IoT Safety/Security Development Guidelines
(Second Edition)

: Important Points to be understood by Software Developers toward the Smart-society

Software Reliability Enhancement Center, Technology Headquarters,

Information-technology Promotion Agency

Introduction

In recent years, efforts toward the IoT (Internet of Things) have progressed in different countries. However, as things that were previously unconnected or not assumed to be connected can now be connected, Safety/Security risks are expected to increase. Many devices and systems, such as automobiles and home electrical appliances, are used for 10 or more years, and therefore measures against IoT risks must immediately be implemented. Developing devices and systems that can protect data, software etc. is also expected to contribute to strengthening international competitiveness.

The Software Reliability Enhancement Center, Technology Headquarters, Information-technology Promotion Agency (IPA/SEC) therefore compiled the Safety/Security matters to at least be considered by companies involved in devices and systems characteristic of the "Smart-society," in which new values are created by various things connected to each other, to serve as the "IoT Safety/Security Development Guidelines" (hereinafter referred as the "Development Guidelines").

The Development Guidelines describe not concrete individual compliance standards but the direction of Safety/Security measures to be taken across industries. For the guidelines described in Chapter 4, individual measures should be considered by parties concerned, though implementation based on the consideration is to be made at each party's discretion.

Safety/Security of the Smart-society is expected to be achieved through the understanding and implementation of the Development Guidelines by the corporate managers, developers, and maintenance staff of the companies involved in the development of devices and systems.

Table 1 specifically intended readers

Chapter		Manager	Developer	Maintenance staff
Chapter 1		○	○	○
Chapter 2			○	
Chapter 3			○	
Chapter 4	4.1	○	○	○
	4.2		○	
	4.3		○	
	4.4		○	○
	4.5		○	○
Chapter 5			○	

The abbreviations used in the Development Guidelines are as follows:

Table 2 List of abbreviations

Abbreviation	Term in full
ASIL	Automotive Safety Integrity Level
ATM	Automatic Teller Machine
AV	Audio Visual
BBF	Broadband Forum
BIOS	Basic Input/Output System
CAN	Controller Area Network
C2C-CC	CAR 2 CAR Communication Consortium
CCDS	Connected Consumer Device Security council
CD-ROM	Compact Disc Read Only Memory
CPS	Cyber Physical System
CSIRT	Computer Security Incident Response Team
DAF	Dependability Assurance Framework for Safety Sensitive Consumer Devices
DNS	Domain Name System
DRBFM	Design Review Based on Failure Model
D-Bus	Desktop Bus
EAL	Evaluation Assurance Level
ECU	Engine Control Unit
EDSA	Embedded Device Security Assurance
FA	Factory Automation
GSN	Goal Structuring Notation
HDD	Hard Disk Drive
HEMS	Home Energy Management System
ICT	Information and Communication Technology
ID	Identification
IEC	International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
I/F	Interface
IIC	Industrial Internet Consortium
IoT	Internet of Things
IPA	Information-technology Promotion Agency, Japan
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
JPCERT	Japan Computer Emergency. Response Team Coordination
METI	Ministry of Economy, Trade and Industry
NIST	National Institute of Standards and Technology
OBD	On-Board Diagnostics
OCF	Open Connectivity Foundation
OS	Operating System
OSS	Open Source Software
POS	Point of Sales
PL	Performance Level
RFID	Radio Frequency Identifier
SAL	Security Assurance Levels
SIL	Safety Integrity Level
SMS	Short Message Service
SoS	System of Systems
TAL	Trust Assurance Levels
USB	Universal Serial Bus

Table of contents

Chapter 1
Smart-society and Purposes of Development Guidelines

IoT (Internet of Things) indicates a society in which all sorts of "things" are connected to each other, and is expected to have various advantages. For the "things" that were previously unconnected, however, there are risks that security measures may not be sufficiently implemented when compared with information devices such as servers and PCs that have always been connected, and safety issues may occur due to the connections.

This chapter explains the Smart-society, its risks, and the purposes of the Development Guidelines toward reducing the risks. Figure 1-1 shows the flow of this chapter.

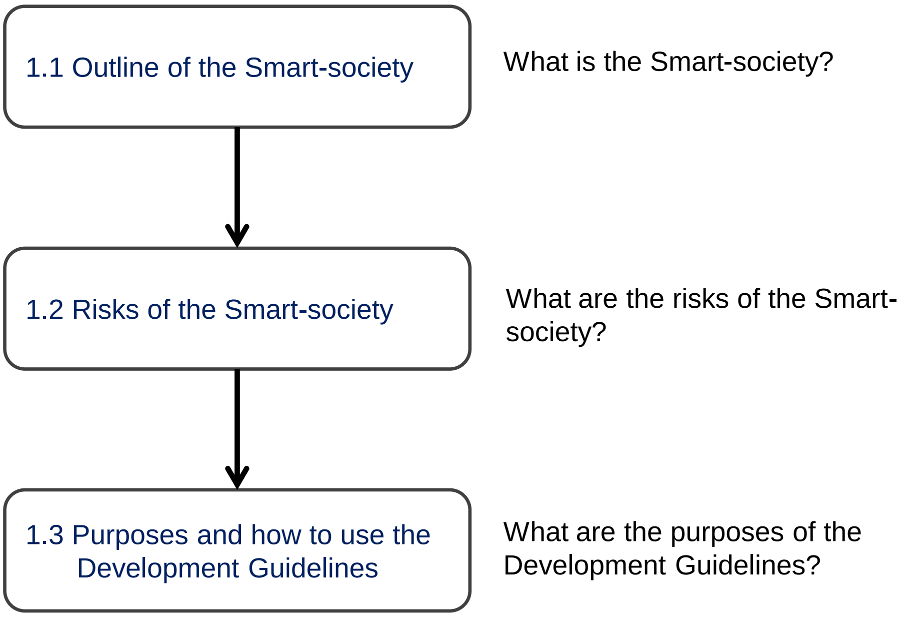

1.1 Outline of the Smart-society
What is the Smart-society?
1.2 Risks of the Smart-society
What are the risks of the Smart-society?
1.3 Purposes and how to use the Development Guidelines
What are the purposes of the Development Guidelines?

Figure 1-1 Flow of this chapter

1.1 Outline of the Smart-society

1.1.1 IoT and the Smart-society

IoT is an abbreviation for "Internet of Things", and, according to Kevin Ashton, who proposed the IoT in 1999, is a concept that computers will be able to save human resources and to observe, identify, and understand the society by quickly and accurately collecting information from "things" using RFID and sensors [1]. In the current IoT, its important characteristics also include the ability to obtain new knowledge using vast amount of data (big data) and to control devices and systems in real time.

In recent years, car navigation systems, home electrical appliances, health care devices, etc., have been equipped with computer systems and have information collection, data transmission, and remote control functions. The fact that many of these embedded systems use general-purpose OS and communications standards has been a contributing factor for the Smart-society in which various "things" can easily be connected.

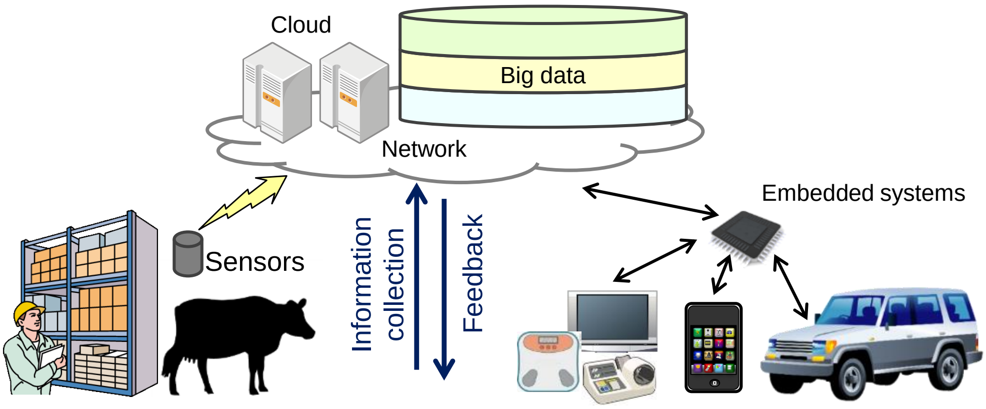


Figure 1-2 IoT in which all sorts of things are connected

The concept of "System of Systems (SoS)" in which multiple systems collaborate as a larger system to achieve new values can be a good reference for the IoT.

Main characteristics of System of Systems (SoS)

1. Operational Independence of the Elements: If the system-of-systems is disassembled into its component systems the component systems must be able to usefully operate independently. The system-of-systems is composed of systems which are independent and useful in their own right.
2. Managerial Independence of the Elements: The component systems not only can operate independently, they do operate independently. The component systems are separately acquired and integrated but maintain a continuing operational existence independent of the system-of- systems.
3. Evolutionary Development: The system-of-systems does not appear fully formed. Its development and existence is evolutionary with functions and purposes added, removed, and modified with experience.
4. Emergent Behavior: The system performs functions and carries out purposes that do not reside in any component system. These behaviors are emergent properties of the entire system-of-systems and cannot be localized to any component system. The principal purposes of the systems-of-systems are fulfilled by these behaviors.
5. Geographic Distribution: The geographic extent of the component systems is large. Large is a nebulous and relative concept as communication capabilities increase, but at a minimum it means that the components can readily exchange only information and not substantial quantities of mass or energy.

Source: "Architecting Principles for Systems-of-Systems," Mark W. Maier

The "Smart-society" in the Development Guidelines also implies the society of SoS, in which "things" are not only connected each other but also managed independently, and the individual IoT that are useful on their own further evolve as a larger IoT through connection with others to achieve new objectives or functions. The characteristics of the SoS are shown as 1.-5 in Figure 1-3.

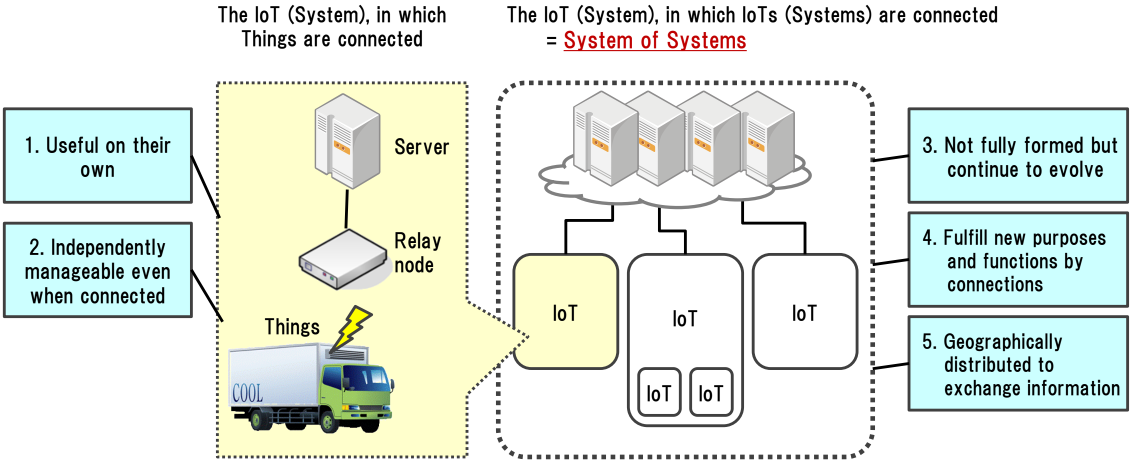
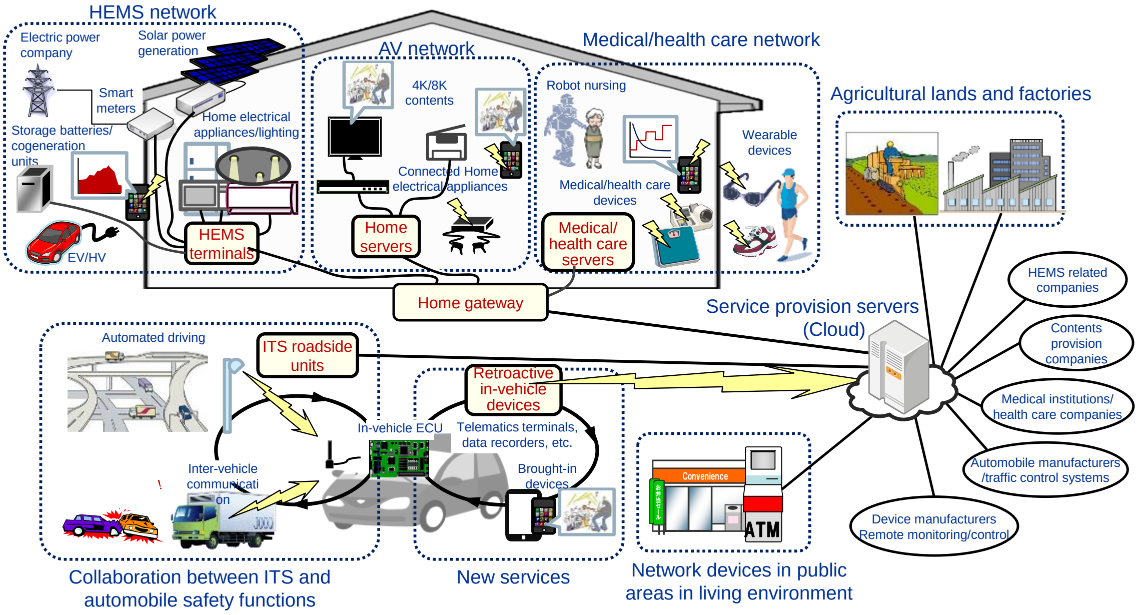

The IoT (System), in which Things are connected
The IoT (System), in which IoTs (Systems) are connected = System of Systems
1. Useful on their own
2. Independently manageable even when connected
Server
Relay node
Things
COOL
IoT
IoT
IoT
IoT
IoT
3. Not fully formed but continue to evolve
4. Fulfill new purposes and functions by connections
5. Geographically distributed to exchange information

Figure 1-3 Image of the "Smart-society" = IoT with the SoS characteristics

1.1.2 Ever-changing massive infrastructure

The number of devices that can be connected to the IoT is expected to increase to 25 to 50 billion by 2020, comprising a massive infrastructure that spans across homes, public spaces, offices, factories, agricultural lands, etc. The IoT is considered to be an important infrastructure for the entire society, including companies and consumers.


HEMS network
Electric power company
Solar power generation
Smart meters
Storage batteries/ cogeneration units
Home electrical appliances/lighting
EV/HV
HEMS terminals
AV network
4K/8K contents
Connected Home electrical appliances
Home servers
Medical/health care network
Robot nursing
Wearable devices
Medical/health care devices
Medical/ health care servers
Agricultural lands and factories
Home gateway
Service provision servers (Cloud)
HEMS related companies
Contents provision companies
Medical institutions/ health care companies
Automobile manufacturers /traffic control systems
Device manufacturers Remote monitoring/control
Automated driving
ITS roadside units
Retroactive in-vehicle devices
In-vehicle ECU
Telematics terminals, data recorders, etc.
Brought-in devices
Inter-vehicle communicati on
Convenience
ATM
Collaboration between ITS and automobile safety functions
New services
Network devices in public areas in living environment

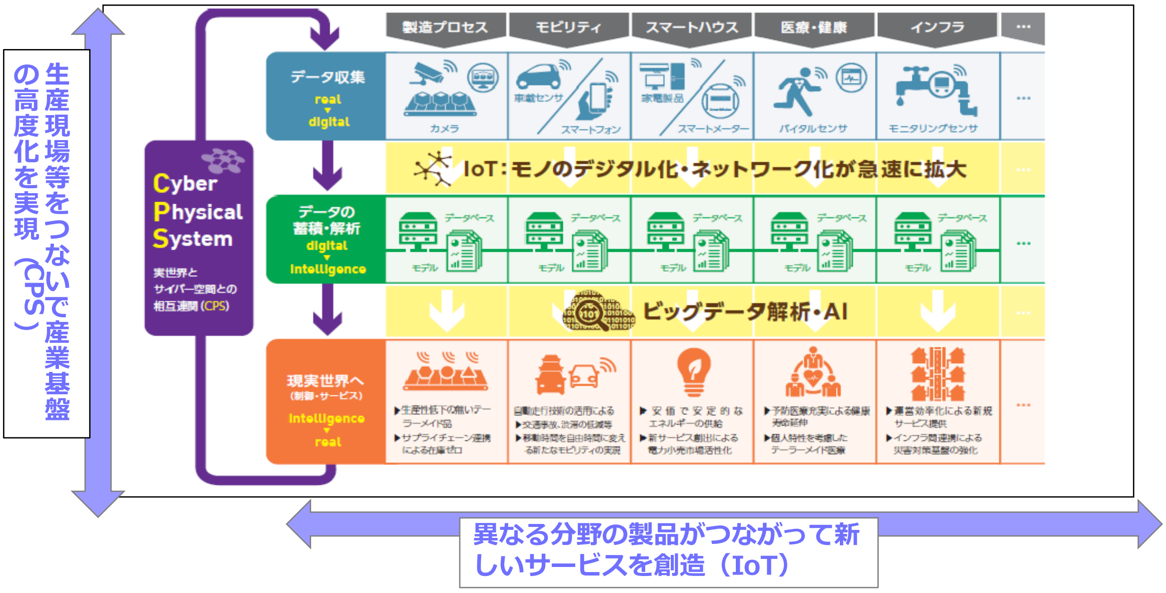
Source: Prepared by amending the figure in "Secure Life 2020," The Connected Consumer Device Security Council

Figure 1-4 The IoT as an infrastructure spanning across society

The IoT is different from the "Critical Information Infrastructure [2]," specified by the government, however, in that it keeps changing as various devices and systems are connected by service providers and consumers on a daily basis, and wearable devices and automobiles are connected while they are moving. Understanding the whole context of the IoT is therefore difficult.

In 2015, the Information Economy Subcommittee for the Ministry of Economy, Trade and Industry published the image of a Cyber Physical System (CPS) for advancing the industrial base in the interim report (proposed) (Figure 1-5). This figure shows the image of a vertical CPS in each sector collaborating horizontally as the IoT to create new values by analyzing big data, etc.

This means that a CPS in each sector becomes the IoT through horizontal collaboration, and the abovementioned concept of “System of Systems” is applicable as it creates new values.


生産現場等をつないで産業基盤の高度化を実現（CPS）
Cyber Physical System
実世界とサイバー空間との相互連関(CPS)
製造プロセス
モビリティ
スマートハウス
医療・健康
インフラ
…
データ収集
real
digital
カメラ
車載センサ
スマートフォン
家電製品
スマートメーター
バイタルセンサ
モニタリングセンサ
IoT：モノのデジタル化・ネットワーク化が急速に拡大
データの蓄積・解析
digital
intelligence
データベース
モデル
ビッグデータ解析・AI
現実世界へ（制御・サービス）
intelligence
real
▶生産性低下の無いテーラーメイド品
▶サプライチェーン連携による在庫ゼロ
自動走行技術の活用による
▶交通事故、渋滞の低減等
▶移動時間を自由時間に変える新たなモビリティの実現
▶安価で安定的なエネルギーの供給
▶新サービス創出による電力小売市場活性化
▶予防医療充実による健康寿命延伸
▶個人特性を考慮したテーラーメイド医療
▶運営効率化による新規サービス提供
▶インフラ間連携による災害対策基盤の強化
異なる分野の製品がつながって新しいサービスを創造（IoT）

Source: Prepared by amending the interim report (proposed) of the Information Economy Subcommittee for the Ministry of Economy, Trade and Industry

Figure 1-5 Image of CPS and IoT

1.2 Risks of the Smart-society

1.2.1 Characteristics of the risks of the Smart-society

The Smart-society is different from conventional information systems and Critical Information Infrastructure in that the following risk factors exist:

(1) Occurrence of unexpected connections

In recent years, general-purpose OS and standard communication interfaces have been used in devices and systems, enabling business operators other than the manufacturers to easily build IoT services and even consumers to connect devices out of mere curiosity. This raises concerns over the occurrence of unexpected connections, leading to external attacks and information leakage.

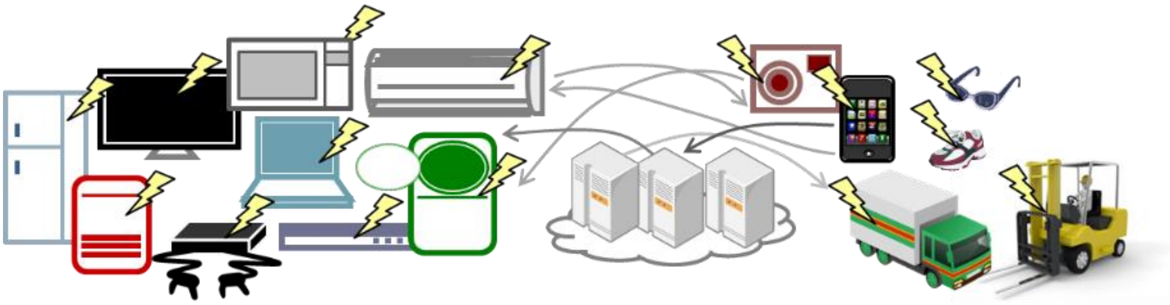


Figure 1-6 Occurrence of unexpected connections

(2) “Things” that are not properly managed can also be connected

Unlike the information systems of companies, “things" that are not properly managed can also be connected to the IoT, including wearable devices, automobiles in parking spaces, household equipment and electrical appliances at home, and devices that are being disposed. It is therefore relatively easy for malicious third parties to directly embed malicious software in devices and systems, or retrieve data and software from disposed devices. In addition, devices that are not properly maintained after 10 or more years of use can also co-exist, thus harming the Safety/Security of the entire IoT.

Figure 1-7 Devices and systems at home and in public spaces not physically managed by manufacturers

(3) Spread of physical and property harm through connections

For devices and systems such as home electrical appliances and automobiles, accidents and malfunctions can cause injury or damage (hereinafter referred to as "harm") to the health of people and property. For ATM and vending machines, harm to cash and goods may be caused. The extent of harm may be limited with individual devices, but there are concerns over the spreading of harm through connections to the IoT.

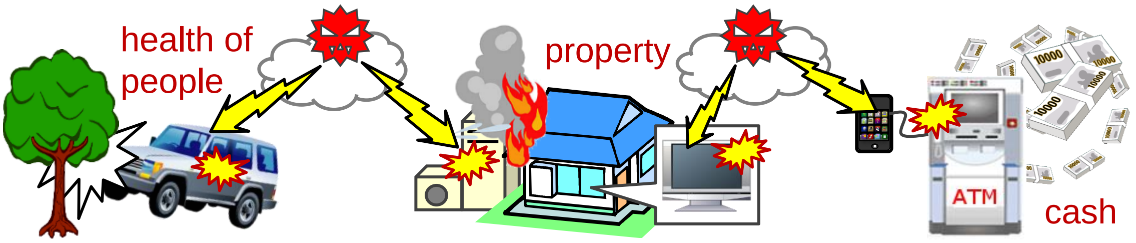


Figure 1-8 Harm to the health of people and property

(4) Difficulty of consumers to detect the occurrence of problems

Physical abnormalities such as failures and breakages are easy to detect, but software problems such as information leakage due to virus infection, setting errors, etc., are not visible. Unauthorized access and improper connection via wireless are also difficult to detect. Therefore, in the IoT, consumers are unlikely to notice the occurrence of problems due to connections.

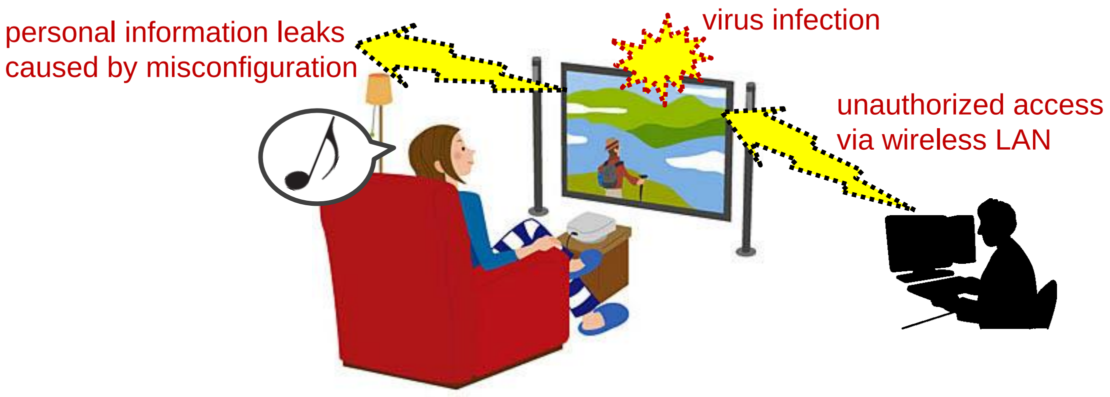

personal information leaks caused by misconfiguration
virus infection
unauthorized access via wireless LAN

Figure 1-9 Invisible risks of the IoT

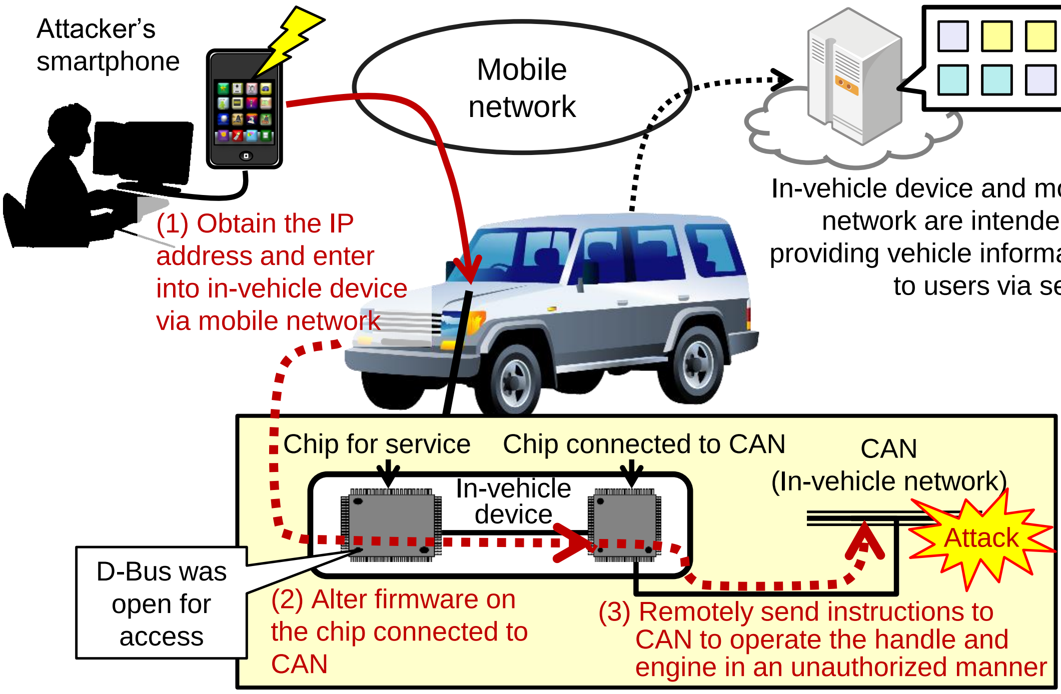
As described above, the IoT is an important infrastructure spanning across the entire society, but at the same time can harm users' health and property. There are many issues, however, such as difficulties in detecting connections, finding risks, and managing devices and systems. Safety/Security measures for devices and systems to be connected are therefore required.

1.2.2 Examples of risks of the Smart-society

Examples of risks of the Smart-society are presented here.

(1) Examples of risks that affect safety

At the global information security event “Black Hat 2015,” a demonstration was held to show that the handles and engines of moving automobiles could be controlled in an unauthorized manner by remotely accessing their in-vehicle devices. The risk is considered to be significant because serious harm involving human lives is assumed, and attacks can be made remotely without the attackers being seen. After the presentation, a total of 1.4 million vehicles of the target models were recalled.


Attacker’s smartphone
Mobile network
In-vehicle device and mobile network are intended for providing vehicle information to users via server
(1) Obtain the IP address and enter into in-vehicle device via mobile network
Chip for service
Chip connected to CAN
CAN (In-vehicle network)
In-vehicle device
Attack
D-Bus was open for access
(2) Alter firmware on the chip connected to CAN
(3) Remotely send instructions to CAN to operate the handle and engine in an unauthorized manner

Source: “生活機器の脅威事例集”, Connected Consumer Device Security Council

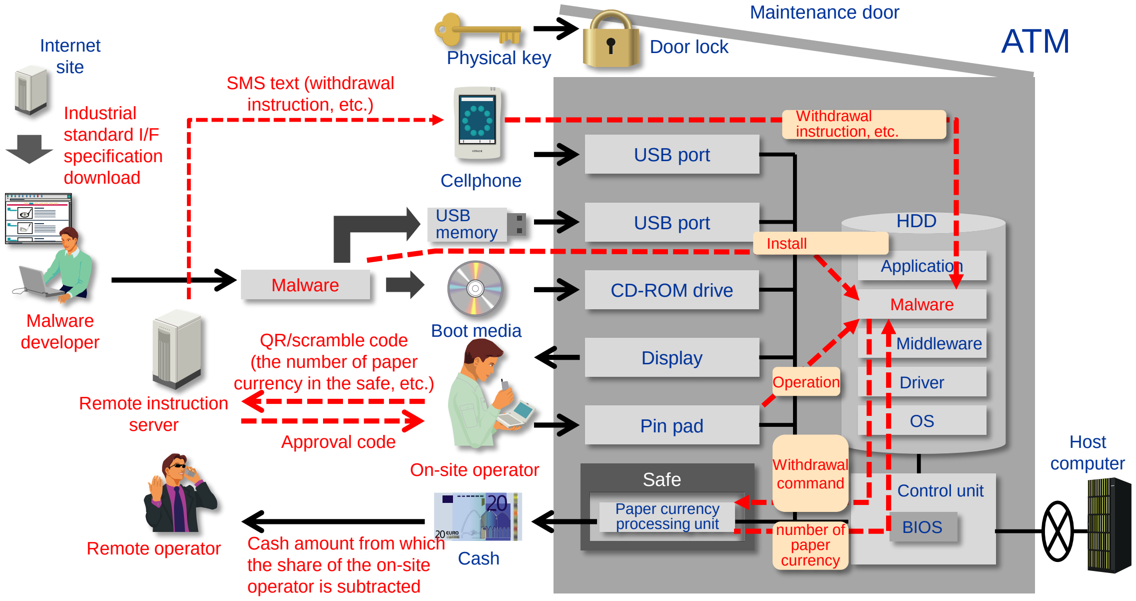
Figure 1-10 Remote attack against automobile

The main causes include the fact that the constituent elements such as mobile networks, in-vehicle devices, in-vehicle networks, and vehicle information display services were designed without considering the abovementioned attack. This enabled a series of attacks in which the attackers entered from mobile networks, got unauthorized access to in-vehicle devices, and altered the firmware on chips to send unauthorized instructions to in-vehicle networks. In the Smart-society, attacks must be stopped somewhere at some constituent elements.

In addition, conventional safety measures do not cover intentional attacks. In the Smart-society, the risks of external attacks imposed on safety functions also need to be dealt with.

(2) Examples of risks that affect security

In recent years, cases have increased overseas of withdrawing cash by illegally obtaining the physical keys to maintenance doors and opening ATM chassis to connect cellphones, etc., and install virus infections. Because of the existence of explicit harm of cash robbery and occurrence of an actual incident, the risk is considered significant.



Source: Document of Connected Consumer Device Security Council

Figure 1-11 Case of ATM risk (overseas case)

For ATMs, common specifications are used to enable banks to freely choose suppliers, and analyzing certain models can make attacks against other manufacturers' models easier. In particular, many ATMs developed in recent years use general-purpose OS, and are considered to be more vulnerable to attacks made by connecting devices that can handle the said OS.

In addition, not just for ATMs but for all devices, even high-security devices are considered not capable of handling those cases where insiders install malicious software on devices or disclose information regarding the settings and operations of devices.

