IoT Product Security Conformity Assessment Scheme Policy (Provisional Translation)

August 2024

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

Table of Contents

1. Introduction

The number of IoT products connected to the Internet is increasing rapidly; according to the Ministry of Internal Affairs and Communications' 2023 White Paper on Information and Communications in Japan[1] , the number of IoT products worldwide is expected to continue to grow, reaching 39.9 billion by 2024 and 44 billion by 2025. As the number of IoT products increases, so does the number of cyber threats that target their vulnerabilities, which is why countries including Japan are making efforts to ensure security of IoT products. Major efforts in other countries include the following:

- In the U.S., a Final Rule[2] was published in July 2024 for the U.S. Cyber Trust Mark[3] , a voluntary cybersecurity labeling scheme for wireless consumer IoT products. The scheme is expected to launch during 2024 and individual security requirements are expected to be defined for certain devices such as consumer grade routers and smart meters.
- In the EU, the Cyber Resilience Act, which introduces mandatory requirements for products with digital elements placed on the EU market with some exceptions, was first proposed in September 2022. The Act includes cybersecurity requirements for design, development and production before placing products on the EU market, as well as requirements to report actively exploited vulnerabilities and incidents after the product has been placed on the market, among others. It is set to enter into force in the second half of 2024 and will become mandatory by 2027 with the exception of reporting requirements.[4]
- In the UK, the PSTI Act[5] , which requires manufacturers etc. of consumer connectable products to provide a statement of compliance that they and their products meet relevant minimum security requirements, was passed in December 2022. Following the signing into law of a regulation[6] in September 2023, the regime is in effect since April 2024.
- Singapore launched a voluntary Cybersecurity Labelling Scheme for consumer IoT devices in October 2020, which mutually recognizes with similar schemes in Germany and Finland.

Japan has also promoted efforts to ensure the security of IoT products. As representative efforts, the Ministry of Economy, Trade and Industry (METI), its incorporated administrative agency Information-technology Promotion Agency (IPA), and the Ministry of Internal Affairs and Communications (MIC) have issued several guidelines to support security measures by business operators that manufacture IoT products. In April 2020, the Ministry of Internal Affairs and Communications partially revised the Ordinance Concerning Terminal Facilities Etc., making it mandatory in principle to implement access control functions, functions that encourage the user to

---

[1] Ministry of Internal Affairs and Communications, White Paper on Information and Communications in Japan 2023
https://www.soumu.go.jp/johotsusintokei/whitepaper/r05.html

[2] Federal Register, Cybersecurity Labeling for the Internet of Things
https://www.federalregister.gov/documents/2024/07/30/2024-14148/cybersecurity-labeling-for-internet-of-things

[3] The White House, Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers
https://www.whitehouse.gov/briefing-room/statementsreleases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smartdevices-to-protect-american-consumers/

[4] European Council, Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[5] legislation.gov.uk, Product Security and Telecommunications Infrastructure Act 2022
https://www.legislation.gov.uk/ukpga/2022/46/contents/ enacted

[6] legislation.gov.uk, The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023
https://www.legislation.gov.uk/uksi/2023/1007/contents/made

set appropriate usernames and passwords for access control, and software (firmware) update functions for IoT products that directly connect to telecommunication carriers' networks. The Ordinance Concerning Terminal Facilities Etc. stipulates security standards for terminal facilities to conform to technical standards under the Telecommunications Business Act and is expected to prevent malware infection of IoT products to ensure a network environment that can be used safely and stably by everyone. Other measures request business operators that manufacture or sell IoT products ("IoT product vendors") to voluntarily take security measures to ensure the security of their IoT products.

However, it is currently difficult for IoT product vendors to demonstrate their security measures to procurers and end-users. From the perspective of procurers and end-users, it is difficult to judge whether appropriate security measures are in place for a product. In addition, efforts by government agencies and enterprises to manage supply chain risks are increasing on broader terms, including the security of the products they procure as well as the security of the product vendors. However, few organizations have implemented a process to check the security functions and countermeasures of products at the time of product selection and procurement, which should be performed by the organization.

To solve these issues, there are certification schemes to evaluate and visualize the security functions of products using a common standard. Examples include the Common Criteria (CC) based Japan Information Technology Security Evaluation and Certification Scheme (JISEC)[7] and the Component Security Assurance (CSA) certification scheme based on IEC 62443-4-2 for industrial products. However, these certification schemes require relatively high levels of security, causing significant monetary and time costs to obtain the certifications. As a result, many IoT product vendors find it difficult to use these certification schemes. Although there are existing certification schemes by private organizations for certain IoT product categories, for government agencies to use a certification scheme as a product security evaluation for procurement, it is desirable to use a scheme that covers a wide range of procurable IoT products and is widely accepted in Japan.

Therefore, the government will take initiative in establishing a scheme that evaluates the security measures of IoT products and its conformance to a certain level of security requirements, then visualizes the results in a way that both procurers and end-users can understand by means of certification and labeling, while also reducing monetary and time costs, targeting a large number of IoT products, and taking into account similar efforts in other countries. This will enable IoT product vendors to demonstrate that their IoT products have appropriate security measures in place, making it easier for procurers and end-users to select secure products.

IoT products are indispensable devices that connect people and things, adding value to society through the advanced integration of cyberspace and physical space. On the other hand, the security environment throughout the world is becoming increasingly uncertain, and cyber threats targeting vulnerabilities in IoT products are expected to become increasingly serious. Therefore, it is essential that IoT products not only interconnect cyber space and physical space, but also take appropriate security measures, a demand seen both domestically and internationally. Against this background, the IoT Product Security Conformity Assessment Scheme is a scheme that will meet not only domestic but also international needs by clearly indicating IoT products that have taken appropriate security measures through conformity assessment and labeling. Introducing large numbers of IoT products into the market that conform to this scheme can be considered an important international contribution.

[7] IPA, IT Security Evaluation and Certification Scheme (JISEC) https://www.ipa.go.jp/security/jisec/index.html

To this end, METI held the "Study Group for Establishment of a IoT Product Security Conformity Assessment Scheme[8] (hereinafter referred to as the "Study Group")" since November 2022 to discuss current issues, as well as the objective and contents of the conformity assessment scheme to be established. Based on discussions in the Study Group in FY 2022, METI held the "Preliminary Study Committee for Establishment of Criteria for a IoT Product Security Conformity Assessment Scheme" (hereinafter referred to as the "Preliminary Committee") since August 2023 to discuss and formulate draft security requirements, draft conformance criteria, and draft evaluation procedures to be required in the scheme, and conducted a proof of concept on actual products (hereinafter referred to as "POC") based on these drafts. Based on the results of the discussions in the Study Group and the Preliminary Committee, the "Final Summary of the Study Group for Establishment of a IoT Product Security Conformity Assessment Scheme" was published in March 2024.

This document describes the policy for the IoT Product Security Conformity Assessment Scheme (hereinafter referred to as the "Scheme") to be established based on the contents of the "Final Summary of the Study Group for Establishment for a IoT Product Security Conformity Assessment Scheme".

[8] Ministry of Economy, Trade and Industry, Working Group 3 (Study Group for Establishment of a IoT Product Security Conformity Assessment Scheme)

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/ iot_security/index.html

2. Purpose and positioning of the security conformity assessment scheme to be established

2.1. Necessity and Purpose of the Scheme

To ensure the security of IoT products, it is necessary to establish a Japanese conformity assessment scheme for IoT products and widely disseminate it throughout society. To this end, it is essential that procurers and end-users preferentially select products with the label for a required security level. Once this demand is generated, IoT product vendors will then actively acquire labels, as IoT products without labels will be less likely to be selected in the market. In addition, IoT product vendors may outsource evaluation to third-party independent test laboratories and testing service providers to increase the reliability and objectivity of the evaluation, while lowering the burden of conducting a security evaluation on their own.

To create such a cycle, the Scheme will aim to

(1) incorporate the label into IoT product procurement requirements for organizations that are expected to have a high societal security risk as well as solid scheme use, such as government agencies, critical infrastructure providers, and local governments, and

(2) ensure certain sectors have sector-specific standards in place such that IoT product vendors will be able to manufacture/sell, and procurers will be able to select/procure labeled products based on the sector-specific standards. As the Scheme steadily spreads through these means, we will work to promote its use in procurement requirements of large private-sector companies, as well as its dissemination to small and medium-sized enterprises and consumers.

