Cybersecurity Management Guidelines

for Japanese Enterprise Executives

Ver. 3.0

Ministry of Economy, Trade and Industry (METI)

Information-technology Promotion Agency, Japan (IPA)

Contents

Revision highlights of Cybersecurity Management Guidelines Ver. 3.0

The Cybersecurity Management Guidelines, released as Ver. 1.0 in 2015, have been steadily spreading as a guide for implementing organizational cybersecurity measures under the leadership of corporate managers in domestic companies. An increasing number of guidelines for corporate governance published by the Ministry of Economy, Trade and Industry require companies to refer to these guidelines for cybersecurity risks, and together with the Information Security Guidelines for SMEs (published by the Information-technology Promotion Agency (IPA))[1], these guidelines serve as a common language for implementing cybersecurity measures amongst domestic companies.

Since the last release as Ver. 2.0 in 2017, the following changes have occurred in the environment surrounding corporate cybersecurity measures:

- Diversification of work styles based on the utilization of the digital environment, represented by telework, etc.
- Closer connections between cyberspace (represented by the internet) and physical space (where physical transactions are conducted), and the emergence of associated risks
- Changes and expansion of the target of cyber security, from protecting only information assets and the IT environment that handles them, to protecting digital infrastructure including control systems
- Damage caused by ransomware[2] has become apparent, cyber security-related damage in companies is not limited to information leaks, and the impact of such damage has expanded to the suspension of business activities of companies.
- Growing need to promote security measures throughout the entire supply chain in light of the spread of cybersecurity-related damage through domestic and overseas supply chains
- Growing interest in efforts to improve corporate governance and enterprise risk management accompanying the expansion of ESG (Environment, Society, Governance) investment

In light of these developments, in formulating Ver. 3.0, the content of the document was reviewed to ensure awareness of the latest situation and implementation of countermeasures, while maintaining the basic structure of the "Three principles which management need to recognize" and the "Ten important items of cybersecurity management" established in Ver. 2.0. In addition, in light of the development of tools and related guidelines that can be used in conjunction with the Cybersecurity Management Guidelines, improvements have been made to enhance the convenience of companies using the Guidelines, including the addition of a chart outlining the relationship between these tools and guidelines.

Ver. 1.0 and Ver. 1.1 of the Guidelines were reviewed and compiled by the Study Group on Cybersecurity Risk and Corporate Management, which is cosponsored by the Ministry of Economy, Trade and Industry and the Information-technology Promotion Organization (IPA), and Ver. 2.0 and Ver. 3.0 were reviewed and compiled by the Study Group on Revision of the Cybersecurity Management Guidelines. Ver. 3.0 was formulated based on interviews with institutional investors and cybersecurity experts, etc. conducted to understand the security measures required for companies in the future.

[1] For details of the ″Information Security Guidelines for SMEs″, see Appendix B (Reference Information on Cybersecurity Measures).

[2] For damage caused by ransomware, see the relevant item in Appendix E (Definition of Terms).

Outline of the Cyber Security Management Guidelines

I. Cybersecurity as part of enterprise risk management

○ Currently, many corporate activities depend on the digital environment. It is necessary to consider cybersecurity risks in the construction of internal control systems required by the Companies Act, maintenance of necessary human resources, disclosure and dialogue based on the Corporate Governance Code, etc. Companies must incorporate cybersecurity into the practice of enterprise risk management.

○ The origins of cyberattacks in the diversifying supply chain are widespread, and all companies with indirect connections through the supply chain—including small and medium-sized companies that do not have direct transactions with large companies—are required to manage risk by taking into account risks stemming from cyberattacks in addition to geopolitics[3] and natural disasters.

○ If the cybersecurity system decided by the organization's decision-making body is not commensurate to the scale and work of the organization, and the company or a third party incurred damages due to the leakage of information held by the organization, the decision-making body faces legally responsible stipulated in the Corporate Law, Civil Code, etc., and accountability to stakeholders, such as liability for damages based on failure of responsible management or negligence of duty. In addition, management decisions such as business suspension in the case of serious damage and budgetary measures to deal with new threats are required, and it is not permissible to delegate everything to the person in charge of cybersecurity.

○ It is important to characterize cybersecurity measures as **investments (expenses essential for future business activities and growth)**[4]. Although it is difficult to calculate direct profits, cybersecurity is an **essential investment to reduce costs and losses in corporate activities** in order to maintain and increase corporate value. **It is the social responsibility of a company** to understand and evaluate cybersecurity risks from this perspective and **reduce cybersecurity risk to a level that is acceptable to the company through the implementation of cybersecurity measures.**[5] It is **the responsibility of business managers to put this into practice.**

○ These guidelines are aimed at the corporate management of major companies as well as small and medium-sized companies (excluding small-scale enterprises) and include, from the viewpoint of protecting companies from cyberattacks, three principles which management needs to recognize and ten important items which management should direct their executive in charge (e.g. CISO) to observe in implementing cybersecurity measures.

[3] In this document, "geopolitical risks" are treated as risks that affect supply chains and markets in corporate business activities, resulting from conflicts, the use of force, political instability, large-scale disasters, etc. in specific regions.

[4] The concept of "investment" has different definitions in various fields such as accounting and management. Although investment in cybersecurity does not bring direct profits (returns), it is used in this document as a means of curbing future risks and bringing about positive results in terms of the sum of risks and profits.

[5] For specific examples of risk assessment and risk reduction measures, see Direction 4 of the Ten Important Items for Cybersecurity Management. Regarding the allowable level, it is necessary to consider the guidelines of own industry and the requests from client companies.

II. Three principles which management needs to recognize

It is essential that management recognizes the following three principles and drives cybersecurity measures.

1. Corporate executives need to recognize that cybersecurity risk is an important issue in their company's risk management and take measures at their level to address this.

   (Corporate executives should take the initiative to drive cybersecurity measures considering the risks of cyberattacks and their impact on the company while also conducting security investment to ensure business continuity.)

2. In order to fulfill the responsibility of ensuring cybersecurity, it is necessary to pay attention to cybersecurity measures not only for the company itself but also for the entire supply chain, including domestic and overseas bases, business partners and outsourcing organizations.

   (In addition to the cyber security measures of one’s own company, it is necessary to be conscious of the entire supply chain, including all external connections via the digital environment, such as the use of cloud services that go beyond the form and scale of conventional parts procurement, and implement comprehensive cybersecurity measures.)

3. Active communication with relevant parties is necessary to implement effective cybersecurity measures in both normal times and emergencies.

   (Disclose information on cybersecurity measures in addition to business continuity to stakeholders outside the company (shareholders, customers, etc.) as well as internal stakeholders (security officers such as CIOs, business managers, etc.) during normal times. Be prepared to foster a relationship of mutual trust and ensure smooth communication even when an incident occurs.)

(For details, refer to #2 of “Three principles which management needs to recognize” listed above.)

III. Ten important items of cybersecurity management

Management needs to ensure that the following ten critical items are implemented in a manner appropriate to the organization through directions[6] to the person or department responsible for implementing cybersecurity measures (CISO, cybersecurity officers, etc.). This is not simply a matter of providing instructions; management in charge of the organization's risk management must exercise leadership in their role to facilitate these items by reviewing implementation policies related to risk measures, allocating budgets and personnel, checking on the status of implementation, and identifying and responding to problems.

Direction 1 ：Recognize cybersecurity risks and develop an organization-wide policy

Direction 2 ：Build a management system for cybersecurity risk

Direction 3 ：Secure resources (budget, workforce, etc.) for cybersecurity measures

Direction 4 ：Identify cybersecurity risks and develop plans to address them

Direction 5 ：Establish systems to effectively address cybersecurity risks

Direction 6 ：Continuously improve cybersecurity measures through a PDCA cycle

Direction 7 ：Develop a cybersecurity incident response team and relevant procedures

Direction 8 ：Develop a business continuity and recovery team and relevant procedures in preparation for damage due to cyber incidents

Direction 9 ：Understand the status of and implement measures considering the entire supply chain, including business partners and outsourcing organizations

Direction 10 ：Facilitate the gathering, sharing and disclosure of information on cybersecurity

(For details, refer to #3 of "Ten important items of cybersecurity management" listed above.)

[6] In this case, "direction" is synonymous with "direct" in ISO/IEC 38500:2015 (Information Technology – IT Governance) and is used in the sense of practicing IT governance. It's not about leaving everything to the person in charge, but taking responsibility for seeing the results of the practice.

1. Introduction

1.1. Background and Positioning of Cybersecurity Management Guidelines

(1) Necessity of risk management including cyber security

In the past, cybersecurity was discussed with the main purpose of protecting a company's IT systems and the information assets handled therein from cyberattacks. However, as many corporate activities now rely on the digital environment, it is impossible to build appropriate internal control systems required by the Companies Act, develop necessary systems, and disclose and engage in dialogue based on the Corporate Governance Code without taking cybersecurity risks into consideration. It is necessary to practice enterprise risk management that incorporates cybersecurity.[7]

The sources of cyberattacks on diversified supply chains are widespread, and risk management that considers cybersecurity risks is required for all companies that have indirect connections through the supply chain.[8] even small and medium-sized companies that do not directly engage in transactions with listed companies.

Table: Calculation example of incident damage costs[9]

Incident type	Amount of damage	Damage breakdown
Large scale malware infection	376 million yen	･Investigation cost to determine cause and extent of damage: 100 million yen ･Replacement costs for employee terminals, servers, etc.: 142 million yen ･Recurrence prevention cost: 50 million yen ･Profit loss: 84 million yen (sales that should have transpired during the suspension)
Leakage of credit card information, etc. from EC sites	94.9 million yen	･Accident response costs: 28.9 million yen (including introduction of recurrence prevention measures) ･Profit loss: 30 million yen (sales that should have b transpired during the suspension) ･Compensatory damages: 36 million yen (claimed amount for damages)
Minor malware infection	6 million yen	･Investigation cost of determining cause and extent of damage: 5 million yen ･Recurrence prevention measures: 1 million yen

In light of these changes, these guidelines for implementation under the leadership of management are provided for the purpose of identifying and assessing risks associated with cybersecurity, and to encourage the implementation of appropriate investments and measures to meet the social demands

[7] In the United States, National Institute of Standards and Technology (NIST) has published a document for a similar purpose. NISTIR 8286 "Integrating Cybersecurity and Enterprise Risk Management (ERM)"
https://csrc.nist.gov/publications/detail/nistir/8286/final
In addition, the Ministry of Economy, Trade and Industry defines "Information security governance" as "building and operating an internal control system within a company from the perspective of information security."
https://www.meti.go.jp/policy/netsecurity/secgov-concept.html

[8] In these guidelines, the supply chain includes not only relationships such as parts procurement in the manufacturing industry, but also through the digital environment, such as the use of external digital services such as cloud services, and cooperation between systems via APIs (application program interfaces). It also includes connections between diverse and atypical companies.

[9] Quoted from "Incident Damage Investigation Report 2021" by Non-Profit Organization Japan Network Security Association.
https://www.jnsa.org/result/incidentdamage/2021.html

required of companies, such as controlling residual risks[10] to remain below acceptable levels through appropriate risk response.

