Collection of Use Case Examples Regarding Management Methods for Utilizing Open Source Software and Ensuring Its Security

Ministry of Economy, Trade and Industry
Commerce and Information Policy Bureau
Cybersecurity Division

May 10, 2022

Table of Contents

1. Objectives

As industrial activities become more service-oriented, the importance of software in industry is increasing. In particular, in recent years, software has been introduced for control of industrial machinery and automobiles, and it is expected that various added values will be created by building systems on general-purpose hardware and adding various functions to software.

Among them, open source software (OSS), whose source code is open to the public and can be used, modified, and redistributed for commercial or non-commercial purposes, has been actively adopted in recent years for commercial products and services of companies, mainly for general-purpose libraries and Linux systems. It is now difficult to build products and services without using OSS.

As an effort to ensure software security, the Working Group (WG) 1 (Systems, Technologies and Standardization) under the Study Group for Industrial Cybersecurity compiled the Cyber/Physical Security Framework (hereinafter referred to as "CPSF") in April 2019. Although the CPSF mentions, among others, software configuration management and integrity confirmation, it does not specifically clarify how to continue to maintain software security and or how to confirm it, as software becomes more complex, and the use of OSS expands. Overseas, the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) established a joint public-private study system called Software Component Transparency in July 2018 and has been discussing how to manage software vulnerabilities using the Software Bill of Materials (SBOM). Under these circumstances, the Ministry of Economy, Trade and Industry (METI) established the Task Force for Evaluating Software Management Methods, etc. toward Ensuring Cyber/Physical Security (hereinafter referred to as the "Software Task Force")[1] in September 2019 to study specific software security measures based on the CPSF.

In the discussions of the Software Task Force, it was recognized that while the importance of OSS utilization in the industry is increasing, companies are facing challenges, including the management of OSS and other software and the handling of vulnerabilities. In light of the current situation where companies are taking various measures to deal with these issues, we came to the conclusion that it is effective to

[1] Task Force for Evaluating Software Management Methods, etc. toward Ensuring Cyber/Physical Security (in Japanese)
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/index.html

share knowledge in the industry.

This Collection organizes the perspectives of issues related to corporate OSS utilization and compiles various cases for each perspective. The purpose is to provide reference information for companies to consider for their own management method for OSS utilization and its security assurance and to promote appropriate OSS utilization in consideration of OSS points of concern. It is also hoped that removing barriers to the use of OSS by companies will encourage further use of OSS and lead to improved competitiveness by clarifying the benefits of OSS in industry.

2. OSS Overview

2.1. What is OSS?

OSS is software in which the source code is made available to the public, and anyone is allowed to use, modify, and redistribute it. The concept and orientation of OSS is that users around the world should treat the source code as common intellectual property and continue modifying and improving it.

AS general OSS requirement, there is a widely known license document called “The Open Source Definition”[2]. This document is developed and published by the Open Source Initiative[3], which is working to raise awareness of the culture of open source.

The Open Source Definition lists the following conditions that OSS must meet:

1. Free Redistribution.
2. Source Code.
3. Derived Works.
4. Integrity of The Author's Source Code.
5. No Discrimination Against Persons or Groups.
6. No Discrimination Against Fields of Endeavor.
7. Distribution of License.
8. License Must Not Be Specific to a Product.
9. License Must Not Restrict Other Software.
10. License Must Be Technology-Neutral.

In addition, one of the major features of OSS is the activities of an OSS community (hereinafter referred to as "Community") for development, improvement, and sharing of know-how. A Community is composed of users, developers, and enthusiasts in a

[2] An organization founded in 1998 in the United States to educate and support the interests of an "open source" and to bridge the gap between various members of the open source community.
https://opensource.org/

[3] The Open Source Definition
https://opensource.org/docs/osd

specific OSS project, and is operated for non-profit purposes. A Community plays a major role in the ecosystem to promote the utilization of OSS by sharing source codes among members around the world, who engage in joint development, send related information through mailing lists, and hold study sessions. Since it is a great advantage for companies and organizations to be able to use high-quality OSS thanks to active community activities, more and more companies and organizations are actively supporting Community activities of their employees as OSS utilization advances. Major Communities include the Linux Foundation and the Apache Software Foundation.

In contrast to OSS, there is proprietary software. This is software in which the software distributor retains its intellectual property and is restricted from modification or reproduction. Specifically, in proprietary software, the source code is not made public, and its use is legally restricted under a software license agreement. It is distributed in the market as commercial software for a fee. On the other hand, there is software that is provided free of charge as free software.

2.2. OSS utilization areas

The areas of OSS utilization are diverse, ranging from OS[4] to business applications, databases, big data, and AI (artificial intelligence). In order to understand the major OSS, it is effective to refer to the OSS bird's eye view compiled by the Japan OSS Promotion Forum.[5] This provides a whole view of OSS used in various domains (Figure **2.2-1**).

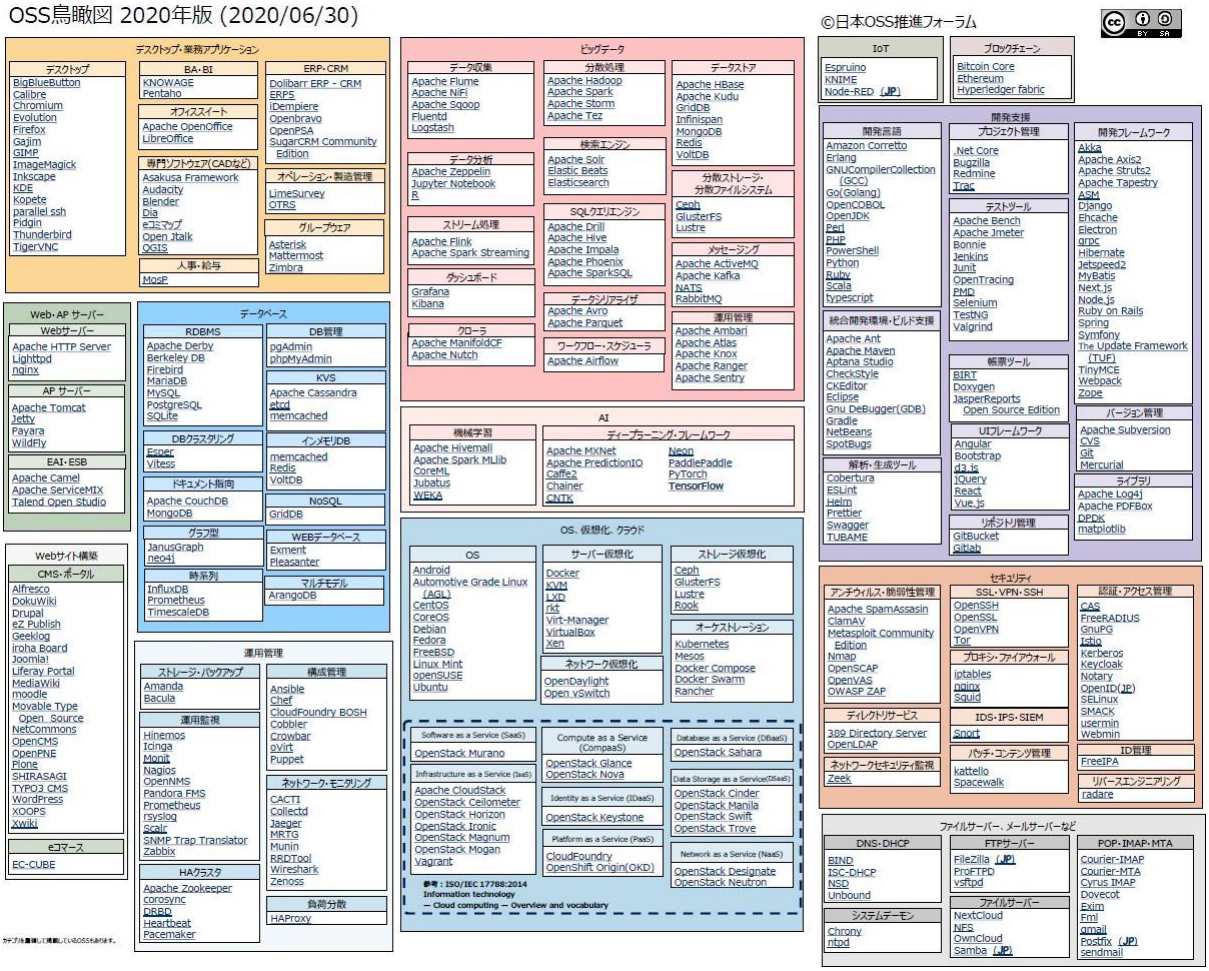


Figure 2.2-1: OSS bird's eye view, FY2020 (in Japanese)[6]

[4] Operating System

[5] Japan OSS Promotion Forum (in Japanese)
http://ossforum.jp/

[6] OSS Bird's Eye View (2020 version) (in Japanese)
http://ossforum.jp/node/1332

For example, in the area of OS, Linux, an OSS, is installed in a wide variety of hardware, including supercomputers, servers, personal computers, and embedded systems such as smartphones and home appliances. Linux is one of the most successful OSS projects, and its wide range of utilization makes it an indispensable software for products and services that support our daily lives. As mentioned earlier, this indicates that OSS is widely accepted because it offers many benefits to companies that develop systems and products for its features such as being able to be used, modified, and redistributed. The benefits are also returned to the companies and consumers who are the final users of the systems and products in terms of price, etc.

2.3. Advantages of OSS utilization

There are a wide range of advantages to using OSS. The main advantages are as follows:

(1) Cutting development costs and shortening development periods by improving development efficiency.

(2) Ensuring high stability, quality, and transparency.

(3) Creating new values through a wide variety of products and avoiding vendor lock-in.

The details of each merit are described below:

(1) Cutting development costs and shortening development periods by improving development efficiency

If the functions that developers need are already implemented in OSS, they can expect to reduce development costs and shorten the development period. In the ICT-related industry, where the competitive and business environment is changing rapidly, streamlining the development process can provide a huge advantage.

(2) Ensuring high stability, quality, and transparency

Based on the open source orientation, OSS has been improved by an unspecified number of users, and has high stability and quality required of software. As a result, OSS has a high level of stability and quality as software, and developers can use it with confidence because it has been used by many users. In addition, the source code is open to the public, making it possible to constantly check for illegal programs and vulnerabilities.

(3) Creating new values through a wide variety of products and avoiding vendor lock-in

Currently, there are many types of OSS, and many functions are available in OSS, which can create new value and greatly improve efficiency of existing operations, such as implementation of the latest technology using AI. OSS also makes it possible to avoid vendor lock-in[7].

[7] Adoption of products, services, systems, etc. that rely heavily on the proprietary technology of a

Because of the above advantages, many companies are developing systems and products that employ OSS. It is believed that this trend will continue to grow in the future.

particular vendor (manufacturer) makes it difficult to switch to similar products, services, systems, etc. provided by other vendors.

2.4. Points of attention in OSS utilization

While the utilization of OSS has many advantages, there are also several points that must be kept in mind. The main points to keep in mind are as follows:

(1) License compliance.

(2) A short life cycle (support period, etc.) and insufficient support.

(3) Use of OSS in the supply chain.

These points of attention are described in detail below:

(1) License compliance

Since each OSS software has its own license, users are required to comply with the license. Many OSS users are in charge of development and may not have sufficient knowledge of legal issues such as licensing. In such cases, events such as violations of OSS licenses, may occur without being noticed, and thus there can be corporate compliance risks occurring.

(2) A short life cycle (support period, etc.) and insufficient support

Compared to commercial software, OSS has a relatively short life cycle (support period, etc.) as software, and support may not be sufficient. Therefore, when bugs or software vulnerabilities are found, users need to deal with them on their own, and a certain level of skills and know-how is required for utilization.

(3) Use of OSS in the supply chain

The same OSS may be used not only by the one company but also by other companies in the supply chain of the company's products and system development. Even in such cases, it is necessary to identify the OSS used in deliverables, and to take the aforementioned measures to deal with licensing and bugs/software vulnerabilities in the same way as when the OSS is used by the company itself. Therefore, it is necessary to collect information on OSS used by each company in the supply chain in an appropriate manner.

Appropriate responses to these points of attention are very important for OSS utilization. The issues that may arise when appropriately addressing these points of attention will be discussed in Section 3.2.

2.5. Disputes and incidents related to OSS

To supplement the points mentioned in Section 2.4, the following provides some examples of past disputes and incidents related to OSS:

(1) A dispute related to OSS licensing: Example of in-flight entertainment software[8]

In March 2017, a competing company sued the developer of in-flight entertainment software in New York federal court for alleged licensing violations. The suing company, pointing out that the source code for the Linux-based software was not properly disclosed, demanded $100 million in damages, claiming that the case was not a negligent license violation, but a deliberate attempt to prevent competitors from developing similar software. The two companies settled the case in January 2018, but the number of damages has not been disclosed.

(2) An incident related to OSS vulnerabilities: Heartbleed[9] case[8]

In April 2014, it was announced that a vulnerability had been found in the Heartbeat extension of OpenSSL (an OSS library for the SSL/TLS[10] protocol). The Heartbeat extension maintains a TLS session connection even when no communication is taking place between devices and checks whether the other party is present. It was found that, by sending a modified Heartbeat request to a vulnerable version of an OpenSSL server, the server's memory data could be included in the response, leading to the compromise of the ID/password or private key of the SSL server certificate (Figure 2.5-1).

[8] The Task Force for Evaluating Software Management Methods, etc. toward Ensuring Cyber/Physical Security, 1st Meeting (in Japanese)
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/001_04_00.pdf

[9] This vulnerability was named "Heartbleed" because of the "Heartbeat" feature.

[10] SSL: Secure Sockets Layer TLS: Transport Layer Security
Both are a type of protocol for sending and receiving data over the Internet in encrypted form.

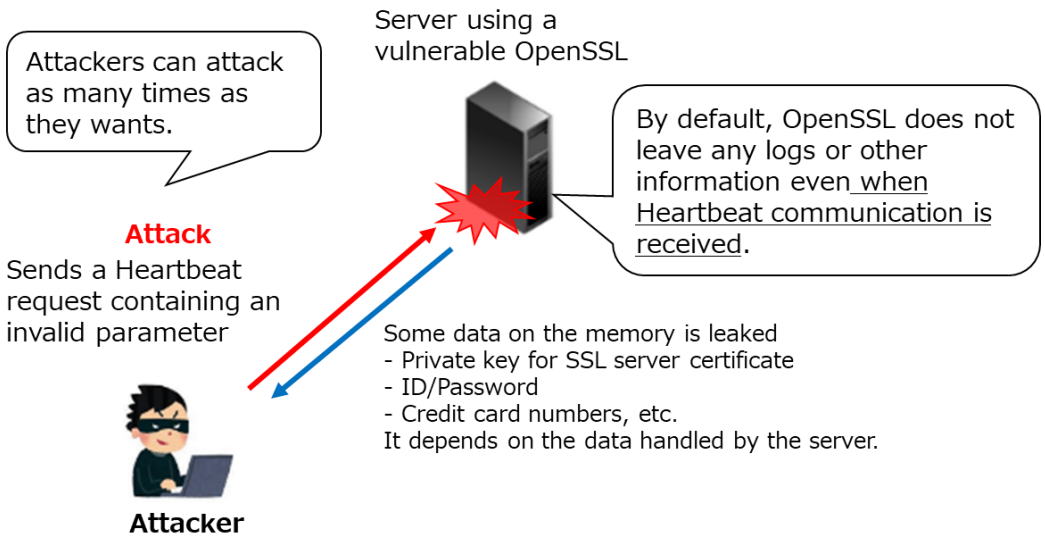


Figure 2.5-1: Image of an attack using the Heartbeat extension[11]

[11] Excerpts from the first document of the Task Force for Evaluating Software Management Methods, etc. toward Ensuring Cyber/Physical Security (in Japanese)
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/001_04_00.pdf

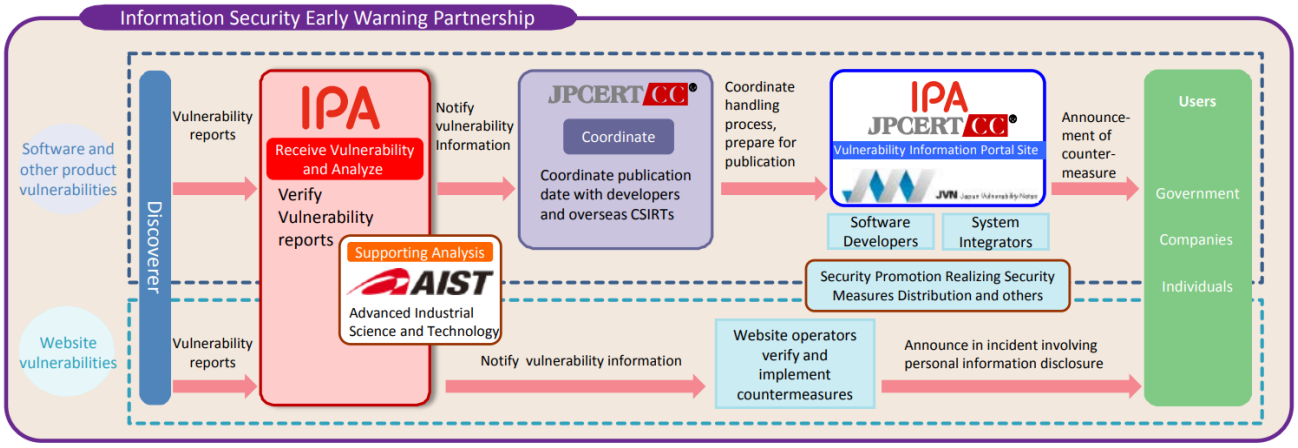
2.6. Major initiatives contributing to the utilization of OSS

2.6.1 Information Security Early Warning Partnership and Japan Vulnerability Notes

The main initiatives to support the use of OSS include the Information Security Early Warning Partnership and Japan Vulnerability Notes (JVN), jointly operated by Information-technology Promotion Agency, Japan (IPA) and JPCERT Coordination Center (JPCERT/CC). When OSS is used in products, services, or systems, and vulnerabilities related to the OSS are found, it is very important to respond to the vulnerabilities quickly and appropriately to maintain security. The Information Security Early Warning Partnership and JVN provide users with the information necessary to take a series of these actions.

The Information Security Early Warning Partnership is a framework designed to ensure the proper distribution of vulnerability-related information on software and other products in Japan, based on the Directive “the Rules for Handling Software Vulnerability Information and Others” issued by the METI in 2017. The IPA receives security (vulnerabilities) reports related to websites and software products discovered by the public or researchers, and JPCERT/CC coordinates with the discoverer of the vulnerability, the software product developer, and the website operator to take action (Figure 2.6-1).

JVN is an information portal site that discloses vulnerability information and other information discovered based on the Information Security Early Warning Partnership, together with the compiled countermeasures. In addition to the information based on the Information Security Early Warning Partnership, JVN also publishes vulnerability information in cooperation with overseas coordination organizations such as CERT/CC (Figure 2.6-2). Specifically, the information includes such matters as the damaged product and its version, the details of the vulnerability, analysis results, countermeasures provided by the product developer, and links to related information. The countermeasures may include not only patches but also workarounds.



* JPCERT/CC: Japan Computer Emergency Response Team Coordination Center AIST: National Institute of Advanced Industrial Science and Technology

Figure 2.6-1: Framework for the Information Security Early Warning Partnership[12]

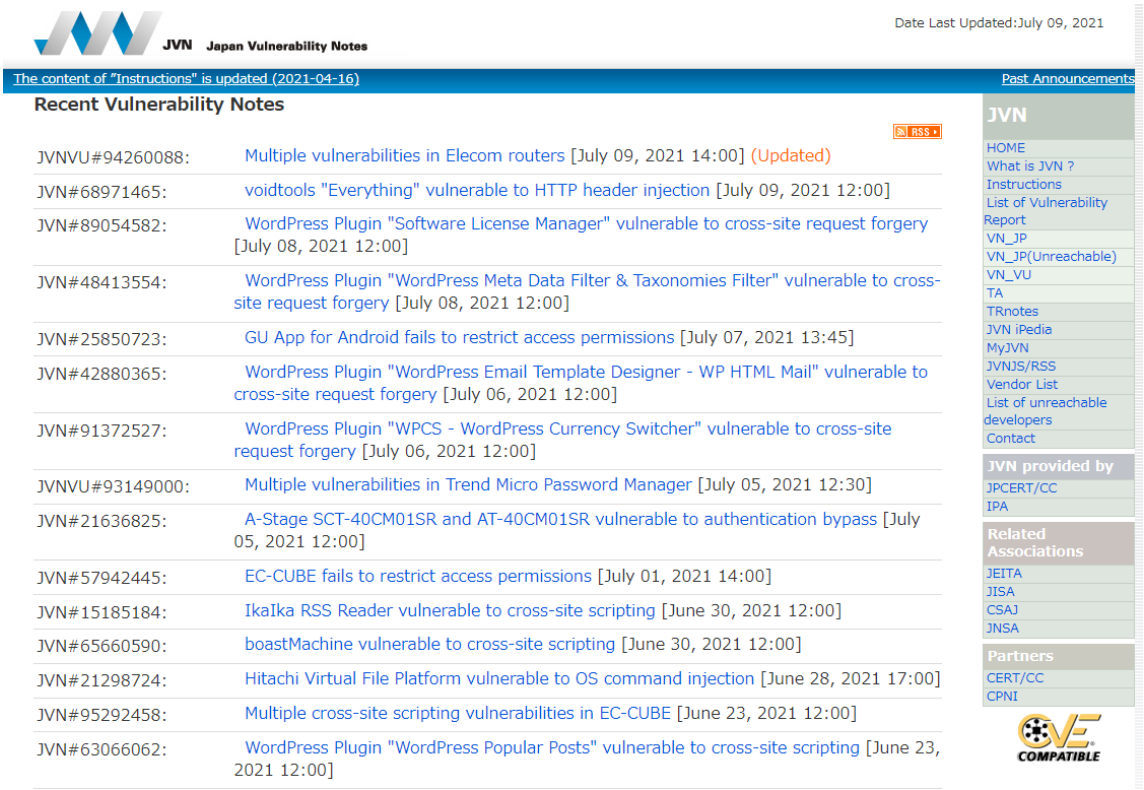


Figure 2.6-2: JVN Home Page[13]

[12] Excerpt from Introduction to the Information Security Early Warning Partnership https://www.ipa.go.jp/files/000044732.pdf

[13] Excerpts from the Japan Vulnerability Notes (JVN) website: http://jvn.jp/en/

2.6.2 Open Source Guide for Enterprises (Linux Foundation)

The TODO Group, under the Linux Foundation, shares knowledge and experience of OSS utilization at member companies and supports them in solving problems with product and service development.

The "Open source best practices for the enterprise" is a guidebook that collects OSS-related efforts of companies. This guidebook consists of the following 12 guides under 2 themes: "Running an Open Source Program Office" and “Managing an Open Source Project in Your Organization”[14].

<Running an Open Source Program Office>

- Creating an open source program.
- Tools for managing open source programs.
- Measuring your open source program’s success.
- Recruiting open source developers.
- Participating in open source communities.
- Using open source code.

< Managing an Open Source Project in Your Organization >

- Starting an open source project.
- Improving your open source development impact.
- Open source reading list.
- Winding down an open source project.
- Building leadership in an opens source community.
- Setting an open source strategy.

In addition, the Linux Foundation has also published other useful guides and white papers, including “Enterprise Open Source: A Practical Introduction"[15], which explains

[14] Open Source Guide for Enterprises
https://www.linuxfoundation.org/resources/open-source-guides/

[15] Enterprise Open Source: A Practical Introduction

a practical approach to developing an OSS utilization strategy, and "Software-defined Vertical Industries: Transformation through Open Source"[16], which introduces advanced examples of OSS use in various industries.

https://www.linuxfoundation.org/resources/publications/enterprise-open-source-a-practical-introduction

[16] Software-defined vertical industries: transformation through open source https://www.linuxfoundation.org/resources/publications/software-defined-vertical-industries-transformation-through-open-source/

3. Organizing the Case Study

3.1. Organizing Commercial Flow and stakeholders surrounding OSS

The OSS supply chain is formed by various stakeholders (Figure 3.1-1). The commercial flow of OSS starts with the development and provision of OSS by development stakeholders such as the OSS development community and companies participating in the community. After that, it goes through intermediate layers, such as distributors who distribute OSS as commercial packages, final product manufacturers who develop products and systems using OSS, suppliers, system integrators[17], and service providers who provide cloud services using OSS. Finally, companies and consumers as end users of products and end users of systems pay for products and systems and enjoy their benefits.

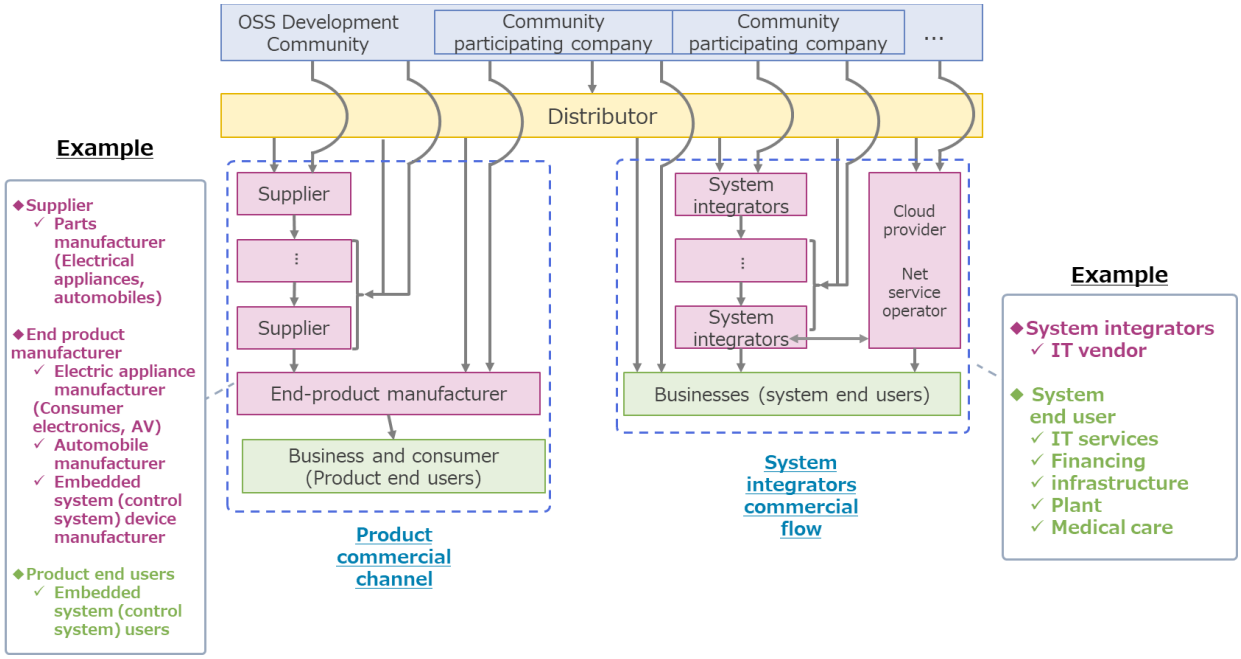


Figure 3.1-1: Commercial Flow of OSS and Stakeholders[18]

The OSS commercial flow can be roughly divided into the commercial flow that occurs mainly in order to supply final products (product commercial flow) and the commercial flow that occurs for system introduction in companies (system integrators commercial

[17] Enterprises that undertake the construction and operation of information systems for companies and governments in bulk.

[18] Compiled based on interviews, etc.

flow). This Collection introduces the efforts of post-distributor stakeholders in the product commercial flow and the system integrators commercial flow. The outline of each commercial flow and the main stakeholders are as follows:

- Product commercial flow

It is a commercial flow formed by end-product manufacturers and suppliers who supply components to end-product manufacturers. The product is ultimately purchased by the end-user of the product. The suppliers form a supply chain, which may have multiple layers of component supply. OSS is widely used in product development by end-product manufacturers and in component development by suppliers at each stage of the supply chain. The main stakeholders in the product commercial flow are as follows:

  - Supplier:
    Suppliers are manufacturers that supply components to end-product manufacturers. In the OSS commercial flow, they are manufacturers that produce and deliver components (products) that incorporate software, including OSS. Depending on the end product, there may be unique or specialized suppliers (e.g., auto parts manufacturers, electronic parts manufacturers).
  - End-product manufacturer:
    These are manufacturers that manufacture final products using components developed by themselves and parts supplied by suppliers in the supply chain (e.g., automobile manufacturers, electronics manufacturers). In some cases, OSS is used for in-house development, while in other cases, OSS is used for parts supplied by suppliers.
  - Product end user:
    All organizations and individuals who purchase and use products manufactured by end-product manufacturers are product end-users.

- System integrators commercial flow

This is a commercial flow in which system integrators develop and deliver business systems, etc. in response to orders from system end users (e.g., companies). In some cases, system integrators form a supply chain and carry out development through multilayered outsourcing, while combining cloud services and other services to build the final system. OSS is widely used by system integrators at each stage of the supply chain and by each service provider. The main stakeholders in the system integrators commercial flow are as follows:

  - Service providers:

There are companies that provide cloud services and Internet services to system integrators and system end users, and system integrators and system end users use these services to build systems.

- System integrators:
  The system integrators include businesses that provide information system integration and businesses that develop and build information systems on consignment and deliver them. There are also companies that have their own IT products and provide them while undertaking development on consignment. Since each industry has similarities in the types of business systems used and the characteristics required, there are system integrators and system developers that are unique or specialized for each industry (e.g., system integrators for the financial industry, system integrators for the manufacturing industry).
- System end user:
  System end users include companies, government agencies, municipalities, and other organizations that use business systems.

- Internet service commercial flow

This is a commercial flow in which an Internet service provider develops a system to provide a service and provides the service via the Internet. Some Internet service providers develop final systems and provide services, while combining cloud services and other services. Internet service providers widely utilize OSS to provide services on a BtoB or BtoC basis through subscriptions or free of charge. Compared with those in the product commercial flow or the System integrators commercial flow, Internet service providers are able to respond quickly to business risks such as licensing violations. The Internet service commercial flow involves the following stakeholders:

- Service provider:
  There are providers that offer cloud services, internet services, etc. to Internet service providers, who in turn leverage those services to offer their services.
- Service end user:
  All organizations and individuals who use services provided by the Internet provider are service end users.

3.2. Extraction of problems with OSS utilization

3.2.1 Organizing issues for the Software Task Force on software management to ensure cyber-physical security

The Software Task Force has organized issues related to the utilization of software including OSS and a management method to ensure its security as "direction of consideration" based on past cases related to management, vulnerability response, and licensing of software in Japan and overseas, as shown in Figure 3.2-1.

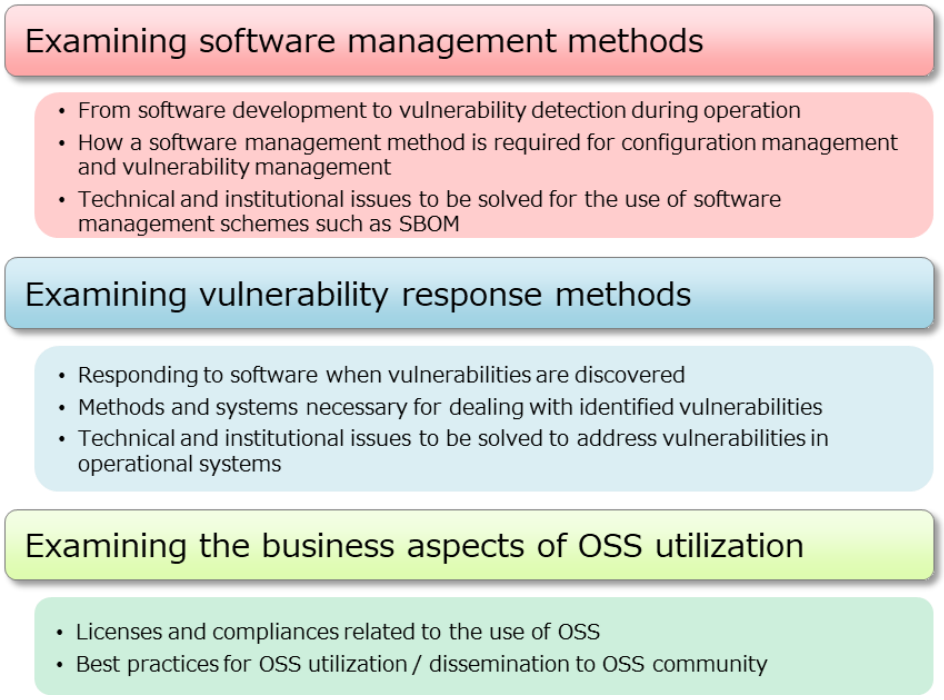


Figure 3.2-1: Direction of Consideration by the Task Force [19]

The Software Task Force recognized the importance of appropriate OSS management in responding to OSS vulnerability and licenses. The task force also identified, as future issues, the granularity of OSS management and how to tackle it as an organization. It emphasizes the need to promote the development of systems and structures for OSS management. As a response to these issues, acknowledging the importance of sharing

[19] Excerpts from the third document of the Task Force for Evaluating Software Management Methods, etc. toward Ensuring Cyber/Physical Security (in Japanese)
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_03_00.pdf

knowledge of each company's initiatives for OSS management, the task force has a common understanding that the creation of case studies on management methods for OSS utilization and its security assurance is highly effective.

