認証サーバアプライアンス

AXIOLE

Authentication Services' Platform

CaseStudy

NetSpring AXIOLE 導入事例

業種：教育機関 Vol.04

札幌学院大学

学内認証基盤の学認への接続にAXIOLEを導入しeduroamアカウント発行の運用を改善した札幌学院大学

MISSION

- 学術認証フェデレーションへの接続に必要な認証基盤整備
- 対象システムごとに構築した認証システムの相互連携
- 認証システムに求められるセキュリティと可用性の確保

SOLUTION

- 学術認証フェデレーションに準拠したAXIOLE IdPを採用
- LDAP連携機能を使い管理用認証サーバの情報を自動反映
- アプライアンス製品ならではの安定性と容易なセキュリティ対応

導入の経緯

大学が相互に認証連携を実現する仕組みとして、学術認証フェデレーション（以下、学認）やeduroamがある。学認は、自身の所属大学のIDとパスワードを使って他大学や商用のサービスをシングルサインオンで利用する仕組み。技術ベースとなっているのはShibboleth認証だ。またeduroamは参加大学間で無線LANを相互利用可能にするもの。技術基盤にはIEEE802.1X認証が採用されている。

2012年より札幌学院大学はeduroamに参加しており、IDやパスワードの管理には東北大学が作成したeduroam代理認証システムを活用している。希望者には利用申請書を提出してもらい、管理者が代理認証システムにログインしてIDを発行していた。「申請が来るたびにID発行の操作をしなければならないので、運用面での負荷が課題でした。（情報処理課長松本賢彦氏）」

導入決定のポイント

転機となったのは2014年。学内のPC教室にMacを導入し、Mac向けとWindows向けに認証基盤を再整備することになった。そのタイミングで認証システムも見直されることになった。eduroamでは国立情報学研究所が学認のSP（サービスプロバイダー）として、学生や教員が自らeduroamのアカウントを発行できるeduroam仮名アカウント発行システム（現：eduroamJP認証連携IDサービス）を提供しているが、札幌学院大学は当時学認に参加していなかった。

「学認に参加し、認証基盤を独自にIdP（アイデンティティ・プロバイダ）として接続するにはノウハウが必要ですが、これをアプライアンスとして提供していたのがAXIOLE IdPオプションでした。他大学で既に導入が広がり始めており、実際に使っている先生たちに聞いたところクチコミも上々だったので採用を決めました。（情報処理課原田寛之氏）」

学認への参加により、学生や教員が自らShibboleth認証にてeduroam仮名アカウント発行システムにログインし、アカウントを発行できるようになるので、従来の運用と比べて管理者の負担を大幅に削減できる。紙の申請書は不要になり、出先で急に使いたくなったとしてもその場で申請できるなど、ユーザーの使い勝手も向上すると期待された。AXIOLEはLDAPベースの認証アプライアンス製品であり、単独でLDAPやRADIUS認証を行わせることも可能であるが、eduroamのRADIUS proxy等は既に札幌学院大学で問題なく運用されていたためIdPオプションで既存のLDAPサーバをそのまま学認に接続する機能に特化して利用することができることが大きなポイントとなった。

導入企業

SGU

札幌学院大学

大　学　名：札幌学院大学
学　　長：鶴丸　俊明
開　　学：1946（昭和21）年
学　生　・
教職員数：学生約2,400名、教員約110名、
　　職員約80名
キャンパス：
［第1キャンパス］北海道江別市文京台11番地
［第2キャンパス］北海道江別市文京台63番地

http://www.sgu.ac.jp/

1946年に開学した札幌文科専門学院を前身とし、第二次大戦後に生き方を模索する若者を導くために生まれた札幌学院大学。開学時に掲げられた建学の精神―「学の自由」「独創的研鑽」「個性の尊重」―に込められた息吹きと気概は、その後、学園が札幌短期大学、札幌商科大学そして札幌学院大学へと発展する歴史を通して脈々と受け継がれている。