(2) Subjects and Responsibilities of These Guidelines

The intended primary audience for these guidelines is representatives of companies who are responsible for management (i.e., CEOs) and those who receive directions from management and are responsible for the implementation of cybersecurity measures (CISO, etc.). It is anticipated other readers will include practitioners who directly assist executives, CISOs, etc. in implementing cybersecurity measures.

Management may cause damage to their company or a third party in the event they instate a cybersecurity system unsuitable for supporting the scale and work of their organization, which in turn results in information leaks.

In the event of such a situation, they bear legal responsibility and accountability to stakeholders as stipulated in corporate law, civil code, etc., such as liability for damages based on failure of responsible management or negligence of duties.

Furthermore, since the following judgments are required in business management, management cannot simply "leave everything to the person in charge" such as the CISO. In addition to providing directions on cybersecurity measures, it is necessary for management to obtain information necessary for making decisions on a regular basis, such as by regularly checking in the status of implementation.

- Management decisions when the damage is serious: Depending on the severity of the cyberattack, it may be necessary to suspend all or a portion of the business, and top management is required to make an appropriate decision according to the situation at hand.
- Management decisions regarding responses to changes in risks: Unlike financial, disaster prevention, and other risks, cybersecurity risks change rapidly, and there are cases where the sudden and unavoidable review of measures and budgetary measures are required.

(3) Companies referenced in these guidelines

The descriptions in these guidelines assumed that readers' companies are large companies or SMEs (excluding small businesses).[11] In light of the increasing importance of economic security (ensuring national security from an economic perspective), readers should consider the threats to economic security separately from the considerations of impacts on supply chains and social responsibility.

[10] See Appendix E. A risk that may still occur after implementing various risk countermeasures.

[11] The companies which are utilizing digital technologies, promoting digital transformation (DX) or connected with the supply chain containing all external connections through digital environments (core information systems, control systems in factories, products, services, etc.) are required to consider cybersecurity risks regardless of the size of the company. However, it is so difficult to provide descriptions for any company size, that the contents of these guidelines are assumed to target for large companies and SMEs (excluding small businesses).

(4) Positioning of these guidelines

The Cyber Security Management Guidelines have the following relationship with various guidelines and frameworks covering corporate governance and enterprise risk management. In addition, the various tools shown in the figure can be used in specific initiatives such as disclosure of information on risk response and establishment of systems.

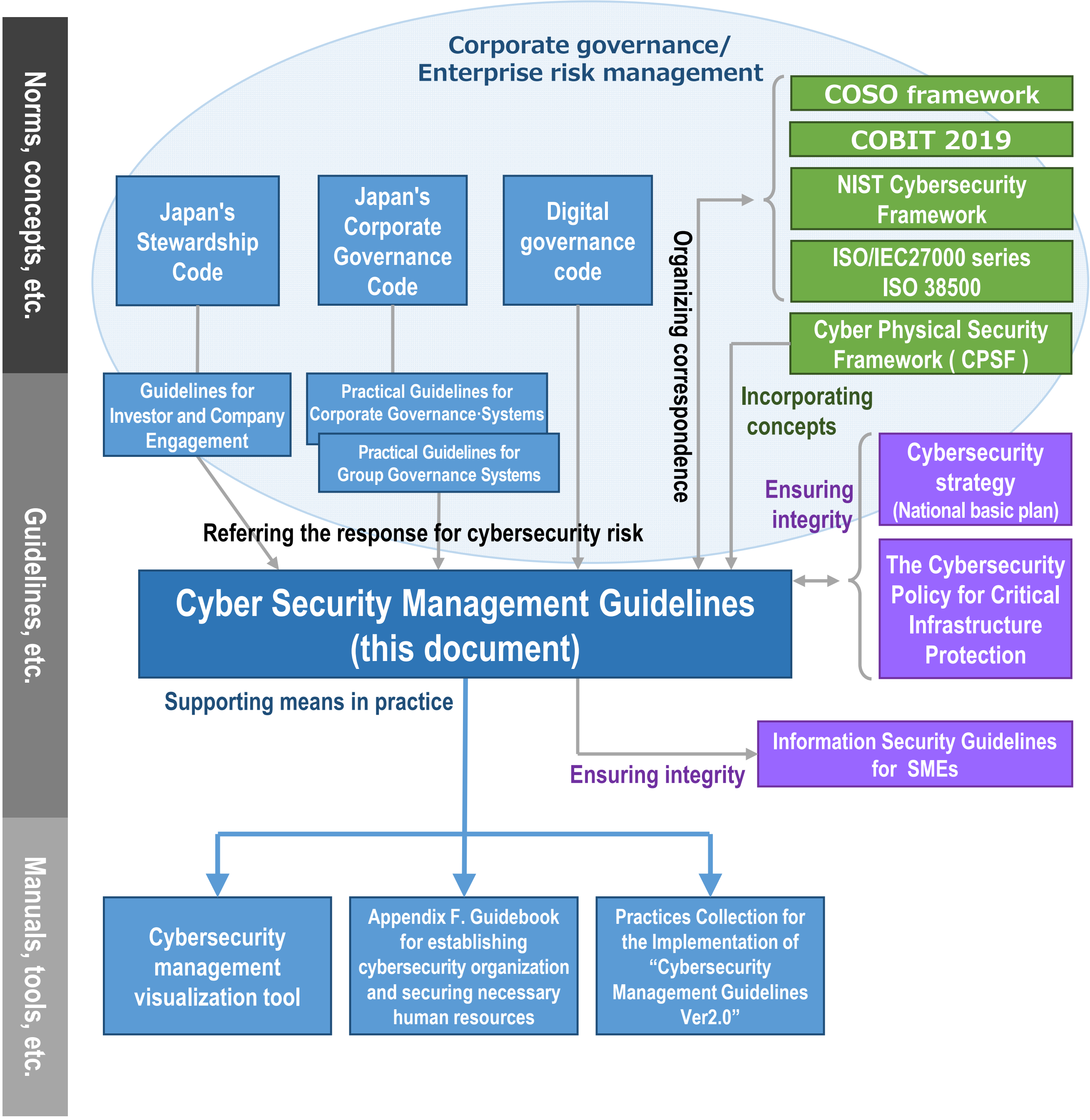
Norms, concepts, etc.
Guidelines, etc.
Manuals, tools, etc.
Corporate governance/
Enterprise risk management
Japan's Stewardship Code
Japan's Corporate Governance Code
Digital governance code
Organizing correspondence
COSO framework
COBIT 2019
NIST Cybersecurity Framework
ISO/IEC27000 series
ISO 38500
Cyber Physical Security Framework (CPSF)
Incorporating concepts
Guidelines for Investor and Company Engagement
Practical Guidelines for Corporate Governance·Systems
Practical Guidelines for Group Governance Systems
Ensuring integrity
Cybersecurity strategy
(National basic plan)
The Cybersecurity Policy for Critical Infrastructure Protection
Referring the response for cybersecurity risk
Cyber Security Management Guidelines
(this document)
Supporting means in practice
Ensuring integrity
Information Security Guidelines for SMEs
Cybersecurity management visualization tool
Appendix F. Guidebook for establishing cybersecurity organization and securing necessary human resources
Practices Collection for the Implementation of “Cybersecurity Management Guidelines Ver2.0”

Fig. 1: System of cybersecurity management guidelines

1.2. Structure and Use of the Guidelines

The structure of the guidelines is as follows. The above summary is intended for management. Chapters 2 and 3 are intended for executives responsible for cybersecurity measures (CISOs) or personnel responsible for security.

Outline of the Cybersecurity Management Guidelines

1. Introduction
2. Three principles which management needs to recognize
3. Ten important items of cybersecurity management

(Appendix)

A) Check list on cybersecurity management
B) Reference material on cybersecurity measures
C) Reference information for preparing for cybersecurity incidents (separate sheet)
D) Relationship with relevant standards and frameworks
E) Definition of terms
F) Guidebook for establishing cybersecurity organization and securing necessary human resources (separate volume)

Managers should, at a minimum, read the overview at the beginning of the book, recognize the three principles, and give directions to the CISO, etc. in line with the “ten important items.” It is necessary for managers to demonstrate leadership through the consideration of implementation policies, allocation of budget and human resources, confirmation of implementation status, and understanding and responding to problems. The CISO, etc. will give more specific directions to the security staff and promote the efforts of security measures while referring to the "example measures" on the explanation page of each of the “ten important items.” Furthermore, they must provide management with the necessary information to make appropriate decisions through timely status reports.

This guideline additionally provides information for reference when implementing the “Ten important items” in the appendix. The contents of the appendices are as follows:

Appendix A Check sheet to confirm whether the “ten important items” are being implemented appropriately

Appendix B Reference materials for implementing cybersecurity measures

Appendix C Items that should be organized within management and an organization in preparation for an incident

Appendix D Relationship between the “ten important items” and the contents stipulated by various standards and frameworks

Appendix E Definition of terms used in these guidelines

Appendix F. Specific practice guides for Directions 2 and 3

For recommendations on managing risks of internal threats such as leakage of information committed by employees, refer to IPA’s "Guidelines for the Prevention of Incidents by Internal

Threats."[12]

In addition, IPA’s "Information Security Guidelines for SMEs" also serves as a reference for companies planning to implement cybersecurity measures.

[12] Guidelines for Preventing Internal Improprieties in Organizations (IPA) https://www.ipa.go.jp/security/fy24/reports/insider/

2. Three principles which management need to recognize

It is necessary for management to take note of the following three principles when implementing countermeasures.

(1) Corporate executives need to recognize that cybersecurity risk is an important issue in their company's risk management and take measures at their level to address this.

(Explanation)

- Dependence on the digital environment is increasing. Use of digital technology spans from business development and productivity improvement within a country, to corporate business activities such as remote management of a control system's environment, utilization of IoT devices, online communication with external parties, commerce, collaboration, etc. Under these circumstances, the potential impact of cyberattacks on business activities is increasing and becoming more serious. Cybersecurity measures are an essential investment to reduce costs and losses in corporate activities, and it is the responsibility of management to reduce the residual risk related to cybersecurity to an acceptable level.
- In addition, in the event of information leakage or loss of business continuity due to cyberattacks, etc., there is a possibility of impact on human life and violation of laws and regulations. In such instances, the fate of the company depends on whether it is able to respond quickly and appropriately.
- For this reason, cybersecurity risks fall under the category of management risks (other examples include natural disasters, geopolitical events, fluctuations in foreign exchange and raw material prices, etc.). In addition to appointing executives (CISO, etc.) who will be responsible for implementing cybersecurity measures, it is necessary for **management to demonstrate leadership by understanding the risks in the company's organization and business, and to lead the promotion of countermeasures accordingly.**

(2) In order to fulfill the responsibility of ensuring cybersecurity, it is necessary to pay attention to cybersecurity measures not only for the company itself but also for the entire supply chain, including domestic and overseas bases, business partners and outsourcing organizations.

