Beyond Digital
Innovation Platform Agency, Japan

JST-SR-03-01-2026

Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR) STAR-3 Security Requirements for Network Devices (tentative)

June 2026

Innovation Platform Agency, Japan (IPA)

Table of Contents

1. Introduction

1.1 What is JC-STAR?

JC-STAR (Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements) is a Japanese Scheme to confirm and visualize conformance of IoT products to conformance requirements based on its own conformance requirements (security technical requirements), in harmony with ETSI EN 303 645, NISTIR 8425, and other standards. For details of the Scheme, refer to the following:

Scheme details (in English): https://www.ipa.go.jp/en/security/jc-star/index.html

JC-STAR has set four levels of security technology requirements in accordance with the required security level: STAR-1 conformance requirements and assessment procedures for products to respond to the minimum level of threats, and STAR-2 to STAR-4 conformance requirements and assessment procedures for each type of IoT product.

IoT products covered by STAR-3 include IoT devices that are expected to be procured and installed by government agencies, critical infrastructure providers, local governments, and large enterprises. This document describes the STAR-3 requirements for "network devices."

Table 1: Positioning of Requirement Levels in JC-STAR

<table>
<tr><th>Level</th><th>Positioning</th><th>Conformance Requirements</th><th>Evaluation/ Assessment Method</th></tr>
<tr><td>STAR-4</td><td rowspan="2">Defining generic security requirements for each product type for use in critical systems of government agencies, critical infrastructure providers, local governments, and large enterprises, and indicating an independent third party’s evaluation that these requirements are satisfied.</td><td rowspan="3">By product type</td><td rowspan="2">Evaluation by third party</td></tr>
<tr><td>STAR-3</td></tr>
<tr><td>STAR-2</td><td>Defining basic security requirements that should be added to STAR-1 in consideration of the characteristics of each product type and indicating a self-declaration by the product vendor that these requirements are satisfied.</td><td rowspan="2">Self-declaration of conformance</td></tr>
<tr><td>STAR-1</td><td>Defining minimum security requirements commonly required for products, and indicating a self-declaration by the product vendor that these requirements are satisfied.</td><td>Common product type</td></tr>
</table>

1.2 What is a Conformance Label?

A conformance label **indicates that an IoT product has achieved the minimum level of security functionality required** to counter the threats anticipated by the conformance requirements and assessment criteria for conformance. In order to promote the fact that their IoT products have already acquired a conformance label, IoT product vendors can include, attach, or use the conformance label on the product itself, packaging, instruction manuals, brochures, websites, etc., and this will allow them to appeal their security measures to procurers and purchasers.

Figure 1: STAR-3 conformance label (sample)

The following points shall be noted when acquiring and maintaining the conformance label.

The label indicates conformance to the specified conformance requirements but does not assure complete and total security.

- STAR-1 and STAR-2 are self-declaration of conformance methods whereby IPA grants a conformance label based on a checklist describing the results of self-assessment conducted by IoT product vendors in accordance with the conformance requirements and assessment procedures specified in this Scheme. IPA does not check whether the vendor conforms to the conformance requirements at the time the conformance label is issued. In other words, the reliability of the assessment depends on the vendor's reliability.
- STAR-3 and STAR-4 are intended for products for government agencies, critical infrastructure providers, etc., whereby IPA certifies and grants a conformance label, based on the Evaluation Reports from independent third-party Evaluation Bodies, which ensures a higher level of reliability.
- In the case of mutual recognition with overseas schemes, the evidence may be required to be submitted for a longer period of time than required by JC-STAR, so the retention period of the evidence shall be noted.

On the other hand, in the case of conformance labeled products where there are any doubts about the conformance of a labeled product to the conformance requirements, IPA has the right to conduct surveillance, and if necessary, IPA may request the submission of evidence, re-implementation and reporting of conformance assessment/evaluation. IPA also balances credibility by including a mechanism whereby conformance label may be revoked depending on the results of the surveillance.

In addition to the level of conformance label and registered ID acquired by the IoT product, the conformance label will incorporate a two-dimensional barcode that embeds the URL of the IoT product information page (for each conformance labeled product) managed by IPA to confirm the IoT product information. The product information page incorporates a mechanism to provide a wide scope of information on IoT products with a conformance label, including applicant information, product information, conformance label information, security information (update information, vulnerability information, etc.), and contact information, in a one-dimensional format while keeping the information up to date.

Table 2: Status Indication with Conformance Label Information

Status of conformance label	**Summary**
Active	The conformance label is within the validity period and there are no grounds for withdrawal or revocation.
Deferral of expiration (Extension procedure in progress)	The validity period of the conformance label has expired, but the application procedure for the extension of the validity period is in process.
Expired	The validity period of the conformance label has expired and has not been extended. The conformance label is no longer valid.
Withdrawn	A condition in which a conformance label has been withdrawn by the IoT product vendor at the request of the IoT product vendor during the validity period of the conformance label.
Revoked	A state in which IPA mandatorily suspends the validity of a conformance label when an event that constitutes grounds for revocation of a conformance label occurs during the validity period of the label and no corrective action is taken to resolve the event within a specified period.

1.3 Flow of STAR-3 to Grant a Conformance Label based on the Self-declaration of Conformance

The procedure differs depending on the level of conformance label for which the application is made. It is mandatory that STAR-3 level conformance evaluation shall be conducted by a third-party Evaluation Body (JC-STAR Evaluation Body) approved by IPA.

The main procedures from the application for a conformance label to the grant of the conformance label are as follows. For details, refer to the latest procedures on the website.

Application Process (in English)

https://www.ipa.go.jp/en/security/jc-star/shinsei/index.html

[Procedures]

1. IoT product vendors shall apply to IPA for acquisition of a conformance label.
2. IPA shall conduct the necessary verification procedures together with the Ministry of Economy, Trade and Industry (METI). If the application is deemed acceptable as a result of the verification procedures, a "Letter of Acceptance of Application/Notification of Application Fee" will be issued. If the application is deemed incomplete, the application is returned, and the documents shall be resubmitted. If the application is not accepted, the application will be rejected, and the procedure will be terminated.
3. Upon receipt of the "Letter of Acceptance of Application/Notification of Application Fee," the IoT product vendor shall pay the application fee to IPA.
   Note that IPA will not start the certification process until the prescribed application fee has been transferred.
4. The IoT product vendor shall select an Evaluation Body from the "JC-STAR Evaluation Bodies" and request the conformance evaluation by presenting the "Letter of Acceptance of Application" to the Evaluation Body.
   It is acceptable to consult with the JC-STAR Evaluation Body prior to applying for a conformance label and requesting evaluation.
5. After submitting a request for evaluation of IoT products, the IoT product vendor will receive the "Evaluation Body Evaluation Services Eligibility Checklist" from the Evaluation Body and shall submit the checklist to IPA.
6. The Evaluation Body shall conduct the conformance evaluation in accordance with the conformance requirements and evaluation procedures for STAR-3 (Level 3) and submit a "Notification of Certification Work in Charge" describing the evaluation results to IPA.
7. IPA performs the certification work based on the “Conformance Evaluation Report.” If there is any doubt about the contents of the Evaluation Report, a Certification Review will be issued,

and additional evaluation will be requested. If the final conformance decision is acceptable, IPA will grant a conformance label to the IoT products for which the application is submitted.
If the certification process is not completed within 12 months from the date of issuance of the "Letter of Acceptance of Application/Notification of Application Fee," the certification will not be acceptable, and the application will be rejected.

1.4 Validity Period of STAR-3

The validity period is two years from the date of issuance of the conformance label (or a validity period of less than two years can be set upon application).
To extend the validity period, the IoT product vendor shall submit an extension application to IPA, and the necessary verification procedures will be conducted on the application documents. If the verification process determines that the extension is acceptable, the validity period of the conformance label will be extended for one year (or for a period of one year or less upon request). The validity period can be extended up to three times for a total of five years from the date of issuance of the first conformance label. If the total validity period exceeds five years, the STAR-3 conformance label shall be re-certified within the validity period.

Even if there is a major revision of the conformance requirements during the validity period (addition of items or major changes in the conformance requirements) and the grace period (transition period during which the old version is kept along with the new version) ends, the conformance label will not expire in the middle of the validity period. However, an extension of the validity period after the grace period cannot be applied for, and re-certification of the STAR-3 conformance label will be required.

If any changes are made to the security functions, etc., of STAR-3 products during the validity period that may affect the results of the STAR-3 conformance evaluation, a re-evaluation by the Evaluation Body may be required.
If there are any updates or changes to firmware or IoT products during the validity period, refer to IPA website separately and take necessary actions.

