PROCENTER SaaS

Cabinet Administrator Manual

Version 1.0

July, 2024

NEC Solution Innovators, Ltd.

・NEC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

・Use, copying, and distribution of any NEC software described in this publication requires an applicable Service use consent.

・All other trademarks used herein are the property of their respective owners.

Revised history

Ver	Revised date	Function
1.0	2024.08.28	New creation

Table of contents

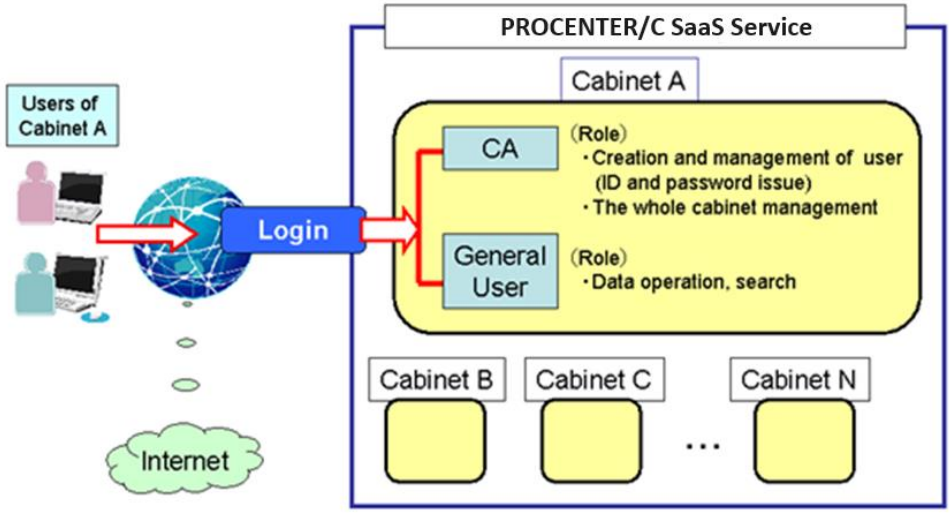
Introduction

Thank you very much for introducing "PROCENTER SaaS Service" (following, this Service) provided by NEC.

This Service is a web application Service which offers various functions for managing documents. This Service is based on “PROCENTER/C” software product to enable controlling distribution / duplication of documents with keeping rules of preservation and disposal strictly.

In this Service, we offer a new cabinet per contract. Through the Internet, you can freely access and use the cabinet that you belong.

There are two types of users, Cabinet Administrator (CA) and general user. The following is use image of Service.



In addition, the system requirements of this Service is as follows. Be sure to confirm before using.

OS	Microsoft Windows 10 (32bit/64bit)
Browser	Microsoft Edge ※ When using Edge, be sure to perform "Before using Edge" in the appendix.

Chapter 1 Preface

This manual is functional description for Cabinet Administrators in this Service.
In case using this Service, refer to "PROCENTER SaaS User Manual" collectively about each function.

Chapter 2 Overview

This chapter is explaining the overview of function in which only Cabinet Administrator can operate, and cabinet management work.

2.1 About cabinet administrator

Cabinet administrator is called “Cabinet Administrator” (following, CA).CA has privilege as the administrator in cabinet. CA can do the following operations.

- All operations to the folders and files in a cabinet (creation, reference, updating, and deletion)
- Changing of all “Access control” and Owner to folders and files in cabinet
- Changing of all expiration date to folders and files in a cabinet and the cabinet
- Creation, reference, updating, and deletion of users in cabinet
- Creation, updating, deletion, and member changing of local group in cabinet
- Role grant as a administrator (group administrator: following GA) of created group (GA role)
- CA appointment and release to users in a cabinet
- User batch processing functional operation
- Log management functional operation
- Renewal of a cabinet

——Supplementary explanation——

■Role

Role is defined by the form which gives the authority of operation to user. Role cannot be given to group (group: state which summarized one or more users). Priority is given to the authority lodged with role over the authority lodged by “Access control”.

2.2 Cabinet administrator's operation ambit

Cabinet Administrator (CA) has the following authority about user operation and group operation.

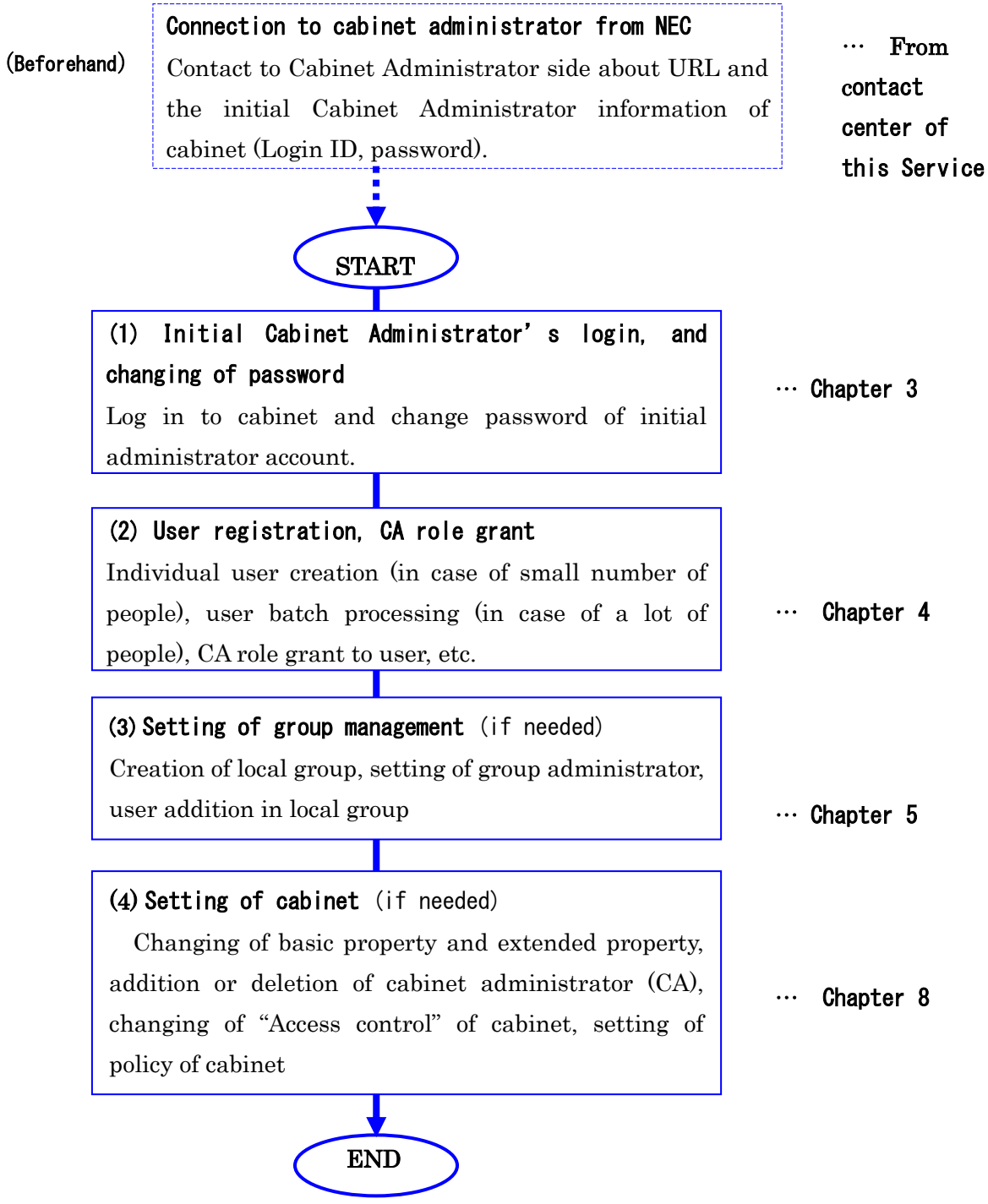
Item	CA	GA	General User
Setting of CA (appointment, dismissal)	○	—	—
Setting of GA (appointment, dismissal)	○	○	—
User new creation	○	—	—
User property changing	○	—	—
User deletion	○	—	—
User addition in local group	○	○	—
User deletion from local group	○	○	—
User search in cabinet	○	—	—
User batch processing function	○	—	—
Log management function	○	—	—
Changing of Access control in cabinet	○	—	—
Changing of owner in cabinet	○	—	—
Changing of expiration date of data in cabinet	○	—	—
Changing of “Access control” of local groups	○	○	—
Changing of Owner in local group	○	○	—
Renewal of cabinet	○	—	—

※ User cannot be restored when CA carries out user deletion.

2.3 About Cabinet Administrator's work（overview）

(1) At the time of initial employment

The work immediately after cabinet delivery serves as the following flows. Details of operation in flow and setting should read chapter indicated on right-hand side.



(2) At the time of routinely operation

Work under routinely operation has the following kinds.

Details of each operation and setting should read the chapter indicated on right-hand side.

(1) Management of user

User creation, user batch processing, changing of user information, CA role grant / deletion, user deletion and Owner changing, changing of user password

… Chapter 4

(2) Management of group

Local group creation, member addition to group, changing property of local group, member management in local group, local group deletion

… Chapter 5

(3) Management of data

Changing of Owner, changing of “Access control”, locking and unlocking of data

… Chapter 6

(4) Log operation function

User group operation, data manipulation

… Chapter 7

(5) Setting of cabinet

Changing of basic property and extended property, addition or deletion of cabinet administrator (CA), changing of “cabinet Access control”, setting of policy of cabinet

… Chapter 8

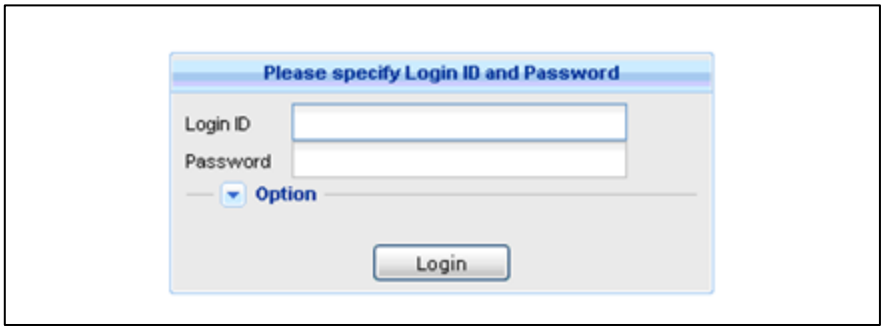
Chapter 3 Login / Logout

3.1 Login

3.1.1 Login（No "TOTP authentication"）

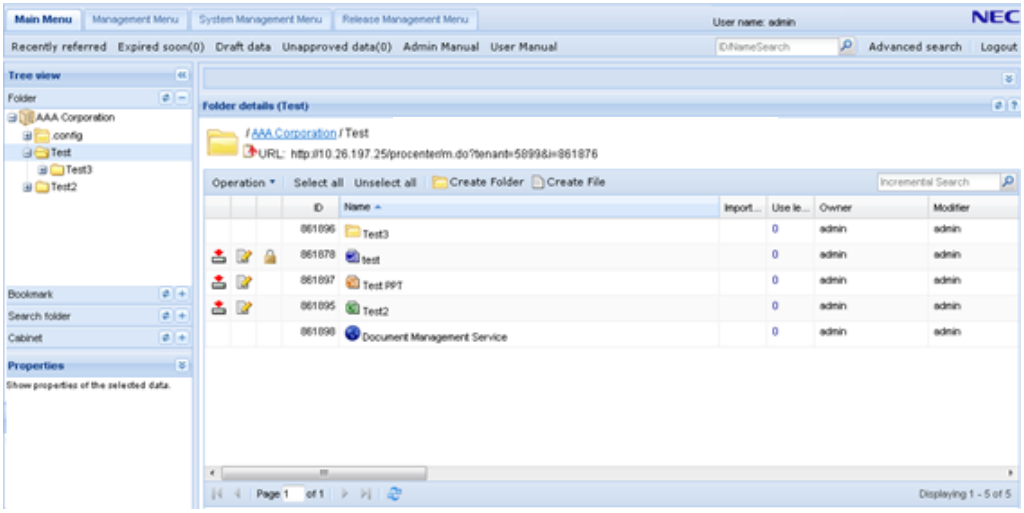
Log in to this Service by using **[Login ID] / [Password] / [Login URL]** connected from contact center of this Service.

1. Access login URL to connect from contact center of this Service.
   https://procenter-global.com/procenter/?tenant=XXXXX
2. On login screen, input **[Login ID] / [Password]** and click a **[Login]** button.
   - Inputted password is displayed by black symbol.
   - Role of CA needs to be given to user who logs in to operate Cabinet Administrator function.



Language can be set by specifying **Option**. In standard, it is set as same setting of a browser.

3. When inputted user ID and password are right, main screen of cabinet is displayed.



Service folder (.config) and sample of CSV file for user batch processing (template file for import) are registered into cabinet folder immediately after cabinet delivery.
Service folder (.config) is displayed only on person of authority more than CA role. Since it is for Service management, do not register data in it.

Moreover, import file (CSV) for user batch processing is a template file performing batch processing the user. Do not delete.

――Notes――

■ About login ID in case of managing two or more cabinets

About Cabinet Administrator (CA) belonging to two or more cabinets, login ID in the login screen, you can use ID of unification (Since Login URL differs for every cabinet). However, number of cabinets displayed on operation screen is one.

■ About account automatic lock

- User account is locked when it does not log in for 180 days. User account is locked similarly, if user does not log in for 180 days after user creation.
- User account is locked if you mistake login processing 5 times continuously.
- Although locked account by 5 times login processing mistake is canceled automatically, it takes 15 minutes.

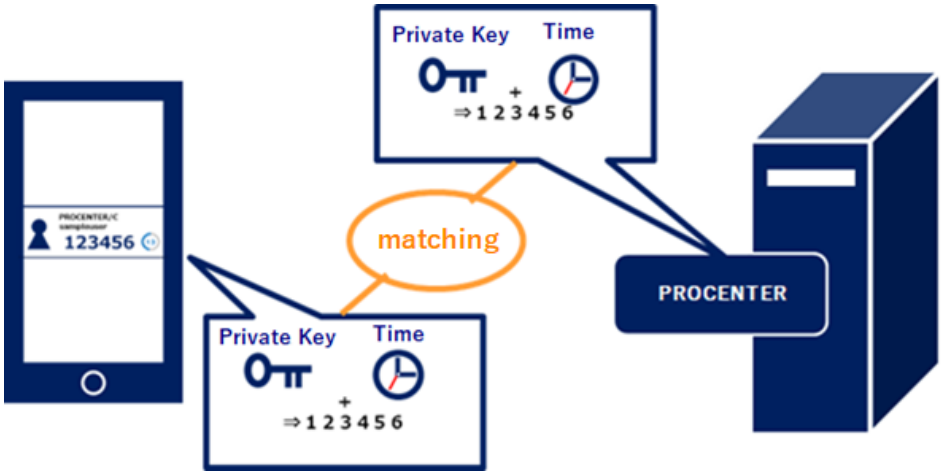
3.1.2 Login（"TOTP authentication" available）

（1） What is "TOTP authentication function"

This is a function that uses "TOTP (Time-based One-Time Password) Authentication" to allow login with a one-time password.

By enabling the "TOTP function", multi-step authentication using a one-time password is required when logging in to PROCENTER, in addition to authentication using normal user ID and password and IP address restriction.

By entering the password displayed on the smart device on the PROCENTER authentication screen within the expiration date, the password is checked against the password calculated and generated by the PROCENTER side, and if it matches, login is successful.



（２） Preparation in advance for using "TOTP authentication"

For "TOTP authentication", it is necessary to install an application capable of TOTP authentication on the smart device owned by each user in advance.
You must install one of the following authenticator apps.

- Microsoft Authenticator
- Google Authenticator

◆ Download "Microsoft Authenticator "
https://www.microsoft.com/ja-jp/security/mobile-authenticator-app

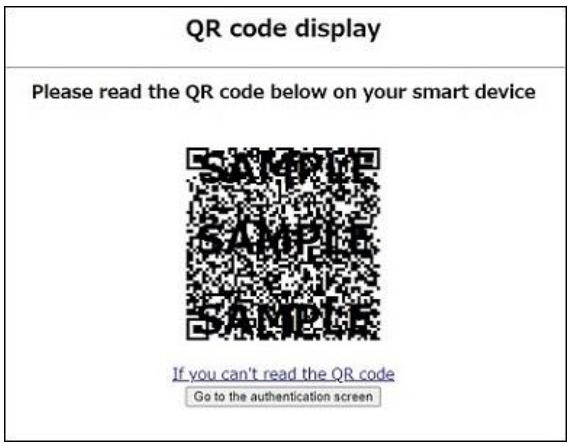
◆ Download "Google Authenticator"
https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

◆ The setting to enable "TOTP authentication" is made by the cabinet administrator.

（３） How to log in "When TOTP authentication is enabled"

1) Access the login URL (https://procenter-global.com/procenter/?tenant=XXXX) with a web browser and display the login screen.
2) On the login screen, enter [User ID] and [Password] and click the [Login] button.
3) The QR code display screen is displayed. (※ Only for the first time.)

【QR code display screen】



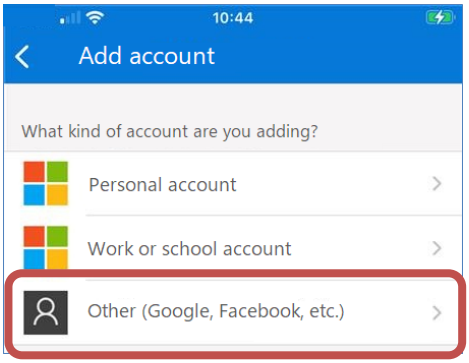
4) Use the smart device's authentication app to scan the QR code.

※ Do not use the camera app of the smart device to read the QR code. Please be sure to start the authentication application and read the QR code.

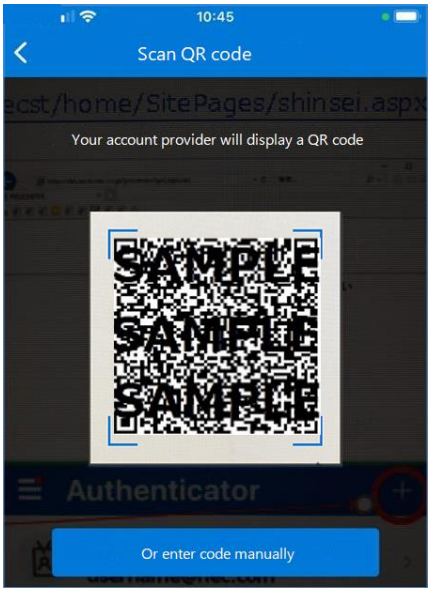
【When reading with "Microsoft Authenticator"】

① Press the + button.

② Select "Other".

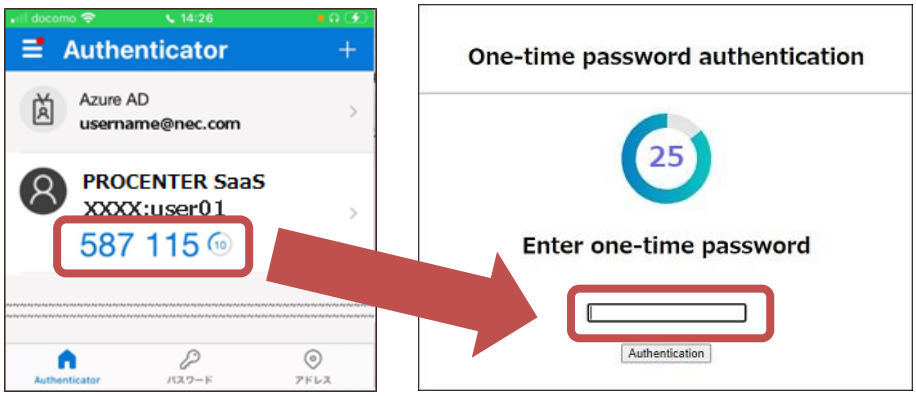


③ Scan the "QR code" of your web browser.



5) After reading "QR Code" is completed, select the [Go to authentication screen] button.

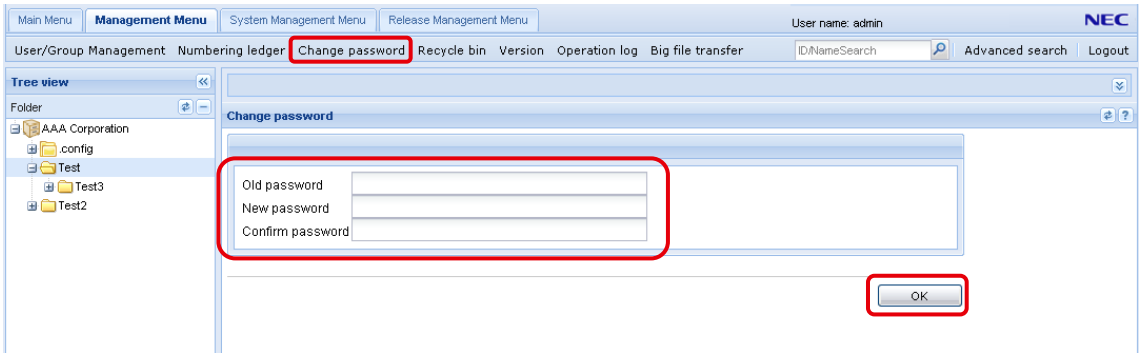
6) After entering the one-time password displayed on the authentication application on the smart device side in the input field on the one-time password authentication screen, click the [Authentication] button. If the one-time password you entered matches, log in.



3.2 Changing of password

You can change password in the following procedures.

1. Click a **[Change password]** of the **"Management Menu"**, "Password change screen" is displayed.
2. Input **[Old password]** and **[New password]**. Input into **[Confirm password]** the same character string as what was inputted into **[New password]**.
3. Click a **[O.K.]** button. Then, changing of password is performed.
   - New password can be used from next login.



——Notes——

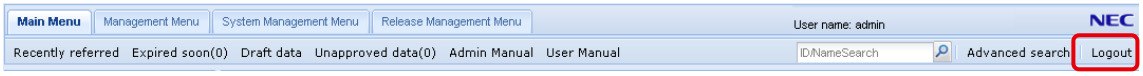
- It is necessary to specify the password 8 characters or more and 16 characters or less.
- It is necessary to specify the password including a number as a password.
- It is necessary to specify the password including a symbols as a password.
- If a password has not been changed for 182 days, a dialog prompting password change will be displayed at the time of login.

3.3 Logout

When operation is completed, be sure to log out in order to prevent incorrect operation. From the menu of the upper area of the screen, re-login screen is displayed by clicking a **[Logout]** button.

■ Logout will be completed if you click a **[Close].**

■ If you click a **[Login]** button, you can log in again.



――Notes――

・ When there is no access for 60 minutes after login, logout processing is performed compulsorily.

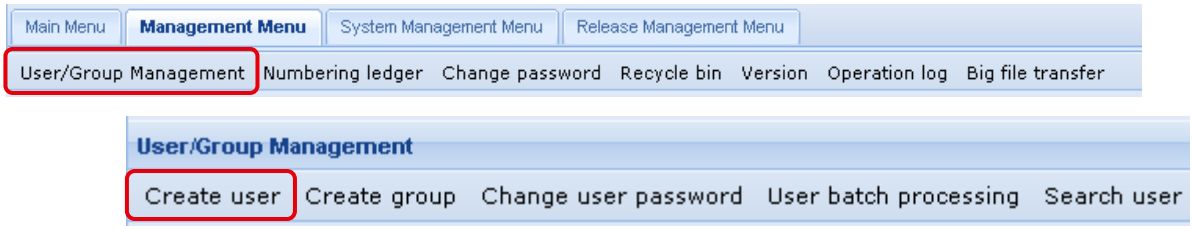
Chapter 4 User management

4.1 User creation

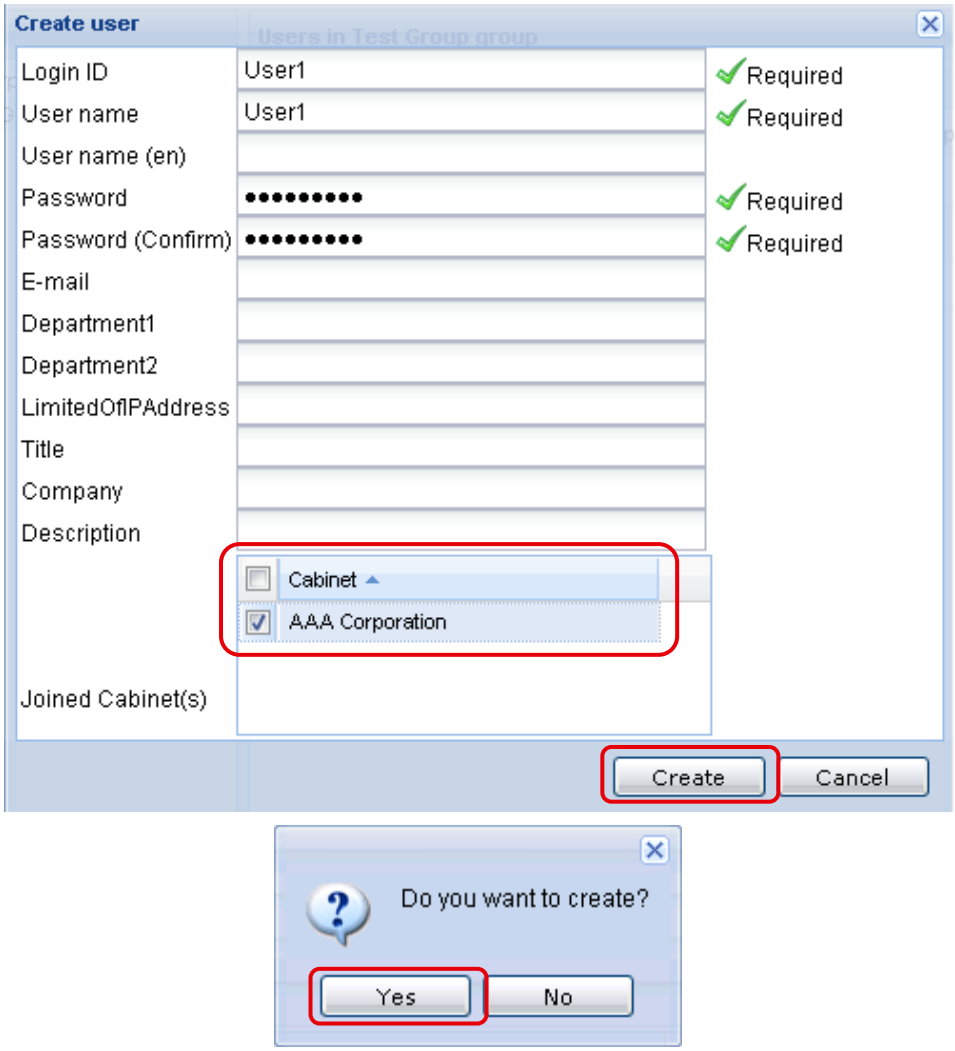
Following, procedure creation (registering) for every user is described.

