CCDS-SH02-2021
CCDS-SH03-2021

Security Guidelines for Product Categories

- Smarthomes -

Ver. 1.0

CCDS Security Guidelines WG
Smarthome WG

Revision History

Edition	Date	Description
Ver.0.1	2018/11/26	Newly released as a draft version.
Ver.1.0	2019/10/29	Draft version revised into a new release.

■Trademarks

・All company names, product names and the like in this document are either trademarks or registered trademarks of their respective companies.

■Notice

・Information in this document is that available at the time of publication of this document and is subject to change without notice.

・Duplication or reproduction of the contents of this document without prior permission from the CCDS is strictly prohibited.

Contents

1 Introduction

Safety standards have been formulated separately from each product industry to another to date. As cyber security standards, a standard relating to organizational operations (ISO27001) and a standard relating to security assessment and certification (ISO15408) have been set forth. And recently, even standards targeting control systems for key infrastructures (plants and facilities essential to social infrastructures) (ISO62443) have come into existence.

With the growing popularity of the Internet of Things (IoT) initiative, familiar consumer devices in our lives have come to boast a variety of networking capabilities, threatening more security concerns than ever. In the circumstances, security standards essential to IoT products and services are yet to be fully developed to suit consumer devices. In the meantime, moves are underway in various parts of the U.S. and European nations to explore security standards from industry-specific safety standards (U.K. Code of Practice for Consumer IoT Security [21] and U.S. California State's Regulating Internet of Things (IoT) (Senate Bill No.327, Chapter 886) [1] and others). In Japan as well, concerns over security have loomed to reflect growing urges for deliberation, but specific discussions have launched in very few categories of industry.

It was under the circumstances that the Connected Consumer Device Security Council (CCDS) was inaugurated as a general incorporated association. The activity of the Council has been committed to the goal of crafting an environment in which users can safely use IoT products, by formulating security standards for consumer devices while administering a CCDS certification program designed to verify and validate product compliance with these standards.

While the IoT Security Guidelines [2] compiled on July 5, 2016 by the IoT Acceleration Consortium, the Ministry of Economy and Trade and Industry and the Ministry of Internal Affairs and Communications offers a basic insight into the common issues encompassing comprehensive product fields, the CCDS has worked out this Guidelines to drive design and development efforts directed at security assurance in the individual product categories.

1.1 Status and Issues of Smarthome Security

A smarthome is a dwelling that is connected to the Internet or the like and that is furnished with IoT-compatible housing equipment and home appliances to deliver safe, secure and comfortable living to the homeowner by leveraging information technologies, such as IoT and AI.

IoT devices have an expanding scope of applications as they get closer to our day-to-day lives than ever. For example, if there is a way to control consumer devices installed within one's home from a remote location, then locking of the home, opening and/closing of the shutters and water supply/drainage facilities would be controllable. IoT devices have come into rapid popularity and the pace is expected to hasten even faster in the future. Annual Report 2016: Information and Communications in Japan [3] cited projections by IHI Technology to forecast leaps in the number of consumer devices from about 5.4 billion units worldwide in 2015 to 12.5 billion units, a more than twofold increase, in 2020.
These IoT devices can be connected to the Internet to offer a variety of services, but also threaten potential risks to information security. Since the presence of malware targeting IoT devices has been confirmed, it is feared to risk our lives and properties. The causes of attacks launched at IoT devices can be viewed in two aspects: users and providers. Attacks attributable to users might include, for example, the use of IoT devices without their default settings being changed, use of passwords that can be easily guessed and a lack of knowledge about security. Those attributable to providers might include a product design that grants access to anybody with the default settings and a lack of their assumption of users' concept of security.

In March 2016, Smart-society Development Guidelines [4] was publicized by the Information-technology Promotion Agency, Japan (IPA), an independent administrative agency, to define a general concept of the risks and actions to be taken into consideration by those who develop IoT devices. In July 2016, IoT Security Guidelines compiled by the Ministry of Economy, Trade and Industry, the Ministry of Internal Affairs and Communications and other were publicized to provide providers and users a conceptual approach to exploring security actions for IoT devices, systems and services. Such approach includes, for example, implementing important security updates to IoT devices properly after their initial delivery.

The CCDS is now working to forge a CCDS certification program, which is a security certification plan that encompasses a complete classification of products, including ATMs, IoT gateways, on-board devices and open POS terminals. The program contemplates to assign Certification Mark ★ to those products and services for which Certification Level 1 is defined to specify a minimum set of security requirements to be fulfilled by IoT devices; Certification Mark ★★ or ★★★ to those for which Certification Level 2 or 3 is defined by trade organizations according to specific product categorizations and that have been verified to meet these security requirements through voluntary assessment or third-party certification.

Despite the growing popularity of IoT devices, smarthomes still remain in their budding period and housing companies have only begun to pursue them seriously. While guidelines on smarthome security are yet to be formulated, discussions have been initiated through demonstration testing so far.

In Fiscal 2016, for example, a connected IoT device security verification testbed for smarthomes was built as part of an IoT service creation project driven by the Ministry of Internal Affairs and Communications. In this project, a smarthome testbed environment was fabricated to verify the security of IoT devices used in our day-to-day lives. Findings of this verification work were compiled into IoT security verification guidelines for smarthomes. In Fiscal 2017, the FY2016 Social System Maintenance Project Leveraging Modified IoT (Smarthome Data Utilization Environment Maintenance Promotion Project) was implemented. The project came up with a formulation of Smarthome Field Security and Product Safety Action Guidelines (Checklists).

To work out security guidelines for smarthomes, it would be necessary to presume in what context IoT devices are used. For example, the IoT devices used to protect a user’s life and property and those used to improve the user's comfort or convenience should differ in the security requirements for the system that runs the devices. While a growing number of IoT devices continue to penetrate homes as explained above, some seem to be installed without a full prior review of their security characteristics. For this reason, security standards should be formulated to meet the importance of the objects to be protected with regard to Certification Levels 2 and 3 under the Certification Program defined by the CCDS with a view to authenticating smarthome security, so Certification Marks ★★ and ★★★ will be assigned to services compliant

with these standards.
Users would then be able to check the Certification Mark label appearing on a smarthome service to make certain that the service is a safe and secure service.

This document presents specific action guidelines that reflect components and life cycles specific to the smarthome field based on IoT Security Guidelines [2] compiled by the IoT Acceleration Consortium, and also defines relevant security requirements for the smarthome field in accordance with the Cyber Physical Security Framework (CPSF) [20] developed by Japan's Ministry of Economy, Trade and Industry, U.K. Code of Practice for Consumer IoT Security [21] and U.S. California State's Regulating Internet Of Things (IoT) (Senate Bill No.327, Chapter 886) [1].
Discussions launched in this document focus on topics characteristic of the security actions for the smarthome field. Issues, such as organizational information security management, network security and safety actions and the like are beyond the scope of this Guideline. For information about these topics, the reader is directed to associated guidelines established by other associations.

1.2 Scope of Application

Written mainly for corporate developers who plan, design, construct and operate smarthomes, and services and housing equipment, this Guidelines presents security action policies that should deserve consideration as they go through their life cycles.

1.3 Intended audiences are:

1)Designers, developers, producers and distributors of consumer devices
2)Operations representatives responsible for operating and maintaining housing equipment
3)Smarthome designers, producers and constructors, administrators and site supervisors
4)Operations representatives responsible for operating and maintaining smarthomes

1.4 Glossary

This section gives definitions of the terms used in this document.

Table 1-1: Glossary

Term	Definition
House	A dwelling house, residence or living home. In this document, the term refers to a detached house for general households, rental house, multiple-dwelling house or the like, excluding offices, facilities and shops.
Housing company	A company that planning, sells, designs and constructs houses, such as a housing maker, contractor, builder or design firm. In this document, the term refers to any company that plans, sells, designs or constructs smarthomes.
Smarthome	A house furnished with IoT-compatible housing equipment and home appliances utilizing a communications architecture, such as the Internet.
Housing equipment	Equipment that makes up or that is incidental to a house. In this document, the term refers to housing equipment and home appliances connected with the Internet or the like.
Home gateway	Communications equipment installed in the premises of a smarthome. Home gateways also serve to connect premises housing equipment and home appliances to an external cloud in a secure manner.
Device manufacturer cloud	A cloud provided by a housing equipment or home appliance manufacturer to manage and control products of its own. Device manufacturer clouds often support an API via which the external society (such as third parties) can gain access to the functions of target devices or information stored in them.
Constraction manager	A person who supervises and overseas the construction of a house on site.
Site supervisor	A person who guides and supervises the construction so that the building be able to build according to the planning.
HEMS	Short for Home Energy Management System.

	A management system that takes advantage of information technology to help visualize and streamline the process of energy utilization by home appliances and the like in general households.
Entry point	A point in a smarthome service, IoT device or path of communication that could pose a security threat because of its accessibility from outside.
User interface	A scheme of exchanging information between a user and a smarthome. This scheme can be implemented in a variety of methods, such as on-screen display and manual entry, as with a smartphone, and voice speech and recognition, as with a smart speaker.
Device	An IoT device, such as housing equipment, a home appliance or sensor, installed in the premises of a smarthome.
Risk analysis and assessment	The process in which the assets to be protected and the potential threats and damages are analyzed, and security actions are defined from their risk metrics (severity of the damages).

Definitions of the abbreviations used in this document are listed below.

Table 1-2: Abbreviations

Abbreviation	Name
API	Application Program Interface
CCDS	Connected Consumer Device Security council
CPU	Central Processing Unit
CSIRT	Computer Security Incident Response Team
CVSS	Common Vulnerability Scoring System
DoS	Denial of Service
ETSI	European Telecommunications Standards Institute
GW	Gateway
HEMS	Home Energy Management System
IEC	International Electrotechnical Commission
I/F	Interface
IoT	Internet of Things
IoT-GW	Internet of Things-Gateway
IP	Internet Protocol
IPA	Information-technology Promotion Agency
ISO	International Organization for Standardization
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
LAN	Local Area Network
OTA	Online Trust Alliance
OWASP	The Open Web Application Security Project
VPN	Virtual Private Network
WG	Working Group
Wi-Fi	Wireless Fidelity
Information Security	Information Security that maintains confidentiality, integrity, and availability affects both cybers and physical area. ※This guideline uses “Information Security” that extends to cyber and physical area.
Cyber Security	Security in the scope of cyber

2 Definition of Smarthome Services and System Configuration

Preparatory to exploring security actions required in the smarthome field, this chapter defines services and identifies their relationships with certification. It proceeds to define the systems that make up a smarthome and introduces typical use cases of smarthome services.

2.1 Definition of Smarthome Services

Operations of an IoT device installed in the premises of a smarthome could cause damage to life and property under certain circumstances. For example, if a third party tampers the setting of a hot water server by exploiting its vulnerability, a fire or accident might result. And, If an electronically managed electronic lock is unlocked illegally a theft might ensue. Because different services offer different functions, use cases and compatible devices, the kinds of asses to be protected vary accordingly. Assuming that the assets that impact life and property should require foremost protection, smarthome services have been classified into the following two categories according to the importance of assets to be protected:

1) Services relevant to user comfort or convenience

Services in which premises housing equipment, intelligent home appliances, sensors and so on are controlled either automatically or as preprogrammed, as they collaborate with a system on a cloud, offering augmented user comfort or convenience.
Service examples:
・Products and services that remote-control or manage the schedules of air-conditioners, lighting fixtures, electric shutters and the like and that automate or otherwise manipulate their operations in sync with sensors.
・Products and services that help visualize the progress of power metering or energy-saving.
・Products and services linked to day-to-day health care, and more.

2)Services relevant to life and property

Services in which an information platform, such as a crime-prevention system or life-saving system, collaborates with security cameras, electronic locks, sensors and third-party service providers, to ensure users' day-to-day safety, security and life-saving in times of emergencies.

Examples:

・Products and services relevant to crime prevention or life-saving in times of emergencies

・Products and services requiring rigid control because they could lead to accidents, such as fires and physical injury, and more

Definitions of the terms “service” and “system” used this document are given below on table2-1.

Table 2-1: Definitions of a Service and a System

Term	Definition
Service	The process of a service provider delivering devices or systems, and a value, such as usefulness or satisfaction, through operation of such devices or systems, is defined as a “service.” In the smarthome field, service providers might be house makers utilizing the devices or systems they installed, device or systems makers utilizing products of their own or third parties utilizing services, devices or systems made by other companies.
System	An aggregate of devices configured to realize a value to a user is defined as a “system.” In the smarthome field, the term covers an IoT device environment, a cloud system used to integrate and manage service data and controls and so on. A system is defined not to include human operations.

2.2 Definitions of Security Levels of Smarthome Products an d Services

The CCDS released IoT Field Common Security Requirements Guidelines FY2018 (draft) [5] in November 2018. This Guidelines defines certification levels in a three-layer model, with each level designating a specific security level with a given number of star marks (★, ★★, ★★★) to promote better understanding by consumers. Further, 11 items of security requirements have been publicized to specify a "minimum set of common requirements to be fulfilled by connected devices."

This hierarchical model is adopted in the smarthome field as well, in which compliance with a minimum set of common requirements (Level ★) is assumed and in which Level ★★ represents products and services relevant to user comfort or convenience and Level ★★★ represents products and services relevant to life and property. In this document, security action policies and security requirements are discussed individually for Level ★★ and Level ★★★ products and services.

A hierarchical model of certification in the smarthome field is shown in Figure 2-1.

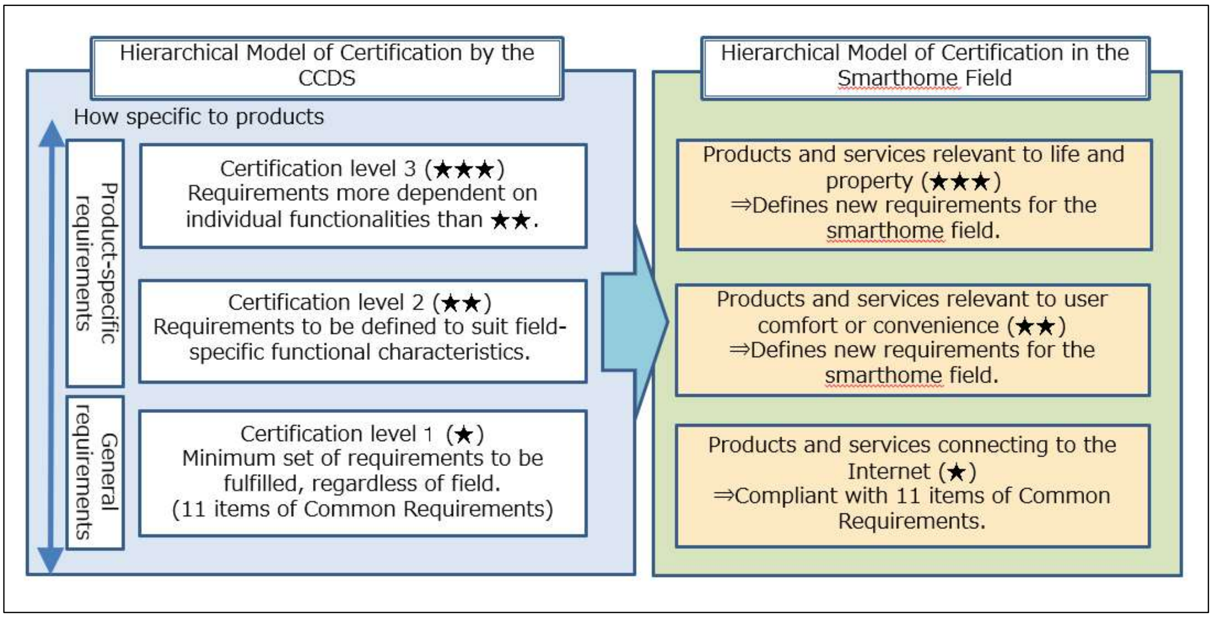

Hierarchical Model of Certification by the CCDS
How specific to products
Product-specific requirements
General requirements
Certification level 3 (★★★) Requirements more dependent on individual functionalities than ★★.
Certification level 2 (★★) Requirements to be defined to suit field-specific functional characteristics.
Certification level 1 (★) Minimum set of requirements to be fulfilled, regardless of field. (11 items of Common Requirements)
Hierarchical Model of Certification in the Smarthome Field
Products and services relevant to life and property (★★★) ⇒Defines new requirements for the smarthome field.
Products and services relevant to user comfort or convenience (★★) ⇒Defines new requirements for the smarthome field.
Products and services connecting to the Internet (★) ⇒Compliant with 11 items of Common Requirements.

Figure 2-1: Hierarchical Models of Smarthome Products and Services

Table 2-2 summarizes definitions of the respective levels.

Table 2-2: Certification Levels of Smarthome Products and Services

Level	Corresponding Service	Explanation
★★★	A product or service relevant to life and property (hereafter a “Level ★ ★★ service”)	Enforce security actions needed to protect assets that impact life and property, in addition to being compliant with the requirements of Level ★★.
★★	A product or service relevant to user comfort or convenience (hereafter a “Level ★★ service”).	Enforce security actions needed to realize user comfort or convenience, in addition to being compliant with the requirements of Level ★.
★	An Internet connectivity product or service.	Compliant with the 11 items of Common Requirements defined in “IoT Field Common Security Requirements Guidelines.”

Certification at Level ★★ or ★★★ aims at smarthome services and is intended to verify compliance with Section 5.5¸"Security Requirements for Smarthome Services." Because this Guidelines adheres to the concept of smarthome services endorsing a certain level of security actions as a whole, it does not go as far as guaranteeing security actions taken for a Service Information Platform over a cloud or for individual devices in the premises of a smarthome. Hence, the specification of individual certification requirements for a Service Information Platform or devices is beyond the scope of this Guidelines.

To help clarify the line of demarcation for responsibility for a service, however, the Service Information Platform or individual devices installed in the premises of a smarthome must be chosen to comply with the secondary requirements for ★★ or ★★★ services defined in Section 5.6.

For example, if an electronic lock can be unlocked by running a smartphone application in one use case, it is classified as a service relevant to user comfort or convenience (★★) and should require compliance with security secondary requirements for ★★ services. If the same electronic lock can be unlocked by a field representative stationed closest rushing to the source of fault notification to unlock the electronic lock remotely in another use case, then it is classified as a service relevant to life and property (★★★), requiring compliance with the security secondary requirements for ★★★ services.

Service providers act in the following procedural flow to determine whether the services they provide are classified as ★★ or as ★★★:
1) Service providers review use cases in the service planning stage and postulate applicable services tentatively to reflect the component devices and systems.
2)Service providers conduct risk analyses based on the use cases and check to see whether sensitive data, such as personal information, is handled and whether there will be any life and property impact and then determine compatible services.

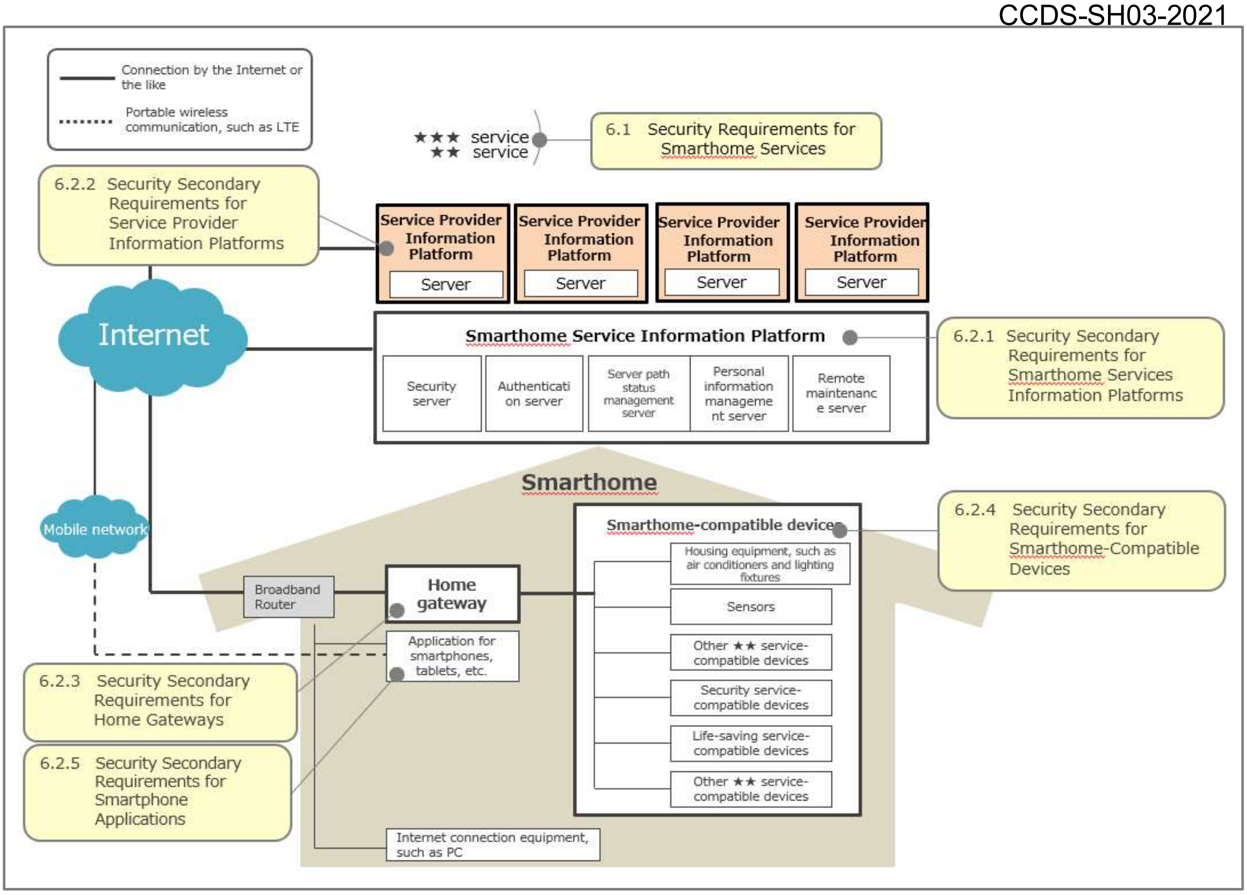

Connection by the Internet or the like
Portable wireless communication, such as LTE
★★★ service
★★ service
6.1 Security Requirements for Smarthome Services
6.2.2 Security Secondary Requirements for Service Provider Information Platforms
Service Provider Information Platform
Server
Service Provider Information Platform
Server
Service Provider Information Platform
Server
Service Provider Information Platform
Server
Internet
Smarthome Service Information Platform
Security server
Authentication server
Server path status management server
Personal information management server
Remote maintenance server
6.2.1 Security Secondary Requirements for Smarthome Services Information Platforms
Smarthome
Mobile network
Smarthome-compatible devices
Housing equipment, such as air conditioners and lighting fixtures
Sensors
Other ★★ service-compatible devices
Security service-compatible devices
Life-saving service-compatible devices
Other ★★ service-compatible devices
6.2.4 Security Secondary Requirements for Smarthome-Compatible Devices
Broadband Router
Home gateway
Application for smartphones, tablets, etc.
6.2.3 Security Secondary Requirements for Home Gateways
6.2.5 Security Secondary Requirements for Smartphone Applications
Internet connection equipment, such as PC

Figure 2-2 Responding to Security Requirements/Security Secondary Requirements for Smarthome Services

To find out more about the 11 items of Common Requirements, refer to IoT Field Common Security Requirements Guidelines FY2018 (draft) [5].

2.3 Defining a System Model

A schematic view of a basic system model of smarthomes is given in Figure 2-3. In reviewing this model, Figure 5-3, "Threats to Smart Houses and Typical Discussions of Security Actions," on P59, "A Guide to Security Design in IoT Development" compiled by the IPA has been consulted.

A Smarthome Service Information Platform is built to underlie the delivery of services intended to enhance the quality of life of users built on the equipment installed in their smarthomes. Smarthome Service Information Platforms control user premises devices according to collected and stored smarthome and user information. Device operations may be carried out by the users from inside or outside of their premises or remotely by third parties, such as service providers, depending on the kind of services provided.

Device operations from a Smarthome Service Information Platform can be carried out in two different ways: using the API available from a device manufacturer cloud and directly from the Smarthome Service Information Platform. Direct device operations require the Smarthome Service Information Platform to connect to a premises network beforehand, because they go through a HEMS controller or edge server connected to the premises network. Particularly, to be able to make the process of running devices relevant to life and property in a safer, more secure manner, a home gateway should be installed in the premises to make for secure communication with the Smarthome Service Information Platform. Because the home gateway positioned on the boundary between an external Internet and a premises smarthome environment serves as a secure gateway, a scheme of identifying between service-compatible devices with a certain level of security endorsed and devices individually set by users is desired.

