新大阪大学全学 IT 認証基盤システムの構築

村尾 靖子 ‡　　山口 文雄 ‡　　江原 康生 †

‡ 大阪大学 情報推進部情報基盤課
† 大阪大学 情報基盤本部

1　はじめに

大阪大学情報基盤本部では，学内で運用されている様々な情報システムが PKI 認証技術のもとで統合的かつ安全に機能する全学 IT 認証基盤システムの運用・管理を行い，SSO(シングルサインオン) による認証連携及びデータ連携，ログイン認証等に供している．しかし，平成 18 年 10 月に導入された旧システム [1] は，現在の学内情勢において要求される下記 (1)~(3) の機能要件を十分に提供できない状況となってきている．

(1) **学内利用者及び連携システムの増加に伴うシステムリソースの不足**
年度初めの学務情報システムなどの集中利用に伴い，学内 LAN に接続された多数のクライアント端末から同時に多数の認証処理が発生する．このため，サーバの CPU 使用率等が上昇し，安定した認証連携を継続させることが非常に困難となっている．

(2) **新規に連携を希望する学内システムへの対応**
既存システムでは新たな SSO 認証連携には柔軟に対応できるが，データ連携に関してはシステム間で大規模な改修が必要とされるため，柔軟に対応することができない．

(3) **事務基幹系システムとの SSO 認証及びデータ連携**
本学では新たに事務基幹系システムとの SSO 認証及びデータ連携に向けた検討が進んでいる．しかし，学内の事務基幹系システム間で利用者の属性情報のコード体系は統一化されておらず，現在は手作業によるデータ連携の対応に迫られるため，業務量増大の要因となっている．システム全体の最適化を視野に入れた各システム間のデータ連携を実現させるために，ユーザ属性情報の一元管理への必要性が高まっている．

今後，学内システムに対する SSO 認証連携及びデータ連携を更に推進していく上で，上記に示すような課題が生じている．ゆえに，学内システムを統合的かつ安全に運用させるために必要とされる機能を有したシステム更新を行い，有用な認証基盤システムを構築する必要がある．本稿ではこれらの要求の実現に向けたシステム構築を行い，平成 22 年 10 月より運用を開始した新全学 IT 認証基盤システムの概要について述べる．

2　システム構成

図 1 に新全学 IT 認証基盤システムの構成図を示す．本システムは認証局システム，SSO(シングルサインオン) システム，マスターデータベースシステムから構成される．各システムはハイ・アベイラビリティなシステムとして，システム障害時においてもサービスを停止させないための対策を実施している．図 2 に新全学 IT 認証基盤システムと学内システムとの各連携状況を示す．現在，学内の 18 システムに対して SSO 連携，6 システムに対して IDM, ディレクトリサーバによるユーザ属性情報の連携を実現している．特に平成 22 年度より，ICHO(事務用グループウェア)，勤務管理，出張旅費，財務会計などの事務基幹系システムとの SSO 連携を開始している．

2.1　認証局システム

認証局システムでは CA システム (外部ホスティング) および RA システムを構築し，学内の各システムおよびユーザの電子証明書申請を受け付け，電子証明書および電子証明書失効リストなどの発行を行う．これらのサブシステムとして IC カードシステムを構築し，認証局システムより発行された電子証明書および鍵ペアを格納した IC カードの発行を行う機能を有している．

