「マルチメディア，分散，協調とモバイル
(DICOMO2013)シンポジウム」 平成25年7月

統合 ID 管理におけるメンバ属性を用いた拡張可能なグループ管理

清水さや子[†1][†2]　戸田勝善[†2]　岡部寿男[†1]

近年，一組のアカウントとパスワードで，複数のシステムが利用できる統合 ID の導入が進んでいる．統合 ID を管理する際，統合 ID を使用するユーザの情報やシステムの情報を中央で一元的に管理することが求められる．しかし，大学のような分散管理組織では，ユーザの情報やシステムの情報は，それぞれの担当部局で管理されているため，それらを中央で統合的にまとめて管理することが難しく，実際にも統合的な管理が普及していない実態がある．本研究では，大学のような分散管理組織において，中央での統合的な管理を実現する統合管理システムと，統合管理を行う際に課題とされるグループ管理に対して，メンバ属性を用いた拡張可能なグループ管理システムの提案を行う．提案では，分散管理組織の特性を生かし，それぞれの情報に対して担当範囲と担当係を割り当て，担当係ごとに分散して管理を行う．中央では，統合管理システムが，分散して多重に管理されている情報を統合的に取りまとめる．現在，東京海洋大学での実運用を想定し，提案するシステムを二段階に分けて設計し実装している．第一段階では，統合 ID の利用者や統合 ID を利用するシステムの情報を統合的に管理する統合管理システムの設計を行う．そして，統合管理システムを管理運用していく上で顕在化した，複雑なグループに対する対応方法の検討を，第二段階で行う．組織にはさまざまなグループが存在しており，一人につき複数のグループに所属していることが多いが，ユーザ登録を分散して行った場合，登録担当係では主の所属グループ以外の把握が難しい．そこで，ユーザの所属するグループが複雑な場合に対して，複雑なグループやメンバ属性を統合的に管理が行えるグループ管理システムを設計し実装する．

Attribute based extenshible group-membership management in integrated ID management

SAYAKO SHIMIZU[†1][†2]　MASAYOSHI TODA[†2]　YASUO OKABE[†1]

1. はじめに

近年，多くの組織において，一組のアカウントとパスワードで，複数のシステムが利用できる統合 ID の導入が進んでいる 1)2)．最近では，大学間連携のための認証基盤のサービスも整備されつつあり 3)4)，統合 ID を導入する組織も増えている 5)6)．そして，統合 ID の利用者や統合 ID を利用するシステム（以下，連携システムとする）の増加に伴い，管理運用においてもさらなる工夫が必要となる．

統合 ID を管理する際，ユーザ情報や連携システムに対する利用権を中央で一元管理することが望まれる．しかし，大学などの組織に典型的なユーザ情報やシステム情報が中央で一元管理されていないことより，分散的に管理されている組織（以下，分散管理組織とする）において，統合 ID を一元管理することは難しい．

分散管理組織では，大学などの組織のように，学生や教職員の他に様々な身分の人が様々な期間在籍しているが，身分ごとに管理部局が異なり，それぞれの部局で管理しているため，全構成員の把握が難しい．また，提供する様々な情報サービスは中央で管理するサービスの他に，学部や学科等の部局ごとに異なるサービス（以下，部局管理システムとする）があり，それらを中央で一元管理しているのではなく，部局ごとに分散して管理されている場合も多いため，全情報サービスの把握が難しい．このような分散管理組織において，統合 ID を導入する際，中央で統合的にまとめて管理することが求められるが，統合的な管理はなかなか普及されない実態がある．統合的な管理の普及されない理由は，それぞれの部局で管理している情報を，中央で統合的にまとめることが難しく，統合的にまとめるための情報が収集できた場合でも，内容が複雑なことにより，取りまとめが困難であること，などが上げられる．

本研究では，大学のような分散管理組織において，中央で統合的な管理が実現できるよう対応策の提案を行う．提案では，分散管理組織ではさまざまな情報が分散して管理されているという特性を生かし，それぞれの情報に対して担当範囲と担当係を割り当てることで，それぞれの情報の管理は分散して行う．その際，中央システムでは，それぞれの情報の管理を行わず，分散して管理された情報を統合的に取りまとめるシステムの管理を行う．具体的には，システムの提案は二段階に分けて行う．まず，第一段階では，統合 ID の利用者情報や連携システム情報を，統合的に管理するためのシステムの設計を行う．そして，設計したシステムを実際に管理・運用していく上で，顕在化した複雑なグループに対する対応方法の検討を，第二段階で行う．第二段階では，複雑なグループに対して，メンバ属性の管理が統合的に行えるシステムの設計を行う．なお，第一段階で実現した統合管理システムは，最近，類似する商品が市場に出てきているが 7)8)，統合管理システムではグルー

†1 京都大学
Kyoto University
†2 東京海洋大学
Tokyo University of Marine Science and Technology

