IoT Security Checklist Illustration Diagram

JPCERT Coordination Center

June 27, 2019

JPCERT CC®

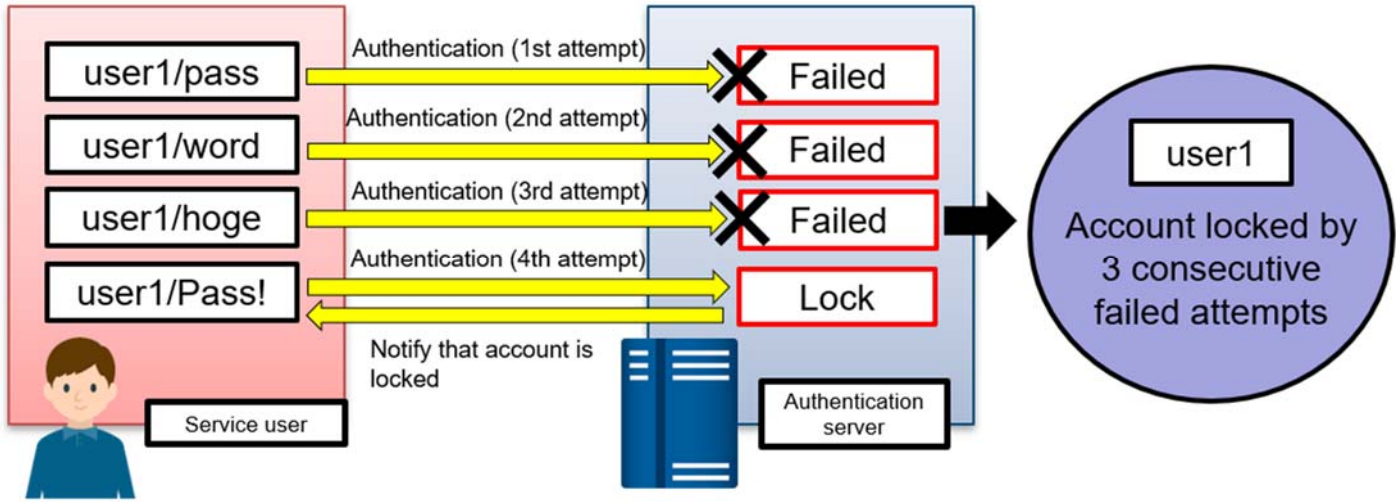
Contents

JPCERT CC®

No. I-1 User management: Account lockout mechanism

Purpose of this item: Prevent improper operation of the device by a third party

Scope: Sensor, Aggregator, eUtility, Decision Trigger



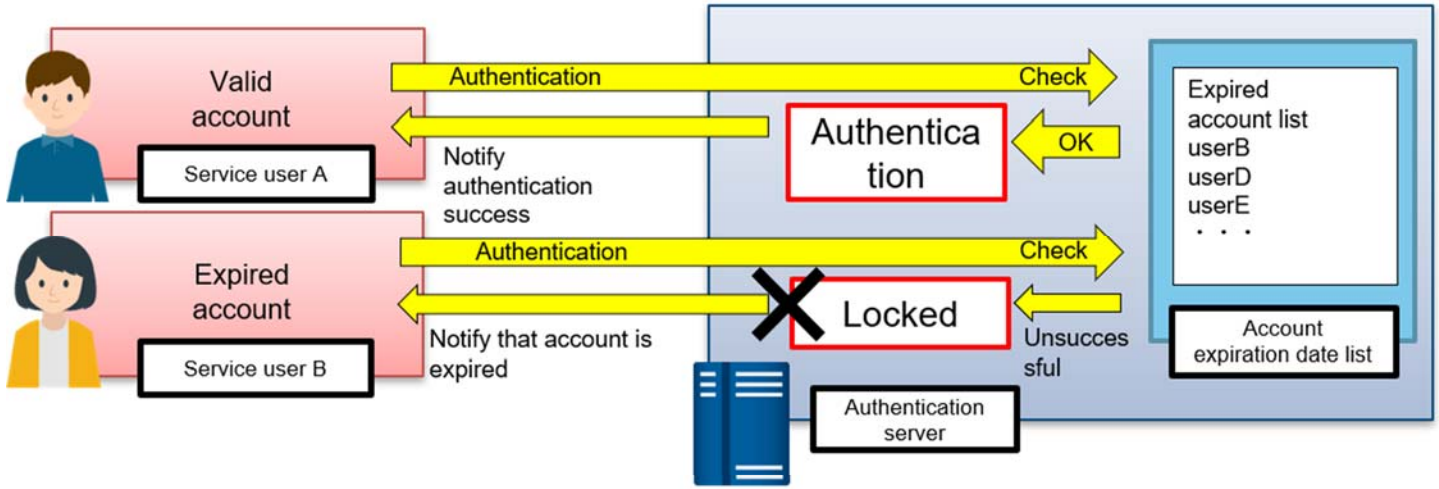
User:
Check available account lockout settings, and check that the account is locked as configured

Developer:
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 found

No. I-2 User management: Option to force-expire accounts not used for a certain period of time

Purpose of this item: Prevent login from accounts not used for a certain period of time

Scope: Aggregator, eUtility, Decision Trigger



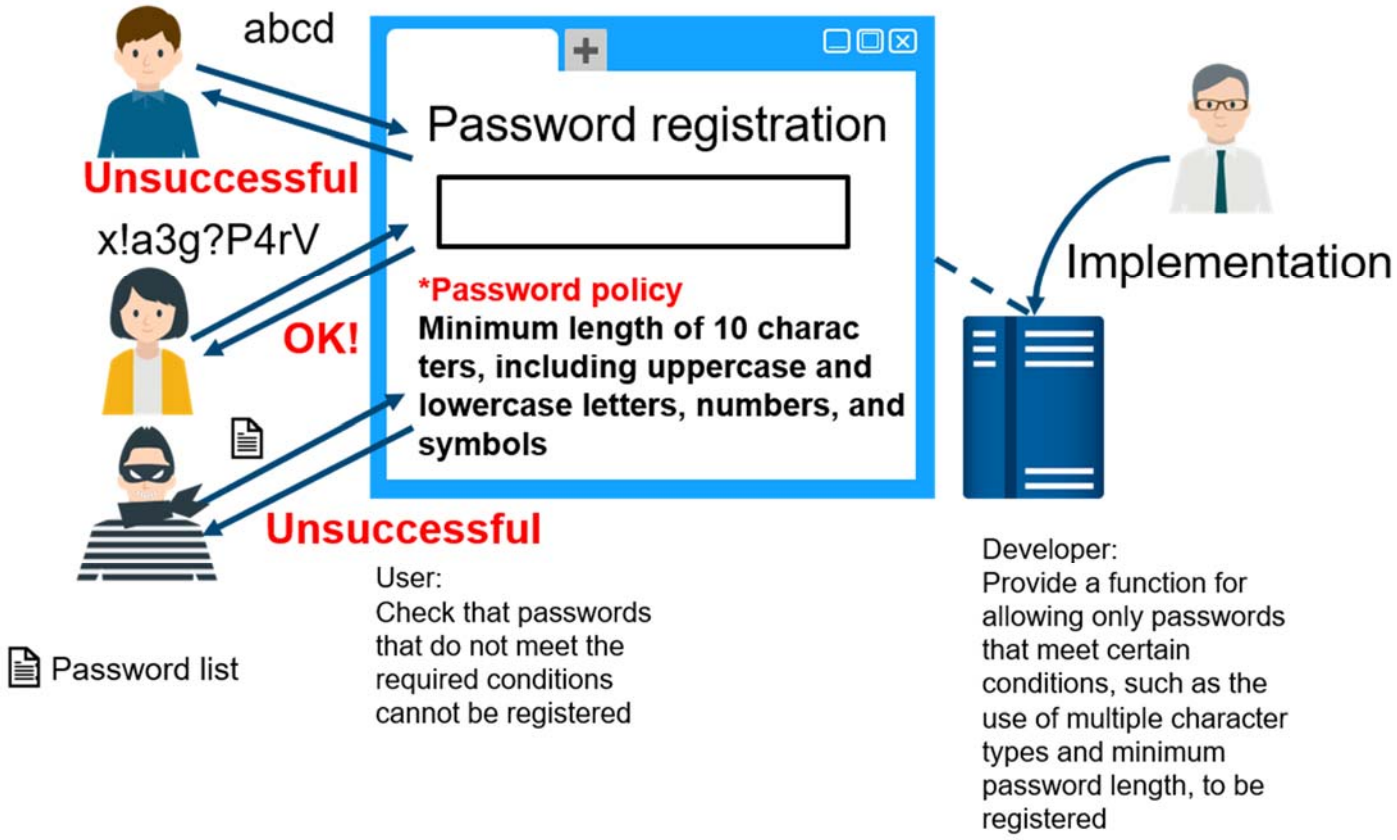
User:
Check that accounts expire at the end of the expiration period

Developer:
Provide a function for locking an account that has elapsed a set expiration period

No. I-3 User management: Function for ensuring password strength

Purpose of this item: Prevent unauthorized login by brute force, dictionary, and other attacks

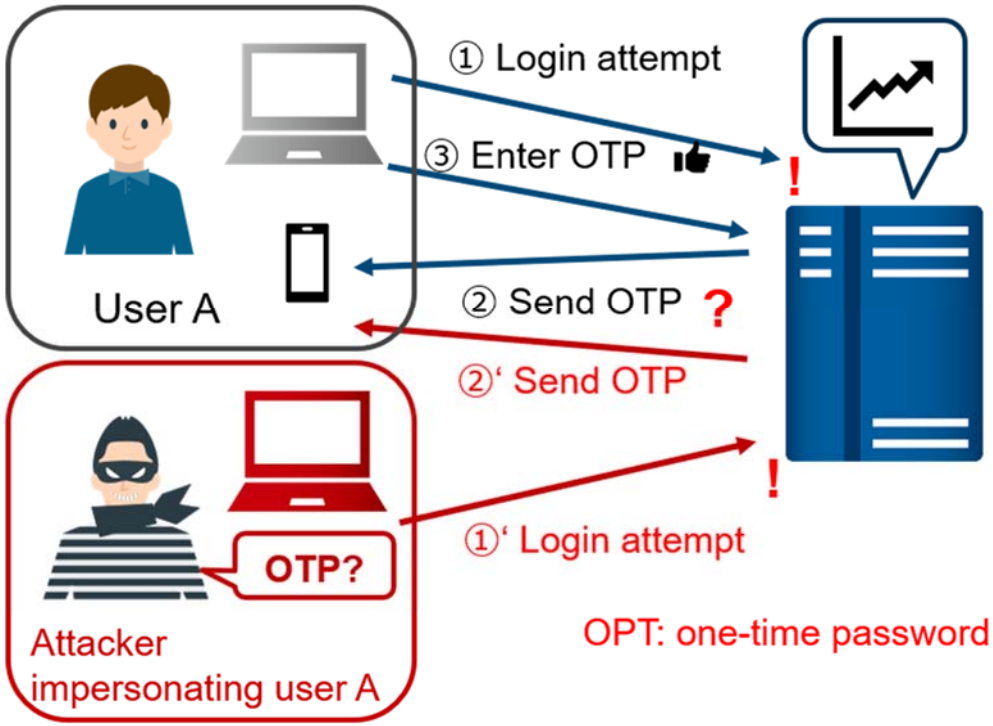
Scope: Aggregator, eUtility, Decision Trigger



No. I-4 User management: Password security options (two-factor authentication, etc.)

Purpose of this item: Make it difficult for a third party to log in to the system

Scope: Aggregator, eUtility, Decision Trigger



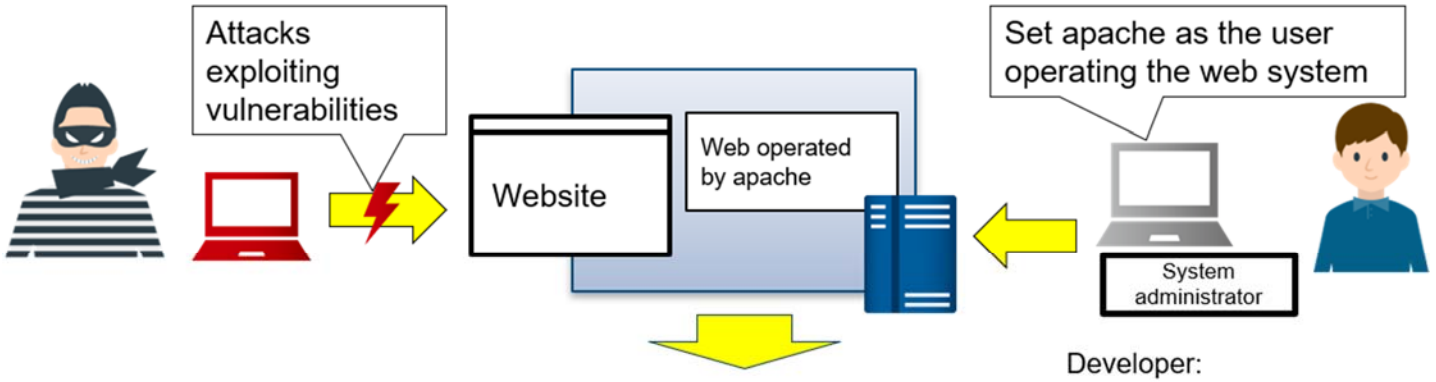
User:
Check that password security options can be used

Developer:
Enable the use of password security options (e.g., two-factor authentication)

No. I-5 User management: Permission management for accounts used to launch services and processes

