賛助会員だより

サイオステクノロジー株式会社

認証基盤の統合とクラウド化
～自治医科大学への導入～

■認証基盤の複雑化を解消

自治医科大学では2020年４月、認証サーバー群を刷新すると同時にそれまで複数あった学内のID管理システムを一つの基盤に統合。オンプレミス環境でなくクラウドサービス「Microsoft Azure」上に構築し、稼働を開始しました。

学内外の様々なシステムには、教職員や学生などのユーザーが正当であるかを確認する、認証プロセスが欠かせません。従来は各システムがそれぞれユーザーIDやパスワードなどの認証情報を管理しており、ユーザーはシステムごとに異なるIDやパスワードを入力する必要がありましたが、近年では、一度の認証で複数のシステムにログインできるSSO（Single Sign On）が普及してきています。

自治医科大学でも、複数の認証基盤が存在し、それぞれが個別にIDを管理していました。

一つは、図書館管轄の認証システムで、このシステムが学認（学術認証フェデレーション）への認証連携も担っていました。それに対し、主に教職員が使うワークフローシステムや、そのワークフローを支えるクラウドサービス「G Suite」の認証を行うのは、電算課（現：情報システム課）の管轄で2013年に構築された別の認証システムです。さらに、その後に導入された「Office 365」でも、個別に認証を行っていました。

この課題を解消すべく、ワークフローやG Suiteと連携する認証基盤の構築や運用を手掛けた、サイオステクノロジーがSSOを支援することとなりました。

■認証サーバーをクラウド基盤上に構築

情報システム課は当初、認証サーバー群を学内データセンターに設置し運用することを検討していましたが、サイオステクノロジーはクラウド基盤上での構築・運用を提案しました。クラウド化によるメリットは、クラウド事業者が提供する機能を生かした運用性の向上です。例えばバックアップ機能は、認証基盤を構成する各サーバーのバックアップ作業を自動化できます。また、アクセス集中やサーバーの部分的な障害に備え、冗長化したサーバーを効率的に利用するためのロードバランサーも、調達や設定、運用の負担がほとんど不要となります。

ただし、認証基盤をクラウド化するには、学内データセンターのサーバー群と認証連携を行うための通信経路も考慮する必要があります。自治医科大学では、独自のセキュリティポリシーとして、G SuiteやOffice 365などクラウドサービスとの認証連携にも、学内データセンターを経由する方針だったため、この経路には高速で、セキュリティや信頼性の高い回線が必要になります。

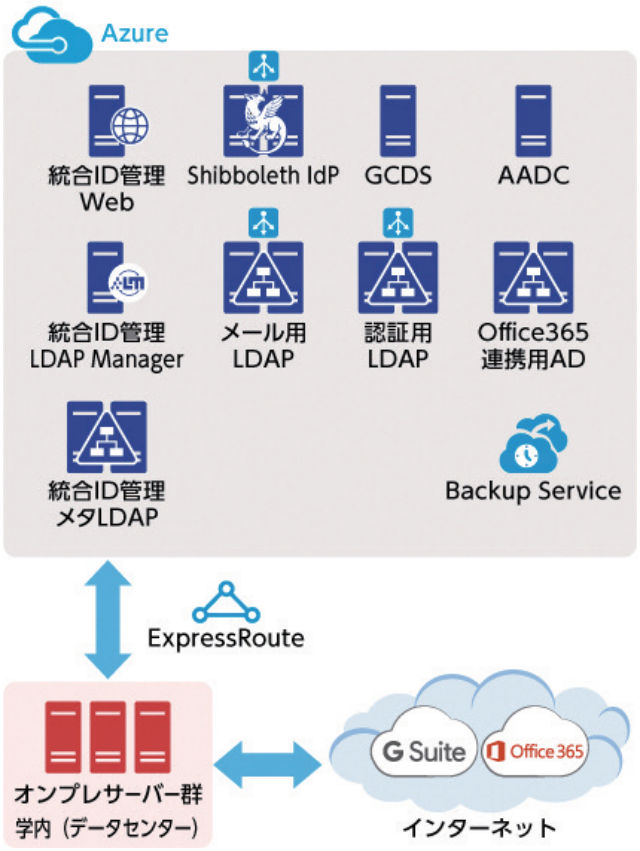

図１　自治医科大学の認証基盤システム環境の概要

この要件に対して、サイオステクノロジーでは、「Microsoft Azure」が持つ仮想プライベートクラウド接続サービス「ExpressRoute」を活用することを提案。これにより、高速で、通信量あたりのコストも抑えられ、信頼性やセキュリティの面でも有利となります。

