# ADFS による学術認証フェデレーション対応 SharePoint サービスの構築

# Development of SharePoint Service for Gakunin by using ADFS

伊藤智博[†,††]，立花和宏[†]，奥山澄雄[†]，高野勝美[†,††]，田島靖久[‡,††]，吉田浩司[‡,††]
Tomohiro Ito[†,††], Kazuhiro Tachibana[†], Sumio Okuyama[†], Katsumi Takano[†,††],
Yasuhisa Tajima[‡,††]，Hiroshi Yoshida[‡,††]
tomohiro_ito@ieee.org, h9rbvq3x@yz.yamagata-u.ac.jp, sumio@ieee.org, ktakano@ieee.org,
tajima@sci.kj.yamagata-u.ac.jp, yoshida@ncsc.yamagata-u.ac.jp

† 山形大学大学院理工学研究科
‡ 山形大学基盤教育院
† ‡ 山形大学情報ネットワークセンター
992-8510 米沢市城南 4-3-16

† Graduate School of Science and Engineering, Yamagata University,
‡ Institute of Arts and Sciences, Yamagata University
† ‡ Networking and Computing Service Center, Yamagata University
4-3-16 Johnan, Yonezawa 992-8510 Japan

## 概要

山形大学で行われた SharePoint サービスを学術認証フェデレーションに提供するための様々な試みについて報告する．SharePoint の個人識別子について定め，mail 属性(OID: 0.9.2342.19200300.100.1.3)を採用した SharePoint サービスと学認で採用されているシボレスは直接認証連携が技術的にできないため，Active Directory Federation Service (ADFS)を経由して, SharePoint と ADFS を WS-Federation 連携することで解決した．また，ADFS は，学認のメタデータを直接読み込むことができないため，データベースサーバとメタデータ変換用ウェブサーバを組み合わることでメタデータの構造を自動変換することで解決した．これらの開発によって，学認に SharePoint Foundation サービスを提供することができた．

## キーワード

SharePoint, Active Directory Federation Service，シボレス認証，WIF， XML，学認

## 1. はじめに

山形大学では，従来，各部局や部署が，システム毎に独自のアカウントを発行して，システムを構築・運用していた．2003 年の時点では，情報系センター（当時の情報処理センター；以下センター）のアカウントですら，UNIX 系と Windows 系で独立しており，パスワードの取り扱いが複雑になる問題が生じていた．また，山形大学は，4 つからなる分散キャンパスであるため，運用方針についても，キャンパス毎に異なる要望があり，その要望に応えるため，様々な運用形態が生まれ複雑化していた．2004 年度より，工学部が設置されている米沢キャンパスのセンターが中心になって，認証統合の技術的な解決策と試行運用が開始された．検証課題として，「デジタル証明書」，「UNIX 系と Windows 系のパスワード同期」，「ネットワーク装置からの Active Directory(AD)への認証」，「オブジェクト識別子(OID)の設計」，「複数認証基盤の連携」を掲げ，それぞれの課題の技術面及び運用面での解決が試みられた. 2005 年には, 全ての課題について, 問題解決がなされ，工学部の利用者は，センターが提供するリソースに対して，1 つのアカウントで全てのサービスが提供できるようになった．その後，80 番ポートを介在して増殖するワームの対策の 1 つとして，工学部では，外部接続時にネットワーク利用者認証を必須とする運用方針が適用され、アカウントの利用者数は，米沢キャンパスのネットワーク利用者数である約 4000 人へと増加した．また，2007 年に実施した教育用実習システムの更新では，全てのキャンパスに米沢キャンパスと同様の統合認証を導入した．これによって，センターが提供する全てのサービスがシングルサインオンで提供できるようになった．

教務システムや会計システムなどの業務系のシステムとの認証の統合については，様々な議論の結果，センターが中心となって運用している学術系の認証情報とは統合しないという結論に至った. 議論の内容を要約すると, 教育・研究現場では, 学問の自由が許されている. 一方, 業務システムでは，堅牢なセキュリティシステムが必要とされる. この 2 つのポリシーは、互いに相反するため, その両方を同一の認証基盤で円滑に運用することは，困難であると判断した．すなわち，山形大学では，センターが管理・提供する「教育研究用認証基盤」と事務が中心となって管理・提供する「業務系認証基盤」のセキュリティレベルが異なる 2 つのアカウントが存在する．

2006 年度から，国立情報学研究所(NII)及び全学共同利用情報基盤センターが中心となり，全国大学共同電子認証基盤構築事業（UPKI : University Public Key Infrastructure）を 3 年計画で実施した[1]．この事業では，各大学にある計算機資源や情報インフラなどを大学間で，シームレスかつ安全に活用すること目的して，「デジタル証明書」，「グリッドコンピューティング」，「証明局」，「シングルサインオン」，「無線 LAN ローミング」を中心に認証基盤のプロトタイプ試験を実施した．

