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

2007－ＱＡＩ－23（９）
2007／5／30

キャンパスIT認証基盤の構築
－大阪大学における導入事例と課題－

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†

†大阪大学サイバーメディアセンター 〒567-0047 大阪府茨木市美穂ヶ丘5-1
E-mail: †{akiyama, teranisi, okamura, sakane, hasegawa, baba, nakano, shimojo}@cmc.osaka-u.ac.jp

あらまし 大阪大学では，業務システムのオンライン化に伴い，全学の認証基盤をよりセキュリティを考慮した全学IT認証基盤システムに更新した．全学IT認証基盤システムでは，公開鍵認証基盤（PKI）を導入し，公開鍵暗号による認証を行うことで，パスワード認証で問題となるパスワード解読の脅威を回避する機能を実現している．一方で，PKIでのセキュリティと利便性の確保には鍵管理デバイスの利用が必須であり，コスト面等の課題からすべてのユーザがPKIを利用できるとは限らない．そのため，SSOと併用することで，パスワード認証からの段階的な移行や複数の認証方式の混在を可能にしている．本稿では，本学で導入した全学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報告する．

キーワード 認証基盤，PKI，シングルサインオン，ディレクトリ統合管理システム，ID管理

The Construction of Campus-wide IT Authentication Infrastructure
－Installation Examples and Issues in Osaka University－

Toyokazu Akiyama† Yuichi Teranishi† Shingo Okamura† Eisaku Sakane† Go Hasegawa†
Ken-ichi Baba† Hirotaka Nakano† Shinji Shimojo†

† Cybermedia Center, Osaka University 5-1 Mihogaoka, Ibaraki-shi, Osaka, 567-0047 Japan
E-mail: †{akiyama, teranisi, okamura, sakane, hasegawa, baba, nakano, shimojo}@cmc.osaka-u.ac.jp

Abstract In Osaka University, since many academic affairs systems are going to become online, we have upgraded campus-wide IT authentication infrastructure to support higher security. The new infrastructure resolves vulnerability of the password authentication by introducing PKI authentication. Since key management devices are required to establish secure and convenient PKI, not all of the campus-users can use PKI. We combine PKI and single-sign-on to enable step-by-step migration from password to PKI and to support mixed authentication method. In this paper, we will describe the architecture, the operation status and the future works of the campus-wide IT authentication infrastructure.

Keyword Authentication Infrastructure, PKI, Single-Sign-On, Directory Integration System, Identity Management

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），ポータルシステムをはじめとする学内のITサービスの導入・運用を行ってきた．2002年にユーザの利便性と運用面の改善を目的として，ITサービスで利用するIDを統合した統一アカウントを導入した．また，ポータルシステムに簡易シングルサインオン（SSO）機能を追加することで，他の部局で提供しているWebアプリケーションの認証に統一アカウントを利用できる機能を提供した．これにより統一アカウントシステムは事実上，全学のITサービスの認証基盤として利用可能となった．その後，学内システムのオンライン化が進み，本人認証を必要とするシステムが増加してきた．特に学務情報システム（Knowledge of Osaka University Academic Nucleus: 以下KOAN）等の業務システムにおいては学生の科目履修情報や成績などの個人情報を登録するため，高いセキュリティのもとで本人認証する仕組みが要求される．また，認証基盤システムは複数のシステムと連携するため，どのベンダー製品で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．CMCの事務部門が情報推進部として事務局本部に改組され，統一アカウントシステムが業務システムのID管理を担うことになったため，システム更新にあわせてセキュリティ機能やインタフェースの改善を検討し[1]，全学IT認証基盤システムとして再構築した[2]．

全学IT認証基盤システムでは，高いセキュリティが

求められるアプリケーションでの利用を想定して，公開鍵基盤（PKI）を導入し，公開鍵暗号による認証を行うことで，パスワード認証で問題となるパスワード解読の脅威を回避する機能を実現している．一方で，PKI でのセキュリティと利便性の確保には鍵管理デバイスの利用が必須であり，コスト面等の課題からすべてのユーザが PKI を利用できるとは限らない．そのため，SSO と併用することで，パスワード認証からの段階的な移行や複数の認証方式の混在を可能にしている．本稿では，本学で導入した全学 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報告する．

