任意のグループと統合 ID を使ったメンバの管理を行うグループ管理システムの実装

清水 さや子[†1†2]　戸田 勝善[†2]　岡部 寿男[†1]

大学のような組織は，人やシステムの管理が中央で一元的に管理されておらず，それぞれ分散して管理されていることが多い．本稿ではそのような組織を分散管理組織と呼ぶ．分散管理組織で提供される情報システムには，中央で提供するシステムの他に部局などで管理するシステムがあり，中央で一元管理されていない．このような組織において，中央に統合認証システムを導入する際，連携するシステム側ではアクセス制限のためにグループを使用する．しかし，部局などで管理する連携システムがグループを使用する際，中央の統合認証システムで管理するグループでは，不足する場合が多い．本研究では，部局などで管理する連携システムの管理者などが任意にグループを作成でき，メンバの管理を行えるグループ管理システムを提案する．グループ管理システムのメンバ管理は統合 ID と紐付けて行う．グループは事務担当者の存在の有無により公式グループと非公式グループに分け，それぞれ，メンバ登録や管理における工夫を行う．本研究では提案するグループ管理システムを実装し，試験運用を数ヶ月間行った結果を述べる．

Implementation of a Group-Membership Management System for Managing Arbitrary Groups and Membership Using Integrated ID

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

In most large and complex organizations like universities, the information systems and the members are managed not in centralized manner but separately by each department. In this paper, we refer to such an organization as a distributed management organization, where, aside from the systems managed by the central, the other systems are separately managed by the respective departments. In such organizations, access control to a coordinated system managed by a department is done based on groups when an integrated authentication system is introduced. However, in many cases, the number and the complexity of groups which can be provided and stored by the integrated authentication system is not sufficient for the requirements of the coordinated systems. In this research, we propose a new group management system, such that the administrator of the respective coordination system is able to create arbitrary groups optionally and manage the members using the groups. The administrators manage the members of the group management systems by relating them to the integrated ID codes provided by the integrated authentication system. Depending on whether the group contains the office staffs or not, the group is categorized into a formal group or an informal one, and the members are registered and managed in a suitable manner for each category. In this paper, we present the results of implementation of our proposed group management system and operation of it a few months.

1. はじめに

近年，大学などの組織では，一人につき一組のアカウント（以下，統合 ID とする）とパスワードを発行し，メールシステムやポータルシステムなど，様々な情報システムの利用時に統合 ID を使って認証する統合認証システムの導入が進んでいる[1][2]．これらは，LDAP などの認証サーバを用いることにより認証を行っている．

統合認証システムを導入している組織では，統合 ID を使って認証を行うシステム（以下，連携システムとする）が多く存在する．これらの連携システムで，利用者のアクセス制限を設定する際，認証システム上のグループなどの属性を使うことが望まれる．しかし，中央の認証システムでは，組織全体のユーザ情報を格納し，管理していることより，グループはそれぞれのユーザの主務の所属や身分などに対してのみ割当てられている場合が多い．それらのグループには，兼務者が含まれない場合や，詳細なグループが分けられていない場合が多い．

大学などの組織を含め，ユーザ情報やシステム情報を中央で一元管理せず，それぞれの部局などで分散的に管理している組織を，本研究では，分散管理組織と呼ぶ．分散管理組織の特徴として，組織内は複数の情報システムを提供しているが，それらのシステムは中央で一元管理されていない．中央で管理するシステムの他，部局などで分散的に管理するシステムがある．これらの分散管理組織においては，連携システムにおいても，中央で管理する連携システムの他，部局などの単位で管理する連携システムがある．本稿では，部局などが管理する連携システムのアクセス制限を行う際に，中央の認証システムのグループでは，情報が不足する場合の対応について述べる．複数の異なる連携システムにおいて，アクセス可能なメンバが同じ場合，それぞれの連携システムにユーザ登録し管理することは，連携システムの管理者に負担がかかる．このような場合，連

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

携システムごとにそれぞれユーザ登録を行わず，別途グループ登録を行い，メンバの管理が 1 箇所でできることが望まれる．

そこで，本研究では，連携システムのアクセス制限のためのグループが，中央の認証システムに格納されているグループでは不足する場合，新たに連携システムの管理者などが任意でグループを作成し，統合 ID と紐付けてメンバの追加や管理を行うことができる，グループ管理システムを提案する．任意でグループを作成する際，使われなくなったグループがいつまでも残る可能性や，メンバ情報が更新されない可能性などがあるが，本研究では，それらに対する対応策の検討を行う．また，メンバとして登録されるユーザの身分や主務の所属が変更になった際，中央で管理する認証システム上では，グループなどの属性が変更になるが，本研究ではそれに対する対応策の検討も行う．なお，提案するシステムは，既存の認証システムや連携システムの管理運用に関するコストを最小限に抑えるため，既存のシステムには極力手を加えず，新たに構築するものとする．

