複数認証基盤に対応する複合 SSO 環境でのユーザエクスペリエンス

Proposing User Experience based on WEB-SSO with Multiple Backends of Authentication/Authorization Engine

松浦健二†，上田哲史†，佐野雅彦†
Kenji Matsuura†, Tetsushi Ueta†, Masahiko Sano†

ma2@tokushima-u.ac.jp, ueta@tokushima-u.ac.jp, sano@tokushima-u.ac.jp

†徳島大学情報化推進センター

† Center for Administration of Information Technology, The University of Tokushima

概要

個人の ID が複数存在する場合の個人認証には，単一の認証源に登録されている場合だけでなく，複数の異なる内容での認証源に登録されている事もある．これをシングルサインオンのバックエンド情報源として利用する際には，その特性や扱う属性に注意しながら慎重に実装しなければならない．これらはセキュリティを考慮しつつ利便性および耐障害性を高めるための設計方針および運用方針を要し，本論文では本学での実装について述べる．さらに，異なるシングルサインオン技術を用いた異なるカテゴリでの統合的な操作環境について述べる．

キーワード

WEB-SSO, Shibboleth, Kerberos, ADFS

1. はじめに

組織内外で利用される個人の識別子（ID）は，その発行主体および運用方針に依存して，同一サービスに対する同一個人においてでさえ複数存在する事がある．大学等高等教育機関における本事象の要因として，例えば，下部組織が独立して臨時職員等を雇用するケースや，ID の発行主体となるシステムあるいは組織内下部組織の運用が独立しているケースなど幾つかのパターンがある．これらは，名寄せの問題やその応用となる生涯 ID 問題として研究される事がある．例えば，名古屋大学では，名古屋大学 ID として一貫性のある生涯 ID の設計がなされている[1]．生涯 ID の導入は，かなり長期間に渡る設計思想を必要とし，この長期間に外部組織による ID 発行・管理機関の登場など，多くの不確定要素もある．ただし，こうした長期間に渡り適用可能なスケーラビリティを要する設計思想自体は，組織のユーザ管理，中でも大学のような人の入れ替わりに特徴を有する組織での管理方針に，重要な示唆を与えうる．

ここで，一度整備・普及している ID の変更は大きな運用上のコストとリスクを伴うが，生涯 ID の導入に限らず，ID 運用方針の変更などを契機に，再整理されることもある．こうした場合には，重複期間なく新 ID に切り替える立場と，重複期間を設けた上でユーザへの説明

を重ねながら移行する立場もとれる．

ユーザ管理の方針が固まれば，その方針の下で ID 利用・運用する個人認証サービスが導入される事が一般的である．個人認証サービスの応用となるフロントエンドのアプリケーション個々の活用のされ方や，運用支援によって，ユーザの利用頻度やサービスの技術的な構成も変化する．大阪大学では，統合認証基盤を構築し，様々なアプリケーションに適用することでユーザの利便性向上が図られている[2]．さらには，統合認証基盤をバックエンドとする組織内外でのシングルサインオン環境も整えられている[3]．一旦シングルサインオン環境が整備されると，組織内のアプリケーション開発はこの基盤を用いて容易に実現できるようになる[4]．

国立情報学研究所を中心とする「学認」等の組織を跨ぐシングルサインオンでは，とりわけ個人情報の扱いに注意を要し，技術的あるいは運用上の様々な工夫を要する．一方で，単体組織内のシングルサインオンにおいても，パブリックなクラウドサービス[5]をシステムの系に採り入れることも多くなり，組織内の合意形成や運用的な対応は基より，技術的な対応も必要となる．さらには，統合認証基盤の利用とシングルサインオン環境の下では，認可制御方針を決めた上で，適切にそれを実装することが求められる．例えば，A 学部における教授会資料へのアクセスについてはその学部の教授に限定という要件もあれば，同じ大学内でも B 学部における教授会資料へのアクセスには，B 学部の教員(教授以外含む)全てに許可される要件もある．こうした様々な認可要件に対する柔軟性のある選択および実装が求められる．また，これらを実現するシングルサインオンの技術自体も，適用可能範囲や適性があるため，技術的に統一する方針にするか，適材適所で適応させるかは組織の意思決定に依存する．

こうした設計思想を背景に，ユーザ側の利便性をいかに高めて提供できるかは，近年ユーザエクスペリエンスとして議論されている[6]．ユーザエクスペリエンスという言葉自体は，近年のスマートフォンやタブレット等でのマルチタッチ操作などを含む様々な文脈で用いられるが，本論文ではシンプルに，従来よりも相対的に利便性の高い操作全般として捉えている．

