全学共通認証基盤サービスの手続きの電子化について

菅尾, 貴彦
九州大学情報システム部 : 職員

戸川, 忠嗣
九州大学情報システム部 : 職員

太田, 美和
九州大学情報システム部 : 職員

橋倉, 聡
九州大学情報システム部 : 職員

他

出版情報：第20回全国共同利用情報基盤センター研究開発連合発表講演会, 2008-10
バージョン：
権利関係：

全学共通認証基盤サービスの手続きの電子化について

菅尾 貴彦[1]　戸川 忠嗣[1]　太田美和[3]　橋倉聡[1]　平野広幸[1]　伊東栄典[3]
市川広大[2]　先立英喜[2]
1. 九州大学情報システム部情報基盤課
2. 九州大学情報システム部情報企画課
3. 九州大学情報基盤研究開発センター

{sugao, togawa, ohta, hasikura, hirano, itou}@cc.kyushu-u.ac.jp ,
{kou-ichikawa, hid-sendachi }@jimu.kyushu-u.ac.jp

1. はじめに

現在，九州大学には多数の学内向け情報サービスが存在している。これらの情報サービスでは利用者認証にID･パスワードを用いているが、これまで各サービスが個別に整備されてきたため，利用者ID・パスワードも個別に発行されてきた。

その結果，情報サービスが増えるにつれ，利用者認証の煩雑さ，パスワード管理の煩雑さ，情報サービス提供者側のシステム管理作業の煩雑さという，三つの煩雑さが発生していた。これらの煩雑さは，情報サービスを使った作業効率の低下，サービス拡充の妨げ，および安全性の低下の原因になっている。

また、近年では詐称メールや詐称サイトも問題となっている。大学が内外に発信する電子情報を信頼できるものにするためには，利用者認証による本人性確認が必要である。近年話題となっている情報の内部統制に対応するには，誰がどのような情報を発信したのか，誰が情報を編集・操作したのかを記録する必要がある。同時に情報サービスを提供するサーバ，およびそこから提供されるコンテンツも信頼できるものでなければならない。

学内向け情報サービスで上記の問題を解決し，利便性・信頼性・安全性（セキュリティ）を向上させて大学の様々な活動を効率化・充実化・信頼化するために，九州大学情報統括本部では，全学共通認証基盤の整備を平成１９年度から進めてきた。情報サービス毎に異なっていたID・パスワードを単一化し，認証機構を一元化することで，利用者認証の煩雑さやパスワード管理の煩雑さを解消し、かつ共通の認証基盤を使うことで，サービス提供者の管理作業の煩雑さも解消する。認証機構を経ることで提供サービスやメール内容の信頼性を向上でき、さらに認証機構を強固なものにすることで，情報セキュリティの向上を実現する。

本稿では，九州大学における全学共通認証基盤サービスを実現するために実施している全学共通認証基盤サービスの手続きの電子化について、この電子化を行うに至った経緯も含めて述べる。

