IoT System Security

UMEZAKI, Kazuya*

ABSTRACT

The current rapid growth of the Internet of Things (IoT) leads to a significant increase in cyberattacks and security incidents on the IoT devices. To address the IoT security risks, efforts to produce standards and guidelines has been progressing in Japan and other countries. Fuji Electric has established the information security policy based on the IoT security standards and guidelines and takes technical, physical, organizational, and personnel measures to build IoT systems that are secure and safe from their threat.

1. Introduction

Internet of Things (IoT) devices have been rapidly increasing in number recently. In 2020, about 30 billion IoT devices are predicted to be connected to the Internet[1]. As a result, cyberattacks and security incidents targeting IoT devices are also increasing rapidly. Thus, standards and guidelines for IoT security are being developed in Japan and overseas.

On the basis of this situation, Fuji Electric is proceeding with IoT security efforts.

This paper explains examples of IoT system security problems and threats, the concept of IoT security measures based on guidelines in Japan and overseas, and Fuji Electric's efforts.

2 IoT Security Trend

2.1 Security problems of IoT system

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[2),(3)]." The following effects are expected[3].

(a) Connecting things to a network makes it possible to collect information quickly and accurately, and control devices and systems in real time.

(b) Mutually linking devices and systems in different fields enables new functions to be provided.

The following would be IoT security problems[3].

○ The extent of threat impact resulting from various devices and systems being connected

○ Difference in security concepts and requirements among various devices and systems

○ Limitation on security measures that can be taken associated with restrictions on the functions and performance of IoT devices

○ Insufficient monitoring of IoT devices

○ Long life cycle of IoT devices

Thus, connecting IoT produces values. On the other hand, there is a concern that the devices and equipment that have not been conventionally connected to the Internet may undergo cyberattacks, increasing security threats.

2.2 Example of security threat against IoT devices

The examples below are known as security incidents of IoT devices[3].

(a) Web cameras and home energy management systems (HEMS) connected to the Internet were accessible from the outside because of improper setting.

(b) A vulnerability in the multimedia system of an automobile was attacked, enabling unauthorized remote operation that affected driving.

In both cases, there was unauthorized access from the connection path to the outside such as the Internet or Wi-Fi*1. Unauthorized access succeeded because the device users did not perform appropriate setting and management (access via the development and maintenance interface remained possible, or the default password was not changed) and IoT devices were vulnerable.

Hijacked IoT devices may be used as a stepping stone and cause further invasion and attacks on other parts of a system. In September 2016, several distributed denial-of-service (DDoS) attacks were caused by "Mirai," the botnet of malware targeting vulnerable

* Corporate R&D Headquarters, Fuji Electric Co., Ltd.

*1: Wi-Fi: Trademark or registered trademark of Wi-Fi Alliance

IoT devices. This brought great confusion to the Internet in the entire area of the East Coast of the United States.

3 IoT Security Measure

Regarding IoT security, standards and guidelines related to security are being developed in Japan and overseas. Table 1 shows the main standards and guidelines.

There are various IoT security approaches to these security standards and guidelines, but the basic concept is as follows.

(1) Risk analysis

Identify the assets to be protected, and analyze threats and its influence.

(2) Security measure

Determine and implement the measures against threats on the basis of risk analysis.

3.1 Risk analysis

Risk analysis comprises following three steps: clarifying system configuration, identifying information assets, and analyzing threats.

(1) Clarifying system configuration

There is a slight difference depending on the standards and guidelines, but the IoT system is generally classified into 4 layers as shown in Fig. 1.

The components (devices and systems) in each layer of the IoT system and the dataflow between them are identified and documented.