プ分けとそれぞれのポリシーが重要になることより，本章では，グループに関する管理について重点的に述べる．

グループは，身分や所属により利用権が異なるサービスに対して，利用権の取り決めを行うために必要とするものである．組織内には様々なグループが存在し，1 人につき複数のグループに所属していることが多いことより，グループ分けの定義は重要になる．分散管理組織では，グループ分けを行う際，中央では把握できないグループが存在することや,常に変動するグループやメンバ属性が存在する．それらに対して，全てを中央で一元管理することは，非常に負荷がかかるため難しい．これらより，本研究では，これらの複雑なグループに対しては，メンバ属性を用いて拡張可能なグループ管理ができる仕組みを提案する．

2 章では分散管理組織と分散管理組織におけるグループについて説明し，大学のような組織におけるグループの整理を行い，組織構成に基づくグループ分けを行う．3 章では，提案の第一段階として，統合 ID を管理するために設計した統合管理システムと，運用上見えてきた課題について述べ，4 章では，提案の第二段階として，統合管理システムの運用上の課題であるグループ分けについて提案するグループ管理システムについて述べ，最後にまとめを述べる．

2. 分散管理組織におけるグループ

2.1 分散管理組織

大学や大学共同利用機関等の組織は，学生や教職員が在籍する以外に，派遣等の契約職員や企業からの共同研究者など様々な身分の者が様々な期間在籍し，組織の様々なシステムを利用するという傾向がある．そして，学生，教職員，派遣等の職員，研究等で出入りする共同研究者などに対して，身分ごとに担当部局が分かれている．しかし，これらの組織の全構成員をとりまとめる部局がないことが多く，全構成員を把握することが非常に難しい．

また，大学などの組織では，様々な情報サービスを提供しているが,提供するサービスは全体のサービスのほかに,学部や学科のセグメントごとに異なるサービスがあり，身分・所属により利用できるサービスが異なる．これらの情報サービスのすべてが中央で一元管理されているのではなく，組織の特徴として縦割り運営が行われていることや，それに対して学部や学科ごとの特性を出すため，部局ごとに個別に管理されている場合も多い．最近では，全学的に統合認証システムを導入している組織も多いが，連携システムに対して，中央システム側では，アクセスしてきた情報の照合をすることはできるが，管理部局の異なる各システムからの認証に対しては，利用者に利用権を与えるいわゆる認可を行うことは難しく，行う場合は管理者に非常に負荷がかかるため行わないことが多い．

2.1.1 分散管理組織における先行研究

著者らは分散管理組織において，IC カードを導入する際，担当部局が多部局にわたっており，全体把握や管理が難しいとされている一時利用者に対して，身分・所属ごとに異なるサービスが利用できる仕組みを提案している．

一時利用者に対する管理運用の煩雑さやカード発行に関するコストを最低限に抑えるため，一時利用者には IC カードを発行せず，本人が日常利用している交通系 IC カードなどの共通規格に基づいて発行されている IC カード（一般カードと呼ぶ）を使い，IC カードを使ったサービスが利用できるようにする．その際，システムの重要性に応じて要求されるセキュリティレベルの格付けを行うが，中程度以上のセキュリティレベルが要求されるシステムに対しては，本人のみ知りうるキー情報（以下，PIN コードとする）による認証を併用する．PIN コード認証を行う際，分散管理組織では，それぞれのサービスに対する利用者の管理は，提供するサービスを管理する部局ごとに行うことより，中央で一元管理することは難しい．そのため，部局ごとの管理者が容易に管理できるよう，カード内情報のカードごとに異なる値を利用して，PIN コードを生成する手法を提案している（図 1）9).

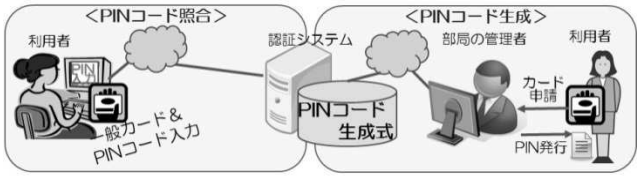


図 1　PIN コード生成手法

先行研究では，分散管理組織において，管理が難しい一時利用者が，それぞれの部局ごとに提供するサービスを利用する際，中央ではなく，部局ごとに提供するサービスの管理者が利用希望の一時利用者に対して PIN コードを発行すれば，それぞれのサービスが利用出来る仕組みを提案している．本研究においても，同じく分散管理組織において，統合 ID を導入する際，統合 ID の利用者と連携システムに関する情報は，それぞれの担当部局によって管理し，中央ではそれらを統合的に管理する仕組みを提案する．さらに，これらの管理を行う際に問題となる複雑なグループに対しては，それぞれのグループに担当係を割り当て，それぞれの担当係がメンバ属性を管理し，それらを中央で統合的に管理する仕組みを提案する．

2.2 グループ

グループは，身分や所属により利用権が異なるサービスに対して，グループごとに利用権を決める際や，ユーザ情報の管理をグループごとに行う際などに利用する．

組織内には様々なグループが存在する．グループには，ユーザの所持する属性を利用したものが多く，例えば，学部，学科，研究科，附属センター，委員会などの所属によ

るグループ，教員，職員，常勤教職員，非常勤職員，非常勤講師，派遣契約，客員教員などの身分によるグループ，研究会，研究チーム，サークルなどの所属や身分を超えた集団のグループなどがある．グループは，１人につき１つのグループではなく，複数のグループに所属していることが多い．

