認証連携を利用したデジタルアーカイブシステムのアクセス制御の取り組み

五島敏芳†，戸田健太郎†，高田良宏‡

†京都大学総合博物館　‡金沢大学総合メディア基盤センター
（連絡先）五島 h.gotoh@inet.museum.kyoto-u.ac.jp

（要約）

ふつうアーカイブズは資料の閲覧者を制限しないが，教育研究の記録，データやそこから生じたアーカイブ資料は誰もが閲覧するのに相応しくない内容を含むことがある。本報告は，教育研究のアーカイブ資料への閲覧の制限をデジタルアーカイブシステム上で実現するのに認証連携を利用する試みの紹介である。

「認証連携」とは，各機関でそれぞれ実現している認証管理を，機関の枠を越えて利用するための取り組みである。本報告では，日本の認証連携の連合体の一つである学術認証フェデレーション「学認」に対応した京都大学研究資源アーカイブの京都大学デジタルアーカイブシステム（愛称 Peek）を取り上げる。

Peek は，2013 年 9 月に「学認」のサービス提供者として承認され，「学認」参加機関発行のアカウントでログインするときだけ閲覧・検索できるメタデータやデジタルデータを提供している。しかしログインしようとすると失敗する報告が寄せられた。その原因を「学認」参加機関の多くが外部へ提供していない認証情報を要求していたことにあると考え，2018 年にリニューアルされた Peek では多くの機関が送出できる属性のみ要求するようにした。その結果，いくつかの手続きを経た場合のみログインが成功した。

この経験は，まだ日本の学術関係認証連携の利用に課題があることを示している。これに対し，技術的解決の可能性と関係各所間の相互理解や制度的整備の必要を展望する。

Access control of a digital archive system using identity federation

GOTOH, Haruyoshi†； TODA, Kentaro†； TAKATA, Yoshihiro‡
†The Kyoto University Museum; ‡Information Media Center, Kanazawa University

Although archives generally does not restrict users, archives of materials about educational and research activities may contain information that is not appropriate to be open to the public. In this report, we introduce a case about using identity federation to accomplish access control of archives about educational and research activities on a digital archive system.

デジタルアーカイブシステムへの認証連携の利用状況，先行類例，問題の所在

教育研究の記録・データやそこから生じたアーカイブ資料は，誰もが閲覧するのに相応しくない内容を含むことがある。そのためユーザを区別してアクセス制御する必要が生じるが，デジタルアーカイブシステム単独で一元的にユーザアカウントを管理するにはコスト的・利便性的に困難がある。そこで，複数の機関の認証の仕組みを連携し，他の組織の認証情報によってアクセス制御を行う方針が考えられる（これを認証連携と呼ぶ)。

ふつうデジタルアーカイブシステムは公開前提のため，ユーザ認証はスタッフによる管理機能の利用などに限られ，認証連携を利用した例も少ない。日本の認証連携の一つ，学術認証フェデレーション「学認」では，京都大学デジタルアーカイブシステム Peek を数えるのみである[1]。

かつて，教育研究世界の認証連携の多くが研究者にデジタル資源を活用してもらうための環境整備の一部であるように見えると指摘し，Peek の認証連携を利用した研究者の遠隔・共同編集によるメタデータ整備の試みは既存の認証連携の事例に見出せないとした[2]。この指摘はおよそ今も有効ながら，複数組織に所属する研究者間で，研究の過程に生じるコンテンツの共有を図るため認証連携を利用する「ARCADE」という近い問題関心からの取り組みは存在した[3]。

しかし，この Peek・ARCADE の例は，データ編集やコンテンツ共有の当事者が既知・特定的といえる。すなわち，それぞれのデータにアクセスできる人物は事前に特定できており，認証連携を利用しつつも一元的に管理する方式に近い。本来の目標は，(a)事前には特定できていない人物にもデータを閲覧・検索してもらいたい，ただし(b)データを正しく理解し取り扱うことのできる「研究者」に限定したい，できれば(c)その「研究者」は学術関係機関単位より詳しく区別したい，かつ(d)デジタルアーカイブシステムでは「研究者」個人を特定する情報をできるだけ保持したくない，というものである。なお(c)の区別は，実際は大学院生・教員・職員といった形式的区別とせざるをえない。

諸前提：データへの権限設定，データアクセスのユーザ・グループ

そもそもデジタルアーカイブシステムのデータへ公開可否とその範囲（ユーザ，グループ）を設定できなければ，閲覧・検索を制限できない。Peek は，ユーザやグループへの閲覧・検索の可否を個々のデータへ付与できる。

およそグループの種類は，システムの機能，認証，場所により大別され，さらに認証や場所により資料公開の範囲が異なる（表 1)。このグループへユーザを所属させることで，ユーザがどこまでの機能上の権限を持つか区別される。

機能	認証	場所	対象データ	備考
システム管理	ログイン必須	（認証優先）	非公開とも	非公開には保存用データを含む
データ登録・編集	ログイン必須	（認証優先）	非公開とも	
閲覧・検索	ログインあり	（認証優先）	限定公開 1	限定公開の数字は公開範囲の順位ではない。
	ログインなし	学内施設内	限定公開 2	
		学内	限定公開 3	
		学外	一般公開	

表 1. Peek で想定しているグループ

ここでは，閲覧・検索のみを対象とし，とくにログインありの場合を取り上げる。特定の場所だけに条件付きのデータを閲覧・検索できるようにすることは，その場所と対応するIPアドレスの範囲で実現しているが，認証と組み合わせるまでに至っていない。

