# Guidelines for ensuring safety with the IoT connection of electrical and gas appliances

**April, 2021**
**Ministry of Economy, Trade and Industry**

# Guidelines for ensuring safety with the IoT connection of electrical and gas appliances

## CONTENTS

## 1. Background of these guidelines

- Today, the Internet is widely used, and Japan is aiming for Society 5.0. In the midst of this trend, not only smartphones and PCs but also electrical and gas appliances are already expected to be conveniently used through Internet connections.
- For example, it is expected that appliances subject to the four Product Safety Acts [1] will be linked with new services to provide novel benefits to users, such as remote operation of electrical appliances through the voice assist function of smart speakers.
- On the other hand, there are concerns about cyberattacks on the vulnerabilities of these ordinary electrical appliances, and it is assumed that communication and service infrastructures will be illegally accessed.
- In this context, it is necessary to take measures to ensure the safety of electrical appliances and other products not only in the case of mis-operation but also communication fault and cyberattacks, with regards to the risks assumed when they are used in the Internet environment.
- From this perspective, we held the 'Study Group on ensuring safety with the Internet of Things (IoT) connection of electrical and gas appliances', to summarise how to ensure the safety with IoT connection of electrical and gas appliances. The details are provided in the attached report, 'FY2020 Project for Research and Development of Technical Standards for Industrial Safety and Security (Survey on trends in safety assurance with the IoT connection of electrical and gas appliances)'[2].
- These guidelines are intended to be publicised to the relevant industry groups and calls for necessary measures to be taken.
- In addition to international standards such as IEC 60335-1:2020 (Household and similar electrical appliances - Safety - Part 1: General requirements), ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements) and so on, the situation in Europe and the United States was also referred to in preparing these guidelines.
- As cyber security measures, it is necessary to take measures for the fundamental safety[3] of appliances, in addition to supply chain measures related to the IoT system against cyberattacks that are becoming more

---

[1] Consumer product safety act, Electrical appliance and material safety act, the Act on the securing of safety and the optimisation of transactions of liquefied petroleum gas and Gas business act

[2] This report is available in Japanese only.

[3] Safety that ensures no direct physical damage such as injury, electric shock or burns

sophisticated day by day. In particular, the fundamental safety measures of the appliances were discussed in detail.

## 2. Future direction

- Until now, the concept of product safety has been based on the assumption of manufacturers and importers regarding possible hazards in the situation where the product will be used, and to ensure fundamental safety in design, etc. so that the product itself does not cause harm to the human body or damage to property, and to design the product so that even if an accident occurs, the degree of harm or injury will be small (fundamental safety). In addition, safety protective measures (functional safety) are taken through electrical and electronic control mechanisms, such as physically stopping the product when a certain temperature, voltage or other dangerous thresholds are exceeded.
- In product development and design, a common concept for ensuring safety is to reduce risks in the three steps, called the three-step method.
  - Inherently safe design (elimination of the basis of hazardous events, reduction of the degree of harm and frequency of occurrence)
  - Guards and protective devices (protective measures, such as safety devices)
  - Information for use (informing of residual risks and encouraging safe activities such as warning signs)
- In future, we will move into an era of collaborative safety, in which people, products, environments and systems share information with each other and ensure safety through collaboration and harmonisation.
- It is necessary to avoid unsafe situations where fundamental safety and functional safety (collectively called 'safety functions') are affected in some way by the Internet and other communication lines, causing to serious product accidents, etc. even in situations where electrical appliances and other products are controlled through Internet, by having remote operation systems.
- For this reason, the guidelines call for the separation of the safety function from communication lines, and require that the safety function is maintained even if the communication lines fail.
- In addition, the new concept of 'supportive safety functions' has been introduced and is required to be introduced to the extent possible. 'Supportive safety functions' is not one of the safety functions, but is expected to be effective in reducing the risk of remote operation due to: overconfidence; mis-operation or misuse; and to prevent product accidents and danger to those who are in the vicinity of the appliance. It is defined as one of the functions of 'collaborative safety,' in which people, things, surroundings and systems share information with each other to ensure safety through collaboration and harmonisation.
- Furthermore, when manufacturers and importers conduct risk assessments of appliances, the handling of remotely operated appliances is broadly

classified into ‘attended appliances, which operate with user attention’ (hereafter referred to as “attended appliances”), and ’unattended appliances, which operate without user attention’ (hereafter referred to as “unattended appliances”), with the former being categorised as appliances that should not be operated remotely.

