Smart City Security Guideline

(Ver 1.0)

October, 2020

Ministry of Internal Affiars and Communications, Japan

目次

1. Background and purpose of the guideline 3

1.1. Background 3

1.2. Purpose 3

1.3. Scope 4

1.4. Assumed reader 4

1.5. Overall configuration 5

1.6. How to use 6

2. Concept of Smart City security 7

2.1. Smart City Reference Architecture 7

2.2. Consideration approach for Smart City security 13

2.3. Security concept in each category (overview) 15

3. Security in each category 18

3.1. Governance 18

3.2. Service 21

3.3. City OS 25

3.4. Asset 30

4. Security considerations specific to Smart Cities 34

4.1. Security considerations and security measures 34

4.1.1. Cooperation among multi-stakeholders 34

4.1.2. Ensuring the reliability of data and services 36

4.2. Possible risks and examples of security measures 38

5. Example of security requirements 47

5.1. List of security measures 47

5.2. Consistency with domestic and overseas guidelines and standards 50

1. Background and purpose of the guideline

1.1. Background

Smart City is an initiative that will, by utilizing advanced technology, solve various problems by improving the efficiency and sophistication of functions and services in cities and regions, and create new value including comfort and convenience. In "Integrated Innovation Strategy 2020" (Cabinet decision on July 17, 2020), Smart City is positioned as a place for the advance realization of Society 5.0, and efforts for Smart City will be promoted under cooperation among related ministries and agencies.

On the other hand, since smart cities have a large number of IoT devices such as sensors and cameras, and it is expected that various data will be distributed, there is always a risk of cyber attacks. For example, since various data are distributed on a common platform, it is also required to ensure the authenticity of the data and to build a mechanism for appropriate data flow management. Furthermore, since various actors are involved in the system construction and operation of smart cities, it is necessary to foster a certain level of common understanding among the parties concerned regarding the security of a smart city as a whole.

In Japan, many research studies have been conducted on security in general IoT systems, and guidelines have been created. On the other hand, research specialized in Smart City security is not sufficient, and at present, common guidelines have not been created.

Therefore, the concept of smart city security and specific security considerations with regard to Smart Cities are described in this guideline, considering discussions in a working group consisting of academics, local government experts, Smart Cities experts, and experts from ICT companies involved in security, in order to realize a safe and secure Smart Cities in various regions and local public organizations.

It is expected that this guideline will serve as a reference for all parties involved in Smart Cities to consider and discuss the ideal form of smart city security.

1.2. Purpose

Smart Cities are characterized by the complex cooperation of various actors and the distribution of various data. Therefore, this guideline describes the concept of security that each entity should implement and consider, and also describes the problems that may occur and the measures to realize safe and secure Smart Cities, and it will contribute to and promote the spread of Smart Cities.

Specifically, it is expected that the following effects will be realized in the cooperation of each entity through this guideline.

- Ensuring the security, safety, reliability and resilience of smart cities by implementing security measures with reference to this guideline.[1]
- Examination and implementation of security measures through smooth cooperation by fostering a common understanding of security among each entity.

1.3. Scope

This guideline is based on the Smart City Reference Architecture (hereinafter referred to as "the Reference Architecture") defined in the Cabinet Office's Strategic Innovation Creation Program (SIP). In addition, as this guideline describes security not only in technology aspects but also in management aspects, the security of a Smart City as a whole can be taken into consideration.

The ideas, problems, and examples of measures described in this guideline are items that are particularly recommended to be examined and implemented when constructing and operating a smart city, but they are not exhaustive. Therefore, it is recommended that readers use this guideline as a reference for considering security measures in Smart Cities in which they are involved, and it is also recommended to refer to international standards and guidelines other than this guideline as necessary (Some of the external standards and guidelines are described in "5.2. Correspondence to domestic and foreign guidelines and standards".). In addition, it should be noted that, while Smart Cities are expected to be used in various fields such as transportation and medical care, this guideline describes problems and points to be considered in common in each field.

In addition, although various examples of security measures are described in this guideline, it is recommended that who should implement the measures should be considered for each individual Smart City, as it depends largely on the service and business form of the Smart City.

1.4. Assumed reader

The target readers assumed by this guideline are shown below.

1. Service owner/primary promoter (local public organizations, businesses, etc.) that controls the entire Smart City

[1] "Safety and security" in this guideline is a concept that realizes trustworthiness including "safety", "security" and "reliability", and it also means that the safety, security and reliability of the smart city life cycle are ensured. In addition, in NIST "CPS Framework", "resilience" is an element of credibility along with "security", "safety", "reliability", etc..

2. Businesses and users involved in Smart City business
   - System providers for cloud infrastructure, City OS, etc.
   - Device manufacturers such as IoT devices and network devices, etc.
   - Service providers for software, applications, etc.
   - Data providers such as sensor data and field data, etc.

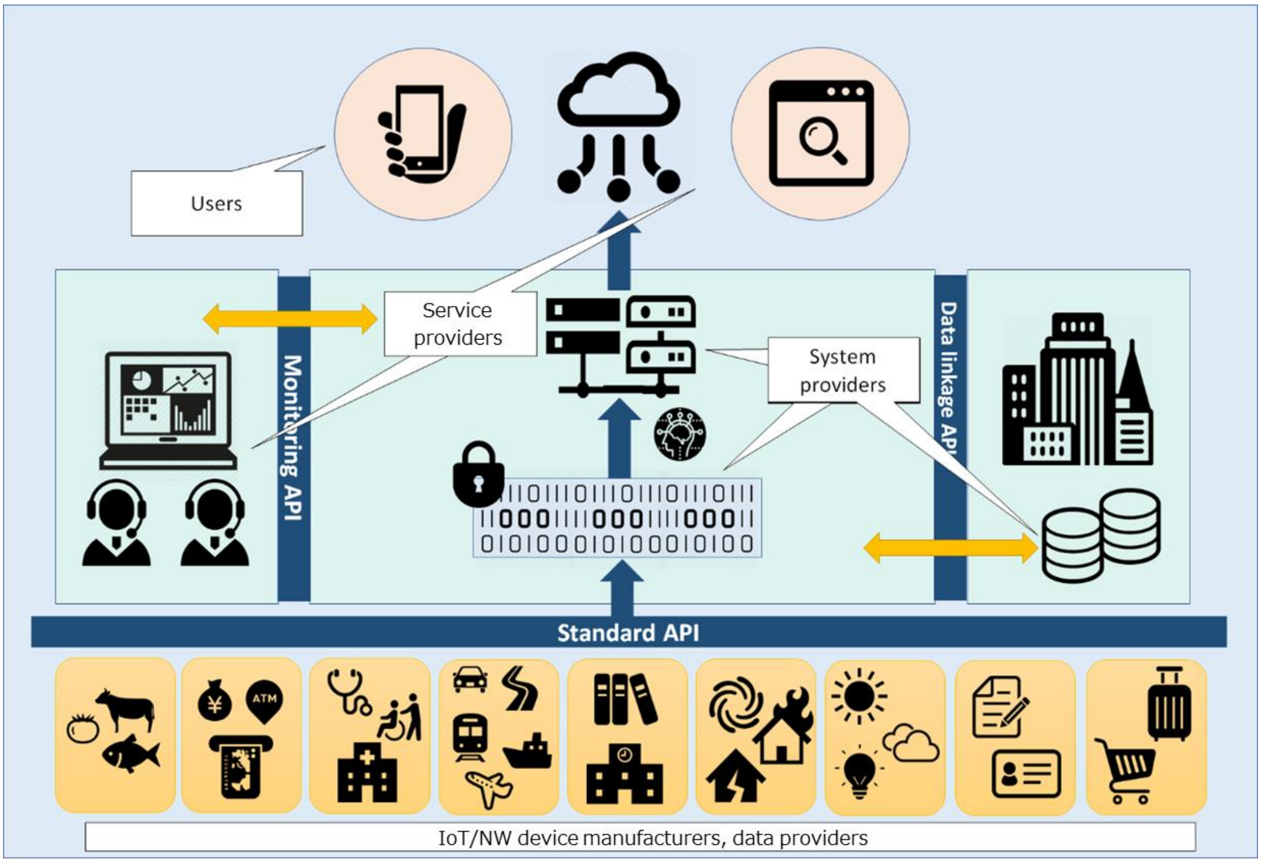


Figure 1 Image of assumed reader

1.5. Overall configuration

This guideline consists of 5 chapters: "1. Background and purpose of the guideline", "2. Concept of Smart City security", "3. Security in each category", "4. Specific security considerations in Smart City", "5. Security requirements and examples of measures".

- Chapter 1 describes the background, purpose, scope, overall structure, etc. of this guideline.

- Chapter 2 explains the Reference Architecture that realizes Smart City framework and the concept of Smart City security in a corresponding manner.

- Chapter 3 describes the security measures required in each category which is classified based on the concept shown in Chapter 2.

- Chapter 4 summarizes the viewpoint of security points specific to Smart Cities to be considered apart from the security in each category, and exemplifies the problems that may occur and measures to addres them.
- Chapter 5 describes use cases and examples of measures for each field based on the contents of Chapters 3 and 4.

1.6. How to use

The way how to use this guideline is shown below.

1. In Chapter 1, understand the background, purpose, scope, etc. of this guideline.
2. In Chapter 2, understand the concept of Smart City security.
3. In Chapter 3, understand the security measures that should be concretely implemented based on the concept of Chapter 2.
4. In Chapter 4, understand security considerations, risks, and measures based on the characteristics of Smart Cities.
5. After conducting a risk analysis based on the fields and characteristics of the Smart City which you promote, select security measures by referring to the security measures examples in Chapter 5.

2. Concept of Smart City security

2.1. Smart City Reference Architecture

This guideline is made for each entity involved in Smart Cities, such as the entity promoting Smart Cities, to consider security measures in IoT devices, infrastructure for data utilization, services, data distribution, etc.

Smart City is a currently developing concept and initiative, and the frameworks that each stakeholder has in mind may differ among Smart Cities. Therefore, in considering the security of Smart Cities, this guideline is based on the framework of the Reference Architecture defined by the Cabinet Office.

In addition, based on the Reference Architecture, this guideline focuses on security measures at the planning, design/development, and operation phases, which are particularly important in the system life cycle.

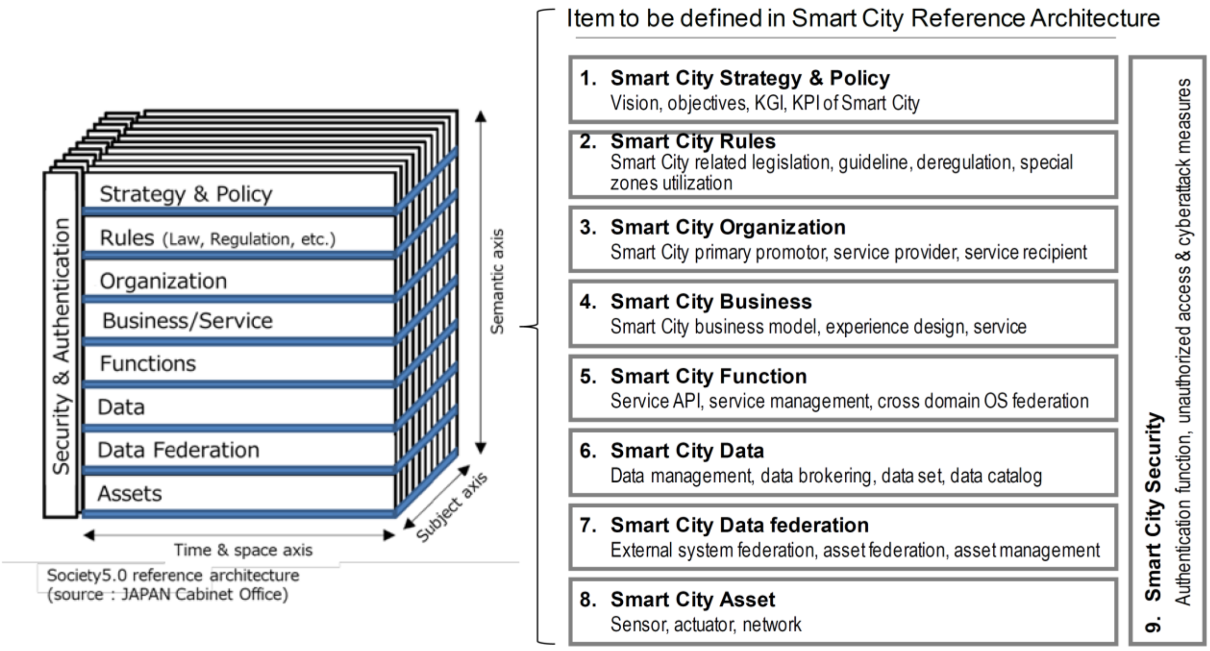

Security & Authentication
Strategy & Policy
Rules (Law, Regulation, etc.)
Organization
Business/Service
Functions
Data
Data Federation
Assets
Semantic axis
Subject axis
Time & space axis
Society5.0 reference architecture
(source : JAPAN Cabinet Office)
Item to be defined in Smart City Reference Architecture
1. Smart City Strategy & Policy
Vision, objectives, KGI, KPI of Smart City
2. Smart City Rules
Smart City related legislation, guideline, deregulation, special zones utilization
3. Smart City Organization
Smart City primary promotor, service provider, service recipient
4. Smart City Business
Smart City business model, experience design, service
5. Smart City Function
Service API, service management, cross domain OS federation
6. Smart City Data
Data management, data brokering, data set, data catalog
7. Smart City Data federation
External system federation, asset federation, asset management
8. Smart City Asset
Sensor, actuator, network
9. Smart City Security
Authentication function, unauthorized access & cyberattack measures

Figure 2-1 Items to be defined in Smart City Reference Architecture

The definitions of each layer in the Reference Architecture described in the "Smart City Reference Architecture White Paper" published by the Cabinet Office are shown below.

1. Smart City Strategy

Smart City Strategy describes the roadmap of how each region achieves its goals and the framework of formulating strategy is presented in Reference Architecture. By way of this framework, Smart City goals based on the regional issues are organized hierarchically and it leads to the implementation of the measures and provision of services.

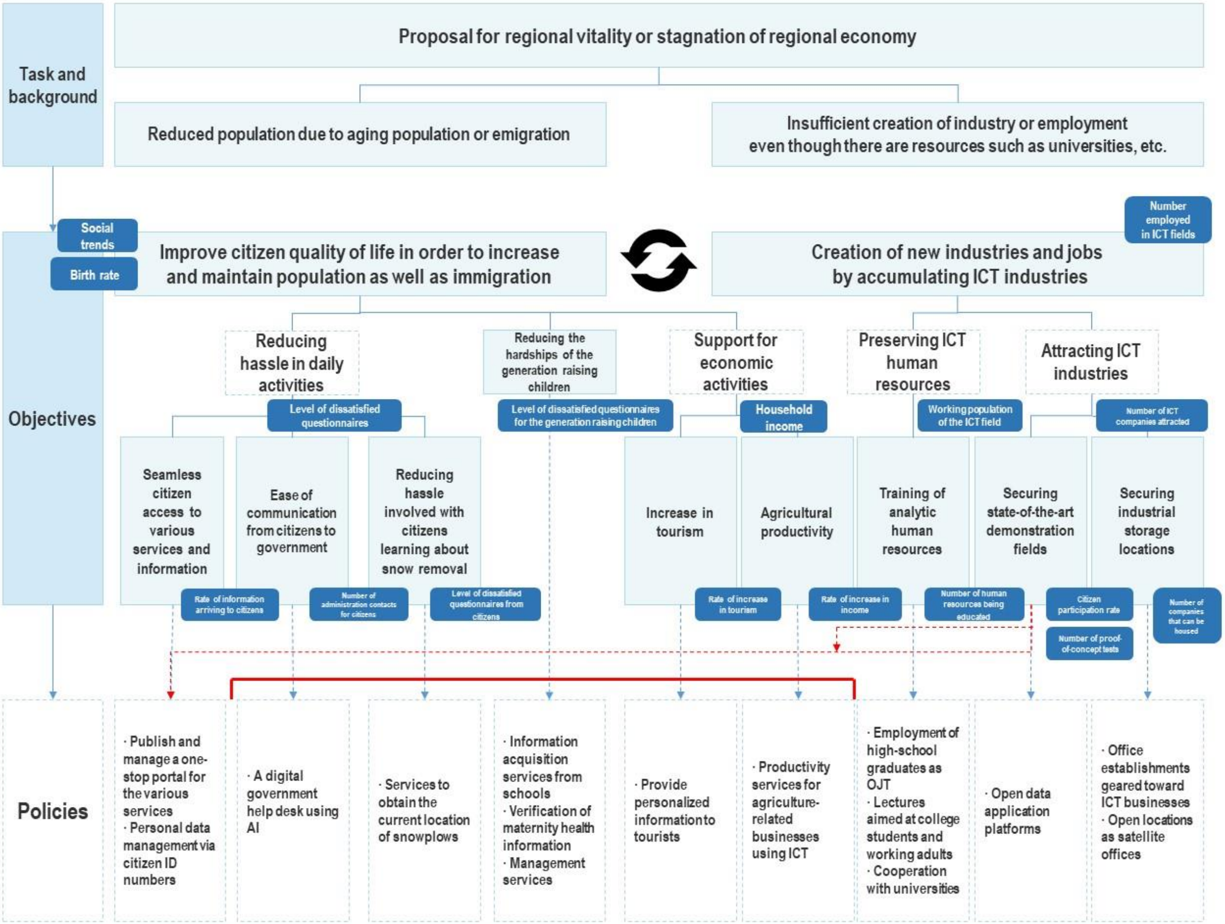
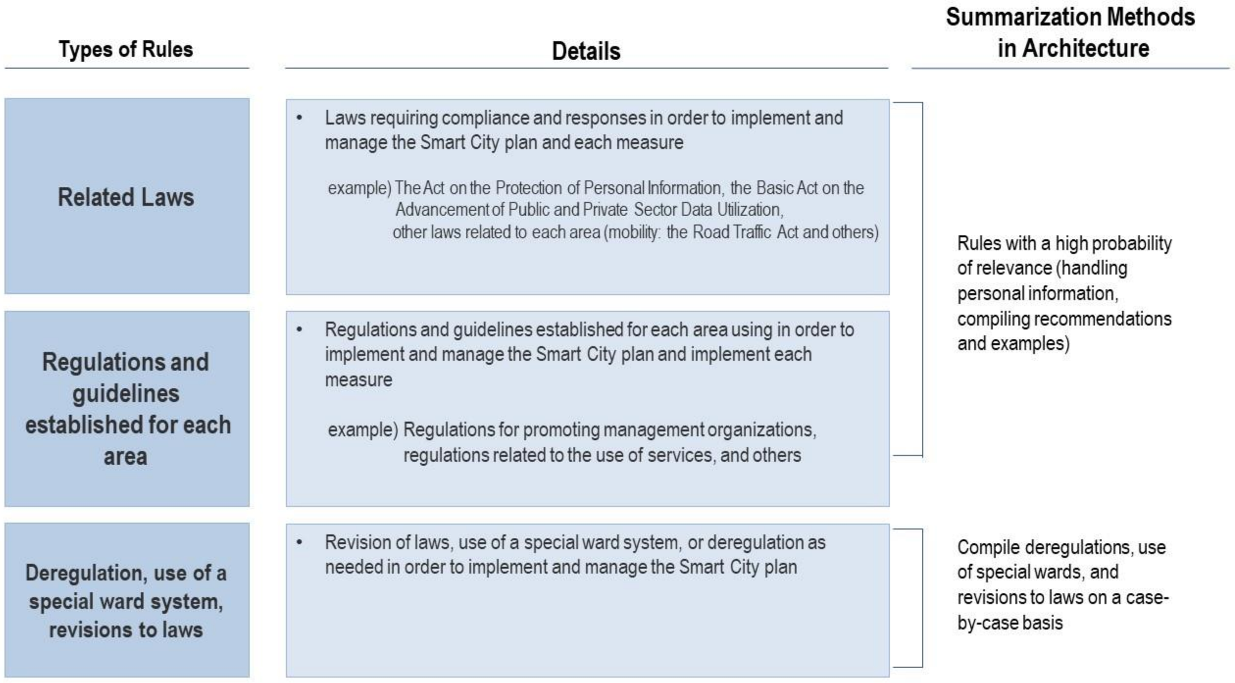

Task and background
Proposal for regional vitality or stagnation of regional economy
Reduced population due to aging population or emigration
Insufficient creation of industry or employment even though there are resources such as universities, etc.
Objectives
Social trends
Birth rate
Improve citizen quality of life in order to increase and maintain population as well as immigration
Creation of new industries and jobs by accumulating ICT industries
Number employed in ICT fields
Reducing hassle in daily activities
Reducing the hardships of the generation raising children
Support for economic activities
Preserving ICT human resources
Attracting ICT industries
Level of dissatisfied questionnaires
Level of dissatisfied questionnaires for the generation raising children
Household income
Working population of the ICT field
Number of ICT companies attracted
Seamless citizen access to various services and information
Ease of communication from citizens to government
Reducing hassle involved with citizens learning about snow removal
Increase in tourism
Agricultural productivity
Training of analytic human resources
Securing state-of-the-art demonstration fields
Securing industrial storage locations
Rate of information arriving to citizens
Number of administration contacts for citizens
Level of dissatisfied questionnaires from citizens
Rate of increase in tourism
Rate of increase in income
Number of human resources being educated
Citizen participation rate
Number of proof-of-concept tests
Number of companies that can be housed
Policies
· Publish and manage a one-stop portal for the various services
· Personal data management via citizen ID numbers
· A digital government help desk using AI
· Services to obtain the current location of snowplows
· Information acquisition services from schools
· Verification of maternity health information
· Management services
· Provide personalized information to tourists
· Productivity services for agriculture-related businesses using ICT
· Employment of high-school graduates as OJT
· Lectures aimed at college students and working adults
· Cooperation with universities
· Open data application platforms
· Office establishments geared toward ICT businesses
· Open locations as satellite offices

Figure 2-2 Image of Smart City Strategy

2. Smart City Rules

In implementing and operating Smart City plans and providing various measures and services, it is important to formulate and operate appropriate rules for the operation of Smart City organizations and the provision of services in each region. In Smart City plans, "relevant laws and regulations", "codes and guidelines set by each region" and "utilizations of deregulation and special zones system, and revision of the laws" are defined as components of the rules.



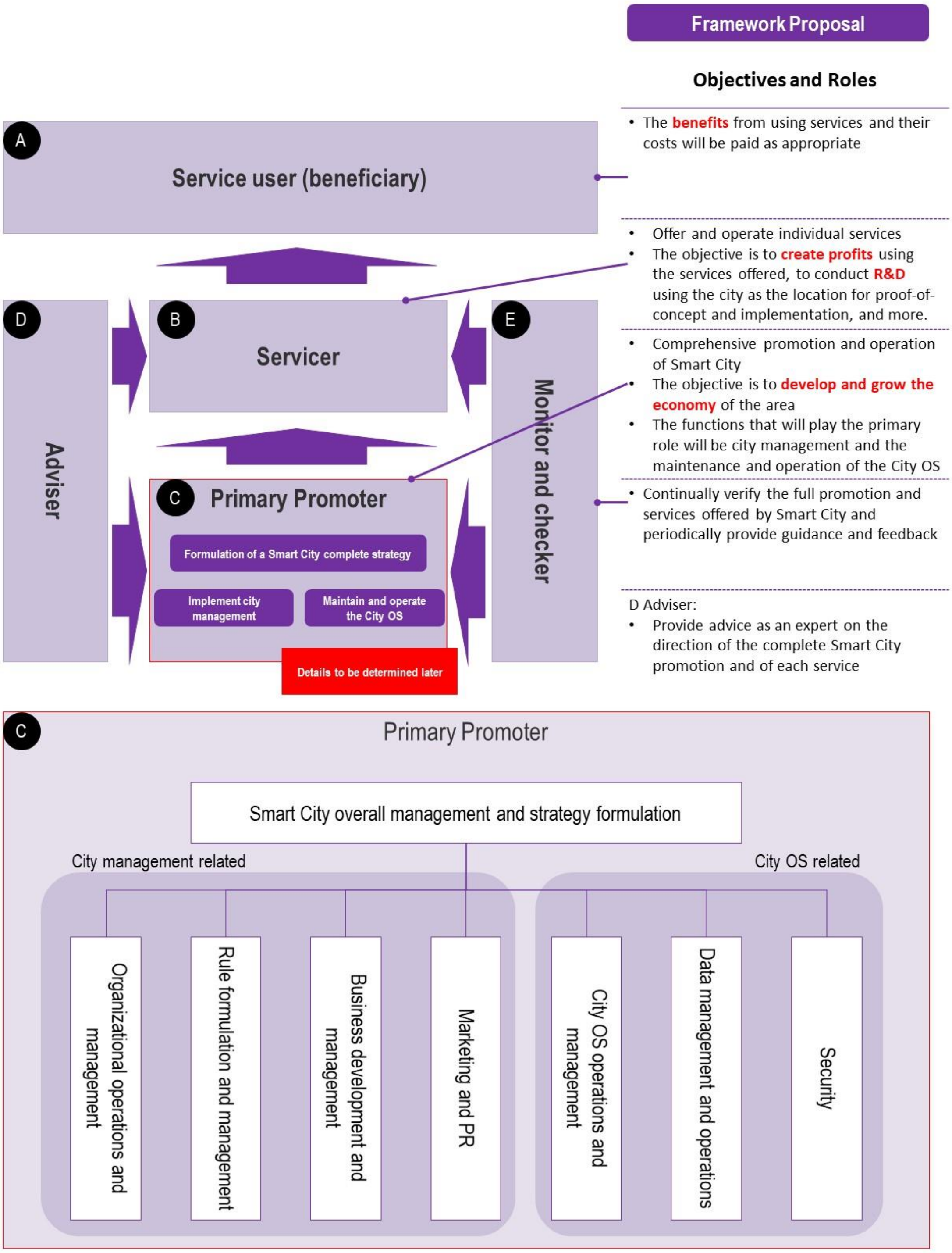
Types of Rules	Details	Summarization Methods in Architecture
Related Laws	• Laws requiring compliance and responses in order to implement and manage the Smart City plan and each measure example) The Act on the Protection of Personal Information, the Basic Act on the Advancement of Public and Private Sector Data Utilization, other laws related to each area (mobility: the Road Traffic Act and others)	Rules with a high probability of relevance (handling personal information, compiling recommendations and examples)
Regulations and guidelines established for each area	• Regulations and guidelines established for each area using in order to implement and manage the Smart City plan and implement each measure example) Regulations for promoting management organizations, regulations related to the use of services, and others	
Deregulation, use of a special ward system, revisions to laws	• Revision of laws, use of a special ward system, or deregulation as needed in order to implement and manage the Smart City plan	Compile deregulations, use of special wards, and revisions to laws on a case-by-case basis

Figure 2-3 Image of Smart City Rules

3. Smart City Organization

Smart City Organization is composed of “primary promoter” who is expected to have primary responsibility, decision-making authority, leadership, etc. for the promotion and operation of Smart City as a whole, and various players (stakeholders such as “service provider” who provides Smart City service[2]), who are in charge of efficient promotion and operation of Smart City. The detail of stakeholders and its relationship is shown in fig.2-4. In this guideline, among the stakeholders in the table, the entity that promotes and operates Smart Cities excluding service users (beneficiaries) is called "multi-stakeholder".

