IoT Devices Security Requirements 2023: Conformity Criteria Guidelines CCDS-GRC01-2023 Ver. 1.0

General Incorporated Association
Connected Consumer Device Security Council

December 28, 2022

Update History

Revision	Date of Update	Description of Update	Formulated by
Rev. 1.0	Dec. 28, 2022	Ver. 1.0 release	CCDS

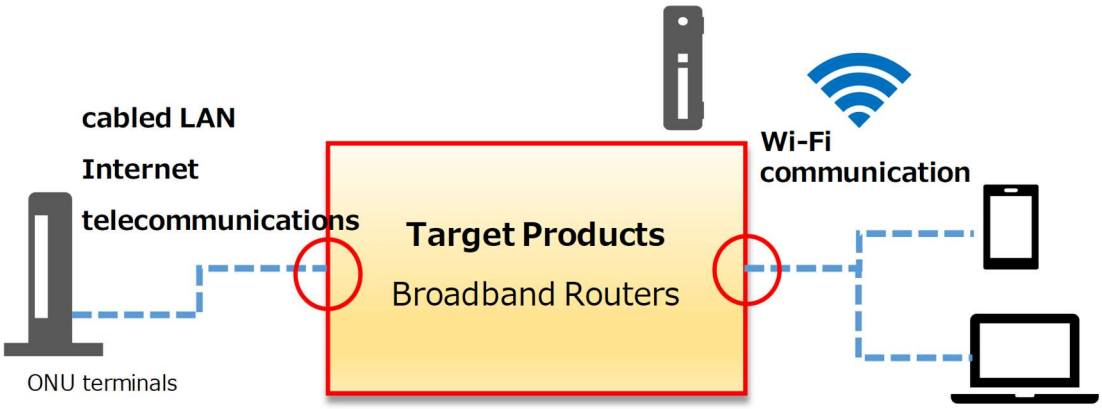
Table of Contents

1. Purpose of This Document

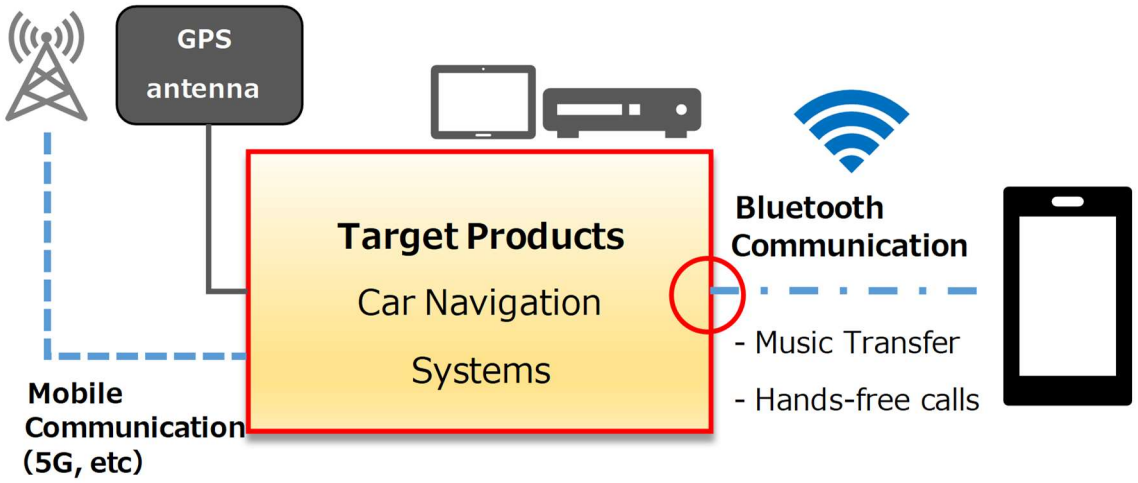
Based on the security requirements shown in the "CCDS IoT Device Security Requirements_2023 Edition," these guidelines define specific security functional requirements to be followed, and the contents to be inspected against the functional requirements, inspection methods and the Conformity criteria.

2. Scope of Granting of the CCDS Certification Mark

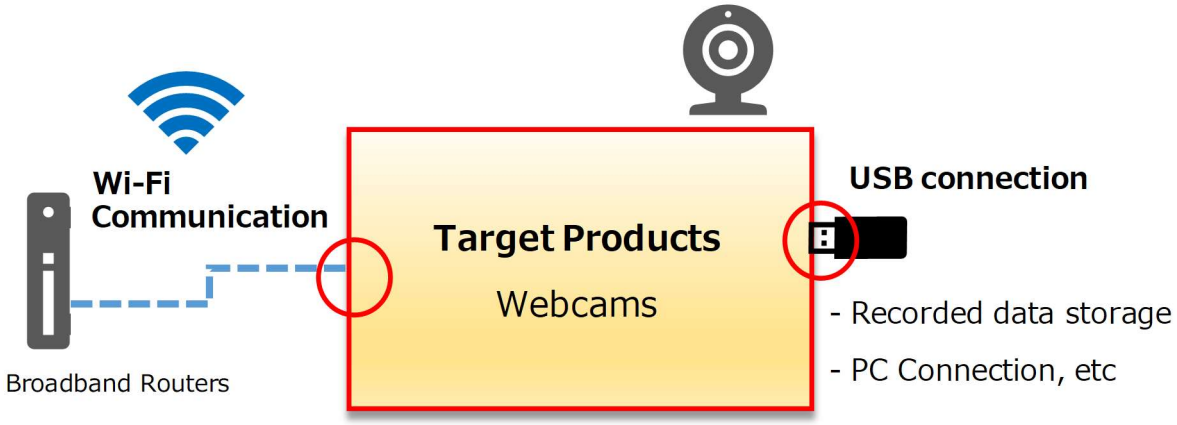
The scope of granting of the CCDS Certification Mark encompasses those devices and systems with Internet Protocol-ready hardware and software interfaces. It also covers devices and systems with Wi-Fi, Bluetooth, and/or USB interfaces (see Figures 1 to 3 below), because relatively more vulnerabilities and attacks related to these interfaces are observed among IoT devices.



[Figure1] Example 1 of certification-eligible products that implement a subject interface: Broadband Routers



[Figure2] Example 2 certification-eligible of products that implement a subject interface: Car Navigation Systems



[Figure 3] Example 3 of certification-eligible products subject implement a subject interface: Webcams

3. Conformity Criteria for the CCDS Certification Mark

In granting the CCDS certification mark, it is premised that a risk assessment has been performed on the target of verification, and Conformity with the security requirements described in Chapter 7 is required (excluding requirements for non-implemented functions).

For Conformity criteria, be sure to refer to the latest guidelines presented by CCDS at the time of application and verify the target of verification and related documents according to the guidelines.

Regardless of the conformity with the requirements of this document, the device subject to the Telecommunications Business Law is required to acquire Technical Regulations Conformity.

4. Documents and materials to be submitted to the designated verification operator

The applicant submits the documents described below to the designated verification operator as evidence of Conformity with each security requirement and inspection results. There is no need to submit the design documents of the target of verification. Each applicant is required to keep them for possible investigation after obtaining the certification.

4.1. Designated documents required to be submitted for document verification

4.1.1 Documents showing the environment configuration and requirements of the system

The applicant submits a system configuration diagram of the environment in which the target of verification is actually operated.

In the configuration diagram, specify the communication standards to be implemented and the communication protocols to be used for communication paths with other devices. The applicant ensures that the target of verification will be used in accordance with the submitted system environment configuration and specifications.

4.1.2 Verification questionnaire on the implementation specifications of the target of verification

In order to prove that the target of verification meets each security requirement under the conformity criteria, the applicant fills out and submit the attached ”Form 1) CCDS-GR01-2023_Conformity verification questionnaire (hereinafter referred to as the verification questionnaire).”

