

[0068]

(f210-5): a function of transmitting the policy evaluation response including the determination result to the authentication collaboration handling unit 209 of the transmission source of the policy evaluation request.

5 [0069]

The IDP account provisioning unit 211 receives the account collaboration request from the authentication collaboration handling unit 209, and executes account provisioning on the service provider device 300. Specifically, for example, the IDP account provisioning unit 211 has the following functions (f211-1) to (f211-8).

10 [0070]

(f211-1): a function of reading some item names of the user attribute from the SP user setting rule store 204 based on the service provider ID included in the transmitted account collaboration request.

[0071]

15 (f211-2): a function of reading the deletion target account information 207a from the deletion target account store 207 based on the service provider ID included in the transmitted account collaboration request.

[0072]

20 (f211-3): a function of acquiring item names matching corresponding some item names and user attribute partial information including an item value associated with the item name from the user attribute information 201a including the user ID matching the user ID in the IDP user repository 201 based on read some item names and the user ID included in an account collaboration request message.

[0073]

25 (f211-4): a function of issuing the authentication collaboration ID shared

CLAIMS

1. An authentication collaboration system, comprising
an ID provider device that performs a log-in process on a user terminal operated
5 by a user; and
a service provider device that transmits service data to the user terminal when
the log-in process is completed,
wherein the user terminal transmits a service use request to the service provider
device,
10 the ID provider device includes
an IDP user repository that stores user attribute information in which an item
name of a user attribute specifying the user is associated with an item value of the user
attribute, the user attribute information including a user ID identifying the user,
an IDP service use status store that stores service use status information in which
15 the user ID, a service provider ID identifying the service provider device, and a use
status of the service provider device are associated with one another,
an authentication collaboration policy store that stores authentication
collaboration policy information representing a user which is a target to which
transmission of service data by the service provider device identified by the service
20 provider ID is permitted for each service provider ID,
an SP user setting rule store that stores the service provider ID in association
with some item names among item names of a user attribute in the user attribute
information,
a deletion target decision policy store that stores deletion target decision policy
25 information representing a user which is a target in which transmission permission of
service data is deleted in a service provider device identified by the service provider ID
for each service provider ID,
a service use status acquiring unit that acquires service use status information
transmitted from the service provider device when a predetermined cycle comes or

when the use status of the service provider device is changed, and updates the IDP service use status store based on the acquired service use status information,

a deletion target account deciding unit that decides a deletion target account of each service provider ID included in the service use status information based on the user attribute information, the service use status information, and the deletion target decision policy information,

an authentication collaboration handling unit that transmits a user authentication request including address information of a user terminal in the authentication collaboration request when an authentication collaboration request including the service provider ID of the service provider device and the address information of the user terminal is received from the service provider device that has received the service use request,

an IDP authentication collaboration unit that transmits a log-in request to the user terminal based on the address information of the user terminal in the transmitted user authentication request, and executes a log-in process of authenticating the user ID and the user authentication information received from the user terminal based on a user ID and a password in the IDP user repository,

wherein the authentication collaboration handling unit transmits a policy evaluation request including the user ID used in the log-in process and the service provider ID in the authentication collaboration request when the log-in process is successfully performed,

an authentication collaboration policy evaluating unit that reads the user attribute information from the IDP user repository based on the user ID in the transmitted policy evaluation request,

reads the authentication collaboration policy information from the authentication collaboration policy store based on the service provider ID in the transmitted policy evaluation request,

determines whether or not transmission of service data is to be permitted based on the read authentication collaboration policy information and the read user attribute information, and

transmits a policy evaluation response including a determination result to a transmission source of the policy evaluation request,

wherein the authentication collaboration handling unit transmits the account collaboration request including the user ID and the service provider ID in the policy evaluation request when the determination result in the policy evaluation response represents permission,

an IDP account provisioning unit that reads some item names of a user attribute from the SP user setting rule store based on the service provider ID in the transmitted account collaboration request,

acquires user attribute partial information including item names matching some item names and item values associated with the item names from the user attribute information including a user ID matching a user ID in the IDP user repository based on read some item names and the user ID in the account collaboration request,