In addition, considering the widespread use of imported IoT products and the international expansion of domestic IoT product vendors, the Scheme should not be closed to the domestic market, but should rather

(3) coordinate with other countries' schemes and aim for mutual recognition.

Based on the above, the following three objectives will be set as the initial main goals of the Scheme, to which the Scheme will be built in line with:

1. The Scheme will facilitate the selection and procurement of IoT products that meet the security levels required by organizations by making it possible to evaluate and visualize IoT product security using a common standard.
2. The Scheme will define security requirements for IoT products to be procured/used in specific sectors, and allow each industry organization, etc. to specify necessary certifications and labels, so that only IoT products with the security level required in those specific sectors will be chosen in that sector.
3. The Scheme will reduce IoT product vendors' cost of conformity assessment required when exporting IoT products overseas by coordinating with other countries' schemes, and aim for mutual recognition.

In the future, it is desirable that this Scheme contribute to ensuring the security of IoT products in society as a whole, including the following:

- Procurers and end-users will recognize the value of security measures in IoT products, and IoT product vendors will be able to appropriately reflect the cost of such measures in the product price.
- Procurers and end-users, including consumers, will be able to choose IoT products with appropriate measures in place, without relying on their own skills and knowledge of security.
- Procurers and end-users will be considered to have fulfilled certain responsibilities as a procurer or end-user by procuring and using labeled products.

- Procurers and end-users will understand that they must not only purchase IoT products with security measures in place, but also take security measures and perform management on their own after purchase, such as setting appropriate passwords and implementing security updates.

2.2. Positioning the Scheme

This Scheme will initially be operated as a voluntary scheme. The intent of this Scheme is to improve products' added value by granting labels to products that have undergone conformity assessment to security requirements. For products procured by organizations such as government agencies, it is recommended that labeled products that meet the security level required by each organization be selected and procured. By making this mandatory in the future, IoT product vendors will be given incentives to acquire labels.

This Scheme should be developed after a comparative study of its relationship with existing related schemes, both within Japan and in other countries. The Scheme should also be developed with the Ordinance Concerning Terminal Facilities Etc. in mind, to avoid conflict with existing domestic laws and regulations. In addition, a policy for future integration, separation, or coordination with related existing domestic voluntary schemes should be agreed upon, and consideration should be given to IoT product vendors to avoid confusion or redundancy caused by the disorderly proliferation of schemes.

2.3. Initial Target of the Scheme

Based on the main purpose of this Scheme, the main initial target for procurement of IoT products to which the label of this Scheme is granted (hereinafter referred to as "labeled products") is defined according to the conformity assessment levels shown in Section 3.3. First, we will encourage government agencies, critical infrastructure providers, and local governments to incorporate the selection of labeled products that meet the necessary security requirements into their procurement requirements, which will encourage IoT product vendors to obtain labels. Second, if IoT products are used in a specific sector and there is a request from industry to establish security requirements for such IoT products as a sector-specific standard so that procurers and end-users can confirm IoT products meet this security requirement via a label, the Secretariat of the Scheme (defined in Section 3.1) will work with relevant industry associations and working groups (WGs). Priority should be given to critical infrastructure sectors, as well as systems that are widely used and deployed in society. For details on incorporation into various procurement requirements, see Section 3.8.1. For details on collaboration with industry associations and WGs on use of the Scheme in specific sectors, see Section 3.8.2.

3. The Security Conformity Assessment Scheme to be Established

3.1. Operational Structure of the Scheme

In light of the difficulties in promoting a new, unknown voluntary scheme, as well as the possibility of causing confusion for procurers and end-users due to proliferation of schemes, the Scheme will utilize an existing evaluation scheme. It is important that the Scheme Owner, who is responsible for this Scheme and will maintain its basic rules, is overseen by effective government governance, as the Scheme will be used as an alternative to product security evaluations conducted by government agencies for procurement and will need to coordinate mutual recognition with other countries' schemes. In light of the above, the Scheme Owner will be IPA, an incorporated administrative agency under the jurisdiction of METI, who will establish the Scheme in accordance with this Policy and will operate the Scheme under METI's supervision. IPA will establish and operate the Scheme by expanding the JISEC Scheme it currently operates from its CC certification only nature to include this Scheme.

The proposed operational structure is shown in Figure 3.1-1. The Steering Committee and the Technical Advisory Committee for the Scheme will be established under the president of IPA. The Steering Committee will be established as an extension of the existing JISEC Steering Committee and will deliberate on matters related to the operational policies and management of the CC certification and this Scheme. The Technical Advisory Committee for this Scheme will be newly established as a successor to the Preliminary Committee and will discuss the approval of conformance criteria and other technical matters of this Scheme. In addition, the Conformance Criteria WGs will be established under the Technical Advisory Committee to formulate the draft conformance criteria for each product category. The Conformance Criteria WGs for STAR-2 and above will be composed mainly of IoT product vendors, major procurement organizations, and their related organizations and groups, and will submit the draft conformance criteria to the Technical Advisory Committee for approval. In addition, IPA and METI will establish a Secretariat for the Scheme to expand the Scheme, integrate and coordinate with existing domestic schemes, coordinate with other countries on cooperation such as mutual recognition, promote its use in government procurement requirements, promote its use to private companies and consumers, and promote certification by IoT product vendors.

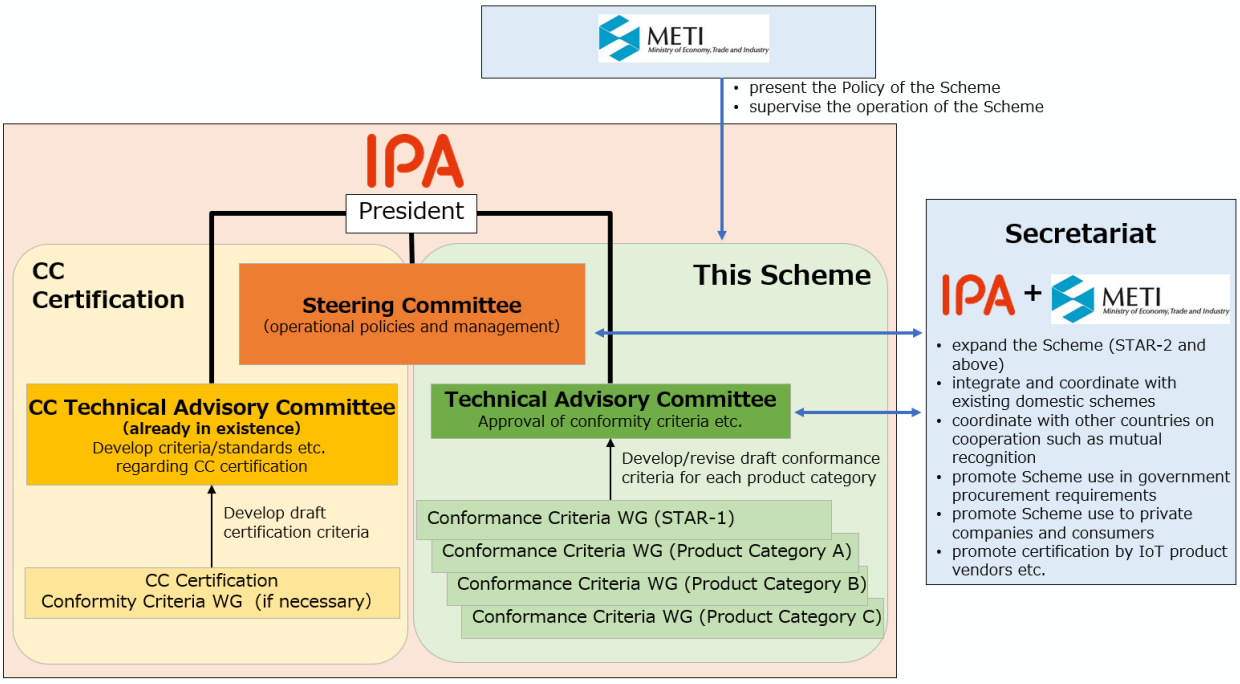


Figure 3.1-1 Proposed Operational Structure of the Scheme

3.2. Scope of Products Covered by the Scheme

According to ETSI EN 303 645 for Consumer Internet of Things, an "IoT product" is defined as a "consumer IoT device and its associated services". A "consumer IoT device" is defined as a "network-connected (and network-connectable) device that has relationships to associated services and are used by the consumer typically in the home or as electronic wearables" and "associated services" are defined as "digital services that, together with the device, are part of the overall consumer IoT product and that are typically required to provide the product's intended functionality".