2. 全学 IT 認証基盤システム

全学 IT 認証基盤システムの構成を図 1に示す．キャンパス PKI を実現するための CA，RA 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る SSO システム，連携システムへの ID 同期，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．

2.1. 大阪大学個人 ID

CMC が 2002 年に導入した統一アカウントは KOAN および人事給与システムの ID である学籍番号や教職員番号から生成していたため，以下のような問題があった．

ID の有効期間の相違：学籍番号は学籍保存のために所属等の変更に伴い番号が変更される．ユーザ利便性と運用面の改善を考慮し，学籍番号の変更によらず在籍中は同一の ID を利用可能とするため，学籍番号とは独立した ID が必要である．

セキュリティ：教職員番号は共済組合員番号と連動する形で生成されており，オンラインシステムの ID に利用した場合，不必要に個人情報をさらすことになる．個人情報と切り離した ID が必要である．

そこで，全学 IT 認証基盤システムでは，従来の統一アカウントを変更し，新たにランダムに生成される「大阪大学個人 ID」を利用することとした．

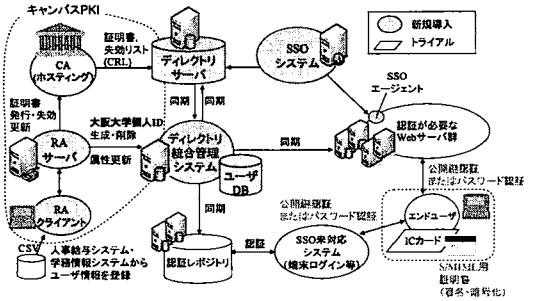

図 1 全学 IT 認証基盤システム

2.2. 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，SSO サーバとして Sun Java System Access Manager，ディレクトリサーバとして Sun Java System Directory Server を採用した．ディレクトリサーバには，2.4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 システムの基本的な動作を図 2に示す．認証が必要な Web サーバには，SSO エージェントを導入する．SSO エージェントは Web サーバのモジュールとして実装されており，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．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 Cookie 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ブラウザに SSO Cookie が設定される．Cookie は異なるドメイン名の Web サーバに提示することができないが，Liberty Browser POST Profile[3]と同様な方式で，異なるドメイン間での SSO 機能も提供している．モジュールが提供されていない Web サーバの場合，リバース Proxy サーバにモジュールを導入し，Web サーバの手前に設置することで SSO が利用できる．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．アプリケーション側の改修が難しい場合は，ID・パスワードを代理入力する機能をリバース Proxy サーバに作りこむことで対応する．

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[4]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．

SSO サーバは SAML2.0 に対応しており，将来的に大学間の認証連携に利用することができる．SAML2.0 の実装の多くは 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が，連携構築を容易にするためには，Internet2 の

MACE-Dir Working Group[5]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．

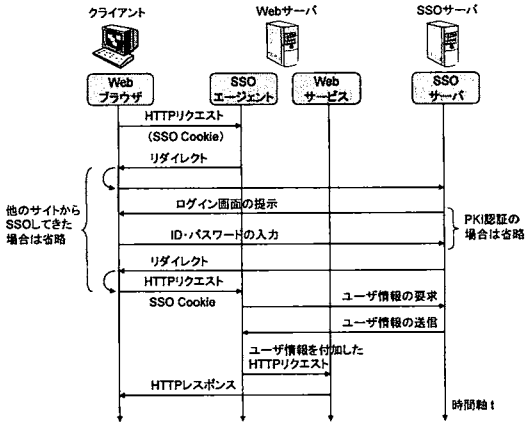

図 2 SSOシステムの基本的な動作

2.3. キャンパスPKI

大阪大学のキャンパス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．

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．これらのデータベースをID管理の情報源とすることで，登録局（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．

認証局（CA）はインハウスによってコストを抑えるアプローチも検討した．しかし，全学IT認証基盤システムはS/MIMEの導入によりメールでの個人情報の受け渡しにおけるセキュリティを向上させることを目標の一つとしていたため，以下のような課題があった．