acquires a deletion target account from the deletion target account decided by the deletion target account deciding unit based on the service provider ID in the transmitted account collaboration request,

generates an account collaboration request message by adding an account registration instruction to the acquired user attribute partial information as an operation instruction and adding an account deletion instruction or an account invalidating instruction to the acquired deletion target account as an operation instruction,

transmits the account collaboration request message to a service provider device of a transmission source of the authentication collaboration request, and

transmits an account collaboration response representing operation completion when operation completion including the service provider ID of the service provider device and the address information of the user terminal in the user attribute partial information is notified from a service provider device of a transmission destination of the account collaboration request message,

wherein the authentication collaboration handling unit transmits an authentication collaboration execution request including the service provider ID

included in the operation completion in the transmitted account collaboration response and the user ID, and

wherein the IDP authentication collaboration unit transmits an authentication collaboration response including the user ID in the authentication collaboration execution request to the service provider device of the transmission source of the authentication collaboration request when the authentication collaboration execution request is received, and

the service provider device includes

an SP user repository that stores user attribute partial information in which some item names and item values are associated with each other among item names and item values of a user attribute in the user attribute information in the IDP user repository in association with an SP side user ID identifying the user in the service provider device,

a service data store that stores the service data,

an SP service use status store that stores the user ID in association with the use status of the service provider device,

a service use status providing unit that acquires the use status of the service provider device from the SP service use status store, and transmitting the acquired use status to the ID provider device,

an SP authentication collaboration unit that determines whether or not the service request includes an authentication token when the service request is received from the user terminal, transmits the authentication token and service data in the service data store to the user terminal when it is determined that the service request includes an authentication token, and transmits the authentication collaboration request to the ID provider device when it is determined that the service request does not include an authentication token,

an SP account providing unit that issues a new SP side user ID and registers the issued SP side user ID and the user attribute partial information in the account collaboration request message to the SP user repository in association with each other when the account collaboration request message is received, and the operation

instruction included in the account collaboration request message represents the account registration.

searches the SP user repository based on the deletion target account in the account collaboration request message and deletes the user attribute partial information including the user ID matching the deletion target account when the operation instruction included in the account collaboration request message represents the account deletion, and

notifies the ID provider device of the transmission source of the account collaboration request message of update completion including the registered user ID in the user attribute partial information or the deleted user ID in the user attribute partial information and the service provider ID of the service provider device after the registration or the deletion.

wherein the SP authentication collaboration unit performs verification of the authentication collaboration response when the authentication collaboration response is received from the ID provider device, issuing the authentication token when a verification result represents permission, and

transmits the service execution request including the user ID included in the authentication collaboration response and the authentication token, and transmits the authentication token in the service execution request and service data in the service data store to the user terminal based on the transmitted service execution request.

2. The authentication collaboration system according to claim 1, wherein the authentication collaboration policy evaluating unit determines whether or not transmission of service data is to be permitted based on the service use status information.

3. The authentication collaboration system according to claim 1 or claim 2, wherein

the service account provisioning unit invalidates the user attribute partial information when the deletion target account matches the user ID included in the user attribute partial information.

4. The authentication collaboration system according to any one of claims 1 or 2, wherein

the service provider device transmits the use status to the ID provider device when the use status of the service provider device stored in the SP service use status store changes.

5. An ID provider device that is connected with a service provider device transmitting service data to a user terminal operated by a user to configure an authentication collaboration system, transmits a service use request to the service provider device, and performs a log-in process on the user terminal, the ID provider device comprising:

an IDP user repository that stores user attribute information in which an item name of a user attribute specifying the user is associated with an item value of the user attribute, the user attribute information including a user ID identifying the user;

an IDP service use status store that stores service use status information in which the user ID, a service provider ID identifying the service provider device, and a use status of the service provider device are associated with one another;

an authentication collaboration policy store that stores authentication collaboration policy information representing a user which is a target to which transmission of service data by the service provider device identified by the service provider ID is permitted for each service provider ID;

