Vol.2018-GN-103 No.29
Vol.2018-CDS-21 No.29
Vol.2018-DCC-18 No.29
2018/1/27

統合 ID に基づく効率的な権限移譲が可能なグループ管理システム

清水さや子[†1†2]　戸田勝善[†2]　横田賢史[†2]　岡部寿男[†1]

概要：本研究では，統合認証基盤と連携した「グループ」機能を用いて，認可情報を統合的に管理する際，グループの管理権限をシステム管理者からグループ管理者へ効率的に移譲する仕組みを提案する．これまでのグループ管理の仕組みでは，グループの柔軟性が低くグループの管理を行う人や管理できる範囲が限定されていた．また，グループ管理者が不在となった場合のグループの継続性の管理も課題となっていた．本論文では，これらの課題が管理者間の権限移譲を効率的に行えるようにすることで解決できることを示し，それによりシステム管理者およびグループ管理者の管理の負担を軽減する仕組みを提案する．提案する仕組みでは，一般ユーザが自由にグループを作成し管理することを許す．本論文では，このようなグループを「一般グループ」と呼ぶ．一方，業務などで使用するため継続性が求められるグループは「公式グループ」として区別して扱い，グループ管理者の交代が自動的に行えるよう，グループ管理者を属性などで指定することを許す．これら二種類のグループを使い分け，システム管理者からグループ管理者，そしてグループ管理者から新グループ管理者へ，円滑にグループ管理の権限移譲を行う．提案方式に基づくグループ管理システムを LDAP proxy として実装し，Web サーバなどと連携しつつ，試行的に運用を行った．

キーワード：統合認証基盤，認可，属性，グループ管理，権限移譲

A Group Management System for Efficient Authority Transfer Based on Integrated ID and Attributes

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

Abstract: In this research, we propose a mechanism to transfer group management authority efficiently from the system administrator to group administrators using a group management feature organized on an integrated authentication infrastructure, so that authorization, as well as authentication, is managed integrally on the authentication infrastructure. In previous group management mechanisms, the group flexibility is low, and people who manage the group and the range that they can manage groups were limited. It has also been a problem how to manage continuity of a group when the group administrator becomes absent. In this paper, we clarify that these challenges can be solved by efficient authority transfer between administrators, and thereby propose a mechanism which lightens the burden of system administrators and group administrators. In the proposed mechanism, it is allowed for an ordinary user to create arbitrary groups and to manage them. In this paper, we call such a group *a general group*. On the other hand, we give distinguished treatment to groups that require continuity in business and call such a group as *an official group*. Administrators of an official group may be specified by attributes, so that the group administrators can be replaced automatically. By using these two types of groups selectively, it become possible to carry out authority transfer in group management smoothly, from the system administrator to a group administrator, and from a group administrator to another new group administrator. We have implemented a group management system based on the proposed scheme as an LDAP proxy, and we have been operating it experimentally in cooperation with web servers and others.

Keywords: Integrated Authentication Infrastructure, Authorization, Attributes, Group Management, Authority Transfer

1. はじめに

情報ネットワーク技術の発展により，業務や教育・研究などにおける様々な仕組みがオンライン化され，大学などの組織では情報システムは必要不可欠なものになっている 1)．そして，各システムで個別に発行されていた ID が組織において統合化され，統合認証基盤として整備が進んでいる．

統合認証基盤に関しては，認証情報の統合化や管理の効率化に向けた研究が多くなされている 2）3)．また，それらの技術を用いた組織間認証連携に対する研究も進められている 4）5)．しかし，認証と連動してアクセス制限などを行ういわゆる認可の統合化については，依然として十分な普及に至っておらず，認証情報が中央の認証用のサーバ（以下，認証サーバとよぶ）で一元管理されるようになっていても，認可のために必要な情報はサービスごとにばらばらに管理されるのが一般的である 6）7)．認可情報としては，サービスごとにアクセスを許可するユーザリストとして保持するか，認証サーバに格納されている属性の値に基づくか，あるいはこれらを組み合わせて指定し，それらに対してアクセス権限を設定するのが一般的である．しかし，中央の認証サーバに格納されているユーザの属性は，組織において共通に定義されているものであり，認証サーバの属性を指定するだけでは，各サービスが求める詳細なアクセス制限を行うことが難しい．また，各サービスの認

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

Vol.2018-GN-103 No.29
Vol.2018-CDS-21 No.29
Vol.2018-DCC-18 No.29
2018/1/27

可で使用するユーザの集合（以下，認可ユーザとよぶ）はサービス間で共通ないし重複する場合も多く，サービスごとに管理するのでは非常に効率が悪い．そのため，認可情報についても中央で統合的に管理できる仕組みが求められている．

