Security Guidelines for Product Categories

- IoT GW -

Ver. 2.0

CCDS Security Guidelines WG
Home GW SWG

Revision History

Version	Date	Description
Ver.1.0	/2016/06/08	Created a new edition
Ver.1.01	2016/06/13	Maintained Partial Format
Ver.2.0	2017/05/29	・Added items to the Design, Manufacturing, Operation and Maintenance and Disposal Phases ・Made other minor changes

Contents

1 Introduction

To date, every product industry has formulated its own safety standards. Security standards relating to organizational administration (ISO27001) and product design security assessment and authentication (ISO15408) have already been formulated, while recent years have witnessed the formulation of standards targeting control systems for critical infrastructure (plants and facilities essential to social infrastructure) (IEC62443).

With the popularity of IoT, devices in widespread use are supporting a variety of networking features, increasing security concerns. That said, it is undeniable that security standards relevant to IoT products and services are not yet sufficiently in place.

In the U.S. and European nations, moves are underway to determine security standards by using industry-specific safety standards. However, while in Japan there are tangible security concerns that may lead to the establishment of security standards, there are few areas where practical discussions have yet led to action.

The Connected Consumer Device Security Council (CCDS) was established in response to this situation. The Council is committed to formulating security standards for common devices and launching an authentication program to confirm and verify compliance with these standards in order to reassure users of IoT products.

On August 5, 2015, the Information-technology Promotion Agency, Japan, Japan（IPA）launched the IoT Safety/Security Development Guidelines Review WG to initiate discussions on security at the national level. The CCDS has come together with the IPA-WG to establish a number of proposals concerning the results of the reviews of guidelines within the CCDS.

On March 24, 2017, the results of the reviews at the IPA-WG were compiled and released as “IoT Safety/Security Development Guidelines - Important Points to be understood by Software Developers toward the Smart-society 0“. While the IPA’s development guidelines focus on the common subjects by comprehensive approach, the CCDS field-specific guidelines is developed for locating individual industry specific security promotion of design or development process.

1.1 Current Status and Issues of IoT-GW Security

Internet of Things (IoT) devices continue to play an integral part in our lives.

In the healthcare and fitness field, wearable devices have been introduced to deliver advice on improving our dietary life or running forms. If, for example, sensors installed in a home are synced with a smartphone so they can be remote-controlled, the smartphone can be used to lock the home and control its lighting and power sources. IoT devices are not confined to individuals and homes but have penetrated offices and urban districts at a significant pace, and still promise further growth. According to preliminary calculations by the survey firm Gartner, the number of IoT devices will advance from 6.4 billion units in 2016 to 20.8 billion units in 2020 0.

As these IoT devices are connected to the Internet, they are ready to offer a variety of services, but they are also open to threats to information security at the same time. It is feared that these threats may endanger human lives at times.

The causes of attacks being launched on IoT devices can be considered from two perspectives: user and provider. The cause of attack resulting from users might include, for example, the use of IoT devices without their initial settings changed, use of readily presumable passwords and a lack of the concept of security. The cause of attacks resulting from providers might include, for example, a design practice of the equipment making it accessible to anybody without its initial settings unchanged, and their unpreparedness for users' lack of the concept of security.

Behind these factors is the absence of standards or schemes relevant to the assessment of security risks, which should be of major concern to the loT industry as it aims to achieve further growth. It is hard to require to all users to eliminate the cause of attacks, providers should take into consideration use situations of their products while they are being developed and designed, as well as considering how to update them after release.

This document presents the factors to be considered when developing IoT-GWs as guidelines. It analyzes possible security threats in depth and states how to remove them.

1.2 Scope of the Guidelines

This document concerns IoT-GWs that collect data from things in offices and plants, as well as customer premises, transmits it to and from networks, and summarizes key factors for consideration in their development to assure security.

1.3 Recipients of This Document

The objective of this document is to help reduce security risks as described in the preceding section. It presents the design and development processes that are to be taken into consideration starting from the product design stage and continuing even after the product release to allow relevant security countermeasures to be implemented in IoT devices.

Thus, this document addresses the following types of recipients:

1) Equipment designers and developers

2) Equipment design project development supervisors

3) Decision-makers on the budgeting and staffing of equipment design projects

1.4 Abbreviations

Abbreviations used in this document are defined in the table below.

Table 1-1 Abbreviation List

Abbreviation	Name
API	Application Program Interface
BGA	Ball Grid Array
CCDS	Connected Consumer Device Security council
CPU	Central Processing Unit
CRYPTREC	Cryptography Research and Validation Committees
CVSS	Common Vulnerability Scoring System
DNS	Domain Name System
DoS	Denial of Service
ETSI	European Telecommunications Standards Institute
FBGA	Fine pitch Ball Grid Array
FIRST	Forum of Incident Response and Security Teams
GMITS	Guidelines for the Management for IT Security

ID	Identification
IoT-GW	Internet of Things-Gateway
IP	Internet Protocol
IPA	Information-technology Promotion Agency
IT	Information Technology
JTAG	Joint Test Action Group
LAN	Local Area Network
LGA	Land Grid Array
OS	Operation System
OSS	Open Source Software
OWASP	The Open Web Application Security Project
PC	Personal Computer
PPPoE	Point-to-Point Protocol over Ethernet
ROM	Read Only Memory
SNS	Social Networking Service
SQL	Structured Query Language
WAN	Wide Area Network
XSS	Cross Site Scripting

2 IoT-GW System Configuration

2.1 IoT-GW-Based System Model

Figure 2-1 shows the general-purpose model of a system to which IoT-GW is applied. Table 2-1 explains the components of the model. In this model, the IoT-GW collects observation data in a physical space from field sensors and actuators and transfers it to the head-end system. The head-end system stores the received data and delivers it to various applications and services via an API. Depending on the use case, the applications or services may control the actuators and the like as a result of having analyzed the received data. The head-end system and IoT-GW management are installed as a server mix on the center side, as in a cloud. Component elements below the IoT-GW are installed in the field, as in customer premises or a production field. The location of installation varies from one use case to another.

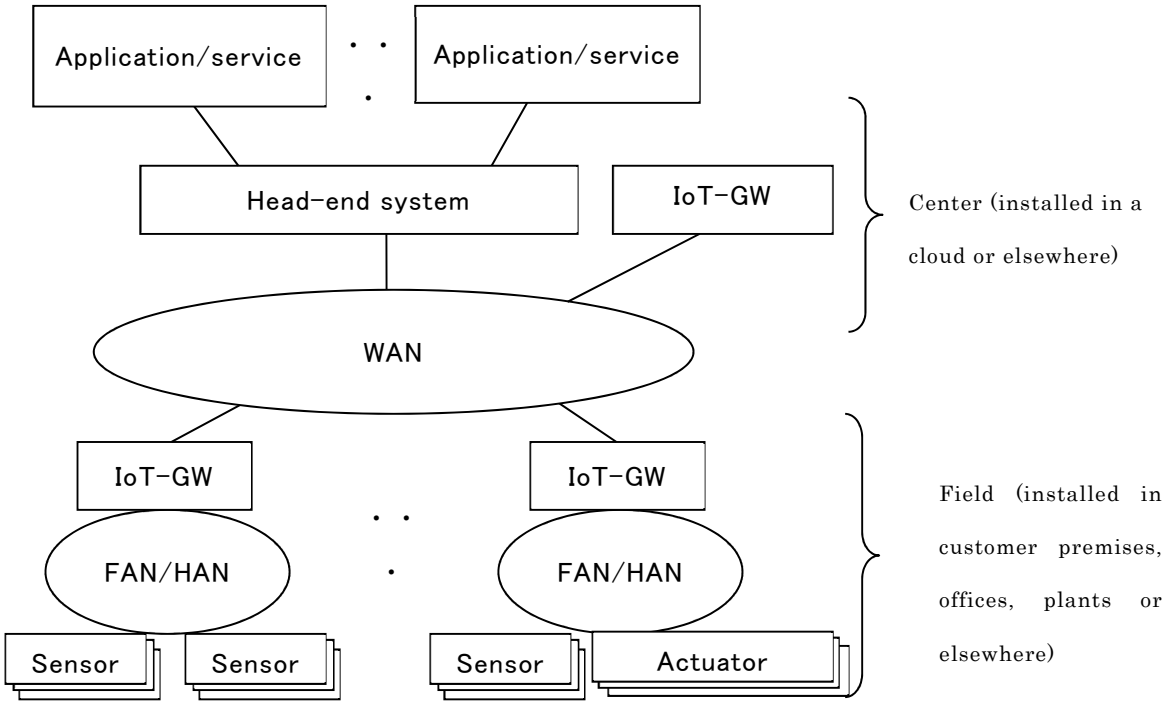

Figure 2-1 IoT-GW-Based System Model

Table 2-1 Component Elements of the System Model

Name	Explanation
Sensor	A device that digitizes objects invisible to the naked eye to collect data for use by applications/services and the like.
Actuator	A generic term covering apparatuses that are powered by electric or other energies to carry out mechanical work.
FAN/HAN	FAN: Field Area Network/HAN: Home Area Network. Networks used in general homes, corporate offices or labs, plants and elsewhere, employing various modes of access, such as wired/wireless and IP/non-IP.
IoT-GW	A device that links an IoT device and the Internet together when that device is unable to connect to the Internet for reasons, such as control.
WAN	WAN: Wide Area Network. Examples include the Internet (public network), a wide-area closed network, mobile communications network and more.
Head-end system	A mix of server devices that collect data and implement communications control.
IoT-GW management	A server device that implements IoT-GW device authentication and operation management.
Application/service	Stores the results of data gathering and analysis in a database for real-time notification, visualization and so forth.

2.2 Services and Use Cases Realized by IoT-GW

Services and use cases realized by IoT-GW-based systems can be many and varied. This section focuses on four use cases that are essential in analyzing the risks that may be presented to IoT-GW-based systems.