Purpose of this item: Restrict permissions for launching services and processes by account, and keep the scope of impact when an incident occurs to within services and processes

Scope: Aggregator, eUtility, Decision Trigger



Even if an attack is successful, the scope of impact is limited to areas apache has control over *May vary depending on vulnerabilities

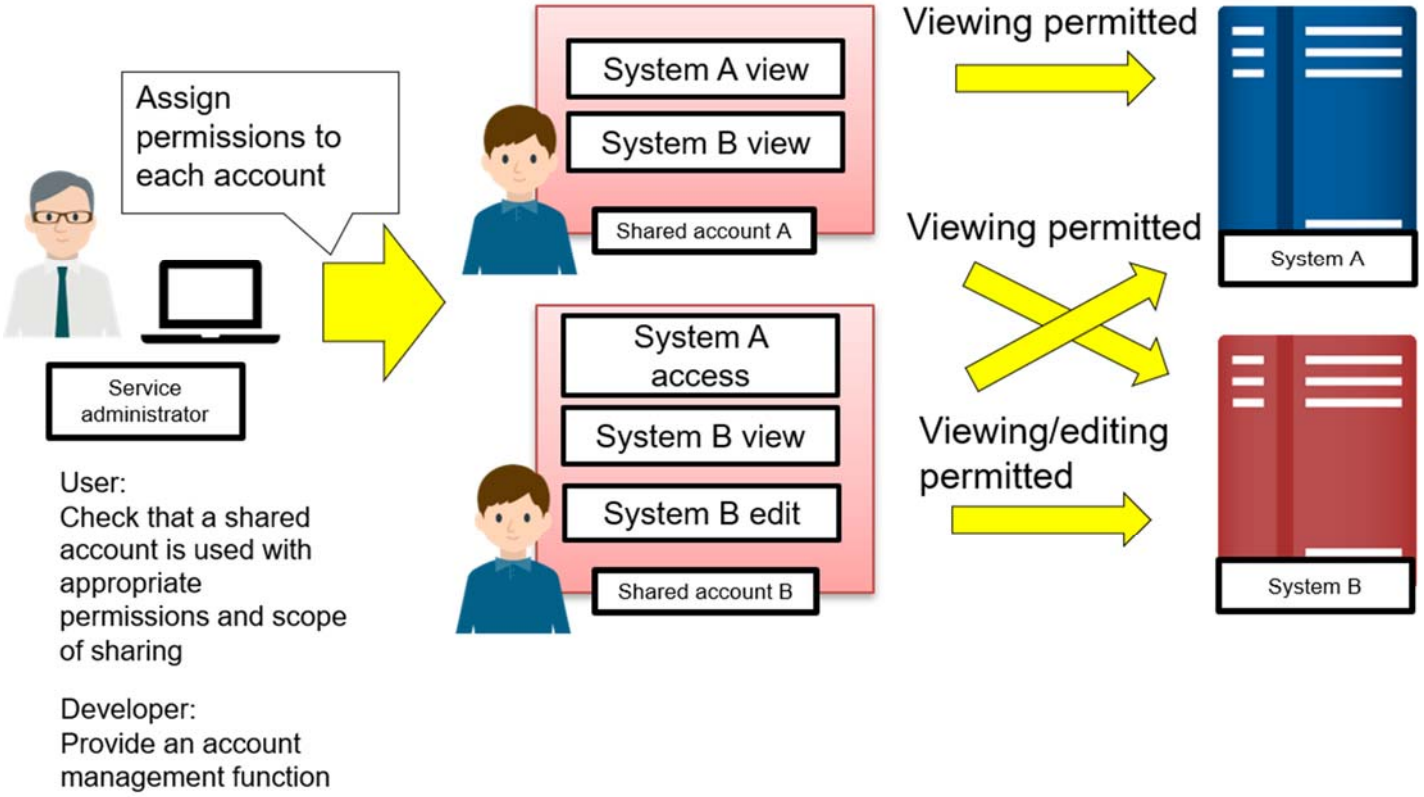
Developer:
Do not require a superuser when launching services and processes

User:
Check that the system operates with a dedicated user for services and processes

No. I-6 User management: Shared user account

Purpose of this item: Enable the assignment of appropriate permissions according to use

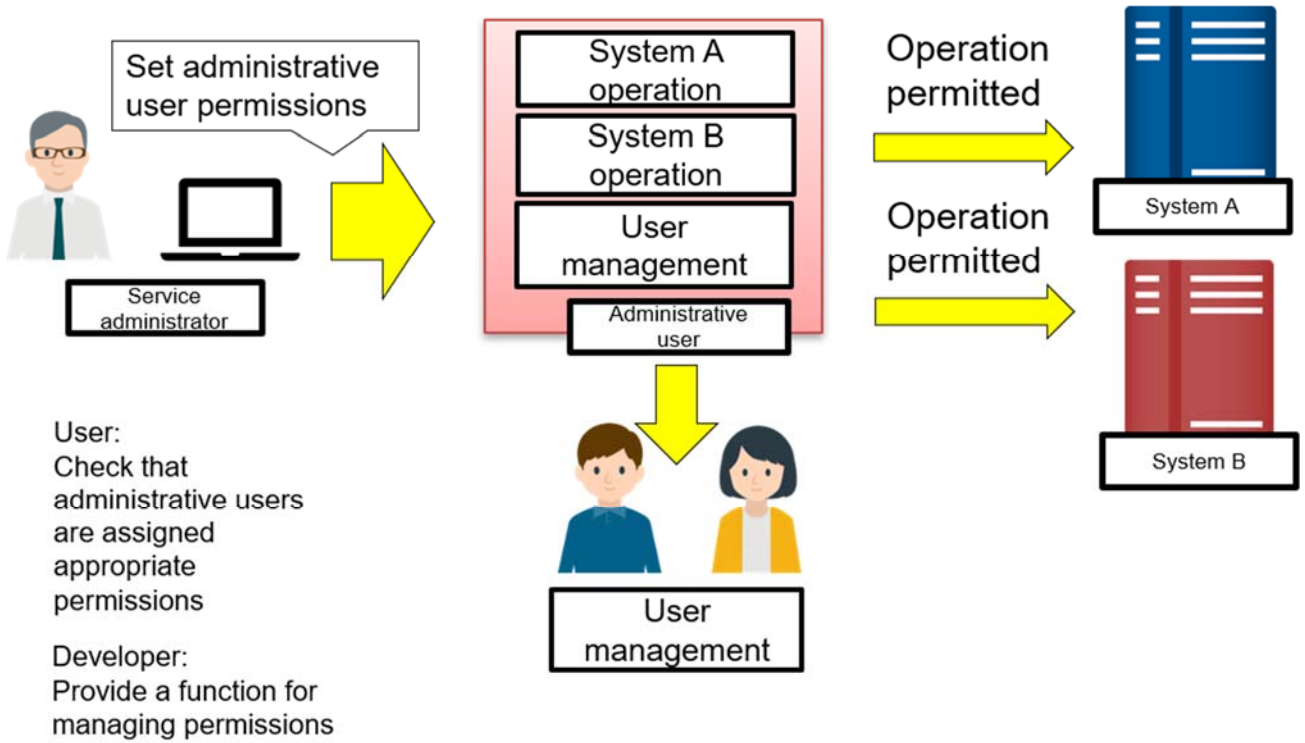
Scope: Aggregator, eUtility, Decision Trigger



No. I-7 User management: Assignment of appropriate permissions to administrative users

Purpose of this item: Enable administrative users to use necessary permissions

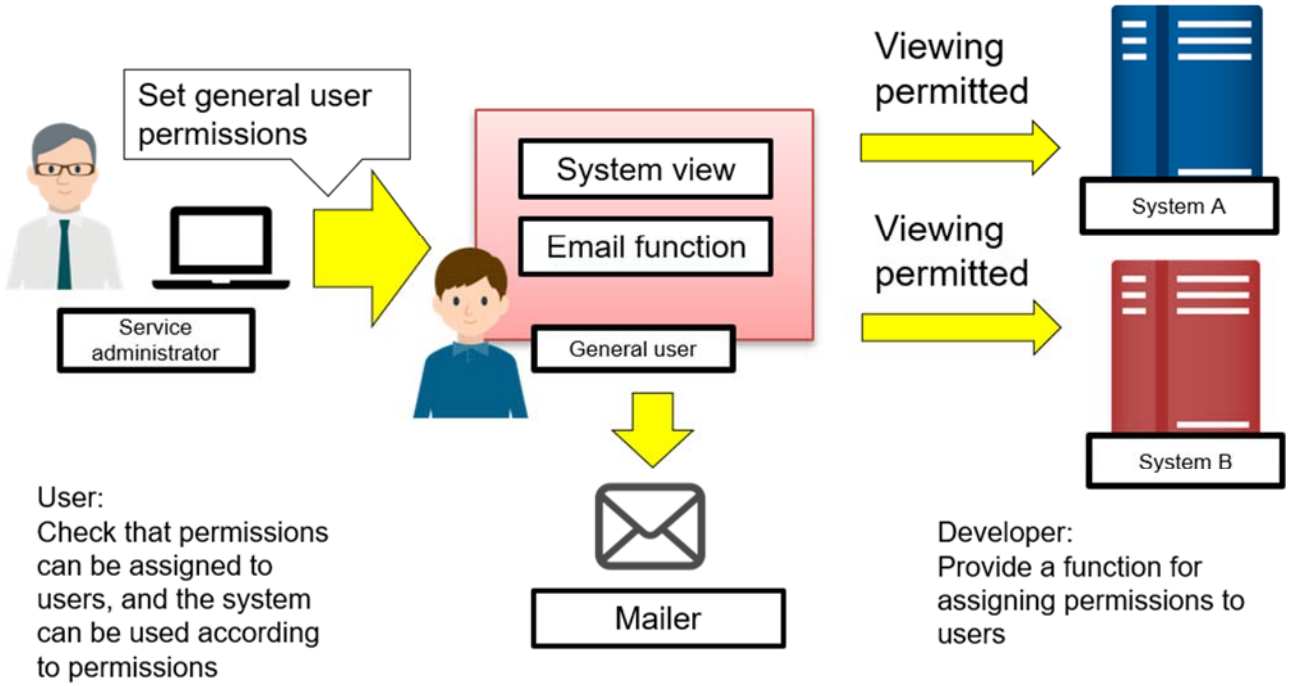
Scope: Aggregator, eUtility, Decision Trigger



No. I-8 User management: Function for assigning permissions to general users

Purpose of this item: Enable users to use only necessary permissions

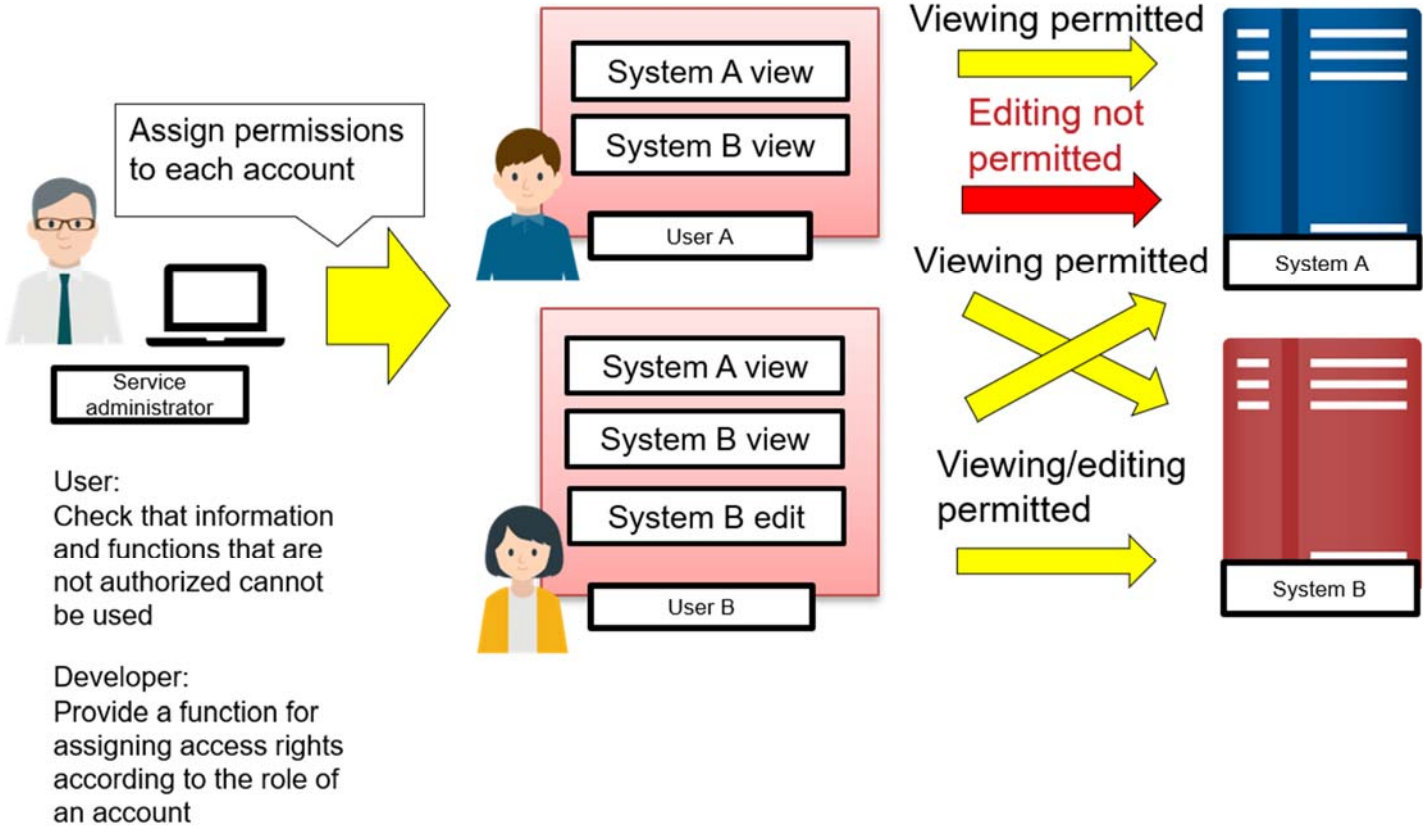
Scope: Aggregator, eUtility, Decision Trigger



