経済産業省

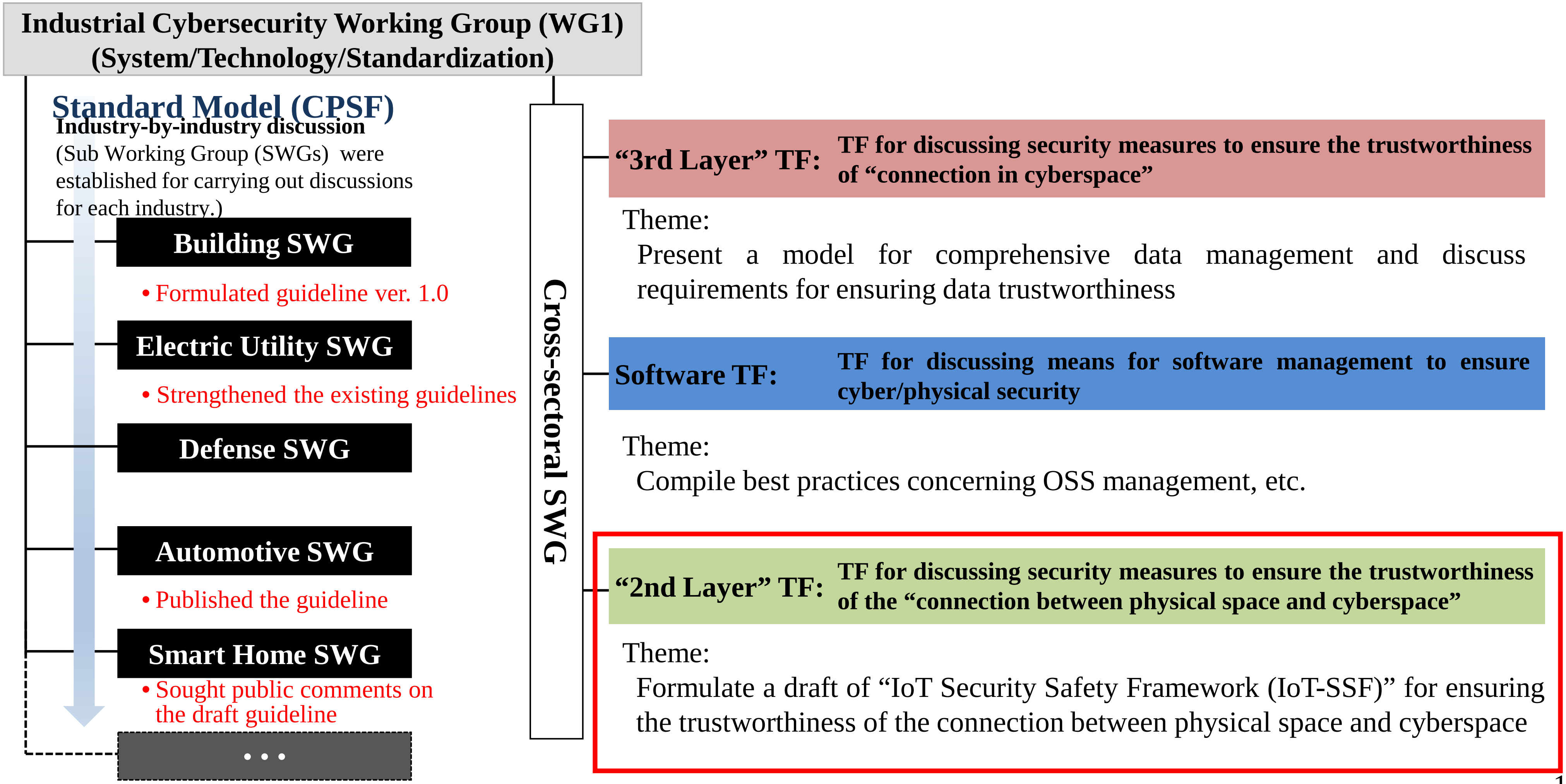
Outline of the IoT Security Safety Framework (IoT-SSF)

November 5, 2020

Cybersecurity Division,
Commerce and Information Policy Bureau,
Ministry of Economy, Trade and Industry

Status of Discussions by Theme-specific TFs

- In April 2019, **the Cyber/Physical Security Framework (CPSF)** was formulated.
- In order to promote specification and implementation of security measures based on the CPSF, **Task Forces (TFs)** focused on each theme **have held discussions**.



