◇◇◇◇◇
解説
◇◇◇◇◇

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

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.

本稿では，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手法，利用者向けに提供するサービスの選定，利用者へ提供するサービスの概要 (2011 年度末時点) 等について解説します.

2　学術認証フェデレーション (学認) の概要

近年，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 (IdP)，電子ジャーナル等のサービスを提供するシステム (SP) の連携によって構築されています．学認は正式サービスの運用から 2 年弱と，まだまだ歴史の浅い基盤ですが，参加する IdP および SP は月単位で増加しており，今後の更なる利便性の向上が期待できます.

3　本学における学認参加の経緯

本学が学認への参加に至った経緯は，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

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

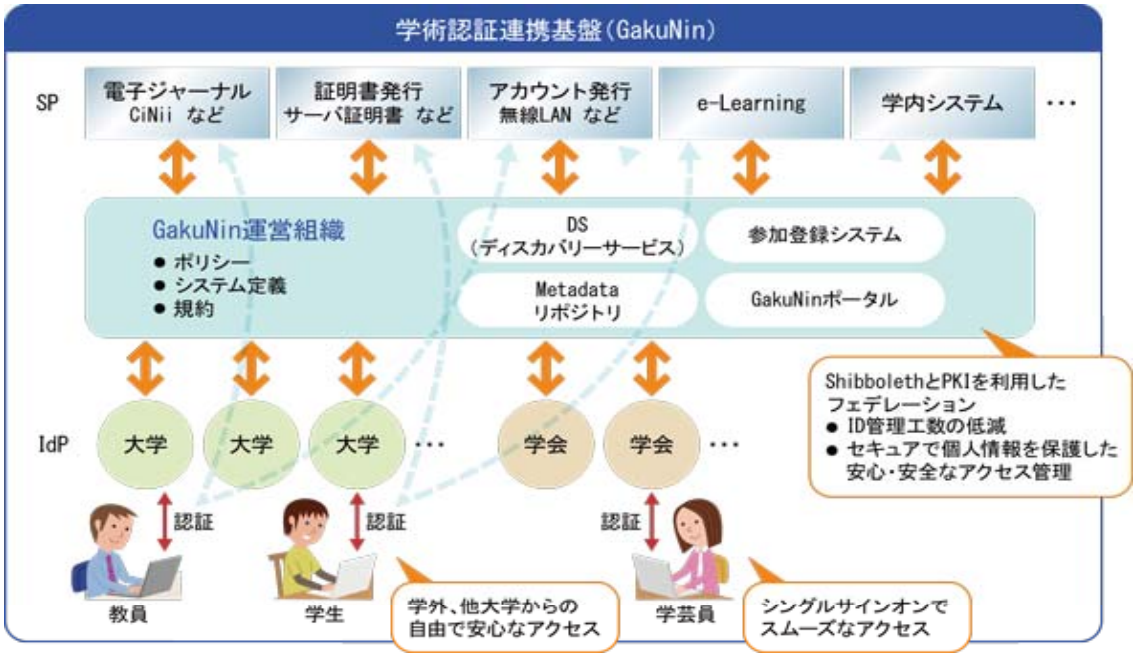


図 1: 学術認証フェデレーション概要

2. 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たためです.

3.1 本学中期目標 (統合認証基盤の活用) との合致

現在，国立大学法人では，教育研究等の質の向上を目的とした目標と計画の策定と実行が定められています．本学においても，目標と計画が定められており，現在は第 2 期中期目標（平成 22〜27 年度）を実施しています．この中期目標の中には，情報システムを活用した教育研究等の質の向上を目的とした計画が含まれており，これを達成するため，情報科学センターでは主に統合認証基盤の整備を担っています.

全学統合 ID 管理システムの導入

2009 年度に全学統合 ID 管理システムの導入と運用を開始しました (図 2).

全学統合 ID 管理システムは，利用者情報を管理する ID データベース部と，各情報システムとの間で利用者情報の転送制御を行うシステム間連係部から構成されています．ID データベース部には利用者のアカウント情報を保存するための RDBMS システム (Oracle DB) を採用し，システム間連携部には，各部局のアカウント管理システムへ情報を伝搬するため，Sun Identity Manager (導入当時の製品名) を採用しています．各部局に設置された情報システムは，全学統合 ID 管理システムとのアカウント連携インタフェースを準備することにより，アカウント情報の統合が実現できます.