2.2.1 Use Case 1: Home Gateway

In this use case, the home gateway is a device complete with the functions necessary to visualize and control the status of home appliances and other equipment installed indoors and in customer premises. Figure 2-2 shows an example of the configuration of a home gateway-based system. Data, such as temperature, humidity and power consumption, is collected from sensors installed indoors or in customer premises and subjected to statistical manipulations before being made visible to the user. A service might be available in the future, for example, that uses collected data to place air conditioners and lighting

systems under optimal control from the center.

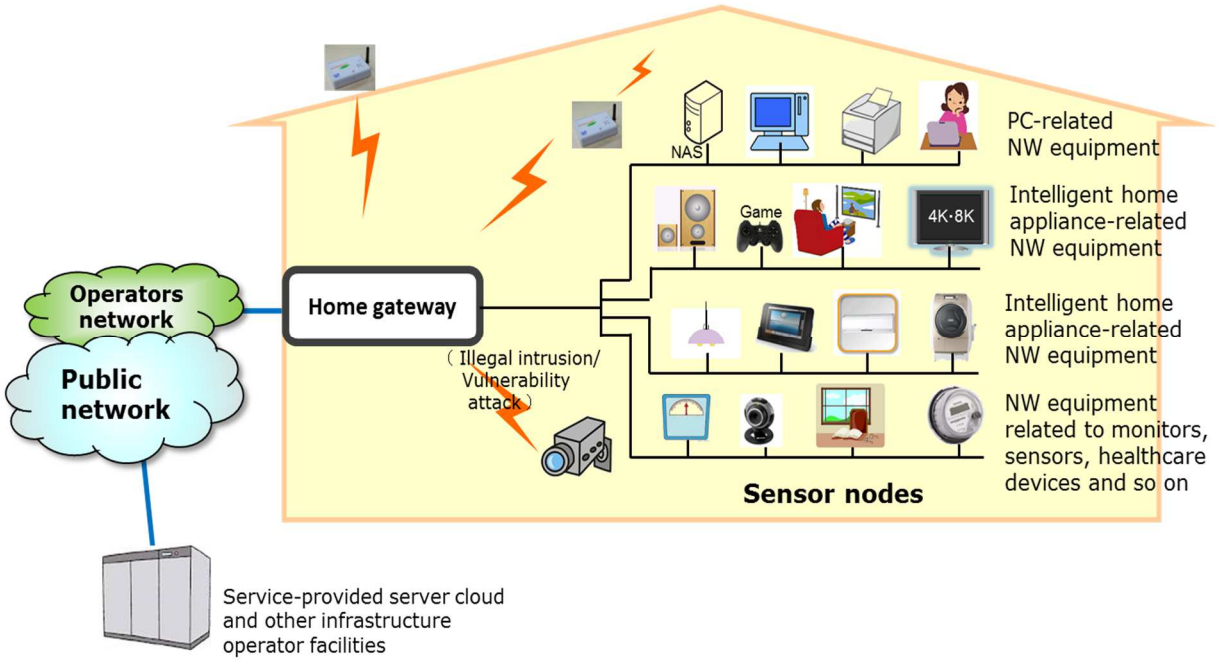

Figure 2-2 Home Gateway

2.2.2 Use Case 2: Smart Maintenance

Smart maintenance is a use case aimed at visualizing the degree of deterioration of public facilities, infrastructures and others, evaluating when to maintain them optimally and thus cutting the maintenance costs required. Figure 2-3 shows an example of the configuration of a smart maintenance system as a use case. With a gas turbine power generator plant, for example, facilities, such as turbines, compressors, boilers and pumps, are observed from sensors or machine data (signals) to collect data that helps estimate the degree of facility deterioration. Data collected is assessed to determine whether the degree of facility determination has reached a level suggested for maintenance and inspection (or when it will reach such level). Railway facility maintenance is handled in some use cases.

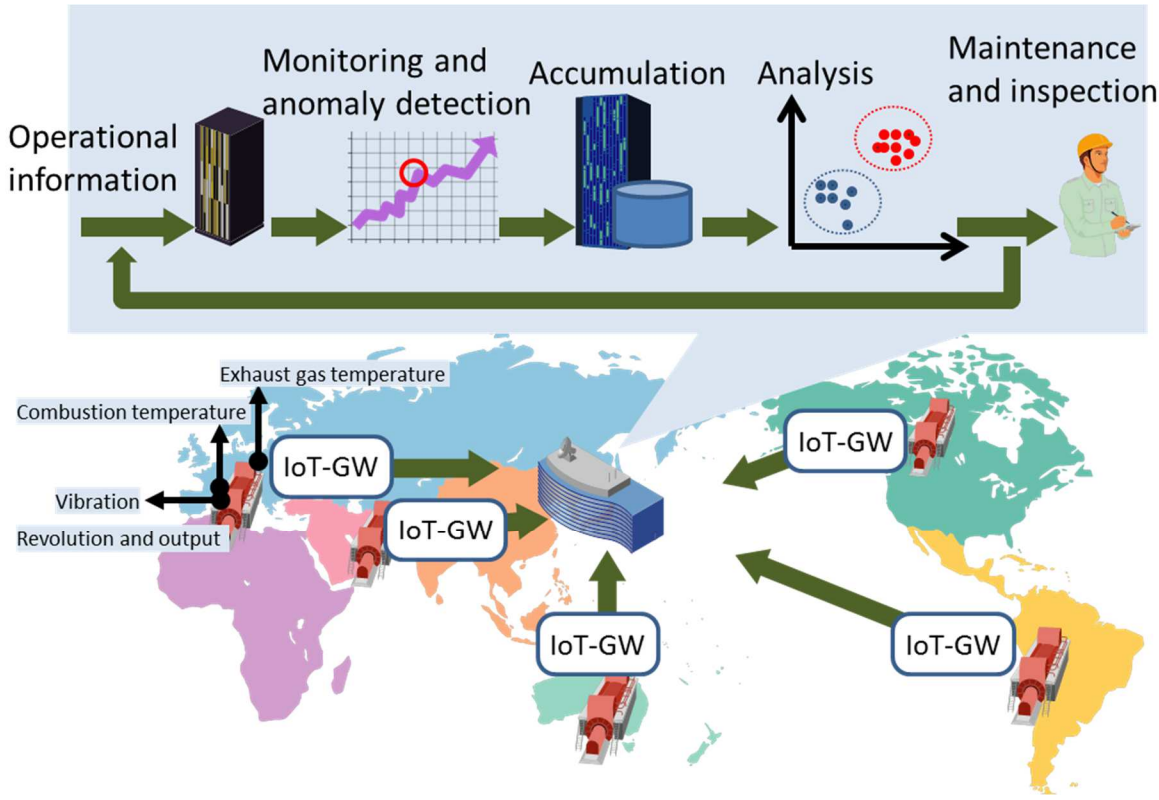

Figure 2-3 Smart Maintenance

2.2.3 Use Case 3: Supply Chain Management and Production Line Optimization

Supply chain management and production line optimization is a use case aimed at monitoring the demand-responsive optimal reordering of parts, restructuring of production lines, in-plant delivery of intermediate materials and the status of physical distribution. Figure 2-4 shows an example of the configuration of a supply chain management and production line optimization system. Part and intermediate goods inventory information, customer and market demand information, supplier capacity information and the current production status at each supplier are collected as data. Data thus collected is analyzed to devise production line change plans, in-plant inventor and shipment plans and so forth to suit ordered materials, their vendors, order quantities and demand so that the near-future supply chain will be optimized as a whole. In-plant distribution (as by belt conveyors and forklifts), program delivery to production lines and more may be remote-controlled in the future.

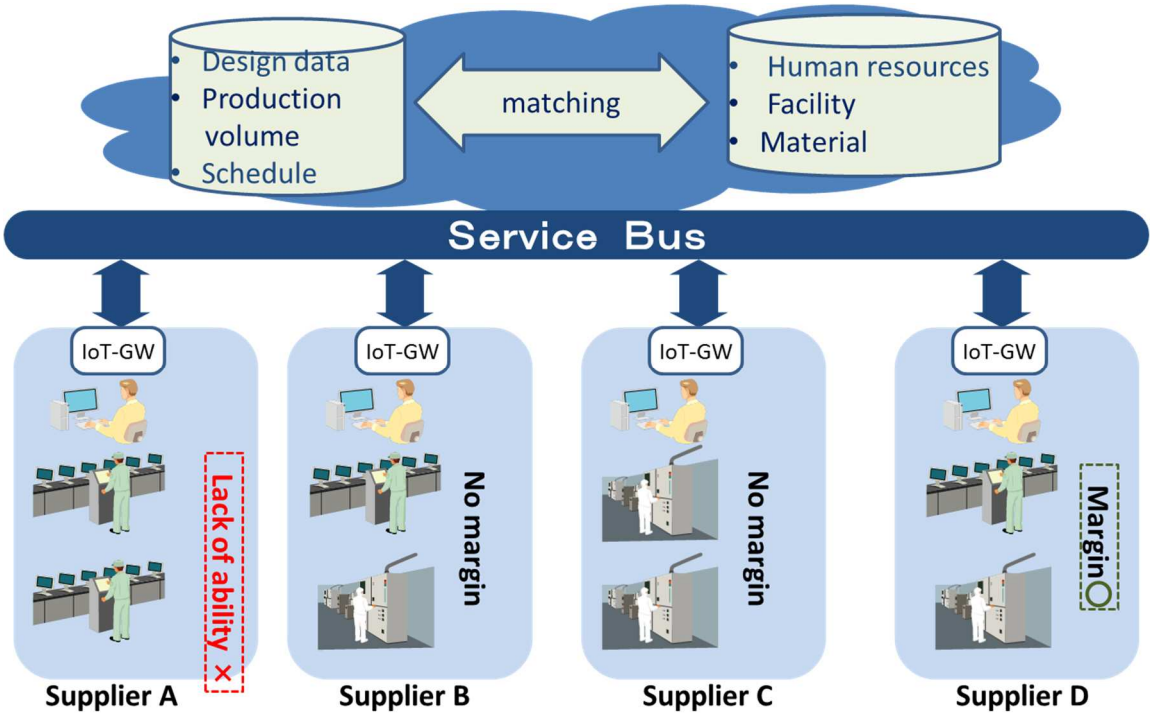

Figure 2-4 Supply Chain Management and Production Line Optimization

2.2.4 Use Case 4: Video Monitoring

Video monitoring is a use case in which video data originating from field cameras or other devices is analyzed automatically to secure safety in urban areas, at stations and in other facilities. Figure 2-5 shows an example of the configuration of a video monitoring system. It detects camera video data and passage detection sensor data that trigger the start of video recording and tags it for purposes, such as detecting suspicious individuals, recording their evidence and searching for them. Remote camera orientation control and on/off control is also possible.

