Data Management Framework for Collaborative Data Utilization

– A New Approach toward an Establishment of Trust in a Data-Driven Value Creation

Version 1.0

Cyber Security Division, Commerce and Information Policy Bureau,

Ministry of Economy, Trade and Industry

April 8, 2022

Revision history

Version	Revision date	Modified section	Modified contents
1.0	April 8, 2022	-	Newly created

1. New data management methods

1-1. The third layer in CPSF (connections in cyberspace)

1-1-1. Introduction to CPSF

In an industrial society where cyberspace and physical space are highly integrated, the process (supply chain) that creates the value of products and services is changing from conventional standards and linear processes to dynamic and flexible processes through various connections. Cyber Physical Security Framework (CPSF) summarizes the idea of ensuring the security of a new industrial society by organizing security issues and measures with such new value creation processes. CPSF says, “The security of physical data produced by IoT devices – and its digitization, transport, storage, and analysis – is very different from interactions between two trusted entities in a conventional supply chain. Often this IoT data is used to generate new data through automated analysis. Data is also used to create physical products and services in physical space by controlling physical IoT devices. All these interactions and more must be secured and controlled by value creation process participants.” Three different anchor point of trustworthiness are set: the first layer puts the anchor point of trustworthiness on connections between companies; the second layer puts it on mutual connections between physical space and cyberspace; and the third layer puts it on connections in cyberspace. Security issues with the entire economic society are identified, and countermeasures against them are summarized by focusing on these anchor points.

1-1-2. Positioning of the third layer

Cyberspace is expanding rapidly as everything is connected to networks, and the amount of digitized data that is exchanged between them is exploding. In cyberspace, data can be freely distributed, and can be obtained, edited, and processed without limitation of physical distance, and a large amount of data that was previously difficult to process can be analyzed from various perspectives to extract intelligence. Activities like these to create new value are now expanding at an accelerating pace. New services provided over networks are deployed on physical information systems such as servers, but in many cases the activities that create the services are achieved through logic rather

than physical characteristics.[1] Data that does not depend on physical characteristics creates added value. The data is basically neutral to systems and organizations and is freely distributed and utilized by being appropriately handled according to standards that require their neutrality. The third layer is where these activities and connections in cyberspace are developed, and where data is the anchor for creating added value in cyberspace.

It does not mean that only companies (organizations) whose trustworthiness of management has been confirmed in the first layer are involved in each process of the life cycle such as data generation, transfer, and processing in the third layer. Various entities are involved in the data life cycle, and if incorrect data is distributed and utilized due to improper measures by the participants, the value creation involving the data cannot bring value, and can actually lead to harmful consequences. For example, physical damage could arise if a wrong operation command is sent from the cyberspace to an IoT system because even if the trustworthiness of the transcription function in the second layer is ensured, the IoT system can operate faithfully by “correctly” transcribing the wrong command.

In other words, the most important premise in the third layer is that the data itself is correct.[2] The data on which the creation of added value (value creation) is based must be the anchor point of trustworthiness to ensure the trustworthiness of the value creation process.

1-2. Ensuring trustworthiness of data: Establishing the data management concept

CPSF regards the dynamically constructed supply chain as a value creation process in an industrial society in which cyberspace and physical space are highly integrated. This is a framework where it is possible to comprehensively identify the risks in the dynamic and complicated value creation process and to implement countermeasures by setting

---

[1]With the development of middleware, functions that were unable to be achieved without specific hardware in the past can now be achieved using software without being bound by the characteristics of hardware.

[2]It is necessary to maintain the confidentiality, integrity, and availability of data to ensure security. Here, the importance of the fact that the data in the third layer is correct (integrity) is specifically emphasized, and confidentiality and integrity must also be taken into consideration when considering countermeasures.

three layers for the industrial society and introducing the anchor points of trustworthiness accordingly. The positioning of the third layer in that framework is as already mentioned, but in order to implement comprehensive security measures based on the anchor point of trustworthiness of data itself, it is necessary to identify risks throughout the data life cycle and to implement various measures to ensure security.

It should be noted here that while the third layer places the anchor point of trustworthiness on data, the life cycle of data does not close within the third layer.

CPSF states “The third layer requires that data in cyberspace and its processing, analysis, and storage be reliable.” It also states “Trustworthiness of the data transcribed from physical space to cyberspace is guaranteed by ensuring trustworthiness of the transcription function in the second layer. However, it should be noted that data is created, edited, processed, and freely exchanged in cyberspace outside the second layer process as well, and not only by organizations with confirmed trustworthiness.” It clarifies the possibility of data generation place belonging to the second layer instead of the third layer and shows the approach of ensuring trustworthiness of data generation by combining the second and third layers.

In other words, in order to ensure the trustworthiness of data, while using the concept of the third layer of CPSF as a basis, it is necessary to expand the scope of application of the concept and to implement data-centric measures considering the entire life cycle from data generation/acquisition to disposal. More specifically, it is necessary to set a framework as to what data management should be. In this framework, various forms of “involvement” that occur in each process of the data life cycle are regarded as data management, and by modeling this, risks related to data are identified and countermeasures are organized.

It is necessary to keep the following three perspectives in mind while proceeding with the organization process based on this idea.

(1) There are no established definitions for data management.

(2) When considering data management from the perspective of data trustworthiness, it is necessary to put the focus on data, rather than seeing from the perspective of the entities involved in data processing activities, and the concept of data management should be organized from the perspective of how data is handled in

each process of the life cycle.

(3) When data management is organized as an aggregate of various involvements that occur in each process of the data life cycle, the entities involved are not limited to the same or a single entity. Therefore, data management does not preclude becoming a collective action by multiple entities.

What is derived from the viewpoint of (1) is that each person's understanding of the term data management is not the same from the beginning.

In this framework, instead of simply incorporating definitions for data management set out by other organizations, we should define the concept of data management that is necessary to consider security measures centered on data using CPSF as the basis. It has been difficult for each organization and country to engage in discussions on data management, and it has also been difficult to coordinate rules related to data management established by each organization. By sharing the concept of data management shown here and using this framework as a common tool to gain a common understanding of data management, the necessary adjustments can be made to ensure the same level of data security between different data management rules, etc., even if data is distributed across the rules.

The point of view (2) is emphasized because the idea of data management presented by various organizations so far is organized from the perspective of “how an organization can utilize the asset of data” and does not capture the entire data life cycle, so it is necessary to clarify that it is not a frame for comprehensively ensuring the trustworthiness of data.

Based on the characteristic that data is basically neutral to organizations, etc., the trustworthiness of data is ensured by organizing and implementing the necessary measures with putting the focus on the data and it is necessary to clarify again that the measures that are organized from the standpoint of the participants as what they should take are merely part of all the measures originally required for the data.

The viewpoint of (3) clarifies that since the viewpoint of (2) frees data management from the idea that it is done by a single entity, more than one entity is involved in the life cycle process at the same time and that the measures required for the involvement of the entities may differ depending on each entity. By introducing the viewpoint of (3), the

requirement to be addressed by each entity on a cloud service which is realized by services of multiple providers (for example, in the case where the SaaS of company B used by user company A is deployed on the PaaS of company C, and the PaaS of company C is deployed in the IaaS of company D), and the architecture based on the concept of zero trust considering the characteristic that data is basically neutral to the system etc. will be possible to clearly organized.

The above three perspectives are the basic conditions for understanding this framework, and the importance will be emphasized here again.

1-3. Objective of this framework

This framework is intended to make it possible to implement the measures necessary to ensure the security of data flowing between entities through appropriate data management, in order for the value creation process to create added value by ensuring the trustworthiness of the data. To this end, the framework puts the focus on data and visualizes the state of the data throughout the data life cycle to identify risks to the data. Since the risks faced in each process of the data life cycle are not limited to those that can be addressed by a single entity with actionable measures it is necessary to ensure the security of data through collective activities with other entities realized as the well-coordinated measures assigned to each participant in the data life cycle process. In addition, concrete measures that should be taken by each entity as part of collective activities need to be appropriately implemented under the governance of each entity.

Therefore, this framework does not organize the management of a single organization. However, from the perspective of dealing with the risks centered on the data, it is a framework that promotes the cooperation of the entities involved in the data = stakeholders to implement necessary measures including the governance of the organization.

Regarding the measures necessary to ensure data security, various international standards related to information security that have been published so far have already been compiled as the “Data Management Body of Knowledge (DMBOK)”. For measures against risks identified using this framework, it is possible to select specific measures by referring to existing documents such as DMBOK.

In addition to the role of clarifying risks in the environment in which data is placed and ensuring security, this framework also has the role of clarifying the conditions necessary to realize an environment for promoting data distribution.

This framework identifies risks by visualizing the state in which data is placed, and clarifies appropriate measures required for each entity involved in dealing with risks (“As-Is” measures). Expanding the way of thinking, clarifying what conditions the data state should meet when trying to transition data to a different environment ensures security in different environments and makes it possible to transition without problems (“To-Be” measures) can be done. For example, in order to achieve an environment in which data

can be freely exchanged between different systems such as data exchange platforms without the need for special measures, preparing a protocol for data exchange implemented in both systems in addition to setting of an API for functional coordination between systems. In such a case it becomes easier to design the protocol by utilizing this framework.

In addition, if the concept of this framework is widely shared and established as a general activity, it will be difficult for a system with a stronger influence among systems to black-box the protocol required for data exchange and to make other systems depend on the system (“bundle”). It will be able to secure freedom of data linkage and system combination in an open environment and achieves a more efficient data utilization model.

From a broader perspective, this can also be used as a model for clarifying differences (gaps) in conditions and measures that are required to ensure data security between various data management rules.

The data management rules established by each organization set conditions and measures related to data management for their respective purposes such as privacy protection and information sensitivity retention, but there is no function to automatically adjust between rules. Therefore, the data is effectively “enclosed” in one system, which often hinders the distribution of data as the conditions, etc. differ for each rule. Even globally, despite the same purpose that is to protect personal information, institutional conditions and measures differ in each country, making it difficult to distribute data across national borders in some cases[3].

The data management conditions and measures required by these rules must have the same data management conditions and measures if they have the same purpose. But in reality, they do not focus on the state of the data, it is often considered that it was set in consideration of managing the entities involved, which creates a gap between the rules.

This framework places the focus on data, visualizes the state of the data as an object, and identifies the conditions that data and related environment should satisfy and the measures that are being taken. As this framework makes it possible to organize the conditions that are originally required for data and its management activities without

[3]On the other hand, there are cases where the system, such as “Data Portability Right” in the GDPR, plays a role in ensuring data portability rather than a means of enclosing data.

excessive consideration of the entities involved, it is possible to perform gap analysis between the rules of each country, model the analysis results, and clarify the gap adjustment measures necessary to enable data distribution.

1-4. Target audience of this framework

As mentioned above, this framework has a function that enables data management to ensure data security, and a function that enables accurate analysis of gap between data transition points to achieve an environment for distributing data. It can be used from the field level of data management to the design of data management mechanisms and rules, and the creation of international data sharing mechanisms.

Therefore, it is expected that this framework will be used by the following people.

- Those who handle data that is authentic and requires appropriate security, especially those who participate in the value creation process by utilizing data
- Providers of services for data utilization
- Those involved in designing, building, and operating systems for data utilization
- A person who intends to provide an appropriate level of trust service when it is necessary to guarantee an appropriate trust as a condition required for data
- Those involved in establishing data security guidelines and rules

2. Data management model of this framework

2-1. Overview

2-1-1. Data management modeling overview

Data is generated and acquired with some purpose. It is distributed from time to time, and it is utilized in various ways while changing its properties to create added value. Ensuring security throughout the data life cycle is the key to adding value in the third layer. Therefore, this framework places the focus on data and visualizes the state of the data throughout the data life cycle in order to establish an environment where efforts can be made to ensure data security on a risk basis throughout the entire data life cycle.

The key to this approach is the method of visualizing the state in which the data is, and the model of data management that will function as a framework for visualization.

In this framework, data management is defined as “managing the processes during

which data properties change due to events in the domains based on the life cycle", and data management is organized as a model consisting of three elements: a "property", that are the properties of data, a "domain" that shares a specific norm, and "events" that generate, alter, or maintain data properties.

It is possible to clarify what risks exist for data and how to deal with them by visualizing the state of data using these three elements. In addition, since these three elements have a mutual influence, the change in state is regarded as continuous, in which data is transferred and one of the elements changes and the other elements also change. By increasing the predictability of changes that will occur next, it will be easier to understand the points when performing data management.

The relationship between the three elements is organized as follows.

"Property" is a data property such as the kind of category it is classified into, the kind of confidentiality that is required, who can exercise its rights, etc. This "property" is not just changed by the action on the data ("events") so that the personal information becomes anonymously processed information through the action of anonymous processing. For example, "property" depending on "domain" requirements such as how data must be handled based on the Personal Information Protection Law[4] and how the internal rules of a specific organization stipulate the access right holder of data. There is a part where the contents of are determined, and "property" and "domain" are in a mutually dependent relationship. Similarly, for example, in the law concerning the electric power business, when the electric power company provides the customers' data on the electric power use for the purpose of used by an entity other than the electric power company, the contents of data processing that the electric power company should perform are defined. It often happens that the "domain" in which the data resides requires a specific action "events" in order to properly manage the "properties" of the data. Therefore, it is necessary to consider "domains" and "events" as being related to each other.

In other words, "property", "domain", and "events" are in a mutually influential relationship, and it is limited that each is determined independently without being influenced by other elements. When "property" and "domain" are changed by "events",

[4] In this paper, the term "Personal Information Protection Law" is used as an abbreviation for the "Act on the Protection of Personal Information (Act No. 57 of 2003)."

they have continuity in relation to each other. Therefore, the life cycle of data is regarded as a continuous change in the state of data. And, based on predictability, it is possible to understand the content and range of change that are allowed for the three elements when transitioning to the next state. By using this model, it exerts its function when considering more realistic and efficient countermeasures in data management.

In addition, as described in the objective of this framework, when multiple entities will be involved in each process of the data life cycle and data management efforts based on a common understanding among stakeholders will be required, it will be easier to share awareness among stakeholders as the state of data is visualized by the three elements, and the interdependence of the three elements ensures a certain degree of predictability regarding changes in the data due to data transitions. Therefore, it also makes it easier to consider the measures that should be implemented by each entity based on common understanding, and to achieve an environment for ensuring appropriate data management by all the stakeholders.

2-1-2. Risk analysis procedure

In order for stakeholders involved in a series of value creation processes to consider measures to be taken by each entity based on a common understanding, it is necessary to identify the risks related to data in the value creation process and share awareness among the entities. At that time, it is possible to identify the risk by visualizing the state of data using the three elements of “property”, “domain” and “events” in accordance with the following four steps.

STEP 1　Visualize the data processing workflow (“events”)

- First, visualize the rough data flow and “events” in the assumed data utilization process from data generation/acquisition to disposal.
- In that case, the level of “events” details to be disclosed must be adjusted based on the objectives of the data flow organization. For example, when considering measures to handle data that is circulated between multiple stakeholders, the “events” of transferring data between a server and a client on an internal network may be omitted as it differs from the essence of the examination. At that time, it can

substitute by presenting management rules related to data handling and showing that they are handled in accordance with them.

STEP 2　Organize the necessary institutional conditions and measures (“domains”)

- Examine “domains” that contribute to data protection and set appropriate ones from the perspective of law and contract. At that time, it is conceivable that several “domains” overlap for one data, namely, requires are made for the data from various viewpoints.

STEP 3　Specify the “properties”

- Identify the “properties” that should be managed based on the set data, “events”, and “domains”.
- In some cases, additions will be made as appropriate while organizing the “properties” of data, if there are any omissions in the “domains” where this data should be handled or “events” that must be implemented.

STEP 4　Identify the risks of each “events”

- The risk assumed for each “events” is extracted and the set “properties” are reviewed from the viewpoint of the “domains” set.
- Risks must not only be identified from the perspectives of cybersecurity (i.e., confidentiality, integrity, availability), but also from the point of view of compliance (i.e., laws, regulations).

As mentioned above, since “properties”, “domains”, and “events” are mutually dependent on one another, each of STEPS 1 through 3 should be considered based on mutual feedback. Namely, each step is not irreversible, and it may prove necessary to add “events” while considering, for example, STEP3. In that case, return to STEP1 and add the necessary “events”, and in that state, review STEP2 and STEP3 again to sufficiently organize the “properties”, “domains”, and “events”, Then, it will be possible to identify risks in an appropriate manner by proceeding to STEP4. Even after completing the steps up until STEP 4, new risks could presumably appear and assumptions could

change if the details of properties, domains, and events previously identified change due to internal/external factors. Therefore, it is desirable to review the consideration results from STEPS 1 through 3 and re-assess the risk points whenever there is a change to the data utilization process, relevant legal systems, etc., or at an appropriate interval configured based on relevant processes, characteristics of handled data, etc.

2-2. Specifications

In 2-1, the method of identifying risks using this framework has been outlined, but when actually using this framework, it is essential to set “properties”, “domains”, and “events” appropriately. Therefore, the details of modeling and risk analysis are summarized as below.

However, especially with regard to “domains” and “properties,” the contents vary depending on the nature of the data handled and the nature of the stakeholders that make up the value creation process, and it is difficult to show them comprehensively. When utilizing the framework, please note that it is necessary to set the “events”, “domains”, and “properties” based on the actual situation of the organization, etc., while referring to the following description, and identify the risks.

2-2-1. Modeling (“events”)

“Events”, which generate, alter, or maintain data “properties”, can be largely classified into the following five categories: “generation/acquisition”, “processing/usage”, “transfer/provision”, “storage”, and “disposal”. Examples of risks to be considered for each “events” are shown in the Appendix B.

- Generation/acquisition

  In the value creation process, data exchanged in the cyberspace begin their lifecycle when they are generated/acquired automatically by sensor measurements, etc. or manually by humans, etc.

  As mentioned above, data is sometimes generated in the second layer instead of the third layer. Therefore, this shows the approach of ensuring trustworthiness of data generation by combining both layers. If cyberspace and physical space are

highly integrated so that a large volume of information from physical space is transcribed to the cyberspace and is shared in real-time such as data acquisition by sensors, then it is necessary to note that the trustworthiness of data generation/acquisition devices and systems, that are not conventionally regarded as part of data management, must be considered in order to consider the trustworthiness of data existing in cyberspace connections. For example, the trustworthiness of data utilized in the third layer can be ensured right from the initial lifecycle stage by ensuring that data become correctly transcribed to the cyberspace in the second layer such as by generating data from trustworthy IoT devices that have not been security breached (i.e. software tampering) and accurately transmitting the said data to servers, etc. to prevent any impersonation, tampering over the network, etc. This matter was also mentioned in the “IoT Security Safety Framework” which examined security and safety measures for IoT devices and systems to ensure trustworthiness in the second layer of CPSF (the connection between cyberspace and physical space). It has a structure that works together between frameworks.

Typical risks that can be considered at this event are that the transcription failures such as measurement results are different from the actual ones and spoofing the measuring equipment, stoppage of generation/acquisition due to system failure, acquisition of personal information due to inappropriate processes, etc. can be mentioned.

- Processing/usage

The generated/acquired data does not necessarily simply create added value as it is but is accompanied by added value through some action. For example, various processes such as extraction and trimming are performed according to the purpose of use to make the data easier to use from so-called raw data. And, browsing the data and extracting the intelligence from such data using AI etc., which leads to added value. In this framework, an action for creating an added value for data shall be regarded as processing/usage.

The act of removing some items, elements, records, etc. of data from the

analysis process and stored data set shall be regarded as a form of processing, and shall be regarded separately from disposal, which will be described later.

In addition, the action of accessing (browsing) data by a person who does not have the data is appropriate to be regarded as a form of usage because it is an action to create added value. However, if data is copied and shared for browsing, the contents of “Transfer/provision” should be considered when identifying risks since data will be retained not only by the entities which holds the data originally, but also by the entities which acquire data from them.

Typical risks that can be considered at this event are unintended use of data, improper processing, etc.

- Transfer/provision

In Society 5.0, a society in which cyberspace and physical space are highly integrated and various entities dynamically construct the supply chain, transfer across organizations is inevitable in the process. Even when connecting companies to form a fixed supply chain, the transfer and provision of data between organizations has been carefully treated while considering risks. When the supply chain is dynamically constructed, it is necessary to create an environment in which data can be transferred and provided more freely in order to maximize the effect. However, it will be required to respond to risks more effectively, and an environment including a system for that purpose must be prepared.

Further, in most cases where data is transferred or provided, the data is copied and remains at the source, and the entity to which the data is transferred will also manage the data. Therefore, as described in the processing/usage section above, to identify risks in the action of accessing (browsing) data by a person who is not the owner of the data, transfer/provision factors must be considered.

In addition, the transfer/provision in this framework also handles the transfer/provision of data between devices, such as servers and clients. This could inhibit risks such as network eavesdropping by malicious actors and data corruption due to malfunctions of data transfer/provision systems, etc.

Therefore, in this framework, target transfer/provision events are organized based on four units: country/region, organization/person, system/service, and device. When organizing the risks and other points of concerns regarding a transfer/provision event, several units can be simultaneously considered depending on the specific method, etc. that are being used. This is considered to be useful in comprehensively identifying technical and non-technical risks. The following illustrates the overview of the four units and the matters that should actually be considered.

- Country/region

  This unit identifies the countries/regions that are relevant to the applicable transfer/provision events as well as the data protection-related policies, laws, guidelines, etc. in the said countries/regions (including those that apply outside the region), and organizes the necessary procedures, etc. for managing the associated risks. This unit should be considered when such transfers/provisions are taking place outside of the countries/regions to which the specific laws and regulations are currently applicable, or in a way that makes it seem so despite the transfers/provisions taking place within the countries/regions (i.e., behaviors such as deemed exports). Specific examples include: Cross-border transfers of personal information under laws related to personal information protection; exportation of technical information, etc. under laws related to export control such as the Foreign Exchange and Foreign Trade Act; and regulations and extraterritoriality rules on domestic storage of specific data under overseas data protection laws. When making such considerations, it is desirable to also identify the associated risks (i.e., violation of laws and regulations, loss of social credibility) and necessary procedures for ensuring legitimate transfers/provisions (i.e., obtaining individual consent, debriefing the data subjects, etc. when transferring personal data from Japan to overseas third parties).

- Organizations/people

  This unit identifies the organizations and people relevant to the applicable transfer/provision events as well as the data protection policies, systems, etc. of the said entities, and organizes the associated risks, necessary measures, etc. This unit should be considered when such transfers/provisions are made from an organization/person to another organization/person with different security policies, etc. Note that even if data are transferred/provided within the same corporation, this unit will still apply if it was between departments with different applicable security policies (i.e., between HQ and a production base). For example, when transferring/providing business-useful data from one organization to another, there is a potential risk of leakage of important data from an organization/person with relatively lower security standard. Possible countermeasures include verifying the implementation status of data protection measures including security measures (i.e., whether an ISMS certification, etc. has been acquired) of the transfer-receiving organization/person.

- Systems/services

  This unit identifies the systems executing the transfers/provisions, the functions as services provided by these systems (including protocols, etc. being used), and their data protection functions, as well as organizes the potential risks (i.e., network eavesdropping, impersonation of sender/receiver) and necessary countermeasures. This unit should be considered when such events occur electronically between devices through a network. There are various systems/services that can be used to transfer/provide data such as cloud storage, email, and file transfers (i.e., FTP, HTTP). It is desirable to choose a method with sufficient security standard, etc. based on the category, value (importance level), etc. of the data to be actually transferred/provided. For example, when transferring/providing data using cloud storage, potential risks include data leakage due to the exploitation of vulnerabilities of the cloud storage, as well as external accesses to data through misconfiguration, etc.

by service users. Possible countermeasures include verifying the implementation status of security functions of the cloud service in advance, as well as documenting measures that must be taken by the users when using the service.

- Devices

  This unit identifies individual system components (i.e., servers, IoT devices, network devices) that facilitate the transfers/provisions as well as their data protection functions and organizes the potential risks (i.e., unintended data transfers through fraudulent components in the device, device operation suspension due to denial-of-service attacks, etc.) and necessary countermeasures. This unit should be considered when such events occur through a network, portable media, etc. For example, when transferring/providing data using cloud storage, potential risks include fraudulent access from external sources to terminals that access the cloud storage and ultimately to the cloud storage data. Possible countermeasures include strengthening the authentication requirements for using such terminals and the endpoint security measures for these terminals (i.e., implement anti-malware software, EDR).

