大阪大学における全学 IT 認証基盤の構築

秋山豊和[†1] 寺西裕一[†2] 岡村真吾[†1]
坂根栄作[†1] 長谷川剛[†1] 馬場健一[†1]
中野博隆[†1] 下條真司[†1] 長岡亨[†3]

大阪大学では，高いセキュリティレベルと標準的なインタフェースを兼ね備えた認証技術として注目されている公開鍵基盤（PKI: Public Key Infrastructure）に基づく全学 IT 認証基盤を導入した．本学で導入した全学 IT 認証基盤システムでは，署名・暗号化，学内認証，グリッドシステム認証，という異なるポリシに対応する複数の CA を導入・共存させている．これら複数の CA 向けの証明書発行を自動化することにより，安全性と利便性を両立した証明書発行サービスを実現している．また，PKI に対応したシングルサインオン（SSO）機能を導入し，学内ユーザが各システム間で統一的なインタフェースにより認証を行えるようにした．アプリケーション Web サーバに認証機能を組み込むエージェント型の SSO 機能の導入により，1 度アプリケーションを SSO 対応させてしまえば，アプリケーションを変更することなくシームレスにパスワード認証から PKI 認証へ移行・共存することが可能となった．さらに，ユーザ ID 体系として，公開用に変更を許容するユーザ ID と，システム間連携用に 1 人に 1 つ決まる不変のユーザ ID とを設け，それらの対応付けを内部的に行うことにより，安全性・柔軟性ある運用を可能とした．本稿では，本認証基盤の設計と実装について述べるとともに，システムの導入により得られた技術的ノウハウや今後の展開についても述べる．

Campus-wide IT Authentication Infrastructure Development in Osaka University

Toyokazu Akiyama,[†1] Yuuichi Teranishi,[†2] Shingo Okamura,[†1]
Eisaku Sakane,[†1] Go Hasegawa,[†1] Ken-ichi Baba,[†1]
Hirotaka Nakano,[†1] Shinji Shimojo[†1] and Toru Nagaoka[†3]

In Osaka University, a campus-wide IT authentication infrastructure based on Public Key Infrastructure (PKI), which is regarded as a technology providing high security and standard interface to many applications, has been adopted. In this authentication infrastructure, multiple CAs for the different purposes such as signing and encryption, intra-campus authentication and grid system authentication coexist. To realize security and convenience, we developed an online certificate issuance service for those multiple CAs. We also introduced PKI enabled Single Sign-On (SSO) system to provide unified authentication interface. Since the SSO system supports 'SSO agent', which provides SSO functionality for web applications by installing a web server module, it is possible to migrate from password authentication to PKI authentication without modifying applications. Furthermore, we established secure and flexible identity management by separating changeable, public user ID and static, internal system ID. Internal system ID is used for managing and federating user profiles among the systems. The mapping between those two IDs is done by the SSO system. In this paper, we describe design and implementation of our authentication infrastructure, know-how of system establishment and future works.

†1 大阪大学サイバーメディアセンター
Cybermedia Center, Osaka University
†2 大阪大学大学院情報科学研究科
Graduate School of Information Science and Technology, Osaka University
†3 大阪大学情報基盤デザイン機構
Organization for Information Infrastructure Design, Osaka University

1. はじめに

大阪大学サイバーメディアセンター（以下 CMC）では，キャンパスネットワーク，教育用計算機システム（Linux，Windows），各種 Web システムといった学内の IT サービスの導入・運用を行っている．近年，大阪大学を含めた教育や研究の現場において，業務シス

テム等のオンライン化が進むに従って，システムの複雑化，セキュリティの維持が課題となっており，CMCにおいてもシンプルかつ安全なITサービスの実現が求められてきた．こうした状況のもと，大阪大学では学生の学籍管理，履修登録，成績管理を統合する学務情報システムKOAN（Knowledge of Osaka University Academic Nucleus）や，WebCT，NetAcademy等のe-Learningシステム，人事給与システム，図書館の貸し出し管理システムといったオンラインWebアプリケーションが次々に本格導入されるに至り，これらの学内アプリケーションのセキュリティやインタフェースの統合を目指した検討を進め[1]，**全学IT認証基盤システム**を導入することとした[2]．

上記のうち，たとえばKOANにおいては学生の学籍情報や科目履修情報，e-Learningシステムにおいては学生個々の成績，人事給与システムにおいては教職員の人事情報等，重要な個人情報が管理される．したがって，システムを利用できる利用者を正しく識別し，認証できる仕組みを，高いセキュリティを保ったうえで実現する必要がある．このとき，複数システムを連携させることや将来の拡張性を考慮すると，どのベンダであっても対応できる標準的なインタフェースの採用が望ましい．

高いセキュリティレベルと標準的なインタフェースを兼ね備えたセキュリティ技術としては，公開鍵基盤（PKI: Public Key Infrastructure）が広く普及している．PKIを利用し，認証デバイス等に秘密鍵を保持することで，パスワード認証で問題となるパスワードの漏えいや管理の問題を解決することができる．また，認証だけでなく，S/MIME等の技術によりEnd-to-Endでの署名・暗号化を応用した様々なアプリケーションの実現が可能である．そこで，大阪大学では全国の国立大学法人に先駆け，このPKIを全学IT認証基盤において本格導入することとした．

PKIを大学の認証基盤として導入するうえでは，まず，認証局（CA: Certificate Authority）構築時の運用ポリシ選択が課題となる．将来的な大学間認証連携を考慮した場合，大学によって実現されるPKIの運用ポリシは異なると考えられ，連携のために共通のCAを立てることは現実的ではない．また，たとえば，計算リソースの共有を行うグリッドシステム向けのPKIと，セキュリティを重視した学内サービス認証のためのPKIのポリシは異なる．したがって，大学間・システム間のポリシの違いを考慮したCAの構築が必要となる．

また，通常，大阪大学のような総合大学においては，複数の部局がそれぞれ独自にオンラインアプリケーションを構築することがつねであるため，必ずしもすべてのシステムをPKI対応として均一に更新できないという点も課題となる．パスワード認証からPKIへの移行あるいは共存が可能な仕組みが必要である．

さらに，アプリケーションでPKIを利用するには，証明書に記載されるユーザIDに基づき認可を行う必要がある．このため，ユーザIDや認可に必要となる属性を連携アプリケーションにおいて共有しなければならない．証明書のユーザIDは，他組織との連携にPKIを用いた場合，周知のものとなるため，悪意ある者に漏えいする可能性を想定したうえで，システム間で安全かつ運用性高くユーザID，属性を共有できる方法をとる必要がある．

本稿では，これらの課題に対処し，大阪大学において導入した全学IT認証基盤システムの設計と実装について述べる．以下，2章ではシステム導入における問題点について分析し，3章において解決方法を示す．4章ではシステムの実装，5章ではシステムの運用状況・性能評価について述べる．6章では，今後の課題について述べ，7章でまとめる．

2. 全学IT認証基盤実現上の課題

大阪大学において，全国の国立大学法人に先駆け，PKIを全学IT認証基盤として本格導入するにあたり，多くの解決すべき課題があった．本章では，それらのうちいくつかの本質的課題について述べる．

2.1 CA構築時のポリシ選択

大阪大学では学内アプリケーションのセキュリティ向上を目的としてPKIを導入するため，秘密鍵は認証デバイスに格納する等，保証レベルの高いCA運用ポリシ（CP/CPS: Certificate Policy/Certification Practice Statement）を選択する必要がある．

一方，国立大学の法人化後，各大学が保有する共同利用センタの統合が推進され，大学間での施設の相互利用が急速に進みつつある．UPKI（University Public Key Infrastructure）プロジェクト[3),4)]では，大学間の相互連携を推進するための基盤整備を進めている．

PKIを導入するにあたり，各大学によってポリシはそれぞれ異なると考えられる．たとえば，標準的なポリシに基づいて運用する大学もあれば，標準的なポリシでは不足と考え独自のポリシのもとに高度なPKIを望む大学もあると考えられる．これは各大学・研究機関が所有する研究リソースが異なることからも必要な差異であると考えられ，全国800有余の大学・研究機関が一元的なポリシでPKIを運用することは現実

的ではない．

一方，大学間連携の一例として，グリッド技術を用いることで，計算機センタ間で計算リソースを共有し，さらに高性能な計算サービスを提供する試みとして，本学でも組織間連携を想定したグリッドシステムの構築を進めている[5]．グリッド分野では，組織間のリソース共有を進めるために，IGTF（International Grid Trust Federation）[6] において，各組織が運用している CA の相互運用のためのポリシを策定している．現時点ではユーザの利便性を重視し，サーバ側でユーザの PKI の鍵ペアを管理し，本人認証は ID・パスワード等の認証で実施する形式の運用（Short-Lived Credential Service Profile）を採用しているサイトが多い．学内アプリケーション認証向けには認証デバイス等に秘密鍵を保持することとすると，グリッド用の CA と学内アプリケーション認証向けの CA を共通の CP/CPS で運用することはできないことになる．PKI の導入にあたっては，このような大学間・システム間のポリシの違いを考慮した CA の構築が必要である．