2. 全学共通認証基盤のシステム概要

以下の図１に，九州大学全学共通認証基盤のシステム概要を示す。

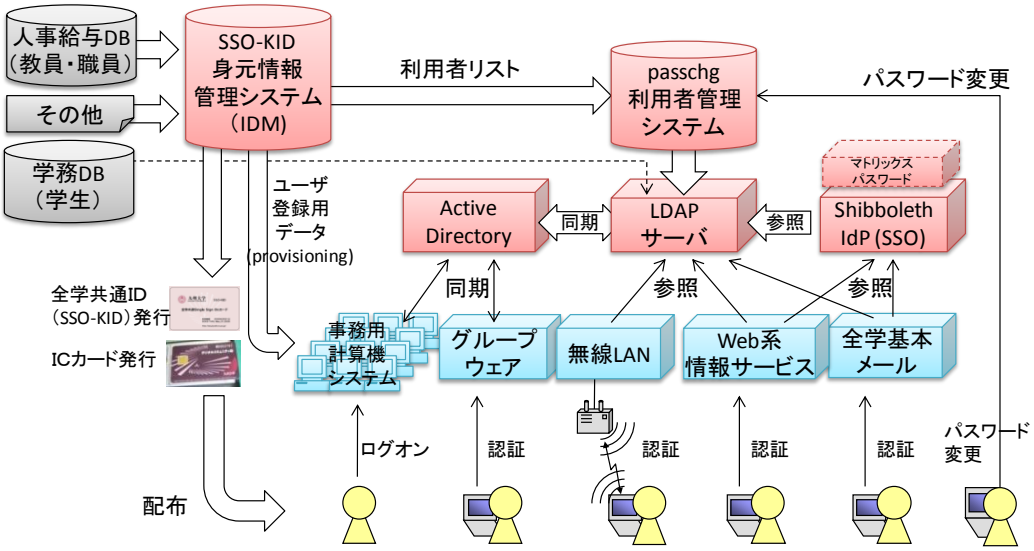

図 1：全学共通認証基盤システムの概要

以下に認証サーバ群の性能諸元を示す。

表 1：認証用 LDAP サーバ・性能諸元

ハードウェア	富士通 PRIMEPOWER 250
OS	Sun Microsystems Solaris 10
LDAP	Sun Java System Directory Server

表 2：利用者管理システム・性能諸元

ハードウェア	富士通 PRIMERGY TX200 S3
OS	Windows Server 2003 R2 SP2
RDB	Microsoft SQL Server 2005
Web サーバ	Apache + OpenSSL

表 3：SSO-KID 管理システム・性能諸元

ハードウェア	VMware の仮想マシン上に実現
OS	Windows Server 2003
DB	Microsoft SQL Server 2003

3. 全学共通認証サービスの内容

九州大学情報統括本部の全学共通認証サービスでは，三つのサービスを提供している。一つ目は，九州大学の全構成員を対象とする全学共通 ID（SSO-KID）の発行サービスである。残りの二つは，認証機能の提供サービスと，サーバ証明書の配付サービスであり，この後者二つのサービスの対象者は，学内向けに情報サービスを提供するサービスの提供者・運用責任者・システム管理者である。

3.1　全学共通 ID 発行サービス

九州大学では,平成１９年(２００７年)９月から学内の全職員に向けて全学共通ID(SSO-KID)を発行している[1]。この全学共通 ID（SSO-KID）は，学内向け情報サービスでの利用者認証を一元化するために制定したものである。平成２０年９月現在，新しく着任された職員へのSSO-KID カード・パスワード発行を毎月一回行っている。カード・パスワードは，安全性を考慮して対面での本人確認後に手渡しで配付している。また，利用者へのサポート窓口も運用しており，パスワード忘れ，全学共通 ID カード紛失，全学共通 ID の新規発行申請および再発行申請などに対応している。

平成２０年（２００８年）４月からは，九州大学の業務・研究・教育活動へ公にかかわる方で，人事給与システムに登録のない方への SSO-KID 発行も開始している。これらの方へは，申請を受け付けたのち，利用者登録と SSO-KID およびカードを発行している。申請により，全学共通 ID を発行する対象者としては，以下の方々を想定している。

- 九州大学の業務に従事すると部局等の長が認めるもの
  - 派遣業者から派遣されて業務に従事する方
- 九州大学における教育研究活動に従事すると部局等の長が認めるもの
  - 学術研究員（給与が出向元から支給されている方）
  - 共同研究などで，九州大学の職員とともに活動する他組織の方
    - 産学連携のために活動する福岡市職員
    - 包括連携等で共同研究活動に従事する企業の方
  - 九州大学の授業に従事する学外非常勤講師
  - 名誉教授
  - 日本学術振興会採用の特別研究員
- 九州大学病院における医療活動に従事すると部局等の長が認めるもの

