経済産業省

国家サイバー統括室
National Cybersecurity Office

Guidelines on the Roles Expected of Cyber Infrastructure Providers (draft)

—Appropriate division of roles and responsibilities between customers and cyber infrastructure providers to ensure cybersecurity and improve resilience in software development, supply, and operation—

Summary

Oct. 2025

Study Group on the Roles Required of Cyber Infrastructure Providers - Summary

- To **strengthen cybersecurity measures in software supply chains**, a working group consisting of experts from industry and academia, jointly hosted*1 by the Critical Infrastructure Expert Examination Committee and the Ministry of Economy, Trade and Industry's Industrial Cybersecurity Study Group, was created in September 2024. The **roles expected of cyber infrastructure providers** were considered, with the aim of protecting customers who use software.
- These were compiled as the Guidelines (draft) in FY2024, and in fiscal year 2025, the Guidelines will be finalized. In addition, measures to promote utilization will be considered, such as expanding checklists as annex documents and examining dissemination strategies, including referencing the Guidelines in government agency and critical infrastructure procurement.

Background and Challenges

*1: Following its abolition in July 2025, National center of Incident readiness and Strategy for Cybersecurity (NISC) was repositioned as a cross-sectoral sub-working group in Working Group 1 of the Industrial Cybersecurity Study Group and as the joint working group of National Cybersecurity Office (NCO).

・Threats of cyberattacks exploiting software vulnerabilities are increasing in number

⇒ Necessity for cyber infrastructure providers **who develop, supply, and operate software to take greater responsibility for providing responses**

⇒ NCO co-signs an international document on **secure by design/default**

・However, **no domestic guidelines exist** in which the roles expected of cyber infrastructure providers are arranged

Image of the Guidelines (draft) under consideration

・Determine responsibilities expected of cyber infrastructure providers and customers, and requirements for fulfilling the responsibilities (specific measures)*2

Cyber infrastructure provider

◯**Software***3
- **Developer**
- **Supplier**
- **Operator**

Customer

◯ Customer (including government agencies and critical infrastructure operators)

(1) Design, development, supply, and operation of software with security quality ensured

(2) Software supply chain management

(3) Prompt response to remaining vulnerabilities

(4) Arrangement of governance for software

(5) Strengthening information sharing and collaborative relationship between cyber infrastructure providers and stakeholders

(6) Risk management and software procurement/operation by the leadership of the customer management

*2: Refer to relevant guidelines in other countries.

*3: In addition to software provided to customers as a product, this also includes software services such as cloud services, embedded software and firmware provided as part of hardware products such as IT/OT/IoT devices, and software provided as components of systems or services.

Cyber infrastructure providers and stakeholders (1)

- The Guidelines (draft), assuming "cyber infrastructure providers" involved in the development, supply, and operation of software as intended targets, provide a categorization of three main roles: developer, supplier, and operator.
- To improve the software cybersecurity resilience, cyber infrastructure providers are required to strengthen relationships in various aspects, not only in terms of involvement aimed at protection against incidents but also as collaborators in information collection, analysis, and response coordination in pre- and post-incident responses.

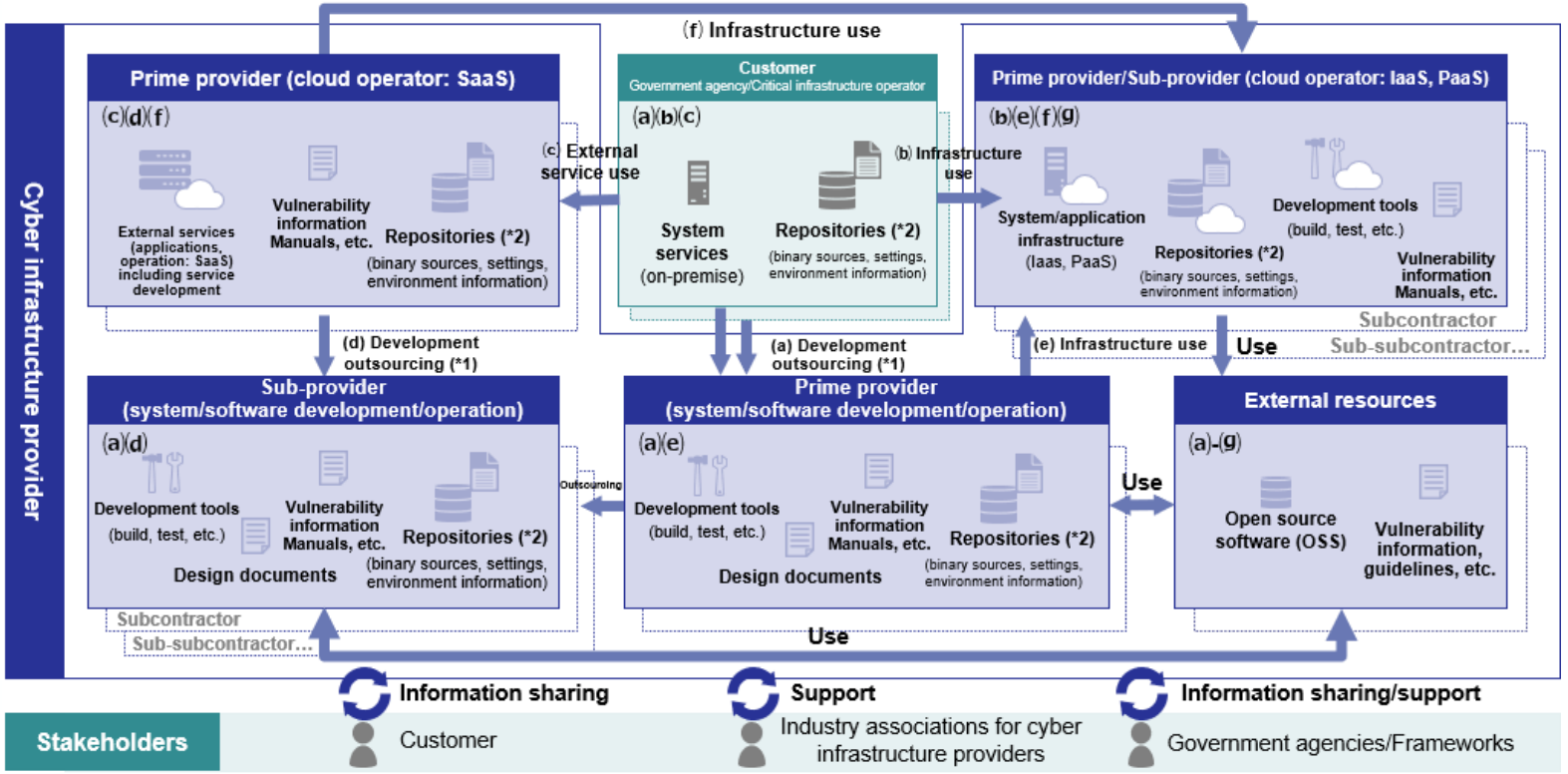
Classification	Name	Description
Cyber infrastructure provider	Developer	Business or personnel engaged in designing, development, or integration of software products, software services, embedded software, and/or systems and services that are composed of such software. Developers are entities that develop or integrate software for a software development vendor, software service provider, device development vendor, software and system development contractor, software component developer, infrastructure operator, development department for in-house developed software, etc.
	Supplier [1]	Business or personnel that provides customers with software products, software services, embedded software (including hardware products), or systems and services that are composed of such software. Suppliers are entities that provide software or systems/services to a sales company of software products and devices; they include software/software service providers, system development and operation contractors, infrastructure operators, and software development vendors.
	Operator	Business or personnel that performs tasks to support the operation of systems and services for customers.
Stakeholder	Customer	Businesses who are the main entities of software utilization, like government agencies, critical infrastructure operators.
	Other related organization [2]	Organizations responsible for supporting the improvement of cyber resilience.

