◇◇◇◇◇◇
解　説
◇◇◇◇◇◇

本学における学術認証フェデレーション (学認) に対する取り組み

林　豊洋[1]

1　はじめに

本学は 2011 年 3 月より，電子ジャーナル等の Web アプリケーションに対する学外からの円滑な利用を推進するため，国立情報学研究所が構築する学術認証フェデレーション (学認) へ参加し，利用者向けにサービスを開始しました．

サービス開始からおよそ 5 年が経過し，連携サービス数は開始当初の 3 から 21 に増加しました．また，認証サーバである IdP も，利用者に対する属性送信同意機能の付加 (2013 年)，IdP による属性値の加工を行わない方式 (Trusted DB) の実現 (2014 年)，IdP バージョン 3 系列への移行 (2015 年) 等，学認の推奨する基準に準拠しました．

本稿では，本学における学認への参加から現在に至る取り組みについて，導入当初の経緯，認証システムの構築・機能拡張，提供サービスの追加方針，利用状況を通して解説を行います．

2　学術認証フェデレーション (学認) の概要

電子ジャーナル，電子メールクライアント，e-Learning システム等の研究者・学生向けのサービスや，一部業務システムの Web アプリケーション化が進んでいます．Web アプリケーションは利用環境を選ばずに利用可能であるため，利用者にとってメリットが大きいものの，各種 Web アプリケーションごとに ID 管理を行っていることが多く，その管理コストが問題となります．

利用者にとっても，Web アプリケーションごとにログイン作業が必要となるため，ID 管理・ログインの手順が煩雑となります．加えて，他の学外研究機関で電子ジャーナル等のサービスを利用したい場合，その研究機関がサービスに契約しているにも関わらず，学内 ID を用いた利用は考慮されていないため利用できません．これらの問題を解決するための方法として，それぞれの研究機関が連携し，ユーザ認証を分散化し，多くの学外研究機関で学内 ID を用いたサービスが利用できる枠組み (Shibboleth を活用した認証フェデレーション) が提案されています (図 1，学術認証フェデレーションウェブサイトより転載)．

日本においては，国立情報学研究所によって，学術認証フェデレーション (学認, http://gakunin.jp/) が構築され，平成 22 年度より正式サービスが開始されています．図 1 の通り，学認は，学外からの利用者認証を行うためのシステム (アイデンティティプロバイダ：IdP)，電子ジャーナル等のコンテンツを提供するシステム (サービスプロバイダ：SP) の連携によって構築されています．

[1]情報科学センター　助教　toyohiro@isc.kyutech.ac.jp

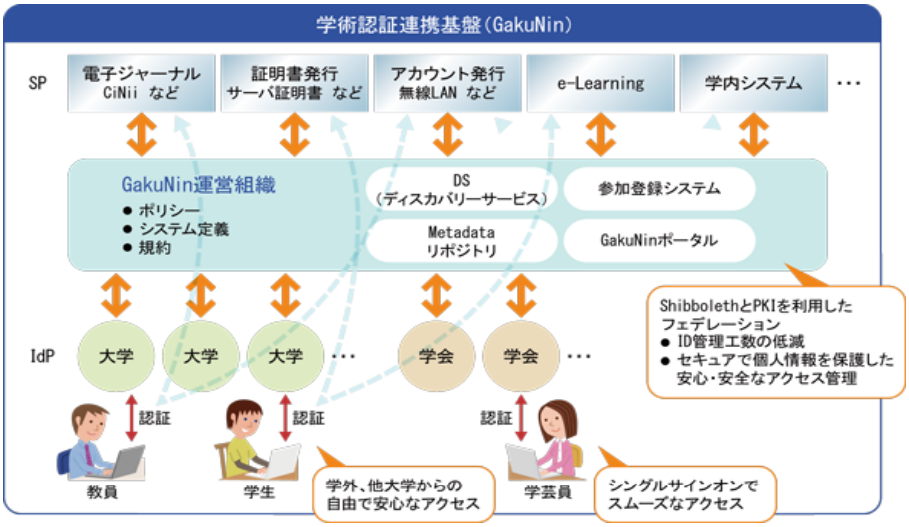

図 1: 学術認証フェデレーションの概要

3　本学における学認参加の経緯

本学は，学認が以下に示す二つの側面

1. 大学の中期目標 (統合認証基盤の活用) との合致
2. 大学構成員対象コンテンツ（電子ジャーナルや学内向けサービス等）の，学外での利用者認証手段としての活用

を有しており，本学にとって大きなメリットをもたらすと判断し，学認への参加を検討しました．

特に，検討を開始した 2010 年当時は，大学構成員対象のコンテンツの公開には，コンテンツにアクセス可能な IP アドレスを限定化する，という方法が主流でした．具体的には，本学が有する IPv4 ネットワークからの接続であれば，本学の構成員からの利用であると認識し，構成員対象コンテンツへのアクセスが許可されます．ただし，この方法では学外からのアクセスは拒否されます．VPN 接続サービスを活用し，学内からのアクセスとして振る舞うことにより制限を回避することも可能ですが，VPN 経由での利用を禁止するコンテンツも存在するため，アクセス元 IP アドレスで大学構成員を識別する手法は適切ではありません．

学認は，学内・学外からのアクセスを問わず，本学の構成員であることをサービスプロバイダに通知することが可能な枠組みであり，利用者認証の問題を解消することが可能です．

3.1　学認導入の方針

上記の通り，学認は統合認証基盤の活用や学外での利用者認証手段として有用です．情報科学センターでは，本学においても学認を導入すべきであると考え，2010 年度後期 (2010 年 10 月) より検証作業を開始し，既存の認証基盤と Shibboleth IdP による認証サーバを構築することにより，導入が可能であることが確認できました．

その後，全学委員会である学術情報委員会に対して学認への参加に関する提案を行い (2010 年 12 月)，その可否の審議がなされました．委員会では，「学外からの学内 ID 認証が実現することは有用である」との意見が主要であり，本学の学認への参加が決定・承認されました．

委員会での参加承認の後，学認テストフェデレーションへ参加し，本学の IdP を利用して学認が利用可能であるかテスト作業を開始しました．テスト作業の結果，学外に構築されたテスト用 SP との属性情報の交換が正しく行えることが確認されました．

この段階で，学認へ正式参加するための準備が全て整った状態となり，学認の正式サービスである運用フェデレーションへの参加申請を行いました．本学の学認への参加に関わる作業が国立情報学研究所によって行われ，2011 年 1 月 25 日に本学 IdP が運用フェデレーションに登録され，本学において学認が利用可能となりました．

4　学認対応の認証システムの構築

学認の利用に関して，本学は学術情報委員会にて，全学統合 ID 管理システムと連携した IdP の設置が承認されました．本節では，学認対応の認証システム構築の概要と，全学統合 ID 管理システムと IdP の連携を行う際に要した，属性情報の対応付けに関する対処策について解説します．

4.1　認証システムの概要 (導入当初)

学認対応の認証システムとして，本学の利用者情報を管理する全学統合 ID 管理システム，全学統合 ID 管理システムと連携した LDAP サーバ，LDAP サーバから LDAP 属性情報を受け，学認に対応した属性情報の生成と利用者認証を行う IdP サーバを構成しました．導入当初の認証システムの概要を図 2 に示します．

図 2: 学認対応の認証システムの概要 (2011 年〜2013 年)

導入当初は，LDAP サーバとして情報科学センター教育システム向け LDAP サーバ，IdP サーバとして Shibboleth Identity Provider Software ver.2 系列を用いていました．Shibboleth Identity Provider Software を用いた IdP サーバの構築には，HTTP インタフェースとして Apache，ミドルウェアとして Tomcat(および Tomcat を動作させるための Java) を要します．加えて，IdP の設定を行うためのコンフィグレーションは多数の設定ファイル (XML 形式) を本学の構成に合わせて変更する必要があります．

一見自己構築が難しく感じますが，学術認証フェデレーションを主導する国立情報学研究所が，詳細な構築手順を示した学認技術ガイド (`https://www.gakunin.jp/docs/fed/technical/idp/install/idpInst1`) を公開しています．本学では学認技術ガイドの手順に従い構築を行ったところ，大きなトラブルもなく IdP の構築を行うことができました．

IdP は，SP が要求する Shibboleth 属性情報を利用者毎に生成し，SP へ返答する必要があります．利用者に依存しない属性情報 (機関名など) は，IdP サーバ単体で生成することが可能です．利用者毎に異なる属性情報は，LDAP サーバからの参照が望ましい構成となります．学認導入に関する技術検証時に，全学統合 ID 管理システムが持つ属性情報と Shibboleth 属性情報の対応関係を調査した結果，大半の情報は無加工で利用できることがわかりました．

しかし，導入当初用いた情報科学センター教育システム向け LDAP サーバは，学認導入を想定しておらず，利用者の職種が参照できない状況でした．具体的には，利用者の職種を表す情報が，Shibboleth では文字列 (eduPersonAffiliation，値：faculty, staff, student) であることに対し，教育システム向け LDAP サーバでは整数値 (グループ ID，値の例： 教員 1000, 職員 2000 or 2001, 学生 3000) で表現されていました．この問題への対処として，学認技術ガイド内の,「IdP のコンフィグレーションファイル (attribute-resolver.xml) 内に読み替え規則を記述し対処する手法 (大阪大学での事例，既存システムへの変更点を最小限にしたまま eduPerson 形式での属性受け渡しの実現方法：`https://www.gakunin.jp/docs/fed/feasibility/report/osaka/append1`)」を適用し，利用者の職種を生成することが可能となりました．

4.2 利用者への属性送信同意機能の付加 (2013 年)

Shibboleth では，サービス利用可否の判断のため，SP 毎に異なる属性値を要求することが可能です．Shibboleth IdP バージョン 2 系列の標準では，IdP が SP にどのような属性値を送信する設定であるか，利用者は知ることが出来ません．これは,「利用者に属性値の送信に対する同意を得ていない」と解釈でき，運用上問題となり得ます．

この問題に対応するため，属性送信同意機能を付加するプラグインとして，uApprove が開発され，機能強化・日本語化がなされた uApprove.jp が公開されています (図 3)．

図 3: 属性送信同意機能 (uApprove.jp ユーザーマニュアルより転載)

本学では，2013 年に uApprove.jp プラグインを付加し，利用者に属性値送信の同意を得ることが可能となりました．また，uApprove.jp は，利用者が認証を行った SP と日時に関するログをデータベース

(RDB) に保存する設計であるため，SP へのアクセスログ取得機能としても用いることが可能です．

4.3 Trusted DB の実現 (2014 年)

前述のとおり，導入当初は IdP に利用者の属性情報を提供する LDAP サーバが，学認を想定した設計ではありませんでした．従って，一部の属性値を IdP サーバ内で生成し，運用を開始しました．学認で用いる IdP の運用ポリシーは「学術認証フェデレーション実施要領およびシステム運用基準」として定められています．運用ポリシーでは，利用者の属性値は上流の信頼性のある情報のみを用いて提供すべきである，とされています．信頼性を有するデータベースについて，学認では「Trusted DB」と呼んでいます．

本学においても，Trusted DB の実現を検討する必要がありました．検討を進めている同時期に，全学統合 ID 管理システムが次期システム（第二期）に更新されることとなりました．次期システムでは，従来のシステムと比較して，利用者情報として多様な属性値を容易に定義することが可能となりました．この特性を活用し，IdP 専用の LDAP サーバを設置し，全学統合 ID 管理システムが Shibboleth 属性値と無加工で対応できる LDAP 属性値を伝搬する設計を行いました (図 4)．

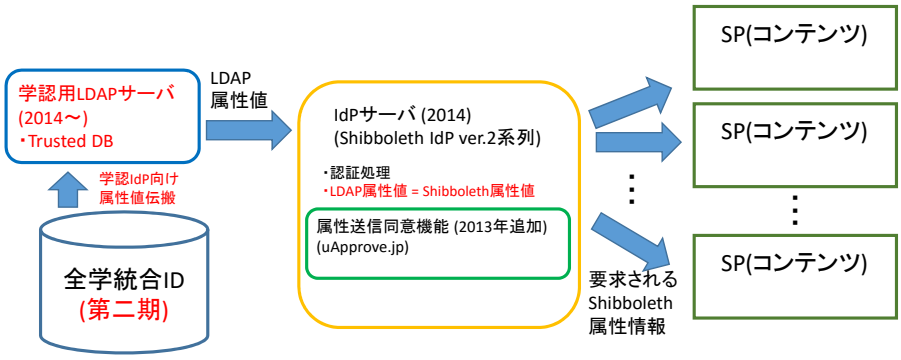

図 4: 学認対応の認証システムの概要 (2014 年)

本設計により，IdP サーバは LDAP 属性から Shibboleth 属性値を生成することなく，学認が推奨する Trusted DB が実現できました．

4.4 Shibboleth IdP バージョン 3 系列の導入 (2015 年)

本学では，学認への参加当初から，IdP サーバを Shibboleth IdP バージョン 2 系列により自己構築を行い，運用を継続してきました．2014 年に Shibboleth IdP のバージョンが 3 系列に更新され，バージョン 2 系列の新規開発が停止・2016 年 7 月末にサポートを含めて完全に対応を終えることが発表されました．この発表に基づき，学認においても，Shibboleth IdP を用いる機関に対して，バージョン 3 系列への更新依頼がなされました．

本学でバージョン 3 系列の動作検証を行った結果，バージョン 3.1(2015 年 11 月以前バージョン) 以前では，電子ジャーナルを提供する SpringerLink に対する認証が行えないことが判明しました．更に調査を進めた結果，IdP の機能が不十分であることが原因であり，バージョン 3.2 より認証可能であることがわかりました．バージョン 3.2 がリリースされた 2015 年 11 月末に再検証を行った結果，SpringerLink への認証が行えることが確認できたため，2015 年 12 月末に更新を完了しました (図 5)．

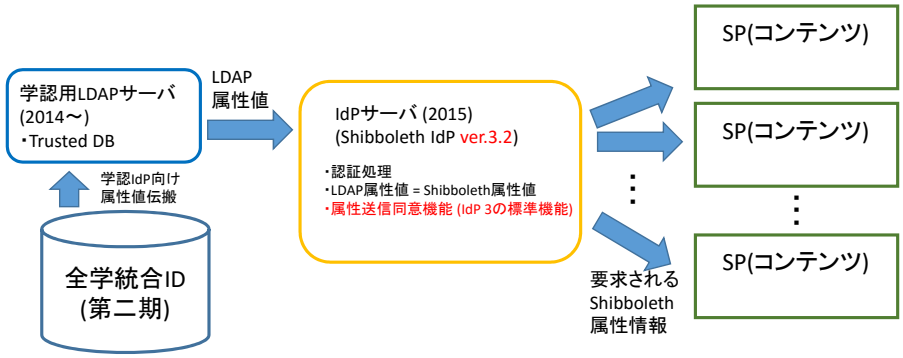

図 5: 学認対応の認証システムの概要 (2015 年)

更新後目立った不具合は発生していませんが，利用者への送信同意機能が uApprove.jp と比較して不便であること，データベースにアクセスログが保存されないこと等の問題があります[2].

5　利用者へのサービス提供

本節では，本学における IdP と連携する SP の選定基準・IdP への追加まで流れおよび提供中のサービスプロバイダについて示します.

学認への参加当初は,「SP に詳細な個人情報が伝播しないこと」,「利用者への利便性が高いもの」を基準として，情報科学センターが試行的に 3 つの電子ジャーナル (CiNII，Science Direct，SpringerLink) を選定しました.

その後，以下の手順に基づき，IdP と連携する SP を追加することとなりました.

1. 追加を希望する部局が学術情報委員会での審議を依頼する．承認後，IdP との連携設定を行う
2. ただし，SP が要求する属性値が連携済みであれば，学術情報委員会への報告のみで良い

2015 年度末時点における，本学の IdP による認証処理を経て利用可能なサービスプロバイダは表 1 の通りです．利用可能なサービスプロバイダは，導入当初は 3 サービスのみでしたが，その後純増しており，2015 年度末時点では 21 サービスとなりました.

5.1　利用状況

本学の IdP による認証処理を経た各サービスプロバイダの利用状況を示します．uApprove.jp の導入を行った 2013 年 3 月より利用状況の記録が可能となったため，本節における統計取得期間は 2013 年 3 月～2015 年 12 月の期間となります.

IdP による認証処理を行った利用者数 (ユニークユーザ数) は 4416 名，SP へのアクセス数は 27,840 を示しました．各サービスプロバイダの利用割合を図 6 に示します.

利用割合が示す通り，本学においては，学内サービスであるオンラインガイドや教育システム WWW サイトの学外からの閲覧を目的とした IdP の利用が大半を占めているといえます．また，eduroam の一時アカウントの発行のための利用も多い状況です．本来想定した利用手段である電子ジャーナルの認証処理にも用いられており，多岐なサービスで IdP が用いられています.

[2]IdP バージョン 3 系列で uApprove.jp 相当の送信同意機能の実現について，現在国立情報学研究所が調査を進めています.

表 1: 本学 IdP と連携するサービスプロバイダ (2015 年度末時点)

サービス名	用途	提供開始時期
CiNII	電子ジャーナル	2011 年 3 月
Science Direct	電子ジャーナル	2011 年 3 月
SpringerLink	電子ジャーナル	2011 年 3 月
eduroam-shib	学外サービス	2011 年 6 月
Web of Knowledge	電子ジャーナル	2011 年 7 月
Fshare	学外サービス	2011 年 12 月
FaMCUs	学外サービス	2011 年 12 月
DreamSpark	学外サービス	2011 年 12 月
EBSCO host	電子ジャーナル	2012 年 10 月
IOPscience	電子ジャーナル	2012 年 10 月
IEEE Xplore	電子ジャーナル	2012 年 10 月
ISC オンラインガイド	学内向けコンテンツ	2012 年 12 月
ISC 教育システム WWW（戸畑・飯塚）	学内向けコンテンツ	2012 年 12 月
ProQuest	電子ジャーナル	2013 年 3 月
Nature	電子ジャーナル	2013 年 3 月
WILEY ONLINE LIBRARY	電子ジャーナル	2014 年 3 月
JapanKnowledge Web	電子ジャーナル	2014 年 10 月
Maruzen eBook Library	電子ジャーナル	2015 年 1 月
豊橋技科大 LMS	単位互換	2015 年 3 月
学認連携 Moodle	学外サービス	2016 年 1 月

なお，運用を開始した 2011 年当時は，一日あたりのアクセス数が 2 程度とほぼない状況であり，学認への参加が有効であったか判断が難しい利用率と言えました．運用から 5 年が経過し，一日あたりのアクセス数は平均で 30 程度となり，利用率が 10 倍に向上しています．

6 まとめ

本稿では，学術認証フェデレーション (学認) の概要，本学における学認参加までの経緯，認証システムの構築・機能拡張等，利用者へ提供するサービスプロバイダの推移，利用状況について解説を行いました．

学認参加へ向けた検討を開始した 2010 年末から 5 年が経過し，利用可能なサービスプロバイダは電子ジャーナル，学外サービス，学内コンテンツ，単位互換向け LMS と多岐にわたります．利用者も，開始当初の 10 倍に向上しています．認証システムも，送信同意機能の付加，全学統合 ID 管理システムの更新に合わせた Trusted DB の実現，IdP バージョン 3 への更新など，学認 IdP 運用ポリシーに準拠したものとなりました．

今後も多くのサービスプロバイダを追加し，更に便利な認証基盤として整備する予定です．学認の利用方法に関する質問やご意見・ご要望がありましたら，support@isc.kyutech.ac.jp までお気軽にお問い合わせください．

2010 年 10 月 検証作業の開始 (学内テスト IdP, SP 構築)

2010 年 12 月 本学学術情報委員会にて参加承認 (Shibboleth IdP の導入)

2011 年 1 月 4 日 テストフェデレーション参加・テスト作業の開始

2011 年 1 月 7 日 運用フェデレーションへの参加申請

2011 年 1 月 25 日 運用フェデレーションへの登録・学認が利用可能となる

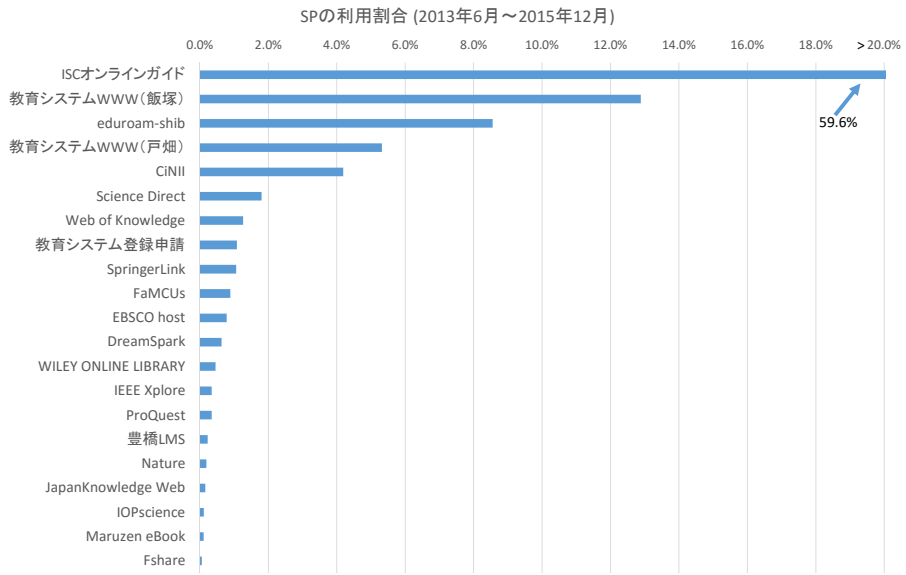

図 6: 各サービスプロバイダの利用割合

2011 年 3 月 CiNII, Science Direct, SpringerLink の追加 (利用者へのサービス提供開始)

2011 年 6 月 eduroam-shib の追加 (本学の eduroam への参加に伴う措置)

2011 年 7 月 Web of Knowledge の追加 (附属図書館からの依頼に基づく追加)

2011 年 12 月 Fshare, FaMCUs, DreamSpark の追加 (学認の更なる利用促進のための措置)

2012 年 10 月 EBCSO host，IOPscience，IEEE Xplore の追加（附属図書館からの依頼に基づく追加）

2012 年 12 月 情報科学センターオンラインガイド，教育システム Web サイト（戸畑・飯塚），サービス登録申請サイトの追加

2013 年 3 月 ProQuest の追加（附属図書館からの依頼に基づく追加）

2013 年 3 月 Nature の追加（附属図書館からの依頼に基づく追加）

2013 年 3 月 Shibboleth IdP に属性送信同意機能 (uApprove.jp) 追加

2014 年 3 月 WILEY ONLINE LIBRARY の追加（附属図書館からの依頼に基づく追加）

2014 年 3 月 全学統合 ID 管理システム更新に合わせ，統合 ID からの学認属性値の配信開始 (Trusted DB の実現)

2014 年 10 月 JapanKnowledge Web の追加（附属図書館からの依頼に基づく追加）

2015 年 1 月 Maruzen eBook Library の追加（附属図書館からの依頼に基づく追加）

2015 年 3 月 豊橋技科大との単位互換 LMS の追加（本学事務局からの依頼に基づく追加）

2015 年 12 月 Shibboleth IdP 3.2 への更新

2016 年 1 月 学認連携 Moodle（国立情報学研究所）の追加（情報セキュリティポリシー策定専門部会からの依頼に基づく追加）

参考文献

[1] 林豊洋，本学における学術認証フェデレーション (学認) の導入について，九州工業大学情報科学センター広報第 24 号，pp.23–33，`http://www.isc.kyutech.ac.jp/kouhou/kouho24/pdf/kaisetu4.pdf`，2012.