No.		Primitive					Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Comm
		S	A	C	E	D							
I	1	○	○		○	○	User management	Account lockout mechanism	Prevent improper operation of the device by a third party	Provide a function for locking the account and preventing login when	Check available account lockout settings, and check that the account		
	2		○		○	○		Option to force-expire accounts not used for a certain period of time	Prevent login from accounts not used for a certain period of time	Provide a function for locking an account that has elapsed a set expiration period	Check that accounts expire at the end of the expiration period		
	3		○		○	○		Function for ensuring password strength	Prevent unauthorized login by brute force, dictionary, and other attacks	Provide a function for allowing only passwords that meet certain conditions, such as the use of multiple character types and minimum	Check that passwords that do not meet the required conditions cannot be registered		
	4		○		○	○		Password security options (two-factor authentication, etc.)	Make it difficult for a third party to log in to the system	Enable the use of password security options (e.g., two-factor authentication)	Check that password security options can be used		
	5		○		○	○		Permission management for accounts used to launch services and processes	Restrict permissions for launching services and processes by account, and keep the scope of impact when an incident occurs to within	Do not require a superuser when launching services and processes	Check that the system operates with a dedicated user for services and processes		
	6		○		○	○		Shared user account	Enable the assignment of appropriate permissions according to use	Provide an account management function	Check that a shared account is used with appropriate permissions and scope of sharing		
	7		○		○	○		Assignment of appropriate permissions to administrative users	Enable administrative users to use necessary permissions	Provide a function for managing permissions	Check that administrative users are assigned appropriate permissions		
	8		○		○	○		Function for assigning permissions to general users	Enable users to use only necessary permissions	Provide a function for assigning permissions to users	Check that permissions can be assigned to users, and the system can be used according to permissions		
	9		○		○	○		Authorization control function	Enable the assignment of access rights according to roles	Provide a function for assigning access rights according to the role of an account	Check that information and functions that are not authorized cannot be used		
	10		○		○	○		Service linkage	Ensure login information is not relayed to other services more than necessary	Provide a function for indicating to the user the information relayed to other services when linking those services	Check what information is relayed to other services		
II	1				○	○	Software management	Web application firewall	Enable the use of web application firewalls	Enable web application firewalls	Check that web application firewalls can be used		
	2		○		○	○		Firewall function included with the product	Use the firewall function included with the product to increase security	Enable the firewall function included with the product	Check that the firewall function included with the product can be used		
	3		○		○	○		Software version	Use the software version that addresses vulnerabilities, bugs, and other issues to ensure security	Provide a function for updating the software and a function for checking the version	Check that the software can be updated and the version can be checked		
	4		○		○	○		Anti-virus function	Use the anti-virus function included with the product to increase security	Enable the use of the anti-virus function included with the product	Check that the anti-virus function included with the product can be used		
	5		○		○	○		Improper data processing	Prevent unintended system operations	Provide a function for restricting data to be accepted	-		
	6		○	○	○	○		Data traffic	Take DDoS and other attacks into consideration in designing the amount of data traffic handled by the system	Provide a function for restricting the amount of data traffic to be accepted, or other similar functions	Check the amount of data traffic to be accepted		
III	1		○		○	○	Security management	Log management function	Save logs so that the situation can be assessed in the event of an incident or otherwise when needed	Provide a log management function for recording events that occurred against the system	Check that log information can be accessed		
	2		○		○	○		Session management (Cookie settings)	When the system uses cookies, provide appropriate attributes	Set the Secure and HttpOnly attributes to the appropriate values of cookies	Check that the Secure and HttpOnly attributes are set to the appropriate values of cookies		
	3		○		○	○		Session management (URL rewriting)	Ensure session IDs are not leaked due to unnecessary URL rewriting	Check whether URL rewriting is necessary	Check that session IDs are not embedded in URLs		
	4		○		○	○		Session management (Issuance of session ID when logging in and processing	Reduce the risk of confidential information getting stolen through the theft of session information	A new session ID should be issued when logging in and after processing important confirmation, and the old session ID should be	Check that session IDs differ before and after logging in and processing important confirmation		
	5		○		○	○		Security measures against client data manipulation	Prevent the data of other accounts from being viewed and manipulated	Provide a data management function for each account	Check that the data of other accounts cannot be viewed and manipulated		
	6		○		○	○		Security measures against system data manipulation	Allow system data to be viewed and manipulated only by limited users	Provide a function that enables only designated system administrators to view and manipulate system data	Check that users other than designated system administrators cannot view and manipulate system data		
	7				○	○		Cloud interface and network vulnerabilities (API interface, cloud-based web interface, etc.)	Check that no known cloud interface and network vulnerabilities exist in the system	Check publicly available vulnerability information, and provide a function for indicating the services being used to the user	Check publicly available vulnerability information		
	8				○	○		Vulnerability of XSS, SQLi, and CSRF	Check that no known vulnerability of XSS, SQLi, CSRF, etc. exists in the system being used	Practice secure coding, and avoid including any vulnerability of XSS, SQLi, CSRF, etc.	Check publicly available vulnerability information		
	9				○	○		Web application SSL certificate	Implement an SSL certificate in a manner suited to one's own system	Provide a certificate suited to the system (e.g., EV certificate)	Check the certificate used		
IV	1		○		○	○	Access control	Access by uncontrolled physical means	Prevent system access by uncontrolled physical means	Provide a function for enabling restriction of physical means (USB, etc.) to access the system according to use	Check that access by uncontrolled physical means is restricted		
	2		○		○	○		Default ports for remote access	Prevent attacks targeting default ports for remote access functions	Provide a function for changing default ports	Check that default ports can be changed		
	3		○	○	○	○		Wireless communication security (encryption method)	Use a secure encryption method to prevent the stealing of communicated content using vulnerabilities	Enable the use of secure encryption methods	Check that a secure encryption method is selected upon connection		
	4		○	○	○	○		Wireless communication security (WPS)	Prevent compromising security due to errors in wireless settings	Consider security when providing a WPS function (e.g., MAC address filtering)	Check that WPS functions properly		
V	1		○		○	○	Unauthorized connection	Restriction of network ports	Make only appropriate ports available according to the anticipated use	Provide a function for opening or closing ports according to the purpose of use	Check that ports are opened or closed as configured		
	2		○		○	○		UPnP	Make UPnP available on devices anticipated to be used	Provide a function for enabling and disabling UPnP	Check that the device behaves as configured when connected		
	1		○	○	○	○		Data encryption function	Prevent sending data in plain text and allowing communications to be eavesdropped	Provide a function for encrypting individual data	Check that a data encryption function is available		