No. I-9 User management: Authorization control function

Purpose of this item: Enable the assignment of access rights according to roles

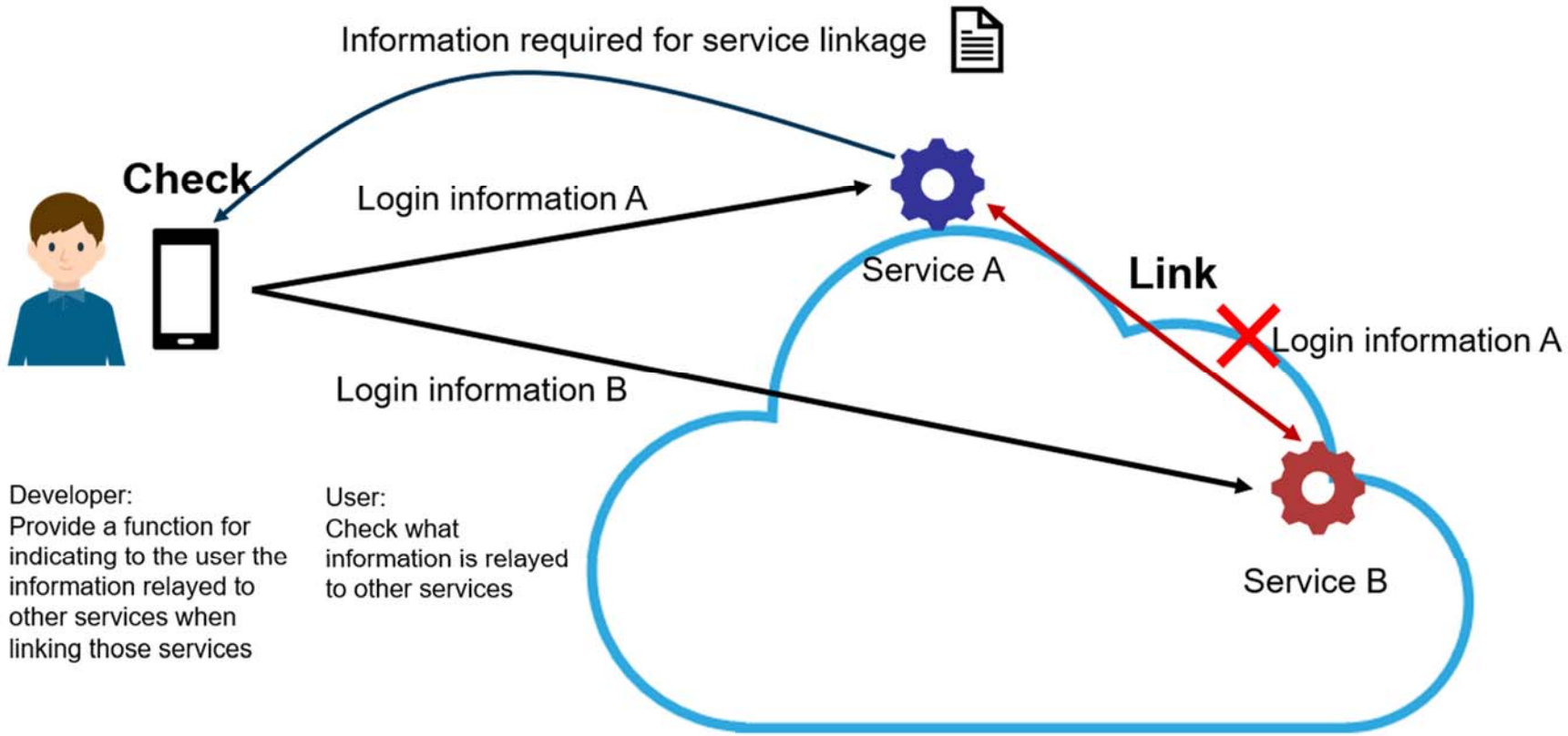
Scope: Aggregator, eUtility, Decision Trigger



No. I-10 User management: Service linkage

Purpose of this item: Ensure login information is not relayed to other services more than necessary

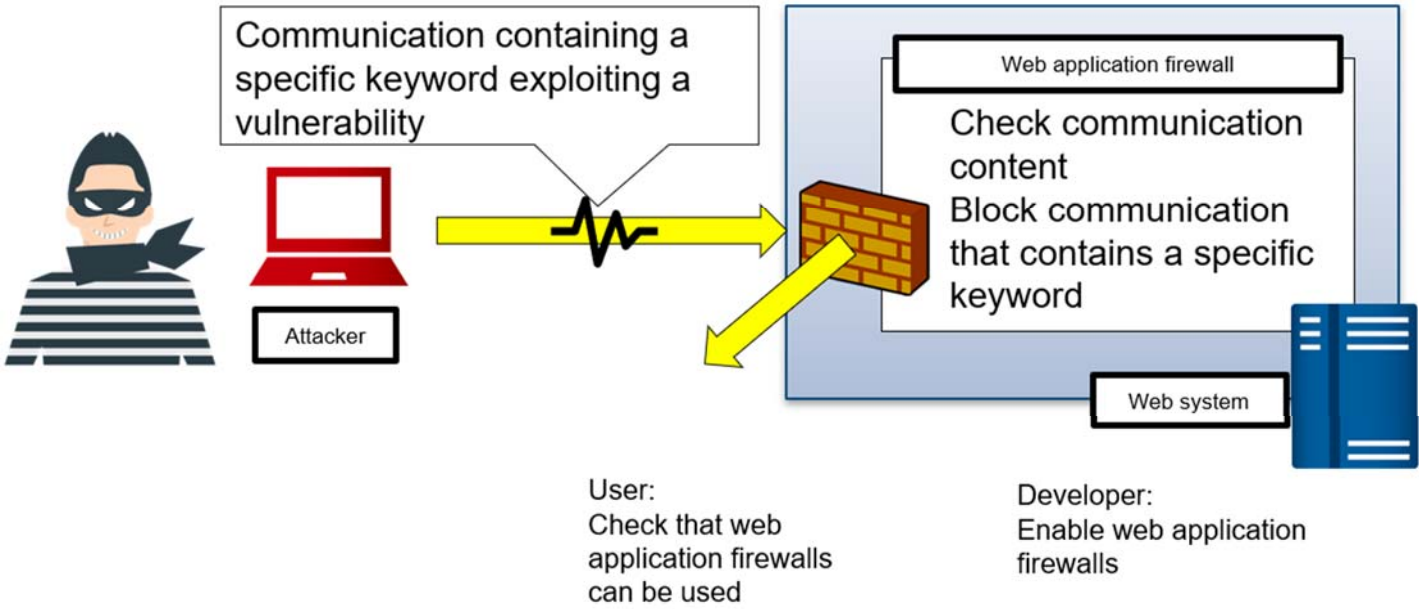
Scope: Aggregator, eUtility, Decision Trigger



No. II-1 Software management: Web application firewall

Purpose of this item: Enable the use of web application firewalls

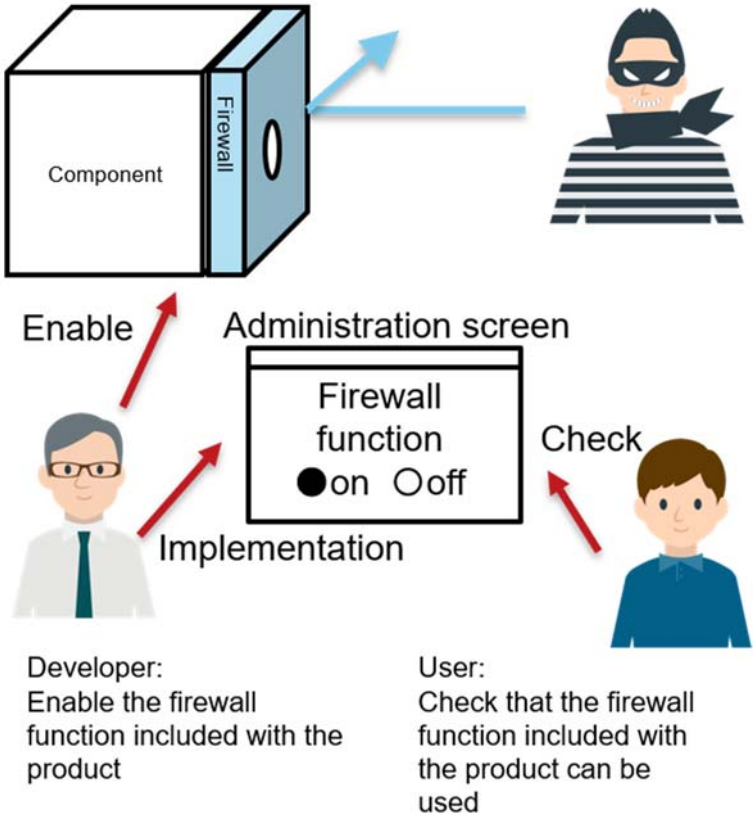
Scope: eUtility, Decision Trigger



No. II-2 Software management: Firewall function included with the product

Purpose of this item: Use the firewall function included with the product to increase security

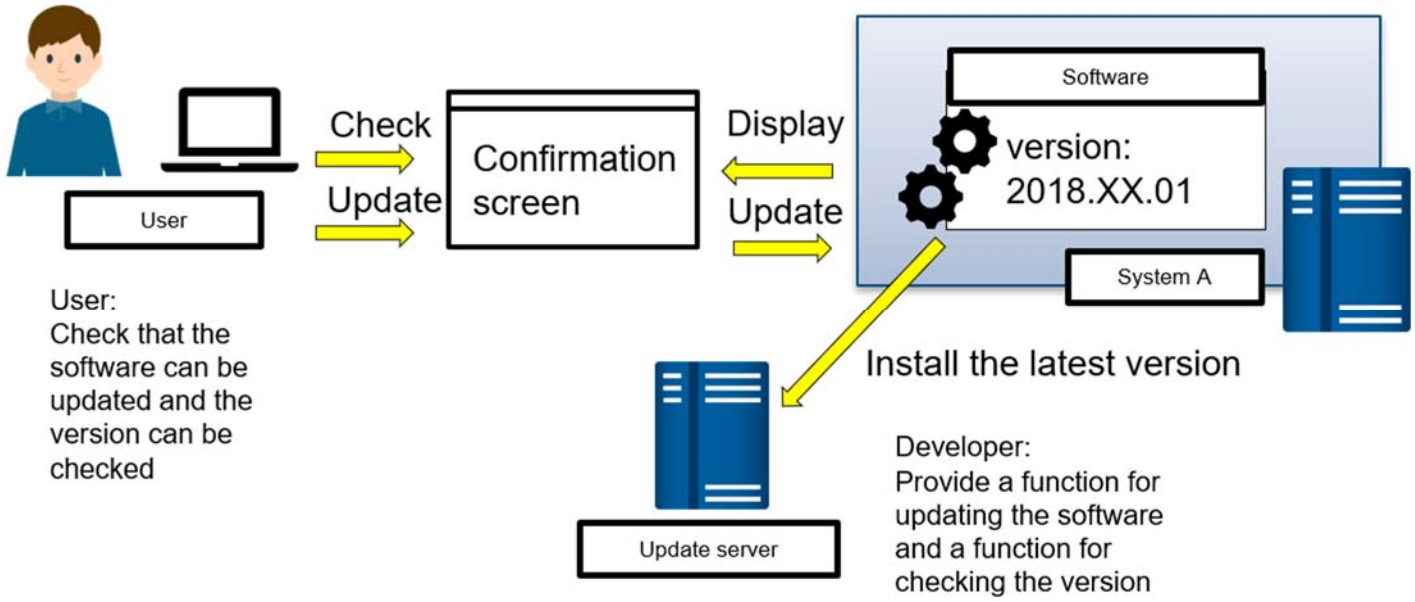
Scope: Aggregator, eUtility, Decision Trigger



No. II-3 Software management: Software version

Purpose of this item: Use the software version that addresses vulnerabilities, bugs, and other issues to ensure security

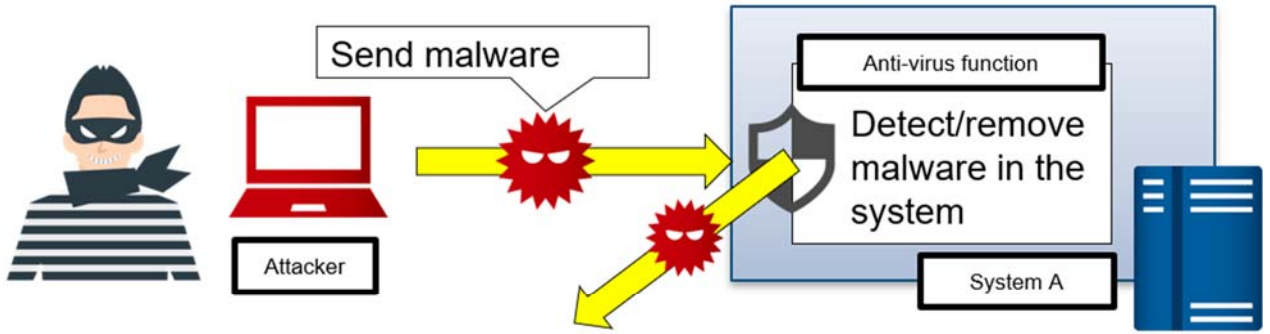
Scope: Aggregator, eUtility, Decision Trigger



