第18回学術情報処理研究集会
発表論文集 pp.51−56

徳島大学における学認利用申請システムの開発と運用

Development and practical use of GakuNin application system at Tokushima University

関 陽介†，松浦 健二†，上田 哲史†，佐野 雅彦†
Yosuke Seki†, Kenji Matsuura†, Tetsushi Ueta†, Masahiko Sano†

seki@tokushima-u.ac.jp, ma2@tokushima-u.ac.jp, ueta@tokushima-u.ac.jp, sano@tokushima-u.ac.jp

†徳島大学 情報センター

† Center for Administration of Information Technology, Tokushima University

概要

信頼された組織間の認証連携や，情報システムの共有を実現する学術認証フェデレーションを利用するためには，参加機関用のガイドラインに準拠した運用が求められる．徳島大学では，教育用システムを利用するために必要な個人アカウントを，入学時や着任時に提供しており，学認も当該アカウントを用いて利用できる．また本アカウントは個人アカウントだけでなく，学会等の受付メールアドレス取得などを目的に擬人アカウントとして要請に応じて提供している．ただし，個人アカウントは自動でライフサイクル管理が行われるが，擬人アカウントの継続管理は年度末の棚卸作業に限られ，個人アカウントとは異なる管理・利用方法で運用されている．そのため，学認のガイドラインに非準拠となる場合が懸念される．本稿では，学認の利用における本学のアカウント管理の問題点を取り上げ，ガイドラインに準拠するアカウント判定方法の提案と，その運用実績に基づく結果について報告する．

キーワード

学術認証フェデレーション, Shibboleth，認証

1. はじめに

近年，外部システムに学内認証システムを用いて利用する認証連携が注目を集めている．日本においては，国立情報学研究所（以下，NII とする）が中心となり，複数の大学間で組織相互を信頼する学術認証フェデレーション(以下, 学認)が運用されている. これは, Shibboleth [1]を用いて認証連携や情報システム共有の実現を目指している [2]. また，すでに認定を受けた大学も存在する，信頼性評価の国際標準である Level of Assurance（以下，LOA とする） [3]を取得することで，米国の政府機関などが提供する一定の高信頼システムに対しても，認証連携が可能となる．

徳島大学は 2013 年から正式に運用フェーズとして学認に参加している．学認に参加することで，専用アカウントの作成を要求する電子ジャーナルや researchmap 等を，学内で提供するアカウントで利用でき，利用者の利便性向上に大きく貢献できる．また，Fshare（ファイル共有サービス）や meatwiki（情報共有サイト）など，学認参加機関向けに限定して提供されるシステム（以下，

学認提供システムとする）を利用できる．

しかし，学認に参加するためには，参加機関用のガイドラインに準拠した運用が要求される．例えば，利用者アカウントの再利用期間の設定や，同一性の保障などがある．本学では入学，着任時に教務システムやメールシステム等の教育用システムや学認を利用可能な，個人アカウントを提供している． また，本アカウント管理上は擬人アカウントを要請に応じて提供しており，個人の利用に留まらない管理を要する．擬人アカウントは個人アカウントに準拠した権限を保有するが，個人アカウントとは異なるポリシで運用されている．このため，学認で定められたガイドラインを一部非準拠となる可能性が懸念される．

そこで本稿では，学認を利用可能なアカウントの判定方法を設計し，実運用について述べる．

2. アカウント管理・利用方法の問題

本学では学内用の認証システムとして Shibboleth を利用しており，アカウントの一元管理や教育用システムのシングルサインオン [4]を実現している [5]．Shibboleth とはシングルサインオンのための一つの実装であり，Internet2/MACE プロジェクト [6]で開発が始められ，日本に限らず世界中の学術機関で利用されるフレームワークである．Shibboleth のアーキテクチャは，SP(Service Provider)， IdP(Identity Provider)，それらにアクセスする UA(User Agent)の 3 種類のエンティティから構成される．SP は教務システムやメールシステム等のサービスを提供する WEB システムを指し，UA にサービスの提供や，認可を行う．IdP はバックエンドのリポジトリ(ディレクトリサービスや RDB)を参照して，利用者の認証情報や属性情報を SP に送付する．なお，本学ではリポジトリを LDAP として扱う．UA は SP を利用する学生，教職員などの利用者の環境を指す．