(Explanation)

- In an environment where business use of digital technology has become widespread, the supply chain is not limited to the form and scale of conventional parts procurement, but also the use of cloud services and mobile devices, the maintenance of equipment that handles information, and the media that records information. It includes all external connections the company has through the digital environment, which are nontraditional connections in the sense that they change from moment to moment.
- If countermeasures against cyberattacks are inadequate at domestic and overseas locations which are connected as part of a supply chain (encompassing business partners and all

subcontractors, to include those in charge of system management), organizations with weak security will become a medium enabling cyberattacks to target others in the supply chain. This will not only lead to the exfiltration of critical information and bring the functions of the entire supply chain to a standstill, but it will also cause problems such as serious damage to one's company.[13]. In addition, if the cause of damage is the inadequacy of measures taken by the company, the company becomes the perpetrator of damage to other companies in the supply chain.

- For this reason, it is necessary **for the company to have a holistic awareness that it is responsible for a portion of a supply chain which encompasses domestic and overseas business partners and all subcontractors (including those in charge of system management), and thoroughly implement comprehensive security measures.** To reduce the company's risk stemming from nontraditional connections and gain the trust of customers and society, it is necessary to reduce the risk of the entire, interconnected supply chain. The promotion of cybersecurity measures is the responsibility of the management of all companies, regardless of their size, in the supply chain.

(3) Active communication with relevant parties is necessary to implement effective cybersecurity measures in both normal times and emergencies.

(Explanation)

- In the event that damage due to a cyberattack occurs, if appropriate communication of security risks with relevant parties occurred during normal times, it will be possible to mitigate distrust amongst those concerned. Here, "relevant parties" within the company refers to not only security personnel such as CISOs, but also those responsible for implementing security measures. – "Relevant parties" outside the company refers to IPAs, JPCERT/CC, chambers of commerce, etc., that handle cybersecurity-related information, as well as security-related product and service providers.
- As a result, it is necessary to **actively communicate** with relevant parties during normal times (e.g. regarding awareness of cybersecurity risks and countermeasures, and to share concerns). This kind of communication system functions as a contact system in the event of an incident, enabling prompt reporting and understanding of the situation, expediting the initial response to the incident, and enabling smooth explanations to external parties.

[13] For examples of damage caused by cybersecurity, see Appendix B (Reference information on cybersecurity measures).

3. Ten important items of cybersecurity management

Management must ensure that the following 10 important items are implemented in a manner suitable for the organization through directions to the CISO, etc. This is not simply a matter of giving directions; those in management responsible for the risk management of the organization are expected to exercise leadership in that role by reviewing implementation policies, allocating budgets and human resources, checking on the status of implementation, and identifying and responding to problems.

Management should consider outsourcing some items that are difficult to handle within the organization itself or for which implementation by specialized vendors is appropriate.

<Drive security measures under the leadership of management>

(Build a structure or process for cybersecurity risk management)

Direction 1: Recognize cybersecurity risks and develop an organization-wide policy

Direction 2: Build a management system for cybersecurity risk

Direction 3: Secure resources (budget, workforce, etc.) for cybersecurity measures

(Identify cybersecurity risks and implement measures)

Direction 4: Identify cybersecurity risks and develop plans to address them

Direction 5: Establish systems to effectively address cybersecurity risks

Direction 6: Continuously improve cybersecurity measures through a PDCA cycle

(Establish a system to prepare for the occurrence of incidents)

Direction 7: Develop a cybersecurity incident response team and relevant procedures

Direction 8: Develop a business continuity and recovery team and relevant procedure in preparation for damage due to cyber incidents

<Drive security measures in the supply chain>

Direction 9: Understand the status of and implement measures considering the entire supply chain, including business partners and outsourcing organizations

<Drive communication with stakeholders and other relevant parties>

Direction 10: Facilitate the gathering, sharing and disclosure of information on cybersecurity

3.1. Building a cyber security risk management system

Direction 1　Recognize cybersecurity risks and develop an organization-wide policy

- ● Recognize cybersecurity risk as a management risk that management should be responsible for and have management formulate a (security) response policy for the entire organization.
- ● Publish the formulated response policy for an external audience.

Scenarios in case of no action

・If management does not recognize cybersecurity risk as a management risk, necessary decisions will not be made when business decisions such as business suspension are required, and as a result, there is a risk that the damage will spread.

・If an organization-wide response policy for cybersecurity risks is not formulated, responses within the organization will be inconsistent.

・Simply formulating a (security) response policy in and of itself does not clarify the responsibility for response within the organization, and therefore cannot be expected to enable effective risk response.

・Declaring a response policy as a company will increase trust with stakeholders (shareholders, customers, business partners, etc.) and lead to the improvement of brand value. If there is no such declaration, the importance the company places on cybersecurity measures will not be communicated to stakeholders, which precludes increased levels of trust.

Examples of recommended actions

・Formulate a security policy that is consistent with the company's management policy such that management can establish a response policy for the entire organization both inside and outside the organization[14]. When doing so, consider a response policy that addresses cyber security risks for all infrastructure (equipment, systems, information and other assets, distribution processes, etc.) on which the business is based, encompassing areas such as manufacturing, sales, and services.

・The company’s security policy should be posted somewhere that is easily accessible to employees (such as an internal portal site) and management should ensure that employees are thoroughly familiar with the policy by conducting employee education and through other methods.

- By publicly announcing its security policy, the company will be able to show its security posture to stakeholders and society and increase trust.

・Based on the developed and published security policies, the PDCA cycle, which is dealt with in Direction 6, should be used to periodically ascertain whether measures are being continuously implemented in response to changes in cybersecurity risks, and the organization is committed to continuous improvement.

[14] See Appendix B (Reference Information on Cybersecurity Measures) for information on how to formulate security policies.

Direction 2 Build a management system for cybersecurity risk

- ● Establish a risk management system after clarifying the roles and responsibilities of each person involved in cybersecurity risk management.
- ● Building a cybersecurity risk management system, ensure consistency with corporate governance, internal control, and other systems for risk management.

Scenarios in case of no action

・If a cybersecurity risk management system is not in place, responsibility will be ambiguous, appropriate countermeasures will not be taken, and damage will increase in the event of an incident.

・If the cybersecurity risk management system is inconsistent with other risk management systems within the organization, this may lead to inconsistencies within the overall risk management policy of the organization.

Examples of recommended actions

・In securing and developing human resources for cybersecurity measures, refer to the content of the "Guidebook for Establishing Cybersecurity Organization and Securing Necessary Human Resources" shown in Appendix F (separate volume).

・Companies involved in critical infrastructure should establish a system based on the roles and responsibilities of management, the CISO, strategic management, and systems personnel, and based on the needs of the entire organization.

・Clarify roles within the system to ensure the effectiveness of cybersecurity measures and the achievement of objectives, such as ensuring the reliability of reporting, from the perspective of enabling functioning internal controls.

・The CISO should establish a cybersecurity risk management system that encompasses all business areas within the organization and clarify the scope of responsibilities in each role.

・The CISO and others should participate in committees on management risk established within the organization.

・Directors and auditors audit whether the cybersecurity risk management system is properly established and operated.

・Depending on the responsibilities, expertise and human resource situation required, separate roles that should be handled by in-house personnel from those that should be outsourced to external professional services.

・Consider the content of NIST IR 8286 (see footnote on page 7) when considering consistency with other risk regimes in an organization in a global enterprise.

・Based on the concept of "Security by Design", the development and operation structure considering cybersecurity risk management should cover the planning / design phase as well as later phases.

Direction 3 Secure resources (budget, workforce, etc.) for cybersecurity measures

- Consider measures to keep cybersecurity-related residual risks below the permissible range, secure the resources (budget, human resources, etc.) necessary for implementation, and then work on specific measures.
- Make all officers and employees aware of security in the execution of their duties, and implement human resource development measures to improve skills related to cybersecurity measures.

Scenarios in case of no action

・It is difficult to implement cybersecurity measures and obtain the necessary workforce within an organization or to outsource the requirement to a reliable vendor without a suitable budget.

・It is not possible to secure human resources with the commensurate skills for implementing cybersecurity measures and retain them without upkeeping and revising the provision of satisfactory treatment for such personnel.

Examples of recommended actions

・When securing and training human resources for cybersecurity measures, refer to the contents of the "Guidebook for Establishing Cybersecurity Organization and Securing Necessary Human Resources" shown in Appendix F (separate document).

・Clarify the necessary cybersecurity measures to ensure the safety of all the infrastructure on which the business is based, and secure the necessary expenses.

・Secure a budget for training employees and personnel in charge of cybersecurity and consistently provide training in accordance with their roles.

・Encourage the acquisition of "Plus-Security" knowledge and skills, not only for personnel engaged in security measures, but also for personnel engaged in all operations (e.g. in digital departments, business departments, and administrative departments).

・If it is difficult to secure human resources with high-level expertise in cybersecurity within the organization, consider using specialized vendors.

・Consider developing internal human resources for cybersecurity[15] including through external hiring, and designing a career path for them as part of the organization's IT human resources development strategy.

・If it is difficult to implement education and training in the security field within the organization ,

[15] (Reference) As one of the indicators for measuring the skills possessed by cybersecurity personnel, it is also effective to utilize professional qualifications provided by private providers and the system of registered information security specialist implemented by IPA.

consider using security training services[16] provided by external organizations.

[16] (Reference) IPA (Industrial Cyber Security Center) also provides programs to train security personnel engaged in work related to information and control systems for social infrastructure and the industrial base.

3.2. Identify cybersecurity risks and implement measures

Direction 4 Identify cybersecurity risks and develop plans to address them

- ● Identify the digital environment, services, and information used in business, and based on the threat and impact of cyberattacks (including from negligence and internal fraud), identify the cybersecurity risks in the organization and its products and services.
- ● Formulate a risk response plan that includes the use of cyber insurance and outsourcing to a specialized vendor for protecting information and digital infrastructure, along with the identification of residual risks after the response.

Scenarios in case of no action

・Cybersecurity risks differ depending on the business content and organizational makeup of a company. Formulating a risk response plan that does not match the actual situation by referring to other companies' cases and proposals from vendors, etc., without assessing cybersecurity risks may incur unacceptable losses for management such as business interruption and confidential information leaks due to unaddressed risks.

・Similarly, if a risk countermeasure plan is formulated without considering the impact on the company's business on the grounds that "risks can be reduced by establishing strict measures", inconveniences such as hindrance to normal business operations may occur.

Examples of recommended actions

・Identify what information within the organization should be protected from the viewpoint of management strategy, and understand where it is stored and where it is handled. In doing so, appropriately reflect the impact of managing the company's trade secrets in an external cloud service and introducing new work styles such as teleworking.

・Understand possible cybersecurity risks to the information and systems to be protected by conducting risk assessments according to the company's business model and the technology used. When conducting risk assessments, use appropriate methods from among the approaches outlined below, depending on the company's business content and characteristics.

- Identification of risk
  Examples: Identification and comprehension of information and systems to be protected. In addition to analysis of past accidents and similar cases of other companies, utilize knowledge of threat intelligence, geopolitics, industrial psychology, organizational psychology, etc.
- Consideration of conditions under which risks become apparent
  Examples: Differences due to information usage situations (telework, etc.), evaluation of effectiveness of multi-layered defense
- Analysis of risk characteristics
  Example: Ranking frequency of occurrence and magnitude of impact
- Quantification of risks (possible damage estimate)
  Example: Trial calculation of the amount of damage due to the leakage of trade secrets with significance for management strategy

・Considering the cybersecurity measures to be implemented for the identified risks from the following perspectives.

