IoT Security Guidelines
Ver. 1.0

July 2016

IoT Acceleration Consortium
Ministry of Internal Affairs and Communications
Ministry of Economy, Trade and Industry

Introduction

The Internet of things (IoT) is rapidly spreading, as things that have not been connected to the Internet or other networks are being provided with communications functions, connected to the Internet, and operated over the network. It is forecasted that 53 billion IoT devices[1] will be in use by 2020. This, however, will cause more risks of cyberattacks over the network on IoT devices and equipment. IoT systems consist of networks, a wide variety of IoT devices that will may be used for more than 10 years, such as connected cars or smart houses, and devices, including those with restricted computing resources, such as sensors. Actions on IoT security are urgently needed with a focus on characteristics of IoT systems and services.

Japan’s Cybersecurity Strategy decided by the Cabinet in September 2015 states that the development of mechanisms, including the promotion of new business and the formulation of guideline, and technological development are to be advanced with the security of IoT. The fundamental development is essential to create innovative IoT business models and to realize a safe and secure society.

The IoT Security Guidelines aim to suggest basic strategies for providers and users of IoT devices, systems, and services across industries to consider appropriate and risk-based cybersecurity measures, recognizing that new risks on IoT, including cyberattacks, would cause an adverse influence on the safety of the IoT and IoT users and the protection of critical information, such as personal information and technology information. We expect that the Guidelines will promote the providers and users of IoT devices, systems, and services to recognize their roles and to address IoT security with the characteristics of each industry.

[1] (Source) IHS Technology

Table of Contents

Chapter 1
Background and Purpose

This chapter explains why it is imperative to have IoT security measures by describing the growth trends and cyberthreat examples of IoT as well as IoT’s characteristics, as the background of the development of the Guidelines.

Furthermore, the chapter explains that the purposes of the Guideline are to show basic security measures that IoT stakeholders in any industry should take and to promote all stakeholders on an IoT system to share a common recognition for the security among them. In addition, the chapter covers the scope of IoT targeted in the Guidelines.

1.1 Background of Guidelines

1.1.1 Trends of IoT and Recent Cyberthreat Examples

In recent years, it has become common for “things” that were not connected to the Internet or other networks to have communications functions and operated online. It is expected that the number of network-connected IoT devices will increase to 53 billion by 2020. It is forecasted that 52.7% of all IoT devices will be used for consumer services such as home energy management system (HEMS) equipment in 2020. Many examples of IoT cyberthreats in consumer services, such as HEMS equipment, and automotive-related services, such as connected cars, were reported at international security conferences over the past a few years. Many cases of a malware infection and a compromise of IoT devices have been found in past surveys[2]. Furthermore, these infected devices were reported to be used for DDoS attacks. As IoT devices and systems are connected to the Internet, cyberattacks and system failures on IoT may have an adverse influence on physical safety and cause a leakage of important information such as about a personal life.

Table 1 IoT cyberthreat examples categorized by field

(Source: M2M Security Demonstration Project of the Ministry of Internal Affairs and Communications)

Category	Subcategory	Year of presentation/Conference	Outline
Automotive-related service	•Connected car •Subsystem	2015/Black Hat, U.S.A.	A demonstration showed a vulnerability allowing remote operations of automobiles through the Internet. In the demonstration, the controller of the multimedia system of an automobile was connected through the Internet, the firmware was overwritten with that of a different controller, malformed commands were sent on the CAN (*1) bus, and the steering wheel, engine, etc. of the automobile were remotely controlled.
Consumer service	•Home energy management system (HEMS)	2015/Black Hat, U.S.A.	An example of the risk of the insecure development of home automation. The KNX (*2) net/IP protocol used for the management of in-room equipment of a hotel was captured and analyzed, whereby the equipment was remotely controlled illegally.
Industry-specific service	•Medical care	2012/Breakpoint Security Conference	A demonstration introduced the illegal remote control of a pacemaker. The communication between a dedicated device and an implantable pacemaker was intercepted and analyzed, whereby unauthorized communication with the pacemaker made it possible to work improperly.

(*1) CAN: A vehicle network protocol that Robert Bosch GmbH introduced in 1986. The protocol was approved as an international standard (ISO 11898) in 1994.

(*2) KNX: A smart house communications protocol that KNX Association, an European organization, introduced in 2002. The protocol was approved as an international standard (ISO/IEC 14543-3) in 2006.

1.1.2 IoT-specific Characteristics and Necessity for Security Measures

With consideration of the trends of the IoT and cyberthreat examples, while the growth of the IoT will accelerate corporate activities and innovations on products and services, it will be necessary to take security measures with consideration of IoT-specific characteristics and risks. The characteristics specific to general IoT devices and equipment are described below.

[2] https://www.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf

[IoT-specific characteristics]

Characteristic 1: Large influence on a wide range in case of a cyberattack

IoT devices and equipment, including HEMS equipment and connected cars, are connected to networks. Therefore, once a single IoT device is attacked, it is highly possible that not only the attacked IoT device but also other connected IoT systems and services will be affected. The more IoT devices increase, the more ranges are affected. For example, if the attack influences the control (actuation) of IoT devices in the automotive field or medical field, humans' lives could be at risk. Furthermore, IoT devices and systems may store important information (e.g., personal life data and production information obtained from factory devices), and that would cause leakages of such information.

Characteristic 2: Long life cycle of IoT

Many IoT devices will be used for 10 years or more as the average life cycle of an automobile is said to be 12 or 13 years and many factory control devices are used for 10 to 20 years.

Therefore, IoT devices may be connected to the Internet insecurely with out-of-date security measures due to the long life cycle.

Characteristic 3: Difficulty in monitoring IoT

Unlike personal computers and smartphones, many IoT devices are not provided with monitoring screens. In such cases, it is not easy for the users to monitor and check abnormalities in such IoT devices. Therefore, the IoT devices that are not properly monitored by the users may be connected to the Internet and infected with malware.

Characteristic 4: Insufficient mutual understanding between stakeholders on the IoT device side and the network side

Neither stakeholders on the IoT device side nor those on the network side sufficiently understand the surrounded environment and characteristics of the other party, which may cause difficulty in satisfying required safety and performance when the IoT devices are network connected. It must be kept in mind that the environment of the network to be connected may change the security requirement of the IoT device side.

Characteristic 5: Limited functions and computing performance of IoT

For example, it may not be possible to apply security measures to particular IoT devices such as sensors due to the limited computing resources.

Characteristic 6: Unintended network connections of IoT even for the manufacturers

As many devices are being provided with a communications function and being connected to the Internet as IoT, an influence not initially imagined by the manufacturers may occur due to the connections.

1.2 Purpose of Guidelines

The purpose of the Guideline is to suggest required basic security strategies on IoT devices and services based on “Security by Design Principle” and to lead IoT stakeholders to take proactive actions in industries with consideration of characteristics of IoT.　It also aims to create an environment where users can utilize IoT devices, systems, and services securely.

The purpose of the Guidelines is not to clarify all the legal responsibility of the stakeholders when they are involved in a cyber security incident but to promote their awareness of necessity of IoT security protections and to lead them to share necessary information among the stakeholders.

For this reason, the purpose of the Guidelines is to expect the stakeholders to consider appropriate security protections based on what they must protect and risks they face, rather than to require the stakeholders to take a single standardized security protection.

In addition, the Guidelines address five essentials that should be noted by general public, because a large number of IoT devices, systems, and services have been spread in people’s daily lives.

1.3 Scope of IoT in Guidelines

1.3.1 About IoT

The IoT stands for the Internet of Things. Recommendation ITU-T Y.2060 (Y.4000) of International Telecommunication Union (ITU) specifies that the IoT is "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies," whereby the following items are expected.

1) It will be possible to collect accurate information more quickly and control devices, equipment, and systems in real time as things are network connected.
2) Devices, equipment, and systems in different fields, such as car navigation systems, consumer electronics, and healthcare products, will link together, thus making it possible to provide new services.

The IoT will not only produce just a value by connecting things over network. Furthermore, the IoT has a nature of System of Systems (SoS), in which different IoT systems will be connected together to produce a further added value. The characteristics of the SoS is shown in 1 through 5 in Figure 1.

IoT (system) connecting things.

IoT (system) connected to different IoT (systems), i.e., System of Systems

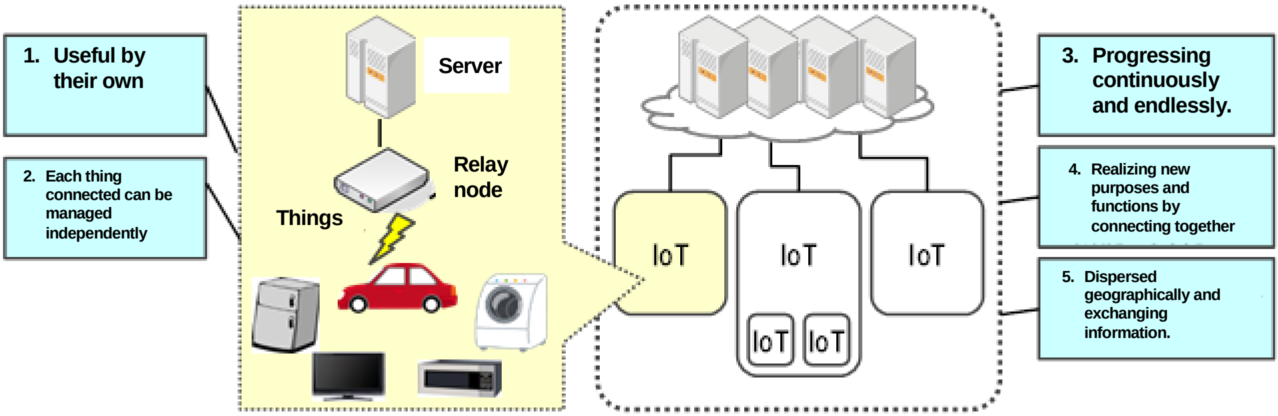

1. Useful by their own
2. Each thing connected can be managed independently
Server
Relay node
Things
IoT
IoT
IoT
IoT
IoT
3. Progressing continuously and endlessly.
4. Realizing new purposes and functions by connecting together
5. Dispersed geographically and exchanging information.

Fig. 1 IoT with SoS Features = Image of "Connecting World"

1.3.2 IoT Devices, Systems, and Services

The IoT has the superiority of producing a new value by connecting things. On the other hand, as the operating structure expands and changes constantly, the re-assessment of the IoT security is very important.

In the Guidelines, network connected devices, and systems that consist of devices and other systems are defined as "IoT devices and systems" and services utilizing these devices and systems are defined as "services."

1.4 Target Readers

The following figure shows the target readers of this Guidelines.

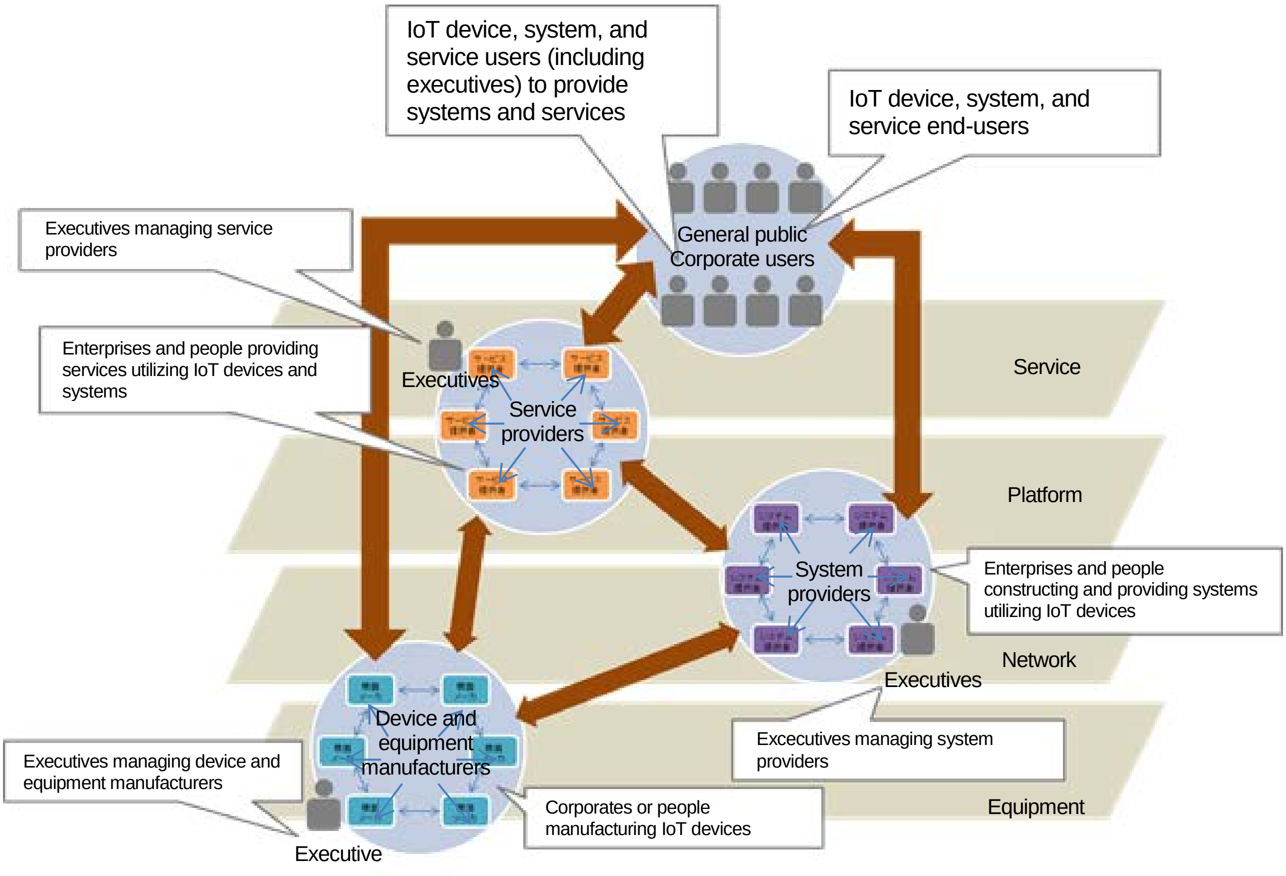

IoT device, system, and service users (including executives) to provide systems and services
IoT device, system, and service end-users
Executives managing service providers
General public
Corporate users
Enterprises and people providing services utilizing IoT devices and systems
Executives
Service providers
Service
Platform
System providers
Enterprises and people constructing and providing systems utilizing IoT devices
Network
Executives
Device and equipment manufacturers
Excecutives managing system providers
Executives managing device and equipment manufacturers
Corporates or people manufacturing IoT devices
Equipment
Executive

Fig. 2 Target Readers

The following target readers are assumed.

- IoT device, system, and service providers and executives managing the providers
  - Device manufacturers
  - System providers
  - Service providers
- IoT device, system, and service users
  - Corporate users[3]
  - General users

A number of IoT devices, systems, and services are mutually utilized to realize many functions and services. Therefore, it is necessary for providers of systems or services to recognize themselves as also the users.

[3] The Guidelines assume that corporate users are businesses that manage and utilize IoT devices, systems, and services incorporated into their production activities, provision of services, or other business operations.