統合 ID を用いた利便性の高いサービス = 学認の導入

全学統合 ID 管理システムの整備が行われたため，今後は利用者にとって利便性の高い情報システム・サービスを統一的な ID 体系で提供することが重要であると考えられます．特に，学生や教員が効率的

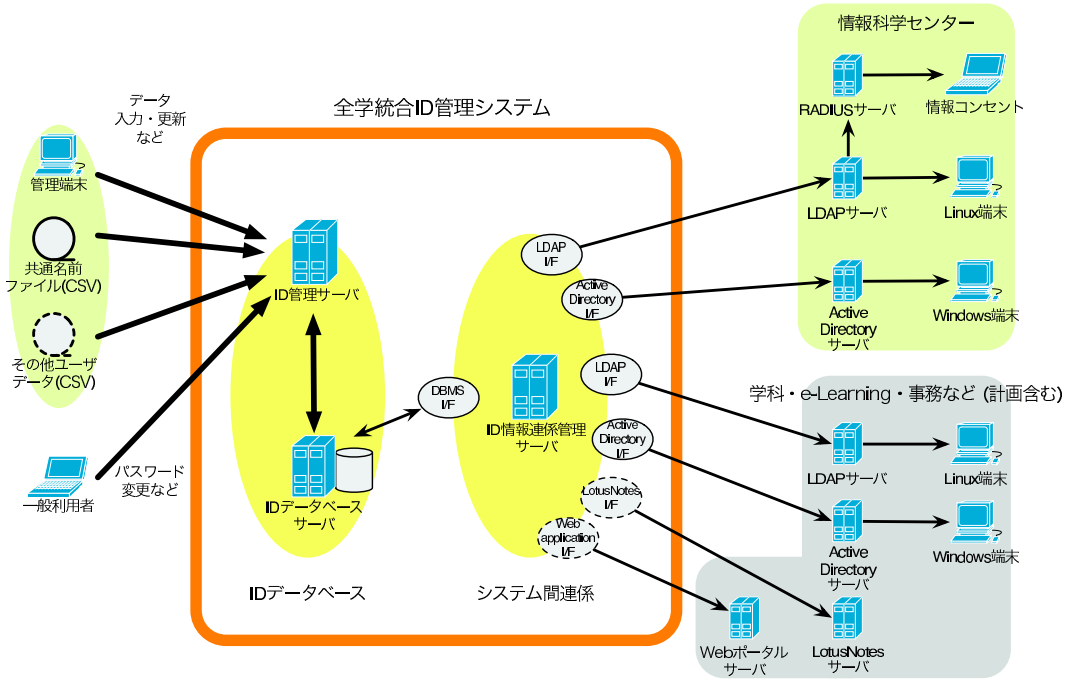


図 2: 全学統合 ID 管理システム構成の概要

な研究の遂行を目的として多く利用する，電子ジャーナルやポータルサイト等の情報システムに対して統合 ID が利用できれば，利便性は大きく向上します．

学認の導入は，この観点から最適であると考えられます．学認が利用者認証に用いる IdP サーバは，アカウント情報の照会を行うバックエンドとして，LDAP サーバを利用することが可能です．情報科学センターは，全学統合 ID 管理システムと連携した LDAP サーバを有しているため，統合 ID を用いた各種情報システムに対する利用者認証が実現できます．また，情報システムを提供する SP には，本学図書館が契約を行っている電子ジャーナルをはじめ，eduroam の仮名アカウント発行サービス，ファイル転送サービス，ソフトウェアのダウンロードサービスなど，研究に有用なシステムが多数整備されています．学認を導入することにより，統合 ID を用いてこれらのサービスを利用できるため，本学の利用者にとって有用であると考えられます．

3.2 学外での利用認証手段としての活用

前節で述べたとおり，学生や教員は効率的に研究を遂行するため，電子ジャーナルサービスによる論文の検索および取得を行うことが恒常化しています．本学では，附属図書館が電子ジャーナルの契約や管理を一括して行っており，現在 10 種類の電子ジャーナルサービスを利用することができます．