[2] “Smart City service” is defined as the service which is provided to users in cooperation with data and other services through City OS.


A
Service user (beneficiary)
D
Adviser
B
Servicer
E
Monitor and checker
C
Primary Promoter
Formulation of a Smart City complete strategy
Implement city management
Maintain and operate the City OS
Details to be determined later
C
Primary Promoter
Smart City overall management and strategy formulation
City management related
City OS related
Organizational operations and management
Rule formulation and management
Business development and management
Marketing and PR
City OS operations and management
Data management and operations
Security

Framework Proposal

Objectives and Roles

- The **benefits** from using services and their costs will be paid as appropriate

- Offer and operate individual services
- The objective is to **create profits** using the services offered, to conduct **R&D** using the city as the location for proof-of-concept and implementation, and more.

- Comprehensive promotion and operation of Smart City
- The objective is to **develop and grow the economy** of the area
- The functions that will play the primary role will be city management and the maintenance and operation of the City OS

- Continually verify the full promotion and services offered by Smart City and periodically provide guidance and feedback

D Adviser:

- Provide advice as an expert on the direction of the complete Smart City promotion and of each service

Figure 2-4 Image of Smart City Organization

4. Smart City Business

Smart City Business is composed of "business model" which enables structural understanding of the interaction for the provision of goods, services, etc. and the payment of money or other consideration, "experience design" which provides the services designed to meet the needs of users and "service" which is defined as what is provided to users by federating and/or integrating data and other services via City OS. The general example of "service" is websites or applications.

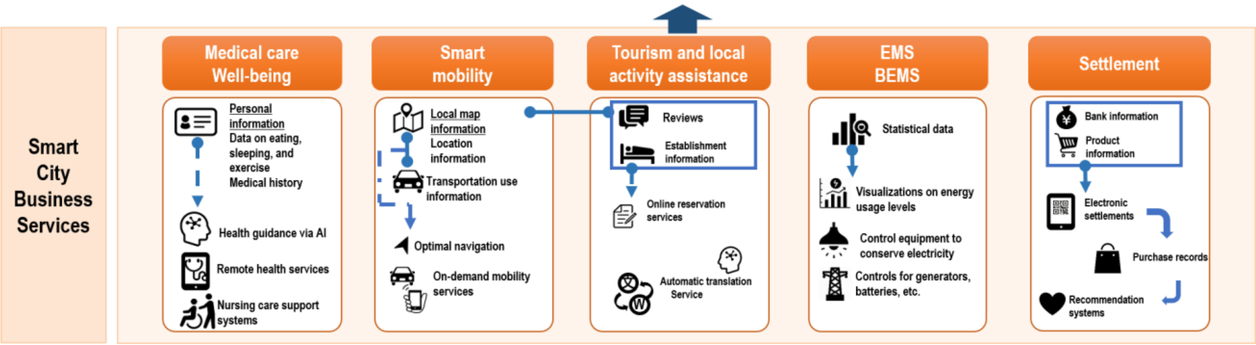

Smart City Business Services
Medical care Well-being
Personal information
Data on eating, sleeping, and exercise
Medical history
Health guidance via AI
Remote health services
Nursing care support systems
Smart mobility
Local map information
Location information
Transportation use information
Optimal navigation
On-demand mobility services
Tourism and local activity assistance
Reviews
Establishment information
Online reservation services
Automatic translation Service
EMS BEMS
Statistical data
Visualizations on energy usage levels
Control equipment to conserve electricity
Controls for generators, batteries, etc.
Settlement
Bank information
Product information
Electronic settlements
Purchase records
Recommendation systems

Figure 2-5 Image of Smart City Business

5. Smart City Function

Smart City Function is composed of "service federations" to federate various Smart City services, which operate on City OS, to City OS and other Smart City services, "authentication" to provide appropriate authentication methods for users of City OS, applications and other systems which are federated with City OS, and "service management" to manage and appropriately operate Smart City services federated with City OS.

6. Smart City Data

Smart City Data contains "data management" to enable management of data stored and accumulated on City OS, and brokering of data distributed across standalone cities, multi-cities, and other systems.

7. Smart City Data Federation

Smart City Data Federation consists of "asset management"to manage data collection, and registration, deletion, etc. of Smart City assets and other systems to be connected, and execute control over Smart City assets, and "external data federation" to manage the interface between City OS and Smart City assets as well as other systems, and absorb the mismatch in data models and protocols.

* The three layers of Smart City Function, Smart City Data, and Smart City Data Federation are collectively called "City OS". It is the core of the system for the implementation and operation of Smart Cities, and integrates the functions commonly used by the regions trying to utilize Smart Cities. In other words, the City OS is an IT system that makes it easy to introduce services in various fields implemented as Smart Cities.

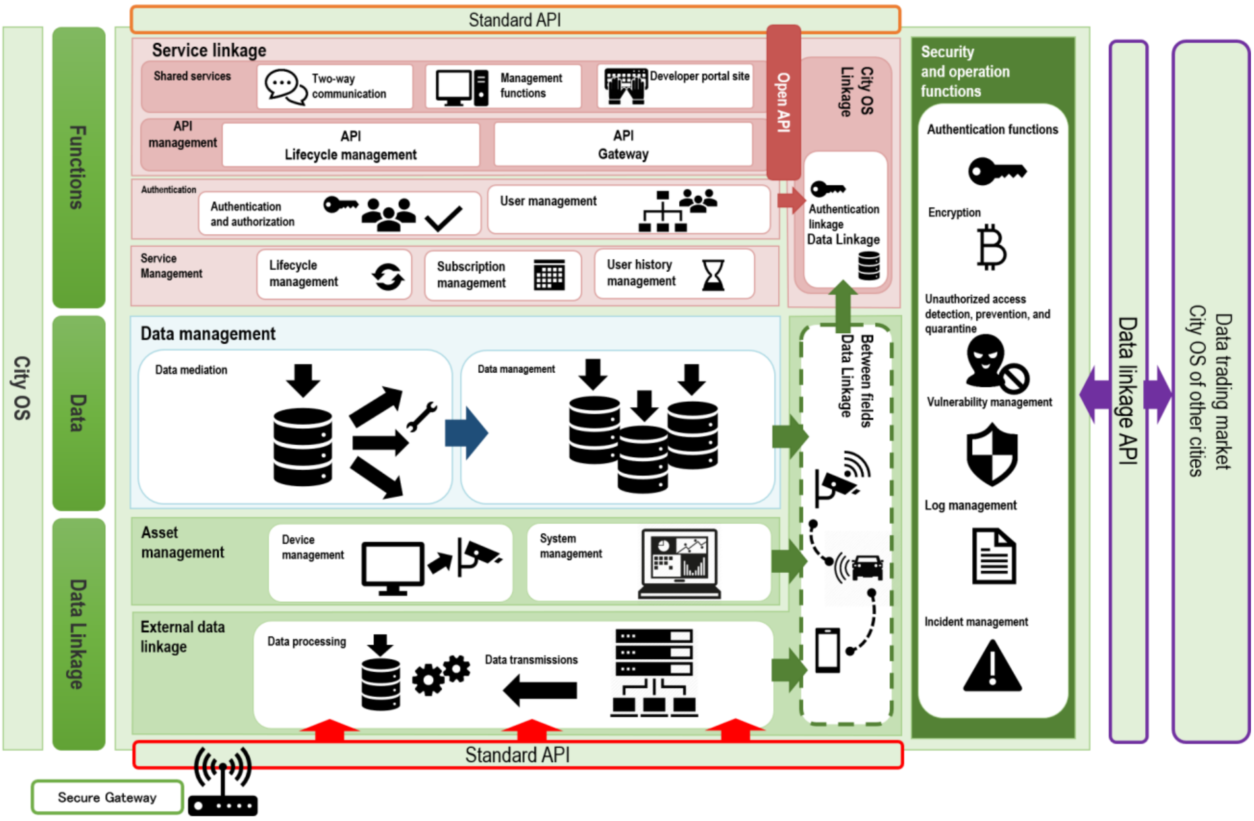


Figure 2-6 Image of City OS

8. Smart City Asset

Smart City Asset is mainly properties and resources associated with the city which could be converted into data and controlled via City OS.

Smart City asset is designed to generate data required to resolve issues and consists of the devices to convert properties and resources into data, and network and transmitters to federate them to City OS.

There are various types of the generated data such as environmental data like river and tidal water levels generated by sensor debvices such as various IoT sensors placed across the region, operation status data of public transportation, and so on.

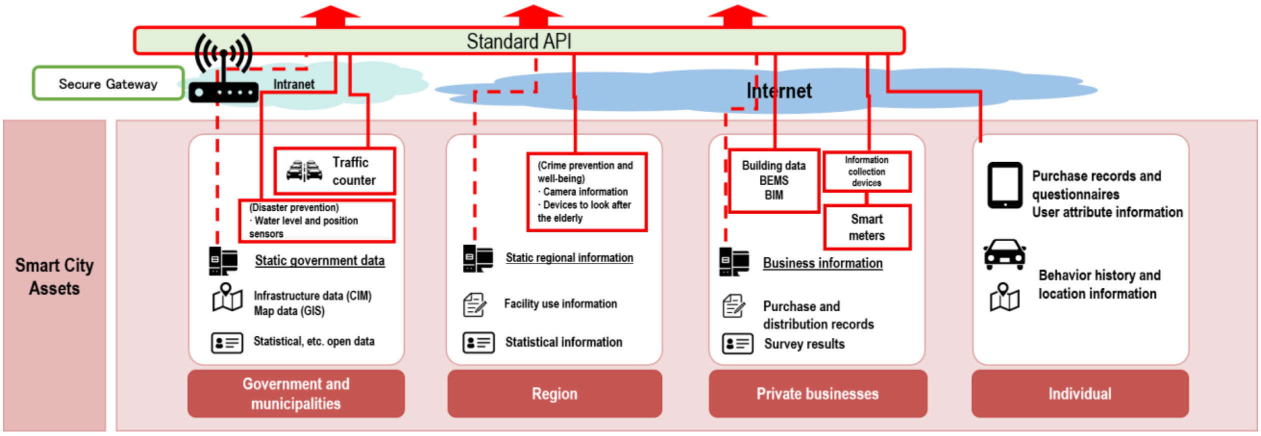

Standard API
Secure Gateway
Intranet
Internet
Smart City Assets
Traffic counter
(Disaster prevention)
· Water level and position sensors
Static government data
Infrastructure data (CIM)
Map data (GIS)
Statistical, etc. open data
Government and municipalities
(Crime prevention and well-being)
· Camera information
· Devices to look after the elderly
Static regional information
Facility use information
Statistical information
Region
Building data
BEMS
BIM
Information collection devices
Smart meters
Business information
Purchase and distribution records
Survey results
Private businesses
Purchase records and questionnaires
User attribute information
Behavior history and location information
Individual

Figure 2-7 Image of Smart City Asset

2.2. Consideration approach for Smart City security

In this guideline, as an approach to examine the security of Smart Cities, the eight layers defined in the Reference Architecture are rearranged into categories that have common threats, risks and security measures. That is, as shown in Fig. 2-8, the eight layers are classified into four categories: "Governance," "Service," "City OS," and "Asset". After that, the points and examples of security measures in each category are summarized.

From another point of view, these four categories can be classified into two aspects, a management aspect and a technical aspect. By considering security from both approaches, it is possible to ensure whole Smart City security.

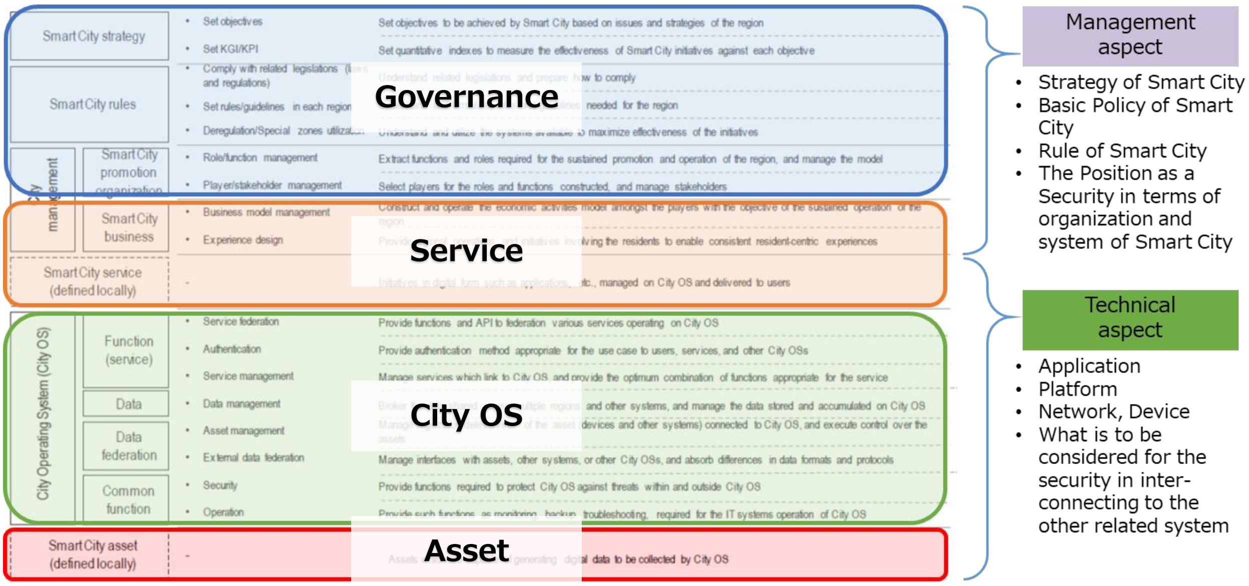

Governance
Service
City OS
Asset
Smart City strategy
Smart City rules
City management
Smart City promotion organization
Smart City business
Smart City service (defined locally)
City Operating System (City OS)
Function (service)
Data
Data federation
Common function
Smart City asset (defined locally)
Set objectives
Set KGI/KPI
Comply with related legislations and regulations
Set rules/guidelines in each region
Deregulation/Special zones utilization
Role/function management
Player/stakeholder management
Business model management
Experience design
Service federation
Authentication
Service management
Data management
Asset management
External data federation
Security
Operation
Set objectives to be achieved by Smart City based on issues and strategies of the region
Set quantitative indexes to measure the effectiveness of Smart City initiatives against each objective
Extract functions and roles required for the sustained promotion and operation of the region, and manage the model
Select players for the roles and functions constructed, and manage stakeholders
Provide functions and API to federation various services operating on City OS
Provide authentication method appropriate for the use case to users, services, and other City OSs
Manage interfaces with assets, other systems, or other City OSs, and absorb differences in data formats and protocols
Provide functions required to protect City OS against threats within and outside City OS
Management aspect
Strategy of Smart City
Basic Policy of Smart City
Rule of Smart City
The Position as a Security in terms of organization and system of Smart City
Technical aspect
Application
Platform
Network, Device
What is to be considered for the security in inter-connecting to the other related system

Figure 2-8 Categorization based on Smart City Reference Architecture

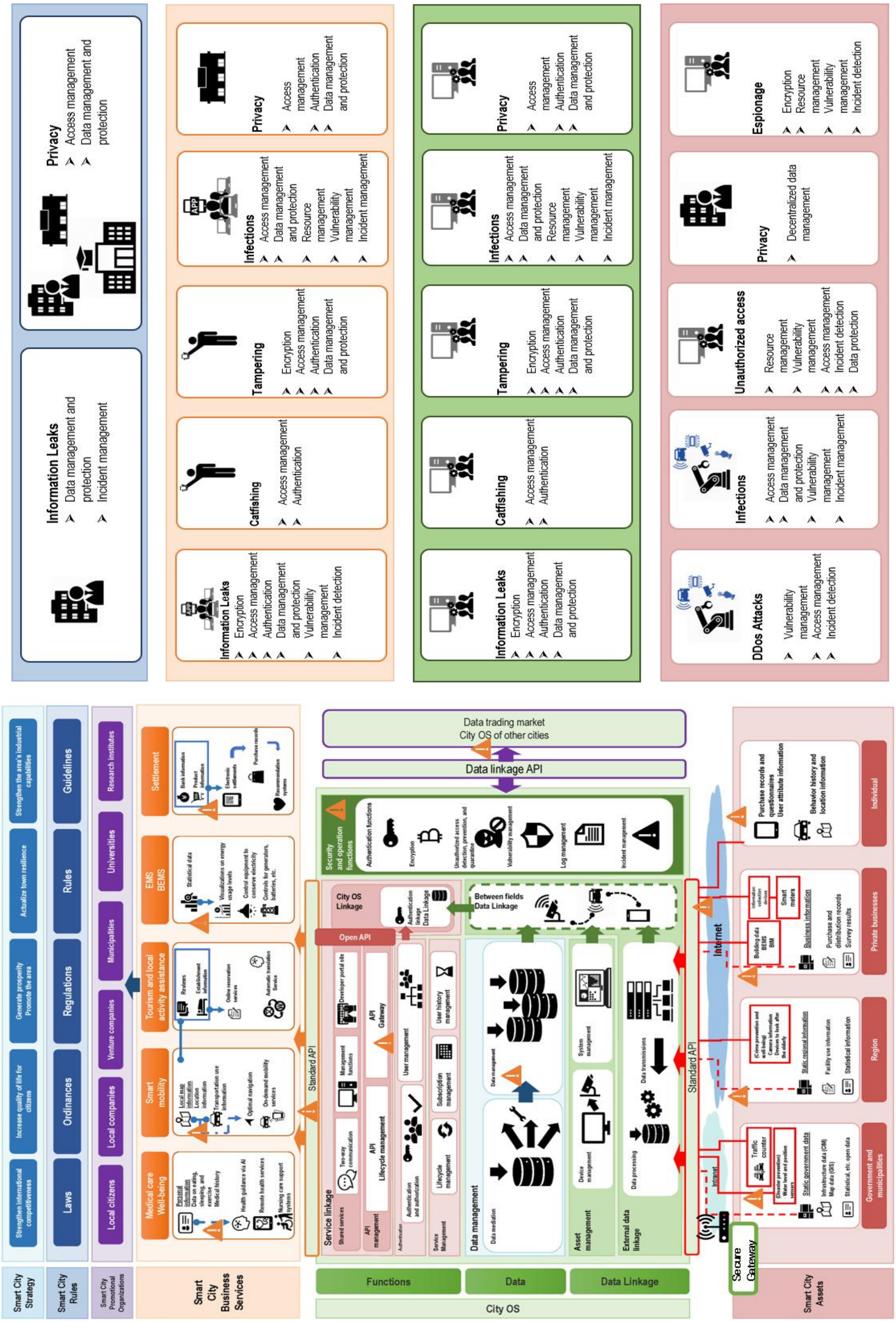


Figure 2-9 assumed threats and examples of security measures in each category

2.3. Security concept in each category (overview)

The basic concepts of security in the four categories are shown below.

Governance

"Governance" is a category where determining how a Smart City should be. It includes determining the direction of efforts and measures for the entire Smart City, creating rules and basic policies for continuing the efforts, and building an organizational structure. The content decided in this category (how to utilize, develop, expand and manage a Smart City in the local community and economy) greatly affects the direction of the content of the other three categories as well as security.

From the perspective of security, it is important to formulate policies such as “what kind of security policy should be formulated for a Smart City as a whole”, “what kind of security standards should be required” and “what kind of organizational structure should be operated”, as a common understanding among multiple stakeholders.

When formulating rules for Smart Cities, it should be noted that the domestic and foreign laws such as "the Personal Information Protection Law", "the Basic Law for Promotion of Public-Private Data Utilization", “the General Data Protection Regulation”, and business laws/guidelines in each field, should be taken into consideration.

In addition, it is desirable to discuss the business continuity plan (BCP) for continuing a Smart City as a service among multi-stakeholders and define the basic policy, roles, and the procedure for incident responses.

Service

"Service" is a category that incorporates the direction determined in the "Governance" category into services, and services and business models of a Smart City are defined in this category. From the viewpoint of security, it is important to identify the functions and assets (facilities and data) which should be protected based on the defined services. In addition, since the relationship between multi-stakeholders becomes clear by the definition of business model, it is important to determine the demarcation point of responsibility regarding security based on its model. For "City OS" and "Assets", it is required to consider and implement appropriate security measures in consideration of the contents determined in this category.

In addition, services may be provided to users through websites or applications in some cases. In those cases, since such services have contact point with users, it is required to consider and implement security measures of the webisties of applications.

Since it is assumed that business models will gradually change through the operation of a

Smart City, it is necessary to consider security measures according to the changing business model. In addition, when considering application security, it should be noted that balanced proper security should be implemented so that the usability of the application would not be complicated and the convenience of the service would not be significantly impaired.

City OS

"City OS" is a category that categorizes and accumulates information collected from the "Assets" category and plays a role mainly as a platform for providing data to "Service" and other City OSs. Since it is assumed that a City OS will be constructed on cloud infrastructure, general cloud security measures (authentication management, access control, data protection, system and security monitoring, vulnerability management, etc.) are required as the security of the platform.

A City OS has a connection point with external systems such as "Service", "Asset" and other City OSs, and it is assumed that various data flows through a City OS. Therefore, it is also necessary to give considerations to using encryption and secure protocols for external communication from the City OS.

In addition, when adopting IaaS/PaaS provided by a cloud operator as the platform of the City OS, it is recommended to use a cloud service that can guarantee the robustness and availability to meet the service level required in the City OS.

Besides, there are not enough demonstrations and discussions in Japan regarding data federations across fields within a City OS and how data should be managed when federating with other City OSs. Therefore, these issues will be reviewed and reflected in this guideline when it is revised in the future.

Asset

"Asset" is a category that generates data and sends it to "City OS" in order to solve regional issues, which consists of devices, networks, and relay devices. In this category, methods such as how to collect data required for "service" and how to send the data to "City OS" will be examined. Since it is assumed that IoT devices and the handled data will be various depending on provided service, it is difficult to expect common security measures for all assets.

On the other hand, as this category is the source of all Smart City data, integrity is relatively important. Therefore, it is required to detect an abnormality in devices, physically protect them, and encrypt communications when communicating with the outside of “Asset”via the Internet.

From a viewpoint other than integrity, when handling data which contains highly confidential information such as personal information, it is necessary to pay sufficient attention to confidentiality. In addition, in the case of providing services that have a large physical impact, such as actuator control, it is necessary to pay attention to availability from the viewpoint of protecting human life.

3. Security in each category

3.1. Governance

This category includes the efforts of an entire Smart City, the determination of the direction of measures, the formulation of rules and basic policies, and the construction of an organizational structure. In the security context, it is necessary to formulate basic policies on security of the smart city as a whole, create rules for security measures in plain/emergency situation, and build an organization that controls security measures.

<Points>

1. Establish basic policies on security in your organization and supply chain in consideration of risk assessment and data life cycle, define security measure standards, scope of responsibility, risk tolerance level, etc., and share them appropriately among multi-stakeholders.

2. Develope security roles and responsibilities, information management system and information sharing methods in your organization.

3. Develop rules that take into account domestic and international laws and regulations such as the Personal Information Protection Law, the Basic Law for Promotion of Public-Private Data Utilization, and GDPR, as well as business laws and industry guidelines in each field.

4. For the continuous provision of Smart Cities, consider the dependencies, important functions and resilience (recovery) among your own organization and other related organizations.