The following table shows examples of readers categorized by field or service.

Table 1. Examples of Readers by field or service

Field	Service	Provider			User
		Executive	IoT device manufacturer	System and service provider/Corporate user[4]	General public
Automobile	Connected car service	Executives of the IoT device manufacturers and system and service providers specified on the right-hand fields.	• Automobile manufacturers	• Automobile manufacturers • Network operators	• Automobile owners and drivers
Home electronics	HEMS	Executives of the IoT device manufacturers and system and service providers specified on the right-hand fields.	• HEMS equipment manufacturers • Communications equipment manufacturers	• HEMS operators • Housing manufacturers • Network operators	• Residents
Medical care	Home medical care service	Executives of the IoT device manufacturers and system and service providers specified on the right-hand fields.	• Medical equipment manufacturers • Communications equipment manufacturers	• Home health service providers • Hospitals (system management departments) • Network operators	• Patients and their families • Doctors • Nurses • Care managers
Factory	Control system	Executives of the IoT device manufacturers and system and service providers specified on the right-hand fields.	• Control equipment manufacturers • Sensor manufacturers for control equipment	• Factory system builders • Factory managers • Network operators	[5]

It is expected that IoT stakeholders recognize risks on IoT and consider to take necessary security measures according to the Guidelines. It is also expected that the Guidelines be a reference even to industries, where in the safety- and security-related standards, laws, and regulations have been already developed, when they connect their devices, systems, and services with other industries.

[4] The Guidelines assume that corporate users are businesses that manage and utilize IoT devices, systems, and services incorporated into their production activities, provision of services, or other business operations.

[5] It is assumed that factory control systems may influence general users, including their personal information, if the factory systems are connected to IoT devices and systems.

1.5 Overall Structure of Guidelines

Chapter 1 described the background and the purpose of the Guidelines, the scope of the IoT and target readers in the Guidelines.

Chapter 2 explains five guiding principles of IoT security measures for the executives of IoT devices, systems, and services, device manufacturers, system providers, and service providers (partly including corporate users). The five guiding principles specify a number of key concepts for the lifecycle “policy”, “analysis”, “design”, “implementation and connection”, and “operation and maintenance” of the IoT, and show the points, explanations, and examples of measures. The content of the five guiding principles has been discussed in reference to *Development Guidelines for Connecting the World* (issued in March 2016 by the Information-technology Promotion Agency (IPA), Japan)[6] and extended to cover wider readers such as IoT service providers.

Chapter 3 describes IoT security essentials that general public should take note of

Chapter 4 shows matters to be considered in the future discussion.

[6] http://www.ipa.go.jp/files/000051411.pdf

The following table specifies the target users classified by each chapter, section, and key concept.

Table 2 Target Users Classified by Chapter, Section, and Key Concept

[Legend] ○: Target readers

Chapter/Section			Providers (including corporate users)			Users
			Executive	IoT device manufacturer	System and service provider/Corporate user	General public
Introduction			✔	✔	✔	✔
Chapter 1			✔	✔	✔	✔
Chapter 2	2.1 Policy	Key concept 1	✔	✔	✔	
		Key concept 2	✔	✔	✔	
	2.2 Analysis	Key concept 3		✔	✔	
		Key concept 4		✔	✔	
		Key concept 5		✔	✔	
		Key concept 6		✔	✔	
		Key concept 7		✔	✔	
	2.3 Design	Key concept 8		✔	✔	
		Key concept 9		✔	✔	
		Key concept 10		✔	✔	
		Key concept 11		✔	✔	
		Key concept 12		✔	✔	
	2.4 implementation and connection	Key concept 13		✔	✔	
		Key concept 14			✔	
		Key concept 15			✔	
		Key concept 16		✔	✔	
	2.5 Operation and Maintenance	Key concept 17		✔	✔	
		Key concept 18		✔	✔	
		Key concept 19		✔	✔	
		Key concept 20		✔	✔	
		Key concept 21			✔	
Chapter 3						✔
Chapter 4			✔	✔	✔	

Chapter 2
Five Guiding Principles of IoT Security Measures

Chapter 2 shows a guiding principle of security measures on each one of required five phases of IoT development, namely, policy, analysis, design, implementation and connection, and operation and maintenance. For the each principle, key concepts are specified as well as the points, explanations, and examples of measures.

Existing laws and regulations for safety and performance requirements must be followed in any applicable industry. On top of that, it is important to address IoT security measures and the implementation of them with consideration of possible risks and accidents that may occur in the respective industry fields.

The guiding principles are listed below.

Table 3 List of Guiding Principles for Security Measures

Stage	Principle	Key concept
Policy	Principle 1: Establish a basic policy with consideration of the nature of the IoT	Key concept 1. Executives are committed to IoT security
		Key concept 2. Prepare for internal fraud or mistakes
Analysis	Principle 2: Recognize risks on IoT	Key concept 3. Identify what to protect
		Key concept 4. Assume what risks will result from connections
		Key concept 5. Assume what risks will spread from connections
		Key concept 6. Recognize physical risks
		Key concept 7. Learn from past cases
Design	Principle 3: Consider a design to protect what should be protected	Key concept 8. Make a design that protects each individual and all
		Key concept 9. Make a design that will not cause trouble to connecting destinations
		Key concept 10. Establish design consistency to ensure safety and security
		Key concept 11. Designing to ensure Safety/Security even when connected to unspecified entities
		Key concept 12. Verify and evaluate a design to ensure safety and security
implementation and connection	Principle 4: Consider security measures on network side	Key concept 13. Provide a function to grasp and record the condition of devices
		Key concept 14. Connect IoT devices to a network properly based on the function and purpose
		Key concept 15. Pay attention to initial settings
		Key concept 16. Prepare/Provide an authentication function
Operation and maintenance	Principle 5: Maintain a safe and secure state and dispatch and share information	Key concept 17. Maintain product safety and security after product shipment and release
		Key concept 18. Grasp IoT risks after shipment or release and keep relevant stakeholders informed of what should be observed
		Key concept 19. Notify general users of connection risks
		Key concept 20. Recognize the roles of the stakeholders of IoT systems and services
		Key concept 21. Grasp all vulnerable devices and give appropriate cautions

2.1 [Policy] Principle 1 Establishing a basic policy with consideration of the nature of the IoT

In the IoT, a user's body, life, and property may be exposed to danger in the case of the malfunctioning or unauthorized operation of IoT devices, or systems, including automobiles, consumer electronics, healthcare products, ATMs, and other payment settlement machines. In that case, the influence may spread in a wide range over the network. Furthermore, it is difficult to monitor all IoT devices and systems while the functions and performance of IoT devices and systems have limits. IoT security measures are issues related to the survival of enterprises using the IoT as well as that of the developers of devices and systems. There is a need for executives to recognize IoT risks and take the leadership to promote security measures.

Accordingly, this guiding principle specifies Key concepts of IoT security measures that executives and all other parties concerned should recognize.

Key Concept 1.	**Executives are committed to IoT security**
Key Concept 2.	**Prepare for internal fraud or mistakes**

Key Concept 1. Executives are committed to IoT security

(1) Point

1) Each executive takes measures with consideration of the Cybersecurity Management Guidelines, establishes a basic policy on IoT securities for the enterprise, and keeps all employees of the enterprise informed of the basic policy while continuously grasping and reviewing the status of implementing the basic policy. Furthermore, the executive develops a necessary system and human resources for the foregoing.

(2) Commentary

Risks may be diversified and spread and affect the survival of the enterprises. Furthermore, countermeasure against risk on development sites require costs and may be beyond the judgment of the sites in many cases. Therefore, it is considered necessary for the management to take the initiative in showing the policy on measures.

On top of that, a system will be required to take emergency measures, make an analysis of cause, and implement drastic measures and an environment to verify and evaluate the measures. The IoT consists of devices and systems of various enterprises. Therefore, the cooperation of systems is necessary for enterprises to cooperate. Accordingly, the maintenance and development of human resources will be necessary, who will make use of their knowledge and technology and take measures.

With consideration of the Cybersecurity Management Guidelines, each enterprise should establish a basic policy on IoT security, keep all employees of the enterprise informed of the same, while continuously grasping and reviewing the status of implementing the basic policy. Furthermore, a necessary system and human resources should be developed.

(3) Examples of measures

1) Working on organizational measures

- With the consideration of the Cybersecurity Management Guidelines, the management works on IoT security based on the leadership of the management.
  - Cybersecurity Management Guidelines (December 28, 2015, the Ministry of Economy, Trade and Industry, Information-technology Promotion Agency, Japan)
    http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf
- Turn the plan-do-check-act (PDCA) cycle, and recognize IoT system and service risks, and construct and maintain the organization’s measures. The CSMS Users’ Guide is informative for specific implementation methods of risk assessment.
  - CSMS Users’ Guide (http://www.isms.jipdec.or.jp/csms/doc/JIP-CSMS111-08.pdf)

Key Concept 2. Prepare for internal fraud or mistakes

(1) Points

1) Recognize the potential possibility of internal fraud that will threaten the safety of the IoT and consider measures.
2) Prevent the mistakes of parties concerned and consider safety measures to cover mistakes, if any.

(2) Commentary

Crimes taking advantage of improper security measures have been reported overseas. These crimes include a crime of a retiree dissatisfied with the company that the retiree worked for, in which the retiree remotely operated a management service for an automobile, thus making it impossible to start the automobile or keeping the horn sounding. In another case, a perpetrator used a duplicated physical key and opened the maintenance door of a bank's ATM, infected the ATM with a virus, connected a mobile device to a USB terminal of the ATM, and stole cash. Measures are required against the internal fraud of employees and retirees who are familiar with the design and construction of equipment and systems that make up IoT services in order to prevent their unauthorized use of the access rights and keys.

Furthermore, measures are necessary against mistakes caused without malicious intentions, such as the leakage of design information by virus infection as a result of opening a file attached to targeted attack e-mail or losing information taken outside.

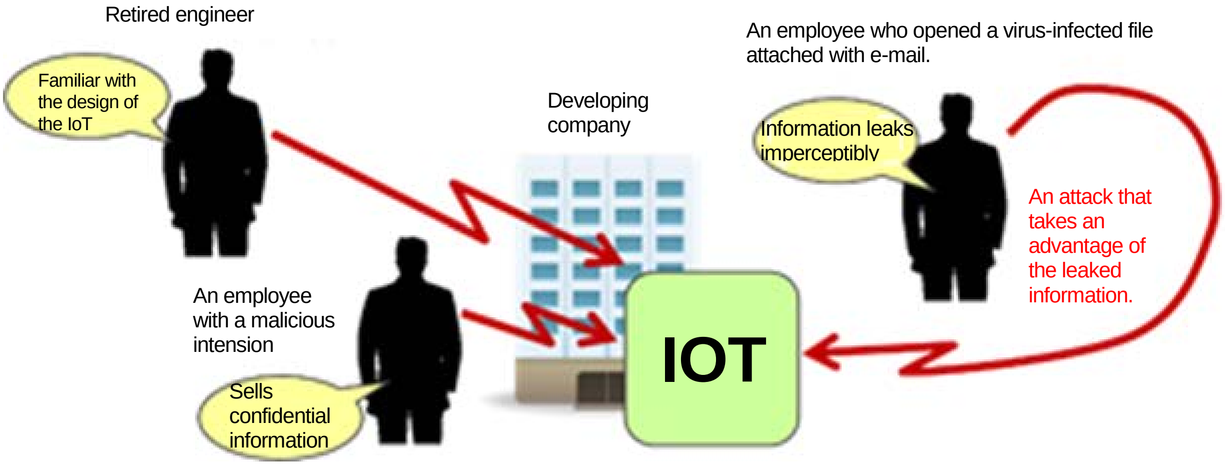

Retired engineer
Familiar with the design of the IoT
An employee who opened a virus-infected file attached with e-mail.
Developing company
Information leaks imperceptibly
An attack that takes an advantage of the leaked information.
An employee with a malicious intension
Sells confidential information
IOT

Fig. 3 Impact of Internal Fraud or Mistakes

(3) Examples of measures

1) Measures against internal fraud

IoT-related internal fraud has a significant influence on other companies' devices and systems as well as users. Therefore, it is necessary to understand the cause and recognize the necessity for measures.

- According to the IPA's survey, internal fraud mainly occurs for the purpose of obtaining money illegally or finding an advantageous career change and because of employees' dissatisfaction at work. The results of this questionnaire survey on conditions tempting employees into conducting fraud show that the issuance of an unfair notice and a chance of an advantageous job change for another company with better conditions are top-ranked causes. It is necessary for each company to correct internal problems, if any, and develop training in order to prevent employees' fraud.
- The IPA's Guidelines for Organizations' Internal Fraud Prevention provide five basic principles of

internal fraud, which should be referred to because the principles cover matters common to the internal fraud risk of connected devices and systems.

Table 4 Five Basic Principles of Internal Fraud

Five basic principles	Overview
Make it difficult to commit crimes (less easy to conduct fraud)	Reinforce measures to make it difficult to conduct the criminal activities.
Increase the possibility of getting caught (found with ease)	Increase the risk of getting caught with reinforced control and monitoring.
Reduce the return of crimes (do not pay)	Prevent the crimes by hiding or eliminating the targets and making the deeds unprofitable.
Reduce the causes of crimes (not tempting people)	Deter the crimes by not allowing them to be in the mood of committing the crimes.
Do not justify crimes (Do not let the perpetrators' excuse)	Eliminate the justification of the perpetrators' actions.

Source: IPA's Guidelines for Organizations' Internal Fraud Prevention

2) Measures against employees' mistakes and violations

In recent years, targeted e-mail attacks have been increasing in number. These attacks are made by e-mail with virus-infected files attached (targeted e-mail attacks) to particular companies and organization from senders introducing themselves as parties concerned with the companies or organizations, government-related organizations, or other highly reliable organizations. These viruses not only cause information leakage but also infect bank accounting systems and draw money from ATMs through the unauthorized operation of the ATMs. No matter what types of devices are used, what types of systems are developed, and what types of maintenance sites are managed, it is necessary for all companies to keep all employees informed of the prevalence of these attacks.

Targeted e-mail attacks have become very clever recently, and people ends up opening the attached files infected with viruses in many cases. Therefore, it is necessary to design corporate intra-network with measures to prevent information leakage caused by viruses. The IPA released the System Design Guide for Measures against Highly Advanced Targeted Attacks to prevent the operation of viruses after infection and minimize damage.

2.2 [Analysis] Principle 2: Recognize risks on IoT

There is a need for specifying items to be protected and making a risk analysis for them in order to take IoT security measures. In the case of the IoT, in particular, there is a possibility that other devices that are network connected may be affected or the connection of such devices may cause unexpected problems. For this reason, it is necessary to specify items to be protected and make a risk analysis again.

This principle explains five key concepts to be worked on for risk recognition.

Key Concept 3.	Identify what to protect
Key Concept 4.	Assume what risks will result from connections
Key Concept 5.	Assume what risks will spread from connections
Key Concept 6.	Recognize physical risks
Key Concept 7.	Learn from past cases

Key Concept 3. Identify what to protect

(1) Points

1) From the viewpoint of the safe and secure IoT[7], specify original functions and information to be protected.
2) Specify connecting functions as protected items for the safety and security of original functions and information.

