Cybersecurity Guidelines for Energy Resource Aggregation Business Ver 2.0

This English translation text is for reference only.

Please refer to the original Japanese text for the official version.

Formulated on Apr. 26, 2017

Revised on Nov. 29, 2017

Revised on Dec. 27, 2019

Agency for Natural Resources and Energy
IPA: Information-technology Promotion Agency, Japan

Table of Contents

1. Introduction

Since the Great East Japan Earthquake, the energy resource aggregation business (ERAB) is attracting attention as a new business area with the diffusion of distributed and consumer-side energy resources (e.g., solar power generation, stationary storage batteries, electric vehicles, ENE-FARM, and negawatts). In light of power system reform and the development of IoT, fostering the development of the aggregation business as a new energy industry is a key challenge to effectively use distributed and consumer-side devices in the overall energy system.

On November 26, 2015, at the Public-Private Dialogue for Future Investment, the Prime Minister's directive was issued to create a negawatt trading market by 2017, which enables the trading of an amount of electricity saved by utilizing solar power generation and IoT in households and, to this end, to establish trading rules between companies and communications standards for remote control of energy equipment by the end of FY 2016.

Accordingly, Japan is aiming to realize ERAB, which makes an integrated network of IoT-applied devices of consumers and other stakeholders to function as if it were a single power plant (Virtual Power Plant: VPP), and also to serve as the balancing capacity of the grid, through market and negotiated trading. In ERAB, aggregators will play a central role, and various services are expected to be provided through interconnection with various recipients, including electricity Transmission/Distribution Service Operator (TSO/DSO) businesses, electricity retailers, energy management companies operating Building Energy Management System (BEMS) and Home Energy Management System (HEMS), consumers, and renewable-energy utilities.

In addition, electricity TSO/DSO businesses and electricity retailers will be able to request that aggregators optimize the remote control of energy-creating devices/systems, energy-storing devices/systems, and load devices/systems of consumers and other stakeholders in a format supporting new forms of electricity trading, such as negawatt trading and turn-up DR. The ERAB system is the foundation necessary for this purpose.

In the ERAB system, various systems are operated by interconnection with each other via the Internet and other public networks, VPNs, leased lines, and other networks of various qualities. In particular, a major feature of the ERAB system is that energy devices, which have been so far used only within the respective consumers, are connected to external systems and networks.

In this context, there are concerns that any weak cybersecurity measures implemented by any of the companies may affect the use of electricity by consumers; therefore, the Agency for Natural Resources and Energy established a Cybersecurity WG as a subordinate body of the ERAB Study Group to specifically focus on cybersecurity in the ERAB study.

In its study, the Cybersecurity WG compared the added value obtained by aggregators from ERAB's

main service model with the threats and risks generated in the process of added value creation, and summarized the following four points:

First, the ERAB system is a cyber-physical system, which combines the physical and electrical characteristics with the cyber control of the devices operating the power system. The requirements for cybersecurity measures for cyber-physical systems differ significantly from those for typical IT systems, where it is necessary not only to protect information but also to ensure resilience of physical systems for continuous operation. For cyber-physical systems, the Ministry of Economy, Trade and Industry (METI) formulated the Cyber/Physical Security Framework[1] (CPSF) and proposed a three-layer structure approach to properly identify risk sources in entire supply chains and to present the security measures that should be considered without omissions.

- Third Layer (connections in cyberspace): Ensuring data reliability.
- Second Layer (connections between cyberspace and physical space): Ensuring the reliability of the function of accurate transcription between cyber/physical space.
- First Layer (connections between companies): Ensuring the trustworthiness of entities based on proper management.

Second, as the types and probability of occurrence of the threats and risks assumed in ERAB vary significantly, depending on the service model that may be adopted by aggregators, it is necessary for companies participating in ERAB (specifically, electricity TSO/DSO businesses, aggregation coordinators, resource aggregators, electricity retailers, and energy management companies [referring to renewable-energy utilities and manufacturers of devices and systems installed in consumers]) to conduct their own assessment of the threats and risks in an appropriate manner. There could be a model where electricity retailers even provide such services that would be offered by playing the role of an aggregation coordinator or resource aggregator, but in such a case, it is necessary to assess the threats and risks also from the standpoint of the aggregation coordinator or resource aggregator.

Third, companies participating in ERAB need to share the measures considered high priority based on the criteria of the impact on ERAB as a whole and the frequency of occurrence of threats and risks.

Fourth, when considering security measures, it is important to ensure that the measures are fully synchronized with other similar efforts, such as the IoT Security Guidelines (July 2016) jointly compiled by the IoT Acceleration Consortium, the Ministry of Economy, Trade and Industry, and the Ministry of Internal Affairs and Communications, in order to strengthen the effectiveness of the measures.