3.2.2 Perspectives on issues related to OSS utilization

The perspectives of issues related to the utilization of OSS and its management method to ensure its security were organized based on the discussions of the Software Task Force and interviews with Task Force members (experts and companies).

In this Collection, the main issues that OSS stakeholders face when utilizing OSS are classified from the following perspectives:

- Selection Evaluation.
- Licensing.
- Vulnerability Response.
- Maintenance and Quality Assurance.
- Supply Chain Management.
- Personal Competence and Education.
- Organizational Structure.
- Community Activities.

The figure below (Figure 3.2-2) shows the main issues for each of the above perspectives. These perspectives is categorized into the following three perspectives: the perspective of issues that occur in the selection and management processes for OSS utilization ("process perspective"); the perspective of issues that occur in improving the literacy of human resources and organizations involved in OSS and in system development ("people/organization perspective"); and the perspective of issues related to contribution to and expansion of the OSS ecosystem, such as OSS community activities ("community perspective").

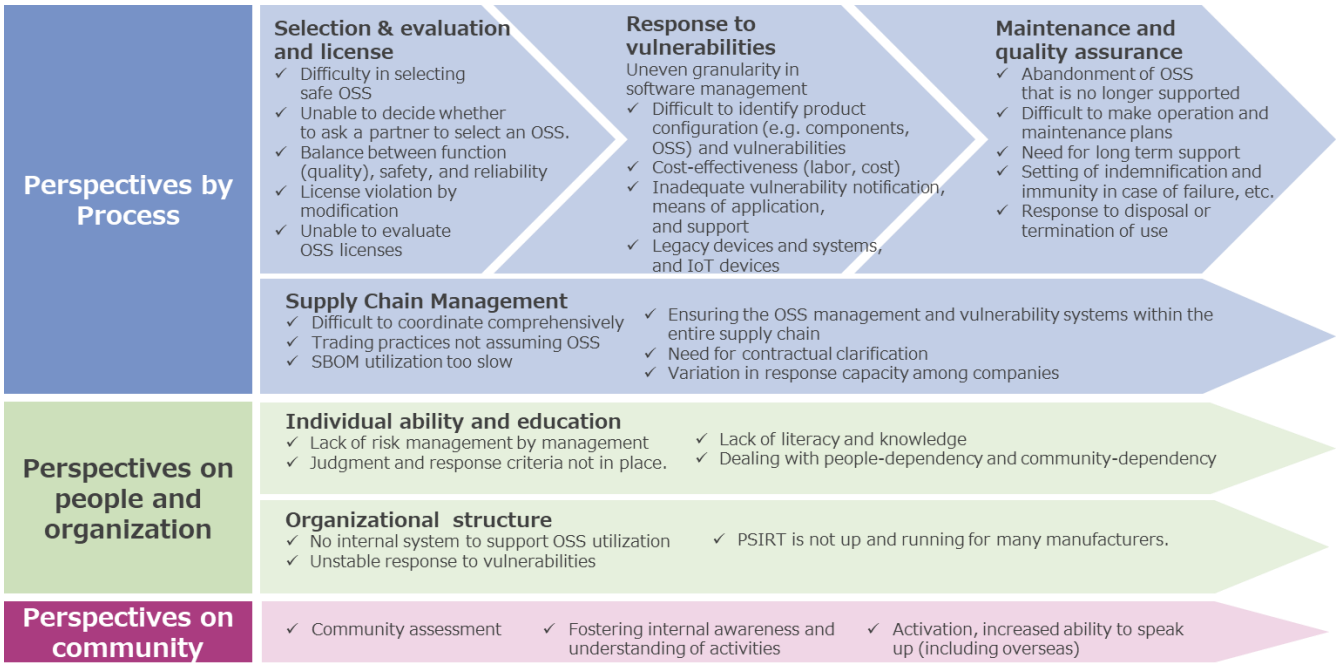


Figure 3.2-2: Perspectives on OSS and their issues (an example) [20]

[20] Compiled based on interviews.

3.3. List of featured cases

This Collection contains 20 examples from domestic companies collected through interviews and three examples from overseas collected through a survey of published literature.

Based on the organization of Commercial Flow and stakeholders surrounding OSS in Section 3.1 and the organization of OSS issue perspectives in Section 3.2, the following table (Table 3.3-1) shows the correspondence of each case in this Collection. The details of each case are described in the next and subsequent sections. In Table 3.3-1, each case is assigned a related perspective, such as "L1" and "S1," and it is possible to move to the description of the initiatives for the corresponding perspective. It does not exhaustively show all approaches taken by each company.

Table 3.3-1: List of featured cases

Commercial flow	Stakeholders	Featured company	Perspectives relevant to the case							
			Selection Evaluation (S)	Licensing (L)	Vulnerability Response (V)	Maintenance and Quality Assurance (M)	Supply Chain Management (S)	Personal Competence and Education (P)	Organizational Structure (O)	Community Activities (C)
Company surveyed by interview										
Product commercial flow	End-product manufacturers	Toyota		L1			S1			C1
		Sony		L2-1 L2-2	V2		S2		O2	C2
		Olympus		L3			S3	P3	O3	C3
		Hitachi		L4						C4
		Omron			V5-1 V5-2		S5	P5	O5-1 O5-2	
		Toshiba	S6	L6	V6	M6	S6	P6	O6	C6
		Mitsubishi Electric Information Systems (MDIS)	S16	L16	V16	M16				C16-1 C16-2
	Supplier	DENSO		L7	V7		S7			

Commercial flow	Stakeholders	Featured company	Perspectives relevant to the case							
			Selection Evaluation (S)	Licensing (L)	Vulnerability Response (V)	Maintenance and Quality Assurance (M)	Supply Chain Management (S)	Personal Competence and Education (P)	Organizational Structure (O)	Community Activities (C)
Product commercial & System integrators commercial flow	System integrators & End product manufacturer	Fujitsu	S8	L8	V8-1 V8-2	M8	S8	P8	O8-1 O8-2	C8
		NEC	S9-1 S9-2	L9-1 L9-2	V9-1 V9-2	M9		P9	O9-1 O9-2	
System integrators commercial flow	System integrators	NTT			V10				O10	
		Company A	S11			M11				C11
	System integrators & End user	Company B			V12			P12		
	End-user	Sompo Japan Insurance		L13	V13			P13		
		Visional Group			V14					
		Cybozu	S15	L15	V15			P15	O15	C15
		OSSTech		L17	V17		S17			
		SCSK	S20		V20-1 V20-2		S20	P20	O20	
Internet service provider		Yahoo Japan	S18	L18	V18	M18	S18	P18	O18	C18
		LaKeel	S19	L19	V19				O19	
Company surveyed by literature review										
System integrators commercial	Service provider	Microsoft			V21					
	End user	Zalando		L22						

Commercial flow	Stakeholders	Featured company	Perspectives relevant to the case							
			Selection Evaluation (S)	Licensing (L)	Vulnerability Response (V)	Maintenance and Quality Assurance (M)	Supply Chain Management (S)	Personal Competence and Education (P)	Organizational Structure (O)	Community Activities (C)
flow										
Others (survey results)		Census II Project			V23					

4. Use Case Examples (Interview Survey)

4.1. Toyota Motor Corporation: Understanding software usage in the supply chain

■ Company information

Head Office	Toyota, Aichi-ken
Industry	Manufacturing (Automobiles)
Employees	370,870（as of the end of March 2019）
Commercial Flow	Product commercial flow/end product manufacturer
Perspectives	[Licensing] [Supply Chain Management] [Community Activities]

■ Essence of this case

- Efforts are being made to clarify software management rules to reduce the risk of license violations and to improve the ability of the entire supply chain to respond to OSS-related security vulnerabilities.
- In concluding the guideline on software use, we sought understanding from suppliers by emphasizing the importance of OSS compliance.
- We adopted the SPDX Lite format for providing the list of software to be used by suppliers, in consideration of operational aspects.
- By sharing and discussing internal initiatives related to OSS management in community activities, an open PDCA cycle is formed, contributing to raising the level of OSS compliance in the entire supply chain.

■ Background and issues

In the automotive industry, there are not only end-product manufacturers but also multilayered suppliers, and many companies form a supply chain. Each company in the supply chain uses OSS, and in order to comply with the OSS license, it is necessary to accurately identify the usage status. However, since the management granularity of software used and the governance system are different among companies within the supply chain, how to integrate them into a unified operation is an issue.

■ Initiatives

<[Licensing (L1)] [Supply Chain Management (S1)] Knowing the status of software (including OSS) use in the supply chain>

Toyota is working on the development of internal processes, authorities, and organizational structures such as operational rules, audit rules, and forms related to OSS compliance under the direct control of the company-wide organization. In particular, the following two initiatives are being implemented for suppliers (Tier 1[21] to understand the software used in the supply chain (Table 4.1-1).

(1) Agreeing with each supplier on guidelines for software to be used.

(2) When supplying parts, the engineering department of the company and each supplier agree on the operating rules for reporting the software used.

Table 4.1-1: Specific Items in Guidelines and Operation Rules [22]

Guidelines (Agreement on basic rules between companies)	● The role of OSS compliance in the supply chain ● Demarcation of responsibility ● How to handle each license ● Agreement to provide a list of software used
Operating rules (Agreement on working-level operating rules)	● Format of the list ● Workflow ● Timing of the report ● Contact

The details of each initiative are described below:

(1) Agreeing with each supplier on guidelines for software to be used

The companies agree on guidelines regarding the role of OSS compliance in the supply chain, as well as the provision of a list of software to be used and licenses to be paid attention to. Although there had been some business practices in the automotive industry to avoid providing more information than necessary to suppliers, the importance of compliance, especially in the area of licensing, was emphasized in the process of agreeing on the guidelines.

[21] Manufacturers that supply components directly to end-product manufacturers.

[22] Based on materials from Open Compliance Summit 2019: https://static.sched.com/hosted_files/ocs19/d3/Open%20Source%20Compliance%20in%20Supply%20Chains.pdf

(2) When supplying parts, the engineering department of the company and each supplier agree on the operating rules for reporting the software used

Based on the aforementioned guidelines, the operational rules regarding the provision of the list of software used in the supplied parts are agreed upon at the working (engineering) level for each supply relationship (project) with each supplier. Specific rules are established for each project on such matter as the scope of application of the rules (e.g., products, services), the method of reporting the list of software used (e.g., who to report to whom, timing of reporting, including reporting at the development stage), the format, copyright information required by the license, and the specific method of disclosure of source code (e.g., publication in the manual, publication on the Web). The format, copyright information required by the license, and specific methods of handling source code disclosure (e.g., posting in the manual, publication on the Web) are specified for each project. As a result of considering the ease of handling by each supplier, Toyota has adopted SPDX Lite, a format discussed on OpenChain[23]. SPDX Lite is a simplified version of SPDX[24] and can be managed using Excel or other formats (Figure 4.1-1). The information to be listed and the rules for listing it in SPDX Lite are under continuous review for improvement in order to achieve the best possible operation.

SPDX Lite field example

- Package Name
- Package SPDX Identifier
- Package Version
- Package File Name
- Package Download Location
- Files Analyzed
- Package Home Page
- Concluded License
- Declared License
- Comments on License
- Copyright Text
- Modified Status
- Package Comment
- License Identifier

●A part of SPDX Lite Sample

SPDX Lite section no.	L2.1	L2.2	L2.3	L2.4	L2.5	L2.6	L2.7	L2.8	L2.9
SPDX section no.	3.1	3.2	3.3	3.4	3.7	3.8	3.11	3.13	3.15
Tag	PackageName	Package SPDX Identifier	Package Version	PackageFileName	PackageDownloadLocation	Files Analyzed	PackageHomePage	Concluded License	Declared License
	LibXML2		2.99	libxml2-2.9.9.tar.gz	ftp://xmlsoft.org/libxml2/	FALSE	http://xmlsoft.org/	MIT	MIT
	PCRE		8.4343	pcre-8.43.tar.gz	ftp://ftp.pcre.org/pub/pcre/	FALSE	https://www.pcre.org/	BSD-3-Clause	BSD-3-Clause
	Zlib (1.2.3)		1.2.11	zlib-1.2.11.tar.gz	https://www.zlib.net/	FALSE	https://www.zlib.net/	Zlib	Zlib
	cURL (7.41.0)		7.66.0	curl-7.66.0.tar.bz2	https://github.com/curl/curl/releases	FALSE	https://curl.haxx.se/	MIT	MIT

Figure 4.1-1: SPDX Lite Format (Sample)[25]

[23] A project of the Linux Foundation. It aims to create and disseminate industry standards to achieve OSS compliance throughout the supply chain. https://www.openchainproject.org/

[24] The software package data exchange format (SPDX: Software Package Data Exchange) is a standard format for exchanging components, licenses, copywrites and other information related to software packages supported by the Linux Foundation. It is a standard format for exchanging information such as components, licenses and copywrites related to software packages supported by the Linux Foundation.

[25] Excerpts from materials provided by Toyota Motor Corporation.

As a result of the above efforts, the importance of software management has been recognized and its management rules have been clarified, enabling the reduction of variation in the quality of software management among suppliers. This has not only reduced the risk of license violations but has also enhanced the ability of the entire supply chain to respond to security vulnerabilities related to OSS.

<[Community Activities(C1)] Activities in the community to promote OSS utilization>

Toyota has been contributing to the standardization of these efforts, while endeavoring to understand software usage in the supply chain. One example is its activities for OpenChain.

OpenChain is a project of the Linux Foundation that aims to create and disseminate industry standards to achieve OSS compliance throughout the supply chain. Many companies from Japan are participating in the project, mainly manufacturers of electrical appliances and information and communication equipment. The main deliverables[26] of the project (Figure 4.1-2) are the following three items:

(1) Specification: Defines the requirements of the compliance program that a company should establish within its organization.

(2) Conformant: A certification can be obtained by answering a web questionnaire on whether or not the system conforms to the specifications. In principle, self-certification is used, but third-party certification is also available.

(3) Curriculum: A collection of educational materials that can be used within a company for conformance to specifications.

[26] Based on these deliverables, Toyota has established the aforementioned internal system for OSS compliance.

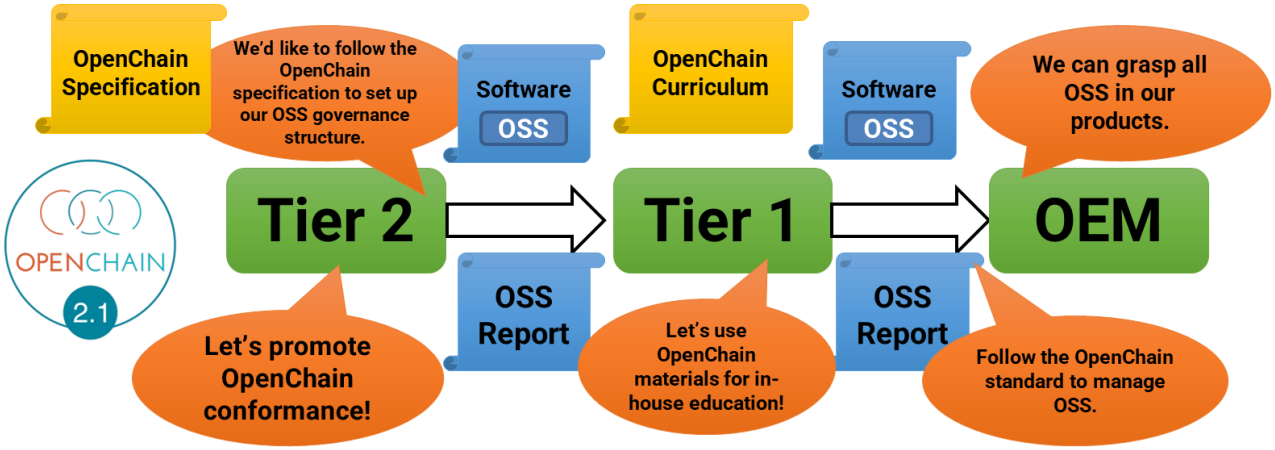


Figure 4.1-2: Image of the use of OpenChain deliverables[27]

The specification in (1) was internationally standardized as ISO/IEC 5230 in December 2020. It is expected that more companies will obtain certification of conformance to the specifications, as recognition will increase with international standardization. Since before the international standardization, Toyota has been working in its OSS management efforts to comply with the OpenChain specifications. In addition, Toyota was the world's first to announce its conformance to the specifications (self-certification), after international standardization. Since the number of departments that comply with the specifications is currently limited to a few, it is seeking to expand the use of this technology throughout the company.

OpenChain has several working groups (WG), and Toyota plays a central role and contributes to the Japan WG[28] and the Automotive WG[29] (Table 4.1-2). The Japan WG discusses SPDX Lite, while seven other sub-working groups (SWGs) are active under their respective themes. The Automotive WG shares best practices and promotes awareness of the importance of OSS compliance.

Table 4.1-2: Summary of each WG[30]

WG name	OpenChain Japan WG	OpenChain Automotive WG
Date of	December 2017	July 2019

[27] Excerpts from materials provided by Toyota Motor Corporation. Toyota Motor Corporation uses SPDX Lite for the SBOM (Software Bill of Materials) shown in the figure.

[28] The WG is led by the Japanese companies participating in The OpenChain Project.

[29] The WG is mainly composed of automobile-related companies participating in The OpenChain Project.

[30] Compiled based on the documents and hearings from the 3rd meeting of the Task Force for Evaluating Software Management Methods, etc. toward Ensuring Cyber/Physical Security (in Japanese)

WG name	OpenChain Japan WG	OpenChain Automotive WG
establishment		
Participating companies	More than 70 domestic companies, including Toyota, Sony, and Hitachi.	Toyota, Bosch, Panasonic, etc., (including 12 domestic and overseas automakers)
Objective	To create a place to exchange information in Japanese about issues and solutions unique to Japanese companies regarding OSS compliance.	Three objectives have been established: • To share best practices within the automotive industry. • To review automotive industry standards for OSS supply chain management. • To communicate the importance of OSS compliance to the industry.
Activities	Establishing standards, providing support, and translating relevant information for companies and organizations to comply with open source licenses. In addition, setting themes at the SWG level for promoting their own activities.	Introductions of each company's initiatives are conducted among participating companies. In FY2020, Toyota is planning to create a collection of practices.

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_04_00.pdf

WG name	OpenChain Japan WG	OpenChain Automotive WG
SWG	• Planning SWG • FAQ SWG • Leaflet to Supplier SWG • Education material for roles SWG • License information exchangeSWG* • Tooling SWG • Promotion SWG *Discussion made on SPDX Lite	–

The results of each participating company's OSS compliance efforts will be fed back to The OpenChain Project and discussed to create better deliverables. In this way, an open PDCA cycle is formed by each participating company.

The OpenChain Project also includes suppliers to the automotive industry. Therefore, it is not the intention of the end-product manufacturers alone to establish industry standards. Therefore, it is easy to obtain understanding from the suppliers, and it is expected to expand in the future.

Toyota is improving the accuracy of its subsequent efforts by implementing the aforementioned open PDCA cycle for the results of its own efforts. At the same time, the benefits of the PDCA cycle are spreading throughout the entire supply chain, which has the effect of raising the level of OSS compliance efforts in the entire supply chain (Figure 4.1-3).

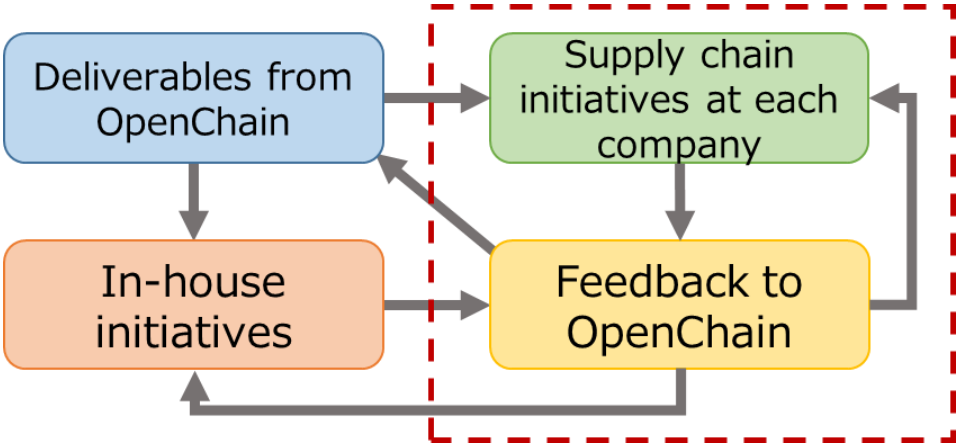


Figure 4.1-3: Open PDCA Cycle in OpenChain[31]

In addition to the OpenChain activities, Toyota Motor Corporation is also implementing the following activities to promote the utilization of OSS:

(1) Joint development of tools to reduce the burden of OSS license interpretation.

(2) Activities to promote SBOM at exhibitions, etc.

The details of each activity are described below:

(1) Joint development of tools to reduce the burden of OSS license interpretation

Toyota, Hitachi and Hitachi Solutions have jointly developed the "OSS License Simple Viewer," a tool to reduce the burden of interpreting OSS licenses. While some OSS licenses are written in English and are complicated, this tool allows users to easily understand the contents of the license by simply entering the license type and the use of the OSS and displaying the responsibilities and disclaimers of the license. It is also possible to customize the responsibilities and disclaimers displayed in line with the license interpretation of each company.

The tool itself made open[32] as an OSS in order to have more companies use it and promote the use of OSS. It is expected that this tool will be improved into a more value-added tool in coordination with the OSS management system at companies.

(2) Activities to promote SBOM at exhibitions, etc.

Toyota Motor Corporation is also contributing to activities to promote the

[31] Compiled based on interviews.

[32] OSS License Simple Viewer
https://github.com/OLSV-oss/OSSLicenseSimpleViewer

necessity of SBOM creation for OSS utilization at exhibitions and other events. As an example, at CES2020[33] held in January 2020, a demonstration of SPDX Lite creation was held at the booth of Automotive Grade Linux, a Linux Foundation project supported by Toyota, as part of the activities of the OpenChain Automotive WG. As part of its activities, the OpenChain Automotive WG demonstrated the creation of SPDX Lite. It demonstrated how easy it is to create SPDX Lite using a free tool and tried to raise awareness of the use of SBOM among visitors. Toyota is also involved in other activities, such as promoting the importance of SBOM at seminars of companies that provide SBOM creation tools. Through such events, the automaker intends to continue disseminating information on OSS utilization, including the necessity of SBOM management.

[33] Electronic equipment trade show held in Las Vegas, USA, every January.

4.2. Sony Group Corporation: Proactive initiatives by each business unit

■ Company information

Head Office	Minato-ku, Tokyo
Industry	Electrical equipment
Employees	111,700（as of the end of March 2020）
Commercial Flow	Product commercial flow/end product manufacturer
Perspectives	[Licensing] [Vulnerability Response] [Supply Chain Management] [Organizational Structure] [Community Activities]

■ Essence of this case

- OSS management is left to the discretion of each business unit, while ensuring quality in compliance with established standards, enabling Sony to follow up on a diverse range of products.
- In terms of OSS license compliance, Sony has established a cross-organizational response system and has been participating in the OpenChain Japan WG[34].

■ Background and issues

Sony has a diverse product lineup and has established processes and rules to ensure that each business unit can respond optimally to its own product market. In OSS licensing and software management, each business unit must flexibly consider and adopt methods to ensure product quality while maintaining the competitiveness of each product.

■ Initiatives

<[Licensing (L2-1)] [Vulnerability Response (V2)] Flexible response by each business unit in OSS management (product security)>

Sony has recognized the merits of OSS utilization and has been using OSS since around 2000. Initially, the company started with initiatives necessary for OSS license compliance, and then implemented OSS management (product security) while utilizing the knowledge gained from these initiatives.

[34] The specific efforts of the OpenChain Japan WG are described in the case study of Toyota Motor Corporation.

As an initiative for product security, each business unit thoroughly understands the OSS used in each product, manages the list, and periodically updates the list based on the company-wide Quality Management System (QMS)[35].

In addition, when OSS vulnerabilities are discovered, Sony PSIRT[36] takes the lead in handling[37] them. A product security initiative based on the QMS is operated at the discretion of each business unit according to its situation.

This is because the most efficient way to do this is to flexibly choose a method that best suits different development processes and resources held by the products of each business unit. This makes it possible to follow up on Sony's diverse product lines while ensuring the quality of information in the QMS.

<[Licensing (L2-2)] [Supply Chain Management (S2)] [Organizational Structure (O2)] [Community Activities (C2)] System and community activities related to OSS license compliance>

In 2010, Sony established a cross-organizational response organization for the OSS license compliance system, which has been in place to date. The internal committee was formed with members selected from the corporate divisions of legal affairs, intellectual property, public relations, and quality control, as well as from almost all business divisions and overseas business bases, to promote the OSS license compliance initiative (Figure 4.2-1). In this way, various in-house know-how can be utilized, and flexible development in line with the situation of each business unit can be expected as business units are decentralized in promoting this initiative.

[35] Quality Management System: A system for managing and supervising the quality of manufactured goods and services to be provided, intended to achieve customer satisfaction and continuous improvement in the organization's activities centered on quality management.

[36] Product Security Incident Response Team: An organization that seek to improve the security level of products and services manufactured and developed by Sony and respond to incidents when they occur. The Sony PSIRT works closely with each business unit to provide opportunities for communication with related parties on a regular basis in order to respond to various product groups across the company.

[37] Collects information on product vulnerabilities, serves as a contact point, makes decisions on responses, and communicates to relevant departments.

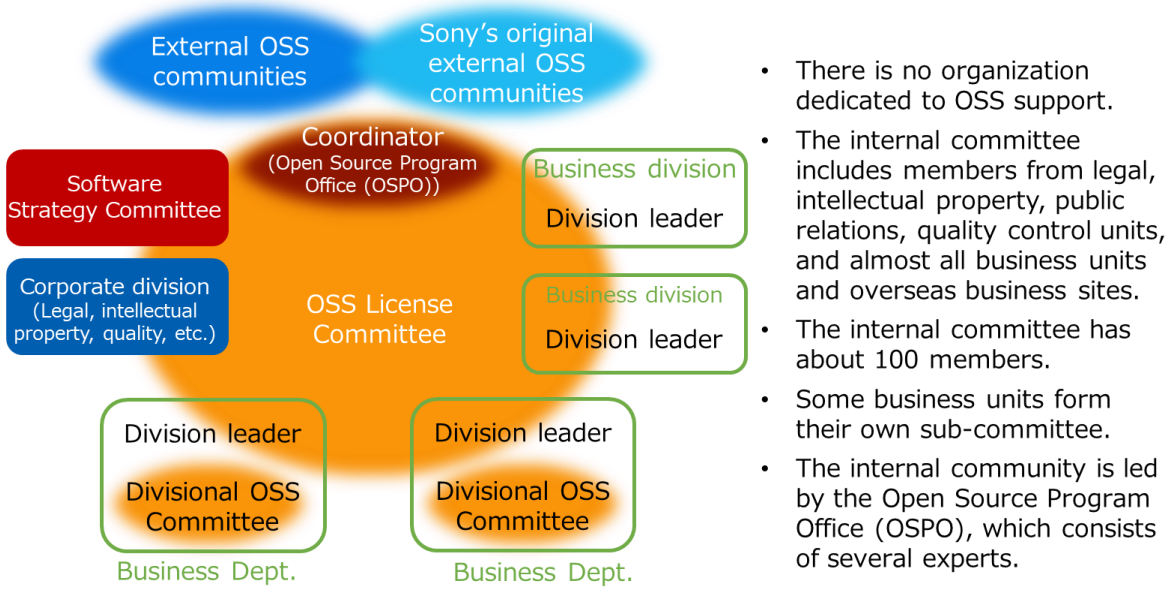


Figure 4.2-1: Image of a cross-organizational structure for license handling[38]

As a specific effort in promoting OSS license compliance, Sony is strengthening its supply chain management by leading the activities of the OpenChain Japan WG as a platinum member. The company is keenly aware of the need to properly identify the OSS contained in software provided by suppliers of Sony products, such as SoC[39] vendors and OEM[40]/ODM[41] vendors. In the past, Sony has had a particularly difficult time knowing the OSS usage status of overseas suppliers. After struggling to understand the status of OSS use by overseas suppliers, Sony concluded that it would be more effective to behave in the OpenChain Japan WG rather than as Sony alone to encourage suppliers to take action.

For example, the OpenChain Japan WG will translate its deliverables (e.g. educational materials on OSS license compliance) not only into Japanese, but also into English, Chinese (traditional and simplified), and Vietnamese.

---

[38] Prepared based on materials from the OpenChain Japan WG meeting: https://wiki.linuxfoundation.org/_media/openchain/openchainjwg_organization_lt_20180419_jpen_.pdf

[39] System on a Chip: A design method in which many or all of the functions necessary for the operation of a system are implemented on a single semiconductor chip.

[40] Original Equipment Manufacturing (Manufacturer): The manufacture of products under another company's brand or a company who engage in such manufacture.

[41] Original Design Manufacturing (Manufacturer): The design and manufacture of products under another company's brand or a company who engages in such design and manufacture.

In addition, the OpenChain Japan WG continues to actively communicate with overseas manufacturers and suppliers (Figure 4.2-2). As a result, similar WGs have been formed in Korea, China, India, Germany, and the UK, as the awareness of OSS compliance is increasing. In this context, changes are beginning to appear, including overseas suppliers showing their understanding of measures such as the disclosure of software used.

Although the activities of the OpenChain Japan WG are currently focused on major companies, the WG is expected to further enhance its effectiveness by expanding its activities to include small and medium-sized companies.

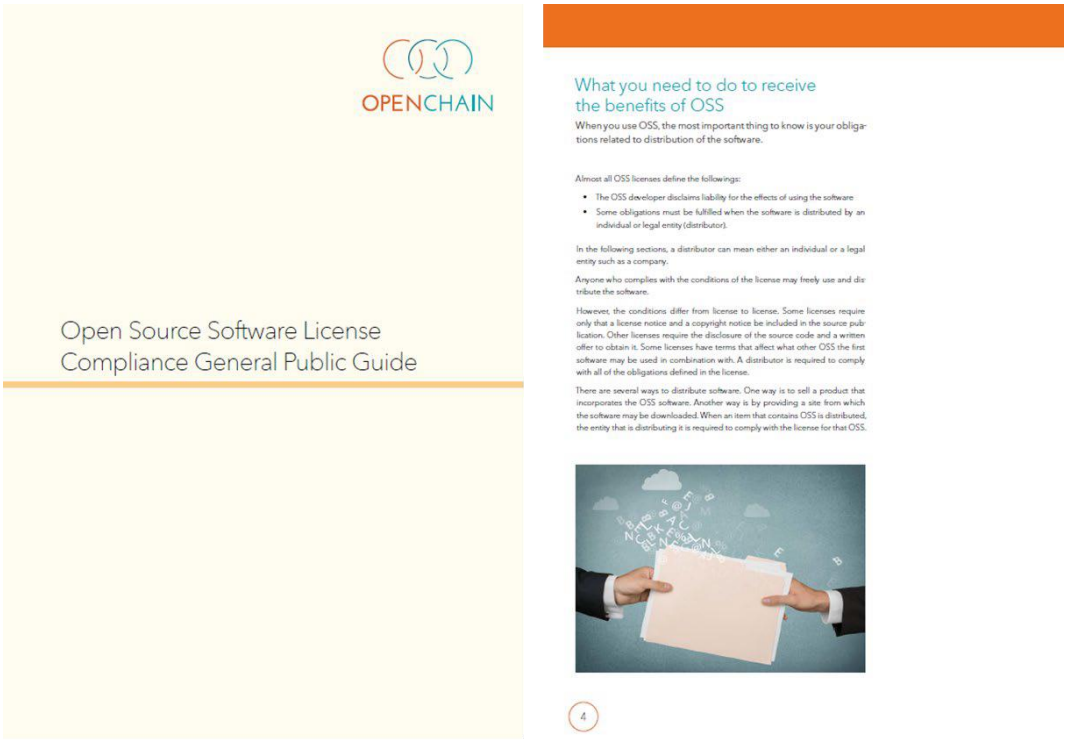


Figure 4.2-2: Leaflet to promote the importance of OSS license compliance [42]

[42] Excerpts from the third document of the Task Force for Evaluating Software Management Methods, etc. toward Ensuring Cyber/Physical Security (in Japanese)
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_04_00.pdf
General Public Guide to Open Source Software License Compliance:
https://github.com/OpenChain-Project/Curriculum/tree/master/supplier-leaflet

4.3. Olympus Corporation: Company-wide initiatives triggered by near-miss events

■ Company information

Head Office	Shinjuku-ku, Tokyo
Industry	Precision equipment
Employees	35,174 （as of the end of March 2020）
Commercial Flow	Product commercial flow/end product manufacturer
Perspectives	[Licensing] [Supply Chain Management] [Personal Competence and Education] [Organizational Structure] [Community Activities]

■ Essence of this case

- Past near-miss events have led to the development of a company-wide approach to software management for OSS license compliance.
- A compliance system for OSS licensing was established by focusing on the creation of mechanisms for "systems," "processes," "tools," "education," and "supply chain management.

■ Background and issues

Olympus products cover a wide range of medical, imaging and scientific fields. These products are manufactured based on the supply of parts and software from various supply chains. In this context, the need for company-wide unified and appropriate software management was recognized after the occurrence of a near-miss event involving OSS license in delivered products.

