社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－DPS－126（12）
2006－CSEC－32（12）
2006／3／16

大阪大学におけるキャンパス PKI の構築

岡村真吾　寺西裕一　秋山豊和　馬場健一　中野博隆

大阪大学サイバーメディアセンター
{okamura, teranisi, akiyama, baba, nakano}@cmc.osaka-u.ac.jp

大阪大学では、多くの学内システムを統合的かつ安全に機能させるため、全学にわたる公開鍵認証基盤（キャンパス PKI）を構築する計画を進めている。公開鍵暗号を用いた認証を行なうことで、パスワードによる認証において問題となるパスワード解読の脅威に対する耐性を高めることができる。キャンパス PKI を構築するにあたり、ユーザ公開鍵・秘密鍵の管理方法や認証局の運用形態といった PKI の運用方法や、Web シングルサインオンや計算機ログイン認証といった PKI を利用したアプリケーションについての検討を行った。本稿では、それらの検討内容や構築中のキャンパス PKI の構成について述べる。

Campus PKI in Osaka University

Shingo OKAMURA, Yuuichi TERANISHI, Toyokazu AKIYAMA,
Ken-ichi BABA, and Hirotaka NAKANO

Cybermedia Center, Osaka University

In Osaka University, a campus-wide authentication infrastructure based on public keys, called Campus PKI, is being constructed to make computer systems more secure. A public key authentication is more secure against password cracking than a password authentication. At the constructing of the Campus PKI, some issues of operations and applications of the Campus PKI are discussed. In this paper, the discussions are described and the configuration of the Campus PKI is shown.

1. はじめに

近年の業務システム等のオンライン化にともない、システムの複雑化、セキュリティに対する懸念が問題となっている。大阪大学においても、学務情報システム、経理システムといった業務システムのオンライン化が予定されており、シンプルかつ安全なシステム化が要求されている。こうしたオンラインサービスにおいては、個人認証が必須となる。特に、学務情報システム等では、成績などの各個人の機密に関わる情報を扱わねばならないため、本人性を高いセキュリティのもと確認できる仕組みが必要となる。しかし、従来の ID・パスワードによる認証方法は、盗聴、解読による脅威に十分な耐性があるとはいい難い。また、従来の ID・パスワードによる認証では、個人がそれぞれのシステムに対応した ID や複雑なパスワードの管理を記憶に頼って行なわねばならない。通常、解読防止のために、定期的にパスワードを更新する対処が行なわれるが、多数のシステムを使い分けることは困難である。

そこで、これらの問題を解決するために、大阪大学では、PKI による学内統合認証基盤（キャンパス PKI）の構築を検討している。PKI で公開鍵暗号を用いた認証を行なうことで、パスワードによる認証において問題となるパスワード解読の脅威に対する耐性を高めることができる。また、PKI は Web におけるサーバ・クライアント間の通信の暗号化、サーバ認証の枠組みとしても採用されており、Web ベースのアプリケーションとの親和性も高い。さらに、メール暗号化・電子署名(S/MIME[1])、無線 LAN 認証といったさまざまなアプリケーションにおいても PKI は用いられており、応用範囲が広い。

本稿では、大阪大学におけるキャンパス PKI の整備に向けた検討状況について報告する。以下、キャンパス PKI の構築にあたっての検討内容と構築中のシステム構成について述べる。

2. キャンパス PKI の検討

2.1. ユーザ公開鍵、秘密鍵の管理

PKI 認証環境を実現する上では、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。本認証基盤では、専用デバイスに格納する方法を採用することとした。デバイスを用いて秘密鍵の生成、電子署名等を実行することで、外部に秘密鍵を取り出すことなく運用することが可能となる。また、万一盗難にあったとしても、デバイス自体が耐タンパ性を持ち、読み出すことが物理的にできないようになっており、かつ、PIN によるアクセス制御も行なわれるため、安全度は高い。専用デバイスとしては、現在 IC カード、USB キーという選択肢が取り得る。本認証基盤では、

・身分証明書を兼ねることができる
・非接触のインタフェースを共存させることで電子マネーなどにも利用できる

などの利点から IC カードを選択した。

非接触アプリケーションと、PKI 認証との双方を IC カードにおいて用いて実現する方法として、次の 3 つの形態が考えられる。

① 接触・非接触で別々のカードを用いる
② ハイブリッドカードを用いる（図 1）
③ デュアルカードを用いる（図 2）

①は実現が最も容易であるが、ユーザに複数枚のカード管理を強いることとなり、利便性が低い。②は 1 枚のカードの上に接触・非接触の機能が独立して共存する形態であり、③は共通のカード上の機能を接触・非接触のインタフェースを通じて利用する形態である。これらは①の問題である複数枚のカード管理の手間を避けることができる。うち、③は、現状では Windows OS 以外の OS では利用できないものがほとんどである。一方②の方法は、Windows 以外の OS での運用実績があるものが存在するが、一つのカードに複数の記憶領域へのインタフェースが共存するかたちとなり、カードの単価が高価となる可能性がある。したがって、利用 OS や、コストに応じてどの形態