2008 年度には，UPKI 認証連携基盤実現のために技術的及び制度的な検証を行うために，「UPKI 認証連携基盤によるシングルサインオン実証実験（SSO 実証実験）が実施された．山形大学では，分散キャンパスで円滑に認証連携を進めるための技術的なノウハウを蓄積することを 1 つの目的として，LDAP プロキシや Radius プロキシによる複数認証基盤を統合し，SSO 実証実験及び大学間無線 LAN ローミング eduroam (eduroam)に参加した[2,3]. 2009 年には，UPKI-学術認証フェデレーションの試行運用フェデレーション（現在の学術認証フェデレーション；以下学認）に参加し，本格的な利用者サービスを開始した[4]．Shibboleth (シボレス)認証は，東日本大震災が発生した際に，本学の安否確認システムを 6 時間程度で構築できることから，開発コストを軽減できるツールの１つであった[5]. 2011 年には, 東日本大震災を踏まえて, 複数 ISP と分散データベースによる高可用性認証連携システムを構築し，学認をはじめとする様々なフェデレーションとの認証連携機能の可用性を向上した[6,7].

本学では，学内の利用者向けにグループボードワークスペースによるグループウェアサービスを展開している. 本学の研究者から，卒業生や学外の研究者との情報を共有できるグループウェアを提供してほしいとの要望があった．学外研究者とのコラボレーションツール提供の要望に応えるためには，グループウェアを学認に対応することが有効であると考えられる．本報告では，山形大学で構築した ADFS による学認対応 SharePoint サービスの構築について述べる．

## 2. 設計と使用した情報機器

### 2.1. ポリシー設計

SharePoint サービスを利用するためには，個人を識別するための個人識別子を使うことが必須になっている．すなわち，AD や学認から個人識別子がない場合は，利用することができない仕組みになっている．AD を認証基盤としてサービスを展開する場合は，ユーザログオン名(ドメイン¥ユーザ名)によって個人を特定し, SharePoint サービス内のメンバー登録に利用することができる．また，AD を利用する場合，AD の認証基盤を検索することも可能なため，サイトの管理者側の登録作業の負担も軽

減される．一方，学認で展開した場合，管理者が容易に利用者登録できる個人識別子を選択する必要がある．そこで，学認で定めている属性一覧から個人識別子を検討した結果，次に示す2つの属性名が適当であると考えられる [8].

・ePPN (OID:1.3.6.1.4.1.5923.1.1.1.6)
・mail (OID:0.9.2342.19200300.100.1.3)

これらの2つを比較したところ，ePPN 属性は学認内で一意性を保証しており，個人を識別することは容易である．しかし，各大学の諸事情などから，属性値から個人を直接推測できないように，ハッシュなどの不可逆暗号を行っている場合がある[9]．そのため，SharePoint サービスの管理者は，利用者から属性値を聞き出すなどの手順が必要になり，サイトを運用する上で，管理者への負担が大きい．一方，mail 属性は，一意性を保証するものではないが，個人を特定することが可能であるため，管理者の運用コストは軽減できる．特に，SharePoint Foundation サービスは，グループ内のワークスペースやスケジュール管理，ドキュメント共有を目的としているため，個人を特定して権限を付与することが必要不可欠である．このような背景のもと，SharePoint サービスで利用する個人識別子は, mail 属性を利用することにした.

SharePoint サービスは，グループに権限を付与することもできる．学認内で，グループ属性になり得る属性名としては，ePSA(OID: 1.3.6.1.4.1.5923.1.1.1.9)であった[8]. この属性を SharePoint のグループへの権限付与に使うことによって，特定の大学に所属する特定の職位の人に，権限を付与できる．例えば，山形大学の構成員に，SharePoint 内の特定サイトに読み込み権限を付与することができるようになる．もし，このようなグループ属性による管理機能がない場合，一人一人の mail アドレスをサイト利用者として登録するため，サイト管理者の負担が増大する．すなわち，グループ識別子による利用者登録が可能であることにより, 利便性の向上が期待される.

以上を踏まえて，SharePoint サービスの運用ポリシーをまとめると，

・個人識別子には，mail 属性
・グループ識別子には，ePSA 属性

を利用することにした.

## 2.2. 構築上の問題点とシステムの概要

SharePoint サービスを学認に対応するためには, 2つの大きな問題点を解決する必要がある．1つ目の問題点は，SharePoint サービスが提供する Security Assertion Markup Language (SAML)ベースの認証方式であるクレームベース認証は，学認が推奨するシボレスと直接連携が難しいことである．2 つ目の問題点は，Active Directory Federation Service (ADFS)は，学認が提供するような複数の認証プロバイダ(IdP)やサービスプロバイダ(SP)の信頼情報を1つのファイルに集約したメタデータを直接読み込めないことである. この2つの問題を解決するために，図 1 に示すようなシステムを構築した．1 つ目の問題点は，ADFS サーバがシボレス IdP からの SAML アサーションを WS-Federation 用の SAML アサーションに変換する認証ゲートウェイのような機能を利用することで解決した．2 つ目の問題点は，学認が提供するメタデータを読み込み解析するウェブクローラーモジュールを開発し，ADFS に対応したメタデータに変換し，読み込ませることで解決した.

