# 横断的アクセス管理：
# ケーススタディ
# （ビジネス・ケース・ツールキット補足資料）

横断的アクセス管理：

# ケーススタディ

## （ビジネス・ケース・ツールキット補足資料）

CC297D002-1.0

2007 年 7 月 10 日

表紙＋42 ページ

チャーリー・デイビス博士

マット・シュリーブ

**Curtis+Cartwright Consulting Limited**

Main Office: Surrey Technology Centre,

Surrey Research Park, Guildford

Surrey GU2 7YG

tel: +44 (0)1483 295020

fax: +44 (0)1483 295021

email: postmaster@curtiscartwright.co.uk

web: http://www.curtiscartwright.co.uk

Registered in England: number 3707458

Registered address:

Baker Tilly, The Clock House,

140 London Road, Guildford,

Surrey GU1 1UW

**目次**

このページは敢えて空白にしてある

## 略語一覧

| | |
|---|---|
| ASMIMA | 複数 ID 管理アプリケーションのための Shibboleth 採用［Adoption of Shibboleth for Multiple Identity Management Applications］ |
| AY | 学年度［Academic Year］ |
| CAS | 集中型認証サービス［Central Authentication Service］ |
| CM | コア・ミドルウエア［Core Middleware］ |
| FE | 継続教育［Further Education］ |
| FTE | 全日制換算［Full Time Equivalent］ |
| HE | 高等教育［Higher Education］ |
| ICT | 情報通信技術［Information and Communications Technology］ |
| IdP | ID プロバイダー［Identity Provider］ |
| IDM | ID 管理［IDentity Management］ |
| I2 | Internet2 |
| INSRV | 情報サービス［INformation SeRVices］ |
| IT | 情報技術［Information Technology］ |
| JISC | 合同情報システム委員会［Joint Information Systems Committee］ |
| KC-ROLO | キッダーミンスター・カレッジ・レポジトリ・オブ・ラーニング・オブジェクト［Kidderminster College - Repository Of Learning Objects］ |
| MATU | ミドルウエア採用支援サービス［Middleware Assisted Take-Up］ |
| MCE | メンバー分類・資格付与［Member Categorisation and Entitlement］ |
| MIS | 管理情報システム［Management Information System］ |
| MWE | 近代的 IT 作業環境［Modern IT Working Environment］ |
| RSC | 地域サポートセンター［Regional Support Centre］ |
| SAML | セキュリティ・アサーション・マークアップ言語［Security Assertion Markup Language］ |
| SP | サービス・プロバイダー［Service Provider］ |
| TCO | 総所有コスト［Total Cost of Ownership］ |
| VLE | 仮想学習環境［Virtual Learning Environment］ |
| VRE | 仮想研究環境［Virtual Research Environment］ |
| WAYF | 所属組織特定機能［Where Are You From］ |
| WG | 作業部会［Working Group］ |
| WM | ウェスト・ミッドランド［West Midlands］ |

このページは敢えて空白にしてある

# 1 はじめに

## 1.1 全般

1.1.1 本補遺は、情報システム合同委員会［Joint Information Systems Committee：JISC］によるビジネスケース（投資対効果検討用）ツールキット［business case toolkit］を補足するものである。各機関において、横断的アクセス管理［federated access management］[1]の実施に関わる意思決定を行う上で、その一助となるように作成された。本文書では、横断的アクセス管理を実際に実施した場合にどうなるのか、4 件の詳細なケーススタディを通じて具体的に検討してゆく。

## 1.2 背景

1.2.1 教育および研究のためのアクセス管理のあり方は、英国内でも世界でも、大きく変貌しつつある。電子リソースや各種サービスを保護するため、新たなテクノロジーやサービスが生み出されている。大学などの教育・研究機関は、こうした変化や新たに生じている機会にどのように対処していくのかを決定する必要に迫られている。

1.2.2 2006 年 11 月、情報システム合同委員会（JISC）は、「教育と研究のための英国アクセス管理フェデレーション［UK Access Management Federation for Education and Research］」（「フェデレーション［the Federation］」）を発足させた。これにより英国における新たな横断的アクセス管理インフラの開発が具体化している。

1.2.3 既存の Athens システムは、2008 年 8 月から、フェデレーション内の加入制の有料サービスを通じて提供される。この日付以降、JISC は Athens への資金提供を中止するため、Athens のような外部の ID プロバイダーを使用している全ての機関は加入の申し込みを行わなければならない。

1.2.4 JISC は、新規インフラを計画・準備するための 2 つの開発プログラムを 2004 年 4 月から 2006 年 3 月にかけて実施した。これらの「コア・ミドルウエア」プログラム［Core Middleware programmes：CM プログラム］により、当該インフラの初期要素が確立されたと同時に、将来、諸機関に役立つと思われる教訓も得ることができた。CM プログラムは、横断的アクセス管理の内部利用、第三者利用、機関間相互利用、臨時共同利用を対象として準備を行った。

## 1.3 ケーススタディ

1.3.1 本文書に収めたケーススタディでは、ID 管理・アクセス管理のシステムおよびプロセスを改善するためのプロジェクトを実施した 4 つの機関を取り上げている。これらの機関はいずれも、アクセス管理に関する戦略面・運用面の意思決定を行い、プロジェクトを完遂し、便益を実現してきた経験を有している。各機関については、次ページで簡単に紹介し、その後詳述する。

[1] *CC297D001-1.0 federated access management: institutional business case toolkit*（2007 年 7 月 10 日）

### カーディフ大学

カーディフ大学は28の学部と5の事務部局に約5000人の職員と1万8000人の学生を擁する大規模な機関である。NHSウェールズとも緊密に連携している。

プロジェクトの主たる目的は、Shibbolethテクノロジーの早期採用者としてJISCから資金を受け、既存のClassic Athensアクセス管理システムの後継としてShibbolethテクノロジーを実装することであった。

本件プロジェクトは、カーディフ大学の情報サービス局［INformation SeRVices：INSRV］により実施された。INSRVの目的は、コンピュータ、図書館、メディアに関する、より優れたサービスを提供し、カーディフ大学における研究、学習、教育、コミュニティ活動、管理機能に確かな貢献を果たすことである。

### キッダーミンスター・カレッジ

キッダーミンスター・カレッジはウェスト・ミッドランドにある小規模なカレッジで、約5100人の学生を有する（うち、1000人が全日制）。キッダーミンスターは幅広い全日制・定時制課程（最長で2年間）を提供している。

プロジェクトの主たる目的は、キッダーミンスター・カレッジ内でShibbolethテクノロジーを用いて横断的アクセス管理を実装し、ウェブベースのリソースの連携を図ることであった。

同プロジェクトは、ICTサービス内部の開発チームにより実施された。キッダーミンスターの開発チームは、多くのFEカレッジと異なり、IT開発に特化し、サポート業務を担当しない。ICTサービス開発チームは十分な資金供給を受けており、訓練を積んだスタッフが積極的に開発に取り組み、オープンソース・ソフトウエアの扱いにも通じている。

### サリー大学

サリー大学は比較的大規模な大学で、その情報システムは約1万8500人のユーザーをサポートしている。同大学では、成熟した商用システムを実装するという全学的な方針を立てており、情報システムを担当するスタッフ数も非常に少ない。

プロジェクトの主たる目的は、サリー大学におけるアクセス管理システムをClassic Athensから権限委譲型の認証システムに切り替えて、IT担当スタッフの負担を軽減することにあった。

プロジェクトは図書館とIT部門により実施された。両者は別個の組織であるものの、いずれも情報サービス部門長の権限の下にある。ITサービス部門は、サリー大学の学術ニーズとビジネスニーズの双方を満足する高品質でユーザー指向のITサービスを提供する。

### ウォーリック大学

ウォーリック大学は職員約5000人と学生1万6000人からなる大規模な機関である。主要学部はウォーリック・ビジネス・スクールを含め5つある。

プロジェクトの主たる目的は、ウォーリック大学における既存のアクセス管理システム（ウェブサービスへのアクセスを管理する）をアップグレードして、セキュリティの向上を図ることであった。

プロジェクトはウォーリック大学のEラボ（同大学ITサービスの開発部門）により実施された。Eラボには複数のチームがあり、それぞれウェブサービスやeラーニング、プロジェクト開発、ビジネスシステムを担当している。Eラボの目的は、開発、特にウェブ関連作業の中心を担うことである。

図1-1：機関別ケーススタディ

# 2 カーディフ大学

## 2.1 概要

2.1.1 カーディフ大学は Shibboleth の早期採用者として JISC から資金提供を受け、既存の Classic Athens アクセス管理システムの後継として Shibboleth テクノロジーを実装するプロジェクトに着手した。Shibboleth プロジェクトを可能にしたのは、同大学の ID 管理［IDentity Management：IDM］手順をアップグレード・合理化するプロジェクトであったが、一方で、Shibboleth プロジェクトは、IDM プロジェクトによるユーザー資格の確立・付与を推進する上で重要な役割を果たした。

2.1.2 同プロジェクトの成功要因として、図書館スタッフと IT スタッフ間の意思疎通が極めて円滑に行われたことがあげられる。カーディフ大学には、図書館と IT 部門を統合した情報サービス局（INSRV）があるため、両者間の意思疎通が促進されたのである。プロジェクトは 2 つの部分に分割された。ひとつはインフラの開発であり、もうひとつは実装と展開（ユーザーへの普及）である。前者は IT スタッフが担当し、後者は図書館スタッフが担当した。Shibboleth テクノロジーは新規ユーザーを対象に 2006 年 7 月に展開されたが、全ユーザーを対象とした展開は 2007 年夏の予定である。Classic Athens は OpenAthens が加入制の有料サービスになる 2008 年 7 月までに停止される。

| | |
|---|---|
| **JISC Collections 社類型** | B |
| **ユーザー数** | 学生 1 万 8000 人（全日制換算）、職員 5000 人 |
| **プロジェクト開始期** | 2005 年 4 月 |
| **プロジェクト終了期** | 継続中（Shibboleth は 2006 年 7 月に新規ユーザー向けに展開済み） |
| **プロジェクトの主要目的** | 既存の Classic Athens アクセス管理システムの後継として Shibboleth テクノロジーを実装すること |
| **意思決定に携わる関係者** | プロジェクト・ディレクター（情報サービス担当アシスタントディレクター）、プロジェクト・マネジャー（戦略・プロジェクト・連絡担当主席コンサルタント）、決定事項を承認するプロジェクト運営グループ |
| **財源** | 内部の INSRV 予算および JISC 早期採用者向け援助資金 |
| **主要マイルストン** | 新規ユーザーへの Shibboleth テクノロジーの展開 |
| **現行のアクセス管理システム** | Shibboleth（I2 リファレンス実装） |
| **以前のアクセス管理システム** | Classic Athens（およびカーディフ大学の統合サインオン・システム） |
| **フェデレーションへの加入** | 加入済み |

## 2.2 背景

*カーディフ大学*

2.2.1 カーディフ大学は緩やかに統合された総合大学であり、ウェールズ大学医科大学と

このほど合併し、28 の学部と 5 の管理部局に職員 5000 人と学生 1 万 8000 人を擁する機関となった。

2.2.2 INSRV は IT 部門と図書館部門を束ねたカーディフ大学の一部局である。多種多様なシステムを管理しており、多数のプラットフォーム、ベンダー、システム（Unix/Linux 系のシステムとツール、Novell 製品を含む）を網羅した幅広い専門知識を有する。カーディフ大学には 18 の学部図書館があり、相互に独立しながらも INSRV という共通の枠組みの下に緊密に連携している。各図書館には個別分野ごとの図書館員もいる。

2.2.3 カーディフ大学は Athens による保護サービスの主要ユーザーであり、Athens のサービスに対するカーディフ大学からのログインは毎年 100 万回を超える。Classic Athens のサービスは、ユーザーのアカウントと資格証明の集中型レポジトリで、ローカルレベルで管理されていた。新学期が始まるたびに数千の Athens アカウントが作成され、各ユーザーは図書館スタッフから自分の Athens 用ユーザー名・パスワードを取得していた。