On April 26, 2017, the Cybersecurity Guidelines for ERAB Ver. 1.0 were developed for the purpose of describing the standard measure requirements to be addressed by companies participating

[1] https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

in ERAB. Subsequently, the Cybersecurity Guidelines for ERAB Ver. 1.1 were revised on November 29, 2017, to add cybersecurity measures in the ERAB system, assuming that a dispatch command is received from an electricity TSO/DSO business. On the recent assumption of the connection[2] of aggregation coordinator and resource aggregator systems to the systems (simplified signal dispatching systems) of electricity TSO/DSO businesses, the Cybersecurity Guidelines for ERAB Ver. 2.0 (hereinafter referred to as ERAB Cybersecurity Guidelines 2.0)are revised to add the cybersecurity measures required for ERAB systems and companies participating in ERAB.

[2] The systems that will be interconnected with the systems of electricity TSO/DSO businesses are the systems owned by aggregation coordinators.

2. Position of the Guidelines

ERAB Cybersecurity Guidelines 2.0 provide the minimum requirements for security measures to be implemented by companies participating in ERAB in order to maintain the service level of ERAB based on the approach of the Power Control System Security Guidelines[3] and the *Guide to Security Design in IoT Development*.[4] Therefore, companies participating in ERAB shall, on their own responsibility, implement security measures based on ERAB Cybersecurity Guidelines 2.0 and other guidelines.

For the purposes of ERAB Cybersecurity Guidelines 2.0 , the term “mandatories” is defined as mandatory actions to be imposed on companies participating in ERAB to implement under these Guidelines. On the other hand, the term “recommendations” is defined as suggested actions to be considered by companies participating in ERAB to implement on their own responsibility under these Guidelines.

3. ERAB system

3.1. ERAB system configuration

The ERAB system consists of electricity transmission/distribution service operation business and systems (simplified signal dispatching system), electricity retailer systems, aggregation coordinator systems, resource aggregator systems, energy management systems of HEMSs and BEMSs,[5] gateways (GW)[6] between energy devices and external systems, and energy devices subject to ERAB control.

Figure 1 shows the components and interfaces of the ERAB system. In this model, a combination of GWs and controllers collects data from on-site devices and sends it to the head-end system. A head-end system, including cloud services, manages GWs and controllers and provides services based on the received data. The interfaces are between the simplified signal dispatching system and the aggregation coordinator (R1), between the electricity retailer and the aggregation coordinator or resource aggregator (R2), between the aggregation coordinator and the resource aggregator (R3), and between the resource aggregator and the GW or energy management system, such as BEMS and HEMS (R4).

---

[3] Japan Electric Association Information Subcommittee publication *Power Control System Security Guidelines*, Japan Electric Association, which are applicable to the Japan Electrotechnical Standards and Codes Committee Standards (JESC Standards) established by the Japan Electrotechnical Standards and Codes Committee (JESC: Japan Electrotechnical Standards and Codes Committee)

[4] Information-technology Promotion Agency, Technology Headquarters Security Center *Guide to Security Design in IoT Development*, Information-technology Promotion Agency, Japan (IPA)

[5] Resource aggregators’ systems and energy management systems, such as HEMSs and BEMSs, may be integrated.

[6] In the definition of HEMS by the Japan Electrical Manufacturers' Association, it has a service coordination function and a controller function.

The connection point for R4 is defined by the Japan Electrical Manufacturers' Association[7] to be installed by the service coordination function of the energy management system on the server or in a HAN (Home Area Network) where energy devices to be controlled by ERAB are placed as the case .

Furthermore, energy devices subject to ERAB control to be installed on the consumer side have an interface (R5) between energy devices subject to ERAB the consumer side under the GW. There may be the following two use cases for these energy devices: 1) devices directly connected to the ERAB system via the GW, and 2) devices connected to the ERAB system through an EMS controller, such as the HEMS controller.