－Implementation of risk reduction measures (measures to reduce the probability of risks)
Examples: Access control to important information, thorough software updates

- Implementation of risk avoidance measures (measures to eliminate the possibility of risk occurrence)
Example: Prohibition of data storage on personal devices (avoiding the risk of information leaks)

－Implementation of risk transfer measures (measures to transfer risks to other companies, etc.)
Examples: Use of cloud services, purchase of cyber insurance[17]

・When identifying risks and considering countermeasures, refer to the "Cyber Physical Security Framework (CPSF)" and "Cyber Security Management Visualization Tools" shown in Appendix B , appropriately identify the risk sources that may affect business activities (e.g. "Malware infection that exploits security vulnerabilities in the system, internal fraud by authorized users", etc. described in Attachment B of the CPSF), and be sure to determine what security measures should be considered.・ When identifying cybersecurity risks, consider risks not only within the organization but throughout the entire supply chain,　In addition to cyberattacks, also consider risks such as false information, misjudgments in machine learning, overseas legal violations, etc.[18]

・When considering the probability of risk occurrence and the damage, etc. when cyber incidents occur, identify risks for which it is judged unnecessary or difficult to implement cybersecurity measures as residual risks.

・Regarding information for which security control measures are legally required, consider whether measures are taken to identify risks in consideration of legal handling and to promptly protect information in the event of an emergency.

・For products and services, consider cyber security measures from the planning and design stage based on the perspective of security by design.

・Risk management requires constant review in response to changes in threats. Periodically check whether the risks in the organization and the countermeasures against them have become mere formalities.

[17] Both the use of cloud services and the purchase of cyber insurance do not reduce the risks borne by the company to naught, and it is necessary to consider implementation after understanding the effects and scope of responsibility for each.

[18] See Appendix B (Reference Information on Cybersecurity Measures) for information on how to gather up-to-date information on cybersecurity.

Direction 5 Establish systems to effectively address cybersecurity risks

- As protection measures to deal with cyber security risks, build a system that encompasses defense, detection, and analysis functions.
- Conduct reviews of the system in order to respond to changes in the business environment and risks.

Scenarios in case of no action

・If appropriate measures are not taken in response to the cybersecurity risks clarified through direction 4, cyberattacks cannot be prevented, and business continuity may be affected if they occur. There is a possibility that damage will spread and affect society as a whole (e.g. through leaks and cyberattacks against other companies).

・Even if technical measures are taken, the situation regarding cyberattacks cannot be grasped accurately and in a timely manner if appropriate operations to detect and analyze attacks are not carried out, and responses based on such operations cannot be taken. In the absence of such operations, there is a risk of fatal damage, such as an attacker stealing important information within the organization.

・Even if an organization implements changes such as migration to cloud services and adoption of a Zero Trust model after reviewing the digital environment of the organization (e.g. in response to the diversification of work styles), maintaining the conventional mechanism it had in place to detect incidents without amendments will result in oversights and delayed responses.

Examples of recommended actions

・Implement multi-layered defense for terminals, networks, systems, or services (including cloud services) that perform critical operations.

- If necessary, separate network segments with switches and firewalls, etc., and establish separate policies for operating these segments
- Conduct vulnerability assessments and other inspections to detect system vulnerabilities and respond to them.
- For important information such as trade secrets, highly sensitive technical information, and personal information, introduce mechanisms to protect information such as encryption and electronic signatures, as well as mechanisms to detect data manipulation[19].
- When implementing measures based on the Zero Trust model, work to strengthen authentication, etc. given that there can be no expectation of cybersecurity based on perimeter defense. Build a mechanism and system that can immediately detect and target incidents at the first sign of an incident.[20].
- When selecting cloud services, consider the security functions provided by the cloud services, utilize

[19] See related terms in Appendix E (Definitions of Terms) to ensure the effectiveness of encryption as a countermeasure.

[20] For organizations that find it difficult to develop mechanisms and systems on their own, it is possible to utilize measures for SMEs such as the "Cybersecurity supporters service" to support them. See Appendix B (Reference Information on Cybersecurity Measures) for more information.

those functions, and ensure that settings such as access restrictions and account management are properly maintained and managed.[21]

- If it is not possible to secure personnel with the necessary skills to implement countermeasures in-house, use external companies that provide specialized information security services.
  Refer to the "Lists of Services that Meet Information Security Service Standards" published by IPA.[22]
  - Even when outsourcing services, recognize that it is necessary to have human resources who possess the skills to properly understand the contents of reports from providers of vulnerability diagnosis and monitoring services, etc. and reflect them in countermeasures. It is necessary to work on securing and training the necessary human resources.
- Formulate a plan (BCP) to ensure that operations do not stop in the event of a system outage due to cybersecurity risks, acquire backups, and develop alternative means of operating.
- Educate employees on a regular basis and be prepared on a daily basis to respond appropriately to cybersecurity risks.

[21] For cloud service measures, see Appendix B (Reference Information on Cybersecurity Measures).

[22] Lists of services that meet Information Security Service Standards https://www.ipa.go.jp/security/it-service/service_list.html

Direction 6 Continuously improve cybersecurity measures through a PDCA cycle

- ● Operate a PDCA cycle based on the characteristics of cybersecurity risks in order to respond to changes in risks and continuously improve risk response in organizations and businesses.
- ● Management should strive to detect problems early on through regular reports on the status of countermeasures, and to make improvements if signs of problems are visible.
- ● Appropriately disclose the status of improvements in order to increase trust with shareholders and stakeholders.

Scenarios in case of no action

・Without a system to properly implement PDCA (Plan , Do , Check , Act , etc.), it may not be possible to make improvements in response to changes in risks (e.g. being unable to respond to new threats).

・If management does not receive regular reports, etc. and is not aware of risks and problems, appropriate security measures will not be implemented, and there is a risk of cyberattacks.

・A PDCA cycle that targets cybersecurity risks is characterized by the fact that cybersecurity risks can change rapidly compared to risks such as natural disasters and equipment failures. Unless the company operates within a structure that can respond to changes in the cycle, it will not be able to implement effective countermeasures.

・In the absence of continuous improvements, there is a high possibility that corporate value will be damaged through incidents caused by new risks. In addition, if companies do not disclose the status of their improvement efforts appropriately, they may lose the trust of stakeholders in their business response to cybersecurity risks from the perspective of corporate social responsibility.

Examples of recommended actions

・Develop a PDCA process and its implementation system to continuously respond to changes in cybersecurity risks .

- Ensure that the planning process reflects the latest risk treatment plan in Direction 4.
- When performing the Check, use "Appendix A" and the "Cybersecurity Management Visualization Tool" as a reference for checking items. Also evaluate whether the implemented measures are effective against the current risks.

・The PDCA process should be developed in a format that includes not only one's organization, but also relevant parties such as product vendors, etc. according to risk characteristics.

・If necessary, certify the PDCA management system through an international standard such as ISMS (based on the ISO/IEC 27001 standard).

・Key performance indicators (KPIs) for cybersecurity risk management. Report the status to management at the committee on management risk within the organization. As KPIs, the following indicators are conceivable from the viewpoint of evaluating performance within the organization regarding risk response.

- Amount of damage if countermeasures are not taken
- Service interruption time due to causes related to cybersecurity
- Attendance rate of cybersecurity training
- Average level of self-evaluation of skills of personnel engaged in cybersecurity measures
- Average level of self-evaluation of security maturity level in the organization

・If necessary, use external services[23] such as vulnerability diagnosis, penetration test, information security audit, etc. to manage cybersecurity risk, detect problems in the current system and cyber security measures, and make improvements.

・If additional measures are necessary due to the discovery of new cybersecurity risks, etc., promptly revise the response policy.

・In accordance with the nature and degree of cybersecurity risks, work on the disclosure of the status of cybersecurity measures via information security reports, CSR reports, sustainability reports, securities reports, etc., or via individual disclosures to supply chain stakeholders.

[23] When selecting external services, it is possible to select services that ensure a certain level of quality by using the ″Lists of services that meet Information Security Service Standards″ published by the Information technology Promotion Agency, Japan. https://www.ipa.go.jp/security/it-service/service_list.html

3.3. Establish a system to prepare for the occurrence of incidents

Direction 7 Develop a cybersecurity incident response team and relevant procedures

- ● Develop a system (CSIRT, etc.) that can respond to incidents throughout the supply chain, including the control system, in order to identify the extent of impact and damage, implement initial responses to prevent damage from spreading and consider measures to prevent recurrence in a timely manner.
- ● In addition to understanding who should be notified after damage is discovered and the information that needs to be disclosed, establish a system that enables management to provide explanations inside and outside the organization when disclosing information on damages.
- ● Conduct practical exercises as appropriate on incident response.

Scenarios in case of no action

・If an emergency response system is not in place, it will not be possible to communicate with relevant parties inside and outside the organization during efforts work to identify the cause, and prompt action will not be taken.

・In the event information is not disclosed promptly, there is a risk that customers and business partners will be harmed and the organization may be held responsible in claims for damages.

・If there are any legal agreements and obligations to report to the appropriate authorities, penalties may be applied in the absence of prompt notifications.

・If an unforeseen takes place , the person in charge will not be able to take appropriate action in the event of an emergency. As a result, it be difficult to bring the situation under control as soon as possible; additionally, the damage could spread and the impact could be prolonged.

Examples of recommended actions

・In order to establish a rapid response system to minimize damage in an emergency, establish a response system (CSIRT) that can address the following actions:.

- When building an incident response system, it is necessary to be conscious of how to respond to spillovers from outside the company or to other companies. In a highly networked supply chain, it is necessary to consider the myriad connections with external.
- If there is concern a cyber incident has occurred, the response system should enable prompt reporting to management and other concerned parties.
- In the event of damage from a cyberattack, in order to quickly identify and analyze the cause of the damage, establish a system that can promptly preserve evidence such as various logs and secure infected terminals, and facilitate investigations based on cooperation with relevant organizations. It is helpful to refer to "Appendix C Reference Information for Preparing for Cybersecurity Incidents" when investigating the causes of incidents.
- Conduct exercises that encompass the formulation of recurrence prevention measures post-incident

along with reporting procedures to the appropriate ministries and agencies.

- When considering the emergency response system, consider utilizing the knowledge of external experts as necessary.
- Prepare an emergency contact network (contacts for system operation, security vendors, etc.) and a list of information disclosure notification destinations, including those outside the company, and share them with members involved in response efforts.
- Consider what kind of business impact will occur at the time of the initial response and make arrangements in advance so that each department within the organization (general affairs, planning, sales, etc.) can cooperate promptly in an emergency.
- Check relevant laws and regulations and confirm the procedures in place to ensure fulfillment of legal obligations.
- Report the damage caused by the incident and the impact on other companies, etc. to management.

・With regards to products and services designed, developed, manufactured, provided, etc. by one's organization: Implement countermeasures in preparation for the occurrence of situations in which customers are disadvantaged due to vulnerabilities or failures in their software, and establish and operate a PSIRT[24] to investigate the cause and transmit information to counter such incidents.

