（5）UPKI認証連携基盤シングルサインオン

システム情報工学研究科・学術情報メディアセンター　佐藤　聡
システム情報工学研究科・学術情報メディアセンター　古瀬一隆
システム情報工学研究科博士前期課程　高田真吾

1．はじめに

利用者本人を特定し，対象とする利用者にのみ適切にサービスを提供するための機構として，認証機構は重要な役割を果たしている。特に電子図書館システムを中心とした図書館情報システムの場合には，図書館内はもちろんのこと，学内・学外のさまざまな環境から利用されるため，利便性と堅牢性を兼ね備えた認証機構の必要性は非常に高い。

以上のことから，本取り組みでは平成18年度に開始された全国大学共同電子認証基盤構築事業UPKI (University Public Key Infrastructure)[1]の枠組みのもと，電子図書館システムにシングルサインオン型の認証基盤を構築した。

また，シングルサインオン型のサービスの開発，構築の実証実験を行うために，図書館に設置されているキヨスク端末をシングルサインオンにより利用可能となるサービスの開発を行った。

本稿では，これらの取り組みの詳細と成果について報告する。

2．シングルサインオン環境の実装

シングルサインオン（single sign-on）とは，利用者の特定を必要とする複数のシステムにおける認証機構を一元化し，一度のサインオン（ログオン）処理によって連携するすべてのシステムの認証を済ませる機構のことをいう。シングルサインオン機構を用いると，いくつかのシステムを連続して（あるいは組み合わせて）使用するような場合でも個々のシステムに別個にサインオンする必要がなくなるため，利用者にとっては利便性が高い。特に書誌・所蔵・典拠情報等の管理システムや電子ジャーナルシステム等の複数のサブシステムの組み合わせとして全体が構成される電子図書館システムの場合，シングルサインオン機構の導入は高い効果が期待できる。また，シングルサインオン機構の導入により認証に必要となるパスワード等の秘密情報の流通を制限することが可能となるため，セキュリティの向上にも寄与する。

本取り組みでは，本学で平成17年度より稼働している統一認証システムと連動させることにより，シングルサインオン環境を構築した。以下にその詳細を記す。

2.1. 統一認証システム

統一認証システムは本学で稼働している認証システムであり，学術情報メディアセンターによって管理・運営がなされている。本システムには職員（教員を含む）や学生等の本学に籍を置く人物のアカウント情報（ユーザ名，パスワード等）が登録されている。本システムと連動するシステムでは，同一ユーザ名・同一パスワードでのサインオンが可能であり，全学計算機システムや学内無線LANシステム等，全学的なサービスを展開するシステムを中心に利用されている。

本システムで用いている認証プロトコルはLDAP（Lightweight Directory Access Protocol）である。LDAPはもともと各種の情報を管理し，必要に応じてそれを提供するディレクトリサービス（directory service）の一種として開発されたものであるが，ここにパスワードを含む利用者のアカウント情報を登録することにより，認証を一元化するための機構としても広く使われている。本学ではLDAPのディレクトリ

に職員・学生等の利用者情報を登録している。

統一認証システムを用いることにより，利用者は様々なシステムに同一のユーザ名やパスワードでサインオン（ログオン）することができる。ただし，統一認証システム自体はシングルサインオンの機構を有していないので，利用者は利用するサービスごとに個別にサインオンの手続きを行う必要がある。

2.2. Shibboleth

Shibbolethは，次世代インターネット関連研究開発組織Internet2の教育機関向けプロジェクトMACE（Middleware Architecture Committee for Education）において開発されているWebシステム用のシングルサインオンシステムのオープンソースによる実装である[2]。認証情報の交換にはSAML（Security Assertion Markup Language）を用いる等，インターネット標準に基づいた設計・実装となっている。Shibbolethは特に教育・研究機関におけるシングルサインオンシステムとして国際的に利用が拡大しており，事実上の標準となっている。

Shibbolethにおいては，認証を行うサーバをIdP（identity provider）と呼び，IdPに対して認証を依頼するWebサーバをSP（service provider）と呼ぶ。利用者が電子図書館システム等のSPを利用する場合，その認証はIdPが行う。SPとIdPの関係と処理の流れを図１に示す。

一般に，Shibbolethによるシングルサインオンを実装しているWebサービスに利用者がアクセスする場合の処理手順は，以下のようになる。

①利用者がSPにアクセスする
②（サインオン状態にない場合には）SPはIdPへのリダイレクト（HTTP redirect）を行う
③利用者端末にIdPの認証画面が表示されるので，利用者はその画面でパスワード等の認証情報を入力する
④認証の結果に基づき，IdPがSPに対して利用者の属性情報を提供する
⑤SPが利用者に対してサービスを提供する