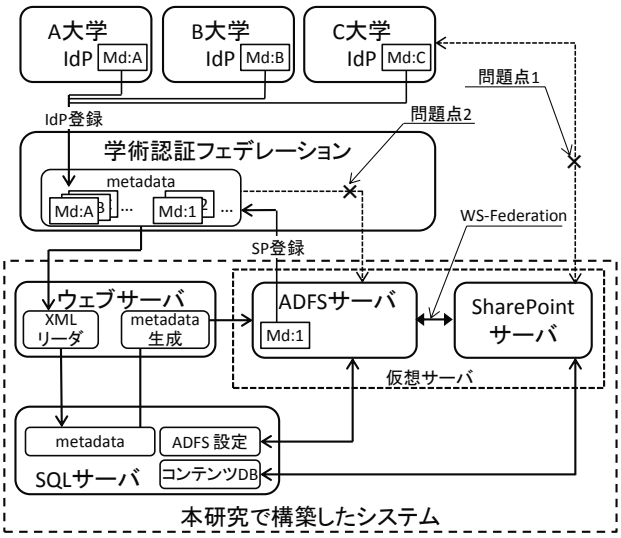


**図 1. 学認対応 SharePoint サービスの概略**

## 2.3. 各サーバのスペック

サービスの実運用において，ADFS サーバ，SharePoint サーバ，SQL サーバ，メタデータ変換用メタデータ変換用ウェブサーバを使用した. 学内の認証基盤は, Windows Server 2008 上の AD サービスによって提供されている．仮想サーバは，ADFS サーバ，SharePoint サーバをはじめとする 25 のゲストマシーンが動作している．今後，新しいサービスを展開することを想定し，40 程度のゲストマシーンを動作できるように設計した．SQL サーバは，研究やログの解析にも利用されおり，現在，約 1500 万件／日のトランザクションを処理している．導入時に，2 億件／日のトランザクションを処理できるように設計した．以下に，それぞれのサーバのスペックを示す.

[仮想サーバ]
CPU: AMD Opteron 6180SE 2.5GHz ×4
メモリ: 128 GB
ローカル HDD: 1.8 TB
共有 HDD: 10 TB
OS: VMware vSphere 5.0 Enterprise Plus
備考：冗長性を保つために，複数の物理サーバで構成

[ADFS サーバ]
CPU:2 (仮想サーバ上で動作)
メモリ：4GB
HDD: 90 GB
OS: Microsoft Windows Server 2008 R2 Enterprise Edition
アプリケーション：ADFS 2.0, Visual Studio 2008 Professional

[SharePoint サーバ]
CPU:2 (仮想サーバ上で動作)
メモリ: 4GB
HDD: 128 GB
OS: Microsoft Windows Server 2008 R2 Standard Edition
アプリケーション：SharePoint Foundation Server 2010

[SQL サーバ]
CPU: AMD Opteron 6282SE 2.6GHz ×2
メモリ：64GB
HDD: 3.6TB (900GB×8, RAID 6)
OS: Microsoft Windows Server 2008 R2 Enterprise Edition
アプリケーション： Microsoft SQL Server 2008 R2 Enterprise Edition

[メタデータ変換用ウェブサーバ]
CPU: Intel Pentium E2160 1.8GHz ×1
メモリ：4GB
HDD: 1.0TB (1TB×2, RAID 1)
OS: Microsoft Windows Server 2003 Standard Edition
アプリケーション： Visual Studio 2005 Professional

[クライアント PC]
CPU: Intel Core　i7 M620×1
メモリ：8GB
HDD: 128GB
OS: Microsoft Windows 7 Professional
アプリケーション： Internet Explorer 9, Firefox 13.0

## 3. 各機能モジュールの構築と総合評価

SharePoint サービスを学認に対応するためには，シボレス IdP は直接認証連携できない問題を解決することが必要不可欠である．本節では SharePoint サービスを学認に対応するために開発したモジュールと総合的な動作確認について述べる．

### 3.1. 学認メタデータ読み取りモジュール

ADFS に学認のメタデータを対応するためは，複数の IdP が一塊になっている XML ファイルをエンティティごとに分割し，ADFS に登録する必要がある．そこで，図 2 に示すような学認のメタデータを自動的に読み込み，エンティティごとに分割し，SQL サーバに登録するモジュールを開発した．