札幌学院大学
情報処理課長
松本　賢彦 氏

札幌学院大学
情報処理課
原田　寛之 氏

NetSpring

学術認証フェデレーションへの接続を容易に実現
４年以上の運用で確信した使い勝手と機能

安定性とセキュリティの高さは アプライアンス製品ならでは

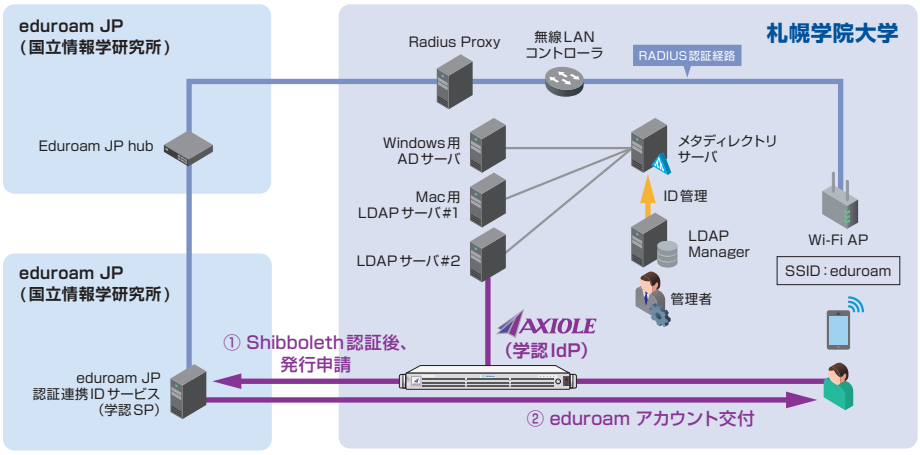
札幌学院大学が2014年に導入したのはAXIOLE IdP専用モデルの仮想アプライアンス版で、学認へのIdP接続や学認SPの接続など導入時の設定はSIerが担当した。その後自分たちで設定の追加や変更を行ったが、わかりやすいWebUIが用意されているので悩むことはなかったという。

導入から取材まで4年以上が経過していたが、その間の運用を通じてアプライアンス製品ならではのメリットも実感できた。「認証技術は共通規格なので、汎用サーバで作り込むこともできます。しかし汎用サーバではOSや認証システムのセキュリティを常に気にしなければなりません。アプライアンス製品ならそうした脅威への対応も、ファームウェア更新だけで対応できます。学認の仕様がShibboleth2からShibboleth3へ変わったときも、対応するファームウェアを導入して設定をチェックしただけで移行対応できました。安定性の高さも、運用者としては嬉しいポイントですね。アップデート以外では止めたこともありません。（松本氏）」

誰にでも安心して引き継げる 認証基盤の構築を実現

AXIOLE導入時に再構築した認証基盤は、複数の認証サーバから成り立っている。PC教室で使われるWindows用LDAP認証サーバ、Mac用LDAP認証サーバ、それに加えて学認用LDAP認証サーバの３系統。これらを個別に管理するのは手間がかかるだけではなくセキュリティの観点からも好ましくない。そこでこれらを統合管理するメタLDAPサーバを設置し、各認証サーバはメタLDAPサーバの情報を参照するよう設定されている。「LDAPサーバを直接操作することはなく、普段のID管理にはLDAP Managerを使っています。大学では毎年１学年分の学生データが入れ替わりますが、LDAP ManagerにCSVで一気に読み込み、各認証サーバに自動反映されるよう設定しています。（原田氏）」

構築時のコンセプトは、担当者が変わってもID管理業務に支障が出ないこと。担当者の異動などで管理者が変わることは、どのような業務でも起こりえる。そのときに後任がLDAP、ActiveDirectory、Shibbolethのすべてに精通している人とは限らない。フロントUIとしてLDAP Managerを採用したのも、Shibboleth認証が必要な学認への接続にAXIOLEを選んだのもそうした考えに従ったものだ。アプライアンス製品なら、Shibboleth特有の知識がなかったとしても、運用やトラブルシュートにベンダーのサポートを得られる。



リース期間満了後も続投を決定 ４年以上の運用で確信した使い勝手と機能

2014年の導入からもうすぐ5年。リース期間の終了が迫っているが、AXIOLEを引き続き利用していくことは決定しているという。2021年には新札幌に新しいキャンパスを開設する予定になっている。新キャンパスのセキュリティも、AXIOLEが担っていくことになるようだ。

現状の構成に充分満足しているようだが、管理対象となるアプリケーションが増えた場合に使えるセキュリティ強化オプションが用意されているので、安心して続投を決められたようだ。「ワンタイムパスワードなど多要素認証の機能については、現状では利用予定はないものの、SAML対応のアプリケーションが学内に増えた場合など、セキュリティ強化が必要になった際にすぐに対応できるのは安心感があります。現在は学内だけに閲覧を限定している電子ジャーナルを自宅から見たいというような要望が出てきたとしても、すぐに対応できますから。（原田氏）」

【製品ホームページ】http://www.axiole.jp/

開発元
NetSpring®
株式会社ネットスプリング
http://www.netspring.co.jp お問い合わせ先 E-mail:info@netspring.co.jp
本社 〒108-0073 東京都港区三田3-12-16 山光ビル2F
TEL.03-5440-7337 FAX.050-3737-1458 サポートセンター TEL.050-5536-4841

お問い合わせ