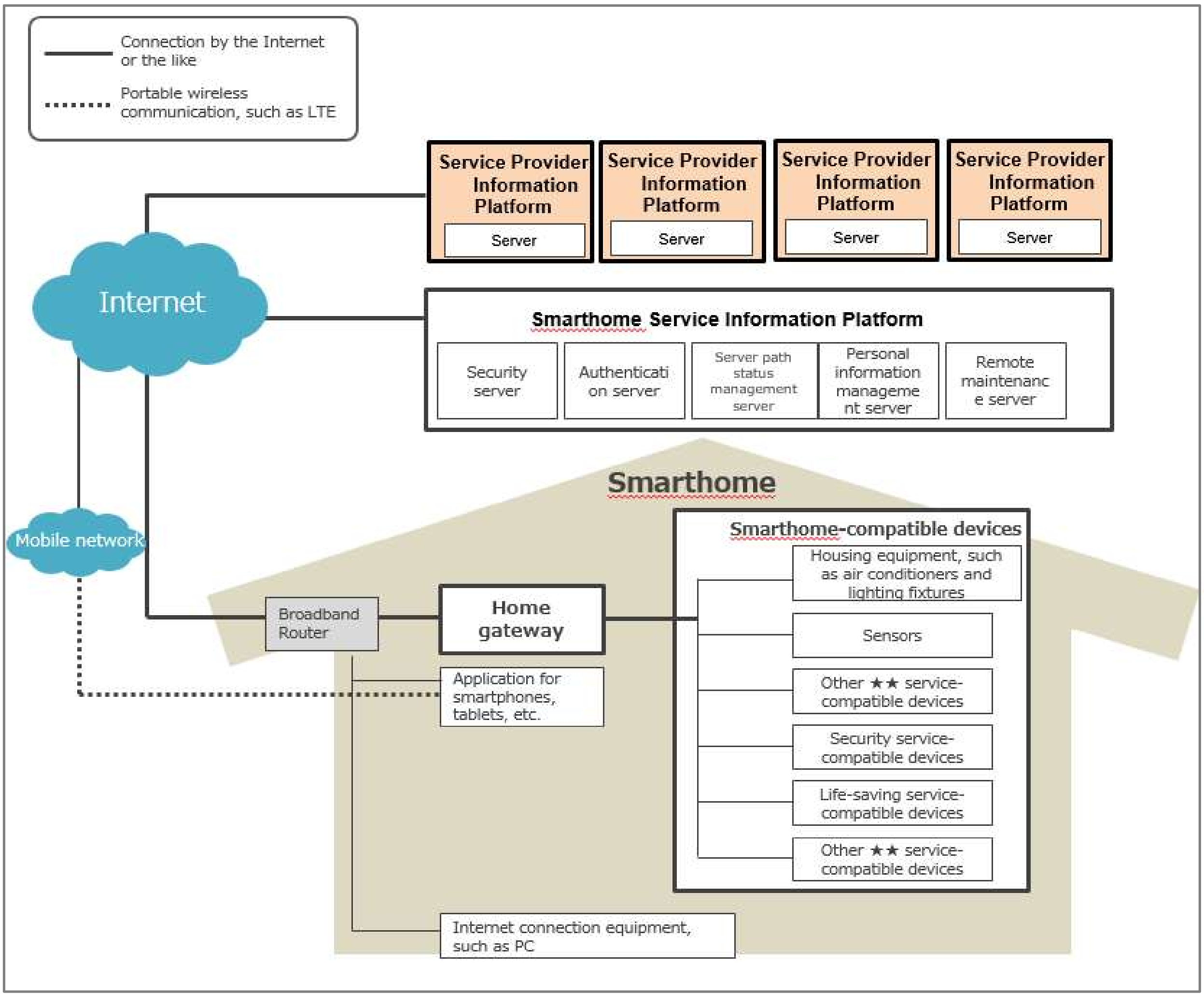

Connection by the Internet or the like
Portable wireless communication, such as LTE
Service Provider Information Platform
Server
Service Provider Information Platform
Server
Service Provider Information Platform
Server
Service Provider Information Platform
Server
Internet
Smarthome Service Information Platform
Security server
Authentication server
Server path status management server
Personal information management server
Remote maintenance server
Smarthome
Mobile network
Smarthome-compatible devices
Housing equipment, such as air conditioners and lighting fixtures
Sensors
Other ★★ service-compatible devices
Security service-compatible devices
Life-saving service-compatible devices
Other ★★ service-compatible devices
Broadband Router
Home gateway
Application for smartphones, tablets, etc.
Internet connection equipment, such as PC

Figure 2-3: Smarthome System Model Schematic

Table 2-3 gives a summary description of the components of the system model.

Table 2-3: System model components

Name	Description
■Smarthome Service Information Platform A system designed to manage the devices that make up the smarthome and provide essential services.	
Security server	Supervises the security of a Smarthome Service Information Platform.
Authentication server	Authenticates users, operators and the home gateway in using a Smarthome Service Information Platform.
Service device status management server	Manages the status of individual devices based on information sent from user premises smarthome service-compatible devices.
Personal information management server	Manages user information about the users of the Smarthome Service Information Platform.
Remote maintenance server	Manages and releases software updates for the home gateway and smarthome service-compatible devices.
■Smarthome	
Home gateway	Installed between the Internet and a smarthome, a home gateway connects information platforms to housing equipment and service-compatible devices while assuring their security.
Housing equipment, such as air-conditioners and lighting fixtures	Facilities and equipment installed in the premises of a home, such as air-conditioner and lighting fixtures.
Home appliance	An electrical appliance installed in the premises of a general home, such as TV, personal computers, refrigerators and washing machines.
Sensor	A sensor that detects a house temperature, humidity, human sensation and so on.
Other ★★ service-compatible device	All other devices compatible with★★ services, such as HEMS controllers and intelligent home appliances.
■Service Provider Information Platform A collaborating information system, such as a call center, that helps deliver optional	

Name	Description
services, such as security and life-saving services.	
Server (such as a cloud)	A server needed to provide services, set up above a cloud or elsewhere.

2.4 Definitions of Use Cases

IoT devices (housing equipment, home appliances and sensors) used to deliver smarthome services vary in their level of significance to cyber security, depending on their intended uses. For example, a human sensor might be used to enhance the convenience of our lives (e.g., for automatically opening and closing room doors) or to enhance our life and property (e.g., for identifying between an individual's life and death). More exacting cyber security actions would be required in the latter case. Because the risk factors and characteristics and issues of cyber security vary from one use case to another as outlined in Product Field-Specific Security Guidelines IoT-GW _Ver2.0 [10], typical use cases of the ★★ and ★★★ services will be defined to aid in subsequent discussions of security actions.

2.4.1 Use Case in ★★ Services

To illustrate a use case in which the asset to be protected is important information, a service that allows an electric shutter to open and close automatically (“Automatic Shutter Opening/Closing Service) according to a user-preset schedule is considered (Figure 2-4, Table 2-4).

This service remote-controls an electric shutter installed in the premises of a smarthome from a Smarthome Service Information Platform according to a schedule set from a user-run application. Because remote operations of the electric shutter are linked to personal information, allowing access, for example, to the user’s life pattern or residence/absence information, this use case can be classified as a ★★ service.

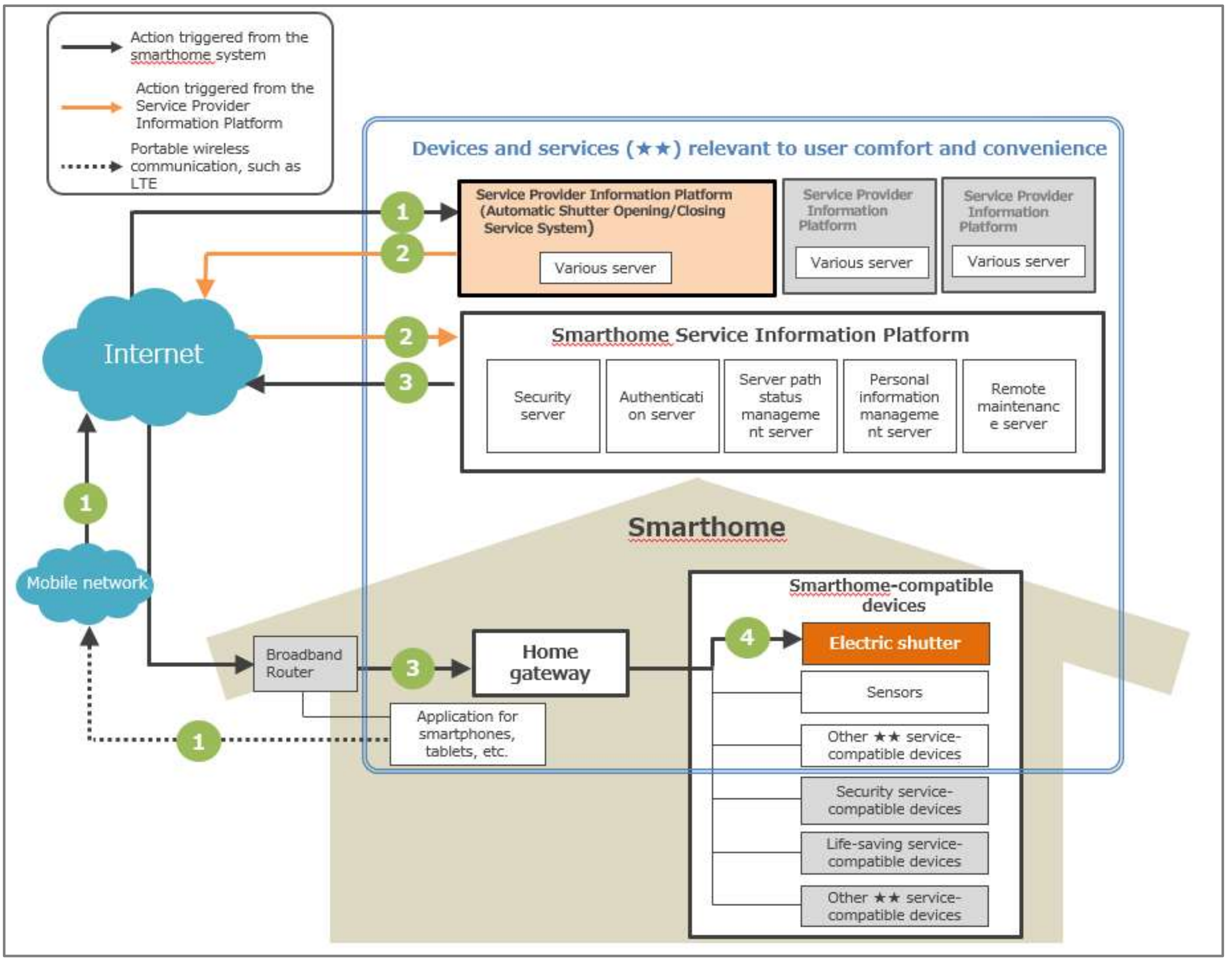

Action triggered from the smarthome system
Action triggered from the Service Provider Information Platform
Portable wireless communication, such as LTE
Devices and services (★★) relevant to user comfort and convenience
Service Provider Information Platform (Automatic Shutter Opening/Closing Service System)
Various server
Service Provider Information Platform
Various server
Service Provider Information Platform
Various server
1
2
Internet
2
3
Smarthome Service Information Platform
Security server
Authentication server
Server path status management server
Personal information management server
Remote maintenance server
1
Mobile network
Smarthome
Smarthome-compatible devices
4
Electric shutter
Sensors
Other ★★ service-compatible devices
Security service-compatible devices
Life-saving service-compatible devices
Other ★★ service-compatible devices
Broadband Router
3
Home gateway
Application for smartphones, tablets, etc.
1

Figure 2-4:Smarthome Use Case (Automatic Shutter Opening/Closing Service)

Table 2-4:Smarthome Use Case (Automatic Shutter Opening/Closing Service)

Figure#	Action	Description
1	Set an opening/closing schedule	Once an electric shutter opening/closing schedule is set from a user-run application, it is recorded with the user being linked to the automatic shutter opening/closing service system.
2	Order opening and/or closing of the electric shutter	When a preset time comes around, the automatic shutter opening/closing service system orders the Smarthome Service Information Platform to open and/or close the electric shutter.
3	Execute opening and/or closing of the electric shutter from the Smarthome	On receiving the order to open and/or close the electric shutter, the Smarthome Service Information Platform in turn orders the home gateway relevant to the home

Figure#	Action	Description
	Service Information Platform	to open and/or close the electric shutter.
4	Open and/or close the electric shutter	The home gateway opens and/or closes the electric shutter.

2.4.2 Use Case in ★★★ Services

To illustrate an instance of life and property as an asset to be protected, a use case of a security service ("On-Call Security Service"), in which personnel rush to the site upon detection of any abnormal conditions in the target home, is used (Figure 2-5, Table 2-5).

According to this service, the staff member stationed nearest to a home rushes to that home upon notification from a premises burglar sensor detecting any abnormal condition, such as trespassing, and enters the house through an entrance as it is unlocked from the call center in a remote operation, checks the internal conditions of the home and takes any action as appropriate in the circumstances.

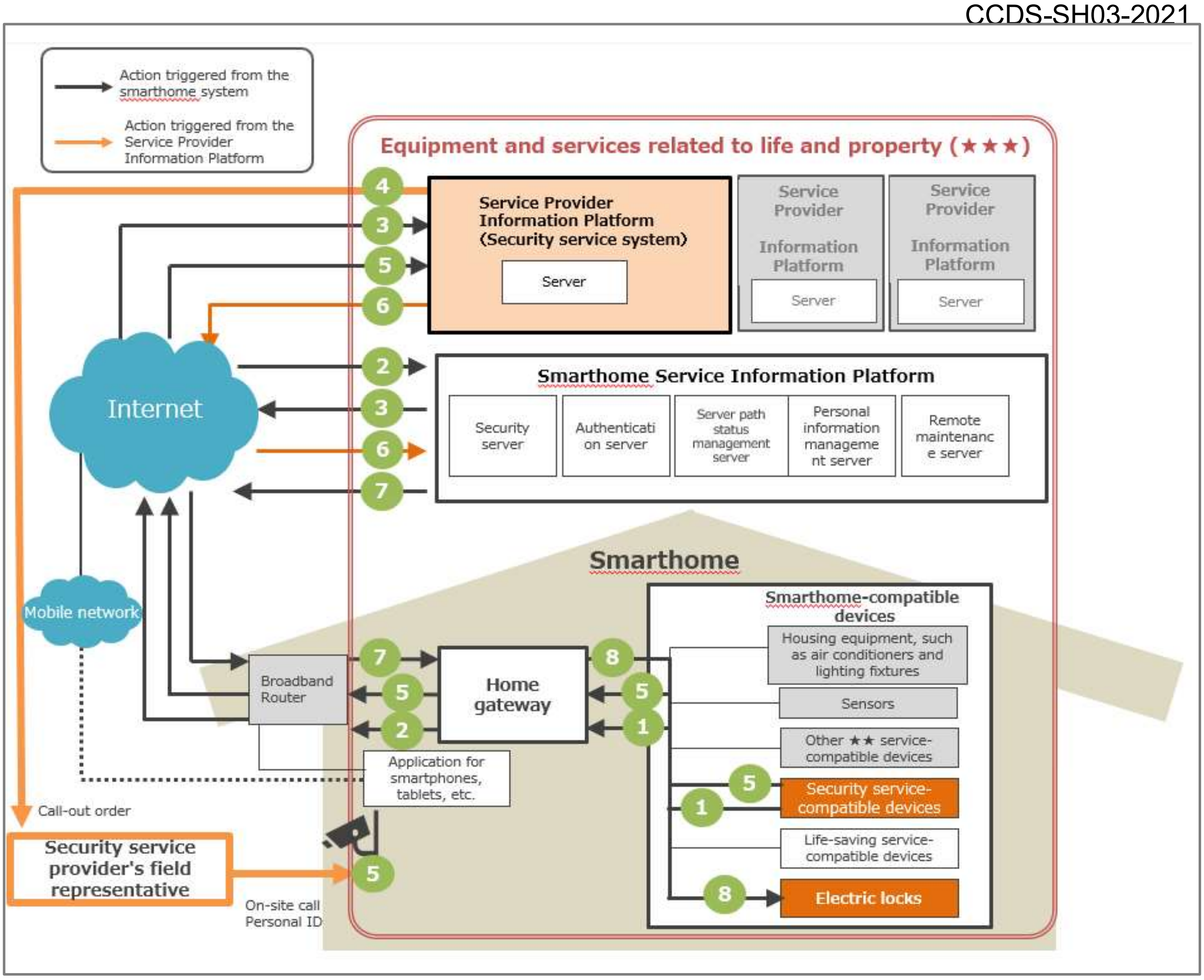

Action triggered from the smarthome system
Action triggered from the Service Provider Information Platform
Equipment and services related to life and property (★★★)
Service Provider Information Platform (Security service system)
Server
Service Provider
Information Platform
Server
Service Provider
Information Platform
Server
Internet
Smarthome Service Information Platform
Security server
Authentication server
Server path status management server
Personal information management server
Remote maintenance server
Mobile network
Smarthome
Smarthome-compatible devices
Housing equipment, such as air conditioners and lighting fixtures
Sensors
Other ★★ service-compatible devices
Security service-compatible devices
Life-saving service-compatible devices
Electric locks
Broadband Router
Home gateway
Application for smartphones, tablets, etc.
Call-out order
Security service provider's field representative
On-site call
Personal ID
1
2
3
4
5
6
7
8

Figure 2-5: Smarthome Use Case (On-Call Security Service)

Table 2-5 Smarthome Use Case (On-Call Security Service)

Figure#	Action	Description
1	Detection of any abnormal conditions by burglar sensors and security cameras	A burglar sensor or security camera installed in the premises of a smarthome detects any abnormal conditions, such as trespassing. The status of the burglar sensors and security cameras is being monitored by the home gateway, so any abnormal conditions will be detected upon occurrence.
2	Notification to the Smarthome Service Information Platform	As soon as any abnormal conditions in the smarthome are detected, they are reported from the home gateway to the Smarthome Service Information Platform through a secure path of communication.
3	Notification to the security service provider	The Smarthome Service Information Platform displays the detected abnormal conditions on a security service system screen monitored at the security service provider's call center.
4	Callout to a field representative	The field representative stationed nearest to the reported home is called out to rush to that home.
5	Field representative arrival check	The arrival of the field representative at the reported home and the identity of the field representative are verified.
6	Order to unlock the electronic lock	On confirming the arrival of the field representative, the call center worker gains authorization according to a predetermined chain of command before unlocking the electronic lock at the entrance through a call-out security service screen.
7	Unlocking of the electrical lock from the Smarthome Service Information	When ordered to unlock the electronic lock, the Smarthome Service Information Platform orders the home gateway for the home to unlock the electronic lock through a secure path of communication.
8	Unlocking of the electrical lock	The home gateway unlocks the electronic lock at the entrance.

3 Risk Analyses of Smarthome Products and Services

Risk analyses and assessment are carried out to define the cyber security risks existing in the services provided to a smarthome and the security requirements to provide against them. In the risk analysis and assessment process, the information assets to be protected in providing such services are identified, along with potential threats to the information assets and their risk characteristics, and the impacts from the threats occurring are measured. Then, the actions against the risks and their priority levels are established from the risk characteristics and impacts thus analyzed.

This chapter presents a summary insight into the procedural flow of the cyber security risk analysis and assessment process for smarthome services.

3.1 Risk Analyses and assessment Procedures

Risk analyses of smarthome services are carried out in the procedural flow described below. Detailed descriptions of the procedural steps follow.

Table 3-1:Risk Analyses and Assessment Procedures

No.	Step	Description
1	Define a use case	Define the components of a system to be analyzed and assessed and its users and the way the users and the system interact with each other.
2	Identify the assets to be protected	Among all information assets handled by the system appearing in the use case, identify those that need protection.
3	Analyze potential threats	Specify entry points based on the system model and analyze potential threats.
4	Analyze the potential threats in detail	Review potential threat cases and analyze them in detail.
5	Calculate risk metrics	Calculate the risk metrics that represent the impact of potential threats when they occur.
6	Define security actions	Define the security actions to be taken in providing services, from the results of risk metric analyses and assessment. In defining security actions, it is necessary to take into consideration the frequencies with which incidents could occur, impacts (risk metrics) of their occurrence and the cost of the actions taken.

3.2 Identification of the Assets to be Protected

Regarding the use case defined in the foregoing section, identify the assets to be protected. The availability of a smarthome service, particularly ★★★ service, or the ability to provide one without interruption, is considered an important protected asset, because the user's life or property could be impacted if the availability of a function relating to life saving in times of emergencies or to day-to-day crime prevention is impeded by attacks. Moreover, if a smarthome product or service is assumed, the target assets need to be identified exhaustively from the information they handle, from the functionalities they provide and so on for each of the elements (such as an IoT device or cloud) that make up the service.
The assets to be protected are exemplified in Table 3-2 below.

Table 3-2: Examples of Assets to be Protected among Smarthome Systems and Products

Entry Point	Device Name	Asset Type	Asset to be Protected
Smarthome Service Information Platform	Security server	Primary asset (※1)	Hardware, software (security function itself)
			Setup information, log information
	Authentication server	Primary asset	Hardware, software (function itself)
		Secondary asset(※2)	Authentication information
			Encryption key
	Service device status management server	Primary asset	Hardware, software (function itself)
			Device status management information
	Personal information management server	Primary asset	Hardware, software (function itself)
			Personal information (user's name, address, phone number and the like)
	Remote maintenance server	Primary asset	Hardware, software (function itself)
			Update software

Path of communication between the Smarthome Service Information Platform and the Internet	—	Primary asset / Secondary asset	Data on a communication path
Service Provider Information Platform	Third-party service server	Primary asset	Hardware, software (function itself)
			Device status management information
			Personal information (user’s name, address, phone number and the like)
			Setup information, log information
		Secondary asset	Authentication information （Authentication key)
			Encryption key
Path of communication between the Service Provider Information Platform and the Internet	—	Primary asset /Secondary asset	Data on a communication path
Home gateway	Home gateway	Primary asset	Hardware, software (function itself)
			Setup information, log information
			Personal information (dependent on the functional implementation of the target device)
		Secondary asset	Authentication information
			Encryption key
Path of communication between the home	—	Primary asset / Secondary asset	Data on a communication path

gateway and the Internet			
Smarthome-compatible devices	Air-conditioners, lighting fixtures and the like	Primary asset	Hardware, software (function itself)
			Control signal
		Secondary asset	Authentication information
	Sensor	Primary asset	Hardware, software (function itself)
			Sensing data
		Secondary asset	Authentication information
	Other ★★ service-compatible device	Primary asset	Hardware, software (function itself)
			Control signal
			Sensing data
			Personal information (dependent on the functional implementation of the target device)
		Secondary asset	Authentication information
	Security service-compatible device	Primary asset	Hardware, software (function itself)
			Control signal
			Sensing data
			Personal information (dependent on the functional implementation of the target device)
		Secondary asset	Authentication information
	Life-saving service-compatible device	Primary asset	Hardware, software (function itself)
			Control signal
			Sensing data
			Personal information (dependent on the functional implementation of the target device)

		Secondary asset	Authentication information
Path of communication between the home gateway and compatible devices	—	Primary asset / Secondary asset	Data on a communication path ・Control signal 、Sensing data ・Personal information (dependent on the functional implementation of the target device) ・Authentication information
Smartphone application	—	Primary asset	Software (function itself)
			Control signal
			Personal information or confidential information stored in the smartphone
		Secondary asset	Authentication information
Path of communication between a smartphone and the home gateway	—	Primary asset / Secondary asset	Data on a communication path

Note to *1 and *2:"Primary asset" and "Secondary asset" used in the table are defined as follows:

・Primary asset:Any asset to be protected itself are defined as a "primary asset."

・Secondary asset:An encryption measure needed to protect a primary asset and a subsidiary assets relevant to authentication are defined as a "secondary asset."

3.3 Analysis of Potential Threats

Cyber security threats to the assets to be protected as identified in the preceding section are analyzed here.