Operation explanation：

1. Click a **[Create user]** in **[User/Group Management]** of the **"Management Menu"**.



2. If you perform following operation, the check dialog of **"Do you want to create"** is displayed.
   - Input required user information on **"Create User"** screen.
   - Select **[Joined Cabinet(s)]**.
   - Click a **[Create]** button.



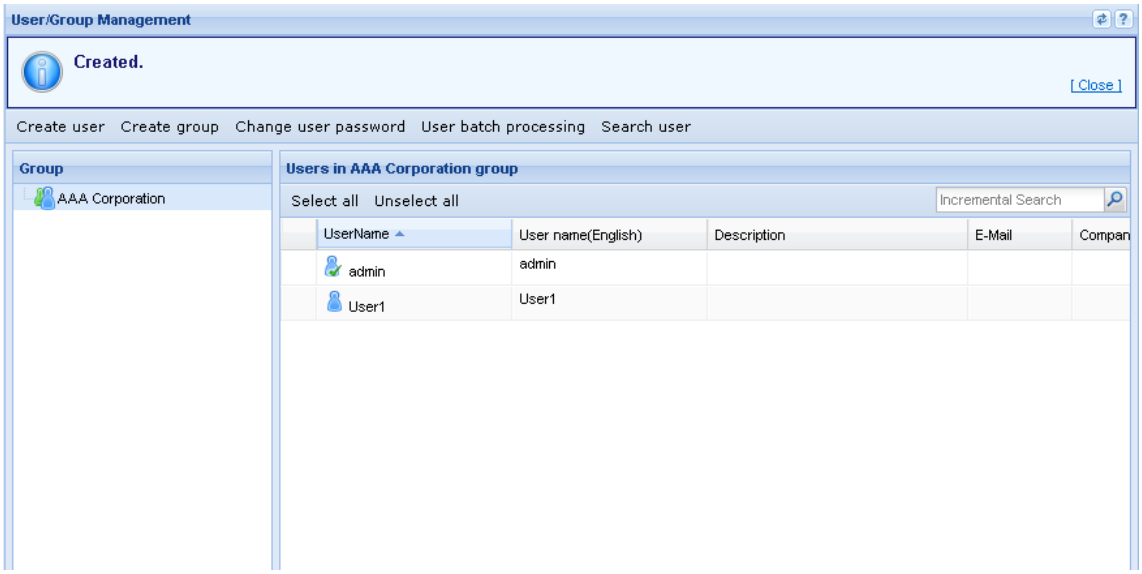
■Property of indispensable specification is as follows at the time of user creation

Property name	Description
Login ID	It is 1-byte alphanumeric character or sign (control character use of TAB, new-line, etc. is impossible) of less than 40 characters. It is necessary to be unique character string within cabinet. It becomes error when it is not unique.
Username (Native language)	Arbitrary character strings (multi-language correspondence). It is not necessary to be unique.
Password	12 to 16 characters long. Must include numbers and symbols.
Confirm password	Same as the above

■Property which is arbitrary specification at the time of user creation

Property name	Description
User name（en）	No more than 256 characters.
Description	No more than 256 characters.
E-mail	You can specify one address. No more than 256 characters.
Title	No more than 256 characters.
Department1	No more than 256 characters.
Department2	No more than 256 characters.
Limited of IP Address	Case where "Access permitted IP Address" is set in cabinet and case where not using IP address filtering function to user individually, set "OFF". ✓ This setting is unnecessary when "Access permitted IP Address" is not set in cabinet.
Company	No more than 256 characters.
Joined Cabinet(s)	

3. Click a **[Yes]** of check dialog, the message **"Created"** is displayed. Created user can be checked by user list of Cabinet group.



4.2 CA role grant and CA role cancellation

CA can give or delete CA role to cabinet member.

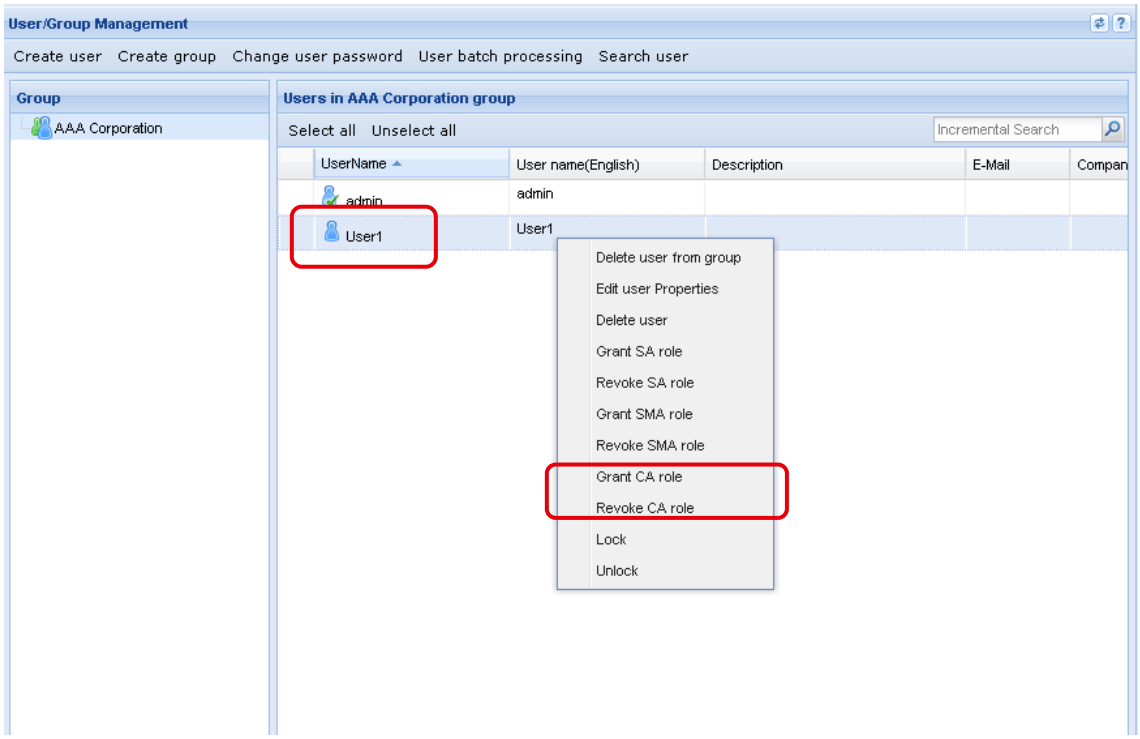
Operation explanation :

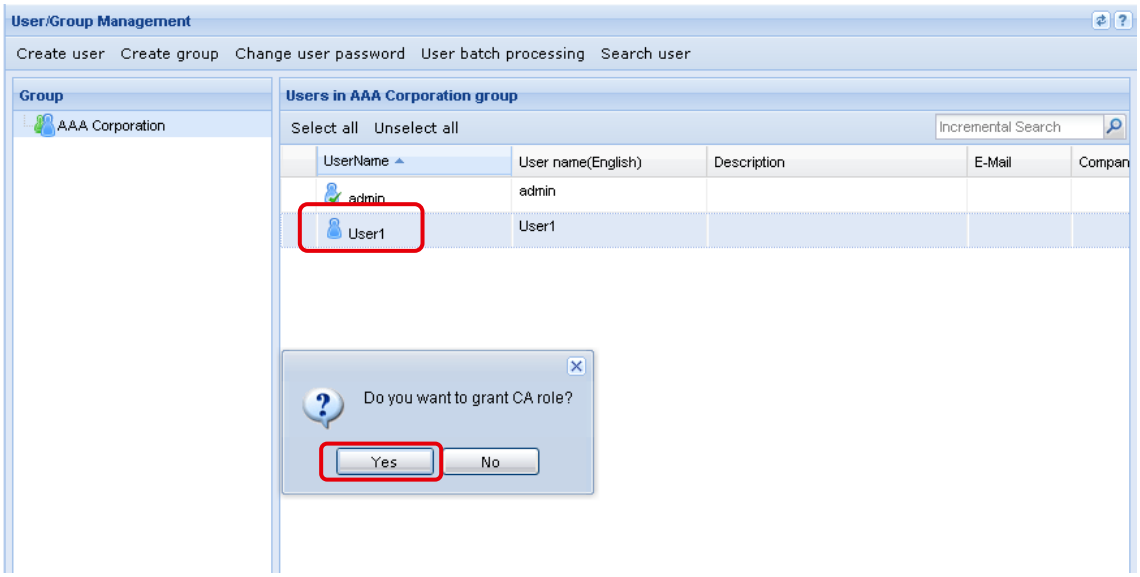
■ Case of CA role grant

1. Specify user you want to give CA role from user list of Cabinet group.
2. Click the **[Grant CA role]** of right-clicking menu.
3. Check dialog of **"Do you want to grant CA role?"** is displayed.
4. Message of **"Grant CA role"** is displayed if you click a **[Yes]**.

■ Case of CA role cancellation

1. Specify user who you want to cancel CA role from user list of cabinet group.
2. You can cancel CA role by clicking **"Remove CA role"** of right-clicking menu.





✓ A mark  which shows that user to whom CA role was given is CA administrator is attached.

4.3 User batch processing

You can perform user batch processing creation / updating by uploading from screen of "User batch processing". You use the CSV file of appointed file format.

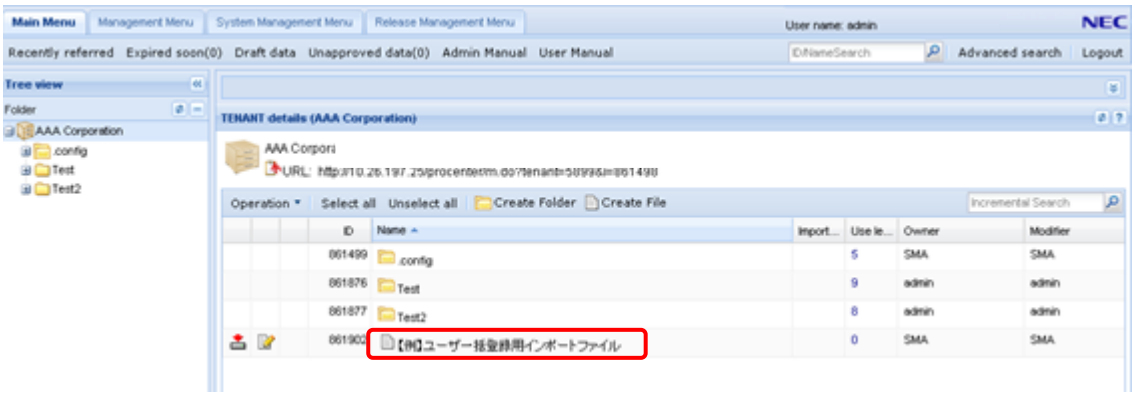
User already registered into cabinet is performed updating of properties, and user who does not exist in cabinet is created newly.

Operation explanation :

1. Creation of the data file for batch process creation

   Sample of CSV for user batch processing (template file for import) is registered into cabinet folder immediately after cabinet delivery.

   (Template file name :【Example】Import file of user batch processing.csv)



Download template file locally. Open the downloaded file by Excel. Edit description item like sample, and named and saved. Character code of description item/file and file format **should observe the following strictly.**

■ **Order of item** :

・The first column is format of entry item.

(Entry example) :

Login ID / User name / Password which is not enciphered / User name / Description/ E-mail / Title / Department 1 / Department 2 / Limited of IP Address / Company

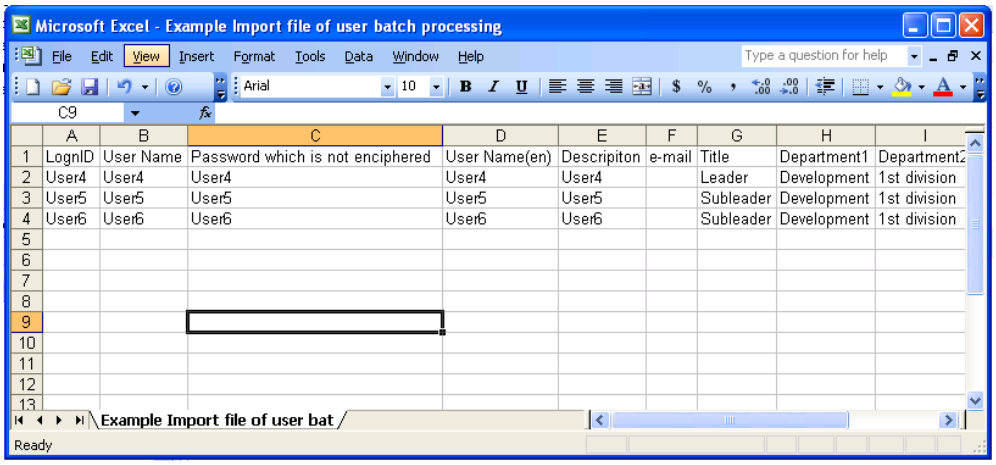
・Edit user information you want to perform batch processing from second line, consulting entry item of template file. Or, make column into blank.

■ **Character code** : UNICODE（UnicodeLittle）

■ **File format** : CSV

■ **Sample :** test_user4.csv

CSV Import file after edit :



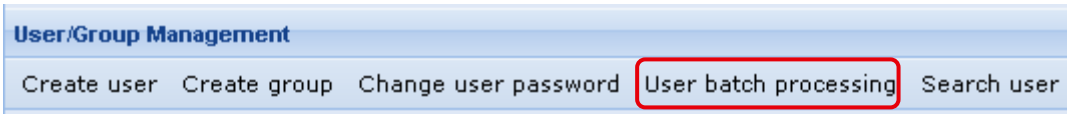
	A	B	C	D	E	F	G	H	I
1	LognID	User Name	Password which is not enciphered	User Name(en)	Descripiton	e-mail	Title	Department1	Department2
2	User4	User4	User4	User4	User4		Leader	Development	1st division
3	User5	User5	User5	User5	User5		Subleader	Development	1st division
4	User6	User6	User6	User6	User6		Subleader	Development	1st division
5									
6									
7									
8									
9									
10									
11									
12									
13									

■Description item of CSV file is as follows.

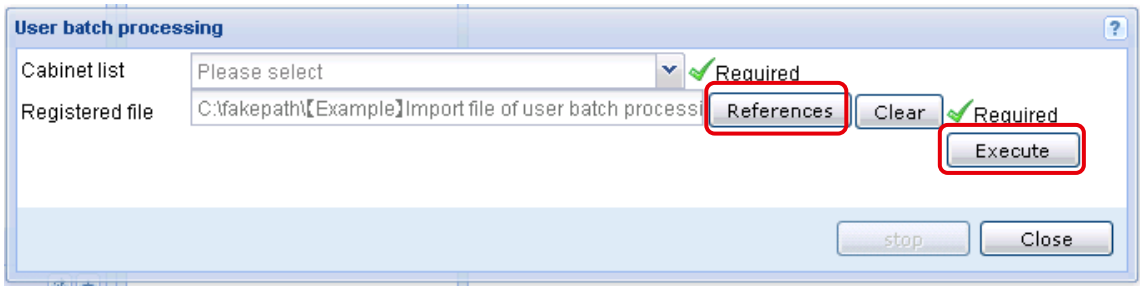
Property name	Description
「Login ID」	Specify one-byte alphanumeric character of less than 40 characters.
「User name」	Specify within 256 characters.
「Password which is not enciphered」	Specify one-byte alphanumeric character of less than 16 characters.
「User name(en)」	Specify within 256 characters.
「Description」	Specify within 256 characters.
「E-mail」	Specify one-byte alphanumeric character of less than 256 characters.
「Title」	Specify within 256 characters.
「Department 1」	Specify within 256 characters.
「Department 2」	Specify within 256 characters.
「Limited IP Address」	Case where "Access permitted IP Address" is set in cabinet and case where not using IP address filtering function to user individually, set "OFF". ✓ This setting is unnecessary when "Access permitted IP Address" is not set in cabinet.
「Company」	Specify within 256 characters.

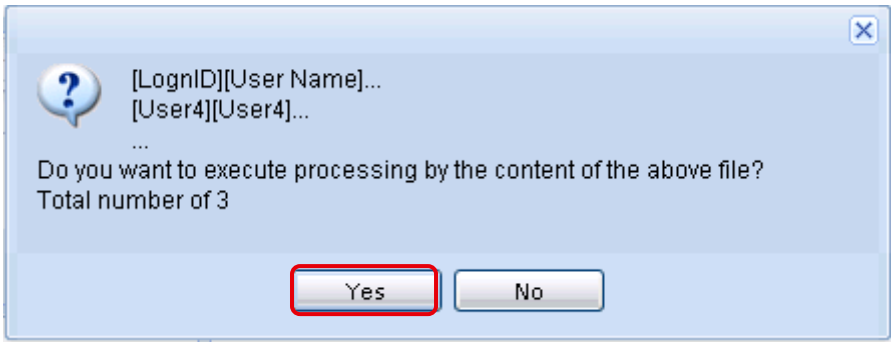
2. Implementation of user batch processing

1) Click a **[User batch processing]** menu in the **"User/Group Management"** of **"Management Menu"**.

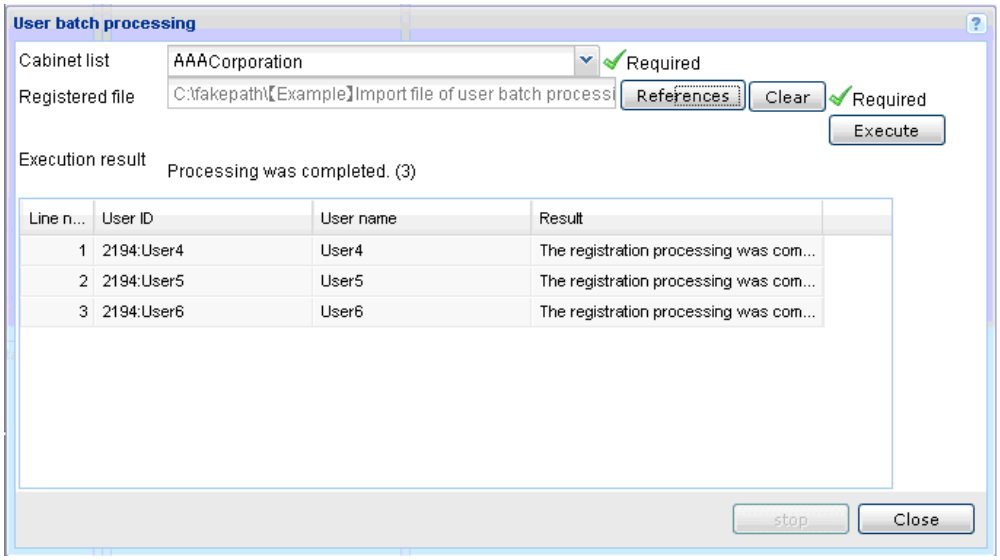


2) You can specify a file if you specify **[Cabinet]** on **"User batch processing"** screen and click a **[Reference]** button. If you click a **[Execute]** button, a check dialog of **[User batch processing]** is displayed.





3) If you click a **[Yes]** of the check dialog, execution result of User batch processing is displayed.



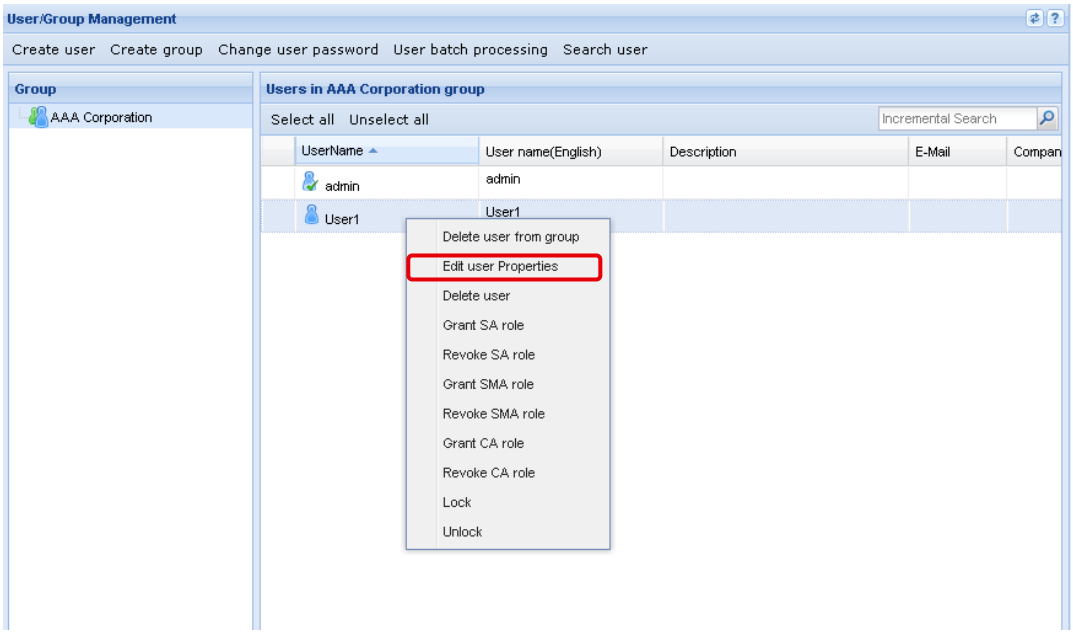
4.4 Changing of user information

You can change Cabinet group member's properties. However, you cannot change User ID.

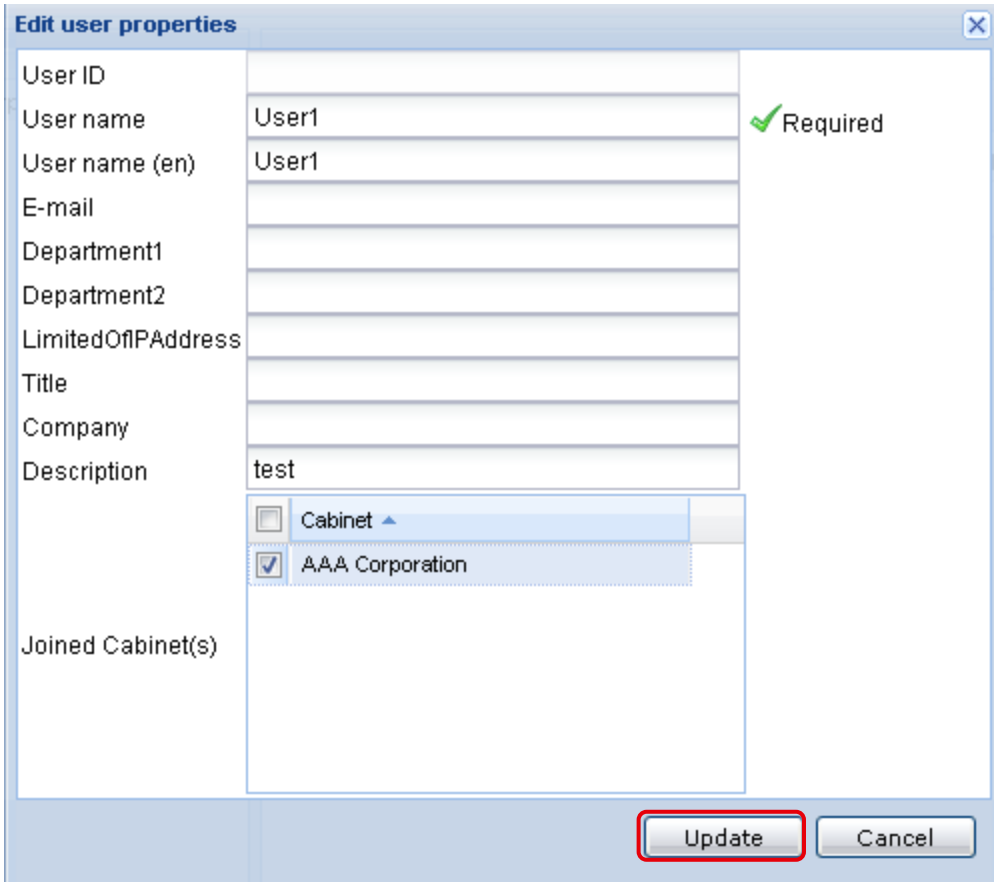
（Refer to 5.1-(1) about explanation of Cabinet group.）

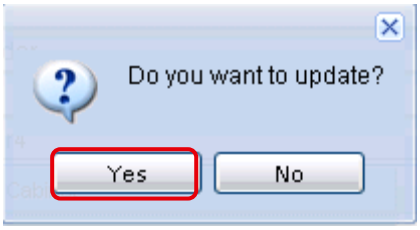
Operation explanation：

1. Specify user you want to edit user information from Cabinet group member list, and click **[Edit user Properties]** of right-clicking menu.



2. If you perform the following on **"Edit user Properties"** screen, a check dialog of **"Do you want to update"** is displayed.
   - Input required item.
   - Select joined cabinet.
   - Click a **[Update]** button.
     (User ID cannot be changed.)



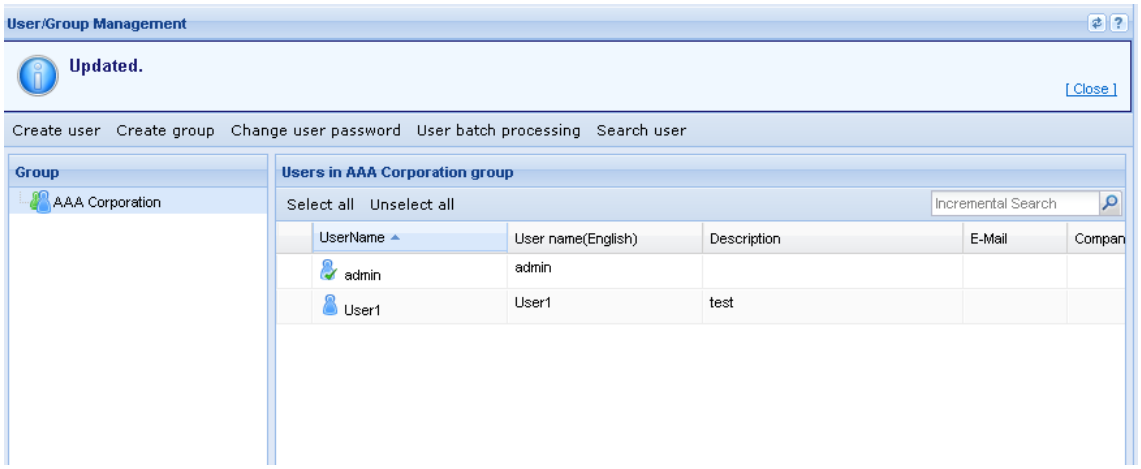


■ Editing properties are as follows at the time of user information changing.