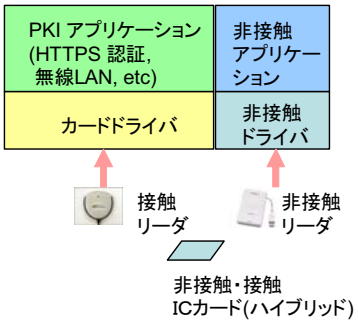

図 1 ハイブリッドカードを用いる形態

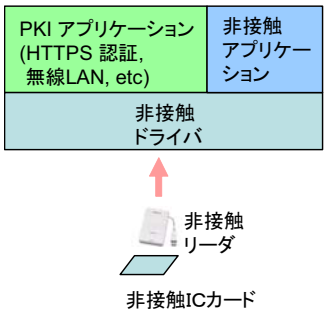

図 2 デュアルカードを用いる形態

を利用するかを選択する必要がある。

2.2. 認証局の運用形態

認証局(CA: Certificate Authority)の機能は、登録局(RA: Registration Authority)の機能と発行局(IA: Issuing Authority)の機能に分けられる。ユーザ証明書を発行する認証局の運用方法として、次の 3 つが挙げられる。

① 第三者機関に RA および IA の全運用を委ねる
② 組織内にて RA を運用し、IA の運用を第三者機関に依頼する（図 3）
③ 組織内で RA および IA を運用する

①は第三者機関に証明書を発行してもらうため、大学には CA が存在しない、即ち、本人確認を第三者機関に委ねることとなる。②③は大学において本人確認を実施する。ユーザ証明書は、大学としてユーザが大学の一員であることを証明するものであるため、大学が本人確認を行なう必要がある。よって、②③のように大学内で RA を運用する必要がある。

また、CA の運用形態をパブリック CA とするかプライベート CA とするかについても選択しなければならない。ここで言うパブリック

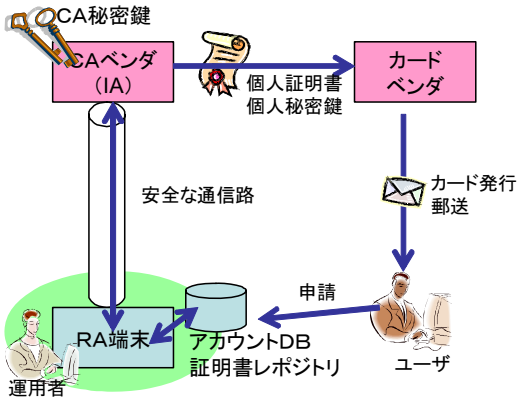

図 3　IA の運用を第三者機関に委託

CA とは、一般的な Web ブラウザや PC に承認済みルート証明書として証明書が埋め込まれた CA もしくはその子 CA を指す。

キャンパス内のシステムにおいてユーザ認証を行なう上では、必ずしもパブリック CA が発行したユーザ証明書を用いる必要はない。ユーザ証明書を発行したプライベート CA の証明書を、ユーザ認証を行うシステムに対して正しく配布できれば、その証明書を用いてユーザ証明書を検証できる。ただし、証明書を正しく配布するには、配布元と配布先の間で決められた手順で正確に運用がなされねばならない。

一方、ユーザ証明書を S/MIME[1]の公開鍵証明書として用いる上では、プライベート CA では不十分となる。プライベート CA から発行されたユーザ証明書の場合、このプライベート CA の証明書を承認済みルート証明書として認識できているユーザ間でしか、安全に電子署名や暗号化が施されたメールのやりとりを行なえない。キャンパス内でのみメールをやりとりするのであれば問題ないが、他大学、個人、企業とやりとりするメールにおいて S/MIME を利用できないのではその意義が薄れる。よって、S/MIME ではパブリック CA が発行した証明書を用いることが望ましい。

したがって、本認証基盤では少なくとも S/MIME の証明書はパブリック CA の形態でユーザへ発行、ユーザ認証用の証明書はパブリック CA もしくはプライベート CA の形態で発行することを目指す。ポリシーをあわせることができれば、S/MIME 証明書とユーザ認証の証明書は同一のものとしたい。