(2) Commentary

Conventional devices and systems are provided with safety functions to protect the bodies, lives, and property of the users of the devices and systems, in addition to functions specific to the devices and systems, such as cooling and heating functions in the case of air conditioners. It is necessary to protect these specific functions (original functions) while maintaining the safety and security of the users if the devices or systems are connected to remote servers or other home electric appliances. Furthermore, it is necessary to prevent the leakage of information on the operation of the devices or system-generated information as a result of the connection of the devices.

It is necessary to protect connecting functions so that they will not be gates for external attacks or spread the influence of malfunctions externally. Therefore, in terms of IoT safety and security, it is necessary to specify original functions and connecting functions as items to be protected.

Furthermore, it is necessary to recognize the risk, assuming the case that many IoT devices are connected to IoT.

(3) Examples of measures

1) Clarification of original functions and information

1) Clarification of original functions

Clarify the original functions of IoT devices and systems (e.g., the functions of running, turning, and stopping in the case of automobiles and the functions of cooling and heating in the case of air conditioners) and information, such as generated sensor data and log data. In some cases, the addition of connecting functions, including remote control functions, is assumed along with the generation of information for such functions. Therefore, clarify matters related to networks, including network configuration.

2) Clarification of information

Clarify sensor data and personal information (including privacy information) collected by IoT devices and systems and technical information, such as design information, owned. Also identify software and their settings information, comprising the functions 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 5 Examples of information to be protected in embedded systems

Information asset	Description

[7] The expression “safe and secure” used in the Guidelines includes the concepts of safety, security, and reliability, and refers to a state of target devices and systems with their safety, security, and reliability maintained.

Content	E.g., multimedia data, such as voice, image, and video data (including copyright management data on the use of commercial content and private content), and content usage history (it is important to protect the usage history of content).
User information	E.g., each user's personal information (such as the user's name, address, phone number, date of birth, credit card number), authentication information, usage history, and GPS-acquired positional information.
Device information	E.g., information on degital consumer electronics itself (such as model, ID, and serial ID information), and device authentication information.
State information of software	Specific status information of software (such as operating status information and network usage information).
Software setting information	E.g., Specific setting information of software (such as operation setting, network setting, permission setting, and version information).
Software	E.g., operating systems, middleware, and applications (sometimes referred to as firmware)
Design information and internal logic	Design information, such as specific information, and includes the logic read from electromagnetic waves generated at the time of the analysis and operation of the software.

Source： Based on the IPA's Security Guide to Embedded Systems

2) Clarification of functions and information to be protected

Clarify additional functions, such as communications, linking, and integration functions, and information to make conventional devices and systems into IoT devices and systems. Businesses that construct and connect IoT services may change setting information for connecting functions, in particular. Therefore, clarify not only information but also the setting function to be protected.

Organize all items clarified to be protected in order of importance.

Key Concept 4. Assume what risks will result from connections

(1) Points

1) Assume risks on the condition that devices and systems intended for closed networks will be used as IoT devices and networks.
2) Assume risks in maintenance work and those resulting from the unauthorized use of maintenance tools.

(2) Commentary

An incident occurred in 2004, in which an HDD recorder was used for a stepping-stone. In 2013 and 2015, data accumulated in multifunction printers of a number of manufacturers was disclosed on the Internet. It seemed that these incidents occurred because the manufacturers had not assumed the use of them in environments directly accessible from the Internet and the products had been shipped without setting initial passwords or had not requested the users to make password changes. Furthermore, there was a case, in which a factory system isolated from the Internet was infected with a virus via a USB memory stick brought in at the time of maintenance.

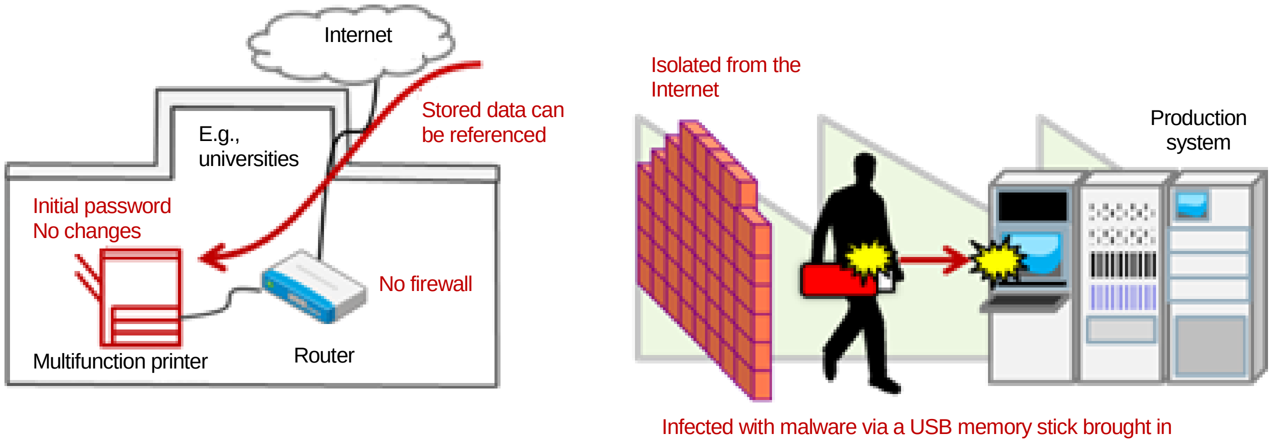


Fig. 4 Case Example—An incident occurred because the system was set on the assumption that it would not be Internet connected.

In the above case in 2004, the HDD recorder was used on the assumption that it would be used in an environment restricted with a firewall. In the other case in 2013 and 2015, the printers were isolated from the Internet. In both cases, it seemed that security measures taken for the products were insufficient. It is necessary to consider possible risks on the assumption that devices and systems incorporating communications functions may be used as IoT devices and systems regardless of the current usage environments of the devices or systems.

Furthermore, a tool that extracted the resetting function of an automobile anti-theft system is sold on the Internet and used for automobile theft. It is necessary to make preparations for preventing the unauthorized use of maintenance tools.

(3) Examples of measures

1) Risks assumed as IoT devices and systems

1) Risks on the assumption that devices and systems intended for closed networks may be used as IoT

devices and systems

Design the devices and systems on the assumption that they may be used as IoT devices and systems as long as they incorporate IoT functions even if they are supposed to be used at home or in corporate LAN environments.

Specific examples are shown below.

- Set a different initial password for each device or system before shipping. Make sure that each password is difficult to be figured out.
- Design the products that require users' mandatory password changes and check the strength of auto-generated or user-entered passwords.
- Limit functions if incorrect passwords are input for a certain number of times.
- Do not provide a server function unless it is mandatory. If the products need a server function, minimize the number of open ports and disable all unnecessary ports.
- Do not set administrative privileges for all internal functions. Assign appropriate user privileges.
- Install anti-virus software to isolated network devices and systems or make virus checks on personal computers and USB memory sticks to be brought in.

2) Response to problematic situations

In the future, it is expected to check the connection environment of the devices and systems and provide functions to prompt measures if there are any problems. Specifically, the provision of a function to display a message prompting the users to make changes or a function to notify members of support in the following cases, for example, is expected.

- Attacks are likely to occur and the users should make setting changes.
- The products are installed in externally accessible environments.

3) Implementation of penetration testing

Conduct the verification of devices and systems (so-called penetration testing) from the viewpoint of attackers in order to prevent trouble caused by cyberattacks.

2) Risks at the time of maintenance and the unauthorized use of maintenance tools

1) Assumption of the risk of attacks during maintenance

It is assumed difficult to eliminate internal fraud perfectly even if measures against internal fraud are taken to all employees and affiliated companies. Assume maintenance risks whenever necessary in addition to the suppression of internal fraud. Specifically, the following examples are considered.

- Malware to be carried in by members of maintenance as a result of the insecure management of terminals.
- The fraud of members of maintenance (e.g., the installation of malicious software).
- Unauthorized use of maintenance interfaces by third parties (e.g., setting the devices into private maintenance mode or the acquisition of physical keys to the ATMs).

2) Assumption of the risk of the unauthorized use of maintenance tools

Assume the unauthorized use of maintenance tools and the risk of attacks by modified tools. Specifically, the following examples are considered.

- The unauthorized use of maintenance tools stolen or unlawfully delivered (e.g., unlawful setting changes).
- Attacks against the vulnerability of maintenance tools (e.g., a viral infection)
- Development of attack tools based on the leakage or the reverse engineering or an analysis of design information on maintenance tools.

Key Concept 5. Assume what risks will spread from connections

(1) Points

1) Assume risks of security threats and failures in devices spreading to other devices that will be connected.
2) Assume an increase in the risk of spreading the influence if the measures of devices or systems connected are low in level.

(2) Commentary

In the IoT, there is a concern that the influence may propagate extensively through connections if a device or system fails to operate or a device or system is infected with a virus. A functional failure will affect the devices and systems operating in cooperation. If an IoT device or system is utilized for a stepping-stone, the IoT device or system will turn into a perpetrator from a victim. There is a case where IoT devices or systems cannot recognize their own abnormal state or their attacks against other devices.

It is assumed that the connection of IoT devices with measures of different levels may lower the entire level of measures. A vulnerable IoT device or system low in the level of measures may become a gate for attacks. Defects and incorrect settings may influence the entire IoT.

It is assumed that each industry is different in the risk assumption and design policy of IoT devices and systems. A coordinated response is necessary to risks that will spread through connections with consideration of network connection patterns.

(3) Examples of measures

1) Assumption of risks that may spread from connections

1) Assumption of risks that may spread from abnormal connections

Assume cases where device and system abnormalities will affect other IoT devices and systems or viruses will spread throughout the IoT network from connections.

Assume not only cases of suffering damage but also cases where the stoppage of functions will affect connecting devices and systems or cases where IoT devices and systems will turn into perpetrators from victims because they are infected with viruses and utilized for stepping-stones. Furthermore, assume cases where devices or systems cannot recognize their own abnormal state or their attacks against other devices.

2) Assumption of spreading risks through devices and systems used jointly.

For example, devices and systems that are assumed to be used jointly by a number of service providers, such as domestic robots, display devices, and IP cameras, will not operate normally when simultaneous operations compete with each other. Furthermore, the influence will expand in the case of unauthorized access to common interfaces, if any.

2) Assumption of risks with an increased influence as a result of connecting devices and systems low in the level of measures

Assume cases where IoT devices and systems low in the level of measures may become gates for attacks as a result of connecting IoT devices with measures of different levels. Furthermore, assume the overall risk of the IoT network that may occur as a result of the connection of IoT devices and systems low in the level of measures are connected to different IoT networks.

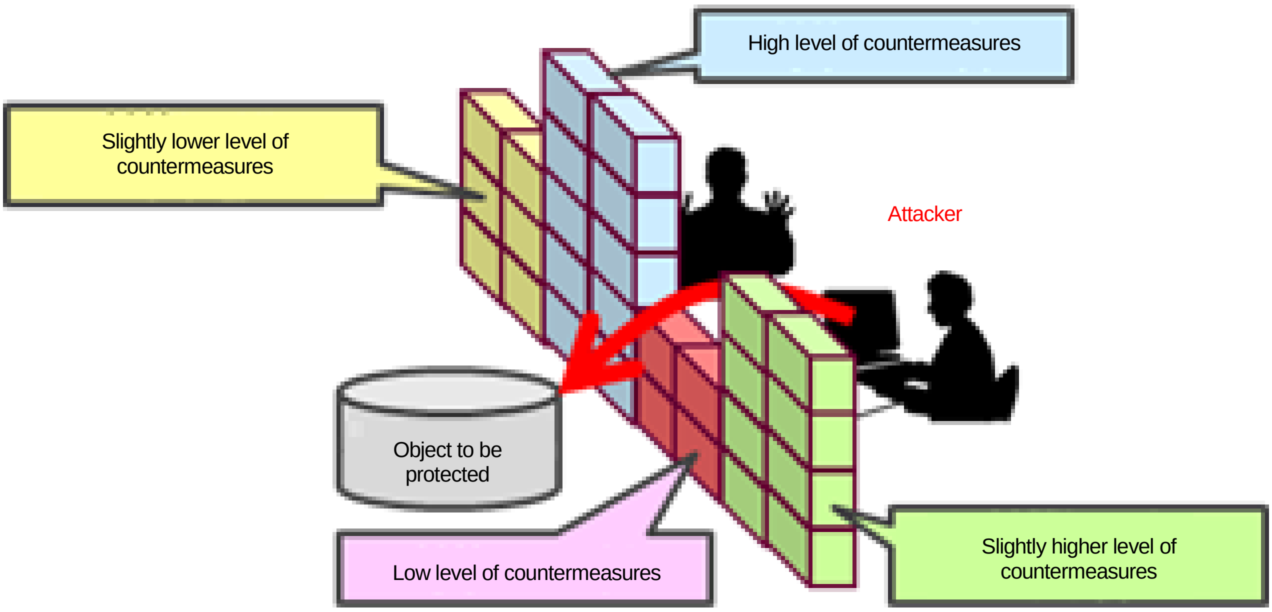

High level of countermeasures
Slightly lower level of countermeasures
Attacker
Object to be protected
Low level of countermeasures
Slightly higher level of countermeasures

Fig. 5 Image of Risk Generated from Vulnerable Part

While IoT networks are connected together to constitute a larger IoT network, it is necessary to assume possibilities of the risk of each IoT device and system to spread throughout the entire IoT network.

Key Concept 6.　Recognize physical risks

(1) Points

1) Assume risks of the illegal operation of stolen or lost devices or physical attacks at locations without administrators.
2) Assume risks of third parties' reading of information in used equipment or discarded equipment or the rewriting or re-selling of software.

(2) Commentary

Devices and systems carried around or installed in homes or public spaces will constitute the IoT. For this reason, there is a risk of the illegal operation of stolen or lost devices or third parties' physical attacks against devices installed in parking lots, gardens, or public spaces. Information may leak from discarded devices. Furthermore, devices incorporating malicious software may be reused or resold.

Fig. 6 Devices and Systems in Homes and Public Spaces Not Physically Managed by Manufacturers

(3) Examples of measures

1) Assumption of physical risks

1) Assumption of risks arising from stolen or lost IoT devices

Assume risks of the illegal operation of stolen or lost devices or physical attacks at locations without administrators. Assume risks of stolen devices illegally operated or lost devices operated to cause IoT service malfunctions.

2) Assumption of risks of being physically attacked in places without administrators.

Assume risks, where the covers of energy saving devices placed inside automobiles in parking lots or placed in gardens are opened and the energy saving devices are connected to illegal devices and remotely operated. Furthermore, assume risks of intruders making setting changes in home appliances while the families are out and connecting the home appliances to unauthorized sites.

2) Assumption of illegal reading and rewriting

1) Assumption of risks of reading information from discarded IoT devices on what should be protected

Assume risks of third parties' reading of software of discarded IoT devices or settings and analyzing the mechanisms of connections to be utilized for IoT attacks or reading personal information to be used for unauthorized access by spoofing.