Referring to definitions in both domestic standards and schemes and those of other countries, the scope of products covered by the Scheme will include the following devices that have the ability to send and receive data using Internet Protocol (IP). An image is shown in Figure 3.2-1.

- Devices that can be connected to the Internet: Devices with the ability to send and receive data over the Internet using IP
- Devices that can be connected to a network: Devices that are connected to "Devices that can be connected to the Internet" or other "Devices that can be connected to a network" and have the ability to send and receive data using IP

The above IoT devices and their associated services, or IoT products, will be covered in the scope of this Scheme.

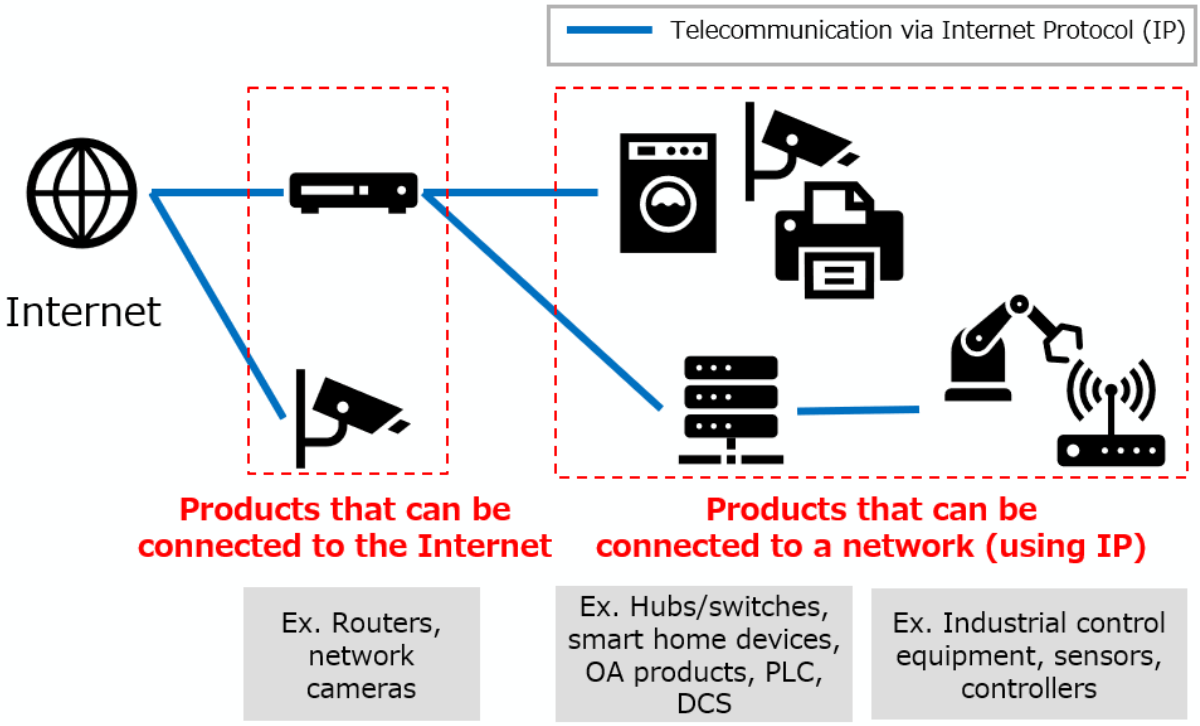


Figure 3.2-1 Image of products covered by the Scheme

As with certain existing domestic and other countries' schemes, general-purpose IT products (PCs, tablets, smartphones, etc.) to which users can easily alter security measures such as via software products are excluded. IoT products with a general-purpose OS will be considered to be in scope if users cannot easily add security measures to the product itself.

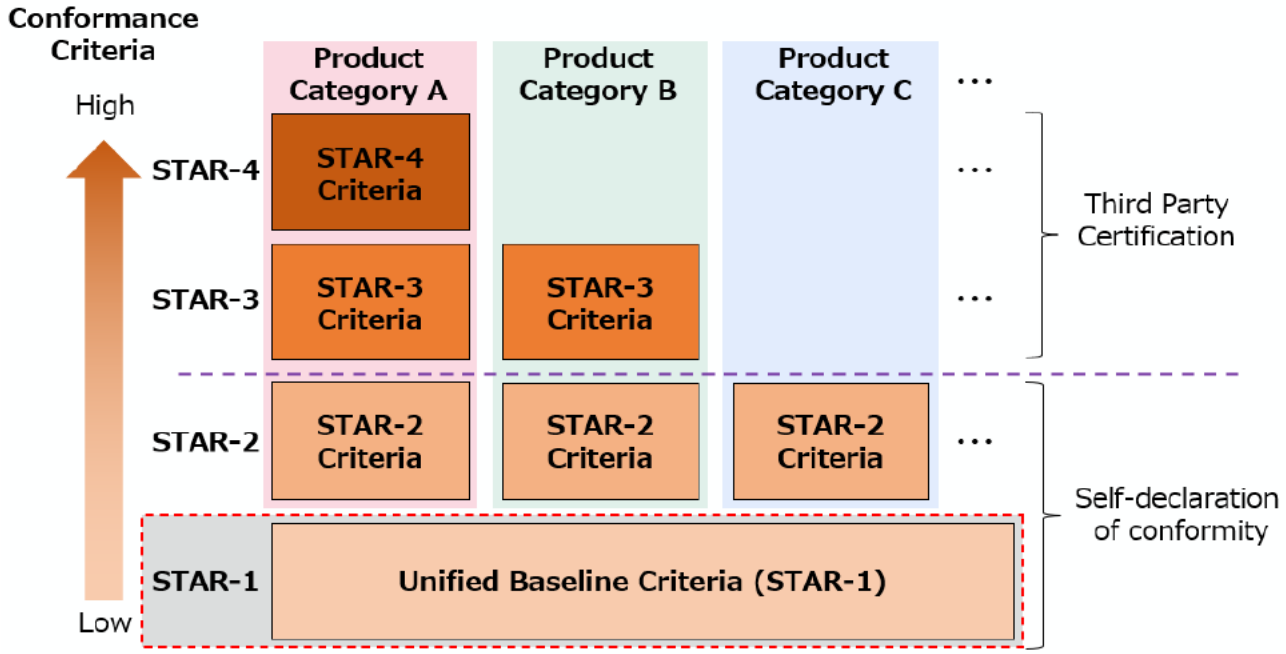
3.3. Conformity Assessment Levels in the Scheme

The Scheme will establish security requirements, conformance criteria, evaluation procedures and evaluation methods according to the characteristics of each product category. Table 3.3-1 shows the positioning of each conformity assessment level. For STAR-1, security requirements, conformance criteria, and evaluation procedures common to all product categories are organized based on the assumption that minimum threats common to all IoT products in scope are to be addressed. For STAR-2 and above, security requirements, conformance criteria, and evaluation procedures are organized per product category. As indicated in Section 3.5, self-declaration of conformity by IoT product vendors is allowed for STAR-1 and STAR-2, while third-party certification is required for STAR-3 and above. Figure 3.3-1 shows an image of conformity assessment levels.

Table 3.3-1 Positioning of each conformity assessment level

Level	Positioning
STAR-3 and above	General conformance criteria for each IoT product category that is intended for use in critical systems of government agencies, critical infrastructure providers, and large companies, and is evaluated and certified by an independent third party.
STAR-2	IoT product vendors self-declare that their product conforms to the basic conformance criteria for each IoT product category in addition to STAR-1.
STAR-1	IoT product vendors self-declare that their product conforms to the unified baseline conformance criteria for all IoT products in scope.

