IoT 系统的安全

IoT System Security

梅崎　一也 UMEZAKI, Kazuya

近年来，随着 IoT（Internet of Things）设备的快速增加，以 IoT 设备为目标的网络攻击、安全意外事件激增。为此，日本国内及海外各国正在不断完善与 IoT 安全相关的规格及指南。富士电机针对 IoT 系统面临的威胁，制定符合 IoT 安全相关规格及指南的安全方针，通过在技术、物理、组织、人员方面采取对策，建立可安全安心利用的 IoT 系统。

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　引言

近年来，IoT（Internet of Things）设备急速增加，预测 2020 年约有 300 亿台 IoT 设备将与互联网连接[1]。以 IoT 设备为目标的网络攻击、安全意外事件也随之激增。为此，日本国内及海外各国正在不断完善与 IoT 安全相关的规格及指南。

富士电机基于上述情况正在就 IoT 的安全采取相关措施。

本文将对 IoT 系统安全方面的课题及面临的威胁事例、基于日本国内外指南等 IoT 安全对策的思考方式，以及富士电机所采取的措施进行介绍。

2　IoT 的安全动向

2.1　IoT 系统的安全课题

IoT 是“为了建立信息社会，利用现有或开发中的可相互运用的信息通信技术，连接实际或虚拟的物体，实现高级服务的全球基础设施[2]、[3]”，预计可达成以下事项[3]。

(a)　物体与网络互联后，可快速准确地收集信息，并实时对设备及系统进行控制；

(b)　不同领域的设备及系统相互协作，可提供新功能。

IoT 的安全课题列举如下[3]。

- 由于连接众多设备及系统，威胁影响波及范围广
- 众多设备及系统之间对安全的思考方式及重要条件的要求存在差异
- 基于 IoT 设备功能性能方面的制约，可采用的安全对策受到限制
- 对 IoT 设备的监视不充分
- IoT 设备的较长生命周期

如此，IoT 通过联网产生价值，但另一方面，将过去没有联网的装置及设备连接到互联网后，这些设备受到网络攻击等安全威胁的可能性增加。

2.2　威胁 IoT 设备安全的事例

针对 IoT 设备安全意外事件的具体事例如下[3]：

(a)　联网的网络摄像头、HEMS（Home Energy Management System）因设定不正确等原因导致有可能从外部进行访问；

(b)　对汽车多媒体系统的脆弱性进行攻击后，可执行对驾驶造成影响的非法远程操作。

无论哪种都是经由互联网或 Wi-Fi〈注〉等与外部的连接路径进行的非法访问。非法访问之所以成功，可能是因为设备使用者没有进行正确的设定和管理（仍然可从开发及维护用接口进行访问，密码为默认设置而没有修改等），以及 IoT 设备存在脆弱性。

IoT 设备被攻占后，可能会以此为跳板进一步入侵到内部，或者用于其他攻击。2016 年 9 月以 IoT 设备为目标的恶意软件“Mirai”僵尸网络进行了多起 DDoS（分散式阻断服务）攻击，导致整个美国东海岸的互联网使用发生巨大混乱。

3　IoT 的安全对策

针对 IoT 的安全性，日本及海外各国已经制定了安全相关的规格及指南。主要规格与指南如**表 1** 所示。

这些与安全相关的规格及指南针对 IoT 的安全做出了各种各样的规定，但基本思考方式如下：

(1)　风险分析

确定需要保护的对象，对预期的威胁及其影响进行分析。

(2)　安全对策

〈注〉Wi-Fi：Wi-Fi Alliance 的商标或注册商标

表 1　与 IoT 安全相关的规格及指南

分类	发行方 *	规格及指南名称	发行日
海外	oneM2M	oneM2M 技术规格书 安全技术的运用	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	针对 IoT 早期引进方的安全指导	2016-02（V1.0）
	OTA	OTA IoT Trust Framework	2016-03（V1.0） 2017-06（V2.5）
日本国内	IPA	IoT 开发的安全设计手册	2016-05（初版） 2018-04
	IoT 推进协会	IoT 安全指南	2016-07（V1.0）