運用の方法としては、③を採用すると IA の運用も含め学内で行なわなければならないが、パブリック CA の IA の運用には WebTrust for CA 認定[2]が要求されるため、莫大なコストと設備が必要となり、かつ手続きに長大な期間がかかる。したがって、本認証基盤では②の IA の運用を第三者機関に依頼する方法を採用することとする。

2.3.　Web シングルサインオンの実現

キャンパス内の情報システムは Web ブラウザをクライアントとして用いたアプリケーションが主流である。通常、大学においては各部局が必要に応じて独自のシステムを構築するため、それぞれ独自の方式、ID、パスワードで認証が行われてきた。大阪大学では、これを改善し、利用者がシステム毎に異なる ID・パスワードで認証を行なわずとも、統一的な ID・パスワードを用いて認証を行なえるよう、統一アカウント、認証連携の仕組みを整備してきた。本認証基盤では、この枠組みをさらに進めたシングルサインオンを、PKI によるユーザ認証を含め実現する。

2.3.1.　認証プロセスの簡略化

キャンパス内の情報システム全てを PKI 認証対応に改造すれば、パスワードをシステム毎に入力する手間を解消できる[1]。しかし、PKI 認証は複雑な処理であるため、キャンパス内の情報システムを渡り歩く過程で、各システムで毎回認証処理を行なっていてはブラウジングに時間がかかってしまう。

本認証基盤では、Web サーバに対するアクセスは、いったん認証サーバへリダイレクトさせて認証サーバで PKI 認証を行ない、その認証結果を各 Web サーバへ再リダイレクトして引き継ぐ形態のシングルサインオンを実現する。認証サーバにおいて一定時間 PKI 認証の状態を記録しておくセッション Cookie を発行すれば、PKI 認証をサーバ毎に行なうオーバヘッドを軽減することができる。認証サーバへリクエストをリダイレクトさせ、認証結果を引き継ぐ仕組みを実現するため、各 Web サーバ

[1] デバイスを用いた PKI 認証には PIN 入力が必要であるが、IC カードの PIN はキャッシュされるため、毎回入力する必要はない。

に専用のエージェント(プラグイン)を設置する。このエージェントがリダイレクト、認証処理の引き継ぎなどを受け持ち、各アプリケーションでは、それらの処理を意識せずに済むようにする。

2.3.2. 本人性保証レベルに基づく認証

システムによっては、キャンパス内のユーザだけでなく、海外の元留学生などの IC カードを配布することが困難なユーザが含まれる場合がある。このようなシステムでは ID・パスワードによる認証を認めざるを得ない。ID・パスワードによる認証と、IC カードを用いた PKI 認証を行なう場合では、なりすましの脅威への耐性が違うため、本人性の保証レベルが異なる。

そこで本認証基盤では、シングルサインオンを導入する際、各アプリケーションはどれだけの本人性の保証レベルを求めるかというポリシーを決め、それを満たさなければ認可しない、といった設定を可能とする。これにより、ID・パスワードと PKI 認証とを共存させ、かつそれら認証処理の違いを各アプリケーションから隠蔽することができる。また、新たな認証方式が追加された場合も、各アプリケーションは直接対応せずとも、その認証方式に対応することが可能となる。

2.3.3. 属性による認可

業務システムによっては、職種(教員、職員、学生等)、役職、所属といったユーザの属性に応じて、アクセスの認可を与えるか否かを変更しなければならない場合がある。例えば、教員には、成績データベースへのアクセスを許可するが、学生にはアクセスを許可すべきではない。最も単純な属性管理法として、ユーザ証明書に各属性を埋め込む方法が考えられる。しかし、この方法では、職員の異動や学生の所属変更などにより証明書更新が発生してしまう。また、ID・パスワードによる認証には対応できない。

そこで、本認証基盤においては、ユーザ証明書には最低限の属性のみを保持し、ほとんどの属性は、LDAP によるディレクトリサービスにおいて管理を行なうこととする。属性を得るには、ユーザ証明書の ID 属性（CN 属性など）をキーとして、ディレクトリサーバに対して属性の検索を行なえばよい。このとき、ユーザ証明書の ID 属性と、ID・パスワード認証における ID とは一致させておく必要がある。属性の取得は、前記各 Web サーバに設置するエージェントが行って、HTTP リクエストヘッダ等を通じてアプリケーションへ引き渡す。

2.3.4. 各 Web アプリケーションの対応

Web アプリケーションをシングルサインオン対応とするには、各 Web アプリケーションの改造が必要となる。必要な改造の度合いは、アプリケーションがユーザ毎に独自の属性を保持する必要があるか否かによって異なる。