3.2　認証機能の提供サービス

先に述べたように，平成２０年４月から，学内の情報サービスに対し，利用者認証機能の提供も開始している。図 2 に利用者認証機能の概念を示す。

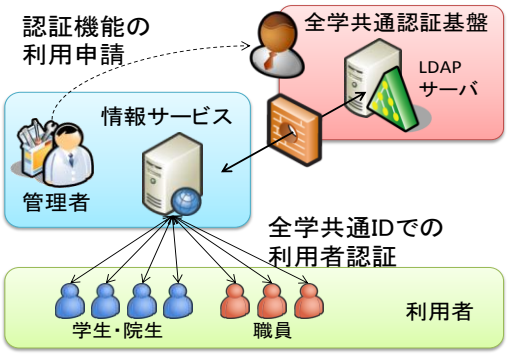

図 2：学内の情報サービスへの利用者認証機能

利用者認証機能の提供では，安全性・情報セキュリティの問題を抱えるため，利用者認証機能の提供にあたり，利用要項を定めている。利用要項は以下のサイトで要項を公開している。

全学共通認証基盤サービス認証機能利用要項

http://sso.kyushu-u.ac.jp/forms/files/service_youkou.pdf

以下に要項を簡単に説明する。まず，認証機能を利用可能な学内の情報サービスは，以下の条件を満たすものに制限している。

- 各部局等の長の承認を受け運用している情報システムであること。
- 九州大学のドメイン（kyushu-u.ac.jp）であること。

利用者認証機能の提供は，情報セキュリティに係る問題を含んでいるため，申請のあった全ての情報サービスに認証機能を提供するものではない。情報サービスがどのようなものであるか，学内向けの公的なサービスであるか，運用体制は堅実なものか，等の審査を慎重に行った後に，認証機能を提供するようにしている。

また要項では，認証機能の提供を受ける情報サービスのシステム管理者は，次の事項を遵守するように規定している。まず，認証に用いる秘密情報（パスワード）の保存や，漏洩は禁止している。また，自らが管理する情報システムの情報セキュリティを適正に保持することを要求している。

さらに，学内の情報サービスで，利用者アカウントの登録が必要な場合や，利用者の属性を用いた認可を行う場合，利用者情報の提供を行っている。利用者アカウントの登録には，学内構成員の一覧データを定期的に提供している。また，所属や役職といった属性を用いた認可のためには，認証サーバ・LDAP サーバ側で保持する属性を利用した，利用者アカウント登録時の提供する属性情報を利用することを許可している。ただし，利用者リストの提供や，属性情報の提供では，個人情報保護のための情報漏洩防止が必須となる。そこで，個人情報保護に関する覚書の取り交わしと，利用者リストの処理状況を保護するように求めている。

3.3　サーバ証明書の配付サービス

国立情報学研究所（以下，NII と記述）の学術情報ネットワーク運営・連携本部「認証作業部会」では，平成１９年度から「サーバ証明書の発行・導入における啓発・評価研究プロジェクト」を行っている。このプロジェクトは，大学等のサーバ証明書の普及推進と証明書発行プロセスの研究を目的としているもので，NII は WebTrust for CA 認定ルート認証局の下位認証局として「NII オープンドメイン認証局」を実際に構築し，その運用と参加機関への証明書発行を行っている。

NII サーバ証明書発行・導入における啓発・評価研究プロジェクト

https://upki-portal.nii.ac.jp/cerpj

九州大学情報統括本部でも，NII が行う「サーバ証明書の発行・導入における啓発・評価研究プロジェクト」に参加しており，九州大学内のサーバへの証明書申請受付を行っている。

