京都大学における Shibboleth IdP の IC カード対応と災害対策の取り組み

中井 隆史 [1)], 針木 剛 [1)], 片桐 統 [1)], 石橋 由子 [1)]

1) 京都大学 情報環境機構

ninsho-staff@iimc.kyoto-u.ac.jp

IC Card Authentication and Disaster Recovery of Shibboleth IdP in Kyoto University

Takashi Nakai [1)], Tsuyoshi Hariki [1)], Osamu Katagiri [1)], Yoshiko Ishibashi [1)]

1) Institute for Information Management and Communication, Kyoto University.

概要

京都大学では Shibboleth IdP を用いて情報システムの認証処理の集約とシングルサインオンの実現に取り組んでいる。教職員用システムについては財務会計システムや人事系システムで利用している安全性の高い IC カード認証の実現が課題となっていた。Shibboleth IdP の IC カード対応に取り組み、2018 年度に主要な教職員用システムとの連携を実現した。また、Shibboleth IdP を運用してきた吉田キャンパスが被災すると同時に多くの情報システムが利用できなくなる懸念への対策として、Shibboleth IdP の遠隔地(関東)のデータセンターへの移行に取り組んだ。結果として京都大学の主要キャンパスである吉田キャンパスの被災時にもメール等のサービスが利用継続できる可能性を向上できた。

1 はじめに

京都大学では教職員や学生など教育・研究・業務等の活動を行う構成員に対し、全学アカウントと IC カードを提供し活用している。教職員向けに提供している認証 IC カードには特別に接触 IC チップに記録したクライアント証明書による個人識別機能があり、財務会計システムや人事系システムの一部の重要な教職員用システムにおける安全性の高い認証として利用している。また、LDAP と Shibboleth IdP を中心とした統合認証基盤の運用を 2010 年に開始し、構成員が使用する情報システムの認証処理の集約とシングルサインの実現に取り組んでいる。

学生用システムについてはシングルサインオンの利便性を目的に Shibboleth IdP 対応を進めてきた。一方で、教職員用システムについては独自の認証システム(Tivoli Access Manager: TAM)を利用しており、他の情報システムとの間でシングルサインオンできない状況となっていた。IC カードを用いた認証方法の可否が教職員用システムの Shibboleth IdP 対応が進まなかった理由の一つであった。2018 年度に教職員メール、グループウェア等の教職員用情報システムの多くがリプレース時期を迎えたことに合わせて、Shibboleth IdP の IC カード対応に取り組み、2018 年 8 月に本番環境での利用を実現した。結果として多くの教職員用システムの認証処理を Shibboleth IdP に集約し、シングルサインオンの実現と TAM の廃止を行うことができた。

一方、Shibboleth IdP に認証機能を集約するということは、Shibboleth IdP の利用不能になると多くの情報システムが使用できなくなることを意味している。京都大学では中期目標・中期計画に防災機能強化を掲げており、情報インフラのサービス継続は非常に重要な課題である。Shibboleth IdP については、2010 年の運用開始から京都大学のメインキャンパスである吉田キャンパス(京都府京都市)で稼働させてきた。そのため、吉田キャンパスが被災した際に長期にわたって Shibboleth IdP を利用する多くの情報システムが利用できなくなることが懸念されてきた。そこで遠隔地(関東)のデータセンターに新たに構築した Shibboleth IdP へ 2018 年 8 月に移行し、吉田キャンパスをスタンバイ環境とするように構成の変更を行った。京都大学では教職員メール/学生メールを始めとしてクラウドサービス利用が進んできている。今回行った Shibboleth IdP の災害対策によって、吉田キャンパスの被災時にも、これらの情報サービスの利用を継続できる可能性を向上することができた。

本稿では京都大学の Shibboleth IdP の IC カード対応と災害対策の取り組みについて紹介する。

2　統合認証基盤

2.1 全学アカウント

京都大学では全学アカウントを構成員に提供し、情報システムの認証等に利用している。全学アカウントには教職員向けの SPS-ID と学生向けの ECS-ID の 2 種類がある。2019 年 9 月時点の全学アカウントの内訳を表 1 に示す。