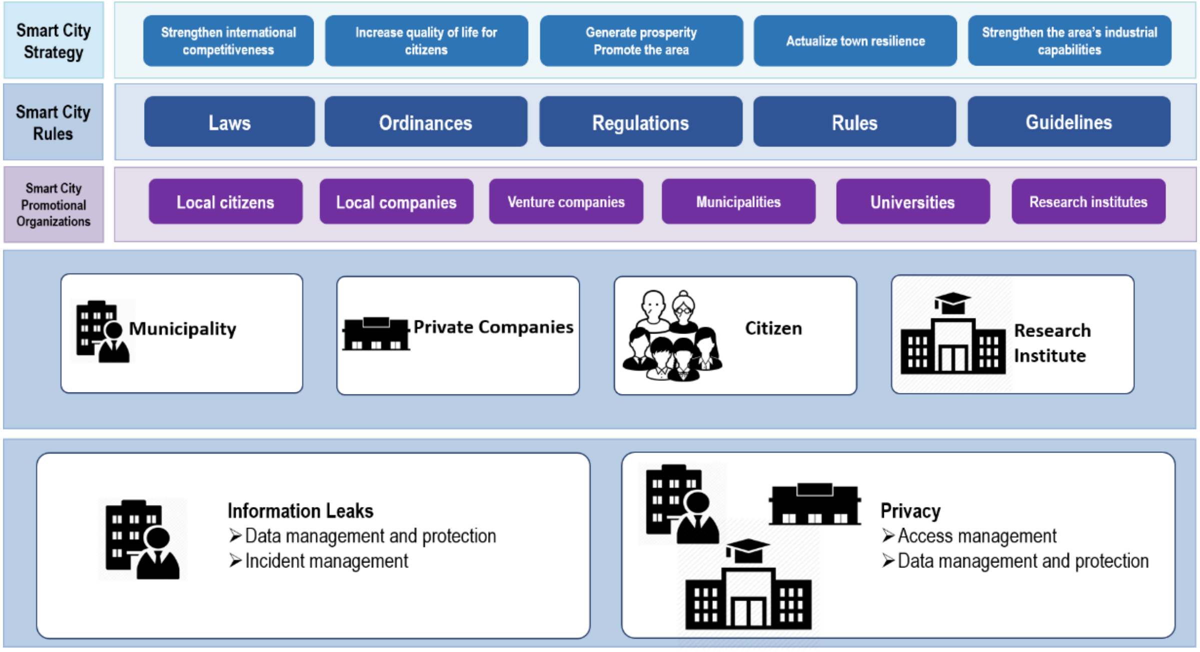


Figure 3-1 Image of Governance

<Examples of measures>

1. Establish basic policies on security in your organization and supply chain in consideration of risk assessment and data life cycle, define security measure standards, scope of responsibility, risk tolerance level, etc., and share them appropriately among multi-stakeholders.

When implementing and operating a Smart City, it is required to evaluate the expected security risks and the effects caused by those risks, and to consider how and what kind of security measures to implement. This series of work is called risk assessment, and it is necessary to work on security measures after clarifying their roles and responsibilities not only in a certain organization but also in various organizations related to the supply chain.

In addition, when considering the content of security measures, it is necessary to develop security policies/standards including the supply chain taking into account of data life cycle of handled data. For example, it is necessary to create a contract document that clarifies the roles and scopes of responsibility for handling information between your organization and the contractor so that both parties have a common understanding, and to identify security risks in a Smart City and to consider necessary measures

2. Develope security roles and responsibilities, information management system and information sharing methods in your organization.

By primarily clarifying the incident response policy of your organization in advance in the system provided in "Service" and "City OS", it is possible to reduce the possibility that the impact of damage in an emergency situation will increase due to the delay of countermeasures.

In addition, since there are many stakeholders and the relationships are complicated in Smart City initiatives, it is necessary for multi-stakeholders to improve management and sharing methods of information and to understand them in common. For example, it is necessary to create a contract document that clarifies the person in charge (such as the appointment of a chief information security officer) and the scope of responsibility for information handling in your own organization and other related organizations.

3. Develop rules that take into account domestic and international laws and regulations such as the Personal Information Protection Law, the Basic Law for Promotion of Public-Private Data Utilization, and GDPR, as well as business laws and industry guidelines in each field.

If only the rules and security measures formulated within the organization are implemented, there is a possibility that the viewpoints that should be considered may be ignored or that security measures may be insufficient. Therefore, it is necessary to formulate the minimum rules and security measures in consideration of domestic and foreign laws, regulations and security guidelines in each field.

The following are examples of laws and guidelines that are recommended to be considered when considering security measures.

- Personal Information Protection Law
- Unfair Competition Prevention Law
- Public-Private Data Utilization Promotion Basic Law
- Cyber/Physical Security Framework
- IoT Security Guidelines
- Information security measures guidelines for cloud service provision
- EU General Data Protection Regulation (GDPR)

4. For the continuous provision of Smart Cities, consider the dependencies, important functions and resilience (recovery) among your own organization and other related organizations.

In operating a smart city, it is important that your own organization and other related organizations will respond appropriately and restore services as soon as possible, when an incident such as a system abnormality, unauthorized access from the outside, or information leakage occurs.

In addition, when performing resilience (recovery), it is possible to take appropriate measures by identifying the importance of the points where an abnormality or failure has occurred and the dependency with other organizations and systems in advance. For example, by organizing the importance and risk of each system, function, device, and handled data which are components of a Smart City, it is possible to suppress misjudgment when an incident occurs and realize prompt incident response and information sharing.

3.2. Service

"Service" is a category that incorporates the direction determined in the "Governance" category into services, and services and business models of a Smart City are defined in this category.

Since the importance and information handled differ depending on the service and business model, it is necessary to identify the functions and information to be protected in the service and take security measures to appropriately protect them.

<Points>

1. Identify the functions and information that should be protected with regard to provided services.

2. Remove vulnerabilities related to service content breach and illegal command input to services at the planning, design, and development phases.

3. Check or monitor illegal commands and requests to applications.

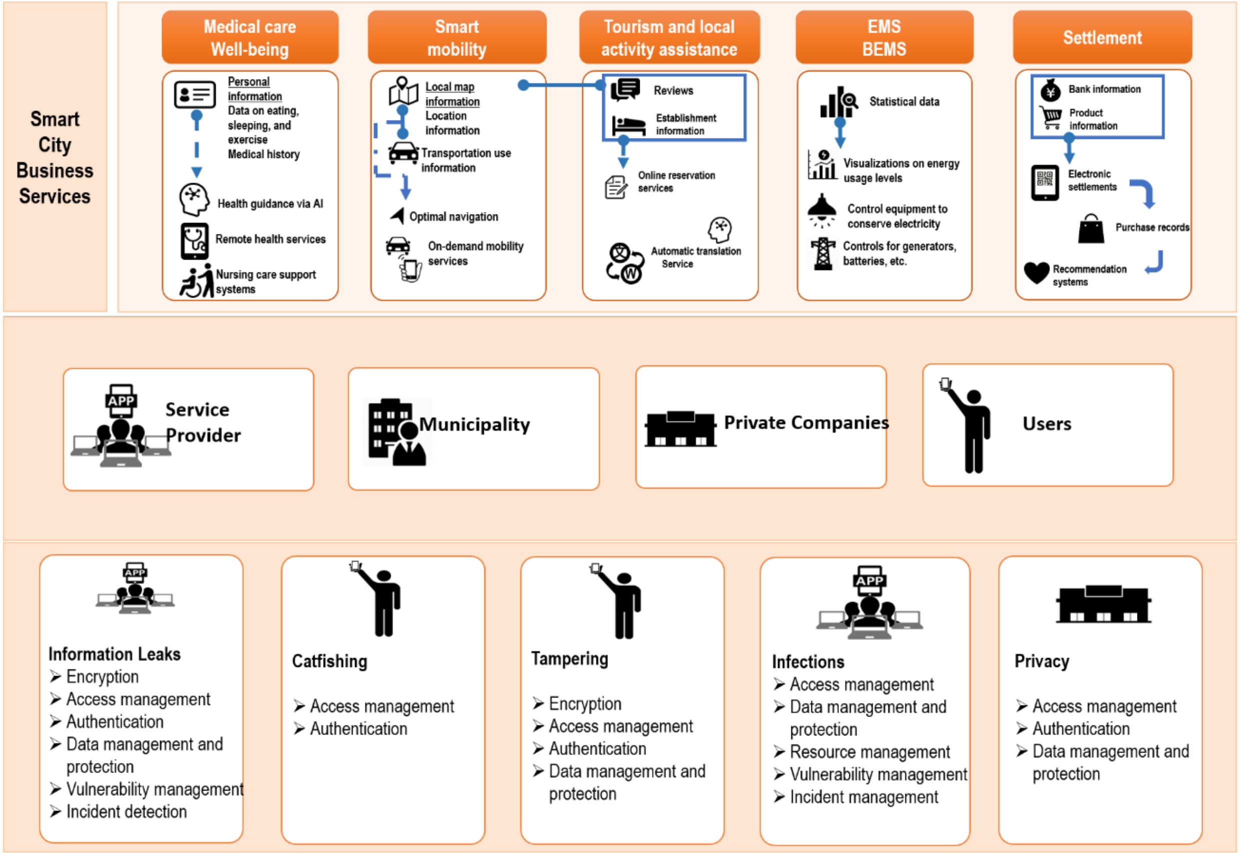


Figure 3-2 Image of Service

<Examination image>

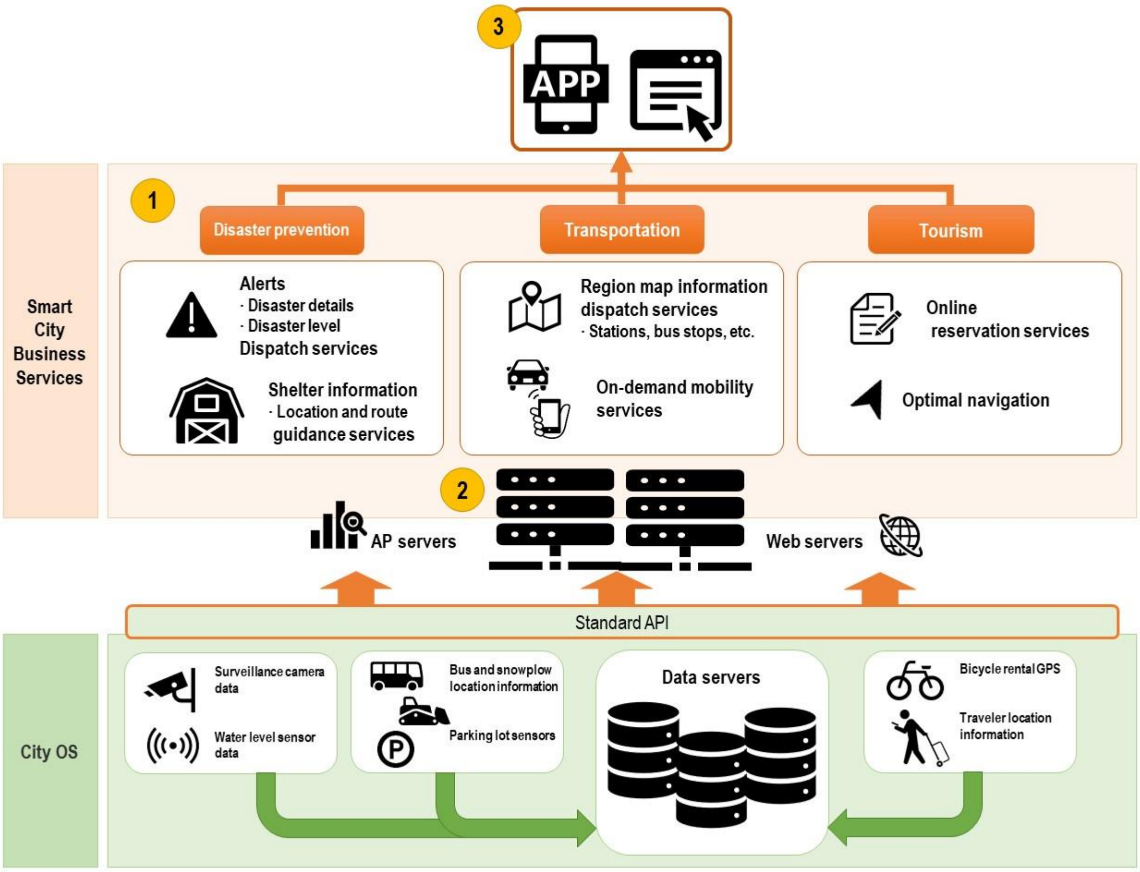


Figure 3-3 Image of security measures in Service

<Examples of measures>

1. Identify the functions and information that should be protected with regard to provided services.

Identify the functions (communication, display, control, etc.) and information (personal information, design information, etc.) provided in the "Service" category. In addition, as security threats other than leakage and falsification of information, there are risks that Smart City services will be used as stepping stones and bots to attack other systems, and that the provided service itself will be illegally controlled.

Table 3-1 Examples of information assets to be protected by embedded systems

Information assets	Description
Contents	Multimedia data such as audio, images, and moving images (copyright management data and private content when using commercial content), content usage history (it is important to protect the content usage history)
User information	User personal information (name / address / phone number / birth date / credit card number, etc.), user authentication information, usage history, etc.
Equipment information	Information on the information appliance itself (model, ID, serial ID, etc.), device authentication information, etc.
Software status	Status data (operation status, network usage status) etc. unique to each software.
Software settings	Setting data (operation setting, network setting, authority setting, version) etc. unique to each software
Software	Operation System, middleware, applications, etc. (sometimes called firmware)
Design data and internal logic	Design information of specifications / design documents generated in the planning / design phase

* This table is created referring to “Embedded System Security Guide” published by IPA (Information-technology Promotion Agency), Japan

2. Remove vulnerabilities related to service content breach and illegal command input to services at the planning, design, and development phases.

(1) Verification and evaluation of safe and secure design

It is required to verify and evaluate the functions and information to be protected in the provision of various applications in "Service" category specified in the previous section according to the level of safety and security measures. For verification and evaluation, it is possible to utilize the requirements in various standards in each industry and objective evaluation such as third-party certification.

(2) Introduction of authentication function

When it is necessary to restrict the use of services by user, it is necessary to authenticate the identity of users before allowing them to access the service. As security measures against illegal access and spoofing, there are authentication methods which use knowledge information (identifier, password), possession information (IC card, client certificate, SMS authentication), or biometric information (finger vein authentication and glow authentication). In order to enhance security, it is desirable to adopt multi-factor authentication that combines multiple factors from those factors. In addition, as measures against spoofing from the connected systems/services, it is important to mutually authenticate the connected systems/services using an encryption key, an electronic certificate and so on.

(3) Initial settings

As a provider of Smart City services, It should be noted for providers of Smart City services to initially set the appropriate configurations such as password setting and management, disable unnecessary services/ports, apply access control, and update software version when installing and connecting.

(4) Encryption

In order to prevent information theft from the outside, the data stored in applications in “Service” category and communication with the outside via the Internet should be encrypted. When applying an encryption, a cryptography and hash algorithm which have appropriate strength defined in "CRYPTREC cipher list (e-government recommended cipher list)" should be adopted.

3. Check or monitor illegal commands and requests to applications.

It is necessary to be able to detect the abnormal state at first when an abnormal operation occurs due to a defect or attack in the application in order to prevent the spread of the effect caused by the abnormal operation. For example, in the case of a service that receives inputs from users, it is necessary to check whether the inputs contain an illegal command that causes unexpected effect on the service.

3.3. City OS

This category is positioned as the core of an entire Smart City system, and “City OS” has a platform function that classifies and stores the information collected by "Assets" and provides data to "Services" or other City OS.

Since a City OS is assumed to utilize cloud infrastructure in general, it is required to implement general cloud security measures from the viewpoint of security of the platform itself. In addition, securing data distribution inside the City OS, protecting the data handled, construction/operation with few faults at the connection point with other categories, and examination and implementation of security measures for data protection are required role in this category.

<Points>

1. Encrypt communications with the outside via the Internet.

2. Implement an appropriate access control on communication from the outside to the City OS.

3. Implement authentication for access by the maintenance operators of a City OS for verifying their identities.

4. In the case of handling critical information such as personal information in City OS, properly manage it by such as storing it with encryption and deleting unnecessary information.

5. Keep the version of server OS, middleware, software, etc. up to date.

6. Monitor system status and detect occurrence of errors in the system.

7. Monitor status of devices and detect occurrence of an abnormality in the devices.

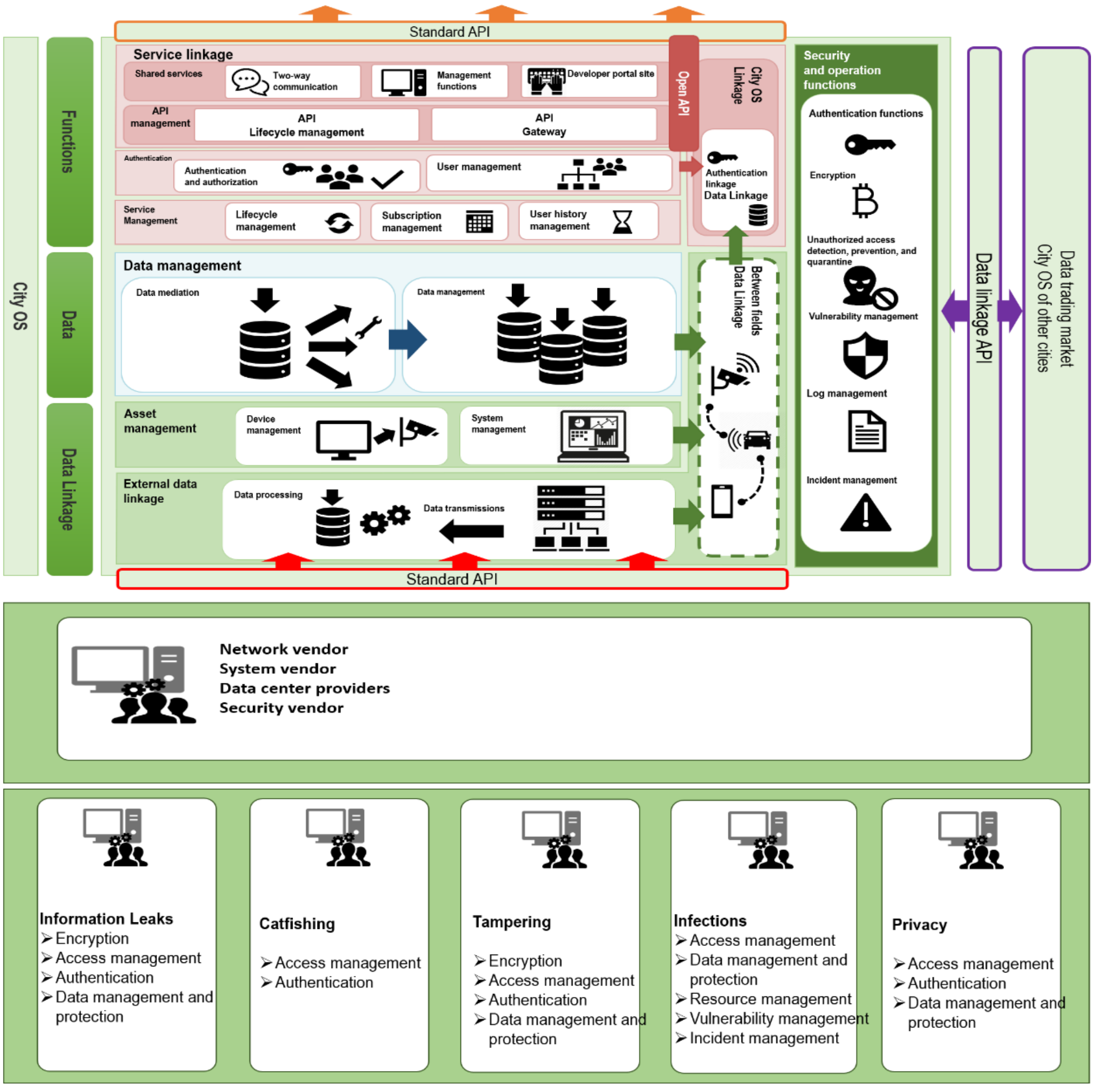


Figure 3-4 Image of City OS

<Examination image>

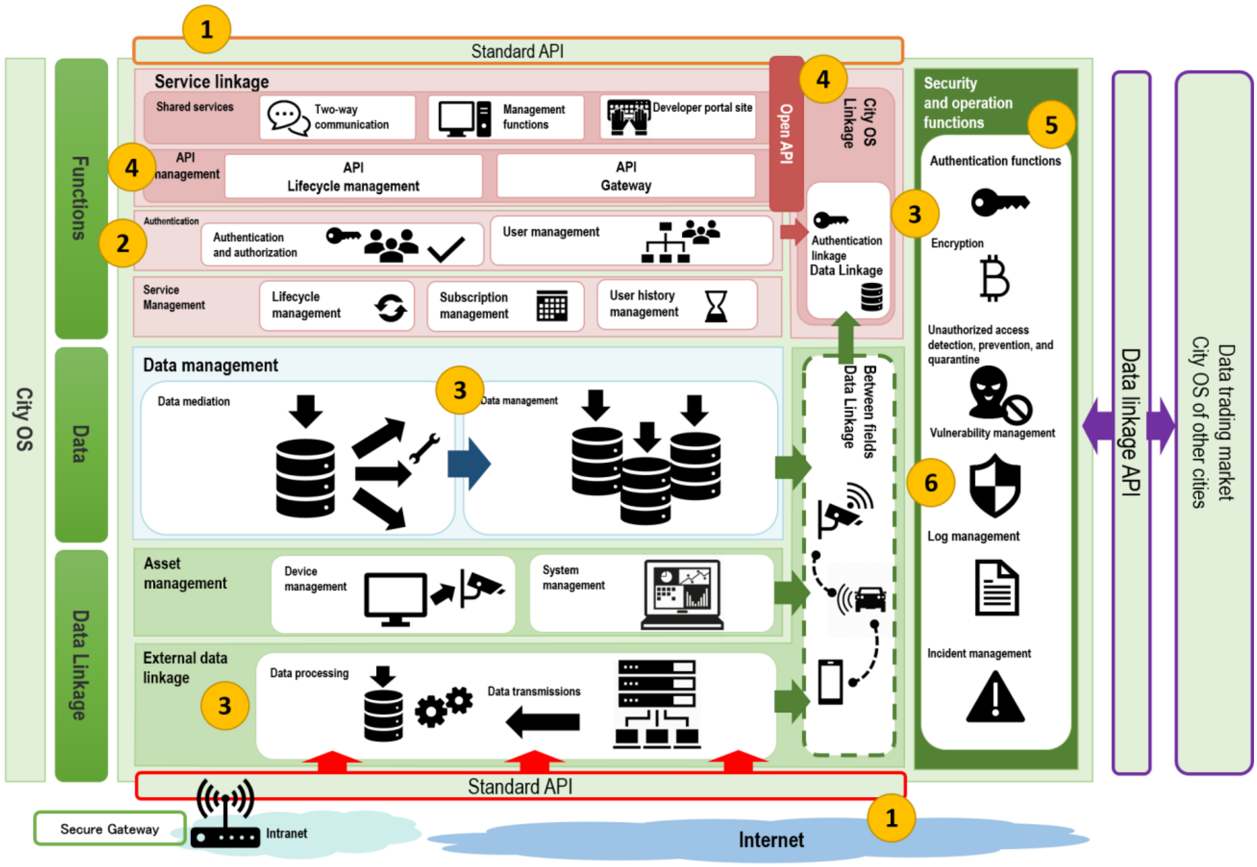


Figure 3-5 Image of security measures in City OS

<Examples of measures>

1. Encrypt communications with the outside via the Internet.

In the case of communication with an external network via the Internet, since there is a possibility that the communication data is sniffed and tampered by third parties, it is necessary to implement data federations by API and encrypt communications with “Services” and “Assets”.

2. Implement an appropriate access control on communication from the outside to a City OS.

In order to prevent unauthorized access to a city OS and cyber attacks that exploit vulnerabilities, it is necessary to implement appropriate access control so that third parties cannot easily access the City OS. For example, it is important to allow only the very minimum access by means of restrictions on communication sources and destinations, disabling the use of unnecessary service/ports, and so on.

3. Implement authentication for access by maintenance operators of a City OS for verifying their identities.

It is required to implement authentication methods to uniquely identify a person who can access a City OS. There are authentication methods which us knowledge information (identifier, password), possession information (IC card, client certificate, SMS authentication), or biometric information (finger vein authentication and glow authentication). In order to enhance security, it is desirable to adopt multi-factor authentication that combines multiple factors from those factors.

4. In the case of handling critical information such as personal information in City OS, properly manage is by such as storing it with encryption and deleting unnecessary information.

In the case of storing information such as personal information, it is basically necessary to limit the people who can access the information and control it appropriately.

However, since the risk of physical theft or illegal access cannot be completely eliminated, it is necessary to encrypt the data when storing such information in a City OS. For encryption, it is recommended to use a secure encryption protocol defined in the "CRYPTREC cipher list (e-government recommended cipher list)" such as AES 128bit or higher and SHA-256bit or higher.

5. Keep the version of server OS, middleware, software, etc. up to date.

Vulnerabilities in server OS, middleware, and software are discovered on a daily basis, and patches that address these vulnerabilities are released by vendors.

In order to protect the system from unauthorized access and attacks that exploit vulnerabilities made by malicious actors, it is necessary to update the server OS, middleware, and software versions as appropriate. In addition, it is necessary to continuously collect vulnerability information distributed by vendors of server OS, middleware, and software, and to apply patches as necessary.

6. Monitor system status and detect occurrence of errors in the system.

It is important to implement functions to detect system abnormalities for preparing not only system failures but also cyber attacks to the system such as unauthorized access, tampering, contamination of malicious program and data destruction.

In order to prevent the expansion of the influence of damages and to recover the system quickly, it is necessary to properly monitor the system according to the importance of the system and the assumed impact of risks when system failure occurs.

- Monitor the status of the system to detect abnormalities such as system errors and unexpected events.
- An operation and management procedure regarding the initial action and the convergence of the situation should be created for an appropriate incident response when an abnormality in the system is detected, and the procedure should be evaluated and reviewed as necessary.

7. Monitor status of devices and detect occurrence of an abnormality in the devices.

In the Reference Architecture, asset management is defined as one of the functions of City OS, and device status monitoring is also one of the roles required in City OS.

When an abnormality occurs in devices such as unauthorized access to the devices, theft, or failure of the devices, it is important that it can be detected therough monitoring of the devices. For that purpose, in order to prevent the expansion of the influence of damages and restore the service promptly, it is necessary to properly monitor devices according to the importance of the assets and the assumed impact of risks when an abnormality occurs in the devices.

- Monitor the status of devices to detect abnormalities such as errors and unexpected events of the devices.
- An operation and management procedure regarding the initial action and the convergence of the situation should be created for an appropriate incident response when an abnormality in the device is detected, and the procedure should be evaluated and reviewed as necessary.