[1] In some cases, developers and operators are also suppliers. In addition, in cases in which a sales company is also a cyber infrastructure provider, responsibilities equivalent to those of the supplier are required of them.

[2] Although it is usual that customers, who are the main entity of software utilization, operate software, specialized knowledge and skills are often required to operate systems and services or the software that composes them. In this context, it is assumed that cyber infrastructure providers support the operation of software (or part thereof) in accordance with contracts with customers.

Cyber infrastructure providers and stakeholders (2)

- Figure below illustrates the relationships between the development, contract form, and usage form of software systems/assets handled by cyber infrastructure providers for which the Guidelines (draft) are intended.
- Two roles described below are assumed for cyber infrastructure providers from the perspective of system development, contract, and usage:
  Prime provider: First-tier contractor that contracts directly with customers and develops, supplies, and operates systems and cloud services.
  Sub-provider: Business that contracts with the prime provider and develops, supplies, and operates systems and cloud services.



*1 There are cases where subcontractors are not used in (a) and (d). There are also cases where a customer conducts development for itself as a cyber infrastructure provider.

*2 The ownership of software varies depending on the service and system development, form of contract, etc., but there is no mention about the ownership.

[Examples of forms of system development, operation, and use]
(a): On-premise system (development outsourcing to prime provider)
(b): Customer uses IaaS, PaaS
(c): Use of system using SaaS
(d): Cloud provider (SaaS) outsources development
(e): Prime provider (SIer, etc.) uses IaaS, PaaS
(f): Cloud provider (SaaS) uses IaaS, etc.
(g): Cloud providers (IaaS, PaaS) have interoperation

Guidelines on the Roles Expected of Cyber Infrastructure Providers (draft) - General summary

To improve cybersecurity resilience in software supply chains, the responsibilities required of cyber infrastructure providers and customers (items similar to basic principles) and requirements for fulfilling the responsibilities are arranged into six categories. Going forward, efforts will be made to expand checklists as annex documents to promote the utilization of the Guidelines.

Background of the Guidelines (draft)

- Threats of cyberattacks exploiting software vulnerabilities and vulnerabilities lurking in supply chains are increasing in number.
- Institutional arrangements related to strengthening of cybersecurity measures in digital products and services, such as secure by design/default, co-signed by NISC (current NCO) and others, are being accelerated.

Purpose of the Guidelines (draft)

- The purpose is to represent an approach that can provide a reference for operators and people concerned to ensure the effectiveness of cybersecurity measures, while responses by "cyber infrastructure providers," who provide cyber infrastructure by using software in line with efforts in other countries are to be arranged.

Examples of future initiatives

- Measures to promote the utilization of the Guidelines, such as expanding checklists as annex documents and conducting public relations activities, are under consideration.

Outline of the Guidelines (draft)

Six responsibilities Basic principles to be recognized to improve resilience related to cybersecurity	Six requirements Cybersecurity measures to be implemented jointly for the purpose of resilience improvement related to cybersecurity	Intended organizations
Design, development, supply, and operation of software with security quality ensured	Secure design, development, supply, and operation	Cyber infrastructure provider (software development vendor, software distributor, software operation vendor, etc.)
Software supply chain management	Life cycle management and assurance of transparency*	
Prompt response to remaining vulnerabilities	Prompt response to remaining vulnerabilities	
Arrangement of governance for software	Arrangement of human resources, processes, and technologies	
Strengthening of information sharing and collaborative relationship between cyber infrastructure providers and stakeholders	Strengthening of relationships between cyber infrastructure providers and stakeholders	
Risk management and software procurement/operation by the leadership of the customer's management	Risk management and secure software procurement/operation by customers	Customer

* For SBOM-related contents on "Life cycle management and assurance of transparency," it is possible to use the "Guidance on Introduction of Software Bill of Materials (SBOM) for Software Management, ver. 2.0" by the Ministry of Economy, Trade and Industry as a reference.

Responsibilities of cyber infrastructure providers (1)

- To improve cybersecurity-related resilience, complementary effects can be obtained when cyber infrastructure providers and customers fulfill their respective responsibilities.
- Cyber infrastructure providers must be aware of the following five responsibilities to improve cybersecurity resilience. All of these responsibilities must be recognized by the management of each cyber infrastructure provider, and efforts to fulfill these responsibilities must be implemented under the leadership of the management.