In the video monitoring use case, cameras may be directly connected to a WAN or LAN in some patterns. For now, however, IoT-GW is introduced to allow the installation of cameras on a more extensive scale.

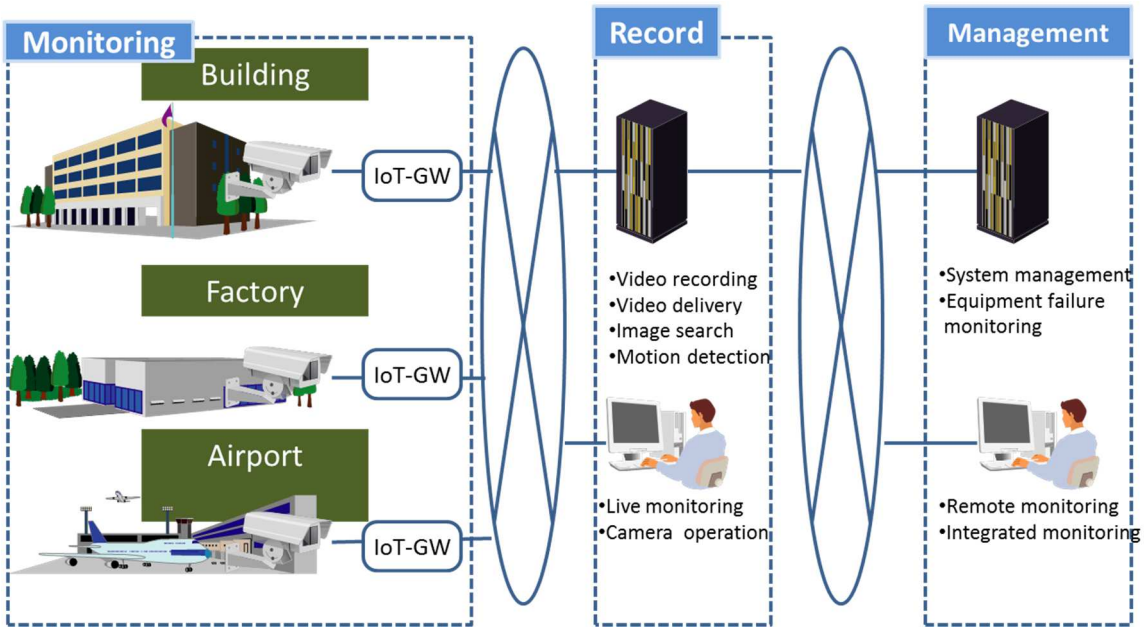

Figure 2-5 Video Monitoring

2.3 Assets to be Protected and Impacts to be Considered

In Figure 2-1 IoT-GW-Based System Model“, a system model based on IoT-GW is presented. This system model is divided into four broad parts as listed below. In IoT, the operations of these parts may be managed by a single organization or by separate organizations. Characteristically, they combine as a whole to make up a larger system.

- End point (IoT-GW, FAN/HAN, sensor, actuator)
- Network (WAN)
- Server (head-end system, IoT-GW management)
- Service (application/service)

Like a general information system, these individual parts contain assets that execute services and processes and assets to be protected, such as confidential and personal information. In IoT, on the other hand, data collected at end points moves through these elements. IoT requires such moving data to be handled as assets to be protected across the eco-system.

In the target system model, actuators that physically impact the real world exist. If such actuators should run out of control, they could endanger human lives. Hence, the assessment of any threat should be taken into consideration regarding impacts upon the system itself, plus impacts upon surrounding entities, such as other companies or organizations, human lives or communities. Table 2-2 gives examples of the asset to be protected, and possible damages and impacts in the individual use cases.

Table 2-2 Assets to be Protected, and Possible Damages and Impacts in Individual Use Cases

Use case	Asset to be protected	Possible damage and impact
Home Gateway	・Personal information ・Financial asset data ・Configuration information ・Log information ・Network	・Springboard for launching attacks by takeover ・Loss of financial assets ・Spoofing ・Disruption of communication
Smart Maintenance	・Sensor information ・Productive facilities	・Destruction or shutdown of power generation plants

	・Infrastructures ・Human lives ・Network	・Destruction or shutdown of productive facilities on power failure, shutdown of infrastructures ・Serious damages risking human lives on power failure ・Disruption of information
Supply chain management and production line optimization	・Sensor information ・Control system information ・Productive facilities ・Infrastructures ・Human lives ・In-plant environment ・Network	・Data acquisition disabled, resulting in a degraded functionality or accuracy. ・Facility shutdown, overproduction/underproduction, nonconformity occurrence ・Destruction or shutdown of productive facilities, shutdown of infrastructures, production robots out of control or any other chances of risking human lives ・Disruption of information
Video Monitoring	・Video data ・Sensor information ・Camera control information ・Personal information ・Network	・Injection of false data (such as an overestimated passenger count) into data collected from a surveillance camera, with the result of secondary users (e.g., users using a navigation service or marketing information) providing services based on such false data. ・Breach of privacy by seizing cameras or the like ・Disruption of information

3 Possible Security Threats

Figure 3-1 is a schematic view of the relationship between IT security and IoT security. IT security is the security of an existing typical information system. IT security and IoT security overlap in many areas of security action. As described in 2.1, however, a target IoT system has different types of devices connected to it to differentiate itself from any other information system to date. Accordingly, this chapter focuses on new areas of consideration required for IoT security and explains about the possible security threats to systems with IoT-GW implementations.

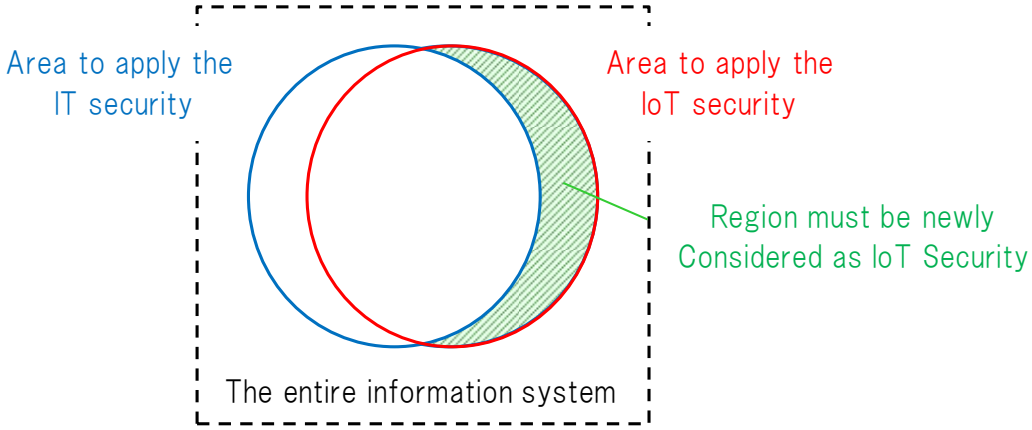

Figure 3-1 Relationship between IT Security and IoT Security

3.1 Cases of Attacks Launched on Network-Ready Devices

While the number of attacks targeting network-ready devices continues to grow from year to year, this section introduces those cases of attacks that have been related to IoT-GW from a past record of threat cases.

(1) Referencing false DNS servers after illegal changes made to router settings [3]

Cases of attacks exploiting IoT-GW vulnerabilities were presented at the 2012 FIRST Symposium, Sao Paulo, held in Brazil in March 2012. These attacks reportedly exploited vulnerabilities in the IoT-GW in common use in Brazil to change administrator passwords and to reference the DNS server offered by the attackers. Attackers' DNS would return a false response, leading the users to a fake site where they might be prompted to install malware to disable their security software and thus have their confidential information stolen.

(2) Cases of abuse of broadband router vulnerabilities

On May 16, 2012, information was publicized stating the presence of security vulnerabilities in part of a wireless LAN broadband router. If such a wireless LAN broadband router was used, the PPPoE authentication ID and password set by the user would be saved in plaintext open to acquisition from outside. A firmware fix to this vulnerability was released on May 24, 2012, but damages have since followed, including list-type access attacks launched on the list membership service site on a spoofing collection that used an Internet connection ID and password stolen from a broadband router having such vulnerabilities. Monetary damage is known to have occurred as a consequence of changes to the events that had been used as infrastructures thus attacked or to the source users' contractual information.

(3) Case of pacemaker hacking [4]

Barnaby Jack made a presentation on pacemaker hacking at the Breakpoint 2012 Security Conference in October 2012 by running a video to demonstrate how hacking was done. The video showed how an 830-volt current could be induced in a pacemaker placed within 15 meters by using a note PC after a wireless transmitter was reverse-engineered to uncover vulnerabilities in the pacemaker. Such vulnerabilities allowed device control information to be exploited by way of a special command. The presentation also suggested that a large number of pacemakers could be hacked simultaneously if illegal firmware could be uploaded into the devices used for wireless communication with these pacemakers.

In addition to the events described above, numerous events have taken place. Because many of the attacks that have targeted IoT devices are similar to those launched on servers and PCs, more IoT devices are predicted to be predisposed to damages similar to servers and PCs. Regarding threats to servers, PCs and the like, a document entitled "10 Major Threats to Information Security" [5] has been published by the IPA, listing the ranks of security threats having a major social impact. Table 3-1 lists 10 major threats to information security for the last three years. Attention should also be paid to these threats on IoT devices.