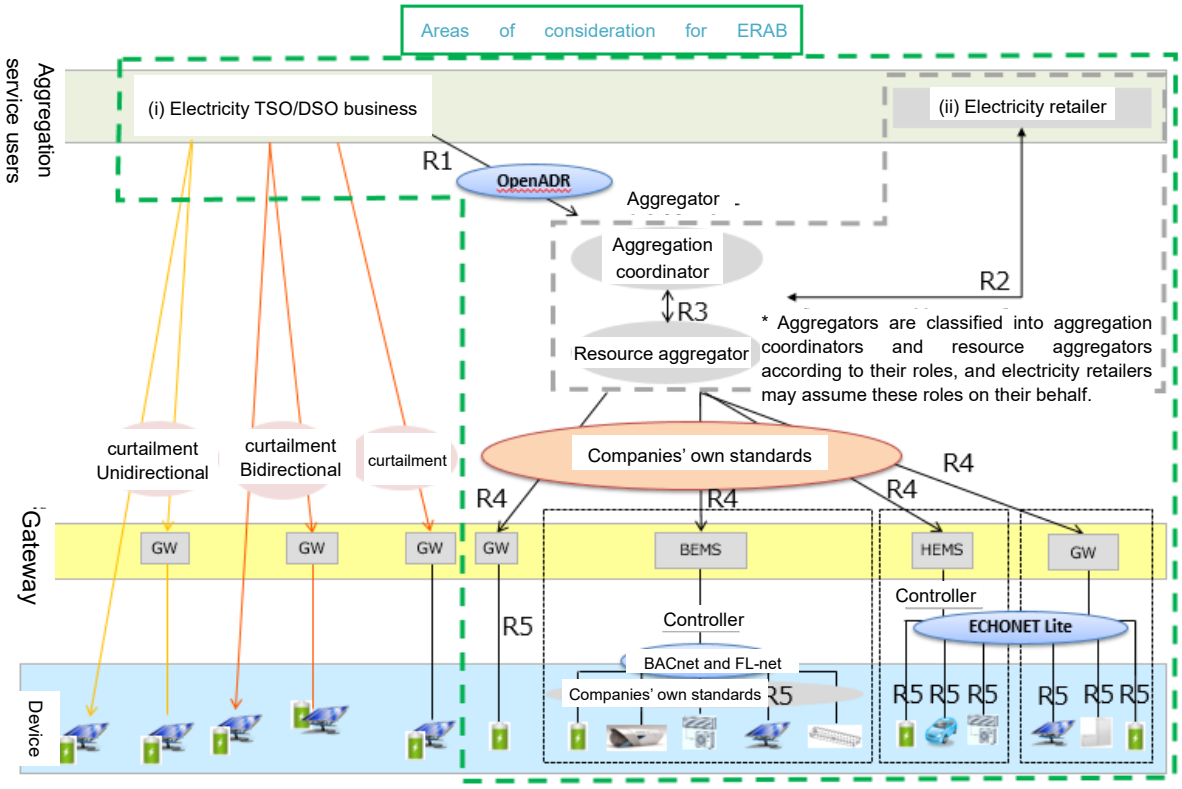

Figure 1. Overview for the ERAB system

3.2. Basic policy to note for the ERAB system

[Mandatories]

- Each company participating in ERAB shall provide[8] information about vulnerability and its countermeasures with users.
- Each company participating in ERAB shall determine its approach for sharing vulnerability

[7] Japan Electrical Manufacturers' Association, HEMS Technical Committee "Definition of HEMS in Cooperation with External Systems," a material presented at the ERAB Study Group on September 14, 2016.

[8] The method of notification shall be based on the specific measure requirements of each company participating in ERAB.

countermeasure information and threat information and shall provide cooperation in this approach.[9]

[Recommendations]

- The ERAB system should be designed with attention to three requirements:[10] the confidentiality, integrity, and availability of the hardware handled by the system and the data held by the hardware.

3.3. Threats to be assumed by the ERAB system

[Recommendations]

- The ERAB system should pursue the study of measures based on the following perspectives:
  - Assuming a targeted attack,
  - Obtaining system logs for incident detection,
  - Not standing on the idea that a closed network is safe, and
  - Continuing to improve security measures, as a complete secure state is never achieved.

Sensors and energy devices are assumed to be devices at the R5 interface. For example, there are reported use cases, such as direct communication with energy devices and sensors located under the GW located at the boundary of the external and internal networks, and indirect communication via the BEMS/HEMS controller. In these use cases, the following threats are discussed, and the security of the ERAB system is required to function as the security of IoT system in order to address these threats:

- An attacker sends unauthorized data to BEMS/HEMS controllers, devices, and sensors located at the endpoints over the GW via the network, causing them to malfunction, to stop functioning, or to be unable to obtain data.
- Internal data tampering and theft attacks occur on energy devices and sensors located at the endpoints.
- Unauthorized modification of energy devices and sensors causes malfunctions and cessation of functioning.
- The processing load is increased by sending data from hijacked sensors and energy devices to the servers that make up the ERAB system, resulting in the suspension of all ERAB services.
- An attacker hijacks energy devices and sensors and makes them complicit in a DoS attack on

[9] Information-technology Promotion Agency, Japan (IPA) has publicly released the vulnerability countermeasure information, including that of IoT systems, along with the database and its usage functions (e.g., a function to retrieve all applicable vulnerabilities by product name or version), as the Vulnerability Countermeasure Information Database JVN iPedia (https://jvndb.jvn.jp/), which can be used by companies participating in the ERAB project as one of the means to disseminate vulnerability information.