1. Design, development, supply, and operation of software with security quality ensured

- **Provision of secure software and evaluating measures**
  - In accordance with the principles of "secure by design" and "secure by default," take measures to reduce threats to software development and operation using a risk-based approach, and determine their effectiveness.
  - Enforce minimum security standards for the software.
- **Consideration of cybersecurity throughout the entire software life cycle**
  - Starting with an agreement on security requirements, consider cybersecurity throughout the software life cycle agreed upon with the customer, including secure build, testing, and operation.

Responsibilities of cyber infrastructure providers (2)

2. Software supply chain management

- **Sharing of implementation status of security control measures**
  - To allow users to make decisions regarding software procurement and implementation—including the selection of risk-based solutions—suppliers should disclose the status of their software development efforts. Ensure transparency with customers regarding all necessary aspects of cybersecurity.
- **Sharing of software configuration information**
  - For measures against vulnerabilities by users, use information from software configuration management, including the software bill of materials (SBOM), and configuration information, including OSS.
- **Promotion of risk management including supply chains**
  - Include suppliers (such as system integrators, external system service providers, and partners), developers, and all other businesses related to IT/OT/ICT systems in the scope of software supply chain risk management activities.

3. Prompt response to remaining vulnerabilities

- **Communication and response to vulnerabilities and threat information**
  - Arrange vulnerability disclosure policies appropriately and establish a vulnerability response system.
  - Vendors are responsible for identifying and disclosing vulnerabilities in cloud service software, providing the information necessary for secure service configuration and operation, upgrading services, developing and distributing patches, and documenting upgrade/patch application processes so that customers understand how to participate in the processes.
  - Maintain a mechanism for sending notifications to customers.

Responsibilities of cyber infrastructure providers (3)

4. Arrangement of governance for software

- **Integration of software supply chain risk management into enterprise risk management**
  - Software supply chain risk management covers activities throughout the software life cycle and is as part of the enterprise risk management process.
  - Arrange the resources necessary to reduce risk to an acceptable level (people, materials, and money) in your organization. Position cybersecurity as a key management issue, and the top management must be made responsible for implementing risk management.
  - Comply with laws and regulations.

5. Strengthening of information sharing and cooperation systems between cyber infrastructure provider and stakeholder

- **Sharing of threat and vulnerability information among stakeholders and response to it**
  - Share threat and vulnerability information with government and industry partners in a prompt and timely manner.
  - Suppliers must share software vulnerability information with the relevant agencies that have jurisdiction.
- **Collaboration among stakeholders engaged in cybersecurity**
  - All stakeholders, including communities, must work together in a healthy manner.
  - Work together to develop a framework for identifying potential risks and assessing supply chain risk dependencies related to cybersecurity.
  - In terms of security measures, take initiative and share responsibilities throughout the entire supply chains, including platform providers and consumer tenant organizations.
  - In cooperation with the government, the private sector must continually adapt to the necessary requirements and improve the security of the technologies, products, and services supporting businesses that provide critical infrastructure.
  - Appropriate and timely participation of stakeholders enables sharing of knowledge and awareness, which leads to appropriate risk management.

Requirements for customers of cyber infrastructure providers

- In activities related to the security of software that constitutes a system in which a customer has ownership, the customer is required to fulfill the following responsibilities:

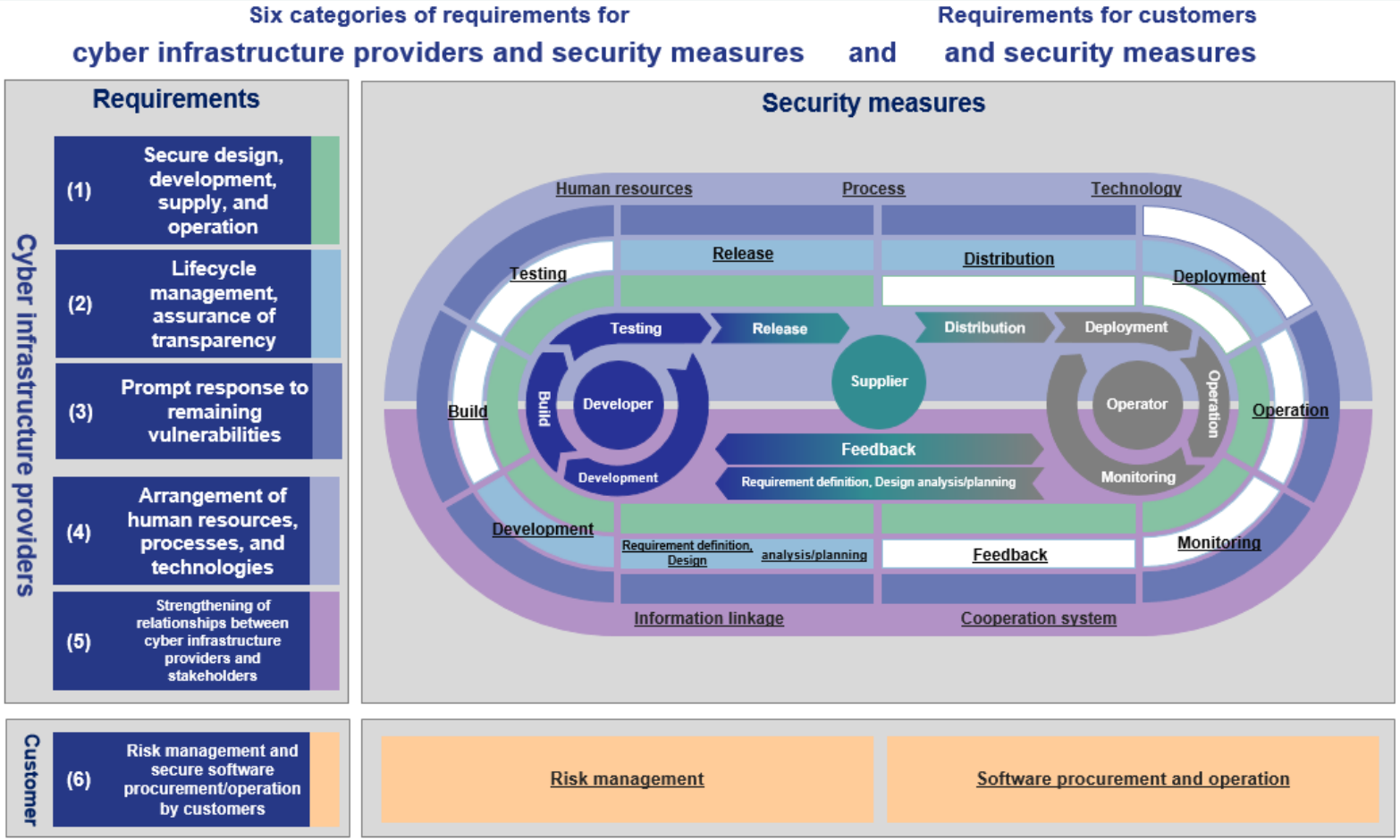
6. Risk management and software procurement/operation by the leadership of the customer's management