2.2.1 グループ管理の製品例

グループ管理の概念は，様々なグループウェアやファイルサーバ上においても存在しており，グループごとに利用権の設定を行うことができる 10)11)12)．また，統合 ID の認証システムとして使用される LDAP や Active Directory などにおいても，ユーザ管理やグループ管理，グループポリシーの作成が可能である．ただし，上記のシステムでは，ユーザ管理やグループ管理，グループポリシーの作成等はシステムの全管理者権限が必要となる．

2.2.2 分散管理組織におけるグループ

大学のような分散管理組織では，中央で存在する全てのグループを定義し，それぞれのグループに対するメンバ属性の管理をすることが難しい．

例えば，主の所属が工学部である教授が，医学部を兼務し，工学部と農学部で構成する全学委員会の委員であり，工学部と医学部で構成する研究会メンバである等，一人で複数の所属に属していることが多い．しかし，中央では，主の所属である工学部は把握できるが，医学部の全所属者を把握するのは学部事務の担当係，全学委員会のメンバを把握するのは委員会の担当係，研究会のメンバを把握するのは研究会の担当者等，分散管理組織ではグループごとにメンバを把握できる部局が異なる．そのため，中央で把握できる工学部グループのみに割り当てられた場合，医学部グループが利用出来るシステムや，委員会や研究会所属者だけが利用できるシステムを使用したい場合でも，該当グループに所属していないため，利用できない状態となる．

2.3 分散管理組織におけるグループ分けのパターン

グループを整理していくため，大学のような組織に存在するグループを大きく以下の 3 つのパターンに分けた．それぞれのグループに対する特徴と整理を行う（表１）．

① 主のグループ：組織図等により公式的に公表されてグループであり，ユーザの身分・所属ごとに異なる担当部局(本部事務)が把握できるグループ．

② 公式グループ：上記①以外の組織図等により公式的に公表されてグループであるが，ユーザの身分・所属ごとに異なる担当部局(本部事務)では，所属の把握が難しいとするグループ．

③ 非公式グループ：組織図等により公式的に公表されていないグループ．研究チームや研究サークル等．

本研究では，これらの３パターンに対して，グループの管理方法とメンバ属性の管理方法についての検討を行う．詳細は４章にて述べる．

表 1　グループ分けのパターンと特徴

	主のグループ	公式グループ	非公式グループ
グループ作成のベースとなる物	組織図等による	組織図等による	特になし (それぞれの担当係の必要に応じて作成)
特徴	ユーザ情報登録時に割当てるグループ	ユーザ情報登録担当者では，把握が難しいグループ	組織図等にはこだわらない必要に応じて作成されるグループ
存在把握の可否	可能	可能	把握困難
メンバ属性の管理担当者（把握部局）	人員担当部署 (ユーザの身分所属により異なる担当係)	各々の担当事務（公式グループにはそれぞれ担当事務がいる）	グループを必要とする連携システムの担当係等
グループの変動	組織編成時以外は固定	組織編成時以外は固定	随時変動あり（中央で把握不能）
備考	組織改編時以外は変更なし	組織改編時以外は変更なし	以下の問題可能性有 ・不要なグループがいつまでも残る ・グループ管理者が不明になる ・メンバ属性情報が更新されない

3. 統合管理システムの構築と運用評価

統合 ID を使用するユーザや連携システム，グループおよびメンバ属性について，それぞれの情報は担当係による分散的な管理を行うが，システム上では統合的な管理を行う．これらの第一段階として，ユーザや連携システム，グループ情報を統合的に管理する統合管理システムを設計した．この統合管理システムは現在，東京海洋大学で稼働しているが，管理・運用の経験上見えてきた複雑なグループに関する対応について，第二段階でグループとメンバ属性を統合的に管理するグループ管理システムの設計を行う．第二段階については４章で述べる．

3.1 統合管理システムの構築

一般的に大学のような組織でユーザ登録を行う際，ユーザからの申請により登録を行う方法，ユーザの身分・所属に応じた本部事務の人員担当部局がそれぞれのユーザを管理する DB より必要な情報を抜き出し，その情報を元に登録する方法，それぞれの人員担当部局が管理する DB と連携させ，自動的にユーザ情報の登録・削除を行う方法などが考えられる 13)．

東京海洋大学では，ユーザの身分・所属に応じた本部事務の人員担当係がそれぞれのユーザを管理する DB より必要な情報を抜き出し，それぞれの人員担当係がユーザ情報を登録する．教職員は教職員担当係，学生は学生担当係，派遣職員等の契約が発生する職員は契約担当係など，身分に応じて担当係が異なる．過去にはユーザからの申請により中央で登録を行う方法を採用していたが，採用後，本人

からユーザ登録の申請が行われないため，アカウントが発行されないことや，退職後も削除申請が行われず，いつまでもアカウントが利用できる状態になっていることが頻発し，アカウントの管理が曖昧になっていたことより，それぞれの人員担当係が登録・管理を行うことになった．その際，人員担当係が管理する DB と連携させることも検討したが，個人情報を扱うシステムに対してとの連携のため，取り決めに非常に時間がかかることより，見送った．