アプリケーションがユーザ毎に独自の属性を保持することがない場合は、単純にシングルサインオンエージェントを Web サーバに組み込むのみでよい。各アプリケーションはエージェントで認証され、認可ポリシーを満たしているかどうかのみをチェックする。例えば、学生と教員でそれぞれ異なるアクセス制限を設けるなど、ユーザの属性に応じてアプリケーションの動作を変える必要があれば、エージェントが LDAP 経由で得るユーザ属性を HTTP ヘッダ経由で取得する設定を行い、アプリケーションの動作を変更すればよい。

一方、アプリケーションがシングルサインオンのエージェントから得られる属性以外に独自の属性を管理する必要がある場合（例えば、e-Learning システムにおける各ユーザの受講状態や成績など）、ユーザ属性管理のためのレポジトリをアプリケーション内に持つ必要がある。このユーザ属性レポジトリを、マスターとなる LDAP レポジトリに同期させるための手法として、次の 2 種類が考えられる。

① 認証時に同期
② 更新時に同期

①は、シングルサインオンで認証が成功した際、認証された ID に対応するユーザをユーザ属性レポジトリに追加する方法である。例えば、ID1000 の阪大太郎という名前を持つユーザが、初めてシングルサインオンのエージェントで認証されたとき、アプリケーションのレポジトリに「ユーザ ID：1000、名前：阪大太郎」というユーザエントリが追加される。2 回目以降、このユーザが認証に成功したとき、認証されたユーザ ID1000 を基にユーザ属性レポジトリを検索して得られるユーザエントリを用いる。

この方法では、マスターとなる LDAP レポジトリのユーザエントリが削除されたとしても、アプリケーション側でそれを認識することができない。したがって、頻繁にユーザエントリが削除される場合には、アプリケーションのレポジトリとマスターとなる LDAP レポジトリを比較し、マスターにないエントリを削除するガベージコレクションを一定期間おきに行う等の対処が必要となる。

②は、LDAP レポジトリが更新されるたびにアプリケーションのレポジトリを反映させる方法である。この方法は、①の方法と異なり、ユーザエントリの削除についても反映することができる。しかし、LDAP のエントリが変更されるたびに、ユーザ属性レポジトリのエントリも更新しなければならないため、頻繁に更新される場合や、アプリケーションが大量にある場合に、更新のオーバヘッドが大きくなる問題がある。また、アプリケーション側で全ユーザの数をカウントする必要がある場合や、ログインしたことがないユーザについても情報を得なければならない場合には、この方法を取らざるを得ない。

本認証基盤では、アプリケーションに応じて①、②のいずれの方法を取るかを選択することとする。現在のところ、e-Learning システムのようなユーザ申請型のアプリケーションは①の形態、教員データベースのように、ユーザの情報を強制的に登録する必要があるアプリケーションは②の形態といった使い分けとなるのではないかと考えている。

2.4. 計算機ログインの統合

学内の計算機ログインを本認証基盤の IC カードを用いて統合的に行える仕組みは、Windows におけるスマートカードログオンの仕組みや Linux における PAM モジュールとスマートカードを用いた PKI 認証の仕組みを用いることで実現する予定であるが、当面は、ID・パスワードによるログイン認証は継続する。リモートログインについては、PKI 対応の SSH を用いるなどの方策も考えられるが、まずは VPN のレベルで PKI に基づくユーザ認証を実施し、その後計算機へは ID・パスワードによりログインすることで対応することを考えている。

3. キャンパス PKI の構築

以上の検討を基に、現在大阪大学では全学 IT 認証基盤システムという名称でキャンパス PKI の構築を進めている（図 4）。システムは、主に CA システム、RA システム、シングルサインオンシステム、ディレクトリ統合管理システム、管理・監視システムから構成される。以下に、それぞれのシステムの概要を示す。

3.1. CA システム

CA システムでは電子証明書の発行及び失効を行う。本認証基盤では、CA システム（IA）は第三者機関に委託する前提であるため、システムとしてはホスティングの形態で構築することとなる。CA が行う主な業務内容は、次に示すものである。

・教職員用電子証明書発行、失効
・学生用電子証明書発行、失効
・内部サーバ用電子証明書発行、失効
・電子証明書失効情報等の情報開示
・CP/CPS 及びサービス内容などの情報開示
・IC カード発行ベンダと連携したカード発行

本格運用のためには、CA と連携して IC カード発行を行うための方法を検討する必要がある。大量に IC カードを発行する場合は、外部の発行ベンダに委託する必要があるが、利用者が IC カードを紛失した場合であっても即日