an SP user setting rule store that stores the service provider ID in association with some item names among item names of a user attribute in the user attribute information;

a deletion target decision policy store that stores deletion target decision policy information representing a user which is a target in which transmission permission of

service data is to be deleted in a service provider device identified by the service provider ID for each service provider ID;

a service use status acquiring unit that transmits a use status acquisition request to the service provider device, acquires service use status information transmitted from the service provider device based on the use status acquisition request, and updates the IDP service use status store based on the acquired service use status information;

a deletion target account deciding unit that decides a deletion target account of each service provider ID included in the service use status information based on the user attribute information, the service use status information, and the deletion target decision policy information;

an authentication collaboration handling unit that transmits a user authentication request including address information of a user terminal in the authentication collaboration request when an authentication collaboration request including the service provider ID of the service provider device and the address information of the user terminal is received from the service provider device that has received the service use request;

IDP authentication collaboration unit that transmits a log-in request to the user terminal based on the address information of the user terminal in the transmitted user authentication request, and executes a log-in process of authenticating the user ID and the user authentication information received from the user terminal based on a user ID and a password in the IDP user repository;

wherein the authentication collaboration handling unit transmits a policy evaluation request including the user ID used in the log-in process and the service provider ID in the authentication collaboration request when the log-in process is successfully performed,

an authentication collaboration policy evaluating unit that reads the user attribute information from the IDP user repository based on the user ID in the transmitted policy evaluation request.

reads the authentication collaboration policy information from the authentication collaboration policy store based on the service provider ID in the transmitted policy evaluation request,

5 determines whether or not transmission of service data is to be permitted based on the read authentication collaboration policy information and the read user attribute information, and

transmits a policy evaluation response including a determination result to a transmission source of the policy evaluation request;

10 wherein the authentication collaboration handling unit transmits the account collaboration request including the user ID and the service provider ID in the policy evaluation request when the determination result in the policy evaluation response represents permission,

15 an IDP account provisioning unit that reads some item names of a user attribute from the SP user setting rule store based on the service provider ID in the transmitted account collaboration request,

acquires user attribute partial information including item names matching some item names and item values associated with the item names from the user attribute information including a user ID matching a user ID in the IDP user repository based on read some item names and the user ID in the account collaboration request,

20 acquires a deletion target account from the deletion target account decided by the deletion target account deciding unit based on the service provider ID in the transmitted account collaboration request,

25 generates an account collaboration request message by adding an account registration instruction to the acquired user attribute partial information as an operation instruction and adding an account deletion instruction or an account invalidating instruction to the acquired deletion target account as an operation instruction,

transmits the account collaboration request message to a service provider device of a transmission source of the authentication collaboration request, and

30 transmits an account collaboration response representing operation completion when operation completion including the service provider ID of the service provider

device and the address information of the user terminal in the user attribute partial information is notified from a service provider device of a transmission destination of the account collaboration request message;

wherein the authentication collaboration handling unit transmits an authentication collaboration execution request including the service provider ID included in the operation completion in the transmitted account collaboration response and the user ID, and

wherein the IDP authentication collaboration unit transmits an authentication collaboration response including the user ID in the authentication collaboration execution request to the service provider device of the transmission source of the authentication collaboration request when the authentication collaboration execution request is received.

6. A non-transitory computer readable medium for causing a computer to perform operations of an ID provider device that is connected with a service provider device transmitting service data to a user terminal operated by a user to configure an authentication collaboration system, transmits a service use request to the service provider device, and performs a log-in process on the user terminal, the operations comprising:

a function of storing user attribute information in which an item name of a user attribute specifying the user is associated with an item value of the user attribute, the user attribute information including a user ID identifying the user;

a function of storing authentication collaboration policy information representing a user which is a target to which transmission of service data by the service provider device identified by the service provider ID is permitted for each service provider ID;

a function of storing the service provider ID in association with some item names among item names of a user attribute in the user attribute information;

a function of storing deletion target decision policy information representing a user which is a target in which transmission permission of service data is to be deleted

in a service provider device identified by the service provider ID for each service provider ID;