電子ジャーナルサービスとの契約は，大学単位で行われるため，多くのサービスがアクセス制限を設けています．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，本学の利用者であると認識し，電子ジャーナルサービスへのアクセスが許可されます．このアクセス制限は合理的であると言えますが，学外からの電子ジャーナルへのアクセスは拒否されます．教員や大学院生は，自宅などの学外から電子ジャーナルを利用する機会が多いため，この制限は問題となります．

この問題に対応するため，本学では戸畑と飯塚の両キャンパスに VPN サーバ (Nortel Network 社 Contivity 1700) を整備し，2003 年度より VPN(PPTP) 接続サービスの提供を開始しました．VPN 接続サービスを利用することにより，利用者は学外ネットワークを経由し，学内ネットワークへ接続することが

可能となります．加えて，対外ネットワークへの接続も学内ネットワークからの接続と認識されるため，学外からの電子ジャーナルサービスへのアクセスが可能となりました (図 3).

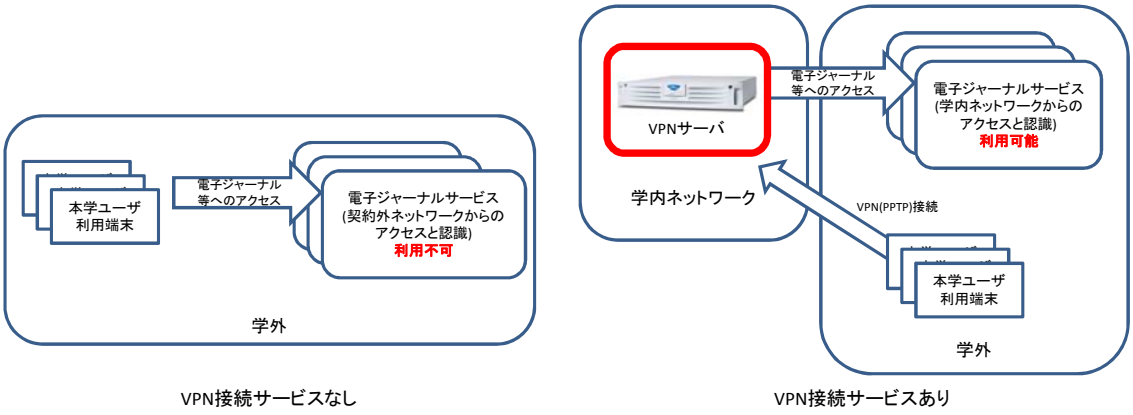


図 3: VPN 接続サービスを用いた電子ジャーナルの利用

しかし，近年は VPN 接続サービスに関して種々の問題が発生しています．特に，以下の 2 点が主要な問題となりました．

1. **VPN サーバの経年による問題**
   VPN 接続サービス提供のため導入された Contivity 1700 は，運用開始から 8 年以上が経過しており，機器の保守サービスが打ち切りとなりました．機材の経年も進行したため，機材トラブルによるサービスの停止が頻発し，サービスの安定した提供が困難となりました．新たな VPN サーバへ機材更新を行い，サービスを継続する方針が考えられますが，Contivity 1700 には

   - 多数の接続や様々な OS に対して，安定したサービスが提供可能 (同時接続が増えるとサービスが停止する機材や，利用する OS に制約のある機材が存在します)
   - 接続先を制限する ACL にホスト名が指定可能 (多くの機材は IP アドレス，ネットワークアドレスのみが指定可能)

   等の利点があり，電子ジャーナルサービス向けの有力な後継機種は少ないといえます．

2. **VPN 接続サービスを経由したインシデントの発生**
   近年，計算機を利用した様々なインシデントが発生し，問題となっています．特に，ネットワークを利用したファイル共有ソフトは容易にインストールでき，利用方法も容易であるため，多くの利用例・インシデントが存在します．本学の VPN サービスへ接続したままファイル共有ソフトを利用した場合，接続経路は学内ネットワーク経由となるため，この行為は本学から発生したセキュリティインシデントとなります．