*早期採用者*

2.2.4 2005 年 4 月、カーディフ大学の情報サービス局は、JISC のコア・ミドルウエア・プログラム、「複数 ID 管理アプリケーションのための Shibboleth 採用［Adoption of Shibboleth for Multiple Identity Management Applications：ASMIMA］」プロジェクトのための資金提供を受けた。同プロジェクトの中心的な狙いは、以下を目的としてカーディフ大学で Shibboleth テクノロジーを実装することであった。

- Classic Athens の使用から切り替えること
- カーディフ大学／NHS 合同スタッフのコンピュータ経験の向上に資すること
- e サイエンス・アプリケーションに対するアクセス管理の手法として Shibboleth テクノロジーを検討すること

*サービス・プロバイダー*

2.2.5 Athens で保護している e ジャーナル以外にも、カーディフ大学はいくつもの内部ウェブサービスを有し、ユーザーに供用している。こうしたサービスの多くはアクティブ・ディレクトリに対してユーザーを認証し、統合サインオン・システムの一部となっている。カーディフ大学において、統合サインオン・システムの一部としてユーザーが利用可能なウェブサービスには、以下のようなものがある。

- Blackboard 仮想学習環境（VLE）
- Voyager 図書館管理システム
- 電子メール

***ID 管理***

2.2.6 カーディフ大学は、各人が単一の ID に基づいてシステムへのアクセスおよび利用を行えるようにするとともに、単一のインターフェースを通じてアクセスおよび利用を管理できるようにするため、同学の ID 情報（例えばデータベースとディレクトリサービスに保持されている ID 情報）をアップグレードするプロジェクトを行っている。

2.2.7　1998 年、カーディフ大学は、ユーザー名ではなく ID を管理する必要性に気づき、IDM と集中型レポジトリの検討を始めた。IDM プロジェクトは 2002 年（Shibboleth プロジェクトの 3 年前）に開始された。IDM の便益はすでに現れ始めており、例えば、ユーザーアカウントの自動プロビジョニングによって、1 学部 1 年あたりで 2～3 週間分の労力と時間が節約できると期待されている。

2.2.8　IDM プロジェクトは Shibboleth プロジェクトを実現するための必須要素と考えられていた。一方で、Shibboleth プロジェクトもまた、IDM プロジェクトによるユーザーへの資格付与を推進する上で重要な役割を果たした。Shibboleth に対応して情報システムを利用できるようにするためには、ユーザーはカーディフ大学のアカウントを持たねばならず、カーディフ大学のメンバーでなければならないからである。2005 年末に向けて、以下の事項を決定するため、メンバー分類・資格［Member Categorization Entitlement：MCE］作業部会［Working Group：WG］が設置された。

- 誰をカーディフ大学のメンバーとするか
- 各ユーザーはどのようなサービス享受資格を有するか
- ユーザーグループをどのように分類するか

2.2.9　これは非常に人手のかかる作業で、特に最初の 3 カ月間はこの作業に多くの時間を割いたが[2]、これまで既に 18 カ月間かかっている。この作業の結果、大学理事会の承認を経て、大学レベルで資格ポリシー（と統治プロセス）が確立される予定である。カーディフ大学には医学部が付随していることから、同大学におけるユーザー資格の付与はとりわけ複雑な作業となっている。医学部には、多数の例外的ユーザーグループが存在するからである。その一例が、カーディフの学生の指導にあたっている NHS コンサルタントで、このグループのユーザーは、指導に活用するため VLE の要素にある程度アクセスできる必要がある。

## 2.3　目的

2.3.1　本ケーススタディは ASMIMA プロジェクトの第一の目的、すなわち既存の Classic Athens アクセス管理システムの後継として Shibboleth ID プロバイダー［Shibboleth Identity Provider：IdP］をカーディフ大学で実装することに焦点を当てている。

## 2.4　範囲

2.4.1　このプロジェクトの範囲は Athens 保護リソースを Shibboleth 対応にすることであった。Blackboard VLE、電子メールおよび Modern IT Working Environment（MWE）[3]は対象範囲外である。VLE および電子メールはカーディフ大学の統合サインオン・システムにすでに組み込まれているため、現時点では、急いで Shibboleth 対応化を行う必要はない。

## 2.5　計画

[2] ユーザー資格マネジャー（User Enabler Manager）が 0.75FTE 相当で約 3 カ月この作業に費やした。これ以外に他のメンバーも作業部会に出席している。

[3] Modern IT Working Environment：MWE（現代的 IT 作業環境）は、職員と学生にとって、大学生活における多様な側面（必読文献リストや時間割から、社交イベント、ネットワーク作り、共同作業空間を介した情報共有まで）をオンライン上で管理しやすくするためのプログラムである。

*戦略的推進要因*

2.5.1 プロジェクトの主要な戦略的推進要因は次のとおりである。

- Classic Athens は図書館スタッフにとって管理業務およびサポート提供の面で大きな負担を伴っていた。[4]
- 新学期ごとに繰り返されるアカウント作成の管理プロセスは時間のかかる作業で、プレッシャーがかかっていた。
- 記憶すべき複数のパスワードがあることは、良好なユーザーエクスペリエンスにつながらず、電子リソースの利用を拡大する上での障壁と見なされていた。
- JISC のイニシアチブと整合し、国際的に認知された規格を採用する。

*オプションの評価*

2.5.2 2005 年の時点で、カーディフ大学は同学の Classic Athens システムの後継を積極的に探していた。INSRV の局長補は技術的な進歩と動向を注視しており、横断的アクセス管理ならびに利用可能ないくつかの技術的ソリューション（Internet2 の Shibboleth テクノロジー、AthensDA、Liberty Alliance ID-FF ソリューションなど）について認識していた。

2.5.3 INSRV 局長補が AthensDA を実装するプロジェクトを提案しようとしていたところに、JISC が CM プログラムの下に Shibboleth の早期採用者向けの支援計画を公表した。INSRV の関係者は会合を持ち、AthensDA よりも Shibboleth テクノロジーの方を採用することを決定した。

2.5.4 Shibboleth 採用に伴う主なリスクは次のとおりと見られた。

- Shibboleth は実績のないテクノロジーであった。
- カーディフ大学で Shibboleth テクノロジーを展開する時点に間に合うように、Athens サービス・プロバイダーが Shibboleth-Athens ゲートウエイとの互換性を確保することができないかもしれない。

2.5.5 Shibboleth 採用の主な利点は次のとおりと見られた。

- 作業の重複の最小化。英国の教育研究セクターは、Shibboleth テクノロジーを選択してこれに一本化しつつあるようであったので、いずれにせよ、将来的に Shibboleth テクノロジーを実装する必要が生じる可能性が高かった。
- カーディフ大学は早期採用者として資金提供に応募することが可能であった。早期採用者プロジェクトには実用に移行する意図を持って申し込むが、絶対的な確約は必要なかった。[5]

2.5.6 Shibboleth は実績のないテクノロジーであったが、国際的に広く採用され、今後のアクセス管理の手法として広く受け入れられていた。万一、Shibboleth テクノロジ

[4] 図書館スタッフは各ユーザーに、ユーザー名とパスワードをそれぞれ 2 つずつ（Athens とローカル）発行する必要があったことから、特に大きな問題となっていた。ヘルプデスクには多大な経費がかかっていたが、問い合わせの大半はパスワード忘れに関するものであった。

[5] しかし、Shibboleth テクノロジーこそ英国教育セクターが選択しつつあるテクノロジーであるとカーディフ大学が認識した後に、たとえ JISC から資金を得られなかったとしてもカーディフ大学は Shibboleth テクノロジーの実装を選択していたであろうと大学は述べている。

ーがカーディフ大学の要件に合致しないことが分かり、不成功に終わった場合にも、AthensDA が代替テクノロジーとして、まだ利用可能なはずである。

*コスト負担*

2.5.7 Shibboleth プロジェクトに先立ち、カーディフ大学は IDM プロジェクトに 100 万ポンド超を投じていた。

2.5.8 カーディフ大学は ASMIMA プロジェクトのため JISC から 5 万ポンドを受領した。会計上、正式な資金はこれだけであったが、追加的な費用が発生した場合には、INSRV 予算から賄われた。Shibboleth プロジェクトに関しては、負担が不可能になるほどの費用が発生することはなかった。

2.5.9 Shibboleth プロジェクトの中核的作業（MCE WG を含む）に要したコストを事後的に概算したところ、その内訳は以下のとおりであった。

- **技術的実装とテクノロジーの調査：**専従 IT 担当者 1 名の労働時間 2 カ月分
- **コンプライアンスのため出版者の承諾を得る作業：**図書館員 1 名の労働時間 1～2 カ月分
- **ユーザー資格付与：**ユーザー資格マネジャーの労働時間 2 カ月分＋関係者会合に 1 カ月分
- **コミュニケーション：**変更の連絡周知のため 1 人月
- **プロジェクトマネジメント：**プロジェクト・マネジャーの労働時間 0.5 カ月分
- **教育訓練：**1 人月

2.5.10 ID 管理システムに一定の変更を行うため専門技術者 1 人を迎え入れた。

2.5.11 ハードウエア購入費は 6000 ポンドであった。ただし、負荷分散装置は内部で利用可能なものがあったために別途購入はしていない。フルセットの Shibboleth IdP の運用にかかる技術的費用の見積もりはサーバー1 台（寿命 3 年）につき 3000 ポンド。すなわち、同大学で導入したサーバー2 台の運用に年間 2000 ポンドが出費されることになる。

2.5.12 上記の内訳を総計すると費用は約 3 万ポンドとなる。しかし、カーディフ大学の概算によると、実際のプロジェクト経費総額は 7 万 5000～10 万ポンドに達した。

*達成可能性*

2.5.13 アセスメントの結果、プロジェクトは INSRV が保有する能力および人員の範囲内で達成可能であり、INSRV はプロジェクト実行に必要な技能を十分に備えていると判断された。しかし、JISC の早期採用者資金によって専任の IT 担当者を雇用することが可能になった。同担当者は、これまでに Shibboleth テクノロジー、IDM およびディレクトリサービスに関して多大な専門知識を培っている。

2.5.14 カーディフ大学は ASMIMA プロジェクトのためのプロジェクトチームを設置し、同学のプロジェクトマネジメントの枠組みに従った[6]。また、INSRV の複数の局長補

[6] この枠組みは当初、100 万ポンド以上のプロジェクトのみを対象に用いられているが、この事例では ASMIMA プロジェクトに関し JISC が求める報告要件を満たすために適用された。

とユーザー代表から成るプロジェクト運営グループも設置された。この運営グループは、プロジェクトチームが行った決定を承認する権限を有し、プロジェクトの対象範囲や財務事項に大きな変更が生じた場合などの例外的事態に対処する役割を与えられた。プロジェクトチームは定期的な会合を持ち、より下位のレベルでも会合が行われた（例えば、ある時点においては関係図書館スタッフが隔週で会合を行っていた）。

## 2.6 実施

### *成果*

2.6.1 プロジェクトは 2 つのサブプロジェクトに分割され、それぞれ別の部署が担当した。

- IT インフラの開発（IT スタッフ）
- 実装と展開（図書館スタッフ）

2.6.2 プロジェクトの技術的側面は比較的単純な側面と見られ、Internet2 Shibboleth のリファレンス実装も、カーディフ大学の要件を満たすのに十分であった。障害許容力および負荷試験は、プロジェクトの早い段階に組み込まれた。（例えば、負荷試験計画を作成したり、負荷分散装置の背後に 2 つのサーバーを実装し、障害許容力の向上を図ったりした。）2 つのサーバーを常時稼働させるというポリシーを満たすため、保全およびアップグレードに備え第 3 の仮想サーバーが実装されている。INSRV は、サーバーが負荷に確実に対処できるよう、Shibboleth テクノロジーへのユーザーの移行を徐々に進めることを決定した。