■ Initiatives

<[Licensing (L3)] [Supply Chain Management (S3)] [Personal Competence and Education (P3)] [Organizational Structure (O3)] [Community Activities (C3)] Company-wide initiatives triggered by near-miss events>

In Olympus, a near-miss event occurred in the past when it was discovered that OSS had been used in software developed by a supplier in a way that might have violated the license. Although the incident was resolved by taking immediate action on OSS licensing just before shipment of the product with the software, Olympus

decided to take thorough measures for OSS licensing compliance.

The initiative was intended to comply with the license when using OSS and never to include any OSS that is unintended for use. Specifically, the initiative focused on the following five point:

(1) System

(2) Process

(3) Tools

(4) Education

(5) Supply chain management

The details of each initiative are described below:

(1) System

In terms of structure, a company-wide committee for OSS licensing (OSS Promotion Committee[43]) was established. Committee members are appointed from each business division and corporate department, who make decisions on OSS compliance measures and share information (Figure 4.3-1).

In particular, since each business division (medical, imaging, and science) has its own market characteristics, it is important for the company-wide committee to streamline opinions to determine company-wide unified policies. In addition, the committee makes decisions on principle matters (e.g., OSS use policy) but, to ensure flexibility, leaves specific matters to the discretion of each business unit.

[43] The number of members is about 10, and the meeting is held regularly about once a month. The OSS Compliance Office, an organization dedicated to OSS support, serves as secretariat.

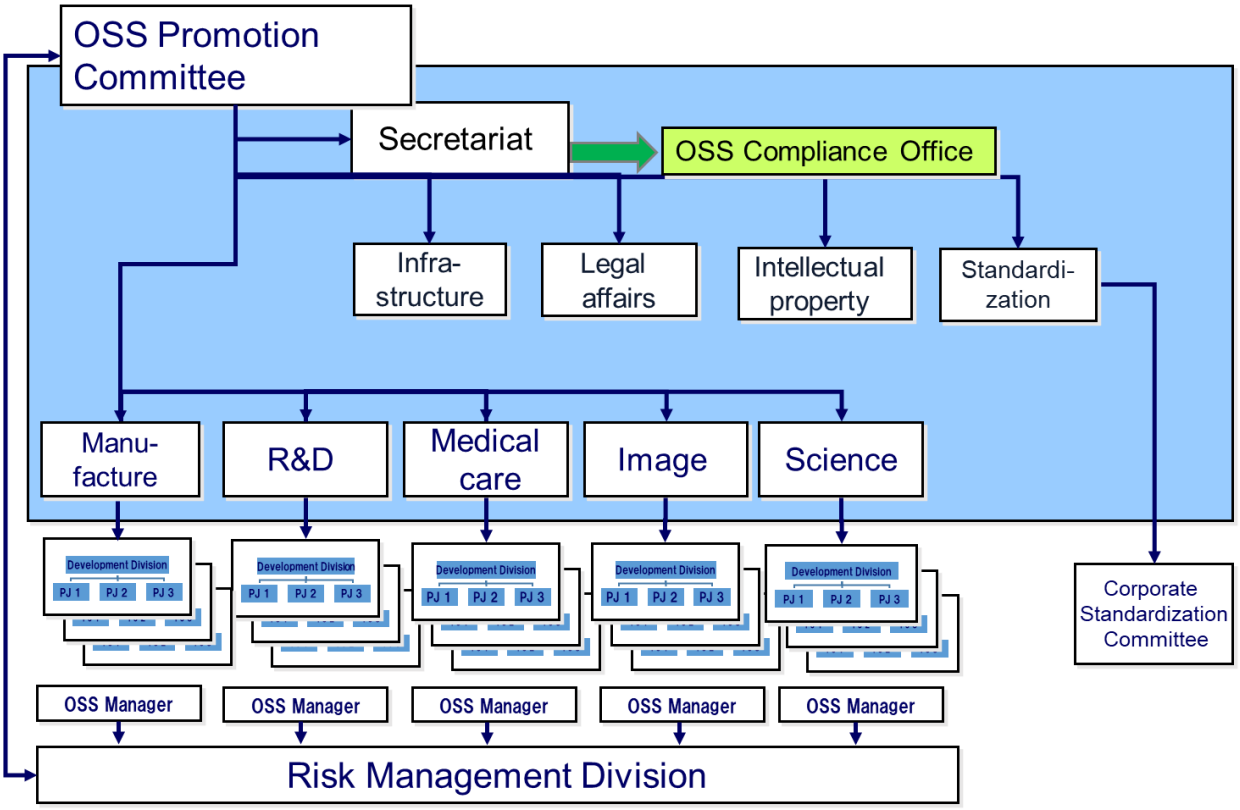


Figure 4.3-1: Structure of the company-wide committee[44]

(2) Process

To support OSS, a series of processes was established and incorporated into the existing company-wide product realization process (hereinafter referred to as the "Standard Process") (Figure 4.3-2).

[44] Compiled based on data provided by Olympus.

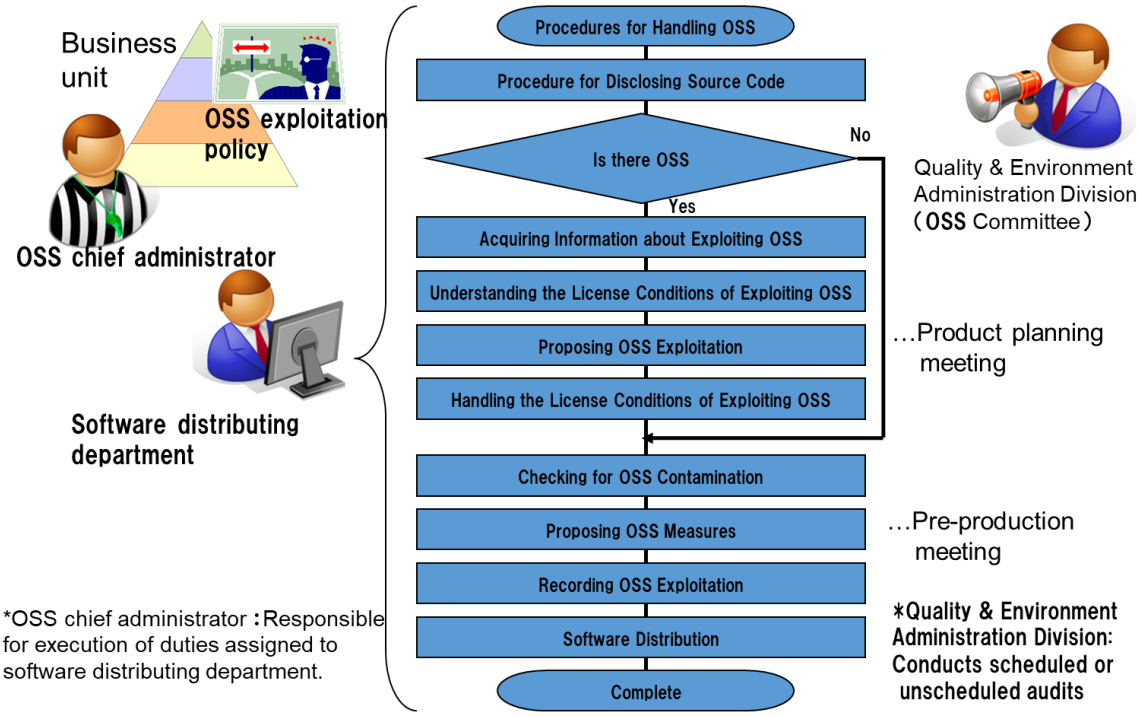


Figure 4.3-2: OSS-related processes included in company-wide Standard Process[45]

In this process, all products must be verified for inclusion of OSS using commercial tools, regardless of whether the OSS use is declared or not. The OSS Compliance Office confirms, records, and manages the information. Some business units use these records as references when responding to software vulnerabilities.

Although there was opposition from the development staff to the addition of the new process because it increased their load, the corporate culture of compliance with the Standard Process was originally fostered, the personnel naturally came to comply with the OSS-related process as it was incorporated into the Standard Process. In addition, one of the group companies implemented this process ahead of others and clarified its effects to gain a sense of acceptance.

[45] Excerpts from materials provided by Olympus.

#	Information for Each OSS				
1	**Basic Information**				
	Name				
	Version				
	Developer (copyright holder)				
	Source URL				
	License conditions				
	License name				
	License type	GPL type	LGPL type	MPL type	BSD type
	Method of Exploitation				
	Link format	Static link	Dynamic link	Interprocess communication	Stand-alone program

Figure 4.3-3: Information for each OSS to be included in the OSS report[46]

(3) Tool

Two tools are used. One is a commercial tool to check for OSS inclusion, as described above. As in (2) above, one group company used the tool first, and after confirming its effectiveness, all group companies adopted it. Currently, the entire group is required to use this tool.

The other tool is designed to build a knowledge site for collecting information on OSS. It delivers such information as cautions for OSS use, license types, and the status of OSS use in in-house products.

(4) Education

Olympus offers educational programs to familiarize employees with the process and various tools for OSS compliance (Figure 4.3-4). OSS education[47] is provided not only for practitioners but also for management[48] and partners. In addition, by preparing English teaching materials, etc., employees in overseas locations can also receive education.

[46] Excerpt from materials provided by Olympus

[47] Lectures and meetings are held by top executives of engineering certification organizations targeted at executive officers and divisional executives

[48] This is an educational menu with the same content as the basic education material "OSS Basics" for employees (see Figure 16), but partially customized for external use.

Figure 4.3-4: Education menu for various target groups (in Japanese)[49]

(5) Supply chain management

Olympus participates in the OpenChain Japan WG [50] with the aim of educating the entire supply chain about OSS compliance. This was triggered by the awareness that, in order to prevent the aforementioned near-miss events, it is necessary to not only take internal measures within the company or group, but also to encourage the supply chain.

Olympus requires suppliers to submit a written confirmation (confirmation of OSS use (Figure 4.3-5)) at the time of delivery of parts and software. In order to obtain the understanding of suppliers on such measures, the company is using the OpenChain Japan WG to disseminate information. One concrete example of the communication is the sharing of the operation of the aforementioned OSS report format in the OpenChain Japan WG. This led to the adoption of the SBOM format (SPDX Lite) disseminated by the WG. The SPDX Lite format discussed in the OpenChain Japan WG has been adopted as an international standard as part of ISO/IEC 5962:2021.

[49] Excerpts from materials provided by Olympus

[50] The specific efforts of the OpenChain Japan WG are described in the case study of Toyota Motor Corporation.

To _____

We would like to ask you whether deliverables from your company, including but not limited to products, parts, units, software packages, or services, contain, exploit, or are based on publicly exploitable software known as "open source software" (hereinafter "OSS"). Please let us know your answer by filling in and sending us the following form, and, if the answer is YES, please also provide the following information for each deliverable. Your cooperation is greatly appreciated.

1) Name of the deliverables which contain, exploit, or are based on the OSS.
2) A list of the names of all the OSS packages.
3) License terms and exploitation conditions for all the OSS packages.
4) Copyright notice for the OSS packages, if necessary.
5) Source code, object code, or any other information accompanied with them for the OSS packages, if necessary.
6) Other necessary information for us to copy, adapt, modify or redistribute the OSS or its derivatives.

Our answer is as follows:

Name of the deliverable: _____
Do the deliverables contain, exploit, or are based on any OSS? (Yes / No)

Figure 4.3-5: Written confirmation of OSS use[51]

[51] Excerpts from materials provided by Olympus.

4.4. Hitachi Limited: Thorough OSS management in the product realization process

■ Company information

Head Office	Chiyoda-ku, Tokyo
Industry	Electrical equipment
Employees	301,000（as of the end of March 2020）
Commercial Flow	Product commercial flow/end product manufacturer
Perspectives	[Licensing] [Community Activities]

■ Essence of this case

- In the process of commercialization of IT products, management by the Software Bill of Materials (SBOM) and checking of OSS with commercial tools are always conducted to realize centralization and efficiency of OSS management and thorough license compliance.
- Hitachi makes a wide range of contributions in community activities and retrieves the results for its own business development.

■ Background and issues

Since the latter half of the 1990s, Hitachi has been making efforts to promote the spread of OSS, including community contributions to Linux and others. Even today, it positions OSS utilization as an important element of its growth strategy and is further strengthening its OSS initiative.

■ Initiatives

<[Licensing (L4)] Utilization of Software Bill of Materials (SBOM) and use of commercial tools in the process of product realization>

At Hitachi, the OSS Solution Center, an organization dedicated to OSS support, and corporate divisions (intellectual property, legal affairs, procurement, and QA[52]) collaborate to promote and support the spread of OSS utilization. In addition, the technical aspects of OSS security (e.g., vulnerability response, tool development and

[52] Quality Assurance.

operation) are covered by in coordination with the Security Management Department.

Hitachi uses OSS in a variety of ways. In particular, since many OSS are used in IT products such as information processing equipment, telecommunication devices, and software, as well as in the service and SI (system integrations) fields, OSS management is thoroughly implemented in license compliance. Specifically, the following two efforts are being made (Figure 4.4-1):

(1) Management by a system using a software bill of materials (SBOM)

(2) Effective identification of OSS through the use of commercial tools.

The details of each initiative are described below:

(1) Management by a system using a software bill of materials (SBOM)

In order to achieve optimal management, Hitachi developed its own management system using SBOM, which was put into operation by the software development division in 2013. Currently, the system is being used in the IT sector (IT products, services, and SI (system integrations)).

In the current IT sector, OSS is centrally managed by this management system. By consolidating internal and external information on OSS use, it is possible to conduct efficient license surveys. In addition, the database of OSS used, and the workflow system functions ensure traceability and procedural efficiency.

In the product development stage, the development team registers OSS to be used in the management system. The registered OSS is verified for appropriateness of use in terms of license through a review workflow system, taking into account past use records. The OSS used in each project is registered in the database after SBOM is created, accumulated as usage results, and fed back to the next development.

(2) Effective identification of OSS through the use of commercial tools

In the IT sector of Hitachi commercial tools have been introduced for the purpose of investigating OSS licenses in the early development stage and checking whether unrecognized OSS is included in outsourced development products[53] and

[53] In development consignment, the basic contract with the consignee includes a clause to notify the consignee in advance if OSS is to be used, or, the purchase order includes as a condition a mention of the possibility of using OSS.

products before release. This prevents license violations caused by any OSS that cannot be identified by registration in the management system alone. In addition, OSS identified by commercial tools are automatically registered in the aforementioned management system. In addition, the functions of the commercial tools (for creating e-mails in the event of a vulnerability) can be used to respond to the software vulnerability after the release of the product.

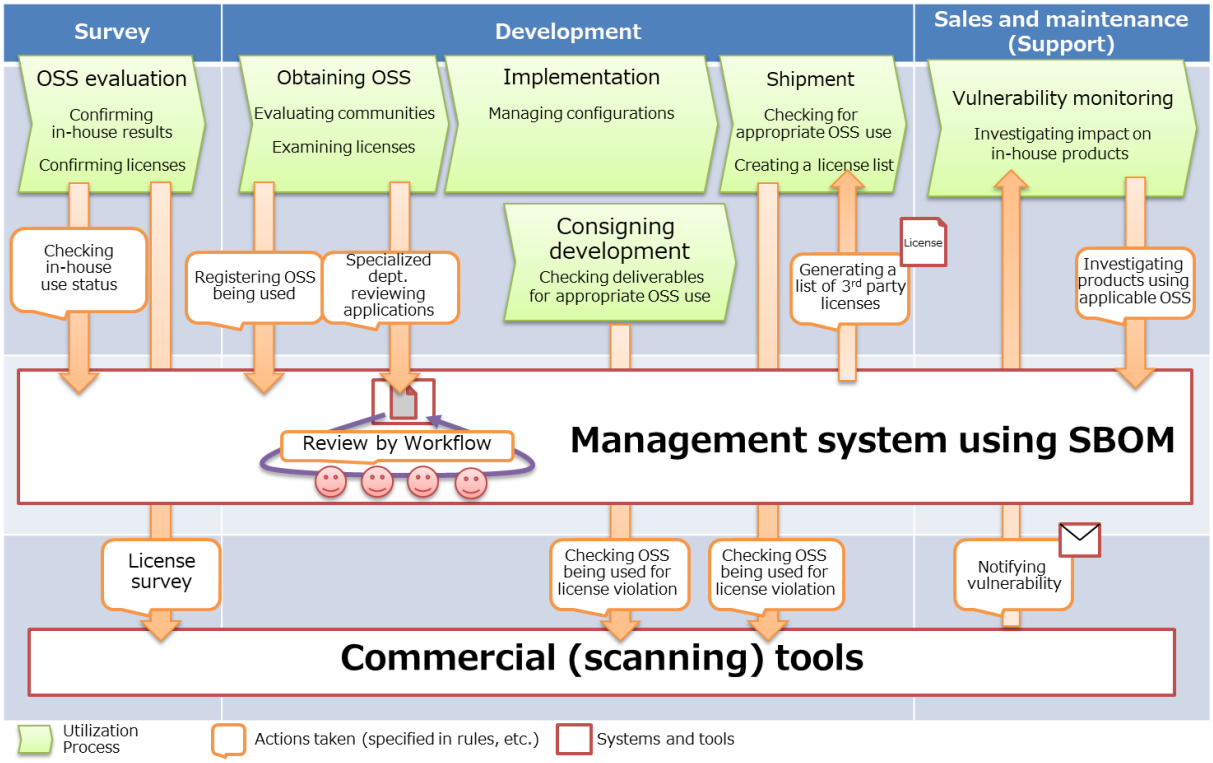


Figure 4.4-1: Utilization of a management system and commercial tools in the development process[54]

For IT products, the use of the management system and these tools is established in an internal rule, as a mandatory to be implemented for commercialization. On the other hand, some development sites have voiced their concerns about the workload involved in OSS registration and other work, so the department that mainly provides software development support has set up a menu to register some OSS on their behalf.

Furthermore, in OSS management, the names of OSS in systems, tools, and information sites are not unified, and thus it is often difficult to distinguish them. To

[54] Compiled based on data provided by Hitachi Limited.

deal with this, Hitachi is studying the construction of a system to organize names by using AI.

Also, in the OT (Operational Technology) business, Hitachi has its own software configuration management and vulnerability response mechanism but is currently in the process of expanding the use of these management system and tools in order to reach the same level as IT products.

<[Community Activities (C4)] Extensive contributions to community activities>

Hitachi is making a wide range of contributions, including the participation of its employees as members in various community activities related to OSS development, investigation and verification, and dissemination and promotion, with the aim of further expanding the utilization of OSS (Figure 4.4-2).

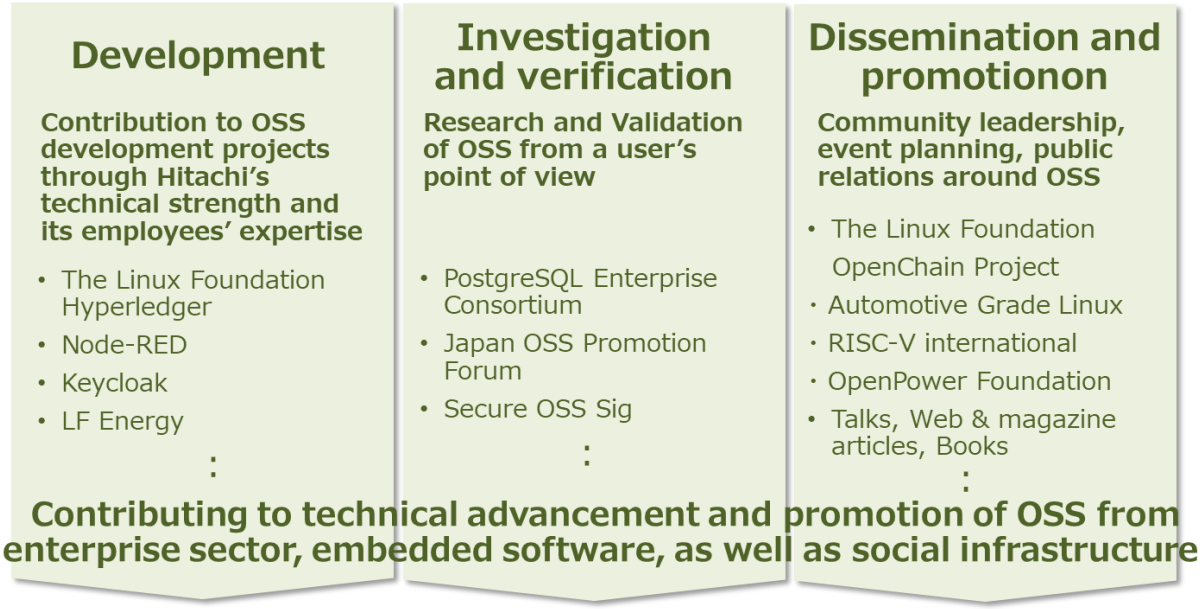


Figure 4.4-2: Major communities in which Hitachi participates[55]

Hitachi participates in a number of communities while assessing their relevance to its various business domains. The results of these community activities are being used by Hitachi for its own business development. Specifically, by demonstrating the OSS development achievements of these communities at external lectures and other opportunities, Hitachi is not only gaining more inquiries from customers, but also using the advanced approaches and best practices learned through community

[55] Excerpts from materials provided by Hitachi Limited.

activities for improvement in the efficiency of their own processes and the review of their training content.

In addition, Hitachi is leading the trend of OSS utilization by giving lectures at various events in Japan and overseas, and by actively disseminating information[56] through various media. The company also provides solutions to support the utilization of OSS, and these solutions are provided to a wide range of customers, including the financial, public, telecommunication, and healthcare industries.

[56] Hitachi introduces its own initiatives for OSS and specific use cases of OSS utilization.

4.5. OMRON Corporation: OSS support through PSIRT collaboration

■ Company information

Head Office	Kyoto City, Kyoto
Industry	Electrical equipment
Employees	28,006（as of the end of March 2020）
Commercial Flow	Product commercial flow/end product manufacturer
Perspectives	[Vulnerability Response] [Supply Chain Management] [Personal Competence and Education] [Organizational Structure]

■ Essence of this case

- A PSIRT has been organized with members from the head office and each business unit. It conducts OSS management, education, vulnerability response, etc. with a clear division of roles.
- A working group has been set up as a consultative body for cooperation between the head office and each business unit. Discussions and regular information exchanges are conducted on improvement measures and group-wide rules related to product security, etc.

■ Background and issues

OMRON has a diverse business portfolio, including control equipment and FA systems, electronic components, healthcare, and social systems, and is developing them under a company system that includes spin-offs. In this context, it is necessary to implement security initiatives, including OSS support, with appropriate coordination between the head office and each business unit.

■ Initiatives

<[Vulnerability Response (V5-1)] [Supply Chain Management (S5)] [Personal Competence and Education (P5)] [Organizational Structure (O5-1)] PSIRT system and cooperation between the head office and each business unit>

At OMRON, a PSIRT has been organized with members from the head office and each business unit (company and business subsidiary) and is promoting product security initiatives including OSS support. The head office division formulates group-wide rules for product quality and security and conducts coordination. On the other hand, each business unit has a system to take practical measures for security related to the products they are in charge of.

The head office and each business unit regularly hold a working group (consultative body) on product security, to discuss improvement measures and group-wide rules related to product security, communicate measures to deal with vulnerability information, and exchange other information (Figure 4.5-1).

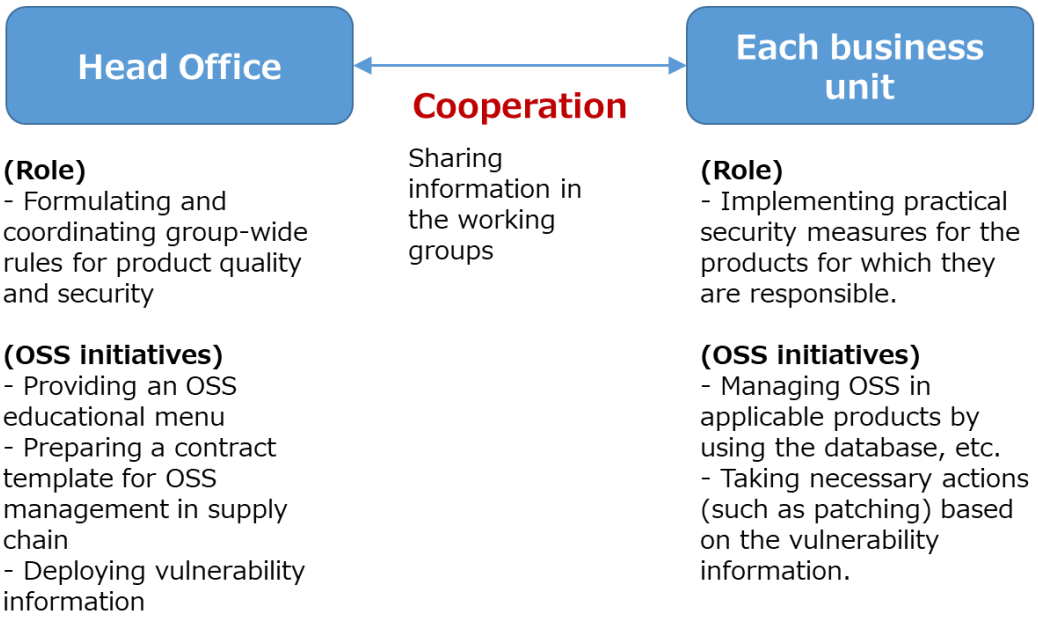


Figure 4.5-1: Division of roles between the head office and each business unit and the OSS-related initiative[57]

Specific OSS-related initiative is implemented as each business entity manages OSS using a database and other information obtained. Since the security requirement level and the frequency of OSS use differ among such business entities, each business entity

[57] Compiled based on interviews.

decides the granularity of OSS management and the method of OSS management, while following the unified group security rules. Some entities use commercial tools for management.

On the other hand, the head office complements the OSS management of each business unit. Specifically, education on OSS is provided[58] for developers, focusing on the outline of OSS, OSS management risks (e.g., cases of unintentional inclusion of OSS), and license compliance. Depending on the content of the education, the person in charge of the legal department or the development process improvement department serves as a lecturer to make the education more practical. In addition, there are cases where non-developers, such as managers, take the courses, which contributes to raising the level of literacy throughout the company.

In addition, the head office department has prepared a template of a contract to be exchanged with external contractors to prevent unintentional inclusion of OSS in the supply chain. The template stipulates that OSS should not be used in principle, and that if OSS is used, the OSS should be notified to the contractor. The personnel in charge of each business entity appropriately manage OSS in the supply chain by using this template.

<[Vulnerability Response (V5-2)] [Organizational Structure (O5-2)] Cooperation among PSIRTs for in software vulnerability response>

At OMRON, the staff of the head office PSIRT regularly collects OSS vulnerability information, and when an OSS vulnerability is found, the information is sent to the PSIRT staff of the related business unit by e-mail. Vulnerability information obtained from the Information Security Early Warning Partnership is tagged with technology keywords[59], and the related entities are identified based on the keywords. At the discretion of the head office PSIRT, important vulnerabilities are flagged to raise the priority of response and are then deployed. Based on the deployed information, each entity takes measures such as applying patches to the target OSS. The response status is also reported to the head office according to the level of risk. In addition to the Information Security Early Warning Partnership, vulnerability information from both inside and outside the company is coordinated between the head office and each business unit, and vulnerability risk assessment and countermeasures are

[58] Education is conducted in person or via the Web.

[59] This is a technical term that JPCERT/CC requires each vendor that receives vulnerability information to register. The list is provided to each vendor reference information for JPCERT/CC to select a vendor to contact when any vulnerability-related information is reported.

implemented according to the rules.

OMRON is currently considering the introduction of a system to unify the vulnerability information management conducted by each business unit at the head office. The purpose of the system is to improve operational efficiency by having the head office manage the vulnerability information in one place and to improve the accuracy of response decisions by making the past OSS response history available to all groups. In addition, OMRON plans to automate the flow of e-mail notification of any obtained vulnerability information by linking it to the system.

4.6. Toshiba Corporation: Consistent OSS support within the group

■ Company information

Head Office	Minato-ku, Tokyo
Industry	Electrical equipment
Employees	125,648 (as of the end of March 2020)
Commercial Flow	Product commercial flow/end product manufacturer
Perspectives	[Vulnerability Response] [Organizational Structure] [Selection Evaluation] [Licensing] [Maintenance and Quality Assurance] [Supply Chain Management] [Personal Competence and Education] [Community Activities]

■ Essence of this case

- The Toshiba-SIRT serves as the primary contact point and has established a consistent response system for software vulnerability handling in the group.
- A collaborative software development platform has been established to promote OSS utilization and improve efficiency and quality through reuse of development results and OSS compliance process results.
- In order to expand the use of OSS in the area of social infrastructure, which is one of Toshiba's strengths, the company is participating in related community activities.

■ Background and issues

Toshiba is developing its business in the areas of energy, social infrastructure, electronic devices, and digital solutions, and is particularly promoting digital transformation in the area of social infrastructure. In this business domain where critical quality is required, Toshiba is strengthening its efforts in product security so that many consumers can use Toshiba Corporation's products, systems and services with peace of mind.

■ Initiatives

<[Vulnerability Response (V6)] [Organizational Structure (O6)] The Toshiba SIRT taking the initiative in software vulnerability response and SIRT Assistance System>

In Toshiba, the CISO[60] has authority over product security. In order to enhance product security, Toshiba has established a cyber security management system under its CISO, which is coordinated by the Toshiba-SIRT[61] set up in the Cyber Security Center and PSIRTs of major group companies. Under this management system, the company is focusing on responses to software vulnerabilities and security incidents, secure development management, etc. In particular, in response to software vulnerabilities, Toshiba participates in the Information Security Early Warning Partnership and has established a consistent response system for the entire Toshiba Group to ensure prompt and reliable response in active cooperation with external organizations.

Specifically, if any vulnerability is discovered in the Toshiba Group's products, systems, or services, the Toshiba-SIRT acts as the primary contact point to collect vulnerability information and share it both internally and externally. If a software vulnerability in any OSS used in a product is identified, the Toshiba-SIRT will deal with it through collaboration with the PSIRT of the group company handling the product and the related business unit (Figure 4.6-1). The Toshiba-SIRT also publishes the results of the response on its website and JVN.

[60] Chief Information Security Officer.

[61] Security Incident Response Team. An organization that responds in the event of a security threat in a computer system, etc.

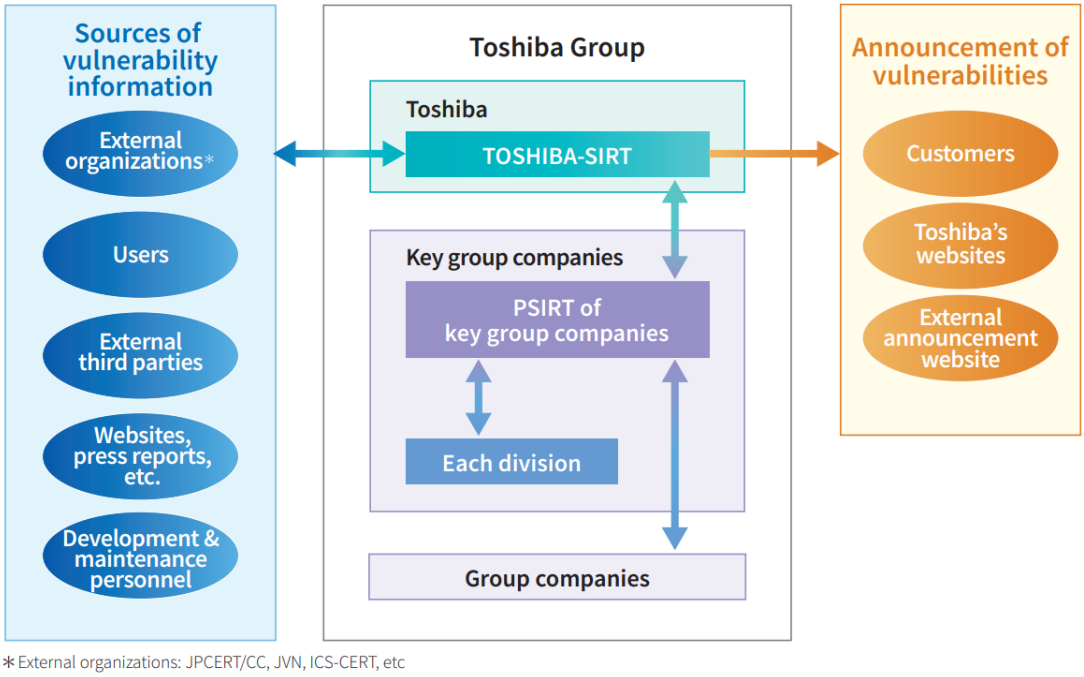


Figure 4.6-1: Toshiba Group's vulnerability handling system[62]

Toshiba has also built a system (SIRT Assistance System) to notify group companies and business units of software vulnerability information collected by the Toshiba-SIRT. This system links the registered software configuration information and the vulnerability information by CPE[63] or product name, and automatically notifies the relevant parties (Figure 4.6-2). Software configuration information is managed by each group company and business unit and is registered in advance in the SIRT Assistance System. If a group company has its own system for managing software configuration information, Toshiba automatically links that information and register it in the SIRT Assistance System. Vulnerability information is automatically collected through API linkage with vulnerability information databases such as JVN and NVD[64], and is also registered manually when reported by customers.

