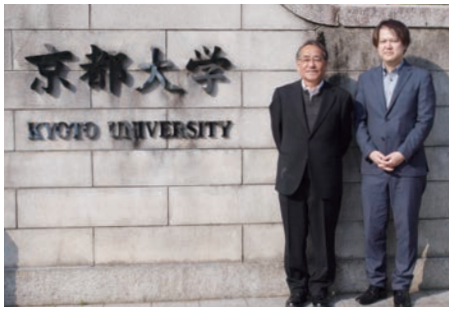
シングルサインオン製品「OpenAM」導入事例



国立大学法人 京都大学 様

Shibbolethに対応困難なシステムも OpenAMの活用によりシングルサインオンを実現

我が国、そして世界を代表する大学として、質の高い高等教育と先端的学術研究を推進している京都大学。同大学は、サーバーの更新のタイミングで、オンプレミスで運用していた各種業務システムをクラウド上へ移行することになりました。これに合わせて教職員向けグループウェアの更改や認証基盤の見直しを進めることになったのですが、一部の業務システムが学術認証フェデレーション（Shibboleth<シボレス>）が提供するSAML（認証連携）に対応できないことが判明しました。そこでオープンソース・ソリューション・テクノロジ（以下、OSSTech）の「OpenAM」を導入し、これを認証ハブとして利用することで、統合化されたシングルサインオンの仕組みを実現しました。これによりセキュリティが強化されるとともに、教職員の利便性が高まりました。

課題

学術認証フェデレーション（学認：Shibboleth）のSAML（認証連携）に対応できない業務システムも、シングルサインオンさせたい

解決

OpenAMを認証ハブとして利用し、統合化されたシングルサインオンの仕組みを実現

一部の業務システムが学認（Shibboleth）の認証連携方式（SAML）に対応できない

1897年の創設以来、自由の学風のもとで対話を根幹とした自主独立と創造の精神を涵養し、多元的な課題の解決に挑戦してきた京都大学。これまでにも社会の各方面で活躍する人材を数多く輩出しており、ノーベル賞受賞者もアジアの大学で最多となる10名（2019年度4月1日現在）を数えています。

さて同大学では、組織改革の一環として2005年4月に情報環境機構を設置しました。そのミッションについて情報環境機構 IT企画室 室長の永井靖浩氏は「情報環境機構はいわばバーチャルな組織で、専任の教員約10名からなるIT企画室と、企画・情報部に属する事務職員および技術職員によって構成されています。これらが一体化して活動することで、京都大学全学のITサービスの企画・設計・運用を担っています」と説明します。

情報環境機構では、財務会計システムや教務情報システム、人事給与システム、健康管理システムといった全学で利用する業務システムを、“事務用汎用コンピュータ”としてまとめて運用しています。以前は、システムごとに独立した物理サーバーでそれぞれ運用していましたが、2014年にサーバーを集約・仮想化。その後、サーバー機器の次期更新のタイミングで、業務システムサーバーの信頼性・可用性の向上、効率的なバックアップの確保、事業継続計画・災害復旧(BCP/DR)対策の強化などの観点から、一部の機微なデータを扱うサーバーを除き、学外のクラウド(IaaS)への移行を決定しました。

またこれに合わせ、教職員向けのグループウェアとして長年利用してきたNotes/Dominoも新たなものへ切り替えることにしました。企画・情報部 情報基盤課 業務システム管理掛（兼）情報環境機構 IT企画室の宮部誠人氏は「これまで様々な作り込みを行い、利便性を高めてきましたが、Webを利用したグループウェアの技術的進歩は著しく、SaaS化の流れも進んでいることから、一新すべき時が来たと判断しました」と語ります。

業務システムのクラウド化とグループウェアの更新に際し、問題となったのが認証です。情報環境機構ではNotes/Dominoを導入した2005年に、シングルサインオン実現のためTivoli Access Manager（以下、TAM）を導入。また2010年にはICカード／電子証明書の認証の仕組みも取り入れるなど、全学共通の認証基盤を構築してきました。

一方で、2010年度より、学術認証フェデレーション「学認（GakuNin）」の提供が始まり、これを全国の大学や研究機関などが採用するようになったことから、同大学も学生向けシステムや図書館システムなどで利用を開始しました。