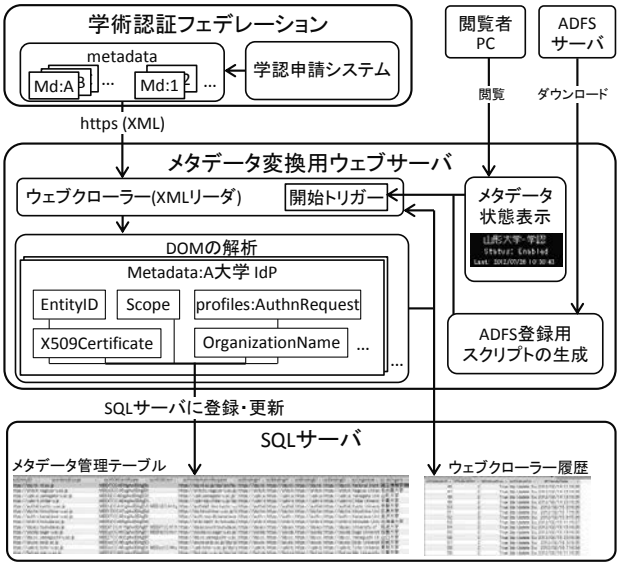


**図 2. 学認メタデータ読み取りモジュールの概略**

具体的には，メタデータ変換用ウェブサーバ内にウェブクローラーモジュールを開発した. このモジュールは，開始トリガーによって実行され，SQL サーバに記録されているウェブクローラー履歴を閲覧し，最後に，学認のメタデータの読み込みおよび SQL サーバへの登録・更新が成功した最終更新日時を得る．最終更新日時と現在の日時の差が 4 時間以上ある場合，学認のメタデータを https プロトコル経由で，読み込み，ドキュメントオブジェクトモジュール（DOM）の解析プログラムに学認のメタデータを受け渡す．DOM 解析プログラムは，受け取ったメタデータをエンティティごとに分割する. さらに，それぞれのエンティティの XML を解析し，要素や属性値に抽出する．それぞれの要素の属性値は，SQL サーバ内のメタデータ管理テーブルと照合され，登録または更

新の処理が行われる. すべてのエンティティを SQL サーバに登録・更新処理が完了した場合，ウェブクローラー履歴テーブルに，処理完了の履歴が記録される.

ウェブクローラーモジュールがクロールを開始するトリガーは，メタデータ変換用ウェブサーバ内の特定のアクティブサーバページに http 接続にしたときに有効になるようにした．具体的な特定ページとは，メタデータの更新状態をアイコン画像として表示するページと後述する ADFS サーバが IdP を登録するときに使用する ADFS 登録用スクリプト生成ページの 2 つである．ウェブページをトリガーにしたことによって，外部サーバとの連携が容易にできるようになっている.

### 3.2. ADFS の学認 IdP の自動管理

ADFS では，シボレスのようにメタデータを一括で読み込むことができない．通常は，GUI の管理ツールやコマンドラインから，手動で登録する．学認のメタデータには，2012 年 6 月の時点で 41 機関が IdP 登録されており，今後も増えることが予想される．サービス継続性を考慮すると，学認に登録された IdP を自動的に管理することによって，運用コストを軽減することが必要不可欠である．この問題を解決するために，図 3 に示すような SQL サーバと連携した ADFS への自動管理モジュールを構築した.

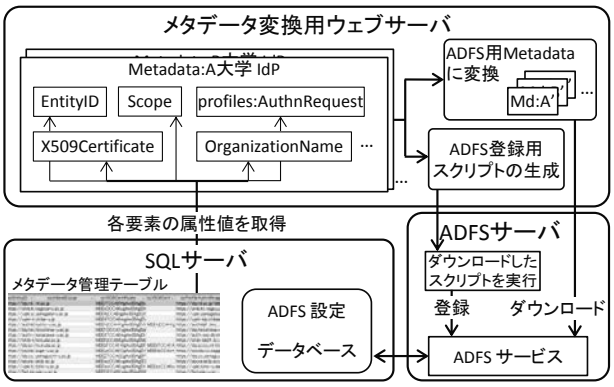


**図 3. ADFS 用メタデータ自動管理システムの概略**

具体的には，SQL サーバ内のメタデータ管理テーブルを参照し，表 1 の 1 に示すような ADFS に IdP 登録するためのスクリプトを自動生成する．スクリプトの 1 行目に記述されたコマンドによって，ADFS を管理するためのモジュールを読み込み初期化した．次に，2 行目に記述されたコマンドにより，ADFS の要求プロバイダ (Claims Provider Trust)に追加登録され，スクリプトに記述された Metadata URL から，ADFS 用に変換されたメタデータを読み込まれる．ADFS は，メタデータを解析し，種々の要素に関する属性値を取得し，登録する．シボレス IdP と ADFS とでは，セキュアハッシュアルゴリズムの既定値が異なるため，正常に SAML アサーションを送受信できない．この問題は，ADFS のセキュアハッシュアルゴリズムを SHA-1 に設定することで解決した. シボレス IdP から送信された SAML アサーションを ADFS が受け取るためには，要素 ID を表 2 示すように再定義する必要がある．3 行目のコマンドは，変換規則を記述した設定ファイルを読み込むことにより，ADFS に変換規則を定義した．また，2 行目と 3 行目のコマンドを繰り返すことによって，複数の IdP を登録・変換規則の定義を行うスクリプトを動的に生成するようにしている.