2 章では，分散管理組織と分散管理組織におけるシステムについて述べ，3 章では，グループ管理に関する関連技術と提案するシステムの要件について，4 章では，グループ管理システムの実装と，5 章では，実際にグループ管理システムを試験運用した評価について述べ，最後に，6 章ではまとめを述べる．

2. 分散管理組織と連携システム

2.1 分散管理組織

大学などの組織では，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ている．在籍する構成員は身分・所属などに応じて，組織の様々なシステムを利用する．しかし，構成員の管理は，学生は学生担当係，教員は人事担当係，研究員は研究担当係など，身分や所属ごとに分散して管理されていることが多い．また，様々な身分の一時利用者も在籍するが，身分や所属ごとに分散して管理されている場合が多い．そして，全構成員をとりまとめる部局がなく，全構成員の把握が非常に難しいことが多い．

提供する情報システムは，中央で提供するシステムの他に，学部や学科などが提供するシステムもあるが，全システムを中央で一元管理するのではなく，それぞれ部局ごとに管理していることが多いため，全システムの把握が難しい．このような，構成員やシステムに関する情報が分散的に管理されている組織を，本研究では分散管理組織と呼ぶ．

分散管理組織では，様々な部局などにおいて，研究チーム向けのシステムや，部局を超えた共同プロジェクト向けのシステムなど，さまざまな情報システムが運用されている．これらのシステムは，ユーザの身分・所属などにより利用できるサービスが異なる．そして，それぞれのシステムに対するアクセス制限は，それぞれシステムを管理する部局などで行っている[3]．

2.2 分散管理組織における統合認証システム

分散管理組織では，ユーザの身分・所属などにより管理部局が異なるため，統合 ID の発行や管理を行う際，以下３つのパターンでユーザ登録と統合 ID の発行・管理がなされていることが多い．

A) ユーザが個別に申請し，申請書を元にユーザ情報の登録（削除），統合 ID の発行（失効），管理する．

B) ユーザの身分・所属に対する管理係より，定期的に在籍者情報を受理し，ユーザ情報の登録（削除），統合 ID の発行（失効），管理する．

C) ユーザの身分・所属に対する管理係用の DB から自動で，もしくは管理係が，都度，在籍者情報を登録（削除）し，統合 ID の発行（失効），管理する．

A)の場合，ユーザの採用・退職の都度，中央の認証システム上で登録・管理の作業を必要とするため，管理者に非常に負荷がかかる．それだけでなく，中央では，ユーザの卒業・退職時に情報が把握できないため，籍が無くなってもいつまでも登録されている場合や，身分変更があっても初回に登録された情報のままである場合が多い．B）の場合は，中央の認証システム上では，都度ではないが定期的に，各管理係より受理し，登録・管理の作業が必要となるため，管理者に負荷がかかる．また，都度ではなく定期的であるということは，退職者情報などにタイムラグが生じ，退職後も一定の期間は登録されている場合もある．そのため，C)のように，それぞれの身分・所属に対する管理部局が，保持する DB や担当係から，利用者情報の登録および統合 ID の発行・管理が行われることが望まれるが，管理部局との連携が必要である．

C）については，各 DB や担当係が直接認証システムにメンバ登録するのではなく，統合 ID の管理用のシステムを構築し，そこで ID 管理や中央で管理する連携システムの利用権限などの管理を行うことが望ましい．この統合管理システムは，現在，東京海洋大学にて稼働中である（図 1）[4][5].

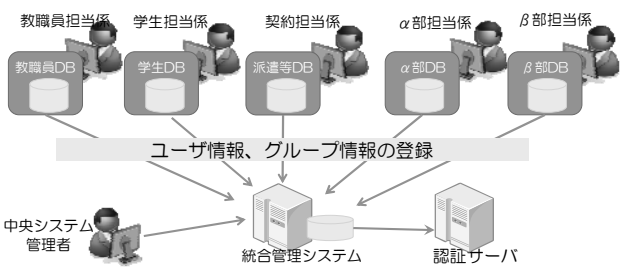

図 1　統合管理システムの構築

Figure 1　Construction of integrated management system.