No		Primitive					Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Comment
VI	2		○	○	○	○	Encryption	Communication encryption function	Prevent sending data in plain text and allowing communications to be eavesdropped	Provide a function for performing encrypted communication using SSL/TLS, etc. between the devices that make up the system	Check that encrypted communication can be used		
	3		○	○	○	○		Encryption method	Enable checking the encryption method used	Provide a function for checking the encryption method used	Check the encryption method used		
	4		○	○	○	○		Certificate update function	Ensure certificates do not expire	Provide a function for updating certificates	Check that certificates are valid		
VII	1	○					System settings	Function for checking the status of sensor operation	Enable checking the status of operation	Provide a function for checking or notifying the current status of sensor operation	Check the status of sensor operation		
	2		○		○	○		Log security management	Prevent logs from being accessed or falsified by a third party	Provide a function for specifying users who can access logs and preventing falsification of their content	Check that users without access permissions cannot access logs, and that users who can access logs cannot modify them		
VIII	1	○					Notification	Alert and notification function for security events (irregular state, etc.)	Enable rapid response when a security event occurs by sending an alert	Provide a function for sending an alert when a security event occurs (e.g., irregular state)	Check that the system operates according to specifications		
	2		○		○	○		Alert and notification function for security events (authentication failure, expired certificate, etc.)	Enable rapid response when a security event occurs by sending an alert	Provide a function for sending an alert when a security event occurs (e.g., authentication failure, expired certificate)	Check that the system operates according to specifications		