Property name
「User ID」
「User name」
「User name（en）」

「E-mail」
「Title」
「Department 1」
「Department 2」
「Limited of IP Address」
「Company」
「Description」
Joined Cabinet(s)

3. If you click a **[Yes]** of the check dialog, user information is updated. You can check updated user information by user list of cabinet group.



4.5 Change of the Owner at the time of user deletion

（1）User deletion

You can select user from cabinet group member lists, and can delete member.

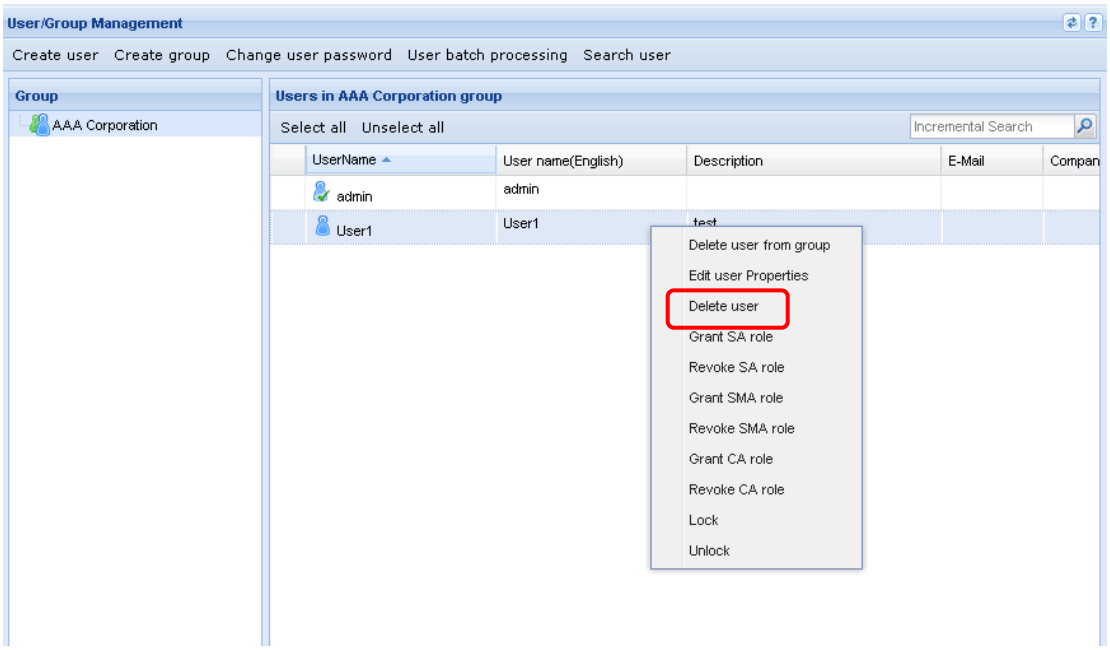
（2）Owner changing

You can change owner (Owner) of folders / files at the time of user deletion (taking over to other users or groups). Items to be carried over, is "owner", "lock owner", "access rights" and "default owner". In addition, when “Access control” is already set as taking over users or groups, only strong “Access control” is set.

Operation explanation：

1) Specify user you want to delete from Cabinet group member.

2) Click a **[Delete user]** of right-clicking menu, then "**[Delete user]** screen" is displayed.



✓ It becomes impossible to register again by same ID as deleted user when **[Delete User from Group]** is performed with right-clicking menu. So, when you delete user, select and be sure to perform **[Delete user]**.

Be sure to perform Owner changing before performing user deletion. When you set Owner, perform the following.

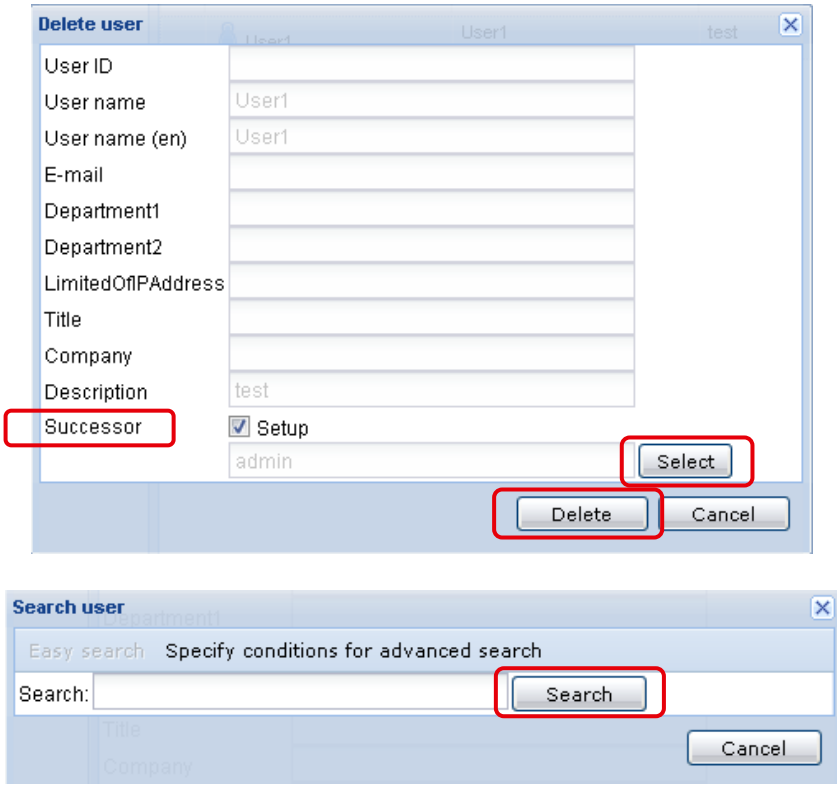
① Check to a check box **"Successor " [Setup]**.

② Click a **[Select]** button.

③ Specify a **[Successor]** by **[Search user]**.

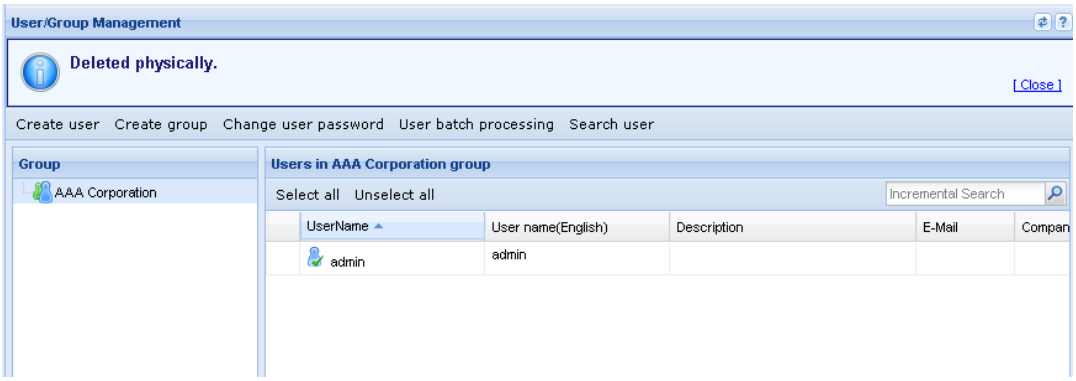
④ Click a **[Delete]** button.

(Default alternative user becomes operator (CA).)



3) A check dialog of **"Are you sure you want to delete?"** is displayed.

4) If you click a **[Yes]** of the check dialog, message of **"Removed physically"** is displayed.



4.6 *Locking and unlocking of user*

In order to eliminate unjust (unfair) login, user locking and unlocking function are offered.

In addition, to users in cabinet group, you can perform locking or unlocking manually. Moreover, locked users cannot log in to Service until unlocked.

■Assessment of user locking

Assessment of locking is performed only at the time of login. And it can be continuously used until user performs logging out or session timeout, when locked after login.

- Locked user also counts as one user on license.

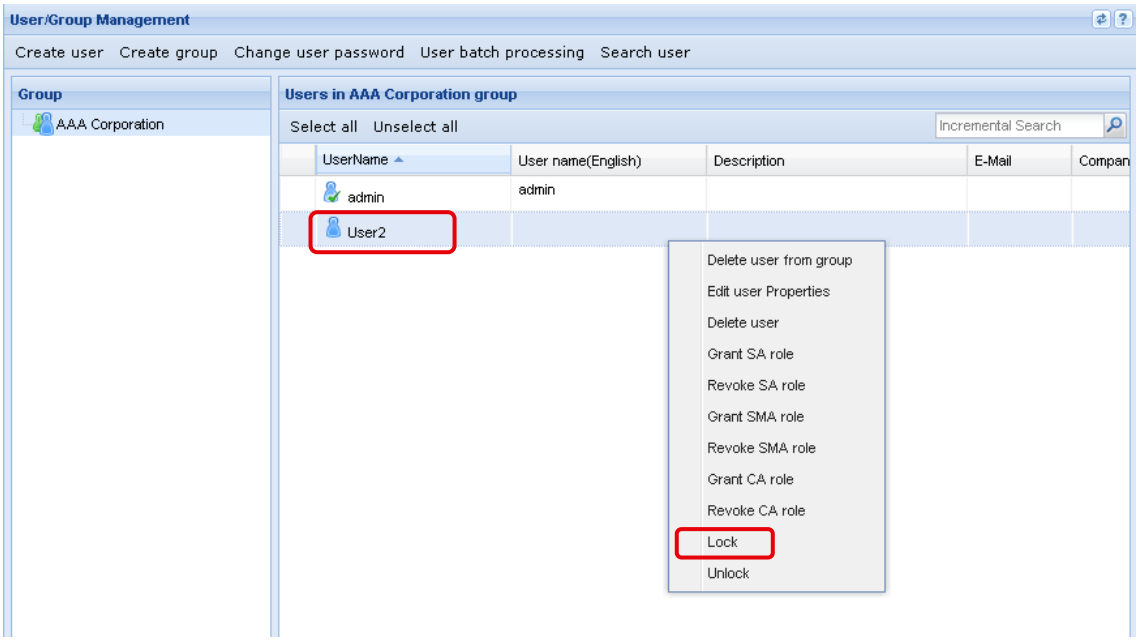
（1） User locking

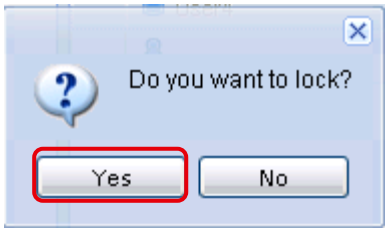
A user who does not log in for 180 days is locked automatically. CA needs to perform unlocking manually.

✓ (In this Service, if it passes 180 days without logging in once after user creation, user locking is carried out similarly.)

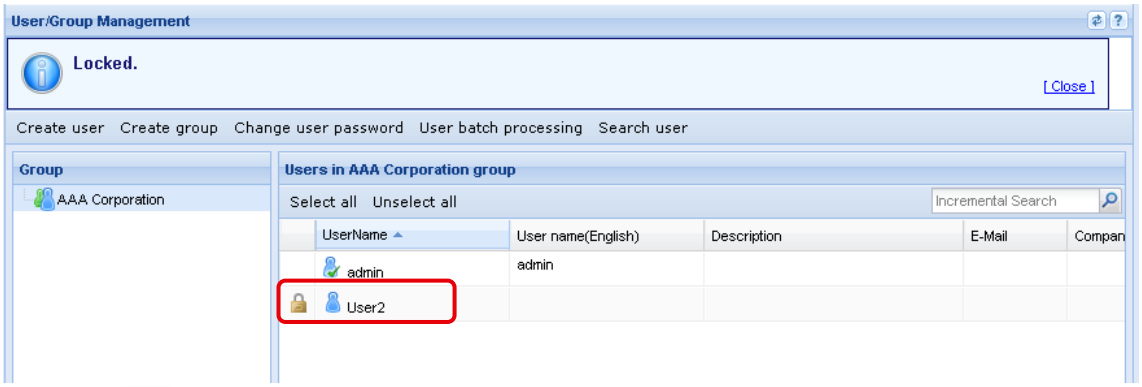
Operation explanation：

1. Specify target user you want to lock from user list of cabinet groups, and click **[Lock]** of right-clicking menu.
2. A check dialog of **"Do you want to lock?"** is displayed.



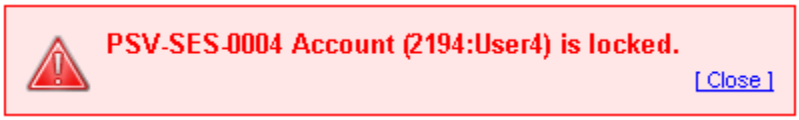


3. If you click a **[Yes]** of the check dialog, message of "Locked" is displayed.



※ A lock mark is attached to the locked user.

4. If locked user logs in on login screen, error message is displayed and cannot log in.



(2) User unlocking

You can perform user unlocking by following procedure.

Operation explanation :

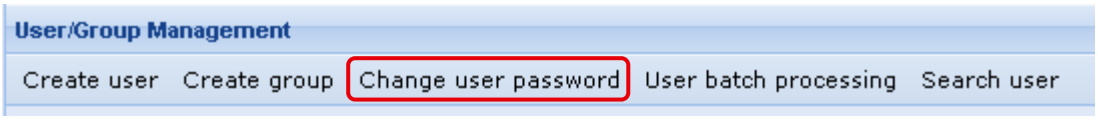
1. Specify user you want to perform unlocking and click a **[Unlock]** with right-clicking menu.
2. A check dialog of **"Do you want to unlock?"** is displayed.
3. If you click a **[Yes]** button, unlocking is performed.

4.7 User password changing

When Cabinet group members forget the login password, you can publish password again.

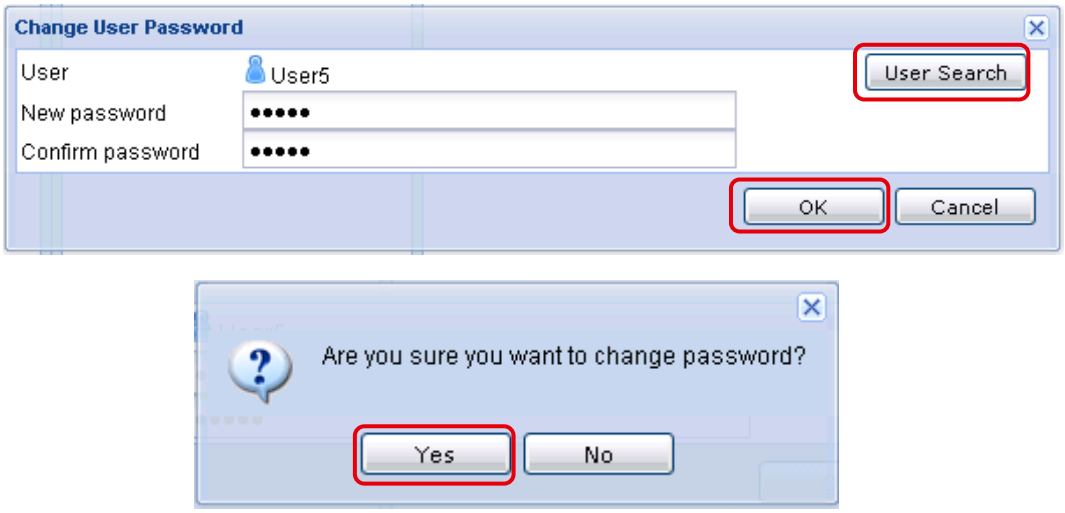
Operation explanation :

1. Click a **[Change user password]** of **"Management Menu"** in **[User/Group Management]**.

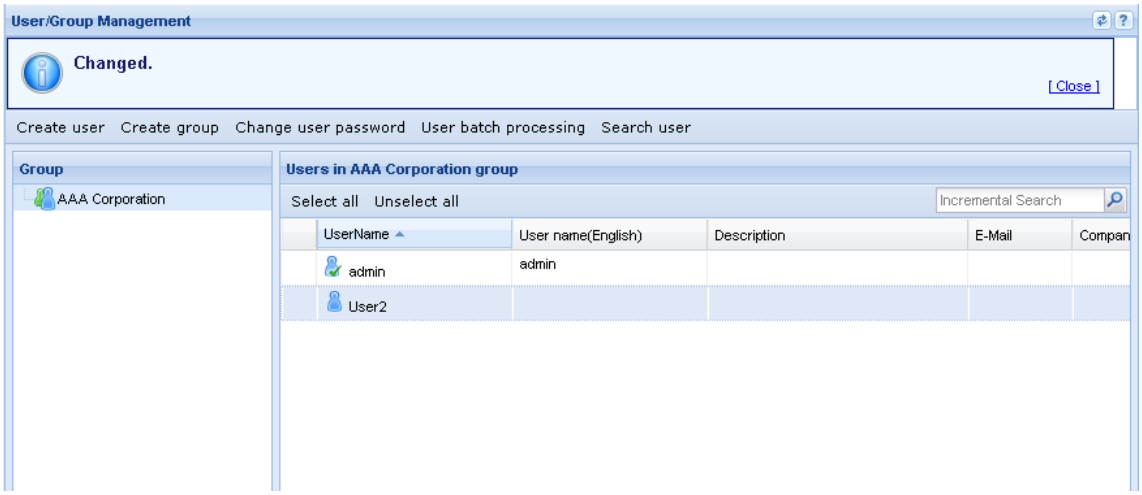


2. Click a **[User Search]** button on **"Change User Password"** screen, and specify user you want to make password changing.

3. Input **[New password]** and **[Confirm password]**, and click a **[O.K.]** button. A check dialog of **"Are you sure you want to change password"** is displayed.



4. Click a **[Yes]** of the check dialog. Then, message of "Changed" is displayed.



✓ Recommend member changing of password after login with the password after publish again.

4.8 Enabling and disabling TOTP authentication for users

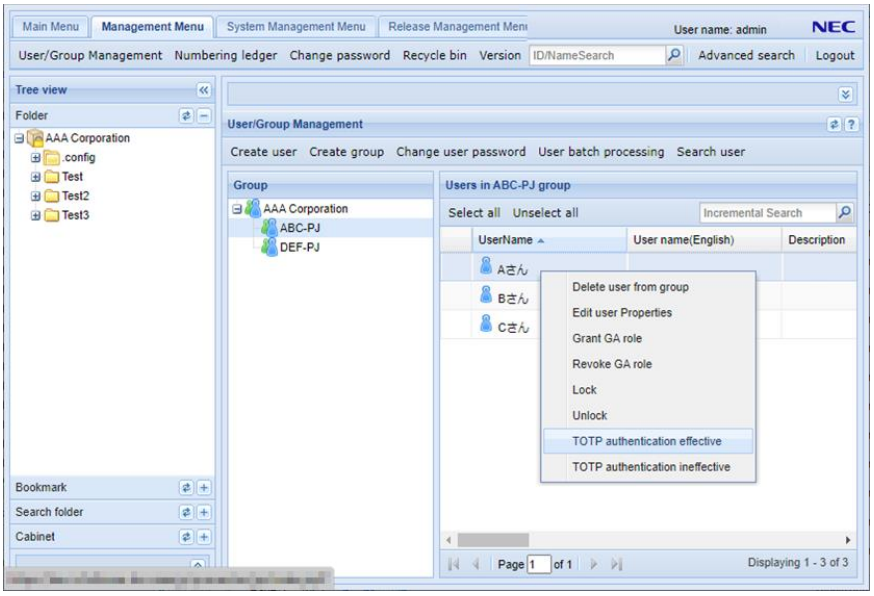
Set TOTP authentication to enable or disable. There are two setting methods: "Individual setting" and "Bulk registration".

4.8.1 Individual Settings

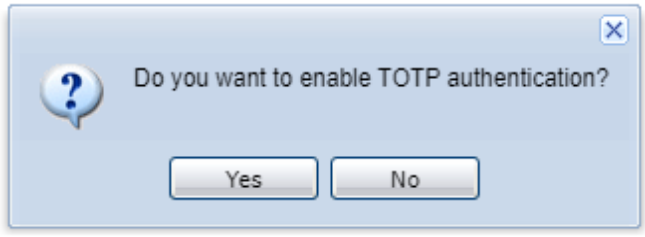
The administrator user sets the enable/disable of TOTP authentication for each user on the user list screen. The default setting is TOTP authentication disabled (one-time password input is not required).

（1） Activation Procedure

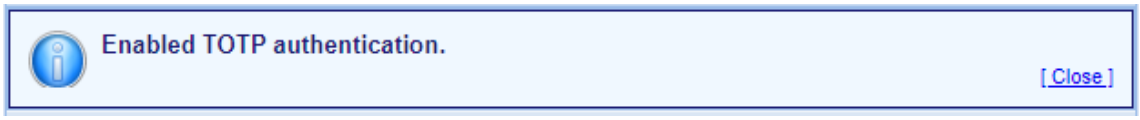
① Select the target user (multiple selections) in "User List" and click "Enable TOTP authentication" in the right-click menu.
https://procenter-globa.com/procenter/?tenant=XXXXX



② Click "Yes" on the "Are you sure you want to enable TOTP authentication?" screen.

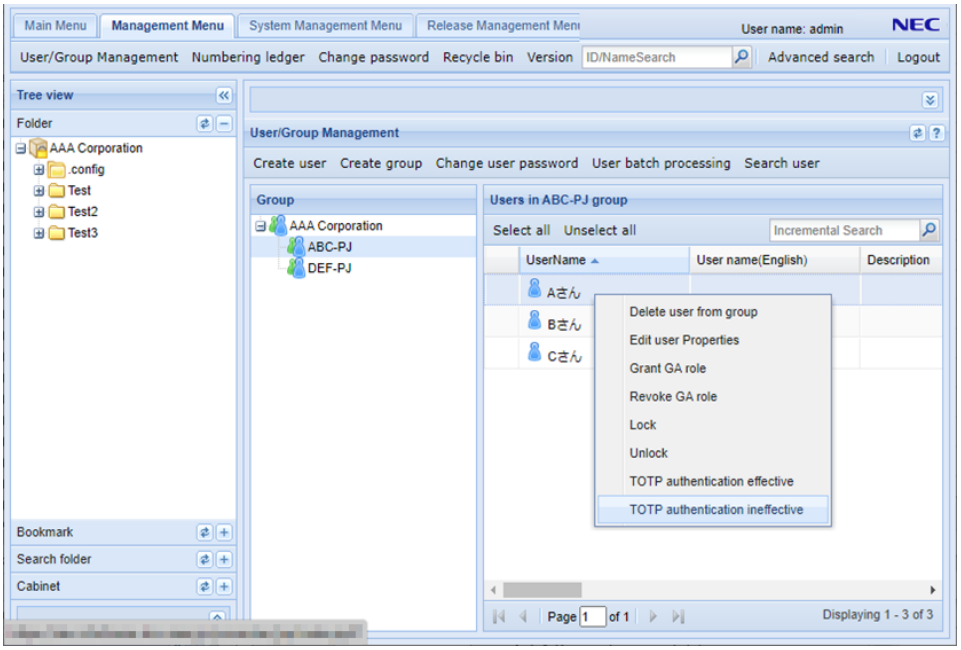


③ The execution result is displayed.

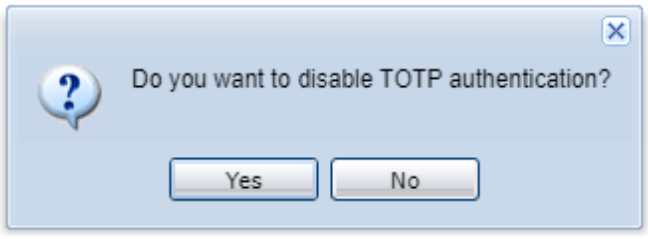


（2） Deactivation procedure

① Select the target user (multiple selections) in the "User List" and click "Disable TOTP authentication" in the right-click menu.



② Click "Yes" on the "Are you sure you want to disable TOTP authentication?" screen.



③ The execution result is displayed.

4.8.2 Bulk Registration

With the batch user registration on the user list screen, it is possible to set it together using CSV.

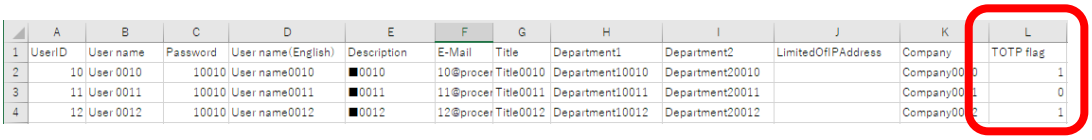
※ IT IS ASSUMED THAT USER MANAGEMENT IS PERFORMED IN EXCEL.

※ The batch download function of user information is being prepared for provision.

※ Multiple specifications can be made from the screen and TOTP authentication can be turned ON / OFF, so please use it.

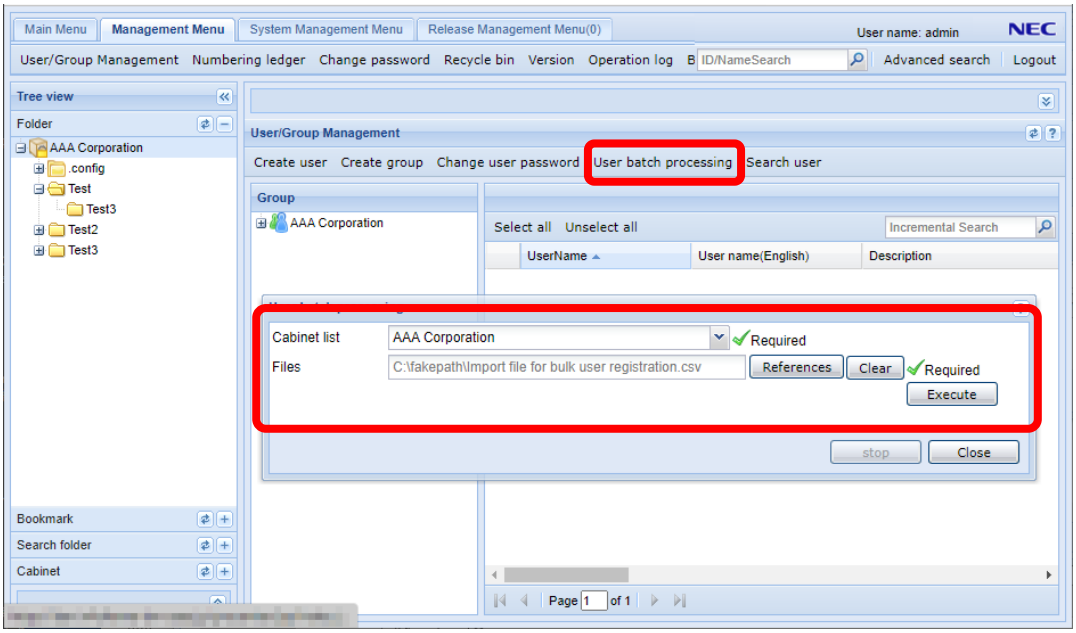
(1) "Batch user registration" procedure (enable/disable)

① Add "TOTP authentication flag" to the final column (column 12) of the CSV.
The setting values are "Enabled: 1" and "Disabled: 0".
※If you do not want to update the TOTP authentication settings, the "TOTP Authentication Flag" column is not required.