- In addition, case studies were conducted on ‘unattended appliances’; subject to remote operation, taking into account the acts of remotely turning the appliances on and off, and adjusting the settings of the appliances, for reference by manufacturers and importers.
- Although appliances with a remote operation system may be used to download, update software, etc. using communication lines, these guidelines cover appliances for which the manufacturers and importers determine the specifications for the entire function, including the communication function.

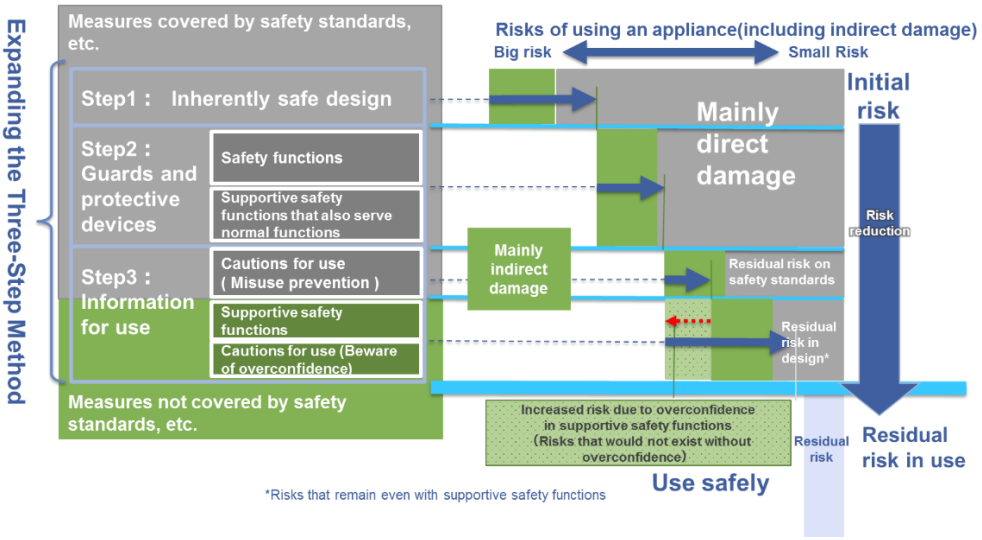
## 3. Approach to ensuring safety in these guidelines

When electrical and gas appliances have remote operation systems, it is necessary to avoid unsafe situations that may cause to serious product accidents, etc. due to some influence from communication lines such as the Internet.

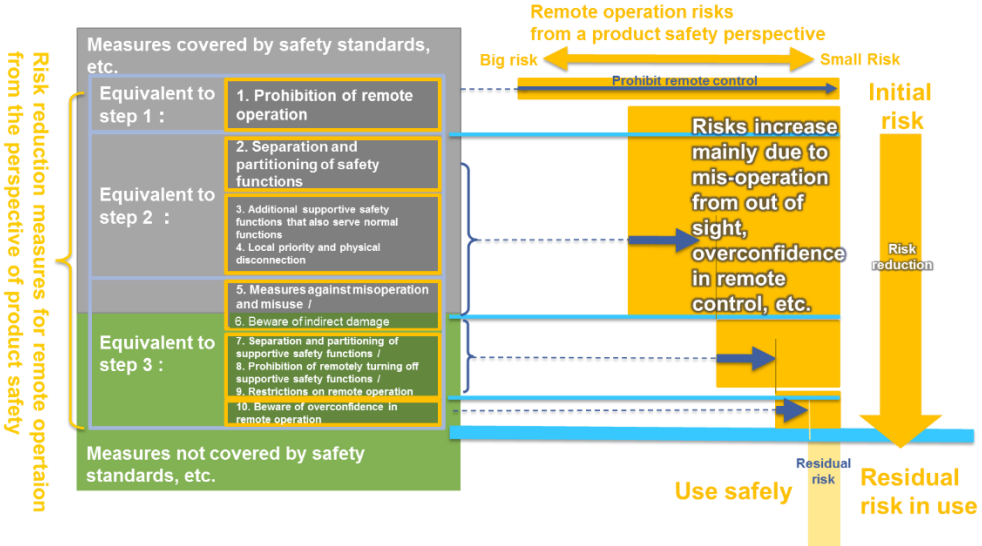
The concept of the three-step method was expanded to address new risks, such as indirect damage and risks due to remote operation, including communication fault and cyberattacks.