   VPN 接続サービスを経由したファイル共有ソフトの利用例は数件存在し，セキュリティポリシー遵守の観点から好ましくない状況となっています．この問題に対処するため，VPN 接続サービスからの学外接続を原則不許可とし，電子ジャーナルサービスへの接続は特例として許可する方針も検討対象となりましたが，コンテンツ検索・閲覧時の負荷分散のため，ホスト名や IP アドレスが一意でないことが多く，対処は難しいといえます．

3.3 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，非常に高い親和性を有しているといえます．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，センター内にて IdP,SP を構築し，2010 年度後期 (2010 年 10 月) より検証作業を開始しました．検証作業の結果，全学統合 ID 管理システムと学認向け IdP の連携が可能であることが明らかになりました．

学認を導入するための技術的な課題は達成できたため，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ったため，以下に示す条件

- 全学統合 ID 管理システムと連携した IdP の設置許可
- 学外 SP への詳細な情報公開を避けるため，個人情報に関しては以下の属性送信を許可
  - eduPersonTargetedID (ユーザ名，組織名のハッシュ文字列)
  - eduPersonAffiliation (職種)
  - eduPersonScopedAffiliation (組織名付き職種, 2011 年 7 月追加承認)

のもと，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．

上述した学認参加までの主要なスケジュールを以下に示します．

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

2010 年 12 月 21 日 本学学術情報委員会にて参加承認 (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

本学では，学認の導入に関わる技術検証の開始から運用開始まで，3ヶ月弱の期間で達成できました．これは，国立情報学研究所が整備する学認の環境構築マニュアルが充実しており，技術検証を行うためのテスト環境の構築が非常に良好であったことと (IdP の構築については 4 節にて解説します)，学認の有用性に対して，本学の理事の理解が高く，委員会での承認を短期間にて得たことが理由となります．

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 認証システム構築の概要

学認対応の認証システムは，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マスター 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 Shibboleth 属性情報の生成と利用者認証を行う IdP サーバによって構築されます．認証システムの概要を図 4 に示します．

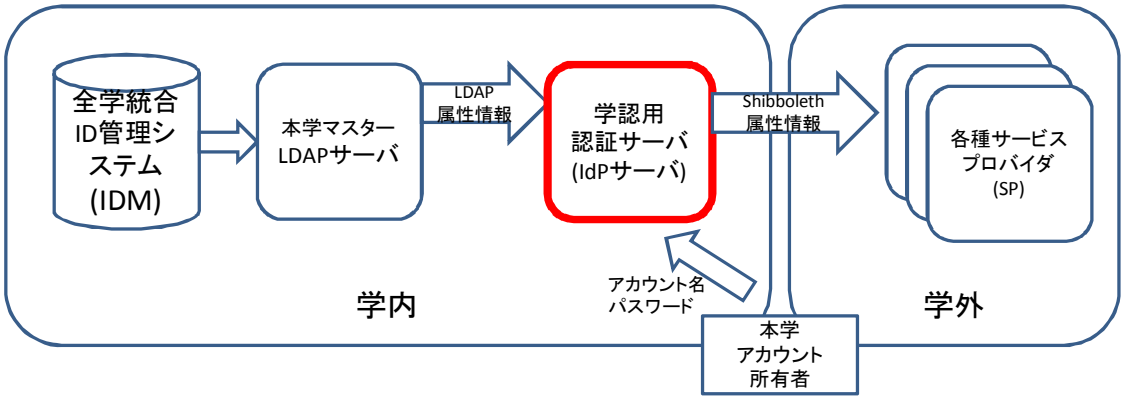


図 4: 学認対応の認証システムの概要

図中の全学統合 ID 管理システムおよびマスター LDAP サーバは，既に統合認証システムの一部として構築され利用可能です．学認への対応は，新たに IdP サーバの構築を行うことで実現できます．本学では IdP サーバとして，利用実績の多い Shibboleth Identity Provider Software(Internet2 による開発・配布) を選択しました．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が複雑であり，コンフィグレーションファイルの書式も XML 形式で可読性が低く，構築には敷居が高い印象を受けました．

この問題への解決策として，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，IdP サーバの構築を行いました．学認技術ガイドには曖昧な記述がなく，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．