Refer to “Form 1) CCDS-GR01-2023_Compliant verification questionnaire.”

[Table 1] List of content to be filled in the verification questionnaire

requirements	Description
1-1	Implemented authentication and access restrictions
1-1-1	- Open port numbers - Usage of each port - Timing/conditions for the ports to be opened
1-1-2	Policy on changing credentials
1-2	Data protection policy
1-2-1	Policy on functionality to delete information configured and acquired
1-3	Policies on the implementation of software updates
1-4-1	Policy on the Wi-Fi implementation and authentication protocols
1-4-2	Policy on the Bluetooth implementation, authentication protocols, and profiles About OS and software versions
1-4-3	Policies on the USB implementation and device classes used

1-4-4～1-4-6	Policies on the implementation of web features
2-1	Implementation of a contact regarding product vulnerabilities Implementation of the security support system
2-2	Policy on managing documents related to products
2-3	Policy on provision of information to users
3-1	Implementation policy on recording and storing of audit log
3-1-1	Implementation policy on time management functionality

4.2 Designated materials required to be submitted for actual machine inspection

4.2.1 Videos and/or still images when checking the operation of the actual machine

Videos and/or still images (e.g., screenshots and photos) that can prove that the conformity criteria are met when checking the actual operation of the target of verification.

4.2.2 Output logs and reports as confirmation results using reference inspection tools

The vulnerability list , individual reports on detected vulnerabilities, output logs, etc., as a result of vulnerability scan with reference inspection tools.

4.2.3 Submission of the “Form 2) CCDS-GR-01-2023_Conformity Inspection Procedure/Result Table (hereinafter referred to as the inspection procedure/result table)” with inspection results of the target of verification fulfilled

Enter the results of the inspection against the security requirements in the inspection procedure/result table and submit it.

- Clearly indicate pass/fail for inspection results.
- Enter the date of the test, the version of the software and/or firmware at the time of the test, and the name of the person who performed the test.

Refer to “Form 2) CCDS-GR01-2023_Conformity Inspection Procedure/Result Table.”

5. Retention of submitted documents

Documents and materials designated to be submitted to the designated verification operator shall be retained by the applicant and the designated verification operator for three years as evidence of the CCDS certification mark.
If the applicant company has regulations to retain the evidence more than three years, the applicant should follow the company regulations instead.

6. Composition of the Conformity criteria

6.1 Security requirements to be met

The security requirements in this document are divided into “mandatory requirements” and “recommended requirements.”
“Mandatory requirements” are the requirements that must be met by IoT devices/services for general users, and “recommended requirements” are the requirements that are necessary for IoT devices/services that require a higher level of security.

6.2 Terminology in Conformity Criteria

Terms used in the Conformity criteria of this document are defined below.

[Table 2] Definitions of terms in the Conformity criteria

the term	explanation
privileged user	Indicates a user who is authorized to access functions that enable critical configuration changes, including security-related functions of the target of verification.
audit log	Indicates the chronological and continuous record of the transaction details and processes of the target of verification or system.

6.3 Composition and perspectives of Conformity criteria

Table 3 shows the IoT Device Security Requirements 2023 Edition (CCDS-GR01-2023) that this document covers. This document presents the Conformity criteria for the security requirements from the following points of view.

- A: Confirmation of documents for the implementation of the target of verification
- B: Confirmation of actual machine operation

[Table 3] CCDS IoT Device Security Requirements_2023 Edition (CCDS-GR01-2023) List

Classification	ID	Security Requirements (subset ID, security requirements)		Purpose of requirement
1. Functional requirements for IoT devices	1-1	**Access Control and Authentication**		Identification, access control, configuration change, privilege management, authentication
		1-1-1	Disabling of TCP/UDP ports	
		1-1-2	Change of credentials	
	1-2	**Data Protection**		Data protection, protection of credentials and key information
		1-2-1	Data erasure function	
	1-3	**Software Update**		Operational incident response
	1-4	**Requirements with a particularly large number of incidents and high impact**		
		1-4-1	Wi-Fi authentication method	
		1-4-2	Bluetooth vulnerability countermeasures	
		1-4-3	USB access control	
		1-4-4	Injection countermeasures	
2. Requirements for the operation of IoT devices	2-1	**Contact point and security support system**		Operational incident response
	2-2	**Product document management**		Documentation of security activities
	2-3	**Provision of information to users**		Operational support
3. Requirements for auditing IoT devices	3-1	**Audit log recording**		Operational incident response
		3-1-1	Time management function	

6.4 Satisfying Conformity standards by obtaining ISO certification

If you have acquired the following ISO certifications, you will be able to omit the security inspection as you will be deemed to have satisfied the Conformity criteria for the items in question.

[Table 4] Correspondence between the requirements, 2023 edition and ISO certification standards

*Items marked with a "C" are considered to satisfy the security requirements, and the inspection can be omitted.

Classification	ID	Security Requirements (subset ID, security requirements)		Applicable ISO certification standards		
				ISO9001	ISO27001[1]	ISO15408[2]
1. Functional requirements for IoT devices	1-1	**Access Control and Authentication**				
		1-1-1	Disabling of TCP/UDP ports			C
		1-1-2	Change of credentials			
	1-2	**Data Protection**				
		1-2-1	Data erasure function			
	1-3	**Software Update**				C
	1-4	**Requirements with a particularly large number of incidents and high impact**				
		1-4-1	Wi-Fi authentication method			
		1-4-2	Bluetooth vulnerability countermeasures			
		1-4-3	USB access control			
		1-4-4	Injection countermeasures			

[1] Currently, there are no applicable items for which inspections are omitted due to acquisition of ISO27000.
[2] For ISO15408 (Common Criteria), only if the certification conforming to the following common protection profile for specific purpose equipment is obtained. Be eligible. In addition, if the above is met, it is considered that the applicable requirements are satisfied up to the recommended requirements.
reference)JISEC Equipment for specific use common protection profile
https://www.ipa.go.jp/files/000079196.pdf

2. Requirements for the operation of IoT devices	**2-1**	**Contact point and security support system**		C[3]		
	2-2	**Product document management**		C[4]		
	2-3	**Provision of information to users**		C[5]		
3. Requirements for auditing IoT devices	**3-1**	**Audit log recording**				C
		3-1-1	Time management function			

[3] ISO9001:2015 Corresponds to “8.2.1 Communication with Customers”
[4] ISO9001:2015 Corresponds to “8.2.2 Clarification of requirements for products and services”
*However, only if the organization has documented security requirements for the product or service in question.
[5] ISO9001:2015 Corresponds to “8.2.1 Communication with Customers”
*However, this is limited to cases where the organization has established a policy of providing information on cybersecurity of the target product or service.

7. Conformity criteria for security requirements

Conformity criteria and inspection methods for each security requirement are shown below. Requirements and conformance criteria shall need to be met with AND conditions, except when being explicitly specified.

For implementation examples, you can choose one of them according to the implementation of the target of verification unless a condition, e.g., AND or OR, is explicitly specified.