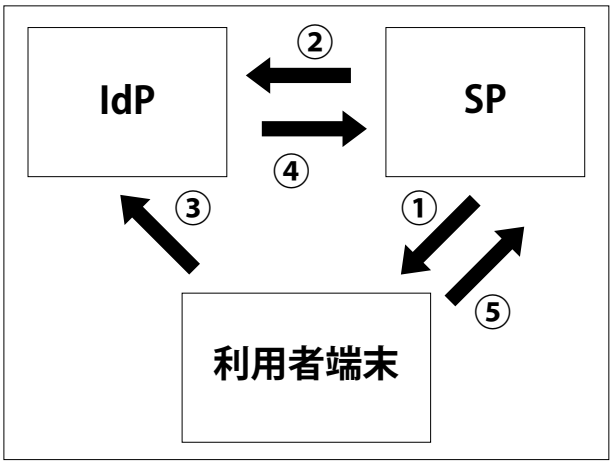

図１. Shibbolethにおける認証処理の流れ

すでにサインオン状態にある利用者がSPにアクセスした場合，上記の処理手順の②と③は省略される。したがって，最初に認証が済んでサインオン状態になった利用者は，その後新たにSPにアクセスしても，その都度認証情報を入力する必要なくサービスを受けることができる。これによってシングルサインオンの機構が実現されている。

なお，上記の処理手順からわかるように，Shibbolethを用いる場合，利用者が入力するパスワード等の認証情報はSPを経由することなくIdPに直接送られることとなる。このため，SPにおける不具合等によって認証に係る機密情報が漏れる恐れが一切ないという利点がある。

2.3. 電子図書館システムTulipsにおけるシングルサインオンの実装

本学の電子図書館システムTulipsは平成22年にシステムの更新が行われ，この際に統一認証システムと連動したShibbolethによる認証機構が実装された。システム構成の概略を図２に示す。