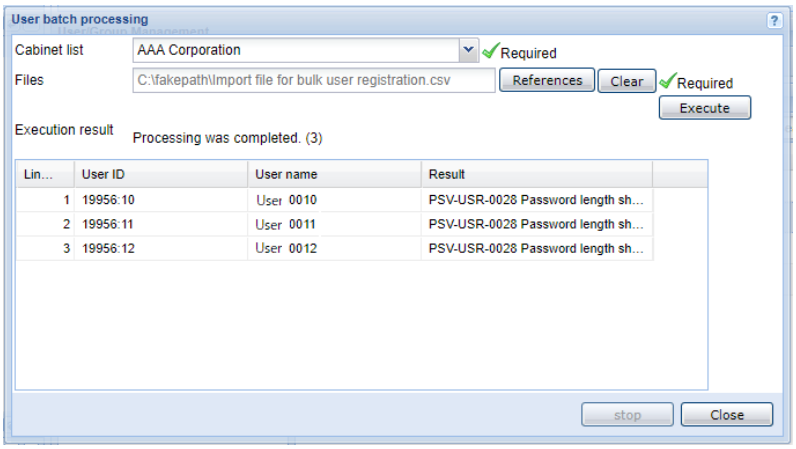


	A	B	C	D	E	F	G	H	I	J	K	L
1	UserID	User name	Password	User name(English)	Description	E-Mail	Title	Department1	Department2	LimitedOfIPAddress	Company	TOTP flag
2	10	User 0010	10010	User name0010	■0010	10@proce	Title0010	Department10010	Department20010		Company00	1
3	11	User 0011	10010	User name0011	■0011	11@proce	Title0011	Department10011	Department20011		Company00	0
4	12	User 0012	10010	User name0012	■0012	12@proce	Title0012	Department10012	Department20012		Company00	1

② Select a cabinet in the batch user registration, specify CSV in the registration file, and execute it.

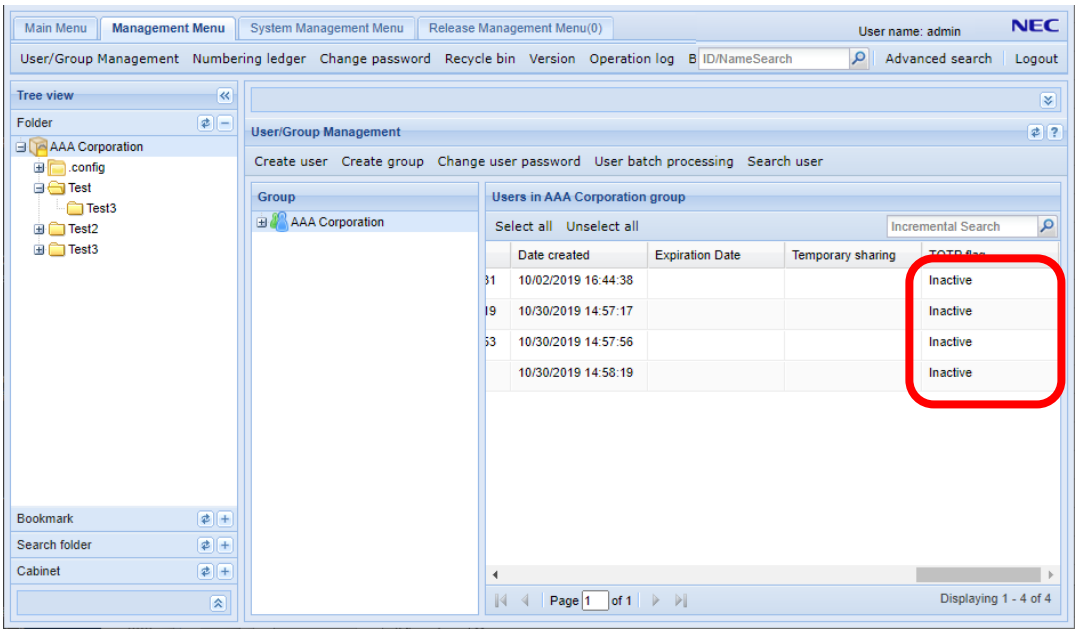


③ The execution result is displayed in a list.



4.8.3 How to check the setting status of TOTP authentication

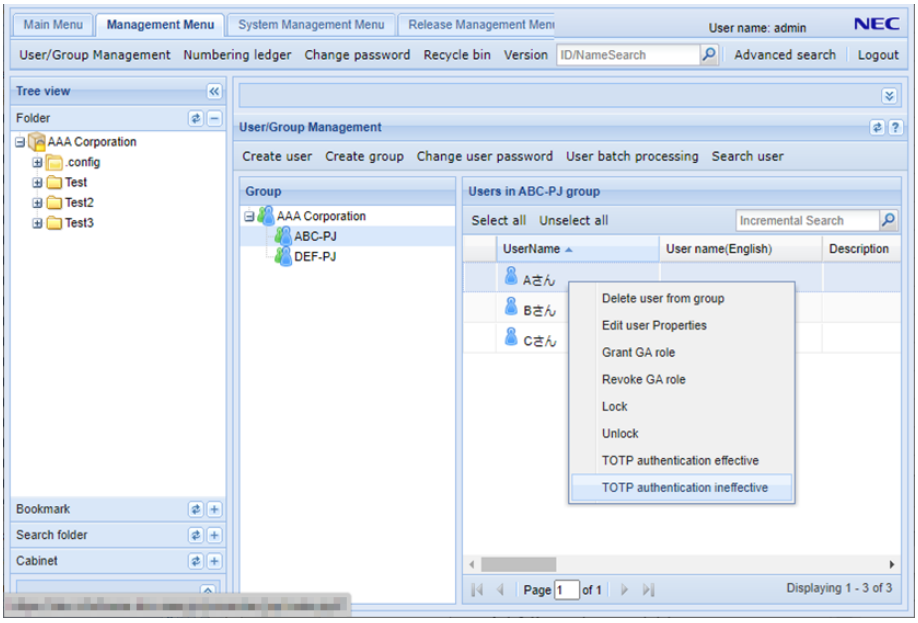
You can check the TOTP authentication status (enabled/disabled) with the TOTP authentication flag in the user list.



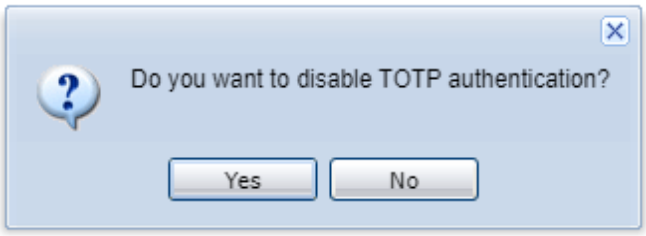
4.8.4 How to reset TOTP authentication

If you need to read the QR code again, such as when changing your mobile device or when the one-time password does not match, reset the TOTP authentication setting. For the setting method, set TOTP authentication to "Disabled" on the user list screen and then set it to "Enabled" again.

① Select the target user in the user list (multiple selections are possible), and click "Disable TOTP authentication" in the right-click menu.



② Click "Yes" on the "Are you sure you want to disable TOTP authentication?" screen. A message of the execution result is displayed.



③ Select the target user in the user list (multiple selections are possible) and click "Enable TOTP authentication" in the right-click menu.

④ Click "Yes" on the "Are you sure you want to enable TOTP authentication?" screen. A message of the execution result is displayed.

Chapter 5 Management of group

CA can create a group (Local group) which summarized two or more users in Cabinet group, and can add or delete member to created Local group. Moreover, it is also possible to specify group as “Access control” or Owner. However, it is impossible to log in to this Service by group.

5.1 Classification of group

Group is classified into “Cabinet group” and “Local group”.

(1) Cabinet group

Cabinet group cannot be referred to from other cabinet users. CA can change member in the Cabinet group from which self serves as CA.

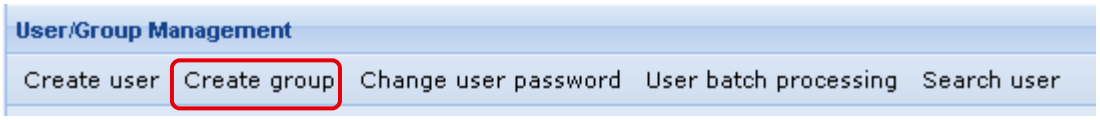
(2) Local group

It is the group defined within cabinet. Cabinet can have two or more Local groups. Local group cannot be referred to from other cabinet users. Moreover, users of other cabinets cannot be added to the local group. Therefore, composition member of the Local group always belong to Cabinet group.

5.2 Local group creation and setup of local group administrator

CA can create a Local group limited in a cabinet, and can set users in Local group as Local group administrator (GA).

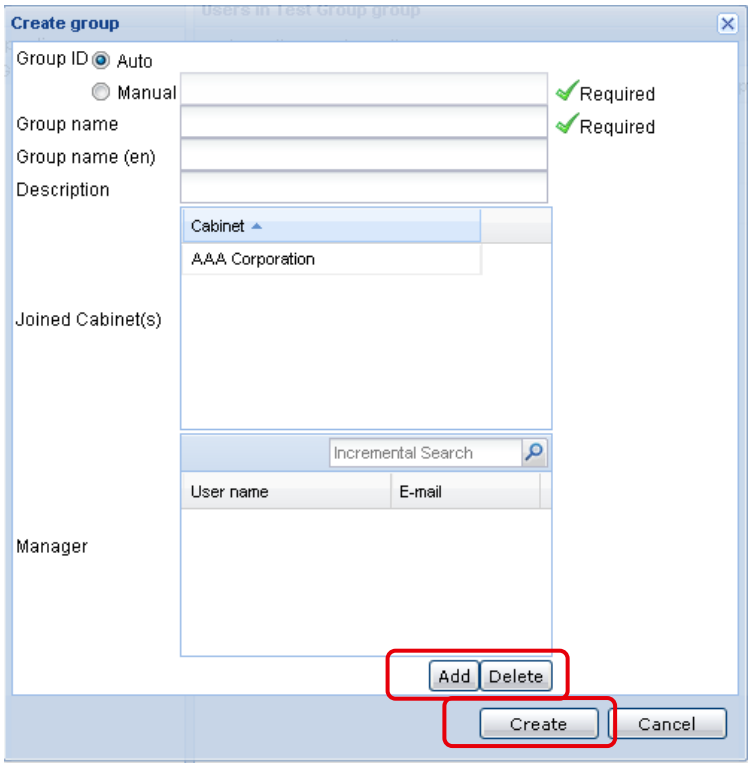
1. Click a **[Create group]** in the **[User/Group Management]** of **"Management Menu"**. **"Create group"** screen is displayed.



2. Input required information on **"Create Group"** screen.
   When you set Local group administrator (GA), perform the following.

- ➢ Click a **[Add]** button.
- ➢ Specify user by user search.
- ➢ Click a **[Create]** button.

- ✓ Local group administrator can be set by searching and adding user.
- ✓ You can delete administrator (GA), if you check local administrator currently displayed and click a **[Delete from list]** button.



You can specify following properties at the time of Local group creation.

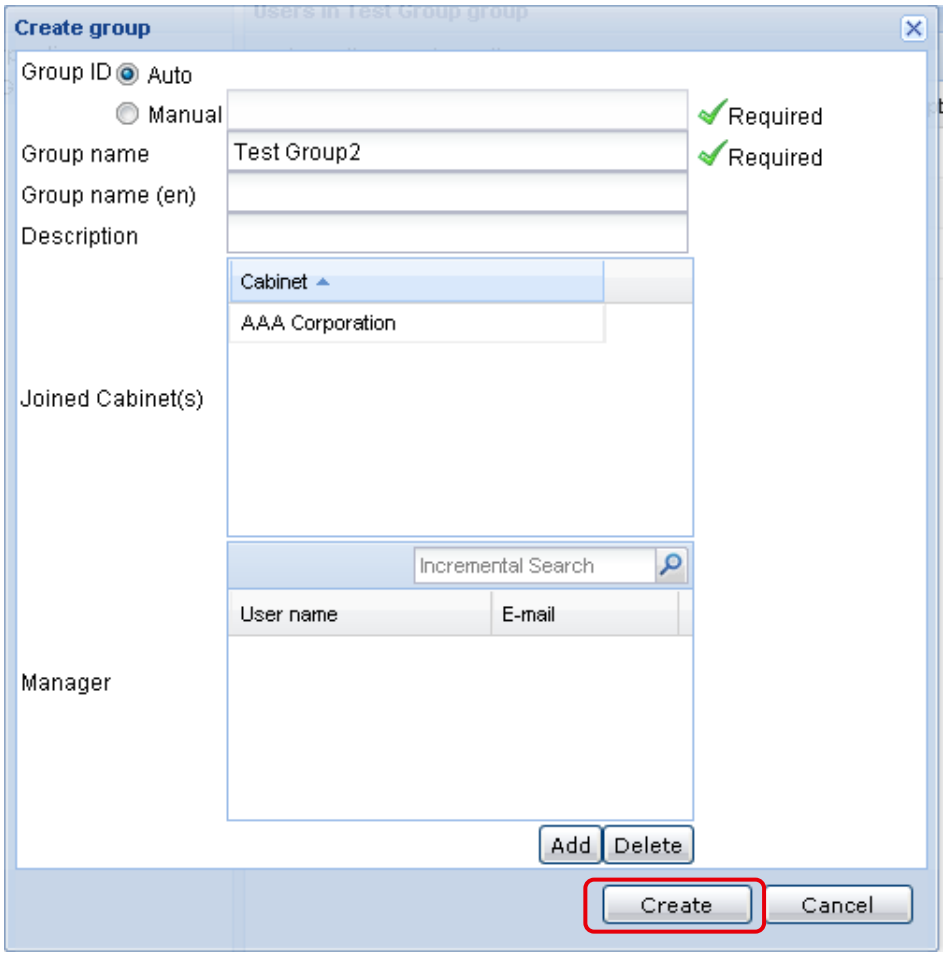
■Property of indispensable specification at the time of group creation.

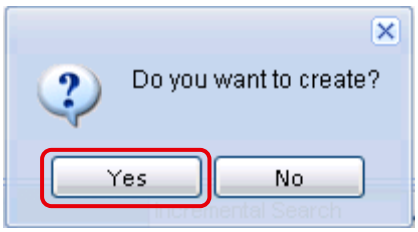
Property name	Description
Group ID	1. Auto : Service creates unique ID automatically. 2. Manual: One-byte alphanumeric character or sign of less than 50 characters（Control characters, such as TAB and new-line, are not included.）and unique character string within Service.
Group name（Native language)	Arbitrary character strings (multi language correspondence). It is not necessary to be unique.

■Property of arbitrary specification at the time of group creation.

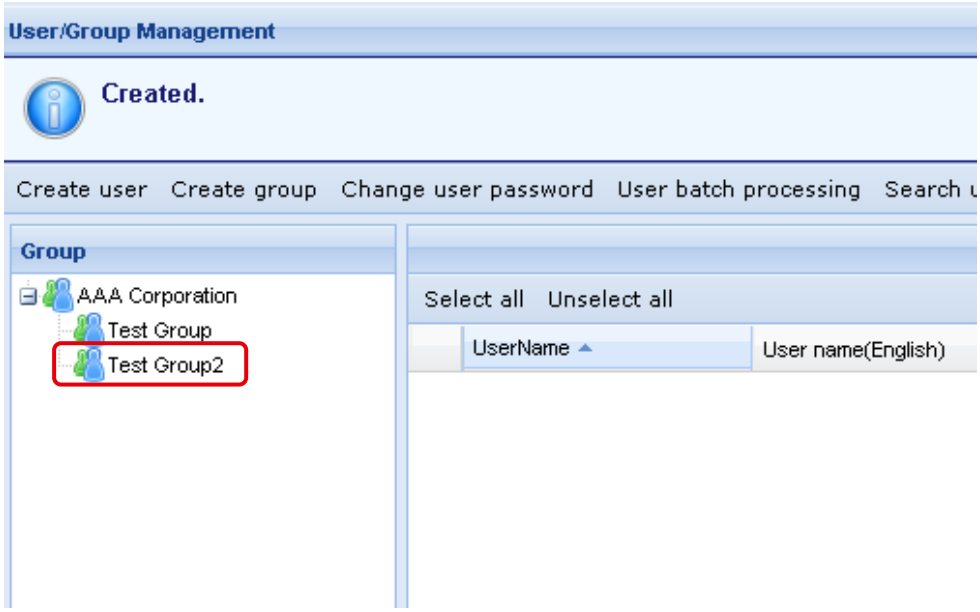
Property name	Description
Group name（en）	
Description	
Joined Cabinet(s)	

3. If you click a **[Create]** button, a check dialog of **"Do you want to create?"** is displayed.





4. If you click a **[Yes]** of the check dialog, message of **"Created"** is displayed. Local group created in the Cabinet group is displayed on **[Group Select]**.



5.3 Management of Local group

CA can perform the following to Local group.

- Changing of properties of each Local group.
- Addition of affiliation member.
- Deletion in self-cabinet.

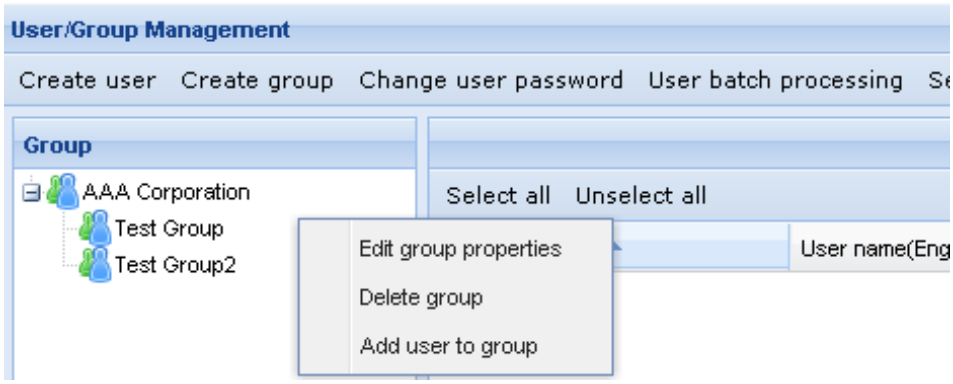
Group ID cannot be changed. (GA can manage affiliation member within self-local group.)

- You can perform addition of group member within the limits of user you can refer to.
- Member changing of group has the following two kinds of methods.
  - ✧ Addition or deletion of users who belongs to group
  - ✧ Addition or deletion of groups which belongs to user.

5.3.1 Changing of properties of group

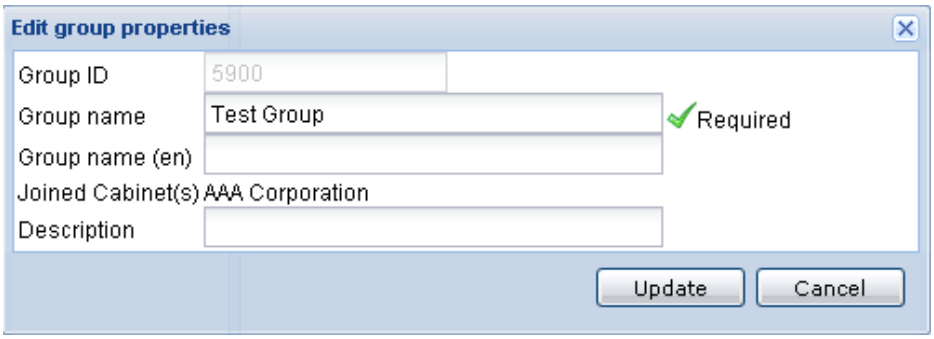
Operation explanation :

1. Specify local group to change and click a **[Edit group properties]** of right-clicking menu.

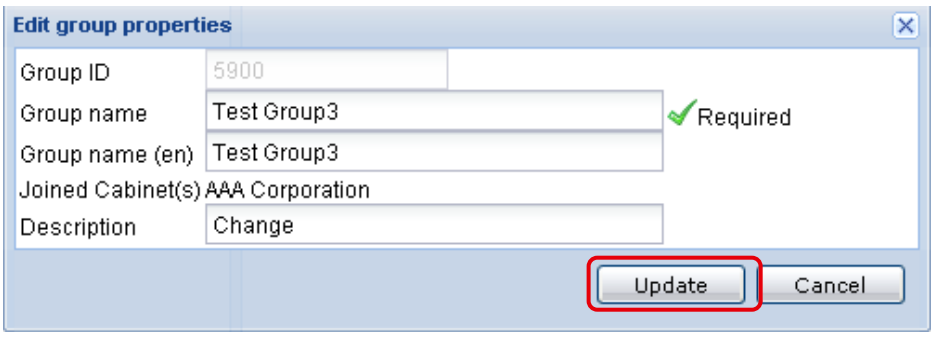


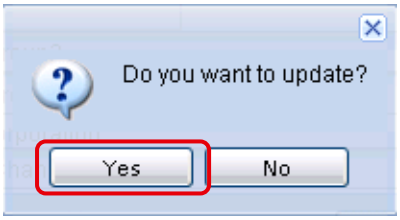
2. Edit item of **[Group name]**, **[Group name (en)]**, and **[Description]** on **"Edit group Properties"** screen.

■Group information before edit



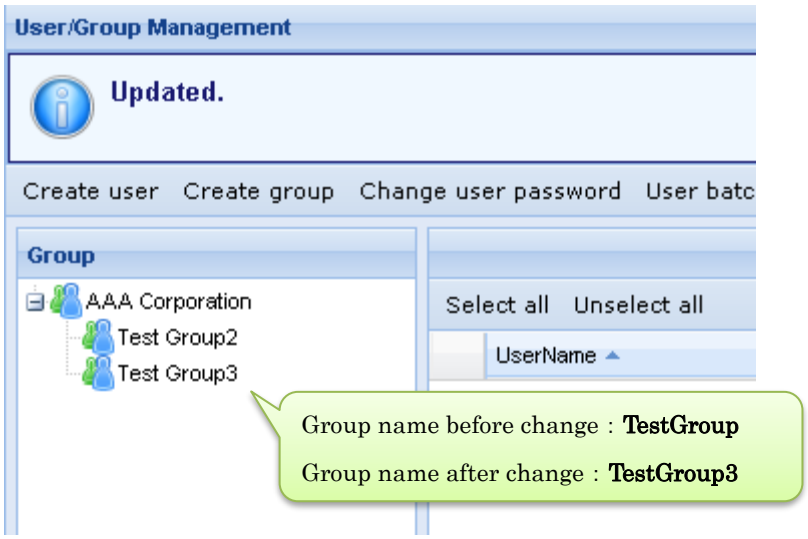
■Group information after edit





If you click a **[Update]** button, a check dialog of **"Dou you want to update?"** is displayed.

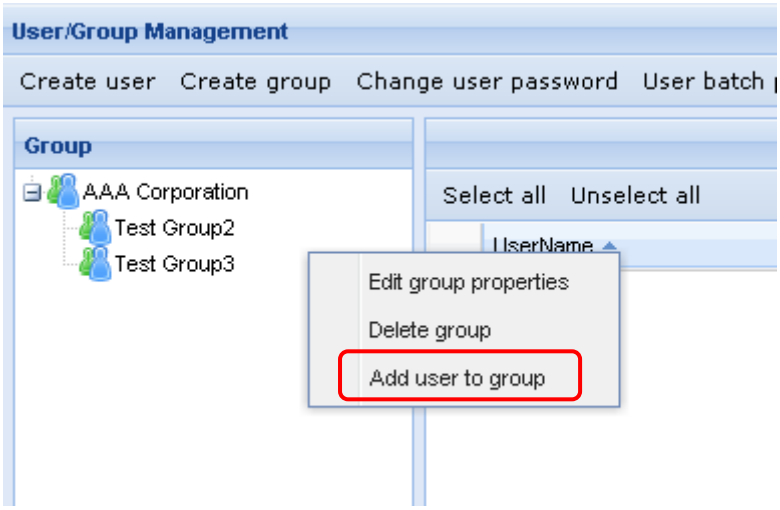
3. If you click a **[Yes]** of the check dialog, message of **"Updated"** is displayed.



