JAMA/JAPIA

JAMA/JAPIA Cybersecurity Guidelines V2.1 Handbook

Ver. 2.1 Rev.1

May 31, 2024

Revision History

Edition	Date Issued	Revision Details
First Edition	December 12, 2022	First version
Version 2.1	September 1, 2023	Revision and modification following the publication of Guideline Ver. 2.1. The edition became Ver. 2.1 to align with the Guideline version.
Version 2.1 Rev.1	May 31, 2024	Enhancement of explanations (addition of Targets for Expanded Explanation)

Table of Contents

1. Position of This Handbook

This handbook extracts and further expands upon terms, requirements, achievement criteria, and other parts of the JAMA/JAPIA Cybersecurity Guidelines V2.1 that may be difficult to interpret. To the greatest extent possible, "parts that are difficult to interpret" have been picked out and had explanations added from a viewpoint of all companies, though please note that explanations from all viewpoints have not been added for all items.

This handbook is intended for those belonging to security departments and other related departments.

2. Targets for Expanded Explanation

This handbook extracts and further expands upon items in the JAMA/JAPIA Cybersecurity Guidelines V2.1 that may be difficult to interpret.

No.	Point to be Explained	Page
Common	Checklist evaluations in the case of group companies	p.9
1	Information security policy items and scope of application	p.10
4	Points to note when establishing non-disclosure rules	p.11
	Methods to enforce non-disclosure rules	p.12
5	Ways of thinking about the written contents of a letter of commitment to non-disclosure	p.13
6	Ways of thinking about the written contents for the confidentiality of external leaks	p.14
7	Scope of IT equipment/devices to be collected	p.15
8	Items to be observed/prohibited during the usage of IT equipment/devices	p.16
9	Content of training and frequency of education regarding laws related to information security	p.17
	Applicable information security-related laws	p.18
10	Scope and content of training regarding personal information	p.19
13	Concept regarding clarification of the roles and responsibilities of information security officers	p.21
	Points to note when creating a list of contact persons for normal situations	p.21
14	Necessity of appointing an information security officer	p.23
16	Approach for detecting new methods of cyberattacks and information leaks	p.24
	Methods for establishing a system for monitoring and analyzing cyberattacks and signs	p.25
	Ways of thinking about signs of cyberattacks	p.26
17	Ways of thinking about systems for monitoring and analyzing cyberattacks and signs	p.26
	Ways of thinking about correlation analysis	p.27
18	Document defining the roles and responsibilities of information security officers in an emergency	p.28
	Points to note when creating a list of contact persons in an emergency	p.28
21	Business continuity plan and emergency response plan differences and roles	p.30
23	Document defining the scope of information security incidents	p.32
24	Procedures for responding to information security incidents	p.33
26	Procedures for responding to malware infections	p.35
28	Content of training regarding malware infections via email	p.36
29	Content of training regarding malware infections during online browsing	p.37
31	Targeted email training content and implementation criteria	p.38
38	Ways of thinking about the education and training on the responses when information security incidents or accidents occur	p.39
39	Ways of thinking about security incidents across organizations	p.41
41	Ways of thinking about the flow of goods and data shared with suppliers	p.42
	Definition and scope of important suppliers	p.43

3. How to Read This Handbook

The method with which this handbook should be read is as follows.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
1 Policies	As a company, demonstrate basic concepts and policies regarding security and enhance awareness of information security within the organization	An in-house information security policy shall be established and communicated within the organization	1	Lv1	**(A)** An in-house information security policy is established	· An in-house information security policy shall be established and documented

[Explanation]
■ **Condition(s) for Achievement**
① **Are there any samples that satisfy the items established in the "information security policy"?**
Concrete samples can be found in the "Information Security Policy Samples Ver. 1.0" (2016) (*1), published by JNSA (NPO Japan Network Security Association). The samples created in 2002 were revised on March 29, 2016 in order to support the emergency of new technologies and services such as smart devices, cloud computing, and social media. As of 2022, many companies, regardless of size, are still using these as reference material, and the explanations of the items that should be established should be helpful.
(B) For small- and medium-sized companies, "Information Security Policy (an SD)" IPA, 2019) (*2) can serve as a reference.
Looking at these, it is possible to gain an understanding on how to define the basic policy for ensuring information security as a company, as well as the systems and countermeasure standards for that policy. However, these examples are only reference information, and it is important to establish a policy after making substitutions in accordance with your company's organization and environment. ↓
Reference (*1): https://www.jnsa.org/result/2016/policy/
Reference (*2): https://www.ipa.go.jp/files/000072146.docx

<Figure: Sample from the handbook>

The handbook is structured as follows.

A) Guideline item(s) to be explained

The content of the original guideline (label, objective, requirement, No., level, condition(s) for achievement, and achievement criteria) is described.

In addition, the applicable parts of the guideline to be further explained have been highlighted.

B) Explanation

An explanation is provided for the parts of the guideline that may be difficult to interpret. The specific parts are indicated as follows using the "■" symbol and quotations.

Example: Giving an explanation regarding the information security policy in the guideline's condition(s) for achievement
[Explanation]
■ Condition(s) for Achievement
① For "information security policy,"...

4. Handbook

■ **Common items**

① **In the case of a group company, are checklists filled out for each company individually, or is it only a single checklist for the group?**

For group companies, please fill out a checklist for each individual company, as opposed to one consolidated checklist.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
1 Policies	As a company, demonstrate basic concepts and policies regarding security and enhance awareness of information security within the organization	An in-house information security policy shall be established and communicated within the organization	1	Lv1	An <mark>in-house information security policy</mark> is established	・An in-house information security policy shall be established and documented

[Explanation]

■ **Condition(s) for Achievement**

① **Are there any samples that satisfy the items established in the "information security policy"?**

Concrete samples can be found in the "Information Security Policy Samples Ver. 1.0" (2016) (*1), published by JNSA (NPO Japan Network Security Association). The samples created in 2002 were revised on March 29, 2016, in order to support the emergence of new technologies and services such as smart devices, cloud computing, and social media. As of 2022, many companies, regardless of size, are still using these as reference material, and the explanations of the items that should be established should be helpful.

For small- and medium-sized companies, "Information Security Policy (Sample)" (IPA, 2019) (*2) can serve as a reference.

Looking at these, it is possible to gain an understanding on how to define the basic policy for ensuring information security as a company, as well as the systems and countermeasure standards for that policy. However, these examples are only reference information, and it is important to establish a policy after making substitutions in accordance with your company's organization and environment.
Reference (*1): https://www.jnsa.org/result/2016/policy/

Reference (*2): https://www.ipa.go.jp/files/000072146.docx

② **Are overseas bases also included as part of "in-house"?**

As mentioned in Explanation (1) of Common items, they are individual companies and so are not included.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
2 Rules for handling confidential information	Prevent the leakage of confidential information by defining rules for handling confidential information and communicating those rules within the organization	In-house rules to ensure security for confidential information shall be defined	4	Lv1	Non-disclosure rules in the company are established and enforced	[Rule(s)] ・Non-disclosure rules shall be established and documented ・Explanations regarding non-disclosure rules are provided when new employees (including outside employees) join the company ・Confidential information shall not be carried outside the company when an employee resigns or their contract date expires [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.)

[Explanation]

■ **Condition(s) for Achievement**

① **Though "non-disclosure rules are established in the company" is stated, what kind of non-disclosure rules should be specifically established?**

When establishing non-disclosure rules, it is important to determine which information should be considered confidential based on the potential impact it could have if it were to be leaked and whether it could be useful to competitors. It is recommended to define the scope of non-disclosure and then establish clear rules for maintaining non-disclosure. The "Handbook for Protecting Confidential Information" published by the Ministry of Economy, Trade and Industry (METI) can provide helpful guidelines. For example, rules should include the following: (Examples below)

・ Identify the group of people to whom the non-disclosure rules apply (executives, employees, temporary employees, outsourced employees, etc.).
・ Identify the type of confidential information applicable (management information, personal information, sales information, technical information including intellectual property, etc.).
・ Classify the confidential information (For Executives Only, For Department Use Only, For Company Use Only).
・ Implement measures to prevent any leakage of confidential information (e.g., ensuring that employees maintain non-disclosure through work rules/a letter of commitment to non-disclosure, executing non-disclosure agreements with third-party vendors when starting a business, etc.)
・ Establish penalties in case of any leakage of confidential information.

<Example of non-disclosure rules for in-house employees>

Specific non-disclosure rules for in-house employees include work rules relating to employee conduct and the management of confidential information, as outlined in Reference Material 2, "Reference Examples of Various Contracts, etc." of the "Handbook for Protecting Confidential Information" published by the METI.

<Example of non-disclosure rules for outside employees>
When your company outsources work to an external party, it provides them access to a significant amount of information related to the company and its operations. If the outsourced company leaks confidential or personal information, your company will also be held responsible for the breach. Therefore, it is essential to consider signing a non-disclosure agreement or adding a confidentiality clause to the outsourcing contract. For specific examples of confidentiality clauses, it is recommended to refer to the "Reference Examples of Various Contracts, etc." in the "Handbook for Protecting Confidential Information" published by the METI, and it is advisable to seek guidance from the company's legal personnel.

*The "Handbook for Protecting Confidential Information" includes a section titled "3-4 Specific Examples of Measures to Prevent Information Leakage," which provides specific countermeasures for information leakages and specific examples for protecting confidential corporate information. Furthermore, Reference Material 2, "Reference Examples of Various Contracts, etc." has two sections - the "first" section includes examples of employee work rules, and the "second" section includes examples of confidential information management rules.
Reference: Handbook for Protecting Confidential Information (Ministry of Economy, Trade and Industry)
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

Reference: Reference Material 2, Reference Examples of Various Contracts, etc. (Ministry of Economy, Trade and Industry)
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf

② **Though non-disclosure rules are "enforced" in the company is stated, how can the company ensure the enforcement of non-disclosure rules?**
As previously mentioned in the explanation ①, it is crucial to define the scope of non-disclosure and properly mark any material or items that contain confidential information as such. Additionally, the following measures can be taken for both in-house and outside employees. (Examples below)

< Enforcing non-disclosure rules on in-house employees >
・ Provide education and training on how to manage confidential information to ensure that the rules are well understood and followed.
・ If a conversation includes confidential information related to the department, it must be recorded in the minutes and clearly informed that the information is confidential.
・ Require employees to submit a letter of commitment to non-disclosure at the time of joining or retiring.
・ Establish a whistle-blowing contact point for reporting any violations.

< Enforcing non-disclosure rules on outside employees >
・ Provide education and training on how to manage confidential information to ensure that the rules are well understood and followed.

- Record all conversations related to the disclosure or provision of confidential information, and inform outside employees that the information is confidential.
- Include a clause in the non-disclosure agreement that the other party will cooperate with audits related to measures taken to prevent the leakage of confidential information and provide access logs to confidential information.
- Include a clause in the non-disclosure stating that if the confidential information is breached, the company will seek cooperation with the investigation, demand compensation for damages, and take legal action if necessary.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
2 Rules for handling confidential information	Prevent the leakage of confidential information by defining rules for handling confidential information and communicating those rules within the organization	In-house rules to ensure security for confidential information shall be defined	5	Lv2	Non-disclosure rules in the company are established and enforced	[Rule(s)] ・A letter of commitment for non-disclosure shall be submitted (excluding outside employees)

[Explanation]

■ Achievement Criteria

① **Where can the reference for specific information about the "letter of commitment for non-disclosure" be found?**

It is not sufficient to only establish the non-disclosure rules for employees within the company. To ensure that all employees are aware of their non-disclosure obligations, it is important that they submit a letter of commitment for non-disclosure. Additionally, information leakage is possible even after an employee leaves the company. Therefore, the contents of the letter must be drafted in a way that the non-disclosure obligation remains valid not only during the employees' tenure but also after they leave the company. Reference Material 2, "Reference Examples of Various Contracts, etc." of the "Handbook for Protecting Confidential Information" (Ministry of Economy, Trade and Industry) contains a sample letter of commitment to confidentiality that can serve as a reference.

The "Handbook for Protecting Confidential Information" includes a section titled "3-4 Specific Examples of Measures to Prevent Information Leakage," which explains the importance of having employees submit a letter of commitment for non-disclosure, provides some essential points to keep in mind, and can be used as a helpful reference. Moreover, in Reference Material 2, "Reference Examples of Various Contracts, etc.," there is an example of a letter of commitment to confidentiality in the "third" section.

Reference: Handbook for Protecting Confidential Information (Ministry of Economy, Trade and Industry)
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

Reference: Reference Material 2, Reference Examples of Various Contracts, etc. (Ministry of Economy, Trade and Industry)
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
2 Rules for handling confidential information	Prevent the leakage of confidential information by defining rules for handling confidential information and communicating those rules within the organization	In-house rules to ensure security for confidential information shall be defined	6	Lv2	A non-disclosure agreement is entered into with the dispatching/transferring company for temporary and transferred employees	[Rule(s)] ・<mark>For non-disclosure, a statement shall be included stating that information obtained in the course of business will not be divulged</mark> [Timing] *When to enter into a contract for confidentiality obligations ・Before starting business

[Explanation]

■ **Achievement Criteria**

① **Though "for non-disclosure, a statement shall be included stating that information obtained in the course of business will not be divulged" is mentioned, where can the reference for specific information about non-disclosure be found?**

To prevent temporary or transferred employees from disclosing confidential or personal information related to the company or their work, it is highly recommended to discuss the following points with the in-house legal personnel and incorporate them into the agreement:

- Temporary/transferred employees shall maintain confidentiality.
- Temporary/transferred employees shall allow them to be instructed on company policies and procedures regarding the prevention of confidential information leakage
- Temporary/transferred employees shall cooperate with audits regarding measures against leakage of confidential information.
- In the event of a breach, temporary/transferred employees shall cooperate with investigations, compensate for damages, and undergo legal actions.
- At the end of their employment, temporary/transferred employee shall return all confidential information and information equipment. (Refer to Requirement No.7)

The Ministry of Health, Labor, and Welfare and the labor bureaus of each prefecture offer templates and samples of worker dispatch contracts. For information on confidentiality, refer to Articles 14 and 15 of the "Template of Standard Contract for Dispatch Workers" published by the Ministry of Health, Labor and Welfare.
Reference: Template of Standard Contract for Dispatch Workers (Ministry of Health, Labor and Welfare)
https://www.mlit.go.jp/common/001383155.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
2 Rules for handling confidential information	Prevent the leakage of confidential information by defining rules for handling confidential information and communicating those rules within the organization	In-house rules to ensure security for confidential information shall be defined	7	Lv2	The necessary confidential information, IT equipment/devices, etc., is collected when an employee resigns or their contract date expires	[Standards] ・A checklist or form shall be created for the list of items to be collected ・Procedures shall be prepared and utilized that prevent collection omissions ・It shall be checked that collection is done in accordance with the procedure, and the procedure shall be corrected as necessary [Items to be collected] -Information (printed materials, storage media) -IT equipment/devices (PCs, smart devices) -Access rights (ID, keys) *In addition to the above, each company shall determine what items will be necessary to collect [Confirmation of collection status, frequency of procedure correction] -Once or more per year

[Explanation]

■ **Achievement Criteria**

① **If an employee is given permission and uses their own device for business purposes, is that device included in the "equipment/devices" that should be collected?**

It is not included. However, from the perspective of "preventing the leakage of confidential information," which is the objective of this item, it is advisable to implement an alternative measure for the collection of IT equipment/devices. (Examples below)

・ Use a system that prevents business data from being saved on the device (thin client, etc.)

・ Establish operating rules for deleting business data when use of the device ends, and create a letter of commitment with employees in advance

These personal devices used by employees for work are called BYOD (Bring Your Own Device) devices, and while they provide advantages such as increased business efficiency, they also have the disadvantage of increased security risks such as information leakage if they are not handled properly. Therefore, it is necessary to create operating rules that include what is and is not allowed, with No. 8 being the applicable item for that.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
2 Rules for handling confidential information	Prevent the leakage of confidential information by defining rules for handling confidential information and communicating those rules within the organization	In-house rules to ensure security for confidential information shall be defined	8	Lv1	Rules for the usage of IT equipment/devices employed for business operations are defined and communicated within the organization (including rules for personal devices [BYOD])	[Rule(s)] ・ Rules for the usage of IT equipment/devices (computers, servers, communications equipment, storage media, smart devices, etc.) shall be established that include procedures for starting/ending usage, ==items to be observed/prohibited during usage==, and procedures for when such equipment/devices are lost ・ Rules for the usage of IT equipment/devices shall be in a format that is easily accessible [Applies to] ・ Executives, employees, outside employees (including temporary employees, etc.) [Frequency] ・ Rules shall be communicated within the organization regularly and whenever revised

[Explanation]

■ **Achievement Criteria**

① **What kind of content should be included in "items to be observed/prohibited during the usage" of IT equipment/devices?**

The "Information Security Measure Guidelines for Small and Medium-sized Enterprises" and Appendix 3, "Five-Minute Information Security Self-Diagnosis" (IPA) provide examples of security measures that employees should follow while using IT equipment/devices. These are recommended as references.

Below are some key points and examples of security measures to consider when using IT equipment/devices.

・ Keep the operating system and software of your IT equipment/devices up-to-date to ensure information security.
・ Do not leave your IT equipment/devices unattended on your desk and store them safely when you leave your desk or finish work to prevent loss or theft.
・ When taking your IT equipment/devices outside of the company, make sure that you take measures such as data encryption within the IT equipment/device.
・ Personal devices are generally not allowed in the workplace. However, if personal devices are necessary for business purposes (BYOD), strict management rules must be followed.

The "Information Security Measure Guidelines for Small and Medium-sized Enterprises" and Appendix 3, "Five-Minute Information Security Self-Diagnosis" (IPA), contain information security diagnosis items and countermeasures that can be used as a reference.