[10] The *General Framework for Secure IoT Systems* (August 26, 2016) set out by the National Information Security Center states that the confidentiality, integrity, availability, and security shall be ensured. ERAB Cybersecurity Guidelines 2.0 are based on the basic principles of the General Framework.

external systems via the GW.

- The destruction or shutdown of systems results in the interruption of the ERAB services and triggers actions that endanger human life.

3.4. Service levels to be maintained by the ERAB system

[Mandatories]

- In the ERAB system, the simplified signal dispatching systems of electricity TSO/DSO businesses and the systems owned by aggregation coordinators are interconnected. Attention should be paid to managing the risk of cyberattacks and other influences spreading over the grid network.

Under such circumstances, the respective companies and their owned systems are required to ensure the service levels as defined below:

- A service level in accordance with the requirements of the capacity, supply and demand balancing, and other markets
- Companies owning simplified signal dispatching systems and their systems: A service level in accordance with the Power Control System Security Guidelines[11]
- Aggregation coordinators and their systems: A service level in accordance with ERAB Cybersecurity Guidelines 2.0,[12] as well as a service level in accordance with the Power Control System Security Guidelines at the direct connections with a simplified signal dispatching system,[13] and a service level in compliance with the security measures with requirements separately defined by electricity TSO/DSO businesses operating the simplified signal dispatching system under the Power Control System Security Guidelines and ERAB Cybersecurity Guidelines 2.0
- Resource aggregators and their systems: When connecting to aggregation coordinators, a service level in accordance with ERAB Cybersecurity Guidelines 2.0,[14] as well as a service level in compliance with the security measures with requirements separately defined by aggregation coordinators under these Guidelines

---

[11] The 9th ERAB Study Group *Cybersecurity WG Report*, Agency for Natural Resources and Energy, 2019

[12] The 9th ERAB Study Group *Cybersecurity WG Report*, Agency for Natural Resources and Energy, 2019

[13] An aggregation coordinator may design a logical or physical separation of direct connections to a simplified signal dispatching system and any other parts in the same system. When a separation design is difficult, the whole of the aggregation coordinator's system must comply with the Power Control System Security Guidelines, and a service level in compliance with the security measures with requirements separately defined by electricity TSO/DSO businesses operating the simplified signal dispatching system under the Power Control System Security Guidelines and ERAB Cybersecurity Guidelines 2.0 must be ensured.

[14] The 9th ERAB Study Group *Cybersecurity WG Report*, Agency for Natural Resources and Energy, 2019

3.5. Classification of system criticality in the ERAB system

[Mandatories]

- In ERAB Cybersecurity Guidelines 2.0, the system criticality is defined based on the Power Control System Security Guidelines as shown below. Companies participating in ERAB shall classify their own systems based on the following definitions.

Criticality A refers to systems that are considered to have a relatively large impact on the stable supply of electricity.

Criticality B refers to systems with limited impact on the stable supply of electricity.

Target systems by level of criticality

Criticality	Target systems
A	Systems with a controlled electricity demand at a scale of 500,000 kW or more
B	Systems with a controlled electricity demand at a scale of less than 500,000 kW

3.6. Cybersecurity measures in the ERAB system

[Mandatories]

- Companies participating in ERAB shall take the following steps in the ERAB system:

Step 1: Clarify the overall configuration of the target IoT products and service systems and the demarcation points of responsibility.

Step 2: Clarify the information, functions, and assets to be protected in the system.

Step 3: Identify possible threats to the information, functions, and assets to be protected.

Step 4: Identify candidate measures (best practices) to counter threats.

Step 5: Select which measures to implement, considering the threat level, damage level, and cost.

Step 6: Verify the implementation, focusing on the items specified in the mandatories, by means of third-party audits (including certification) and educational programs.

Step 7: Conduct design, operation, and training for response procedures in the event of an accident.

- In the event of being unable to check the implementation by an interconnection partner of the mandatories of ERAB Cybersecurity Guidelines 2.0,[15] companies participating in ERAB shall promptly suspend the interconnection between the relevant systems with the aim of minimizing security damage to the entire ERAB system. [Suspension of interconnection]

[15] The check method is a relative check conducted by each company based on the specific measure requirements. Continued discussions will be held on how to handle disputes.