2.6.3 実装および展開（ユーザーへの普及）の監督役には図書館スタッフが最適であると判断された。図書館スタッフは、ユーザーにより近い存在であることから、新しいテクノロジーをユーザーに普及する上で適任であると考えられた。その上図書館は、大学に入ってくる全ての新規ユーザーと顔を合わせることになる。図書館は新しいアクセス管理システムの所有権も得た。

2.6.4 同プロジェクトの中で大きな部分を占めたのが、JISC コミュニティと共同で、サービス・プロバイダーに圧力をかける、という仕事であった。カーディフ大学で Shibboleth テクノロジーを実際に展開する時点までに、サービス・プロバイダーの過半数で Shibboleth-Athens ゲートウエイへの対応が済んでいるよう、確実を期する必要があったのである。

2.6.5 カーディフ大学は 2006 年 9 月に全てのユーザーに新サービスを展開した。当初は、新サービスの案内を新規加入者（職員と学生を合わせて約 4500 人のユーザー）に対してのみ行った。移行を漸次的に進め、システムの障害許容力をモニタリングできるようにするためである。図書館も、電子リソースへのアクセスを求めるユーザーに対して Athens アカウントの発行を停止し、その代わりに Shibboleth 対応アカウントを与えた。

2.6.6 現在では全トラフィックの 52%が Shibboleth-Athens ゲートウエイを経由している。Shibboleth 経由でリソースにアクセスするユーザー数は 1 万人に上っている。これはすなわち、新サービスの案内を受けた以外のユーザーも、独自の判断で予定より早く移行したということを意味する（1 年生は 2500 人しかいない）。こうした既存ユーザーによる独自の移行は、宣伝・広報活動をしていないのに実現されている。

2.6.7　実装および展開を行うために、全ての図書館間で協調を図り、スタッフの教育訓練に当たる必要があった。スタッフの教育訓練は次の手段によって実現した。

- 分野ごとの図書館員に対する電子メール
- 図書館スタッフに対するプレゼンテーション（2006 年 5 月と 6 月に開催）。Shibboleth テクノロジーとは何か、カーディフ大学はなぜこのテクノロジーを導入するのかを説明。
- プレゼンテーションを通じて図書館スタッフが収集した情報を他の図書館スタッフに配布

2.6.8　ユーザー周知は個々の学部への連絡と多様な媒体を通じた公示によって達成された。広範な対象に通知できるよう、幅広い媒体を使用して可能な限り公示を行った。その例は次のとおりである。

- 新サービスの使用法の手引きをウェブページに掲示
- 図書館にチラシを用意
- 共有ドライブ上でのプレゼンテーション

2.6.9　現在では、全ての図書館のどの図書館端末からでも、ユーザーの Shibboleth 対応ローカル・パスワードを変更できるようになった。パスワードは単一の中央電子メールアドレスを介してリセット可能である。

### *実現した便益*

2.6.10　このプロジェクトは多くの便益をカーディフ大学にもたらしている。

- Classic Athens の使用に伴う管理面での負担が無くなったために、管理プロセスは格段に円滑になった。ヘルプデスクへの問い合わせは半減し、図書館チームはサポート業務の負担から解放された。
- ユーザーエクスペリエンスが向上した。職員および学生からのフィードバックは全て肯定的であり、ことさら宣伝・広報活動を行っていないにもかかわらず、既存ユーザーの多くが統一サインオン方式の便益を享受するために予定よりも早く独自に移行を行っている。
- ユーザーがウェブリソースに外部からアクセスできる。
- Shibboleth の実装によりカーディフ大学の経費が節減された。総所有コストは OpenAthens 加入利用料よりも少ないと見積もられている。
- カーディフ大学によるライセンス管理が向上した。誰がカーディフ大学のメンバーであるのか、および、各メンバーが有する具体的な資格が正確に把握できるようになったのでライセンス監査への対応が改善された。
- カーディフ大学は長い移行期間をとることができたので、詳細な障害許容力および負荷試験を実行することができた。加えて、多数のユーザーが独自に移行してくれたため、教育訓練の負担が軽減した。
- Shibboleth プロジェクトによって IDM プロジェクトにさらなる弾みがついた。また、これまでは思いつきもしなかったものの、明確化するべき様々な問題があることにも気づかされた。例えば、招聘教員や NHS スタッフといった例外的なカテゴリーのユーザー資格をどのように定義するかなどの問題である。
- カーディフ大学の横断的アクセス管理インフラは、将来的に横断的アクセス管理を有する他の組織との連携を促進し、複数機関にまたがる研究グループの活

動を可能にしてゆく。

## 2.7 直面した課題と得られた教訓

2.7.1 プロジェクトは大成功であったと考えられている。プロジェクト全体を通じて直面した課題は非常に少なかった。テクノロジーは支障なく機能し、初期故障などの問題はほとんどなかった。実際に持ち上がったのは次の課題である。

- 全てのサービス・プロバイダーが、横断的アクセス管理に対応済み、あるいは対応を予定しているわけではない。このため 2006 年夏、カーディフ大学へのサービス提供を継続するには Shibboleth-Athens ゲートウエイへの対応が必要であることを各サービス・プロバイダーに周知するために、多額の経費を要した。現在では、カーディフ大学への主要サービス・プロバイダーのうち、未対応のプロバイダーは 1 社だけである。当面は代替的なアクセス機構が構築され、満足とは言えないものの、十分その機能を果たしている。このたった 1 社の例外により、カーディフ大学が横断的アクセス管理の稼働開始を見送ることは考えられなかったものの、2006 年 8 月までプロジェクトが中断してしまう可能性もあったのである。
- Shibboleth を用いて Athens にログインすると新規の Athens アカウントが作成されるが、一部の事例においては、パーソナライズ機能の一部が失われることがある。例えば、検索とアラートは移行されない。
- ユーザーアクセスに対するきめ細かい制御を行うためには、各ユーザーカテゴリーが有するサービス享受資格をいちいち指定する必要があった。

2.7.2 カーディフ大学のプロジェクトを通じて次の教訓が明らかになった。

- IT 部門と図書館が緊密に協働することが不可欠である。
- 専従の IT 担当者を置いたことが、実装プロセスの迅速化に有益であった。
- Shibboleth の導入により、本来ならすでに確立しているべきだが、実際には実現できていない場合が多い、いくつかの事柄の実施を強いられることになる（例：包括的な ID 管理システム、適切なディレクトリサービス、機関内部の政治的友好関係など）。また、さまざまなカテゴリーの職員・学生とそれぞれのグループが有する資格について、明確なポリシーとガイドラインを設ける必要性が、いっそう明らかになった。こうしたポリシーの厳格化はユーザーからの抵抗に遭う可能性がある（例：退職した職員の資格についてなど）。
- 大学に医学部が付随する場合には、IDM は非常に複雑になる。資格を指定しなければならない多数の例外的ユーザーカテゴリーが生じるからである。プロジェクト着手時に、こうした資格付与の作業規模を見積もるのは難しく、不可能な場合もあるものの、この作業に適切に備えておくことが重要である。
- 今後数年間にわたり、英国のアクセス管理環境は、非常に複雑化することが予想されるが（例：Shibboleth、Shibboleth-Athens ゲートウエイ、Athens-Shibboleth ゲートウエイ、Classic Athens、IP 認証が全て並存する状況）ユーザーの混乱を防ぐためには、明確な文書化およびユーザーガイドが必要である。
- INSRV は基本的にボトムアップ型のプロジェクトを完遂したが、プロジェクトが進むにつれて各プロセスに伴う問題と機会が明らかになっていった。INSRV は、幸運なことに、そうした問題を解決し、機会を活用することができた。全てのプロセスを大局的に把握した「全体像」が当初から見えていれば、潜在的な問題を早期に特定するのに役立っただろうが、プロジェクト着手の段階で全

体像をつかもうとすれば、初期段階は格段に難しいものとなっていたであろう。
- 必要なバックエンド要件が全て整備されていれば、Shibboleth IdP の実装は技術的にはかなり単純である。Shibboleth テクノロジーは、ひとたび稼働を開始し運用に移行すれば保全にさほどの労力を要さない。

## 2.8 将来の計画

2.8.1 カーディフ大学は将来に向けて次の計画を掲げている。

- カーディフ大学は、2007 年夏までに全ユーザーに対して Shibboleth テクノロジーを展開し、有料化される 2008 年 7 月までに Classic Athens を停止する意向である。
- ユーザーエクスペリエンスをさらに向上させることが検討されている。例えば、ユーザー問題のほとんどを引き起こしている WAYF を迂回する方法などが検討されている。
- カーディフ大学は同学のサービスへのアクセスを管理するため、Shibboleth サービス・プロバイダー（SPs）を利用する計画である。例えば、他機関との共同研究の実現などを図る。
- プロジェクト実施により蓄積された専門知識を活用して、カーディフ大学より小さい機関に対し外部 ID プロバイダーとして商業的にサービス提供することを検討している。
- 医学生の Athens アカウントを単一アカウントに一本化できるよう NHS と共同作業する（現在、医学生は 2 つのアカウントを有している。ひとつは NHS 用、もうひとつはカーディフ大学用）。
- カーディフ大学は、例えば MetaLib（統合検索環境）など、他のアプリケーションの Shibboleth 対応化や、Blackboard VLE の Shibboleth 対応化版使用についても検討している。

## 2.9 有用な資料

2.9.1 カーディフ大学の活動に関する詳細情報については、次の資料を参照されたい。

- ASMIMA プロジェクトからの最終報告
- MCE WG による典型的ユーザーカテゴリー
- Shibboleth IdP アーキテクチャの障害許容力に関する資料
- 展開における試験計画

2.9.2 これらの資料は次のウェブページから入手可能である。

- <http://www.jisc.ac.uk/whatwedo/themes/access_management/federation/federation_res_casestudy.aspx>

# 3 キッダーミンスター・カレッジ

## 3.1 概要

3.1.1 キッダーミンスター･カレッジはウェブベースのリソースを連結するため Shibboleth テクノロジーを用いた横断的アクセス管理を導入している。主たる目的は、ネットワークと VLE へのシームレスなアクセスを実現することによって、同学の Moodle VLE の利用を増やすことにあった。プロジェクトは円滑に進み、本格的サービスは 2006 年 4 月に稼働を開始した。キッダーミンスターは現在、シングル･サインオン･システムを運用しており、これによってユーザーエクスペリエンスが向上し、ウェブリソースへの外部からのアクセスが可能になっている。

| | |
|---|---|
| **機関名** | キッダーミンスター・カレッジ |
| **JISC Collections 社類型** | I |
| **ユーザー数** | 学生 5100 人（うち全日制は 1000 人） |
| **プロジェクト開始期** | 2004 年 4 月 |
| **プロジェクト終了期** | 2006 年 4 月 |
| **プロジェクトの主要目的** | キッダーミンスターの Moodle VLE の利用を増やすこと。そのため、VLE とネットワークアクセスをシングル・サインオン・システムで結び、VLE の使いやすさを向上させること。VLE を使用する機関との間で特定の課程を共有する意向もあった。 |
| **意思決定に携わる関係者** | 副学長<br>ICT サービス責任者 |
| **財源** | JISC 早期採用者向け資金および ICT 予算 |
| **主要マイルストン** | Shibboleth 本格サービス稼働開始（2006 年 4 月） |
| **現行のアクセス管理システム** | Shibboleth v1.3 |
| **以前のアクセス管理システム** | 大半のサービスについてユーザー名とパスワードを併せて使用。Classic Athens も使用。 |
| **フェデレーションへの加入** | 加入済み |

## 3.2 背景

### *キッダーミンスター・カレッジ*

3.2.1 キッダーミンスター・カレッジはウェスト・ミッドランドにある小規模なカレッジで、約 5100 人の学生を擁し、そのうち 1000 人が全日制である。キッダーミンスターは幅広い全日制・定時制課程（最長で 2 年間）を提供しており、特に舞台芸術学科の評価が高い。キッダーミンスターには、ウースター大学の学生も、キッダーミンスター・カレッジの課程を履修している。