As mentioned above, the level of “events” details to disclose must be adjusted based on the objectives of the data flow organization. For example, the “events” of transferring data between a server and a client in an internal network may be omitted when considering data management in the case of continuous distribution among multiple stakeholders.

- Storage

  Storage always occurs in conjunction with other “events”[5]. During various stages of a lifecycle, data can become stored in storage devices and services that are

[5] In this paper, “archiving” (conducted for long-term data storage) also falls under the category of storage.

connected to a network (includes both on-premise and cloud), portable media such as a client's hard disk or USB flash drive, or temporary storage area of devices, etc. In identifying data handling risks and considering security measures, it is best to position storage as a type of “events”, because there may be different risks than transfer/provision or processing/usage.

- Disposal

  The processed and used data needs to be properly disposed of at the end of the life cycle.

  Further, in this framework, the term “disposal” refers to rendering all dataset unusable[6]. Data can be replicated on a variety of media, not just those under the direct control of an organization. Therefore, organizations must appropriately manage the authorities pertaining to such data and the status of their replication, distribution, etc. based on the category, importance level, etc. of the data. If the duplicated data at the destination also need to be disposed when disposing the original data, appropriate disposal efforts must be made based on the context such as by discussing with relevant stakeholders. For example, regarding personal data collected through individual consent, the act of excluding the data from a dataset via a withdrawal of the consent is best regarded as a form of processing/usage.

  Typical risks that can be conceived in this “events” are data that should be disposed remain and become leaked; data that should not be disposed become disposed, etc.

Each of the five “events” may have overlapping characteristics. For example, browsing data published by other organizations outside the country has the characteristic of processing/usage the data, but it also has the characteristic of transfer/provision data between countries/regions and between organizations. Furthermore, the transfer

[6] Depending on the “properties” and norms in the “domains” of data, standards on data disposal requirements may vary such as forcing specific methods (for example, destroying hard drives and other physical devices or cryptographic erase) or accepting more common methods. This makes it critical to use appropriate disposal methods required by specific situations.

between devices within the own organization is also included. Thus, it is necessary to appropriately grasp the “events” according to the purpose and identify the risks.

2-2-2. Modeling (“domains”)

As mentioned above, “domain” is defined as the scope of sharing a particular norm for data. There are various forms of norms for data, such as those stipulated by the laws and regulations of each country/region, internal rules stipulated by organizations, and contracts exchanged individually between organizations. Which “domains” to be set also depend on the nature of the data and the location where the data is used. Note that during this process, not only the laws and regulations of the country where the data are currently located but also those of other countries with extraterritoriality rules, if applicable, must be identified as the domains. Additionally, an implicit common understanding (including those not necessarily explicitly stated) about handling data shared across a community or terms and conditions of digital platforms can work as a “domain.” In this way, how to apply a “domain” largely depends on specific situations and circumstances of involved entities, and it is impossible to define a uniform setting method or form. More specific consideration of such domains is expected to be elaborated through future discussions and the accumulation of case studies.

Stakeholders such as data holders within the applicable data utilization process can appropriately configure domains by organizing the following four categories for example to examine the requirements while reducing the risk of omission (i.e., one important element that constitutes domains is laws and regulations). On the assumption that “domains” are configured in conjunction with laws and regulations, etc., that require certain common data handling procedures, the four categories are organized based on the potential purposes of requiring common data handling procedures. Note that these four categories are just examples and do not necessarily apply to all cases because duplications and omissions could potentially occur depending on the context (i.e., the positioning of the entity to adopt the framework) and perspectives to be emphasized.

At that time, an example of “property” set according to the request of “domain” is also described. Therefore, please use it to identify “domain” and “property”.

- Personal data protection
  - Examples of “domains”: Act on the Protection of Personal Information (Japan), GDPR (Europe), purpose of use agreed to by the individual concerned when personal information is acquired
  - Examples of specified “properties”: categories (personal information, anonymously processed information), data rights holder, data controller
- Intellectual property (including trade secrets) protection
  - Examples of “domains”: Unfair Competition Prevention Act, Copyright Act, contracts between entities (NDAs, etc.)
  - Examples of specified “properties”: categories (trade secrets, provided data with limitations), scope of disclosure, data rights holder
- Sensitive technology management
  - Examples of “domains”: Foreign Exchange and Foreign Trade Act, U.S. Export Administration Regulations
  - Examples of specified “properties”: categories (subject technology for export control, etc.), scope of disclosure, data controller
- Maintenance of appropriate social functions
  - Examples of “domains”: Financial Instruments and Exchange Act (e.g., provisions about insider trading), various confidentiality obligations
  - Example of specified “properties”: scope of disclosure

Besides the aforementioned classification methods of relevant provisions, etc., there are also the following classifications[7] that organize them from different viewpoints.

- Imposition of management responsibilities on information-managing businesses: Types of legal systems that impose the responsibility (including the obligations, etc. of businesses handling personal information according to the Act on the Protection of Personal Information) of managing the relevant information on information managing businesses.
- Imposition of legal responsibility on wrongdoers: Types of legal systems that

[7] Ministry of Economy, Trade and Industry, “Requirements for Information Security Related Laws and Regulations” (April 2011)

impose legal responsibility (including trade secret protection provisions, etc. stipulated in the Unfair Competition Prevention Act) on wrongdoers.

2-2-3. Modeling (“properties”)

The “property” indicates the properties of the data such as the legal category and disclosure range of the data and the purpose of use permitted by the acquisition source. By organizing the “properties” of the data, the organization can identify the relevant usage constraints and take the necessary measures to ensure security, thereby enabling proper handling of data. Although it is difficult to comprehensively show the “property” items of data, typical “properties”, parameters, and the points for organizing “properties” are shown below.

As mentioned above, some parts of “properties” are defined by requirements from “domains”. Section 2-2-2 lists the examples of “properties” that are specified by the “domains”. It is important to be based on the organized “domains” to consider requirements on data and identify relevant specific “properties”.

- Category

  When requiring a special action (“events”) for data (personal information, anonymously processed information, trade secrets, provided data with limitations, etc.), especially in conjunction with “domains”, the legal implications should be organized as a category.

- Scope of disclosure

  Organize the scope of disclosure specified in the data, including civil law contracts and internal organizational rules. Note that even if data is internally handled by an organization, there could potentially be a multi-layered application of the limitations of the scope of disclosure if data is transferred between countries or regions, or if it is a deemed export under the U.S. Export Administration Regulations.

- Purpose of use

  When there are restrictions on the purpose of use such as personal information and licenses based on laws and regulations, etc., it is necessary to handle the

data within the scope of the purpose of use throughout the process of continuous distribution from one entity to another and creating added value. Therefore, it is necessary to specify it as a “property”.

- Data controller

  As the supply chain is dynamically constructed, various players will be involved in the data, but at some point, in the data flow, legally or contractually, the entity responsible for managing the data is identified. The entity will be an important promoter when actually taking cyber security measures. In this framework, which puts the focus on data, the data controller also changes in the process of data distribution, and it is treated as one of the “properties” of data. In addition, when using cloud services, or when outsourcing data processing, etc., there are instances where the data controller becomes ambiguous. Therefore, it is important to identify the data controller and appropriately understand the changes.

- Data rights holder

  Apart from the data controller, there can be an entity that has the right to data. Even if an entity receives data as a result of transfer/provision in the value creation process, the data rights holder (i.e., data subject in the case of personal information, and right-holding organizations in the case of business-useful data) is considered to continue to have the right to the data that is managed by the receiver. It needs to be managed as a “property” in the process in which the data controller changes from time to time, for example, in the case of withdrawal of consent under the Personal Information Protection Law, handling of licenses such as copyright law, and providing data related to the competitiveness of a company (i.e., product design data, device/facility operation status at a manufacturing base).

- Value (Importance)

  Identify the business value (importance) of the data. Organizations should adopt appropriate risk countermeasures for systems and organizations that actually handle the data, depending on the magnitude of the identified value. Various methods can be applied depending on the data category, industry, etc. for calculating the value. One example is to evaluate the degree of business impact

that a data breach can cause from the perspective of confidentiality, integrity, and availability, with the largest one being the evaluation value.

- Media, storage destination

  Generally, digitized data is easy to copy, but depending on the data category and the content of the applied policy, it may be necessary to specify the media and services used for storing, processing, and analyzing the data and continuously manage the location of data so that the required level of security can be maintained. The main types of media and storage destinations include portable electronic media, PCs, mobile terminals, in-house servers, and external servers (e.g., cloud services).

- Expiration Date

  If the law, separately concluded contract, related policy, etc. stipulate the expiration date of the data, timeless disposal after completion of use, return to provider, etc., it is necessary to specify the start date and end date of the data use, and manage whether the data remains available even after the expiration date.

3. Utilization method

3-1. Utilization between the supply chain stakeholders

As mentioned in the objective of this framework, this framework puts the focus on data and enables to visualize the state of the data throughout the data life cycle to identify risks to the data. This makes it possible to take the necessary measures to ensure security through appropriate data management.

Stakeholders involved in the value creation process need to share an awareness of the risks faced at each step of the data lifecycle when considering the necessary security measures through the collective activities of multiple entities. Data trustworthiness could presumably be ensured by visualizing the risks using the framework and having each entity implement measures that they each should be implementing while discussing with other entities.

Also, as already mentioned, data is basically neutral and the data in the value creation process and the entities involved in the data should be considered separately. For

example, misuse or abuse of data in circulation can be understood as a problem of the entity who did it, and not a problem of the data itself. Therefore, each entity participating in the value creation process takes responsibility for the collective activities shown in this framework by concluding and fulfilling contracts, etc. after mutually presenting the conditions related to data distribution among the related stakeholders. In addition, it is possible to confirm whether the contract, etc. is being fulfilled by each entity by means of audits, etc. Therefore, it is expected that this framework will also be used for the examination of IT governance (digital governance) by management in the future.

In this framework, the concept of identifying risks related to data that is exchanged between entities is organized. The security measures that each entity should implement against the identified risks have already been summarized in various international standards related to information security that have been published so far. Please refer to existing standards, etc. when selecting specific measures. The main standards are as follows.

< Examples that illustrate the overall risk management process >

- ISO 31000:2019
- ISO/IEC 27001:2013
- NIST SP 800-30 Rev.1

< Examples that illustrate the general security requirements, etc. >

- Data Management Body of Knowledge (DMBOK) 2nd Edition
- ISO/IEC 27001:2013 Annex A, ISO/IEC 27002:2013
- NIST SP 800-53 Rev.5
- CPSF

< Examples that illustrate the details of the security measures, etc. of each event >

- *Generation/acquisition:* How to Secure Your Website 7th Edition8 (when using a website for data generation/acquisition), NISTIR 8259 (when using IoT devices for data generation/acquisition)
- *Transfer/provision*: ISO/IEC 27033-1:2015, NIST SP 800-47 Rev. 1

[8] Information-technology Promotion Agency, Japan (IPA), How to Secure Your Website 7th Edition (in Japanese) https://www.ipa.go.jp/security/vuln/websecurity.html

- *Processing/Usage*: Contract Guidelines on Utilization of AI and Data: Data Section
- *Disposal:* NIST SP 800-88 Rev.1

3-2. Analysis of the gap between the rules

As mentioned in the objective of this framework, this framework can also be used as a model to clarify the difference (gap) between the requirements and measures that are required to ensure data security within various data management rules.

For example, regarding the transfer of personal information from Europe, it is possible to sort out the differences between the United States, where the Privacy Shield was determined to be invalid by the Schrems II decision related to GDPR, and Japan, which has been certified adequacy decision, as follows. Here, in order to simplify the situation, it is assumed that the data will be transferred to an overseas base by the same entity, and the transfer will be within the range of the purpose of use set in advance.

Regarding the transfer from Europe to Japan, the “events” of transfer will move the “domain” from the legal system such as GDPR in Europe to the Act on the Protection of Personal Information and related guidelines in Japan. At that time, since Japan has obtained adequacy decision, it is considered that the data protection required by the European GDPR is substantially secured even under Japan's Act on the Protection of Personal Information and related guidelines. In terms of data properties, only the Japanese base will be added to the data controller. Any changes to the data controller are regarded as having been recognized and allowed beforehand through adequacy decision, assuming that the requirements for the legal processing of personal data according to GDPR are met during relevant processes

On the other hand, when transfers from Europe to U.S. are made through legal means stipulated in the GDPR, etc., the “domain” becomes subject to various U.S. legal systems if the data resides in the U.S. Under the U.S. legal system for example, the U.S. could be deemed as the physical location of the data through a transfer event since such events can be subject to surveillance by the U.S. government agencies to ensure national security, etc. It is thought that when data become physically present in the U.S. through a transfer event, the data controller will change, and the data properties will also change because the U.S. government becomes added to the potential scope of

disclosure. In light of this situation, it is currently required that cross-border transfers of personal data from Europe to the U.S. be based on the conclusion of standard contractual clauses (SCCs) approved by the European Commission[9]. For this reason, it could be argued that there is a gap in the rules for cross-border transfers of personal data from Europe between Japan and the U.S., which conduct such transfers based on adequacy decision.

In this way, visualization of changes to data “domains” and “properties” can help understand the differences in requirements and measures that are required to ensure data security.

[9] Note that even when the SCC is used to transfer/provide data from Europe to the U.S., one must particularly pay attention to the procedures for making disclosures to the U.S. government.

Appendix A. Use Cases

A-1. Analysis of POS Data

The retail and distribution industries, which have direct contact with consumers, traditionally hold diverse and large amounts of data compared to other industries, and proactively use data incidentally generated during sales, purchasing, etc. to improve and optimize customer service. The usage of POS and ID-POS data held by the retail industry is especially progressing.

Businesses are also developing omni-channels to integrate physical stores, EC, etc. Through the proliferation of smartphones and social media (SNS), consumers are now able to gain new purchasing experiences through various sales channels.[10] It is said that businesses can more effectively implement these initiatives by comprehensively utilizing the data gathered through various channels instead of sporadically accumulating and utilizing them on a channel or department basis.

Taking the aforementioned background into consideration, the following data utilization process (hereinafter within A-1, “Use Case”) flow shall be regarded as the Use Case of the framework for the retail/distribution industries.

- Retailer X (Company X), a retailer that has traditionally had stores in various parts of Japan, currently sells products in various channels including physical stores and EC site. They also collect sales data by offering membership, etc. and linking purchaser IDs[11], purchases, etc.
- Data acquired from each channel are individually stored in a way that can be interconnected with other data, and are integrated for marketing, etc. while referencing documents such as various master data (i.e., customer master[12], product master) that are separately created.
- Integrated data can be used in various ways, but here, they are used to display the number of members, sales, etc. of each area by linking them with a map software in order for Business X to optimize their PR efforts such as flyer

[10] Commerce Distribution and Industrial Safety Policy Group of Ministry of Economy, Trade, and Industry, Survey report of the Study Group on the Utilization and Application of Information in the Distribution and Logistics Field (February 2016, in Japanese) https://dl.ndl.go.jp/info:ndljp/pid/11279357

[11] The Use Case presumes that the same member ID is used in physical stores and the EC site.

[12] In this paper, the customer master data of Company X are called “membership information” (i.e., member name, gender, address, contact information).

distribution, ad displays, etc.

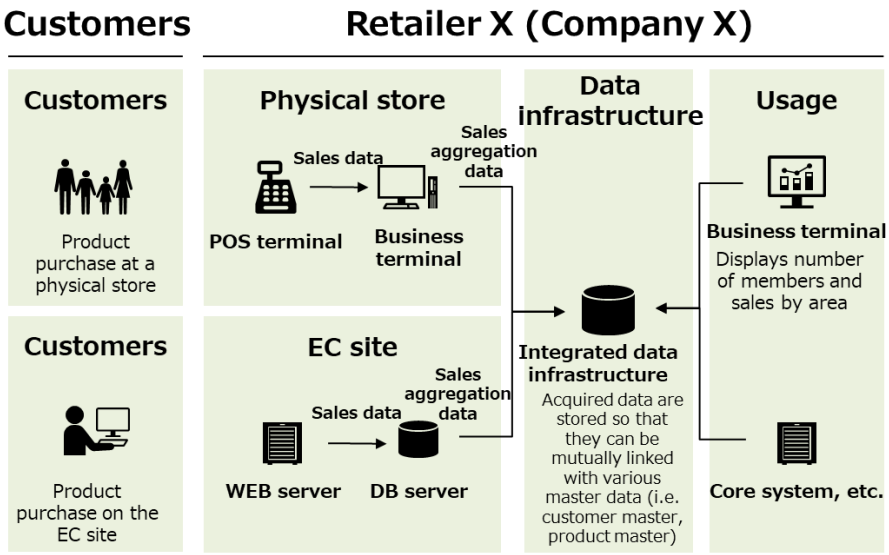


Figure A-1.1: Overview of the target processes

As illustrated in Figure A-1.2, the supply chains of the retail and distribution industries consist of phases such as manufacturing, intermediate distribution, and sales[13]. Each phase is handled by a different business with exceptions like SPA (manufacturing/retail). In the retail/distribution industries, data can also be used for the manufacturing and intermediate distribution phases of the corresponding products. But the Use Case will especially focus on using data such as the sales data in the retail phase for purposes like marketing.

Figure A-1.2: Positioning of the target processes of the supply chains in the retail/distribution industries

When establishing or revising a data utilization mechanism as illustrated in Figure A-

[13]Refer to sections such as “5) Sophistication of the supply chain through collaboration among manufacturing, distribution, and sales of the following: Ministry of Economy, Trade and Industry, Survey report of the Study Group on the Utilization and Application of Information in the Distribution and Logistics Field (February 2016, in Japanese) https://dl.ndl.go.jp/info:ndljp/pid/11279357

1.1, Company X can use the framework to generally implement consistent security measures while maintaining the collaboration between relevant departments (i.e., physical store department, EC department, information system department). In doing so, the following stakeholders should be considered in the Use Case.

- Customers: Those who purchase products from Company X's stores
  - Physical store customers
  - EC site customers
- Company X: Manages/operates stores used by customers
  - Physical store management/operation departments
  - EC site management/operation departments (EC department)
  - Information system department
  - Marketing department
- IT service provider: An entity contracted by Company X to develop, operate, etc. systems

A-1-1. STEP 1 Visualize the data processing workflow ("events")

- *First, visualize the rough data flow and "events" in the assumed data utilization process from data generation/acquisition to disposal.*
- *In that case, the level of event details to be disclosed must be adjusted based on the objectives of the data flow organization. For example, as the "event" of transferring data between a server and a client on an in-house network may differ from the essence of the examination when considering measures when handling data that is circulated between multiple stakeholders, it is omitted. It is also conceivable to substitute by presenting management rules related to data handling and showing that they are handled in accordance with them.*

STEP 1 is the stage of understanding the process by which data is utilized in a series of data life cycles from generation and acquisition to disposal. The Use Case is comprised of the following processes as illustrated in Figure A-1.1.

(1) Individual sales data are generated and acquired every time a customer makes a purchase through a sales channel including physical stores and EC site. Sales

data consist of information such as sales date/time, store, purchased product, price, volume, etc.

(2) Sales data are accumulated as sales aggregation data for each store, site, etc.

(3) After being aggregated into the integrated data infrastructure of Company X, the sales aggregation data stored by each store, site, etc. are processed/used for the integrated sales data that serve as the infrastructure for marketing analysis, etc. that link several sales channels.

(4) Through linkage with a mapping software, the integrated sales data are processed/used for the area-based sales/membership data to optimize PR efforts such as flyer distribution.

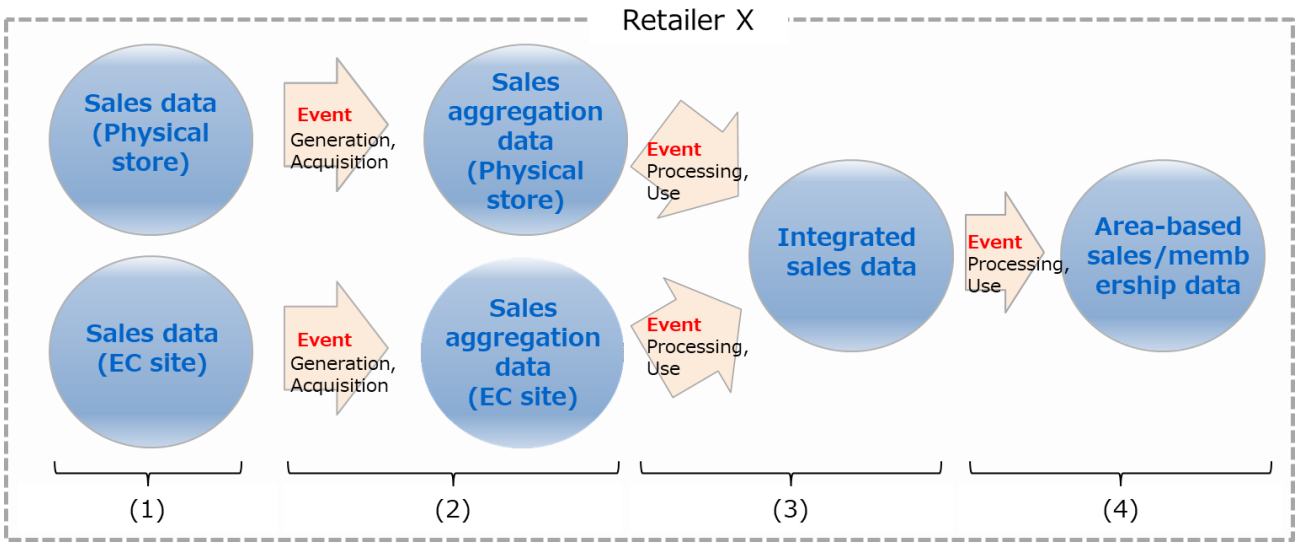


Figure A-1.2: Visualization of data processing flow (POS data analysis)

This was omitted in Figure A-1.2, but in the aforementioned process consisting of four stages (1 through 4), the sales aggregation data, integrated sales data, and area-based sales/membership data are stored in business terminals and various databases over the medium to long term to ensure timely and lawful use of various types of data, and are deleted on a record basis or disposed on a data set basis through appropriate means at the end of their predetermined usage period. If possible, it is ideal in STEP 2 and 3 to identify the data storage and disposal requirements since these are important inputs for identifying the attributes that help manage data in STEP 3.

In addition to the processes illustrated in Figure A-1.2, Company X generates and acquires customer member information through the member registration page of their EC

website, responses to application forms distributed in physical stores, etc. Based on universal member IDs, this information is matched with various sales data and ultimately processed and used for their integrated sales data, etc., which are regarded as personal information. During this process, the member information acquired at physical stores through application forms, etc. are expected to not be stored at the branch office of each store/region to protect personal information and are expected to be centrally managed by the integrated data infrastructure managed by the information system department of the headquarters.

The level of detail in describing events such as generation/acquisition and processing/usage has been adjusted according to the purpose of data flow organization. Here, we extracted those that can be regarded as constituting “trust boundaries”[14] or those that affect business importance or category (i.e., applicability of personal information), which are data attributes that in no small way affect the level of data management and the details of the measures taken.

A-1-2. STEP 2 Organize the necessary institutional safeguards (domains)

- *Examine "domains" that contribute to data protection and set appropriate ones from the perspective of law and contract. At that time, it is conceivable that several "domains" overlap for one data, namely, requests are made for the data from various viewpoints.*

STEP 2 is the stage of understanding the types of data protection rules (standards) also known as domains that are applied to the identified series of data utilization processes. In the Use Case, the following rules can be specified as the domain when considering the nature of the handled data, business type, etc.

(1) Installment Sales Act/PCI-DSS[15]: When using credit cards as a settlement method for a physical store or EC website, participating merchants such as Company X must take measures such as appropriately manage sales data, etc. that

[14] It refers to the boundaries that are drawn where the managing organization or interface changes, as identified in the data flow diagram (DFD) created as part of threat analysis.
[15] It refers to a security standard (Payment Card Industry Data Security Standard) designed to ensure the secure handling of credit card member data by merchants and service providers.

correspond to credit card numbers, etc. and provide information management guidance to their own consignees in accordance with Article 35-16 of the Installment Sales Act. In a practical guideline called the “Security Guideline for Credit Cards,” merchants must either not retain credit card information or comply with PCI DSS if otherwise.