・Refer to the "Guidance for Sharing and Disclosure of Information on Damage from Cyberattacks"[25] when developing systems and rules for incident response, and to deepen the company's understanding on this area.

・Regularly conduct emergency response drills in response to simulated cyber incidents for executives and employees, so that all relevant parties understand through experience what procedures should be followed in an initial response in an emergency.

- The subject of the exercise is not limited to information system incidents, but also includes incidents that affect control systems.
- Consider conducting exercises for projects other than incidents that may affect corporate activities (system migration, etc.).
- Consider the implementation of exercises across companies, not limited to within one company.
- If it is not possible to obtain knowledge within the company on what to do in exercises, use external training courses, etc. that include exercises.

[24] Here, PSIRT (Product Security Incident Response Team) is shown as an organization that targets products, but there are also FSIRT (for factories), DSSIRT and SSIRT (for factories). It is appropriate to consider building and operating a cybersecurity incident response organization according to the business content of the organization.

[25] For details, see "Guidance for Sharing and Announcing Information concerning Damage from Cyberattacks" described in Appendix B (Reference Information on Cybersecurity Measures).

Direction 8 Develop a business continuity and recovery team and relevant procedures in preparation for damage due to cyber incidents

- ● In the event of business suspension due to an incident, identify the date by which recovery should be achieved (considering the impact on business management), formulate a procedure manual for recovery, and establish a recovery response system.
- ● Establish an effective and consistent recovery objective plan for the entire organization, such as cooperation with the BCP, to include the control system.
- ● Conduct practical exercises on recovery response after the suspension of business operation that include the supply chain, without limiting the parameters to IT systems, internal companies, and incidents.

Scenarios in case of no action

・If important operations cannot be restored within an appropriate time, there is a risk of serious damage to customers and fatal impact on the company's management.

・With the increasing dependence of business on the digital environment, it may not be possible to resume business simply by restoring the IT environment. From the perspective of business continuity for an organization, it is necessary to prepare a restoration plan and system for the digital environment that is consistent with the business restoration process.

・Without having exercised response measures, the person in charge will not be able to take the appropriate step in an emergency when an unforeseen situation occurs.

Examples of recommended actions

・Establish a recovery system that can implement the following in the event of business suspension.

－In order to be able to recover quickly in the event of a cyberattack that results in a suspension of business, predetermine the items to be confirmed in order to prevent recurrence and specific recovery procedures as part of a recovery plan. Additionally, consult with relevant organizations to determine a cooperation framework to utilize during recovery periods.

- The company as a whole should coordinate to set goals for when important operations should be restored by (e.g. consistent with goals set in the BCP).

・When drafting a capital investment plan, add cyber security risks to factors that affect business continuity such as natural disasters, pandemics, etc. and include countermeasures in the required specifications.

・Periodic recovery drills will help those involved in the recovery process understand the procedures through experience.

- The subject of the exercise is not limited to information system incidents, but also includes incidents that affect control systems.

- Consider conducting exercises for projects other than incidents that may affect corporate activities (system migration, etc.).
- Consider the implementation of exercises across companies versus internal exercises limited to a single company.
- If it is not possible to obtain knowledge within the company on what to do in exercises, use external training courses, etc. that include exercises.

* Directions 7 and 8 mention exercises on incident response and recovery respectively. Companies should consider whether to execute them separately or together based on the content of the drills and the roles of the relevant parties of the organization.

3.4. Drive security measures in the supply chain

Direction 9 Understand the status of and implement measures considering the entire supply chain, including business partners and outsourcing organizations

- ● To ensure that appropriate cybersecurity measures are taken throughout the supply chain, it is necessary to comprehend the status of measures, including domestic and overseas bases, business partners, and system management contractors.
- ● In contracts with business partners, clarify respective roles and responsibilities in dealing with cybersecurity risks, and consider appropriate measures to increase the effectiveness of measures throughout the supply chain, such as supporting the introduction or joint implementation of measures.

Scenarios in case of no action

・If appropriate cybersecurity measures are not taken at domestic and overseas bases of one's own company, affiliated companies, and domestic and overseas business partners in the supply chain, the perpetrator of a cyberattack may target the company through these entities. As a result, there is a risk of inducing secondary damage to other companies and becoming a perpetrator[26]. In addition, when identifying the cause of an emergency, the lack of cooperation from these companies hinders business continuity.

・In outsourced work such as system management, the boundary between the portion handled by one's own organization and the portion to be outsourced becomes unclear, and necessary measures may not be implemented.

・The ways in which companies are connected are diversifying(e.g. using external services such as the cloud, and connecting other companies' systems with their own systems through API linkage). In this type of environment, simply requiring the protection of information provided to the other party (as in the case of conventional security measures surrounding product orders), is insufficient as a countermeasure against cybersecurity risks originating from the supply chain.

・As a result of not considering risks such as geopolitical risks and natural disasters when selecting outsources, the business will be forced to stop operations unexpectedly.

Examples of recommended actions

・According to the circumstances of each industry, the division of roles within the supply chain, and the ability of the other party to respond, implement measures such as those listed below:

- Based on the agreement of companies participating in the supply chain, each company will establish cybersecurity measures to be implemented, and ensure their effectiveness through audits or self-inspections.
- Through methods such as clarifying who is responsible for cybersecurity measures in the contract, each company understands the role it should play and prevents omissions in measures.

[26] See Appendix B (Reference Information on Cybersecurity Measures) for measures to avoid becoming a perpetrator.

- If it is not possible to change the company's cybersecurity measures as stipulated in the terms and conditions of the other party, procure or contract cybersecurity features after confirming that the residual risk in the company if the terms and conditions are applied is within the allowable range.
- Define measures to be implemented according to the rank of confidentiality and importance of information handled in the supply chain. Prevent measures from becoming a mere formality and do not implement excessive measures.
- Share information on cyber security risks within the supply chain.

・Confirm that affiliated companies, supply chain business partners, system management contractors, etc. are implementing "SECURITY ACTION"[27]. It is more effective to have a security management certification such as ISMS[28] in place.

・When selecting contractors, consider not only costs, systems, and technical capabilities, but also the influence of environmental risks (natural disasters, pandemics, etc.), geopolitical risks (terrorism, political instability, etc.), and economic risks (economic crises and fluctuations in raw material prices). etc.).

・Utilize measures for supporting SMEs such as "Cybersecurity Supporters Services"[29] as a means of raising the minimum cybersecurity measures utilized in the supply chain.

・Recommend subcontractors enroll in cyber insurance[30] as a means of compensating for damage stemming from subcontractors in preparation for emergencies.

・When contracting out work from other companies, comply with security-related requirements such as the handling of information agreed with the outsourcer at the time of contract.

・As a means of ensuring cybersecurity measures in the supply chain, use the results of evaluation and verification by third parties (utilization of certification systems, implementation of advisory-type external audits, etc.).

[27] A program for SMEs to declare the implementation of essential security measures by themselves.
https://www.ipa.go.jp/security/security-action/

[28] Even if a business partner has not acquired ISMS certification, it can be considered, for example, confirming that the certification of Technology Information Control System has been acquired.
https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html

[29] Essential cybersecurity services for SMEs including inquiry counter, monitoring of systems, emergency support, and simple cyber insurance.
https://www.ipa.go.jp/security/otasuketai-pr/

[30] Cyber insurance can be a means of financial compensation for damages caused by cyber security incidents such as information leaks. However, it is necessary to consider that in some cases the entire damage is not covered by compensation, and that in the case of a national level attack, it may be treated as a war and not covered by compensation.

3.5. Drive communication with stakeholders and other relevant parties

Direction 10　Facilitate the gathering, sharing and disclosure of information on cybersecurity

- ● Based on the awareness that it is necessary to provide appropriate information in order to obtain useful information, build relationships to share information on cyberattacks and measures, and prepare to report and publicize damage.
- ● Create an environment for effective utilization of the information obtained.

Scenarios in case of no action

・By participating in information sharing activities, it is possible to prevent similar damage in other companies by using information such as analyzed attack methods. Conversely, in the absence of information-sharing, new attack information cannot be obtained. This leads to delays in countermeasures and an increase in the risk of being targeted.

・If a company is not prepared to engage in incident response, a company may end up violating domestic and foreign laws and regulations by virtue of being unable to comply with the obligation to report information leaks to the applicable ministries and agencies in the event of a cybersecurity incident, or carry out the timely disclosure required of listed companies. In addition, failure to disclose information appropriately creates a sense of distrust amongst shareholders and business stakeholders.

Examples of recommended actions

・It is important for society as a whole to protect against cyberattacks through two-way information sharing, such as obtaining and providing information. In order to prevent cyberattacks through information sharing, it is necessary not only to obtain information, but also to actively provide information.

・Actively disclose information (e.g. daily efforts to prepare for cyber security incidents at opportunities such as dialogues with shareholders and stakeholders and disclose information to the general public through public relations.

・Refer to the "Guidance for Sharing and Announcing Information concerning Damage from Cyberattacks" to understand in advance the perspectives for sharing information with specialized cybersecurity organizations and disclosing information related to damage in preparation for incidents.

・Use alert information such as vulnerability information from IPA and the JPCERT Coordination Center, and communication with security-related products and services providers for cybersecurity measures.

・Share information among CSIRTs and collect information through participation in community activities such as the Japan CSIRT Association and industry-specific security information sharing organizations (ISAC), etc., and use them for cyber security measures.

・Report malware information and unauthorized access information to IPA based on notices (computer virus countermeasure standards, computer unauthorized access countermeasure standards).

- Provide information on the incident to the JPCERT Coordination Center and request coordination as necessary.
- In the case of critical infrastructure operators, use information sharing mechanisms such as J-CSIP .
- On a daily basis, proactively cooperate with external businesses involved in their own business, such as the providers of server system and website developers, regarding the sharing of cybersecurity-related information.
- In the case of small and medium-sized enterprises, secure partners with whom information can be shared locally through chambers of commerce, associations of commerce and industry, etc.

Appendix A: Check sheet of cybersecurity management

Appendix A-1 Check Sheet for "Three principles which management needs to recognize"

* This check sheet is supposed to be self-conducted by management, but it does not require that management directly manage all of the items covered, as roles and authority are delegated according to the size of the company, group composition, etc. In such instances, it is appropriate to confer with the person responsible for cybersecurity to complete the check sheet and understand the contents.

* If it is difficult for management to confirm the contents of the check sheet, it is possible to use it as a communication tool. For instance, management could have the CISO, who receives directions from management, confirm the details of the company's cybersecurity efforts, and use them to explain these efforts to management.

(1) Corporate executives need to recognize that cybersecurity risk is an important issue in their company's risk management and take measures at their level to address this.

□ Management positions cybersecurity risk as one of the key risks to be considered in various business decisions of the company and recognizes the need for security investments to ensure business continuity.

□ Management recognizes that it is their responsibility to reduce risks to acceptable levels through the implementation of cybersecurity measures.

□ Management regularly checks to ensure that the instructions given as measures to address cybersecurity risks are being implemented appropriately, and if they are not being implemented, management is not negligent in urging action.

