

KUINS ニュース No. 71

京都大学 情報環境機構 KUINS 運用委員会

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



京大生協カンフォーラ (左) と楽友会館 (右)

目 次

京都大学情報環境機構講習会開催報告.....	856
第6回京都大学情報環境機構 KUINS 利用負担金検討委員会報告.....	856
ポットネットを通じた犯罪の加害者にならないために.....	856
学外にメールサーバを設置する際の注意について.....	858
PubMed の認証システム対象化について.....	859
SINET4 への移行について.....	859
ソフトウェアライセンスの適正管理の徹底について.....	860
「PPTP-VLAN 固定接続サービス」利用の案内.....	861
認証付き情報コンセントサービスのご案内.....	864
SSL-VPN 接続サービスの試行について.....	865
SSH ポートフォワーディング接続サービスのSPS-ID 対応について.....	865
無線 LAN 基地局に関するお知らせ.....	865
京都大学生協 食堂施設の無線 LAN 接続環境について.....	866
京都大学楽友会館の無線 LAN アクセスポイントについて.....	866
国立情報学研究所の提供するテレビ会議用 MCU 予約サービスとの連携.....	867
「livedoor Wireless」の学内実証実験について.....	870
衛星ブロードバンドシステムを利用した遠隔地接続実証実験.....	870
桂キャンパスのスイッチ交換について.....	871
KUINS 会議日誌.....	872
お知らせ.....	872

京都大学情報環境機構講習会開催報告

去る平成 22 年 10 月 7 日 (木)、今年度 2 回目の情報環境機構講習会を開催しました。今回も、新たに京都大学の構成員になられた皆様に情報環境機構のサービス全体を把握して頂き、情報基盤利用開始にかかる皆様の手間をなるべく軽減するために開催しました。KUINS 以外に講習を行った内容は、「教育に係わる情報環境」、「ホスティングサービス・ホームページサービスと全学メールサービス」、「情報セキュリティ対策の心得」です。今回も、希望があった宇治地区、熊取地区へ遠隔配信を行いました。参加者数は、合計 47 名 (吉田 43 名、宇治 3 名、熊取 1 名) でした。今後も講習会を充実させて行くよう努力しますので、今後周囲に新規着任される方がおられましたら、是非受講をお勧め下さいますよう、お願い致します。

第 6 回京都大学情報環境機構 KUINS 利用負担金検討委員会報告

平成 22 年 11 月 15 日 (月)、事務本部棟 5 階大会議室において、KUINS 利用負担金検討委員会が開催されました。本委員会は、KUINS 利用負担金規程を審議することを主な目的とし、予算や運用方針の審議、KUINS の現状報告なども同時に行われることになっています。

例年同様、接続状況やネットワークサービスの実施状況報告、今後展開するサービスプランの説明等を行いました。また、情報環境機構情報セキュリティ対策室の業務報告、情報環境機構がサービスしている全学メール概説及び情報環境機構・学術情報メディアセンター組織改革の骨子説明がありました。さらに、全学で検討されている全学委員会の見直し話題にも触れ、KUINS 利用負担金検討委員会を対象となっている事も報告されました。

最後に負担金額についての審議が行われ、平成 23 年度も、負担金額を現在と同じく一月当たり KUINS-II アドレス 1,500 円、KUINS-III 情報コンセント 300 円とすることが認められました。

ポットネットを通じた犯罪の加害者にならないために

力武 健次
学術情報メディアセンター 連携研究部門
情報セキュリティ分野 (機構連携)
(情報セキュリティ対策室 運営委員会委員長)

最近「ポットネット」(Botnet) を使った犯罪が増えています。ポットネットの「ポット」(Bot) とは、悪意の攻撃者からの指示によって動作するコンピュータウイルスの一種です。この攻撃者は、時に数十万台から数百万台にも達する、ポットに感染したコンピュータのネットワークである「ポットネット」を操って、さまざまな攻撃を仕掛けます (図 1)。