7.1-1 Access control and authentication

Target security requirements			
Classification	ID	Security Requirements (subset ID, security requirements)	Purpose of requirement
1. Functional requirements for IoT devices	**1-1**	**Access Control and Authentication**	**Identification, access control, configuration change, privilege management, authentication**
Mandatory requirements	1) Have an ID that allows users (general users and privileged users) and other IoT devices to uniquely identify the target of verification. 2) Enforce appropriate authentication or access control for access from users and other IoT devices for TCP/UDP communication that is necessary for system operation. For authentication, the default password shall be unique to each device. 3) Take countermeasures against consecutive login attempts in user authentication, e.g., sending alert notifications to privileged users, equipment operators or maintenance personnel when login attempts exceed a certain number of times, or disabling the target account for a certain period of time. 4) Identify and authenticate users for functions that enable to change significant configurations, including device security-related functions to restrict anyone other than privileged users, device operator or maintenance personnel from executing the functions. 5) After network communication is broken, re-establish the connection with other devices in a secure state through the access control and/or authentication processes. **Remarks** Concerning the above item (2) "The default password shall be unique to each device," the implementation that requires for the user to change the password when starting up for the first time according to Section 7.1-1-2 (2) will meet the Conformity criteria.	
Recommended requirements	None		

7.1-1A	Conformity criteria
Inspection method	Conformity inspection of documentation
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) To have an ID that enables users (general users and privileged users) and/or other IoT devices to uniquely identify the target of verification. 2) To enforce authentication for every TCP/UDP communication. Or limit the communication destination by access control. 3) To take countermeasures against consecutive login attempts. 4) To have a mechanism to identify and authenticate users or privileged users for access to functions that perform significant configuration changes, including security-related functions of the target of verification. 5) To re-establish the connection with other devices in a secure state through the process of authentication and access control according to the specifications of 2) above, after network communication is broken. **Remarks** The authentication specified in 2) above can be excluded if the applicant cannot guarantee the settings necessary for the operation of the target of verification or the protocol does not support authentication. Example of exception protocol: - ARP and ICMP (because they are lower layer protocols than TCP/UDP) - DHCP, DNS and NTP (because they are protocols that do not support authentication) **Recommended requirements** Not applicable
Implementation example	**Implementation example 1)** **Authentication and access control (Mandatory requirement 2)** **[A) User authentication using user IDs and passwords] (AND condition)** ・ The default password is not set such a value that can be easily guessed, e.g., public information such as the MAC address, the Wi-Fi® SSID, the device serial number, the model number, the name (abbreviation), a proper noun, and a simple pattern string. ・ Passwords can be eight characters or more and can be a mixture of numeric letters, lowercase letters and uppercase letters.

	・ The default password is set to a value unique to each device, or the target of verifications has a mechanism that automatically generates passwords. ・ When implementing a mechanism that automatically generates passwords, it is specified that the generated values have no clear regularity and do not include values that are easy to guess. **Remarks** ・ If it is difficult to implement using a combination of alphanumeric characters including lowercase letters and uppercase letters, ensure the same entropy (randomness of values) with the password length. **[B) Device certification] (OR conditions)** ・ Support standard authentication methods, for example, using digital certificates. ・ Supports standard authentication methods such as OpenID Authentication* for Web API authentication. *Compliant with RFC 6749 "The OAuth 2.0 Authorization Framework" **[C) Multi-factor authentication]** ・ The target of verification supports multi-factor authentication using multiple authentication factors. **[D) Communication access control] *When implementing authentication is difficult** ・ The targets to communicate with are restricted with the settings of the target of verification (e.g., iptables for Linux). - Ex.) Targets to communicate with are restricted by IP address, etc. -Ex.) Targets to communicated with are limited to devices within the LAN.
	Implementation example 2) **Countermeasures against consecutive login attempt attacks (OR condition)** ・ Implement a delay in response time is according to the number of consecutive authentication failures. ・ Limit the number of authentication attempts, and set a suspension period during which login is not permitted if the limit is exceeded. ・ Limit the number of authentication attempts, and lock the authentication function when the limit is exceeded. ・ Ensure adequate entropy for authentication values based on cryptographic best practices. ・ Notify the user (and the privileged user) or the person in charge of operation (or maintenance) of the target of verification when login attempts are repeated.

Documents to submit	Documents specified by CCDS
7.1-1B	Conformity criteria
Inspection method	Conformity inspection of functional operation with the target of verification
Conditions of conformity	**Mandatory requirements** If the verification result of the target of verification meets the following conditions, the Conformity criteria will be satisfied. 1) Not applicable: Inspect documents based on 7.1-1A. 2) Authentication and access control functions for connected devices and user access work in compliance with the specifications. - Only access with the configured credentials is authorized and access without the credentials is denied. - The access control of the target to communicate with works properly according to the specifications. 3) As a result of the tool inspection based on the inspection procedure example, the set password cannot be analyzed. 4) The countermeasure against consecutive login attempt attacks works in compliance with the specifications. 5) Not applicable: Inspect document inspection based on 7.1-1A. **Remarks** ・ The item 3) and 4) above are not applicable, if B) device authentication, C) multi-factor authentication, or D) communication access control is implemented. **Recommended requirements** Not applicable
Actual machine inspection procedure example	Regarding the item 3) above, in addition to the normal authentication operation, use a password analysis tool to confirm that authentication with the passwords using the specified dictionary file is not successful. **Remarks** ・ Reference tool example: THC Hydra (Version 9.3 or later) ・ Use the ID dictionary file specified for inspection ・ Use the password dictionary specified for inspection * Original dictionaries specified by the designated verification operator can also be used. * If it is difficult to perform the actual machine inspection using a dictionary file due to the implemented countermeasures against the consecutive login attempt attack, the test using the password analysis tool can be excluded. (Only the normal

	authentication operation will be inspected)
Documents to submit	Inspection results and inspection logs required by CCDS

7.1-1-1 Disabling of TCP/UDP ports

Target security requirements			
Classification	ID	Security Requirements	Purpose of requirement
	(subset ID, security requirements)		
1. Functional requirements for IoT devices	1-1	Access Control and Authentication	Identification, access control, configuration change, privilege management, authentication
	1-1-1	Disable TCP/UDP ports	
1. Functional requirements for IoT devices	1) Close TCP/UDP ports not required for system operation. 2) Regarding ports required for system operation, demonstrate that they meet the specified conformity criteria through vulnerability inspection. **Remarks** Vulnerability inspection covers the following. Refer to the relevant conformity criteria for detailed implementation procedures and conditions. ・ Perform scanning TCP/UDP ports. ・ Perform a vulnerability scan (network scan) against open ports.		
Recommended requirements	1) Implement a function that can identify open TCP/UDP ports and can change their open/close statuses. 2) Allow only privileged users, equipment operators and maintenance personnel to change the opening/ closing TCP/UDP ports.		
7.1-1-1A	Conformity criteria		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) Specify the TCP/UDP ports that are open (LISTEN), and clarify the target port number, purpose of use, opening timing and conditions. 2) Not applicable: Perform actual machine inspection according to 7.1-1-1B. **Recommended requirements** ・ If the description of the submitted designated documents meets to the following conditions, the conformity criterial will be satisfied. 1) It is specified that the target of verification has the following mechanisms. - It has a mechanism that allows the target of verification to identify open TCP/UDP ports. - It has a mechanism to open as well as close the target ports.		

	2) It is specified that the mechanism to open and close the target port can be restricted from being executed by anyone other than the privileged users or the personnel in charge of operation (maintenance) of the target of verification.
Implementation example	None
Documents to submit	Submission of documents specified by CCDS
7.1-1-1B	**Conformity criteria**
Inspection method	Conformity inspection of functional operation with the target of verification
Conditions of conformity	**Mandatory requirements** If the verification result of the target of verification meets the following conditions, the Conformity criteria will be satisfied. 1) The result of the port scan by the tool matches the information described in the designated document. 2) The open ports are tested for known vulnerabilities using a tool, and no security issues with a score of 7.0 or higher have been detected. **Remarks** If any issue with a CVSS v3 score of 7.0 or higher is detected by the vulnerability scan in the item 2) above, the issue will need to be examined with the developer. If the security issue falls into any of the following as a result of the examination, the issue will be excluded and the Conformity criteria will be satisfied (OR condition). In this case, the applicant needs to submit the relevant examination record. A) In case that it is a false positive * When the function corresponding to the detected vulnerability is not implemented, etc. B) In case that countermeasures including operational measures have already been taken C) In case that it is possible to prove that the detected vulnerability has no impact in the actual environment. D) In case that additional attacks using actual exploit are performed and they do not succeed. **Recommended requirements** ・ If the verification result of the target of verification meets the following conditions, the Conformity criteria will be satisfied. 1) When the target port is closed, it is confirmed that the port is in a close state using a port scanning tool.