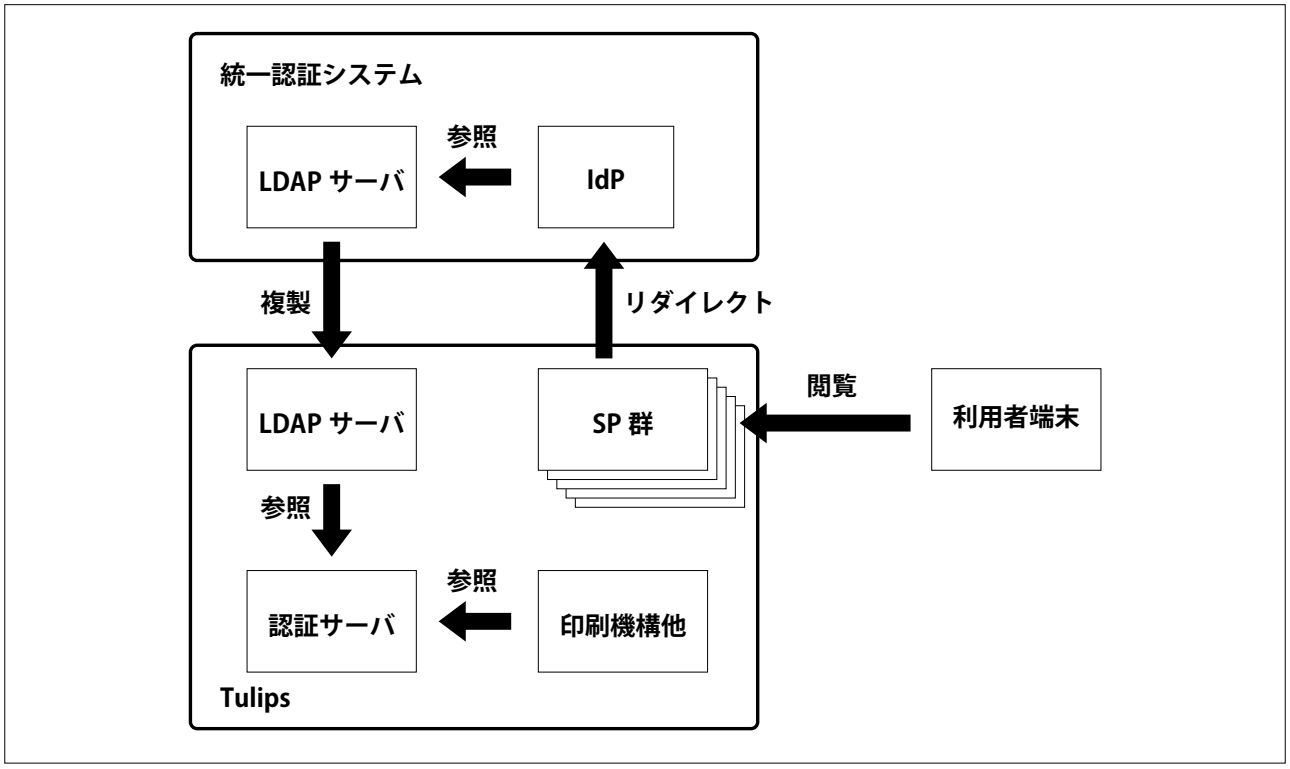

図 2 . システム構成

一般利用者に提供されるTulipsのサービスを構成するサーバ群（ポータルインターフェース，RefWorks，EZproxy等を含む）は，ShibbolethのSPとして実装されている。先に述べたとおり，サインオン状態にない利用者が端末からこれらのSPにアクセスするとIdPにリダイレクトされ，認証が行われる。IdPは統一認証システムのLDAPサーバをオンデマンドに参照し，パスワードによる認証処理を行う。認証後，IdPはLDAPに登録されている利用者の氏名等の属性情報をSPに提供する。

印刷枚数の制限等を行う印刷機構や携帯電話向けインターフェース等のWebサービス以外の機構ではShibbolethによる認証を行うことができないため，TulipsではShibbolethとは別個に認証サーバも有している。ここでも統一認証システムと同一の認証情報を用いるため，Tulipsでは統一認証システムのディレクトリ情報を複製した独自のLDAPサーバを設置している。統一認証システムに登録されている情報は，数分に１回の頻度で登録情報の更新（同期）を行っている。

以上により，Tulipsでは認証の一元化とWebサービス群のシングルサインオンの機構を構築している。Tulipsではさまざまな機能がさまざまなサブシステムによって提供されているが，利用者からは全体が一つのシステムとして機能するインターフェースが実現されている。

2.4. 認証フェデレーション「学認」への参加

Shibbolethにおいては，特定の規程（ポリシー）のもとに構成されたIdPやSPの集合体をフェデレーションという。フェデレーションに参加することはIdPやSPの運用が定められた規定の条件を満足しているということが担保されるということを意味しているため，これにより他機関等との認証の相互連携が実現可能となる。SPによっては，フェデレーションに参加しないIdPとは接続を行わないという運用方針も持っている場合もある。

国内で運用されている認証フェデレーションとしては，国立情報学研究所（NII）と全国の大学の連携に

よって構築されているフェデレーション「学認（GakuNin)」がある。本学のIdPも，平成22年度にこのフェデレーションへの加盟手続きを行い，正式参加を果たした。

３．キヨスク端末における認証機構の実現

附属図書館の利用者が，館内に設置されたキヨスク端末を用いて外部のWebサイトを閲覧する際に，利用者をShibboleth認証により識別し，その利用者ごとに定められたルールに従いアクセス制御を行うシステムの設計を行った。

現在はLDAPシステムにより認証を行うプロキシシステムが稼働しているが，以下のような問題がある。

1）学内構成員は，この端末を使うときと，電子図書館システムを使うときの２度認証が必要となる。このとき，同じ認証基盤を利用しているため，利用者は同じID同じパスワードを入力する。

2）学外の利用者においては，学外のサイトの閲覧を希望する際に，IDを申請しなければならない。また図書館側もIDの管理をしなければならない。

このシステムをShibboleth化することにより，１）の問題はシングルサインオン化されるため，利用者の不便さは解消される。また２）については，学認と連携することにより，学外利用者のID申請およびID管理が不要となる。

設計するシステムでも既存のシステムと同様にプロキシサーバのアクセス制御により，利用者によるキヨスク端末からのアクセスを制御する。プロキシサーバのアクセス制御はShibbolethにおける利用者属性について設定可能とする。これにより，役職や役割を意味するAffiliation, Entitlement属性について，「どのサイト（URLパターン）へのアクセスを許可/拒否するか」を記述することができる。また，ホワイトリストやブラックリストによる制御機能をもたせることにより，認証を受けることなくアクセスすることが許可するサイト（本学WebサイトやOPACなど）についての対応も可能となる。

平成21年度ではこのシステムの開発を行った。これらの研究は，平成21年度にシステム情報工学研究科で行われた，システム開発型特別プロジェクト　ICTソリューション･アーキテクト育成プログラムのプロジェクトとして遂行され，その成果を情報処理学会 インターネットと運用技術研究会において研究会発表を行った［1］。

４．おわりに

電子図書館システムに構築したシングルサインオン型の認証基盤について，その概要について述べた。また本学独自の取り組みとして，図書館内に設置されるキヨスク端末の利用者認証をシングルサインオン化するためのシステムの設計開発について述べた。今後は，このシステムを図書館のキヨスク端末に導入し，本学の認証基盤と連携させ，実証実験を行う予定である。

---

[1] https://upki-portal.nii.ac.jp/

[2] http://shibboleth.internet2.edu/

参考文献

［1］高田真吾，金子直矢，齊藤剛，佐藤聡，新城靖，中井央，板野肯三．UPKI認証連携基盤を用いたWebアクセス制御．情報処理学会研究報告2010-IOT-8, No.38, pp. 1-6, March 2010.