徳島大学では，以上の議論の下，ユーザ ID を見直して構築し，これに伴う複数種のバックエンド認証基盤を運用することとなった．さらには，端末認証を活用した複数種のシングルサインオン技術を導入した操作環境も設計した．具体的には，ADFS と Shibboleth に加え，Kerberos を利用したシームレスな操作環境の構築である．これにより，教育環境を利用する学内構成員へのログインサービスとして高い利便性をもったサービス提供が可能となった．本稿では，この設計思想および，運用後の利用状況から得られる動向について述べる．

2. ID 運用の見直し

2.1. 体制上，技術上の従来の問題

組織内で全学的な認証基盤が構築される以前から開発・運用されてきた単独の学内全学向けアプリケーションサービスがある場合には，そのサービス側でユーザ情報をローカルに持つ方式で開発されることが多かった[7]．したがって，認証基盤への要望が後から高まった際には，このような利用頻度の高い全学アプリケーションサービスのユーザ情報を基にした認証基盤を構築する方が効率的であった．その場合には，ID 体系のスケーラビリティに依存して，ユーザ視点および管理者視点双方からの利便性の問題，あるいは ID ライフサイクルの問題が運用途中で出てくる事もある．

一方，現在多くの大学では，情報センター系組織等が主体となって，ID プロビジョニングの仕組みを検討し，基盤化してから外部サービスがそれを使うように設計するアプローチが多数見られる．認証基盤を大学全体で構築することは，利便性を高めるだけでなく，セキュリティ水準を全学的に一定以上に担保する上でも重要である．本学では，教職員については前者の経緯に基づく実装が人事課の業務フローと連動した形で確立されてきた．一方で，学生については後者のような認証基盤が学務課の業務フローを系に含む形で実装されてきた．すなわち，技術的な ID 発行・管理主体も異なるが，その業務フローに介在する人的な組織も独立していた．

これら異なる事務所掌組織に対して，ネットワークシステムで利用する ID の管理運用主体も統一化されずに運用されてきた．このため，二つの認証基盤を教職員向け，学生向けといった形でデータ分離し，一方で両者を扱う WEB サービスのためには，それらをプロクシする認証中継サービスを導入する形で，かろうじて認証基盤として統一的に見せていた．

この形で運用上生じる問題は，ID の発行主体が組織として複数存在し，運用方針もそれぞれに独立依存する形であるが故の煩雑さがある．パスワードや個人証明書等による認証基盤としてだけ考えれば，このような複数認証基盤であっても大きな問題とはならないが，ライフサイクルのずれを鑑みた場合には運用の手間が顕在化する．さらには，ユーザの属性情報を含めた認可制御を考慮すれば，異なる認証基盤で異なるスキーマによる属性運用では管理上の困難も生じる．

2.2. 統合化と並行期間の運用

徳島大学では，コンピュータシステム更新の契機に，

教職員も学生と同一の認証基盤に乗せることで，前節の問題を改めて解消することとした．両既存基盤とは独立して全く新しい認証基盤を構築するよりも，いずれかにまとめた方が既存のフロントエンドサービスへの影響が少なく，かつ設計上も容易になるためである．ここでは教職員の方が学生と比較して少数であり，かつ連絡が行き渡りやすい事から，教職員側を寄せる方針とした．

認証基盤の統合化に際し，ID 設計上の体系および運用が異なるため，サーバサイドでの ID を移行する事も検討したが，技術的および運用的に困難であった．そこで，一時的にユーザへの負担をかけることとはなるが，新しく ID を追加付与するという形をとることとした．他大学等でも ID 再構成の際には，追加という形が見られ，一定の実績も上がっている．なお，従来はユーザのマスタデータをそれぞれ異なる部署が所掌する形で，それに連動して独立した ID 管理体制であったが，本方式実現のためにオンラインでのプロビジョニング／デプロビジョニングを実現した．これは，他大学でのユーザ管理データベースと同様である[8].

