

KUINS ニュース No. 66

京都大学 情報環境機構 KUINS 運用委員会

<http://www.kuins.kyoto-u.ac.jp/>



生存圏研究所木質材料実験棟 (木質ホール)(左) と
木質ホール設置の船鉾車輪 (今秋公開予定)(右)

目 次

全学情報システムとして指定したシステムについて	796
グループウェア用認証 ID (SPS-ID) による電子ジャーナル・データベース認証について	797
PPTP サーバ増強について	797
平成 21 年度第 2 回 KUINS 利用講習会の案内	798
全学認証基盤の構築 ～全学 ID と統合ディレクトリ～	798
国立情報学研究所 (NII) の新サーバ証明書プロジェクトについて	800
無線 LAN 基地局に関するお知らせ	801
宇治地区生存圏研究所木質材料実験棟 (木質ホール) への無線 LAN 設置について	802
平成 21 年度の KUINS 機器更新予定に関する続報	803
不在になった教職員の KUINS 接続機器登録データベースからの削除について	803
SSH Port Forward サーバを利用する方法 (Windows Vista 編及び Mac OS X 編)	803
KUINS 会議日誌	804
お知らせ	804

全学情報システムとして指定したシステムについて

最高情報セキュリティ責任者

大西 有三

平成 21 年 6 月 9 日開催の全学情報セキュリティ委員会において、京都大学情報セキュリティ対策基準第 4 条により、次の情報システムが全学情報システムとして指定されましたのでお知らせいたします。したがって、同対策基準第 5 条により、全学情報システムの情報セキュリティ対策は、全学情報セキュリティ委員会が執り行うことになります。管理運営は、情報環境機構が行うことになります。全学情報システムの利用規程については、策定作業を行っているところで、確定出来次第公開いたします。システムの使い勝手については現行と変わることは無いと思われます。ご理解、ご協力いただきますようお願いいたします。

(1) 統合認証システム

- ・ 全学生認証ポータルシステム
- ・ 教職員グループウェアの認証システム
- ・ 教育研究コミュニティ認証連携システム
- ・ 統合 LDAP システム
- ・ 京都大学電子認証局

(2) 学術情報ネットワーク (KUINS)

【参考】京都大学情報セキュリティ対策基準抜粋

(管理運営組織)

第 4 条 最高情報セキュリティ責任者は、全学の情報基盤として供される本学情報システムのうち、情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システム (以下「全学情報システム」という。) を指定する。

2 全学情報システムの運用・管理を行う組織 (以下「管理運営組織」という。) を置き、情報環境機構をもって充てる。

3 管理運営組織は、前項に定めるほか、情報セキュリティ実施責任者の指示により、以下の各号に定める事務を行う。

- (1) 全学情報セキュリティ委員会の運営に関する事務
- (2) 本学情報システムの運用と利用における情報セキュリティポリシーの実施状況の取りまとめ
- (3) 講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ
- (4) 本学の情報システムの情報セキュリティに関する連絡と通報
- (5) 全学情報システムと部局情報システムとの接続等の調整及び対外接続に関する取りまとめ

(組織体制)

第 5 条 全学情報システムの情報セキュリティ対策は、基本方針及び規程に従い、最高情報セキュリティ責任者の下、全学情報セキュリティ委員会が執り行うものとする。

2 部局情報システムの情報セキュリティ対策は、基本方針並びに規程及び部局の運用方針に従い、当該情報システムを管理する部局の部局情報セキュリティ責任者の下、部局情報セキュリティ委員会が執り行うものとする。

3 情報セキュリティに関する全学及び部局間の技術的な連絡調整は、全学情報セキュリティ幹事会が執り行うものとする。

4 情報ネットワークに関わる危機管理に関する事項は、情報ネットワーク危機管理委員会が執り行うものとする。

5 情報ネットワークにおける人権侵害、著作権侵害等に該当し、又は該当するおそれのある情報の発信防止等に関する事項は、情報ネットワーク倫理委員会が執り行うものとする。