The system is also equipped with a function to know how the notified software

[62] Excerpt from Toshiba Corporation Group Cyber Security Report 2020. https://www.global.toshiba/content/dam/toshiba/migration/corp/securityPrivacyAssets/security/en/files/CyberSecurityReport2020_en.pdf

[63] Common Platform Enumeration. An ID that uniquely identifies the vendor's name, product name, and the version.

[64] National Vulnerability Database: A database of vulnerability information maintained by the U.S. National Institute of Standards and Technology (NIST).

vulnerability information has been handled by the group companies and business units. A responsible person is appointed at each level in the design and development department, the business division, and major group companies, and that person takes the lead in after-sales follow-up.

As of October 2020, the SIRT Assistance System is in trial operation, and group companies and business units have just started using it. In particular, group companies that handle highly security-sensitive products (e.g., social infrastructure companies) are using the system to obtain software configuration information without fail and register it in the SIRT Assistance System.

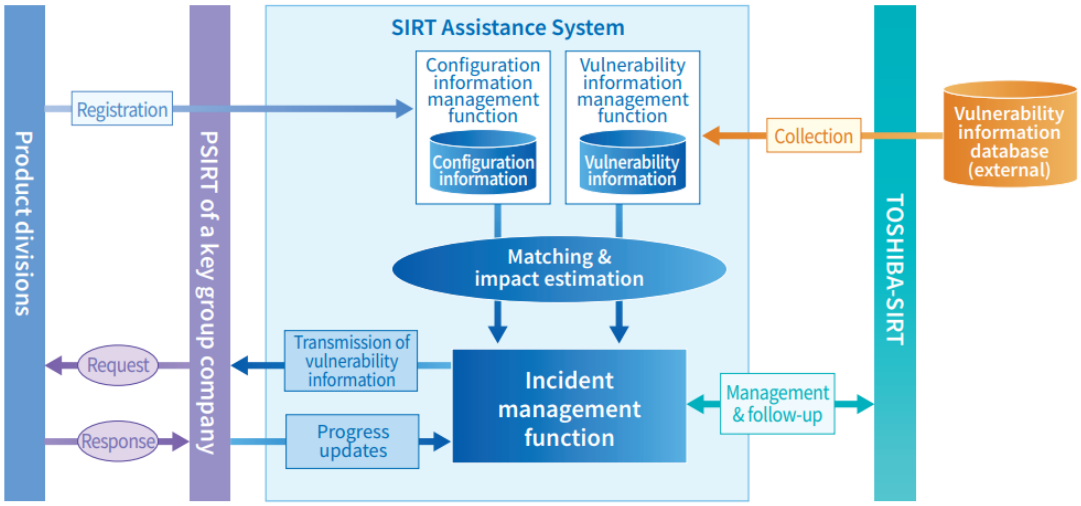


Figure 4.6-2: Overview of the SIRT Assistance System[65]

<[Selection Evaluation (S6)] [Licensing (L6)] [Maintenance and Quality Assurance (M6)] Reuse of the OSS and the development results using a collaborative software development platform>

In anticipation of further OSS utilization, Toshiba has built a collaborative software development platform led by the Software Technology Center. This is a system that records and manages technical findings obtained in the preceding development and the results of the OSS compliance process and enables them to be reused in another development. This will make it possible to reduce the man-hours required for the development of products, systems, and services, improve their functions, enhance their quality, and promote the use of OSS. Consisting of

[65] Excerpts from the Toshiba Group Cyber Security Report 2020: https://www.global.toshiba/content/dam/toshiba/migration/corp/securityPrivacyAssets/security/en/files/CyberSecurityReport2020_en.pdf

(1) a software development management system and (2) a software asset management system, and the collaborative software development platform is capable of simultaneously executing the procedures of the conventional software development operation process and the OSS compliance process (Figure 4.6-3). The platform is being developed for use by the entire Toshiba Group.

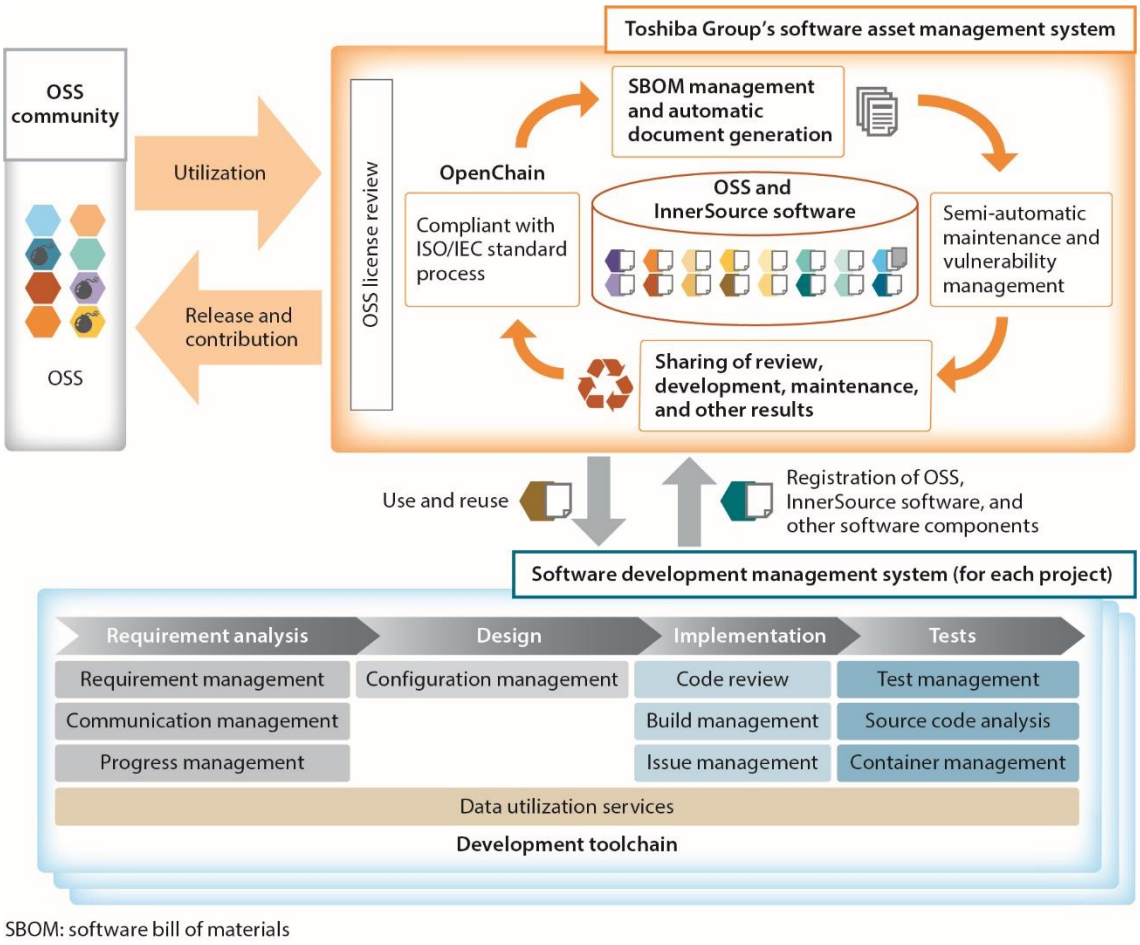


Figure 4.6-3: Structure of the collaborative software development platform[66]

The functions of the two systems that make up the collaborative software development platform are as follows:

(1) Software development management system

The software development management system consists of a software

[66] Excerpt from the TOSHIBA REVIEW SCIENCE AND TECHNOLOGY HIGHLIGHTS 2021 https://www.global.toshiba/content/dam/toshiba/ww/technology/corporate/review/2021/toshiba-review-science-and-technology-highlights-2021/2101.pdf

development tool chain utilizing OSS. Tools with development management functions, such as static analysis of source code, requirements management for efficient traceability assurance, and vulnerability detection, are provided as services.

(2) Software asset management system

The software asset management system provides tools to be used in a series of OSS-related processes, such as license review when using OSS and software management by SBOM required for license compliance.

Currently, Toshiba is focusing on software management using SBOM. While educating group companies on the importance of software configuration management, it is also working on standardization and improvement of operations, aiming at highly accurate SBOM operations that can be used for security measures. In addition, related parties such as the IP department work together with the license reviews of OSS conducted by each business division and carefully judge whether or not to adopt OSS, based on the viewpoint of usage such as "community activity status", "whether it has ever been adopted", "whether it will be used in evaluation", and "whether it will be used in products". At such an opportunity, the Software Technology Center provide support as necessary.

<[Supply Chain Management (S6)] Outsourced development and acceptance>

Software and other items procured from external sources are to be verified for intellectual property relations, including licensing, vulnerability, and quality. Therefore, when using or procuring software from third parties, including OSS, Toshiba also checks the composition of the software. These points remain the same whether Toshiba uses the software itself or provides it to its customers. OSS licensing and vulnerabilities are treated as important issues from the early development and planning stages. When selecting and using OSS, the company needs to consider various factors such as OSS licensing conditions, functions, and requirements for business operations. In addition, it is important to form an agreement with customers and business partners on how to deal with vulnerabilities and future updates.

<[Personal Competence and Education(P6)] Education on OSS utilization>

Toshiba has established a manifesto on OSS to promote a culture and mindset that, as a recipient and user of intellectual property from the OSS community, Toshiba should give back to the OSS community and contribute to the development of the open source ecosystem. Based on this philosophy, Toshiba provides a step-by-step

training program for each job, including introductory training for all positions and basic training with more detailed content, mainly for software developers, in accordance with their practical work. In addition, each group company provides its own training as needed. For example, the introductory training covers the characteristics of open source software and the importance of OSS in corporate activities, as well as intellectual property, licensing compliance, vulnerability management, and other issues to be considered when using OSS. In addition, after basic training, training will be provided on process management for utilizing OSS, while taking ISO/IEC 5230 (OpenChain Specification) into consideration, which is a process management standard for open source compliance. At the same time, to deepen understanding of open source licensing, practical training on licensing compliance is provided using specific examples such as the GPL. Further, Toshiba is also promoting an inner source policy, under which an open source development style is introduced into the organizations. At the same time, a hands-on, practical training program is made ready for development of software, including OSS.

<[Community Activities (C6)] Collaboration within the company and with external parties through communities for the utilization of OSS>

Toshiba has set up a committee consisting of business units within the group (including corporate departments such as legal affairs) as a framework for OSS utilization and holds a wide-range discussion on such matters as information sharing on OSS license compliance and the development of policies and guidelines.

The company also collaborates with external organizations through participation in communities. Specifically, it engages in the development community of OSS tools and make proposals for functional improvements. Toshiba also participates in OpenChain[67] to contribute to the realization of OSS compliance in the supply chain.

In addition, Toshiba is one of the core members of an OSS project called Civil Infrastructure Platform (CIP) under the Linux Foundation. This is a project focusing on solving common problems in order to use OSS safely in systems that are used for a long time and require high reliability, such as social infrastructure. As an example, Linux is increasingly used as an OS in social infrastructure systems and industrial equipment used in factories, but the support period for Linux is only a few years, which poses a problem. The CIP is discussing a system that allows OSS to be used for a longer period (10 years

[67] For an outline of OpenChain activities, see the case study of Toyota Motor Corporation.

or more). As Toshiba Corporation strengthens its business in the social infrastructure domain, it aims to maximize the benefits of OSS utilization through the activities of the CIP.

4.7. DENSO CORPORATION: Optimal OSS management in the entire supply chain

■ Company information

Head Office	Kariya, Aichi-ken
Industry	Transportation equipment
Employees	170,932（as of the end of March 2020）
Commercial Flow	Product commercial flow/supplier
Perspectives	[Licensing] [Supply Chain Management] [Vulnerability Response]

■ Essence of this case

- In order to manage licenses throughout the supply chain, DENSO CORPORATION has established its own internal rules, made arrangements with Tier 2[68] suppliers, coordinated and agreed with them, and standardized the format of software list to be shared with suppliers.
- For OSS vulnerability response, the company is operating a vulnerability research system through the use of commercial tools and external resources.

■ Background and issues

In the automotive industry, there are not only end-product manufacturers but also multi-layered suppliers, and many companies form a supply chain. DENSO CORPORATION, which is a major Tier 1 supplier, sometimes uses OSS in its own product development and uses OSS in products supplied by Tier 2 and later suppliers. It is necessary to manage the usage of these products in an integrated manner.

■ Initiatives

<[Licensing (L7)] [Supply Chain Management (S7)] Initiatives related to OSS licensing, involving the entire supply chain>

DENSO CORPORATION started using OSS first in multimedia products such as car navigation systems and has been gradually expanding the range of products in which it is used. In this process, DENSO CORPORATION has been working to

[68] Suppliers who supply components to Tier 1 suppliers.

establish a company-wide rule and a management system.

Currently, the engineering administration division oversees the OSS licensing initiative as the company-wide office and has established rules for OSS licensing as one of the rules related to design and development. In addition, the OSS Management Office and OSS management leader/person in charge are set up in the engineering department of each business unit. The rules set by the engineering administration division are deployed in the engineering department.

According to the OSS management rules, when the development team plans to use some OSS, it must apply to the OSS Management Office/leader in the technical department for approval. When preparing the application, the development team uses the commercial tools provided by the engineering administration division to know the usage status of OSS. The OSS Management Office/leader check whether there is any problem with the license of the OSS described in the application form, based on the company-wide OSS licensing rules. Once approved, the application forms are stored in a database and can be referred to by the OSS Management Office/leader and the engineering administration division (Figure 4.7-1).

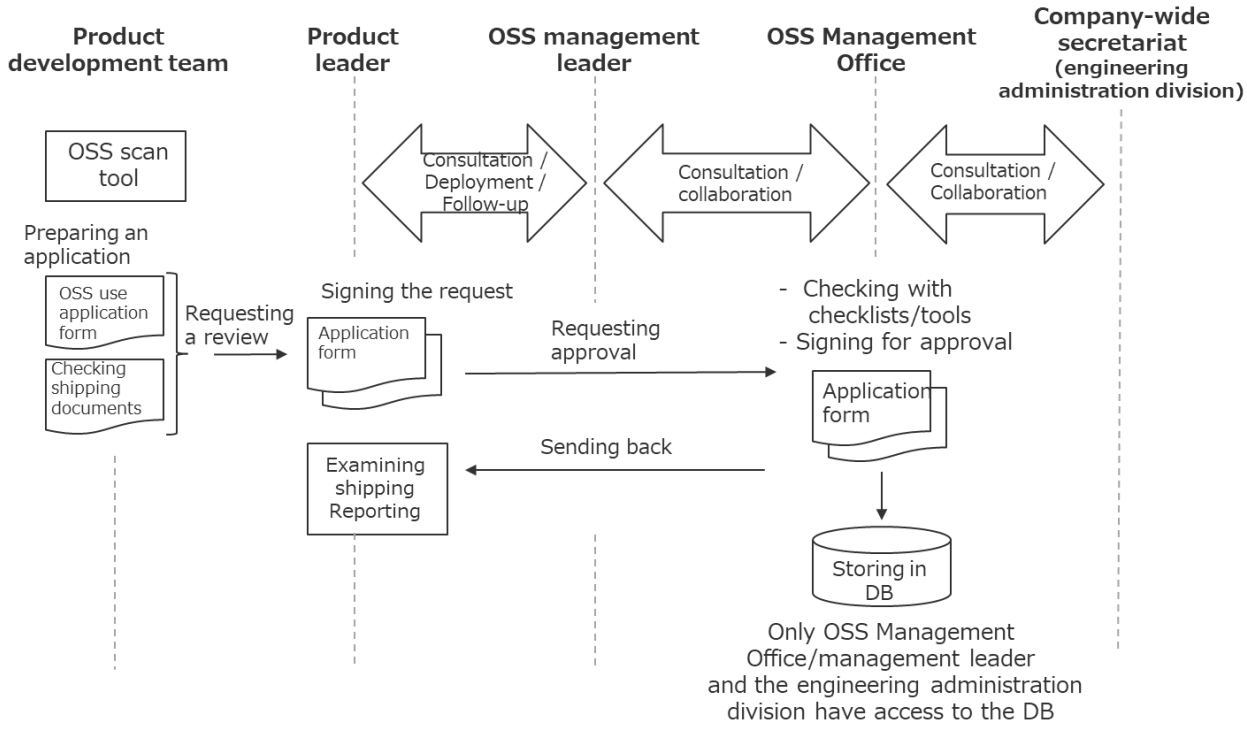


Figure 4.7-1: Flow of OSS usage application approval[69]

[69] Compiled based on materials provided by DENSO CORPORATION.

In addition to the use of OSS in its own product development, DENSO CORPORATION often uses OSS in parts supplied by suppliers (Tier 2), and it is necessary to check OSS licenses for these parts as well. In many cases, only binary data is delivered, although the source code can be verified using the aforementioned commercial tools where available. Therefore, DENSO CORPORATION is coordinating with each supplier based on the template of a contract that includes OSS information provision so that suppliers can receive information on OSS used by contractual arrangements. In addition, the format of the list of software used has been standardized so that software information can be shared from downstream (Tier 2 and later) to upstream (final product manufacturers) of the supply chain. SPDX Lite is used as the format. This is because Toyota and others are promoting the use of this format in OpenChain[70]. Coordination with suppliers (Tier 2) regarding the provision of information on OSS to be used is sometimes difficult. In order to ensure agreement, DENSO CORPORATION works to communicate the importance of compliance, while seeking compromises within the scope of what each supplier can handle.

[70] For an outline of OpenChain activities, see the case study of Toyota Motor Corporation.

<[Vulnerability Response (V7)] Response to vulnerabilities using a vulnerability investigation system>

For OSS vulnerability response, efforts are being made using the vulnerability investigation system operated by the information security promotion division.

Specifically, product designers in each business unit are asked to provide information on the software components of OSS used in their products. Under this system, the product designers of each business unit create a Software Bill of Material (SBOM) for the OSS used in their products and have it registered in the vulnerability research system. The SBOM information is stored and managed in a database. Software vulnerability information is automatically collected from NVD, JVN, and other sources. In addition, the information security promotion division collects vulnerability information from Auto-ISAC, JPCERT/CC, and other sources, and shares it with the vulnerability research system. The vulnerability research system checks such vulnerability information against the registered SBOM information, and automatically notify the product designer of the information with the highest degree of match. The product designer decides whether the information is relevant or not and takes any necessary measure. If the necessary measure is not taken after a certain period of time, the vulnerability research system automatically sends another reminder (Figure 4.7-2).

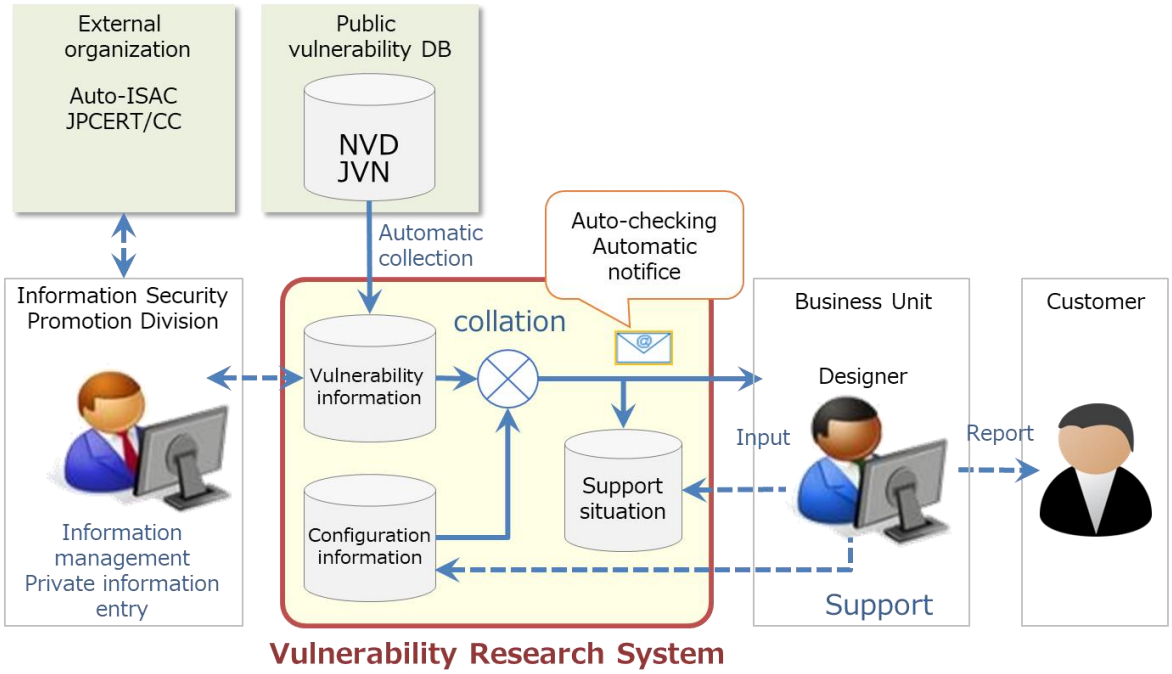


Figure 4.7-2: Outline of the Vulnerability Research System[71]

Some commercial tools and external resources are also used to address vulnerabilities. The information security promotion division provides an environment that allows each designer to use commercial tools when creating SBOMs. Depending on the product, many OSS may be used. In such a case, SBOMs can be created using these commercial tools, which helps reduce the load.

Since the names of OSS programs are not unified in DENSO CORPORATION, the collected software vulnerability information may not exactly match the information in the company's SBOM. This fact may lead to omissions, such as a notice not being automatically issued. In order to prevent such incidents, DENSO CORPORATION manually checks the information using external resources to see if there is any OSS that is identified as different software due to different names.

Furthermore, DENSO CORPORATION is also making efforts in education and training. Since the product line consists of automotive parts, which require a high level of safety, each designer has a high awareness of quality. DENSO CORPORATION is trying to motivate designers to take a series of actions by making them aware that software vulnerability is an important quality issue. At the same time, DENSO CORPORATION also provides relevant educational programs for designers, because dealing with OSS requires knowledge different from that of ordinary quality issues.

[71] Compiled based on materials provided by DENSO CORPORATION.

Since there are many small and medium-sized companies among the Tier 2 and later suppliers, DENSO CORPORATION believes that it is necessary for the entire industry to consider how it can operate while reducing the burden of OSS management.

In license management, an extremely large number of OSS programs are identified at DENSO CORPORATION by the commercial OSS detection tools. This raises the issue of how to manage them efficiently.

In addition, vulnerability response and license management are currently handled separately because the required granularity of relevant information is different and because of the historical background of internal efforts. DENSO CORPORATION has begun to consider how to standardize these groups of information. As the first step, the company is discussing to unify the groups so that SBOM can be created with less man-hours.

4.8. Fujitsu Limited: Cross-divisional OSS support system and uniform software management company-wide

■ Company information

Head Office	Minato-ku, Tokyo
Industry	Manufacturing (Electrical equipment)
Employees	132,138（as of the end of March 2019）
Commercial Flow	System integrators commercial flow/System integrators & Product commercial flow/end product manufacturer
Perspectives	[Licensing] [Supply Chain Management] [Personal Competence and Education] [Organizational Structure] [Community Activities] [Selection Evaluation] [Vulnerability Response] [Maintenance and Quality Assurance]

■ Essence of this case

- The OSS support system was established on a cross-divisional basis in close cooperation with not only the OSS support organization but also the development and administration divisions.
- Clarifying rules for participation in community activities and offering education and other measures to support employees to contribute to communities.
- Enhancing OSS utilizing visualization and OSS-related risk detection in software lifecycle by providing company-wide unified tools and services.
- OSS usage status management activities are in cooperation with software products security ensuring activities.

■ Background and issues

Fujitsu, which is a major domestic system integrator and information and communication equipment manufacturer, has more than 1,000 development projects in progress at any given time, and many OSS programs are used in each project. In order to manage the vast amount of OSS in use, in addition to taking appropriate measures at each phase of the project, Fujitsu takes comprehensive and multifaceted measures, such as establishing a company-wide system and improving the literacy of employees.

■ Initiatives

<[Supply Chain Management (S8)] [Personal Competence and Education (P8)] [Organizational Structure (O8-1)] [Community Activities (C8)] Development of an organizational structure and an educational system for OSS support and community activities>

Fujitsu has established the OSS Technology Center[72] as an organization specializing in OSS and is implementing initiatives in a wide range of aspects, including OSS dissemination and promotion, technical support, governance, risk management, and security.

For company-wide OSS support, a formation is formed not only with the OSS Technology Center but also with the development department, the management department, and internal communities[73]. Specifically, personnel with expertise in each department and organization form cross-organizational response projects for each OSS initiative and regularly conduct activities to resolve issues. When a project achieves its objective, the role may be taken over by an existing organization.

For example, for OSS licensing and security risks, a working group is formed by IP staff of the management division and security staff of the management division and the development division to deal with these risks in a cross-organizational system (Figure 4.8-1). In addition, there are cross-organizational activities conducted by the development division, the SE (Software Engineering) division, OSS technology centers, and other units to strengthen support for specific OSS.

[72] Established in November 2005 to provide support for everything from system construction to operation using OSS middleware. It is a unit mainly composed of engineers that provides a wide range of OSS solutions to meet the needs of systems using OSS in cooperation with the Fujitsu Group, OSS vendors, communities, governments, and OSS organizations.

[73] A number of employee-led entities organized for the purpose of promoting the utilization of OSS, developing human resources, and expanding support systems.

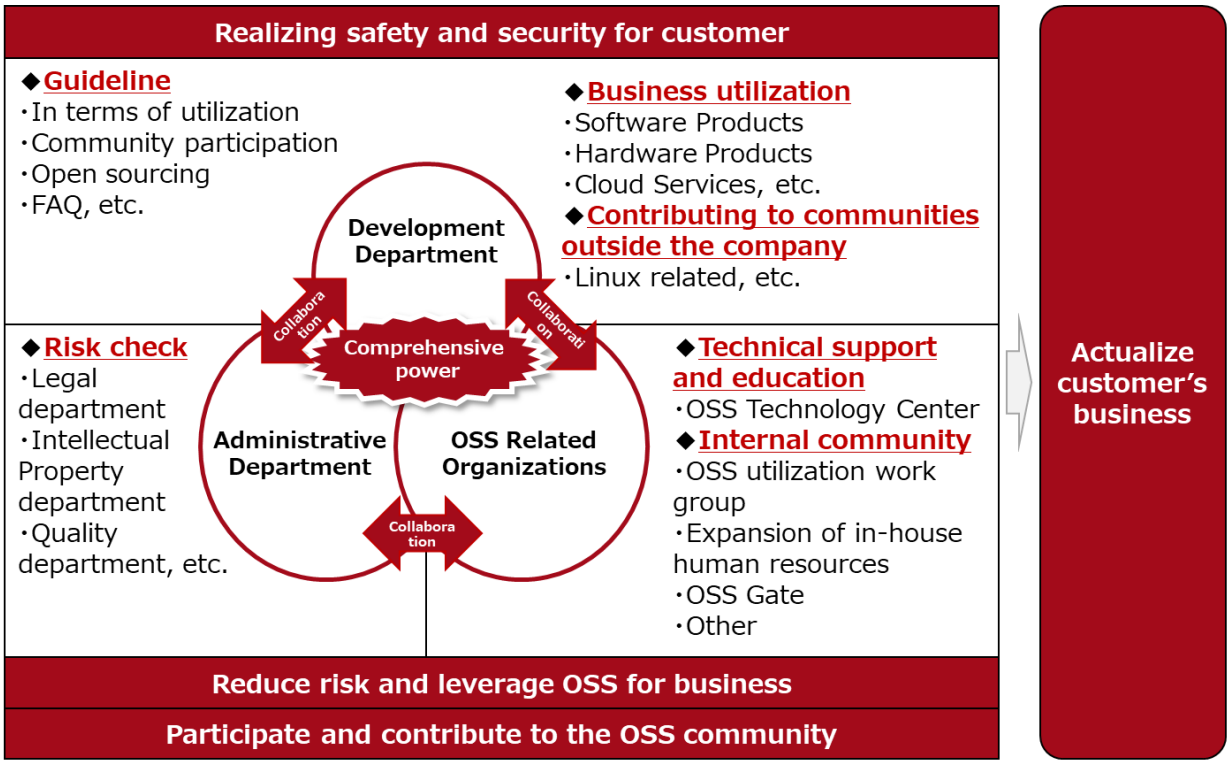


Figure 4.8-1: Creating a system and framework to support company-wide OSS utilization[74]

The reason for this system is that it is impossible to solve problems related to OSS using only a single knowledge domain. By establishing a cross-divisional system in which the core unit and personnel in charge are placed while collaborating with necessary units and personnel in other divisions, it is possible to demonstrate high responsiveness to OSS risks.

In addition to organizational measures, Fujitsu is also focusing on education. It provides educational courses through e-learning for acquiring the knowledge needed to use OSS. In addition to providing detailed courses for engineers who can learn each field in detail, Fujitsu also provides courses for users of systems that include OSS, because OSS knowledge is related to the company's DX strategy. In addition to these e-learning courses, the company also provides education for OSS developers on the knowledge required in situations such as becoming an OSS developer or participating in GitHub[75].

In addition, Fujitsu clearly positions external community activities as an effective means of contributing to the business utilization of OSS. However, because they are

[74] Compiled based on data provided by Fujitsu.

[75] Software development platform services for hosting source code.

external activities, it is necessary to implement appropriate governance for its employees' community activities. As an example, it is necessary to manage participating communities as a company because community activities that are beneficial to one business unit may be detrimental to another. Therefore, Fujitsu has established OSS community participation guidelines and controls them to ensure that appropriate community activities are carried out (Table 4.8-1).

Table 4.8-1: Summary of OSS Community Participation Guidelines[76]

Objective	To clarify internal procedures, items to be observed by software developers, and the roles of relevant internal departments for submitting programs, etc. to OSS communities.
Target	In Fujitsu Group, the department that contributes programs and documents to the OSS community to reflect them in existing OSS, and related parties such as developers.
Composition	< Chapter 1: Applying to Join the OSS Community> ● Community assessment Are there any inconsistency in the license of the target OSS? Are community activities active? ● Application procedure On the internal web, the application will be checked by the legal department and approval by the technical department. ● Operational decisions of the applying department The applying department decides on the submission destination, contributors, submission procedure. < Chapter 2: Self-checking for Submitting a Program> ● Copyright Does it contain other companies' copyrighted material or OSS? ● Confidential information Does it contain confidential information of the company or other companies? ● To add a function Is there any patent infringement? Is the function patentable? ● Submission Submit according to procedures set by the department. Submission management is the responsibility of the executive staff of the submitting department.

In addition to training for community participants on risks such as information leakage in external activities, education for contributing to the community is also provided, including training to motivate employees to participate in the community and to enable them to exercise their presence in the community. Through these series of efforts, Fujitsu aim to sustain the revitalization of community activities and the resulting development of its own OSS utilization.

A concrete example of a community in which Fujitsu participates is OpenChain[77]. As

[76] Based on data from Japan Technical Jamboree 60 (2017). (in Japanese)
https://elinux.org/images/e/e7/%E3%80%90CEWG%E3%80%91OSS%E3%82%B3%E3%83%9F%E3%83%A5%E3%83%8B%E3%83%86%E3%82%A3%E5%8F%82%E5%8A%A0%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6.pdf

[77] For and outline of OpenChain activities, see the case study of Toyota Motor Corporation.

OSS expands its role from commercial alternative software to one that is widely expected in the market regardless of industry and creates de facto and standards, Fujitsu will become a platinum member in March 2019, with the aim of watching the current trend and foreseeing the future.

Fujitsu has joined the OpenChain. Specifically, it is leading discussions in the Japan WG[78] and its sub-WGs (Tooling SWG[79], FAQ SWG[80], and Planning SWG[81]. In November 2019, it self-certified its compliance with the OpenChain2.0 "Specifications," which is a compliance requirement for managing OSS[82]. Fujitsu has started to acquire certification for departments that incorporate OSS into their products. Now, it is urging departments related to supply chain management to acquire certification, while stepping up its efforts to ensure that certification is also acquired by group companies.

<[Selection Evaluation (S8)] [Licensing (L8)] [Vulnerability Response (V8-1)] Software lifecycle management>

Fujitsu has established internal guidelines and rules to check whether OSS is used appropriately in each phase. The following shows the structure of the guidelines (OSS Utilization Guide) for applying OSS in a project (Figure 4.8-2). In particular, Chapter 2, "Actions required and descriptions for each development phase," mandates appropriate OSS selection in the planning phase, thorough license compliance in each phase of development, preservation of evidence for implementation of necessary re-shipment procedures, and establishment of a support system.

[78] For activities of the OpenChain Japan WG, see the case study of Toyota Motor Corporation.

[79] SWG for reviewing and validating tools for OSS compliance.

[80] SWG for sharing OSS licenses related FAQs.

[81] SWG for discussing how to proceed with the Japan WG.