(2) Act on the Protection of Personal Information: Sales data, etc. of various channels can identify individual customers through member IDs. These data alone cannot identify the identities of individuals, but are processed and used as personal data by being matched, etc. with other member information in an integrated data infrastructure, etc. If internal information management rules of Company X prohibit personal data from being handled by the physical stores, data such as sales data must be made so that these cannot be easily matched with other information such as by disabling access of physical store representatives and other affiliates to the integrated data infrastructures, etc. that handle member information. If personal data (i.e., sales aggregation data (EC site), integrated sales data) are to be managed by Company X, then it must adhere to various rules stipulated as obligations of businesses handling personal information in the Act on the Protection of Personal Information such as the obligation to clarify purpose of use, establish restrictions based on the purpose of use, take security control action, establish procedures for third party provisions, etc.

(3) Unfair Competition Prevention Act: Sales aggregation data, integrated sales data, etc. gathered and stored by Company X are usually considered highly valuable to the business. The general consensus is to manage such information as trade secrets in a way that ensure legal protection from fraudulent acquisition, usage, and disclosure.

(4) Internal information management rules of Company X

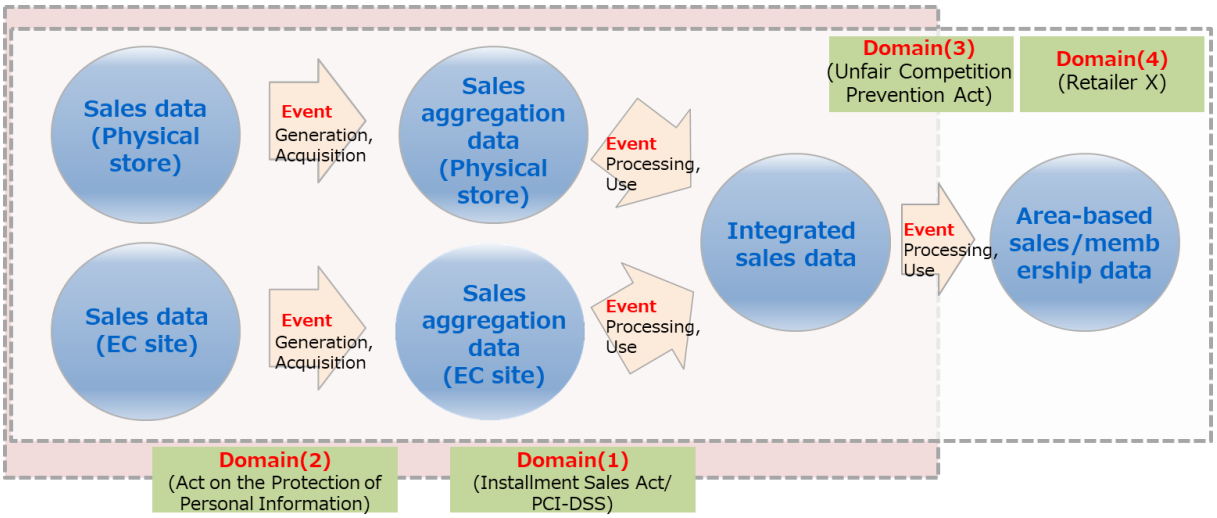


Figure A-1.3: Organization of necessary institutional safeguards (POS data analysis)

A-1-3. STEP 3 Specify the “properties”

- *Identify the "properties" that should be managed based on the set data, "events", and "domains".*
- *In some cases, additions will be made as appropriate while organizing the "properties" of data, if there are any omissions in the "domains" where this data should be handled or when there are "events" that must be implemented.*

STEP 3 is the stage of identifying the data properties that contribute to the effective and efficient adherence of data protection rules (domains) identified in STEP 2. The main properties that must be identified in detail are as explained in section 2-2-3 of this paper, and many of these strongly relate to domains that are identified in STEP 2. The rules that we believe should be considered when configuring the parameters of each property are as follows.

Table A.1-2: Rules (domains) that should be considered when considering the properties

		Installment Sales Act, etc.	Act on the Protection of Personal Information	Unfair Competition Prevention Act	Internal information management rules of Company X
Category	**Personal data protection**		○		
	Intellectual property (including trade secrets) protection			○	
	…	…	…	…	…
Scope of disclosure		○	○	○	○
Purpose of use			○		
Data controller		○	○		○
Data rights holder		○	○		
Value (Importance)		○	○	○	○
Media, storage destination			○		○
Expiration Date		○	○		○

Many of the data introduced in the Use Case fall under the category of personal information, which makes it especially important to appropriately configure purpose of use, expiration date, and scope of disclosure, as well as monitor compliance status, etc. It is ideal to specify the purpose of use and expiration date by referencing the provisions in the membership agreement, etc., as well as limit the scope of disclosure to only the essential internal affiliates to maintain the confidentiality of the trade secrets according to the “need to know” principle[16] and “need to use” principle[17]. The following are examples of possible parameters of data presented in the Use Case that have been embodied through the consideration of the aforementioned.

[16] The idea that only access to information necessary to carry out their respective duties should be granted
[17] The idea that only access to IT devices, applications, procedures, rooms, etc. necessary to carry out their respective duties and tasks should be granted

Table A-1.1: Examples of property parameters of data presented in the Use Case

		Sales data (Physical store)	Sales aggregation data (Physical store)	Integrated sales data	Area-based sales/membership data
Category	**Personal data protection**	personally referable information, etc.	personally referable information etc.	Personal data	Statistics (Non-personal information)
	Intellectual property (including trade secrets) protection	Trade secret	Trade secret	Trade secret	Trade secret
	…	…	…	…	…
Scope of disclosure		Internally within Company X[18]	Internally within Company X	Internally within Company X	Internally within Company X
Purpose of use		• Execution of sales contract • Implementation of various after-sales services • Product planning, development	Same as on the left	Same as on the left	Optimize PR activities
Data controller		Each physical store	Each physical store	Information system department	Information system department, marketing department
Data rights holder		Purchaser, Company X	Purchaser, Company X	Purchaser, Company X	Company X
Value (Importance)		Moderate	High	Extremely high	High
Media, storage destination		POS terminal (Located in the stores)	Business terminal (Located in the stores)	Internal server (Integrated data infrastructure)	Internal server, business terminal
Expiration Date		Five years from the end of the membership agreement	Five years from the end of membership agreement (for each record)	Same as on the left	None in particular

As for the categories, the data to be handled can be specified as data that should be managed as personally referable information[19], individual data, or non-personal

[18] Several internal departments of Company X are involved in the data utilization in the Use Case. But to clarify the division of responsibilities among the departments concerned, it is ideal to specify the scope of disclosure in more detailed units such as departments and roles for actually managing assets.

[19] Refers to information relating to a living individual which does not fall under personal information, pseudonymously processed information, or anonymously processed information; the same applies hereinafter. (Article 26-2 (Paragraph 1) of the Act on the Protection of Personal Information) Examples include an individual's website browsing history, product purchasing history, and service usage history collected through cookies and other terminal identifiers.

information under the Act on the Protection of Personal Information, or as trade secrets under the Unfair Competition Prevention Act, to comply with various rules configured as domains. During this process, precaution must be taken about how the same data could be classified in various ways due to the varying systems (i.e., personal information protection, trade secret protection). We must especially accurately recognize that the positioning of data within the Act on the Protection of Personal Information is changing within the utilization process, and each data must be managed differently[20].

The above presents data in tabular form and their properties. But it is also effective to enter the attributes in figures created up until STEP 2 like Figure A.1-4 to illustrate a more advanced bird's eye view of the relationship between changes in data properties and events in the overall data utilization process.

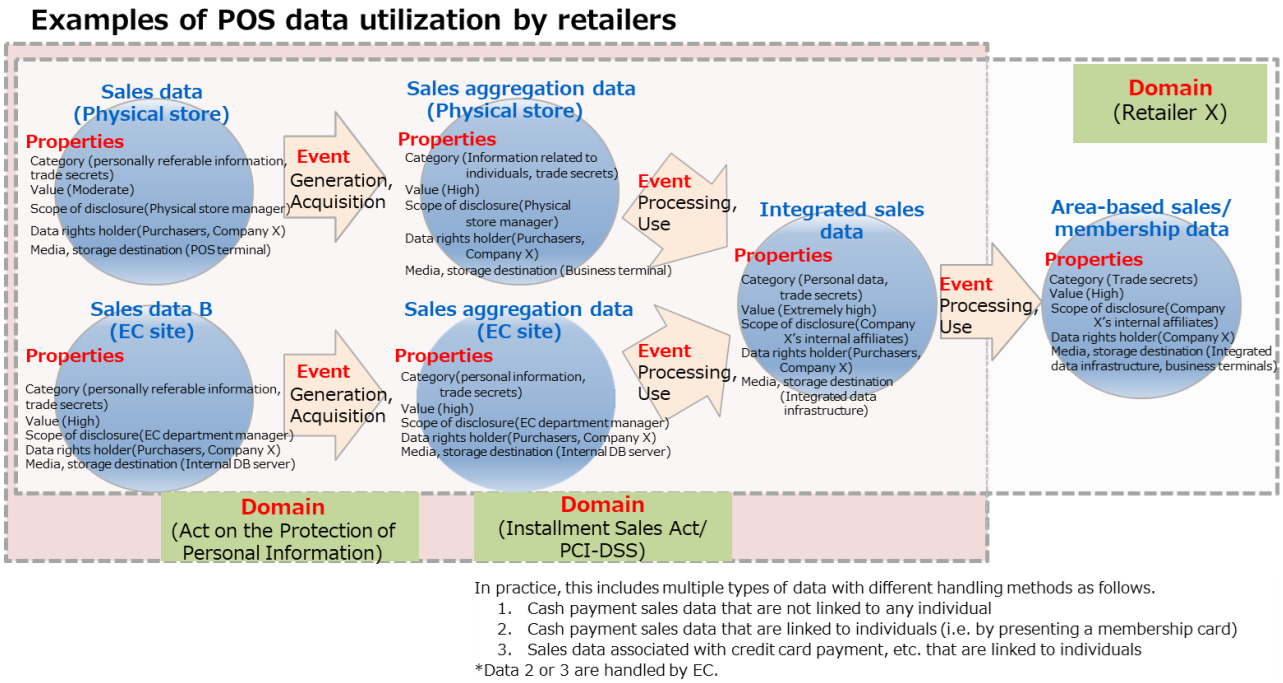


Figure A.1-4: Examples of how to present properties

[20] For example, individual sales data cannot always be said to be usable for identifying the individual at the stage when it is generated at a POS terminal. However, sales aggregation data stored in business terminals of stores can be used to easily identify a specific individual by comparing it with the membership information managed by the terminal.

A-1-4. STEP 4 Identify the risks of each “event”

- *The risk assumed for each "event" is extracted and the set "property" is reviewed from the viewpoint of the "domain" set.*
- *Risks must not only be identified from the perspectives of cybersecurity (i.e., confidentiality, integrity, availability), but also from the point of view of compliance (i.e., laws, regulations).*

A-1-4-1. Identify the risks of each “event”

STEP 4 is the stage of identifying the expected risks in terms of security, relevant laws, and regulations, etc. within the data utilization process that has been detailed up until STEP 3. Out of the Use Cases for example, the following risks can be expected regarding the generation/acquisition of sales aggregation data (EC site) illustrated in Figure A.1-4 and the incidental storage process from the viewpoint of security protection (confidentiality, integrity, availability), relevant legal system (personal data protection, intellectual property (including trade secrets) protection), etc.[21] The same considerations as below are made in a similar way for other data and events in the overall process.

Table A.1-2: Examples of possible risks of generating, acquiring, and storing sales aggregation data (EC site)

Major classification	Middle classification	Examples of possible risks of generating, acquiring, and storing sales aggregation data
From the viewpoint of security protection	Confidentiality	● Sales aggregation data become leaked after the internal DB server that stores them are fraudulently accessed by a malicious third party. ● Sales aggregation data stored in an internal server become intentionally taken out by a legitimate employee.
	Integrity	● Fraudulent product transactions are carried out by impersonating a legitimate user. ● Sales aggregation data stored in an internal server become intentionally tampered by a legitimate employee.

[21] See Appendix B for existing frameworks, etc. that can be applied when comprehensively extracting risks (threats) that should be considered.

	Availability	● EC site transactions become temporarily suspended due to denial of service attacks, etc. ● The internal server where the sales aggregation data are stored becomes infected with malware, and the said data become encrypted, etc., and therefore unusable. ● A malfunction occurs in the facilities or devices related to the operation of the EC site, resulting in a temporary suspension of transactions. ● A natural disaster (earthquake, tsunami, etc.) causes damage to facilities and devices related to the EC site operation, resulting in a temporary halt to transactions.
From the viewpoint of relevant legal systems	Personal data protection	● Rules, etc. do not clearly indicate the purpose of use of the generated/acquired sales data or the purpose is not aligned with the actual use. ● Employees handling sales aggregation data are not appropriately supervised.
	Intellectual property (including trade secrets) protection	● Sales aggregation data become acquired, disclosed, and used through fraudulent means by a malicious third party.
	. . .	. . .

Note that after identifying the risks, you can review again the attributes that reduce the said risks and add them as necessarily to the progress in STEP 3.

A-1-4-2. Considering the challenges for the further sophistication of data management

Through the process of applying the framework from STEP 1 to STEP 4, Company X can properly understand the specific nature of its data utilization and the risks that lie within it and strengthen the foundation for continuously improving its risk management. Depending on the current state of data management by Company X, the specific improvement proposals will vary widely and may include the following for example.

- Strengthen data handling governance of physical stores, etc.
  The physical stores, which domestically exist numerously, handle personal information such as sales data and sales aggregation data. But it could be presumably difficult for them in some cases to uniformly ensure a high level of data protection because they are different from integrated data infrastructure, EC

site, etc. In the Use Case, the physical stores are prohibited from pairing their data with member information that is separately collected and the stores in general are prohibited from handling personal information to address the aforementioned concerns. To ensure accurate management, specific measures can be considered such as reviewing the accesses from physical stores, etc. of member information managed by the integrated data infrastructure, and reviewing the operation rules including access control policies, after considering the need of each physical store to access personal information.

- Considerations of protective measures based on actual data usage by marketing departments, etc.
  After verifying the actual usage patterns of integrated sales data, etc. managed by the integrated data infrastructure, as well as the compliance level to one's personal information protection policy and disclosures such as membership agreement (i.e. provisions regarding the purpose of use), regardless of the usage format illustrated in Figure A-1.2, the following measures can be possibly considered if activities deviate or could potentially deviate in the future from the initial purpose of use.

  - Revise relevant provisions (i.e., clauses regarding purpose of use) such as personal information protection policy and membership agreement, notify customers, and conduct other necessary procedures
  - Processing and usage as pseudonymized information, such as integrated sales data, and anonymously processed data

A-2. Implementation of elderly life support projects

Due to the proliferation of IoT through consumer products in recent years, a wide variety of devices, such as home appliances, wearables, and sensors, are now capable of collecting lifestyle information. A rapid increase is expected in the number of smart homes, which are defined as “a new way of IoT living[22] that promotes services geared towards various lifestyles and needs of the child-rearing generations, seniors, single people, etc.”

An example of specific measures that aim to facilitate the development of smart homes is the elderly life support services that utilize data collected from homes and facilities. Regarding the elderly life support, it has been advocated for some time to materialize the community-based comprehensive care system, which uniformly provides support for housing, medicine, long-term care, prevention, and lifestyle. But it has also been recognized that the lack of services to support the elderly in terms of both quality and quantity is an issue, partly due to the lack of data to accurately understand the living conditions and health status of the elderly at home.

Based on the aforementioned background, we have decided to showcase elderly life support projects (hereinafter within A-2, the “Use Case”) that utilize data held by various businesses as a use case of the framework in the smart home field[23].

- Through numerous groups of devices installed in general detached homes, fee-based senior homes, etc., data regarding elderly life and health conditions are generated and accumulated in servers operated by each of the device vendors (Companies A through D).
- Device vendors provide the collected data to the data infrastructures operated by third parties (platform providers) in exchange for earning fixed revenue. Data provided by the device vendors are aggregated on the data infrastructures in a way that prevents the identification of specific individuals and are processed into

[22] “Cyber/Physical Security Guidelines for the Safety and Security of Smart Homes Formulated” (https://www.meti.go.jp/english/press/2021/0401_004.html) (https://www.meti.go.jp/press/2021/04/20210401005/20210401005.html , in Japanese)

[23] For details about the Use Case, please refer to the *FY2018 Final Report - Groundwork Project for Creating Industrial Models Using IoT* (R&D theme no. 6: Development of advanced utilization system of life data using IoT technology (Research and development of life support service platform for the elderly by life data from IoT home appliances and sensors))

higher-level data including information about elderly lifestyle rhythm and well-being.

- Such data including information about elderly lifestyle rhythm and well-being are provided by these third parties to other service providers as needed and are linked with data subject individuals to provide more advanced support services. To provide services such as elderly monitoring, we presume that these service providers obtain consent from the data subjects in advance regarding the linkage of data acquired by various devices to the specific residents and the process of utilizing these data acquired from devices.
- Device vendors (Companies A through D), platform providers, services providers, etc., that are directly or indirectly affiliated with the service provision, form a consortium, and develop commonly applied rules, share timely information, etc.

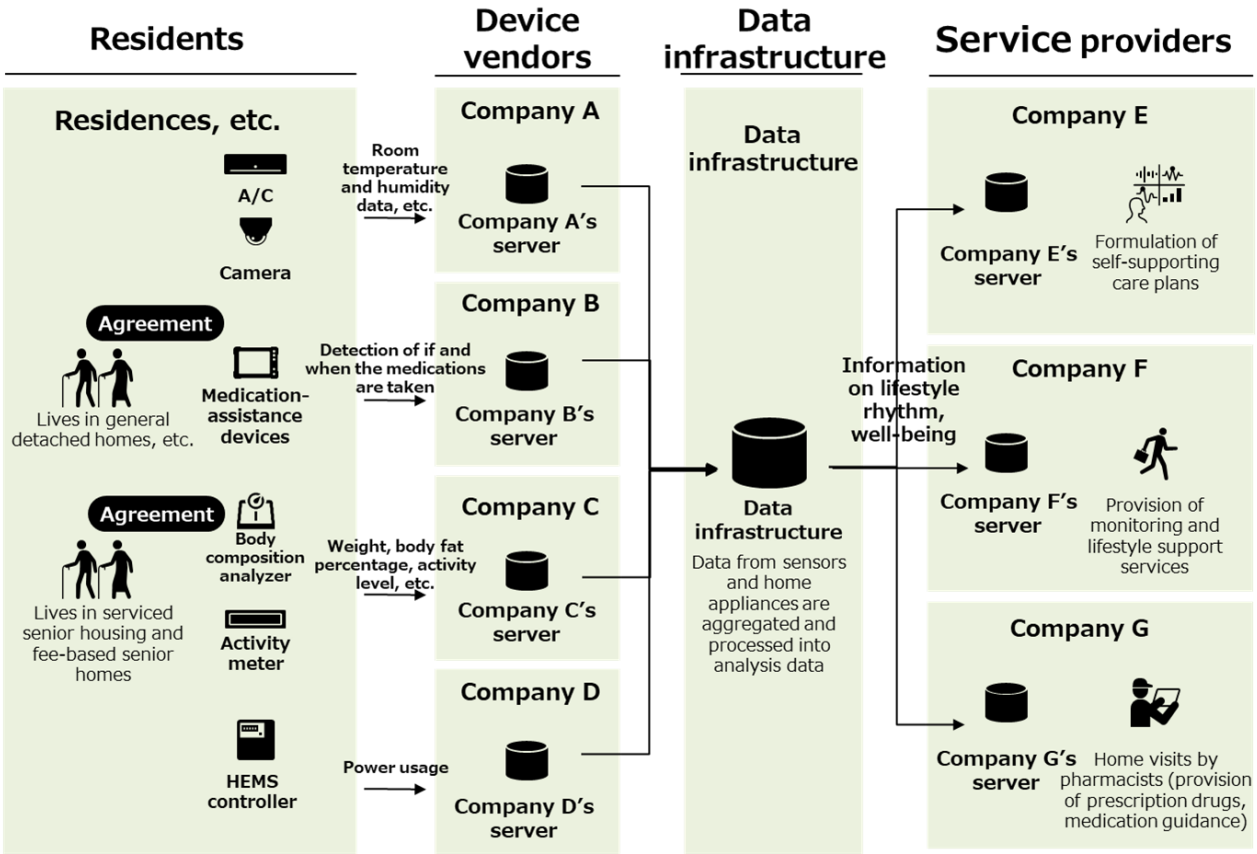


Figure A-2.1: Overview of the target processes

As illustrated below, there are a large number of stakeholders associated with the Use Case. Since handled data consist of information that could be regarded as sensitive personal data, the consortium, etc. must deliberate the matter and implement an

adequate level of data protection measures across the entire supply chain surrounding data usage.

- Residents: Entities who use various IoT devices and services on a daily basis and provide data about themselves incidentally generated to service providers upon completing appropriate procedures including giving consent to data usage.
  - Elderly people living in general detached homes, etc.
  - Elderly people living in serviced senior housing and fee-based senior homes
- Device vendors (Companies A through D): Manufacturers and sellers of devices that are installed in houses and facilities that collect and manage data acquired from operating devices upon completing appropriate procedures including gaining individual consent.
  - Company A: Manufactures and sells household IoT devices including A/Cs and monitoring cameras and uses the collected data for their in-house services and also provides them to platform providers.
  - Company B: Manufactures and sells medication-assistance devices that detect the presence or absence of prescription medication, the time it was taken, etc., and uses the collected data for their in-house services and also provides them to platform providers.
  - Company C: Manufactures and sells healthcare devices such as body composition meters and activity meters and uses the collected data for their in-house services and also provides them to platform providers.
  - Company D: Provides a service for visualizing power usage status of smart meter-implemented homes, and also provides the collected data to platform providers.
- Platform provider: Aggregates data gathered from devices installed in homes and facilities and processes and analyzes them as appropriate.
- Service providers (Companies E, G): Uses data from the platform providers to provide more advanced elderly support services.

In establishing such a mechanism of cross-organizational data utilization, we hope

that stakeholders will use the framework to streamline the process of sharing with each other the possible risks in each stage of the data lifecycle in a setting such as the consortium and of discussing with other stakeholders about the measures that each stakeholder should be taking.

A-2-1. STEP 1 Visualize the data processing workflow (“events”)

The data processing flow in the Use Case consists of the following processes, as shown in Figure A-2.2.

(1) After completing appropriate procedures such as gaining individual consent, various data are generated and acquired through devices installed in elderly homes and facilities and are transferred and provided to servers managed by device vendors (Companies A through D), and finally accumulated and stored as integrated data. It is presumed that these data are linked to the device identifier information when acquired, and the device vendors do not know which residence the said device is from. This is omitted from the figures to prevent complication, but as illustrated below, numerous devices provided by several providers are installed in residences and facilities. Since the number of installed devices may increase or decrease based on demand for utilization, residents, device vendors, etc. should detect the changes in the device composition and manage them appropriately.

Table A-2.1: Main installed devices and collected data

Manufacturers/sellers	Name	Collected data
Company A	A/C	Room temperature and humidity information
	Monitoring system using radio wave sensors	Respiratory conditions, activities, and movements on bed
	Communication camera	Room temperature, human movement, video
Company B	Medication-assistance devices	Detection of if and when the medications are taken
Company C	Activity meter	Activity level, steps
	Body composition analyzer	Weight, measurement date/time
Company D	Power usage aggregation platform using HEMS	Power usage

(2) Integrated data held by each device vendor are transferred and provided to the data

infrastructures operated by the platform providers, and then integrated and stored. It is presumed that the integrated data are managed based on the user identification information linked to the device identifier information and are configured so that individuals cannot be identified from the said data. Based on the purpose of this study, which is to develop a mechanism for cross-organizational data utilization, the flow omits the in-house data that are individually utilized by each device vendor and focuses more on the data transfers and provisions between the providers.