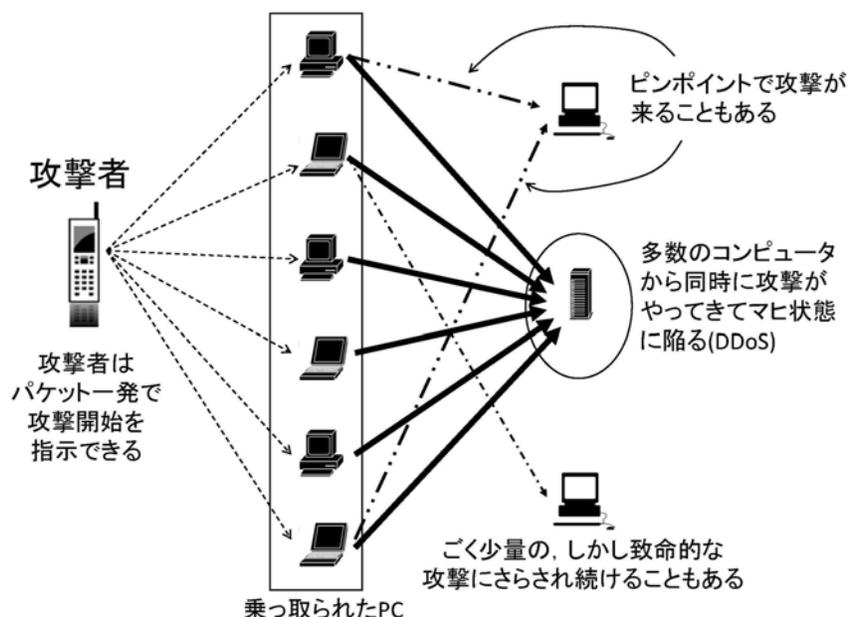


図 1. ボットネットを使った攻撃の仕組み

ボットネットによる典型的な攻撃のパターンとして、特定の Web サイトに大量の攻撃パケットを送信し動作不能にする「分散サービス不能 (DDoS) 攻撃」や、個人情報の不正取得などのために悪意のあるサイトへ利用者を誘導するフィッシング行為を目的とした「大量の迷惑メールの送信」があります。その他にも、攻撃可能なホストを探るための探索や、ボットネット自身の拡大を目的とする既知の脆弱性を利用したシステム侵入の試みなど、実にさまざまな攻撃が行われています。

ボットネットによる攻撃の恐ろしさの 1 つは、ボットに感染したコンピュータを遠隔操作で操っているため、誰が攻撃を仕掛けたかが直接わからないことです。攻撃を受けた側からはボットネットのコンピュータ群だけが攻撃元として判明するにすぎず、そのボットネットを誰がどう操ったかの証拠を収集することは大変困難です。

また、ボットに感染したコンピュータの利用者や管理者は、間接的とはいえ「ボットネットによる犯罪の加害者」となってしまいます。仮に大学の中のコンピュータがボットネットに使われたとなると、大学の管理責任までが問われかねません。

ボットに感染する典型的なパターンは、他のコンピュータウイルスと同様、以下のものがあります。

- ・コンピュータの基本ソフトやアプリケーションの脆弱性を利用して、ネットワークを介して感染するもの
- ・メールの添付ファイルをクリックして開くことにより感染するもの
- ・Web ブラウザで特定のページを閲覧することにより感染するもの
- ・迷惑メールの中に組込まれた URL へアクセスすることで感染するもの
- ・USB メモリ、デジタルカメラ、デジタル音楽プレーヤ、携帯電話など USB 外部記憶装置の機能を持つ装置を介して感染するもの

ボットの特徴は、「感染していることに気づきにくい」ことです。ボットは潜伏して活動することを目的としており、利用者が日常的に行う業務にはできるだけ影響を与えないよう行動します。また、昨今のコンピュータは性能が向上しており、従来のコンピュータウイルスのように性能低下だけでは感染がわかりにくいようになっています。また、ボットの多くはより高機能なものに自動更新する機能を持ち、その種類も多く、ウイルス対策ソフトウェアでの発見を困難にしています。

ボットネットに自分のコンピュータを利用されないためには、日頃からコンピュータの脆弱性対策を十分にしておくことが必要です。ウイルス対策ソフトやその定義ファイルは、常に最新のものを使いましょう。また、Windowsなどの基本ソフトも、自動更新などの機能を利用して常に最新の状態に保っておくことが必要です。もしボットネットの活動が疑われる場合、あるいは被害に遭ったことが疑われる場合は、速やかに情報セキュリティ対策室までご連絡ください。

[参考文献ならびに関連情報]

- ・サイバークリーンセンター: ボットとは
(<https://www.ccc.go.jp/bot/index.html>)
- ・情報環境機構 情報基盤部 情報セキュリティ対策室
(<http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/index.html>)
email: i-s-office@iimc.kyoto-u.ac.jp
電話: 075-753-7490/7491/7492
- ・情報セキュリティ対策室 セキュリティ関連情報
(<http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/whatsnew/security/>)