Table 1 Standards and guidelines related to IoT security

Classification	Publisher*	Name of standards and guidelines	Date of issue
Overseas	oneM2M	oneM2M Technical Specification Application of Security Technology	2016-03 (V1.0.0) 2018-02 (V2.0.1)
	GSMA	GSMA IoT Security Guidelines	2016-02 (V1.0) 2017-10 (V2.0)
	IIC	IIC Security Framework	2016-09 (V1.0)
	CSA	Security Guidance for Those Adopting IoT at Early Stage	2016-02 (V1.0)
	OTA	OTA IoT Trust Framework	2016-03 (V1.0) 2017-06 (V2.5)
Japan	IPA	Guidance on Security Designing in IoT Development	2016-05 (first edition) 2018-04
	IoT Promotion Consortium	IoT Security Guideline	2016-07 (V1.0)

* oneM2M: International standards organization of M2M and IoT technologies in the electronic information communication field
GSMA: GSM Association. Business organization of the GSM scheme, which is one kind of mobile phone systems.
IIC: Industrial Internet Consortium. Business organization that promotes implementation of industrial IoT.
CSA: Cloud Security Alliance. Non-profit organization specialized in cloud security.
OTA: A lower branch of Internet Society, an international non-profit organization related to the Internet
IPA: Information-technology Promotion Agency

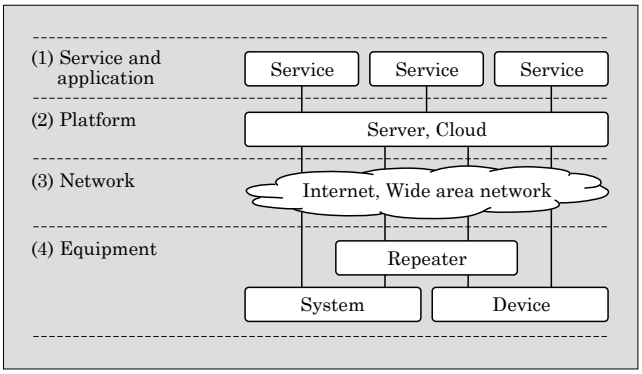

Fig.1 Hierarchical structure of IoT system

(2) Identifying information assets

The information, functions, and assets contained in the IoT system components are clarified, and then objects to be protected are identified by importance.

(3) Analyzing threats

Existing analysis methods are applied in threat analysis for IoT systems. STRIDE, which is one of the analysis methods, performs analysis for the types of threats shown in Table 2, and extracts vulnerable parts that may be affected by the threats[(3) to (5)]. The degree of influence is analyzed on the extracted threat. In DREAD, which is one of the analysis methods, the in-

Table 2 Threat types and examples of STRIDE

Types of threats	Examples of threats
Spoofing	Unauthorized acquisition of IDs and credentials (passwords, for example) causes spoofing of IoT devices and users.
Tampering	Data is rewritten in one of the stages of data collection, processing, migration or storage in the IoT system.
Repudiation	Bad data is supplied to the system by unauthorized device connection, not allowing the system to operate properly.
Information Disclosure	Data is accessed in an unauthorized manner in one of the stages of data collection, processing, migration or storage in the IoT system.
Denial of Service	A large amount of data is transmitted to the IoT system components, and the system functions become unavailable.
Elevation of Privilege	Devices and users without authority can access functions and data of the IoT system.

Table 3 Risk evaluation method DREAD

Evaluation axis of influence	Description
Damage potential	Degree of damage when vulnerability is attacked
Reproducibility	How easy attacks can be reproduced (success)
Exploitability	How easy attacks can be misused
Affected users	Scale of users influenced by attacks
Discoverability	Possibility that attackers find vulnerability

Table 4 Classification of security measures

Types of measures	Examples of measures
Technical measures	User identification and authentication, device identification and authentication, access control, firewall, intrusion detection system, communication path encryption, data encryption, log collection, etc.
Physical measures	Information processing area management, prevention of information asset theft, management of electronic media, deletion and disposal management of information assets
Organizational measures	Building organizational system, operation in accordance with rules and procedures, system monitoring, vulnerability handling system, incident response system, etc.
Personal measures	Improvement of employee awareness, education, training, etc.

fluence of the attack on the vulnerability is evaluated by the evaluation axes shown in Table 3[4].

3.2 Security measure

Based on the risk analysis result, security measures are selected and implemented for those risks with a large influence.

Security measures can be divided into 4 types—technical measure, physical measure, systematic measure and personal measure—as shown in Table 4.

4. IoT Security Efforts of Fuji Electric

4.1 Fuji Electric IoT platform

As shown in Fig. 2, our IoT platform has a configuration in which field devices link with services on the cloud with IoT devices called edge controllers as gateways.