2.2 パスワード認証方式との併存と移行

大阪大学では，これまで全学的に統一したユーザアカウント ID を採用し，パスワード認証を行ってきた（統一アカウントシステム）．この統一アカウントシステムを採用していたアプリケーションを，全学 IT 認証基盤の連携アプリケーションとして移行する必要がある．このとき，既存の連携アプリケーションは，パスワード認証を想定した実装のみであるためシステムの更新が必要である．しかし，各アプリケーションは，それぞれ別の部局が独自に構築したものであり，同時期にシステムの対応を行うことができない．さらに，システムの運用を長期間停止させることも許されないため，すべてのシステムが PKI 対応を完了するまで待つことはできない．また，PKI の秘密鍵を格納する認証デバイスの導入コストが大きいため，大阪大学では最初からすべてのユーザを PKI に移行することは難しく，一部ユーザから段階的に PKI を利用可能とすることとしている．このように，通常，パスワード認証は PKI の導入が完了するまでは継続する必要がある．さらに，学内アプリケーションによっては，キャンパス内のユーザだけでなく，海外の元留学生や地域住民といった，認証デバイスを配布することが不可能，もしくは困難なユーザが含まれる場合がある．このようなアプリケーションでは，実現されるセキュリティレベルが低くても ID・パスワードによる認証を認めざるをえない．

ID・パスワードによる認証と，PKI 認証を認証デバイスにより行う場合では，なりすましの脅威への耐性が異なるため，本人性の保証レベルが異なる．こうした保証レベルの違いに応じた認可の選択をアプリケーションに与えたうえで，双方を併存もしくは移行できる認証の仕組みが必要となる．

2.3 キャンパス ID 管理との連携

アプリケーションで PKI を認証等に利用するためには，各アプリケーションで用いるユーザ ID が，証明書の DN（Distinguished Name）に記載された ID と対応付けられている必要がある．たとえばグリッド分野では各リソース上の ID と証明書の DN を対応付ける gridmap file を管理している．しかし，各連携アプリケーションでこのような対応を管理すると，運用コストが大きくなってしまう．運用コストを抑えるには，各アプリケーションのユーザ ID の統合が必要となる．

証明書の DN 定義の際，一般的には，DN に所属等の属性情報を含むこととなる．証明書の有効期限はユーザの利用期間や在籍期間に合わせて設定されるが，属性は異動等によって変更される可能性があり，属性の有効期限は証明書の有効期限と一致しない．このため，DN に所属等の属性情報を含むと，属性が変更されるたびに証明書を再発行する必要が生じる．これを避けるためには，ユーザ ID にユーザの属性情報を含まない ID 設計が必要となる．

ユーザ ID と属性情報を分離することで，個人情報の保護や運用面での ID 再発行業務は削減できるが，連携システムとの間で属性情報の共有を行う必要が生じる．証明書のユーザ ID は，他組織との連携に PKI を用いた場合，周知のものとなるため，悪意ある者に漏えいする可能性を想定し，変更可能とする必要がある．しかし，各連携アプリケーションシステムに，分散保存されるユーザ ID を更新することは容易ではない．たとえば，アプリケーションが e-Learning の成績情報をバックアップしアーカイブしていた場合，これを更新することは困難である．システム間で安全かつ運用性高くユーザ ID，属性を共有できる方法をとる必要がある．

3. 全学 IT 認証基盤の設計

本章では，2 章で述べた課題に対処すべく構築した全学 IT 認証基盤の設計について述べる．

3.1 異なるポリシを持つ CA の並行運用

2.1 節で述べたとおり，学内サービス用とグリッド用の 2 つのユーザ認証ポリシが存在する．したがって，大学間連携用のグリッドシステム向け CA は学内サー

表 1 発行する証明書に応じた CA の構築方法
Table 1 Suitable type of CA for each certificate usage.

発行する証明書	CA 構築方法
ユーザ用（認証）	クローズドドメイン CA
ユーザ用（署名・暗号化）	オープンドメイン CA
ユーザ・サーバ用（グリッド）	クローズドドメイン CA
サーバ用	オープンドメイン CA

ビス用の CA とは分けて構築する必要がある．

また，学内サービス用の CA については，さらに 2 つのポリシに分類される．1 つは S/MIME 等の End-to-End の署名・暗号化用途，もう 1 つはユーザ認証用途である．

S/MIME 署名・暗号化のようにエンドユーザが利用するサービスでは，サービスを利用するすべてのユーザが，相手の証明書を検証できるよう CA 証明書や CRL（Certificate Revocation List）を安全に配布する必要がある．よって，信頼の拠点となるルート CA を学内に設置するクローズドドメイン CA では，他大学や企業との相互利用を考えた場合に運用が困難となる．このように，署名・暗号化用途においては，信頼の拠点となるルート CA の証明書が一般の PC 等にあらかじめ信頼済み証明書として格納されるオープンドメイン CA の利用が現実的である．オープンドメイン CA をインハウスで構築するためには，WebTrust for CA 認定[7] が必要となり，莫大な運用コストが必要となる．よって，オープンドメインの CA が必要となる署名・暗号化用途の証明書発行はアウトソースとせざるをえない．このようにオープンドメイン CA をアウトソースした場合，発行できる証明書の有効期限はアウトソース先のポリシで決定される．

一方，後者のユーザ認証用途においては，認証を要求するサービス側が，ユーザの証明書（ユーザ認証用証明書）を検証できればよい．よって，ユーザ認証用証明書の検証に必要となる CA 証明書や CRL は，サービス提供者に安全に配布されればよい．また，ユーザ認証用証明書においては，学生や非常勤職員等，在籍期間が決まっているユーザに対しては，あらかじめ在籍期間と同じ有効期限を設定した証明書を，学内の運用に合わせて発行する必要がある．よって，安全性の観点からも，有効期間設定の柔軟性の観点からも，ユーザ認証用証明書を発行する CA はクローズドドメインがふさわしい．

表 1 は，以上で述べた認証基盤として必要となる PKI の証明書とその CA の構築方法の関係をまとめたものである．表に示したとおり，ユーザが保持しなければならない証明書は，認証，署名・暗号化，グリッドと 3 種類存在することとなり，これらをユーザの利便性を損なわないよう連携させなければならない．

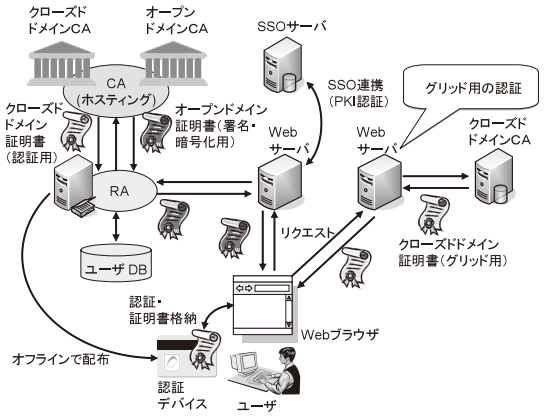


図 1 ユーザ用証明書の配布方法
Fig. 1 The user certificate distribution procedure.