1.5 Structure of STAR-3 Conformance Requirements, etc.

STAR-3 Conformance Requirements, etc., consist of three parts: "**STAR-3 Security Requirements,**" "**STAR-3 Conformance Requirements, " and "STAR-3 Evaluation Guide**."

- "**STAR-3 Security Requirements**" are the security measures and requirements that shall be satisfied for an IoT product to qualify as STAR-3 level.

- "**STAR-3 Conformance Requirements**" are specific requirements that shall be satisfied for STAR-3 level IoT products, such as functions that STAR-3 level IoT products shall have and measures that IoT product vendors shall take, in response to the measures and requirements described in STAR-3 security requirements.
- "**STAR-3 Evaluation Guide**" describes the evaluation methods to check whether the requirements for the STAR-3 conformance requirements satisfy [Document evaluation] and [Device check].

This document describes "STAR-3 Security Requirements."
For actual evaluation of conformance and certification, "STAR-3 conformance requirements" shall be satisfied in order to determine that the "STAR-3 security requirements" in this document are satisfied. In addition, the specific evaluation method described in the "STAR-3 Evaluation Guide" is used to determine whether the "STAR-3 conformance requirements" have been satisfied.
In other words, even if you take measures based on your own interpretation of the "STAR-3 Security Requirements" in this document, your IoT product will not be able to acquire a conformance label unless the product is certified through a conformance evaluation against the "STAR-3 Conformance Requirements" and the "STAR-3 Evaluation Guide."

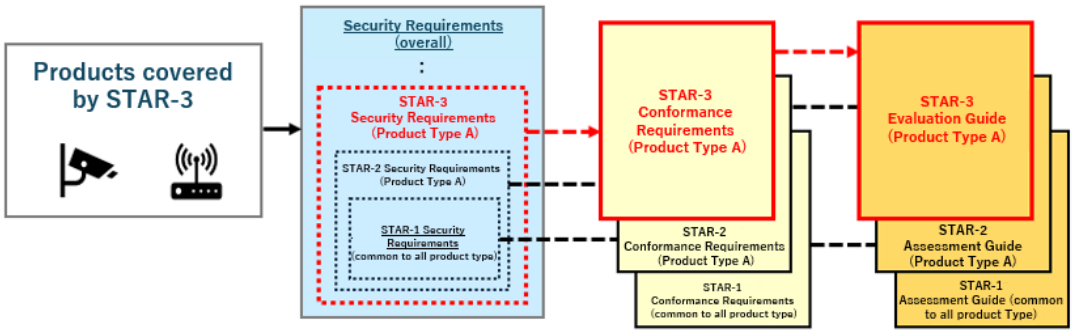


Figure 2: Structure of STAR-3 Conformance Requirements

The domestic and international security requirements considered for STAR-3 NW cameras covered in this document are listed below.

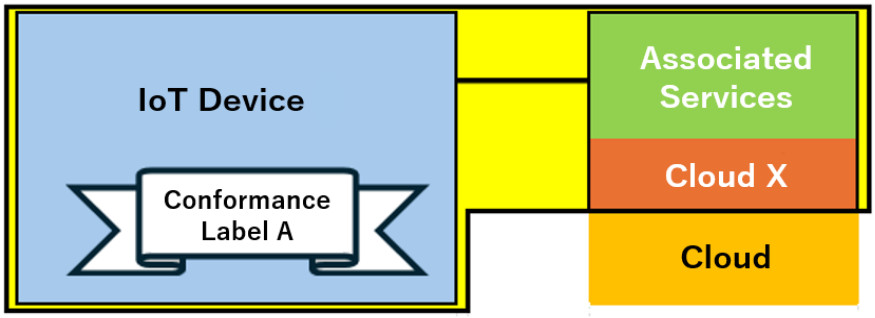
Table 3: Domestic and International Security Requirements

No.	Name of Scheme/Guideline
1	ETSI EN 303 645 V3.1.3 (2024-09)
2	Cybersecurity Labelling Scheme (CLS) Publication No. 4 Version 1.2 April 2025
3	Cyber Resilience Act (CRA) 23 October 2024
4	Radio Equipment Directive (RED): 28.12.2024
5	EN 18031-1 / -2 / -3:2024
6	IEC 62443-4-1 2018
7	IEC 62443-4-2 2019
8	NIST IR 8425 September 2022
9	UK PSTI Act Regulation 2023
10	Partial revision of the Guidelines for the Establishment of Standards for Measures by Government Agencies (September 2025)
11	CCDS Guidelines for Conformance Requirements for Security of IoT devices 2025 Ver. 1.0
12	RBSS Security Camera Certification Criteria 2024.04.01
13	Specific Purpose Devices Common Security Protection Profile Ver. 1.0
14	MIC: Ordinance Concerning Terminal Facilities, etc., Enacted October 1, 2025

1.6 Explanation of "IoT products" and "IoT devices"

"IoT products" under JC-STAR refer to products that serve as a unit of being sold by the supplier or being purchased by users, and include either a single "IoT device" designed to achieve an intended purpose, or a complete set consisting of "IoT devices" and "associated services." "Associated services" refer to services that "must be used as a set" by the target "IoT device." Specifically, they are services that are provided in conjunction with the IoT device in cases [where the IoT device itself cannot provide the purpose intended by the IoT products.]

For example, if a network device is configured to send and store logs related to communication access to a specific cloud service, the service is considered an associated service. In this case, the scope of evaluation/assessment for the conformance label includes the "network device," the "cloud service," and the entire communication path connecting the two. Note that the conformance label is granted to the "network device."



[Note] Cloud X: Cloud area directly utilized by the service

Figure 3: Example of Classification of IoT products and IoT devices

There are no restrictions on the form of the provision of associated services other than the condition that they are "provided as a set with the competing IoT device." For example, associated services may include digital services, such as mobile applications, cloud computing/storage, and third-party application programming interfaces (APIs).

Note, however, that if the opposing services to IoT devices cannot be identified, the services are considered "external systems" which do not fall under "associated services."

In this document, the distinguishing factor between associated services and external systems is whether the services provided on the system are provided under the control of the IoT device manufacturer. In other words, if services are provided under the manufacturer's control, they are referred to as "associated services"; if they are used under the control of users rather than the manufacturers, they are referred to as "external systems."

2. STAR-3 Network Devices

2.1 Main Scope of STAR-3 Conformance Label (Network Devices)

It is considered that "Network devices" as assumed in STAR-3 conformance label refer to **network devices with representative function and management function that handle IP packets, which are mainly procured and installed by government agencies, critical infrastructure providers, local governments, and large corporations**, rather than network devices intended for general households (home routers, residential Wi-Fi routers, etc.).

For example, it is expected to be installed in the following locations

- Areas requiring management measures (e.g., security areas, server rooms, etc.)
- Inside locked racks or other locations within a facility
- Compartments in common areas within a facility where physical security is taken into consideration (e.g., government offices, personnel areas, etc.)
- Compartments of common areas in the facility (e.g., waiting halls, common areas, atriums, etc. in city halls)

The scope of coverage assumes network devices with functions such as routing/switching, filtering, VPN, etc., in the type of use as shown in Figure 4 (e.g., the devices in the red box plus the associated services in the green box).

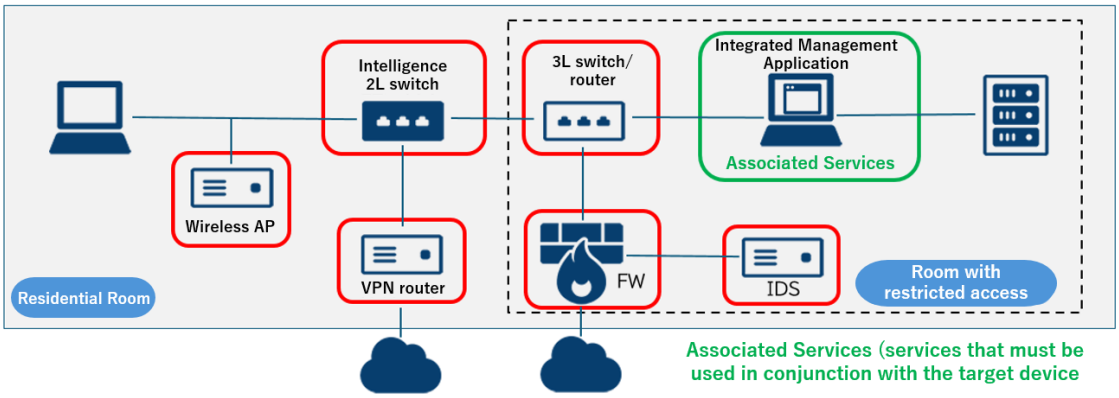


Figure 4: Example of STAR-3 Network Devices

3. STAR-3 Security Requirements for Network Devices

3.1 Concept of Deriving STAR-3 Security Requirements for Network Devices

In deriving security requirements and conformance requirements for STAR-3 network devices, we examined the main threats that should be considered for network devices for government, etc., as well as threats in communications in general, and extracted attack methods at CAPEC based on its threat list. Specifically, threats to be considered are listed based on the assumption of a level that can prevent past incidents caused by intermediate-level attackers who have a certain level of expertise and use undisclosed information and simple tools to conduct attacks.