No. II-4 Software management: Anti-virus function

Purpose of this item: Use the anti-virus function included with the product to increase security

Scope: Aggregator, eUtility, Decision Trigger



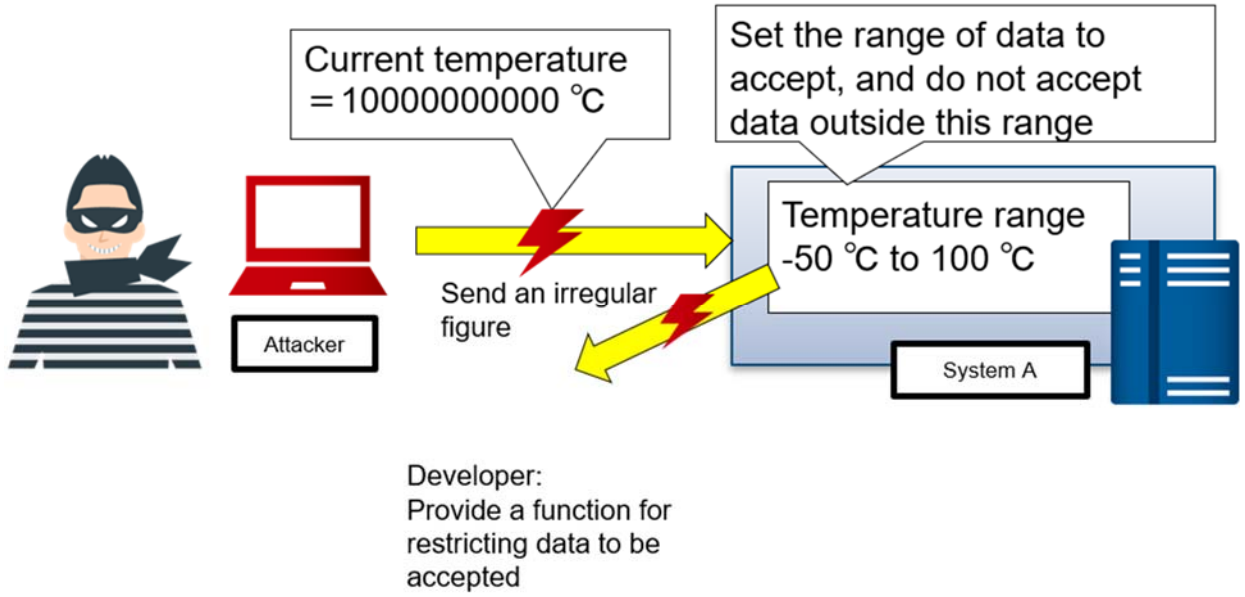
Developer:
Enable the use of the anti-virus function included with the product

User:
Check that the anti-virus function included with the product can be used

No. II-5 Software management: Improper data processing

Purpose of this item: Prevent unintended system operations

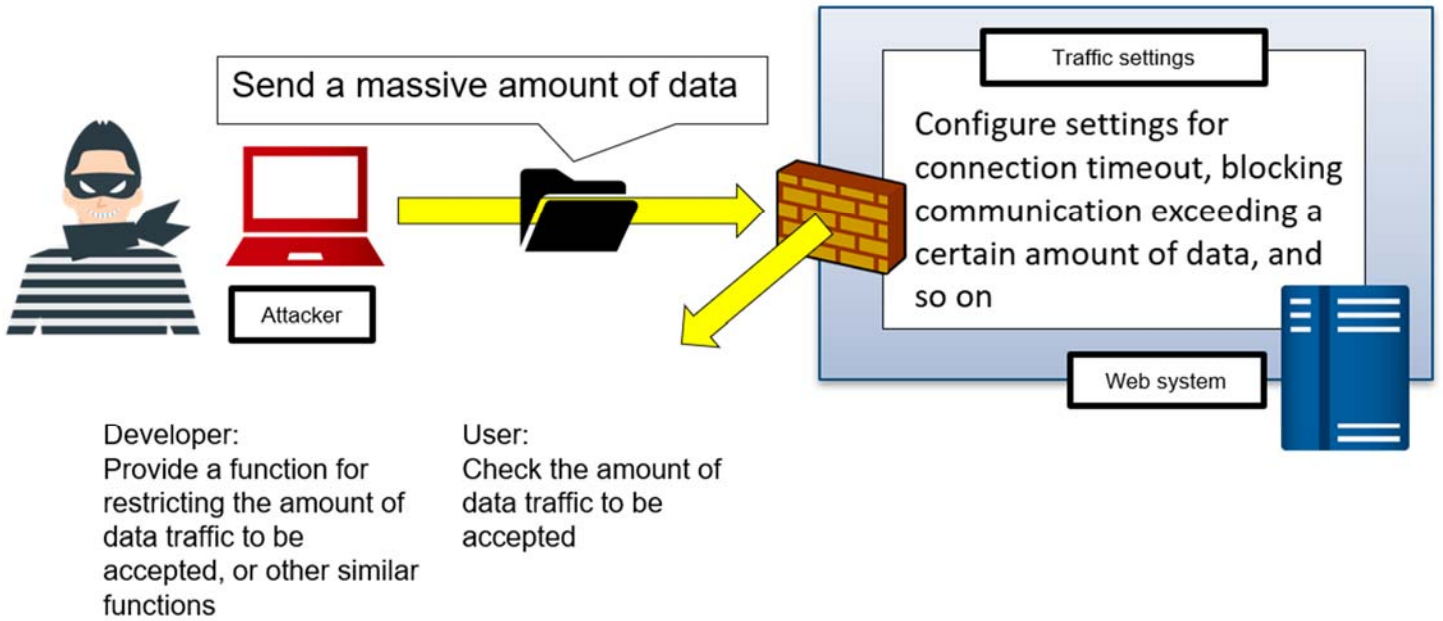
Scope: Aggregator, eUtility, Decision Trigger



No. II-6 Software management: Data traffic

Purpose of this item: Take DDoS and other attacks into consideration in designing the amount of data traffic handled by the system

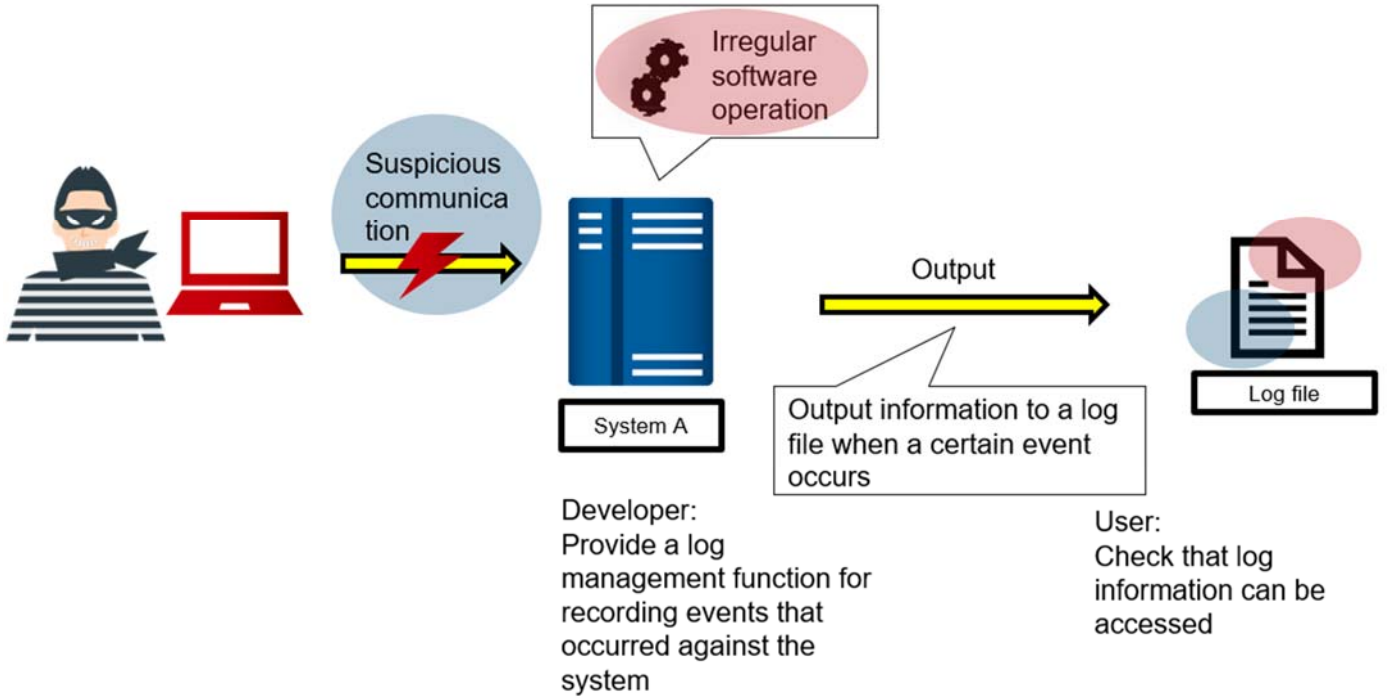
Scope: Aggregator, Communication Channel, eUtility, Decision Trigger



No. III-1 Security management: Log management function

Purpose of this item: Save logs so that the situation can be assessed in the event of an incident or otherwise when needed

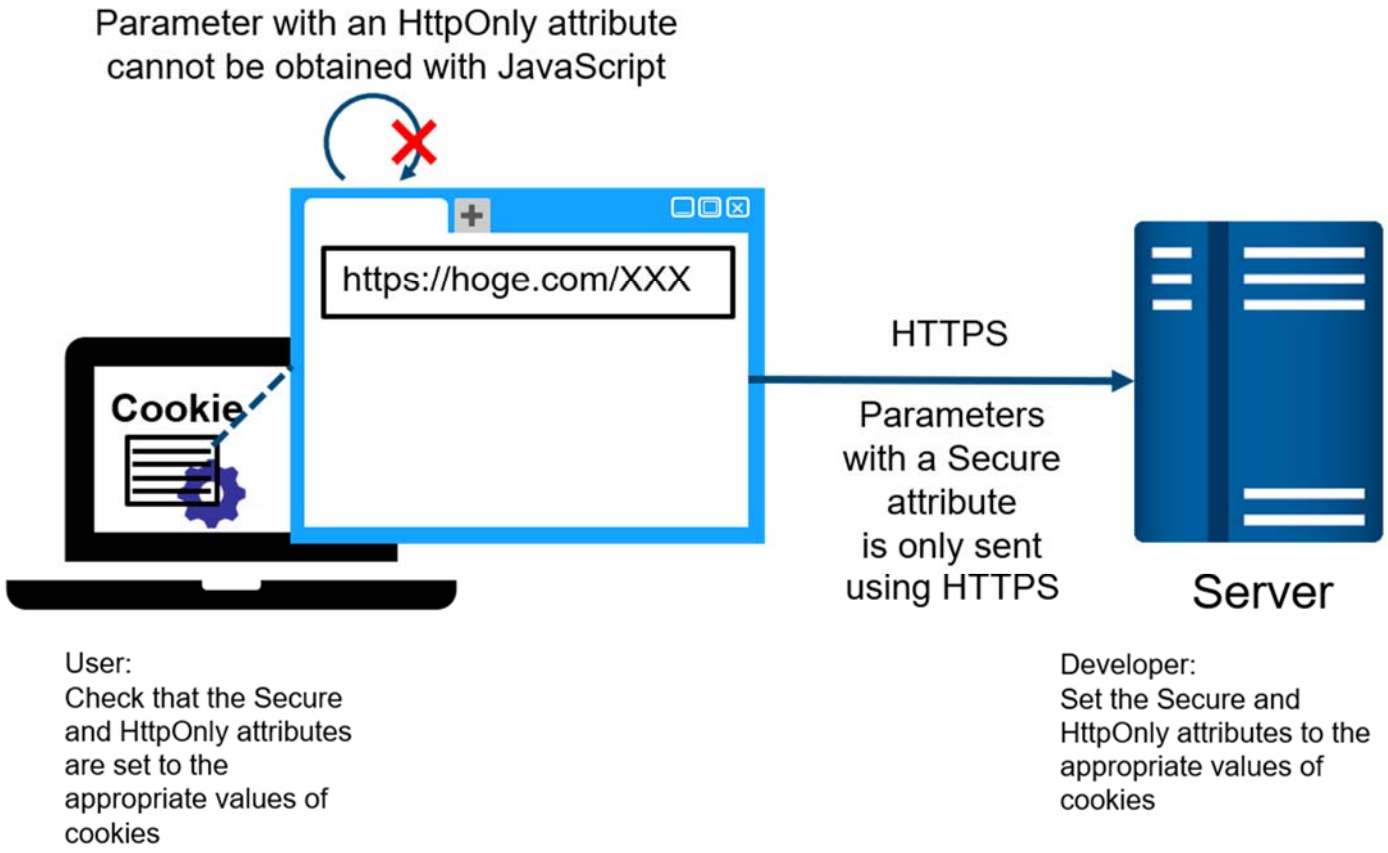
Scope: Aggregator, eUtility, Decision Trigger



