

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

伊東，栄典
九州大学情報基盤研究開発センター：准教授：情報学

<https://hdl.handle.net/2324/15946>

出版情報：九州大学情報統括本部ITマガジン．2 (1)，pp.1-4，2008
バージョン：
権利関係：



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

伊東 栄典¹, 情報統括本部 全学共通認証事業室²

本稿では, 情報統括本部の全学共通認証サービスで提供する 3つのサービスについて紹介します。一つ目は全学共通 ID (SSO-KID) の発行サービスで, 九州大学の全構成員を対象としています。残りの二つのサービスは, 認証機能の提供サービスと, サーバ証明書の配布サービスです。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・システム管理者になります。全学共通認証サービスについて, 不明な点がございましたら, 表 1 表 1 の窓口へお問い合わせください。

表 1. 問合せ窓口・サポート窓口

担当	情報統括本部・全学共通認証事業室／情報システム部情報基盤課・情報管理室
電話	箱崎 (99) 7234, (外線 092-642-7234)
E-Mail	id-room@cc.kyushu-u.ac.jp
Web	http://sso.kyushu-u.ac.jp/

1. 全学共通 ID 発行サービス

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) を発行しています[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す。現在では, 毎月一回, 着任された職員へ SSO-KID カードを発行・配付しています。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ます。

また, 利用者へのサポート窓口も運用しており, 全学共通 ID のパスワード忘れ, SSO-KID 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おります。サポート窓口の問い合わせ先は, 上記の電話・メール・Web サイトになります。

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 発行も開始しています。これらの方は, 申請により SSO-KID を発行しています。具体的には, 以下の方々へ, 申請があれば SSO-KID を発行しています。

- 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
 - 給与が出向元から支給されている方³

¹ 九州大学情報統括本部情報基盤研究開発センター itou@cc.kyushu-u.ac.jp

² 九州大学情報統括本部・全学共通認証事業室 id-room@cc.kyushu-u.ac.jp

³ 現在, SSO-KID カードの自動発行を検討中です。

- ・ 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

情報セキュリティのためには、定期的なパスワード変更が推奨されています。表 2 に全学共通 ID に対応するパスワードの変更サイトを示します。

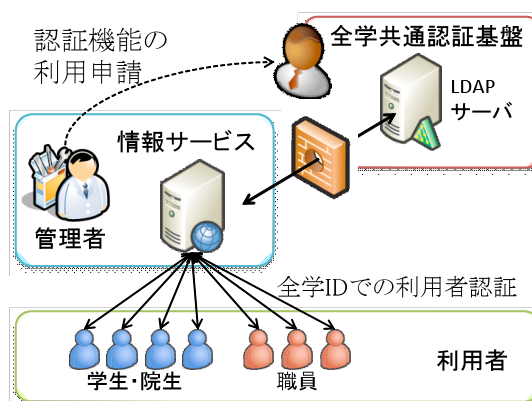
表 2. パスワード変更サイト

職員	https://passchg.kyushu-u.ac.jp/
学生	https://web-passwd.s.kyushu-u.ac.jp/tpass/

2. 認証機能の提供

全学共通認証サービスでは平成 20 年（2008 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ました。学内の情報サービスが全学共通認証サービスの認証機能を利用する条件は以下のとおりです。

- ・ 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みます。そのため、どのような情報サービスであるかについては、慎重に審査を行います。また、認証機能の提供をうける情報サービスのシステム管理者は、次の事項を遵守しなければなりません。まず、認証に用いる秘密情報（パスワード）を保存せず漏洩させてはなりません。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しなければなりません。

認証機能利用のための要項は、以下のサイトで公開しています。学内向け情報サービス提供者・管理者の方で、九州大学全学共通 ID (SSO-KID および学生 ID) での利用者認証を希望する方は、要項を理解した上で、表 1 の窓口へ相談下さい。

全学共通認証基盤サービス認証機能利用要項

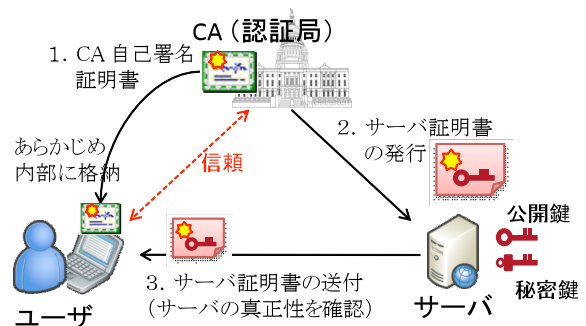
http://sso.kyushu-u.ac.jp/forms/files/service_youkou.pdf