(3) Integrated data received by each vendor and aggregated in the data infrastructure are processed and used as high-order data (i.e., information about lifestyle rhythm, well-being) that suit the usage by the service providers. Note that in the processes of (2) and (3), handled data are not linked to specific individuals.

(4) High-order data are transferred and provided from the platform providers to the receiving entities after reviewing necessary information according to the service content of the entities and individual requirements and are cross-checked with the service user data separately held by the service providers, and then finally processed and used as “data for service provision.”

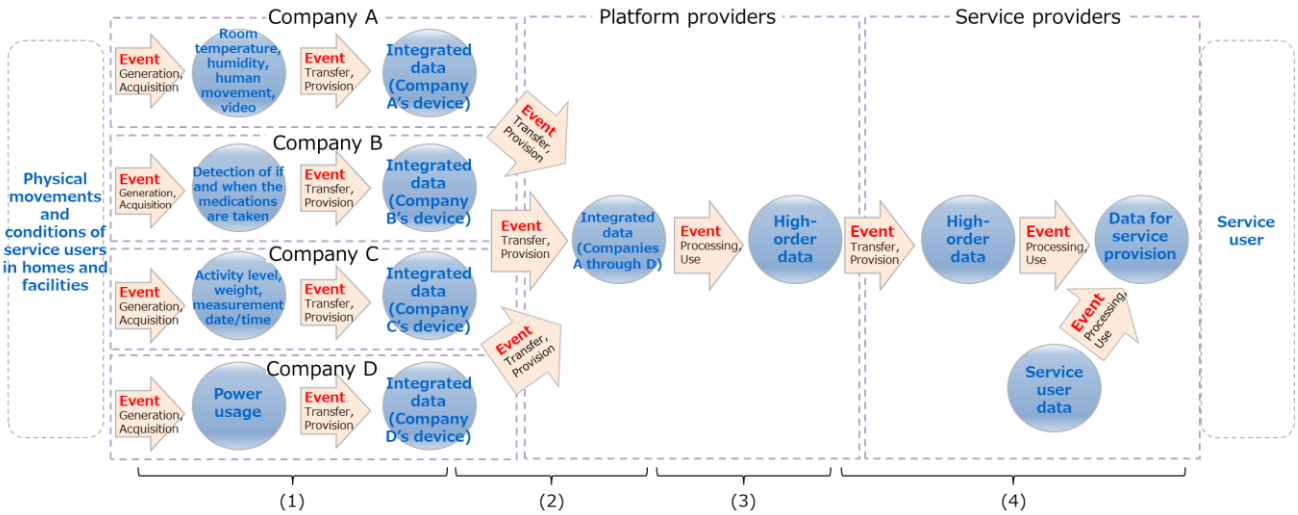


Figure A-2.2: Visualization of data processing flow (provision of elderly life support projects)

A-2-2. STEP 2 Organize the necessary institutional safeguards (domains)

Considering the fact that the handled data in the Use Case are personal information and the said data are provided to numerous businesses, the following rules, for example, as well as rules that are not necessarily explicitly stated by each company, could potentially be identified as the domain.

(1) Act on the Protection of Personal Information: Since data used in the Use Case are personal information of the residents (elderly people in this case) and processed by service providers in a way that can identify the specific individuals in order to ultimately provide services to these residents, the said data are believed to fall under the category of “personal data” or “personally referable information” according to the Act on the Protection of Personal Information[24]. Since “data for service provision” are regarded as personal data, it is presumed that service providers fall under the category of personal information-handling businesses and that data collected by device vendors and integrated data aggregated into platforms are managed in a manner that is not necessarily tied to specific individuals based on anonymous user-identifying information and device-identifying information. Therefore, the said data are believed to fall under the category of “personally referable information,” etc., rather than “personal data.” Since it can be easily presumed that such data can be acquired as personal data by the data-providing service providers, it should be kept in mind that device vendors and platform providers are obligated to verify the acquisition status of individual consent as a business handling information related to individuals, as well as to retain records in the case of data providers. On the other hand, if the integrated data held by the device vendors or platform providers become managed as “personal data” and provided to service providers, which would deviate from the expectations surrounding the Use Case, then mechanisms like the following could presumably be implemented so that such personal data could be smoothly provided between businesses participating in the consortium based

[24] Applicable entities must make careful considerations as to which information type the corresponding data will fall under according to the Act on the Protection of Personal Information while also considering the trends in the revisions of the said act.

on the reasons indicated in Article 23, Paragraph 5 of the Act on the Protection of Personal Information[25].

- Entrustment (Related to Article 23, Paragraph 5, Item 1 of the Act)
  If a data-providing business (a device vendor or platform provider) commissions a service provider, etc. to handle all or part of the personal data within the scope necessary to satisfy the purpose of use, the said data-receiving entity shall not be considered as a third party.
- Joint utilization (related to Article 23, Paragraph 5, Item 3 of the Act)
  If the individuals are notified beforehand regarding the list of personal data jointly utilized by the device vendors, service providers, etc., the scope of shared usage, the purpose of use of the data users, and the name or alias of those responsible for managing the said personal data, then the entities receiving the said personal data shall not be considered as a third party.

(2) Terms of device use: Concluded between the residents and the device vendors. Although data collected in the Use Case do not necessarily fall under the category of "personal data" by themselves, it can be presumed that resident consent must be obtained regarding the rules that are prescribed for data handling, etc. (i.e., provision of data acquired from devices to platform providers).

(3) Data provision agreement: In the Use Case, it is presumed that advanced services can be provided to the elderly by streamlining data transfer between device vendors and service providers through the platform providers. The distribution of data may involve risks such as leakage of trade secrets and invasion of privacy. Appropriate contractual and technical measures could minimize risks by clarifying the roles and divisions of responsibility of each entity.[26] Therefore, businesses must mutually discuss and agree on various requirements, etc. regarding the following two types of data provision events while also incorporating residents into

---

[25] For the specific provisions, etc., refer to sections such as Section 3-4-3: Cases in which entities are not considered third parties (Related to Article 23, Paragraphs 5 and 6 of the Act)) of the *Guidelines for Protection of Personal Information* (General Provisions) (in Japanese)
https://www.ppc.go.jp/personalinfo/legal/2009_guidelines_tsusoku/.

[26] For details on agreement matters that must be considered, refer to the section on agreements (sharing data through platforms) in a section called “No. 6 “Data sharing type (platform type)”) of *Contract Guidelines on Utilization of AI and Data Version 1.1* (in Japanese)
https://www.meti.go.jp/press/2019/12/20191209001/20191209001.html.

the discussion.

- Provision from device vendors to platform providers (Domain (3) in Figure A-2.3)
  - What type of data should be provided to the platform providers?
  - Under what purposes and methods could the platform providers use the provided data?
  - How should the authority to use derived data and other artifacts resulting from processing, etc. by the platform providers be handled?
- Provisions from platform providers to service providers (Domain (4) in Figure A-2.3)
  - Which components of data received from device vendors should be provided to each service provider based on the details of the services that are scheduled to be provided?
  - For what purposes and in what ways can the service providers use data and services?
  - How should the authority to use derived data and other artifacts resulting from processing, etc. by the service providers be handled?

(4) Service agreement: An agreement concluded between a resident and service providers that consists of provisions regarding service details, provision period, and handling of acquired personal data. Since service providers in the Use Case not only acquire personal data individually, but also acquire resident data from various devices provided by the device vendors, they should debrief the process to ensure transparency for the residents regarding the overall data utilization

process.

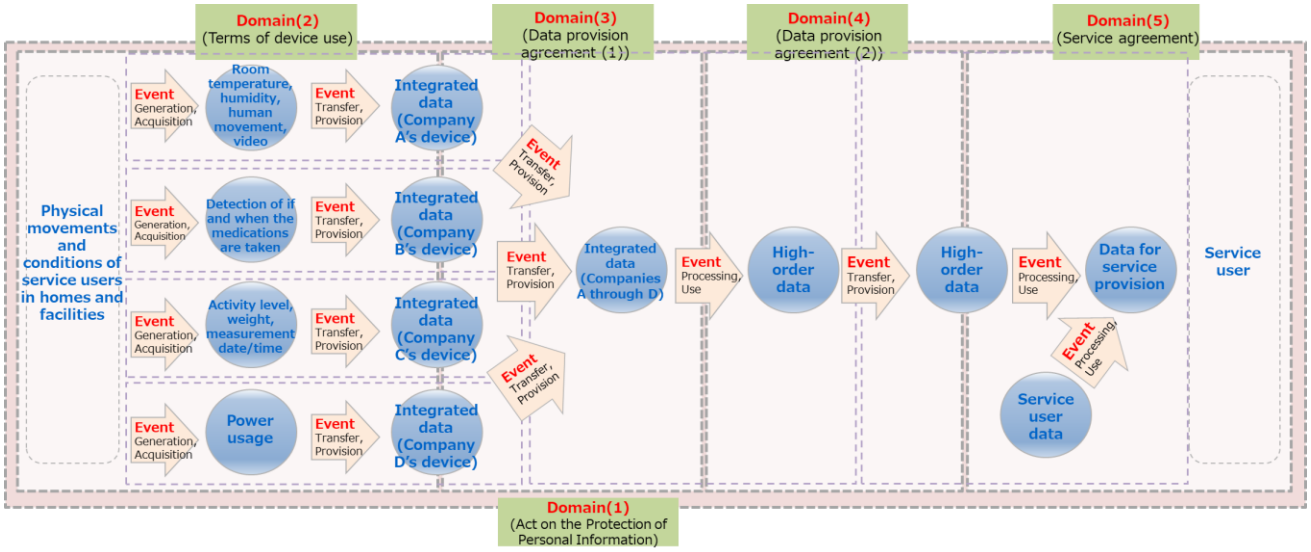


Figure A-2.3: Organization of necessary institutional safeguards (Provision of elderly life support projects)

A-2-3. STEP 3 Specify the “properties”

Specify the properties for managing various data considering the domains that were identified in the previous step. Since information regarding individuals (i.e., the elderly) are handled in the Use Case, the Act on the Protection of Personal Information is a rule that should also be referenced when considering the properties. Furthermore, the various contracts and rules concluded between the parties are useful in identifying matters that also relate to the divisions of responsibility between businesses such as scope of disclosure, data controller, expiration dates, etc.

Table A.2.2: Rules (domains) that should be considered when considering the properties

		Act on the Protection of Personal Information	Terms of device use	Data provision agreement	Service provision agreement
Category	**Personal data protection**	○			
	Intellectual property (including trade secrets) protection			○	
	…	**…**	**…**	**…**	**…**
Scope of disclosure		○	○	○	○
Purpose of use		○	○	○	○
Data controller			○	○	○
Data rights holder		○	○	○	○
Value (Importance)			○	○	○
Media, storage destination			○	○	○
Expiration Date			○	○	○

Many of the data handled in the Use Case fall under the category of personal data, personally referable information, etc. Data collected from devices can be considered to fall under the category of personally referable information, etc. as long as these are not paired with other user data, etc. But if these could presumably become personal data in the hands of third parties receiving the data, then it becomes important to verify that individual consents are being obtained. Hence, as subsequently mentioned, the status of consent acquisition, etc. should ideally be managed separately from the property items shown above. The following are examples of possible parameters of data presented in the Use Case that have been embodied through the consideration of the aforementioned.

Table A-2.3: Examples of attribute parameters of some of the data presented in the Use Case

		Integrated data (Company A)	**Integrated data (Companies A through D)**	**High-order data**	**Data for service provision**
Category	**Personal data protection**	Personally referable information, etc.	Personally referable information, etc.	Personally referable information, etc.	Personal data
	Intellectual property (including trade secrets) protection	Trade secret (Company A)	Trade secrets, etc.[27] (PF providers)	Trade secret, etc. (PF providers)	Trade secret (Service providers)
	…	**…**	**…**	**…**	**…**
Scope of disclosure		Internally within Company A	Internally within PF providers	Internally within PF providers	Internally within service providers
Purpose of use		Provision of various services using the acquired data	Same as on the left	Same as on the left	Same as on the left
Data controller		Company A	PF providers	PF providers	Service providers
Data rights holder		Residents, Company A	Residents, device vendors, PF providers	Residents, PF providers	Residents, Service providers
Value (Importance)		High	Extremely high	Extremely high	Extremely high
Media, storage destination		Company A's server	PF provider's server	PF provider's server	Service providers Server
Expiration Date		None in particular	One year from the end of the data provision agreement	One year from the end of the data provision agreement	Until the end of the service provision period

The above presents data in tabular form and their properties. As in Figure A.2-4, you can enter the properties in figures created up until STEP 2 to illustrate a more advanced bird's eye-view of the relationship between changes in data properties and events in the overall data utilization process.

[27] Data presented in Table A-2.3 that are shared between specific businesses can presumably fall under the category of "provided data with limitations" under the Unfair Competition Prevention Act.

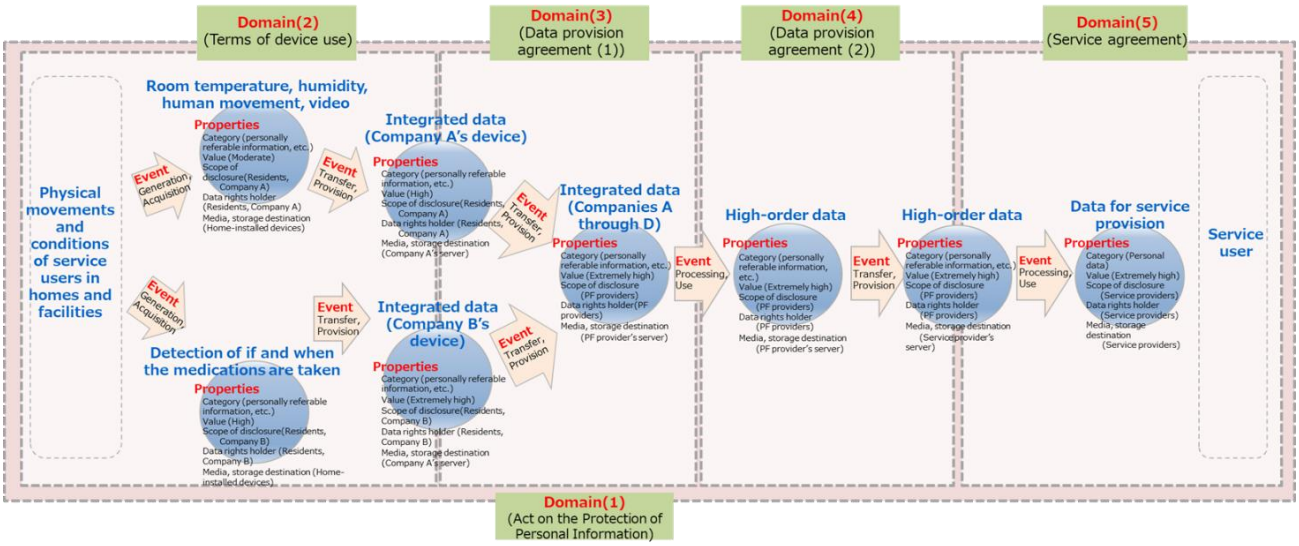


Figure A.2-4: Examples of how to present properties

A-2-4. STEP 4 Identify the risks of each “event”

A-2-4-1. Identify the risks of each “event”

Based on the rules (domains) that should be recognized and data utilization flow that have been identified so far and the details of the properties that help data management, the following kinds of risks can be expected in the transfer/provision process of integrated data held by the device vendors illustrated in Figure A.2-2 among those described in the Use Case. The same considerations as below are made in a similar way for other data and events in the overall process.

As already mentioned, risks pertaining to the relevant transfer and provision events can be organized based on the four categories (country/region, organization/person, system/service, and device). In the Use Case, the following types of risks can be identified as examples.

<Country/region>

- Not applicable since data transfers and provisions between countries or regions are not expected

<Organization/person>

- Before providing the integrated data, the information-providing device vendor fails to verify whether the information-receiving platform provider will acquire this data as personal information.
- When identifying individuals on a platform, the data becomes provided to the platform provider without proper steps such as obtaining the consent of the resident.

<System/service>

- A malicious third party intercepts the communication between the server managed by the device vendor and the server operated by the platform provider, causing communication leakage.

<Device>

- A malicious internal or external entity transmits information from a server managed by the device vendor to a destination (i.e., server) that was not originally intended to be connected to.

Table A.2-4: Examples of possible risks of transferring and providing the integrated data of device vendors to PF providers

Major classification	Middle classification	Examples of possible risks of transferring and providing the integrated data of device vendors to PF providers
From the viewpoint of security protection	Confidentiality	● A malicious third party intervenes in the communication between the server managed by the device vendor and the platform provider's server, and the communication contents become leaked. ● A malicious internal or external entity transmits data from the server managed by the device vendor to servers, etc. that were not initially designed to be connected to.
	Integrity	● A malicious third party intervenes in the communication between the server managed by the device vendor and the platform provider's server to alter the data.
	Availability	● A malicious third party conducts a DoS attack that randomly calls for the API of the data infrastructure, thereby suspending the processes of the platform provider’s server.
From the viewpoint of relevant legal systems	Personal data protection	● Before providing the integrated data, the data-providing device vendor fails to verify whether the data-receiving platform provider will use the data as personal information. ● When identifying specific individuals on a platform, the data are provided to the platform provider without obtaining consent, etc. from the resident.

	Intellectual property (including trade secrets) protection	● The integrated data of each company are acquired, disclosed, or used through fraudulent means by a malicious internal or external entity.
	…	●

If it is presumed that data such as personally referable information will be acquired as personal data to provide advanced services, etc. by data providers as seen in the Use Case, greater risks could potentially manifest in terms of confidentiality, personal data protection, etc. Such risks include not only the usual cyber security risks such as data leakage, etc. by external attackers, but also fraudulent data usage (including both intentional and unintentional) by legitimate businesses. Considering the relevant regulations in the context of the Use Case, privacy protection risks can be presumably reduced by conducting measures indicated in A-2-3, as well as measures to identify factors, such as consent acquisition status regarding the processing of the aforementioned data and data validity, as properties that should be managed, and measures to ensure that relevant organizations, etc. design and build data management mechanisms within their policies and systems.

A-2-4-2. Considering the challenges for the further sophistication of data management

As clarified through the process of applying the framework from STEPS 1 through 4, numerous businesses are involved in the process of collecting data from various devices, processing the said data, and finally using these data as illustrated in the Use Case. In such a complex business structure, there are specific risks rooted in the interdependence of businesses. If this kind of system is foreseen in advance or is currently in place, it could be presumably effective for each participating member of the consortium to use its framework and mutually collaborate to reduce the risks. The measures necessary to achieve this are presumably very diverse when considering the complex data utilization process, but the following examples are good candidates for this.

- Indication of purpose of use, acquisition of consent, etc. that cater to the complex data utilization process

  In a complex business structure involving a large number of devices, services, and providers, as in the Use Case, it is more difficult to ensure transparency of the data utilization process for the residents (data subjects). Considering the fact that sensitive data including health status and detailed activity logs are also utilized in the Use Case, there could be a service continuity issue in the worst case scenario. To reduce the risks associated with the transparency of such data utilization, it is important to present and clearly explain to the data subjects (residents including the elderly) the bird's eye-view of the services including the roles of each provider, the benefits for the data subjects, and the comprehensive policies for handling personal data, etc. Such measures, however, place a certain level of burden on the providers and service users, which has given rise to issues such as excessive consent acquisition. Hence, it is ideal to consider methods that take such burden into consideration.

- Ensure security, etc. of various IoT devices that may be related to the generation and acquisition of sensitive data

  In the Use Case, various numerous manufactured devices such as A/Cs, medication-assistance devices, and activity meters are used especially in the data generation/acquisition stage. Security management of information systems, where such data is aggregated and processed in an integrated manner, has always tended to be an issue. However, security measures for peripheral IoT devices that generate and acquire such data are still being developed in many cases despite the fact that these devices are important elements for ensuring data trustworthiness. Depending on the device, relatively sensitive personal data could be handled. Hence, it is ideal for device vendors to implement security measures at an appropriate level and for relevant providers and service users to verify such measures while considering the possible risks and their magnitude.

A-3. Examples of providing services using IaaS, PaaS, SaaS, etc.

As the promotion of value creation through digital technology is being recognized as a societal challenge, cloud computing technology is garnering attention as an important base technology and the number of cloud service users is significantly growing. The appropriate usage of such services is expected to benefit the users by optimizing expense burdens and implementation time cost and improving the security level, flexibility, and the ability to adapt to technological innovation[28].

Concerns such as those of security levels that have conventionally been recognized as problematic have been lessening through improvements in cloud infrastructure security, enhancement of user support functions, etc. However, it has been pointed out that there are still unresolved issues such as increase in the number of incidents due to configuration errors, etc. of cloud users themselves arising from insufficient recognition of division of responsibility between the service providers and users, as well as lack of transparency in the geographic location, etc. of data due to system complication[29].

In light of the aforementioned circumstances, the following data utilization process flow (hereinafter within A-3, the “Use Case”) based on cloud services illustrates an example of considerations that ensure the clarification of division of responsibilities between providers and data flow transparency.

- Company A provides not only products and services through their physical stores under their conventional business model, but also has been striving in recent years to further enhance customer value, such as by building a member portal site and using customer management services (SaaS).
- By registering and logging in to Company A’s portal site, customers can download images and video data onto their own PCs and smartphones. Through the portal site, customers can also purchase related products. Previously, Company A’s employees burned the taken images and videos on a medium such as CDs and DVDs and mailed them to customers. The implementation of this system has been

[28]Basic policy on the use of cloud computing services in government information systems (in Japanese) (https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20210330kihon.pdf)

[29] For risks of using cloud services, refer to A. (Reference) Risks of using cloud services in Annex of the *Information Security Management Guidelines for the Use of Cloud Computing Services* (2013 Version, in Japanese) https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf by METI; and *Top Threats to Cloud Computing The Egregious Eleven* by Cloud Security Alliance (CSA).

beneficial in significantly reducing the man-hours needed to deliver the images and videos to customers and allowing customers to view the taken images and video data from various terminals, process and download data based on preference, etc.

- Company A's portal site is built on PaaS (web app development/operation platform) provided by Company B. Information about members, product purchases, etc. acquired on the site is not only stored in the customer DB that comprises the portal site, but also shared with Company's customer management system that is separately provided as SaaS by Company B for managing product sales, etc.
- Company A uploads images and video data taken by customers in studios, etc. to its own online storage using SaaS provided by Company C. As aforementioned, customers can access this storage through the portal site and download and process their own image and video data. Histories such as data download are periodically shared with the customer management system.

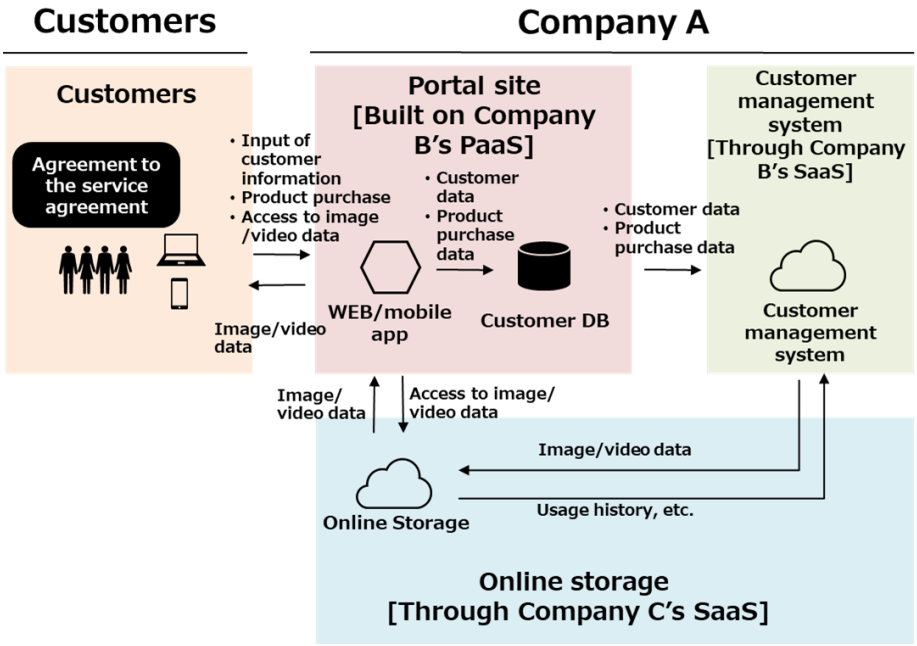


Figure A-3.1: Overview of the target processes

In the Use Case, Company A uses several cloud services of different nature, such as PaaS and SaaS. Stakeholders such as the following should be considered by Company A when trying to ensure trustworthiness and appropriate security level within the

aforementioned scope.