Figure 3.3-1 Image of Conformity Assessment Levels



3.4 Security Requirements, Conformance Criteria, and Evaluation Procedures in the Scheme

The relationship between the "security requirements" to be required for IoT products covered by this Scheme, the "conformance criteria" that indicate the criteria to which IoT products must conform at each conformance assessment level, and the "evaluation procedures" that indicate the procedures to evaluate whether the product conforms to the conformance criteria, is shown in Figure 3.4-1.

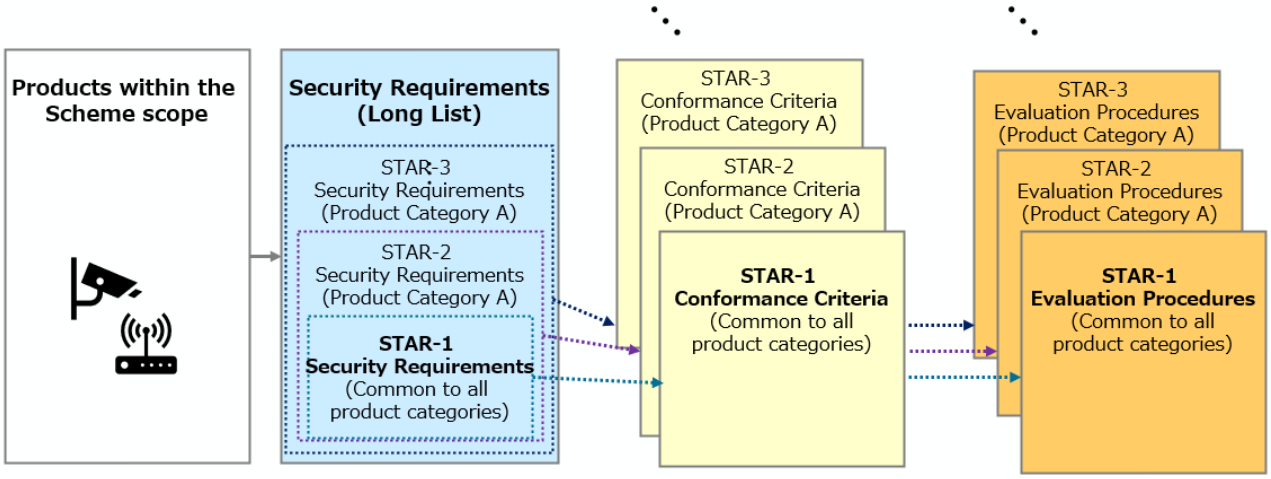


Figure 3.4-1 Relationship between security requirements, conformance criteria, and evaluation procedures

In the FY2023 Study Group and Preliminary Committee, discussions focused on the security requirements for the Scheme as a whole, as well as the security requirements, conformance criteria, and evaluation procedures for the baseline STAR-1. After discussions in the Preliminary Committee, a POC was conducted on the draft STAR-1 security requirements, conformance criteria, and evaluation procedures, which was then revised based on improvements and modifications found as a result of the POC.

For security requirements for the Scheme as a whole, as shown in Figure 3.4-2, a "Long List" of security requirements for all conformity assessment levels was first created, by extracting overlapping requirements in both domestic standards and schemes and those of other countries, including ETSI EN 303 645, NISTIR 8425, and the EU CRA. The security requirements for each conformity assessment level were then extracted from this "Long List".

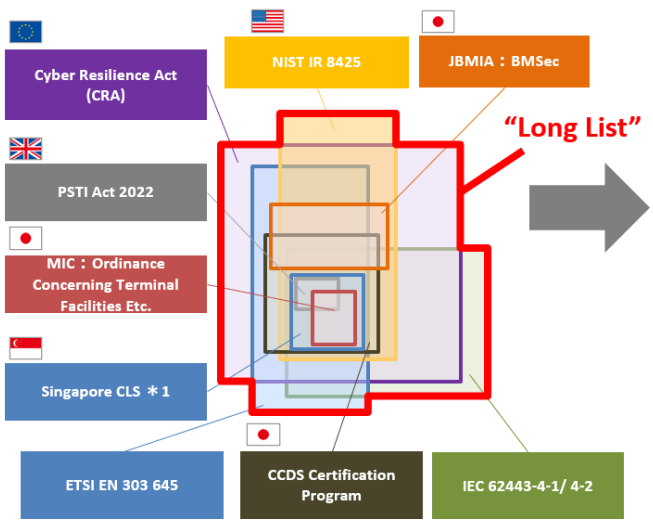


Image of "Long list"	
1. No universal default passwords	1-1. For devices that use passwords, passwords that match a defined quality scale are set, or can be set by the user.
	1-2. …
	1-3. …
	1-4. …
	1-5. …
2. Implement a means to manage reports of vulnerabilities	2-1. Require manufacturers to publish a vulnerability disclosure policy that describes the means by which reports and inquiries about the security of their products are received in [defined manner and format].
	2-2. …
	2-3. …
・・・	・・・

Figure 3.4-2 Creating the Long List of security requirements

To extract the security requirements for STAR-1 out of the "Long List" of security requirements, we first organized the assumed threats to be considered for STAR-1 based on the positioning of STAR-1 in this Scheme, the main assets to be protected for STAR-1, and the attack surfaces of products in STAR-1 scope. Then, the security requirements for STAR-1 were established by organizing the countermeasures to be implemented against the assumed threats and extracting the security requirements to implement such countermeasures from the "Long List".

The following threats were organized as the main threats to be considered in STAR-1:

- Threat of information leaks, tampering, and functional abnormalities due to (1) weak authentication functions, (2) neglect of vulnerabilities, and (3) activation of unused interfaces, which would make the product subject to unauthorized external access, malware infection, stepping stone attacks, etc.
- Threat of equipment communications being intercepted and leakage of information assets to be protected
- Threat of leakage of information assets to be protected from equipment that have been disposed of or resold
- Threat of abnormal security functions in the event of network disconnections, power outages, etc.

The information assets to be protected for STAR-1 were organized as follows:

- Configuration information related to communication functions
- Configuration information related to security functions

- Information[9] that is generally sensitive, such as personal information, that is collected, stored, or communicated by the device in the intended use [10] of the device.

To determine the conformance criteria for STAR-1, a draft of the conformance criteria was organized based on ETSI EN 303 645, a standard widely used in other countries, while also referring to the criteria of existing schemes such as Singapore's CLS and the Japanese CCDS Certification Program.

For the evaluation procedure of STAR-1, an "evaluation method" was developed by referring to the evaluation procedures of existing domestic and overseas schemes such as Singapore CLS and the CCDS Certification Program. The "evaluation method" is either "document" or "device check"; however, to allow for self-declaration of conformity by IoT product vendors at the lowest possible cost, the "evaluation method" in STAR-1 focuses on "document," which is assumed to require less man-hours for evaluation.

The draft STAR-1 conformance criteria and evaluation procedures were discussed in the Study Group and Preliminary Committee in parallel with a POC of the draft to calculate cost for evaluation. In the POC, 10 products were evaluated based on the draft, through both self-evaluation by IoT product vendors and third-party evaluations by independent test laboratories (See Section 3.5 for definition of independent test laboratories). The man-hours required for evaluation averaged 23.9 man-hours, and there was no significant difference between man-hours for self-evaluation and third-party evaluation. The conformance criteria that required a particularly large number of man-hours were those related to port scanning and vulnerability scanning on devices, but this was attributed to the fact that a large number of man-hours were required to initially construct the tool environment, and it was confirmed that the expected man-hours for second and subsequent evaluations were shorter in time.

In the POC, there were differences in evaluation results between self-evaluation and third-party evaluation for several criteria in several products. The two main reasons for the differences were that the conformance criteria and evaluation procedures were ambiguous, and that the third party could not receive documents for document evaluation from the vendor. To address the former, the conformance criteria and evaluation procedures were clarified to ensure uniqueness of the results. To address the latter, the handling of documents for document evaluation was organized.