本論文では，統合認証基盤と連携したグループ機能を用いて，統合的に認可ユーザを管理する仕組みについて論ずる．著者らは，本研究の初期段階としてグループを効率的に管理できるようグループの体系化を行った 8）9）10）11）．本論文においては，体系化したグループを実運用と合わせて，効率的に管理する仕組みについて述べる．グループ管理の仕組みについては古くから検討されているが 12）13），最近のものとしては，統合認証基盤と連携した分散管理の環境のために設計された米国の Grouper などが代表的である 14）15）．しかし，Grouper などの仕組みでは，グループの管理を柔軟かつ詳細にするほど，その管理システム全体の管理を行う人（以下，システム管理者とよぶ）や各グループの管理を行う人（以下，グループ管理者とよぶ）の負担が大きくなる．本論文では，統合認証基盤と連携したグループ管理の仕組みにおいて，既に開発されている Grouper などのシステムを実運用と照らし合わせ，グループに対する柔軟性やグループの継続性などの課題がシステム管理者からグループ管理者への権限移譲にあることを明確にした上で，それを解決しつつ，システム管理者およびグループ管理者の管理の負担を軽減する仕組みを提案する．

グループ管理の権限をシステム管理者からグループ管理者に移譲する際，プライバシーや個人情報保護などの要請により，属性などの取り扱いは，厳密な管理が必要となる 16）17）．そのため，通常はグループ管理者ごとに，参照できるユーザやユーザ属性の範囲の設定が必要となる．たとえば Grouper においては，グループ管理者に設定されたユーザやユーザ属性などの情報を参照する権限（以下，参照権限とよぶ）の範囲内でのみグループのメンバ管理が行えるという制約を課している 14）15）．そのため，グループを定義する際にはそのメンバの範囲とグループ管理者の選任に制約があり，特に組織横断型のグループのグループ管理者になれる人は非常に限定されてしまう．また，グループ管理者ごとの参照権限の設定は，グループ管理者が交代する度に操作が必要となり，システム管理者に対する負担が大きい．

それに対し本研究で提案する仕組みは，グループ管理の権限を一般ユーザにも拡張し，参照権限にとらわれない柔軟なグループが作成できるものとする．そのために，グループ管理者に対しては都度参照権限を設定するのではなく，あらかじめユーザ属性ごとにグループ管理者の参照権限を条件式として設定しておく．そして，参照権限の範囲を越えたユーザをメンバにするには，直接入力や条件式から導いたメンバを閲覧不可にすることで安全性を確保する．これにより，グループに対する柔軟性が増し，システム管理者の管理の負担も軽減される．

一方，これまでのグループ管理の仕組みでは，グループが組織において公式のものかどうかやその重要度に関わらず，グループ管理者が転出等で不在になった際にグループが自動的に削除され，継続が必要な場合はシステム管理者が個別対応を行う必要がある点で，システム管理者の管理の負担が高かった．

本研究では，グループの重要度に合わせ，業務などで継続性の確保が必要なグループを「公式グループ」，通常のグループを「一般グループ」と区別する．公式グループでは，グループ管理者が不在とならないように，システム管理者がグループ管理者の管理を行う．システム管理者の負担を下げるよう，グループ管理者は属性から導くことができる仕組みとする．

本論文で提案する仕組みを取り入れることで，システム管理者からグループ管理者へ，グループ管理者から新グループ管理者への効率的な権限移譲が期待できる．なお，本研究で提案するグループ管理システムは，概念に沿って LDAP Proxy として実装し，東京海洋大学にて複数の Web サービスと連携しつつ，試行的に約 3 年間運用を行った．

2 章では関連技術として，統合認証基盤とグループ管理について述べ，3 章では提案する仕組みと 4 章では実装について述べる．最後に，5 章でまとめを述べる．

2. 関連技術

本研究では，アカウントや情報サービスが中央で一元管理されておらず，各部局などで分散的に管理されている大学のような組織（以下，分散管理組織とよぶ）で，かつ，統合認証基盤が整備されている組織を前提とする．

2.1 グループを用いた統合的なユーザ情報の管理

分散管理組織において，各サービスの認可ユーザの情報を統合的に管理するために，統合認証基盤と連携し，アクセス可能なユーザの集合を「グループ」として管理する仕組みが存在する．大学間連携の学術認証フェデレーション（GakuNin）においては，グループを属性として提供するための仕組みが提案されている 18）．

「グループ」を用いる場合，各サービス側では，アクセスを許可するグループとそれに対するアクセス範囲の指定を行う．複数のサービスで認可情報が重複する場合，該当するグループを指定すればよく，サービスごとに認可情報を詳細に管理することは不要となる．

2.1.1 グループを用いた仕組みの例

統合認証基盤と連携し，中央でグループ管理を行う仕組みの例としては，米国 INTERNET2 のプロジェクトで大学

Vol.2018-GN-103 No.29
Vol.2018-CDS-21 No.29
Vol.2018-DCC-18 No.29
2018/1/27

などの分散管理の環境のために設計された中央アクセス管理システムである Grouper14）15），Exgen Networks 社の統合ディレクトリ管理を行うソフトである LDAP Manager 19）のオプション機能にあるグループ管理機能，国立情報学研究所で研究開発されている GakuNin に参加する組織において，所属組織を越えたメンバをグループとして管理できる GakuNin mAP 20）21）などがある．