なお，本学では，仮想化システムである VMWare ESX 上にサーバ OS として利用が想定されている CentOS5 を自己構築し，IdP の構築を行いましたが，VMWare で利用可能な IdP サーバのイメージファイル (CentOS5，Apache，Java，Tomcat，Shibboleth IdP，学認対応のコンフィグレーションファイルのテンプレートがインストール済み) が国立情報学研究所によって提供されています．このイメージを用いることにより，より容易に認証システムの構築が可能となります[2]．

4.2 統合 ID と学認との属性情報の対応付け

学認に対応したサービスを利用する場合，サービスを提供する側である SP は，IdP に対して利用者に関する属性情報 (Shibboleth 属性情報) を要求します．学認で利用される主要な属性情報を表 1 に示します．

[2]本学では IdP 構築のノウハウを確立するため自己構築を選択しました

表 1: 学認で利用される主要な属性情報

	属性	Shibboleth 属性情報
a	メールアドレス	mail
b	氏名	sn
c	組織名	o
d	内部組織名	ou
e	職種等	eduPersonAffiliation
f	一意識別子	eduPerson
g	アプリケーション 利用資格	PrincipalName eduPerson Entitlement
h	職種等 (スコープ付き)	eduPerson ScopedAffiliation
i	uid，組織名 (hash 値)	eduPerson TargetedID
j	氏名 (日本語)	jasn
k	組織名 (日本語)	jao
l	内部組織名 (日本語)	jaou

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の生成には，属性情報を有するデータベースへの照会が必要となります．本学では，全学統合 ID 管理システムが利用者の属性情報を有しています．IdP サーバからはマスター LDAP サーバを経由し，LDAP プロトコルを用いて参照することが可能です．

ただし，全学統合 ID 管理システムからは本学が独自に定めた属性情報のみが獲得できます．したがって，IdP サーバによる Shibboleth 属性情報への対応付けが必要となります．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．ただし，属性値によっては，全学統合 ID 管理システムでは整数値での表現に対し，Shibboleth 属性情報では文字列での表現となるため，対応付けが必要となりました．

属性値の対応付けへの対処方法として，IdP サーバ構築時に利用した学認技術ガイド内に，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) に関する記述がありました．本学では，この対処手法を利用し，職種情報の対応付けを実現しました．

5　利用者へのサービス提供

本節では，本学の IdP を用いて利用可能なサービスプロバイダの利用方法，サービスプロバイダの導入 (サービスの提供開始) スケジュールおよび利用状況について紹介します.

5.1　本学で利用可能なサービスプロバイダ (SP) (2011 年度末時点)

3.3 節にて述べたとおり，本学では学外 SP への詳細な情報公開を避けるため，以下に示す Shibboleth 属性情報

- eduPersonTargetedID (ユーザ名，組織名のハッシュ文字列)
- eduPersonAffiliation (職種)，eduPersonScopedAffiliation (組織名付き職種)

を利用するサービスの提供が可能です．本学では，これらの属性情報のみを利用し，

1. 本学で契約がなされ利用可能な電子ジャーナルサービス
2. 利用者にとって有用な情報システム

の基準で選定を行い，提供を行っています．2011 年度末時点で，これらの条件に合致する 8 つのサービスプロバイダ (電子ジャーナル 4，情報システム 4) が利用可能です．以下に，各サービスプロバイダの概要および利用方法を示します.

1. **電子ジャーナル等**

   - CiNii (学術論文検索データベース, 国立情報学研究所)
     URL　http://ci.nii.ac.jp/
     アクセス方法：ログインページ https://register-ci.nii.ac.jp/auth/action/login の「所属機関の学内認証システムでログインする方」を利用してください.

   - Science Direct (電子ジャーナル, Elsevier)
     URL　http://www.sciencedirect.com/
     アクセス方法:http://www.sciencedirect.com/science の「Login → Go to Athens / Other Institution login」を利用してください.

   - Springer Link (電子ジャーナル, Springer)
     URL　http://www.springerlink.com/
     アクセス方法：ログインページ http://www.springerlink.com/log-in/institution/ の「Select your institution → Kyushu Institute of Technology」を利用してください.