(2) In order to fulfill the responsibility of ensuring cybersecurity, it is necessary to pay attention to cybersecurity measures not only for the company itself but also for the entire supply chain, including domestic and overseas bases, business partners and outsourcing organizations.

□ Management recognizes that connections through diverse supply chains that are not restricted to order-receiving relationships can have a significant impact on the cybersecurity of the company and society.

□ When considering their own risk management, management confirms that the scope of identifying cybersecurity risk factors includes group companies and even outsourced contractors.

□ In order to reduce cybersecurity risks throughout the supply chain understanding that any company has the potential a perpetrator, and that each company needs to implement comprehensive security measures management, confirms the state of implementation of these measures.

(3) Active communication with relevant parties is necessary to implement effective cybersecurity measures in both normal times and emergencies.

□ Management is prepared for an appropriate response in the event of an incident and is mindful of practicing communication on cybersecurity risks with relevant parties in normal times.

□ Management knows who is responsible for dealing with cybersecurity incidents within the company and is prepared to communicate appropriately in an emergency.

□ Management understands what information should be disseminated to maintain the trust of external stakeholders when cybersecurity incidents occur at their companies or contractors.

Appendix A-2 Check Sheet for "Ten important items of cybersecurity management"

* The subject of this check sheet is the implementation status of the items instructed by management, and it is appropriate for practitioners to run the check sheet according to the size of the company and for management to confirm the results.

* Based on the items in this check sheet, the following tools are provided to support visualization of the implementation status of the Directions in the Cybersecurity Management Guidelines.

[Cybersecurity Management Visualization Tool] (IPA)
https://www.ipa.go.jp/security/economics/checktool/index.html

* This check sheet covers basic items. It is also important to take additional measures according to the company's situation.

* Going forward, the relationship between these check sheet items and the NIST Cybersecurity Framework[31] will also be include and displayed. (The information in brackets corresponds to the subcategory identifiers in the NIST Cybersecurity Framework.).

Direction 1 Recognize cybersecurity risks and develop an organization-wide policy

□ Management recognizes cybersecurity risk as one of the management risks they are responsible for. (-)

□ Management formulates and declares a basic cybersecurity policy that considers the cybersecurity risks of the organization as a whole. (ID.GV-1)

□ Management understands the requirements of laws, contracts and guidelines, and has these requirements reflected in basic policies, etc. (ID.GV-3) (DE.DP-2)

Direction 2 Build a management system for cybersecurity risk

□ A structure for cybersecurity risk management consisting of a CISO, etc. has been established based on the organization's foundational policy. (ID.GV)

□ The roles and responsibilities of each stakeholder in managing cybersecurity risk are clear. (ID.GV-2)

□ The relationship between the risk management system for governance, internal control, and business continuity within the organization and the cyber security risk management system is clear. (ID.GV-4)

Direction 3 Secure resources (budget, workforce, etc.) for cybersecurity measures

□ Cybersecurity measures and resources (budget, human resources, etc.) that can implement them through discussions at management meetings, etc. have been clarified. (ID.AM)

□ With regard to cybersecurity measures, there is an appropriate separation between the portion that is handled by the organization itself and the portion that is outsourced. (ID.BE-3) (ID.BE-4) (ID.SC-2)

[31] For detail of the NIST Cybersecurity Framework, see Appendix B (Reference Information on Cybersecurity Measures).

□ The requirements for security personnel the organization seeks are clear, the organization has secured and developed cybersecurity personnel in a systematic way, and is treating cybersecurity personnel in a satisfactory manner. (PR.AT-1) (PR.AT-2) (PR.AT-3) (PR.AT-4) (PR.AT-5)

□ Acquisition of cybersecurity knowledge and skills has been implemented for personnel responsible who are in roles of "Plus-Security". (PR.AT-1) (PR.AT-5)

□ For the portion of cybersecurity to be outsourced, appropriate external resources are selected and utilized in consideration of the company's own issues, budget, location, etc. (ID.BE-3) (ID.BE-4) (ID.SC-3) (ID.SC-4)

Direction 4 Identify cybersecurity risks and develop plans to address them

□ Digital environments, services and information to be protected are identified and measures are prioritized based on the location, business value and other aspects of the asset. (ID.AM-1) (ID.AM-2) (ID.AM-3) (ID.AM-4) (ID.AM-5)

□ Threats of and vulnerabilities to cyberattacks (including negligence and internal impropriety) against the digital environment, services and information to be protected have been identified, and the company understands how these cybersecurity risks affect its business. (ID.RA-1) (ID.RA-3) (ID.RA-4) (ID.RA-5) (ID.RM-1) (ID.RM-2)

□ A risk response plan based on risk assessment results has been developed. (ID.RA-3) (ID.RA-6)

Direction 5 Establish systems to effectively address cybersecurity risks

□ Asset, configuration, and patch management of critical systems are performed. (PR.IP-1) (PR.IP-2) (PR.IP-3) (PR.PT-3)

□ Measures have been taken to prevent the use of shadow IT within the organization. (PR. AC)

□ Risk assessment is performed at the time a system in being designed, and necessary security features are embodied and implemented at development time. (ID.RA-6) (ID.RM-3)

□ Multiple technical measures are implemented for terminals, servers that perform critical tasks. (PR.AC) (PR.DS) (PR.PT-1) (PR.PT-2) (PR.PT-3)

□ Multiple technical measures are put in place for networks that perform critical tasks. (PR.AC) (PR.DS) (PR.PT-4)

□ Plans are made and implemented for vulnerability countermeasures, such as regular vulnerability checks for systems, continuous patching and other mitigation measures. (PR.IP-12) (DE.CM-8) (RS.MI-3)

□ Logs from terminals and networks are being collected and analyzed. (PR.MA-1) (PR.MA-2)

□ Incident response mechanisms have been introduced, such as blocking communications when a cyberattack is detected. (DE.AE) (DE.DP)

□ Incident management mechanisms are in place. (PR.IP-9)

□ Cyber security education and exercises are conducted for employees. (PR.AT-1)

Direction 6 Continuously improve cybersecurity measures through a PDCA cycle

□ KPIs for cybersecurity operations management are defined. (ID.RM-1) (ID.RM-2) (ID.RM-3)

□ Management regularly receives reports on the implementation status of cybersecurity measures, discusses them, and gives directions. (ID.GV)

□ Cybersecurity audits have been conducted and, based on the results, cybersecurity measures are being reviewed in a timely manner. (PR.IP-7) (RP.PT-1)

□ There is communication with stakeholders about the state of action against cybersecurity risks. (ID.SC) (RS.CO-3) (RS.CO-4) (RS.CO-5)

Direction 7 Develop a cybersecurity incident response team and relevant procedures

□ An incident response plan is developed that considers the entire supply chain. (PR.IP-9) (RS.RP-1) (RS.IM-1) (RS.IM-2) (RS.AN-4)

□ A dedicated team for incident response (CSIRT etc.) has been established and is being maintained. (RS.CO-1)

□ The content and timing to be shared/reported/published outside the organization are specified. (RS.CO-2) (RS.CO-1)

□ Emergency response exercises are conducted regularly in the event of an incident. (PR.IP-10)

□ An implementation plan has been developed to enable rapid log analysis and investigation at the time of an incident and to identify the scope of impact. (PR.MA-1) (PR.MA-2) (PR.PT-1) (RS.AN-4)

Direction 8 Develop a business continuity and recovery team and relevant procedures in preparation for damage due to cyber incidents

□ A business recovery plan considering the entire supply chain in the event of damage has been developed. (ID.BE-5) (PR.IP-9) (RC.RP-1) (RC.IM-1) (RC.IM-2)

□ Exercises to deal with recovery are conducted regularly. (PR.IP-10) (RC.CO)

Direction 9 Understand the status of and implement measures considering the entire supply chain, including business partners and outsourcing organizations

□ The state of countermeasures against cybersecurity risks in transactions and collaborations with group companies is understood. (ID.RA) (ID.BE-1)

□ It has been confirmed that appropriate measures have been taken based on the roles and areas of responsibility regarding cybersecurity risks agreed upon in contracts with business partners such as contractors. (ID.AM-6) (ID.BE-1) (ID.SC)

□ It has been confirmed that cybersecurity risk does not exceed acceptable levels across the supply chain affecting the company’s business. (ID.RA-5) (ID.SC)

Directive 10 Facilitate the gathering, sharing and disclosure of information on cybersecurity

□ Information is shared through the acquisition of warning information provided by related organizations and participation in the industry's security community, etc., and is being utilized for the company's own countermeasures. (ID.RA-2) (RS.AN-5)

□ When there is an incident such as a malware infection or unauthorized access, incident information is shared and reported to related organizations and communities, and provided for reference through appropriate publication. (RS.CO)

Appendix B: Reference information on cybersecurity measures

The information sources and materials that will serve as a reference for implementing “the ten items of importance” in these guidelines in departments in charge of cybersecurity measures are shown below. Since these may be updated, efforts should be made to refer to the latest version as appropriate.

General Reference Material

○ Cybersecurity Portal Site (National Cyber Security Center (NISC))

(Houses a variety of information disseminated by relevant organizations for the purpose of spreading awareness and developing human resources, targeting the management level of companies.)

https://security-portal.nisc.go.jp/curriculum/classified/6office_exe.html

○ Cybersecurity contents for business management (IPA)

(As part of the activities of the Supply Chain Cybersecurity Consortium (SC3) Attack Trend Analysis and Countermeasures Working Group, IPA interviews corporate executives implementing cybersecurity measures and posts columns explaining security themes that managers should be aware of, etc.)

https://www.ipa.go.jp/security/sc3/activities/kougekiWG/content/

○ Information Security Guidelines for SMEs [3rd Edition] (IPA)

(Guidelines explaining considerations for small and medium-sized enterprises to undertake security measures. It includes appendices such as the Five Articles of Information Security which lay out the minimum cybersecurity measures required, security policy samples, the Five-Minute Information Security Self-Diagnosis and guidance for safe use of cloud computing services.)

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

○ Q&A Handbook on Cybersecurity Laws and Regulations [Ver1.0] (NISC)

(In addition to legal matters related to cybersecurity measures in normal times and responses to incidents in companies, legal issues arising from changes in laws and circumstances, etc., related to the handling of information are described in plain language as much as possible.)

https://security-portal.nisc.go.jp/law_handbook/

○ ISO/IEC 27002:2022 (ISO/IEC)

(The international standard which sets the specifications for information management systems. It provides the best practices in information security management.)

○ Framework for Improving Critical Infrastructure Cybersecurity [Version 1.1] (NIST)

(US guidelines dividing cybersecurity measures that companies involved with critical infrastructure should implement into the five functions of "identify," "protect," "detect," "respond," and "recover," the functions of which are further divided into 22 categories. This framework can be utilized by companies other than those engaged with critical infrastructure as well.)

https://www.nist.gov/cyberframework/framework (Parallel translation) https://www.ipa.go.jp/files/000071204.pdf

○ SP800-53 [Rev.5] (NIST)

(US guidelines outlining security measures that federal agencies should implement. When providing cloud services to the US federal government, compliance with these guidelines may be required.)

