【TOPIC】

学術認証フェデレーションについて

神戸大学 情報基盤センター 学術認証フェデレーション担当チーム

1 はじめに

本稿では，国立情報学研究所 (NII) の **学認** [*1] と連携することにより，神戸大学情報基盤センターで提供している**学術認証フェデレーション** について，技術的な内容を中心に概要を説明する．具体的な利用方法などについては情報基盤センターのホームページ中の以下を参照されたい．

- http://www.istc.kobe-u.ac.jp/services/StandardService/fed

学認は，Web アプリケーションへの組織を超えた **シングル・サイン・オン** (SSO) を実現している．すなわち，神戸大学の学生や教職員は，情報基盤センターで発行しているログイン ID とパスワードにより一旦ログインすれば，その後は学認で提供されている外部 Web サービス (各種電子ジャーナルサイトなど) に対し，いちいちログインせずに自由に利用できる．また，その際，利用者のパスワードなど秘匿性の高い個人情報は，外部 Web サーバーに渡されることはなく，安全性が保たれている．

このように，学認のサービスは，利便性と安全性を両立させた優れた利点を持っている．以下では，学認の概要について述べた後，シングル・サイン・オンを実現する技術であるシボレスと認証フェデレーションについて説明し，最後に神戸大学から利用できるサービスを示す．

なお，情報基盤センターでは学内 Web サービスに対するシングル・サイン・オンを実現するため，同様の技術を用いて **認証フェデレーション** Knossos を提供しているが，本稿では対象としない．

2 学認の概要

学認は，米国の高等教育機関の IT 組織による団体である EDUCAUSE によって 2000 年に開発された**シボレス** (Shibboleth) [*2] ソフトウェアを利用した学術認証フェデーレーションと呼ばれる仕組みに基づいている．日本以外では，欧米を中心に 17 カ国で学術認証フェデレーションが運用されており，学認は日本における対応組織となる [2].

学認は，図 1 に示すように，2009 年から試行運用，2010 年から本格運用が開始されている．2014 年 5 月末の時点で，大学を中心に 130 以上の機関が学認に登録されており，また海外を含め利用できる外部 Web サービスは 50 以上である[*3]．今後も登録機関および外部 Web サービスの数は，順調に増大すると考えられる．

[*1] http://www.gakunin.jp
[*2] http://shibboleth.internet2.edu
[*3] 神戸大学との契約等が必要な場合があり，すべてのサービスを神戸大学から利用できるわけではない．

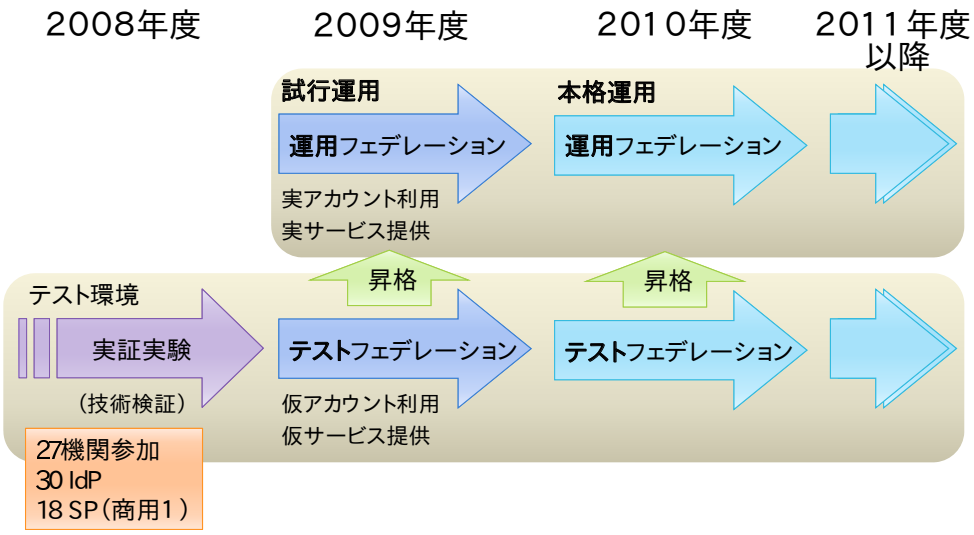

図 1　学認の歩み ([3] より引用)

