金沢大学における統合認証への取り組み

～　大学内統合認証から大学間連携まで　～

情報部情報企画課（総合メディア基盤センター）　松平　拓也

1 はじめに

インターネットの急速な普及により，多くの情報システムをオンラインで利用できる環境が整備されてきています．各情報システムにアクセスする際にはIDとパスワードを用いて認証を行い，本人確認を行うのが一般的です．しかしながら図1のように，ユーザが各情報システムで用いるIDとパスワードは，各システムで異なる場合がほとんどです．そのため，ユーザは多くのIDとパスワードの組を記憶していなければなりません．ユーザはIDとパスワードをポストイットやメモ帳などに記入したり，覚えやすいように簡単なものにしたりするために，情報システムのセキュリティ低下をもたらす原因となっています．

そこで金沢大学では「シングルサインオン」という技術を用いてこれらの問題を解決しようと試みています．さらに，最近では国立情報学研究所が大学間での認証連携を推進しており，金沢大学も積極的に参加しています．

以降，これらのことについて技術的に詳しく説明していきたいと思います．

2 シングルサインオン

シングルサインオン（SingleSignOn）とは，一度認証を行うだけで複数の情報システムに認証せずにアクセスできる機能を指します．

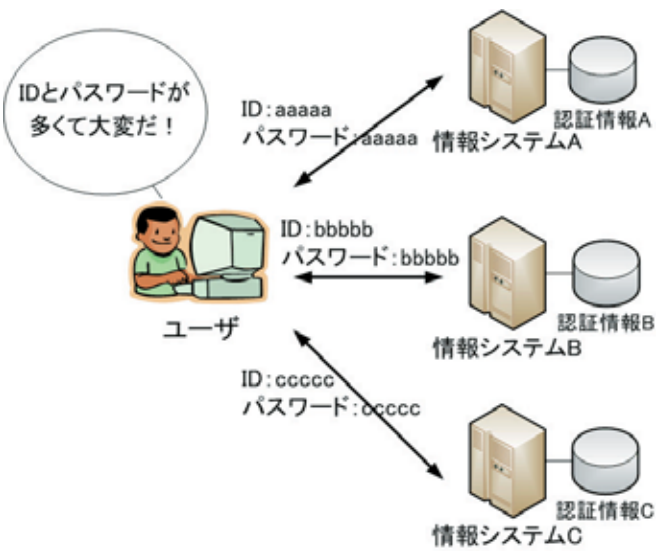

図1　従来の情報システムへのログイン

シングルサインオンを実現するためには，まず図2に示すように，各情報システムがもつ認証情報を統一する必要があります．

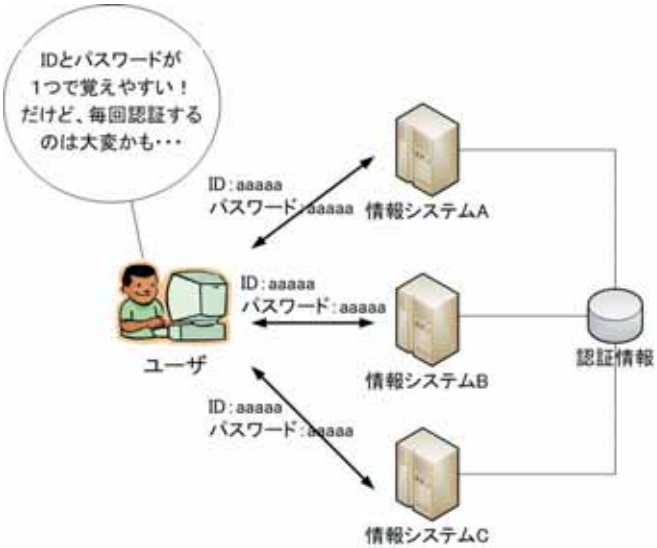

図2　認証情報を一元化した場合

このように，各情報システムに同一の認証情報を利用することにより，ユーザは一対のIDとパスワードを記憶しておくだけでよくなります．そのため，ユーザの利便性やシステムのセキュリティが向上します．しかし，ユーザは各情報システムにアクセスする度に毎回認証を行わなければいけません．

そこで，毎回認証する手間を省略する機能がシングルサインオンです．シングルサインオンを用いた認証の概念図を図3に示します．

ユーザがまず，情報システムAにアクセスすると仮定します．情報システムAにアクセスに行くと，認証サーバに転送されます．そこで，ユーザはIDとパスワードで認証を行います．認証に成功すると，情報システムAにアクセスできるようになります．その後，情報システムB，Cにアクセスに行っても認証を行うことなくアクセスすることができるようになります．

このようにシングルサインオンを利用することで，ユーザの利便性は飛躍的に向上します．また，情報システム管理者も，各システムで個別に認証情報を扱う必要が無くなり，負担が軽減されるメリットがあります．金沢大学では現在，情報システムのシングルサインオン化を推進しており，導入を検討しています．