Reference: Information Security Measure Guidelines for Small and Medium-sized Enterprises, Version 3.1 (IPA)

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

Reference: Appendix 3, "Five-Minute Information Security Self-Diagnosis" (IPA)
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
3 Compliance	As a company, comply with laws regarding information security	In-house rules shall be established to ensure compliance with laws regarding information security (Examples of laws: Act on the Protection of Personal Information, Unfair Competition Prevention Act)	9	Lv1	To ensure compliance with laws regarding information security, rules are established and education/communication are provided within the organization	[Rule(s)] ・In-house rules shall be established to ensure compliance with laws regarding information security ・Established in-house rules shall be communicated within the organization and education provided on those rules [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) [Frequency] (Training) ・Whenever a new employee joins the company and once per year (Communication within the organization) ・Rules shall be communicated within the organization regularly and whenever revised

[Explanation]

■ **Condition(s) for Achievement**

① **While there are the three perspectives of establishing rules, implementing education, and communicating, what kind of content should be included in education on laws regarding information security?**

Instead of providing education on the details and interpretations of laws, it is more important to provide education on the in-house rules established based on those laws. Since the objective is to improve compliance and understanding regarding in-house rules, including an explanation of items to be complied with and risks to the organization should compliance not occur should be sufficient.

② **Should the impact of education be confirmed?**

The requirement does not include the need to confirm the impact of education. However, it may be desirable to do so in order to clarify the return on investment and make future improvements.

③ **What exactly is meant by "laws regarding information security"?**

Since the laws to be complied with will differ depending on the nature of the business, collecting information on related laws and establishing in-house rules based on those should be sufficient.
For reference, representative Japanese laws include the following. (Examples below)

- Unfair Competition Prevention Act

- Act on Electronic Signatures and Certification Business

- e-documentation Act (Act on Utilization of Telecommunications Technology in Document Preservation, etc. Conducted by Private Business Operators, etc.)

- Act on the Protection of Personal Information

- Act on Prohibition of Unauthorized Computer Access

In addition, it is advisable to confirm matters related to the above laws with those in charge of legal affairs. If there is no such department, it is necessary to consult with outside experts to clarify relevant information.

■ **Achievement Criteria**

④ **Specifically, what are considered "regular" frequencies and methods regarding communication?**

As an example, once a year via email or chat/distribution of materials. Any method is acceptable as long as it involves notifying employees so that they do not violate the laws.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
3 Compliance	As a company, comply with laws regarding information security	In-house rules shall be established to ensure compliance with laws regarding information security (Examples of laws: Act on the Protection of Personal Information, Unfair Competition Prevention Act)	10	Lv2	For companies with ==personal information==, there are ==in-house rules stipulated that are specifically for the handling of personal information==	[Rule(s)] ・In-house rules shall be established regarding the handling of ==customer personal information== [Details for clarification] ・Establish a personal information management system ・Notify and clearly indicate purpose of use at the time of acquisition ・Use within the scope of consent of the individual ・Do not provide to a third party without the consent of the individual ・Requests for disclosure, correction, suspension of use, deletion, etc., by the individual shall be responded to ・Rules for the handling of personal information shall be established ・Information shall be collected regarding information security laws and regulations such as the Act on the Protection of Personal Information, GDPR, and Unfair Competition Prevention Act ・Procedures for responding to information leaks ・ [Applies to] - Those in charge of handling personal information

[Explanation]

■ **Condition(s) for Achievement**

① **What items should be handled as "personal information"?**

There are a wide range of items which depend not only on individual pieces of information, but also on use and information combinations. While there are some differences in the definitions of items depending on the laws and regulations of each region/country, taking the Japanese Act on the Protection of Personal Information as an example, the following items are treated as personal information. (Examples below)

・ Name

・ Information that associates the DOB or contact information (address, location, phone number, email address) with the name of an individual

・ Video information that allows an individual to be identified, such as security camera recordings

・ Voice recording information that allows a specific individual to be identified due to containing the individual's name, etc.

*   Additional case examples can be found in the "Guidelines for the Act on the Protection of Personal Information (General Rules)" (Personal Information Protection Commission, 2022).

Reference: https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a2-1

② **Are there any examples that can be used as reference for stipulating "in-house rules that are specifically for the handling of personal information"?**

The Personal Information Protection Commission of Japan has provided guidelines for reference (see the reference link in (1) above). The guidelines also explain the interpretations and examples used for each clause. As such, it is advisable to select the necessary parts as in-house rules based on this content.

■ **Achievement Criteria**

③ **Though "customer personal information" is stated, is it ok to include the personal information of our own employees as well?**

In an of itself, personal information should include not only that of customers, but also information related to various subjects, including employees, business partners, and other related organizations. However, in the achievement criteria for this item the target is focused on the customer, taking into consideration the degree of damage caused when information is leaked.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
4 System (Normal)	Clarify systems and roles for information security and thoroughly enact and reinforce measures for cybersecurity and protecting against data leakage	A system for managing information security risks for use in normal situations shall be constructed to enable the collection and sharing of information without incident	13	Lv1	The system, roles and responsibilities (incl. information security officers) during normal situations are clarified	[Rule(s)] ・The roles and responsibilities of the executive that presides over information security (CISO, etc.) and those of the department in charge of information security shall be clarified ・A list of contact persons shall be established

[Explanation]

■ **Condition(s) for Achievement**

① **What kind of document should "the clarification of roles and responsibilities" be defined in?**

In order to "clarify roles and responsibilities", it is advisable to define them in documents related to information security within the company. However, those documents include high-level regulations that stipulate the outline of requirements, those that stipulate procedures from the perspective of on-site operations, etc., so it can be difficult to determine which documents the information should be written in. That said, "roles and responsibilities" are important decisions that also relate to accountability as an organization. It is therefore common to describe them in higher-level regulations at the policy level, such as the "information security policy". The related JIS standard "JIS Q 27001" also states that roles and responsibilities should be described in the relevant document.

It is important to remember that the documentation itself is simply a means to an end and not the ultimate goal. It is important to disseminate and communicate the documented content so that recognition is shared throughout the company.

■ **Achievement Criteria**

② **What aspects should be considered when establishing a "list of contact persons"?**

The two important aspects when establishing a list of contact persons are ensuring that the necessary contact information is covered and confirming that security promotion activities function in practice.

<Covering the necessary contact information>

In order to register the necessary contact information for normal situations without any omissions, it is recommended to check based on the following points.

・ There is a clear point of contact for receiving inquiries regarding information security rules, etc., from within the company

・ Routes for communicating internal information and requests from the information security department are established for each objective and scope

・ Contact information for information security officers and system administrators are clarified

In addition, it is advisable to ensure the appropriate contact methods (email, chat, telephone, etc.) are secured in accordance with the use cases that can be assumed for each contact.

<Confirming functionality>

It is important to not only create a list of contact persons, but to make sure it actually functions and to ensure that functionality is maintained.

Therefore, it is advisable to have operating rules such as confirming whether an individual can actually be contacted using the methods listed and regularly updating the list to ensure it remains up to date. By having a shared awareness of the list of contact persons and each contact, cooperation when contacting someone can be made more efficient.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
4 System (Normal)	Clarify systems and roles for information security and thoroughly enact and reinforce measures for cybersecurity and protecting against data leakage	A system for managing information security risks for use in normal situations shall be constructed to enable the collection and sharing of information without incident	14	Lv2	The system, roles and responsibilities (incl. information security officers) during normal situations are clarified	[Rule(s)] ・Understanding that information security risks have a significant impact on management, a system shall be established that enables systematic management decisions

[Explanation]

■ **Achievement Criteria**

① **Is it necessary to appoint information security officers or an executive as a member of a promotion committee in order to establish a "system that enables systematic management decisions"?**

They do not necessarily need to be an officer. The important point is to appoint a person with authority. As such, the question becomes "what type of authority does the person have?" In many companies, decision-making authority tends to be at the executive level. However, depending on the scale of the organization or business, there are cases where those at the level of department manager are appointed. The latter tends to be particularly strong when it is possible to submit matters for deliberation to higher-level meetings (management meetings, Board of Directors meetings, etc.) (as decisions are ultimately made by the higher-level meeting body).

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
4 System (Normal)	Clarify systems and roles for information security and thoroughly enact and reinforce measures for cybersecurity and protecting against data leakage	A system for managing information security risks for use in normal situations shall be constructed to enable the collection and sharing of information without incident	16	Lv1	<mark>New methods of cyberattacks or leaking information</mark> are detected and corresponding security measures are shared with departments in the company	[Rule(s)] ・In accordance with the system for normal situation, examples of information security incidents/accidents and corresponding security measures shall be shared with departments in the company [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) [Frequency] ・Once per year, or when a serious information security event/incident occurs either inside or outside the company

[Explanation]

■ **Condition(s) for Achievement**

① **What is the typical approach to detecting "new methods?"**
Understanding the methods of cyberattacks, sharing this knowledge with relevant departments within the company, and implementing countermeasures are essential for improving information security. To learn about specific attack methods, it is recommended to refer to the "Information Security Measure Guidelines for Small and Medium-sized Enterprises" (IPA). Examples of these methods include "10 Major Security Threats" (IPA) and "Early Warning Information" (JPCERT/CC). Additionally, it is useful to review reports published by security vendors and seek advice from vendors with whom the company has ongoing business relationships.

* In the "Information Security Measure Guidelines for Small and Medium-sized Enterprises" (IPA), the subsection "(1) Gathering and sharing of information" under "5. Measures to Strengthen Information Security" lists the sources that can be used to collect information for detecting attack methods as reference information.
Reference: Information Security Measure Guidelines for Small and Medium-sized Enterprises, Version 3.1 (IPA)
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

* The "10 Major Security Threats" (IPA) is a publication that lists 10 types of threats extracted from information security incidents that significantly impact society each year.
https://www.ipa.go.jp/security/10threats/index.html

* "Early Warning Information" (JPCERT/CC) provides threat information that may have a serious impact on important information infrastructure.
https://www.jpcert.or.jp/wwinfo/wwdata.html

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
4 System (Normal)	Clarify systems and roles for information security and thoroughly enact and reinforce measures for cybersecurity and protecting against data leakage	A system for managing information security risks for use in normal situations shall be constructed to enable the collection and sharing of information without incident	17	Lv2	A ==system is in place for monitoring and analyzing cyberattacks and signs==	[Rule(s)] ・Build a system that will utilize public and non-public information regarding cyberattacks and vulnerabilities ・Allow for detection of cyberattacks and signs using correlation analysis, and build a system that can derive the appropriate responses from analysis results *Correlation analysis: 　A method for finding signs and traces of information security incidents/accidents by ==analyzing complex logs, etc.==

[Explanation]

■　**Condition(s) for Achievement**

①　**What are "signs" of cyberattacks?**

Here, "signs" refer to events that remind us that a cyberattack could occur in the future. Examples include suspicious posts on social media or communications confirming communication from a destination that is not normally accessed.

②　**What kind of organization does a "system for monitoring and analyzing cyberattacks and signs" refer to?**

Generally speaking, this refers to security organizations such as a Security Operation Center (SOC), which detects and identifies cyberattacks, or a Computer Security Incident Response Team (CSIRT), which handles incident response. For these organizations, either the company establishes a system itself, or they utilize contractors. One point to note is that in the latter case, it is important to consider the use of external services that provide specialized systems and functions, as well as how they all fit together, developing a system that can be introduced taking the company's situation into consideration.

*The IPA's Cybersecurity Help Team is one such service for achieving this item.

Reference: https://www.ipa.go.jp/security/otasuketai-pr/

■ **Achievement Criteria**

③ **What exactly is meant by "analyze complex logs, etc."?**

This refers to collecting logs from various network security devices and analyzing them cross-sectionally based on keys such as access destination IP addresses and time information. SIEM (System Information and Event Management) products and services are those that detect and give notification regarding suspicious behavior in real time based on those analysis results. SIEM introduction methods are described in the explanation for No. 145.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
5 System (adverse situations)	Clarify systems and roles for information security and minimize damage in the event of an incident/ accident to enable recovery to normal operations as quickly as possible	A system for responding to information security incidents/accidents and its corresponding officers shall be clarified	18	Lv1	A system for responding to information security incidents/accidents and its corresponding <mark>roles and responsibilities</mark> is clarified	[Rule(s)] ・The roles and responsibilities of the executive that presides over information security (CISO, etc.) and those of the department in charge of information security shall be clarified ・Criteria for information security incidents/accidents shall be clarified, as shall <mark>contact persons inside/outside the company and contact routes thereof</mark>

[Explanation]

■ **Condition(s) for Achievement**

① **If the procedures for responding to information security incidents/accidents have been created, is it possible to say that the "roles and responsibilities" have been clarified?**

Only creating response procedures is not enough. Response procedures are documentation that clarify what the criteria is, who should respond, and how they should respond from the viewpoint of on-site operations. However, since "roles and responsibilities" are important decisions that also relate to accountability as an organization, it is advisable to stipulate this information in a policy-level document such as the "information security policy", which is a set of rules higher than the response procedures.

■ **Achievement Criteria**

② **What are the important aspects for clarifying "contact persons inside/outside the company and contact routes thereof"?**

It is important to be able to contact the necessary members at the necessary times in the event of an emergency. Therefore, it is good to confirm that not only is the necessary contact information covered, but also that it works and is up to date.

<Covering the necessary contact information>

The following three points should be confirmed in order to clarify the necessary contact information for emergency situations without any omissions.

・　There is a clear point of contact for receiving reports of security incidents from both inside and outside the company

・　Communication routes within the information security organization have been established

・　There is a list of contacts for external organizations in the event of an information security accident

Regarding the contact information of external organizations, it is of course important to clarify the contact information for related business partners, but it is also particularly important to ask for cooperation from specialized external organizations (JPCERRT/CC, security companies, etc.). Furthermore, in organizations that have clarified the procedures to take in order to respond to security incidents/accidents, it is advisable to confirm that the contact information listed in the procedure is covered.

In addition, it is advisable to ensure the appropriate contact methods (email, chat, telephone, etc.) are secured in accordance with the use cases that can be assumed for each contact.

<Confirming functionality>

It is important to not only create a list of contact persons, but to make sure it actually functions and to ensure that functionality is maintained.

Therefore, it is advisable to have operating rules such as confirming whether an individual can actually be contacted using the methods listed and regularly updating the list to ensure it remains up to date. By having a shared awareness of the list of contact persons and each contact, cooperation when contacting someone can be made more efficient.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
6 Proced ures in adverse situatio ns	Clarify systems and roles for information security and minimize damage in the event of an incident/ accident to enable recovery to normal operations as quickly as possible	Positioning information security incidents/accid ents in the company's business continuity plan or emergency response plan	21	Lv3	A ==business continuity plan== or ==emergency response plan== is created for the company that includes information security incidents/accidents	[Standards] ・Devise a countermeasure plan based on the response history for security incidents/accidents and ==risk assessment== results ・It shall be confirmed that the measures are implemented in accordance with the countermeasure plan [Details of the countermeasure plan] -Descriptions of measures (what kinds of measures should be taken for what events) -Schedule (start and end times and the period required for each process of the countermeasure) [Countermeasure progress confirmation] -Once or more per year

[Explanation]

■ **Condition(s) for Achievement**

① **What do the terms "business continuity plan" and "emergency response plan" refer to?**

The purpose of a business continuity plan is to continue business from a management and business perspective, or detail plans for recovery with that purpose in mind, and includes a longer-term perspective. Generally referred to as a BCP, the term refers to plans for companies to continue or quickly restore core operations while minimizing damage in the event of an emergency.

1. Definitions of emergencies that would affect business continuity

2. Approaches for analyzing the above as risks

3. An overview of systems, criteria, and procedures in the event that a risk actually materializes

4. Schedules, etc., for implementing the series of measures

Emergency action plans, on the other hand, focus on activities from a short-term perspective in order to quickly recover from system/business failures and issues. 1 to 4 above are summarized with a focus on the system/business. Generally referred to as an EAP, the term refers to documented strategic plans for coordinating the roles of stakeholders to ensure prompt and optimal action aimed at temporarily restoring IT services in the event of an emergency or system disruption. Temporary

measures include relocating IT systems and operations to a separate site, restoring IT functionality through the use of alternate equipment, manually performing IT functions, etc.

■ **Achievement Criteria**

② **When creating business continuity/emergency action plans, is it necessary to have information security as the top priority in the "risk assessment"?**

Information security does not necessarily need to be the top priority.

Information security-related risks should be treated in the same way as natural disasters, fires, etc., evaluating and prioritizing their impact on business continuity.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
6 Procedures in adverse situations	Clarify systems and roles for information security and minimize damage in the event of an incident/accident to enable recovery to normal operations as quickly as possible	Procedures for addressing information security incidents/accidents at an early stage shall be clarified	23	Lv2	The scope of information security incidents/accidents is clarified and communicated throughout the company	[Rule(s)] ・The following scopes shall be clarified [Details for clarification] -Events treated as accidents/incidents -Accident/incident levels [Applies to] ・Communicating to executives, employees, temporary employees, and seconded employees

[Explanation]

■ **Condition(s) for Achievement**

① **How should the "scope of information security incidents/accidents" be clarified and communicated?**

If the scope is described in regulations such as an incident response manual that includes initial response procedures, it should be sufficient.