- Attacks by Mirai and Mirai variants (response to the risk of becoming a bot)
- Malware infection by automated attacks (response to the risk of malicious code inclusion)
- Intrusion using valid IDs and passwords (response to the risk of intrusion into internal networks)
- Attacks on other devices via jump server (response to the risk of being used as a jump server)
- Attacks exploiting known and unknown vulnerabilities (response to vulnerabilities and risks associated with inadequate vulnerability testing)
- Denial-of-service attacks targeting governments, municipalities, and enterprises (response to malicious attack risk)
- Attacks with backdoors in the supply chain (response to supply chain risk)

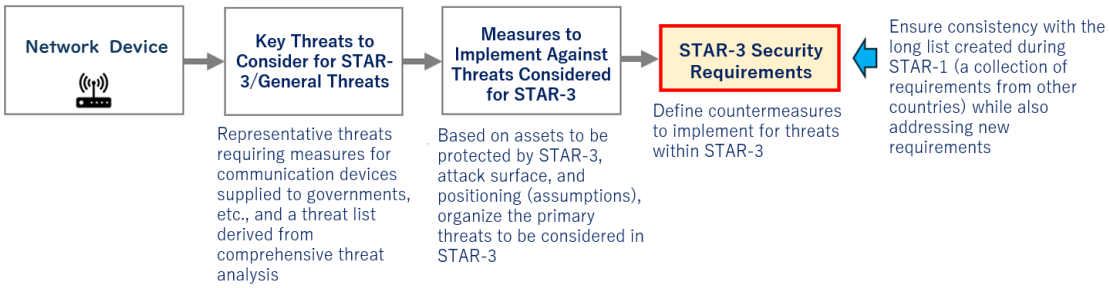


Figure 5: Image of the Process for Extracting STAR-3 Security Requirements

Security requirements were selected from the following three perspectives as measures that should be realized by IoT products themselves or by IoT product vendors and summarized as shown in Table 4.

1) Measures against major attack methods against network devices based on the threats listed in the above analysis
2) Measures also required by STAR-1

3) Measures judged to be necessary in consideration of the level of other schemes and standards for network devices

Note that STAR-3 conformance requirements that need to be satisfied specifically, such as functions that need to be equipped against security requirements and measures that need to be taken by IoT product vendors, will be described in the "Conformance Requirements and Evaluation Guide."

Table 4: Security Requirements to be Realized in STAR-3 to Counter Attack Methods

<table>
<tr><th rowspan="3">Major attack methods to be considered in STAR-3</th><th colspan="6">Security requirements to be realized in STAR-3 to counter attack methods</th></tr>
<tr><th colspan="3">Measures to be taken by IoT products</th><th colspan="3">Measures to be taken by IoT product vendors</th></tr>
<tr><th>Types of measure</th><th>Overview of STAR-3 conformance requirements</th><th>Require-ment No.</th><th>Types of measure</th><th>Overview of STAR-3 conformance requirements</th><th>Require-ment No.</th></tr>
<tr><td rowspan="6">1. Unintended access attacks from outside due to the use of vulnerable passwords</td><td rowspan="6">Identifica-tion/authen-tication, access control</td><td>- Implement a mechanism to prevent the setting of passwords that can be easily guessed</td><td>S3.2-02</td><td rowspan="6">Information provision</td><td rowspan="6">- Provide information on secure usage</td><td rowspan="6">S3.2-03</td></tr>
<tr><td rowspan="4">- Provide a secure authentication mechanism</td><td>S3.2-01</td></tr>
<tr><td>S3.2-05</td></tr>
<tr><td>S3.2-06</td></tr>
<tr><td>S3.2-07</td></tr>
<tr><td>- Provide mechanisms to prevent brute force authentication attempts</td><td>S3.2-04</td></tr>
<tr><td rowspan="2">2. Measures against attacks leading to information leaks, tampering, or functional</td><td rowspan="2">Security software and software updates</td><td>- Measures against known vulnerabilities of high severity and major CWEs</td><td>S3.1-42</td><td rowspan="2">Acceptance and provision of information and inquiries</td><td>- Provide information on products and vulnerabilities</td><td>S3.1-14</td></tr>
<tr><td>- Implement mechanisms to enable software components to be updated</td><td>S3.1-10</td><td>- Publish a vulnerability disclosure policy</td><td>S3.1-09</td></tr>
</table>

anomalies caused by unpatched vulnerabilities resulting from unaddressed vulnerabilities, as well as malware infections and jump server attacks		- Implement an automatic update function	S3.1-10			S3.1-43
		- Implement measures to prevent unauthorized update packages from being applied	S3.1-12	Disclose update methods	- Provide information on how to apply security patches	S3.1-11
			S3.1-19	Management of update patches	- Manage to apply the latest patches	S3.1-13
3. Measures against attacks leading to information leakage, tampering, attacks that lead to functional anomalies, malware infections, and jump server attacks, caused by external access via unintended interfaces	Management of connected devices	- Filtering function	S3.1-08	--		
	Logical access to interfaces	- Disable unnecessary interfaces	S3.1-23			
		- Minimum execution privileges	S3.1-28			
	Access to physical interfaces	- Disable unused interfaces	S3.1-25			
		- Disable debug interfaces	S3.1-25			
		- Minimal execution privileges	S3.1-28			
	Minimal software services	- Default enabled software services are the minimum required	S3.1-24			
			S3.1-26			
			S3.1-27			
4. Eavesdropping on sensitive information in communications	Data protection	- Implement safeguards against information leakage and modification to protect protected information transmitted in	S3.1-20	Management processes	- Secure management of encryption keys	S3.1-21
			S3.1-22			

		communications via the Internet				
5. Theft of securely stored information from discarded or resold devices	Data protection	- Provide a function that allows the deletion of information to be protected stored in a device while the device is in use, via the product itself or related services	S3.1-36	Information provision	- Provide information on secure disposal methods. - Provide information on initialization methods - Provide information on how to delete data	S3.1-36
		- Provide functions to protect information that should be protected from the outset in the device.	S3.1-16			S3.1-37
		- Provide initialization function of the device	S3.1-37			
6. Attacks such as network disconnections and power outages aimed at anomalies in security functions	Improve resilience	- Even if an event such as network disconnection or power failure occurs and the system is restored, authentication information and software settings do not return to their initial state and the state before the power was turned off shall be provided	S3.1-33	--		
			S3.1-34			
7. Attacks on stored telemetry data	Data protection	- Provide functions to protect telemetry data to be protected held by devices	S3.1-35	Information provision	- Provide information on secure disposal methods	S3.1-44
			S3.1-40		- Provide information on the data types of telemetry data collected on devices	S3.1-32
						S3.1-40
8. Attacks on securely stored information	Data protection	- Provide functions to protect securely stored information held by the device	S3.1-16	Information provision	- Provide information on secure disposal methods	S3.1-36
			S3.1-17			S3.1-39

			S3.1-18			
		- Provide implementation of a function that allows users to delete/destroy personal information, configuration information, etc.	S3.1-36		- Provide information on the types of personal data collected on devices	
			S3.1-41			
9. Denial of Service Attacks	Improving resilience	- Provide a function to recover from a network load condition caused by a denial-of-service attack	S3.1-45	--		
10. Physical Attacks	Enclosure tampering	- Provide mechanisms to prevent physical destruction or modification of the enclosure	S3.1-46	--		
11. Attacks due to unintended entry or data	Verification of input data	- Provide a function to check the validity of data entry to the device	S3.1-38	--		
12. Attacks that activate unintended software	Secure boot	- Provide the ability to verify the integrity of software to be activated	S3.1-31	--		
13. Supply chain attacks	Software controls	- Secure third ware components shall be incorporated.	S3.1-30	Introduction of SBOM (Software Bill of Materials)	- Create SBOM and manage software components including vulnerabilities and licenses	S3.1-15
					- Software development is securely managed	S3.1-29

3.2 Types of Information Assets to be Protected in STAR-3 Network Devices

"Protecting information" has two meanings. The first means "taking measures to prevent security issues, such as unauthorized access or data breaches, from occurring when information that should be protected is leaked to unauthorized parties due to improper disclosure or exposure"; that is, "protecting the confidentiality of information." The other means "taking measures to ensure that information is not relied upon or used despite the fact that its reliability or integrity has been compromised by tampering or forgery, thereby creating a dangerous situation"; that is, "protecting the integrity of information."