2) Assumption of risks of illegal mechanisms embedded in IoT devices and sold as second-hand products.

Assume risks of third parties' overwriting of software of IoT devices to be connected to unauthorized sites and put into auctions or sold at used stores.

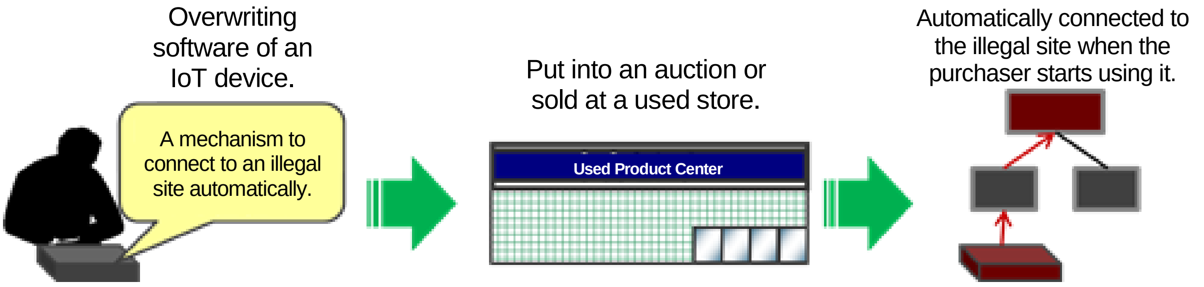


Fig. 7 Risk example of the sale of a used IoT devices connecting to an illegal site

Key Concept 7. Learn from past cases

(1) Points

1) Learn about examples of attacks and measures from past cases of attacks against ICT, including personal computers.
2) Learn about examples of attacks and measures from precedent IoT attack cases.

(2) Commentary

At the time of implementing security measures for IoT devices, it will be possible to refer to examples of past attacks and measures to prevent incidents or take measures against incidents that have occurred.

At the time of connecting to the Internet or other networks, there will be a threat of being attacked through the Internet or other networks. Many attacks against IoT devices have been using past methods of ICT attacks, and it is effective to consider security measures for IoT devices by referring to past cases of ICT attacks and countermeasure, including those against personal computers and measures. Furthermore, precedent IoT attack cases and measures can be referred to for security measures.

As a precedent case of an IoT security incident, it became clear that multifunction peripherals (MFPs) and web cameras not provided with suitable security measures were in a condition allowing third parties' unauthorized access through the Internet. In response to such precedent IoT attack cases, concerned organizations, including the IPA and IoT device manufacturers have been providing information calling for users' attention to security measures.

(3) Examples of measures

1) Examples of attacks against ICT, including personal computers, and measures

Examples of attacks against personal computers are shown below.

Several types of malicious and influential malware were discovered in personal computers around 2001. The malware adversely influenced not only local networks inside enterprises but also the mail servers of Internet service providers, which went down as a result, and routers, which made it impossible to handle enormous traffic and obstructed normal communication.

Specific examples of security measures for ICT, including personal computers, are shown below.

1) Enhanced firewall functions
   Block unnecessary services and packets to prevent unnecessary communication.
2) Automatic installation of updates
   Fix security holes quickly to prevent attackers from intruding.
3) Forced installation of antivirus software
   Automatically check the installation of antivirus software, and forces the installation of antivirus software if it is not installed.
4) Implement a mechanism to deactivate malware even if has intruded.
   Preliminarily register executable programs and control the startup of programs, thus preventing the activation of malware even if it has intruded. (Whitelist technology)

2) Examples of attacks and measures in precedent IoT attack cases

Examples of attacks in precedent IoT attack cases are shown below.

MFPs of a number of universities were ready to be viewed through the Internet. The accumulated data in these MFPs were easily accessible through the Internet if there were no firewalls for the MFPs and initial IDs and passwords were kept unchanged.

Furthermore, it became clear that the images of web cameras (73,000 cameras used for cafes, shops, malls, factories, bedrooms, etc.) around the world were open to the public without permission from suppliers and users unless suitable security measures were taken.

The following example shows security measures for IoT devices to be newly network connected.

1) Stop unnecessary Internet connections
   Do not connect IoT devices to the Internet unless it is necessary to do so.
2) Firewall installation
   Install firewalls for IoT devices, such as MFPs, to be connected to the Internet if they are accessible with ease through the Internet.
3) Password change
   Change the factory-set passwords for IoT devices to prevent unautorized access by spoofing from malicious third parties.

2.3 [Design] Principle 3: Consider a design to protect what should be protected

In order to realize IoT security measures within a limited budget and personnel, it is effective to narrow down what should be protected and isolate particular areas that should be protected. It is also effective to protect IoT devices and systems linking to other IoT devices and systems with low countermeasure functions. Furthermore, it is desirable to design IoT devices to maintain security even if IoT service providers and users connect unspecified equipment and systems, thus not causing inconvenience to connecting destinations even if an abnormality occurs.

The principle explains the five points to be considered at the time of designing to protect what should be protected in addition to the above design considerations.

Key Concept 8. Make a design that protects each individual and all

Key Concept 9. Make a design that will not cause trouble to connecting destinations

Key Concept 10. Establish design consistency to ensure safety and security

Key Concept 11. Make a design that ensures safe and safety regardless of connecting destinations

Key Concept 12. Verify and evaluate a design to ensure safety and security

Key Concept 8. Make a design that protects each individual and all

(1) Points

1) Consider measures for individual IoT devices and systems against risks via external interfaces, inclusion, and physical contact.
2) If measures for individual IoT devices or systems are not sufficient, consider measures to include IoT devices and systems at higher levels.

(2) Commentary

Risks that arise in IoT devices and systems include risks via external interfaces (I/Fs), i.e., I/Fs for normal use, maintenance use, non-regular use), inclusion risks, and risks resulting from physical contact. Attacks such as DoS, viruses, and spoofing and abnormal data from other equipment are assumed as risks via external interfaces.

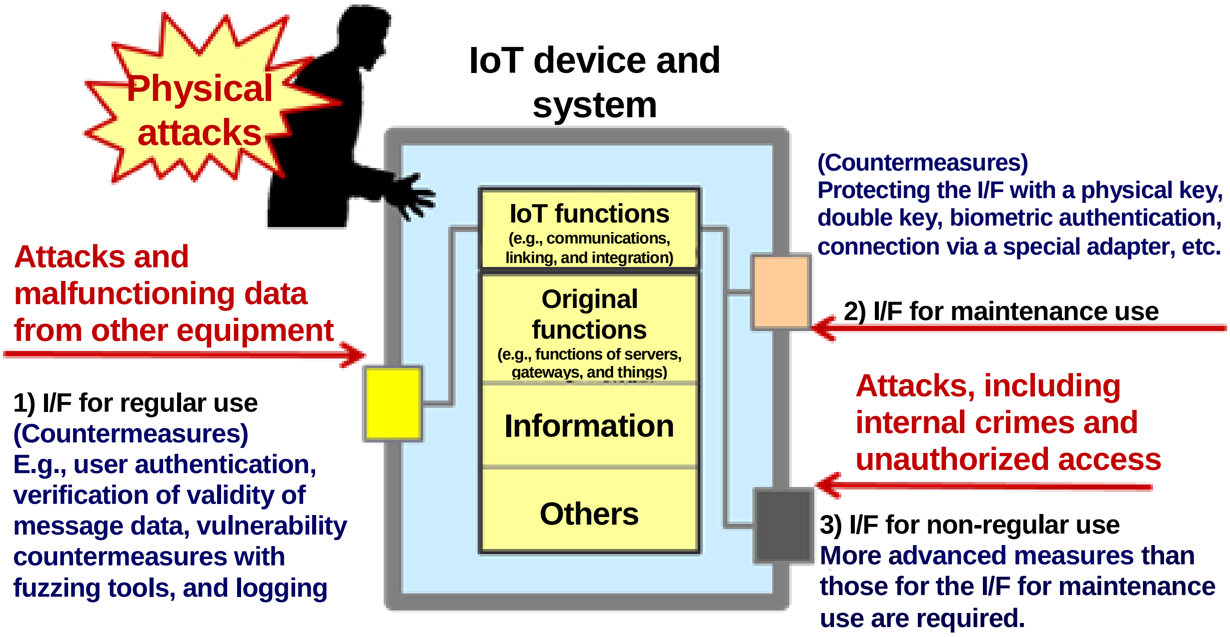

Physical attacks
IoT device and system
IoT functions
(e.g., communications, linking, and integration)
Original functions
(e.g., functions of servers, gateways, and things)
Information
Others
Attacks and malfunctioning data from other equipment
1) I/F for regular use
(Countermeasures)
E.g., user authentication, verification of validity of message data, vulnerability countermeasures with fuzzing tools, and logging
(Countermeasures)
Protecting the I/F with a physical key, double key, biometric authentication, connection via a special adapter, etc.
2) I/F for maintenance use
Attacks, including internal crimes and unauthorized access
3) I/F for non-regular use
More advanced measures than those for the I/F for maintenance use are required.

Fig. 8 Measures against Risks of External Interfaces

Inclusion risks are security problems in the designs, specifications, settings, etc. of devices and systems. Specifically, potential defects, misconfiguration, and malware illegally embedded before shipment, for example, are assumed. Risks resulting from assumed physical contact with devices include the theft and disassembly of the devices placed at home or in public spaces and the illegal replacement of any parts of the devices. Measures against these risks are necessary.

IoT devices and systems include low-performance devices, such as sensors, for which it is difficult to implement independent measures. In that case, it is necessary to consider measures to protect the IoT devices and systems, including those at upper levels.

(3) Examples of measures

1) Measures against risks via external interfaces/inclusion/physical contact

1) Measures against risks via external interfaces
   - Measures against risks via I/Fs for normal use, include user authentication, the verification of the

validity of message data, vulnerability measures with fuzzing tools used, and logging.

- I/Fs for maintenance use are for maintenance members and operators. Therefore, measures include the authentication of connected devices and user authentication. There are an increasing number of cases where particularly important devices are protected with physical keys and connections through double keys, biometric authentication, and special adapters.
- I/Fs for non-regular use are for particular purposes, such as debugging purposes, and they have high authority in many cases. Therefore, high-security functions are required compared with other I/Fs.

2) Measures against inclusion risks

- Measures are taken against the external procurement of parts and software, where design data and quality data is obtained to check that there are no illegal embedding or quality problems.
- There are cases of checking the validity of internal data and software and the appropriateness of generated data as measures at the time of implementing devices handling contents. Concealment measures, such as the use cryptography, are taken for important data.
- Regular clock adjustments making use of external reliable systems and the tamper resistance performance of clock functions as measures are taken for devices with built-in clocks. In cases where multiple IoT devices and systems are involved, measures against the time synchronization among them are seen.
- Inspection tools, such as source code checker, are used in software development for smartphones, since those are capable of working on several platforms.

3) Examples of measures against risks occurring from physical contact

Design devices in order not to extract important data, software included. Examples are shown in the table below.

Table 6 Examples of measures against risks resulting from physical contact (tamper resistance)

Type of countermeasure	Example of countermeasure
Secure design of hardware, and structural settings	- Designs to cut off the wiring in devices or destructing interfaces if the devices are disassembled. - Removal of unnecessary non-regular I/Fs and exposed wiring - Designs that prevents access internally unless dedicated authentication devices are connected. - Electromagnetic shields are used so as not to expose electromagnetic waves. - Internalization of chips and wiring.
Secure design of data, and software	- Implementation of a function that remotely locks terminals stolen or lost. - Software obfuscation and encryption. - Encryption of confidential data and the time reduction of the existence of confidential data in memory in use. - Prevention of the execution of the program and data falsification in memory.

Mobile devices, such as smartphones, implements a function to clear data on their storage, so as not to expose data to others. This function is used in case those are rented, reused, or disposed.

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

A cost reduction is possible by taking measures against what should be protected instead of protecting the entire devices and systems.

- It is possible to divide systems or divide devices that make up IoT devices and systems into a number of domains through physical or virtual gateways and localize the influence of abnormalities, if occurred, or protect important functions with multiple gateways.

- There is a method to use peripheral devices at a high-security level to read, encrypt, and send important information associated with financial settlement directly to a server instead of using ordinary devices so that no important information will be left in the ordinary devices. This method makes it possible to strengthen security and reduce countermeasure and management costs, and the POS industry is promoting the standardization of the method.

2) Measures to protect low performance IoT devices and systems using higher layer

Consider measures to use high-ranking IoT devices and systems to protect IoT devices and systems that cannot incorporate security functions due to their insufficient performance.

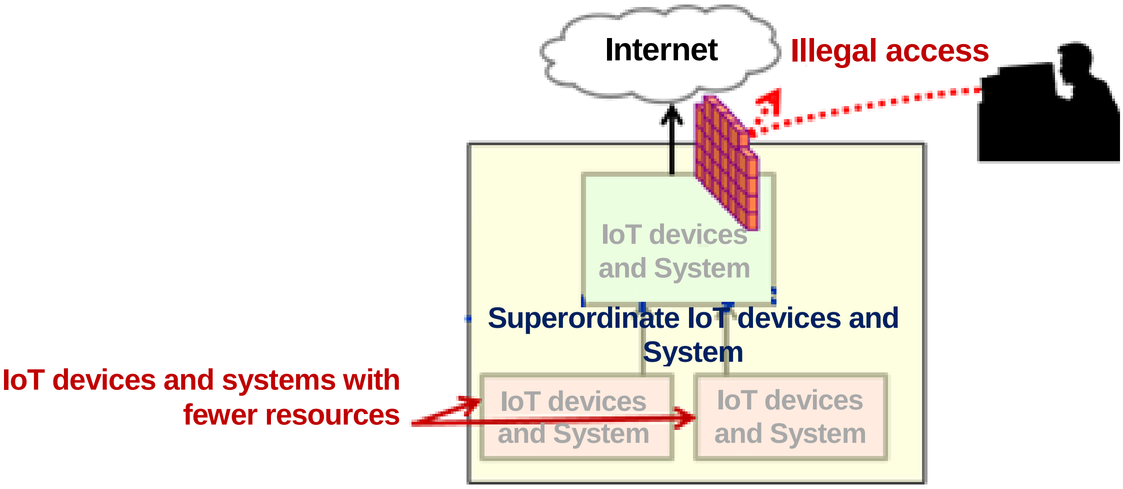


Fig. 9 Image of the superordinate IoT devices and system protecting low-ranking IoT devices and systems

- Design to block cyberattacks at the contact point between internal IoT devices, systems and external internet.
- In addition, use other IoT devices and systems incorporating monitoring functions to monitor the devices and systems to detect errors and find probable causes. The Broadband Forum (BBF) specifies TR-069 as a standard specification for the remote management of home appliances.

- Developers of IoT devices and systems for which no adequate measures can be taken due to restrictions on the product specifications specify countermeasure against risk to be considered at the time of using the IoT devices and systems in manuals and usage guides.

Key Concept 9. Make a design that will not cause trouble to connecting destinations

(1) Points

1) Consider a design that can detect abnormalities in IoT devices and systems.
2) Consider appropriate behaviors at the time of detecting abnormalities.