本学では，学内用システムを利用するためのアカウントを下記に示す異なる体系で管理しており，大学構成員は入学・着任時の配布や，任意の申請により各アカウントを取得できる．主な学内用システムのアカウントは，以下 4 つ存在する（図-2 に示す）．

1. 個人アカウント
2. 擬人アカウント
3. 無線・VPN 用アカウント
4. 教育・研究者情報データベース用アカウント

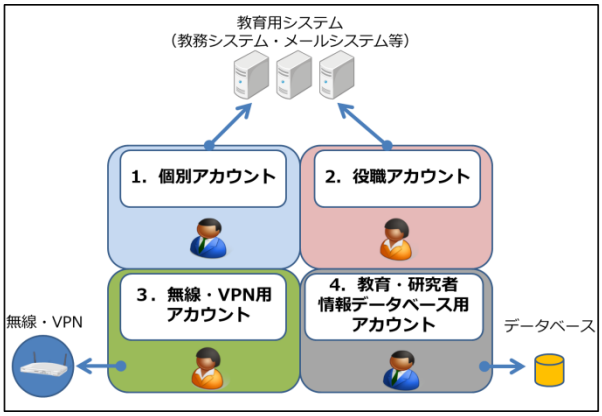

図-1．学内用システムのアカウント

個人アカウントは，教務システムや大学ドメインのメールシステムなど，大学生活を送る上で必要な教育用システムを利用するために用いられ，学生は入学時，教職員は着任時に配布される．

本学のメールシステムは，上記個人アカウントに紐づくものと，そうではないシステムとに主に分かれる．前者は 2012 年に教育用システムの改修に合わせて導入されたメールシステムであり，後者は従来からのものである．これは，各部局をサブドメインで区別するメールシステムになる．統合メールシステムは個人アカウントから独立しており，各部局管理者に管理を委託しているため，部局内で任意にアドレスを作成・削除できる．

しかし，統合メールシステムは導入から数年経過し，サーバの老朽化が懸念されたため，2015 年 3 月に廃止する予定となった．そのため，学会の受付用などで使用するアドレスを，新規に得るためには個人アカウントを取得することとなるが，当該アカウントは大学構成員に対して 1 つしか配布されず，複数保有することは基本的に許されていない．

そこで，本学では個人アカウントとは別に，申請に応じて擬人を対象にした擬人アカウントを提供している．当該アカウントは学会やセミナーの窓口等のメールアドレスを取得する際に利用されたり，役職持ちの事務職員に役職用アドレスを提供するために使用される．役職用アドレスは soumu-kachou@tokushima-u.ac.jp（仮）の様に，アドレス名に所属と役職名が付与される．当該アドレスを日常業務で利用することで，定期的な異動に伴う引継ぎを容易にできる．

本学では個人アカウントと擬人アカウントを同じ LDAP で管理しており，一部の個人アカウントは擬人アカウントと同じ属性で管理される．つまり，学認提供システムを利用するためのアカウントに個人アカウントを対応させた場合，擬人アカウントも含まれることを意味する．

このような運用において注意を要するのが，学認や学

認提供システムのガイドラインである. 前章で述べたが，学認のガイドラインには利用者アカウントの再利用期間の設定や同一性の保障など，多くの運用基準が定められている．個人毎に提供される個人アカウントは自動でライフサイクル管理が行われ，学認のガイドラインに準拠した運用で管理される．しかし，擬人アカウントは個人アカウントとは異なるポリシで運用されるためガイドラインに厳密には準拠しない可能性が生じる．

例えば，擬人アカウントの役職用アドレスを利用することで，事務職員は異動等に伴う引継ぎを容易にできるが，それは後任者に擬人アカウントを渡すことを意味する．しかし，ガイドラインでは最終の利用時から最低 24 ヶ月間の再利用を認めていない．また学会やセミナー等の受付用メールアドレスを利用するために，複数の利用者が擬人アカウントを利用する可能性があるが，ガイドラインでは同一アカウントでのアクセスが，同一人物であることの保証を要求する．これらは複数存在する要求事項の一部であり，上記以外にも注意を要する項目が存在する．また擬人アカウントを，研究費等で雇われたパート職員等の学外者が利用する可能性も考えられる．学認提供システムは, それぞれが利用規約を保持しており，学外者に利用を認めないものが存在する可能性もある．