ユーザの身分・所属に応じた本部事務の人員担当係がユーザ登録を行う際，同時にグループ割り当ても行う．各登録担当係には担当する範囲内の登録権限を与えることにより，教職員担当係であれば，教職員が所属するグループに対してのみ割り当てることができ，学生や派遣職員等が所属するグループに対して割り当てることはできない．また，各登録担当係は，それぞれ登録した担当範囲内のユーザ情報のみ変更や削除を行う事ができる．

統合管理システム上には，グループに対して連携システムの利用権を設定したリストを格納している．ユーザのグループが割り当てられたあと，そのリストを元に，利用権が設定されている連携システムに対して，ユーザ情報の割り当てを行うが，中央で管理する連携システムに関しては，システム管理者により個別に利用権の変更を行うこともできる（図２）14)．

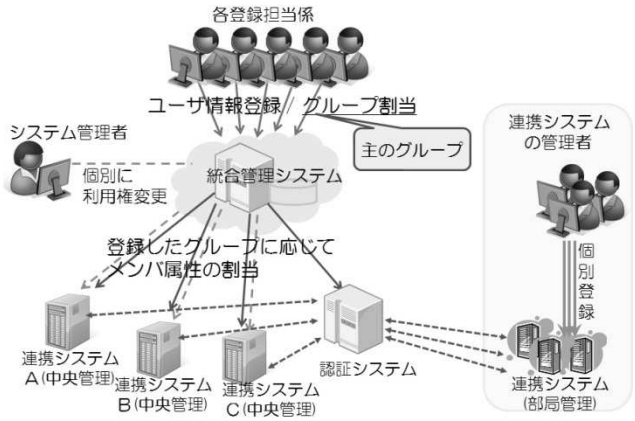


図 2　東京海洋大学の統合管理システム

3.2 グループ属性と管理

東京海洋大学では，ユーザ情報の登録時に 2.2 の主のグループとして，身分に関するグループ，所在地に関するグループ，詳細な身分に関するグループの 3 つのグループを，それぞれのユーザに対して割当てる．所属によるグループは設定していない．中央で管理する連携システムでは，所属ごとに利用権が異なるものがないことと，ユーザの所属が変更になることが多いため，所属グループを作成することにより管理が煩雑になると考えるためである．

3.2.1 主のグループと利用権

身分に関するグループは，教職員，学生，それ以外の３つの属性である．教育システム上の E-Learning ソフト利用時に，利用できるレベルが教職員と学生および一般で異なるため，必要とする．所属地に関するグループは，品川，越中島，その他の 3 グループである．所属地により，電子ジャーナルの利用できる範囲が異なるため，必要とする．

詳細な身分に関するグループは，学生であれは学部・学科および入学年度ごと，教職員であれば，教員，有期雇用教員，名誉教授，客員教員，技術系職員，事務系職員などの属性がある（表 2）．教職員以外にも，派遣契約の職員や研究員等が多く存在することより，それらの身分を含めた属性は，約 100 のグループが存在する．約 100 のグループに対して中央で管理する連携システムの利用権がすべて異なるわけではなく，ユーザ情報の管理運用における便宜上のため，詳細に分けている．例えば，教員と有期雇用教員の違いは，有効期限の有無の違いであるが，有期雇用教員グループでは，契約更新の際に有効期限の延長が必要なグループとして，分けていることで管理しやすくしている．また，詳細な身分に関するグループは，それぞれのグループ属性と担当係を割り当てることで，登録担当係の担当範囲の指定を行う．

表 2　グループ分けと利用権の例

グループ種別	Windows ドメイン	教育用プリンタ	教育用 Linux	LMS	研究システム	図書システム
総管理者	○	○	○	○	○	○
教員	○	○	○	○	○	○
有期雇用教員	○	○	○	○	○	○
名誉教授	○	○	○	○	○	×
客員教員	○	○	○	○	○	×
技術系職員	○	○	○	○	○	○
事務職員(常勤)	○	○	○	○	×	○
事務職員(非常勤)	○	○	○	○	×	○
受入研究員等	○	○	○	○	○	×
派遣職員	×	○	○	○	×	○

3.2.2 主のグループの管理方法

主のグループは，公式的に公表されている属性によるものであるため，中央システムの管理者は把握可能であるため，あらかじめ設定しておくことができる．ユーザ登録時に各担当係があらかじめ設定されているグループからそれぞれの必要な属性を割り当てる．

それぞれのグループは，大きな組織改編がない限り，変更は行わないが，詳細な身分に関するグループの設定は年度始めに見直しを行い，新入学生等に対応するグループの追加，卒業して不要になったグループの削除等を行う．

3.3 運用により出てきたグループ管理の問題

統合管理システムは，連携システムが中央で管理するシステムを対象に設計していた．中央で管理するシステム以外に，事務局内の 3 つの部局がそれぞれ管理するシステム

を連携システムとして認証時に連携させたいという希望があった．しかし，中央で管理するシステムとは異なることと，中央で管理するシステムでは認証は行うことができるが，認可を行うことができないことより，3 つのシステムについては，それぞれのシステムの管理者が個別にユーザ登録を行い,認証時のみ認証システムに参照を行っていた．