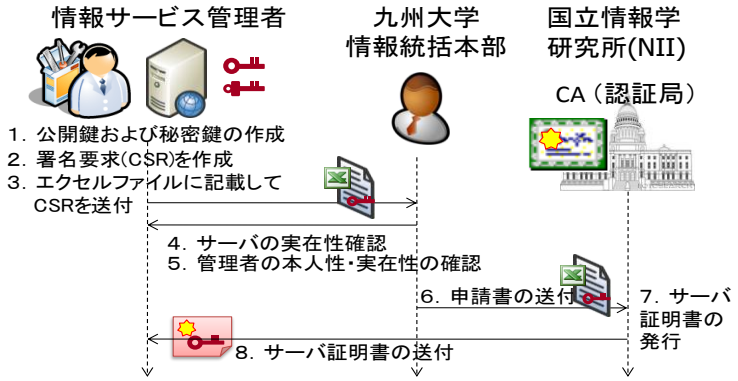

図 3：サーバ証明書申請受け付け手続き

4. 全学共通認証基盤サービスの手続きの電子化

ここでは本稿の主たる内容である，全学共通認証サービスの電子化について述べる。平成２０年９月現在，九州大学の全学共通認証サービスが持つ問題は，以下の４つである。それぞれについて電子化による効率化を検討した。また，一部については電子化を実現した。

- 全学共通 ID 発行の迅速化
- 利用者への全学共通 ID カード配付作業の効率化
- 各情報サービスへ安全に利用者リストを提供する作業の効率化
- サーバ証明書申請作業の効率化

4.1 全学共通 ID 発行の迅速化

図４に平成２０年９月現在の全学共通 ID（SSO-KID）の発行手順・頻度および問題点を示す。

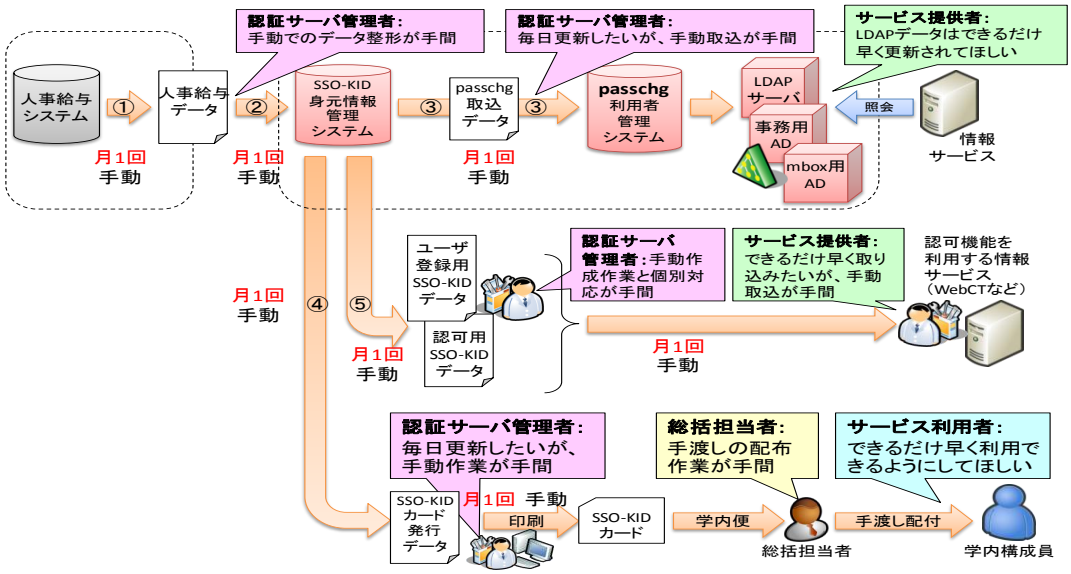

図 4：全学共通 ID 発行および認証サーバ・情報サービスへの利用者登録までの流れ

平成２０年９月まで，九州大学全学共通 ID の発行頻度は月に１回であった。全学共通 ID は人

事給与データベースに連動して発行されている。人事給与 DB の更新は給与支給を契機としているため，更新頻度は月に１回である。また，全学共通 ID カードとパスワードは学内便で配送され，本人確認の後に手渡しされているため，利用者が全学共通 ID カードを受け取るまでにカード発送から約半月かかっている。そのため，各月の一日に着任した人は一カ月後に，給与支給データの更新直後に着任した方は一カ月半後に全学共通 ID およびパスワード配付されていた。