2.3 分散管理組織における連携システム

組織内には，多くの連携システムが存在する．それぞれの連携システムに対するアクセス制限は，中央の認証システム上のグループなどの属性により設定する場合と，認証システム上のグループなどは用いず，連携システム側にそれぞれユーザ登録，管理を行い，アクセス制限を行う場合がある．

部局などが管理する連携システムでアクセス制限を設定する場合，中央の認証システム上に格納されているグループでは，足りないことが多い．中央の認証システム上のグループは，ユーザの主務の所属や身分に対してのみ割当てられている場合が多く，兼務者が含まれていない場合や，詳細な研究チームなどのグループには分けられていない．また，中央の認証システムでは，アクセスしてきた情報に対して，認証の照合をすることはできるが，部局などの管理する連携システムのアクセス制限を決定することはできない．詳細な取り決めを行えば，技術的にできなくはないが，中央の認証システム管理者に非常に負荷がかかるため，行わないことが多い．そのため，部局などが管理する連携システムのアクセス制限は，それぞれの連携システム側で行うことが多い．

3. グループ管理の要件と提案システムの検討

組織内には様々なグループが存在する．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．このように組織内には様々なグループが存在する．そして，１人につき１つのグループに所属しているのではなく，１人につき複数のグループに所属していることが多い．本章では，中央の認証システムで杏里する主務の所属グループ以外の兼業を含んだグループや詳細な区分のグループ管理方法について検討する．

3.1 関連技術と関連技術に対する本研究での提案

情報システム上におけるグループという概念は，グループウェアやファイルサーバなど様々なシステムで用いられている[6][7]．近年，流行している SNS などのサイトにおいても，自身の投稿に関するアクセス制限のためのグループ設定を行うことができる[8]．その際，グループやメンバの管理は，それぞれの管理者が行う．

また，統合認証システムの認証時に使用される LDAP や Active Directory などにおいても，ユーザ管理やグループ管理，グループポリシー作成などが可能である[9][10]．認証システム上のグループは，連携システムのアクセス制限のために利用することはできる．しかし，認証システムは組織の認証基盤となるシステムであるため，主務の所属や身分で分けられており，それらには兼務者が含まれていないことや，詳細なグループ分けがされていないことが多い．

3.2 部局管理の連携システムとグループ

例えば，管理部局が異なる A チーム用 Web システムと A チーム用掲示板システム，B チーム用 Web システムと B チーム用スケジュール管理システムがあるとする．これらのシステムのアクセス制限が与えられているユーザが，それぞれ同じメンバである場合でも，それぞれのシステム上にメンバを登録することになる．

その際，A チーム用 Web システムと A チーム用掲示板システムのアクセス制限は，工学部グループとしたい場合，中央の認証システム上に工学部グループがあれば使用することができる（図 2）．ただし，中央の認証システム上の工学部グループは，兼務者を含まないため，アクセス制限に兼務者も含めたい場合は，認証システム上の工学部グループを使用するだけでは不足する．

また，B チーム用 Web システムと B チーム用スケジュール管理システムのアクセス制限は，工学部と理学部の中の研究チームとする場合，中央の認証システム上にはそのようなグループがないため，中央の認証システムのグループは使用せず，B チーム用 Web システムと B チーム用スケジュール管理システムの上でそれぞれアクセスを許可するユーザ情報を登録，管理することになる．このように，中央の認証システム上のグループを部局などの連携システムのアクセス制限で使用するには，情報が不足することがよくある．

組織内に部局の連携システムが少なく，連携システムの増減がない場合は，中央の認証システム上で部局の連携システムのためのグループを設定することは可能であると考える．しかし，連携システムの数は，増減を辿りながら，運用年月と比例して増え続けていることや，2.2.2 のとおり，アクセス制限のためのグループを全て中央の認証システム側で管理するのは難しい．

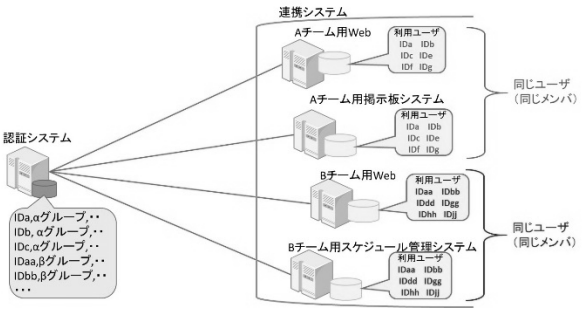

図 2　連携システムとアクセス制限の例

Figure 2　Examples of coordinated system and access control.