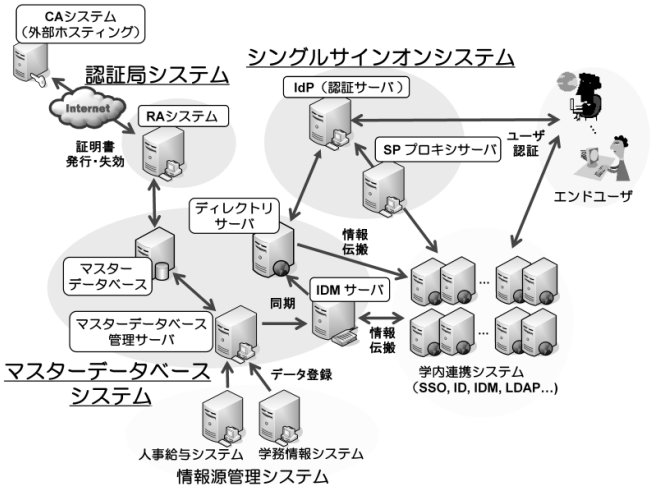


図 1: 新全学 IT 認証基盤システムの構成

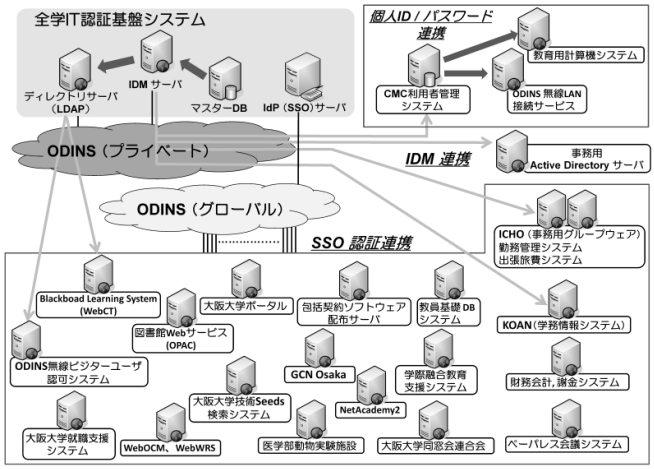
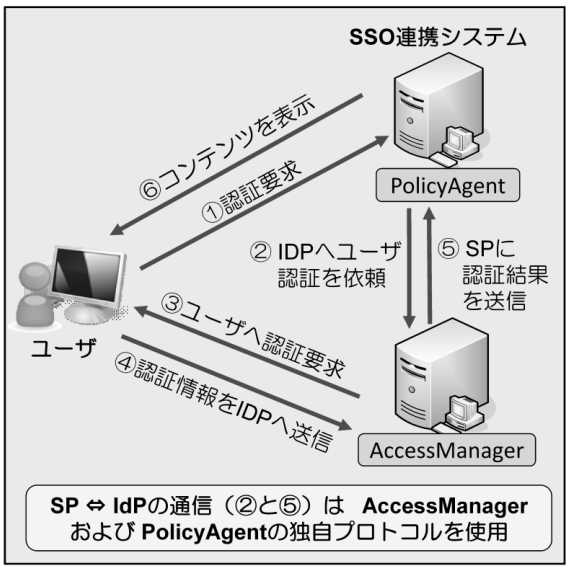


図 2: 学内システムとの連携状況

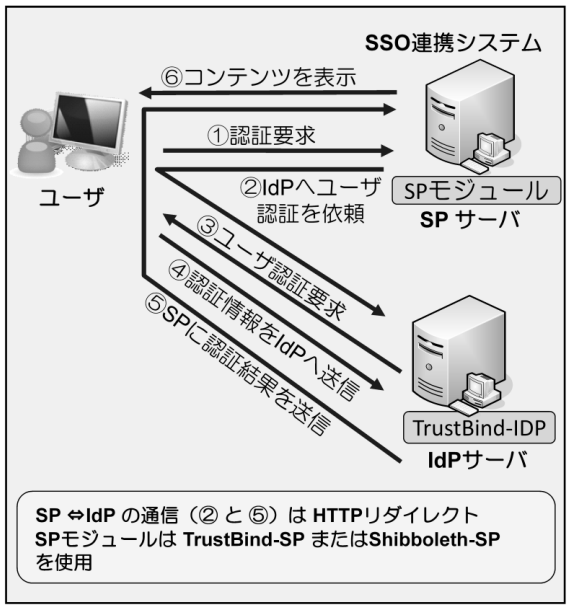
2.2 SSO システム

SSO システムは学内の各システムの Web アプリケーションと連携して，SSO 認証機能を提供する．本システムでは認証サーバとして，旧システムの Sun Java System Access Manager に代わり，NTT ソフトウェア (株) 製の TrustBind IdP[2] を導入した．TrustBind IdP サーバと SP サーバ (学内 SSO 連携システム) 間では，Liberty Alliance による OASIS-SAML2.0 に準拠した SAML 2.0 プロトコル [3] による SSO 認証連携を実現する．学内の連携システム側で動作する SP サーバ機能として，オープンソースの Shibboleth SP[4] を各連携システムの Web サーバに実装を行った．Shibboleth SP の実装が困難なシステムについては，別途構築した SP Proxy サーバを用いて SSO 認証連携を行うこととした．なお，本システムにおけるクライアントと IdP サーバ間の通信はロードバランサの SSL アクセラレータ機能を用いて SSL によるデータの暗号化を行い，通信の安全性を確保する．