Threats to IoT devices have been introduced in a project called "The Open Web Application Security Project (OWASP) [6]." This project works on web application security risks only, offering web application diagnostic tools and the like. It releases information on

visualizing security climates and responding to risks to enable anybody to make decisions on relevant information. Table 3-2 lists 10 major security risks [7] that have been publicized by OWASP.

Table 3-1 10 Major Threats to Information Security, 2014, 2015 and 2016

Order	2014	2015	2016
1st	Espionage or intelligence aimed at organizations via targeted email	Abuse of Internet banking or credit card information	Abuse of Internet banking or credit card information
2nd	Illegal login・Abuse	Information leakage caused by internal fraudulence	Information outflow caused by targeted attacks
3rd	Website falsification	Intelligence conducted by launching targeted attacks	Fraudulence or exploitation using ransomware
4th	Leakage of user information from a Web service	Unauthorized login to Web services	Theft of personal information from a Web service
5th	Illegal remittance from online banking	Theft of customer information from a Web service	Unauthorized login to Web services
6th	Malicious smartphone applications	Cyberterrorism launched by hacker groups	Website falsification
7th	Thoughtless disclosure of information to SNS	Website falsification	A smartphone application bypassing a review to penetrate the official market
8th	Information leakage caused by losses or inadequate settings	Attacks making base use of Internet basic technologies	Information leakage caused by internal fraudulence
9th	Fraud or extortion using viruses	Attacks prompted by the release of vulnerability information.	Increasingly sophisticated and malicious one-click fraud
10th	Service interference	Malicious smartphone application	Increased exploitation of vulnerabilities following the release of countermeasure information

Table 3-2 10 Major Security Risks to IoT Publicized by OWASP

No.	English title	Japanese title
1	Insecure Web Interface	セキュリティが確保されていない Web インタフェース
2	Insufficient Authentication/Authorization	不十分な認証
3	Insecure Network Services	セキュリティが確保されていないネットワークサービス
4	Lack of Transport Encryption	暗号化されていない通信路
5	Privacy Concerns	プライバシーに関する懸念
6	Insecure Cloud Interface	セキュリティが確保されていないクラウドインタフェース
7	Insecure Mobile Interface	セキュリティが確保されていないモバイルインタフェース
8	Insufficient Security Configurability	不十分なセキュリティ設定
9	Insecure Software/Firmware	セキュリティが確保されていないソフトウェア/ファームウェア
10	Poor Physical Security	物理的セキュリティの脆弱さ

3.2 Characteristics and Issues of IoT-GW-based Systems

Based on the use cases explained in 2.2 and threat cases examined in 3.1, the characteristics and issues of an IoT-GW-based system have been extracted. The following is a discussion of its issues:

(1) No governance in the field, hence threats to devices and terminals are significant

Devices and terminals may be installed outside the scope of the owners or users' physical management, or in places readily and physically accessible to attackers.

(2) Difficulty taking costly security countermeasures because of low-cost field equipment and terminals

Because of only low costs justified for equipment and terminals installed in the field, it is sometimes impractical to implement security measures, such as full strength encryption and firewalls.

(3) Actuators are connected in the field

Because not only sensors used for measurement but also the controlled objects, such as actuators and control system controllers, are networked, attacks that exploit device vulnerabilities or unauthorized access attempts, if launched, could result in serious impacts and damages (risking human lives and causing social chaos).

(4) Difficulty updating systems intended for extended periods of service

Because social infrastructures and industrial systems are often used for longer than 10 years, it may happen that one has to continue using software past its support period or experiences difficulty updating a system once it is put into service. If vulnerabilities are found in such a system, they could be left uncorrected.

(5) Increased dependence on specific data after inter-organizational overall optimization

One of the objectives of IoT implementation is overall optimization using big data. IoT implementation might hence drive interorganizational data sharing between organizations and usage to such an extent that the infrastructures and system maintained by each organization would have increased dependence on specific data, making the infrastructures and systems more vulnerable to targeted attacks or to decoding by malicious programs.

3.3 Possible Security Threats to IoT-GW-based Systems

Ten security threat and risk items have been extracted from the preceding discussions of characteristics and issues of an IoT-GW-based system as follows:

(1) Data collection made impossible by sensor shutdowns. [Threat No. 1]

Sensors might be shut down as a consequence of their theft, failures, power discontinuity, DoS attacks launched on them, natural disasters and so forth, making it impossible to collect data and resulting in degraded accuracy or quality. In the smart maintenance use case, for example, the unavailability of certain data, such as temperature and revolutions, could detract from maintenance and inspection quality.

(2) Invalid data being delivered from illegally modeled sensors. [Threat No. 2]

If field sensors are physically remodeled illegally by insiders or third parties with malicious intent or fake sensors are installed, they could deliver invalid data or falsify data to impact applications/services. Possible impacts in a use case of supply chain management and production line optimization might include, for example, facility shutdowns, overproduction/underproduction and product rejection.

(3) Sensors seized to play a role in launching DoS attacks. [Threat No. 3]

If sensors are seized, DoS attacks, such as requests and bandwidth occupancy, might be imparted to other devices as well. In a use case of video monitoring, for example, data gathering from other devices might be disabled. Sensors have a low capacity and do not generate large traffic by themselves, but can be a source of threat depending on how many of them are installed.

(4) Destruction or shutdown of productive facilities, shutdown of infrastructures or induction of any operation risking human lives. [Threat No. 4]

The takeover of actuators or controlled controllers could result in the destruction or shutdown of plant productive facilities, shutdown of infrastructures, such as power plants and water and sewerage, or operations that might risk human lives, such as vehicles or robots running out of control. In a use case of supply chain management and production line optimization, for example, a controller might be seized from an

external world to drive a robot arm out of control, impacting workers at work there.

(5) Attacks launched on end-point devices from a network. [Threat No. 5]

As devices become newly connected to a network when they have not previously been expected to do so, they would be exposed to greater chances of being attacked, such as by illegal access, takeovers and DoS attacks. DoS attacks, once launched on such devices, would deliver damages because they have low throughput or a narrow network bandwidth. In a use case of smart maintenance, for example, attacks launched on tunnel walls or on mountain rainfall sensors might impede train services.

(6) Intruding into a FAN/HAN physically to launch attacks. [Threat No. 6]

Unauthorized equipment physically connected to a FAN/HAN installed in a plant or customer premises in the field might compromise security. In a home gateway use case, for example, using a tampered used home appliance or gateway could make it possible to launch attacks on a network or steal personal information.

(7) Throughput and power consumption increased by data transmitted from sensors to a server [Threat No. 7]

If data is transmitted at the same timing from a large number of sensors, server throughput and power consumption could surge, leading to a server shutdown, even though the data is normal by itself. In a use case of video monitoring, for example, if video data is transmitted from a large number of cameras simultaneously, the server would be unable to process the data in time, resulting in a failure to operate as intended by the developers or system designers.

(8) Data theft resulting from end-point devices with an insufficient encryption strength. [Threat No. 8]

If advanced encryption is not implemented under the constraints of the throughput and power consumption of end-point devices, such as sensors, threats, such as communications interception, would not be prevented. In a use case of supply chain management and production line optimization, for example, information assets, such as open data, may not be confidential by nature but still could have an increased impact on productive activity.

(9) False data injected or propagated. [Threat No. 9]

If false data is injected or data is deleted or modified in part, invalid data might be left on a database and generated into false statistical data for transmission to society. In a use case of supply chain management and production line optimization, for example, if data collected from sensors is injected with data falsified by spoofing or the like (for example, overestimated production data), then the supply chain, the secondary user of the data, could decide on its manufacturing process based on the false information. Information assets of a highly public nature, such as open data, do not have confidentiality but could exert a major impact on society.

(10) Being attacked by exploiting vulnerabilities in a system difficult to renew. [Threat No. 10]

Also, if a system, such as a social infrastructure or production line, is attacked by exploiting its vulnerabilities, the system operation or service must still be continued. Placing uninterrupted availability on top of anything, however, could delay the implementation of vulnerability countermeasures, with the threat that attacks could be launched by exploiting such vulnerabilities. In a use case of supply chain management and production line optimization, for example, attacks or vulnerabilities could be left unattended without being able to shut down the production line.

While 10 security threats have been listed above, threats and issues continue to grow in pace with technological advances, commanding a periodical review.

4 Security Efforts Made in the Development Phase

4.1 Definitions of Phases of a Lifecycle

The workflow of product development activity can be divided into five broad phases: product planning, design and manufacturing, assessment, operation and maintenance and disposal. Sufficient countermeasures should be implemented in these successive phases to ensure product security quality.

Figure 4-1 Phases of a Product Lifecycle

Table 4-1 Definitions of Phases

Phase	Explanation
Product planning	Formulates product concepts, budgets and requirements.
Design and manufacturing	Carries out design, implementation and manufacturing pursuant to the requirements defined in the product planning phase.
Assessment	Assesses the authenticity of the manufactured product.
Operation and maintenance	Sells the product to its owner (user). Responds to incidents occurring while the user uses the product, maintains and services the product and so forth.
Disposal	The owner of the product implements a disposal procedure.

4.2 Security Efforts Made in the Individual Phases

This section explains about the implementation of security efforts in the individual phases of a lifecycle as outlined in the foregoing section.

4.2.1 Product Planning Phase

Assuring product security quality requires implementing a security design from a higher level. This section describes how to assure security quality in the product planning phase.