The security requirements and conformance criteria for STAR-1 are shown in the Annex. Evaluation procedures and evaluation guides for the conformance criteria of STAR-1 were also developed based on the results of the Study Group and Preliminary Committee. The security requirements, conformance criteria, evaluation procedures for STAR-1 established by the Preliminary Committee this year will be discussed and finalized in the Technical Advisory Committee during FY2024. Security requirements, conformance criteria, evaluation procedures for STAR-2 and above will be discussed in the Technical Advisory Committee and the Conformance Criteria WG starting FY2024.

In order to reduce difficulties for STAR-1 evaluation as much as possible, support documents (FAQs) will be prepared and provided including those related to the initial construction of the tool environment required for device checks. In addition, security requirements, conformance criteria, and evaluation procedures will be periodically

[9] For example, in the case of equipment that has no intended use with respect to personal information, but whose data handled by the equipment may contain personal information, the subject data is treated as information assets to be protected only when there is an unacceptable risk with respect to the threat of eavesdropping in the assumed operating environment. A specific example would be the personally identifiable images (personal information) collected by security cameras, etc. However, personal information transmitted to routers does not fall under "collected by the equipment in the intended use of the equipment," and is therefore not subject to this requirement.

[10] Use in accordance with information provided with a product or system, or, in the absence of such information, by generally understood patterns of usage. (JIS Z 8051:2015)

reviewed after the start of this Scheme, as required security measures change daily according to technological progress and threat conditions. As later indicated in Section 3.5, self-declaration of conformity by the IoT product vendor is allowed for STAR-1, and application for the label is a checklist based on the results of a self-evaluation by the IoT product vendor. If a IoT product vendor conducts self-evaluation and applies for the label, it is not required to provide the documents referenced for evaluation at the label application stage. If a IoT product vendor finds it difficult to self-evaluate, it is possible to request a third-party such as an independent test laboratory to evaluate the IoT product, then apply for the label based on the third-party's evaluation results. However, in this case, it is necessary to provide reference documents for evaluation to the third-party. In addition, as indicated in Section 3.7, if there is any doubt about the contents of an application after a label is granted, IPA may request the submission of evidence used in evaluation to address the doubt.

3.5 Entities that Perform Conformity Assessment in the Scheme

To promote this system widely, self-declaration of conformity is allowed for STAR-1 and STAR-2. For STAR-1 and STAR-2, IoT product vendors themselves will conduct self-evaluation and apply for labels based on the checklist describing the evaluation results. Upon receiving the application, the IPA will check the format of the checklist and grant the label. The evaluation may be outsourced to a qualified individual, testing service provider, or independent test laboratory.

Since STAR-3 and above are intended for use by organizations and business operators who provide functions and services that require high reliability such as government agencies and critical infrastructure providers, products will be evaluated by an independent test laboratory and will be certified by IPA, which will serve as the certification body.

IPA will make inquiries to relevant government agencies, including METI, regarding supply chain risk[11] before granting the label, and will grant the label based on the inquiry result.[12]

Figure 3.5-1 and Figure 3.5-2 show the flow of conformity assessment at each conformity assessment level. The main responsibilities of each entity at each conformity assessment level are as shown in Table 3.5-1. For details on qualified individuals, see Section 3.7. For details on testing service providers and independent test laboratories, see Section 4.3.

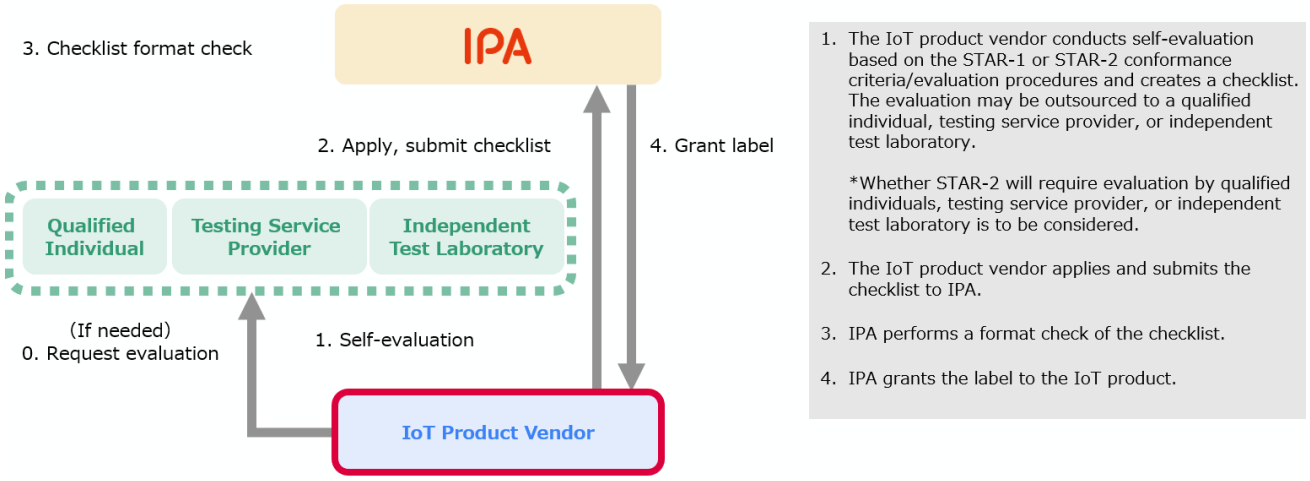


Figure 3.5-1 Flow of conformity assessment for STAR-1 and STAR-2

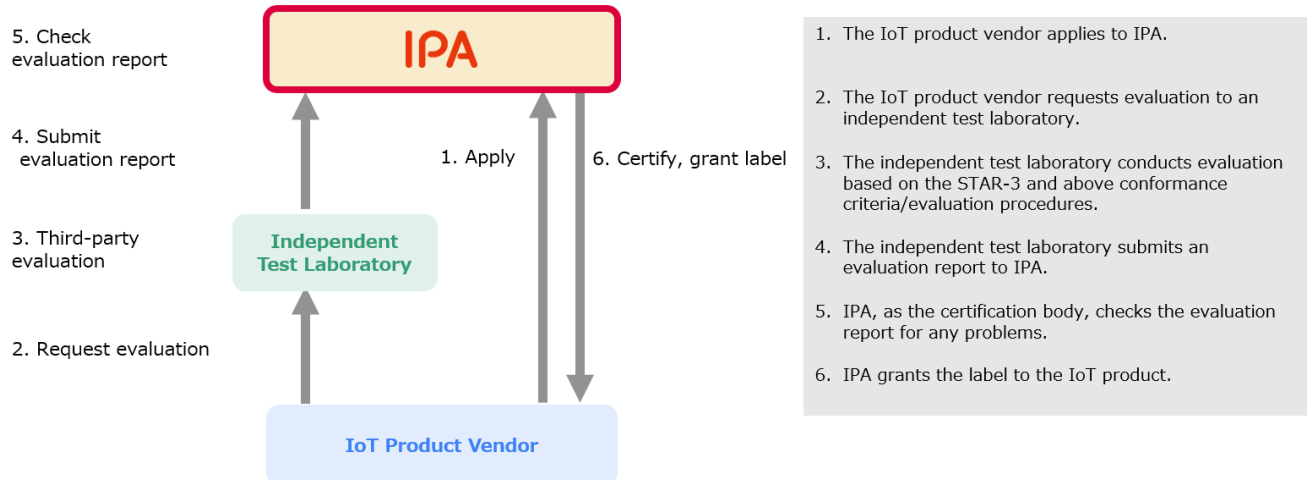


Figure 3.5-2 Flow of conformity assessment for STAR-3 and above

[11] Cybersecurity Strategy (September 2021) (in Japanese)
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf

[12] Relevant government agencies will determine presence of supply risk based on factors such as the following:
- The IoT product vendor of the IoT product being applied for is compliant with domestic laws and international standards etc., including past compliance.
- The IoT product vendor will not be affected by foreign legislation etc. in ensuring cybersecurity of the IoT product being applied for.