In the Smart-society, internal fraud measures in addition to risk measures are required for all types of devices and systems.

(3) Examples of risks that affect reliability

In recent years, there had been an incident in the TVs of some manufacturers causing repeated power-on/off while viewing or recording. According to the announcement made by one of the manufacturers, the cause of the incident was improper processing of other companies' data in certain broadcasting data (common program listings, firmware update data for certain models, etc.) transmitted with TV programs. For the products of that manufacturer alone, up to 1.62 million units of 118 models were subject to correction of the defect [3].

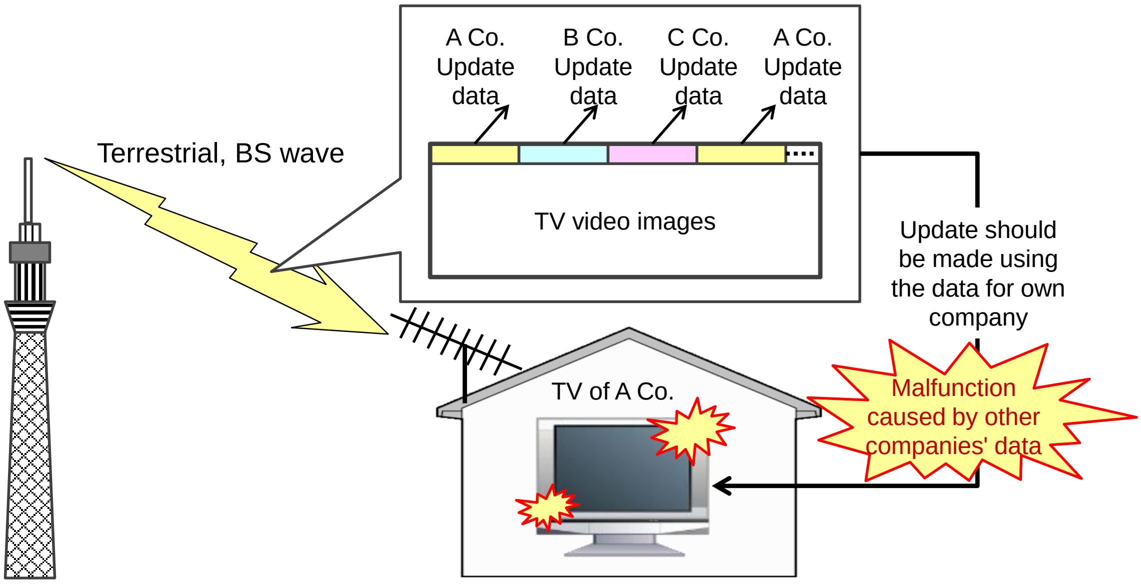


Figure 1-12 TV malfunction caused by update data

In another case, there was an incident of significant slowing down of PCs due to a defect in the pattern files of antivirus software. Because it happened on Saturday, damage to companies was limited to newspaper companies and transportation-related companies, etc., yet approximately 161,000 telephone inquiries were received for software for personal use and 13,000 for software for corporate use, of which only around 4,000 cases were dealt with in the beginning [4].

In the Smart-society, not only PCs but also automobiles, home electrical appliances, and various other devices and systems are connected to networks. If they become unavailable all at once for any reason, as in the above case, impacts to daily life can be significant. For software updates, sufficient consideration must be given not to affect "reliability," that is to allow users to use the software whenever they want.

1.3 Purposes and how to use the Development Guidelines

(1) Purposes of the Development Guidelines

In the Development Guidelines, Safety/Security-related matters to be considered in relation to the abovementioned risks in the development of IoT products are compiled as guidelines. Each guideline consists of the "Points" of efforts, "Description" of background, and concrete "Example measures." It aims to reduce the risks of the Smart-society by discussing all the points. Safety/Security of the Smart-society is expected to be achieved through use of the Development Guidelines by the corporate managers, developers, and maintenance staff of the companies involved in the development of devices and systems.

The intended readers of the Development Guidelines are mainly developers of the companies involved in the development of devices and systems, but matters that are difficult to deal with only by developers should also be read by corporate managers and maintenance staff.

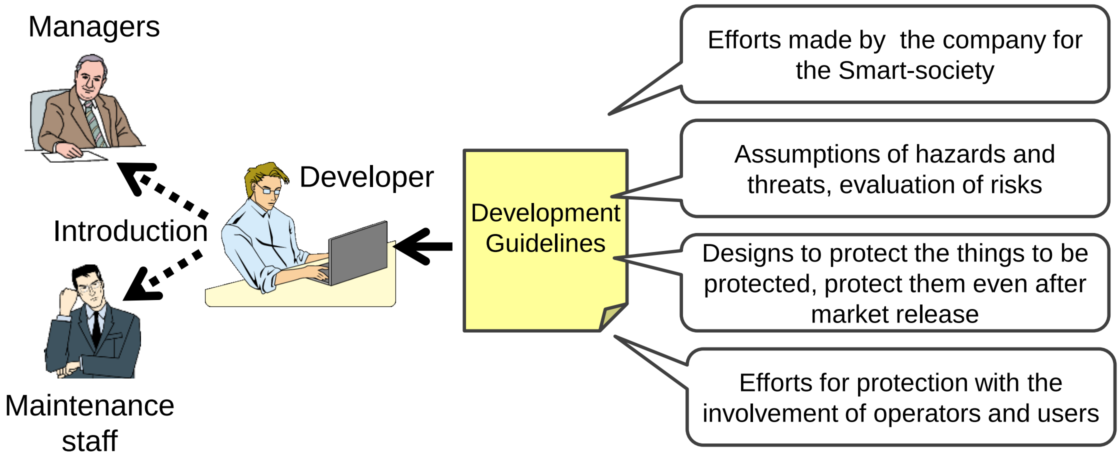

Managers
Developer
Introduction
Maintenance staff
Development Guidelines
Efforts made by the company for the Smart-society
Assumptions of hazards and threats, evaluation of risks
Designs to protect the things to be protected, protect them even after market release
Efforts for protection with the involvement of operators and users

Figure 1-13 Image of the Development Guidelines

(2) How to use the Development Guidelines

In the formulation of the Development Guidelines, the concepts of IoT and SoS described in 1.1 were taken into consideration. That is, the society in which the devices and systems of different industries collaborate with each other to achieve new purposes and functions is covered. Therefore, broad descriptions are presented, from the points of individual companies' efforts to common points that contribute to industrial collaboration, with reference to the status of Safety/Security efforts and precedent cases of each industry.

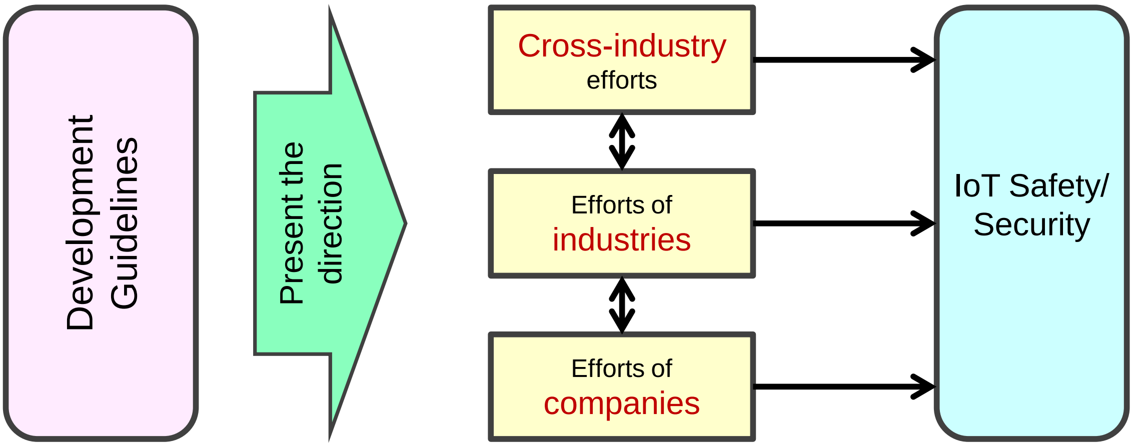


Figure 1-14 Coverage of the Development Guidelines

In addition, a checklist is given as an appendix to enable companies to verify the status of their current Safety/Security efforts and compliance with the guidelines.

In order to utilize the Development Guidelines effectively the following are assumed:

- Each point of each guideline is considered.
- Implementation of measures is to be determined by relevant parties. When implementing measures, example measures of each guideline can be used as a good reference.

For industries in which security standards, etc., are already established, the guidelines can be used as a reference when collaborating with devices and systems of other sectors.

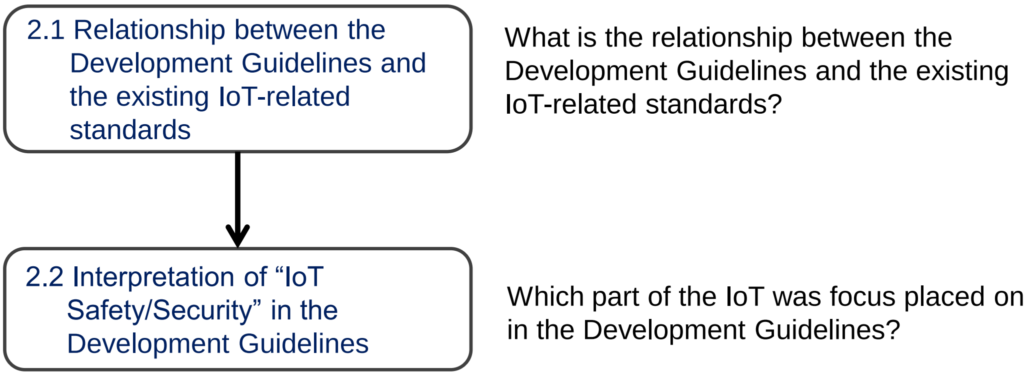
The concrete utilizing the Development Guidelines assumes the following:

- Use the guidelines as a checklist when developing IoT products or systems.
- Customize the items in the guidelines according to the actual conditions of companies, organizations, and industries when considering them.
- Use the guidelines not only for internal development but also for verifying the requirements when outsourcing.
- Use the check results as the evidence of activities.

We expect that, through utilization of the Development Guidelines, efforts for IoT Safety/Security in each industry and collaboration between different industries will advance, and the Safety/Security of the Smart-society will be achieved.

Chapter 2
Coverage of the Development Guidelines

While new devices and systems are being added to the IoT every day, those used for 10 or more years, including automobiles and home electrical appliances, also exist. In addition, the scale of the IoT is extremely large, spanning across the entire society, and its composition changes from day to day. All these make the identification of the whole context difficult. As such, this chapter explains which part of the "Smart-society" was focused on and the approach used. Figure 2-1 shows the flow of this chapter.


2.1 Relationship between the Development Guidelines and the existing IoT-related standards
2.2 Interpretation of "IoT Safety/Security" in the Development Guidelines

What is the relationship between the Development Guidelines and the existing IoT-related standards?

Which part of the IoT was focus placed on in the Development Guidelines?

Figure 2-1 Flow of this chapter

2.1 Relationship between the Development Guidelines and the existing IoT-related standards

IoT standards have been developed by various organizations, and can be classified into "common/universal standards" that are commonly used across industries/sectors and "industrial/specific standards" that apply to specific industries/sectors. The former includes IEEE, ISO/IEC, NIST and oneM2M standards, and the latter includes Industrie4.0 and IIC standards.

Table 2-1 Major universal/common international IoT standards and industrial IoT standards

	Standard/ organization	Outline	Main contributing member, etc.
Common/universal standard	IEEE P2413	A project for discussing cross-domain platforms in the IoT	-
	ISO/IEC 30141	A reference architecture discussed by WG10, which succeeded JTC1 SWG5	-
	NIST CPS PWG	Public WG for discussing CPS framework	-
	oneM2M	A collaborative project among 7 major standardization organizations. Horizontal integration of conventional vertically integrated M2M services using common PF	Approximately 200 industrial organizations, including Continua, HGI, and OMA
Representative industrial/specific	Industrie 4.0	Led by the German government as an innovation policy in the manufacturing industry	Siemens, Bosch, SAP, etc.
	IIC	Focused on energy, medical, manufacturing, transportation, and public administration	Approximately 150 companies, including GE, AT&T, IBM, Cisco, and Intel
	OCF	Standards for interoperability between various devices at home and in companies	Intel, Samsung Electronics, Cisco, MS, Qualcomm, LG, etc.
	HomeKit	Standards for connecting iOS with other devices	Approximately 20 companies, including Apple

Because the matters related to Safety/Security in "industrial/specific standards" reflect the characteristics of the industry, they may not easily be used as a reference for other industries. In contrast, matters related to Safety/Security in "common/universal standards" are also described in the common/universal level and are not sufficiently practical.

These matters are therefore compiled at a practical level in the Development Guidelines based on the examples of actual risks in each industry while enabling their use in a common and cross-sectional manner in each industry. Figure 2-2 shows the image.

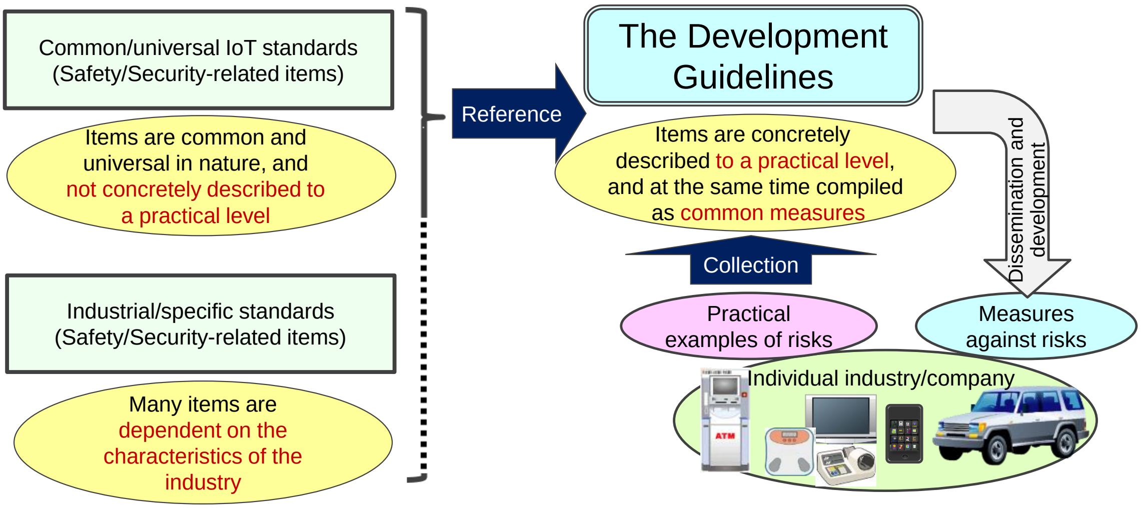

Common/universal IoT standards (Safety/Security-related items)
Items are common and universal in nature, and not concretely described to a practical level
Industrial/specific standards (Safety/Security-related items)
Many items are dependent on the characteristics of the industry
Reference
The Development Guidelines
Items are concretely described to a practical level, and at the same time compiled as common measures
Dissemination and development
Collection
Practical examples of risks
Measures against risks
Individual industry/company
ATM

Figure 2-2 Position of the Development Guidelines

2.2 Interpretation of “IoT Safety/Security” in the Development Guidelines

2.2.1 Classification by “IoT component” and “connection”

In many cases, Safety/Security-related design and validation are performed on the basis of basic configurations of devices and systems. As described in 1.1.1, however, the IoT configuration changes from moment to moment with the IoT themselves being connected to and disconnected from each other. This requires review and re-validation of Safety/Security designs on a daily basis, but it is not realistic.

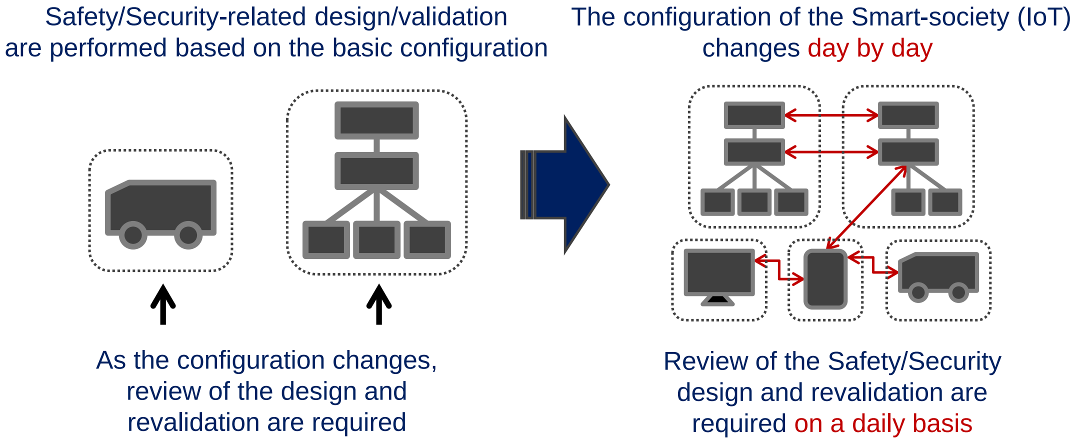

Safety/Security-related design/validation are performed based on the basic configuration
The configuration of the Smart-society (IoT) changes day by day
As the configuration changes, review of the design and revalidation are required
Review of the Safety/Security design and revalidation are required on a daily basis

Figure 2-3 Safety/Security design and validation of ever-changing “Smart-society (IoT)”

In the Development Guidelines, the smallest units of SoS described in 1.1.1, i.e., devices and systems comprising the IoT that fulfill purposes and functions on their own, are called “IoT components,” and the IoT is defined as an entity composed of “IoT components” and “connections (networks, information communications, etc.).” Based on these definitions, measures to improve the Safety/Security of the entire IoT through Safety/Security design and validation of “IoT components” are discussed here.

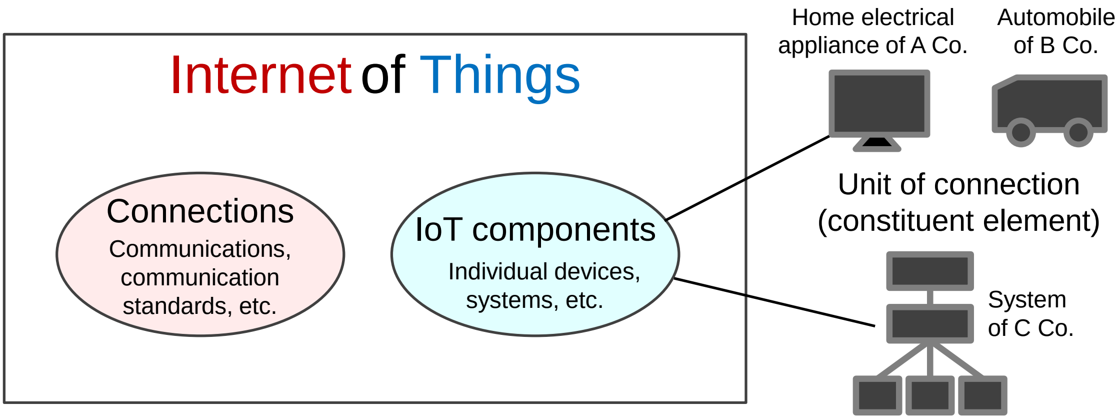

Internet of Things
Connections
Communications, communication standards, etc.
IoT components
Individual devices, systems, etc.
Home electrical appliance of A Co.
Automobile of B Co.
Unit of connection (constituent element)
System of C Co.

Figure 2-4 The IoT composed of “IoT components” and “connections”

2.2.2 Interpretation of Safety/Security of "IoT components"

Safety/Security design and validation of individual devices and systems (IoT components), including home electrical appliances, automobiles, and energy-saving services, are performed by manufacturers and service providers. In addition, performing designs/validations to enable the maintenance of Safety/Security of IoT components even when they are connected is expected to improve the Safety/Security of the entire IoT even when IoT components are combined for use by integrators and users. In such cases, informing the integrators/users of the design content and conditions in an easy-to-understand manner is also necessary.

Therefore, the designs for maintaining Safety/Security even when IoT components are connected and the guidelines for informing the relevant parties of the information on the design content, restrictions, etc., are described in the Development Guidelines.

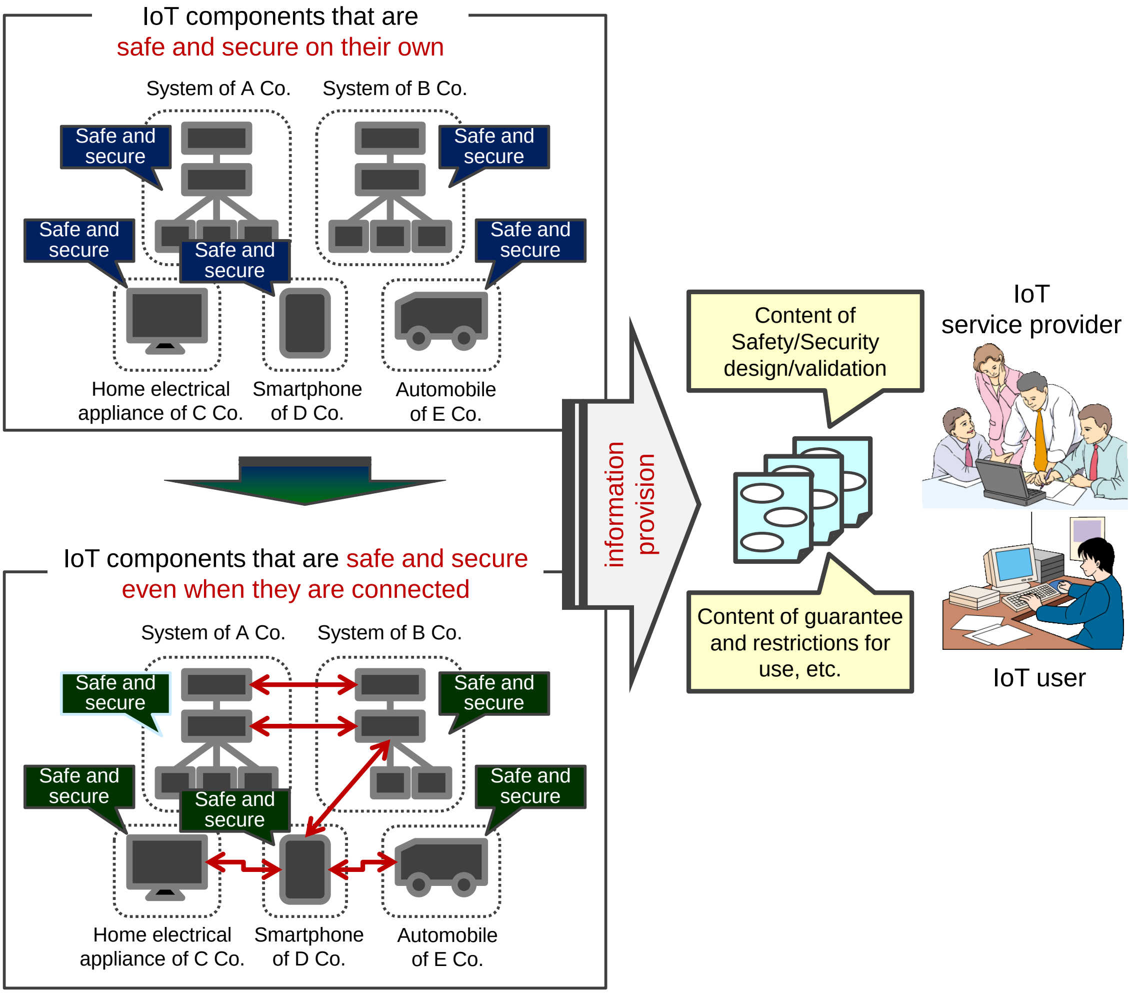


Figure 2-5 Safety/Security of IoT components

2.2.3 Dual nature of the Safety/Security of "IoT components"

In order to improve the Safety/Security of IoT components, not only the designs to protect the components themselves but also the protecting of other IoT components connected to them is important.

The IoT is also assumed to contain low-functionality/low-cost IoT components and older-generation IoT components for which Safety/Security design is difficult to perform. In such cases, protecting them by blocking attacks by other IoT components is necessary. In the case of failure or virus infection, not allowing abnormal operations in one device to spread to other devices that are connected, etc., is also required.

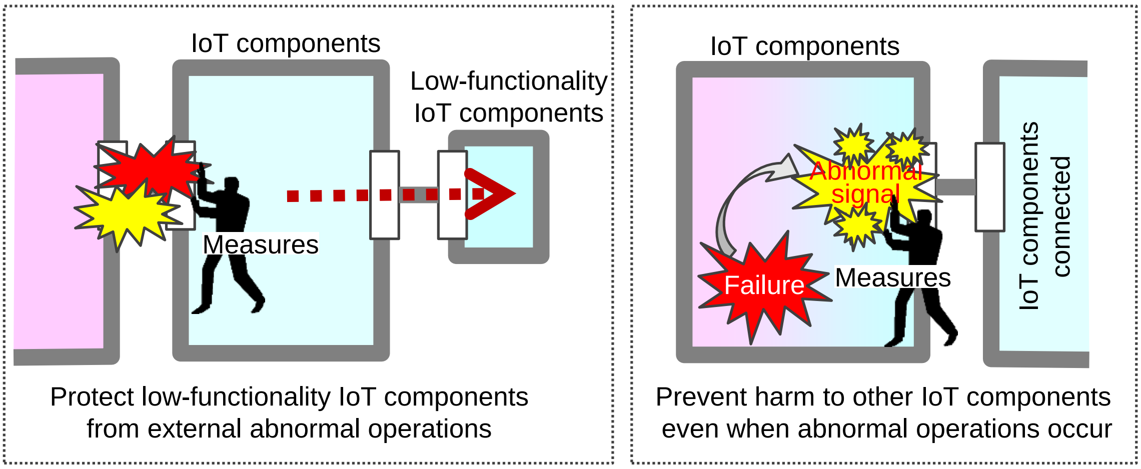

IoT components
Low-functionality IoT components
Measures
Protect low-functionality IoT components from external abnormal operations
IoT components
Abnormal signal
Failure
Measures
IoT components connected
Prevent harm to other IoT components even when abnormal operations occur

Figure 2-6 Image of achieving the Safety/Security of other IoT components

As described above, in addition to the designs to protect IoT components themselves, the designs to protect other devices and systems connected to them also need to be discussed in the Safety/Security design of IoT components.

2.2.4 Interpretation of Safety/Security of “connections”

Safety/Security of IoT “connections” includes communication security, communication stability, etc. These are discussed in international standards listed in Table 2-1, and referring to them helps to achieve Safety/Security measures that can be internationally collaborative.

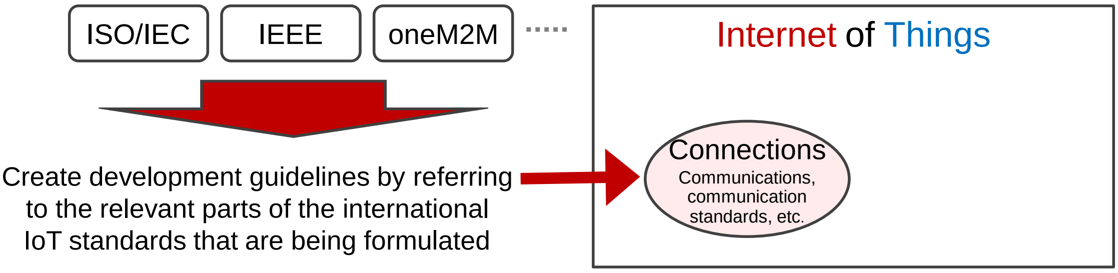
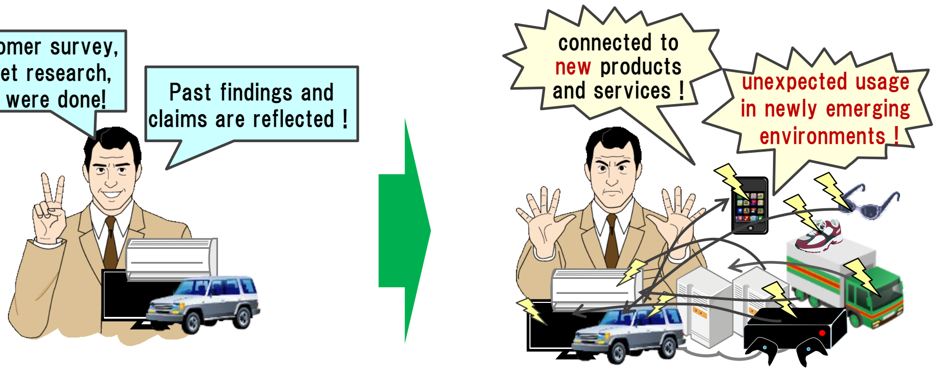

ISO/IEC
IEEE
oneM2M
·····
Create development guidelines by referring to the relevant parts of the international IoT standards that are being formulated
Internet of Things
Connections
Communications, communication standards, etc.

Figure 2-7 Policies for discussing “connections”

-COLUMN- "Quality in Use" and Safety/Security in the Smart-society

SQuaRE (ISO/IEC 25000 series), which is the international standard for "Systems and software Quality Requirements and Evaluation", specifies not only "Product Quality" of the product itself but also the "Quality in Use" when used by real users. The "Quality in Use" includes characteristics such as satisfaction level of various users in various environments and avoidance of risks. Generally companies design products considering the "Quality in Use". However, in the "Smart-society", there are possibilities of using products in unexpected ways in newly emerging environments, therefore it is not easy to maintain user satisfaction and to avoid risks over a long period of time.

Developed considering "quality in use" well ! .... But in the Smart-society, full of "unexpected usage"!


Customer survey, market research, etc. were done!
Past findings and claims are reflected !
connected to new products and services !
unexpected usage in newly emerging environments !

In order to maintain Safety/Security in the "Smart-society", the user-centric design should be realized to minimize risks due to users' environments by involving users from the planning and design stage. In addition, it is necessary to recognize r and analyze the usage status and environment of the products on the market, and also to add functions and to update software for Safety/Security. Furthermore, it is necessary to implement into products not only the countermeasures against technical risks but also the mechanism that makes users intuitively know what is connected and what happens by their operation or shows users the actual result of their operation so as to make them feel safe.

It is necessary to consider the "Quality in Use in the Smart-society" in design and operation processes as described above.

IPA established the "Quality in Use WG" [5] in September 2016 and compiled the viewpoint of approach to the "Quality in Use in the Smart-society" into the WG report [6]. Also, based on the WG report, the development guideline are revised and this second edition is published.

Chapter 3

Assumption of risks of the Smart-society

In order to formulate development guidelines for achieving the Safety/Security of the extremely large and ever-changing IoT, assuming the underlying IoT risks of diverse nature with as varied characteristics as possible is desirable. This chapter explains what viewpoints were used to organize the IoT and what steps were taken to assume the risks in formulating the Development Guideline. Figure 3-1 shows the flow of this chapter.