No.		Primitive					Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Comm
		S	A	C	E	D							
I	1	○	○		○	○	User management	Account lockout mechanism	Prevent improper operation of the device by a third party	Provide a function for locking the account and preventing login when evidence of multiple consecutive login failures beyond a designated number of times, multiple logins, or other suspicious activities are	Check available account lockout settings, and check that the account is locked as configured		
	2		○		○	○		Option to force-expire accounts not used for a certain period of time	Prevent login from accounts not used for a certain period of time	Provide a function for locking an account that has elapsed a set expiration period	Check that accounts expire at the end of the expiration period		
	3		○		○	○		Function for ensuring password strength	Prevent unauthorized login by brute force, dictionary, and other attacks	Provide a function for allowing only passwords that meet certain conditions, such as the use of multiple character types and minimum password length, to be registered	Check that passwords that do not meet the required conditions cannot be registered		
	4		○		○	○		Password security options (two-factor authentication, etc.)	Make it difficult for a third party to log in to the system	Enable the use of password security options (e.g., two-factor authentication)	Check that password security options can be used		
	5		○		○	○		Permission management for accounts used to launch services and processes	Restrict permissions for launching services and processes by account, and keep the scope of impact when an incident occurs to within services and processes	Do not require a superuser when launching services and processes	Check that the system operates with a dedicated user for services and processes		
	6		○		○	○		Shared user account	Enable the assignment of appropriate permissions according to use	Provide an account management function	Check that a shared account is used with appropriate permissions and scope of sharing		
	7		○		○	○		Assignment of appropriate permissions to administrative users	Enable administrative users to use necessary permissions	Provide a function for managing permissions	Check that administrative users are assigned appropriate permissions		
	8		○		○	○		Function for assigning permissions to general users	Enable users to use only necessary permissions	Provide a function for assigning permissions to users	Check that permissions can be assigned to users, and the system can be used according to permissions		
	9		○		○	○		Authorization control function	Enable the assignment of access rights according to roles	Provide a function for assigning access rights according to the role of an account	Check that information and functions that are not authorized cannot be used		
	10		○		○	○		Service linkage	Ensure login information is not relayed to other services more than necessary	Provide a function for indicating to the user the information relayed to other services when linking those services	Check what information is relayed to other services		

No.		Primitive					Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Comm
		S	A	C	E	D							
II	1				○	○	Software management	Web application firewall	Enable the use of web application firewalls	Enable web application firewalls	Check that web application firewalls can be used		
	2		○		○	○		Firewall function included with the product	Use the firewall function included with the product to increase security	Enable the firewall function included with the product	Check that the firewall function included with the product can be used		
	3		○		○	○		Software version	Use the software version that addresses vulnerabilities, bugs, and other issues to ensure security	Provide a function for updating the software and a function for checking the version	Check that the software can be updated and the version can be checked		
	4		○		○	○		Anti-virus function	Use the anti-virus function included with the product to increase security	Enable the use of the anti-virus function included with the product	Check that the anti-virus function included with the product can be used		
	5		○		○	○		Improper data processing	Prevent unintended system operations	Provide a function for restricting data to be accepted	-		
	6		○	○	○	○		Data traffic	Take DDoS and other attacks into consideration in designing the amount of data traffic handled by the system	Provide a function for restricting the amount of data traffic to be accepted, or other similar functions	Check the amount of data traffic to be accepted		

No.		Primitive					Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Comment
		S	A	C	E	D							
III	1		○		○	○	Security management	Log management function	Save logs so that the situation can be assessed in the event of an incident or otherwise when needed	Provide a log management function for recording events that occurred against the system	Check that log information can be accessed		
	2		○		○	○		Session management (Cookie settings)	When the system uses cookies, provide appropriate attributes	Set the Secure and HttpOnly attributes to the appropriate values of cookies	Check that the Secure and HttpOnly attributes are set to the appropriate values of cookies		
	3		○		○	○		Session management (URL rewriting)	Ensure session IDs are not leaked due to unnecessary URL rewriting	Check whether URL rewriting is necessary	Check that session IDs are not embedded in URLs		
	4		○		○	○		Session management (Issuance of session ID when logging in and processing important confirmation)	Reduce the risk of confidential information getting stolen through the theft of session information	A new session ID should be issued when logging in and after processing important confirmation, and the old session ID should be discarded	Check that session IDs differ before and after logging in and processing important confirmation		
	5		○		○	○		Security measures against client data manipulation	Prevent the data of other accounts from being viewed and manipulated	Provide a data management function for each account	Check that the data of other accounts cannot be viewed and manipulated		
	6		○		○	○		Security measures against system data manipulation	Allow system data to be viewed and manipulated only by limited users	Provide a function that enables only designated system administrators to view and manipulate system data	Check that users other than designated system administrators cannot view and manipulate system data		
	7				○	○		Cloud interface and network vulnerabilities (API interface, cloud-based web interface, etc.)	Check that no known cloud interface and network vulnerabilities exist in the system	Check publicly available vulnerability information, and provide a function for indicating the services being used to the user	Check publicly available vulnerability information		
	8				○	○		Vulnerability of XSS, SQLi, and CSRF	Check that no known vulnerability of XSS, SQLi, CSRF, etc. exists in the system being used	Practice secure coding, and avoid including any vulnerability of XSS, SQLi, CSRF, etc.	Check publicly available vulnerability information		
	9				○	○		Web application SSL certificate	Implement an SSL certificate in a manner suited to one's own system	Provide a certificate suited to the system (e.g., EV certificate)	Check the certificate used		