Table 3.5-1 Main responsibilities of each entity at each conformity assessment level

	IoT product vendors	Independent test laboratory	IPA
STAR-1, STAR-2 (Self-declaration of conformity)	• Properly conduct the evaluation, take responsibility for the contents of the checklist, and explain the contents to the procurer or end-user if requested to do so. • Use the granted label appropriately. • Properly store evidence of evaluation for the duration of the label validity period and disclose the information to the scheme owner to demonstrate that the evaluation was properly conducted. • Manage any changes in application content or product specifications, and take appropriate action as stipulated in the event of any changes for the duration of the label validity period.	- (The use of independent test laboratories and testing service providers is optional)	• Check that the checklist format is appropriate and grant the label. • Disclose information on labeled products to procurers and end-users. • Manage the labels so that they are properly used. • Take appropriate action upon recognizing an inappropriate use of a label.
STAR-3 and above (Third-party certification)	• Use the granted label appropriately. • Manage any changes in application content or product specifications, and take appropriate action as stipulated in the event of any changes for the duration of the label validity period.	• Properly conduct the evaluation.	• Properly check the content of the evaluation report, then certify and grant the label. • Disclose information on labeled products to procurers and end-users. • Manage the labels so that they are properly used. • Take appropriate action upon recognizing an inappropriate use of a label.

3.6 Implications of the Label

Based on the responsibilities of each entity at each conformity assessment level, the implications of the labels granted to IoT products at each conformity assessment level are as shown in Table 3.6-1. This label is only an indication of conformity to the established conformance criteria and does not guarantee that the IoT product is fully secured. The relationship with various laws and regulations (e.g., Consumer Contract Act) will be organized and discussed in the future.

Table 3.6-1 Implications of the label at each conformity assessment level

Conformity Assessment Level	Implication of the Label
STAR-1, STAR-2 **(Self-declaration of conformity)**	The label is a self-declaration by the IoT product vendor that the IoT product conforms to the conformance criteria defined at the time the label is acquired (including reacquisition at the time of renewal). The attestation entity is the IoT product vendor. IPA, as a label granting body, will perform a format check of the checklist describing the evaluation results, but IPA does not certify the security conformity of the IoT product.
STAR-3 and above **(Third-party certification)**	The label indicates that IPA, as the certification body, has certified that the product conforms to the conformance criteria defined at the time the label is acquired (including at the time of re-evaluation). The attestation entity is IPA. IPA will certify conformity to the conformance criteria after checking the evaluation report by an independent test laboratory, which will be aligned with the conformance criteria and evaluation procedures as stipulated in the Scheme. However, while IPA is responsible for appropriately checking the evaluation report by the independent test laboratory, IPA makes no warranty, explicit or implied, with respect to the labeled product.

3.7 Mechanisms for Ensuring Label Reliability

Due to the voluntary nature of the Scheme, there is no obligation to display the label, but IoT product vendors may voluntarily affix the label of this Scheme on the product itself, package, manual, pamphlet, website, etc. to demonstrate that the product has acquired the label.

To provide procurers and end-users with up-to-date, wide-ranging information on labeled products, a webpage providing information on each labeled product will be established on the website of this Scheme to display information such as an overview of the Scheme, product information, label information, conformity assessment results, and safety information. A QR code with the URL of the webpage will be provided along with the label of the Scheme. The proposed information to be posted on the webpage, which will be in Japanese, is shown in Table 3.7-1. The label information will include the classification of the evaluator so that the procurer and end-user can identify whether the evaluation was conducted by a person with evaluation capabilities. The following evaluator categories are proposed: IoT product vendor, IoT product vendor (qualified individual), third-party qualified individual, testing service provider, and independent test laboratory. To list that a qualified individual has conducted the evaluation, the individual must have a designated qualification (e.g., Registered Information Security Specialist) and have completed complete training on IoT security evaluation or take an oath that he/she

understands the evaluation guide. The Technical Advisory Committee will consider whether to limit the designated qualification for qualified individuals to Registered Information Security Specialists or to allow other equivalent qualifications, as well as development of necessary training programs. Refer to Section 4.3 for a description of testing service providers and independent test laboratories.

Affixing labels on products scheduled for shipment after the label expiration date (after the expiration date when there is no plan to reapply for the label) will be prohibited, but removing the label from products that have already been manufactured or are in the process of being manufactured will not be required, in consideration of the workload on IoT product vendors. Instead, the status of the product on the webpage will be listed as "label expired".

Table 3.7-1 Proposed information to be posted on the webpage

Information to be listed	Listing Details
Outline of the Scheme	• URL of the webpage explaining the outline and details of this Scheme
Product Information	• Product name • Model number • IoT product manufacturer name *Disclosure to the public is optional • Country or region of manufacture *Disclosure to the public is optional • Product overview • Product webpage URL • Contact information for product inquiries • Certification numbers for other certifications
Label Information	• Label identification number • Conformity assessment level of the product (STAR-1 to 4) • Product category of the product *for STAR-2 to 4 • Version of conformance criteria evaluated • Conformity assessment results (checklist or evaluation report) • Label status information • Date of label issue/renewal • Label expiration date • Label applicant name (IoT product vendor) • Evaluator category
Security Information	• Vulnerability information of the product • Contact information for the reporting of vulnerabilities
Other Security-related Information	• Security-related information from IoT product vendors to procurers and end-users, if necessary

The validity period of STAR-1 and STAR-2 labels will be up to two years from the date of label acquisition (the validity period may be set to less than two years if requested upon application). After two years, a new self-declaration of conformity will be needed. If there is a major revision of conformance criteria during the validity period (addition of conformance criteria or major change of conformance criteria) and the grace period (the transition period during which the old version and the new version coexist) expires, the label will not be revoked.

However, if there is a change in the product security specifications etc. that affects the evaluation within the validity period, the IoT product vendor will confirm the change and report it to the Scheme Owner, at which point the label will be revoked.

The validity period of STAR-3 and above labels will be considered after FY2024, taking into consideration response to security trends, product lifetime, cost required for evaluation, and ease of understanding for procurers and end-users.

To check for nonconformance of and ensure the reliability of labeled products after distribution, the Scheme Owner will have the right to inspect and conduct surveillance on labeled products and IoT product vendors that have obtained the label will cooperate. However, for STAR-1 at the time of Scheme launch, periodic surveillance such as sampling will not be conducted from the viewpoint of cost. When there is any doubt about a labeled product's conformity to the conformance criteria based on information from a procurer/end-user or the judgement of the Scheme Owner, the Scheme Owner will request the IoT product vendor to submit evidence used for evaluation and conduct inspection/surveillance. When submitting the evidence, a non-disclosure agreement (NDA) will be concluded between the IoT product vendor and the Scheme Owner, if necessary. If disclosure of the evidence is difficult regardless of whether an NDA has been concluded, the IoT product vendor will be allowed to prepare an explanatory document and provide an explanation for the doubt. In addition, a mechanism to revoke labels will be established to ensure the reliability of the Scheme. Specifically, if any of the following are discovered, the label will be revoked.

- The application content is found to be false
- Failure of IoT product vendors, etc. to fulfill their stipulated obligations
- The product no longer meets the conformance criteria
- Nonconformity is discovered during surveillance and appropriate corrective action is not taken during the grace period

The Scheme Owner will inform the public of any nonconformity that is malicious in nature or has a significant impact on procurers and end-users.

3.8 Mechanisms for Cooperation with Related Institutions, Domestic and International Schemes

In order to achieve the three main objectives of Section 2.1, the Scheme will cooperate with related institutions and related domestic and international schemes.

3.8.1 Promotion for Reflection in Procurement Requirements of Organizations

One goal of this Scheme is to facilitate the selection and procurement of IoT products that meet the security levels required by organizations based on the Scheme, while conducting additional checks as necessary.

For government agencies, the National center of Incident readiness and Strategy for Cybersecurity (NISC) and the Secretariat of the Scheme have agreed on the necessity of cooperating on the Scheme, as well as its inclusion in the

"Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies [13] " to ensure its enforcement. Specifically, incorporating the selection of IoT products with at least STAR-1 for "Low Importance" systems and IoT products with at least STAR-3 Stars for "High to Medium Importance" systems in the product selection standard of each agency will be considered, in accordance with the importance of the information system. In addition, it is agreed that government agencies will make procurement of labeled products mandatory by the time labeled products become widely used, in accordance with the required security levels. It has also been confirmed that network cameras, drones, firewalls, routers (wired and wireless), etc. have high priority as product categories that are expected for STAR-3 and above for procurement by government agencies. In addition to the inclusion in the Common Standards and the identification of product categories with high priority for STAR-3 and above, it will be important to publicize product procurement based on this Scheme in meetings with various government ministries and agencies.