Therefore, information that requires protection of either "confidentiality" or "integrity" is referred to as "information assets to be protected." Taking into account use cases and implementation environments for network devices, Table 5 defines the "information assets to be protected" for STAR-3 network devices. For these assets, protection of either "confidentiality" or "integrity" is required as necessary for each specific information asset.

Furthermore, "information assets that require confidentiality protection when transmitted over the network" are referred to as "sensitive communication information," and communication via a communication protocol that employs appropriate encryption is required. The information assets subject to this requirement are specified in Table 5 (1).

"Information assets to be protected that are stored on IoT devices" are referred to as "securely stored information," and appropriate protection of either "confidentiality" or "integrity" is required. The information assets subject to this requirement are specified in Table 5 (2).

Note that Table 5 lists the minimum types of "information assets to be protected" for which secure management is required for all STAR-3 network devices; this does not preclude treating other information assets not included in this list as "information assets to be protected" on their own.

Table 5: Types of Information Assets to be Protected by Network Devices
(1) Sensitive communication information, (2) Securely stored information
Legend: ○ indicates included; – indicates excluded

Information assets held by STAR-3 network devices	Information to be protected	(1)	(2)
CSP (Critical Security Parameter)	Confidential security-related information whose exposure or tampering could compromise the security of a security module. Examples: secret encryption keys, passwords and other authentication values, PINs, private elements of certificates	○	○
PSP (Public Security Parameter)	Publicly available security-related information which, if tampered with, could compromise the security of security modules. Example 1: Public keys used to verify the authenticity and integrity of software updates. Example 2: Public elements of certificates.	–	○
Configuration information related	Information that shall be configured in advance to prepare for communication.	○	○

to communication functions (*1)	Example: Communication settings: IP address, subnet mask, default gateway, DNS server, domain name, etc. Router configuration function: Routing, QoS, DHCP (server/relay agent), etc. Function settings: HTTP port configuration (HTTP/HTTPS), IEEE 802.1X network access control settings.		
Configuration information related to security functions (*1)	Information that shall be configured in advance to prepare for enabling security functions. Example: Router configuration settings: firewall, VPN, logs, statistics management, etc. Firewall configuration settings: filtering, networks permitted for administrator access, application control, etc. Function-related configuration settings: authentication information (user authentication/host authentication), digital certificates, user privilege settings.	○	○
Alert Information	Alert information triggered when network devices detect signals indicating anomalies, the specific details of the anomalies, or security-related anomalies.	○	–
Program code	Software	–	○
Logs (telemetry data, audit logs)	Telemetry data (e.g., metrics) generated while the network device is in operation.	–	○
	Audit logs (including communication logs, event logs, etc.) generated while the network device is in operation (*2).	○	○

(*1): This assumes that communication is required as a prerequisite for enabling the function.

(*2): It is assumed that audit logs on network devices refer to communication logs, event logs, etc. Since these audit logs may contain personal information, they are subject to "sensitive information" to be protected.

3.3 Classification Categories of Measures

As shown in Table 6, there are various measures that should be implemented to counter various attack methods.

Therefore, classification categories that summarize similar measures are defined as follows.

Conformance requirements are organized according to these categories. Note that not all measures in all categories are required.

Table 6: Classification Categories of Measures

Classification Category	Outline
Category 1: Not using vulnerable authentication/ authorization mechanisms (e.g., universal default passwords, vulnerable passwords)	Measures to prevent easy unauthorized access or privilege seizure that could cause security problems
Category 2: Implementing means to manage vulnerability reporting	Measures to clarify the process by which security researchers and others can report problems and the policy for handling vulnerability reports so that information on vulnerabilities affecting the product can be quickly collected
Category 3: Keeping software up-to-dated	Measures to ensure that products do not continue to be used without addressing vulnerabilities that are discovered or reported
Category 4: Secure storage	Measures to protect the information assets to be protected from information leaks and tampering
Category 5: Secure communication	Measures to protect sensitive communication from eavesdropping and tampering during transmission over communication channels
Category 6 Minimizing exposed attack surfaces	Measures to minimize accessible functions and interfaces to reduce the risk of attacks
Category 7: Ensuring software integrity	Measures to protect software integrity so that software tampered with by attackers is not installed on or run by products
Category 8: Ensuring that personal data is secure	Measures to protect personal data
Category 9: Making the system resilient to outages	Measures to ensure that systems have a certain level of resilience and can operate securely in the event of power or network outages
Category 10: Verifying and protecting system telemetry data	Measures to enable detection of security anomalies during operation by collecting logs and telemetry data

Category 11: Allowing users to easily erase data	Measures to prevent leakage of data (especially user-related data) generated and accumulated during product use by transferring or disposing of the product
Category 12: Facilitating product installation and maintenance	Measures to enable users to easily configure secure settings during product installation and subsequent operation
Category 13: Checking the validity of input data	Measures to protect products from input containing unauthorized code by attackers by checking the format of data received
Category 14: Processing personal data appropriately	Measures to ensure that when personal data is collected or used by the product, it is not used for unauthorized purposes for which the user did not intend
Category 15: Making products identifiable	Measures to ensure that the target device can be uniquely identified in security functions
Category 16: Identifying and testing threats	Measures to reduce security risks by analyzing possible threats to the use of the product and testing and verifying that the necessary security functions are implemented
Category 17: Providing information on products	Measures to require manufacturers to provide users with the information necessary to use their products securely
Category 18: Documentation	Measures to require manufacturers to create and maintain security-related documentation throughout the product development life cycle
Category 19: Ensuring product availability	Measures to require effective design and implementation to protect product availability
Category 20: Establishing secure sessions	Measures to protect against spoofing, tampering, and eavesdropping in communications and to establish secure communications
Category 21: Ensuring hardware integrity	Measures to protect against threats such as physical destruction or tampering with the product

4. STAR-3 Security Requirements for Network Devices

[STAR-3 Structure of security requirements]

The following structure is described for each security requirement.

Table 7: Structure of Security Requirements

Category	Classification category to which the measures to STAR-3 security requirements required are applied
Security Requirement Number: S3.1-xx	Security requirement number
STAR-3 Security Requirements	Security measures and requirements that shall be satisfied for STAR-3 level IoT products.
Conditions for being Not Applicable (NA) and Supplementary explanation of the requirement	Conditions for being Not Applicable (NA) from STAR-3 security requirements and supplementary explanation of STAR-3 security requirements. When claiming that it falls under "Not Applicable (NA)," the documentation demonstrating that the "Conditions for being Not Applicable (NA)" as described in this item are satisfied shall be provided to the Evaluation Body.

Category 1: Not using vulnerable authentication/authorization mechanisms (e.g., universal default passwords, vulnerable passwords)

Security Requirement Number: S3.1-01

STAR-3 Security Requirements

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

For operations such as important setting changes, the above authentication methods shall be re-enforced.

Conditions for being Not Applicable (NA)

There is no mechanism for access. (The rationales for why there is no external access shall be described in the "Reasons for being Not Applicable (NA).")

Supplementary explanation of the requirement

[Term: user]

The scope of users shall include all natural persons and organizations that use the IoT products which have access to the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-02

STAR-3 Security Requirements

For IoT products that use passwords in the user authentication mechanism via the network for IoT products, when a default password is used at the time of installation of the IoT product, either of the following requirements (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 8 characters in length that cannot be easily guessed.

(2) A function that requires users to change the password at the first startup shall be implemented, and users are required to set a password of 8 characters or more that cannot be easily guessed as a password that can be set in the function.

Conditions for being Not Applicable (NA)

There is no mechanism for user authentication using passwords. (The rationales for why user authentication using passwords is not required to counter threats shall be described in the "Reasons for being Not Applicable (NA).")

Supplementary explanation of the requirement

[Term: user]

The scope of users shall include all natural persons and organizations that use the IoT products which have access to the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-03

STAR-3 Security Requirements

It shall be possible to change the authentication values used for user authentication of access to IoT products through the networks from other IoT devices or users, regardless of the authentication type (password, token, fingerprint, etc.).

Conditions for being Not Applicable (NA)

There is no mechanism for user authentication or device authentication. (The rationales for why user authentication and device authentication are not required to counter unauthorized access from outside shall be described in the "Reasons for being Not Applicable (NA).")