グループウェア用認証ID(SPS-ID)による電子ジャーナル・データベース認証について

図書館機構

現在、教育用コンピュータシステム利用コード (ECS-ID, a0xxxxxx (xは数字)) のみに対応している電子ジャーナル・データベース認証システムが、本年10月から、グループウェア用認証ID (SPS-ID) にも対応予定です。

10月以降は基本的に、学生はECS-ID、教職員はSPS-IDを用いることになります。これまで、教職員は電子ジャーナル・データベースを利用するために、ECS-IDを取得する必要がありましたが、これにより、ほとんどの本学構成員が、認証システムを利用するためだけの申請手続きは不要になります。もちろん、教職員でも従来のECS-IDで引き続きご利用可能です。

情報環境機構と図書館機構が連携して準備をしております。サービス開始時には、あらためてお知らせします。

PPTP サーバ増強について

平成17年4月のPPTPサーバの運用開始以来、PPTP利用者は年々増加してきております。これに伴い、サーバの過負荷等の原因により接続ができない等の問題が発生するようになってきました。この対策として、8月10日(月)より、PPTPサーバを3台から6台に増強して運用を開始しています。

この増強により、PPTPサーバのIPアドレスが変更になっていますので、PPTPサーバをIPアドレス指定で接続されている方は、ホスト名「**pptp0.kuins.kyoto-u.ac.jp**」で接続するよう設定変更下さい。また、部局等のサーバにおいて、DNS逆引きにてアクセス制御されている方は、以下のアドレスからのアクセスができるように設定してください。

h1～h253.100.226.10.104601.vlan.kuins.net.

h1～h253.135.232.10.104602.vlan.kuins.net.

h1～h253.128.236.10.104603.vlan.kuins.net.

h1～h253.73.238.10.104604.vlan.kuins.net.

h1～h253.75.240.10.104605.vlan.kuins.net.

h1～h253.95.242.10.104606.vlan.kuins.net.

h1～h253.117.244.10.104608.vlan.kuins.net.

h1～h253.103.249.10.104607.vlan.kuins.net.

平成 21 年度第 2 回 KUINS 利用講習会の案内

KUINS 講習会を下記日程にて開催します。この講習会は、KUINS に関する各種の情報を提供するために開催するもので、新規採用教職員を主な対象としていますが、それに限らず多くの皆様に御参加頂きたい講習です。講習内容は、

- ・ 京都大学学術情報ネットワーク (KUINS) の構成、運用体制
- ・ 京都大学におけるネットワークセキュリティ対策
- ・ KUINS への利用方法の解説

などです。詳細は KUINS ホームページ等で追ってご案内します。多くの方の参加をお待ちしております。

日時：平成 21 年 10 月 9 日 (金) 午前 10 時～

場所：学術情報メディアセンター北館 3 階講習室

全学認証基盤の構築 ～全学 ID と統合ディレクトリ～

情報環境機構
認証システム運用委員会

京都大学で導入を進めている認証基盤システムの紹介記事を連載していきます。第一回目は、学内の様々なシステムで共通に利用できる全学 ID と、その情報を格納する全学的な統合ディレクトリについて紹介します。

全学 ID

京都大学では、学内の構成員全員 (学生、教職員、その他) が電子システムの認証に利用できる全学 ID が提供されていなかったため、システム毎に ID が乱立し、利用者はシステム毎に異なる ID とパスワードの組み合わせを覚える必要がありました。また、システム管理者は対象とするシステムのためだけの ID ライフサイクルを管理・運用する必要がありました。近年、殆どのサービスが Web 化されてきたため、利用者にも管理者にも大きな負担となっていました。そこで、これらの負担軽減を目指し、情報環境機構では全学の様々なシステムで共通に利用可能な全学 ID を提供することにしました。

教育用コンピュータシステムや、全常勤職員に ID が発行されているグループウェアサービスが既に存在していましたが、どちらもライセンス数や費用の点から、京都大学の全構成員に対して ID を発行する余裕はありませんでした。しかし、この二種類の体系の ID を併用すれば学生と教職員それぞれの全構成員に ID を発行することは十分に可能であり、また、利用者にとっては既存の ID を再利用できるため切り替えの大きな混乱が無いという利点もありました。