3. サーバ証明書の配布

3.1 サーバ証明書とは

インターネットの普及に伴い様々な情報サービスが提供されるようになりました。サービス拡充で便利になる反面、それを悪用するものも現れました。フィッシングサイトと呼ばれるサイトでは、利用者を騙しての ID・パスワード盗聴や、入金操作をさせるなどの行為を行わせます。また、サイトが本物であるとしても、通信経路が安全とは限らないため、通信の暗号化も必要です。

そこで、公開鍵暗号方式を用いてネットワーク上で身元証明を行うための、PKI (Public Key Infrastructure, 公開鍵基盤) と呼ばれる仕組みが考案されました。PKI の電子証明書を使うことで、サーバの真正性（本当に正規のサーバであること）を保証できます。同時に通信路の暗号化も実現します。



3.2 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

サーバ証明書は従来、発行業務を行う企業から購入するしかなく、有効期限が 1 年の証明書が数万円していたため、多数のサーバへ証明書を導入することは困難でした。そこで、管理者が自作の証明書を作成することが行われていました。しかし自作の証明書はサーバ証明書の正当性を確認できないため Web ブラウザに警告が表示され、かえって利用者に不安を与える結果になっていました。

この問題を解決し、安全安心な情報サービスを展開するため、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」を行っています。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ます。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ます。詳細は以下エラー! 参照元が見つかりません。のサイトを参照ください。

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>

3.3 九州大学におけるサーバ証明書発行

九州大学情報基盤研究開発センターも、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ます。情報サービス提供者・サーバ管理者の方で、サーバ証明書発行を希望する方は表 1 の窓口へ

相談下さい。なお、特定の個人だけがアクセスするサーバなど、本プロジェクトの証明書利用がふさわしくないとと思われる場合は、発行をお断りする場合があります。

サーバ証明書の発行については、下記のマニュアルを参照ください。

サーバ証明書インストールマニュアル

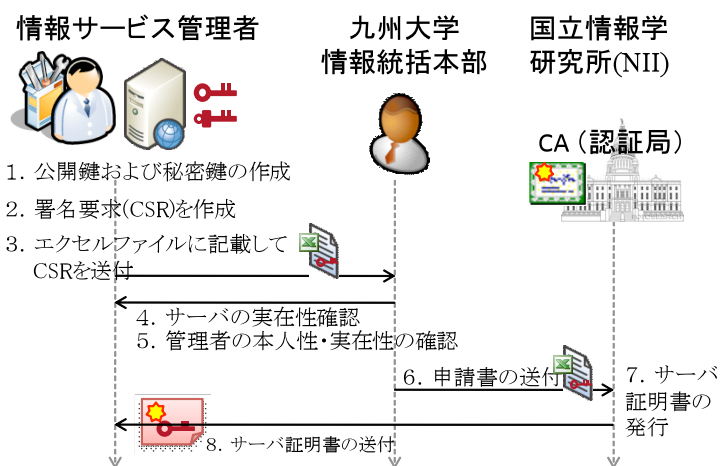
<https://upki-portal.nii.ac.jp/cerpj/niodcmanual-v1-0.pdf>

以下、大まかな手順を示します。

最初に、サーバ用の公開鍵および秘密鍵を作成します。**エラー! 参照元が見つかりません。**のマニュアルでは、OpenSSL による公開鍵および秘密鍵の作成方法が示されています。次に、公開鍵にサーバ名等の身元情報を添えた証明書の原型を作成します。この原型を元に CA の署名を依頼する署名要求ファイル (CSR, certificate signing request) を作成します。CSR が作成できたら、所定のエクセルファイルに CSR の内容を記載し、

情報統括本部・全学共通認証事業室へ送付ください。

情報統括本部・全学共通認証事業室では、そのサーバの実在性確認と、サーバ名(FQDN)の登録確認、およびサーバ管理者(申請者)が本当に九州大学の職員であるかを確認します。それらの確認作業が終わった後、NIIへCSRを送付します。送付されたファイルに問題が無ければ、NIIにより、管理者の元へサーバ証明書がメールにて送付されます。



4. 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で提供する3つのサービス、全学共通 ID (SSO-KID) の発行サービス、認証機能の提供サービス、およびサーバ証明書の配布サービスについて紹介しました。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・信用性の向上です。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ます。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す。

参考文献

- [1] 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”, 九州大学情報統括本部 IT マガジン Vol.1, No.2, pp.42-48, 2007.