- **Risk management by the leadership of the customer's management**
  - Risk management with independent and proactive initiatives and cooperative measures by the customer based on a contract with a cyber infrastructure provider
  - Allocation and preparation of resources to respond to known vulnerabilities proactively and implement measures for mitigation
  - Utilization of communities and cooperative systems aimed at security improvement
- **Software procurement/operation by the leadership of the customer's management**
  - Presentation of security requirements to incorporate security functions into software design plans
  - Disclosure of requirements for security practices in software procurement/implementation
  - Decision-making based on risk assessment in software procurement/implementation
  - Budgeting for software operation, risk response, and contracts considering the life cycles

Requirements for cyber infrastructure providers and customers (general)

- To fulfill their responsibilities toward improving cybersecurity resilience, cyber infrastructure providers and customers are required to implement the cybersecurity measures described below (six categories and 21 requirements) in a manner that is appropriate to the characteristics of the intended software and the organization.

- Therefore, under the leadership of the management responsible for risk management in the organization, it is necessary to proceed with the implementation policy of measures appropriate to the risks, allocation of budgets and human resources, confirmation of the implementation status, identification of problems, responses to problems, and cooperation with other related organizations.



Requirements for cyber infrastructure providers and customers (list)

- Requirements for fulfilling responsibilities are arranged into categories with a one-to-one relationship with responsibilities.
- The five requirements for cyber infrastructure providers and one requirement for customers are described below.

	Requirement categories and summary	Requirements
Cyber infrastructure provider	(1) Secure design, development, supply, and operation Develop, supply, and operate software that checks vulnerabilities and has security	(1)-1 Risk assessment during design and tracking of countermeasures (1)-2 Secure build (1)-3 Testing (1)-4 Monitoring of services
	(2) Life cycle management and assurance of transparency Provide an assurance of transparency in software management throughout life cycles and manage risks including those in the supply chain	(2)-1 Arrangement of secure components (2)-2 Secure archiving of release files and data (2)-3 Establishment of security requirements among stakeholders (2)-4 Appropriate information provision for users
	(3) Prompt response to remaining vulnerabilities Identify vulnerabilities remaining in released software and respond to them promptly	(3)-1 Continuous vulnerability investigation (3)-2 Responses to detected vulnerabilities (3)-3 Application of results of countermeasures to in-house process improvement
	(4) Arrangement of human resources, processes, and technologies Arrange human resources, processes, and technologies related to software at the organizational level	(4)-1 Human resources: Commitment from management and arrangement of personnel (4)-2 Process: Establishment of a development policy and compliance with laws and regulations (4)-3 Process: Establishment of an operational policy and compliance (4)-4 Process: Establishment of development and operation standards (4)-5 Technology: Arrangement of secure development tools (4)-6 Technology: Arrangement of secure development environments
	(5) Strengthening of relationships between cyber infrastructure providers and stakeholders Reinforce information sharing and cooperation between cyber infrastructure providers and stakeholders	(5)-1 Organizational system for information sharing (5)-2 Strengthening of cooperation systems
Customer	(6) Risk management by customers, and procurement and operation of secure software Implement risk management, and secure software procurement and operation under the leadership of the customer's management	(6)-1 Risk management by the leadership of the customer's management (6)-2 Software procurement/operation by the leadership of the customer's management

<Reference>

Guidelines on the Roles Expected of Cyber Infrastructure Providers (draft) (whole)

[Cyber infrastructure provider requirement 1]
Secure design, development, supply, and operation (1)

Risk assessment during design and tracking of countermeasures

Analyze and assess the risks of software to be developed in accordance with the principles of "secure by design" and "secure by default"; track risk responses, security requirements, and design decisions; and maintain countermeasures.

S(1)-1

- **Developer**
- Supplier
- Operator
- Customer

Itemized requirements

- ☐ **S(1)-1.1 Risk-based security requirements definition**
  Perform risk-based analysis and assessment of the software to be developed or the system/service using the software, and define security requirements that serve as mitigation measures.
- ☐ **S(1)-1.2 Design review**
  Through a review of the software design, confirm that it meets all security requirements and adequately addresses identified risk information, and apply the review results.
- ☐ **S(1)-1.3 Risk response records**
  Maintain records of design decisions, responses to risks, and approved exceptional measures for audit and maintenance purposes throughout the software life cycle.
- ☐ **S(1)-1.4 Periodic risk-based review**
  Review all approved exceptions to security requirements and software design, as well as the results of the risk-based analysis and assessment created during the software design, and periodically check whether risks are being addressed appropriately.

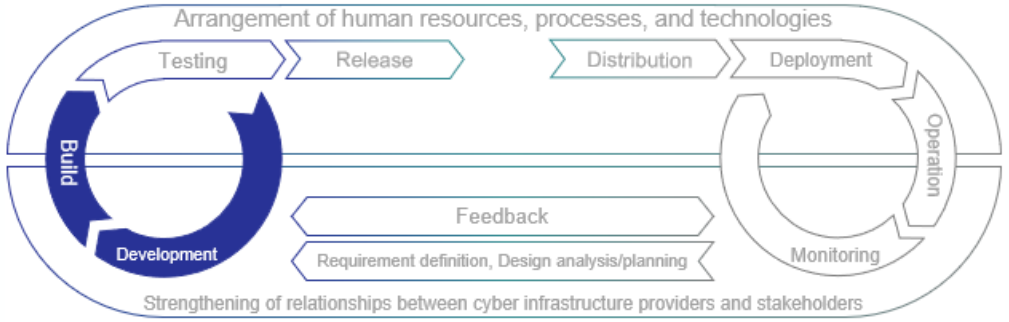
[Cyber infrastructure provider requirement 1]
Secure design, development, supply, and operation (2)

Secure build

Define secure coding and system construction processes that are appropriate for development languages and development environments, and generate and build code accordingly. Review and analyze code, including configurations, and feed the results back to the process.