The following is a schematic diagram of risk reduction measures to ensure safety in these guidelines. The definition of the terms in the conceptual diagram is explained in the Annex.

Risk reduction measures for indirect damage




Risk reduction measures for remote operation



## 4．Risk assessment

### （1）Estimated damage

When designing an appliance that can be remotely operated, it is necessary to consider not only the direct damage caused by the appliance but also the indirect damage that may be caused in the vicinity of the appliance or near the appliance.

In these guidelines, indirect damage is limited to damage that has a high probability of being assumed at this point in time, but it should be noted that this will change with future variation in tolerable risk of society and trend, etc. in product accidents.

### （2）Direct damage

The basic idea of risk reduction measures for remote operation systems using communication lines of the target appliance is to apply the risk assessment based on ISO/IEC Guide 51.

The decision-making procedures for risk assessment are mentioned in 'the Report of Understanding Remote Operation in Appendix Table 4 and 8 (November 18, 2019)[4]' of the Electrical Appliances and Materials Research Committee, etc. Directly occurring damage in these guidelines are the damage caused by hazard sources that should be taken into consideration as mentioned in the above reports[5].

### （3）Indirect damage

Indirect damage refers to damage that occurs directly to the user in the vicinity of the appliance or to near the appliance due to remote operation by the operator, as well as damage caused by the continued operation and stop of the appliance.

The scope of damage was examined based on the cases of use and risk scenarios of possible damage by selecting appliances that already have a remote operation system and target appliances that may be remotely controlled in the future. Specific damage is assumed to include heat stroke, drowning of children, indirect health damage (dizziness, nausea, carbon

---

[4] This report is available in Japanese only.

[5] Electric shock, smoke/fire, burns, mechanical hazards (moving parts, rotating parts, vibration, explosion, implosion, etc.), chemical and biological hazards, prevention of harm from electromagnetic waves emitted from electrical appliances, hazards due to disregard of ergonomic principles, combinations of hazard sources and hazard sources associated with the environment in which electrical appliances are used.

monoxide poisoning, etc.), indirect fire, burns, etc.

## 5. Supportive safety functions

When remotely operating an appliance, it is necessary to confirm that there is no risk, such as harm to the user who is in the vicinity of the appliance or damage to the property by remotely operating the appliance from a position where the operator cannot see the appliance. It is also necessary to take measures to prevent malfunction regardless of the location of the remote operator.

For this reason, apart from safety functions, functions that are expected to have the effect of reducing risk that increase due to remote operation are defined as, 'functions that can prevent or reduce damage caused by operator overconfidence or mis-operation of the remote operation system and harm to user in the vicinity of the remotely operated appliance', based on the cases of use and risk scenarios of highly probable harm which are caused near the appliance by the remotely operated appliance. The main examples are as follows:

- An additional or optional function to prevent or reduce harm to the user who is in the vicinity of the appliance.
- A function that can prevent or reduce direct or indirect damage caused by overconfidence, mis-operation, or misuse of the remote operator, as well as unintentional harm caused by remote operation to the user who is in the vicinity of the appliance.
- A function that indicates that the appliance is being operated remotely and confirms the safety of the area near the appliance and other situations also includes an alarm for the user who is in the vicinity of the appliance. A function that reduces the risk of remote operation by requesting the operator and the user who is in the vicinity of the appliance to take action.
- A function that checks the safety of the area near the remotely operated appliance and other situations automatically activates mechanisms, such as controlling and locking, to avoid or reduce risks during remote operation.
- A function that safely stops the appliance when the built-in detection function or the external detector used in combination with the built-in detection function, detects that the operator near the appliance has left the appliance or that there is a change in the area near the appliance.
- A function that prevents or reduces harm to the operator or the user in the vicinity of the appliance at its own judgment through best-effort control that incorporates advanced technology and software.

## 6. Classification of remote operation appliances

### (1) Appliances that can be remotely operated

Appliances other than those classified in '6.(2)' and 'appliances for which remote operation are permitted by Ministerial Order on Technical Requirements for Gas Equipment and Ministerial Order on Technical Requirements for Liquefied Petroleum Gas Appliances, etc.' are reorganised as 'unattended appliances[6]' and 'appliances that can be remotely operated'.

### (2) Appliances that are unsuitable for remote operation

The following appliances are unsuitable for remote operation and could pose a risk of harm to the user who is in the vicinity of the appliance or the area near the appliance, considering the location where it will be installed, the intended use, the duration of use and the influence on the area near the appliance, etc. For this reason, 'attended appliances[6]' are basically classified as appliances that are not remotely operated.

- The functions and roles of the appliance are achieved when the operator switches on the appliance to start operation.
- Exposure to dangerous parts during operation, such as causing burns from touching hot surface of the appliance or injuries from touching moving parts.
- Remote operation significantly increases the risk of danger.

When considering the pros and cons of remote operation of such appliances in response to future variation in tolerable risk of society, etc. careful consideration should be given to the avoidance of conveying a wrong message to consumers that the appliances can be operated remotely by enabling remote operation, in addition to risk reduction measures for the appliances.
For example, in electrical appliances sector, such as irons, sewing machines, hair care appliances and most of cooking appliances are included in 'appliances unsuitable for remote operation'.

[6] For definition of this term, refer to Terms and definitions

## 7. Considerations in product design

### (1) Separation of safety functions, including functional safety, from communication lines

In IEC 60335-1, the basic principle is that the safety function should be achieved by a protective device, such as a fuse and an over-temperature protection device. However, even if the safety function is not ensured by a fuse, an over-temperature protection device, etc., but only a protective electronic circuit[7], a test against electromagnetic noise and a reliability evaluation of the embedded software, if any, should be performed as part of the functional safety evaluation.

However, as appliances become more IoT-oriented and unauthorised access, such as cyberattacks, are predicted to increase in the future, the risk of safety functions becoming insecure due to tampering, etc. may not be eliminated if software updates for protective electronic circuits are distributed via network interfaces.

For this reason, to ensure that functional safety works from the design stage when the target appliances are designed as IoT oriented products, these guidelines basically recommend that physical protection devices such as fuses are incorporated from the design stage to ensure the safety, rather than ensuring safety functions only with protective electronic circuits; and strongly recommend that circuit of communication lines and functional safety are independent, if they cannot be separated by physical means.

Even when it is unavoidable that communication lines and functional safety cannot be separated, it is recommended that the safety of appliances is not dependent on remote communication by separating software related to safety functions (including functional safety) and software for remote communication with public communication lines.

### (2) Supportive safety functions

When the appliance is operated remotely, it is recommended that the functions shown in Section 5 as the examples are incorporated from the design stage, to the extent possible, in order to avoid harm to people who are near the appliance or to the area around the appliance.