グループ管理者やメンバとして登録されているユーザが，退職などにより統合認証基盤からユーザ情報が削除されれば，グループ管理者やメンバからも削除される．そのため，グループ管理者やメンバがいつの間にかゼロになる場合がある．そして，グループ管理者の全員が不在になった場合，通常は，グループは自動的に削除される仕組みとされている．ただし，グループ管理者が不在となり管理されなくなったグループを直ちに削除せず，年に 1 回程度不要グループを削除するなどの運用をしている場合もある．なお，Grouper では，グループ管理者は複数名登録可能であり，追加や変更時は列挙型により操作する．

2.1.2 グループを用いた著者らの先行研究

グループは，グループごとに用途や作成時期，消滅時期，メンバの管理方法などが異なることや，1 人が複数のグループに所属するなど管理が複雑である．そこで，本研究の初期段階として著者らは，グループを「ユーザの集合とそれを管理する人（グループ管理者）の集合の組」とし，複雑なグループを効率よく管理できるようグループの体系化を行った 8）9）10）11）．そこでは，グループに対する管理の権限をグループごとの管理者に移譲することが必要であること，また，権限が移譲されたグループ管理者の管理の負担を軽減できるよう，グループには，ユーザを列挙するだけでなく，ユーザ属性や既存のグループからも導けることが必要であることを述べてきた．また，グループ作成時に必要とするメンバ登録方法を表 1 のように定義した．

表 1　グループ作成時に必要とされるメンバ登録方法
Table 1　Registration methods of members required when creating a group.

列挙型	メンバのリストを列挙する
属性型	属性（数値や文字列等）に関する条件式（=，＜，＞等）とそれらを組み合せる論理演算（and，or，not 等）から導く
複合型	すでに作成されているグループを集合演算により組み合せる

2.2 既存のグループ管理の仕組みと課題

本研究では，既存のグループ管理の仕組みと実運用と照らし合せた際に，比較的大きな課題となる以下の 2 点の課題について取り上げる．

一つは，グループの柔軟性が低いことである．既存のグループ管理の仕組みでは，グループ管理の権限をシステム管理者からグループ管理者に移譲する際に，グループ管理者ごとに設定された参照権限の範囲内でメンバ登録を行うため，作成されたグループは非常に限定的なものになる．また，システム管理者は，グループ管理者の新規登録時や交替時，参照権限が変更になる度に対応が必要であり，グループが増えるほど負担が増える．

もう一つは，グループの公式性や重要性に関わらず継続性が確保されていないことである．グループ管理者が不在になり管理されなくなったグループを残すと，リソースの無駄であるだけでなく誤用や悪用によるセキュリティインシデントにつながる懸念もあるため，通常はグループ管理者が不在になったグループは速やかに削除される．しかし，実際に業務などで使用するグループに対してグループ管理者が不在になったことにより直ちに削除されると，業務に大きく支障をきたす場合も多々ある．そのような場合，システム管理者に新たにグループ管理者を設定するような個別対応が求められる．このような運用では，グループ数が増えるほど，システム管理者の負担が増える．

3. 効率的な権限移譲が可能なグループ管理システムの提案

本章では，2.2 節で提起した既存のグループ管理の仕組みの課題を解決することで，システム管理者からグループ管理者，グループ管理者から次のグループ管理者へスムーズに権限移譲を行うための仕組みを提案する．また，システム管理者やグループ管理者の管理の負担を削減し，コストを抑えつつ実用的かつ安全な仕組みとすることを設計の目標とする．なお，提案する仕組みでは，Grouper などで実装されている一般的な機能に対しては同機能として取り入れるが，本論文で詳細を述べることは省略する．

3.1 前提条件と要件

本研究で提案する仕組みは，以下のような組織で利用することを前提とする．

- 分散管理組織で統合認証基盤が整備されている
- 中央の認証サーバには，構成員の統合 ID や共通に定義される属性が格納されている
- 中央の認証サーバのユーザ情報は，ユーザごとの管理部局や別に管理されるサーバなどと連携を行い，日々最新の情報に更新されている

グループ管理機能に対する基本的要件は以下とする．

- グループごとにグループ管理者を立て分散的に管理できること

Vol.2018-GN-103 No.29
Vol.2018-CDS-21 No.29
Vol.2018-DCC-18 No.29
2018/1/27

- 統合認証基盤と連携することより，グループ管理者やメンバの指定に，統合 ID や属性を使用できること
- 列挙型，属性型，複合型によりメンバ登録できること

3.2 既存のグループ管理の仕組みの課題に対する提案

課題解決のために次の二つの提案を行う．一つは，グループの柔軟性の向上のために，グループ管理者になれる権限を一般ユーザにも拡張し，参照権限を確保しつつ参照権限の範囲外のユーザもメンバにできるようにすることである．もう一つは，グループの必要に応じて継続性を確保するため，業務などで使用するグループで継続性が必要とされるグループを「公式グループ」と定義し，システム管理者がグループ管理者の管理を行う．グループ管理者の交替がスムーズに行えるよう，グループ管理者を属性でも指定可能とする．以下にそれぞれの詳細について述べる．