3.3.1 Potential Threats to Smarthome Products and Systems

Using the smarthome system model, entry points (exploitable points) are extracted and potential threats are analyzed regarding each of these entry points. In this document, use is made of the STRIDE+CCDS model [12], which is an enhancement made by the CCDS to a Microsoft-advocated threat analysis technique called " STRIDE model" [11]. The STRIDE model has six kinds of threats (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) defined, which are used to analyze potential threats to systems. The STRIDE+CCDS model has an additional five kinds of threats added to respond to IoT devices and systems.

Table 3-3 List of Threat Categories Based on the STRIDE+CCDS Model

Type	Threat	Description
STRIDE MODEL	Spoofing	To pretend to be another user or device to the computer.
STRIDE MODEL	Tampering	Unauthorized alteration of data to disrupt its integrity.
STRIDE MODEL	Repudiation	To repudiate any action taken by a user, without the user having no way to verify that action.
STRIDE MODEL	Information Disclosure	The Information Disclosure to an individual without access privileges.
STRIDE MODEL	Denial of Service （DoS）	To impede a regular user from accessing a server or service.
STRIDE MODEL	Elevation of Privilege	The acquisition of access privileges by an unauthorized user.
THREAT ADDED BY THE CCDS	Unauthorized access	Access made by an individual without access privileges.
THREAT ADDED BY THE CCDS	Malware Infection	A source of contamination to other devices, causing an interference with one's business with ransomware or the like.
THREAT ADDED BY THE CCDS	Springboard	Used as a relay point in attempting unauthorized access or the like to any other device.
THREAT ADDED BY THE CCDS	Unauthorized modification	The theft of internal data or installation of a vulnerability trap by making unauthorized (illegal) modifications to hardware or software.

THREAT ADDED BY THE CCDS	Unknown vulnerability	A vulnerability yet to be publicly known or one produced by a new attach technique.

Considering the system model outlined above, what kinds of threat will reach the assets to be protected are examined exhaustively regarding to entry points (exploitable points). In the analysis case illustrated in Figure 3-1 below, those devices and paths of communication that could form an entry point are each designated by a red mark and assigned a number (EP number) from (1) to (10) in association with Table 3-4.

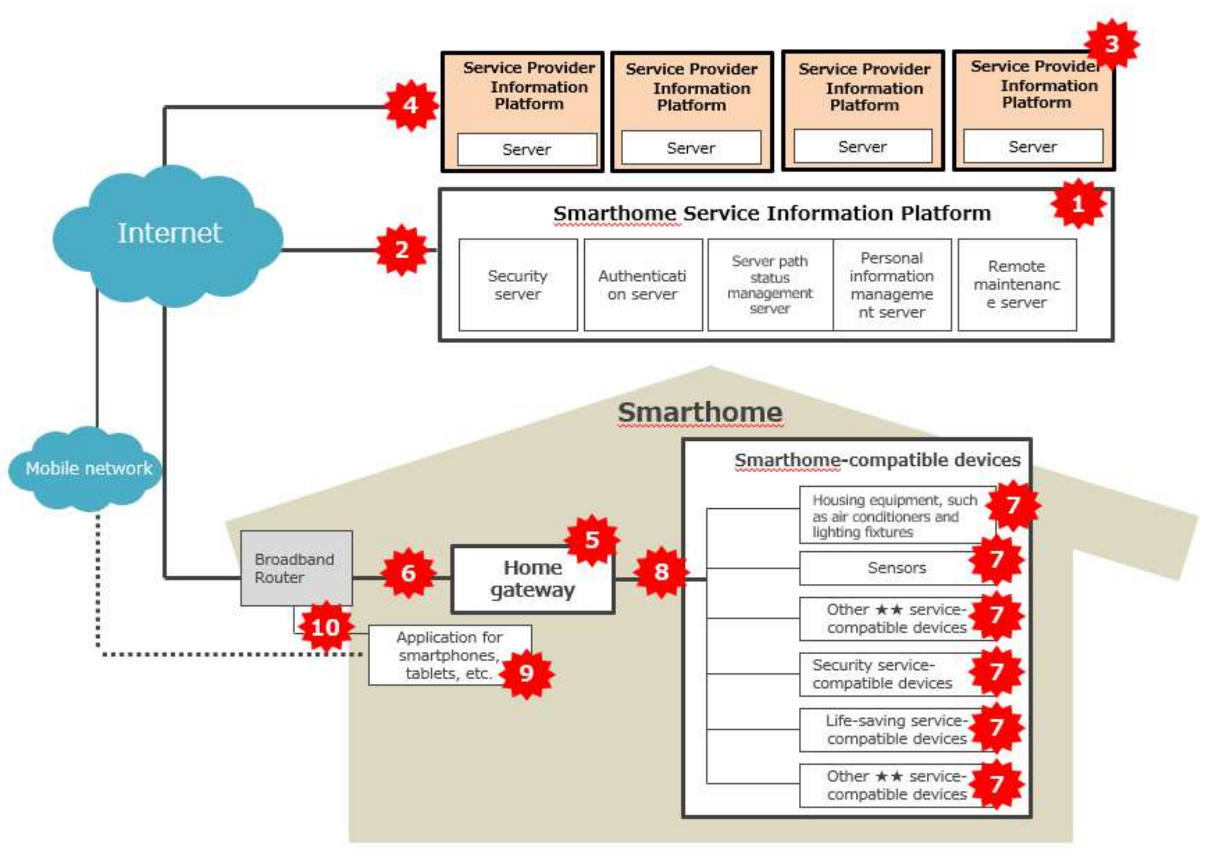

Service Provider Information Platform
Server
Service Provider Information Platform
Server
Service Provider Information Platform
Server
Service Provider Information Platform
Server
3
4
Internet
2
Smarthome Service Information Platform
1
Security server
Authentication server
Server path status management server
Personal information management server
Remote maintenance server
Mobile network
Smarthome
Smarthome-compatible devices
Housing equipment, such as air conditioners and lighting fixtures
7
Sensors
7
Other ★★ service-compatible devices
7
Security service-compatible devices
7
Life-saving service-compatible devices
7
Other ★★ service-compatible devices
7
Broadband Router
6
Home gateway
5
8
10
Application for smartphones, tablets, etc.
9

Figure 3-1: Threat Analysis Cases on the Smartphone System Model

Table 3-4: Examples of Threat Categories Based on the STRIDE+CCDS Model

Entry Point	Entry Point Number (EP Number) on the System Model	Threat Category on the STRIDE+CCDS Model
Smarthome Service Information Platform	EP①	Unauthorized access
		Information Disclosure
		Tampering
		Spoofing
		Malware Infection
		Denial of Service
Path of communication between the Smarthome Service Information Platform and the Internet	EP②	Information Disclosure
Service Provider Information Platform	EP③	Unauthorized access
		Information Disclosure
		Tampering
		Spoofing
		Malware Infection
		Denial of Service
Path of communication between the Smarthome Service Information Platform and the Internet	EP④	Information Disclosure
Home gateway	EP⑤	Unauthorized access
		Information Disclosure
		Tampering
		Spoofing
		Malware Infection
		Denial of Service
		Springboard

Path of communication between the home gateway and the Internet	EP⑥	Information Disclosure
Smarthome-compatible devices	EP⑦	Unauthorized access
		Information Disclosure
		Tampering
		Spoofing
		Malware Infection
		Springboard
Path of communication between smarthome-compatible devices and the home gateway	EP⑧	Spoofing
		Information Disclosure
Smartphone application	EP⑨	Information Disclosure
		Spoofing
Path of communication between a smartphone and the home gateway	EP⑩	Spoofing
		Information Disclosure

3.3.2 Potential Threats Other Than Cyber Security

If Availability is positioned as an asset of importance to a smarthome service, threats other than cyber security should require consideration as well. Typical potential threats are enumerated below.

- Accidents, such as natural disasters and fires
- Hardware failures
- Software faults
- Operation errors committed by operations representatives, acts of negligence, internal fraud
- Maintenance work (software and hardware update)
- Service providers' service shutdown or withdrawable from business
- Damage to hardware and software by physical invasion

Chapter 5 of this document discusses actions to be taken against threats other than those to cyber security listed above, as well as finds of the cyber security threat analyses presented in this section.

3.4 Detailed Analysis of Potential Threats

This section launches a more detailed analysis of potential threats based on the analysis findings presented in the foregoing sections, with their case studies, risk characteristics and other factors taken into consideration.

It is assumed that the risk characteristics are assigned the items (see Table 3-5) outlined below.

Table 3-5: List of Detailed Analysis Items of Potential Threats

No.	Item	Description
Description of potential threats		
1	Entry point	The entry point assumed by a potential threat (IoT device, cloud).
2	Asset to be protected	An asset that is exposed to the potential threat (see Table 3-2).
3	Threat category based on the STRIDE+CCDS model	A classification of the potential threat (see Table 3-3).
4	Example of the potential threat	An example of the potential threat.
Risk characteristics		
5	Connection I/F	The route of threat invasion (see Table 3-6).
6	Who (who connected)	The entity that is connected to the entry point (see Table 3-7).
7	Whom (what has been harmed)	What has been harmed by the threat (see Table 3-8).
8	Where (where the threat has occurred)	Where the threat has occurred (see Table 3-9).

The items listed on the connection I/F are listed below.

Table 3-6: Connection I/F Items

A) Connection I/F on a wired connection		
No.	Item	Description
1	Ethernet	A standard under which data is transmitted at rates from 10Mbps to 1Gps over CAT cables as communication media. Standardized as IEEE802.3.
2	HD-PLC	High Definition Power Line Communication, or a standard that uses the frequency band of 2 to 30 MHz to achieve communication of multiple streams of HDTV video.
3	Wired communication	Wired communication by means other than 1 and 2 above.

	other than above.	
B) Connection I/F on a wireless connection		
No.	Item	Description
4	Wi-Fi	Wi-Fi (wireless fidelity) is a brand name that designates the certification (Wi-Fi Certified) by the Wi-Fi Alliance of the interconnectivity between wireless LAN devices adhering to IEEE802.11 Series (IEEE802.11a/IEEE802.11b).
5	Bluetooth	A wireless technology standard used for exchanging simple data between information devices over short distances, ranging several meters to several tens of meters.
6	ZigBee	ZigBee is one of the short-distance wireless communication standards designed mainly for sensor networks. Electrical specifications of its basic part are standardized as IEEE802.15.4. For device-to-device communications protocols higher than the logical layer, specifications have been formulated by the ZigBee Alliance.
7	Wi-SUN	Short for Wireless Smart Utility Network, Wi-SUN is an interconnect specification for wireless communications based on IEEE802.15.4g, standardized by the trade organization, Wi-SUN Alliance.
8	Specified low-power radio communication	Since diversified life styles or business scenes have come to dictate means of simple communication over short ranges, the demand for radio communication in relatively narrow service areas is growing. In this background, a system aiming at specified low-power radio stations has been created, allowing anybody to use low-power radio communication without being required to comply with the radio operator standard or acquire a radio station license,
9	LTE/LTE-Advanced	A communication standard for digital cellular telephony
10	Wireless communication other than the above.	Wireless communication other than 4 to 10 above.

Note:Prepared by the CCDS by consulting TR-1043 and TR-1064 worked out by the Telecommunication Technology Committee (TTC), a general incorporated association.

The descriptions of Who, Whom and Where are listed below. These descriptions have been defined to suit the needs for smarthome services by consulting “Patterns of Connectivity,” “What Needs to be Protected” and “Locations of Risks” described in the IPA’s Smart-society Development Guidelines, Second Edition.

Table 3-7: Who (who connected) Items

No.	Item	Description
1	Device manufacturer	For a connection that was envisioned by the IoT device manufacturer at design time.
2	Service provider	For a device or system connected to implement a service. This case includes a connection that was not envisioned by the device manufacturer at design time.
3	User (intentional)	For an intentional connection made by a user.
4	User(wrong connection)	For a wrong connection made by a user.
5	Attacker	For a malicious connection that targets a vulnerability.
6	Accidental	For a connection made by accident.

Table 3-8: Whom (what has been harmed)

No.	Item	Description
1	IoT function	Any function (such as communication or security action) required by an IoT device to connect to a system.
2	Original function	Original functions provided by IoT deices and systems.
3	Service	A service provided through collaboration between an IoT device and a system.
4	Information	Personal information about users, device information collected, IoT devices andsystem setup information.
5	Life and property	A user’s own life and property
6	Others	All other objects.

Table 3-9: Where (where the threat has occurred)

No.	Item	Description
1	Ordinary-use I/F	A user operation panel, wired/wireless service I/F, USB terminal and so on.
2	Maintenance I/F	Examples include an administrator control panel, remote control communication I/F or software update USB terminal.
3	Nonordinary-use I/F	An unnecessary port left uncovered, USB terminal used only during manufacture or the like.
4	Included risk	A defect or bug that could result in failure, a vulnerability possibly open to attacks, a function that might cause harm as a result of a failure, abuse or the like.
5	Physical contact	To come into direct contact with a body (as for unauthorized replacement or alteration of parts).

Table 3-10 and Table 3-11 below present examples of detailed threat analyses of the systems and devices that make up a smarthome according to the items listed above.

Table 3-10: Examples of Detailed Threat Analyses of a Smarthome Service and a Service Provider Information Platform

Entry Point	EP#	Asset to be Protected	Threat Category Based on the STRIDE+CCDS Model	Example of Potential Threats	Connection I/F Table 3-6	Who Table 3-7	Whom Table 3-8	Where Table 3-9
Smarthome Service Information Platform	EP ①	【Primary asset 】 ・Hardware, software (security function itself) ・Setup information, log information ・Device status management information ・Personal information	Unauthorized access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	Ethernet	Attacker	★★ Service ★★★ Life and property	Ordinary-use I/F
			Information Disclosure	Theft of information from data stored in the Service Information Platform (access control or authentication overridden).	Ethernet	Attacker	★★ Information ★★★ Information	Ordinary-use I/F
			Tampering	Tampering of data or settings in the Smarthome Service Information Platform.	Ethernet	Attacker	★★ Service ★★★	Ordinary-use I/F

		(user's name, address, phone number and the like) ・Update software 【Secondary asset】 ・Authentication information ・Encryption key					Life and property	
			Spoofing	The Service Provider Information Platform or the home gateway is attacked by spoofing or tampered messaging during communication via an API.	Ethernet	Attacker	★★ Service ★★★ Life and property	Ordinary-use I/F
			Malware Infection	Malware infection of the Service Information Platform (attacks launched via an external network).	Ethernet	Attacker	★★ Service ★★★ Life and property	Ordinary-use I/F
			Denial of Service	DDoS (DoS) attack.	Ethernet	Attacker	★★ Service ★★★ Life and property	Ordinary-use I/F
			Information Disclosure	Information Disclosure via a carried-in storage device.	Wired communication	Service Provider	★★ Information	Nonordinary-use I/F

					other than above		★★★ Information	
			Malware Infection	Malware infection via a carried-in storage device.	Wired communication other than above	Service Provider	★★ Service ★★★ Life and property	Nonordinary-use I/F
			Information Disclosure	Theft of update software information.	Ethernet	Attacker	★★ Information ★★★ Information	Maintenance I/F
			Tampering	Tampering of update software	Ethernet	Attacker	★★ Service ★★★ Life and property	Maintenance I/F
Path of communication between the Smarthome Information	EP ②	【Primary asset /Secondary asset】 Data on a	Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack	Ethernet	Attacker	★★ Information ★★★ Information	Ordinary-use I/F

Platform and the Internet		communication path						
Service Provider Information Platform	EP ③	【Primary asset 】 ・Hardware, software (function itself) ・Setup information, log information ・Device status management information ・Personal information (user's name, address, phone	Unauthorized access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	Ethernet	Attacker	★★ Service ★★★ Life and property	Ordinary-use I/F
			Information Disclosure	Theft of information from data stored in the Service Information Platform (access control or authentication overridden).	Ethernet	Attacker	★★ Information ★★★ Information	Ordinary-use I/F
			Tampering	Tampering of data or settings in the Smarthome Service Information Platform.	Ethernet	Attacker	★★ Service ★★★ Life and property	Ordinary-use I/F
			Spoofing	Smarthome Service Information Platforms	Ethernet	Attacker	★★ Service	Ordinary-use I/F

		number and the like) 【Secondary asset】 ・Authentication information ・Encryption key		are attacked by spoofing or tampered messaging during communication via an API.			★★★ Life and property	
			Malware Infection	Malware infection of the Service Information Platform (attacks launched via an external network).	Ethernet	Attacker	★★ Service ★★★ Life and property	Ordinary-use I/F
			Denial of Service	DDoS (DoS) attack.	Ethernet	Attacker	★★ Service ★★★ Life and property	Ordinary-use I/F
			Information Disclosure	Information Disclosure via a carried-in storage device.	Wired communication other than above	User (intentional)	★★ Information ★★★ Information	Nonordinary-use I/F
			Malware Infection	Malware infection via a carried-in storage device.	Wired communication	User (intentional)	★★ Service	Nonordinary-use I/F

					other than above		★★★ Life and property	
			Information Disclosure	Theft of update software information.	Ethernet	Attacker	★★ Information ★★★ Information	Maintenance I/F
			Tampering	Tampering of update software	Ethernet	Attacker	★★ Service ★★★ Life and property	Maintenance I/F
Path of communication between the Smarthome Service Information Platform and the Internet	EP ④	【Primary asset /Secondary asset】 Data on a communication path	Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack	Ethernet	Attacker	★★ Information ★★★ Information	Ordinary-use I/F

Table 3-11: Detailed Threat Analysis Cases for Home Gateways, Smarthome-Compatible Devices and Smarthome Applications

Entry Point	EP#	Asset to be Protected	Threat Category Based on the STRIDE+CCDS Model	Example of Potential Threats	Connection I/F	Who	Whom	Where
Home gateway	EP ⑤	【Primary asset 】 ・Hardware, software (function itself) ・Setup information, log information ・Personal information (user's name, address, phone number and the like)	Unauthorized access	Unauthorized access to a home gateway（attacks exploiting known vulnerabilities）	Ethernet	Attacker	★★ Original function	Ordinary-use I/F
							★★★ Original function	
					Ethernet	Attacker	★★ Service	Ordinary-use I/F
							★★★ Life and property	
			Information Disclosure	Theft of information from data or settings stored in a home gateway (access control	Ethernet	Attacker	★★ Information	Ordinary-use I/F
							★★★ Information	

		【Secondary asset】 ・Authentication information ・Encryption key		or authentication overridden).				
			Tampering	Tampering of data or settings stored in a home gateway	Ethernet	Attacker	★★ Original function	Ordinary-use I/F
							★★★ Original function	
					Ethernet	Attacker	★★ Service	Ordinary-use I/F
							★★★ Life and property	
			Spoofing	The home gateway is attacked by spoofing of a Service Provider Information Platform and tampered messaging during communication via an API.	Ethernet	Attacker	★★ Service	Ordinary-use I/F
							★★★ Life and property	

			Malware Infection	Home gateway malware infection (attacks launched via an external network)	Ethernet	Attacker	★★ Service ★★★ Life and property	Ordinary-use I/F
			Denial of Service	DDoS (DoS) attack.	Ethernet	Attacker	★★ Service ★★★ Life and property	Ordinary-use I/F
			Information Disclosure	Information Disclosure via a connected storage device.	Wired communication other than above	User(intentional)	★★ Information ★★★ Information	Ordinary-use I/F
			Malware Infection	Malware infection via a connected storage device.	Wired communication other than above	User(intentional)	★★ Original function ★★★ Original function	Ordinary-use I/F
						User(intentional)	★★	

					Wired communication other than above		Service	Ordinary-use I/F
							★★★ Life and property	
			Malware Infection	Malware Infection from internal LAN-attached devices	Ethernet Wi-Fi Wireless communication other than the above.	Attacker	★★ Original function・Information	Ordinary-use I/F
							★★★ Original function・Information	
					Ethernet Wi-Fi Wireless communication other than the above.	Attacker	★★ Service	Ordinary-use I/F
							★★★ Life and property	
			Springboard	Abused as a springboard for launching attacks, e.g., as a bot.	Ethernet	Attacker	★★ IoT function	Ordinary-use I/F
							★★★ IoT function	

Path of communication between the Home gateway and the Internet	EP ⑥	【Primary asset /Secondary asset】 Data on a communication path	Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack	Ethernet	Attacker	★★ Information	Ordinary-use I/F
							★★★ Information	
Smarthome Service Compatible Devices	EP ⑦	【Primary asset 】 ・Hardware, software (function itself) ・Control signal ・Sensing data ・Personal information (user’s name, address, phone number and the like)	Unauthorized access	Unauthorized access to a device (attacks exploiting known vulnerabilities).	Ethernet Wi-Fi Wired communication/wireless communication other than above.	Attacker	★★ IoT function	Ordinary-use I/F
							★★★ IoT function	
					Ethernet Wi-Fi Wired communication/wireless communication other than above.	Attacker	★★ Service	Ordinary-use I/F
							★★★ Life and property	
			Information Disclosure	Theft of information from data or settings stored in a	Ethernet Wi-Fi	Attacker	★★ Information	Ordinary-use I/F

		【Secondary asset】 ・Authentication information ・Encryption key		device (access control or authentication overridden).	Wired communication/wireless communication other than above.		★★★ Information	
			Tampering	Tampering of data or settings stored in a device.	Ethernet Wi-Fi Wired communication/wireless communication other than above.	Attacker	★★ Original function	Ordinary-use I/F
							★★★ Original function	
					Ethernet Wi-Fi Wired communication/wireless communication other than above.	Attacker	★★ Service	Ordinary-use I/F
							★★★ Life and property	
			Spoofing	The device is attacked by spoofing of the Home gateway and tampered messaging during communication.	Ethernet Wi-Fi Wired communication/wireless communication other than above.	Attacker	★★ Service	Ordinary-use I/F
							★★★ Life and property	

			Information Disclosure	Information Disclosure via a connected storage device (any compatible device, such as a USB interface).	Wired communication other than above	User (intentional)	★★ Information	Ordinary-use I/F
							★★★ Information	
			Malware Infection	Malware infection via a connected storage device (any compatible device, such as a USB interface).	Wired communication other than above	User (intentional)	★★ Original function・Information	Ordinary-use I/F
							★★★ Original function・Information	
					Wired communication other than above	User (intentional)	★★ Service	Ordinary-use I/F
							★★★ Life and property	
			Springboard		Ethernet Wi-Fi	Attacker	★★ Others	Ordinary-use I/F

				Abused as a springboard for launching attacks, e.g., as a bot.	Wired communication/wireless communication other than above.		★★★ Others	
Path of communication between Smarthome Service Compatible Devices and the Home gateway	EP ⑧	【Primary asset /Secondary asset】 Data on a communication path ・Control signal 、 Sensing data ・Personal information (dependent on the functional implementation of the target device)	Spoofing	Spoofing of a device control signal by launching a man-in-the-middle attack.	Wi-Fi Wireless communication other than the above.	Attacker	★★ Original function	Ordinary-use I/F
							★★★ Original function	
					Wi-Fi Wireless communication other than the above.	Attacker	★★ Service	Ordinary-use I/F
							★★★ Life and property	
			Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack	Wi-Fi Wireless communication other than the above.	Attacker	★★ Information	Ordinary-use I/F
							★★★ Information	

		・Authentication information						
Smartphone application	EP ⑨	【Primary asset 】 ・Software (function itself) ・Control signal ・Personal information or confidential information stored in the smartphone 【Secondary asset】 ・Authentication information	Information Disclosure	Information Disclosure on stored in a device due to a vulnerability in a smartphone application.	Wi-Fi LTE/LTE-Advanced	User (intentional)	★★ Information ★★★ Information	Ordinary-use I/F
			Information Disclosure	Information Disclosure due to an unauthorized login to a smartphone application.	Wi-Fi LTE/LTE-Advanced	Attacker	★★ Original function ★★★ Original function	Ordinary-use I/F
			Spoofing	Any unauthorized operation of a device caused by illegally logging in to a smartphone application.	Wi-Fi LTE/LTE-Advanced	Attacker	★★ Original function ★★★ Original function	Ordinary-use I/F
Path of communication between a	EP ⑩	【Primary asset /Secondary asset】	Spoofing	Spoofing of a device control signal by launching	Wi-Fi	Attacker	★★ Original function	Ordinary-use I/F

smartphone and the home gateway		Data on a communication path		a man-in-the-middle attack.			★★★ Original function	
			Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack	Wi-Fi	Attacker	★★ Information	Ordinary-use I/F
							★★★ Information	

3.5 Calculation of Risk Metrics

Once potential threats and their risk characteristics are analyzed, the next step is to calculate their risk metrics. Various methods of calculating risk metrics have been proposed [15], including the CVSS and the OWASP Risk Rating Methodology, ETSI TS102 165-1. Risk metrics assume different values depending on how they are calculated, so that only a comparison of the risk metrics determined in the same method will be meaningful.