★ oneM2M　：电气信息通信领域的 M2M/IoT 技术国际标准化团体
GSMA　：GSM Association 手机系统之一的 GSM 方式的行业团体
IIC　：Industrial Internet Consortium 动工业 IoT 产业实装的行业团体
CSA　：Cloud Security Alliance 专门开展云安全活动的非营利团体
OTA　：互联网相关国际非营利团体 Internet Sociery 的下级组织
IPA　：信息处理推进机构

依据风险分析结果，根据重要性确定并采取针对威胁的对策。

3.1　风险分析

在风险分析中，明确系统结构，确定信息资产，实施威胁分析。

⑴　明确系统结构

系统结构根据规格及指南会有些许差异，但是 IoT 系统如**图 1** 所示，可分为四个阶层。

对各个阶层中有哪些设备及系统，相互之间如何协作（信息交换）进行分析，并制作成文档。

⑵　确定信息资产

找出 IoT 系统构成要素中所含的信息、功能、资产，并根据重要性确定需保护的对象。

⑶　威胁分析

威胁分析使用了现有的分析方法。运用分析方法之一的 STRIDE 对**表 2** 所示威胁类型进行分析，提取可能受威胁影响的部位（脆弱性）[3]～[5]。

对提取的威胁分析其影响度。使用分析方法之一的 DREAD 根据**表 3** 所示的评价轴对攻击脆弱性的影响进行评价[4]。

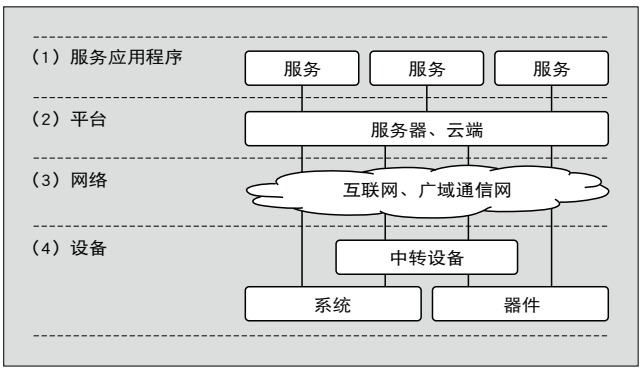

图 1　IoT 系统的层次结构

表 2　STRIDE 的威胁类型与示例

威胁类型	威胁示例
Spoofing（幌骗）	以非法途径获取各种 ID 及资格信息（密码等），伪装成 IoT 设备及用户
Tampering（篡改）	在 IoT 系统的数据收集、加工、转发、保存的各阶段改写数据
Repudiation（否认）	与非法设备连接，将不良数据供应给系统，导致系统无法正常运行
Information Disclosure（信息泄露）	对 IoT 系统构成要素发送大量数据，陷入无法使用系统功能的状态
Denial of Service（拒绝服务）	对 IoT 系统构成要素发送大量数据，陷入无法使用系统功能的状态
Elevation of Privilege（权限提升）	原本不具有权限的设备及用户可以访问 IoT 系统的功能及数据

表 3　风险评价方法 DREAD

的评价轴	说明
Damage potential（潜在破坏）	脆弱性遭受攻击时的损失程度
Reproducibility（重现性）	重现（成功）攻击的便捷性
Exploitability（可利用性）	针对攻击的滥用便捷性
Affected users（受影响用户）	受攻击影响的用户规模
Discoverability（可发现性）	攻击者发现脆弱性的可能性

表 4　安全对策分类

对策种类	对策示例
技术对策	使用者识别及认证、设备识别及认证、访问控制、防火墙、入侵检测系统、通信路径加密、数据加密、日志收集及分析 等
物理对策	信息处理区域管理、信息资产防盗、电子媒体等的管理、信息资产的删除及废弃管理 等
组织对策	组织体制的完善、基于使用规定等的运用、系统监视体制、脆弱性应对体制、意外事件应对体制 等
人员对策	提高员工意识、教育及培训 等