3.3 グループを管理するシステムの検討

本研究では，部局などが管理する複数の連携システムのアクセス制限が，同一メンバである場合，かつ，中央で管理する認証システム上のグループでは不足する場合におい

て，新しくグループとメンバを作成し，管理できるシステムを提案する．提案するシステムでは，部局などの連携システムの管理者が任意でグループを作成し，統合 ID と紐付けてメンバ追加や管理が行えることとする．

3.3.1 GakuNin mAP **の例**

統合認証システムを使った組織におけるグループを管理するシステムの類似システムの例を挙げる．近年，組織内だけではなく，大学間連携のための学術認証フェデレーション（学認：GakuNin）が展開されており[11][12][13][14]，その SP（Service Provider）のアクセス制限のためのグループ設定ができる GakuNin mAP がある．GakuNin mAP は，研究室・共同研究プロジェクトといった任意の仮想的なグループをグループの管理者が自由に作成・管理できる．作成されたグループの情報は他の学認参加サービスに対して提供され，グループ単位でのアクセス制限などきめ細やかなサービスを提供できる[15].

GakuNin mAP を使う際には，それぞれの組織ごとに構成員情報を流すためのサーバ，IdP（Identity Provider）の構築・運用管理が必要になる．また，連携システムは，それに準拠する SP である必要がある．本研究においては，極力，既存のシステムに手を加えず，中央のシステム管理者にも部局のシステム管理者にも，管理・運用における負担を増やさないこととする．そのため学認に対応していない組織やシステムに対して，新しく IdP や SP を構築することはせず，GakuNin mAP は使用しないこととする．ただし，GakuNin mAP の実現方式は 4 章で構築する際に参考とする．

3.4 公式グループと非公式グループ

連携システムで認証できるユーザは，中央の認証システムで登録されているユーザである．そのため，本研究で提案するグループのメンバは，グループのメンバは統合 ID と紐づける．紐づける際のユーザ登録・管理の方法を検討する．例えば，工学部などの学部に所属する兼務者やアルバイトなどを全て含めたグループを作成したい場合，グループの管理者は登録するメンバの数が多いため，個々の統合 ID を登録していくのは非常に負担である．そのため，中央の認証システムから，グループや身分などの属性によりソートし，必要なユーザを選択すればよいと考える．

ただし，全てのグループの管理者が中央の認証システムに登録されているユーザ情報が閲覧出来ると，プライバシーや個人情報などの問題につながる可能性がある．そこで本研究では，組織図などに基づき作成するグループで，メンバ管理を行える担当事務が存在する場合，公式なグループ（以下，公式グループと呼ぶ）として，担当事務に該当のグループ管理者権限を割り当てる．

しかし，学部事務などの正式な担当事務が存在する場合はよいが，研究チームなどが管理する連携システムでは，正式な担当事務が存在せず，教員や技術職員などがシステムの管理をしているような場合が多い．そのようなグループは，非公式なグループ（以下，非公式グループと呼ぶ）として，メンバを登録する際には，中央の認証システムに登録されているユーザ情報は閲覧できないようにし，メンバの統合 ID を直接入力し，認証システム上に登録済みの統合 ID か否かの照合を行い，登録済みの ID であれば登録すればよいと考える（表 1）（図 3）．

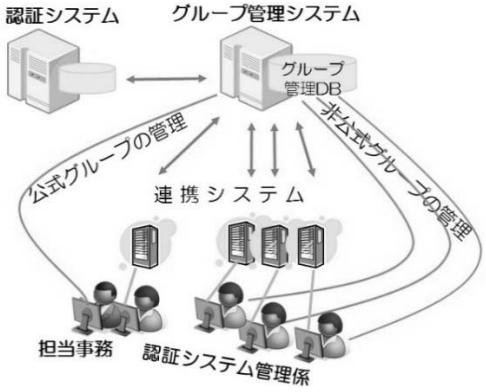

図 3　公式グループと非公式グループの管理

Figure 3　Management of the formal group and the informal one.

表 1　公式グループと非公式グループの比較

Table 1　Comparison of the formal group and the informal one.

	公式グループ	非公式グループ
グループ管理者	担当事務	教員や技術職員など
グループの例	兼務者などを含む工学部グループ，情報学専攻グループなど	認証研究チーム，数理計算研究チーム　など
メンバ登録方法	中央の認証システムから属性などによりソートし，該当メンバを選択する	メンバの統合 ID を直接入力／該当メンバにメールなどを送り統合 ID の登録してもらう
メリット	・ グループ管理者が不在になる可能性が低い ・ 階層などの構成と担当事務が確定すれば，先にグループ作成，管理者割当てすることができる ・ 下位階層から上位階層にメンバ情報引継可能	統合 ID 保持者であれば，誰でもグループの管理者になれる
デメリット	メンバ登録の際に個人情報を含むため，グループ管理者は担当事務に限定	① メンバ登録時に統合 ID が不明な場合がある ② 一旦作成されたグループは，不要になってもいつまでも残る可能性あり ③ グループの管理者がいつの間にか不在になる可能性があり