For security on this IoT platform, we have developed a security policy considering the risk analysis

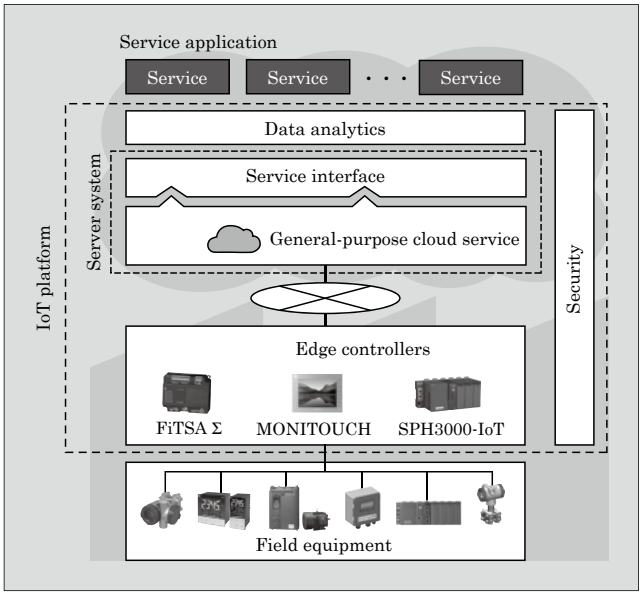

Fig.2 Configuration of Fuji Electric IoT platform

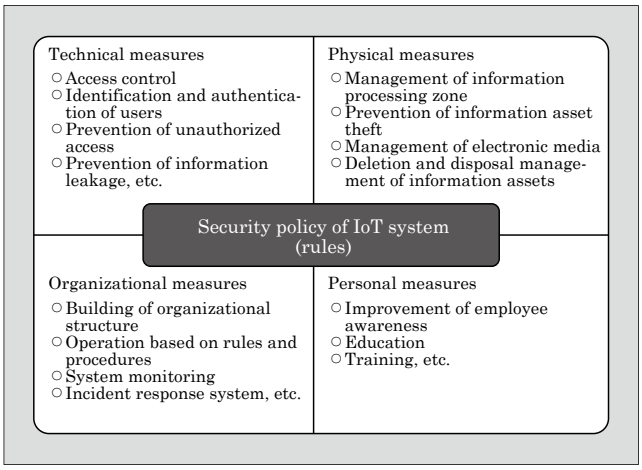

Fig.3 IoT security policy of Fuji Electric

result and various guidelines, and we are promoting measures shown in Fig. 3 based on the policy.

4.2 Security policy of IoT system

We have developed an in-house standard for IoT system security. The standard is applicable to our IoT systems and related business activities, such as development, construction, operation, and maintenance, computers and electronic storage media used for these tasks, and the employees who work for the tasks. The in-house standard is based on the concept of security standards and guidelines such as ISO/IEC 27017: 2015[6] and IoT security guidelines[3].

4.3 Technical and physical security measure

(1) Measure in general-purpose cloud service

The server system of the IoT platform is built on an external general-purpose cloud service. The general-purpose cloud service is selected and used after checking the security measure status. Specifically, the cloud service provider has acquired ISO 27001 and ISO 27017 certifications and takes the following measures to secure confidentiality, integrity and availability (CIA).

(a) Measure as data center

Intrusion prevention, entry/exit management, operation evidence management, etc.

(b) Measure against network

Firewall, intrusion detection, communication encryption, redundancy etc.

(c) Measure against physical storage and physical server

Access restriction, data encryption, virus infection prevention, operation evidence management, redundancy, etc.

(d) Measure against the virtualization infrastructure

Separation by network virtualization, vulnerability information support, auto failover, etc.

(2) Measure against server system and service on cloud

For the service IoT platforms such as data analytics and service interfaces developed by Fuji Electric, the following security measures of the conventional server cloud application are applied.

(a) Avoidance of vulnerability
Conformity with guidelines for secure software development

(b) Prevention of unauthorized access
Identification and authentication of users of service, access control, protection of important data, etc.

(3) Measures on edge controllers and communication

Regarding edge controllers, which access the IoT platform on a cloud, identification, authentication and communication encryption are performed as follows to prevent unauthorized access.