3.2.1 グループの柔軟性の向上

2.2 節で述べたように，これまではシステム管理者がグループ管理者を登録しグループ管理者ごとに設定された参照権限の範囲内でしかグループのメンバ登録ができなかったのに対し，グループ管理の権限を特定のユーザだけではなく一般のユーザにも移譲することでグループの柔軟性を拡張する．その際にグループ管理者は与えられた参照権限を保持しつつ，参照権限にとらわれない柔軟なメンバ構成のグループが作成できる仕組みを提案する．グループ管理者は，与えられた参照権限を越えたユーザもメンバとして登録可能とする．具体的には，個々にユーザを登録する，もしくは，属性に対する条件式によりメンバを導く．

ただし，近年，個人情報保護などの要請により，ユーザ担当掛などである場合を除き，一般ユーザは，同組織内であっても所属や身分が異なる人の在籍情報を知ることができない場合が多くなっている．属性型のグループのメンバかどうかが判ればそのユーザの属性値が判ってしまうことから，原則，グループ管理者は，条件式から導かれたグループのメンバリストに加え，メンバ数も閲覧不可とする．メンバリストの閲覧ができない場合，属性情報が想定するものと異なることや条件式の誤りなどにより，グループ管理者の意図しないメンバ構成になることが考えられる．しかし，Web サービスのアクセス制限においては，認証サーバに格納されているユーザの属性を直接指定して認可の判断を行う場合，認可の条件に該当するユーザのリストを直接閲覧することはできない．これと同様に，本研究におけるグループにおいても，Web サービスのアクセス制限などでの利用を前提とすることより，原則，作成したグループのユーザリストはグループ管理者が閲覧できなくてもよいこととする．なお，意図しないメンバがアクセスすることを許さない取扱注意の重要情報サイトなどへのアクセス制限にグループを使用する場合は，グループを 3.2.2 節で記す公式グループとして作成することにより，ユーザリストの閲覧を可能とする．

システム管理者はあらかじめ，ユーザごとに割当てられた身分や所属などの共通の属性に対して，条件式を設定し参照権限の設定を行っておく．これにより，新規ユーザの追加時やユーザの所属や身分などの属性値の変更時に，都度グループ管理者の参照権限の設定変更を行うことの負担が軽減される．なお，条件式は，運用方針の変更時や組織改編などにより属性や属性値の構成変更時には変更が発生するが，日常的に変更されることを想定しないものとする．

また，分散管理組織では，教職員と学生，外部組織に所属する研究者など様々な身分により構成されるため，一般ユーザとなる構成員全員にグループ管理者になれる権限を与えると責任問題に発展する可能性が高まることより，グループ管理者になれる権限を常勤教職員のみに限定するなど，システム管理者があらかじめ認証サーバで共通に定義される属性を用いて制限を行う．

3.2.2 グループの必要性に応じた継続性の確保

これまでのグループ管理の仕組みでは，グループが公式なものであるか，重要なものであるかなどを区別せずに管理されてきたのに対し，本研究では，グループの重要度に合わせて，業務などで継続が必要なグループを「公式グループ」として定義づける．それに対して，3.2.1 節で述べた一般ユーザが自由に作成できるグループを「一般グループ」として，区別して扱う．

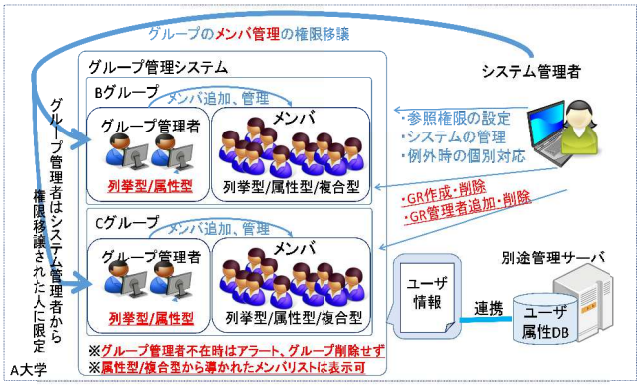

図 1　公式グループの概要

Figure 1　Overview of official groups.

公式グループでは，グループ管理者が不在になってもグループが継続できるよう，システム管理者がグループおよびグループ管理者の管理を行う．グループ管理者は，システム管理者から権限移譲された人に限定し，指定されたグループに対してメンバ管理のみ行う．それにより，業務などで使用するグループがグループ管理者の不在時にいきなり削除される状況を回避する．公式グループでは，グルー

Vol.2018-GN-103 No.29
Vol.2018-CDS-21 No.29
Vol.2018-DCC-18 No.29
2018/1/27

プ管理者に対する権限は業務としてシステム管理者からメンバ管理のために移譲されたものであり，重要なグループにおいて意図しないメンバ構成とならないようにすべき必要があるため，例外的に属性型や複合型から導かれたメンバリストの参照を可能とする．

公式グループは，業務などで使用するグループであることより，グループ管理者が掛などで決められている場合が多い．そのようなグループに対して，グループ管理者が変更する度に該当するグループのグループ管理者を変更操作することは，システム管理者の負担が非常に高く，登録・削除漏れが発生する可能性も上がる．そこで，公式グループのグループ管理者は属性を用いた条件式から導けることとする（図 1）．これらにより，グループ管理者から新グループ管理者へスムーズな権限移譲を行う．

なお，一般グループにおけるグループ管理者の追加は，これまでのグループ管理の仕組みと同様，グループ管理者が個々に列挙することで行う．グループ管理者の集合が空になったグループは，一定期間後削除する（図 2）．

提案する公式グループと一般グループについて表 2 にまとめる．

図 2　一般グループの概要

Figure 2　Overview of ordinary groups.