For critical infrastructure providers, NISC and the Secretariat of the Scheme have agreed to incorporate use of the Scheme into the "Guideline for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure" etc. based on the "Cybersecurity Policy for Critical Infrastructure Protection "[14] . In addition, NISC and METI have agreed to work on incorporating this Scheme into the procurement of critical infrastructure providers and to request use of systems of at least STAR-2 and above in select systems in critical infrastructure sectors, in coordination with the steering committee of the CEPTOAR Council[15] .

For local governments, MIC and the Secretariat of the Scheme will consider incorporating the Scheme into the "Guidelines for Information Security Policy in Local Governments[16] " after the "Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies" is revised, and in accordance with the situations of local governments.

The Secretariat of the Scheme, NISC, and MIC etc. will cooperate and collaborate to promote these efforts. As it will be difficult to directly approach the procurement requirements of other private companies, the Secretariat of the Scheme will promote efforts in cooperation with entities such as industry organizations and ISACs.

However, even if the selection of labeled products is incorporated into the procurement requirements such as those of government agencies, critical infrastructure providers, and local governments, if labeled products are not widely used at the time of procurement, comparisons between products on non-security factors cannot be made, and options will be limited. Therefore, it is necessary to obtain support from the related industry organizations of IoT products, to collaborate and encourage their member companies to actively obtain the label. The industry organizations that have expressed support for this Scheme at present are shown in Attachment 1.

---

[13] NISC, Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies
https://www.nisc.go.jp/eng/pdf/kijyunr3-en.pdf

[14] NISC, Critical Infrastructure
https://www.nisc.go.jp/eng/index.html#sec4

[15] NISC, CEPTOR Council Meeting Documents (Overview of CEPTOR Council) (in Japanese)
https://www.nisc.go.jp/policy/group/infra/siryou/#si09

[16] Ministry of Internal Affairs and Communications, Study Group on Revision of Guidelines for Information Security Policy in Local Governments (in Japanese)
https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html

3.8.2 Collaboration with Industry Associations and WGs on Schemes in Specific Sectors

IoT products are not only procured alone as single products but are also procured and used when integrated into systems of specific sectors. Given that SMEs and consumers who lack security knowledge are exposed to cyber security risks by being unaware of using IoT products with insufficient security measures, priority should be given to systems in sectors where such procurers and end-users are significant in number. In addition, systems in critical infrastructure sectors should also be given priority due to their social impact in the event of an incident. Specifically, smart home systems, building systems, factory systems, and electric power systems are potential candidates.

The Secretariat of the Scheme will cooperate with industry organizations and working groups of these "systems in specific sectors" that have a high priority, to consider the security requirements and conformance criteria for STAR-2 and above for IoT products incorporated in these systems, including necessity. If a certain percentage of procurers/end-users or business operators of select IoT products express support for a label of said products for procurement/selection or manufacture/sale, (ie. an industry standard can be expected), the Scheme will consider the IoT product for STAR-2 and above.

Security guidelines and certification schemes for the “systems in specific sectors” will be discussed in the respective industry organizations and working groups, and the Secretariat of the Scheme will collaborate as an observer.

3.8.3 Collaboration with Other Countries’ Schemes

Other countries are considering similar conformity assessment schemes for IoT products. The cost to obtain each country’s label is expected to rise for domestic vendors exporting to such countries. It is important that the Scheme reduce such cost by collaborating with other countries’ schemes. The Scheme will examine outlook on such collaboration based on characteristics of schemes of other countries.

Table 3.8-1 Current characteristics of schemes of other countries (non-exhaustive)

Country /Region	Singapore	United Kingdom	United States of America	European Union
Scheme name	Cybersecurity Labelling Scheme (CLS)	Product Security and Telecommunication Infrastructure Act	U.S. Cyber Trust Mark	Cyber Resilience Act (CRA) (December 2023 factsheet)
Implementation	Since October 2020	Into effect in April 2024	Expected to launch during 2024	Set to enter into force in second half of 2024
Mandatory /Voluntary	Voluntary	Mandatory	Voluntary	Mandatory
Scope	Consumer IoT Devices	Consumer connectable products	Wireless consumer IoT devices	Products with digital elements, with exceptions

Security Requirements	*: Part of ETSI EN 303 645[17] **: Part of ETSI EN 303 645[18] in addition to * requirements *** and ****: The nine lifecycle criteria of the IMDA "IoT Cyber Security Guide" in addition to the ** requirements	Part of ETSI EN 303 645 (5.1-1, 5.1-2, 5.2-1, 5.3-13)	Expected to be based on NISTIR 8425	• Expected to include cybersecurity requirements for design, development and production before placing products on the EU market, as well as requirements to report actively exploited vulnerabilities and incidents after the product has been placed on the market, among others • Standardization requests are to be issued after entry into force.
Conformity Assessment	*and**: Self-declaration of conformity *** and****: Self-declaration of conformity and evaluation by a test laboratory	Self-declaration of conformity	Third-party certification	TBD

The conformance criteria for STAR-1 was designed to encompass the criteria for Singapore's CLS and the United Kingdom's PSTI Act, which will be implemented by the time of STAR-1 launch. With regard to the European Union's Cyber Resilience Act (CRA) and the U.S. Cyber Trust Mark, which are expected to be in the development phase at the time of STAR-1 launch, the Secretariat of the Scheme will confirm differences between respective conformance criteria, by either revising the Scheme to address the differences (through revision of the

[17] Provisions 5.1-1, 5.1-2, 5.1-3, 5.1-4, 5.1-5, 5.2-1, 5.3-2, 5.3-3, 5.3-7, 5.3-8, 5.3-10, 5.3-13, 5.3-16 of ETSI EN 303 645

[18] Provisions 5.4-1, 5.4-2, 5.4-3, 5.4-4, 5.5-5, 5.5-7, 5.5-8, 5.6-1, 5.6-2, 5.6-4, 5.8-2, 5.8-3, 5.11-1, 5.13-1 of ETSI EN 303 645 and data protection provisions 6.1, 6.2, 6.3 6.1, 6.2, 6.3, 6.4, 6.5

STAR-1 conformance criteria or through formulation of conformance criteria for STAR-2 and above), or by announcing the additional measures required to address the differences.

For the schemes of Singapore and the United Kingdom, which will be implemented by the time of STAR-1 launch, outlook on mutual recognition will be announced at the time of the official STAR-1 announcement. For the schemes of the United States of America and the European Union, which are expected to be in the development phase at the time of STAR-1 launch, outlook on mutual recognition will be announced in due course. In addition, it is necessary to coordinate with ongoing discussion on international standardization, such as ISO/IEC 27404.

4 Measures for Scheme Growth

4.1 Measures to Promote Label Acquisition by IoT Product Vendors

There are various costs incurred by IoT product vendors in undergoing conformity assessment. In addition, there are many IoT product vendors who lack the capabilities necessary to undergo conformity assessment. From the viewpoint of encouraging dissemination of the Scheme, it is necessary to consider support measures to reduce cost and provide capabilities.

The Secretariat of the Scheme will consider measures such as providing explanations on the Scheme to IoT product vendors, and providing documents (best practices, evaluation guides, etc.) that can be used as reference when making self-declarations of conformity. In the future, providing automated tools for self-evaluation will also be considered. In addition, the Secretariat of the Scheme will consider coordinating with subsidies, as well as discounts for application fees and third-party evaluation fees, with the aim of reducing the burden on IoT product vendors. In addition, the program's dissemination to international IoT product vendors will also be considered.

4.2 Measures to Promote the Scheme to Procurers and End-users

The most significant incentive for IoT product vendors to acquire labels is to ensure that labeled products are actively purchased. In addition, since IoT products are subject to stepping stone attacks, it is important to educate procurers and end-users about the security risks of IoT products, the meaning of labels, the merits of selecting and purchasing labeled products, and security measures that users should take after purchase. It is necessary to consider effectiveness of these measures, as well as possibility of coordination with other measures, and specific methods to raise awareness.