3.4. Asset

The“Asset” category is an area that has direct connection with the physical area, and is a category that generates data necessary for solving regional issues and sends it to the "City OS". In this category, it is necessary to consider the security of physical devices, networks and relay devices for distributing data to "City OS".

<Points>

1. Keep the device firmware and software version up to date.

2. Encrypt communications with the outside via the Internet.

3. Physically protect devices.

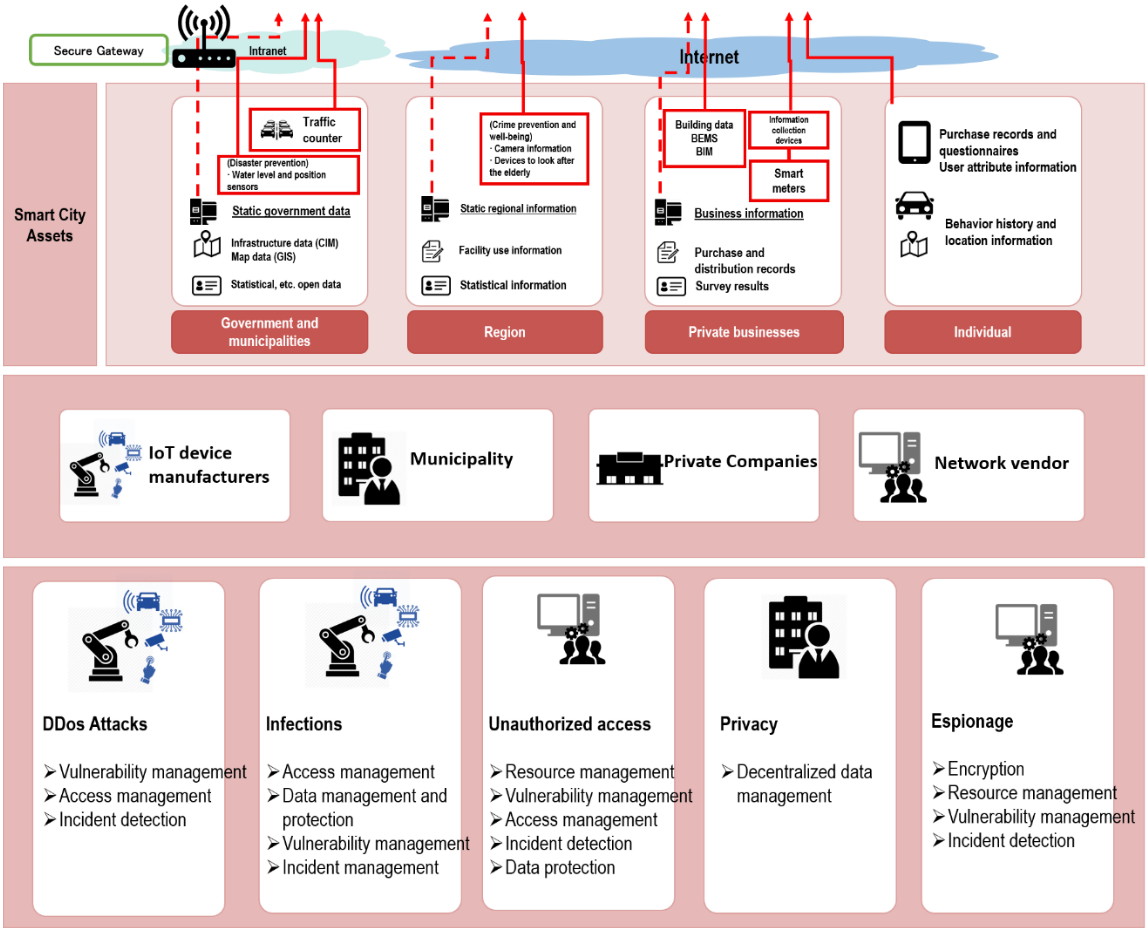


Figure 3-6 Image of Asset

<Examination image>

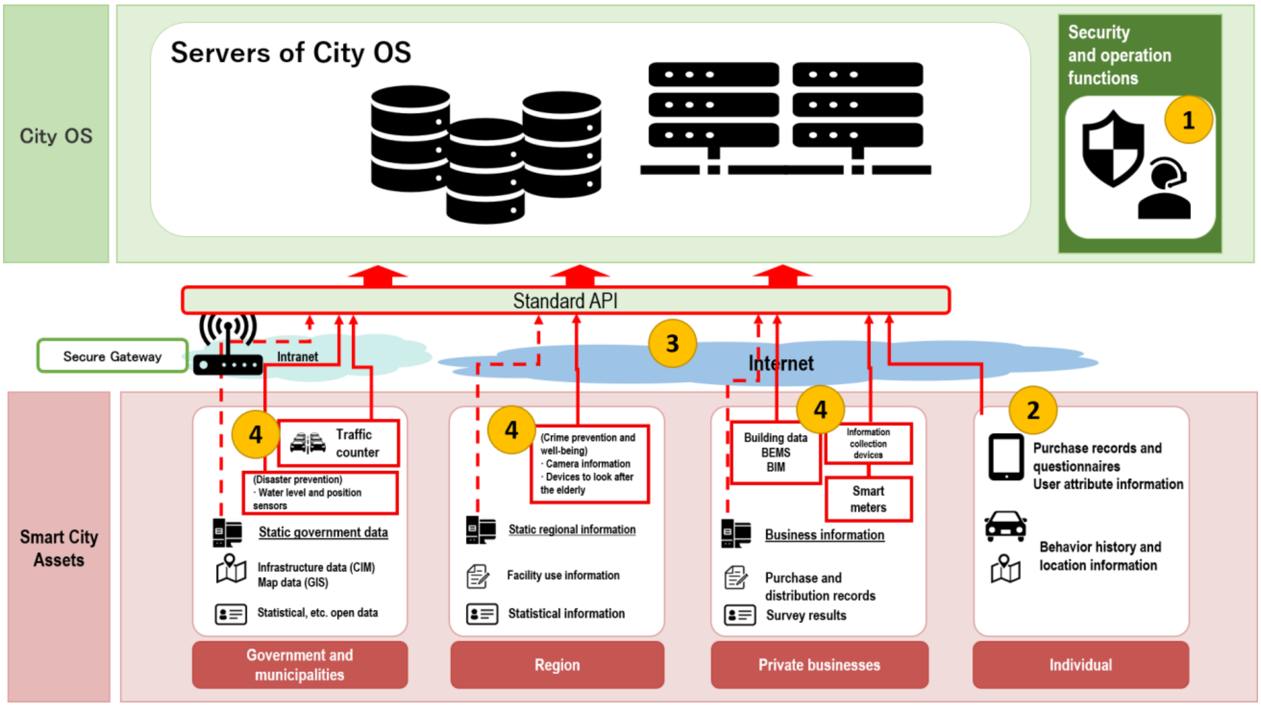

City OS
Servers of City OS
Security and operation functions
1
Standard API
Secure Gateway
Intranet
3
Internet
Smart City Assets
4
Traffic counter
(Disaster prevention)
· Water level and position sensors
Static government data
Infrastructure data (CIM)
Map data (GIS)
Statistical, etc. open data
Government and municipalities
4
(Crime prevention and well-being)
· Camera information
· Devices to look after the elderly
Static regional information
Facility use information
Statistical information
Region
4
Building data
BEMS
BIM
Information collection devices
Smart meters
Business information
Purchase and distribution records
Survey results
Private businesses
2
Purchase records and questionnaires
User attribute information
Behavior history and location information
Individual

Figure 3-7 Image of security measures in Asset

<Examples of countermeasures>

1. Keep the device firmware and software version up to date.

Vulnerabilities in IoT devices and relay devices are discovered on a daily basis, and patches that address these vulnerabilities are released by vendors.

In order to protect devices from unauthorized access and attacks that exploit vulnerabilities made by malicious actors, it is necessary to update the firmware and software versions of IoT devices and relay devices as appropriate. In addition, it is necessary to continuously collect vulnerability information distributed by vendors of IoT devices and relay devices, and to apply patches as necessary.

2. Encrypt communications with the outside via the Internet.

The data collected by IoT devices is sent to "City OS" via the Internet. Since there is a possibility that the communication data is sniffed and tampered data by third parties, it is necessary to encrypt the communication with "City OS".

3. Physically protect assets.

Depending on the service, there are cases where IoT devices are carried around by users or installed in users’ homes or public spaces. In such cases, there are risks of physical attack such as the device being stolen or the devices lost by the users being illegally controlled by a malicious third party.

In addition, there is a possibility that information is leaked from discarded devices, or devices incorporating malicious software is sold second-hand. Therefore, it is necessary to physically protect unauthorized access to the device from the outside.

- Devices deployed in homes or public institutions should restrict physical access by anyone other than those involved.
- Monitor the status of devices for detecting abnormalities such as physical destruction of the devices.

<Tips>

Although the examples described above explain specific measures in operation phase, it should be noted that assets with functions related to 1 to 3 will be procured and introduced in the planning, design and development phases.

4. Security considerations specific to Smart Cities

4.1. Security considerations and security measures

4.1.1. Cooperation among multi-stakeholders

Smart City as a place for the advance realization of Society 5.0 is expected to be highly networked in the future, with various actors participating in the dynamically constructed supply chain. In that case, security measured conducted by one company will likely be insufficient to ensure the security of entire Smart City. Therefore, it is desirable that, with sufficient cooperation among multi-stakeholders led by primary promoter, the wide range of security measures such as “implementation of security measure of assets and services in plan, design and development phases as Smart City life cycle”, “implementation of proactive security measure in operation phase”, and “preparation of organizational framework to deal with incident response” are considered and implemented.

The points which should be taken care when cooperating among multi-stakeholders are shown below.

1. Develop common security policies.
2. Clarify the demarcation point of responsibility among multi-stakeholders and establish an implementation system for the entire Smart City.
3. Share 1 and 2 among multi-stakeholders and make them recognized as common understanding.

Each considerations points will be briefly explained in the following sentences.

1. Develop common security policies.

Security-related policies should cover security management standards, data handling policies, and a risk criteria. For example, information which one organization thinks should not be disclosed may be disclosed by another organization due to the difference of their data handling policies. In another case, because of the difference of risk criteria, there is a possibility that one organization judges that there was no problem, while a major problem occurs in another organization. To prevent those situations, it is desirable to discuss in advance among multi-stakeholders and formulate a common policy for the Smart City as a whole.

2. Clarify the demarcation point of responsibility among multi-stakeholders and establish an implementation system for the entire Smart City.

As the problem which occurs because of involvement of multi-stakeholders, demarcation point of responsibility may be ambiguous. For example, when a problem occurs in the operation of a smart city, if there is no pre-determined agreement on which organization will grasp the event and which will respond to the problem, each party may respond in an ad hoc, on-the-spot manner, which may result in causing a possibility that the continuous provision of Smart City functions, the maintenance of security strength and service level, and the smooth response to incidents will be hindered. As a solution to this problem, it is possible to respond quickly to these problems by discussing with multi-stakeholders in advance and clarifying the demarcation points of responsibility and their roles, and building a collaborative system in plain/emergency situation.

3. Share 1 and 2 among multi-stakeholders and make them recognized as common understanding.

The most important thing in solving the problems caused by involvement of multi-stakeholders is for multi-stakeholder to recognize the contents of 1 and 2 as common understandings. The contents such as policies, demarcation points of responsibility, and implementation systems should not be defined by one organization. They can be meaningful only when multi-stakeholders involved in Smart City participate in discussion and commonly understand them. Although it depends on the business model of each Smart City, it is generally desirable to have a forum led by primary promoter and to determine the direction of the Smart City as a whole based on a common understanding.

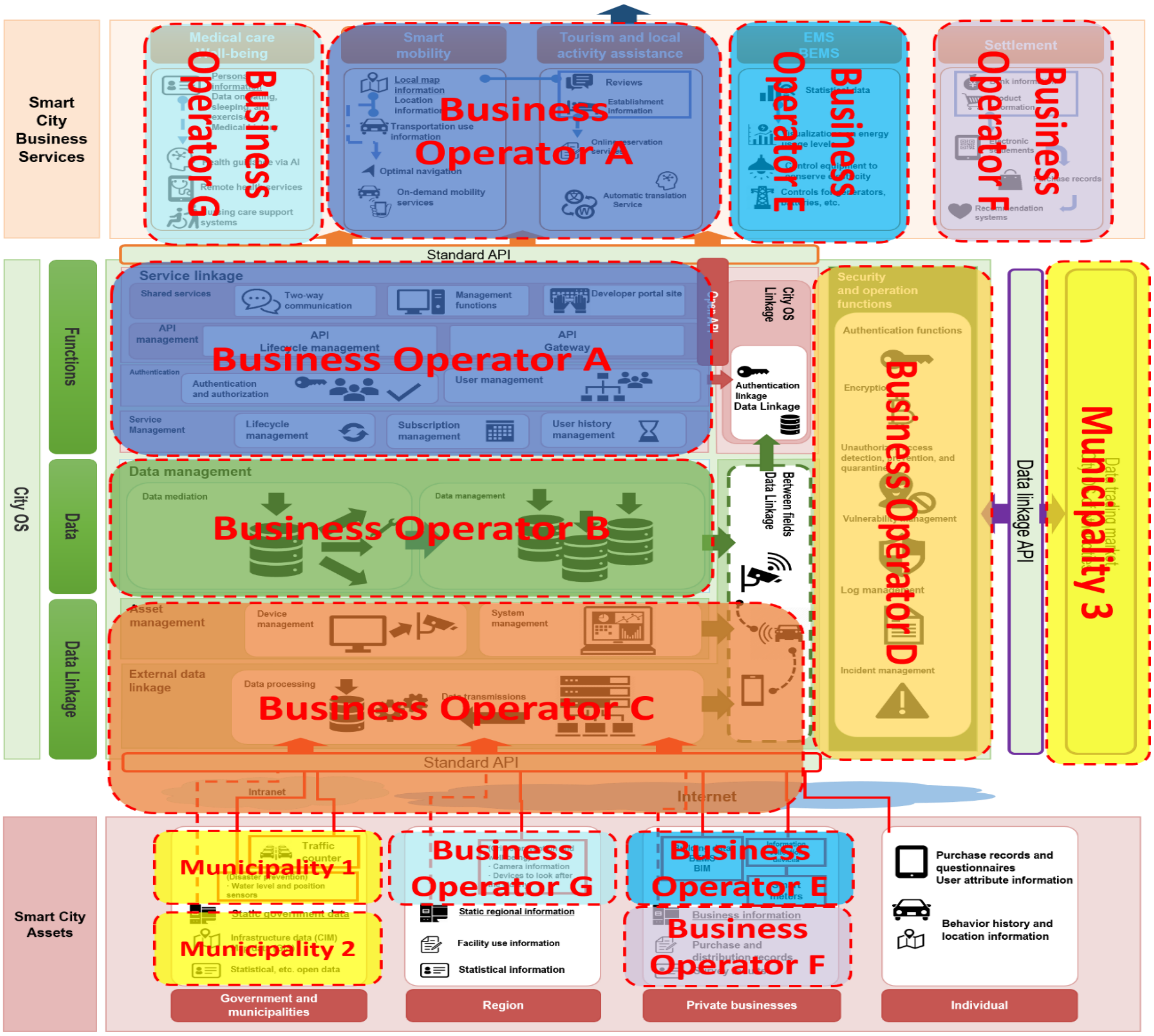


Figure 4-1 Image of multi-stakeholders in Smart City

4.1.2. Ensuring the reliability of data and services

Another consideration point to be taken care of in a Smart City is ensuring the reliability of data and services. As various operators are involved in a complicated manner in a Smart City, the existence of unreliable components which lack reliability of their organization or data would not only lower the service level of the entire Smart City, but also lead to system service outages and information leaks in the worst case. As a result, the reliability of the entire Smart City service will be lost.

Therefore, it is necessary to ensure the reliability of organization by proper supply chain management, and to use electronic certification in data federations between components such as devices and platforms for ensuring integrity and authenticity, which will ensure the reliability of the service.

In addition, it is recommended to build SOC/CSIRT to protect Smart City services as a whole so that problems are not handled as matters specific to individual components or organizations. Specifically, it is recommended that SOC/CSIRT grasp the situation of cyber attacks and security incidents in real time, share information with multi-stakeholders, and deal with these incidents in cooperation with the multi-stakeholders.

4.2. Possible risks and examples of security measures

I. Multi-stakeholder security policy issues

Possible problems

Case 1: Problems caused by different security policy levels among multi-stakeholders

If, among multi-stakeloders in s Smart City, a service provider such as software and applications provider has a vulnerable security management structure, even if unauthorized login to its management system is found, information collection about access to its system by the service provider may be delayed. As a result, the investigation of the cause of the incident may be delayed and the damage may spread.

In addition, if there are variations in security implementation system among multi-stakeholders, for example, in the case that falsification of information in a Smart City is found, while City OS vendors collect information necessary for case investigation, a service provider may not collect information for investigation, which may delay the investigation of the cause of the incident. As a result, the status report to a service owner or a primary promoter who controls the entire Smart City may be delayed, and the user's reliability to the entire Smart City may be lost.

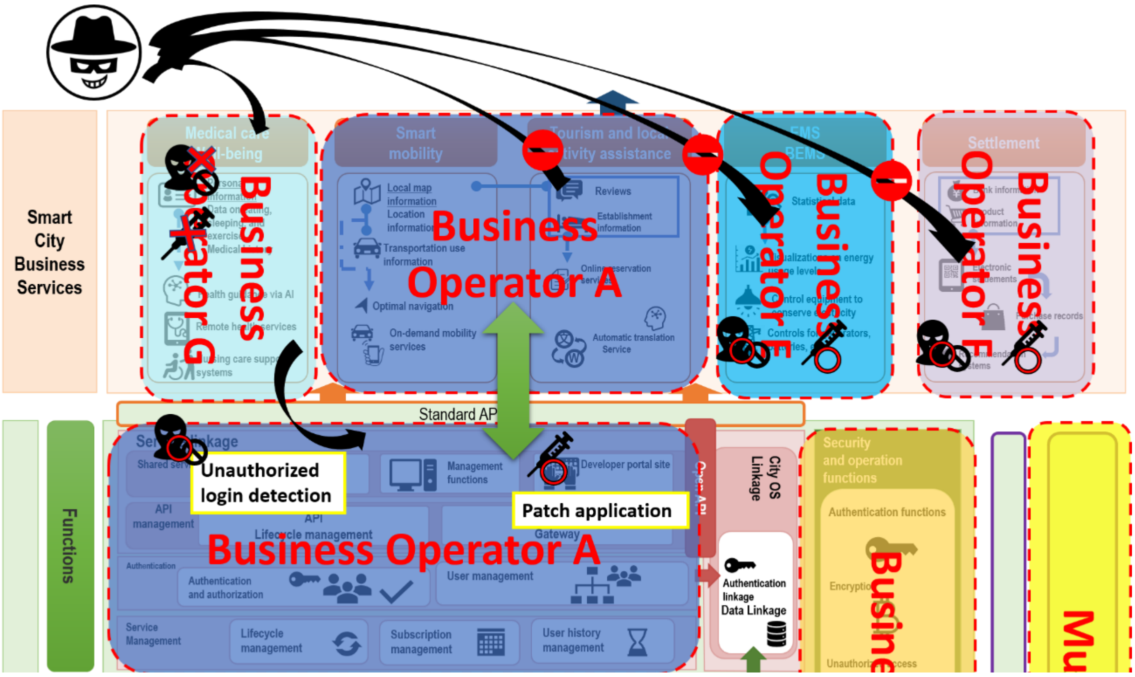


Figure 4-2 Problems caused by different security policy levels among multi-stakeholders

Case 2: Problems caused by unclear demarcation of roles among multi-stakeholders

If the demarcation of roles among multi-stakeholders is unclear, even if falsification of information is found, the information sharing among the businesses in charge of each component and the investigation in each component may be insufficient, which may prevent them from identifying damages and cause of the incident.

Example of security measures

Essential measures

1. Determine a superviser, such as the service owner or primary promoter that controls the whole Smart City.
2. The supervisor understands the business operators (vendor, etc.) which participate in the entire Smart City or each service provided in the Smart City, and shares it among multi-stakeholders.
3. All multi-stakeholders set up a contact point in the case of emergency situation and share it among them.
4. A system/service provider such as a vendor prepares procedures for fault isolation and recovery in the event of a system/service failure, procedures for stopping/recovering the system/service in the event of a security incident, and procedures for investigation of the cause of an incident.

Recommended measures

1. The supervisor understands the security level of all multi-stakeholders.
   - Understanding the risk analysis results of each business operator
   - Understanding the response structure in the event of a system failure or incident at each business operator
   - Regularly updating its knowledge of the risk analysis results and the response structure in each business operator
2. The supervisor plays a central role in creating an organization such as SOC/CSIRT related to Smart City, and build a smooth cooperation system among multi-stakeholders.
3. SOC/CSIRT continuously collect threat information and take active security measures by utilizing the information.

II. Problems related to the demarcation of responsibilities among multi-stakeholders

Possible problems

Case: Problems caused by unclear demarcation points of responsibility

When the primary promoter and other businesses (vendors, etc.) involved in a Smart City make a contract regarding provision of services in the Smart City, a non-disclosure agreement is also concluded. If the contents of the agreement are insufficient, in a case that information leakage is found, it may be unclear which of the primary promoter or the contractor should take responsibility for the incident. As a result, since no organization coordinates the response to the incident, it may take time to understand the situation, the incident response may be delayed, and the damage may spread. In addition, even if the primary promoter and the service provider make a contract for Smart City services and agree on which organization will coordinate emergency response, unless the contract between the service provider and the vendor which is the contractor stipulates who will respond the incident with responsibility, the organization in charge of coordination of incident response cannot collect sufficient information. As a result, since the situation cannot be grasped, it takes time to consider countermeasures, and the damage may spread.

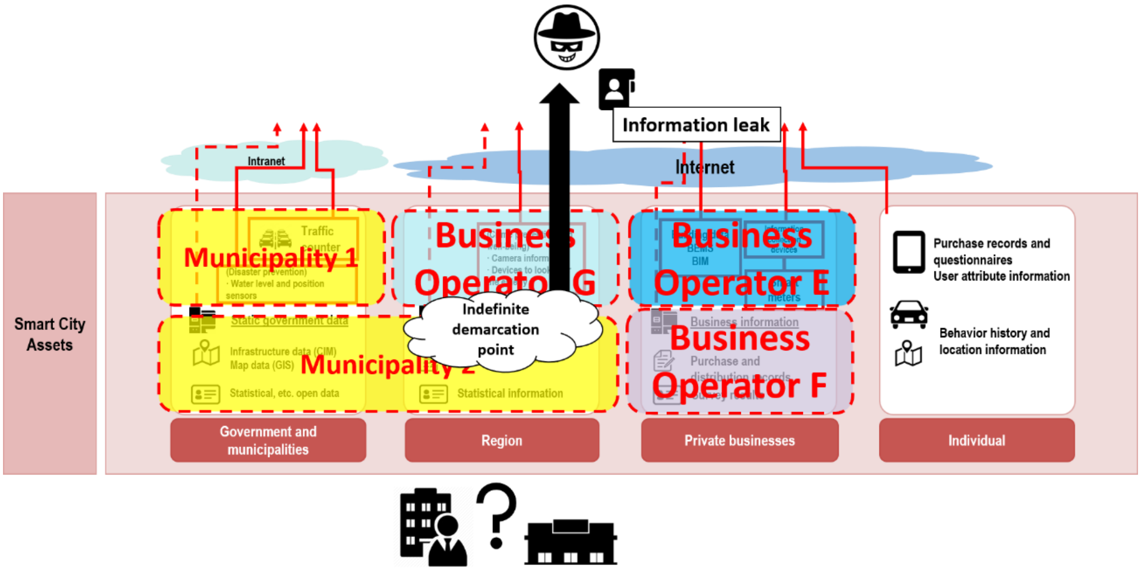


Figure 4-3 Problems caused by unclear demarcation points of responsibility

Example of security measures

Essential measures

1. When making a contract regarding a Smart City among multi-stakeholders, clarify and agree on information to be handled, functions, operation methods, scope of responsibility and so on.
2. Periodically check and review the contents agreed in 1.

Recommended measures

1. Develop a configuration diagram and system diagram that clarify the demarcation points of responsibility for systems and functions.
2. The promotion entity confirms the configuration diagram, system diagram, etc., and confirms that there are no blank areas in management.

III. Problems related to data management policies in multiple stakeholders

Possible problems

Case 1: Problems caused by unclear purpose, authority, and scope of data use

If the purpose, authority, and scope of use of the data stored in a City OS are not clearly defined in the contract among multi-stakeholders, it may be used by those who do not originally have the right to access, or used for other than the original purpose. For example, in a case that a service provider contracts with a primary promoter and starts providing a service using closed data already stored in the city OS, and the service exceeds the original purpose of use of the data, it would mean that the service provider unjustly utilizes the closed data to make a profit, which may eventually lead to a litigation problem.

Case 2: Problems caused by ambiguous data restrictions and handling

When a service provider starts to provide a location information service using data already stored in the city OS, if the data includes not only the de-identified information (open data), but also location information and personal authentication information (closed data), personally identifiable information may be leaked.