図 3 に旧システムとの SSO 認証連携方式の比較を示す．旧システムでは Access Manager(認証サーバ) と PolicyAgent(SSO 連携システム) 間で，独自プロトコルによる SSO 認証連携を行っていた．しかしこの方式ではクライアントからのアクセス数が集中する際には認証処理が増大し，システム負荷上昇による性能劣化の問題が生じるケースが見られた．新システムでは IdP サーバと SP サーバ間の通信において，HTTP リダイレクトを利用することで，この問題の改善を行っている．



(a) 旧システム



(b) 新システム

図 3: SSO 認証方式の比較

本システムではSSO認証機能に加えて，各連携システムに対する利便性の向上を目的とした認可機能の実現を目指している．SSO認証・認可機能とは，ユーザに払い出された個人ID・パスワードによる認証後にユーザの属性情報によって連携システムのアクセスや利用できるサービスを制限したり，また与えられたアクセス権限により資源へのアクセスを制御する機能である．

2.3 マスターデータベースシステム

マスターデータベースシステムは，ユーザに関する主要な属性情報を一元管理し，学内の連携システムに効果的に参照させることで最新かつ適正な属性情報の保持を実現させることを目的とする．構成として，マスターデータベース及び管理Webサーバシステム，IDM(ユーザデータ配布)サーバ，ディレクトリサーバからなる．

マスターデータベース管理Webサーバは，ユーザ属性情報の登録・編集・削除を行う機能をWebベースのGUIで実現している．またRAシステムと連携することで電子証明書の発行処理も行うことができる．IDMサーバは全学IT認証基盤システムの各システムへデータを連携する機能を提供する．IDM機能のソフトウェアとして株式会社インテック製のパッケージ製品「結人」[5]を導入した．IDMシステムを使用することにより，マスターデータベースからJDBCのプロトコルでユーザ属性情報を取り込み，各連携システムに対してLDAP，DCOM，JDBC等の各種プロトコルを使用して情報連携を実現する．

3 個人ID体系の再設計

全学IT認証基盤システムでは大阪大学個人ID(以下，阪大個人ID)と呼ばれるIDを，学内の規程に基づき，学内のユーザにID発行を行っている．しかし旧システムでは，複数の所属や身分を持つユーザに対して，複数の阪大個人IDの発行を行ってきた．それに該当するユーザは利用する学内連携システムの形態に応じて，阪大個人IDを使い分けてログインする必要があり，ユーザにとって煩わしい運用形態となっていた．

この問題を解決するために，新全学IT認証基盤システムではSSO認証ログインで使用する阪大個人IDを一つに統一し，連携システムへのログインの際には，職名，身分などのユーザ属性情報が異なる複数のIDの使い分けを可能とする新たな個人ID体系の再設計を行った．

新全学IT認証基盤システムでは，複数の阪大個人IDを所有していたユーザに対して，SSO認証用のIDを人物固有の属性情報(氏名，生年月日など)が紐づくPersonal ID (新阪大個人ID)に統一する．所属部署，役職などの属性情報についてはRole IDという形で紐付けることで，システム内部で2種類のIDを関連付けた形で管理を行う．図4に新旧システムにおける阪大個人IDの管理体系を示す．

利用者が異なる所属，身分などの属性情報を新たに持つ毎にRole IDが追加される．Personal IDは阪大個人IDとして引き続き同じIDを利用すること可能である．複数のRole IDを持つユーザは，その中から代表IDをPersonal IDを選択し，全学IT認証基盤システムの認証サーバでPersonal IDとパスワードでSSO認証後，Role IDを選択してSSO連携システムにログインを行う方式を実現させる．

氏名	阪大個人ID	所属	職名、身分名
ユーザA	u000123a	大学院工学研究科	非常勤講師
ユーザA	u000456b	大学院人間科学研究科	准教授

(a) 旧システム

氏名	阪大個人ID (Personal ID)	Role ID	所属	職名、身分名
ユーザA	u000456b	u000123a	大学院工学研究科	非常勤講師
		u000456b	大学院人間科学研究科	准教授