Note that since this includes communicating the information as achievement criteria, it is necessary to clarify the scope of information security incidents/accidents, distributing materials and carrying out training.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
6 Procedures in adverse situations	Clarify systems and roles for information security and minimize damage in the event of an incident/ accident to enable recovery to normal operations as quickly as possible	Positioning information security incidents/accidents in the company's business continuity plan or emergency response plan	24	Lv1	<mark>Procedures (initial procedures, system recovery procedures, etc.) for responding to information security incidents/accidents</mark> are defined	[Rule(s)] ・If necessary, the organization shall include the following response procedures (1) Procedures for reporting discovery of incidents/accidents, (2) Initial procedures, (3) Investigation/response procedures, (4) Recovery procedures, (5) Final reporting procedures

[Explanation]

■ **Condition(s) for Achievement**

① **What kind of content should be included in the "procedures for responding to information security incidents/accidents"?**

Content such as the following should be included as necessary as response measures to be taken in the event of an information security incident/accident (including cyberattacks such as malware infection). (Examples below)

・ Establishing a point of contact for reporting incidents and informing employees of its existence

・ Determining criteria for judging how much information should be shared regarding the details of an incident that has occurred

・ Recording incidents experienced in the past so that they can be referenced when a similar incident occurs

・ Including procedures for determining who to notify, to what extent, and by what means

・ Defining control measures and decision makers

・ Including post-recovery monitoring instructions

・ Stating what recurrence prevention measures will be taken

*"Internal CSIRT Creation Reference Material: Creating an Incident Response Manual" (JPCERT CC, 2015) serves as reference material for what should be included.

Reference: https://www.jpcert.or.jp/csirt_material/files/18_incident_response_manual_20151126.pdf

② **Are there any reference materials for learning specific methods to "respond to information security incidents/accidents"?**

Refer to the "Computer Security Incident Handling Guide" (IPA, 2008), which is a set of guidelines for handling procedures when an information security incident occurs.

Reference: https://www.ipa.go.jp/files/000025341.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
6 Procedures in adverse situations	Clarify systems and roles for information security and minimize damage in the event of an incident/ accident to enable recovery to normal operations as quickly as possible	Procedures for addressing information security incidents/accidents at an early stage shall be clarified	26	Lv1	<mark>Procedures for responding to malware infections</mark> are defined	[Rule(s)] ・If necessary, the organization shall include the following procedures in responding to malware infections (1) Procedures for reporting discovery of incidents/accidents, (2) Initial procedures, (3) Investigation/response procedures, (4) Recovery procedures, (5) Final reporting procedures

[Explanation]

■ **Condition(s) for Achievement**

① **Are there any reference materials for learning specific methods to "respond to malware infections"?**

The various types of malwares are becoming more sophisticated and complex with each passing day. As such, the most effective method for staying on top of the latest procedures is to search for and read reports and articles published by each security vendor. However, as far as malware types and definitions and orthodox countermeasures are known, the "Guide to Malware Incident Prevention and Handling for Desktops and Laptops" (IPA, 2008) can serve as a reference.

Reference: https://www.ipa.go.jp/files/000025349.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
7 Daily education	Have employees understand the risks surrounding malware and confidential information, as well as the correct handling methods thereof, in order to prevent information security incidents/accidents	Employees shall be educated to be aware of risks	28	Lv1	In-house <mark>education</mark> is provided regarding malware infections via email	[Rule(s)] ・Education on preventing malware via email shall be provided by distributing/posting educational materials, e-Learning, or group education, etc. ・Review the content of training and improve the content of the next training [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) who use email [Frequency] ・Whenever a new employee joins the company and once or more per year

[Explanation]

■ **Condition(s) for Achievement**

① **What should be included in "education"?**

The items to be included will differ depending on the target audience/objective, but it is necessary to provide training separately depending on if the target audience are system administrators (IT personnel), including for email systems, or if they are general employees who use email. When conducting education for the purpose of "improving understanding", it is advisable to provide explanations centered around recent world trends and company regulations. However, when conducting education for the purpose of "raising awareness", it is advisable to specifically introduce examples of "things that employees need to watch out for" or "things employees shouldn't do" by interweaving examples from other companies. Both this item and No. 29 require education regarding malware infection, but while this item assumes malware infection from email, No. 29 assumes infection from online browsing. Depending on that context, the explanations and preventative measures that need to be taken will differ. As such, it is advisable to provide education that assumes each infection route.

② **Should the impact of education be confirmed?**

This item does not require implementation to that extent. Implementation is the achievement criteria, which does not include confirming the impact from each participant's point of view.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
7 Daily education	Have employees understand the risks surrounding malware and confidential information, as well as the correct handling methods thereof, in order to prevent information security incidents/accidents	Employees shall be educated to be aware of risks	29	Lv1	In-house education is provided regarding internet connections	[Rule(s)] ・Education on preventing malware during online browsing shall be provided by distributing/posting educational materials, e-Learning, or group education, etc. ・Review the content of training and improve the content of the next training [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) who use the internet [Frequency] ・Whenever a new employee joins the company and once or more per year

[Explanation]

■ **Condition(s) for Achievement**

① **What should be included in "education"?**

The items to be included will differ depending on the target audience/objective, but it is necessary to provide training separately depending on if the target audience are system administrators (IT personnel), including for email systems, or if they are general employees who use email. When conducting education for the purpose of "improving understanding", it is advisable to provide explanations centered around recent world trends and company regulations. However, when conducting education for the purpose of "raising awareness", it is advisable to specifically introduce examples of "things that employees need to watch out for" or "things employees shouldn't do" by interweaving examples from other companies. Both this item and No. 28 require education regarding malware infection, but while this item assumes malware infection from online browsing, No. 28 assumes infection from email. Depending on that context, the explanations and preventative measures that need to be taken will differ. As such, it is advisable to provide education that assumes each infection route.

② **Should the impact of education be confirmed?**

Similar to No. 28, this item does not require implementation to that extent. Implementation is the achievement criteria, which does not include confirming the impact from each participant's point of view.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
7 Daily education	Have employees understand the risks surrounding malware and confidential information, as well as the correct handling methods thereof, in order to prevent information security incidents/accidents	Employees shall be educated to be aware of risks	31	Lv2	Training on targeted emails is being implemented	[Rule(s)] ・Training on targeted emails shall be implemented ・Include in the training content what to do if an email is opened ・Review the methods and content of training and improve the content of the next training [Applies to] ・Those who use email [Frequency] ・Once or more per year

[Explanation]

■ **Achievement Criteria**

① **What should be done for "targeted email training"?**

Hands-on training is required. More specifically, it is common to mass distribute dummy emails that imitate the company's business to employees at the same time and check whether they click the links in the email. This is an effective method for enlightening employees, reminding them not to carelessly respond to emails containing suspicious file links, even if the subject or text is related to their own work.

*The "Email Training Guidebook" (Nippon CSIRT, 2022) can be used as a guide for all stages of email training from planning to improvement.

Reference: https://www.nca.gr.jp/activity/imgs/nca-mail-exercise-guidebook-v1.0.pdf

② **If training is carried out on a company-wide level at the same time, the IT department could be overwhelmed by inquiries. Are there standards for how training should be conducted?**

There are no official standards. It is important to conduct the training in accordance with the organization and in a way that does not hinder business operations. Note that it is more important to clarify the objective and adopt a suitable method rather than doing it all at once (e.g. improving proficiency level, clarifying issues, motivation, etc.).

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
7 Daily education	Make advanced preparations for prompt and appropriate responses aimed at preventing further damage to enable prompt recovery when an information security incident/accident occurs	Education/training on information security incidents/accidents that have an impact within or across organizations, and methods of minimizing their impact, shall be provided	38	Lv1	Education/training for responding to information security incidents/accidents is provided	[Rule(s)] ・Education and training on responding to information security incidents/accidents shall be provided by distributing/posting educational materials, e-Learning, or group education, etc. [Applies to] ・Executives, employees, outside employees (temporary employees, etc.) [Frequency] ・Whenever a new employee joins the company and once or more per year

[Explanation]

■ **Achievement Criteria**

① **How can "education and training" be provided in an effective manner?**

By improving your understanding of internal response procedures through education and enhancing your ability to respond to information security incidents and accidents through training, you will be better equipped to respond quickly and appropriately to such incidents. To provide effective education and training, it is essential to customize the content for each individual, as their job roles and responsibilities may vary. For general employees, it is crucial to educate and train them on company rules regarding the handling of sensitive information and IT equipment/devices. On the other hand, for information security personnel, it may be possible to provide education and training on response procedures outlined in Requirement No. 24, among other examples. (Examples below)

<For general employees>
 - Education on company rules regarding handling of information and IT equipment/devices (e.g. education on company rules through e-learning)
 - Training on handling information and IT equipment/devices (e.g. training on how to report when receiving targeted emails and how to respond to malware infections)

<For information security personnel>

- Education on the incident response (e.g. education on the organizational CSIRT (Computer Security Incident Response Team) structure and response procedures)
  - Training on the incident response (e.g., response training for reporting findings, initial response, system recovery, and other necessary actions when an incident occurs)

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
7 Daily education	Make advanced preparations for prompt and appropriate responses aimed at preventing further damage to enable prompt recovery when an information security incident/accident occurs	Education/training on information security incidents/accidents that have an impact within or across organizations, and methods of minimizing their impact, shall be provided	39	Lv3	Education/training for responding to <mark>information security incidents/accidents across organizations</mark> is provided	[Rule(s)] ・Education and training on responding to information security incidents/accidents across organizations shall be provided by distributing/posting educational materials, e-Learning, or group education, etc. [Applies to] ・Security-related departments [Frequency] ・Once or more per year

[Explanation]

■ **Condition(s) for Achievement**

① **What exactly is meant by "information security incidents/accidents across organizations"?**

As written, it is assumed that multiple organizations are involved, but there are several patterns that can be assumed, and the following cases can apply. (Examples below)

<Occurs in an external organization => Spreads to your company>

・ A business partner was the target of a cyberattack and has been infected with malware. Through that, unauthorized access into your own company's network occurred.

<Occurs in your company => Spreads to an external organization>

・ Your organization's servers were accessed maliciously, and those servers were used as a stepping stone to attack business partners.

44

Note that "across organizations" in this item can refer not only to across companies as described above, but also across divisions of one's own company.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
8 Information security requirements between companies	Prevent the leakage of confidential information in the supply chain and enable prompt response to accidents	Information security requirements for the supply chain shall be clarified	41	Lv3	The flow of goods and data is shared with suppliers	[Rule(s)] ・Must be able to identify important suppliers ・Must be able to identify the flow of goods and data ・An overview of transactions shall be illustrated and shared with the supplier [Applies to] ・Suppliers with which business occurs

[Explanation]

■ **Condition(s) for Achievement**

① **What exactly is meant by the "flow of goods and data"?**

In this case, goods refer to products and the parts, materials, etc., that tie into the production and manufacture of those products. Data refers to information that ties into the manufacturing and production of products such as design drawings, as well as order information, customer information, and electronic information related to those things. Flow refers to the process flow for the execution of business, though the important point here is the "supply chain" perspective. In other words, it is important to focus on how inter-organizational collaboration occurs as opposed to how business processes within your own organization progress and how goods and data are related within those. Confirmation of the sharing status based on this is what is required.

② **Is it necessary to create data flow diagrams to understand the "flow of goods and data"?**

Creating data flow diagrams is not necessary, as it is sufficient if the flow of goods and data can be specified as they are in the achievement criteria.

With this, you should be able to grasp the following three points.

・ An overview of business relationships, such as where orders from your organization go, your organization, and where orders to your organization come from

・ An overview of the relevant supply chains and an understanding of the roles they play in your overall organization

- The impact on direct business partners and the supply chain as a whole in the event of a security incident that negatively affects business

■ **Achievement Criteria**

② **How do you determine who an "important supplier" is?**

There are a wide range of various suppliers, so it is virtually impossible to cover all of them. Realistically, it is necessary to weigh them and increase the intensity of management the more important a supplier is. The scale of "importance" here will differ from company to company, but it is important to clarify that scale according to each situation taking into account the management situation for each company. (Examples below)

- Does a supplier handle the company's highly confidential technical information?

- Would disruption to the supplier's operations cause fatal delays in the company's own development and production?

- Have there recently been leaks, etc., caused by the supplier? Are there concerns about a risk of recurrence?

④ **Is it acceptable to only cover important suppliers?**

All suppliers with whom you do business are covered by the achievement criteria. In addition to that, it is necessary to identify important suppliers. The important thing is to have an understanding of the overall picture and to be able to identify the proper areas to focus on.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
8 Information security requirements between companies	Prevent the leakage of confidential information in the supply chain and enable prompt response to accidents	Information security requirements for the supply chain shall be clarified	42	Lv3	Have a grasp of the status of security measures of ==business partners== that handle important confidential information	[Rule(s)] Grasp the state of countermeasures of business partners by referring to the following examples: ・Create a checklist and receive answers from business partners ・Visit business partners and carry out inspections [Target companies] ・Subsidiaries, suppliers, etc., that provide and share important confidential information of the company 　Example: Companies that share "top secret" confidential information [Frequency] 　・Once or more per year

[Explanation]

■ **Condition(s) for Achievement**

① **What exactly is meant by "business partners"?**

This refers to subsidiaries, suppliers, etc., that provide and share important confidential information of the company as specified in the achievement criteria.

Sometimes it can be difficult to confirm security implementation status for information classified as confidential from business partners.
In such cases, it is advisable to enter into a confidentiality agreement. If that is difficult, consider the various regulations regarding the handling of information for both parties, the sensitivity and importance of the data to be handled, the depth of the security measures, etc., and after consultation, come to an agreement regarding the extent of information that can be presented and whether it contributes to understanding the status of security measures.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
8 Information security requirements between companies	Prevent the leakage of confidential information in the supply chain and enable prompt response to accidents	Information security requirements for the supply chain shall be clarified	43	Lv3	Confidential information, access rights, etc., are collected or disposed of at the end of a contract	[Rule(s)] ・A checklist for confidential information, access rights, etc. to be collected shall be created ・Use the checklist at the end of a contract to collect confidential information, access rights, etc. ・Confirm that collection or disposal has been carried out without omission, and make corrections as necessary [Target companies] ・Subsidiaries, suppliers, etc. that provide and share confidential information [Frequency] ・Once or more per year

[Explanation]

■ **Achievement Criteria**

① **Though "a checklist shall be created" and "a checklist shall be used" are stated, how can you create and use a checklist effectively?**

When sharing or providing confidential information or access rights, it is important to create a checklist that includes all the necessary information to be collected or destroyed. This can be done by managing the information in a ledger in advance. The following details should be recorded in the ledger. (Examples below)

・ Contents of confidential information and access rights
・ Date and time of provision/sharing
・ Method of provision/sharing (such as storage medium or email)
・ Recipient of information (such as company, department, or individual in charge).

Moreover, presenting the checklist only at the end of the contract may make it difficult to recognize the items that need to be collected or destroyed, making information collection or destruction more difficult. To avoid this, it is helpful to use ledgers, checklists, and other tools during the contract period to make sure the recipient or sharer is aware of the information that needs to be collected or destroyed. Additionally, subcontractors must sign a non-disclosure agreement to collect and destroy information. Please refer to Requirement No. 44 for further guidance.

*In the "Handbook for Protecting Confidential Information," there is a subsection titled "3-4 Specific Examples of Measures to Prevent Information Leakage, (3) Measures for Business Partners," which points to keep in mind when disclosing confidential information to business partners. This section can serve as a useful reference.

Reference: Handbook for Protecting Confidential Information (Ministry of Economy, Trade and Industry)

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
8 Information security requirements between companies	Prevent the leakage of confidential information in the supply chain and enable prompt response to accidents	Information security requirements for the supply chain shall be clarified	44	Lv1	Methods of handling confidential information between companies are clarified	[Rule(s)] ・Methods of handling confidential information shall be exchanged before starting business [Applies to] ・Companies that share confidential information

[Explanation]

■ **Condition(s) for Achievement**

① **Should "other companies" include all partner companies, business partners, suppliers, etc.?**

The objective is to prevent the leakage of confidential information from parties outside your company. Therefore, all companies that share your company's confidential information are applicable.

■ **Achievement Criteria**

② **Though "methods of handling confidential information shall be exchanged" is stated, what should be exchanged?**

The method for handling confidential information is typically the exchange of a non-disclosure agreement. For detailed examples of clauses related to confidentiality, please refer to Reference Material 2, "Reference Examples of Various Contracts, etc." in the "Handbook for Protecting Confidential Information" published by the Ministry of Economy, Trade and Industry. We recommend consulting with your company's legal department for further guidance. A non-disclosure agreement may include the following details: (Examples below)

・ Contents of confidential information

- Procedure for handling confidential information (e.g., designating a person responsible for information handling, strictly storing and managing the information, and prohibiting the use for other purposes or providing it to third parties)
- Obligation to return confidential information (e.g., whether collection or destruction is necessary, and if data is to be deleted, a written report must be submitted.)

* The "Handbook for Protecting Confidential Information" provides an example of a non-disclosure agreement in "item No. 4" of Reference Material 2, "Reference Examples of Various Contracts, etc." in the section "3-4 Specific Examples of Measures to Prevent Information Leakage."
Reference: Handbook for Protecting Confidential Information (Ministry of Economy, Trade and Industry)
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

Reference: Reference Material 2, Reference Examples of Various Contracts, etc. (Ministry of Economy, Trade and Industry)
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
8 Information security requirements between companies	Prevent the leakage of confidential information in the supply chain and enable prompt response to accidents	Information security requirements for the supply chain shall be clarified	46	Lv1	Roles and responsibilities when an information security incident/accident occurs are clarified with other companies	[Rule(s)] ・When sharing confidential information, the <mark>roles and responsibilities of each company when an information security incident/accident occurs shall be documented</mark>

[Explanation]

■ **Achievement Criteria**

① **Though "the roles and responsibilities of each company when an information security incident/accident occurs shall be documented" is stated, what kind of contents should be documented?**

Incidents or accidents related to information security in the supply chain can happen within your company or at other companies, such as subcontractors. In either case, if there is an information leak, it is crucial that the company where the leak occurred reports the incident immediately to minimize the damage and scope of impact. Therefore, it is necessary to establish clear contact information between your company and business partners to facilitate swift communication in the event of an information leak. For key points on how to clarify contact information, please refer to the explanation ② of Requirement No. 18.