Supplementary explanation of the requirement

[Term: 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 password information. For the biometric fingerprint authentication, the authentication value is the fingerprint data of the index finger of the left hand, for example.)

[Term: user]

The scope of users shall include all natural persons and organizations that use the IoT products which have access to the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-04

STAR-3 Security Requirements

The mechanism for user authentication via the network to IoT devices shall make brute force attacks difficult.

Conditions for being Not Applicable (NA)

There is no mechanism for user authentication. (The rationales for why user authentication is not required to counter unauthorized access from outside shall be described in the "Reasons for being Not Applicable (NA).")

Supplementary explanation of the requirement

[Term: user]

The scope of users shall include all natural persons and organizations that use the IoT products which have access to the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-05

STAR-3 Security Requirements

Digital certificates used for authentication in IoT products shall have sufficient security strength.
Digital certificates used in IoT products shall be renewable.

Conditions for being Not Applicable (NA)

No digital certificates are used for authentication. (The fact that digital certificates are not used shall be described in the "Reasons for being Not Applicable (NA).")

Security Requirement Number: S3.1-06

STAR-3 Security Requirements

When SSH is used for public key authentication in IoT products, the public key authentication function shall use secure cryptographic algorithms.

Conditions for being Not Applicable (NA)

SSH is not used for public key authentication. (The fact that SSH is not used for public key authentication shall be described in the "Reasons for being Not Applicable (NA).")

Security Requirement Number: S3.1-07

STAR-3 Security Requirements

IoT products with VPN gateway function shall meet all of the following requirements (1) and (2).

(1) The product shall have a function to perform multi-factor authentication for user authentication.
(2) It shall have a function to restrict the devices, etc., from which it is connected.

Conditions for being Not Applicable (NA)

IoT products do not have a VPN gateway function. (The fact that IoT products do not have a VPN gateway function shall be described in the "Reasons for being Not Applicable (NA).")

Supplementary explanation of the requirement

[Term: VPN gateway function]
A function that is placed at the boundary between an internal network and an external network such as the Internet to create an encrypted communication path between users.

Security Requirement Number: S3.1-08

STAR-3 Security Requirements

IoT devices shall implement a function to identify connecting devices and to reject the connection of unauthorized devices.

Conditions for being Not Applicable (NA)

IoT devices do not have L2/L3 switching functions. (The fact that IoT devices do not have L2/L3 switching function shall be described in the "Reasons for being Not Applicable (NA).")

Category 2: Implementing means to manage vulnerability reporting

Security Requirement Number: S3.1-09

STAR-3 Security Requirements

The manufacturer shall publish (e.g., post on the manufacturer's website) a vulnerability disclosure policy that includes the information listed in items (1) through (3) below, and shall have the process described in (4) below.

(1) Contact information for reporting to the manufacturer regarding security issues of IoT products (e.g., URL, phone number, and email address of the manufacturer's or other entity's website)
(2) Procedures to be taken by the manufacturer after receiving a report on the security of IoT products (e.g., how the report on security will be accepted, what procedures and methods will be used to communicate with the reporter afterwards, how the manufacturer will respond to the report, declaration of legal disclaimer for good faith reports, etc.), and outline of the process

(3) Procedures for updating the status of IoT products and vulnerabilities until the vulnerability is resolved (e.g., how investigations and countermeasures will be conducted until the vulnerability is resolved, how the status will be managed and announced, and what actions will be taken in response to reporters) and an outline of these procedures

(4) Declaration that the vulnerability will be reported in a timely manner to the appropriate reporting organization.

Conditions for being Not Applicable (NA)

Not applicable

Category 3: Keeping software up-to-dated

Security Requirement Number: S3.1-10

STAR-3 Security Requirements

All of the following requirements (1) through (4) shall be satisfied for the update function of firmware (software) packages included in IoT products.

(1) It shall be possible to update the firmware (software) package of IoT products.

(2) The firmware (software) package shall have a means to confirm that the latest firmware (software) is installed, such as being able to check the version of the firmware (software) package.

(3) The version of the firmware (software) package that has been updated shall be maintained even after the power is turned off.

(4) If online updates are available, the device shall have an automatic update function.

Conditions for being Not Applicable (NA)

Response to vulnerabilities shall be implemented using alternative measures other than updates. (The rationales for being able to address vulnerabilities without updates shall be described in the "Reasons for being Not Applicable (NA).")

Security Requirement Number: S3.1-11

STAR-3 Security Requirements

It shall be possible to perform software updates in an easy and understandable procedure when users apply updates.

Conditions for being Not Applicable (NA)

Response to vulnerabilities shall be implemented using alternative measures other than updates by users. (The rationales for being able to address vulnerabilities without updates by users shall be described in the "Reasons for being Not Applicable (NA).")

Supplementary explanation of the requirement

[Term: user]

The scope of users shall include all natural persons and organizations that use the IoT products which have access to the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-12

STAR-3 Security Requirements

When updating software, a function that satisfies all of the following (1) through (3) shall be implemented.

(1) IoT products shall have a mechanism to confirm the integrity and authenticity of the software prior to an update.

(2) If authenticity or integrity is not satisfied, the update shall be suspended.

(3) Anti-rollback function shall be provided.

Conditions for being Not Applicable (NA)

Response to vulnerabilities shall be implemented using alternative measures other than updates by users. (The rationales for being able to address vulnerabilities without updates by users shall be described in the "Reasons for being Not Applicable (NA).")

Security Requirement Number: S3.1-13

STAR-3 Security Requirements

The manufacturer shall document policies and guidelines for determining priorities of security updates for the purpose of promptly updating security issues.

Conditions for being Not Applicable (NA)

Not applicable

Security Requirement Number: S3.1-14

STAR-3 Security Requirements

Model numbers for IoT products shall be provided to users in one of the following ways.

(1) The model number and serial number of the IoT product shall be described directly on the IoT product itself.

(2) The model number and serial number shall be recognizable by users from the GUI or web UI, etc., of the IoT products, and from the GUI or web UI, etc., of the software or applications (smartphone applications, etc.) accompanying the IoT products.

Conditions for being Not Applicable (NA)

Not applicable

Supplementary explanation of the requirement

[Term: user]

The scope of users shall include all natural persons and organizations that use the IoT products which have access to the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-15

STAR-3 Security Requirements

A uniquely identifiable software bill of materials (SBOM) that includes third-party components used in IoT products shall be created and operated. Specifically, all of the following requirements (1) through (4) shall be satisfied.

(1) For the management of known vulnerabilities in the operation phase after product shipment, the SBOM for software that is a component of the product (including third-party components) shall be created and updated during the support period.

(2) During the support period, the SBOM shall be periodically checked for vulnerabilities based on the information in the SBOM, and a process shall be implemented to determine the priority of the vulnerabilities to be addressed before updating the SBOM or implementing operational countermeasures.

(3) During the support period, there shall be a process to manage the licenses of the components used based on SBOM information.

(4) It shall be ensured that software cannot be installed by means other than official updates after the product is shipped, or a mechanism shall be implemented that allows only authorized software to be installed.

Conditions for being Not Applicable (NA)

Not applicable

Category 4: Secure storage

Security Requirement Number: S3.1-16

STAR-3 Security Requirements

Securely stored information that is stored in the storage of IoT products (including securely stored information that is stored on storage media such as SD cards) shall be securely stored.

Conditions for being Not Applicable (NA)

Not applicable

Supplementary explanation of the requirement

[Term: securely stored information]

The following information. Refer to Section 3.2.

- CSP (Critical Security Parameter)
- PSP (Public Security Parameter)
- Configuration information on communication functions
- Configuration information on security functions
- Program code
- Logs (telemetry data, audit logs)

Security Requirement Number: S3.1-17

STAR-3 Security Requirements

CSPs (Critical Security Parameters) used in IoT products shall not be hard-coded into IoT devices. Furthermore, all of the following requirements (1) and (2) shall be satisfied to prevent tampering with PSPs (Public Security Parameters) hard-coded into IoT devices (such as device-specific identifiers or authentication codes used to verify identities).

(1) The full scope of the PSPs (Public Security Parameters) hard-coded into IoT devices shall be understood and listed.

(2) All PSPs (Public Security Parameters) listed in (1) shall be implemented in such a way that they are resistant to tampering by physical, electrical, or software means.

Conditions for being Not Applicable (NA)

There is no hard-coded CSP (Critical Security Parameter) or PSP (Public Security Parameter). (It shall be clearly stated in the "Reasons for being Not Applicable (NA)" that there is no hard-coded CSP (Critical Security Parameter) or PSP (Public Security Parameter).)

