「マルチメディア，分散，協調とモバイル
(DICOMO2014)シンポジウム」 平成26年7月

統合 ID と属性を用いたグループの体系化

清水 さや子[†1][†2]　　戸田 勝善[†2]　　岡部 寿男[†1]

組織には様々なグループが存在する．情報システムにおいてもグループは存在し，システムの利用権限を設定する際などにおいて用いられる．しかし，グループは，グループごとに用途やメンバ，管理方法や作成，消滅時期が異なることや，一人につき複数グループに所属するなど，管理が複雑である．そのため，グループ管理においては，条件式などが定義されず，グループ管理者にとっては非常に負荷となっていた．そこで，本研究では，グループ管理に必要な条件によりグループを 4 つに分類し，それぞれのグループに対する管理手法を定義し，グループの体系化を行う．また，本研究では，体系化したグループを管理するためのシステムを設計し，実装を行う．グループを管理する際にユーザ属性を使用するが，近年，ID の統合化が進んでいることより，中央の認証サーバなどで管理される共通に定義された属性を使用する．グループは，中央で一元管理せず，分散的に管理できるシステムとする．なお，本稿で，実装するシステムは，既存システムとの連携試験を行うため，組織内に限定したシステムであるが，本研究で提案するグループ管理手法は，組織を超えたグループも管理可能とする．

Systematic management of group membership using integrated ID and attributes

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

1. はじめに

組織には多くのグループが存在している．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．また，1 人につき 1 つのグループに所属するのではなく，複数のグループに所属するなど，グループの管理は複雑である．そのため，グループ管理においては，条件式などの定義がなされておらず，管理者にとって非常に負荷が高かった．

情報システムにおけるグループは，ユーザ管理の他，システムのアクセス権限や利用権限など，いわゆる認可情報を設定する際に使用される場合が多い．

既に，様々な情報システムにおいて，グループ管理の機能が用いられている．既存のシステムにおけるグループ管理方法は，グループごとにユーザリストを作成して管理する方法，もしくは，既に登録済みの属性から導く方法である．少人数向けの詳細なグループを管理する際には，前者でよいが，規模が拡大すれば管理が困難になり，後者が求められる．しかし，後者では既に設定されている属性値より詳細な単位のグループを作成することが難しい．

また，近年，情報システムの増加に伴い，多くの組織では，認証基盤を整備し，ID の統合化が進んでいる 1)2)3)．これにより，統合された ID（以下，統合 ID とする）などの認証情報は，中央の認証サーバで管理されるが，依然として認可情報は，各々の連携するシステム（以下，連携システムとする）側で行う 4)．そこで，認可情報を管理する際に，グループが必要となる．連携システム側の認可情報は，アクセスを許可するユーザリストを格納する方法と，認証サーバに格納されているグループなどの属性を指定する方法などがあるが，後者の方が管理者の負荷が低く，好まれる．しかし，中央で管理される認証サーバの属性は，共通に定義されたものが多く，特定のシステムに対する詳細な属性が必ずしも存在しているわけではない．

これまでのグループ管理の方法では，管理方法が上記に限定されることが多く，詳細なグループに対する管理の負荷が高かった．そのため，詳細なグループを柔軟に管理できることが求められる．

本研究では，グループを管理する際の条件により，グループを大きく 4 つに分類し，それぞれのグループに対する管理方法を定義することで，グループの体系化を行う．分類するグループは，既存のグループ管理の方法を用いたグループだけでなく，既存の管理方法を組合せて作成するグループ，また，既に作成済のグループの派生より導かれるグループとする．そして，提案する管理方式を使用することで，詳細なグループでも複雑なグループでも対応でき，管理負担の軽減につながる．

なお，提案する管理方式を用いた場合でも，グループごとに管理方法が異なるため，中央で一元管理せず，必要に応じてグループ管理者を立て，分散的に管理することとする．グループ管理の際に使用するユーザ属性は，共通に定義されたものであることとし，グループ管理者の管理負担

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

の軽減のため, グループ管理者やメンバは ID 連携を行う．そのため，属性の管理者により，ユーザ情報が削除されると，グループからも削除されることになる．グループ管理者がいつの間にか不在になることも考えられるため，複数設定するなど，属性を使用することによる課題に対する検討も行う．

2 章では，グループとグループ管理の関連技術について述べ, 3 章では, グループの定義と体系化について述べる．4 章では，体系化したグループの管理を実現するシステムの実装と、実装することで見えてきた課題について述べ，最後に 5 章では，まとめを述べる．

2. 関連技術

2.1 グループのライフサイクル

グループは，組織の編成など，必要に応じて作成される．グループの目的は様々であり，管理方法や作成，消滅時期などはグループごとに異なる．運用していくうちに，拡大や縮小を繰り返し，メンバ交代なども行われる．そして，何度も見直しが行われ，目的が達成すると解散，解体する（図 1）．

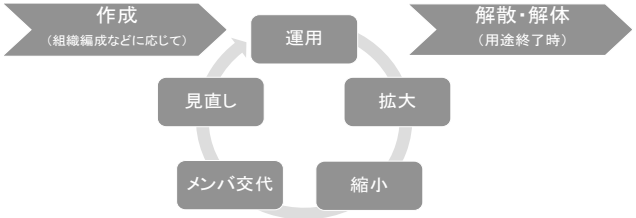

図 1 グループのライフサイクル

一つの組織内には多くのグループが存在するが，管理が必要なグループ全てを中央で一元管理することは，管理者にとって非常に負荷がかかる．そのため，グループの管理は，分散的に管理されることが求められる．

2.2 情報システムとグループ

情報システムは，かつては，システムごとに利用可能なユーザを登録し，グループごとに利用権限を設定していた 5)．しかし，近年，情報システムの増加に伴い，多くの組織では認証基盤が整備されつつある．統合認証基盤システムを導入すると，メールシステムやポータルシステム，E-Learning システムなどの多くの連携システムが，一組の ID とパスワードで利用可能となる 6)．認証情報は，中央に LDAP などの認証サーバを用いることにより管理される．

認可情報は，依然として，それぞれの連携システム側で管理が必要である．認可情報の管理は，連携システムにアクセスを許可するユーザリストを格納したり，ユーザに対してグループを設定することで，行っていた．しかし，それでは，ユーザの登録や削除などが漏れる場合があり，管理の負担も大きい．そのため，最近では，アクセス制限には，中央の認証サーバに格納されているグループなどの属性に対する条件式のみを設定する場合も多くなっている（図 2）．しかし，中央で管理される属性は，組織内の共通フォーマットとして管理することができる氏名や性別，メールアドレス，生年月日などのほか，身分や所属，職責などである．個々の部局で管理する成績情報や発注情報などは属性情報には含まない 7)．

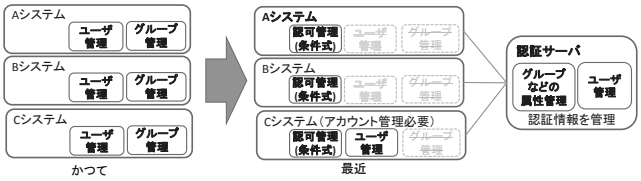

図 2 各システムのグループ管理の遷移

2.3 分散管理組織とグループ

人やシステムの管理が中央で一元管理されておらず，身分や所属ごとに管理する部局が異なり，分散的に管理されている組織がある．本研究では，それらの組織を分散管理組織と呼び，著者らは，これまで，分散管理組織における分散型の管理手法に関する研究を行ってきている．

分散管理組織で提供されるシステムは，中央が提供する全体向けのシステムの他に，学部や学科などの部局が提供するシステム，研究室やプロジェクトごとに提供するシステムなど，さまざまなシステムが存在する．これらのシステムは中央で一元管理されず，部局などにより分散的に管理されている．このような分散管理組織においても，近年では認証連携が進んでいる．その際，中央に認証サーバを構築し，認証情報の照合は行うが，認可情報の管理は，連携システム側でそれぞれ行う．

2.3.1 分散管理組織のユーザ管理

分散管理組織において，中央でユーザ情報の管理を行う際，ユーザの身分や所属に応じた担当部局が管理する情報と連携し，管理することが求められる．

そこで，著者らは，分散管理組織でユーザ情報の管理を行う際，担当部局により分散的な管理を行い，さらに必要に応じてユーザ情報をプロビジョニングする機能を保持する統合ディレクトリシステムを提案済である 7)．

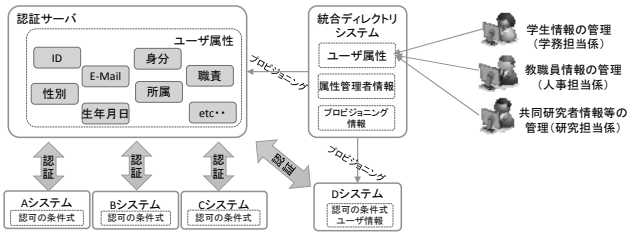

図 3 分散管理組織におけるユーザの分散管理例

提案済みのシステムの管理は，分散管理となるため，管理する属性は，共通に定義されたものとなる．また，プロビジョニングするシステムは, 中央が管理するシステムや, 中央と連携する部局などが管理するシステムが対象である（図 3）.

2.3.2 分散管理組織の属性管理

組織内には，多くの兼務者が存在する．しかし，中央で管理される属性の数は，全ユーザ共通であり，ユーザごとに異なるわけではない．そのため，中央では，主務の所属や身分に関する情報のみが管理される場合が多い. しかし，実際は主務の所属だけでなく，兼務やさらに詳細なグループ単位で動くことも多い.

例えば，G センター所属の O 教授は，J 研究科の教授職も兼務している場合を考える．共通で定義される所属属性は，G センターになり，兼務の所属である J 研究科グループには含まれない場合，J 研究科が提供するシステムの認可設定において，所属属性が J 研究科のみアクセス可能と設定されていた場合，O 教授はそのシステムが利用できない．それだけだはなく，J 研究科システムの管理者は，設定した属性に含まれるユーザ情報が分からないため，O 教授がアクセス不可であることも，わからない場合もある.

2.4 既存システムのグループ機能

既存システムでグループという機能は，ファイルサーバ 9)10)や LDAP 11)，Active Directory 12)などの認証サーバ，その他, 多くのグループウェア 13)14)などで存在している．Web 上では, Facebook 14)など 16)の SNS においても使用されており，グループごとに，アクセス制限を設定したり，サービスを提供したりできる．また，グループにメンバの追加や削除，参加の承認や禁止などの設定ができる.

既存システムでグループを管理する際に使われる方法は，メンバを個々に列挙して管理する方式，もしくは，既に格納されているグループなどの属性から導き出す条件式を設定して管理する方式である.

前者は，属性などにとらわれない詳細なグループを作成できる．しかし，個々にメンバの管理が必要なため，メンバの所属などの異動時に対応が困難となる．退職後にいつまでも削除されないメンバが存在する場合や，着任時に漏れる可能性がある．さらに，メンバの数が増大したとき，管理が煩雑になる.

後者は，個別にメンバ管理を行う必要がないため，登録や削除漏れは発生しない．しかし，共通に定義された属性を使うことが多いため，詳細なグループを作成することが難しい.

2.5 著者らが既に提案中の分散管理組織におけるグループ管理システム

メンバを個々に列挙する際, ID 情報の取り扱いレベルの検討が必要になる．そこで我々は，グループ管理者の身分に応じて，ユーザ情報の閲覧権が異なるシステムを提案中である 8)．提案中のシステムでは，認証基盤が整備されている分散管理組織で，中央の認証サーバと連携し，メンバ管理には ID 連携する.

提案するシステムは，グループ管理者が公式に組織から任命された場合のグループと，そうでない場合のグループに分け，前者を公式グループ，後者を非公式グループと呼ぶ．公式グループは，所属や身分などの属性を元に指定された範囲において，統合 ID の閲覧を可能とする．メンバ登録時には，閲覧可能な情報から，属性でソートし，該当する統合 ID を選択することで，登録を行う．非公式グループは，公式に任命された管理者ではないため，統合 ID の閲覧権限は与えず，メンバの統合 ID を直接入力することでメンバ登録を行う．登録時に統合 ID の存在有無の確認を行う（図 4）.

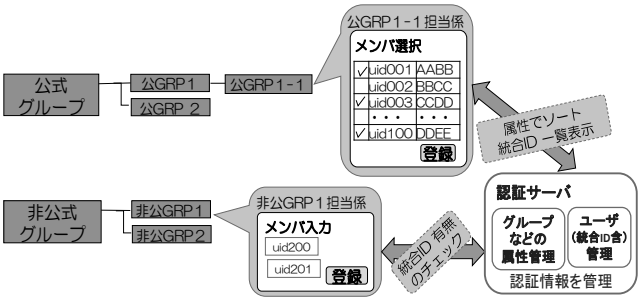

図 4 提案中のグループ管理システム

メンバの所属などが変更になる際，公式グループは，グループ管理者に変更通知を行い，グループ管理者が必要に応じてメンバの更新を行う．非公式グループは，あらかじめ属性などを開示されたものでないため，変更通知は行われない.

3. グループの定義と体系化

ここでは，グループの定義を行い，グループとメンバ管理方法に対してグループを４つに分類して体系化を行う.

3.1 グループの定義（数学的，構成的）

本研究では，グループの定義を以下と考える.

- そのグループのメンバを定義するルール
- そのグループの管理者または「管理者のグループ」（これ自体もグループ）の組

3.2 グループの分類

3.2.1 列挙型グループと属性型グループ

本研究では，2.4 節の既存システムのグループ管理方法も使用する．メンバを個々に列挙することで管理されるグループを列挙型グループと呼び，属性からメンバを導き出し管理されるグループを属性型グループと呼ぶ．両グループの特徴を表 1 にまとめる．

表 1　列挙型グループと属性型グループの特徴

	列挙型 GR	属性型 GR
詳細なグループ作成	**可能**	不可能
メンバを個々に追加	**可能**	不可能
メンバの所属などの異動時の対応	必要	**不要**
登録や削除漏れの可能性	高	**低(属性に依存)**
メンバ数が増大したときの管理の煩雑さ	大	**小**

※下線は，長所とする

表 1 より，詳細なグループを作成したりメンバを個々に管理する際には，属性型グループより列挙型グループの方が柔軟に対応できる．しかし，グループの規模が大きくなり，長期的に管理する場合，列挙型グループでは，メンバの所属などの異動時に登録や削除漏れが起こる可能性が高く，属性型グループの方が管理の負荷が小さいといえる．

3.2.2 複合型グループと派生型グループ

列挙型グループと属性型グループはそれぞれにメリットとデメリットがある．それらを踏まえて，グループを管理する際に，属性型グループと列挙型グループを組み合せて作成することができるグループが必要である．本稿では，このグループを複合型グループとよぶ．

さらに，既に定義されているグループを組合せることで導かれるグループも必要である．本稿では，このグループを派生型グループとよぶ．派生型グループは，作成済のグループに対して，メンバを追加する際，追加するメンバのためのグループを作成し，組合せることとなる．複合型グループと派生型グループの特徴を表にまとめる（表 2）．

複合型グループは，列挙型グループと属性型グループを含む比率により，グループ管理者の管理の負担が異なる．列挙型グループの割合が高い場合は，列挙型グループと同様，詳細なグループの作成は可能となるが，管理の負荷は高くなる．

派生型グループは，既に定義されているグループに対して組合せるため，属性型グル―プと同様，作成済のグループに従うものとし，メンバの所属などの異動時の対応は不要であり，管理の負荷は低い．

表 2　複合型グループと派生型グループの特徴

	複合型 GR	派生型 GR
詳細なグループ作成	**可能**	不可能（原則）
メンバを個々に追加	**可能**	不可能
メンバの所属などの異動時の対応	必要	**不要**
登録や削除漏れの可能性	中	**低(グループに依存)**
メンバ数が増大したときの管理の煩雑さ	中	**小**

※下線は，長所とする

3.3 グループの体系化

3.2 節で分類した 4 つのグループを体系化するため，表 3 に整理する．

表 3　分類したグループの体系化

A	属性型 GR	属性に関する条件式
B	列挙型 GR	メンバリスト
C	複合型 GR	A と B の組み合わせ（和集合，積集合，差集合，補集合）
D	派生型 GR	すでに定義されているグループ（A,B,C）の集合演算（和集合，積集合，差集合，補集合）により導かれるグループ

D は，元となっているグループにそのグループの管理者がメンバを追加したときにそれが波及するものとする．

3.4 属性連携に関する検討

属性を使用する際に，閲覧権限などの検討が必要になる．

3.4.1 属性値の使用

中央の認証サーバ上の属性および属性値は，公開されているものと非公開のものがある．公開されているものは使用できるが，非公開の属性を使用することは難しい．そのため，原則，公開されている属性に対する属性値を使用することとする．

ID は，一般的には公開されていないものであるため，使用方法を検討する必要がある．列挙型グループのメンバ登録時，所属などの属性ベースにメンバの ID を選出できるとよいが，ID は公開しているものではないため，グループ管理者は，メンバの ID を知らない場合も多い．公開すると悪用される可能性もあるため，全てのグループ管理者に公開するわけにはいかない．一研究室付きの職員がグループ管理者になり，比較的小規模のグループの場合，メンバの ID が分からない場合は，メンバに確認すればよい．しかし，グループ管理者が組織から公式に任命され，比較的規模の大きいグループを管理する場合，すべてのメンバの

ID を確認するのは非常に負荷がかかる．

そこで，列挙型グループにおける ID の閲覧制限においては，既に提案中である 2.5 節を引継ぎ，グループ管理者の権限により，利用制限を付けることとする．本稿では，2.5 節の公式グループを公式タイプ，非公式グループを非公式タイプとよび，ID の閲覧権限は，2.5 節を引き継ぐ．

3.4.2 グループの閲覧権限

次に，グループの閲覧権限を考える．作成されたグループには，特命調査グループなど，グループの存在自体を非公開にしなければならないグループがある．そのため，グループ作成時に公開か非公開，一部公開（メンバのみ公開）を設定する必要がある．

派生型グループは，既に作成されたグループを組み合せるが，組み合わせることができるグループは，公開設定がされているグループのみとする．属性型グループは，使用する属性の管理者がグループ管理者と異なるため，基本的には，メンバリストの閲覧はできないものとする．グループ作成時の条件式は，公開，非公開，一部公開の設定できるものとする．

メンバの管理は，それぞれのグループ管理者が行うため，メンバ情報に関して，公開か非公開，一部公開を設定できることが必要である．これらは，グループの作成時に設定できればよいと考える．

3.4.3 メンバの属性変更や削除

メンバの身分や所属などの属性に変更があり，メンバ変更が必要な場合を考える．属性型グループの場合，属性が変更されれば，グループに含まれるメンバは自動で変更されるため，対応は不要である．

列挙型グループの場合，個々に列挙して管理されているメンバに対して，メンバリストの基準を明確化することが難しく，自動で変更を行わない方がよいと考える．そのため 2.5 節を引継ぎ，グループ管理者に変更通知を行い，グループ管理者が必要に応じてメンバの更新を行えばよいと考える．

複合型グループは，その中に含まれる属性型グループにおいては，属性の変更に応じて自動で変更されるため，対応は不要である．列挙型グループは，対応を必要とする．

派生型グループは，作成済のグループの変更に応じて，自動で変更されるため，対応は不要である．

また，グループの種類に関わらず，退職や卒業などにより，ID が削除されれば，グループのメンバから自動で削除される．

3.4.4 グループ管理者とグループ管理者用グループ

属性からグループ管理者として登録されている ID が削除されれば，グループ管理者からも削除され，いつの間にか，グループ管理者がゼロになる可能性がある．そのため，グループ管理者は複数設定できればよいと考える．

グループ管理者を複数設定する際，グループ管理者用のグループを作成する．しかし，誰でもグループ管理者になれたり，グループ管理者用のグループに所属できると，グループが悪用される可能性も考えられる．そのため，ある程度の制限が必要となる．そこで，グループの管理者は，最低でも一人は，責任が取れる身分の者（正規の職員）とする．ID の削除により，グループ管理者用のグループに正規の職員が一人もいなくなる場合は，アラートを上げるなどの対応が必要となる．

3.5 グループの作成，管理手法

それぞれのグループに対する作成方法および管理方法を，グループ作成方法を表 4 にまとめる．

表 4　グループ作成手順，管理方法

<table>
<tr><td>A)属性型 GR</td><td colspan="2">①グループ作成，グループ管理者設定
②メンバ登録，公開属性に関する条件式を設定
③グループの公開，非公開，一部公開を設定
④条件式の公開，非公開，一部公開を設定
（メンバリスト閲覧不可（属性によるため））
メンバ変更時の対応不要，自動（属性によるため）</td></tr>
<tr><td rowspan="2">B)列挙型 GR</td><td colspan="2">①グループ作成，グループ管理者設定
②メンバ登録，メンバを列挙（※）
③グループの公開，非公開，一部公開を設定
④メンバリストの公開，非公開，一部公開を設定
⑤メンバ変更時には都度対応</td></tr>
<tr><td>（※）公式タイプの場合：所属などの属性からソートし ID 表示（管理者ごとに閲覧権限異なる），その後，メンバの ID 選択，登録</td><td>（※）非公式タイプの場合：属性によるソートなし，メンバの ID 列挙，その後，ID の存在確認（照合），登録</td></tr>
<tr><td>C)複合型 GR</td><td colspan="2">①グループ作成，グループ管理者設定
②メンバ登録，公開属性に関する条件式とメンバを列挙し組合せるための条件式を設定
③グループの公開，非公開，一部公開を設定
④メンバリストと条件式の公開，非公開，一部公開を設定
⑤メンバ変更時は都度対応</td></tr>
<tr><td>D)派生型 GR</td><td colspan="2">①グループ作成，グループ管理者設定
②既に作成済の A)，B)，C)を組合せるための条件式を設定，または，それらに個別にメンバを追加
③グループの公開，非公開，一部公開を設定
④グループを組合せた条件式の公開，非公開，一部公開を設定
メンバ変更時の対応不要，自動（既存グループによるため）</td></tr>
</table>

以下には，それぞれのグループを作成する際の条件式の例を記す．

A) 属性型グループの例
groupAA = ("N**"="n**") and ("N**"≧"0")
B) 列挙型グループの例
groupBB = (id = "userA","userB","userC","userD")
C) 複合型グループの例
groupCC = ("N**"="n**") and ("N**"="0") or (id = "userX","userY","userZ")
D) 派生型グループの例
groupDD = groupAA and groupBB

(group**=グループ名　N**=属性名　n**=属性値
id=ID)

4. グループ管理システムの実装

ここでは，3 章で体系化した 4 つのグループを実際に管理する為のシステムを，設計し実装する．本研究で提案するグループ管理方式は，組織を超えたグループでも対応可能であるが，本稿における実装では，組織内におけるグループ管理を対象とする．

4.1 前提条件

提案するグループ管理システムを実装するにあたって，前提条件を以下に記す．

- 3 章で分類した 4 つのグループが管理できるシステムとする
- グループの管理は，分散して行う
- グループの管理者は複数名設定可能とする
- グループには様々な機能が求められるが，本稿におけるグループの機能は，表 5 とする
- 表 5 の機能は，グループ作成時に設定することとする

表 5　グループの機能

機能	操作		
グループ名	公開	非公開	一部公開
メンバ情報 (属性を使う場合は条件式)	公開	非公開	一部公開
グループの有効期限	公開	非公開	一部公開

グループの機能は，グループの参加時に「誰でも可」,「メンバが追加」,「メンバから招待」なども求められるが，本稿では省略する．

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内ではユーザ属性の管理が必要であるが，ユーザ属性を管理するサーバ等と連携することで，グループ管理システム内では直接操作しないこととする（図 5）．使用する属性は，属性の元となるサーバ側で決められている使用可能なものを使用する．ユーザの所属などの変更時に，属性の元となるサーバ側でユーザ属性値に変更があれば，グループ管理システム内の属性にも反映される．

各グループの作成は，表 3 に従い作成する．また，グループ作成時には，表 5 の機能の設定を行う．派生型グループを作成の際，作成済のグループを組合せるが，その際に使用できるグループは公開設定されているグループのみである．

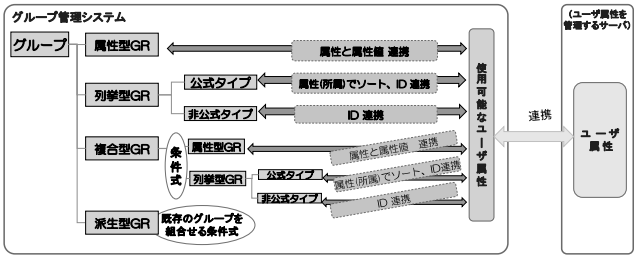

図 5 グループ管理システムの構成

メンバとグループ管理者は，ID 連携により管理を行う．ID 連携を行う場合，連携サーバ側でユーザ情報が削除されれば，メンバやグループ管理者として登録されていたとしても削除される．グループ管理者がゼロにならないよう，グループ管理者を複数設定可能とする．そのため，グループ作成時に，グループ管理者用のグループを作る．グループは一人でもグループとみなし，それぞれのグループには，必ずグループ管理者用のグループを作成する（図 6）．グループ管理者用のグループには最低でも一人は正規の職員を含むこととし，正規職員が不在になる場合は，システム管理者にアラートを上げる．そのため，グループ管理者は身分属性と連携しておく．

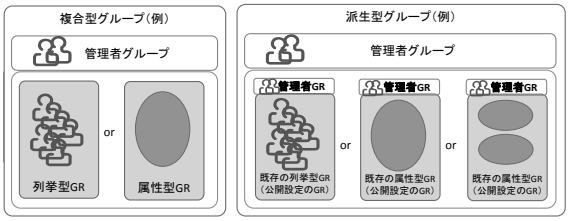

図 6　グループとグループ管理者の構成例

4.3 LDAP Proxy によるグループ管理システムの実装

近年，認証基盤が整備されている組織が多い．そのため，本稿では，実装時に使用する属性は，組織の中央で管理さ

れている認証サーバと連携し，その中に格納されている属性の中で使用可能なものを使用することとする．

認証サーバには，LDAP を用いることにより，LDAP サーバと容易に組み合わせることができる LDAP サーバのプロキシサーバ（以下，LDAP Proxy とする）を構築し，その中でグループ管理の機能を実現する 17)18)（図 7）．LDAP には，OpenLDAP を用いる．LDAP サーバより，属性に必要な情報を取得し，同期する．

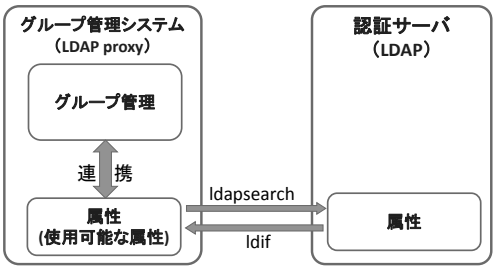

図 7　実装したグループ管理システム

4.4 連携システムからの認証認可の検証

本稿では，設計したグループ管理システムで作成したグループを，連携システムから認可に使用できるか検証を行う．認可の設定は，連携システム側に認可で使用するサーバ（グループ管理システム）とその中で使用するグループを設定する．LDAP Proxy を用いることで，認証においても同サーバを指定するだけで，LDAP Proxy から LDAP サーバに認証を行い，結果を連携システムに返すことができる．

利用者は，まず，連携システムに問い合わせを行い，ID とパスワードを入力する．連携システムは，グループ管理システムに対して，あらかじめ設定している認可のためのグループに，利用者の ID が含まれているかの照合を行う．照合に成功すれば，グループ管理システムから認証サーバに利用者の ID とパスワードの問い合わせを行う．認証に成功すれば，連携システムが利用可能となる（図 8）．

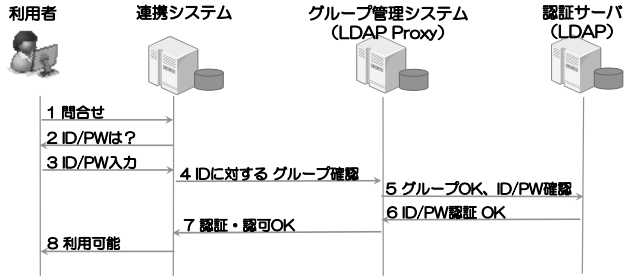

図 8　グループ管理システムを使った認証・認可フロー

4.5 グループ管理システムの課題

連携システムのアクセス制限時にグループ管理システムを使う場合，属性の参照権限などの課題が残る．ただし，グループ管理システムは，グループを管理するものであるため，ここで述べる課題に対しては，グループ管理システム側で対応するか，連携システム側で対応するかを含めて，今後検討が必要であると考える．

4.5.1 属性の参照権限

グループ作成時に属性を使用する際，属性の参照権限の検討が必要になる．

属性に含まれるメンバの情報を知らなくとも提供できる Web のアクセス制限などのサービスだけであればよいが，アカウント追加が必要なシステムも存在する．たとえば，メールサーバなどではメールサーバ上にアカウント追加が必要となるため 19)，メールサーバの管理者にアカウントの通知をしなければならない．このような場合，メンバに対して案内を行い，メンバ自身が登録できる仕組みが必要になると考える．

4.5.2 属性の管理

認証サーバ上の属性は，身分や所属ごとの管理部局により登録されているものであるが，登録されている情報が完全とはいいきれない．例えば，女性支援機構などが提供するシステムがあり，属性を使って女性研究者向けのグループを作成したい場合を考える．認証サーバ上の性別が誤って女性として登録されている男性がいた場合，その男性もメンバとして含まれる．逆に，女性であるが，誤って男性として登録されている場合，そのメンバに含まれない．グループ管理者は認証サーバの属性に含まれるメンバは見ることができないため，認証サーバ上の属性に委ねることになる．