Moreover, it is important to ensure that contract documents, such as outsourcing contracts, state the obligation to notify in case of an information leak. The documents should also specify that your company will be allowed to participate in discussions about measures to prevent recurrence.

* The "Handbook for Protecting Confidential Information" provides an example of a business outsourcing contract with useful description examples of roles and responsibilities in case of an accident in "Item No. 6" of Reference Material 2, "Reference Examples of Various Contracts, etc." in the section "3-4 Specific Examples of Measures to Prevent Information Leakage."

Reference: Handbook for Protecting Confidential Information (Ministry of Economy, Trade and Industry)

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

Reference: Reference Material 2, Reference Examples of Various Contracts, etc. (Ministry of Economy, Trade and Industry)

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/reference2.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
8 Information security requirements between companies	Prevent the leakage of confidential information in the supply chain and enable prompt response to accidents	Information security requirements for the supply chain shall be clarified	48	Lv3	Understand how ==important confidential information== obtained from other companies is handled within the company	[Rule(s)] ・The ==history of handling other company's important confidential information in-house shall be recorded and stored== ・Confirm that recording and storage is done appropriately, and make corrections as necessary [Frequency of recording, checking storage status, correcting] ・Once or more per year

[Explanation]

■ Condition(s) for Achievement

  ① **What specifically can be considered as "important confidential information?"**

Determining the level of importance of confidential information based on the potential impact on business is essential. For instance, if confidential information were leaked, it could result in a decline in social trust and legal action such as compensation for damages. The section, "(2) Evaluation of Retained Information" in the "Handbook for Protecting Confidential Information" published by the Ministry of Economy, Trade and Industry provides guidance on evaluating information from different viewpoints and can be used as a reference.

■ Achievement Criteria

  ② **Though "history of handling other company's important confidential information in-house shall be recorded and stored" is stated, what are the possible methods?**

Important confidential information received from other companies must be handled in accordance with contracts such as non-disclosure agreements. The specific recording method requires managing the received confidential information in a ledger, which includes the following details: (Examples below)

    • The confidential information received

- Date and time of receipt
- Method of receipt (e.g. email, post)
- Storage location (e.g. building, room, server, cabinet)
- Custodian (e.g. company, department, person in charge)

Storing confidential information in a place that all general employees can access makes it difficult to prove that confidential information has not been leaked if any lawsuits are received from other companies regarding the leakage of such information. Therefore, as a preventive measure against potential lawsuits, storing confidential information separately from other company information is recommended. Also, non-disclosure agreements require confidential information to be collected and destroyed when it is no longer needed due to the contract's expiration. Therefore, it is advisable to store confidential information separately as well. Specifically, confidential information must be stored in a secure location separate from the company's information. Access rights to confidential information should be managed with proper locking mechanisms in place. Additionally, records of access and lending should be thoroughly maintained for any confidential information taken out or referenced.

* Section "(2) Evaluation of Retained Information" in the "Handbook for Protecting Confidential Information" provides viewpoints for evaluating the importance of your company's information and that of other companies that can serve as a reference. Furthermore, sections "3-4 Specific Examples of Measures to Prevent Information Leakage" and "5-2 Preventing Unintentional Infringement of the Confidential Information of Other Companies" provide useful information on the measures to prevent information leakage and precautions for handling confidential information of other companies.
Reference: Handbook for Protecting Confidential Information (Ministry of Economy, Trade and Industry)
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
9 Access rights	Prevent unauthorized access to confidential areas or systems due to inadequacies in access right settings	Access rights (room and system access rights) shall be managed appropriately	49	Lv1	Rules for managing access rights (room and system access rights) in the event of personnel transfers are defined	[Rule(s)] ・ Management rights shall be defined to include the following: ・ An application/approval system shall be used for issuing, changing, and revoking access rights ・ Granted room entry permissions and access rights shall be limited to the scope necessary ・ Methods of taking inventory for room entry rights and access rights shall be defined ・ Applications and ledgers for granted room entry permissions and access rights shall be managed [Applies to] ・ Systems used for business operations and user IDs for logging onto computers ・ Locations or rooms in which considerations for confidentiality are required

[Explanation]

■ Achievement Criteria

① **What are the important considerations when defining "management rules" for access rights in the event of personnel transfers?**

Among personal transfers, attention must be paid with regard to retired employees, temporary employees, and subcontractors in particular. There have been instances where these individuals have leaked confidential information due to their continued access to rooms or systems even after their employment has ended. To prevent this from happening, it is essential to immediately revoke access rights for retired employees, temporary employees, and subcontractors as soon as their work has come to an end.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
9 Access rights	Prevent unauthorized access to confidential areas or systems due to inadequacies in access right settings	Access rights (room and system access rights) shall be managed appropriately	50	Lv2	Rules for managing access rights (room and system access rights) in the event of personnel transfers are defined	[Rule(s)] ・For systems handling <mark>important information</mark>, clarify the conditions for <mark>granting access rights</mark> ・Setting of access rights should be carried out under strict management by clarifying the requirements and settings for the system administrator. ・Systems handling important information should have an environment in which authority is not concentrated on individuals, such as by separating the authority of those using information and system administrators. ・Monitor the operation/usage state for systems handling important information.

[Explanation]

■ **Achievement Criteria**

① **What are the specific conditions for determining whether or not to "grant access rights"?**

The condition is whether they have the authority to perform the task. The viewpoints for determining this are as follows. (Examples below)

・ The department they belong to

・ Their position

・ Their role within the department (e.g. confidentiality manager)

② **What exactly is meant by "important information"?**

This will differ depending on the organization. Generally speaking, in most cases important information is clearly defined in regulations related to confidentiality management, and it is important to comply with such regulations. There is also a general tendency to treat the following as "important information". (Examples below)

・ Personal information (customers, employees, business partners, etc.)

- Management information (financial, strategic, personnel-related, etc.)
- Trade secret information (research, design, development, etc.)

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
9 Access rights	Prevent unauthorized access to confidential areas or systems due to inadequacies in access right settings	Access rights (room and system access rights) shall be managed appropriately	51	Lv1	Access rights are issued, changed, disabled, or revoked in accordance with management rules	[Rule(s)] ・<mark>Inspections of the compliance status of the management rules</mark> defined in No. 49 shall be performed

[Explanation]

■ **Achievement Criteria**

① **What exactly is performed in the "inspections of the compliance status of the management rules?"**

Inspecting the compliance status of management rules means to confirm that management rules are being operated appropriately. Periodic inspections not only help identify and correct any violations but also raises awareness among employees about compliance with management rules. A specific method to inspect compliance is to check whether any access rights have been issued, changed, disabled, or revoked without being recorded in the application form or ledger for entry permission/access rights. For example, you could compare and confirm the history of access rights issued, changed, disabled, or revoked on the system with the records in application forms and ledgers. If it is difficult to confirm the entire history, conducting sampling checks can help suppress any violations of management rules.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
11 Management of information assets (equipment/ devices)	Appropriately manage IT assets to reduce the risks associated with information security incidents/accidents and shorten response times when an information security accident occurs	IT equipment/devices owned by the company and information (version information, administrator, administrating department, location installed, etc.) on the OS and software used by the equipment/device shall be managed appropriately	59	Lv1	Management rules for IT equipment/devices, OS, and software are defined based on ==importance==	[Rule(s)] ・==Management rules== shall be defined that include equipment/device adoption, installation, network connections, application of security patches, etc.

[Explanation]

■ Condition(s) for Achievement

① **How can the "importance" of information assets be decided?**

The importance of information assets is determined based on the degree of impact on the business in case the asset is compromised. For example, if the information handled by that IT asset is compromised, will the impact be limited to the company itself, or will it also affect business partners such as direct customers and suppliers?

■ Achievement Criteria

② **What factors should be considered while defining "management rules" for information assets?**

To define effective management rules, it is recommended to consider the following points:

• Both hardware and software assets should be included in the rules.

• Procedures and mechanisms for keeping IT asset information up to date should be defined. (Ex. rules for applying security patches to servers and standard OS should be established).

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
11 Management of information assets (equipment/devices)	Appropriately manage IT assets to reduce the risks associated with information security incidents/accidents and shorten response times when an information security accident occurs	IT equipment/devices owned by the company and information (version information, administrator, administrating department, location installed, etc.) on the OS and software used by the equipment/device shall be managed appropriately	60	Lv1	A list is created of IT equipment/devices and information (version information, administrator, administrating department, location installed, etc.) on OS and software	[Rule(s)] ・A list of information for IT equipment/devices, OS and software shall be created that includes version information, administrators, administrating departments, locations installed, etc.

[Explanation]

■ Achievement Criteria

① **"What are the specific items managed using the "list?"**

The main objectives of managing a list are to ensure that the IT assets' information security is up to date by applying software security patches and to be able to respond quickly in case of an information security incident/accident. Only those items that serve these purposes need to be managed. Specific items managed using the list are as follows.

- Device name (hardware device, hostname)
- Software information (software name, version information)
- Network information (MAC address, IP address)
- Installation location (office/data center/cloud, etc.)
- User (department name, name, contact information)
- Administrator (department name, name, contact information)
- Support contact information (internal or external support contact person)

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
11 Management of information assets (equipment /devices)	Appropriately manage IT assets to reduce the risks associated with information security incidents/accidents and shorten response times when an information security accident occurs	IT equipment/devices owned by the company and information (version information, administrator, administrating department, location installed, etc.) on the OS and software used by the equipment/device shall be managed appropriately	61	Lv2	A list of IT equipment/devices and information (version information, administrator, administrating department, location installed, etc.) on OS and software is ==reviewed== regularly or as necessary	[Frequency] ・Once or more per year

[Explanation]

■ **Condition(s) for Achievement**

① **Does "review" mean that an inventory is taken?**

The objective of this item is to be able to quickly determine and respond to whether an old OS that is no longer supported, or a vulnerable version of software, etc., is being used. It is important to keep the current version information, administrator information, etc., up to date. Based on these points, inventory work should be carried out with the following points in mind. (Examples below)

・ Do the items on the list match the actual goods?

・ Should anything be deleted from the list due to having been destroyed, etc.?

・ Should anything be added to the list due to official purchases, etc.?

・ Is there anything that should be separated from the system such as unapproved devices and software?

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
11 Management of information assets (equipment/devices)	Appropriately manage IT assets to reduce the risks associated with information security incidents/accidents and shorten response times when an information security accident occurs	IT equipment/devices owned by the company and information (version information, administrator, administrating department, location installed, etc.) on the OS and software used by the equipment/device shall be managed appropriately	63	Lv3	Management of information assets (equipment/devices) is performed in accordance with management rules based on importance	[Rule(s)] Regularly check that <mark>devices and installed software</mark> are genuine by using serial numbers and hash values according to importance [Frequency] ・Once or more per year (when taking inventory of assets, etc.)

[Explanation]

■ **Achievement Criteria**

① **By what means is it possible to confirm that "devices and installed software" are genuine?**

The following methods can be used for IT equipment and software. (Examples below)

<IT equipment>

・ Using an asset detection tool, check whether the devices connected to the network match the IT asset management ledger.

・ Take inventory and compare the serial numbers on the actual items with those in the IT asset management ledger or delivery slips from the time of purchase.

・ Carry out identification by affixing a control sticker, etc., at the time of delivery and then confirm that the sticker is present.

<Software>

・ Using a tool, regularly check the hash value of software to confirm it is genuine.

・ Confirm that the installed software matches the content of license agreements by taking inventory or using a tool.

・ Confirm that it has been distributed in accordance with procedures based on license agreements.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
11 Management of information assets (equipment/devices)	Appropriately manage IT assets to reduce the risks associated with information security incidents/accidents and shorten response times when an information security accident occurs	IT equipment/devices owned by the company and information (version information, administrator, administrating department, location installed, etc.) on the OS and software used by the equipment/device shall be managed appropriately	64	Lv2	Unauthorized installation of applications on <mark>smart devices</mark> is restricted, and installation status is checked regularly	[Rule(s)] ・Applications that can be installed are defined, and installation status is checked regularly. [Applies to] ・Company-supplied smart devices [Frequency of check] ・Once a year

[Explanation]

■ **Condition(s) for Achievement**

① **What is meant by a "smart device"?**

Highly portable mediums that are easy to carry (excluding computers). Such devices are presumed to have communication functionality, and the term specifically refers to smartphones, tablets, and other small terminals that have network communication and information processing functionality.

② **It is possible to omit the rules for this item for objects that are not "smart devices"?**

They are not covered by this item. However, No. 98 requires software installation restrictions on PC terminals, so it is necessary to check accordingly.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
11 Management of information assets (equipment/devices)	Appropriately manage IT assets to reduce the risks associated with information security incidents/accidents and shorten response times when an information security accident occurs	IT equipment/devices owned by the company and information (version information, administrator, administrating department, location installed, etc.) on the OS and software used by the equipment/device shall be managed appropriately	65	Lv2	At the time of disposal (including at the end of a lease), the <mark>data on the storage medium is erased</mark>	[Rule(s)] ・When disposing of information assets (equipment) (including at the end of a lease), delete the data so that it cannot be restored ・Keep a record of having erased the storage area of information assets (equipment) or a vendor disposal certificate *Disc formats are not possible as data may be recovered [Applies to] -Servers, company-supplied client PCs, smart devices, external storage media

[Explanation]

■ **Condition(s) for Achievement**

① **What methods are there for "erasing data on a storage medium"?**

You can either physically destroy the storage medium or logically erase the data. The key point here is to make it so the data cannot be recovered. Regardless of which method is used, if the means or procedures used aren't appropriate (e.g. erasing data through a disk format, incomplete physical destruction due to not using the proper procedures, etc.), data may be restored. As such, it is advisable to take secure measures such as using a dedicated data erasure tool or outsourcing to a dedicated company.

Additionally, if the data stored is highly confidential and you wish to further ensure the data has been properly erased, the data can be logically erased in-house before entrusting a dedicated contractor to physically destroy it, combining multiple methods/means.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
12 Risk response	Identify information asset security risks and take organizational measures as a company to minimize impacts to operations	Measures for information security risks shall be taken within the organization (organizational operations also include outsourced operations)	66	Lv1	Risks are identified when the three elements of information assets—confidentiality, integrity, and availability—cannot be ensured	[Rule(s)] ・The impact on operations when an information security incident/accident occurs to the target information asset shall be understood in terms of scope of impact and frequency of occurrence 　[Applies to] ・Information assets identified in No. 56 [Viewpoints] ・External threats ・Company vulnerabilities *Consider threats and vulnerabilities caused by business partners as necessary ・Value of information assets [Methods] ・Determine the target information and information systems ・Establish evaluation rules for each viewpoint and risk level rules that take those into consideration 　・For each piece of information and information system, determine the risk level from the evaluation from each viewpoint [Frequency] ・When reviewing important information assets or once or more per year

[Explanation]

■ **Achievement Criteria**

① **What should be done to "understand the impact on operations when an information security incident/accident occurs in terms of scope of impact and frequency of occurrence"?**

Performing the following three processes, commonly referred to as a "risk assessment", should be sufficient.

1. Risk identification... Identify what information assets are held and what kinds of risks exist for each (external threats, company vulnerabilities).

2. Risk analysis... Investigate and analyze the characteristics, frequency of occurrence, and level of impact of each identified risk.

3. Risk evaluation... Make an assessment based on the value of the target information assets and the frequency of occurrence and level of impact for risks, and then consider risk countermeasures and priorities.

This type of risk assessment is described in JIS Q 27001, the JIS standard for security, with the purpose of selecting appropriate countermeasures against risks. No. 68 is the appropriate item for that.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
13 Understanding details of business transactions and methods	Prevent information leakages, etc., during the course of business transactions by clarifying what methods are used to exchange information assets and with what business partners	Information assets exchanged over the course of business transactions with each business partner, as well as the methods used for such transactions, shall be understood	70	Lv1	A list is created for the ==information exchanged== with each company and the ==methods used== (methods of exchanging information, such as for receiving/sending orders)	[Rule(s)] ・This list shall include information assets exchanged/used during transactions, as well as how they are handled, and mutually understood by the business partner [Applies to] ・Business partners with which important information assets (such as the highly confidential information assets defined in No. 54) are shared [Frequency] ・When starting business transactions or when changes are made to information exchanged and methods used

[Explanation]

■ **Condition(s) for Achievement**

① **Is it necessary to create a list of "information exchanged and the methods used" for all business partners?**

This is not necessarily required for all business partners. The aim is to quickly recover from the perspective of BCP in the event of a security incident, and so it is advisable to create a system that prioritizes business partners with whom important information assets are shared and those others who are at a high security risk.

② **To what extent should "information exchanged and the methods used" be listed?**

For the information exchanged, it is sufficient to clarify the category important information falls under according to the company's confidentiality management rules (e.g. highly confidential, confidential, internal-use only, general) and list those. For example, design drawing data, information regarding orders accepted/sent (accounts payable, accounts receivable, etc.), and personal information (customers, employees, business partners, etc.) can be considered targets to be listed.

For the methods of exchange, it should be sufficient to list the specific method, such as email, cloud storage, electronic data exchange between companies, or other physical media (USB, CD, DVD, etc.) together with the timing and frequency.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
13 Understanding details of business transactions and methods	Prevent information leakages, etc., during the course of business transactions by clarifying what methods are used to exchange information assets and with what business partners	Managing information security risks regarding the procurement of IT equipment	72	Lv3	<mark>Security requirements for the procurement of IT equipment</mark> are established and communicated within the organization	[Rule(s)] ・A list shall be made of the security requirements for procuring equipment ・Security requirements can be easily confirmed when procuring equipment [Applies to] [Equipment] ・IT equipment connected to the internal network [Communication] ・Executives, employees, outside employees (including temporary employees, etc.) [Frequency] ・Information shall be communicated within the organization regularly and whenever the security requirements for procuring equipment are revised

[Explanation]

■ **Condition(s) for Achievement**

① **What kind of requirements should be presented as "security requirements for the procurement of IT equipment"?**

The security requirements that need to be presented to suppliers will differ depending on the importance of the information handled by the product. However, it is not necessary to require the same level of management rules as for internal use, and so presenting what is required considering your company's environment should be sufficient. For example, client PC terminals can include the following. (Examples below)

・ Password authentication function when the power is turned on and administrator password authentication function

・ HDD lock function

・ Security lock cable and key

・ Compliant with wireless LAN standards to prevent the interception of wireless communication

・ Supports remote activation to allow security patches to be applied at night while unattended

*Security threats and the requirements for countermeasures against them are listed in the "Security Requirements List for the Procurement of IT Products" (METI, 2018), which can be used for reference.