(2) Commentary

If an abnormality occurs as a result of a software or hardware malfunction or attack, it will be necessary to detect the condition of the abnormality in order to prevent the influence of the abnormality. If an abnormality is detected in an IoT device or system, there is a possibility that the influence may spread to other IoT devices or systems depending on the content of the abnormality. Accordingly, it is necessary to consider measures such the separation of the IoT device or system from the network.

When IoT devices and systems 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 devices and systems that are using the functions of the IoT devices and systems.

(3) Examples of measures

1) Detection of abnormal conditions and prevention of the influence from spreading

1) Detection of abnormal conditions

First, it is necessary for each individual IoT device and system to detect abnormal conditions. However, there are cases where the IoT device or system cannot detect its own abnormality depending on its specifications and the abnormal state. There is an example of measures to detect such an abnormal state by referring to log information on the IoT device or system through a monitoring server.

An example of log monitoring is shown below.

- Monitoring a number of linking IoT devices and systems
  In cases where importance is attached to a number of IoT devices and systems, a method to confirm the consistency of the processing results of relevant components will be available to monitoring systems. A study on effective methods to detect abnormalities is making progress.
- Load increase suppression with IoT device and system monitoring

Log monitoring consumes resources on the server side, such as CPU, storage area, and network bandwidth resources. Therefore, a proper monitoring method needs to be set for each system and IoT device according to the scale of the system and the performance of each IoT device and system.

2) Suppression of the spread of the influence of abnormal condition

- If the IoT devices or systems detect the abnormalities, the IoT devices or systems come to a stop or disconnect themselves from networks to suppress the influence of abnormalities that may affect other IoT devices or systems.
  If a monitoring server on a network detects an abnormality in IoT devices or systems, the monitoring server will instruct the IoT devices or systems to come to a stop or disconnect themselves from the network or will use appropriate devices, such as routers, to disconnect them from the network.

2) Method of recovery from abnormalities

1) Suppression of functions with the occurrence of abnormalities

If an abnormality that has occurred is determined to be limited to a function, the execution of the function will be restricted while other functions will be executable. An example of the restriction of functions is shown below.

- Closing only the reception port of the function.
- Stopping only the process of executing the function
- Making environment settings so that the function will always return an error.

2) Restarting/Reconnecting IoT devices and systems

- Depending on the situation, there are cases where the abnormalities of IoT devices or systems will be resolved by restarting the IoT devices or systems. The IoT devices or systems will restart themselves upon detecting abnormalities or external devices, such as monitoring servers, will restart the IoT devices or systems.
- The IoT devices or systems disconnected to prevent the spread of the abnormalities will be restored in accordance with their operation policies or functions and reconnected to the networks.

3) Resilience of IoT devices and systems

- The restoration performance of systems and services is treated under a concept of resilience, to which importance has been attached in the IoT field. Resilience has been taken up by major standards and can be used as a reference in considering measures.[8]

[8] The International Organization for Standardization (ISO) has been making progress in resilience-related standardization. In the ICT/IT system field, ISO/IEC 27031 (Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity) and ISO/IEC 27001 (Information security management) standards have been formulated. Besides, in the NIST CPS Framework, resilience is an element of credibility in addition to security, privacy, safety, and reliability.

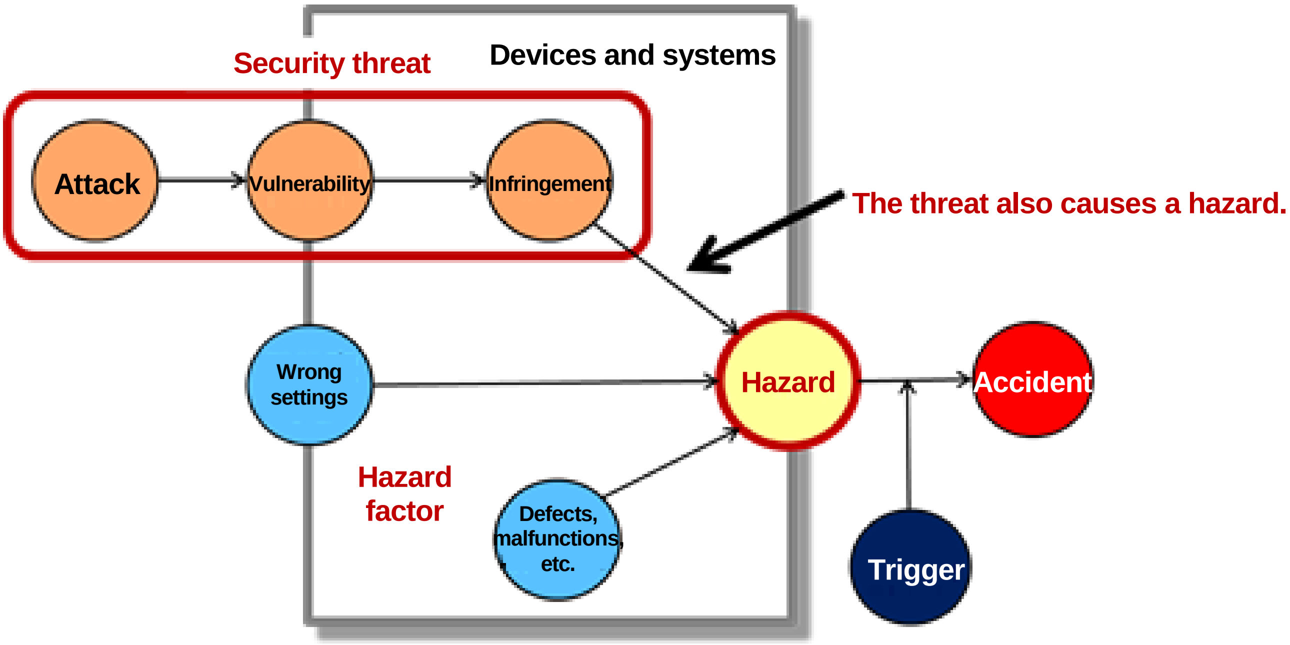
Key Concept 10. Establish design consistency to ensure safety and security

(1) Points

1) Visualize designs to achieve safety and security.
2) Confirm the mutual influence of designs to achieve safety and security.

(2) Commentary

There are cases where a security threat can be a hazard factor of safety. For example, there is a possibility that some trigger causes a malfunction if an illegal invasion of an IoT device or system by a third party interfere with software or data. Attention is required to attacks against safety functions, in particular, which may lead to a system down or accident. Furthermore, the incorporation of safety functions may adversely affect the performance of the original functions of the IoT device or system. The visualization of safety and security designs is effective to confirm whether these measures are properly taken.



Source： Created on the basis of the SESAMO project *SECURITY AND SAFETY MODELLING FOR EMBEDDED SYSTEMS*

Fig. 10 Model of security problems affecting safety

At the time of checking the design quality of safety and security, it is necessary to confirm not only hazards and threats along with risks caused by them but also the mutual influence of safety and security. At that time, it is also effective to visualize the mutual influence and make it easy to confirm design consistency among engineers of different departments and different companies.

Furthermore, it is a major premise to secure safety according to safety regulations, if any.

(3) Examples of measures

1) Visualization of safe and secure designs

- The visualization of designs is to visualize the processes of each design, such as the analysis, designing, and evaluation processes, including the background and basis. It is expected to be useful for mutual design quality sharing among safety and security engineers. It can also be used to understand and evaluate design quality when diverting existing functions to new products.

- The visualization of designs can be utilized to explain and agree on the design quality of safety and security not to developers of the designs but also to other parties, including design managers, ordering parties, and subcontractors. Even if an accident happens, it is possible to fulfill the accountability to the victim without hastily checking the situation or preparing materials. Various visualization methods have been devised and utilized according to the development object and development environment.
- As an international standard for achieving the dependability of consumer devices, *Dependability Assurance Framework for Safety Sensitive Consumer Devices (DAF)* as a Meta-standard is available for visualizing safety and security designs and developing them while mixing.

2) Confirmation of the mutual influence of safety and security

- It is necessary to identify functions to be protected and analyze threats and risks as security measures. Examples of studies are shown below.
- Analyze threats and risks against functions (requirements) to be protected, study security measures, and analyze and evaluate the influence of effects and functions to be protected. Reanalyze and restudy if the results of the evaluation are not acceptable.
- If the scale of functions to be protected is large, it will be complicated to conduct an impact analysis of security measures in full. The Design Review Based on Failure Model (DRBFM) is an example of an influence analysis method in this case. In this method, designers focus on changes and variations, carefully identify concerns and think about responses from designing viewpoints and prevent problems by reviewing the designs from many insights with opinions from experts and professionals.
- The biggest risk to be expressed by IoT conversion is that it is not possible to guarantee the expected results of the designed functions of the IoT devices and it is necessary to consider that cyberattacks and system failures can occur. It is difficult to make all risks zero. When designing IoT devices and systems, it will be necessary to consider measures systematically in advance. Furthermore, it will be necessary to make a transition to a safe state in order to secure the level of safety required by existing laws and regulations if the IoT devices or systems fall into a situation where the results cannot be guaranteed. (e.g., Fail Safe and Fail As Is)

Key Concept 11. Designing to ensure Safety/Security even when connected to unspecified entities

(1) Point

1) Consider a design to determine how to connect IoT devices and systems according to the destination and connecting situation.

(2) Commentary

In many cases, even combinations of devices not connection tested by the manufacturers of the devices are utilized by connecting devices having industry standard functions. For that reason, as the IoT becomes widespread, there are an increasing number of cases where unspecified devices not intended by manufacturers for IoT use are connected and used by integrators and users. In that situation, if a device with low reliability is connected, confidential information may easily leak out or an unexpected action may occur. Furthermore, with an elapse of time, there will be increasing cases with no connection checks made on products manufactured by the same company but different in model, version, or shipment period. It is necessary to consider a design to determine how to connect IoT devices and systems according to the destination and connecting situation.

(3) Examples of measures

1) A design to check the connecting party and connected situation and determine how to connect them

When connecting to another device, it will be possible to consider a design to determine whether or not to connect according to the content of information on the identity of the partner device, including the manufacturer, year of production, and compliance standard. Furthermore, a design that extends the scope of connections is considered while suppressing risks within an acceptable range by changing the ranges of functions and information to be provided according to the identity of each connection partner.

- Restrictions will be considered in a way that allows full connections to all devices the same in manufacturer and connections with certain restrictions to devices manufactured by companies belonging to the same industry group.
- There is a way to raise the security level by using important functions only when the connected counterpart is confirmed as a device appropriately authorized. For example, an overseas ATM is used for the purpose of preventing operation at an unauthorized terminal at maintenance.
- On the other hand, a higher business chance and greater user convenience in the IoT are expected from a wider range of connections. Therefore, devices of other companies in different industries or companies with no business relations can be provided with minimum functions and information as long as the devices comply with certain safety and security standards.
- An attempt has been made to accumulate information on the connection style and usage of devices that cause errors and utilize the information for the prevention of errors.

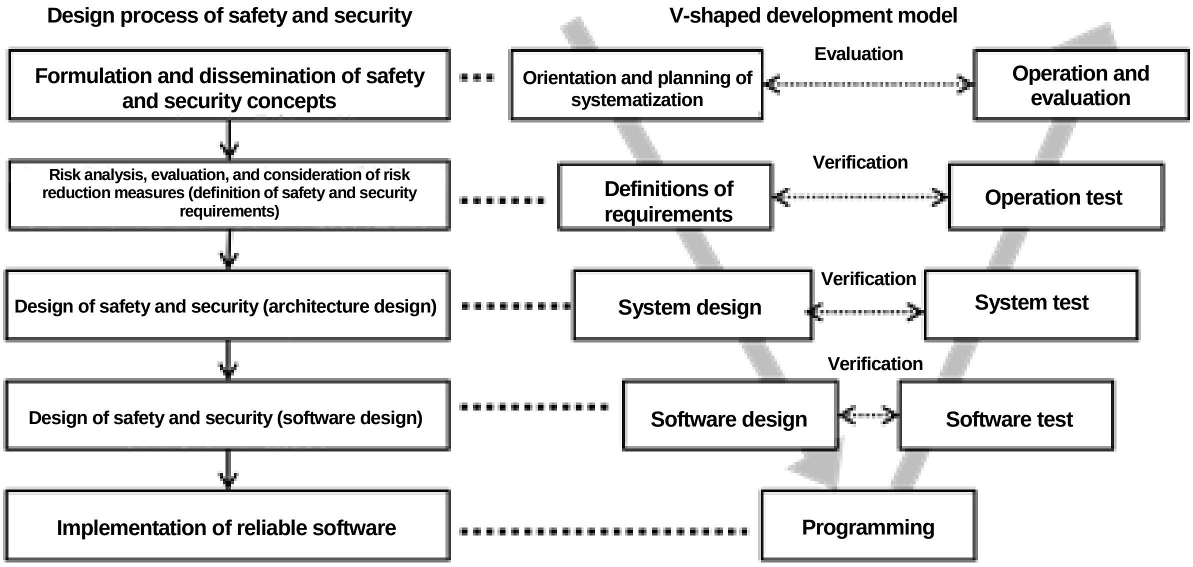
Key Concept 12. Verify and evaluate a design to ensure safety and security

(1) Point

1) Verify and evaluate the designs of connecting devices and systems to ensure safety and security with consideration of risks unique to the IoT.

(2) Commentary

A V-shaped development model can be cited as a plan for verifying and evaluating that the design is realized in devices and systems. The figure below shows an example of a V-shaped development model in safety and security design.


Design process of safety and security
V-shaped development model
Formulation and dissemination of safety and security concepts
Orientation and planning of systematization
Evaluation
Operation and evaluation
Risk analysis, evaluation, and consideration of risk reduction measures (definition of safety and security requirements)
Definitions of requirements
Verification
Operation test
Design of safety and security (architecture design)
System design
Verification
System test
Verification
Design of safety and security (software design)
Software design
Software test
Implementation of reliable software
Programming

Source: Introduction of Safety and Security Design of Connecting World

Fig. 11 Verification and Evaluation of Safety and Security Design

In the case of IoT devices and systems, there will be a possibility of unexpected hazards and threats only when they are connected. Therefore, it will be necessary not only to verify that the devices and systems satisfy safety and secure design requirements but also to evaluate and ensure that the safety and secure designs of the devices and systems are appropriate in the IoT.

(3) Examples of measures

1) Examples of reflection items in verification and evaluation

1) Reflection on each guideline

Reflect the content of each guideline with necessary items in the evaluation.

2) Validation and evaluation according to the level of safety and security measures for devices and systems

With regard to safety and security, international standards have been established in some industries, and the requirements can be used for in-house item extraction and validation. Furthermore, the objective evaluation of the level of safety and security measures is also implemented by third party certification based on the standards.