For this reason, once a given method of calculating the risk metrics of smarthome products and services is defined, it must be put into continued use thereafter.

The work of calculating the risk metrics of smarthome products and services should also take their uses, particularly, their Life and Property impact, into consideration.

3.5.1 Calculation of Risk Metrics Based on CVSS v3 and Issues

No analytical techniques are currently available for risk analyses and assessment of smarthome products and services, since this endeavor has not yet been carried out to date. Preparatory to compilation of this Guidelines, risk analyses and assessment techniques were surveyed and reviewed and the calculation of risk metrics based on CVSS v3 [16][17], a commonly used framework of assessing information security vulnerabilities, was tried.

CVSS Base Scores are to be used in the calculation of threat risk metrics that precedes the implementation of security actions. Risk metrics of the threats assumed for ★★ and ★★★ services based on CVSS v3 are summarized.

Table 3-12 Service Risk Metrics Based on CVSS v3(Common to ★★ and ★★★) ※Excerpt

Threat Example				Base Metrics											
Entry Point	EP number	Threat Category	Threat examples	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk Score	Risk Score Rank
Smarthome Service Information Platform	EP①	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Information Disclosure	Theft of information from data stored in the Service Information Platform (access control or authentication overridden).	Network	Low	Low	None	Unchanged	High	None	None	None	None	6.5	Medium
		Tampering	Tampering of data or settings in the Smarthome Service Information Platform.	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Malware Infection	Malware infection of the Service Information Platform (attacks launched via an external network).	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Denial of Service	DDoS (DoS) attack	Network	Low	None	None	Unchanged	None	None	High	None	None	7.5	High
		Information Disclosure	Information Disclosure via a carried-in storage device.	Physical	Low	Low	Required	Unchanged	High	None	None	None	None	4.1	Medium
		Malware Infection	Malware infection via a carried-in storage device.	Physical	Low	Low	Required	Unchanged	High	High	High	None	None	6.4	Medium
		Information Disclosure	Theft of update software.	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Tampering	Tampering of update software.	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
Smarthome Service Information Platform	EP②	Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack.	Adjacent	High	Low	None	Unchanged	High	None	None	None	None	4.8	Medium

Issues involved in the application of CVSS v3 to the calculation of risk metrics in the smarthome field are listed below.

Table 3-13: Issues of Risk Metrics Calculation Based on CVSS v3

Issue	Description
① The importance of assets to be protected cannot be reflected in the calculation of risk metrics.	Because the CVSS does not allow for the importance of assets to be protected as a risk factor, even threats exerting a major impact on an asset in a ★★ service, such as the disclosure of personal information, is not reflected in the calculation of risk metrics.
② The Life and Property impact cannot be reflected in the calculation of risk metrics.	Because the CVSS calculates the extent of impact incidents may have upon confidentiality, integrity and availability as a key risk factor, any Life and Property impact, such as that feared in a ★★★ service, is not reflected in the calculation of risk metrics.

While the application of the CVSS in the smarthome field has yielded issues in (1) and (2) above, actual calculation results made no differences in the risk metrics between the ★★ and ★★★ services. For this reason, a new, unique method of calculating risk metrics ("Smarthome Unique Method"), with security characteristics of smarthome products and services taken into consideration, is defined based on CVSS v3 in this document.

3.5.2 Definitions of Risk Metrics Calculations Based on the Smarthome Unique Method

A scheme of calculating smarthome product and service risk metrics (Smarthome Unique Method) is defined based on CVSS v3. The Smarthome Unique Method uses the following two values to rate service vulnerabilities.

Table 3-14: Vulnerability Scoring Criteria Based on the Smarthome Unique Method

No.	Item	Description
1	Base Score	The Base Score represents the severity of a vulnerability itself and is used for scoring, ahead of the implementation of security actions. ・Base Scores are calculated by rating the access confidentiality, attack impacts on the system security characteristics of Confidentiality, Integrity and Availability and on the service security characteristics of Life and Property and the Importance of Information handled, such as personal information, and so on. ・The Base Score reflects a vulnerability-specific severity and does not depend on time changes surrounding the vulnerability and the status of security actions taken in the working environment.
2	Environmental Score	The Environmental Score is a value that represents the severity of a vulnerability in a system that provides an actual service and is used to evaluate the implementation of security actions. ・The Environmental Score is calculated by reassessing the access confidentiality in the service delivery environment, impact of attacks, the status of security action implementation and so on.

These Base and Environmental Scores are calculated by solving the formulas given below, with the results being expressed from 0.0 (lowest Severity) to 10.0 (highest Severity) (in increments of 0.1).

In these Base and Environmental Score formulas, parameters for rating security characteristics (Life and Property Impact and the Importance of Information Handled) have been added to CVSS v3 for use as factors (Figure 3-2, Figure 3-3) relevant to the impacts for calculating CVSS v3 Risk Metrics. More specifically, when a product or service is exposed to a threat, if Life and Property are impacted, the Impact is raised by 1.5 times; if the product or service handles any personal information as defined by the Personal Information Protection Law, the Impact is raised by 1.2 times (see Table 3-16, Table 3-17, Table 3-25, Table 3-26). To find out more, see the Base Score and Environment Score formulas appearing later.

(1) Base Score formula

The Base Score formula is given below.

(1)Impact

Unadjusted Impact=1 - (1-C) x (1-I) x (1-A)

Impact (if Scope is Unchanged) = 6.42×Unadjusted Impact×LP×II

Impact (if Scope is changed) = (7.52 x (Unadjusted Impact -0.029) - 3.25 (Unadjusted Impact -0.02)$^{15)}$ ×LP×II

(2)Exploitability

Exploitability = 8.22×AV×AC×PR×UI

(3)Base Score

If Impact ≦ 0, Base Score = 0

If Impact > 0,

・If Scope is Unchanged

Base Score = Impact + Exploitability (*)

・If Scope is changed

Base Score = 1.08 x (Impact+ Exploitability) (*)

(*)Rounded at the second decimal place. If the result exceeds 10.0, also 10.0.

Figure 3-2: Base Score (Smarthome Unique Method) Formula

LP/II, C/I/A and AV/AC/PR/UI appearing in the formula are defined in Table 3-15. LP and II are parameters specific to smarthome products and services and represent the Life and Property Impact and the Importance of Information handled, such as personal information, respectively. Other parameters are identical to those defined by CVSS v3.

Table 3-15: Base Score Calculation Parameters

No.	Item	Description
1	Life and Property (LP) Impact	Assesses the possibility of a vulnerability attack impacting Life and Property.
2	Information Importance (II)	Assesses the importance of information (such as personal information) that is impacted by a vulnerability attack.
3	Confidentiality(C) Impact	Assesses the possibility of information leaking from the possible scope of impact from a vulnerability attack.
4	Integrity(I) Impact	Assesses the possibility of information in the possible scope of impact being tampered on a vulnerability attack.
5	Availability(A) Impact	Assesses the possibility of operations in the possible scope of impact being delayed or shut down on a vulnerability attack.
6	Attack Vector (AV)	Assesses from where an attacker can successfully attack the vulnerable component.
7	Attack Confidentiality (AC)	Assesses the confidentiality of the conditions an attacker must meet before successfully attacking a vulnerable component.
8	Privileges Required (PR)	Assesses the level of privileges an attacker must possess before successfully attacking a vulnerable component.
9	User Interaction (UI)	Assesses the level of user interaction an attacker must possess before successfully attacking a vulnerable component.
10	Scope (S)	Assesses the scope of impact from attacks at a vulnerable component.

The values that can be assumed by the individual items are listed below.

Table 3-16 Life and Property (LP) Impact

Item	Description	Value
Yes（Y）	If a threat occurs, it would have impact on Life and Property.	1.5
None（N）	If a threat occurs, it would no impact on Life and Property.	1.0

Table 3-17: Information Importance (II)

Item	Description	Value
High (H)	Any sensitive information as defined below is contained. Personal information specified in the Personal Information Protection Law (Article 2) is the kind of information that relates to an existing individual and that falls under any of the following categories: ・Information that contains the name of an individual, that individual's date of birth and so on allowing that individual to be identified. Such information includes what can be easily checked against other information to help identify an individual. ・Information that contains a personal identification code (which allows a particular individual to be identified by itself). A code that represents properties of a part of a body, converted for computer use. A code that is assigned to each individual concerned in service usage or in a document.	1.2
None (N)	No sensitive information is contained.	1.0

Table 3-18: Confidentiality (C), Integrity (I) and Availability (A) Impacts

Item	High (H)	Low (L)	No (N)
Confidentiality (C)	When a threat occurs, user information and sensitive system information is compromised in its entirety, with the impact extending to the whole.	When a threat occurs, user information and sensitive system information is compromised in part, but with the impact being limited.	When a threat occurs, user information and sensitive system information is not compromised, with no impact arising.
	Value: 0.56	Value: 0.22	Value: 0.0

Integrity（I）	When a threat occurs, user information and sensitive system information becomes accessible for tampering, with the impact extending to the whole.	When a threat occurs, user information and sensitive system information becomes accessible for tampering, but with the impact being limited.	When a threat occurs, user information and sensitive system information is not accessible for tampering, with no impact arising.
	Value: 0.56	Value: 0.22	Value: 0.0
Availability（A）	When a threat occurs, the service may be shut down completely.	When a threat occurs, the service may be temporarily shut down or delayed.	When a threat occurs, the service is neither shut down nor delayed, with no impact arising.
	Value: 0.56	Value: 0.22	Value: 0.0

Table 3-19: Attack Vector (AV)

Item	Description	Value
Network (N)	The vulnerable component can be remotely attacked via a network. ・The Smarthome Service Information Platform is attacked from the Internet (N). ・The gateway is attacked from the Internet.	0.85
Adjacent (A)	The vulnerable component needs to be attacked from an adjacent network. ・The attack is launched by making connections to a Smarthome Service Information Platform network. ・The attack is launched by making connections to the wireless LAN of a wireless router to which the gateway is connected. ・The attack is launched by making connections to the gateway LAN terminal or wireless LAN.	0.62
Local (L)	The vulnerable component needs to be attacked from a local environment.	0.55

	・The attack is launched by logging in to a Smarthome Service Information Platform server. ・The attack is launched by making connections to the gateway serial console.	
Physical (P)	The vulnerable component needs to be attacked from a physical access environment. ・The attack is launched by making connections to a physical terminal of the gateway, such as a JEM-A terminal (HA terminal) or USB terminal.	0.20

Table 3-20: Attack Confidentiality (AC)

Item	Description	Value
Low (L)	An attacker can always attack the vulnerable component, without needing special attack conditions.	0.77
High (H)	Attack conditions that depend on other than the attacker exist. These conditions might include, for example: ・An attacker needs to collect information about the vulnerable component beforehand, such as setup information, sequence numbers and common keys. ・An attacker needs to define the environmental conditions for a successful attack, such as the conditions under which contention occurs and those under which heap spraying succeeds. ・An attacker requires an environment to launch a man-in-the-middle attack.	0.44

Table 3-21: Privileges Required (PR)

Item	Description	Value	
		if Scope is Unchanged	if Scope is changed
None (N)	An attacker does not require any special privileges.	0.85	
Low (L)	An attacker only requires basic privileges on the vulnerable component.	0.62	0.68
High	An attacker requires an equivalent of administrator	0.27	0.50

(H)	privileges on the vulnerable component.		

Table 3-22: User Interaction (UI)

Item	Description	Value
None (N)	Vulnerabilities can be exploited without interaction from any user.	0.85
Required (R)	User interaction, such as clicking a link, browsing a file or changing settings, is required for a successful exploit.	0.62

Further, “if Scope is changed” and “if Scope is Unchanged” are defined in Table 3-23.

Table 3-23: Scope (S)

Item	Description
Unchanged (U)	The scope of impact falls in the same extent of authentication as the target. For example, Unauthorized Access to a system that shares an access token is an Unchanged Scope.
Changed (C)	The scope of impact differs from the vulnerable component in its extent of authentication.

(2) Environmental Score formula

The Environmental Score formula is given below.

(1)Modified Impact

Modified Unadjusted Impact =min [(1 - (1 - MC CR)× (1 - MI IR)× (1 - MA AR)),0.915]

◎if Scope is Unchanged

Modified Impact = 6.42×Modified Unadjusted Impact×MLP×MII

◎if Scope is changed

Modified Impact = (7.52× (Modified Unadjusted Impact -0.029)

-3.25× (Modified Unadjusted Impact -0.02)$^{15)}$ ×MLP×MII

(2)Modified Exploitability

Modified Exploitability = 8.22× MAV× MAC× MPR× MUI

(3)Environmental Score

If Modified Impact≦ 0, Environmental Score = 0

If Modified Impact > 0

◎if Scope is Unchanged

Modified Base Score =Modified Impact+Modified Exploitability (※1)

Environmental Score =Modified Base Score ×E×RL×RC (※2)

◎if Scope is changed

Modified Base Score = 1.08× (Modified Impact+Modified Exploitability) (*1)

Environmental Score =Modified Base Score×E×RL×RC (※2)_

(※1)Rounded at the second decimal place. If the result exceeds 10.0, also 10.0.

(※2)Rounded at the second decimal place.

E: Exploitability, RL: Remediation Level, RC: Since the value of Report Confidence is unchanged from the current method of metrics calculation, refer to CVSS v3 [16][17].

Figure 3-3: Environmental Score (Smarthome Unique Method) Formula

MLP/MI, CR/IR/AR, MC/MI/MA and MAV/MAC/MPR/MUI appearing in the formula are defined in Table 3-24. Here, MLP/MII represent Life and Property Impact and Information Importance of personal information, etc., respectively, and correspond to LP and II in the Base Score metrics. Other parameters are identical to those defined by CVSS v3.

Table 3-24: Environmental Score Calculation Parameters

No.	Item	Description
Life and Property impact and Information Importance.		
1	Modified Life and Property Impact (MLP)	Reassesses the possibility of a vulnerability attack impacting Life and Property.
2	Modified Information Importance (MII)	Reassesses the importance of information (e.g., personal information) when it is impacted by a vulnerability attack.
Security requirements for the target system		
3	Confidentiality Requirement (CR)	Scores the level of importance of confidentiality in the target system.
4	Integrity Requirement (IR)	Scores the level of importance of integrity in the target system.
5	Availability Requirement (AR)	Scores the level of importance of availability in the target system.
Reassessment of Base metrics with environmental conditions taken into consideration.		
6	Modified Confidentiality Impact (MC)	Reassess the possibility of information leaking from the possible scope of impact from a vulnerability attack.
7	Modified Integrity Impact (MI)	Reassess the possibility of information in the possible scope of impact being tampered on a vulnerability attack.
8	Modified Availability Impact (MA)	Reassesses the possibility of operations in the possible scope of impact being delayed or shut down on a vulnerability attack.
9	Modified Attack Vector (MAV)	Reassesses from where an attacker can successfully attack the vulnerable component.
10	Modified Attack Confidentiality (MAC)	Reassesses the confidentiality of the conditions an attacker must meet before successfully attacking a vulnerable component.
11	Modified Privileges Required (MPR)	Reassesses the level of privileges an attacker must possess before successfully attacking a vulnerable component.
12	Modified User Interaction (MUI)	Reassesses the level of user interaction an attacker must possess before successfully attacking a vulnerable

		component.
13	Modified Scope (MS)	Reassesses the scope of impact from attacks at a vulnerable component.

The values that can be assumed by the individual items are listed below.

Table 3-25: Modified Life and Property Impact (MLP)

Item	Description	Value
Not Defined (X)	Not assessed (the same items as for calculating the Base Score are used).	
Yes（Y)	Same as the definition used for calculating the Base Score （See Table 3-16)	1.5
No (N)		1.0

Table 3-26: Modified Information Importance (MII)

Item	Description	Value
Not Defined (X)	Not assessed (the same items as for calculating the Base Score are used).	
High (H)	Same as the definition used for calculating the Base Score （See Table 3-17)	1.2
No (N)		1.0

Table 3-27: Security requirements for the target system （CR/IR/AR）

Item	Not Defined (X)	High (H)	Medium (M)	Low (L)
Confidentiality Requirement (CR)	This item is not assessed.	Loss of Confidentiality is likely to have a catastrophic adverse effect.	Loss of Confidentiality is likely to have a serious adverse effect.	Loss of Confidentiality is likely to have a limited adverse effect.
	Value: 1.0	Value: 1.5	Value: 1.0	Value: 0.5
Integrity Requirement (IR)	This item is not assessed.	Loss of Integrity is likely to have a catastrophic adverse effect.	Loss of Integrity is likely to have a serious adverse effect.	Loss of Integrity is likely to have a limited adverse effect.
	Value: 1.0	Value: 1.5	Value: 1.0	Value: 0.5
Availability Requirement (AR)	This item is not assessed.	Loss of Availability is likely to have a catastrophic adverse effect.	Loss of Availability is likely to have a serious adverse effect.	Loss of Availability is likely to have a limited adverse effect.
	Value: 1.0	Value: 1.5	Value: 1.0	Value: 0.5

Table 3-28: Modified Confidentiality Impact (MC)

Item	Description	Value
Not Defined （X)	Not assessed (the same items as for calculating the Base Score are used).	
High (H)	Same as the definition used for calculating the Base Score （See "Confidentiality" in Table 3-18)	0.56
Low （L)		0.22
No (N)		0.0

Table 3-29: Modified Integrity Impact (MI)

Item	Description	Value
Not Defined （X)	Not assessed (the same items as for calculating the Base Score are used).	
High (H)	Same as the definition used for calculating the Base Score （see "Integrity" in Table 3-18)	0.56
Low （L)		0.22
No (N)		0.0

Table 3-30: Modified Availability Impact (MA)

Item	Description	Value
Not Defined （X)	Not assessed (the same items as for calculating the Base Score are used).	
High (H)	Same as the definition used for calculating the Base Score （see "Availability" in Table 3-18)	0.56
Low （L)		0.22
No (N)		0.0

Table 3-31: Modified Attack Vector (MAV)

Item	Description	Value
Not Defined （X)	Not assessed (the same items as for calculating the Base Score are used).	
Network （N)	Same as the definition used for calculating the Base Score （See Table 3-19)	0.85
Adjacent (A)		0.62
Local (L)		0.55
Physical (P)		0.20

Table 3-32: Modified Attack Confidentiality (MAC)

Item	Description	Value
Not Defined（X）	Not assessed (the same items as for calculating the Base Score are used).	
Low（L）	Same as the definition used for calculating the Base Score（See Table 3-20）.	0.77
High (H)		0.44

Table 3-33: Modified Privileges Required (MPR)

Item	Description	Value	
		if Scope is Unchanged	if Scope is changed
Not Defined（X）	Not assessed (the same items as for calculating the Base Score are used).		
None (N)	Same as the definition used for calculating the Base Score（See Table 3-21）.	0.85	
Low（L）		0.62	0.68
High (H)		0.27	0.50

Table 3-34: Modified User Interaction (MUI)

Item	Description	Value
Not Defined（X）	Not assessed (the same items as for calculating the Base Score are used).	
None (N)	Same as the definition used for calculating the Base Score（See Table 3-22）.	0.85
Required（R）		0.62

Table 3-35: Modified Scope (MS)

Item	Description
Not Defined（X）	Not assessed (the same items as for calculating the Base Score are used).
Unchanged (U)	Same as the definition used for calculating the Base Score（See Table 3-23）.
Changed（C）	

(3) Severity rating scale

According to the Smarthome Unique Method, severity ratings are set the same way as under CVSS v3, as follows:

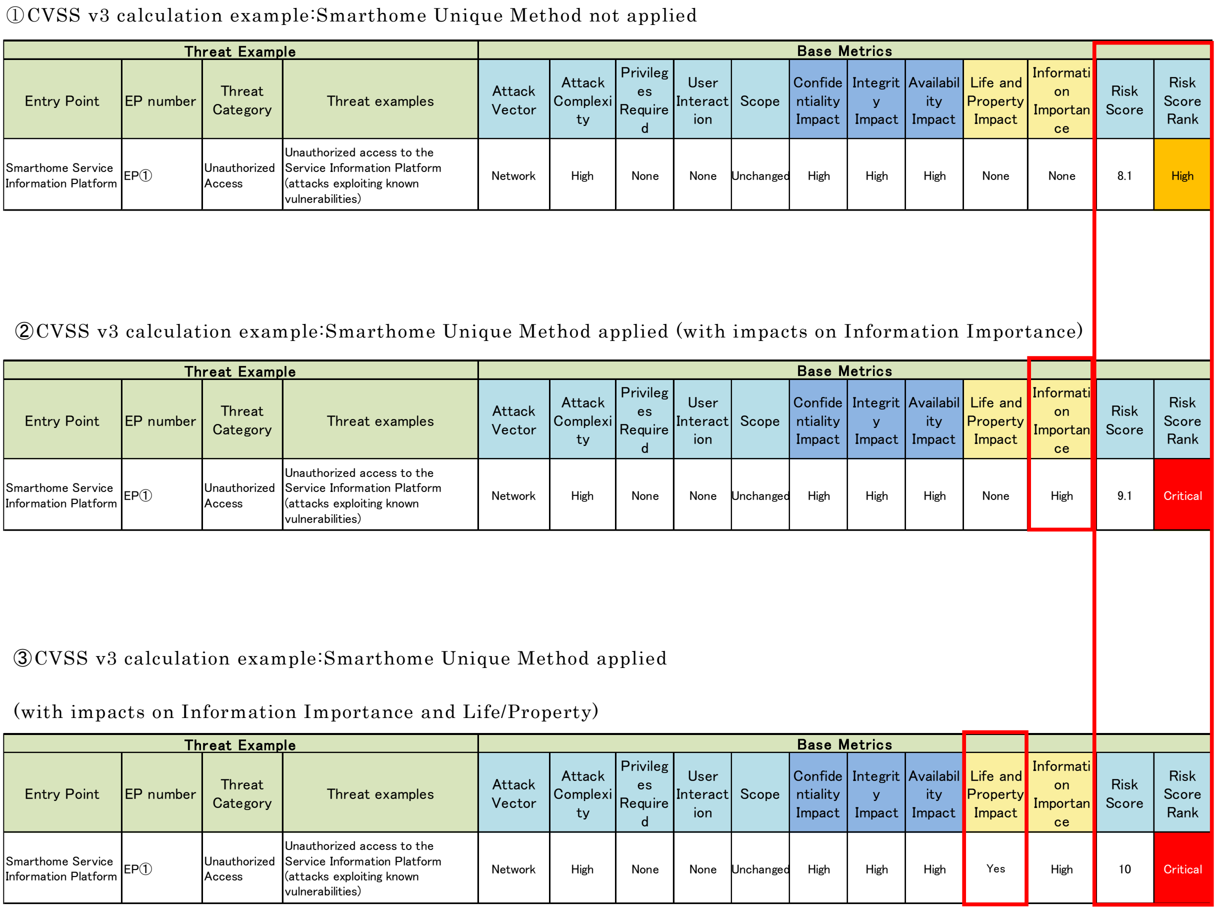
Table 3-36: Severity Rating Scale

Severity	Critical	High	Medium	Low	None
Score	9.0～10.0	7.0～8.9	4.0～6.9	0.1～3.9	0

(4) Calculation of risk metrics based on the Smarthome Unique Method

Table 3-37 summarizes the calculations of risk metrics based on the Smarthome Unique Method.

Table 3-37: Risk Metrics of Services Based on the Smarthome Unique Method



①CVSS v3 calculation example:Smarthome Unique Method not applied

Threat Example				Base Metrics												
Entry Point	EP number	Threat Category	Threat examples	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk Score	Risk Score Rank
Smarthome Service Information Platform	EP①	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High

②CVSS v3 calculation example:Smarthome Unique Method applied (with impacts on Information Importance)

Threat Example				Base Metrics											
Entry Point	EP number	Threat Category	Threat examples	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk Score	Risk Score Rank
Smarthome Service Information Platform	EP①	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	Network	High	None	None	Unchanged	High	High	High	None	High	9.1	Critical

③CVSS v3 calculation example:Smarthome Unique Method applied

(with impacts on Information Importance and Life/Property)

Threat Example				Base Metrics											
Entry Point	EP number	Threat Category	Threat examples	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk Score	Risk Score Rank
Smarthome Service Information Platform	EP①	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical

First, (1) gives an example of risk metrics calculated under the current CVSS v3 without the Smarthome Unique Method applied, where a risk metric value of 8.1 (High) is determined. In (2), a risk metric value of 9.3 (Critical) is determined for the same potential threats when a use case in which personal information is handled in a ★★ service is assumed. Further, in (3) above, a risk metric value of 10 (Critical) is worked out for the same potential threats involving the use of personal information or possible the Life and Property impact.