表 2　提案する公式グループと一般グループ

Table 2　Proposed official groups and ordinary groups.

	公式グループ	一般グループ
グループの作成者	システム管理者	一般ユーザ
グループ管理者の登録者	システム管理者	グループ管理者
グループ管理者の登録方法	個々に列挙，属性を指定 既存公式グループを指定	個々に列挙
メンバの管理者	グループ管理者	グループ管理者
グループ管理者不在時のグループの操作	継続（システム管理者にアラート）	削除

運用上，公式グループか一般グループかの判断は，組織ごとに重要性と継続性の確保がどれくらい求められているかにより決定するものとする．グループとしては重要であっても，例えば，使用期間が 10 日間であるグループは，その間にグループ管理者が変わらない可能性が高いため，公式グループでなくてもよい．一方，ほとんど使用しないグループであるが，10 年間継続しなければならないグループは，継続期間中にグループ管理者の交替が発生する可能性が高く，その際にグループ管理者が不在時になる可能性も考えられる．このようなグループにおいては，公式グループとする方がよいと考える．グループは 1 年間以上継続される場合，グループ管理者が交替されることを考えた方がよく，その際に継続性の確保が必要な場合は，公式グループとして扱う方がよい．

3.3　提案するグループ管理システムの設計

提案するグループ管理システムを実現するためには，グループやユーザに関するデータの格納が必要であることより，データベース構造を用いる．グループ管理システムには，グループを作成し操作するためのルールや参照権限などのルール，ユーザがアクセスする際のインターフェースなどの他，作成したグループに関するグループテーブル，メンバを登録するための元となるユーザ属性テーブルをデータベースとして管理する．ユーザ属性テーブルには，氏名，統合 ID，所属，身分など共通に定義された属性を格納する．格納する情報は，中央でユーザ属性を管理する認証サーバなどと常に連携することで，最新の状態に保つ．中央のサーバに格納されていない兼務などの情報をユーザ属性テーブルに格納したい場合は，別途，他部局で管理されるサーバと連携するか，システム管理者が他部局からデータを受領し，直接ユーザ属性テーブルに追加する．グループテーブルには，作成されたグループ ID やグループ管理者，メンバ，グループの種類などを格納する．グループテーブルの情報は，ユーザ属性テーブルのユーザ属性の変更が発生すると，属性型や複合型により作成されたグループのメンバリストも更新する．

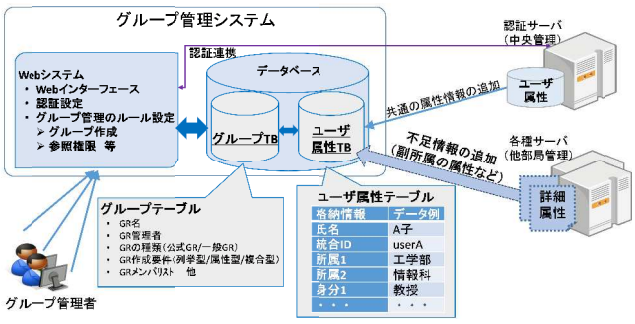

図 3　提案するグループ管理システムの概要

Figure 3　Overview of the proposed group management system.

グループ管理者が操作するための Web インターフェースを用意し，ログインする時には，各ユーザの統合 ID にてログインできるよう，別途中央で管理されている認証サ

Vol.2018-GN-103 No.29
Vol.2018-CDS-21 No.29
Vol.2018-DCC-18 No.29
2018/1/27

ーバと連携する．参照権限の条件式は属性と属性値に対してあらかじめ作成しておくものであり，常に変更が発生するものではないため，Perl スクリプトなどで自由に記述できるようにしておく（図 3）．

4. 提案するグループ管理システムの実装

本章では，3 章で提案する仕組み元に実装したグループ管理システムについて述べる．実装するグループ管理システムは，Grouper などで用いられている一般的な機能を取り入れつつ構築を行った．

4.1 実装するグループ管理システムの概要

作成したグループは Web サービスなどの認可に使用するため，認証サーバである LDAP サーバのプロキシサーバになるよう LDAP Proxy 機能を用いて統合グループ管理システムとして構築し，その上でグループ管理システムを実現した 25）26）．実現する際の言語には Perl を用いた．データベースには MySQL を用いた．グループ管理者が操作するための Web インターフェースには，Apache を用いた 27）．Web インターフェースにログインする時には，統合 ID にてログインできるよう，別途，中央で管理されている LDAP サーバと連携を行った（図 4）．

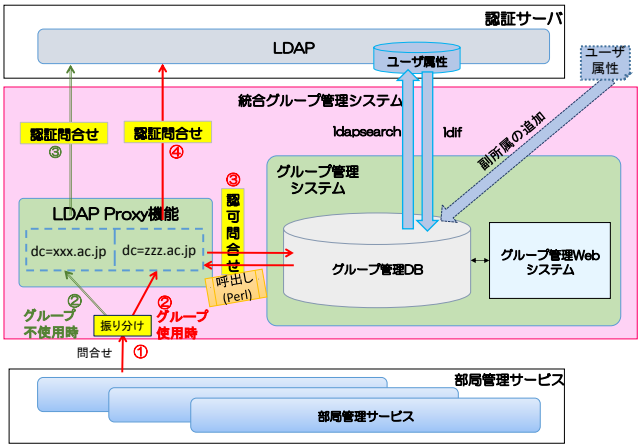

図 4　実装するグループ管理システムの全体構成
Figure 4　Overall composition of the proposed group management system.