Industrial Cybersecurity Working Group (WG1) (System/Technology/Standardization)

Standard Model (CPSF)

Industry-by-industry discussion
(Sub Working Group (SWGs) were established for carrying out discussions for each industry.)

Building SWG
- Formulated guideline ver. 1.0

Electric Utility SWG
- Strengthened the existing guidelines

Defense SWG

Automotive SWG
- Published the guideline

Smart Home SWG
- Sought public comments on the draft guideline

• • •

Cross-sectoral SWG

"3rd Layer" TF: TF for discussing security measures to ensure the trustworthiness of "connection in cyberspace"

Theme:
Present a model for comprehensive data management and discuss requirements for ensuring data trustworthiness

Software TF: TF for discussing means for software management to ensure cyber/physical security

Theme:
Compile best practices concerning OSS management, etc.

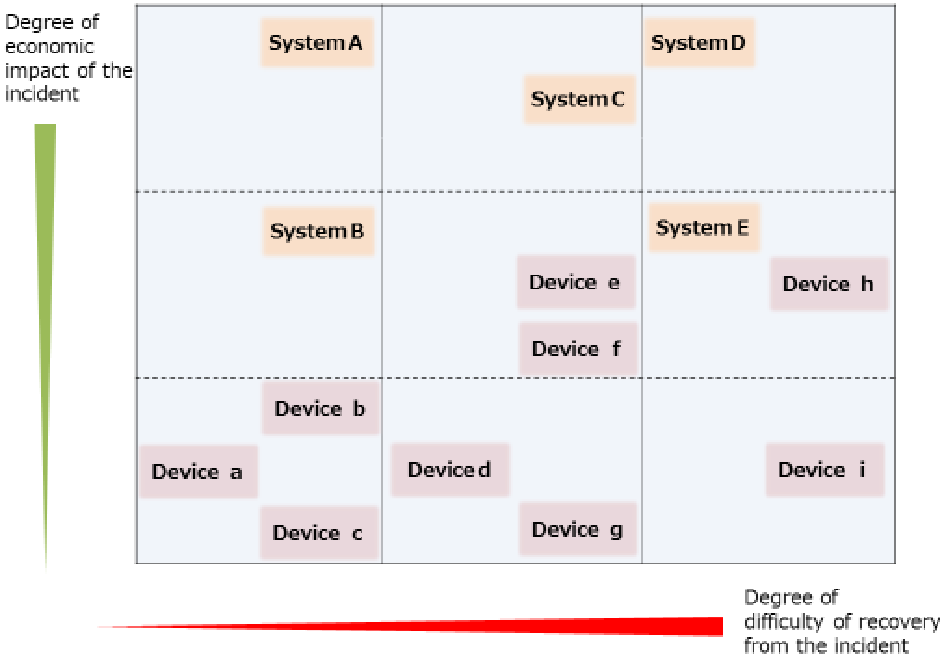
"2nd Layer" TF: TF for discussing security measures to ensure the trustworthiness of the "connection between physical space and cyberspace"

Theme:
Formulate a draft of "IoT Security Safety Framework (IoT-SSF)" for ensuring the trustworthiness of the connection between physical space and cyberspace

IoT Security Safety Framework (IoT-SSF)