   - Web of Knowledge(電子ジャーナル，Thomson Reuters)
     URL：http://www.webofknowledge.com/
     アクセス方法：ログインページ (http://www.webofknowledge.com/) 内の「所属機関ログイン (Shibboleth)」の選択後,
     機関アクセス (Shibboleth) 内の「Japanese Research and Education(Gakunin)」所属機関欄より「九州工業大学」を選択してください.

2. 情報システム・サービス等

- Eduroam-Shib (eduroam 利用のためのアカウント発行サービス，国立情報学研究所)
  URL：https://eduroamshib.nii.ac.jp/

  サービスの概要：Eduroam-Shib を利用することにより，本学を含む世界約 50ヶ国，国内 22 機関が参加する無線 LAN 基盤 (eduroam) を利用することが可能です．eduroam の利用に関する詳細は，本学ウェブサイト (http://eduroam.isc.kyutech.ac.jp/) をご覧ください．

  アクセス方法：ログインページ (https://eduroamshib.nii.ac.jp/) 内の所属機関選択欄から，「九州工業大学」を選択してください．

- FShare (大容量ファイル転送サービス，国立情報学研究所)
  URL：https://fshare.sinet.ad.jp/

  サービスの概要：FShare を利用することにより，学認が利用できる指定した相手に対して，複数のファイルを公開することができます．具体的には，
  - 最大 10 人の相手に同時公開
  - 最大 10 個のファイルを同時公開
  - 合計 2G バイトのファイルを公開
  - 90 日間の保存期限
  - SL による暗号通信

  が可能です．詳細は，利用ガイド (https://fshare.sinet.ad.jp/how_to_use.html) を参照してください．

  アクセス方法：ログインページ (https://fshare.sinet.ad.jp/) 内の所属機関選択欄から，「九州工業大学」を選択してください．なお，初回アクセス時に，連絡用メールアドレスの登録が必要となります．

- FaMCUs (テレビ会議用多地点接続装置共用サービス，国立情報学研究所)
  URL：https://mcus.nii.ac.jp/

  サービスの概要：FaMCUs を利用することにより，Polycom 等のテレビ会議システムを用いた複数地点での会議に必要となる MCU(多地点接続装置) を時間単位で借り受けることができます．利用できる MCU は以下の 3 つです．
  - Polycom RMX 2000(国立情報学研究所設置)
  - Tandberg Codian MCU 4505(国立情報学研究所設置)
  - Tandberg Codian MCU 4505(京都大学設置)

  また，Skype からの MCU 接続に関しても，テスト運用が開始されています．MCU 装置の概要，予約，接続，制御方法の詳細については，ログインページ内の利用マニュアルを参照してください．

  アクセス方法：ログインページ (https://mcus.nii.ac.jp/) 内の所属機関選択欄から，「九州工業大学」を選択してください．なお，初回アクセス時に，連絡用メールアドレスの登録が必要と

なります.

- DreamSpark(学習目的のプログラミング環境無償提供サービス，Microsoft)
  URL：https://www.dreamspark.com/default.aspx

  サービスの概要：DreamSpark では，学生を対象に，プログラミングに必要な Microsoft 社の各種環境
  - 開発環境 (Visual Studio 2010 Professional，Expression Studio 4Ultimate)
  - サーバ OS(Windows Server 2008 Standard)
  - データベースシステム (SQL Server 2008 Developer)

  等が無償で提供されています．これらの環境を学習目的として利用することができます.

  アクセス方法 (各種ソフトウェアの取得方法)：ウェブサイト内の DreamSpark サイトの利用方法 (https://www.gakunin.jp/docs/fed/technical/connect/sp/microsoft/users) を参照してください．なお，DreamSpark へのログイン時に，Windows Live ID が別途必要となります.

5.2 利用者向けサービスプロバイダの導入スケジュール

現在本学では 8 つのサービスプロバイダが利用可能です．電子ジャーナルサービスに関しては，運用開始時には 3 サービスのみが利用可能でしたが，本学図書館からサービス追加の依頼を受け，学術情報委員会にて新たに要する Shibboleth 属性情報の送信に関する承諾を得た後，2011 年 7 月より 4 サービスが利用可能となりました.