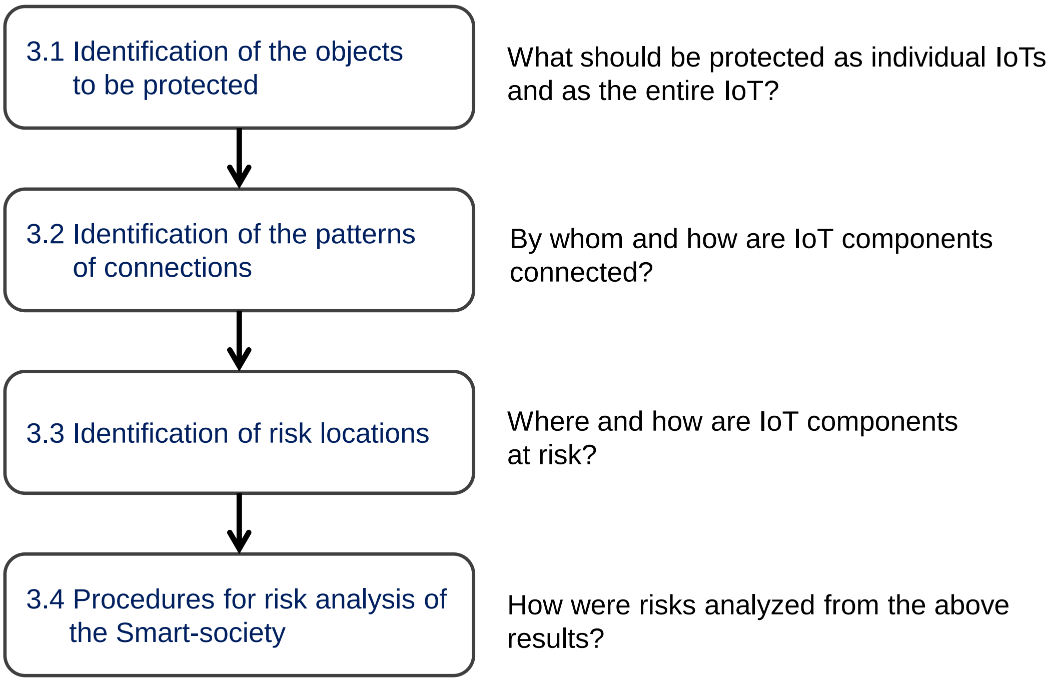

3.1 Identification of the objects to be protected
What should be protected as individual IoTs and as the entire IoT?
3.2 Identification of the patterns of connections
By whom and how are IoT components connected?
3.3 Identification of risk locations
Where and how are IoT components at risk?
3.4 Procedures for risk analysis of the Smart-society
How were risks analyzed from the above results?

Figure 3-1 Flow of this chapter

3.1 Identification of objects to be protected

In information systems, the “objects to be protected” generally include “functions” and “information.” In the case of IoT components, however, items of high value, such as automobiles and construction machinery, and items containing goods or cash, such as vending machines and ATMs, are also included. In addition, some home electrical appliances, medical devices, wearable devices, and machine tools can harm people's health and property by malfunctioning, and therefore the scope of the objects to be protected needs to be extended. Figure 3-2 shows examples of the objects to be protected in IoT components, organized by the IPA.

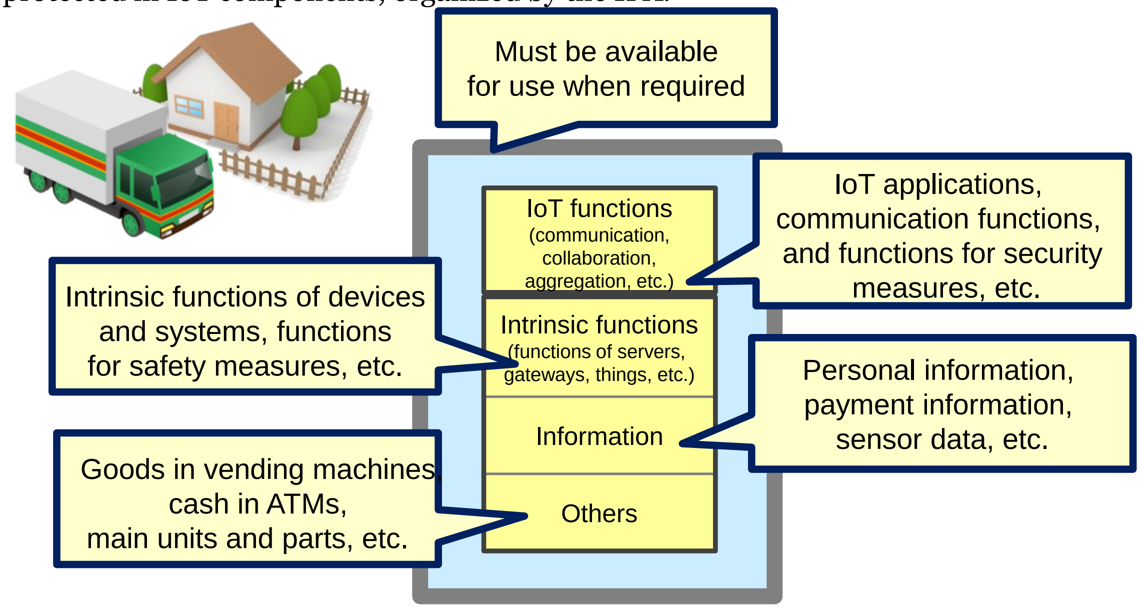

Must be available
for use when required
IoT functions
(communication, collaboration, aggregation, etc.)
IoT applications, communication functions, and functions for security measures, etc.
Intrinsic functions of devices and systems, functions for safety measures, etc.
Intrinsic functions
(functions of servers, gateways, things, etc.)
Information
Personal information, payment information, sensor data, etc.
Goods in vending machines, cash in ATMs, main units and parts, etc.
Others

Figure 3-2 Examples of the objects to be protected in IoT components

The meanings of the ”objects to be protected” in the figure are as given in Table 3-1. Because the IoT is a society in which various “things” are equipped with communication functions and connected to networks, it is organized by classifying the functions of “things” into “intrinsic functions” and “IoT functions” for communication, etc.

Table 3-1 Meanings of the “objects to be protected”

Objects to be protected	Meaning of term	Example of risk
IoT functions	Functions of devices and systems to be connected with IoT.	Unauthorized access, spoofing, virus infection, etc., through the IoT.
Intrinsic functions	Intrinsic functions of “things (home electrical appliances and sensors)”, safety measure functions, etc.	Attacks against safety measure functions to disable protection from damage in the case of failure.
Information	Users’ personal information, collected information, setting information of various functions, etc.	Malfunctions induced by setting change, leakage of personal information, etc.
Others	Physical values contained in IoT components.	Theft of cash, goods, main units/parts, etc.

3.2 Identification of the patterns of connections

Not only manufacturers of devices and systems but also IoT service providers and advanced users often build the IoT by connecting devices and services of various manufacturers. In some cases, malicious third parties connect devices to mount attacks such as installing viruses. In addition, the methods of connections vary: wired/wireless and fixed/dynamic (connections are made when used).

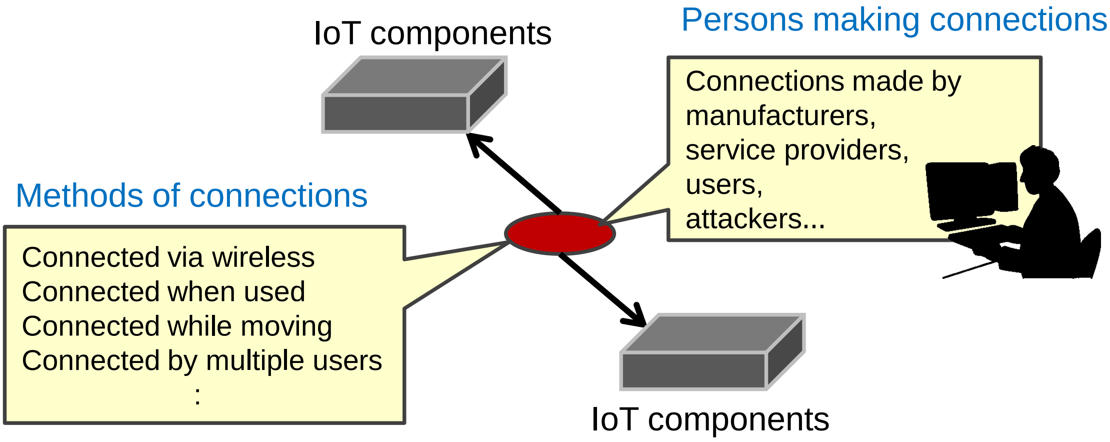

IoT components
Persons making connections
Connections made by manufacturers, service providers, users, attackers...
Methods of connections
Connected via wireless
Connected when used
Connected while moving
Connected by multiple users
:
IoT components

Figure 3-3 Interpretation (image) of connections of IoT components

The following table shows examples of the patterns of connections assumed by the IPA. In some cases, users connect devices and systems to the IoT themselves, and the methods of connections also vary. Maintaining IoT Safety/Security is therefore considered difficult.

Table 3-2 Examples of the patterns of connections

Pattern of connections		Outline
Person making connections	Manufacturer	Connections assumed by the manufacturer in the design phase.
	IoT service provider	Devices and systems are connected to build IoT services. Connections not assumed by manufacturers can be made as a result of relay systems being developed, etc.
	User	Devices and systems are combined to make connections. There may be connections not assumed by manufacturers, including privately imported devices, self-build smartphone apps, etc., being connected.
	Attacker	Mobile devices, etc., are connected for the purpose of making attacks.
Method of connections	Direct/indirect	Indirect connections indicate connections that are made through gateways or aggregation devices.
	Wired/wireless	There can be various wireless connections, including mobile phone networks, Wi-Fi, Wi-SUN, etc.
	Fixed/dynamic	Dynamic connections indicate connections that are made when required, including connections made while moving.
	Dedicated/ shared	Shared connections indicate scenarios in which multiple users use a single device.
	Combined	Combinations of the above.

3.3 Identification of risk locations

The threat and hazards to the “objects to be protected” in IoT components identified in the previous section are identified, and the locations where they may occur are also identified here. Figure 3-4 shows the image of locations where threats and hazards assumed by the IPA may occur, and Figure 3-5 shows examples of the threats and hazards assumed.

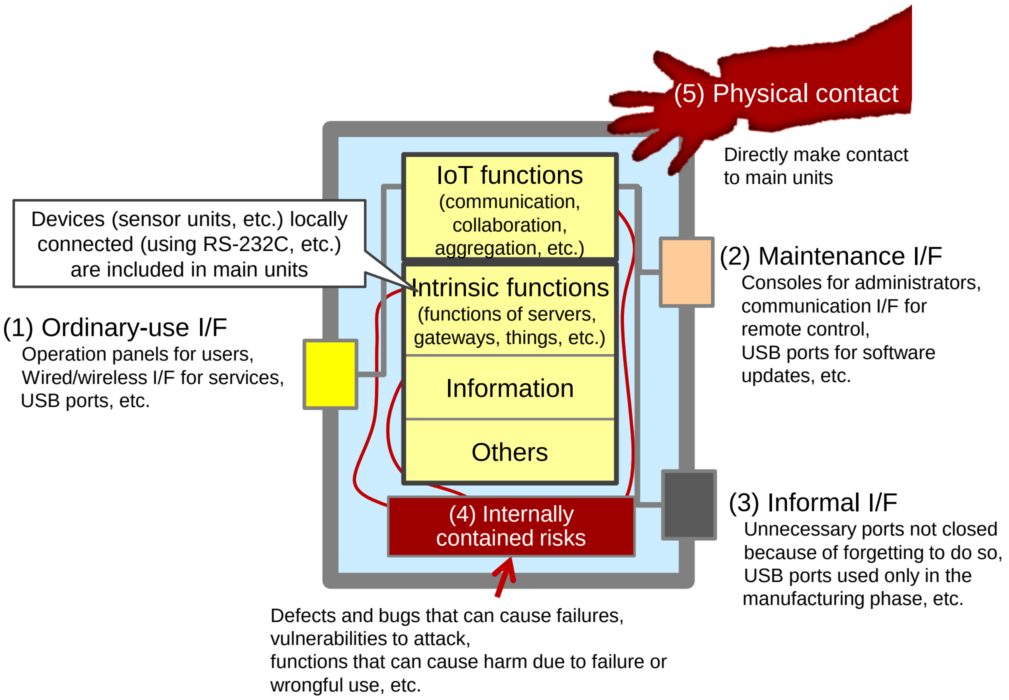

(5) Physical contact
Directly make contact to main units
IoT functions (communication, collaboration, aggregation, etc.)
Intrinsic functions (functions of servers, gateways, things, etc.)
Information
Others
(4) Internally contained risks
Devices (sensor units, etc.) locally connected (using RS-232C, etc.) are included in main units
(1) Ordinary-use I/F
Operation panels for users, Wired/wireless I/F for services, USB ports, etc.
(2) Maintenance I/F
Consoles for administrators, communication I/F for remote control, USB ports for software updates, etc.
(3) Informal I/F
Unnecessary ports not closed because of forgetting to do so, USB ports used only in the manufacturing phase, etc.
Defects and bugs that can cause failures, vulnerabilities to attack, functions that can cause harm due to failure or wrongful use, etc.

Figure 3-4 Examples of risk locations of IoT components

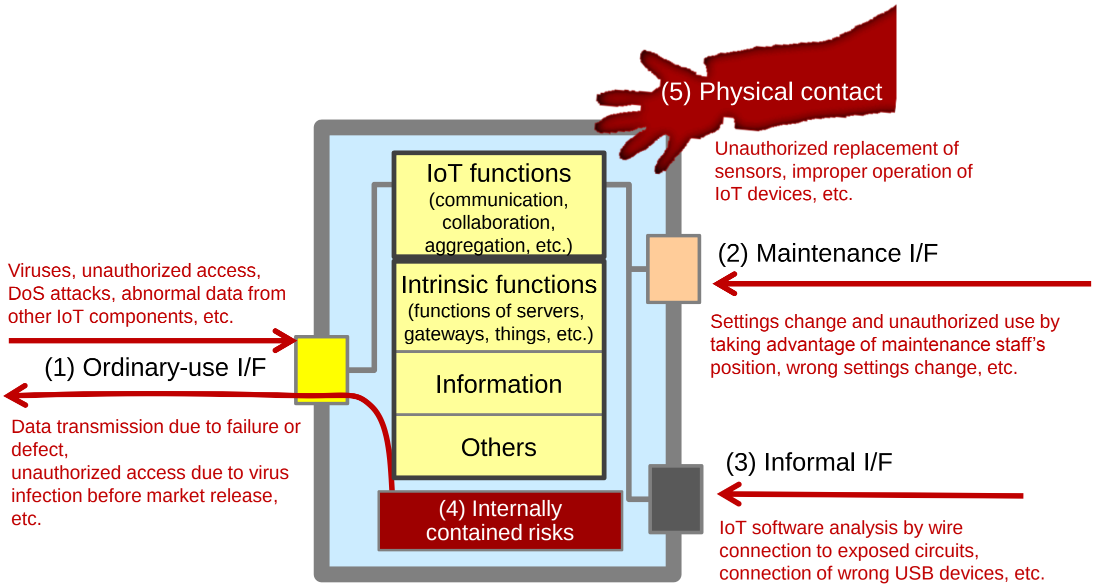

(5) Physical contact
Unauthorized replacement of sensors, improper operation of IoT devices, etc.
IoT functions (communication, collaboration, aggregation, etc.)
Intrinsic functions (functions of servers, gateways, things, etc.)
Information
Others
(4) Internally contained risks
Viruses, unauthorized access, DoS attacks, abnormal data from other IoT components, etc.
(1) Ordinary-use I/F
Data transmission due to failure or defect, unauthorized access due to virus infection before market release, etc.
(2) Maintenance I/F
Settings change and unauthorized use by taking advantage of maintenance staff’s position, wrong settings change, etc.
(3) Informal I/F
IoT software analysis by wire connection to exposed circuits, connection of wrong USB devices, etc.

Figure 3-5 Examples of threats and hazards to IoT components

Based on the discussions in this section, concrete risks are identified in the next section.

3.4 Procedures for risk analysis of the Smart-society

In many cases, the ISO/IEC Guide 51 and ISO 31000 are generally referred to in the risk analysis of safety and security, respectively. For security, information assets to be protected are identified in advance. In the Development Guidelines, after identifying the "objects to be protected" as described in 3.1, guidelines are formulated as risk analysis and measures, using ISO/IEC Guide 51 and ISO 31000 as reference. Figure 3-6 shows the image of the procedures. In the figure, "hazards" refer to potential factors related to safety that can cause damage to the health of people, property, functions information, etc., and "threats" refer to those related to security.

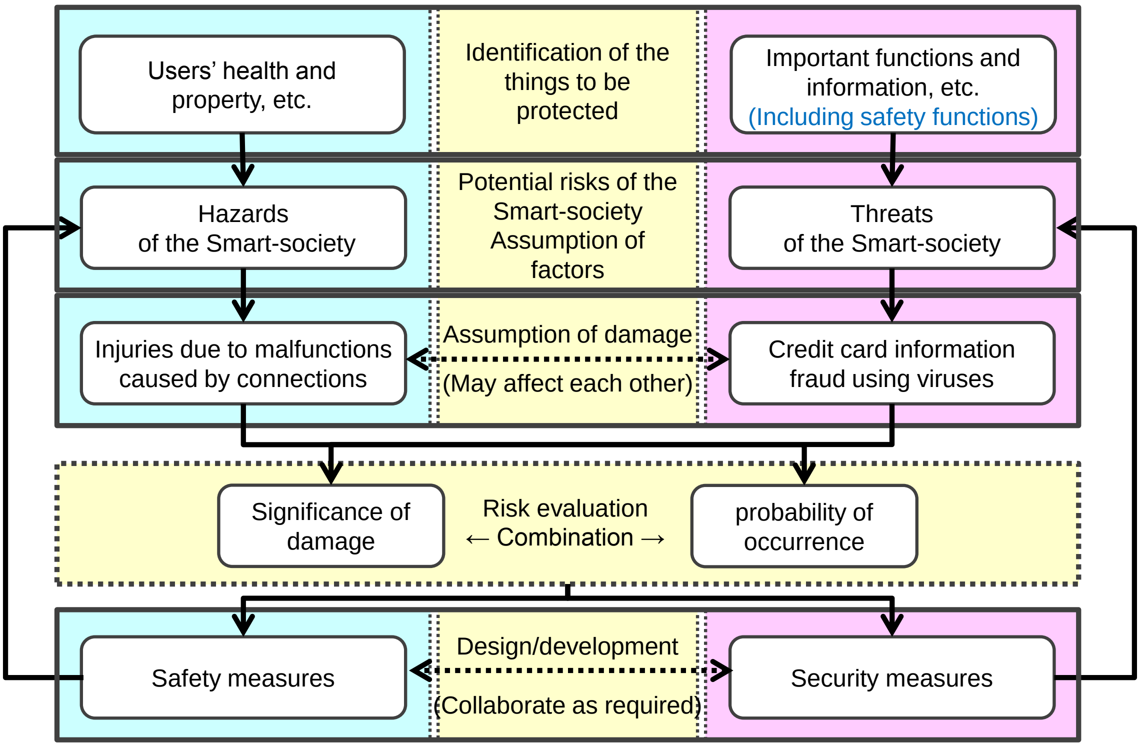

Users' health and property, etc.
Identification of the things to be protected
Important functions and information, etc.
(Including safety functions)
Hazards of the Smart-society
Potential risks of the Smart-society Assumption of factors
Threats of the Smart-society
Injuries due to malfunctions caused by connections
Assumption of damage
(May affect each other)
Credit card information fraud using viruses
Significance of damage
Risk evaluation
← Combination →
probability of occurrence
Safety measures
Design/development
(Collaborate as required)
Security measures

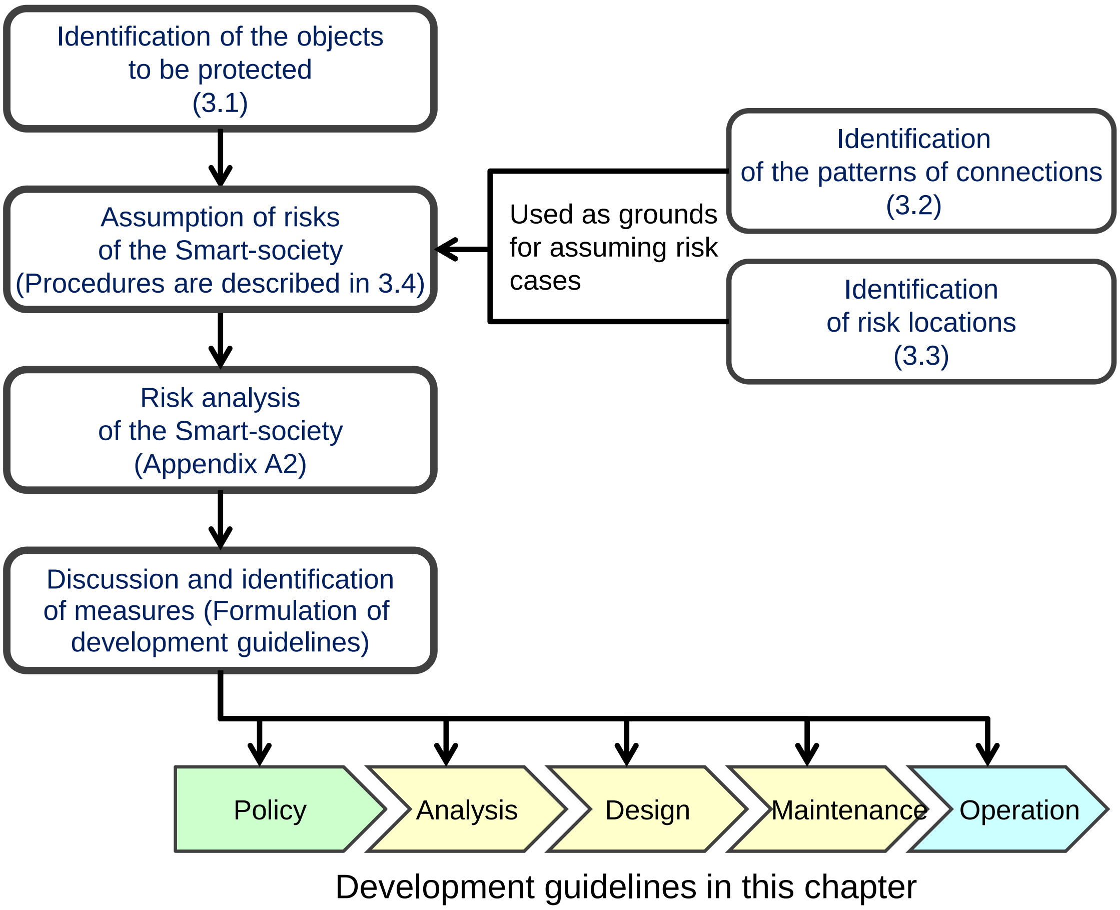
Figure 3-6 Identification of hazards and threats, risk analysis and considering measures for the Smart-society

In the assumption of risks, the patterns of connections described in 3.2 and the risk locations described in 3.3 are selected in a varied manner for the measures of risks with as varied characteristics as possible (see Appendix A2 for details).

Chapter 4

Development Guidelines for the Smart-S ociety

Measures against the risks of the Smart-society were discussed using the procedures described in the previous chapter based on the comments of engineers in relevant industries and academic experts. In addition, the results were organized under the phases of "policy," "analysis," "design," "maintenance," and "operation," and compiled as development guidelines. Figure 4-1 shows the flow of the discussion.


Identification of the objects to be protected (3.1)
Assumption of risks of the Smart-society (Procedures are described in 3.4)
Risk analysis of the Smart-society (Appendix A2)
Discussion and identification of measures (Formulation of development guidelines)
Used as grounds for assuming risk cases
Identification of the patterns of connections (3.2)
Identification of risk locations (3.3)
Policy
Analysis
Design
Maintenance
Operation
Development guidelines in this chapter

(Note) In the development guidelines in the above figure, the green section indicates the content to be discussed by managers, the yellow sections by developers, and the blue section by developers for operations.

Figure 4-1 Flow of the formulation of the Development Guidelines

Table 4-1 shows the list of development guidelines. Outlines of the respective proposed development guidelines are also described in later sections.

Table 4-1 List of development guidelines that should be discussed

Major item		Guidelines	
Policy	4.1 Making corporate efforts for the Safety/Security of the Smart-society	Guideline 1	Formulating the basic policies for Safety/Security
		Guideline 2	Reviewing systems and human resources for Safety/Security
		Guideline 3	Preparing for internal frauds and mistakes
Analysis	4.2 Understanding the risks of the Smart-society	Guideline 4	Identifying the objects to be protected
		Guideline 5	Assuming the risks caused by connections
		Guideline 6	Assuming the risks spread through connections
		Guideline 7	Understanding physical security risks
Design	4.3 Considering the designs to protect the objects to be protected	Guideline 8	Designing to enable both individual and total protection
		Guideline 9	Designing so as not to cause trouble in other connected entities
		Guideline 10	Ensuring consistency between the designs of Safety/Security
		Guideline 11	Designing to ensure Safety/Security even when connected to unspecified entities
		Guideline 12	Verifying/validating the designs of Safety/Security
Maintenance	4.4 Considering the designs to ensure protection even after market release	Guideline 13	Implementing the functions to identify and record own status
		Guideline 14	Implementing the functions to maintain Safety/Security even after the passage of time
Operation	4.5 Protecting with relevant parties	Guideline 15	Identifying IoT risks and providing information after market release
		Guideline 16	Informing relevant business operators of the procedures to be followed after-market release
		Guideline 17	Making the risks caused by connections known to general users

4.1 Making corporate efforts for the Safety/Security of the Smart-society

In the Smart-society, malfunctions and unauthorized operations occurring in devices and systems, including automobiles, home electrical appliances, health care devices, ATMs, and payment devices, can cause harm to users' health and property, etc. In addition, the impacts can spread extensively through networks. Because the Safety/Security of the Smart-society is an issue concerning the existence of the companies that develop devices and systems, not only developers but also managers need to understand it.

This chapter therefore explains three guidelines for the Safety/Security of the Smart-society to be addressed by the company.

[Guideline 1] Formulating the basic policies for Safety/Security

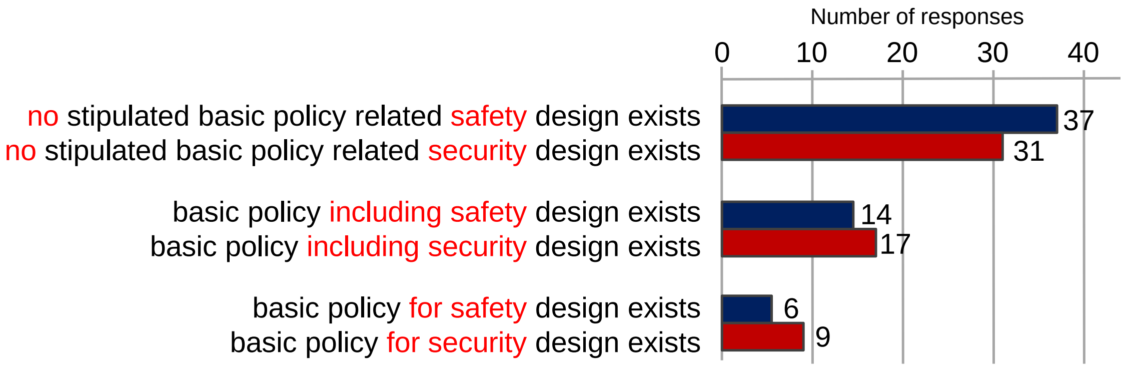
(1) Points

(i) Managers shall formulate the basic policies for the Safety/Security of the Smart-society, make them known within the company, continuously evaluate their achievement status, and review them as required.

(2) Description

In the Smart-society, the risks are varied and may spread to have impacts on the existence of the company. In addition, measures against such risks entail costs, and thus it is assumed that in many cases decisions cannot be made at the development site. Managers are therefore required to take the initiative in establishing the response policies.

According to a questionnaire survey conducted by the IPA targeting companies assumed to have been taking the lead in making efforts for measures against risks, however, less than half of the companies had formulated the basic policies for Safety/Security. Formulating and making known the basic policies for Safety/Security is therefore an urgent issue.



Source: Results of the questionnaire survey on the actual conditions of safety/security design conducted by IPA

Figure 4-2 Status of formulation of the basic policies for safety and security

In addition, to improve the Safety/Security of the Smart-society, it is important to consider the "Quality in Use" for avoiding risks caused by the change of the usage environment or the way to use. It is also necessary to embed the “Quality in Use” into the basic policies.

Toward the Smart-society, it is necessary to formulate basic policies on Safety/Security, make them known within the company, evaluate the achievement status, and review them as required.

(3) Example measures

Formulate basic policies for the Safety/Security of the Smart-society with the involvement of management.

(i) Matters to be considered toward the Safety/Security of the Smart-society (examples)

1) Examples of items to be described by the company regardless of IoT (the content depends on the business type/category)

- Coverage of Safety/Security (users' lives and property, etc.) and outlines of measures
- Establishment of Safety/Security management systems, and development of and compliance with relevant rules and regulations
- Suitable personal/organizational/technical measures and continued education
- Rapid identification of the causes and inhibition of damage when problems occur, and prevention of recurrence after that
- Compliance with laws and regulations, guidelines stipulated by the government, and other social norms
- Methods for making known within the company, continuous review and improvement, etc.

2)Matters required for the Smart-society (the content depends on the business type/category)

・Security measures from the management point of view

In "Cyber Security Management Guidelines [7]" by Ministry of Economy, Trade and Industry /IPA, three principles that managers should recognize are provided in order to protect companies against cyber-attacks.

･Efforts for Safety/Security from the planning/design phase (Safety/Security by Design)

There are many issues in the reactive implementation of Safety/Security measures in terms of costs and efficiency, and therefore efforts should be made at an early phase in the design process. Planning and designing should be done considering the “Quality in Use” for Safety/Security according to the results of monitoring and analyzing the usage status and environments of users.

･Support policies for the Smart-society

For the ever-changing Smart-society, specify the policies for maintaining the Safety/Security of released devices and systems, and the policies concerning the warranty period for Safety/Security, the restrictions for use, etc.

･Verification/validation policies for the Safety/Security of the Smart-society

Establish the verification/validation policies (including the product release requirements) for Safety/Security against external impacts and functions that can cause external impacts in the Smart-society.

･Policies for rapidly responding to accidents and incidents in the Smart-society

Establish the policies for rapidly responding to the accidents/incidents when they occur in the IoT, an infrastructure that supports life and business.

･Monitoring and reviewing

In the Smart-society, for which unexpected problems are assumed, while identifying the status of achieving the Safety/Security of companies’ devices and systems, collect the information on the latest risks and the methods for achieving Safety/Security, and review the policies through a PDCA (Plan-Do-Check-Act) cycle. Especially, it is necessary to review the plan/design from the “Quality in Use” point of view based on the analysis of the user survey, the feedbacks from users, etc.

[Guideline 2] Reviewing systems and human resources for Safety/Security

(1) Points

(i) Establish systems and environments for discussing the Safety/Security issues of the Smart-society in an integrated manner.
(ii) Secure/develop human resources (developers and maintenance staff) for that purpose.

(2) Description

In the Smart-society, unexpected problems can occur, and the impacts can spread extensively. It is therefore necessary to establish systems for performing emergency response, analyzing the causes, and taking drastic measures, and environments for verifying/validating the measures.

Figure 4-3 Necessity of emergency response to Safety/Security issues

Because the Smart-society is composed of the devices and systems of various companies, “collaboration of vendors” is also necessary to address the problems.
It is important to the system operations department to make a mechanism that elicits opinions from users, to collect exposed/potential trouble and incident examples of Smart-society and to work on the improvement and the prevention collaborating with planning/design departments. It is effective to involve users in the stage of planning/designing and to build a frameworks to introduce measures to avoid potential risks in the use cases into the development process.
In addition, the securing/developing human resources who can use their knowledge and skills to respond to the problems is also needed.

(3) Example measures

(i) Examples of systems and environments for Safety/Security

Collaborate the systems for discussing Safety/Security, and establish systems and environments that can deal with the issues of the Smart-society in an integrated manner. Examples are shown below:

1) Establishment/maintenance/improvement of product safety management systems

(organizational systems)

In “1.3 Organizational systems” of the “Handbook for Companies about Product Safety (June 2012)” [8] published by Ministry of Economy, Trade and Industry, one suggestion was that “business operators need to clarify the roles and authorities of the organizations within and outside the company, and continue to verify the state of the organizations from the point of view of establishing/
maintaining/improving product safety management systems in order for business operators to archive the targets of internal controls in relation to product safety.”.