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

○ SP800-161 [Rev.1] (NIST)

(Guidance for identifying, assessing, and mitigating cybersecurity risks across the supply chain at all levels of an organization.)

https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

○ SP800-171 [Rev.2] (NIST)

(US guidelines outlining security measures that should be implemented by organizations other than federal agencies and to protect CUI.[32] When being contracted to do work for the US federal government, compliance with these guidelines may be required.)

https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

○ CIS Controls [Version 8] (Center for Internet Security)

(A categorized set of high-priority controls for organizations to implement. It is updated regularly by a non-profit organization in which U.S. security-related public and private organizations participate. The target organizations are categorized into three levels, ranging from small and medium-sized enterprises to organizations with security experts.)

https://www.cisecurity.org/controls

Reference material related to “Three principles which management needs to recognize”

○ Cyber Risk Handbook for Japanese Corporate Directors（Nippon Keidanren）

（Five principles on cybersecurity presented in the literature on cyber risk published for directors in the United States and the United Kingdom respectively, translated and organized for Japanese companies.)

https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.html

Reference material relating to Directives 2 and 3

○ Guidebook for Establishing Cybersecurity Organization and Securing Necessary Human Resources (Ministry of Economy, Trade and Industry (METI))

(As Appendix F of these guidelines, this guidebook explains matters to be considered in

[32] An abbreviation for Controlled Unclassified Information. CUI indicates important information that should be controlled, but for which the federal government has not prescribed special classifications such as secret, top secret, or confidential.

establishing a cybersecurity system and securing and developing human resources, as well as how to implement these issues.)
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

Reference material relating to Directives 3

- ○ Guide for developing human resources in charge of information security with the use of IT skill index (IPA)

  (Guidelines illustrating what kind of measures are necessary to prevent cyberattacks, what kind of human resources are necessary to implement such measures, and summarizing tips for training human resources.)

  https://www.ipa.go.jp/files/000039528.pdf

- ○ Skill-up guide for information security administrators at the workplace [September 2015] (IPA)

  (Guidelines illustrating what kind of measures should be implemented for security threats and preventing damage, and outlining the specific role of security administrators.)

  https://www.ipa.go.jp/files/000047872.pdf

Reference material relating to Directives 4

- ○ Cyber Physical Security Framework [Ver1.0] (METI)

  (Present guidelines addressing how to deal with new risks that industry’s activities in the environment of “Society 5.0”—where new value is created by the fusion of cyberspace and physical space, with an increase in sources of cyberattacks and the impact of damage on physical space—face.)

  https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html

- ○ Recent vulnerability information, etc. (IPA)

  (Providing information on security issues and countermeasures that pose a high risk of unauthorized access or data theft if left unattended.)

  https://www.ipa.go.jp/security/announce/alert.html

Reference material related to Direction 5

- ○ Examination and Registration Authority Standards for Information Security Services (METI)

  (The lists of services are published as lists of services that meet the technical requirements and quality control requirements stipulated by the Information Security Service Standards.)

  https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html

- ○ System design guide for responding to 'Advanced Targeted Attack' [September 2014] (IPA)

  (Guidelines that explain internal countermeasures for a targeted attack to prevent the spread of the breach and to strengthen surveillance, give the premise that an internal breach has already occurred.)

https://www.ipa.go.jp/files/000046236.pdf

○ How to use and analyze logs in dealing with advanced cyberattacks [version 1.2] (JPCERT/CC)

(Guidelines that describe the concept of implementing a function that can be utilized normally which leaves traces of the activities of a cyberattacker, methods of finding traces from those logs, etc.)

https://www.jpcert.or.jp/research/apt-loganalysis.html

○ Guidelines for the Prevention of Internal Misconduct in Organizations [5th Edition] (IPA)

(Guidelines that present 30 measures based on 10 perspectives (compliance, work environment, etc.) as measures to be taken to prevent internal misconduct in organizations.)

https://www.ipa.go.jp/security/fy24/reports/insider/

○ Handbook for Protecting Confidential Information [May 2020] (METI)

(Handbook that collects and introduces examples of measures to prevent leaks of confidential information.)

https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

○ Information security management guidelines for use of cloud computing services (METI)

(Provides advice on selecting and implementing appropriate management measures from JIS Q 27002 for risk management related to the use of cloud services and guidance for their optimal implementation.)

https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

○ Guidebook for utilizing information security management guidelines for the use of cloud computing services (METI)

(Guidebook based on actual incidents in cloud services and various security issues that businesses face. Explains the risks and security measures related to cloud services as IT services for both businesses and users.)

https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf

○ Information security measures for the use of cloud computing services (Ministry of Internal Affairs and Communications)

(Describes what companies and organizations should confirm when selecting providers and services in the case of using public cloud services.)

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_admin_15.html

Reference material related to Direction 6

○ Information Security Management System (ISMS) Conformity Assessment System (JIPDEC)

(A scheme for third-party certification for information security management systems based on international standard ISO/IEC27001)

https://isms.jp/isms.html

○ Cyber Security Management System (CSMS) Conformity Assessment System (JIPDEC)

(A scheme for third-party certification for cyber security management systems based on international standard IEC62443-2 targeting industrial automation and control systems.)

https://isms.jp/csms.html

○ Information Security Management Standards (Ministry of Economy, Trade and Industry)

(Comprehensive standards covering the establishment of information security management to concrete management measures that are consistent with international standard ISO/IEC27001.)

https://www.meti.go.jp/policy/netsecurity/is-kansa/index.html

○ Information Security Measures Benchmark (IPA)

(A tool to display a company's status of implementation of security measures as a scatter diagram, radar chart, scores, etc., by answering questions online. It also allows companies to compare their status of measures with that of other companies.)

https://www.ipa.go.jp/security/benchmark/

○ How to Secure Your Website [7th Edition] (IPA)

(Guidelines presenting technical measures to create a website that takes security into account. A supplementary volume also provides online health diagnosis specifications presenting test items to check a website for vulnerabilities.)

https://www.ipa.go.jp/security/vuln/websecurity.html

○ Japan Vulnerability Notes (JVN) (IPA, JPCERT/CC)

(A portal site for measures against vulnerabilities, which provides information on vulnerabilities in software used in Japan and countermeasures.)

https://jvn.jp/

○ Handbook on Disclosures of Information on Cybersecurity Measures (Ministry of Internal Affairs and Communications)

(Examples of disclosure items related to cybersecurity measures in disclosure documents and a collection of examples of disclosure documents that have already been made public are included as reference materials for companies considering how to disclose information.)

https://www.soumu.go.jp/main_content/000630516.pdf

Reference material related to Direction 7

○ CSIRT Materials (Concept, Establishment, and Operation) (JPCERT/CC)

(Guidelines explaining points to take into account at the "initiative phase," "establishment phase," and "operation phase" respectively for establishing a CSIRT in order to conduct systematic incident response.)

https://www.jpcert.or.jp/csirt_material/

○ Reference materials useful for building a CSIRT (Nippon CSIRT Association)

(A collection of reference materials for each stage of establishing a CSIRT. Meant for beginners, for explaining the process to managers, and to provide information in each step of the planning, construction, and operation process for persons in charge of establishing a CSIRT.)

https://www.nca.gr.jp/ttc/wtda.html

https://www.nca.gr.jp/activity/build-wg-document.html

○ Guidance for Sharing and Announcing Information concerning Damage from Cyberattacks (NPA, the Ministry of Internal Affairs and Communications, METI, NISC, JPCERT/CC)

(Guidance materials aiming to revitalize information sharing on cyberattack damage. Outlines key points for smooth and effective information sharing while ensuring the protection of affected organizations.)

https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

Reference material related to Direction 8

○ Business Continuity Guidelines [Revised in April 2021] (Cabinet Office)

(Guidelines which clarify the necessity of business continuity and present items for which implementation is necessary and items for which implementation is recommended for the development and revision of a business continuity plan.)

https://www.bousai.go.jp/kyoiku/kigyou/keizoku/pdf/guideline202104.pdf

Reference material related to Direction 9

○ Building partnerships with business partners to strengthen cybersecurity of whole supply-chains (METI, Japan Fair Trade Commission)

(A summary of measures to support cybersecurity measures at small and medium-sized enterprises and the application of relevant laws and regulations to support and request measures from business partners.)

https://www.meti.go.jp/policy/netsecurity/index.html#partnership

○ Guidelines on the promotion of the improvement of subcontracting transactions in information service/software industry [March 2017] (METI)

(Guidelines developed for the purpose of promoting fair subcontracting transactions, which explains items to take into account for efforts related to personal information protection and security measures.)

https://www.chusho.meti.go.jp/keiei/torihiki/2014/140313shitaukeGL3.pdf

○ Technology Information Control System (METI)

(A system that certifies companies' efforts to manage information, covering all information forms, including paper.)

https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html

○ Security Self-Declaration program for SMEs "SECURITY ACTION" (IPA)

(A program for small and medium-sized companies to declare their commitment to security measures.)

https://www.ipa.go.jp/security/security-action/

○ Cybersecurity Supporters Services (IPA)

(Essential cybersecurity services for SMEs including monitoring of systems, emergency support, and cyber insurance.)

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

Reference material related to Direction 10

○ Report, Consult, and Share Information (Report Unauthorized Access, Viruses, Etc.) (IPA)

（A website that provides report templates, report contacts, and report statuses for reports on malware such as computer viruses, unauthorized access, and vulnerabilities.)

https://www.ipa.go.jp/security/outline/todoke-top-j.html

○ Special help desk for targeted cyberattacks (IPA)

(A consultation desk for expert counselors to consult after receiving a targeted cyberattack.)

https://www.ipa.go.jp/security/tokubetsu/

○ Initiatives for Cyber Security Information sharing Partnership of Japan (J-CSIP) (IPA)

（An initiative to share information and conduct early response in critical infrastructure equipment manufacturing, electricity, gas, chemical, oil, resource development, automotive, and credit industries.)

https://www.ipa.go.jp/security/J-CSIP/

○ Incident reporting (JPCERT/CC)

(Incident response activities related to Japan include receiving reports on incidents, supporting responses, grasping the status of occurrence, analyzing modus operandi, and giving advice to prevent recurrence.)

https://www.jpcert.or.jp/menu_reporttojpcert.html

○ @police (National Police Agency)

(A website that provides various information related to network security, in order to prevent cybercrimes and cyber terrorism as well as prevent damage from cybercrimes and cyber terrorism from spreading.)

https://www.npa.go.jp/cyberpolice/

Appendix D: Relationship with relevant standards and frameworks

* This table provides reference information for practitioners who practice the "Ten important items of cybersecurity management", showing the correspondence between international standards (ISO/IEC 27000 series) and cybersecurity-related frameworks used by companies.

