JST-EG-01-01-2024R1

Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR) STAR-1 Assessment Guide

May 2025

Information-technology Promotion Agency, Japan (IPA)

Table of Contents

1. Introduction.

This guide describes specifically how to perform the assessment required by the assessment method described in "STAR-1 Level Conformance Requirements and Assessment Method."

1.1 How to describe the checklist

The assessment results included in the checklist must be carried out according to the assessment items and assessment guide described in this document.

[Results of the assessment]

For each of the 16 assessment items in the STAR-1 Conformance Requirements, an assessment based on this guide will be conducted, and a conclusion will be reached as "Conforming (Y)," "Non-conforming (N)," or " Not Applicable (NA)." Please note that "Not Applicable (NA)" cannot be selected if the conditions for being "Not Applicable (NA)" are not satisfied.

[Note] In case there is even one "Non-conforming (N)" among the assessment results of 16 assessment items, application for a conformance label is unacceptable.

[Evidence]

- In the case of "Conforming (Y)," information on evidence including the following shall be included in the checklist column for each assessment item.
    - ➢ For assessments based on "Document Assessment":
      Name, website, document number, etc., of the technical documents, internal documents, regulations, etc., used in the assessment, as well as information identifying the relevant sections with the rationale (e.g., document name, document number, page number, chapter number, URL)
    - ➢ For assessments based on "Device Check":
      Names of information or documents, etc., (e.g., photos, videos, screenshots, logs (system output) that can confirm the verification results of the device check, and a summary of the assessment results.
        - ✧ It is available to use the results of tests conducted at the time of product development or documents created and evaluated at the time of obtaining other certifications (e.g., Common Criteria) as evidence for device check under this Scheme. In such cases, such documents should be kept as evidence.

- In the case of "Not Applicable (NA)," a document or other evidence explaining the reason for being "Not Applicable (NA)" should be prepared. In the "Reason for being Not Applicable (NA)," the rationale for determining that appropriate measures are being taken against the threat (why there is no problem even if it is not eligible, or why alternative measures are being taken) should be described. The specific details to be described are described in "Conditions for being Not Applicable (NA)" in each assessment item, and the reasons must be explained accordingly.

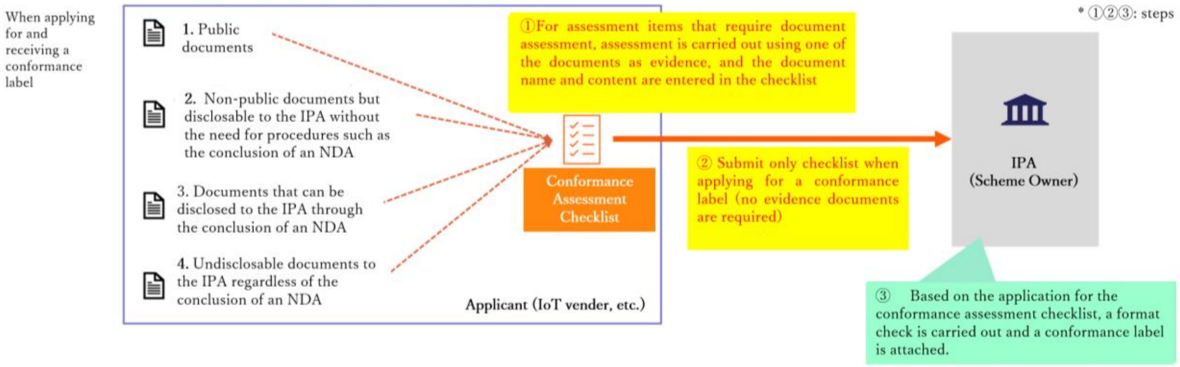
1.2 Handling of Evidence

For each assessment item of STAR-1, the format for how to prepare the documents to be evaluated for the document evaluation can be selected by the IoT vendor.

As described in section 1.1, assessment shall be conducted based on the evidence of the prepared documents, etc., and the names of the documents and the assessment results shall be listed in the checklist.

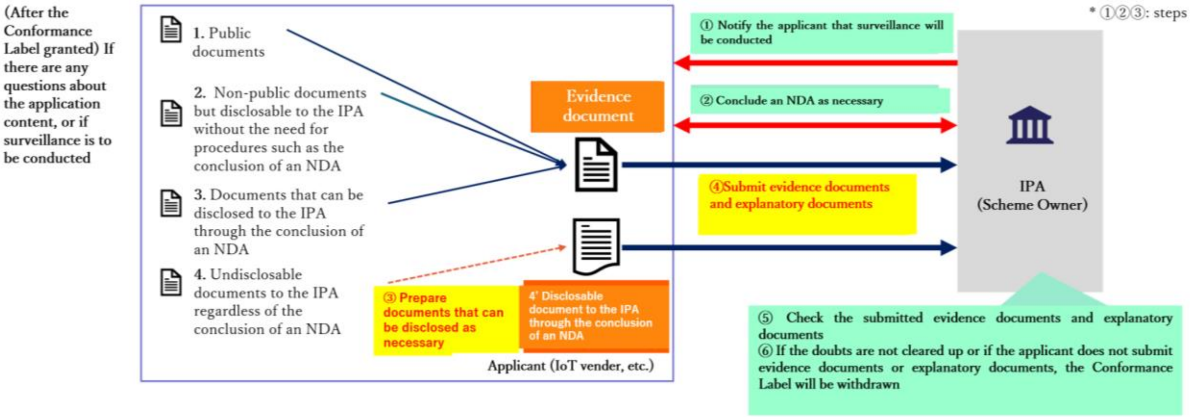
[Handling at the time of application]

- When applying for a conformance label, the applicant is only required to submit a conformance assessment checklist and is not required to submit evidences.
- It is required that the retention of documentary evidence during the validity period of the conformance label


When applying for and receiving a conformance label
1. Public documents
2. Non-public documents but disclosable to the IPA without the need for procedures such as the conclusion of an NDA
3. Documents that can be disclosed to the IPA through the conclusion of an NDA
4. Undisclosable documents to the IPA regardless of the conclusion of an NDA
Applicant (IoT vender, etc.)
Conformance Assessment Checklist
①For assessment items that require document assessment, assessment is carried out using one of the documents as evidence, and the document name and content are entered in the checklist
② Submit only checklist when applying for a conformance label (no evidence documents are required)
IPA (Scheme Owner)
③ Based on the application for the conformance assessment checklist, a format check is carried out and a conformance label is attached.
* ①②③: steps

[Handling in Surveillance, etc.]

- If there is any doubt about the contents of the application after the conformance label is granted, or if surveillance is conducted, the IPA will request the applicant to submit documentary evidence. For "documents that cannot be presented to IPA regardless of NDA conclusion," an explanation in a separately disclosable document will be accepted.
- The conformance label is canceled in case it is not deemed to be an adequate explanation.


(After the Conformance Label granted) If there are any questions about the application content, or if surveillance is to be conducted
1. Public documents
2. Non-public documents but disclosable to the IPA without the need for procedures such as the conclusion of an NDA
3. Documents that can be disclosed to the IPA through the conclusion of an NDA
4. Undisclosable documents to the IPA regardless of the conclusion of an NDA
Evidence document
③ Prepare documents that can be disclosed as necessary
4' Disclosable document to the IPA through the conclusion of an NDA
Applicant (IoT vender, etc.)
① Notify the applicant that surveillance will be conducted
② Conclude an NDA as necessary
④Submit evidence documents and explanatory documents
IPA
(Scheme Owner)
* ①②③: steps
⑤ Check the submitted evidence documents and explanatory documents
⑥ If the doubts are not cleared up or if the applicant does not submit evidence documents or explanatory documents, the Conformance Label will be withdrawn

1.3 Use of external organizations such as JC-STAR evaluation bodies and JC-STAR assessment bodies

Although the self-conformance declaration is intended to be a self-conformance assessment by the IoT product vendor itself, since the STAR-1 Conformance Requirements and Assessment Methods also include device check by using tools, the assessment and checklist creation can be requested to external organizations such as the JC-STAR evaluation body or JC-STAR assessment body if there are reasons such as not being able to perform sufficient conformance assessments using the company's existing systems and equipment, or wanting to reduce the cost, time, and workload of assessment.

Within Accreditation System of National Institute of Technology and Evaluation (ASNITE) of the National Institute of Technology and Evaluation (NITE), a JC-STAR evaluation body accreditation system based on ISO/IEC17025 will be established (from FY2025 onwards) for service providers that can perform JC-STAR assessment of STAR 3 or more, and service providers that have appropriate capabilities and systems in place will be certified as "JC-STAR Evaluation Body."
It is also possible to request a conformance evaluation from a JC-STAR Evaluation Body, and if the JC-STAR Evaluation Body creates the entire checklist, and it is possible to apply for a conformance label as a "conformance evaluation by a JC-STAR Evaluation Body."
Until the JC-STAR Accreditation System for Evaluation Body begins, a provisional measure will be taken to deem evaluation body that conduct evaluations and Security Target (ST) confirmation for the "software" product field under the "Japan Information Technology Security Evaluation and Certification Scheme (JISEC)" to be equivalent to "JC-STAR Evaluation Body."
For information on these evaluation bodies, please refer to the JISEC Evaluation Body List page.

JC-STAR Assessment body is the body whose services have been registered in the "Equipment Verification Service (registration opened in September 2023)" category of the "Information Security

Service Standards Examination and Registration System" that examines and registers conformance with the "Information Security Service Standards" established by the Ministry of Economy, Trade and Industry. If the entire checklist is prepared by a JC-STAR assessment body, it is available to apply for a conformance label as a "conformance assessment by a JC-STAR assessment body." For registered bodies of equipment verification services, please refer to the Services for Verification of Equipment list in the Information Security Service Standards Conformance Services list.

[Handling of checklists when using outside organization]

- In case a JC-STAR evaluation body or JC-STAR assessment body is requested to conduct an assessment and prepare a checklist, "conformance assessment outsourcing" can be selected as the assessment method in the "Checklist."
- However, if there is even one item that could not be evaluated by the JC-STAR evaluation body or JC-STAR assessment body due to the fact that the JC-STAR evaluation body or JC-STAR assessment body could not receive the evidence document from the vendor, the entire checklist shall be considered as "the result of self-assessment by the applicant" and not "the result of assessment conducted by the JC-STAR evaluation body or JC -STAR assessment body."
- There is no problem to use an external organization other than a JC-STAR evaluation body or JC-STAR assessment body. However, it is necessary to select "self-conformance assessment" for the assessment method in the "Checklist."

2. Concept of STAR-1 Level Conformance Requirements

2.1 Concept of (Definition of) Target IoT Products

The main objective of this Scheme is to require IoT products that meet all of the following conditions to be equipped with the necessary security functions in advance. The intention behind this is to ensure that IoT products that have the potential to be connected to the Internet and for which the procurer/user has no other means of ensuring security than to "continue to use the security functions provided at the time of purchase," it is important to "confirm in advance whether the necessary security functions are provided" "before the product is purchased." The intention behind this is also to "visualize the security functions in the form of a conformance label."