S(1)-2

- **Developer**
- Supplier
- Operator
- Customer



Itemized requirements

- ☐ **S(1)-2.1 Definition of a secure development process**
  Define processes related to secure coding, secure build, and secure by default, by considering secure coding perspectives, the build timing and method, the use of automation tools, and training.
- ☐ **S(1)-2.2 Secure build**
  Generate and build code using a compiler, an interpreter, and build tools that provide functions to improve the security of executable formats.
- ☐ **S(1)-2.3 Verification and feedback**
  Identify root causes of problems discovered through verification by review and analysis, and then feed the results back to the processes.
- ☐ **S(1)-2.4 Codebases**
  For objects subject to review and analysis, not only source codes but also codes in various formats (such as configuration files) that the organization determines to be readable should be targets.

[Cyber infrastructure provider requirement 1]
Secure design, development, supply, and operation (3)

Testing

Design and implement vulnerability testing and penetration testing as well as functional testing to find vulnerabilities not identified in the review and analysis up to the build phase, and subsequently take countermeasures against identified vulnerabilities.

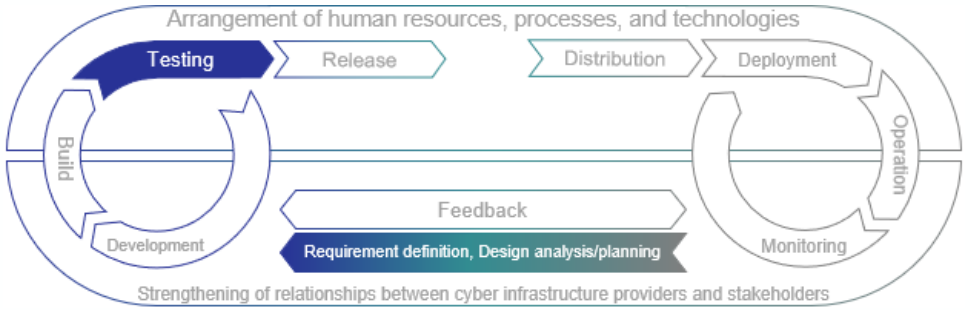
S(1)-3

Developer

Supplier

Operator

Customer



Itemized requirements

- ☐ **S(1)-3.1 Test planning**
  Based on threat models and risk analysis, determine a test scope and test method, and develop a test plan.
- ☐ **S(1)-3.2 Test method**
  Include functional testing, vulnerability testing, fuzzing, penetration testing, etc. in the test method.
- ☐ **S(1)-3.3 Test implementation**
  Design and implement tests according to the test plan, and document the test results.
- ☐ **S(1)-3.4 Response to problems**
  Incorporate all problems identified through testing and recommended countermeasures into the development team's workflows to solve them.

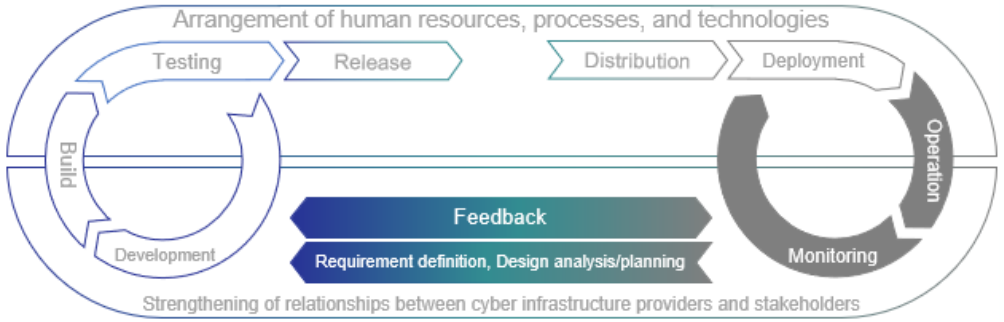
[Cyber infrastructure provider requirement 1]
Secure design, development, supply, and operation (4)

Monitoring of services

Arrange a process and system that monitors software protects and maintains information assets and is consistent with the environment in which it is implemented (network, platform, service, etc.), and implement these.

S(1)-4

- **Developer**
- Supplier
- **Operator**
- Customer



Itemized requirements

- ☐ **S(1)-4.1 Asset management**
  Operators arrange asset management procedures and asset lists related to assets handled by systems and services as well as assets that constitute the systems and services.
- ☐ **S(1)-4.2 Development of a monitoring environment**
  Operators separate systems appropriately to minimize the potential impact of a risk when it occurs, and arrange a monitoring environment to monitor risks that are important to protect assets by means of software.
- ☐ **S(1)-4.3 Arrangement of a security mechanism**
  An appropriate security mechanism is arranged that allows software and systems and services to which the software is applied to protect and monitor the confidentiality and integrity of information assets and data in operating environments or resources such as digital infrastructure.
- ☐ **S(1)-4.4 Monitoring and evaluation**
  Operators monitor the operation of mechanisms applied to software that provides important services, periodically conduct security assessments, and integrate them into the risk management framework of the organization.

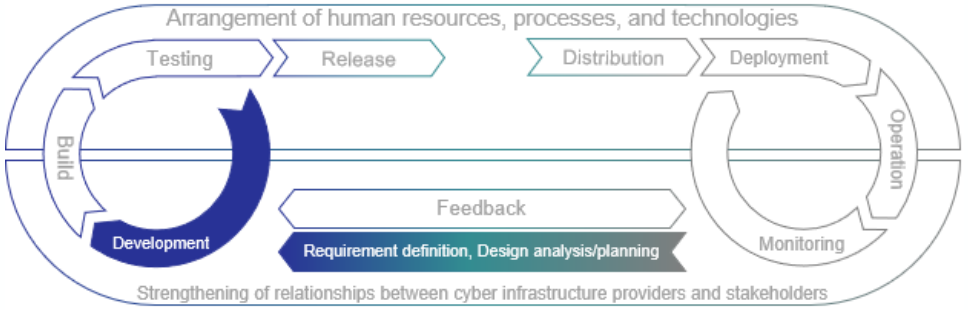
[Cyber infrastructure provider requirement 2]
Life cycle management and assurance of transparency (1)

Arrangement of secure software components

Verify that commercial, open-source, and other third-party software components procured from outside comply with the defined in-house requirements throughout their life cycles.