近年，学科や研究室，研究グループで提供するシステムでも，認証の際に中央の認証システムと連携したいという要望が増えている．しかし，中央で管理する統合管理システム上には，部局管理システムに対応するグループ属性がないことが多いことや，中央で管理するシステムでは，部局管理システムの認可を行うことができないため，事務局管理のシステムと同様，個別にユーザ情報の管理を行い，認証のみ認証システムを参照することになる．

しかし，部局管理システムの中には，利用者が全く同じメンバであるシステムも多々あることより，統合管理システムではさらなるグループ分けの検討が必要になった．ただし，既に稼働しているシステムに対して拡張することが難しいことと，中央の統合管理システム上で常に変動があるかもしれないグループの管理を行うことは，グループ数が膨大になりシステムが破綻するおそれも考えられるため，新しく拡張可能なグループ管理の検討を始めることとなった（図３）．

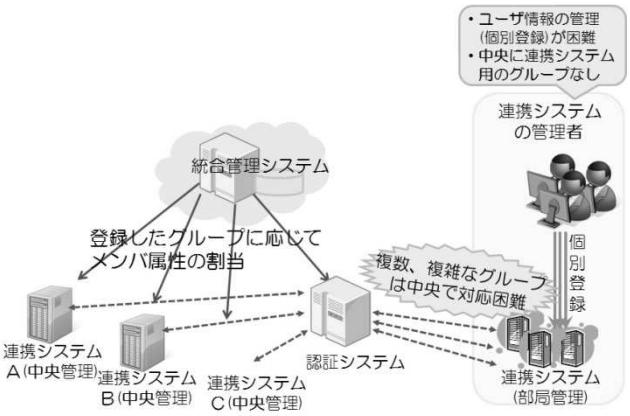


図 3　連携システムとグループ

4. グループ管理システムの実装と評価

本章では，第二段階として，統合管理システムを運用していく上で，顕在化してきた複雑なグループに対して，グループとメンバ属性を統合的に管理する方法について提案を行う．提案するシステムでは，先に稼働している統合管理システムには手を加えず，新たにメンバ属性を用いた拡張可能なグループ管理ができるグループ管理システムの提案を行う．

4.1 グループ管理システムの検討

分散管理組織では，それぞれの情報が分散して管理されているため，グループ管理を行う際も，それぞれのグループに対して担当係を割当て，担当係が管理を行う情報に対して，中央では統合的に管理できるシステムとする方がよいと考える．また，既に稼働しているシステムに手を加えないことより，複雑なグループの管理が可能なシステムを新たに構築することを検討する．主のグループと主のグループに属するメンバ属性は統合管理システム上で管理することより，それ以外の公式グループや非公式グループを新しく管理できるシステムを検討する．

公式グループと非公式グループはグループ作成方法やメンバ属性の管理方法について異なるため，それぞれ分けて検討を行っていく．

4.1.1 公式グループの検討

公式グループは，ユーザの登録担当部署では，所属の把握が難しいとされるグループであるが，組織図等に基づくグループであることより，中央システムの管理者が存在するグループを把握することができることより，中央システムの管理者があらかじめ作成しておくとよいと考える．その際，例えば東京海洋大学では，図 4 のように，組織図を元に学部や学科に対して階層化しておくことにより，全ての所属に対して，グループ管理を行わなくても，下位階層から上位階層にグループ情報を引き継ぐことが可能となる．公式グループは公式的にメンバ属性を把握している担当事務の係が存在することより，それぞれのグループに対しては担当の事務係を割り当て，メンバ属性の管理を行えばよいと考える．

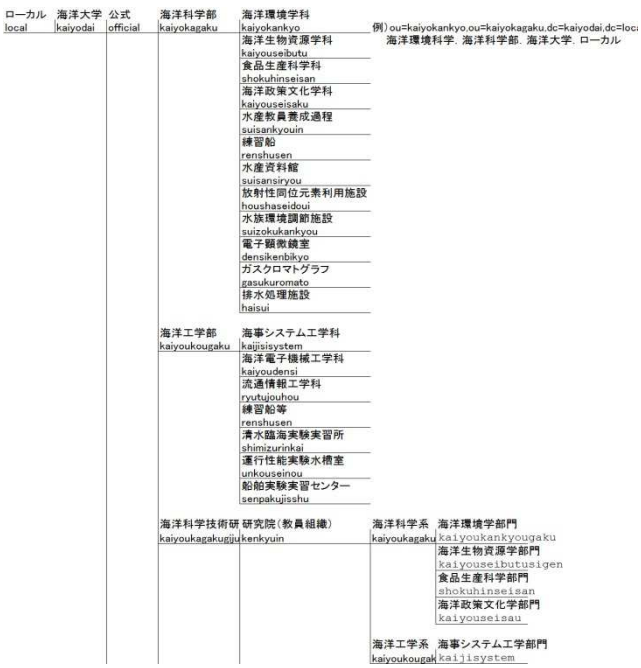


図 4　東京海洋大学組織図の階層化図（一部）

4.1.2 非公式グループの検討

非公式グループは，組織図等による公式的に公表されているものではないため，存在するグループを知ることがで

きないため，中央システムの管理者があらかじめグループを設定することができない．また，担当の事務の係が存在しないことも多い．さらに，グループやグループに所属するメンバ属性の変更が随時発生することが考えられる．そのため，非公式グループの作成を希望する部局管理システムの管理者などに対して，必要に応じてそれぞれのグループの担当係として割り当て，グループの担当者が，グループの作成からメンバ属性の登録や管理を行えるとよいと考える．