- Measures shall be implemented assuming the threat and risk of unauthorized control or loss of control of energy devices on the consumer side as a result of spoofing by malicious attackers issuing unintended commands. [Anti-Spoofing Measures]
- Measures shall be implemented assuming the threat and risk of unauthorized control of energy devices on the consumer side as a result of falsification of information by malicious attackers using interception and man in the middle attacks on communication devices or communication channels. [Measures against falsification of data]
- The system shall apply security patches to address vulnerabilities, and measures against malware shall be implemented on the devices and external storage media comprising the system. In addition to properly assigning administrative privileges in the system, a mechanism must be put in place to prevent unauthorized actions and program execution and to prevent processes from running, if not intended by the original operation. The devices and external storage media comprising the system and the data to be handled shall be understood, properly managed, and protected. [Measures against malware]

ERAB Cybersecurity Guidelines 2.0required the implementation of measures in Sections 3.6.1 through 3.6.5 by interface in the ERAB system, in addition to the existing general measures for system security.

3.6.1. Aggregation coordinators' systems and R1 (interface between simplified signal dispatching system and aggregation coordinator)

[Mandatories]

(Measures for companies and their systems)

- Aggregation coordinators shall be responsible to electricity TSO/DSO businesses for ensuring the service quality, including their own security and the security of their resource aggregators, when entering into a balancing capacity contract with electricity TSO/DSO businesses.
- The direct connections with an aggregation coordinator's simplified signal dispatching system shall comply with the Power Control System Security Guidelines and the interconnection security requirements separately specified by electricity TSO/DSO businesses operating the simplified signal dispatching system under the Power Control System Security Guidelines and ERAB Cybersecurity Guidelines 2.0.

(Measures for interface)

- Authentication shall be implemented at the points of interconnection with external systems and communication messages shall be protected by encryption.
- The direct connections with an aggregation coordinator's simplified signal dispatching system shall be, in principle, separated from the network accessible by an unspecified number of people.

- At the direct connections with an aggregation coordinator's simplified signal dispatching system, connection points with other networks shall be minimized and protective measures shall be applied to the connection points.

3.6.2. R2 (interface between electricity retailer and aggregation coordinator or resource aggregator)

[Mandatories]

(Measures for interface)

- Authentication shall be implemented at the points of interconnection with external systems and communication messages shall be protected by encryption .
- Aggregation coordinators or resource aggregators shall, when making connections to electricity retailers' systems, require electricity retailers to ensure that their systems comply with ERAB Cybersecurity Guidelines 2.0.[16] Also, they shall require the retailers to establish and comply with security measures with requirements separately defined under these Guidelines.

3.6.3. Resource aggregators' systems and R3 (interface between aggregation coordinator and resource aggregator)

[Mandatories]

(Measures for companies and their systems)

- Resource aggregators and their own systems are required to comply with ERAB Cybersecurity Guidelines 2.0 when making connections to aggregation coordinators,[17] as well as security measures with requirements separately defined by aggregation coordinators under these Guidelines.

(Measures for interface)

- Authentication shall be implemented at the points of interconnection with external systems and communication messages shall be protected by encryption. .

3.6.4. R4 (interface between resource aggregator and GW or energy management system such as BEMS and HEMS)

[Mandatories]

(Measures for companies and their systems)

- Resource aggregators' devices subject to control or energy management systems, such as BEMS and HEMS, are required to comply with ERAB Cybersecurity Guidelines 2.0 when connecting

[16] The 9th ERAB Study Group *Cybersecurity WG Report*, Agency for Natural Resources and Energy, 2019

[17] Same as footnote 16

to aggregation coordinators,[18] as well as security measures with requirements separately defined by aggregation coordinators under these Guidelines.

* ERAB Cybersecurity Guidelines 2.0 assume that a public network is used as a communication channel[19] between a resource aggregator or a BEMS/HEMS server and a GW. When networks with secure and reliable end-to-end transmission lines are used, it is considered that companies may be given a certain degree of discretion regarding the strength of measures, subject to security guarantees.

(Measures for interface)

- Authentication shall be implemented at the points of interconnection with external systems and communication messages shall be protected by encryption.

3.6.5. R5 (interface between energy devices subject to ERAB control to be installed on the consumer side under the GW[20])

[Recommendations]

(Measures for companies and their systems)

- Energy devices and sensos subject to ERAB control, some of which are resource-constrained devices, include existing systems and other devices where it is difficult to add or update security functions. Measures shall be implemented in reference to the *Guide to Security Design in IoT Development*[21] and the Product-Specific Security Guidelines IoT-GW Edition.[22]

(Measures for interface)

- Authentication shall be implemented at the points of interconnection with external systems and communication messages shall be protected by encryption..

3.7. Design of ERAB systems based on differences in information handled

[Mandatories]

- Companies participating in ERAB shall clarify the differences in information handled and design a system that matches the results.

---

[18] Same as footnote 17.

[19] In the definition of "HEMS" by the Japan Electrical Manufacturers' Association, it is a communication channel between an aggregator and the service coordination function of an energy management system, and between the service coordination function of an energy management system (if on a server) and the EMS controller function.