	2) It is confirmed that the mechanism to open and close the target port is restricted from being executed by anyone other than privileged users or the personnel in charge of equipment operation (maintenance) of the target of verification.
Actual machine inspection procedure example	**Mandatory requirements** 1) Use a port scanning tool to investigate TCP/UDP ports from 0 to 65535. **[Example of inspection tool command (NMAP)]** ・ Scan all TCP/UDP ports, starting with port 0, using the command below. nmap -r -sS -sU -Pn -p 0-65535 "IP address" 2) Scan the network for vulnerabilities using a vulnerability scanner. **[Setting example of inspection tool (GVM)]** ・ Settings of "Target" Port list: "All TCP and Nmap top 100 UDP" * If any UDP port not included in the above settings is detected as a result of a port scan, create and set a list of target UDP ports. ・ Settings of "Scan Task" Scanner: "OpenVAS Default" Scan Config: "Full and fast" **Remarks** ・ Examples of reference tools - Port scan: NMAP (Ver7.93 or later) - Vulnerability inspection: GVM (OpenVAS): Ver.21.4 or later, NVTs Version: Latest version at the time of inspection ・ If open ports vary depending on the operation mode, perform a port scan and vulnerability scan in each mode.
Documents to submit	Submission of inspection results and inspection logs required by CCDS

7.1-1-2 Change of credentials

Target security requirements			
Classification	ID	Security Requirements	Purpose of requirement
	(subset ID, security requirements)		
1. Functional requirements for IoT devices	1-1	Access Control and Authentication	Identification, access control, configuration change, privilege management, authentication
	1-1-2	Change of credentials	
Mandatory requirements	1) Implement a function to change credentials such as user IDs and passwords, and ensure that the credentials are not hard-coded. 2) Implement a function that requires the user to change the password when the target of verification starts for the first time if a unique default password is not unique to each target. 3) Restrict those other than privileged users, equipment operators or maintenance personnel from changing credentials.		
Recommended requirements	None		
7.1-1-2A	Conformity criteria		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) Implementation of a function that can change credentials, and clearly stating that credentials such as user IDs and passwords are not hard-coded. 2) It is specified that the default password is unique to each target of verification, or that a function that requires the user to change the password when the target of verification starts for the first time is implemented. 3) It is specified that only the privileged user or the person in charge of operation (or maintenance) of the target of verification is allowed to access the function to change credentials. **Remarks** ・ Regarding (2) and (3) above, if the “mechanism for automatically generating a password” described in 7.1-1 A Implementation example is implemented or if B) device authentication is implemented, the conformity criteria in this section will be satisfied. ・ This section is not applicable if D) Communication access control described in 7.1-1 A implementation example is implemented.		

	Recommended requirements Not applicable
Implementation example	None
Documents to submit	Submission of documents specified by CCDS
7-.1-1-2B	**Conformity criteria**
Inspection method	Conformity inspection of functional operation with the target of verification
Conditions of conformity	**Mandatory requirements** If the verification result of the target of verification meets the following conditions, the conformity criteria will be satisfied. * However, for (2), it is mandatory only when a unique password that differs for each device cannot be set. 1) After changing the settings, it shall be possible to confirm by the operation of the target of verification that access with the changed credentials is authorized and access with other information is not authorized. 2) If a unique default password cannot be set for each device, a function must be implemented that requires the user to change the password at the first startup. 3) 3) Execution of the credentials modification function shall be restricted to those other than privileged users or equipment operation (maintenance) personnel. **Recommended requirements** Not applicable
Actual machine inspection procedure example	This is confirmed by a system test using an actual machine.
Documents to submit	Inspection results and inspection logs required by CCDS

7.1-2 Data Protection

Target security requirements			
Classification	ID	Security Requirements	Purpose of requirement
	(subset ID, security requirements)		
1. Functional requirements for IoT devices	**1-2**	**Data Protection**	**Data protection, Protection of credentials and key information**
Mandatory requirements	1) Protect information assets stored in the storage area of the target of verification from unauthorized access and modification. (The same applies to data stored in storage media such as SD cards. 2) Protect information assets transmitted to other IoT devices and servers (including cloud servers) from information leak and alteration. 3) Manage credentials (password, private key, etc.) in an area protected from unauthorized access (tampering, theft, etc.) via the network, when the target of verification stores the credentials. **Remarks** ・ For data handled as information assets, perform a risk analysis for each product/service and clarify the target information.		
Recommended requirements	1) Implement encryption and prevent tampering data. Encryption algorithms and key management methods shall conform to the guidelines shown below. 2) Protect keys and certificates used for encryption from unauthorized access and modification. **[Guidelines related to cryptography]** - "List of reference ciphers for e-government procurement (CRYPTREC)" (Last revised: March 30, 2022, CRYPTREC LS-0001-2012R7) - "Criteria for setting cryptographic strength requirements (algorithm and key length selection)" (First Edition: June 2022, CRYPTREC LS-0003-2022) **[Supplementary documents for the above guidelines]** - "CRYPTREC Cryptography Guidelines (SHA-1) Revised version"(CRYPTREC GL-2001-2013R1) - "CRYPTREC Cryptographic Technology Guidelines (Lightweight Cryptography)" (CRYPTREC GL-2003-2016JP) - "Encryption key setting guidance " (CRYPTREC GL-3003-1.0)		

	- “Encryption Key Management System Design Guidelines (Basics)” (CRYPTREC GL-3002-1.0) “TLS cipher setting guidelines” (CRYPTREC GL-3001-3.0.1)
7.1-2A	**Conformity criteria**
Inspection method	Conformity inspection of documentation
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) The information assets to be protected are identified and protective measures are taken against unauthorized access and alteration. 2) For information assets transmitted to other IoT devices and servers (including cloud servers), protection measures against information leaks and alterations are taken. 3) Credentials (passwords, private keys, etc.) in the target of verification is protected from unauthorized access (tampering, theft, etc.) via the network, and protective measures are in place. **Recommended requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) It is specified that the adopted encryption algorithms and key management method comply with standards or best practices. 2) Keys and certificates used for encryption comply with standards or best practices (documents are exemplified in Recommended requirements), and it is specified that they are protected from unauthorized access or modification.
Implementation example	**Mandatory requirements** **Implementation example1)** **Protective measures for information assets to be protected (OR conditions).** ・ The software or hardware cryptography that is used in the market or in the company is adopted to protect the information assets. ・ Saved passwords are protected by hashing. ・ Personal information is stored after being converted into anonymously processed information or pseudonymously processed information. **Implementation example2) Protection measures for transmitted data** ・ The target of verification is always used only in an environment connected via a VPN or a dedicated line.