そこで，全学 IT 認証基盤では，認証用証明書を格納した認証デバイスをユーザへ配付したのち，署名・暗号化用証明書やグリッド用証明書をオンラインで認証デバイスにエンロールする Web システムを設計・開発した．エンロールにより証明書を発行する Web サーバは，認証デバイスに格納されたユーザ認証用証明書と秘密鍵を用いてユーザ認証を行う．各証明書は，認証デバイス上で生成される秘密鍵に対応する証明書発行要求に応じて各 CA から発行される（**図 1**）．署名・暗号化用証明書は，S/MIME で利用可能とするため，電子メールアドレスを証明書発行時に証明書に埋め込んでいる．本学では，職員，学生向けのメールサービスは提供しているが，教員向けのメールサービスはなく，事実上全学のメールサービスがない状態である．よって，エンロール時にユーザが S/MIME で利用したい電子メールアドレスを指定可能としている．

表 1 に示したとおり，ユーザ証明書以外に，サーバで HTTPS を利用するためにサーバ証明書が必要となる．サーバ証明書は，署名・暗号化用途の証明書と同様，すべてのユーザが証明書を検証できるようオープンドメイン CA を利用する必要がある．オープンドメイン CA による証明書発行サービスは一般的になりつつあり，大阪大学においても同様に一般の証明書発行サービスを用いる．

3.2 Web シングルサインオンと PKI の併用

2.2 節で示した，パスワード認証と PKI 認証の並行運用と移行をシームレスに行うため，全学 IT 認証基盤では，Web シングルサインオン（SSO）を導入す

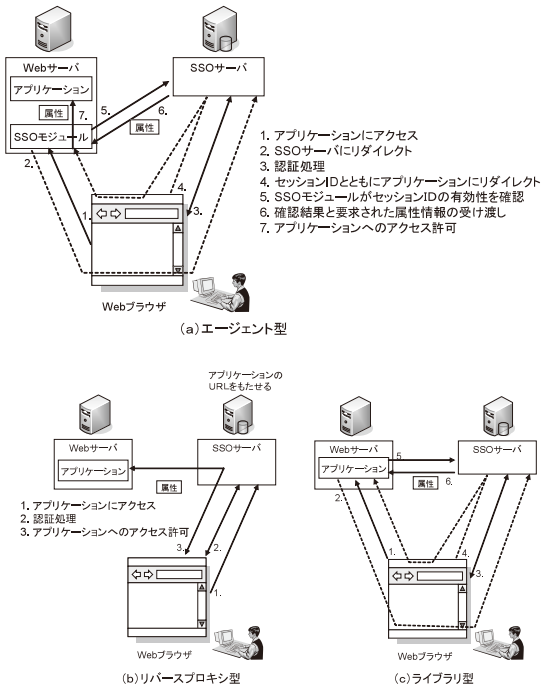


図 2 Web SSO の実装の分類
Fig. 2 A classification of the Web SSO implementation.

る．Web SSO の実装方法は大きく分けて以下の 3 つに分類できる．

(1) エージェント型

エージェント型の動作概要を**図 2** (a) に示す．エージェント型では，対象となる Web サーバに SSO エージェントをモジュールとして組み込む．SSO エージェントが導入された Web サーバにアクセスした際，クライアントが SSO サーバによって設定された「セッション ID」を提示しなければ，SSO サーバにリダイレクトされる．SSO サーバでログインが完了するとセッション ID が渡される．SSO エージェントは提示されたセッション ID が正しいかどうかを確認し，確認できた場合には，Web アプリケーションに HTTP リクエストを転送する．リバースプロキシサーバに SSO エージェントを導入することで，リバースプロキシ型としても利用できる．ただし，対象となる Web サーバに対応したモジュールが提供されている必要がある．リダイレクトを利用せず，最初に SSO サーバで認証させてからアプリケーションへのリンクを選択してログインさせる運用も可能である．

(2) リバースプロキシ型

リバースプロキシ型の概要を図 2 (b) に示す．Web アプリケーションから見た動作はエージェント型とほぼ同様で，SSO エージェントが別サーバで動作しており，そこに SSO サーバの機能が統合された形になる．リダイレクトが不要になるが，Web サービスへのアクセスがリバースプロキシサーバを経由することになるため，アプリケーションの要求によっては，高性能なリバースプロキシサーバが必要となる．

(3) ライブラリ型

ライブラリ型の概要を図 2 (c) に示す．ブラウザ側から見た動作はエージェント型と同様である．ライブラリ型では，様々なプログラミング言語用の SSO ライブラリを提供し，SSO の機能をアプリケーション内に組み込む形で実装する．SSO エージェントの機能が Web アプリケーション内で提供される形態と見なすことができる．独自に SSO 機能を実装した場合も同様に，アプリケーション内部に SSO 処理を組み込むことになる．

いずれのタイプの SSO でも，ユーザ認証はアプリケーションを提供する Web サーバとは別の SSO サーバで実施される．このとき，SSO サーバにおいて，最初に PKI 認証を受け付け，ユーザが PKI に対応していない状態，すなわち，認証デバイスがユーザのクライアントに接続されていない，もしくは，ブラウザが対応していない場合に，パスワード認証に移行する動作とすれば，双方の認証方式を併存させることが可能となる．また，SSO サーバにおいて，どの認証方式で認証を行ったかを対象アプリケーションへ通知することにより，PKI でのみログインを許可するといった選択をアプリケーションに与えることが可能となる．たとえばパスワード認証から PKI 認証に移行することをあるアプリケーション運用者が決めた場合，そのアプリケーションの Web サーバ側の設定を変更すればよい．このとき，他のアプリケーションの運用に影響を与えることはない．

ただし，SSO に対応するためには，アプリケーション側の変更が必要となる．前述のとおり，総合大学では各部局が独自にサービスを導入することが多く，異なるベンダによって導入されたアプリケーションを統合することになる．そのため，アプリケーションと SSO サービスの切り分けが容易であることが望ましい．そこで，全学 IT 認証基盤では，エージェント型の SSO を採用することとし，Web サーバやアプリケーション側の都合でエージェントの導入が難しい場合には，リバースプロキシ型を併用することとした．エージェント型およびリバースプロキシ型では，SSO 関連の設定変更は SSO エージェントや SSO サーバの設定変更のみで対応できるため，アプリケーション側の変更が不要となる．ただし，Web アプリケーションの認

証を SSO エージェントに対応した認証に作り変える必要がある．パッケージ製品等でどうしても認証部分を作り変えるのが難しい場合には，アプリケーションの認証処理を代行するリバースプロキシサーバを導入し，リバースプロキシサーバとアプリケーションサーバの間で認証情報を同期する仕組みを構築する必要がある．

現在，大学間の認証連携に SAML（Security Assertion Markup Language）2.0[8] を採用することが検討されている．SSO として SAML に対応させることにより，将来的な大学間認証連携への移行も可能となる．

3.3 キャンパス ID の再設計とディレクトリ統合管理

大阪大学では，入学時に対面で本人確認された学生のデータが学務情報システム KOAN に登録される．また，採用された教職員も同様に採用時の手続きに基づき人事給与システムに登録される．全学 IT 認証基盤では，これらのシステムへ登録されたユーザであることが，PKI としてユーザの存在を保証することとなる．全学 IT 認証基盤では，これらのシステムから得られる個人情報をもとに，システム間で安全かつ運用性高くユーザ ID，属性を共有できるよう，ID 体系を新たに定義した．

以下に全学 IT 認証基盤のユーザ ID 体系について，概要を示す

(1) 大阪大学個人 ID（Public User ID，PID）
半角 8 byte の英数字列であり，大阪大学の学内情報システムを利用する大阪大学関係者 1 人に対して識別子を割り当てる．文字列としてユーザの属性情報に基づかず，ランダムに生成される文字列とする．PID が，学内情報システムを利用するユーザに配付する公開ユーザ ID である．PID が悪意あるユーザに流出し，攻撃の対象となっている場合等やむをえない理由があるときは，変更可能とする．

(2) システム個人 ID（System User ID，SID）
個人情報を扱う学内情報システムがユーザを識別するために用いる識別子であり，1 人に対して生涯同じ識別子を割り当てる．SID は東京工業大学の構築例を参考に導入した．文字列としてユーザの属性情報に基づかず，ランダムに生成される文字列とする．学内の個人情報を扱う各情報システムにおいてユーザを識別するユーザ ID は，このシステム ID であり，情報システム内のデータベースは基本的にシステム ID をキーとして構築されるものとなる．

(3) ローカル個人 ID（Local User ID，LID）
学外ユーザやゲストユーザを独自に扱う必要があるシステムにおいて，それらのユーザ向けに，学内ユーザと独立して割り当てるための個人 ID である．阪大個人 ID，システム ID とは名前空間が異なり，文字列が重なることはない．

ランダムに生成する ID 体系を構築することで，属性情報を独立させ，情報源システムの ID への依存を解消できる．その結果，ID のライフサイクルはユーザの在籍期間に一致させるものとし，KOAN 上での進学や所属変更に対して，同一 ID を引き継ぐことで，ユーザの利便性を向上させ，ID 再発行の運用負荷を削減することができる．

PID と SID を分けることにより，システムごとに記録する個人情報と本人識別用の情報を分割して記録することが可能になる．また，PID が変更となった場合も，SID を変更する必要はなく，連携システムにおいて，別媒体にデータをバックアップ等していたとしても，それらに影響は及ばない．

PID と SID の対応は，SSO サーバにのみ記録しておき，SSO 連携システム上には SID をキーとして各種属性を格納しておく．SSO サーバに PID でログイン後，アプリケーション側には対応する SID および必要となる属性情報を渡すことで，アプリケーション側には PID や個人を限定可能な属性情報を記録しなくてもアクセス制御や該当する個人情報の取り出しが可能となる．

ただし，SSO に対応していないシステムでは，個人を特定可能な属性情報とともに，PID や認証情報（パスワード等）を同期させる必要がある．

4. 全学 IT 認証基盤システムの実装

全学 IT 認証基盤システムの構成を**図 3** に示す．キャンパス PKI を実現するための CA サーバ，登録局（RA: Registration Authority）サーバ，IC カード発行システム，Web アプリケーションの認証を統合す

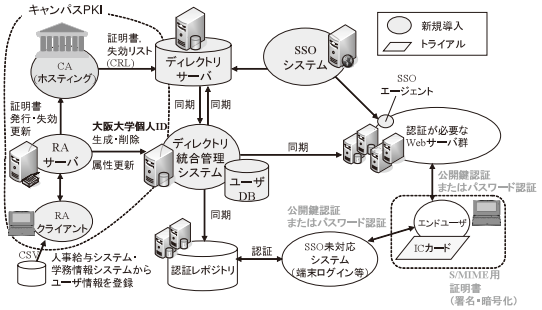


図 3 全学 IT 認証基盤システム
Fig. 3 Campus-wide IT authentication infrastructure.