In addition, manufacturers and importers are requested to provide remote operators of appliances with information on the conditions of use, risks and cautions and actions to be taken in case of an abnormality notification (priority of local operation, disconnection of the

[7] The protective electronic circuit may include a microcontroller.

communication line by a nearby user), etc. so that they do not overconfidence, mis-operate or misuse the functions of the appliances and cause unintentional harm to the user near appliances, etc.

（3）Prevention for unauthorised access

For appliances that can be remotely operated, if it is unavoidable to ensure functional safety only with protective electronic circuits, it is necessary to test software updates before shipping and confirm that they do not affect the functional safety of the appliances.

In addition, for protective electronic circuits that control functional safety, manufacturers and importers need to ensure a means of providing necessary information to the remote operators so that software can be properly downloaded after appliance shipment. The specific measures are as follows:

- Formulation, operation and management of secure software that meet security requirements, such as authenticity and integrity.
- How to provide software updates.
- Terms and conditions of provision for security performance and updates of appliances.
- Warning when unauthorised access is detected.

## 8．Considerations after appliance shipment

### （1）Repair and maintenance

To ensure that functional safety works, it is desirable to maintain the separation between communication lines and functional safety, incorporating not only protective electronic circuits but also protective devices, such as fuses, from the design stage to ensure the safety.
However, when relying on protective electronic circuits for functional safety, IEC 60335-1 states that if the software of the protective electronic circuits for functional safety is to be changed; authenticity, integrity, encryption, etc. are required at the time the software is provided, and compliance to the safety requirements of the standard must not be compromised during or after installation. This is also required in these guidelines.
Furthermore, when manufacturers repair and maintain their appliances, devices comprising connections to communication lines that cannot be updated with software, must be isolated and replaced, and the time of replacement must be notified to the remote operators.

### （2）Update software, etc.

To ensure that functional safety works, it is desirable to maintain the separation between communication lines and functional safety, incorporating not only protective electronic circuits but also protective devices, such as fuses, from the design stage to ensure the safety.
However, when functional safety relies on protective electronic circuits, updating the software of the protective electronic circuits requires the following measures to ensure the authenticity, integrity, etc. of the devices in the appliance for functional safety.

- Identify the current software in the appliance and check the appropriateness of the software to be updated
- Ensure the authenticity and integrity, etc. of devices related to functional safety by ensuring software protection, including the use of cryptographic techniques and redundant memory, to prevent data corruption and interruption of data, etc. transmission during updates

### （3）Clarification of requirements for remote operators and users

When remotely operating appliances, it is necessary to: clarify the conditions of use; risks and cautions for use; actions to be taken when notified of an abnormality (prioritising local operations, disconnecting communication lines by nearby users); cautions for software updates; and other requirements that encourage users to take active actions, to prevent overconfidence, mis-operation, misuse and unintentional harm to the user who is in the vicinity of the appliance and surroundings. Specifically, the

following requirements are included.

i ) Precautions for use

- Provide information on what to watch out for, during remote operation due to the loss of remote monitoring, such as the information that the appliance will automatically stop in the event of a communication failure.
- Means of warning remote operators and users in the event of a communication failure, including unauthorised access, should be secured.
- Thoroughly implement a system that disconnects communication lines easily and prioritises local operations by the user who is in the vicinity of the appliance.

ii ) Software update

- Consideration shall be given to allow the remote operators to easily update the software.
- Continued operation of the appliances during the update is important for users. As described in Section 7.1, separation of communication lines and functional safety is strongly recommended in product design, but when updating software for protective electronic circuits that control functional safety, the function of remote operation during updating is not properly managed. However, when updating the software of the protective electronic circuits that control functional safety, there is a risk that the remote operation will not be properly managed during the update. For this reason, a means of notifying the remote operator and the user when the operation of the appliances stops during the update shall be secured.
- Notify the remote operator that a security update software exists.
- Provide a security update software to the remote operator.
- For appliances that contain devices that cannot be updated with software, the reason why the software cannot be updated and the support period along with the method for replacing the hardware should be provided.