- Customer: Accesses Company A's portal site, processes and downloads images and video data previously taken, and purchases related products.
- Company A: A business that provides services, sells goods, etc. that has been building and operating a portal site, customer management system, etc. to increase customer value by using various cloud services provided by Companies B and C as a cloud service customer[30].
- Cloud service providers[31]: Providers of various cloud services to Company A
  - Company B: Provides a web app development/operation platform as PaaS for building the portal site and a customer management system service as SaaS to Company A.
  - Company C: Provides Company A with an online storage service as SaaS that stores image and video data, and also separately provides a peer cloud service[32] as IaaS that serves as the platform for services provided by Company B.
- Cloud service partner: Builds a portal site on Company B's PaaS and develops the linkages between each service.

As aforementioned, the Use Case deals with a cloud supply chain in which Company B, which directly contracts with Company A (cloud service customer), provides PaaS and SaaS by using the IaaS of Company C, which is a third party under the said contract. Figure A-3.2 gives an overview of the supply chain associated with the provision of cloud services in the Use Case while referencing the service model classifications[33] of cloud services. Since issues such as the following could generally occur[34] in such cloud supply

---

[30] A "cloud service customer" refers to a "business affiliate that uses a cloud service." (ISO/IEC 17789:2014) They are also referred to as cloud users.
[31] A cloud service provider refers to a "party that provides a cloud service." (ISO/IEC 17789:2014)
[32] A peer cloud service refers to a "cloud service of a single cloud service provider that is used as part of a cloud service provided by one or more other cloud service provider(s)." (ISO/IEC 17789:2014)
[33] Refer to prominent literatures that define service model classifications such as the following: *The NIST Definition of Cloud Computing* by the National Institute of Standards and Technology (NIST); Basic policy on the use of cloud computing services in government information systems decided during a liaison meeting of the chief information officers (CIO) of each ministry (in Japanese)
https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf
[34] *Guidelines for the Use of Cloud Computing Services* (2013 Version, in Japanese)
https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf by METI

chains, both cloud service providers and cloud service customers should ideally take measures[35] such as conducting audits based on timely information disclosers, appropriate agreements, etc.

- Even if there is no problem with the direct contractor (in this case, Company B) from the perspective of a cloud customer such as Company A, when there is a problem with the underlying PaaS or IaaS, it will cause a chain reaction of problems.
- When business activities become damaged somehow due to such failures, division of responsibilities between providers tends to become more ambiguous.
- Despite the fact that data should not be positioned in a way that subjugates them to foreign countries and foreign laws due to regulatory issues and security policies for cloud service customers, the existence of providers under the control of supply chains could create conditions that violate the intentions of customers.

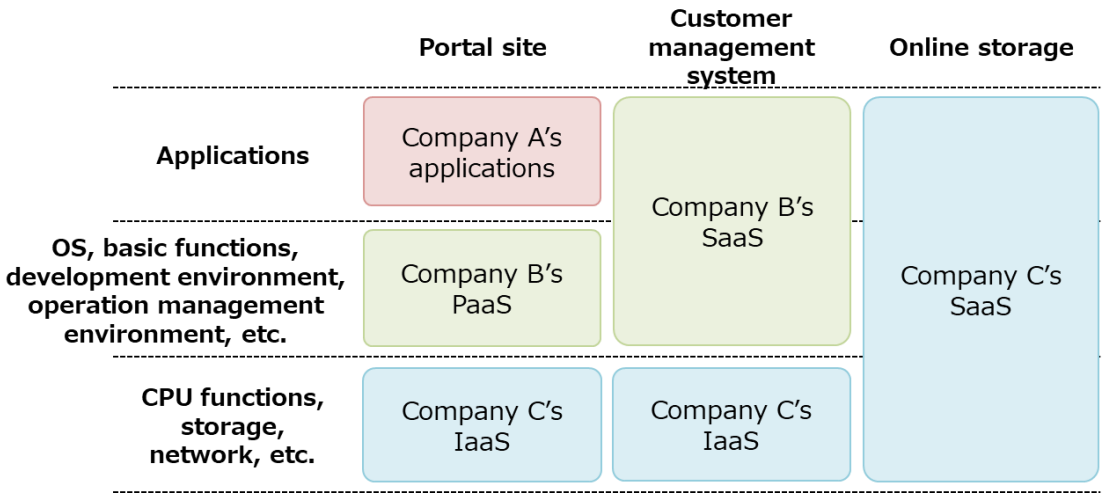


Figure A-3.2 Overview of supply chains associated with cloud service provision

A-3-1. STEP 1Visualize the data processing workflow (“events”)

The data processing flow in the Use Case consists of the following processes, as shown in Figure A-3.3. The current and subsequent sections will visualize the data

[35] Examples of specific measures include: verification of compliance with certification standards by cloud security certification systems (i.e., IMS cloud security certification, Information System Security Management and Assessment Program (ISMAP)) through utilization and verification of whitepapers; verification using existing audit reports (i.e., SOC2 report), individual investigations, etc.

processing flow and organize the necessary institutional safeguards (domains), especially for the processes in (2).

(1) Based on appropriate agreements, etc., customer image/video data are generated and acquired through Company A's photographic equipment, transferred, and provided by Company A's employees to an online storage provided by Company C and stored there. According to customer request, the image/video data are processed/used (i.e., photoshopping on the online storage) and then transferred/provided to customer terminals (i.e., PCs, smartphones).

(2) On the portal site, data such as customer data and product purchase data are generated/acquired through customer actions such as input of one's own data, purchases, etc., and then stored in the customer DB. Such data are transferred/provided in a timely manner to the customer management system provided by Company B and processed/used by Company A's employees according to the individual internal needs of Company A. When visualizing the process flow, we must pay attention to the fact that the portal site is built on Company B's PaaS that has its OS, development environment, operating environment, etc. on the physical/virtual infrastructure (i.e., CPU functions, storage, network) provided as IaaS by Company C.

As mentioned earlier, the usage of a cloud service that organizes a supply chain consisting of services from multiple providers, as in the Use Case, poses specific possible risks due to its complexity, etc. Therefore, when organizing the data processing flow and necessary institutional safeguards (domains) and attempting to identify possible risks as comprehensively as possible, it is ideal to make considerations that take the provision systems of multi-layered services into considered from the viewpoint of ensuring cloud supply chain transparency and clarifying the division of responsibilities as needed. There are various possible viewpoints from which to demonstrate the multi-layered-ness of a service. Based on similar classifications as Figure A-3.2 as an example, Figure A-3.3 presents domains including the division of responsibilities of each company from three different viewpoints ((1) applications; (2) OS, basic functions, development/operating environment, etc.; (3) CPU function, storage, network, etc.) and describes the form in

which these are uniformly facilitating the data processing (event).

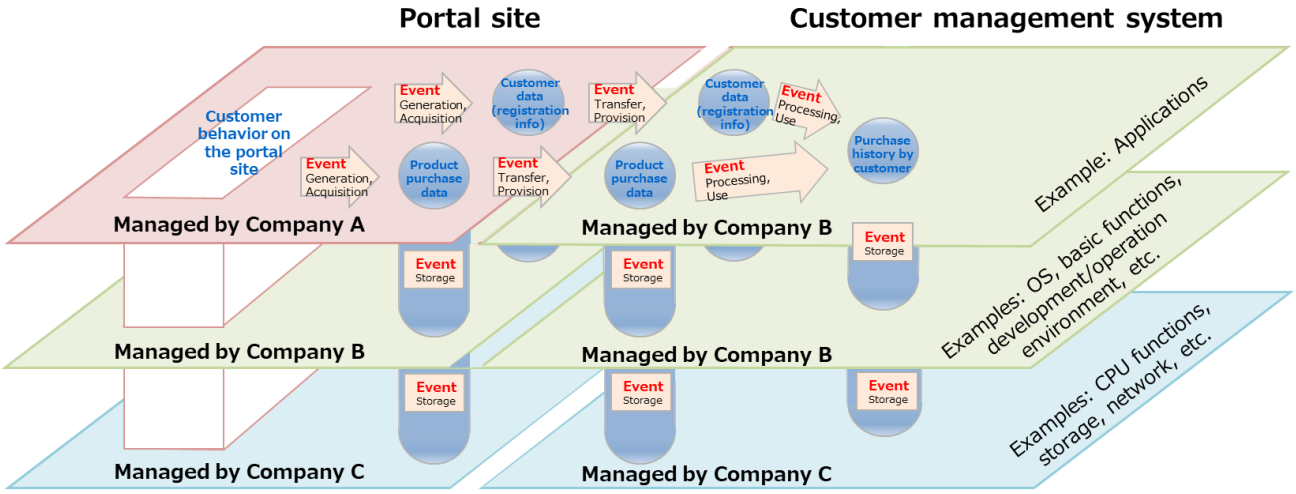


Figure A-3.3: Visualization of data processing flow
(Services that use IaaS, PaaS, SaaS, etc.)

A-3-2. STEP 2 Organize the necessary institutional safeguards (domains)

As an example, the following rules, as well as rules that are not necessarily explicitly stated by each company, could presumably be identified as the domains for the Use Case when considering how data such as customer data fall under the category of personal data, and the system that processes and manages the said data is comprised of several cloud services.

(1) Company A's service agreement, etc.: Company A needs to establish terms and conditions with its customers in relation to the use of the portal site, etc., and obtain their consent. Terms, personal information protection policies that are separately determined, etc. should not only contain prohibitions and disclaimers regarding the content and use of the service, but also regulations for protecting customer data (registration information) such as name, address, contact information, and image and video data. Such regulations should be complied with across all processes that handle relevant personal data in the Use Case.

(2) Act on the Protection of Personal Information: Since customer data that are acquired from and each customer's purchase history that is incidentally acquired from customers by Company A could be considered personal data, Company A must adhere to the disciplines that are imposed on personal information-handing

businesses. Data must be appropriately conducted based on the results of, but not limited to, the following decision tree: Would Company A's usage of cloud services provided by Companies B and C fall under the category of "provision of personal data to third parties" (i.e., will personal information be handled by Companies B and C)? If so, would this be considered as "entrusting" to Company B or Company C? Would individual consent be required[36]? Would this provision be considered as "provision to third parties in foreign countries"? In the Use Case, the following services are presumed to be taking appropriate access controls and declaring the intent in their contract clause of not handling personal data stored in their servers: (1) Services of Company B and Company C used for the development and operation of the portal site; (2) Company C services used for the development and operation of the customer management system.

(3) Terms of use of various cloud services: Company A's various systems in the Use Case are developed and operated using the cloud services provided by Companies B and C. As previously mentioned, it is ideal to identify the terms of use, etc. of relevant cloud services as the domains when making considerations such as of cloud supply chains and their associated risks. Examples of terms, etc. that should be identified here include the following.

- Terms of service use between Companies A and B and Companies B and C that are necessary for Company A to operate its portal site (referred to as terms of use of Company B's PaaS and terms of use of Company C's IaaS, respectively)
- Company B's terms (terms of use of Company B's SaaS) that are necessary for Company A to use the customer management system and terms of Company C (terms of use of Company C's IaaS) in providing physical/virtual

[36] Whether the usage of a cloud service falls under the category of "provisions to third parties that require individual consent" or "consignment" depends on how the personal data are handled by the data-receiving business. For example, a cloud service provider would not be considered as a personal data handler if the contract clause specifies the intent of not having such external providers handle personal data stored on a server, and if access controls are appropriately being taken, for example. If such cloud service provider is not to handle personal data, then individual consent would not be required since it would not be considered as provision of personal data by the personal information-handling provider. [Q&A Q7-53 of *Guidelines for Protection of Personal Information* and What to do in the event of a personal data leak, etc. by the Personal Information Protection Commission (in Japanese) https://www.ppc.go.jp/personalinfo/legal/#APPI]

infrastructures (CPU function, storage, network, etc.) to Company B

- Agreements related to the operation of data linkage functions (provided by Company B) between Company A's portal site and the customer management system

It is also ideal to clarify the security roles and responsibilities of each organization provisioned in the aforementioned terms, etc. For example, in terms of Company A's usage of the customer management system (SaaS) provided by Company B, Company B or C would handle the various security measures including those against the vulnerabilities of various hardware, OS, middleware, and applications, for example. But generally, Company A would be responsible for taking measures such as establishing security measures and configuring the scope of file disclosure for terminals that use the SaaS, as well as managing, authenticating, approving, etc. the accounts of employees, etc. The inability to accurately grasp one's organizational roles, responsibilities, their fulfillment status, etc. could lead to unintentional security incidents. Therefore, it is ideal for each affiliate to carefully consider this and take countermeasures.

(4) Laws and regulations on data center locations (related to data handling overseas, etc.): In the case of an online cloud service, it is not rare to see its data center being located overseas due to service operation cost. To allow the said service provider and its users to clarify the domains, it is important to determine which country's laws and court decisions need to be consulted in the event of security incidents, etc. In terms of private laws[37], service provision agreements, etc. between cloud service customers and cloud service providers generally contain clauses that designate the governing laws and consensual jurisdictions. In terms of public laws on the other hand, unexpected risks could materialize such as the data of cloud service customers becoming searched and seized by law enforcement in the country where the data center is located, since the principle of territoriality is applied to public laws in principle. In that case, various stakeholders (i.e., Company A, individual users of Company A's service) in the Use Case could

[37] Here, public laws refer to those that govern the legal relationships between the national government and private individuals. Private laws refer to laws that govern legal relationships between private individuals.

become affected. When using cloud services, etc. of Companies A and B in relation to the aforementioned, it is ideal to examine the services including their data center location while also considering whether or not there are any specific contentious risks foreseen in relation to laws and regulations pertaining to data handling in foreign countries.

Figure A-3.4 organizes the domains of (1) through (4) as specified above from the perspective of each relevant provider while keeping in mind the division of responsibility of each provider as outlined in Figure A-3.2. Note that the indication or absence of events in the figure indicates whether or not the relevant providers are responsible for implementing the corresponding events.

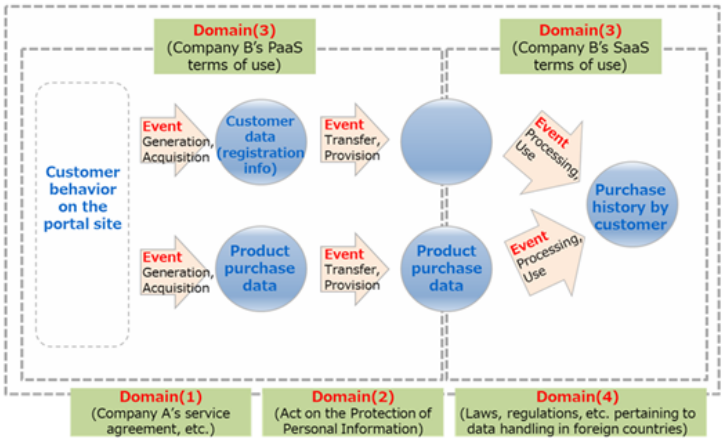
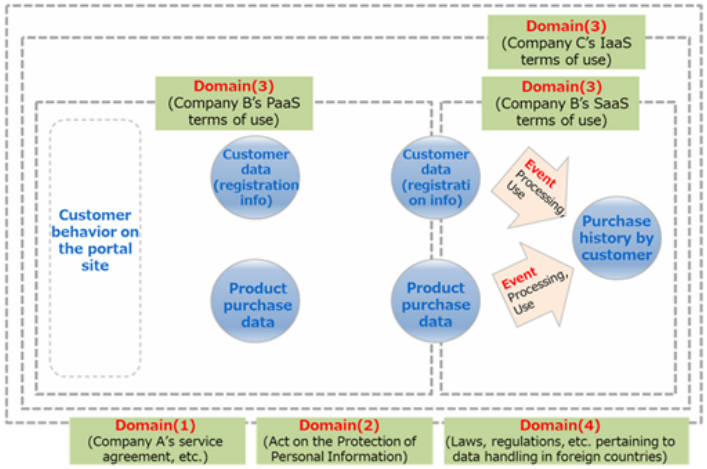
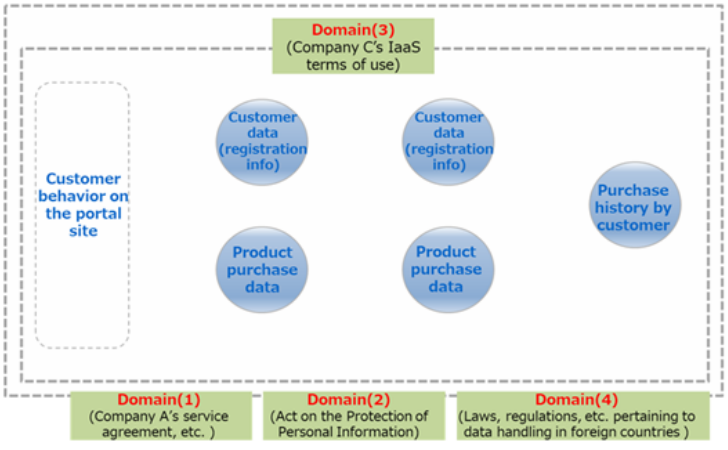
Organized based on the perspective of each provider	Examples of organization of necessary institutional safeguards (A service that uses IaaS, PaaS, SaaS, etc.)
Organized from the perspective of Company A	
Organized from the perspective of Company B	
Organized from the perspective of Company C	

Figure A-3.4: Examples of organizing the necessary institutional safeguards (services that use IaaS, PaaS, SaaS, etc.)[38]

[38] In the figure, the dashed line indicates the scope at which the same standards are applied to the portal site

A-3-3. STEP 3 Specify the “properties”

Since image/video data reveal individuals including the customers themselves in the Use Case, the personal information protection legislation is a rule that should definitely be referenced when considering the properties as in A-2. In addition, when identifying matters related to usage restrictions such as scope of data disclosure, data controller, expiration dates, etc., it is useful to reference laws and regulations related to data center location when considering the terms of use of various cloud services, the appropriateness of storage medium/destinations, etc.

Table A-3.1: Rules (domains) that should be considered when considering the attributes

		Company A’s service agreement, etc.	Act on the Protection of Personal Information	Terms of use of various cloud services	Laws and regulations related to data center location
Category	**Personal data protection**	○	○		
	Intellectual property (including trade secrets) protection			○	
	…	…	…	…	…
Scope of disclosure		○	○	○	
Purpose of use		○	○	○	
Data controller		○	○	○	
Data rights holder		○	○		
Value (Importance)		○	○		
Media, storage destination				○	○
Expiration Date		○		○	

Since customer data, product purchase data, and image/video data all fall under the category of personal data as aforementioned, data rights holders are the customers themselves, and Company A must appropriately respond to disclosure requests[39] from customers as part of their obligation as a personal information-handling business. In

and the customer management system. The solid line indicates the scope at which separate standards are applied to each.

[39] Refer to Article 32 of the Act on the Protection of Personal Information (Last revision: Act No. 44 of June 12, 2020)

Company C's service that is used for developing and operating the customer management system, Companies A and B, which are responsible for substantially accessing data and managing them up to a certain level, are delegated as the data controller, since their contractual clause will stipulate that personal data saved on the server will not be handled, and since access controls will be conducted appropriately. Note that when a specific service is provided through a division of labor among several cloud service providers as in the Use Case, cloud service customers such as Company A could end up having to use the service without necessarily becoming aware of who the providers are such as Company C. Especially in cases where data location is restricted due to relevant legal systems and internal organizational policies, it is necessary to request the cloud service provider (Company B in the Use Case) to disclose information before concluding the agreement, and collect information regarding the location, etc. of data stored in media/destinations that are equivalent to the following.

Table A-3.2: Examples of property parameters of some of the data presented in the Use Case

		Customer data[40]	Product purchase data	Image/video data
Category	**Personal data protection**	Personal data	Personal data	Personal data
	Intellectual property (including trade secrets) protection	Company A's trade secrets	Company A's trade secrets	-
	…	**…**	**…**	**…**
Scope of disclosure		Company A, customers	Company A, customers	Company A, customers
Purpose of use		・ Provision of various services to customers ・ Handling customer inquiries ・ Sending advertisements and mail magazines to customers		・ Provision of various services to customers
Data controller		Companies A, B	Companies A, B	Company A
Data rights holder		Customers	Customers	Customers
Value (Importance)		High	High	High
Media, storage destination		Company B's SaaS (Company C's IaaS)	Company B's SaaS (Company C's IaaS)	Company C's SaaS

[40] In A-3-3, data stored in Company A's customer management system are exclusively handled as customer data and product purchase data. Customer data include identifiers, authentication information, address, name, email address, etc.

Expiration Date	Two years from the end of the membership agreement	Two years from the end of the membership agreement	Two years after the data is taken

A-3-4. STEP 4 Identify the risks of each “event”

A-3-4-1. Identify the risks of each “event”

Based on the considerations made up to STEP 3, the following types of risks can be expected in the Use Case regarding the process of processing, using, and storing customer data handled by Company A in the customer management system provided by Company B as illustrated in Figure A.3-4. Just as in A-1 and A-2, the following considerations are made in the same way as for other data and events in the entire process.

Table A.3-3: Examples of possible risks of processing, using, and storing customer data in the customer management system

Major classification	Middle classification	Examples of possible risks of processing, using, and storing customer data handled by Company A on the customer management system provided by Company B
From the viewpoint of security protection	Confidentiality	● A malicious external entity impersonates an employee of Company A through a password list attack, etc., and externally leaks customer data stored in the customer management system. ● A malicious external entity takes advantage of the vulnerabilities of the customer management system (Company B’s SaaS) to fraudulently access the customer management system and externally leaks customer data. ● Customer data become disclosed to unexpected entities due to insufficient security settings for the rights, etc. of Company A’s employees in accessing Company B’s SaaS. ● Customer data that need to be sufficiently safeguarded become disclosed when shared servers, etc. become seized due to requests from domestic or foreign judicial organ, etc.
	Integrity	● The application becomes tampered with by a malicious internal or external entity, resulting in unauthorized processing of customer data. ● A malicious internal/external entity tampers with stored customer data.

	Availability	● A malicious third party launches a DoS attack on Company B's SaaS, which suspends processes for numerous customers including Company A's system. ● Company B's SaaS or Company C's IaaS receives excessive traffic resulting in massive peak load, regardless of whether it was maliciously intended, which suspends processes for numerous customers including Company A's system.
From the viewpoint of relevant legal systems	Personal data protection	● Customer data become used by legitimate users of Company A or B in a way that deviates from the purpose of use notified to the customers. ● Company A's representatives, etc. fail to sufficiently and appropriately conduct necessary supervision on Company B.
	Intellectual property (including trade secrets) protection	● A malicious internal/external entity (which could include Company B's employee) acquires customer data through legitimate means and uses them to gain unfair advantage or inflict damage to Company A.
	. . .	

Furthermore, when concluding an agreement to ensure that personal data will not be handled by the cloud service providers involved in providing services to the cloud service customers like in the Use Case, safeguards must be implemented on the personal data handled by the company. In cases where some of the personal data are handled overseas,[41] safeguards must be implemented upon understanding the systems, etc. pertaining to personal information protection in the relevant countries. To that end, systems, etc. related to personal information protection in the relevant countries must be understood by establishing criteria such as "data-handling country" other than the properties illustrated in Table A-3.2. To gather information necessary to make such considerations, it is necessary, for example, to form agreements with the cloud service providers, etc. and have them disclose information so that their data center locations, etc. can be recognized. Note that when handling retained personal data in a foreign

[41] Cases such as those in which personal data are handled by overseas branches or sales offices, as well as a cloud service provided by a foreign cloud service provider is used and personal data are stored on the server managed by the said provider (as well as when personal data are stored on a domestically located server of the said provider) fall under the category of personal data being handled in a foreign country.
https://www.ppc.go.jp/files/pdf/2109_APPI_QA_4ejj3t.pdf

country, safety control measures must be taken on the retained personal data, including clarifying the names of the cloud service providers and the foreign countries where the servers that store these data are located, as well as announcing the details of measures taken based on the systems, etc. of the relevant foreign countries.