- クローズドドメインCAをS/MIME用証明書の発行に利用した場合，認証局証明書を承認済みルート証明書として導入しているユーザ間でしか，暗号化・署名メールをやり取りできない．認証局証明書の管理がエンドユーザ依存になるため，信頼性の維持が困難となる．また，他大学，個人，企業のユーザと暗号化・署名メールが利用できない．
- オープンドメインCAを利用する場合，インハウスで構築するためには，WebTrust for CA認定[6]が必要となり，莫大な運用コストが必要となる．

そこで，S/MIMEを利用する学内ユーザ用には日本ベリサインのアウトソースCAを採用し，グリッドミドルウェアの利用に証明書を用いるグリッドユーザ用にはNAREGI-CAソフトウェアを用いたアウトソースCAを採用した．CAにアクセスするための証明書発行用サーバとして，東芝製Targusysを導入している．

オープンドメインCAをアウトソースする場合，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ーで決定される．しかし，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発行した方が，利便性が向上し，運用コストを低減できる．そこで，ユーザ認証用証明書の発行にクローズドドメインCAを採用し，S/MIME用証明書の発行にオープンドメインCAを採用した．また，S/MIME用証明書はユーザ認証用証明書を用いてオンラインで取得できるように設計した．S/MIME用証明書に記載するメールアドレスは，学生の場合全学メールサービスのアドレスを自動登録し，教職員の場合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．

PKIを利用する上では，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．セキュリティの向上と，ユーザの利便性を考慮した場合，鍵ペアを鍵管理デバイスで管理する必要があり，全学IT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カードを想定してシステムを構築した．また，ICカードの運用を検討するため，トライアルICカードを導入した．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，医学部等の部署でMacOSが利用されていることがわかっていたため，これらのプラットフォームをサポート可能なICカードとしてGiesecke & Devrient社製のStarCOSカードを採用した．

SSOシステムではユーザのセッション情報がCookieとしてネットワーク上で受け渡しされるため，セッションの横取りを防ぐために，サーバの認証と通信路の暗号化が必要となり，HTTPSを利用するためのサーバ証明書が必要となる．SSO連携システムのためのサーバ証明書はユーザ用の証明書とは別に購入する必要があるが，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[7][8]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．

2.4. ID同期

全学IT認証基盤システムは2.3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た上で，部局管理のデータベースに登録した上で，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 サーバは証明書発行サーバ Targusys 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，運用者がそれらの修正を可能にするため，CSV による手動での入力形式を採用している．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．

上記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，ディレクトリ統合管理システム Sun Java System Identity Manager (以下 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．2.2 節で述べた複数認証方式が共存可能な SSO システムの利点を生かすためには，認証は SSO システムに統一するのが望ましい．しかし，端末ログインのように SSO システムに対応していないサービスもあるため，これらのシステムには，認証情報（パスワード）も同期する．

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 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，例えば WebCT[9]のようなコースマネジメントシステム（CMS）では，履修情報や成績など，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．

- 初回ログイン時に登録
  SSO の機能で受け渡した属性情報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．
- 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 から同期するため，LDAP により同期している．また，語学学習用の CMS 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. システムの運用状況

図 3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 などが 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．

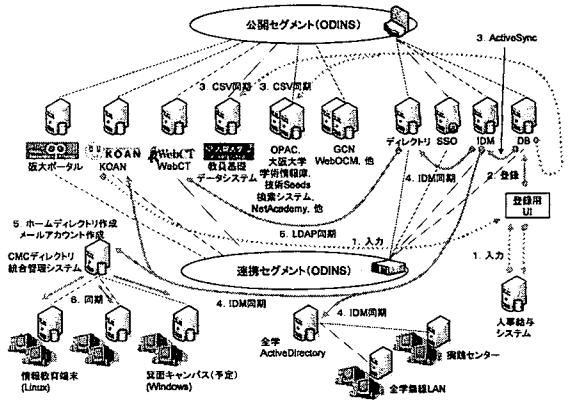

図 3 システムの連携状況

3.1. 統一アカウントからの移行

ID を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そのまま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い合わ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．

3.2. 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．以下ではこれまでに発生したトラブルについて紹介する．