	・ It complies with the documents referred to in the recommended requirements, and supports TLS 1.2 or higher. **Recommended requirements** **Implementation example1)** **Protection measures for information resources to be protected** ・ Store information assets to be protected in a secure area using virtualization technology or security chips. ・ Adopt standardized or best-practice cryptography in accordance with the document referred to in the recommended requirements. **Implementation example2)** **Protection of critical security parameters** ・ ETSI EN303 645 defines passwords and private keys as important security parameters and recommends storing them in the following secure storage areas. - Trusted Execution Environment (TEE: Trusted Execution Environment) - Hardware Cryptographic Storage or Secure Elements (SE: Secure Elements) - Dedicated security component (DSC: Dedicated Security Components), UICC (Universal Integrated Circuit Card) **Remarks** ・ Public keys are public information and are not classified as important security parameters. ・ It is recommended that important security parameters not only in storage but also on memory should be protected using an equivalent implementation. **Implementation example3)** **Communication path encryption method** ・ It complies with the document referred to in the recommended requirements, and supports TLS 1.2 or higher. * Refer to Recommended requirements in 7.1-2.
Documents to submit	Submission of documents specified by CCDS
7.1-2B	**Conformity criteria**
Inspection method	Conformity inspection of functional operation with the target of verification
Conditions of conformity	**Mandatory requirements** (1)～(3) Not applicable: Perform document inspection according to 7.1-2A. **Recommended requirements**

	If the verification result of the target of verification meets the following conditions, the conformity criteria will be satisfied. 1) Not applicable: Perform document inspection according to 7.1-2A. 2) Regarding the encryption of the communication path, capture data of the communication log is obtained, and the notation of the cipher suite in the log matches the method described in the specifications.
Actual machine inspection procedure example	**Recommended requirements** *** Example of inspection procedure for Conditions of conformity (2)** ・ Acquire communication log capture data (Client Hello packets) and confirm that the listed cipher suite conforms to standards or best practices. **[Description of cipher suite]** ・ Up to TLS v1.2: TLS_[Kx]_[Au]_WITH_[Enc]_[Hash/Mac] ・ Up to TLS v1.3: TLS_[Enc/Mac]_[Hash]
Documents to submit	Submission of inspection results and inspection logs required by CCDS

7.1-2-1 Data erasure function

Target security requirements			
Classification	ID (subset ID, security requirements)	Security Requirements	Purpose of requirement
1. Functional requirements for IoT devices	1-2	Data Protection	Data protection, Protection of credentials and key information
	1-2-1	Data erasure function	
Mandatory requirements	1) Ensure that the information configured by the user and the information obtained during use of the target of verification can be easily deleted. 2) Ensure that updated system software is maintained even after deleting the information.		
Recommended requirements	None		
7.1-2-1A	Conformity criteria		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) It is specified that a function that allows user-changeable setting values and information acquired by the target of verification during use to be deleted is implemented. 2) It is specified that the updated system software version will be maintained even after deleting the information.		
Implementation example	None		
Documents to submit	Submission of documents specified by CCDS		
7.1-2-1B	Conformity criteria		
Inspection method	Conformity inspection of functional operation with the target of verification		
Conditions of conformity	**Mandatory requirements** ・ If the description of the submitted designated documents conforms to the following conditions, the judgment of conformity will be given. 1) It is specified that the updated system software version will be maintained even after deleting information. 2) Confirm that the updated system software version is maintained even after deleting the information. **Recommended requirements** Not applicable		

Actual machine inspection procedure example	This is confirmed by a system test using an actual machine.
Documents to submit	Inspection results and inspection logs required by CCDS

7.1-3 Software Update

Target security requirements			
Classification	ID	Security Requirements	Purpose of requirement
	(subset ID, security requirements)		
1. Functional requirements for IoT devices	**1-3**	**Software Update**	**Operational Incident Response**
Mandatory requirements	1) Implement software update functionality. 2) Ensure that the software update status is maintained even after the power is turned off. 3) Have a means to confirm that the software update has been completed normally, such as displaying the version after the update. 4) Regarding the update program, the applicant shall guarantee that only genuine update is applicable, without any alterations through the update process (countermeasures against alteration). **Remarks** Either of the following methods is applicable. The software update is: - automatically initiated; or - manually performed by maintenance personnel or privileged users who have explicit management responsibility.		
Recommended requirements	1) Have a mechanism to verify the authenticity of the update software when the target of verification installs the update (countermeasures against tampering). 2) Encrypt communication channels or encrypt data during transmission for update software (data protection). 3) Restrict anyone other than privileged users, equipment operators or maintenance personnel from executing a function that disables the software update function, if implemented. 4) Implement a function to enable and disable notification of updates.		
7.1-3A	**Conformity criteria**		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) The implementation of the software update function shall be specified. 2) It is specified that the updated system software version will be maintained even after the power is turned off.		

	3) The means by which it can be confirmed that the installation of the software version has been successfully completed shall be specified. 4) The software update process and the means by which the authenticity of the update process can be confirmed shall be specified. **Recommended requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) Implementation of a mechanism to verify the authenticity of the software on the target of verification side when installing update software is specified. 2) The transmission of update software is protected by encrypting the communication path or encrypting the data at the time of transmission. In addition, it is specified that the adopted encryption method and key management method comply with standards or best practices. 3) When a function to disable the software update function is implemented, the restriction on execution by anyone other than the privileged user or the person in charge of operation (maintenance) of the target of verification is specified as a function. 4) Implementation of a function to enable or disable notifications about updates is specified.
Implementation example	**Mandatory requirements** **Implementation example1)** **How to verify successful installation of update software** ・ It has a function to check the version information of the installed software. ・ It has a function to notify or display the status of installation failure to the user. **Implementation example2)** **Means of ensuring the authenticity of software** ・ Operation (maintenance) personnel who have explicit management responsibility directly update software that has been approved in-house (in the case of operation support). **Recommended requirements** **Implementation example1)** **Software Authenticity Verification Method on the Target of Verification** ・ Before installing update software, it checks against the given electronic signature, and stops the installation if tampering is detected.

	Implementation example2) **Communication path encryption method** ・ Comply with the document describing the recommended requirements, and support encryption methods of TLS 1.2 or higher.
Documents to submit	Documents specified by CCDS
7.1-3B	**Conformity criteria**
Inspection method	Conformity inspection of functional operation with the target of verification
Conditions of conformity	**Mandatory requirements** If the verification result of the target of verification meets the following conditions, the conformity criteria will be satisfied. 1) The software update function operates as specified, and the software can be updated normally. 2) When the power is turned off and on after updating the software, the updated version of the system software is maintained. 3) The means by which it can be verified that the installation of the software version has been successfully completed conforms to the specification and is operating. 4) Not applicable: Perform document inspection according to 7.1-3A. **Recommended requirements** If the verification result of the target of verification meets the following conditions, the conformity criteria will be satisfied. 1) When updating software is installed, the mechanism for verifying the authenticity of the software on the target of verification conforms to the specifications and operates normally. From 2) to 4) : Not applicable: Perform document inspection according to 7.1-3A.
Actual machine inspection procedure example	**Recommended requirements** *** Example of inspection procedure for Conditions of conformity (1)** ・ The update is not performed and the target of verification can be used normally when using data that modifies part of the binary of the authorized software.
Documents to submit	Inspection results and inspection logs required by CCDS

7.1-4 Requirements with a particularly large number of incidents and high impact

7.1-4-1 Wi-Fi authentication method

Target security requirements			
Classification	ID	Security Requirements	Purpose of requirement
	(subset ID, security requirements)		
1. Functional requirements for IoT devices	1-4	Requirements with a particularly large number of incidents and high impact	None
	1-4-1	Wi-Fi authentication method	
Mandatory requirements	1) Implement the latest authentication method recommended by the Wi-Fi Alliance®.		
Recommended requirements	None		
7.1-4-1A	Conformity criteria		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) The specified document clearly states that the Wi-Fi authentication method satisfies the following standards. **[Conformity criteria for Wi-Fi authentication]** - Authentication method: Compatible with WPA2 or higher - Encryption protocol: equivalent to or better than CCMP - Encryption Algorithm: AES (128-bit or higher) - A password that can be set by default or that can be set must be eight characters or more and must contain a mix of lowercase letters, numbers, and uppercase letters. **Remarks** ・ If it is difficult to implement using a combination of lowercase letters and uppercase letters, ensure the same entropy (randomness of values) with the password length. **Recommended requirements** Not applicable		
Implementation example	None		