次に，スクリプトのダウンロードおよびスクリプトを起動するために，表 1 の 2 に示すようなコマンドを実行した．このコマンドは，前述したスクリプトをメタデータ変換用ウェブサーバからダウンロードし，パイプを経由して，PowerShell プログラムに渡し，スクリプトが実行されるようになっている. タスクなどの機能を使って，定期的に実行することで, 学認に IdP が追加されたとき，自動的に追加できるようにした．また，ADFS の設定情報は，SQL サーバに記録するように設定し，可用性や拡張性を高めている.

**表 2　ADFS 内に設定した要素名の変換規則**

| シボレスの要素名 | ADFS 側の要素名 |
|---|---|
| mail[1)] | 電子メールアドレス[2)] |
| ePSA[3)] | 役割(Role)[4)] |

それぞれの SAML の要素の ID は，'urn:oid:0.9.2342.19200300.100.1.3'(1) ; 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress' (2) ; 'urn:oid:1.3.6.1.4.1.5923.1.1.1.9' (3) ; 'http://schemas.microsoft.com/ws/2008/06/identity/claims/role' (4) である.

**表 1 ADFS の IdP 登録用スクリプトの例と登録スクリプトのダウンロードおよび実行コマンド**

| | |
|---|---|
| 1.　ADFS 登録用スクリプトの例 | 1 行目: Add-PSSnapin Microsoft.Adfs.PowerShell<br>2 行目: Add-ADFSClaimsProviderTrust -Name '学認／National Institute of Informatics'<br>-MetadataURL 'https://a.yamagata-u.ac.jp/amenity/network/AdfsIdPMetadataXml.aspx?IdPID=151'<br>-AutoUpdateEnabled 1 -MonitoringEnabled 1　-SignatureAlgorithm 'http://www.w3.org/2000/09/xmldsig#rsa-sha1'<br>3:行目：Set-ADFSClaimsProviderTrust -TargetName '学認／National Institute of Informatics'<br>-AcceptanceTransformRulesFile 'C:¥Gakunin-adfs¥Gakunin-IDP-to-ADFS.tpl'<br>・・・ |
| 2. ダウンロードおよび実行コマンド | wget http://a.yamagata-u.ac.jp/amenity/network/AdfsIdPAddPSCommand.aspx?FederationID=2 -O - \| powershell -File - |

### 3.3. SharePoint サーバのクレーム認証の設定

SharePoint サーバの認証に，シボレス認証を利用するためには，ADFS の認証ゲートウェイ利用することが必要である．そこで，SharePoint サーバのクレームベース認証の信頼 ID プロバイダに ADFS を設定した．
SharePoint サーバの Web アプリケーション（SharePoint の仮想サイトのこと）には，「クラシックモード認証」と「クレームベース認証」の 2 種類の認証モードがある．ADFS などをはじめとする SAML による認証連携を行うときは，「クレームベース認証」を選択することが必須になっている．そのため，学認用 Web アプリケーションの認証モードは，「クレームベース認証」を選択して，大学間連携グループ情報共有サイトを構築した．次に，大学間連携グループ情報共有サイトと ADFS 間に，WS-Federation の信頼関係を設定した．信頼関係を設定しただけでは，ADFS は，属性情報を送信しないので，表 3 に示すように大学間連携グループ情報共有サイトに属性情報を送信するように ADFS の要求規則を設定した．

**表 3　SharePoint サービスへの属性情報の要求規則**

| ADFS の要素 | SharePoint サービスの要素 |
|---|---|
| 電子メールアドレス [1)] | 電子メールアドレス [1)] |
| 役割(Role)[2)] | 役割(Role)[2)] |

それぞれの要素の ID は，"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"(1)；"http://schemas.microsoft.com/ws/2008/06/identity/claims/role"(2) である．

### 3.4. ADFS のカスタマイズ

ADFS は，学認に SharePoint サービスを提供した場合，所属機関の IdP を選択するディスカバリーサービス(DS)のような役割を果たす．利用者への利便性を向上するために，「アクティブディレクトリ(AD)による認証の無効化」と「利用者の IdP の候補を表示するための機能追加」の 2 つのカスタマイズを行った．