Ten important items	ISO/IEC 27001:2022 (●), ISO/IEC 27002:2022 (・)		NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1		CIS Critical Security Controls Version 8	
Direction 1: Recognize cybersecurity risks and develop an organization-wide policy	●5.1	Leadership and commitment	ID.GV	Governance	-	-
	●5.2	Policy				
	●7.3	Awareness				
	・5.1	Policies for information security				
	・5.4	Management responsibilities				
Direction 2: Build a management system for cybersecurity risk	●5.3	Organizational roles, responsibilities and authorities	ID.BE	Business Environment	-	-
	・5.2	Information security roles and responsibilities				
	・5.3	Segregation of duties				
Direction 3: Secure resources (budget, workforce, etc.) for cybersecurity measures	●7.1	Resource	ID.AM	Asset Management	14	Security Awareness and Skills Training
	●7.2	Competence	PR.AT	Awareness and Training		
Direction 4: Identify cybersecurity risks and develop plans to address them	●6.1	Actions to address risks and opportunities	ID.RA	Risk Assessment	01	Inventory and Control of Enterprise Assets
	●6.2	Information security objectives and planning to achieve them	ID.RM	Risk Management Strategy		
	●8.2	Information security risk assessment			02	Inventory and Control of software Assets
	●8.3	Information security risk treatment			04	Secure Configuration of Enterprise Assets and Software
	・5.7	Threat intelligence				
	・5.9	Inventory of information and other associated assets				
	・5.10	Acceptable use of information and other associated assets				
	・5.12	Classification of information				
	・5.32	Intellectual property rights				
Direction 5: Establish systems to effectively address cybersecurity risks	●7.5	Documented information	PR.AC	Identity management and Access Control	03	Data Protection
	・5.13	Labeling of information	PR.DS	Data Security	05	Account Management
	・5.14	Information transfer	PR.IP	Information Protection Processes and Procedures	06	Access Control Management
	・5.15	Access control			09	Email and Web Browser Protections
	・5.16	Identity management	PR.PT	Protective Technology	10	Malware defenses
	・5.17	Authentication information			12	Network Infrastructure Management
	・5.18	Access rights			16	Application Software Security
	・5.33	Protection of records				
	・5.34	Privacy and protection of PII				
	・5.37	Documented operating procedures				
	・6	People controls				
	・7	Physical controls				
	・8	Technological controls				

Ten important items	ISO/IEC 27001:2022 (●), ISO/IEC 27002:2022 (・)		NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1		CIS Critical Security Controls Version 8	
Direction 6: Continuously improve cybersecurity measures through a PDCA cycle	●7.4	Communication	PR.MA	Maintenance	07	Continuous Vulnerability Management
	●8.1	Operational planning and control	DE.AE	Anomalies and Events	08	Audit Log Management
	●9.1	Monitoring, measurement, analysis and evaluation	DE.CM	Security Continuous monitoring	13	Network Monitoring and Defense
	●9.2	Internal audit	DE.DP	Detection Processes	18	Penetration Testing
	●9.3	Management review				
	●10.1	Continuous improvement				
	●10.2	Nonconformity and corrective action				
	・5.8	Information security in project management				
	・5.11	Return of assets				
	・5.31	Legal, statutory, regulatory and contractual requirements				
	・5.35	Independent review of information security				
	・5.36	Compliance with policies, rules and standards for information security				
Direction 7: Develop a cybersecurity incident response team and relevant procedures	・5.24	Information security incident management planning and preparation	RS.RP	Response Planning	17	Incident Response Management
			RS.AN	Analysis		
	・5.25	Assessment and decision on information security events	RS.MI	Mitigation		
	・5.26	Response to information security incidents	RS.IM	Improvements		
	・5.27	Learning from information security incidents				
	・5.28	Collection of evidence				
Direction 8: Develop a business continuity and recovery team and relevant procedure in preparation for damage due to cyber incidents	・5.29	Information security during disruption	RC.RP	Recovery planning	11	Data Recovery
	・5.30	ICT readiness for business continuity	RC.IM	Improvements		
Direction 9: Understand the status of and implement measures considering the entire supply chain, including business partners and outsourcing organizations	●8.1	Operational planning and control	ID.SC	Supply Chain Risk Management	15	Service Provider Management
	・5.19	Information security in supplier relationships				
	・5.20	Addressing information security within supplier agreements				
	・5.21	Managing information security in the ICT supply chain				
	・5.22	Managing the monitoring, review and change of supplier services				
	・5.23	Information security for use of cloud services				
Direction 10: Facilitate the gathering, sharing and disclosure of information on cybersecurity	・5.5	Contact with authorities	RS.CO	Communications	-	-
	・5.6	Contact with special interest groups	RC.CO	Communications		

Appendix E: Definitions of Terms

The terms and abbreviations used in these guidelines are defined below.

1) Encryption

The conversion of data via a prescribed calculation process such that the contents of the data cannot be known by anyone other than those who know the encryption key. Whether or not the encrypted data can be decrypted by a third party depends on the length and complexity of the information used as the encryption key and the mathematical strength of the calculation method.

2) Incident

A state of affairs in which a cybersecurity risk is realized or materialized.

3) Tampering detection

Using encryption technology to technically determine whether certain data has been tampered with by a third party.

4) Audit

A systematic, independent and documented process for collecting evidence and objectively determining whether or not cybersecurity measures are appropriately implemented in an organization. An audit can be executed either internally (primary) or externally (secondary or tertiary) or through a combination of internal and external audits.

5) Cyber space

A virtual space that encompasses a computer system or network.

6) Cyberattack

Any attack with malicious intent which illegally infiltrates a computer system or network to steal, destroy, or execute an unauthorized program.

7) Cybersecurity

Efforts to prevent information leaks or IT system malfunctions which occur due to cyberattacks.

8) Cybersecurity risk

The probability of negative impact on business management resulting from the occurrence of cybersecurity-related problems.

9) Cyber Physical Security Framework (CPSF)

Guidelines for dealing with new risks faced by activities that create added value, based on the fact that they involve new risks different from those in the past, in the environment surrounding industrial society in "Society 5.0" where new value is created by the fusion of cyberspace and physical space, expandsion of the starting point of cyberattacks, and increase in the impact of damage on physical space.

10) Supply chain

Though a "supply chain" traditionally refers to connections between various business operators for the purpose of exchanging goods and information via contracts, in these Guidelines, it refers to all value-added creation activities spanning across both physical and cyber space and that are dynamically connected to things and data (equivalent to the "value creation process" in the "Cyber Physical Security Framework" outlined in Appendix B).Of note, it is not limited to the relationship between companies that manufacture parts and companies that use those parts to assemble products. Cooperation between companies is also included in the supply chain.

11) Residual risk

Any risk which remains after the completion of risk response (avoidance, reduction, transfer of risk). It is also referred to as "risk acceptance".

12) Information Security Report

A report which aims to ensure that a company's initiatives are properly evaluated by such stakeholders as customers and investors by disclosing information on the company's management, information systems, and other security initiatives of high public interest

(Reference: "Model for information security report" by Ministry of Economy, Trade and Industry: http://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf)

13) Stakeholder

All persons or organizations that can affect, can be affected by, or are aware of being affected by a company's decision making or actions. In other words, shareholders, creditors, customers, and business partners.

14) Security policy

Policy developed by management to officially express their objectives and views on information security in organizations. Security policy contains the provisions of security measures in organizations.

15) Multi-layer protective system

It is expected that the introduction of a multi-layer protective system including physical layer, network layer and data layer will help to reduce the risk of breach by unknown malware or new type of attack more smoothly than depending on a single point of defense such as a single device, software, or perimeter protective system (mainly network perimeter).

IPA recommends the following four points as examples of multi-layer protective measures: (i) reduction of malware infection risk (ii) segregation of terminals and networks (iii) restricted access to servers with important information (iv) post-incident preparation.

16) Electronic signature

Additional electronic information based on cryptographic technology used to assure that certain data has not been altered.

17) Business partner

Companies with which any company has business relationships such as outsourcing or procurement of goods or services.

18) Physical space

The material world outside of cyberspace.

19) Plus-security

The ability to have security awareness in carrying out one's own work and to acquire the ability to implement necessary and sufficient security measures, or the state of having acquired it.

20) Malware

Any malicious programs that cause damage to security including computer viruses, spyware, and bots. These programs perform malicious actions by infiltrating a computer against the will of users or administrators (or before they become aware of it).

21) Ransomware

A coined word combining "Ransom" and "Software". It encrypts the data of the infected computer and makes it unusable, and demands money in exchange for unlocking it. Furthermore, as a new attack method, it infiltrates the network of the target company or organization, steals data on terminals such as personal computers and servers, and encrypts it all at once to make the system unusable, making it difficult to recover data. In some cases, double threats are made, such as demanding money in return for not disclosing stolen data in addition to demanding money.

22) Risk

International Standard (ISO/IEC 27000) defines "risk" as the "effect of uncertainty on objectives."

23) Risk response (avoidance, reduction, transfer and acceptance)

Ways to respond to risk mainly consist of the four responses of "risk avoidance," "risk reduction," "risk transfer" and "risk acceptance." According to JIS Q 0073 "Risk Management -Vocabulary", these risk responses are categorized into seven elements : risk avoidance, risk taking or increasing to gain opportunity, elimination of risk reduction, alternation of risk likelihood, change of result, risk transfer, and risk acceptance.

(1) Risk avoidance

"Risk avoidance" means the possibility of risk occurrence should be eliminated by removing factors enabling risk occurrence or employing another method. (E.g. cutting off external connections by suspending disclosures on the Web, citing the threat of unauthorized access from the internet.)

(2) Risk reduction

Reducing the possibility of a threat by taking measures of information security against vulnerabilities. It includes such methods as encrypting information to be saved against loss, theft and leakage; ensuring control of access to server rooms using biometric identification techniques against unauthorized access; and providing training on information security for personnel.

(3) Risk transfer

Transferring risk to other companies or organizations. It includes such methods as claiming damages with insurance policy when risk becomes apparent, and outsourcing the operation of internal information system through contracts with other companies to be able to claim damages due to unauthorized access or malware infection based on these contracts.

(4) Risk acceptance

Accepting a potential loss depending on the nature of certain risk.

24) Risk assessment

The process in which the results of risk analysis are compared with risk criteria (which acts as reference to evaluate risk based on objectives and the internal/external environment of organizations) to determine whether or not the level of risk is acceptable.

25) Risk analysis

Process through which one can apprehend the nature of risk and determine level of risk (size of risk based on combination of result and likelihood of an incident).

26) Log

A record of use of a computer or of data transmission. A log contains the identity of users, date operated, operation, etc. Logs are used for security and to identify the cause of an incident.

27) Business Continuity Plan (BCP)

A plan that sets out methods for business continuity in normal times and in emergencies for the continuity of the core business of a company and to enable early recovery when the company incurs damage due to a natural disaster, terror attack, cyberattack, etc.

28) Chief Information Security Officer (CISO)

The individual responsible for performing information security measures, designated from among the management or appointed by a top executive.

29) CSIRT (Computer Security Incident Response Team)

Construct for cyber security incident response.

30) PDCA

This is the acronym for Plan - Do - Check - Act. This is a well-known methodology for continuous improvement by reiterating the following steps.

1. Plan: Make plans to accomplish a target determined after sorting out issues.
2. Do: Perform actual work based on a target and its plans.
3. Check: Verify and evaluate whether or not the initial target was accomplished in accordance with plans.
4. Act: Improve the work based on the result of evaluation.

31) Product Security Incident Response Team (PSIRT)

A system for responding to incidents related to the company's products and services.