以下，公式グループと非公式グループのグループ作成方法やメンバ登録・管理方法について，それぞれ検討する．

3.4.1 公式グループ

公式グループは，担当事務が必要に応じて，メンバを登録し管理する．担当事務がグループ管理者となりメンバを

管理することにより，グループの管理者が不在になる可能性が低くなる．また，メンバの異動などに応じて，更新されることが期待される．

公式グループは，組織図などを元にして作成する場合，階層などの構成と担当事務が決まれば，先にグループおよびグループ管理者を割り当てておいてもよいと考える．また，組織図は学部や学科などに対して階層化されていることより，それらに対するグループも階層化し，下位階層から上位階層にグループのメンバ情報を引き継ぐことも可能である．

3.4.2 非公式グループ

非公式グループは，部局や部局をまたいだ研究チームなどが管理する連携システムの管理者がメンバを登録し管理する．

公式グループは担当事務が存在することに対して，非公式グループは担当事務が存在しない．そのため，グループ管理者は，教員や技術職員などがグループの管理者となるが，メンバの登録や管理方法について，以下が懸念される．

① メンバ登録時に統合 ID が不明な時がある可能性がある．
② 一旦作成されたグループは，不要になってもいつまでも削除されず残る可能性がある．
③ グループの管理者がいつの間にか不在になり，グループの削除やメンバ変更できなくなる可能性がある．

これらの懸念事項の対応策を検討する．①については，それぞれのメンバから統合 ID の情報を受理するか，メンバに対してメールを送信し，個々に統合 ID を登録すればよいと考える．②については，ある程度の期間（例えば 1 年に一度など）において更新手続きを行い，更新手続きを行わないグループは削除すればよいと考える．③については，グループの管理者を複数設定できれば，グループの管理者が不在になった場合でも，別の管理者が即時に対応することができると考える．

3.5 メンバの身分や主の所属が変更する場合の検討

ユーザの身分や主の所属に変更が生じる際，中央で管理する認証システム上では，グループや属性情報が変更される．それに伴い，本研究で提案するグループ管理システムにおいても，認証システム内に登録されているユーザ情報と連携していることより，登録されているグループおよびメンバに対する対応の検討が必要になる．

例えば，理学部が主の所属である研究員の B さんが，同じ組織内の工学部の准教授になる場合，中央で管理する認証システム上では，所属グループは理学部から工学部へ，身分属性が非常勤職員から教員へ，などの変更が生じる．その際，グループ管理システム上のグループのメンバに B さんが含まれている場合，グループ管理システムの公式グループの場合と非公式グループの場合に分けて考える．

公式グループは，中央の認証システムで管理するグループより詳細なグループであり，かつ兼担者を含んだグループである．B さんが理学部物理学科グループに所属している場合，主の所属グループが変更になるが，理学部物理学科の委員などを兼務することもある．しかし，兼務などの情報は，中央の認証システムでは格納しないことが多く，中央の認証システムでは，B さんが理学部の委員であるということの管理を行わないことが多い．B さんを理学部物理学科用のメンバとして継続するか削除するかは，グループの管理者でないと判断が難しい．よって，B さんの主の所属グループが変更になった際，グループの管理者に通知し，グループ管理者が継続もしくは削除の手続きを行えばよいと考える．

非公式グループにおいては，メンバの登録時に，認証システムに格納されている所属グループなどの情報を使わない．ID を登録後，認証システム上に登録した ID が格納されているか確認を行うのみとするため，所属や身分の変更時には，何も行わなくてよいと考える．

グループ管理システムにおけるメンバの管理は，統合 ID をベースとしている．そのため，学籍番号に沿って作成された ID で，卒業後には使われなくなるような ID を持つ学生が教職員になる場合，身分の変更と同時に ID が変更になるため，該当グループのメンバ管理として，新たに ID 情報の登録が必要となる．

4. グループ管理システムの実装

前章で述べたグループ管理に関する要件を基に，グループ管理システムを実装する．まずは実装方式を検討し，実装したグループ管理システムの構成とグループの作成からメンバの追加・管理方法などについて述べる．

4.1 実装方式の検討

グループ管理システムの実現には，さまざまな実装方式があるが，既存システムに手を加えず，新たにシステムを構築するために，実現可能性を含めて，LDAP の Proxy 方式と GakuNin mAP のような方式の２つの方式で検討を行う．

