

Revision of the Japan Cyber/Physical Security Framework (CPSF) Overview of the CPSF Revision

October 23, 2026

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

0. Agenda

1. Key Takeaways of This Document
2. Background to the CPSF Revision and Future Plans
3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs
4. Revision of the Main Text of the CPSF
5. Revision of Appendix B
6. Revision of Appendix C
7. Revision of Appendix D
8. Revision of Appendix E

1. Key Takeaways of This Document

(1) Purpose of This Document

- This document provides an overview of the background to and key changes made in the revision of the CPSF from Version 1.0 to Version 1.1.

(2) Background to the CPSF Revision and Future Plans (P.4~8)

- This section explains why CPSF Version 1.0, published in 2019, was revised and outlines the approach to future revisions.

(3) Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (P.9~37)

- The cross-reference table shows how each security measure requirement in CPSF Version 1.0 corresponds to, or has been consolidated into, the requirements in Version 1.1.
- The tracked-changes version of CPSF Version 1.1 shows how the security measure requirements have been revised, but does not show the relationship between the requirements in Versions 1.0 and 1.1. Please refer to the cross-reference table in this document when comparing the two versions.

(4) Revision of the Main Text of the CPSF (P.38)

- This fiscal year's revision of the main text primarily concerns the security measure requirements in Part III. Changes to the other parts have been limited. For details of specific changes other than those to the security measure requirements, please refer to the tracked-changes version of CPSF Version 1.1.

1. Key Takeaways of This Document

(5)Revision of Appendix B (P.39)

- Appendix B shows the relationships between incidents, risk sources, and security measure requirements. As only the security measure requirements were revised this fiscal year, a detailed cross-reference between Versions 1.0 and 1.1 was considered unnecessary. This document therefore provides only an overview of the changes to Appendix B.

(6)Revision of Appendix C (P.40~43)

- The changes to Appendix C fall mainly into three categories: security measure requirements, examples of security measures, and referenced guidelines. Of these, the newly added examples of security measures represent the most significant new content and are presented on the following pages. For changes to the security measure requirements, please refer to the cross-reference table above. For changes to the referenced guidelines, please refer to the overview materials and other information published by the respective issuing organizations.

(7)Revision of Appendix D (P.44)

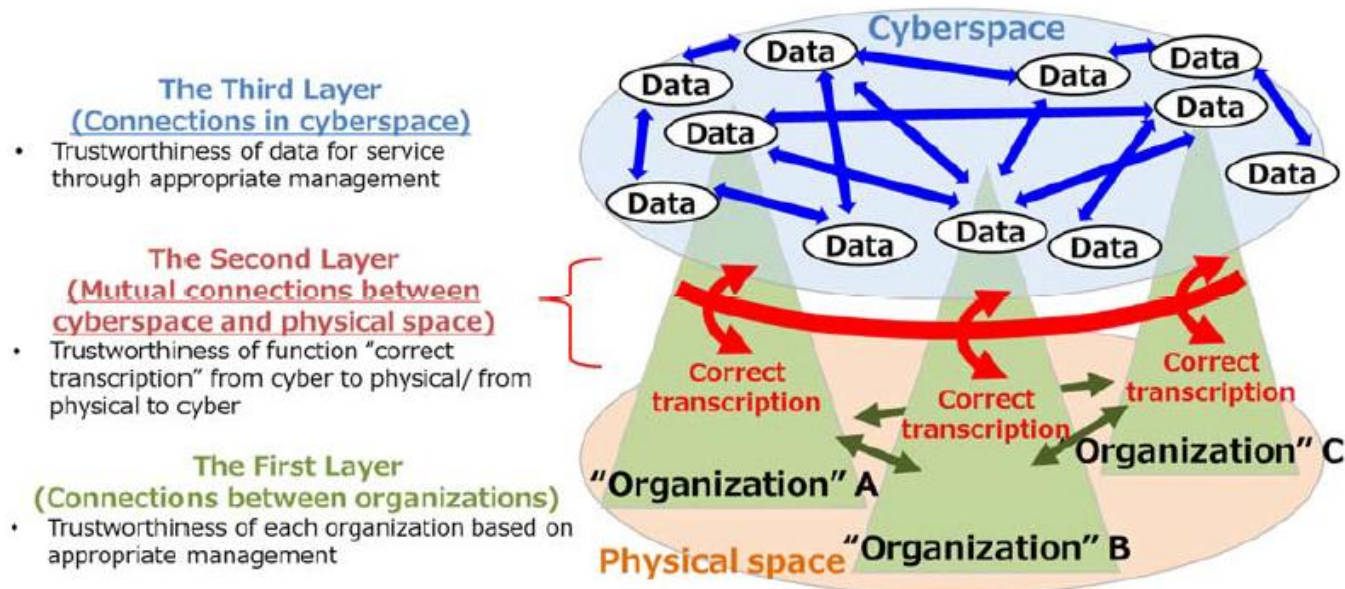
- As the international standards referenced in CPSF Version 1.0 have themselves been revised, a detailed cross-reference between Versions 1.0 and 1.1 was considered unnecessary. This document therefore provides only an overview of the changes to Appendix D.

(8)Revision of Appendix E (P.45)

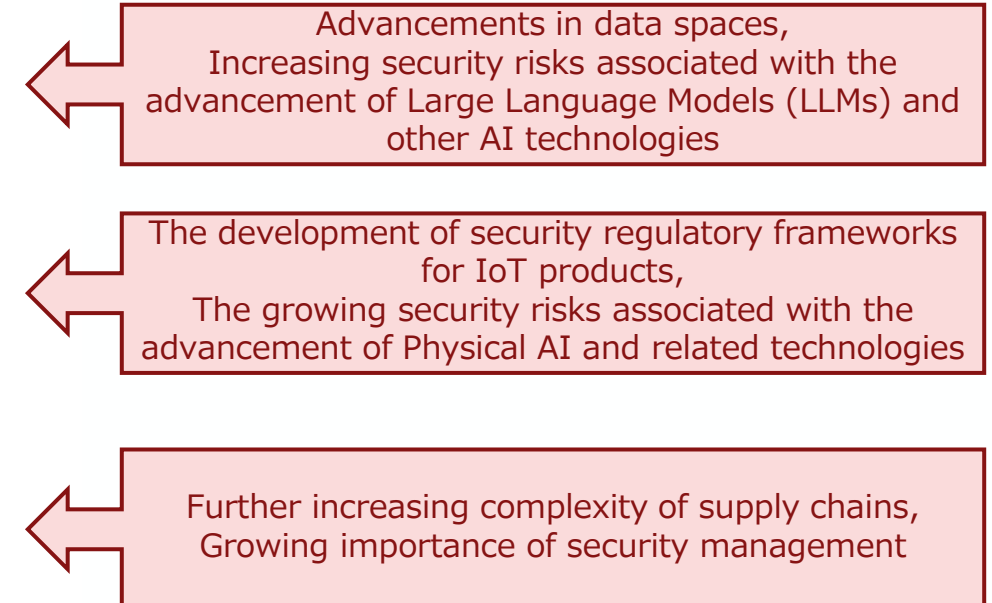
- The revision of Appendix E primarily reflects updates to the standards and other sources referenced for individual terms. Please refer to the tracked-changes version of the glossary for details.