(b) 新システム

図 4: 阪大個人ID体系の新旧比較

4 SSO(シングルサインオン)に伴う各種機能

4.1 利用者情報登録・変更

本システムでは新規に阪大個人IDを発行したユーザに対して，SSO連携システムへの初回ログイン時にパスワード，メールアドレス，内線番号を登録する機能を実装した．またユーザによる登録情報の変更も同様の処理で可能としている．こ

の機能は旧システムのユーザによるパスワード変更機能に加えて，ユーザの連絡先の最新情報を保持することを目的としている．ユーザがメールアドレスの登録・変更を行った際，メールの到達確認を行うため，入力されたメールアドレスに仮登録メールを送信する．そのメール本文に記載されたURLへアクセスし，確認することで本登録が完了とする．

4.2 利用者による Role ID 選択

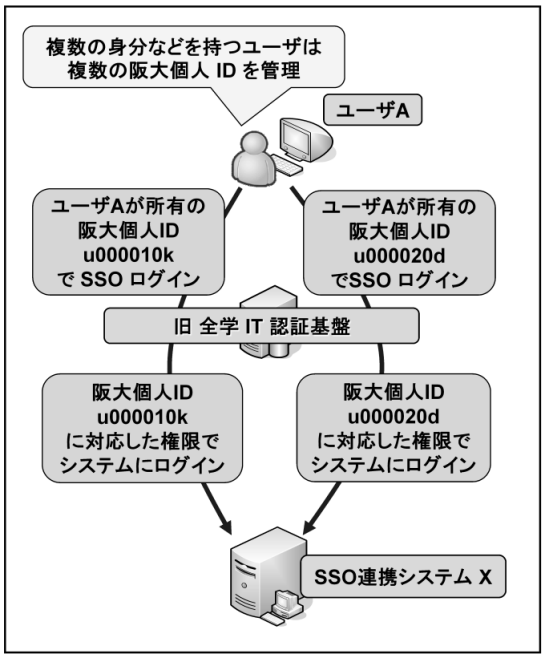
3. で述べた通り，新システムでは個人ID体系の再設計を行ったことで，ユーザのSSO認証ログイン方式を変更している．図5にSSO認証ログイン方式の新旧比較を示す．(a) の旧システムでは，複数の阪大個人IDを管理するユーザは利用するSSO連携システム X の形態に応じて，阪大個人IDを使い分けてログインする必要があった．(b) の新システムでは複数の Role IDを持つユーザは，全学IT認証基盤システムの認証サーバで Personal IDとパスワードでSSO認証を行った後，Role IDを選択することで，ユーザの属性に応じたSSO連携システム X へのログインを可能としている．

図6にSSO認証ログイン時における Role ID選択画面を示す．学内のSSO連携システムにアクセスする際には，図6の上の画面に示すように，最初は全学IT認証基盤サービスへのログイン画面が表示される．Personal ID(阪大個人ID) とパスワードを入力して「ログイン」ボタンを押すと，下の画面に移り，ユーザが所有している全てのロールIDが表示される．この画面上でSSO連携システムで利用したい「所属」及び「職名/身分」の Role IDを選択して「OK」ボタンを押すことでログイン処理が完了する．

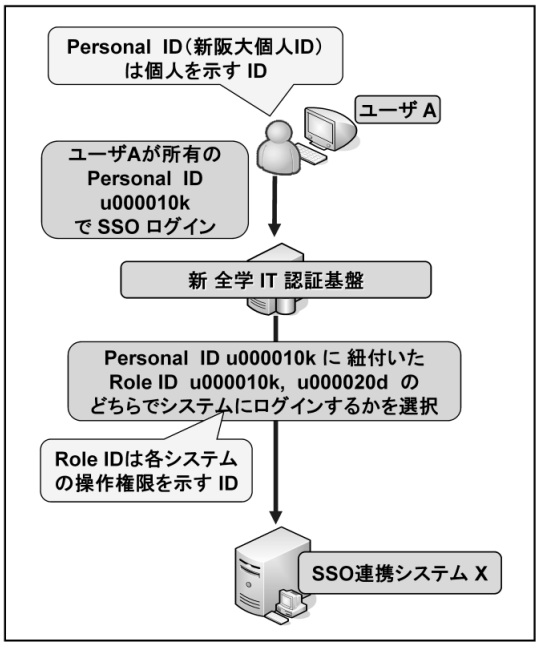
4.3 入力代行設定機能

学内SSO連携システムで発生する教員の業務を事務系職員に代行させて入力処理などを実施したいという要求がこれまでも多くみられるが，旧システムでは本人による認証ログインしか受け付けていなかった．そのため，入力代行などを行いたい場合は教員本人の個人ID，パスワードを他人に受け渡すなどの行為が行われており，本来の認証機能が損なわれる事態が生じている．この問題を受けて，新システムではSSOによる入力代行設定機能を実装した．本機能は，あるユーザ (代行元) の操作権限を別のユーザ (代行先) に代行設定を行うことで，SSO連携システムに代行元ユーザの環境でログインして利用することができる．