[82] OpenChain2.1, which has almost the same content as OpenChain2.0, has been incorporated into an ISO standard (ISO/IEC 5230:2020). Companies that have obtained certification in accordance with OpenChain2.0 will automatically comply with the requirements of ISO/IEC 5230:2020.
https://www.openchainproject.org/featured/2020/12/15/openchain-2-1-is-iso5230

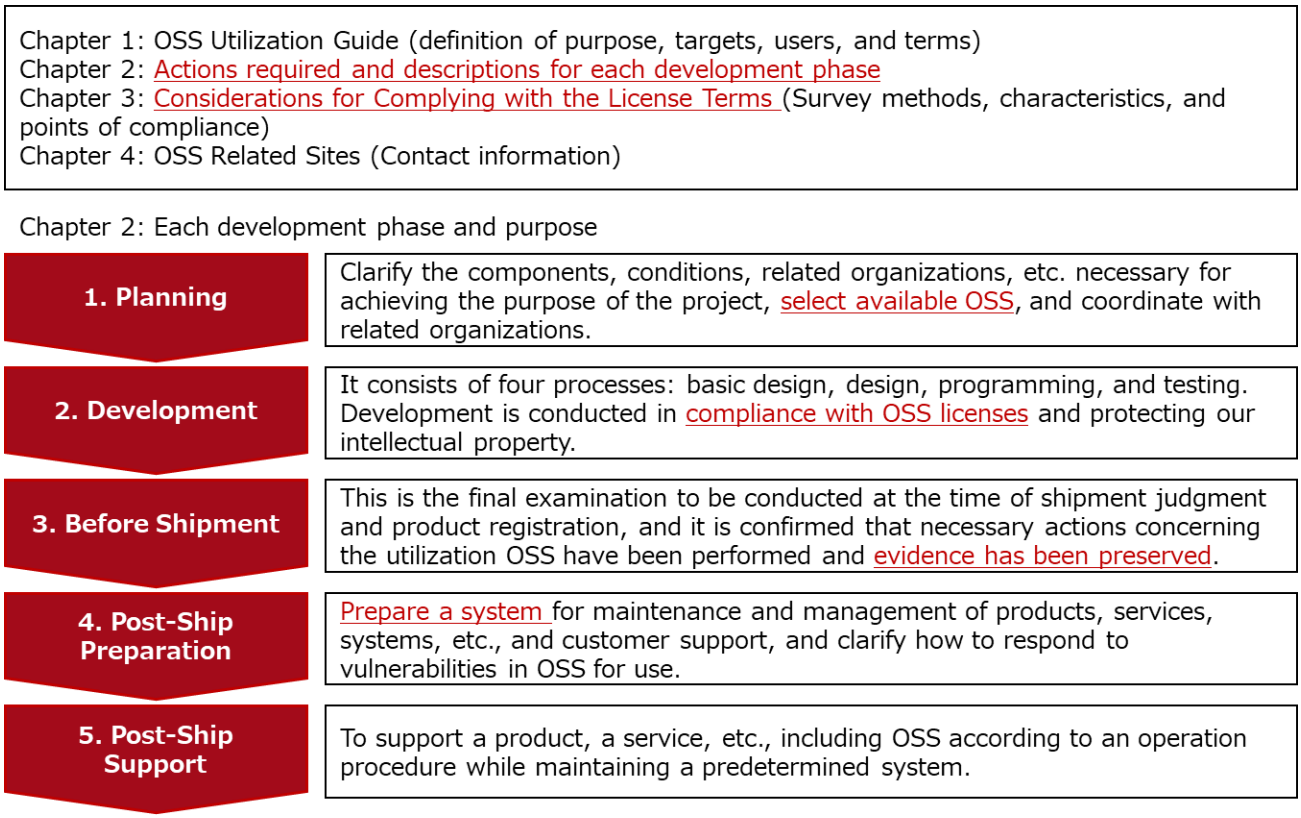


Figure 4.8-2: Structure of the OSS Utilization Guide and details of Section[83]

In addition, the status of OSS use in each project (OSS used, version, license) is managed company wide. Specifically, in each phase of development, the management department, the OSS Technology Center, and the CRIRT[84] team work together to provide the following services to projects (Figure 4.8-3):

(1) Self-checking tools for OSS licenses are provided at the review and design stage.

(2) In the development/introduction stage, Fujitsu provides a service to examine OSS inclusion.

(3) In the maintenance and operation phase, the service manages vulnerabilities and EOL[85], including major functional bugs, and issues alerts to the relevant departments.

[83] Compiled based on data provided by Fujitsu.

[84] Computer Security Incident Response Team: A team dedicated to responding to computer security incidents.

[85] End of Life.

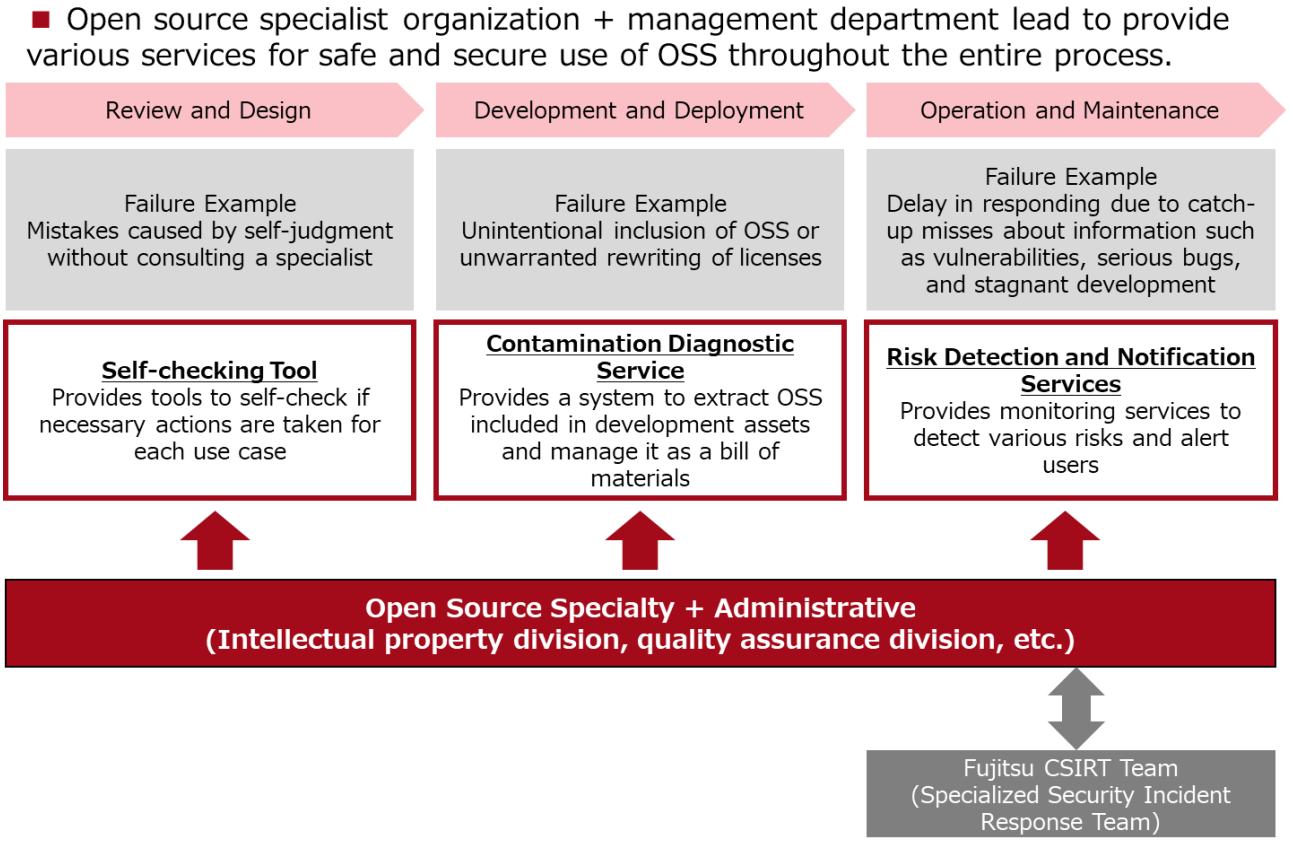


Figure 4.8-3: An example of OSS management[86]

In addition, as a service in (1), Fujitsu has created a database of OSS development trends, licenses, and past vulnerabilities (information on such matters as trends and period until closure, etc.) to be used by the company and made it available to the public for the purpose of supporting the selection of appropriate OSS. The use of these various tools and services is also specified in the rules and regulations, which are thoroughly applied to all projects throughout the company.

As described above, by providing company-wide tools and services and conducting unified operations as an enterprise, Fujitsu has achieved a software lifecycle with a low security vulnerability risk and a license risk.

<[Vulnerability Response (V8-2)] [Maintenance and Quality Assurance (M8)] [Organizational Structure (O8-2)] Support for OSS in various initiatives to ensure security>

Before delivering systems to customers, Fujitsu conducts a security audit at its independent internal security audit department. If any OSS is used in the system,

[86] Compiled based on data provided by Fujitsu.

the department checks for the OSS version, the existence of vulnerabilities inherent in the version, and the existence of failed response, in coordination with the aforementioned tools used for OSS management.

In addition, since Fujitsu provides a number of OSS-based cloud services, it has organized Fujitsu Cloud CERT[87] for the purpose of responding to security incidents relating to the cloud services. In the event of a security incident caused by OSS, Fujitsu Cloud CERT will take an emergency response in coordination with related internal departments such as the OSS technology center.

In addition, Fujitsu provides a verification service that uses AI-based technology to assess and identify undetectable vulnerabilities in software products[88]. Some Fujitsu products and services have begun to use this verification service to improve security quality.

[87] Compute Emergency Response Team: An organization that collects and provides information on security, unauthorized access on the Internet, software vulnerabilities, etc.

[88] Launched "Vulnerability Verification Service".
https://www.fujitsu.com/jp/group/fct/resources/news/press-releases/2016/1101.html

4.9. NEC Corporation - From divisional initiatives to company-wide initiatives

■ Company information

Head Office	Minato-ku, Tokyo
Industry	Manufacturing （Electrical equipment）
Employees	112,638 (as of the end of April 2020)
Commercial Flow	System integrators commercial flow/System integrators & product commercial flow/end product manufacturer
Perspectives	[Selection Evaluation] [Licensing] [Vulnerability Response] [Personal Competence and Education] [Maintenance and Quality Assurance] [Organizational Structure]

■ Essence of this case

- By establishing unified guidelines and an OSS information sharing system, NEC has sublimated the OSS initiative at each business unit to a company-wide initiative.
- In order to centrally manage the OSS usage status of the entire company and realize one-stop support, an "OSS Utilization Process" utilizing tools and a workflow system was established.
- By making the OSS utilization process a company-wide rule and giving top-down instructions for its application, the number of projects to which it can be applied has been increased, resulting in high effectiveness.

■ Background and issues

NEC, which is a major system integrator in Japan, has many development projects in progress at any given time. At the same time, NEC is also providing products such as software and information and communication equipment and services in the form of SaaS[89]. In the midst of providing such diverse value, NEC is required to manage and respond to OSS in a manner that is consistent across the entire company while matching the status of each business.

■ Initiatives

[89] Software as a Service: Software provided in the cloud.

<[Selection Evaluation (S9-1)] [Licensing (L9-1)] [Organizational Structure (O9-1)] From a divisional approach to a company-wide approach>

NEC started to use OSS in the Linux server business in the early 2000s. From the need to take licensing into consideration[90], NEC has been implementing OSS management at its own business units from early on, mainly for embedded products (cell phones, etc.) and the B2B2C[91] SI (system integrations) business. Since 2010, as the merits of OSS utilization have been recognized and its use has increased, NEC has recognized the need to expand OSS utilization and management, which had been implemented at each business unit, to the entire company. To this end, the company formed a task force in 2014 and started company-wide OSS management. At present, the OSS Promotion Center, a company-wide OSS support organization, is working on OSS utilization across the business.

(1) Establishment of guidelines.

(2) Maintenance of a recommended OSS list, etc., and risk investigation of unrecommended OSS programs.

(3) Development of an OSS information sharing system.

(4) Support for OSS code verification and OSS license compliance.

The details of each initiative are described below:

(1) Establishment of guidelines

Regarding compliance items for OSS use, a set of guidelines was developed step by step to be referred to in each phase of a software-related project (Figure 4.9-1). For example, the Decision Guidelines for OSS Use defines standards for considering whether to introduce OSS and its license in the planning and development phases. Since each guideline is defined individually, it is continuously reviewed to make the whole guideline more unified. In addition, contract templates are shared.

[90] It is necessary to comply with the license because the software (OSS) is redistributed with the product.

[91] Business to Business to Consumer. A form of business transaction in which a company provides goods or services to another company, and the receiving company in turn provides them to general consumers.

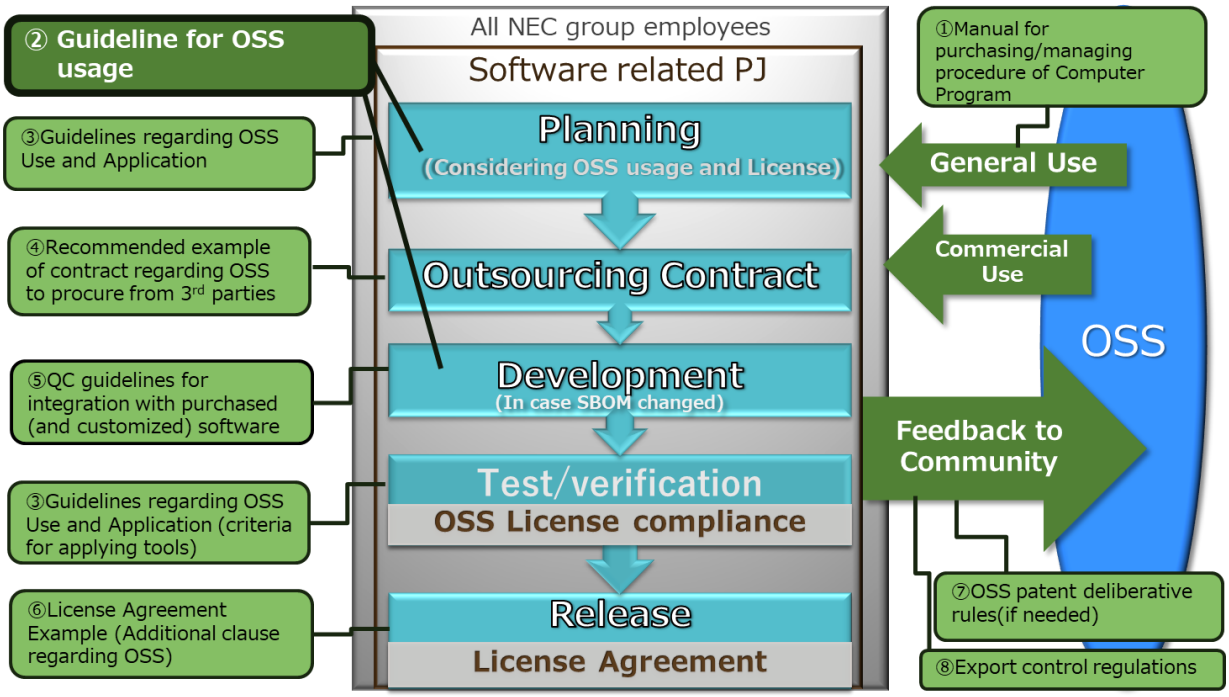


Figure 4.9-1: Guidelines referred to in each phase of a software-related project[92]

(2) Maintenance of a recommended OSS list, etc., and risk investigation of unrecommended OSS programs

By making a list of OSS recommended for use and providing it internally, NEC is able to substantially reduce risks (e.g., licenses, vulnerabilities, EOL). The OSS programs recommended for use are determined based on the existence of support, the entity implementing the support, and the actual use within the company. In addition, a list of "high-risk" and "unrecommended" OSS programs has been prepared to clarify which OSS programs should not be used[93]. An OSS program is classified as "high-risk" if they have serious vulnerabilities or EOL, and as "unrecommended" if it is completely unsupported. Even for unrecommended OSS, the OSS promotion center examines it upon receiving a requests or question and provides advice on risk avoidance.

(3) Development of an OSS information sharing system

In addition to the recommended OSS list in (2), NEC provides publicly known

[92] Excerpts from materials provided by NEC.

[93] Each list is updated periodically (every few months).

information[94] on major OSS in each software field[95] and information (e.g., support system) on its own internal use of the OSS on the Web portal (information sharing system). The OSS Promotion Center periodically updates this information.

(4) Support for OSS code verification and OSS license compliance

NEC provides an in-house service to detect whether actual products and systems contain unrecognized OSS mixed in by external diversion, etc. using commercial tools. In addition, the company has launched a consultation service to support appropriate responses and compliance with OSS licenses, including documentation and source code disclosure.

<[Selection Evaluation (S9-2)] [Licensing (L9-2)] [Organizational Structure (O9-2)] Implementation of comprehensive OSS management>

As mentioned above, NEC has been promoting company-wide efforts for OSS utilization and its management. It has recently established an "OSS Utilization Process" to manage OSS more comprehensively in line with the development speed of Agile and DevSecOps[96] (Figure 4.9-2). This enables the OSS Promotion Center to watch the usage status of OSS throughout the company and to provide one-stop support for it. In building the OSS utilization process, NEC added new measures to the existing process for software-related projects. This applies to all of NEC's products, services, and SI (system integrations).

[94] Each software field is referred to from the OSS bird's eye view created by the Japan OSS Promotion Forum.

[95] The information on version, scale, language, license, vulnerability, and activity is collected from Black Duck Open Hub, JVN iPedia, and each OSS website.

[96] Applications and infrastructure security should be considered from the outset.

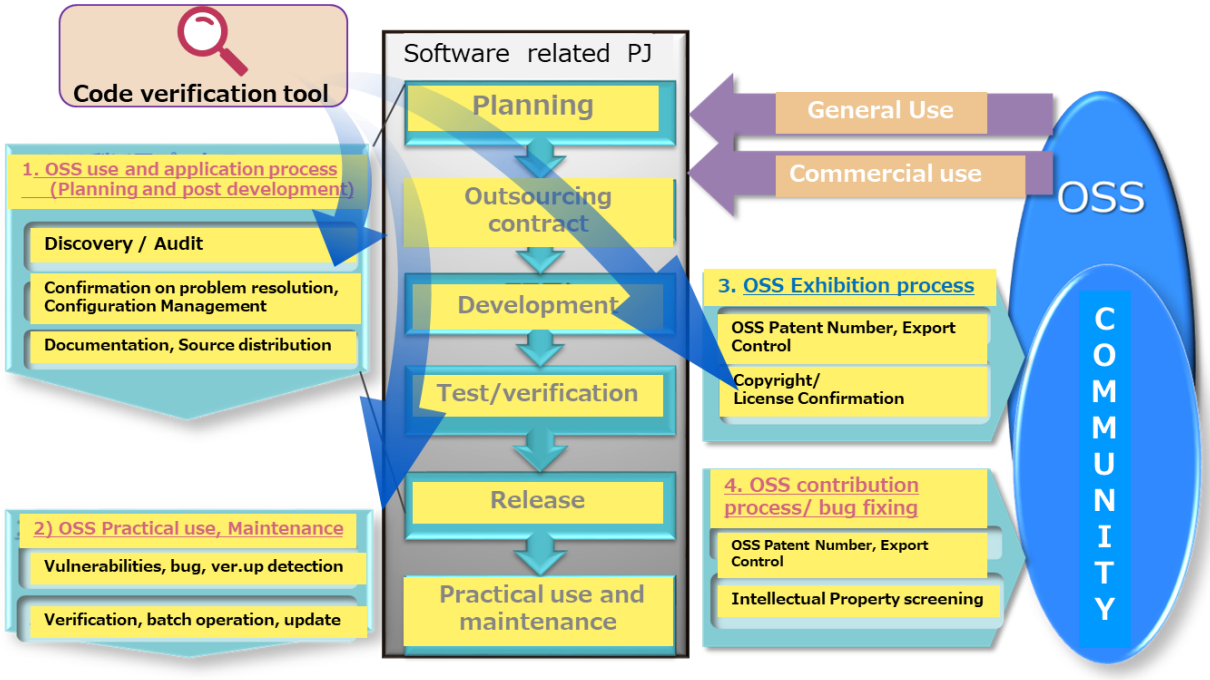


Figure 4.9-2: Overall view of the OSS utilization process[97]

The OSS utilization process proceeds on a workflow system. As an example, the following steps indicates the flow for OSS license compliance after development.

(1) Adopting the list OSS programs used into the workflow system and providing OSS risk information.

(2) Addressing OSS risks and recording OSS configuration information.

(3) Watching OSS license compliance.

(4) Managing OSS codes to be disclosed.

The details of each initiative are described below:

(1) Adopting the list OSS programs used into the workflow system and providing OSS risk information

OSS used in the project will be incorporated into the workflow system starting from the application (submission of an OSS risk management form) or OSS detection by the code verification tool. The OSS Promotion Center provides the project with information such as risks related to the OSS to be used.

[97] Excerpts from materials provided by NEC.

(2) Addressing OSS risks and recording OSS configuration information

If any OSS has risks, the project decides how to deal with them, and the OSS Promotion Center confirms them. If there is no problem as a result of the confirmation, or if there is no risk, the OSS Promotion Center shall record and centrally manage the software configuration information.

(3) Watching OSS license compliance

The OSS Promotion Center will support the preparation of notices and other documents necessary to comply with the OSS license. After final confirmation by the OSS Promotion Center, the source code is distributed with OSS or published at a designated place.

(4) Managing OSS codes to be disclosed

The OSS Promotion Center follows up on the management of source code, etc. distributed or released.

The OSS utilization process also includes an operational flow in which each project can check vulnerabilities, bugs, version upgrade information, etc., using the functions of the code verification tool, while the OSS Promotion Center will encourage them to take action as necessary.

Initially, the OSS utilization process was developed in a grassroots manner on a "request" basis for each project. Later, in order to increase the effectiveness of the process, NEC established the application of the OSS utilization process as a company-wide rule and made the new rule known at meetings attended by the management. The company-wide rules and top-down instructions have raised awareness of the application of the OSS utilization process within the company, and the number of applications is on the rise. For the purpose of building a PDCA cycle to utilize information obtained through the operation of the OSS, NEC is considering the creation of a system to send information on OSS with a large number of use records and OSS used in combination to the recommended OSS list and the next-generation OSS information sharing system (Figure 4.9-3).

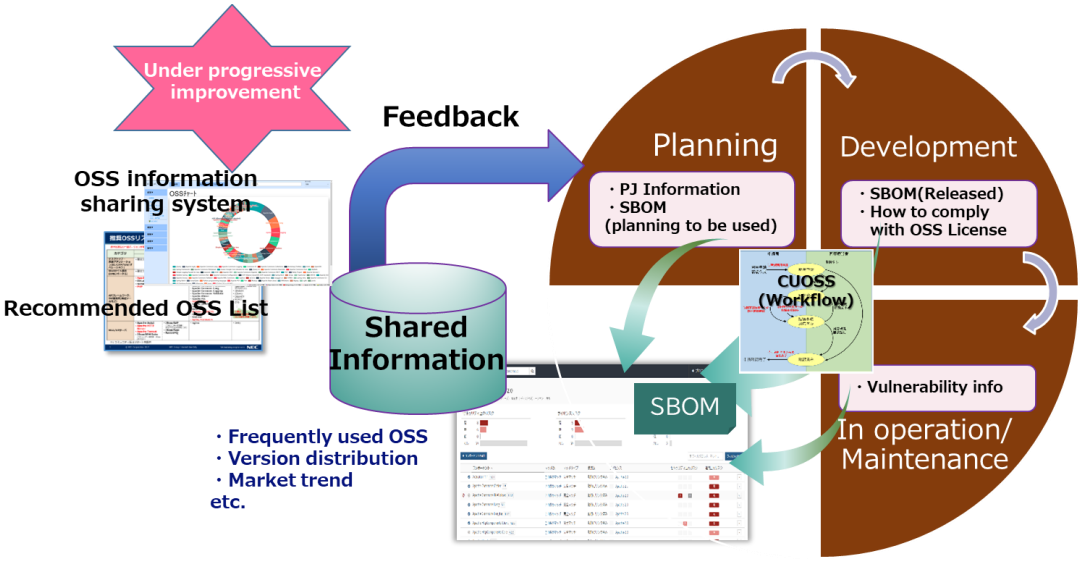


Figure 4.9-3: PDCA cycle of the OSS utilization process (Example)[98]

NEC is also considering the introduction of new tools such as PoC[99] as a future initiative. At the same time, the company is considering the automation of various flows and other measures to improve efficiency, while unifying the OSS name masters of tools. In addition, it is promoting multifaceted efforts to further raise awareness of OSS within the company.

<[Vulnerability Response (V9-1)] [Personal Competence and Education (P9)] Establishing a PSIRT>

The NEC Group established a PSIRT in 2004. At that time, there was an increasing number of threats, such as Code Red/Nimda, SQL injection, and other cyberattacks. In addition, NEC felt that there was a limit, in terms of systems and cost, to having staff individually taking charge of vulnerability management of its own products and customer systems. Therefore, they decided to establish a specialized unit to develop a mechanism (refer to the description of VPS below). In addition, when the PSIRT was first established, there was no information available to help the staff. However, after FIRST's PSIRT Services Framework[100] was released, they used it to collect

[98] Excerpts from materials provided by NEC.

[99] Proof of Concept: A pre-production validation or demonstration of a new concept, theory, principle, or idea.

[100] A guide to help organizations that develop and provide products and services establish and continuously operate PSIRTs and improve their capacity. FIRST publishes Security Incident Response Teams (SIRTs) Services Framework Version 1.0, 30 Mar 2016、Press Releases 2016、

information for PSIRT construction and responses.

The PSIRT now serves as a liaison with JPCERT/CC, external vendors, individuals, etc., while obtaining vulnerability information (including both publicly disclosed and unreleased information). Based on the vulnerability information obtained, the team organizes the affected products and response policies, and investigates and addresses the vulnerabilities in cooperation with the responsible persons on the development side involved.

In addition, the team collects and disseminates vulnerability early warning information and indicator information to internal stakeholders, alerts them to vulnerabilities that are prevalent in the world, prepares reports, and discloses them to the public.

Further, to ensure accountability in the event of an incident, the PSIRT provides centralized consultation on how to report and address vulnerabilities in NEC Group products when they are discovered. The NEC Group is taking initiatives to ensure an appropriate vulnerability response.

<[Vulnerability Response (V9-2)] [Maintenance and Quality Assurance (M9)]
Vulnerability Preventive Management System (VPS)>

PSIRT has established a Vulnerability Preventive Management System (VPS). A VPS registers configuration information of systems to be developed and manages vulnerability countermeasures along with the configuration information. The system collects vulnerability information that has been discovered and disclosed and distributes the vulnerability information to relevant parties within the company if any of the registered configuration information is affected. After distribution, information on planned countermeasures is registered in the VPS to ensure that no action is omitted, and the actual status of the countermeasures is reported to the business manager on a monthly basis. Vulnerability information is collected using the vulnerability information collection service of NEC Solution Innovator, an NEC affiliate, and is linked to Japanese-translated vulnerability information in a timely manner (distributed at least once a day).

<https://www.first.org/newsroom/releases/2016>

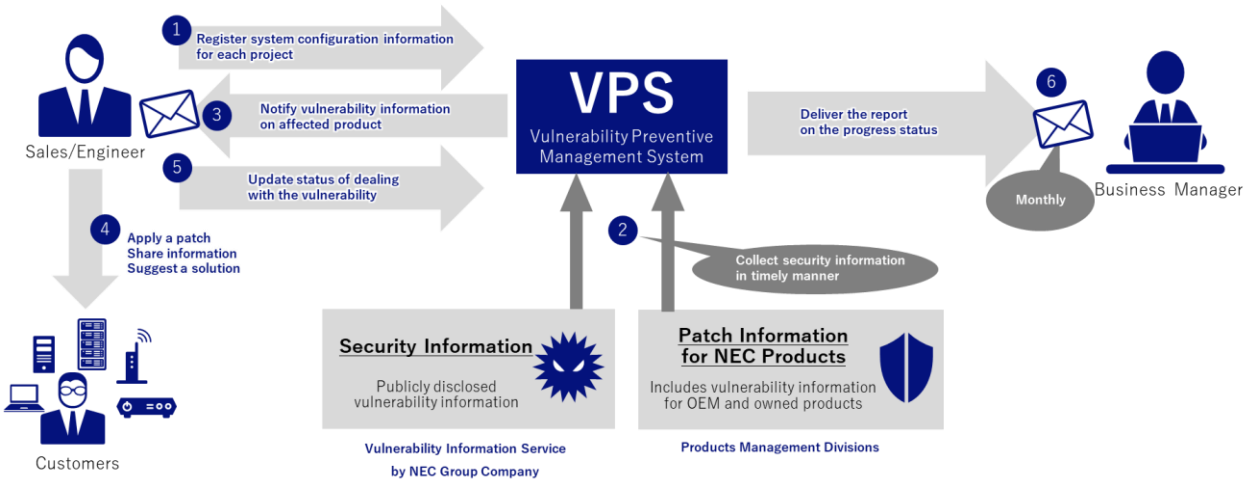


Figure 4.9-4 Mechanism of the Vulnerability Preventive Management System (VPS)

The service was launched and expanded in stages around 2006 and has been operating under its current structure since 2011, as shown in Figure 4.9-4. Specifically, the following functions were added: a configuration information input and management functions for OSS, etc.; a vulnerability information collection and viewing functions; a vulnerability information matching and distribution function; an input function for decisions on response and application of patches; and a periodic reporting function for business managers.

The system configuration information to be pre-registered in the VPS is granular in terms of OS, middleware, modules, etc. The reason for this is that the VPS is supposed to be directly managed and operated by human operators and that the minimum granularity of vulnerabilities to be managed is focused on the OS, middleware, modules, and other units. If the product manager or the project manager wishes to distribute vulnerability information or manage configuration information for a specific component, such information is managed in components, which are a more detailed unit.

Matching of vulnerability information with products registered in the VPS is performed by searching for vulnerability information from a list based on the software name and version in the product information. The good point of the VPS is that vulnerability information is in Japanese, so it is easy to understand at the field level when used at sites in Japan. In the case of configuration management tools from overseas vendors, even if it is possible to understand the information down to the component level, it is difficult to understand the vulnerability information at the field level because it is written in English. For this reason, NEC uses both VPS and configuration management tools from overseas vendors.

Functional enhancements are ongoing, with the most recent being the introduction of a service that distributes scripts to collect configuration information and registers the information on behalf of the VPS, in order to resolve the high workload of acquiring configuration information and status data and registering it with the VPS. In the future, the company is considering reflecting the concept of DevOps[101] by incorporating, into the VPS, the results of vulnerability scans conducted prior to shipment.

[101] A development approach in which software developers and operation staffs cooperate.

4.10. Nippon Telegraph and Telephone Corporation (NTT): Appropriate role sharing for OSS support

■ Company information

Head Office	Chiyoda-ku, Tokyo
Industry	Information and communication
Employees	303,350（as of the end of March 2019）
Commercial Flow	System integrators commercial flow/System integrators
Perspectives	[Vulnerability Response] [Organizational Structure]

■ Essence of this case

- The OSS support system was established by appropriately assigning roles to the OSS support organizations of each group company.

■ Background and issues

NTT, as one of Japan's major information and telecommunications companies, has many group companies. Many development projects are in progress at all times at both NTT and its group members, and many OSS are used in each project. To deal with OSS-related problems, it is necessary to make a unified effort as a group under an appropriate division of roles beyond the framework of companies.

■ Initiatives

<[Vulnerability Response (V10)] [Organizational Structure (O10)] Establishment of an OSS support system>

NTT has established the NTT OSS Center ("OSS Center") as a specialized organization for OSS support. The OSS Center offers OSS inquiry support in project design, development, and operation, troubleshooting services, provision of technically verified OSS stack model (OSSVERT[102]), and information provision services. The OSS Center also has a research function, and with the mission of creating innovative ICT services and expanding solutions, it is actively engaged in development collaboration with various communities.

[102] OSs Suites VERified Technically： Activities to verify the performance and appropriate settings of multiple OSS programs combined, and to compile them into technical documents as reference information, and to provide such information.

The OSS Center provides NTT Group companies with services tailored to the needs of each company. For example, in the software lifecycle management initiative, the OSS Center provides the NTT Group companies with a list of software that has reached the end of its maintenance period, for the purpose of effective governance, while providing each group company with on-site support for OSS version upgrades.

In addition, the portal site, which is the inquiry window of the OSS Center, actively provides the latest technical information on OSS that is not yet supported. The OSS Center provides technical support upon request, analyzes the access status of the information provision page, and takes a necessary approach. It provides optimal services in response to the rapidly evolving OSS market, and promotes OSS utilization by quickly responding to the needs of each group company.

In terms of support, the OSS Center collaborates with NTT's research department and support vendors. When an OSS-related vulnerability occurs, the center works with NTT's technical department and the group's CSIRT (NTT-CERT). It is also building cooperative relationships with other departments in various ways. As a concrete example, the OSS Center members are active in various communities and can quickly obtain the latest vulnerability information and security-related information. In such cases, the OSS Center participates in NTT-CERT's threat information distribution scheme to share the information.

The following figures show the activities of the OSS Center and its participation in the NTT Group's security threat information distribution scheme (Figure 4.10-1 and Figure 4.10-2).

Figure 4.10-1: Outline of OSS Center activities and positioning (in Japanese)[103]

[103] Excerpts from materials provided by NTT.