4.2 グループ登録時の操作

グループ管理者に参照権限が与えられていないユーザをメンバとして登録する具体的な方法について，列挙型，属性型，複合型のそれぞれに分けて以下に述べる．

列挙型では，グループ管理者がメンバにしたいユーザの ID を直接入力し，メンバ追加をする．ユーザの ID が不明な場合はユーザに直接問い合わせるなど行うことで ID を登録する．属性型では，属性に対する条件式を入力する事で，メンバを導く．複合型は，自身がグループ管理者になっている既存のグループ，もしくはグループの存在を公開しているグループを組み合せることでメンバを導く．属性型と同じく，原則，導かれたメンバリストの閲覧，導かれたメンバ数の閲覧も不可とする．ただし，属性型と複合型のいずれの場合も，グループ管理者毎に設定された参照権限により，作成されたグループの全メンバがそのグループ管理者の参照権限の範囲内に含まれるユーザである場合には，メンバリストの閲覧を許可する．

4.3 参照権限の条件式

参照権限の条件式は Perl スクリプトで自由に記述できるようにしており，Perl の正規表現などを用いることも可能である．条件式は，参照する人と参照される人のそれぞれに割当てられている身分や所属などの指定された属性に対して，属性値が一致する場合や属性値が特定の値である場合に参照可となることを，関係演算子（＝，＜，＞等）を用いて記述する．複数の属性値を組み合わせる場合は，論理演算子∧(and)，∨(or)と￢(not)を用い，条件式を複数設定することで，それらのいずれかが成り立てば参照可とする．

例えば，一緒に業務を行うような同じ身分かつ同じ所属の人に対する場合や教員が担当するゼミを受講する学生に対する場合，大学院掛が大学院生に対する場合など，一般的に参照を許可してよい範囲に対して参照権限を与える条件式を設定する．これらの例を条件式で表すと以下になる．

条件式の例：

$x.a$ = "職員" ∧ $y.a = x.a$ ∧ $y.b = x.b$ (1)

$x.a$ = "教員" ∧ $y.a$ = "学生" ∧ $y.c = x.c$ (2)

$x.b$ = "大学院掛" ∧ $y.a$ = "学生" ∧ $y.d \geqq 5$ (3)

x：参照する人（グループ管理者）
y：参照される人（ユーザ）
$x.a$：属性値（a：身分　b：所属　c：担当ゼミ名/受講ゼミ名　d：勤続年数/学年）

条件式では，X を参照する人の集合，Y を参照される人の集合，その要素をそれぞれ x, y とする．ここでは，説明を簡単にするために参照権限に利用する属性値の成分を a:身分，b:所属，c:担当ゼミ名もしくは受講ゼミ名，d:を勤続年数もしくは学年とする．使用する属性は一般ユーザに割当てられた共通のものとする．

条件式(1)は，グループ管理者 x の身分属性の値が職員であれば，身分属性と所属属性の値が同じユーザに参照権限を与えるという式である．条件式(2)では，グループ管理者

Vol.2018-GN-103 No.29
Vol.2018-CDS-21 No.29
Vol.2018-DCC-18 No.29
2018/1/27

x の身分属性の値が教員，ユーザの身分属性の値が学生であり，グループ管理者の担当ゼミとユーザの受講ゼミが同じ場合に参照権限を与える．条件式(3)の場合は，グループ管理者 x の所属属性の値が大学院掛であり，ユーザの身分属性の値が学生であり学年が 5 以上（大学院生）の人に参照権限を与える．試験運用時では，参照権限の条件式は，参照する人の身分属性が教職員であり，参照する人と参照される人の詳細な所属属性の値が同じ場合のみとした．

4.4 部局等が管理するサービスとの連携

実装したグループ管理システムと部局等が管理するサービスの連携においては，各サービス側にアクセス範囲とアクセスを許可するグループの指定を行う．部局等が管理するサービスからの認証認可を行う際, LDAP Proxy 機能に対して問合せを行い，グループ管理システムに対して該当ユーザが該当のグループに所属するか否かの問い合わせを行う．LDAP Proxy は，将来的に全ての部局等が管理するサービスからの認証認可の窓口となるよう，認可にグループを使用しない場合でも経由できる仕組みとした．一般グループのグループ管理者になれる一般ユーザは，常勤教職員の属性を保持しているユーザのみとした．