この実現には，構成員に対して重ねてアナウンスを行い，周知広報活動を何度も展開した上で，当面の間並行利用することとした．すなわち，並行利用する間の利用動向を調査しながら，方針を柔軟に決めていけることになる．このような方針を採用する際には，重複 ID がこれら新旧の認証基盤には存在しない事が重要である．

3. シングルサインオン設計

3.1. SSO サービス

本節では，前述の認証基盤を利用したシングルサインオンについて述べる．これは，個人認証で最も利用されているパスワードなどの流通経路を隘路にすることで，セキュリティ上のリスク軽減を実現し，なおかつ認証操作の頻度を減少させる効果がある．

インターネット上には，OpenID 等の多用な技術が開発されているが，組織内で用いられるシングルサインオン技術として多用される主なものには，ADFS や Shibboleth といった SAML 対応のソリューションや，Kerberos など多種存在する．SAML や Kerberos はその特徴や，対応システムが異なる事が多い．そのため，いずれかを選択利用するという形では，対応できないアプリケーションも出てくる懸念がある．

徳島大学では，2007 年頃から分散 SNS を対象とした Shibboleth の拡張について研究を行っていた[9]．2010 年には，全学的な SSO 実現のための基盤技術として Shibboleth の採用が決まり，各種の SSO 対応 WEB サービスは Shibboleth へ，という流れが構成された．

2012 年 4 月の時点では，Shibboleth を用いた WEB-SSO として，下記のようなサービスが導入されている．また，内製の出席管理システムや WebDAV，ネットワーク監視などこの他にも同じ SSO に参加しようと幾つか計画段階のものもある．なお，下記に列挙しているサービスは元々 SAML 対応しているものもあるが，本学向けに Shibboleth 対応したものも含まれる．

- 全学統合ポータル（パブリックサービス）
- LMS（パッケージ）
- LMS（Moodle）
- ネットワーク利用申請（独自開発）
- ソフトウェアダウンローダ（独自開発）
- グループウェア（OSS カスタマイズ）
- 図書館システム（パッケージカスタマイズ）

3.2. WEB-SSO の認証連携拡張

前節で挙げた各種の WEB サービスは，アプリケーションサービスであり，個々に個人認証を経て，個人に依存したコンテンツを提供する．ここで，個人認証は，アクセスしているユーザが本人である事を確認するのが本質であり，その点からはアプリケーションサービスに限った要件ではない．例えば，個人認証を要する対象には，こうしたサービスの他，オペレーティングシステムやネットワークも含まれる．これらは適用場面の違いであり，個人認証そのものの本質は等しいと考える．このような適用場面を超えた SSO の枠組みも研究されており，例えばネットワーク認証を行うゲートウェイに Shibboleth を導入する研究がある[10].

個人認証の方式に関する運用方針は，それぞれの組織の実装に適した方式を検討すべきである．例えば，徳島大学では，ネットワークの一時利用（VPN や無線 LAN）を行うためのパスワード認証については，オンデマンドで必要に応じて発生するものとの判断があり，認証基盤を直接利用する対象とはしていない．一方で例えば，Windows ドメインへの参加については，学内のほとんどの構成員が教育場面や業務場面において，必須利用する．さらにはアプリケーションサービスも業務利用するものが多いことから，これらは透過的なサービスと考える．こうしたサービスには，Windows ドメインログインを以て，上位のアプリケーションサービスへも SSO できる環境の設計を行った．

ここで，Windows のドメインサーバは，ActiveDirectory で構成される．ドメイン参加によって Kerberos が利用できるようになる．Kerberos は各種の OS でサポートされ，ブラウザがそれを利用できるものもある．例えば，Windows 上の InternetExplorer や Firefox が対応している．