こうして、2020年４月に稼働を開始する計画で、Azureの採用を決定しました。

■利用者の利便性が向上、今後の拡張も容易に

新たな認証基盤システムの構築は2019年秋から開始。サイオステクノロジーはAzure環境のサーバー構築・運用に豊富なノウハウを有しており、大きな不具合もなく、計画どおり2020年４月から稼働しました。

新たな認証基盤を構成するのは、合計14台の仮想サーバーです。各サーバーは、いずれもAzureの「Azure Backup Service」によりバックアップされているほか、負荷分散や障害対策のため並列化されている一部のサーバーにはAzureの仮想ロードバランサー「Azure Load Balancer」が適用されています。これらの機能の活用で、運用の負担は、想定していたとおり大幅に軽減されました。

認証基盤の中核となるのは「統合ID管理LDAP Manager」で、複数の認証基盤で管理されていたユーザー情報がすべて集約されています。複数のシステムにあった、同一人物が持つユーザー情報を正しく見極め結合させる「名寄せ」の作業も、サイオステクノロジーが支援しました。その他のサーバーは、学認との認証連携に使われるミドルウェア「Shibboleth」のサーバーや、メールサーバーとの認証を行うサーバーなど、各システムとの連携を担います。Office 365との連携には、専用のActive Directory（AD）サーバーと、連携を司る「Azure Active Directory Connect（AADC）」という２組のサーバーが用意されています。

認証情報を集約したことで、教職員や学生は単一のID・パスワードの組み合わせで学内外のシステムを利用できるようになり、利便性が大きく向上しました（メールのみ、セキュリティポリシーにより別のパスワードが必要）。

また、新たな認証基盤ではID管理が完全に情報システム課の管理下に置かれるため、セキュリティ統制の強化にも寄与しています。

さらに、LDAP、AD、Shibbolethのすべてに対応できる基盤となり、認証にまつわる新たな取組みが進めやすくなりました。今回の導入は今後の変革への基本となる認証基盤と言えるでしょう。

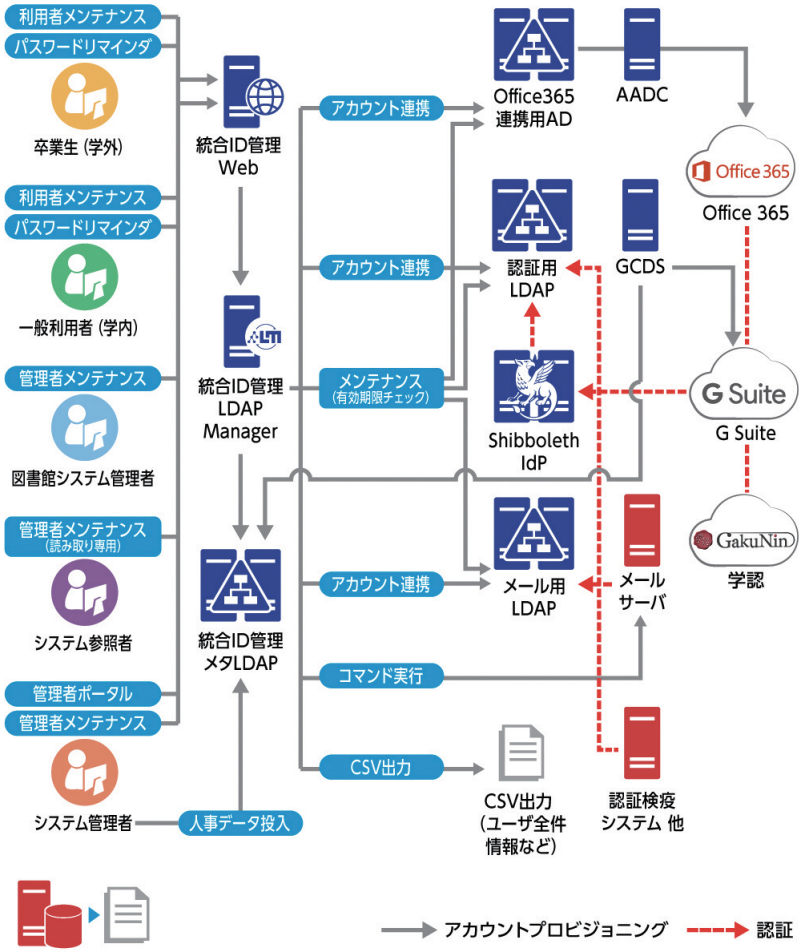

図２　認証基盤のシステム構成

問い合わせ先

サイオステクノロジー株式会社
プロフェッショナルサービスSL
TEL：03-6401-5189
Mail：ps-info@sios.com
URL：https://sios.jp/