3.2.2 キッダーミンスターには ICT サービスチームがあるが、多くの FE カレッジと異なり、ICT サービスの開発チームは IT 開発に特化し、サポート業務を担当しない。同開発チームは、十分な資金供給を受けており、訓練を積んだスタッフが積極的に開発に取り組み、オープンソース・ソフトウエアの扱いにも通じている。こうした能力は 2003 年に実施されたオープンソース（Moodle）VLE の導入およびその後の開発を通じて培われた。

### *JISC CM プロジェクト*

3.2.3 キッダーミンスター・カレッジは、e ラーニング普及促進プログラム［Distributed e-Learning Programme］において JISC が資金提供した地域的パイロットプログラムの一環として、2 つのプロジェクト（WM-share[7]および ePistle[8]）の Shibboleth コンポーネントに取り組んだ。これらのプロジェクトへの取り組みに伴い、同カレッジは、横断的アクセス管理を実装・展開し、エンドユーザーへの必要なリソースの配信を促進している。

3.2.4 加えて、キッダーミンスター・カレッジは（プロジェクト・パートナーであるウースター大学および RSC ウェスト・ミッドランドとともに）、2 年間にわたる同大学のプロジェクト、キッダーミンスター・カレッジ学習教材リポジトリ［Kidderminster College - Repository of Learning Objects: KC-ROLO］に対し、JISC の CM テクノロジー開発プログラムに基づく資金提供を受けている。このプロジェクトの主たる目的は、キッダーミンスター・カレッジと地域サポートセンター［Regional Support Centre：RSC］ウェスト・ミッドランド[9]との間に横断的アクセス管理を実装し、セキュリティが確保された方法でレポジトリや VLE を共有できるようにすることであった。

3.2.5 KC-ROLO プロジェクトにおける最初の取り組みは、Shibboleth IdP と Shibboleth SP をキッダーミンスター・カレッジにおいて実装することだった。JISC から資金提供を受けたプロジェクト要素のうち、本ケーススタディで焦点を当てるのもこの部分である。しかし、その後も KC-ROLO プロジェクトの作業は継続して進められており、複数の IdP を導入したほか、地域フェデレーションを実現するために WAYF をキッダーミンスターにおいて設置している。

### *サービス・プロバイダー*

3.2.6 キッダーミンスターにおいて提供されるサービスの過半が内部サービスである。全ユーザーが次のサービスにアクセスできる。

- VLE
- ファイルサービスおよびプリントサービス
- 電子メール（現在は職員のみ。学生用の電子メールは 2007 年 7 月開始の見通し）
- Athens の保護リソース（ただし少数。これらのリソースへのユーザー需要は非常に小さい）[10]
- ウェブベースの情報レポジトリ（コンテンツを追加できるのは職員のみ）

### *ID 管理*

3.2.7 学生がキッダーミンスターに入学すると、固有の ID 番号を与えられる。学生はこれを使って自分自身のユーザーアカウント（ユーザー名およびパスワード）を作成する。このアカウントは IT サービスから別段の通知がない限り 1 年後に自動的に失効

[7] WM-share（ウェスト・ミッドランド共有プロジェクト）：パートナー機関のみがアクセスできるように保護された学習リソースのレポジトリを構築するためのプロジェクト。

[8] ePistle（e ピッスル）：フラッシュ・ベースの e ポートフォリオで、セキュリティ保護された認証を実現し、生年月日などユーザー固有のデータを取得するために属性使用を活用するもの。

[9] ウースター大学で類似の態勢を実施する前。

[10] 例外は映画制作課程に在籍する学生と美容師訓練パッケージを利用する訓練生。

する。失効アカウントはアーカイブされる。

3.2.8 ユーザー情報は管理情報システム［Management Information System：MIS］に保存される。キッダーミンスターのアクティブ・ディレクトリは、ユーザーアカウントを属性（「職員」または「学生」）と結びつけてユーザー認証を行い、MIS と 10 分ごとに同期して最新の情報にアップデートしている。セキュリティ侵害の影響を最小化するため、アクティブ・ディレクトリには最小限の情報だけが保存される。

## 3.3 目的

3.3.1 内部プロジェクト[11]の目的は、キッダーミンスター・カレッジ内部で Shibboleth テクノロジーを用いて横断的アクセス管理を実装し、ウェブベースのリソースの連携を図ることであった。

3.3.2 ICT サービス部門が設定した目標は、「全てのリソースおよびサービスを、シングル・サインオンを用いて、3 クリック以内でアクセス可能にすること。」

## 3.4 範囲

3.4.1 内部プロジェクトの範囲に含まれるサービスは、キッダーミンスター・ポータル、Athens 保護リソース、学科別 Moddle VLE およびスタッフ用エクストラネット Moodle VLE ならびに情報レポジトリである。

3.4.2 範囲外のサービスとしては、特定の図書館リソースおよび職業関連リソースがあり、これらについては独自のアクセス制御が保持された。

3.4.3 JISC の資金提供を受け、キッダーミンスターが参加したプロジェクトは、上述の内部プロジェクトよりもはるかに広い範囲を対象としており、複数の IdP を実装したほか、情報共有と連携の促進を図るための地域フェデレーション[12]を設立した。

## 3.5 計画

### *戦略的推進要因*

3.5.1 プロジェクトの主要な戦略的推進要因は次のとおりであった。

- VLE のアクセス性と使いやすさを向上させて、VLE の活用を促進するため。その一環として、キッダーミンスターのユーザーが外部から VLE にアクセスできるようにする。
- 革新的なプロジェクトを通じて、やりがいのある環境を提供することによって ICT サービス・スタッフを留保する必要性。
- 高価なソフトウエアライセンスへの依存を減らさなければならないというコスト面での圧力。
- 地域の他機関との連携体制を構築する必要性。他の大学や機関のユーザーが VLE にアクセスできるようにすることで、提供範囲を拡大し、教育能力や資源の活用を図るため。

[11] JISC が資金提供したプロジェクトのうち、キッダーミンスター内部における横断的アクセス管理インフラ整備にのみ関係する要素。

[12] KC-ROLO フェデレーション。

– 管理費やサポート提供にかかる経費の負担削減。[13]

*オプションの評価*

3.5.2 キッダーミンスター・カレッジでは、Shibboleth テクノロジー以外のオプションについては検討を行わなかった。その大きな理由は、JISC が Shibboleth 実装プロジェクトに資金提供することを調査の初期段階で知り、これに応募して資金を獲得したためである。

3.5.3 当初から、Shibboleth はリスクの低いオプションであると考えられた。キッダーミンスター・カレッジの IT サービス開発チームは、人員も十分でオープンソースのソフトウエアに精通していたからである。また、Shibboleth は VLE をさらに前進させる手段としても有効であると見なされた。

*コスト負担*

3.5.4 JISC のプロジェクトに先立って、キッダーミンスター・カレッジでは、オープンソース・ソフトウエアに関する能力や知識、組織内の専門能力を強化するため、オープンソースに関する研究調査プロジェクトが開始されていた。このプロジェクトの成果が、後に、Moodle VLE や Shibboleth テクノロジーの開発や展開を支えることになったのである。このプロジェクトには、約 3 万 9500 ポンドの費用がかかったと概算されている。その内訳は次のとおりである。

- **研究調査：**これにかかった作業は、開発者の労働時間 1 年分（フルタイム換算）と推定され、その費用は約 2 万 5000 ポンド相当。
- **スタッフ開発：**スタッフ開発訓練コース（例：Linux、SAML）に約 4000 ポンドを支出。
- **設備：**プロジェクトを支援するための特定の設備（例：サーバー）に約 3500 ポンドを支出。
- **施設とインフラ：**他の大学資源（スタッフおよびハードウエアなど）に約 5000 ポンド、作業場所（施設、暖房、照明など）に約 2000 ポンドが使われた。

3.5.5 上述の内部プロジェクトより広い範囲を対象とした JISC プロジェクト全体に対し、キッダーミンスターは次の資金を受け取った。

- 早期採用者プロジェクトの Shibboleth 実装について 4 万ポンド
- KC-ROLO プロジェクト（第 3.2.4 項参照）について 9 万 2000 ポンド
- ウースター大学から JISC 資金 2 万 4000 ポンド

3.5.6 事後の概算によると、JISC 資金に加えて、キッダーミンスターが KC-ROLO に拠出したのは 1 万 9500 ポンドと推定された。キッダーミンスターは、JISC 資金がなくても Shibboleth を実装した可能性が高いが、JISC 資金が無ければ、これほど早期に、かつ迅速に整備されることはなかったであろうと考えられる。

3.5.7 キッダーミンスターの事例においては、JISC プロジェクトは横断的アクセス管理の実装以外の要素も含んでいるため、実装そのものに要した費用を具体的に提示する

[13] これはキッダーミンスターで課程を履修するウースター大学の学生にとって特に問題であった。アカウントの手作業による発行が必要であったからである。

ことができない。しかし、Shibboleth IdP や SP を実装・サポートするサービスを他の機関に提供してきた経験から、キッダーミンスターは横断的アクセス管理の導入に必要な活動は概ね次のとおりであるとしている。

- **内部審査：**構成やファイル保管、セキュリティ等の監査
- **アクティブ・ディレクトリの実装：**内部スタッフの教育訓練（5 日）、監査（支援を得て 3 日）、実装（内部で実装する場合は 6 カ月程度の期間をかけて実質 20～30 日の作業、または外部の専門家を使用）
- **ファイアウォール構成：**1 日
- **属性格納場所の設定**：支援を得て 2 日

*達成可能性*

3.5.8 プロジェクトは、IT サービス開発チームの人員および能力を活用して達成された。開発チームのスタッフは、Linux を扱った経験を有するなど、当初から良好なスキル基盤を有していたが、Apache や電子認証など他のテクノロジーについても調査研究を行う必要があった。

3.5.9 作業の大半を担ったのは、1 人の開発者であった。しかし、キッダーミンスターでは、新規技術や既存の技術分野において、スタッフにさらなる訓練を提供するとともに、開発スタッフを新たに雇い入れるなど、この機会を活用して専門能力の一層の強化を図っている。

## 3.6 実施

*成果*

3.6.1 意思決定は、ICT サービス部門長が ICT 担当運営責任者である副学長とともに行った。両者は毎週会合を持ち、プロジェクトについて協議した。

3.6.2 プロジェクトの開始にあたって、Shibboleth 試験サービスが実施された。IT サービス部門は、キッダーミンスターVLE についても責任を負っている。この 2 つの作業の流れは、互いに緊密なコミュニケーションを図りながら進められた。図書館は、プロジェクトの後期まで関与しなかった。Athens 保護リソースへのシングル・サインオンはプロジェクトの主要な目的ではなかったからである。

3.6.3 Shibboleth の本格サービス（Shibboleth 保護ポータル、学科別 Moodle VLE、スタッフ用エクストラネット Moodle、Shibboleth 対応レポジトリ）は、2006 年 4 月に職員および学生に展開された。

3.6.4 学生および職員は現在、複数回にわたりサインオンしなくても、内部のウェブリソースにアクセスすることができると同時に、横断的アクセス管理を通じて外部の Athens 保護リソースにもアクセスできるようになった。