A-3-4-2. Considering the challenges for the further sophistication of data management

As elucidated from the process of applying the framework in STEPS 1 through 4, the cloud service customers in the Use Case use several cloud services based on the required function including a service provided through the configuration of supply chain by several providers, which poses various potential risks that are different from building and operating an on-premise system. The following countermeasures to such risks for example can be implemented by Company A and relevant providers.

- Ensure transparency regarding the physical location of data
  If the location of the data center where customer data, product purchase data, etc. are currently stored is not clear at the framework application stage, regardless of whether the portal site is already being operated or not, Company A must request disclosure of said information from the representatives of the direct service providers (Company B (portal site, customer management system) and Company C (online storage)), ensure consistency of the information with regulations such as one's own service agreement, further investigate and verify compliance with the legislative system, etc. of the data center location, and then make this information transparent to the customers.

- Clarify one's own division of responsibility and review the operation status
  Unlike managing an on-premise system, the provision or usage of a cloud service requires an appropriate overall management by ensuring division of responsibility in security and compliance management between the cloud service customers and cloud service providers, and ensuring that both parties fulfill their own responsibilities, disclose necessary information in a timely manner, etc. Such

management style is sometimes called the shared-responsibility model[42]. In the Use Case, Company A uses several services with different scope of responsibilities such as SaaS and PaaS. As aforementioned, the security of data such as customer data could become compromised if there is inadequacy in the security configuration (i.e., application operation management, access rights), which is the responsibility of Company A to manage as a cloud service customer. To reduce the risks induced by insufficient management on the customer side, it is ideal for Company A to further materialize the division of responsibilities between providers that were clarified in STEP 2 by having each company re-identify necessary management measures (i.e., secure terminals that access the cloud service, manage access rights) that must be implemented for using the cloud service and review their fulfillment status using operation support tools, etc.

[42] The difference between the responsibilities of cloud service providers and cloud service customers can be expressed by the terms “security ‘of’ the cloud” and “security ‘in’ the cloud,” respectively. (https://aws.amazon.com/jp/blogs/news/rethinksharedresponsibility/)

A-4. Examples of overseas development, operation, etc. of IT services provided domestically

While the importance of business transformation through the advanced use of digital technology, such as the realization of digital transformation (DX), has been recognized by society, there are widespread cases of having difficulty implementing this internally by ensuring human resources to develop, maintain, operate, etc. IT systems that require advanced specialization. In such instances, it is said that businesses could better allocate resources to other projects by appropriately and externally outsourcing this development and enjoying high quality third party services while aspiring to ensure one's own resources for such development in the long-run. Furthermore, IT-related developments have often been conventionally outsourced to providers with an overseas base to globalize business, reduce cost, etc.

On the other hand, when data such as technical information that is useful for the business and personal data are to be handled overseas instead of domestically, great care must be generally taken to protect personal information, manage exports pertaining to technical information, etc. Nowadays, as data must sometimes have to be handled across the boundaries of organizations, countries, and regions, this issue is considered more important than ever before.

Based on the aforementioned background, the following process flow (hereinafter within A-4, the "Use Case") serves as an example for considering the appropriate management method of such data when business data are expected to be handled overseas.

- Company A domestically operates nationwide and is comprised of several group companies that have traditionally built and operated their own systems and shared data to the headquarters as appropriate. To conduct various HR tasks on the cloud including managing group talents, payroll, etc., Company A has been building a company-wide integrated system using the cloud service provided by Company C.
- Company A outsources to Company B its responsibility to manage part of the operation regarding the aforementioned system. Specifically, Company B is outsourced to provide a help desk (respond to inquiries), constantly monitor the

system, handle failures, develop add-on functions as needed, etc.

- Company B's operation center is located in a foreign country, where staff with high expertise in IT system operation are available 24 hours a day, 365 days a year. Reports such as on the operation status and failure response status are sent to Company A's system department located in its headquarters by the staff members of Company B's Japan base after receiving reports from its operation center.

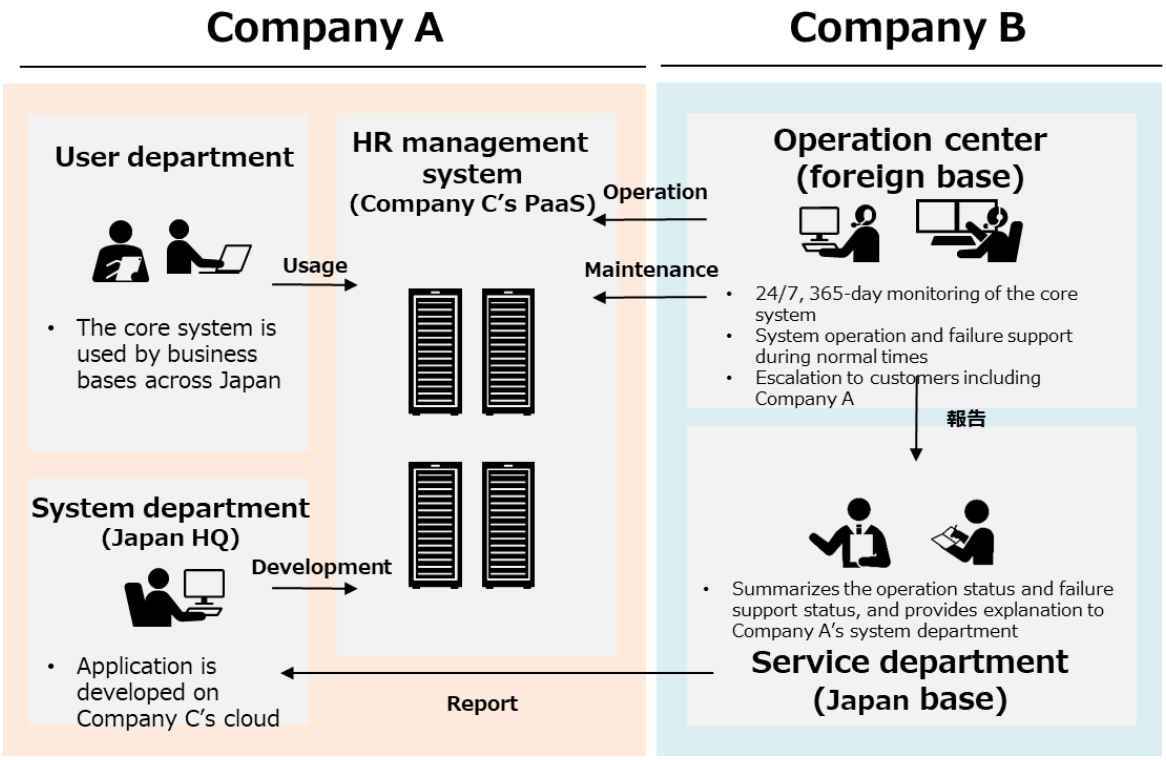


Figure A-4.1: Overview of the target processes

In the Use Case, Company A should consider the following stakeholders for example when managing the overall security, etc.

- Company A: A business with business bases in various parts of Japan that builds and operates a company-wide HR management system on Company C's cloud service.
- Company B: A business that has been consigned by Company A and has supported the construction of HR management systems in the past, and utilizes the knowledge gained from such experience to operate and maintain Company A's HR management system by using a foreign operation center.
- Company C: Provides a cloud service to Company A.

A-4-1. STEP 1 Visualize the data processing workflow (“events”)

The data processing flow in the Use Case consists of the following processes, as shown in Figure A-3.2.

(1) Various HR management data (includes, but not limited to, employee attribute data, attendance status, and personnel evaluation data shown in Figure A-4.2) are generated/acquired through inputs made by the departments that use the HR management system such as employees including the HR managers. For example, these data could be processed and used not only for conventional purposes such as calculating payroll, but also for cultivating talents, reducing job turnover, etc.[43] Through the aforementioned series of systems, system operation data are continuously generated and acquired.

(2) System status data and data required for operation, management, etc. (i.e., system operation design data) are transferred and provided to Company B (operation maintenance contractor) and used to provide services. Note that various HR management data are not provided to Company B at least in the implementation of normal operation tasks such as the following.

- Performance management of various applications
- Distribution and application of bug-fixing patches for the HR management system
- Inquiry responses and investigations and handling of failures by Company A’s system department

[43] There are various ways of processing and using such data, but they are not considered in Figure A-4.1 due to deviation from the main objective.

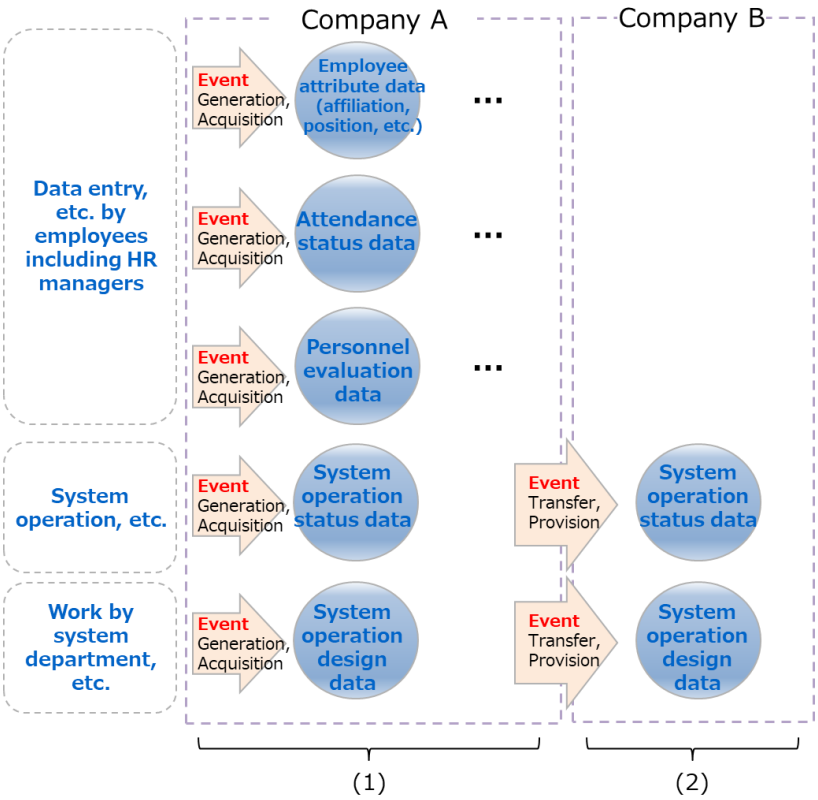


Figure A-4.2: Visualize the data processing flow

(Examples of overseas development, operation, etc. of IT services provided in Japan)

A-4-2. STEP 2 Organize the necessary institutional safeguards (domains)

As an example, the following rules as well as rules that are not necessarily explicitly stated by each company could presumably be identified as the domains for the Use Case when considering how data such as customer data fall under the category of personal data, and the system that processes and manages the said data is comprised of several cloud services.

(1) Act on the Protection of Personal Information: Company A must comply with the obligations imposed on personal information-handling businesses due to holding highly sensitive HR data. Furthermore, when considering the scope of application outside of Company A, it must be clarified whether contractors (Companies B, C) receive personal data from Company A based on the details of their agreement. During this process, if the contractors are to handle the personal data stored in the system, then it will be deemed that personal data will

be provided to the contractors, which will require ensuring legitimacy such as by acquiring individual consent, concluding entrustment contracts, etc., as mentioned in A-3. Note that in the aforementioned case, we must also keep in mind that Company A must[44] supervise the contractors to ensure that they implement equivalent measures as the safety management measures that Company A must implement based on Article 20 of the Act on the Protection of Personal Information. On the other hand, if the contractors provision the fact that they do not handle personal data in their contract clauses, then they (Companies B, C) will not be deemed as being provided with personal data as long as they appropriately ensure access controls, etc.[45] In that case, Company A must take appropriate safety measures that it is responsible to implement while verifying that personal data are not being handled by contractors such as Company B or C[46,47].

(2) Export control laws and regulations[48]: In general, when providing non-residents of Japan (foreigners and Japanese people who are settled outside of Japan) with cargo exports of one's company, technical information (i.e. design documents, source codes, and operational tools), etc., it is necessary to determine whether such provision falls under the scope of export controls under the Foreign Exchange and Foreign Trade Act and, if necessary, to implement procedures such as obtaining a license from the competent ministry. The following can become subject to export controls under the Use Case: Data necessary for the

---

[44] " Section 3-3-4: Supervision of contractors (related to Article 22 of the Act) of the *Guidelines for Protection of Personal Information* (General Provisions, in Japanese)

[45] Q&A Q7-53 of *Guidelines for Protection of Personal Information* and What to do in the event of a personal data leak, etc. by the Personal Information Protection Commission (in Japanese)

[46] Q7-54, same as above

[47] If Companies B nor C will handle personal data according to the agreements, Company A will be regarded as a personal information-handling business that handles personal data in a foreign country. Hence, Company A must understand the personal information protection systems, etc. of the corresponding foreign countries, clarify the names of the countries where the cloud service provider (Company B in this case) and the personal data-storing server(s) are located as part of its personal data safety management measure, and make the details of the measures that were implemented based on the systems, etc. of the corresponding foreign countries transparent to the data subjects. If that is difficult, Company A must make the following transparent to the data subjects in place of the name of the foreign countries where the servers are located: (1) The details and reasons as to why the countries where the servers are located cannot be identified, and (2) any other referential information for the data subjects. (See Q10-25 of the same)

[48] For details about export control laws and regulations in Japan, refer to materials such as the *Security Export Control Handbook 10th Edition* by the Security Export Inspection Office, Trade Control Policy Division, Trade and Economic Cooperation Bureau, Ministry of Economy, Trade, and Industry.

implementation of services such as system operation design data, and if applicable, the provisions of operation tools, on-site guidance, etc. Companies A and B must complete beforehand the internal procedures necessary for the export controls and examine and verify the export feasibility before transactions and during shipments.

(3) Operation and maintenance entrustment agreement: This agreement determines matters such as the specifications of the entrustment agreement between Companies A and B. For example, it must clearly provision that Company B will not handle personal information of Company A's employees during the course of business, as well as provision the handling procedure of Company A's technical information (i.e., confidentiality agreement), etc.

(4) Company A's personal information protection rules

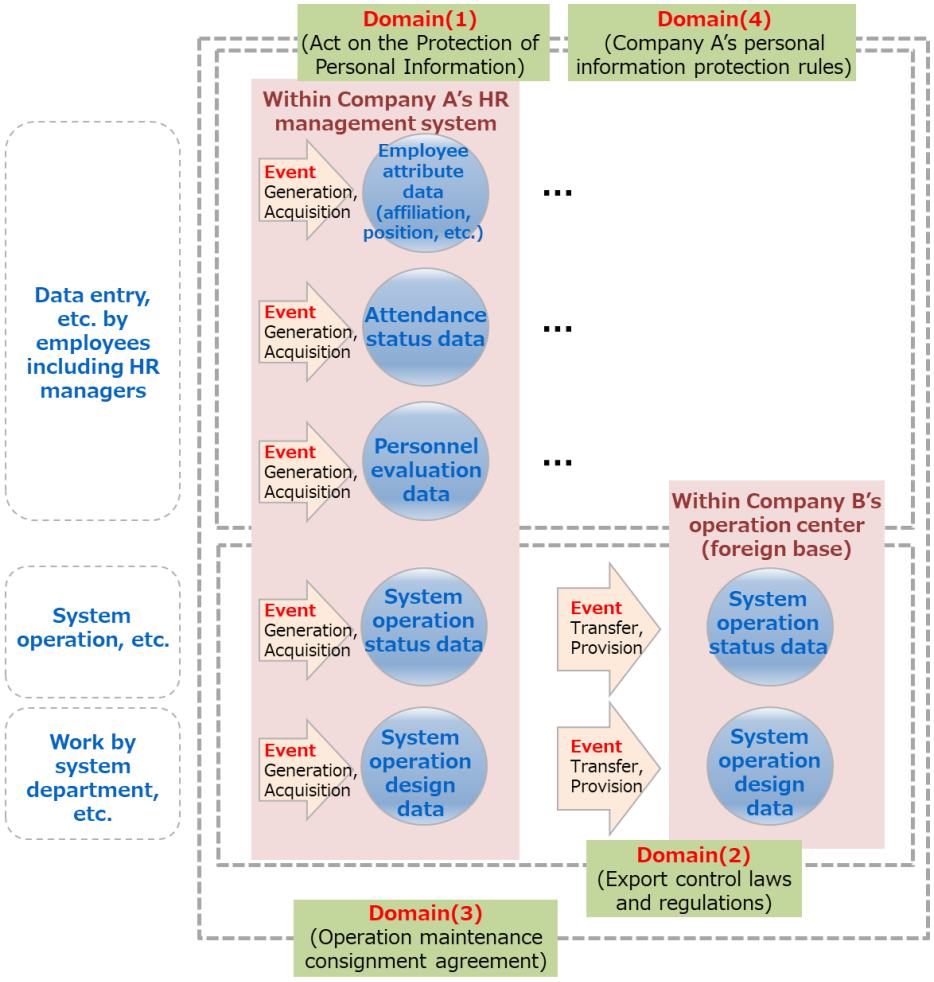


Figure A-4.3: Examples of how to organize the necessary institutional safeguards (Examples of overseas development, operation, etc. of IT services provided in Japan)

A-4-3. STEP 3Specify the “properties”

Since Company A will handle data of its employees for HR management in the Use Case, it could be presumed that Company A must reference personal information protection laws when considering properties while considering categories, scope of disclosure, etc. In addition, its internal personal information protection rules will perhaps be useful in determining the purpose of use of employee data, the data controller, the storage destinations/mediums, expiration dates, etc. Furthermore, provisions related to the scope of disclosure (including scope of handling), storage destinations/mediums, expiration dates, etc. of each data could be presumably determinable based on the operation maintenance entrustment agreement between Companies A and B.

Table A-4.1: Rules (domains) that should be considered when considering the properties

		Act on the Protection of Personal Information	Export control laws and regulations	Operation maintenance consignment agreement	Company A’s personal information protection rules
Category	**Personal data protection**	○			○
	Intellectual property (including trade secrets) protection			○	○
	…	**…**	**…**	**…**	**…**
Scope of disclosure		○	○	○	○
Purpose of use		○			○
Data controller		○			○
Data rights holder		○			○
Value (Importance)		○			○
Media, storage destination			○	○	
Expiration Date		○		○	○

Table A-4.2 illustrates the parameters of various properties regarding the three data (employee attribute data, system operation status data, system operation design data) among the data that are identified in Figures A-4.2 and A-4.3. As mentioned earlier, employee attribute data are considered personal data, which require Company A to fulfill

the obligations as a personal information-handling business (i.e., identify purpose of use, ensure safety management). Personal information protection rules that target Company A's employees can be used to specify properties such as scope of disclosure, purpose of use, data rights holders (and rights that can be exercised by employees who are the rights holders), expiration dates, etc. Note that since the HR management system is built on the PaaS provided by Company C, the said PaaS can be specified as the storage destination/medium. Since the agreements of Companies A and C provision that Company C would not handle personal data, the scope of disclosure is strictly within Company A, which requires access controls, etc. to be appropriately implemented to ensure that such management is conducted.

Unlike employee attribute data, system operation status data and system operation design data must be managed as data that do not contain personal data because Companies B and C are not supposed to handle personal data. Like Company C, Company B's access must also be appropriately controlled of various personal data managed by Company A including employee data, and such access control must be continuously maintained and managed[49]. The system operation status data, system operation design data, etc. that are transferred and provided to Company B based on the operation maintenance entrustment agreement are to be used only during the consignment agreement period for the sole purpose of operating the applicable systems, conducting maintenance work, handling failures, etc., and are to be disposed through appropriate means after the end of the said period.

Table A-4.2: Examples of property parameters of some of the data presented in the Use Case

		Employee attribute data	System operation status data	System operation design data
Category	**Personal data protection**	Personal data	Non-personal information	Non-personal information
	Intellectual property (including trade	Company A's trade secrets	Company A's trade secrets	Company A's trade secrets

[49] See Q&A Q5-35, etc. of *Guidelines for Protection of Personal Information* and What to do in the event of a personal data leak, etc. issued by the Personal Information Protection Commission

	secrets) protection			
	…	**…**	**…**	**…**
Scope of disclosure		Internally within Company A	Company A's system department, Company B's operation manager	Company A's system department, Company B's operation manager
Purpose of use		· HR tasks, and calculation, determination, payment of payroll · Manage employment (i.e., hiring, retirement, attendance) · Manage health of employees · Communication, etc. from company personnel to employees	· Operate and maintain applicable systems · Handle failures · Consider measures, etc. to prevent failure recurrence, further optimize operation, etc.	· Operate and maintain applicable systems · Handle failures
Data controller		Company A	Companies A, B	Companies A, B
Data rights holder		Company A, employees	Company A	Company A
Value (Importance)		Extremely high	High	Extremely high
Media, storage destination		Company C's PaaS	Company B's terminals, Company C's PaaS	Company B's terminals
Expiration Date		During the employment contract period	During the consignment agreement period	During the consignment agreement period

A-4-4. STEP 4 Identify the risks of each "event"

A-4-4-1. Identify the risks of each "event"

Based on the considerations made up until STEP 3, the following kinds of risks can be presumed in terms of the Use Case regarding the transfers and provisions of the system operation design data illustrated in Figures A. 4-2 and A. 4-3 and the subsequent storage process. Potential risks in the process of data transfer and provision may vary depending on the technical means used. Here, we have extracted the risks associated with conducting such transfers and provisions through an external cloud storage service (SaaS). In light of the fact that the transfers and provisions of such data can be considered as an exportation of technical information overseas, the following table also considers sensitive technology management as one of the variables that determine the relevant legal systems, etc.

The risks of applicable transfer/provision events are organized based on four categories (country/region, organization/person, system/service, and device). As examples, the following risks can be identified.

<Country/region>

- Not applicable from the perspective of personal data protection if it is presumed that personal information is not included in system operation design data.
- Before actually transferring or providing the system operation design data, no confirmation is made in the export controls implemented internally by Company A for verifying the concerns related to export controls associated with providing technical information.

<Organization/person>

- A malicious employee of Company B's overseas base fraudulently takes the system operation design data outside the company, such as by inserting a USB memory stick.

<System/service>

- Insufficient security configuration of access controls, etc. of Company A's employees in using the cloud storage service leads to the disclosure of the system operation design data to unexpected entities.
- A malicious third party intercepts the communication between Company A's business terminals and the server provided by the external cloud storage service and falsifies the data.

<Device>

- A server provided by the external cloud storage service becomes infected by malware, which delays the transfers and provisions of the system operation design data.

Table A. 4-3: Examples of potential risks of transferring, providing, and storing system operation design data

Major classification	Middle classification	Examples of potential risks of transferring, providing, and storing system operation design data
From the viewpoint of security	Confidentiality	● A malicious external entity exploits a vulnerability in an external cloud storage service used by Company A to gain unauthorized access to the stored system operation design data.

		● Due to an insufficient security configuration such as access rights in the cloud storage service by Company A's employees, the system operation design data become disclosed to an unforeseeable entity. ● A malicious external entity fraudulently accesses operation/maintenance terminals held by Company B and the system operation design data. ● A malicious employee of Company B living overseas illegally carries system operation design data outside the company through the insertion of a USB memory stick or other means.
	Integrity	● A malicious third party intervenes in the communication between Company A's business terminals and the server providing the external cloud storage service and falsifies the data.
	Availability	● A server hosting the external cloud storage service becomes infected with malware, which delays the transfers and provisions of the system operation design data.
From the viewpoint of relevant legal systems	Personal data protection	● Not applicable if we presume that personal information is not included in the system operation design data.
	Intellectual property (including trade secrets) protection	● A malicious internal/external entity (i.e., external attacker, Company B's employee) acquires, discloses, and uses through fraudulent means the system operation design data.
	Sensitive technology management	● Prior to the actual transfers and provisions of the system operation design data, no confirmation is made on whether the export control concerns regarding the provision of technical information will be made valid pertaining to the export control procedures implemented internally by Company A.