各種情報システムに関しては，本学の eduroam への参加に合わせ，2011 年 6 月に eduroam-shib の提供を開始しました．その後，学認の更なる利用を促すため，ファイル転送サービス，MCU の共用サービス，学生を対象としたプログラミング環境提供サービスの追加を行い，2011 年 12 月より 4 サービスが利用可能となりました.

これらサービスプロバイダの導入スケジュールを以下に示します.

2011 年 1 月 運用フェデレーションへの登録・学認が利用可能となる

2011 年 2 月 運用開始時に提供を開始する SP の選定

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)

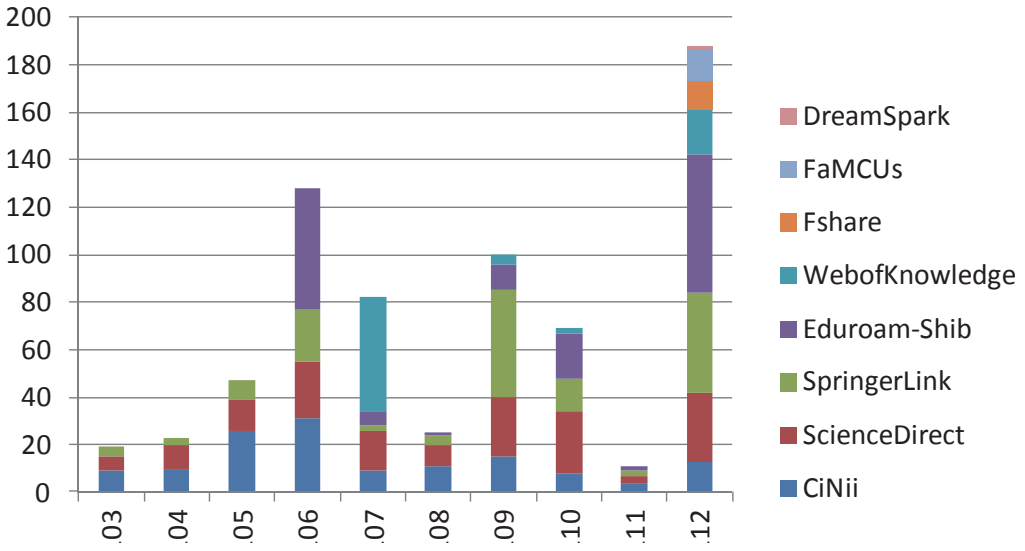
2011 年 7 月 Web of Knowledge の追加 (本学図書館からの依頼に基づく追加)

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)

5.3 利用者数

本学の IdP サーバを用いた各サービスプロバイダの利用者数 (2011 年 3 月から 12 月まで) を図 5 に示します.

各サービスの利用開始時に利用者数は一旦増加するものの，1 日辺りの利用者数は 2 人程度に留まっており，積極的に利用されているとは言い難い状況です．今後もより利便性の高いサービスプロバイダを追加し，利用者へ広報する必要があると考えています.



	2011/03	2011/04	2011/05	2011/06	2011/07	2011/08	2011/09	2011/10	2011/11	2011/12	Total
CiNii	9	10	26	31	9	11	15	8	4	13	136
ScienceDirect	6	10	13	24	17	9	25	26	3	29	162
SpringerLink	4	3	8	22	2	4	45	14	2	42	146
Eduroam-Shib				51	6	1	11	19	2	58	148
WebofKnowledge					48	0	4	2	0	19	73
Fshare										12	12
FaMCUs										14	14
DreamSpark										1	1
Total	19	23	47	128	82	25	100	69	11	188	692

図 5: 各サービスプロバイダの利用者数

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手法，利用者へ提供するサービスプロバイダの概要 (2011 年度末時点) と利用者数についてについて解説を行いました．学認を利用することにより，本学が整備を行った統合 ID 管理システムを用いた学外からの利用者認証が実現します．情報科学センターでは，2010 年度の後期より学認の参加へ向けた検証を開始しました．国立情報学研究所が整備した学認技術ガイドを参照することにより，学認向けの認証システムの検証および構築は予想を上回る期間で完了し，2010 年度末に正式運用を開始することができました．

前述の通り，現状では 1 日辺りの利用者数が 2 人程度と少ないため，今後も多くのサービスプロバイダを追加し，利用者に学認を活用して頂きたいと考えています．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．