For this reason, this Scheme targets IoT products that are "IoT devices that can communicate with the Internet (conditions 1), 2), and 3)) , but that use the security functionality provided in the IoT product at the time of purchase and for which it is difficult/unlikely to add new security measures later (other than updates for vulnerability countermeasures) (condition 4)).

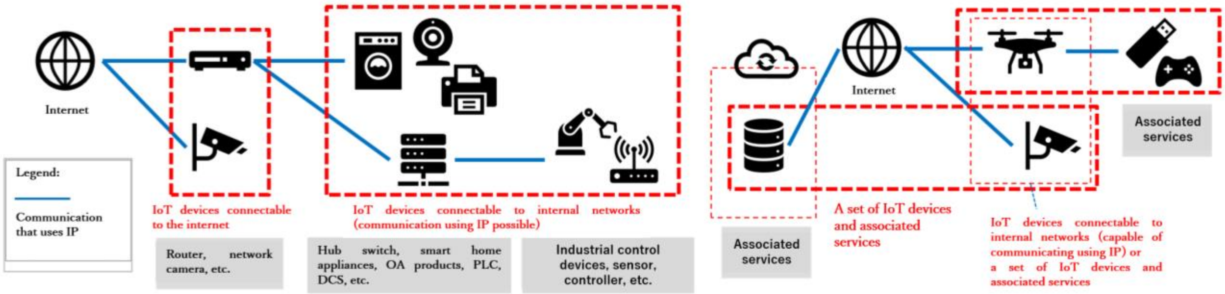
In addition to the products listed as examples, IoT products that meet all of the conditions 1) through 4) may be eligible. On the other hand, PCs, smartphones, tablets, etc., are excluded from the scope because they do not meet condition 4). Whether or not an IoT product under consideration for obtaining a conformance label is subject to the requirements should be determined based on whether or not it meets all of the conditions 1) through 4):

1) The device is included (labels are assigned to device.)

2) The device has ability to send and receive data using Internet Protocol (IP.)

3) The device is possible/deniable to connect directly or indirectly to the Internet.

4) It is necessary to use the security functions provided at the time of purchase and difficult/impossible to add security functions later (at the procurer's/user's own will) other than by updating the security functions.


Internet
Legend:
Communication that uses IP
IoT devices connectable to the internet
Router, network camera, etc.
IoT devices connectable to internal networks (communication using IP possible)
Hub switch, smart home appliances, OA products, PLC, DCS, etc.
Industrial control devices, sensor, controller, etc.
Associated services
Internet
A set of IoT devices and associated services
IoT devices connectable to internal networks (capable of communicating using IP) or a set of IoT devices and associated services
Associated services

[Supplementary Information]

- Condition 1) means that software and cloud services without device are not eligible because the target of the conformance label is device.
- Conditions 2) and 3) imply that if the device has a possibility of an attack from the Internet side, it is eligible. Thus, the device that has any connection to the Internet whether direct or indirect is eligible.
  - For example, even in an environment where boundary protection is provided by logical controls (access control) such as Virtual Private Network device and Firewall devices for communications from the Internet side, and communications to the inside are restricted, there is still the risk of unauthorized access to such access control, etc. Therefore, it cannot be judged as completely separated from the Internet. For this reason, the device that is even placed inside an environment being separated from the Internet by logical control (access control) is judged to have "the possibility/undeniability of being connected to the Internet" and is included in the scope of this Scheme.
  - If a device connected to the Internet performs some kind of conversion process on communications from the Internet side, and if the environment is separated by physical separation or complete logical disconnection so that IoT devices inside the device are not allowed to communicate directly from the Internet, then the IoT device is considered to be completely isolated from the Internet. In such a case, it can be judged that the IoT device inside the device is "not assumed to be connected to the Internet," therefore the IoT device is outside the scope of this Scheme. However, depending on the IoT device, it may be difficult for procurers and users to determine whether "the IoT device is not subject to this Scheme because it is not assumed to be connected to the Internet and therefore does not have a conformance label," or "the IoT device is subject to this Scheme because it is likely to be connected to the Internet but does not have a conformance label." In such cases, IoT product vendors may voluntarily decide to apply for a conformance label even if their products are not covered by the system.
- Condition 4) means that it is impossible/difficult to incorporate another security software, etc., supplied by a vendor other than the IoT manufacturer into the relevant IoT product. Please note that the addition of new security functions by the IoT manufacturer vendor itself through updates is part of "support" and does not fall under "adding security functions later" in Condition 4).
- In principle, PCs, smartphones, tablets, etc., are excluded from the scope of this Scheme because they do not meet condition 4). However, if all of the following conditions are met, it is available to obtain a label as an IoT product even if it is based on a PC, smartphone, tablet, etc.
  I. The installation (addition) of security functions is completely controlled by the company's application or OS and is designed to prevent the installation of security

functions (at all, except for the software provided as updates) by circumventing the management functions of the application or OS.

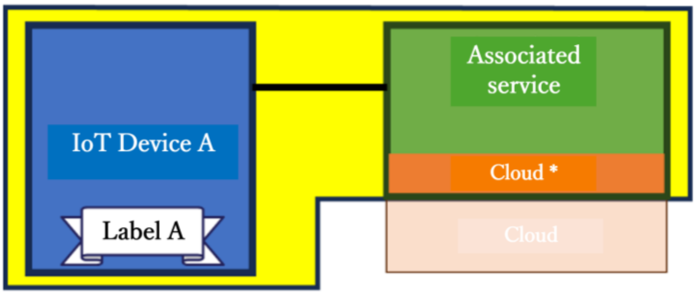
II. Measures are in place to prevent the use of the system as a general-purpose PC or tablet, even if the company's own applications are deleted, formatted, or the OS is replaced, etc.

III. Appropriate control over the application of vulnerability responses provided by general-purpose OS vendors (e.g. proprietary distribution of OS security patches as a distribution)

2.2 Concept of Associated Services

Associated services refer to "services that must be used as a set" with the subject "IoT device." Specifically, they are services that are provided in conjunction with the IoT devices in cases where the IoT devices themselves cannot provide the intended purpose of the IoT products.

EXAMPLE: When a network camera (IoT device A) is configured to store the images it captures in a specific cloud service X, said service X is associated service. In this case, the scope of assessment for the conformance label is "IoT Device A," "Cloud Service X," and the entire communication path connecting the two. The conformance label is assigned to "IoT Device A."



* Cloud area directly used by the service

There are no restrictions on the form of provision of associated services other than the condition that they are "provided as a set with the opposing IoT device. However, please note that if the opposing service is not identified from the perspective of IoT devices, the service is not an associated service.

2.3 Concept of security level to be achieved by STAR-1

The purpose of STAR-1 is to counter the minimum threats that any IoT product should counter, from the perspective of a unified standard for a wide range of IoT products, rather than focusing on a specific product type. In view of this purpose, the concept of the security level to be achieved in STAR-1 is as follows:

① Infection with malware and becoming a bot shall be prevented. Especially the spread of infection from infected devices shall be prevented.

② Assuming remote attacks mainly from the Internet side, the scheme is designed to provide practical resistance to script kiddie level attacks (attacks that take advantage of system vulnerabilities using crack tools and other tools available on the Internet and the dark web, etc., with limited expertise), such as unauthorized access and eavesdropping.

③ Response and support policies for product defects and vulnerabilities shall be clarified, and it shall be ensured that support (e.g. provision of update files) is provided within the validity period of the conformance label

④ Appropriate measures are taken against the threat of leaks of information to be protected, such as the ability to properly delete data generated during the operation of IoT products at the time of disposal or resale.

Based on the above concept, information assets, attack surfaces, threats and countermeasures that are mainly assumed in STAR-1 are examined and defined as conformance requirements, assessment methods and assessment items.

2.4 Concept of information assets to be protected

STAR-1 assumes (1) that information assets are remotely attacked from the Internet side during operation (attacks that involve physical contact due to loss, theft, trespassing, etc., are not assumed) and (2) that information assets generated during operation are deleted at the time of disposal or resale.

Information assets that should be protected in STAR-1 are information assets that need to be considered how to be protected even under such assumptions.

[Examples of information assets to be protected at STAR-1]

For example, the asset to be protected at STAR-1 can be considered as follows:

- The "wired communication function," "wireless communication function," and "security function" are functions that should be managed by the manufacturing vendor and are information assets that should be protected throughout their lifecycle.

- "Configuration information related to IoT functions (communication functions)" and "Configuration information related to security functions" are information assets that should be protected during operation because they are information that is used at all times during operation. Information should be deleted or defaulted at the time of disposal or resale.
- In principle, "generally sensitive information collected, stored, or communicated by the IoT device" is an information asset that should be protected. However, depending on the method of storage of such information, the treatment may be divided as follows, for example:
  - If it can be stored indefinitely or recalled from the Internet, it is treated as an information asset that should be protected during operation.
  - If the information is set to be automatically deleted or destroyed after a reasonable period of time, it can be treated as an information asset not subject to protection. Information must be deleted at the time of disposal or resale.

2.5 Concept of secure storage (protection method)

"Protecting" information assets does not necessarily mean only protecting confidentiality. For example, "configuration information related to IoT functions (communication functions)" can be categorized as information requiring "confidentiality protection," "integrity protection," "authenticity confirmation," or information not requiring such protection (some information may fall under more than one category). Depending on the category, information assets that require either "confidentiality protection," "integrity protection," or "authenticity confirmation," require corresponding measures.

① "Confidentiality protection" is required for information assets that need to be protected from unauthorized disclosure to outside parties.

② "Integrity protection" is required for information assets that need to be protected from tampering.

③ "Authenticity protection" is required for information assets that need to be protected from being impersonated.

For example, in "secure storage," it is important to specify even "how to protect and securely store" each information asset that needs to be protected.

In STAR-1, "secure storage" assumes countermeasures for the following two threats:

1) Unauthorized access through the network without access control

2) Unauthorized access without network or access control

The "unauthorized access without access control" mentioned above refers to unauthorized access that does not go through an interface that performs legitimate access control, and is assumed to be a case where, for example, malware exploits files with unauthorized privileges or directly accesses the storage of discarded IoT devices. (For "unauthorized access via access control," the System considers that the threat is countered by measures to properly authenticate users.)

Specifically, in STAR-1, assuming the attacker's ability to be at the "script kiddie level," the threat is assumed to be an attack that uses system vulnerabilities using crack tools, etc., that are published on the Internet, dark web, etc., and physical unauthorized access to information assets to be protected that are held by IoT devices after being disposed of or resold. Based on the concept that countermeasures against such threats are to be taken, "secure storage" shall be considered when protective measures similar to or beyond any of the following are taken. In particular, for d. through f. below, "confidentiality" and "integrity" protections are considered to have been achieved at the same time:

a. Information assets to be protected, whose confidentiality should be protected, are stored in encrypted form using encryption methods employing appropriate cryptographic techniques.
b. Information assets to be protected whose integrity must be protected, have data integrity protected by signatures using appropriate cryptographic techniques.
c. Information assets to be protected, whose integrity must be protected, have data integrity verified by message digests using appropriate hash functions.
d. Information assets to be protected are stored in secure areas provided as hardware functions, such as security chips.
e. Information assets to be protected are stored in secure areas with virtualization technology and sandboxes provided as a function of operating systems such as iOS/Android.
f. Information assets to be protected are stored in storage areas that cannot be easily removed that are built into IoT devices and cannot read or write data directly via externally invoked interfaces, or are not equipped with such interfaces.