学外にメールサーバを設置する際の注意について

kyoto-u.ac.jp 配下のサブドメインを利用されていて、部局や教室などでメールサーバを外部委託しているケース (Gmail 等) があります。元々、メールサーバは 130.54.0.0/16 や 133.3.0.0/16 のような学内グローバル IP アドレスを持っていることを前提にしています。その前提で KUINS が提供しているウィルスチェックサーバや送信用サーバ等のメールサーバ群が設計されています。

このため、通常通り KUINS-II 上の IP アドレスを設定してメールサーバを運用されている場合は問題が発生しませんが、学外のメールサーバを利用している場合は IP アドレスが本学以外のものになるため、正しく配送されないというトラブルが発生します。外部委託される場合、業者等が『DNS サーバの A レコードと MX レコードを変更していただければお使いになれます』と謳っているケースがありますが、KUINS 内部のネットワーク設計と整合性が取れなくなりますので、上記のような問題が発生し、ユーザの方々がメールを受信出来なくなってしまうという事態に発展する恐れがあります。

以上のような事情がありますので、外部委託を検討される前に、学術情報基盤グループの転送サービスと、最終的なスプール用に全学メールを組み合わせることを検討ください。また、どうしても外部委託を行わなければならない場合は、情報環境部 ネットワークグループまで、事前にご相談ください。

本件に関する御相談およびお問い合わせ先は、以下の通りです。

本記事の内容一般:

- ・お問い合わせ先: q-a@kuins.kyoto-u.ac.jp

学術情報基盤サービス:

- ・ホームページ: <http://www.iimc.kyoto-u.ac.jp/ja/services/whs/>
- ・お問い合わせ先: whs-qa@media.kyoto-u.ac.jp

全学メール:

- ・ホームページ: http://www.iimc.kyoto-u.ac.jp/ja/account/system/kumail_system.html
- ・お問い合わせ先: kumail-qa@mail2.adm.kyoto-u.ac.jp

PubMed の認証システム対象化について

情報環境機構
図書館機構

本年 12 月から PubMed の利用に認証が必要になりますので、お知らせいたします。PubMed は、米国国立医学図書館が無料公開している医学生物学分野の文献データベースです。学内のネットワークから利用される場合は、12 月から ECS-ID または SPS-ID とパスワードで認証していただくことになりました。12 月からの 2 ヶ月間は試行として行い、調整のうえ支障がなければ来年 2 月から本運用とします。

PubMed の検索結果から続けて、有料の電子ジャーナル本文をご覧になる場合、あらためて ID/パスワードを入れていただく必要はありません。また、EndNote からの PubMed 検索機能のように、PubMed の公開インターフェースを使った機能については、従来どおりお使いいただけるようにいたします。

この度の認証導入の経緯について、以下に御説明いたします。

- ・ PubMed も、電子ジャーナルと同様、多量アクセスを理由にアクセスを遮断されることがあります。本年 5 月には 5 日間、2006 年 6 月には 2 週間も遮断され、本学の研究・教育活動に大きな影響がありました。
- ・ 遮断の解除には、発生原因の調査と提供元への報告が必要です。しかし IP アドレスなど出版社から通知されるわずかな情報では、発生元の特定に時間がかかってしまいます。
- ・ PubMed を認証システムの対象とすると、すみやかに発生元を特定できるため、遮断の早期解決を図ることができ、教育・研究活動への影響を最小限に抑えることができます。
- ・ PubMed へのアクセスが遮断された場合の影響の大きさと、前項の効果を比較検討した結果、この度の措置を実施することになりました。

なお、本件に関するご質問等がございましたら、附属図書館情報管理課電子化推進グループ（電子メール：ejdb@kulib.kyoto-u.ac.jp）までご連絡ください。

SINET4 への移行について

KUINS ニュース No.70 でお知らせしております通り、京都大学が学外との接続用回線として使用している「SINET3」回線（国立情報学研究所（NII）が運営）が、高速化・高信頼化等を目指した「SINET4」回線に移行することになり、平成 23 年 4 月から運用開始されることになりました。この切り替えに伴い、京都大学の SINET 接続に以下のような変更が生じます。

- ・ 宇治キャンパスに設置されていたノードが廃止
- ・ 京都大学に設置されていた SINET ノードが京都データセンターに移設（ただし、当初は現在の接続とそれほどの変化はない）
- ・ 霊長類研究所、理学研究科附属飛騨天文台、防災研究所地震予知研究センター上宝観測所にて、ネットワーク停止が伴う切替作業を実施