これらの理由から、学生系と教職員系の二系統に分けて、全学 ID を提供する方法を採用することにしました。なお、学生系の全学 ID を **ECS-ID**、教職員系の全学 ID を **SPS-ID** と名付けました。統合ディレクトリやシングルサインオン (SSO) システムを用いて、学内の様々なシステムでの認証に ECS-ID や SPS-ID を利用できる環境を整え、利用者の利便性を向上させています。

ECS-ID

ECS-ID (Educational Computer System ID) は、教育用コンピュータシステムのログインやメールサービス等で利用されており、“a0xxxxxx” (xxxxxx は数字) という形式の ID です。本人の氏名や学生番号等と一切関係がないため、学生番号等を用いるのに比べ安全な ID 体系です。

学生は、情報環境部 情報基盤課 共同利用担当に申請を行い、学術情報メディアセンター南館で実施される利用コード交付講習会を受講すれば、この ID を取得することができます。

SPS-ID

SPS-ID (School Personnel System ID) は、教職員グループウェアへのログインに利用されており、ID の文字列中に氏名のローマ字表記と三桁の数字を合わせた“taro000kyoudai”のような形式になっています。

三桁の数字は、氏名だけでは容易に ID を推測できることを抑制する点と、同姓同名への対策のために導入されています。常勤教職員全と、部局担当から申請のあった非常勤教職員に対して、情報環境部 電子事務局が ID を発行し、ID と初期パスワードを封筒に入れて学内便で送付しています。

統合ディレクトリの導入

2007 年度に OpenLDAP を用いた統合ディレクトリを構築し、ECS-ID と SPS-ID の両方の全学 ID を格納しました。2008 年度には安定性の向上と将来の高負荷への対策のため、情報環境機構に導入された基盤コンピュータシステム上の仮想サーバを利用し、ソフトウェアを Fedora Directory Server に変更して統合ディレクトリを再構築しました。

現在の構成では、二台の負荷分散装置の配下の二台の仮想サーバで LDAP サーバが動作しています。今後、サービスの充実に伴って統合ディレクトリの負荷が上昇した場合は利用する仮想サーバを増加させて対応する予定です。

データ構造

統合ディレクトリでは、表 1 に挙げたような LDAP で一般的に利用されている inetOrgPerson オブジェクトクラスの属性に加えて、京都大学で独自拡張した複数のオブジェクトクラスを利用して、一人の人物が複数の身分を持ったり、複数の組織に所属したりできるデータ構造としています。cn, sn, givenName などに日本語名を登録する場合は、言語タグ lang-ja を利用しています。

表 1: 主な属性

属性名	内容
uid	利用者の ID (ECS-ID または SPS-ID)
userPassword	パスワード
cn	氏名
sn	姓
givenName	名

以下に独自拡張したオブジェクトクラスについて説明します。追加したオブジェクトクラスは表 2 のように、教員用、職員用、学生用ごとに分けて 3 種類あり、N は 1 から 3 までの 3 個ずつ用意してあります。

表 2: 拡張オブジェクトクラス

拡張オブジェクトクラス名	内容
kyotoUniversityStudentN	学生用
kyotoUniversityTeacherN	教員用
kyotoUniversityStaffN	職員用

それぞれのオブジェクトクラスには表 3 のような複数の属性が登録されています (表 3 は オブジェクトクラス kyotoUniversityTeacher1 の例です). これらの拡張属性でも, 日本語で登録する場合は言語タグ lang-ja を利用します.

表 3: オブジェクトクラスの拡張属性の例

拡張属性名	内容
teacher1	本オブジェクトクラスの内容の有効/無効
teacher1EmployeeNumber	職員番号
teacher1Mail	メールアドレス
teacher1TelephoneNumber	電話番号
teacher1FacsimileTelephoneNumber	FAX 番号
teacher1O	組織第一階層
teacher1Ou	組織第二階層
teacher1PilotOrganization	組織第三階層
teacher1Title	役職名

対応サービス

現在, 統合ディレクトリを利用して認証を行なっているサービスは, 語学用 e-Learning システム (工学研究科), 名簿・メーリングリスト管理システム, セキュリティ e-Learning システム, ホームページホスティングサービス, 学習支援システム (WebCT)(情報環境機構) 等です.