S(2)-1

- **Developer**
- Supplier
- Operator
- Customer



Itemized requirements

- ☐ **S(2)-1.1 Arrangement of software components**
  With respect to commercial, open-source, and other third-party software components procured from outside, adopt those that are highly secure and meet the defined in-house requirements.
- ☐ **S(2)-1.2 Development and maintenance of software components**
  When the software components are not procured from outside, develop highly secure software components in-house in accordance with established in-house security standards and practices, and maintain them.
- ☐ **S(2)-1.3 Risk assessment of software components**
  Acquire and analyze information regarding locations from where the respective software components are obtained and assess the risks resulting from the components.
- ☐ **S(2)-1.4 Confirmation of publicly known vulnerabilities of software components**
  Regularly check for publicly known vulnerabilities and periods during which respective software components are supported.
- ☐ **S(2)-1.5 Update of software components**
  Implement a process to update the respective software components to a new version securely.

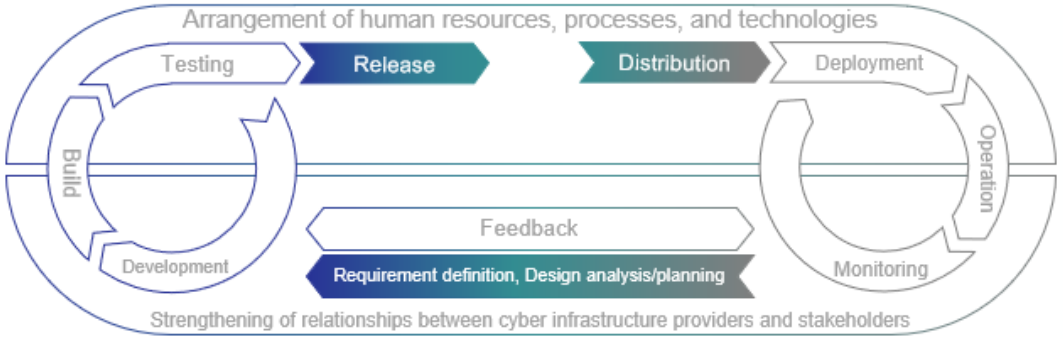
[Cyber infrastructure provider requirement 2]
Life cycle management and assurance of transparency (2)

Secure archiving of release files and data

Archive the necessary files and data to be retained during software release and restrict access to only necessary personnel, tools, and services. Collect, protect, maintain, and share provenance data for all components of the respective releases through the gradual adoption of the SBOM, etc.

S(2)-2

- **Developer**
- **Supplier**
- Operator
- Customer



Itemized requirements

- ☐ **S(2)-2.1 Protection of codebases**
  To protect codebases in all forms from unauthorized access and tampering, store the codes and configuration information in a repository and implement access control based on the principle of least privilege so that only authorized personnel, tools, and services can access it.
- ☐ **S(2)-2.2 Archiving of releases**
  Archive the respective software releases to protect them so that vulnerabilities identified following release can be analyzed and identified.
- ☐ **S(2)-2.3 Sharing of release provenance data**
  Collect, protect, maintain, and share provenance data for all components of the respective software releases.

[Cyber infrastructure provider requirement 2]
Life cycle management and assurance of transparency (3)

Establishment of security requirements among stakeholders

Establish security requirements for the parties involved to agree upon and include them in contracts or policies to be shared.

S(2)-3	Developer
	Supplier
	Operator
	Customer

Itemized requirements

- ☐ **S(2)-3.1 Agreement on security requirements**
  Include explicit security requirements in contracts or policies to be shared with third parties that provide IT products (including commercial software components for use in in-house software) or services.
- ☐ **S(2)-3.2 Responses to supply chain security requirements**
  Respond to supply chain security requirements equivalent to those adopted by the organization that receives or acquires IT products or services that it provides.
- ☐ **S(2)-3.3 Establishment of a response process for risks that do not meet security requirements**
  Arrange a process to respond to risks in the case in which there are security requirements that IT products or services made by a third party to be received or acquired do not meet.

[Cyber infrastructure provider requirement 2]
Life cycle management and assurance of transparency (4)

Appropriate information provision to users

Ensure that software users can apply guidance that facilitates secure use throughout the entire software life cycle—from introduction and installation to operation and termination of use.

S(2)-4	**Developer**
	Supplier
	Operator
	Customer

Itemized requirements

- ☐ **S(2)-4.1 Secure introduction, configuration, operation, modification, disposal, and termination**
  Ensure that software users can continuously use information for securely introducing, configuring, and operating software, as well as information related to the impact of changes, disposal, termination of provision, and termination of use.
- ☐ **S(2)-4.2 Provision of integrity verification information**
  Ensure that software users can continuously use information that is necessary for verifying the integrity and completeness of software.

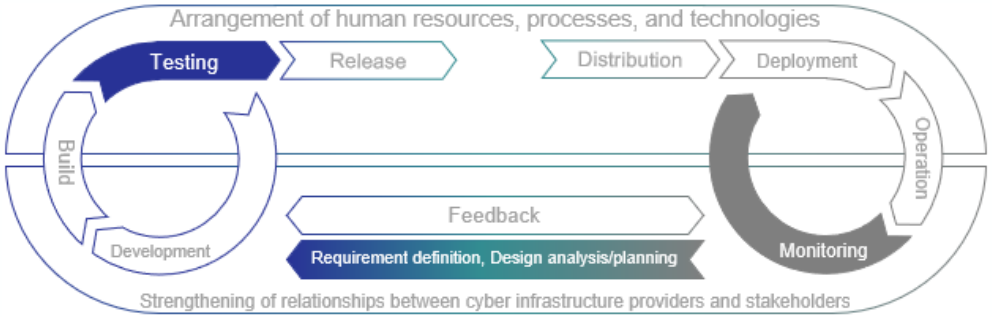
[Cyber infrastructure provider requirement 3] Prompt response to remaining vulnerabilities (1)

Continuous vulnerability investigation

Establish a policy for disclosure and remediation of software vulnerabilities, define roles, responsibilities, and processes required for the policy and implement them.