a function of transmitting a use status acquisition request to the service provider device, acquiring service use status information transmitted from the service provider device based on the use status acquisition request, and storing service use status information in which the user ID, a service provider ID identifying the service provider device, and a use status of the service provider device are associated with one another based on the acquired service use status information;

a function of deciding a deletion target account of each service provider ID included in the service use status information based on the user attribute information, the service use status information, and the deletion target decision policy information;

a function of transmitting a user authentication request including address information of a user terminal in the authentication collaboration request when an authentication collaboration request including the service provider ID of the service provider device and the address information of the user terminal is received from the service provider device that has received the service use request;

a function of transmitting a log-in request to the user terminal based on the address information of the user terminal in the transmitted user authentication request, and executing a log-in process of authenticating the user ID and the user authentication information received from the user terminal based on a user ID and a password of the user attribute information;

a function of transmitting a policy evaluation request including the user ID used in the log-in process and the service provider ID in the authentication collaboration request when the log-in process is successfully performed;

a function of reading the user attribute information based on the user ID in the transmitted policy evaluation request;

a function of reading the authentication collaboration policy information based on the service provider ID in the transmitted policy evaluation request;

a function of determining whether or not transmission of service data is to be permitted based on the read authentication collaboration policy information and the read user attribute information;

a function of transmitting a policy evaluation response including a determination result to a transmission source of the policy evaluation request;

a function of transmitting the account collaboration request including the user ID and the service provider ID in the policy evaluation request when the determination result in the policy evaluation response represents permission;

a function of reading some item names of a user attribute based on the service provider ID in the transmitted account collaboration request;

a function of acquiring user attribute partial information including item names matching some item names and item values associated with the item names from the user attribute information including a user ID matching a user ID based on read some item names and the user ID in the account collaboration request;

a function of acquiring a deletion target account from the decided deletion target account based on the service provider ID in the transmitted account collaboration request;

a function of generating an account collaboration request message by adding an account registration instruction to the acquired user attribute partial information as an operation instruction and adding an account deletion instruction or an account invalidating instruction to the acquired deletion target account as an operation instruction;

a function of transmitting the account collaboration request message to a service provider device of a transmission source of the authentication collaboration request;

a function of transmitting an account collaboration response representing operation completion when operation completion including the service provider ID of the service provider device and the address information of the user terminal in the user attribute partial information is notified from a service provider device of a transmission destination of the account collaboration request message;

- 5 | a function of transmitting an authentication collaboration execution request including the service provider ID included in the operation completion in the transmitted account collaboration response and the user ID, and a function of transmitting an authentication collaboration response including the user ID in the authentication collaboration execution request to the service provider device of the transmission source of the authentication collaboration request when the authentication collaboration execution request is received.

[NAME OF DOCUMENT] CLAIMS

1. An authentication collaboration system, comprising
an ID provider device that performs a log-in process on a user terminal
operated by a user; and
a service provider device that transmits service data to the user terminal when
the log-in process is completed,
wherein the user terminal transmits a service use request to the service provider
device,
the ID provider device includes
a user attribute information storage unit that stores user attribute information in
which an item name of a user attribute specifying the user is associated with an item
value of the user attribute, the user attribute information including a user ID identifying
the user,
a first service use status storage unit that stores service use status information
in which the user ID, a service provider ID identifying the service provider device, and
a use status of the service provider device are associated with one another,
an authentication collaboration policy storage unit that stores authentication
collaboration policy information representing a user which is a target to which
transmission of service data by the service provider device identified by the service
provider ID is permitted for each service provider ID,
a partial item name storage unit that stores the service provider ID in
association with some item names among item names of a user attribute in the user
attribute information,
a deletion target decision policy storage unit that stores deletion target decision
policy information representing a user which is a target in which transmission

permission of service data is deleted in a service provider device identified by the service provider ID for each service provider ID,

a unit that acquires service use status information transmitted from the service provider device when a predetermined cycle comes or when the use status of the service provider device is changed, and updates the first service use status storage unit based on the acquired service use status information,