全学共通 ID およびパスワードの配付に時間がかかるため，業務システムにおける利用者認証を全学共通 ID で行うことは，業務に支障をきたすことになる。そのため，いくつかのシステムでの利用者認証への導入が見送られていた。

幸いなことに，今年度（平成２０年度）に人事給与システムが更新される。平成２０年度後半から稼働する新しい「人事給与統合システム」では，毎日人員データを出力することができるようになった。この機能を用いて，人事給与システムと全学共通認証基盤システムの間のデータ流通を電子化（自動化）し，全学共通 ID 発行を迅速化することにした。

以下の図 5 に変更したシステムを示す。

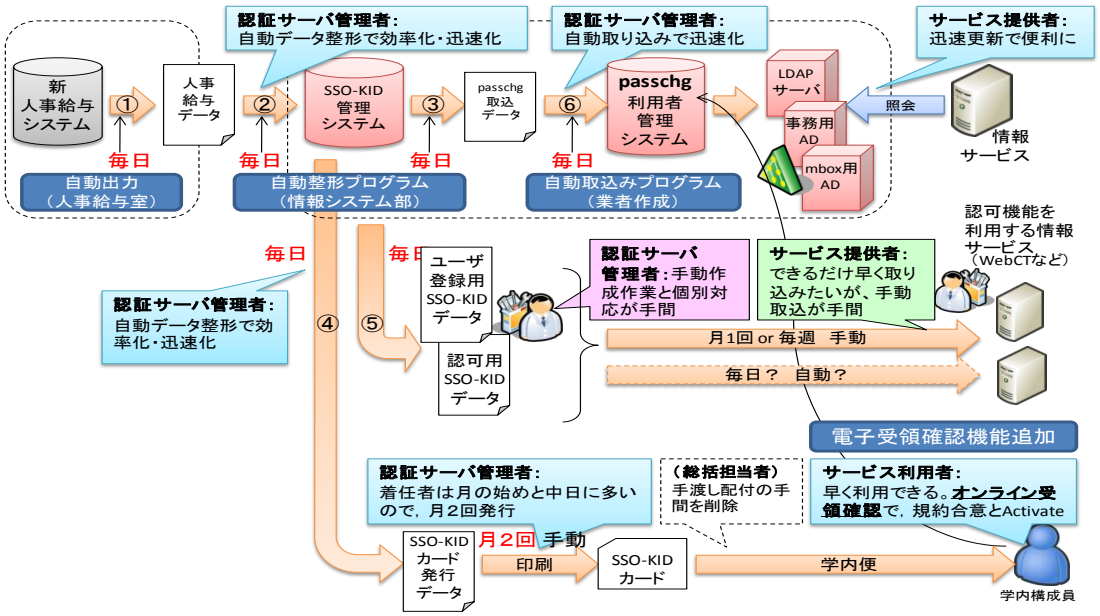

図 5：電子化・自動化による全学共通 ID 発行の迅速化

電子化した後の処理について詳細を述べる。①人事給与システムから，全員のデータが CSV 形式で出力される。データは，事務用ネットワークに接続されたファイルサーバの共有フォルダに出力される。②出力された人員データを定期的に取得し，内部を解析，データ整形，全学共通 ID 付与を行う自動整形プログラムを開発した。これを SSO-KID 管理システムと名付けている。SSO-KID 管理システムは，③認証サーバ（LDAP サーバ）に登録するためのデータを出力するとともに，④全学共通 ID カード（SSO-KID カード）印刷のためのデータの出力，⑤各種情報サービスに提供する利用者リストの出力も行う。これらの SSO-KID 管理システムは，マイクロソフト Access および VB スクリプトを用いて開発している。最後に，⑥業者から導入した利用者管理システム（パスワード変更装置を兼ねているため passchg と名付けている）にも定期的かつ自動的に更新する仕組みを導入した。業者へ依頼して，利用者管理システムに，定期的に更新データ（新規着任者の登録，異動・退職者の削除，氏名変更など内容の変更）を取り込み，それを認証