通常，連携システムから認証サーバへ，ID とパスワード，グループなどの属性を問合せる．LDAP の Proxy 方式で実現する場合は，連携システムから認証サーバに直接問合せず，グループ管理システムを経由し，間接的に認証サーバに問合せる．グループ管理システムで，アクセス制限の照合を行ったあと，認証サーバに該当 ID とパスワードの認証を行う（図 4）．

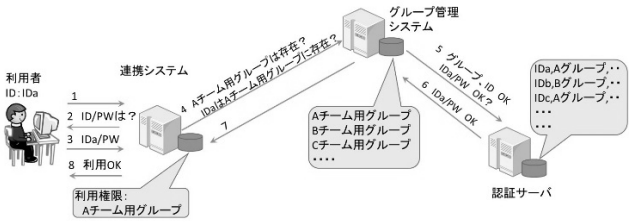

図 4　LDAP Proxy 方式による実現

Figure 4　The realization by the LDAP Proxy method.

学認 mAP のような方式で実現した場合，まずは通常と同じく，連携システムから認証サーバへ ID とパスワードの認証を行う．認証に成功すれば，グループ管理システムにアクセスを許可するグループに該当 ID が所属しているか確認を行う（図 5）.

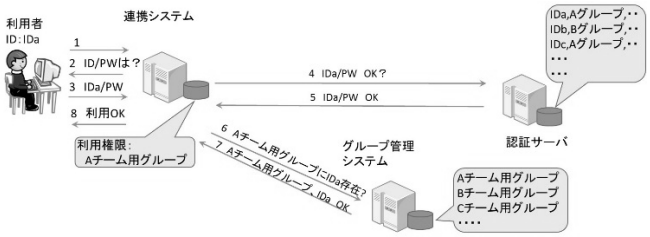

図 5　GakuNin mAP のような方式で実現

Figure 5　The realization in such a manner as GakuNin mAP.

LDAP Proxy 方式では，連携システム側では，認証時の問合わせ先を LDAP Proxy に変更するだけでよいが，GakuNin mAP のような方式では，認証サーバに問合わせた後，グループ管理システムに問合わせるため，2 段階の問合わせが必要になる．本研究においては，既存システムに極力影響をなくするため，連携システムの管理運用の負担が少ない LDAP Proxy 方式にて実現することとする．

4.2 グループ管理システムの構成

グループ管理システムは，OpenLDAP を用いて LDAP サーバのプロキシサーバ（以下，LDAP Proxy とする）を構築し，実現する[16]．LDAP Proxy では，メンバの登録を行う際，統合 ID と紐付けるため，既存の LDAP サーバなどの認証サーバと連携する（図 6）．また，グループの管理者がグループの作成やメンバの追加を Web 上で行えるよう，Apache を用いている．

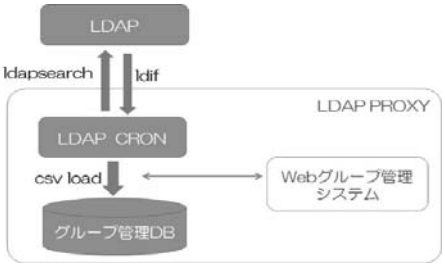

図 6　グループ管理システムの構成

Figure 6　The composition of the Group management system.

4.3 グループ作成とメンバ登録

公式グループは，必要に応じて，それぞれのグループに担当事務を割当て，メンバの登録・管理を行う．非公式グループは，連携システムの管理者などが必要に応じて作成する．しかし，試験運用段階では，グループの作成はグループの管理者による申請制にし，グループ作成は中央のグループ管理システムの管理者が行う．グループ作成後，グループの管理者がメンバの登録・管理，管理者の追加などを Web 上で行う．

Web 上からグループ管理システムにログインする際，統合 ID とパスワードでログインする．グループ作成後は，メンバを登録するが，操作するグループを公式グループか非公式グループから選択すれば（図 7），自身が管理者となっているグループが表示される．

将来的には，管理運用上の負担軽減のため，統合 ID が発行されているユーザであれば，自身の ID とパスワードでグループ管理システムにログインでき，グループの作成，メンバの登録・管理が行えることが望ましいと考えている．

図 7　ログインとメンバ登録の方法

Figure 7　Method of login and member registration.

公式グループと非公式グループのメンバ追加方法が異なるため，以下に分けて説明する．

4.3.1 公式グループの作成とメンバ情報の登録

公式グループのメンバ追加の際には，認証システム上に登録されている全ユーザの統合 ID や氏名，主のグループなどの属性情報が表示される．その際，グループなどの属性でソートしたり，絞込み条件とする文字列入力が可能である．その後，メンバ追加したいユーザを選択し，登録を行う（図 8）.