a unit that decides a deletion target account of each service provider ID included in the service use status information based on the user attribute information, the service use status information, and the deletion target decision policy information,

a unit that transmits a user authentication request including address information of a user terminal in the authentication collaboration request when an authentication collaboration request including the service provider ID of the service provider device and the address information of the user terminal is received from the service provider device that has received the service use request,

a unit that transmits a log-in request to the user terminal based on the address information of the user terminal in the transmitted user authentication request, and executes a log-in process of authenticating the user ID and the user authentication information received from the user terminal based on a user ID and a password in the user attribute information storage unit,

a unit that transmits a policy evaluation request including the user ID used in the log-in process and the service provider ID in the authentication collaboration request when the log-in process is successfully performed,

a unit that reads the user attribute information from the user attribute storage unit based on the user ID in the transmitted policy evaluation request,

a unit that reads the authentication collaboration policy information from the

authentication collaboration policy storage unit based on the service provider ID in the transmitted policy evaluation request,

a unit that determines whether or not transmission of service data is to be permitted based on the read authentication collaboration policy information and the read user attribute information,

a unit that transmits a policy evaluation response including a determination result to a transmission source of the policy evaluation request,

a unit that transmits the account collaboration request including the user ID and the service provider ID in the policy evaluation request when the determination result in the policy evaluation response represents permission,

a unit that reads some item names of a user attribute from the partial item name storage unit based on the service provider ID in the transmitted account collaboration request,

a unit that acquires user attribute partial information including item names matching some item names and item values associated with the item names from the user attribute information including a user ID matching a user ID in the user attribute storage unit based on read some item names and the user ID in the account collaboration request,

a unit that acquires a deletion target account from the deletion target account decided by the deletion target account deciding unit based on the service provider ID in the transmitted account collaboration request,

a unit that generates an account collaboration request message by adding an account registration instruction to the acquired user attribute partial information as an operation instruction and adding an account deletion instruction or an account invalidating instruction to the acquired deletion target account as an operation

instruction,

a unit that transmits the account collaboration request message to a service provider device of a transmission source of the authentication collaboration request,

a unit that transmits an account collaboration response representing update completion when update completion including the service provider ID of the service provider device and the address information of the user terminal in the user attribute partial information is notified from a service provider device of a transmission destination of the account collaboration request message,

a unit that transmits an authentication collaboration execution request including the service provider ID included in the update completion in the transmitted account collaboration response and the user ID, and

a unit that transmits an authentication collaboration response including the user ID in the authentication collaboration execution request to the service provider device of the transmission source of the authentication collaboration request when the authentication collaboration execution request is received, and

the service provider device includes

a user attribute partial information storage unit that stores user attribute partial information in which some item names and item values are associated with each other among item names and item values of a user attribute in the user attribute information in the user attribute information storage unit in association with an SP side user ID identifying the user in the service provider device,

a service data storage unit that stores the service data,

a second service use status storage unit that stores the user ID in association with the use status of the service provider device,

a unit that acquires the use status of the service provider device from the

service use status storage unit, and transmitting the acquired use status to the ID provider device,

a unit that determines whether or not the service request includes an authentication token when the service request is received from the user terminal, transmits the authentication token and service data in the service data storage unit to the user terminal when it is determined that the service request includes an authentication token, and transmits the authentication collaboration request to the ID provider device when it is determined that the service request does not include an authentication token,

a unit that issues a new SP side user ID and registers the issued SP side user ID and the user attribute partial information in the account collaboration request message to the user attribute partial information storage unit in association with each other when the account collaboration request message is received, and the operation instruction included in the account collaboration request message represents the account registration,

a unit that searches the user attribute partial information storage unit based on the deletion target account in the account collaboration request message and deletes the user attribute partial information including the user ID matching the deletion target account when the operation instruction included in the account collaboration request message represents the account deletion,

a unit that notifies the ID provider device of the transmission source of the account collaboration request message of update completion including the registered user ID in the user attribute partial information or the deleted user ID in the user attribute partial information and the service provider ID of the service provider device after the registration or the deletion,

a unit that performs verification of the authentication collaboration response

when the authentication collaboration response is received from the ID provider device, issuing the authentication token when a verification result represents permission, and transmits the service execution request including the user ID included in the authentication collaboration response and the authentication token, and

a unit that transmits the authentication token in the service execution request and service data in the service data storage unit to the user terminal based on the transmitted service execution request.