No. III-2 Security management: Session management (Cookie settings)

Purpose of this item: When the system uses cookies, provide appropriate attributes

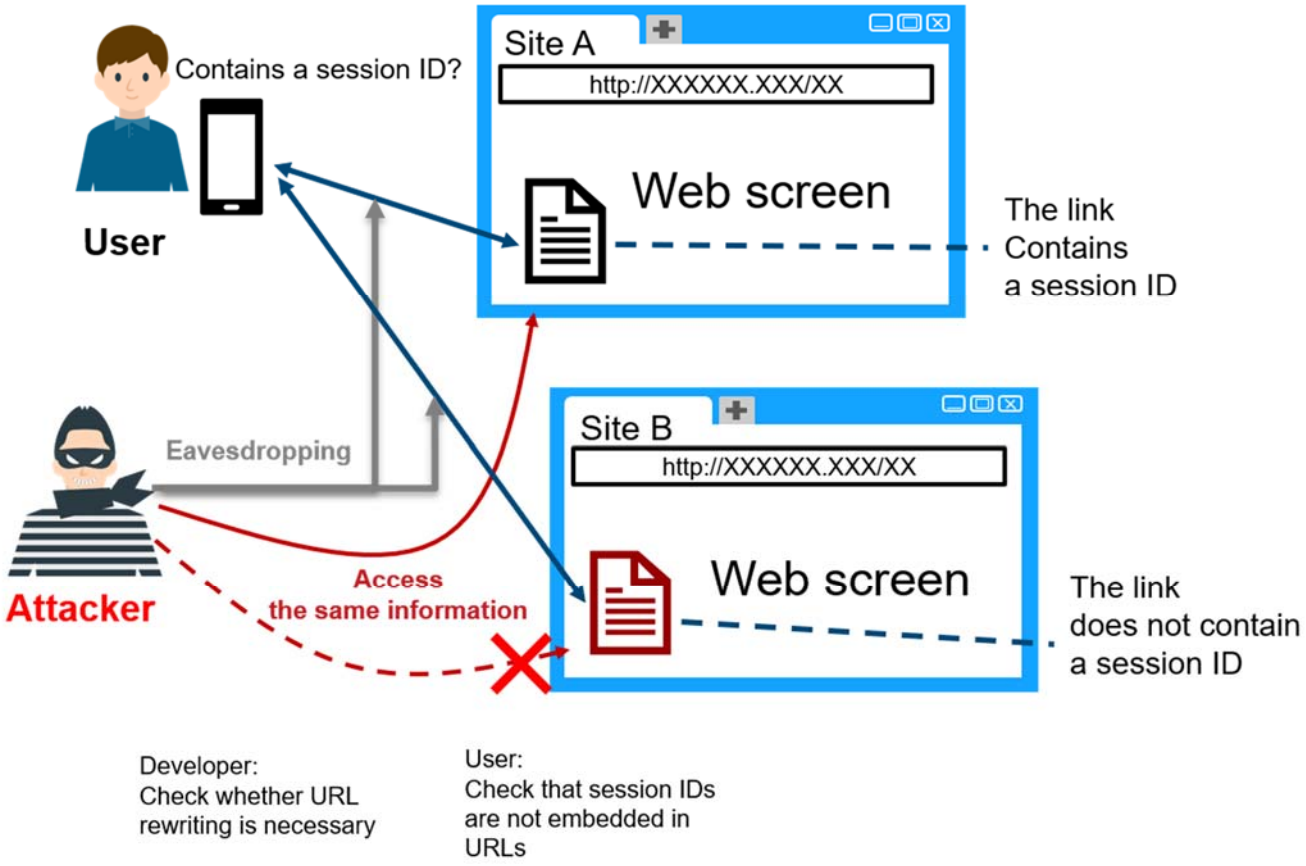
Scope: Aggregator, eUtility, Decision Trigger



No. III-3 Security management: Session management (URL rewriting)

Purpose of this item: Ensure session IDs are not leaked due to unnecessary URL rewriting

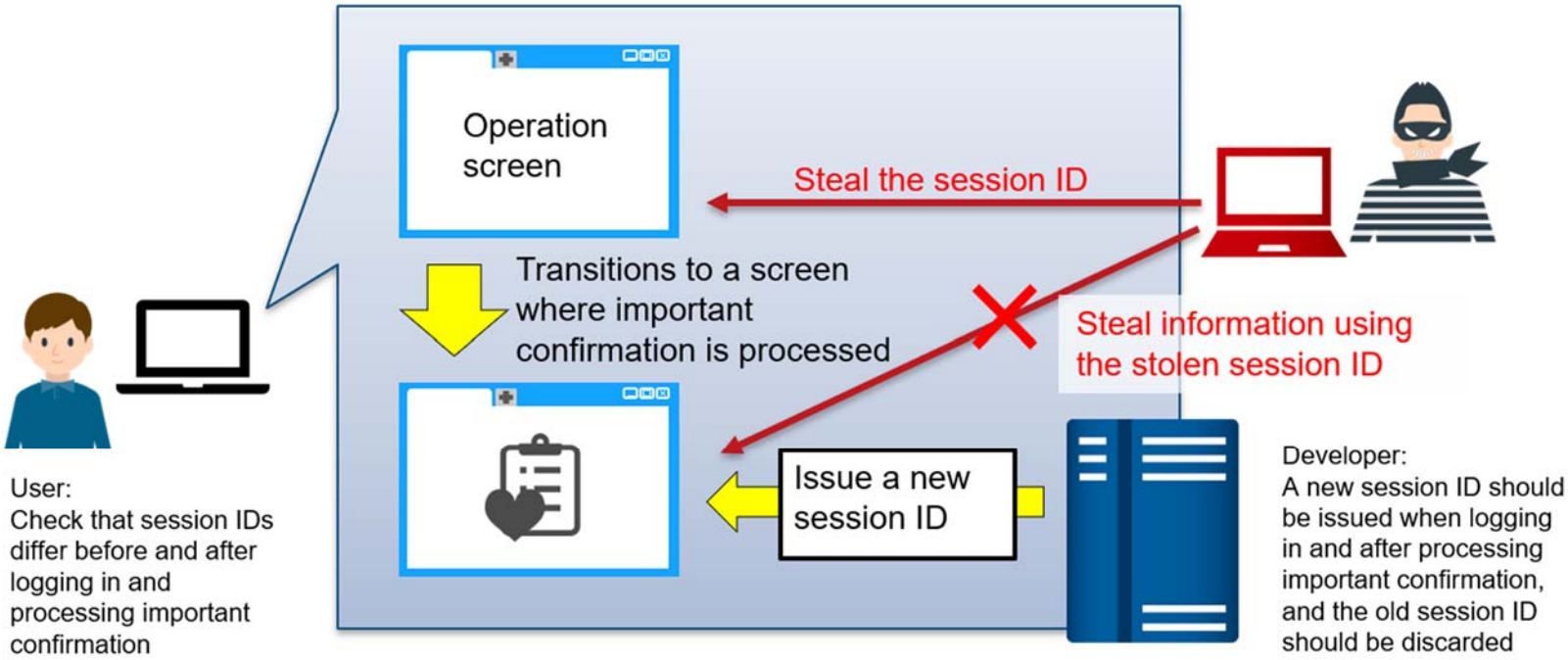
Scope: Aggregator, eUtility, Decision Trigger



No. III-4 Security management: Session management (Issuance of session ID when logging in and processing important confirmation)

Purpose of this item: Reduce the risk of confidential information getting stolen through the theft of session information

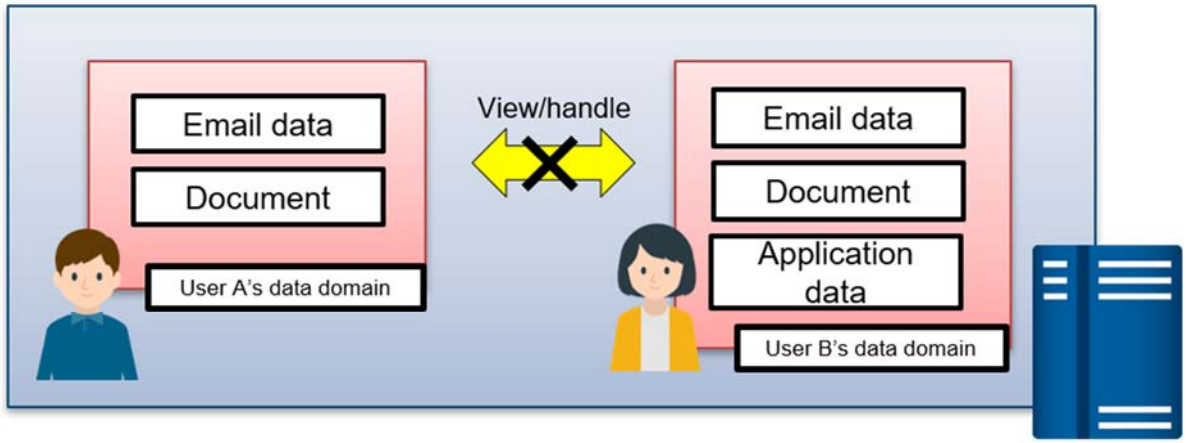
Scope: Aggregator, eUtility, Decision Trigger



No. III-5 Security management: Security measures against client data manipulation

Purpose of this item: Prevent the data of other accounts from being viewed and manipulated

Scope: Aggregator, eUtility, Decision Trigger



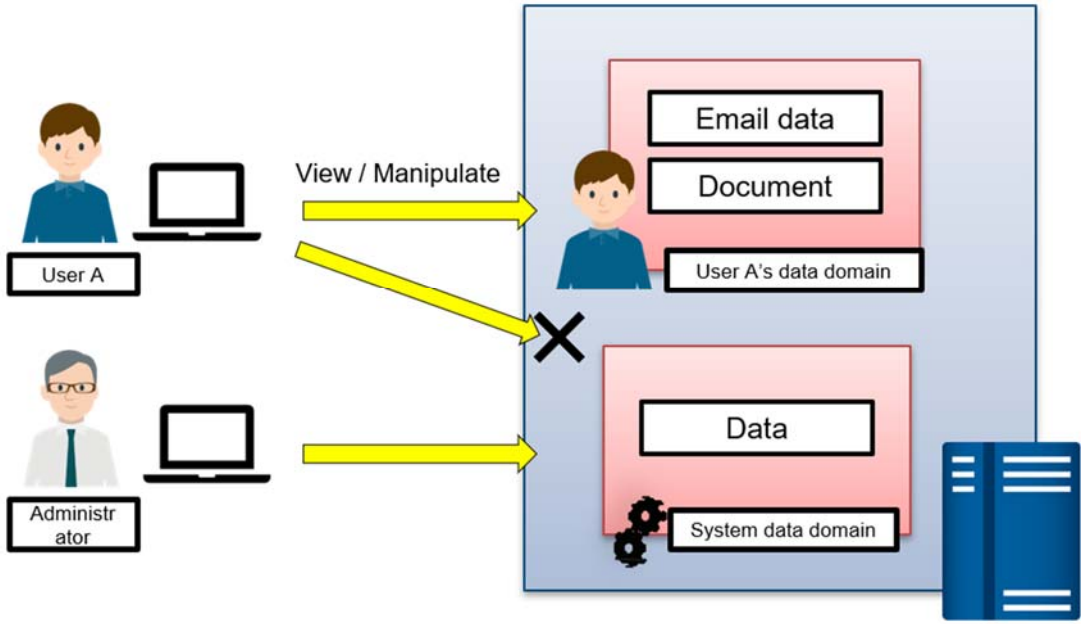
User:
Check that the data of other accounts cannot be viewed and manipulated

Developer:
Provide a data management function for each account

No. III-6 Security management: Security measures against system data manipulation

Purpose of this item: Allow system data to be viewed and manipulated only by limited users

Scope: Aggregator, eUtility, Decision Trigger



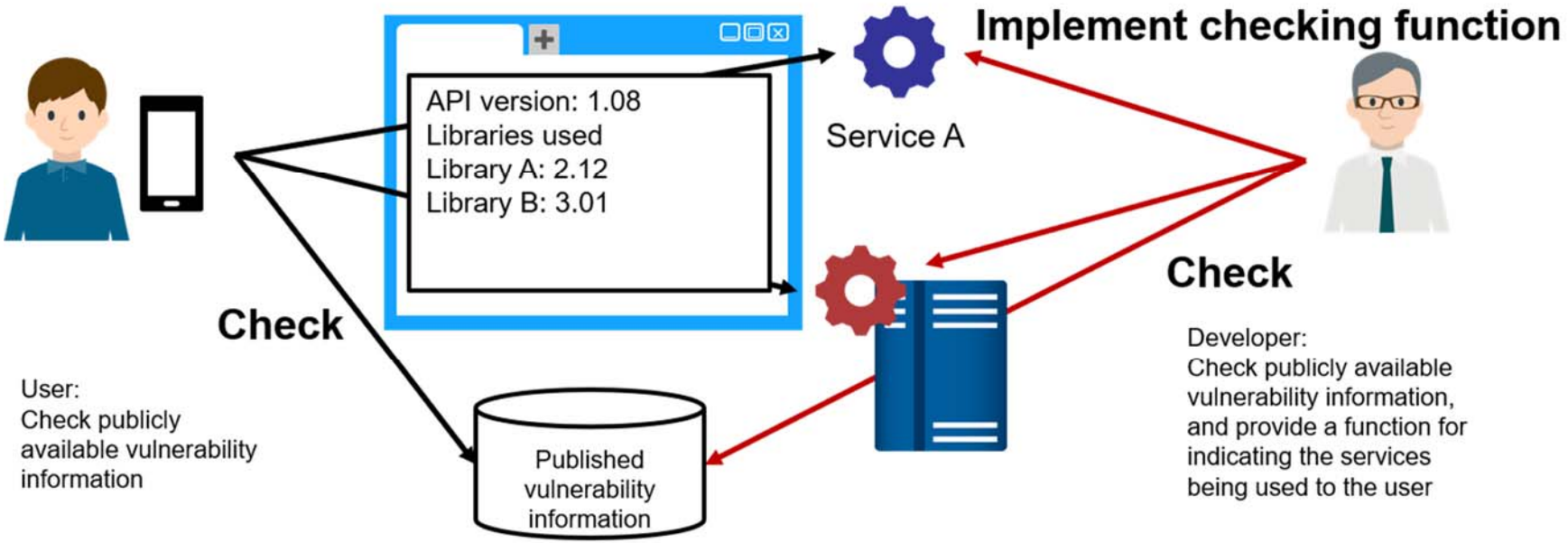
User:
Check that users other than designated system administrators cannot view and manipulate system data

Developer:
Provide a function that enables only designated system administrators to view and manipulate system data

No. III-7 Security management: Cloud interface and network vulnerabilities (API interface, cloud-based web interface, etc.)