- International safety standards
  With regard to functions to achieve safety, IEC 61508 for functional safety and its derived standards (e.g., 26262 for the automobile field and IEC 62061 for the industrial machine field) have been established. As for IEC 61508, security matters have been added in the second edition.
- International product security standards
  - Common criteria (ISO/IEC 15408)
    A standard to evaluate the proper designing and installation of devices and systems related to information technology from the viewpoint of information security while devices and systems approved in accordance with international agreements are recognized to be effective in member countries.
  - Embedded Device Security Assurance (EDSA) authentication
    This is a security evaluation system for control equipment and consists of three evaluation items, i.e., evaluation of security, implementation of security functions, and communications robustness testing.
- Others
  Third-party evaluation by the private sector is also effective in fields where international standards are not being developed. In the United States, security evaluation agencies such as ICSA Labs and NSS Labs are conducting evaluations of communications equipment. In Japan, the Connected Consumer Device Security Council (CCDS) prepared security evaluation guidelines for equipment such as ATMs and on-vehicle equipment (e.g., car navigation systems).

3) Confirmation that measures are taken against known hazards and threats

With regard to the IoT, it is assumed that new hazards and threats will occur as the IoT is widely spread in the future. Accordingly, grasp the latest information in collaboration with stakeholders and evaluate the information in the evaluation of the IoT.

2.4 [Implementation and Connection] Principle 4: Consider security measures on the network side

In the IoT where devices and systems with diverse functions and capabilities are connected to each other, it is important to consider security measures from the aspects of IoT devices, systems, and networks, not only to demand security measures to devices.

This section explains four requirements for secure connection and construction of services and systems.

Key Concept 13. Provide a function to grasp and record the condition of devices

Key Concept 14. Proper establish network connections according to the function and use

Key Concept 15 Pay attention to the default settings

Key Concept 16. Prepare/Provide an authentication function

Key Concept 13. Provide a function to grasp and record the condition of devices

(1) Points

1) Consider a function of grasping and recording the state of devices and their status of communication with other devices.
2) Consider a function to prevent records from being illegally deleted or falsified.

(2) Commentary

With various devices and systems connected to a network, it is not easy to grasp what kinds of devices and systems are connected, how they are connected, what problems are happening in the devices, and where are the problems on the network. In order to detect and analyze the occurrence of abnormalities, clarify the causes, or consider measures, it is necessary for each IoT device and system to collect and grasp its own state and status of communication with other devices. Furthermore, it is necessary to investigate the causes of the abnormalities because all collected information needs to be kept on log record. However, even if the log records are kept, no effective measures can be taken if attackers illegally delete or alter the contents. Accordingly, it will be necessary to take measures to ensure correct recording.

Furthermore, some IoT devices and systems include low-function devices, such as sensors, and it is sometimes difficult for such devices and systems to manage a large number of logs and take measures such as encrypting log records by themselves. For such devices, it is necessary to take other measures such as the preparation of equipment for log management.

(3) Examples of measures

1) Grasp and record the state of each device and the status of communication with other devices.

- Put the operation of each IoT device and system on log record.
  Example of contents to be recorded)
  - For security analysis: Attacks, user authentication, data access, configuration management information updating, running applications, log recording start/stop, communication, door opening/closing, checksum, movement history
  - For safety analysis: Failure information (hardware/software)
  - For reliability analysis: Result information, status information, operating environment information (temperature, humidity, CPU load, network load, resource usage etc.) and software updating
- Formulate a storage policy because the resources for storing logs are finite.
- Synchronize the clocks so that related IoT devices and systems will coincide in log recording time.
- Consider the timing of log recording for the entire IoT devices and systems instead of making individual settings for each device.
- Describe in manuals that log recording is for the maintenance of IoT devices and systems.

2) Illegal deletion of records and prevention of tampering

- There is a method of setting log access authorization and encryption for IoT devices and systems.
- There is a method of regulally sending data collected by IoT devices and systems to other IoT devices and systems or dedicated devices incorporating a function to keep log records.
- Describe in manuals that logs are recorded for the purpose of maintaining the integrity of IoT devices.

Key Concept 14. Proper establish network connections according to the function and use

(1) Points

1) Consider a method of network connections depending on the function and use of each network, and construct and connect the network.
2) When considering the method of network connections, also consider the level of the function and performance of each IoT device.

(2) Commentary

It is necessary to construct, connect, and provide each IoT system and service with consideration of the functions and use of IoT system and service, the functions and performance of the IoT devices to be used, and the network configuration and security function.

It is necessary to implement security measures after considering whether to select either wired connections or wireless connections depending on the function and use. In addition, it will be difficult for IoT devices to achieve necessary security measures by themselves if the function and performance of IoT devices are limited in the IoT system and service. Accordingly, it is necessary for the IoT system and service to ensure the entire security of the IoT system and service including the devices.

(3) Examples of measures

1) Network connections according to function and use

Assuming an environment where IoT devices with different function and performance levels coexist, it will be necessary to design, construct, and connect IoT systems and services that will ensure the entire security of the IoT systems and services.

1) Basic network connection policy
   Make sure that security measures are taken to IoT devices connected to the Internet and keep in mind not to connect IoT devices without security measures taken or unnecessary IoT devices. Keep in mind that only IoT devices necessary for IoT systems and services are connected to the Internet.
2) Application of authentication function
   Implement security measures such as password authentication in each environment, e.g., wired connections or wireless connections or connections via secure gateways. Specific authentication functions are described in Key Concept 16.
3) Application of cryptographic function
   Security measures with cryptographic functions are implemented in each environment, e.g., wired connections or wireless connections or connections via secure gateways. In applying cryptographic functions, pay attention to the adoption of suitable cryptographic algorithms and hash functions, refer to the CRYPTREC Cryptography List (e-Government Recommended Ciphers List) of the Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry, and confirm whether there is no change or there is no fear of compromising during use.
   CRYPTREC Cryptography List (e-Government Recommended Ciphers List):
   http://www.cryptrec.go.jp/list.html
   A specific example of applying cryptographic functions is shown below.
   - Apply network encryption such as TLS for wired connections and WPA2 for wireless connections and take measures against the eavesdropping and falsification of data on the

network communication paths.

- Take measures against theft and unauthorized access of data on the cloud by applying file encryption and database encryption according to the cloud storage services delivery type on the cloud. Machines dedicated to encryption are recommended to use highly confidential data such as cryptographic keys.

4) Third party conformity evaluation system

System and service providers should consider using highly reliable systems and services certified by an appropriate third-party conformity assessment system, such as the ISMS conformity evaluation system.

2) Consideration of function and performance level of IoT device

Security measures, such as cryptography, cannot be applied to IoT devices with limited functions or performance, e.g., sensors. In order to secure the security of IoT devices with such constraints, it will be necessary to devide the role of security measures for each hierarchy of devices, networks, platforms, services, etc. as well as security measures for IoT devices alone in order to secure the entire security of the networks.

For example, when IoT devices that are difficult to take security measures are connected to the network, measures are taken to ensure security measures such as passing through a secure gateway before connecting to the Internet.

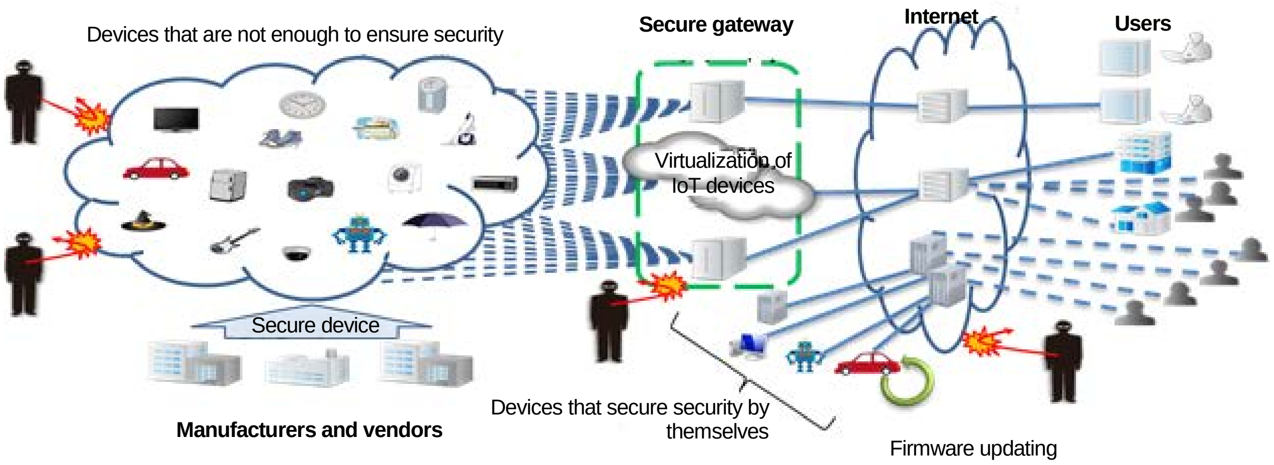

Devices that are not enough to ensure security
Secure gateway
Internet
Users
Virtualization of IoT devices
Secure device
Manufacturers and vendors
Devices that secure security by themselves
Firmware updating

Fig. 12 Connections via Secure Gateway

Key Concept 15. Pay attention to the default settings

(1) Points

1) Secure default settings should be made when implementing or connecting IoT systems and services.
2) Bring the default settings to users' attention.

(2) Commentary

When IoT system and service providers implement or connect systems and services, be careful of secure settings so as not to implement vulunerable systems which are easily attacked. Furthermore, it is necessary to bring the default settings to users' attention for the systems and services.

(3) Examples of measures

1) Default settings with consideration of security when constructing and connecting IoT systems and services

An IoT system and service provider should thoroughly make and manage password settings, such as those for administrator authority, stop unnecessary services and ports, and pay attention to default settings.

1) Suitable password settings and management

Proper management of password settings for administrators as well as users protect identity theft and unauthorized access by malicious third parties.

Specific examples are shown below.

- Do not leave the initial password settings. Properly make changes (with paying attention to the number of characters and the types of characters after the changes) and securely manage the passwords so that they will not be known to third parties.
  - Do not share passwords with unauthorized users.
  - Do not share passwords with other systems and services.

2) Application of access control

Perform appropriate access control with a firewall or other measures and prevent unauthorized access from outsiders.

3) Software update

There is a possibility that updated versions of firmware etc. have been released from an IoT device manufacturer after the IoT device is shipped and before the system or service is released. Therefore, at the time of releasing the system or service, check whether any updated versions are available. If the newest versions have been released, the IoT system or service provider should updates the firmware etc. by determining the necessity of the same and making sure that there is no problem updating the firmware etc. It should be kept in mind that such an updated version is to be downloaded from trustworthy websites, e.g., the IoT device manufacturer's website, through a reliable route and verified to be free of malicious modifications with a proper digital signature attached to it.

4) Stop unnecessary service ports

Prevent unauthorized access from the outside by stopping unnecessary network services, such as TELNET services, and ports as security measures other than authentication, access control, and software update.

Specific examples are shown below.

- Check and stop unnecessary network services, if any.
- Check and stop unnecessary ports, if any, not required for the service.

2) Bring the default settings to users' attention

Alert users about default settings from the standpoint of the IoT system and service provider.

1) Password change

Call users' attention to the change of initial password set at the time of shipping the IoT device. It will be effective to limit the functions unless the initial password is changed.

2) Firewall settings

If firewalls are effective to the IoT system and IoT devices, such as multifunction devices, alert users to install appropriate firewall.

Key Concept 16. Prepare/Provide an authentication function

(1) Points

1) Apply authentication functions for each IoT system or service that will ensure the security of the entire IoT system or service.
2) Use an suitable authentication method based on the constraints on the functions and performance of IoT devices.

(2) Commentary

Users' privacy information may leak as a result of an unauthorized IoT device passes itself as an authorized IoT device. An unauthorized user may impersonate an authorized user and take over and control an IoT device illegally. Furthermore, data on network communications paths and cloud platforms can be Eavesdropping and users' privacy information may leak. The introduction of mechanisms, such as authentication and encryption, are necessary as measures against such spoofing, eavesdropping, and threatening.

(3) Examples of measures

1) Authentication function that secures security of the entire IoT system and service

Apply an authentication function that ensures the security of the entire IoT system and service.

Specific examples are shown below.

- Take measures against the spoofing of IoT devices to be connected. Conduct authentication based on the IDs of the IoT devices, the client certificated, and message authentication. Furthermore, make connection rejection settings for unauthorized IoT devices.
- Take measures against user spoofing. Identify each user with the user's ID, password, IC card, or biometric authentication, etc.
- Take measures against the spoofing of systems and services to be connected. Mutually authenticate the IoT systems and services to be connected using keys or digital certificates.

2) Suitable authentication method based on constraints on the function and performance of IoT devices

According to the type of information handled, adopt authentication technology that can prevent data falsification and leakage regardless of any restrictions on the IoT devices or network.

Specific examples are shown below.

- Application of authentication using encryption

  Falsification or other threats are assumed by negligence or on purpose upon updating firmware for IoT devices. In order to update the firmware for the IoT devices correctly to reject such threats, it is necessary to ensure the validity of the updated data. In order to update firmware under restrictions on the function and performance of IoT devices or networks, the use of cryptography is effective.

2.5 [Operation and Maintenance] Principle 5 Maintaining a safe and secure state and disclose and share information

Various devices exist in the IoT, and devices and systems used for a long period in excess of 10 years are assumed. Accordingly, not only failures in devices but also various environmental changes are considered, including the deterioration of security measures and network environmental changes. Therefore, it is important to think of security measures after devices, systems, and services are shipped or released.

This guiding principle assumes the situation of devices, systems, and services after they are put into the market and explain five key concepts that parties concerned with the IoT devices, systems, and services should deal with.

Key Concept 17. Maintain product safety and security after product shipment and release

Key Concept 18. Grasp IoT risks after shipment or release and keep relevant stakeholders informed of what should be observed

Key Concept 19. Have general users know connection risks

Key Concept 20. Recognize the roles of the stakeholders of IoT systems and services

Key Concept 21. Grasp all vulnerable devices and give appropriate cautions

Key Concept 17. Maintain product safety and security after product shipment and release

(1) Points

1) IoT system and service providers should consider and apply methods in a timely manner to implement updates and other necessary matters that are important from the security viewpoint of IoT devices.

(2) Commentary

The vulnerability of IoT devices may be discovered after they are shipped. Therefore, it is necessary to provide means to distribute updated software with measures against the vulnerability of the IoT devices.

It is necessary for IoT system and service providers to apply important security-related updates to IoT devices at necessary timing with consideration of the characteristics of each IoT system and service field.

This guiding principle does not intend to keep IoT devices updated but recommend to keep IoT devices in a safe and secure state by properly implementing important security updates.

(3) Examples of measures

1) IoT device updating

IoT system and service providers apply important security-related updates to IoT devices at necessary timing with consideration of the characteristics of each IoT system and service field.

1) Consideration of updating methods

Study an updating method with consideration of the IoT system and service environments. For example, study the use of remote or USB media. In the case of using USB or similar media, make virus checks at the time of updating to prevent virus contamination.

Furthermore, check that automatic firmware updating for IoT devices is not problematic.

If the performance degradation of the IoT devices during firmware updating or an adverse influence on the functions and safety of the IoT devices is expected due to network bandwidth insufficiency, consider a method to specify updating date and time settings or enable bandwidth control. Consider a method that enables automatic version down as well (in the case of automatic updating, in particular) if the IoT devices stop working after firmware updating.

In the case of remote updating, it is necessary to take security measures for updating functions so that the updating functions will not be taken over and abused.