Reference: https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
13 Understanding details of business transactions and methods	Prevent information leakages, etc., during the course of business transactions by clarifying what methods are used to exchange information assets and with what business partners	Managing information security risks regarding the procurement of IT equipment	73	Lv3	Security requirements for the procurement of IT equipment are shared with the provider, and results of the evaluation at the time of purchase are recorded and stored	[Rule(s)] ・Security requirements are clearly stated in the purchase contract, etc. ・When procuring equipment, security requirements are evaluated and the results are stored ・There are regular checks confirming the storage of check results [Applies to] 　IT equipment connected to the internal network [Frequency of checking storage status] 　Once or more per year

[Explanation]

■ **Condition(s) for Achievement**

① **Does "IT equipment" mean all IT equipment?**

Since IT equipment as a whole includes a large number of types and numbers, this item prioritizes "IT equipment connected to the internal network", as stated in the achievement criteria. Because there is a serious risk of malware infection, etc., as long as equipment is connected to the network, it is recommended to add gradation in accordance with the level of risk for each device.

■ **Achievement Criteria**

② **What exactly is meant by "evaluating security requirements"?**

Confirming that the security requirements are satisfied is sufficient. This can be done by confirming the acquisition of certification based on international standards, acceptance tests when acceptance inspections are carried out, etc.

When carrying out such evaluations, the specific examples for the various cases described in "2.(1).(b) Secure IT Product Procurement Flow -> "Guide ②" Decision Points" of the "Guidebook for the Utilization of Security Requirement Lists for the Procurement of IT Products" (IPA, 2018) will be helpful.

Reference: https://www.ipa.go.jp/files/000038924.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
14 Understanding the statuses of external connections	Ensure safety and trust when using external information systems, while enabling prompt response to information security incidents/accidents	For relations with affiliated organizations (including suppliers, etc.), understand the communication network structure for your own organization and monitor the status of cooperation with other organizations as well as the flow of data	74	Lv2	Network and data flow diagrams are created, and <mark>communication with affiliated organizations (including suppliers, etc.) are monitored</mark>	[Standard] ・<mark>Network diagrams shall be created</mark> [Scope] -Networks where the company's own IT equipment/devices exists [Frequency of review] -Once or more per year <Addition> [Standard] ・<mark>Data flow diagrams shall be created</mark> [Scope] -Data within the company exchanged over the network between affiliated organizations [Standard] ・Communication with affiliated organizations shall be monitored [Scope] -Data exchanged on the network between affiliated organizations [Frequency] -Always

[Explanation]

■ **Condition(s) for Achievement**

① **What exactly is meant by "communication with affiliated organizations is monitored"?**

Ensuring that devices that control communications (e.g. firewalls, proxy servers) and devices that detect and defend against attacks (e.g. IPS, IDS) are installed in locations where communications between the company and affiliated organizations pass through, and that a system capable of monitoring the communication logs between those devices has been constructed, should be sufficient.

Construction of such a system can be done through the building of a monitoring system in-house or by using an external service.

In the latter case, it is important to consider the use of external services that provide specialized systems and functions, as well as how they all fit together, developing a system that can be introduced taking the company's situation into consideration.

■ **Achievement Criteria**

② **Considering that it states "network diagrams shall be created" and "data flow diagrams shall be created", is it necessary to require both?**

Both are required. If there is only a flow of data, then just a data flow diagram is not a problem. However, since the level of risk will vary between communication via the internet and communication via a closed network, in addition to data flow, it is also important to understand the state of connections and the communication occurring on the network, including the "state of linkage with other organizations".

*Sections 3.2 and 3.3 of the "Control System Security Risk Analysis Guide" (IPA, 2017) can be used as references for creating network diagrams and data flow diagrams.

Reference: https://www.ipa.go.jp/files/000080712.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
14 Understanding the statuses of external connections	Ensure safety and trust when using external information systems, while enabling prompt response to information security incidents/accidents	External information systems (such as those of customers, subsidiaries, affiliated companies, contractors, cloud services, external information services) shall be clarified and their usage status managed appropriately	76	Lv1	Rules for using external information systems connected to organizational assets are defined	[Rule(s)] ・Usage rules shall be defined to include the following: ・Non-disclosure agreements are entered into with entities that connect with external information systems ・Security requirements for using external information systems are defined ・Service details are checked to conform that security requirements for using external information systems are met and evidence of the approval thereof is saved

[Explanation]

■ **Achievement Criteria**

① **What reference should be taken for determining the "security requirements for using external information systems?"**
Establishing security requirements when utilizing external information systems like cloud services from the perspective of system selection, operation, and management is important. (Examples below)

<Viewpoint for selection>
・ Compatibility between the service provider's information security policy and in-house security policy
・ Reliability of service availability, frequency of failures, etc.
<Viewpoint for operation>
・ Whether it is possible to set authentication settings to restrict use to authorized users
・ Whether data backup is available
<Viewpoint for management>
・ Presence of security measures and functions
・ Confirmation of the storing location and storage period of the data

*Appendix 6, "Guidance for Safe Use of Cloud Computing Services for Small and Medium-sized Enterprises" of the "Information Security Measure Guidelines for Small and Medium-sized Enterprises" explains important points and checklists for safe use of cloud services and is useful as a reference.
Reference: Information Security Measure Guidelines for Small and Medium-sized Enterprises, Version 3.1 (IPA)
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

Reference: Appendix 6 Guidance for Safe Use of Cloud Computing Services for Small and Medium-sized Enterprises (IPA)
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
14 Understanding the statuses of external connections	Ensure safety and trust when using external information systems, while enabling prompt response to information security incidents/accidents	External information systems (such as those of customers, subsidiaries, affiliated companies, contractors, cloud services, external information services) shall be clarified and their usage status managed appropriately	77	Lv1	A list of external information systems that are used is created	[Rule(s)] ・A list of external information systems shall be created

[Explanation]

■ **Condition(s) for Achievement**

① **What items should be managed when creating a "list of external information systems"?**

The objective behind creating a list of external information systems is to understand the information systems being used by the organization's personnel, to take measures when risks are recognized in the use of said systems, and to respond when an information security incident/accident occurs. It is sufficient if items are managed so that that objective is satisfied. (Examples below)

<Management items related to users>

・ User name, department

・ Application

<Management items related to external information systems>

・ System overview, system name

・ Vendor name

<Management items related to agreements>

・ Name of agreement, name(s) of those entered into agreement with

・ Contract date, date of expiration

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
14 Understanding the statuses of external connections	Ensure safety and trust when using external information systems, while enabling prompt response to information security incidents/accidents	External information systems (such as those of customers, subsidiaries, affiliated companies, contractors, cloud services, external information services) shall be clarified and their usage status managed appropriately	78	Lv1	The list of external information systems is ==reviewed== regularly or as necessary	[Rule(s)] ・In addition to regularly taking inventory, new external information systems shall be added to the list and those for which usage has stopped removed from the list [Frequency] ・Once or more per year and whenever use of new system starts or use of a system stops

[Explanation]

■ **Condition(s) for Achievement**

① **What should be performed in "reviews?"**

The objective of this task is to update the list of external information systems that were created in No. 77 to respond efficiently in case of an information security incident. As such, it is sufficient to maintain an inventory of external information systems considering the following points: (Examples below)

・ Update the information on the external information systems that are currently in use.

・ Update the status of external information systems that are no longer in use.

・ Add any newly started using external information systems to the inventory.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
15 Internal commu nication rules	Minimize damage such as information leaks and malware infections by appropriately managing the use of internal communicatio n networks	When connecting to internal networks, measures shall be implemented to minimize unauthorized usage of information systems and IT equipment/devices	79	Lv1	Rules for connecting IT equipment/devices used for business to internal networks are defined	• Connection rules for equipment/devices such as computers and servers: [Rule(s)] ・Rules regarding connections to internal networks shall be defined [Applies to] ・All equipment/devices that connect directly to in-house networks ・Including standard company equipment/devices and equipment/devices brought in from the outside • Additional rules for connecting from external to internal networks: [Rule(s)] ・Rules for using remote access shall be defined [Applies to] ・All equipment/devices that connect to internal networks from outside the company via public internet or leased lines

[Explanation]

■ **Achievement Criteria**

① **What are the key points and examples for defining the "rules regarding connections to internal networks?"**

Regarding security measures for devices connected to internal networks, it is recommended to refer to the "Information Security Measure Guidelines for Small and Medium-sized Enterprises" and Appendix 3, "Five-Minute Information Security Self-Diagnosis" (IPA) for examples of measures that can be taken.

Below are key points and examples of countermeasures to consider regarding the rules for connecting to the internal network.

・ Implement security measures for connected devices such as operating system patches and security software.

・ Restrict devices that can connect to the company network, especially personal devices.

*The "Information Security Measure Guidelines for Small and Medium-sized Enterprises" is a resource that offers specific guidance to small and medium-sized enterprises on how to take appropriate measures against information security risks. Additionally, Appendix 3, "Five-Minute Information Security Self-Diagnosis," provides a list of information security diagnosis items and their corresponding countermeasures that can be used as a reference.

Reference: Information Security Measure Guidelines for Small and Medium-sized Enterprises, Version 3.1 (IPA)

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

Reference: Appendix 3, Five-Minute Information Security Self-Diagnosis (IPA)
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf

② **What are the key points and examples for defining the "rules for using remote access?"**

Remote access can provide a convenient solution for employees who are on business trips or working remotely. It allows them to access the company network from their home or while traveling, which can save time and enable flexible working styles like working from home. However, since employees work in environments outside of the company's control, such as their own homes, there is a risk of cyberattacks exploiting vulnerabilities in VPNs. Therefore, it is essential to consider the benefits of remote access as well as security measures before introducing remote access into your company. It is recommended to establish rules for using remote access based on guidelines such as the "Information Security Measure Guidelines for Small and Medium-sized Enterprises" (IPA) and the "Telework Security Guidelines" (Ministry of Internal Affairs and Communications).

Here are some important points and examples to consider in the rules for using remote access:

・　Security measures should be introduced for connected devices, such as introducing operating system patches and security software.
・　There should be restrictions on the devices that can be connected from external networks, as it involves handling company assets and personal property.
・　There should be restrictions on connection methods, such as VPN connection or VDI connection.
・　Application and approval should be required for starting the connection.

* In the "Information Security Measure Guidelines for Small and Medium-sized Enterprises," subsection "(4) Information Security for Telework" under "Measures to Strengthen the System" also covers information security in remote work and serves as a useful reference.
Reference: Information Security Measure Guidelines for Small and Medium-sized Enterprises, Version 3.1 (IPA)
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

* The "Telework Security Guidelines" provide a useful reference for executives, system/security managers, and remote workers on implementing security measures for remote work.
Reference: Telework Security Guidelines, 5th Edition (Ministry of Internal Affairs and Communications)
https://www.soumu.go.jp/main_content/000752925.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
15 Internal communication rules	Minimize damage such as information leaks and malware infections by appropriately managing the use of internal communication networks	When connecting to internal networks, measures shall be implemented to minimize unauthorized usage of information systems and IT equipment/devices	80	Lv3	There is a system that restricts connections to the internal company network, except for authorized devices	[Rule(s)] ・A system shall be introduced to detect and block connections other than those from authorized devices [Applies to] ・Devices connecting to the company network

[Explanation]

■ **Achievement Criteria**

① **What are some examples of the "system to detect and block connections other than those from authorized devices?"**

To detect and block connections other than those from authorized devices, a system shall be introduced that allows only authorized devices to connect. There are different ways to implement such a system including the following:

・ Allowing only authenticated devices (for instance, those that have been authenticated using a client certificate)

・ Allowing only MAC addresses that have been pre-registered.

・ Allowing only IP addresses that have been pre-registered.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
15 Internal communication rules	Minimize damage such as information leaks and malware infections by appropriately managing the use of internal communication networks	For remote work environments, measures are taken to prevent security incidents (primarily information leakage and spoofing)	82	Lv2	Rules have been established and are operated under regarding conditions for confidential information and IT equipment/devices used in remote work	[Rule(s)] ・Rules shall be established and communicated within the company regarding conditions for confidential information and IT equipment/devices used in remote work ・Confirm compliance with rules and make corrections as necessary [Targets for communication] 　-All employees, temporary employees, and seconded employees working remotely [Timing for communication] 　-Before the start of remote work [Content of rules] 　-IT equipment/devices that are permitted to be used in remote work 　*Including application and approval methods as necessary 　-Confidentiality classifications and types of files that can be downloaded to personally owned terminals [Frequency for checking the content of rules and compliance status] 　-Once or more per year

[Explanation]

■ **Achievement Criteria**

① **What kind of "IT equipment/devices and confidential information are used in remote work?"**

In a remote work environment, the risk of confidential information leakage is high. To avoid such risks, it is important to limit the usage of IT equipment/devices and the handling of confidential information during remote work. Therefore, it is necessary to have prior knowledge of the IT equipment/devices and confidential information used in such environments.

Examples of IT equipment/devices used in remote work environments include:
- ・ PCs, smartphones, and tablets provided by the company
- ・ Personally owned PCs, smartphones, and tablets
- ・ Personally owned printers.

Information can be classified as "confidential information," "business information," or "public information." Examples of "confidential information" include:

- Personal information (customers, employees, business partners, etc.)
- Trade secrets (finance, strategy, human resources, etc.)
- Management information
- Non-public information received from customers

② **What are the key points and examples that should be established in "rules for confidential information and IT equipment/devices used in remote work?"**
As previously mentioned in No. 79, it is recommended to establish regulations for remote access in accordance with guidelines such as the "Information Security Measures Guidelines for Small and Medium Enterprises" (IPA) and the "Telework Security Guidelines" (Ministry of Internal Affairs and Communications) to ensure effective remote work. Since remote work allows employees to work from anywhere, like home or a restaurant/café, there is a higher possibility of information leaks due to the loss of information devices, such as personal computers. Therefore, in addition to restricting the devices that can be used during remote work, it is also crucial to set rules about confidential information that is handled during remote work. Particularly, it is advisable to prevent access to highly sensitive information, such as customer personal information, in a remote work environment, as the impact of such information leakage can be significant.

The rules for using IT equipment/devices during remote work should include the following points:
- Restrictions on the kind of devices that can be used for remote work, taking into account the handling of company assets and personal property.
- Implementation of security measures for connected devices, such as introducing OS patches and security software.
- Limitations on connection methods, for example, VPN connection and VDI connection.
- A method for monitoring the usage status, such as VPN log monitoring.

The rules for handling confidential information during remote work should specify the following point:
- Clear restrictions on the types of information that can be accessed, particularly highly sensitive data such as personal customer information.

* In the "Information Security Measure Guidelines for Small and Medium-sized Enterprises," subsection "(4) Information Security for Telework" under "5. Measures to Strengthen the System" also covers information security in remote work and serves as a useful reference.
Reference: Information Security Measure Guidelines for Small and Medium-sized Enterprises, Version 3.1 (IPA)
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

* The "Telework Security Guidelines" provide a useful reference for executives, system/security managers, and remote workers on implementing security measures for remote work.
Reference: Telework Security Guidelines, 5th Edition (Ministry of Internal Affairs and Communications)
https://www.soumu.go.jp/main_content/000752925.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
15 Internal communication rules	Minimize damage such as information leaks and malware infections by appropriately managing the use of internal communication networks	For remote work environments, measures are taken to prevent security incidents (primarily information leakage and spoofing)	83	Lv2	Rules have been established and are operated under regarding working remotely	[Rule(s)] ・Rules shall be established and communicated within the company regarding working remotely ・Confirm the details of rules and compliance status, and make corrections as necessary [Targets for communication] -All employees, temporary employees, and seconded employees working remotely [Timing for communication] -Before the start of remote work [Frequency of checking and correcting the content of rules and compliance status] -Once or more per year

[Explanation]

■ **Achievement Criteria**

① **What are the key points that should be established in the "rules for working remotely?"**

To ensure information security during remote work, it is necessary to establish rules for the execution of remote work in addition to those provided in No. 82. However, merely establishing rules is not enough; it is crucial to educate and raise awareness among remote workers about the purpose of the rules, and the benefits of complying with them. Specifically, referring to guidelines such as the "Information Security Measures Guidelines for Small and Medium-sized Enterprises" (IPA) and the "Telework Security Guidelines" (Ministry of Internal Affairs and Communications) can be effective in establishing the rules for remote work execution.

The following points should be established in the rules for working remotely.
・　Applying for and obtaining approval for remote work.
・　Attending training on remote work.
・　Updating software and applying patches to devices used for remote work (e.g. OS patches).
・　Imposing restrictions on hardware/software/services that can be used for remote work.
・　Imposing restrictions on the use of removable media (e.g. USB memory, CD/DVD).

- Imposing restrictions on printer connection.
- Imposing restrictions on software/apps installed.
- Imposing restrictions on the use of cloud services.
- Outlining expected behavior during remote work (e.g. rules for carrying devices, PC screen filters, PC screen lock when away from work).
- Establishing procedures in the event of loss of IT equipment/devices or leakage of confidential information.