図7に入力代行設定画面を示す．入力代行設定は本学の事務用グループウェアである ICHO のワークフロー機能を用いて行う．ユーザは ICHO にログインして，入力代行設定のメニューを選択する



(a) 旧システム



(b) 新システム

図 5: SSO 認証ログイン方式の比較

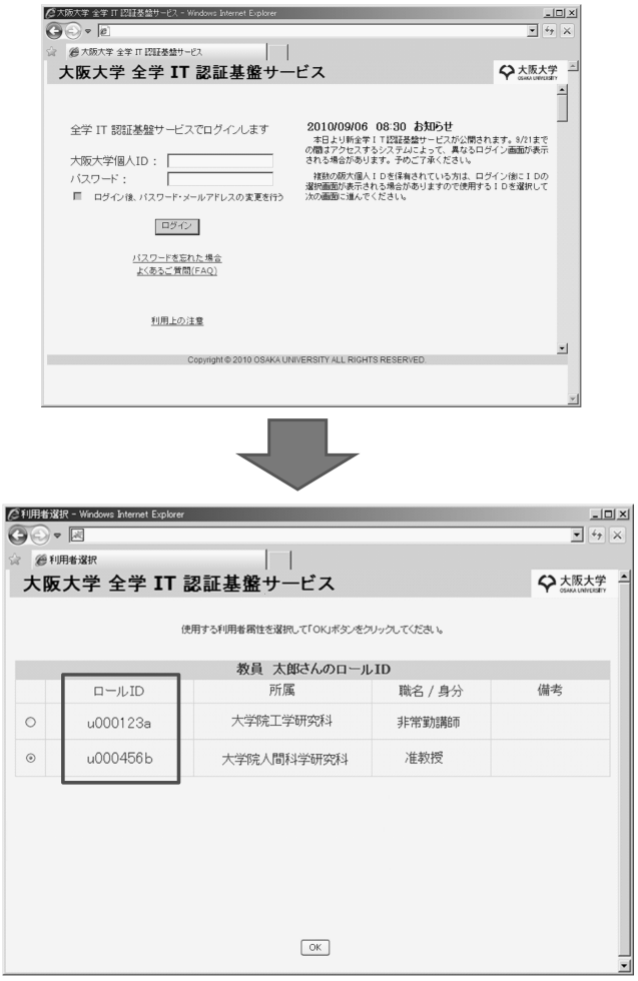


図 6: SSO 認証ログイン時における Role ID 選択

と図 7 の画面が表示され，設定申請を行うことができる．ユーザから申請された入力代行設定の情報はマスターデータベース上で管理される．IdP サーバは SSO 認証ログイン後にその情報を参照し，入力代行分を含め複数の Role ID を保持している利用者の場合と同様に，図 6 に示す利用者選択画面上に併せて選択項目として表示される．

5 マスターデータベースによる属性情報の一元管理

全学 IT 認証基盤システムでは学内の人事，学務情報システムからユーザの属性情報を取得している．しかし，これらの属性情報が最新になっていないケースが多い．特にユーザの所属に関しては人事上の所属情報がそのまま登録されるため，実際に所属する部局名と一致していないユーザが多数存在するといった問題が生じている．その他の