Supplementary explanation of the requirement

[Term: CSP (Critical Security Parameter)]

[Term: PSP (Public Security Parameter)]

Refer to Section 3.2.

Security Requirement Number: S3.1-18

STAR-3 Security Requirements

In order to confirm that CSPs (Critical Security Parameters) are not included in the SSPs (Sensitive Security Parameters) directly described in the source code, all of the following requirements (1) and (2) shall be satisfied.

(1) All SSPs (Sensitive Security Parameters) directly described in the source code shall be known and listed.

(2) Among SSPs (Sensitive Security Parameters), CSPs (Critical Security Parameters) that are used during the operation of IoT products shall not be included in the list in (1).

Conditions for being Not Applicable (NA)

There is no SSP (Sensitive Security Parameter) in the source code. (It shall be clearly stated in the "Reasons for being Not Applicable (NA)" that there is no hard-coded SSP (Sensitive Security Parameter) in the source code.)

Supplementary explanation of the requirement

[Term: CSP (Critical Security Parameter)]

[Term: PSP (Public Security Parameter)]

Refer to Section 3.2.

[SSP (Sensitive Security Parameter)]

Information assets comprising both CSP and PSP.

Security Requirement Number: S3.1-19

STAR-3 Security Requirements

Among the CSPs (Critical Security Parameters) used by IoT products, the CSPs (Critical Security Parameters) used to check the integrity and authenticity of software updates and to protect communications with associated services shall be unique to each IoT device.

Conditions for being Not Applicable (NA)

If the CSP is not used to check the integrity and authenticity of software updates or to secure communication with associated services. (It shall be stated in the "Reasons for being Not Applicable (NA)" that the CSP is not used to check the integrity and authenticity of software updates or to secure communication with associated services.)

Supplementary explanation of the requirement

[Term: CSP (Critical Security Parameter)]

Refer to Section 3.2.

Category 5: Secure communication

Security Requirement Number: S3.1-20

STAR-3 Security Requirements

All of the protection measures listed in the following (1) and (2) shall be taken for sensitive communication information transmitted over the network.

(1) IoT products shall confirm the legitimacy of the destination of the sensitive communication information.

(2) For sensitive communication information, IoT products themselves shall take protection measures against eavesdropping and tampering of information.

Conditions for being Not Applicable (NA)

There is no sensitive communication information transmitted over the network. (It shall be stated in the "Reasons for being Not Applicable (NA)" that there is no sensitive communication information transmitted over the network.)

Supplementary explanation of the requirement

[Term: sensitive communication information]

The following information. Refer to Section 3.2.

- CSP (Critical Security Parameter)

- Configuration information related to communication functions
- Configuration information related to security functions
- Alert information
- Audit logs

Security Requirement Number: S3.1-21

STAR-3 Security Requirements

Secure management processes shall be implemented for each life cycle of generating, distributing, storing, and updating CSPs (Critical Security Parameters) used in IoT products.

Conditions for being Not Applicable (NA)

Not applicable

Supplementary explanation of the requirement

[Term: CSP (Critical Security Parameter)]

Refer to Section 3.2.

Security Requirement Number: S3.1-22

STAR-3 Security Requirements

IoT products with wireless LAN function shall implement a function to encrypt communications using an appropriate method and device authentication using IEEE802.1X in the wireless communication section.

Conditions for being Not Applicable (NA)

IoT products do not have wireless LAN functions. (It shall be stated in the "Reasons for being Not Applicable (NA)" that IoT products do not have wireless LAN functions.)

Category 6: Minimizing exposed attack surfaces

Security Requirement Number: S3.1-23

STAR-3 Security Requirements

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 for

IoT products shall be performed. Specifically, all of the following requirements (1) and (2) shall be satisfied.

(1) For the following interfaces that are used frequently in IoT products and are assumed to be at risk of vulnerability, etc., those interfaces that are unnecessary for the use of IoT products and at risk of being attacked shall be disabled.

A) TCP/UDP ports

B) Bluetooth

C) USB

(2) Known vulnerabilities shall be checked by vulnerability scanning tools for IoT products to ensure that no vulnerabilities that could be exploited by attacks are detected.

Conditions for being Not Applicable (NA)

Not applicable

Security Requirement Number: S3.1-24

STAR-3 Security Requirements

In the initialized state, security-related information that can be viewed without authentication from network interfaces enabled on IoT products shall be minimized, including

A) Configuration information of device

B) Kernel version

C) Software version

Conditions for being Not Applicable (NA)

Not applicable

Security Requirement Number: S3.1-25

STAR-3 Security Requirements

IoT devices shall have all of the following protection measures (1) and (2) against physical attacks.

(1) Unnecessary physical interfaces of IoT devices shall have a mechanism to protect them from exposure.

(2) Debugging interfaces of IoT devices shall be physically or logically disabled.

Conditions for being Not Applicable (NA)

Not applicable

Security Requirement Number: S3.1-26

STAR-3 Security Requirements

In designing and implementing IoT products, manufacturers shall enable only those services that are used or required for the intended use or operation of the devices.

Conditions for being Not Applicable (NA)

Not applicable

Security Requirement Number: S3.1-27

STAR-3 Security Requirements

Manufacturers shall employ code minimization practices in implementing and testing software deployed in IoT products.

Conditions for being Not Applicable (NA)

Not applicable

Security Requirement Number: S3.1-28

STAR-3 Security Requirements

Manufacturers shall design and implement software deployed in IoT products based on the principle of least privilege. Specifically, all of the following requirements shall be satisfied.

(1) Minimization of default privileges

Default privilege settings shall be kept to the minimum necessary to ensure that unnecessary broad privileges are not granted.

Conditions for being Not Applicable (NA)

Not applicable

Supplementary explanation of the requirement

[Term: user]

The scope of users shall include all natural persons and organizations that use the IoT products which have access to the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-29

STAR-3 Security Requirements

During the implementation and testing phases of the product, secure coding practices shall be implemented and reviewed against the source code created. Specifically, at a minimum, the following practices shall be included.

(1) Security-conscious coding conventions and implementation principles shall be prescribed.

(2) Coding conventions shall be notified to engineers and training shall be provided.

(3) The codes created shall be reviewed and security testing shall be conducted.

(4) Coding conventions and implementation principles shall be updated.

Conditions for being Not Applicable (NA)

Not applicable

Security Requirement Number: S3.1-30

STAR-3 Security Requirements

When incorporating third-party components into IoT products, a process that satisfies all of the following requirements (1) and (2) shall be adopted to ensure that known vulnerabilities are not included.

(1) Vulnerabilities shall be managed with respect to third-party components that are clearly used.

(2) When vulnerabilities are detected, appropriate action shall be taken.

Conditions for being Not Applicable (NA)

Third-party components are not used in the target IoT products. (It shall be clearly stated in the "Reasons for being Not Applicable (NA)" that no third-party components are used.)

Category 7: Ensuring software integrity

Security Requirement Number: S3.1-31

STAR-3 Security Requirements

Secure boot mechanisms shall be implemented for IoT products to verify the integrity of software loaded during the system startup process.

Examples of secure boot mechanisms include the following. An implementation similar to any of these

shall be conducted.

A) Verification of digital signatures

B) Security measures equivalent to digital signature verification

Conditions for being Not Applicable (NA)

Not applicable

Category 8: Ensuring that personal data is secure

Security Requirement Number: S3.1-32

STAR-3 Security Requirements

Manufacturers shall take measures to meet the following requirements when IoT devices perform sensing

(1) For information to be sensed, the purpose of collection and the overview of functions shall be described in the user manuals, etc., which can be easily understood.

Conditions for being Not Applicable (NA)

In case the IoT device does not have a sensing function. (It shall be stated in the "Reasons for being Not Applicable (NA)" that there is no sensing function.)

Category 9: Making the system resilient to outages

Security Requirement Number: S3.1-33

STAR-3 Security Requirements

When the power supply and network function are turned off and restored due to a power outage or other reasons, 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 factory default settings.

Conditions for being Not Applicable (NA)

Not applicable

Security Requirement Number: S3.1-34

STAR-3 Security Requirements

IoT products shall implement a backup function that can correctly retain and restore configuration information at specific times.

Conditions for being Not Applicable (NA)

Not applicable

Category 10: Verifying and protecting system telemetry data

Security Requirement Number: S3.1-35

STAR-3 Security Requirements

In order to detect security anomalies, IoT products shall implement the ability to record logs (telemetry data and audit logs). Specifically, all of the following requirements (1) through (3) shall be satisfied.