る SSO システム，連携システムへの ID 同期や SSO 未対応なシステムへの認証情報の同期を行うディレクトリ統合管理システムから構成されている．以下では各サブシステムについて述べる．

4.1 キャンパス PKI

キャンパス PKI は，CA システム，RA システム，トライアル IC カードにより実現されている．

3.3 節で述べたとおり，KOAN および人事給与システムのデータベースを ID 管理の情報源とすることで，RA 業務が簡素化できる．そのため，RA はインハウスで構築した．

CA は 3.1 節で述べた構成を実現するため，学内ユーザ用の CA としては日本ベリサインのアウトソース CA を採用した．ユーザ認証用証明書および署名・暗号化（S/MIME）用証明書をこのアウトソース CA より発行する．

うち，署名・暗号化用証明書は，S/MIME 用証明書として利用できるよう，メールアドレスを含む証明書とした．S/MIME 用証明書に記載するメールアドレスは，学生には全学メールサービスのアドレスを自動登録し，教職員には希望するアドレスを登録できるインタフェースを提供している．このインタフェースはユーザ認証用証明書を用いて認証を行っており，大阪大学の構成員であれば，PKI 認証により署名・暗号用の証明書をオンラインで取得できる．日本ベリサインの CA にアクセスするための証明書発行用サーバとして，Targusys [9] を導入している．

グリッド用には NAREGI-CA [10] を用いたインハウス CA を採用した．NAREGI-CA は，従来ライセンス ID を用いて証明書を発行するウェブインタフェースを標準としていた．今回この NAREGI-CA に，学内の利用者管理システムから得られる情報と，学内ユーザ認証用証明書を用いた認証により，グリッド用の証明書を発行する機能拡張を施した．これにより，グリッド証明書の証明書取得プロセスを簡素化することができる．

PKI を利用するうえでは，公開鍵，秘密鍵をいかにユーザに管理させるかが問題となる．セキュリティの向上と，ユーザの利便性を考慮した場合，鍵ペアを認証デバイスで管理する必要があり，全学 IT 認証基盤では，IC カードを想定してシステムを構築している．

HTTPS を利用するためのサーバ証明書は，システムごとに購入した場合，個別に煩雑な手続きを行う必要があり，また費用もかかる．そこで，一部のサーバでは UPKI プロジェクトが提供しているサーバ証明書発行サービスを利用し，コストの低減を図っている．

4.2 SSO システム

SSO システムは SSO サーバと Directory サーバからなる．全学 IT 認証基盤システムでは，3.2 節で述べた機能を実現するため，SSO サーバとして Sun Java System Access Manager [11]，ディレクトリサーバとして Sun Java System Directory Server [11] を採用した．ディレクトリサーバには，4.3 節で述べるとおり，ディレクトリ統合管理システムによりユーザ情報が同期される．

SSO システムは 3.2 節で述べたエージェント型のシステムで，SAML2.0 に対応している．SSO エージェントとして Apache や IIS をはじめとする主要な Web サーバおよび Tomcat 等の J2EE サーバ用のモジュールが用意されている．セッション ID は Cookie，または，Liberty Browser POST Profile [12] と同様な方式で受け渡しする．リダイレクトを利用する SSO システムでは，悪意のあるサイトにより，偽のログインページに誘導される危険性があるが，本システムでは SSO エージェントが導入された連携システムの URL を事前に登録できるため，任意サイトの指定を回避できる．Web アプリケーションが認証後に ID やその他の属性情報（職種，所属等）を必要とする場合は，SSO エージェント側で指定することで，ディレクトリサーバ上の任意の属性を HTTP リクエストのヘッダまたは Cookie として付加できる．アプリケーション側の SSO 対応は，アプリケーションのログイン処理部分を，HTTP リクエストから必要な属性を取得するコードに置き換えることで対応できる．

SSO サーバはパスワード認証，PKI 認証等，複数の認証方式に対応しており，PKI 認証に失敗したらパスワード認証に切り替えるといった認証方式の連鎖も指定できる．ユーザがログイン時に利用した認証方式が SSO サーバ側で定義した認証レベルを満たしているかどうかをパラメータとして Web アプリケーションに受け渡しできるため，アプリケーションに応じて要求する認証レベルを変更できる．SSO サーバは OpenSSO Project [13] においてオープンソース化されており，今後 SSO システムの導入を検討している組織にとって，試験導入が容易である．

4.3 ディレクトリ統合管理システム

全学 IT 認証基盤システムは 3.3 節で述べたとおり，KOAN，人事給与システムを情報源としており，各情報源システム上に登録されたエントリに同期する形で ID の生成・削除・更新を行う．ID に付随する属性情報は，各情報源で管理されているものをそのまま登録する．KOAN，人事給与システムに登録されない人員

（無給の非常勤教職員等）が連携システムを利用する場合には，人員の関係部局が部局長の承認を得て，部局管理のデータベースに登録したうえで，全学 IT 認証基盤に登録する．

ID 登録用のインタフェースは独自に開発しており，RA サーバの機能を兼ねている．RA サーバは 4.1 節で述べた証明書発行サーバと連携して動作し，証明書の発行処理も行う．現時点では情報源システムのデータが旧システムから受け継いだ正規化されていないデータを含んでおり，運用者による修正を可能にするため，CSV 形式での手動入力を採用している．データ連携のため CSV 形式でのデータ出力もサポートしている．

3.3 節で述べた属性情報の配信や連携システムへの ID 同期の機能を実現するため，ディレクトリ統合管理システム Sun Java System Identity Manager（以下 IDM）[11] を導入した．IDM は，データベースサーバやディレクトリサーバ等，様々なレポジトリに対応したインタフェースを提供している．上述のインタフェースで登録・削除・更新された ID と属性情報はユーザ DB 上に記録され，IDM により，ディレクトリサーバおよび連携システムのレポジトリに PUSH により同期される．

ユーザ情報の同期は，連携システムとの間に設置したプライベートセグメントを経由して行う．セキュリティ面からは全学 IT 認証基盤システムから連携システムに PUSH 型で同期する IDM による連携が望ましい．しかし，現状のシステム構成では追加できる連携先の数に限界があることや，連携システム側から能動的にデータ取得する方が連携構築のコストを抑えられるケースがある．そのため，PULL 型の同期方法として，ディレクトリサーバを用いて，LDAP（Light weight Directory Access Protocol）によるデータ提供も行っている．また，コスト面等から自動連携を構築できなかったシステムについては，CSV 出力により手動でデータ連携している．

連携システムにおいて，ID の有無や KOAN，人事給与システムから取得した属性情報（職種，所属等）により，システムの利用権限が判断できる場合は，SSO システムの機能で必要な属性をアプリケーションに受け渡して認可決定を行う．SSO 未対応なシステムでは，必要な属性を自身のレポジトリに同期し，ローカルで認可決定する．

SSO 連携しているシステムでは認証・認可情報を同期する必要はないが，たとえば WebCT のような e-Learning システムでは，履修情報や成績等，アプリケーションが記録するユーザ情報を管理するために，データベース上に ID を登録する必要がある．ID の登録方法としては，以下の 2 つの方法がある．

(1) 初回ログイン時に登録

SSO の機能で受け渡した ID をデータベースに記録する．ユーザ DB 上で ID が削除されたことを検出できないため，アプリケーション側で不要になったユーザ情報を定期的に削除する必要がある．

(2) IDM，LDAP，CSV で同期

ユーザ DB の情報と同期する．ID が削除された場合も同期できる．同期先が増加すると，全学 IT 認証基盤システムの負荷や運用コストが増加する．事前に他のシステムとデータ連携する必要がある場合は，この方法を用いる必要がある．