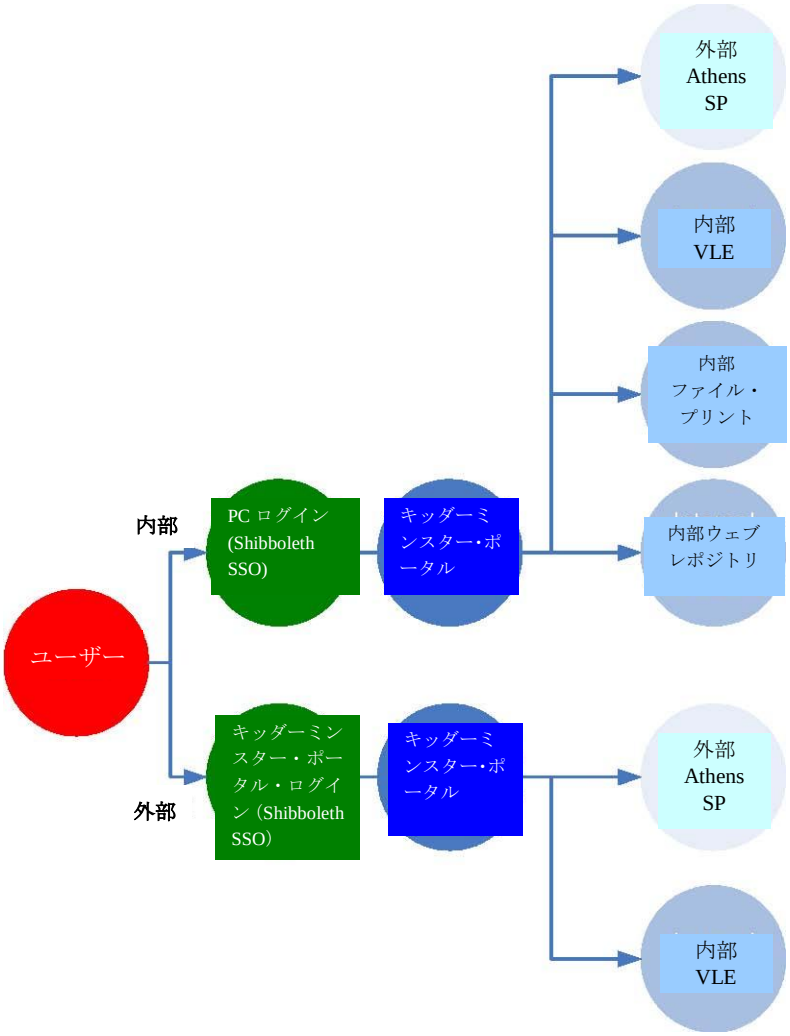


図 3-1：キッダーミンスターにおける現在のアクセス管理態勢

*実現した便益*

3.6.5 このプロジェクトは多くの便益をキッダーミンスター･カレッジにもたらしている。

- ネットワークやウェブリソースへのアクセスに利用できるシングル・サインオン・システムが実装され、ユーザーエクスペリエンスが向上した。
- 外部ユーザーがキッダーミンスターのウェブリソース（VLE など）にアクセスできるようになった。このため、例えば、キッダーミンスターの外部で過ごすことが多い遠隔地学習者にとっての利便性などが格段に改善された。
- IT サービスチームによると、VLE の利用が増えた。
- セキュリティが確保された方法により、機関間でリソースを共有することができるようになった。リソースに対する機関相互アクセスへの可能性が開け、職員や学生が連携して学習リソースを利用できるようになった。リソース共有は柔軟に行うことができ、例えば、キッダーミンスターで課程を履修している通学ユーザーが VLE へのアクセス権を得ることもできる。
- 管理経費が削減された（特に、キッダーミンスターの課程を履修しているウースター大学の学生について）。
- キッダーミンスターは、これまでに蓄積した専門知識を活用して、他の機関に対し、Shibboleth IdP や SP を実装・サポートするサービスを提供している。キッダーミンスターのチームは、他の機関で専門的なサポートと支援を提供し、このテクノロジーに関するスタッフの教育訓練に役立っている。
- オープンソース・ソフトウエアへの取り組みは、開発チームにとって良い刺激となり、スタッフの定着に効果があっただけでなく、同部門の拡大にもつながった。

## 3.7 直面した課題と得られた教訓

3.7.1 キッダーミンスターでの Shibboleth の実装は非常に円滑に進み、大きな課題には直面しなかった。

3.7.2 キッダーミンスターでは、このプロジェクトを通じて次の教訓が明らかになった。

- Shibboleth の実装には初めに学ばなければならないことが非常に多い。しかし、ひとたびスキルを獲得してしまえば、管理やサポートが比較的簡単なテクノロジーである。
- 導入を予定している機関に、例えば属性格納などの必要条件が整備されていない場合には、初期費用はもっと高くなるかもしれない。
- IdP を導入する際の事務的手続が一部の機関では非常に煩瑣であることを考えると、導入を予定どおり進めるためには、しっかりとした事前計画が必要である。
- 図書館利用案内時が「リソース使用」の呼びかけをユーザーに行き渡らせるための主要な機会である。図書館利用案内に間に合うよう各種の変更を実施し、トレーナーの教育訓練を実施しなければならない。
- 実装チームと図書館の間で良好なコミュニケーションが必要である。
- 共通のテクノロジーだけでは、連携は実現しない。コンテンツの共有について、全ての当事者による合意と関与が不可欠である。
- プロジェクトのスポンサーは、熱意と責任をもって臨まなければならない。

### 3.8 将来の計画

3.8.1 キッダーミンスターは将来に向けて次の計画を掲げている。

- 第 2 の IdP を実装することによってサービスの障害許容力を高める。
- 他のリソースも Shibboleth 対応化する（例：電子ポートフォリオ）。
- KC-ROLO フェデレーションのためのキッダーミンスターWAYF の使いやすさを向上させる。

### 3.9 有用な資料

3.9.1 次の文書がキッダーミンスターによって著されている。

- Shibboleth in Further Education（継続教育における Shibboleth の利用）10 May 2006（2006 年 5 月）, Tim Hall, ICT Services Development Team, Kidderminster College（キッダーミンスター・カレッジ ICT サービス開発チーム、ティム・ホール）<http://www.matu.ac.uk/uploaded-pdf/Shib_FE_Final_KM.pdf>
- KC-ROLO Final Report（KC-ROLO 最終報告書）, 14 March 2006（2006 年 3 月 14 日）, Graham Mason and Ed Beddows（グラハム・メイソンとエド・ベドーズ）<http://www.jisc.ac.uk/media/documents/themes/access_management/kc-rolo final report.doc>
- Shibboleth user guide（ユーザーガイド）<http://Kidderminster.ac.uk/kc-rolo>

# 4 サリー大学

## 4.1 概要

4.1.1 Classic Athens アクセス管理システムを新システムに切り替えるサリー大学のプロジェクトは、2005 年 4 月に着手された。プロジェクトの主たる目的は権限委譲型の認証システムを実装することによって IT スタッフの管理面での負担を軽減するとともに、ユーザーが覚えておかなければならないユーザー名やパスワードの数を減らすことであった。サリー大学は AthensDA の実装を決定した。AthensDA は、成熟したシステムで、多くの機関で既に導入された実績がある上に、Eduserv によって技術サポートが提供されるからである。さらに、サリー大学は非常にコンパクトなスタッフ構造を採っており、IT スタッフも少ないことから、Shibboleth のようなオープンソース・テクノロジーの導入に必要な広範な技術的専門知識を内部に保有していない。

4.1.2 サリー大学は 2006 年 6 月に AthensDA と新たな IDM システムの運用を開始した。2006/2007 学年度の新規ユーザー全員に対し、ローカルのユーザー名とパスワードしか発行しなかった。2006 年 11 月までに、サリー大学は、既存ユーザーが Classic Athens のユーザー名とパスワードでは、リソースにアクセスできなくなるようにした。

| | |
|---|---|
| **機関名** | サリー大学 |
| **JISC Collections 社類型** | D |
| **ユーザー数** | 1 万 8500 人（学生 1 万 6000 人、職員 2500 人） |
| **プロジェクト開始期** | 2005 年 2 月 |
| **プロジェクト終了期** | 2006 年 11 月 |
| **プロジェクトの主要目的** | Classic Athens システムの管理負担を軽減すること、サリー大学の統合サインオン・システムに Athens 保護リソースを組み込んでユーザーエクスペリエンスを向上すること |
| **意思決定に携わる関係者** | 次席 IT 責任者<br>e 戦略およびリソース・マネジャー（図書館）<br>学術サービス・グループ・マネジャー（IT サービス部門）（プロジェクト・マネジャー） |
| **財源** | 図書館予算（プロジェクト・スポンサー : 図書館サービス部門長） |
| **主要マイルストン** | AthensDA 稼働開始（2006 年 7 月）<br>Classic Athens 機能停止（2006 年 11 月） |
| **現行のアクセス管理システム** | AthensDA およびサリー統合サインオン・システム |
| **以前のアクセス管理システム** | Classic Athens およびサリー統合サインオン・システム |

## 4.2 背景

### *サリー大学*

4.2.1 サリー大学は比較的大規模な総合大学で、その情報システムは約 2 万 6000 人のユーザーをサポートしている。サリー大学の IT サービスは、主として運用・ビジネス指

向で、研究・開発指向ではない。このため、リスクが高いと思われるテクノロジーを避ける傾向がある。同大学では、オープンソース・ソフトウエアよりも、有料サポートサービス付の成熟した商用システムを実装するという全学的な方針をとっている。これは主に、サリー大学のスタッフ構造がコンパクトで、特にオープンソース・ソフトウエアに関しての広範な技術的専門知識を内部に保有していないためである。

4.2.2 図書館は、サービス・プロバイダーへの加入、および、Athens のどのリソースにアクセスできるかを制御する許諾指定に関して責任を負っていた。一方 IT サービス部門は、毎年作成される各ユーザーの Classic Athens アカウントの作成・維持に責任を負っていた。IT サービス部門は、学生および職員のためのヘルプデスクも運営し、パスワード管理にも責任を負っていた。当時は、サリー大学のローカル・ユーザー名とそれとは別個の Athens ユーザー名およびパスワードが各新規ユーザーに発行されていたのである。

4.2.3 サリー大学における IT の提供は比較的分散されている。IT サービス部門はサリー大学キャンパスにおける全システムに対して全面的な統制を行っているわけではなく、例えば、各学部で独自のコンピュータを運用している。IT サービス部門の管理下にある学生用コンピュータは、定期的に（週に 1 回）リビルドされている。

*サービス・プロバイダー*

4.2.4 サリー大学におけるユーザーが使用可能なウェブサービスには、次のものがある。

- 電子ジャーナル、電子データベース、電子書籍
- Blackboard VLE
- 電子メール
- 図書館文献目録

***ID 管理***

4.2.5 サリー大学の IDM は 2006 年夏にアップグレードされた。AthensDA システムの主要目的は、ユーザーの ID を IDM システムが作成したコンピューティング・アカウントから認証することであった。新しい自動コンピューティング・アカウント登録システムは 2006 年 6 月に稼働を開始した。

4.2.6 新システムは次のシステムから情報を抽出することによって全ての学生および職員についてコンピューティング・アカウントを作成する。

- 学籍簿システム（学生データベース）
- 人事システム（職員データベース）
- マニュアル・アカウント登録システム（招聘教員など一時的ユーザーを登録するために使用）

4.2.7 権限委譲型の認証と属性に基づく権限付与を実現するため、属性格納は、登録システムの全ユーザーアカウントに加え、固有 Athens 識別子、各ユーザーに適切な許諾指定の組合せを含む Oracle テーブルとして維持されている。このテーブルに最新の状態に維持するため、登録データベースと毎夜同期している。サリー大学のユーザーには、職員と学生の 2 種類のユーザー許諾指定の組合せしかない。図書館がこの

指定に関して責任を負っている。ユーザーのログインは、アクティブ・ディレクトリに照らして認証される。

## 4.3 目的

4.3.1 Classic Athens アクセス管理システムを新システムに切り替えるプロジェクトの主たる目的は、IT スタッフの管理負担を軽減するとともに、単一のユーザー名・パスワードに一本化することによりユーザーエクスペリエンスを向上させるため、権限委譲型の認証システムを実装することであった。

## 4.4 範囲

4.4.1 サリー大学は、ユーザーが単一のユーザー名とパスワードを用いて、各種のローカル･リソースにアクセスできる統合サインオン･システムをすでに運用していたが、この範囲を拡大して、Athens 保護リソースへのアクセスも含めたいと考えた。統合サインオン・システムの範囲に含まれるサービスは、次の内部リソースなどである（キャンパス内外からアクセス可能)。