また，非公式グループは，公式な担当係が存在せず，それぞれのグループに応じて担当者がグループを作成するため，以下の問題が起こることが考えられる．

- グループが不要になっても削除されず，いつまでも使わないグループが残る
- グループの担当者が退職等により，いつの間にか不明になり，メンバ属性の変更に対応できない
- グループの担当者の変更が多く，誰がグループの担当者かわからなくなる

これらの問題については，別途，対応方法の検討が必要となる．

4.2 グループ管理システムの実装

4.2.1 グループ管理システムの構成

グループ管理システムでは，OS は CentOS 6.4，ソフトは OpenLDAP 2.4 と Apache2.2 を用いて実現する．OpenLDAP では，LDAP サーバのプロキシサーバ（以下，LDAP Proxy とする）を構築し，LDAP Proxy では，それぞれのグループの担当係によって，グループおよびグループに属するメンバ属性の定義を行う 15)16)．公式グループに対しては，所属するユーザを特定するため，LDAP サーバより uid 情報を取得し，グループ管理 DB と同期をとる（図 5）．

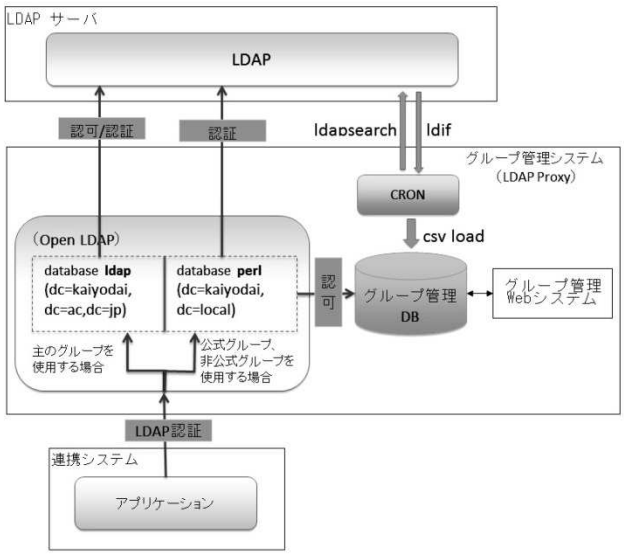


図 5　グループ管理システムの構成図

4.2.2 グループ管理システムを使った認証認可方法

連携システムから公式グループもしくは非公式グループを使って認証認可を行う場合，図 5 のように，"dc=kaiyodai,dc=local"による問合わせを行い，perl バックエンドで処理を行う．この場合， perl プログラムにより，あらかじめ登録している「グループ管理 DB」に問合せて認可を行い，認証は LDAP サーバに問合せ，その結果を返す．主のグループを使って認証認可を行う場合，もしくは，グループを使用しない場合，"dc=kaiyodai,dc=ac,dc=jp"による問合せを行い，LDAP サーバによる認証認可を行い，その結果を返す．

4.2.3　既存システムとの連携

既に稼働している統合管理システムには手を加えないことより，既に稼働している連携システムの問合せは，これまでどおり既存の認証システムに問合せを行う．

今後，新しく連携するシステムにおいては，既存の認証システムではなく，グループ管理システムに問合せを行い，グループ管理システムの中のポリシーに従って認証認可を行う（図 6）．本システムの本格稼働後は，既に稼働しているシステムに対しては，すべての連携システムがグループ管理システム経由で認証認可が行えるよう，連携システムのリプレイス時等に合わせて，問合せ先をグループ管理システムに変更していくことを検討する．