表 1 全学アカウントの種類と発行数

種類	発行対象	発行数
SPS-ID	教職員	約 13,000
ECS-ID	学生	約 24,000
	名誉教授 学振特別研究員等	約 3,000

ECS-ID は、学生に加えて名誉教授や学振特別研究員等の SPS-ID の付与対象でない構成員も対象としている。

2.2 IC カード/電子認証局

SPS-ID 対象者には認証 IC カード、学生には学生証、その他の構成員には必要に応じて施設利用証の 3 種類の IC カードを提供している。IC カードに搭載している IC チップと発行数を表 2 に示す。

表 2　IC カードの搭載 IC チップと発行数

種類	非接触チップ	接触チップ	発行数
認証 IC-カード	○	○	約 13,000
学生証	○	×	約 24,000
施設利用証	○	×	約 4,000

非接触 IC チップを利用した共通の機能として Felicitous Common use Format (FCF)に対応した学生番号や教職員番号、氏名等の情報提供機能を有している。施設立入管理や講義出席確認などに利用している。

教職員用の認証 IC カードについては、接触 IC チップを搭載し、個人識別可能なクライアント証明書を記録している。クライアント証明書を利用するためには接触式カードリーダーと利用者本人が登録した PIN の入力が必要である。クライアント証明書の発行・失効は専用に運用しているプライベート電子認証局で行っている。財務会計システムや人事系システムの一部の重要なシステムの認証に利用している。

2.3 Shibboleth IdP と LDAP

本稿の取り組みによる構成変更を行った 2018 年 8 月以前の統合認証基盤から Shibboleth IdP に関連するシステムを抜粋した構成図を図 1 に示す。拠点内の冗長構成は省略している。

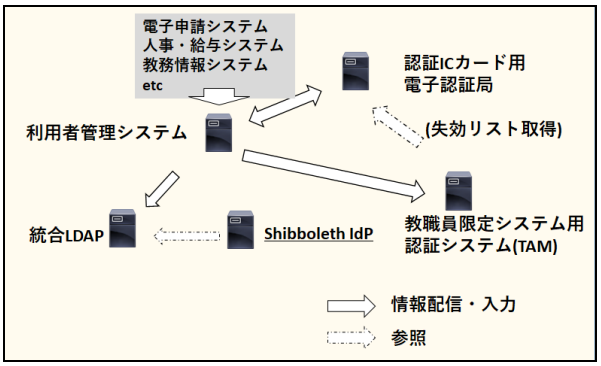

図 1 統合認証基盤システム構成図
(2018 年 8 月以前)

SPS-ID に関する申請用の電子申請システムや人事・給与システム、教務情報システム等から提供される在籍・離籍情報や氏名、学籍番号・教職員番号等を元に利用者管理システムが全学アカウントの発行や失効、属性情報の管理と配信を行う。利用者管理システムは LDAP サービス(以下、統合 LDAP)に全学アカウントと属性情報を配信する。Shibboleth IdP は統合 LDAP を参照することでパスワード認証と属性情報の取得・送信を実現している。学内の情報システムは Shibboleth IdP もしくは統合 LDAP の利用することで全学アカウントによる認証と属性情報取得ができる。

なお教職員グループウェアや財務会計システムといった教職員用システムの多くは 2017 年時点では IC カードに対応していた Tivoli Access Manager (以下 TAM)を認証システムとして利用していたため、Shibboleth IdP のシングルサイン環境にはログインできなかった。2018 年度に行われた教職員用情報システムの更新では原則 Shibboleth IdP で認証処理を行わせると方針とされた。次章で述べると取り組みなどの結果、TAM の維持は不要と判断され 2019 年 2 月に廃止された。

3 Shibboleth IdP に関する取り組み

3.1 認証 IC カード対応

教職員用情報システムを Shibboleth IdP に対応させる上での課題の一つに、TAM で処理されていた認証 IC カードを用いた認証の実現があった。認証 IC カードのクライアント証明書は、利用時にカードリーダーや PIN 入力が必要な点を除くと、ブラウザにインストールされた通常のクライアント証明書と同様に動作する。そのため学認技術ガイドにて公開されている情報[1]を参考に認証 IC カード用電子認証局に関する設定を行うことで認証 IC カードを利用した認証が可能な状態にできた。

ただし、検証を開始した 2017 年度時点で京都大学が運用していた Shibboleth IdP バージョン 3.2 では一部の操作を行うと処理が進まなくなる不具合が見つかり解決には至らなかった。その後、バージョン 3.3 で改善を確認できたため、Shibboleth IdP のバージョンアップ(3.2⇒3.3)や設定の組み込み等の本番環境への導入準備を進め、2018 年 8 月に本番環境で認証 IC カードの利用が可能になった。2018 年 12 月に財務会計システム等の認証処理が Shibboleth IdP に移されたことで本格的な利用が始まった。