Table 4-2 Security Efforts Made in the Product Planning Phase

No.	Item	Description
1	Identify the assets to be protected and threats and analyze risks	In developing a product that is planned to meet market needs and customer requirements, identify what assets are to be protected and the threats with its product profile, assumed usage environment, assumptions, protected data, mapping between protected data and the human environment, possible threats and known issues with similar products taken into consideration. For specific analysis examples, see Chapter 5. Define what threats are involved in the data that is handled by the equipment, or define “any threats other than the data handled,“ such as a product being exploited as a springboard for launching attacks on others, and then take countermeasures against such threats in the design and operation stages. Conduct risk analyses in the method of risk analysis and assessment described in Chapter 5, with the identified protected assets and threats taken into consideration and then take countermeasures against such threats in the design and operation stages.
2	Extract security requirements	As in “Identify assets to be protected and threats and analyze risks“ above, extract security requirements for the product with the product profile, assumed usage environment and the like taken into consideration and then proceed with implementation in the succeeding phase of design and manufacturing. Typical security requirements are listed below. Because these requirements may be too many or too few for a particular product under development, developers should fully review and extract relevant security requirements. ・Prevention of outflow of confidential information ・Fault recovery ・Countermeasures against springboard attacks ・Alert function (in times of attacks launched, illegal intrusion or the like) ・Logging function ・Service function ・Countermeasures against direct attacks launched on hardware ・Countermeasures against side-channel attacks ・Confidential information scrapping function

3	Response as a corporate organization	Each corporate organization must establish information security policies and define information security rules pursuant to these policies, then take information security measures. Examples of information security rules ・Organization and position of management regulations ・Management framework and responsibilities ・Practice of education and inspections

4.2.2 Design and Manufacturing Phase

Based on the risk analyses and the results of security requirements extraction in 4.2.1 implement countermeasures in the design and manufacturing phase.

Table 4-3 Security Efforts Made in the Design and Manufacturing Phase

No.	Item	Description
1	Selection of a development platform	(1) Verify known vulnerabilities ・Verify that the OS, boot program and application programs to be integrated into the product under development and their versions are free of known security vulnerability issues. ・Verify that the CPU to be used in the product under development is free of security vulnerability issues. (2) Confirm technological trends concerning cryptographic technologies used for authentication or information protection. ・In Japan, reports are available from CRYPTREC as a reference in developing built-in systems that use cryptography to carry out authentication and safeguard information. ・Because different countries overseas have their own arrangements, it is necessary to reference their encryption standards.
2	Implementation of security functions	Implement functions to comply with the security requirements in the equipment according to their definitions. Examples of measures to comply with the security requirements listed in No. 2, Table 4-2 are given below. (1) Prevention of outflow of confidential information

		・Use a cryptographic algorithm to suit the degree of confidentiality ・Use of encrypted memories or the like ・Access control implementation ・Disable unnecessary services ・Disable automatic execution of removable media ・Set passwords that are difficult for others to guess ・Prevent password entry retries ・Assign relevant account privileges ・Protect password information ・Disable file sharing ・Access permission setting on files ・Log acquisition ・Illegal access monitoring ・NAT function implementation ・Firewall function implementation (2) Fault recovery ・Fault detection and notification ・Log acquisition ・Duplexing of configuration information (3) Countermeasures against springboard attacks ・Detection of too much packet data received during a given period of time ・Detection of too many instances of incorrect password entry for a given period of time ・Port scan detection ・Detection of reception of overly large data ・Suppression of illegal operations ・Implementation of a specification that does not transmit a reply in response to a ping or that sets a rate limit if a reply is transmitted ・Sandboxing　intra-equipment data to prevent vulnerabilities from being propagated (4) Alert function (in times of attacks launched, illegal intrusion or the like)

		・Notifies users of attacks launched, as by lamp indications. ・Displays warnings on actions that could lead to vulnerabilities, such as opening of a port by a user. ・Displays possible risks and threats that may be caused by user's usage in the manual. (5) Logging function ・Recording of the time of illegal access occurring to the equipment, source IP address, port number, protocol type and so forth ・Device users' decision-making on whether to install an authentication log recording function or not. User ID, login count, login error count, time and more. ・Review the size of memory required in the equipment to retain logs described above. (6) Maintenance functions ・Differentiation of maintenance screens between maintenance experts and general users ・Authentication to differentiate privileges between maintenance experts and general users ・Removal of any irrelevant functions, such as debugging ・Function for remote program updating to compensate for vulnerabilities ・Appearance of product management screens to prompt users to update programs or of lamp indications to articulate whether the latest program updates are available or not. ・Initialization (factory reset) function ・Implementation of a complete erasure function allowing for characteristics of the target storage media (for flash ROM, wear leveling) to ensure positive data initialization. *For more information about data sanitization, refer to NIST SP 800-88 Guidelines for Media Sanitization 0 and others.
3	Protocol risk review	Some of the protocols generally used for IoT-GW have either their specifications standardized of publicized and are open to possible exploitation from attackers because of such standardization. It is necessary to identify which protocols to use in the design stage, and vulnerabilities and impacts relating to the protocols and implement countermeasures during design and manufacturing. Appendix 1 gives a typical

		listing of the protocols used, their vulnerabilities and impacts. Enumerating protocols and their vulnerabilities and possible impacts in this way would help better define countermeasures necessary to cope with known vulnerabilities and enhance their comprehensiveness.
4	Software implementation	(1) Secure programming Secure programming enables the writing up of a robust program that resists attacks from attackers, malware and other sources. This refers to a program that is capable of functioning as intended even when it has received unintended data. To prevent security vulnerability issues from being built into product development activity, it is necessary to implement secure programming. The IPA Secure Programming Course published by the IPA discusses specific secure programming methods. It is available for download from the IPA Website for implementation in actual programming practice. (2) Use of security features implemented in the OS The OS itself comes with its own repertoire of security-conscious features, including Address Space Layout Randomization (ASLR), which randomizes the address space each time a program is loaded to lower the threat level. Whether these features can be used or not should be discussed in a proactive manner.
5	Hardware implementation	(1) Countermeasures against physical attacks launched on hardware Countermeasures against physical attacks launched on hardware may include the following: ・Data analyses by probing can be made difficult by avoiding the use of component assignments, layer structures and connections that have been copied from a reference in their entirety, and use components that require a mounting method that is difficult to probe, such as BGA, FBGA and LGA. Moreover, run vital signal lines not by surface layer wiring but by inner layer wiring. ・While debug and diagnostic ports adhering to certain standards, such as JTAG are often installed on a product during its development, care should be taken to keep the debug ports from being disclosed when the product is released. ・Remove the description of the CPU to be mounted to prevent information about its address map and registers from being

		readily collected from the data sheet. (If there is no knowing what kind of part is used, modification of the register settings and the like is not permitted.) ・Provide holes in the equipment so that wire locks can be attached to them to stop the equipment from being carried away. ・Use tamper-proof screws. ・Use security labels to prevent cabinets from being opened. ・Provide a cabinet opening detection function (which clears the memory of its contents upon detection of the cabinet opening). ・Structures must not be easily openable. ・Shield with metallic seals. (2) Countermeasures against side-channel attacks Countermeasures against side-channel attacks might include: ・Hide or shield side-channel information (power consumption or electromagnetic leakage). These are typical measures in terms of hardware implementation and additional measures may be required depending on the specific product under development.
6	Efforts made by development outsourcing contractors	Specify purchaser design rules and standards to contractors for them to comply with [11],[12]. (1) Development of standards relating to outsourcing Develop standards and procedures relating to outsourcing as follows: ・ Standard for establishing an acceptable scope of outsourcing and the range of information assets to which contractor access is granted. ・Contractor selection procedures and criteria, and standard relating to contractor requirements ・ Procedures for responding to breaches of information security in an outsourced operation ・Standard for assessing the status of implementation of information security measures by contractors (2) Selection of contractors Select contractors based on the predefined contractor selection procedures and criteria, and a standard relating to contractor

		requirements. Notify contractor candidates of the following beforehand: ・Description of the information security measures to be implemented by contractors undertaking to fulfill a given outsourced operation. ・Procedures for responding to breaches of information security in an outsourced operation. ・Procedures for verifying the status of implementation of information security measures by contractors and for remedying information security measures found inadequate. (3) Contracts concluded with contractors Contracts concluded with contractors must generally cover the following: ・Scope of the information that is subject to outsourcing and the information system ・Arrangements for handling and management of confidential information ・Action to be taken in times of breaches of confidentiality or contractual obligations ・Arrangements for re-outsourcing, and return and disposal of information upon termination of the contracts ・Procedures for responding to information security accidents and incidents ・Procedures for correcting inadequate fulfillment of information security measures ・Identification of workers involved in the practice of outsourcing operations and prohibition of involvement of any other individuals ・Acceptance of an information security audit ・Arrangements concerning the level of service provided (4) Supervision of contractors After outsourcing, supervisor contractors as appropriate, with primary regard to the following points: ・Description of the specific efforts to be made by representatives of the outsourced operations to achieve a required level of security ・Verify that the outsourced operations are carried out only by

		workers agreed upon by both parties. ・Verify the status of information security measures by conducting an information security audit. (5) Others Other possible efforts are as follows: ・Make only a limited range of information available to contractors. In making information available to providers, use a secure method of delivery, such as masking or irrelevant parts of the information or encrypting the information, and also keep a record of the delivery of information. ・In renewing any outsourcing contract, review the validity of the renewal based on the predefined selection procedures, selection criteria and contractor requirements. ・Upon termination of the contract, verify that the information and the information system that have been provided on outsourcing are returned or destroyed upon termination of the contract.

4.2.3 Assessment Phase

In the Assessment Phase, verify whether the security measures discussed in 4.2.2 are in place and also whether the equipment is free of vulnerabilities.

Table 4-4 Security Efforts Made in the Assessment Phase

No.	Item	Description
1	Verification of vulnerabilities	(1) Verification of vulnerabilities Vulnerabilities could be fabricated potentially as a result of inadequate specifications, failure to implement secure programming and so forth. The laborious manual work of vulnerability verification can be eased by using a vulnerability verification tool to check for vulnerabilities in a comprehensive and efficient manner. Table 4-5 lists some of the tools that are available as OSS. Use of all these tools might ensure the comprehensiveness of vulnerability verification. Because all these tools are OSS and the OSS development community is ready to respond to any new vulnerabilities that may be found in them, developers should benefit from installing them. CCDS also expects to develop OSS-based tools as listed in Table 4-5 and release

		them. From the viewpoint of preventing access to downstream equipment on the IoT-GW, the network and servers used to search for open ports or working services should be checked for vulnerabilities on a priority basis by using tools (for example, OpenVAS). (2) Timing of vulnerability verification While vulnerability verification work is to be conducted during development or in the assessment stage prior to product shipment, it should be carried out periodically even after the start of operation as vulnerabilities grow in volume from day to day. (3) Vulnerability verification items Appendix 1 lists the protocols that are commonly used with the IoT-GW and typical examples of their vulnerabilities. These vulnerabilities should be verified by using tools. (4) Considerations for vulnerability verification ・Verify that tools are functioning correctly. ・Check the reports or other data generated by tools to verify the presence or absence of vulnerabilities. Reports may cover both conditions that are suspected vulnerabilities and those that could manifest depending on how the system is used. Verify their descriptions to determine whether specific conditions are vulnerabilities or not.