大阪大学では，WebCT を導入しており，授業の履修情報をあらかじめ KOAN から同期させるため，LDAP により同期させている．また，語学学習用の e-Learning システムである WebOCM も導入しているが，こちらは履修情報の事前同期を行っていないため，初回ログイン時の登録を採用している．

3.3 節で述べたように，ID 体系として，PID と SID を分けることで個人情報の保護を目指したが，WebCT をはじめとする e-Learning システムでは，教員が学生ユーザの一覧を参照して成績の投入や授業に関する質問への対応等を実施する必要があり，学生を特定する情報がある程度提示されていなければ，利用できない機能がある．図書館において窓口職員が利用者の代わりに図書貸し出し処理等を実施する場合にも同様の問題が発生する．このようなことから，一部のシステムでは PID，SID の分割が行えず，事実上形骸化している．しかし，個人情報の保護は重要な課題の 1 つであり，今後引き続き検討していく必要がある．

4.4 認証デバイスの実装

全学 IT 認証基盤では，認証デバイスとして，IC カードを想定してシステムを構築している．IC カードは，PKI 利用だけでなく，非接触インタフェースを共存させることで簡易認証や少額決済機能を搭載することが可能である，券面印刷により身分証明書機能を兼ねることができる，等の利点をあわせ持つ．

そこで大阪大学では，PKI 利用のための接触チップ，簡易認証のための非接触チップの 2 種類のチップを搭載したハイブリッド型の IC カードを採用することとした（**表 2**）．1 チップで 2 種類のインタフェースを持つデュアル型 IC カードも存在するが，学内では，教育用計算機システムとして Linux，Windows の端末が存在し，理学系，医療系部局で MacOS が多く採用されていることが分かっており，当時 Windows にし

表 2 トライアル IC カードの仕様
Table 2 The specification of Trial IC Card.

IC カードタイプ
接触と非接触のハイブリッド型 ・接触部分：ギーゼッケアンドデブリエント社製 ・非接触部分：FeliCa 磁気ストライプ
用途
接触部分：個人電子証明書（プライベート、パブリック）を格納する 非接触部分：簡易認証に用いる 磁気ストライプ：既存システムでの利用のために用いる
IC カードリーダライタ（接触部分）
USB 接続タイプ 対応 OS： Windows（2000、XP SP2 以降）、MacOS（10.x 以降）、Linux（カーネル 2.4 以降）

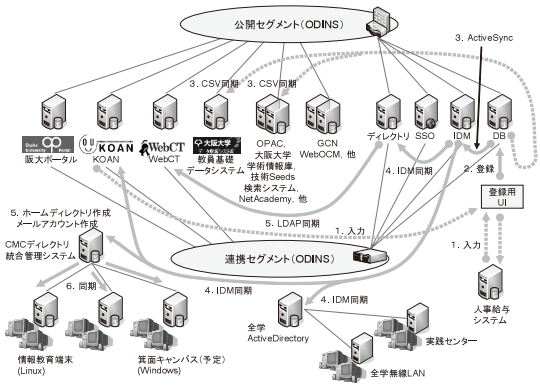


図 4 システムの連携状況
Fig. 4 Current status of the system federation.

か対応しておらず，かつインタフェース速度が不十分だったため，採用には至らなかった．

接触チップには，上記 OS に対応したドライバを有する G&D 社製，非接触チップには FeliCa が採用された．接触チップには，クローズドドメイン CA から発行されたユーザ認証用証明書を格納している．さらに，接触チップには複数の証明書が格納でき，オープンドメイン CA から発行された S/MIME 用のパブリック証明書もあわせて格納する．非接触チップである FeliCa は，入退室管理や出欠管理等で利用する場合，一般にはメモリに専用アプリケーションを導入しておく必要がある．すなわち，カード設計時にアプリケーションを決定したうえでメモリ設計を行い，IC カード制作時にアプリケーションをあらかじめ導入しておかなければならない．そのため，新しいアプリケーションやシステム改変への対応が難しく，運用の柔軟性に欠ける．そこで，固有番号であるチップ製造番号 IDm を利用することを検討している．すなわち，メモリに専用アプリケーションを導入せず，システム側に IDm と個人を連携させるしくみを持たせ，運用の柔軟性を確保する．いわゆる TypeB 等，非接触チップの種類によっては，あとからアプリケーションを追加導入することも可能であるが，ユーザにアプリケーションをダウンロードさせること等により，トラブルのリスクが増えることから実際の運用を考えると望ましいとは考えていない．

これらの実装に従い，IC カードの運用を検討するため，トライアル IC カードを導入している．トライアル IC カードについては 5.4 節で述べる．

5. システムの運用状況

図 4 に 2007 年 5 月時点でのシステムの連携状況を示す．図中矢印は ID 同期のデータの流れを示し，実線は自動，点線は手動の連携を示す．公開セグメントに設置された Web サービスは SSO で連携している．KOAN の携帯電話サービス，C/S インタフェース，教育用計算機システム，無線 LAN 等が SSO に対応していない．これらのサービスで PKI を利用するためには，Smart Card ログオンのような PKI 対応を個別に実施する必要がある．現時点ではトライアル IC カードのユーザ以外は，パスワード認証を用いている．WebCT では WebCT サーバとは別に用意した認証用サーバに SSO エージェントを導入し，ユーザが認証用サーバにログインすると，CGI スクリプトが WebCT 独自の SSO プロトコルを用いて自動的に WebCT サーバにリダイレクトする実装とした．また，教員の業績を管理するシステムである教員基礎データシステムは近々システム更新を予定していたため，リバースプロキシ型で連携した．以下の節では，これまでの運用状況について述べる．

5.1 統一アカウントからの移行

ID を統一アカウントシステムで利用していた統一アカウントから大阪大学個人 ID に移行する際，教職員については学内便で新 ID を郵送できるが，学生は部局窓口で受け渡す必要があり，授業のない期間中に移行できない可能性がある．そのため，在学生については統一アカウントを阪大個人 ID として利用することにした．1 月から 3 月を移行期間とし，統一アカウントシステムから全学 IT 認証基盤システムにパスワードを移行した．統一アカウントシステムでは生パスワードを保存していなかったため，移行期間中に統一アカウントシステムでパスワードを変更させるシステムを用意し，変更後のパスワードを全学 IT 認証基盤システムに同期させた．パスワード移行期間中にパスワード変更しなかったユーザは，4 月の授業開始時に窓口に問合せに来させることとした．そのため，在

学生の ID を変更した場合に対してどの程度窓口業務が削減できたかは定かではないが，授業開始前の 3 月に KOAN で在学生の履修登録を実施し，ある程度の登録を完了できたことから，ID を継続利用しパスワードを移行した意味はあったと考えている．

5.2 SSO システムの運用状況

2007 年 1 月より SSO システムの KOAN 連携の運用を開始した．以下ではこれまでの運用状況について紹介する．

(1) Web ブラウザの PKI 対応

SSO サーバでは，公開鍵認証に対応するため，SSL のクライアント認証を要求しており，クライアントが証明書を提示しない場合，サーバ認証のみの SSL にフォールバックする設定を採用している．そのため，SSL のクライアント認証に対応していないブラウザでは，SSO のログインに失敗する問題が発生した．MacOS の 10.2 以前のバージョンで採用されていた Internet Explorer では，SSL のクライアント認証にまったく対応しておらず，認証ページ自体が表示されなかった．また，Safari では，クライアント証明書を選択する機能がないため，全学 IT 認証基盤システム以外から発行された証明書がインストールされたブラウザでは，認証の失敗が発生した．これらのケースでは他のブラウザの利用を推奨した．現時点での推奨環境は全学 IT 認証基盤サービスの FAQ[14] に記載している．上記以外にも，クライアント認証の要求により，証明書の有無にかかわらず Internet Explorer でダイアログが提示されること，Firefox で証明書の提示をうまくキャンセルできない等，PKI 周辺のブラウザの実装の問題が残されている．今後実装が改善されることに期待したい．

(2) SSO エージェントの通信エラーによる Internal Server Error

KOAN は 5 台の Web サーバで負荷分散しており，1 つのグローバル IP アドレスを共有している．通常の Web アクセスでは，Global から Private へのアクセスしか発生しないが，SSO エージェントから SSO サーバへの通信を行う際には，逆方向の通信が発生し，負荷分散装置（f5 networks BIG-IP: 以下 BIG-IP）がアドレス変換を行う．KOAN と SSO サーバのネットワーク接続を**図 5** に示す．ここで，BIG-IP のデフォルトの動作がアドレス変換（NAT）のみでポート変換（NAPT）は実施しない仕様となっている．また，Solaris では，クライアント側のポートは，デフォルトでは 32768 から昇順に利用される．そのため，**図 6** に示すようなセッションが発生した場合，次のような問題が発生する．

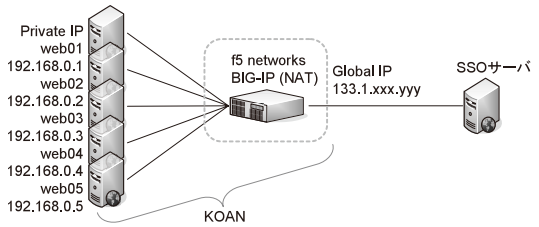


図 5 KOAN と SSO サーバ間の接続
Fig. 5 The connection between KOAN and SSO server.