Documents to submit	Documents specified by CCDS
7.1-4-1B	**Conformity criteria**
Inspection method	Conformity inspection of functional operation with the target of verification
Conditions of conformity	**Mandatory requirements** If the verification result of the target of verification meets the following conditions, the conformity criteria will be satisfied. 1) WPA2-compliant authentication is implemented, and access only with the configured credentials is authorized, and access without the credentials is not authorized. **Recommended requirements** ・ Not applicable
Actual machine inspection procedure example	Regarding the item 1) above, in addition to the normal authentication operation, use a Wi-Fi passphrase analysis tool to confirm that the password based on the specified dictionary file is not successful. **Remarks** ・ Reference tool example: aircrack-ng (Ver1.7 or later) ・ Use a password dictionary specified for inspection. ・ A dictionary file for SSIDs is not used since they can be monitored. * Original dictionaries specified by designated verification operators can also be used.
Documents to submit	Inspection results and inspection logs required by CCDS

7.1-4-2 Bluetooth vulnerability countermeasures

Target security requirements			
Classification	ID	Security Requirements	Purpose of requirement
	(subset ID, security requirements)		
1. Functional requirements for IoT devices	1-4	Requirements with a particularly large number of incidents and high impact	None
	1-4-2	Bluetooth vulnerability countermeasures	
Mandatory requirements	1) Implement the latest pairing method recommended by Bluetooth SIG. 2) Ensure that unnecessary Bluetooth profiles are not recognized. 3) Ensure that the target of verification is not vulnerable to Bluetooth's Blueborne vulnerability.		
Recommended requirements	None		
7.1-4-2A	Conformity criteria		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) The authentication method at the time of pairing shall clearly indicate conformity with the following. ・ For Bluetooth Classic - Compliant with Secure Simple Pairing (SSP mode) ・ For Bluetooth Low Energy - Compliant with LE Secure Connections for Bluetooth 4.2 and above 2) The specified document clearly states that the implemented Bluetooth profile satisfies the following criteria. - The profile to be used is specified and the obsolete profile is not used. - Profiles other than those specified are configured not to work even when connected. 3) In the specified document, the target of verification with Bluetooth functions do not use the following versions of OS/software that may be vulnerable to Blueborne. ・ Android - Android without security patch level September 2017 (CVE-2017-0781, CVE-2017-0782, CVE-2017-0783, CVE-2017-0785) ・ Linux - kernel 4.13.2 or later version		

	-BlueZ 5.47 and later versions ・ Windows -Not applying the September 2017 Microsoft Security Updates -Windows Vista or later Windows (CVE-2017-8628) ・ iOS, tvOS -iOS 9.3.5 and earlier, AppleTV tvOS 7.2.2 and earlier (CVE-2017-14315) **Remarks** ・ Regarding the item 1) above, even if SSP is implemented, if the following modes and authentication methods are used, the conditions of conformity are not satisfied. A) For Bluetooth Classic - Security mode: “Mode 1: Non-Secure” - Authentication method: “Just works” B) For Bluetooth LE - Security mode: “LE Security Mode 1: Level 1: No security” ・ See below for the obsolete profiles in the item 2) above. Bluetooth SIG, Inc “Specifications and Test Documents List”[6] * ”Status: Withdrawn” is the obsolete profile. **Recommended requirements** Not applicable
Implementation example	None
Documents to submit	Documents specified by CCDS
7-.1-4-2B	**Conformity criteria**
Inspection method	Conformity inspection of functional operation with the target of verification
Conditions of conformity	**Mandatory requirements** If the verification result of the target of verification meets the following conditions, the conformity criteria will be satisfied. 1) It is confirmed that the pairing authentication method conforms to Secure Simple Pairing (SSP mode) or LE Secure Connections, and pairing must be possible normally by manually operate the target of verification. 2) As a result of scanning with an inspection tool (a tool for checking usage profiles), no profiles other than those described in the specified document are detected. 3) As a result of scanning with an inspection tool (vulnerability confirmation tool), no

[6] Bluetooth SIG, Inc "Specifications and Test Documents List"
https://www.bluetooth.com/specifications/specs/?status=withdrawn&show_latest_version=0&show_latest_version=1&keyword=&filter=

	vulnerabilities falling into the following CVEs have been detected. - CVE-2017-0782 - CVE-2017-0785 - CVE-2017-1000250 - CVE-2017-1000251 **Recommended requirements** Not applicable
Actual machine inspection procedure example	1) Perform pairing with the target of verification manually. 2) Use a tool such as “sdptool” and “nRF connect for Mobile” to check the installed profile. 3) Confirm the presence or absence of each vulnerability described in the conditions of conformity using the PoC tool. **Remarks** For the CVE vulnerability described in the item 3) above, a Proof of Concept (PoC) tool for demonstrating the vulnerability has been published on the web, and the presence or absence of the vulnerability is verified by inspection with this tool.
Documents to submit	Inspection results and inspection logs required by CCDS

7.1-4-3 USB access control

Target security requirements			
Classification	ID	Security Requirements	Purpose of requirement
	(subset ID, security requirements)		
1. Functional requirements for IoT devices	1-4	Requirements with a particularly large number of incidents and high impact	None
	1-4-3	USB access control	
Mandatory requirements	1) Appropriately control access to the USB interface and restrict access rights.		
Recommended requirements	1) Do not implement USB ports that are not necessary for the service. 2) Take measures to make the USB ports difficult to be utilized by anyone other than the person in charge of operation.		
7.1-4-3A	Conformity criteria		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) Appropriate access control to the USB interface and restrictions on access rights are specified. **Recommended requirements** 1) The intended use of the USB interface is specified, and unnecessary USB ports are not used. 2) Some measures are introduced so that anyone other than the person in charge of operation cannot easily access the USB ports.		
Implementation example	**Mandatory requirements** **Implementation example for USB access control (OR condition)** ・ Enable only the required device classes and disable the others - USB usage restrictions with Windows Group Policy - USB whitelist setting using dedicated software ・ USB protection with external solutions ・ Use of USBGuard software framework (in case of Linux Red Hat)		
Documents to submit	Documents specified by CCDS		
7.1-4-3B	Conformity criteria		
Inspection method	Conformity inspection of functional operation with the target of verification		
Conditions of conformity	* No inspection of functional operation required		

Actual machine inspection procedure example	None
Documents to submit	None

7.1-4-4 Injection countermeasures

Target security requirements			
Classification	**ID**	**Security Requirements**	**Purpose of requirement**
	(subset ID, security requirements)		
1. Functional requirements for IoT devices	**1-4**	**Requirements with a particularly large number of incidents and high impact**	**None**
	1-4-4	**Injection countermeasures**	
Mandatory requirements	1) Significant vulnerabilities such as injection via Web input have been fixed.		
Recommended requirements	None		
7.1-4-4A	**Conformity criteria**		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) It is specified whether the target of verification has settings or functions (web functions) that use the http/https protocol. If the web functions are implemented, the following vulnerabilities in the actual machine inspection specified in 7.1-4-4B are not detected or countermeasures have been taken. [Target Vulnerability] - CWE-78: OS command injection - CWE-89: SQL injection - CWE-352: Cross Site Request Forgery (CSRF) - CWE-22: Path Traversal **Remarks** * Not required if not implemented This requirement is mandatory only when the target of verification has settings and functions (web functions) that use the http/https protocol in the target of verification itself or in the system (including cloud collaboration and mobile collaboration).		