Purpose of this item: Check that no known cloud interface and network vulnerabilities exist in the system

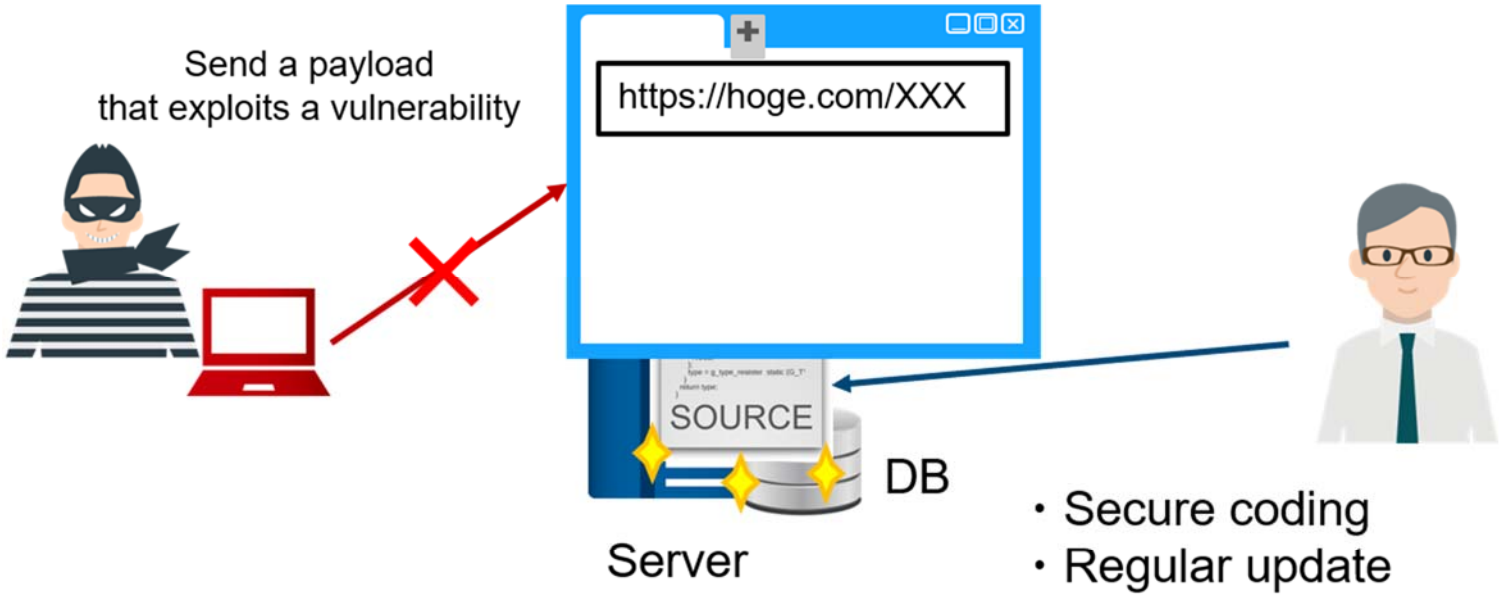
Scope: eUtility, Decision Trigger



No. III-8 Security management: Vulnerability of XSS, SQLi, and CSRF

Purpose of this item: Check that no known vulnerability of XSS, SQLi, CSRF, etc. exists in the system being used

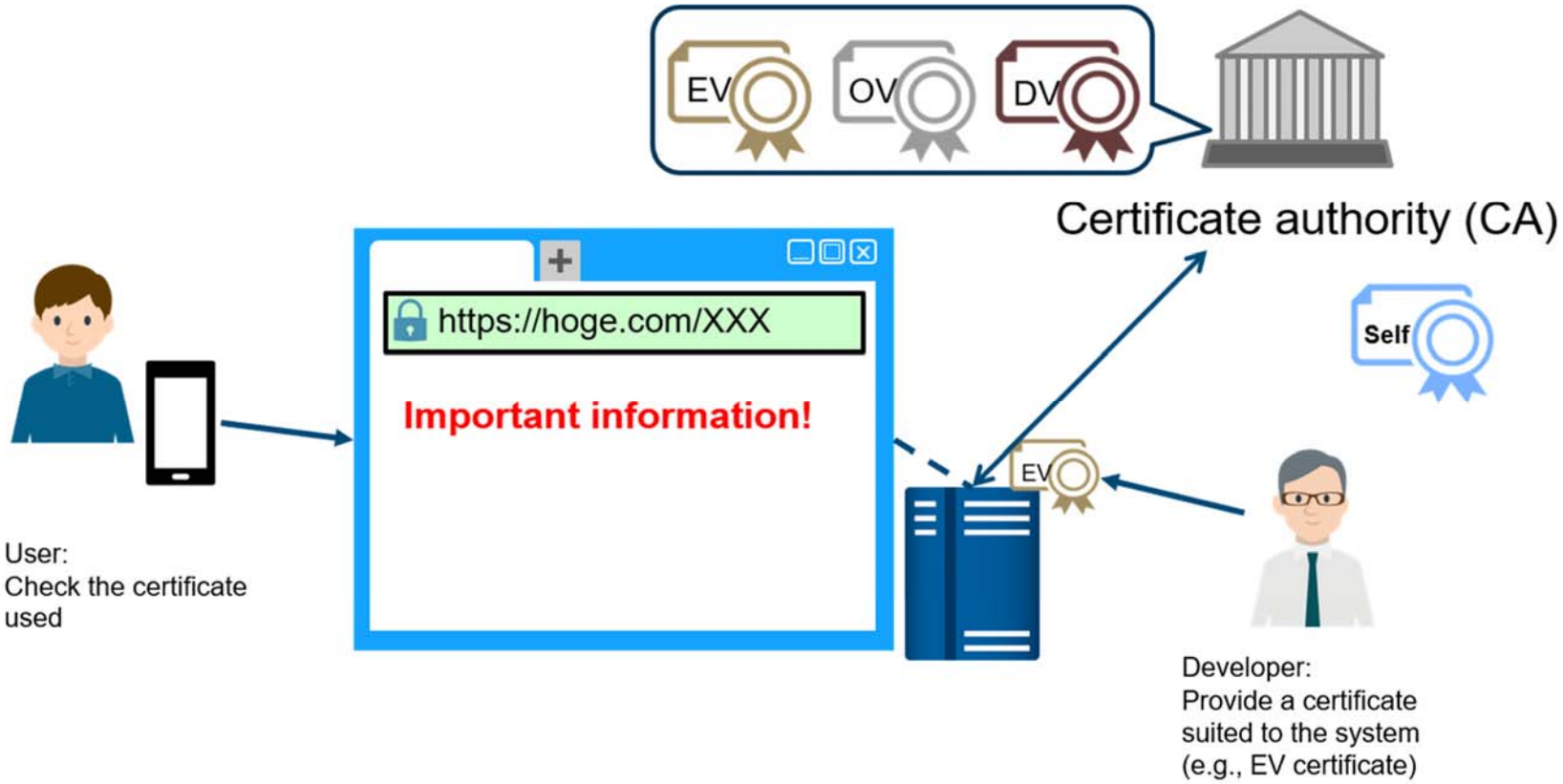
Scope: eUtility, Decision Trigger



No. III-9 Security management: Web application SSL certificate

Purpose of this item: Implement an SSL certificate in a manner suited to one's own system

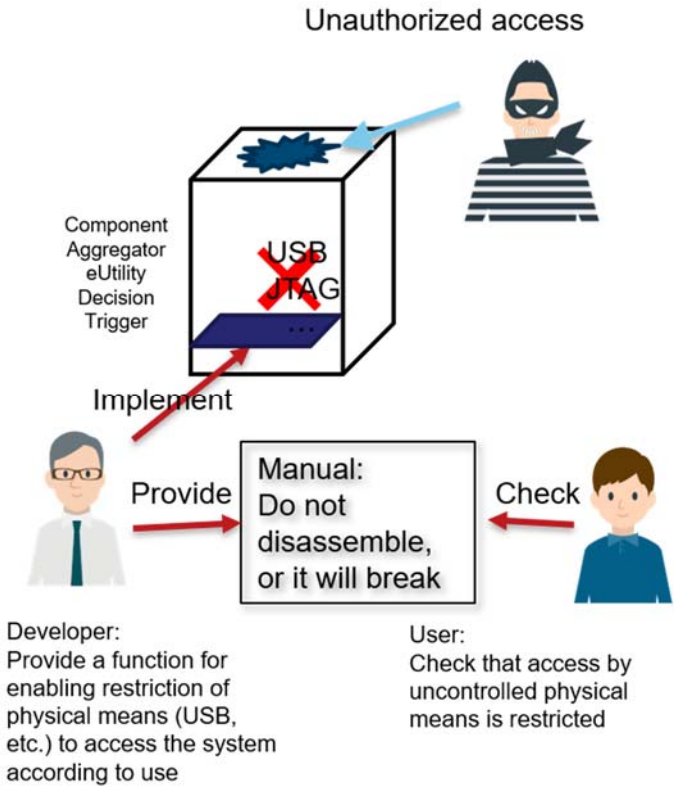
Scope: eUtility, Decision Trigger



No. IV-1 Access control: Access by uncontrolled physical means

Purpose of this item: Prevent system access by uncontrolled physical means

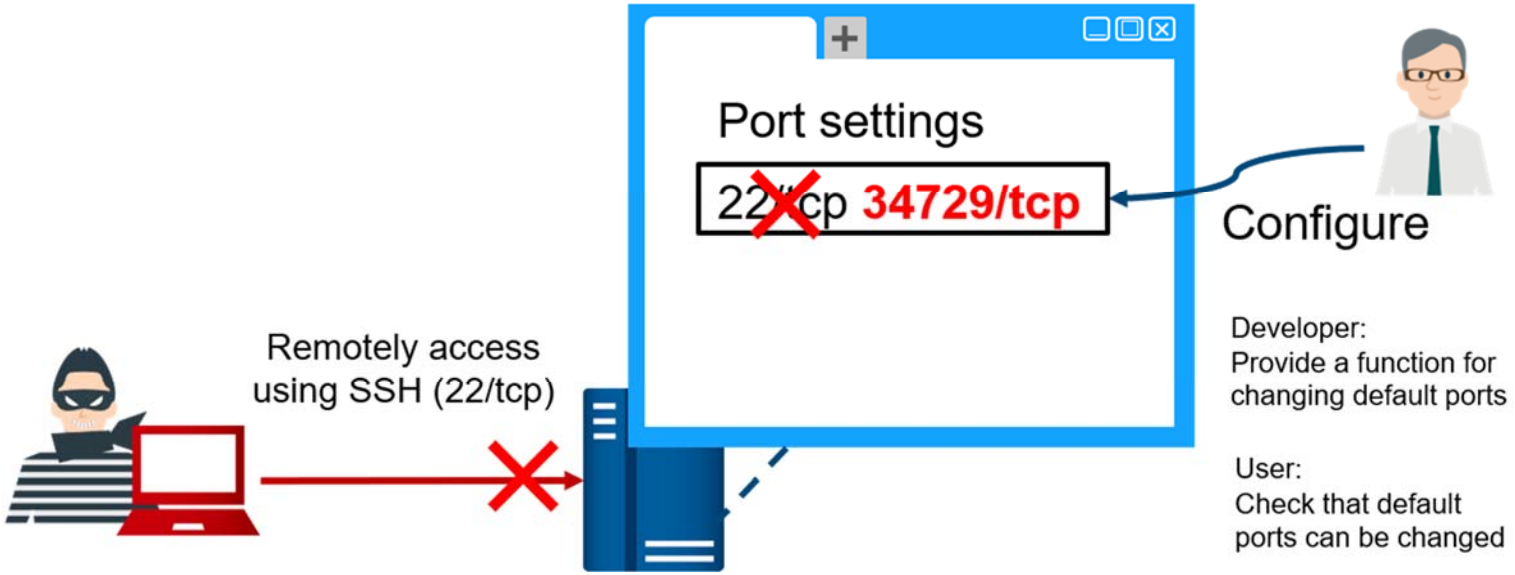
Scope: Aggregator, eUtility, Decision Trigger



No. IV-2 Access control: Default ports for remote access

Purpose of this item: Prevent attacks targeting default ports for remote access functions