[20] Specifically, "between the GW located at the boundary of the external and the internal networks and the devices and sensors located at the endpoints" and "between the BEMS/HEMS controller (located on the endpoint side of the GW or having GW functions) and the devices and sensors under the controller."

[21] IPA Technology Headquarters Security Center *Guide to Security Design in IoT Development*, Information-technology Promotion Agency, Japan (IPA)

[22] CCDS Security Guidelines WG Home GW SWG *Security Guidelines for Product Categories - IoT GW* -, Connected Consumer Device Security Council [CCDS]

ERAB systems have very different characteristics in terms of their assumed threats and risks, depending on the added value created by aggregators.

Therefore, as a precondition for establishing a framework for security measures for ERAB systems, it is appropriate to set minimum service levels assumed at present, to be met by companies participating in ERAB, and to apply security measures to achieve these service levels. For example, an aggregator designing services similar to IoT services using sensor data and an aggregator designing service development using personal information require different measures.

3.7.1. Companies designing services similar to IoT services using sensor data

[Mandatories]

- There is a need for measures against threats and risks of interception and falsification of data held. For information other than personal information, there is no explicit obligation imposed by law for its proper management. However, in light of the General Framework for Secure IoT Systems of the National center of Incident readiness and Strategy for Cybersecurity, it should be taken for granted that companies must properly manage the information held, even if it is not personal information. The Framework states that, as a requirement for ensuring security for IoT systems and connections between IoT systems, it is necessary to define requirements at each stage of basic policy establishment, risk assessment, system design, system construction, and operation and maintenance, with clarification as follows:
  - Clarify the definition of IoT systems, including scope and target, once again, and since IoT systems are diverse, classify the systems based on their properties in light of the risks and clarify the responses accordingly.
  - Clarify the requirements necessary to ensure the confidentiality, integrity, and availability of information for IoT systems and to ensure the security of users in the operation of things.
  - Clarify the requirements necessary to ensure reliable operation and rapid service recovery in the event of failure, including the establishment of functional guarantees.
  - Then, clarify the security level (legal and customary requirements) required for connected things and the network used.
  - Clarify that each of the confidentiality, integrity, availability, and security shall be ensured even in the event of the malfunction of connected things and network or cyberattacks and that rapid service recovery shall be done in the event of failure.
  - Clarify how data should be handled, including discussions on the demarcation points of responsibility and ownership of information related to IoT systems.

3.7.2. Companies designing service development using personal information

[Mandatories]

- In addition to measures against threats and risks of interception and falsification of data held, if the system handles personal information, measures shall be implemented in accordance with the Personal Information Protection Act.
- With respect to personal information held by companies participating in ERAB, companies are required to maintain a service level for proper management of personal information by imposing the duty to take security control action[23] for personal data under the Personal Information Protection Act. Furthermore, as for specific measures to be implemented by companies to maintain a service level for proper management of personal information, there are the Guidelines on the Act on the Protection of Personal Information (Volume on General Rules) and another three volumes[24] established by the Personal Information Protection Commission under the Personal Information Protection Act,[25] and the Responses to Personal Data Leakage. Companies participating in ERAB shall implement measures in accordance with the Guidelines on the Act on the Protection of Personal Information (Volume on General Rules) and another three volumes and the Responses to Personal Data Leakage, and other voluntary necessary measures in reference to the respective guidelines.

3.8. Design of specific measure requirements based on standard measure requirements

[Mandatories]

- Companies participating in ERAB shall, on their own responsibility, develop specific cybersecurity measures to withstand actual operation, based on the approach of standard measure requirements.

ERAB Cybersecurity Guidelines 2.0 provide the Standard measure requirements. Considering the need to continuously improve measures on the assumption that accidents may happen, the Standard measure requirements specify the basic approach for working on security measures for the ERAB system, and the purpose and approach for implementing the respective security management requirements and describe the minimal security measures to be implemented by companies to maintain the service level of the ERAB system.

The Specific measure requirements apply when companies participating in ERAB develop, on their

[23] As provided for in Article 20 of the Personal Information Protection Act.

[24] Other three volumes are: Volume on Provision to a Third Party in a Foreign Country, Volume on Confirmation and Record-Keeping Obligations upon Third-Party Provision, and Volume on Anonymously Processed Information.

[25] As provided for in Article 8 of the Personal Information Protection Act.

own responsibility, specific measures to be implemented based on the approach of the Standard measure requirements to withstand actual operation. Specifically, based on the threats assumed for each component of the ERAB system and the correlation between such threats and business risks, examples of measures against such threats shall be studied in detail and specified for each of the following phases: (i) deterrence, (ii) internal defense and information protection, (iii) intrusion and attack detection, and (iv) damage assessment and business continuation. In addition to the above, measures for specific themes related to the ERAB system shall be specified, such as measures against targeted attacks and measures against a combination of cyber and physical attacks, other than measures to be implemented for each component.