	Recommended requirements Not applicable
Implementation example	None
Documents to submit	Documents specified by CCDS
7.1-4-4B	**Conformity criteria**
Inspection method	Conformity inspection of functional operation with the target of verification
Conditions of conformity	**Mandatory requirements** If the verification result of the target of verification meets the following conditions, the conformity criteria will be satisfied. 1) Perform a known vulnerability inspection with a vulnerability scanning tool, and no vulnerabilities corresponding to the CVE-IDs listed at the following URL are detected. [URL] https://nvd.nist.gov/vuln/search [Search condition] Search Type: Advanced Category: - OS Command Injection - SQL Injection - Cross-Site Request Forgery (CSRF) - Path Traversal **Remarks** If any relevant security issue is detected by the vulnerability inspection in the item 1) above, examine the issue together with the developer. If the security issue falls int any of the following as a result of the examination, the issue will be excluded and the conformity criterial will be satisfied (OR condition). In this case, the applicant needs to submit the relevant examination record. A) In case that it is a false positive * When the function corresponding to the detected vulnerability is not implemented, etc. B) In case that countermeasures including operational measures have already been taken C) In case that it is possible to prove that the detected vulnerability has no impact in the actual environment. D) In case that additional attacks using actual exploit are performed and they do not succeed.

	Recommended requirements ・ Not applicable
Actual machine inspection procedure example	1) Scan the network for vulnerabilities using a vulnerability inspection tool. **[Setting example of inspection tool (GVM)]** ・ Settings of Target Port list: “All TCP and Nmap top 100 UDP” * If any UDP port not included in the above settings is detected as a result of a port scan, create and set a list of target UDP ports. ・ Settings of Scan Task Scanner: “OpenVAS Default” Scan Config: “Full and fast” **Remarks** ・ Reference tool example: GVM (OpenVAS): Ver.21.4 or later, NVTs Version: Latest version at the time of inspection ・ If open ports vary depending on the operation mode, perform vulnerability inspection in each mode.
Documents to submit	Inspection results and inspection logs required by CCDS

7.2-1 Contact point and security support system

Target security requirements			
Classification	ID	Security Requirements	Purpose of requirement
	(subset ID, security requirements)		
2.Requirements for the operation of IoT devices	2-1	Contact and security support	Operational Incident Response
Mandatory requirements	1) Have a contact regarding product vulnerabilities, and it is open to the public. 2) Have a mechanism to provide security updates of products in a timely manner.		
Recommended requirements	None		
7.2-1A	Conformity criteria		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) A contact for informing and inquiring about product vulnerabilities is established and opened to the public. 2) A system and process are in place to enable timely updates in response to possible security issues of the target product. **Recommended requirements** ・ Not applicable		
Correspondence example	**point of contact for product vulnerabilities)** ・ E-mail addresses and phone numbers for contact and/or a transmission form is maintained on the website, so that anyone, not just product users, can report problems. **Security update system, example of process)** ・ PSIRT or a system in charge of an equivalent role is in place, and a process for collecting information on vulnerabilities, triage, analysis, improvement and remediation is in place. ・ In addition to the above, a system is in place to enable timely responses to issues that require updates.		
Documents to submit	Documents specified by CCDS		
7.2-1B	Conformity criteria		
Inspection method	Conformity inspection of functional operation with the target of verification		
Conditions of conformity	* No inspection of functional operation required		

Actual machine inspection procedure example	None
Documents to submit	None

7.2-2 Product document management

Target security requirements			
Classification	ID	Security Requirements	Purpose of requirement
	(subset ID, security requirements)		
2.Requirements for the operation of IoT devices	**2-2**	**Product document management**	Security response status stipulation
Mandatory requirements	1) Define and manage information related to cyber security throughout the life cycle of the product, which includes recording it in documents and updating them.		
Recommended requirements	None		
7.2-2A	**Conformity criteria**		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) Documentation is properly managed regarding the status of product security measures. **Recommended requirements** Not applicable		
Correspondence example	**Example of document management related to products)** ・ **Specifying of product composition and clarifying of cyber security functions** - In system models, clarify the software configuration and hardware configuration, and specify each function (including cyber security related functions). ・ **Clarifying of the physical usage environment:** - In use cases, specify the physical usage environment (installation location, etc.) and related actors (stakeholders). ・ **Clarifying of responsibilities:** - Define system models and use cases based on product requirements. In system models, clarify the points of division of responsibility between service providers and affiliated companies such as outsourcers. ・ **Maintenance:** - Define and document maintenance, maintenance work requirements and procedures, and cybersecurity considerations. In addition, when outsourcing, define the criteria of the outsourcing company.		
Documents to submit	Documents specified by CCDS		
7.2-2B	**Conformity criteria**		

Inspection method	Conformity inspection of functional operation with the target of verification
Conditions of conformity	* No inspection of functional operation required
Actual machine inspection procedure example	None
Documents to submit	None

7.2-3 Provision of information to users

Target security requirements			
Classification	ID	Security Requirements	Purpose of requirement
	(subset ID, security requirements)		
2.Requirements for the operation of IoT devices	**2-3**	**Provision of information to users**	**Operational support**
Mandatory requirements	1) Clearly indicate the procedure for users to use the products securely regarding configurations and/or usage that can impact cybersecurity. 2) Inform users of the content and necessity of product software updates, and the impact in case of not updating software. 3) Inform users of disclaimers for possible accidents and failures. 4) Notify the user of the support period and end-of-support policy for the relevant products and/or services. 5) Inform users of the assumed risks of disposing of the target of verification with data remaining in them, and how to securely dispose of the target of verification, including data deletion.		
Recommended requirements	None		
7.2-3A	**Conformity criteria**		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	**Mandatory requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) It is specified that the procedures for initial settings, usage, etc. that could affect cybersecurity for users. 2) A policy to notify users of the content and necessity of software updates for the product and the impact in case of not updating software is clearly stated. 3) A policy is specified to inform users of the exemptions for assumed accidents and failures. 4) A process is clearly defined to notify users of the support period and the end-of-support policy for the target product or service. 5) It is specified that the user is informed of the assumed risks of disposing of the target of verification with data remaining and how to securely dispose of the target of verification, including data deletion. **Recommended requirements** Not applicable		

Correspondence example	**Example of providing information to users)** **1) Disclosure examples of settings and methods of use that affect information security** -Disseminate information on how to change user IDs and passwords, how to change passwords using hard-to-identify values, and how to make initial settings that are safe from a security standpoint, through manuals, web pages, etc. **2) Examples of security update information provision** -Regarding security updates, the following information will be disseminated on the web page and by e-mail, etc. **[Purpose of update]** -Indicate whether it is a feature addition or change, or a bug or vulnerability fix **[Information about bugs and vulnerabilities]** -Provides an overview of the issues encountered and their impact on users -Provides software/firmware version information where the problem occurs **[How to update]** -Indicates whether automatic update or manual update is required -For manual updates, provide specific instructions and where to get the update program (web link or URL) -If the update will affect the function of the target of verification, or if it is difficult to update the target of verification, the reason and countermeasures will be presented. **[Updated by]** -Indicate whether it is performed by the user or by the product provider (operation or maintenance staff, etc.) **3) Inform users of disclaimers for possible accidents and failures** ・ Distinguish between what should be handled as part of the scope of product support and disclaimers that are not applicable to support in the event of an assumed accident or failure, and notify users in advance through contracts, manuals, web pages, etc. **4) Disseminate support deadlines and end-of-support policies for target products and services** ・ Users will be informed of the deadline for support for the target product, the period of prior notice of the end of support, and the actions required of users after the end of support, in advance contracts, manuals, web pages, etc. * A policy is in place to disseminate information on the above.