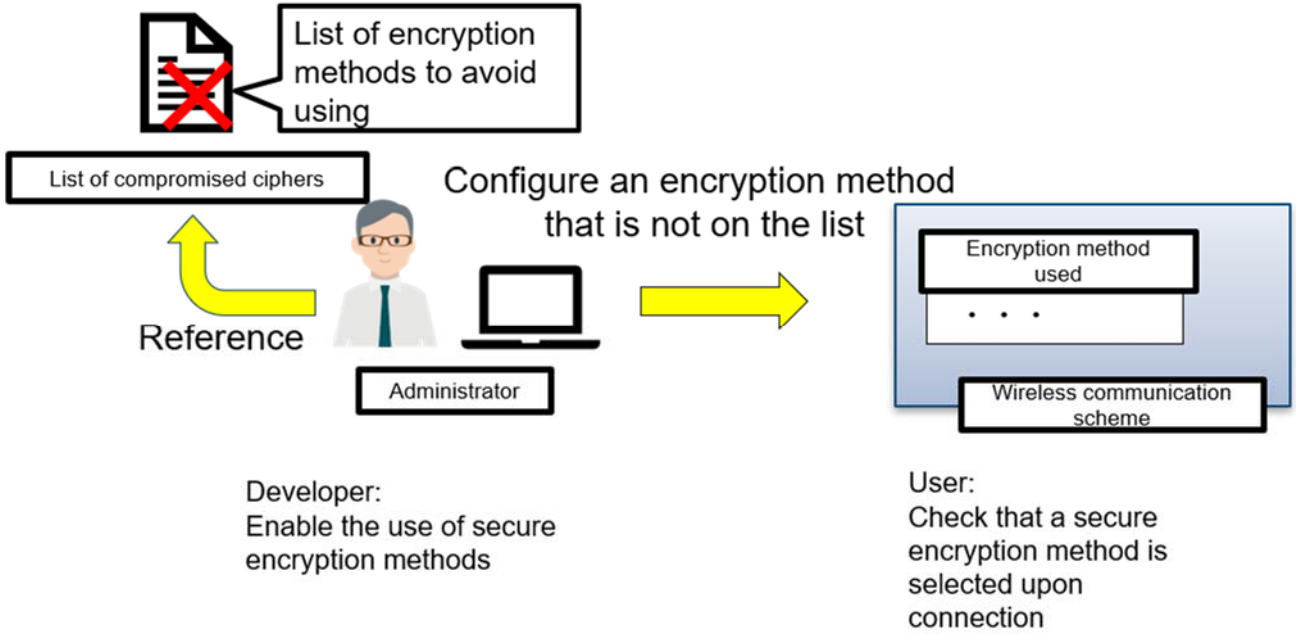
Scope: Aggregator, eUtility, Decision Trigger



No. IV-3 Access control: Wireless communication security (encryption method)

Purpose of this item: Use a secure encryption method to prevent the stealing of communicated content using vulnerabilities

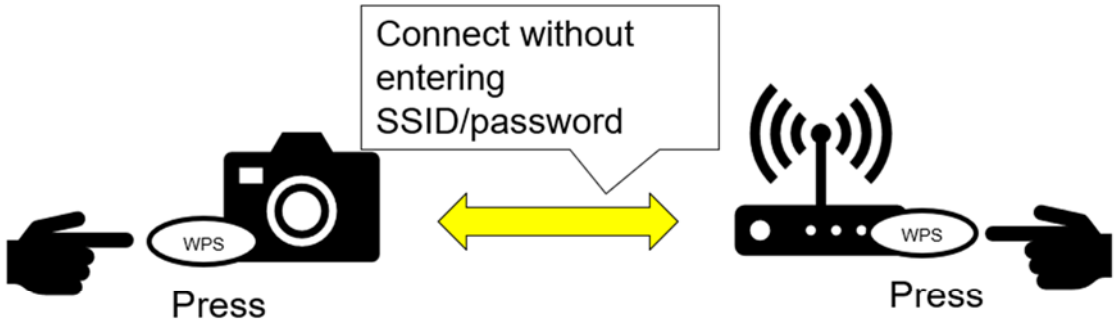
Scope: Aggregator, Communication Channel, eUtility, Decision Trigger



No. IV-4 Access control: Wireless communication security (WPS)

Purpose of this item: Prevent compromising security due to errors in wireless settings

Scope: Aggregator, Communication Channel, eUtility, Decision Trigger



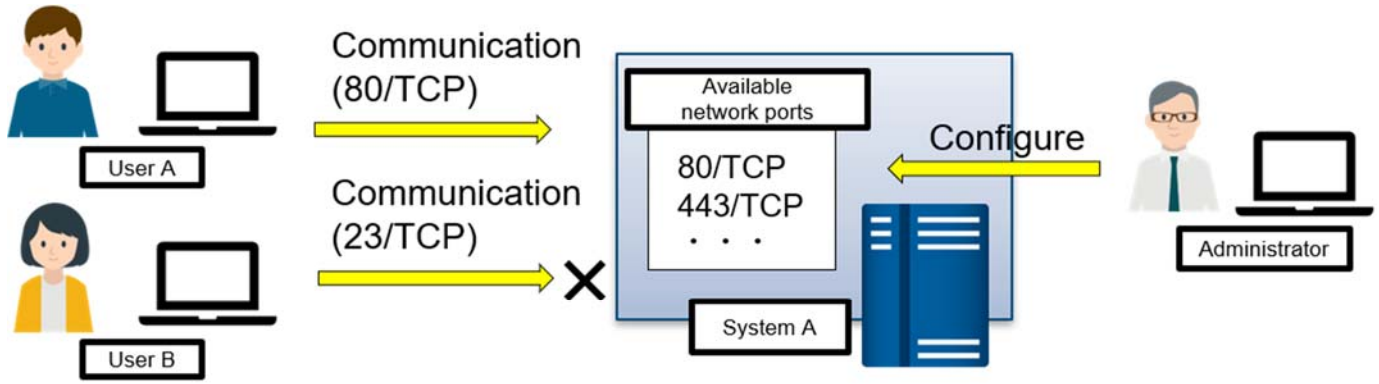
Developer:
Consider security when providing a WPS function (e.g., MAC address filtering)

User:
Check that WPS functions properly

No. V-1 Unauthorized connection: Restriction of network ports

Purpose of this item: Make only appropriate ports available according to the anticipated use

Scope: Aggregator, eUtility, Decision Trigger



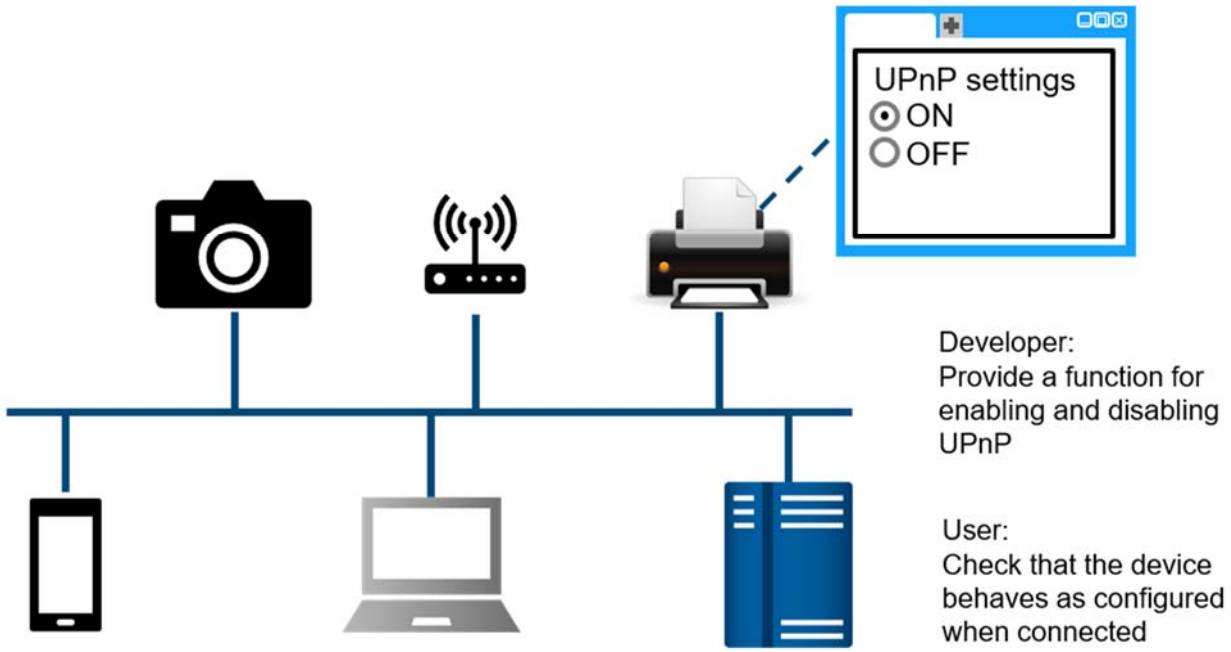
Developer:
Provide a function for opening or closing ports according the purpose of use

User:
Check that ports are opened or closed as configured

No. V-2 Unauthorized connection: UPnP

Purpose of this item: Make UPnP available on devices anticipated to be used

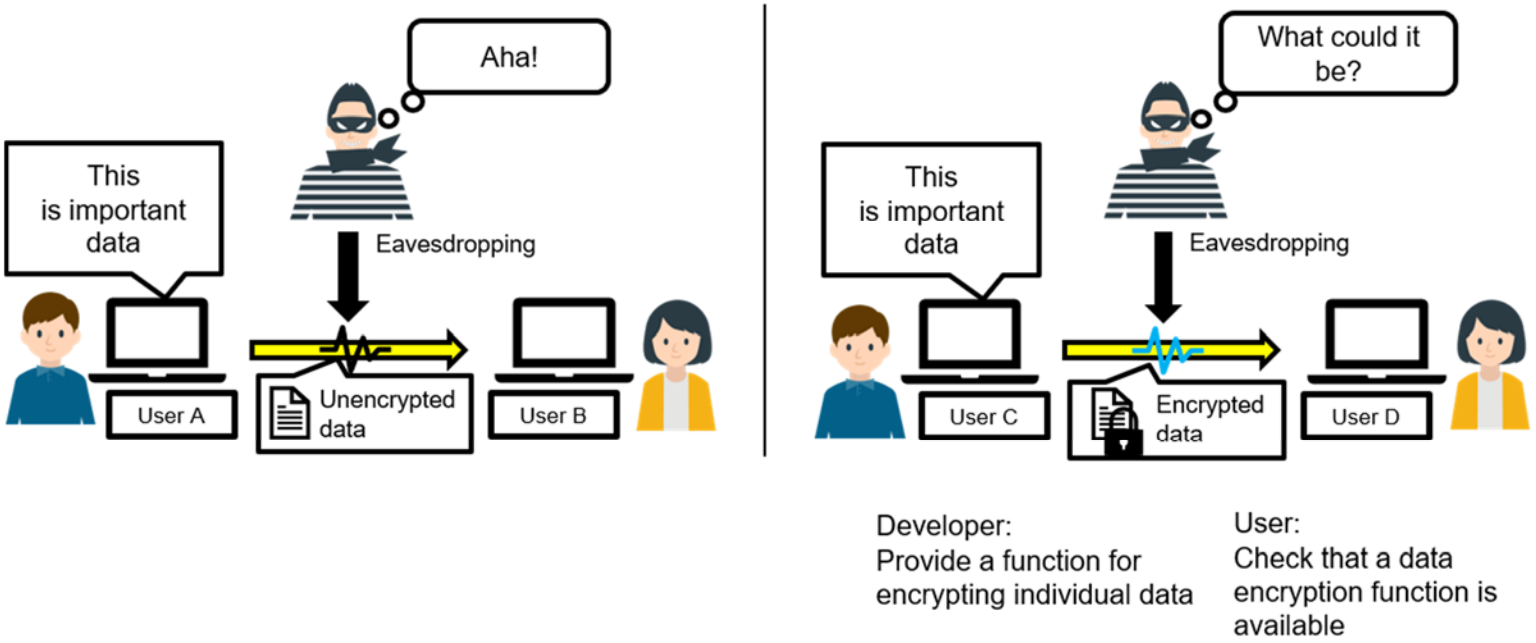
Scope: Aggregator, eUtility, Decision Trigger



No. VI-1 Encryption: Data encryption function

Purpose of this item: Prevent sending data in plain text and allowing communications to be eavesdropped