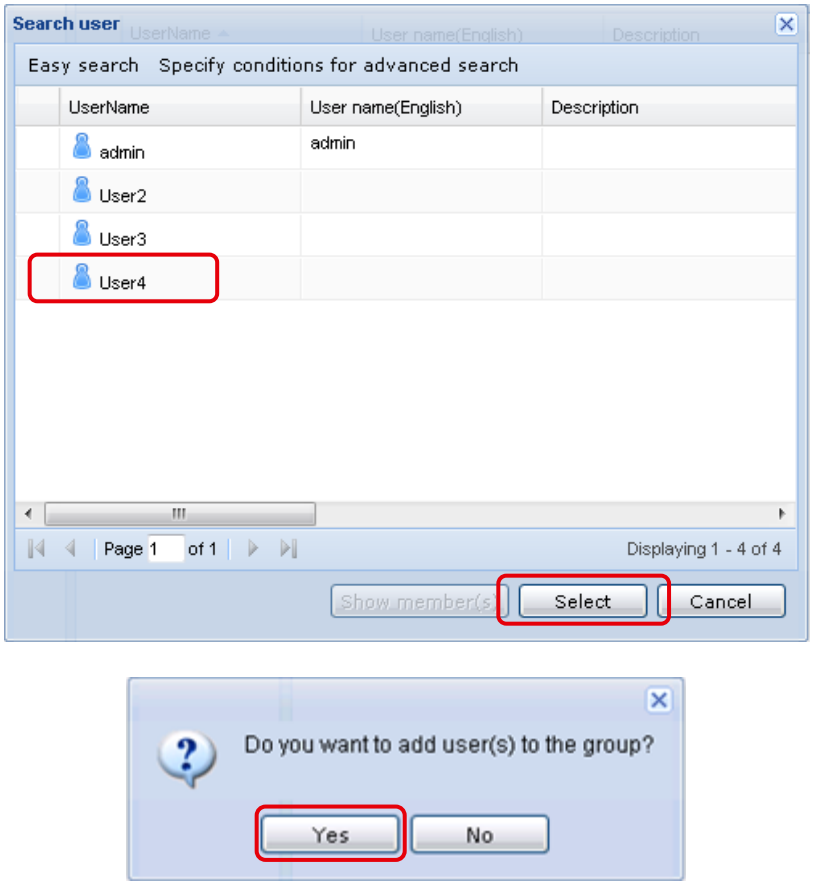
5.3.2 Member addition in group

Operation explanation :

1. Specify local group and select a **[Add user to group]** of right-clicking menu.

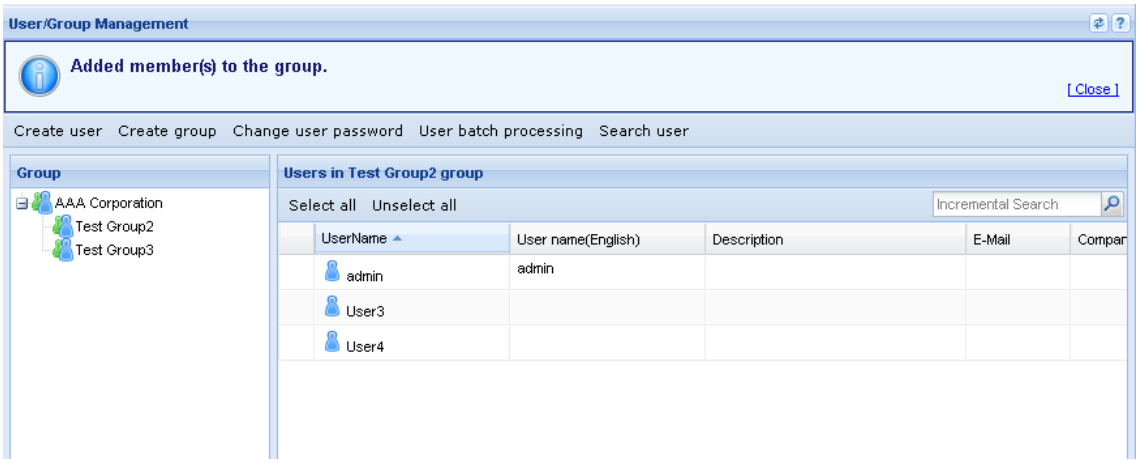


2. Specify member you want to add to group from cabinet group member by **[User Search]**.



If you click a **[Select]** button, a check dialog of **"Do you want to add user(s) to group?"** is displayed.

3. If you click **[Yes]** of the check dialog, message of **"Added member(s) to the group"** is displayed.



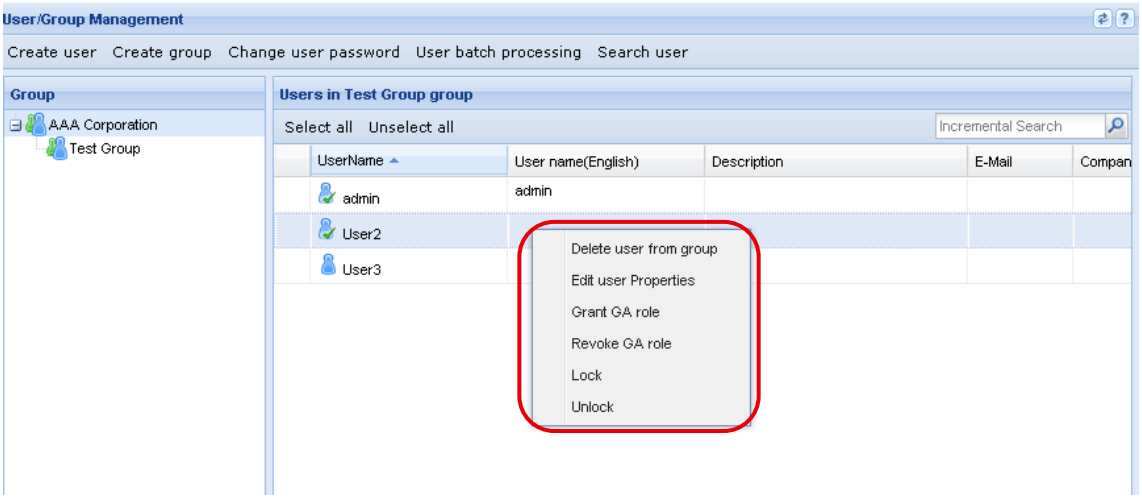
5.3.3 User management (inside of local group)

User with authority that can create local group can manage all users in Local groups within the ambit.

- Delete user from group
- Grant of GA role, and deletion of GA role
- Locking and unlocking

Operation explanation :

1. Specify user from user list of target Local groups. All users in the Local groups are manageable by menu displayed by right-clicking.



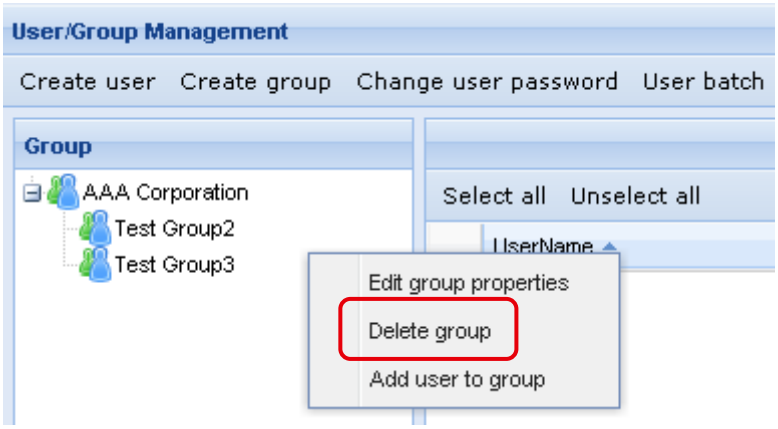
- Delete User from group : You can delete user from group. (Multi deletion is also possible.)
- Grant GA Role : You can give GA role to user.
- Revoke GA Role : You can cancel GA role to user.
- Lock : You can lock user. If user is locked, user becomes impossible to log in to this Service.
- Unlock : You can cancel user locking.

5.4 Local group deletion

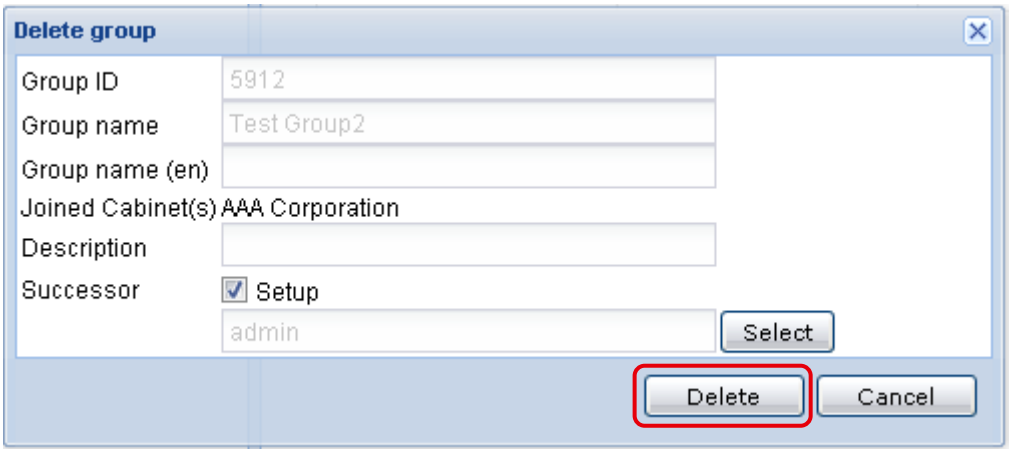
If deletion of group is performed, Owner of data with which applicable group is owner is changed CA or GA who operate. When you change into other users and groups, specify alternative users or groups at the time of group deletion. In addition, when “Access control” is already set as alternative users or groups, only strong “Access control” is set.

Operation explanation：

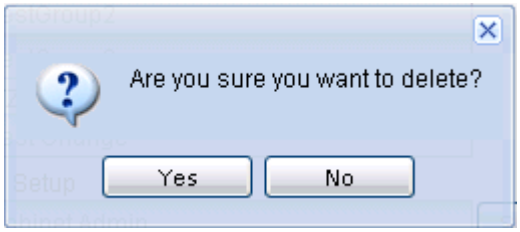
1. Specify Local group you want to delete and click a **[Delete group]** of right-clicking menu.



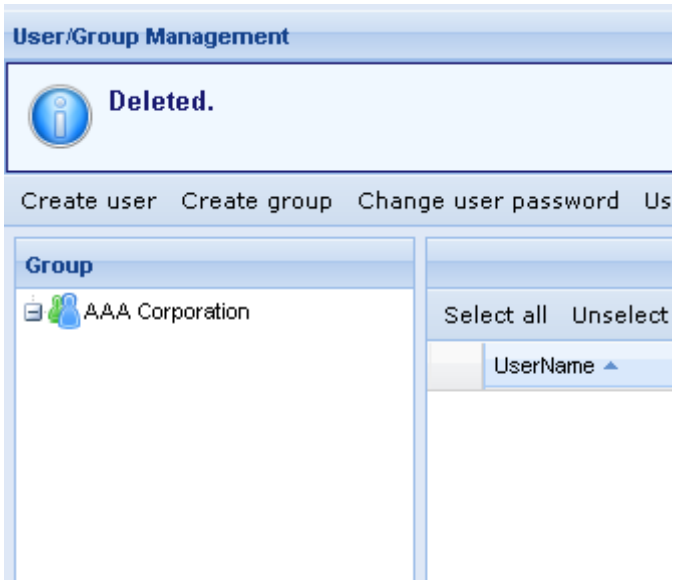
2. Be sure to perform Owner changing before performing group deletion. Check to a check box of **[Setup]** of **"Successor"**, and click a **[Select]** button. Specify succeeds user by **"User Search"** and click a **[Delete]** button.



3. A check dialog of **"Are you sure you want to delete?"** is displayed.



4. If you click a **[Yes]**, message of **"Deleted"** is displayed.



Chapter 6 Management of data

6.1 Owner changing of data

6.1.1 Owner changing

Owner of folders / files can change to other one user or group. The following users have Owner changing authority also to data whose self is not owner.

- GA can change Owner of data with which the member of group from which self serves as GA is owner.
- CA can change Owner to all data in cabinet in which self serves as CA.

6.1.2 Owner changing of the data in folder by batch

Owner of data in folder or cabinet can be changed by batch.

6.1.3 Changing operation explanation of Owner

Refer to changing of Owner of ("PROCENTER SaaS" User Manual) for changing operation explanation of Owner.

6.2 Changing of "Access control" (Changing, Addition, and Deletion)

6.2.1 Changing of "Access control"

When you change "Access control" (setting state) set at the time of folder and file creation, you can perform in three modes, [Update], [Add], and [Delete].

■ **[Update mode]**

You can replace "Access control" of groups or users you specify. When folders and files under are also made into target, "Access control" of all folders / files is replaced.

■ **[Add mode]**

You can add groups or users you specify to existing "Access control". When folders and files under are also made into target, "Access control" is added to all folders and files.

■ **[Delete mode]**

You can delete groups or users you specify from "Access control". When folders and files under are also made into target, "Access control" is deleted from all folders and files.

※ When two or more Owner is set, even if the following users are not Owner, they can change "Access control".

- CA can change "Access control" to all data in cabinet in which self serves as CA.
- GA can change "Access control" of data with which member of group where self serves as GA is Owner.

6.2.2 "Access control" changing of the data in folder by batch

About data in folder / cabinet, you can change "Access control" by batch.

6.2.3 Changing operation explanation of "Access control"

Refer to changing of "Access control" of "PROCENTER SaaS User Manual" for changing operation explanation of "Access control".

6.3 *Locking and unlocking of file*

Locking is operation effective only in file by act in which user deprives other users of write-in authority and deletion authority temporarily to specific file. If locking of file is performed, locked time and user is recorded in property of file. These properties are cleared at the time of unlocking. It becomes impossible other than person who locked until file is unlocked to write or to delete.

The following users can perform unlocking.

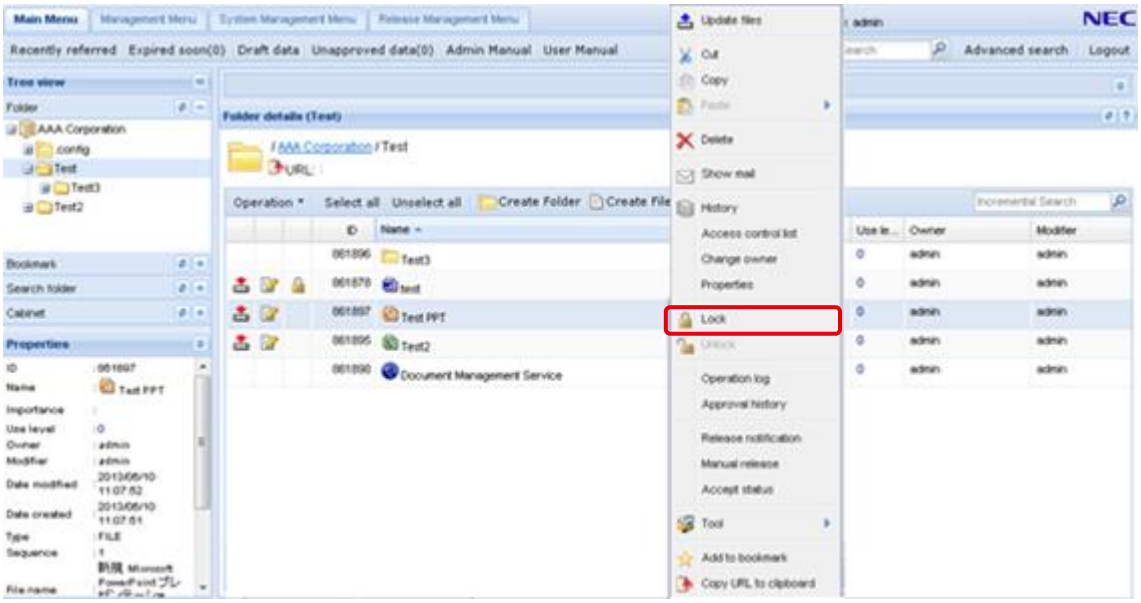
- **CA**

  CA can perform unlocking of all data in cabinet.

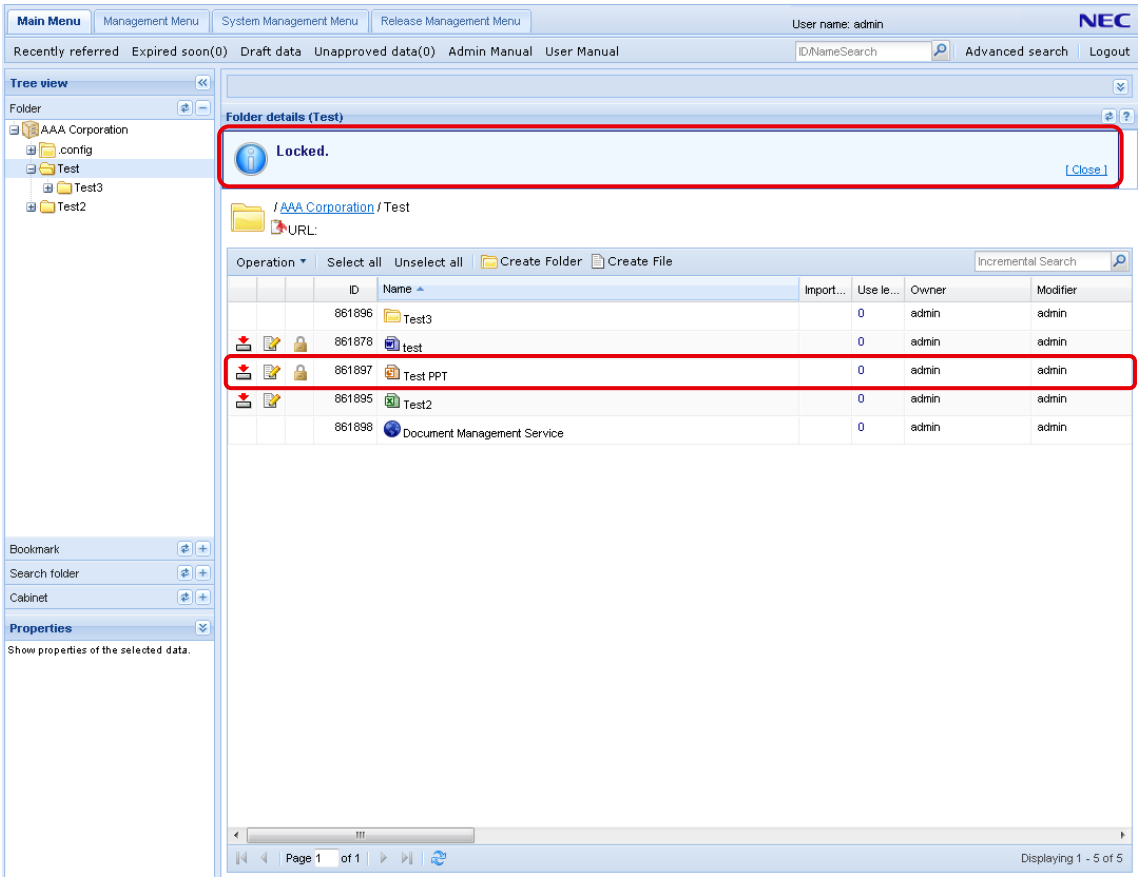
- **User who locks**

Operation explanation :

1. If you specify file you want to lock from **"Folder Detail"** screen and click **[Lock]** of right-clicking menu, a check dialog of **"Do you want to lock"** is displayed.



2. If you click a **[Yes]**, message of **"Locked"** is displayed.



When performing unlock of a locked file, unlock is performed if you specify target file and click a **[Unlock]** with right-clicking menu.

6.4 Changing of expiration date

6.4.1 About changing of expiration date

Expiration date holds storage term (date) as property for all folders or files in cabinet, and user with write authority can specify it at the time of data creation or updating. (Please refer to the "PROCENTER SaaS" User Manual for the details of expiration date setting.)

However, even if CA does not have write authority, CA can change expiration date.

Moreover, CA can change expiration date to all data in cabinet in which CA himself belongs.

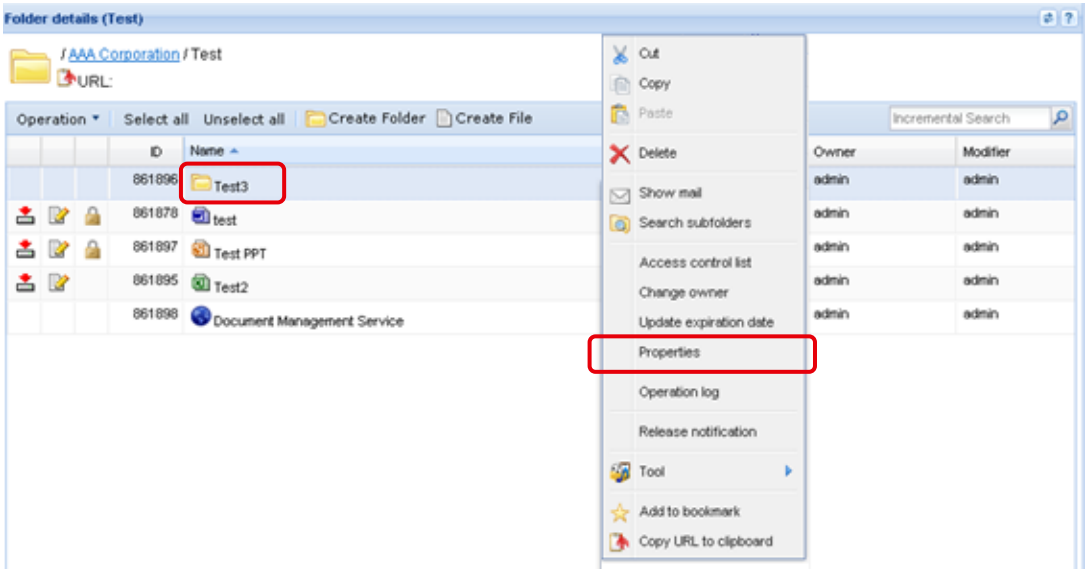
Furthermore, CA can change expiration date to cabinet which belongs. (Refer to [Cabinet policy changing (expiration date)] of [Chapter 8 Setting of cabinet].)

6.4.2 Operation explanation of expiration date changing

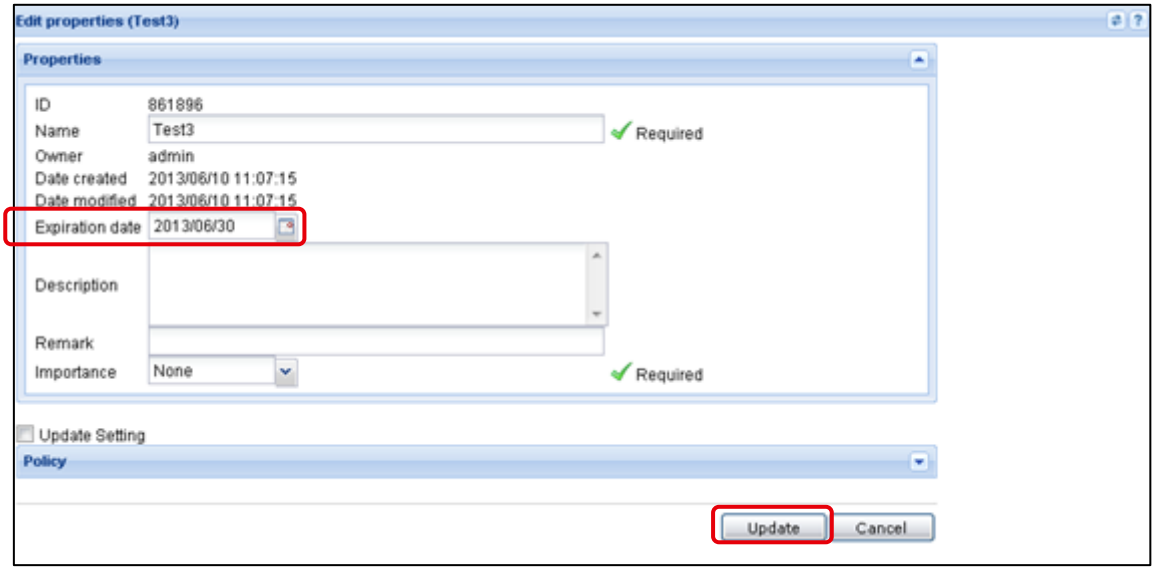
Perform following procedures when you change expiration date of data in cabinet.

Operation explanation :

1. If you specify a file which you want to change expiration date from **"Folder Detail"** screen and click a **[Properties]** of right-clicking menu, **"Edit property"** screen is displayed.



2. Change **[Expiration date]** on **"Edit properties"** screen and click a **[Update]** button.



6.4.3 Automatic deletion of expiration date of data

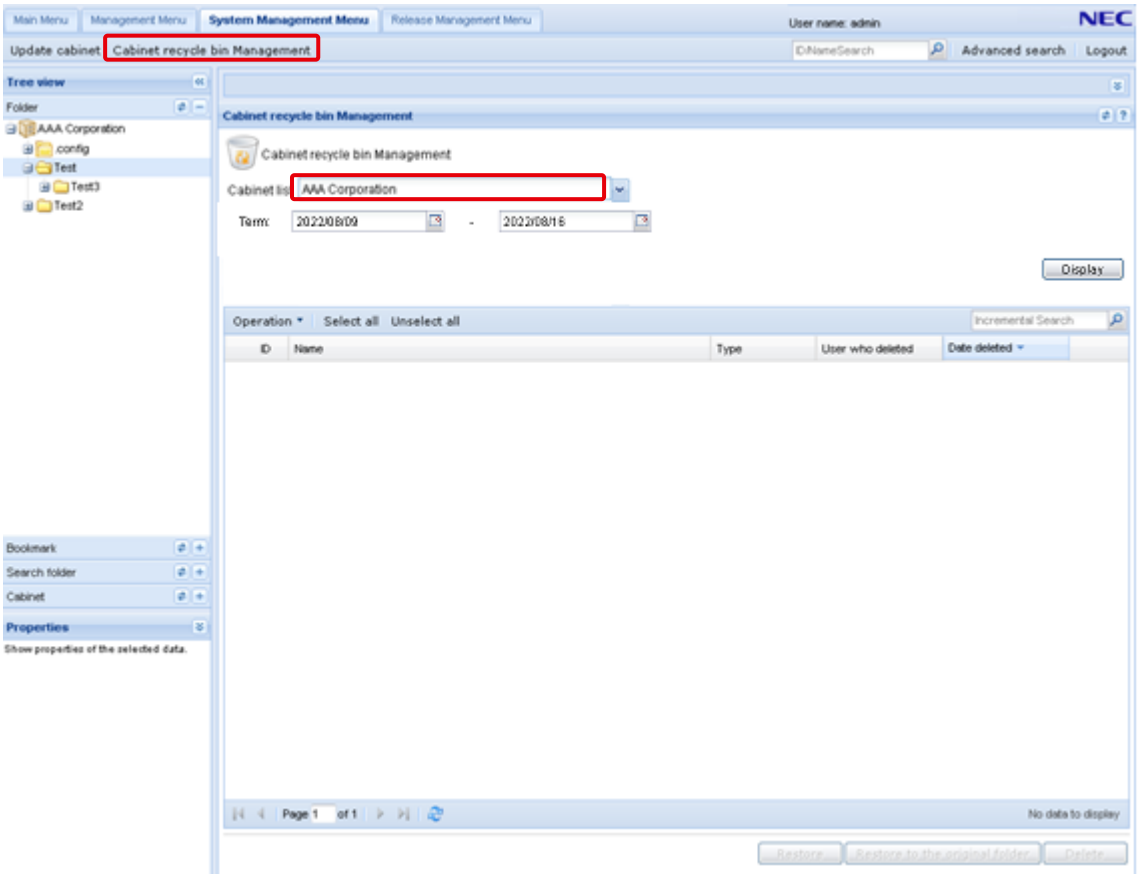
By the case where expired date is set as folder and setting date has expired about all data under folder, all the data under folder is moved to "Cabinet Recycle bin." （If there are some files which have not expired,  is attached to folder in which date expired）

You can restore or delete data which moved to Cabinet Recycle bin. If you select cabinet, data automatically deleted within cabinet is displayed. It is possible to restore in place which had data origin, or to specify path by self and to restore.

Operation of Cabinet Recycle bin is explained below.