Table 4-5 List of Vulnerability Verification Tools

No.	Kind	Tool name	Objective
1	Fuzzing tool	Sulley	Check target software for the presence or absence of vulnerabilities. Raise an exception intentionally by feeding unpredictable input data and verify the behavior of that exception to check for vulnerabilities.
2	Network vulnerability test	OpenVAS	Verify the versions, settings, configurations and other aspects of the software installed on the IoT-GW and check them for the presence or absence of vulnerabilities.
3	Web application vulnerability	OWASPZAP	Check the Web server/applications for the presence or absence of vulnerabilities. Send a request to the Web server facilities

	test		installed in the equipment under test to check for vulnerabilities in response to XSS, SQL/command injections and so forth.
4	Packet generation	Ostinato	Create illegal packet data and transmit it to IoT-GW to verify its behavior on the receipt of illegal packets. Transmit a large number of IP packets to verify behavior under a high load, to provide against possible DoS attacks and the like.
5	Web request generation	Gatling	Verify behavior under a high load condition to provide against possible DoS attacks and the like. Load a Web application of interest under a specified set of conditions (number of requests/second, user behavior, such as screen input and screen transitions).

4.2.4 Operation and Maintenance Phase

To assure the security quality of a product, take measures in the product itself and maintain the security quality after its release. This section describes how to assure security quality in the operation and maintenance phase.

Table 4-6 Security Efforts Made in the Operation and Maintenance Phase

No.	Item	Description
1	Responses to latest vulnerabilities	(1) Responses to latest vulnerabilities Check the OS, boot program and applications used for vulnerabilities by keeping a constant eye on the following types of vulnerability information and updating the programs if any vulnerabilities of concern are found: ・Common Vulnerabilities and Exposures (CVE) ・National Vulnerability Database (NVD) ・Japan Vulnerability Notes (JVN) ・JVN iPedia ・Open Source Vulnerability Database (OSVDB)

2	Response as a corporate organization	・If vulnerabilities are found, notify users by way of own website, email and so forth and alert them to the vulnerabilities. ・Open a point of contact on which to receive vulnerability information from users or the agencies listed above and build a framework for relating such information to developers as soon as possible. ・Decide beforehand who will handle vulnerabilities and how once they are detected and the information is conveyed to the developer. ・Formulate the flow of responding to vulnerabilities, such as scoring their impacts, verifying their repercussions and creating program fixes. ・Installation of a mechanism to prevent recurrences in the upstream processes. ・Specify a service contract with developers to prohibit them from taking out confidential information when they quit.
3	Time limits for equipment usage	・Because algorithms and key lengths presently accepted adequate could become inadequate in the future, consider recommending users to discontinue equipment usage at a given point of time. ・With the IoT-GW estimated to have a long usage period, define the maintenance period as a vendor and make it well-known to the users through documentation or at a Website.
4	Educational activities	・Encourage users to change default passwords in user documentation or else. ・Make it well-known, in user documentation or else, that a single configuration error committed could put equipment at risk as it is directly connected to a network. ・Make equipment capacities well-known and what risks would be threatened if they were exploited.

5	Operating method proposals	・Make well-known the need to safeguard the whole system from threats, as by placing equipment within a protected network. ・Advise users to turn off those equipment functions that are not used (for example, UPnP, wireless LAN, PPP and IPv6). ・Make well-known the need to prevent unintended access to a wireless LAN, by MAC address filtering, as well as limiting access with SSIDs and passwords.

4.2.5 Disposal Phase

IoT-GW handles a diversity of data, which may include valuable data. Such data is typically transferred to a network and currently is not stored within the equipment, but some equipment comes with internal data storage. Hence, care should be taken in scrapping such equipment. This section describes how to assure security quality in the disposal phase.

Table 4-7 Security Efforts Made in the Disposal Phase

No.	Item	Description
1	Announcement of the method of device scrapping	・Specify, in user documentation or else, the possible threats and risks of scrapping equipment with data left inside. ・Use user documentation or else to suggest users who choose to scrap equipment to initialize its settings and stored data (to factory defaults). ・If the disposal of equipment by destruction is recommended, make it well-known to users, in user documentation or else, that they should abide by local regulations to dispose of equipment. ・ If scrapping equipment, recommend users, in user documentation or else, to confirm that the equipment has been properly destroyed so it cannot be put to reuse.

5 Risk Analyses and Assessment

In designing and developing a safe and secure IoT device, it is necessary to extract possible threats to the system and analyze risks in order to formulate security for formulating the security action policies to be implemented.

According to guidelines found in the International Organization for Standardization's ISO/IEC TR 13335-3 (GMITS Part 3)[10], risk scores can be calculated by multiplying the asset value, threat base value, vulnerability base value and frequency base value with one another. Because the impact sub score of a threat varies among use cases, the base values mentioned above may be tailored to suit each specific use case for the purpose of analyzing and assessing risks.

Here, a simplified method of risk analysis that is based on ISO/IEC TR 13335-3 is introduced. The principal workflow of risk analysis activity is shown in Figure 5-1 "Risk Analysis Procedures."

Use case definition

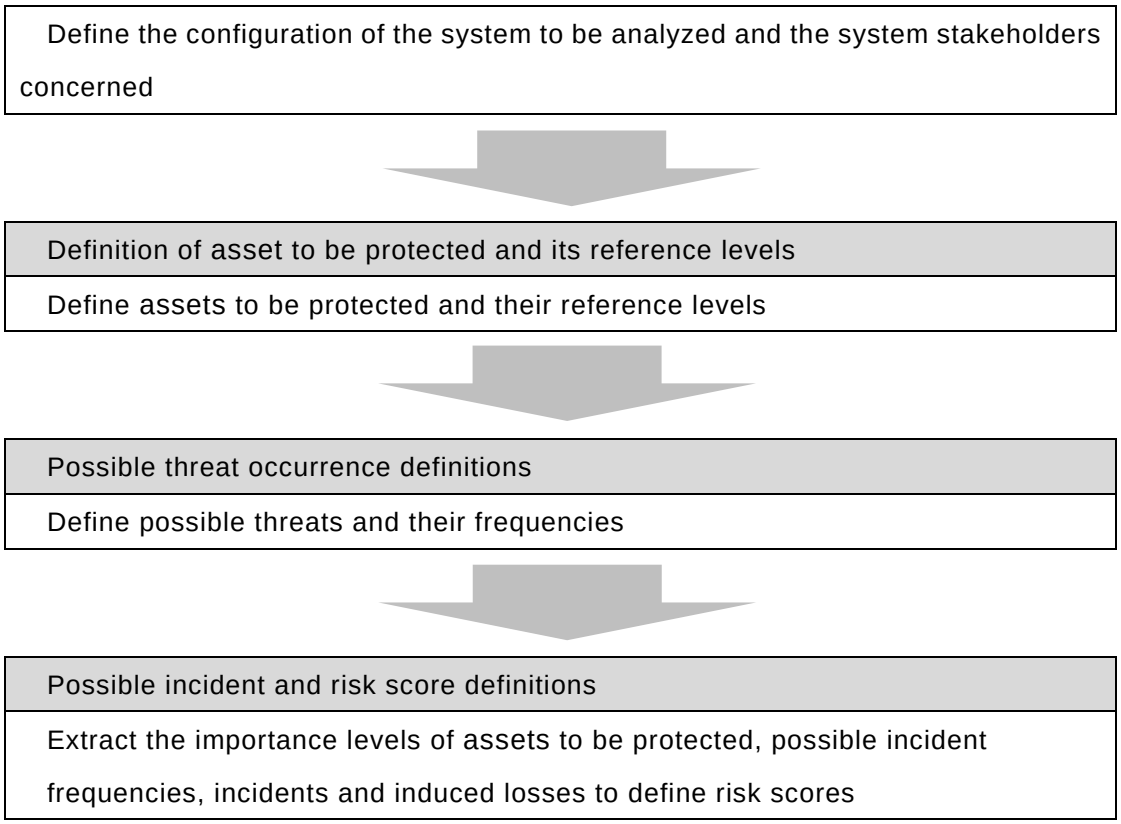

Figure 5-1 Risk Analysis Procedures

5.1 Use Case Definitions

Risk items vary greatly among different use cases in the world of IoT. The relevant characteristics and issues of IoT security and risk items differ from one use case to another, making the use cases difficult to group. What is important is to give a precise assessment to each individual use case. In this document, the system configuration to be analyzed and the information assets to be protected are defined based on the four use cases presented in Section 2.2.

5.2 Definitions of Assets to be Protected and Their Importance

Asset to be protected needs to be identified from the use cases defined in the foregoing section. They should be assumed from various aspects, including the kind of information handled by IoT devices, functions and bodies of the IoT devices themselves and more. Importantly, designers familiar with the product as a whole should identify all assets to be protected completely. Table 5-1 lists examples of the information assets to be protected in a use case of home gateways. Figure 5-2 shows the system configuration.

Table 5-1 Examples of Assets to be Protected Using Home Gateways as a Use Case

Asset to be protected (possible damage)	Causal security threat
Personal information	・Data theft resulting from end-point devices with an insufficient encryption strength. ・Attacks launched on end-point devices from a network.
Financial asset data	・Data theft resulting from end-point devices with an insufficient encryption strength. ・Attacks launched on end-point devices from a network.
Configuration information	・Data theft resulting from end-point devices with an insufficient encryption strength. ・Attacks launched on end-point devices from a network.
Log information	・Data theft resulting from end-point devices with an insufficient encryption strength. ・Attacks launched on end-point devices from a network.
Security information (digital certificates, cryptographic keys)	・Data theft resulting from end-point devices with an insufficient encryption strength. ・Attacks launched on end-point devices from a network.
Home gateway body	・Attacks intruding into a FAN/HAN physically to launch attacks.