In addition, Chapter 4 describes measures to prevent product accidents from occurring and to prevent damage from spreading through collaboration/cooperation with consumers, retailers, providers, etc., as “collaboration/cooperation with stakeholders.”

2) Establishment of CSIRT (Computer Security Incident Response Team)

CSIRT is a generic name for the organizations that respond to incidents and perform incident measure activities within the company, and a starter kit is published by a related organization (see Guideline 15).

3) Establishment/update of verification environments

Establishing/updating dedicated environments for verifying the effectiveness of risk measures is desirable. Because establishing the environments by individual companies entails costs, however, utilizing public verification systems is also effective.

(ii) Useful sources of information on human resources

1) Introduction to Safety & Security Design in Smart Society (IPA)

Toward the achievement of the Safety/Security of the Smart-society, accident and incident cases, safety and security design methods, methods for visualizing safety/security design quality that are effective in sharing information between relevant parties and explaining to users, etc., are described [9].

2) Reference documents on strengthening information security skills (IPA)

Guidebooks on human resource development have been published, including “Information Security Personnel Training Guide Utilizing IT Skill Index” and “Information Security Skill Improvement Handbook” [10].

3) Security Design Guide for loT Development (IPA)

Threat analysis and countermeasure considerations in security design for IoT are provided using the examples of a digital television, a health care apparatus, a smart house and a car [11].

4) "Quality in Use" for Smart-society (IPA)

Result of the examination about the "Quality in Use" of IoT products and services is published. This guide includes the point of view such as avoidance of the risks caused by users, receptiveness for users not to stop security functions, etc. [12].

5) Approaches for Embedded System Information Security (2010 Revised Edition) (IPA)

A guidebook on security measures for embedded systems. Assumptions of and measures against attacks to embedded systems that use IPv6, which is assumed to be used in the IoT, are added in the revised version [13].

6) Approaches for Vehicle Information Security −second edition- (IPA)

A security guidebook on embedded systems with particular focus on automobiles. In addition to examining precedent cases in the EU, risks are assumed and countermeasures are discussed by setting “IPA car” as a model. The second edition is published in March, 2017. [14].

7) Japan's Information Technology Engineers Examination (IPA)

The available examinations include Information Security Management Examination and Embedded Systems Specialist Examination (information security is included in the scope) [15]. RISS (Registered Information Security Specialist) was also started in spring of 2017 [16].

[Guideline 3] Preparing for internal fraud and mistakes

(1) Points

(i) Recognize the possible existence of internal fraud that can be a threat to the Safety/Security of the Smart-society, and discuss the measures to guard against it.
(ii) Discuss the measures to prevent mistakes by relevant parties and to protect Safety/Security even when mistakes are made.

(2) Description

There was an overseas case where a dissatisfied retired person remotely performed unauthorized operations of automobile management services to disable automobiles from starting, sound horns, etc. [17], and another overseas case where cash was withdrawn from an ATM by copying a physical key of the ATM managed by a bank, using it to open the maintenance door of the ATM, infecting the ATM with a virus, and then connecting a mobile device to the USB port of the ATM [18]. Measures against “internal fraud” by employees and retired persons who have extensive knowledge of the design and architecture of devices and systems that comprise services of the Smart-society and who can use access privileges and keys in an unauthorized manner are necessary.

Additionally, even in the absence of malicious intent, measures are needed against “mistakes,” such as the leakage of design information by opening files attached to targeted attack e-mails or misplacing the information taken outside the company.

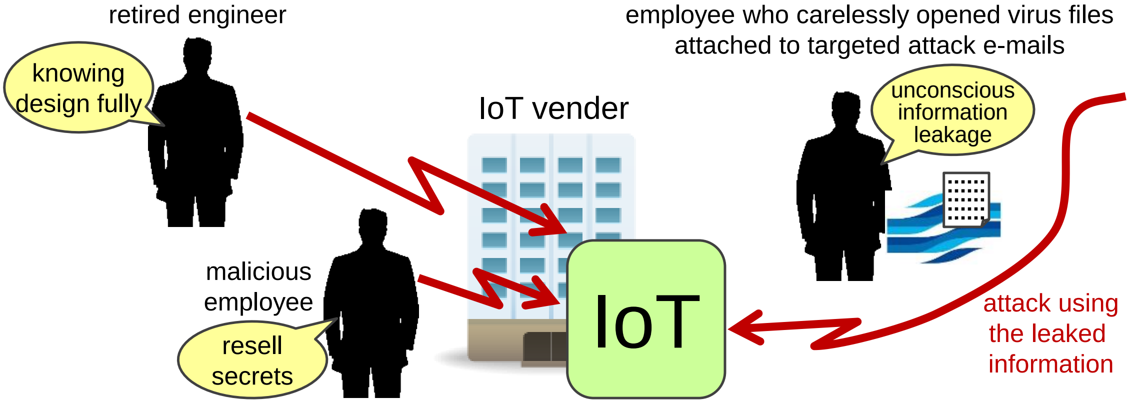

retired engineer
knowing design fully
employee who carelessly opened virus files attached to targeted attack e-mails
IoT vender
unconscious information leakage
malicious employee
resell secrets
IoT
attack using the leaked information

Figure 4-4 Impacts of internal fraud and mistakes

(3) Example measures

(i) Examples of measures against internal fraud

Because internal fraud in the Smart-society can significantly affect the devices and systems of other companies and users, understanding the causes and recognizing the necessity of countermeasures are necessary.

・According to an investigation conducted by the IPA, the main causes and objectives of committing internal fraud include obtaining money, creating advantageous conditions for career changes, and job dissatisfaction. In the investigation, the results of a questionnaire survey on the “conditions that motivate the committing of fraud” also included “receiving an unjust dismissal notice” and “making a career change to companies with favorable conditions” as top answers (Table 4-2). Depending on the situation of the individual company, correcting issues and promoting education within the company to prevent employees from committing fraud is necessary.

Table 4-2 Conditions that motivate a person to commit fraud (results of the questionnaire survey)

Classification	Rank	Content	Percentage*
Incentive/ pressure	1st	Receiving an unjust dismissal notice	30.0%
	2nd	Making a career change to companies with favorable conditions	10.2%
	3rd	Not satisfied with personnel evaluation within the company	8.2%
Environment/ opportunity	1st	Rules are frequently and repeatedly broken in the workplace	8.8%
	2nd	There is no penalty for breaking the rules and regulations of the company	8.7%
	3rd	The system is poorly managed, and I know that customer information can easily be taken outside	8.4%
Knowledge/ experience	1st	Although I am not an information system administrator, I can easily delete the evidence of unauthorized operations	9.8%
	2nd	I know how to take important information, such as customer information, outside without being noticed by anyone in the company	9.5%
	2nd	I have never received any warning or caution by anyone when I took important information, such as customer information, outside	9.5%

* The percentage of those who answered that they were motivated to commit fraud.
Source: Survey on incidents caused by fraudulent acts by insiders, IPA [19]

・IPA published the five basic principles concerning internal fraud in “Guidelines for Internal Fraud Prevention in the Organization” [20]. The Guidelines should be used as a reference as it contains a number of matters to be connected that commonly apply to the risks of internal fraud against devices and systems.

Table 4-3 Five basic principles concerning internal fraud

Five basic principles	Outline
Make offenses difficult (make them difficult to commit)	Make the criminal acts difficult by strengthening the countermeasures
Increase the risk of being caught (will be found out if offenses are committed)	Increase the risk of being caught by strengthening management and monitoring
Reduce the rewards of offenses (make them not worth the risk)	Prevent offenses by hiding/removing the targets and/or eliminating the benefits
Reduce the motivation for the offenses (inhibit the willingness)	Suppress offenses by inhibiting the willingness to commit offenses
Deny the justifications for offenses (disallow excuses)	Eliminate the justifications made by the offenders for the acts they commit

Source: “The Guidelines for Internal Fraud Prevention in the Organization,” IPA

(ii) Examples of measures against mistakes and offenses by employees

In recent years, attacks have increased involving the spoofing of staffs of highly reliable organizations, such as relevant parties and government-affiliated organizations and the sending of e-mails containing viruses in their attachments (targeted attack e-mails), to certain companies and organizations. There are viruses that cause not only the leakage of information but also the withdrawal of money from ATMs by infecting core banking systems to make them perform unauthorized operations.

opening attached files causes virus infection
A mail from IPA? ...a document of security measures...
government organization staff

Figure 4-5 Actual case of targeted attack e-mail

Making the prevalence of such attacks known not only to the development and maintenance sites of devices and systems to be connected but also within the entire company is important. However, targeted attack e-mails are very cleverly crafted, resulting in the attachments containing viruses being carelessly opened in many cases. Measures to prevent information leakage due to viruses by appropriately designing networks within the company are also necessary.

The IPA published “System Design Guide for Targeted Attack E-mails Countermeasures” for minimizing the damage by preventing virus operations after the virus infection [21].

4.2 Understanding the risks of the Smart-society

In order to achieve the Safety/Security of the Smart-society, identifying the objects to be protected and analyzing their risks are necessary, as described in Chapter 3. Particularly in the Smart-society, other devices connected through networks may also be affected, and unexpected problems may be caused by connections. For this reason, identification of the objects to be protected and assumption of the risks need to be performed again.

This chapter explains four guidelines to be addressed for understanding the risks of the Smart-society.

[Guideline 4] Identifying objects to be protected

(1) Points

(i) Identify the intrinsic functions, information, etc. to be protected from the point of view of the Safety/Security of the Smart-society.

(ii) The functions for connections (IoT functions) should also be identified to be protected for the Safety/Security of the intrinsic functions and information.

(2) Description

In addition to the functions specific to devices, such as the cooling and heating functions of air conditioners, conventional devices and systems are equipped with functions to protect the health and property of users even when accidents and malfunctions occur. In order to enable devices and systems to maintain Safety/Security as before, even after they are connected with remote servers and other home electrical appliances, these functions (intrinsic functions) need to be protected. In addition, information relating to the operations of devices and information generated by devices and systems also need to be protected to prevent leakage due to connections. It is also necessary to identify information to be protected such as sensor data or personal information collected by IoT components. Especially in the Smart-society, it is necessary to consider the privacy of users in passive information such as personal images taken by surveillance cameras or drive recorders.

Functions for connections (IoT functions) must also be protected to prevent them from becoming entry points for external attacks, and the impacts of malfunctions from externally spreading.

Therefore, as shown in Figure 3-6 in 3.4, identifying the intrinsic functions and IoT functions to be protected from the point of view of the Safety/Security of the Smart-society is required.

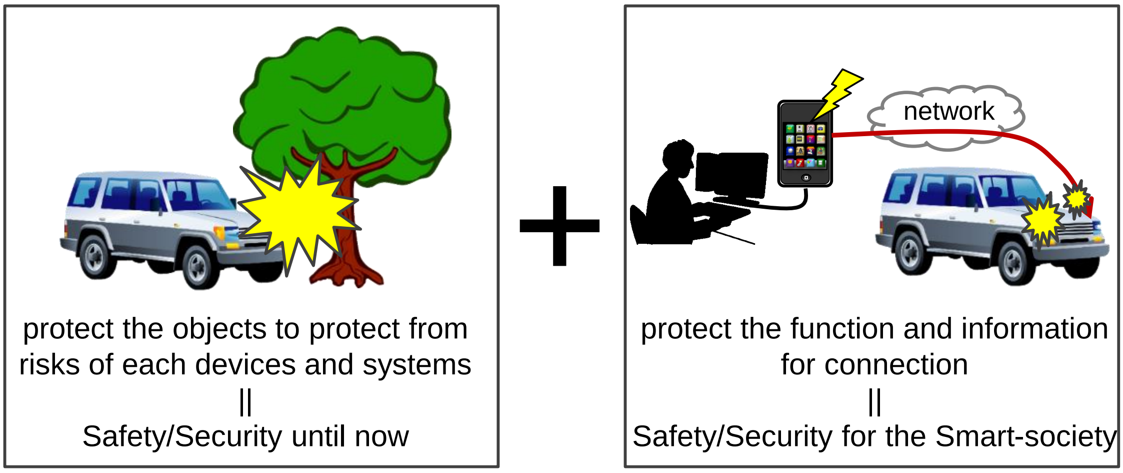

network
protect the objects to protect from risks of each devices and systems
||
Safety/Security until now
protect the function and information for connection
||
Safety/Security for the Smart-society

Figure 4-6 Safety/Security required in the Smart-society

(3) Example measures

(i) Identification of the intrinsic functions and information to be protected

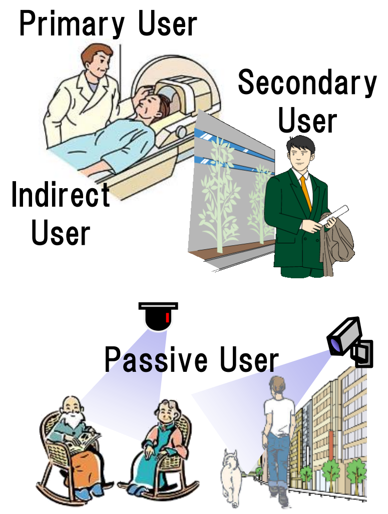
1) Identification of intrinsic functions

Identify the intrinsic functions of IoT components (functions such as “run,” “turn,” and “stop” for automobiles), information generated such as sensor data and logs, etc. Cases in which functions that take advantage of connections, such as remote operations, are added and cases in which information used by such functions are generated are also assumed, and therefore the identification must be carried out radically.

2) Identification of information

Identify the information, such as sensor data and personal information (including those related to privacy), collected by IoT components. Table 4 4 shows classification of users.

Classification of users in the Smart-society

Classification		Definition	Image
Direct user		Person who interacts with the product.	 Primary User Secondary User Indirect User Passive User
	Primary user	Person who interacts with the system to achieve the primary goals. E.g. Medical technologists who operates medical equipment.	
	Secondary user	Person who provides support. For example, content provider, system manager, security manager. E.g. Persons in charge of medical equipment maintenance.	
Indirect user		Person who receives output from a system, but does not interact with the system. E.g. Patients who are examined with medical equipment.	
Passive user		Person who is affected by a system regardless of their intention. E.g.1 An elderly person who is watched by the watching system. E.g.2 A passerby who appears in a surveillance camera.	

Source: "Guide of the quality in use for IoT", IPA

Especially in IoT, "passive user", whose personal information is collected regardless of their intention, should be considered. "Camera Image Utilization Guidebook ver1.0 [22] [23]" of the IoT Acceleration Consortium is useful to consider this issue.

Also identify software comprising the functions and its setting information as the objects to be protected because of the risks that they may be retrieved and used for devising attack methods or falsified to perform unauthorized operations.

Table 4-4 Examples of the information to be protected by embedded systems

Information asset	Description
Contents	Multimedia data, such as voices, images, videos, content usage histories , etc.
User information	Users' personal information (name, address, telephone number, birth date, credit card number, etc.), user authentication information, and usage/operation histories, etc.
Device information	Information on home electrical appliances (model, ID, serial ID, etc.), device authentication information, etc.
Software status information	Status information of software (operating status, network usage status, etc.)
Software setting information	Setting information of software (operation settings, network settings, privilege settings, versions, etc.), record of the setting change.
.Software	OS, middleware, applications, etc.
Design information, internal logics	Design information, such as specifications and designs, including the logics that may be retrieved through software analysis or electromagnetic waves generated during operation, etc.

Source: Prepared based on "Action Guide to Security of Embedded Systems", IPA

(ii) Identification of the IoT functions and information to be protected

Identify the IoT functions such as communication, collaboration, and aggregate functions and information that are added to make conventional devices and systems into IoT components. In particular, the setting information of IoT functions should be identified as the objects to be protected because they may be altered by IoT service providers.

In addition, identified "objects to be protected" should be prioritized as needed.

[Guideline 5] Assuming the risks caused by connections

(1) Points

(i) Even for devices and systems intended for closed networks, assume the risks on the basis that they are used as IoT components.

(ii) The risks that the connected entity is fake or hijacked should be assumed.

(iii) The risks during maintenance and risks due to the illegal use of maintenance tools should also be assumed.

(2) Description

There was an incident in 2004 where HDD recorders were used as springboards, and incidents in 2013 and 2015 where data stored on the multifunction printers of multiple manufacturers were open to public access over the Internet [24]. The fact that their use in environments accessible over the Internet was not assumed, and thus the initial passwords of the main units were not set when released and instructions to users to set the passwords were not enough were considered to be the cause of these incidents. There was also a case where factory systems that were operated isolated from the Internet were infected by viruses through a USB memory device brought in at the time of maintenance [25].

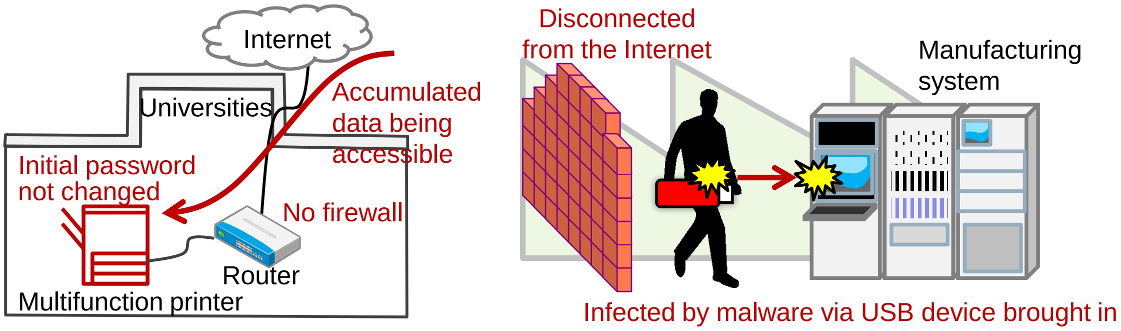

Internet
Universities
Accumulated data being accessible
Initial password not changed
No firewall
Router
Multifunction printer
Disconnected from the Internet
Manufacturing system
Infected by malware via USB device brought in

Figure 4-7 Examples of incidents due to the assumption that devices/systems are not connected to the Internet

Security measures for the main units were considered insufficient due to the assumption that the printers would be used in environments protected by firewalls, etc., for the former case, and due to the fact that the systems were isolated from the Internet for the latter cases. Regardless of the assumptions on the environments for use, risks need to be assumed on the basis that devices and systems equipped with communication functions are used as IoT components. In addition, as new IoT systems and services come out year by year, patterns of the connection of devices and systems and the usage increase exponentially. It complicates mutual relations of users and environments rapidly. Therefore the risks should be considered on users and environments as well.

Furthermore, there may be risks that an IoT component is connected to a malicious server by attacks to DNS or that even an authorized entity might become unreliable under an environment infected by viruses. Thus, it is necessary to consider them as well.

As for maintenance, tools created by extracting from the re-registration function of immobilizers were sold on the Internet and used for automobile thefts [26]. Therefore, the illegal use of maintenance tools also needs to be considered to prepare for unauthorized use.

(3) Example measures

(i) Assumption of risks as IoT components

1) Assuming the risks as IoT components even for devices and systems intended for closed networks

Devices and systems equipped with the functions to be connected with the IoT should be designed and operated on the basis that they are used as IoT components even if they are assumed to be used in home LANs or internal company LANs.

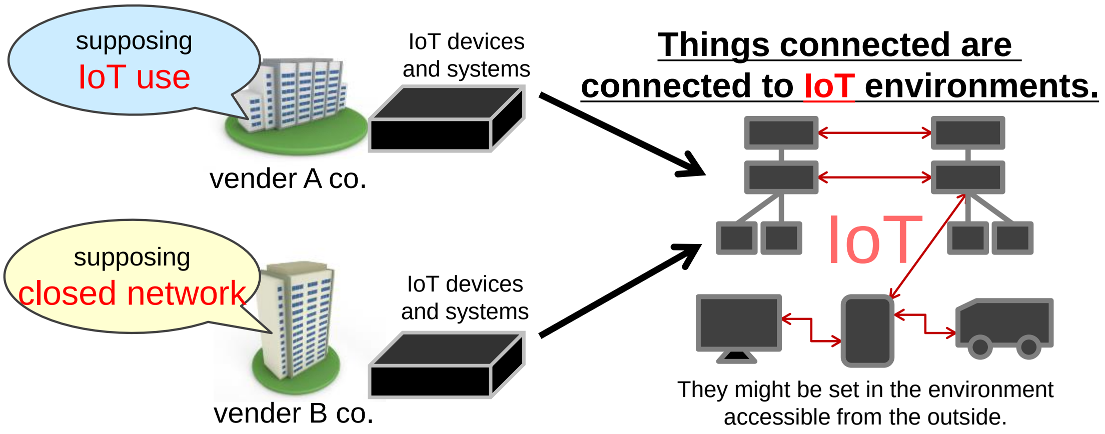

supporsing
IoT use
IoT devices and systems
vender A co.
supporsing
closed network
IoT devices and systems
vender B co.
Things connected are connected to IoT environments.
IoT
They might be set in the environment accessible from the outside.

Figure 4-8 Things that can be connected are connected IoT

Concrete examples are as follows:

- The same initial password should not be used at every release of a product. In addition, easy-to-guess-passwords should be used.
- Password shall be changed by users, and automatic password generation or strength checking of passwords entered by users should be implemented.
- Functions should be restricted when user authentication failure exceeds a certain number of times.
- Devices should not have server functions if they are not required. If they are equipped with server functions, the ports used must be restricted to the minimum and other ports must not be available for use.
- Administrator permissions should not be assigned to all internal functions, but suitable

user permissions should be assigned.

- Install antivirus software on devices and systems on disconnected networks, and perform virus checks on PCs and USB memory devices that are brought in.

2) Responding to unexpected situations

Functions that check for the connection environments of devices and systems and urge users, etc., to take measures if any problem is found are expected to be implemented in the future. Concrete examples include functions to urge users to make changes or notify support staff of the problem when the following conditions are detected:

- Devices are installed in environments that are externally accessible
- Devices might have been attacked, etc.

3) Application of risk analysis methods on users and environments included.

The STAMP/STPA is a method to identify risks in consideration of interaction among devices and systems, people, environments, etc. [27] [28]. This method is based on the thought that accidents are caused not only by troubles of devices constituting the system or operational errors but also by the interactions among the safety-related entities of the system including users and environments. This method for safety is also applicable for security.

(ii) Assumption of risks as IoT components

1) Assuming the risks of connecting to malicious objects

Risks to be connected to a malicious server by a rewritten setting information or to a fake access point unconsciously should be assumed. Examples are as follows:

- A fake application downloaded to a smartphone hijacks the Wi-Fi home router to refer to a fake DNS server and makes the smartphone connect to malicious servers.
- Mobile devices may be connected to a fake Wi-Fi access point which has the same SSID and password a public Wi-Fi access point of a certain public organization [29].

2) Assuming the risks of hijacking authorized connected devices and systems

The risks that authorized devices and systems the IoT component connects to are hijacked or be infected by viruses are should be assumed. An example is as follows:

- The risk that the core system is virus-infected by a targeted attack email and gives malicious commands to the connected IoT component.

(iii) Assumption of risks of attacks during maintenance especially by illegal use of maintenance tools

1) Assuming the risks of attacks during maintenance

Even if measures against internal fraud are taken for employees and relevant companies based on Guideline 3, completely suppressing them is assumed to be difficult. Therefore, in addition to deterring internal fraud, risks during maintenance should also be assumed. Concrete examples include the following:

- Fraudulent acts by maintenance staff (installation of malicious software, etc.)
- Unauthorized use of maintenance I/F by third parties (invocation of unpublished maintenance modes, acquisition of physical keys of ATMs, etc.)

2) Assuming the risk of illegal use of maintenance tools

Assume the risks that maintenance tools are used in an unauthorized manner or altered to mount attacks. Concrete examples include the following:

- Illegal use of maintenance tools that are stolen or illegally sold (unauthorized settings change, etc.)
- Attacks against the vulnerabilities of maintenance tools (virus infection, etc.)
- Development of attack tools based on leaked design information or the disassembly/analysis of maintenance tools.

[Guideline 6] Assuming the risks spread through connections

(1) Points

(i) Assume the risks of spreading security threats and the impacts of device failures due to connections with other devices.
(ii) Assume in particular that the risks of spreading the impacts increase when devices and systems with low level of Safety/Security measures are connected.

(2) Description

In the IoT, there are concerns that the impacts will spread extensively through connections when failures or virus infections occur in devices and systems. Operation stoppage can affect collaborating devices and systems, and victims may be turned into perpetrators by being used as springboards by virus infection. There may be cases where devices and systems cannot recognize their own abnormal states or the fact that they are attacking other devices. It is also necessary to recognize risks assuming that there are numerous IoT components.

Furthermore, cases of the overall level of Safety/Security measures being lowered by connecting IoT components with different levels of Safety/Security measures are also assumed. Vulnerabilities of IoT components with low level of Safety/Security measures may be used as entry points for attacks, and defects and wrong settings can affect the entire IoT.

The risks of IoT components assumed and methods for Safety/Security design are expected to vary in different industries, and therefore the risks of spreading due to connections need to be dealt with in a coordinated manner.

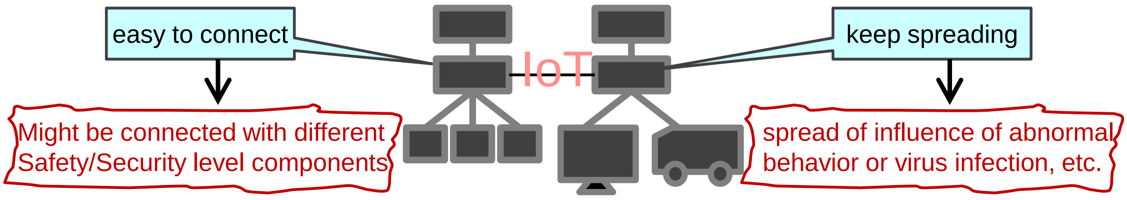

easy to connect
Might be connected with different Safety/Security level components
IoT
keep spreading
spread of influence of abnormal behavior or virus infection, etc.

Figure 4-9 Example of increased risks due to connections

(3) Example measures

(i) Assuming the risks of spreading through connection

1) Assuming the risks of abnormalities spreading through connection

Assume cases where the abnormalities of devices and systems affect other IoT components, and cases where viruses, etc., spread to the entire IoT through connections.

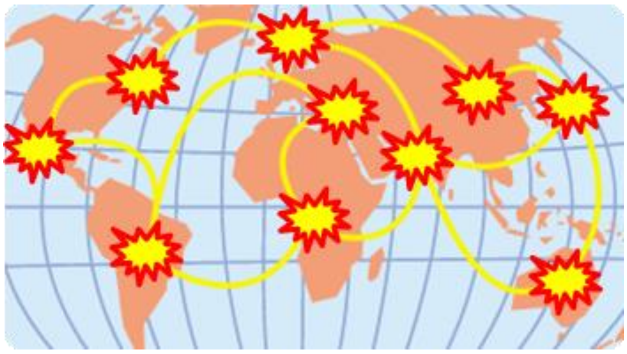


Figure 4-10 Image of the risks of spreading through connections

Assume not only the cases of damage, but also the cases where collaborating devices and systems are affected by operation stoppage, and victims are turned into perpetrators by being used as springboards by virus infection. In addition, assume the cases where devices and systems cannot recognize their own abnormal states or the fact that they are attacking other devices.

2) Assuming the risks of spreading through shared devices and systems

Devices and systems that are assumed to be shared for use by multiple service providers, including domestic robots, display devices, and IP cameras, may not function normally when competing operations are performed. In addition, the use of common interfaces increases the impacts of unauthorized access.

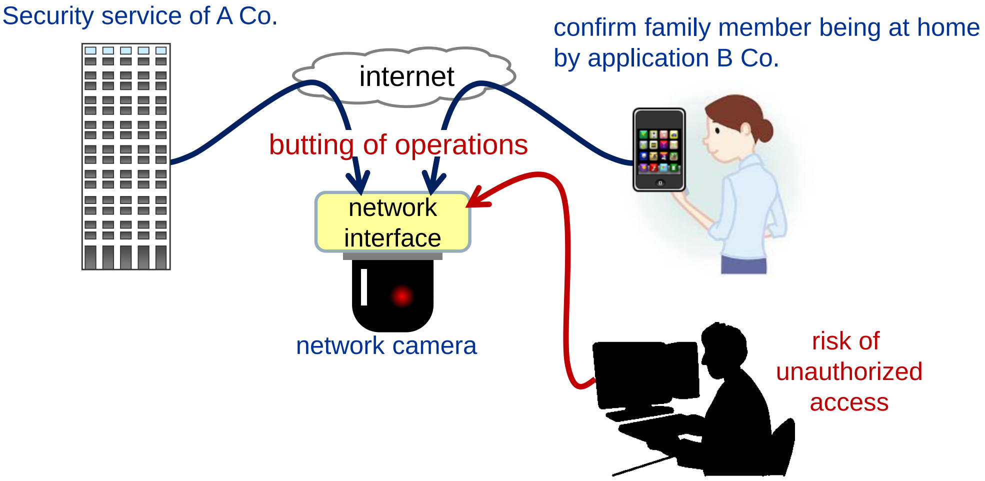


Figure 4-11 Image of the risks of shared devices

(ii) Assuming that the risks of spreading the impacts increase when connected to devices and systems with low level of Safety/Security measures

Assume that IoT components with low level of Safety/Security measures can be entry points for attacks when IoT components with measures of different levels are connected. In addition, assume that the risks can spread to the entire IoT when an IoT system connected with IoT components with low level of measures are connected to another IoT system.

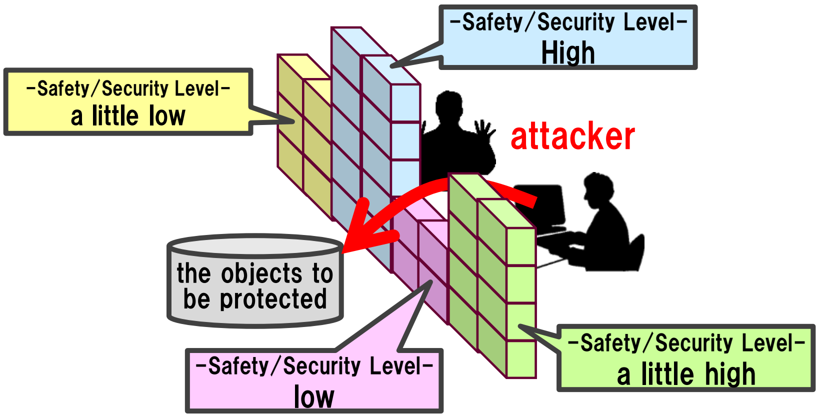


Figure 4-12 Image of the risks spreading from the weaker parts

Because the IoT is a System of Systems as described in 1.1.1, the possibility of the risks of individual IoT components spreading to the entire IoT when IoT systems are connected to each other to become a larger IoT system needs to be assumed.

[Guideline 7] Understanding physical security risks

(1) Points

(i) Assume the risks of unauthorized operations of stolen or lost devices, and physical attacks at locations where no administrator is present.

(ii) Assume the risks of information retrieval, software alternation, and resale of secondhand or disposed devices.

(2) Description

In the Smart-society, devices and systems that are carried around or installed at home or in public spaces can also be part of the IoT. Therefore, there are risks that stolen or lost devices are operated in an unauthorized manner, and that devices installed in public spaces are physically attacked by third parties. In addition, information may be leaked from disposed devices, and devices installed with malicious software may be sold as secondhand.