Thus, the Smarthome Unique Method has been found to identify differences in the assessment results even in the threat cases in which personal information is among the assets to be protected or in which a Life and Property impact is involved, when compared with the current CVSS v3.

3.5.3 Results of Risk Metrics Calculations Based on the Smarthome Unique Method

Risk metrics are calculated for each individual incident using the Smarthome Unique Method defined in the foregoing section. Table 3-38 and Table 3-39 summarize the results of calculation of the Automatic Shutter Opening/Closing Service (★★) and the On-Call Security Service (★★★), respectively.

Table 3-38 Automatic Shutter Opening/Closing Service (★★) Risk Metrics (before Security Action)

Threat Example				Base Metrics											
Entry Point	EP Number	Threat Category	Threat Example	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk value	Risk value rank
Smarthome Service Information Platform	EP①	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities).	Network	High	None	None	Unchanged	High	High	High	None	High	9.3	Critical
		Information Disclosure	Theft of information from data stored in the Service Information Platform (access control or inadequate authentication).	Network	Low	Low	None	Unchanged	High	None	None	None	High	7.2	High
		Tampering	Tampering of data or settings in the Service Information Platform.	Network	High	None	None	Unchanged	High	High	High	None	High	9.3	Critical
		Spoofing	Attack by tampered message by disguising oneself as the Service Provider Information Platform or the home gateway during communication via an API.	Network	High	None	None	Unchanged	Low	High	High	None	High	8.8	High
		Malware Infection	Malware infection of the Service Information Platform (attacks launched via an external network).	Network	High	None	None	Unchanged	High	High	High	None	High	9.3	Critical
		Denial of Service	DDoS (DoS) attack.	Network	Low	None	None	Unchanged	None	None	High	None	None	7.5	High
		Information Disclosure	Information Disclosure via a carried-in storage device.	Physical	Low	Low	Required	Unchanged	High	None	None	None	High	4.9	Medium
		Malware Infection	Malware infection via a carried-in storage device.	Physical	Low	Low	Required	Unchanged	High	High	High	None	High	7.6	High
		Information Disclosure	Theft of update software.	Network	High	None	None	Unchanged	High	High	High	None	High	9.3	Critical
		Tampering	Tampering of update software.	Network	High	None	None	Unchanged	High	High	High	None	High	9.3	Critical
Path of Communication between the Smarthome Service Information Platform and the Internet	EP②	Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	Adjacent	High	Low	None	Unchanged	High	None	None	None	High	5.5	Medium

Threat Example				Base Metrics											
Entry Point	EP Number	Threat Category	Threat Example	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk value	Risk value rank
Service Provider Information Platform	EP③	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Information Disclosure	Theft of information from data stored in the Service Information Platform (access control or inadequate authentication).	Network	Low	Low	None	Unchanged	High	None	None	None	None	6.5	Medium
		Tampering	Tampering of data or settings in the Service Information Platform.	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Spoofing	Attack by tampered message by disguising oneself as the Smarthome Service Information Platform during communication via an API.	Network	High	None	None	Unchanged	Low	High	High	None	None	7.7	High
		Malware Infection	Malware infection of the Service Information Platform (attacks launched via an external network).	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Denial of Service	DDoS (DoS) attack.	Network	Low	None	None	Unchanged	None	None	High	None	None	7.5	High
		Information Disclosure	Information Disclosure via a carried-in storage device.	Physical	Low	Low	Required	Unchanged	High	None	None	None	None	4.1	Medium
		Malware Infection	Malware infection via a carried-in storage device.	Physical	Low	Low	Required	Unchanged	High	High	High	None	None	6.4	Medium
		Information Disclosure	Theft of update software.	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Tampering	Tampering of update software.	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
Path of Communication between the Service Provider Information Platform and the Internet	EP④	Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	Adjacent	High	Low	None	Unchanged	High	None	None	None	None	4.8	Medium

Threat Example				Base Metrics											
Entry Point	EP Number	Threat Category	Threat Example	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk value	Risk value rank
Home Gateway	EP⑤	Unauthorized Access	Unauthorized access to the home gateway (attacks exploiting known vulnerabilities).	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Information Disclosure	Theft of information from data or settings stored in the home gateway (access control or inadequate authentication).	Network	Low	Low	None	Unchanged	High	None	None	None	None	6.5	Medium
		Tampering	Tampering of data or settings stored in the home gateway.	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Spoofing	Attack by tampered message by disguising oneself as the Service Provider Information Platform during communication via an API.	Network	High	None	None	Unchanged	Low	High	High	None	None	7.7	High
		Malware Infection	Malware infection of the home gateway (attacks launched via an external Internet)	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Denial of Service	DDoS (DoS) attack.	Network	Low	None	None	Unchanged	None	None	High	None	None	7.5	High
		Information Disclosure	Information Disclosure via a connected storage device.	Physical	Low	Low	Required	Unchanged	High	None	None	None	None	4.1	Medium
		Malware Infection	Malware infection via a connected storage device.	Physical	Low	Low	Required	Unchanged	High	High	High	None	None	6.4	Medium
		Malware Infection	Malware Infection from internal equipment on the LAN	Adjacent	Low	None	None	Unchanged	High	High	High	None	None	8.8	High
		Springboard	Abused as a springboard for launching attacks, e.g., as a bot.	Network	Low	Low	None	Change	None	None	None	None	None	3.2	Low
Path of Communication between the Home Gateway and the Internet	EP⑥	Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	Adjacent	High	Low	None	Unchanged	High	None	None	None	None	4.8	Medium

Threat Example				Base Metrics												
Entry Point	EP Number	Threat Category	Threat Example	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk value	Risk value rank
Smarthome-compatible Devices	EP⑦	Unauthorized Access	Unauthorized access to a device (attacks exploiting known vulnerabilities).	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Information Disclosure	Theft of information from data or settings stored in a device (access control or inadequate authentication)	Network	Low	Low	None	Unchanged	High	None	None	None	None	6.5	Medium
		Tampering	Tampering of data or settings stored in a device.	Network	High	None	None	Unchanged	High	High	High	None	None	8.1	High
		Spoofing	Attack by tampered message by disguising oneself as the home gateway during communication.	Network	High	None	None	Unchanged	Low	High	High	None	None	7.7	High
		Information Disclosure	Information Disclosure via a connected storage device (any compatible device, such as a USB interface).	Physical	Low	Low	Required	Unchanged	High	None	None	None	None	4.1	Medium
		Malware Infection	Malware infection via a connected storage device (any compatible device, such as a USB interface).	Physical	Low	Low	Required	Unchanged	High	High	High	None	None	6.4	Medium
		Springboard	Abused as a springboard for launching attacks, e.g., as a bot.	Network	Low	Low	None	Change	Low	None	None	None	None	5	Medium
Path of Communication between Smarthome-compatible Devices and the Home Gateway	EP⑧	Spoofing	Spoofing of a device control signal by a man-in-the-middle attack.	Adjacent	High	Low	None	Change	Low	High	High	None	None	7.9	High
		Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	Adjacent	High	Low	None	Unchanged	High	None	None	None	None	4.8	Medium

Threat Example				Base Metrics											
Entry Point	EP Number	Threat Category	Threat Example	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk value	Risk value rank
Smartphone Application	EP⑨	Information Disclosure	Information Disclosure stored in a device due to a vulnerability in a smartphone application.	Network	High	None	None	Change	High	None	None	None	High	7.6	High
		Information Disclosure	Information Disclosure due to an unauthorized login to a smartphone application.	Network	Low	Low	None	Unchanged	High	None	None	None	High	7.2	High
		Spoofing	Any unauthorized operation of a device caused by illegal login to a smartphone application. (spoofing)	Network	Low	Low	None	Change	None	None	High	None	None	7.7	High
Path of Communication between a Smartphone and the Home Gateway	EP⑩	Spoofing	Spoofing of a device control signal by a man-in-the-middle attack.	Adjacent	High	Low	None	Change	Low	High	High	None	None	7.9	High
		Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	Adjacent	High	Low	None	Unchanged	High	None	None	None	High	5.5	Medium

※Assumptions of Risk Metrics Calculation

・According to the use case of the automatic shutter opening/closing service, no personal information will be stored on or transmitted to and from Smarthome-compatible devices.

Table 3-39: On-Call Security Service (★★★) Risk Metrics (before Security Action)

Threat Example				Base Metrics											
Entry Point	EP number	Threat Category	Threat examples	Attack Vector	Attack Confidentiality	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk Score	Risk Score Rank
Smarthome Service Information Platform	EP①	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
		Information Disclosure	Theft of information from data stored in the Service Information Platform (access control or inadequate authentication)	Network	Low	Low	None	Unchanged	High	None	None	None	High	7.2	High
		Tampering	Tampering of data or settings in the Service Information Platform.	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
		Spoofing	Attack by tampered message by disguising oneself as the Service Provider Information Platform or the home gateway during communication via an API.	Network	High	None	None	Unchanged	Low	High	High	Yes	High	10	Critical
		Malware Infection	Malware infection of the Service Information Platform (attacks launched via an external network).	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
		Denial of Service	DDoS (DoS) attack.	Network	Low	None	None	Unchanged	None	None	High	Yes	None	9.3	Critical
		Information Disclosure	Information Disclosure via a carried-in storage device.	Physical	Low	Low	Required	Unchanged	High	None	None	None	High	4.9	Medium
		Malware Infection	Malware infection via a carried-in storage device.	Physical	Low	Low	Required	Unchanged	High	High	High	Yes	High	10	Critical
		Information Disclosure	Theft of update software.	Network	High	None	None	Unchanged	High	High	High	None	High	9.3	Critical
		Tampering	Tampering of update software.	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
Path of Communication between the Smarthome Service Information Platform	EP②	Information Disclosure	Theft of information on an Internet path by-a man-in-the-middle attack.	Adjacent	High	Low	None	Unchanged	High	None	None	None	High	5.5	Medium

Threat Example				Base Metrics											
Entry Point	EP number	Threat Category	Threat examples	Attack Vector	Attack Confidentiality	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk Score	Risk Score Rank
Service Provider Information Platform	EP③	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
		Information Disclosure	Theft of information from data stored in the Service Information Platform (access control or inadequate authentication).	Network	Low	Low	None	Unchanged	High	None	None	None	High	7.2	High
		Tampering	Tampering of data or settings in the Service Information Platform.	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
		Spoofing	Attack by tampered message by disguising oneself as the Smarthome Service Information Platform during communication via an API.	Network	High	None	None	Unchanged	Low	High	High	Yes	High	10	Critical
		Malware Infection	Malware infection of the Service Information Platform (attacks launched via an external network).	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
		Denial of Service	DDoS (DoS) attack.	Network	Low	None	None	Unchanged	None	None	High	Yes	None	9.3	Critical
		Information Disclosure	Information Disclosure via a carried-in storage device.	Physical	Low	Low	Required	Unchanged	High	None	None	None	High	4.9	Medium
		Malware Infection	Malware infection via a carried-in storage device.	Physical	Low	Low	Required	Unchanged	High	High	High	Yes	High	10	Critical
		Information Disclosure	Theft of update software.	Network	High	None	None	Unchanged	High	High	High	None	High	9.3	Critical
		Tampering	Tampering of update software.	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
Path of communication between the Service Provider Information Platform and the Internet	EP④	Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	Adjacent	High	Low	None	Unchanged	High	None	None	None	High	5.5	Medium

Threat Example				Base Metrics											
Entry Point	EP number	Threat Category	Threat examples	Attack Vector	Attack Confidentiality	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk Score	Risk Score Rank
Home Gateway	EP⑤	Unauthorized Access	Unauthorized access to the home gateway (attacks exploiting known vulnerabilities).	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
		Information Disclosure	Theft of information from data or settings stored in the home gateway (access control or inadequate authentication).	Network	Low	Low	None	Unchanged	High	None	None	None	High	7.2	High
		Tampering	Tampering of data or settings stored in the home gateway.	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
		Spoofing	Attack by tampered message by disguising oneself as the Service Information Platform during communication via an API.	Network	High	None	None	Unchanged	Low	High	High	Yes	High	10	Critical
		Malware Infection	Malware infection of the home gateway (attacks launched via an external Internet)	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
		Denial of Service	DDoS (DoS) attack.	Network	Low	None	None	Unchanged	None	None	High	Yes	None	9.3	Critical
		Information Disclosure	Information Disclosure via a connected storage device.	Physical	Low	Low	Required	Unchanged	High	None	None	None	High	4.9	Medium
		Malware Infection	Malware infection via a connected storage device.	Physical	Low	Low	Required	Unchanged	High	High	High	Yes	High	10	Critical
		Malware Infection	Malware Infection from internal equipment on the LAN	Adjacent	Low	None	None	Unchanged	High	High	High	Yes	High	10	Critical
		Springboard	Abused as a springboard for launching attacks, e.g., as a bot.	Network	Low	Low	None	Change	None	None	None	None	None	3.2	Low
Path of Communication between the Home Gateway and the Internet	EP⑥	Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	Adjacent	High	Low	None	Unchanged	High	None	None	None	High	5.5	Medium

Threat Example				Base Metrics											
Entry Point	EP number	Threat Category	Threat examples	Attack Vector	Attack Confidentiality	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk Score	Risk Score Rank
Smarthome-compatible Devices	EP⑦	Unauthorized Access	Unauthorized access to a device (attacks exploiting known vulnerabilities).	Network	High	None	None	Unchanged	High	High	High	Yes	High	10	Critical
		Information Disclosure	Theft of information from data or settings stored in a device (access control or inadequate authentication).	Network	Low	Low	None	Unchanged	High	None	None	None	High	7.2	High
		Tampering	Tampering of data or settings stored in a device.	Network	High	None	None	Unchanged	High	High	High	Yes	None	10	Critical
		Spoofing	Attack by tampered message by disguising oneself as the home gateway during communication.	Network	High	None	None	Unchanged	Low	High	High	Yes	None	10	Critical
		Information Disclosure	Information Disclosure via a connected storage device (any compatible device, such as a USB interface).	Physical	Low	Low	Required	Unchanged	High	None	None	None	High	4.9	Medium
		Malware Infection	Malware infection via a connected storage device (any compatible device, such as a USB interface).	Physical	Low	Low	Required	Unchanged	High	High	High	Yes	High	10	Critical
		Springboard	Abused as a springboard for launching attacks, e.g., as a bot.	Network	Low	Low	None	Change	Low	None	None	None	None	5	Medium
Path of Communication between Smarthome-compatible Devices and the Home Gateway	EP⑧	Spoofing	Spoofing of a device control signal by a man-in-the-middle attack.	Adjacent	High	Low	None	Change	Low	High	High	Yes	None	10	Critical
		Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	Adjacent	High	Low	None	Unchanged	High	None	None	None	High	5.5	Medium

Threat Example				Base Metrics											
Entry Point	EP number	Threat Category	Threat examples	Attack Vector	Attack Confidentiality	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability Impact	Life and Property Impact	Information Importance	Risk Score	Risk Score Rank
Smartphone Application	EP⑨	Information Disclosure	Information Disclosure stored in a device due to a vulnerability in a smartphone application.	Network	High	None	None	Change	High	None	None	None	High	7.6	High
		Information Disclosure	Information Disclosure due to an unauthorized login to a smartphone application.	Network	Low	Low	None	Unchanged	High	None	None	None	High	7.2	High
		Spoofing	Any unauthorized operation of a device caused by illegal login to a smartphone application.	Network	Low	Low	None	Change	None	None	High	None	None	7.7	High
Path of Communication between a Smartphone and the Home Gateway	EP⑩	Spoofing	Spoofing of a device control signal by a man-in-the-middle attack.	Adjacent	High	Low	None	Change	Low	High	High	None	None	7.9	High
		Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	Adjacent	High	Low	None	Unchanged	High	None	None	None	High	5.5	Medium

3.6 Risk Analysis and Assessment Summary

The preceding sections have presented the summary and the procedural flow of risk analyses and assessments of smarthome products and services. In the process, a new and unique method of calculation has been defined to allow the Life and Property impact and Importance of Information handled, such as personal information, to be reflected in the calculation of risk metrics.
The application of the Smarthome Unique Method to the use case described in Sections 2.4.1 and 2.4.2 has verified that the Life and Property impact and Importance of Information handled are reflected in the risk metrics of the threats influencing Life and Property and of handling personal information.

3.7 Exploring Security Actions

Possible security actions are explored starting with threats having the highest level of severity based on risk metrics calculations. Security action can be set by consulting “Table 3-6 and Table 3-7 Action Candidate Lists" in “A Guide to Security Design in IoT Development”[6], "Annex2 Action Item List for Physical and Technical Action" in “Guidelines on Information Security Actions in Providing Cloud Services(Second Edition)” [9], and frameworks, such as those detailed in OTA [18] and OWASP [19]. In exploring possible actions, allowance should also be made for the occurrence frequency of each incidence, the impact when it occurs, the cost of actions to deal with and so on. Security actions considered in this document will be detailed in Chapter 4 and after.

Once security actions are thus formulated, the validity and cost effectiveness can be verified by assessing the CVSS environmental metrics.

Table 3-40 and Table 3-41 show the metric calculations of the Automatic Shutter Opening/Closing Service (★★) and the On-Call Security Service (★★★), respectively.

Table 3-40 Automatic Shutter Opening/Closing Service (★★) Risk Metrics (after Security Action)

Threat Example				Environmental Metrics														
Entry point	EP Number	Threat Category	Threat Example	Requirement for Confidentiality	Requirement for Integrity	Requirement for Availability	Modified Attack Vector	Modified Attack Complexity	Modified Privileges Required	Modified User Interaction	Modified Scope	Modified Confidentiality Impact	Modified Integrity Impact	Modified Availability Impact	Modified Life and Property Impact	Modified Information Importance	Risk Score	Risk Score Rank
Smarthome Service Information Platform	EP①	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Information Disclosure	Theft of information from data stored in the Service Information Platform (access control or inadequate authentication).	High	High	Low	Network	High	High	None	Unchanged	Low	Low	None	None	High	5	Medium
		Tampering	Tampering of data or settings in the Service Information Platform.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Spoofing	Attack by tampered message by disguising oneself as the Service Provider Information Platform or the home gateway during communication via an API.	Low	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	6.9	Medium
		Malware Infection	Malware infection of the Service Information Platform (attacks launched via an external network).	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Denial of Service	DDoS (DoS) attack.	Low	Low	High	Network	Low	None	None	Unchanged	None	None	Low	None	None	6.1	Medium
		Information Disclosure	Information Disclosure via a carried-in storage device.	High	Low	Low	Physical	Low	High	Required	Unchanged	Low	None	None	None	High	2.8	Low
		Malware Infection	Malware infection via a carried-in storage device.	High	High	High	Physical	Low	High	Required	Unchanged	Low	Low	Low	None	High	5.6	Medium
		Information Disclosure	Theft of update software.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Tampering	Tampering of update software.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
Path of Communication between the Smarthome Service Information Platform and the Internet	EP②	Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	High	High	Low	Adjacent	High	High	None	Unchanged	Low	None	None	None	High	3.1	Low

Threat Example				Environmental Metrics														
Entry point	EP Number	Threat Category	Threat Example	Requirement for Confidentiality	Requirement for Integrity	Requirement for Availability	Modified Attack Vector	Modified Attack Complexity	Modified Privileges Required	Modified User Interaction	Modified Scope	Modified Confidentiality Impact	Modified Integrity Impact	Modified Availability Impact	Modified Life and Property Impact	Modified Information Importance	Risk Score	Risk Score Rank
Service Provider Information Platform	EP③	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.8	Medium
		Information Disclosure	Theft of information from data stored in the Service Information Platform (access control or inadequate authentication).	High	High	Low	Network	High	High	None	Unchanged	Low	Low	None	None	None	4.3	Medium
		Tampering	Tampering of data or settings in the Service Information Platform.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.8	Medium
		Spoofing	Attack by tampered message by disguising oneself as the Smarthome Service Information Platform during communication via an API.	Low	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.1	Medium
		Malware Infection	Malware infection of the Service Information Platform (attacks launched via an external network).	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.8	Medium
		Denial of Service	DDoS (DoS) attack.	Low	Low	High	Network	Low	None	None	Unchanged	None	None	Low	None	None	6.1	Medium
		Information Disclosure	Information Disclosure via a carried-in storage device.	High	Low	Low	Physical	Low	High	Required	Unchanged	Low	None	None	None	None	2.4	Low
		Malware Infection	Malware infection via a carried-in storage device.	High	High	High	Physical	Low	High	Required	Unchanged	Low	Low	Low	None	None	4.8	Medium
		Information Disclosure	Theft of update software.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.8	Medium
		Tampering	Tampering of update software.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.8	Medium
Path of Communication between the Service Provider Information Platform and the Internet	EP④	Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	High	High	Low	Adjacent	High	High	None	Unchanged	Low	None	None	None	None	2.7	Low

Threat Example				Environmental Metrics														
Entry point	EP Number	Threat Category	Threat Example	Requirement for Confidentiality	Requirement for Integrity	Requirement for Availability	Modified Attack Vector	Modified Attack Complexity	Modified Privileges Required	Modified User Interaction	Modified Scope	Modified Confidentiality Impact	Modified Integrity Impact	Modified Availability Impact	Modified Life and Property Impact	Modified Information Importance	Risk Score	Risk Score Rank
Home Gateway	EP⑤	Unauthorized Access	Unauthorized access to the home gateway (attacks exploiting known vulnerabilities).	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.8	Medium
		Information Disclosure	Theft of information from data or settings stored in the home gateway (access control or inadequate authentication)	High	High	Low	Network	High	High	None	Unchanged	Low	Low	None	None	None	4.3	Medium
		Tampering	Tampering of data or settings stored in the home gateway.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.8	Medium
		Spoofing	Attack by tampered message by disguising oneself as the Service Information Platform during communication via an API.	Low	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.1	Medium
		Malware Infection	Malware infection of the home gateway (attacks launched via an external Internet)	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.8	Medium
		Denial of Service	DDoS (DoS) attack.	Low	Low	High	Network	Low	None	None	Unchanged	None	None	Low	None	None	6.1	Medium
		Information Disclosure	Information Disclosure via a connected storage device.	High	Low	Low	Physical	Low	High	Required	Unchanged	Low	None	None	None	None	2.4	Low
		Malware Infection	Malware infection via a connected storage device.	High	High	High	Physical	Low	High	Required	Unchanged	Low	Low	Low	None	None	4.8	Medium
		Malware Infection	Malware Infection from internal equipment on the LAN	High	High	High	Adjacent	Low	None	None	Unchanged	Low	Low	Low	None	None	7.4	High
		Springboard	Abused as a springboard for launching attacks, e.g., as a bot.	Low	Low	Low	Network	Low	High	None	Change	None	None	None	None	None	2.3	Low
Path of Communication between the Home Gateway and the Internet	EP⑥	Information Disclosure	Theft of information on an Internet path by a man-in-the-middle attack.	High	High	Low	Adjacent	High	High	None	Unchanged	Low	None	None	None	None	2.7	Low

Threat Example				Environmental Metrics														
Entry point	EP Number	Threat Category	Threat Example	Requirement for Confidentiality	Requirement for Integrity	Requirement for Availability	Modified Attack Vector	Modified Attack Complexity	Modified Privileges Required	Modified User Interaction	Modified Scope	Modified Confidentiality Impact	Modified Integrity Impact	Modified Availability Impact	Modified Life and Property Impact	Modified Information Importance	Risk Score	Risk Score Rank
Smarthome–compatible Devices	EP⑦	Unauthorized Access	Unauthorized access to a device (attacks exploiting known vulnerabilities).	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.8	Medium
		Information Disclosure	Theft of information from data or settings stored in a device (access control or inadequate authentication).	High	High	Low	Network	High	High	None	Unchanged	Low	None	None	None	None	2.9	Low
		Tampering	Tampering of data or settings stored in a device.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.8	Medium
		Spoofing	Attack by tampered message by disguising oneself as the home gateway during communication.	Low	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.1	Medium
		Information Disclosure	Information Disclosure via a connected storage device (any compatible device, such as a USB interface).	High	Low	Low	Physical	Low	High	Required	Unchanged	Low	None	None	None	None	2.4	Low
		Malware Infection	Malware infection via a connected storage device (any compatible device, such as a USB interface).	High	High	High	Physical	Low	High	Required	Unchanged	Low	Low	Low	None	None	4.8	Medium
		Springboard	Abused as a springboard for launching attacks, e.g., as a bot.	Low	Low	Low	Network	Low	High	None	Change	None	None	None	None	None	2.3	Low
Path of Communication between Smarthome–compatible Devices and the Home Gateway	EP⑧	Spoofing	Spoofing of a device control signal by a man–in–the–middle attack.	High	High	High	Physical	High	High	None	Change	Low	Low	Low	None	None	5.8	Medium
		Information Disclosure	Theft of information on an Internet path by a man–in–the–middle attack.	High	High	Low	Adjacent	High	High	None	Unchanged	Low	None	None	None	None	2.7	Low