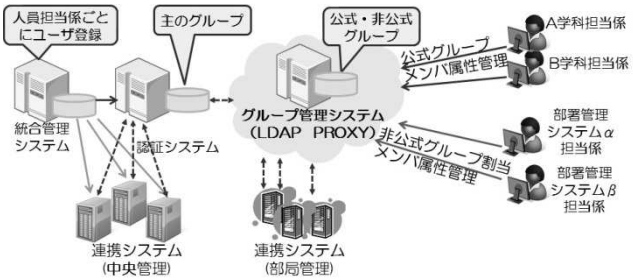


図 6　グループ管理システムの構成

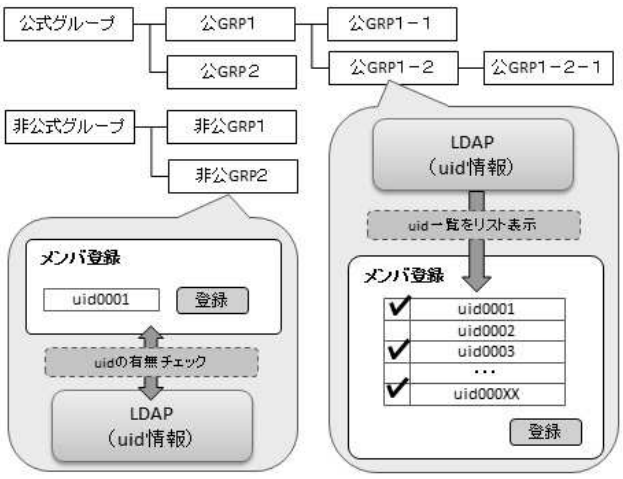
4.3 公式グループと非公式グループのメンバ属性割当て

公式グループと非公式グループはメンバ属性の管理方法が異なるため，それぞれのグループごとにメンバ属性の割り当て方法，管理方法について述べる．

公式グループのメンバ属性の割り当て方法は，それぞれのグループの担当係が Web 上のグループ管理システムで行う．それぞれのグループに対するメンバ属性は LDAP の uid 情報を取得することで，表示されたユーザの一覧より，グループに必要なメンバを選択する．ユーザ属性の一覧は，ユーザの数が多ければ多いほど選択が困難になるため，ユーザの検索条件（利便性を考慮し，uid，ユーザ英語名，ユーザ日本語名は，その一部を指定し曖昧検索が可能）を指定することで，ユーザ属性の一覧に表示する件数を絞り込み，選択時の負担を軽減することを検討中である．また，階層化をすることより，下位階層グループのメンバ属性が

親グループに引き継ぐことにより，管理の軽減を行う．階層化を行う際，下位階層グループに所属していないが，親グループのみに所属するメンバが存在することも想定し，親グループの担当係は下位階層グループから引き継がれ他メンバ以外に新たにメンバを追加することが可能である．

非公式グループの担当係は，公式グループのように管理を委任された者ではない．そのため，メンバ属性は，公式グループと同様に LDAP の uid 情報を取得した場合，登録されているユーザが一覧に表示されるため，個人情報の取り扱い問題に発展する可能性もあるため，非開示とし一覧表示は行わない．それぞれ必要なメンバの uid 情報を個別に指定し登録することで，メンバ属性の管理を行う．その際，uid 情報の有無は，登録時に LDAP に問い合わせを行う．非公式グループの階層化においては，現時点では多くの要望がないため，本研究においては，並列的に管理を行う．ただし，グループを割り当てる際，グループ名の重複を避けるよう命名規則の作成が必要になるため，グループ名の最初には作成順が分かる文字列を指定する．



【認可用メンバ登録情報】

公式フラグ	階層レベル	親グループ	自グループ	メンバ
1	2	公GRP1	公GRP1-2	uid0001
1	2	公GRP1	公GRP1-2	uid0003
1	2	公GRP1	公GRP1-2	uid000XX
0	1	(空)	非公GRP2	uid0001

図 7　メンバ属性割り当て方法

本研究においては，グループの管理者には複数人を割り当てることとする．複数人でグループやメンバ属性の管理が行えることにより，担当者が 1 名の時に比べて，グループやメンバ属性の正確な情報の管理が行われることを期待する. また, 担当者が複数名いることで 1 名が退職しても，他の担当者が対応できることより，担当者不明になる確率が下がり，正確な情報の管理が期待できると考える．ただし，担当者を複数名設定することで想定外の更新が行われることも考えられるため, 運用における対応が必要になる．

4.4 グループ管理システムの評価

本研究で構築したグループ管理システムにおいて，管理する公式グループと非公式グループのメンバ属性は，中央システムの管理者による管理が難しいものである．公式グループはそれぞれのグループに事務の担当係を割り当てるが，メンバ属性が変更になる度に，登録情報の変更をする必要がある. 公式グループは公のグループとすることより，メンバ属性が常に最新の情報にしておく必要がある．しかし，実際は全ての公式グループが最新状態を保つことは難しく，最新状態であることが把握できるのは担当係だけであるため，運用方法の検討が必要であると考える．また，本研究では，担当係は中央システムの管理者が割り当てることとしているが，担当係を事務系の職員とした場合，数年に 1 度は異動があるため，担当者の変更に関する作業が発生する．これは，グループ数が増えれば増えるほど，作業回数が増加するため，担当係が変更になる際の引き継ぎ方法等の検討が必要になると考える．

非公式グループは，連携システムの管理者が必要に応じてグループを作成し，メンバ属性を登録するものであることより，公にはグループの存在が分からないため，常に最新状態を保つ必要はないが, 4.1.2 のような問題が起こる可能性がある．本研究においては，問題回避のために，1 グループにつき担当者を複数名割り当てられることとしたが, それだけでは，問題が解消されない可能性も高く，また，そのことにより別の問題が発生する可能性もある．一定期間，使用されていないグループについては削除を行うことや，一定期間ごとに担当当者が存在しているか確認を行うなど，今後，運用しつつ，対応を検討していかなければならないと考える．

5. まとめ

大学のような分散管理組織において，統合 ID の管理をする際，中央システムでは，ユーザ情報や連携するシステムに対して統合的な管理が求められるが，実際には統合的な管理の普及が進んでいない．本研究では，中央で統合的な管理の普及が進まない理由の中から，取りまとめが困難となる原因の一つである，グループ分けが複雑な場合において，対応策の提案を行った．まずは，大学におけるグループを主のグループ，公式グループ，非公式グループの 3 パターンに分け，それぞれのグループに対して，特徴の整理と，統合 ID を統合的に管理する際の，グループの管理方法とメンバ属性の管理方法についての検討を行った．