*Home gateway use case

Wired LAN: PC (net surfing, net banking, net stock trading)

Wireless LAN: PCs, smartphones, portable games

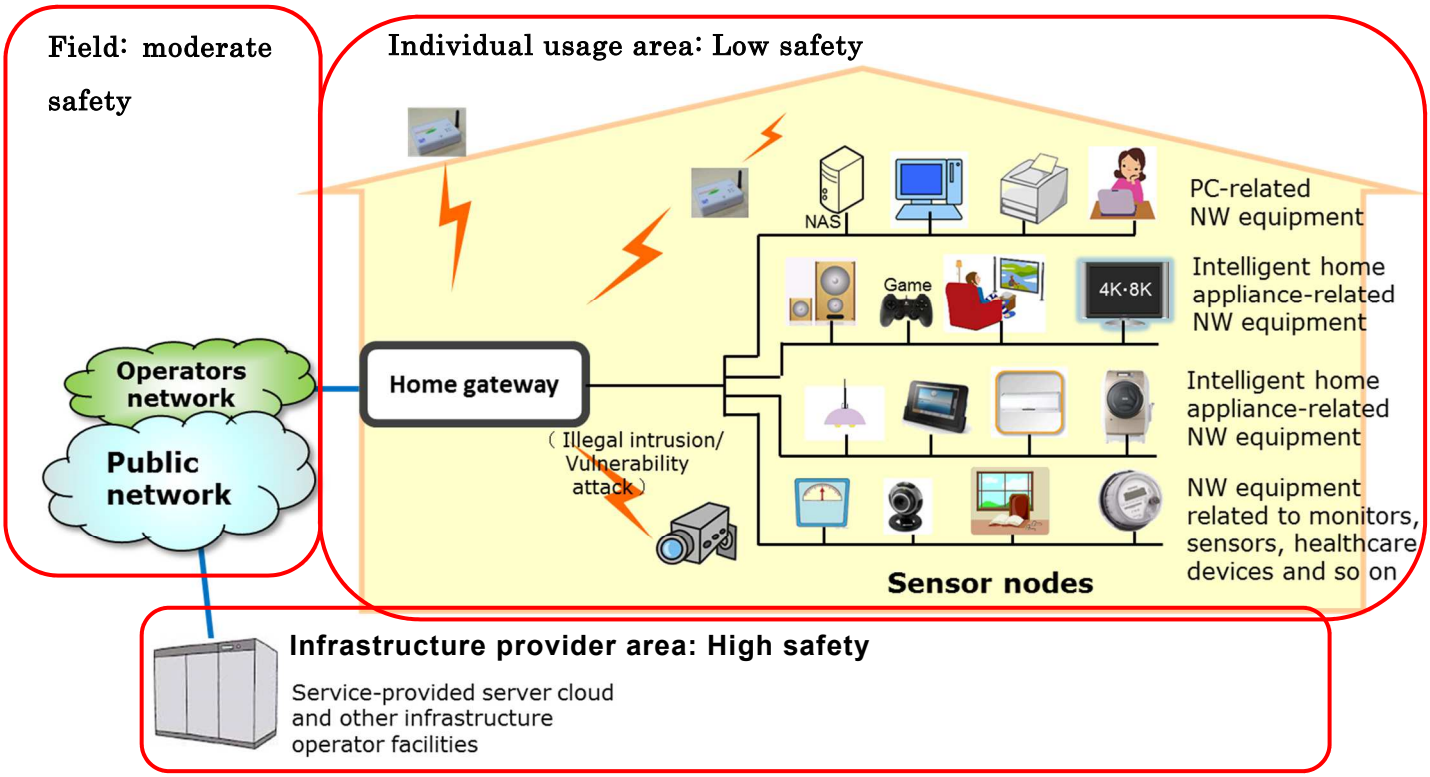

Figure 5-2 System Configuration in a Use Case of a Home Gateway

Next, define the importance of the information assets to be protected. Table 5-2 gives typical definitions of the importance of the information assets to be protected in the individual use cases established based on the NIST IR7628 importance criteria.

.

Table 5-2 Importance Definitions of Assets to be Protected

	Importance criteria		
	3 High	2 Moderate	1 Low
Confidentiality	Information that could compromise users' privacy or seriously endanger a system if leaked.	Any other information than that mentioned to the left, which is in constant use on a system and that could pose a threat for a certain period of time if leaked.	Any other information than that mentioned to the left, which only poses a transient and minor threat if leaked.
Integrity	Information that could produce illegal charging	Any other information than that mentioned to	Any other information than that mentioned to

	or adversely affect terminal control to cause physical damages if falsified.	the left, whose falsification could interfere with usage or administration for a certain period of time.	the left, whose falsification would incur only minor failures.
Availability	Complete loss of the availability of a system that handles information.	Loss of the availability of a system that handles information for a certain period of time.	Loss of the availability of a system that handles information only for a transient period of time and in part.

Table 5-3 and Table 5-4 each deal with the use case of a home gateway and give an example of the decisions made on whether to protect the assets handled by the home gateway. The importance of the assets to be protected is defined like this. Here, those information and physical assets having an importance score of 2 or higher are defined as requiring protection.

Table 5-3 Typical Definitions of Information Assets in a Home Gateway

No.	Information asset	Confidentiality (C)	Integrity (I)	Availability (A)	To be protected?
1	Personal information	3	3	2	Yes
2	Financial asset data	3	3	2	Yes
3	Configuration information	3	3	2	Yes
4	Log information	2	2	1	Yes
5	Security information (digital certificates, cryptographic keys)	3	2	2	Yes

Table 5-4 Important Definitions of Information Assets to be Protected in a Home Gateway

No.	Physical asset	Information assets No. to be generated or maintained	Confidentiality (C)	Integrity (I)	Availability (A)	To be protected?
6	Home gateway	1,2,3,4,5	3	3	3	Yes

	body					

5.3 Possible Threat Occurrence Definitions

Considering the frequencies with which the possible security threats exemplified in 3.3 will occur is an essential part of risk analyses. In this document, frequencies are divided into four levels as listed in Table 5-4 with the condition of long-term device usage characteristic of IoT taken into consideration.

Table 5-5 Possible Threat Occurrence Definitions

Frequency	1: (minimal)	2: (low)	3: (medium)	4: (high)
	Once every 10 years or more	Once every 5 years or more	Once every 2 years or more	Once every 1 year or more

5.4 Possible Incident and Risk Score Definitions

To illustrate a use case of home gateways, possible incidents have been extracted from threat analyses and risk calculations conducted using the importance and frequency parameters of the incidents. Typical results are presented in Table 5-6. The risk scores calculated here are relative assessments and cannot be used as definite criteria for determining that an incident having a certain score or higher is risky or not, but, if the risk calculation is implemented in the product planning stage, it should still help define the security action policies to be pursued in the design and manufacturing phase.

Table 5-6 Possible Incidents and Results of Risk Scoring

Incident	Induced loss	Possible threat*	Related assets	Importance			Frequency	Risk score
				C	I	A		
GW breakage and shutdown	Disrupted communication with public networks	5 DoS attacks 6 Alteration or destruction	2,6	-	-	3	2	6
GW information leakage	Leakage of information between a public network	5 Tampering of settings 10 Illegal firmware loading	1-6	3	-	-	4	12

	and a GW	9 Spoofing device usage 10 Virus infection 8 Communications data interception						
GW malfunctioning	Falsification of information between a public network and a GW	5 Tampering of settings 10 Illegal firmware loading 9 Spoofing device usage 10 Virus infection 8 Communications data interception	1-6	-	3	3	3	27

*Correlated to threat numbers given in Section 3.3.

Apart from discussions of the simple methods to carry out risk analyses above, numerous methods of analyzing and assessing risks in an information system exist. Typical methods are ETSI TS 102 165-1 [8] and CVSS v3.0 [9]0. The following is a summary description of these two methods, along with their issues.

5.5 ETSI Assessment Method

ETSITS102165-1 is a method of risk analysis and assessment for information systems involving communication as formulated by the European Telecommunications Standards Institute (ETSI). It assesses the risks of vulnerabilities detected in a system to help operations managers prioritize the vulnerability countermeasures to be taken. Score risks by multiplying the likelihood of attack (calculated from assessments of the attack time required, attacker expertise, required system knowledge, attack opportunity and attack equipment) and the attack impact sub score (calculated from assessments of the impact on assets and attack intensity. ETSI TS 102 165-1 may be considered as a simple method of assessment based on the calculation of the likelihood of attack multiplied by the impact sub score.

5.6 CVSS Assessment Method

CVSS v3.0 is an open and versatile method of evaluating vulnerabilities in an information system, managed by a federation of global security teams, the Forum of Incident Response and Security Teams (FIRST). Like ETSI TS 102 165-1, the objective of CVSS v3.0 is to help operation managers evaluate the risks of vulnerabilities uncovered in a system and prioritize vulnerability countermeasures. It assesses the attack vector, attack complexity, privilege required level, user interaction scope, confidentiality impact, integrity impact(information falsification) and availability (business suspension) impact as base metrics and calculates an assessment score according to a predefined formula. In addition to the base metrics above, temporal metrics and environmental metrics are also calculated to score risks from a comprehensive perspective. CVSS v3.0 thus offers a tool of evaluating the risks of vulnerabilities at large.

5.7 Analysis and Assessment System Issues

The ETSI and CVSS assessment methods, when compared with the methods introduced in 5.1 to 5.5, have difficulty assessing a certain repertoire of parameters because they are not designed to provide a tool of risk assessment in a pre-system implementation stage. They do not pay heed to impacts on human lives and societies as described in 2.3 either. Use of any existing assessment method should allow for the aforementioned issues.