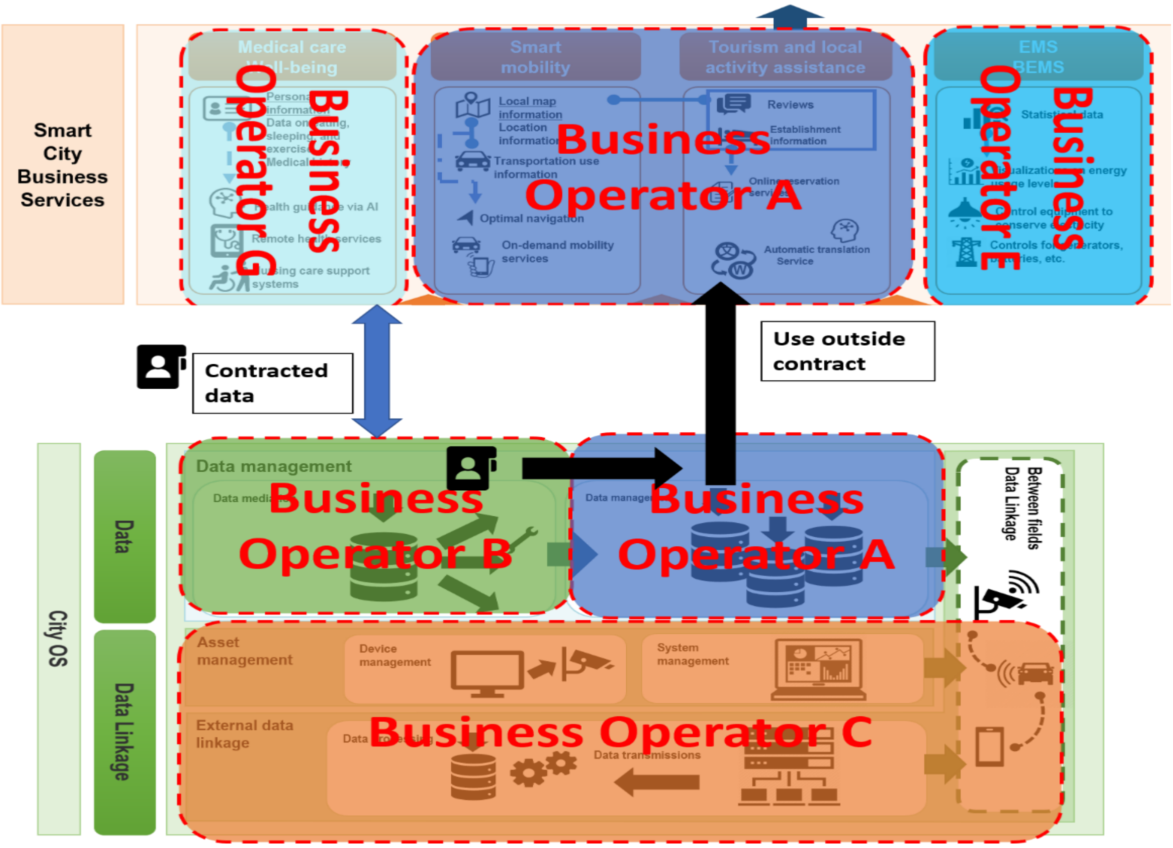


Figure 4-4 Problems caused by unclear purpose, authority, and scope of data use

Example of security measures

Essential measures

1. The information manager of a Smart City (primary promoter, service owner, etc.) lists all the data created and distributed throughout the Smart City.
2. Clarify the purpose of use, authority, scope of use, and owner of the data handled in the Smart City, and agree on it among all multi-stakeholders.
3. Periodically check and review the contents agreed in 2.
4. When disclosing data, clearly indicate the scope of use and the owner of the data.

Recommended measures

1. Before the launch of the system for providing a specific service, confirm that each multi-stakeholder is designed to access only the necessary data.
2. Regarding the data collected in the City OS, delete closed data such as personal information that is unnecessary for providing Smart City services to sanitize it.
3. Regarding the data collected in the City OS, handle the data as statistical data by grouping the contents so that individuals cannot be identified.
4. Monitor and analyze access to the system.
5. Consider traceable (traceability-guaranteed) system configurations and security designs that utilize technologies such as trust services/blockchain.

IV. Problems related to building a security management system

Possible problems

Case: Problems caused by insufficient understangin of the entire Smart City system

There may be cases that the supervisor (service owner or primary promoter) outsources system construction and operation to a service provider and the service provider subcontracts it to another company. In that case, for example, the security and system requirements from the supervisor may not be sufficiently communicated to the subcontractor, and vulnerable security measures may be taken. As a result, there is a possibility that the reliability of the users to the Smart City as a whole may be lost due to problems such as information leakage at the subcontractor.

Example of security measures

Essential measures

1. Determine a superviser, such as the service owner or primary promoter that controls the whole Smart City.
2. The supervisor understands the data flow, linked systems, and the supply chain including subcontracting and re-consignment for each service provided in the smart city, and manages the entire Smart City system.

Recommended measures

1. The supervisor understands the security level of the partner company.
   - Understanding the risk analysis results of each business operator
   - Understanding the response structure in the event of a system failure or incident at each business operator
   - Regularly updating its knowledge of the risk analysis results and the response structure in each business operator
2. The supervisor plays a central role in creating an organization such as SOC/CSIRT related to Smart City, and build a smooth cooperation system among multi-stakeholders.
3. The supervisor will take the initiative in conducting security incident response training for understanding the points where incident response is delayed and security measures are insufficient, and improve the points.
   <Examples>
   - Review of supply chain management system including subcontracting and re-consignment
   - Clarification of risks and security measures of each multi-stakeholder.

- Establishment of contact points and systems among multi-stakeholders in the event of a security incident.
- Development of information sharing methods and service recovery procedures when an incident occurs.
- Implementation of regular security incident response training.

Tips

SOC/CSIRT collaboration for grasping situation, information gathering, incident response etc.

The following are examples of security factors that should be ensured in a Smart City.

- Preventing leakage of important information in Smart City systems
- Prevention of unauthorized access to the system
- Ensuring the integrity and reliability of the IoT devices
- Ensuring the authenticity of assets (data) sent from IoT devices
- Ensuring the integrity and authenticity of communication among components

In order to secure these factors and prevent the occurrence of serious security incidents, it is recommended to monitor and analyze logs, detect security incidents promptly, and respond immediately. In addition, from the viewpoint of incident prevention, it is desirable to collect information on a daily basis and take systematic and regular security measures. To achieve this, it is recommended to establish a SOC/CSIRT containing cross-cutting security support functions.

<Expected roles in SOC/CSIRT>

SOC

- Threats detection/notification
- Incidents detection/notification

CSIRT

- Proactive measures (information collection, configuration management, risk assessment)
- Post-event response (correlation analysis, incident response)
- Information sharing

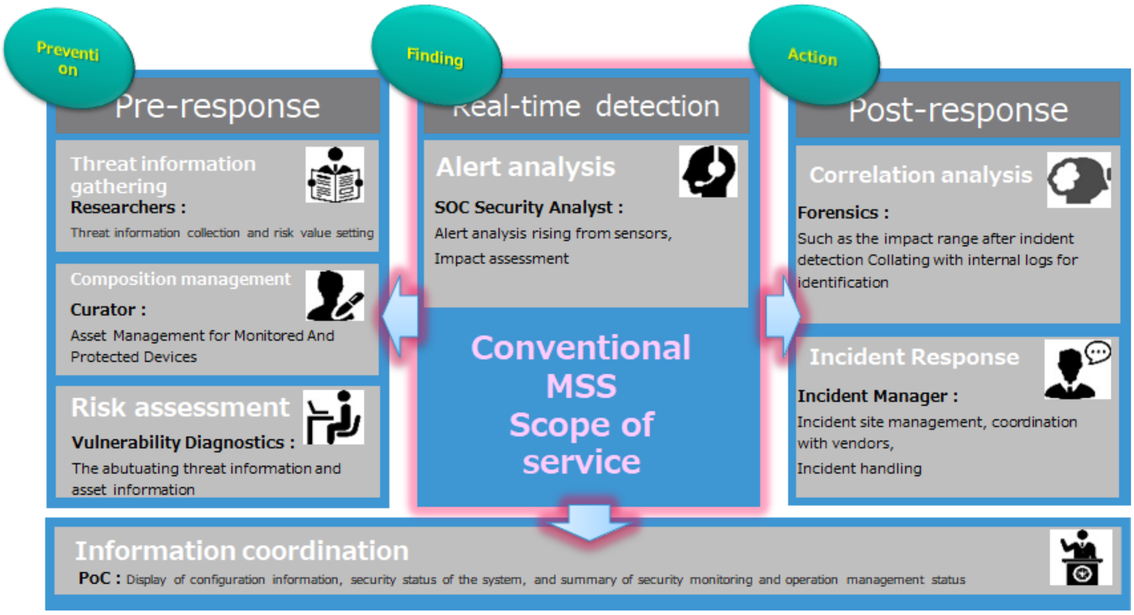

Preventi on
Pre-response
Threat information gathering
Researchers :
Threat information collection and risk value setting
Composition management
Curator :
Asset Management for Monitored And Protected Devices
Risk assessment
Vulnerability Diagnostics :
The abutuating threat information and asset information
Finding
Real-time detection
Alert analysis
SOC Security Analyst :
Alert analysis rising from sensors, Impact assessment
Conventional MSS Scope of service
Action
Post-response
Correlation analysis
Forensics :
Such as the impact range after incident detection Collating with internal logs for identification
Incident Response
Incident Manager :
Incident site management, coordination with vendors,
Incident handling
Information coordination
PoC : Display of configuration information, security status of the system, and summary of security monitoring and operation management status

Figure 4-5 Expected roles in SOC/CSIRT

5. Example of security requirements

In the previous chapters, the concept of security in the establishment and operation of Smart Cities and the security measures that should be implemented by the parties involved in the promotion and operation of Smart Cities including the supply chain are discussed.

Chapter 5 aims to provide a list of security measures that should be implemented by each entity involved in a Smart City with respect to the viewpoints of security measures and risks, and to help multi-stakeholders select security measures.

The examples of security measures organized in the list of security measures are just examples, and do not deny various domestic and overseas guidelines and other implementations. It is recommended to consider appropriate security measures by referring to the list in consideration of the importance and risk of a system in each entity and the relative cost when selecting security measures.

5.1. List of security measures

It is recommended to consider which security measures shoulde be implemented by a primary promoter or each entity involved in a Smart City in the following order.

1. In Chapters 3 and 4, understand the concept of security in Smart Cities and typical security measures.
2. Identify the functions and assets (data) to be protected in your Smart City system/service.
3. Based on the identified functions and assets to be protected, derive the risks (incidents, threats, vulnerabilities) that are assumed to occur in your Smart City system/service.
4. Extract the relevant risks from Attachment A "Risk List" and confirm the corresponding [Security measure requirement ID].
5. Use the [Security measure requirement ID] to find the specific content of the security measure from Attachment B "List of Security Measures".

An example using a use case is shown below.

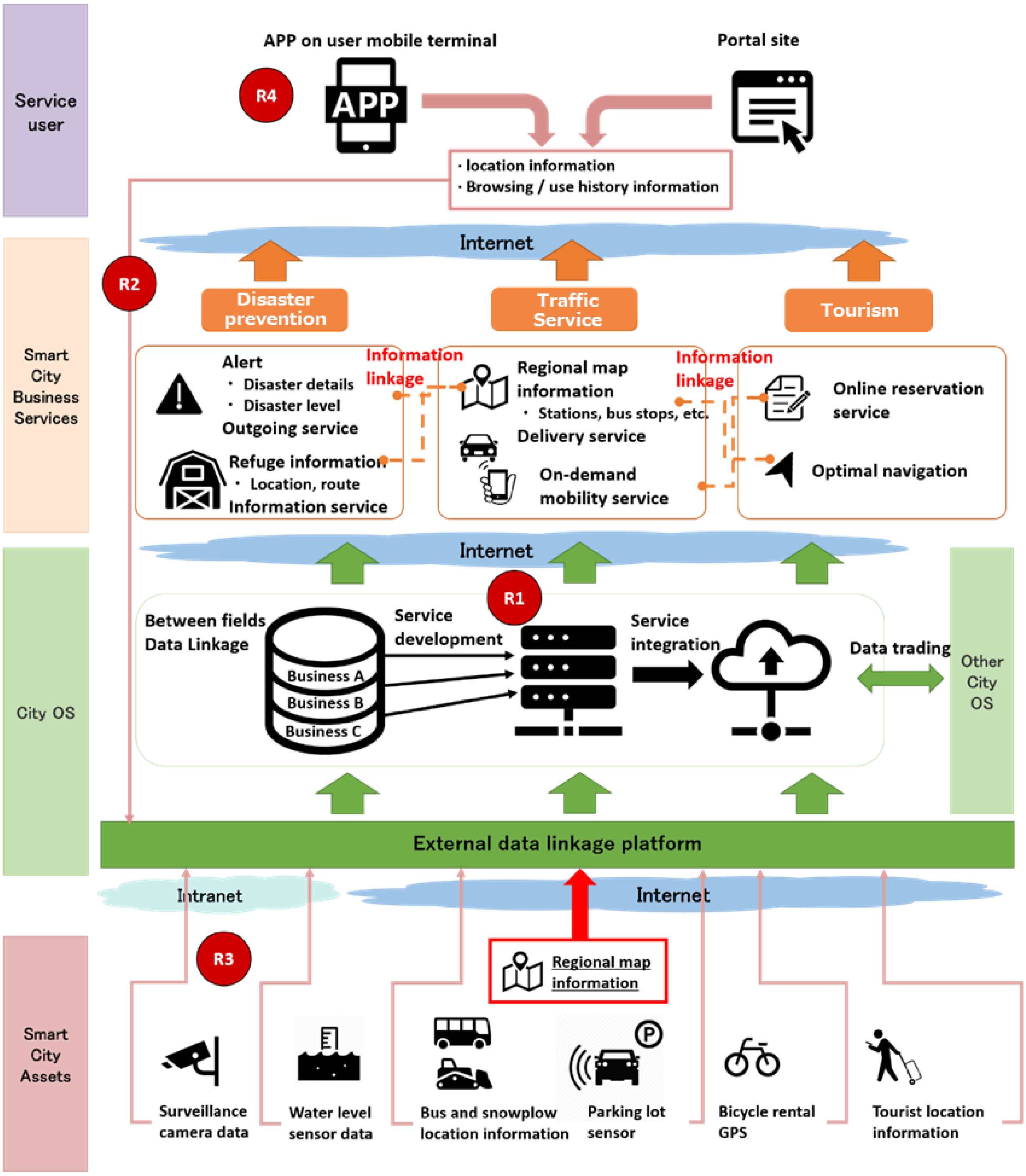


Figure 5-1 An example of use case in Smart City

Table 5-1 An example of risks

Source of Risk	Risk overview	Countermeasure number
R1	Fraudulent reception by impersonation	CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9, CPS.IP-2, CPS.IP-10, CPS.MA-1, CPS.MA-2, CPS.RA-2, CPS.CM-6, CPS.CM-7
	System outage due to denial-of-service attacks, ransomware infections etc.	CPS.RA-1, CPS.RA-3, CPS.RA-4, CPS.RA-5, CPS.RA-6, CPS.RM-2, CPS.DS-6, CPS.DS-7
	Organization's protected data is tampered with	CPS.AC-7, CPS.AC-9, CPS.DS-2, CPS.DS-3, CPS.DS-4, CPS.DS-11
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.RA-4, CPS.RA-6
R2	Data to be protected from other related organizations is leaked from the area (data storage) managed by own organization	CPS.AC-1, CPS.AC-5, CPS.AC-6, CPS.AC-9, CPS.GV-3
	Incorrect analysis results due to malfunction of the data processing / analysis system	CPS.CM-3, CPS.CM-4
R3	The tampered IoT device is connected to the network, causing a failure or transmission of unclear data	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6, CPS.DS-8, CPS.SC-4
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.CM-3, CPS.AE-1, CPS.CM-1, CPS.CM-5, CPS.PT-1, CPS.RP-1
	Unauthorized access to IoT devices	CPS.IP-1, CPS.PT-2, CPS.DS-15, CPS.RA-4, CPS.RA-6, CPS.SC-4
	Wiretapping of communication on networks using security vulnerabilities of IoT devices	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6
R4	Receiving inappropriate data from organization / human / things (spoofing etc.)	CPS.DS-3, CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9

5.2. Consistency with domestic and overseas guidelines and standards

This guideline is based on the Reference Architecture, and summarizes the security concept, assumed risks, and security measures for the entire smart city. On the other hand, when considering security measures for IoT devices in smart city assets, there is the "IoT Security Guideline" that systematically shows the risks of IoT devices and their measures, focusing on the life cycle of IoT devices (policy, analysis, design, construction/connection, operation/maintenance).

For considering measures against IoT device risks, this guideline refers to the viewpoint in the "IoT Security Guideline" and takes care to maintain consistency with the description in the "IoT Security Guideline".　In addition, examples of security measures required to provide applications and systems in smart cities are given in Attachment B "List of Security Measures". Since this list refers to guidelines such as "Information Security Measures Guidelines for Cloud Service Provision", "NIST SP800-171", "NIST SP800-53", and "Cyber Physical Security Framework" by implementing the requirements in the list, it is possible to indirectly comply with international standards.

It is expected that the viewpoint of security that should be emphasized in Smart Cities described in this guideline is combined with the security measure examples in the list, and to contribute to the implementation of higher security Smart Cities.

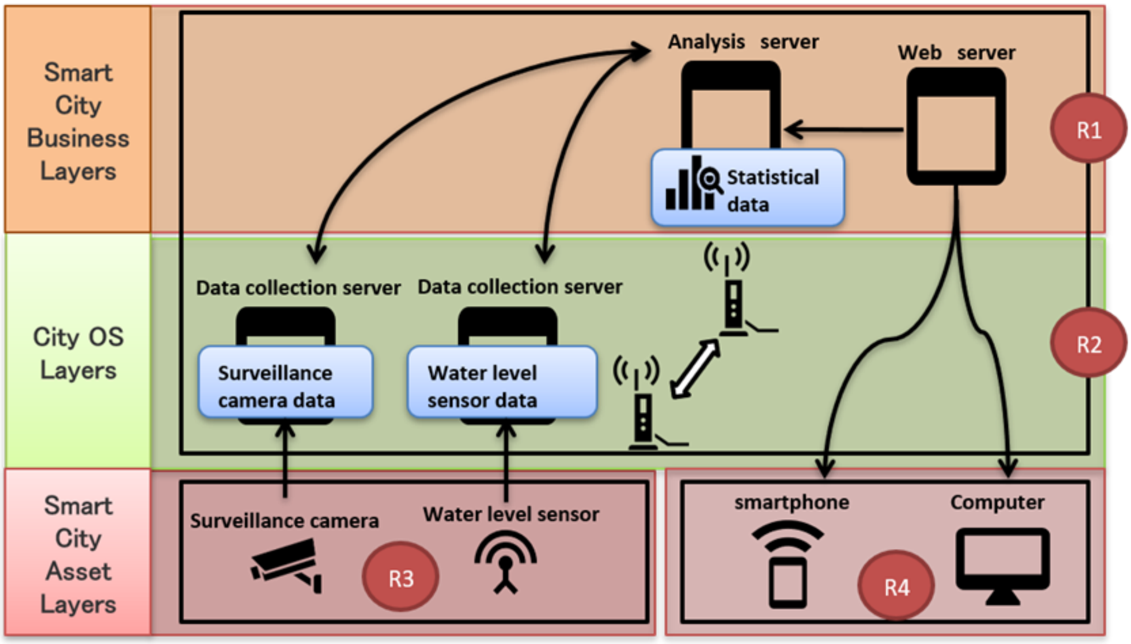
Table 5-2 Referred guidelines

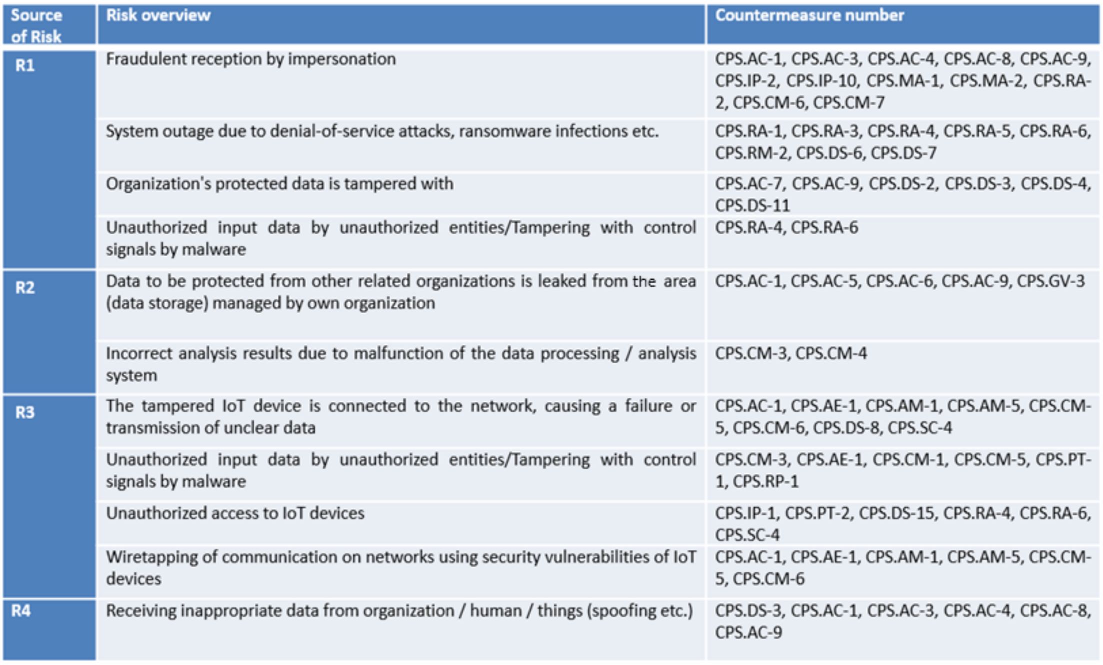
	Applicable measure requirements in "the cyber physical security measure framework"	Reference guidelines					
		NIST Cyber Security Framework Ver 1.1	NIST SP 800-171,53	ISO/IEC 27001:2013 "Annex A"	ISO/IEC 27017:2015	IoT security guidelines Ver 1.0	Guidelines for Information Security Measures in Providing Cloud Services
Smart city governance management	CPS.AC-1,2,5 CPS.AE-1～5 CPS.AM-2～7 CPS.AN-1～3 CPS.AT-1～3 CPS.BE-1～3 CPS.CM-1,2,6 CPS.CO-1～3 CPS.DP-1～4 CPS.DS-1,11,13～15 CPS.GV-1～4 CPS.IM-1,2 CPS.IP-1,3,7～10 CPS.MI-1 CPS.PT-1 CPS.RA-1～3,5,6 CPS.RM-1,2 CPS.RP-1～3 CPS.SC-1～11	◎	○	◎	○	◎	○
Smart city business service	CPS.AC-1～9 CPS.AE-1 CPS.AM-1～3,5 CPS.CM-1～7 CPS.DS-2～11,13 CPS.GV-3 CPS.IP-1,2,4～6,10 CPS.MA-1,2 CPS.PT-1,2 CPS.RA-1,2,4,6 CPS.RP-1,4 CPS.SC-3,4,8	○	○			○	○
Smart city OS	CPS.AC-1～9 CPS.AE-1,3 CPS.AM-1,2,5 CPS.CM-1～7 CPS.DP-4 CPS.DS-1～13 CPS.GV-3 CPS.IP-1,2,4～6,10 CPS.MA-1,2 CPS.PT-2,3 CPS.RA-1～6 CPS.RM-2 CPS.RP-1 CPS.SC-3,4,8	○	○	○	◎	○	◎
Smart city assets	CPS.AC-1～4 CPS.AC-7～9 CPS.AE-1 CPS.AM-1,5 CPS.CM-2,3,5～7 CPS.DS-3,6～8,10,11,13,15 CPS.IP-1,2,4～6 CPS.MA-1～3 CPS.PT-2 CPS.RA-4,6 CPS.SC-3,4,8	○	○			◎	◎

(Reference) Considerations on “disaster prevention”, “medical/welfare”, “settlement”, “transportation” and “tourism”

Disaster prevention

【Use case example】
Water level sensors and security cameras will be used to obtain advance information on floods, landslides, and river floods, and take measures such as developing disaster prevention measures at appropriate locations and evacuation guidance to residents.