A-4-4-2. Considering the challenges for the further sophistication of data management

As elucidated in the aforementioned framework application process, the Use Case illustrates a business (Company A) that has commissioned a contractor (Company B) with an overseas maintenance base to operate the general HR management system that Company A has developed through the support of external providers to reduce cost, enhance quality, etc. The unique challenges in this case include not only protecting the HR management system itself that handles many personal data, but also ensuring the governance of transferring and providing employee data and system operation data that

are handled there. The following countermeasures to such challenges for example can be implemented by Company A and relevant providers.

- Reviewing the status of Company B's access to Company A's data
  As aforementioned, Company B is not supposed to handle the personal data managed by Company A. But continuous compliance to the clauses of the underlying agreements, etc. must still be ensured. For example, the outsourced work should not contain any work that must handle personal data such as the reproduction and validation of information system failures using personal data. If such clause is not specified, then a potential countermeasure is to verify that personal data are not being accessed from Company B's bases (i.e., through analysis of provisioned account/access rights, reviews of access logs during the contract period).

- Confirmation of security management at overseas bases of Company B
  Although Company B does not handle personal data of Company A's employees, etc., its bases do handle data that are valuable for Company A's business such as system operation design data and system operation status data. In recent years, cases of information leakage, etc. due to external attacks, internal frauds, human errors, etc. have been reported due to relatively insufficient security management at the sites of contractors like Company B, overseas branches, etc. such as in the Use Case. If sufficient measures are not implemented for risks that could arise during the application of the framework in the consignment agreements, etc. between Companies A and B, then Company A could take useful measures such as provisioning a more specific safety control measures to ensure that Company B achieves the same management standard as Company A, and verifying compliance status in writing or through auditing, etc.[50]

[50] For details on security control measures in respect to business contractors, etc., see various examples in Section 15.1 "Information security in supplier relationships" of ISO/IEC 27002:2013.

Appendix B. Illustration of the Identified Risks of Each Event

B-1 How to describe, etc. the typical risks of each event

This chapter lists examples of typical risks and effective countermeasure requirements that should ideally be considered by businesses, etc., that wish to apply the framework, when identifying potential risks in their own data utilization process[51].

Table B.1-1: How to describe, etc. the typical risks of each event illustrated in Appendix B

From the viewpoint of protection	Classification of threatening entities	Examples of potential security incidents, etc.	Threats	Examples of effective countermeasure requirements
Confidentiality	Adversaries (Malicious entities)	Data generated and acquired become intercepted and leaked over the network by malicious insiders or external attackers.	Information leakage	Protect communication routes through encryption, etc.

According to the format illustrated in Table B-1, B-2 illustrates examples of applicable functions and assets of each event type (i.e., generation/acquisition, processing/usage, transfer/provision, storage, disposal) and lists the typical risks. The following outline not only illustrates the examples of potential security incidents, etc. that fall under the category of the described risks, but also further clarifies the coverage and scope of the identified risks.

- From the viewpoint of protection

  Presents the protection viewpoints that should be considered when identifying the examples of potential security incidents, etc. Such viewpoints include those related to security protection (i.e., confidentiality, integrity, availability) and those that relate to relevant legal systems, etc. (protection of personal data, intellectual property (including trade secrets), etc.).
- Classification of threatening entities

  There are four categories of threatening entities that can have an (often negative) impact on the applicable data utilization process.

[51] The risks that can be identified in each case are not necessarily limited to those listed here.

Table B.1-2: Examples of classifications of threatening entities[52]

Classification of threatening entities	Overview
Adversaries (Malicious entities)	Individuals, groups, organizations, or nations that try to take advantage of an organization's dependency on cyber resources (i.e., electronic data, information communication technology, and information communication processing abilities generated through such technology). In general, this includes external cyber or physical attacks, internal crimes, etc.
Accidental	Erroneous actions (including human errors) taken by individuals who are not necessarily malicious in the course of fulfilling their day-to-day responsibilities.
Structural	Failures of devices, environmental controls, or software due to aging, resource depletion, or any other circumstance that exceeds the predicted operating parameters.
External environment-related	Impact from a natural disaster or failure of important infrastructure that the organization is dependent on but is outside the control of the organization.

Framework-adopting entities should ideally identify the entities that could be potentially threatening to one's data utilization process and the incidental risks from as comprehensive a perspective as possible including not only malicious internal/external entities (adversaries) that conduct cyber attacks, etc., but also human errors (accidental) of legitimate employees, etc., natural disasters, infrastructure failures, etc.

- Threats

Describes specific threats that could manifest from entities in the above categories. Based on STRIDE, which is one of the means to brainstorm the threats, we present here additional threat types (including malware infection, unauthorized modification, misuse[53], failures of systems, etc., natural disasters) while also considering the properties of IoT devices, etc. involved in the generation, acquisition, processing, usage, etc., of data, as well as the threats from non-advisory entities[54].

[52] Make additions, etc. as appropriate by referencing "Appendix D: Threat Sources - Taxonomy of Threats Sources Capable of Initiating Threat Events in the *NIST Special Publication 800-30 Revision 1* (IPA translation)

[53] "Misuse" here specifically refers to a non-malicious usage by a user.

[54] We added as appropriate the types of threats from threatening entities other than advisories (malicious entities) while also considering the descriptions of threats with high chance of not being extracted via STRIDE described in Separate Volume 1 A detailed guide to threat analysis and security validation of A guide to security validation to ensure cyber security of devices issued (in Japanese, https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html) by the Cybersecurity division of METI.

Table B.1-3: Examples of threat classifications via STRIDE

Threats	Details
Spoofing	Impersonating another user or device when corresponding with a computer.
Tampering	Tampers with data without access rights and destroys data integrity
Repudiation	A user denies that he/she conducted a particular action and the counterparty has no way of proving that he/she did do it
Information leakage	Disclosure of information to an individual without any access rights
Denial of service	When a server, service, etc. becomes inaccessible by legitimate users *Such as due to service interruptions through a DoS attack, jamming, etc.
Elevation of authority	Acquisition of access rights by a user without any rights

Table B.1-4: Examples of threat classifications additionally defined in this document

Threats	Details
Malware infection	Can be a source of infection to other devices. Businesses could also be interrupted due to a ransomware, etc.
Unauthorized modification	Through a fraudulent (illegal) hardware/software modification, internal data are extracted, and vulnerability factors are introduced
Misuse	Usage by a device user for purposes, etc. not originally intended
Failure of system, etc.	Refers to a device failure, an environmental control failure, or a software bug
Natural disasters, etc.	Negative impact on a data utilization process due to natural phenomena such as earthquakes, tsunamis, and heavy rains, or external utility defects such as electricity, communication, water supply, gas, etc.

- Examples of effective countermeasure requirements

Requirement examples of countermeasures that are believed to be effective in reducing the identified risks are illustrated with correspondence to the reference literatures given below. The reference literatures include general ones that pertain to all event types, and detailed ones that somewhat focuses on specific event types.

< General >

- CPSF
- ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements
- SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations
- *Data Management Body of Knowledge (DMBOK) 2nd Edition*

< Generation, acquisition >

- *How to Secure Your Website 7th Edition (in Japanese)*
  https://www.ipa.go.jp/security/vuln/websecurity.html

- NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers

< Transfers, provisions >

- SP 800-47 Rev. 1 Managing the Security of Information Exchanges
- ISO/IEC 27033-1:2015 Information technology – Security techniques – Network security – Part 1: Overview and concepts

< Processing, usage >

- The guidelines for use of AI and data (in Japanese) https://www.meti.go.jp/press/2019/12/20191209001/20191209001.html

< Disposal >

- SP 800-88 Rev. 1 Guidelines for Media Sanitization

From the viewpoint of data protection, we have illustrated the relevance of the following reference literatures (guidelines pertaining to various laws and regulations) for incidents, etc. that require the consideration of protections of personal data and intellectual properties (including trade secrets).

< Personal data protection >

- *Guidelines for Protection of Personal Information* (General Provisions)
- *Guidelines for Protection of Personal Information* (Obligation to check and record during third party provisions)
- *Guidelines for Protection of Personal Information* (Anonymously processed data)

< Intellectual property (including trade secrets) protection >

- *Management Guidelines for Trade Secrets*

B-2 Illustration of the identified risks of each event

According to the format illustrated in Table B.1-1, this section illustrates the typical risks and useful countermeasure requirements upon exemplifying functions and assets applicable to each event type (i.e., generation/acquisition, processing/usage,

transfer/provision, storage, disposal).

B-2-1 Illustration of risk identification in the data generation/acquisition process

Data generation/acquisition through sensor measurements, manual inputs, etc. constitutes the initial data life cycle stage, and holds an important position in ensuring data trustworthiness in the subsequent utilization process. Since some generations/acquisitions could be conducted through various means, risk assessment should ideally be conducted after specifically identifying the assessment method. The following exemplifies applicable functions and assets, potential risks, and effective countermeasure requirements that are common to such various methods, etc.

< Applicable functions >

- A function that reads physical events in physical space, converts them into digital information based on certain rules, and sends them to cyber space
- These also refer to functions that generate/acquire data through direct input into an online system, etc., collection of usage history, etc.

< Applicable assets >

- Facilities and devices related to data generation and acquisition (i.e., sensors, web servers, business terminals)
- Networks connected to any of the above

Table B.2-1: Illustration of risk identification in the data generation/acquisition process

From the viewpoint of protection	Classification of threatening entities	Examples of potential security incidents, etc.	Threats	Examples of effective countermeasure requirements
Confidentiality	Adversaries (Malicious entities)	Data generated and acquired become intercepted and leaked over the network by malicious insiders or external attackers.	Information leakage	**Protect communication routes through encryption, etc.**
				Monitoring and handling of communication routes, terminal behavior, etc.
	Adversaries (Malicious entities)	Generated/acquired data become shared to a fraudulent destination from a device, facility, etc. infected with a malware.	Information leakage	**Maintenance and execution of vulnerability handling processes**
				Introduction of anti-malware measures on terminals and networks
				Monitoring and handling of outward communications
	Accidental	Facilities and devices related to data generation and acquisition are improperly	Information leakage	**Manage changes to the initial settings, configurations, etc. of**

		configured, allowing data to be viewed by entities not originally intended.		**devices and services**
				Implementation of appropriate standard levels for users, devices, services, etc.
				Monitoring and handling of communication routes, terminal behavior, etc.
Integrity	Adversaries (Malicious entities)	Generation/acquisition of inaccurate data due to impersonation by a legitimate user (especially when data are input manually).	Impersonation	**Implementation of appropriate standard levels for users, devices, services, etc.**
				Input value validation
	Adversaries (Malicious entities)	Generation/acquisition of inaccurate data due to impersonation of a device from which data originated by a fraudulent device.	Impersonation	**Implement access control in the physical environment where the devices, etc. are installed**
				Monitoring of the physical environment where the devices, etc. are installed
				Monitoring and handling of communication routes, terminal behavior, etc.
				Input value validation
	Adversaries (Malicious entities)	Generation/acquisition of inaccurate data due to an unauthorized modification of currently-operating device(s) from which data originated.	Unauthorized modification	**Strengthen physical resistance of devices, etc.**
				Implement access control in the physical environment where the devices, etc. are installed
				Monitoring of the physical environment where the devices, etc. are installed
	Adversaries (Malicious entities)	Generation/acquisition of inaccurate data from a non-originating device due to a physical disturbance by a malicious employee or third party.	Impersonation	**Input value validation**
				Monitoring of the physical environment where the devices, etc. are installed
	Adversaries (Malicious entities)	Data generated and acquired from legitimate devices are intercepted and tampered with on the network.	Tampering	**Protect communication routes through encryption, etc.**
				Protection of data integrity and authenticity
	Structural	An event such as transmission of defective or inaccurate data, transmission of data to an unexpected destination, etc. occurs due to a network connection by an IoT device with low quality or trustworthiness.	Failure of system, etc.	**Authenticity validation of devices/systems during operation**
	Accidental	Generation/acquisition of inaccurate data due to an incorrect input by a legitimate user (especially when data are input	Misuse	**Input value validation**

		manually).		
Availability	Adversaries (Malicious entities)	Temporary suspension of facilities and devices during data generation/acquisition due to a denial-of-service attack, etc.	Denial of service	**Ensure redundancy and backup of devices, communication devices, lines, etc.** **Monitoring and handling of communication routes, terminal behavior, etc.**
	Adversaries (Malicious entities)	Data cannot be generated/acquired due to activity suspension of a facility or device such as a sensor due to malware infection.	Malware infection	**Maintenance and execution of vulnerability handling processes** **Introduction of anti-malware measures on terminals and networks**
	Structural	Temporary suspension of processes due to defects in a facility or device involved in data generation/acquisition.	Failure of system, etc.	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
	Environmental	Temporary suspension of processes due to a damage to a facility or device involved in data generation/acquisition due to a natural disaster such as an earthquake or tsunami.	Natural disasters, etc.	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
Personal data protection	Accidental	The organization from which the data is acquired does not clearly indicate the purpose of use of the data it generates or obtains to the data-originating individuals or does not present the purpose in correspondence with the actual use of the data.	Insufficient compliance	**Presentation of purpose of use, etc. at the time of data acquisition**
	Accidental	A data-acquiring organization acquires personal information through fraudulent means such as fabrication.	Insufficient compliance	**Data acquisition through legitimate means**
Intellectual property (including trade secrets) protection	Adversaries (Malicious entities)	A malicious employee or retiree including a third party acquires trade secrets managed on paper, etc. as data through fraudulent means (including theft, fraud, duress).	Information leakage	**Manage trade secrets, etc. in a way that ensures confidentiality**
	Accidental	Another company's trade secrets, etc. are unintentionally acquired such as through the inclusion of such information in data brought in by a job transferee from another company, etc.	Insufficient compliance	**Ensure the security of the personnel of one's own organization, contractors, etc.**

B-2-2 Illustration of risk identification in the data processing/usage process

Data do not necessarily create added value just by being generated, acquired, and stored, but through some kind of processing and use. On the other hand, if a failure occurs in the processing/usage process, the data trustworthiness and potential benefits from data

utilization could become significantly undermined. Therefore, it is important to correctly recognize the risks and take appropriate measures just like in any other event. The following exemplifies the applicable functions and assets of the processing/usage process, the potential risks, and the requirements for effective countermeasures.

< Applicable functions >

- Data processing/analysis functions

< Applicable assets >

- Facilities and devices for processing/using data (i.e., servers, business terminals, and software assets installed there)

Table B.2-2: Illustration of risk identification in the data processing/usage process

From the viewpoint of protection	Classification of threatening entities	Examples of potential security incidents, etc.	Threats	Examples of effective countermeasure requirements
Confidentiality	Adversaries (Malicious entities)	A malicious internal/external entity references all or part of the applicable data without legitimate authority during the processing/usage process and identifies confidential data of the company or other companies.	Information leakage	**Secure the processing/usage process via encryption, etc.**
	Accidental	Data that need to be generally protected become externally viewable due to a misconfiguration of access controls, etc. for applications, databases, etc.	Information leakage	**Allocate the minimum necessary authority in principle**
				Manage changes to the initial settings, configurations, etc. of devices and services
Integrity	Adversaries (Malicious entities)	The application becomes tampered with by a malicious internal or external entity, resulting in unauthorized processing of data	Tampering	**Implementation of appropriate standard levels for users, devices, services, etc.**
				Allocate the minimum necessary authority in principle
				Continuously manage application security
	Adversaries (Malicious entities)	A malicious internal/external entity tampers or deletes all or part of the data through intentional processing/usage.	Tampering	**Choose appropriate personnel and services**
				Ensure the security of the personnel of one's own organization, contractors, etc.
				Monitoring and handling of communication routes, terminal behavior, etc.

	Accidental	A legitimate employee accidentally changes or deletes all or part of the data through data processing/usage without any malicious intention.	Misuse	**Choose appropriate personnel and services**
				Ensure the security of the personnel of one's own organization, contractors, etc.
				Ensure redundancy and backup of devices, communication devices, lines, etc.
	Structural	Part of a facility or device that processes/uses data fails or malfunctions, resulting in loss of integrity.	Failure of system, etc.	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
Availability	Adversaries (Malicious entities)	Facilities and devices that process/use data become temporary suspended due to a denial-of-service attack, malware infection, etc.	Denial of service	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
			Malware infection	**Maintenance and execution of vulnerability handling processes**
				Input value validation
				Introduction of anti-malware measures on terminals and networks
	Structural	A facility or device that processes/uses data malfunctions due to excessive processing requests, etc., and processes become temporarily suspended.	Failure of system, etc.	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
	Environmental	Temporary suspension of processes due to a damage to a facility or device involved in data processing/usage due to a natural disaster such as an earthquake or tsunami.	Natural disasters, etc.	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
Personal data protection	Adversaries (Malicious entities)	Employees use the data for purposes that are different from what were notified in advance to the data subjects without taking necessary procedures.	Insufficient compliance	**Restrict processing/usage based on the purpose of use, etc.**
	Adversaries (Malicious entities)	Pseudonymized information and anonymously processed data become compared with other information to identify the identity of the original data subjects.	Insufficient compliance	**Prohibit identification behaviors that use pseudonymized information and anonymously processed data**
	Accidental	Personal information is not being processed into a pseudonymized information or anonymously processed data through an appropriate method that satisfies the requirements stipulated by laws, regulations, etc.	Insufficient compliance	**Appropriately process pseudonymized information and anonymously processed data**
Intellectual property (including trade secrets)	Adversaries (Malicious entities)	A malicious internal/external entity (including retirees) uses data that it has acquired through legitimate	Insufficient compliance	**Ensure the security of the personnel of one's own organization, contractors, etc.**

protection		means to gain unfair advantage or cause harm to the rights holder.		**Monitoring and handling of communication routes, terminal behavior, etc.**
	Accidental	Data become used by employees, without taking necessary procedures, through methods that differ from the terms of use (purpose use, usage rights, etc.) agreed upon in advance with the data-providing organization.	Insufficient compliance	**Restrict processing/usage based on the purpose of use, etc.**

B-2-3 Illustration of risk identification in the data transfer/provision process

In recent years, as more and more data have been generated, acquired, processed, and used, the importance is being recognized of sharing (transferring, providing) data within an organization or between several organizations to maximize the benefits derived from data. But since the networks where transfers and provisions mainly take place pose potential risks and threats that differ from the process of processing, using, or storing data, it is important to correctly identify them and take measures. The following exemplifies functions and assets that are relevant to the transfer/provision process, the potential risks, and the effective countermeasure requirements.

< Applicable functions >

- Functions to send and receive data

< Applicable assets >

- Facilities and devices related to the transfer and provision of data (i.e., networks, network devices, servers, business terminals)

Table B.2-3: Illustration of risk identification in the data transfer/provision process

From the viewpoint of protection	Classification of threatening entities	Examples of potential security incidents, etc.	Threats	Examples of effective countermeasure requirements
Confidentiality	Adversaries (Malicious entities)	Data become intercepted and leaked by a malicious third party on a network related to the transfer or provision.	Information leakage	**Protect communication routes through encryption, etc.**
	Adversaries (Malicious entities)	Data become transferred/provided to a fraudulent destination from a device, facility, etc. infected with a malware.	Malware infection	**Maintenance and execution of vulnerability handling processes**
				Introduction of anti-malware measures on terminals and networks
			Information leakage	**Monitoring and handling of outward communications**
	Adversaries (Malicious entities)	Data become transferred/provided to a fraudulent destination that is impersonating as a legitimate destination.	Impersonation	**Protect communication routes through encryption, etc.**
				Monitoring and handling of communication routes, terminal behavior, etc.
	Accidental	A legitimate non-malicious user transfers/provides data to a destination not originally foreseen.	Information leakage	**Monitoring and handling of communication routes, terminal behavior, etc.**
				Monitoring and handling of outward communications
Integrity	Adversaries (Malicious entities)	Data become intercepted and tampered by a malicious third party on a network related to the transfer or provision.	Tampering	**Protect communication routes through encryption, etc.**
				Protection of data integrity and authenticity
Availability	Adversaries (Malicious entities)	Temporary suspension of facilities and devices during data transfer/provision due to a denial-of-service attack, etc.	Denial of service	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
				Monitoring and handling of communication routes, terminal behavior, etc.
	Adversaries (Malicious entities)	Facilities and devices related to the transfer and provision of data become infected with malware, and data cannot be transferred or provided.	Malware infection	**Maintenance and execution of vulnerability handling processes**
				Introduction of anti-malware measures on terminals and networks
	Structural	Temporary suspension of processes due to defects in a facility or device involved in data transfer/provision.	Failure of system, etc.	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
	Environmental	Temporary suspension of processes due to a damage to a facility or device involved in data transfer/provision due to a natural disaster such as an earthquake or tsunami.	Natural disasters, etc.	**Ensure redundancy and backup of devices, communication devices, lines, etc.**

Personal data protection	Accidental	Personal data become provided to a third party without specific reasons under laws, regulations, etc. and without conducting procedures, etc. related to acquiring individual consent or processing opt-out requests in advance.	Insufficient compliance	**Ensure justifiable basis for provision to third parties**
	Accidental	When providing personal data to third parties, records are not being created nor verified by the data provider and/or the receiver.	Insufficient compliance	**Create and verify records during provision to third parties**
	Accidental	When providing personal data to third parties in foreign countries, mandatory procedures such as acquisition of individual consent and provision of appropriate information are not being conducted.	Insufficient compliance	**Implement necessary procedures when providing data to third parties in foreign countries**
Intellectual property (including trade secrets) protection	Adversaries (Malicious entities)	A malicious employee or third-party including retirees transfers and provides trade secrets acquired through fraudulent means (i.e., theft, fraud, duress).	Insufficient compliance	**Manage trade secrets, etc. in a way that ensures confidentiality**
	Adversaries (Malicious entities)	A data-receiving entity (through a transfer/provision) acquires trade secrets without knowing, either intentionally or through gross negligence, about the fact that fraudulent acquisition was involved.	Insufficient compliance	**Manage trade secrets, etc. in a way that ensures confidentiality**
	Accidental	A data-receiving entity (through a transfer/provision) acquires trade secrets without knowing, either intentionally or through gross negligence, about the fact that fraudulent acquisition was involved, and then later starts harboring malicious intent or gross negligence after the acquisition regarding the fraudulent acquisition, and then ultimately discloses the trade secrets to a third party.	Insufficient compliance	**Manage trade secrets, etc. in a way that ensures confidentiality**
	Adversaries (Malicious entities)	An adversary discloses the trade secrets received from a transfer/provision originator to gain unfair benefit or cause harm to the said data holder.	Insufficient compliance	**Manage trade secrets, etc. in a way that ensures confidentiality**
	Accidental	An employee or retiree discloses the trade secrets managed by one's own company to an external business, etc. without realizing that these were trade secrets.	Insufficient compliance	**Ensure confidentiality for sharing trade secrets to internal or external parties**

B-2-4 Illustration of risk identification in the data storage process

During various data lifecycle stages, data could become stored in external services (including cloud storage), network-connected storage devices, client hard disks, portable media such as USB memory, and temporary storage areas of devices. As data are becoming more actively utilized and the types and volume of accumulated data are further increasing, it is becoming even more important to secure large scale data storage and stored data. The following exemplifies functions and assets that are relevant to the said process, the potential risks, and the effective countermeasure requirements.