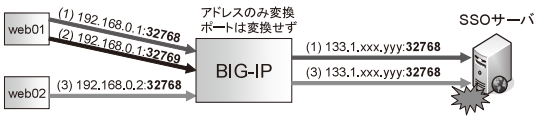


図 6 SSO エージェントの通信障害
Fig. 6 The communication failure of the SSO agent.

- (1) のセッションが終了していない段階で (3) のセッションが開始すると，BIG-IP 上で (3) はリセットされる．
- (1) のセッションが終了後，SSO サーバ側が TIME_WAIT の状態で (3) のセッションが開始すると，SSO サーバ上で (3) は破棄される．

以上のような原因により，SSO エージェントが Internal Server Error を出力していた．BIG-IP のファームウェアをバージョンアップし，NAPT の設定を投入することで，解決した．既存システムに SSO 機能を導入する場合，負荷分散装置における外向き通信には注意が必要である．

(3) SSO サーバの性能に関する考察

4 月 4 日から 6 日にかけて新入生による KOAN の履修登録が実施された．約 2,700 人の新入生を 6 つのグループに分け，各グループ約 1 時間ずつ，大学内の教育用計算機 500 台を使用して履修登録を実施した．さらに 6 日には，4 日の抽選登録の結果を確認するために，すべての新入生が抽選結果の参照を行った．これが現在までで最もアクセスが集中したケースであった．6 日のアクセス状況を**図 7**，**図 8** に示す．SSO サーバは Sun Fire V240（UltraSPARC IIIi × 2，Memory 8 GB，Sun Crypto Accelerator 500）が 2 台で，SSO エージェント側で利用するサーバを切り替えるホットスタンバイ構成である．図 7 は，SSO サーバの認証数と CPU 負荷の関係を示している．認証数が 350 で頭打ちになっているのは，KOAN 側の負荷分散装置で瞬間最大流量を 350 程度に絞っていたためである．このグラフより，認証数のピークよりも CPU 負荷のピークが後に来ていることが分かる．さらに SSO サーバ

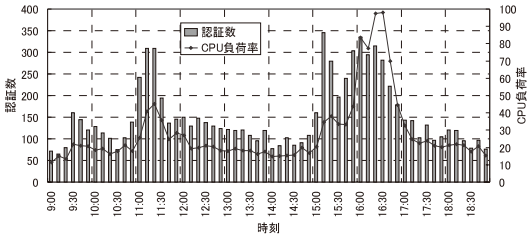


図 7 SSO サーバの認証数と CPU 負荷率
Fig. 7 The number of logins and CPU loads on SSO server.

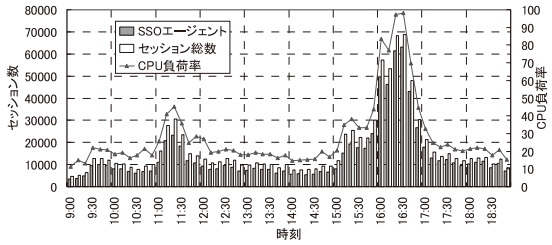


図 8 SSO サーバのセッション数と CPU 負荷率
Fig. 8 The number of sessions and CPU loads on SSO server.

の HTTP セッション数と CPU 負荷を比較した結果を図 8 に示す．このグラフよりセッション数と CPU 負荷に相関があることが分かる．また，ほとんどのセッションが SSO エージェントからの通信によって占められていることが分かる．SSO エージェントには，ログインしたユーザのセッション情報や属性情報をキャッシュする機能があるため，それほど頻繁に SSO サーバにアクセスする必要はない．実際に，J2EE 用の SSO エージェントでは，この例よりも SSO エージェントからの通信は少ない．

ここで，Apache 用の SSO エージェントは，HTTPD の子プロセスごとに別のプログラムが動作し，プログラム間でキャッシュを共有しない実装となっている．また，KOAN の Apache HTTPD は，プロセス起動のオーバヘッドを回避するため，サーバごとに 50 の子プロセスが起動される設定になっている．そのため，ロードバランサによって，同一セッションのユーザが同じサーバに振り分けられたとしても，処理に割り当てられるプロセスが異なると，キャッシュが機能せず，SSO サーバへのアクセスが発生する．その結果，ユーザから Web サーバへのアクセスが発生するたびに SSO サーバへのアクセスが発生していると考えられる．KOAN のプロセス数を減少させることである程度性能は改善されると考えられるが，KOAN 側の処理性能に影響が発生する可能性があるため，7 章で述べるテスト環境が整備でき次第，性能テストを実施する方向で検討中である．

図 9 トライアル IC カードと入退館管理システム
Fig. 9 Trial IC Card and entry control system.

5.3 ディレクトリ統合管理システムの運用状況

図 4 に示したように，端末ログイン認証のレポジトリは CMC ディレクトリ統合管理システムを経由して管理されている．IDM は，ID 同期処理の前後に外部システムを呼び出す機能を持たないため，ID 同期のタイミングで CMC ディレクトリ統合管理システムの同期処理を起動することができない．そのため，CMC ディレクトリ統合管理システムから各レポジトリへの同期処理は定期的に更新差分を確認して起動するしかない．現在 30 分ごとに差分確認処理を起動しているが，最悪パスワード変更が反映されるまで 1 時間程度かかることがある．システムの導入予算，納入業者の切り分けのため，このような構成をとらざるをえなかったが，可能であればディレクトリ統合管理システムは 1 つにするのが望ましい．

IDM の同期処理は夜間にバッチで実行しているが，3,000 件で同期に約 5 時間かかっている．同期先のレポジトリを 1 つ追加すると 1 件の ID 同期時間が約 1 秒程度増加する．現在想定される連携先にすべて IDM 同期を採用した場合，夜間に処理が完了しない可能性がある．IDM の処理自体は，各レポジトリの処理性能やストレージ性能等に依存するため，処理性能の向上にはコストがかかる．3,000 件以上の新規登録は年度末の登録処理等時期が限られているため，該当期間の日中の処理を制限する運用対処を検討している．

5.4 トライアル IC カードの運用状況

2007 年 1 月から IC カードのトライアル運用を行っている．**図 9** にトライアル IC カードの券面印字例を示す．職員証として利用することを想定し，公印の印字等について検討している．学内の 10 組織からトライアル参加の応募があり，約 250 枚のカードを発行している．トライアル IC カードのアプリケーションとしては，4.2 節で述べた SSO システムの認証，人事課におけるシンクライアントシステム[15] のログイン，入退室管理（図 9）等がある．

5.5 パブリック証明書の利用

S/MIME 用のパブリック証明書については，UPKI

プロジェクトで先行して試験運用を開始しており，UPKI の証明書で S/MIME のトライアル利用に参加している．UPKI の証明書の有効期限が切れ次第，順次全学 IT 認証基盤システムが発行する証明書に移行する予定である．S/MIME は，連携システム間で個人情報を手動連携する際の暗号化等に用いている．

パブリック証明書に関してこれまでに発生している問題としては，5.2 節で述べたようなブラウザの実装による問題，S/MIME に対応していないメーラで，メールが読めなくなるという問題が発生している．特に携帯電話においては，S/MIME 署名をつけたメールは本文ごと消失してしまうという問題が発生している．今後実装の改善を期待したい．

6. 既存システムとの比較

大学における全学認証基盤は，2000 年頃から各大学で整備されてきた[16]．大阪大学でも 2001 年度に 2.2 節で述べた統一アカウントシステムを導入している．これらの全学認証基盤の多くは，教育用の計算機システムやメールサービス等の学内サービスの利便性向上を目的として，ID・パスワードをベースとしたシステムとして導入された．LDAP またはメタディレクトリにより連携システムのパスワードを統一した場合，連携先の一部のシステムにセキュリティ上の問題が発生したとき，そこから個人情報が漏洩する可能性があり，システム全体のセキュリティレベルが，連携システムのセキュリティに依存する．また，パスワードは統一されていても，システムごとにログインを行う必要があり，必ずしもシームレスに連携システムを利用できない．本認証基盤システムは，PKI およびシングルサインオンを導入することで連携システムへのセキュリティ面での依存を解消し，また，1 度認証すれば，学内システムを認証なしで利用できる点が，LDAP やメタディレクトリによる認証基盤との相違点である．