* In the "Information Security Measure Guidelines for Small and Medium-sized Enterprises," subsection "(4) Information Security for Telework" under "5. Measures to Strengthen the System" also covers information security in remote work and serves as a useful reference.
Reference: Information Security Measure Guidelines for Small and Medium-sized Enterprises, Version 3.1 (IPA)
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

* The "Telework Security Guidelines" provide a useful reference for executives, system/security managers, and remote workers on implementing security measures for remote work.
Reference: Telework Security Guidelines, 5th Edition (Ministry of Internal Affairs and Communications)
https://www.soumu.go.jp/main_content/000752925.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
16 Physical security	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Physical security measures shall be implemented for areas where equipment such as servers are installed	87	Lv2	Unauthorized intrusions and suspicious behavior in areas where equipment such as servers are installed is monitored	[Rule(s)] ・Items brought in/taken out are checked when entering or leaving ・The behavior of visitors is monitored

[Explanation]

■ **Condition(s) for Achievement**

① **There are numerous ways to "monitor unauthorized intrusions and suspicious behavior". From what point of view should measures be selected?**

Countermeasures are roughly divided into three categories. It is advisable to select the most suitable measures after taking into account the characteristics of facilities and divisions, and the flow and amount of people entering and exiting. (Examples below)
<Personnel measures>

・ Inspection of belongings

・ Regular review of entry/exit records

<Physical measures>

・ Locks

・ Gates

<Technical measures>

・ Surveillance cameras

・ Biometric authentication

② With regard to "areas where equipment such as servers are installed", if they are installed in a location other than a dedicated server room (such as a private room in the corner of an office), is such an area included in the regulation?

The definition of a "server" is important. If important data and files for the organization are stored on it and are used via network communication, that terminal should be included as a server. For example, even if it is a laptop, it is positioned as a server if the above applies to it. Even if it is in a private room in the corner of an office, that should be recognized as an installation area.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
16 Physical security	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Measures are taken to prevent security incidents (primarily unauthorized intrusion, unauthorized removal, information leakage, and suspicious behavior) with regard to entering or exiting the company	88	Lv2	Rules are established, communicated within the company, and operated under regarding entry and exit	[Rule(s)] ・Rules regarding entering and exiting the company shall be defined ・Entry/exit rules shall be communicated within the company ・Confirm the details of entry/exit rules and compliance status, revising and re-informing employees as necessary [Targets for communication] ・All personnel entering/exiting the company [Content of entry/exit rules] ・Areas with restricted entry are defined ・Application and approval when entering/exiting ・Identity confirmation measures when entering/exiting (wearing employee ID cards, entry permits, etc.) ・Rules for issuing entry permits and gate passes [Frequency of checking and correcting the content of entry/exit rules and compliance status] ・Once or more per year

[Explanation]

■ **Achievement Criteria**

① **Though it is stated that "areas with restricted entry are defined" in the rules, what is the specific perspective for defining these?**

Designating restricted entry areas for each company's premises, buildings, and rooms is preferred. For instance, in the case of a building, in a factory where manufacturing equipment is classified as confidential information, a restricted area may be set up to prevent unauthorized access. Regarding rooms, besides server rooms, it is crucial to include offices where the company's information assets and personal employee data are handled in the restricted area. Furthermore, as a general rule, it is imperative to establish rules that discourage outsiders from approaching restricted areas unless necessary.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
16 Physical security	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Measures are taken to prevent security incidents (primarily unauthorized intrusion, unauthorized removal, information leakage, and suspicious behavior) with regard to entering or exiting the company	89	Lv2	Access to important areas and rooms are restricted, and entry/exit records are stored	[Rule(s)] ・Entry into and exit from important areas and rooms shall be restricted ・Entry/exit records for important areas and rooms shall be obtained and stored [Items to be recorded] ・Entry/exit date and time ・Name of the individual (name, affiliation, contact information, etc.) ・Reason for entering ・Approved by [Record storage period] ・Six months or more

[Explanation]

■ **Achievement Criteria**

① **Though "entry/exit records shall be obtained and stored" is stated, what is the specific method for doing it?**

Aside from recording and storing information in handwritten ledgers, an effective way is to introduce a system that can restrict entry and exit while simultaneously managing records. However, there are costs involved in implementing and operating such a system, so it is important to consider this when introducing it to your company.

* The "Information Security Measure Requirements Checklist for Entry/Exit Control Systems" describes the requirements for improving security when using entry/exit control systems. This checklist can be used as a reference when purchasing a new entry/exit control system.
Reference: Information Security Measure Requirements Checklist for Entry/Exit Control Systems, Version 1 (IPA)
https://www.ipa.go.jp/security/jisec/about/knowledge/cdk3vs00000024ph-att/checklist_ecs.pdf

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
16 Physical security	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Measures are taken to prevent security incidents (primarily unauthorized intrusion, unauthorized removal, information leakage, and suspicious behavior) with regard to entering or exiting the company	90	Lv2	<mark>Unauthorized intrusions and suspicious behavior is monitored</mark>	[Rule(s)] ・Unauthorized intrusions and suspicious behavior shall be monitored for <mark>important locations in the company</mark> ・Confirm that monitoring is functioning normally and make corrections as necessary [Frequency of confirming and correcting monitoring status] ・Once or more every six months

[Explanation]

■ **Condition(s) for Achievement**

① **What measures are there for "monitoring unauthorized intrusions and suspicious behavior"?**

Measures similar to No. 87 are required. (Examples below)

\<Personnel measures\>

・ Inspection of belongings

・ Regular review of entry/exit records

\<Physical measures\>

・ Locks

・ Gates

\<Technical measures\>

- ・ Surveillance cameras
- ・ Biometric authentication

■ **Achievement Criteria**

② **What exactly is meant by "important locations in the company"?**

This refers to areas where confidential information is handled, such as research, design, and development areas, server rooms, etc. Since many companies define divisions as regulations related to confidentiality management, it is advisable to make judgments based on such rules (However, if such regulations do not exist, they should be confirmed and defined, including for internal general affairs-related organizations).

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
16 Physical security	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Measures shall be taken to understand what should be targeted for countermeasures when a vulnerability is discovered and to prevent information leakage, etc., using external storage media	100	Lv2	For important data that would interfere with business if it were damaged by malware (data encryption, etc.), rules are established and communicated that it is stored outside of PCs	[Rule(s)] ・Important data shall be stored in a location other than client PCs [Targets for communication] ・Executives, employees, temporary employees, and seconded employees

[Explanation]

■ **Achievement Criteria**

① **While it states "important data", what perspectives should be used to determine if something is important or not?**

As stated in the conditions for achievement, the point is whether or not it interferes with work. This will differ depending on the industry, but in the case of the manufacturing industry, stopping production and not being able to ship and sell products are major short-term obstacles. From a long-term perspective, the leakage of sensitive management data, cutting-edge technology, and other data that could be a source of competitiveness would also pose a major obstacle. It is advisable to judge whether something is important based on perspectives such as those.

② **What is the reason for storing it in a "location other than client PCs"?**

There are two reasons. The first is that PCs used by employees are more likely to be damaged by malware infections, etc., than servers. As such, it is necessary to habitually store data on a file server environment in a secure area on the company network. The second is backup. Important server environments are backed up regularly, and in the event of damage due to a cyberattack, etc., data can be restored from those backups.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
16 Physical security	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	For systems that store and use important information, measures are taken to minimize the damage caused by human error regarding setting mistakes	101	Lv2	Unnecessary features on servers are disabled <mark>Use of default user IDs is stopped</mark> Default passwords are changed	[Rule(s)] ・Unnecessary services and daemons shall be disabled ・Use of default user IDs shall be stopped ・Default passwords shall be changed

[Explanation]

■ **Condition(s) for Achievement**

① **If "stopping the use of default user IDs" has an impact such as stopping a system, should it be stopped?**

As a general rule, this should be stopped after considering a workaround so that the system is unaffected. The reason for this is that default user IDs are information that can easily be learned by a third party, making it an easy target for cyberattacks such as unauthorized logins, so the use of default IDs is high risk.

However, taking into consideration the feasibility of workarounds, the level of impact on business in the event of stoppage, etc., if it is absolutely necessary to continue using default IDs, risk mitigation measures need to be taken such as restricting access to the relevant servers from specific terminals only and restricting logging in from other specific systems.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
17 Communication control	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Communication is controlled to information systems, IT equipment/devices, and malicious websites to prevent cyberattacks and internal information leaks	103	Lv2	A firewall is installed at the boundary between the internet and the internal company network to restrict communication.	[Rule(s)] ・A system shall be introduced to restrict internal and external network communication [Introduction location] 　-Boundaries between internal and external networks [Items to be restricted] 　-The IP addresses of connection sources and connection destinations 　-Communication ports

[Explanation]

■ **Achievement Criteria**

① **Though "restrict internal and external network communication" is stated, from what perspective should the communication be restricted?**

A firewall is a security feature that regulates network communication, controlling traffic from inside the company to outside and vice versa. As a general rule, it is important to deny all communications by default and only allow necessary ones. To do this, you need to identify the services required for business and set clear firewall rules accordingly. For example, outgoing communication from the internal network to outside may be limited to only http/https (port number: 80, 443) for web browsing. Similarly, incoming communication from outside to the internal network may be limited to specific services such as the company's website (port number: 443), email server (port number: 587, etc.), and remote access (port number: 3389, etc.).

Since the installation and configuration of a firewall require specialized knowledge of information security, it is advisable to consult with a security vendor for network vulnerability diagnosis or other related services.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
17 Communication control	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Communication is controlled to information systems, IT equipment/devices, and malicious websites to prevent cyberattacks and internal information leaks	104	Lv2	Firewall filtering settings (communication permissions/blocking settings) are recorded, with regular checks for unnecessary settings	[Rule(s)] ・Filtering settings for internal and external network communications shall be recorded ・Periodically check for unnecessary filtering settings ・Delete unnecessary filtering settings [Items to be recorded] ・Applicant name, IP addresses of connection source and destination, communication direction, protocol, port number, usage, registration date, expiration date [Confirmation frequency] ・Once a year

[Explanation]

■ **Achievement Criteria**

① **Though "periodically check for unnecessary filtering settings" is stated, what are the specific methods and precautions for doing it?**

Periodic checking of unnecessary filtering settings of your firewall is necessary to ensure they are configured as intended. To identify unnecessary settings, you will need to compare the filtering settings record with the actual filtering settings. It is especially crucial to record and manage filtering settings that are temporarily granted. Leaving these settings unattended can make your system vulnerable to cyber-attacks. So, restoring filtering settings immediately is recommended when they are no longer required. For instance, sometimes temporarily granted settings to an external vendor are not restored to the original settings even after the work is completed, so extra attention is needed.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
17 Communication control	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Communication is controlled to information systems, IT equipment/devices, and malicious websites to prevent cyber-attacks and internal information leaks	105	Lv2	Remote access IDs are managed with ==regular checks for unnecessary IDs==	[Rule(s)] ・The issuing, changing, and deleting of remote access IDs are carried out through an application/approval system ・There shall be regular checks for unnecessary IDs ・Unnecessary IDs are deleted [Confirmation frequency] ・Once a year

[Explanation]

■ **Condition(s) for Achievement**

① **What are specific situations in which "unnecessary IDs" aren't needed?**

Employee retirement, leave of absence, secondment, transfer, etc., all apply. However, even without such a personnel change, if the role, etc., an employee has within the organization changes and their duties change as a result, it may be a case of an unnecessary ID.

② **What is the reason for "regular checks for unnecessary IDs"?**

It is because unnecessary IDs are likely to fall outside the scope of management and can become a blind spot, leading to risk. There is also the risk that unauthorized use of unnecessary IDs could lead to important information being taken as an insider crime, or attackers infiltrating from an external network may hijack unnecessary IDs and use them to attack. Because of this, it is important to regularly check whether there are any such IDs.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
17 Commu nication control	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Communicatio n is controlled to information systems, IT equipment/devi ces, and malicious websites to prevent cyberattacks and internal information leaks	106	Lv2	Networks are separated according to business and data importance.	[Rule(s)] ・Systems shall be classified according to business content and data importance, and they shall be installed in dedicated network [Applies to] - ・Network where external public servers are in place. Network for PCs and servers, Factory network/OA network and others.

[Explanation]

■ **Condition(s) for Achievement**

① **With regard to "separated networks", how exactly should they be separated?**

This can be done from both a physical and logical perspective. With the former it is just as is written, with network lines physically separated. With the latter, even if the lines are the same, the data flowing through them are virtually managed as separate divisions. (Examples below)

<Physical separation>

・ If an industrial control system exists, that network is configured separately from the information system network.

<Logical separation>

・ Servers that are publicly accessible are placed in a separate virtual segment called a DMZ.

・ Even if it is on the same HDD, there are separate divisions within it so that communication is managed through a separate virtual space.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
17 Communication control	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Communication is controlled to information systems, IT equipment/devices, and malicious websites to prevent cyberattacks and internal information leaks	108	Lv2	<mark>Access to malicious websites is restricted</mark>	[Rule(s)] ・Access to malicious websites shall be restricted [Applies to] -Client PCs, web gateways

[Explanation]

■ **Condition(s) for Achievement**

① **What sort of filtering methods should be introduced to "restrict access to malicious websites"?**

Introducing the following methods should be sufficient. (Examples below)

- Restrict access by pre-registering website URLs

- Restrict access via the content of each page on a website

② **What sort of devices and services should be introduced to "restrict access to malicious websites"?**

Introducing devices and services with the following web filtering functionality should be sufficient. (Examples below)

- Filtering using software installed on the PC

- Filtering using security equipment installed on the network (firewalls, etc.)

- Filtering using cloud services

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
17 Communication control	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Communication is controlled to information systems, IT equipment/devices, and malicious websites to prevent cyberattacks and internal information leaks	109	Lv2	A Web Application Firewall (WAF) is installed for web applications published on the internet	[Rule(s)] ・WAF (Web Application Firewalls) shall be installed [Applies to] ・Important external public web applications

[Explanation]

■ **Achievement Criteria**

① **Do the "important external public web applications" mentioned here include cases where cloud services are used?**

Yes, they do. However, when using a general-purpose cloud service, it is often difficult to request introduction of a WAF due to service usage agreements. As such, the reality is that there are many cases where it is simply a matter of confirming whether a WAF has been introduced or confirming the SLA (document stipulating service levels) on the service provider side when entering into a contract. On the other hand, if you have a cloud environment that is part of your own infrastructure, there is an increased chance of introducing a WAF at your organization's own discretion.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
17 Communication control	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Communication is controlled to information systems, IT equipment/devices, and malicious websites to prevent cyberattacks and internal information leaks	110	Lv2	Measures are implemented to continue the service of websites and systems published on the internet even if subjected to DDoS attacks	[Rule(s)] ・A system shall be introduced to continue service in the event of a DDoS attack [Applies to] ・Important external public websites, DNS servers

[Explanation]

■ **Achievement Criteria**

① **Do the "important external public websites, DNS" mentioned here include cases where cloud services are used?**

Yes, they do. However, when using a general-purpose cloud service, it is often difficult to request implementation of DDoS countermeasures due to service usage agreements. As such, the reality is that there are many cases where it is simply a matter of confirming whether DDoS countermeasures exist or confirming the SLA (document stipulating service levels) on the service provider side when entering into a contract. On the other hand, if you have a cloud environment that is part of your own infrastructure, there is an increased chance of implementing DDoS countermeasures at your organization's own discretion.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
17 Communication control	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Communication is controlled to information systems, IT equipment/devices, and malicious websites to prevent cyberattacks and internal information leaks	111	Lv2	Communication is encrypted to prevent eavesdropping and tampering with communication via the internet	[Rule(s)] ・Internal and external network communications shall be encrypted [Applies to] ・Communication with authentication between the user and an external public server ・Remote access communication from outside the company

[Explanation]

■ **Achievement Criteria**

① **Do the "communication with authentication between the user and an external public server" and "remote access communication from outside the company" items mentioned here include cases where cloud services are used?**

Yes, they do. When using a general-purpose cloud service, communication is usually encrypted on the service provider side. However, due to the service usage agreement, there are many cases where it is difficult to specify the encryption technology used and the strength of the encryption. Because of this, it is advisable to confirm details such as the encryption scheme and encryption strength with the service provider when entering into a contract, then negotiate to enter into an SLA (document stipulating service levels) that matches the company's requirements as closely as possible.

On the other hand, if you have a cloud environment that is part of your own infrastructure, your organization will need to implement encryption itself.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
17 Communication control	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Communication is controlled to information systems, IT equipment/devices, and malicious websites to prevent cyberattacks and internal information leaks	112	Lv2	Communication between terminals and wireless LAN access points is encrypted	[Rule(s)] ・Communication between terminals and access points shall be encrypted ・Do not use cryptographic technology that has been compromised according to CRYPTREC [Applies to] ・In-house wireless LANs

[Explanation]

■ **Achievement Criteria**

① **What are some points to note when outsourcing the building of an "in-house wireless LAN" environment?**

It is important to make a selection from the perspective of post-construction support and trust.

With regard to the "encrypting communication between terminals and access points" stated in this item, even if the encryption scheme is secure at the time of construction, it may become dangerous during operation due to technological progress or the discovery of vulnerabilities, and so it may be necessary to change the settings. It is therefore necessary to make a selection considering support during operation after construction has been completed.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
18 Authentication/ Approval	▪ Prevent information leakage/unauthorized modification and ensure stable information system operation by preventing unauthorized usage or unauthorized operation/modification of information systems ▪ Enable the causes of information leakage, unauthorized modification, or system stoppages to be investigated	Authentication and approval measures shall be used for information systems and IT equipment/devices	116	Lv2	Rules for the setting of passwords for external information systems are defined and communicated within the organization	[Rule(s)] ・ Target passwords shall not be set in external web services *If the same authentication platform (SSO, etc.) is used, this does not count as being reused [Target passwords] ・ Passwords when logging into PCs ・ Mail system passwords (Microsoft 365, etc.) [Targets for communication] ・ Executives, employees, temporary employees, and seconded employees

[Explanation]

■ **Condition(s) for Achievement**

① **What should be considered in the "rules for the setting of passwords for external information systems?"**

The password-setting rules specified in requirement No. 115 can also be applied to setting up passwords for external information systems. Moreover, the password setting rules should include instructions to avoid the reuse of passwords to minimize the impact in case of a password leak or security incident. (Examples below)

• Avoid using the same password for multiple external information systems.