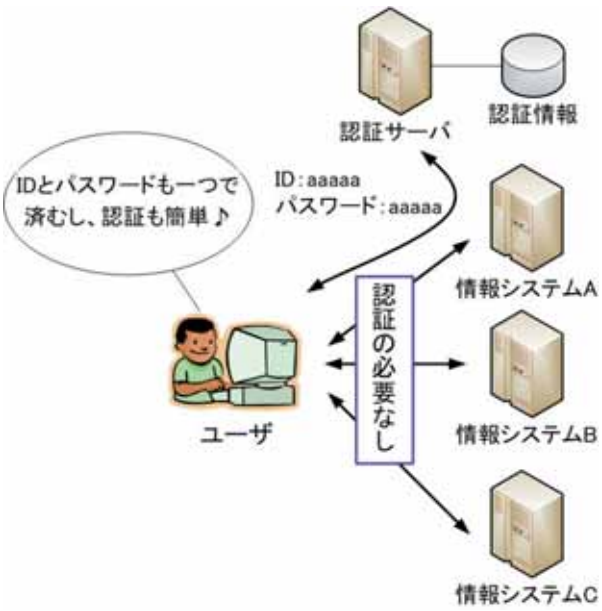

図 3　シングルサインオンによる認証

3 大学間ユーザ認証連携

国立情報学研究所（以下 NII）では，大学間ユーザ認証連携を推進しています．この活動は University Public Key Infrastructure（以下 UPKI）と呼ばれています．金沢大学は「UPKI 認証基盤によるシングルサインオン実証実験」に参加しています．参加の目的は，UPKI への貢献とシングルサインオンなどの技術要素の取得です．UPKI の仕組みを図 4 に示します．

A 大学所属のユーザ A が B 大学のサービスを利用したいとき，まず，ユーザ A は B 大学の情報システムにアクセスを試みます（①）．情報システムを Service Provider（以下 SP）と呼びます．SP は NII が管理している Discovery Service（以下 DS）にアクセスを転送します（②）．ユーザ A は DS から，自分の所属である A 大学の Identity Provider（以下，IdP）を選択します（③）．ユーザ A は IdP で自分の ID とパスワードで認証を行います（④）．認証に成功すると，IdP はユーザ A の情報を SP に送信します（⑤）．SP はその情報を基に，ユーザ A のアクセスを許可します（⑥）．

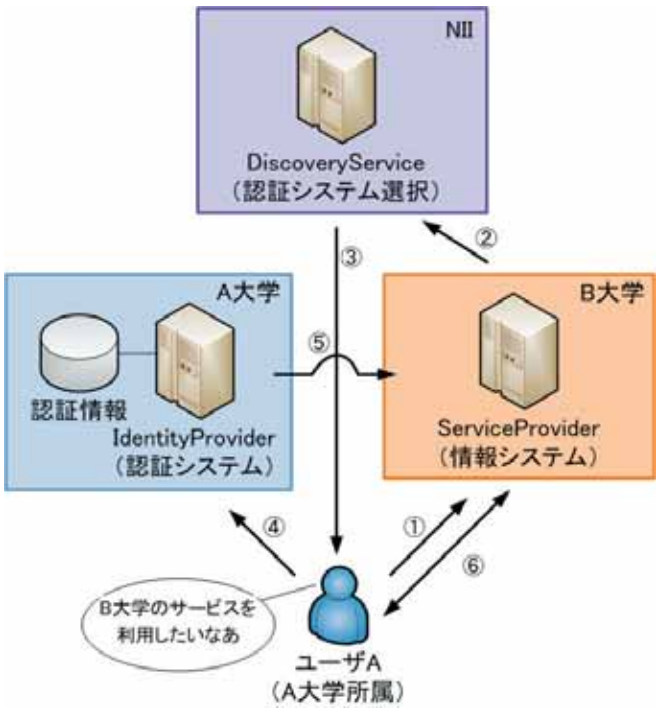

図 4　UPKIの概念図

現在金沢大学では，IdP を 1 台，SP を 2 台構築し，他大学との連携を実証実験中です．試験中の SP サンプル例を以下に紹介します（実験サイトのため非公開）．

■ ファイル送信サービス

ファイル送信サービス（https://imcsv1.kanazawa-u.ac.jp/sendfile-s/）は，メールでは添付できない大容量のファイルを送信するサービスです．現在は利用条件をメールアドレスが金沢大学のものに限定しています．実験サイトでは，送信時と受信時に自分が所属する大学の IdP で認証を受けることで，他大学のユーザでも，セキュアにサービスを提供できるようにしました．

■ デジタルコンテンツ公開サービス

学術情報部門では，図書館では取り扱わない各種デジタルコレクションや実験観測データのリポジトリ化を行っています（図 5）．その中のあけぼの衛星による地球周辺の電波観測データのスペクトル画像を，IdP で認証を受けることにより閲覧できるように構築しました．

図5　デジタルコンテンツ公開サービス

4 おわりに

金沢大学では情報システムのシングルサインオン化を進め，ユーザの利便性の向上を目指しています．
また，NII の UPKI を利用することで，他大学の構成員の身元が判別でき，大学間においてセキュアにサービスを提供できる環境の実現に向けて努力しています．

問合せ先：takusng@kenroku.kanazawa-u.ac.jp
情報部情報企画課（総合メディア基盤センター）　松平 拓也