具体的には，AD の認証を無効化するために，web.config ファイルを次のように変更した．

（無効化前）

```
<localAuthenticationTypes>
        <add name="Integrated" page="auth/integrated/" />
        <add name="Forms" page="FormsSignIn.aspx" />
        <add name="TlsClient" page="auth/sslclient/" />
        <add name="Basic" page="auth/basic/" />
</localAuthenticationTypes>
```

（無効化後）

```
<localAuthenticationTypes>
<!–
        <add name="Integrated" page="auth/integrated/" />
        <add name="Forms" page="FormsSignIn.aspx" />
        <add name="TlsClient" page="auth/sslclient/" />
        <add name="Basic" page="auth/basic/" />
–>
</localAuthenticationTypes>
```

ADFS の DS 機能は，HomeRealmDiscoveryPage Class のライブラリーによって提供されている．このライブラリーと独自のコードを組み合わせ，利用者の IP アドレスから候補となる IdP を表示するプログラムを開発した．具体的な動作は，利用者が ADFS に接続すると，DS のモジュールは，ソース IP アドレスを元に，SQL サーバ内にある IdP 選択履歴テーブルを検索する．検索結果から，履歴があった場合，最後に選択された IdP を，候補 IdP として利用者の DS の画面の上部に表示する．履歴がなかった場合，候補 IdP としては，OpenIdP を表示する．DS の画面には，候補 IdP とは別に，学認に参加している全ての IdP の一覧が表示されているので，候補 IdP が誤っていた場合，所属機関の IdP を選択できるようになっている．利用者が IdP を選択すると SQL サーバの IdP 選択履歴テーブルが更新され，最後に利用したソース IP アドレスと IdP が記録されるようになっている．次回からの利用では IP アドレスが変わらない限り，利用者が前回に利用した IdP が候補として表示されるため，利用者の利便性を向上できる．

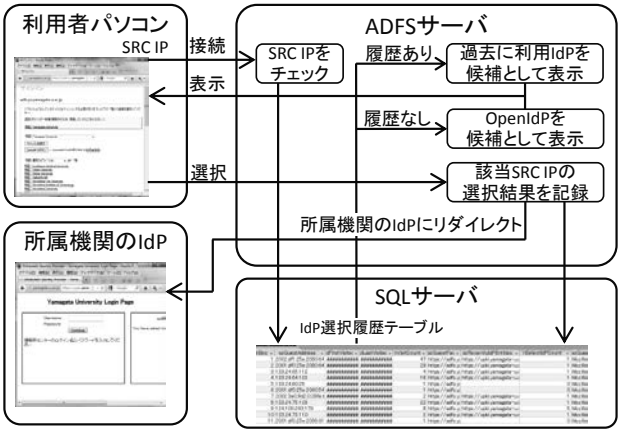


**図 4. 利用者の IdP の候補検索モジュールの概略**

### 3.5. 総合的な動作確認と IPv6 への対応

SharePoint サービスの動作確認を行った．利用開始ページに接続してから，SharePoint サービスが利用可能になるまでの一連の動作画面を図 5 に示す．まず，SharePoint サービスを利用するためには，利用開始ページ(https://adfs.yz.yamagata-u.ac.jp/)に接続する．利用開始ページの「利用開始」のリンクをクリックすると，SharePoint サービスのサインインページにリダイレクトされる．「学認ログイン」を選択すると，ディスカバリーサービスのページにリダイレクトされる．所属機関の IdP を選択すると，所属機関の IdP のページにリダイレクトされる．所属機関の認証方式に従って認証操作を行い，認証が成功すると，SharePoint サービスが利用開始される．