4.5 グループ管理システムの試験運用と評価

実装したグループ管理システムは，2013 年 5 月より約 3 年間，東京海洋大学品川キャンパス内にて試験運用を行った．グループは資産を管理するためのシステムや，ユーザを限定する Web ページへのアクセスなどの部局等が管理するサービスの認可ユーザとして使用された．グループ管理システムには，多い時には約 150 のグループがあり，公式グループが約 100，一般グループが約 50 存在した．それぞれのグループのメンバ数は，平均して 1 グループにつきメンバは 10 名から 20 名程度の登録であった．

公式グループはグループ管理者になる人の申請により，システム管理者がグループとグループ管理者を登録する仕組みとした．公式グループの用途は，研究室などの小単位で管理されているネットワーク機器情報等の資産を管理するシステムへのアクセス制限などで利用された．

一般グループは，グループ管理システムにアクセスできる人は身分属性が教員か職員とし，該当する身分属性の人がグループ管理者になり，自由にグループを作成できる仕組みとした．一般グループの用途は，授業やゼミ，委員会などの単位で利用する Web サービスへのアクセス制限などに用いられた．各 Web サービスの管理者などがグループ管理者となり，アクセス可能なユーザをメンバとして登録する．参照権限が無く ID が不明なユーザに対しては，授業などで ID を確認しつつ個々に ID の追加を行った．

試験運用では，公式グループのグループ管理者においては，多くのグループが属性を指定せず，個々に ID を登録していた．その理由として，属性を指定する際に用いる別途中央で管理する認証サーバ上の属性情報が，公式グループの管理者を特定するには詳細さや正確さが足りなかったことが挙げられる．例えば「所属」属性に対しては，部，課，掛など階層が異なる情報が格納されていることや，何も格納されていない場合があること，変更が即時に反映されないことなど，属性情報の管理が十分になされていなかった．そのため，試験運用段階では，グループ管理者の ID を個々に登録し，変更時に都度操作を加える必要があった．

提案する仕組みでは，別途中央で管理される認証サーバの属性情報において，属性の設計がグループの作成を意識したものになっていることと，属性の情報が遅滞なく反映されていることの 2 点が前提となっている．しかし，実際の大学などの分散管理組織における現状では必ずしもそうはなっていない．中央の認証サーバの属性情報や管理体制を即時に見直すことは難しいため，本提案の仕組みを効果的に使うためには，中央の認証サーバが更新される時期と合わせて属性の構成の見直しと属性の正しい管理体制を整えることが必要である．公式グループにおいては，グループ管理者に属性を用いて指定できるよう，組織全体を通して属性の構成と管理体制を整えることが望まれる．

本研究で提案するシステムでは，参照権限を越えた属性型や複合型により導かれたグループのメンバリストを原則として閲覧不可としているが, 連携する Web サービスなどから認証認可を行う際には, その Web サービスの管理者はアクセスしたユーザ情報を知ることができることが判明している．これが運用上，認められない場合には，Shibboleth 等のプライバシーに配慮した認証連携の仕組みを取り入れていく必要がある．

5. まとめ

本研究では，統合認証基盤に基づき，グループ機能を用いて認可情報を統合的に管理する際，グループを体系的かつ効率的に管理するための仕組みの検討を行った．大学などの分散管理組織の実態に合わせて，グループの管理を分散的に行えるよう，メンバ登録時には，列挙型，属性型，複合型を用いるなどを前提条件として，既に開発されているグループ管理の仕組みである米国で開発された Grouper などを参考に，実運用におけるグループ管理を検討し，課題を洗い出し, システム的に解決に導く仕組みを提案した．

これまで課題とされてきたグループに対する柔軟性と継続性に対して，各管理者の権限移譲に着目しつつ，対応策の提案を行った．柔軟性については，一般ユーザが自由にグループを作成でき，参照権限の範囲を越えてメンバ登録できる仕組みとした．継続性については，公式グループと一般グループに分けて定義し，公式グループでは，グル

Vol.2018-GN-103 No.29
Vol.2018-CDS-21 No.29
Vol.2018-DCC-18 No.29
2018/1/27

ープの継続性を確保しつつ，グループ管理者は属性などを用いて管理することも可能とした．

本研究で提案する仕組みを用いることで，システム管理者からグループ管理者，グループ管理者から新しいグループ管理者にスムーズな権限移譲ができることより，グループ管理における管理の負担が削減され，運用コストの削減にもつながることが期待できる．

本研究で提案する仕組みを元に実装したグループ管理システムは，試験運用を行いつつ，順次，連携するサービスの追加を行った．現在，全学展開に向けて進めている．また実装したグループ管理システムをオープンソースソフトウェアとして公開できるよう検討を行っている．

本研究で提案するグループ管理システムでは，メンバにできるユーザを組織内のユーザに限定しているが，本研究で提案する仕組みの概念は，組織を越えたグループにも対応できるものである．今後，組織を越えたグループにも対応したシステムとしていけるよう検討を進める予定である．

謝辞　本研究で提案する仕組みを構築するにあたってご協力頂いたアイティフラッグス社の小岩氏，複数の Web サービスを連携するにあたって，安定運用するためにご協力いただいた東京海洋大学情報処理センター品川地区教職員の各位に，謹んで感謝の意を表する．