2.6 Concept of the scope of required (or excludable) secure communication

Since "remote attacks from the Internet side" during operation is mainly assumed in STAR-1, the scope of IoT devices that are subject to secure communication requirements and IoT devices that can be excluded from secure communication requirements is considered as follows:

A) IoT devices that are within a scope where they may be connected from the Internet side are subject to secure communication requirements.

This means "may be connected" includes the case where "logically, even if the access is controlled so that it cannot directly communicate with the Internet without permission, the part that controls the access can be called from the Internet" in addition to being in a state where direct communication with the Internet is possible. For example, there is the case where a login screen is displayed. IoT devices placed in a closed network isolated from the Internet by a Virtual Private Network device, router, etc., are also included if they can communicate with the Internet via the Virtual Private Network device, router, etc.

B) IoT devices that are placed in a closed network isolated from the Internet by a Virtual Private Network device, router, etc., and that can block the possibility of being connected from the Internet side (communication with the Internet is not permitted), can be exempted from the requirement for secure communication, provided that users are explicitly warned that they are to be used by connecting to a device that blocks communication from the Internet. Specifically, a wired network environment used in an access-controlled area or a wireless LAN environment configured to restrict devices to be connected by WPA2/WPA3, etc., and separated from the Internet by a Virtual Private Network device/router/firewall, etc., is assumed, and in such a network environment, the risk of eavesdropping is considered to be prevented even if communications are not encrypted, since the necessary protection measures are taken against unauthorized access from the Internet.

For example, for IoT products used within a home network where access from the Internet side is blocked by the home router settings, a caution such as "This product must be used by connecting to a home router that securely controls accessibility from the Internet."

2.7 Obligation to Support Provision

For the validity period of the conformance label, the vendor is obligated to provide security patches/update files to address product defects and vulnerabilities (including alternative measures such as product replacement if security patches/update files cannot be provided) as support.

In principle, the validity period of STAR-1 is two years, but if support is known in advance at the time of application to be terminated within two years, the validity period is until the date of termination of support. If support is discontinued during the validity period, the conformance label will expire on the date of discontinuation of support (the validity period is until the date of implementation of support).

The reason for imposing the obligation to provide support during the validity period of the conformance label is to prevent the IoT product from continuing to be left uncorrected because a security patch/update file is not properly provided despite the discovery of a defect correction/vulnerability in the IoT product. Therefore, it is necessary that security patches/update files be provided equally to all users of the relevant IoT product, and therefore, one of the following is mandated as a method of providing support:

① Support will be provided free of charge to all users during the support period.

② Providing support for a fee is permitted only when a separate contract, such as a maintenance or sales contract, is made a condition of sale and the product is sold only to procurers who have concluded such a contract.

In the case of continued paid support after the expiration of the free support period, the conformance label shall be "Expired- The expiration date has passed," but information to the effect that "paid support is continued" may be included in the "Support Information" and "Update Information" fields.

3. STAR-1 Conformance Assessment Guide

This section is an assessment guide for each requirement of the STAR-1 Conformance to specifically determine whether the assessment result for that requirement is "Conforming (Y)," "Non-conforming (N)," or "Not Applicable (NA)." The evaluator shall conduct the assessment according to the contents described in this assessment guide and enter the result in the appropriate section of the STAR-1 checklist.

[Composition of the STAR-1 Conformance Assessment Guide]

The following structure is described for each conformance requirement:

[STAR-1 Conformance Requirement S1.1-xx]	conformance requirement number
Conformance Requirement	(Adapted from STAR-1-level Conformance Requirement and Assessment Methodology) Criteria for STAR-1 Conformance Requirement
Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement	(Adapted from STAR-1-level Conformance Requirement and Assessment Methodology) Conditions for being Not Applicable (NA) for the STAR-1 Conformance Requirement, and supplementary explanation of the Conformance Requirement. If a Decision of Not Applicable (NA) is made, the evaluator must retain evidence that the "Conditions for being Not Applicable (NA)" described in this item have been met.
Assessment Method	(Adapted from STAR-1-level Conformance Requirement and Assessment Methodology) Assessment methods for conformance assessment

STAR-1 Assessment Guide	
1. Conformance Assessment Criteria	The assessment items to be conducted to specifically determine whether the product is "Conforming (Y)" or "Non-conforming (N)" to such conformance requirement, and the criteria for determining "Conforming (Y)" are defined. The assessor should conduct the assessment according to the contents described in each assessment item and obtain the final judgment result. In addition, the documents and

	assessment reports used for the judgment should be kept as evidences.
2. Supplementary Explanation	
2.1 Supplementary Explanation of Conformance Assessment Criteria	Supplementary explanations of the contents of the conformance assessment criteria, supplementary explanations for conformance judgments and interpretation of the criteria, supplementary explanations of terminology, etc., are compiled for reference.
2.2 Conformance Decision in Exceptional Cases	Concept of conformance judgment in exceptional cases are summarized. It summarizes the criteria and supplementary explanations that apply only to IoT devices that fall under exceptional cases, and shows the approach for judging "Conforming (Y)" or "Non-conforming (N)" based on different judgment criteria than usual and for setting usage conditions, assuming that the devices are used in a limited usage environment.

[Description in STAR-1 checklist]

The checklist consists of an "Assessment Result Entry Sheet" on which the assessment results are entered for each conformance requirement and an "Assessment Result List" sheet. Note that the contents of the "Assessment Results Entry Sheet" will be automatically transferred to the "Assessment Results List" sheet.

The evaluator shall enter the results of the assessment conducted in accordance with the contents described in this Assessment Guide for each requirement of the conformance requirement in the "Assessment Result Entry Sheet." The contents to be filled in are as follows:

STAR-1 Conformance Criteria No.	S1.1-01
Assessment Results	Select "Conforming (Y)," "Non-Conforming (N)" or "Not Applicable (NA)."
Name of evidence	Describe the following information [Document assessment] ● Name of technical documents, etc., used in the assessment ● Name of internal documents, regulations, etc., used in the assessment

	[Device check] ● Names of information/documents (e.g., reports, photos, videos, screenshots, logs (system output)) that can confirm the results of the verification of the device check Reuse of check results conducted at the time of product development and assessment results at the time of obtaining other certifications are acceptable.
Evidence-based rationale/reasons for being Not Applicable (NA)	Describe the following information for each assessment item ● For assessments based on "document assessment": Information that shows the relevant part where the evidence based on the trail (evidence) is described (e.g., document name, document number, description part (e.g., page number, chapter number, URL) ● For assessments based on "device check": Summary of assessment results ● For "Not Applicable (NA)": The basis for determining that appropriate measures are being taken against the threat (why it is acceptable to determine that the assessment item is not applicable (NA) / why alternative measures are being taken) in accordance with the supplementary explanation.

[STAR-1 Conformance Requirement S1.1-01]

Conformance Requirement

Access control based on appropriate authentication shall be in place for access by other IoT devices or users to the information assets to be protected via IP communication to the IoT product.

Note that IoT products that have acquired technical standards conformity certification including technical standards for terminal equipment security based on the Telecommunications Business Act (IoT products to which the Technical Qualification [T] Mark or [A] Mark is granted) are deemed to be in conformance with this conformance requirement. In this case, the "Technical Standards Conformity Certification Number, etc., under the Telecommunications Business Act (Design Certification Number for the Technical Qualification [T] Mark or Technical Standards Conformity Certification Number for the [A] Mark)" shall be described on the JC-STAR label application form. (Please note that JC-STAR label application form is attached to the Assessment Guide in Japanese version only.)

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

No mechanism exists for authentication and access to the information assets to be protected via IP communication. (The rationale why user authentication is not required to counter unauthorized access from outside shall be described in the "Reasons for being NA" field.)

[Definition of Terms: information assets to be protected]

All of the following information:

- Setting information on communication functions
- Configuration information on security functions
- Generally sensitive information, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device

Assessment Method

- Document assessment: subject

It shall be assessed that the technical documentation of the IoT product clearly describes the method of access control based on appropriate authentication for access to the information assets to be protected from other IoT devices or users.

- Device check: None

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment result of the following document assessment is judged as "Conforming (Y)."

[Document Assessment]

It shall be assessed that the technical documentation of the IoT product clearly describes the method of access control based on appropriate authentication for access to the information assets to be protected from other IoT devices or users. Only when it is confirmed that the following assessment item 1 is satisfied, the assessment result of the document assessment of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

For IP communications necessary for the intended use of the IoT product (excluding the "exceptional protocols" listed below), ensure that both (1) and (2) below are satisfied for access to the information assets to be protected from other IoT devices or users.

(1) Access control based on appropriate authentication is in place, and only other IoT devices or users who are authorized to access the information assets to be protected are allowed to access such information assets.

(2) The authentication or access control method used is an implementation similar to or more advanced than any of the following items:

A) Implementation of user authentication with passwords used for user authentication in conformance with "STAR-1 Conformance Requirement S1.1-02"

B) Implementation of multi-factor authentication functionality using multiple authentication factors

C) Implementation of an authentication function using digital certificates

D) Implementation of authentication functionality through external authentication services based on standard authentication methods such as OpenID Connect

E) Implementation of a function to restrict the target of permitted communication by IP address, etc.

F) Implementation of a function to restrict communication to only devices within a LAN.

*) **Exceptional protocol**

Example 1: ARP, ICMP (because they are lower layer protocols than TCP/UDP)

Example 2: DHCP, DNS, NTP (because these protocols do not support authentication)

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1. Scope of users

The scope of users in Assessment Item 1-(1) must include all natural persons and organizations using the IoT devices that have access to the information assets to be protected in the IoT devices, such as users, administrators, vendor customer engineers, and owners of the IoT devices. In addition, any access must be denied to anyone who is not included in this scope.

If this condition is not met, the result of this conformance requirement is judged as "Non-conforming (N)."

2.1.2. Customer engineer certification

Conformance to this conformance requirement is also required for authentication of customer engineers.

However, it does not necessarily require the same authentication method or the same operation in the usage environment as general users. It is acceptable to adopt an authentication method exclusive for customer engineers that differs from the authentication method described in Assessment Item 1- (2), if the IoT product vendor judges that it is appropriate from security perspective because of the restriction of usage ports, access range, and customer engineer functions in the customer engineer's usage environment. In such cases, the vendor may exclude the assessment of Assessment Item 1-(2) by clearly stating in the technical documentation the basis for judging that the authentication method is appropriate from a security perspective (e.g., conditions for use restrictions) and an explanation of the authentication method adopted. In the absence of such a statement, Assessment Item 1-(2) must also be satisfied.

2.1.3. Scope of information assets to be protected

The target scope of information assets to be protected should be determined with reference to Section 2.4. In addition, the access control in the assessment item 1-(1) must function appropriately for the scope of the information. If it cannot be confirmed that the access control functions appropriately for the scope of the information, this conformance requirement shall be judged as "Non-conforming (N)."