名古屋大学では，Yale 大学で開発され，JA-SIG が開発を継続している CAS（Central Authentication Service）[17] を先行導入し，学内 Web サービスのシングルサインオンを実現している[18]．しかし，名古屋大学では学内システム向けの PKI の導入を検討し始めたところであり，本認証基盤システムが提供するセキュリティレベルには達していない．また，本稿執筆時点では，CAS は SAML 等の組織間連係のための標準に対応しておらず，同大学の認証基盤は組織間連携の実現が難しい．一方，本認証基盤システムは，SAML ベースの SSO 機能を持つため，将来的な標準化技術への対応が比較的容易である．

東京工業大学では，SAML2.0 ベースのシングルサインオンシステムを導入しており，マトリックスコードの採用により安価でセキュアな認証基盤を構築している[19]．東京工業大学で導入されたシステムは Entrust 社の商用製品であるため，同大学で蓄積されたノウハウは同製品を導入しなければ共有できない．一方，本学のシステムはオープンソースプロジェクトである OpenSSO [13] からほぼ同等のソフトウェアが提供されているため，本学で蓄積したノウハウは，他大学において低コストでシングルサインオンを導入する際にも生かせると考える．

東京工業大学の認証基盤は，本認証基盤システムと同様，PKI に対応している．東京工業大学以外にも東京大学，名古屋工業大学，徳島大学，文部科学省等で PKI 対応したシステムの導入が進められている．しかし，これらはいずれもクローズドドメインの認証局である．これに対し本認証基盤システムでは，3.1 節で述べたようにオープンドメイン認証局も同時に提供しており，クローズドドメイン認証局間の連携構築を待たなくても，他大学や他組織のユーザと S/MIME によるメール交換が可能である．本学のような大規模な総合大学では，部局ごとにメールサーバ等の情報システムの運用が独立しているケースが多く，メールアドレスをユーザが設定可能な本学の認証局構築方式は他大学においても参考になると考える．

一方，海外の大学においても，出版社等の学外サービスとの連携，大学間の e-Learning の相互連携等が始まっており[20]，大学の情報サービス向上が進められている．また，グリッドの分野でも米国，欧州，アジア各地域においてサービス連携が始まっている[6]．組織間のサービス連携においても，PKI およびシングルサインオン技術が導入されている．

これら海外で導入されている SSO システムは，ほとんどがパスワードベースで運用されている．また，PKI は，運用コストやユーザの利便性を考慮して，Short-Lived Credential Service Profile 等の低いセキュリティレベルで運用されることが多い．これらに対し本認証基盤システムでは，3.2 節で述べたように，SSO とセキュリティを考慮した PKI を併用することで，PKI による高いセキュリティレベルを持つアプリケーションとそうでないアプリケーションを併存可能とする柔軟な実装となっている点が異なる．

7. 今後の課題

本章では，今後システムの検証や開発が必要となる

課題について述べる．

7.1 SSO システムおよびディレクトリ統合管理システムの課題

SSO システムおよびディレクトリ統合管理システムの課題を以下に示す．

(1) テスト環境の整備

これまでの運用では，5.2，5.3 節で述べたとおり，連携構築時に本番環境と同じネットワーク環境においてテストを実施できなかったために発生したトラブルが多い．SSO 連携，IDM 連携ともにネットワーク環境の変更による影響を大きく受けるため，本番環境と同じネットワーク環境で負荷テストも含めて接続テストを実施できるテスト環境の整備が必須であると考えている．

(2) 大学間認証連携の構築

WebCT をはじめとするアプリケーションの大学間の相互連携を視野に，SAML2.0 を用いた大学間連携についても検討する必要がある．すでにグリッド分野では PKI による相互連携が開始されているが，2.1 節で述べたように，異なる保証レベルを持つ CA が存在することや，パスワード認証のような異なる認証方式を採用している大学も存在することから，認証連携は SSO で実現し，認可ポリシの擦り合わせは個々のアプリケーション間で実現する方法も考えられる．

SAML2.0 は ID 変換をサポートしており，各大学が独自の ID 空間を利用していても連携が可能である．しかし，各アプリケーションでの実装上の制約やユーザからみた ID 識別の容易性等を考慮し，連携構築を容易にするためには，Internet2 の MACE-Dir Working Group [21] が定義している eduPersonPrincipalName のようなグローバルな ID 定義も含めて，今後大学間で検討していく必要がある．

(3) SSO 未対応システムの ID 連携

現在，SSO に対応していない端末ログインや無線 LAN 等のシステムは，ディレクトリ統合管理システムから，認証情報を同期することで ID 連携を実現している．しかし，他大学からのゲストが一部のシステムを利用する場合や，部局の小規模システムにおいて，学内ユーザのうち，一部のユーザのみ利用する場合等，ID を同期させるシステムやユーザを抽出するために，付加的な属性を管理する必要がある．このような連携を容易にするために，SSO に対応していないシステム用に，SSO で認証を実施する ID 登録 Web アプリケーションを用意している大学もある．学内システムの ID 統合，大学間連携を進めるうえで，SSO 未対応なシステムも含めた ID 連携について，今後引き続き検討していく必要がある．

7.2 キャンパス PKI の課題

事務情報システムの電子化の一環として，会計処理の電子化があげられる．現在紙と印鑑による決済を行っているが，S/MIME によるディジタル署名を利用することで，電子決済に置き換えられる可能性がある．しかし，現状のグループウェアアプリケーションの多くは Web アプリケーションとして構築されており，手元にある IC カードで署名する機構が実現されていない．同じ問題は Web メールにおける S/MIME 利用でも発生する．サーバ側に鍵ペアを置いて S/MIME を利用する Web メールシステムは存在するが，IC カードでの利用を想定したものがない．このような Web アプリケーション向けの PKI（IC カード）アプリケーション基盤を構築する必要がある．また，書類の決裁にディジタル署名を採用した場合，長期文書保存の問題が発生する．長期文書保存の標準化動向も含めて，検討していく必要がある．

7.3 属性情報管理の課題

4.3 節で述べたとおり，全学 IT 認証基盤システムでは，教職員の属性情報は人事給与システムから取得している．しかし，大阪大学の人事給与システムが保持している所属は本人の正式な所属ではなく，人事上のポストを提供した所属が記録される．たとえば，複数の部局が共同で設立した新部局のポストの場合，新部局にポストを提供した部局名が記録されることがある．人事課では辞令の発行履歴は管理しているが，教職員番号に結び付けて記録しておらず，辞令から最新の所属を取得することはできない．そのため，全学 IT 認証基盤システムが提供する所属は，公開情報や認可決定に用いると問題が発生する．現在教職員の所属を収集しているのは職員録を作成している総務部総務課だけであり，職員録はシステム化されていない．今後認可決定や初期データ登録のコストを削減するためには，新たに全学 IT 認証基盤システムと連携して所属を管理するデータベースを作成し，データ連携を構築する必要がある．また，その際 eduPerson [21] や FCF [22] のような標準的な属性定義についても検討する必要がある．

大学においては，教授の業務を秘書が代理で実施することが多い．しかし，現状のアプリケーションでは，本人による処理しか受け付けておらず，秘書が代理入力等を行う場合，パスワードや IC カードの委譲等，本来の本人認証機能を損なう運用が行われる可能性が高い．そのため，今後本人が適切に IC カードを利用しながら権限委譲を実現する仕組みを検討していく必

要がある．

8. おわりに

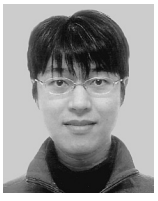
本稿では，大阪大学で導入した全学 IT 認証基盤システムの構成，システムの運用状況，今後の課題について述べた．学内システムの利便性の向上と他大学との連携構築のために，SAML 連携や属性情報の管理等について引き続き検討することで，学術情報分野のインフラ構築に貢献したいと考えている．