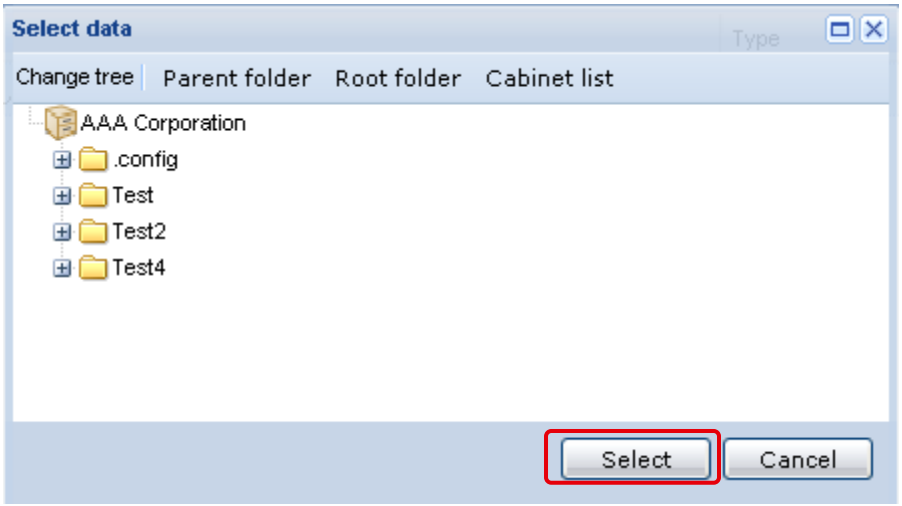
Operation explanation：

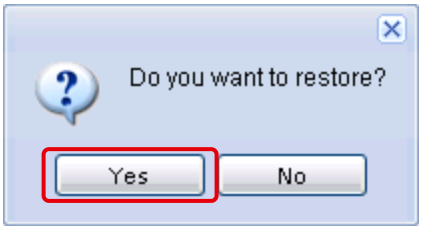
1. Click **[Cabinet Recycle bin Management]** in **"Service Management Menu"**.
2. If you specify cabinet as **[Cabinet list]**, data automatically deleted within cabinet is displayed.
   In "Term", specify the deletion date and time (the date of the operation on which the delete operation was performed) and click the [View] button to display the data for the specified time period. The default is a week-long display.



3. 1) **Case of restoring data**

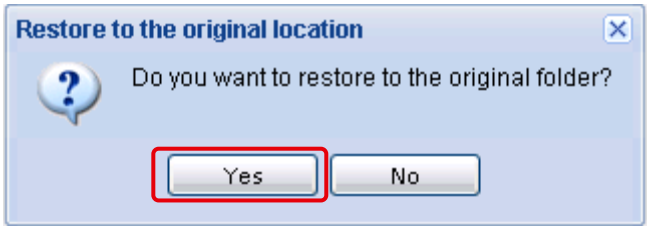
Select data to restore from **[Cabinet Recycle bin Management]**. If you click a **[Restore]** button, “Data select screen” of restoration place is displayed. Select data of restoration place and click a **[Select]** button. Since a check dialog of **"Do you want to restore"** is displayed, restoration of data is performed if you click a **[Yes]** button.





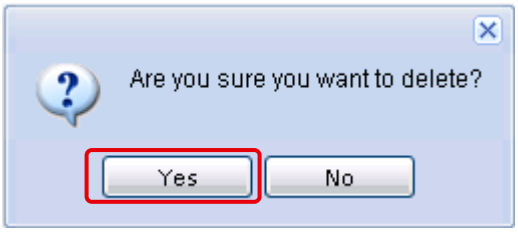
2) **Case of restoring data in the original place**

Select data to restore from **[Cabinet Recycle bin Management]**. If you click a **[Restore to the original location]** button, a check dialog of **"Do you want to restore the original folder?"** is displayed. If you click a **[Yes]** button, restoration of data to deleting agency is performed.



3) **Case of deletion data**

Select data to delete from **[Cabinet Recycle bin Management]**. If you click a **[Delete]** button, a check dialog of **"Are you sure you want to delete?"** is displayed. If you click a **[Yes]** button, deletion is performed.



——Notes——

- When you restore in original place, and the original place is already deleted, error occurs.

6.5 Numbering format definition

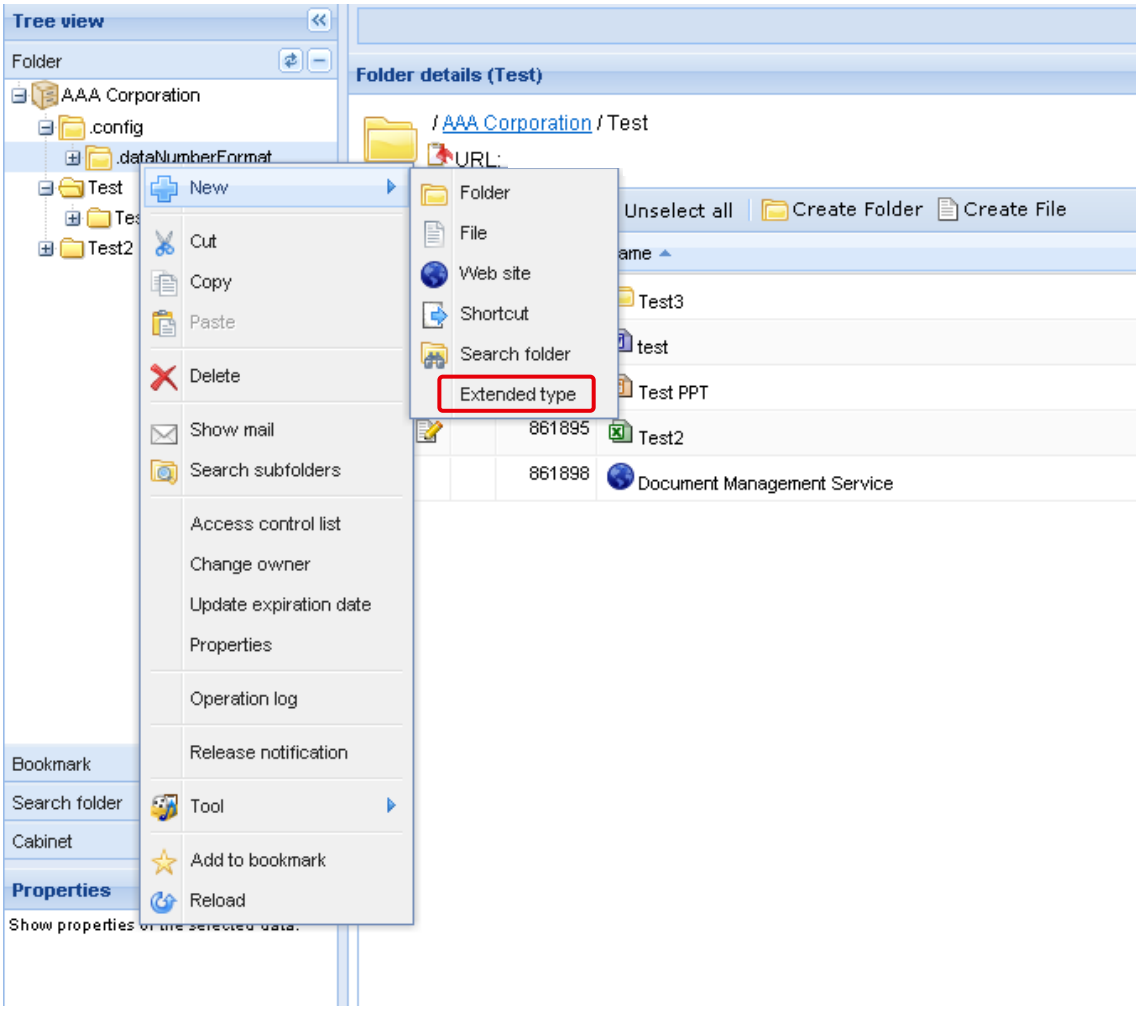
Numbering format definition is definition of format at the time of numbering management number of file, it is necessary to create under **[cabinet] /.config/ dataNumberFormat**. You can refer to numbering format definition created here at the time of using numbering.

6.5.1 Creation of numbering format folder

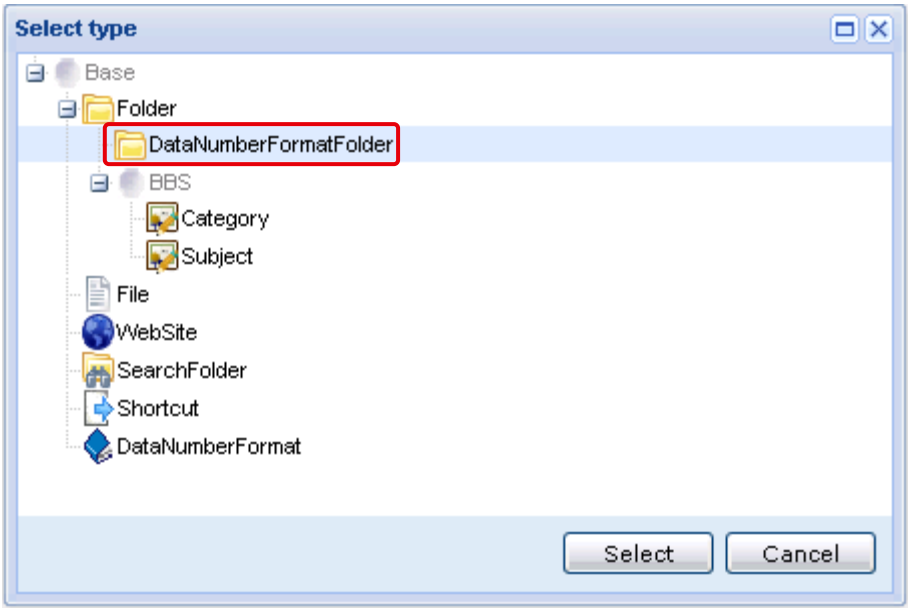
If you want to arrange numbering format, it is necessary to create numbering format folder previously.

Operation explanation：

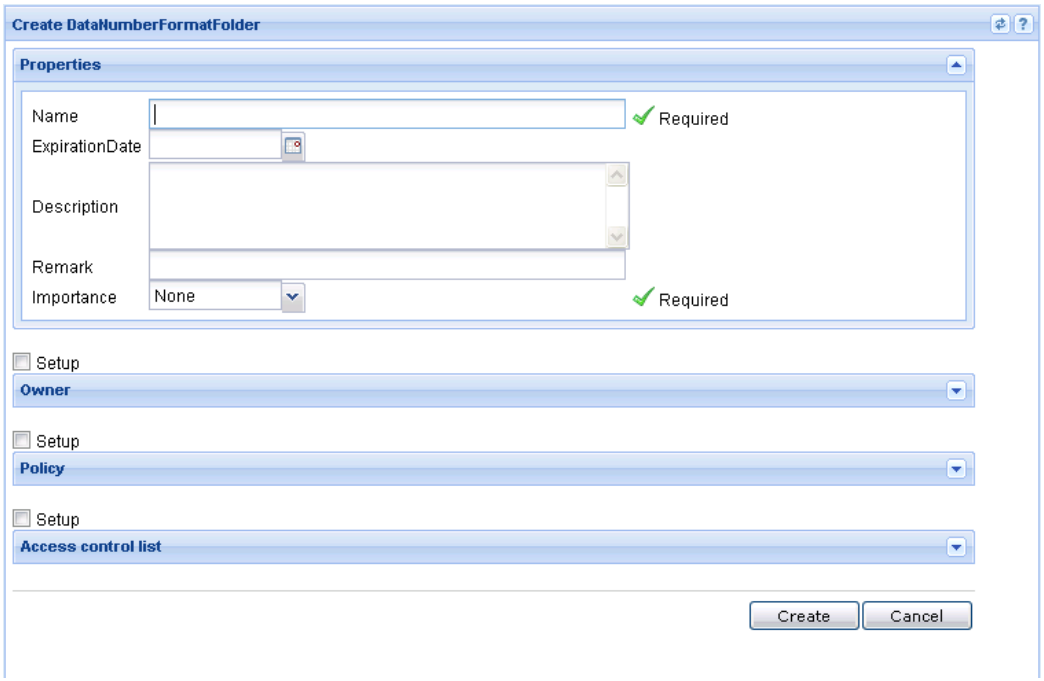
1. Select **[New] -> [Extended type]** from right-clicking menu of .dataNumberFormat in folder tree.



2. Select **[DataNumberFormatFolder]** from “Select type window”.



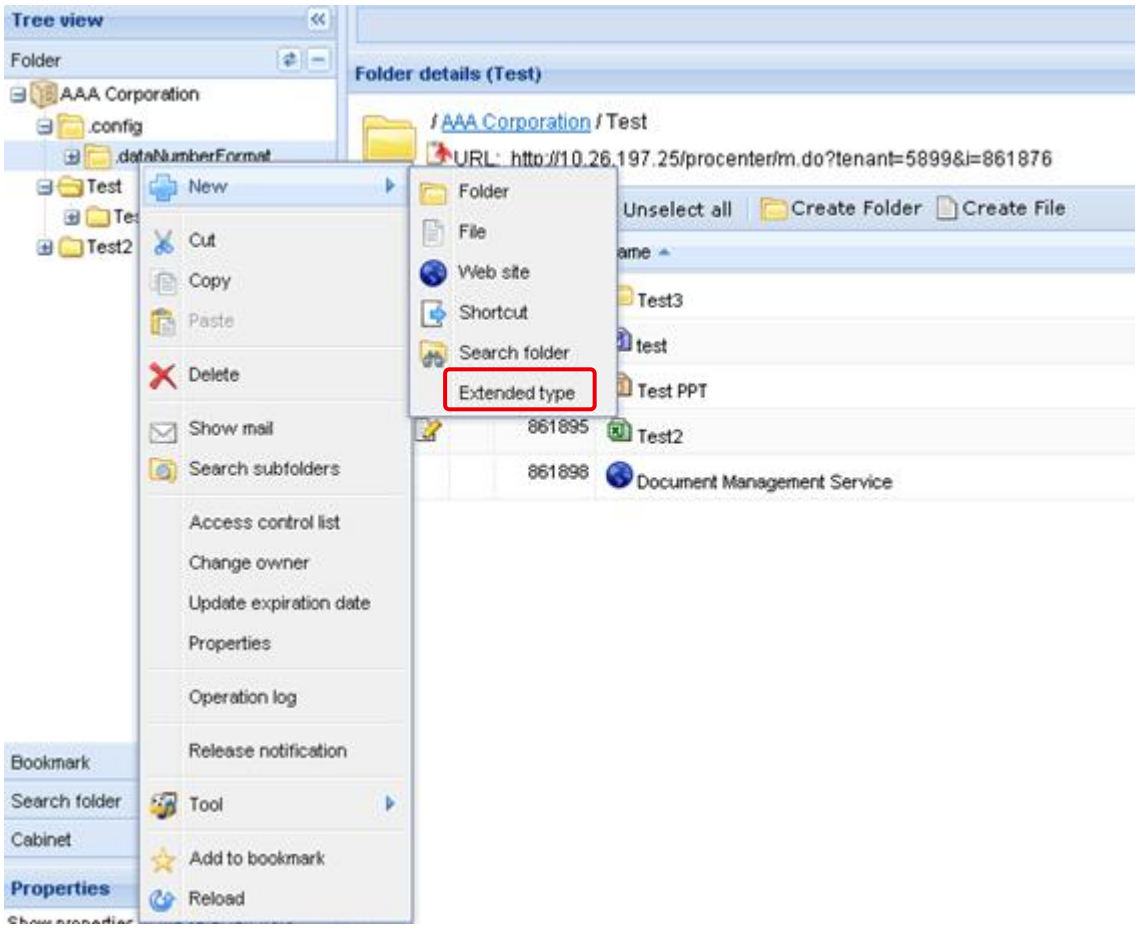
3. “Create numbering format folder screen” is displayed. Concrete creation method of numbering format folder is the same as that of folder.



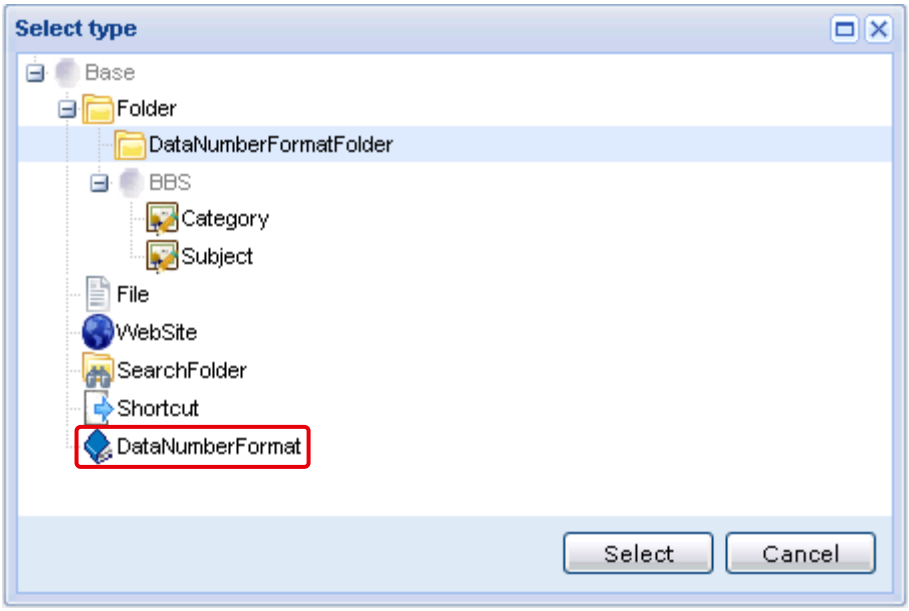
6.5.2 Creation of numbering format definition

Operation explanation：

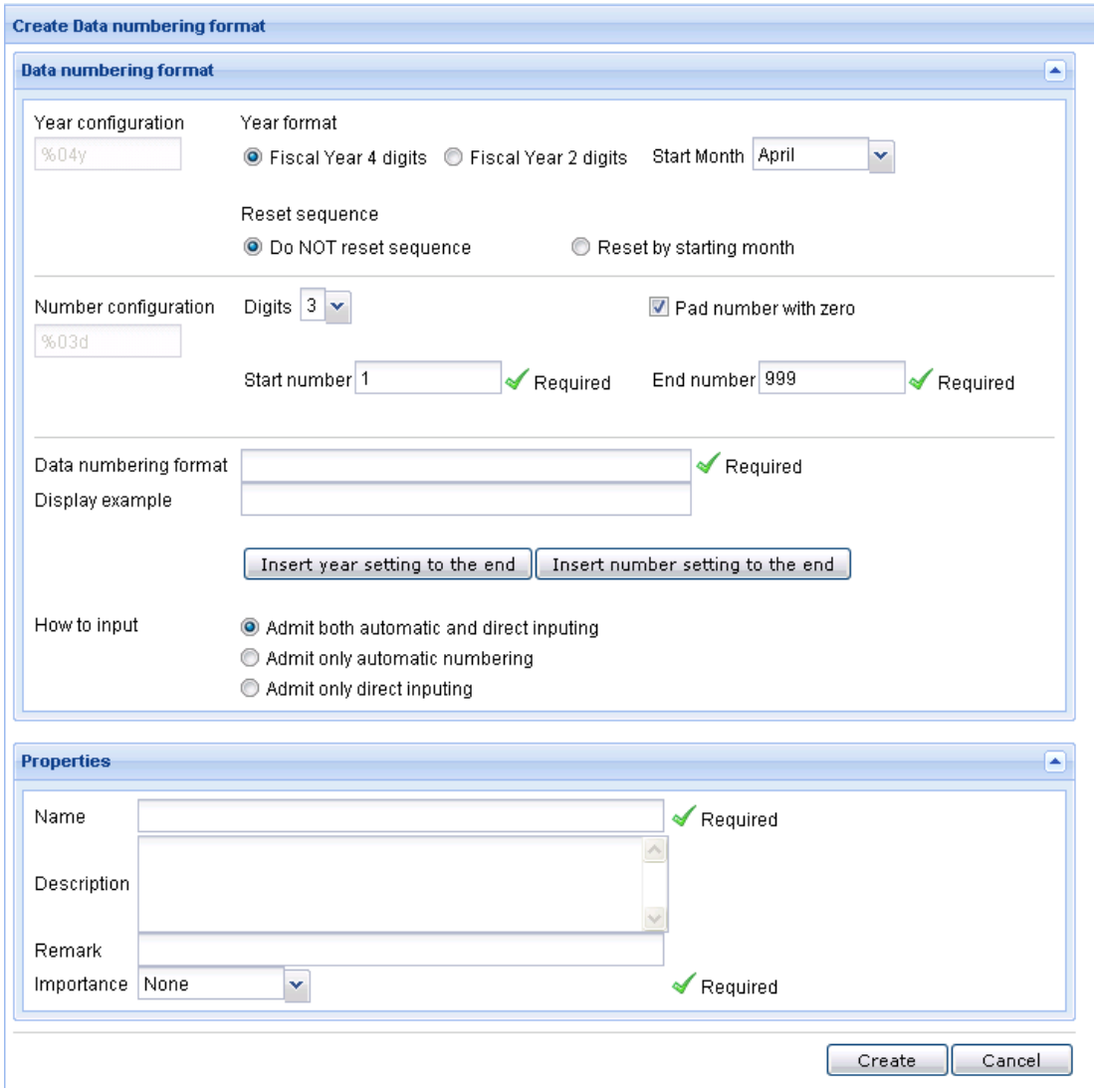
1. Select **[New] -> [Extended type]** from right-clicking menu of .dataNumberFormat in folder tree, or created numbering format folder.



2. Select [DataNumberformat] from “Select type window”.

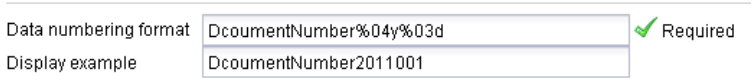


3. Open “Numbering format definition creation screen” and set properties of numbering format definition.



■Properties of indispensable specification are as follows at the time of numbering format definition creation.

Property name	Note
Year format	Select how many digits of fiscal year is displayed. Value displayed to year setting text box changes depending on selected value.
Start Month	Select month which fiscal year starts.
Reset sequence	Select whether sequence is reset or not to start month of fiscal year.

Digits	Select digit number of number. Value displayed on number setting text box changes depending on selected value. As shown in "0001", when less than digit number and burying by 0, confirm [Pad number with zero].
Start number	Set minimum number that can be used for numbering. When you perform automatic numbering for the first time using this numbering format definition, numbering is performed by this number.
End number	The maximum number that can be used for numbering is set.
Data numbering format	Set data numbering format. Setting of format, sample of management number on [Display example] is displayed.  **[Insert year setting to the end]** button inserts the format of setting year form in the end of numbering format. **[Insert number setting to the end]** button inserts the format of setting number form in the end of numbering format.
How to input	Select whether only automatic numbering is permitted, only number direct input is permitted, or both automatic numbering and number direct input are permitted. Number cannot be changed when you select **[Admit only automatic numbering]**. When you select **[Admit only direct inputting]**, it does not numbering automatically.
Name	The name is set like file etc.
Importance	Select importance like file etc.

■Arbitrary specification property at the time of numbering format definition creation

Property name	Note
Description	
Remark	

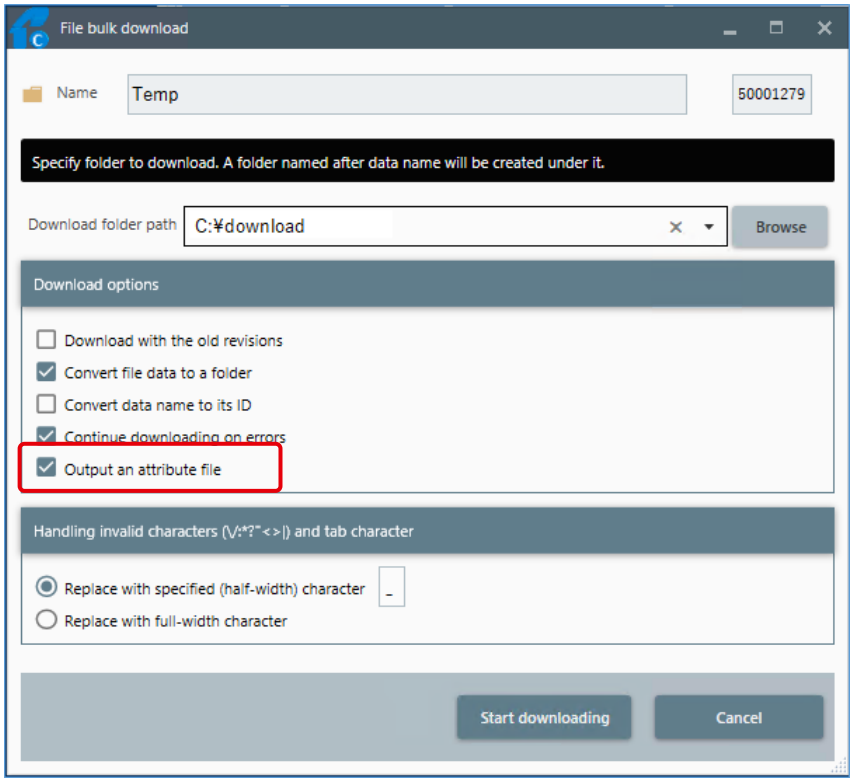
3. If you click a **[Create]** button, numbering format definition is created.

6.6 *Exporting attribute file when bulk downloading files*

When a cabinet administrator (CA) execute file bulk downloading, he/she can download attribute information of downloaded data in XML.

6.6.1 How to export attribute file

If you'd like to export data attribute information, check **[Export attribute file]** in the main window of file bulk downloading tool and click **[Download]** button.
attribute file (file name is procenter-export.xml) will be created in the destination folder.