In cases where generally sensitive information such as personal information is temporarily stored in caches or memory in IoT devices, such information may be excluded from the scope of "information assets to be protected" on the condition that a function to automatically erase such information after necessary processing or after a certain period of time is enabled by default, and that the IoT devices are used within a "protected network environment*)" is clearly indicated to the user. In such cases, the information may be excluded from the scope of "information assets to be protected" on the condition that the user is explicitly warned that the IoT device should be used within a "protected network environment*)." In this case, the rationale for the exclusion must be clearly stated in the evidence.

*) A protected network environment is a communication environment isolated from the Internet by devices that block communication from the Internet side (e.g., gateways, firewalls, Virtual Private Network devices).

2.1.4 Reuse of test results for products certified with the technical conformity mark

For products with the technical conformity mark ([T] mark or [A] mark) that meet the requirements of the technical standards for terminal equipment security (Article 34-10 of the Rules for Terminal Facilities) based on the Telecommunications Business Act, the document assessment in this conformance requirement may be substituted by the test results that were done when the product was certified for the technical conformity. In this case, the test results at the time of receiving the "Technical Standards Conformity Certification Number, etc., under the Telecommunications Business Act (i.e. Design Certification Number for [T] Mark or Technical Standards Conformity Certification Number for [A] Mark)" shall be retained as rationale based on the evidence.

2.2 Conformance Decision in Exceptional Cases

2.2.1. Alternative access control through network connection control of IoT devices

In STAR-1, if access control based on "network access authentication" is being implemented, which checks whether or not IoT device can connect to the network each time it connects, and even if the IoT device does not have access control functions based on "user authentication" or "device authentication," it is considered that "access control based on appropriate authentication" is being implemented if all of the following conditions (1) to (5) are met:

(1) On the condition that the connection is made within a closed network isolated from the Internet by a separate device such as a Virtual Private Network device or router, a connection availability check is performed each time the connection is made to the network.

(2) The device in (1) above must be configured to block the possibility of being connected to the IoT device from the Internet side (communication with the Internet is not permitted).

(3) It must be ensured that the user of the IoT device is an authorized user by some means. For example, the IoT device is placed in a location where only authorized users are allowed to enter.

(4) In manuals or other documents that are easy for users to obtain and check, there must be warnings to the effect that "only trusted users are allowed to use the system" and "the system must be connected to a device that blocks communication from the Internet side."

(5) The technical documentation shall clearly state that an access control function based on "network access authentication" is used instead of an access control function based on "user authentication" or "device authentication" and the functional mechanism of the access control function.

[STAR-1 Conformance Requirement S1.1-02]

Conformance Requirement

If IoT product uses passwords in the user authentication mechanism via the network and a default password is used at the time of installation of the IoT product, either of the following criteria (1) or (2) shall be satisfied.

(1) The default password shall be a unique value that differs for each IoT device and shall be at least 6 characters in length that cannot be easily guessed.

(2) For the default password, a function that requires the user to change the password at the first startup shall be implemented, and the user is required to set a password of 8 characters or more that can be set in such a function.

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

No mechanism for password-based user authentication over the network.

(The rationale why password-based user authentication is not necessary to counter threats shall be described in "Reasons for being NA" field.)

Assessment Method

- Document assessment: subject
  It shall be assessed that the technical documentation of IoT product clearly describes the measures for default passwords for the user authentication mechanism via network when installing the IoT product that uses passwords.
- Device check: None

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment result of the following document assessment is judged as "Conforming (Y)."

[Document Assessment]

It shall be assessed that the technical documentation of IoT product clearly describes the measures for default passwords for the user authentication mechanism via network when installing the IoT products that uses passwords. Only when it is confirmed that the implementation satisfies either of the following assessment items 1 or 2 regarding the default password, the assessment result of the document assessment of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

The default password shall be unique for each IoT device, and must be at least 6 digits, not falling under any of the following A) to D) below:

A) Passwords with common strings or simple patterns (e.g., "admin," "root," "QWERTY")

B) Easy-to-remember passwords using famous proper nouns, names of people, places, etc. (e.g., "baseball," "mustang," "michael")

C) Password based on an increasing counter (e.g., "123456," "aaaaaaaa," "1234abcd," "password1")

D) Passwords based on public information such as MAC address, Wi-Fi SSID, IoT product serial/model number, name (abbreviation), etc.

Assessment Item 2:

The default password is implemented with a function that requires the user to change the password the first time it is started, and the password that can be set in this function is enforced to be at least 8 characters long. In the case of IoT products that can be used without the network function, it is acceptable to require the user to change the password when using the network function for the first time, rather than at the time of initial startup.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1 Target user authentication

The user authentication covered by these conformance requirements is authentication by natural persons or organizations, and does not include authentication between devices (device authentication) for the purpose of coordination between devices. However, authentication based on knowledge information by a device, etc., used to access the target IoT device on behalf of the natural person is included in user authentication (and is not considered device authentication).

2.2 Conformance Decision in Exceptional Cases

2.2.1 Password handling for authentication of administrators and customer engineers

Authentication using passwords for administrators and IoT product vendor customer engineers during maintenance is also subject to assessment of this conformance requirement.

However, only when the user authentication using a password is performed by an administrator or customer engineer directly operating the maintenance interface or maintenance port on the IoT device without going through the network, such user authentication is not subject to this conformance requirement. In such a case, the rationale for the exclusion shall be clearly stated in the technical documentation.

2.2.2 Conformance Decision for IoT devices that have the ability to automatically connect to a network during installation

IoT devices that have a function to automatically connect to a network at the time of installation can be exceptionally designated as "Not Applicable (NA)" as devices that do not have a mechanism for user authentication via a network, only when all of the following conditions (1) through (3) are met. In this case, the rationale for the decision of "Not Applicable (NA)" shall be clearly stated in the evidence.

(1) There are no user accounts to authenticate via the Internet at the time of installation

(2) Default passwords are set for accounts that authenticate via local access only, not via the Internet.

(3) A caution to the effect that the IoT device is designed to be used within a "protected network environment*)" is clearly indicated.

*) A protected network environment is a communication environment isolated from the Internet by devices (e.g., gateways, firewalls, Virtual Private Network devices) that block communication from the Internet side.

[STAR-1 Conformance Requirement S1.1-03]

Conformance Requirement

It shall be possible to change the authentication value used for user authentication through the network to the IoT product, regardless of the type of authentication (e.g., password, token, fingerprint).

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

There is no mechanism for user authentication over the network. (The rationale why user authentication is not necessary to counter unauthorized access from outside shall be described in the "Reasons for being NA" field.)

[Definition of Terms: authentication value]

Individual values of attributes used in authentication mechanisms for IoT products. (e.g. For the password-based authentication mechanism, the authentication value is a string of characters. For the biometric fingerprint authentication, the authentication value is the fingerprint data of the index finger of the left hand, for example.)

Assessment Method

- Document assessment: subject
  It shall be assessed that the technical documentation of the IoT product clearly describes the method to change the authentication values used in user authentication for the IoT product.
- Device check: None

STAR-1 Assessment Guide

1. **Conformance Assessment Criteria**

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment result of the following document assessment is judged as "Conforming (Y)."

[Document Assessment]

It shall be assessed that the technical documentation of the IoT product describes changes of the authentication values used in user authentication of the IoT product. Only when it can be confirmed that both of the following assessment items 1 and 2 are satisfied, the assessment result of the document assessment of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

It shall be clearly stated that the authentication value can be changed regardless of the type of authentication (e.g., password, token, fingerprint).

Assessment Item 2:

Procedures for using the above functions shall be provided to users through manuals or other means.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1. Scope of user

The scope of user in this conformance requirement is for all those who perform user authentication via a network. It must include all natural persons or organizations that perform user authentication via a network with the relevant IoT device, such as users, administrators, vendor customer engineers, and owners of IoT devices, as well as devices that access IoT devices on behalf of natural persons. (Another device that is connected to the device in order for the devices to work together is not included as a user. In other words, device authentication is not included.). If this condition is not met, this conformance requirement is judged as "Non-conforming (N)."

2.2.2. Provide procedures for changing authorization values for specific users, such as customer engineers

In Assessment Item 2, it is acceptable to limit the applicable persons as to the "user" to whom the usage procedure for changing the authentication value is provided. In addition, the contents to be provided may differ depending on the different "users." What is important is that the user is able to change the authentication values related to the user authentication used by himself/herself and that the procedure for changing the authentication values is provided to the user, and it is not required to provide the procedure to change the authentication values that is related to the authentication used by other users.

For example, user authentication used by customer engineers may be interpreted as "user = customer engineer (not including general users)." In this case, the procedure for changing the authentication value should be described in the manual for customer engineers, etc., and need not be described in the manual for general users. The same applies to user authentication used by system administrators.

2.2 Conformance Decision in Exceptional Cases

Not applicable

[STAR-1 Conformance Requirement S1.1-04]

Conformance Requirement

If the IoT device is not a constrained device, the IoT device shall employ the mechanism of user authentication over the network to the IoT device that make brute force attack difficult.

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable **(NA)]**

One of the following conditions applies. (OR Condition)

- There is no mechanism for user authentication over the network for IoT devices. (The rationale why user authentication is not necessary to counter unauthorized access from the outside shall be described in the "Reason for being Not Applicable (NA)" field.)
- The IoT device falls under the category of "constrained device. " (The rationale why the device falls under the category of "constrained device " shall be described in the "Reason for being Not Applicable NA" field.)

[Definition of Terms: constrained device]

Device that has physical constraints for its intended use, either in its ability to process data, communicate data, store data, or interact with the user.

Assessment Method

- Document assessment: None
- Device check: subject

  Through device check, it shall be assessed that the mechanism for user authentication via the network for the IoT devices employ a mechanism that makes brute force attacks difficult.

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment result of the following device check is judged as "Conforming (Y)."

[Device check]

Through device check on the target IoT devices, it shall be assessed that the mechanism for user authentication via the network for the IoT devices is a mechanism that makes brute force attacks difficult. Only when it can be confirmed that the mechanism similar to or better than one of the following assessment items 1 or 2 is implemented, the assessment result of the device check for this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

For user authentication via a network, in the event of a "certain number*)" of consecutive authentication attempts being unsuccessful, the following authentication attempt restrictions shall be applied:

A) Prohibition of additional authentication

B) Suspension of authentication for a certain period of time

C) Constant time delay in issuing authentication response

*) Certain number shall be the value that is specific value (one or more times) to IoT device or the value that was assigned by the administrator within the scope of acceptable value.

Assessment Item 2:

Multi-factor authentication shall be used.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1. Authentication attempt limitations on failed authentication attempts

In Assessment Item 1, the restriction of authentication attempts upon a certain number of consecutive failed user authentication attempts is required only for accounts that have failed authentication, and not necessarily for the authentication function of IoT device itself. If it can be confirmed through a device check that there are restrictions on authentication attempts for accounts that have failed authentication, it can be judged that assessment item 1 has been met.