The design of the Specific measure requirements shall be in accordance with the *Guide to Security Design in IoT Development*[26] published by the Information-technology Promotion Agency, Japan (IPA) Technology Headquarters Security Center, and the Power Control System Security Guidelines established by the Japan Electrotechnical Standards and Codes Committee (JESC), in addition to these Guidelines.

Table 1. Standard measure requirements and specific measure requirements

The Standard measure requirements * Corresponding to ERAB Cybersecurity Guidelines 2.0	・ Specifying the basic approach for working on security measures for the ERAB system, and the purpose and approach for implementing the respective security management requirements, considering the need to continuously improve measures on the assumption that accidents may happen, standard measure requirements. ・ Specifying the minimum security measures to be implemented by companies to maintain the service level of the ERAB system.
The Specific measure requirements	・ Specific measures developed by companies participating in ERAB on their own responsibility, which shall be implemented based on the approach of the Standard measure requirements to withstand actual operation. ・ Specifically, based on the threats assumed for each component of the ERAB system and the correlation between such threats and business risks, specifying measures against such threats for each of the following phases: (i) deterrence, (ii) internal defense and information protection, (iii) intrusion and attack detection, and (iv)

[26] IPA Technology Headquarters Security Center *Guide to Security Design in IoT Development*, Information-technology Promotion Agency, Japan (IPA)

	damage assessment and business continuation, as well as measures against targeted attacks and measures against a combination of cyber and physical attacks.

3.9. Continuous improvement of guidelines

[Mandatories]

- Companies participating in ERAB shall regularly check and update the Specific measure requirements.
- Companies participating in ERAB shall update the Specific measure requirements as needed, when vulnerabilities become apparent, or otherwise immediate measures are required.

It is important to continuously update the Standard measure requirements and specific measure requirements in response to social changes and occurrence of security incidents and to improve them to the level of measures ultimately required by companies participating in the ERAB.

In particular, since the Specific measure requirements specify examples of specific measures to be implemented based on the approach of the Standard measure requirements, it is considered that the frequency of required updates is higher compared to the Standard measure requirements specifying general security management requirements.

The update frequency of the Standard and the Specific measure requirements should be determined primarily by the organization responsible for updates, but at least the Specific measure requirements need to be checked and updated on a regular basis. urgent measure requirements shall be updated as needed, when vulnerabilities become apparent, or otherwise immediate measures are required. Since the Standard and the Specific measure requirements are interlinked, it is important that when one is reviewed, the other should be appropriately addressed if it is determined that a review of the other is necessary.

4. Recommended approach to measures in companies in accordance with ERAB Cybersecurity Guidelines 2.0

4.1. Continuous implementation of security measures with the PDCA cycle by companies participating in ERAB

[Mandatories]

- Companies participating in ERAB shall, under the responsibility of their management, clarify the current status of their security measures and their ultimately intended security measures and then consider specific measure requirements and the process to implement them.
- The security measures shall be verified and improved through the PDCA cycle ((i) establishment

of security measures, (ii) implementation of security measures, (iii) assessment of security measures, and (iv) establishment and implementation of appropriate improvement measures), and companies participating in ERAB shall, on their own responsibility, voluntarily and continuously implement security measures, aiming for even higher levels.

- The personnel responsible for security management shall be designated and a collaborative framework for sharing information among such personnel shall be constructed.
- Roles for security purposes shall be clarified in companies and for customers and other stakeholders.
- Security-related information shall be documented and controlled.
- Matters to be reported on the implementation status of security measures shall be determined and reported in a timely manner.
- Security education and training shall be planned and conducted in a timely manner, so that appropriate security measures can be implemented. Also, effectiveness of security education and training shall be confirmed.
- Companies participating in ERAB shall establish an organization responsible for security management as a responsible body for promoting security management and building security governance and create an operation and management system that follows the PDCA cycle under the management of this organization.
- Since there is no upper bound on how far security measures should be implemented, measures shall be evaluated taking into account the cost of implementation and shall be implemented to the extent necessary and sufficient without an excessive investment.

4.1.1. Establishment and implementation of security measures in companies participating in ERAB

[Mandatories]

- Companies participating in ERAB shall properly establish measures to be complied with by their ERAB system, beyond the requirements specified in ERAB Cybersecurity Guidelines 2.0.

Companies participating in ERAB shall, when establishing security measures for the ERAB system, properly establish measures to be complied with by their ERAB system, beyond the requirements specified in ERAB Cybersecurity Guidelines 2.0, after assessing business risks appropriately, since the risks that may occur and the acceptable risks are considered to be different for each company.