(1) Functions of acquiring and storing logs (telemetry data and audit logs) shall be implemented for IoT products. At a minimum, logs (telemetry data and audit logs) generated by firmware (software) or OS shall be acquired and stored. The target of security events to be recorded includes records of disconnections (reconnections) of devices and networks, records of login attempts (successful and unsuccessful attempts), records of login attempts that exceed threshold values, records of time changes (including time before and after the change), and records of the use of management functions, including acquisition and restoration of backups, records of software changes, records of hardware changes (when audit logs can be acquired), firewall operation status records (when firewall function is implemented), and remote management service operation status records (when CWMP, etc., is enabled).

(2) Logs (telemetry data and audit logs) shall have the necessary capacity for auditing, and if the storage capacity is exceeded, administrative measures shall be taken, such as sequentially overwriting older records. Note that the required storage capacity shall be separately reviewed based on the intended use of each product.

(3) The time management function shall be provided to record the date and time of security events on logs (telemetry data and audit logs).

Conditions for being Not Applicable (NA)

Not applicable

Supplementary explanation of the requirement

[Term: telemetry data]

It refers to data from devices which can provide information that can help manufacturers identify problems or information regarding the use of products.

[Term: audit log]
It refers to data that records product processes and operations in a chronological and continuous manner in order to enable users to detect security anomalies in products.

Category 11: Allowing users to easily erase data

Security Requirement Number: S3.1-36

STAR-3 Security Requirements

All of the following requirements (1) and (2) shall be satisfied for the deletion function of data stored in the storage of IoT products during the use of IoT products.

(1) It shall be possible to delete at least the following data related to users via the IoT device itself or associated services (e.g., mobile applications) by users.
   A) Information assets (including personal information) acquired while using IoT products
   B) User configuration values
   C) Authentication values set by users, encryption keys and digital signatures acquired while using IoT products

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

Conditions for being Not Applicable (NA)

Not applicable

Supplementary explanation of the requirement

[Term: user]
The scope of users shall include all natural persons and organizations that use the IoT products which have access to the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Category 12: Facilitating product installation and maintenance

Security Requirement Number: S3.1-37

STAR-3 Security Requirements

IoT devices shall be able to restore secure default configuration settings.

Conditions for being Not Applicable (NA)

Not applicable

Category 13: Checking the validity of input data

Security Requirement Number: S3.1-38

STAR-3 Security Requirements

For all interfaces of the IoT product, a function to verify the validity of input data and to reject requests if the input data is invalid and unauthorized shall be implemented.

Conditions for being Not Applicable (NA)

Not applicable

Category 14: Processing personal data appropriately

Security Requirement Number: S3.1-39

STAR-3 Security Requirements

Manufacturers shall explain what personal data is collected and how it is processed if personal data obtained from IoT products is processed, and what functions are implemented to process it.

Conditions for being Not Applicable (NA)

In case IoT products do not have a function to collect or process personal information. (It shall be stated in the "Reasons for being Not Applicable (NA)" that IoT products do not have a function to collect or process personal information.)

Security Requirement Number: S3.1-40

STAR-3 Security Requirements

When IoT products collect logs (telemetry data, audit logs) and contain personal information (including information related to individuals), the collected personal information shall be limited to the minimum necessary to achieve the purpose of audits.

Conditions for being Not Applicable (NA)

In case the logs do not contain personal information. (It shall be stated in the "Reasons for being Not Applicable (NA)" that logs do not contain personal information.)

Security Requirement Number: S3.1-41

STAR-3 Security Requirements

Manufacturers shall disclose to users what logs (telemetry data/audit logs) IoT products record and for what purposes.

Conditions for being Not Applicable (NA)

In case IoT products do not have a function to collect or process personal information. (It shall be stated in the "Reasons for being Not Applicable (NA)" that IoT products do not have a function to collect or process personal information.)

Category 16: Identifying and testing threats

Security Requirement Number: S3.1-42

STAR-3 Security Requirements

The manufacturer shall resolve any security issues detected as a result of third-party penetration testing.

Conditions for being Not Applicable (NA)

Not applicable

Category 17: Providing information on products

Security Requirement Number: S3.1-43

STAR-3 Security Requirements

Product security information provided to users shall be in the specified language.

Conditions for being Not Applicable (NA)

Not applicable

Supplementary explanation of the requirement

[Term: user]

The scope of users shall include all natural persons and organizations that use the IoT products which have access to the IoT products, such as users, administrators, manufacturers' customer engineers, and owners of the IoT products.

Security Requirement Number: S3.1-44

STAR-3 Security Requirements

Manufacturers shall take measures that satisfy all of the following requirements (1) through (5) in regard to providing information on the security of IoT products.

(1) The procedures for secure use of IoT products, such as initial setup methods, and other settings and usage methods that may affect cybersecurity in the use of IoT products, shall be made known.

(2) A system shall be implemented to inform the public of the contents and necessity of security updates for IoT products when such updates are released, as well as the consequences of not updating.

(3) Disclaimers of liability shall be made known for accidents and failures assumed or generally expected when updates are not performed.

(4) The policy for the support expiration date or termination of support for the target product or service shall be made known to the public.

(5) To make known the risks assumed when disposing of or selling used IoT products with securely stored information remaining in the IoT products, and the secure termination method of using IoT products including data erasure.

Conditions for being Not Applicable (NA)

Not applicable

Supplementary explanation of the requirement

[Term: securely stored information]

The following information. Refer to Section 3.2.

- CSP (Critical Security Parameter)
- PSP (Public Security Parameter)
- Configuration information on communication functions
- Configuration information on security functions
- Program code

- Logs (telemetry data, audit logs)

Category 19: Ensuring product availability

Security Requirement Number: S3.1-45

STAR-3 Security Requirements

IoT devices shall have a mechanism to recover from a network overload state caused by a denial-of-service attack.

Conditions for being Not Applicable (NA)

Not applicable

Category 21: Ensuring hardware integrity

Security Requirement Number: S3.1-46

STAR-3 Security Requirements

To prevent unauthorized access to components and interfaces in devices through physical destruction or modification of the enclosure, a mechanism to improve the tamper resistance of the enclosure shall be implemented.

Conditions for being Not Applicable (NA)

Not applicable

Appendix A: Glossary

Terms	Definition
administrator	A user who has the highest-privilege level possible for a user of the device, which can mean they are able to change any configuration related to the intended functionality
associated services	Digital services that, together with the device, are part of the overall IoT product and that are typically required to provide the product's intended functionality Example 1: Associated services can include mobile applications, cloud computing/storage and third party Application Programming Interfaces (APIs). Example 2: A device transmits telemetry data to a third-party service chosen by the device manufacturer. This service is an associated service.
audit log	Data that chronologically and continuously records the product's processing contents, processes, and operation history to enable users to detect security anomalies within the product
authentication mechanism	A method used to prove the authenticity of an entity Note: An "entity" can be either a user or machine. Example: An authentication mechanism includes to request a password, to scan a QR code, or to use a biometric fingerprint scanner.
authentication value	An individual value of an attribute used by an authentication mechanism Example: When the authentication mechanism is to request a password, the authentication value can be a character string. When the authentication mechanism is a biometric fingerprint recognition, the authentication value can be the index fingerprint of the left hand.
best practice cryptography	Cryptography that is suitable for the corresponding use case and has no indications of a feasible attack with current readily available techniques Note 1: This does not refer only to the cryptographic primitives used, but also implementation, key generation and handling of keys. Note 2: Multiple organizations, such as SDOs and public authorities, maintain guides and catalogues of cryptographic methods that can be used. Example: The device manufacturer uses a communication protocol and cryptographic library provided with the IoT platform and where that library and protocol have been assessed against feasible attacks, such as replay.

configuration settings	A set of parameters that can be changed in hardware, software, or firmware that affect the security posture and function of an information system
constrained device	A device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use Note 1: Physical limitations can be due to power supply, battery life, processing power, physical access, limited functionality, limited memory or limited network bandwidth. These limitations can require a constrained device to be supported by another device, such as a base station or companion device. Example 1: A window sensor's battery cannot be charged or changed by the user; this is a constrained device. Example 2: The device cannot have its software updated due to storage limitations, resulting in hardware replacement or network isolation being the only options to manage a security vulnerability. Example 3: A low-powered device uses a battery to enable it to be deployed in a range of locations. Performing high power cryptographic operations would quickly reduce the battery life, so it relies on a base station or hub to perform validations on updates. Example 4: The device has no display screen to validate binding codes for Bluetooth pairing. Example 5: The device has no ability to input, such as via a keyboard, authentication information. Note 2: A device that has a wired power supply and can support IP-based protocols and the cryptographic primitives used by those protocols is not constrained. Example 6: A device that is powered via an electrical outlet and communicates primarily using TLS (Transport Layer Security).
consumer	A natural person who is acting for purposes that are outside her/his trade, business, craft or profession Note: Organizations, including businesses of any size, use consumer IoT. For example, Smart TVs are frequently deployed in meeting rooms, and home security kits can protect the premises of small businesses.
CSP (Critical Security Parameter)	Security-related secret information whose disclosure or modification can compromise the security of a security module