今後, 統合ディレクトリで対応する全学 ID でのサービスとして, SAML 対応のシングルサインオンシステム, KUINS の提供する VPN 接続サービスや無線 LAN 認証用の eduroam アカウント発行システム等を予定しています.

以上のように, 学内の部局等で新たな Web サービス等を導入する際, 統合ディレクトリを参照して認証を行うことが可能なので, 情報環境部へお問い合わせ下さい.

おわりに

今回は全学 ID と統合ディレクトリについて紹介をしました. 次回は, シングルサインオンシステムと, 2010 年 4 月に利用開始予定の, IC 学生証・IC 職員証について紹介します.

国立情報学研究所 (NII) の新サーバ証明書プロジェクトについて

国立情報学研究所 (NII) では「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」(旧プロジェクト)の後継プロジェクトとして,「UPKI オープンドメイン証明書自動発行検証プロジェクト」(本プロジェクト)を開始しました. 旧プロジェクトで発行したサーバ証明書は 2009 年 9 月 30 日で失効処理が行われるため, 今後も継続してサーバ証明書を利用したい場合は, 下記 URL から新プロジェクトで発行申請を行なって下さい. なお, 旧プロジェクト発行の証明書については, NII 側で一括失効しますので, 置き換え終了後に失効申請していただく必要はありません.

- ・新プロジェクト 利用の手引き (加入者編) (<https://upki-portal.nii.ac.jp/docs/odcert/howto/ee>)
- ・証明書申請ページ (<https://db.kuins.kyoto-u.ac.jp/cerpj/>)
- ・証明書申請ページへ京都大学ポータルサイト経由でアクセス (SPS-ID が必要です)
(<https://www.tam2.adm.kyoto-u.ac.jp/kuinsdb1/cerpj/>)

なお、旧プロジェクトでの証明書とは下記のような点で異なります。詳しくは上記の申請ページ内の案内をご覧ください。

- ・CSR 作成時に登録する L (Locality Name) を Academe から Academe2 へ変更になりました。
- ・ルート CA や証明書チェーンが変更されました。
- ・サーバ証明書の有効期間は発行日から 25ヶ月になりました。
- ・OU (Organization Unit) 属性にコンマ (,) を登録できなくなりました。
- ・証明書の取得は、ダウンロード用 URL がメールで加入者に通知されて、加入者が直接取得する方法になりました。

無線 LAN 基地局に関するお知らせ

KUINS ニュース No.65 以降に追加されました無線 LAN 基地局についてお知らせいたします。

今回は、総合研究 2 号館 (教育学研究科関係 1 階及び地下 1 階)、留学生ラウンジ「きずな」、事務本部棟、理学部 6 号館 (3 階及び 4 階)、キャンパスプラザ京都、医学研究科人間健康科学系専攻 杉浦ホール、生存圏研究所木質ホール (3 階)、農学部総合館 (情報技術室)、文学研究科に設置しました。現在の設置箇所 (部局・建物) の一覧は、KUINS ホームページの「MIAKO ネット仕様無線 LAN アクセスポイント設置場所」を御覧下さい。

以前から要望の高かった事務本部棟 1 階から 5 階まで全フロア利用可能となりましたので、会議・打ち合わせ時等の際にお使いいただけます。そして、宇治地区での展開ということで、電話庁舎・防災研に続き、生存圏研究所木質ホールでの利用が可能になりました。こちらの詳細を本号別記事 (「宇治地区生存圏研究所木質材料実験棟 (木質ホール) への無線 LAN 設置について」) として、利用に関する注意点や案内、宇治地区での今後の展開等について、宇治地区事務部総務課総務・企画広報グループにお願いしました。そちらの方も御参照下さい。