(a) Authentication and encryption on the communication path.
(b) Intrusion prevention at connection points (firewall, VPN, etc.) to a network.
(c) Mutually authentication between the server system and edge controllers.
(d) Access control to the server system.
(e) Device authentication for the edge controller as a data source by the service interface.

4.4 Organization and human security measure

(1) On the basis of the Fuji Electric Risk Management Rules, which were formulated in May 2006, the Company manages risk in a coordinated, systematic manner. Information security is managed as a part of the risk management (see Fig. 4). To protect confidential and personal information properly, Fuji Electric has formulated and implemented a policy and rules related to information security. We seek to strengthen information security by instituting annual training programs for employees and endeavor to prevent information leaks. Companies that handle customer's confidential and personal information and require a high-level information security management have acquired external certification, such as an information security management system (ISMS) certification and Privacy Mark certification.

(2) Fe-CSIRT

We have established the Computer Security Incident Response Team (Fe-CSIRT) in April 2017 to enhance flexibility and defense capability against security threats that are becoming diversified and complicated such as targeted cyberattacks and attacks on the control system and IoT vulnerability.

As one of the IT strategy groups of Fuji Electric, the team deals with and prevents information security incidents that occur within the Fuji Electric groups under the existing information security management system in cooperation with the office that leads monitoring, audit and education.

Regarding IoT, we also constructed an organization and operational structure for incident response as with the Fe-CSIRT system.

5. Postscript

Security of an IoT system has been explained in this paper. Cyberattacks and security incidents are increasing with the increase in the number of IoT devices. We are constructing an IoT system that can be used safely and securely by developing security policies considering the threats against an IoT system and implementing measures in terms of the system and the mechanism.

Cyberattacks are progressing every day, and it is indispensable to have an ongoing approach to security measures. Fuji Electric will continue developing technology to ensure the security of IoT systems.

References

(1) 2018 White Paper on Information and Communications in Japan. Ministry of Internal Affairs and Communications.
(2) ITU-T Y. 2060 (4000), Overview Of Internet Of Things. 2012.
(3) IoT Security Guidelines Ver. 1.0. IoT Acceleration Consortium; Ministry of Internal Affairs and Communications; Ministry of Economy, Trade and Industry. 2016.
(4) Security Guidance for Early Adopters of the Internet of Things (IoT). Cloud Security Alliance. 2015.
(5) IIC Security Framework. 2016.
(6) ISO/IEC 27017: 2015.

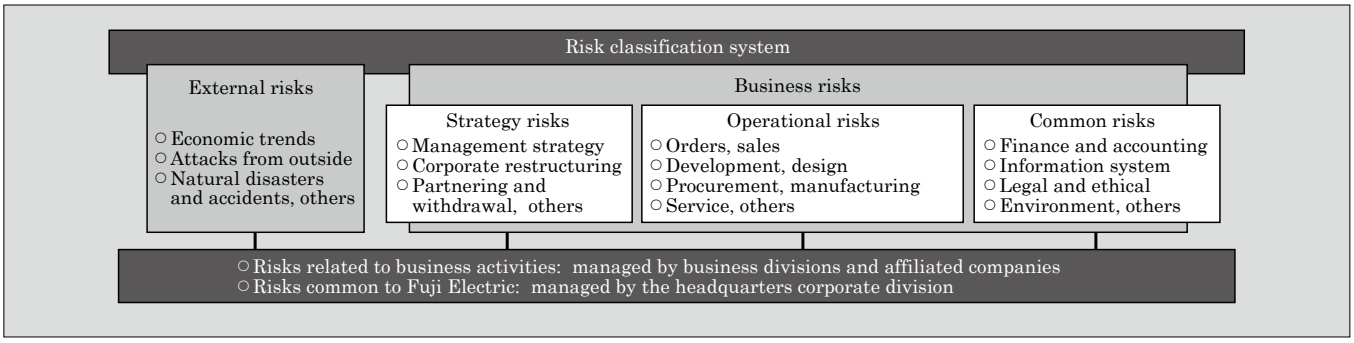

Fig.4 Risk classification system and management system of Fuji Electric

Fuji Electric

Innovating Energy Technology