

九州大学全学共通認証基盤と全学共通ID「SSO-KID」 の紹介

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

<http://hdl.handle.net/2324/15945>

出版情報 : 九州大学情報統括本部ITマガジン. 1 (2), pp.42-48, 2007-07. 九州大学情報統括本部
バージョン :
権利関係 :



九州大学全学共通認証基盤と全学共通 ID「SSO-KID」の紹介

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、情報統括本部で導入を進めている九州大学全学共通認証基盤と、全学共通 ID「SSO-KID」についてご紹介します。「全学共通認証基盤」とは簡単に申しますと、「1組の ID（識別子）とパスワードで持って一旦個人認証を済ませてしまえば、後はアクセスが許可されている各種の学内情報システムに対して自由にアクセスすることを可能とする」、すなわち、「シングルサインオン（Single Sign On）」のための情報通信基盤のことです。この全学共通認証基盤整備の第1歩として、「九州大学全学共通 ID『SSO-KID』」を本学の全教職員に交付致します。「SSO-KID」とは、シングルサインオン（Single Sign On）のための九州大学の ID（Kyushu univ. ID）から取ったもので、学内向け情報サービスで共通に使える利用者 ID です。

なお、全学共通認証基盤の整備は、今年度（平成19年度）から設立された情報統括本部内の全学共通認証事業室で担当しています。情報統括本部には、研究開発を行う情報基盤研究開発センターと、サービスに関する実務を行う情報システム部に加えて、情報環境整備推進室があります。全学共通認証事業室は、情報環境整備推進室内の一つの事業室で、全学的な認証に関する活動を行います。

1. 背景

現在、九州大学内には多数の情報サービスが存在しており、各サービスシステムは個別に利用者の ID・パスワードを発行しています。この状況は、三つの煩雑さを発生させており、その煩雑さが情報サービスを使った作業効率の低下、サービスの拡大や充実の妨げ、および情報サービスにおける安全性低下の原因になっています。

一つ目の煩雑さは、利用者による ID・パスワードの記憶についての煩雑さです。ID・パスワードによる利用者認証では、自分だけが記憶している知識（この場合はパスワード）を持っていることが情報サービスの安全性を保障しています。しかし、成績登録の様なめったに使わない情報サービスの利用者 ID・パスワードは、なかなか思い出せません。そのため、利用開始時に ID とパスワードを探す手間が発生します。効率化のための情報システム導入が、逆に作業の妨げになってしまいます。

二つ目の煩雑さは、利用者によるパスワード変更作業の煩雑さです。パスワードを破りに対処するため、情報サービス管理者はパスワードの変更を利用者に求めています。しかし、多数の情報サービスが存在すると、各サービスシステムでパスワード変更をせねばならず、その作業は煩雑なものになります。

三つ目の煩雑さは、情報サービス提供者側のシステム管理作業の煩雑さです。学内に常時利用

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

可能な構成員 DB（データベース）が無いため、情報サービスの提供者はサービスシステムの構築と同時に、利用者認証用の DB（利用者 ID とパスワードの一覧）も作成しなければなりません。サービス対象者を漏れなく登録することは煩雑な作業ですし、新規の参加者や転出者の管理作業も煩雑です。さらに、利用者の ID 紛失やパスワード忘れへの対応もしなければなりません。本来、情報サービスを充実させることが目的であるはずなのに、利用者情報の管理や利用者対応などでサービス充実に専念できない状況が発生していました。

これら三つの煩雑さが、情報サービスを使った作業効率の低下、サービスの拡大や充実の妨げ、および情報サービスにおける安全性低下の原因になっていました。

2. 全学共通認証基盤の整備と全学共通 ID「SSO-KID」の発行

以上の問題を解決するために、学内向け情報サービスで使える認証基盤を構築することとなりました。情報サービス毎に異なっていた ID・パスワードを一元化することで、記憶に関する煩雑さ解消します。認証機構を一元化することで、パスワード変更作業の煩雑さも解消されます。また、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できます。強固な認証基盤を構築すれば、安心かつ安全な情報サービスの運用が可能になります。

この全学共通認証基盤整備の第 1 歩として、「九州大学全学共通 ID『SSO-KID』」を本学の全教職員に交付致します。「SSO-KID」は、学内向け情報サービスで共通に使える利用者 ID です。配布する SSO-KID カードと、ID/パスワードを印刷した台紙については 4 節を参照下さい。