2. Background to the Development of the CPSF

- The 5th Science and Technology Basic Plan (Japanese Cabinet Decision of January 22, 2016) has defined “Society5.0” as a human-centered super-smart society with advanced digital technologies. Japan’s Ministry of Economy, Trade and Industry (METI) has established the Cyber/Physical Security Framework (CPSF), developing a model for appropriately identifying and assessing the risks faced by value-creating activities in the emerging industrial society. The framework clarifies sources of risk and provides a set of security measures and guidelines that industry can use to address its own cybersecurity challenges. **The CPSF's importance has continued to grow, driven by advancements in technologies such as IoT, digital twins, data spaces, and, more recently, Physical AI.**



After CPSF 1.0(2020-2026)



2. Background to the Development of the CPSF

- Cyber/Physical Security Framework (CPSF) was established to contribute to the global harmonization by providing a framework that can be applied at the operational level of security measures implemented by individual organizations, with the entire value creation process (*) in the new industrial society defined as its scope of application.

Purpose and Scope	■ The scope of identifying risk sources and applying security measures under this framework encompasses the entire value creation process (*) in the new industrial society ■ (*)A value creation activity in which various physical assets, systems, and data are dynamically interconnected across both cyberspace and physical space to generate added value. (a "Society 5.0"-type supply chain)
Intended Readers	■ Chief Information Security Officers (CISOs) ■ Personnel in strategy and planning departments responsible for supply chain management (primarily Part I) ■ Security professionals at companies, organizations, and other entities involved in the value creation process ■ Personnel responsible for the development and quality assurance of information and control system equipment, as well as system design, implementation, and verification ■ Personnel responsible for data management ■ Representatives of industry associations and similar organizations responsible for developing security guidelines and related measures for their respective industrial sectors
Features of the Framework	■ Can be utilized at the operational level of the security measures implemented by individual organizations. ■ Enables organizations to understand the cost implications of security by illustrating both the necessity of security measures and examples of appropriate levels of protection. ■ Contributes to the realization of global harmonization.

2. Background to the revision of the CPSF

- The CPSF is structured in three parts, separating the components that require frequent review and updates (Part III and the Appendices) from the components that provide stable fundamental concepts and ensure the framework's reliability (Part I).

Structure of CPSF

Part I: Concept

Organizes a model for identifying and analyzing risk sources in the value creation process from a cybersecurity perspective, consisting of a three-layer structure and six constituent elements.

Provides stable foundational concepts to ensure the reliability of the framework.

Part II: Policy

Presents a method for identifying and organizing risk sources using the model described in Part I, and specifies the security requirements corresponding to those risk sources.

Part III: Method

Provides examples of security measures that address the security requirements presented in Part II.

Appendices

- Use cases demonstrating the application of the three-layer structure model to representative industries
- Mapping between risk sources and security requirements
- Examples of security measures corresponding to specific security requirements
- Mapping to major international standards and regulations
- Glossary of terms

Elements that should be reviewed and updated regularly, taking into account international standards such as ISO, NIST CSF, and the NIST SP series.

2. Background to the revision of the CPSF

- Approximately seven years have passed since the first establishment of the CPSF1.0 by METI, and following challenges have emerged.

Challenge 1. Security Requirements and Controls Are Not Fully Aligned with the Latest International Security Standards

Major standards referenced in the development of CPSF 1.0 have been successively updated, including the release of the NIST Cybersecurity Framework (CSF) 2.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 3, and ISO/IEC 27001:2022, the existing security requirements and example controls no longer fully reflect the latest cybersecurity trends and practices.(security control examples are unclear for users which standards and guidance documents should serve as their primary point of reference.)

Challenge 2. New Risks Arising from AI Must Be Addressed

AI is expected to introduce new security risks, including the immaturity of security technologies for AI agents and the increasing sophistication, scale, and intensity of AI-enabled cyberattacks.

At the same time, international frameworks and standards for AI security are still under development.



METI Japan's Plan:

- **The fiscal year:** To address Challenge 1, Part III: Method and the Appendices will be revised based on the latest major standards and frameworks.
- **From the Next Fiscal Year Onward:** As preparation for addressing Challenge 2, trends in the development of international AI security frameworks and the risks posed by AI to Cyber-Physical Systems (CPS) will be examined. Based on the findings, Part II: Policy and Part III: Method will be revised as necessary.
- **Future:** To fully address Challenge 2, after international frameworks for AI security have matured, Part I: Concept will be revised, including the “three-layer structure in which the value creation process operates” and the “six constituent elements.” Part II: Policy and Part III: Method will also be revised as necessary.

2. Background to the revision of the CPSF

- Only Part III and Appendices B through E of CPSF are updated this fiscal year. Parts I and II and Appendix A are scheduled to be revised in the future.

No.	Structure of CPSF	Whether revised or not	Key revisions
1	Part I: Concept Industrial cybersecurity for connected cyber and physical systems	-	✓ Since the scope of this fiscal year's revision is to reflect the latest security standards, Part I is not included in the scope of the revision. ✓ Part I is scheduled to be revised in the future, taking into account international security frameworks for AI that are expected to be developed, as well as ISO/IEC TS 5689, which is the international standardization of the CPSF.
2	Part II: Policy Identification of risk sources and measure requirements	-	✓ Same as above
3	Part III: Method Security measures – requirements and examples	✓	✓ Revise the security measure requirements based on the changes made to the international frameworks referenced in CPSF Version 1.0, such as NIST CSF.
4	Appendix A: Use case	-	✓ Planned for future revision based on the content of Parts I and II.
5	Appendix B: Relationship between risk sources and measure requirements	✓	✓ Revise the cross-reference table between risk sources and security measure requirements based on the security measure requirements revised in Part III.
6	Appendix C: Examples of security measures according to measure requirements	✓	✓ Based on the security measure requirements revised in Part III, assign the star3 and star4 assessment criteria and other elements of the Supply Chain Security Assessment Program of Japan to the relevant examples of security measures, and update the referenced guidelines to their latest versions.
7	Appendix D: Relationship with major overseas standards	✓	✓ Revise the cross-reference table between the security measure requirements and the latest versions of the major standards referenced in CPSF Version 1.0, including the NIST CSF, NIST SP 800 series, and ISO/IEC 27001.
8	Appendix E: Glossary	✓	✓ Update the definitions of existing terms and add new terms based on the latest versions of the source documents referenced for each term.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Govern Function)

- A cross-reference table of previous and revised security measure requirement IDs has been prepared to clarify the revisions to the requirements in Part III of CPSF Version 1.1.

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
1	Govern (CPS.GV)	CPS.GV.OC-01	The organization understands its mission and uses it to inform cybersecurity risk management decisions.	-	-
2		CPS.GV.OC-02	The organization understands legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—as well as industry guidelines, and establishes internal rules that appropriately reflect and address these requirements or guidelines.	CPS.GV-2	Formulate internal rules considering domestic and foreign laws, including the Act on the Protection of Personal Information and Unfair Competition Prevention Act, as well as industry guidelines, and review and revise the rules on a continuing and timely basis in accordance with any changes in relevant laws, regulations, and industry guidelines.
				CPS.DP-2	Detect security events in the monitoring process, in compliance with applicable local regulations, directives, industry standards, and other rules.
3		CPS.GV.OC-03	The organization identifies dependencies and critical functions across both its own organization and related external entities to sustain business operations and shares them with those external entities.	CPS.BE-3	Identify the dependency between the organization and other relevant parties and the important functions of each in the course of running the operation.
4		CPS.GV.RM-01	The organization defines risk management objectives and agrees on them with relevant stakeholders.	-	-
5		CPS.GV.RM-02	The organization develops a cybersecurity strategy to ensure effective cybersecurity risk management.	CPS.GV-4	Develop a strategy and secure resources to implement risk management regarding security.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Govern Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
6	Govern (CPS.GV)	CPS.GV.RM-03	The organization establishes its risk appetite and risk tolerance, and communicates them across the organization.	CPS.RM-2	Determine the organization's risk tolerance level based on the result of the risk assessment and its role in the supply chain.
7		CPS.GV.RM-04	The organization integrates cybersecurity risk management activities and their outcomes into the organizational risk management process, managing cybersecurity risks within that process.	-	-
8		CPS.GV.RM-05	The organization formulates policies regarding risk response options and their operations, and shares them within the organization.	-	-
9		CPS.GV.RM-06	The organization establishes and maintains lines of communication across the organization regarding cybersecurity risks, including risks posed by partners and other third parties.	-	-
10		CPS.GV.RM-07	The organization standardizes methodologies for assessing, documenting, classifying, and prioritizing cybersecurity risks, and shares them within the organization.	CPS.RM-1	Confirm the implementation status of the organization's cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Govern Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
11	Govern (CPS.GV)	CPS.GV.RM-08	The organization identifies strategic opportunities (positive risks for the organization), clarifies their characteristics, and integrates them into organizational cybersecurity risk deliberations.	-	-
12		CPS.GV.RR-01	Organizational senior management is responsible and accountable for cybersecurity risk, fostering a culture that is risk-aware, ethical, and continually improving.	-	-
13		CPS.GV.RR-02	The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.	CPS.BE-1	Identify and share the role of the organizations in the supply chain.
				CPS.AM-7	Define roles and responsibilities for cyber security across the organization and other relevant parties.
14		CPS.GV.RR-03	The organization appoints a security manager, establishes a security response organization (SOC/CSIRT), and maintains a structure to detect, analyze, and respond to security incidents within the organization.	CPS.AE-2	Appoint a chief security officer, establish a security management team (SOC/CSIRT), and prepare a system within the organization to detect, analyze, and respond to security events.
15	CPS.GV.RR-04	The organization allocates necessary resources commensurate with its cybersecurity strategy, roles, responsibilities, and policies.	-	-	

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Govern Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
16	Govern (CPS.GV)	CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.	CPS.IP-9	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.
17		CPS.GV.PO-01	The organization formulates security policies based on its organizational context, cybersecurity strategy, and priorities, communicates them within the organization and to relevant external parties (including suppliers and third-party providers, as needed), and implements them.	CPS.GV-1	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.
				CPS.BE-2	Define policies and standard measures regarding security that are consistent with the high-priority business and operations of the organization, and share them with parties relevant to the organization’s business (including suppliers and third-party providers).
18		CPS.GV.PO-02	The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization’s mission.	-	-
19	CPS.GV.OV-01	The organization reviews the outcomes of its cybersecurity strategy and, taking into account these results and changes in the internal and external context, revises the cybersecurity strategy as well as enterprise-wide strategy and direction as necessary.	-	-	

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Govern Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
20	Govern (CPS.GV)	CPS.GV.OV-02	The organization reviews the implementation status of its cybersecurity risk management and updates it as necessary.	-	-
21		CPS.GV.SC-01	The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.	-	-
22		CPS.GV.SC-02	The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.	CPS.AM-7	Define roles and responsibilities for cyber security across the organization and other relevant parties.
				CPS.DP-1	Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.
23		CPS.GV.SC-03	The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.	-	-
24		CPS.GV.SC-04	The organization identifies and prioritizes organizations and people that play an important role relevant in each layer of the three-layer structure to sustain business operations.	CPS.SC-2	Identify, prioritize, and evaluate the organizations and people that play important role in each layer of the three-layer structure to sustaining the operation of the organization.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Govern Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
25	Govern (CPS.GV)	CPS.GV.SC-05	The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means.	CPS.SC-1	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.
				CPS.SC-5	Formulate and manage security requirements applicable to members of other relevant organizations, such as business partners, who are engaged in operations outsourced from the organization.
				CPS.DS-1	If the organization exchanges protected information with other organizations, agree in advance on security requirements for protection of such information.
26		CPS.GV.SC-06	Before concluding contracts with suppliers and other third parties, the organization evaluates the cybersecurity management posture of said suppliers and third parties, and takes necessary measures to mitigate risks as needed.	CPS.SC-3	When signing contracts with external organizations, check if the security management of the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.
27		CPS.GV.SC-07	When entering into contracts with other relevant organizations such as business partners, the organization considers its objectives and risk management outcomes, verifying that products and services provided by them conform to the organization's security requirements.	CPS.SC-4	When signing contracts with external parties, check if the products and services provided by the other relevant organizations properly comply with the security requirements defined by the organization while considering the objectives of such contracts and results of risk management.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Govern Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
28	Govern (CPS.GV)	CPS.GV.SC-08	The organization periodically evaluates other relevant organizations such as business partners using audits, test results, or other forms of assessment to confirm that they are fulfilling their contractual obligations.	CPS.SC-6	Conduct regular assessments through auditing, test results, or other checks of relevant parties such as business partners to ensure they are fulfilling their contractual obligations.
29		CPS.GV.SC-09	The organization establishes and implements procedures to be followed when non-compliance with contractual requirements is identified through audits or testing of other relevant organizations such as business partners.	CPS.SC-7	Formulate and implement procedures to address noncompliance to contractual requirements found as a result of an audit, test, or other check on relevant parties.
30		CPS.GV.SC-10	The organization monitors the implementation of supply chain security measures across the lifecycle of technology products and services.	-	-
31		CPS.GV.SC-11	The organization establishes and implements procedures to be followed upon the termination of contracts with partners and other parties.	CPS.SC-10	Develop and manage a procedure to be executed when a contract with other relevant organizations such as business partners is finished. (e.g., expiration of contract period, end of support)
32		CPS.GV.SC-12	The organization collects and securely retains information (data) to demonstrate that it is fulfilling its contractual obligations to other relevant organizations and individuals, ensuring it can be disclosed to an appropriate extent when necessary.	CPS.SC-8	Collect and securely store data proving that the organization is fulfilling its contractual obligations with other relevant parties or individuals, and prepare them for disclosure as needed within appropriate limits.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Identify Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
33	Identify (CPS.ID)	CPS.ID.AM-01	The organization develops and appropriately manages inventories of hardware, software, and their management information (e.g., name, version, network address, designated manager, and license information) that comprise its system.	CPS.AM-1	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.
34		CPS.ID.AM-02	The organization develops and appropriately manages communication network diagrams and data flow diagrams within the organization.	CPS.AE-1	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.
				CPS.AM-4	Create and manage appropriately network configuration diagrams and data flows within the organization.
35		CPS.ID.AM-03	The organization develops and appropriately manages inventories of external information systems connected to its organizational assets.	CPS.AM-5	Create and manage appropriately a list of external information systems where the organization's assets are shared.
36		CPS.ID.AM-04	The organization categorizes and prioritizes resources (e.g., components, data, and systems) based on their function, criticality, and business value, defines management responsibilities, and communicates them to relevant organizations and people involved in their operation.	CPS.AM-6	Classify and prioritize resources (e.g., People, Components, Data, and System) by function, importance, and business value, and communicate to the organizations and people relevant to those resources in business.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Identify Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
37	Identify (CPS.ID)	CPS.ID.AM-05	The organization develops and appropriately manages inventories of data and metadata in its possession.	-	-
38		CPS.ID.AM-06	The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.	-	-
39		CPS.ID.AM-07	The organization establishes identification methods to ensure traceability according to the importance of the components it produces within the supply chain.	CPS.AM-2	Specify a method to ensure traceability based on the importance of the components produced by the organization's supply chain.
40		CPS.ID.AM-08	The organization prepares and implements internal rules regarding records of production activities in order to create records concerning production date and time, conditions, and states, and store them for a certain period according to importance.	CPS.AM-3	Create records such as the date of production and condition of components depending on importance, and prepare and adopt internal rules regarding records of production activities in order to store components for a certain period of time.
41		CPS.ID.RA-01	The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.	CPS.RA-1	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.
42		CPS.ID.RA-02	The organization establishes a process to collect, analyze, respond to, and utilize vulnerability and threat information from internal and external sources (e.g., internal tests, security information, and security researchers).	CPS.RA-2	The security management team (SOC/CSIRT) collects information, including vulnerability and threats from internal and external sources (through internal tests, security information, security researchers, etc.), analyzes the information, and establishes a process to implement and use measures.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Identify Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
43	Identify (CPS.ID)	CPS.ID.RA-03	- The organization identifies and documents potential security incidents, their impacts, and their causal factors regarding organizational assets. - From the planning and design stages of IoT devices and IoT-integrated systems, the organization verifies that no unacceptable known security risks exist, incorporating safety hazard perspectives.	CPS.RA-3	Identify and document the assumed security incidents, those impacts on the organization's assets, and the causes of those.
				CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.
44		CPS.ID.RA-04	The organization identifies the potential impact and likelihood of threats exploiting vulnerabilities by periodically conducting risk assessments to evaluate the effectiveness of security rules for component management, including their implementation methods.	CPS.RA-4	- Conduct risk assessments regularly to check if the security rules for managing the components are effective and applicable to the components for implementation. - Check the presence of unacceptable known security risks, including safety hazards, from the planning and design phase of an IoT device and systems incorporating IoT devices.
				CPS.RA-5	Consider threats, vulnerability, likelihood, and impacts when assessing risks.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Identify Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
45	Identify (CPS.ID)	CPS.ID.RA-05	The organization shares information regarding the effectiveness of protective technologies with appropriate partners.	CPS.IP-8	Share information regarding the effectiveness of data protection technologies with appropriate partners.
46		CPS.ID.RA-06	- Based on risk assessments, the organization clearly defines response measures for potential security risks, documents the defined scope and priorities of response actions, monitors the implementation progress, and communicates this status to relevant parties. - The organization appropriately addresses security and associated safety risks identified through the assessment in the planning and design stages of IoT devices and IoT-integrated systems.	CPS.RA-6	- On the basis of the results of the risk assessment, clearly define the details of measures to prevent possible security risks, and document the organized outcome from the scope and priorities of the measures. - React accordingly to the security risks and the associated safety risks identified as a result of the assessment conducted at the planning and design phase of an IoT device and systems incorporating IoT devices.
47		CPS.ID.RA-07	The organization assesses the risk impact posed by significant organizational changes and security requirement exceptions, and records and manages the results.	-	-
48		CPS.ID.IM-01	The organization continuously improves its cybersecurity management posture under normal and adverse conditions, including the perspectives outlined in CPS.ID.IM-02 and subsequent requirements.	-	-
49		CPS.ID.IM-02	The organization continuously improves supply chain security standards and associated procedures.	CPS.SC-11	Continuously improve the standard of security measures relevant to the supply chain, related procedures, and so on.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Identify Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
50	Identify (CPS.ID)	CPS.ID.IM-03	The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.	CPS.AT-3	Improve the contents of training and education regarding security to members of the organization and other relevant parties of high importance in security management of the organization.
51		CPS.ID.IM-04	The organization continuously improves asset protection processes by integrating lessons learned from security incident response as well as from monitoring, measuring, and assessing internal and external attacks.	CPS.IP-7	Assess the lessons learned from security incident response and the results of monitoring, measuring, and evaluating internal and external attacks, and improve the processes of protecting the assets.
52		CPS.ID.IM-05	The organization applies lessons learned from the analysis of detected events such as alerts and logs, to continuously improve security event detection processes.	CPS.DP-4	Continuously improve the process of detecting security events.
53		CPS.ID.IM-06	The organization incorporates lessons learned from responses to security incidents to continuously improve its incident response plan.	CPS.IM-1	Review the lessons learned from the responses to security incidents, and continuously improve the security operation process.
54		CPS.ID.IM-07	The organization incorporates lessons learned from responses to security incidents to continuously improve its business continuity plan or emergency response plan.	CPS.IM-2	Review the lessons learned from the responses to security incidents, and continuously improve the business continuity plan or emergency response plan.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Protect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
55	Protect (CPS.PR)	CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.	CPS.AC-1	Establish and implement the procedure to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.
56		CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).	CPS.AC-3	Properly authorize wireless connection destinations (including users, IoT devices, and servers).
				CPS.AC-6	Adopt high confidence methods of authentication where appropriate based on risk (e.g. multi-factor authentication, combining more than two types of authentication) when logging in to the system over the network for the privileged user.
				CPS.AC-8	Restrict communications by IoT devices and servers to those with entities (e.g. people, components, system, etc.) identified through proper procedures.
				CPS.AC-9	Authenticate and authorize logical accesses to system components by IoT devices and users according to the transaction risks (personal security, privacy risks, and other organizational risks).

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Protect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
57	Protect (CPS.PR)	CPS.PR.AA-03	The organization prevents unauthorized logins to IoT devices, servers, and related assets by implementing mechanisms such as account lockout after a specified number of failed authentication attempts and enforcing delays on subsequent login attempts until security conditions are verified.	CPS.AC-4	Prevent unauthorized log-in to IoT devices and servers by measures such as implementing functions for lockout after a specified number of incorrect log-in attempts and providing a time interval until safety is ensured.
58		CPS.PR.AA-04	The organization protects, transmits, receives, and verifies information regarding authenticated entities (ID assertions).	-	-
59		CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.	CPS.AC-5	Segregate duties and areas of responsibility properly (e.g. segregate user functions from system administrator functions)
60		CPS.PR.AA-06	The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.	-	-
61		CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.	CPS.AC-2	Implement appropriate physical security measures such as locking and limiting access to the areas where the IoT devices and servers are installed, using entrance and exit controls, biometric authentication, deploying surveillance cameras, and inspecting belongings and body weight.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Protect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
62	Protect (CPS.PR)	CPS.PR.AT-01	The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.	CPS.AT-1	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.
63		CPS.PR.AT-02	The organization provides appropriate training and security education to designated personnel of external partners critical to security management, who may be involved in security incident response for the organization, enabling them to fulfill their assigned roles, and maintains records of such activities.	CPS.AT-2	Provide appropriate training and security education to members of the organization and other relevant parties of high importance in security management that may be involved in the security incident prevention and response. Then, manage the record of such training and security education.
64		CPS.PR.DS-01	The organization accurately understands the required level of data protection mandated by various laws, regulations, and agreements regarding data shared exclusively among relevant organizations, establishes data classification methods based on respective requirements, and appropriately protects data commensurate with its classification throughout the entire lifecycle.	CPS.GV-3	Understand the level of data protection required by laws and arrangements regarding handling of data shared only by relevant organizations, develop data classification methods based on each requirement, and properly classify and protect data throughout the whole life cycle.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Protect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
65	Protect (CPS.PR)	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.	CPS.DS-2	Encrypt information with an appropriate level of security strength, and store them.
				CPS.DS-5	Securely control encryption keys throughout their life cycle to ensure proper operation and securely transmitted, received and stored data.
				CPS.DS-11	Perform integrity checking on information to be sent, received, and stored.
66		CPS.PR.DS-03	The organization protects the confidentiality, integrity, and availability of data-in-transit.	CPS.DS-3	Encrypt the communication channel when communicating between IoT devices and servers or in cyberspace.
				CPS.DS-4	Encrypt information itself when sending/receiving information.
				CPS.DS-5	Securely control encryption keys throughout their life cycle to ensure proper operation and securely transmitted, received and stored data.
				CPS.DS-11	Perform integrity checking on information to be sent, received, and stored.
67		CPS.PR.DS-04	The organization protects the confidentiality, integrity, and availability of data-in-use.	-	-

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Protect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
68	Protect (CPS.PR)	CPS.PR.DS-05	The organization maintains, updates, and manages data provenance, including data sources and processing history, throughout the entire lifecycle.	CPS.DS-14	Maintain, update, and manage information such as the origination of data and data processing history throughout the entire life cycle.
69		CPS.PR.DS-06	The organization performs routine backups of data (e.g., component configurations and operational data), protects backup data, and tests restoration capabilities.	CPS.IP-4	Perform a periodical system backup and testing of components (e.g., IoT devices, communication devices, and circuits).
70		CPS.PR.PS-01	The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.	CPS.DS-12	Introduce an integrity check mechanism to verify the integrity of hardware.
				CPS.DS-13	Confirm that IoT devices and software are genuine products during the booting-up process.
71		CPS.PR.PS-02	When procuring devices that process sensitive information or have important functions for its organization, the organization utilizes tamper-resistant devices.	CPS.DS-8	When handling information to be protected or procuring devices that have an important function to the organization, select the IoT devices and servers equipped with anti-tampering devices.
72		CPS.PR.PS-03	The organization utilizes products that implement appropriate security measures to ensure the trustworthiness of sensing data by preserving measurement availability and integrity.	CPS.DS-15	Use products that provide measurable security in order to ensure the availability of security reporting and the trustworthiness of sensing data through integrity protection.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Protect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
73	Protect (CPS.PR)	CPS.PR.PS-04	The organization deploys IoT devices that implement security safeguards designed for network connectivity.	CPS.PT-3	Introduce IoT devices that implement safety functions, assuming that these devices are connected to the network.
74		CPS.PR.PS-05	The organization integrates secure software development practices (e.g., security reviews during the design stage, application of secure coding rules, and pre-release vulnerability assessments) into the system development life cycle and verifies their implementation.	CPS.IP-3	Introduce the system development life cycle to manage the systems.
75		CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).	CPS.IP-1	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.
				CPS.IP-2	Restrict the software to be added after installing in the IoT devices and servers.
				CPS.PT-2	Minimize functions of IoT devices and servers by physically and logically blocking unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers etc.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Protect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
76	Protect (CPS.PR)	CPS.PR.PS-07	The organization prevents the installation and execution of unauthorized software.	CPS.DS-10	Conduct integrity checks of software running on the IoT devices and servers at a time determined by the organization, and prevent unauthorized software from launching.
				CPS.DS-13	Confirm that IoT devices and software are genuine products during the booting-up process.
77		CPS.PR.PS-08	The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan.	CPS.IP-10	Develop a vulnerability remediation plan, and modify the vulnerability of the components according to the plan.
78		CPS.PR.PS-09	The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.	CPS.MA-1	- Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updates with managed tools properly and in a timely manner while recording the history. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.
79		CPS.PR.PS-10	The organization performs maintenance on its own IoT devices, servers, and related assets with prior approval from the department that owns the target component or system, logging maintenance activities and preventing unauthorized access.	CPS.MA-2	Conduct remote maintenance of the IoT devices and servers while granting approvals and recording logs so that unauthorized access can be prevented.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Protect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
80	Protect (CPS.PR)	CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.	CPS.PT-1	Determine and document the subject or scope of the audit recording/log recording, and implement and review those records in order to properly detect high-risk security incidents.
81		CPS.PR.PS-12	Upon the disposal of IoT devices, servers, and related assets, the organization deletes or renders unreadable all internally stored data, unique identifiers of legitimate devices and systems, and critical security information (e.g., private keys and digital certificates).	CPS.IP-6	When disposing of an IoT device and server, delete the stored data and the ID (identifier) uniquely identifying the genuine IoT devices and servers as well as important information (e.g., private key and digital certificate), or make them unreadable.
82		CPS.PR.IR-01	The organization protects networks and environments from unauthorized access and use by implementing network segmentation (e.g., separating development/test environments from production environments, and isolating IoT device environments from other networks within the organization).	CPS.AC-7	Develop a policy about controlling data flow, and according that protect the integrity of the network by means such as appropriate network isolation (e.g., development and test environment vs. production environment, and environment incorporates IoT devices vs. other environments within the organization).
				CPS.DS-9	Properly control outbound communications that send information to be protected to prevent improper data breach.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Protect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
83	Protect (CPS.PR)	CPS.PR.IR-02	The organization implements physical safeguards to comply with policies and rules regarding the physical operating environment of its IoT devices, servers, and related assets, such as ensuring uninterruptible power supplies, fire protection equipment, and flood protection measures.	CPS.IP-5	Implement physical measures such as preparing an uninterruptible power supply, a fire protection facility, and protection from water infiltration to follow the policies and rules related to the physical operating environment, including the IoT devices and servers installed in the organization.
84		CPS.PR.IR-03	The organization implements mechanisms to achieve requirements for the continuous operation of systems and services under normal and adverse conditions.	-	-
85		CPS.PR.IR-04	The organization secures sufficient resources (e.g., people, components, and systems) to minimize the impact of attacks and maintain critical functions, even in the event of cyberattacks such as ransomware or denial-of-service (DoS) attacks.	CPS.DS-6 CPS.DS-7	Secure sufficient resources (e.g., People, Components, system) for components and systems, and protect assets properly to minimize bad effects under cyber attack (e.g., DoS attack). Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, conduct replacement work, and update software for IoT devices, communication devices, circuits, etc.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Detect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
86	Detect (CPS.DE)	CPS.DE.CM-01	The organization monitors networks and network services to properly detect security events.	CPS.CM-1	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.
87		CPS.DE.CM-02	The organization monitors the operational status of hardware and software across IoT devices, servers, and related assets, as well as network connection status, to properly detect security events.	CPS.CM-6	As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.
88		CPS.DE.CM-03	The organization monitors communications with external service providers to properly detect security events.	CPS.CM-5	Monitor communication with external service providers so that potential security events can be detected properly.
89		CPS.DE.CM-04	The organization monitors the activities of internal and external personnel, including their access to and operations on elements (components, systems, etc.), to properly detect security events.	CPS.CM-6	As part of the configuration management of devices, constantly manage software configuration information, status of network connections (e.g., presence/absence of connections and access destination), and information transmission/reception status between other "organization", people, components, and systems.
90		CPS.DE.CM-05	The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.	CPS.CM-2	Perform setting, recording, and monitoring of proper physical access, considering the importance of IoT devices and servers.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Detect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
91	Detect (CPS.DE)	CPS.DE.CM-06	The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation.	CPS.CM-7	Confirm the existence of vulnerability that requires a regular check-up in IoT devices and servers managed within the organization.
92		CPS.DE.CM-07	The organization verifies the integrity and authenticity of information received from cyberspace prior to operation.	CPS.CM-4	Validate the integrity and authenticity of the information provided from cyberspace before operations.
93		CPS.DE.CM-08	The organization deploys IoT devices that detect anomalies or suspend operations by comparing commanded operations with actual operational outcomes. The organization verifies that information received from cyberspace does not contain malicious code and remains within permissible operating parameters prior to execution.	CPS.CM-3	- Use IoT devices that can detect abnormal behaviors and suspend operations by comparing the instructed behaviors and actual ones. - Validate whether information provided from cyberspace contains malicious code, and is within the permissible range before any action based on the data.
94		CPS.DE.CM-09	As part of its monitoring operations, the organization periodically tests and validates whether functions detecting security events operate as intended.	CPS.DP-3	As part of the monitoring process, test regularly if the functions for detecting security events work as intended, and validate these functions.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Detect Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
95	Detect (CPS.DE)	CPS.DE.AE-01	The organization analyzes potential security events to understand their details.	-	-
96		CPS.DE.AE-02	The organization accurately identifies security incidents by implementing procedures to correlate security events and analyze them against external threat information.	CPS.AE-3	Identify the security events accurately by implementing the procedure to conduct a correlation analysis of the security events and comparative analysis with the threat information obtained from outside the organization.
97		CPS.DE.AE-03	The organization identifies the impact of security events, including the adverse effects on relevant external organizations.	CPS.AE-4	Identify the impact of security events, including the impact on other relevant organizations.
98		CPS.DE.AE-04	The organization establishes criteria for determining whether a security event constitutes an incident, and declares an incident when the criteria are met.	CPS.AE-5	Specify the criteria to determine the risk degree of security events.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Respond Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
99	Respond (CPS.RS)	CPS.RS.MA-01	To clarify response actions, priorities, and remediation scope following the occurrence of a security incident, the organization predefines and implements response procedures (security operation processes) for the organization, people, components, and systems after detecting an incident.	CPS.RP-1	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.
				CPS.SC-9	Prepare and test a procedure for incident response with relevant parties involved in the incident response activity to ensure action for incident response in the supply chain.
100		CPS.RS.MA-02	The organization verifies that events reported as security incidents are not false positives or duplicate reports, and validates their legitimacy as incidents.	-	-
101		CPS.RS.MA-03	The organization classifies and prioritizes detected security incidents based on the severity of impact, entry route, and other factors.	CPS.AN-3	Categorize and store information regarding the detected security incidents by the size of security-related impact, penetration vector, and other factors.
				CPS.AE-5	Specify the criteria to determine the risk degree of security events.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Respond Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
102	Respond (CPS.RS)	CPS.RS.MA-04	Once a security incident is declared, the organization executes incident response in accordance with predefined procedures, coordinating with other relevant organizations such as business partners.	CPS.RP-2	As part of the security operation process, define the procedure and the division of roles with regard to cooperative relations with relevant parties such as partners, and implement the process.
103		CPS.RS.MA-05	The organization takes appropriate actions for components (products) suspected of having quality defects, such as those produced using equipment damaged during a security incident.	CPS.RP-4	Take appropriate measures on goods (products) whose quality is expected to be affected by some reasons, including its production facility damaged by the occurrence of the security incident.
104		CPS.RS.MA-06	The organization determines the initiation of recovery based on predetermined criteria, taking into account the characteristics of the security incident and the impact of recovery activities on business operations.	-	-
105		CPS.RS.AN-01	The organization collects data and metadata related to security incidents (including the history of actions taken during incident response), preserves their integrity, and retains them in a state where acquisition sources, timestamps, and related provenance can be referenced.	-	-

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Respond Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
106	Respond (CPS.RS)	CPS.RS.AN-02	After a security incident occurs, the organization conducts digital forensics to identify the root cause. In doing so, it preserves records of the investigation process in a tamper-resistant manner.	CPS.AN-2	Implement digital forensics upon the occurrence of the security incident.
107		CPS.RS.AN-03	Based on the full scope of the security incident and the inferred intent of the threat actor, the organization assesses the impact on society as a whole, including the organization itself and relevant external organizations.	CPS.AN-1	Understand the impact of the security incident on the whole society including the organization and relevant parties such as partners based on the full account of the incident and the probable intent of the attacker.
108		CPS.RS.CO-01	The organization develops and implements rules governing internal communication and external disclosure after the occurrence of a security incident.	-	-
109		CPS.RS.CO-02	Based on established rules, the organization escalates incidents to executive decision-makers within the organization and relevant external entities as necessary.	-	-
110		CPS.RS.MI-01	The organization minimizes the spread of damage from security incidents, eradicating causes or mitigating adverse impacts.	CPS.MI-1	Take measures to minimize security-related damages and mitigate the impacts caused by such incident.