2. The authentication collaboration system according to claim 1, further comprising

a unit that determines whether or not transmission of service data is to be permitted based on the service use status information.

3. The authentication collaboration system according to claim 1 or 2, further comprising

a unit that invalidates the user attribute partial information when the deletion target account matches the user ID included in the user attribute partial information.

4. The authentication collaboration system according to any one of claims 1 to 3, further comprising

a unit that transmits the use status to the ID provider device when the use status of the service provider device stored in the second service use status storage unit changes.

5. An ID provider device that is connected with a service provider device

transmitting service data to a user terminal operated by a user to configure an authentication collaboration system, transmits a service use request to the service provider device, and performs a log-in process on the user terminal, the ID provider device comprising:

a user attribute information storage unit that stores user attribute information in which an item name of a user attribute specifying the user is associated with an item value of the user attribute, the user attribute information including a user ID identifying the user;

a first service use status storage unit that stores service use status information in which the user ID, a service provider ID identifying the service provider device, and a use status of the service provider device are associated with one another;

an authentication collaboration policy storage unit that stores authentication collaboration policy information representing a user which is a target to which transmission of service data by the service provider device identified by the service provider ID is permitted for each service provider ID;

a partial item name storage unit that stores the service provider ID in association with some item names among item names of a user attribute in the user attribute information;

a deletion target decision policy storage unit that stores deletion target decision policy information representing a user which is a target in which transmission permission of service data is to be deleted in a service provider device identified by the service provider ID for each service provider ID;

a unit that transmits a use status acquisition request to the service provider device, acquires service use status information transmitted from the service provider device based on the use status acquisition request, and updates the service use status

storage unit based on the acquired service use status information;

a unit that decides a deletion target account of each service provider ID included in the service use status information based on the user attribute information, the service use status information, and the deletion target decision policy information;

a unit that transmits a user authentication request including address information of a user terminal in the authentication collaboration request when an authentication collaboration request including the service provider ID of the service provider device and the address information of the user terminal is received from the service provider device that has received the service use request;

a unit that transmits a log-in request to the user terminal based on the address information of the user terminal in the transmitted user authentication request, and executes a log-in process of authenticating the user ID and the user authentication information received from the user terminal based on a user ID and a password in the user attribute information storage unit;

a unit that transmits a policy evaluation request including the user ID used in the log-in process and the service provider ID in the authentication collaboration request when the log-in process is successfully performed;

a unit that reads the user attribute information from the user attribute storage unit based on the user ID in the transmitted policy evaluation request;

a unit that reads the authentication collaboration policy information from the authentication collaboration policy storage unit based on the service provider ID in the transmitted policy evaluation request;

a unit that determines whether or not transmission of service data is to be permitted based on the read authentication collaboration policy information and the read user attribute information;

a unit that transmits a policy evaluation response including a determination result to a transmission source of the policy evaluation request;

a unit that transmits the account collaboration request including the user ID and the service provider ID in the policy evaluation request when the determination result in the policy evaluation response represents permission;

a unit that reads some item names of a user attribute from the partial item name storage unit based on the service provider ID in the transmitted account collaboration request;

a unit that acquires user attribute partial information including item names matching some item names and item values associated with the item names from the user attribute information including a user ID matching a user ID in the user attribute storage unit based on read some item names and the user ID in the account collaboration request;

a unit that acquires a deletion target account from the deletion target account decided by the deletion target account deciding unit based on the service provider ID in the transmitted account collaboration request;

a unit that generates an account collaboration request message by adding an account registration instruction to the acquired user attribute partial information as an operation instruction and adding an account deletion instruction or an account invalidating instruction to the acquired deletion target account as an operation instruction;

a unit that transmits the account collaboration request message to a service provider device of a transmission source of the authentication collaboration request;

a unit that transmits an account collaboration response representing update completion when update completion including the service provider ID of the service

provider device and the address information of the user terminal in the user attribute partial information is notified from a service provider device of a transmission destination of the account collaboration request message;

a unit that transmits an authentication collaboration execution request including the service provider ID included in the update completion in the transmitted account collaboration response and the user ID, and

a unit that transmits an authentication collaboration response including the user ID in the authentication collaboration execution request to the service provider device of the transmission source of the authentication collaboration request when the authentication collaboration execution request is received.