サーバ（LDAP サーバ）へ反映するプログラムを開発してもらった。

平成２０年９月現在，テストではデータの迅速な更新が可能になっていることを確認している。新しい人事給与システムが本稼働した後では，全学共通 ID の発行が迅速化し，業務システムにも適用できるようになると考えている。

4.2　利用者への全学共通 ID カード配付作業の効率化

教員・職員への全学共通 ID カードは，安全性のため対面による本人確認の後に，手渡しでカード配付が行われている。重要な学内向け情報サービスを，単一の全学共通 ID・パスワードで認証することにしているため，他者へ ID・パスワードがわたることは情報セキュリティ上重大な問題になるためである。しかしながら，手渡しによる全学共通 ID カード・パスワードの配付には時間がかかるし，海外に長期滞在する方や，病院などの大学事務との関係が薄い場合には手渡し配付が困難である。また、各部局等の配付担当者へは新たな業務として負担をお願いすることとなっている。この問題を解決するために，郵便や宅配便による自宅配付も検討した。しかし，最新の自宅住所情報を保持していないことの問題，職務として使うものを自宅へ配送することの問題，郵送費の問題から，郵便や宅配便による配付は行わなかった。そこで，学内便による ID カード・初期パスワードの配付と，受領確認およびパスワード変更を電子的に行う仕組みを検討した。

全学共通 ID カードおよび初期パスワードを学内便で配付する場合，郵便物の誤送や，他者による閲覧が問題となる。現在の全学共通認証基盤では，ID とパスワードのみで利用者認証を行っているため，ID・パスワードを知れば他人になりすまして情報サービスを利用することが可能である。学内便では，誤送で宛先者でない人が開封してしまう場合や，秘書が代理で開封することなどが問題となる。

そこで，以下の仕組みを検討した。まず，全学共通 ID カードの受領確認を利用者自身が行うまでは，情報サービス側の利用者認証機構を停止しておく。受領確認をオンラインで行う際，受領確認作業者が本当に利用者であるかを確認するために，その利用者しか知らない秘密情報を用いる。人事システムが保持する情報項目で，個人の秘密情報となりそうな項目を受領確認時に全学共通 ID・初期パスワードとともに，本人に入力してもらう。これにより，本人性を確立したのちに，全学共通 ID カードの受領確認および認証機能のアクティベイトを行う。

しかしながら、検討した電子的受領確認機能は近い将来、職員に配付する全学共通 ID カードが IC カード職員証と融合化することも考えられているなど配付方法について再検討が必要となったため、現在のところ実現していない。

4.3　各情報サービスへ安全に利用者リストを提供する作業の効率化

全学共通認証サービスでは，学内の情報サービス向けに全学共通 ID による利用者認証機を提供すると伴に，情報サービスで利用者アカウント登録や属性による認可制御のために，学内構成員の一覧データを提供している。これらの一覧データ提供は，安全性のため暗号化したファイルを USB メモリに格納し，それを手渡しすることで行われている。そのため，迅速な利用者登録が実現できていない。人事給与システムへの登録および全学共通 ID 発行・認証サーバへの登録の後，なるべく迅速に情報サービス側の利用者登録されることが望ましい。そこで，電子的な利用者情報提供（provisioning）による効率化について検討した。

九州大学内では，用途の異なる多数の情報サービスが個別に整備されてきた。そのため，各情報サービスは，独自の利用者登録環境を持っており，利用者アカウント登録を一元的に行うことは困難である。従って情報サービスごとの個別対応が必要になる。

情報サービスへの利用者情報提供を個別対応で行う場合，二つの問題がある。一つは情報サービスに適した登録利用者リスト作成することで，もう一つは情報サービスへの利用者登録を安全かつ自動的に行う方法である。

一つ目の情報サービスに適した登録利用者リスト作成については，スクリプトを作成することで実現する。提供できる属性項目数は決まっているため，それらのうちからどの属性が必要であるかを決め，それらの属性情報を抽出するスクリプトを作成する。