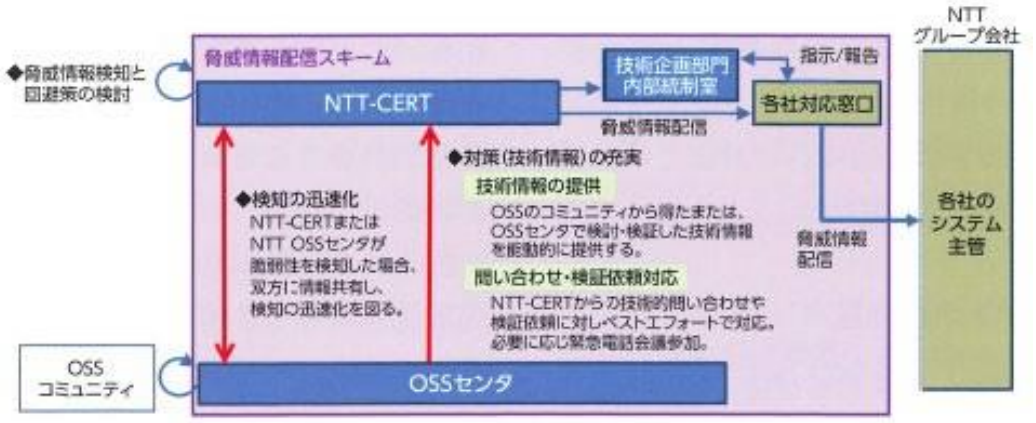


Figure 4.10-2: OSS Center's participation in NTT Group's Security Threat Information Distribution Scheme (in Japanese)[104]

On the other hand, each group company has its own OSS support unit, and the OSS center and the OSS support unit of each group company have a cooperative relationship and respond to each other's needs under an appropriate division of roles. For example, in support operations, the OSS Center responds to inquiries escalated[105] from the OSS support unit of each group company.

[104] Excerpts from materials provided by NTT.

[105] The OSS support unit of each group company decides whether to respond to an inquiry by itself or escalate it to the OSS center, depending on the nature of the inquiry.

4.11. Company A - Clarification of OSS selection criteria and community activities

■ Company information

Head Office	–
Industry	Information and communication
Employees	–
Commercial Flow	System integrators commercial flow/System integrators
Perspectives	[Selection Evaluation] [Maintenance and Quality Assurance] [Community Activities]

■ Essence of this case

- A list of OSS programs recommended for use and a list of OSS programs prohibited for use are maintained, and OSS selection criteria are clarified.
- The company views community activities as part of its business and fully supports participations.

■ Background and issues

Company A uses many OSS programs in its development projects. Therefore, measures for OSS need to be implemented under company-wide unified rules.

■ Initiatives

<[Selection Evaluation (S11)] [Maintenance and Quality Assurance (M11)] Company-wide unified OSS selection>

Company A considers the OSS selection phase to be the most important in OSS risk management. Specifically, a list of OSS programs recommended for use and a list of OSS programs unrecommended for use are prepared and shared internally. Of these, the selection criteria for recommended OSS programs are generally as follows:

(1) Support and other services are ensured because the commercial flow is through distributors.

(2) Community activities of the OSS are active.

(3) In-house engineers can access to the source code and propose workarounds[106].

Each list is reviewed periodically. In the review, updates such as addition and deletion of target OSS are made as necessary. In Company A, each list is used as a standard for selecting OSS[107]. In addition, the OSS support department[108] of Company A supports only OSS listed in the recommended OSS list[109].

In combination with Company A's long history of OSS initiatives, these lists are highly trusted within the company. Due in part to these efforts, there is little resistance to OSS utilization in company.

<[Community Activities (C11)] Support for community activities>

Company A participates in many community activities. The company considers community activities to be within the scope of its business and fully supports participation in them, based on the belief that the activation of the community and the conversion of its software to OSS are effective for the utilization of OSS in its business.

The company also seeks to raise the awareness of community activities by providing a place for internal presentations and an award system. In addition, expert employees in each community activity participate in the community activities together with younger employees to pass on development skills through OJT.

[106] Temporary measures.

[107] In some cases, OSS not included in these lists may be used due to client requests or other reason.

[108] The department is mainly staffed by engineers with experience in system development and operation or in software research and development in research departments.

[109] As an exception, support may be provided depending on the type of software and the status of the project. In such cases, problems can be resolved by working with the support vendor, using information from the community, or checking the source code.

4.12. Company B - Security enhancement focused on system integrators in the group

■ Company information

Head Office	–
Industry	Information and communication (System integrator of a subsidiary of a chemical manufacturer)
Employees	–
Commercial Flow	System integrators Commercial Flow & end user (chemical manufacturer)
Perspectives	[Personal Competence and Education] [Vulnerability Response]

■ Essence of this case

- Company B is promoting integrated security enhancement measures in deep cooperation with its group companies.
- Consideration is being given to the introduction of a system to centrally manage the OSS used.

■ Background and issues

Company B is a system integrator that is a subsidiary of a chemical manufacturer and provides IT solutions to the process industries that have chemical plants and other facilities on site.

■ Initiatives

<[Personal Competence and Education (P12)] Strengthen security mainly at system integrators in the Group>

Company B plays a central role in the IT functions under a chemical manufacturer and within its group companies. While providing IT solutions and system management to group companies, the company also promotes security enhancement. As an example, Company B has seconded its employees to its parent company, a chemical manufacturer, to work on security initiatives in all areas from the endpoint to the server side in its information system department. As part of such security activities, the company is also promoting OSS security initiatives.

In the series of actions related to the management of OSS usage described below, there are a number of situations involving human judgment, such as checking the accuracy of software vulnerability information and considering and implementing specific countermeasures. Therefore, Company B employees, who play a central role in security in the series of actions related to the management of OSS usage described below, there are a number of situations involving human judgment, such as checking the accuracy of software vulnerability information and considering and implementing specific countermeasures. Therefore, Company B employees, who play a central role in security enhancement within the group, need to have a high level of literacy about security as well as OSS. Company B has maintained a web-based education system for security for more than 10 years, and has been focusing on human resource education, and is trying to raise the level of literacy by providing education to employees until they obtain a certain score in an exam. In addition, Company B plans to provide the same level of education as Company B employees to IT-related personnel working at the parent company's global bases.

<[Vulnerability Response (V12)] Discussion on unified management of the OSS usage status>

A chemical manufacturer, which is the parent company of Company B, and its group companies use many OSS programs in their systems (including critical systems related to production) used in offices and chemical plants. In Company B, which is responsible for the management of these systems, the business unit in charge of applications and the business unit in charge of system infrastructure are currently managing the usage of OSS on an application basis and on a service basis, respectively. Each division also collects vulnerability information manually, and regularly collects software vulnerability information from IPA, communities, and Black Duck Open Hub. When necessary, the company applies security patches and takes other actions. However, since it is difficult to adjust the maintenance of applications if the actions are taken too frequently, the company conducts minor version upgrades, including the application of security patches about once a year, unless urgent action is required.

In recent years, as a result of the development and usefulness of functions such as package managers, OSS can include OSS components that are not recognized by developers. For this reason, Company B was fully aware of the problem that the OSS usage status is still be visualized company-wide, and since 2018, started examining the possibility of centralized management of OSS usage status, including versions, licenses, and vulnerabilities.

Company B studied commercial tools that enable centralized management of OSS usage and found that certain tools can automate the process of identifying the OSS used in applications, as well as the relevant OSS licenses and vulnerability information. Meanwhile, it was found that the tools sometimes offered multiple ways to deal with discovered vulnerabilities, and that human judgment was needed to select the best way to deal with them.

Based on the results of this study, Company B is planning the following system: the security department of Company B will centrally manage data on OSS usage status in each application and service, by using commercial tools; when vulnerability information is obtained, the team in charge of the application will respond to the vulnerability, based on the data; and then the department in charge of security will examine the validity of the response.

4.13. Sompo Japan Insurance Inc.: Vulnerability management using a Software Bill of Materials

■ Company information

Head Office	Shinjuku-ku, Tokyo
Industry	Finance (Insurance business)
Employees	24,689 (as of the end of April 2020)
Commercial Flow	System integrators commercial flow/system end user (Finance)
Perspectives	[Personal Competence and Education] [Licensing] [Vulnerability Response]

■ Essence of this case

- Utilizing the Software Bill of Materials (SBOM), risk management for vulnerabilities, licenses, etc. is implemented thoroughly.
- The management is strongly aware of the importance of cyber security and is making efforts to have the employees understand the necessity, such as top-down awareness-raising on vulnerability response.

■ Background and issues

Since 2015, Sompo Japan has been working with its systems subsidiary to revamp its core system and promote digital transformation (DX) in various aspects in order to meet the diversifying needs of financial services. In order to promote these activities, it is necessary to handle a wide range of technologies including OSS. In addition, due to the characteristics of the industry, a critical service level is required, which requires advanced software management in system development and operation.

■ Initiatives

<[Personal Competence and Education (P13)] Cybersecurity initiatives starting with the CIO>

At Sompo Japan, the CIO takes the lead in promoting cyber security initiatives. Specifically, the CIO personally collects information from advanced companies and IT vendors in Japan and abroad and is continuously involved in the development of a cyber security system by hiring and training external personnel.

In this context, Sompo Japan' OSS response unit[110] is strengthening its software management and vulnerability management by appointing skilled personnel in cooperation with its system-related subsidiaries. In particular, the system-related subsidiary has established an organization dedicated to software management and has set up a system to keep up with the rapidly changing DX.

Meanwhile, at the frontline (system operators) level, the priority of security is relatively low due to the busy workload associated with the rapid progress of DX. Risks may not be properly recognized even if there is a possibility that the system may be affected by vulnerabilities. In order to prevent such a situation, the CIO and others have been making efforts to raise awareness of risks by providing top-down education.

In 2018, Sompo Japan also set up a digital lab in Tel Aviv, Israel, to gather solutions and expertise on cybersecurity.

<[Licensing(L13)] [Vulnerability Response (V13)] Use of the Software Bill of Materials (SBOM) >

In recent years, Sompo Japan Insurance Inc. has built a system that uses a number of OSS modules. This system has been applied to in-house production, receipt of deliveries from vendors, etc., and other work processes. In these processes, OSS management using the software bill of materials (SBOM) is thoroughly implemented to ensure OSS vulnerability management and risk management. Specifically, the SBOM is used for system "before development," "during development," "final delivery," and "after delivery".

(1) In the pre-development phase, the general framework of OSS usage is summarized on an application basis and incorporated into procurement

[110] The main task is to identify and manage risks to internal information security and to develop strategies for software use.

management.

(2) During the development phase, a detailed description of the OSS usage status is created using a scanning tool, and an SBOM is created based on the description. The SBOM is reflected in the process management.

(3) In the final delivery and operation phase, the created SBOMs are stored in a database for each system and utilized in vulnerability management and risk management.

The details of each phase are described below:

(1) Pre-development phase

Based on the application from each project, the OSS usage status (usage location, version, etc.) is clarified. Also, based on the application, risk analysis and evaluation are conducted to clarify "version," "quality (vulnerability, community activity status)," "need for export control" [111] and "license (occurrence of obligation or not)" (Figure 4.13-1).

In addition, based on the evaluation and the importance [112] of the system, countermeasures are considered as necessary. This is intended to address risks such as licensing issues that can be identified in the pre-development stage at an early stage. This series of tasks is integrated into the procurement flow and managed.

NO	OSS Name	Outline	Service used *The version is shown in the parentheses.				Risk Category			
			Service A	Service B	Service C	Service 4	Version used	Quality (Vln, etc.)	Eport management	License (Mandatory provision)
1	△△	A package of software necessary for software development in the programming language XX	✓ (X123)				✗			
				✓ (X456)				✗		
					✓ (X789)					
						✓ (X789)				✗

Visualization of usage locations and versions | **Risk analysis**

Figure 4.13-1: OSS checklist format to be prepared at the time of application for development[113]

[111] When OSS is used in a system, Sompo Japan checks whether the system will be used overseas in the future, and if so, whether the OSS used does not contain cryptographic modules, etc., so as not to violate Japan's export regulations.

[112] The importance of a system is determined from the perspective of whether the system is critical enough to be used in business or whether it has only a small impact on productivity.

[113] Compiled based on materials provided by Sompo Japan Insurance Inc. The "X" mark in the risk classification column indicates that countermeasures need to be taken.

(2) Development phase

In the development stage, the OSS usage status of the actual software is determined using commercial tools. In this process, OSS information that could not be fully clarified in the pre-development phase (1) is acquired, and risks are detected by static analysis. Sompo Japan uses the acquired OSS information as SBOM. With the tool, OSS risks and vulnerabilities can be visualized by library unit using SBOM. These risks are analyzed for each application, leading to early detection and response to problems. These series of operations are managed as part of the development process (Figure 4.13-2).

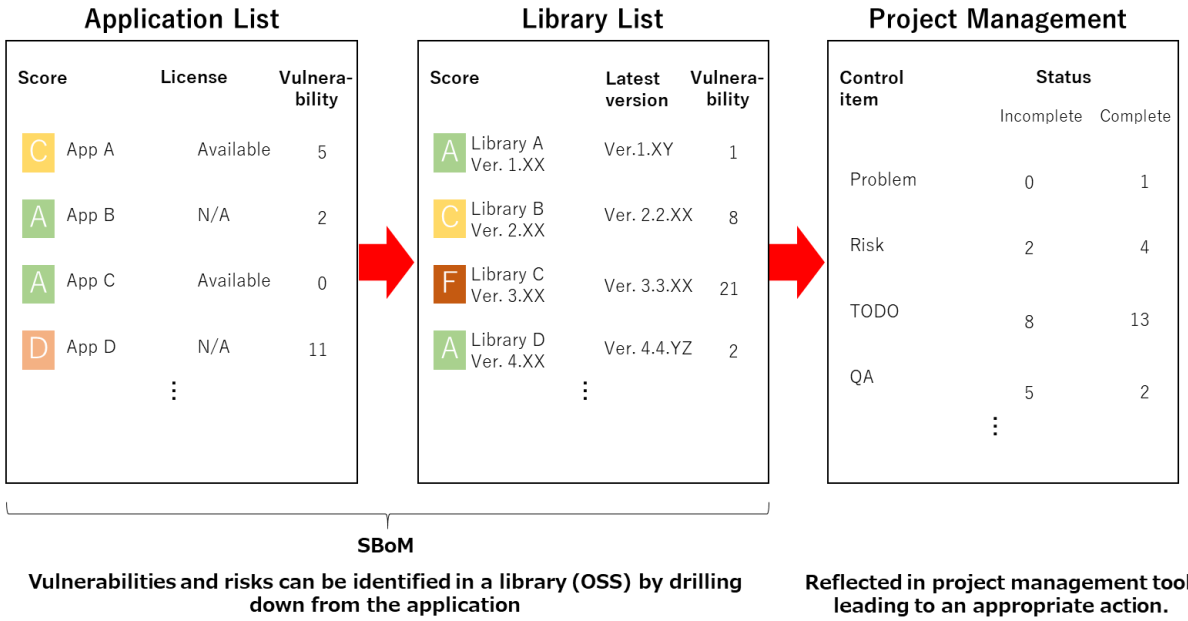


Figure 4.13-2: Image of utilization of SBOMs created by the tool during development[114]

(3) Final delivery and operation phase

Before the delivery of a system, the entire system is rescanned with a tool to make sure that it does not contain any unrecognized OSS. At the same time, the system is analyzed while it is running (dynamic analysis) to detect any risks that could not be confirmed by the static analysis made in (2). SBOMs reflecting the results of the final check are stored in a database for each system and is used for daily vulnerability management. Specifically, based on the information on vulnerabilities obtained by the tool from external sources on a daily basis, alerts are automatically issued to the personnel in charge of the system that may be

[114] Compiled based on materials provided by Sompo Japan Insurance Inc.

affected by the vulnerabilities.

In addition, Sompo Japan's OSS response unit follows up with system staff who receive alerts as necessary, and other mechanisms are in place to ensure that vulnerability responses are completed appropriately.

In the past, Sompo Japan used to manage OSS manually. Since the names of OSS programs registered in the database were not unified, it was complicated to check the usage status. However, after the automation of database creation using commercial tools in (2) and (3), these operational problems were solved.

4.14. Visional Group: Using the best tool for the situation

■ Company information

Head Office	Shibuya-ku, Tokyo
Industry	Information and communication
Employees (Group employees)	1,385 (as of the end of January 2021)
Commercial Flow	System integrators commercial flow/system end user (IT service)
Perspectives	[Vulnerability Response]

■ Essence of this case

- While the use of OSS is relatively free at the development site, Visional developed and commercialized a tool that fits its own situation where many vulnerabilities are detected at once.
- In developing the tool in-house, the company has improved its functions through repeated internal and external testing and feedback.
- OSS management using tools has been established as a rule, and the security department has taken the lead in setting up a vulnerability response system.

■ Background and issues

As an IT company, BizReach[115] (now Visional Group[116]) considers it an important value that engineers in the development field can freely select and use the most appropriate technology to create services. In this context, OSS was actively used for reasons such as reduction of development man-hours.

On the other hand, as the business took off, the number of OSS programs used in each service was diverse, and manual management was not enough to deal with the large amount of software vulnerabilities that occurred.

[115] BizReach is a Visional group company. The OSS vulnerability management tool "yamory" discussed in this case study was initially released by BizReach in 2019. Later, with the transition to a group management structure, the Visional Group was created, and Visional Incubation was established to handle new business development. Currently, Visional Incubation is responsible for the development and sales of yamory.

[116] A corporate group including Visional Incubation and BizReach.

- Initiatives

  <Development and commercialization of optimal tools for the company's situation>

  BizReach searched for the best OSS management method, based on the awareness of the need to ensure security by firmly addressing software vulnerabilities. The company needed to create a security standard and management system that should be adhered to at the very least, while respecting the culture that had allowed it to freely choose technologies.

  Under such circumstances, BizReach engineers, who felt challenges in OSS management, conducted interviews with several companies regarding OSS management. The survey revealed that other companies also had the same issue recognition, raising the need to develop new tools to efficiently manage security risks.

  Although it was difficult for Visional to secure internal resources for the development of a tool to be used in-house, they thought that, if other companies also had needs, they should develop it as a security countermeasure software business and started the development of the OSS vulnerability management tool "yamory" by utilizing the internal new business planning system.

  <Improvement of tool functions based on feedback from inside and outside the company>

  In the development of yamory, Visional improved its performance through repeated prototyping and feedback from internal tests. In addition, once the product concept was solidified, it conducted external tests for commercialization. Upon a proposal based on the results of internal tests, dozens of companies participated in the tests, and as a result, Visional successfully obtained a lot of feedback[117].

  Based on these feedbacks, Visional created a function to support vulnerability triage (classification according to urgency) according to their urgency when a large number of vulnerabilities are detected and also devised a mechanism to display the

  vulnerability information in an easy-to-understand list on the dashboard (Figure 4.14-1). These functions have made OSS management and vulnerability response much more efficient.

[117] Visional has received requests for the implementation of management functions for license risks and middleware/OS layer vulnerabilities.

Figure 4.14-1: The dashboard of yamory, which clearly shows the vulnerability of each level by the triage function (in Japanese)[118]

<[Vulnerability Response (V14)] Development of internal rules using a developed tool>

Currently, the Visional group has made it a group-wide rule to use yamory for OSS management. Before release of a service, the service development team must scan for any OSS in the service by using yamory. In addition, the development team automatically scans the OSS they are using on a daily basis in cooperation with GitHub, which manages the development and source code. The OSS list created by the scan is combined with the OSS vulnerability information collected on a daily basis and is used to detect the presence of vulnerabilities in the company's services after release.

Vulnerability information is classified (triaged) according to the risk level on the yamory dashboard and displayed for each service or as a company-wide overview (Figure 4.14-2). This information is routinely verified by each business department and the group security department. When any vulnerability is detected, the group security department takes the initiative to instruct the relevant business department to take necessary actions. In addition, once every six months, the group security department conducts a group-wide security check[119] for each service. At that time, a report stating that all OSS-related vulnerabilities have been resolved must be

[118] Excerpts from materials provided by Visional Group.

[119] Not only do the department check for vulnerabilities related to OSS, but also it performs a total product security check. At this time, checks are also made for OS, major middleware, software EOL, etc. that cannot be managed by the tool.

prepared and submitted using yamory.

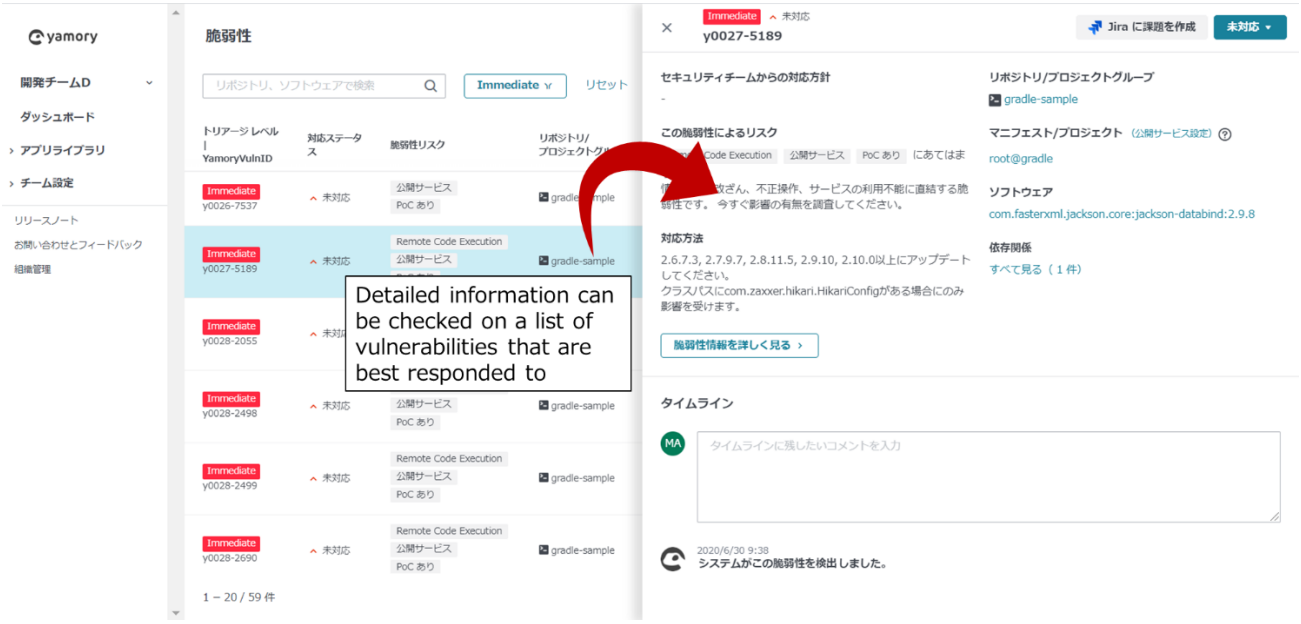


Figure 4.14-2: Vulnerability list screen, which contains a detailed description of the response[120]

In order to establish a group-wide rule for OSS management using yamory, the development team appealed to the development sites of each service that the triage function would reduce the burden of handling vulnerabilities related to OSS. In fact, each development site was burdened with its own vulnerability management and accepted the use of the tool. Eventually, the security department became more aware of the need for efficient and appropriate management of OSS, which led to the establishment of group-wide rules.

<Future Outlook>

In the future, Visional plans to add functions related to EOL management and vulnerability management of middleware and OS, which are not yet covered by yamory, as well as promoting research and development to enable more intensive OSS management.

The yamory sales unit has received various comments from customers on OSS management (requests for additional functions, consultations on operation, etc.). Companies use different OSS management methods depending on the quality of information handled and the type of industry. Some companies are having difficulty in appropriate OSS management. Visional Incubation will continue to improve its

[120] Compiled based on materials provided by Visional Group.

products (tools) and operational methods within the group to increase the value provided to customers.

4.15. Cybozu, Inc.: OSS policy contributing to the OSS ecosystem

■ Company information

Head Office	Chuo-ku, Tokyo
Industry	Information and communication
Employees	741 (as of the end of December 2019)
Commercial Flow	System integrators commercial flow/system end user (IT service)
Perspectives	[Licensing] [Personal Competence and Education] [Community Activities] [Selection Evaluation] [Vulnerability Response] [Organizational Structure]

■ Essence of this case

- In order to contribute to the OSS ecosystem, a cross-divisional organization was established, and a company-wide OSS policy was formulated.
- The PSIRT plays a central role in handling software vulnerability information and operating a vulnerability reward system to ensure thorough efforts to eliminate software vulnerabilities in the company's services.

■ Background and issues

Cybozu uses a large amount of OSS in the infrastructure of its mainstay web services, kintone and cybozu.com. However, until a few years ago, when using OSS, developers and legal staff individually verified the licenses and complied with the licenses subject to the approval of their superiors, and there was no company-wide policy including OSS development.

■ Initiatives

<[Licensing (L15)] [Personal Competence and Education (P15)] [Community Activities (C15)] Formulation of OSS policies that contribute to the OSS ecosystem>

Cybozu established the OSS Preparation Office in 2017 for the purpose of formulating OSS policies that support and encourage employees to contribute to open source activities. This office is a cross-departmental organization consisting of representatives from various OSS-related departments throughout the company, with the ultimate goal of contributing to the development of OSS.

The OSS Preparation Office formulated the OSS Policy and applied its rules to the entire company, and also developed the OSS Guidelines, which are detailed regulations that complement the OSS Policy. The OSS policy stipulates the handling of copyrights, patents, and trademark licenses, etc. The Cybozu OSS policy is published in the public domain (CC0) (Table 4.15-1).

Table 4.15-1: Composition of Cybozu OSS policy[121]

0. About This Document	
1. Introduction	
2. Copyright	2.1 Attribution of copyrights
	2.2. Transfer of copyrights
3. Open sourcing of Employees' Personal Works and Use of Our Trademarks	3.1 Disclaimer
	3.2 Use of our trademarks
4. Open sourcing of Our Works	4.1 Publishing under an OSS license
	4.2 Providing for third-party OSS
5. Use of Third-party OSS	5.1 Checking third-party OSS for license
	5.2 Handling license documents, etc.
	5.3 Reporting defects in third-party OSS
6. Incorporation of Third-party Works into Our OSS	6.1 Handling third-party works offered
	6.2 Managing a contributor list
7. Responding to License Violations	7.1 Responding to the use in violation of our OSS license
	7.2 Responding to internal OSS license violations

[121] Cybozu OSS policy. (in Japanese)
https://cybozu-oss-policy.readthedocs.io/ja/latest/

Since Cybozu often converts software developed in-house into OSS, its OSS policy also stipulates the items that must be observed in such conversion. The OSS policy includes a provision that enables OSS conversion with a simplified approval procedure, as part of its contribution to the OSS ecosystem. Furthermore, to motivate developers to promote the use of OSS, there is a provision that software created voluntarily by employees shall be the copyrighted work of the employee who developed it, unless it contains a Cybozu license or confidential information. Thus, the OSS policy is designed for wide utilization of OSS.

The company's proactive stance toward the use of OSS has produced a variety of effects. These effects include a practical benefit of feedback obtained from outside the company about bugs in OSS-versioned software, as well as the use of OSS as a material to appeal the company's technical capabilities and its liberal corporate culture in recruitment activities.

As a company whose main service is groupware such as kintone, Cybozu had an environment in which all employees could easily communicate through groupware. In this context, the then general manager of the operations division took the lead in launching the OSS Preparation Office and formulating and disclosing the policy, raising awareness of the necessity from the top down, and strongly promoting the initiatives.

The OSS Preparation Office was dissolved in 2018, with its functions taken over by the newly established Open Source Program Office [122]. Currently, the Open Source Program Office maintains the OSS Guidelines, which define OSS policies and bylaws.

<[Selection Evaluation (S15)] [Vulnerability Response (V15)] [Organizational Structure (O15)] Dealing with various software vulnerability led by PSIRT>

When using OSS for its services, Cybozu's development team must conduct a study of the OSS they wish to use, in accordance with the OSS policy and OSS guidelines mentioned above. As a result of the study, if it is confirmed that the license conforms to the guidelines established within the company and that it is regularly updated, then the OSS may be used. Even if the license does not meet the guidelines or is not regularly updated, the OSS may still be available subject to a legal review and a check to see if the company is capable of handling bugs and other issues.

Each development team registers information on the OSS it uses, in a database, after conducting such a review. The information is finally reviewed by the development

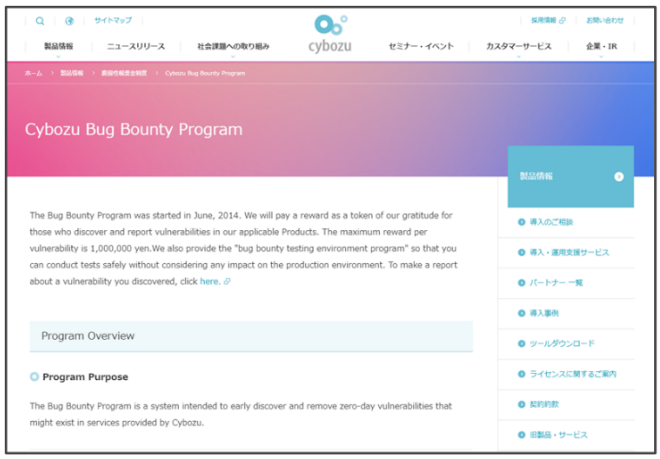
[122] As of January 2021, there are seven members.

team to ensure that there are no omissions. The PSIRT of Cybozu regularly refers to the database, and a cycle is established to provide feedback to the development team when there is information on version upgrades, etc.

The PSIRT collects software vulnerability information from primary sources such as OSS repositories and sites, JVN, security news sites, on a daily basis. When software vulnerability information is obtained, the PSIRT searches the database for services that use related OSS and checks them. If a relevant service is identified, the PSIRT takes the lead in handling the information and issues an alert to the person in charge of the service via groupware (kintone).

When an OSS program is newly used in the company, the OSS is registered as a master, and the service and the OSS used are centrally linked in the database, starting from the master. Therefore, even if the OSS name information in the software vulnerability information is inconsistent, the company can respond quickly.

The Cybozu PSIRT operates a bug bounty program (Figure 4.15-1). This system pays rewards to external parties who discover and report vulnerabilities in Cybozu products, including vulnerabilities in the services themselves and the use of vulnerable OSS. The rewards are determined based on sincere responses, such as providing an environment for verification. In order to eradicate vulnerabilities so that the amount of incentive payments will not be too high, the PDCA cycle starting with this incentive system is being operated. This cycle includes a measure to reduce the number of external suggestions as much as possible, such as having the company's own vulnerability assessment by a specialized security company, as well as a measure to develop the skills and literacy of employees to respond appropriately to external suggestions.



- This program implemented since 2014 to improve the security quality of services
- In FY2019, 489 received, 193 certified (provisional), and 15.35-million-yen reward payment amount (provisional)
- Holding events to gather bug hunters and have them find vulnerabilities.

Figure 4.15-1: Bug Bounty Program website and its overview[123]

[123] Bug bounty program website
https://cybozu.co.jp/products/bug-bounty/en/

2019 Reward Program Results (in Japanese)
https://blog.cybozu.io/entry/2020/05/07/110331

4.16. Mitsubishi Electric Information Systems Corporation (MDIS): Solution deployment based on OSS characteristics

- Company information

Head Office	Minato-ku, Tokyo
Industry	Information and communication
Employees	1,279（as of the end of March 2021）
Commercial Flow	Product commercial flow/end product manufacturer
Perspectives	[Selection Evaluation] [Maintenance and Quality Assurance] [Community Activities] [Vulnerability Response] [Licensing]

- Essence of this case

  - In providing solutions that involve OSS, MDIS agrees in advance with its clients on the concept of vulnerability management and costs associated with responding to updates when using OSS for a long period of time.
  - In order to properly understand and manage the OSS used, it is important to be involved with the community. When bugs are discovered, MDIS not only reports bugs to the community but also contributes by informing them of remedial measures.

- Background and issues

The Mitsubishi Electric Group utilizes OSS in the products and solutions it develops and has established a company-wide organizational structure for OSS management while conducting research activities.

MDIS provides OSS-based solutions for communication providers and service providers. The telecommunications industry provides large-scale services to many customers (e.g., SMS/MMS services for cell phones), which would incur huge licensing costs if paid software were used. Therefore, the telecommunications industry is actively using free OSS instead of paid software.

■ Initiatives

<[Selection Evaluation (S16)] Providing open source utilization solutions>

MDIS provides open source utilization solutions for service providers, supporting the entire OSS-based system lifecycle. As mentioned above, the telecommunications industry, to which MDIS provides solutions, is active in utilizing OSS, and MDIS provides systems and solutions that utilize OSS based on requests from their clients. In utilizing OSS, the company places importance on researching and selecting OSS, as well as maintaining OSS operations after development. MDIS assumes that systems and solutions will be in use for approximately five years, and to maintain OSS operations during that time, MDIS monitors patches and vulnerability information and applies patches as needed, while remaining involved in the OSS community.