一連の作業は、全学インセンティブ経費「アクセスネットワーク」(詳しくは、KUINS ニュース No.63 をご覧ください) による設置の一環として実施しております。現在、無線 LAN 基地局の設置を先行実施中です。講義室や会議室等、公共性の高い空間への設置を進めておりますので、部局担当者様からの御相談・お問い合わせをお待ちしております。お問い合わせは q-a@kuins.kyoto-u.ac.jp までお願いいたします。(件名に【無線 LAN 基地局設置】と御記入いただけますと幸いです。)

今回、別記事にて「SSH Port Forward サーバを利用する方法 (Windows Vista 編及び Mac OS X 編)」を掲載しております。前号では Windows XP に関する設定でしたが、今回は Windows Vista 及び Mac OS X での設定方法を記述しました。無線 LAN 利用時にもお使いいただけますので、是非御活用下さい。

今回 KUINS 側で設置しました場所以外に部局で追加設置される際、部局で購入された無線 LAN 基地局が KUINS 仕様であり、部局としての要望がありましたら、その基地局を KUINS 管理に移管することが可能です。現在 KUINS で導入している無線 LAN 基地局は AT-TQ2403 です。御検討されている場合は、まずは q-a@kuins.kyoto-u.ac.jp までお問い合わせ下さい。

(iPhone 及び iPod Touch ユーザの方々へのお知らせ)

6月18日に iPhone OS 3.0 がリリースされましたが、3.0 にアップデート後、みあこネットへの接続が出来ないというお問い合わせを複数件いただいています。この問題に関しましては、現在 Apple に問い合わせ中ですので、しばらくお待ち下さい。なお、eduroam では利用可能ですので、iPhone 及び iPod Touch ユーザの方々はこちらをお使い下さい。(マニュアルに関しては、用意させていただきますので、今しばらくお待ち下さい。)

宇治地区生存圏研究所木質材料実験棟(木質ホール)への無線 LAN 設置について

宇治地区事務部総務課
総務・企画広報グループ

7月上旬に宇治地区生存圏研究所 木質材料実験棟(木質ホール) 3階セミナー室に無線 LAN アクセスポイントが設置されました。木質材料実験棟(木質ホール)は生存圏研究所所属の建物ですが、3階セミナー室は部局の枠を超えて宇治地区構成員共通の会議室として利用されています。ただし、セミナー室自体は共通として利用していますが、手軽に自由に誰もが利用できるネットワークの構築という点では課題がありました。このことから、宇治地区構成員の強い要望もあり、情報環境部及び宇治地区関係教職員の協力のもと、安全かつ簡便に利用出来る無線 LAN アクセスポイントの設置を実現できました。

通信エリアは3階セミナー室、3階会議室、2階大部分と、1階階段付近で、みあこネット及び eduroam 両対応となっています。通信自体は教育用コンピュータシステムアカウント(ECS-ID)を利用し、PPTP 接続(詳細な設定方法については KUINS ホームページをご参照ください)にて認証と通信経路の暗号化を行いますので、安全かつ信頼できるネットワーク構成となっています。また、ゲストアカウント(KUINS ニュース No.52 および No.63 を参照)の発行によりビジターの方もご利用になれますので、シンポジウムや学会等開催の際にはたいへん便利です。

今回の無線 LAN アクセスポイントの設置は宇治地区においては、電話庁舎、本館 E 棟 326 号室防災研究所セミナー室に続き 3箇所目となります。今後、宇治地区においては、10月竣工予定の宇治おうばくプラザきはだホールにも同様に設置予定であり、宇治生協にも設置計画が進行中です。

最後になりましたが、今回の無線 LAN アクセスポイントの設置にあたりご尽力いただきました情報環境部及び宇治地区関係教職員の皆様に心よりお礼を申し上げます。

平成 21 年度の KUINS 機器更新予定に関する続報

KUINS ニュース No.65 にてお知らせしておりましたとおり、今年度、学内のスイッチの大幅な入れ替えを予定しております。この入れ替えに関して、設計の最適化を行い、必要設置台数を絞ることができました。この結果、執行予定額に余裕ができましたので、入れ換え対象構内に吉田南構内を追加することが出来ました。結果として、入れ換え対象となるのは、北部、吉田南、医学部、病院、病院西、宇治、犬山、熊取、大津の各構内で、総合計 602 台の館内スイッチ・末端スイッチが入れ換えとなります。

今回のスイッチ入れ換えにより、情報コンセントまでの接続速度が 100Mbps から 1Gbps へと高速化します。また、このスイッチではアクセスネットワークとしてサービスしている IEEE802.1X の技術が利用できるようになりますので、認証されたユーザにのみ通信を許可するといったことが可能となり、セキュリティ面でも改善されることとなります。

今後、10 月初めから 3 月末にかけて各構内ごとに館内スイッチ・末端スイッチの入れ換えを順次実施する事になります。入れ替えの対象となる皆様には、ネットワークの停止等でご迷惑をおかけしますが、ご理解とご協力をお願いいたします。

不在になった教職員の KUINS 接続機器登録データベースからの削除について

KUINS 接続機器登録データベース（以下、「KUINS データベース」という）への接続アカウントは、原則として本学の教職員のみにて発行しております。従いまして、情報環境機構では、事務局管理の人事データと KUINS データベースのアカウントデータを定期的に照合し、不在となった教職員は速やかにデータベースから削除しております。ところが、削除対象者が管理責任者、支払責任者等の責任者になっているため、すぐには削除できない場合があります。そのような場合は、同一機器の他の責任者や、部局のネットワーク担当者等、適切と思われる方にお尋ねし、後任の方への変更手続きを行っております。このような事情で、皆様の所へもお問い合わせする場合がありますが、ご協力下さいますよう、お願い致します。また、できるだけ退職や異動前に、後任の方への引き継ぎを KUINS データベース上で行って頂きますよう、こちらもご協力をお願い致します。

SSH Port Forward サーバを利用する方法 (Windows Vista 編及び Mac OS X 編)

KUINS ニュース No.65 でも御案内しましたように、自宅から学内限定サービスに接続するための手段として、「PPTP サーバを利用する方法」以外に「SSH Port Forward サーバを利用する方法」があります。ブロードバンドルータが VPN パススルーに対応していないという理由で、前者が利用出来ない場合に有効です。それ以外にもみあこネット対応無線 LAN 基地局に接続する場合にも利用出来ます。

今回は Windows XP での設定のみの紹介でしたが、今回 Windows Vista 編と Mac OS X 編を用意しました。いずれの場合もフリーソフトのみで設定可能です。(Mac OS X に関しては、ターミナルでも利用可能ですが、コマンドラインに抵抗のない方向けです。)

両者のマニュアルを KUINS ホームページ上 (トップページ → 「KUINS 利用に関する情報」 → 「学外から学内限定サービスを利用する方法 (SSH port forward および PPTP を利用する方法)») に用意しましたので、御参照下さい。

KUINS 会議日誌

平成 21 年 5 月 31 日～平成 21 年 8 月 30 日

情報環境機構 KUINS 運用委員会

平成 21 年 6 月 10 日 (平成 21 年度 第 3 回)

- 無線 LAN の管理について
- KUINS ニュースの発行について
- 平成 21 年度概算要求+アクションプラン調達について
- KUINS の今後の整備について
- kyoto-u ドメイン申請
- KUINS 無線 LAN アクセスポイントの状況報告
- KUINS 状況報告
- その他

平成 21 年 7 月 29 日 (平成 21 年度 第 4 回)

- KUINS 光ファイバー借用について

- 無線 LAN の設置場所希望調査について
- サブドメイン管理責任者調査について
- KUINS ニュースの発行について
- 平成 21 年度 KUINS 予算について
- 平成 21 年度概算要求+アクションプラン調達について
- kyoto-u ドメイン申請
- 遠隔地設置 YAMAHA ルータの脆弱性対応について
- 平成 21 年度耐震改修工事対象建物
- KUINS 無線 LAN アクセスポイントの状況報告
- KUINS 状況報告
- その他

お知らせ

KUINS ニュースへの寄稿を歓迎します。詳細は kuins-news@kuins.kyoto-u.ac.jp
または下記までお問い合わせください。

問い合わせ先

情報環境部 情報基盤課 ネットワーク・遠隔講義支援グループ (075-753-7841, 7432)