The Secretariat of the Scheme will not only provide procurers and end-users with an overview of the Scheme, but will also inform consumers, in cooperation with IoT product vendors and retailers, of how this Scheme contributes to safety and security, and what differences exist between products with and without labels. In addition, the Secretariat of the Scheme will consider coordinating with subsidies to stimulate demand from procurers and end-users such as small and medium-sized enterprises (SMEs).

4.3 Support Measures for Independent Test Laboratories and Testing Service Providers

As third-party evaluation will be mandatory for STAR-3 and above, it is important that independent test laboratories participate in this Scheme. In addition, IoT product vendors who have difficulty in self-evaluation may request evaluation from independent test laboratories and testing service providers for STAR-1 and STAR-2, and thus it is considered necessary to encourage these entities to provide evaluation and testing services for the Scheme. In light of the above, it is necessary to consider whether support should be provided to independent test laboratories, etc. and, if so, what measures would be best.

Evaluation for STAR-3 and above must be conducted by entities who possess sufficient evaluation and testing capabilities and can conduct objective evaluations independent of IoT product vendors. For this purpose, it is necessary to establish an accreditation scheme based on ISO/IEC17025 to accredit entities that can conduct evaluations of STAR-3 and above under the Accreditation System of National Institute of Technology and

Evaluation (ASNITE)[19] of the National Institute of Technology and Evaluation (NITE). Only these accredited entities with sufficient capabilities and systems will be considered "independent test laboratories" and will be able to conduct evaluations for STAR-3 and above. To continuously secure such independent test laboratories, it is important to continuously secure demand for evaluation of STAR-3 and above through the efforts described in section 3.8.1 and 3.8.2.

Although the self-declarations of conformity of STAR-1 and STAR-2 allow for self-evaluation by the IoT product vendors themselves, the conformance criteria and evaluation procedures for STAR-1 discussed in Section 3.4 also include device check using tools, and is assumed that more specialized capabilities and testing environments will be required for STAR-2 and above. For IoT product vendors who are unable to conduct sufficient evaluation in their own existing systems and facilities, an operator that possesses a certain level of evaluation and testing capabilities can be commissioned to conduct such evaluation with confidence. Such operators will be considered "testing service providers". Since more IoT products are expected to obtain the labels for STAR-1 and STAR-2 than STAR-3 and above, it is necessary to secure not only independent test laboratories but also a wider range of testing service providers. Testing service providers whose services are registered as a Device Testing Service of the Information Security Service Standards Assessment and Registration System [20], which examines and registers conformity to the Information Security Service Standards[21] defined by METI, and whose services are listed in the Information Security Service Standards Compliance Service List[22] , will be considered "testing service providers". In addition, to promote the use of independent test laboratories and testing service providers in the self-declaration of conformity, the following measures to IoT product vendors will be considered.

- Demonstrating the necessary capabilities, prerequisites, and assumed man-hours required for the evaluation of the self-declaration of conformity, and helping to recognize the cost advantages of outsourcing the evaluation to independent test laboratories or testing service providers.
- Posting on the webpage for labeled products whether the evaluation for the self-declaration of conformity was a self-evaluation by the IoT product vendor or by a third-party (an independent test laboratory or testing service provider) for procurer and end-user identification.
- Providing support such as subsidies for third-party evaluation fees for IoT product vendors that are small and medium-sized enterprises that do not have sufficient systems and facilities to conduct self-evaluation and have difficulty in securing the cost of outsourcing to independent test laboratories or testing service providers.

4.4 Measures to Secure Resources to Address Risks

Even if IoT product vendors, procurers/end-users, independent test laboratories, certification bodies, etc. fulfill their respective responsibilities, the possibility of damage caused by cyber-attacks cannot be reduced to zero. It is

[19] NITE, National Institute of Technology and Evaluation (ASNITE) Accreditation System https://www.nisc.go.jp/policy/group/infra/siryou/#si09 https://www.nite.go.jp/en/iajapan/asnite/index.h
[20] JASA, Information Security Service Standards Assessment and Registration System (in Japanese) https://sss-erc.org/
[21] Ministry of Economy, Trade and Industry, Information Security Service Standards (in Japanese) https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html
[22] IPA, Information Security Service Standards Compliance Service List (in Japanese) https://www.ipa.go.jp/security/service_list.html

necessary to consider what kind of effective measures should be taken to secure resources to properly deal with an incident when it occurs, including remedying the damage and correcting the cause of the incident. Specifically, there is possibility to collaborate with the "Information Security Early Warning Partnership," which is a framework to achieve an appropriate flow of vulnerability-related information and insurance to diversify risks in society.

It is appropriate to build a society that widely diversifies damages in preparation for incidents. For example, collaborating with product cyber insurance schemes that cover compensation damages and cost damages of cyber accidents caused by products that received services provided by independent test laboratories or testing service providers could be considered. In addition, the Secretariat of the Scheme will take the lead in studying the establishment of a mechanism to promote early response by establishing an appropriate flow of vulnerability-related information of labeled products in cooperation with the "Information Security Early Warning Partnership".

4.5 Measures to Improve Efficiency of the Entire Scheme

Various types of devices are widely deployed as IoT products, and the number of products within scope for evaluation is expected to increase. Under these circumstances, the challenge is to improve the efficiency of certification and management of this Scheme. Establishing an efficient process will reduce the time and costs involved in the product labeling and certification process and will help ensure the sustainability of the Scheme. Based on the above, it is necessary to study the efficiency of certification and management operations.

To streamline and simplify the operational process, improvement methods will be studied by the Secretariat of the Scheme, and feasibility of such methods will be evaluated. In addition, the Secretariat of the Scheme will also consider the possible use of SBOM and early warning partnerships to appropriately share vulnerability information and promptly apply patches in order to address vulnerabilities in labeled products with STAR-3 and above. In doing so, the committee will pay attention to coordination with industry associations that are already working on SBOM.

5 Outlook and Schedules for Future Consideration

For STAR-1, the Secretariat of the Scheme plans to explain the Scheme to major IoT product vendors and their industry associations to request preparation for label acquisition in the first half of FY2024, and to officially announce the start of the Scheme in the middle of FY2024 (around late September). At the time of official announcement, the Secretariat of the Scheme plans to present outlook on mutual recognition with Singapore and the United Kingdom, whose schemes will be implemented by the time of STAR-1 launch. For the European Union and the United States of America, whose schemes are expected to be in the development phase at the time of STAR-1 launch, outlook will be announced in due course. The target for STAR-1 launch, or start of labeling products for STAR-1, is during FY2024 (by March 2025).

For STAR-2 and above, conformance criteria will be discussed in cooperation with industry organizations and working groups of "systems in specific sectors" in the first half of FY2024. Conformance criteria for certain IoT product categories will be developed in the second half of FY2024. The target for STAR-2 launch or start of labeling products for STAR-2 in certain IoT product categories, is during or after the second half of FY2025.

In parallel, the Secretariat of the Scheme will coordinate the mandatory procurement of labeled products in government agencies, etc. and encourage critical infrastructure providers and local governments to incorporate the use of the Scheme into their IoT product procurement rules.

Scheme development during and after FY2024 will be managed mainly by the Steering Committee and Secretariat of the Scheme.

List of Supporting Organizations Related to IoT Product Vendors

*in alphabetical order, as of March 2024

Organization Name	Abbreviation	Homepage	Membership
Communications and Information network Association of Japan	CIAJ	https://www.ciaj.or.jp/	140 companies/organizations (as of March 2024) • Full members 89 companies/organizations • Supporting members 51 companies/organizations
Japan Electronics and Information Technology Industries Association	JEITA	https://www.jeita.or.jp/	380 companies/organizations (as of February 14, 2024) • Full members 343 companies/organizations • Affiliate Members 37 companies/organizations
Japan Security Systems Association	SSAJ	https://www.ssaj.or.jp/	275 companies/organizations (as of June 2023) • Full members: 76 companies • Associate members: 150 companies • Affiliate members: 5 organizations • Special members: 44 organizations