以上より，ガイドラインや利用規約に準拠することで不正利用を防ぐために，学認で利用されるアカウントの整理が必要となる．

3. 設計方針の検討

本学は，個人アカウントと擬人アカウントを同じ LDAP で管理しており，一部の個人アカウントは擬人アカウントと同じ属性で管理される．異なるリポジトリ，または属性で管理していれば，個人アカウントを学認用アカウントとして，認証システムの参照先に設定することで，容易にアクセス制限をかけることが可能である．

しかし，システム導入から数年運用している設計を変更することは，作業コストを考慮すると容易に対応できない．各アカウントに判定値を登録することで判定することも可能であるが，すでに多くの擬人アカウントが提供されているため，技術的には可能でも作業負荷を考慮した場合，現実的ではない．

学認の利用対象は全ての大学構成員ではなく，一部の学生・教職員である．学認を利用すると，CiNii や SpringerLink などの電子ジャーナルを学外から閲覧したり，Microsoft が提供している DreamSpark を，学認を用いて在学証明することで，開発用ソフトウェアを取得できる．ただし，これらは教務システムなどの教育用システムとは異なり, 一部の大学構成員に利用は限定される．そのため，個人アカウントと擬人アカウントが学内に混在しており，利用者が大学構成員の一部であることを考慮すると，利用希望者の申請に基づくアクセス制御の実現が，適していると考える [7]．申請制とすることで，管理部局が申請されたアカウントを審査し，必要に応じてアクセス権限を付与することで，ガイドラインや利用規約に準拠したアカウントに限定して，認証システムを利用させる設計となる．

4. システム設計

前節の設計方針を元に，学内に提供する申請システム（以下，学認利用申請システムとする）のシステム設計を行った．

学認を利用可能なアカウントは個人アカウントに限定されるため，その管理部局は申請されたアカウントが擬人アカウントなどの要件を満たさないアカウントではないことを確認できればよい．

そこで WEB サイトを用いたオンライン利用申請を提供し，申請されたアカウントを，管理部局が審査する設計とした．ただし，アクセス制御を行うのは学認提供システムではなく，本学が管理する認証システムである．つまり，審査の結果に基づいたアクセス制御を認証システムで実現する必要がある．

そこで，我々は NII が提供している Shibboleth のプラグインソフトウェアである FPSP（Filter Per SP） [8] [9] に注目した．Shibboleth の設計では，IdP から渡される利用者の属性情報を元に，SP が認可制御を行う．つまり，従来の設計では IdP 自体で利用可能な SP の選択を行うことは困難であったが, FPSP を実装することで, 利用者の属性情報に基づいた，特定 SP へのアクセス制御を実現できる．例えば，特定の電子ジャーナルを，工学部に所属する大学構成員に限定して提供する，等のアクセス制御を IdP で実現できる．我々はこの FPSP を IdP に実装することで，認証システムにアカウントを判定させる設計とした．具体的には，申請されたアカウントに問題がなければ管理部局（本学では情報センター）で判定値を登録し，認証システムはその値を判定基準としてアクセス制御を行う．

ただし, ガイドラインや利用規約を準拠したとしても，学認提供システムを利用するためには，IdP は要求される属性情報を送付する必要がある．教育用などの学内システムとは異なり，例えば，氏名やメールアドレスなどの個人情報を学外に送付する必要がある場合，その取扱いについて，利用者の同意を得るなどの対応が求められる．

そこで我々は，利用者同意取得システムである

uApprove.jp [10]を実装することにした．FPSP と同じく，NII が提供するプラグインソフトウェアであり，IdP に uApprove.jp を実装することで，個人属性を求める学認提供システムに対して，その送付の同意を利用者に求めることができる．

5. システム実装

第 4 章で述べたシステム設計を元に実装を行った．本学では学内用の認証システムとして Shibboleth を運用しているが，リソースの負荷分散や障害時のリスク回避を理由に，学内用 IdP とは別に学認用 IdP を新たに構築した．なお，表 1 に本実装で用いた学認利用申請システムと学認用 IdP の仕様を示す．共に，Citrix XenServer 上の仮想マシンとして稼働している．

表-1. 各システムの仕様

システム	ソフトウェア
学認利用申請システム	CentOS release 6.4
	Apache 2.2.15
	php 5.5.16
	Mysql 5.1.69
	Shibboleth SP 2.5.2
学認用 IdP	CentOS release 6.4
	Apache 2.2.15
	Apache tomcat 7.0.55
	Shibboleth IdP 2.4.0
	uApprove.jp 2.2.1
	FPSP 1.10

利用者が学認提供システムを利用するまでの一連の流れと，システム全体像は以下となる．（図-3 に示す）

1. 利用者が学認利用申請システムに学認で使用するアカウントを申請
2. 管理部局（情報センター）が審査し，アカウントに応じて判定値を登録し，結果を利用者に通知
3. 2 に問題なければ，学認提供システムを利用

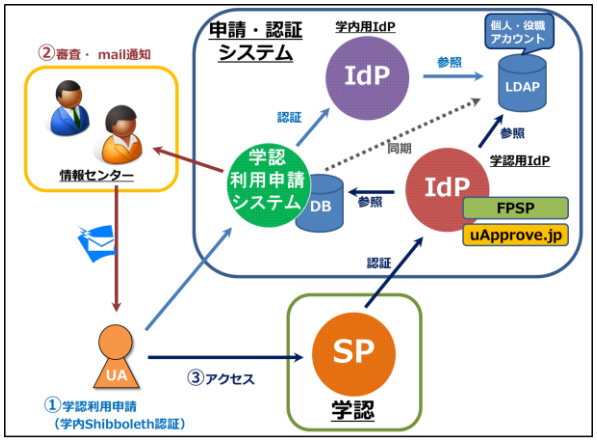

図-2. システムの全体像

ここからは学認利用申請システムと学認用 IdP のシステム実装について述べる．

5.1. 学認利用申請システム

学認利用申請システムは学認の案内サイトも兼ねており，学認の概要や FAQ 等の情報を公開している [11]．また，利用者認証として学内で利用している Shibboleth を設定しており，申請者を大学構成員に限定している．

本システムは一般的な WEB 申請システムであり，アカウントや氏名などフォーム入力等により取得した情報を，バックエンドの DB に登録する．情報センターはアカウントを審査し，個人アカウントであり，学認の要件を満たすと判断した場合に，判定値を追加登録する．次節で述べるが，この値を学認用 IdP が参照し，アクセス制御の判定に使用する．なお，判定値は管理者用ページから GUI（Graphical user interface）で登録でき，管理者を Shibboleth 認証と管理者アカウントの認可設定でアクセス制御している．

本システムの DB を，個人アカウント等が登録されている LDAP と同期している．本学では卒業・退職等により大学構成員でなくなった場合に，個人アカウントを自動で削除している．シェルスクリプトを用いてその削除結果を日々同期させることで，申請されたアカウントが大学構成員のものであるか確認し，必要に応じて判定値を無効化している．

5.2. 学認用 IdP

学内用 IdP とは別に，FPSP と uApprove.jp を実装した学認用 IdP を構築した．構築手順としては，NII が公開しているドキュメントを参考にしている．

FPSP は利用者の属性情報を元にアクセス制御を実現する．IdP は複数のリポジトリを参照することが可能で

ある．つまり，IdP に既設の LDAP と学認利用申請システムの DB を参照させ，LDAP に登録された利用者のアカウントに紐づく判定値を DB から取得し，FPSP がその値を元にアクセス制御を実現する仕組みである．例として，図-3 は申請が許可されたアカウントに限り，SpringerLink をアクセス可とする設定情報である．アカウントが許可された場合，status に ok が登録され，FPSP がその値を判定してアクセス制御を行う．

```
<EntityDescriptor entityID="https://fsso.springer.com">
  <Attribute attributeID="status">
      ok
  </Attribute>
</EntityDescriptor>
```

図-3. FPFP の設定情報

uApprove.jp は，利用者に属性送付の同意を取る機能を提供する．ただし，全ての学認提供システムを対象とする必要はなく，個人情報を要求するものに限定すればよい．そこでブラックリスト機能を用いることで，例えば eduPersonPrincipalName を要求する reseaechmap など，システムに応じて同意を求める設定にしている．なお，属性情報については，NII が公開している情報を参考にしている [12].

学認を利用するために申請が必要であるが，未申請で学認提供システムにアクセスする利用者もいると推測される．そこで，IdP の認証画面に学認利用申請システムのリンクを貼ることで，申請漏れを防ぐことにした（図-4 に示す）．

図-4. 学認用 IdP の認証画面

6. 効果および考察

前節で述べた設計と実装を元に学認利用申請システムを構築し，2014 年 1 月から本番環境に提供している．従来は，電子ジャーナルや researchmap 等を利用するために専用アカウントが必要であった．しかし，学認に参加することで，個人アカウントの使用が可能となり，利用者の利便性向上や，アカウント管理負荷軽減などにおいて一定の貢献ができている．また FPSP を実装することで，学認や学認提供システムのガイドラインや利用規約に準拠でき，uApprove.jp を実装することで，各利用者に属性送付の同意を取ることが可能となった．

学認利用申請の推移グラフと，学認提供システムの利用数を図-5，図-6 に示す．

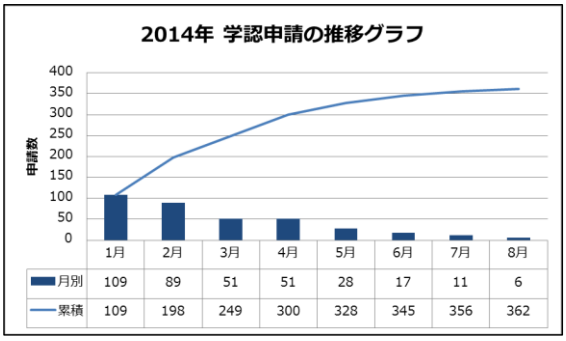

図-5. 学認申請の推移グラフ

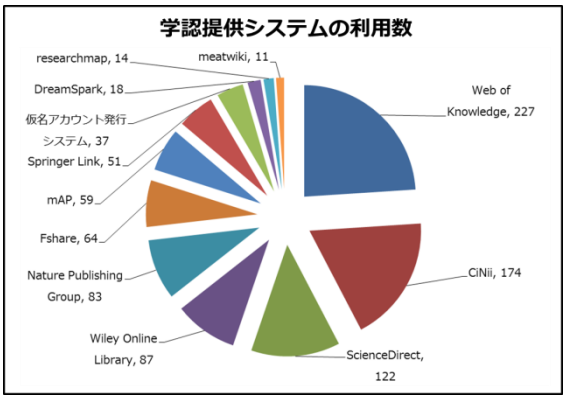

図-6. 学認提供システムの利用数

学認の申請数は本システムの提供当初に多くあり，4 月末時点で 300 に達したが，それ以降は一定水準のまま推移している．申請者の区分として，学生は 146，教職員は 216 であった．また，LDAP への同期で，判定値が無効化されたアカウントは 31 であった．今後も一定水準を保つとは考えられるが，周知活動を強化して，学認の申請者数を増やしたい．

学認提供システムの利用数については，合計は 947 であり，6 つの電子ジャーナルの合計は 758 である．つまり，全体の 80%を占めており，本学では電子ジャーナルの利用者が多いことを示している．researchmap の利用が想定より低くなったが，本システムは個人情報を使用するため，uApprove.jp の対象となる．ただし，uApprove.jp を実装した都合で，researchmap の提供は 6 月 23 日となり，その周知を案内サイト以外に未実施であったため，必然的に利用数が低くなったと考えられる．

学認利用申請システムに未申請で，学認提供システム

にアクセスした擬人アカウントは存在しなかった．しかし，学認利用申請システムに擬人アカウントの申請が3件あり，いずれも否認となった．学認の案内サイトに利用可能なアカウントについて案内していることもあり，否認された数は多くはないが，学術提供システムの不正利用を防ぐことができていると考えられる．

7. おわりに

本稿では，徳島大学で運用している学認利用申請システムについて述べた．本学では教育用システム用に個人アカウントと擬人アカウントを管理しているが，同じLDAPに登録されているため，どちらのアカウントを用いても学認提供システムを利用することができる．

学認や学認提供システムは厳しく定められたガイドラインや利用規約が存在するため，アカウント管理はそれらに準拠した運用が求められる．しかし，本学では個人アカウントは自動でライフサイクル管理が行われるが，擬人アカウントの整理は年度末の棚卸作業に限られ，個人アカウントとは異なるポリシで運用されている．そのため，ガイドラインや利用規約に非準拠する項目が発生することで，不正利用に繋がる可能性があった．

そこで我々は，非準拠項目に対する対策手段として，学認利用申請システムと，FPSPとUApprove.jpを実装した学認用IdPを構築した．利用者がアカウントを申請し，擬人アカウントでなければ情報センターが判定値を登録することで，学認用IdPに実装したFPSPでアクセス制御を行う設計である．

2014年1月より本番環境で稼働し，8月時点で学認利用申請システムに365件の申請があり，3件否認された．当該システムは，学認の案内サイトも兼ねており，学認の概要や利用可能なアカウント等の情報を公開している．つまり，学認利用申請システムと案内サイトを運用することで，一定のガイドラインや利用規約を準拠する運用に貢献できていると考えられる．

本学は，次のステップとして米国国立衛生研究所 [13]が提供する PubMed [14]等のサービスや，認証基盤の信頼性評価を得るために，LOA1 取得も検討している．毎年秋に行われる学認アンケート [15]の回答結果から，ガイドラインの遵守性が審査される．そのため，本稿記載の成果が貢献できると期待している [16].

参考文献

1. Shibboleth Project, http://shibboleth.internet2.edu (2014. 8.10 参照).

2. 学認, https://www.gakunin.jp/index.php?action=pages_view_main (2014. 8.10 参照).

3. LOA, http://www.nii.ac.jp/service/openforum/setsumeikai2013/?action=common_download_main&upload_id=925 (2014. 08.28 参照）.

4. シングルサインオン, http://itpro.nikkeibp.co.jp/article/Keyword/20131206/523123 (2014. .8.10 参照）.

5. 松浦 健二, 上田 哲史, 佐野 雅彦 : “複数認証基盤に対応する複合SSO環境でのユーザエクスペリエンス,” 学術情報処理研究, Vol. 16, No.16, pp. 138‐145, 2012.

6. Internet2/MACE ‐ Middleware Architecture Committee for Education, http://middleware.internet2.edu/MACE (2014.8. .28 参照).

7. 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構築,” 学術情報処理研究, No. 15, pp. 1‐9, 2006.

8. FPSP. https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158554（2014.8.21 参照）.

9. 西村 健, 中村 素典, 山地 一禎, 佐藤 周行, 大谷 誠, 岡部 寿男, 曽根原 登 : “多様なポリシーを反映可能な認証フェデレーション機構の実現,” 電子情報通信学会論文誌 D, Vol. J96-D, No. 6, pp. 1400‐1412, 2013.

10. Uapplove. https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=13501031（2014.8.21 参照）.

11. 吉冨 健一, 岩沢 和男, 三戸 里美 : “ヘルプデスク解析を応用した学生向けの情報提供,” 学術情報処理研究, Vol. 15, pp. 117‐124, 2011.

12. 学術認証フェデレーションと個人情報, http://www.gakunin.jp/?active_action=repository_view_main_item_detail&page_id=85&block_id=227&item_id=32&item_no=1 （2014. 8.30 参照）.

13. 米国国立衛生研究所, http://nihlibrary.nih.gov/Pages/default.aspx (2014. 8.29 参照）.

14. PubMed, http://www.ncbi.nlm.nih.gov/pubmed?otool=nihlib （2014. 8.29 参照）.

15. 学認アンケート, https://www.gakunin.jp/?active_action=repository_view_main_item_detail&page_id=85&block_id=227&item_id=33&item_no=1 （2014. 8.29 参照）.

16. 河野 圭太, 中村 素典 : “Shibboleth IdPにおけるLoAを考慮した認証方式グループ化機能の開発,” 情報処理学会研究報告, Vol. 2014-IOT-26, No. 2, pp. 1‐6, 2014.