Scope: Aggregator, Communication Channel, eUtility, Decision Trigger



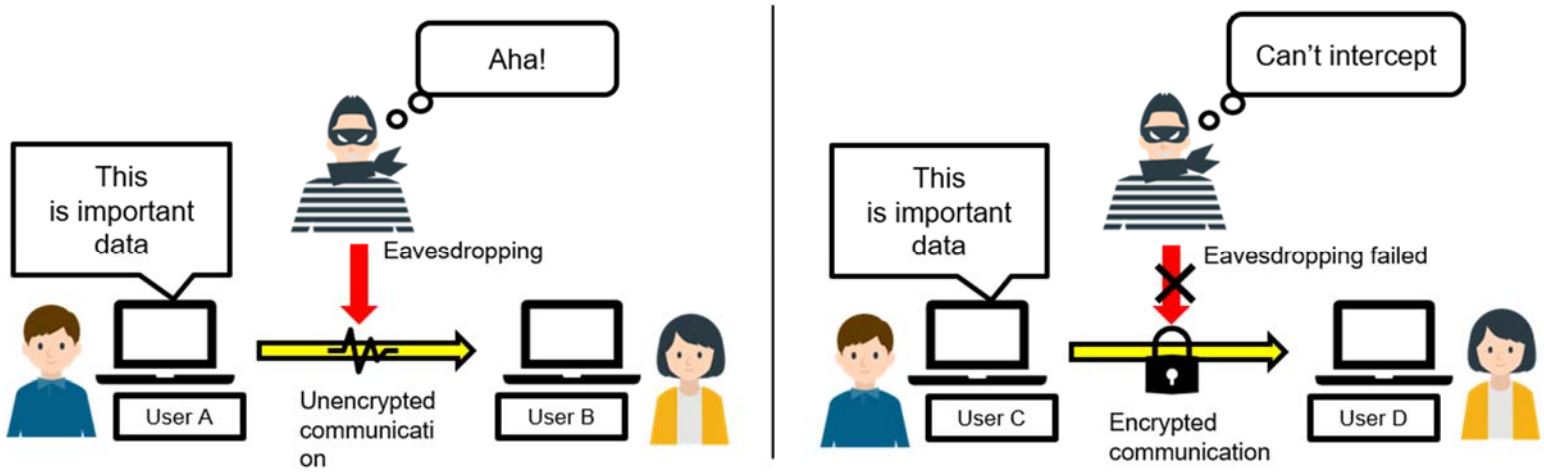
Developer:
Provide a function for encrypting individual data

User:
Check that a data encryption function is available

No. VI-2 Encryption: Communication encryption function

Purpose of this item: Prevent sending data in plain text and allowing communications to be eavesdropped

Scope: Aggregator, Communication Channel, eUtility, Decision Trigger



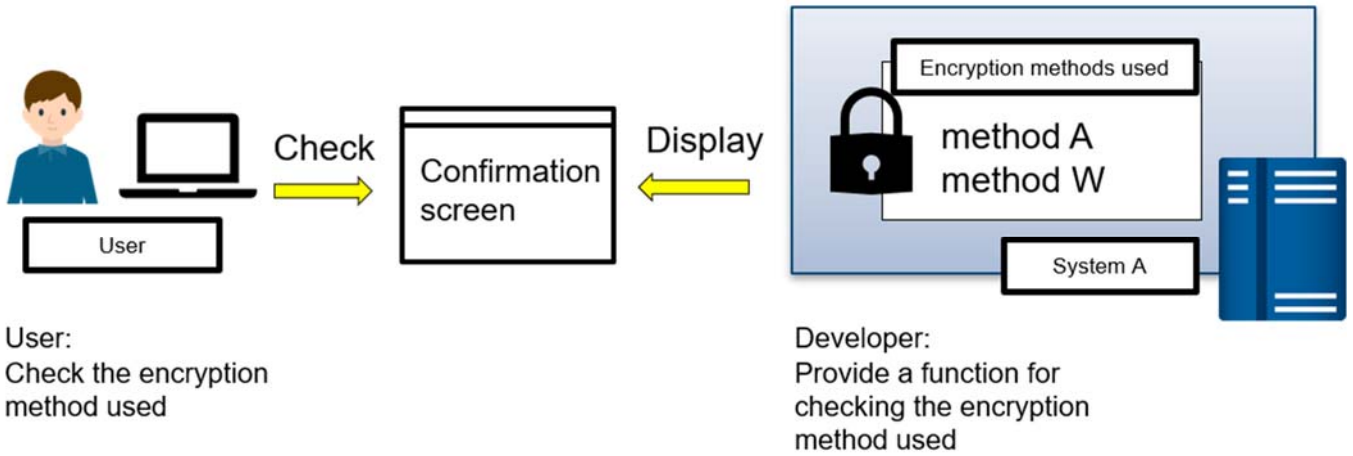
Developer:
Provide a function for performing encrypted communication using SSL/TLS, etc. between the devices that make up the system

User:
Check that encrypted communication can be used

No. VI-3 Encryption: Encryption method

Purpose of this item: Enable checking the encryption method used

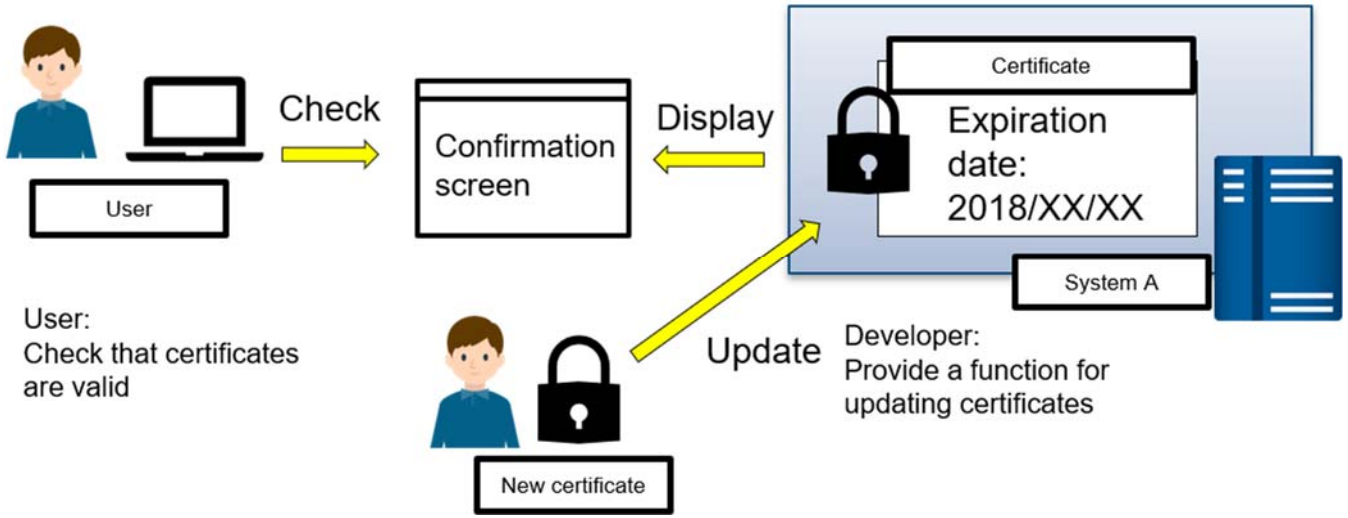
Scope: Aggregator, Communication Channel, eUtility, Decision Trigger



No. VI-4 Encryption: Certificate update function

Purpose of this item: Ensure certificates do not expire

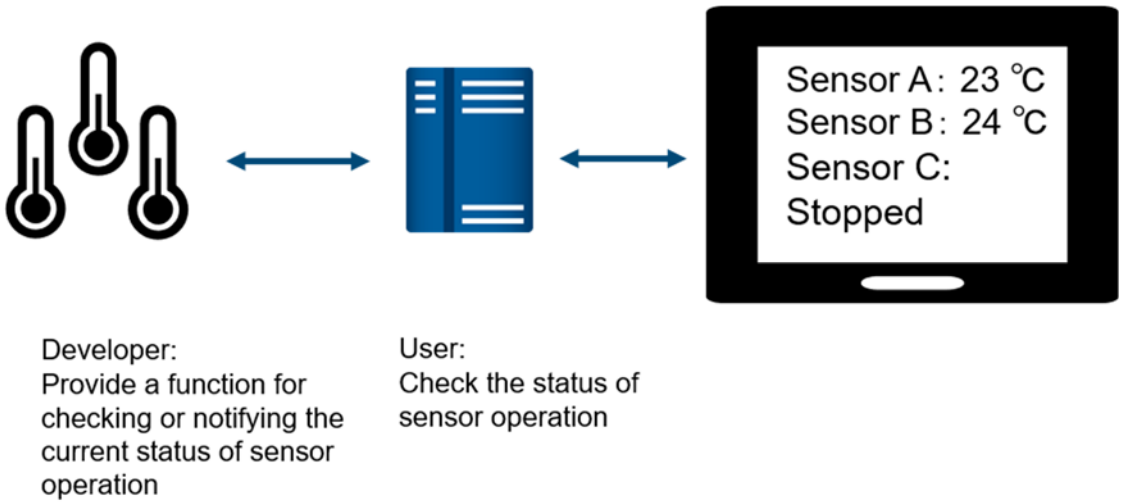
Scope: Aggregator, Communication Channel, eUtility, Decision Trigger



No. VII-1 System settings: Function for checking the status of sensor operation

Purpose of this item: Enable checking the status of operation

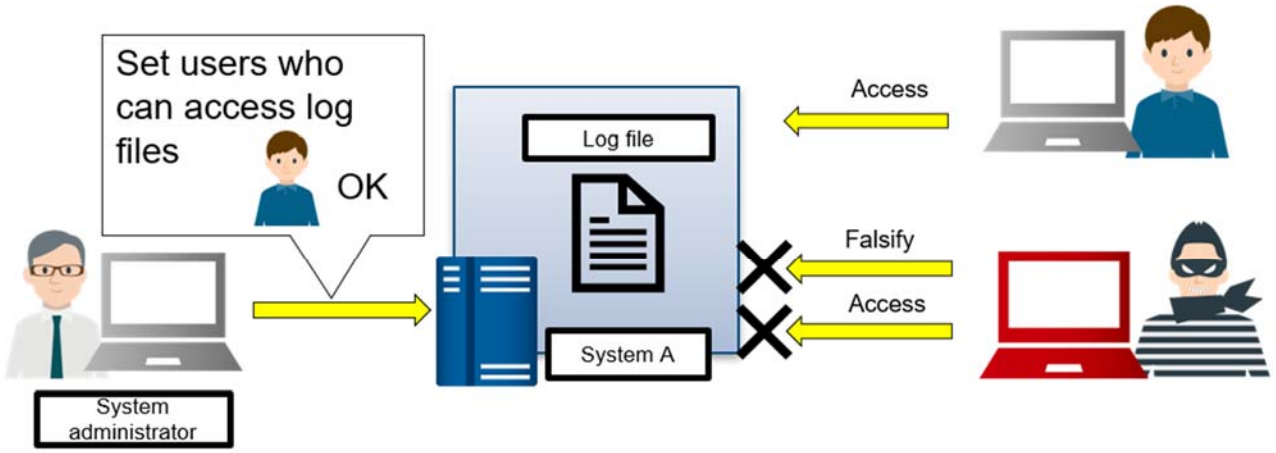
Scope: Sensor



No. VII-2 System settings: Log security management

Purpose of this item: Prevent logs from being accessed or falsified by a third party

Scope: Aggregator, eUtility, Decision Trigger



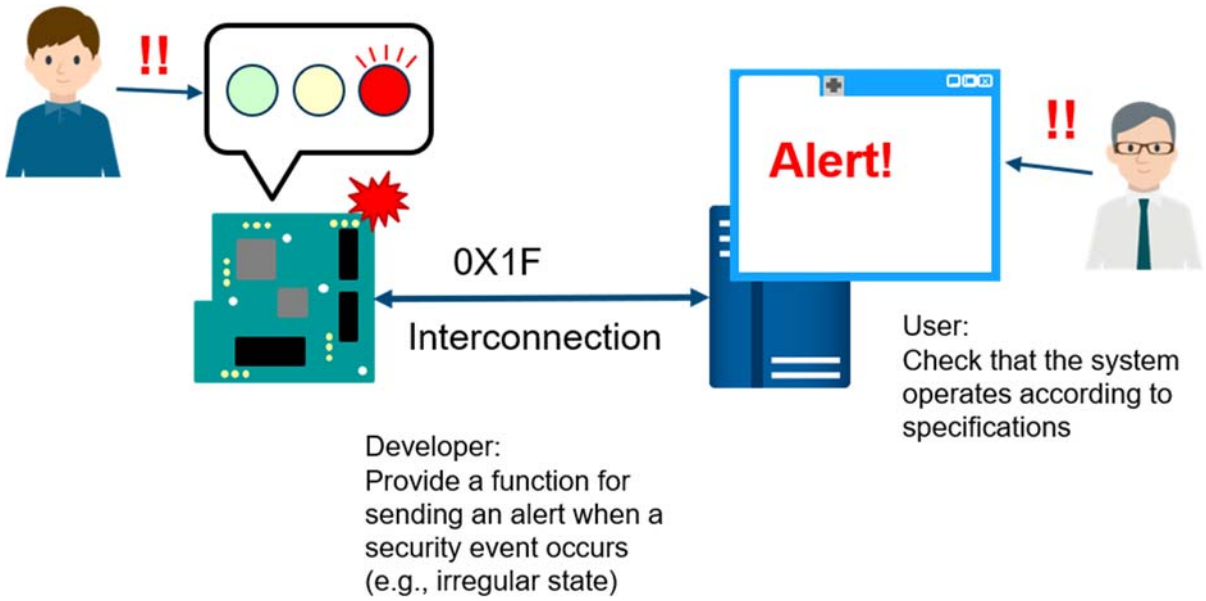
User:
Check that users without access permissions cannot access logs, and that users who can access logs cannot modify them

Developer:
Provide a function for specifying users who can access logs and preventing falsification of their content

No. VIII-1 Notification: Alert and notification function for security events (irregular state, etc.)

Purpose of this item: Enable rapid response when a security event occurs by sending an alert

Scope: Sensor



No. VIII-2 Notification: Alert and notification function for security events (authentication failure, expired certificate, etc.)

Purpose of this item: Enable rapid response when a security event occurs by sending an alert

Scope: Aggregator, eUtility, Decision Trigger

Developer:
Provide a function for sending an alert when a security event occurs (e.g., authentication failure, expired certificate)

User:
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