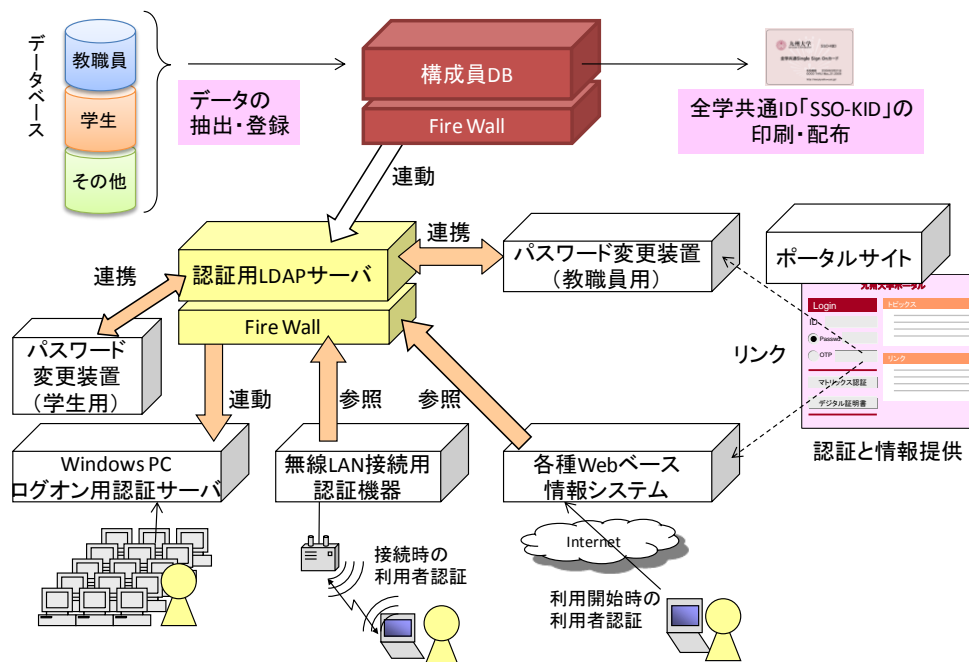


図 1：全学共通認証基盤のシステム構成

もちろん SSO-KID による利用者 ID の共通化だけで、情報システム利用時の認証が実現されるわけではありません。SSO-KID の発行と同時に、認証用システムの構築も行っています。学内構成員の情報を保持するデータベースの構築と、構成員への ID・パスワードの付与、さらに各種情

報サービスからの利用者情報の問合せを受け付ける LDAP サーバを準備しています。認証基盤における情報システム構成は図 1 をご覧ください。

3. SSO-KID の ID 体系

SSO-KID の文字列は 10 桁のランダムな数値です。10 桁の数値であれば、0 番から 9 億 9999 万 9999 番までの 10 億個の ID を利用可能です。10 億個の ID は、将来 100 年間に九州大学の所属者に配布することを想定しても、十分な数であるといえます。新規発行時である現在の構成員数は 30000 人、毎年新たに九州大学に入ってくる人が、学生・院生は 3500 人、教職員は 800 人、その他の方が 1000 人と想定しても、100 年で 56 万人になります (3 万人 + (3500 人 + 800 人 + 1000 人) × 100 年)。ですから、56 万個の ID があれば足ります。過去 100 年間の大学関係者に配布しても、学会参加者などの一時的な訪問者へ配布しても、十分な数であるといえます。

ランダムな数値を ID に用いているのは、不正アクセスによる情報漏洩の防止や、プライバシーの保護のためです[1]。不正アクセスのための攻撃として、ID とパスワードの総当りで試す攻撃があります。このような総当り攻撃に対する防御では、文字列の推測しにくさが重要です。もしも ID が続き番号 (シリアルナンバー) になっていれば、利用者に与えられた ID 番号を推測することが簡単に行えます。ID が推測できれば、残りはパスワードを総当りすれば良く、不正アクセスが容易になります。一方、ID がランダムな数値であれば、有効な ID を調べる段階で簡単には ID を推測できなくなります。また、将来 SSO-KID を個人への通信宛先 (メールアドレスなど) に利用した場合でも、いたずら通信 (迷惑メール) に対する障壁になります。

ランダムな数値はプライバシーの保護にも役立ちます。例えば入社・入学年度など意味のある数字が ID の中に入っている場合、ID 番号を見ただけで利用者の年齢などを推測可能です。ID に部局コードが入っている場合、ID から所属を判別できてしまいます。ID は通信データが保護されない環境で入力する場合や、メールアドレスのように通信の宛先として使うことも考えられます。宛先から利用者の個人情報などを推測できなくするためにも、ランダムな数値である ID 文字列が役に立ちます。

4. 全学共通 Single Sign On カード (SSO-KID カード) の配布

2007 年度の 10 月に、全学の職員向けに SSO-KID カードを配布します。配布する SSO-KID カードおよび台紙を図 2 に示します。カードはラミネート加工した紙カードで、印字面に氏名と SSO-KID 番号が印刷されています。SSO-KID と共に用いるパスワードは台紙に印刷されています。