4.1.2. Verification and improvement of security measures in companies participating in ERAB

[Mandatories]

- Companies participating in ERAB shall build ERAB systems based on security measures and evaluate and improve the implementation status of security measures.

Companies participating in ERAB shall build an ERAB system based on the security measures established on their own and improve their own security measures by evaluating the implementation status and the effectiveness of the security measures.

4.1.3. Third-party certification of security measures in companies participating in ERAB

[Recommendations]

- Companies participating in ERAB should conduct an internal audit of a certain level of quality to ensure security measures.

For systems classified as Criticality A in Section 3.5 (Classification of system criticality in the ERAB system), the implementation of third-party certification is strongly suggested, considering their impact on the stable supply of electricity.

The international standards[27] serve as a reference when companies participating in ERAB implement and improve security measures based on the PDCA cycle described in Section 4.1 (Continuous implementation of security measures with the PDCA cycle by companies participating in ERAB).

It is desirable that internal audits should be conducted to evaluate the implementation status of security measures under ERAB Cybersecurity Guidelines 2.0 and external audits by a third party in accordance with international standards,[28] in addition to internal audits, should be conducted to evaluate the effectiveness of the security measures. Conducting audits by an external organization is expected to further enhance the effectiveness of continuous improvement of security measures.

4.1.4. Monitoring and response systems in companies

[Mandatories]

- Companies participating in ERAB shall share and manage vulnerability-related information among companies, system builders, organizations responsible for coordination between companies, and organizations responsible for analysis of vulnerability-related information.
  * The Information-technology Promotion Agency, Japan (IPA) has publicly released the vulnerability countermeasure information in IoT systems, along with the database and its usage

[27] Examples of international standards: CC (ISO/IEC 15408), CSMS (IEC 62443-2), ISMS (ISO/IEC 27001), and ISO/IEC 27017 for cloud use

[28] Same as footnote 27.

functions (e.g., a function to retrieve all applicable vulnerabilities by product name or version), as the Vulnerability Countermeasure Information Database JVN iPedia,[29] which can be used by companies participating in ERAB as one of the means to disseminate vulnerability information.

- Based on the assumption of creating an operation and management system that follows the PDCA cycle, a system capable of monitoring system status and responding to incidents shall be created.
  * When creating a management system, an example of security operation system in a smart meter system (Table 2) can be used as a reference.
- Considering the damage in the event of an incident, a response and response system shall be created to minimize the anomalies of the incident, so that the incident does not develop into a larger accident.
- On the assumption that incident response is achieved not only by creating a system, but an accident may actually occur, a contingency plan in case of emergency shall be developed to respond to actual situation.
- Drills based on a contingency plan in case of emergency shall be conducted on a continuing basis.

[Recommendations]

- The monitoring of the system status shall be conducted to detect system anomalies and to identify the cause of the anomalies when occurred by selecting logs to be collected and analyzing them constantly.
- As for the system related facilities and systems to be installed in the facilities, security compartments to be protected shall be clearly defined and properly protected, and access control shall be implemented to ensure that only authorized persons have access. Security specifications shall be clarified at the time of system procurement, and compliance shall be confirmed at the time of design and manufacturing, and security measures shall be reconstructed when specifications are changed.

[29] https://jvndb.jvn.jp/

Table 2. Example of security operation system in a smart meter system (reference)[30]

Function name	Normal time response	Emergency response
Security control	(i) Control of company-wide security initiatives (planning, implementation, and management of risk assessments and penetration tests) (ii) Provision of information on security to management and relevant departments	(i) Provision of information on security incidents to management and relevant departments (ii) Explanation to external stakeholders, such as government agencies, and provision of information to internal public relations departments
Security accident response	(i) Development of a contingency plan in case of emergency and the conduct of drills (ii) Provision, receipt, and analysis of attack information (iii) Performance of cross-sectional analysis of security-related logs	(i) Secondary response and support to incidents (ii) Procurement of external resources for incident investigation (as needed) (iii) Analysis of incidents and preparation of reports
Security surveillance	(i) Operating instruction to the operational monitoring function and management of operational results (ii) Routine analysis of security-related logs	(i) Primary response to incidents, communicated from the operational monitoring function (ii) Emergency operating instructions to the operational monitoring function and management of operational results involving incidents
Operation monitoring	(i) System monitoring (performance monitoring, life-and-death monitoring, and event monitoring) (ii) Notification to the security monitoring at the time of incident detection (iii) Normal system operations	(i) Performance of response operations as instructed by the security monitoring function (ii) Collection of logs required for incident response (as needed)

[30] Described based on the Smart Meter System Study Group Security Study Working Group Report Appendix "Items to be Included in Standard Measure Requirements of the Unified Guidelines."