図 8　公式グループのメンバ登録

Figure 8　Member registration of the formal group.

4.3.2 非公式グループの作成とメンバ情報の登録

非公式グループはあらかじめ作成されていないため，必要に応じて作成する．連携システムの管理者などが非公式グループを作成したい場合，代表の管理者が，表 2 の内容を申請する．中央のグループ管理システムの管理者は，申請内容を元にグループを作成し，グループの管理者を割り当てる．

表 2　非公式グループ作成に必要なデータ

Table 2　Necessary data to create an informal group.

グループ ID（英語名）	例）sec_team
グループ ID（日本語名）	例）セキュリティ研究チーム
グループ管理者所属	例）工学部
グループ管理者氏名	例）工学　太郎
グループ管理者メールアドレス	例）taro@*********

非公式グループのメンバ追加の際には，全ユーザの一覧は表示しないため，それぞれ，個別に統合 ID を登録する．メンバ追加時に，入力した統合 ID が存在するか文字列確認し，存在する場合にのみ登録可能となる．試験運用段階では，認識違いなどにより誤った統合 ID の登録を避けるため，メンバの追加時に存在するユーザの場合，そのユーザの名前などの属性を表示し，確認を行い，間違いがなければ，登録を行うようにしている．

4.4 管理者の追加・削除

自分が管理者として登録されているグループに対して，新たな管理者の登録および既存管理者の削除を行うことができる．管理者の登録や削除が必要な場合，該当グループを選択し，［管理者追加・変更］項目を選択すると，登録されている管理者の一覧が表示される. 管理者の追加登録は，非公式グループのメンバ追加時と同じく，管理者として追加したいユーザの統合 ID を入力し，入力した統合 ID の存在確認を行う．管理者を削除する際，一覧から削除したい統合 ID を選択し，削除処理を行う（図 9）．削除処理を行う際，結果として正規教職員が一人もいなくなる場合は削除できない．

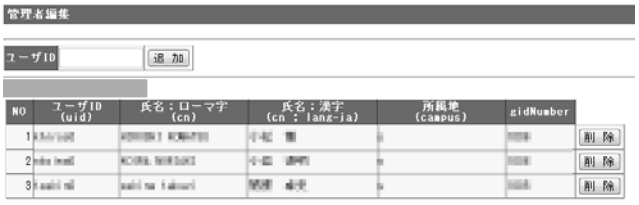

図 9 グループ管理者の追加と削除

Figure 9　Add or Remove group administrator.

4.5 連携システムとの連携

本研究では，既存システムに手を加えず，新しくグループ管理システムを構築し，グループ管理システム内に公式グループや非公式グループを格納する．そのため，部局などで管理する連携システムからの認証認可時には，直接 LDAP などの認証サーバに問合せるのではなく，グループ管理システムを経由することになる．

連携システム側における設定は，Apache の httpd.conf や .htaccess で設定する場合，認証情報の問合せ先（AuthLDAPURL）を，グループ管理システムの URL および，該当のグループ ID を指定する．

例）AuthLDAPURL ldap://*グループ管理システムのアドレス*/dc=****, dc=local?uid?sub?(ou=*グループ ID*)

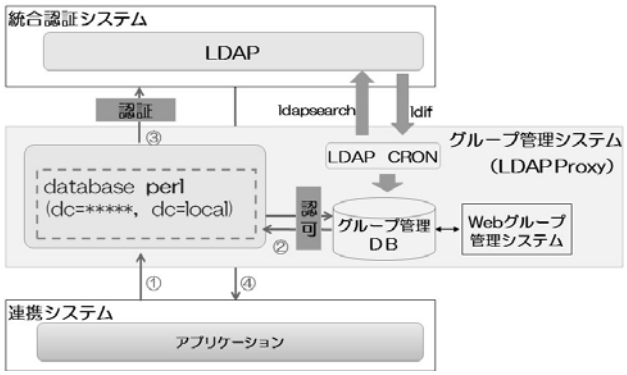

図 10　認証認可の流れ

Figure 10　Flow of Authentication and Authorization.