- ネットワークログイン
- VLE
- 電子メール

## 4.5 計画

### *戦略的推進要因*

4.5.1 このプロジェクトの主要な戦略的推進要因は次のとおりである。

- 各新規ユーザーに 2 つのユーザー名とパスワードを作成するための経費が管理上の大きな負担となっており、改善が必要と見なされていた。
- 各学年度の始まりにおける Athens アカウントの自動作成は負担が大きかったため、負荷ピーク時には、不具合も生じやすく、修正のために手作業による介入が必要であった。
- 記憶すべき複数のパスワードがあることは、良好なユーザーエクスペリエンスにつながらず、電子リソースの利用を拡大する上での障壁と見なされていた。

### *オプションの評価*

4.5.2 サリー大学は新しいアクセス管理システムについて､次のような要件を設けていた。

- 信頼性が高く成熟したテクノロジーで、本格運用が行われる環境において全機関規模ですでに導入された実績を有するもの。
- 有料サポートサービス付の商用テクノロジーの方が望ましい。
- 2 つのサービスを同時に運用することは避けたい。

4.5.3 サリー大学は Classic Athens システムの後継として 3 つのオプションを検討した。

- AthensDA
- Shibboleth テクノロジー

- AthensIM

4.5.4 プロジェクト・マネジャーが各オプションについて、それぞれの利点と考慮すべき事項を調査し、2005 年 4 月にオプションに関する意思決定用の文書にまとめた。さらに、意思決定に携わる関係者がミドルウエア採用支援サービス［Middleware Assisted Take-Up : MATU］チーム[14]と 2005 年 11 月に会合し、これらのオプションについてさらに協議を進めた。

4.5.5 サリー大学にとって、各オプションの利点とリスクは次のとおりとされた。

- **AthensDA：**
  - **利点：**権限委譲型認証が可能。成熟しており、いくつもの機関ですでに導入実績あり。Eduserv による技術サポートあり。
  - **リスク：**AthensDA は短期的なソリューションとなる可能性が高い。JISC でも国際的にも、Shibboleth が選択されつつあり、やがては Shibboleth が AthensDA に取って代わると予想されることから、コスト面での利点が低減する。
  - **コスト：**実装時間（リソース要件がより少ない）、OpenAthens 利用料（検討時には不明）。

- **Shibboleth テクノロジー：**
  - **利点：**大学全体にシングル・サインオン・システムを整備することが可能。英国の教育研究界についての JISC の計画と整合。
  - **リスク：**外部の技術サポートは得られない。コミュニティに依存。これまでの実装実績は、ほとんどパイロット環境のみ。
  - **コスト：**ソフトウエアは無料。実装に際し、多大な内部技術リソースが必要。

- **AthensIM：**
  - **利点：**大学全体にシングル・サインオン・システムを整備することが可能。英国の教育研究界についての JISC の計画と整合。Eduserv からサポートが得られると予想される。
  - **リスク：**AthensIM は 2005 年 2 月にリリースされたばかりで小規模なパイロット環境でしか導入されていない。
  - **コスト：**ソフトウエアは無料。実装に際し、多大な内部技術リソースが必要。

4.5.6 最も好ましいオプションは AthensDA または AthensIM を実装することであった。その主たる理由は、Shibboleth テクノロジーを実装するためには、コミュニティのサポートに依存しなければならなかったが、サリー大学はこれを望まなかったためである。AthensDA を飛ばして、Shibboleth へと「一足飛びに」先取りするというオプションが、長期的ソリューションとして優れていることは認識されていたものの、AthensDA が全員一致で採択された。サリー大学としては、堅牢なサービスであることが何より肝要であり、実際に運用するサービスで最先端を走りたいとは望まなかったからである。

[14] MATU サービスは JISC の CM プログラムの一部であった。FE・HE 機関のうち、横断的アクセス管理の早期採用者に対し助言と支援を与えた。

*コスト負担*

4.5.7 プロジェクトの資金はITサービス部門の予算の中から拠出され、図書館サービス部門長がプロジェクトのスポンサーとなった。プロジェクトのための資本支出は少なかったが、多大な人手を要した。各チームの要員に求められる作業量の当初見積もりは、プロジェクト着手文書［Project Initiation Document］に示されているが、実際に要した作業量の総計は次のとおりであった。

- IT サービス：15 週
- 技術開発：2.5 週
- 図書館試験実施：3 週[15]

4.5.8 電子リソースを含め、図書館の全リソースは、図書館リソース予算（年間 180 万ポンド）から賄われる。2008 年から有料化される OpenAthens の利用料をどの部門が負担するかは今のところまだ明らかでない。

*達成可能性*

4.5.9 アセスメントの結果、プロジェクトは図書館と IT サービス部門の現在の能力の範囲内で達成できると判断された。外部からの技術的サポートは、必要に応じて Eduserv が提供した。

4.5.10 意思決定に携わる関係者は 3 人で構成された。プロジェクト・マネジャーに加えて、IT サービス部門と図書館サービス部門のそれぞれの代表者である。

4.5.11 プロジェクトチームの構成は以下の通りであった。

- プロジェクト・マネジャー（IT サービス部門の学術サービスグループから）
- 技術責任者（IT サービス部門から）
- インフラ開発担当開発者（IT サービス部門のコーポレート・インフラ・チームから）
- 試験・周知担当の図書館スタッフ（e 戦略およびリソース・マネジャー）

## 4.6 実施

*成果*

4.6.1 サリー大学は、2006 年 7 月に AthensDA の稼働を開始した。2006/2007 学年度の新規ユーザー全員に対し、ローカルのユーザー名とパスワードしか発行しなかった。2006 年 11 月、サリー大学は既存ユーザーが Classic Athens のユーザー名とパスワードを使ってリソースにアクセスできないようにした。移行期間を比較的短期間しかとらなかったが、この方法は成功した。

4.6.2 AthensDA 実装の作業を時系列に並べると次のとおりであった。

- 2005 年 4 月：プロジェクト・マネジャーがオプション評価文書を作成。
- 2005 年 11 月：サリー大学が採りうるオプションについて、さらに協議するため

[15] 2006 年 1 月から 2006 年 11 月までのプロジェクト期間全体を通じて折々に実施された。

MATU と会合。
- 2005 年 12 月：AthensDA の実装を決定。
- 2006 年 1～3 月：AthensDA システムを構築。
- 2006 年 3～5 月：AthensDA システムを試験（各種リソースの対応状況の試験を含む）。
- 2006 年 6 月：稼働開始を決定（新 IDM システムも稼働開始）。
- 2006 年 7 月：AthensDA 本格サービスを展開。
- 2006 年 8 月：サービスの組み込み。
- 2006 年 11 月：全ての既存 Classic Athens アカウントが失効。

4.6.3 新しいインフラの技術的な開発と試験に並行して、AthensDA とその導入が持つ意味を AthensDA の稼働開始に先だってユーザーに徹底的に周知した。その一環として、ユーザーに一連の電子メールを送ったほか、図書館のウェブサイトに宣伝のためポスターを掲示し、各課程の掲示板にも変更について掲載した。2 台のサーバーを稼働させ、負荷分散ソフトウエアを使用することにより、システムに障害許容性を確保した。これは、実際にもよく機能している。

4.6.4 サリー大学のアクセス管理システムは現在、次の要素で構成されている。

- **統合サインオン：**ネットワーク、VLE、AthensDA リソース、電子メール、職員用イントラネット。
- **図書館システム：**バーコード、PIN（図書館アカウントのみ）。
- **特定サインオン：**特定サービスのための特定ユーザー名・パスワード（例：SAP）。
- **キャンパス外からのアクセス：**キャンパス外のユーザーもゲートウエイによって情報リソース（IP 認証を介してのみ利用可能）とユーザーの個人／共有集中ファイル・ストレージにアクセスすることができる。

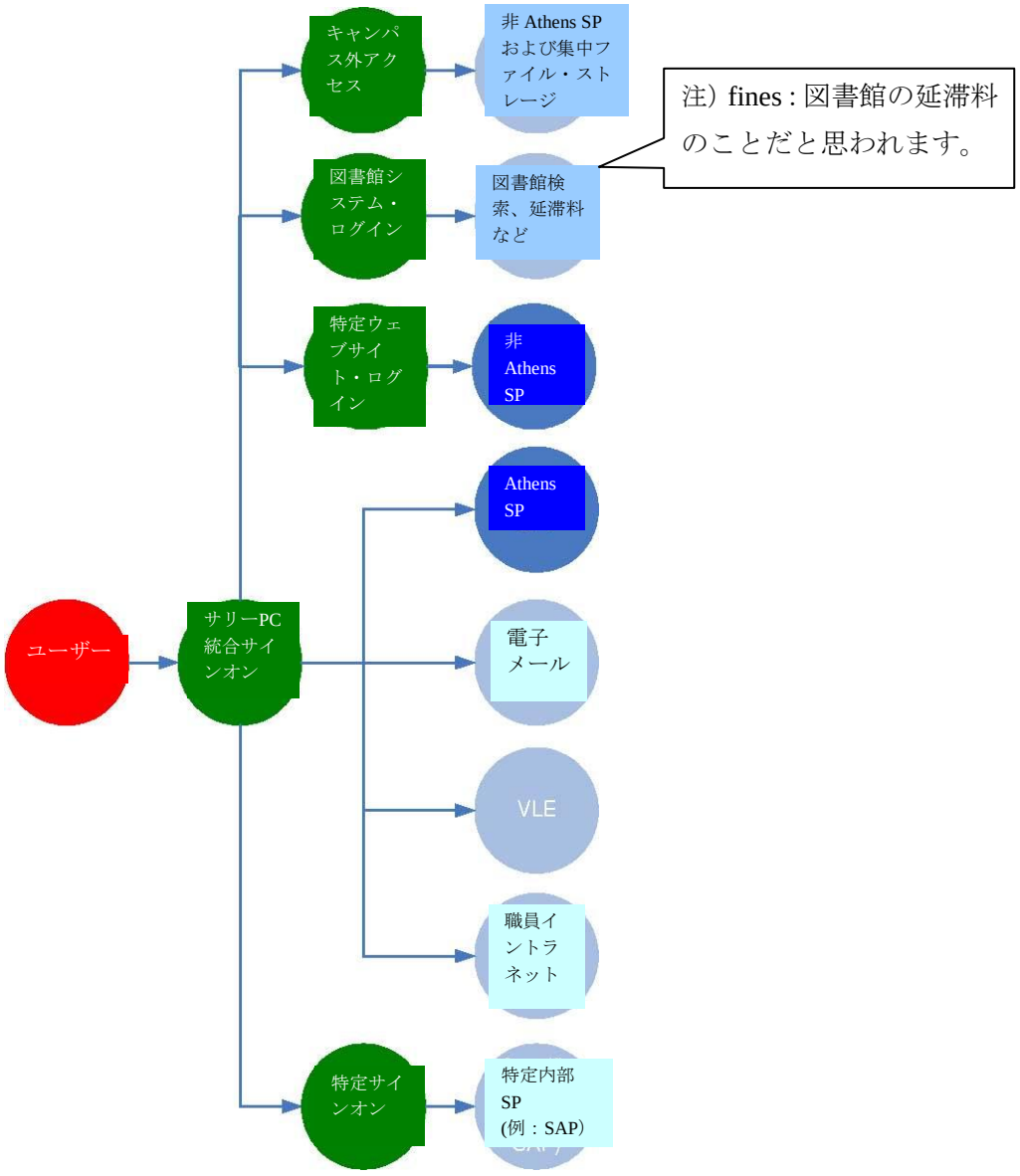


図 4-1：サリー大学における現行のアクセス管理態勢

*実現した便益*

4.6.5 このプロジェクトは多くの便益をサリー大学にもたらしている。

- Athens 保護リソースが、統合サインオン・システムの一部となり、ローカルのユーザー名とパスワードでアクセスできるようになった。新システムについてユーザーから肯定的な反応が図書館に寄せられており、ユーザーエクスペリエンスを向上させたと考えられている。
- ヘルプデスクへの問い合わせのために要していた図書館経費が軽減された。現在問い合わせがあるのは、あるひとつの「よくある問題」（4.7.1 の項を参照）についてだけで、その他の問題はあまり発生していない。この特定の問題については、標準的な対応が用意されている。
- ユーザー間でのアカウント共有が減ったと考えられている。ユーザーは Classic Athens アカウントに比べ、自分のローカル・アカウントを共有することは少ないからである。
- ピーク時のアカウント作成に IT サービスのスタッフが手作業で介入する必要が減少した。
- AthensDA プロジェクトのために、サリー大学は ID 管理プロセスをアップグレードしなければならず、認証の責任を大学が負うようになった。これで横断的アクセス管理の採用に向けて一歩近づいたと考えられる。