利用の本格化後に認証エラーの原因調査が難しいという課題に直面した。学認技術ガイド[1]を参考にした構成・設定をそのまま行うと認証 IC カード(クライアント証明書)の認証エラーの多くは Apache HTTP Server のログに SSL/TLS のネゴシエーションエラーとして記録される。しかし、デフォルトの LogLevel である warn では認証エラー時に使用されたクライアント証明書の情報が記録されず、ユーザーからの問い合わせに対して該当するログの抽出が困難であった。そこで京都大学では LogLevel を図 2 のように設定し、SSL/TLS 関連のみ LogLevel を debug にすることで、サイズの増加を押さえつつ記録される情報を増やすことで対応している。これによってログの抽出と原因調査のための分析が可能になった。

```
LogLevel warn ssl:info
```

図 2 Apache HTTP Server の LogLevel

3.2 災害対策

Shibboleth IdP の災害対策として、遠隔地(関東)のデータセンターに新たに環境を構築し、2018 年 8 月にそれまでの吉田キャンパスで運用していた環境から移行した。移行後の統合認証基盤のシステム構成を図 3 に示す。

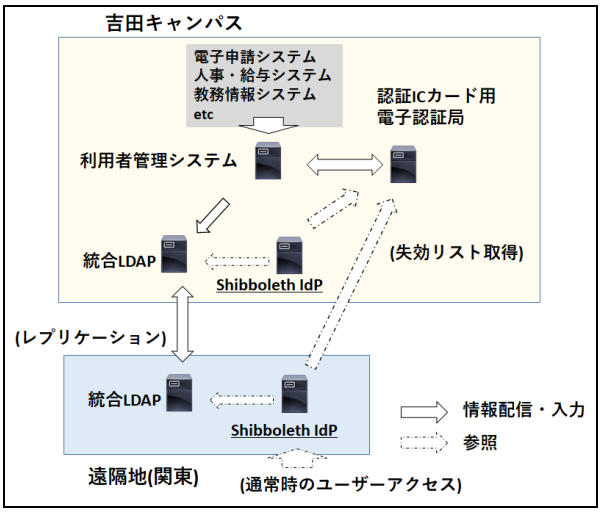

図 3 統合認証基盤システム構成図
(2018 年 8 月以降)

吉田キャンパスの環境は遠隔地(関東)への移行後も DNS A レコードの切り替えだけでユーザーのアクセス先を切り替えることが出来るホットスタンバイ状態を維持している。アクティブ環境を遠隔地とした理由は、吉田キャンパスが被災した際には、ネットワークの停止や関係教職員の被災が同時に起こり対応できない可能性が考えられるためである。

2019 年現在、京都大学では学生メールや教職員メールなどクラウドサービスを利用しつつ SAML 連携で Shibboleth IdP で認証を行う構成が増えている。本取り組みにより吉田キャンパス被災時にも利用不能にならない情報システム・サービスを増やすことができたと考えられる。

4 今後の課題

認証 IC カードの利用開始から 10 年が過ぎ、関連機器の老朽化等の運用コストの増加が課題となってきている。マイナンバーカード等の接触 IC チップの利用が大規模には進まなかったこともあり、ベンダーの取り組みが進まずカードリーダーのドライバが最新ブラウザに対応しない、PC 以外では利用できないといった課題も出てきている。一方で ID/パスワード認証では安全性に問題があるため、IC カードより簡単で比較的安全性の高いワン

タイムパスワード等を用いた多段階/多要素認証の導入を検討している。

5 おわりに

本稿では、京都大学における Shibboleth IdP の IC カード対応と災害対策の取り組みについて述べた。教職員に配付している認証 IC カードに対応したことによって多くの教職員用情報システムについても Shibboleth IdP に認証処理を集約することができた。また遠隔地に環境を移すことによって吉田キャンパスが被災した際にもメール等の情報システムの利用を継続できるよう対策を行った。

今後も安定した運用を行うと共に多段階/多要素認証の実現などサービス改善に取り組んでいく所存である。

参考文献

[1] "認証方法の変更、設定（証明書による認証）", 学認技術ガイド, https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158431, (参照 2019-09-09)