なお、下記日程にて、学外との通信停止を伴う作業が発生する予定です。

- ・ 平成 23 年 2 月 22 日に、霊長類研究所のネットワーク停止が伴う接続変更作業
- ・ 平成 23 年 3 月 5 日に、京都大学全体のネットワーク停止が伴う接続変更作業
- ・ 平成 23 年 3 月 13 日に、理学研究科附属飛騨天文台、防災研究所地震予知研究センター上宝観測所のネットワーク停止が伴う接続変更作業

詳細につきましては、KUINS 運用委員会ホームページに掲載しますのでご覧ください。

ソフトウェアライセンスの適正管理の徹底について

情報環境機構情報システム管理センター

市販のソフトウェアについては、著作権者の許諾を得た正規のライセンスを有するソフトウェアのみを使用する事を社会から求められています。そのため、組織はその所属する職員に市販のソフトウェアを使用させるにあたり、ソフトウェアが正規のライセンスを有する事を証明しなければならず、適正管理に努めなければなりません。

本学のソフトウェアライセンスの適正管理への取り組みにつきましては、平成 20 年 6 月から事務組織に所属する職員の日常使用する PC にインストールされているソフトウェアを対象として実施しています。すでに 2 年を経過しますが、事務組織の職員を対象として実施しているだけでは、本学がソフトウェアライセンスの適正管理に努めていると社会に対して主張する事ができず、そのためどうしても教育研究に携わる方々の協力が必要となってきました。

本年 4 月に情報担当理事により、「ソフトウェアライセンスの適正管理の徹底について」を策定し、翌 5 月に開催された部局長会議で報告していただいたところです。以後、京都大学に所属する全ての教職員等を対象として、ソフトウェアライセンス管理を実施する運びとなりました。

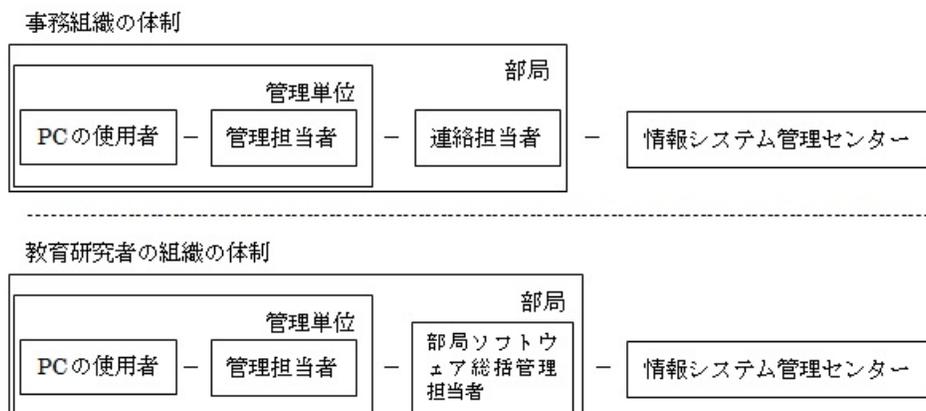
ソフトウェアライセンス管理の目的は、大きく分けて二つあります。一つは、ソフトウェアの不正（違法）コピーを行いにくい仕組みを構築すること。二つ目は、教育、研究、事務に必要なソフトウェアは正規の手続きを以て利用できるようにすることです。

対象となるソフトウェアは、本学がライセンスを持つ有償のソフトウェアの内、教職員の方々が日常使用する PC（メール・Web 検索・文書作成等で利用される PC）にインストールされているものを指し、実験、計測、制御用の PC にインストールされ PC のハードウェアとともに管理されているソフトウェアは対象としません。また、特定のシステムの端末として使用されている PC についても、ハードウェア、ソフトウェアともにシステムの一部とみなされ、システム全体を特定の管理者が管理されているので対象としません。さらに、教育用として、広く開放している PC のソフトウェアについても、特定の管理者が管理されているので対象としません。

ソフトウェアライセンス管理を実施する体制ですが、

- (1) 事務組織が既に実施後 2 年を経過していること。
- (2) 教育研究者の組織には事務組織の場合と異なり、個人所有の PC も利用されていること。
- (3) 既にソフトウェアライセンス管理を独自の方法で実施されている研究室（分野）があること。
- (4) 組織の改編に即応できるようにすること。