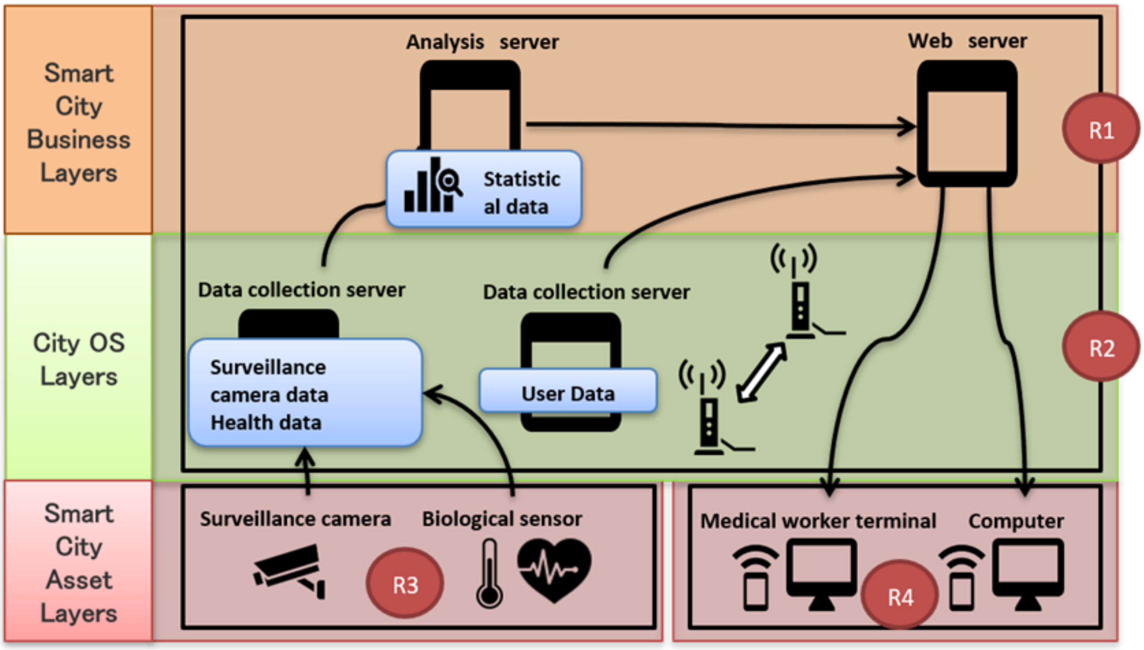


Source of Risk	Risk overview	Countermeasure number
R1	Fraudulent reception by impersonation	CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9, CPS.IP-2, CPS.IP-10, CPS.MA-1, CPS.MA-2, CPS.RA-2, CPS.CM-6, CPS.CM-7
	System outage due to denial-of-service attacks, ransomware infections etc.	CPS.RA-1, CPS.RA-3, CPS.RA-4, CPS.RA-5, CPS.RA-6, CPS.RM-2, CPS.DS-6, CPS.DS-7
	Organization's protected data is tampered with	CPS.AC-7, CPS.AC-9, CPS.DS-2, CPS.DS-3, CPS.DS-4, CPS.DS-11
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.RA-4, CPS.RA-6
R2	Data to be protected from other related organizations is leaked from the area (data storage) managed by own organization	CPS.AC-1, CPS.AC-5, CPS.AC-6, CPS.AC-9, CPS.GV-3
	Incorrect analysis results due to malfunction of the data processing / analysis system	CPS.CM-3, CPS.CM-4
R3	The tampered IoT device is connected to the network, causing a failure or transmission of unclear data	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6, CPS.DS-8, CPS.SC-4
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.CM-3, CPS.AE-1, CPS.CM-1, CPS.CM-5, CPS.PT-1, CPS.RP-1
	Unauthorized access to IoT devices	CPS.IP-1, CPS.PT-2, CPS.DS-15, CPS.RA-4, CPS.RA-6, CPS.SC-4
	Wiretapping of communication on networks using security vulnerabilities of IoT devices	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6
R4	Receiving inappropriate data from organization / human / things (spoofing etc.)	CPS.DS-3, CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9

Medical / welfare

【 Use case example 】

By collecting and accumulating health information of elderly people and patients, doctors and family members can always grasp the health information of patients.

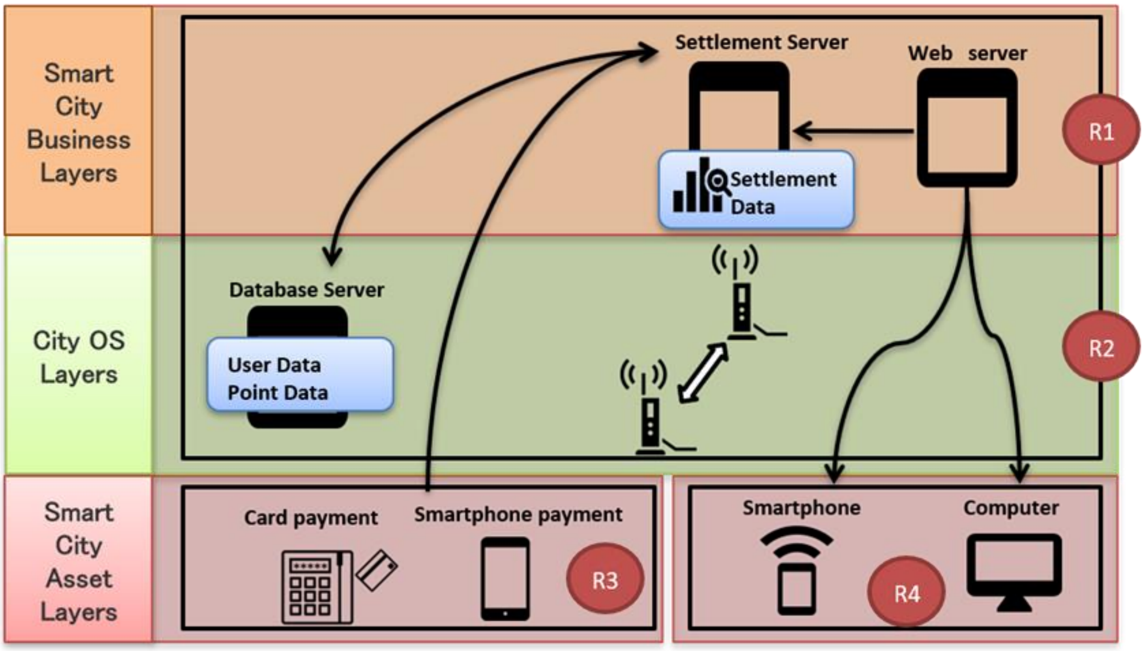


Source of Risk	Risk overview	Countermeasure number
R1	Fraudulent reception by impersonation	CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9, CPS.IP-2, CPS.IP-10, CPS.MA-1, CPS.MA-2, CPS.RA-2, CPS.CM-6, CPS.CM-7
	System outage due to denial-of-service attacks, ransomware infections etc.	CPS.RA-1, CPS.RA-3, CPS.RA-4, CPS.RA-5, CPS.RA-6, CPS.RM-2, CPS.DS-6, CPS.DS-7
	Organization's protected data is tampered with	CPS.AC-7, CPS.AC-9, CPS.DS-2, CPS.DS-3, CPS.DS-4, CPS.DS-11
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.RA-4, CPS.RA-6
R2	Data to be protected from other related organizations is leaked from the area (data storage) managed by own organization	CPS.AC-1, CPS.AC-5, CPS.AC-6, CPS.AC-9, CPS.GV-3
	Incorrect analysis results due to malfunction of the data processing / analysis system	CPS.CM-3, CPS.CM-4
R3	The tampered IoT device is connected to the network, causing a failure or transmission of unclear data	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6, CPS.DS-8, CPS.SC-4
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.CM-3, CPS.AE-1, CPS.CM-1, CPS.CM-5, CPS.PT-1, CPS.RP-1
	Unauthorized access to IoT devices	CPS.IP-1, CPS.PT-2, CPS.DS-15, CPS.RA-4, CPS.RA-6, CPS.SC-4
	Wiretapping of communication on networks using security vulnerabilities of IoT devices	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6
R4	Receiving inappropriate data from organization / human / things (spoofing etc.)	CPS.DS-3, CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9

Settlement

【 Use case example 】

Enables settlement by local currency and local points. Users can check their acquisition points and usage status from the Web service.

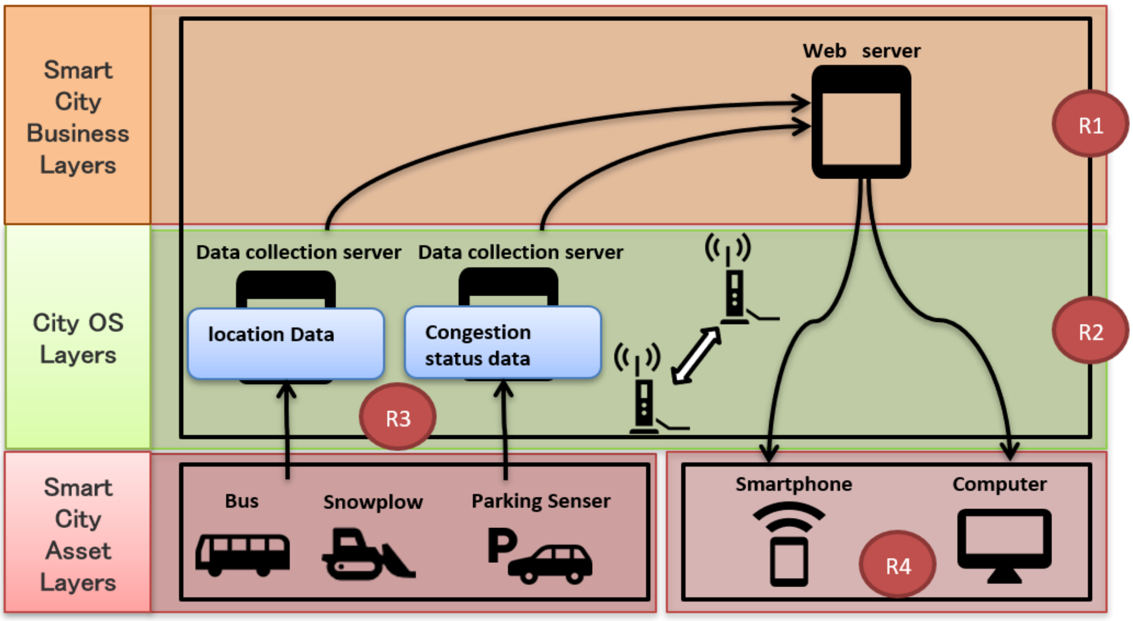


Source of Risk	Risk overview	Countermeasure number
R1	Fraudulent reception by impersonation	CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9, CPS.IP-2, CPS.IP-10, CPS.MA-1, CPS.MA-2, CPS.RA-2, CPS.CM-6, CPS.CM-7
	System outage due to denial-of-service attacks, ransomware infections etc.	CPS.RA-1, CPS.RA-3, CPS.RA-4, CPS.RA-5, CPS.RA-6, CPS.RM-2, CPS.DS-6, CPS.DS-7
	Organization's protected data is tampered with	CPS.AC-7, CPS.AC-9, CPS.DS-2, CPS.DS-3, CPS.DS-4, CPS.DS-11
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.RA-4, CPS.RA-6
R2	Data to be protected from other related organizations is leaked from the area (data storage) managed by own organization	CPS.AC-1, CPS.AC-5, CPS.AC-6, CPS.AC-9, CPS.GV-3
	Incorrect analysis results due to malfunction of the data processing / analysis system	CPS.CM-3, CPS.CM-4
R3	The tampered IoT device is connected to the network, causing a failure or transmission of unclear data	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6, CPS.DS-8, CPS.SC-4
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.CM-3, CPS.AE-1, CPS.CM-1, CPS.CM-5, CPS.PT-1, CPS.RP-1
	Unauthorized access to IoT devices	CPS.IP-1, CPS.PT-2, CPS.DS-15, CPS.RA-4, CPS.RA-6, CPS.SC-4
	Wiretapping of communication on networks using security vulnerabilities of IoT devices	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6
R4	Receiving inappropriate data from organization / human / things (spoofing etc.)	CPS.DS-3, CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9

Traffic Service

【 Use case example 】

We will acquire the location information of buses and snowplows and distribute them to residents and tourists to promote the use of transportation.In addition, by distributing the usage status of the parking lot, the use of residents and tourists is encouraged.

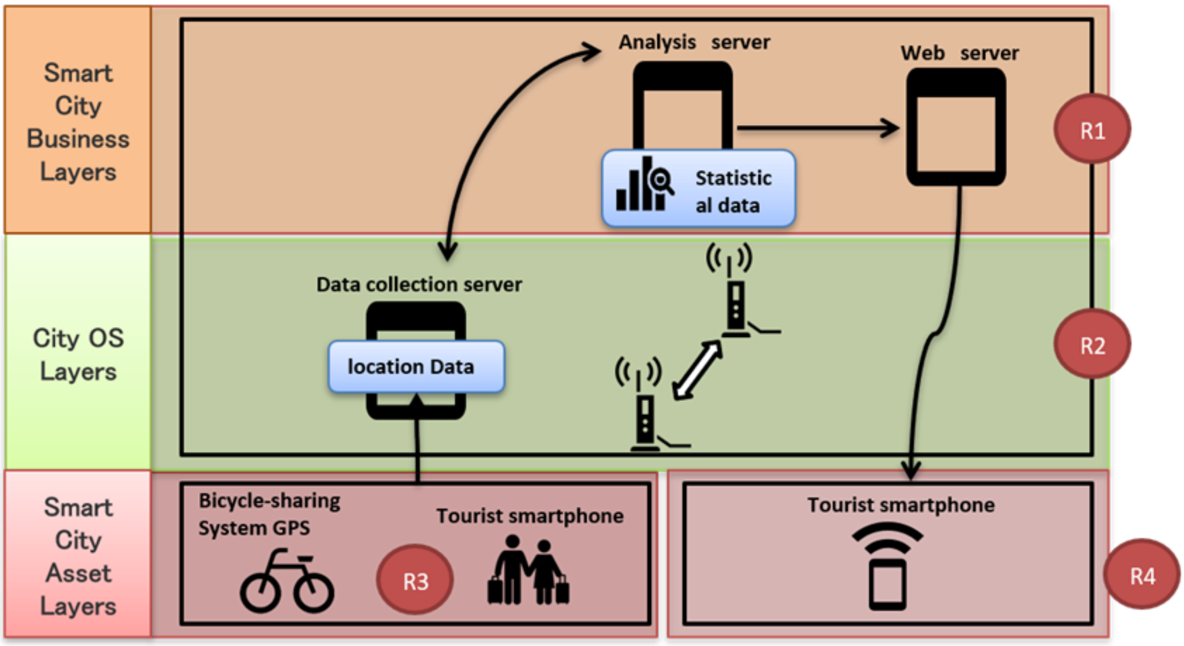


Source of Risk	Risk overview	Countermeasure number
R1	Fraudulent reception by impersonation	CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9, CPS.IP-2, CPS.IP-10, CPS.MA-1, CPS.MA-2, CPS.RA-2, CPS.CM-6, CPS.CM-7
	System outage due to denial-of-service attacks, ransomware infections etc.	CPS.RA-1, CPS.RA-3, CPS.RA-4, CPS.RA-5, CPS.RA-6, CPS.RM-2, CPS.DS-6, CPS.DS-7
	Organization's protected data is tampered with	CPS.AC-7, CPS.AC-9, CPS.DS-2, CPS.DS-3, CPS.DS-4, CPS.DS-11
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.RA-4, CPS.RA-6
R2	Data to be protected from other related organizations is leaked from tan area (data storage) managed by own organization	CPS.AC-1, CPS.AC-5, CPS.AC-6, CPS.AC-9, CPS.GV-3
	Incorrect analysis results due to malfunction of the data processing / analysis system	CPS.CM-3, CPS.CM-4
R3	The tampered IoT device is connected to the network, causing a failure or transmission of unclear data	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6, CPS.DS-8, CPS.SC-4
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.CM-3, CPS.AE-1, CPS.CM-1, CPS.CM-5, CPS.PT-1, CPS.RP-1
	Unauthorized access to IoT devices	CPS.IP-1, CPS.PT-2, CPS.DS-15, CPS.RA-4, CPS.RA-6, CPS.SC-4
	Wiretapping of communication on networks using security vulnerabilities of IoT devices	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6
R4	Receiving inappropriate data from organization / human / things (spoofing etc.)	CPS.DS-3, CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9

Tourism

【 Use case example 】

By installing GPS in the rental cycle for tourists and acquiring behavioral information of tourists, appropriate tourist information is distributed to tourists at sightseeing spots.



Source of Risk	Risk overview	Countermeasure number
R1	Fraudulent reception by impersonation	CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9, CPS.IP-2, CPS.IP-10, CPS.MA-1, CPS.MA-2, CPS.RA-2, CPS.CM-6, CPS.CM-7
	System outage due to denial-of-service attacks, ransomware infections etc.	CPS.RA-1, CPS.RA-3, CPS.RA-4, CPS.RA-5, CPS.RA-6, CPS.RM-2, CPS.DS-6, CPS.DS-7
	Organization's protected data is tampered with	CPS.AC-7, CPS.AC-9, CPS.DS-2, CPS.DS-3, CPS.DS-4, CPS.DS-11
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.RA-4, CPS.RA-6
R2	Data to be protected from other related organizations is leaked from the area (data storage) managed by own organization	CPS.AC-1, CPS.AC-5, CPS.AC-6, CPS.AC-9, CPS.GV-3
	Incorrect analysis results due to malfunction of the data processing / analysis system	CPS.CM-3, CPS.CM-4
R3	The tampered IoT device is connected to the network, causing a failure or transmission of unclear data	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6, CPS.DS-8, CPS.SC-4
	Unauthorized input data by unauthorized entities/Tampering with control signals by malware	CPS.CM-3, CPS.AE-1, CPS.CM-1, CPS.CM-5, CPS.PT-1, CPS.RP-1
	Unauthorized access to IoT devices	CPS.IP-1, CPS.PT-2, CPS.DS-15, CPS.RA-4, CPS.RA-6, CPS.SC-4
	Wiretapping of communication on networks using security vulnerabilities of IoT devices	CPS.AC-1, CPS.AE-1, CPS.AM-1, CPS.AM-5, CPS.CM-5, CPS.CM-6
R4	Receiving inappropriate data from organization / human / things (spoofing etc.)	CPS.DS-3, CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9

Appendix A “Risk Table”

Anticipated security incident	Source of risk		Security measure requirement ID
	Threat	Vulnerability	
Receiving improper data from an organization, individual, object, etc. (that have been catfished, etc.)	- Catfishing of a legitimate entity from an unauthorized organization, individual, object, or system - Receiving improper data from a legitimate object or system that has been tampered with	- The credibility of the data collection target that will act as the source for data transmissions or an organization assigned for processing, analysis, etc. is not verified before or after a contract	CPS.SC-7 CPS.SC-8
Receiving improper data from an organization, individual, object, etc. (that have been catfished, etc.)	- Catfishing of a legitimate entity from an unauthorized organization, individual, object, or system - Receiving improper data from a legitimate object or system that has been tampered with	- The manager at the contractor is not sufficiently aware of the handling for the security of data that the organization should protect	CPS.AT-2 CPS.AT-3
Receiving improper data from an organization, individual, object, etc. (that have been catfished, etc.)	- Catfishing of a legitimate entity from an unauthorized organization, individual, object, or system - Receiving improper data from a legitimate object or system that has been tampered with	- Vulnerabilities that should be addressed for collection, analysis, etc. of data on the system are neglected	CPS.IP-2 CPS.IP-10 CPS.MA-1 CPS.MA-2 CPS.RA-2 CPS.CM-6 CPS.CM-7
Receiving improper data from an organization, individual, object, etc. (that have been catfished, etc.)	- Catfishing of a legitimate entity from an unauthorized organization, individual, object, or system - Receiving improper data from a legitimate object or system that has been tampered with	- Transmission lines are not adequately secured	CPS.DS-3
Receiving improper data from an organization, individual, object, etc. (that have been catfished, etc.)	- Catfishing of a legitimate entity from an unauthorized organization, individual, object, or system - Receiving improper data from a legitimate object or system that has been tampered with	- A system for promptly detecting and addressing abnormalities in security is not implemented into the organization's system	CPS.AE-1 CPS.CM-1 CPS.CM-5 CPS.RP-1 CPS.PT-1
Receiving improper data from an organization, individual, object, etc. (that have been catfished, etc.)	- Catfishing of a legitimate entity from an unauthorized organization, individual, object, or system - Receiving improper data from a legitimate object or system that has been tampered with	- At the start of transmissions in cyberspace, the end point of transmissions is not identified and verified	CPS.AC-1 CPS.AC-3 CPS.AC-4 CPS.AC-8 CPS.AC-9
Receiving improper data from an organization, individual, object, etc. (that have been catfished, etc.)	- Catfishing of a legitimate entity from an unauthorized organization, individual, object, or system - Receiving improper data from a legitimate object or system that has been tampered with	- The system that will be filtering data transmissions sent from the end point of the transmission partner is not introduced or is not in operation	CPS.CM-3 CPS.CM-4
Receiving improper data from an organization, individual, object, etc. (that have been catfished, etc.)	- Catfishing of a legitimate entity from an unauthorized organization, individual, object, or system - Receiving improper data from a legitimate object or system that has been tampered with	- The credibility of the data collection target that will act as the source for data transmissions or an organization assigned for processing, analysis, etc. is not	CPS.SC-2 CPS.SC-3 CPS.SC-4 CPS.SC-6

		verified before or after a contract	
(During operations of a piece of equipment installed in an improperly monitored location or after theft, etc. following disposal of equipment) Compromised IoT equipment is connected to the network and transmissions, etc. of damaged or inaccurate data occur	- Network connections from IoT equipment that has been illegitimately modified via theft, etc. - Tampering by an individual inside or outside the organization with malicious intent - Tampering with the measured values, thresholds, or settings of sensors	- The equipment in use is not resistant to tampering and cannot defend against physical tampering	CPS.DS-8
(During operations of a piece of equipment installed in an improperly monitored location or after theft, etc. following disposal of equipment) Compromised IoT equipment is connected to the network and transmissions, etc. of damaged or inaccurate data occur	- Network connections from IoT equipment that has been illegitimately modified via theft, etc. - Tampering by an individual inside or outside the organization with malicious intent - Tampering with the measured values, thresholds, or settings of sensors	- The safety of connection equipment is not checked regularly	CPS.DS-10 CPS.DS-12
(During operations of a piece of equipment installed in an improperly monitored location or after theft, etc. following disposal of equipment) Compromised IoT equipment is connected to the network and transmissions, etc. of damaged or inaccurate data occur	- Network connections from IoT equipment that has been illegitimately modified via theft, etc. - Tampering by an individual inside or outside the organization with malicious intent - Tampering with the measured values, thresholds, or settings of sensors	- Unauthorized equipment connecting to the network cannot be adequately detected	CPS.AM-1 CPS.CM-6
(During operations of a piece of equipment installed in an improperly monitored location or after theft, etc. following disposal of equipment) Compromised IoT equipment is connected to the network and transmissions, etc. of damaged or inaccurate data occur	- Network connections from IoT equipment that has been illegitimately modified via theft, etc. - Tampering by an individual inside or outside the organization with malicious intent - Tampering with the measured values, thresholds, or settings of sensors	- Physical security countermeasures for monitoring, access controls, etc. to the area where IoT equipment is installed is not performed	CPS.AC-2 CPS.CM-2 CPS.IP-5 CPS.PT-2
(During operations of a piece of equipment installed in an improperly monitored location or after theft, etc. following disposal of equipment) Compromised IoT equipment is connected to the network and transmissions, etc. of damaged or inaccurate data occur	- Network connections from IoT equipment that has been illegitimately modified via theft, etc. - Tampering by an individual inside or outside the organization with malicious intent - Tampering with the measured values, thresholds, or settings of sensors	- Procedures for data erasure (or ensuring that data cannot be read) when disposing of IoT equipment do not exist	CPS.IP-6
(During operations of a piece of equipment installed in an improperly monitored location or after theft, etc. following disposal of equipment)	- Network connections from IoT equipment that has been illegitimately modified via theft, etc. - Tampering by an individual inside or outside the organization with malicious intent -	- The status of equipment connected to the organization’s information system or industrial control systems is not understood	CPS.AM-1 CPS.CM-6 CPS.IP-1

Compromised IoT equipment is connected to the network and transmissions, etc. of damaged or inaccurate data occur	Tampering with the measured values, thresholds, or settings of sensors		
(During operations of a piece of equipment installed in an improperly monitored location or after theft, etc. following disposal of equipment) Compromised IoT equipment is connected to the network and transmissions, etc. of damaged or inaccurate data occur	- Network connections from IoT equipment that has been illegitimately modified via theft, etc. - Tampering by an individual inside or outside the organization with malicious intent - Tampering with the measured values, thresholds, or settings of sensors	- Physical wrongdoing to IoT equipment by an individual inside or outside the company cannot be protected against	CPS.AC-2 CPS.CM-2 CPS.SC-5
The organization's data handling system stops due to a DoS attack, ransomware infection, etc.	- DoS attacks towards computer or transmission equipment like servers, etc. that constitute the system - Malware infections that exploit vulnerabilities in security on the system - Transmission of jamming signals	- Risk management involving other organizations that should be involved regarding security is not conducted based on appropriate procedures	CPS.AM-6 CPS.BE-2 CPS.IP-3 CPS.SC-1 CPS.SC-2
The organization's data handling system stops due to a DoS attack, ransomware infection, etc.	- DoS attacks towards computer or transmission equipment like servers, etc. that constitute the system - Malware infections that exploit vulnerabilities in security on the system - Transmission of jamming signals	- Individuals are not sufficiently aware of the safety and security risks involving themselves	CPS.AT-1 CPS.AT-3
The organization's data handling system stops due to a DoS attack, ransomware infection, etc.	- DoS attacks towards computer or transmission equipment like servers, etc. that constitute the system - Malware infections that exploit vulnerabilities in security on the system - Transmission of jamming signals	- Governance of risks related to the safety and security of individuals is insufficient	CPS.SC-8 CPS.IP-9
The organization's data handling system stops due to a DoS attack, ransomware infection, etc.	- DoS attacks towards computer or transmission equipment like servers, etc. that constitute the system - Malware infections that exploit vulnerabilities in security on the system - Transmission of jamming signals	- The security and network connection status of objects constituting the information system and industrial control systems are not managed (e.g.: asset inventories, monitoring)	CPS.AC-1 CPS.AE-1 CPS.AM-1 CPS.AM-5 CPS.CM-5 CPS.CM-6
The organization's data handling system stops due to a DoS attack, ransomware infection, etc.	- DoS attacks towards computer or transmission equipment like servers, etc. that constitute the system - Malware infections that exploit vulnerabilities in security on the system - Transmission of jamming signals	- Technical countermeasures based on the organization's risks are either not implemented or their implementation is not verified	CPS.RA-1 CPS.RA-3 CPS.RA-4 CPS.RA-5 CPS.RA-6 CPS.RM-2
The organization's data handling system stops due to a DoS attack, ransomware infection, etc.	- DoS attacks towards computer or transmission equipment like servers, etc. that constitute the system - Malware infections that exploit vulnerabilities in security on the system - Transmission of jamming signals	- Communications for IoT, servers, etc. are not adequately controlled	CPS.CM-1 CPS.PT-2