## 4.7 直面した課題と得られた教訓

*課題*

4.7.1 AthensDA の実装は成功し、非常に円滑に進んだ。プロジェクト・マネジャーが優秀だったことが幸いした。直面した主な課題は次のとおりである。

- **クッキー管理：**AthensDA では、ユーザーが永続的なクッキーを使う必要がある。どの組織が認証を行うべきかをこのクッキーによって特定するのだが、Athens アクセス管理システムが検出するにはユーザーが実際に使用している PC にクッキーが存在していなければならない。しかし、サリー大学のユーザーはローミング・プロファイルを有さず、学生は複数の PC を使用する。さらに、キャンパスにある学生用 PC は毎週リビルドされるため、クッキーは全て削除されてしまう。このため、IT サービス部門がサポートするキャンパス内 PC から AthensDA リソースにアクセスするユーザーのために、IT サービス部門は回避策を講じた。ユーザーが PC にログインする際に、当該ユーザー用のクッキーが、自動的かつ透過的に生成されるようにした。しかし、キャンパス外の PC を使用するユーザーは、自分の PC にクッキーを生成するようアドバイスされている。これが、一部のユーザーにとっては問題となりうる。
- **Athens リソースのアクセス性：**NHS のファイアウォールは制限が厳しく、サリー大学は NHS の学生による AthensDA リソースへのアクセスをめぐり問題に直面した。
- **アカウント移行：**AthensDA では、ユーザーが一部のサービス・プロバイダー（例：ScienceDirect）に詳細情報を再度登録するよう要求された。こうした個人アカウントの機能性／属性（例：保存した検索、統計データについての登録）は Classic Athens から AthensDA アカウントに移行されなかった。この点も、ユ

ーザーにとっての問題となったが、そうした機能を使用する者は個人の登録情報を再作成したため、大きな問題にはなっていない。

***教訓***

4.7.2 次の教訓が明らかになった。

- 学生が使用するオープンアクセスのデスクトップなど、共有 PC 設備においてクッキーの使用が及ぼす影響を理解する必要がある。デスクトップ管理方針を精査し、AthensDA の組織クッキーにどのような影響を与えるかをよく理解することが重要である。
- 潜在的な課題を事前に特定しやすくするため、同じアクセス管理システムを既に実装している他の機関に話を聞くことが有益である。
- 試験環境を持つことが有益であった。より自信をもって本格サービスを展開できるからである。
- 新システムをユーザーに広く周知することが不可欠である。どんなに広報を徹底しても、新システムには問い合わせがつきものである。

## 4.8 将来の計画

4.8.1 サリー大学は将来に向けて次の計画を掲げている。

- AthensDA が OpenAthens 有料サービスの一部になる 2008 年 7 月以降もサリー大学は AthensDA を使用し続けると予想される。サリー大学は、Shibboleth テクノロジーが成熟し、本格サービスとして他機関で導入されるようになるのを待ってから、サリー大学での実装を検討することになるであろう。
- 多様なグループと提携する機会が増え、サリー大学のリソースを使用する資格を持たないユーザーのグループとも提携することが多くなるにつれ、アクセス粒度が問題になり始めている。例えば、サリー大学のユーザーとして登録されないものの、サリー大学で英語を勉強する「スタディー・グループ［Study Group］」課程の場合がそうである。粒度がもっと高ければ、ユーザーに特定のリソースへのアクセス権を付与し、ベンダーと交渉してライセンス契約を増やすこともできたであろう。サリー大学では現在、IT 部門の責任者を交代し、IT 部門の再編成を行っている最中であるため、将来について計画を立てることが非常に困難になっている。しかし、Shibboleth テクノロジーの利点については検討を行っている。さらに、IT サービス部門が Kerberos その他のベンダーのソリューションを含め、シングル・サインオン・ソリューションを調査している。

このページは敢えて空白にしてある

# 5. ウォーリック大学

## 5.1 概要

5.1.1 2005 年 1 月、既存のシングル・サインオン・アクセス管理システムをアップグレードし、セキュリティを向上させるプロジェクトを開始した。ウォーリック大学は Shibboleth プロファイル・ベースのシステムを開発した。Athens リソースには Shibboleth-Athens ゲートウエイを介してアクセスする。これによりウォーリック大学は、必要に応じてフェデレーションへの加入と横断的アクセス管理の導入を行うことができる準備が整った。

| | |
|---|---|
| **JISC Collections 社類型** | C |
| **ユーザー数** | 職員最大 5000 人、ユーザー最大 2 万人 |
| **プロジェクト開始期** | 2005 年 1 月 |
| **プロジェクト終了期** | 継続中。2006 年 9 月に主要マイルストンを達成 |
| **プロジェクトの主要目的** | 既存のアクセス管理システム（SSOv2）をアップグレードして、さらにセキュリティを強化した堅牢なシングル・サインオン・システムを、ウォーリック大学でウェブサービスにアクセスするユーザーに提供すること。 |
| **意思決定に携わる関係者** | IT サービス |
| **財源** | 特定のプロジェクト財源はなく、ウェブチームの予算の中から賄われた。 |
| **主要マイルストン** | SSOv3 の導入<br>Shibboleth-Athens ゲートウエイの稼働開始 |
| **現行のアクセス管理システム** | カスタマイズされた AthensIM を実装した SSOv3（Shibboleth-Athens ゲートウエイを使用）。Shibboleth 非対応の Athens リソースへのアクセスには AthensDA を使用。 |
| **以前のアクセス管理システム** | SSOv2（Java およびクッキー）ならびに Classic Athens |
| **フェデレーションへの加入** | 現在は未加入 |

## 5.2 背景

*ウォーリック大学*

5.2.1 ウォーリック大学は緩やかに統合された総合大学であり、職員約 5000 人と学生 2 万人を擁している。ウォーリック大学には豊富な資金とリソースを備えた IT サービス部門があり、高い能力と実績を有する自前の開発チームがある。E ラボは、IT サービス内の一部門であり、ウォーリック大学の e 戦略プログラムの実施に関する調整や、新しいテクノロジー、特にウェブサービスと e ラーニングの分野における研究開発を担当している。E ラボはこれまでに、可用性が高く革新的な一連のウェブサービスを提供してきた成果を誇っている。E ラボは現在、ITIL サービス管理に移行しつつある。

5.2.2 ウォーリック大学は 2002 年以来、シングル・サインオン・システムを運用し、ウェブサービスやウェブアプリケーションへのアクセスの円滑化を図ってきた。これは

当初、クッキーによるシンプルなアプローチに Classic Athens を組み合わせたもの（SSOv1）であったが、やがてクッキーを用いた Java ベースのシステムと Classic Athens を組み合わせたもの（SSOv2）にアップグレードされた。

*サービス・プロバイダー*

5.2.3 ウォーリック大学のシングル・サインオン・システムには約 40 のサービスが含まれている。これらは全て内部サービスで、ウォーリック大学が自ら開発したものである。いくつかの例をあげると、コンタクト管理、ブログ用プラットフォーム、フォーラムシステム、パーミッション・ベースの検索エンジン、ウェブグループ・システム（例：時間割、モジュール登録）などがある。唯一の外部サービス・プロバイダーは Athens 保護リソースである。

5.2.4 キャンパス内のコンピュータへの初回ログオンとウェブメールは、シングル・サインオン・システムの一部ではない。ウォーリック大学のユーザーの中には、一部のデータベースなど、外部の非 Athens サービスへのアクセスが必要な場合もある。

***ID 管理***

5.2.5 学生の記録と登録情報は集中管理型のメンバーシップ・データベースに入り、当該データベースは 5 つほどのサテライト・サーバーに入る。他にも別個のデータベースがあり、他のメンバー・グループの ID 情報を保持している。例えば、ビジネススクール（ウォーリック大学のビジネススクールは、大学からの独立性が高い）、同窓会、優秀な生徒のための国立アカデミー［National Academy for Gifted and Talented Youth：NAGTY］（4 万～5 万人のユーザーがいる）では、別個のデータベースを有している。

5.2.6 ID データベースの合理化を目的とした IT サービス・プロジェクトを 2006 年の初めに着手、現在も継続中である。

**5.3 目的**

5.3.1 プロジェクトの主たる目的は、ウォーリック大学における既存のアクセス管理システム（ウェブサービスへのアクセスを管理する）をアップグレードし、そのセキュリティの向上を図ることであった。

**5.4 範囲**

5.4.1 プロジェクトの範囲は現行のシングル・サインオン・システムとシングル・サインオン・システム対応のサービスであった（第 5.2.3 項を参照）。

**5.5 計画**

*戦略的推進要因*

5.5.1 近年、ウォーリック大学は多数のウェブサイトを構築したが、その多くで、学生が独自の資料を公開できるようになっている。こうした仕組みには、ユーザーID のセキュリティが侵害される潜在的な可能性がある。例えば、他者の ID を用いて情報を掲載したり、他者向けの資料にアクセスしたりすることによって、セキュリティが

侵害される危険がある。

5.5.2 既存のシングル・サインオン・システムをアップグレードした主たる戦略的推進要因は、クロスサイト・アタックに対する堅牢性とセキュリティを向上させる必要性である。

*オプションの評価*

5.5.3 利用可能な技術的オプションを評価するため、2005 年、E ラボは資料調査を実施した。ウォーリック大学は以下にあげるような、いくつかの既製ソリューションの仕様を検討した。

- Microsoft のソリューション。
- Sun Access Manager。
- エール大学の集中型認証サービス［Central Authentication Service：CAS］。
- Liberty Alliance の ID-FF ソリューション。
- Internet2 の Shibboleth テクノロジー。

5.5.4 ウォーリック大学はすでにシングル・サインオン・システムを運用していたため、同大学が新システムに求める要件について、明確な考えを持っていた。ソリューションは現行のアーキテクチャと手法（例：Java ベース）に適合すると同時に、現行の全ての機能に対応でき、その上で、セキュリティと堅牢性の向上が図れるものでなければならなかった。調査の途上で、JISC がイギリスの FE および HE 向けに Shibboleth テクノロジーを選択する方向に向かっていることが判明した。

5.5.5 ウォーリック大学の要件に合致するオプションは多くなかった。例えば、CAS はシングル・サインオンを実現するものの、シングル・ログアウトには対応していなかった。彼らの要件に合致する唯一のオプションが Shibboleth テクノロジーであった。しかし、2005 年初めの段階では Shibboleth プロファイルの実装例は少なく、ウォーリック大学のアーキテクチャと手法に適合しなかった。そこで、Shibboleth プロファイルの AthensIM リファレンス実装を独自に開発し、これをより広範なシングル・サインオン・システムに組み込むというオプションを選択したのである。

*コスト負担*

5.5.6 このプロジェクトは、特定プロジェクトとして資金供給を受けたわけではないので、予算獲得のための特定要件がなかった。プロジェクトの資金は、IT サービス部門のウェブチームの予算から直接拠出された。

5.5.7 作業の大半を担ったのは、1 人の開発者で、ほぼ 1 年間をかけて集中的に取り組まなければならなかった。現在でも一部の作業は続けられている。作業の半分以上は AthensIM リファレンス実装のカスタマイズ実装に関する調査研究に充てられた。

*達成可能性*

5.5.8 アセスメントの結果、プロジェクトは E ラボの現行の能力および人員の範囲内で達成可能であり、E ラボはプロジェクトを実行するに十分な技能を内部に有していると判断された。