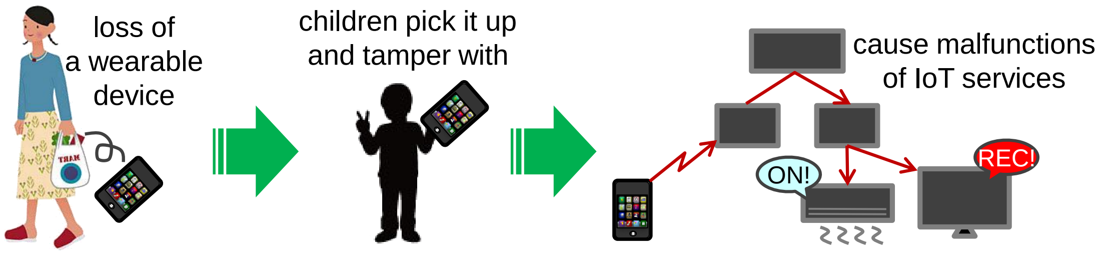
Figure 4-13 Devices and systems at home and in public spaces not physically managed by manufacturers (repeat)

(3) Example measures

(i) Examples of physical risks assumed

1) Assumption of the risks caused by stolen or lost IoT components

Assume the risks that stolen devices are operated in an unauthorized manner, and that IoT services malfunctions are caused by devices that are lost and then found and tampered with.



loss of a wearable device
children pick it up and tamper with
cause malfunctions of IoT services
ON!
REC!

Figure 4-14 Example of physical risks caused by lost IoT components

2) Assumption of the risks of physical attacks at locations where no administrator is present

Assume the risks that the covers of automobiles in parking lots or HEMS devices in yards are opened, and then unauthorized devices are connected to them for remote operation. In addition, consider the risks that someone enters empty homes and changes the settings of home electrical appliances to connect them to malicious sites.

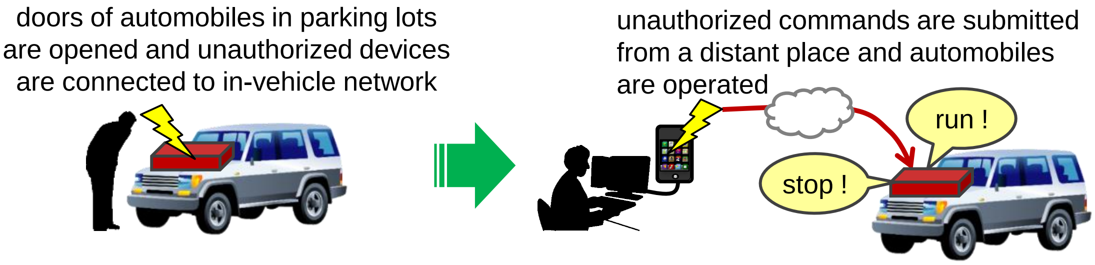

doors of automobiles in parking lots are opened and unauthorized devices are connected to in-vehicle network
unauthorized commands are submitted from a distant place and automobiles are operated
run !
stop !

Figure 4-15 Example of physical risks of attacks against automobiles in parking lots

(ii) Examples of unauthorized retrieval and alteration assumed

1) Assumption of the risks that the objects to be protected are retrieved from disposed IoT components

Assume the risks that software and settings of disposed IoT components are retrieved, analyzed, and then communication protocol is derived and used for attacks against the IoT, and that personal information contained in it is retrieved and used for unauthorized access by spoofing.

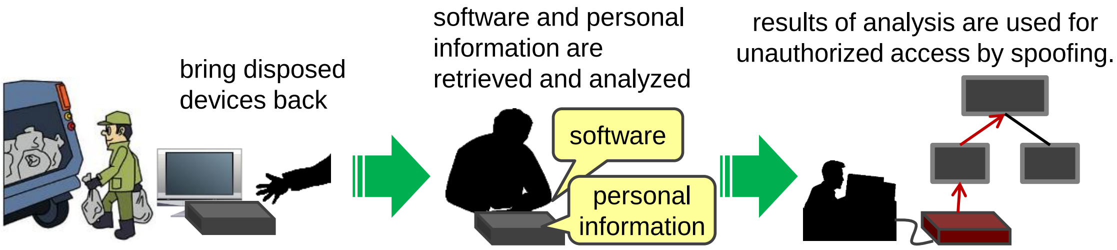

bring disposed devices back
software and personal information are retrieved and analyzed
software
personal information
results of analysis are used for unauthorized access by spoofing.

Figure 4-16 Example of the risks that disposed IoT components are used for attacks

2) Assumption of the risks that IoT components are embedded with illegal mechanisms and sold as secondhand

Assume the risks that the software of IoT components is altered to connect them to malicious sites, and then the components are auctioned off or sold to secondhand shops.

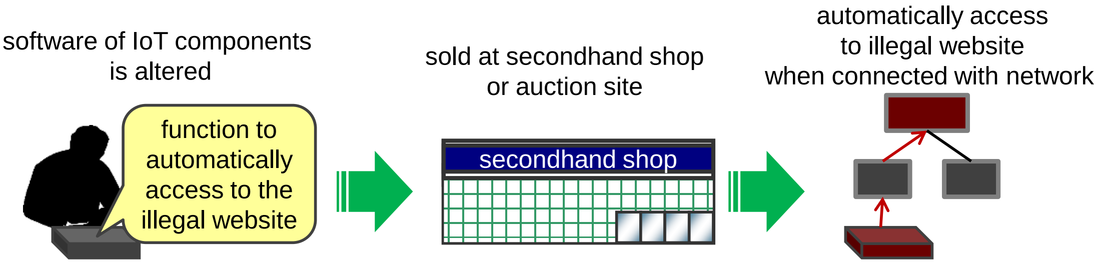

software of IoT components is altered
function to automatically access to the illegal website
sold at secondhand shop or auction site
secondhand shop
automatically access to illegal website when connected with network

Figure 4-17 Example of the risks that IoT components connected to malicious sites are sold as secondhand

4.3 Considering the designs to protect the objects to be protected

In order to achieve the Safety/Security of the Smart-society with limited budgetary and human resources, narrowing down the objects to be protected, separating out the areas in particular need of protection, and protecting IoT components with low level of measure functions by other IoT components are effective. In addition, designs to maintain Safety/Security even when unspecified devices and systems are connected by IoT service providers and users, and not to cause trouble in connected IoT components even when abnormalities occur are desirable.

This chapter explains five guidelines to be addressed in the designs to protect the objects to be protected, including the abovementioned designs.

[Guideline 8] Designing to enable both individual and total protection

(1) Points

(i) Discuss the measures to be taken at individual IoT components against the risks via external interfaces, internally contained risks, and physical security risks.
(ii) If the risks cannot be handled by individual IoT components, discuss the measures to be taken at upper-layer IoT components that include them.

(2) Description

In 3.3, risks via "external interfaces (ordinary-use I/F, maintenance I/F, and informal I/F)," "internally contained risks," and "physical security risks" are listed as risks that can exist in IoT components. For risks via external interfaces, attacks such as DoS, viruses, and spoofing, and abnormal data from other devices are assumed. Potential defects and wrong settings, and malware illegally embedded before the product release are assumed for internally contained risks; and theft/disassembly of devices installed at home or in public spaces, and unauthorized replacement of parts are assumed for physical security risks. Measures against these risks are necessary.

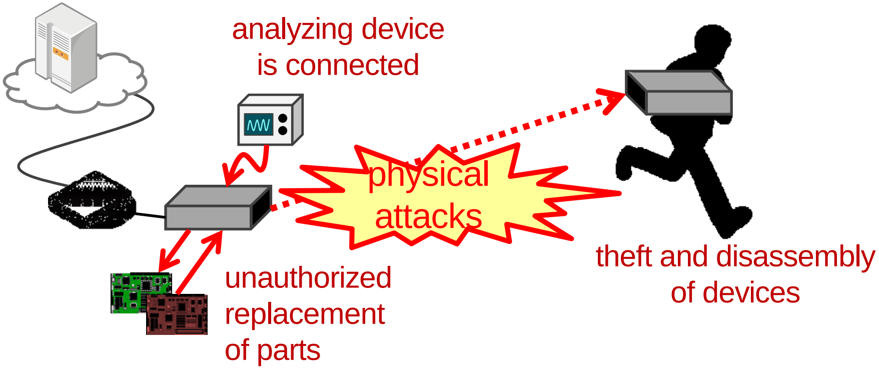

analyzing device is connected
physical attacks
theft and disassembly of devices
unauthorized replacement of parts

Figure 4-18 Physical security risks of devices

Some IoT components such as sensors are of low performance, and thus implementing measure functions by themselves may be difficult. In such cases, discuss the measures to protect them by upper-layer IoT components that include them.

(3) Example measures

(i) Measures against risks via external interfaces, internally contained risks, and physical security risks

1) Measures against risks via external interfaces
- For measures against the risks via ordinary-use I/F, user authentication, verification of authenticity of message data, vulnerability management using fuzzing tools, and logging have been implemented [13].

- Because maintenance I/F is intended for use by maintenance/operation staff, measures such as device authentication, user authentication, etc., are implemented in some cases. For devices of particular importance, cases of protecting I/F by physical keys, using double keys, biometrics, and making connections via special adapters are increasing.
- Informal I/F is used for debugging purposes and often assigned with high-level privileges, and therefore higher-level security functions than other I/F are required.

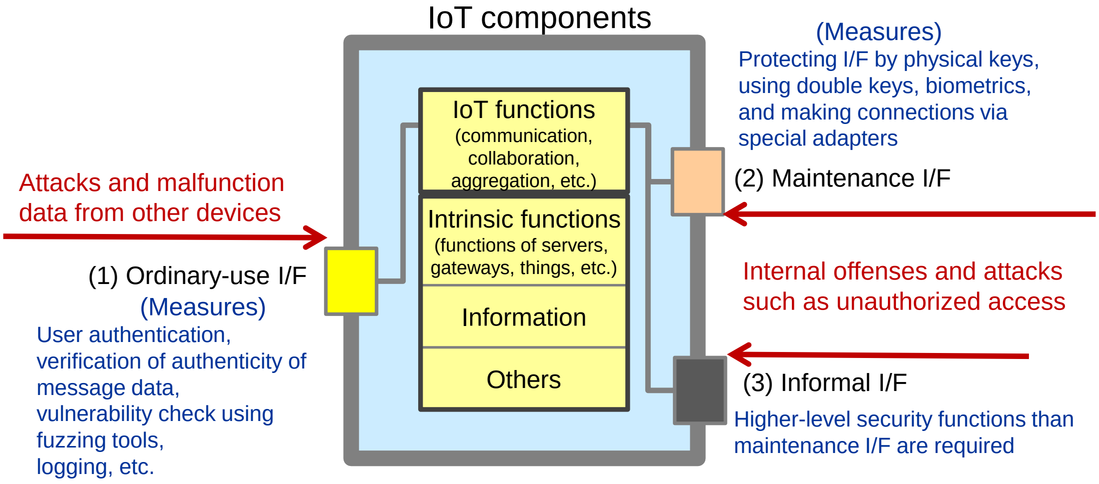

IoT components
IoT functions
(communication, collaboration, aggregation, etc.)
Intrinsic functions
(functions of servers, gateways, things, etc.)
Information
Others
Attacks and malfunction data from other devices
(1) Ordinary-use I/F
(Measures)
User authentication, verification of authenticity of message data, vulnerability check using fuzzing tools, logging, etc.
(Measures)
Protecting I/F by physical keys, using double keys, biometrics, and making connections via special adapters
(2) Maintenance I/F
Internal offenses and attacks such as unauthorized access
(3) Informal I/F
Higher-level security functions than maintenance I/F are required

Figure 4-19 Measures against risks via external interfaces

2) Measures against internally contained risks

- In cases where parts and/or software are outsourced, measures to obtain documents related to design and quality, and to verify the absence of unauthorized embedding and quality problems are implemented [9].
- For devices that handle charged contents, measures are taken at runtime in some cases, including checking the authenticity of internal data and software, and checking the adequacy of generated data. In addition, confidentiality measures are taken for important data, including encryption.
- For devices with internal clocks, regular time correction using trusted external systems, and strengthening of the tamper resistance of clock functions are implemented. In cases where multiple IoT components are involved, measures are taken for clock synchronization between them.
- In the development of software that runs on open platforms such as smartphones, vulnerability management that use security inspection tools for source code, etc., are taken.

3) Measures against physical security risks

Disable the retrieval of data and software contained in devices even when the devices are stolen and disassembled. Table 4-5 shows examples.

Table 4-5 Examples of measures against physical security risks (tamper resistance)

Type of measures	Example measures
Measures by hardware and structural design	- Designs to prevent analysis by cutting wires or breaking interfaces when devices are disassembled. - Elimination of unnecessary informal I/F and exposed wiring - Designs to disallow internal access unless dedicated authentication devices are connected - Electromagnetic shields to disable assumption of internal processing from electromagnetic emanations - Internalization of chips and wires
Measures by data	- Implementation of functions to remotely lock terminals when stolen or lost

and software design	- Obfuscation and encryption of software - Encryption of confidential data, shortening the time in memory, etc., when used - Prevention of falsification of programs and data on memory at runtime

In order to prevent the retrieval of data left on rented, secondhand, disposed devices, etc., the functions to erase data on nonvolatile memory are implemented for smartphones, etc.

4) Security measures according to the importance of the objects to be protected

Costs can be reduced by taking measures mainly for the objects to be protected, rather than protecting all the devices and systems.

- By sectioning off devices and systems comprising IoT components into multiple areas (hereinafter referred to as “domains”) physically or by virtual gateways, the extent of the impacts can be localized, and important functions can be protected by multiple gateways.
- For important information generated at settlements, the method to retrieve/encrypt the data using high-security peripheral devices and sending the data directly to servers, thereby not leaving the important information on the main units, can be used. This method enables both the strengthening of security and reduction of measure/management costs, and is in the process of being standardized in the POS industry.

(ii) Measures to protect IoT components with insufficient level of measures by superordinate IoT components

Discuss the measures to protect IoT components that cannot implement security functions due to insufficient performance by “superordinate IoT components” that include them, as shown in the figure below.

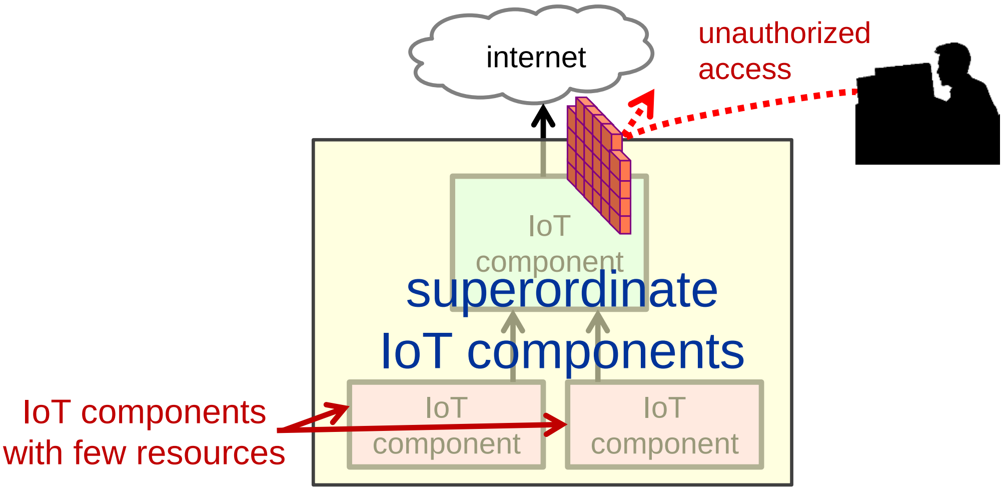


Figure 4-20 Image of protection by superordinate IoT components

- Execute designs to block attacks by reducing the points at which IoT components are connected to the Internet, and establishing gateways.
- Furthermore, use IoT components with monitoring functions to monitor devices and systems to detect abnormalities and guess at the causes. TR-069 of Broadband Forum (BBF) is available as a standard specification for the remote management of home electrical appliances [30].

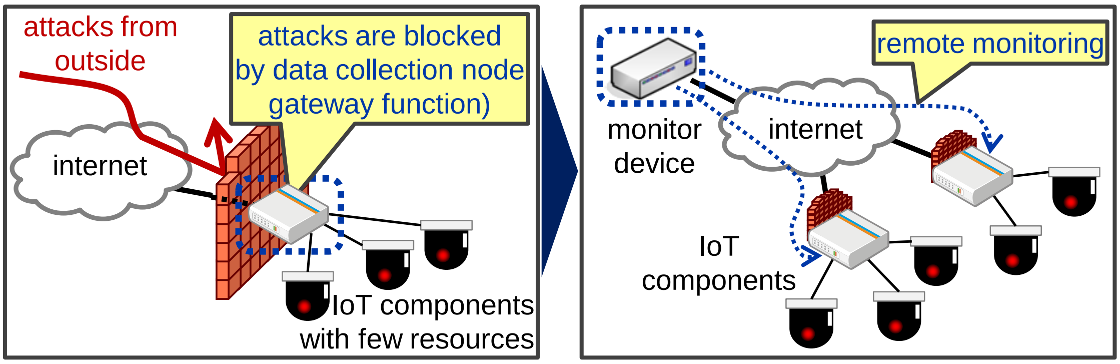

attacks from outside
attacks are blocked by data collection node gateway function)
internet
IoT components with few resources
remote monitoring
monitor device
internet
IoT components

Figure 4-21 Image of measures for IoT components with low level of measure functions

Developers of IoT components for which sufficient measures cannot be taken due to restrictions in the product specifications, etc., must clearly specify the matters to be considered in relation to measures against the risks of using such IoT components in manuals and user instructions.

[Guideline 9] Designing so as not to cause trouble in other connected entities

(1) Points

(i) Discuss the designs to enable the detection of abnormalities of IoT components.
(ii) Discuss suitable behaviors when abnormalities are detected.

(2) Description

When abnormal operations due to software/hardware defects or attacks occur, the abnormal states need to be detected first to prevent the impacts from spreading. In addition, when the abnormal states are detected, the impacts may, depending on the content, spread to other IoT components. In order to prevent this, therefore, measures to disconnect such IoT components from networks, etc., need to be discussed.

When IoT components are disconnected from networks or their operations are stopped, the designs to enable prompt recovery according to the situations are necessary to reduce the impacts on users and other IoT components that are using the functions of the IoT components.

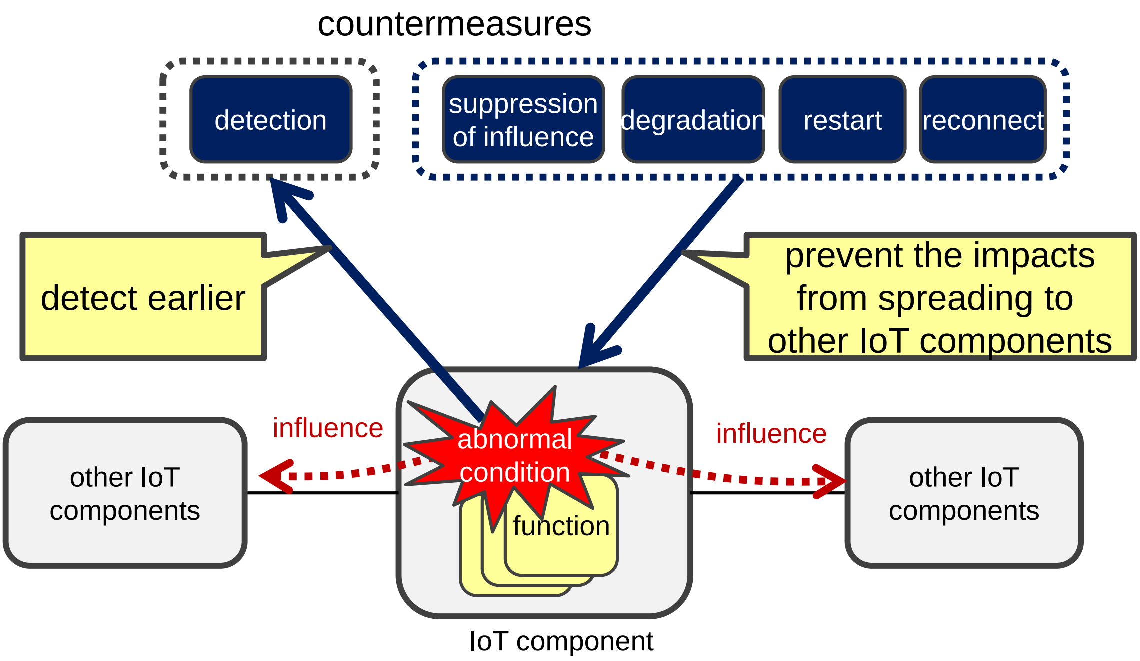


Figure 4-22 Image of disconnection and recovery of functions

(3) Example measures

(i) Detection of abnormal states

The detection of abnormal states must initially be performed individually by each IoT component. In some cases, however, IoT components cannot detect their own abnormalities depending on the specifications or conditions of abnormalities. As an example measure for such cases, monitoring servers can refer to the log information of IoT components to detect abnormal states.

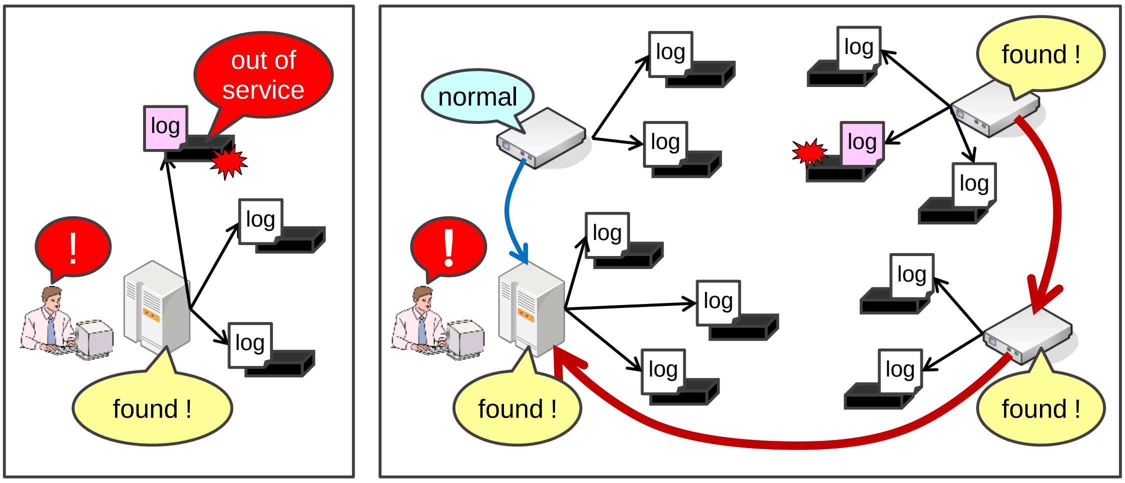
Examples of monitoring using logs are as follows:

- Monitoring multiple, collaborating IoT components

  In cases where the collaboration of multiple IoT components is considered important, a method in which monitoring systems detect abnormalities by verifying the consistencies of the processing results of the components involved can be used.

- Suppressing increase in processing load by monitoring IoT components

  Because log monitoring consumes server resources such as CPU usage, memory, and network bandwidth, the monitoring methods need to be appropriately designed according to the scale of the systems subject to monitoring and performance of the IoT components. Figure 4-23 shows examples.



If some, monitor them directly.

If many, share monitoring (load sharing).

Figure 4-23 Examples of monitoring methods that take into consideration the performance of IoT components

(ii) Spreading prevention and recovery in the case of abnormalities

1) Suppression of the spread of the impacts of abnormal states

- When IoT components detect their own abnormal states and if the impacts can possibly affect other IoT components, the IoT components should terminate their operations or disconnect themselves from networks to suppress the spread of the impacts.
- When monitoring servers detect abnormalities of IoT components, they should direct the IoT components to terminate their operations or disconnect from networks, or forcibly disconnect them from networks using routers, etc., depending on the content of the abnormalities.

2) Fall back of functions in which abnormalities occur

When abnormalities are deemed to be limited to certain functions, restrict only the operations of the functions concerned and continue to allow operations of other functions. Examples of measures by restricting functions are as follows:

- Close only the receiving ports of the functions concerned
- Terminate only the processes that execute the functions concerned
- Configure the functions concerned to always return an error by settings

3) Restart/reconnection of IoT components

- Depending on the situation, the abnormal states may be resolved and restored to normal state by restarting the IoT components concerned. Restart can be performed by the IoT components themselves upon detection of abnormalities or from outside by monitoring servers, etc.
- Recover the disconnected IoT components for the reason of not spreading abnormalities by the procedures based on the operation policies and functions, and then reconnect them to networks.

4) Resilience of IoT components

- Resilience of systems and services are also considered important in the IoT sector. Resilience is addressed in major standards, and they can be used as reference when discussing the measures.

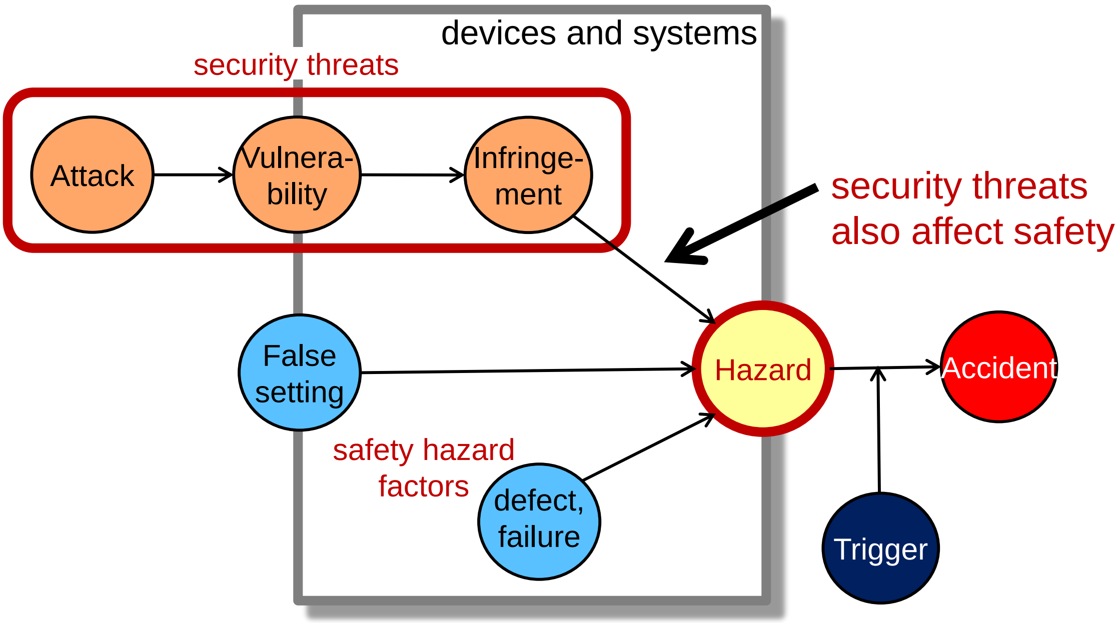
[Guideline 10] Ensuring consistency between the designs of Safety/Security

(1) Points

(i) Visualize the designs of Safety/Security.
(ii) Verify the mutual impacts of the designs of Safety/Security.

(2) Description

In some cases, security threats can cause safety hazards. For instance, if software or data falsification is performed by third parties through unauthorized intrusion into IoT components, malfunctions may be caused by some triggers. In addition, implementing security functions may affect the performance of intrinsic functions that include safety-related functions. “Visualization” of safety and security designs is effective for verifying whether the measures are appropriately implemented.



Source: Prepared based on “SECURITY AND SAFETY MODELLING FOR EMBEDDED SYSTEMS,” SESAMO Project

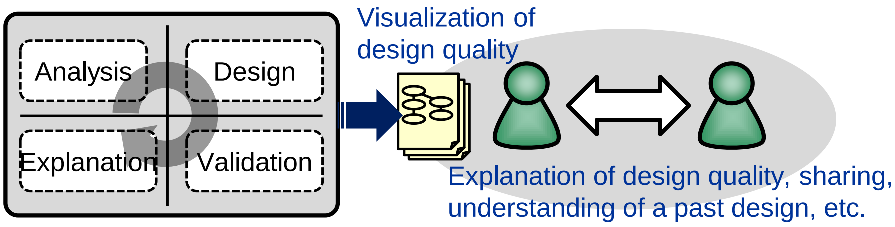
Figure 4-24 Model of security problems affecting safety

In the verification of the quality of safety and security designs, not only the verification of measures for risks caused by hazards/threats, but also the mutual impacts of designs of safety and security need to be verified. In doing so, effective measures include visualization of their mutual impacts to make verification of the consistency of the designs by engineers of different departments/companies easier.

(3) Example measures

(i) Visualization of Safety/Security design

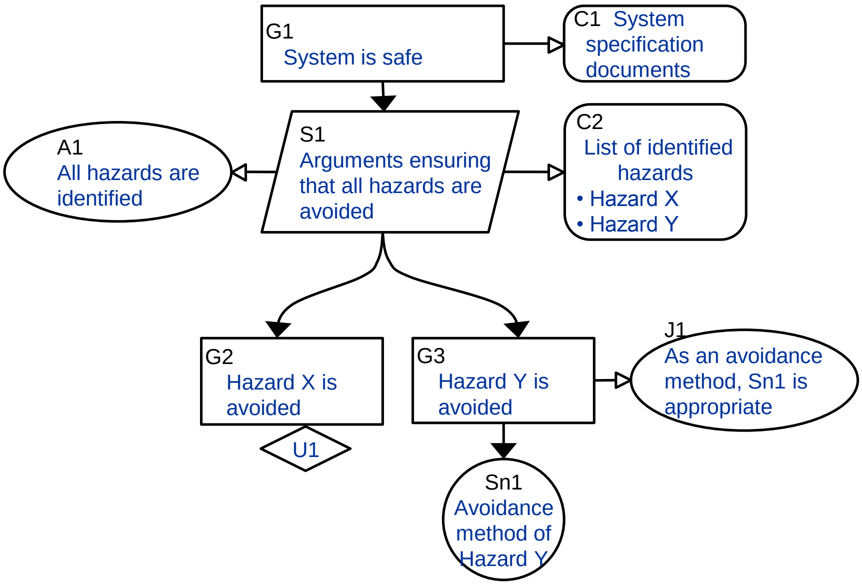
- “Visualization” of a design means making the analysis, design, and evaluation processes in the design, including the background and rationale, visible, and is expected to be effective in mutually sharing the design quality among safety and security engineers. In addition, it can also be effectively used in understanding and evaluating the design quality when using the existing functions in new products.


Analysis
Design
Explanation
Validation
Visualization of design quality
Explanation of design quality, sharing, understanding of a past design, etc.

Source: Introduction to Safety & Security Design in Smart Society

Figure 4-25 Visualization of software design quality

- Visualization can also be used in explaining to and obtaining consent for the safety and security design quality from not only developers but also management, ordering companies, and companies to which work has been outsourced. Even when accidents occur by chance, accountability to the victims can be fulfilled without verifying the situations and preparing documents in a hurry.
- Various visualization methods have been developed and used, according to the development objects and environments. Figure 4-26 shows an example of GSN notifications, which is a well-known visualization method. For details of visualization of designs, see “Introduction to Safety & Security Design in Smart Society” [9].


G1
System is safe
C1 System specification documents
S1
Arguments ensuring that all hazards are avoided
A1
All hazards are identified
C2
List of identified hazards
• Hazard X
• Hazard Y
G2
Hazard X is avoided
U1
G3
Hazard Y is avoided
J1
As an avoidance method, Sn1 is appropriate
Sn1
Avoidance method of Hazard Y

Source: Introduction to Safety & Security Design in Smart Society

Figure 4-26 Example of GSN notifications

- As an international standard for achieving dependability of consumer devices, “Dependability Assurance Framework for Safety Sensitive Consumer Devices (DAF for SSCD)”, which is a meta-standard for development based on the visualization of safety/security design and adjustments, is available [31].

(ii) Verification of the mutual impacts of safety and security

In security measures, the functions to be protected (intrinsic functions and safety-related functions) need to be identified, and threat and risk analysis performed. Examples of the discussions are described below.

- Perform threat/risk analysis for the functions to be protected (requirements), discuss security measures, and analyze/validate the effectiveness and impacts on the functions to be protected; and then if the validation results are not considered tolerable, perform analysis/discussions again.