2.2 Conformance Decision in Exceptional Cases

Not applicable

[STAR-1 Conformance Requirement S1.1-05]

Conformance Requirement

The manufacturer shall make publicly available (e.g. post on the manufacturer's website) a vulnerability disclosure policy that includes all of the following information (1) through (3) below:

(1) Contact information for reporting IoT product security issues to the manufacturer (e.g., Web site URL of the manufacturer etc., phone number, email address)

(2) Procedures and overview of what manufacturer does after receiving reports on the security of IoT product

(3) Procedures and overview of what manufacturer does for status updates of the IoT product and vulnerability until the vulnerability is resolved.

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

None

Assessment Method

- Document assessment: subject
  It shall be assessed that the vulnerability disclosure policies are clearly stated on IoT product websites or the other user-accessible media.
- Device check: None

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment result of the following document assessment is judged as "Conforming (Y)."

[Document Assessment]

It shall be assessed that the vulnerability disclosure policy is clearly stated on the IoT product's website or the other user-accessible media. Only when it is confirmed that all of the following assessment items 1 to 4 are satisfied, the assessment result of the document assessment of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

The vulnerability disclosure policy shall include contact information (e.g. manufacturer's website URL, phone number, email address) for reporting to the manufacturer regarding security issues of the IoT product.

Assessment Item 2:

The vulnerability disclosure policy shall include a description of the procedures that the manufacturer will follow after receiving a report on the security of an IoT product, as well as an overview of these procedures. (It is not necessary to disclose detailed procedures, etc., but it is necessary to disclose an overview of how the manufacturer will receive reports on security, what procedures and methods will be used to contact the reporter after that, what response will be made to the report, a declaration of legal immunity for good-faith reports, etc.)

Assessment Item 3:

The vulnerability disclosure policy shall include a description of the procedures and an outline regarding the updating of the status of IoT products and vulnerabilities until the vulnerability is resolved. (it is not necessary to disclose detailed procedures, etc., but it is necessary to disclose an overview of how investigations and countermeasures will be carried out until the vulnerability is resolved, how the situation will be managed and disclosed, and what kind of response will be made to the reporter.)

Assessment Item 4:

It should be verified that the Vulnerability Disclosure Policy is posted in a user-accessible medium. As evidence that the policy is posted in a user-accessible medium, the location where the vulnerability disclosure policy is posted is to be described in the checklist.

However, only in the case that the IoT product has not yet been released for sale and whose vulnerability disclosure policy is not publicly available at the time of assessment, if a document specifying the vulnerability disclosure policy to be released and information on the expected release (e.g. URL and location of planned release) shall be prepared as evidence, and the following information shall be included in the "Rationale based on evidences," this assessment item can be considered to be confirmed.

The following statement shall be included

A) Scheduled release date (must be prior to the IoT product sales date)

B) Method and Location of Publication

C) Vulnerability Disclosure Policy you plan to disclose (can be attached separately)

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

Not applicable

2.2 Conformance Decision in Exceptional Cases

Not applicable

[STAR-1 Conformance Requirement S1.1-06]

Conformance Requirement

All of the following criteria (1) through (3) shall be met for the update function of software components of the IoT product:

(1) The firmware (software) package of the IoT product shall be updatable.

(2) The firmware (software) package shall have a means to verify that the latest firmware (software) is installed, e.g., the IoT product implements a function to check the version of the firmware (software) package.

(3) The version of the updated firmware (software) package shall be kept after the power is turned off.

Note that IoT products that have acquired technical standards conformity certification including technical standards for terminal equipment security based on the Telecommunications Business Act (IoT products to which the Technical Qualification [T] Mark or [A] Mark is granted) can be deemed to be in conformance with this

Conformance Requirement. In this case, the "Technical Standards Conformity Certification Number, etc., under the Telecommunications Business Act (Design Certification Number for the Technical Qualification [T] Mark or Technical Standards Conformity Certification Number for the [A] Mark)" shall be described on the JC-STAR label application form. (Please note that JC-STAR label application form is attached to the Assessment Guide in Japanese version only.)

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

None

Assessment Method

- Document assessment: None
- Device check: subject

  It shall be assessed the update functions for software components included in the target IoT products by device check.

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y) " will be made only when the assessment result of the following device check is judged as "Conforming (Y)."

[Device check]

The update function for software components of the target IoT product shall be evaluated by device check. Only when it is confirmed that all of the following assessment items 1 - 3 are satisfied, the assessment result of the device check of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

The update operation shall be performed on the firmware (software) package of the IoT product, and the update shall be able to be completed successfully.

Assessment Item 2:

The firmware (software) package shall have a means to verify that the latest firmware (software) is installed, e.g., having a function to check the version of the firmware (software) package.

Assessment Item 3:

The version of the updated firmware (software) package shall be kept after the power is turned off.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1. Method of updating to be checked in assessment item 1

There are three update methods: (1) automatically initiated, (2) manually performed by the user, and (3) performed only by maintenance personnel such as customer engineers or privileged users who explicitly have management responsibility. In Assessment Item 1, conformance judgments shall be conducted for all update methods implemented in the relevant IoT devices.

2.1.2 How to check the latest firmware (software) version in Assessment Item 2

There are several measures to check that the latest firmware (software) has been updated as follows. It is not necessarily required that IoT devices have function to display the "firmware (software) version."

Example 1: The firmware (software) version information and installation status are displayed on the IoT device display to verify that the firmware (software) installed on the IoT device is the latest.

Example 2: The firmware (software) version information and installation status are displayed on the connected PC or smartphone to verify that the firmware (software) installed in the IoT device is the latest.

Example 3: The status of LEDs, etc., mounted on IoT devices lighting up or blinking shows whether the latest firmware (software) is installed in the IoT device, although version information is not displayed.

Example 4: The firmware (software) version checking tool on the company's website enable to check whether the latest firmware (software) is installed in the IoT device by using the tool.

2.1.3 Scope of software components requiring updates

In this conformance requirement, software components that need to be updated are software components for which security measures need to be implemented, and the target is selected by the IoT product vendor. Such software components specifically include firmware (software) that has security functions and requires security patches to be provided to maintain security functions when security defects or vulnerabilities are discovered.

At a minimum, the firmware (software) listed in the application form shall always be eligible for updating.

2.1.4 Reuse of test results for products certified with the technical conformity mark

For products with the technical conformity mark ([T] mark or [A] mark) that meet the requirements of the technical standards for terminal equipment security (Article 34-10 of the Rules for Terminal Facilities) based on the Telecommunications Business Act, the assessment based on device check in this conformance requirement can be substituted by the test results that was done when the product was certified for the technical conformity. In this case, the test results at the time of receiving the "Technical Standards Conformity Certification Number, etc., under the Telecommunications Business Act (i.e. Design Certification Number for [T] Mark or Technical Standards Conformity Certification Number for [A] Mark)" shall be retained as rationale based on the evidence.

2.2 Conformance Decision in Exceptional Cases

2.2.1. Alternative update without update function

Some IoT devices may not have update functions for software components included in IoT products due to some restrictions or business reasons. However, even such IoT devices shall provide some measures (alternative updates) to maintain security functions when security defects or vulnerabilities are discovered.

Therefore, in cases where updates cannot be performed despite software components requiring security measures, as an alternative to testing on actual equipment, by documenting the reason why updates cannot be performed and the appropriate alternative measures to replace updates when vulnerabilities are discovered and retaining as evidence, conformance requirement can be judged as "Conforming (Y)."

If appropriate alternative measures to correct the vulnerability cannot be provided, this conformance requirement is judged as "Non-conforming (N)."

Examples of case that requires alternative updates that do not use the update function

Example 1: The IoT device uses bootloader-like software that is written only once at the time of manufacture and cannot be updated thereafter

Example 2: Multiple microcontrollers are built into IoT devices, and some of the software on them is not rewritable.

Example 3: Software updates are prohibited or restricted by law or regulation

Example 4: Physical resource constraints on the IoT device do not allow the update function to be implemented in the IoT device.

Example 5: For business reasons, instead of incorporating an update function in IoT devices, an alternative update, such as replacing the device with an alternative device that supports the vulnerability, is performed.

[STAR-1 Conformance Requirement S1.1-07]

Conformance Requirements

It shall be enabled for users to perform software updates in an easy and understandable procedure when applying updates.

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

None

Assessment Method

- Document assessment: subject
  It shall be assessed that easy and understandable procedures for software updates are clearly stated in the user-accessible media (e.g., manuals, websites of IoT product).
- Device check: None

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment result of the following document assessment is judged as "Conforming (Y)."

[Document Assessment]

It shall be assessed that easy and understandable procedures for software updates are clearly stated in the user-accessible media (e.g., manuals, websites of IoT product).

Only when it is confirmed that the procedure for updating the software (it is acceptable to use multiple update methods) is clearly stated the procedure similar to any of the following assessment items 1 to 4, the assessment result of the document assessment for this conformance requirement will be judged as "Conforming (Y)."

Assessment Item 1:

It shall be clearly stated that the update will be performed automatically. In addition, it shall be clearly stated what to do if the automatic update fails.

Assessment Item 2:

The procedure for users to perform updates using the IoT product's associated services (e.g., mobile applications) shall be clearly defined.

Assessment Item 3:

The procedure for users to perform updates via the IoT product interface (e.g., web interface) shall be clearly defined.

Assessment Item 4:

The procedure for users to download the update file from the IoT product vendor's website and to perform the update by installation shall be clearly stated.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1. "Easy and understandable procedures"

The easy and understandable procedure required by this conformance requirement means a procedure that is designed so that even users who do not have expert knowledge can usually successfully update the software by following the instructions of the installer, manuals, work procedures, etc.

2.1.2. Updates by customer engineers

Software updates by customer engineers are also subject to this conformance requirement.

However, in this case, the scope of disclosure of the update procedure is limited to between the IoT product vendor and the customer engineer, and it is sufficient if the update procedure is clearly indicated on a medium that the customer engineer can access, so there is no need to disclose it to general users.　In addition, as for "the procedure is easy and straightforward," if the customer engineer can perform the update without any problems, that would be sufficient.

Based on this premise, an assessment of the software update by the customer engineer shall be conducted.

2.2 Conformance Decision in Exceptional Cases

Not applicable

[STAR-1 Conformance Requirement S1.1-08]

Conformance Requirement

When updating software via a network, there shall be a mechanism to verify software integrity prior to updating.

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

No mechanism exists to update software over the network. (The assumed update mechanism shall be described in the "Reason for being an NA" field.)

Assessment Method

- Document assessment: subject
  It shall be assessed that the technical documentation of the IoT product clearly describes the implementation of a mechanism to verify software integrity prior to updating.
- Device check: None

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment result of the following document assessment is judged as "Conforming (Y)."

[Document Assessment]

It shall be assessed that the technical documentation of the IoT product clearly indicates the implementation of a mechanism to check the integrity of the software before updating. Only when the implementation of a mechanism similar to or beyond any of the following assessment items 1 to 4 are clearly stated, and when it is confirmed that assessment item 5 is satisfied, the assessment result of the document assessment of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

It shall be clearly stated that the hash value assigned to the update software is checked against the hash value before or during installation of the update software, and that if a mismatch is detected as a result of the check, the installation will be terminated.

Assessment Item 2:

It shall be clearly stated that the digital signature assigned to the update software is verified before or during the installation of the update software, and that if the verification results show NG, the installation will be terminated.