3.2　安全对策

依据风险分析的结果，针对影响较大的选择并实施安全对策。

安全对策如**表 4** 所示，可分为技术对策、物理对策、组织对策、人员对策的 4 种。

4　富士电机在 IoT 安全上采取的措施

4.1　富士电机 IoT 平台

如**图 2** 所示，富士电机 IoT 平台的结构为：以被称为边缘控制器的 IoT 设备作为网关，将现场的现场设备与云端上的服务连接。

为了确保该 IoT 平台的安全，依据风险分析结果和各种指南制定安全方针，然后根据该安全方针推动**图 3** 所示的对策。

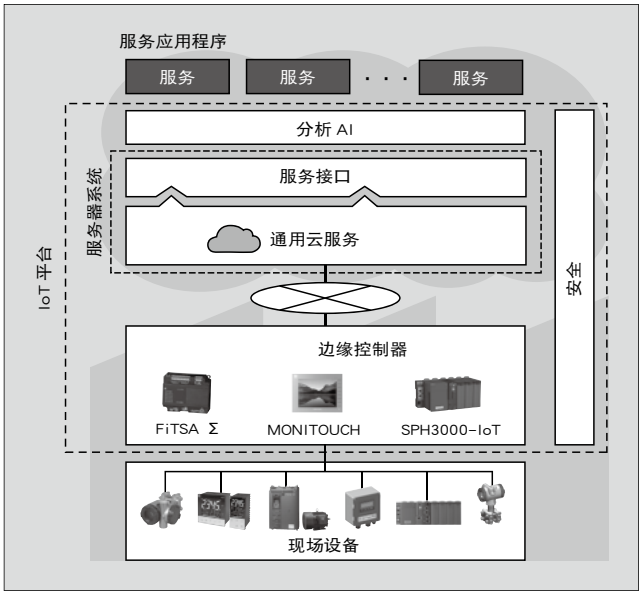

图 2　富士电机 IoT 平台的结构

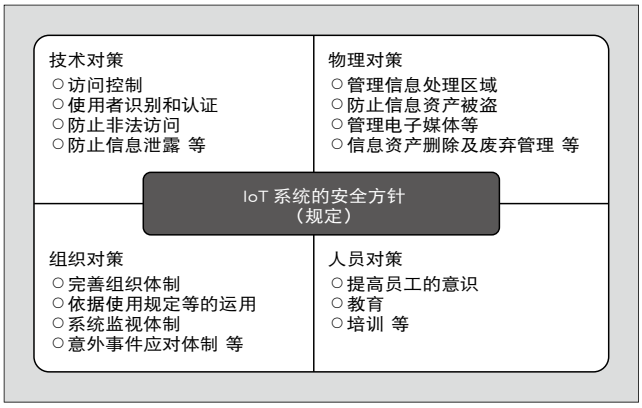

图 3　富士电机的 IoT 安全方针

4. 2　IoT 系统的安全方针

制定了 IoT 系统的安全相关公司内部基准。该基准的适用对象包括：IoT 事业中富士电机提供的 IoT 系统；开展 IoT 系统的开发、建立、运用、维护等事业所需的业务；这些业务中使用的电脑、电子存储媒体；操作这些电脑、电子存储媒体的所有员工。

制定这些基准时，参考了云安全标准规格 ISO/IEC 27017：2015[6]和 IoT 安全指南[3]等安全规格及指南的思考方式。

4. 3　技术及物理安全对策

(1)　通用云服务的对策

IoT 平台的服务器系统建立在外部的通用云服务上。该通用云服务在确认该安全对策情况的基础上进行选择和使用。具体而言，为了取得 ISO 27001 和 ISO 27017 认证，确保 CIA（Confidentiality：机密性、Integrity：完整性、Availability：可用性），而开展以下对策。

(a)　作为数据中心的对策

防止入侵、进出室管理、操作证据管理等

(b)　针对网络的对策

防火墙、检测入侵、通信加密、冗余化等

(c)　针对物理储存器及物理服务器的对策

访问限制、数据加密、防止病毒感染、操作证据管理、冗余化等

(d)　针对虚拟化基础的对策

利用网络虚拟化的分离、支持脆弱性信息、自动故障转移等

(2)　针对云端上的服务器系统及服务对策

富士电机开发的服务接口及分析 AI 等的 IoT 平台适用以下传统服务器及云端应用程序的安全对策。

(a)　避免过度设计脆弱性

依据安全软件开发指南等

(b)　防止非法访问

服务使用用户的识别及认证、访问控制、保护重要数据等

(3)　边缘控制器和通信对策

针对访问云端上 IoT 平台的边缘控制器，按如下方式进行识别、认证和通信加密，防止非法访问。

(a)　连接通信路径时的认证和加密

(b)　在与网络的连接点（防火墙、VPN 等）防止入侵

(c)　服务器系统与边缘控制器之间的相互认证

(d)　控制对服务器系统的访问

(e)　利用服务接口的数据发送源边缘控制器的设备认证

4. 4　组织及人员的安全对策

(1)　富士电机的风险管理体制

富士电机根据 2006 年 5 月制定的“富士电机风险管理规程”，有组织有体系地对风险进行管理。另外，作为风险管理的一个环节还开展信息安全对策（**图 4**）。