徳島大学の教育用コンピュータシステムは，2012 年度以降ネットブートを導入しており，これらブラウザの設定もイメージ更新時に簡単に設定できる．

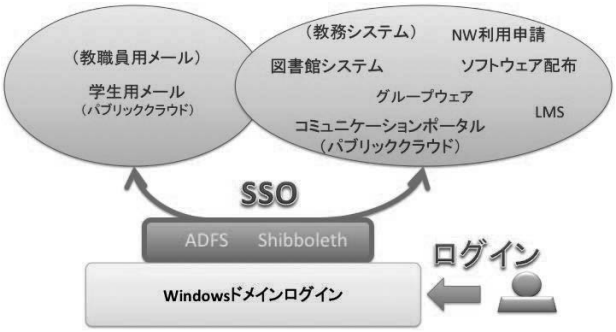

図 1　アプリケーションとドメインログイン

徳島大学において数年来運用している Shibboleth では，Kerberos ハンドラを導入することも可能である．そこで，上述の環境を実現すべく，Shibboleth と Kerberos を組み合わせて，ドメイン参加によるアプリケーションサービスへの SSO を実現する．なお，学生用の Exchange Online を利用したメールサービスは，同様にドメイン参加によるアプリケーションへの SSO が実現可能である．つまり，OS 認証によってアプリケーションログイン時には，ID やパスワードの入力は行わない．これには Shibboleth ではなく，SAML に対応した ADFS が利用されている．したがって，徳島大学では，Shibboleth，ADFS，Kerberos が混在しながらも，Windows ドメインへのログインを以て，上位の WEB アプリケーションサービスへの SSO が実現できることとなる（図１参照）．この場合，いずれを利用した場合にも，再度の認証は要求されず，透過的に各種のサービスを利用できることなる．すなわち，エンドユーザの視点からは ADFS グループや Shibboleth グループといった区分けのないシームレス環境となる．

3.3. アクセス元から見たサービス

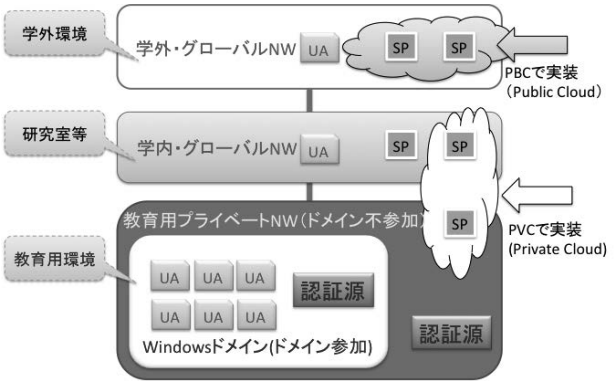

図 2 ネットワーク構造とサービス展開

前述の Kerberos を用いる場合には，図２におけるネットワーク構造のうち，左下部にある Windows ドメイン参加端末が対象となり，ドメイン参加していないコンピュータからは機能しない．図中の一般研究室や学外から本学のサービスを利用する際には，Kerberos を用いない Shibboleth 利用となるため，これら両要件に対応する設計・構築が必要である．補足として，図２中の UA は User Agent（＝ブラウザ）の略であり，SP は Service Provider（＝アプリケーションサービス）の略である．

4. システム構築

4.1. 複数種認証源への対応

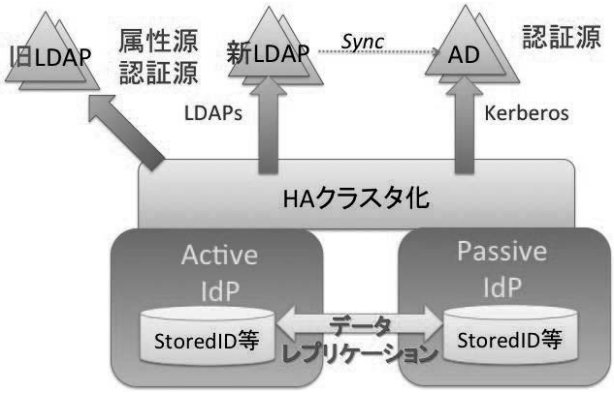

図 3　複数種バックエンドでの IdP 冗長化構成

前章までに述べた用件を実装するに際し，本章では特に Shibboleth の構成を具体的に述べる．図３は，Shibboleth における認証源へのユーザインタフェースを提供する部分（IdP，Identity Provider と呼ぶ）の構成である．徳島大学では，システムのクラスタ化による冗長性確保には，Active-Standby での構成をとって耐障害性を高めている．なお，サーバ自体は 64bit アーキテクチャで十分なメモリを割り当て，ディスクは RAID0+1 で構成している．認証源・属性源および IdP の各サーバは全て耐震固定のラック搭載で UPS が稼働し，これらを保管する部屋の入退室管理は電子錠で自動記録されている．なお，ネットワークアクセスに際しては，アクセス元や接続ポートの制限等だけでなく，運用上は，Nagios を利用した外部からの定期監視・自動通知とホスト内部のログの常時監視・自動通知の両方でセキュリティを高めている．

IdP には，StoredID（SP 毎に異なる ID 生成する機能）やその他の実装のために，内部にデータベース（RDB）を有している．この RDB は，上記のクラスタを実装するためにマルチマスタ構成をとり，Active 系が切り替わってもデータの保存としてはレプリケーションされる．