Whether existing methods are used or an organization’s own methods developed based on its store of know-how are used, they should be selectively used to suit specific use cases from the viewpoint of user convenience.

6 Conclusion

6.1 Relationship with IoT Safety/Security Development Guidelines Prepared by the IPA

This document is a detailed version of the IoT Safety/Security Development Guidelines that have already been published by the IPA. The table below provides the correspondence between the 17 guidelines set forth in the IoT Safety/Security Development Guidelines and this document.

Table 6-1 Correspondence between Smart-society Development Guidelines and this Document

IoT Safety/Security Development Guidelines			Corresponding part of this book	
Major item		Guidelines	Chapter No.	Overview
Policy	Making corporate efforts for the Safety/Security of the Smart-society	Guideline 1 Formulating the basic policies for Safety/Security	4.2.1	Product Planning Phase No.3: Information security policies described as a measure.
		Guideline 2 Reviewing systems and human resources for Safety/Security	4.2.1	Product Planning Phase No.3: Information security policies described as a measure
			4.2.4	Operation Phase 2: Organizational framework described as a
		Guideline 3 Preparing for internal frauds and mistakes	4.2.2	Design and Manufacturing Phase No.6: Efforts in outsourcing development activity described as a measure.
Analysis	Understanding the risks of the Smart-society	Guideline 4 Identifying the objects to be protected	2	Chapter 2 : System configuration defined as a typical implementation and assets to be protected in individual use cases listed.
			4.2.1	Product planning phase No.1 and 2: Risk analysis is described as a measure.
			5	Chapter 5: Examples of use case-specific physical risks introduced.
		Guideline 5 Assuming the risks caused by connections	2	Chapter 2 : Use case-specific damages and impacts listed as a typical implementation.
			3.3	3.3:Examples of possible security risks introduced.
			4.2.1	Product Planning Phase No. 1 and 2: Risk analyses described as a measure.
			5	Chapter 5: Examples of use case-specific physical risks introduced.
		Guideline 6 Assuming the risks spread through connections	(Same as above)	Similar to Guideline 5.
		Guideline 7 Understanding physical security risks	4.2.1	Product Planning Phase No. 1 and 2: Risk analyses described as a measure.
			4.2.2	Design and Manufacturing Phase No. 5 : Countermeasures against physical attacks described as a measure.
			5	Chapter 5: Examples of use case-specific physical risks introduced.
Design	Considering the designs to protect the objects to be protected	Guideline 8 Designing to enable both individual and total protection	4.2.2	Design and Manufacturing Phase No. 2 and 5 : Implementation of security functions described as a measure.
		Guideline 9 Designing so as not to cause trouble in other connected entities	4.2.2	Design and Manufacturing Phase No. 2 : Functions to prevent inconvenience as measures.
		Guideline 10 Ensuring consistency between the designs of safety and security	4.2.1	Product Planning Phase No. 1 and 2: Identification of threats for realizing safety and security described as a measure.
			4.2.2	Design and Manufacturing Phase No. 1, 2,3,4,5: Countermeasures against threats extracted as measures.
		Guideline 11 Designing to ensure Safety/Security even when connected to unspecified entities	4.2.2	Design and Manufacturing Phase No. 3 : Protocols used to communicate with remote partners described as a measure.
		Guideline 12 Verifying/validating the designs of safety and security	4.2.3	Assessment Phase 1 : Assessment to verify problem-free designs described as a measure.
Maintenance	Considering the designs to ensure protection even after market release	Guideline 13 Implementing the functions to identify and record own status	4.2.2	Design and Manufacturing Phase No. 2 : Logging functions used to record the status of local equipment described.
		Guideline 14 Implementing the functions to maintain Safety/Security even after the passage of time	4.2.2	Design and Manufacturing Phase No. 2: Implementation of program update functions described as a measure.
			4.2.4	Operation Phase No. 1: Program updates described as a measure.
Operation	Protecting with relevant parties	Guideline 15 Identifying IoT risks and providing information after market release	4.2.4	Operation Phase No. 1 and 2: Corresponding to the latest vulnerability as a measure and the correspondence of the organization.
		Guideline 16 Informing relevant business operators of the procedures to be followed after market release	4.2.4	Operation Phase No. 1 and 2: Framework to be built by the organization after market release described.
			4.2. 5	Disposal Phase No. 1: Risk indications in the disposal phase described as a measure.
		Guideline 17 Making the risks caused by connections known	4.2.2	Design and Manufacturing Phase No. 2: Risk and threat indications in user documentation described as a measure.

6.2 Conclusion

While this document has been prepared as security guidelines targeting the IoT-GW field, the discussions of possible threats, security efforts to be made in the lifecycle of a product and other topics presented could apply to other fields as well. Positive use of these guidelines is recommended to allow for the implementation of security measures in the processes of developing diverse products.

Efforts will continue to develop threat information at a higher level of refinement and assist in the entrenchment of a system of device authentication certification pursuant to these Guidelines.

Appendix

Appendix 1: Protocols Used and Their Vulnerabilities, and Possible Impacts

No.	Protocol	Possible threat	Possible threat example	Possible impact
1	IPv4	Denial of Service	System crashes occurring on reassembly of fragmented packets (teardrop attack)	If a TCP/IP implementation problem exists that prevents fragmented packets having duplications of data from being processed normally, events, such as a system crash, reboot or hang up, would occur, disabling services as a consequence.
2	ICMP	Denial of Service	Packet overflow during reassembly (ping of death)	Buffers might overflow if an ICMP having a number of fragmented packets is reassembled, resulting in a system crash, reboot and more.
3	TCP	Spoofing	TCP initial sequence number prediction	It makes possible for packets to be received and processed by the receiving host, using the forged IP address of the sender.
4		Denial of Service	Occupancy of server resources by SYN packets (SYN flood attack)	As SYN packets are received, the resources, such as connection backlog in which to store connection information necessary to establish a TCP connection, are exhausted, making it impossible to accept new connections.

5	UDP	Denial of Service	Invalid UDP header length field	Possible impacts include an OS or system crash occurring while processing invalid packets.
6	HTTP	Information Leakage	Attacks based on commands, codes, or query injection	Personal or organizational information could be exploited by SQL injection or through the execution of arbitrary commands.
7	HTTP	Denial of Service	Attack exploiting the protocol element length	Transmits a long character string that exploits vulnerabilities in the parser part of a http header to disable a service, as by squeezing the bandwidth.
8	HTTPS/TLS	Spoofing	Deficiencies in certificates and authentication	If an untrustworthy CA is registered, the authenticity of certificates issued by it would be unpredictable.
9		Information Leakage	Use of anonymous key exchanges	If both a server and its clients use an anonymous authentication mode, they would be essentially made more susceptible to man-in-the-middle attacks to exploit information.
10		Denial of Service	Version rollback attack	Initiates handshaking by falling back to SSL2.0 and exploits uncorrected vulnerabilities in SSL2.0 to launch an attack, resulting in a disabled service.
11	CoAP	Denial of Service	Protocol parser and URI processing	Attacks deficiencies in the implementation of a complex parser or URI processing code to crash a remote node.

12		Denial of Service	Amplification attack	Generally, CoAP servers return a response packet larger than the request packet. Services could be crippled as the bandwidth is squeezed by amplified packets responsive to a large number of request packets.
13	FTP	Falsification	Anonymous FTP	Inadequate file access control could allow anonymous users to read all files or create new files.
14	FTP	Information leakage	Illegal login	Illegal login can be made possible by leaving login ID and passwords unchanged from their defaults, setting no passwords or using easily inferable passwords. As a result, files could be rewritten, malware delivered, information leaked or botnets formed.
15		Privilege escalation	Brute force attack	Brute force attacks during parallel sessions allow identification of privileged users' passwords.

References

[1] H. Takada, A. Goto and et al., “IoT Safety/Security Development Guidelines,” Information-technology Promotion Agency, Japan (IPA), First Edition, 2016, http://www.ipa.go.jp/files/000053920.pdf.

[2] Gartner, "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," 2015. http://www.gartner.com/newsroom/id/3165317.

[3] IIJ, "ホームルータへの不正な設定変更による偽 DNS サーバの参照," Internet Initiative Japan (IIJ), 2012, https://sect.iij.ad.jp/d/2012/06/148528.html.

[4] IPA, "医療機器における情報セキュリティに関する調査," Information-technology Promotion Agency, Japan (IPA), First Edition, 2013, https://www.ipa.go.jp/security/fy25/reports/medi_sec/.

[5] IPA, "情報セキュリティ 10 大脅威 2016," Information-technology Promotion Agency, Japan (IPA), First Edition, 2016, https://www.ipa.go.jp/security/vuln/10threats2016.html https: //www.ipa.go.jp/files/000045039.pdf https: //www.ipa.go.jp/files/000037151.pdf.

[6] OWASP, "Internet of Things Top Ten," Open Web Application Security Project (OWASP), First Edition, 2014, https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf.

[7] DevCentral, "IoT のセキュリティリスク Top10 とそれらへの対応方法," 2015. https://devcentral.f5.com/articles/iot-top-1

[8] ETSI, "ETSI TS 102 165-1 v4.2.3: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis," European Telecommunications Standards Institute (ETSI), First Edition, 2011, http://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/04.02.03_60/ts_10216501v040203p.pdf.

[9] FIRST, "Common Vulnerability Scoring System v3.0: Specification Document," the Forum of Incident Response and Security Teams (FIRST), First Edition, 2015, https://www.first.org/cvss/specification-document.

[10] ISO/IEC TR 13335-3 (GMITS part3): “Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security.“

[11] METI, "アウトソーシングに関する情報正キュリティ対策ガイダンス," Ministry of Economy, Trade and Industry (METI), First Edition, 2009, http://www.meti.go.jp/policy/netsecurity/docs/secgov/2009_OutsourcingJohoSecurityTaisakuGuidance.pdf.

[12] NISC, "外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書," National center of Incident readiness and Strategy for Cybersecurity (NISC), First Edition, 2015, http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0303.pdf.

[13] NIST Special Publication 800-88 Guidelines for Media Sanitization
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf