Vol.2011-IFAT-102 No.5
Vol.2011-DD-80 No.5
2011/3/28

電子書籍閲覧における組織横断型認証のためのグループ管理

西村健[†]　中村素典[†]　井上仁[††]　山地一禎[†]　曽根原登[†]

電子書籍利用においてエンドユーザに対する認証は不可欠である．本論文では大学をはじめとする学術機関で盛んに利用され始めている組織横断型認証連携（フェデレーション）を利用した認証により電子書籍閲覧を制御する方法について考察する．

Group Management System in Access Federation for E-book Services

Takeshi Nishimura[†], Motonori Nakamura[†], Hitoshi Inoue[††], Kazutsuna Yamaji[†] and Noboru Sonehara[†]

It is necessary to provide authentication information to properly use e-book services. We will classify the concept of “groups” in academic access federations and propose the group management system which provides flexible access control to e-book services.

1. はじめに

図書や雑誌は，研究や教育を遂行する上で不可欠な情報源であり，学生，教員，研究者による利用頻度は非常に高い．平成 20 年度の大学における図書雑誌の購入費は，国公私立を合計して約 746 億円にのぼり，これに加えて，個人レベルでも多くの図書が購入されている．これらの経費のうち，すでに国立大学の雑誌に関しては，印刷版よりも電子版に充てる費用が上回っている．電子ジャーナルが提供する，簡易性，即時性，移動性や検索機能による利便性の向上は，研究の推進を飛躍的に向上させ，現在では，紙媒体では成し得なかった複合的なメディアに成長しつつある．一方，大学における図書の電子的な利用は始まったばかりであり，学術分野における電子書籍利用については今後の展開が注目されている．

現在の電子ブックでは，図書と利用者が 1 対 1 の関係になる利用モデルが主であるが，図書館での利用を想定した，NetLibrary や ebrary といったサービスも提供され，いくつかの大学図書館で導入実績を積んでいる．図書館向けのサービスは，従来の電子ジャーナルのようにダウンロードしたファイルに閲覧制限をかけない利用モデルと，特殊なクライアントアプリケーションやウェブによる閲覧で閲覧制限をかける利用モデルに大別できる．前者は，利用者にとっては便利である反面，大学等で利用される単価の高い学術書や専門書を提供する出版社にとっては，不正利用に対するリスクが高い．電子ブックの利用が進むにつれて，このリスクに応じた契約費の増加が生じ，図書館運営を圧迫することが容易に想像される．これに対し後者の利用モデルを提供するプラットフォームには，出版社が安心してコンテンツを提供できるというメリットがある．しかしながら，現状の閲覧制限プラットフォームでは，同時アクセス数の制限や利用可能 OS の限定など，いくつかの機能的な制約により，利用者のニーズを満足するサービスが提供できていない．この問題点を克服しなければ，大学における電子ブックの普及は進まないものと考えられる．

大学では，全学的な図書館だけなく，キャンパス，学部，研究室など様々なレベルで図書が購入され，共有されている．従来のこうした所属レベルでの図書の購入は，物理的距離の問題に対処することのみならず，図書の優先利用や，占有したいというニーズを満たすところが大きい．しかしながら，現在の電子ブック提供プラットフォームは，大学としての機関契約と機関認証をするにとどまり，これまで紙媒体で実現できていた，キャンパスや学部，研究室といった異なる所属レベルでの利用モデルを反映できていない．これは，電子ブックプラットフォームのアクセス制御が，従来な

[†] 国立情報学研究所
National Institute of Informatics
[††] 九州大学
Kyushu University

Vol.2011-IFAT-102 No.5
Vol.2011-DD-80 No.5
2011/3/28

がらの IP アドレスによる認証技術と同レベルにとどまっていることに起因する. 機関における一般的なネットワーク構成では，所属部局に関する情報を，電子ブック提供プラットフォームに到達する IP アドレスから知ることはできない．一方，全てのユーザの所属情報を電子ブック提供プラットフォーム側で収集して管理することも現実問題として不可能であるために，全学という単位での認証しかできなかったのが現状である．こうしたアクセス制御の不備は，利用者にとって電子ブック利用の不便さを強調し，大学における電子ブックの契約ならびに利用促進に対し，大きなマイナス要因となっている．その結果，出版社は電子ブックの本来のニーズや市場を捉えることができず，学術書や専門書の電子化に躊躇する状況を生んでいるものと考えられる．我が国の研究・教育機関における電子ブック利用を促進するためには，利用者の所属レベルに対して, 電子ブックへのアクセス権を柔軟にコントロールできる, 新しい認証・認可技術の導入が必須の課題である．

国立情報学研究所では，最先端学術情報基盤整備の一環として，学術認証フェデレーション「学認 : GakuNin」1),3)の構築に取り組んでいる．学認では，学術関係の Web サービスに，大学の認証システムを利用してログインすることができる．このとき，Web サービス側では，大学の認証システムからユーザの所属情報などの属性を受け取ることにより，柔軟なアクセスコントロールを実現できる．

従来の手法である, サービス提供者がユーザ ID や属性の管理を行っている場合は，利用者は個別のパスワードを各々の Web サービスで設定する必要があった. 複数の ID やパスワードの管理は利用者にとって負担となり，異なる Web サービスに共通の ID やパスワードを設定することはセキュリティ上のリスクを高めることになっていた．

これに対し，学認では，セキュアに管理された所属機関の認証システム（ID とパスワード）を利用して多くの学術サービスを受けることができる．また，認証システムは一カ所にしかないため利用者はサービス毎に ID とパスワードを入力しなくてよいシングルサインオン機能により, 円滑に Web サービスが利用できるという特徴がある. さらに，IP アドレスによる認証とは異なり，自宅や出張先からでも機関の認証システムを使用して機関が契約するサービスが利用できるリモートアクセスが実現できるという利点もある．こうした様々な利便性を提供する学認は，本年度から本格運用を開始し，既に 22 機関の参加のもと総 ID 数は 35 万に達している．また，33 機関が本格運用に向けてのテストを実施しており, 国立情報学研究所が実施したアンケートでは，さらに学認参加に向けて 31 機関が積極的な検討を進めている. このようにＩＣＴ利活用のための認証連携基盤は，わが国では他に例を見ない成功事例であり，新たなビジネスイノベーション基盤としてＩＣＴ産業界，コンテンツ産業界からも期待されている．

現在，学認で利用可能なサービスとしては，電子ジャーナルサイトや TV 会議，e ラーニング, ファイル共有といった e リサーチツールなどがある. これらそれぞれが，大学の認証システムから送られてくるユーザ属性を利用し，認可判断に利用したサービスを提供している．この学認の認証基盤は，電子ブックにも活用可能であると考えられる．そこで，本論文では，大学／キャンパス／学部／研究室といった様々なレベルの認可単位を「グループ」として，学認が提供する組織横断型認証と連携し，グループに対して柔軟な認可判断を行うためのシステムを提案する．

以下，2 節ではフェデレーション内に存在するグループを分類し，グループ情報をサービスに対してどのように提示できるかを検討する．3 節で我々が構築したシステムであるメンバ属性プロバイダを提案し, 4 節で実装および実証実験について触れる．

2. 組織横断型認証で必要とされるグループの分類および実現方法

2.1 グループの規模による分類

特に SAML 2)を利用した組織横断型認証（フェデレーション）においては，ID 基盤上で ID とともにその個人に付随する属性が管理されており，必要な属性をサービスに対して送信することで，当該サービスにおける認可判断に利用している．以下，組織に属する ID 基盤を Identity Provider (IdP)，サービス提供主体を Service Provider (SP) と表記する．従来から用いられているフェデレーションにおいてグループとして認可判断に利用される属性としては以下のようなものがある．

- IdP entityID … IdP の ID．同一 IdP から提供される認証情報には全て同一の IdP entityID が付与される
- organizationName … その利用者の所属組織（大学等）
- organizationalUnitName … その利用者が所属する機関内組織（学部等）
- eduPersonAffiliation … その利用者の職種（学生，教員，職員等）

この他にもフェデレーションで採用されていない属性も含めれば数は増えるが，それらは概して使われない傾向にある．それは，一般的に 1 組織に 1 つある IdP では学科等のより細かな分類に対応できないことが原因と考えられる．同様に organizationalUnitName も管轄外として提供しない IdP も存在する．

さらに考察すると，細分化されたグループを管理する管理主体が，IdP の管理主体と異なるということが IdP の属性として提供されない原因として考えられる．特に大規模な組織では，末端のグループについてはそれに近い上位グループに管理を委譲する傾向にあり, 委譲された側で独自に管理されている. それら全てを再び統合して IdP の属性として送出することは不可能とは言わないまでもコスト面から現実的ではない. また，フェデレーション内で細分化されたグループを一意に識別する識別子がないという実装上の問題もある．これはフェデレーションにおいてグループ ID を管理する管理主体が必要であることを意味する．

以上のことから導かれる結論は, 純粋に IdP と SP からなるフェデレーションでは，

Vol.2011-IFAT-102 No.5
Vol.2011-DD-80 No.5
2011/3/28

eduPersonAffiliation や organizationalUnitName によるおおまかなグルーピングには対応できても，学科レベルや研究室レベルの細分化されたグループには対応できず，それらに対応するためには別途フレームワークが必要であるということである．

2.2 グループ管理者による分類

別の視点で，フェデレーション内のグループをその管理を主導する立場の者により分類すると，以下のようなものが考えられる．

A) IdP 主導グループ
B) SP 主導グループ
C) 第三者主導グループ

A)については先に触れた管理権限の委譲も含めた ID 階層の管理者がそのグループメンバの正しさを担保・保証できるグループである．語弊はあるが人事部が管轄するグループと言い換えられる．学科や研究室をそのまま表すグループは A)に分類される．A)は当該管理者がグループを管理するのが最も効率が良い．

これに対して，SP がグループをコントロールするパターンが B)である．例えば，

- 利用者からの申請を受け，機関の責任者に確認を取った上で当該 ID に機関属性を付与する
- 特定の IP アドレスレンジからアクセスした利用者は，その機関の者とみなし機関属性を付与する

のような形で，既存サービスにも B)のパターンは存在する．ただし，その管理方法の妥当性が明らかでない場合が多いことと作り込みなど煩雑な部分が多いことから，現実に利用されるグループとしては限定的である．

C)は，A)や B)と異なり組織やサービスに直接紐付けられないグループである．自然発生的なコミュニティや，兼業によって発生するグループは本務の組織に紐付かないという意味で第三者的である．C)については誰を管理者／責任者とするか，それによって何を保証するかが他のグループと比較して曖昧であることが多い．

2.1 節および 2.2 節で扱ったグループの分類および従来のフェデレーションで扱える範囲を表 1 にまとめた．

表 1　グループの分類と従来型フェデレーションでの対応

	学科・研究室単位	学部単位	大学単位
IdP 主導グループ	×	△	○
SP 主導グループ	△	△	△
第三者主導グループ	×	×	×

○ … 対応，　△ … 一部対応，もしくは管理が複雑，　× … 非対応

2.3 グループの組み合わせ

その他，これらのグループの組み合わせにより新たなグループが存在することがある．例えば，A 大学の A1 研究室と B 大学の B2 研究室が共同研究をする場合には A1 研究室と B1 研究室の和集合としてグループを定義するのが効率的である．また，各大学の特定学部が集って立ち上げたコンソーシアムのようなグループについては，当該学部をグループとして，それらのグループを合わせたものとしてコンソーシアムグループを構成することができる．

2.4 グループの実装方法

前節の分類の「第三者主導グループ」を鑑みて，既存の IdP/SP 以外に別途エンティティが必要であることは疑いない．また，「IdP 主導グループ」「SP 主導グループ」を包含できるエンティティを構築することによって，フェデレーションで統一したグループの枠組みを提供することができる．

フェデレーションにおいて大勢を占める SAML と親和性の高いグループ情報提供の仕組みとして考えれば，特定の属性（フェデレーション内で合意が取れれば任意の属性で構わないが便宜上“isMemberOf”とする）の属性値としてメンバであるグループ名を列挙して SP に渡すという手法になる．このように，IdP でなく属性のみを提供するエンティティを属性プロバイダ (Attribute Provider, AP) と呼ぶ．ここでは，AP が従来の IdP と SP との間のプロトコルに干渉して SP に属性を提供する仕組みを検討する．isMemberOf 属性の提供には以下の 2 つの方法が考えられる．

(ア)Proxy IdP 方式
(イ)SWITCH VO 方式

Proxy IdP 方式は，上述の AP を IdP と SP の中間に存在する IdP として実現する方式である．本論文ではこの中間の IdP を Proxy IdP と呼ぶ．SP からの認証要求は Proxy IdP が受け，Proxy IdP が本来の IdP に認証要求を行い，IdP から受けた認証結果を Proxy IdP

Vol.2011-IFAT-102 No.5
Vol.2011-DD-80 No.5
2011/3/28

が SP に戻す際に isMemberOf 属性を付加する．フェデレーションにおいて初回の多数ある中からの IdP 選択を行う際には，Discovery Service (DS)という仕組みを用いて利用者が IdP 一覧から IdP を選択するという操作を行うが，ここで Proxy IdP を選択してもらい，Proxy IdP 内でも同様の DS から本来の IdP を選択してもらうこととなる．

後述の SWITCH VO の方式と比較して，従来のフェデレーションの枠組みの中に完全に収まっているためソフトウェアの改修の必要がない，また SP に相対しているのは Proxy IdP のみであるため必要最小限の情報しか流れないというメリットがあるものの，DS が 2 回現れることになるため利用者の操作が煩雑になり間違いやすいという問題がある．

一方，SWITCH VO 方式では，SP から直接 IdP に認証要求を行い認証結果を得た後で，所定の手続きにより AP から isMemberOf 属性の情報を得る．この方式を採用したシステムで有名なものが SWITCH VO であったことから，本論文では SWITCH VO 方式と呼んでいる．SWITCH VO 方式では，IdP に利用者の ID を要求し，その ID を元に AP に isMemberOf 属性を要求する．属性要求の仕組みとしては，ブラウザを経由せずサーバ同士が通信を行うバックチャンネルという方法で属性要求および応答が行われる．

バックチャンネルによる属性要求機能は最近の Shibboleth ソフトウェアには実装されており利用の障壁は少ないが，SP に利用者 ID を通知しなければならないというプライバシー上の問題がある．利用者 ID として SP ごとに固有の Targeted ID を用いるという方法もあるが，最新版のソフトウェアが必要である他，依然として ID が通知されるので SP 内では追跡可能であるという問題が残る．

このように，実装の容易性とプライバシー保護の程度，そして利用者への利便性を考慮してこれらの方式の選択を行うのがよいと考える．

3. メンバ属性プロバイダ GakuNin mAP

前節の考察の下，本論文ではメンバ属性プロバイダ GakuNin mAP を提案する．

GakuNin mAP はフェデレーションの ID に対して isMemberOf 属性を提供する AP であり，単純なフェデレーションの枠組み（IdP および SP の連携）で実現できていない層のグループ属性を付与する．isMemberOf 属性の提供方法には実装の容易性および利用者の利便性から SWITCH VO 方式を選択した．

GakuNin mAP によって，isMemberOf 属性が SP に送信される様子を図 1 に示す．実際には cookie によって各種情報が記憶されるため，2 回目以降のアクセスでは記憶されていて省略可能な通信はスキップされる．

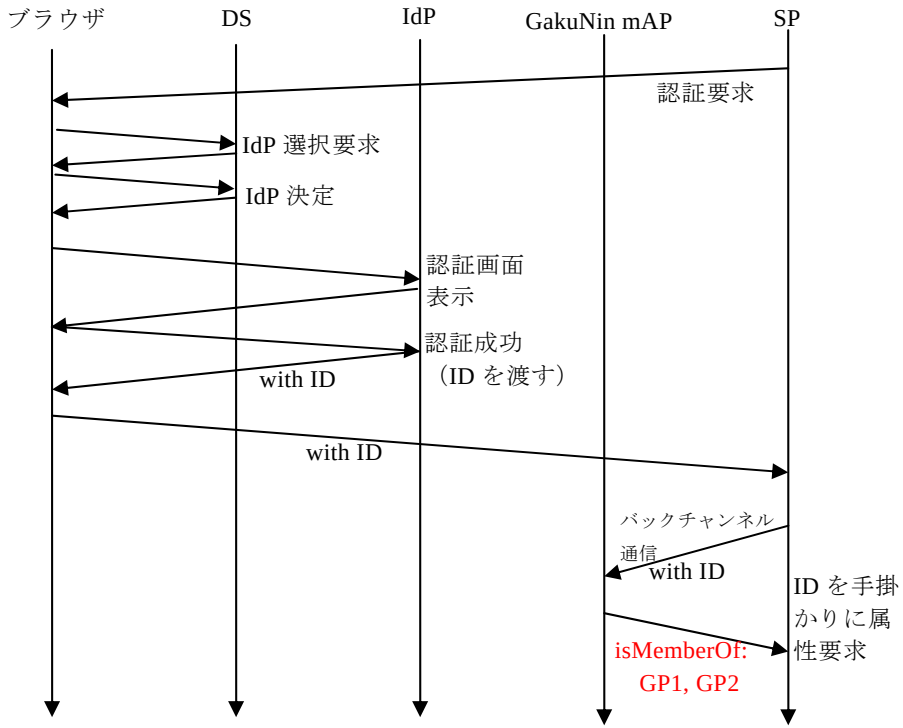

図 1　GakuNin mAP による isMemberOf 属性送信

3.1 グループの階層化

我々が提案する GakuNin mAP の重要な機能としてグループの階層化がある．電子ジャーナル・電子書籍における出版社との契約を見据えた場合，各大学の学部等の組織同士がコンソーシアムという形でつながり，コンソーシアムが主体となって出版社と契約を結ぶことがありうる．コンソーシアムはサービスの側というより大学，つまり ID 管理者側の組織であり，SP に対してはコンソーシアムという一つのグループとし

Vol.2011-IFAT-102 No.5
Vol.2011-DD-80 No.5
2011/3/28

て見せることが合理的である．各学部がグループとして表現されているときにその上位グループとしてコンソーシアムグループを定義することを想定している．つまり，あるグループのメンバとして利用者 A が存在する場合，その上位グループ全てに A は存在しているものとしてグループ情報を扱う．

また，学科を研究室の集まりとして扱う，さらに学部を学科の集まりとして扱う場合も，階層的なグループ構造は効果的であると考えられる．

3.2 SP グループ

階層化グループの特殊形態であるが，特定の SP に紐付くグループを SP グループと呼ぶ．1 つの SP に紐付く SP グループは高々1 つである．SP グループの上に他のグループが存在することはない．この紐付けは当該 SP 管理者のみが行える．

SP グループの概念を用いることで，全てのグループ情報が任意の SP に対して送信されてしまう問題を未然に防ぐことができる．すなわち，SP グループに含まれるグループの属性のみが当該 SP に対して送信されるということであり，各グループ管理者が SP グループへの参加・脱退を適切に管理すれば，必要なグループの属性のみが必要な SP に対して送信されるということが実現できる．別の見方をすれば，あるグループが SP グループの下へ参加したという事象を，当該 SP の利用を開始するというトリガーとして利用することも可能である．

GakuNin mAP によって扱われるグループおよびそれらの関係を図 2 に示す．

4. 実装および実証実験

前節で説明した GakuNin mAP の基本的な部分は実装が完了し実際に稼働している．グループの実装については SNS 等を参考にし，以下のような機能を実装している．

- ID の種類：メンバ，グループ管理者
- 招待／利用者からの入会申請
- 承認／自由参加
- 公開／非公開
- 下位グループからの承認／自由参加
- 上位グループに接続することへの承認／自由接続

これに関連して，本年 2 月 21 日より 1 カ月にわたり東京大学、千葉大学、京都大学、九州大学の有志の協力の下、電子書籍提供プラットフォームを用いた実証実験を行っている．ここで得られた知見を元に，必要とされるグループの規模，用途など，GakuNin mAP が実用に足るかどうかの検討，設計の見直し等を行う予定である．

5. まとめ

学術電子書籍の利用が促進されるためには柔軟なアクセス制御が不可欠であり，フェデレーションにおける柔軟なアクセス制御を行うには GakuNin mAP のような組織をまたがるグループ管理の仕組みが不可欠である．

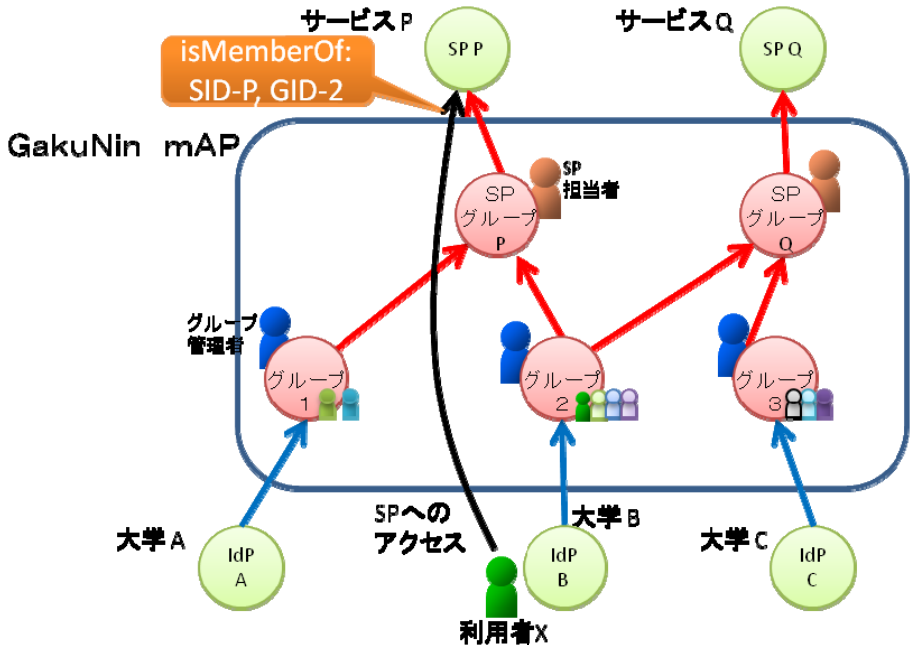

図 2　GakuNin mAP の概念図

今後は，GakuNin mAP の実地での有効性を確かめつつ，メンバ数などグループ情報を SP に提供することによって契約との適合性・信頼性を高めるための機能を導入していきたい．これは IdP でも SP でもない第三者としてのフェデレーションが運用してこそ意味のあるものと思われる．また，isMemberOf 属性の送信については，SWITCH VO 方式のように利便性を高めつつ、プライバシー保護を行える方式を提案していきたい．

謝辞　この研究は総務省「新ＩＣＴ利活用サービス創出支援事業」「研究・教育機

Vol.2011-IFAT-102 No.5
Vol.2011-DD-80 No.5
2011/3/28

関における電子ブック利用拡大のための環境整備」の一環として実施されました.

参考文献

1) 学術認証フェデレーション https://www.gakunin.jp/
2) OASIS Security Service (SAML) TC, http://www.oasis-open.org/committees/tc_home.php?wb_abbrev=security
3) 山地一禎, 中村素典, 片岡俊幸, 西村健, Tananun Orawiwattanakul, 曽根原登, 岡部寿男, “学術認証フェデレーション Gakunin の本格運用”, 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 年 5 月.