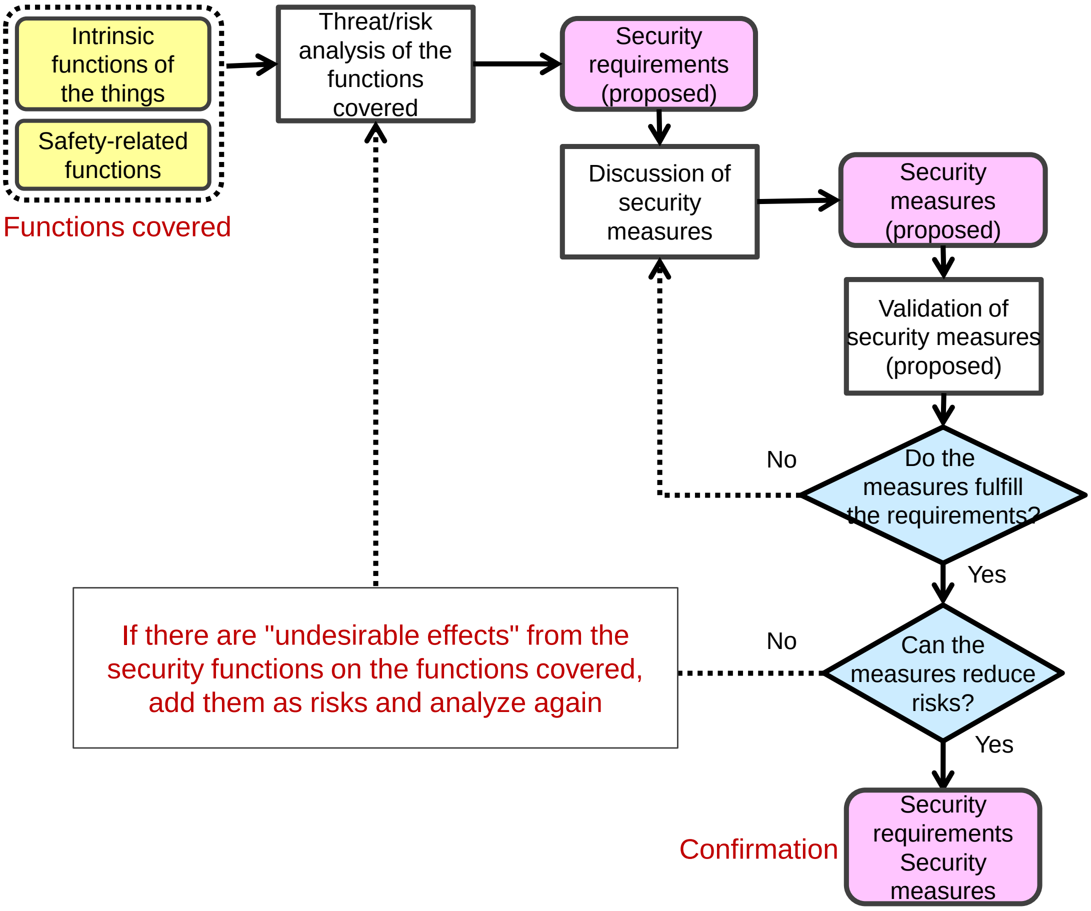

Intrinsic functions of the things
Safety-related functions
Functions covered
Threat/risk analysis of the functions covered
Security requirements (proposed)
Discussion of security measures
Security measures (proposed)
Validation of security measures (proposed)
No
Do the measures fulfill the requirements?
Yes
If there are "undesirable effects" from the security functions on the functions covered, add them as risks and analyze again
No
Can the measures reduce risks?
Yes
Confirmation
Security requirements Security measures

Figure 4-27 Flow of security validation/analysis/measures

- If the scale of the objects to be protected is large, fully analyzing the impacts of security measures requires enormous efforts. Examples of methods for analyzing the impacts in such cases include DRBFM (Design Review Based on Failure Model), etc. [32]

[Guideline 11] Designing to ensure Safety/Security even when connected to unspecified entities

(1) Points

(i) Discuss the designs to enable IoT components to determine the connection methods according to the entities to be connected to and conditions of the connections.
(ii) Consider the design to prevent IoT components and users from a connection which may result in a hazard.

(2) Description

Even for those combinations that had not been tested by the device manufacturers for operation while connected, devices with functions conforming to industrial standards can be connected and used in many cases. For this reason, as the IoT is becoming more popular, cases are increasing where unspecified devices not assumed by the device manufacturers to be used are connected and used by integrators and advanced users.

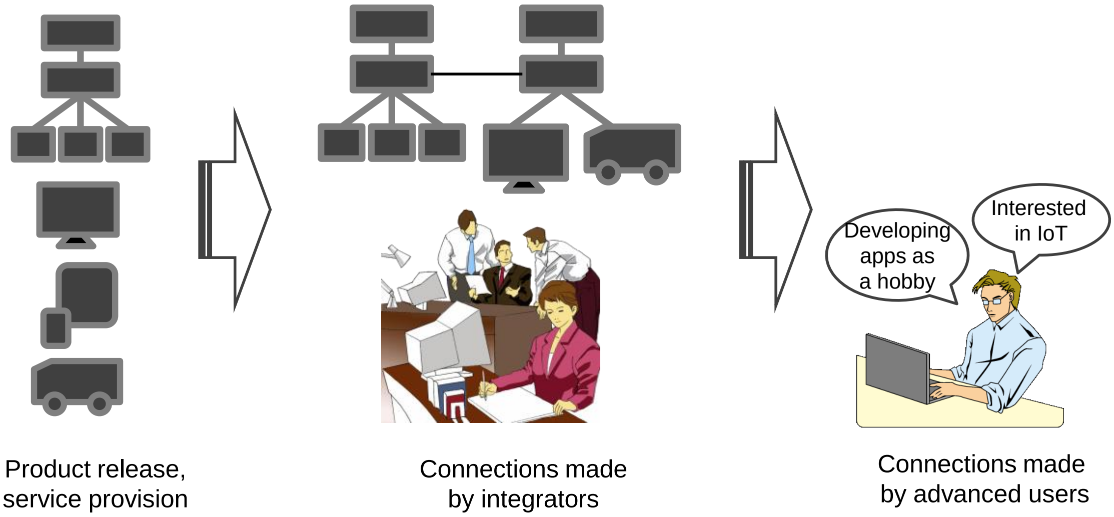

Developing apps as a hobby
Interested in IoT
Product release, service provision
Connections made by integrators
Connections made by advanced users

Figure 4-28 Connections with unspecified devices

Under such circumstances, leakage of confidential information and unexpected operations may occur when devices with low reliability are connected. In addition, because more and more models and versions are released afterward with the passage of time, cases are increasing where even the products of the same manufacturers are not tested for operation while connected. Therefore, designs to determine the connection methods according to the entities to be connected to and conditions of the connections need to be discussed.

Furthermore, the design to lead users and installation engineers not to connect hazardous devices is required. Understanding and analyzing user experiences and usage environments, notification using manuals, labels, warning messages on devices, etc. should be considered.

(3) Example measures

(i) Designs to verify the entities to be connected to and conditions of the connections, and then determine the connection methods according to the results

Designs to verify information such as the manufacturers, model years, and conforming standards of other devices to be connected to, and then determine whether to connect to them, according to the content of the information, may be considered. In addition, designs to extend connections while limiting risks to a tolerable range by changing the extent of functions and information to be provided according to the features of the devices to be connected to may be considered.

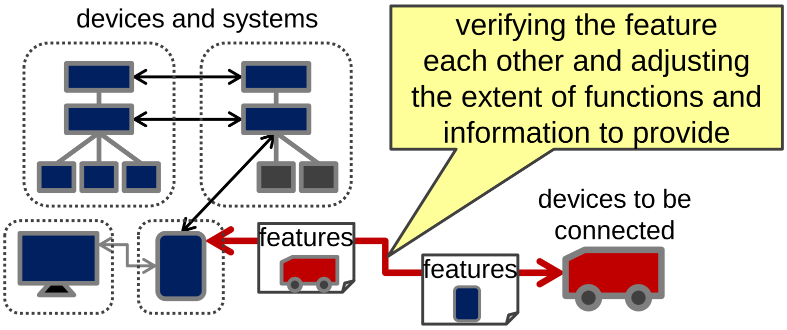

devices and systems
verifying the feature each other and adjusting the extent of functions and information to provide
devices to be connected
features
features

Figure 4-29 Changing functions and information to be provided according to the features of the devices to be connected to

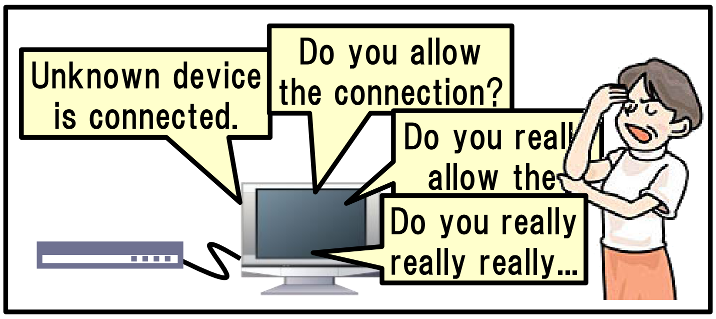
- Imposing restrictions may be considered, in which devices of the same manufacturer can connect to the fullest extent, and devices of the same industrial organization can connect to a certain level.
- A method to raise the security level by allowing important functions to be executed only when the devices to be connected to are verified to have appropriate permissions can also be used. For instance, this method is used overseas for ATMs to prevent operations by unauthorized terminals during maintenance.
- The broader the extent of connections, the greater the business opportunity and users' convenience is expected to be enhanced in the IoT. Therefore, minimal functions and information may be provided even to devices of companies in different industries and companies with no business ties if they conform to Safety/Security-related standards.

Approaches to accumulate information on the connection modes/conditions and forms of use of devices when abnormal cases occur, and to use it to prevent the occurrence of abnormalities are being developed.

(ii) Designs to prevent IoT components and users from hazardous connections

The "misuse case" diagram is the effective tool to identify hazardous or wrong connections. In this tool, normal usages conformant to the specification ("use") and abnormal usages which cause threats ("misuse", including actions by authorized users and unmalicious actions) are expressed in a diagram. This diagram clarifies the vulnerability and the possibility of hazardous operation, and make it possible to confirm that the countermeasures against them do not prevent normal uses.

For the hazardous connection identified as a "misuse case", the implementation of the function to warn users may be considered. For example, it is suggested to implement functions to block automatically, to warn and to let users confirm a connection when they are about to connect their IoT devices to some malicious IoT systems by mistake. These functions are effective not only for avoiding risks but also for letting users recognize the hazardous cases and prevent risks. However, users may stop the functions if warnings are given frequently, therefore the balancing is important.



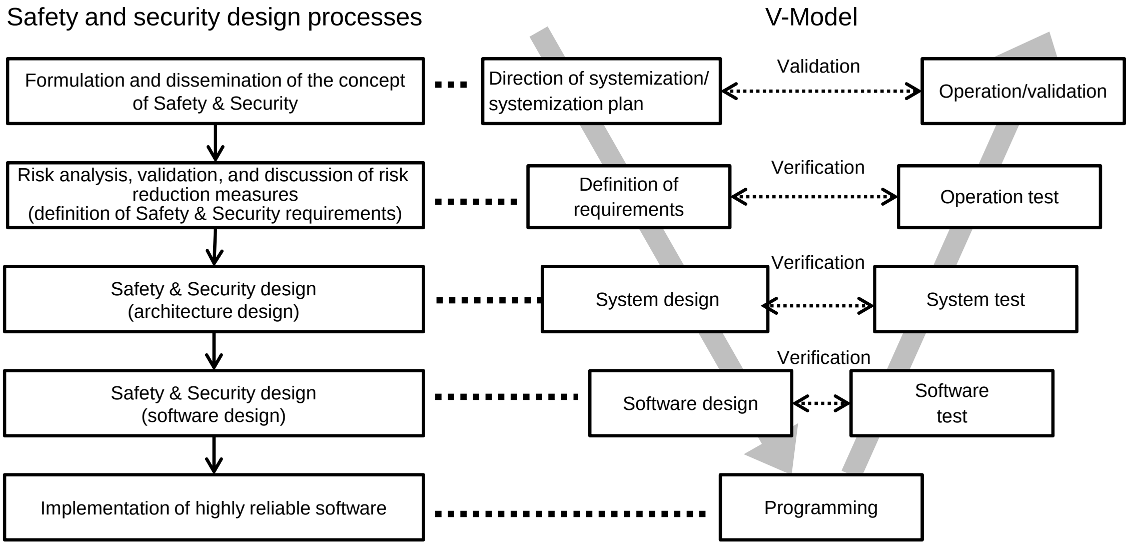
[Guideline 12] Verifying/validating the designs of Safety/Security

(1) Points

(i) Verify and validate the Safety/Security design of devices and systems to be connected, with consideration given to the risks unique to the IoT.

(2) Description

Processes that can be used to verify/validate the achievement of the design of devices and systems include the V-Model. Figure 4-30 shows examples of the V-Model in safety and security designs.


Safety and security design processes
V-Model
Formulation and dissemination of the concept of Safety & Security
Risk analysis, validation, and discussion of risk reduction measures (definition of Safety & Security requirements)
Safety & Security design (architecture design)
Safety & Security design (software design)
Implementation of highly reliable software
Direction of systemization/ systemization plan
Validation
Operation/validation
Definition of requirements
Verification
Operation test
System design
Verification
System test
Software design
Verification
Software test
Programming

Source: Introduction to Safety & Security Design in Smart Society

Figure 4-30 Verification/validation in safety and security designs

There are cases where IoT components have no problems on their own, but unexpected hazards and threats may occur when they are connected. Therefore, not only the "verification" of the fulfillment of the Safety/Security requirements and design but also the "validation" of adequacy of Safety/Security design in the Smart-society needs to be performed.

(3) Example measures

(i) Examples of items to be reflected to verification/validation

1) Reflecting to each guideline

Reflect necessary matters to the validation by discussing the objects to be protected, methods of connections, and risk locations described in Chapter 3 of the Development Guidelines, and then reflecting the contents of Guidelines 1 to 17.

2) Verification/validation according to the levels of Safety/Security measures of devices and systems

International standards on Safety/Security are established in some industries, and their requirements can be used for extracting verification/validation items. In addition, the levels of Safety/Security measures are objectively validated by third-party certifications based on standards.

- International standards on safety

For the functions to achieve safety, a functional safety standard IEC 61508 and its derived standards have been established. Matters related to security were added in the second edition of IEC 61508.

- Common Criteria (ISO/IEC 15408)

Common Criteria is a standard for evaluating whether or not information technology-related devices/systems are appropriately designed and correctly implemented from the point of view of information security. Devices and systems certified in accordance with international agreements are accepted as valid by the member countries.

- EDSA (Embedded Device Security Assurance) certification

EDSA is a security certification program for control devices, and consists of three validation items: software development security assessment, functional security assessment, and communication robustness testing.

- Others

For sectors in which international standards are not established, third-party assessments are also effective. In the U.S., security assessment organizations such as ICSA Labs and NSS Labs conduct assessments of communication devices. In Japan, Connected Consumer Device Security Council (CCDS) formulated the security assessment guidelines by type of product category.

3) Verification of the implementation of measures against existing hazards and threats

As the IoT becomes more popular, unknown hazards and threats are expected to occur. Collaborate with operations staff, etc., to understand the latest information, and then have it reflected in the validation (see Guideline 15).

4.4 Considering the designs to ensure protection even after market release

In the Smart-society, many devices and systems such as automobiles and home electrical appliances are used for 10 or more years, and therefore protecting them from malfunctions and unauthorized operations due to failures, compromise of security functions, etc., is necessary. For this, Safety/Security-related functions are needed to appropriately identify/determine the component's own status and be updated by updating software.

This chapter explains two guidelines to be addressed in the designs to protect devices and systems after their market release.

[Guideline 13] Implementing the functions to identify and record own status

(1) Points

(i) Discuss the functions to identify and record the component's own status and the status of communications with other devices.
(ii) Discuss the functions to disallow unauthorized deletion/manipulation of records.

(2) Description

In situations where various devices and services are connected, understanding what is happening and where it is happening can be difficult. In order to detect abnormalities, analyze the causes, and discuss measures when they occur, individual IoT components should understand their own status and the status of communications with other devices, and record them as logs. On this occasion, automatic collection of data such as operation histories and environments of users make it possible to clarify the vulnerabilities caused by careless operations or connections, and to recognize unexpected usages and their frequency so as to apply the next development of products. Besides, it is necessary to pay attention to handling logs because they may include privacy data of users. In addition, it is necessary to keep the logs secure because elimination or falsification of the log data by attackers makes it impossible to take measures.

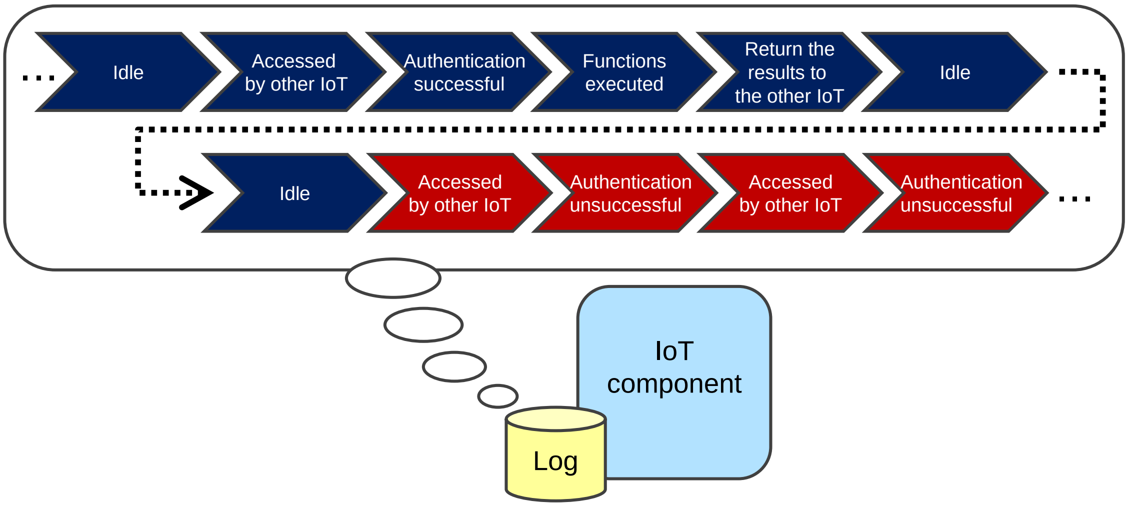

…
Idle
Accessed by other IoT
Authentication successful
Functions executed
Return the results to the other IoT
Idle
Idle
Accessed by other IoT
Authentication unsuccessful
Accessed by other IoT
Authentication unsuccessful
…
IoT component
Log

Figure 4-31 Logging in IoT components (operation histories)

In addition, some IoT components including sensors are of low functionality, and therefore taking measures such as managing massive logs and performing log encryption on their own may be difficult. For such devices, measures need to be taken by establishing other IoT components with the functions to manage logs.

(3) Example measures

(i) Identification and recording of the component's own status and status of communications with other devices

· Record the operations of each IoT component in logs.

Examples of the content to be recorded:

- For security analysis: Attacks, user authentication, data access, updates of configuration management information, execution of applications, start/termination of log recording, communications, opening/closing of doors, checksum, and location histories
- For safety analysis: Failure information (hardware/software)
- For reliability analysis: Results information, status information, operating environment information (temperature, humidity, CPU load, network load, amount of resource usage, etc.), software updates

· Because resources for maintaining logs are limited, formulate the policies for maintaining them.

· In order to make the log recording time consistent across related IoT components, perform clock synchronization [33].

· The log recording timing should not be designed for individual devices, but instead considered for all the IoT components.

· Describe in manuals that logs are recorded for the purpose of maintaining the integrity of IoT components.

(ii) Prevention of unauthorized deletion and manipulation of records

· There are methods to set access privileges to logs and perform encryption in IoT components.

· There are methods to regularly send data collected in IoT components to other IoT components equipped with the functions for maintaining logs or to dedicated devices, etc.

· There are cases where mechanisms to allow only appending to logs are available [34].

[Guideline 14] Implementing the functions to maintain Safety/Security even after the passage of time

(1) Points

(i) Discuss the functions to maintain Safety/Security by updates against increased risks due to aging or changes of usages and environments.

(2) Description

By aging of the products/services, there may be cases such as findings of defects, deterioration of security functions and failure in connection with new products. For example, increasing of risks by the estimation of secret keys or random SEED, analysis of software, leakage of setting information, etc. are taken into account. Also, in the Smart-society, it is anticipated that usages and usage environments are changing rapidly, it is necessary to improve usability and add functions to prevent users from operation errors and hazardous connection.

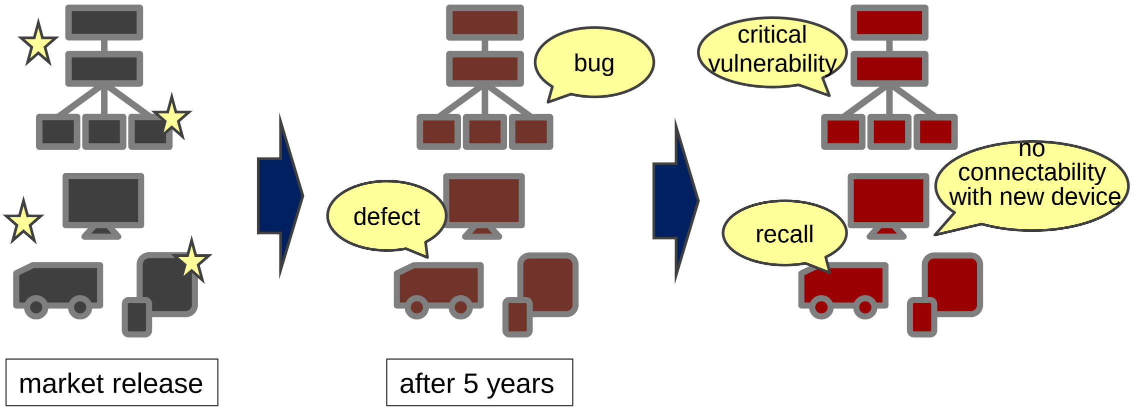


Figure 4-32 Increased risks due to aging

Implementation of functions such as updating are necessary to put the above measures into practice. Because of risks such as abnormal behaviors of IoT components caused by the defect of the update function, decrease in performance of IoT components during updates or shortage of network bandwidth due to simultaneous updates by a number of IoT components, sufficient consideration is necessary. Besides updating, the dynamic configuration change and extensibility should be also considered in development to maintain Safety/Security with the passage of time.

(3) Example measures

(i) Functions to maintain Safety/Security by updates, etc.

1) Functions for updates, etc.

- For IoT components, the automatic/manual, direct/remote update function for improving usability, adding functions, fixing bugs and renewing secret keys, etc. should be implemented.
- Methods to use encryption and digital signature for updating files may be considered to disallow spoofing with the use of update functions.
- In some cases, the update function is used as the measures to limit the functions of devices whose security measures become deteriorated.

2) Reducing the impacts of updates, etc.

- When the impacts to functions and safety due to performance degradation and shortage of network bandwidth during updates are expected, using methods to enable update date/time settings and bandwidth control may be considered. In addition, when IoT components are operating in collaboration with other IoT components, designing the update procedures may be considered.
- Methods to enable an automatic version downgrade if IoT components stop operating correctly after the automatic updates may be considered.
- In order to prevent performance degradation after the updates, ensuring the execution of prior verification may be considered.
- Prevent virus contamination during updates. When updating using a USB device, thorough checking of the USB device should be performed. For components that are generally not connected to networks, security measures may not be implemented, and thus connecting them to networks only for updates is not desirable.

3) Identifying the locations where IoT components are used, etc.

- In order to rapidly and reliably respond to serious defects found in IoT components even after a considerable time has passed after their market release, designs to identify the locations where IoT components are used, display messages, and terminate their operations with the user’s consent may be considered.
- In consideration of cases where IoT components are sold as secondhand, designs to obtain the owner’s consent again when detecting the movement of locations where IoT components are used.

4.5 Protecting with relevant parties

In order to protect the Safety/Security of the Smart-society, the cooperation of not only the developers of devices and systems but also various parties including relevant business operators and general users is necessary. Relevant business operators include maintenance/operation staff, retailers, integrators that provide services by combining the devices and systems of different companies and sectors, and their corporate users. Cooperating with these relevant parties to obtain information and providing them with information are necessary for achieving the Safety/Security of the Smart-society.
This chapter explains three guidelines to be addressed for protecting the Safety/Security of the Smart-society with relevant parties.

[Guideline 15] Identifying IoT risks and providing information after the market release

(1) Points

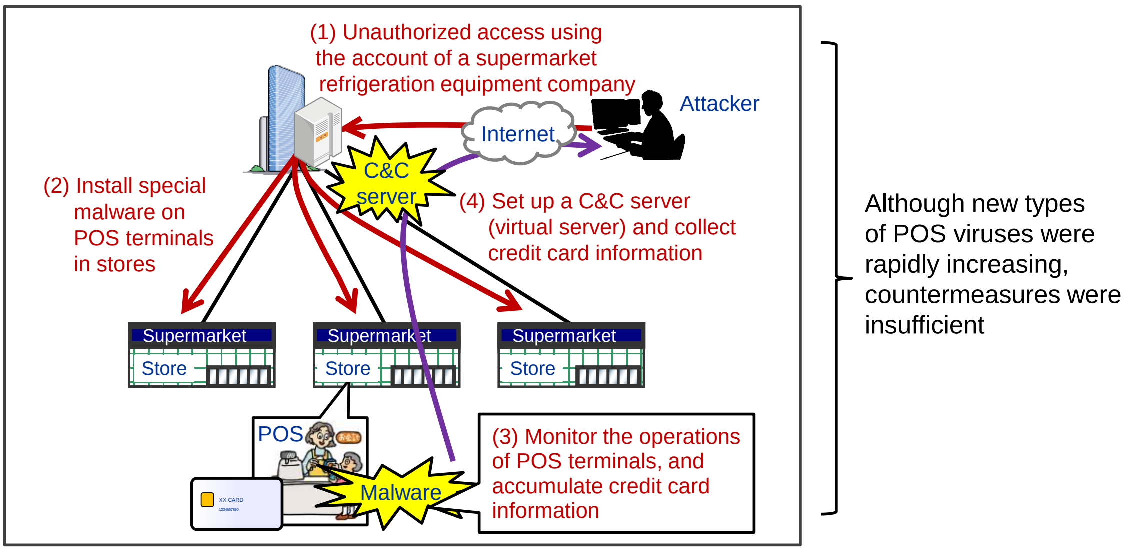
(i) Collect/analyze the latest information on defects, vulnerabilities, accidents, and incidents at all times.

(ii) Provide risk information within the company, to relevant business operators, and on information provision sites as required.

(2) Description

In the Smart-society, there are cases that unexpected problems may occur after the market release.

In 2013, the POS terminals of a large retail chain in the U.S. were infected by a virus, and the credit/debit card information of 40 million persons and the customer information of 70 million persons were leaked (Figure 4-33). Although new types of POS viruses had been rapidly increasing from around 2011, measures might have been insufficient [35]. In addition, there were cases where serious vulnerabilities were found in widely used open source software (hereinafter "OSS"), including Heartbleed in 2014. In cases where security threats affect safety functions in particular, unexpected accidents may be caused.


(1) Unauthorized access using the account of a supermarket refrigeration equipment company
Attacker
Internet
C&C server
(2) Install special malware on POS terminals in stores
(4) Set up a C&C server (virtual server) and collect credit card information
Supermarket
Store
Supermarket
Store
Supermarket
Store
POS
XX CARD
Malware
(3) Monitor the operations of POS terminals, and accumulate credit card information
Although new types of POS viruses were rapidly increasing, countermeasures were insufficient

Source: Prepared based on "Threat Case Studies of Consumer Devices", CCDS

Figure 4-33 Example of attacks against POS terminals

In order to rapidly respond to these problems, developers should continue to collect/analyze information and provide information as required. Feedbacks from users are useful for the developers to recognize the usage situation and to identify the cause of the failure, therefore they should be positively utilized to improve "Quality in Use".

Because there is a limitation to what the developers can do in collecting information and applying the countermeasures, the cooperation with relevant parties is necessary.

(3) Example measures

(i) Examples of collection/analysis of information on accidents and incidents

· Collect/analyze information on accidents and incidents that occurred around the world.

- Examine the impacts on own products based on the information collected.
- If related problems are found to exist in own products, examine also the external impacts to connected entities.
- Select the information for which external impacts are expected that require information provision.

In addition to the above, mechanisms to feed back to developers the information on accidents and incidents identified by relevant parties in contact with on-site staff are also important.

· For information collection, the following can be used as reference: For analysis, see 4.2.

Table 4-6 Cases of information provision sites, etc.

Name		Outline
Domestic cases	Japan Computer Emergency Response Team (JPCERT) Coordination Center	JPCERT Coordination Center is an independent organization that has been collecting information on threats and responding to them as an international security emergency response organization for a long time. It collects/publishes vulnerability information in cooperation with the IPA. -Vulnerability information portal site (JVN: Japan Vulnerability Notes) [36] -Vulnerability information database (JVN iPedia) [37] With the aim of facilitating the wide use of information on measures against vulnerabilities that are found every day through accumulation, vulnerability information posted on JVN and vulnerability information disclosed both domestically and overseas are accumulated in a database and made widely available to the public. Vulnerability information for OSS is also available.
	ISAC (Information Sharing and Analysis Center)	The main activities include sharing industry-specific information on incidents, threats, and vulnerabilities, and information exchange between the members.
	IPA: 10 Major Security Threats	Major threats that occurred each year are disclosed by experts to alert the public [38].
Overseas cases	Black Hat	Black Hat, an international conference on computer security, has been publishing the cases of the most advanced attacks and study cases of measures [39].
	Cyber Treat Alliance	Cyber Treat Alliance, an organization established by a U.S. security company, has been sharing the latest information and publishing white papers, etc. [40]

· For OSS, individual organizations consisting of developers and relevant business operators (OSS communities) exist, in which bug information is shared and patches are created. Information can be found on the communities' websites.

(ii) Examples of provision of information on the risks due to connections

Provide/share information that are collected and analyzed in (1) as risks, as required.

- Implement the above by assigning responsible persons in charge within the company.
- When externally providing/sharing information, care must be taken.

As example measures, the following may be considered.

1) CSIRT (Computer Security Incident Response Team)

The main activities include emergency response to computer security incidents and taking measures. In some cases, a CSIRT is established within the company to receive reports within the company or from customers, perform emergency response, and collaborate with the CSIRTs of other companies in taking measures.

2) Information provision to Japan Computer Emergency Response Team (JPCERT) Coordination Center and ISAC

See (i).

3) Cautions in externally providing/sharing information

･Selection of parties to provide information to

Determine the range of impacts, such as connected entities and users.

･Methods and timing of providing information

Making public the information on risks for which there is no prospect for countermeasures may cause further risks such as zero-day attacks, and therefore the methods and timing must be carefully discussed. The abovementioned ISAC can also be used for sharing information across companies within industries.

[Guideline 16] Informing relevant business operators of the procedures to be followed after-market release

(1) Points

(i) Inform the procedures that need to be followed in deployment, operation, maintenance, and disposal to the staff and external business operators directly involved in them.