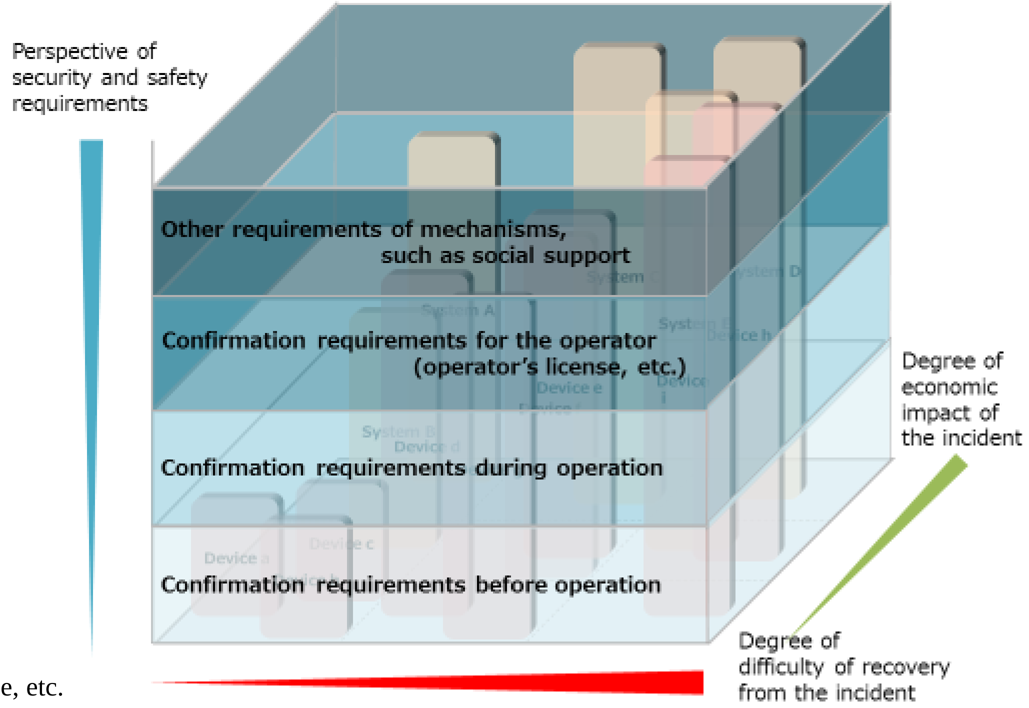
- In “Society 5.0” and “Connected Industries” where cyberspace and physical space are highly integrated, it is extremely important to secure the accurate conversion of information at the border between cyberspace and physical space, i.e., the accuracy of transcription and translation.
- Focusing on the fact that problems vary depending on the nature of IoT devices and systems and the usage environment, METI categorized IoT devices and systems depending on risks and formulated the IoT Security Safety Framework (IoT-SSF) that will contribute to the discussions on security safety requirements for each category.

Categorization of devices and systems connecting physical space and cyberspace (conceptual diagram)



* Mapping destinations of the same device or system may vary depending on the mode of use, etc.
(For example, “Device g” and “Device h” may be the same device but their mode of use differs.)

Perspectives of security safety requirements depending on categories (conceptual diagram)


Perspective of security and safety requirements
Other requirements of mechanisms, such as social support
Confirmation requirements for the operator (operator's license, etc.)
Confirmation requirements during operation
Confirmation requirements before operation
Degree of economic impact of the incident
Degree of difficulty of recovery from the incident

Public Comments on the Draft of “IoT Security Safety Framework (IoT-SSF)”

- METI sought public comments on the draft of **“IoT Security Safety Framework (IoT-SSF)”** from March 31 to June 24, 2020.
- The Framework also attracted attention from overseas, and METI sought public comments in English as well.
- **About 100 comments were received from 15 domestic and 10 overseas organizations and individuals.**

Major comments

(i) Comments on **the concept or scope of the IoT-SSF**

(ii) Comments on **the categorization of IoT devices and systems based on risks**

(iii) Comments on **perspectives of security safety requirements**

(iv) Comments on **specific implementation and requirements**

(v) Comments on **interoperability with other international standards and guidelines**

(vi) Comments on **definition of terms**

(vii) Comments on **future initiatives**