Assessment Item 3:

It shall be clearly stated that the hash value assigned to the update software is checked against the hash value in the associated application on the PC, smartphone, etc., before installing the updated software, and that if a mismatch is detected as a result of the check, the installation will be terminated.

Assessment Item 4:

It shall be clearly stated that the associated application on the PC, smartphone, etc., is verified by the digital signature assigned to the update software before installing the update software, and that if the verification results show NG, the installation will be terminated.

Assessment Item 5:

For hash functions and digital signatures used in assessment items 1 to 4, the algorithm listed in the "e-Government Recommended Ciphers List" of "The list of ciphers that is referred to in the procurement for the e-Government system (CRYPTREC Ciphers List) " shall be used.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

Not applicable

2.2 Conformance Decision in Exceptional Cases

Not applicable

[STAR-1 Conformance Requirement S1.1-09]

Conformance Requirement

The manufacturer shall document policies and guidelines for prioritizing security updates for the purpose of rapid updates to security issues.

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

None

Assessment Method

- Document assessment: subject
  It shall be assessed that the organization's rules, policies, procedures, etc., or technical documentation of IoT products clearly state policies and guidelines for determining security update priorities.
- Device check: None

STAR-1 Assessment Guide

1. Conformance Asessment Criteria

For this conformance requirement, the final Decision of "Conforming (Y)" will be made only when the assessment result of the following document assessment is judged as "Conforming (Y)."

[Document Assessment]

The organization's rules, policies, procedures, etc., or the technical documentation for IoT products shall clearly state the policies and guidelines for determining the priority of security updates. Only when it is confirmed that all of the following assessment items 1 to 3 are satisfied, the assessment result of the document assessment for this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

Guidelines for determining the severity and importance of the vulnerabilities to be addressed and the types of vulnerabilities (e.g., firmware, hardware, software) to determine the priority of security updates shall be described.

Assessment Item 2:

The organizational structure for handling incident response (e.g., PSIRT, incident response system) and a series of response processes and policies, including vulnerability information collection, triage and analysis, countermeasures, and updates, shall be described.

Assessment Item 3:

In the case of a product that is developed and operated by multiple stakeholders, the system for communication among stakeholders (contact information, method of communication, etc.) shall be described.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1. Contents required in assessment item 1

The timeliness of providing security updates depends on the impact and severity of the vulnerability to be addressed, whether it has already been used in an attack, and the difficulty of response. Therefore, in Assessment Item 1, for example, in order to determine whether to respond with "emergency updates" or "planned updates," a decision flow and policy should be documented in terms of "by what criteria," "what happen" and "what to do."

2.2 Conformance Decision in Exceptional Cases

Not applicable

[STAR-1 Conformance Requirement S1.1-10]

Conformance Requirement

The model number of the IoT product shall be provided to the user in one of the following measures

(1) The model number of the IoT product is labelled directly on the IoT product itself.

(2) Users can recognize the model number by the GUI, web UI, etc., of the IoT product or the GUI, web UI, etc., of software or applications (e.g., smartphone apps) associated with the IoT product.

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

None

Assessment Method

- Document assessment: None
- Device check: subject
  Assess whether a method is provided for users to confirm the model number of the IoT product.

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment result of the following device check is judged as "Conforming (Y)."

[Device check]

It shall be assessed that a method to allow user to confirm the IoT product model number is provided to the user. Only when it can be confirmed that either of the following assessment items 1 or 2 is satisfied, the assessment result of the device check of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

The IoT product itself shall be verified and the model number of the IoT product shall be labelled.

Assessment Item 2:

It shall be possible to confirm the model number of the relevant IoT product by actually accessing the GUI, web UI, etc., of the IoT product or the GUI, web UI, etc., of software or applications (smartphone apps, etc.) associated with the IoT product.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

Not applicable

2.2 Conformance Decision in Exceptional Cases

Not applicable

[STAR-1 Conformance Requirement S1.1-11]

Conformance Requirement

Information assets to be protected that are stored in the storage of IoT products (including information assets to be protected that are stored on storage media such as SD cards) shall be stored securely.

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

None

[Definition of terms: information assets to be protected]

All of the following information:

- Configuration information on communication functions
- Configuration information on security functions
- Generally sensitive information, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device

Assessment Method

- Document assessment: subject
- It shall be assessed that the technical documentation of IoT products clearly describes that the information assets to be protected that are stored in the storage of IoT products (including information assets to be protected that are stored on storage media, such as SD cards, etc.) are securely stored.
- Device check: None

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final Decision of "Conforming (Y)" will be made only when the assessment result of the following document assessment is judged as "Conforming (Y)."

[Document Assessment]

In the technical documentation of IoT products, it shall be assessed that information assets to be protected that are stored in the storage of IoT products (including cases where they are stored on storage media) are securely stored. Only when it is confirmed that the following assessment items 1 to 5 or equivalent/better protection measures, the assessment result of the document assessment for this conformance requirement will be judged as "Conforming (Y)." (Different measures may be adopted for each information asset. Multiple measures may also be used in combination.)

Assessment Item 1:

Information assets to be protected that require confidentiality shall be stored after being encrypted using encryption methods that employ cryptographic techniques listed in the "e-Government Recommended Ciphers List" of "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List), " or after being hashed using message digests that employ cryptographic techniques listed in the "e-Government Recommended Ciphers List."

Assessment Item 2:

Information assets to be protected that require integrity protection shall be stored in a form where data integrity can be confirmed by signatures using cryptographic techniques listed in the "e-Government Recommended Ciphers List" of "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List)."

Assessment Item 3:

Information assets to be protected that require integrity protection shall be stored in a form where data integrity can be confirmed by message digests using cryptographic techniques listed in the "e-Government Recommended Ciphers List" of "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List)."

Assessment Item 4:

Information assets to be protected shall be stored in a secure area using virtualization technology, a sandbox provided as a function of an operating system such as iOS/Android, or a security chip.

Assessment Item 5:

The information assets to be protected shall be stored in a storage area that cannot be easily removed and is embedded in the IoT device, and on the storage area, data cannot be directly read or written via an externally invoked interface or there is no such interface.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1. Target information assets to be protected

The target information assets to be protected that are required to be securely stored in this conformance requirement are all information assets that IoT product vendors have judged to be "information assets to be protected" with reference to the concept of information assets to be protected (to be protected) in Section 2.4. All of the targeted information assets are required to be stored using one of the methods indicated in the assessment items 1 to 5. (Different methods may be used for different information assets. Multiple methods may also be used in combination.)

Information assets that are temporarily stored in caches or memory for the convenience of processing in IoT devices may be excluded from the scope of information assets to be protected on the condition that the following security measures are implemented. In such cases, the security measures to be implemented shall be specified in technical documents as a basis for exclusion from information assets to be protected. In the absence of such specification, the information assets cannot be excluded from the scope of the information assets to be protected.

Example 1: The IoT device is used within a protected network environment, isolated from the Internet

Example 2: The IoT device implements appropriate access control to the information assets to be protected

Example 3: The IoT device automatically erases the information assets after completion of processing or after a reasonable period of time

2.1.2. Not easily removable storage area embedded in IoT devices in Assessment Item 5

Not easily removable storage areas embedded in IoT devices are storage areas such as nonvolatile memory (e.g., flash ROM) directly mounted on the substrate. This does not include HDDs, SSDs, or other storage area that can be removed even if stored in a housing.

2.1.3. Area where direct data reading/writing via externally invoked interfaces is not possible in assessment item 5

An area where data cannot be read or written data directly via an externally invoked interface is a storage area that data can only be read or written by software components that do not have an externally invoked interface (boot monitor, BIOS, etc.), and other software components cannot read/write, either directly or indirectly.

2.2 Conformance Decision in Exceptional Cases

Not applicable

[STAR-1 Conformance Requirement S1.1-12]

Conformance Requirement

For information assets to be protected that are transmitted over a network, one of the following protection measures against information interception shall be in place

(1) For information assets to be protected that are transmitted over a network to other IoT devices and servers (including servers in the cloud), the IoT device itself takes protective measures against information eavesdropping.

(2) Information assets to be protected that are transmitted over a network to other IoT devices or servers (including servers in the cloud) are transmitted only in a protected communication environment (Virtual Private Network environment or connection environment via a leased line).

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

There are no information assets to be protected that are transmitted over the network. (The rationale why there are no information assets to be protected that are transmitted over the network shall be described in the "Reason for being NA" field.)

[Definition of terms: information assets to be protected]

All of the following information:

- Configuration information on communication functions
- Configuration information on security functions
- Generally sensitive information, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device

Assessment Method

- Document assessment: subject
  It shall be assessed that the technical documentation of IoT products clearly describes the implementation of protection measures against information eavesdropping for information assets to be protected that are transmitted over the

network; if there is an application that works with IoT products, the information transmitted from the application shall also be assessed as an information asset to be protected.

- Device check: None

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final Decision of "Conforming (Y)" will be made only when the assessment result of the following document assessment is judged as "Conforming (Y)."

[Document Assessment]

It shall be assessed that the technical documentation of IoT products clearly describes the protection measures against information eavesdropping those are implemented for information assets to be protected that are transmitted over a network; if there is an application that works with IoT products, the information transmitted from the application shall also be assessed as an information asset to be protected. Only when it is confirmed that both of the following assessment items 1 and 2 are satisfied, or when it is confirmed that assessment item 3 is satisfied, the assessment result of the document assessment of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

Either A) or B) below shall be clearly indicated in the technical documentation.

A) It shall be clearly described that the data will be transmitted using a communication protocol that employs a cryptographic technique listed in the "e-Government Recommended Ciphers List" of "The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List)."

B) It shall be clearly described that information assets to be protected that are encrypted in accordance with assessment item 1 of "STAR-1 Conformance Requirement S1.1-11" shall be transmitted over a network without decryption.

Assessment Item 2:

The technical documentation shall clearly describe that the "default setting" of the protection measures against information interception is set to be "Enabled."

Assessment Item 3:

In the manuals, websites, and other user-accessible media of the IoT product, it shall be clearly indicated for users to use the IoT product only in a protected communication environment (Virtual Private Network environment, connection environment via a dedicated line, or physically/logically protected network environment).

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1. Communication between IoT devices and associated services via the Internet

When communication between IoT devices and associated services is performed via the Internet or via communication paths that can be connected from the Internet, the information assets to be protected that are communicated between IoT devices and associated services also fall under "information assets to be protected that are transmitted over a network" in this conformance requirement. Therefore, protective measures against eavesdropping shall be also taken for communications between IoT devices and associated services in such a usage environment.

On the other hand, STAR-1 does not require protection measures for communications between IoT devices and associated services that do not involve the Internet.

2.2 Conformance Decision in Exceptional Cases

2.2.1. Handling when using in an environment where communication with the Internet is not possible

As shown in the concept of the scope where secure communication is required (or can be excluded) in Section 2.6, for STAR-1, if an IoT device is placed in a closed network that is isolated from the Internet by a Virtual Private Network device, router, etc., and the possibility of being connected from the Internet side by that device can be blocked (communication with the Internet is not permitted), it is judged that the necessary protective measures against unauthorized access from the Internet have been taken even if the communication is not encrypted.