• Avoid using the same password for multiple users.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
18 Authentication/ Approval	Prevent information leakage/unauthorized modification and ensure stable information system operation by preventing unauthorized usage or unauthorized operation/modification of information systems Enable the causes of information leakage, unauthorized modification, or system stoppages to be investigated	Authentication and approval measures shall be used for information systems and IT equipment/devices	120	Lv3	Multi-factor authentication is implemented for systems that can be used from the internet	[Rule(s)] ・There shall be at least two forms of authentication implemented (knowledge/possession/biometric) for authentication via the internet [Applies to] ・Systems that handle information with a high level of confidentiality ・Privileged accounts ・Remote access

[Explanation]

■ **Condition(s) for Achievement**

① **Does "systems that can be used from the internet" mean internal systems that can be used via a VPN? Or does it include all systems that can be accessed from the internet (web applications, etc.)?**

It includes all systems that can be accessed from the internet.

This means that websites that can be accessed from outside the company and connections to an internal environment using a VPN are also included.

There is a particularly high risk with regard to authentication when using a VPN to connect to an internal environment, so it is necessary to implement multi-factor authentication here.

That said, multi-factor authentication is not essential for authentication to an internal system accessed after a VPN connection, so it is advisable to adjust the strength of authentication in accordance with the importance of the system.

② **Is there an appropriate combination of factors that should be used for "multi-factor authentication"?**

The three factors are knowledge, possession, and biometric. Ensure that authentication is based on a combination of these different factors. (Examples below)

<Knowledge-based authentication>

- User IDs and passwords

<Possession-based authentication>

- Devices, one-time passwords, text messages

- Connection restrictions (IP address, security token, etc.)

<Biometric authentication>

- Fingerprints, iris, veins

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
18 Authentication/ Approval	Prevent information leakage/unauthorized modification and ensure stable information system operation by preventing unauthorized usage or unauthorized operation/modification of information systems Enable the causes of information leakage, unauthorized modification, or system stoppages to be investigated	Authentication and approval measures shall be used for information systems and IT equipment/devices	121	Lv2	Session time-outs are implemented for important systems	[Rule(s)] ・Session time-outs shall be implemented for important systems [Applies to] ・External public systems, important internal systems

[Explanation]

■ **Condition(s) for Achievement**

① **What exactly is meant by "implement session time-outs"?**

This refers to implementing functionality that forcibly logs a user out if they are inactive for a specific amount of time after logging in to a web application, etc.

If the time before forced logout is too long, the risk of cyberattacks increases, but if the time is too short, it may have a negative impact on user convenience. As such, it is advisable to set the amount of time considering the importance of the system.

■ **Achievement Criteria**

② **What kind of systems does "external public systems" refer to specifically?**

It refers to systems that are open to the internet.

Furthermore, the "important systems" mentioned in the Achievement Criteria rules include both the above systems and important internal systems.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
19 Applyi ng patches and updates	Reduce the risk of unauthorized access and malware infection	Avoid using devices, operating systems, and software that is no longer supported	123	Lv2	The use of operating systems and software that is no longer supported is avoided	[Rule(s)] ・Supported OS and software shall be used ・If an OS or software that is not supported must be used, reduce the risk of vulnerabilities being exploited as practicably as possible 　[Applies to] ・OS, browser, office software for company-supplied PCs ・Server OS, middleware ・OS and applications for company-supplied smart devices ・OS and firmware of network devices in contact with the internet

[Explanation]

■ **Achievement Criteria**

① **If it is necessary to continue using "OS or software that are not supported", from what perspective should measures be selected to "reduce the risk of vulnerabilities being exploited as practicably as possible"?**

<Point countermeasures>

To protect a terminal that continues to use the unsupported OS or software itself (hereinafter, the "Terminal"), introduce tools that restrict the launching of applications other than those specified (e.g. whitelists), tools that detect and defend against programs with similar characteristics based on past examples (e.g. anti-virus software), etc. Installing a dedicated network device (firewall functionality) in front of the Terminal in order to block and protect against non-essential communication is also effective.

<Line countermeasures>

To protect not only the Terminal, but also to cross-sectionally protect all information assets connected to the Terminal, separate networks and introduce devices that monitor communications and detect unauthorized behavior (e.g. IDS/IPS).

Furthermore, although the conditions for achievement say to "avoid using devices, operating systems, and software that is no longer supported", keep in mind that the achievement criteria states that even in those cases the criteria are met by reducing risk.

② **What sort of situations are referred to with regard to "must be used"?**

This is referring to a situation in which replacement of the system is not possible, such as in the following cases. (Examples below)

・　There is no alternative device for the system in operation

- Replacement is not possible due to high costs.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria

19 Applying patches and updates	Reduce the risk of unauthorized access and malware infection	Implement measures to prevent unauthorized access using vulnerabilities	124	Lv1	Security patches and updates are properly applied for information systems, IT equipment/devices, and software	[Rule(s)]
						・The ==applying of security patches and updates shall have defined rules and deadlines==
						・If they cannot be applied for an unavoidable reason, record the reason why it cannot be applied
						[Applies to]
						・PCs, smartphones, tablets, servers, network devices, software, etc.
						  - OS, browser, office software for company-supplied client PCs
						  - Server OS, middleware
						  - OS and applications for company-supplied smart devices
						  - OS and firmware of network devices in contact with the internet

[Explanation]

■ **Achievement Criteria**

① **Though "applying of security patches and updates shall have defined rules and deadlines" is stated, how should the rules be defined?**

Performing security patches and updates is crucial to fixing vulnerabilities in IT equipment/devices, and software and protecting them from cybersecurity attacks. From a cybersecurity perspective, it is essential to keep your IT equipment/devices, and software up to date. To achieve this, it is necessary to set deadlines based on the importance and urgency of security patches and updates for IT equipment/device and software.

The following points should be considered when defining rules and deadlines:
- Have rules and deadlines been clearly defined for highly important IT equipment/ devices and software specified in No. 59?
- Have the IT equipment/devices and software included in the information asset list created in No. 60 been considered as targets?
- Are there rules and deadlines based on the importance and urgency of security patches and updates?

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
19 Applying patches and updates	Reduce the risk of unauthorized access and malware infection	Implement measures to prevent unauthorized access using vulnerabilities	125	Lv2	A management system and management process has been set in place for vulnerabilities	[Rule(s)] ・The ==roles and responsibilities of the departments in charge from collecting vulnerability information to responding== shall be clarified ・The ==sources==, tools, and frequency ==for collecting vulnerability/threat information== shall be defined ・Criteria and procedures for determining the necessity of responding to the collected information shall be defined ・Correspondence history shall be recorded and checked monthly

[Explanation]

■ **Achievement Criteria**

① **How should the "roles and responsibilities of the departments in charge from collecting vulnerability information to responding" be decided?**

Vulnerability information is primarily utilized to identify the targets for security patches mentioned in No. 124 and may also support the CSIRT activities mentioned in No.17. When considering the department responsible for collecting vulnerability information, the initial approach is to gather this information in the IT asset management department. However, depending on the company's size, business valuation, and the number of businesses, it might be more efficient to centrally collect vulnerability information in the control department.

* The "Guidebook for Establishing Cybersecurity Organization and Securing Necessary Human Resources" provides key insights for making informed decisions about establishing cybersecurity systems and securing human resources.
Reference: Guidebook for Establishing Cybersecurity Organization and Securing Necessary Human Resources, Version 2.0 (METI, IPA)
http://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

② **What exactly are the sources stated in the "sources for collecting vulnerability/threat information?"**

There are two sources available for collecting vulnerability information: "JVN iPedia" (IPA) and "Important Security Information List" (IPA). It is also advisable to refer to the reports published by security vendors and to seek advice from vendors with whom you have established business relationships. The choice of the method for collecting vulnerability information should depend on the purpose of the collecting said information. (Examples below)

・   If you want to investigate vulnerability information for each IT asset, then "JVN iPedia" (IPA) is the recommended source.

・   If you need to investigate urgent vulnerabilities or threat information, then "Important Security Information List" (IPA) is the recommended source.

* The "JVN iPedia Vulnerability Countermeasure Information Database" is a comprehensive database that offers daily publications of vulnerability information both nationally and internationally. This database enables users to investigate vulnerabilities for each IT asset and the hardware/software that makes up that asset.
Reference: JVN iPedia Vulnerability Countermeasure Information Database (IPA)
https://jvndb.jvn.jp/index.html

* The "Important Security Information List" is a compilation of high-risk security information that may lead to unauthorized access or information leaks. This method is ideal for quickly identifying urgent vulnerabilities.
Reference: Important Security Information List (IPA)
https://www.ipa.go.jp/security/security-alert/index.html

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
19 Applying patches and updates	Reduce the risk of unauthorized access and malware infection	Implement measures to prevent unauthorized access using vulnerabilities	126	Lv3	For servers that are open to those outside of the company, vulnerability diagnoses before and after production are carried out, and measures are taken against identified vulnerabilities	[Rule(s)] ・Platform vulnerabilities shall be diagnosed ・The rules and lead time for determining the necessity of dealing with vulnerabilities shall be defined ・Diagnosis and response results shall be stored [Applies to] ・External public server OS, middleware [Diagnosis frequency] ・Before production: One or more times ・After production: Twice a year and when a major system change takes place ・When a high impact vulnerability is made public

[Explanation]

■ **Condition(s) for Achievement**

① **What should be done for "vulnerability diagnoses"?**

To start, a vulnerability diagnosis refers to checking for the risk of a threat such as unauthorized access or information leakage occurring due to configuration errors, system defects, etc.

Of the various types of vulnerability diagnoses, a platform diagnosis targets server OS and middleware, identifying risks through pseudo-attacks on the system and checking settings values. It is important to analyze the exposed risks and take appropriate measures based on the results of assessment.

In addition, when a web application is running on an OS to be diagnosed, it is generally performed together with a diagnosis similar to No. 128.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
19 Applying patches and updates	Reduce the risk of unauthorized access and malware infection	Implement measures to prevent unauthorized access using vulnerabilities	128	Lv2	Application vulnerability diagnoses are carried out for web applications published on the internet	[Rule(s)] ・Web application vulnerabilities shall be diagnosed ・The rules and lead time for determining the necessity of dealing with vulnerabilities shall be defined ・Diagnosis and response results shall be stored [Applies to] ・Important external public web applications [Diagnosis frequency] ・Before production: One or more times ・After production: When a major application change takes place

[Explanation]
- **Condition(s) for Achievement**
  - ① **What should be done for "application vulnerability diagnoses"?**

    To start, a vulnerability diagnosis refers to checking for the risk of a threat such as unauthorized access or information leakage occurring due to configuration errors, system defects, etc.

    Of the various types of vulnerability diagnoses, an application diagnosis targets web applications, identifying risks through pseudo-attacks on the system, checking settings values, and program analysis. It is important to analyze the exposed risks and take appropriate measures based on the results of assessment.

    In addition, it is common to perform a diagnosis similar to No. 126 for the platform on which this application is running.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
21 Office tool-related	Reduce the risk of unauthorized access and malware infection	The data of information systems and IT equipment/devices is being protected	131	Lv2	Measures are implemented to <mark>prevent information leakage due to email transmission</mark>	[Rule(s)] ・When sending confidential information by email, measures shall be implemented to prevent information leakage

[Explanation]
- **Condition(s) for Achievement**
  - ① **There are various ways to "prevent information leakage due to email transmission". From what point of view should measures be selected?**
    Measures should be selected from the point of view of the following transmission phases. (Examples below)
    \<Before sending\>

    ・ Education/training on information leakage

    \<When sending\>

    ・ Introducing a system to prevent erroneous transmission (confirming destination multiple times, delaying transmission)

    ・ Attachment encryption

    ・ Email body encryption

    \<After sending\>

    ・ Communication encryption

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
21 Office tool-related	Reduce the risk of unauthorized access and malware infection	The data of information systems and IT equipment/devices is being protected	132	Lv2	<mark>Measures</mark> are implemented <mark>to prevent erroneous email transmission</mark>	[Rule(s)] ・Measures shall be implemented to prevent erroneous email transmission [Applies to] ・Mail sent to addresses outside of the company

[Explanation]

■ **Condition(s) for Achievement**

① **What exactly is meant by "measures to prevent erroneous email transmission"?**

The two possible measures are enlightenment through education and the use of system functionality. However, since this item is labeled under "tool-related", the latter measure is what is required. Specifically, it is advisable to utilize system functionality such as the following. (Examples below)

・ A function that displays a final confirmation window and prompts the user to confirm that there are no mistakes when the destination includes an external address.

・ A function that allows email to be sent outside the company only after being approved by a superior registered beforehand if there is an attachment included.

・ A function wherein emails are only sent externally once a certain amount of time has passed after pressing the send button (and it is possible to return the email before that time).

■ **Achievement Criteria**

② **Can this item only be applied to email that has important information?**

If that is possible, then it isn't a problem. However, in reality it is difficult to judge whether an attached file is important information or not, and depending on the function, it may be possible to add a level of gradation so that only certain attachments are targeted under certain conditions, but it is best to consider that a function will need to be designed that targets all file attachments.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
22 Malware countermeasures	Prevent information leakage, unauthorized modifications, and system stoppages due to malware infections	Anti-malware measures shall be implemented to quickly detect security abnormalities	136	Lv1	Software (anti-virus software) is used on computers and servers to detect malware and provide notifications	[Rule(s)] ・Anti-virus software shall be used on each computer and server ・Scans shall be performed by specifying scan scopes and frequencies appropriate for the equipment/device [Applies to] ・All computers and servers connected to networks

[Explanation]

■ **Condition(s) for Achievement**

① **"Anti-virus software" includes EPP: Endpoint Protection Platform and EDR: Endpoint Detection and Response. Is it OK to implement either one?**

EPP alone is sufficient for achieving this item. EPPs are products that aim to protect against "known" malware before infection occurs using pattern matching technology. EDR, on the other hand, is designed to detect the behavior of cyberattackers and malware, regardless of whether it is "known" or "unknown", and raise an alert.

However, in recent years, cyberattacks have been requiring a multi-layered system of defense based on both EPP and EDR as a minimum, as either one alone is no longer a sufficient countermeasure. (No. 138 is the applicable item for introducing EDR.) The conditions for achieving this item state that software that detects and reports malware infections must be installed. However, they also state that the purpose of this is to prevent information leakage, unauthorized modifications, and system stoppages, so it is advisable to keep in mind the defenses described above in view of the intended purpose.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
22 Malware counter measures	Prevent information leakage, unauthorized modifications, and system stoppages due to malware infections	Anti-malware measures shall be implemented to quickly detect security abnormalities	137	Lv1	Anti-virus software pattern files are updated regularly	[Applies to] ・Same as No. 136 [Pattern file update frequency] ・Once or more on days computers/servers are booted and used

[Explanation]

■ **Condition(s) for Achievement**

① **Should this item only be assessed when an EPP: Endpoint Protection Platform is implemented?**

This will depend on the functionality of the EPP implemented.

The two general types of EPP are anti-virus and next-generation anti-virus.

Products such as anti-virus programs, which detect and defend against programs with similar characteristics to attacks that have occurred in the past, are subject to this item because it is important to keep the pattern file updated to increase the detection rate of malware.

That said, products such as next-generation anti-virus programs, which use artificial intelligence to detect and defend against predictive malicious programs, are not subject to this item because there is no pattern file.

Note that for next-generation anti-virus programs, the artificial intelligence installed may need to be updated, so in such cases it is advisable to consider the necessity of updating based on information from the vendor.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
22 Malware counter measur es	Prevent information leakage, unauthorized modifications, and system stoppages due to malware infections	Anti-malware measures shall be implemented to quickly detect security abnormalities	138	Lv3	A behavior tracking system has been introduced that allows for the acquisition of detailed histories at endpoints and remote response after malware infection	[Rule(s)] ・An endpoint countermeasure system shall be introduced [Applies to] ・Company-supplied client PCs ・Servers [System requirements] ・Can obtain terminal operation history, program execution history, registry change history ・Can remotely investigate terminals ・Can remotely disconnect from the network ・Can recover after infection

[Explanation]

■ **Condition(s) for Achievement**

① **What needs to be introduced as a "behavior tracking system that allows for the acquisition of detailed histories and remote response after malware infection"?**

Introducing a tool that satisfies the system requirements in the achievement criteria, that is, one that can acquire various logs and allows for remote operation of the terminal, should be sufficient. (EDR: Endpoint Detection and Response, etc.)

In addition to acquiring various logs, it is also important to be able to remotely inspect terminals and disconnect from the network in response to a malware infection, so tools that can only acquire logs are not sufficient to meet the criteria.

*The IPA's Cybersecurity Help Team is one such service for achieving this item.

Reference: https://www.ipa.go.jp/security/otasuketai-pr/

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
22 Malware countermeasures	Prevent information leakage, unauthorized modifications, and system stoppages due to malware infections	Anti-malware measures shall be implemented to quickly detect security abnormalities	139	Lv2	Malware checks are implemented at email gateways to prevent malware infection by email	[Rule(s)] ・A <mark>malware check function</mark> shall be introduced at the email gateway

[Explanation]

- **Achievement Criteria**

① **What kind of functions should be included in the "malware check function" in general?**

The email gateway's malware check function is designed to prevent malware infections through emails. However, there are other security risks associated with email misuse, such as spam emails and phishing attacks. Therefore, it is important to have a comprehensive set of security functions for emails at the email gateway.