参考文献

1） 大谷誠，江藤博文，渡辺健次，只木進一，渡辺義明．シングルサインオンに対応したネットワーク利用者認証システムの開発 ．情報処理学会論文誌 vol.50,No.3,1-9,2010
2） 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, 2012
3） 渡辺義明，渡辺健次,江藤博文,只木進一．利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発．情報処理学会論文誌， Vol.42, No.12, pp.2802-2809(2001)
4） 島岡政基,片岡俊幸，谷本茂明，西村健，山地一禎，中村素典，曽根原登，岡部寿男．大学間連携のための全国共同認証基盤 UPKI のアーキテクチャ設計．電子情報通信学会論文誌. B，通信 J94-B(10), 1246-1260, 2011
5） 只木進一，江藤博文，大谷誠，渡辺健次．認証基盤の効率化と「学認」への対応．電子情報通信学会技術研究報告. ICM，情報通信マネジメント 112(22), 45-50, 2012
6） 飯田勝吉，新里卓史，伊東利哉，渡辺治．キャンパス共通認証認可システムの構築と運用．電子情報通信学会論文誌 B,Vol.J92-B No.10 pp.1554-1565,2009
7） 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
8） 清水 さや子，戸田 勝善，岡部 寿男，グループ管理システムにおけるグループ管理者の効率的管理,情報処理学会研究報告，2015-IOT-28, 35, pp.1-6, 2015
9） 清水 さや子，戸田 勝善，岡部 寿男: 管理権限を一般ユーザにも移譲できるグループ管理システム,情報処理学会研究報告，2014-IOT-27, 18, pp.1-6, 2014
10） 清水さや子，戸田勝善，岡部寿男．統合 ID と属性を用いたグループの体系化．マルチメディア，分散，協調とモバイル (DICOMO2014)シンポジウム 3G-4, 2014
11） 清水さや子，戸田勝善，岡部寿男，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,情報処理学会第 6 回インターネットと運用技術シンポジウム, 2013
12） 平岩真一．グループ管理支援システムの構築．マルチメディア通信と分散処理 63-21 グループウェア 5-21，157-164，1994
13） Ananthakrishnan, R. ,Bryan, J. Chard, K. , Foster, I. more authors. Globus Nexus: An identity, profile, and group management platform for science gateways and other collaborative science applications. Cluster Computing (CLUSTER), 2013 IEEE International Conference on, 1-3
14） Ineternet2 ”Grouper” http://www.internet2.edu/products-services/trust-identity-middleware/grouper/ last visited December. 1, 2017.
15） “Grouper Wiki Home” https://spaces.internet2.edu/display/Grouper/Grouper+Wiki+Home last visited December. 1, 2017.
16） 柿崎淑郎，吉田啓章，辻秀一．一意なアクセスと属性間関係性の検証可能な属性情報分散管理方式．情報処理学会論文誌, Vol.51，No.2，604-612，2010
17） 千葉昌幸，漆嶌賢二，前田陽二．属性情報プロバイダ：安全な個人属性の活用基盤の提言．情報処理学会論文誌, Vol.47，No.3, 676-685，2006
18） 西村健，坂根栄作，合田憲人，山地一禎，中村素典．個人属性と集合属性が共存する認証認可モデル．電子情報通信学会技術研究報告，vol.114，no.216，IA2014-17，19-24，2014
19） Exgen Networks ”LDAP Manager” http://www.exgen.co.jp/lm/ last visited December. 1, 2017.
20） T.Nishimura, M.Nakamura, M.Otani, K.Yamaji, N.Sonehara. Group Management System for Federated Identities with Flow Control of Membership Information by Subjects. Computer Software and Applications Conference Workshops (COMPSACW), 2012 IEEE 36th Annual, 2012, 94 - 99
21） 松平 拓也，中村 素典，山地 一禎，西村 健，高田 良宏，笠原 禎也．学術組織間デジタル資料分散共有システム「ARCADE」の開発．情報処理学会論文誌，Vol.55 No.5，pp.1485-1497，2014
22） 永井孝幸,杉谷賢一,河津秀利,中野裕司．学認対応認証基盤とユーザ ID 体系移行用 CAS ゲートウェイの構築．第 11 回 CLE 研究発表会, 情報処理学会研究報告, Vol.2013-CLE-11, No.20, 2013
23） Ken Klingenstein, Kevin Morooney, Steve Olshansky. Final Report: A Workshop on Effective Approaches to Campus Research Computing Cyberinfrastructure. Document: internet2-crcc-report-200607.html, 2006
24） Charles F. Leonhardt. The challenges and opportunities in extending Internet2 middleware tools in medical information systems. International Congress Series, 1281(2005), 306–310
25） “The Proxy Cache Engine – Open LDAP” http://www.openldap.org/doc/admin23/proxycache.html last visited December. 1, 2017.
26） Dr. Dobb's Journal “The Open LDAP Perl Backend” http://www.drdobbs.com/the-openldap-perl-backend/199102060 last visited December. 1, 2017.
27） “Apache” https://httpd.apache.org/ last visited December. 1, 2017.