独立した組織間での認証連携を実現

組織間の独立性を保ちつつ認証連携を実現できる Shibboleth を活用　　京都大学

本学では部局の独立性が強く、多くのシステムを各部局が独自に構築している。このような独立性の高い複数の組織をまたぐ認証連携機構を構築し、全学的なシングルサインオンを実現させるため、認証システムに Shibboleth を採用した。

課題

利用者の利便性を考え、本学では一組の ID・パスワードで複数のサービスを使えるようにする全学 ID による一元管理に加え、シングルサインオン（SSO）の導入にも積極的に取り組んできた。しかし、部局の独立性を重視するというポリシーがあり、全学 ID の利活用は進んでいるが、一部の部局独自の Web サービスでは従来通り認証処理は部局で行われており、部局独自サービスに対する認証処理のシステム投資や稼動軽減が進まないという課題があった。

そこで、これまで部局側で構築していた認証処理機能を Shibboleth を活用して全学のプライベートクラウド(PaaS)で提供することを進めている。

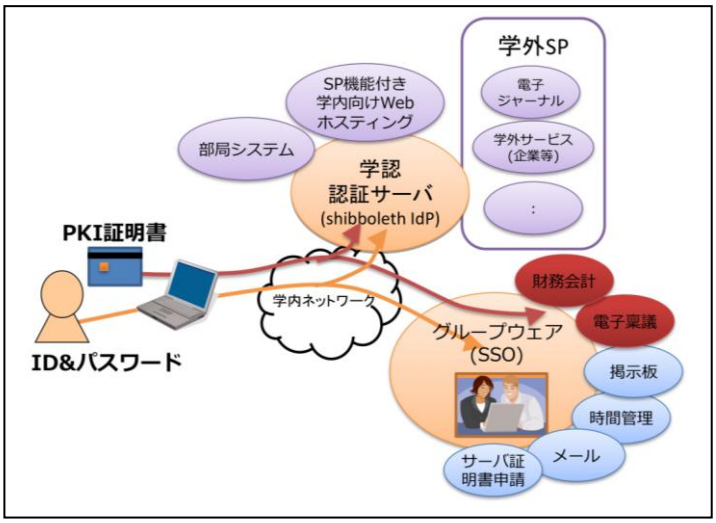
また、Web サービスに要求されるセキュリティレベルにより、パスワード認証と電子証明書認証など多要素認証の機能が必要と考えている。

解決策

本学では、学内外で提供される多種多様な Service Provider（SP）に対応できる統合的で柔軟な認証基盤の構築を目指し、全学的な認証連携機構として Shibboleth の採用を決定した。Shibboleth を採用する理由の 1 つに、異なる組織間で認証連携する場合でも、個人を特定できる情報を外部に出すことなく安全な認証連携を実現できるセキュリティの高さがある。他にも、今まで SP 側で用意していた認証処理が省けるといったメリットもある。

しかし、Shibboleth による認証連携の立ち上げには設定・改修に関わるノウハウが必要になり導入は決して簡単ではない。部局の負担軽減と全学的な SSO 環境を構築するため、本学で実運用している Web ホスティングサービスに、あらかじめ SP 機能をインストールして提供するオプションを追加した。このオプションを利用して、京都大学の 2 つの部局で Shibboleth SP 対応で認証処理を運用している。

本学では学術認証フェデレーション（学認）の実証実験段階から参加しており、Shibboleth による認証連携機構の構築ノウハウを蓄積してきた。現在は運用フェデレーションにも参加し、学認が提供するサービスも利用している。



結果

本学では全学 ID による Web サービスの提供を進めており、セキュアなサービスについては IC カードによる認証を実施している。また、部局独自サービスについても全学 ID の利活用を進めているが、ケースによっては開発投資抑制や運用稼動低減の観点から、Shibbaleth 認証連携の利用を推奨している。現在、基本的な Shibbaleth 認証連携の技術・ノウハウの蓄積をほぼ完了し、電子ジャーナルも含めたサービスの運用に供している。

セキュアなサービスに対する IC カードによる多要素認証などの利用も行っているが、Shibboleth 認証連携でも高セキュアなサービスも当然出てくる。現在、Shibboleth IdP に対して IC カード内の電子証明書認証を追加する方法を検証している段階である。

総じて、学認に参加する他大学との情報交換を通して積極的に全学的な認証基盤の構築を進めていきたい。

（京都大学　学術情報メディアセンター　古村 隆明）