(2) Description

IoT components are used for a long time after market release in a series of processes such as deployment, operation and maintenance. In addition, they may be re-used, but will eventually be disposed. During these phases, Safety/Security issues such as the following are assumed:

- At deployment
  - Installation in environments without firewalls
  - Login passwords not set
- At operation/maintenance
  - Compromise of security functions due to aging, and newly discovered vulnerabilities
  - Password settings that can be easily guessed by others, and software updates not applied
  - The support period not notified, and continued use after expiration of the support period
  - Occurrence of failures that are difficult to recover from, even with recovering functions designed for the systems and devices
- At reuse/disposition
  - Contained personal/confidential information not deleted
  - Countermeasures against transfer or second-hand sales of illegally modified IoT components

The above issues are difficult to deal with using only measures in the planning, design, and development phases, and therefore requests must be made to relevant business operators involved in the deployment, operation, maintenance, and disposal phases for their response. Figure 4-34 shows examples of product/service life cycles and the scope of the Guidelines

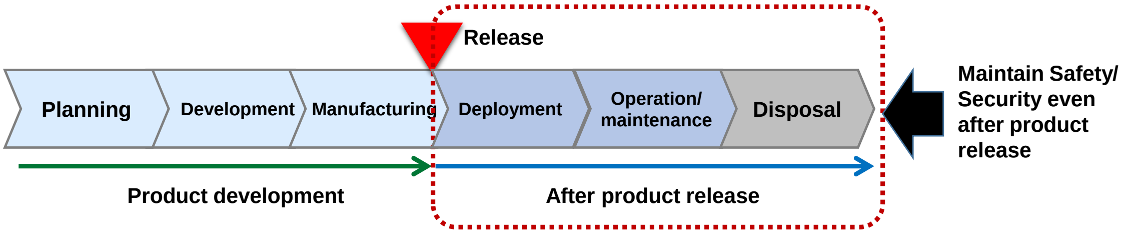


Figure 4-34 Examples of product/service life cycles

(3) Example measures

(i) In order to maintain Safety/Security even after market release, discuss the following measures and make them known directly to the staff and external business operators involved in them.

1) Measures at deployment

･Responding to installation in environments without firewalls

- Make known the requirements to be followed when connecting to external networks (installation in environments inside firewalls, etc.)

･Responding to login passwords not set

- Inform that IDs/passwords should be changed from the initially set values

2) Measures at operation/maintenance

･Responding to the compromise of security functions due to aging, and newly discovered vulnerabilities of IoT components

- Promote the use of software update functions (see Guideline 14)

･Responding to password settings that can not be easily guessed by others, and software updates not applied

- Conduct operational training, and request for strict management
- Request for settings to enable automatic update functions

･Responding to the support period not notified, and continued use after expiration of the support period

- Notify the support period, and provide advance notice and notification of the expiration of the support period
- Post the information on the company website, and display messages on the devices and systems
- In cases where there can be significant risks when devices, etc., continue to be connected and used after the expiration of the support period, technically restrict connections to networks

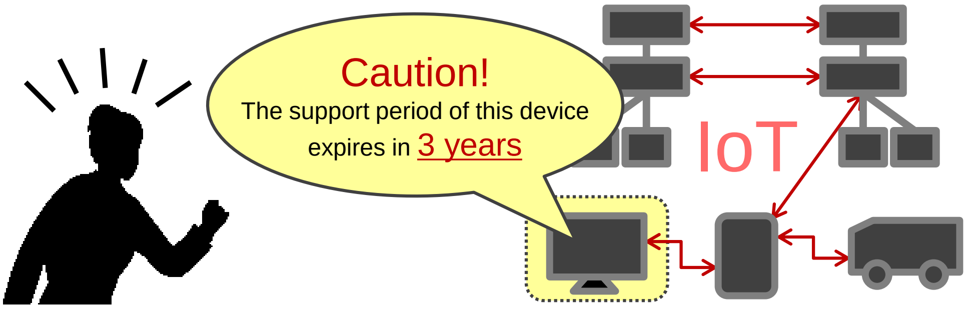


Figure 4-35 Notification of the support period

· Responding to failures that are difficult to recover from even with recovering functions designed for the systems and devices

- Request for discussion on the reconfiguration of software and cryptographic keys, etc., from the management system
- Request for discussion on the use of manual recovery procedures when systematic recovery is not possible
- Request for discussion on the procurement methods and deployment of spare devices, parts, and systems

3) Measures at reuse/disposition

· Responding to contained personal/confidential information

- Keeping everyone informed that personal/confidential information is contained in the IoT components
- Description of the risks of undeleted data
- Installation of the data-deletion functions (see Guideline 8)

· Countermeasures against transfer or second-hand sales of illegally modified IoT components

- Notification of risks such as those caused by tampering with software, settings, user manuals, etc. to the second-hand sales companies and users
- Provision of the checking methods for tampering and the cleaning tools to the sales companies and users
- Guarantee for cleaning performed by the second-hand sales company using the cleaning tools

[Guideline 17] Making the risks caused by connections known to general users

(1) Points

(i) Notify general users that careless connections and unauthorized use not only affect the individual but also damage others or cause adverse impacts on environments.
(ii) Notify general users of the requirements to be followed for maintaining Safety/Security.

(2) Description

There are cases where general users attach unofficial adapters to home electrical appliances or alter infrared remote controllers to enable the remote control of home electrical appliances. Such connections increase the risks of unauthorized remote operations and abnormal behaviors.

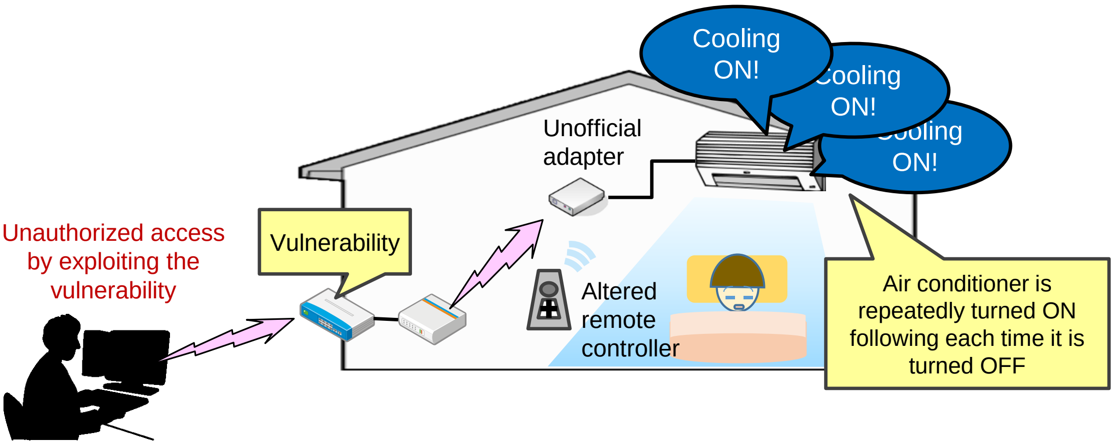

Cooling ON!
Cooling ON!
Cooling ON!
Unofficial adapter
Unauthorized access by exploiting the vulnerability
Vulnerability
Altered remote controller
Air conditioner is repeatedly turned ON following each time it is turned OFF

Figure 4-36 Examples of risks due to unauthorized alteration by general users

In addition, even if various measures are taken to reduce the risks to a tolerable level, there may still be hidden risks that can affect general users or there may be risks that could not be considered to exist at the time of product release but are increased with the passage of time (see Guideline 14). These facts need to be informed to general users. For instance, it is necessary to encourage general users to update their software against vulnerabilities of smartphones.

It is also necessary to inform general users that the Smart-society is convenient but also has risks, and ask them not to carelessly connect devices and systems, to understand the necessity of measures against the defects/vulnerabilities of IoT components, and to cooperate. Recognizing and analyzing the notification effect on general users, the notification method should be improved.

(3) Example measures

(i) Examples of making known the risks due to careless connections

1) Methods of providing information

- Display on the startup screens
- Describe the examples in manuals (information provision from developers and operators to general users)
- Describe in warranty cards
- Post on own websites

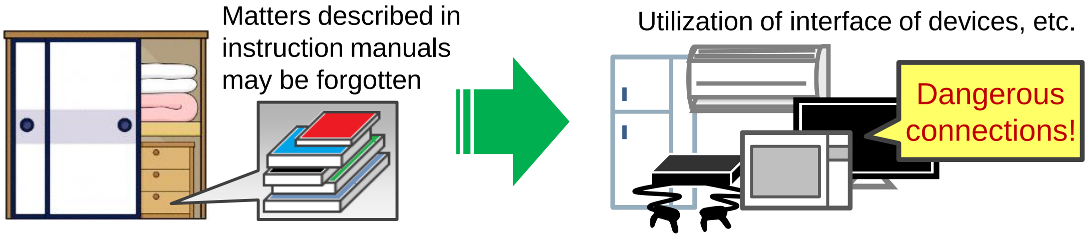

Matters described in instruction manuals may be forgotten
Utilization of interface of devices, etc.
Dangerous connections!

Figure 4-37 Warning using the user interfaces of devices and systems

2) Examples of the content of information to be provided

- Recommended connection methods (for which operations are guaranteed), etc.

(ii) Examples of making known the actions to be taken by general users

Developers should provide general users with information on matters requiring their cooperation and attention. Based on the recognition and analysis of the notification effect on general users, they should also turn the PDCA cycle to improve the notification method.

1) Methods of providing information

- Display on the startup screens
- Describe examples in manuals (information provision from developers and operators to general users)
- Post on own websites, etc.

2) Examples of the content of information to be provided

- Recommend the application of updates
- Automatic update functions, if available, are initially set to ON at product release
- Security settings, including wireless LAN (Wi-Fi, etc.) and security keys
- Recommend the setting of passwords that cannot be easily guessed by others
- Providing information about data-deletion functions as measures against leakage of personal/confidential information at reuse/disposal (see Guideline 8)

Chapter 5

Examples of Measure Technologies That Will Be Required in the Future

In the examples of measures of development guidelines in Chapter 4, technologically established measures are mainly described. In order to ensure the Safety/Security of the Smart-society, however, more advanced study is needed. This chapter describes the examples of measure technologies that are not technologically established at present, but are expected to be required in the future.

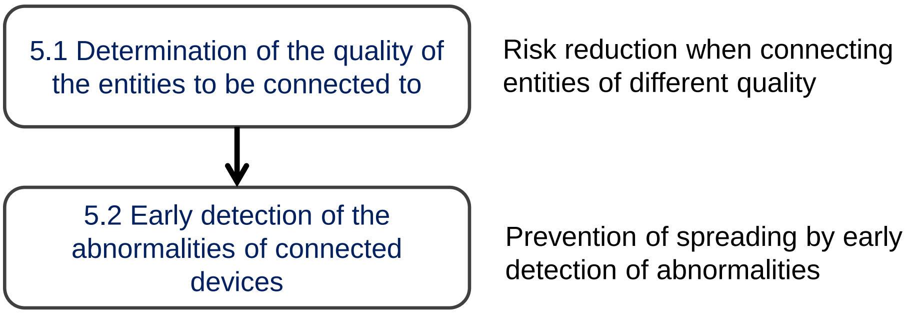

5.1 Determination of the quality of the entities to be connected to
Risk reduction when connecting entities of different quality
5.2 Early detection of the abnormalities of connected devices
Prevention of spreading by early detection of abnormalities

Figure 5-1 Flow of this chapter

5.1 Determination of the quality of the entities to be connected to

In the Smart-society, released IoT components and systems that had gone into service may be altered by service providers or users to enable usage and connections that are not assumed by manufacturers. In addition, as IoT components of different sectors can now be connected to each other, there are risks that expected quality levels cannot be maintained due to differences in their concepts and rules. Furthermore, there is a concern that, even under such circumstances, users may use them without being aware of the risks.

In order to reduce the risks due to connections with different entities, this chapter proposes measures to organize/exchange a set of information by following the procedures below to verify the quality of the entities to be connected to.

1) Organize a set of information to verify the quality of the entities to be connected to

2) Exchange/determine the set of information and notify the results at connection

Exchanging information with the entities to be connected to requires authentication of the entities concerned and establishment of secure connection methods, but they assumed that they have been "implemented" here.

(1) Organization of a set of information for verifying quality

Information on safety, security, and reliability must be able to be exchanged/verified. Examples of information that can be used as the set of information are as follows:

- Security level (EAL, SAL (EDSA), etc.)
- Functional safety level (SIL, ASIL, PL, etc.)
- Information provided by certification bodies within the industry
- Operation rate/resilience
- Systems of the company (for acquiring certifications for relevant standards, etc.), quality assurance information

As for the range for exchange of a set of information, it should be able to be exchanged within the same company, within certain sectors, and even between different sectors. In the case of exchanging it between different sectors, however, specifying common/universal exchange information is difficult, and therefore what information should be exchanged between the products and services to be connected needs to be discussed and specified in advance.

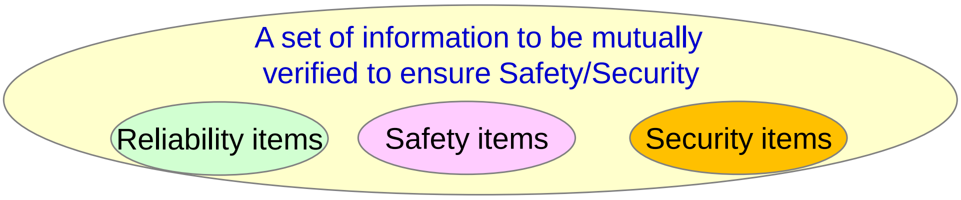

A set of information to be mutually verified to ensure Safety/Security
Reliability items
Safety items
Security items

Figure 5-2 Image of a set of information

(2) Exchange/determination of a set of information and notification of the results

Methods for exchanging a set of information and verifying the quality for connecting IoT components include the following two:

- Static information exchange: A set of information is verified off-line (at device and parts selection)
  - For IoT components available in the market, manually verify the quality using a set of information, determine whether connections can be made, and the range of services to be provided, and store the results list on servers.
  - When IoT components are connected to others, the results list on servers is looked up to determine whether connections can be made, and the range of services to be provided.
- Dynamic information exchange: A set of information is verified on-line (at connection)
  - A set of information is stored on the IoT components themselves, and exchanged when making connections with others to verify the quality of the entities to be connected to and autonomously determine whether connections can be made, and the range of services to be provided.

In either method, the results of the determination are notified to others, the set of information is exchanged, and the results are recorded. For examples of these cases, see Appendix A3.

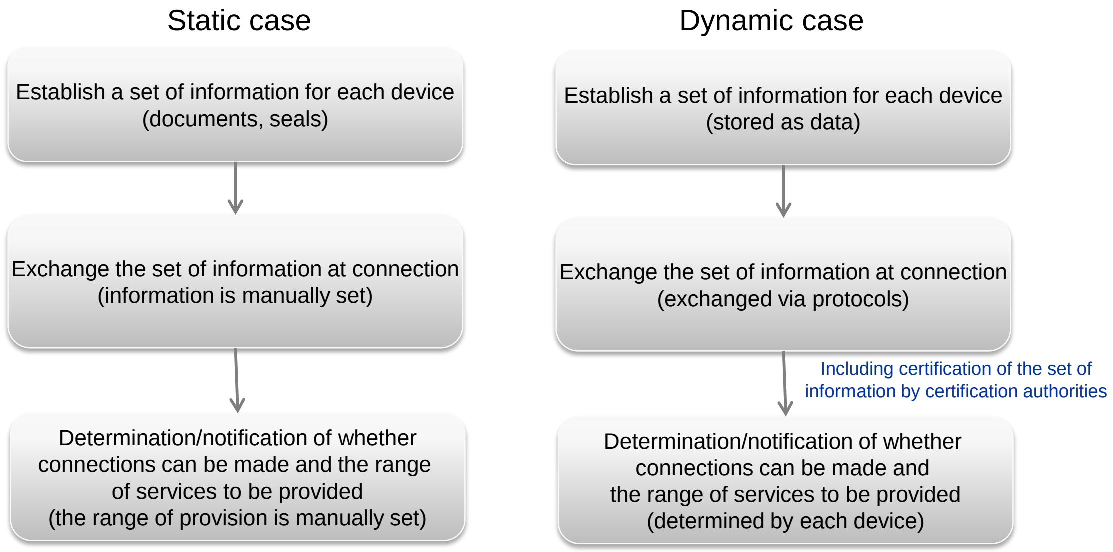

Static case
Establish a set of information for each device (documents, seals)
Exchange the set of information at connection (information is manually set)
Determination/notification of whether connections can be made and the range of services to be provided (the range of provision is manually set)
Dynamic case
Establish a set of information for each device (stored as data)
Exchange the set of information at connection (exchanged via protocols)
Including certification of the set of information by certification authorities
Determination/notification of whether connections can be made and the range of services to be provided (determined by each device)

Figure 5-3 Static/dynamic information exchange/determination

5.2 Detection of abnormalities of the devices connected

In order not to cause trouble in other entities that are connected, each IoT component must protect the objects to be protected (means for not becoming a victim) and prevent its abnormalities from spreading (means for not becoming a perpetrator). More concretely, mechanisms for detecting at an early stage and responding to the situations where IoT components are running out of control and continuing abnormal communications to increase network load, or IoT components are infected by malware and spreading it to others are important.

In the Smart-society, small abnormalities can spread/accumulate to cause significant impact on the entire IoT. However, small abnormalities contained in an IoT component are likely to be overlooked. In addition, in a scenario in which large-scale reorganization often takes place, such as factory lines, formulating the criteria for determining abnormalities requires great effort.

For this reason, methods to automatically formulate the criteria for determining abnormalities by recording normal operations and then perform abnormality detection by comparing them with the actual operations are assumed here.

(1) Recording normal operations

Normal operations can either be recorded statically in advance or dynamically. For static recording, methods to manually record normal operations may be considered for use. For dynamic recording, methods to continuously record normal operations and recognize normal states through machine learning, etc., may be considered.

As for the range of operations to be recorded, either operations of a single IoT component or operations of multiple IoT components can be recorded.

(2) Comparing with normal operations

Detection of abnormalities

- Detect abnormalities by comparing with the range of values of normal operations. In the case of a single IoT component, check whether the operations fall within the range of normal operations. In the case of multiple IoT components, check also for abnormalities in their mutual relationships.

Detection of predictive signs

- In the case of events that are not abnormalities yet but are expected to develop into abnormalities in the near future, the spreading of abnormalities can be effectively prevented by detecting and responding to them even if they fall within the range of normal operations.

- For the detection of predictive signs, methods to detect state changes using machine learning, etc., may be used. For instance, methods to check changes in the trends of periodic states, changes in the trends of state transitions, or changes in the relationships of the states of multiple IoT components with strong correlation may be considered.

For examples of the detection of abnormalities, see Appendix A4.

Conclusion

In the Smart-society, there are concerns that risks that not only consumers but even developers cannot assume may be caused by all sorts of "things," including home electrical appliances and automobiles, being connected to networks. Furthermore, the risks of devices and systems include those that can spread extensively through connections, and those that can harm people's lives and property. They must therefore be promptly dealt with. For this reason, Software Reliability Enhancement Center, Technology Headquarters, Information-technology Promotion Agency (IPA/SEC) compiled the Safety/Security matters to at least be considered by companies involved in devices and systems to serve as guidelines.

Formulating such guidelines under the circumstances where the IoT itself is still developing seemed difficult, but focusing on the Safety/Security of devices and systems comprising the IoT (IoT components) and lengthy deliberations by experts at WG enabled the compilation of the Development Guidelines. We hope the Development Guidelines can be of some help in the efforts of developers of devices and systems to deal with the risks of the Smart-society.

We intend to revise the Development Guidelines as required in the future while keeping track of the situation, such as the trends in relevant standards, development of IoT services, and emergence of unknown risks. Readers are advised to continue to pay attention to the revision status of the Development Guidelines.

Finally, we would like to express our appreciation to WG members who have provided tremendous support in the formulation of the Development Guidelines.

Appendix A

A1. How to use the Development Guidelines (checklist)

This section compiles the common matters to at least be considered for making connections within the industry and between industries in safe and secure as development guidelines/points toward the age of IoT, in which various types of businesses are connected and new services and businesses are created. An example of the checklist for effectively using the Development Guidelines is given below.

Table A-1 Example of checklist for the Development Guidelines

Guideline	Point	Discussion (Done/Yet)	Act (Done/ Restricted/ Warning/ Excluded)	Remark
［Guideline 1］ Formulating the basic policies for Safety/Security	(i) Managers shall formulate the basic policies for the Safety/Security of the Smart-society, make them known within the company, continuously evaluate their achievement status, and review them as required.			
［Guideline 2］ Reviewing systems and human resources for Safety/Security	(i) Establish systems and environments for discussing the Safety/Security issues of the Smart-society in an integrated manner.			
	(ii) Secure/develop human resources (developers and maintenance staff) for that purpose.			

Restricted: Not done yet but supposed to be taken measures hereafter.
Warning: Not done yet and supposed not to be taken measures hereafter either.

A2. Procedures for deriving development guidelines

In formulating the development guidelines, the risks were analyzed by arranging the patterns of connections organized in Chapter 3 on the horizontal axis and examples of the IoT risks on the vertical axis. However, covering all combinations of every pattern requires an enormous number of risk examples. Risk examples are therefore derived in such a way that an element of each pattern is included in at least one of the risk examples. There are not many cases for the IoT, and the number of risk examples is also small. Because there are not enough risk examples for the existing IoT, some risk examples are assumed. Figure A-1 shows an image of the organization.

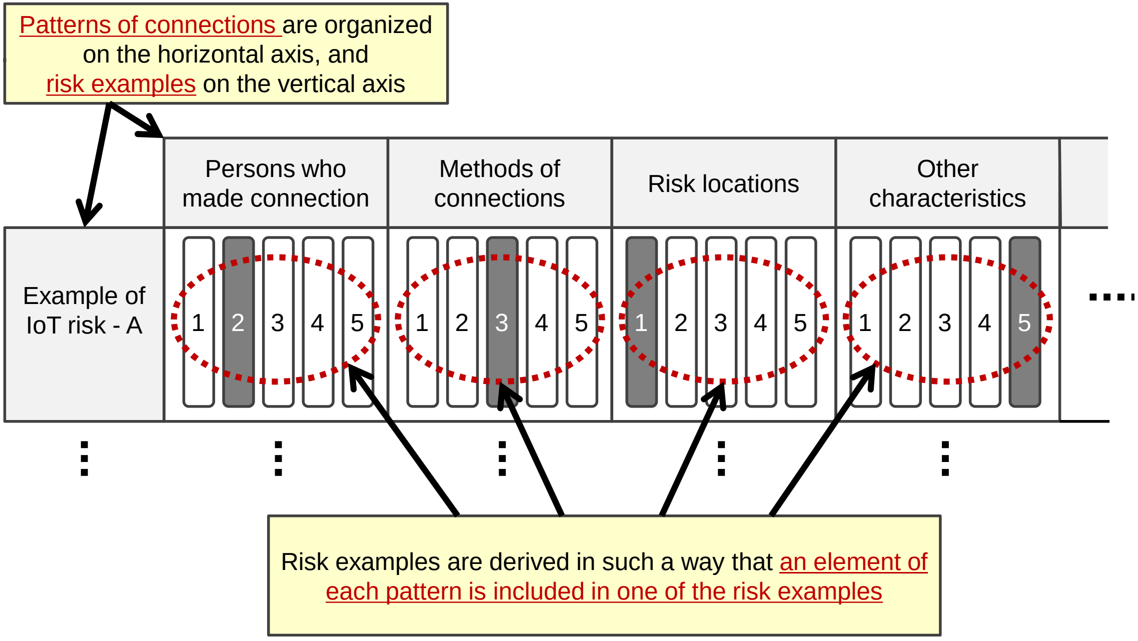

Patterns of connections are organized on the horizontal axis, and risk examples on the vertical axis
Persons who made connection
Methods of connections
Risk locations
Other characteristics
Example of IoT risk - A
1 2 3 4 5
1 2 3 4 5
1 2 3 4 5
1 2 3 4 5
....
Risk examples are derived in such a way that an element of each pattern is included in one of the risk examples

Figure A-1 Organization of the patterns of connections and IoT risk examples

Next, the causes of each risk example are analyzed, and the IoT-focused issues/problems are organized. Table A-2 shows the results.

For the “IoT-focused issues/problems,” those caused by the IoT characteristic that various things are “connected” are included; for example, the problem that “installation in a closed environment protected by firewalls was assumed” and the issue that “Safety/Security must be maintained even with unexpected connections.” In addition, there are many issues that can hardly be assumed by anyone other than security engineers, such as attacks from USB ports for maintenance use, offenses by insiders, and the unauthorized use of update functions. There are cases where security threats lead to safety hazards, clarifying the necessity of Safety/Security measures.

Table A-2 IoT risk analysis table

WHAT		WHO						HOW					WHOM					WHERE					WHEN					WHY	
What happened?		Who made the connections?						How were the connections made?					What was harmed?					Where did it happen?					At what stage did it happen?					Why did it happen?	
Device type	Example of risk	Manufacturer and relevant companies	Service provider	User (intended)	User (improper connection)	Attacker	Incidental	Direct	Indirect	Fixed	Dynamic	Combined	IoT function	Intrinsic function	Data	Health and property	Others	Ordinary-use I/F	Maintenance I/F	Informal I/F	Contained	Physical contact	Planning/design/development	Manufacturing/release	Operation (provider)	Operation (user)	Disposal/recycle	Main cause	IoT-focused issue/problem
Multifunction printer	Data accumulated on multifunction printers, which were not assumed to be connected to the Internet, were open to public view. The initial passwords were also disclosed on documents.	○								○					○				○							○		Insufficient assumptions regarding the Internet connection Insufficient request for changing of the initial passwords Disclosure of documents containing the initial passwords	Installation in environments protected by firewalls was assumed.
ATM	Cash was withdrawn by illegally obtaining physical keys, opening the maintenance doors of ATMs to connect cellphones, etc., and sending e-mails to the cellphones.					○		○			○					□ (Cash)			○			○				○		Insufficient understanding/sharing of attack cases Insufficient access management of maintenance doors Open access to maintenance I/F Virus infection to ATM terminals	Assumptions of risks were insufficient that maintenance doors may be opened by attackers, and cellphones, etc., may be connected to USB ports for maintenance purposes.
IoT in general	(Assumed case) While IoTs are connected to each other, IoTs not assumed to be connected are also connected, resulting in information leakage.						○								○			○						○				Insufficient management of individual IoTs Unavailability of functions to understand the whole context of connections	Safety/Security needs to be maintained even when there are unintended connections.
IoT devices	(Assumed case) While tampering with a device found and picked up, remote functions were invoked and caused damage to user's property.				○						○			○		○		○							○			Insufficient user authentication functions Insufficient verification of questionable operations	Safety/Security needs to be considered even for unexpected uses by finders
Automotive	Services to remotely lock the doors or sound the horns of automobiles of users with delayed loan payments were used by a retired employee in an unauthorized manner		○							○				○				○							○			Insufficient account management Insufficient mechanisms to prevent abnormal use	Internal offenses were not assumed.
In-vehicle devices	The handles and brakes of automobiles were remotely controlled by gaining access to in-vehicle devices through mobile networks, altering firmware on chip, and sending control instructions to in-vehicle networks	○				○			○		○			○					○	○						○		Insufficient access management of mobile networks No protection for communications between smartphones and in-vehicle devices No authentication for in-vehicle device permissions No encryption of update files Insufficient access management of automobile control systems	• The things to be protected were not protected. • Assumptions of the impacts that security problems may have on safety were insufficient. • Security of remote update functions was insufficient.
IoT devices	Devices were infected by a virus during inspection at factory, but were released and connected to the IoT to spread the infection.			○				○									□ (Product)				○			○				Insufficient security inspection at factory Unavailability of virus check functions Unavailability of autonomous control functions under abnormal conditions	Considerations not to affect other connected entities were insufficient.
IoT devices	(Assumed case) When a disposed and recycled device was connected to a network, it was connected to servers because the IoT settings of the former owner were not deleted.				○					○	○						○	○									○	Settings not deleted at disposal/recycle	Measures to be taken at disposal/recycle need to be discussed.
The IoT in general	(Assumed case) At a time of disaster, the IoTs for disaster control went live all at once to cause network congestion, disabling use of the IoTs.						○				○	○	○	○				○							○			Insufficient understanding of the IoT by the entire society	Understanding and responding to the current own and surrounding status is necessary.
POS terminals	Payment information of customers was collected in an unauthorized manner by gaining unauthorized access to the central server and infecting POS terminals with viruses.		○			○			○	○					○			○							○			Insufficient understanding/sharing of attack cases Insufficient access management of the central server Virus infection to POS terminals	Measures were not taken even though attacks on devices related to own company were increasing.
Home electrical appliances	(Assumed case) When a user relayed/extended communications of operating devices for home electrical appliances and remotely operated the home electrical appliances, family members were involved in an accident.			○						○						○		○								○		Insufficient understanding of the risks by the user	The risks of the Smart-society need to be made known to users.

Based on the analysis above, the "direction of measures" was derived. The "direction of measures" here indicates the direction to respond to the IoT-focused issues/problems that are derived and organized based on the causes of the actual damage cases and the assumed cases. FigureA-2 shows an image of this process.

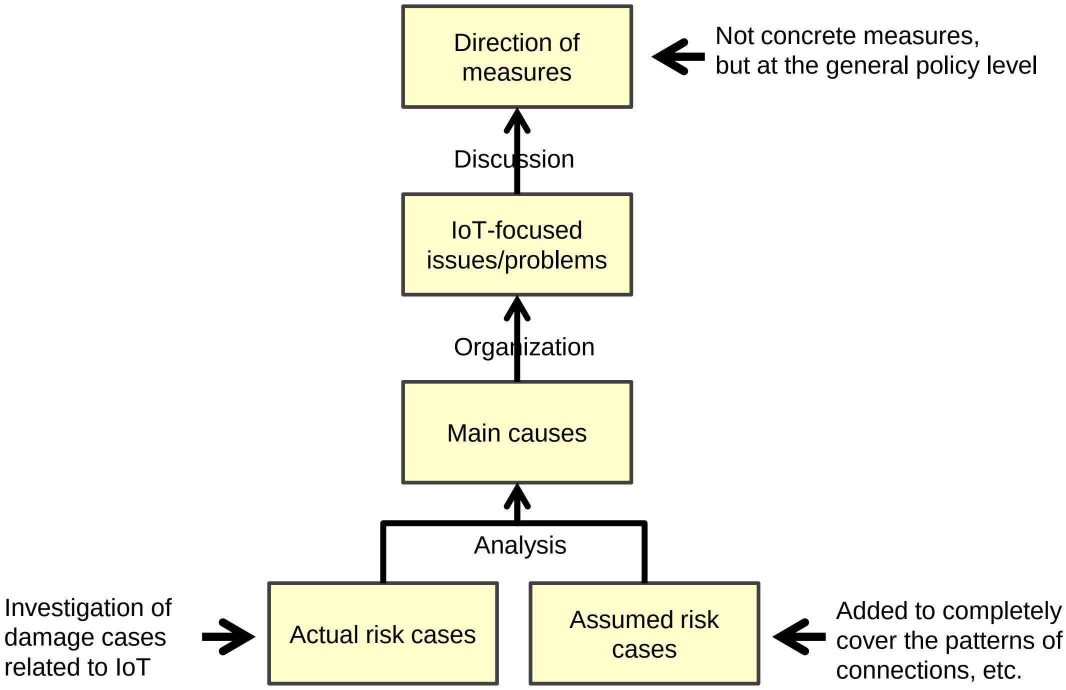

Direction of measures
Not concrete measures, but at the general policy level
Discussion
IoT-focused issues/problems
Organization
Main causes
Analysis
Investigation of damage cases related to IoT
Actual risk cases
Assumed risk cases
Added to completely cover the patterns of connections, etc.

Figure A-2 Image of the process for deriving the "direction of measures"

As shown in the figure above, a bottom-up approach was used to derive the "direction of measures." Table A-3 shows the results.