SSO サーバの JavaVM の OutOfMemory エラー: JavaVM のメモリ不足によるガベージコレクション頻発により SSO サーバが応答しなくなった．負荷試験時には後述の Apache 用 SSO エージェントからの通信負荷を考慮したテストを実施できておらず，必要なメモリ量を少なく見積もってしまったことが原因である．これは JavaVM のメモリを拡張することで解決した．

SSO エージェントを導入した Apache サーバのダウン: KOAN では Solaris 上で Apache を利用しているが，AcceptMutex の設定を sysvsem にしていないと，導入するモジュールの実装によっては，Apache がダウンすることが分かった．上記設定投入により解決した．

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 4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 5に示すようなセッションが発生した場合，

- (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（SAML2.0 の Browser/Artifact Profile を利用する場合も同様）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．

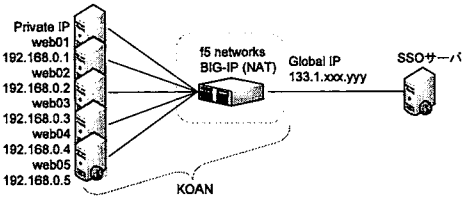

図 4 KOAN と SSO サーバ間の接続

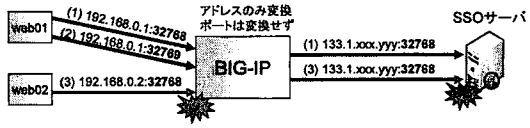

図 5 SSO エージェントの通信障害

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 2700 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するケースであった．6 日のアクセス状況を図 6，図 7に示す．SSO サーバは Sun Fire V240 (UltraSPARC IIIi x 2, Memory 8GB)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 6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 サーバの HTTP セッション数と CPU 負荷を比較した結果を図 7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わかる．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．Apache 用の SSO エージェントの実装で属性情報等のキャッシュがうまく動作しておらず，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．現在ベンダーにフィードバックしており，パラメータの調整等での性能改善方法を調査中である．

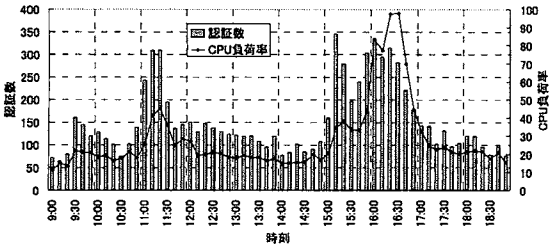

図 6 SSO サーバの認証数と CPU 負荷率

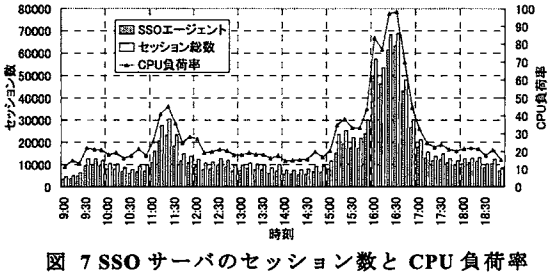

図 7 SSO サーバのセッション数と CPU 負荷率

3.3. ディレクトリ統合管理システムの運用状況

図 3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．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 件で約 5 時間同期にかかっている．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など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．

4. 今後の課題

これまでの運用では，3.2，3.3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．

5. まとめ

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．

6. 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」の一環として行なわれた成果である．

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] Toyokazu Akiyama, Yuuichi Teranishi, Shingo Okamura, Eisaku Sakane, Go Hasegawa, Ken-ichi Baba, Hirotaka Nakano, Shinji Shimojo, “A Report of Campus-wide IT Authentication Platform System Developement in Osaka University,” in Proceedings of SAINT2007 Workshop (Hiroshima), January 2007.

[3] 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

[4] OpenSSO Project: https://opensso.dev.java.net/

[5] Internet2 Middleware Architecture Committee for Education (MACE) Directory Working Group: http://middleware.internet2.edu/dir/

[6] AICPA, WebTrust Program for Certification Authorities, http://www.webtrust.org/

[7] UPKI イニシアティブ: https://upki-portal.nii.ac.jp/

[8] 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 年 5 月．

[9] WebCT: https://webct.ecs.cmc.osaka-u.ac.jp/