	5) Publicize the risk of disposing of the target of verification with data remaining in them and how to dispose of them safely. ・ If data is discarded without erasing it, the remaining data (especially credentials and personal information), the risk of leakage, and what should be done in advance for safe disposal are explained in the manual and on the website. Publicize it on the page, etc.
Documents to submit	Submission of documents specified by CCDS
7.2-3B	**Conformity criteria**
Inspection method	Conformity inspection of functional operation with the target of verification
Conditions of conformity	* No inspection of functional operation required
Actual machine inspection procedure example	None
Documents to submit	None

7.3-1 Audit log recording

Target security requirements			
Classification	**ID**	**Security Requirements**	**Purpose of requirement**
	(subset ID, security requirements)		
3.Requirements for auditing IoT devices	**3-1**	**Audit log recording**	**Operational Incident Response**
Mandatory requirements	None		
Recommended requirements	1) Implement audit trail recording features and enable privileged users, equipment operators or maintenance personnel to access the audit trail. 2) Ensure there is sufficient storage for recording audit trail. If the storage capacity for the audit trail is exceeded, take appropriate measures such as overwriting the oldest records in order. 3) Take measures to prevent unauthorized deletion or modification for recorded audit trail. **Remarks** ・ The audit trail shall be stored in the target of verification itself and/or servers to control the target of verification. ・ The necessary size of the storage shall be separately examined based on the usage of each product.		
7.3-1A	**Conformity criteria**		

Inspection method	Conformity inspection of documentation
Conditions of conformity	**Mandatory requirements** Not applicable **Recommended requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) Audit trail recording features are implemented. In addition, it is specified that only the privileged user or the person in charge of operation (or maintenance) of the target of verification is allowed to access the audit trail. 2) Required storage for audit trail is defined in specifications, and countermeasures in case the size of the audit trail exceeds the storage capacity are also specified. 3) It is specified that measures to prevent unauthorized deletion or modification of the audit trail.
Implementation example	**Example of records for audit trail)** ・ The following events are recommended to be recorded with the type, and date and time of occurrence. - Login attempts (successful and unsuccessful) - Login attempts that exceed thresholds and records of the target of verification responses (See Implementation example 2 in 7.1-1A) - When the maximum record capacity is reached, with the substituted action (records of past audit trails that were deleted when saving the latest audit trails, etc.) - When administrator identification fails in the initial state - Use of administrative functions - When software tampering is detected - When time configuration is changed (including time before and after the change)
Documents to submit	Documents specified by CCDS
7.3-1B	**Conformity criteria**
Inspection method	Conformity inspection of functional operation with the target of verification
Conditions of conformity	**Mandatory requirements** Not applicable **Recommended requirements** If the verification result of the target of verification meets the following conditions, the conformity criteria will be satisfied. 1) An audit trail read from the target of verification is recorded. 2) -3) : Not applicable: Perform document inspection according to 7.3-1A

Actual machine inspection procedure example	None
Documents to submit	Submission of inspection results and inspection logs required by CCDS

7.3-1-1 Time management function

Target security requirements			
Classification	ID	Security Requirements	Purpose of requirement
	(subset ID, security requirements)		
3.Requirements for auditing IoT devices	3-1	Audit log recording	Operational Incident Response
	3-1-1	Time management function	
Mandatory requirements	None		
Recommended requirements	1) Implement a time management function to record the date and time of a security event in the audit trail. **Remarks** The requirement will be satisfied in the case where the date and time of an event can be managed by either the target of verification or the server.		
7.3-1-1A	Conformity criteria		
Inspection method	Conformity inspection of documentation		
Conditions of conformity	**Mandatory requirements** Not applicable **Recommended requirements** If the description of the submitted designated documents meets the following conditions, the conformity criteria will be satisfied. 1) Implementation of a time management function for recording the date and time of occurrence of security event audit trails is specified.		
Implementation example	None		
Documents to submit	Documents specified by CCDS		
7.3-1-1B	Conformity criteria		
Inspection method	Conformity inspection of functional operation with the target of verification		
Conditions of conformity	**Mandatory requirements** Not applicable **Recommended requirements** If the verification result of the target of verification meets the following conditions, the conformity criteria will be satisfied. 1) The date and time of occurrence are recorded normally in the audit trail read from the target of verification.		

Actual machine inspection procedure example	This is confirmed by a system test using an actual machine.
Documents to submit	Inspection results and inspection logs required by CCDS

8. Documents related to this guideline

For a comparison of the security requirements described in this guideline and the overseas security documents shown in Table 5, and the conformity status, please refer to the attachment “ANNEX 1_Correspondence to overseas security guidelines and standards.”

[Table 5] Overseas documents to be compared in Annex 1

Issuer	Issued in	Document name
NIST	September 2022	NIST IR 8425 “Profile of the IoT Core Baseline for Consumer IoT Products”
ETSI	June 2020	ETSI EN 303 645 v2.1.1 “Cyber Security for Consumer Internet of Things: Baseline Requirements”
EUROPEAN COMMISSION	September 2022	“ANNEXES to the PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL”

For the inspection methods described in this guideline, please also refer to the "CCDS IoT Security Evaluation Verification Guideline".

9. References.

References in this document are listed below.

[1. Guidelines related to cryptography]

https://www.cryptrec.go.jp/list.html

"List of reference ciphers for e-government procurement (CRYPTREC)" (Last revised: March 30, 2022, CRYPTREC LS-0001-2012R7))

https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r7.pdf

"Criteria for setting cryptographic strength requirements (algorithm and key length selection)" (First Edition: June 2022, CRYPTREC LS-0003-2022)

https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022.pdf

[Supplementary documents for the above guidelines]

https://www.cryptrec.go.jp/op_guidelines.html

"CRYPTREC Cryptography Guidelines (SHA-1) Revised version"(CRYPTREC GL-2001-2013R1)

https://www.cryptrec.go.jp/report/cryptrec-gl-2001-2013r1.pdf

"CRYPTREC Cryptographic Technology Guidelines (Lightweight Cryptography)" (CRYPTREC GL-2003-2016JP)

https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf

"Encryption key setting guidance " (CRYPTREC GL-3003-1.0)

https://www.cryptrec.go.jp/report/cryptrec-gl-3003-1.0.pdf

"Encryption Key Management System Design Guidelines (Basics)" (CRYPTREC GL-3002-1.0)

https://www.cryptrec.go.jp/report/cryptrec-gl-3002-1.0.pdf

"TLS cipher setting guidelines" (CRYPTREC GL-3001-3.0.1)

https://www.cryptrec.go.jp/report/cryptrec-gl-3001-3.0.1.pdf

[3. Overseas Security Requirements Documents/Standards]

NIST IR 8425 "Profile of the IoT Core Baseline for Consumer IoT Products" (NIST)
https://csrc.nist.gov/publications/detail/nistir/8425/final

ETSI EN 303 645 v2.1.1 "Cyber Security for Consumer Internet of Things: Baseline Requirements" (ETSI)
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

"ANNEXES to the PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL"(EUROPEAN COMMISSION)
https://trade.ec.europa.eu/doclib/docs/2021/december/tradoc_159967.pdf

[4. CCDS-related guidelines】

"CCDS IoT Security Evaluation and Verification Guidelines Version 1.0"
https://www.ccds.or.jp/public_document/index.html#Verification_guidelines1.0