Threat Example				Environmental Metrics														
Entry point	EP Number	Threat Category	Threat Example	Requirement for Confidentiality	Requirement for Integrity	Requirement for Availability	Modified Attack Vector	Modified Attack Complexity	Modified Privileges Required	Modified User Interaction	Modified Scope	Modified Confidentiality Impact	Modified Integrity Impact	Modified Availability Impact	Modified Life and Property Impact	Modified Information Importance	Risk Score	Risk Score Rank
Smartphone Application	EP⑨	Information Disclosure	Information Disclosure stored in a device due to a vulnerability in a smartphone application.	High	High	High	Local	High	None	None	Change	Low	None	None	None	High	4.5	Medium
		Information Disclosure	Information Disclosure due to an unauthorized login to a smartphone application.	High	High	High	Network	Low	High	None	Unchanged	None	None	Low	None	High	3.8	Low
		Spoofing	Any unauthorized operation of a device caused by illegally logging in to a smartphone application.	High	High	High	Network	Low	High	None	Change	None	None	Low	None	None	5	Medium
Path of communication between a smartphone and the home gateway	EP⑩	Spoofing	Spoofing of a device control signal by launching a man-in-the-middle attack.	High	High	High	Physical	High	High	None	Change	Low	Low	Low	None	None	5.8	Medium
		Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack.	High	High	Low	Adjacent	High	High	None	Unchanged	Low	None	None	None	High	3.1	Low

Table 3-41 On-Call Security Service (★★★) Risk Metrics (after Security Action)

Threat Example				Environmental Metrics														
Entry point	EP Number	Threat Category	Threat Example	Requirement for Confidentiality	Requirement for Integrity	Requirement for Availability	Modified Attack Vector	Modified Attack Complexity	Modified Privileges Required	Modified User Interaction	Modified Scope	Modified Confidentiality Impact	Modified Integrity Impact	Modified Availability Impact	Modified Life and Property Impact	Modified Information Importance	Risk Score	Risk Score Rank
Smarthome service information Platform	EP①	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Information Disclosure	Theft of information from data stored in the Service Information Platform (access control or authentication overridden).	High	High	Low	Network	High	High	None	Unchanged	Low	Low	None	None	High	5	Medium
		Tampering	Tampering of data or settings in the Service Information Platform.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Spoofing	The Service Provider Information Platform or the home gateway is attacked by spoofing or tampered messaging during communication via an API.	Low	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	6.9	Medium
		Malware Infection	Malware infection of the Service Information Platform (attacks launched via an external network).	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Denial of Service	DDoS (DoS) attack.	Low	Low	High	Network	Low	None	None	Unchanged	None	None	Low	None	None	6.1	Medium
		Information Disclosure	Information Disclosure via a carried-in storage device.	High	Low	Low	Physical	Low	High	Required	Unchanged	Low	None	None	None	High	2.8	Low
		Malware Infection	Malware infection via a carried-in storage device.	High	High	High	Physical	Low	High	Required	Unchanged	Low	Low	Low	None	High	5.6	Medium
		Information Disclosure	Theft of update software.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Tampering	Tampering of update software.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
Path of communication between the Smarthome Service Information Platform and the Internet	EP②	Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack.	High	High	Low	Adjacent	High	High	None	Unchanged	Low	None	None	None	High	3.1	Low

Threat Example				Environmental Metrics														
Entry point	EP Number	Threat Category	Threat Example	Requirement for Confidentiality	Requirement for Integrity	Requirement for Availability	Modified Attack Vector	Modified Attack Complexity	Modified Privileges Required	Modified User Interaction	Modified Scope	Modified Confidentiality Impact	Modified Integrity Impact	Modified Availability Impact	Modified Life and Property Impact	Modified Information Importance	Risk Score	Risk Score Rank
Service Provider Information Platform	EP③	Unauthorized Access	Unauthorized access to the Service Information Platform (attacks exploiting known vulnerabilities)	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Information Disclosure	Theft of information from data stored in the Service Information Platform (access control or authentication overridden).	High	High	Low	Network	High	High	None	Unchanged	Low	Low	None	None	High	5	Medium
		Tampering	Tampering of data or settings in the Service Information Platform.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Spoofing	Smarthome Service Information Plathome is attacked by spoofing or tampered messaging during communication via an API.	Low	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	6.9	Medium
		Malware Infection	Malware infection of the Service Information Platform (attacks launched via an external network).	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Denial of Service	DDoS (DoS) attack.	Low	Low	High	Network	Low	None	None	Unchanged	None	None	Low	None	High	6.1	Medium
		Information Disclosure	Information Disclosure via a carried-in storage device.	High	Low	Low	Physical	Low	High	Required	Unchanged	Low	None	None	None	High	2.8	Low
		Malware Infection	Malware infection via a carried-in storage device.	High	High	High	Physical	Low	High	Required	Unchanged	Low	Low	Low	None	High	5.6	Medium
		Information Disclosure	Theft of update software.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Tampering	Tampering of update software.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
Path of communication between the Service Provider Information Platform and the Internet	EP④	Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack.	High	High	Low	Adjacent	High	High	None	Unchanged	Low	None	None	None	High	3.1	Low

Threat Example				Environmental Metrics														
Entry point	EP Number	Threat Category	Threat Example	Requirement for Confidentiality	Requirement for Integrity	Requirement for Availability	Modified Attack Vector	Modified Attack Complexity	Modified Privileges Required	Modified User Interaction	Modified Scope	Modified Confidentiality Impact	Modified Integrity Impact	Modified Availability Impact	Modified Life and Property Impact	Modified Information Importance	Risk Score	Risk Score Rank
Home gateway	EP⑤	Unauthorized Acces	Unauthorized access to the home gateway (attacks exploiting known vulnerabilities).	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Information Disclosure	Theft of information from data or settings stored in the home gateway (access control or authentication overridden).)	High	High	Low	Network	High	High	None	Unchanged	Low	Low	None	None	High	5	Medium
		Tampering	Tampering of data or settings stored in the home gateway.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Spoofing	The Service Information Platform is attacked by spoofing or tampered messaging during communication via an API.	Low	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	6.9	Medium
		Malware Infection	Malware infection of the home gateway (attacks launched via an external Internet)	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Denial of Service	DDoS (DoS) attack.	Low	Low	High	Network	Low	None	None	Unchanged	None	None	Low	None	High	6.1	Medium
		Information Disclosure	Information Disclosure via a connected storage device.	High	Low	Low	Physical	Low	High	Required	Unchanged	Low	None	None	None	High	2.8	Low
		Malware Infection	Malware infection via a connected storage device.	High	High	High	Physical	Low	High	Required	Unchanged	Low	Low	Low	None	High	5.6	Medium
		Malware Infection	Malware Infection from LAN-attached devices	High	High	High	Adjacent	Low	None	None	Unchanged	Low	Low	Low	None	High	8.3	High
		Springboard	Abused as a springboard for launching attacks, e.g., as a bot.	Low	Low	Low	Network	Low	High	None	Change	None	None	None	None	High	2.3	Low
Path of communication between the home gateway and the Internet	EP⑥	Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack.	High	High	Low	Adjacent	High	High	None	Unchanged	Low	None	None	None	High	3.1	Low

Threat Example				Environmental Metrics														
Entry point	EP Number	Threat Category	Threat Example	Requirement for Confidentiality	Requirement for Integrity	Requirement for Availability	Modified Attack Vector	Modified Attack Complexity	Modified Privileges Required	Modified User Interaction	Modified Scope	Modified Confidentiality Impact	Modified Integrity Impact	Modified Availability Impact	Modified Life and Property Impact	Modified Information Importance	Risk Score	Risk Score Rank
Smarthome-compatible devices	EP⑦	Unauthorized Acces	Unauthorized access to a device (attacks exploiting known vulnerabilities).	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	High	7.7	High
		Information Disclosure	Theft of information from data or settings stored in a device (access control or authentication overridden).	High	High	Low	Network	High	High	None	Unchanged	Low	None	None	None	High	3.3	Low
		Tampering	Tampering of data or settings stored in a device.	High	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.8	Medium
		Spoofing	The home gateway is attacked by spoofing or tampered messaging during communication.	Low	High	High	Network	High	None	None	Unchanged	Low	Low	Low	None	None	6.1	Medium
		Information Disclosure	Information Disclosure via a connected storage device (any compatible device, such as a USB interface).	High	Low	Low	Physical	Low	High	Required	Unchanged	Low	None	None	None	High	2.8	Low
		Malware Infection	Malware infection via a connected storage device (any compatible device, such as a USB interface).	High	High	High	Physical	Low	High	Required	Unchanged	Low	Low	Low	Yes	High	8.3	High
		Springboard	Abused as a springboard for launching attacks, e.g., as a bot.	Low	Low	Low	Network	Low	High	None	Change	None	None	None	None	None	2.3	Low
Path of communication between smarthome-compatible devices and the home gateway	EP⑧	Spoofing	Spoofing of a device control signal by launching a man-in-the-middle attack.	High	High	High	Physical	High	High	None	Change	Low	Low	Low	Yes	None	8.5	High
		Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack.	High	High	Low	Adjacent	High	High	None	Unchanged	Low	None	None	None	High	3.1	Low

Threat Example				Environmental Metrics														
Entry point	EP Number	Threat Category	Threat Example	Requirement for Confidentiality	Requirement for Integrity	Requirement for Availability	Modified Attack Vector	Modified Attack Complexity	Modified Privileges Required	Modified User Interaction	Modified Scope	Modified Confidentiality Impact	Modified Integrity Impact	Modified Availability Impact	Modified Life and Property Impact	Modified Information Importance	Risk Score	Risk Score Rank
Smartphone Application	EP⑨	Information Disclosure	Information Disclosure stored in a device due to a vulnerability in a smartphone application.	High	High	High	Local	High	None	None	Change	Low	None	None	None	High	4.5	Medium
		Information Disclosure	Information Disclosure due to an unauthorized login to a smartphone application.	High	High	High	Network	Low	High	None	Unchanged	None	None	Low	None	High	3.8	Low
		Spoofing	Any unauthorized operation of a device caused by illegally logging in to a smartphone application.	High	High	High	Network	Low	High	None	Change	None	None	Low	None	None	5	Medium
Path of communication between a smartphone and the home gateway	EP⑩	Spoofing	Spoofing of a device control signal by launching a man-in-the-middle attack.	High	High	High	Physical	High	High	None	Change	Low	Low	Low	None	None	5.8	Medium
		Information Disclosure	Theft of information on an Internet path by launching a man-in-the-middle attack.	High	High	Low	Adjacent	High	High	None	Unchanged	Low	None	None	None	High	3.1	Low

4 Potential Security Threats and Action Guidelines

This chapter identifies characteristic issues that affect smarthome security to help pursue security action guidelines.

4.1 Diversity of Relevant Factors

As can be seen from the system model depicted in Chapter 2, the components of a smarthome are many and diverse, obscuring the transparency of the discussions of security threats and actions.
This issue can be approached by considering that the component elements of a smarthome can be divided into two broad categories from a user value perspective: individual IoT devices and services leveraging these devices. In this Guidelines, security threats to and actions taken for the services provided by a smarthome are explored and assessed on the system model. Likewise, threats and actions are explored and assessed for individual IoT devices by creating relevant guidelines.

4.2 Responding to Product Safety

The structural requirements for remote operations of electrical appliances, including IoT devices, as prescribed in 1 (2) b [7], Technical Standard Appended Table 8, Electrical Appliances and Materials Safety Act dictate "top priority being placed on hand operations" and "abilities to verify action results from feedbacks to ensure successful remote operations." In March 2018, a proposal for an international standard that prescribes the functional safety of multiple devices and systems that run concurrently in a smarthome pursuant to the principles of IEC61508 (electrical/electronic/programmable electronic safety-related systems), a basic standard relating to functional safety, was submitted to the International Electrotechnical Commission (IEC) by the National Institute of Advanced Industrial Science and Technology (AIST), a national research and development agency, and by the Misawa Homes Institute of Research and Development Co., Ltd. and approved [8]. With IoT devices governed by the Product Liability Act and the Consumer Product Safety Act, it is necessary to check to see if their remote operations comply with the requirements of these laws and regulations.

Fail-safe software or other product safety assurance measures must be in place to minimize the possible impact of interruptions in the availability of services caused under the influence of some failures in the Smarthome Service Information Platform or associated cloud.

4.3 Device Collaboration

While smarthomes are populated with numerous IoT devices, these devices may not only work independently but may collaborate with one another. Collaboration among different kinds of devices, however, could give rise to these issues:

(1)Because the appropriateness of the nature and levels of security actions enforced in the connected devices are unknown, whether appropriate security actions are taken as a whole or not cannot be determined.

(2)Where multiple devices varying in their security level collaborate, the one having the lowest level of safety in terms of systems and security implemented among them could make a breakthrough for an attacker, so the security actions to be taken should allow for all component devices connected.

(3)As discussed in the use cases in this document, in the case of providing smarthome services, where multiple enterprises participate as multivendors in the work of systems and equipment development and collaboration with a third-party service, the lines of demarcation for security responsibility among them could be made obscure. This could, in turn, make it difficult for one enterprise as a service provider to present a security standard to other enterprises.

To approach these issues, it would be necessary to implement risk analyses and assessment, at the stage of planning a new service, on the system models that make up the service. Based on risk analysis findings, secondary requirements for a Service Information Platform, a home gateway and housing equipment may be presented as individualized security standards to help encourage better security across the component systems. Then, the lines of demarcation for responsibility between the participating enterprises would also be specified expressly.

4.4 Installation and Removal of IoT Devices by Users

Products compliant with procurement standards set by housing companies (for example, JIS, F☆☆☆☆ for interior building products and CP marks for security building components) are used as building products and housing equipment installed in homes. With smarthomes that are furnished with products having security actions implemented, it would be necessary to verify that these products comply with the relevant standards.

Yet, it may happen that the owner of a home sets up devices of the owner's choice in the home after its delivery from the housing company. The nature and levels of security actions implemented in these owner-installed devices are likely unknown. The security level of a smarthome might be downgraded through the installation of these devices in it. It is imperative, therefore, to consider endorsing the security of a smarthome as a whole, including the devices installed by the homeowner themselves.

This issue can also be approached with the Certification Mark Plan consistent with the CCDS Certification Program. Users may check the Certification Mark label appearing on an IoT device and then purchase and install that device at their choice. Because these devices fulfill the security requirements defined by the CCDS Certification Program, the security standard of the smarthomes furnished by these devices is maintained.

4.5 Keeping Security Action Guidelines for Smarthome Servi ces Organized

Both a Smarthome Service Information Platform and a Service Provider Information Platform relate to the delivery of smarthome services. Security actions applicable to the cloud system for the Service Information Platform should be reviewed from perspectives of both the system itself and the operational background (people, operating environments and operating procedures, etc.). Smarthome Service Information Platforms could handle information that may impact Life and Property or even control actual devices, and sometimes might entrust controls to third parties while the users are absent. Hence, smarthome services should allow for threats, such as Spoofing, Disclosure of Information and Unauthorized Access. Factors for consideration include:

・Enough security actions must be enforced in the Service Information Platform as a system on the cloud.

・Physical security actions must be enforced for service operating facilities, plus people, operating environments and operating procedures.

・Systems and devices that make up a smarthome service must meet Common Requirements ★ in the IoT Field Common Security Requirements Guidelines; the systems and devices that make up ★★ and ★★★ services must meet the security standards (Chapter 6) respectively.

・The authentication of the home gateway by Service Provider Information Platforms (including both the Smarthome Service Information Platform and the Service Provider Information Platform) and that of smarthome-compatible devices by the home gateway must be carried out.

・Secure means of communication or protocols must be used in the paths of communication between each Service Provider Information Platform and the home gateway and between the Service Provider Information Platforms.

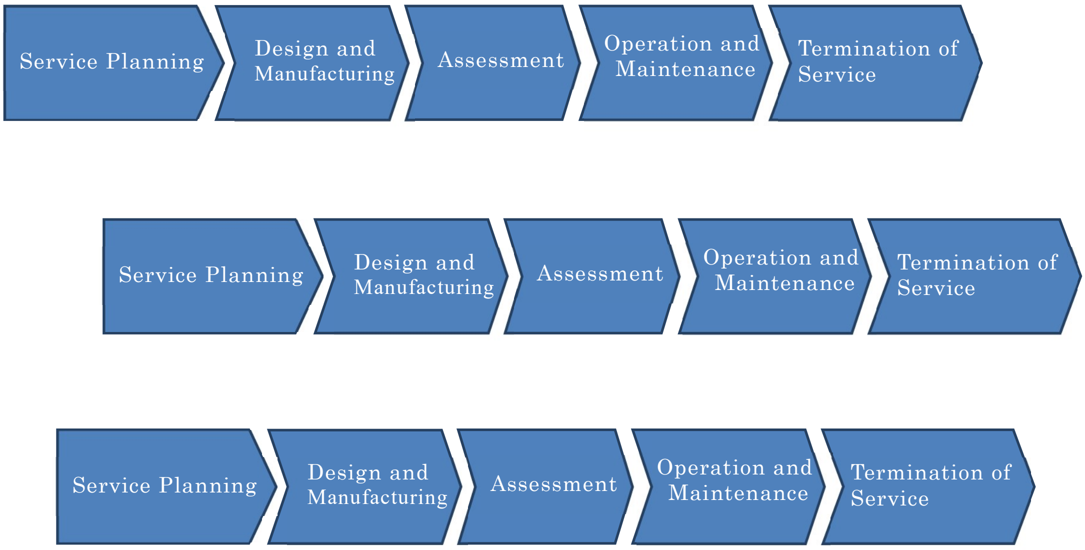
・Device operation logs must be recorded to track down the sources of any illegal device operations attempted and their details.

5 Life Cycle of a Smarthome Service and Security Efforts

The implementation of security actions for smarthomes should also take into consideration the fact that not only the IoT devices installed in the premises could change with their life cycles (purchase, failure, resale, scrapping) but their users themselves might change as well.

5.1 Definitions of the Successive Phases of the Life Cycle of a Smarthome Service

This section defines the security actions to be taken through the life cycle of smarthome development work by service providers. The life cycle of Smarthome Services development work can be broadly divided into five successive phases: Service Planning, Design and Manufacturing, Assessment, Operation and Maintenance, and Termination of Services. To maintain adequate security in providing Smarthome Services, enough actions need to be taken in the successive phase of the life cycle of the services from a broad spectrum of considerations,including the formulation of corporate policies and plans,compliance with the relevant laws and regulations,and people,operating enviroments and procedures.



Figure

5-1: Phases of the Life Cycle of a Smarthome Service

Table 5-1: Definitions of the Phases of a Smarthome Service

Phase	Description
Service Planning	Carry out risk analyses and assessment, etc. based on service concepts, requirements definitions, use case definitions and assumed system models.
Design and Manufacturing	Design, implement and manufacture the systems and devices that make up a service (or outsource these tasks) based on decisions made in the Service Planning phase.
Assessment	Have the construction representative verify installation status and manage and supervise equipment used to preclude failures and incidents while providing the service.
Operation and Maintenance	Run and maintain the service being offered to the user, and take responses to incidents as they occur in the meantime.
Termination of Service	When the service terminates, notify the user beforehand, complete procedures for migrating to an alternate service, destroy personal information collected and so on.

5.2 Security Efforts to be Made in the Life Cycle of a Servi ce

This section reviews the security efforts to be made in the successive phases of the life cycle as outlined in the foregoing section.

5.2.1 Service Planning Phase

This section summarizes security efforts to be made in the Service Planning phase.

Table 5-2: Security Efforts to be Made in the Service Planning Phase

No.	Item	Description
1	Formulation of response policies to be pursued by a corporate organization	・Formulate a system of risk management activity to cope with cyber security, along with rules, in the corporate organization.
2	Formulation of personal information management policies to be pursued by a corporate organization	・Define personal information to be collected and formulate relevant management policies from a viewpoint of personal information protection.
3	Definition of service requirements, and system models and use cases	Define system models and use cases based on the service requirements. With a system model, clarify the lines of demarcation for responsibility between the service provider and its partnering enterprises such as contractors.
4	Risk analyses and assessment, and definition of service levels	・Conduct risk analyses and assessment to assess assets to be protected, potential threat, and risk metrics. ・Review in the course of risk analyses and assessment whether sensitive data,such as personal information,is handled and whether there is any Life and Property impact, and define a Certification Level (★★, ★★★) for the services accordingly.
5	Review of responses to relevant laws and regulations	Extract items that require responses to the laws and regulations relevant to the Smarthome Services and explore possible actions on the part of the devices and systems.
6	Formulation of security action policies	・Formulate the policies of security actions required to reflect the risk analysis and assessment results. Further, launch discussions to allow for availability, etc. from a viewpoint of safety hazards.
7	Definition of a disclaimer for services	・Define a disclaimer to provide against possible failures impacting the services (such as the loss of power caused by accidents, including natural disasters or fires).

5.2.2 Design and Manufacturing Phase

Security efforts to be made in the Production and Construction phase are summarized below.

Table 5-3: Security Efforts to be Made in the Design and Manufacturing Phase

No.	Item	Description
1	Verification of the development vendor's organization	・If the work of device or systems development is outsourced, make certain that the vendor's development organization enforces quality control by adhering to the "Security by Design" concept. Example: ・Static assessment:Secure design, coding review ・Dynamic assessment:Security testing, etc.
2	Outsourcing of development work and solutions	・If a need arises to develop new devices or to implement solutions in the course of providing a service, it will be mandatory to specify security secondary requirements according to the level of authentication of that service to the development or solutions vendors and dictate their compliance with such requirements. ・For a description of specific security actions to take, see: Section 6.2 Security Secondary Requirements for System Service-Compatible Devices

5.2.3 Scoring Phase

Security efforts to be made in the Scoring phase are summarized below.

Table 5-4: Security Efforts to be Made in the Scoring Phase

No.	Item	Description
1	Authentication information and security setting checks during construction	・Preparatory to constructing a smarthome, make certain that the authentication information and security settings have been integrated properly.
2	Vulnerability check	・Check each Service Information Platform and each of the home gateway and smarthome-compatible devices for known vulnerabilities.
3	Responses while producing and constructing a smarthome	※For additional information about the actions to take in the Scoring phase, see the description of the Production and Construction phase in the following life cycle of a smarthome: 5.4.2Production and Construction Phase No.2Ordering devices used, etc. No.3Managing and supervising devices used, etc. No.4Confirming construction

5.2.4 Operation and Maintenance Phase

Security efforts to be made in the Operation and Maintenance phase are summarized below.