謝辞 全学 IT 認証基盤システム構築の一部は，国立情報学研究所委託事業「最先端学術情報基盤の構築に関する研究開発と調査」の一環として行われた成果である．

参考文献

1) 岡村真吾，寺西裕一，秋山豊和，馬場健一，中野博隆：大阪大学におけるキャンパス PKI の構築，情報処理学会研究報告，第 32 回コンピュータセキュリティ研究会（CSEC）2005-CSEC-32, pp.67–72 (2005).
2) Akiyama, T., Teranishi, Y., Okamura, S., Sakane, E., Hasegawa, G., Baba, K., Nakano, H. and Shimojo, S.: A Report of Campus-wide IT Authentication Platform System Developement in Osaka University, *Proc. SAINT2007 Workshop*, Hiroshima (Jan. 2007).
3) 島岡政基，谷本茂明，片岡俊幸，峯尾真一，曽根原登，寺西裕一，飯田勝吉，岡部寿男：大学間連携のための全国共同電子認証基盤 UPKI における認証連携方式の検討，信学技報，Vol.106, No.62, IA2006-3, pp.13–18 (2006).
4) UPKI イニシアティブ. https://upki-portal.nii.ac.jp/
5) 坂根栄作，東田 学，岡村真吾，寺西裕一，秋山豊和，馬場健一，下條真司：全国共同利用環境へのグリッドミドルウェアの適用，情報処理学会研究報告（IPSJ SIG Technical Reports），2007-DSM-45, pp.25–30 (May 2007).
6) International Grid Trust Federation (IGTF). http://www.gridpma.org/
7) AICPA, WebTrust Program for Certification Authorities. http://www.webtrust.org/
8) OASIS Security Services (SAML) TC. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
9) 東芝ソリューション株式会社製 Targusys. http://www.toshiba-sol.co.jp/nsd/sec/p005.htm
10) NAREGI (National Research Grid Initiative) CA Package. http://www.naregi.org/download/index.html#capkg
11) サン・マイクロシステムズ社製 Sun Java System. http://jp.sun.com/products/software/javasystem/
12) Liberty Alliance ID-FF 1.2 Specifications, Liberty ID-FF Architecture Overview. http://www.projectliberty.org/liberty/content/download/318/2366/file/draftliberty-idff-arch-overview-1.2-errata-v1.0.pdf
13) OpenSSO Project. https://opensso.dev.java.net/
14) 大阪大学全学 IT 認証基盤サービスよくあるご質問（FAQ）ブラウザ対応状況. http://repository.cmc.osaka-u.ac.jp/ja/faq.html#6
15) プレスリリース “大阪大学が事務用端末として Sun Ray シンクライアントを採用.” http://jp.sun.com/company/Press/release/2007/0312.html
16) 日本の大学における全学認証基盤の整備状況. http://repository.cmc.osaka-u.ac.jp/ja/other_auth_services.html
17) JA-SIG Central Authentication Service. http://www.ja-sig.org/products/cas/
18) 梶田将司：CAS によるセキュアな全学認証基盤による名古屋大学ポータルの運用，第 3 回日本 WebCT ユーザカンファレンス (June 2005). http://www.webct.jp/c2005/proc/p5_kajita_doc.pdf
19) 飯田，勝吉：キャンパス共通認証・認可システムが拓く高度な研究・教育のための情報通信基盤，情報処理学会研究報告，QAI，Vol.2006, No.109, pp.13–18 (2006). http://ci.nii.ac.jp/naid/110004837945/
20) Internet2 Middleware Architecture Committee for Education (MACE) Shibboleth Project Community. http://shibboleth.internet2.edu/community.html
21) Internet2 Middleware Architecture Committee for Education (MACE) Directory Working Group. http://middleware.internet2.edu/dir/
22) FeliCa 共通利用フォーマット（FCF）推進フォーラム．http://www.fcf.jp/

(平成 19 年 6 月 11 日受付)
(平成 19 年 12 月 4 日採録)



秋山 豊和（正会員）

平成 11 年大阪大学大学院工学研究科修士課程修了．平成 12 年同大学院博士課程中退後，同大学サイバーメディアセンター助手を経て，平成 17 年 1 月より同センター講師．キャンパス情報システム，ソフトウェアフレームワーク等に興味を持つ．博士（工学）（平成 15 年 9 月，大阪大学）．電子情報通信学会，IEEE CS 各会員．

寺西 裕一（正会員）

平成 7 年 3 月大阪大学大学院基礎工学研究科物理系専攻情報工学分野博士前期課程修了．平成 7 年 4 月日本電信電話株式会社入社，同情報通信研究所勤務．平成 14 年西日本電信電話株式会社研究開発センター勤務．平成 16 年 4 月同主査．平成 17 年 1 月大阪大学サイバーメディアセンター応用情報システム研究部門講師，平成 19 年 11 月大阪大学大学院情報科学研究科准教授，現在に至る．ユビキタスコンピューティング，P2P 技術に関する研究開発に従事．博士（工学）（平成 16 年 3 月，大阪大学）．

岡村 真吾（正会員）

平成 17 年 3 月大阪大学大学院情報科学研究科マルチメディア工学専攻博士後期課程修了．博士（情報科学）．平成 17 年 4 月大阪大学サイバーメディアセンター特任助手，平成 19 年 4 月より同特任助教．情報セキュリティ分野，特に暗号プロトコルや認証技術に関する研究を行う．電子情報通信学会，電気学会，ACM，IEEE 各会員．

坂根 栄作（正会員）

平成 12 年 3 月大阪市立大学大学院理学研究科物理学専攻後期博士課程単位修得退学．博士（理学）．平成 18 年 1 月大阪大学サイバーメディアセンター特任助手，平成 19 年 4 月より同特任助教．グリッドコンピューティング，主に運用管理技術に関する研究を行う．日本物理学会，電子情報通信学会各会員．

長谷川 剛

平成 7 年大阪大学基礎工学部情報工学科退学．平成 9 年同大学大学院修士課程修了．平成 9 年同大学院博士後期課程退学．平成 12 年博士（工学）（大阪大学）取得．平成 9 年同大学経済学部助手．平成 12 年同大学サイバーメディアセンター助手．平成 14 年同大学サイバーメディアセンター准教授，現在に至る．トランスポートアーキテクチャ，オーバレイネットワーク，ネットワーク計測技術等に関する研究に従事．IEEE 会員．

馬場 健一

平成 2 年 3 月大阪大学基礎工学部情報工学科卒業．平成 4 年 3 月同大学大学院基礎工学研究科物理系専攻情報工学分野博士前期課程修了．平成 4 年 4 月同大学院博士後期課程に進学し，同年 9 月同大学院退学．同年 10 月大阪大学情報処理教育センター助手として採用，平成 9 年 4 月高知工科大学工学部電子・光システム工学科講師，平成 10 年 12 月大阪大学大型計算機センター助教授，平成 12 年 4 月同大学サイバーメディアセンター助教授，平成 19 年 4 月より准教授として勤務．現在に至るまで広帯域ネットワーク，コンピュータネットワーク，フォトニックネットワークシステムの性能評価に関する研究に従事．電子情報通信学会，IEEE 各会員．

中野 博隆

昭和 47 年東京大学工学部電気工学科卒業．昭和 52 年同大学大学院博士課程修了．工学博士．同年日本電信電話公社（現 NTT）武蔵野通研入所．以来，画像システムの研究開発に従事．平成 11 年 NTT 移動通信網株式会社（現，NTT ドコモ）マルチメディア研究所所長．平成 16 年大阪大学サイバーメディアセンター教授．ユビキタス環境中におけるネットワーク基盤の研究に従事．

下條 真司（正会員）

昭和 61 年 3 月大阪大学大学院基礎工学研究科後期課程修了．昭和 61 年 4 月大阪大学基礎工学部助手．平成元年 2 月同大学大型計算機センター講師．平成 3 年 4 月同センター助教授．この間米国カリフォルニア大学アーバイン校客員研究員．平成 10 年 4 月大阪大学大型計算機センター教授．平成 12 年 4 月同大学サイバーメディアセンター教授・副センター長．平成 17 年 8 月大阪大学サイバーメディアセンター教授・センター長．平成 18 年 8 月大阪大学サイバーメディアセンター教授・副センター長，現在に至る．マルチメディア応用システム，peer-to-peer コミュニケーションネットワーク，ユビキタスネットワークシステム，グリッド技術等の研究に従事．工学博士．志田林三郎賞，日本医用画像工学会論文賞，大阪科学賞受賞．日本学術振興会インターネット技術第 163 委員会委員長．電子情報通信学会，IEEE CS，ACM 各会員．

長岡　亨

昭和63年4月日本電信電話株式会社入社（研究開発部），平成9年10月NTTコムウェア株式会社（研究開発部），平成16年10月西日本電信電話株式会社に転籍．平成18年10月大阪大学テクニカルスタッフ情報基盤デザイン機構特認教授，現在に至るまでに，汎用並列コンピュータOLTPの実用化研究，AJC（Authorized Java Center）日本センター立ち上げ，モバイルエージェントによるテレマティクス実用化研究，プローブデータ解析技術の研究等に従事．