems and issues faced by users utilizing Visualization Data, and to define an action policy to deal with them. The use of Visualization Data in vulnerability management is a highly anticipated use case, and many of the above problems and issues cannot be solved by a single company, so diverse businesses needs to co-create knowledge.

2. Overview

The consortium has co-created knowledge for dealing with the problems and issues raised in the activity vision, by creating a tangible form of vulnerability management, which is one of the use cases where the use of Visualization Data is most anticipated. As an achievement of the consortium, "Visualization Data Utilization to Ensure Security Transparency – Vulnerability Management Edition" has been released on the website[※5]. An overview is given below, along with the problems and issues raised in the activity vision.

(1) Format and Data

There are multiple standard specifications for Visualization Data such as SBOMs, and the output of generating tools varies. Therefore, there is a risk that vulnerabilities that need to be addressed cannot be correctly identified in vulnerability management. To identify vulnerabilities that need to be addressed, the quality of Visualization Data needs to be correctly evaluated, and we will present our knowledge on quality indicators of Visualization Data.

(2) Technology and Tools

Although various technologies and tools for Visualization Data are already available, they are not sufficient for vulnerability management. We will present our knowledge of how users of Visualized Data can make better use of it.

(3) Utilization Cost

For users to utilize Visualization Data for vulnerability management, they urgently need to understand how to utilize Visualization Data through human resource development and to bear the cost of such training. We will present our knowledge on the education required for users to understand Visualization Data and to use it for vulnerability management.

(4) Continuous Use

If vulnerability management had been in place before the use of Visualization Data, it may not have been possible to completely introduce the utilization of Visualization Data in a single step. We will present our knowledge of how to gradually infuse the utilized Visualization Data into existing vulnerability management mechanisms.

(5) Coordination in a Supply Chain

Supply chains of products, services, and systems often consist of multiple tiers, and when vulnerabilities occur, cooperation across organizations is required, not just within a single organization such as individual companies. We will present our knowledge of cooperation and consensus building among organizations in the supply chain.

(6) Impact of Visualization Data

As the utilization of Visualization Data in vulnerability management becomes more widespread and security transparency increases, many vulnerabilities will be detected, and more and more decisions will be required to address even those that did not need to be addressed in the past. We will provide our knowledge with an index for appropriately evaluating and prioritizing vulnerabilities that have been detected.

The results of the Consortium's activities are the first released case study in Japan that summarizes the collaborative efforts of diverse businesses in vulnerability management, a specific use case, to solve problems and issues that many businesses face immediately after starting to utilize Visualization Data such as SBOM or when considering the utilization of Visualization Data. This case study is expected to increase security transparency in vulnerability management and reduce supply chain security risks in diverse industries. It will also serve as a reference case study for promoting the utilization of Visualization Data other than vulnerability management in the future.

3. Outlook

The Consortium will continue to co-create measures to deal with problems and issues in the utilization of Visualization Data through the collaborative efforts of diverse businesses. Target use cases will be compiled as "Visualization Data Utilization to Ensure Security Transparency," regardless of vulnerability management, and will be released on the Consortium's website※5 from 2025 onward. The Consortium is also continuing to expand the number of participating companies ※2※7 and is currently accepting applications for further participation on its website※8 .

Notes

※1

NTT Corporation※6 , a consortium launched in September 2023 with NEC Corporation as the Coordinator.

※2

NTT Corporation

NEC Corporation

ALAXALA Networks Corporation

NRI SecureTechnologies, Ltd.

NTC Corporation

NTT DATA Group Corporation

ZYYX Inc.

LAC Co., Ltd.

Contrast Security, Inc

Covalent Inc.

Cybertrust Japan Co.

Tokyo Electron Ltd

Sumitomo Mitsui Trust Group, Inc.

Mitsubishi Electric Corporation

※3

Data that visualizes the configuration, status, and risk information of software and hardware such as products, systems, and services that are exchanged between businesses in the supply chain.

※4

Software Bill of Materials, a data format for listing the software components included in a product

URL: https://www.ntia.gov/

※5

Security Transparency Consortium Website "Information Dissemination"

URL: https://www.st-consortium.org/?page_id=1327

※6

Through the participation of NTT Corporation, the following NTT Group companies will also cooperate with the consortium

NTT EAST Corporation

NTT WEST Corporation

NTT DOCOMO, INC

NTT Communications Corporation

NTT Advanced Technology Corporation

NTT TechnoCross Corporation

NTT Security Japan

※7

Assured, Inc.

FFRI Security, Inc.

Cisco Systems G.K.

Hitachi, Ltd.

※8

Security Transparency Consortium Website, "About Joining"

URL: https://www.st-consortium.org/?page_id=6

■Contact the consortium

Security Transparency Consortium Office

stc-info@st-consortium.org

■Media Contacts

NTT Service Innovation Laboratory Group

Public Relations

https://tools.group.ntt/en/rd/contact/index.php?param01=R&param02=202

NEC Corporation

Global Innovation Strategy Planning Department

ALAXALA Networks Corporation

Haruki Kobayashi
Shinkawasaki TwinTower. West Tower.13F, 1-1-2 Kashimada, Saiwai-ku, Kawasaki-shi, Kanagawa 212-0058, Japan（former name：Shinkawasaki Mitsui Bldg）

NRI SecureTechnologies, Ltd.
Public Relations
E-mail: info@nri-secure.co.jp

NTC Corporation
Yutaka Koyama

NTT DATA Group Corporation
Public Relations Department
E-mail: nttdata-pr-inquiries@am.nttdata.co.jp

ZYYX Inc.
Public Relations Team, GitLab Partner Business
support-gitlab@zyyx.jp

LAC Co., Ltd.
nbd-support@lac.co.jp

Contrast Security, Inc.
JPNSales@contrastsecurity.com
+81-50-3733-8284

Covalent Co., Ltd.
info@covalent-asia.com

Cybertrust Japan Co., Ltd.
press@cybertrust.co.jp

Tokyo Electron Ltd.
telpr@tel.com
+81-3-5561-7004

Sumitomo Mitsui Trust Group, Inc.
Satoshi Tanaka

Mitsubishi Electric Corporation
Public Relations Division
Tokyo Building,
2-7-3, Marunouchi, Chiyoda-ku, Tokyo 100-8310, Japan
TEL:+81-3-3218-2332