Table 5-5 Security Efforts to be Made in the Operation and Maintenance Phase

No.	Item	Description
1	Personal authentication of the service subscriber	・Service-providing systems (Service Information Platforms, smarthome environment) must support an authentication function to allow only the subscriber to a service contract (or any individual authorized by that subscriber) to use the service under contract.
2	Logging and data	・Service-providing systems must support a logging function to provide against potential incidents occurring, such as

	analysis	Unauthorized Access, and must also be ready to analyze log data collected.
3	Implementation of a data deletion function	・A function for deleting data on the system on which the service runs must be implemented from a standpoint of personal information protection.
4	Authentication of the field representative	As for ★★★ services, a scheme or function must be implemented to validate the qualifications of the field representatives rushing to the smarthomes in times of fault notification.
5	Ruggedization of operations of a Smarthome Service Information Platform (1) (Data access)	・For a Smarthome Service Information Platform, the following actions must be enforced to ruggedize its operations: 1)Definition of data access procedures and rules 2)Minimization of the scope of data access 3)Data access log auditing 4)Security education for operations representatives ※In every case, certification must have been acquired under the following standard or an operation scheme conforming to such certification standard must be implemented: -ISO/IEC27017:ISMS Cloud Security Certification
6	Ruggedization of operations of a smarthome Service Information Platform (2) (Server login)	・For a smarthome Service Information Platform, the following actions must be enforced to ruggedize its operations: 1)Definition of login information management procedures and rules 2)Minimization of the scope of login information release 3)Security education for operations representatives ※In every case, certification must have been acquired under the following standard or an operation scheme conforming to such certification standard must be implemented: -ISO/IEC27017:ISMS Cloud Security Certification
7	Ruggedization of the workrooms for a smarthome Service Information Platform	・Enforce access control to server rooms and operation rooms, using IDs or the like, to prevent unauthorized personnel from entering them. ※Certification must have been acquired under the following

	(1) (Access control)	standard or an operation scheme conforming to such certification standard must be implemented: -ISO/IEC27017:ISMS Cloud Security Certification
8	Ruggedization of operations of a smarthome Service Information Platform (2) (Restriction on carrying-in of devices)	・Enforce critical control over those accessing server rooms and operation rooms by restricting the carrying-in of storage devices, smartphones, PCs and the like ※Certification must have been acquired under the following standard or an operation scheme conforming to such certification standard must be implemented: -ISO/IEC27017:ISMS Cloud Security Certification
9	Ruggedization of operations of a Smarthome Service Information Platform (3) (Access history control)	・Access to and from server rooms and operation rooms must be recorded using security cameras or ID card logging. ※Certification must have been acquired under the following standard or an operation scheme conforming to such certification standard must be implemented: (Access history control) -ISO/IEC27017:ISMS Cloud Security Certification
10	Ruggedization of operations of a Service Provider Information Platform (1) (Data access)	For a Service Provider Information Platform (※),the following actions must be enforced to ruggedize its operations: 1)Definition of data access procedures and rules. 2)Minimization of the scope of data access. 3)Data access log auditing. 4)Security education for operations representatives. ※An example of a Service Provider Information Platform might be a call center system or the like. ※In every case, certification must have been acquired under the following standard or an operation scheme conforming to such certification standard must be implemented: -ISO/IEC27017:ISMS Cloud Security Certification
11	Ruggedization of operations of a Service Provider Information	・For a Service Provider Information Platform, the following actions must be enforced to ruggedize its operations: 1)Definition of login information management procedures and rules.

	Platform (2) (Server login)	2)Minimization of the scope of login information release. 3)Security education for operations representatives. ※An example of a Service Provider Information Platform might be a call center system or the like. ※In every case, certification must have been acquired under the following standard or an operation scheme conforming to such certification standard must be implemented: -ISO/IEC27017:ISMS Cloud Security Certification
12	Ruggedization of operations of a Service Provider Information Platform (3) (Remote unlocking operation)	・If a Service Provider Information Platform is to carry out device operations relevant to crime prevention and life-saving, the following actions must be enforced: 1)Definition of operational routines for device operations relevant to crime prevention and life-saving. 2)Auditing of device operation logs for device operations relevant to crime prevention and life-saving. 3)Security education for operators relevant to crime prevention and life-saving. ※An example of a Service Providers Information Platform might be a call center system or the like. ※In every case, certification must have been acquired under the following standard or an operation scheme conforming to such certification standard must implemented: -ISO/IEC27017:ISMS Cloud Security Certification
13	Ruggedization of the workrooms for a Service Provider Information Platform (1) (Access control)	・Enforce access control to server rooms and operation rooms, using IDs or the like, to prevent unauthorized personnel from entering them. ※An example of a Service Provider Information Platform might be a call center system or the like. (1) ※Certification must have been acquired under the following standard or an operation scheme conforming to such certification standard must be implemented: -ISO/IEC27017:ISMS Cloud Security Certification
14	Ruggedization of the workrooms for a Service	・Enforce exacting control over those accessing server rooms and operation rooms by restricting the carrying-in of storage

	Provider Information Platform (2) (Restriction on carrying-in of devices)	devices, smartphones, PCs and the like ※An example of a Service Provider Information Platform might be a call center system or the like. ※ Certification must have been acquired under the following standard or an operation scheme conforming to such certification standard must be implemented: -ISO/IEC27017:ISMS Cloud Security Certification
15	Ruggedization of the workrooms for a Service Provider Information Platform (3) (Access history control)	・Access to and from server rooms and operation rooms must be recorded using security cameras or ID card logging. ※An example of a Service Provider Information Platform might be a call center system or the like. ※Certification must have been acquired under the following standard or an operation scheme conforming to such certification standard must be implemented: -ISO/IEC27017:ISMS Cloud Security Certification
16	Responding to incidents occurring while providing a service	・Organize a CSIRT (Cyber Security Incident Response Team) to respond to unexpected risks occurring while providing a service and take action to prevent their recurrence. ・Take appropriate responses in reporting vulnerabilities by working in conjunction with relevant organizations, such as Japan Computer Emergency Response Team/Coordination Center (JPCERT/CC).
17	Responding to smarthome services operation and maintenance	※For additional information about the actions to take in the Operation and Maintenance Phase, see the description of the Remodeling in the following life cycle of a smarthome: 5.4.3Post-Construction Phase 5.4.4Remodeling Phase

5.2.5 Service Termination Phase

Security efforts to be made in the Service Termination phase are summarized below.

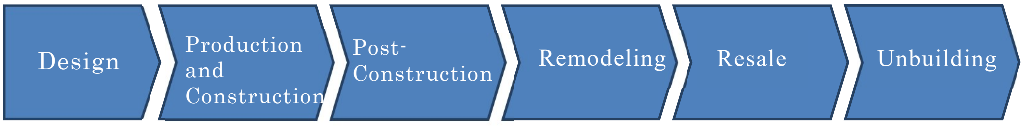
Table 5-6: Security Efforts to be Made in the Service Termination Phase

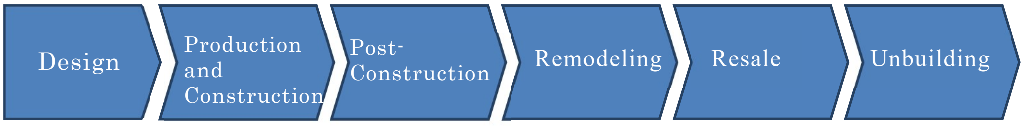
No.	Item	Description
1	End-of-service notification	・Before a service terminates, its user must be given an about one-year prior notice from a viewpoint of user protection. The user must also be given appropriate explanations, including an introduction to alternate services.
2	Destruction of personal information collected	・When a service terminates, personal information collected must be destroyed. If migration to an alternate service takes place, however, the personal information may be appropriated for the implementation of the alternate service, subject to consent from the user.
3	Publicizing of the method of device scrapping	*For information about publicizing the method of device scrapping, see the description of the Unbuilding Phase in the following flow of smarthome development: 5.4.6Unbuilding Phase No. 1Publicizing the method of device scrapping

5.3 Definitions of the Successive Phases of the Life Cycle of a Smarthome

This section defines the security actions to be taken by service providers and system operation vendors through the life cycle of a smarthome (dwelling). The life cycle of a smarthome can be broadly divided into six phases: Design, Production and Construction, Post-Construction, Remodeling, Resale and Unbuilding.

To maintain enough security in providing smarthome services, adequate actions should be taken in these successive phases to bolter the security of the products.





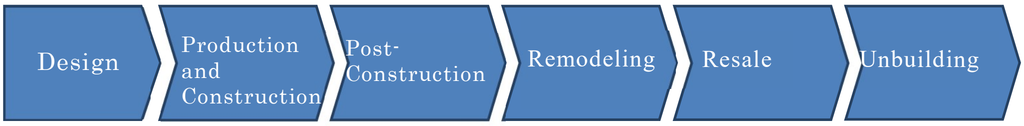


Figure 5-2: Phases of the Life Cycle of a Smarthome

Table 5-7: Definitions of the Phases of a Smarthome

Phase	Description
Phase	Designs smarthomes, including IoT housing equipment.
Production and Construction	Produces and constructs smarthomes, including IoT housing equipment.
Post-Construction	Following the completion of a smarthome, the homeowner starts living in it, utilizing information about the smarthome and running and maintaining it.
Remodeling	Remodels smarthomes.
Resale	Changes smarthome owners.
Unbuilding	Terminates the use of a smarthome and unbuilds it.

5.4 Security Efforts to be Made in the Life Cycle of a Smar thome

This section describes security efforts to be made in the successive phases of the life cycle summarized in the foregoing section.

5.4.1 Design Phase

Security efforts to be made in the Design phase are summarized below.

Table 5-8 Security Efforts to be Made in the Design Phase

No.	Item	Description
1	Service selection	・Explain the content of the service to its user and gain consent to that service from the user.
2	Selection of devices to be installed	・Select devices to meet the relevant security standards according to the certification level of the service provided. ・For a description of specific security actions to take, see the following section of this document: 6.2Security Secondary Requirements for System and Service-Compatible Devices
3	Notation and marking in the design documentation	・List all devices used in the system documentation (including system schematics) without omission.

5.4.2 Production and Construction Phase

Security efforts to be made in the Production and Construction phase are summarized below.

Table 5-9 Security Efforts to be Made in the Production and Construction Phase

No.	Item	Description
1	Acquisition of user consent	・Explain about the handling of personal information, etc. to the service users and gain their consent. ・Specify and explain about the line of demarcation for responsibility. ・Explain about disclaimers in using the services to the

		users and gain their consent.
2	Ordering of devices used, etc.	・Verify consistency with the design documentation (for home gateways, sensors, connections and more).
3	Management and supervision of devices used, etc.	・Check to see if unauthorized devices have not been installed and if the devices used are not in trouble. ・Check the models (descriptions and types) of the devices to be installed in the premises of the smarthome to verify their compliance with the Security Secondary Requirements for services.
4	Construction checks	・Check the subscriber, devices used and the conditions of options. ・Verify and supervise consistency with the design documentation and purchase specifications during and after construction. (Recording by photographs, etc. is allowed.) ・Check the devices used, etc. for successful operations after construction. ・Verify the validity of the system as a whole.
5	Issues management	・Check the quantities of keys, cards and the like issued with the quantities of those actually handed over.
6	Descriptions of devices used and how to use services	・ Descriptions of devices used and how to use services ・ Explain to the users about the devices used and how to use services.
7	Terms of use	・Include a disclaimer notice, how to respond to failures when they occur, service provider contact information and so on.

5.4.3 Post-Construction Phase

Security efforts to be made in the Post-Construction phase are summarized below.

Table 5-10: Security Efforts to be Made in the Post-Construction Phase

No.	Item	Description
1	Provision of the terms or use or instruction manuals	・Define a disclaimer in providing the services expressly in the terms of use or instruction manual for the users to see. ・Present the security action policies of the services to the users.
2	Definition of operational usages	・Specify expressly the extent beyond which users have no authority to alter the device configuration or settings in the smarthomes. Alert the users not to act beyond such extent to make unauthorized alterations. ・Familiarize the user with the objectives and functionalities of the service so they will not use the devices for purposes other than the intended use.
3	User reminder	・Include in the instruction manuals to direct users to contact the service provider when suspicious devices are connected or devices are found to behave abnormally. ・Alert users to the cases, in the instruction manuals, in which the use of defaults, or setup errors could produce vulnerabilities.
4	Responding to latest vulnerabilities	・Watch vulnerability information constantly to check for presence or absence of any vulnerabilities in the OS, boot program and applications used and, whenever associated vulnerabilities are reported, release program updates. ・Notify service users of the availability of the latest versions of programs, alert them to the impact of vulnerabilities and familiarize them with the program update procedures.
5	Issues management	・Check the quantities of keys, cards and the like issued with those handed over. ・Update information about issues in times of their loss.

6	Restriction on device usage	・Algorithms and key lengths currently considered adequate could become inadequate in the future. Consider advising users to terminate their use of devices at a given point of time. ・For gateways that are possibly used over a long period of time, have their maintenance period defined with the service provider and publicize it in manuals or at a website for the users to see.

5.4.4 Remodeling Phase

Security efforts to be made in the Remodeling phase are summarized below.

For the Design Phase and the Production and Construction Phase of remodeling work, see Table 5-8 and Table 5-9.

Table 5-11: Security Efforts to be Made in the Remodeling Phase

No.	Item	Description
1	Verification of compatibility with devices already in position	・Before attempting to add to or exchange devices or add or update relevant information, verify that there will be no impact upon devices already in position.
2	Publicizing the method of device scrapping	*The following are the actions to be taken when the devices installed in the premises of a smarthome are scrapped as the user (homeowner) changes: ・Specify the potential threats and risks associated with the disposal of devices with data left inside in instruction manuals or the like to alert the users. ・Recommend to users in the instruction manuals or the like to initialize device settings and data stored in memory when scrapping devices. ・If scrapping of devices by destruction is to be recommended to users, specify, in the instruction manuals or the like, that their disposal must comply with the relevant local regulations. ・In disposing of security devices (such as electronic locks and door locks), service providers must direct the disposal contractors to initialize the data stored on these devices.

5.4.5 Resale Phase

This section summarizes security efforts to be made in the Resale Phase.

Table 5-12: Security Efforts to be Made in the Resale Phase.

No.	Item	Description
1	Issues management	・Check the quantities of keys, cards and the like issued with the quantities of those actually handed over.
2	Publicizing the method of device scrapping	※The following are the actions to be taken when the devices installed in the premises of a smarthome are scrapped as the user (homeowner) changes: ・Specify the potential threats and risks associated with the disposal of devices with data left inside in instruction manuals or the like to alert the users. ・Recommend to users in the instruction manuals or the like to initialize device settings and data stored in memory when scrapping devices. ・If scrapping of devices by destruction is to be recommended to users, specify, in the instruction manuals or the like, that their disposal must comply with the relevant local regulations. ・In disposing of security devices (such as electronic locks and door locks), service providers must direct the disposal contractors to initialize the data stored on these devices.
3	Management after resale	・ Disseminate disclaimers and security precautions to the next user. ・ For security precautions, refer to the following items in Table 4-4 After Phase. -Provision of instruction manuals -User reminder -Responding to latest vulnerabilities -Restriction on device usage

5.4.6 Unbuilding Phase

Security Efforts to be Made in the Unbuilding Phase are summarized below.

Table 5-13: Security Efforts to be Made in the Unbuilding Phase

No.	Item	Description
1	Publicizing the method of device scrapping	・Specify the potential threats and risks associated with the disposal of devices with data left inside in instruction manuals or the like to alert the users. ・Recommend to users in the instruction manuals or the like to initialize device settings and data stored in memory when scrapping devices. ・If scrapping of devices by destruction is to be recommended to users, specify, in the instruction manuals or the like, that their disposal must comply with the relevant local regulations.

6 Security Requirements for Smarthome Services

This chapter defines security requirements for the services relevant to the certification programs in the smarthome field and security secondary requirements for the components of the services, to reflect the risk analysis and assessment results and security action efforts discussed so far.

6.1 Security Requirements for Smarthome Services

This section defines security requirements for those services that need be addressed by a Certification Program.

Requirements for ★★ and ★★★ services have been selected, respectively, from the following standpoints:

1)Requirements for ★★ services
・Requirements essential for delivering all smarthome services in a safe, secure and consistent manner.
*Actions that are cost-effective against highly serious threats have been mainly selected to reflect the risk metrics calculations.
2)Requirements for ★★★ services
・Requirements sought by services requiring more exacting action to protect lives, properties and personal information.
*Implementable items have been selected, with their cost and cost effectiveness taken into consideration, by checking against the Cyber Physical Security Framework (CPSF) [20], based on the risk metrics calculations.
The security requirements discussed in this section and in Section 6.2 comply with the U.K. Code of Practice for Consumer IoT Security [21] and U.S. California State's Information privacy: connected devices (Senate Bill No.327, Chapter 886) [1] as well.

Table 6-1 Rules of Notation of Security Requirements and Secondary Requirements

Symbol	Status of Response
◎	Not discussed in the associated guidelines but defined in this Guidelines.
○	Detailed in further depth in this Guidelines than in the associated guidelines.
＝	Requirements and secondary requirements essentially correspond to the associated guidelines.

Security requirements and secondary requirements in this document are numbered in accordance with the following rules:

[Requirement/Secondary requirement] [Level]-[Type]-[No.]

Table 6-2 Numbering Rules for Security Requirements and Secondary Requirements

Category	Japanese Name	English Notation	Numbering Rule
Requirement/secondary requirement	要件	Requirements	R
	要求事項	Secondary Requirements	SR
Level	レベル 2	Level2	2
	レベル 3	Level3	3
Type	スマートホームサービス情報基盤	Smarthome Service Information Platform	SP
	第三者サービス情報基盤	Service Provider Information Platform	PP
	ホームゲートウェイ	Home Gateway	H
	スマートホーム 対応機器群	Smart home compatible devices	D
	スマートフォンアプリ	Smartphone application	A

Table 6-3 Security Requirements for Smarthome Services

No.	Level	Scope	Item	Description	UK	SB327	CPSF
R2-1	★★	Service	Risk analyses and assessment, formulation of security action policies	・Conduct risk analyses and assessment on the services to assess the assets to be protected, potential threats and risk metrics. ・Review whether sensitive data, such as personal information, is handled in the course of risk analyses and assessment or not and whether there is any Life and Property impact or not, and define a Certification Level (★★) for the services accordingly. ・Formulate required security action policies to reflect risk analysis and assessment results.	◎	◎	○ CPS.DS-1 CPS.AE-1 CPS.AE-3 CPS.AE-4 CPS.AE-5 CPS.DP-1
R2-2	★★	Service	Use of devices and systems compliant with Security Secondary Requirements	・Service-providing systems (Service Information Platforms, devices installed in the premises of a smarthome and smartphone applications) must be comprised of devices and systems that meet requirements for ★★ services. ・In building a smarthome, check the models (descriptions and types) of the devices to be installed in the premises of the smarthome to	◎	◎	= CPS.SC-3 CPS.SC-4 CPS.SC-5 CPS.PT-3 CPS.DP-1 CPS.RP-2

				verify their compliance with the Security Requirements for ★★services.			
R2-3	★★	Service	Appropriate initial settings for the IoT device (Authentication information and access control for between IoT devices)	・Make certain, at the start of service usage, that authentication information and access control between IoT devices has been initialized properly.	＝ UK6	◎	＝ CPS.IP-1
R2-4	★★	Service	Personal authentication of the service subscriber	When a Smarthome Service is used, the subscriber to the service contract must be authenticated. User authentication information must be updated when the smarthome is resold.	＝ UK12	◎	＝ CPS.AC-6 CPS.AC-9
R2-5	★★	Service	Deletion of personal information used in the premises of a smarthome	・Users of any devices used in the premises of a smarthome must be able to delete personal information loaded into these devices by themselves to allow for their resale or disposal.	＝ UK8	◎	◎
R2-6	★★	Service	Guidance on the secure use of a smarthome	・Specify expressly the extent beyond which users have no authority to alter the device configuration or settings in the smarthomes. Alert the users not to act beyond such extent to make unauthorized alterations. ・Familiarize the user with the objectives and	＝ UK12	◎	◎

				functionalities of the service so they will not use the devices for purposes other than the intended use.			
R2-7	★★	Service	Periodic updating to the latest software	・Software installed in service-providing systems (Service Information Platforms, devices installed in the premises of a smarthome) must be updated periodically. ・If vulnerabilities are reported in the above, release software updates promptly.	＝ UK3	◎	○ CPS.DS-7 CPS.MA-1
R2-8	★★	Service	Update software operating procedures and version management	・Define operating procedures installing updates to the individual Service Information Platforms and the software installed in the devices in the smarthome and keep the software under version management. 1)Management and operating procedures for releasing software updates. 2)Management of the histories of software updates and the associated versions.	＝ UK3 UK7	◎	○ CPS.DS-7 CPS.MA-1
R2-9	★★	Service	Initializing and updating component~~s~~ devices of a smarthome when reselling it	・When reselling a smarthome, take the following actions on its component~~s~~ devices before transferring it to the new owner:	＝ UK3 UK8	◎	○ CPS.DS-7 CPS.MA-1

				1)Initialize information that has been configured, collected and stored. 2)When the construction work is completed, update to the latest software for the service before the new owner starts using it.			
R3-1	★★★	Service	Responding to ★★ service requirements	・Security Requirements for★★ services must be met.	※See ★★.		
R3-2	★★★	Service	Risk analyses and assessment, formulation of security action policies	・Conduct risk analyses and assessment on the services to assess the assets to be protected, possible threats and risk metrics. ・Review whether sensitive data, such as personal information, is handled in the course of risk analyses and assessment or not and whether there is any Life and Property impact or not, and define a Certification Level (★★★) for the services accordingly. ・Formulate the policies of security actions required based on the results of risk analyses and assessment.	◎	◎	○ CPS.DS-1 CPS.AE-1 CPS.AE-3 CPS.AE-4 CPS.AE-5 CPS.DP-1

R3-3	★★★	Service	Use of devices and systems compliant with Security Secondary Requirements	・Service-providing systems (Service Information Platforms and devices installed in the premises of a smarthome) must be comprised of devices and systems that meet the Secondary Requirements for ★★★ services. ・In building a smarthome, make certain that the devices to be installed in the premises meet the Secondary Requirements for ★★★ services (descriptions, types).	◎	◎	＝ CPS.SC-3 CPS.SC-4 CPS.SC-5 CPS.PT-3 CPS.DP-1 CPS.RP-2
R3-4	★★★	Service	Information security management in a cloud service operation	・A scheme of information security management activity must be implemented in a service provider's cloud service operation ・In case of collaborating with a third-party service, make certain that the service provider maintains a reliable scheme of security management. ・Certification must have been acquired under the following standard or an operation scheme conforming to such certification standard be implemented: *ISO/IEC27017:ISMS Cloud Security Certification	◎	◎	○ CPS.AT-1 CPS.AC-2 CPS.IP-9

R3-5	★★★	Service	Logging and data analysis	・Service-proving systems must support a logging function to provide against incidents and also a scheme of operation that allows collected log data to be analyzed.	＝ UK10	◎	＝ CPS.MA-2 CPS.PT-1 CPS.CM-2 CPS.CM-5 CPS.AN-2
R3-6	★★★	Service	Vulnerability check	・Check each Service Information Platform, the home gateway each smarthome-compatible device for known vulnerabilities. The method and timing of such check should be set individually to suit the services provided.	◎	◎	○ CPS.CM-7
R3-7	★★★	Service	Authentication of each servicer	As for each servicer accesses the smart home system, perform appropriate access management.	◎	◎	＝ CPS.AC-2 CPS.AC-3 CPS.AC-5 CPS.AC-9

R3-8	★★★	Service	Responding to incidents occurring while providing a service	Organize a CSIRT (Cyber Security Incident Response Team) to respond to unexpected risks occurring while providing a service, and then respond to incident and take action to prevent their recurrence. ・Work in conjunction with relevant organizations, such as Japan Computer Emergency Response Team/Coordination Center (JPCERT/CC), take appropriate responses in reporting vulnerabilities.	＝ UK2	◎	＝ CPS.IP-7 CPS.IP-10 CPS.AE-2 CPS.RP-4 CPS.CO-1 CPS.AN-2 CPS.AN-3 CPS.MI-1 CPS.IM-1 CPS.IM-2

6.2 Security Secondary Requirements for System Service-Compatible Devices

This section defines security secondary requirements for individual Smarthome Service Information Platforms, home gateways, smarthome-compatible devices and smartphone application devices and systems vendors. While security secondary requirements are defined separately for each device or system to help draw a line of demarcation for responsibility, they are not necessarily mandatory. Their aim is to attain a certain level of security quality across all services by responding to a given need with an alternative component based on threat analyses when the fulfillment of such need is beyond ready reach of an individual device or system.

Security Secondary Requirements for ★★ and ★★★ services have been selected from the following standpoints:

1)Secondary Requirements for ★★ services

・Secondary requirements that are essential to deliver all smarthome services in a safe, secure and consistent way.

*Actions are cost-effective against highly serious threats have been mainly selected based on risk metrics calculations.

2)Secondary Requirements for ★★★ services

・Secondary requirements to be met by services that require more exacting control to protect life, property and personal information.

*Implementable items have been selected, with their cost and cost effectiveness taken into consideration, by checking against the Cyber Physical Security Framework (CPSF), based on the risk metrics calculations.