S(3)-1

- **Developer**
- Supplier
- **Operator**
- Customer



Itemized requirements

- ☐ **S(3)-1.1 Establishment of a vulnerability response system**
  Establish a policy for the disclosure and remediation of vulnerabilities of software products, establish a system for responses to vulnerabilities (including responses to incidents) to support the policy, and define necessary roles, responsibilities, and processes.
- ☐ **S(3)-1.2 Communication plan**
  Establish a communication plan for all stakeholders.
- ☐ **S(3)-1.3 Vulnerability information collection**
  Collect new information regarding vulnerabilities through searches of public information, notifications from software users, the acquisition of external threat information, reviews of system configuration data, and other methods.
- ☐ **S(3)-1.4 Identification of undetected vulnerabilities**
  Conduct software code review, analysis, and testing on an ongoing or regular basis to identify undetected vulnerabilities (including improper settings) to be solved.

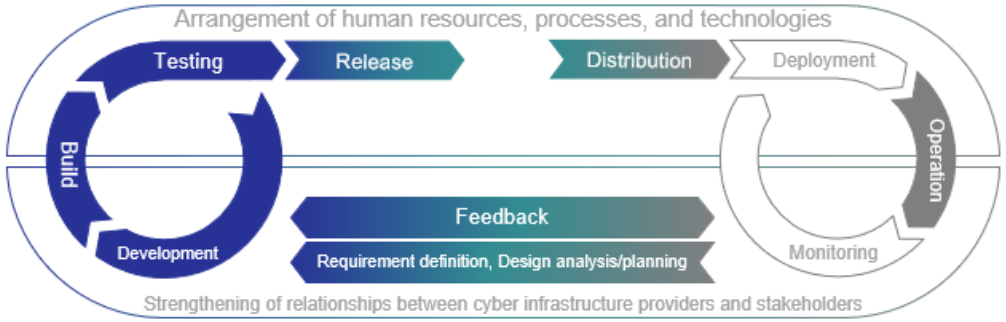
[Cyber infrastructure provider requirement 3] Prompt response to remaining vulnerabilities (2)

Responses to detected vulnerabilities

Regularly create a plan to respond to risks of vulnerabilities remaining in released software and implement it.

S(3)-2

- Developer
- Supplier
- Operator
- Customer



Itemized requirements

- ☐ **S(3)-2.1 Vulnerability analysis**
  Developers collect information necessary to understand the risks associated with the impact of each remaining vulnerability and analyze each vulnerability to plan repairs or other responses to risks.
- ☐ **S(3)-2.2 Risk responses to vulnerabilities**
  Developers create a plan for risk responses for each vulnerability and implement it.
- ☐ **S(3)-2.3 Security recommendations**
  Developers prepare security recommendations, provide the information to the supplier of the released software, and create a report as specified by the relevant systems. In addition, operators implement deployment in accordance with security recommendations.

[Cyber infrastructure provider requirement 3] Prompt response to remaining vulnerabilities (3)

Application of results of countermeasures to in-house process improvement

Based on vulnerabilities, review development and operation processes so that the root causes of problems identified in the software do not recur or the possibility of their recurrence is reduced.

S(3)-3

- **Developer**
- Supplier
- **Operator**
- Customer

Itemized requirements

- ☐ **S(3)-3.1 Identification of root causes**
  Analyze an identified vulnerability to determine its root causes and proactively take countermeasures.
- ☐ **S(3)-3.2 Process improvement**
  Review development and operation processes for the entire software life cycle and revise them as necessary to prevent root causes from recurring or reduce the possibility of their recurrence through software updates or new software creation.

[Cyber infrastructure provider requirement 4]
Arrangement of human resources, processes, and technologies (1)

Human resources: Commitment from management and arrangement of personnel

Define roles and responsibilities covering the entire software life cycle. Make management's commitment to secure development known, secure personnel for security measures, provide training to all personnel related to secure development and operation according to their levels of proficiency and role, and review it regularly.

S(4)-1	Developer
	Supplier
	Operator
	Customer

Itemized requirements

- ☐ **S(4)-1.1 Definition of roles and responsibilities**
  Define roles and responsibilities covering the entire software development life cycle.
- ☐ **S(4)-1.2 Management's commitment**
  Make management's commitment to secure development known to all personnel, and educate them on the importance of secure development and operation to the organization.
- ☐ **S(4)-1.3 Agreement on roles and responsibilities**
  Confirm that all personnel are aware of and agree to their roles and responsibilities.
- ☐ **S(4)-1.4 Training for each role**
  Create a training plan for each role and implement it so that all personnel can be trained according to their level of proficiency and role.
- ☐ **S(4)-1.5 Review of roles and training**
  Review roles and training regularly.

[Cyber infrastructure provider requirement 4]
Arrangement of human resources, processes, and technologies (2)

Process: Establishment of development policy and compliance with laws and regulations

Comply with laws and regulations, document and maintain a security policy for in-house development infrastructures and processes, and secure necessary budgets for security securement.

S(4)-2

- **Developer**
- Supplier
- Operator
- Customer

Itemized requirements

- ☐ **S(4)-2.1 Definition of a software development policy**
  Identify all security requirements for software development infrastructures and processes, and define a security policy for maintenance throughout the SDLC in compliance with laws and regulations.
- ☐ **S(4)-2.2 Definition and maintenance of a software security policy**
  Define a policy that specifies all security requirements that must be met by the software developed by an organization, and maintain the requirements throughout the SDLC.
- ☐ **S(4)-2.3 Sharing of cost recognition and budgeting**
  Secure necessary budgets to ensure security based on a policy.