The organization's data handling system stops due to a DoS attack, ransomware infection, etc.	- DoS attacks towards computer or transmission equipment like servers, etc. that constitute the system - Malware infections that exploit vulnerabilities in security on the system - Transmission of jamming signals	- Physical obstructions to IoT, servers, etc. (e.g.: jamming waves) are not dealt with	CPS.AC-2 CPS.CM-2 CPS.IP-5
The organization's data handling system stops due to a DoS attack, ransomware infection, etc.	- DoS attacks towards computer or transmission equipment like servers, etc. that constitute the system - Malware infections that exploit vulnerabilities in security on the system - Transmission of jamming signals	- Adequate resources (processing capabilities, communication bandwidth, storage capacity) for systems - including IoT equipment - are not secured	CPS.DS-6 CPS.DS-7
The organization's data handling system stops due to a DoS attack, ransomware infection, etc.	- DoS attacks towards computer or transmission equipment like servers, etc. that constitute the system - Malware infections that exploit vulnerabilities in security on the system - Transmission of jamming signals	- Adequate procedures for security-related risk management are not established	CPS.GV-1 CPS.GV-4 CPS.IP-7 CPS.RM-1 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-10 CPS.SC-11
The system handling organizational data in other related organizations stops due to a DoS attack	- DoS attacks towards computer or transmission equipment like servers, etc. that constitute the system - Transmission of jamming signals	- The credibility of the data collection target or an organization assigned for processing, analysis, etc. is not verified before or after a contract.	CPS.SC-2 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8
Functions of IoT equipment, communication equipment, etc. stop due to a DoS attack	- A DoS attack on the communication equipment or IoT equipment that constitute the IoT system	- Adequate resources (processing capabilities, communication bandwidth, storage capacity) for systems - including IoT equipment - are not secured	CPS.DS-6 CPS.DS-7 CPS.IP-4
Functions of IoT equipment, communication equipment, etc. stop due to a DoS attack	- A DoS attack on the communication equipment or IoT equipment that constitute the IoT system	- Countermeasure procedures after detecting a stoppage in IoT equipment are not defined	CPS.RP-1
A violation of regulations established for data management in cyberspace occurs	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Impersonation of a legitimate user using a stolen ID, password, etc.	- Responsibilities within the organization regarding the management of data to be protected are unclear	CPS.AM-6
A violation of regulations established for data management in cyberspace occurs	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Impersonation of a legitimate user using a stolen ID, password, etc.	- There is not sufficient awareness of regulations, etc. for the necessary data protections that require a response	CPS.GV-3
A violation of regulations established for data management in cyberspace occurs	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into	- Stakeholders are not sufficiently aware of how the security of data their own	CPS.AT-1 CPS.AT-3

	the data storage area - Impersonation of a legitimate user using a stolen ID, password, etc.	organization must protect is being handled	
A violation of regulations established for data management in cyberspace occurs	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Impersonation of a legitimate user using a stolen ID, password, etc.	- They have not prescribed the procedure necessary to handle data	CPS.GV-3
A violation of regulations established for data management in cyberspace occurs	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Impersonation of a legitimate user using a stolen ID, password, etc.	- They have not checked whether the way in which data is handled meets the conditions of necessary procedure	CPS.DS-14
A violation of regulations established for data management in cyberspace occurs	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Impersonation of a legitimate user using a stolen ID, password, etc.	- Personal information is dispersed and stored in multiple organizations and systems	CPS.SC-3 CPS.SC-6
A violation of regulations established for data management in cyberspace occurs	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Impersonation of a legitimate user using a stolen ID, password, etc.	Each individual organization has not identified that the data they handle is the specific type of data that requires protection	CPS.DS-1
Data is tampered with on the communication channels between IoT devices and cyberspace	- Attacks by third parties who tamper with data on communications channels	- The company does not check to ensure that features to detect or prevent tampering are installed when procuring new devices	CPS.DS-15 CPS.SC-4
Obtains incorrect analysis results due to malfunction of the data processing / analysis system	- Input data outside the permissible range that exploits security vulnerabilities in a data processing / analysis system to infect it with malware, or contains attack codes directed at the data processing / analysis system	- The company does not check the organization that processes / analyzes data or the safety or reliability of systems, etc. prior to or after concluding an agreement	CPS.SC-2
Obtains incorrect analysis results due to malfunction of the data processing / analysis system	- Input data outside the permissible range that exploits security vulnerabilities in a data processing / analysis system to infect it with malware, or contains attack codes directed at the data processing / analysis system	- The company does not check the organization that processes / analyzes data or the safety or reliability of systems, etc. prior to or after concluding an agreement	CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8
Obtains incorrect analysis results due to malfunction of the data processing / analysis system	- Input data outside the permissible range that exploits security vulnerabilities in a data processing / analysis system to infect it with malware, or contains attack codes directed at the data processing / analysis system	- The system that processes / analyzes data is not securely configured	CPS.CM-6 CPS.CM-7 CPS.IP-1 CPS.IP-2 CPS.IP-10 CPS.MA-1 CPS.MA-2

			CPS.PT-2 CPS.RA-2
Obtains incorrect analysis results due to malfunction of the data processing / analysis system	- Input data outside the permissible range that exploits security vulnerabilities in a data processing / analysis system to infect it with malware, or contains attack codes directed at the data processing / analysis system	- Data is not sufficiently protected in the system	CPS.DS-2 CPS.DS-3 CPS.DS-4
Obtains incorrect analysis results due to malfunction of the data processing / analysis system	- Input data outside the permissible range that exploits security vulnerabilities in a data processing / analysis system to infect it with malware, or contains attack codes directed at the data processing / analysis system	The data to be entered is not sufficiently reviewed	CPS.CM-3 CPS.CM-4
Obtains incorrect analysis results due to malfunction of the data processing / analysis system	- Input data outside the permissible range that exploits security vulnerabilities in a data processing / analysis system to infect it with malware, or contains attack codes directed at the data processing / analysis system	- There is no mechanism in place for early and prompt detection and resolution of security failures in place in the system	CPS.AE-1 CPS.CM-1 CPS.CM-5 CPS.PT-1 CPS.RP-1
A malicious user remotely gains unauthorized access to a system that controls an IoT device, and enters unauthorized input to device to make the system operate in an unpredictable manner.	- Preys on the security vulnerabilities to infect a system with malware / spoofs an authorized user by using a stolen ID or password, etc. /sends unauthorized commands to an IoT device from the system that controls the device	- The company does not have an understanding of the state of security protection measures (such as software configurations or application of patches) in place for the system that controls IoT devices	CPS.CM-6
A malicious user remotely gains unauthorized access to a system that controls an IoT device, and enters unauthorized input to device to make the system operate in an unpredictable manner.	- Preys on the security vulnerabilities to infect a system with malware / spoofs an authorized user by using a stolen ID or password, etc. /sends unauthorized commands to an IoT device from the system that controls the device	- There is not enough control of access to system administration authority	CPS.AC-5 CPS.AC-6
A malicious user remotely gains unauthorized access to a system that controls an IoT device, and enters unauthorized input to device to make the system operate in an unpredictable manner.	- Preys on the security vulnerabilities to infect a system with malware / spoofs an authorized user by using a stolen ID or password, etc. /sends unauthorized commands to an IoT device from the system that controls the device	- Vulnerabilities in the system that should be addressed are not handled properly	CPS.CM-6 CPS.CM-7 CPS.IP-2 CPS.MA-1 CPS.MA-2 CPS.RA-2
A malicious user remotely gains unauthorized access to a system that controls an IoT device, and enters unauthorized input to device to make the system operate in an unpredictable manner.	- Preys on the security vulnerabilities to infect a system with malware / spoofs an authorized user by using a stolen ID or password, etc. /sends unauthorized commands to an IoT device from the system that controls the device	- Countermeasure procedures following a malfunction detected in IoT equipment have not been defined	CPS.RP-1
Data one’s own organization must protect is leaked from domains (data processing / analysis) managed by other related organizations	- Data processing managed by other organizations / Malware infection that exploits security vulnerabilities in the analysis system / Data processing managed by other organizations / A	- The company does not check the organization that processes / analyzes data or the safety or reliability of systems, etc. prior	CPS.SC-2 CPS.SC-3 CPS.SC-4 CPS.SC-6

	physical intrusion by an unauthorized entity into the analysis area / Spoofing an authorized user by use of stolen IDs or passwords / Acts to inappropriately remove data that must be protected by an entity of another organization	to or after concluding an agreement	CPS.SC-7 CPS.SC-8
Data one’s own organization must protect is leaked from domains (data processing / analysis) managed by other related organizations	- Data processing managed by other organizations / Malware infection that exploits security vulnerabilities in the analysis system / Data processing managed by other organizations / A physical intrusion by an unauthorized entity into the analysis area / Spoofing an authorized user by use of stolen IDs or passwords / Acts to inappropriately remove data that must be protected by an entity of another organization	- The company does not check the reliability of personnel from the organization contracted to process / analyze data prior to or after concluding an agreement	CPS.SC-5
Data one’s own organization must protect is leaked from domains (data processing / analysis) managed by other related organizations	- Data processing managed by other organizations / Malware infection that exploits security vulnerabilities in the analysis system / Data processing managed by other organizations / A physical intrusion by an unauthorized entity into the analysis area / Spoofing an authorized user by use of stolen IDs or passwords / Acts to inappropriately remove data that must be protected by an entity of another organization	- Information that our organization should protect is dispersed and stored in multiple organizations and systems without uniform security standards	CPS.SC-3 CPS.SC-6
Data our organization must protect is leaked from the domain (data storage) managed by another related organization	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- The company does not check the organization that stores data or the safety of systems, etc. prior to or after concluding an agreement	CPS.SC-2 CPS.SC-3 CPS.SC-6 CPS.SC-7 CPS.SC-8
Data our organization must protect is leaked from the domain (data storage) managed by another related organization	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- The company does not verify the reliability of personnel from the organization contracted to process data prior to or after concluding an agreement	CPS.SC-5
Data our organization must protect is leaked from the domain (data storage) managed by another related organization	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized	- Information that our organization should protect is dispersed and stored in multiple organizations and systems without uniform security standards	CPS.SC-3 CPS.SC-6

	user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected		
Data that must be protected by our organization is tampered with while it is used by another related organization	- Spoofing an authorized user by use of stolen IDs or passwords / Attacks by a third party who tampers with data on communication channels	- Data on communication channels is not sufficiently protected	CPS.DS-3 CPS.DS-4
Data that must be protected by our organization is tampered with while it is used by another related organization	- Spoofing an authorized user by use of stolen IDs or passwords / Attacks by a third party who tampers with data on communication channels	- There is no mechanism in place to detect tampering of data in use	CPS.DS-11
Data that must be protected by our organization is tampered with while it is stored by another related organization	- Spoofing an authorized user by use of stolen IDs or passwords	- There is no mechanism in place to detect tampering of stored data	CPS.DS-11
A security incident at another related organization prevents appropriate continuity of business at our organization	All threats	- The organization has not assessed the degree to which our physical things, systems and data are linked to other organizations in cyberspace	CPS.AE-1 CPS.AM-4 CPS.AM-5 CPS.CM-5 CPS.CM-6
A security incident at another related organization prevents appropriate continuity of business at our organization	All threats	- The company has not assessed the degree to which our organization is linked in physical space with, or where the boundaries of responsibility lie, with other organizations (such as suppliers)	CPS.AM-7 CPS.BE-1 CPS.BE-3 CPS.RM-1
A security incident at another related organization prevents appropriate continuity of business at our organization	All threats	- People from our organization are unable to take appropriate action when a security incident occurs at another organization	CPS.AT-1 CPS.AT-3 CPS.RP-2
A security incident at another related organization prevents appropriate continuity of business at our organization	All threats	- There is no established procedure to collaborate with other related organizations in responding to a security incident	CPS.RP-2
Physical wrongdoing committed on measuring functions results in transmission of inaccurate data	- Physical wrongdoing committed on measuring equipment by people with malicious intent outside our organization	- When procuring IoT devices, no one checks to ensure measurement security is taken into consideration	CPS.SC-4 CPS.SC-6 CPS.DS-15
Physical wrongdoing committed on measuring functions results in transmission of inaccurate data	- Physical wrongdoing committed on measuring equipment by people with malicious intent outside our organization	- Physical security countermeasures for monitoring, access controls, etc. to the area where IoT equipment is installed is not performed	CPS.AC-2 CPS.CM-2 CPS.IP-5
The system that processes data stops whether under attack or not	- Providing services through a system with low product quality and reliability	- The company does not check the reliability of the organization and systems of service suppliers prior to or after concluding an agreement	CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8

The system that processes data stops whether under attack or not	- Providing services through a system with low product quality and reliability	- Adequate resources (processing capabilities, communication bandwidth, storage capacity) for systems - including IoT equipment - are not secured	CPS.DS-6 CPS.DS-7 CPS.IP-4
The system that processes data stops whether under attack or not	- Providing services through a system with low product quality and reliability	- The company does not check the reliability of the organization and systems of service suppliers prior to or after concluding an agreement	CPS.SC-2
Malicious users spoof an authorized user to gain unauthorized internal access to the IoT device to make the system operate in an unpredictable manner	- Spoofing an authorized host by using a stolen ID, etc. - Unauthorized access that maliciously uses vulnerable protocol that deploys no security measures	- Do not review whether the network is used appropriately	CPS.AE-1 CPS.CM-1 CPS.PT-1
Malicious users spoof an authorized user to gain unauthorized internal access to the IoT device to make the system operate in an unpredictable manner	- Spoofing an authorized host by using a stolen ID, etc. - Unauthorized access that maliciously uses vulnerable protocol that deploys no security measures	- The settings in use are not strong enough from a security perspective (passwords, ports, etc.)	CPS.IP-1 CPS.PT-2
Malicious users spoof an authorized user to gain unauthorized internal access to the IoT device to make the system operate in an unpredictable manner	- Spoofing an authorized host by using a stolen ID, etc. - Unauthorized access that maliciously uses vulnerable protocol that deploys no security measures	- There is not enough control of access to communication recipients	CPS.AC-4 CPS.AC-7 CPS.AC-8 CPS.AC-9
Malicious users spoof an authorized user to gain unauthorized internal access to the IoT device to make the system operate in an unpredictable manner	- Spoofing an authorized host by using a stolen ID, etc. - Unauthorized access that maliciously uses vulnerable protocol that deploys no security measures	- There is no procedure in place to configure security in IoT devices	CPS.IP-1
Malicious users spoof an authorized user to gain unauthorized internal access to the IoT device to make the system operate in an unpredictable manner	- Spoofing an authorized host by using a stolen ID, etc. - Unauthorized access that maliciously uses vulnerable protocol that deploys no security measures	- Countermeasure procedures following a malfunction detected in IoT equipment have not been defined	CPS.RP-1
Operates in a manner that obstructs safety whether it is operating normally or malfunctioning	- Command injection attack by unauthorized entities - Input data outside the capacity permitted from cyberspace - Tampering with control signals by malware	- When procuring devices, the company does not check whether they are equipped for safety	CPS.PT-3 CPS.RA-4 CPS.SC-4 CPS.SC-7 CPS.SC-8
Operates in a manner that obstructs safety whether it is operating normally or malfunctioning	- Command injection attack by unauthorized entities - Input data outside the capacity permitted from cyberspace - Tampering with control signals by malware	- There is no system in place to verify entered data	CPS.CM-3
Operates in a manner that obstructs safety whether it is operating normally or malfunctioning	- Command injection attack by unauthorized entities - Input data outside the capacity permitted from cyberspace - Tampering with control signals by malware	- The security instrumentation does not take into consideration use on a running system.	CPS.RA-4 CPS.RA-6

Operates in a manner that obstructs safety whether it is operating normally or malfunctioning	- Command injection attack by unauthorized entities - Input data outside the capacity permitted from cyberspace - Tampering with control signals by malware	- There is no procedure in place when symptoms are discovered that could be problematic for safety	CPS.RP-1
When a security incident occurs on a channel through which products or services are provided, device failures and other unintended degradation in quality occurs	- Unauthorized tampering / insertion of forged products that imitate authorized devices by people with malicious intent from inside or outside our organization	- No procedure is in place to assess the suitability of a product or service at the time of procurement	CPS.DS-11 CPS.DS-12 CPS.DS-13
When a security incident occurs on a channel through which products or services are provided, device failures and other unintended degradation in quality occurs	- Unauthorized tampering / insertion of forged products that imitate authorized devices by people with malicious intent from inside or outside our organization	- When the company is procuring a product or service, they do not review it to determine whether it is reliable	CPS.SC-3 CPS.SC-4 CPS.SC-7 CPS.SC-8
When a security incident occurs on a channel through which products or services are provided, device failures and other unintended degradation in quality occurs	- Unauthorized tampering / insertion of forged products that imitate authorized devices by people with malicious intent from inside or outside our organization	- Personnel involved in procurement at their own organization are not sufficiently aware of the security risks associated with procurement.	CPS.AT-1
When a security incident occurs on a channel through which products or services are provided, device failures and other unintended degradation in quality occurs	- Unauthorized tampering / insertion of forged products that imitate authorized devices by people with malicious intent from inside or outside our organization	- There is not enough physical security for the products and services procured	CPS.DS-8 CPS.SC-4
Vulnerabilities are maliciously exploited to gain unauthorized internal access to the IoT device and make the system operate in an unpredictable manner	- Infections with malware that exploit security vulnerabilities in IoT devices using attack tools	- Vulnerability and threat information for the IoT devices in use is collected and analyzed, but the company does not respond appropriately.	CPS.MA-1 CPS.MA-2 CPS.MA-3
Vulnerabilities are maliciously exploited to gain unauthorized internal access to the IoT device and make the system operate in an unpredictable manner	- Infections with malware that exploit security vulnerabilities in IoT devices using attack tools	- The IoT devices in use are not equipped with enough security features	CPS.DS-15 CPS.RA-4 CPS.RA-6 CPS.SC-4
Vulnerabilities are maliciously exploited to gain unauthorized internal access to the IoT device and make the system operate in an unpredictable manner	- Infections with malware that exploit security vulnerabilities in IoT devices using attack tools	- The organization does not have an understanding of the state of security (such as software configuration information, and application of patches) of its own IoT devices connected to information systems and industrial control systems	CPS.AM-1
Vulnerabilities are maliciously exploited to gain unauthorized internal access to the IoT device and make the system operate in an unpredictable manner	- Infections with malware that exploit security vulnerabilities in IoT devices using attack tools	- There is no procedure in place at the time of procurement to check whether an item is equipped with an appropriate level of security features	CPS.DS-15 CPS.RA-4 CPS.RA-6 CPS.SC-4

Vulnerabilities are maliciously exploited to gain unauthorized internal access to the IoT device and make the system operate in an unpredictable manner	- Infections with malware that exploit security vulnerabilities in IoT devices using attack tools	- Countermeasure procedures following a malfunction detected in IoT equipment have not been defined	CPS.RP-1
Vulnerabilities are maliciously exploited to gain unauthorized internal access to the IoT device and make the system operate in an unpredictable manner	- Infections with malware that exploit security vulnerabilities in IoT devices using attack tools	- The organization does not have an understanding of the state of security (such as software configuration information, and application of patches) of its own IoT devices connected to information systems and industrial control systems	CPS.CM-6 CPS.IP-1 CPS.IP-2
Vulnerabilities are maliciously exploited to gain unauthorized internal access to the IoT device and make the system operate in an unpredictable manner	- Infections with malware that exploit security vulnerabilities in IoT devices using attack tools	- Vulnerability and threat information for the IoT devices in use is collected and analyzed, but the company does not respond appropriately.	CPS.IP-7 CPS.IP-8 CPS.IP-10 CPS.RA-2
An IoT device of low quality and reliability is connected to the network and sends an error and inaccurate data, or sends data to an unintended recipient.	- Network connection of IoT devices with low quality or reliability / Insertion of forged products that imitate authorized devices	- When the company is procuring an IoT device, no one reviews the procured product to determine whether it is reliable	CPS.SC-2 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8
An IoT device of low quality and reliability is connected to the network and sends an error and inaccurate data, or sends data to an unintended recipient.	- Network connection of IoT devices with low quality or reliability / Insertion of forged products that imitate authorized devices	- No one is checking to ensure that the IoT devices and software that are running are authorized products	CPS.DS-13
An IoT device of low quality and reliability is connected to the network and sends an error and inaccurate data, or sends data to an unintended recipient.	- Network connection of IoT devices with low quality or reliability / Insertion of forged products that imitate authorized devices	- Cannot prevent connections to the network (wired or wireless) from unauthorized devices	CPS.AC-2 CPS.AC-3 CPS.CM-6
An IoT device of low quality and reliability is connected to the network and sends an error and inaccurate data, or sends data to an unintended recipient.	- Network connection of IoT devices with low quality or reliability / Insertion of forged products that imitate authorized devices	- Appropriately detects unauthorized communications to areas outside the organization, but cannot block or otherwise respond to such	CPS.DS-9 CPS.CM-1 CPS.CM-6
An IoT device of low quality and reliability is connected to the network and sends an error and inaccurate data, or sends data to an unintended recipient.	- Network connection of IoT devices with low quality or reliability / Insertion of forged products that imitate authorized devices	- Not equipped with a mechanism to confirm whether a device that connects to cyberspace and authorized devices is an authorized device or not	CPS.AC-1 CPS.DS-13
An IoT device of low quality and reliability is connected to the network and sends an error and inaccurate data, or sends data to an unintended recipient.	- Network connection of IoT devices with low quality or reliability / Insertion of forged products that imitate authorized devices	- When the company is procuring an IoT device, there is no procedure in place to review whether the procured product is reliable	CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8

It cannot be equipped with the standardized security measures prescribed by legal systems	All threats	- The organization is either not aware of the legal systems to which it must adhere, or it has not formulated or does not enforce any rules within the organization that comply with the legal system	CPS.DP-2 CPS.GV-2
It cannot be equipped with the standardized security measures prescribed by legal systems	All threats	- The organization is either not aware of the legal systems to which it must adhere, or it does not adhere to rules within the organization that comply with the legal system	CPS.AT-1
It cannot be equipped with the standardized security measures prescribed by legal systems	All threats	- Items of the type for which the legal systems oblige an organization to have a consistent standard of protection are not receiving the standard of protection required	CPS.GV-2
It cannot be equipped with the standardized security measures prescribed by legal systems	All threats	- Systems of the type for which the legal systems oblige an organization to have a consistent standard of protection are not receiving the standard of protection required	CPS.GV-2
It cannot be equipped with the standardized security measures prescribed by legal systems	All threats	- The nature of the procedures prescribed inside the organization does not comply with the relevant legal systems	CPS.GV-2
It cannot be equipped with the standardized security measures prescribed by legal systems	All threats	- Data of the type for which the legal systems oblige an organization to have a consistent standard of protection are not receiving the standard of protection required	CPS.GV-2
There are no security requirements set or response procedures in place for highly confidential data shared among only some stakeholders	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Internal fraud by an authorized user - Spoofing of a legitimate user using a stolen ID, password, etc.	- There is not sufficient awareness of regulations, etc. for the necessary data protections that require a response	CPS.GV-3
There are no security requirements set or response procedures in place for highly confidential data shared among only some stakeholders	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Internal fraud by an authorized user - Spoofing of a legitimate user using a stolen ID, password, etc.	- Stakeholders are not sufficiently aware of how the security of data their own organization must protect is being handled	CPS.AT-1 CPS.AT-3
There are no security requirements set or response procedures in place for highly confidential data shared among only some stakeholders	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Internal fraud by an authorized user - Spoofing of a	- They have not prescribed the procedure necessary to handle data	CPS.GV-3

	legitimate user using a stolen ID, password, etc.		
There are no security requirements set or response procedures in place for highly confidential data shared among only some stakeholders	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Internal fraud by an authorized user - Spoofing of a legitimate user using a stolen ID, password, etc.	- They have not checked whether the way in which data is handled meets the conditions of necessary procedure	CPS.DS-14
There are no security requirements set or response procedures in place for highly confidential data shared among only some stakeholders	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Internal fraud by an authorized user - Spoofing of a legitimate user using a stolen ID, password, etc.	- The design of the system that handles data does not correspond to the confidentiality of that data	CPS.AC-7 CPS.AC-9 CPS.DS-2
There are no security requirements set or response procedures in place for highly confidential data shared among only some stakeholders	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Internal fraud by an authorized user - Spoofing of a legitimate user using a stolen ID, password, etc.	- Personal information is dispersed and stored in multiple organizations and systems	CPS.SC-3 CPS.SC-6
There are no security requirements set or response procedures in place for highly confidential data shared among only some stakeholders	- A malware infection that exploits a vulnerability on the security in the data management system - Physical intrusion of an unauthorized entity into the data storage area - Internal fraud by an authorized user - Spoofing of a legitimate user using a stolen ID, password, etc.	Each individual organization has not identified that the data they handle is the specific type of data that requires protection	CPS.DS-1
Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- Vulnerabilities that should be addressed on the organization’s own system are neglected	CPS.CM-6 CPS.CM-7
Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	Entities requesting access to stored information are not identified or verified using methods based on the level of confidentiality of the information, or other conditions	CPS.AC-1 CPS.AC-5 CPS.AC-6 CPS.AC-9 CPS.GV-3
Data that must be protected from other related organizations is leaked from	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an	- Physical security countermeasures for monitoring, access controls,	CPS.AC-2 CPS.IP-5 CPS.PT-2

an area (data storage) the organization manages	unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	etc. to the area where IoT equipment and servers are installed are not implemented	
Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- Responsibilities within the organization regarding the management of data to be protected are unclear	CPS.AM-6
Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- Physical security countermeasures for monitoring, access controls, etc. to the area where IoT equipment and servers are installed are not implemented	CPS.CM-2
Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- There is no mechanism in place for early and prompt detection and resolution of security failures in place in the system	CPS.AE-1 CPS.CM-1 CPS.CM-5 CPS.PT-1 CPS.RP-1
Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- There are no procedures in place to check on the class of confidentiality of data consigned for management by another organization and the security measures such requires	CPS.DS-1
Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- The classifications that correspond to protecting data from another organization that the company is consigned to manage are not clear	CPS.GV-3

Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- Protection of information is not implemented according to the stipulated confidentiality classifications	CPS.AC-7 CPS.SC-6
Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- The system that stores data from other related organizations that must be protected is not securely configured	CPS.IP-1
Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- Protection of information is not implemented according to the stipulated confidentiality classifications	CPS.DS-2 CPS.DS-3 CPS.DS-4 CPS.DS-5 CPS.DS-9
Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- The system that stores data from other related organizations that must be protected is not securely configured	CPS.PT-2
Data that must be protected from other related organizations is leaked from an area (data storage) the organization manages	- Malware infection that exploits security vulnerabilities in data storage / A physical intrusion by an unauthorized entity into a data storage area managed by another organization/ Spoofing an authorized user by use of stolen IDs or passwords / Removal by a malicious entity in our organization of data that must be protected	- Vulnerabilities that should be addressed on the organization’s own system are neglected	CPS.IP-2 CPS.IP-10 CPS.MA-1 CPS.MA-2 CPS.RA-2
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of	- Risk management involving other organizations that should be involved regarding security is not conducted based on appropriate procedures	CPS.AM-6

	network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user		
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- The security and network connection status of objects are not managed (e.g.: asset inventories and monitoring)	CPS.AC-1 CPS.AE-1 CPS.AM-1 CPS.AM-5 CPS.CM-5 CPS.CM-6
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Technical countermeasures based on the organization’s risks are either not implemented or their implementation is not verified	CPS.RA-1 CPS.RA-3 CPS.RA-4 CPS.RA-5
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Risk management involving other organizations that should be involved regarding security is not conducted based on appropriate procedures	CPS.BE-2
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Technical countermeasures based on the organization’s risks are either not implemented or their implementation is not verified	CPS.RA-6 CPS.RM-2
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an	- Vulnerabilities that should be addressed on the organization’s own system are neglected	CPS.CM-6 CPS.CM-7 CPS.IP-2 CPS.IP-10 CPS.MA-1 CPS.MA-2 CPS.RA-2

	authorized user - Internal fraud by an authorized user		
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- The system that stores data that must be protected is not securely configured.	CPS.IP-1 CPS.PT-2
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Risk management involving other organizations that should be involved regarding security is not conducted based on appropriate procedures	CPS.SC-1
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	Entities requesting access to stored information are not identified or verified using methods based on the level of confidentiality of the information, or other conditions	CPS.GV-3
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	Entities requesting access to stored information are not identified or verified using methods based on the level of confidentiality of the information, or other conditions	CPS.AC-1 CPS.AC-5 CPS.AC-6 CPS.AC-9
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Physical security countermeasures for monitoring, access controls, etc. to the area where IoT equipment and servers are installed are not implemented	CPS.AC-2 CPS.CM-2 CPS.IP-5 CPS.PT-2

Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Risk management involving other organizations that should be involved regarding security is not conducted based on appropriate procedures	CPS.SC-2
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- There is no mechanism in place for early and prompt detection and resolution of security failures in place in the system	CPS.AE-1 CPS.CM-1 CPS.CM-3 CPS.CM-5 CPS.PT-1 CPS.RP-1
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- The classifications that correspond to protecting data that the company manages are not clear.	CPS.GV-3
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Protection of information is not implemented according to the stipulated confidentiality classifications	CPS.DS-2 CPS.DS-3 CPS.SC-6
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Risk management involving other organizations that should be involved regarding security is not conducted based on appropriate procedures	CPS.IP-3

Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Protection of information is not implemented according to the stipulated confidentiality classifications	CPS.DS-4 CPS.DS-5 CPS.DS-9
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Adequate procedures for security-related risk management are not established	CPS.GV-1 CPS.GV-4
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Adequate procedures for security-related risk management are not established	CPS.RM-1 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Individuals are not sufficiently aware of the security and safety risks in which they are involved.	CPS.AT-1
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Adequate procedures for security-related risk management are not established	CPS.IP-7 CPS.SC-10 CPS.SC-11

Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Individuals are not sufficiently aware of the security and safety risks in which they are involved.	CPS.AT-3
Data that should be protected is leaked from areas managed by our organization	- Infection by malware that exploits security vulnerabilities in a system - Injection attack that targets entry confirmation (SQL injection and XSS are examples) - Physical intrusion by an unauthorized entity into an area that requires monitoring/protection of network communications - Using stolen IDs or passwords to spoof an authorized user - Internal fraud by an authorized user	- Governance of risks related to the security and safety of individuals is insufficient	CPS.SC-5 CPS.IP-9
Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- Adequate procedures for security-related risk management are not established	CPS.SC-7 CPS.SC-10 CPS.SC-11 CPS.IP-7
Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- Communication paths and data on communication channels is not sufficiently protected	CPS.DS-3 CPS.DS-4
Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- There is no mechanism in place to detect tampering of data handled by the organization	CPS.DS-11

Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- Risk management involving other organizations that should be involved regarding security is not conducted based on appropriate procedures	CPS.AM-6 CPS.BE-2 CPS.IP-3 CPS.SC-1 CPS.SC-2
Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- Individuals are not sufficiently aware of the security and safety risks in which they are involved	CPS.AT-1 CPS.AT-3
Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- Governance of risks related to the security and safety of individuals is insufficient	CPS.IP-9 CPS.SC-5
Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- The security and network connection status of objects constituting the information system and industrial control systems are not managed (e.g. asset inventories and monitoring)	CPS.AC-1 CPS.AE-1 CPS.AM-1 CPS.AM-5 CPS.CM-5 CPS.CM-6
Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- Technical countermeasures based on the organization’s risks are either not implemented or their implementation is not verified	CPS.RA-1 CPS.RA-3 CPS.RA-4 CPS.RA-5 CPS.RA-6 CPS.RM-2

Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- The system that stores data that must be protected is not securely configured.	CPS.IP-1 CPS.PT-2
Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- Entities requesting access to stored information are not identified or verified using methods based on the level of confidentiality of the information, or other conditions	CPS.AC-1 CPS.AC-5 CPS.AC-6 CPS.AC-9 CPS.GV-3
Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- The system is not equipped with a mechanism that can promptly detect and addressing network abnormalities (e.g. spoofing and message tampering) in the early stages	CPS.AE-3 CPS.CM-3 CPS.DP-4
Data that must be protected in areas managed by our organization is tampered with	- Using stolen IDs or passwords to spoof an authorized user - Attack by a third party that tampers with data on communication channels - Infection by malware that exploits security vulnerabilities in a system - Internal fraud by an authorized user - Physical intrusion by an unauthorized entity into an area that requires protection - Physical damage of media containing data that requires protection	- Adequate procedures for security-related risk management are not established	CPS.GV-1 CPS.GV-4 CPS.RM-1 CPS.SC-3 CPS.SC-4 CPS.SC-6
Another related organization cannot continue business properly due to a security incident of the organization	All threats	- The organization has not assessed the degree to which our physical things, systems and data are linked to other organizations in cyberspace	CPS.AE-1 CPS.AM-4 CPS.AM-5 CPS.CM-5 CPS.CM-6
Another related organization cannot continue business properly due to a security incident of the organization	All threats	- The company has not assessed the degree to which our organization is linked in physical space with, or where the boundaries of responsibility lie, with other organizations (such as suppliers)	CPS.AM-7 CPS.BE-1 CPS.BE-3 CPS.RM-1

Another related organization cannot continue business properly due to a security incident of the organization	All threats	- A person from another organization cannot take appropriate action when a security event of the organization occurs	CPS.AT-2 CPS.AT-3 CPS.RP-2 CPS.SC-9
Another related organization cannot continue business properly due to a security incident of the organization	All threats	- Goods (products) and services harmed by a security event	CPS.RP-4
Another related organization cannot continue business properly due to a security incident of the organization	All threats	- Records of goods (products) of the organization or provided by the organization (e.g. date of manufacture, identification number, supplier) are not maintained	CPS.AM-2 CPS.AM-3
Another related organization cannot continue business properly due to a security incident of the organization	All threats	- There is no established procedure to collaborate with other related organizations in responding to a security incident	CPS.AE-4 CPS.RP-2
The organization cannot continue business properly due to a security incident of the organization	All threats	- A system has not been established to respond appropriately to security incidents	CPS.IM-1 CPS.IM-2
The organization cannot continue business properly due to a security incident of the organization	All threats	- Appropriate action cannot be taken when a security incident occurs	CPS.AT-1 CPS.AT-3 CPS.RP-1
The organization cannot continue business properly due to a security incident of the organization	All threats	- The business scope (products, etc.) of the organization cannot be specified due to harm by a security incident	CPS.AM-2 CPS.AM-3 CPS.AN-1
The organization cannot continue business properly due to a security incident of the organization	All threats	- Equipment, etc. to properly detect security incidents is not installed or is not operating properly	CPS.AE-3 CPS.CM-1
The organization cannot continue business properly due to a security incident of the organization	All threats	- A system to accurately detect security events has not been established	CPS.AE-2
The organization cannot continue business properly due to a security incident of the organization	All threats	- Procedures for responding to security incidents in the organization have not been formulated	CPS.AE-5 CPS.AN-1 CPS.AN-2 CPS.AN-3 CPS.MI-1 CPS.RP-1
The organization cannot continue business properly due to a security incident of the organization	All threats	- Security incidents are not positioned in the business continuity plan, and the business continuity of the organization is hindered when a security incident occurs	CPS.CO-1 CPS.CO-2 CPS.RP-3
The organization cannot continue business properly due to a security incident of the organization	All threats	- A system to accurately detect security events has not been established	CPS.RA-2

The organization cannot continue business properly due to a security incident of the organization	All threats	- Security incidents are not positioned in the business continuity plan, and the business continuity of the organization is hindered when a security incident occurs	CPS.CO-3
The organization cannot continue business properly due to a security incident of the organization	All threats	- Data which is necessary for business continuity when a security incident occurs is not properly prepared, or the data is prepared but not functioning properly	CPS.AT-1 CPS.AT-2 CPS.IP-4 CPS.RP-3
The organization cannot continue business properly due to a security incident of the organization	All threats	- A system to accurately detect security events has not been established	CPS.AE-2 CPS.DP-1 CPS.DP-2 CPS.DP-3 CPS.DP-4 CPS.RA-2

Appendix B "List of Security Measures"

Security measure requirement ID	Measure requirements	Category
CPS.AC-1	- Establish and implement procedures for issuing, managing, confirming, revoking, and auditing the identification information and authentication information of approved goods, people and procedures.	Governance Service City OS Asset
CPS.AC-2	- Implement physical security measures such as locking areas where there are IoT devices and servers, entrance and exit management, introduction of body authentication, etc., installation of surveillance cameras, and inspection of belongings and body weight.	Governance Service City OS Asset
CPS.AC-3	- Properly authenticate wireless connection destinations (users, IoT devices, servers, etc.).	Service City OS Asset
CPS.AC-4	- Prevent unauthorized login to IoT devices and servers, etc. by implementing functions such as lockout after a certain number of failed login authentications and providing a time interval for re-login until security can be ensured.	Service City OS Asset
CPS.AC-5	- Appropriately divide duties and areas of responsibility (e.g. users and system administrators).	Governance Service City OS
CPS.AC-6	- Adopt a reliable authentication method (e.g. multi-factor authentication that combines more than one authentication function), taking into account the potential risks when a privileged user logs in to the system via a network.	Service City OS
CPS.AC-7	- Define the data flow control policy and properly allocate the network according to it (e.g. development and test environment and actual operation environment, environment including IoT devices and other environments in the organization), etc. to protect the integrity of the network.	Service City OS Asset
CPS.AC-8	- Limit the communication performed by IoT devices and servers to communication with identified entities (people, goods, systems, etc.) in the appropriate order.	Service City OS Asset
CPS.AC-9	- Authenticate and authorize logical access by IoT devices and users to components (goods, systems, etc.) in a way that is compatible with transaction risks (personal security, privacy risks and other organizational risks).	Service City OS Asset
CPS.AE-1	- Identify and implement procedures to identify and manage network operation baselines and the expected flow of information between people, goods and systems.	Governance Service City OS Asset
CPS.AE-2	- Appoint a security management officer, launch a security response organization (SOC/CSIRT), and establish a system to detect, analyze, and respond to security events within the organization.	Governance
CPS.AE-3	- Accurately identify security incidents by implementing procedures to analyze security event correlation and analysis against external threat information.	Governance City OS
CPS.AE-4	- Identify the impact of security events, including the impact on other organizations involved.	Governance
CPS.AE-5	- Define the criteria for determining the level of risk of security events.	Governance
CPS.AM-1	- Create a list of the hardware and software that make up the system and their management information (e.g. name, version, network address, manager, license information), and manage them appropriately.	Service City OS Asset
CPS.AM-2	- Specify specific methods for ensuring traceability according to the importance in the supply chain of the goods produced by the organization.	Governance Service City OS
CPS.AM-3	- Create records of the time of production and its status, etc., according to the importance, and maintain and operate internal rules for records of production activities to keep them for a fixed period.	Governance Service

CPS.AM-4	- Create a communication network configuration diagram and a data flow diagram within the organization, and manage them appropriately.	Governance
CPS.AM-5	- Create a list of external information systems to which the organization's assets are connected and manage them appropriately.	Governance Service City OS Asset
CPS.AM-6	- Classify and prioritize resources (e.g. goods, data, and systems) based on their function, importance and business value, clarify management responsibilities, then communicate this to the organizations and people involved in these organizational resources.	Governance
CPS.AM-7	- Define the cybersecurity roles and responsibilities of the organization and other related organizations.	Governance
CPS.AN-1	- Based on the whole picture of the security incident and the assumed intention of the attacker, understand the impact on the entire society, including the organization and other related organizations.	Governance
CPS.AN-2	- Implement digital forensics after occurrence of a security incident.	Governance
CPS.AN-3	- Classify and store information on detected security incidents based on the degree of security impact and the route of intrusion.	Governance
CPS.AT-1	- Provide appropriate training and education to all personnel in the organization to fulfill their assigned roles and responsibilities to control the occurrence and impact of security incidents, and maintain records.	Governance
CPS.AT-2	- In order that they can appropriately fulfill their roles, provide appropriate training for persons in charge of security management who may be involved with security incidents in the organization and have a high importance in other organizations, implement security education, and maintain those records.	Governance
CPS.AT-3	- Improve the contents of security training and education for organization personnel and personnel of other important related organizations.	Governance
CPS.BE-1	- In the supply chain, identify and share the roles in the organization.	Governance
CPS.BE-2	- Clarify the organization’s previously determined priority business and the security policies and countermeasure standards which are consistent with the organization’s priority business, and share them with people involved in the organization’s transactions (including suppliers and third-party providers, etc.).	Governance
CPS.BE-3	- Identify the dependencies and important functions of the organization and other related organizations which are needed for the organization to continue its business.	Governance
CPS.CM-1	- Implement network monitoring and control, and access monitoring and control at the point of contact between the internal network and the wide area network.	Governance Service City OS
CPS.CM-2	- Consider the importance of IoT devices and servers, etc., and implement setting, recording, and monitoring of appropriate physical access.	Governance Service City OS Asset
CPS.CM-3	- Introduce IoT devices which detect abnormalities and stop operations by comparing specified operation contents with actual operation results. - Verify before operation that information received from cyberspace does not contain malicious code and is within the allowable scope.	Service City OS Asset
CPS.CM-4	- Before operation, confirm the integrity and authenticity of information received from cyberspace.	Service
CPS.CM-5	- Monitor the content of communication with external service providers so that security events can be properly detected.	Asset Service City OS Asset
CPS.CM-6	- In the configuration management of devices, etc., continuously manage software configuration information, network connection status (whether or not there is a network connection, access destination, etc.), and the status of	Governance Service

	transmission and reception of information to and from other organizations, people, goods, and systems.	City OS Asset
CPS.CM-7	- Confirm whether there are vulnerabilities that need to be periodically handled on IoT devices and servers which are managed by the organization.	Service City OS Asset
CPS.CO-1	- Formulate and enact rules for disclosing information after a security incident.	Governance
CPS.CO-2	- Position a business continuity plan in the contingency plan to address the need to restore the organization's social reputation after a security incident.	Governance
CPS.CO-3	- In regard to recovery activities, place the point of communicating recovery activities to the internal and external stakeholders and officers and management team in the business continuity plan and the emergency response plan.	Governance
CPS.DP-1	- To fulfill accountability for explanation of security events, clarify the roles and responsibilities of organizations and service providers when a security event is detected.	Governance
CPS.DP-2	- In monitoring operations, detect security events in accordance with laws, regulations, notifications, and industry standards applicable to each region.	Governance
CPS.DP-3	- As a monitoring task, periodically test whether the function to detect security events operates as intended and verify its validity.	Governance
CPS.DP-4	- Continuously improve the security event detection process.	Governance City OS
CPS.DS-1	- When information to be protected is exchanged between organizations, the security requirements for the protection of the information shall be agreed between the organizations in advance.	Governance City OS
CPS.DS-10	- Verify the integrity of software running on IoT devices and servers at the timing determined by the organization, and prevent unauthorized software from starting.	Service City OS Asset
CPS.DS-11	- Use an integrity check mechanism for information which is transmitted, received or stored.	Governance Service City OS Asset
CPS.DS-12	- Use an integrity check mechanism to verify hardware integrity.	City OS Asset
CPS.DS-13	- Regularly confirm that IoT devices and software are genuine (at startup, etc.).	Governance Service City OS Asset
CPS.DS-14	- Maintain, update, and manage data acquisition sources and processing histories, etc. throughout the life cycle.	Governance
CPS.DS-15	- Use products which take into consideration measurement security in order to ensure the reliability of sensing data by protecting the availability and integrity of measurement.	Governance Asset
CPS.DS-2	- Encrypt and store information in a format with appropriate strength.	Service City OS
CPS.DS-3	- Encrypt the communication path for communication in cyberspace between IoT devices and servers.	Service City OS Asset
CPS.DS-4	- When transmitting and receiving information, encrypt the information itself.	Service City OS
CPS.DS-5	- Throughout their life cycle, securely manage keys which are used for encrypting information data to be transmitted and received and information to be stored.	Service City OS
CPS.DS-6	- Even in the event of a cyberattack such as a denial-of-service attack, secure sufficient resources (e.g., human, goods, systems) in the components so that assets can be properly protected and the effects of the attack can be minimized.	Service City OS Asset

CPS.DS-7	- For IoT devices, communication devices, and lines, etc., do regular quality control, secure spare units and uninterruptible power supplies, perform redundancy, detect failures, replace parts, and update software.	Service City OS Asset
CPS.DS-8	- Use tamper-resistant devices when handling information to be protected or when procuring equipment which has important functions for the organization.	Asset
CPS.DS-9	- In order to prevent inappropriate communication to outside the organization, properly control the transmission to outside the organization of information which must be protected.	Service City OS
CPS.GV-1	- Formulate a security policy, and clarify the security roles and responsibilities of the organization and other related organizations, and methods for sharing information.	Governance
CPS.GV-2	- Develop internal rules that take into account the Act on the Protection of Personal Information, the Unfair Competition Prevention Act, domestic and foreign laws and regulations, and industry guidelines.	Governance
CPS.GV-3	- Accurately grasp the standards for data protection required by various laws and regulations concerning the handling of data shared only between related organizations, develop data classification methods based on each requirement, and appropriately protect data according to the classification.	Governance Service City OS
CPS.GV-4	- Develop strategies and secure resources to properly manage security risks.	Governance
CPS.IM-1	- Learn from the response to security incidents and continuously improve the security operation process.	Governance
CPS.IM-2	- Learn from the response to security incidents, and continuously improve the business continuity plan and emergency response plan.	Governance
CPS.IP-1	- Introduce and operate an initial setting procedure (password, etc.) and setting change management process for IoT devices and servers, etc.	Governance Service City OS Asset
CPS.IP-10	- Create a vulnerability remediation plan and correct the vulnerabilities of components according to the plan.	Governance Service City OS
CPS.IP-2	- Limit the software to be added after the introduction of IoT devices and servers.	Service City OS Asset
CPS.IP-3	- Introduce a system development life cycle for managing systems.	Governance
CPS.IP-4	- Perform periodic system backups of components (IoT devices, communication devices, lines, etc.) and test them.	Service City OS Asset
CPS.IP-5	- Implement physical measures to satisfy policies and rules related to uninterruptible power supplies, fire prevention equipment and flood protection, etc., and the physical operating environment of IoT devices and servers, etc. in the organization.	Service City OS Asset
CPS.IP-6	- When discarding IoT devices and servers, etc., delete all data stored inside as well as the ID (identification key) and important information (private key, electronic certificate, etc.) that uniquely identify a legitimate IoT device or server, and make the device unreadable.	Service City OS Asset
CPS.IP-7	- Learn from security incident responses and from the monitoring, measurement, and assessment of internal and external attacks, and improve the process of protecting assets.	Governance
CPS.IP-8	- Share information about the effectiveness of protection technologies with appropriate partners.	Governance
CPS.IP-9	- Include security-related matters (e.g. invalidation of access authority, examination of employees) in the countermeasures regarding role changes following the transfer of personnel.	Governance

CPS.MA-1	- Appropriately implement and record the history of security-critical updates for IoT devices and servers, etc., using tools which are managed at the required frequency.	Service City OS Asset
CPS.MA-2	- Implement remote maintenance of IoT devices and servers, etc. of the organization with the approval of the owner of the target equipment and system, record logs, and prevent unauthorized access.	Service City OS Asset
CPS.MA-3	- If possible, introduce IoT devices equipped with a remote update mechanism that collectively updates software (OS, drivers, applications) by remote operation.	Asset
CPS.MI-1	- Minimize the spread of damage caused by security incidents and take measures to reduce the impact.	Governance
CPS.PT-1	- In order to properly detect security incidents, determine the target audit records and log records, document them, and implement and review such records.	Governance Service
CPS.PT-2	- Allow only the minimum essential functions of IoT devices and servers by physically or virtually blocking unnecessary network ports, USB and serial ports, etc. on the IoT device or server.	Service City OS Asset
CPS.PT-3	- Introduce IoT devices that implement security according to connection to a network.	City OS
CPS.RA-1	- Identify the vulnerability of the organization's assets and document the list of assets.	Governance Service City OS
CPS.RA-2	- The security response organization (SOC/CSIRT) shall collect, analyze, respond to, and utilize vulnerability information and threat information, etc., from internal and external information sources (internal testing, security information, security researchers, etc.) and establish such process.	Governance Service City OS
CPS.RA-3	- Identify and document conceivable security incidents and their impacts on the organization's assets and their causes.	Governance City OS
CPS.RA-4	- Perform regular risk assessments to confirm that security rules in component management are effective, including implementation methods.	Service City OS Asset
CPS.RA-5	- Consider threats, vulnerabilities, possibilities, and impacts when determining risk.	Governance City OS
CPS.RA-6	- Based on the risk assessment, clearly define the measures to be taken against possible security risks, and document the results of determining the scope and priorities of the measures.	Governance Service City OS Asset
CPS.RM-1	- Confirm the status of implementation of cybersecurity risk management within the organization, and communicate it to the appropriate stakeholders within the organization (e.g. senior management). Also, clarify the responsibilities of the organization and other organizations related to the organization's business (e.g. outsourcing), and establish and implement a process for confirming the status of security risk management implemented by other related organizations.	Governance
CPS.RM-2	- Determine the risk tolerance of the organization from the risk assessment results and the role of the organization in the supply chain.	Governance City OS
CPS.RP-1	- In order to clarify the content, priority, and scope of response after a security incident occurs, define in advance and implement the response procedure (security operation process) of the organization, human, goods, or system after detection of an incident.	Governance
CPS.RP-1	- In order to clarify the content, priority, and scope of response after a security incident occurs, define in advance and implement the response procedure (security operation process) of the organization, human, goods, or system after detection of an incident.	Governance Service City OS
CPS.RP-2	- In the security operation process, determine and operate the procedure and division of roles for coordination with business partners and other related organizations.	Governance

CPS.RP-3	- Position security incidents in the emergency response plan and in the business continuity plan which define response policies and procedures in the event of a natural disaster.	Governance
CPS.RP-4	- Appropriately respond to goods (products) that are expected to have some quality deterioration such as being produced in a facility which is harmed during a security incident.	Service
CPS.SC-1	- Establish security measure standards for the supply chain in consideration of the life cycle of the business relationship, clarify the scope of responsibility, then agree on the contents with the business partner.	Governance
CPS.SC-10	- Formulate and operate procedures to be executed upon termination of contracts with other related organizations such as business partners (e.g. expiration of contract period, end of support).	Governance
CPS.SC-11	- Continuously improve supply chain security measures and related procedures.	Governance
CPS.SC-2	- Identify, prioritize and evaluate organizations and people who play an important role in each layer of the three-layer structure in continuing the business of the organization.	Governance
CPS.SC-3	- When contracting with an external organization, consider the objectives and results of risk management, and confirm that the security management of the other organization conforms to the security requirements of the organization.	Governance Service City OS Asset
CPS.SC-4	- When contracting with an external organization, consider the objectives and results of risk management, and confirm that the products and services provided by the other organization conforms to the security requirements of the organization.	Governance Service City OS Asset
CPS.SC-5	- Develop and operate security requirements for personnel in other related organizations such as business partners, and personnel involved in outsourced operations.	Governance
CPS.SC-6	- Regularly evaluate, using audits, test results, or other forms of evaluation, to verify that other related organizations, such as business partners, are fulfilling their contractual obligations.	Governance
CPS.SC-7	- Develop and operate procedures to be implemented when nonconformity with a contractual matter is found as a result of audits and tests of another related organization such as a business partner.	Governance
CPS.SC-8	- Collect and securely store information (data) to prove that the organization has fulfilled its contractual obligations with other related organizations and individuals, and make it available to the appropriate extent when required.	Governance Service City OS Asset
CPS.SC-9	- Develop and train response processes among personnel involved in incident response activities to ensure incident response activities in the supply chain.	Governance