2) Installing updating function

Install an update function in IoT devices so that firmware updating will be possible.

Specific examples are shown below.

- Install a function that enables IoT devices to update the firmware etc. automatically or manually.
- In the case of IoT devices at remote locations, install a function that enables IoT devices to update the firmware etc. remotely.
- Consider the authentication of IoT devices and encryption of updating files in order to prevent the spoofing of IoT devices to be updated. Also, consider the introduction of a key management system to respond to the compromise of encryption, if necessary.
- Consider installing a simple function to IoT devices used by general users so that firmware updating will be possible with the IoT devices turned off and on.

3) Perform updating

Update the firmware etc. according to the result of 1). Keep in mind to obtain updates after verifying that digitalsignatures are attached to the updates without being falsificationand download updates through reliable websites, such as the manufacturers of the IoT devices.

Key Concept 18. Grasp IoT risks after shipment or release and keep relevant stakeholders informed of what should be observed

(1) Points

1) Collect and analyze vulnerability information, and transmit the information to users and other system and service providers and operators.
2) Explain important points about security in advance to users.
3) Tell stakeholders what should be observed at each stage of the life cycle of IoT devices, i.e., the stages of installation, connection, operation, and maintenance, after the IoT devices are released and shipped.

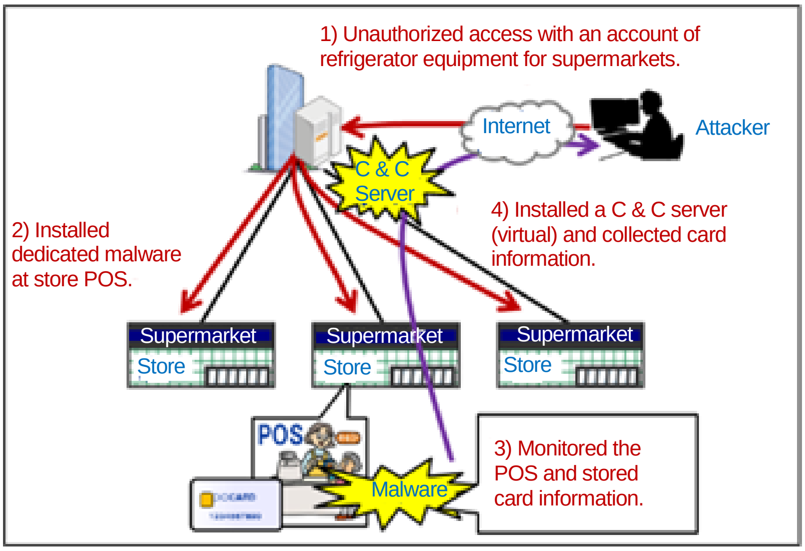
(2) Commentary

It is necessary to gather and analyze vulnerability information, if any, on systems and services to be provided and transmit the information to users and other system and service providers.

Furthermore, IoT system and service providers must state security points to be kept in mind in their system and service conditions or usage precautions and explain the points to users before they start using the systems and services.

There is also a risk that unexpected problems will occur after IoT devices are shipped. For example, a major U.S. retailer was infected with a POS virus in 2013 and information on 40 million credit and debit cards and 70 million customers leaked. Despite a rapid increase of new types of POS viruses since around 2011, measures may have been inadequate. In addition, there were cases where serious vulnerabilities were discovered in widely popular open source software (OSS), such as Heartbleed in 2014. If security threats affect safety functions, in particular, unexpected accidents may occur.

In order to respond quickly to these problems, IoT equipment manufacturers and system and service providers need to cooperate with stakeholders to continuously collect and analyze information.


1) Unauthorized access with an account of refrigerator equipment for supermarkets.
Internet
Attacker
C & C Server
2) Installed dedicated malware at store POS.
4) Installed a C & C server (virtual) and collected card information.
Supermarket Store
Supermarket Store
Supermarket Store
POS
Malware
3) Monitored the POS and stored card information.

Despite the rapid increase of new types of POS viruses, measures were insufficient.

Source: Created on the basis of threat examples against CCDS home appliances

Fig. 13 Attack Cases against POS Terminals

IoT devices and systems are used for a long time at the stage of installation, connection, operation, and maintenance after they are released and shipped. Sometimes they are reused, but finally, they will be discarded. The following safety and security problems are assumed during the life cycle.

- At the installation and connection stages
  - Installation in an environment without a firewall
  - Login password not set yet
- At the operation and maintenance stages
  - Degradation of security functions due to aging.
  - Discovery of new vulnerabilities.
  - Password settings that others can guess.
  - Software updating not yet implemented.
  - Use before or after the support period.
  - Occurrence of troubles that are difficult to recover even with the recovery function designed for the systems or devices.
- At the reuse and disposal stages.
  - Non-erasure of included personal information and confidential information.

Measures at the time of designing are not sufficient for dealing with the above problem, and it is necessary to request measures to companies concerned with the installation, connection, operation, maintenance, and disposal of IoT devices and systems.

(3) Examples of measures

1) Collection, analysis, and dissemination of vulnerability information

It is necessary to gather and analyze vulnerability information, transmit the information to users and other system and service providers, and take necessary measures such as firmware updating. Keep in mind to obtain updates after verifying that electronic signatures are attached to the updates without being tampered and download updates through reliable websites, such as the manufacturers of the IoT devices.

Specific examples are shown below.

1) Collection and analysis of vulnerability information

- IoT system and service providers should collect and analyze information on vulnerability and incidents that occur while operating the IoT systems and services.
  - IoT system and service providers should understand and manage basic configuration information on the IoT devices, systems and services that they provide.
  - IoT system and service providers should investigate the impact of acquired vulnerability information and incident information on the IoT devices, systems, and services that they provide.
  - IoT system and service providers should select pieces of information that need to be transmitted out of all pieces of information expected to affect outside the company.
- Furthermore, it is necessary to consider a mechanism to collect vulnerability information and incident information grasped by stakeholders in contact with actual sites and feedback the information to IoT device manufacturers and IoT system and service providers.
- Collect and analyze information transmitted by IoT device makers, public institutions, ISAC, etc. The following organizations collect such information.

Table 7 Examples of Organizations Collecting Vulnerability Information etc.

Name		Overview
In Japan	JPCERT/CC	A neutral international security emergency response organization that collects and responds to threats for many years, and collects and discloses vulnerability information in collaboration with the IPA. - Vulnerability countermeasure information portal site (JVN) - Vulnerability countermeasure information database (JVN iPedia) A database connecting vulnerability countermeasure information that has been opened to the public in Japan and overseas along with vulnerability countermeasure information published by the JVN and widely opening such vulnerability countermeasure information found on a daily basis for public use. Vulnerability information on OSS can be acquired as well.
	ISAC (Information Sharing and Analysis Center)	Sharing industry-specific information on incidents, threats, and vulnerabilities on an industry-by-industry basis and exchanging information among members.
	IPA: Ten major information security threats	Publicizes the most serious threats reported by experts each year and promotes vigilance.
Overseas	Black Hat	An international conference on computer security announcing research on the latest attack cases and countermeasures.
	Cyber Treat Alliance	An organization established by a US security company aiming at sharing the latest information and publishing white papers and other security-related information.

＊ The OSS Community, an organization consisting of developers and stakeholders, provides OSS vulnerability information, shares bug information, and creates correction patches. Information can be gathered on the Community's website as well.

2) Transmission of information

It is necessary for each IoT system and service provider to transmit information to stakeholders if configuration information matches vulnerability information. Consider utilizing information provision services on portal sites as windows or channels to link with general users' information.

Examples of destinations are shown below.

- Computer Security Incident Response Team (CSIRT)
  A CSIRT responds urgently to computer security incidents and conduct countermeasure activities. There is a case where an enterprise establishes an in-house CSIRT that takes measures in response to in-house and customer reports while cooperating with other enterprises' CSIRTs in taking measures.
- JPCERT/CC
- ISAC

In the case of transmitting information externally or sharing information with outsiders, ascertain the range of parties affected, select destinations, and pay attention to the method and timing of data transmission.

Disclosing vulnerability information without any prospect of measures will cause new risks such as receiving zero-day attacks. Therefore, carefully consider the timing and destination of information dissemination and sharing.

- JPCERT/CC Handling Guidelines for Vulnerability-related Information
  (https://www.jpcert.or.jp/vh/vul-guideline2014.pdf)

2) Explanation of important security issues in advance

IoT system and service providers should describe security concerns in their important explanations (including service conditions and usage precautions) and explain them to users before the users start using systems and services.

Specific examples of explanation methods are described below.

1) Information provided on websites
2) Described in the service agreements, manuals, etc.
3) Displayed on the screens of IoT devices and systems if the screens are available.

3) Informing stakeholders of items to be observed at each life cycle after IoT devices and systems are released and shipped.

The following examples show items that stakeholders should be observed.

1) Countermeasures at the time of installation and connection
- Response to installation in environments without firewalls
  - Transmission of essential items when connecting to an external network (e.g., firewall installation).
- Login password settings
  - Transmission of what should be changed from the initially set ID and password.

2) Measures at operation and maintenance stages
- Response to the degradation of the security functions of IoT devices and systems and new types of vulnerability.
  - Promotion of the use of a software updating function.
- Setting a password difficult for others to guess and software updating.
  - Request for the training and thoroughgoing management of operational training.
  - Request to set up an automatic updating function.
- Use before or after the support period.
  - A notice of the support period, advanced notice of the termination of the support period, and notice of the termination of the support period.
  - Posting of messages on the company's website and displaying messages on the devices and systems.
  - Technically restricting network connections if there is a risk of connections after the support period is terminated.

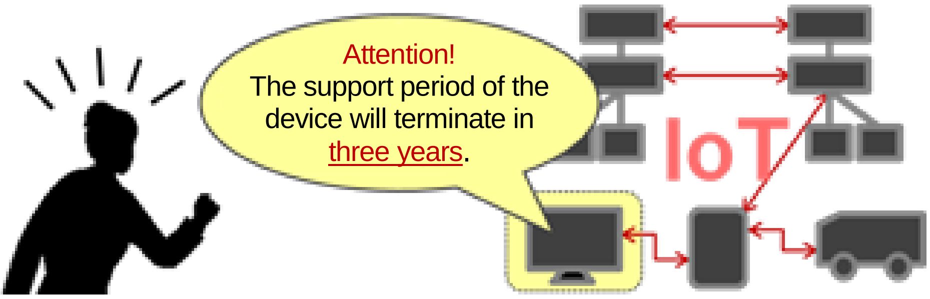

Attention!
The support period of the device will terminate in three years.
IoT

Fig. 14 Notice of Support Period

- Responding to obstacles that make the restoration of systems and devices difficult even with the designed recovery functions of the systems and devices.
  - Request to consider the reconfiguration of software and encryption keys from the viewpoint of management systems.
  - Requesting to consider a manual restoration procedure if systematic restoration is

impossible.

- Request a procurement method and deployment of spare devices, parts, and systems.

3) Measures for reuse and disposal

- Non-erasure of included personal information and confidential information
  - Reminding users that personal information and confidential information exists in IoT devices and systems.
  - Explanation of risks related to the non-erasure of information.
  - Installing a program to completely erase personal information and confidential information.

Key Concept 19. Notify general users of connection risks

(1) Point

1) Inform general users of risks of damaging not only them but also others as a result of careless connections and improper use and risks of affecting the environment, along with matters to be observed by them.

(2) Commentary

General users' careless connections and illegal use will increase a risk of being illegally remote controlled or causing malfunctions.

Even if IoT device manufacturers and IoT system and service providers take various countermeasures and risk reduction measures to an acceptable level, there is a latent risk of affecting general users. Furthermore, risks not assumed at the time of release or shipment may occur. It is necessary to tell general users about the existence of such risks.

When using IoT devices, it is necessary to inform general users of risks as well as the convenience of the IoT devices. It is necessary to inform general users not to connect IoT devices and systems carelessly or use them illegally, explain the necessity for measures against the vulnerability of IoT devices and systems, and gain their cooperation.

(3) Examples of measures

1) Informing general users of risks resulting from careless connections and matters to be observed.

General users' careless connections and illegal use will increase a risk of being illegally remote controlled or causing malfunctions. Therefore, inform general users of such risks.

Specific examples are shown below.

1) Method to inform general users
- If an IoT device has a screen, display the method on the screen.
- Describing such risks in IoT device and system manuals (Information from the IoT device manufacturers and system and service providers to general users).
- Describing such risks in warranty cards.
- Posting such risks on the companies' websites.

2) Content of the information for general users
- Recommended connections (guaranteeing the operation of the IoT devices and systems).
- Updating.
- Factory default settings if automatic updating functions are available.
- Security settings such as wireless LAN key (e.g., Wi-Fi) security key settings.
- Password settings difficult for others to guess.
- Utilization of a program to completely erase private and confidential information as measures against leakage of personal information and confidential information at the time of reuse or disposal.

Furthermore, it is preferable to notify general users properly by referring to the rules for general users described in *Chapter 3 Rules for General Users*.

Key Concept 20. Recognize the roles of the stakeholders of IoT systems and services

(1) Point

1) Arrange the roles of IoT device manufacturers, IoT system and service providers, and general users.

(2) Commentary

Security measures will be delayed and the influence of damage may increase if a discussion to determine who will take what measures after an incident occurs. There is a concern about an apparent lack of cooperation among stakeholders due to not clarifying their roles in advance.

It is necessary for the system and service providers to clarify the role sharing of the stakeholders and have them understand their respective roles before starting the services.

Assumed IoT incidents and risks greatly vary with each field, such as the field of automobiles, medical equipment, smart home appliances, and smart homes. It is necessary to understand the roles of stakeholders for on a field-by-field basis. For example, in the case of the field of automobiles, IoT device manufacturers are automobile manufacturers, IoT system and service providers are network operators such as TSPs and automobile manufacturers, and general users are automobile owners, drivers, etc. Likewise, in the medical field, IoT device manufacturers are medical equipment manufacturers and communications equipment manufacturers, IoT system and service providers are network operators and home medical service providers, and general users are patients and their families, doctors, nurses, care managers, etc.

Thus, many stakeholders exist and have complicated relationships in the IoT. Therefore, it is necessary to organize and understand the roles of stakeholders in advance.

(3) Examples of measures

1) Arrange the roles of IoT device manufacturers, IoT system and service providers, and general users

IoT device manufacturers and IoT system and service providers consider incident scenarios assumed on a field-by-field basis, identify risks, and organize the role of each stakeholder.

The organized roles are described and displayed on the websites of the IoT system and service providers, distributed documents (e.g., service agreements and manual), and IoT devices provided by the IoT system and service providers, notify stakeholders of the roles before the services start so that system and service users can use the systems and services after confirming the roles.

Key Concept 21. Grasp all vulnerable devices and give appropriate cautions

(1) Point

1) Construct a mechanism to grasp IoT devices on the network and identify IoT devices with vulnerability.
2) If an IoT device with vulnerability is identified, call attention to the general users using the vulnerable IoT device.