[Cyber infrastructure provider requirement 4]
Arrangement of human resources, processes, and technologies (3)

Process: Establishment of an operation policy and compliance with laws and regulations

Comply with laws and regulations, and document and maintain all security policies for service operation infrastructures and processes to which soft the ware is applied.

S(4)-3

- Developer
- Supplier
- **Operator**
- Customer

Itemized requirements

- ☐ **S(4)-3.1 Definition of a software service operation policy**
  Identify all security requirements for service operation infrastructures and processes to which the software is applied, and define a security policy for maintenance throughout the SDLC in compliance with laws and regulations.
- ☐ **S(4)-3.2 Definition and maintenance of a service security policy**
  Define a policy that specifies all security requirements that services to which the software is applied must meet, and maintain the requirements throughout the SDLC.
- ☐ **S(4)-3.3 Audit based on an operational policy**
  Confirm through an audit that the protection of service operation infrastructures and processes and security requirements for service are maintained throughout the SDLC in accordance with policy-based governance.

[Cyber infrastructure provider requirement 4]
Arrangement of human resources, processes, and technologies (4)

Process: Establishment of development and operational standards

Define security verification criteria related to software development, collect information necessary to support the criteria, and implement processes and mechanisms for conformance. Track the status of conformance throughout the entire life cycle.

S(4)-4

- **Developer**
- Supplier
- **Operator**
- Customer

Itemized requirements

- ☐ **S(4)-4.1 Definition and tracking of security verification criteria**
  Define software security verification criteria and track the entire SDLC.
- ☐ **S(4)-4.2 Support for decision-making based on security verification criteria**
  Implement processes and mechanisms for collecting and protecting information necessary to support decision-making based on security verification criteria.
- ☐ **S(4)-4.3 Audit based on security verification criteria**
  Track the entire SDLC and verify through audits that the intended effects are achieved with governance to ensure conformance to security verification criteria.

[Cyber infrastructure provider requirement 4]
Arrangement of human resources, processes, and technologies (5)

Technology: Arrangement of secure development tools

Analyze risks throughout the SDLC and implement security measures in development tools.

S(4)-5

- **Developer**
- Supplier
- Operator
- Customer

Itemized requirements

- ☐ **S(4)-5.1 Designation of tools and toolchains**
  Identify tools that are effective in mitigating identified risks, designate which toolchains must be included or need to be included, and determine means of integrating toolchain components mutually.
- ☐ **S(4)-5.2 Deployment, operation, and maintenance of tools and toolchains**
  Deploy, operate, and maintain tools and toolchains in accordance with security practices.
- ☐ **S(4)-5.3 Tool configuration and evidence generation**
  Configure tools to generate evidence regarding support for secure software development practices defined in-house.

[Cyber infrastructure provider requirement 4]
Arrangement of human resources, processes, and technologies (6)

Technology: Arrangement of secure development environments

Analyze risks throughout the SDLC, and protect and strengthen development-related environments.

S(4)-6

Developer

Supplier

Operator

Customer

Itemized requirements

- ☐ **S(4)-6.1 Isolation and protection of environments**
  Isolate and protect the respective environments related to software development.
- ☐ **S(4)-6.2 Protection of development endpoints**
  Protect and strengthen endpoints designed for respective developers to perform development-related tasks using a risk-based approach.

[Cyber infrastructure provider requirement 5] Strengthening of relationships with stakeholders (1)

Organizational system for information sharing

Establish an organizational structure for information sharing between private companies, relevant authorities, and specialized organizations to improve the security of software products and services.

S(5)-1	Developer
	Supplier
	Operator
	Customer

Itemized requirements

- ☐ **S(5)-1.1 Establishment of an organizational system for information sharing**
  Establish an organizational structure for information sharing between private companies, relevant authorities, and specialized organizations to improve the security of software products and services.
- ☐ **S(5)-1.2 Provision of important security-related information**
  Select and identify essential and important security-related information that is specific to the industry and provide it to partners in the supply chain.
- ☐ **S(5)-1.3 Use of vulnerability information notification services**
  Use vulnerability information notification services to share vulnerability information efficiently.

[Cyber infrastructure provider requirement 5] Strengthening of relationships with stakeholders (2)

Strengthening of cooperation systems

To improve the security of software products and services, make use of systems and frameworks for cooperation with private companies, relevant authorities, and specialized organizations.

S(5)-2

- **Developer**
- **Supplier**
- **Operator**
- Customer

Itemized requirements

- ☐ **S(5)-2.1 Utilization of cooperation systems**
  To improve the security of software products and services, make use of communities and cooperation systems aimed at improving software security, in which external businesses, customers, and specialized organizations participate.
- ☐ **S(5)-2.2 Contribution to cooperation systems**
  When participating in a community or cooperation system, actively participate in activities to contribute to the cooperation system.

[Customer requirement 5] Risk management by customers, and procurement and operation of secure software

Risk management under the leadership of the customer's management

Integrate risk management that is implemented in cooperation with cyber infrastructure providers based on the leadership of the customer's management.

Itemized requirements

- ☐ **S(6)-1.1 Risk management**
  Implement risk management in which the customer's independent and proactive efforts are integrated with efforts based on a contract with cyber infrastructure providers.
- ☐ **S(6)-1.2 Resource arrangement**
  Allocate and develop resources to respond proactively to known vulnerabilities and implement mitigation measures (including SBOM utilization).
- ☐ **S(6)-1.3 Utilization of collaborative systems**
  Utilize communities and collaborative systems aimed at improving software security.

Software procurement/operation under the leadership of the customer's management

Procure and operate software securely under the leadership of the customer's management.

Itemized requirements

- ☐ **S(6)-2.1 Definition of security requirements**
  Define security requirements for incorporating security functions into software design plans and present them to cyber infrastructure providers before procuring and deploying software.
- ☐ **S(6)-2.2 Disclosure of security practice requirements**
  Disclose security practice requirements for cyber infrastructure providers before procuring and deploying software.
- ☐ **S(6)-2.3 Decision-making based on risk assessment**
  When procuring and introducing software, make decisions based on risk assessment.
- ☐ **S(6)-2.4 Budget securement**
  Continuously secure budgets related to operation, risk response, and related contracts, considering software life cycles.