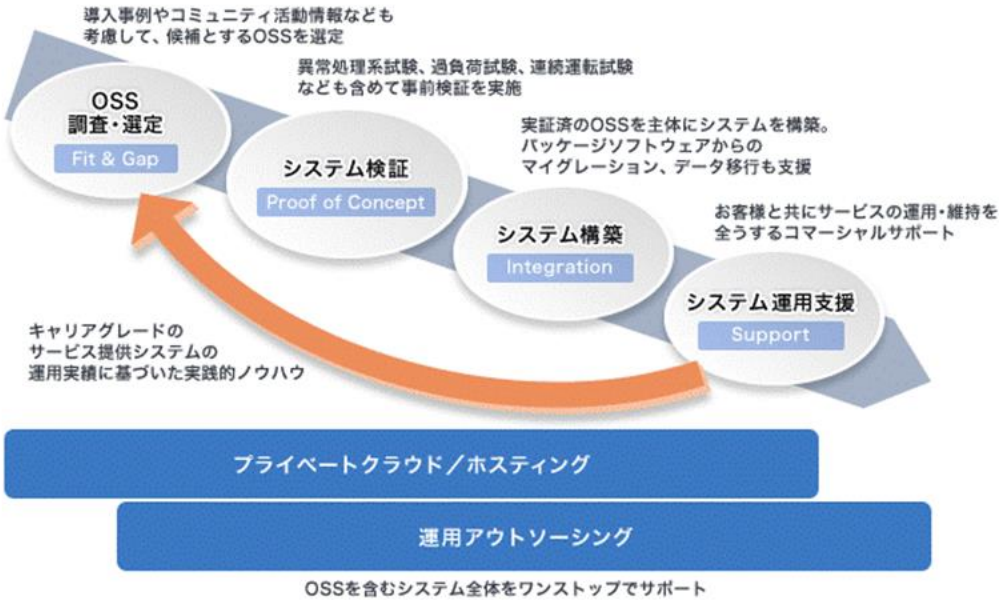


Figure 4.16-1 Open source utilization solution (for communication providers and service providers) overview image (in Japanese)[124]

[124] Excerpt from the introduction page of open source utilization solutions for communication providers and service providers
https://www.mdis.co.jp/service/oss/

<[Maintenance and Quality Assurance (M16)] [Community Activities (C16-1)] Providing open source utilization solutions>

In using OSS for as long as five years, there is a risk that the OSS community will terminate developing and supporting services, including Vulnerability Response. Therefore, the company identifies the risks that may occur in the early stages of development and explains and agrees in advance with the customer on the possible situations that may occur and the maintenance costs for countermeasures. In particular, it is important that customers understand that there is a risk of incurring countermeasure costs even after the relevant development and support have been completed.

When OSS is modified, MDIS once experienced difficulties in how to return it to the development community. Because the OSS community and Github are structured with the assumption that individual developers are involved, it is difficult for companies to treat it as an organizational artifact even when it is modified in an organized manner. Therefore, it was necessary to calculate the degree of contribution among the employees and subcontractors involved in the design, programming, and testing with respect to the modification and to determine a method of return that was acceptable to all members of the team, in light of the contract. It was also necessary to determine how to display the contact information, assuming the support structure and division of labor in subsequent years.

<[Vulnerability Response (V16)] Managing Vulnerability Information>

Information is collected at various sites that disclose OSS vulnerabilities, with reference to the vulnerability information push function included with the configuration management tool. In addition, there is a mailing list for disseminating information including vulnerability information from the OSS community. The mailing list is subscribed to by MDIS development members. On the other hand, in cases where there are no community activities in the OSS community and thus vulnerability information cannot be obtained, vulnerability management tools are sometimes used to analyze vulnerabilities in the OSS used.

<[Licensing (L16)] Configuration Management Method>

SBOM is not actively used in departments that do not use OSS much, use their own software, or complete development within their business unit. However, in the case of outsourcing, OSS may be incorporated without their knowledge, so MDIS uses a

configuration management tool to analyze the software and check whether OSS is incorporated. Believing that preventing licensing violations is important from both compliance and business perspectives, MDIS is working on software analysis using configuration management tools as a self-defense measure against licensing violations.

<[Community Activities (C16-2)] Involvement in the OSS community>

The OSS community is a place where system integrators gather information mainly for OSS selection evaluation and OSS operational maintenance. As part of their contribution to the OSS community, upon finding a bug in OSS, system integrators contact the community not only to point out the bug but also to suggest remedial measures.

The solutions offered by MDIS are characterized by "continuous commercial support". MDIS' role is to support OSS itself or to package it to a commercial level and deploy it in commercial distribution. To play this role, MDIS needs to acquire sufficient information about the OSS. To this end, when MDIS find bugs or obtains any vulnerability, they try to be actively involved in the OSS community, for example, by cooperating with them to improve the OSS.

4.17. OSSTech Corporation: Software management with OSS

- Company information

Head Office	Shinagawa-ku, Tokyo
Industry	Information and communication
Employees	19 (as of August 2021)
Commercial Flow	System integrators commercial flow/system end user (IT service)
Perspectives	[Licensing] [Vulnerability Response] [Supply Chain Management]

- Essence of this case
  - In solutions using OSS, there are points to keep in mind about the way OSS is handled and about the form of contracts with the users to whom the solution is provided.
  - In configuration management, software dependencies are managed while utilizing functions provided by OSS such as a build system.

- Background and issues

OSSTech offers solutions using OpenAM[125], an OSS for authentication system, which requires security-conscious use and operation. In addition, there is a need for a method that can be managed by a small number of people while making specialized use of OSS. As one of such methods, OSSTech is working on the management using the functions of the development environment.

- Initiatives

<[Licensing (L17)] Contractual arrangements with suppliers>

Compared to software developed on a contract basis, it is necessary, when using OSS, to pay attention to points such as licensing of components to be provided to users and contracts that include such provisions as the handling of copyrighted materials developed in connection with the software (sub-modules, documentation

[125] OSS that provides a single sign-on environment.

of developed portions, etc.).

OSSTech aligns the licensing form of functions and modules developed for users with licensing forms based on core components, such as the GPL and Apache License. There may be a discrepancy between OSSTech's terms and those of the users, who desire to limit the conditions of use to their own advantage. Therefore, it is important to clarify and agree on the scope of OSS licensing at the contract stage.

<[Vulnerability Response (V17)] Vulnerability information management >

Recent OSS, such as OpenAM, used and provided by OSSTech are developed and managed collaboratively by the community through the use of GitHub. In the GitHub service, vulnerability information on OSS registered in the repository is distributed. Developers using this OSS check the information sent to them and use it as needed. In this way, software safety can be assured through the use of the service and its mechanism.

Since the areas to be verified and addressed in vulnerability management vary by OSS and product, the development staff for each product collects information from the upstream of the OSS. The information collected by the development staff enables efficient and accurate collection and management of vulnerabilities. In addition, upstream vulnerability information is verified through the developers' mailing list and BTS (bug tracking system)[126] to prevent the lack of action.

<[Supply Chain Management (S17)] Managing software using OSS>

With respect to the management of software using OSS, OSSTech believes that, when SBOM is provided to software users, it is important to provide a tool that automatically check for vulnerabilities at the same time, so that a vulnerability update can be implemented. If users are not able to do this themselves, OSSTech believes that outsourcing to specialized companies, including their support system, is a realistic option, for the following reasons:

- Many users are willing to let the vendor handle everything, including OSS vulnerability updates, for a support fee. Users are not highly conscious of managing software components, while their objective is to ensure security.

[126] A system to manage and share bugs in programs during software development and maintenance.

- In the case of embedded products, it is possible to manage the SBOM using Excel, but if the number of dependent libraries exceeds 100 or 1,000, the management burden will be extremely high.
- If there are no updates to a product, the SBOM will basically remain the same. However, if, for example, a product dynamically links OS standard libraries, the SBOM may need to be updated as there are changes to the library depended upon. For this reason, even if an SBOM is provided to users, it is unclear whether they can utilize the SBOM and properly manage and update vulnerability information.

4.18. Yahoo Japan Corporation: Establishing a system for employees to use OSS correctly

- Company information

Head Office	Chiyoda-ku, Tokyo
Industry	Information and communication
Employees	Unconsolidated: 7,167 (as of the end of March 2021)
Commercial Flow	Internet service provider
Perspectives	[Selection Evaluation] [Licensing] [Vulnerability Response] [Personal Competence and Education] [Organizational Structure] [Maintenance and Quality Assurance] [Supply Chain Management] [Community Activities]

- Essence of this case
  - Governance for the handling of OSS is in place throughout Yahoo Japan, and OSS may be used subject to multiple reviews.
  - Criteria for OSS that may be used are defined in guidelines tied to technical regulations.
  - By using multiple tools, OSS management, and software vulnerability response are conducted without omissions.
  - Although Yahoo does not outsource development when it does, it manages OSS by specifying an OSS list in the order requirements.
  - Yahoo supports employee participation in the community by revising personnel rules and establishing systems that are easy for employees contributing to OSS to use, such as an OSS developer certification program.

- Background and issues

In order to provide better services quickly, Yahoo uses a great deal of OSS in its services and the platforms that support them. For this reason, the company has established guidelines for the use of OSS and has established and complies with various regulations for such matters as OSS selection to implementation, maintenance, and operation to ensure that high-quality services can be provided. In addition, the company's active participation in the community has had a

significant impact on the development of its own business.

- Initiatives

<[Selection Evaluation (S18)] OSS approval through collaboration between the development and the legal department>

Regarding the selection of OSS, Yahoo defines in its guidelines the OSS that may be used after legal confirmation. Basically, licensed OSS may not be used unless legally verified. The OSS that has not undergone legal review may not be used unless it has undergone the prescribed review process to confirm that it has no problems as an open source and has also undergone the approval process by the person in charge of technology. For OSS that has not been approved for use, the above review is conducted at an earlier stage, and if there are no problems, the use is approved and the OSS that has newly become available for use is addressed in the subordinate rules.

<[Licensing (L18)] [Vulnerability Response (V18)] [Personal Competence and Education (P18)] [Organizational Structure (O18)] Compliance system for OSS utilization and operational efficiency >

Yahoo uses so much OSS in its web services that its services would not be possible without it. Around 2009, the use of OSS within the company increased more rapidly than ever before in the rapidly changing Internet industry, and a system was created to strengthen the appropriate use of OSS by employees. In addition, in consideration of the growing compliance awareness across the world, education and examinations on software as well as photos and music are conducted as part of the compliance training for all employees regarding copyrights. Yahoo Japan has established the following three basic policies regarding OSS, and is providing high-quality services through development in compliance with these policies:

・Regulations on the use of open sources.

・Contribution to OSS.

・Open sources made public from within Yahoo.

Currently, when using OSS in services developed by Yahoo, permission to use the OSS is not granted unless the OSS used is declared in accordance with the process set forth in the guidelines, and then it goes through certain checks. Specifically, education is provided to ensure that each OSS user can comply with the rights and

obligations stipulated in the license and that the user can use the OSS stably in the future.

The legal affairs department checks the contents of the OSS license, which is a prerequisite for the specific selection of OSS, and if the OSS license is allowed to be used, the license is listed as a confirmed license and disclosed internally. Before using the OSS, the user should check whether the OSS licensing he/she desires to use is included in the list. Basically, any license that has not been confirmed by the legal department may not be used.

In addition to licensing, Yahoo also checks in the selection process whether certain OSS has no problems in various aspects such as copyright and intellectual property rights for use. For the purpose of reducing the costs involved in the selection process, OSS that are used frequently throughout the company and have high selection costs are subjected to preliminary screening by a specialized unit, rather than the selection process. The OSS concerned is newly added to the subordinate rules of the guidelines.

Other OSS are put through a selection process, during which, it is verified whether the OSS in question is licensed and whether it is acceptable for use. After the selection process is completed, an application for use of the OSS is submitted, reviewed, and approved by the technical manager to ensure that there are no problems with the content of the application. During the selection process, a combination of various tools is used for checking licenses and other matters.

There are two types of software vulnerability response initiatives: CSIRT-led response and tool-based response. For high-risk vulnerabilities, the CSIRT takes the lead in requesting each business unit to take necessary actions based on the regulations. For other vulnerabilities, tools automatically detect vulnerability information and alert the developers, enabling them to quickly respond to software vulnerabilities. To prevent oversights, Yahoo uses multiple tools to check for vulnerabilities at each phase from development to operation.

Furthermore, Yahoo has opportunities to release, as an OSS, software developed in-house or in collaboration with other companies. To contribute to such communities, Yahoo has also established a system whereby software undergoes a check by the technical director to ensure that it does not violate licensing or infringe on the rights of third parties (Figure 4.18-1).

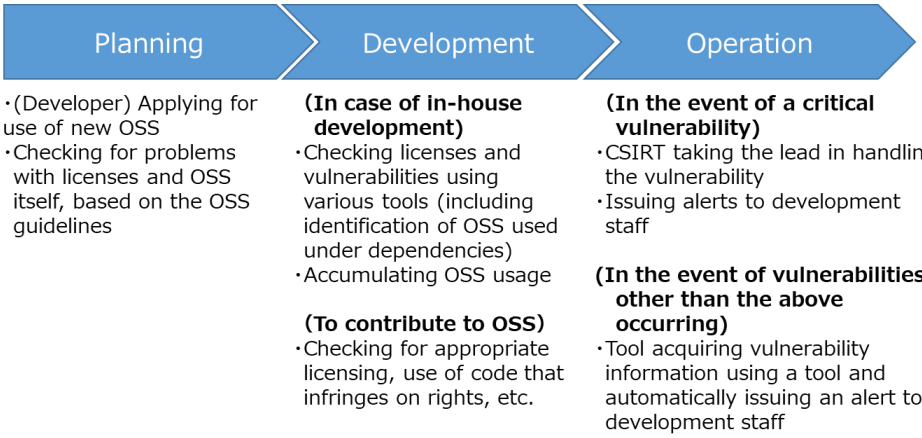


Figure 4.18-1 Overall view of OSS management at Yahoo[127]

In order to get these operations on track, the CTO[128] took a top-down approach to control each business unit and implemented training programs for developers. In order to spread awareness of compliance and security, explanatory meetings, etc. were held for developers and business promotion staff, in which the necessity of taking action was logically emphasized and understandings were obtained through careful communication.

<[Maintenance and Quality Assurance (M18)] Compliance with community-defined lifetime cycle>

Regarding the years of use of services using OSS, the OSS community provides a reference that shows how to operate the services so that they are used in accordance with the lifecycle defined by the OSS community, and the services are basically used on the assumption that they conform to that lifecycle. However, there are cases where Yahoo is responsible for continuing the service after the EOL, such as when a switch cannot be made. For those that continue to use the service after the EOL, Yahoo will consider using paid support from other companies.

<[Supply Chain Management (S18)] Outsourced development>

Yahoo does most of its development on its own, and there are basically only a few cases where it actually outsources development to outside companies. If outsourcing is to be done, a list of OSS is included in the order requirements to be

[127] Based on interviews

[128] Chief Technology Officer

strictly complied with. The granularity of the OSS to be listed is based on the libraries and frameworks explicitly used, and tools are used to know the details of the OSS.

<[Community Activities (C18)] Easy-to-use system for employees contributing to OSS>

Yahoo is contributing to the development of the OSS ecosystem through the aforementioned conversion to OSS of in-house developed software, OSS development in collaboration with other companies, or active participation in the community. These activities not only return profits to the company's business through OSS improvements, but also improve the technical skills of developers.

As one of the most noteworthy initiatives for Yahoo's community activities, in order to encourage employees to freely contribute to the OSS, the personnel regulations provide for the attribution of work products created in the course of their duties to individuals if the company approves. Yahoo also operates an OSS developer certification program. This system was established to provide opportunities to contribute to OSS that Yahoo Japan strategically uses and to create an environment that facilitates activities both inside and outside the company, as the number of employees who develop their own OSS has been increasing. Specifically, employees who contribute as committers to OSS that Yahoo has strategically adopted are certified as developers. In addition, Yahoo provides an environment in which employees can work as a committer in the community, by granting a certain amount of budget [129]for the development of the target OSS and related activities. The OSS developer certification program secretariat under the direct control of the CTO makes a comprehensive judgment of multiple parameters, including [the importance of the target OSS], [the community's evaluation of the developer as a committer], and [the developer's record of activities as a committer in the community]. As of October 2021, a total of 28 developers[130] had been certified.

In addition, Yahoo provides financial support to several communities, including The Linux Foundation and its subsidiary, the Cloud Native Computing Foundation (CNCF).

[129] A wide range of expenses are available, including the cost of purchasing development equipment, writing books, attending conferences, and travel and lodging.

[130] In some cases, certification is granted after building a track record in OSS communities that Yahoo strategically uses, while in other cases, certification is granted after hiring individuals who have already built up a track record in that community.

4.19. LaKeel, Inc.: Efficient development and management of OSS through a combination of OSS selection meetings and validation tools

■ Company information

Head Office	Minato-ku, Tokyo
Industry	Information and communication
Employees	Unconsolidated: 402 Consolidated: 474 (as of April 2021)
Commercial Flow	Internet service provider
Perspectives	[Organizational Structure] [Selection Evaluation] [Licensing] [Vulnerability Response]

■ Essence of this case

- The use of OSS is promoted company-wide, and when a new OSS is to be used, the leaders of the development department and the OSS management department meet to confirm the risks and discuss concerns before deciding whether or not to use it.
- To prevent oversights in OSS management and streamline the work of developers and OSS managers, verification tools (tools for software configuration analysis and license verification; the same applies hereafter) are introduced.

■ Background and issues

The OSS licenses are subject to change by the community, and unless one accurately understands the OSS one is using and collects the latest OSS license information, one may unknowingly be in violation of the license. LaKeel has introduced a verification tool as a solution to this problem and is working to improve the certainty and efficiency of OSS management.

■ Initiatives

<[Organizational Structure (O19)] Organizational structure for OSS management>

The Product Development Division, which uses OSS for its own services, is a department related to OSS. The Product Development Division has

approximately 100 employees. They engage in the development of products. Each product is under the charge of an administrator (who also serves as a manager). The division that develops tools for developers and product management functions (Platform Group) is also in charge of OSS management and manages and inventories the OSS used in all developed products.

<[Selection Evaluation (S19)] New OSS selection meeting>

Highly conscious of actively using OSS in its development, LaKeel aims to increase development efficiency by promoting the use of new OSS, rather than stopping developers from using new OSS, while protecting and securely managing licensing.

When selecting an OSS to use, LaKeel decides whether or not to use the OSS in a meeting of members of the Product Development Division, related parties, and Platform Group members who will use the OSS. When a plan to use OSS is raised, the leaders of the Product Development Division and the Platform Group jointly review the risks and discuss the concerns involved. At the meeting, participants share various types of information, such as licensing of OSS, market share, and the level of activity of the community, while specifically discussing and confirming measures to be taken if the development of the community comes to a halt. For example, they discuss how to respond when vulnerabilities are found in the OSS but not addressed. To date, there have been no cases in which any development for selected OSS communities has been halted. However, the company recognizes development stoppages as a risk and checks the level of community activity and other factors as important indicators in determining whether or not to use OSS, including contingency measures. Currently, the above operation is implemented as a rule. LaKeel is currently formulating a plan to create systematic guidelines for the use and selection of OSS and further improve efficiency through written rules.

<[Licensing (L19)] Efficiency through the introduction of verification tools>

A change in a certain license is the catalyst for raising awareness of OSS management. The change in the license meant that the source code had to be disclosed for commercial use. The OSS concerned was not affected as a result because LaKeel knew in advance the intended use of the OSS. On the other hand, as the use of OSS tends to increase in the future, there was a growing concern

that for other OSS as well, the license might change without LaKeel being aware of it leading to a violation of the license in the same way. In order to prevent such a situation from occurring, it was imperative to "reliably manage OSS" and "collect the latest information on OSS licensing.

Because the company was using a large amount of OSS, however, they felt that Excel-based management would result in oversights, resulting in a greater risk of license violations going unnoticed. Therefore, they decided to select and introduce a verification tool, from a perspective of minimizing oversights in the current management. In addition, the introduction of the verification tool made it possible to detect OSS that was being used recursively. For one product, the number of OSS's in use was assumed to be about 20 to 30, but the number of OSS's detected using the verification tool came out to be several hundred, including recursive ones.

In the past, the platform group was solely responsible for OSS management, while the management process became tighter each time a new OSS was adopted by the development department. However, by using a verification tool, the OSS detection process and information organization process have been automated, which has dramatically reduced the man-hours required. The OSS manager feels that their workload has been reduced to about 10% of what it used to be.

<[Vulnerability Response (V19)] Vulnerability response by DevSecOps[131]>

In product development, GitLab is used for source code management, and CI/CD[132] and verification tools are linked to automate the detection of OSS in use and the check for vulnerabilities in the detected OSS. By incorporating OSS detection and vulnerability checks into the development cycle, LaKeel is able to eliminate omissions in OSS management and vulnerability response, establish a DevSecOps system, and accelerate development speed.

[131] Incorporation of security measures into DevOps, where Development and Operations work together.

[132] Continuous Delivery / Continuous Deployment

4.20. SCSK Corporation: Open source software initiatives

- Company information

Head Office	Koto-ku, Tokyo
Industry	Information and communication
Employees	14,550（as of the end of March 2021）
Commercial Flow	System integrators commercial flow/system end user (IT service)
Perspectives	[Organizational Structure] [Personal Competence and Education] [Supply Chain Management] [Vulnerability Response] [Selection Evaluation]

- Essence of this case

  - The utilization of OSS is positioned as an important company-wide issue. The company has established a PMO that serves as a third-party risk check for development projects and has built an organizational structure by appointing an OSS management support staff in each business group. In addition, SCSK conducts e-learning and study sessions on OSS utilization.
  - To address the issues and risks associated with OSS utilization, SCSK has introduced a system to check unconscious and unintended use of OSS by recursively using OSS as software components, in addition to a system to select a safety-confirmed OSS before using it.

- Background and issues

  It is necessary to identify issues and risks associated with the utilization of OSS and to take necessary measures on a company-wide basis. In addition, when using OSS in software development, it is necessary to know whether the OSS to be used is safe and what kind of OSS it is. It is also necessary to establish a system and mechanism to continue these operations.

■ Initiatives

<[Organizational Structure (O20)] Organizational structure of OSS management>

A project management office (PMO) organization is in place as a unit for checking for development project risks from a third-party standpoint to ensure sound project management. The PMO organization consists of division PMOs in each business group and Corporate PMO that oversees and promotes the PMO policies.

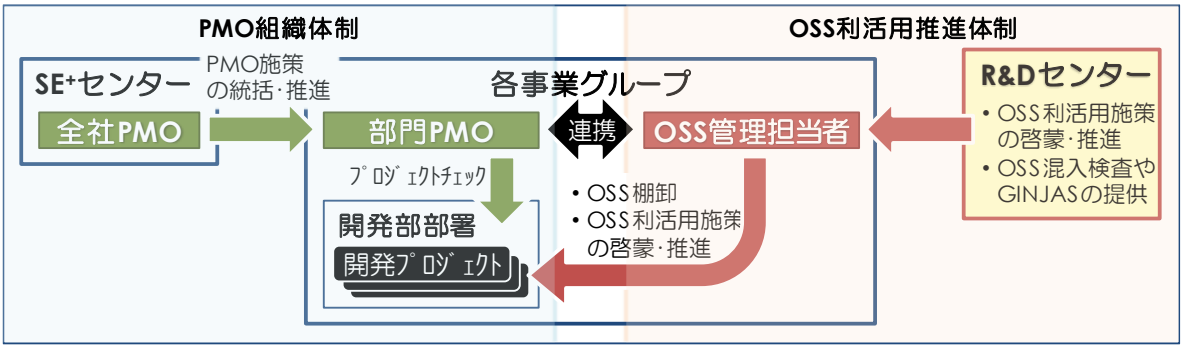


Figure 4.20-1 Relationship between the PMO organizations and OSS utilization promotion system (in Japanese)[133]

The PMO organization confirms that there are no risks are remained with the use of OSS from the planning stage of system development. Specifically, the PMO requires that OSS expected to be used in the system based on customer requests should be registered on the OSS selection and procurement support system (Ginjas), and that a list of OSS should be submitted to the PMO. In addition, the PMO requires that, when registering the OSS planned for use in the system with Ginjas, the project should confirm its terms and conditions of use listed in the licenses.

Each business group has an OSS management support staff to promote OSS management activities. Specifically, an inventory of OSS in use is conducted on a quarterly basis for the division in charge. At the timing of the inventory, the implementation status of the OSS commingling check should be confirmed (for the scheduled implementation period, whether it was completed as scheduled, and if not, the reason), while the use of Ginjas is made known to the employees.

Even engineers who develop systems may not know how to deal with the OSS they

[133] Excerpts from materials provided by SCSK.

are using (for example, how to deal with distribution using GPL License), so a dedicated support desk is in place to handle inquiries. The support desk is staffed by engineers familiar with OSS and its members who check licensing information at the R&D Center, which is the department in charge of the measures. The contact person is trained to acquire basic knowledge of OSS licensing through e-learning and OSS utilization guidelines, to deepen his/her understanding of OSS licensing through activities such as participating in study groups with other companies. The contact person receives inquiries about how to use licenses, whether certain OSS can be used to release the company's own products, and how to handle products developed jointly with customers.

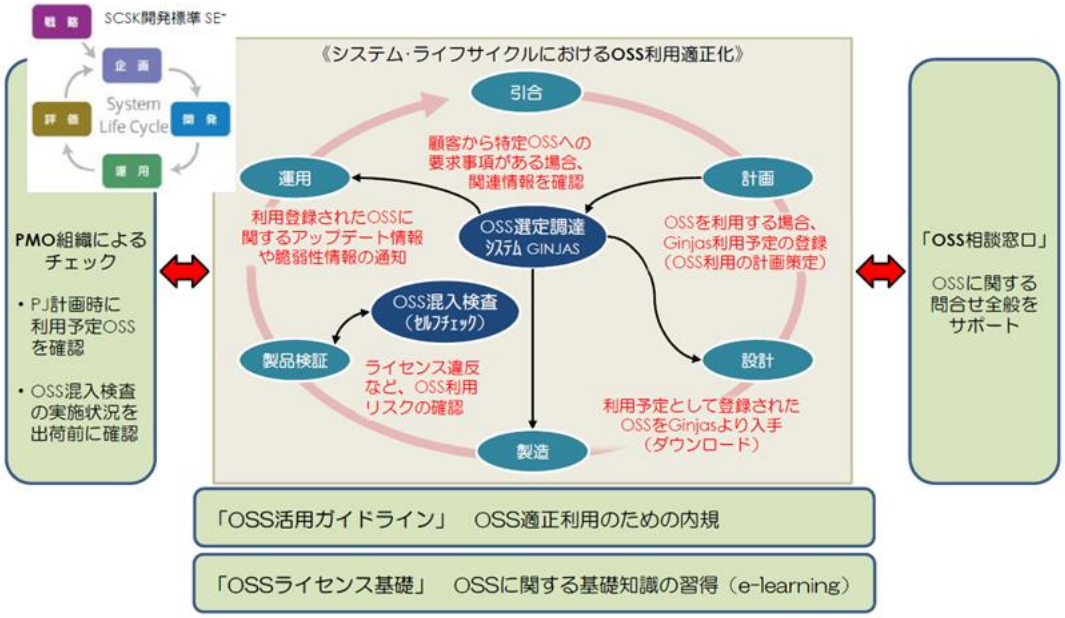


Figure 4.20-2 Overall view of the proper OSS utilization policy (in Japanese)[134]

<[Personal Competence and Education (P20)] Internal and external initiatives for OSS management policies and knowledge>

In addition to stipulating the proper use of software and licenses, including OSS, in the Company's [Information Security Guidelines], OSS utilization guidelines have been created for development units and disseminated to the entire SCSK Group at the field level.

Also, the e-learning program for in-house training includes explanations of OSS licensing, and all employees other than administrative staff take this training course.

[134] Excerpts from materials provided by SCSK.

The content of the e-learning is updated to incorporate the most important and the latest consultation details among the inquiries consulted at the support desk.

As part of OSS awareness-raising activities outside the company, a technical seminar called the OSS X Users Meeting [135] is held. These seminars are intended for OSS users and developers to share information on the latest OSS trends and how to use OSS.

<[Supply Chain Management (S20)] Initiatives aimed at contractors>

Contractors are briefed on SCSK's initiatives and mechanisms for OSS management. Orders to be placed to contractors are subject to the conditions that they are informed of and understand SCSK's OSS guidelines, acceptance inspection, and follow-up after the inspection.

The contents related to OSS in the e-learning program for internal use are shared with them. Furthermore, although a specific format has not been in place, contractors are asked to disclose the OSS they are using.

<[Vulnerability Response (V20-1)] OSS commingling check>

SCSK conducts OSS commingling checks during software verification in the development lifecycle. When software development is outsourced, all commingling checks are performed during acceptance inspection. Although a code scanning tool[136]is incorporated into the OSS commingling inspection system, the following problems were encountered in conducting self-checks in the individual development project.

First, a code scanning tool output candidate OSS that may be commingled. However, when the number of candidates is too large, the burden on the code checking tool of scanning and verifying the output results can exceed its processing capacity.

Second, the output reports contain so many items that it is difficult to identify OSS that require careful handling at the field level, resulting in a high workload.

To solve these problems, SCSK asked VeriServe, an SCSK group company, to wrap

[135] https://technomado.jp/tech/5417/

[136] There is a function of detecting OSS codes for codes to be inspected, by matching against the OSS information database.

the code scanning tools into a simple UI. Specifically, instead of using the operation screen of the scanning tool, which displays a variety of options, the company prepared a screen that allows users to start the inspection in three steps: project name, the e-mail address of the person conducting the scanning (for notification of scanning completion), and source code (ZIP file) registration, thus focusing on items necessary for scanning. In addition, currently, scanning results are reviewed in an Excel report rather than on the scanning tool screen. The Excel report consists of three sheets: a summary sheet of the scanning results, color-coded according to the OSS licensing terms of use; a list sheet with per-file licensing information; and a sheet for reporting the confirmed results (Confirmation Result Report).

In addition, the system was modified so that it can conduct a self-check and output reports in Excel. This system modification enables self-checking at the development site, with newly added functions: a function of giving notice after inspection, a function of automatically determining OSS having a high possibility of being included in the inspection target, and a function of presenting OSS having a high priority license to be handled. In OSS determination, the OSS having the highest match rate among the OSS candidates outputted by the scanning tool is selected. If there are multiple OSSs having the same match rate, the OSS with the strictest licensing conditions is selected from among them. The order of priority of correspondence is given according to the order of the strictest conditions of use. The copyleft type (GPL, AGPL, etc.) has the highest priority, followed by the semi-copyleft type (EPL, MPL, etc.) and the non-copyleft type (Apache, MIT, BSD, etc.).

Regarding the accuracy of the commingling inspection at SCSK, the company detects parts that are recursively used from OSS by inspecting all files included in the deliverables. With the belief that those tools have their limitations, the developers conduct final checks after scan by tools. Specifically, inspectors are required not to rely on the scanning result report, but to confirm the judgment result and submit a confirmation result report describing how to deal with OSS licensing. The final confirmation is made by submitting the confirmation result report to the department in charge of the measures (R&D Center).

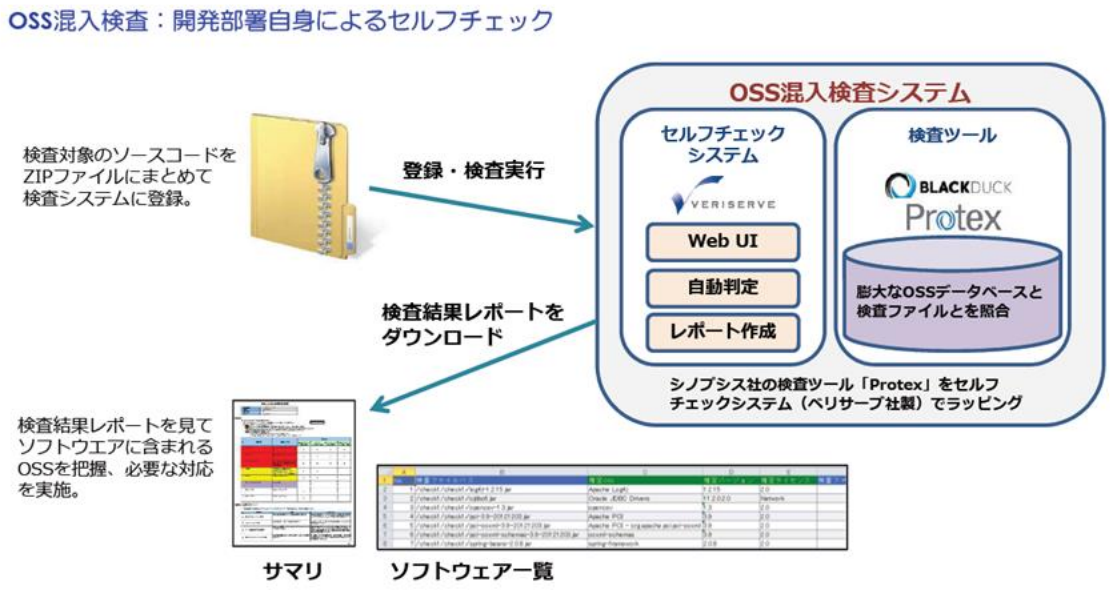


Figure 4.20-3 Image of OSS intermingling inspection system (in Japanese)[137]

Figure 4.20-4 Screen of the OSS intermingling inspection system (registration of files to be analyzed) (in Japanese)[138]

[137] Excerpts from materials provided by SCSK.

[138] Excerpts from materials provided by SCSK.