Table A-3 Derivation of the direction of measures from the IoT-focused issues

WHAT		WHY	
What happened?		Why did it happen?	
Device type	Example of risk	Main cause	IoT –focused issue/problem
Multifunction printer	Data accumulated on multifunction printers, which were not assumed to be connected to the Internet, were open to public view. The initial passwords were also disclosed on documents.	Insufficient assumptions regarding the Internet connection	Installation in closed environments protected by firewalls was assumed.
		Insufficient request for changing of the initial passwords	
		Disclosure of documents containing the initial passwords	
ATM	Cash was withdrawn by illegally obtaining physical keys, opening the maintenance doors of ATMs to connect cellphones, etc., and sending e-mails to the cellphones.	Insufficient understanding/sharing of attack cases	Assumptions of risks were insufficient that maintenance doors may be opened by attackers, and cellphones, etc., may be connected to USB ports for maintenance purposes.
		Insufficient access management of maintenance doors	
		Open access to maintenance I/F	
		Virus infection to ATM terminals	
The IoT in general	(Assumed case) While IoTs are connected to each other, IoTs not assumed to be connected are also connected, resulting in information leakage.	Insufficient management of individual IoTs	Safety/Security needs to be maintained even when there are unintended connections.
		Unavailability of functions to understand the whole context of connections	
IoT devices	(Assumed case) While tampering with a device found and picked up, remote functions were invoked and caused damage to user's property.	Insufficient user authentication functions	Safety/Security needs to be considered even for unexpected uses by finders
		Insufficient verification of questionable operations	
Automotive	Services to remotely lock the doors or sound the horns of automobiles of users with delayed loan payments were used by a retired employee in an unauthorized manner	Insufficient account management	Internal offenses were not assumed.
		Insufficient mechanisms to prevent abnormal use	
In-vehicle devices	The handles and brakes of automobiles were remotely controlled by gaining access to in-vehicle devices through mobile networks, altering firmware on chip, and sending control instructions to in-vehicle networks	Insufficient access management of mobile networks	• The things to be protected were not protected. • Assumptions of the impacts that security problems may have on safety were insufficient. • Security of remote update functions was insufficient.
		No protection for communications between smartphones and in-vehicle devices	
		No authentication for in-vehicle device permissions	
		No encryption of update files	
		Insufficient access management of automobile control systems	
IoT devices	Devices were infected by a virus during inspection at factory, but were released and connected to the IoT to spread the infection.	Insufficient security inspection at factory	Considerations not to affect other connected entities were insufficient.
		Unavailability of virus check functions	
		Unavailability of autonomous control functions under abnormal conditions	
IoT devices	(Assumed case) When a disposed and recycled device was connected to a network, it was connected to servers because the IoT settings of the former owner were not deleted.	Settings not deleted at disposal/recycle	Measures to be taken at disposal/recycle need to be discussed.
The IoT in general	(Assumed case) At a time of disaster, the IoTs for disaster control went live all at once to cause network congestion, disabling use of the IoTs.	Insufficient understanding of IoT by the entire society	Understand and responding to the current own and surrounding status is necessary.
POS terminals	Payment information of customers was collected in an unauthorized manner by gaining unauthorized access to the central server and infecting POS terminals with viruses.	Insufficient understanding/sharing of attack cases	Measures were not taken even though attacks on devices related to own company were increasing.
		Insufficient access management of the central server	
		Virus infection to POS terminals	
Home electrical appliances	(Assumed case) When a user relayed/extended communications of operating devices for home electrical appliances and remotely operated the home electrical appliances, family members were involved in an accident.	Insufficient understanding of the risks by the user	The risks of the Smart-society need to be made known to users.

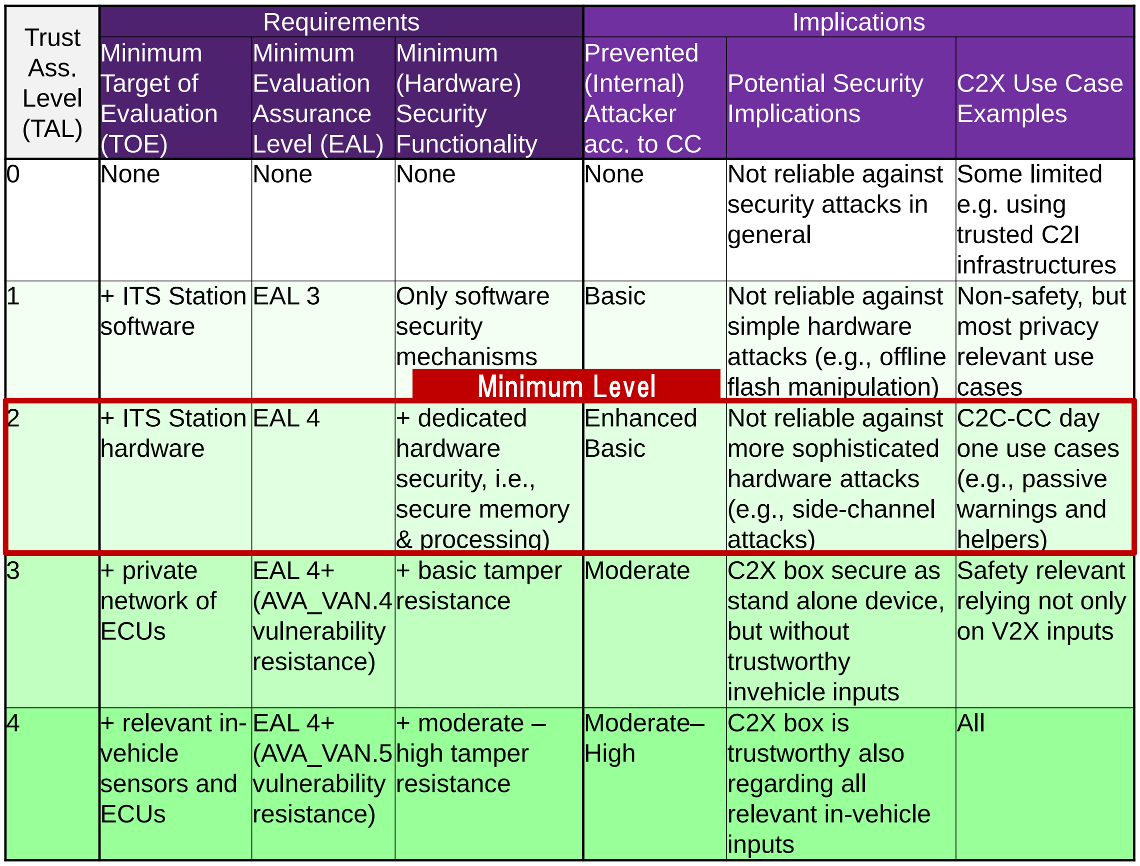
Intended readers Direction of measures	Issues for which measures should be taken		
	Manager	Developer	Maintenance staff
Assuming the risks caused by connections	Basic policies are not formulated.	Risks are not assumed.	
Understanding physical security risks		Risks are not assumed.	
Designing to enable safe and secure connections even with unknown entities		Unexpected usage and connections are not considered.	
Preparing for internal fraud and information leakage	Employee morale/training of employees and risk assumptions are insufficient.		
Verifying the consistency of Safety/Security design		Engineers on the two sides are not collaborating.	
Designing to enable both individual and overall protection		The things to be protected by the IoT and how to protect them are not clear.	
Maintaining Safety/Security even after the passage of time		Safety of update functions is insufficient.	Unauthorized use of update functions cannot be protected.
Designing so as not to cause trouble in other connected entities		Spread of own problems to others cannot be stopped.	Spread of own problems to others cannot be stopped.
Preparing for leakage of confidential information at disposal/recycle		Insufficient measures against leakage of confidential information at disposal/recycle	Insufficient measures against leakage of confidential information at disposal/recycle
Identifying/recording own status	Emergency response systems are not established.	Own problems are not detected.	Own problems are not detected.
Identifying/sharing information on the latest IoT risks			The latest risks are not identified.
Making the risks caused by connections known			The risks of connections made by users are not prevented.

A3. Examples of the determination of the quality of the entities to be connected to

As described in Chapter 5, quality determination will be required in the future. Examples of this process are presented here

(1) Dynamic quality determination using trust assurance levels of in-vehicle systems

Trust assurance levels of in-vehicle systems include TAL, proposed by C2C-CC. In car-to-car communications, verifying the authenticity of messages sent using certificates does not guarantee the integrity of the original data. TAL is defined as an indicator of the extent to which the information of the sender can be trusted, and is used to certify the level of security standards met by automobiles at the development phase. The levels 0 to 4 are defined in TAL, and the use of the trust levels certified by certification authorities to guarantee the sender in car-to-car communications is being discussed [41].



Trust Ass. Level (TAL)	Requirements			Implications		
	Minimum Target of Evaluation (TOE)	Minimum Evaluation Assurance Level (EAL)	Minimum (Hardware) Security Functionality	Prevented (Internal) Attacker acc. to CC	Potential Security Implications	C2X Use Case Examples
0	None	None	None	None	Not reliable against security attacks in general	Some limited e.g. using trusted C2I infrastructures
1	+ ITS Station software	EAL 3	Only software security mechanisms	Basic	Not reliable against simple hardware attacks (e.g., offline flash manipulation)	Non-safety, but most privacy relevant use cases
2	+ ITS Station hardware	EAL 4	+ dedicated hardware security, i.e., secure memory & processing)	Enhanced Basic	Not reliable against more sophisticated hardware attacks (e.g., side-channel attacks)	C2C-CC day one use cases (e.g., passive warnings and helpers)
3	+ private network of ECUs	EAL 4+ (AVA_VAN.4 vulnerability resistance)	+ basic tamper resistance	Moderate	C2X box secure as stand alone device, but without trustworthy invehicle inputs	Safety relevant relying not only on V2X inputs
4	+ relevant in-vehicle sensors and ECUs	EAL 4+ (AVA_VAN.5 vulnerability resistance)	+ moderate – high tamper resistance	Moderate–High	C2X box is trustworthy also regarding all relevant in-vehicle inputs	All

Source: S. Goetz and H. Seudié: "Operational Security," C2C-CC 2012

Figure A-3 Trusted Assurance Level being discussed at C2C-CC

(2) Dynamic quality determination using certification information in the FA sector

Examples of quality determination within a sector include dynamic determination based on certification information conducted by IPA/SEC using industrial robots (hereinafter “robots”) In this case, the determination methods that take into consideration the mixture of robots that have certification information and those that do not were adopted.

1) Risks of using devices of uncertain quality

Even in those environments where robots are used, using devices from multiple vendors is becoming popular, increasing the likelihood that low-quality devices are connected to the systems ordered. Cases in which these-low-quality devices affect the system and increase Safety risks are assumed and dealt with by not connecting low-quality robots.

2) Avoiding Safety risks due to devices of uncertain quality

Public institutions that certify the quality of robots and publish certification information are assumed. Certification information issued by the said institutions is embedded in robots as a set of information, and used for dynamic determination at connection. In actuality, there are newer versions of robots that support the above, and older versions of robots that do not. It is therefore dealt with as follows:

- Older versions

Manually store certification information in a reserved area in robot identification information within robot-specific information, which is the input data.

- Newer versions

Store certification information in a reserved area in robot identification information by firmware update functions of robots. When establishing connections with robots, integrated robot controlling applications check the existence of certification information of robots if robots are of newer versions. If certification information does not exist, integrated applications output errors to logs, disable robot operations, and terminate the entire system.

In this practical case, robots of older versions were used, and manually stored certification information was verified.

Case where robots with a set of information are connected

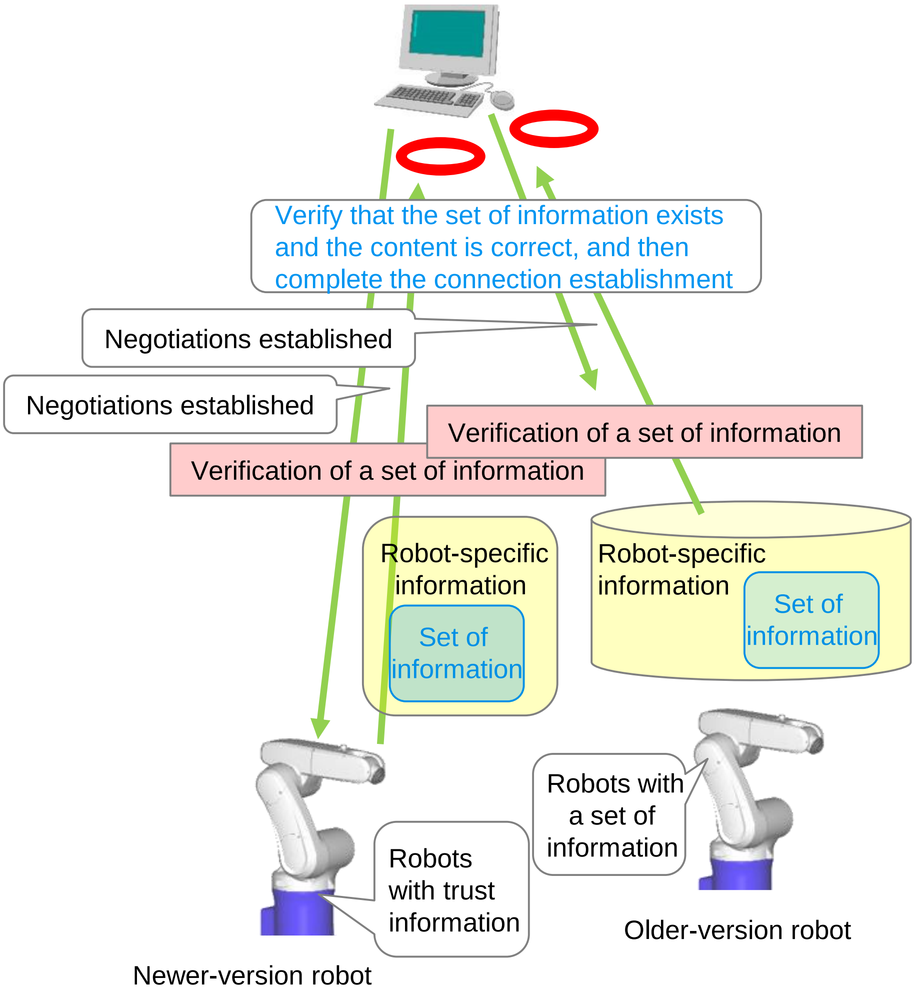

Verify that the set of information exists and the content is correct, and then complete the connection establishment
Negotiations established
Negotiations established
Verification of a set of information
Verification of a set of information
Robot-specific information
Set of information
Robot-specific information
Set of information
Robots with a set of information
Robots with trust information
Older-version robot
Newer-version robot

Figure A-4 Determination of robot connections using a set of information on quality

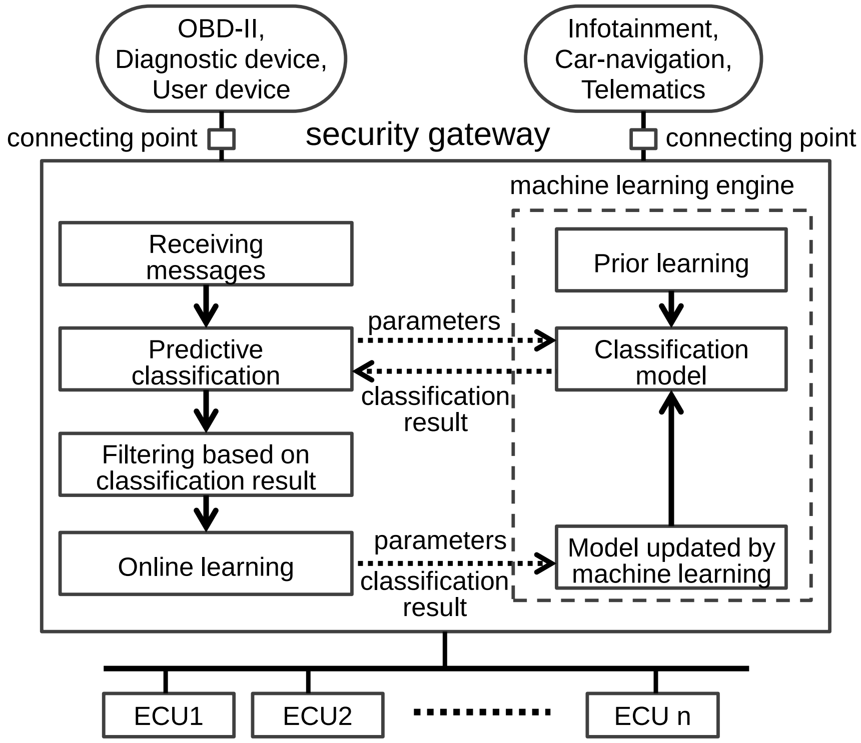
A4. Examples of the detection of abnormalities of connected devices

As described in Chapter 5, the detection of abnormalities of connected devices will be required in the future. Examples of this process are presented here.

(1) Detection of abnormalities by dynamically generating rules using machine learning in security gateways on in-vehicle LANs

For in-vehicle LANs, there are many study cases of intrusions from outside through in-vehicle devices, such as car navigation systems and telematics terminals, and of attacks made by connecting unauthorized devices. In recent years, there has been a trend to equip gateways on in-vehicle LANs with authentication functions. However, maintaining the security functions of automobiles that are likely to be used for a long time is difficult.

In these study cases, filtering functions based on dynamic rules using machine learning are established on gateways on in-vehicle LANs to detect external attacks. More concretely, initial rules are generated from normal traffic (a set of messages) on in-vehicle LANs, and rules for detecting attacks are generated from the traffic that includes attack messages. Furthermore, the detection rate and the false detection rate of attack messages are improved by dynamically updating the rules using machine-learning algorithms.



Source: Tomohiro Date, Hiroshima City University and Hiroyuki Inoue, CCDS: "Detection of abnormalities by dynamically generating rules using machine learning in security gateways on in-vehicle LANs," SCIS2016

Figure A-5 Operations of security gateways

This study is expected to enable the detection of attacks, even if the patterns of attacks are changed, by dynamically updating the rules by machine learning. In addition, the issue that strengthening attack detection increases the possibility of falsely detecting normal messages as attacks can also be used as a reference for other measures.

(2) Detection of abnormalities by comparing with typical operation patterns in the FA sector

There is a demonstration experiment conducted by the IPA/SEC to suppress abnormal operations by detecting abnormal states of industrial robots.

Data that can be transmitted between robots and cell control PCs is becoming more and more complex every year, and connections with systems and other devices can be made more flexibly through networks. On the other hand, the risks of generating wrong data due to operational errors, application defects, etc., are increasing. In the demonstration experiment, a mechanism for detection abnormalities and suppressing abnormal operations was achieved in a relatively easy manner by implementing a measure in which the patterns of normal robot operations are recorded, and if a deviation of the actual operation from the normal patterns is detected, it is recognized as an abnormal state and the operation of the robot concerned is terminated.

1) Detection of abnormal states of robot controlling applications

In cases where cell control PCs are used to control robots, serious problems may be caused if instructions to move to wrong teaching points (coordinate data) not in the existing sequence are made due to defects in cell controllers (by human operational errors, viruses, etc.), or the content of teaching points of robots are altered due to defects in applications other than cell controllers, etc.

Measures were therefore taken to prevent the occurrence of serious problems by monitoring the teaching points output by robot controlling applications, and promptly detecting the instructions of unexpected operations made to robots, if any, and terminating the robot control as required.

2) Measures for detecting abnormal states of robots

For the detection of abnormal operations, monitoring the following three states may be considered:

- Teaching points of robots
- State transitions of robots
- Timing in the time axis of controlling multiple robots

This practical case was dealt with by monitoring the teaching points output by robot controlling applications, and if values different from those of normal operations are detected, recognizing them as abnormal values and terminating the robot operations.

(1) In the preparation phase, collect a series of teaching point data for normal robot operations, and output as normal values to log files for comparing teaching points.

(2) During system operation, monitor the teaching points instructed to robots at suitable time intervals, and compare them with the normal values in the log files collected in (1). In addition, display/store the teaching points monitored to enable their values to be shown if they are determined as abnormal.

(3) Abnormalities occur.

(4) Confirm that the teaching points being monitored are not included in the normal values in the log files, determine them as abnormal and terminate the entire system including the robot operations. At the same time, display a message on the console screen indicating the detection of abnormalities.

(5) Recover the robots to operate correctly.

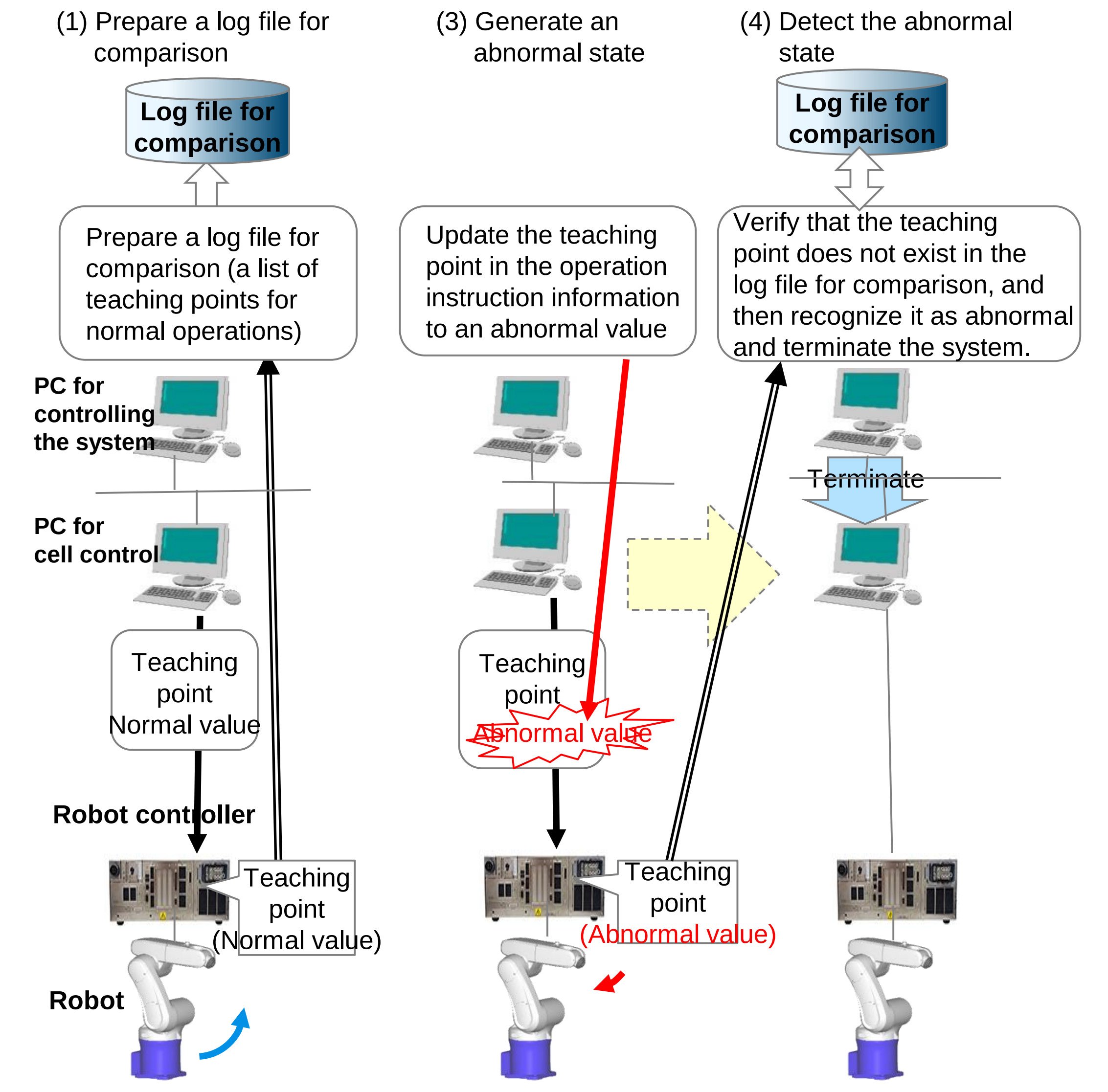

(1) Prepare a log file for comparison
(3) Generate an abnormal state
(4) Detect the abnormal state
Log file for comparison
Log file for comparison
Prepare a log file for comparison (a list of teaching points for normal operations)
Update the teaching point in the operation instruction information to an abnormal value
Verify that the teaching point does not exist in the log file for comparison, and then recognize it as abnormal and terminate the system.
PC for controlling the system
PC for cell control
Terminate
Teaching point Normal value
Teaching point Abnormal value
Robot controller
Teaching point (Normal value)
Teaching point (Abnormal value)
Robot

Figure A-6 Detection of abnormalities by comparing the patterns of robot operations

Appendix B References

[1] K. Ashton, "That 'Internet of Things' Thing," http://www.rfidjournal.com/articles/view?4986.

[2] 内閣サイバーセキュリティセンター（NISC）, "重要インフラ一覧表," http://www.nisc.go.jp/active/infra/pdf/cc_ceptoar.pdf.

[3] 総合電機メーカー, "液晶テレビ受信不具合について," http://www.mitsubishielectric.co.jp/oshirase/20150409/.

[4] ITMedia, "原因は「二重の人為的ミス」　," http://www.itmedia.co.jp/news/articles/0504/24/news008.html.

[5] IPA, "「利用時品質検討ワーキング・グループ」を発足," https://www.ipa.go.jp/sec/info/20160927.html.

[6] IPA, "「つながる世界の利用時の品質～IoT時代の安全と使いやすさを実現する設計～」を公開," http://www.ipa.go.jp/sec/reports/20170330.html.

[7] METI, "METI Formulates the Cybersecurity Management Guidelines," http://www.meti.go.jp/english/press/2015/1228_03.html.

[8] 経済産業省, "製品安全に関する事業者ハンドブック," http://www.meti.go.jp/product_safety/producer/jigyouhandbook.html.

[9] IPA, "つながる世界のセーフティ&セキュリティ設計入門," https://www.ipa.go.jp/sec/reports/20151007.html.

[10] IPA, "情報セキュリティスキル強化についての取り組み," http://www.ipa.go.jp/jinzai/hrd/security/index.html.

[11] 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.

[12] IPA, "つながる世界の利用時の品質," http://www.ipa.go.jp/files/000057850.pdf.

[13] IPA, "組込みシステムのセキュリティへの取組みガイド（2010年度改訂版）," https://www.ipa.go.jp/security/fy22/reports/emb_app2010.

[14] IPA, "自動車の情報セキュリティへの取組みガイド," http://www.ipa.go.jp/security/fy24/reports/emb_car/.

[15] IPA, "情報処理技術者試験　試験区分一覧," https://www.jitec.ipa.go.jp/1_11seido/seido_gaiyo.html.

[16] IPA, "国家資格「情報処理安全確保支援士」," http://www.ipa.go.jp/siensi/.

[17] WIRED, "Hacker Disables More Than 100 Cars Remotely," http://www.wired.com/2010/03/hacker-bricks-cars/.

[18] ITmedia, "ATMを狙うマルウェア、携帯メールで現金引き出す," http://www.itmedia.co.jp/enterprise/articles/1403/26/news037.html.

[19] IPA, "組織内部者の不正行為によるインシデント調査," http://www.ipa.go.jp/security/fy23/reports/insider/.

[20] IPA, "組織における内部不正防止ガイドライン," https://www.ipa.go.jp/security/fy24/reports/insider/.

[21] IPA, "『高度標的型攻撃』対策に向けたシステム設計ガイド," https://www.ipa.go.jp/security/vuln/newattack.html.

[22] IoT推進コンソーシアム, "カメラ画像利活用ガイドブック ver1.0," 31 1 2017. http://www.meti.go.jp/press/2016/01/20170131002/20170131002-1.pdf.

[23] IoT推進コンソーシアム/データ流通促進WG/カメラ画像利活用SWG. http://www.iotac.jp/wg/data/.

[24] 朝日新聞Digital, "ネット接続の複合機など、データ丸見え　大学など２６校," http://www.asahi.com/articles/ASHDD3SMNHDDPTIL006.html.

[25] 日本放送協会「クローズアップ現代」, "サイバー攻撃の恐怖　狙われる日本のインフラ," http://www.nhk.or.jp/gendai/kiroku/detail02_3221_all.html.

[26] 愛知県, "愛知県安全なまちづくり条例," https://www.pref.aichi.jp/police/syokai/houritsu/sekou-kaisei/seian-s/machizukuri.html.

[27] IPA, "はじめてのSTAMP/STPA ～システム思考に基づく新しい安全性解析手法～," http://www.ipa.go.jp/sec/reports/20160428.html.

[28] IPA, "はじめてのSTAMP/STPA（実践編）～システム思考に基づく新しい安全性解析手法～," https://www.ipa.go.jp/sec/reports/20170324.html.

[29] IPA, "【注意喚起】家庭内における無線LANのセキュリティ設定の確認を," https://www.ipa.go.jp/security/topics/alert270612.html.

[30] Broadband Forum, "TR-069 CPE WAN Management Protocol v1.1," https://www.broadband-forum.org/technical/download/TR-069_Amendment-2.pdf.

[31] IPA, "コンシューマデバイスの信頼性確保に向けた取組み～開発方法論の国際標準化に向けて～," https://www.ipa.go.jp/sec/reports/20130930.html.

[32] 多田直弘, モノづくりにおける実践のDRBFM―より高い品質をめざした未然防止手法のすすめ, 夕月書房, 2014.

[33] 丸文株式会社, "ネットワークにおける時刻同期の重要性," http://www.marubun.co.jp/product/network/ntp/qgc18e0000010oqg-att/symmetricom_wp_1.pdf.

[34] 一般社団法人電子情報技術産業協会(JEITA), "WORM技術と暗号化技術," http://home.jeita.or.jp/is/committee/tech-std/std/201104/tape_system_08.pdf.

[35] 一般社団法人重要生活機器連携セキュリティ協議会, "生活機器の脅威事例集," https://www.ccds.or.jp/public_document.html.

[36] "脆弱性対策情報ポータルサイト（JVN）," http://jvn.jp/.

[37] "脆弱性対策情報データベース（JVN iPedia）," http://jvndb.jvn.jp/.

[38] IPA, "情報セキュリティ10大脅威 2016," https://www.ipa.go.jp/security/vuln/10threats2016.html.

[39] Black Hat, https://www.blackhat.com/us-15/.

[40] Cyber Threat Alliance, http://www.cyberthreatalliance.org/.

[41] 一般財団法人日本自動車研究所, "平成26年度　戦略的イノベーション創造プログラム　V2X（Vehicle to X）システムに係わるセキュリティ技術の海外動向等の調査," 3 2015. http://www.meti.go.jp/meti_lib/report/2015fy/000326.pdf.

The Development Guidelines are created by the Working Group on Development Guidelines for the Smart-society, Software Reliability Enhancement Center (SEC), Technology Headquarters, Information-technology Promotion Agency (IPA).

Editors/authors (titles omitted)

Chief editor/ author	Hiroaki Takada	Nagoya University
Vice chief editor/author	Atsuhiro Goto	Institute of Information Security
Member	Masato Iijima	Misawa Homes Institute of Research and Development Co., Ltd.
	Toshiaki Kimura	Technology Research Institute, Japan Society for the Promotion of Machine Industry
	Hisao Ogata	Hitachi-Omron Terminal Solutions, Corp.
	Tsukasa Ogino	Connected Consumer Device Security Council
	Masayuki Okuhara	Fujitsu Limited
	Kazuo Kajimoto	Panasonic Corporation
	Yuichi Takahashi	Information & Telecommunication Systems Company, Hitachi, Ltd.
	Katsutoshi Hasegawa	Embedded Systems Innovation Council
	Hiroshi Hayakawa	DENSO Corporation
	Masaru Matsunami	Japan Smartphone Security Forum
	Seiichi Mikami	JVC KENWOOD Corporation
Secretariat	Masayoshi Nakao	IPA/SEC
	Shinji Miyahara	IPA/SEC
	Mitsuyoshi Kozaki	IPA/SEC
	Makoto Toyama	IPA/SEC
	Keiko Nishio	IPA/SEC
	Hidefumi Maruyama	IPA/SEC

July 29, 2016 First edition, September 28, 2017 Second Edition

Editorial supervisor	Software Reliability Enhancement Center (SEC), Technology Headquarters, Information-technology Promotion Agency (IPA)
Publisher	Takaaki Matsumoto
Publishing office	Information-technology Promotion Agency (IPA) Bunkyo Green Court Center Office 16F 2-28-8 Hon-komagome, Bunkyo-ku, Tokyo 113-6591, Japan URL http://www.ipa.go.jp/sec/