## 5.6 実施

### *成果*

5.6.1 意思決定は全て E ラボが行った。以下の役割も E ラボ内部のスタッフが担った。

- e ラーニングの責任者
- 開発者
- ウェブチームのリーダー

5.6.2 SSOv3 はウォーリック大学が構築したウェブサービスへのアクセスのため 2005 年 9 月に稼働を開始した。しかし、2005 年 9 月時点では、いくつかの重要な Athens データベースが Shibboleth-Athens ゲートウエイ経由でまだ利用可能でなかったため、Athens リソースへの Shibboleth 認証は 2006 年 9 月まで保留された。2006 年 9 月には Athens リソースの大半が AthensDA と Shibboleth-Athens ゲートウエイを経由してアクセス可能になっていたが、2 つの主要なデータベースが未対応だったため、Classic Athens 経由でのアクセスを可能なままとし、まだシングル・サインオン・システムに組み込んでいない。

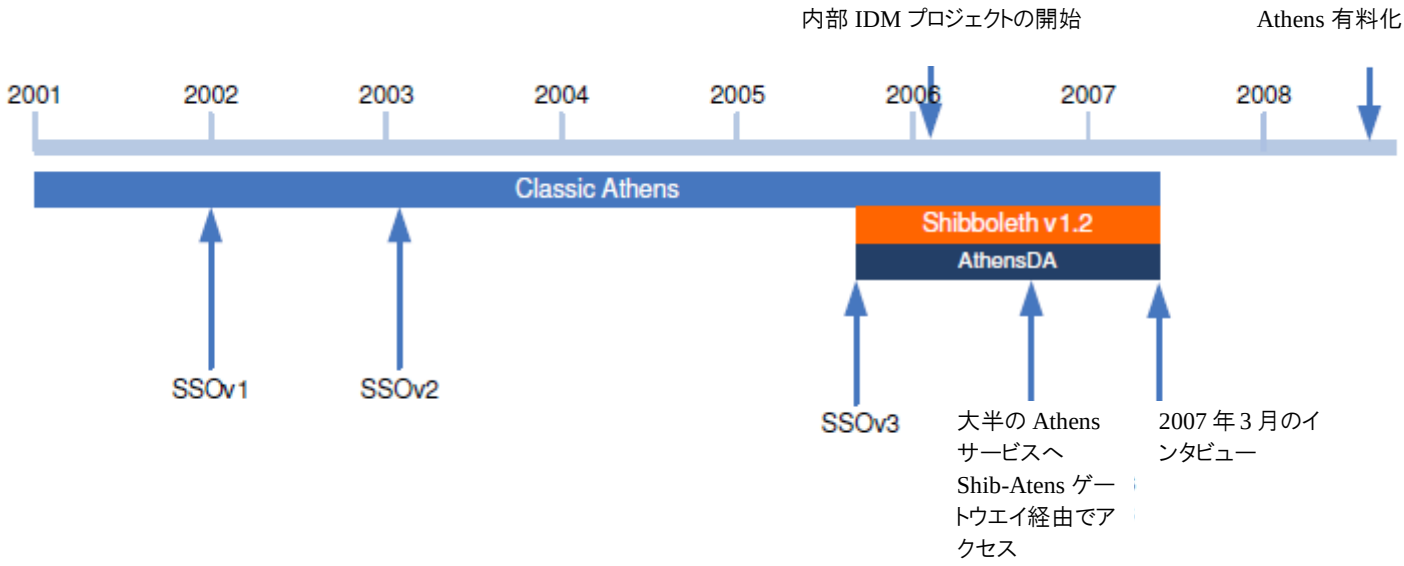


図 5-1：アクセス管理の時系列図

5.6.3 ウォーリック大学における現行のアクセス管理態勢は次の要素で構成される。

- シングル・サインオン（ローカルのユーザー名とパスワード）：
  - 内部（Shibboleth 対応化）ウェブサービス（例：ブログ）
  - Athens リソースの大半
- 統合サインオン（ローカルのユーザー名とパスワード）：

- キャンパス内の PC
- 内部の Shibboleth 非対応サービス（例：電子メール）

- その他（特定のユーザー名とパスワード）：

  - Classic Athens のユーザー名とパスワード経由でアクセスする Shibboleth 非対応の Athens リソース（これらのリソースの使用を希望するユーザーは Athens に登録しなければならない）
  - 図書館のユーザー番号と PIN 経由でアクセスする非 Athens サービス[16]
  - 特定のユーザー名とパスワード経由でアクセスする特定の内部サービス（例：財務システム）

5.6.4 自分たちのアプリケーションを Shibboleth 対応化したいという部門が増えており、IT サービス部門は可能な限り積極的に支援をしている。こうしたアプリケーションはシングル・サインオン・システムの一部ではないが、同一のローカル・ユーザー名とパスワードを有している。

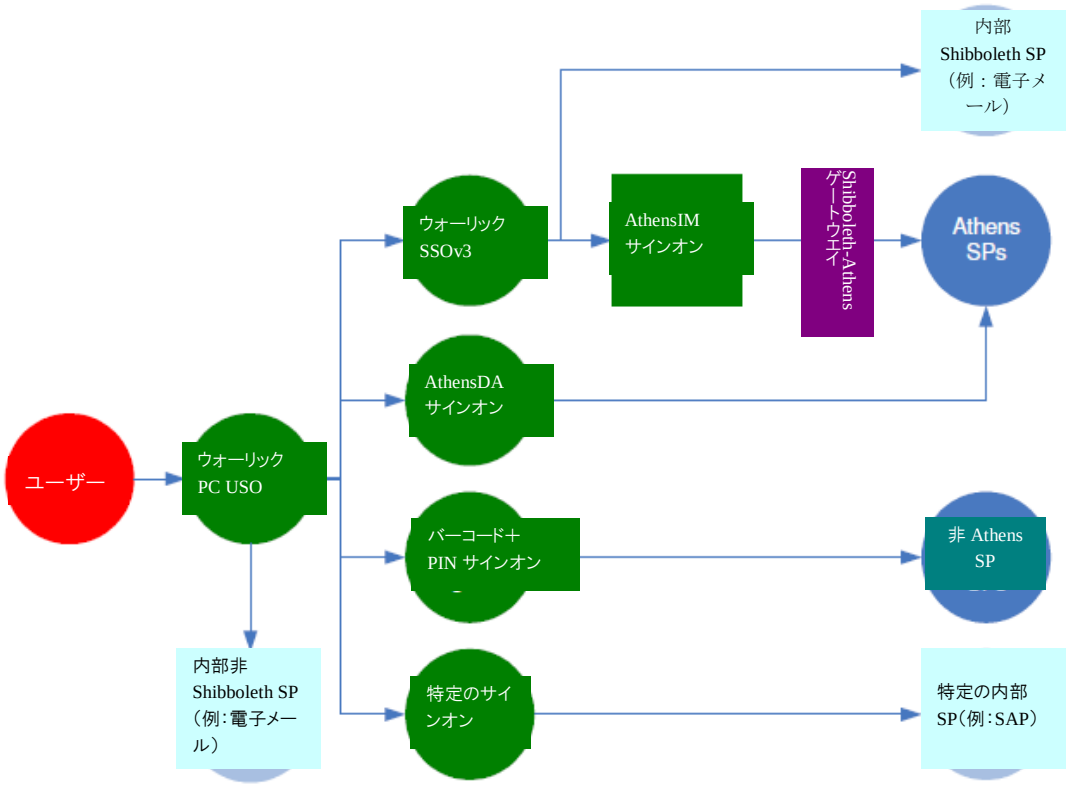


図 5-2：ウォーリック大学における現行のアクセス管理態勢

***実現した便益***

5.6.5 このプロジェクトは多くの便益をウォーリック大学にもたらしている。

[16] 認証はプロキシ・サーバーを介する。これは理想的な状態とは考えられない。特に一部の遠隔学習者にとってはそうである。

- シングル・サインオン・システム対応サービスについては、ユーザーごとに単一のローカル・ユーザー名とパスワードにほぼ一本化されたので、ユーザーエクスペリエンスが向上した。
- ユーザーは外部からウェブリソースにアクセスできる。
- IT サービスによると、パスワードに関するヘルプデスクへの問い合わせは減少した。さらに、問い合わせの内容も変化し、現在は概ね一般的な対応で済んでいる。[17]
- Shibboleth テクノロジーにより、セキュリティ上の利点が実現された（例：永続的なクッキーではなくセッション・クッキーを使用、暗号化通信によるパケット・スニッフィングの減少など)。これまでのところ、明らかになったセキュリティ侵害はない。さらに、ユーザーにとってローカルのウォーリック・パスワードの共有は、Athens パスワードの共有に比べ抵抗があるため、パスワード共有が抑止されている。
- ウォーリック大学は、必要に応じてフェデレーションに加入し、本格的な横断的アクセス管理の使用に対応できる態勢が整った。

## 5.7 直面した課題と得られた教訓

5.7.1 プロジェクト中に直面した最大の課題は Athens サービスと Shibboleth-Athens ゲートウエイとの適合であり、コンフィギュレーション管理の問題に直面した。このため、Athens サービスについての Shibboleth ベース認証を 2006 年 9 月まで延期する必要があった。2 つの主要な Athens サービスが、いまだに Shibboleth-Athens ゲートウエイに対応しておらず、これらのサービスにアクセスするには Athens のユーザー名とパスワードが必要である。

5.7.2 ウォーリック大学ではプロジェクトから次の教訓が得られた。

- プロジェクトは当初の想定よりも困難で複雑になった。多数のアプリケーションを横断して機能し、ユーザーにとって便利で、かつ、セキュリティが確保されたシングル・サインオン・システムを実装することは非常に難しく、予想していたよりもコードの記述が複雑だったからである。
- 各データベースは、Athens とデータベース・サプライヤーが構成しなければならない。こうしたリソースの適合性を試験することが何よりも重要である。サービス稼動時のダウンタイムを最小化したい場合は、特に試験の実施が重要である。
- アクセス管理には包括的な ID 管理システムが整備されていなければならない。
- IT インフラの可用性はユーザーにとって極めて重要であり、それにふさわしい設計と管理が必要である。
- Shibboleth プロファイルの既製ソリューションを実装した場合、シングル・サインオンがもたらす柔軟性をフルに活かすことができないかもしれない。カスタマイズされた実装であれば、将来の市場に対応して、インフラの変更が容易になる。
- 大学のウェブサイトに掲載されるコンテンツを大学が完全に制御しているのでない場合、十分な技術的セキュリティを確保することは非常に困難である。
- IT サービス部門が所有していないウェブアプリケーションについて、変更管理プロセスが必要である。

[17] 大学が 2 つのシステムを並行して運用しているため、まだ問い合わせの減少は見られない。

- このプロジェクトの全ての便益を実現する上で、図書館との緊密な協力が重要であった。一例を挙げれば、プロジェクトの方向性について、上級図書館員の同意が必要であった。
- スタッフがユーザーに使い方を指導することができるよう、スタッフを教育訓練する時間を十分にとらなければならない（例：図書館員を夏季に教育訓練するなど)。

## 5.8 将来の計画

5.8.1 ウォーリック大学は将来に向けて次の計画を掲げている。

- ウォーリック大学が、フェデレーションの中で完全な IdP になれるインフラが整備される予定（2007 年 9 月から 12 月の間に完成)。ただし、今のところブログやフォーラムなどのウォーリック大学のサービスを横断的サービスとして公開する計画はなく、そうしたニーズも予想されていないが、ひとつの可能性としては認識されている。
- ウォーリック大学は代替的な技術的ソリューションに対してオープンかつ柔軟な立場を維持する。規格が成熟し、導入される機能が増えれば、ウォーリック大学も Shibboleth リファレンス実装への切り替えを検討するかもしれない。これにより内部のサポート費用が低減できる可能性がある。
- 非対応の Athens リソースに関する問題をデータベース・プロバイダと Athens による技術的アップグレードを通じて解決する。
- このインフラの利用を希望する部門を支援し、シングル・サインオン・システムの範囲を拡大する。

このページは敢えて空白にしてある