認証連携利用の概要

Peekは「学認」にサービス提供者（SP）として登録することで，独自のユーザアカウントだけでなく，他機関によるユーザアカウントをログインに利用することができる。「学認」参加機関はそれぞれ認証情報提供者（IdP）を持ち，アカウント情報を管理している。「学認」参加機関構成員がSPのサービスを利用しようとすると，「学認」のディスカバリーサービス（DS）を通して所属のIdPへ送られ，IdPの認証結果によりSPが利用資格を判断し，サービスを利用できる，という流れとなる。またSPは，資格判断に必要な属性情報の送出をIdPへ要求する。

「学認」利用の実際，考察

Peekの場合，SPとなった2013年時点で，organizationName（o，組織名称・英字），jaOrganizationName（jao，組織名称・日本語），eduPersonTargetedID（ePTID，フェデレーション内匿名ID）の3つの属性情報を必須として要求していた。その意図は，ログイン利用者としての把握（一般公開利用との区別）と，ログイン状態の表示にあった。

ところが，京都大学以外（学外）からログインできない。ログインしようとした学外の「学認」参加機関構成員からの情報を総合すると，多くのIdPで送出を認めている属性情報の実態と合わなかったためと思われた。じっさい当時o，jao，ePTIDすべてを必須として要求するSPはなく，要求属性の組み合わせとしてもほとんど例がなかった。

これをふまえ2018年のPeekリニューアルに際し，多くのIdPが送出を認めているという属性ePTIDのみを必須で要求するように改めた。10月下旬～12月に「学認」参加機関の構成員へお願いして試してもらった結果，つぎの表2のとおりとなった。

No.	IdP	ログイン可否	機関名表示	接続手続き要否
1	北海道大学	はじめ×，のち○	○	要
2	金沢大学	はじめ×，のち○	○	要
3	名古屋大学	×，「学認」脱退？	−	−
4	大阪大学	○	×	？
5	核融合科学研究所	×	−	−
6	東京大学	×	−	要
7	宮崎大学	はじめ×，のち○	（×？）	要
8	広島大学	○	×	？
9	創価大学	○	×	？
10	関西大学	○	×（のち○）	？（のち要）

表2．Peekへの「学認」参加機関（京大以外）ログイン状況

「ログイン可否」の「○」は，IdPでのログイン後Peekの画面へ戻ってきたことを示し，「×」はIdPがサービスへの接続を拒否したことを示す。「機関名表示」は，ログインを経てPeekの画面へ戻ったとき，ログインした者の所属機関が表示されたかどうかを示

す。この機関名表示がなければ，実は正しくログインできていない。正しくログインできれば一般公開では閲覧・検索できないデータへアクセスできるようにしていたが，機関名表示がない場合そうした制限データは現れなかった。これは所属機関の IdP が正しく認証したという結果だけを返したものと後で判明した。よってログインの成功例は，いずれも Peek の利用希望を所属機関の IdP へ申請し Peek を利用可能な SP として登録した場合であった。つまり「学認」参加機関構成員から同機関 IdP への SP「接続手続き」が必要で，各 IdP の送出する属性情報の種類の問題ではなくそれ以前の問題が明らかとなった。

アクセス制御に関する展望

「学認」参加機関の中には，SP の新規追加を受け付けていないとか新規追加に部局長からの申請を必要とするとか，高い障壁を設けている例もある。新しい SP のサービスへの不信や理解不十分だけでなく，サービス利用のための手続きの案内情報の不足から，制度的問題もうかがえる。

それでも SP がログイン情報を持つことなく IdP からの属性情報だけで自動的にサービス利用資格を判定できる可能性はある。具体的には，属性情報のうち eduPersonAffiliation または eduPersonScopedAffiliation を用いれば，その属性値が faculty，staff，student，member であるため，教員，職員，学生院生，その他構成員を区別できる。この属性情報を必須またはオプションで送出要求すれば，いま Peek は学術関係機関構成員全般のログインによる区別しか実現していないが，閲覧・検索できるデータに対し，教員だけ，学生院生も含む，といった細かなアクセス制御を実現できよう。

アーカイブ資料または学術情報の公開に関する展望

たいてい大量で公開可・不可の内容が混在するアーカイブ資料や，しばしば研究者個人に占有されるか特定研究者間で共有される未公表の内容を含む教育研究世界の情報は，制限された公開範囲の設定が実現されてこそ，未公開非公開のまま放置されずに公開の総量が広がるのではないか。その実現の方途の一つを，本報告は提供したと考える。

参考文献

[1] “IdP・SP 一覧”. 学術認証フェデレーション. https://www.gakunin.jp/participants/ (参照 2019-03-29).

[2] 五島敏芳，戸田健太郎. “3 京都大学研究資源アーカイブにおける研究資料情報の共有”. 〈総合資料学〉の挑戦. 国立歴史民俗博物館編. 吉川弘文館, 2017, p.65-75.

[3] 松平拓也，中村素典，山地一禎，西村健，高田良宏，笠原禎也. 学術組織間デジタル資料分散共有システム「ARCADE」の開発. 情報処理学会論文誌. 2014, vol.55, no.5, p.1485-1497, http://id.nii.ac.jp/1001/00101154/

（謝辞）

Peek の「学認」ログインの状況確認に，つぎの各氏の協力を得た。ここに記して感謝申し上げる。（敬称略・五十音順）石田真衣，遠藤満子，神立孝一，久保田明子，坂口貴弘，研谷紀夫，難波忠清，椋木雅之，山下俊介，山田太造