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Recover Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
111	Recover (CPS.RC)	CPS.RC.RP-01	The organization incorporates security incidents into its business continuity plan or emergency response plan, which defines response policies and procedures for natural disasters.	CPS.RP-3	Include security incidents in the business continuity plan or emergency response plan that outlines the action plans and response procedures to take in case of natural disasters.
112		CPS.RC.RP-02	The organization takes into account critical business functions and the results of cybersecurity risk management when establishing post-incident operational policies.	-	-
113		CPS.RC.RP-03	Upon deciding to initiate the recovery phase, the organization executes recovery based on predetermined recovery plans.	-	-
114		CPS.RC.RP-04	The organization verifies the integrity of backups and other recovery assets prior to use.	-	-
115		CPS.RC.RP-05	The organization verifies the integrity of restored assets, recovers systems and services, and confirms that they are in a normal operational state.	-	-
116		CPS.RC.RP-06	The organization declares the completion of incident recovery based on predetermined criteria and completes the documentation related to the incident.	-	-

3. Cross-Reference Table of Previous and Revised Security Measure Requirement IDs (Recover Function)

CPSF Ver 1.1				CPSF Ver 1.0	
No.	Function	Measure Requirement ID	Measure Requirement	Measure Requirement ID	Measure Requirement
117	Recover (CPS.RC)	CPS.RC.CO-01	The organization establishes and maintains rules regarding information exchange aimed at recovery after the occurrence of a security incident.	CPS.CO-1	Develop and manage rules regarding publishing information after the occurrence of the security incident.
118		CPS.RC.CO-02	The organization incorporates provisions to restore public trust and organizational reputation after the occurrence of a security incident into its business continuity plan or emergency response plan.	CPS.CO-2	Include the item in the business continuity plan or emergency response plan to the effect that the organization shall work to restore its social reputation after the occurrence of a high-risk security incident.
119		CPS.RC.CO-03	The organization specifies within its business continuity or emergency response plans that recovery activities must be communicated to internal and external stakeholders, officers, and management.	CPS.CO-3	Include the item in the business continuity plan or emergency response plan to the effect that the details of the recovery activities shall be communicated to the internal and external stakeholders, executives, and management.

4. Revision of the Main Text of the CPSF

For revisions to the CPSF main text other than the security measure requirements, please refer to CPSF Version 1.1 with tracked changes.

5. Revision of Appendix B

- In the cross-reference table between risk sources and security measure requirements in Appendix B, only the “Security Measure Requirements and Security Measure Requirement IDs” column has been revised this fiscal year.

■ Functions/Assumed Security Incidents/Risk Sources/Measure Requirements in the First Layer

<Scope of This Fiscal Year’s Revision>
The security measure requirements revised in Part III have been mapped to the risk sources.

#	Function	Assumed security incident	Risk sources			Measure Requirement	Measure Requirement ID
			Threat	Vulnerability ID	Vulnerability		
1_1	Establishing the organizational risk management system effective in normal times and appropriately operating it.	Data that must be protected is leaked from an area managed by the organization	- Malware infection that takes advantage of a data storage system’s vulnerability - Injection attack exploiting incomplete input validation (e.g. SQL injection, XSS) - Communication interception on the network - Physical intrusion by an unauthorized person into areas that need to be protected - Identity spoofing using a stolen ID/password of a proper user - Internal fraud by an authorized user	L1_1_a_ORG	[Organization] - Security risks are not managed in accordance with appropriate procedures, and other organizations needed are not involved in risk management.	The organization understands its mission and uses it to inform cybersecurity risk management decisions. The organization identifies strategic opportunities (positive risks for the organization), clarifies their characteristics, and integrates them into organizational cybersecurity risk deliberations. The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders. The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary. The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes. The organization identifies and prioritizes organizations and people that play an important role relevant in each layer of the three-layer structure to sustain business operations. The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means. Before concluding contracts with suppliers and other third parties, the organization evaluates the cybersecurity management posture of said suppliers and third parties, and takes necessary measures to mitigate risks as needed. The organization monitors the implementation of supply chain security measures across the lifecycle of technology products and services.	CPS.GV.OC-01 CPS.GV.RM-08 CPS.GV.SC-01 CPS.GV.SC-02 CPS.GV.SC-03 CPS.GV.SC-04 CPS.GV.SC-05 CPS.GV.SC-06
				L1_1_a_PEO	[People] - People are not fully aware of the security or safety risks that may concern them.	The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization. The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations. The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.	CPS.GV.RR-02 CPS.ID.IM-03 CPS.PR.AT-01

<Planned for Future Revision>

Parts I and II, which serve as the basis for ensuring the trustworthiness of the framework, are not subject to revision this fiscal year.

Accordingly, the functions and security incidents specified in Part II, as well as the threats and vulnerabilities identified based on those incidents, will not be revised this fiscal year.

However, revisions are planned for the future, taking into account the findings of research on risks posed by AI to CPS and other relevant matters.

6. Revision of Appendix C

- Of the main components of Appendix C, (1) Security Measure Requirements and (3) Reference Guidelines have been updated based on the revised requirements in Part III and the latest versions of the guidelines listed below, respectively.
- (2) Examples of Security Measures have been revised based on NIST SP 800 and other standards adopted in CPSF Version 1.0, as well as the evaluation criteria of the Supply Chain Security Assessment Program of Japan and other sources reflecting the latest security trends. (The following pages summarize the revisions by function, focusing on newly added examples. Other minor revisions have also been made as necessary.)

(1) Updated to the Security Measure Requirements revised in Part III

(2) Classified into three categories, Basic, Advanced, and High-Advanced, based on the Supply Chain Security Assessment Program of Japan, CSF 2.0 Implementation Examples, CPGs, and other relevant sources

(3) Updated each of the five reference guidelines used in CPSF Ver 1.0 to its latest version

Measure Requirement ID	Measure Requirement	Corresponding Vulnerability ID	Examples of security measure	Subject that implements measure	Reference Guidelines				
					NIST SP 800-171 Rev.3	NIST SP 800-53 Rev.5 Release 5.2.0	ISO/IEC 27001:2022 Annex A	IEC 62443-2-1:2024	IEC 62443-3-3:2013
CPS.GV.OC-01	The organization understands its mission and uses it to inform cybersecurity risk management decisions.	L1_1_a_ORG L1_1_b_ORG L1_1_c_ORG	Common among <High-Advanced>, <Advanced> and <Basic> - The organization communicates its mission to internal and external personnel, utilizing it as material for judgement to identify, analyze, evaluate, and respond to cybersecurity risks that could impede mission execution.	O	-	○ (PM-11)	-	-	-
CPS.GV.OC-02	The organization understands legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—as well as industry guidelines, and establishes internal rules that appropriately reflect and address these requirements or guidelines.	L1_1_a_PEO L1_1_b_PEO L1_1_c_PEO L1_2_a_ORG L1_2_a_COM L1_2_a_SYS L1_2_a_PRO L1_2_a_DAT L3_4_a_ORG L3_4_b_ORG	Common among <High-Advanced>, <Advanced> and <Basic> - The organization identifies all laws and regulations which are applied to each organization to satisfy requirements related to the type of business. - When the organization operates businesses in other countries, managers consider complying with the laws and regulations in all related countries. - Within its business activities, the organization clearly identifies all related laws, regulations, and contractual requirements in the context of security as well as the organization's effort to fulfill these requirements, documents them, and maintains those documents at their latest. - Prior to formulating internal rules, the organization determines whether any applicable laws and regulations, industry standards, or customer contractual obligations related to monitoring operations exist, and if so, identifies the constraints imposed. - The organization defines and documents detailed management measures and details of responsibilities to satisfy the requirements. - The organization disseminates established and revised internal rules to officers, employees, established, and seconded personnel. - The organization monitors revision statuses of applicable laws, regulations, and contractual requirements, reviewing and assessing internal rules at least annually. [Reference] Information security-related statutes include, for example, the Unfair Competition Prevention Act, the Act on Electronic Signatures and Certification Business, the e-Document Act, the Act on the Protection of Personal Information, and the Act on Prohibition of Unauthorized Computer Access. Furthermore, to ensure compliance with these laws and regulations, it is advised to refer to regulatory guidance issued by relevant ministries and agencies (e.g., Unfair Competition Prevention Act: "Management Guidelines for Trade Secrets" (Ministry of Economy, Trade and Industry, March 2025), "Guidelines on Shared Data with Limited Access" (February 2024); Act on the Protection of Personal Information: "Guidelines on the Act on the Protection of Personal Information (General Rules)" (Personal Information Protection Commission, June 2026), "Guidelines on the Act on the Protection of Personal Information (Anonymously Processed Information)" (Personal Information Protection Commission, April 2026)).	O	○ (03.15.03 Rules of Behavior a.)	○ (AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT, RA-01, SA-01, SC-01, SI-01, SR-01)	○ (A.5.31)	-	-