< Applicable functions >

- Data-storing functions

< Applicable assets >

- Facilities and devices that could store data under various data processes (i.e., servers, business terminals, long-term storage mediums)

Table B.2-4: Illustration of risk identification in the data storage process

From the viewpoint of protection	Classification of threatening entities	Examples of potential security incidents, etc.	Threats	Examples of effective countermeasure requirements
Confidentiality	Adversaries (Malicious entities)	An external attacker fraudulently and externally accesses devices and systems that store data by taking advantage of weak passwords, software vulnerabilities, etc., causing data leakage.	Information leakage	**Implementation of appropriate standard levels for users, devices, services, etc.**
				Allocate the minimum necessary authority in principle
				Encrypt stored data, etc.
				Maintenance and execution of vulnerability handling processes
				Monitoring and handling of outward communications
	Adversaries (Malicious entities)	A malicious employee, a prospective retiree, an employee of an external contractor, etc. gains access to the devices and systems that store data and leaks the data that must be protected.	Information leakage	**Ensure the security of the personnel of one's own organization, contractors, etc.**
				Monitoring of the physical environment where the devices, etc. are installed
				Encrypt stored data, etc.
				Monitoring and handling of communication routes, terminal behavior, etc.
	Adversaries (Malicious entities)	An entity such as an external attacker or a malicious internal/external employee	Information leakage	**Implement access control in the physical environment where the devices, etc. are**

		steals or fraudulently reads data from a data-storing medium (i.e., portable media such as HDD, SSD, USB memory, CD, DVD, etc. within a terminal).		**installed**
				Encrypt stored data, etc.
				Monitoring of the physical environment where the devices, etc. are installed
	Accidental	Facilities and devices related to data storage are improperly configured, allowing stored data to be viewed by entities not originally intended.	Information leakage	**Manage changes to the initial settings, configurations, etc. of devices and services**
				Encrypt stored data, etc.
				Monitoring and handling of communication routes, terminal behavior, etc.
		Data that need to be sufficiently safeguarded become disclosed when shared servers, etc. become seized due to requests from domestic or foreign judicial organ, etc.	Information leakage	**Verify the location of facilities such as servers that process and store data**
Integrity	Adversaries (Malicious entities)	A malicious internal/external entity intentionally tampers or deletes all or part of the stored data.	Tampering	**Implementation of appropriate standard levels for users, devices, services, etc.**
				Allocate the minimum necessary authority in principle
				Protection of data integrity and authenticity
	Adversaries (Malicious entities)	Tampering, deletion, or destruction of all or part of the stored data due to malware infection, etc.	Malware infection	**Manage changes to the initial settings, configurations, etc. of devices and services**
				Maintenance and execution of vulnerability handling processes
				Introduction of anti-malware measures on terminals and networks
	Accidental	A legitimate employee (of one's own company or contractor, etc.) accidentally, without malice, changes or deletes all or part of the stored data.	Non-intentional misuse	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
	Structural	A data-storing facility or device (which could include those operated by a contractor, etc.) fails or malfunctions, resulting in the loss of all or part of the stored data.	Failure of system, etc.	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
Availability	Adversaries (Malicious entities)	Facilities and devices that process/use data become temporary suspended due to a denial-of-service attack, malware infection, etc.	Denial of service	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
			Malware infection	**Maintenance and execution of vulnerability handling processes**
				Introduction of anti-malware measures on terminals and networks

	Structural	A data-storing facility or device (which could include those operated by a contractor, etc.) fails or malfunctions, resulting in the temporary suspension of processes.	Failure of system, etc.	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
	Environmental	Temporary suspension of processes due to a damage to a facility or device involved in data storage due to a natural disaster such as an earthquake or tsunami.	Natural disasters, etc.	**Ensure redundancy and backup of devices, communication devices, lines, etc.**
Personal data protection	Accidental	A data correction or deletion request from the data subject becomes insufficiently handled because the corresponding personal data held and used by the business is not true.	Insufficient compliance	**Correct, suspend use of, etc. held personal data according to the requests from data subjects**
	Accidental	Appropriate safety control measures (including supervision of employees and contractors) are not being taken on personal data stored by the business.	Insufficient compliance	**Implement safety control measures on personal data**
	Accidental	Personal data that do not necessarily have to be used anymore are still being unnecessarily retained or used.	Insufficient compliance	**Erase data without delay**

Intellectual property (including trade secrets) protection	Adversaries (Malicious entities)	A malicious external attacker, employee, prospective retiree, etc. accesses stored data managed as a trade secret, and the data become externally leaked.	Information leakage	**Implementation of appropriate standard levels for users, devices, services, etc.**
				Allocate the minimum necessary authority in principle
				Monitoring and handling of communication routes, terminal behavior, etc.
	Accidental	Information such as trade secrets received by another company is continuously stored without obtaining additional approval, etc., regardless of the fact that the expiration date has already passed.	Insufficient compliance	**Ensure the security of the personnel of one's own organization, contractors, etc.**
				Erase data without delay
	Accidental	External intellectual properties, etc. become contaminated with those held by one's own company, resulting in the inadvertent usage/disclosure of such information.	Insufficient compliance	**Ensure the security of the personnel of one's own organization, contractors, etc.**
				Separately manage secrets, etc. of other companies

B-2-5 Illustration of risk identification in the data disposal process

Data, which are utilized for various purposes, end its life cycle by being disposed and rendered unrecoverable through appropriate means such as data overwriting, physical destruction of media, and encryption of entire disks. The following exemplifies functions and assets that are relevant to the said process, the potential risks, and the effective countermeasure requirements.

< Applicable functions >

-

< Applicable assets >

・ Facilities and devices that could store data under various data processes (i.e., servers, storage mediums on business terminals)

Table B.2-5: Illustration of risk identification in the data disposal process

From the viewpoint of protection	Classification of threatening entities	Examples of potential security incidents, etc.	Threats	Examples of effective countermeasure requirements
Confidentiality	Adversaries (Malicious entities)	An external attacker, malicious employee, etc. fraudulently restores data that were disposed through insufficient means after a business terminated the data's usage.	Information leakage	**Choose appropriate personnel and services**
				Dispose data and media through appropriate means

	Adversaries (Malicious entities)	A malicious employee or employee of a data disposal contractor externally discloses data that were about to be disposed.	Information leakage	**Choose appropriate personnel and services** **Verify the fulfillment of data and media disposal**
	Accidental	Disposal has been outsourced, but it cannot be verified that data have been properly deleted or disposed by the contractor due to reasons such as not having obtained a disposal certificate, etc. from the contractor.	Insufficient compliance	**Verify the fulfillment of data and media disposal**
Integrity	Accidental	Data that should not be disposed are being disposed during the disposal of storage media, etc.	Misuse	**Ensure redundancy and backup of devices, communication devices, lines, etc.**

B-2-6 Countermeasure requirement examples and reference guidelines

The following illustrates the relationship between the effective countermeasure requirements (examples) shown in B-2-1 to B-2-5 and the various reference guidelines, which can be used as a reference to promote initiatives for ensuring data trustworthiness. Note that the said requirement examples refer to the requirements of main countermeasures pertaining to defense and detection that should be implemented during the risk-handling stage, which presumes that a risk management process is already fully established by the applicable entities.

Table B.2-6: Countermeasure requirement examples and reference guidelines

Countermeasures	Applicable events	Reference guidelines
Choose appropriate personnel and services	Processing/usage, disposal	- CPSF Ver.1.0 CPS.SC-4, CPS.SC-5 - ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.2.1 - NIST SP 800-53 Rev. 5 PS-7, SR-5, SR-6 < A more detailed guidelines > Section 5.2(1), (9), 6.4(1), (5) of the The guidelines for use of AI and data (Data edition) - NIST SP 800-88 Rev. 1 4.7 Verify Methods
Ensure the security of the personnel of one's own organization, contractors, etc.	Processing/usage, storage	- CPSF Ver.1.0 CPS.GV-1, CPS.SC-5, CPS.AT-1, CPS.AT-2 - ISO/IEC 27001:2013 A.6.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.3.1, A.15.1.1 - NIST SP 800-53 Rev. 5 AT-1, AT-2, AT-3, AT-4, PS-7, SA-9, SA-16, SA-21 Section 5.4 Data Security in an Outsourced World", Chapter 7, *DAMA-DMBoK* < A more detailed guidelines > ・ Sections 5.2(1), (9), 6.4(1), (5) of the The guidelines for use of AI and data (Data edition)
Implementation of appropriate standard levels for users, devices, services, etc.	Generation, acquisition, transfer/provision, processing/usage,	- CPSF Ver.1.0 CPS.AC-1, AC-4, AC-9 - ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 - NIST SP 800-53 Rev. 5 AC-2, AC-3, AC-7, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

	storage	・ Section 3.3 Identity Management Technology, Chapter 7 of the *DAMA-DMBoK* < A more detailed guidelines > - NISTIR 8259 Activity 3 - NISTIR 8259A Logical Access to Interfaces ・ Section 1.4 Improper Session Management," Section 1.11 "Lack of access/approval controls, Section 2.5 Password measures of the *How to Secure Your Website 7th Edition* ・ Sections 5.2(1), (9), 6.4(1), (5) of the The guidelines for use of AI and data (Data edition) - ISO/IEC 27035-1:2015 8.4 Identification and authentication - NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan

Allocate the minimum necessary authority in principle and obtain approvals	Processing/usage, storage	- CPSF Ver.1.0 CPS.AC-5, CPS.AC-9 - ISO/IEC 27001:2013 A.6.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 - NIST SP 800-53 Rev. 5 AC-1, AC-3, AC5, AC-6, AC-24 ・ Section 2.3.5.3 Data security management and maintenance, Chapter 7, *DAMA-DMBoK* < A more detailed guidelines > ・ Sections 5.2(1), (9), 6.4(1), (5) of the The guidelines for use of AI and data (Data edition)
Protect communication routes through encryption, etc.	Generation, acquisition, transfer/provision	- CPSF Ver.1.0 DS-23 - ISO/IEC 27001:2013 A.13.2.1, A.13.2.3 - NIST SP 800-53 Rev. 5 CA-3, SC-8, SC-11, SC-12, SC-13 Section 3.2 HTTPS, Chapter 7 of the *DAMA-DMBoK* < A more detailed guidelines > - NISTIR 8259 Activity 3 - NISTIR 8259A Data Protection ・ *How to Secure Your Website 7th Edition, Section 2.3 Protect Against Network Sniffing* - ISO/IEC 27035-1:2015 7.2.2 Information on current/planned networking, 8.8 Cryptographic based services - NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan
Encrypt stored data, etc.	Storage	- CPSF Ver.1.0 DS-3 - ISO/IEC 27001:2013 A.10.1.1 - NIST SP 800-53 Rev. 5 SC-28
Secure the data processing/usage process via encryption, etc.	Processing, usage	-
Protection of data integrity and authenticity	Transfer/provision, storage	- CPSF Ver.1.0 CPS.DS-11, CPS.CM-4CPS.DS-10, CPS.CM-3 - ISO/IEC 27001:2013 A.13.2.3, A.14.1.2, A.14.1.3A.12.2.1, A.12.5.1, A.14.2.4 - NIST SP 800-53 Rev. 5 SC-16, SI-7SI-3, SI-7 Section 2.3.5.3 Data security management and maintenance, Section 3.1 Anti-Virus Software / Security Software, Chapter 7 of the *DAMA-DMBoK* < A more detailed guidelines > - ISO/IEC 27035-1:2015 7.2.2 8.8 Cryptographic based services - NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan
Dispose data and media through appropriate means	Disposal	- CPSF Ver.1.0 CPS.DS-6, CPS.IP-6 - ISO/IEC 27001:2013 A.8.3.2, A.11.2.7 - NIST SP 800-53 Rev. 5 MP-6 Section 4.7 Document sanitization, Chapter 7 of the *DAMA-DMBoK* < A more detailed guidelines > - NIST SP 800-88 Rev. 1 4 Information Sanitization and Disposition Decision Making
Verify the fulfillment of data and media disposal	Disposal	- ISO/IEC 27001:2013 A.8.3.2, A.11.2.7 - NIST SP 800-53 Rev. 5 MP-6 < A more detailed guidelines > - NIST SP 800-88 Rev. 1 4.7 Verify Methods, 4.8 Documentation
Manage changes to the initial settings, configurations, etc. of devices and services	Generation, acquisition, storage	- CPSF Ver.1.0 CPS.AM-1, IP-1, IP-2, .PT-2 - ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.14.2.2, A.14.2.3, A.14.2.4 - NIST SP 800-53 Rev. 5 CM-2, CM-7, CM-8, CM-11, PE-20 < A more detailed guidelines > - NISTIR 8259 Activity 3 - NISTIR 8259A Device Identification, Device Configuration - NISTIR 8259B Documentation, Education and Awareness
Authenticity validation of devices/systems during operation	Generation, acquisition	- CPSF Ver.1.0 CPS.DS-13 - ISO/IEC 27001:2013 A.11.2.4 - NIST SP 800-53 Rev. 5 SA-10, SI-7
Continuously manage application security	Processing/usage, transfer/provision	- CPSF Ver.1.0 CPS.DS-10, CPS.DS-13, CPS.IP-2, CPS.MA-1 CPS.CM-3 - ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.12.6.1, A.14.2.4, A.14.2.5 - NIST SP 800-53 Rev. 5 CM-2, CM-5, SI-3, SI-7 ・ Section 3.1 Anti-Virus Software / Security Software, Chapter 7 of the *DAMA-DMBoK* < A more detailed guidelines > ・ Sections 5.2(9), 6.4(5) of the The guidelines for use of AI and data (Data edition) - ISO/IEC 27035-1:2015 - NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan, 3.3 Maintaining the Information Exchange

Introduction of anti-malware measures on terminals and networks	Generation, acquisition, transfer/provision, processing/usage, storage	- CPSF Ver.1.0 CPS.DS-10, CPS.CM-3 - ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.2.4 - NIST SP 800-53 Rev. 5 SI-3, SI-7 ・ Section 3.1 Anti-Virus Software / Security Software, Chapter 7 of the *DAMA-DMBoK* < A more detailed guidelines > - NISTIR 8259 Activity 3 - NISTIR 8259A Cybersecurity State Awareness - NISTIR 8259B Information and Query Reception ・ Section 2.1.1 How to continuously obtain information on vulnerabilities in operating systems and software, and how to deal with these vulnerabilities, Section 2.6 Protect Web Applications with WAF, of the *How to Secure Your Website 7th Edition* ・ Sections 5.2(9), 6.4(5) of the The guidelines for use of AI and data (Data edition)
Maintenance and execution of vulnerability handling processes	Generation, acquisition, transfer/provision, processing/usage, storage	- CPSF Ver.1.0 CPS.RA-1, CPS.RA-2, CPS.IP-10, CPS.MA-1, CPS.CM-7 - ISO/IEC 27001:2013 A.6.1.4, A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.3 - NIST SP 800-53 Rev. 5 CA-2, CA-7, CA-8, RA-3, RA-5, SI-2, SI-4, SI-5 ・ Section 4.2 Immediate Security Patch Deployment, Chapter 7 of the *DAMA-DMBoK* < A more detailed guidelines > - NISTIR 8259 Activity 4, Activity 5, Activity 6 - NISTIR 8259A Device Configuration, Software Update - NISTIR 8259B Information Dissemination ・ Section 2.1.1 How to continuously obtain information on vulnerabilities in operating systems and software, and how to deal with these vulnerabilities of the *How to Secure Your Website 7th Edition* ・ Sections 5.2(4), (9), 6.4(5) of the The guidelines for use of AI and data (Data edition) - ISO/IEC 27035-1:2015 8.2.5 Evaluating network security, 8.3 Technical vulnerability management - NIST SP 800-47 Rev.1 3.3 Maintaining the Information Exchange
Implement access control in the physical environment where the devices, etc. are installed	Generation, acquisition, storage	- CPSF Ver.1.0 CPS.AC-2 - ISO/IEC 27001:2013 A.11.1.2, A.11.1.3, A.11.2.1, A.11.2.6, A.11.2.8 - NIST SP 800-53 Rev. 5 PE-2, PE-3, PE-4, PE-5 < A more detailed guidelines > - NISTIR 8259 Activity 3
Monitoring of the physical environment where the devices, etc. are installed	Generation, acquisition, storage	- CPSF Ver.1.0 CM-2 - ISO/IEC 27001:2013 A.11.1.2, A.11.2.5, A.11.2.6 - NIST SP 800-53 Rev. 5 CA-7, PE-3, PE-6, PE-8, PE-20 < A more detailed guidelines > - NISTIR 8259 Activity 3
Strengthen physical resistance of devices, etc.	Generation, acquisition	- CPSF Ver.1.0 CPS.DS-8 - ISO/IEC 27001:2013 A.8.2.3, A.10.1.2, A.11.1.4, A.11.1.5, A.11.2.1 - NIST SP 800-53 Rev. 5 SR-9, SR-11 < A more detailed guidelines > - NISTIR 8259 Activity 3
Control data flow through network isolation, etc.	Transfer, provision	- CPSF Ver.1.0 CPS.AM-4, CPS.AC-7, CPS.CM-1 - ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 - NIST SP 800-53 Rev. 5 AC-4, CA-3, CA-9, SC-7 ・ Section 3.5 Firewall (prevention), Chapter 7 of the *DAMA-DMBoK* < A more detailed guidelines > - ISO/IEC 27035-1:2015 8.2.5 Evaluating network security, 8.3 Technical vulnerability management - NIST SP 800-47 Rev.1 3.3 Maintaining the Information Exchange

Monitoring and handling of communication routes, terminal behavior, etc.	Generation, acquisition, transfer/provision, processing/usage	- CPSF Ver.1.0 CM-1, CM-5, CM-6 - ISO/IEC 27001:2013 A.12.4.1, A.12.4.2 - NIST SP 800-53 Rev. 5 AU-12, AU-13, AU-14, CA-7, PE-21, SC-7, SI-4 ・ Section 2.3.5.3 Data security management and maintenance, Section 3.4 Intrusion Detection and Prevention Software, Section 3.5 (Firewall (prevention), Chapter 7 of the *DAMA-DMBoK* < A more detailed guidelines > - NISTIR 8259 Activity 3 - NISTIR 8259A Cybersecurity State Awareness - NISTIR 8259B Information and Query Reception ・ Section 2.6 Protect Web Applications with WAF, of the *How to Secure Your Website 7th Edition* ・ Sections 5.2(1), (9), 6.4(1), (5) of the The guidelines for use of AI and data (Data edition) - ISO/IEC 27035-1:2015 8.2.4 Network monitoring, 8.5 Network audit logging and monitoring - NIST SP 800-47 Rev.1 3.3.3 Maintaining the Information Exchange
Input value validation	Generation, acquisition, processing/usage	- CPSF Ver.1.0 CPS.CM-3 - ISO/IEC 27001:2013 A.12.2.1 - NIST SP 800-53 Rev. 5 SI-10 < A more detailed guidelines > - NISTIR 8259 Activity 3 ・ Section 1.1 SQL Injection, Section 1.2 OS Command Injection, Section 1.3 Unchecked Path Parameter / Directory Traversal, Section 1.10 Buffer overflow, Section 2.6 Protect Web Applications with WAF, of the *How to Secure Your Website 7th Edition* ・ Sections 5.2(1), (9), 6.4(1), (5) of the The guidelines for use of AI and data (Data edition)
Monitoring and handling of outward communications	Generation, acquisition, transfer/provision, processing/usage, storage	- CPSF Ver.1.0 CPS.DS-9 - ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.13.1.1, A.13.2.1 - NIST SP 800-53 Rev. 5 AC-4, SC-7, SI-4 ・ Section 2.3.5.1 Assignment of confidentiality levels, Section 2.3.5.2 Assignment of regulated categories, Section 2.3.5.3 Data security management and maintenance, Section 3.6 Metadata Tracking, Chapter 7 of the *DAMA-DMBoK* < A more detailed guidelines > - NISTIR 8259 Activity 3 ・ Section 2.6 Protect Web Applications with WAF, of the *How to Secure Your Website 7th Edition* ・ Sections 5.2(1), (9), 6.4(1), (5) of the The guidelines for use of AI and data (Data edition)
Presentation of purpose of use, etc. at the time of data acquisition	Generation, acquisition	< A more detailed guidelines > ・ Section 3-1-1 Identification of purpose of use, Section 3-1-2 Changing the purpose of use, Section 3-3-2 Acquisition of sensitive personal information, Section 3-3-3 Notification or publication of purpose of use, Section 3-3-4 Direct acquisition in writing, etc., Section 3-3-5 When it is not necessary to notify, etc. the purpose of use of the *Guidelines for Protection of Personal Information* (General Provisions)
Data acquisition through legitimate means	Generation, acquisition	< A more detailed guidelines > ・ Section 3-3-1 Appropriate acquisition (related to Article 17, Paragraph 1 of the Act) of the *Guidelines for Protection of Personal Information* (General Provisions)

Ensure justifiable basis for provision to third parties	Transfer, provision	< A more detailed guidelines > ・ Section 3-4-1 Principle of restriction on provision to third parties (related to Article 23, Paragraph 1 of the Act), Section 3-4-2 Provision to third parties through the opt-out option (related to Article 23, Paragraphs 2 through 4 of the Act)), Section 3-4-3 (If it does not fall under the category of a third party (related to Article 23, Paragraphs 5 and 6 of the Act)), Section 3-4-4 Restrictions on provision to third parties in foreign countries (related to Article 24 of the Act) of the *Guidelines for Protection of Personal Information* (General Provisions) ・ *Guidelines for Protection of Personal Information* (Provision to third parties in foreign countries) (General edition)
Create and verify records during provision to third parties	Transfer, provision	< A more detailed guidelines > ・ Section 3-4-5 Creating, etc. records of provision to third parties (related to Article 25 of the Act)), Section 3-4-6 Verifications, etc. when receiving data from a third party (related to Article 26 of the Act) of the *Guidelines for Protection of Personal Information* (General Provisions) ・ *Guidelines for Protection of Personal Information* (Obligations to verify and record during provision to third parties) (General edition)
Implement necessary procedures when providing data to third parties in foreign countries	Transfer, provision	< A more detailed guidelines > ・ Section 3-4-4 (Restrictions on provision to third parties in foreign countries (related to Article 24 of the Act)) of the *Guidelines for Protection of Personal Information* (General Provisions) ・ *Guidelines for Protection of Personal Information* (Provision to third parties in foreign countries) (General edition)
Prohibit identification behaviors that use pseudonymized information and anonymously processed data	Processing, usage	< A more detailed guidelines > ・ Section 3-1-3 Restrictions based on purpose of use (related to Article 16, Paragraph 1 of the Act)), Section 3-1-4 Business succession (related to Article 16, Paragraph 2 of the Act), Section 3-1-5 Exceptions to the restrictions based on purpose of use (related to Article 16, Paragraph 3 of the Act) of the *Guidelines for Protection of Personal Information* (General Provisions) ・ Section 3-6 Prohibition of identification behaviors (related to Article 36, Paragraph 5 and Article 38 of the Act) of the *Guidelines for Protection of Personal Information* (Anonymously processed data)
Appropriately process pseudonymized information and anonymously processed data	Processing, usage	< A more detailed guidelines > ・ Section 2-8 Anonymously processed information (related to Article 2, Paragraph 9 of the Act)) of the *Guidelines for Protection of Personal Information* (General Provisions) ・ Section 3-2 Proper processing of anonymously processed data (related to Article 36, Paragraph 1 of the Act) of the *Guidelines for Protection of Personal Information* (Anonymously processed data)
Correct, suspend use of, etc. held personal data according to the requests from data subjects	Storage	< A more detailed guidelines > ・ Section 3-5-3 Corrections, etc. of retained personal data (related to Article 29 of the Act), Section 3-5-4 Suspension of use, etc. of retained personal data (related to Article 30 of the Act), Section 3-5-5 Explanation of reasons (related to Article 31 of the Act), Section 3-5-6 Procedures for responding to requests, etc. for disclosures, etc. (related to Article 32 of the Act) of the *Guidelines for Protection of Personal Information* (General Provisions)

Implement safety control measures on personal data	Storage	< A more detailed guidelines > ・ Section 3-3-2 Safety control measures (related to Article 20 of the Act), Section 3-3-3 Employee supervision (related to Article 21 of the Act), Section 3-3-4 Contractor supervision (related to Article 22 of the Act) of the *Guidelines for Protection of Personal Information* (General Provisions)
Erase data without delay	Storage	< A more detailed guidelines > ・ Section 3-3-1 Ensuring, etc. the accuracy of data contents (related to Article 19 of the Act)) of the *Guidelines for Protection of Personal Information* (General Provisions)
Manage trade secrets, etc. in a way that ensures confidentiality	Generation, acquisition, transfer/provision	< A more detailed guidelines > (2) Degree of necessary confidentiality management measures, 2. Confidentiality of the *Management Guidelines for Trade Secrets*
Ensure confidentiality for sharing trade secrets to internal or external parties	Transfer, provision	< A more detailed guidelines > ・ (4) The confidentiality philosophy of sharing trade secrets internally and externally, 2. Confidentiality of the *Management Guidelines for Trade Secrets*
Separately manage secrets, etc. of other companies	Storage	< A more detailed guidelines > ・ (4) The confidentiality philosophy of sharing trade secrets internally and externally, 2. Confidentiality of the *Management Guidelines for Trade Secrets*)
Verify the location of facilities such as servers that process and store data	Storage	-