ここで，２章で述べた複数種バックエンド認証源・属性源への対応実装について述べる．前提として，IdP に

限らず，重要なサーバは物理・論理を問わず冗長化構成をしている．したがって，IdP から見たバックエンドとしては全てフェイルオーバ対応となる．認証源の選択としては，Windows ドメイン参加している場合には，再度のエンドユーザがパスワード入力して認証される必要はない．しかし，そうでない場合には，教職員，学生といった構成員全員のアカウントを有する新しい LDAP，またはそれとは重複のない旧来のアカウントを有する LDAP の二種類をそれぞれ認証源，属性源として登録する．この際，新しい統合 LDAP の方を優先するよう，順番は先に設定しておく．なお，これら新旧の LDAP には，主に下記の点で相違がある．

・バインド方式
・DIT 構造の違い（uid 生成則，DN 等）
・属性数，属性名（オプション含む）および属性値

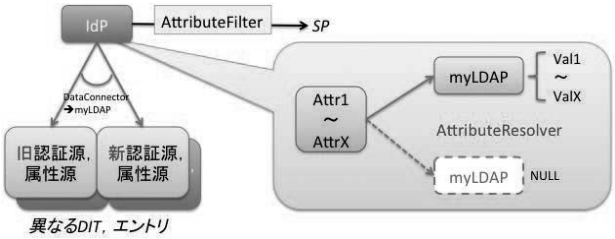

図 4　属性取得の仕組み

ShibbolethIdP では，認証を行った後，属性取得機能には新旧双方を設定する．この実装は AttributeResolver にて行われ，その中で属性定義する際に択一となるよう実装する（図 4 参照）．ここで，属性取得時は，前述のように属性名も異なる場合がある．そのような属性に対しては，単純に複数 LDAP への接続を設定するだけでは動作しない．そこで，徳島大学の実装においては，それぞれに保存される属性を Simple 型で一旦ダミー取得してからそれらを Script 型で属性選択する方式とする．属性取得が択一となるため，Script 中で例外処理を書いておかねばならない．具体的には，属性取得時はプロクシバインドしての検索となるが，これには設定ファイルに記載された順に試される．このため，最初のコネクタで検索失敗した場合には，例外が吐かれて以降の処理が停止するため，例外処理を書いて回避する．また，認証時に Kerberos ハンドラが選ばれているクライアントに対しては，属性検索時のフィルタにセットする値がパスワード認証とは異なる事になり，それぞれ適切に設定する．

4.2. 複数 SSO 技術のシームレス利用

Shibboleth における利用頻度の高いハンドラは，UsernamePassword ハンドラ，つまりバックエンドの認証源に対して，WEB を通じてクライアントから渡されるパスワード照合方法であろう．この時，ドメインログインを含めた処理概要を図 5 に示す．エンドユーザは，ドメインログインは OS 上のドメインログインであり，ブラウザ上での Shibboleth の世界はそれとは独立したものとして，機能的にもインタフェース的にも独立動作する．このため，図中の両領域間は，ユーザ視点においても SSO として機能しない．