3　シボレスと認証フェデレーション

シボレスのシステムには，**IdP** (ID Provider), **SP** (Service Provider) そして **DS** (Discovery Service) と呼ばれる 3 種類のサーバーが存在している．IdP は利用者の所属している組織に存在し，利用者の認証を行う．SP は各種のサービスを提供するサーバーであり，IdP から送信される利用者の情報 (**属性** と呼ばれる) を参照することにより，利用者毎のサービスを提供することが可能になる．DS は IdP を検索するサーバーである．

多数の IdP と SP をスムーズに連携させるための仕組みを **フェデレーション** と呼ぶ．具体的には，運用ポリシーの策定，参加機関の承認，DS の運用，IdP と SP が交換する属性情報の決定，メタデータの交換方法の提供などが必要である [4].

シボレスでの認証の流れは図 2 のようになる [4].

1. 利用者は SP の Web サーバーにアクセスする
2. 「シボレスログイン」等のボタンをクリックする
3. DS により，所属機関を選択する画面が表示される
4. 所属機関を選択する
5. 所属機関の IdP のページが表示され，ID とパスワードを入力する
6. 認証できた場合，IdP は SP に必要な属性を通知する
7. SP の Web ページに自動的に遷移する

所属機関の IdP での認証が一旦成功すれば，Web ブラウザを終了させない限り，他の SP であってもログインせずに利用可能である．すなわちシングル・サイン・オンが実現できている．