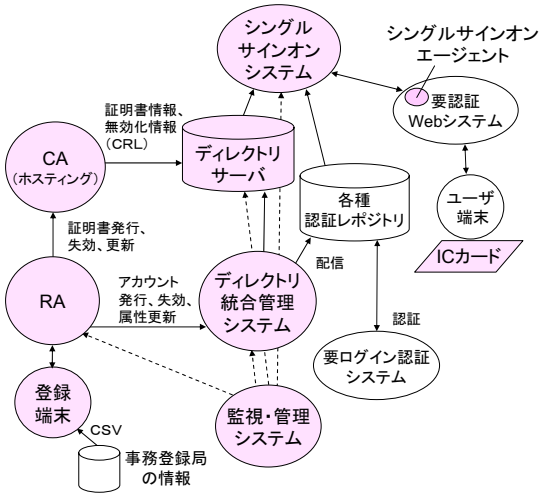

図 4　全学 IT 認証基盤システムの構成

再発行が可能となるよう、大学内で IC カードを発行できる方法も用意する予定である。

3.2. RA システム

RA では、CA のフロントエンドとして、CA と連携したユーザや証明書の登録、管理を行うユーザインタフェースを提供する。RA が持つ主な機能は、次の通りである。

・ユーザの登録、削除
・CA への証明書の発行要求、失効要求の発行
・ユーザの属性変更

個別に IC カード再発行などの対応を行う際、本人確認は RA を操作する職員が行う。初期発行時は、事務登録局（学生の場合は、学務情報システム、職員の場合は、人事給与システム）からエントリとして追加すべきユーザの情報が CSV 形式で得られる。本認証基盤では、この情報が得られた時点で証明書を発行する。発行された証明書が正しく本人に渡るよう、IC カード配布時の運用は慎重に行う必要がある。

3.3. シングルサインオンシステム

認証連携する全学サービス（Web アプリケーション）に対して、ID・パスワードおよび PKI によるシングルサインオン機能を提供する。大阪大学では現在いくつかの学内システムで統一アカウントによる認証連携機能が実現されており、それらを本認証基盤のシングルサインオンに対応できるよう改造する必要がある。ただし、Web サーバに組み込まれるシングルサインオンのエージェントがほとんどの処理を行うため、改造の規模はそれほど大きくはならないものと考えている。また、計算機ログインについては、ID・パスワードによる認証を行うため、ディレクトリ統合管理システムを用いてパスワード配信を行う。

3.4. ディレクトリ統合管理システム

ディレクトリ統合管理システムは、シングルサインオンのためのユーザエントリの更新時同期を実現する。また、計算機ログインのためのパスワード配信も実施する。

当面対象としている Web アプリケーションとしては、教員基礎 DB（大学内教員の業績等を管理、公開するためのシステム）[3]、学務情報システム（学生の履修登録、教員によるシラバス登録、成績登録など、講義に関連する業務を支援するためのシステム）や図書館 DB（利用者に文献データベースを提供するシステム）などが挙げられる。うち、図書館 DB は、学外の文献データベースシステムを利用するシステムであるため、それらの文献データベースをシングルサインオン対応に改造することは不可能となっている。よって、学内にシングルサインオン対応のリバースプロキシ機能を設置し、ユーザはこのリバースプロキシを経由して学外の文献データベースシステムにアクセスする構成を考えている。

また、計算機ログイン認証を行う端末として、情報教育用端末や図書館端末などが想定されている。これらは当面ディレクトリ統合管理システムから配信される ID・パスワードによりログイン認証を行う予定である。多くの端末は Windows および Linux で動作している。学務情報システムへの履修登録などをこれらの端末を通じて行える必要があるため、IC カードリーダが Windows、Linux で利用できることは必須となる。

3.5. 監視・管理システム

監視・管理システムでは、設置されるシステム全体の各サーバの監視・管理を統合的に行える機能を提供する。また、各サーバで得られるログ情報の収集や、バックアップなども実施し、システム全体の安定運用を支援する。

4. まとめ

本稿では、大阪大学における PKI に基づく認証基盤システムの整備に向けた検討状況について述べた。本認証基盤の整備は、学内の研究・教育環境の大幅な前進となると考えている。

参考文献

[1]大西克彦, “大阪大学における基礎データ収集のためのデータベース構築事例,” 大学評価（大学評価・学位授与機構 研究紀要）, 第 3 号, pp.21-30 (2003)
[2]AICPA, WebTrust Program for Certification Authorities, http://www.webtrust.org/
[3]B. Ramsdell, “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification,” RFC3851 (2004)