京都大学
KYOTO UNIVERSITY

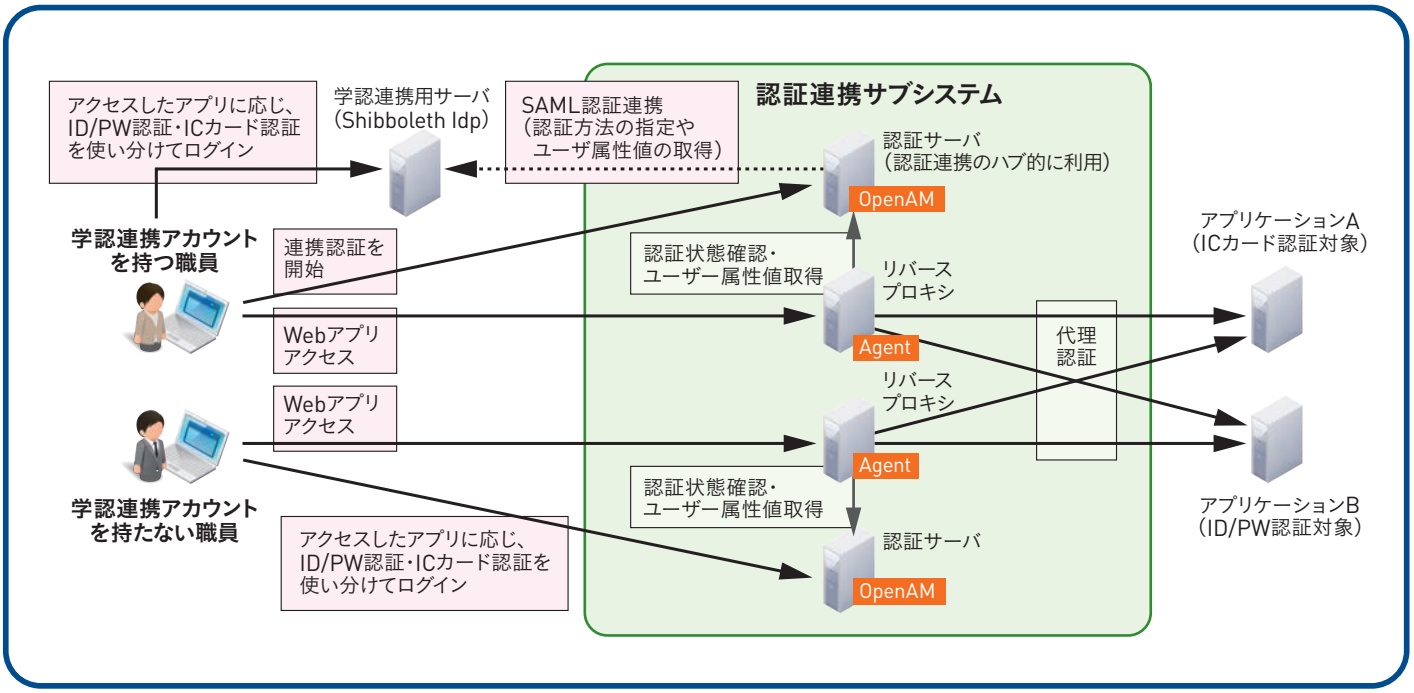
大学名：国立大学法人 京都大学
学長：山極 壽一
創設：1897年6月
教職員数：5,480名
学生数：学部13,227名、大学院9,427名
（2018年度5月1日現在）
組織：総合人間学部・文学部・教育学部・法学部・経済学部・理学部・医学部・薬学部・工学部・農学部の10学部、18の大学院・専門職大学院、13の附属研究所

お話をうかがった皆さん

情報環境機構
IT企画室 室長
教授
永井 靖浩 氏

企画・情報部 情報基盤課
業務システム管理掛（兼）情報環境機構
IT企画室
掛長
宮部 誠人 氏

導入事例：国立大学法人　京都大学様



「教職員向けグループウェアや一部の業務システムはTAMでの運用を続けていましたが、今回、グループウェアを切り替えることになったためTAMを使い続ける必然性もなくなり、全面的に学認へ切り替えることにしたのです」（永井氏）

ところが、システム更新の準備を進めていく中で、これまで運用してきた業務システムのうち、一部のシステムが学認で使用しているShibbolethの認証連携に対応できないことがわかったのです。そこで同大学では、今回の調達に際し、仕様書の中にそれらのシステムのシングルサインオンへの対応を盛り込むことにしました。

OSSTechのOpenAMを活用し統合化されたシングルサイオンを実現

2018年2月、京都大学は事務用汎用コンピュータの入札公告を掲示。その結果、株式会社アルゴグラフィックスが落札しました。同社が提案した内容は、オンプレミスで運用している仮想サーバーをAWS上へ移すというもので、懸案だったシングルサインオンについては、基本的にShibbolethとSAMLでアプリケーションと接続、SAML対応が難しい一部のシステムは、オープンソースのシングルサインオン製品「OpenAM」を認証ハブとして利用し、リバースプロキシ方式でアプリケーションと接続することで、統合化されたシングルサインオンの仕組みを実現しています。OpenAMはハブとしての用途だけでなく、学認アカウントを持たない職員への認証基盤としても利用しています。

この提案を行うに際しアルゴグラフィクスでは、OpenAMを取り扱っているベンダーの中からOSSTechをパートナーに選びました。同社はその理由として、対応したエンジニアの技術レベルが高いだけでなく、問い合わせへのレスポンスが早かったこと、さらに大学や研究機関などへの導入実績も豊富だったことを挙げています。

構築は大きなトラブルもなく進み、2018年8月には認証基盤の仕組みが稼働し、事務用汎用コンピュータ全体がサービスインとなる2019年2月までの間も、認証基盤に関しての支援が手厚く行われました。

OpenAMの柔軟性に期待

京都大学では、2019年2月よりグループウェアを含めすべての業務システムの運用を開始しています。

「グループウェアについては、職員は業務上の必要もあって以前から利用率が高かったのですが、一方で教員にはあまり利用されてきませんでした。理由はいろいろと考えられますが、今回、統合化された認証が実現したことで、教員の利用が増えることを期待しています」（永井氏）

今回のプロジェクトにより、全学共通のシングルサインオンが実現しましたが、まだまだ取り組むべきテーマがあるといいます。

「近年、サイバー攻撃がますます高度化・巧妙化する中、IDとパスワードだけでは安全を担保できなくなりつつあります。そこで、将来的には多要素認証の導入やマイナンバーカードの活用なども検討していますが、そうした仕組みづくりにもOpenAMなら柔軟に対応できそうなので、うまく使っていきたいと考えています」（永井氏）

最後に、OSSTechについて宮部氏は「OpenAMの機能的にはSAMLの範囲を広げてほしいという思いもありますし、活用方法の提案などもいただきたいですね」と期待を語ってくれました。

今回の導入製品

●OpenAM

OSSTech　オープンソース・ソリューション・テクノロジ株式会社　Open Source Solution Technology Corporation
〒141-0031 東京都品川区西五反田1-29-1 コイズミビル 8F　Tel:03-6417-6753　https://www.osstech.co.jp　info@osstech.co.jp