6.6.2 Contents of attribute file

The attribute descriptions are below:

Element	Description
<relations>	Relations of all downloaded data. < relations> has 1 or more <relation>. id: Data ID dummy_id: Data ID name: Data name

<relation>	A relation of downloaded data. A <relation> expresses a folder or file. If there is a <relation> inside a <relation>, it is a relation between parent and child. dummy_id: Data ID name: Data name type: reserved (No meaning so far)
<nodes>	Detail information of all downloaded data. A <nodes> has 1 or more <node>.
<node>	Detail information of data. < node> has <properties> , <contentspolicies> , <permissions> , <files> , <histories> and <approvalhistories>.
<properties>	Properties of all downloaded data. A <properties> has 1 or more <property>.
<property>	Properties of downloaded data. name: Property name value: Property value
<permissions>	Access control list of all downloaded data. A <permissions> has 1 or more <permission>.
<permission>	Access control list of downloaded data. userid: User ID value: Access right
<files>	File information of all downloaded data. A <files> has 1 or more <add_file>. In case of folder, <files> will not be outputted.
<add_file>	File information of downloaded data. sequence: Version filename: File name filepath: Relative path from the destination folder of the file filesize: File size (byte) fileid: File ID filetimestamp: Timestamp of the file valutid: Vault ID asequence: Absolute version revision: Revision

	reason: Reason for update modifierId: User ID who modified last modifierName: User name who modified last modified: Last modified date
<histories>	History information of all downloaded data. A <histories> has 1 or more <history>. In case of folder, <histories> will not be outputted.
<history>	History information of downloaded data. sequence: Version asequence: Absolute version revision: Revision reason: Reason for update modifierId: User ID who modified last modifierName: User name who modified last modified: Last modified date
<approvalhistories>	Approval history information of all downloaded data. A <approvalhistories> has 1 or more <approvalhistory>. In case of folder, <approvalhistories> will not be outputted.
<approvalhistory>	Approval history information of downloaded data. sequence: Version of disclose requestnumber: Request number ordernumber: Approval order approverid: User ID of approver approvaltype: Approval type clientid: User ID of client status: Approval status annotation: Approval comment created: Date of approval request lastmodified: Last status updated date

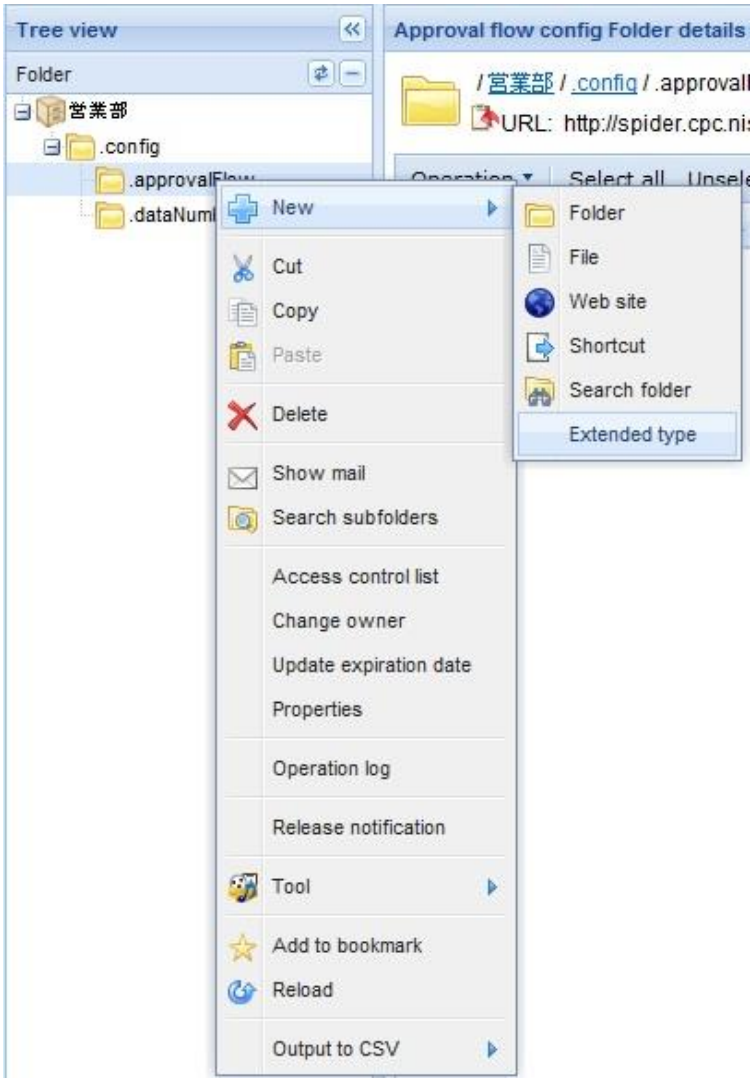
6.7 Creating approval flow

Approval flow definition needs to be created on **[Cabinet]/.config/.approvalFlow.** Users can see approval flow definition you created here when users request approval.

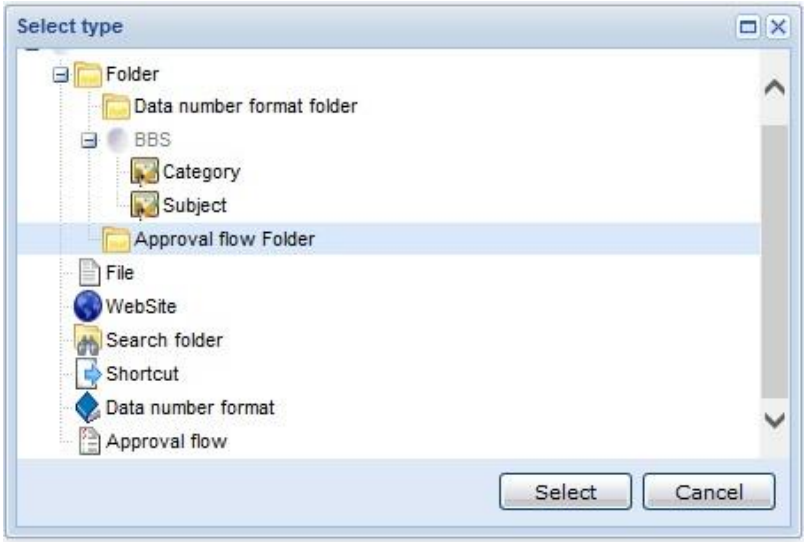
6.5.2 Creating an approval flow folder

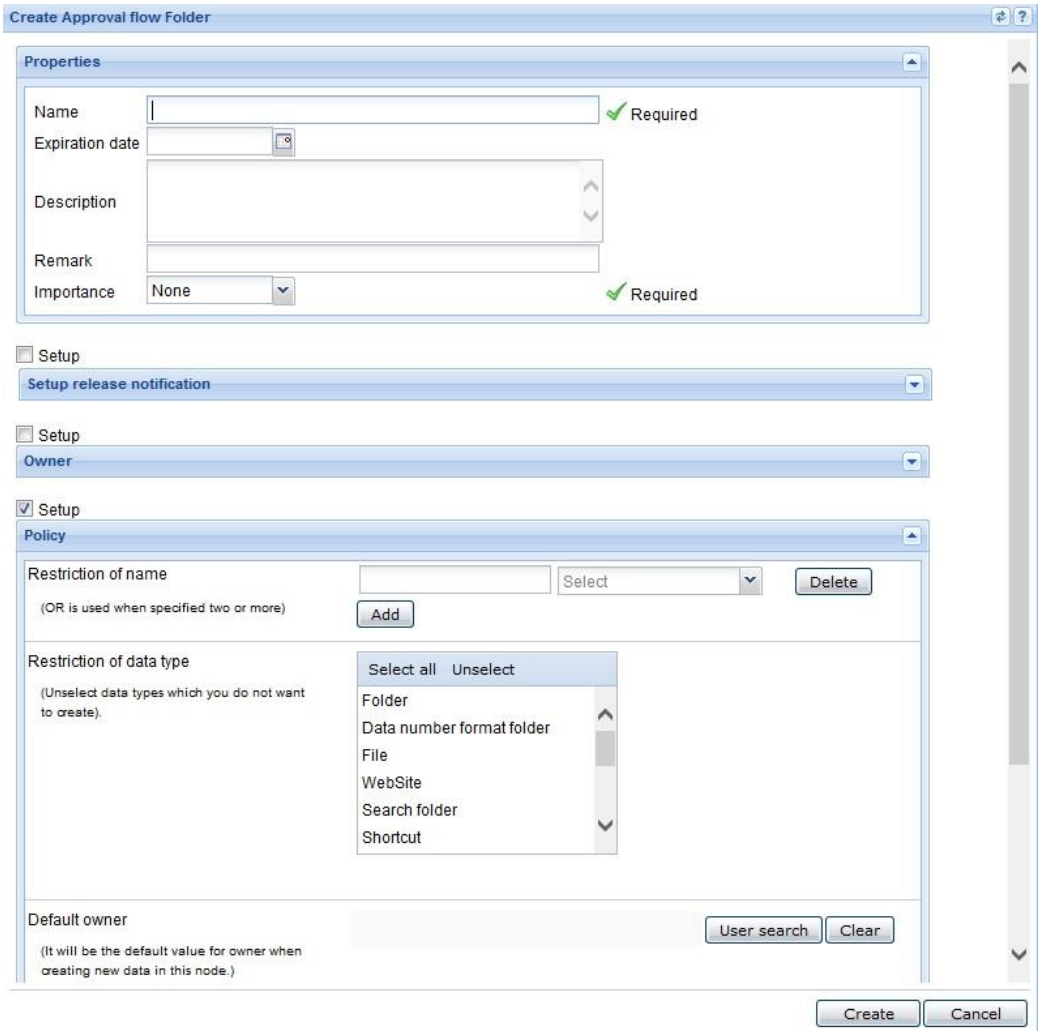
If you want to organize approval flows, you crate an approval flow folder first.

1. Select **[New]** > **[Extended type]** from the right button popup on .approval Flow on the folder tree.



2. Select [Approval flow Folder] from the type selection window.

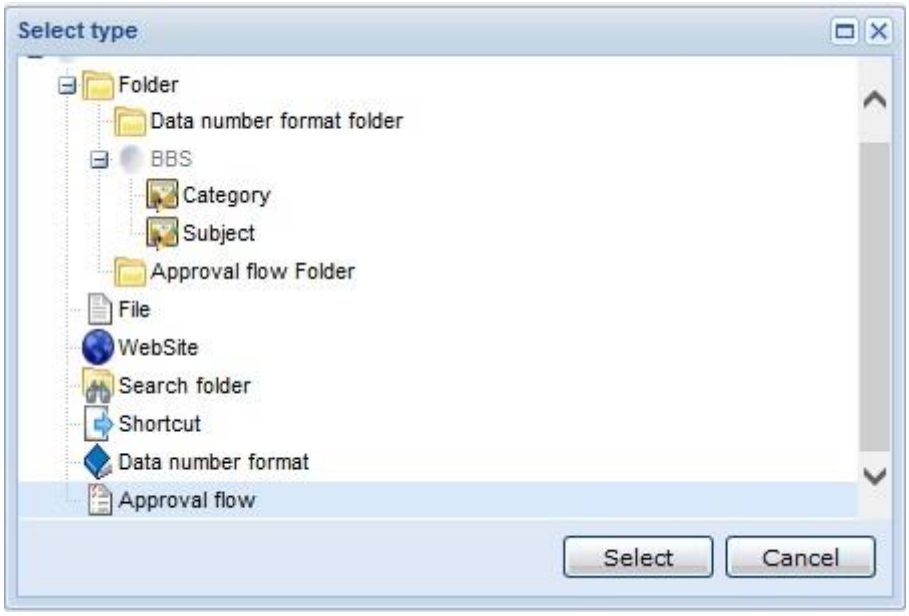




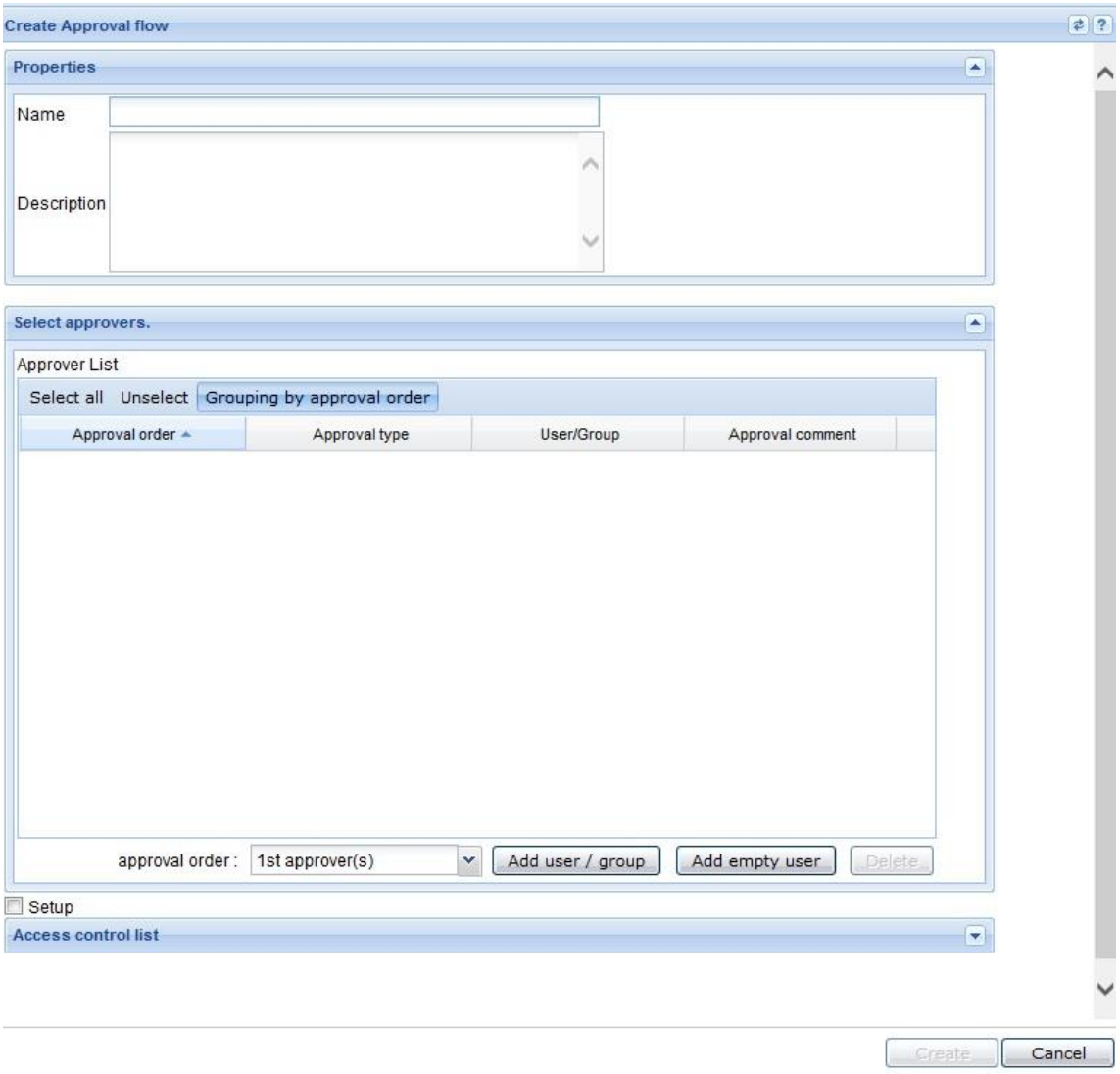
3. Creating approval folder screen is displayed.
   How to create an approval folder is same as to create a folder, please refer to Creating a folder.

6.5.2 Creating an approval flow definition

1. Select **[New]** > **[Extended type]** from the right button popup on .approval Flow on the folder tree or Approval flow Folder you created.
2. Select **[Approval flow]** from the type selection window.

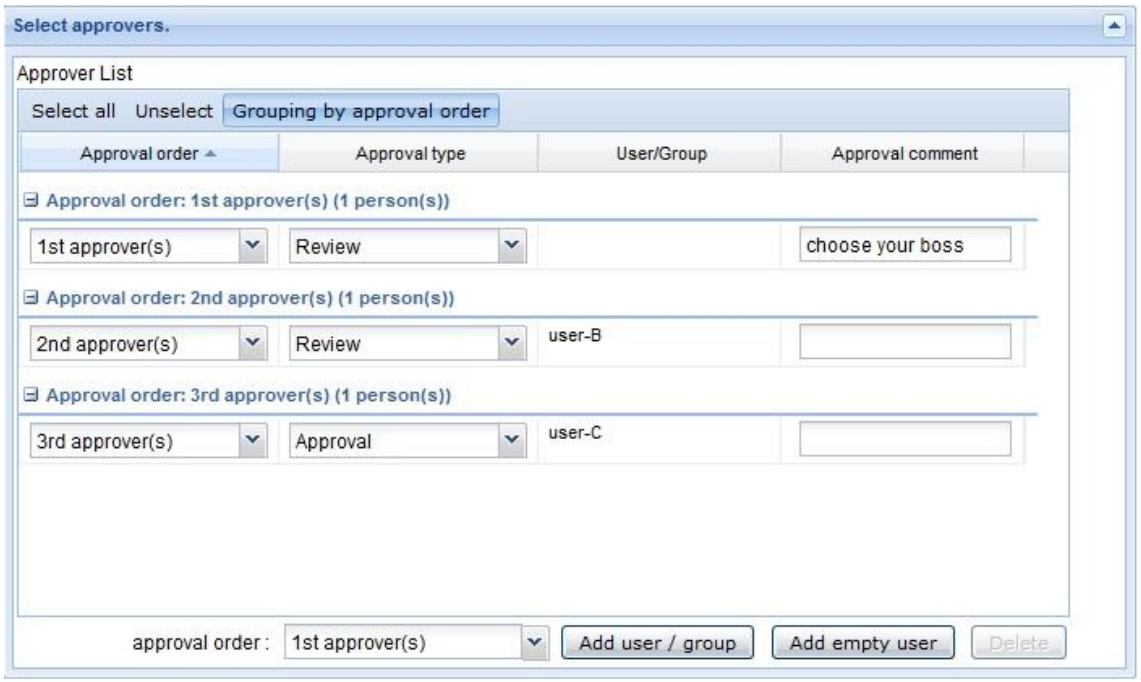


3. Open the creating the approval flow window and create an approval flow definition.



4. Set up approver person for approval flow.
   Specify approval order and select and add a user from [Add user/group] button.
   Please refer to searching user/group for detail.

   If you click **[Add empty user]** button, you can add an approver without specifying user. If you add empty user, users can choose any approvers from requesting approval window. Please use this feature if approver can not be fixed in case such as specifying user's boss. You can enter such as the condition of approver, approver info
   into **[Approval comment]**. **[Approval order]** is the order of approval. Lower number approver can approve first. **[Approval type]** is the type of approval. You can choose Review or Approval.
   * There is no difference in function by [Approval type].



5. Set up the property of Approval flow.

6. Click [Create] button and create the Approval flow.

Chapter 7 Log management function

Log management function is function which CA can search and display history of users / groups operation and data operation from on screen by user in cabinet in which Cabinet Administrator (CA) belongs being applicable. Moreover, you can also perform CSV output of search result.

Operation explanation :

1. Click **[Operation log]** under **"Management Menu"**.

2. Specify target user, period, and target for operation on "Operation Log" screen.

■ **Search user object** :

- ✓ User in cabinet is applicable.
- ✓ You can not specify two or more users.
- ✓ It is targeted at all users that are not deleted when there is no specification of user.

■ **Operation period :**

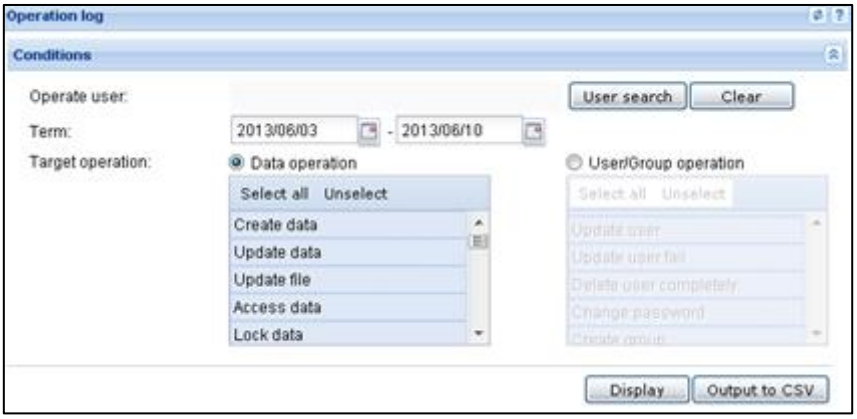
Specifying period is the date of “From” (time 00:00:00) and “To” (time 23:59:59). Together with the operation log, "From" has set "one week before" and "To" as "today" for default value of period.

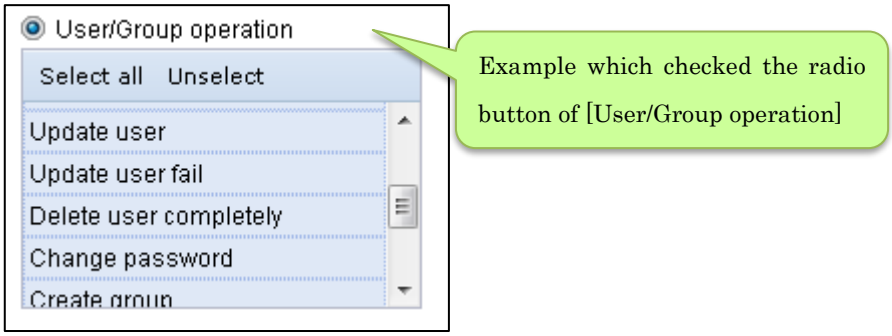
■ **Target operation :**

Select target operation ("User/Group operation" or "Data operation") with radio button. Target operation is as follows.

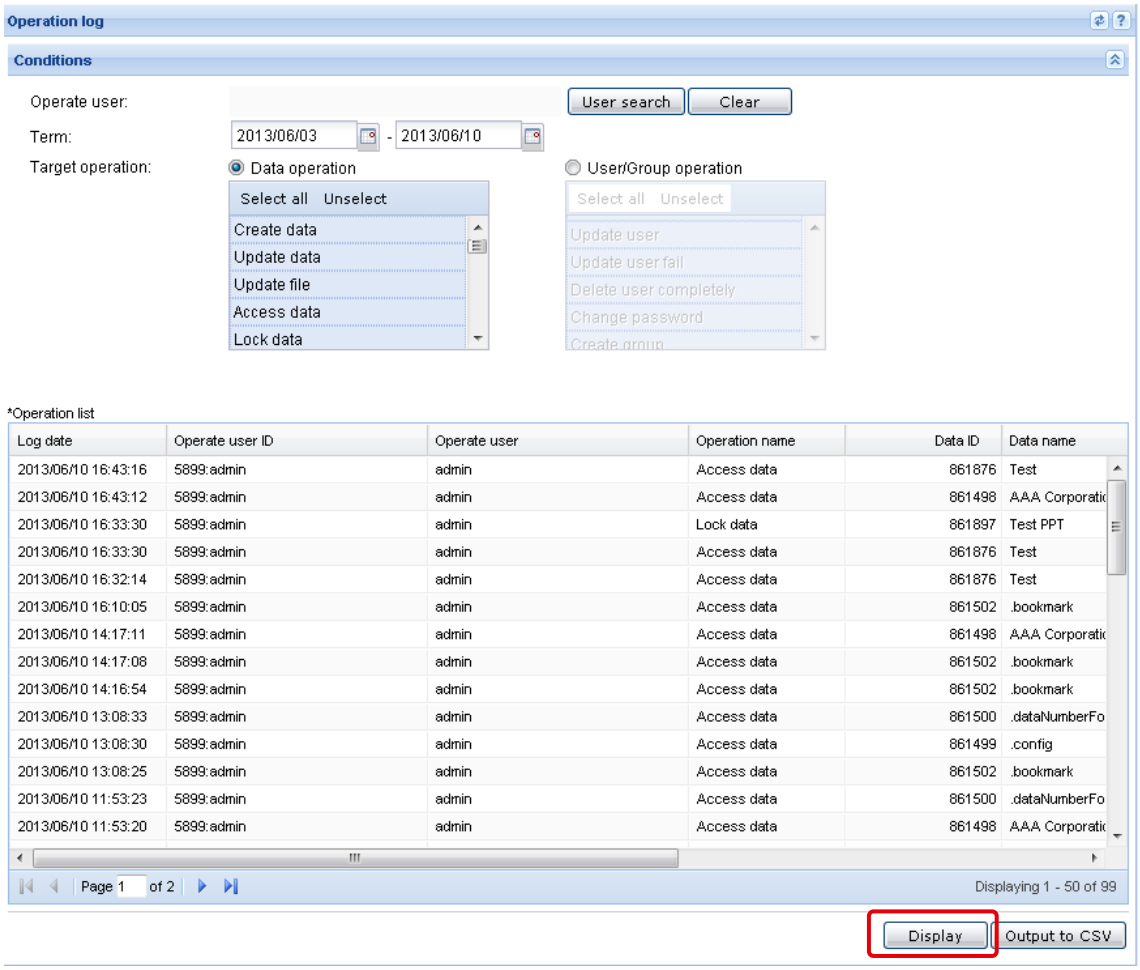
[User/Group]	**[Data operation]**
Login	Create data
Login fail	Update data
Logout	Update file
Create user	Access data
Create user fail	Lock data
Update user	Unlock data
Update user fail	Update ACL
Delete user completely	Delete data
Change password	Delete data completely
TOTP authentication effective	Restore data
TOTP authentication ineffective	Copy data
Create group	Move data
Create group fail	Change owner
Update group	Update contents policy
Update group fail	Update expiration date
Delete group completely	Deletion of retention period

Delete file
Data expired
Approval request
Cancel approval request
Approve
Reject approval request
Disclose
Update address setting
Release data
Accept data





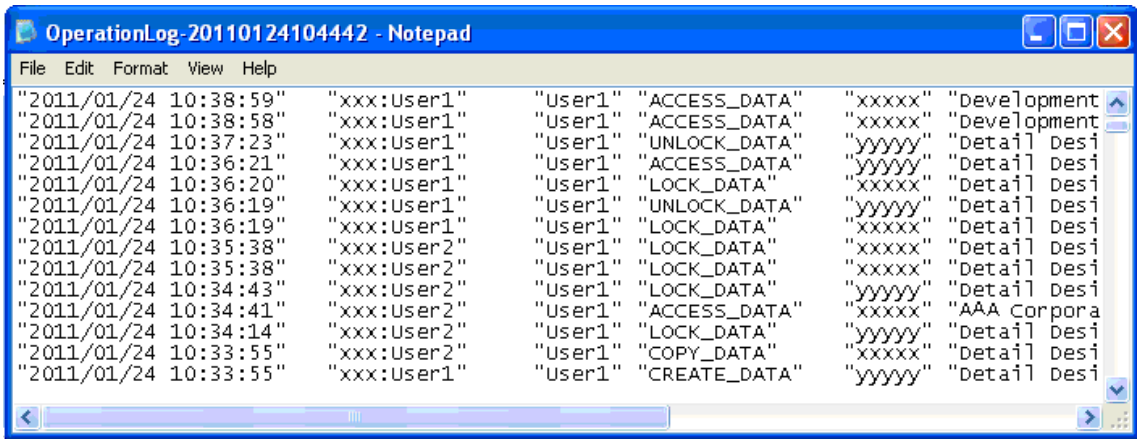
3. If you click a **[Display]** button, operation list is displayed.