2011 年 4 月に JPNIC からの IPv4 アドレス割り当てが終了したことにより，IPv6 アドレスへの移行が進められ

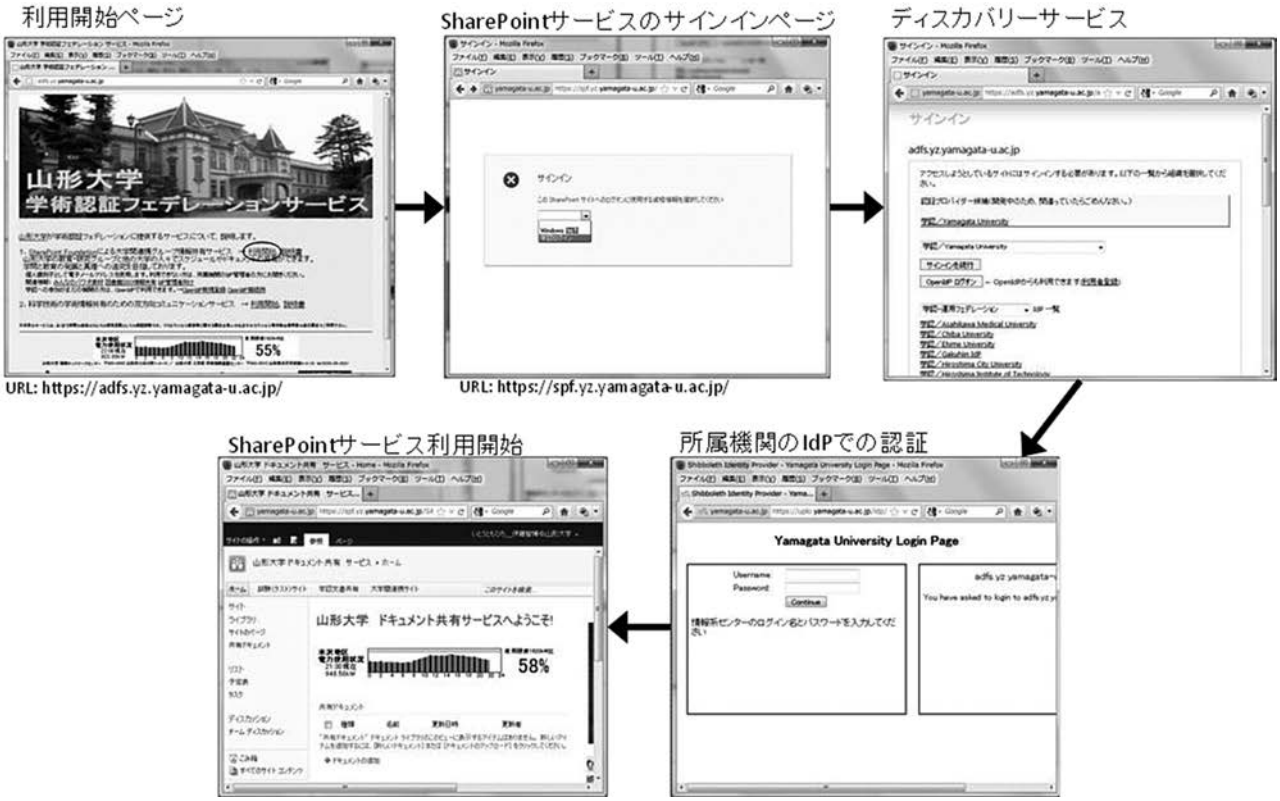


**図 5. 学認に対応した SharePoint サービスの動作画面**

ている[10]．本学の IPv6 ネットワークは，特殊用途用プロバイダ非依存アドレスを JPNIC より取得しており，BGP プロトコルによるマルチホーム構成によって上位 ISP に接続している．SharePoint サーバ，ADFS サーバ，SQL サーバ，IdP サーバに IPv6 アドレスを付加して，次世代 IP アドレスによるサービスの継続性を確認した．学内および学外から IPv4/IPv6 デュアルスタックのクライアント PC を使用して，SharePoint サービスの動作を確認したところ，全ての機能が問題なく動作した．

学認へのサービス提供を開始した 2012 年 3 月から約 200 人が利用している．1 日あたりの平均認証数は，15 件程度であり，2012 年 7 月までの間に，問題は発生していない．また，SharePoint サービスの共有ドキュメント機能を使用するときに，ウェブブラウザーから Office アプリケーションに遷移するときも認証情報がシームレスに接続できるように改良が加えられており，利便性の高いドキュメント共有サービスを提供できるであろう．

## 4. まとめ

学認にサービスを提供するために，個人識別子に関する運用ポリシーを定めた．個人識別子には，学認が定めている mail 属性(OID: 0.9.2342.19200300.100.1.3)を採用した．SharePoint サービスと学認で採用されているシボレスは直接認証連携が技術的にできないため，ADFS を経由して，SharePoint と ADFS を WS-Federation で認証連携することで解決した．ADFS は，学認のメタデータを直接読み込むことができないため，SQL サーバとメタデータ変換用ウェブサーバを組み合わることでメタデータの構造を変換することで解決した．これらの試みにより，学認対応 SharePoint Foundation サービスを提供することができた．現在，本学では卒業生用の認証基盤と認証連携用の IdP サーバの構築が計画されている．SharePoint サービスと卒業生用 IdP サーバが認証連携することで，卒業生へのサポートも充実できることが期待される．

先行事例として，Thia らは，FEMMA(Federation Metadata Manager for ADFS)によって，シボレス IdP のメタデータを管理すること述べている[11]．しかし，FEMMA による管理方法について，学認をはじめとする複数の IdP のメタデータを管理する具体例が述べておらず，大規模なフェデレーションへの展開は難しい．本報告では，メタデータの DOM を解析するプログラムを開発して，データベースに正規化した情報を蓄積することによって，SharePoint サービスの大規模展開を可能にした．フェデレーション毎に，メタデータのフォーマットが異なった場合，DOM 解析プログラムを改良することって様々なフェデレーションのフォーマットにも対応できるなどの利点がある．