	Example: Secret cryptographic keys, authentication values such as passwords, PINs, private components of certificates.
debug interface	A physical interface used by the manufacturer to communicate with the device during development or to perform triage of issues with the device and that is not used as part of the consumer-facing functions Example: Test points, UART, SWD, JTAG.
defined support period	A minimum length of time, expressed as a period or by an end-date, for which a manufacturer will provide security updates Note: This definition focuses on security aspects and not other aspects related to product support such as assurance.
external sensing function	An element or device that collects information on an object and converts it into signals that can be handled by a machine Example: Optical sensors, acoustic sensors, cameras, microphones
factory default	A state of the device after factory reset or after final production/assembly Note: This includes the physical device and software (including firmware) that is present on it after assembly.
hard-coded unique per device identity	A value unique to each device written directly in the source code Example: A master key (private key) used for network access that is unique to the device
initialization	A process that activates the network connectivity of the device for operation and optionally sets authentication function for users or for network access
initialized state	A state of the device after initialization
IoT device / device	Network-connected (and network-connectable) device that has relationships to associated services Note 1: IoT devices are commonly also used in business contexts. Note 2: IoT devices can also be commissioned and/or installed professionally.
IoT product / product	IoT device and its associated services
isolable	It is possible to be removed from the network it is connected to, where any loss of function caused is related only to that connectivity and not to its main function; alternatively, it is possible to be placed in a self-contained environment with other devices if and only if the integrity of devices within that environment can be ensured. Example: A Smart Refrigerator has a touchscreen-based interface that is

	network-connected. This interface can be removed without stopping the refrigerator from keeping the contents chilled.
logical interface	Software implementation that utilizes a network interface and communicates over the network via channels or ports
manufacturer	A relevant parties within the supply chain (including the device manufacturer) Note: This definition acknowledges the variety of actors involved in the IoT ecosystem and the complex ways by which they can share responsibilities. Beyond the device manufacturer, such entities can also be, for example and depending on a specific case at hand: importers, distributors, integrators, component and platform providers, software providers, IT and telecommunications service providers, managed service providers and providers of associated services. Note 2: This definition corresponds to the term "IoT product vendor" as used in the "IoT Product Security Conformity Assessment Scheme Policy."
network interface	A physical interface that can be used to access the IoT functions via a network
network overload status	A state where the network is overloaded, preventing network devices from functioning properly
owner	A user who owns or who purchased the device
personal data	Any information relating to an identified or identifiable natural person Note: This term is used to align with well-known terminology but has no legal meaning within this document.
physical interface	A physical port or air interface (such as radio, audio or optical) used to communicate with the device at the physical layer Example: Radios, ethernet ports, serial interfaces such as USB, and those used for debugging
PSP (Public Security Parameter)	Publicly available security-related information that, if tampered with, could compromise the security of a security module. Example 1: A public key used to verify the authenticity / integrity of software updates. Example 2: The public elements of a certificate.
remotely accessible	It is intended to be accessible from outside the local network
security module	A set of hardware, software, and/or firmware that implements security functions Example: A device contains a hardware root of trust, a cryptographic

	software library that operates within a trusted execution environment, and software within the operating system that enforces security such as user separation and the update mechanism. These all make up the security module.
security update	Software update that addresses security vulnerabilities either discovered by the manufacturer or reported to the manufacturer Note: Software updates can be purely security updates if the severity of the vulnerability requires a higher priority fix.
self-contained environment	An environment that can be used independently without depending on other services
sensitive personal data	Data whose disclosure has a high potential to cause harm to the individual What is to be treated as "sensitive personal data" varies across products and use cases, but examples include video stream of a home security camera, payment information, contents of communication data, and timestamped location data.
software service	Software component of a device that is used to support functions Example: A runtime for the programming language used within the device software, or a daemon that exposes an API used by the device software, such as a cryptographic module's API.
SSP (Sensitive Security Parameter)	Information assets comprising both CSP and PSP
storage	A medium capable of storing data or information and retrieving it.
technical documents	A document that sets forth the technical specifications referenced in the Evaluation/Assessment Procedures and serves as the rationale for demonstrating Conformance Requirements; it includes documents such as product design documents, specifications, development procedures, manuals, etc., documents prescribed based on these documents. Regardless of whether they are disclosed or non-disclosed, the applicant may select such documents at their own discretion. In addition, technical specifications may be provided in formats used by other standards or in free-form formats.
telemetry	Data from devices that can provide information to help manufacturers identify issues or gather information related to the use of the devices. Example: IoT devices report software bugs to manufacturers, enabling them to identify the cause and fix the issue
telemetry data	Data from devices that can provide information to help manufacturers identify issues or gather information related to the use of the products

unique per device	Unique per device within a given product class or type
user	A natural person or an organization
VPN gateway function	A function placed at the boundary between internal networks and external networks such as the Internet, creating an encrypted communication path with users
zone	Each entity resulting from the division of the target system based on functional, logical, and physical (including location) relationships
zone boundary	The boundary between zones

Appendix B: References Links

Existing Schemes and Documents	Link
ETSI EN 303 645 V3.1.3 (2024-09)	https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
Cybersecurity Labelling Scheme (CLS) Publication No. 4 Version 1.2 April 2025	https://isomer-user-content.by.gov.sg/36/03b1d128-7284-40ac-bb1f-fdc94b5842a3/CCC%20SP-151-4%20CLS(IoT)%20Assessment%20Methodology %20v1.2.pdf
Cyber Resilience Act (CRA)23 October 2024	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847
Radio Equipment Directive (RED):28.12.2024	https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-_RED_EN
18031-1 / -2 / -3: 2024	EN 18031-1: https://www.en-standard.eu/bs-en-18031-1-2024-common-security-requirements-for-radio-equipment-internet-connected-radio-equipment/ EN 18031-2: https://www.en-standard.eu/bs-en-18031-2-2024-common-security-requirements-for-radio-equipment-radio-equipment-processing-data- namely-internet-connected-radio-equipment-childcare-radio-equipment-toys-radio-equipment-and-wearable-radio-equipment/ EN 18031-3: https://www.en-standard.eu/bs-en-18031-3-2024-common-security-requirements-for-radio-equipment-internet-connected-radio-equipment- processing-virtual-money-or-monetary-value/
IEC 62443-4-1 2018	https://webstore.iec.ch/en/publication/33615
IEC 62443-4-2 2019	https://webstore.iec.ch/en/publication/34421
NIST IR 8425 September 2022	https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf
UK PSTI Act Regulation 2023	https://www.legislation.gov.uk/uksi/2023/1007/schedule/1/made

Partial Revision of Guidelines for the Establishment of Standards for Measures by Government Agencies (September 2025)	https://www.cyber.go.jp/pdf/policy/general/guider7_9.pdf
CCDS Guidelines for Conformance Requirements for Security of IoT devices 2025 Ver. 1.0	https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2025_v1.0_jpn.pdf
RBSS Security Camera Certification Criteria 2024.04.01	https://www.ipa.go.jp/security/jisec/pps/certified-pps/c0755_it2805.html
Specific Purpose Devices Common Security Protection Profile, Version 1.0	https://bmsec.jbmia.or.jp/file/guide.pdf
MIC: Ordinance Concerning Terminal Facilities, etc., effective October 1, 2025	https://laws.e-gov.go.jp/law/360M50001000031

Appendix C: Revision History

June 10, 2026: SR Version 1.0 (JST-SR-03-01-2026) Published

- The document number has been changed from "CR" (Certification Requirement) to "SR" (Security Requirement). Consequently, "JST-CR-03-01-2026/2026R1" has been discontinued as a security requirement.
- Based on deliberations regarding conformance requirements by the Technical Advisory Committee, some partial revisions were made, primarily to the wording of the security requirements. Refer to the comparison table for details on the revisions.

February 12, 2026: CR Version 1.1 (JST-CR-03-01-2026R1) Published

- Appendix B: Corrected the reference link for "EN 18031-1 / -2 / -3: 2024."

February 6, 2026: CR Version 1.0 (JST-CR-03-01-2026) Published