(2) Commentary

Cyberattacks often exploit vulnerability existing in IoT devices and systems. Therefore, it is effective to mitigate damage if IoT system and service providers check whether there are vulnerable ones on the network among the IoT devices installed for the systems and services they are providing. For that purpose, it is necessary to develop or use a means for grasping information on all devices, including existing IoT devices as well as newly installed IoT devices, and identify devices having vulnerability. Furthermore, if vulnerability is grasped, attention must be given to the administrator of the corresponding IoT device.

(3) Examples of measures

1) Construction of a mechanism to grasp vulnerable IoT devices and the identification of the corresponding IoT devices

Establish or use a mechanism for grasping information on IoT devices on the network, and identify IoT devices with vulnerability from the information.

Specific examples are shown below.

- Scan IoT devices installed in services and systems providing, and find if there exist any vulnerabilities. Save those investigated on the cloud.
- Grasp the installation sites of IoT devices and systems. For example, checks may be possible on whether IoT devices have been relocated illegally from the correct installation locations.

2) Calling attention if vulnerability is grasped

If the vulnerability of IoT devices is grasped, call attention to the administrators properly in accordance with the roles agreed by stakeholders in advance. The content of the attention includes matters related to the firmware updating and detachment of the IoT devices from the network.

Specific examples are shown below.

- Calling attention from T-ISAC-J

  Some commercially available broadband routers include vulnerability that makes the management screen, which is originally accessible only from the LAN side, accessible from the WAN side as well. Furthermore, while routers are connected to the Internet without changing the administrator IDs and passwords from the common settings at the time of shipment, the routers were used for cyberattacks from abroad and sustained damage such as unauthorized access and phishing.

  In response to the damage, T-ISAC-J investigated vulnerable devices via the Internet in order to check their vulnerability and threats to them. While improving the accuracy of detecting vulnerability-retaining devices and the efficiency of user identification, T-ISAC-J called general users’ attention to the threats, and finally had succeeded to reduce the number of vulnerable routers on the Internet.

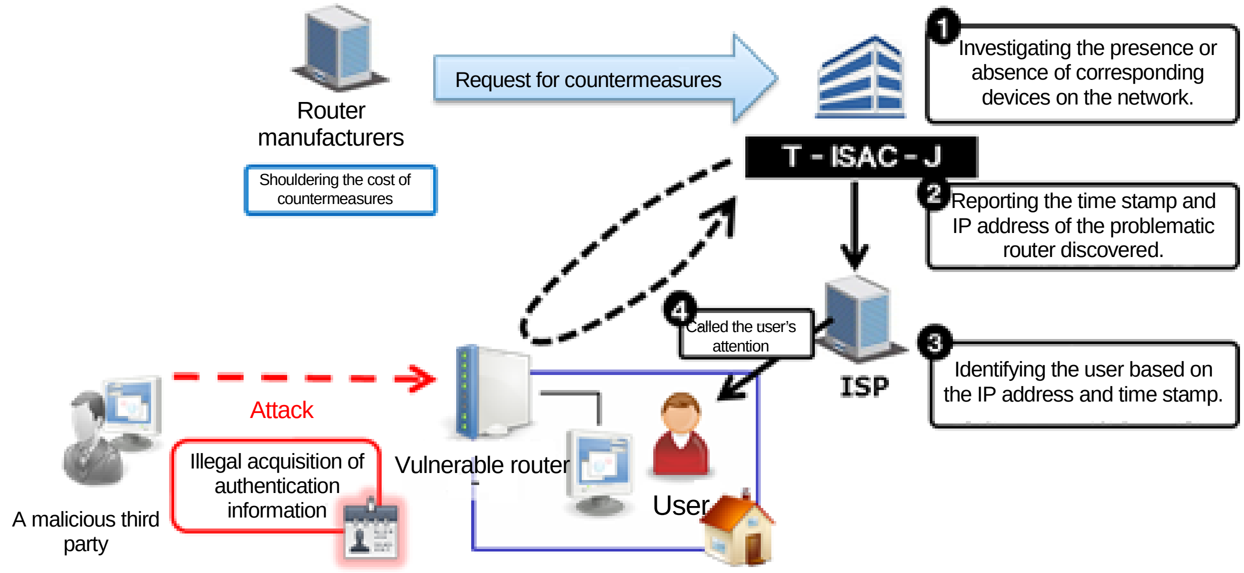

Router manufacturers
Shouldering the cost of countermeasures
Request for countermeasures
T - ISAC - J
1 Investigating the presence or absence of corresponding devices on the network.
2 Reporting the time stamp and IP address of the problematic router discovered.
3 Identifying the user based on the IP address and time stamp.
4 Called the user's attention
ISP
Attack
Illegal acquisition of authentication information
A malicious third party
Vulnerable router
User

Fig. 15 Calling Attention to Attacks Exploiting Router Vulnerability

- Calling attention from JPCERT/CC

The JPCERT/CC website calls attention to system and service providers.

Chapter 3
Recommendations to General Public

This chapter explains recommendations to general public.

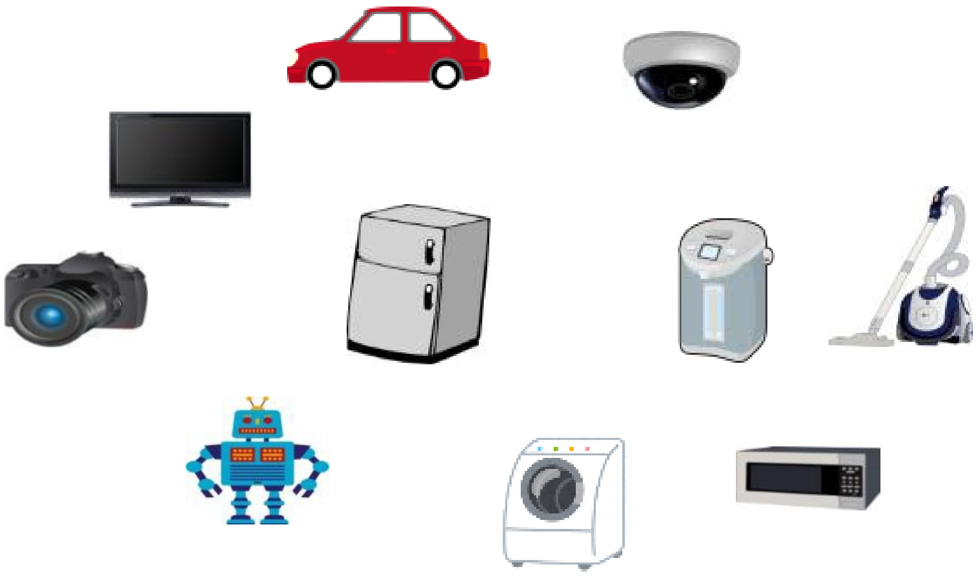
IoT (* 1) devices that are connected to the Internet have spread and increased in society, and general public is beginning to use IoT devices in their daily lives.

Unless IoT devices are handled appropriately, inconvenience will occur in the use of devices or third parties disguising themselves as the users and their families may illegitimately utilize such devices via the Internet, which will result in the leakage of privacy information on the users and their families and cause trouble to other users. Furthermore, there is a possibility that they are involved in crime.

Many of these risks can be mitigated by paying simple attention for the use of IoT devices.

The four recommendations are suggested for general public to pay attention for as IoT security. General public are suggested to keep these in mind and use IoT devices safely.

(*1): IoT stands for the “Internet of things”. Not only personal computers and smartphones but also various devices, such as vehicles and home electronics, are starting to be connected to the Internet. IoT devices mean such things that are connected to the Internet.



Recommendation 1) Refrain from Purchasing and Using Devices or Services For Which No Inquiry or Support Service Is Available

- If there are no inquiry or support service for devices and services connected to the Internet (or support services have been expired), it will be difficult to respond properly to the occurrence of something inconvenient. Furthermore, the proper updating of devices (*2) connected to the Internet will not be possible. Accordingly, it will not be possible to continue using devices or services in a safe state. In case there is anything inconvenient after purchasing or using devices or services, such as the malfunctioning of the devices, promptly contact inquiry or support service, if available.
- Do not purchase or use devices or services that do not have inquiries or support service (or support services have been expired).

(*2): The updating of devices refers to the act of changing the device state to the latest through the Internet for the purpose of improving the improper condition of the devices and preventing the unauthorized use of them.

Recommendation 2) Pay Attention to the Initial Settings

- If users' passwords for devices connected to the Internet leak to third parties, the devices may be taken over through the Internet and they may be used by unauthorized third parties who commit identity theft.
- In the case of using a device for the first time, make ID and password settings for the device. Do not leave the factory-set password for the device or share your password with others. Do not use the same password used for another device. Do not use a password that can be easily guessed by others, such as your birthday.
- Read the instruction manual of the device connected to the Internet, follow the instructions in the manual, and update the device.

Recommendation 3) Turn Off the Power if Devices are No Longer in Use

- If you leave devices that are no longer in use or have defects but are still connected to the Internet, they can be taken over and used unnoticed via the Internet by unauthorized third parties.
- Turn off the power if devices that are no longer in use or have defects.
  For example, do not leave webcams (* 3) or routers (* 4) connected to the Internet if they are no longer in use. Unplug them from the power outlets.

(*3): Webcams are cameras that can be connected to the Internet.

(*4): Routers are information communications devices that connect devices, such as personal computers and smart home appliances, to the Internet.

Recommendation 4) Delete All Data When Disposing of Devices

- User information, including information on users' families, may leak from devices unless the stored data on the devices is deleted in the case of disposing of, selling, or renting out the devices.
- Dispose devices carefully to avoid information leakage to others. Delete all information before disposing of the devices.

Chapter 4
Future Considerations

The Guidelines have been discussed and approved in the IoT Acceleration Consortium in order to clarify fundamental and universal approaches that are applicable from the viewpoint of security and to promote the use of IoT by the industry, academia, and government sectors. IoT is expected to spread into various fields, ranging from scenes in people's daily lives to the social infrastructure that supports the Japanese economy, and to be widely in use with the emergence of new IoT devices and services in the future. It is necessary to consider and address IoT security continuously.

The future considerations are listed below.

- Security measures based on risk analysis for each field

  The IoT will spread into various fields, and apparently the required security level varies field by field. For example, IoT devices used for simple information services are different from those used in factories and social infrastructure systems, in security level, purpose, and priority. It is necessary to assume specific IoT usage scenes, make a detailed risk analysis, and consider security measures according to the nature and characteristics of fields, where a large number of IoT devices are used or expected to be used. In order to make decisions on the implementation of measures, it is also necessary to examine methods for comparing and evaluating the cost of measures and the effect obtained.

- Legal responsibility

  As indicated in *1.4 Target Readers*, IoT services are often provided to the users under the cooperation of a number of stakeholders, such as device manufacturers, system providers, and service providers. For example, in the case of any troubles caused by cyberattacks, it is necessary to consider the legal responsibility such as who will respond to the cyberattacks and the financial costs. The responsibilities are dependent on types of IoT services provided in the future, and laws and regulations applicable to the field where the IoT is used.

- Appropriate data management for IoT

  Each IoT device will vary in stakeholders and places to acquire, retain, manage, use, and discard corporate technical information and personal information, including users' privacy information, according to the style of services. It is necessary to acquire, retain, manage, use, and discard important data, including personal information and technical information, properly with consideration of the characteristics of IoT systems, for which concrete methods should be considered.

- Comprehensive security measures for the IoT

  Initiatives such as those of the Information-technology Promotion Agency, Japan (IPA) to transmit and share vulnerability information on software, the National Institute of Information and

Communications Technology (NICT) to research and develop cybersecurity, including the observation of cyberattacks against the IoT, JPCERT/CC to accept and respond to reports on computer security incidents, and the Telecom ISAC Japan (ICT ISAC Japan) to share and analyze information on cyberattacks in the ICT field have been going on. In order to realize the sound development of the IoT society, a public-private partnership should be considered on alerting public users about the malware infection of IoT devices and relevant efforts in addition to the above initiatives.

The Guidelines will be revised as necessary in the future with consideration of the results of the above initiatives and efforts, social trends surrounding the IoT, changes in the vulnerability and threats of the IoT, and the security measure technology, and other significant factors.

Appendix

The abbreviations used in the Guidelines are described as follows:

Table 8 List of Abbreviations

Abbreviation	Official name
ATM	Automated Teller Machine
CCDS	Connected Consumer Device Security Council
CRYPTREC	Cryptography Research and Evaluation Committees A project to evaluate and monitor the safety of e-Government recommended ciphers and investigate and consider suitable implementation and operation methods of cryptographic technology
CSIRT	Computer Security Incident Response Team An organization to deal with incidents involving computer security
CSMS	Cyber Security Management System A cyber security management system in control system security
DAF	Dependability Assurance Framework for Safety-Sensitive Consumer Devices A development methodology to ensure the reliability of devices used by general users
DoS	Denial of Service An attack that obstructs or stop services provided
DDoS	Distributed Denial of Service An attack that interferes with or stops services to a target computer by giving heavy processing loads from multiple machines to the target computer
DRBFM	Design Review Based on Failure Mode A failure-mode-based design review
EDSA	Embedded Device Security Assurance
HEMS	Home Energy Management System
HSM	Hardware Security Module Dedicated hardware that provides security features such as key management and encryption
ID	Identifier An identifier such as a number that can be used to identify the user of a system
IEC	International Electrotechnical Commission
I/F	Interface Standards or specifications for connecting computers to other computers and peripherals (Referring to standards or specifications for connecting IoT devices and systems to other IoT devices and systems in the Guidelines)
IoT	Internet of Things A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies
IPA	Information-technology Promotion Agency, Japan
ISAC	Information Sharing and Analysis Center A center to share and analyze information related to information security.
ISMS	Information Security Management System

Abbreviation	Official name
ISO	International Organization for Standardization
ISP	Internet Service Provider
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center An organization collaborating internationally in CSIRT activities to promote responses to incidents that threaten information security in Japan
JVN	Japan Vulnerability Notes A vulnerability countermeasure information portal site aiming to provide vulnerability-related information on software used in Japan along with information on measures and contribute to information security measures
LAN	Local Area Network An information and communications networks that connect computers and other devices within a limited range, such as companies, universities, and households.
NICT	National Institute of Information and Communications Technology
OS	Operating System Basic software to control a computer and make computer resources available to application software
OSS	Open Source Software Software the set of source code of which are open to public for free, and is required to open source code to public, redistribute, depending on the license type, such as GPL, LGPL, and MPL.
POS	Point of Sales Point-of-sale information management
SoS	System of Systems A system in which different systems have complex relationships with each other
TEE	Trusted Execution Environment Application programming interface (API) specifications for an authenticated execution environment defined by the Global Platform, a standardization organization for IC card management technology
T-ISAC-J	Telecom-ISAC Japan T-ISAC-J is inherited by ICT-ISAC,
TLS	Transport Layer Security Security protocol that encrypts communication between a pair of devices.
TPM	Trusted Platform Module An LSI chip incorporating security-related processing functions mounted onto a circuit board, such as a computer motherboard
TSP	Telematics Services Provider Companies providing telematics services (wireless communications services for vehicles)
WAN	Wide Area Network A wide area network provided by communications carrier
WPA2	Wi-Fi Protected Access 2 An encryption method with improvements in the security performance of Wi-Fi Protected Access (WPA) to support AES encryption