ユーザが連携システムを使用する際，統合 ID とパスワード認証を行う．その際，まず，連携システムからグループ管理システムに問合せを行い，指定のグループ ID およびメンバの存在確認の照合を行い，照合に成功すれば，該当の統合 ID とパスワードを LDAP に問合せる．問合せに成功すれば，連携システムが利用可能となる（図 10）．

5. グループ管理システムの運用評価

本研究で提案するグループ管理システムは，LDAP Proxy 方式を用いて実現したことにより，既存システムには，ほとんど手を加えることはなく実現できた．また，部局などが管理する連携システムが，直接中央の認証サーバに問い合わせるより，LDAP Proxy を経由することで，セキュリティの強化につながる．

提案するグループ管理システムは，現在，東京海洋大学にて，試験運用中である．グループ管理システム上で運用されているグループは約 10 グループ存在するが，現時点で連携システムから認証時に使用しているグループは 4 グループある．1 つのグループ内に含まれるメンバ数は 5～30 となっており，グループの用途によってメンバ数が異なる．公式グループは 1 件である．現在， 4 つの連携システムから，それぞれ別のグループに対して認証認可を行っている．

連携システムの用途は，Web ページの閲覧権限を対象グループのみとする場合，Web アプリケーションの利用権限を対象グループのみとする場合などである．

公式グループの管理者は，連携システムの管理者とは別の該当の担当事務が公式グループの管理者となっている．非公式グループは，連携システムの管理者が非公式グループの管理者となり，メンバの追加や管理者の追加を行っている．現在は，グループの命名規則をつけておらず，並列であるが，グループが増えると命名規則や階層をつける必要があると考える．

また，現状は特定の期間のみ作成が必要なグループに対して，グループ作成時に期限を設定していない．年度末にグループの管理さに継続の有無を確認する設定であるが，期限を設定すれば，年度内に不要になったグループが残ることを防ぐことができると考える．

本システムの試験運用を開始し，半年に満たないが，その間に大きな問題は発生していない．グループの管理者は複数の管理者を設定できるため，自身以外に非常勤職員や学生などを管理者に充てることにより，より正確なメンバ情報の更新が行われることが期待されているようである．

公式グループの場合，グループの管理者が事務系の職員であり，事務系職員は数年に 1 度は異動があることが多く，異動時に上手く引き継ぎが行えるよう，運用でカバーする必要があると考える．

6. まとめ

本研究では，部局などで管理する連携システムにおいてアクセス制限をするためのグループが，認証システムで格納されているグループ情報では不十分な場合，任意のグループを設定し，メンバ管理を行えるようグループ管理システムを提案し試験運用を行った．

認証システムで格納されているグループ情報は，主務の所属などによるグループが割り当てられているため，兼務者などが含まれていないことが多い．また，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が，中央では，それぞれのユーザに対して詳細なグループの割当てを行うことは難しい．

そのため，部局などで管理する連携システムのアクセス制限として認証システムのグループを使用する際，メンバ情報などが不足している場合がある．本研究では，そのような場合に，部局などの連携システムの管理者などが新しくグループを作成し，それぞれのグループの管理者がメンバ管理し，また，メンバは統合 ID と紐付けて管理するグループ管理システムを提案した．本研究で提案するグループ管理システムに作成できるグループは公式グループと非公式グループである．公式グループは，学部や学科などの組織図などに基づくグループとし，担当事務が存在し，正しくメンバ管理がなされることを期待するグループである．非公式グループは，研究チームなどの比較的小規模で使用するグループであることより，担当事務が存在しないグループである．本研究では，公式グループと非公式グループに対してそれぞれ，グループやメンバ管理における工夫を行った．

本研究で提案するグループ管理システムは，連携システムのアクセス制限のためのグループおよびメンバの管理を想定したシステムであった．しかし，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ことや，グループ内でのメールを共有するなど，さまざまな用途に応用できることが期待できると考える．

謝辞 本研究で提案するグループ管理システムの構築および試験稼働するにあたり，ご協力頂いた東京海洋大学の諸氏に深謝する．

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) 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
4) 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,p131-137，2012
5) 清水さや子，戸田勝善，岡部寿男「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」情報処理学会シンポジウムシリーズ，マルチメディア,分散,協調とモバイル (DICOMO2013)シンポジウム論文集, 1976-1983,2013
6) Google Apps ： http://www.google.com/intx/ja/enterprise/apps/education/
7) Cybozu：http://cybozu.co.jp/Facebook：https://ja-jp.facebook.com/
8) Facebook：https://www.facebook.com/
9) Open LDAP：http://www.openldap.org/
10) Microsoft, Server and Cloud Platform, Active Directory： http://www.microsoft.com/ja-jp/server-cloud/windows-server/active-directory.aspx
11) 学術認証フェデレーション http://www.gakunin.jp/ja/
12) 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
13) 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
14) 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
15) 西村健, 松平拓也「GakuNin mAP (group attribute provider) BoF」Japan Identity & Cloud Summit（学認シンポジウム）,2013
16) The LDAP Proxy Project：http://ldap-proxy.sourceforge.net/