そして，統合 ID の利用者や連携システムの統合的に管理を行うためのシステムの設計を，まず，第一段階として行い，実際に管理・運用を行い，経験上見えてきた問題から第二段階で解決策としてグループを管理するシステムの設計を行った．

第一段階では，ユーザの身分・所属ごとに異なる登録担

当係がユーザの登録を行い，その際にグループの割り当てを行う．グループ割り当ての際，ユーザは多くのグループに所属していることが多いが，登録担当係で把握できるのは主のグループのみである．それ以外のグループも場合によっては把握可能であるが，全てのユーザに対して，全てのグループを正確に割り当てる事は非常に難しいことより，ユーザ登録時に割り当てるグループは主のグループのみとした．

次に，第二段階では，複雑なグループ管理が行えるよう，グループ管理システムの設計を行った．分散管理組織におけるユーザや連携システム情報，グループやメンバ属性の管理を行う際，中央システムの管理の負担を最小限に抑えたいことより，それぞれの担当の部局が管理を行えるシステムとした．主のグループ以外にユーザが所属するグループの対応として，公式グループは，組織図等によるグループを設定し，それぞれのグループに対して担当係を割り当て，メンバ属性を設定できるようにした．非公式グループは部局管理システムの担当者等が必要に応じてグループを作成し，それぞれメンバ属性を登録することで，それぞれの担当係や担当者により，グループとメンバ属性の管理ができる仕組みを構築した．それぞれの担当係や担当者がグループおよびメンバ属性を管理することより，中央システムの管理者は，グループやメンバ属性を管理する負担は増加しない．

本研究では，統合 ID を導入する際に，ユーザや連携システムの情報，グループ情報を統合的に管理するために統合管理システムを構築し，さらに複雑なグループに対して，グループやメンバ属性を統合的に管理するためにグループ管理システムを構築した．グループ管理システムでは，グループやメンバ属性の管理にそれぞれの担当係を割り当てることで，グループ分けが複雑な場合でも，対応可能となる．本研究で提案するシステムは，これまで難しいとされていた分散管理組織における統合的な管理が実現できると考える．

提案するシステムについては，統合管理システムは，現在，東京海洋大学にて実稼働中であるが，グループ管理システムについては実装している段階である．今後，実稼動に向けて，まずは試験稼働を行い，評価を行っていく予定である．提案するグループ管理システムは，連携システムの認可に対して使用することが目的であったが，正確にグループ管理を行うことで，ポータルシステム利用時のお知らせをグループごとに発信するなど，さまざまな用途に応用できることを期待する．

参考文献

1) 江原康生「大阪大学における新全学 IT 認証基盤システムの構築と運用」電子情報通信学会論文誌 D,Vol.J95-D,No.5,1172-1182,2012

2) 沖野浩二，布村紀男「富山大学における認証基盤の整備による業務軽減評価」学術情報処理研究 No. 14, 31-39, 2010

3) 中村素典，山地一禎，片岡俊幸，西村健，庄司勇木，古村隆明，岡部寿男「学術認証フェデレーションを活用するサービスの展開」第 27 回インターネット技術第 163 委員会（ITRC）研究会 CIS 分科会,2010

4) 学術認証フェデレーション http://www.gakunin.jp/ja/

5) 松平拓也，笠原禎也，高田良宏，東昭孝，二木恵，森祥寛「大学における Shibboleth を利用した統合認証基盤の構築」情報処理学会論文誌 52(2), 703-713, 2011

6) 渡辺健次，大谷誠，江藤博文「全面的に Shibboleth に対応した佐賀大学の学術情報基盤システム」教育システム情報学会研究報告 25(3), 43-48, 2010

7) 木幡康博，及川和彦，小宮崇他「大規模情報系システムにおける統合 ID 管理ソリューションの適用」三菱電機技報 86(7),399-403,2012

8) 釜坂 等，池田 健一郎，高橋 洋一「統合 ID 管理システム "iDcenter"の特長と適用事例 」三菱電機技報 85(2),127-130,2011

9) 清水さや子，岡部寿男，吉田次郎「一般カードを使った一時利用者向け認証システムの設計と実装」情報処理学会論文誌コンシューマ・デバイス&システム Vol.3,No.1,34–45,2013

10) Microsoft「Active Directory 技術情報」 http://technet.microsoft.com/ja-jp/windowsserver/bb466131.aspx

11) Japan Total System Co,Ltd「GROUP SESSION」 http://www.gs.sjts.co.jp/

12) Cybozu, Inc「cybouzu」http://cybozu.co.jp/

13) 岩沢和男，宮原俊行，中川敦，岩田則和，西村浩二，吉富健一「センターサービス利用登録システムの再構築」学術情報処理研究 No. 15, 149-152, 2011

14) 清水さや子，戸田勝善，吉田次郎「IC カード全学導入に向けた認証基盤システム整備と評価」学術情報処理研究 No.16,122-130,2012

15) OpenLdap http://www.openldap.org/

16) Dr Dobb's Journal The OpenLDAP Perl Backend http://www.drdobbs.com/the-openldap-perl-backend/199102060