IdP から SP に渡される属性一覧を表 1 に示す [1]．また，どのような内容が渡されるかは，以下のサイトにログインすると確認できる．

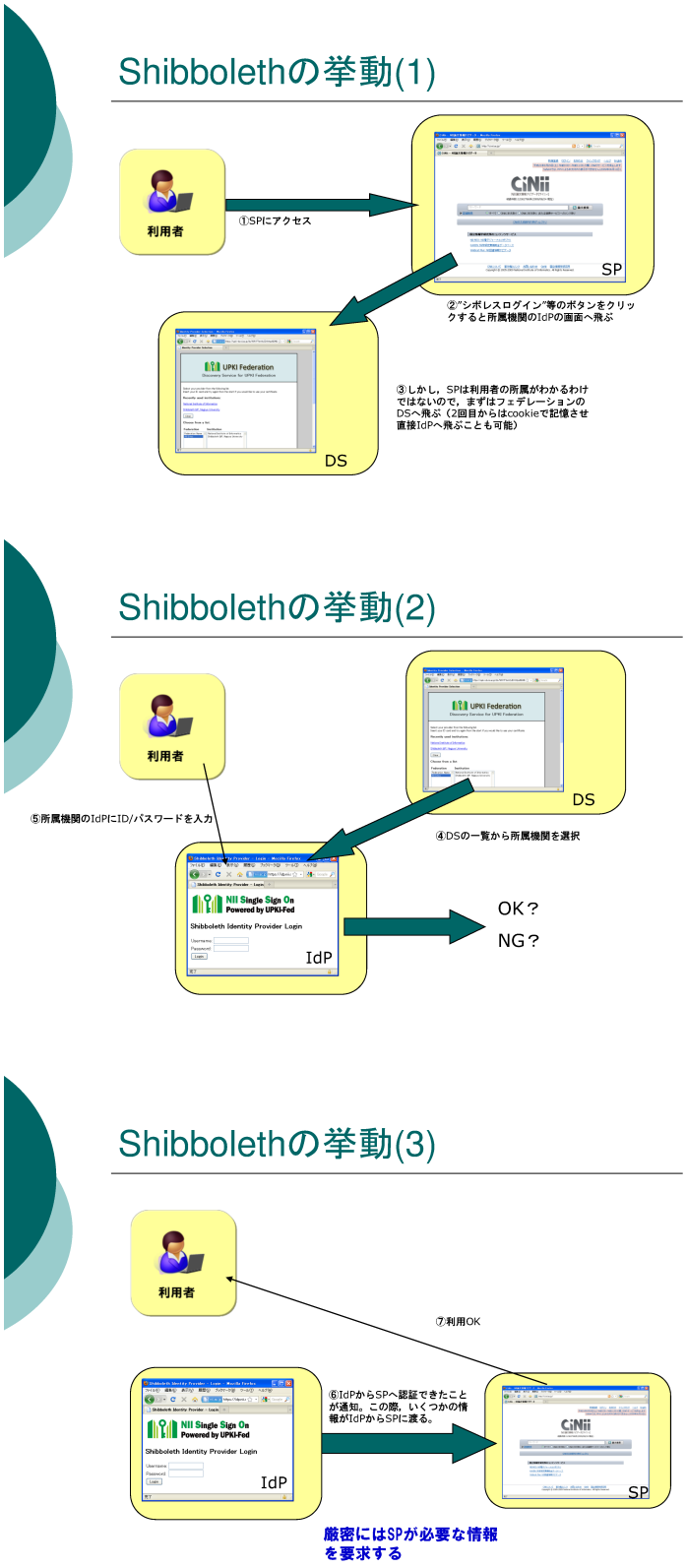

図 2　シボレスでの認証の流れ ([4] より引用)

表 1　学認の属性一覧

属性名	説明	神戸大学での例
organizationName	組織名称 (英語)	kobe-u
jaOrganizationName	組織名称 (日本語)	神戸大学
organizationalUnitName	組織内所属名称 (英語)	X00000Y00000Z00000
jaOrganizationalUnitName	組織内所属名称 (日本語)	X00000Y00000Z00000
eduPersonPrincipalName	フェデレーション内のエンティティ	999999@kobe-u.ac.jp
eduPersonTargetedID	フェデレーション内の匿名エンティティ	https://fed.center.kobe-u.ac.jp/...
eduPersonAffiliation	利用者の職種等	staff;faculty
eduPersonScopedAffiliation	利用者の組織内での職種等	staff@kobe-u.ac.jp;faculty@kobe-u.ac.jp
eduPersonEntitlement	利用資格情報	urn:mace:dir:entitlement:common-lib-terms
surName	姓 (英語)	Kobe
jaSurName	姓 (日本語)	神戸
givenName	名 (英語)	Taro
jaGivenName	名 (日本語)	太郎
displayName	表示用氏名 (英語)	Kobe Taro
jaDisplayName	表示用氏名 (日本語)	神戸　太郎
mail	電子メール	kobetaro@kobe-u.ac.jp
gakuninScopedPersonalUniqueCode	職員番号・学籍番号	使用していない
isMemberOf	所属するグループ名	使用していない

- https://attrviewer20.gakunin.nii.ac.jp

ただし，実際に SP に渡すのはこれらの属性のごく一部である．たとえば神戸大学の IdP から CiNii に渡しているのは organizationName, jaOrganizationName, eduPersonTargetedID だけである．eduPersonTargetedID は，SP において利用者を識別する情報として利用されているが，その値はランダムな文字列であり，SP がその情報だけから個人を特定することはほぼ不可能である．ただし，SP が givenName や mail を要求する場合，そのような SP においては個人を特定できることに注意する必要がある．各 SP にどのような属性が渡されているかは以下のページで確認できるので，利用の参考にされたい．

- http://www.gakunin.jp/participants/

なお IdP から SP への通信経路上は，通信内容は暗号化され秘匿されている．このように，認証フェデレーションでは，個人情報をできるだけ秘匿したままで利用者の利便性を高める工夫がなされている．

4　神戸大学から利用できるサービス

神戸大学は KAISER 2010 の構築に合わせて 2011 年度から学認に参加している．当初は CiNii など数件の SP が利用できるだけであったが，徐々に設定を進め，2014 年 5 月末の時点で 17 件の SP が利用可能になっている．表 2 にその一覧を示す．

5 おわりに

本稿では，組織間をまたがったシングル・サイン・オンを実現する学認について概要を説明した．学認で採用されているシボレスおよび認証フェデレーションの仕組みは，利便性と安全性を両立させた優れた利点を持っている．したがって，今後さらに IdP や SP の数は増大するものと考えられる．情報基盤センターとしても対応する SP を増やし，利用者の利便性を高めたいと考えている．なお，多くの SP は電子ジャーナル等のサイトであり，附属図書館情報管理課情報システム係の協力なしには実現できなかったものである．ここに協力していただいた担当者の方々に心から謝意を評したい．

最後に学術認証フェデレーション担当チームのメンバーを示す (あいうえお順).

- 飯塚 由子
- 角田 美穂
- 北内 一行
- 宋 剛秀
- 田村 直之
- 中嶋 祥子
- 伴 好弘

参考文献

[1] 国立情報学研究所. 学認技術運用基準 (v2.0). http://www.gakunin.jp/join/production/, 2013.

[2] 国立情報学研究所学術認証運営委員会. 学認実施要領 (v1.0). http://www.gakunin.jp/join/production/, 2013.

[3] 大谷誠. Shibboleth, 学認を知ろう. 国立情報学研究所, 2011.

[4] 樋口秀樹. シングルサインオンの基礎知識 〜shibboleth の概要〜. 国立情報学研究所, 2009.

表 2　神戸大学で利用できる SP 一覧

SP 名	説明
Microsoft DreamSpark	Microsoft 社のプロ用の開発・デザインツールを無償でダウンロードできるサービスを利用するための DreamSpark アカウントを取得するサービス
Eduroam-Shib	世界的な学術無線 LAN ローミング基盤である eduroam を利用するための eduroam アカウントを取得するサービス
CiNii	NII 論文検索
KOD	研究社の英和・和英辞典や用例辞典，三省堂の大辞林などを一括検索できるオンライン辞書
SpringerLink	Springer 社の雑誌約 1900 誌が利用できるフルテキストデータベース
EBSCO host	「Business Source Premier」や「Econlit」などの横断検索ができるオンラインデータベース
OvidSP	医学・薬学・保健衛生分野を中心に，各種データベース・電子ジャーナル・電子ブックなどを提供
Cambridge Journals Online	Cambridge University Press 発行の電子ジャーナル 200 誌以上が利用可能
RSC Publishing	化学分野における重要なピアレビュー誌を発行する英国王立化学会のサイト
ScienceDirect	Elsevier 社の雑誌 2000 誌以上が利用できるフルテキストデータベース
Web of Knowledge	分野別の学術文献・引用索引データベース、雑誌評価ツールなどを提供する web プラットフォーム
EndNote Web	Web 版の文献管理ツール
Emerald	「Emerald Management eJournals 200(EMeJ200)」に含まれる雑誌約 200 誌が概ね 1994 年から、「Emerald Backfiles」に含まれる 120 誌以上が初号から概ね 1994 年まで利用可能
NII REO	複数の出版社の電子リソースを NII がホスティングして提供．神戸大学では電子ジャーナルアーカイブとして Oxford University Press, Kluwer，Springer が，人文科学系電子コレクションでは 19,20 世紀の HCCP（英国下院議会文書），MOMW-I（15 世紀半ばから 1850 年までの主として経済史・経営史・社会思想史関係の書籍や定期刊行物を収録）の双方が利用可能
IOP Science	英国物理学会の雑誌約 50 誌の最新年分と過去 10 年分が利用可能
Nature Publishing Group	『Nature』(1869 年の創刊号から最新号) を含む 26 誌が利用可能
John Wiley & Sons	Wiley-Blackwell 社発行の雑誌 1400 誌が概ね 1997 年から利用可能