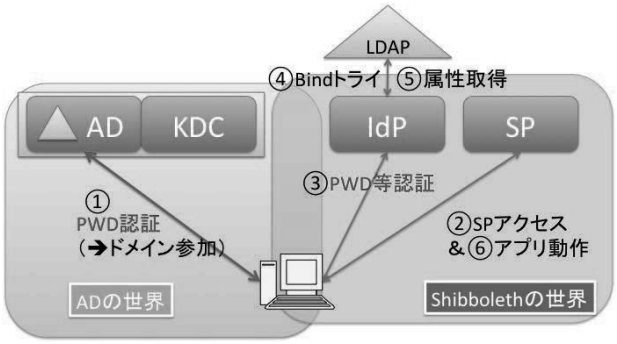

図 5　パスワード利用時の処理概要

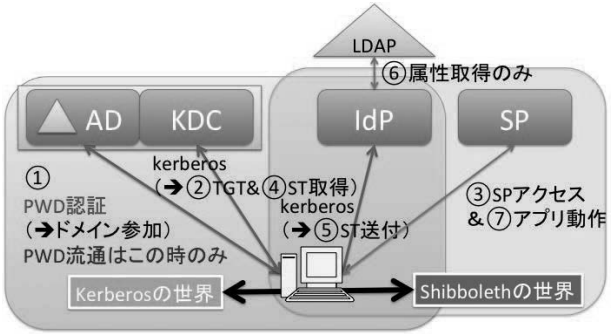

図 6　Kerberos 利用時の処理概要

徳島大学の実装においては，ドメイン参加時には，図 6 のような Kerberos ハンドラを選択できる．Kerberos ハンドラは，ShibbolethIdP を Kerberos の一つのアプリケーションサービスと位置づけることと見なせる．つまり，Kerberos ハンドラは，クライアントから渡されるサービスチケットの検証によって図中の KDC が認めたクライアントと見なす．図 5 と異なり，Windows ドメインの世界と Shibboleth の世界のオーバラップ領域が増え，エンドユーザが入力するパスワードの流通頻度は減少する．一旦 Kerberos のサービスとしての ShibbolethIdP で認証されれば，ShibbolethSP に SSO できることになる．

図 5 および図 6 は，それぞれ異なるハンドラでの実装となる．しかし，ユーザインタフェースとしては，同一の画面内で，エンドユーザのオペレーションによって使われるハンドラを変更するように実装している．具体的には，図 7 のインタフェース上の，画面下部のスニペッツが Kerberos ハンドラ用となり，パスワード入力を行わせる部分は UsernamePassword ハンドラとなる．これらにさらに，個人証明書による認証方式として RemoteUser ハンドラを加えたりすることも技術的には可能である．

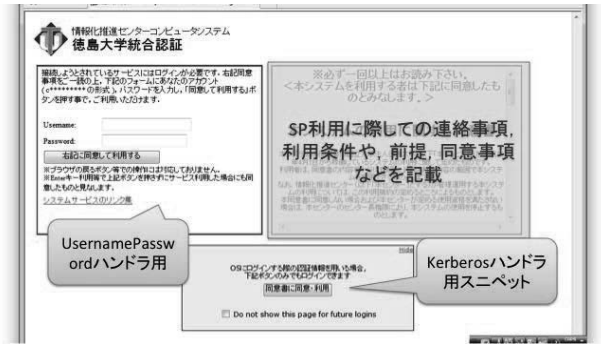

図 7　ログイン時の複数ハンドラの実装

Kerberos ハンドラの実装によっては，図 7 のようなユーザインタフェースを介さなくともよい．しかし，徳島大学での実装上は，隘路となる IdP の画面上で表示させたい同意事項やその他必要に応じて提示したい情報を一旦参照させるために，UsernamePassword ハンドラ用のログイン画面に Kerberos ハンドラへのアクセス用ボタンを含める形で実装している．従来のポータルサービスと異なり，任意方向 SSO となる Shibboleth においては，隘路としてはここが単一点であるため，簡単な伝達事項等はここに示しておくこととした．

5. 利用状況

5.1. ポータルサービス

一般的なキャンパス向けポータルサービスでは，大学の個人向け連絡機能を提供することも多い．徳島大学の全学統合ポータルは，コミュニケーションポータルとも呼び，構成員に対する SNS（Social Network Service）の機能を有する．すなわち，任意の構成員をフォローしたり，任意のグループを作ってフォーラムを開設したり，キャンパス内の情報交換がユーザ同士で双方向に行える．

一方で，従来的なポータルに見られた個人毎や所属毎のお知らせ機能も有する．これを利用して，所属や学年といった単位でのお知らせを掲示したり，就職活動に関する情報を流したりできる．これは主に教職員から学生への一方向のコミュニケーションである．

さらに，本ポータルサービスは，他の Shibboleth 対応サービスとの間でメッセージを受け取り，必要な構成員に秘匿メッセージとして投稿することもできる．例えば，LMS 上で，レポート課題が出されたり，受領されたり，あるいは図書館システムにおける図書の返却期限切れといったイベントを検知した際には，上流のサービスがメッセージを個人宛に投稿し，表示させることになる．この際，詳細な内容は上流のアプリケーションに SSO で遷移して確認するべく，Shibboleth 化されたロケーション URL をメッセージ内に埋め込んでおくことで，利便性の高いメッセージとなる．上流からのメッセージには添付ファイル等は伝播しない事で，一定のセキュリティ向上も図っている．このように，メッセージ集約を本サービスに行わせることで，従来的なポータルサービスの利用方法に近いサービスを提供している．