Figure 4.20-5 Screen of the OSS intermingling inspection system (Analysis result status) (in Japanese)[139]

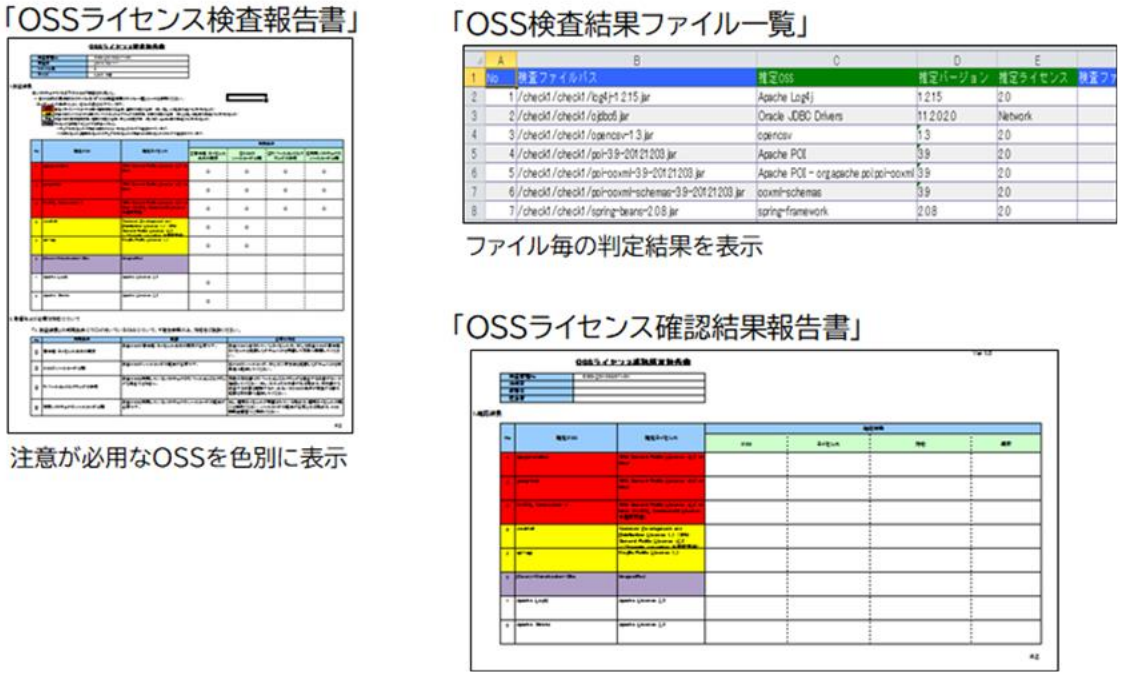


Figure 4.20-6 Screen of the OSS intermingling inspection system (Analysis result report) (in Japanese)[140]

[139] Excerpts from materials provided by SCSK.

[140] Excerpts from materials provided by SCSK.

<[Vulnerability Response (V20-2)] The OSS selection and procurement support system (Ginjas)>

SCSK has in place an OSS selection and procurement support system called Ginjas, which supports the safe use of OSS in each phase of system lifecycle, including planning, design, and operation. For OSS, the SBOM of the OSS and the OSS itself are registered on Ginjas. To use any OSS, engineers need to download OSS from Ginjas. SCSK educates them not to obtain or use any OSS from outside Ginjas.

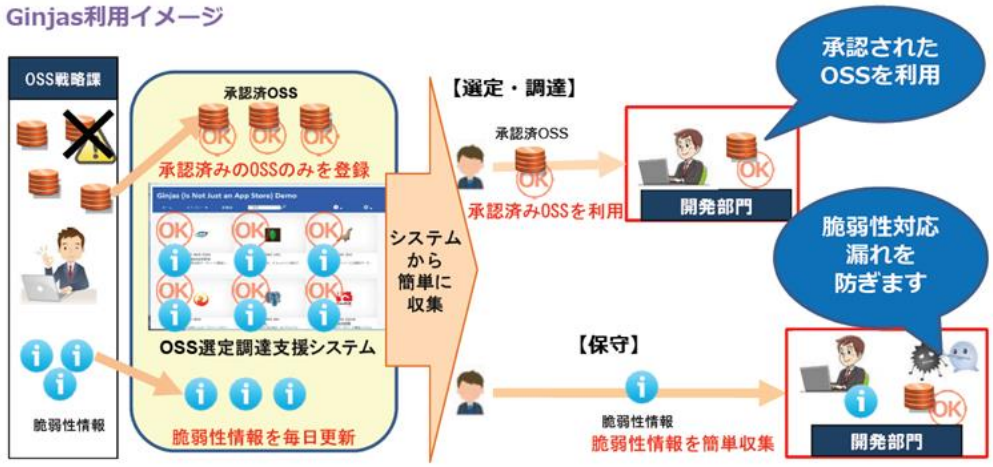


Figure 4.20-7 Image of Ginjas utilization (in Japanese)[141]

Ginjas automatically retrieves vulnerability information from IPA (Information-technology Promotion Agency, Japan) and other information sites, matches the vulnerabilities with the OSS of developed system, and outputs the evaluation results as a report. In order to retrieve this vulnerability information, Ginjas uses Vuls, a vulnerability detection tool, to check for vulnerabilities in the OSS. If there is any vulnerability problem reported in those information, Ginjas issues an alert.

[141] Excerpts from materials provided by SCSK.

Figure 4.20-8 Main screen of Ginjas (list of registered OSS and OSS download) (in Japanese)[142]

The OSS SBOM is registered in Ginjas in SCSK's proprietary format. Specifically, items such as OSS type, version, licensing, and source are managed (see Table 4.20-1). In order to manage items necessary to realize the purpose of Ginjas, SCSK manages those items in its own format, while only referring to formats standardized by SPDX Lite and others.

[142] Excerpts from materials provided by SCSK.

Table 4.20-1 OSS items managed on Ginjas (in Japanese)[143]

分類	項目	内容
基本情報	名称	OSSの名称
	画像	OSSのアイコン画像
	カテゴリ	ライブラリ、フレームワーク等の分類
	ジャンル	Web開発、データアクセス等、主な用途
	ライセンス	ライセンス種別
	プロジェクトURL	プロジェクト公式HPのURL
	リポジトリ	OSSを公開しているリポジトリ
	概要	OSSの説明
	開発元	OSSを開発している企業・団体の名称
	開発元URL	開発企業・団体の公式HPのURL
	組織タイプ	企業、専用基金、個人等の種別
バージョン情報 ひとつのOSSに複数登録	バージョン	バージョン番号、名称
	リリース日	当該バージョンのリリース日
	安定版	当該バージョンが安定版か（True/False）
	アクティブ	EOLになっておらず有効か（True/False）
	アップデート	アップデートが継続されているか（True/False）
	パッケージタイプ	Zip、tar.gz等のGinjasからのダウンロード形式
	URL	当該バージョンを公開しているURL
	プラットフォーム	Windows、Linux等の対応プラットフォーム
CPE情報	CPEベンダ	CPEベンダ名。脆弱性情報の検索用。
	CPE製品	CPE製品名。脆弱性情報の検索用。

<[Selection Evaluation (S20)] If one has a "yardstick" to easily find better OSS, one can avoid mistakes>

SCSK has developed the OSS Radar Scope® as a tool to avoid unnecessary mistakes and to utilize OSS efficiently, by providing a "yardstick" to easily find the best OSS even with limited information and knowledge. OSS Radar Scope® aims to collect general information on OSS published on the Web, such as maturity level, quality, and service overview, and present it in an easy-to-understand format by utilizing SCSK's knowledge.

[143] Excerpts from materials provided by SCSK.

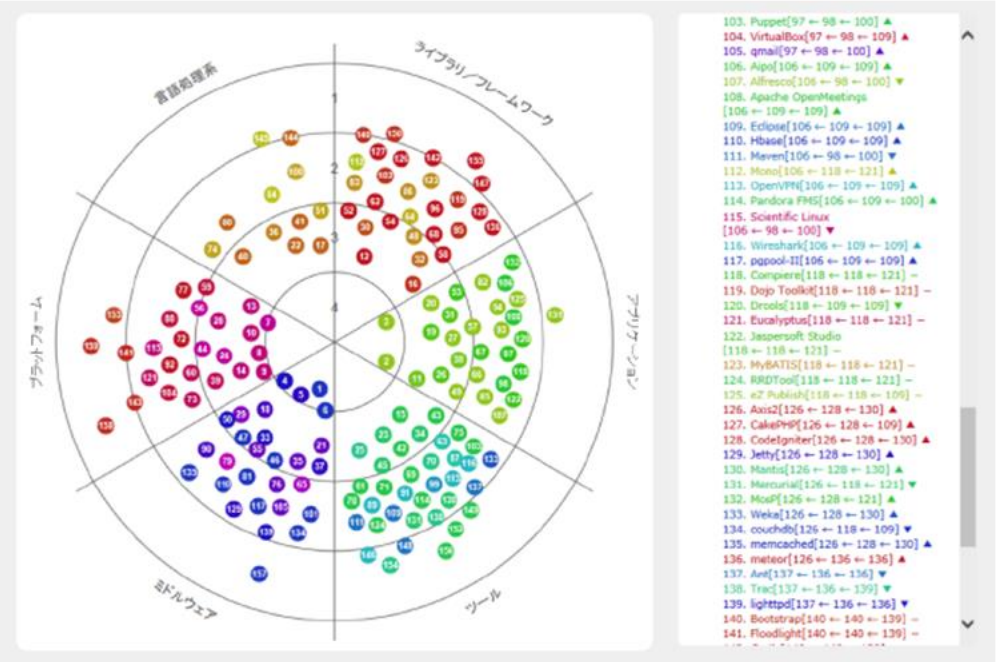


Figure 4.20-9 Structure of OSS Radar Scope® (in Japanese)[144]

OSS Radar Scope® collects objective data regarding five perspectives, updates the information monthly, and provides ratings based on the following two hypotheses:

Hypothesis 1) OSS that undergoes planned version upgrades are more likely to be good quality OSS.

Hypothesis 2) OSS with a large number of published books is likely to be good OSS.

Viewpoint 1) Release history

- OSS that undergoes planned version-up is considered likely to be good quality OSS, while OSS with an appropriate frequency of patch releases is considered likely to be good quality OSS.

Viewpoint 2) Documentation/Related publications

- OSS that focuses on the quality/quantity of documentation for users is considered likely to be good quality OSS, while OSS with a large number of published books is considered likely to be good quality OSS that is easy for users to use.

Viewpoint 3) Support information

- The quality of OSS is considered to be proportional to [the number of vendors

[144] Open Source Software Initiative: Development episodes and the behind-the-scenes of operation https://www.scsk.jp/product/oss/radarscope_1.html

providing services] × [the assortment of services provided].

Viewpoint 4）Status of community activities

- OSS with a lot of open communication among developers and feedback from users is considered likely to be good quality OSS.

Viewpoint 5）Project continuity

- OSS that has been around for a long time since its initial release is considered to be mature, stable, and reliable.

5. Use Case Examples (Literature Review)

5.1. Microsoft Corporation: Security risk mitigation measures for OSS

■ Company information

Head Office	The United States
Industry	Information and communication
Employees	163,000 (as of August 2020)
Commercial Flow	System integrators commercial flow/Service provider
Perspectives	[Vulnerability Response]

■ Initiatives

<[Vulnerability Response (V21)] Security risk mitigation measures for using OSS>

Microsoft has implemented the following four security risk mitigation measures when using OSS[145].

(1) Identification What OSS is Used.

(2) Centrally Catalog Identified OSS.

(3) Ensure the OSS is Secure.

(4) Respond to Security Vulnerabilities.

Those initiatives are detailed below:

(1) Identification What OSS is Used.

The software is scanned for source code using a tool called "discover" to detect the OSS used and generate a report (Bill of Materials (BOM)). This process is

[145] Who Wants a Thousand Free Puppies?
https://download.microsoft.com/download/C/5/E/C5E50D16-6E0B-453A-9A69-195CF3D2C823/LocoMocoSec-2019%20-%20Who%20Wants%20a%20Thousand%20Free%20Puppies%20-%20Michael%20Scovetta%20-%20Microsoft.pdf

highly automated to reduce the effort of software developers.

(2) Centrally Catalog Identified OSS.

The OSS usage status confirmed in (1) above is centrally managed in a database, etc., so that it can be referred to at any time. This makes the OSS usage status of each organization visible and help improve response time and reduce costs when OSS vulnerabilities are found (Figure 5.1-1).

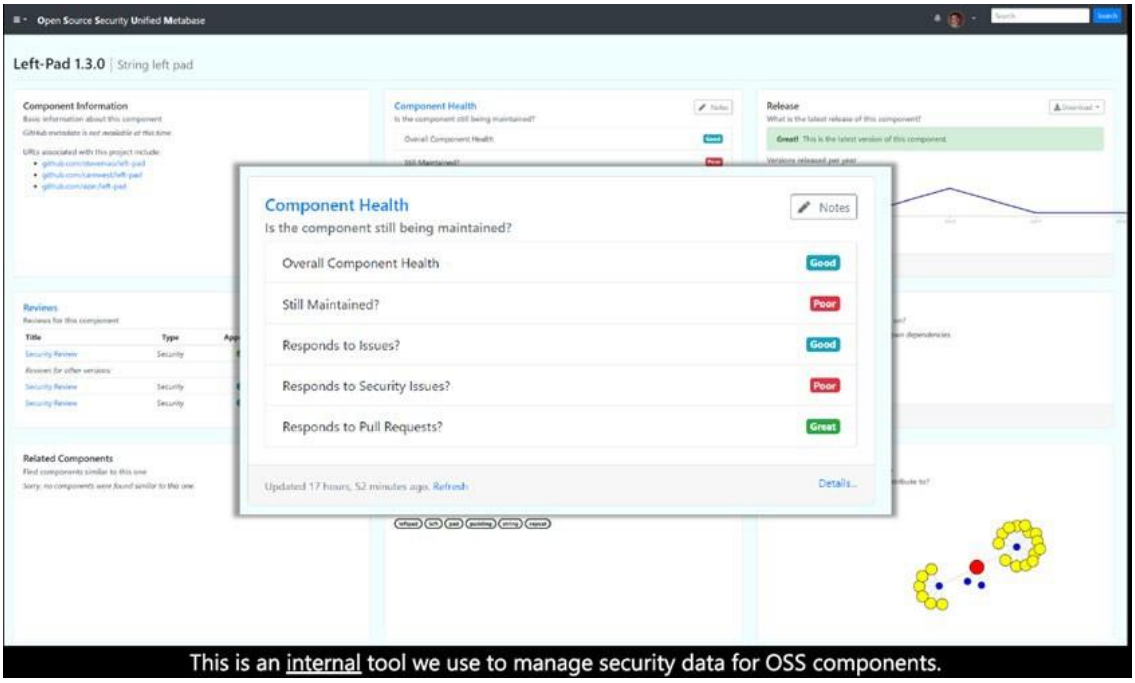


Figure 5.1-1: In-house tool for managing OSS component-related data[122]

(The maintenance status of OSS components is displayed on the screen, and by referring to it, it is possible to identify the potential risks of OSS.)

(3) Ensure the OSS is Secure.

The recognized OSS will be verified for its safety according to the risk tolerance for each unit in the company. All OSS components are verified for vulnerabilities through the collection of public information, commercial database information, and the use of tools. If a higher level of security is required, in addition to the use of the aforementioned tools, security reviews (In-Depth Security Reviews) are conducted to ensure that the OSS components are secure (Figure 5.1-2). This review is conducted by the review team assisted by the team of engineers. It provides a high level of security assurance, albeit at a cost.

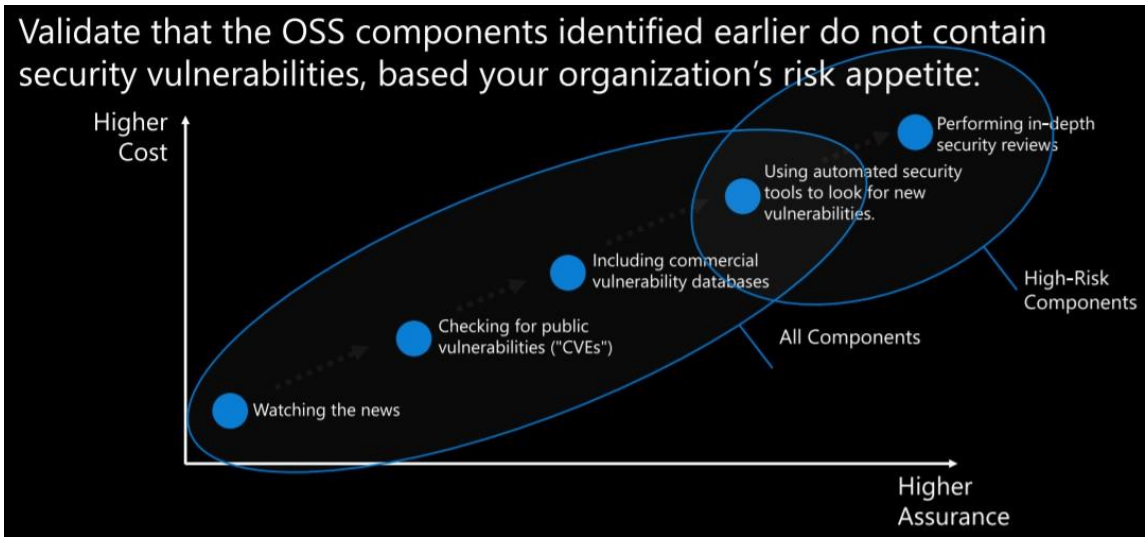


Figure 5.1-2: Securing OSS according to the balance between required security level and cost[122]

The company also uses various other means, such as security assessments and statistical analysis, to keep abreast of vulnerability information, which is updated internally to provide a list of safe OSS programs.

(4) Respond to Security Vulnerabilities.

At Microsoft, the Microsoft Security Response Center, which runs an organizational security program, provides integrated security vulnerability response for OSS. Notable efforts of the Microsoft Security Response Center include the creation of an ecosystem for the discovery of new vulnerabilities through the Microsoft bug reward program and the disclosure of information on discovered vulnerabilities and their countermeasures.

5.2. Zalando SE: Company-wide promotion of the OSS project

■ Company information

Head Office	Germany
Industry	Information and communication (operation of mail-order sites for fashion products, etc.)
Employees	13,825 (as of May 2020)
Commercial Flow	System integrators commercial flow / End user (IT Service)
Perspectives	[Licensing]

■ Initiatives

<[Licensing (L22)] Company-wide promotion of the OSS project>

In order to promote OSS projects, comply with licenses, and contribute to the community, Zalando has established the following three principles related to OSS[146].

- Participate:
  Encourage employees to contribute to OSS projects.
- Share:
  Share codes and processes so that technology can be used to help more people.
- Promote:
  Encourage the engineering team use of open source codes and disseminate practices related to open sources.

In addition, Zalando's open source team conducts cross-departmental activities to encourage the use and development of OSS and to share best practices. Specifically, the following documents related to OSS have been created, deployed, and published both internally and externally[147].

- Open Source Licensing Guide[148]
- Adopting open source code
- Releasing an open source project

[146] Zalando homepage. https://opensource.zalando.com/

[147] Zalando homepage. Documentation https://opensource.zalando.com/docs

[148] Zalando Homepage Licensing: https://opensource.zalando.com/docs/resources/licensing/

- State of open source at Zalando 2018 Report)
- Anti-Harassment Policy.

Of these, (1) "Open Source License Guide " and (2) "Releasing an open source project", which are guidelines related to OSS utilization and development, are outlined below:

(1) Open Source Licensing Guide

The guide explains the licenses that may be used and the licenses that should not be used. Specifically, Zalando permits the use of OSS that falls under the following three types of licenses:

- Permissive licenses:
  A license that allows use, modification, and distribution if accompanied by the copyright and license information, including AFL, Apache, BSD, MIT, MS-PL, ISC, and PHP License.
- Weak copyleft licenses:
  A license that allows use, modification, and distribution if accompanied by the copyright, license, change record, source code, and installation information, including APSL, CDDL, CPL, EPL, IPL, and MPL.
- Strong copyleft licenses:
  A license that allows use, modification, and distribution if accompanied by on the copyright, license, change record, source code, installation information, including BCL, GPL, LGPL, NPL, OSL, and QPL. At Zalando, such licenses are available for internal use only.

On the other hand, Zalando does not allow the use of codes licensed under AGPL or variants thereof, commons clause licensed codes, or unlicensed codes.

(2) Releasing an open source project[149]

Zalando employees may release new open source projects through Zalando-Incubator[150]. The following items are defined as a rule to be followed to

[149] Zalando Homepage: Releasing a new open source project
https://opensource.zalando.com/docs/releasing/index/

[150] Zalando-Incubator is Zalando's GitHub community for helping to launch new open source projects. When a Zalando employee releases a new open source project, a pilot open source project will be launched on Zalando-Incubator, and the project will be reviewed and assessed for sustainability. The

implement a project.

- Coordination of existing operations (Get sign off)
  Employees who start a project need to get approval from their team leader and members to devote work time to the new open source project.
- Compliance (Be Compliant)
  All open source projects must release their code according to the Zalando Rulebook (Rules of Play) and best practices. Specifically, they are required to create the necessary files related to the license, etc., and to set the effective version name of the deliverables.
  Prepare a repository for release by improving the maintainability and readability of the code and by preparing the necessary documentation. Also, checks are made from several perspectives, such as whether the code complies with the aforementioned rules, etc., whether it can run in environments outside of Zalando, and whether there is any confidential information contained in the code.
- Conducting reviews (Get Reviewed)
  When the code is ready for release, it has to be reviewed by the Open Source Review Group. If it passes the review, it will be released via Zalando-Incubator.

Open Source Review Group is responsible for evaluating Zalando-Incubator projects, and if the project meets a certain level of activity and community participation, they will graduate from Zalando-Incubator and be promoted as an open source project in Zalando's main GitHub community. If the project meets a certain level of activity and community participation, it will graduate from Zalando-Incubator and be promoted as an open source project in the main GitHub community. The system is as follows: https://opensource.zalando.com/docs/releasing/incubation/ https://opensource.zalando.com/docs/releasing/graduation/

5.3. Preliminary Report on the Census II Project by the Linux Foundation and Harvard University: A survey on the FOSS components most widely used in applications[151]

- Position in this case study
  Other (Service results)
  Perspectives: "Vulnerability Response"

- Essence of this case
  - Throughout the Census II project, widely used FOSS components have been identified, particularly with respect to Free and Open Source Software (FOSS), which makes up the majority of modern software.
  - More than three quarters of the top contributors to FOSS were found to be employees of businesses.
  - In the course of the study, the following challenges were identified: lack of standardized naming conventions for software components, increasing importance of security for individual development accounts, and persistence of legacy software in OSS.

- Background of Census II

It is estimated that 80-90% of modern software is made up of FOSS components. However, it is unclear what kind of FOSS is most widely used, since there is no organization that guarantees the quality and maintenance of FOSS, and it can be freely copied and modified.

The report emphasizes that, in order to ensure the future health and security of the FOSS ecosystem, it is critical to know what sort of FOSS is being used in the private and public sectors and the extent to which they are maintained and supported. Based on this understanding, the Census II project was launched jointly by the Linux Foundation's Core Infrastructure Initiative (CII)[152] and the Harvard Institute for Innovation Science.

---

[151] Vulnerabilities in the Core Preliminary Report and Census II of Open SourceSoftware https://www.coreinfrastructure.org/wp-content/uploads/sites/6/2020/02/census_ii_vulnerabilities_in_the_core.pdf

[152] An organization established by the Linux Foundation in 2014 in response to the Heartbleed issue (OpenSSL vulnerability).

■ Report summary ([Vulnerability Response (V23)])

As a preliminary report for the Census II project, the "Vulnerabilities in the Core Preliminary Report and Census II of Open Source Software" was published in February 2020. A summary of the report is provided below:

<Purpose of the survey>

(1) To identify the most commonly used FOSS components in product applications.

(2) To investigate those FOSS components for potential vulnerabilities caused by

- Extensive use of older versions.
- Project understaffing.
- Known security vulnerabilities.

(3) To use the information gained to prioritize investments to support the health and safety of FOSS.

<Study results>

Dependency analysis was performed on datasets provided by partner software configuration analysis companies and application security companies to identify the most widely used FOSS components. In the report, the ten most frequently used packages are listed in alphabetical order in the appendix (Table 5.3-1). The JavaScript package was by far the most commonly used. Table 5.3-1 also shows the top packages when the JavaScript package is excluded. Further in-depth research is needed to determine if so-called "legacy software" that is deprecated or has not been updated in several years is still in use today. Also, since the dataset used for this study was limited in both quantity and quality, the findings of this preliminary report do not make any claims as to which FOSS packages are the most important.

Table 5.3-1: FOSS packages used most widely

JavaScript package	Another package than JavaScript
async	com.fasterxml.jackson.core:jackson-core
inherits	com.fasterxml.jackson.core:jackson-databind
isarray	com.google.guava:guava
kind-of	commons-codec
lodash	commons-io

JavaScript package	Another package than JavaScript
minimist	httpcomponents-client
natives	httpcomponents-core
qs	logback-core
readable-stream	org.apache.commons:commons-lang3
string_decoder	slf4j:slf4j

In addition, 75% of FOSS developers were employed by a company and 15% were sole proprietors (the remaining 10% were unknown). This indicates a high percentage of employees of companies. An analysis of the 2017 GitHub data shows that among the most active FOSS developers are many employees of Microsoft, Google, IBM, and Intel. Even though the contributors to the projects listed in the appendix were not paid directly bey their employers for developing these packages, it is noted that their status as members of the FOSS community may have substantiated their eligibility for employment. However, the analysis adds that it is not possible to draw conclusions about this fact without further clarification of the context in which the contributors operate and without direct data to support these hypotheses.

<Issues identified by the survey>

During the early stages of the Census II project, the following issues were identified, separately from the initiatives of this project. While the report states that these issues do not affect the outcome of the study, they are important and deserve more extensive discussion.

(1) Lack of a standardized naming convention for software components

As efforts to address the transparency and security of the software supply chain evolve and become more complex, as evidenced by the NIST[153] and NTIA projects, the lack of naming conventions will be a challenge for industry and governments to protect themselves from software-based incidents.

(2) Increasing importance of security for personal development accounts

Of the top ten most used software packages, seven were developed in individual developer accounts. It is clear that many programs exist in personal development

[153] National Institute of Standards and Technology.

accounts. Individual development accounts may be more vulnerable than corporate accounts. This points to the fact that changes to the code under the control of a personal development account can be made fairly easily and undetected. This has happened in practice. The case of Copay[154], where a malicious person was delegated a legitimate administrative privilege to plant a backdoor, is not strictly a hijacking. However, it has been pointed out that personal development accounts are also at risk of intrusion and hijacking. Also, in a Left-pad[155] case, a developer removed the code from the repository because of a package naming dispute. This caused many packages that depended on the code to stop functioning, even though the code appeared to be trivial at first glance. This is one of those cases where the developer's own actions had a significant impact.

(3) Persistence of legacy software in OSS

There are cases where the usage rate of old packages is higher than that of newer ones, even though the newer packages essentially have the same functionality. The reason for this may be that it is difficult to switch to new software due to concerns over compatibility bugs and the time and cost constraints of retrofitting. Since the number of developers of old packages decreases with time, it has been pointed out that the legacy problem of FOSS needs to be recognized.

[154] Mobile wallet application released by BitPay Inc.

[155] A library written in JavaScript having the ability to adjust strings.

6. Summary

In this Collection, we have introduced 20 cases of domestic companies collected through interviews and three cases of overseas companies collected through a survey of published literature. This chapter summarizes the key points of the initiatives taken in each case for each of the perspectives summarized in Chapter 3.2.2.

■ Selection Evaluation

In OSS Selection and evaluation, clarification of selection criteria was considered important. For example, some companies have established a list of available or unavailable OSS's and have made it a rule to comply with the list when selecting OSS within the company or the group, while others have established a system to support selection and procurement. Some other companies set policies on OSS use and created rules for selecting OSS in accordance with the policies. In addition, there was an effort to establish a standard for easily identifying better OSS, collecting information based on the standard, and make it available to the public.

To ensure that these lists and policies are always the most appropriate standards for OSS use, regular reviews and maintenance by members with expert knowledge were seen. In determining whether or not to use each OSS and in setting policies, companies took into account the perspectives of "licensing," "maintenance and quality assurance," etc., as described below, in addition to such factors as the actual use of the relevant OSS within the company or group and the status of community activities.

■ Licensing

License compliance is often regarded as the most important factor, especially in commercial product distribution. Many companies cited license compliance as a trigger for starting OSS management initiatives. In many cases, license compliance is examined from the perspective of whether the entire organization understands the content of the OSS license and can comply with the corresponding requirements when using OSS. At the same time, efforts are made to ensure reliable license compliance, including the systemization of a series of workflows, the confirmation of the existence of unrecognized OSS using tools, and rules for approval at specific development stages. In some cases, information on the OSS used is accumulated in the workflow system and utilized in the "vulnerability response" described below.

Legal knowledge is essential in dealing with licensing. In some cases, the legal department reviews the workflow or advises the business unit as needed.

In addition, some companies are working on early verification and labor savings by better managing software dependencies and by automating verification tools, while utilizing functions provided in OSS, such as a build system, as license management and configuration management.

■ Vulnerability Response

Many companies used SBOM for vulnerability response, which is created by using the OSS information obtained through the aforementioned license compliance or by using tools. In some cases, the collected OSS vulnerability information is cross-verified with the SBOM to understand the impact, and then the department in charge of the product or service that uses the OSS takes appropriate actions as necessary. Some companies collect OSS vulnerability information from general information sources (news sites, blogs, etc.) in addition to information from JVN, etc., and respond more quickly based on the information. Several companies have set up a PSIRT or the like that plays a central role in handling vulnerabilities, which smoothly coordinate with each department to deal with vulnerabilities.

On the other hand, there are differences in OSS names and information granularity between the information managed by an SBOM and the collected vulnerability information, which makes it difficult to properly collate the information. Some companies are seeking solutions using advanced technologies such as AI.

■ Maintenance and Quality Assurance

In terms of maintenance and quality assurance, some companies also appropriately manage the timing of EOL as part of their OSS management scheme, including SBOM. They also procure OSS through distributors who also provide maintenance services or have rules in place for the use of OSS by in-house personnel as a work-around. For OSS used in social infrastructure systems, discussions are being held on how to achieve long-term maintenance due to the characteristics of the field. In the telecommunications business, system integrators agree in advance with their customers on the risks involved in using OSS over the long term, including, in particular, costs related to vulnerability management and update response.

■ Supply Chain Management

In supply chain management, several companies have made it obligatory to declare OSS in use in an arrangement or contract with suppliers and contractors in order to identify OSS used by companies in the supply chain. When concluding such arrangement and contract, they made steady efforts such as carefully explaining the

necessity of knowing the status of OSS use in the supply chain in order to obtain the understanding from suppliers and contractors.

In addition, notable activities include the acquisition of OpenChain self-certification and the sharing and dissemination of information through OpenChain. Many companies are working to foster a common understanding of the importance of license compliance. These cross-company efforts are contributing to OSS literacy improvement in the entire supply chain.

■ Personal Competence and Education

Some companies prepare educational menus to improve employees' literacy toward OSS. Specifically, a variety of educational menus are prepared for enlightenment on OSS utilization, how to proceed with development using OSS, and license compliance. In order to have employees acquire a high level of literacy, there is also an ingenious way to conduct examinations with a certain score as a target. In addition, some companies have prepared English teaching materials to ensure that their overseas offices have the same level of literacy as domestic employees.

Furthermore, there were several companies whose OSS initiatives were accelerated because key management personnel showed understanding. From this, it can be inferred that in order to promote OSS utilization, it is important not only to improve literacy at the field level but also to gain understanding through enlightenment of and information sharing with the management layer.

■ Organizational Structure

In terms of OSS management, some companies have an organization dedicated to OSS, while others have a cross-divisional, community-like organization with representatives from each division[156]. In some companies, leaders of the development and OSS management departments review risks and discuss concerns with each other in order to make efficient decisions on whether or not to use certain OSS. In addition, in some other companies, employees in the department responsible for security support also support OSS, as often seen in cases where their OSS initiative were still in the development stage.

[156] It is considered that there are "professional organization type" and "committee type", which are the forms of security control functions organized in the " Guidebook for Establishing Cybersecurity Organization and Securing Necessary Human Resources" compiled by the Ministry of Economy, Trade and Industry. (in Japanese)
https://www.meti.go.jp/press/2020/09/20200930004/20200930004-1.pdf

In addition to a thorough understanding of OSS itself and the company's products and services that utilize OSS, OSS management requires broad knowledge that covers multiple departments such as security, legal affairs, procurement, and quality control. Further, since the appropriate system differs depending on the business environment of the product/service, each company has been trying to build a system that appropriately cooperates with each department within the company or group, taking into account the business environment of each product/service.

■ Community Activities

In the utilization of OSS, there are companies that recognize the importance of active participation in community activities. Such companies encourage employees to participate in community activities as part of their business and establish guidelines for such community participation. If there are no problems with the use of OSS, some companies allow employees to give back to the community as individuals. The reason for this is that, in the case of OSS, the performance and quality of OSS improve as community activities become more active, and that employees' participation in and contribution to community activities lead to benefits for the companies using the OSS. In addition, there are companies that strategically utilize the OSS ecosystem, including those that prepare training menus on how to proceed with community-based development so that employees can achieve maximum results in community activities and those that convert self-developed software to OSS and improve performance through community-based development.