Therefore, as a protective measure against eavesdropping of information in this conformance requirement, instead of encryption of communication, it is considered to satisfy Assessment Item 3, provided that users are clearly warned to "connect to and use a device that blocks communication from the Internet side."

2.2.2. Concept of Assessment Item 2 on initial setup

Protective measures against eavesdropping shall be "enabled" by default at the time of IoT product shipment. However, in the exceptional case where both of the following conditions A) and B) are met, by documenting the procedure and retaining it as evidence, even if "protection measures are invalid at the time of shipment of the IoT product," it is deemed that "protection measures against eavesdropping are valid" by changing the initial settings at the time of installation of the IoT device.

A) Installation of IoT devices by the installation operator is assumed (it is documented in manuals, etc., that only the installation operator or system administrator install the IoT devices).

B) The installation work instructions, manuals, or other documents indicate a caution/warning that the IoT device should be configured to "enable protection against eavesdropping" at the time of installation.

The intention is to minimize the risk of "omissions of activating protection measures against eavesdropping" by limiting the installation workers to "installation operators or system administrators" and by making it a procedure to "activate protection measures against eavesdropping" as part of the installation work when activating protection measures during the installation of IoT devices. On the other hand, if the installation work cannot be limited to "installation operators or system administrators," even if the instructions and warnings of "enabling the protection measures against eavesdropping" in the installation work are described in instructions and manuals, etc., it is not cleat that will be implemented as they are, and there is a considerable risk of "omission of enabling settings." So, if condition A) is not met, "protection measures shall be enabled at the time of shipment of the IoT product."

[STAR-1 Conformance Requirement S1.1-13]

Conformance Requirement

In order to reduce the risk of external cyber attacks on IoT products, interfaces that are unnecessary for the use of IoT products and at risk of being attacked shall be disabled, and vulnerability tests shall be performed on IoT products. Specifically, all of the following criteria (1) and (2) shall be met.

(1) In IoT products, for the interfaces that are used frequently and are assumed risks of vulnerability, the following interfaces which is unnecessary to use the IoT product and at a risk of being attacked shall be disabled.

(A) TCP/UDP port
(B) Bluetooth
(C) USB

(2) Vulnerability inspection shall be conducted against the IoT product using vulnerability scanner and no vulnerabilities that could be exploited in an attack are detected.

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

None

Assessment Method

- Document assessment: subject
  In the technical documentation of IoT products, it shall be confirmed and evaluated that all interfaces used in IoT products are identified, that the purpose of use, etc., are clarified, and that no unnecessary items for the use of IoT products are included. In addition, when using ports that are particularly at risk of being misused in attacks, it shall be assessed that whether the technical documentation clearly describes that the system has a management process in place to monitor the attack status and take appropriate action as necessary.
- Device check: subject
  It shall be assessed that interfaces that are unnecessary for the use of IoT products are disabled and that vulnerabilities that could be exploited in attacks are not detected by device check using port scanner and vulnerability scanner.

In principle, both document assessment and device check shall be conducted. However, if there is no recommended port scanner or vulnerability scanner, the device check can be excluded (document assessment only).

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment results of both the following document assessment and device check are judged as "Conforming (Y)."

[Document Assessment]

In the technical documentation of IoT products, it shall be confirmed and assessed that all interfaces used in IoT products are identified, that the purpose of use, etc., are clarified, and that those unnecessary for the use of IoT products are not included. In addition, when using ports that have a particularly high risk of being misused for attacks, it shall be assessed that the technical documentation clearly describes that the management process is in place to monitor the attack status and take appropriate actions as necessary. Only when it is confirmed that all of the following assessment items 1 to 3 are satisfied, the assessment result of the document assessment of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

The technical documentation shall include a description of the target interface for the IoT product.

A) TCP/UDP Port

For inbound communications, for the TCP and UDP ports that are open (LISTEN) the target port number, communication protocol, usage, timing of releasing, and usage conditions (for products that support IPv6, both IPv4 and IPv6 shall be supported) are described, and the ports that are not necessary for use or the ports for which the purpose of use is unclear are not included.

B) Bluetooth Profile

If the IoT product uses Bluetooth, the Bluetooth profile to be used and the purpose of use shall be clearly described, and no unnecessary profiles for use are included.

C) USB class

If the IoT product uses USB, the class name of the USB device class to be used, the purpose of use shall be clearly described, and no unnecessary USB device classes for use are included.

Assessment Item 2:

If there are any interfaces that are physically disabled by the IoT product, the interfaces that are disabled and the method of disabling shall be clearly described in the technical documentation. If there are no such interfaces, it shall be explicitly described that "There are no interfaces that are physically disabled."

Assessment Item 3:

In the technical documentation, if ports with a particularly high risk of being exploited for attacks (e.g., telnet (23/TCP and 2323/TCP)) are used, there shall be a description of the management process that allows the attack situation to be monitored and appropriate action to be taken if necessary. If no such ports are used, it shall be clearly described that "Ports with a particularly high risk of being exploited for attacks are not used."

[Device check]

The assessment is based on a device check using a port scanner and vulnerability scanner, targeting the following interfaces: (A) TCP/UDP port, (B) Bluetooth, and (C) USB, and assessing whether interfaces that are not required for the use of the IoT product have been disabled and whether vulnerabilities that could be exploited in an attack are not detected.

Only when it is confirmed that both of the following assessment items 4 and 5 are satisfied ("Passed"), the assessment result of the device check of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 4:

It shall be checked with a port scanner that the interfaces that are not required for the use of IoT products have been disabled for TCP and UDP ports.　In particular, confirm that all ports other than the TCP and UDP ports specified as open in Assessment Item 1 are disabled. If no TCP or UDP ports that are not open and not disabled are detected, this assessment item is "Passed," and if even one is detected, this assessment item is "Failed."

Assessment Item 5:

It shall be confirmed the absence of vulnerabilities in both i) and ii) below using a vulnerability scanner. If there is no recommended vulnerability scanner (currently Bluetooth and USB), then iii) shall be performed as an alternative to vulnerability testing.

If it is confirmed that there is no vulnerability, this assessment item is "Passed"; if it is not confirmed, it is "Failed." However, please note that if a vulnerability is detected in either i) or ii), an additional analysis and assessment under Assessment Item 6 will be conducted, and if all vulnerabilities detected are confirmed as "no vulnerability issues," this assessment item will be marked as "Passed."

i) It shall be confirmed that no CVSSv3 Criteria Severity 7.0 or higher vulnerabilities are detected for open TCP and UDP ports.

ii) If configurations or functions that use the http/https protocol are implemented, it shall be confirmed that vulnerabilities corresponding to the known vulnerabilities CVE-ID listed in the URL below are not detected.
[URL].
NIST: NATIONAL VULNERABILITY DATABASE
https://nvd.nist.gov/vuln/search
[search conditions].
Search Type：Advanced
Category: All of the following are targeted: "CWE-78 OS Command Injection," "CWE-89 SQL Injection," "CWE-352 Cross-Site Request Forgery (CSRF)," "CWE-22 Path Traversal."

iii) If there is no recommended vulnerability scanner, the following checks shall be performed.

- Bluetooth:

Bluetooth profiles other than those specified as the Bluetooth profiles to be used in assessment item 1 are not available or are set to default disable, and obsolete Bluetooth profiles are not available.

- ➢ USB:
  Device classes other than those specified as USB device classes to be used in assessment item 1 are unavailable or set to default disable.

Assessment Item 6:

If a vulnerability is detected in either i) or ii) of Assessment Item 5, the following analysis and assessment shall be performed for all detected vulnerabilities to confirm that the vulnerability is not a problem for the use of the relevant IoT devices. If it is confirmed that there is no problem for all detected vulnerabilities, it is judged as "no vulnerability problem."

- Analysis of whether the vulnerabilities detected are false positives or not, and assessment of whether the vulnerabilities are safe for the use of the IoT devices.
- Analysis of whether the vulnerability can be considered to have already been addressed through measures including operational measures, and assessment of whether such measures prevent the vulnerability from causing problems in the use of the IoT device.
- Analysis of whether it is proved that the detected vulnerability has no impact in the actual usage environment of the IoT device, and evaluation to prove that there is no impact.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1. Examples of methods to disable interface

There are two methods of disabling an interface: "physically disabling" and "logically disabling."

Physical methods of disabling refer to measures that prevent attackers from easily accessing physical ports, such as the following.

Example 1: The interface is inside an enclosure, and the enclosure cannot be easily opened by screwing it down, etc.

Example 2: The interface is inaccessible by means of a screwed lid

Logical method of disabling refer to measures that prevent an attacker from accessing the logical port unless the attacker illegally changes the software configuration (i.e., installs new software or changes the settings), such as the following.

Example 3: No driver is installed
Example 4: No unnecessary TCP/UDP ports are enabled
Example 5: No unnecessary Bluetooth profiles are installed
Example 6: No unnecessary USB classes are installed

2.2 Conformance Decision in Exceptional Cases

Not applicable

[STAR-1 Conformance Requirement S1.1-14]

Conformance Requirement

When the power supply and network functionality are turned off and restored due to a power outage or other reason, the authentication values (passwords, private keys, etc.) used for access control and the software that has completed the setting and updating shall maintain the state immediately before the power was turned off without returning to the initial factory settings.

Note that IoT products that have acquired technical standards conformity certification including technical standards for terminal equipment security based on the Telecommunications Business Act (IoT products to which the Technical Qualification [T] Mark or [A] Mark is granted) are be deemed to be in conformance with this conformance requirement. In this case, the "Technical Standards Conformity Certification Number, etc., under the Telecommunications Business Act (Design Certification Number for the Technical Qualification [T] Mark or Technical Standards Conformity Certification Number for the [A] Mark)" shall be described on the JC-STAR label application form. (Please note that JC-STAR label application form is attached to the Assessment Guide in Japanese version only.)

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

None

Assessment Method

- Document assessment: None

- Device check: subject
  It shall be assessed by conducting device check for IoT products that have software updated and have changed the authentication values used for access control from factory defaults.

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment result of the following device check is judged as "Conforming (Y)."

[Device check]

The assessment shall be performed on IoT products that have changed the authentication values used for access control and updated software since shipment from the factory by device check. Only when it is confirmed that both of the following assessment items 1 and 2 are satisfied, the assessment result of the device check for this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

After turning off the power supply of the IoT product (in the case of battery-powered products, the power supply should be turned off by disconnecting the battery) and then restoring it, the product shall not revert to the factory default state, and the authentication values and updates immediately prior to the power being turned off shall be maintained.

Assessment Item 2:

After disconnecting and then reconnecting the communication cable or wireless connection, the product shall not revert to the factory default state, and the authentication values and updates immediately prior to the power being turned off shall be maintained.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1 Reuse of test results for products certified with the technical conformity mark

For products with the Technical Conformity Mark ([T] Mark or [A] Mark) that meet the requirements of the technical standards for terminal equipment security based on the Telecommunications Business Act (Article 34-10 of the Rules for Terminal Facilities), the device check assessment under these conformance requirements can be substituted by the test results that was done when the product was certified for the technical conformity.