6. Revision of Appendix C

- The key revision points of Appendix C are summarized for each of the six functions.
- Govern: Examples of security measures were added to strengthen senior management involvement and expand the scope and methods of risk management
- Identify: Examples of security measures were added to improve the identification and management of relevant assets, threat identification, and continuous improvement of the cybersecurity posture

No.	Function	Overview of Revisions to Examples of Security Measures (Focusing on Major Newly Added Examples)
1	Govern (CPS.GV)	The following examples of security measures were added: • Determining the frequency and methods for reporting the organization's cybersecurity posture to senior management, and addressing supply chain cybersecurity risks with senior management involvement, to promote senior management engagement in the organization's cybersecurity posture (GV.RM-06, GV.SC-03) • Identifying strategic opportunities and assessing and prioritizing both positive and negative risks to address cybersecurity risks from both perspectives (GV.RM-08) • Determining whether to obtain cyber insurance to expand the range of cyber risk response options (GV.RM-05)
2	Identify (CPS.ID)	The following examples of security measures were added: • Regularly identifying data requiring protection that is distributed across the organization and protecting associated information, such as data sources and responsible data owners, to ensure the continuous protection of data, products, and services; also ensuring security throughout the lifecycle of products and services (ID.AM-05, ID.AM-06) • Using threat intelligence and conducting threat hunting to understand threat information and identify potential threats (ID.RA-02, ID.RA-03) • Conducting penetration testing, third-party assessments, and other activities to continuously improve the organization's cybersecurity posture; also conducting exercises with suppliers and joint post-incident reviews (ID.IM-01, ID.IM-06)

6. Revision of Appendix C

- Protect: Examples of security measures were added to strengthen authentication and authorization, protect data in use, and ensure the continued operation of systems and services
- Detect: Examples of security measures were added to enhance the monitoring and detection of cybersecurity events and refine incident classification

No.	Function	Overview of Revisions to Examples of Security Measures (Focusing on Major Newly Added Examples)
3	Protect (CPS.PR)	The following examples of security measures were added: • Protecting ID assertions, periodically reviewing access privileges, and implementing a zero trust architecture to strengthen authentication and authorization (PR.AA-04, PR.AA-06, PR.IR-01) • Deleting data remaining in processors and memory and preventing other users or processes on the same system from accessing such data to prevent the leakage and unauthorized use of data in use (PR.DS-04) • Preventing single points of failure and using load balancing to minimize impacts on the continued operation of systems and services (PR.IR-03)
4	Detect (CPS.DE)	The following examples of security measures were added: • Monitoring hardware tampering, deviations from standard software configurations, and the use of storage, power supplies, and other resources to expand the scope of cybersecurity event monitoring (DE.CM-02) • Using deception technologies for monitoring to expand attack detection methods (DE.CM-04) • Classifying incidents by incident level to reflect incident severity in response decisions (DE.AE-04)

6. Revision of Appendix C

- Respond: Examples of security measures were added to strengthen incident response processes and support senior management decision-making
- Recover: Examples of security measures were added to validate the integrity of assets for recovery, apply lessons learned from incident response, and strengthen recovery communications

No.	Function	Overview of Revisions to Examples of Security Measures (Focusing on Major Newly Added Examples)
5	Respond (CPS.RS)	The following examples of security measures were added: • Validating incident reports at an early stage to prevent false detection and duplicate reporting of incidents (RS.MA-02) • Reporting incident status to senior management to support management decision-making on incident response (RS.CO-02) • Assessing the impact of recovery activities on business operations to ensure business continuity during recovery (RS.MA-06)
6	Recover (CPS.RC)	The following examples of security measures were added: • Verifying the integrity of assets before using them for recovery to prevent reinfection after recovery (RC.RP-04) • Checking for evidence of compromise and other issues before migrating recovered assets to the production environment, and monitoring their performance and other aspects after migration, to ensure proper migration (RC.RP-05) • Preparing post-incident reports to apply lessons learned from incident response (RC.RP-06) • Communicating recovery status and measures to prevent recurrence both internally and externally to ensure stakeholder understanding of and cooperation with recovery efforts (RC.CO-01)

7. Revision of Appendix D

- Appendix D consists of three cross-reference tables (D.1, D.2, and D.3) showing the relationships between the CPSF and major international standards.
- As part of the revision to CPSF Version 1.1, the major standards referenced in each table were updated to their latest versions, and their relationships with the security measure requirements revised in Part III were mapped.

Structure

CPSF Ver 1.0

D.1	Cross-Reference Table between the NIST CSF 1.1 Subcategories and the CPSF Ver 1.0 Security Measure Requirements
D.2	Cross-Reference Table between NIST SP 800-171 Rev. 1 and NIST SP 800-53 Rev. 4, and the CPSF Ver 1.0 Security Measure Requirements and Examples of Security Measures
D.3	Cross-Reference Table between Annex A of ISO/IEC 27001:2013 and the CPSF Ver 1.0 Security Measure Requirements and Examples of Security Measures

CPSF Ver 1.1

►	Cross-Reference Table between the NIST CSF 2.0 Subcategories and the CPSF Ver 1.1 Security Measure Requirements
►	Cross-Reference Table between NIST SP 800-171 Rev. 3 and NIST SP 800-53 Rev. 5 , and the CPSF Ver 1.1 Security Measure Requirements and Examples of Security Measures
►	Cross-Reference Table between Annex A of ISO/IEC 27001: 2022 and the CPSF Ver 1.1 Security Measure Requirements and Examples of Security Measures

8. Revision of Appendix E

For details of the revisions to Appendix E,
please refer to the glossary with tracked changes.

END