二つ目の情報サービスへの利用者登録を安全かつ自動的に行う方法については，十分な方法が確立していない。学内の事務用計算機システム内に存在する情報サービスについては，同一プライベートネットワーク上であるため，共有ファイルサーバを経由する方法が考えられる。情報サービスが同一ネットワーク上に存在しない場合，利用者リストファイルの提供は，Web の TLS などの暗号化通信を行いつつファイルをアップロードする方法や，SSH の SCP によりファイルをコピーする方法などが考えられる。他にも，セキュアなグループウェアに利用者リストファイルを定期的にアップロードして，情報サービス側から利用する方法などを検討している。

4.4　サーバ証明書申請作業の効率化

現在，サーバ証明書の申請は情報サービスの管理者が OpenSSL を用いた証明書署名申請の作成を行い，それをメールで送付することにより行っている。サーバ証明書の申請では，OpenSSL コマンドの実行による CSR（certificate signing request，証明書署名要求）の煩雑さと，メールによる申請であるための本人性確認作業が煩雑であることが問題となっている。

OpenSSL コマンドを用いる場合，サーバ証明書発行申請者は OpenSSL の利用法を把握している必要がある。また，コマンドの入力途中で CSR 作成のために必要な情報の入力を間違うと，もう一度最初から作成さなければならないため，大変手間がかかってしまう。

そこで，CSR の作成と，サーバ証明書の申請を Web サイト経由で行う電子化をし，サーバ証明書発行作業の効率化を考えた。サーバ証明書申請サイトの構成は以下の通りである。OpenSSL を用いてサーバ用の公開鍵，秘密鍵，および証明書署名要求（CSR）を作成する。作成した公開鍵・秘密鍵・CSR は作成者がダウンロードする。CSR 作成の終了後，ダウンロードした CSR を用いて，サーバ証明書申請用のエクセルファイルに記入する。最後に，作成したエクセルファイルを Web サイトへアップロードし，申請を終える。この申請サイトでは，サイトの入口で全学共通 ID を用いた利用者認証を行う。以下の図 6 および図 7 に，試作した申請サイトを示す。試作サイトは Apache Web サーバと Perl による CGI プログラムで構築した。