在推动信息安全的过程中，富士电机为了恰当保护机密信息及个人信息，完善并实施与信息安全相关的方针和规程类，每年对员工进行教育等，以加强信息安全，努力防止信息泄露。

需要使用顾客重要信息及个人信息，并进行高水平信息安全管理的部门已取得 ISMS（信息安全管理系统）认证及隐私保护标志认定等外部认证。

(2)　Fe-CSIRT

为了加强针对目标进行的网络攻击、对控制系统及 IoT 脆弱性的攻击等多样化高度化的安全威胁的应对和防卫能力，在 2017 年 4 月设置了 Fe-CSIRT（Computer Security Incident Response Team）。

作为富士电机 IT 战略部门的一个组织，在现有的信息安全管理体制中，与主导监视、稽核和教育等事务局联合，负责富士电机集团内发生的信息安全意外事件的应对和预防工作。

依据该 Fe-CSIRT 体制，针对 IoT 建立了应对意外事件的组织和运用体制。

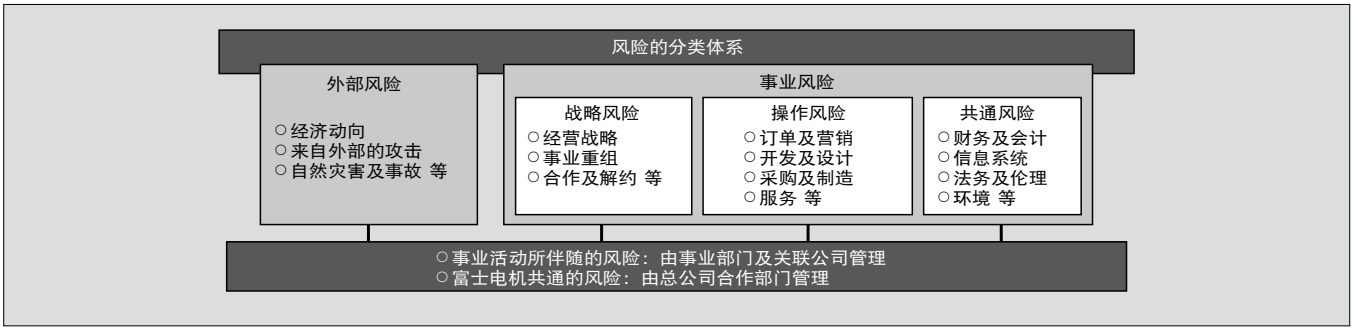

图 4　富士电机的风险分类体系和管理体制

5　后记

本文对 IoT 系统的安全进行了介绍。随着 IoT 设备的增加，网络攻击及安全意外事件激增。富士电机根据 IoT 系统面临的威胁制定了安全方针，从体制和机制两方面采取对策，建立了可安全安心利用的 IoT 系统。

网络攻击日益升级，因此在安全对策方面需要持续不断地采取措施。今后我们将继续推动可确保 IoT 系统安全的技术开发。

参考文献

⑴　平成 30 年版情報通信白書. 総務省.
⑵　ITU-T Y. 2060 (4000)，Overview Of Internet Of Things. 2012.
⑶　IoT セキュリティガイドライン Ver1.0. IoT 推進コンソーシアム・総務省・経済産業省 . 2016.
⑷　IoT 早期導入者のためのセキュリティガイダンス . Cloud Security Alliance. 2015.
⑸　IIC Security Framework. 2016.
⑹　ISO/IEC 27017：2015.

梅崎　一也
从事 IoT 系统相关安全技术的开发。现为富士电机株式会社技术开发本部创新创造中心数字平台开发室嵌入系统研究部主查。

富士电机

Fuji Electric

＊本刊记载的公司名称及产品，有可能是各相关公司的商标或注册商标。