6.2.1 Security Secondary Requirements for Smarthome Service Information Platforms

Security Secondary Requirements for Smarthome Services Information Platform are summarized below. (Entry points: EP (1) to EP (2))

Table 6-4 Security Secondary Requirements for Smarthome Service Information

No.	Level	Scope	Item	Description	UK	SB327	CPSF
SR2-SP-1	★★	Smarthome Service Information Platform	Responding to Common Requirements	・An equivalent of the security actions dictated by Common Requirements ★ in the IoT Field Common Security Guidelines must be enforced.	＝ UK1 UK6 UK13	＝ 1798.91.05	＝ CPS.IP-1 CPS.IP-6 CPS.PT-2
SR2-SP-2	★★	Smarthome Service Information Platform	Authentication over the API	・Implement authentication over the API, supporting a scheme of authentication to allow authentication information to be invalidated and reissued as needed. ・Take responses to combat reported vulnerabilities as part of the authentication over the API.	◎	◎	○ CPS.AC-3 CPS.AC-9
SR2-SP-3	★★	Smarthome Service Information Platform	User authentication on log-in from the administrative screen (interface	A scheme of login user (operator) authentication must be maintained. ・Actions are taken against brute force attacks. The implementation must be such as to allow values to be changed if compromising is suspected.	◎	◎	＝ CPS.AC-3 CPS.AC-5 CPS.AC-6 CPS.AC-9

			over which a service overview is displayed or functions are managed)				
SR2-SP-4	★★	Smarthome Service Information Platform	User authentication on server log-in	・A scheme of login user (operator) authentication must be maintained. ・Actions are taken against brute force attacks. The implementation must be such as to allow values to be changed if compromising is suspected.	◎	◎	＝ CPS.AC-3 CPS.AC-5 CPS.AC-6 CPS.AC-9
SR2-SP-5	★★	Smarthome Service Information Platform	Home gateway authentication	・A scheme of home gateway authentication must be maintained.	◎	◎	＝ CPS.AC-3 CPS.AC-9
SR2-SP-6	★★	Smarthome Service Information Platform	Management of information needed for authentication	・A scheme of preventing the leakage of information needed for authentication must be implemented.	◎	◎	＝ CPS.AC-3 CPS.AC-5 CPS.AC-6 CPS.AC-9

SR2-SP-7	★★	Smarthome Service Information Platform	Installation of security patches	・When security patches are released to fix any vulnerabilities found in the OS, boot program, server software, databases, applications or open-source libraries used, run testing on these patches and then install them.	＝ UK3	◎	＝ CPS.DS-7 CPS.MA-1
SR3-SP-1	★★★	Smarthome Service Information Platform	Responding to ★★ service requirements	・Security Secondary Requirements for a ★★ service platforms must be met.	※See ★★.		
SR3-SP-2	★★★	Smarthome Service Information Platform	Prevention of unauthorized access from an external Internet	・A function must be implemented to prevent unauthorized access attempts from an external Internet. Example:Defensive function based on a firewall	◎	◎	○ CPS.PT-3
SR3-SP-3	★★★	Smarthome Service Information Platform	Actions against attacks that exploit Web application vulnerabilities	Take actions against attacks are launched from an external network by exploiting Web application vulnerabilities. Example:WAF feature ・Where a Website or Web application is implemented, take vulnerability actions adhering to the following guidelines: -"Building a Secure Website" [28]	○ UK13	◎	○ CPS.CM-3

SR3-SP-4	★★★	Smarthome Service Information Platform	Detection and blocking of intrusions	・An intrusion detection function, which monitors hosts or communication line and notifies the administrator when it detects intrusions, and a function that blocks unauthorized access or intrusion communication, must be implemented.	○ UK10	◎	＝ CPS.CM-2 CPS.CM-3 CPS.CM-5
SR3-SP-5	★★★	Smarthome Service Information Platform	DoS protection	・Build a design rugged enough to withstand load testing and a certain level of load to preclude (D) Dos attacks that place server, network and other resources under excessive load or exploit their vulnerabilities.	＝ UK9	◎	○ CPS.DS-6
SR3-SP-6	★★★	Smarthome Service Information Platform	Logging and analysis	・Operation logs, status logs and the like must be kept to allow incidents to be analyzed when they occur.	○ UK10	◎	＝ CPS.MA-2 CPS.PT-1 CPS.CM-2 CPS.CM-5 CPS.AN-2
SR3-SP-7	★★★	Smarthome Service Information Platform	Malware protection	Anti-malware/virus actions must be enforced on service platforms.	◎	◎	○ CPS.PT-3

SR3-SP-8	★★★	Smarthome Service Information Platform	Server security action	・Basic server security actions as outlined below must be enforced: 1)Closure of unnecessary services and deletion of unnecessary applications 2)Change from the default administrative privilege accounts 3)Deletion of unnecessary accounts	○ UK6	◎	○ CPS.AC-8 CPS.PT-2
SR3-SP-9	★★★	Smarthome Service Information Platform	Encryption of communication paths	Paths of communication with Smarthome Service Information Platforms and home gateways must be encrypted. *Otherwise, the communication paths must be configured for higher security strength by using leased lines, VPNs and so on. *If cryptography with authentication is implemented in Secondary Requirement "Authentication" for a ★★ service, however, no response to this secondary requirement is required because such implementation addresses the secondary requirement for an encrypted communication path at the same time. *Cryptography must be implemented to comply with the Guidelines by consulting the following:	○ UK5	◎	○ CPS.DS-3

				“TLS Encryption Setup Guidelines" [22] “List of Cyphers to be Referenced for Procurement for the e-Government" [23] or "CRYPTREC Cryptographic Technology Guidelines (Lightweight Cryptography)" [24]			
SR3-SP-10	★★★	Smarthome Service Information Platform	Encryption of data	・Assets to be protected must be encrypted. *For information about the assets to be protected, see Table 3-2, Section 3.2 of this document. * Encrypt those assets having a higher level of importance based on services and use cases. *Cryptography must be implemented to comply with the Guidelines by consulting the following: “TLS Encryption Setup Guidelines" [22] “CRYPTREC Cyphers List" [23]	○ UK4 UK8	◎	○ CPS.DS-2
SR3-SP-11	★★★	Smarthome Service Information Platform	Key management	・Enforce proper management of the keys used to encrypt communication paths and data. *The method of key management must be implemented to comply with the Guidelines by consulting the following: “NIST SP (Special Publications) 800-57" [25] “Survey and Review for Revising SSL/TLS	○ UK4	◎	○ CPS.DS-5

				Encryption Setup Guidelines and for Creating Key Management Guidelines - Survey Report -" [26]			
SR3-SP-12	★★★	Smarthome Service Information Platform	Minimization of collected data	・The implementation must be such as to minimize the collection of data.	◎	◎	＝ CPS.GV-2
SR3-SP-13	★★★	Smarthome Service Information Platform	Vulnerability scanning and penetration testing	Run vulnerability scanning and penetration testing periodically to check for any vulnerabilities. The method and timing of such check should be set individually to suit the services provided.	◎	◎	○ CPS.CM-7

6.2.2 Security Secondary Requirements for Service Provider Information Platforms

Security Secondary Requirements for Service Provider Information Platform are summarized below. (Entry points: EP③ to EP④)

Table 6-5 Security Secondary Requirements for Service Provider Information Platform

No.	Level	Scope	Item	Description	UK	SB327	CPSF
SR2-PP-1 ～ SR2-PP-7	★★	Service Provider Information Platform	Responding to Common Requirements ～ Installation of security patches	※The same actions as those required by the Security Secondary Requirements for Smarthome Services information platform must be implemented. *To find out more about the Secondary Requirements, see SR2-SP-1 to SR2-SP-7, Section 6.2.1.	※See “Smarthome Service Information Platform.		
SR3-PP-1 ～ SR3-PP-13	★★★	Service Provider Information Platform	Responding to ★★ service requirements ～ Vulnerability scanning and penetration testing	*The same actions as those required by the security Requirements for Smarthome Services information platform must be implemented. *To find out more about the Secondary Requirements, see SR3-SP-1 to SR3-SP13, Section 6.2.1.	※See “Smarthome Service Information Platform.		
SR3-PP-14	★★★	Service Provider	Deletion of personal information	・The platform must support a function for deleting collected personal information when it is no longer needed or when a request to delete is	＝ UK8	◎	＝ CPS.GV-2 CPS.IP-6

		Information Platform		received from the service provider.			
SR3-PP-15	★★★	Service Provider Information Platform	Authentication of each servicer	As for each servicer accesses the infoemation platform, perform appropriate access management.	◎	◎	＝ CPS.AC-2 CPS.AC-3 CPS.AC-5 CPS.AC-9

6.2.3 Security Secondary Requirements for Home Gateways

Security Secondary Requirements for a home gateway are summarized below. (Entry points: EP⑤ to EP⑥)

Table 6-6 Security Secondary Requirements for Home Gateways

No.	Level	Scope	Item	Description	UK	SB327	CPSF
SR2-H-1	★★	Home gateway	Responding to Common Requirements	・Common Requirements ★ defined in the IoT Field Common Security Guidelines must be met.	＝ UK1 UK6 UK13	＝ 1798.91.05	＝ CPS.IP-1 CPS.IP-6 CPS.PT-2
SR2-H-2	★★	Home gateway	Authentication	・A scheme of mutual authentication among the connected devices must be implemented.	◎	◎	＝ CPS.AC-3 CPS.AC-9

SR2-H-3	★★	Home gateway	Management of information needed for mutual authentication	・A scheme of preventing the leakage of information needed for mutual authentication must be implemented.	◎	◎	○ CPS.AC-3 CPS.AC-9
SR2-H-4	★★	Home gateway	Device operation monitoring, fault monitoring	Carry out operation monitoring and fault monitoring of service-compatible devices regarding the following points: 1)Device alive management 2)Connection of unauthorized devices	○ UK10	◎	＝ CPS.DS-7 CPS.CM-2 CPS.CM-3
SR2-H-5	★★	Home gateway	USB terminal protection	・Make USB terminals (ports) hardly accessible to any personnel other than operators to reduce the risks of improper connection. Further, do not install USB terminals that are not needed for service purposes. Example:Use a physical cover on any USB terminal, and so on.	◎	◎	○ CPS.PT-2
SR2-H-6	★★	Home gateway	Release of software updates to fix reported vulnerabilities	・If vulnerabilities have been reported in the OS, boot program or applications used, run testing and release software updates promptly.	＝ UK3	◎	＝ CPS.DS-7 CPS.MA-1

SR3-H-1	★★★	Home gateway	Responding to ★★ service requirements	・Security Requirements for similar devices used for ★★ must be fulfilled.	※See ★★.		
SR3-H-2	★★★	Home gateway	Prevention of unauthorized access attempts from an external Internet	・A function must be implemented to prevent unauthorized access attempts from an external Internet. Example:Defensive function based on a firewall	◎	◎	○ CPS.PT-3
SR3-H-3	★★★	Home gateway	Actions against attacks that exploit Web application vulnerabilities	・If a function managing Web application or Web API-based settings or operations is implemented, take vulnerability actions adhering to the following guidelines: -"Building a Secure Website" [28]	○ UK13	◎	○ CPS.CM-3
SR3-H-4	★★★	Home gateway	Encryption of the paths of communication with external Internet	・For communication with the external Internet, encrypt the communication path. *If cryptography with authentication is implemented in Secondary Requirement No.2 "Authentication" for a ★★ service, however, no response to this requirement is required because such implementation addresses the secondary requirement for an encrypted communication path	○ UK5	◎	○ CPS.DS-3

				at the same time. *Cryptography must be implemented to comply with the Guidelines by consulting the following: -"TLS Encryption Setup Guidelines" [22] -"CRYPTREC Cyphers List" [23] or "CRYPTREC Cryptographic Technology Guidelines (Lightweight Cryptography)" [24]			
SR3-H-5	★★★	Home gateway	Encryption of the paths of communication with LAN-attached devices	・The paths of communication with LAN-attached devices must be encrypted. *This does not apply where the home gateway is wired to devices on the LAN. *If cryptography with authentication is implemented in Secondary Requirement No.2 "Authentication" for a ★★ service, however, no response to this requirement is required because such implementation addresses the secondary requirement for an encrypted communication path at the same time. *Cryptography must be implemented to comply with the Guidelines by consulting the following:	○ UK5	◎	○ CPS.DS-3

				"TLS Encryption Setup Guidelines" [22] -"CRYPTREC Cyphers List" [23] or "CRYPTREC Cryptographic Technology Guidelines (Lightweight Cryptography)" [24]			
SR3-H-6	★★★	Home gateway	Data encryption	・Encrypt the assets to be protected that have been saved. *For information about the assets to be protected, see Table 3-2, Section 3.2 of this document. * Encrypt those assets having a higher level of importance to reflect services and use cases. *Cryptography must be implemented to comply with the Guidelines by consulting the following: -"TLS Encryption Setup Guidelines" [22] -"CRYPTREC Cyphers List" [23] or "CRYPTREC Cryptographic Technology Guidelines (Lightweight Cryptography)" [24]	○ UK4 UK8	◎	○ CPS.DS-2
SR3-H-7	★★★	Home gateway	Key management	・Enforce proper management of the keys used to encrypt communication paths and data. *The method of key management must be implemented to comply with the Guidelines by	○ UK4	◎	○ CPS.DS-5

				consulting the following: “NIST SP (Special Publications) 800-57” [25] “Survey and Review for Revising SSL/TLS Encryption Setup Guidelines and for Creating Key Management Guidelines - Survey Report -" [26]			
SR3-H-8	★★★	Home gateway	Logging and analysis	・Access logs must be kept to allow incidents to be analyzed on the Service Information Platform as they occur.	◎	◎	＝ CPS.MA-2
SR3-H-9	★★★	Home gateway	Vulnerability scanning and penetration testing	・When the development of a new product is completed or software is updated, run vulnerability scanning and penetration testing to check for presence or absence of any vulnerabilities.	◎	◎	○ CPS.CM-7

6.2.4 Security Secondary Requirements for Smarthome-Compatible Devices

Security Secondary Requirements for smarthome-compatible devices are outlined below. (Entry points: EP⑦ to EP⑧)

Table 6-7 Security Secondary Requirements for Smarthome-Compatible Devices

No.	Level	Scope	Item	Description	UK	SB327	CPSF
SR2-D-1	★★	Smarthome-compatible devices	Responding to Common Requirements	・Common Requirements ★ in the Common Security Guidelines must be fulfilled.	＝ UK1 UK6 UK13	＝ 1798.91.05	＝ CPS.IP-1 CPS.IP-6 CPS.PT-2
SR2-D-2	★★	Smarthome-compatible devices	Authentication	・A scheme of mutual authentication must be implemented.	◎	◎	＝ CPS.AC-3 CPS.AC-9
SR2-D-3	★★	Smarthome-compatible devices	Management of information needed for mutual authentication	・A scheme of preventing the leakage of information needed for mutual authentication must be implemented.	◎	◎	＝ CPS.AC-3 CPS.AC-9

SR2-D-4	★★	Smarthome-compatible devices	USB terminal protection	・Make USB terminals (ports) hardly accessible to any personnel other than operators to reduce the risks of unauthorized connection. Further, do not install USB terminals that are not needed for service purposes. Example:Cover USB connection terminals with a physical cover, and more.	◎	◎	○ CPS.PT-2
SR2-D-5	★★	Smarthome-compatible devices	Release of software updates to fix reported vulnerabilities	・If vulnerabilities have been reported on the software or firmware installed in devices, run testing and release software updates promptly.	＝ UK3	◎	＝ CPS.DS-7 CPS.MA-1
SR3-D-1	★★★	Smarthome-compatible devices	Responding to ★★ service requirements	・Security Secondary Requirements for similar devices used for ★★ must be fulfilled.	※See ★★.		
SR3-D-2	★★★	Smarthome-compatible devices	ncryption of the path of communication with LAN-attached devices	・The paths f communication with LAN-attached devices must be encrypted. *No response to this secondary requirement is required for a wired connection. *If cryptography with authentication is implemented in Secondary Requirement No.2	○ UK5	◎	○ CPS.DS-3

				"Authentication" for a ★★ service, however, no response to this secondary requirement is required because such implementation addresses the secondary requirement for an encrypted communication path at the same time. *Cryptography must be implemented to comply with the Guidelines by consulting the following: -TLS Encryption Setup Guidelines" [22] -“CRYPTREC Cyphers List" [23] or ”CRYPTREC Cryptographic Technology Guidelines (Lightweight Cryptography)" [24]			
SR3-D-3	★★★	Smarthome-compatible devices	Key management	・Enforce proper management of the keys used for encrypting communication paths.	＝ UK4	◎	＝ CPS.DS-5
SR3-D-4	★★★	Smarthome-compatible devices	Communications I/F allowing for availability	Implement connectivity with the home gateway to allow for availability to suit the service provided.	◎	◎	＝ CPS.DS-7
SR3-D-5	★★★	Smarthome-compatible devices	Vulnerability scanning and penetration testing	・When the development of a new product is completed or software is updated, run vulnerability scanning and penetration testing to check for presence or absence of any	◎	◎	○ CPS.CM-7

				vulnerabilities.			

6.2.5 Security Secondary Requirements for Smartphone Applications

Security Secondary Requirements for Smartphone Applications are summarized below. (Entry points: EP⑨ to EP⑩)

*At present, relevant Secondary Requirements are limited to ★★.

Table 6-8 Security Secondary Requirements for Smartphone Applications

No.	Level	Scope	Item	Description	UK	SB327	CPSF
SR2-A-1	★★	Smartphone Application	User authentication	・Security actions based on multi-factor authentication must be enforced when smartphone applications are used.	◎	◎	= CPS.AC-3 CPS.AC-9
SR2-A-2	★★	Smartphone Application	Secure design ・Coding	Security-conscious design and coding compliant with the following guidelines must be implemented: “Android Application Secure Design and Secure Coding Guide” [27].	◎	◎	= CPS.RA-4
SR2-A-3	★★	Smartphone Application	Updating Smartphone Applications	・Whenever security holes or bugs that could affect smartphone applications are identified, software updates must be released promptly to fix them.	= UK3	◎	= CPS.DS-7 CPS.MA-1

7 Conclusion

This Guidelines has presented a typical smartphone system model, along with use cases to help discuss possible threats and actions relevant to it. Then, the categorizations of smarthome products and services and the impact of smarthome characteristics upon security were reviewed and threats to use cases and the actions were analyzed and assessed. A summary description of the security actions to be taken in the life cycles of development work for smarthome services and smarthomes (houses) was also included. The Guidelines proceeds to sort security actions required for smarthome services and systems and devices, and compile them into Security Requirements and Secondary Requirements.
The authors hope that this Guidelines will aid readers in taking relevant approaches to planning, designing and developing smarthome products and services in the present context of growing popularity of smarthomes.

While the calculation of risk metrics based on the Smarthome Unique Method presented in this Guidelines has taken Life and Property Impact and Information Importance into consideration, further studies should be directed at determining whether it is necessary to capture other smarthome-specific security characteristics. Further, because the procedural flow of risk analyses and assessment outlined in this Guidelines is a time-consuming step to follow, it should require further refinement.

The authors would like to update the Guidelines to reflect changes of the times by responding to emerging smarthome products and services and by responding to emerging attack techniques, as well as develop responses to these issues at a higher level of refinement.

Although this document has been prepared as Security Guidelines for the smarthome field, its threat assumptions and security efforts made in the life cycle of a smarthome might apply to other categories as well. It is the authors' wish that the reader will make positive use of the Guidelines in pursuing security actions in their respective processes of developing various products and services.

Citation / References

[1] State of California, "SB-327 Information privacy: connected devices.”

http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

[2] IoT 推進コンソーシアム,総務省,経済産業省, ”IoT セキュリティガイドライン”

http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf

[3] 総務省, “平成 28 年版情報通信白書” 第 1 部 第 2 章 第 1 節 1 p.80

http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/pdf/n2100000.pdf

[4] IPA, ”つながる世界の開発指針　～安全安心な IoT の実現に向けて開発者に認識してほしい重要ポイント～”

https://www.ipa.go.jp/files/000051411.pdf

[5] CCDS, ”IoT 分野共通セキュリティ要件ガイドライン 2018 年度版（案）”

https://www.ccds.or.jp/public/document/other/IoT 分野共通セキュリティ要件ガイドライン 2018 年度版（案）.pdf

[6] IPA, “IoT 開発におけるセキュリティ設計の手引き”

https://www.ipa.go.jp/security/iot/iotguide.html

[7] 経済産業省, “別表第八 電気用品安全法施行令（昭和三十七年政令第三百二十四号）別表第一第六号から第九号まで及び別表第二第七号から第十一号までに掲げる交流用電気機械器具並びに携帯発電機”

http://www.meti.go.jp/policy/consumer/seian/denan/kaishaku/gijutsukijunkaishaku/beppyoudai8.pdf

[8] 国立研究開発法人産業技術総合研究所, “国際標準化の新規開発提案が承認される”

https://www.aist.go.jp/aist_j/news/nr20180330.html

[9] 総務省, “クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）”
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00001.html

[10] CCDS, “製品分野別セキュリティガイドライン IoT-GW 編 Ver.2.0”
https://www.ccds.or.jp/public/document/other/CCDS Product Field-Specific Security
Guidelines IoT-GW Ver2.0.pdf

[11]STRIDE:A scheme of threat classification proposed by Microsoft.
https://docs.microsoft.com/ja-jp/azure/security/azure-security-threat-modeling tool-threats

[12] CCDS, “IoT システム調達のためのセキュリティ要件フレームワーク”
https://www.ccds.or.jp/public/document/other/CCDS_IoT システム調達のためのセキュリティ要件フレームワーク.pdf

[13] JPCERT/CC, “インシデントとは？“
https://www.jpcert.or.jp/aboutincident.html

[14] IPA, “つながる世界の開発指針第 2 版”
https://www.ipa.go.jp/sec/reports/20170630.html

[15] CCDS, “IoT セキュリティ評価検証ガイドライン Rev1.0”
https://www.ccds.or.jp/public/document/other/guidelines/CCDS_IoT セキュリティ評価検証ガイドライン_rev1.0.pdf

[16] FIRST (Forum of Incident Response and Security Teams),
“Common Vulnerability Scoring System v3.0: Specification Document”
https://www.first.org/cvss/specification-document

[17] IPA, “共通脆弱性評価システム CVSS v3 概説”
https://www.ipa.go.jp/security/vuln/CVSS v3.html

[18]OTA, “IoT Security & Privacy Trust Framework v2.5”
https://www.internetsociety.org/wp content/uploads/2018/05/iot_trust_framework2.5a_Japanese.pdf

[19 OWASP, “Top 10 IoT Vulnerabilities (2014)”

https://www.owasp.org/index.php/Top_10_IoT_Vulnerabilities_(2014)

[20] 経済産業省, “サイバー・フィジカル・セキュリティ対策フレームワーク Version1.0”

https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

[21] GOV.UK, “Code of Practice for Consumer IoT Security”

https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot security

[22] IPA, “TLS 暗号設定ガイドライン”

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

[23] CRYPTREC, “電子政府における調達のために参照すべき暗号のリスト”

https://www.cryptrec.go.jp/list.html

[24] CRYPTREC, “CRYPTREC 暗号技術ガイドライン(軽量暗号)”

https://www.cryptrec.go.jp/tech_guidelines.html

[25] National Institute of Standards and Technology (NIST), NIST SP800-57 Part 1

“Recommendations for Key Management (Part I: General Matters)”

https://www.ipa.go.jp/files/000055491.pdf

[26] IPA, “SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－”

https://www.ipa.go.jp/files/000067459.pdf

[27] JSSEC, “Android アプリのセキュア設計・セキュアコーディングガイド”

https://www.jssec.org/dl/android_securecoding.pdf

[28] IPA, “安全なウェブサイトの作り方”

https://www.ipa.go.jp/files/000017316.pdf

Authors/Editors

Project General Manager:Sekisui House, Ltd.

Project Deputy Manager:LIXIL Corporation

Smarthome WG

ALPHA Corporation

Sekisui Home Techno Co., Ltd.

Nippon Systemware Co., Ltd.

Bunka Shutter Co., Ltd.

Rinnai Corporation

MAST TOP Co., Ltd.

Guidelines Supervisory Board

President:

Tsukasa OginoRepresentative Director, Connected Consumer Device Security Council, general incorporated association

Membership:

Yasuo Tan, Professor, Graduate School of Science and Technology, Japan Advanced Institute of Science and Technology

Katsunari Yoshioka

Associate Professor, Yokohama National University Graduate School of Environment and Information Sciences/Institute of Advanced Sciences