■Operation Log is displayed. Display item is as follows.

In case of user/group operation	
LogDate	yyyy/mm/dd HH:mm:ss
OperationUserID	Number Integer
OperationUserName	Character string
OperationName	Character string
TargetUser/GroupID	Character string
In case of data operation	
LogDate	yyyy/mm/dd HH:mm:ss
OperationUserID	Number Integer
OperationUserName	Character string
OperationName	Character string
DataID	Number Integer
DataName	Character string

4. If you click a **[Output to CSV]** button, operation log result is outputted by CSV.



-- Notes --

・The operation log will be kept for about three months.

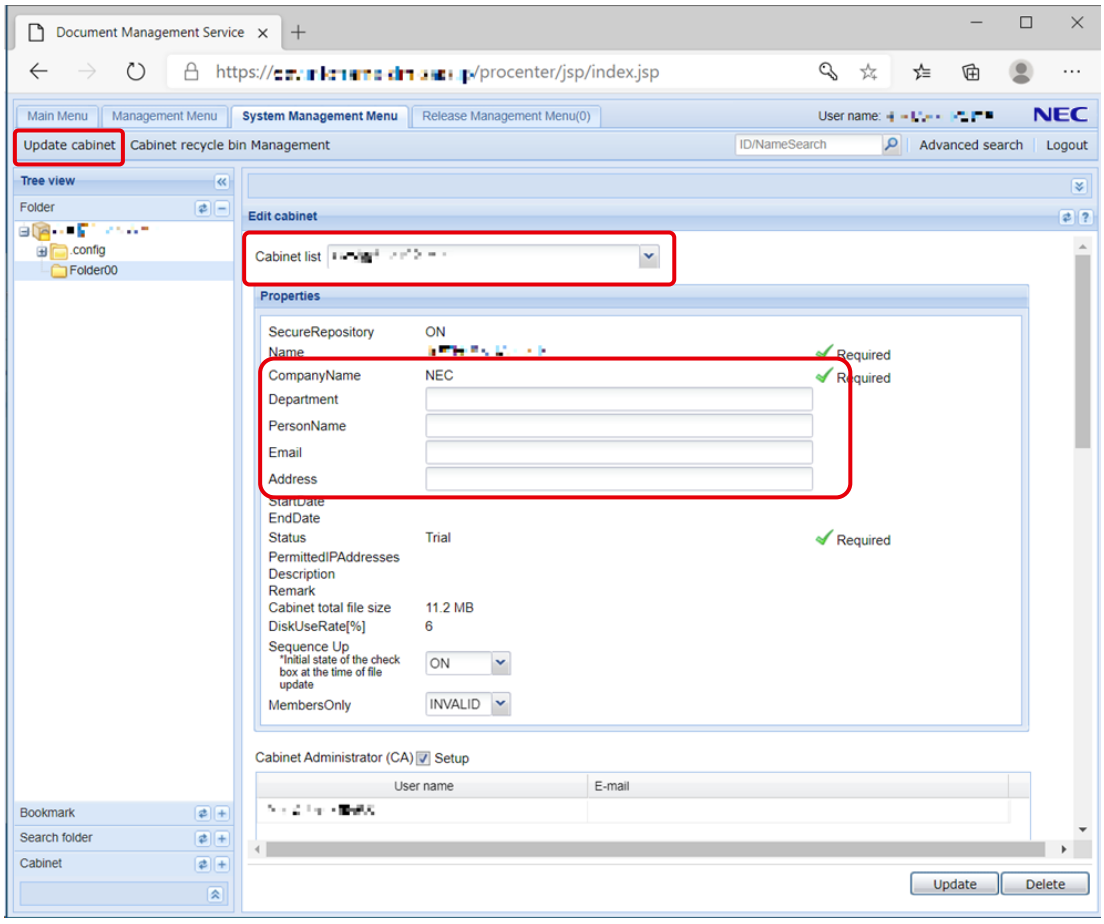
Chapter 8 Setting of cabinet

CA can perform changing operation of cabinet in which self belongs.

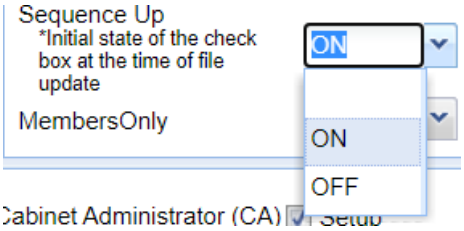
- You can change basic property and extended property (post name, person-in-charge name, mail address, contact).
- You can add or delete Cabinet Administrator (CA).
- You can change “Access control” of cabinet.
- You can perform setting of policy of cabinet.
- You can set default of “SequenceUp/No SerquenceUp”.
- You can set valid or invalid of “MembersOnly”.

1. Click **[Update cabinet]** under **"Service Management Menu"**. **"Update Cabinet"** screen is displayed. Specify cabinet by **"Cabinet list."** Property information on specified cabinet is displayed.

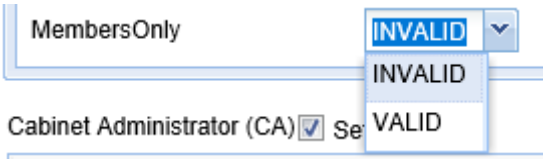
2. Edit basic property and extended property **(post name, person-in-charge name, mail address, contact)** on "Update Cabinet" screen.



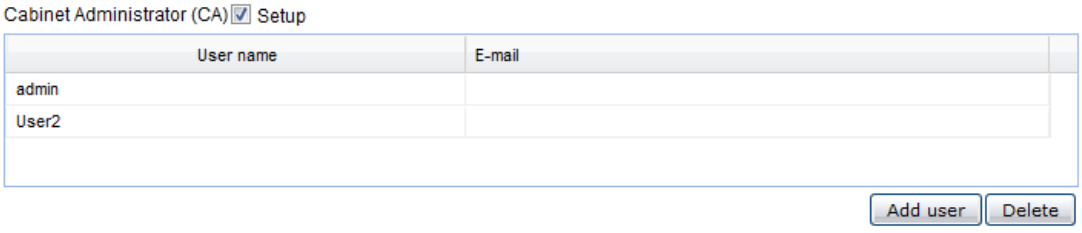
3. Set the default value of “SequenceUp/No SequenceUp”.
   When choosing **[ON]**, **[SequenceUp]** checkbox is checked on a file update screen. The file will be given the new number of sequence and registered with the latest edition.
   When choosing **[OFF]**, **[SequenceUp]** checkbox is not checked on a file update screen. The file will not be given the new number of sequence and the current edition will be renewed.



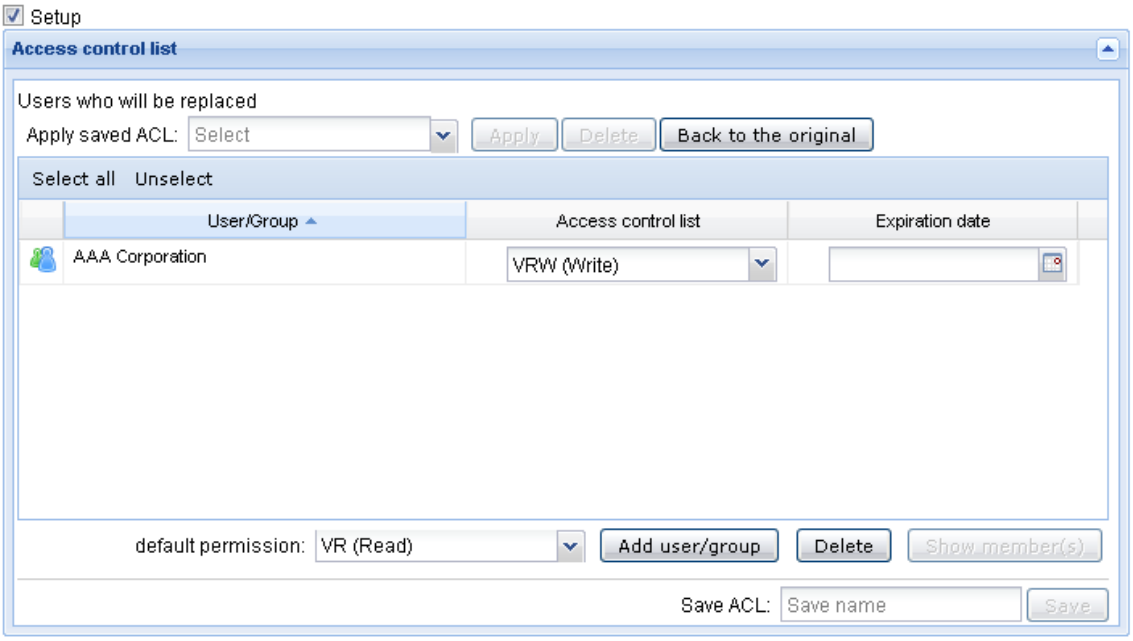
4. Set whether “MembersOnly” is used.
   Please refer to “Chapter 9 MembersOnly" for details of “MembersOnly”.



5. If you check to a check box of [Setup] when you perform "Cabinet Administrator (CA) Setting", “Cabinet Administrator (CA) setting screen” is displayed. You can perform addition or deletion of Cabinet Administrator (CA).



6. If you check to a check box of **[Setup]** when you perform "setting up Access control", “Access control setting screen” is displayed.（Please refer to 4.11.2 Access control setting / changing of "PROCENTER SaaS User Manual" for setting of Access control.）



7. If you check to a check box of **[Setup]** when you perform "Policy setting", “Policy setting screen” is displayed.

■Restriction of Name

: Setting restrictions of name about data registered under cabinet.

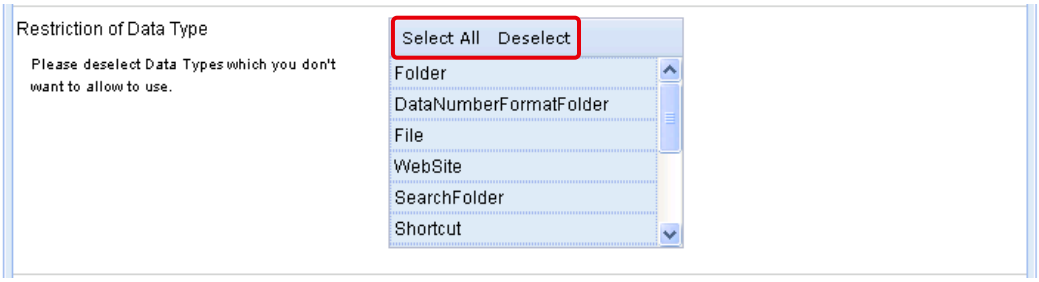
Create restrictions of name on **[Character string]** and conditions (**[begins with], [ends with], [contains]**).Then, data name which breaks restrictions can be registered no longer into folder. Click a **[Add]** button, when you add restrictions. Click a **[Delete]** button, when you delete restrictions.

■Restriction of Data Type

: Restrictions of type are set about data registered under cabinet.

Select from **[Select All]** button / **[Deselect]** button / individual click and select data

type which permits creation. Then, data type which breaks restrictions can be registered no longer into folder.



■Setting Expiration Date

：Set default value of expiration date about data registered under cabinet. Specify conditions from three patterns of **[No expiration]** / **[Expiration N months after creating]** / **[Expiration N days after creating]**, and **[Expiration Date]**.It becomes the default value of expiration date at the time of this registering data under folder.

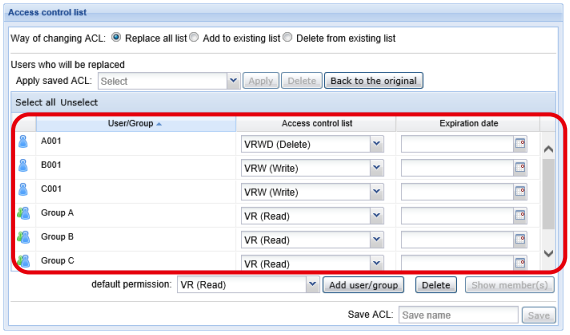
6. If you click a **[Update]** button, cabinet is updated.

Chapter 9 MembersOnly

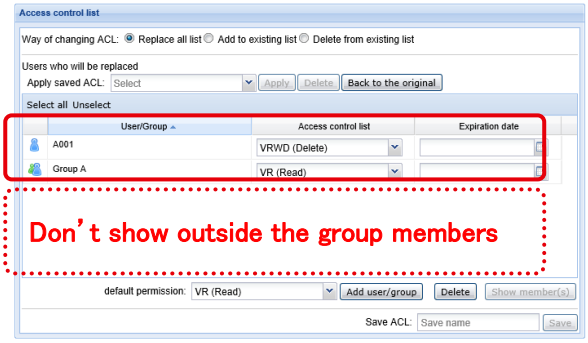
“MembersOnly” is the function that limits shown users in the group members.
It's possible to set “MembersOnly” to valid/invalid to the cabinet unit.
When you use this setting, it's possible to make the user shown to user search and a list of access control limit in the members of group to which the use user belongs.

When “MembersOnly” is valid/invalid, the reference area is as follows.
Example) when a user of “company A” group refer to access control.

・”MembersOnly”: **Invalid**
(Show all access control including other groups.)



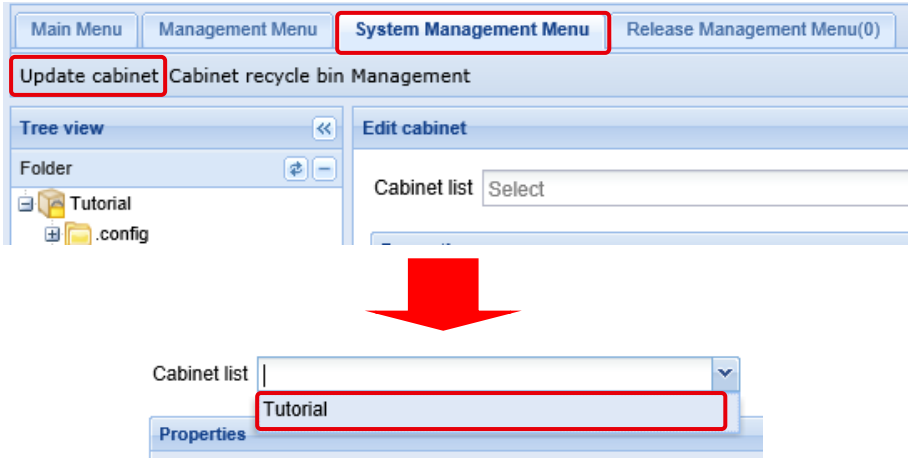
・”MembersOnly”: **Valid**
(Show only access control of group members to which the login user belong.)



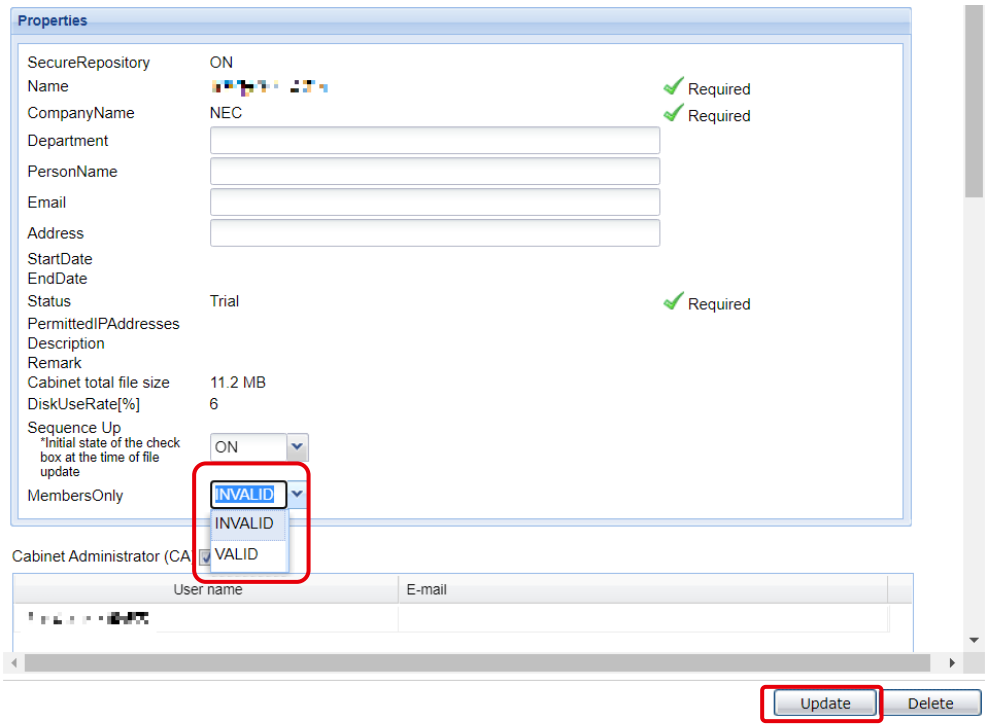
9.1 How to set "MembersOnly"

Please set "MembersOnly" by the next procedure.

1. Click **[System Management Menu]** and **[Update cabinet]**, and choose the cabinet name in **[Cabinet list]**. And cabinet renewal screen is shown.



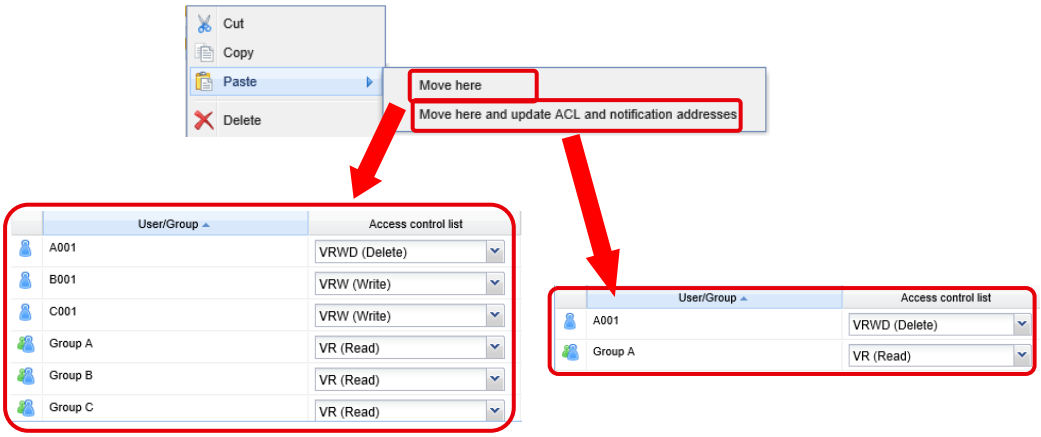
2. Set "MembersOnly" of the screen lower part to **[VALID]** or **[INVALID]**, and Press **[Update]** button. And it's reflected.



9.2 Notes

When using “MembersOnly”, please pay attention to below.

- This function is set to valid/invalid to the cabinet unit.
- **Only CA** can set the function.
- **Set a local group to an access control of used files and folders.** The folder and the file to which a local group isn't set aren't shared.
- **Register all users with a local group.** The user who isn't registered with a local group can't refer the other users.
- **All users' reference in the cabinet is possible by only CA.**
  Because GA can't refer users of the other groups, GA can't add a user to the group newly. It's necessary **to operate the user addition to a local group by CA**.
- When **[Copy here and update ACL and notification addresses (incl. files)]** or **[Move here and update ACL and notification addresses]** is chosen when moving or copying a folder, **only access control of the local group to which you belong** is taken over. **To take all access control including other local groups over**, use **[Copy here (incl. files)]** or **[Move here]**.



- **A property of a file, an approval history list, log information, a transfer situation list and a notice reception data list** is shown as before.
  For a user name can't be seen by the user of a different group, don't set access control of more than one local group to a file.

[Property of file]

Name	Importance	Use level	Owner	Modifier
Schedule		0	A001	A001

[Approval history list]

Disclosed sequence	Request number	Approval order	Approval type	Client	Person expected to approve	Person approved	Approval status
2	1	1st approver(s)	Review	A001	A002	A002	Approved
2	1	2nd approver(s)	Approval	A001	A003	A003	Approved

[Log information]

Date	UserName	Operation	Sequence	File name
11/01/2019 10:42:03	A001	Update file	1	Schedule.xlsx

[Transfer situation list]

UserName	Accept status	Date accepted	Accessed
A002	Accepted	11/01/2019 11:39:46	Unread
A003	Accept waiting		Unread

[Notice reception data list]

Name	Sequence	Release user	Date released	Accept status	Date accepted	Accessed	Date accessed
Minutes	1	A001	11/01/2019 11:15:42	Accept waiting		Unread	

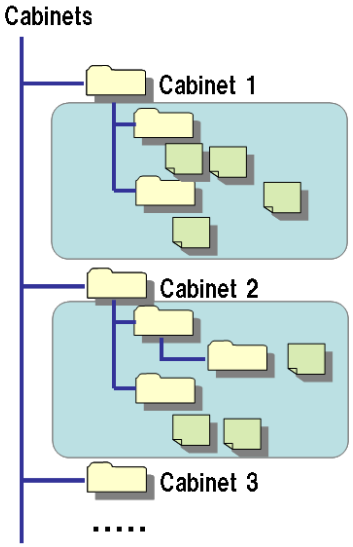
- When lumping changed the right of access of a folder follower, **only a belonging group member is made the change target**. The right of access to which you can't refer by another group is taken over just as it is.
- When a member of another group was included in the right of access preserved in the past by change in the access matter, **a member of another group isn't reflected by an access control list any more at the time of application**.
- When a member of another group was included in the acknowledger who preserved it in the past at the time of setting in an approval request destination, **a member of another group isn't reflected any more in an approval request destination at the time of application**.

- When a member of another group was included in the notice destination preserved in the past by change in the release notice destination, **a member of another group isn't reflected any more in a notice destination at the time of application**.

Appendix (term)

Cabinet

Cabinet is one management space arranged on this Service. If a cabinet is created, Cabinet group which specifies user who can use cabinet is assigned, and Cabinet Administrator (CA) is defined. Cabinet Administrator has privilege as administrator in cabinet (contents of privilege are mentioned later). In addition, user who only user who belongs to Cabinet group can use data in cabinet, and does not belong to Cabinet group cannot recognize existence of cabinet itself.



Definition of role

Role in this Service is defined as follows.

- **User**

  Person using this Service is pointed out. User is divided into administrator (people with management authority), and general user by role.

- **Administrator**

  User with special authority for performing setting and management to this Service is pointed out. Administrator is divided into Service Maintenance Administrator (SMA), Cabinet Administrator (CA), and Group Administrator (GA) by the role. Visitor can use three, CA, GA, and general user.

- **General user**

  User without special authority as administrator is pointed out.

- **Service maintenance administrator(SMA)**

Administrator of this whole Service is pointed out. Although SMA can perform various kinds of setting, cannot perform reference of substance file of data without “Access control”.

- **Cabinet administrator(CA)**

  CA can perform all data operation in cabinet, user's creation, Local group operation, GA role operation to local group, and CA appointment / release to user in cabinet.

- **Group administrator (GA)**

  GA can perform member changing of local group, users in local group are owner changing of owner's data and Access control changing, GA appointment and release to another user in Local group. In addition, only user can be appointed GA. Group cannot be appointed as GA. Moreover, GA is not indispensable setting.

- **Owner**

  Owner points out “owner of data”. To data which is Owner, it has owner authority. If there is owner authority, changing of Owner and changing of “Access control” are possible. When Owner is group, all users that belong to group have owner authority.

- **Lock owner**

  User who is performing lock to data is pointed out. It has lock owner authority to data. Other users except lock owner cannot update and delete data locked. Unlock of data can change lock owner itself, CA, SMA. When the lock owner is a group, user who has CA or SMA role only can unlock it.

- **Classification of group**

  Group is classified into Cabinet group and Local group.

- **Cabinet group**

  It is a group which exists in cabinet and the form of 1 to 1, and user belonging to Cabinet group will call it user of corresponding cabinet. Cabinet group cannot be referred to from user of other cabinets. CA can change member in Cabinet group from which self serves as CA.

- **Local group**

  It is group defined within cabinet. Cabinet can have two or more Local groups. Local group cannot be referred to from user of other cabinets. Moreover, user of other cabinets cannot be added to Local group. Therefore, composition member of Local group will surely belong to Cabinet group. Therefore, although Local

group is served like child group of Cabinet group, function of division by class of group is not supported.

User operation ambit with each role

User operation ambit with each role is as follows.

Operation ＼ Role	SMA	CA	GA	General User
Setting of SMA (appointment, dismissal)	○	―	―	―
Setting of CA (appointment, dismissal)	○	○	―	―
Setting of GA (appointment, dismissal)	○	○	○	―
User new creation	○	○※1	―	―
User attribute changing	○	○	―	―
User deletion	○	○	―	―
User addition in cabinet group	○	―	―	―
User deletion from cabinet group	○	○※2	―	―
User addition in local group	○	○	○	―
User deletion from local group	○	○	○	―
User search in cabinet	○	○	―	―
User search besides cabinet	○	―	―	―

- ✓ When CA creates user, user who creates always belongs to cabinet in which create user is CA.
- ✓ If CA deletes user from Cabinet group, it becomes impossible to refer to user for CA. Moreover, can set this ID and it cannot be re-registered, either.

Data operation ambit with each role

Data operation ambit with each role is as follows.

Operation ＼ Role	SMA	CA	GA	General User
Data new creation	Freely possible	Inside of cabinet is freely possible.	Followed Access control	Followed Access control
Data attribute change	Freely possible	Inside of cabinet is freely possible.	Followed Access control	Followed Access control
Data deletion	Freely possible	Inside of cabinet is freely possible.	Followed Access control	Followed Access control
Data movement / copy	Freely possible	Inside of cabinet is freely possible.	Followed Access control	Followed Access control
File download	Followed Access control	Inside of cabinet is freely possible.	Followed Access control	Followed Access control
Registration and renewal of file	Freely possible	Inside of cabinet is freely possible.	Followed Access control	Followed Access control
Owner change	Freely possible	Inside of cabinet is freely possible.	Case of GA itself / group to which GA belongs/ user to whom he belongs to Local group of GA is Owner is possible.	Case of User itself / group to which user belongs is Owner is possible.
Access control change	Freely possible	Inside of cabinet is freely possible.	Case of GA itself / group to which GA belongs/ the user to whom he	Case of User itself / group to which user belongs is

			belongs to Local group of GA is Owner is possible.	Owner is possible.
Lock of data	Freely possible	Inside of cabinet is freely possible.	Followed Access control	Followed Access control
Unlock of data	Freely possible	Inside of cabinet is freely possible.	GA itself	Only file whose oneself is lock owner is possible.