（Annex） Interpretation of terms in conceptual diagram

1. Prohibition of remote operation
For appliances classified as 'attended appliances[8]', as an essential safety measure, remote operation should be prohibited, unless the risk of remote operation is reduced through the development of new appliances, such as irons; that are designed to function without burns.

2. Separation and partitioning of safety functions
Appliances that are remotely operated should, in principle, use safety functions that do not depend on software, such as fuses, as a measure to prevent fires and other incidents. Even when protective electronic circuits are used, they should be separated from the communication line. If this is not possible, the communication part of the communication line and the software of the protective electronic circuit should be separated into modules.

3. Additional supportive safety functions that also serve normal functions
In addition to supportive safety functions that also serve normal functions like prevention of burns by thermostat temperature control, safety measures for remote operation, such as maintaining a safe state after disconnection, limiting temperature at a value lower than the upper limit of normal temperature control and stopping the appliance turned on by remote operation after a certain period of time, need to be added. These functions mainly refer to measures covered by safety standards, etc., or those that are similarly limited by local operation.

4. Local operation priority and physical disconnection
In case of being risk of indirect damage to the user who is in the vicinity of the remotely operated appliance, local operation has priority. In case the risk cannot be avoided even with the priority on local operation, a communication line disconnection switch, etc. should be installed.

5. Measures against mis-operation and misuse
Operation result feedback, double action, screen lock and other measures to prevent accidental operation; authentication and authorisation of remote operation by the operator and measures to ensure completeness and integrity with encryption and other measures.

[8] For definition of this term, refer to Terms and definitions

6. Beware of indirect damage

Warning of indirect damage caused by remote operation.

This includes a function that warns the user who is in the vicinity of the appliance of danger and encourages them to take active measures based on the fact that the appliance and the area near the appliance are being monitored, remotely operated, etc. and a function that warns the remote operator of danger based on remote monitoring of the appliance and the area near the appliance.

7. Separation and partitioning of supportive safety functions

The software of the supportive safety function is basically separated from the communication line, but if this is not possible, the communication part of the communication line and the software of the supportive safety function are separated into modules.

8. Prohibition of remotely turning off supportive safety functions

Prohibit remote ON to OFF operation of systems that prevent children and other people from operating the equipment, such as child lock, interlock and water supply lock.

9. Restrictions on remote operation

Restrictions should be placed on remote operation functions that increase the risk of remote operation (e.g. remote operation of the ventilation function should not be accepted when the system is operating as 24-hour ventilation under the Building Standard Law). Note that these measures are not covered by the safety standards, etc.

10. Beware of overconfidence in remote operation

Warnings against overconfidence that supportive safety functions will always work (e.g. the risk of leaving the appliance on because of the automatic turn off function).

Warnings against overconfidence that appliance operates normally (e.g. the risk of causing heat stroke or other harm to the user who is in the vicinity of the appliance because normal operation becomes uncertain due to communication fault, even though the user intended to operate the appliance in a proper manner remotely after leaving the house).

Terms and definitions

- manufacturers and importers
  Manufacturers and importers who have submitted a notification based on the four Product Safety Acts in Japan.

- appliances
  Electrical and gas appliances used in the home, including battery-powered appliances and other appliances powered by direct current.

- remote operation
  The operator operates appliances from out of sight. Operations to remotely turn appliances from OFF to ON, ON to OFF or to adjust appliance settings (limited to appliances that are in constant operation).

- out of sight
  A position where the operator cannot directly see the appliance.
  It is further categorised into operation from another room, operation from a shared control room and operation from outside the home.

- operator
  A person who has the ability to operate appliances.

- user
  A person, who is in the vicinity of the appliance or who is out of operator's sight, who benefits from the appliance.

- state of human attention
  A state that the operator or user can maintain or confirm the correct operation of the appliance by operation or visual inspection, etc., and can detect and take action themself in the event of abnormal or dangerous activity.
  Even if the appliance is equipped with a system, etc. to check the safety of the area near the appliance and other situation, it does not mean that the appliance operates in a state of human attention.