Typically, the malware check function includes the following features. (Examples below)

- ・ Spam email filtering (countermeasure for spam emails)
- ・ Scanning and removing email attachments (countermeasure for malware infection)
- ・ Scanning and removing links in emails (countermeasure for phishing attacks)

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
22 Malware counterm easures	Prevent information leakage, unauthorized modifications, and system stoppages due to malware infections	Anti-malware measures shall be implemented to quickly detect security abnormalities	140	Lv2	Extension restrictions are enforced by a system to prevent malware intrusion from email attachments	[Rule(s)] ・A function restricting specific extensions shall be introduced at the email gateway

[Explanation]

■ **Achievement Criteria**

① **Though "restricting specific extensions" is stated, what file extensions should be restricted?**

File extensions that are executed when a file is opened are often used to infect malware. To prevent such occurrences, email gateway vendors have conducted research and compiled a restricted list of file extensions that have caused malware infections in the past. However, if there are other extensions that are not typically used in your company's business, it is recommended to add them to the restricted list.

For instance, there have been cases where the following file extensions are restricted. (Examples below)
".exe, .pif, .scr, .bat, .com, .lnk, .cmd, .vbs, .cpl, .hta, .shs, .url, .desklink, .mapimail"

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
22 Malware counter measur es	Prevent information leakage, unauthorized modifications, and system stoppages due to malware infections	Anti-malware measures shall be implemented to quickly detect security abnormalities	141	Lv2	Malware checks are implemented at ==web gateways== to prevent malware infection by viewing malicious websites	[Rule(s)] ・A ==malware check function shall be introduced at the web gateway==

[Explanation]

■ **Condition(s) for Achievement**

① **What is a "web gateway"?**

This is equipment wherein the communication for accessing online websites from the internal network environment is routed, and has the role of monitoring whether such communication is correct and restricting it if it is dangerous. The equipment is generally installed at the entrance (the gateway) to the internet, and is suitable for implementing the web access restriction functionality in No. 108.

■ **Achievement Criteria**

② **It says to "introduce a malware check function at the web gateway", but what constitutes a malware check function?**

It is functionality that detects and protects against programs that have characteristics similar to attacks that have occurred in the past.

Furthermore, introducing functions that have the ability to run a suspicious program in a safe and isolated environment to determine safety based on its behavior, and functions that monitor the behavior of a program on a PC in order to detect suspicious behavior, are highly effective from the viewpoint of a multi-layered system of defense. This sort of functionality is called an anti-virus gateway, and it can be implemented in various ways, such as by installing dedicated equipment, installing software, or using a cloud-based service. As such, it is advisable to make a selection taking cost, functionality, the company's situation, etc., into consideration.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
23 Detecting unauthorized access	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized access and intrusions	Build a system to constantly monitor unauthorized access to the network	142	Lv2	A system is introduced to constantly monitor the content of communications and detect/block and notify regarding unauthorized access in real time	[Rule(s)] ・A system shall be introduced that detects/blocks unauthorized access in real time [Applies to] ・Communications from the internet to the company ・Communications from within the company to an unauthorized server [Introduction location] ・Boundaries between internal and external networks

[Explanation]

■ **Condition(s) for Achievement**

① **What exactly is meant by a "system to constantly monitor the content of communications and detect/block and notify regarding unauthorized access in real time"?**

This refers to the introduction of equipment that monitors abnormal communications and their logs 24 hours a day, such as those that occur in the event of unauthorized access or network intrusion. More specifically, the introduction of equipment that detects and blocks unauthorized access and intrusion (IPS, IDS), SIEM (described in the explanation for No. 145), etc.

However, because SIEM and IDS do not have a mechanism for automatically blocking unauthorized communication, it is necessary to have an operation/system in place to receive such notices, determine whether or not a block is necessary, and respond accordingly.

The method for implementing SIEM is described in the explanation for No. 145, and the method for setting up an operation/system is described in the explanation for No. 17. In either case, this can be done in-house or by using an external service. It is important to consider the company's situation and take measures that are feasible.

■ **Achievement Criteria**

② **What exactly is meant by "boundaries between internal and external networks"? Also, why are they important?**

This refers to the gateway between the internet and the company's internal environment. It is important to connect the products and services described in (1) with the equipment such as firewalls, proxy servers, etc., that are installed there. This is because communication between the internal environment and the internet passes through these "boundaries between internal and external networks", making them high risk locations. These risks can effectively be reduced by introducing mechanisms to detect and block unauthorized intrusions.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
23 Detecting unauthorized access	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized access and intrusions	Logs shall be acquired so that intrusion and leak routes can be investigated in the event of a security incident or accident	143	Lv2	Logs required for investigation when an incident occurs are being obtained	[Rule(s)] ・The following logs shall be obtained and stored 　[Logs to be obtained (retention period)] -Email transmission/reception logs (6 months) 　Items: Date and time, destination email address, sender email address -Firewall logs (6 months) 　Items: Date and time, source IP address, destination IP address -Proxy server logs (6 months) 　Items: Date and time, requester IP address, URL -Remote access logs (6 months) 　Items: Date and time, connection source IP address, user ID -Authentication server logs (6 months) 　Items: Date and time, connection source IP address, user ID, success/failure -Endpoint (PC, server) operation logs (6 months) 　Items: Date and time, host name, user ID, IP address, operation details *Also includes the use of cloud services *If using a cloud service that cannot meet the regulations for retention period, each company shall determine the period according to risk

[Explanation]

■ **Achievement Criteria**

① **What are the specific methods to "obtain and store logs?"**

There are two methods for storing logs: either on the device that generates them or in a log management system that centrally manages them. Since logs are used for investigations when incidents occur, it is essential to store them with measures against unauthorized access and falsification. Therefore, it is desirable to store logs not only in the device where they are generated but also in a log management system with security measures such as measures against unauthorized access.

You may find the following website helpful in obtaining and storing logs.

Reference: Information Security Measures for Information Management Personnel > Appropriate Acquisition and Storage of Logs (Ministry of Internal Affairs and Communications)

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_admin_22.html

② **What are the precautions to observe regarding the "obtaining and storing logs?"**

When it comes to storing logs, in addition to taking measures against unauthorized log access and falsification, as described in section ① of the explanation, it is important to consider privacy matters depending on the data being collected and stored. For instance, if you are storing logs that include data like sent/received emails and computer operation logs, you should be aware that privacy measures such as obtaining consent for data collection and storage are required.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
23 Detecting unauthorized access	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized access and intrusions	Logs shall be acquired so that intrusion and leak routes can be investigated in the event of a security incident or accident	144	Lv3	Application operation logs are obtained for important systems	[Rule(s)] ・User and administrator operation logs shall be obtained [Applies to] -Important systems *Applicable systems are judged by each company according to risk [Log items to be acquired] -User ID, time stamp, operation details (login, logout, addition/deletion, etc.) [Retention period] -6 months *If using a cloud service that cannot meet the criteria for the retention period, each company shall determine the period according to risk

[Explanation]

■ **Condition(s) for Achievement**

① **What is meant by "important systems?"**

As previously explained in No. 59, the important systems within a company are determined by the degree of impact their compromise would have on the business and are selected by the company. Additionally, the servers that store logs (as explained in Nos. 143 and 144) are also important for security purposes as they are utilized during incident investigations. Therefore, these servers should also be considered important systems.

■ **Achievement Criteria**

② **What is the reason for "obtaining the operation logs of users and administrators?"**

During incident investigations, security audits, and other related scenarios, it is important to check user and administrator operation logs for any unauthorized operations. Since administrators often have the authority to modify or delete information, these logs are used to analyze and investigate any suspicious activities. Therefore, it is important to acquire and store user/administrator operation logs.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
23 Detecting unauthorized access	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized access and intrusions	Take measures to promptly detect and block cyberattacks in order to curb damage caused by targeted attacks and other such cyberattacks	145	Lv2	==A system== is introduced ==to analyze logs and detect cyberattacks==	[Rule(s)] ・A system shall be introduced to constantly analyze logs and given notification when an abnormality is found [Analysis targets] -Proxy servers, IPS/IDS, firewalls, endpoints, or a combination thereof [Monitoring period] -24 hours a day, 365 days a year [Functional requirements] -Incident alerts are issued immediately -Breaking incident reports are created and notifications given

[Explanation]

■ **Condition(s) for Achievement**

① **What sort of means are available for introducing a "system to analyze logs and detect cyberattacks"?**

It is common to introduce SIEM (System Information and Event Management) products and services, which cross-sectionally analyze the relevance of log data from various network security equipment. A system can be built in-house, but it is also possible to utilize the services of vendors who provide systems for monitoring and analysis.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
23 Detecting unauthorized access	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized access and intrusions	Take measures to promptly detect and block cyberattacks in order to curb damage caused by targeted attacks and other such cyberattacks	147	Lv3	For websites published on the internet, a system is introduced to detect site falsification and checks are made regularly	[Rule(s)] ・A system shall be introduced to detect website falsification [Applies to] ・Important external public websites

[Explanation]

■ **Condition(s) for Achievement**

① **What exactly is meant by a "system to detect site falsification"?**

This refers to a system that detects when a file on a website has been tampered with through tools, operational designs, etc. A variety of such tools exist, including those that detect by comparing the differences in the files themselves, those that compare files with past examples of attacks and look for similarities, etc. Operational designs include methods such as contacting the administrator when a file on a website has been updated. Depending on how this mechanism is implemented, the importance of communicating with the website administrator increases, which may also increase the load. As such, it is advisable to consider this after taking into account the importance of the website and the frequency with which it is updated. Various vendors also offer web tampering detection as a service, so introducing a service such as that is another possible method of adoption.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
24 Backup/ Restore	Minimize the impact of system stoppages and data loss on business operations, and enable operations to resume quickly	Measures shall be taken to minimize the damage to important information and impact to system operations caused by cyberattacks	148	Lv1	Backups are performed at appropriate times	[Rule(s)] ・Data, etc. subject to back up and backup frequencies shall be defined

[Explanation]

■ **Achievement Criteria**

① **How should the "data subject to back up and backup frequencies" be determined? "**

When determining what data to back up and how often to perform backups, it's important to consider a few key factors. These include the impact on the business in case of a system stoppage or data loss, how frequently the data is updated, and the cost of performing backups.

・ The importance of the system/data (e.g., core system, customer information, management information) needs to be considered while acquiring it.

・ The frequency of system/data updates (e.g., software and data that are updated frequently) should also be taken into account while acquiring it.

・ The cost of backup (e.g., adjust the acquisition frequency depending on the amount of backup data and the associated cost) should also be factored in.

② **What are some specific examples of the "data subject to back up, backup frequencies," and "performing backups?"**

Below are a few examples of the data subject to back up, backup frequencies, and backup methods:

[Examples of data subject to back up and backup frequencies]

・ Documents and settings information stored on the file server (Frequency: daily for documents, monthly for setting information.

・ Emails and setting information saved on the mail server (Frequency: daily for emails, monthly for setting information.

[Example of backup methods]

・ Use backup servers.

・ Store on external recording media.

* Additionally, the following website may serve as a helpful guide to backup concepts and methods.

Reference: Information Security Measures for Information Management Personnel > Recommended Backup Methods (Ministry of Internal Affairs and Communications)

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_admin_10.html

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
24 Backup /Restore	Minimize the impact of system stoppages and data loss on business operations, and enable operations to resume quickly	Measures shall be taken to minimize the damage to important information and impact to system operations caused by cyberattacks	149	Lv1	<mark>Restore procedures</mark> are established	[Rule(s)] ・Restore procedure manuals shall be established for each type of data, etc., subject to backup

[Explanation]

■ **Condition(s) for Achievement**

① **Does the establishment of "restore procedures" include cases where cloud services are used?**

Yes, it does. When using a general-purpose cloud service, the service provider usually has a system for implementing restoration and procedures in place. However, due to service usage agreements, in many cases it is difficult to specify the level of restoration, such as the target time from backup to restoration or the point in time from which data should be restored. Because of this, it is advisable to confirm details such as the target restoration time and target restoration level with the service provider when entering into a contract, then negotiate to enter into an SLA (document stipulating service levels) that matches the company's requirements as closely as possible.

On the other hand, if your organization has a cloud environment that is part of your own infrastructure, etc., and you can implement a restoration system yourself, you will need to develop procedures for that purpose.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
24 Backup/ Restore	Minimize the impact of system stoppages and data loss on business operations, and enable operations to resume quickly	Measures shall be taken to minimize the damage to important information and impact to system operations caused by cyberattacks	150	Lv1	Alternative means that can be used to perform business operations in the event of a system stoppage are prepared	[Rule(s)] ・Viable alternative means shall be established for use in the event systems are down [Applies to] -Systems requiring a high level of availability (short allowable downtime) *Targets are determined by each company according to risk [Example measures] -Use of analog tools (fax, etc.) -Use of external information systems such as cloud services

[Explanation]

■ **Achievement Criteria**

① **What are the "viable alternative means?"**

In the event of a cyberattack on a company, it is necessary to assume that the information systems within the company's network will become unusable. In such a situation, it is desirable to select an alternative method that is physically or logically separated from the affected system. To prepare for such a system stoppage, the following considerations are necessary:

- Consider ways to continue business operations manually, for example, receiving orders by phone or fax when the ordering system is down.
- Consider system continuity methods, such as switching to the backup system when the main system stops working.
- Consider alternative communication methods, such as securing multiple communication channels in advance.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
24 Backup /Restor e	Minimize the impact of system stoppages and data loss on business operations, and enable operations to resume quickly	Measures shall be taken to minimize the damage to important information and impact to system operations caused by cyberattacks	151	Lv2	==Backup restore tests on important data and systems== are implemented	[Rule(s)] ・It shall be confirmed that restoration is possible according to specified restoration procedures [Applies to] ・Important data and systems [Frequency] ・When constructing systems, making changes, regularly (determined according to risk)

[Explanation]

■ **Condition(s) for Achievement**

① **Does the implementation of "backup restore tests on important data and systems" include cases where cloud services are used?**

Yes, it does. When using a general-purpose cloud service, the service provider usually has a system for implementing restoration in place and conducts tests. However, due to service usage agreements, in many cases it is difficult to specify the level of restoration, such as the target time from backup to restoration or the point in time from which data should be restored, and to request tests to be carried out accordingly. Because of this, it is advisable to confirm details such as test conditions with the service provider when entering into a contract, then negotiate to enter into an SLA (document stipulating service levels) that matches the company's requirements as closely as possible.

On the other hand, if your organization has a cloud environment that is part of your own infrastructure, etc., it is necessary to conduct tests while taking the impact on existing services into consideration.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
24 Backup /Restore	Minimize the impact of system stoppages and data loss on business operations, and enable operations to resume quickly	Measures shall be taken to minimize the damage to important information and impact to system operations caused by cyberattacks	152	Lv2	==Disaster prevention and environmental countermeasures are implemented in locations where equipment such as servers are installed==	[Rule(s)] ・Measures shall be taken against fires, floods, and power outages ・Temperature and humidity shall be controlled

[Explanation]

■ **Condition(s) for Achievement**

① **Does the implementation of "disaster prevention and environmental countermeasures" include cases where cloud services are used?**

Yes, it does. When using a general-purpose cloud service, disaster prevention and environmental countermeasures are usually implemented on the service provider side. However, due to service usage agreements, in many cases it is difficult to specify details such as the scale of the assumed disasters or the specific countermeasures to be implemented. Because of this, it is advisable to confirm details such as the specific measures being implemented with the service provider when entering into a contract, then negotiate to enter into an SLA (document stipulating service levels) that matches the company's requirements as closely as possible.

On the other hand, if you have a cloud environment that is part of your own infrastructure, your organization will need to implement disaster prevention/environmental countermeasures itself.

② **With regard to "areas where equipment such as servers are installed", if they are installed in a location other than a dedicated server room (such as a private room in the corner of an office), are they included in the regulation?**

The definition of a "server" is important. If important data and files for the organization are stored on it and are used via network communication, that terminal should be included as a server. For example, even if it is a laptop, it is positioned as a server if the above applies to it. Even if it is in a private room in the corner of an office, that should be recognized as an installation area.

Contributing Committee Members (shown in alphabetical order of company name)

General Policy Committee / ICT Subcommittee / Cyber Security Subcommittee / SC Guidelines Study Taskforce

Role	Company Name	Name
Leader	Toyota Motor Corporation	Toshiya Ban
Sub-Leader	Nissan Motor Co., Ltd.	Shuntaro Torii
Sub-Leader	Honda Motor Company, Ltd.	Yoshichika Sakakibara
Committee Member	Suzuki Motor Corporation	Hideaki Suzuki
Committee Member	Subaru Corporation	Hidemasa Ito
Committee Member	Daihatsu Motor Co., Ltd.	Nobuyuki Sakata
Committee Member	Toyota Systems	Noboru Taniguchi
Committee Member	Honda Motor Company, Ltd.	Rintaro Aoyagi
Committee Member	Mazda Motor Corporation	Shota Iida
Committee Member	Mitsubishi Motors Corporation	Kenji Taki

Japan Auto Parts Industries Association
DX Committee / Cyber Security Subcommittee

Role	Company Name	Name
Subcommittee Chair	Aisin Corporation	Tomohiro Kajita
Deputy Subcommittee Chair	Hitachi Astemo, Ltd.	Takayuki Nakao
Deputy Subcommittee Chair	DENSO Corporation	Tsutomu Tsunekawa
Committee Member	Aisin Corporation	Satoshi Matsunaga
Committee Member	DENSO Corporation	Shunjiro Goto

Contact address: Vehicle Safety and Environmental Division, Japan Automobile Manufacturers Association, Inc. (JAMA)

Jidosha Kaikan, 1-30, Shiba Daimon 1-chome, Minato-ku, Tokyo 105-0012 Japan
TEL:03-5405-6125 FAX:03-5405-6136