5.2. SSO 開始アプリケーション

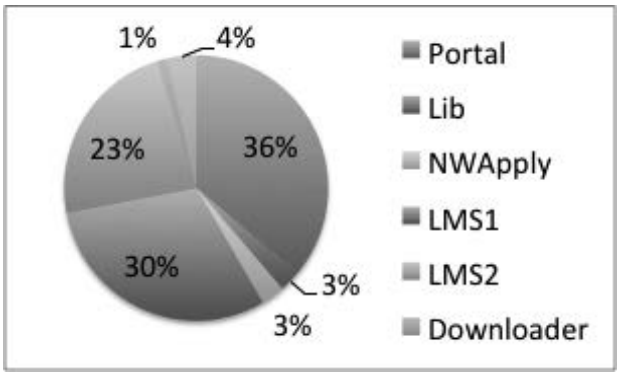

図 8　SSO の開始アプリケーション

徳島大学では，Shibboleth が導入されるまではポータルサービスからの片方向 SSO を実装していた．この場合，エンドユーザの WEB 遷移フローをある程度統制でき，各種の情報提示など片方向の情報発信側には利点が高い．一方で，エンドユーザは目的とするアプリケーションに直接到達できないという問題や，ユーザコミュニケーション向け機能を個別に用意するなども課題となる．

Shibboleth では，SSO の方向としては各種アプリケーションがフラットになるため，任意のアプリケーションから SSO を開始できることとなる．そこで，開始アプリケーションの割合を集計した．図 8 がその割合（2012 年 4 月 1 日から同 5 月 31 日）である．

導入初期には，ポータルが半分以上の割合を占め，そこから各種のサービスへ SSO 遷移する形が多く見られた．ところが，図 8 のように２ヶ月を経過した時点で集計してみると，各種サービスへのリンク集から直接ターゲットのサービスにログインする割合が増え，ポータル経由は 36%まで下がることとなった．一方で，LMS1 が 30%，LMS2 が 23%と増え，学生も教職員も，業務として日々利用する必要のあるサービスに直接アクセスするようになっている．

5.3. ログイン方法

（1）　新・旧の ID 選択状況

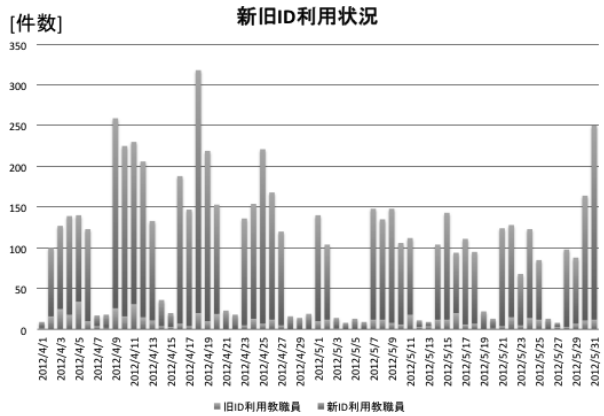

図 9　新旧 ID 利用状況

２章にて述べたように，新しいコンピュータサービスの一部には，旧 ID との並行利用期間を設けた．要求として，授業等で旧来的な ID を利用していたコンテンツが，当時の ID に紐付けられているものがあり，特に教職員からはそれらの再利用が強く求められ，要件定義に加えたものである．これらはほとんどが LMS，すなわち授業での再利用を意図している．

ここで，実運用開始初期の日々の ID 利用集計（教職員のみ）を見てみる（図 9）．このデータによれば，新 ID 利用（赤棒）は定常状態になった．一方で，旧 ID（青棒）はそれまでの切り替え周知を頻繁に実施した結果，当初時点から少なかったが，さらに減少している様子が分かる．新 ID の利用範囲（端末ログインやアプリケーションサービス）が多く，日常的に新しい ID で何らかを利用する機会が増えていると考えられる．

（2）　ログイン全体と Kerberos 利用

3 章以降で述べた Kerberos ハンドラの利用は，構築後間もない現状では，任意利用としている．このため，ドメインログインしない状況での Shibboleth 利用を除き，ドメインログイン状況では，ユーザの選択となる．そこで，総ログイン数の推移に対して，Kerberos 利用割合の推移を見てみることとする．

図 10 は，棒グラフ（主軸）は日々の Shibboleth でのログイン数，折れ線グラフ（第２軸）は Kerberos ハンドラを利用した 2012 年 4 月から 5 月にかけてのログイン数である．前者に注目すると，4 月は様々なシステムを年間で最も利用する時期であるため，5 月に入ってからは若干減数して定常状態となっている．一方で後者は，4 月は認知度が低かったためか，パスワード入力に慣れてしまっているためか，いずれにしても比較的少なかったが，5 月にかけては増加している様子が分かる．したがって，前者に対しては相対的に増加傾向が強いと言える．