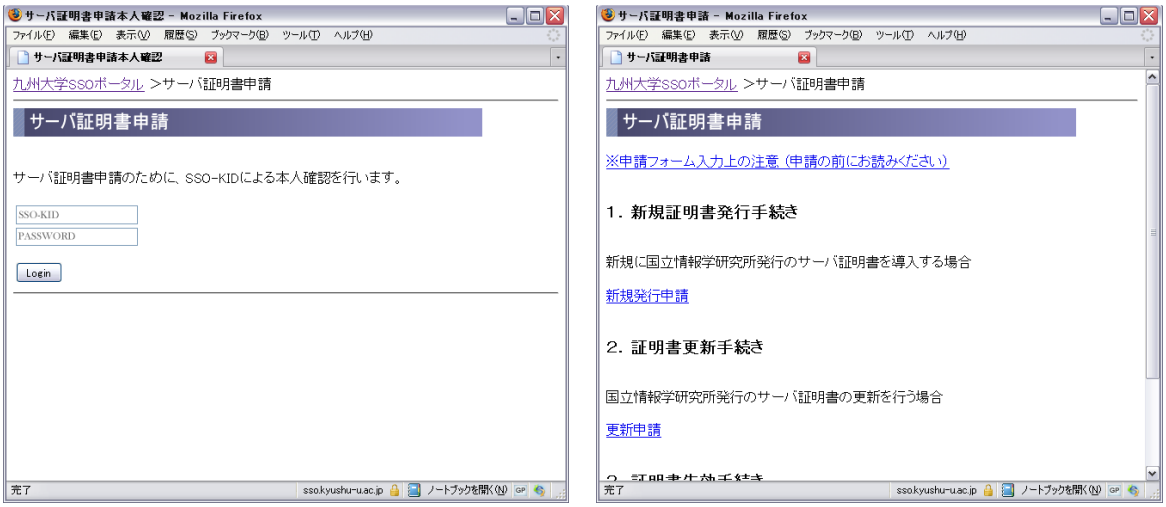

図 6：サーバ証明書申請サイト・利用者認証および機能選択

図 7：サーバ証明書申請サイト・新規発行申請フォーム入力画面

申請サイトの作成により，申請者はサーバ証明書作成のための OpenSSL コマンドを知らなくてもサーバ証明書の CSR を作成できるため，申請者の手間を大いに省くことができる。申請を受け付ける情報統括本部側も，申請サイトで九州大学の教員・職員であるかどうかを全学共通 ID で認証しているため申請者の本人性確認の一つを行うことができる。また，誰が何時，何というホストの証明書を申請したかを機械的に保持することができるため，管理の省力化・効率化を実現できる。

5. 今後の整備計画

ここでは，今後の九州大学全学共通認証基盤の整備計画について述べる。

5.1　シングルサインオンの実現

シングルサインオン（SSO）とは，利用者が一旦 SSO システムでサインオンすると，配下の情報サービスでの利用者認証は不要になり，障壁無しに複数の情報サービスが利用可能になるものである。SSO の実現により，認証を要する情報サービスの利便性が向上する。

現在，国立情報学研究所が行っているシングルサインオン実証実験に参加して，Shibboleth システムによる Web SSO の実験を行っている。いくつかの Web 系情報サービスで Shibboleth シングルサインオンを試している。今後，Web 情報サービスで，Shibboleth あるいは SAML2.0 に対応した認証機構の導入促進を検討している。ただし，Shibboleth や SAML は新しい技術であるため，最近の情報サービスでは導入可能であるものの，従来からある古い情報サービスでは対応できない場合がある。そのようなシステムについては，Shibboleth または SAML に対応した Reverse Proxy 型 SSO システムの導入を検討している。

5.2　マトリックスパスワードの導入

シングルサインオンが実現されると，一度のサインオンで配下の全システムが利用可能になる。ID・パスワードだけで利用者認証を行う場合，悪意のあるものが他人の ID・パスワードを盗用すると，SSO 配下の全情報サービスへの不正利用が可能になってしまう。そのため，SSO を実現する場合，同時に強固な利用者認証機構が必要となる。そこで現在，従来のパスワード認証に加え，マトリックスパスワード認証機構の導入を検討している。市販のマトリックスパスワードシステムを購入するか，大学内で自作するかを検討している。

6.　おわりに

本稿では情報統括本部の全学共通認証サービスの紹介と，全学共通認証サービスの電子化について述べた。電子化については，全学共通 ID 発行の迅速化，利用者への全学共通 ID カード配付作業の効率化，各情報サービスへ安全に利用者リストを提供する作業の効率化，およびサーバ証明書申請作業の効率化を検討し，一部は電子化を実現している。全学共通認証サービスの目的は，情報サービスにおける利便性・安全性・信用性の向上である。それにより，大学の情報サービスの充実，ひいては大学の活動の活性化に結び付くことを期待している。今後も情報サービスにおける認証について，様々な活動を行う予定である。

参考文献

[1] 伊東栄典，全学共通認証事業室：“全学共通認証基盤サービスの紹介　－全学共通 ID 発行，認証機能の提供，およびサーバ証明書の配付－”，九州大学情報統括本部 IT マガジン Vol.2, No.1, 2008.
http://iii.kyushu-u.ac.jp/publish/magazine/ITmag_Vol2No1/zengaku.pdf

[2] 伊東栄典，全学共通認証事業室：“九州大学全学共通認証基盤と全学共通 ID「SSO-KID」の紹介”，情報統括本部 IT マガジン Vol.1, No.2, pp.42-48, 2007.
http://iii.kyushu-u.ac.jp/publish/magazine/ITmag_Vol1No2/SSO-KID.pdf

[3] SSO ポータル：https://sso.kyushu-u.ac.jp/