In this case, the test results at the time of receiving the "Technical Standards Conformity Certification Number, etc., under the Telecommunications Business Act (i.e. Design Certification Number for [T] Mark or Technical Standards Conformity Certification Number for [A] Mark)" shall be retained as rationale based on the evidence.

2.1.2. Assessment method in device check

The assessment method in the device check may be to check the authentication value and update information through the UI or other methods and confirm that it has not changed from the previous state.

2.2 Conformance Decision in Exceptional Cases

Not applicable

[STAR-1 Conformance Requirement S1.1-15]

Conformance Requirement

All of the following criteria (1) and (2) shall be met for the function of deleting data stored in the storage of the IoT product while using the IoT product:

(1) At least the following data about the user can be deleted by the user via the IoT device itself or associated services (e.g., mobile applications.)

A) Information assets (including personal information) acquired while using the IoT products

(B) User set value

(C) Authentication values set by the user, cryptographic keys and digital signatures obtained while using the IoT products

(2) The version of the firmware (software) package related to the updated security functions shall be maintained after the data is deleted.

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

None

Assessment Method

- Document assessment: subject
  It shall be assessed that the technical documentation of IoT product clearly describes the ability for users to erase their information via the IoT device itself and associated services (e.g., mobile applications).
- Device check: subject
  It shall be assessed by device check that the firmware (software) version is maintained after the operation of the data deletion function according to the procedure presented to the user and the data deletion.

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment results of both the following document assessment and device check are judged as "Conforming (Y)."

[Document Assessment]

It shall be assessed that the technical documentation of an IoT product clearly decribles that the product has a function that allows user to delete at least their information via the IoT device itself or an associated service (e.g. mobile application). Only when it is confirmed that all of the following assessment items 1 to 2 are satisfied, the assessment result of the document assessment of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

The technical documentation shall clearly describe the method to delete at least all information (data) in the following A) through C) about the user stored in the storage of the IoT product while using the IoT product. However, even information about the user, configuration information of the IoT product that is not disclosed to the user (information necessary for product characteristics) and technical data generated by the vendor to monitor the performance and system soundness of the IoT product are excluded from the information that the user can delete (e.g., Self Monitoring, Analysis and Reporting Technology (S.M.A.R.T.), number of battery charge cycles, error history).

A) How to erase information assets (including personal information) acquired while users are using IoT products

B) How to erase user configuration values related to the user

C) How to delete authentication values set by the user, cryptographic keys and signatures obtained while using IoT products

Assessment Item 2:

Procedures for using the deletion function described in Assessment Item 1 shall be provided to users through a manual or other user-accessible medium.

[Device check]

It shall be assessed that the data corresponding to the assessment items 1 A) through C) can actually be deleted according to the procedure presented to the user and that the firmware (software) version is maintained after the data deletion. Only when it is confirmed that both of the following assessment items 3 and 4 are satisfied ("passed"), the assessment result of the device check of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 3:

According to the procedure presented to the user, delete the data corresponding to items A) through C) of assessment item 1, and confirm that the data has actually been deleted. If it is confirmed that the data has been deleted, this assessment item is "Passed"; if not, this assessment item is "Failed."

The device check may be a sample test to confirm that some of the data is actually deleted, without deleting all the target data for each the assessment items 1 A) through C).

Assessment Item 4:

It shall be confirmed that the version of the firmware (software) package related to the security function is maintained after performing Assessment Item 3 (after data deletion). If it is confirmed that the updated firmware (software) version is maintained by the version display function, etc., this assessment item is "Passed;" if not, this assessment item is "Failed."

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

2.1.1. Concept of deletion (data erasure) level

STAR-1 requires deletion at a security level ("Clear" level in NIST SP800-88 Rev. 1) that can protect against simple non-invasive data recovery techniques (such as salvage by commercial data recovery software).

NIST SP800-88 Rev1 in Japanese translation
https://www.ipa.go.jp/security/crypto/gmcbt80000005u4j-att/SP800-88rev1.pdf

An example of how to confirm that data has been deleted according to the medium in which it is stored is shown below.

Example 1: General-purpose storage device (HDD):

It shall be verified that it has been rewritten with another meaningless value (at a level where deletion can be performed via standard read/write commands to the storage device), or erased using the HDD's Secure Erase function.

Example 2: General-purpose storage device (SSD):

It shall be verified that data has been erased using the Enhanced Secure Erase function of the SSD.

Example 3: When the overwrite function is not supported on storage devices other than dedicated storage devices (HDD, SSD, etc.):

If the device only provides the ability to reset to factory default or to delete file pointers, it shall be ensured that the storage area is inaccessible by the standard interface of the IoT device.

Example 4: If the associated service is an application that runs on a general-purpose device (e.g., PC, smartphone):

It shall be ensured that the same level deletion is performed by the functionality of the general-purpose device (i.e., the file is automatically deleted during the application's deletion process. The user is presented the information on the file to be deleted, and the user deletes the file using the functions of the general-purpose equipment, etc.).

Example 5: Erase by cryptographic erasure techniques

If the data is stored on a medium (area) where encryption erasure is enabled as an optional function of a cloud service or a function of a general-purpose OS of a PC, etc., make sure that the encryption key used for encryption is erased.

2.2 Conformance Decision in Exceptional Cases

2.2.1. Alternative measures to be taken when users are unable to delete content themselves

In principle, this conformance requirement requires that data about users stored in the storage of IoT products can be deleted by the users themselves.

However, in the case of IoT devices that users cannot delete data by themselves and must request a specialist or IoT product vendor to delete the data, this conformance requirement is deemed to be "Conforming (Y)" if the user is clearly informed in a manual or other document that is easy to obtain and check that "in order to delete data related to the user, it is necessary to request a specialist or IoT product vendor to delete the data."

For example, if the information is stored in a cloud service (associated service) and the user cannot delete it directly, the conformance requirement can be judged as "Conforming(Y)" on the condition that the user is informed that "the IoT product vendor will accept the user's request to delete the information and delete the data from the cloud service."

[STAR-1 Conformance Requirement S1.1-16]

Conformance Requirement

Manufacturer shall take actions to provide information on cyber security of IoT products that meet all of the following criteria (1) through (5) below:

(1) Manufacture shall inform users about safe procedures for setting up and using IoT products that have implications for cybersecurity for the use of IoT products, including how to configure the initial setting.

(2) There shall be a mechanism to inform the content of the update, the necessity of the update, and the consequences of not updating the product when security updates for IoT products are released.

(3) Manufacturer shall inform disclaimers for accidents and failures that can be expected when updates are not made, and for accidents and failures that can be expected in general.

(4) Manufacturer shall inform the policy on the expiration or termination of support for the product or service.

(5) Manufacturer shall inform the possible risks of disposing of or selling used IoT products with information assets to be protected remaining in the IoT products, and how to safely terminate the use of IoT products, including data erasure.

Conditions for being Not Applicable (NA) and Supplementary Explanation of Requirement

[Conditions for being Not Applicable (NA)]

None

[Definition of terms: information assets to be protected]

All of the following information:

- Configuration information on communication functions
- Configuration information on security functions
- Generally sensitive information, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device

Assessment Method

- Document assessment: subject
  It shall be assessed the provision of information on cyber security of IoT products in the manuals, websites, and other user-accessible media of IoT products.
- Device check: None

STAR-1 Assessment Guide

1. Conformance Assessment Criteria

For this conformance requirement, the final decision of "Conforming (Y)" will be made only when the assessment result of the following document assessment is judged as "Conforming (Y)."

[Document Assessment]

It shall be assessed that information on cyber security of IoT products is provided in the manuals, websites, and other user-accessible media of the IoT products. Only when it is confirmed that all of the following assessment items1 to 5 are satisfied ("Passed"), the assessment result of the document assessment of this conformance requirement is judged as "Conforming (Y)."

Assessment Item 1:

It shall be confirmed that users can obtain information about how to safely use IoT products, including how to configure initial settings and how to change passwords that have implications for cyber security.

As evidence of the availability of such information, the method of obtaining such information shall be described in the checklist. If the checklist describes how to obtain such information, this assessment item is treated as "Passed."

Assessment Item 2:

It shall be confirmed that a mechanism and implementation method to inform users of the contents and necessity of security updates for IoT products and the consequences of not updating the products are in place in technical documents. Specifically, this assessment item is treated as "Passed" when mechanisms and implementation methods are clearly described, including the media used to inform users of the necessary information at the time of security update release, the method used to inform users, and the department in charge.

Assessment Item 3:

It shall be confirmed that disclaimers for accidents and failures assumed or generally expected when the device is not updated are clearly stated in a place easily accessible and checked by the user. As the basis for the explicit statement, the location where the disclaimer is clearly stated shall be described in the checklist. If the location is indicated in the checklist, this assessment item is treated as "Passed."

Assessment Item 4:

In STAR-1, the provision of support during the validity period of the conformance label is mandatory, and the support period is announced on the website of the products for which the conformance label has been obtained. Therefore, this assessment item is treated as "Passed" as long as there are no falsehoods in the support period described in the application form for the STAR-1 conformance label and the applicant agrees to the obligation to provide support during the validity period of the conformance label. If there is any false information in the application related to this assessment item, the entire checklist will be marked as "Failed" regardless of the results of the self-conformance assessment, and measures including rejection or cancellation of the application for the conformance label will be taken.

Assessment Item 5:

It shall be confirmed that the risks associated with disposing of or selling used products with information assets to be protected remaining in the IoT product and the safe termination methods including data erasure, are explained in the information easily accessible and verifiable by the user. As a basis for being explicitly stated, the location of such information shall be described in the checklist. This assessment item is treated as "Passed" when the location is described in the checklist.

2. Supplementary Explanation

2.1 Supplementary Explanation of Conformance Assessment Criteria

Not applicable

2.2 Conformance Decision in Exceptional Cases

Not applicable

Appendix A Glossary

Term	Description
Customer Engineer	Refers to maintenance personnel on the vendor side.
Configuration information on communication functions	The followings are examples of configuration information related to communication functions that are information assets to be protected. Example 1: Wi-Fi SSID Example 2: WPA encryption key (Wi-Fi password), etc.
Configuration information on security functions	The following is an example of configuration information related to security functions that are information assets to be protected. Example 1: TLS communication configuration information Example 2: Firewall setting information, etc.
Generally sensitive information	What is the assessment target that is described as "generally sensitive information, such as personal information, collected, stored, or communicated by IoT devices in the intended use of IoT devices" is determined by the IoT product vendor by considering the intended use and environment where IoT device is used. For example, information related to laws and regulations, such as webcam images, generally falls under the category of sensitive information.
Storage for IoT Products	Examples of storage for IoT products are as follows. Storage built into IoT devices and storage included in associated services are the targets. Example 1: Flash ROM Example 2: HDD Example 3: SSD Example 4: Removable storage, etc.

Appendix B. Revision History

2024.12.13 1st version published

2025.05.05 Version 1.1 published

- S1.1-11: In Assessment Item 1, it was clarified that storing using message digests is also acceptable as a secure storage method.
- S1.1-11: In Assessment Item 3, it was clarified that cryptographic techniques other than hash functions is also acceptable as a message digest method.
- S1.1-12: In 2.2.1, “satisfy Assessment Item 2” has been corrected to “satisfy Assessment Item 3.”