そこで，属性に含まれるメンバを知る必要がある場合は，所属するメンバに対して，メンバの確認を行う仕組みが必要になると考える．また，グループに所属するメンバに対して，システム利用権に対する同意を必要とする場合，メンバに対して案内を行い，参加するか否かを問えればよいと考える．

4.5.3 属性変更時の猶予

所属などの属性が変更になる際，該当属性を使用しているグループのメンバは変更になる．しかし，連携システムによっては，グループのメンバではなくなった場合でも一定期間利用可能とする，猶予期間が必要な場合がある．特に，メールサーバなどに対しては，猶予期間が必要な場合が多い．属性の変更は，ID が削除されるわけではないため，ID が存在していれば認証は可能である．しかし，認可で使用するグループのメンバ情報が変更になると使用できなくなるため，これに対する猶予が設定できる仕組みが必要であると考える．

5. まとめ

本研究では，これまで管理が複雑なため，定義が曖昧となっていたグループに対する定義を行った．グループ管理に必要な条件によりグループを 4 つに分類し，体系化を行った．体系化したグループの管理を実現するためにグループ管理システムの実装を行った．

情報システムにおけるグループは，ユーザ管理の他，利用権限などを管理するために用いられている．これまで用いられていたグループの管理方法は，メンバを個々に列挙する方法（列挙型グループ），もしくは，属性から導き出す方法（属性型グループ）であった．列挙型グループでは，メンバ数が増えれば増えるほど，管理が複雑になり，メンバの登録・削除漏れになる可能性が高くなる．属性型グループは，詳細なグループの作成ができなかった．特に，共通に定義される属性を使用する場合，特定のサービスに対する詳細な属性が，必ずしも存在しているわけではないため，必要な属性が含まれていないことが多かった．

本研究では，既存の管理方法で用いられていた列挙型グループ，属性型グループの他，列挙型グループと属性型グループを組み合せることで作成するグループを複合型グループ，そして，作成済のグループから導かれるグループを派生型グループと定義した．定義したそれぞれのグループに対して，管理方法などを検討し，グループ管理における体系化を行った．

さらに，体系化したグループを管理するために，グループ管理システムを設計し，実装を行った．本稿で実装したシステムでは，中央の認証サーバから公開可能な属性を使用した．メンバとグループ管理者は ID 連携を行った．属性は，中央の認証サーバの属性と同期することより，中央の認証サーバ上から ID が削除されると，グループ管理システムからも削除される．そのため，グループ管理者がゼロになる可能性があった．その対応として，すべてのグループに対して，グループ管理者用のグループを設定することで，複数名でグループ管理を可能とした．実装したグループ管理システムで作成したグループを他システムからの認可で使用できるか検証するため，LDAP Proxy を構築し，その中で，グループ管理の機能を実現した．グループ管理システムを実装することで，属性値の参照権限などの課題が判明した. これらの課題に対する詳細な対応策の検討は，今後必要であると考える．

本研究で提案するグループ管理方式は，組織内外を問わず利用できるものである．本稿においては，組織内向けのシステムとして実装を行ったが，今後，組織を超えたグループに対するグループ管理の仕組みを検討していく予定である．

謝辞

グループ管理システムを実装する際の属性連携においては, 東京海洋大学情報処理センター品川地区のスタッフ, およびアイティフラックスの小岩氏にサポートいただいた. ここにおいて，深く御礼申し上げる．

参考文献

1) 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
2) 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
3) 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
4) 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
5) 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
6) 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
7) 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 Vol.2013,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, p1976-1983,2013
8) 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」，情報処理学会インターネットと運用技術シンポジウム 2013, 65-72，2013
9) EMC「ストレージ」http://japan.emc.com/storage/index.htm
10) Buffalo「ストレージ」http://buffalo.jp/products/catalog/storage/
11) OpenLdap http://www.openldap.org/
12) Microsoft「Active Directory 技術情報」http://technet.microsoft.com/ja-jp/windowsserver/bb466131.aspx
13) Japan Total System Co,Ltd「GROUP SESSION」http://www.gs.sjts.co.jp/
14) Cybozu, Inc「cybouzu」http://cybozu.co.jp/
15) Facebook https://www.facebook.com/
16) mixi https://mixi.jp/
17) The Proxy Cache Engine – OpenLDAP http://www.openldap.org/doc/admin23/proxycache.html
18) Dr Dobb's Journal The OpenLDAP Perl Backend http://www.drdobbs.com/the-openldap-perl-backend/199102060
19) The Postfix Home Page http://www.postfix.org/
20)