6. A program of an ID provider device that is connected with a service provider device transmitting service data to a user terminal operated by a user to configure an authentication collaboration system, transmits a service use request to the service provider device, and performs a log-in process on the user terminal, the program causing a computer configuring the ID provider device to execute:

a function of storing user attribute information in which an item name of a user attribute specifying the user is associated with an item value of the user attribute, the user attribute information including a user ID identifying the user;

a function of storing authentication collaboration policy information representing a user which is a target to which transmission of service data by the service provider device identified by the service provider ID is permitted for each service provider ID;

a function of storing the service provider ID in association with some item names among item names of a user attribute in the user attribute information;

a function of storing deletion target decision policy information representing a user which is a target in which transmission permission of service data is to be deleted in a service provider device identified by the service provider ID for each service provider ID;

a function of transmitting a use status acquisition request to the service provider device, acquiring service use status information transmitted from the service provider device based on the use status acquisition request, and storing service use status information in which the user ID, a service provider ID identifying the service provider device, and a use status of the service provider device are associated with one another based on the acquired service use status information;

a function of deciding a deletion target account of each service provider ID included in the service use status information based on the user attribute information, the service use status information, and the deletion target decision policy information;

a function of transmitting a user authentication request including address information of a user terminal in the authentication collaboration request when an authentication collaboration request including the service provider ID of the service provider device and the address information of the user terminal is received from the service provider device that has received the service use request;

a function of transmitting a log-in request to the user terminal based on the address information of the user terminal in the transmitted user authentication request, and executing a log-in process of authenticating the user ID and the user authentication information received from the user terminal based on a user ID and a password of the user attribute information;

a function of transmitting a policy evaluation request including the user ID used in the log-in process and the service provider ID in the authentication collaboration

request when the log-in process is successfully performed;

a function of reading the user attribute information based on the user ID in the transmitted policy evaluation request;

a function of reading the authentication collaboration policy information based on the service provider ID in the transmitted policy evaluation request;

a function of determining whether or not transmission of service data is to be permitted based on the read authentication collaboration policy information and the read user attribute information;

a function of transmitting a policy evaluation response including a determination result to a transmission source of the policy evaluation request;

a unit of transmitting the account collaboration request including the user ID and the service provider ID in the policy evaluation request when the determination result in the policy evaluation response represents permission;

a function of reading some item names of a user attribute based on the service provider ID in the transmitted account collaboration request;

a function of acquiring user attribute partial information including item names matching some item names and item values associated with the item names from the user attribute information including a user ID matching a user ID based on read some item names and the user ID in the account collaboration request;

a function of acquiring a deletion target account from the decided deletion target account based on the service provider ID in the transmitted account collaboration request;

a function of generating an account collaboration request message by adding an account registration instruction to the acquired user attribute partial information as an operation instruction and adding an account deletion instruction or an account

invalidating instruction to the acquired deletion target account as an operation instruction;

a function of transmitting the account collaboration request message to a service provider device of a transmission source of the authentication collaboration request;

a function of transmitting an account collaboration response representing update completion when update completion including the service provider ID of the service provider device and the address information of the user terminal in the user attribute partial information is notified from a service provider device of a transmission destination of the account collaboration request message;

a function of transmitting an authentication collaboration execution request including the service provider ID included in the update completion in the transmitted account collaboration response and the user ID, and

a function of transmitting an authentication collaboration response including the user ID in the authentication collaboration execution request to the service provider device of the transmission source of the authentication collaboration request when the authentication collaboration execution request is received.