METI
Ministry of Economy, Trade and Industry

Guidelines for Cyber/Physical Security Measures for Safe and Secure Smart Home

Cybersecurity Division

Ministry of Economy, Trade and Industry

(Reference) Further discussions based on CPSF

- Based on CPSF, some industry sectors are developing security guidelines for their own sectors to specify and implement security measures.
- In addition, cross-sectoral challenges including data management, software management, and IoT security safety are discussed.

Study Group on Group on Industrial Cybersecurity WG 1

Standard Model (CPSF)

Industry by Industry discussion

- **Building SWG**
  - Developed a guideline ver. 1.0
- **Electric Utility SWG**
  - Revising the existing guideline
- **Defense SWG**
- **Automotive SWG**
  - Developed a guideline ver. 1.0
- **Smart Home SWG**
  - Developed a guideline ver. 1.0
- **Space Industry SWG**
  - Launched in January 2021.
- ・・・

Cross-sectoral SWG

『3rd layer』TF : TF for ensuring the trustworthiness of『Connection in cyber space』

- Developing a model for comprehensive data management to ensure the trustworthiness of data

Software TF : TF for software management to ensure cyber-physical-security

- Developing a practice collection for OSS management, etc.

『2nd layer』TF : TF for ensuring the trustworthiness of『Connection between cyber and physical』

- Developed “IoT Security Safety Framework” for ensuring the trustworthiness between cyber space and physical space

Formulation of the cybersecurity guideline for smart home

- Smart home SWG, established Mar. 2018, formulated ”Guidelines for Cyber/Physical Security Measures for Safe and Secure Smart Home”, incorporating with comments from public consultation.
- Due to various stakeholders including ordinary people to security engineer, the guideline is organized hierarchically from simple guidance to concrete measures.

Guidelines for Cyber/Physical Security Measures for Safe and Secure Smart Home

1. Introduction

2. A Way of Thinking to Consider Security Measures

3. Security Threat in Smart Homes

4. The Minimum-Security Measures Required for Smart Home

4.1. (1) IoT device providers for smart homes
4.2. (2) Business operators responsible for remotely managing IoT devices for smart homes,
(5) Service providers of maintenance and support for smart homes
4.3. (3) Service providers for smart homes
4.4. (4) Business operators who deliver smart homes
4.5 (6) Management associations and management-entrusted companies of smart-homed condominium or housing complex、
(7) Owners and management-entrusted companies of smart-homed rental house
4.6 (8) Residents of smart homes

5. Closing Remarks

Appendix A: Functions/Assumed Incidents/Risk Sources/Measure Requirements for Stakeholders
Appendix B: Organization of Measures and Their Alignment with International and Other Standards
Appendix C: Correspondence Between the Guidance for Stakeholders and Measure Requirements
Appendix D: Instances of Cyberattack, Vulnerability, etc.
Appendix E: Glossary
Appendix F: References

Example of Security Measures: Simple to Detailed

<Chapter 4. The Minimum-Security Measures Required for Smart Home>

Simple Guide

4.1.(1) IoT device providers for smart homes

- Ensure security of IoT devices in the initial state
- Consider safety
- Provide any mechanism to update the software
- Provide information for users to guide usage and application environments of IoT devices to use them securely

<Appendix A Functions/Assumed Incidents/Risk Sources/Measure Requirements involved in "(1) IoT device providers for smart homes"> *example

Detailed

Functions	Assumed incidents	Risk Sources			Measure Requirement ID	Examples of Measure Requirements
		Threat	Vulnerability ID	Vulnerability		
・Read events in physical space, translate into digital information and send the data to cyberspace	・Unexpected behavior	・Unauthorized access to the inside of IoT devices by exploiting software and hardware vulnerabilities	MV.1	・Unused network ports and/or services remain enabled.	MO.1	・Physically or logically block unnecessary network ports, USBs and serial ports that currently have direct access to IoT devices and systems including such IoT devices.

<Appendix B>: Organization of Measures and Their Alignment with International and Other Standards

<Appendix C>: Correspondence Between the Guidance for Stakeholders and Measure Requirements