図 2：配布する SSO-KID と台紙

注意：不正利用の防止や、個人情報保護のためには、皆さん自身が自分の SSO-KID とそれに対応するパスワードを適切に管理していく必要があります。パスワードは利用者自身で変更可能ですので、利用者自身によりすみやかなパスワードの変更をお願いします。パスワードの変更については5節の Web サイトを参照下さい。

5. SSO-KID に関する説明および問合せ先

SSO-KID に関する問合せ先を表 1 に示します。説明の Web サイトも用意しており、Web サイトの URL を表 1 に示します。Web サイトも参照ください。パスワードの変更も、Web サイト経由で可能です。

表 1：SSO-KID の案内 Web サイトおよび問い合わせ先

Web サイト	http://sso.kyushu-u.ac.jp/
責任部局	九州大学・情報統括本部・全学共通認証事業室
連絡先	092-642-7234

図 3 に <http://sso.kyushu-u.ac.jp/> の画面を示します。なお、シングルサインオンの機能は未だ実現されておりません。今後徐々に機能を拡充し、シングルサインオンも実現していく予定です。

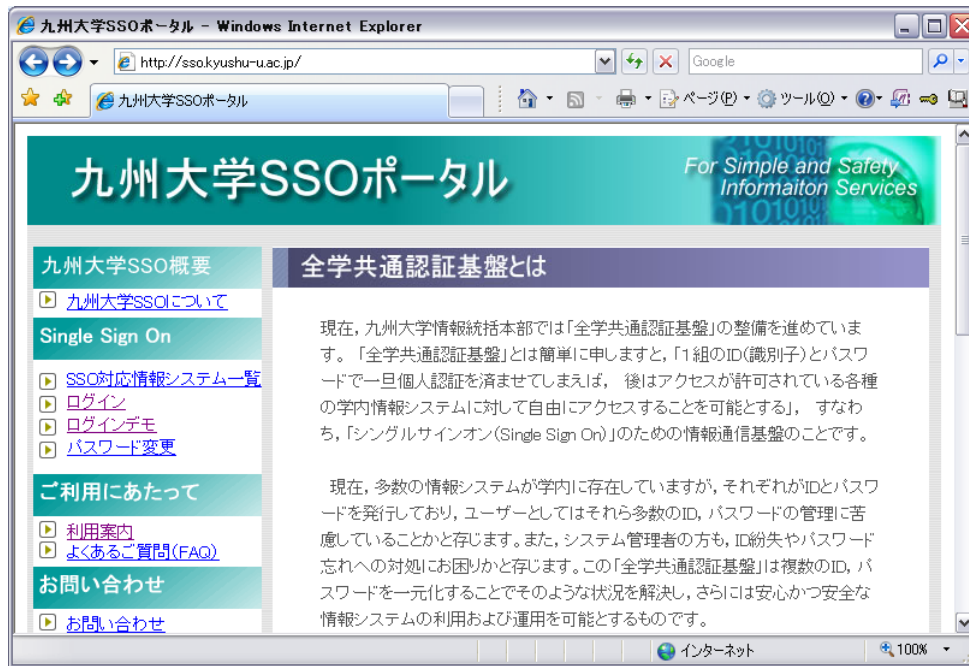


図 3：九州大学 SSO ポータル (<http://sso.kyushu-u.ac.jp>)

6. 利用場面

九州大学 ID「SSO-KID」は、以下のような情報サービスにおける利用を想定しています。太字は平成19年10月現在、SSO-KIDが利用可能な学内情報サービスです。

- Web ベース情報システムへのログイン
 - WebCT (電子教材提供, **e-Learning**)
 - 全学ライセンス取得ソフトウェアの入手 (ダウンロード時の認証)
 - 研究者情報 DB(大学評価システム)
 - 業務システム (財務システム, 学務情報システムなど)
 - 事務用グループウェア
- ネットワーク関連のシステム
 - 学内無線 LAN「**kitenet**」接続時の利用者認証
 - 外部から学内情報資源を利用するための装置への接続 (SSL-VPN 装置)
- 全学共通メールサーバへの接続時認証

できるだけ多くのサービスで利用できるように、今後、段階的にサービスを拡充していく予定です。本稿では、利用可能な情報サービスである WebCT についてご説明します。

6.1 WebCT での利用

情報統括本部では、学内共通の e-Learning システムとして WebCT を導入しています。H17 年度には、WebCT へ全ての学生・大学院生のアカウントが登録されていました。WebCT は学生および大学院生の教育用として活発に利用されています。表 2 に WebCT を運用している e ラー

ニング支援室の情報を記載します。

表 2 : WebCT のサイトと e ラーニング支援室の連絡先

サイト	http://webct.kyushu-u.ac.jp/
担当	九州大学・情報統括本部・教育支援事業室 e ラーニング支援室
連絡先	E-mail: el@cc.kyushu-u.ac.jp Tel: 092-642-7526(内線 99-7526)