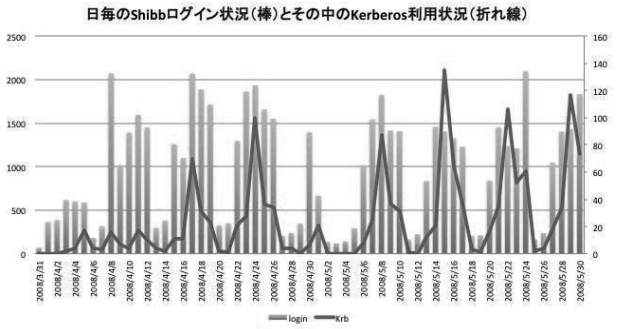

図 10　ログイン時の利用ハンドラの推移

6. おわりに

本論文では，徳島大学における複数種の認証源・属性源を利用した SSO 環境の実装について述べた．具体的に，複数のバックエンドを要する際の ShibbothIdP 設計上の方針を述べ，実装を行った．また，SSO については UsernamePassword ハンドラと Kerberos ハンドラの利用について述べ，かつ ADFS 対応アプリケーションも含めたシームレスな操作を提供できるユーザエクスペリエンス向上について述べた．5 章で見たように，利用開始間もないながらも，相対的に Kerberos 利用は増加傾向にある．しかし，システム利用開始初期のデータにつき，今後もこの動向については継続調査したいと考えている．

また，パスワード利用頻度および流通経路の軽減だけでなく，異なる認証方式や，セキュリティレベルに応じた複数要素認証方式なども今後検討していきたい．

謝　辞

本システムの IdP 設定に際しては，一部 NEC（株）の協力を得て実装している，また，既存の学内認証基盤実装から本論文のシステム検討に際し，徳島大学評価情報分析センター長の大家隆弘教授からは貴重なご意見・ご協力を頂戴した．謹んで感謝の意を表する．

参　考　文　献

[1] 太田芳博，梶田将司，田島嘉則，田島尚徳，平野靖，内藤久資，間瀬健二：大学における生涯 ID のための名寄せ手法，情報処理学会論文誌，Vol.51，No.3，pp. 965—973 (2010).

[2] 秋山豊和，寺西裕一，岡村真吾，坂根栄作，長谷川剛，馬場健一，中野博隆，下條真司，長岡亨：大阪大学における全学 IT 認証基盤の構築，情報処理学会論文誌，Vol.49，No.3，pp. 1249--1264 (2008).

[3] 松平拓也，笠原禎也，高田良宏，東昭孝，二木恵，森祥寛：大学における Shibboleth を利用した統合認証基

盤の構築，情報処理学会論文誌，Vol.~52，No.~2，pp. 703--713 (2011).
[4] 伊藤智博，高野勝美，田島靖久，吉田浩司，災害時に備えた分散キャンパスによる情報基盤の整備，学術情報処理研究, No.15, pp.5—11 (2011).
[5] The NIST Definition of Cloud Service http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (2012 年 6 月 29 日参照)
[6] Effle L-C. Law, Virpi Roto, Marc Hassenzahl, Arnold P.O.S. Vermeeren, Joke Kort: *Understanding, Scoping and Defininf User Experience: A Survey Approach*, Proceedings of CHI2009, pp. 719--728 (2009).
[7] 三好 康夫, 大家 隆弘, 上田 哲史, 廣友 雅徳, 矢野米雄, 川上 博：EDB を利用した学習経路探索を支援する e シラバスシステムの構築, 大学教育研究ジャーナル, No.3, pp.1--9, (2006).
[8] 岩沢和男，宮原俊行，中川敦, 岩田則和，西村浩二, 吉冨健一：センターサービス利用登録システムの再構築, 学術情報処理研究，No.15, pp.89—97 (2011).
[9] 金西計英, 松浦健二, 三好康夫, 高木知弘, 嵯峨山和美, 矢野米雄：大学間 WEB サービス連携のための Shibboleth を用いた許可管理機能の実現，日本教育工学会論文誌, Vol.32(Suppl), pp.93—96 (2008).
[10] 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明：シングルサインオンに対応したネットワーク利用者認証システムの開発, 情報処理学会論文誌, Vol.51 No.3, pp.1031-1039 (2010).