  Note: In the context of these guidelines, the terms "appliances operate in a state of human attention" and "attended appliances" are considered to be synonymous. For more information of "attended appliances", see Sub clause 30.2 of IEC 60335-1 Ed. 6.0.

● state of human inattention
A state that does not apply to “state of human attention”.

Note: In the context of these guidelines, the terms “appliances operate in a state of human inattention” and “unattended appliances” are considered to be synonymous. For more information of “unattended appliances”, see Sub clause 30.2 of IEC 60335-1 Ed. 6.0.

● serious product incidents
Product Incidents falling under the requirements provided for by Cabinet Order with respect to details of the safety hazard or the manner of the incident, being incidents where actual or potential harm is serious, in Article 2, paragraph 6 of the Consumer Products Safety Act.
The applicable examples are as follows:
- Accidents which harm to the life or body of a general consumer, and the harm is serious
- Accidents that consumer products are lost or damaged and there is a risk of serious harm to the life or body of a general consumer

● hazard source
Electrical, mechanical and other hazard sources in Annex A of IEC Guide 104.

● overconfidence
Over-reliance on the remote operation functions of appliances, or on the certainty of one's own memory or actions. Misuse is not included.

● misuse
Remote operation of an appliance in an incorrect manner.
This includes remote operation of an appliance by masquerade of a person other than the operator.

● unintentional harm
When an appliance is operated remotely, unintended actions may cause harm or property damage to the user who is in the vicinity of the appliance or to the area near the appliance.

● software partitioning
A group of software that should meet special requirements should be composed in separate modules so that it can be managed separately from other groups.
Note that division by modularisation is one of the techniques of software

high reliability design, as opposed to communication blocking, where the safe operation of equipment should not depend on communication.

- separation between communication lines and functional safety
  Functional safety does not depend on communication with software or data located outside of local network, such as in a cloud provided by manufacturers and importers of electrical and gas appliances, and the function can be reliably performed even if communication is interrupted.

## Study Group on ensuring safety with the IoT connection of electrical and gas appliances

| | | |
|---|---|---|
| Chair | Masao Mukaidono | Professor Emeritus, Meiji University |
| | Koichi Arimura | Executive Director, Japan Computer Emergency Response Team/Coordination Center |
| | Ryo Ono | Professor, Graduate School of Frontier Sciences, The University of Tokyo |
| | Toshiyuki Kajiya | Director, The Institute of Global Safety Promotion<br>Representative member, IEC/IECEE CMC |
| | Hiroshi Genda | Manager, Financial & Public affairs sales promotion division, Mitsui Sumitomo Insurance Company |
| | Nobuo Gohara | Representative, Gohara Compliance and Law Office |
| | Atsuhiro Goto | President, Institute of Information Security |
| | Junkichi Sumiya | Director, Japan Electrical Safety & Environment Technology Laboratories |
| | Shigeki Takahashi | Former WG chair of International Electrotechnical Commission |
| | Jun Masuda | Representative attorney, Jun Masuda Low Office |
| | Ryoji Mori | Attorney, Eichi Law Office |
| | Watabe Toshinori | President, Techno Quality |

● Observers

- Product Safety Division, Industrial Safety Group, Ministry of Economy, Trade and Industry
- Cyber Security Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
- Information Industry Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
- Japan Electronics and Information Technology Industries Association
- The Japan Electrical Manufacturers' Association
- Japan Industrial Association of Gas and Kerosene Appliances
- National Institute of Technology and Evaluation
- Information-technology Promotion Agency
- National Institute of Occupational Safety and Health
- Association for Electric Home Appliances
- Japan Gas Appliances Inspection Association

- The Japan Gas Association
- Tadashi Sakaguchi, Secretary of IEC/TC61/MT23

● Secretariat

NTT DATA INSTITUTE OF MANAGEMENT CONSULTING Inc.

<For inquiries about these guidelines>

Product Safety Division, Industrial Safety Group, Ministry of Economy, Trade and Industry