今回、全学共通認証基盤となる LDAP サーバの整備と、教職員に SSO-KID を配布することにあわせて、全教職員の SSO-KID を WebCT にも登録していただきました。図 5 に示す WebCT のログイン画面で、SSO-KID とパスワードを入力することで、WebCT を利用できます。どの教職員も WebCT の教材閲覧が可能です。



図 4 : WebCT の案内サイト

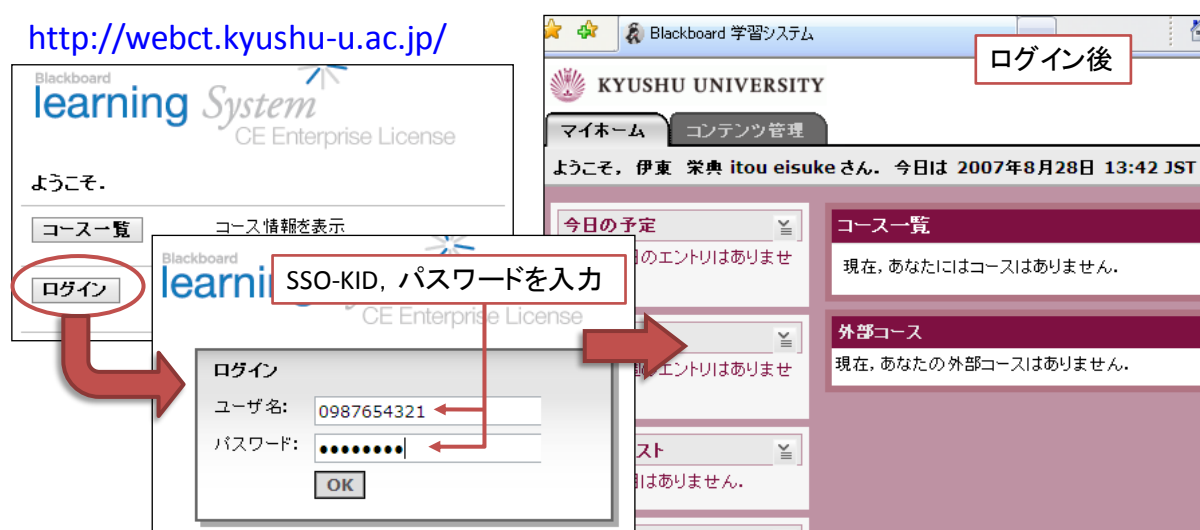


図 5 : WebCT へのログイン画面

7. 全学共通 IC カード（デジタルコミュニティ証）との関係

この記事で紹介する全学共通 ID “SSO-KID” は、伊都キャンパスを中心に実験と導入が進んでいる「全学共通 IC カード（デジタルコミュニティ証）」[2] と相補関係にあります。PC 端末や携帯電話などを介するオンラインの情報サービスでは、ID とパスワードによる利用者認証で十分な場合も多く、それらには全学共通 ID SSO-KID が手軽で便利であると考えています。将来 IC カードおよび IC カードリーダ装置が様々な場面で利用可能になれば、SSO-KID の入力による利用者認証の場面はなくなるかもしれません。

8. おわりに

本稿では情報統括本部で導入を進めている九州大学全学共通認証基盤と、全学共通 ID 「SSO-KID」について紹介しました。情報サービスの充実と、安全・安心な情報環境の整備のために、全学共通認証基盤の構築と、全教職員へ認証用の全学共通 ID 「SSO-KID」を発行しました。今後は SSO-KID を用いた各種サービスについて説明する予定です。

また、SSO-KID と名付けているものの、現在はシングルサインオン（Single Sign On）機構を実現できておりません。近い将来に、1組の ID（識別子）とパスワードで持って一旦個人認証を済ませてしまえば、後はアクセスが許可されている各種の学内情報システムに対して自由にアクセスすることを可能とするシングルサインオンを実現できるように、様々な活動を行う予定です。

参考文献

- [1] のぎ田めぐみ，笠原義晃，伊東栄典，鈴木孝彦：“利用者認証に用いる識別子の決定方法に関する考察”，電子情報通信学会 信学技報 ISEC2006-112, pp.67-72, Dec.13, 2006.
- [2] e-World デジタルコミュニティ証実証実験, <http://www.miid.kyushu-u.ac.jp/>, 2005～2007.
- [3] 間瀬健二，平野靖，梶田将司：名古屋大学 ID の導入について－（I）概要－，名古屋大学情報連携基盤センターニュース, Vol.5, No.4, 2006.11.
- [4] 平野靖，間瀬健二，梶田将司：名古屋大学 ID の導入について－（II）全学 ID からの移行－，名古屋大学情報連携基盤センターニュース, Vol.6, No.2, 2007.5.