No.		Primitive					Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Comment
		S	A	C	E	D							
IV	1		○		○	○	Access control	Access by uncontrolled physical means	Prevent system access by uncontrolled physical means	Provide a function for enabling restriction of physical means (USB, etc.) to access the system according to use	Check that access by uncontrolled physical means is restricted		
	2		○		○	○		Default ports for remote access	Prevent attacks targeting default ports for remote access functions	Provide a function for changing default ports	Check that default ports can be changed		
	3		○	○	○	○		Wireless communication security (encryption method)	Use a secure encryption method to prevent the stealing of communicated content using vulnerabilities	Enable the use of secure encryption methods	Check that a secure encryption method is selected upon connection		
	4		○	○	○	○		Wireless communication security (WPS)	Prevent compromising security due to errors in wireless settings	Consider security when providing a WPS function (e.g., MAC address filtering)	Check that WPS functions properly		

No.		Primitive					Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Comme
		S	A	C	E	D							
V	1		○		○	○	Unauthorized connection	Restriction of network ports	Make only appropriate ports available according to the anticipated use	Provide a function for opening or closing ports according to the purpose of use	Check that ports are opened or closed as configured		
	2		○		○	○		UPnP	Make UPnP available on devices anticipated to be used	Provide a function for enabling and disabling UPnP	Check that the device behaves as configured when connected		

No.		Primitive					Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Comment
		S	A	C	E	D							
VI	1		○	○	○	○	Encryption	Data encryption function	Prevent sending data in plain text and allowing communications to be eavesdropped	Provide a function for encrypting individual data	Check that a data encryption function is available		
	2		○	○	○	○		Communication encryption function	Prevent sending data in plain text and allowing communications to be eavesdropped	Provide a function for performing encrypted communication using SSL/TLS, etc. between the devices that make up the system	Check that encrypted communication can be used		
	3		○	○	○	○		Encryption method	Enable checking the encryption method used	Provide a function for checking the encryption method used	Check the encryption method used		
	4		○	○	○	○		Certificate update function	Ensure certificates do not expire	Provide a function for updating certificates	Check that certificates are valid		

No.		Primitive					Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Comment
		S	A	C	E	D							
VII	1	○					System settings	Function for checking the status of sensor operation	Enable checking the status of operation	Provide a function for checking or notifying the current status of sensor operation	Check the status of sensor operation		
	2		○		○	○		Log security management	Prevent logs from being accessed or falsified by a third party	Provide a function for specifying users who can access logs and preventing falsification of their content	Check that users without access permissions cannot access logs, and that users who can access logs cannot modify them		

No.		Primitive					Category	Item	Purpose of this item	To be checked by developers	To be checked by users	Result	Commer
		S	A	C	E	D							
VIII	1	○					Notification	Alert and notification function for security events (irregular state, etc.)	Enable rapid response when a security event occurs by sending an alert	Provide a function for sending an alert when a security event occurs (e.g., irregular state)	Check that the system operates according to specifications		
	2		○		○	○		Alert and notification function for security events (authentication failure, expired certificate, etc.)	Enable rapid response when a security event occurs by sending an alert	Provide a function for sending an alert when a security event occurs (e.g., authentication failure, expired certificate)	Check that the system operates according to specifications		

Primitive (basic constituent unit of an IoT system) component

Sensor	A function or device for measuring temperatures, acceleration, weight, sound, positions, etc.
Aggregator	A function or device for aggregating data captured by sensors
Communication Channel	A communication path or network for sending and receiving data
eUtility	An interface for viewing data and configuring settings
Decision Trigger	A function for calculating data and triggering an action based on the result

JPCERT Coordination Center

電子署名者 : JPCERT Coordination Center
DN : c=JP, st=Tokyo, l=Chuo-ku, o=Japan Computer Emergency Response Team Coordination Center, cn=JPCERT Coordination Center, email=office@jpcert.or.jp
日付 : 2020.11.04 16:50:03 +09'00'