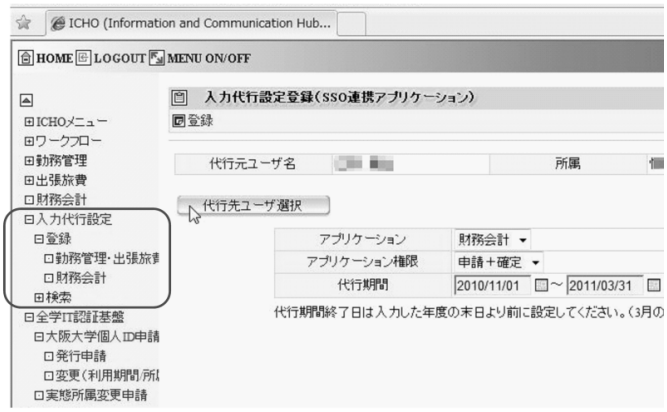


図 7: グループウェアのワークフロー機能による入力代行設定

身分等に関する情報も学内事情に適応できていないため，学内 SSO 連携システムにおける認可処理などに適用できない問題も指摘されている．

このような問題点を受けて，新全学 IT 認証基盤システムではユーザに対する主要な属性情報の一元管理を行い，学内連携システムが本データベースを参照することで，最新かつ適確な属性情報の管理を行い，統制のとれた学内システム間連携の実現に向けて，新たにマスターデータベースシステムを導入した．

マスターデータベースシステムでは，管理するユーザ属性情報の体系の整備，ユーザの実態に合った所属情報の整備 (所属情報の区分方法，コード体系などの見直し)，認証・認可処理にも適応可能な職名，身分，分類情報の整備などを考慮してデータベース構築を実施した．

しかし，所属情報に関しては人事システムや職員録の情報を基にした整備では部局のみが把握している所属情報を取得できないため，対応に限界があることがわかった．そこで，所属情報の変更申請を部局の事務担当者から行ってもらい，ユーザの実態所属情報を取得する方式を取ることにした．図 8 にグループウェアのワークフロー機能による所属情報変更申請画面を示す．申請者である部局の事務担当者は所属情報を変更したいユーザについて，実態の所属情報を選択して申請を行うことで，マスターデータベース側で所属情報の変更処理が行われる．

また，グループウェアのワークフローではこれまでは紙ベースで行っていた大阪大学個人 ID 申請機能も提供している．この機能は全学 IT 認証基盤

システムを利用するユーザのうち人事，学務システムに登録されていないユーザに対する個人 ID 発行申請を行うためである．

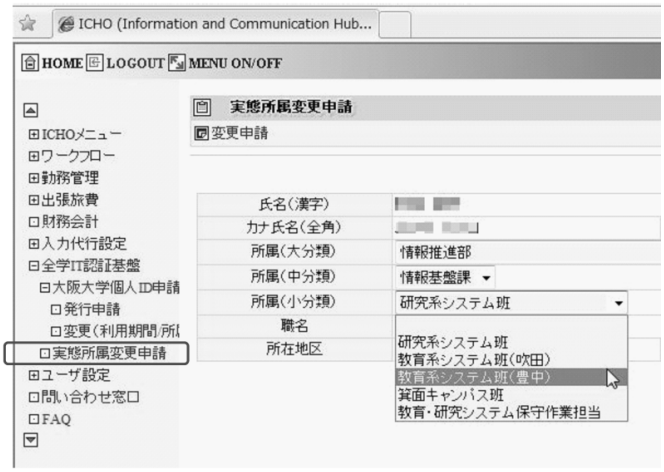


図 8: グループウェアのワークフロー機能による所属情報変更申請

6　まとめ

本稿では，全学 IT 認証基盤システムのこれまでの運用における問題点や今後の学内システムに対する SSO 認証連携及びデータ連携を更に推進していく上で必要とされる課題を受けた形で構築し，平成 22 年 10 月より新たに運用を開始した新全学 IT 認証基盤システムの概要について述べた．

今後の検討課題として，学内連携システムの様々な要望に適応可能なマスターデータベースの更なる整備，個人 ID の発行方式 (名寄せ処理，Personal ID と Role ID の関連性の整理) の検討などが考えられる．また，事務基幹系システムの SSO, データ連携の本格化に従い，業務処理の電子化への対応も急務とされる．これに関しては，IC カード等を活用した PKI アプリケーション基盤の構築などの検討も必要になると考える．

参考文献

[1] 秋山 他, “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.

[2] Web シングルサインオン TrustBind/Federation Manager, http://www.ntts.co.jp/products/trustbind/index.html

[3] JapanSIG/Documents/TechTutorials http://wiki.projectliberty.org/index.php/JapanSIG/Documents/TechTutorials

[4] Shibboleth http://shibboleth.internet2.edu/

[5] IDM 同期システム結人, http://www.intec.co.jp/service/network/yuito.html