技術的な利点として，これまで Windows サーバによる

ウェブサービスを学認に提供するときは，認証ミドルウェアとしてシボレスなどのサードパーティ製の認証ミドルウェアを導入し，ウェブアプリケーションは環境変数として認証情報を受け取るプログラムを開発してきた．サーバ内の環境変数を経由するということは，OS の言語設定が影響するため，日本語文字列などを含む SAML アサーションの文字列(UTF-8)が文字化けすることがあった[12]．SharePoint サービスのクレームベース認証機能は，Windows Identity Foundation (WIF)を基盤に開発されている．WIF は，ASP .NET アプリケーションの開発時に，Windows 認証やクライアント証明書，SAML をはじめとする複数セキュリティトークンを使用した統合的な認証機能を提供する API である．WIF による ASP .NET ウェブアプリケーションの開発においても SharePoint と同様に，ADFS を中継することによって，シボレス IdP とウェブアプリケーションが認証連携できるようになる．すなわち，ASP .NET ウェブアプリケーションと認証連携モジュールを同一のコード内で記述でき，属性値などの認証情報が OS の環境変数を経由しないため，文字化けの問題が改善されることが期待される．また，ウェブアプリケーションを複数の認証(AD,シボレス)に対応させるときに，アプリケーションコードをシンプルに開発できる可能性が高い．

今後，本学が提供しているウェブアプリケーションを WIF と ADFS を組わせて，学認と学内の AD 認証を統合した利便性の高いサービスプロバイダーを開発し，学問の発展に寄与したい．

## 謝辞

IPv6 ネットワーク接続を提供していただきました SINET4 および JGN-X の皆様に深く感謝申し上げます．シボレスおよび学認関連の質問にご回答いただきました国立情報学研究所および学認タスクフォースの皆様に深く感謝申し上げます．本学の認証情報の更新・管理にあたり，常に最新の情報に更新していただいた情報系センターのスタッフの皆様に深く感謝申し上げます．本サービスの一部の構築には，平成 22 年度国立大学法人設備整備費補助金事業の補助を受けて，実施した．

## 参考文献

[1] UPKI イニシアティブ，https://upki-portal.nii.ac.jp/，(参照 2009-07-20).

[2] 伊藤智博、吉田浩司、鈴木勝人、青木和恵 : “既存の複数認証基盤を統合した UPKI-SSO・eduroam 対応認証基盤の構築”，平成 20 年シングルサインオン実証実験報告書 (2009).

[3] “認証基盤も冗長構成化して可用性を向上”，学認活用事例集， https://www.gakunin.jp/docs/fed/info，(参照 2012-02-09).

[4] 学術認証フェデレーション，https://www.gakunin.jp/，(参照 2012-02-01).

[5] 伊藤智博，高野勝美，田島靖久，吉田浩司 : “ 災害時に備えた分散キャンパスによる情報基盤の整備”，学術情報処理研究誌，No. 15，pp. 5-11 (2011).

[6] 伊藤智博 : “分散キャンパスを活用した複数 ISP 接続による eduroam アクセス回線の冗長化について”，eduroam JP ケーススタディ，http://www.eduroam.jp/docs.html (参照 2011-06-10).

[7] 伊藤智博，高野勝美，田島靖久，吉田浩司 : “複数 ISP と分散データベースによる高可用性認証連携サービスの構築”，大学情報システム環境研究，Vol. 15，pp. 72-79 (2012).

[8] “属性リスト”，学術認証フェデレーション，https://www.gakunin.jp/docs/fed/technical/attribute ，(参照 2011-12-25).

[9] 松平拓也，笠原禎也，高田良宏，井町智彦，金沢大学UPKI SSO 実証実験WG: “金沢大学における IdP, SP 構築の現状と今後の展望”，平成 20 年シングルサインオン実証実験報告書 (2009).

[10] “APNIC における IPv4 アドレス在庫枯渇のお知らせおよび枯渇後の JPNIC におけるアドレス管理ポリシーのご案内”，JPNIC，http://www.nic.ad.jp/ja/topics/2011/20110415-01.html (参照 2011-05-01).

[11] Jean-Marie Thia , Philippe Beraud , Benjamin Guinebertière, Stéphane Goudeau : “ Step-by-Step Guide: Federated Collaboration with Shibboleth 2.0 and SharePoint 2010 technologies”，http://go.microsoft.com/fwlink/?LinkId=207916， (参照 2012-01-09).

[12] “IIS 上に Shibboleth SP を構築したときに属性情報の文字化けを修正する方法”，サイバーキャンパス「鷹山」，https://a.yamagata-u.ac.jp/amenity/Laboratory/LaboNoteWeb.aspx?nLaboNoteID=1173， (参照 2009-10-08).