等を踏まえて、既に事務組織の中で実施されている教育研究者の組織を除いて、事務組織の体制と教育研究者の組織の体制に分けて実施していただくことになりました。



事務組織では、一般の会社組織で広く行われている方式を参考にし、全学で統一して支援ツールの ASSETBASE ((株)内田洋行製) を使用してライセンス管理を実施しています。

教育研究者の組織には、様々な形態があり、事務組織のように統一した方式を適用する事は困難と考え、選択制といたしました。部局でライセンス管理の単位を定めていただき、その管理単位ごとに、支援ツールを使用してライセンス管理を実施するか、または独自の方法で実施するかを決めていただくこととし、また、部局全体で支援ツールを使用しないで部局独自の方法で管理していただくことも選択肢の一つとしました。

支援ツールを使用する又は独自の方法で実施のいずれの方法を選択していただいても、その後のソフトウェアの管理は各部局にお任せしています。

ライセンス管理の具体的な方法は、管理単位に置かれた管理担当者がインストール管理台帳(個々のPCごとにインストールされているソフトウェアを管理する台帳)を用意し、PCの使用者が使用しているPCに、本学が管理すべきソフトウェアがインストールされているかどうかを調べ、インストールされている場合、その使用者のPCの情報とソフトウェアの情報を台帳に登録するとともに、正規のライセンスを有する事を証明する書類(ライセンス証書)を保有しているかを調査・照合し、その結果を台帳に記載いたします。支援ツールを使用する場合は、このインストール管理台帳はシステムの中に存在します。

また、定期的にソフトウェアの使用状況を部局単位で取りまとめて、情報システム管理センターへの送付をお願いしています。報告の時期は、事務組織では、9月末と2月末、教育研究者の組織では、2月末とさせていただきます。この報告により、使用されているソフトウェアの状況とライセンスの保有状況を確認するとともに、過去の経過から、ライセンス管理の状況の推移を確認していきます。

本件に関するお問い合わせは、情報環境機構 情報システム管理センター

ホームページ：<http://www.iimc.kyoto-u.ac.jp/ja/services/ismc/>

メール：ismc@mail2.adm.kyoto-u.ac.jp

までお願いいたします。

「PPTP-VLAN 固定接続サービス」利用の案内

KUINS ニュース No.70 でお知らせしていますように、KUINS は 2010 年 10 月 1 日より、新サービスとして「PPTP-VLAN 固定接続サービス」の提供を開始しました。すでに、多くの研究科、研究所等でご利用いただいております。

PPTP-VLAN 固定接続サービスとは、従来の PPTP 接続サービスでは出来なかった、学内の各研究室・部局の KUINS-III VLAN へのアクセスを学内・学外の場所を問わず(注1)可能にするものです。この接続を行うと、学内の個別の VLAN に接続しているのに準じた接続環境となり(注2)、VLAN 内に設置されている各種サーバ、ネットワーク接続ストレージ(NAS)、プリンタ等のネットワーク機器にそのままアクセス出来るようになります。

(注1) KUINS の PPTP サーバにアクセス出来る環境であることが前提です。

(注2) ただし、端末側で見える KUINS-III の IP アドレスと、接続先 VLAN で通信に利用する IP アドレスは異なります。(後述)

サービスの概要については、KUINS ニュース No.70 もしくは KUINS ホームページの「PPTP-VLAN 固定接続」のページをご覧ください。今回は本サービスの仕組みと、申請方法についてお知らせします。

PPTP-VLAN 固定接続の仕組み

このサービスで利用する VLAN 固定方式の PPTP 接続は、接続した PPTP サーバで VLAN 番号と利用者 ID の組み合わせによる認証を行い、NAT 機能でその VLAN のプライベート IP アドレスを提供することで利用者が VLAN へ直接アクセス出来るようにするものです。

従来の PPTP 接続 (図 1) は、

- ・ 利用者の端末から、学内の PPTP サーバへ接続する
- ・ PPTP サーバから認証サーバへアカウント情報 (ECS-ID もしくは SPS-ID) を問い合わせる
- ・ 認証成功後、PPTP 接続専用の KUINS-III VLAN の IP アドレスを割り振り、通信を開始する

という方法で学内のプライベート IP アドレスを提供し、その結果学内からの接続でのみ利用可能な電子ジャーナルやグループウェアにアクセス出来るようになります。しかし、個別の研究室・部局の KUINS-III VLAN とは別の VLAN であるため、それらの VLAN 内にある端末・ネットワーク機器にはアクセス出来ません。

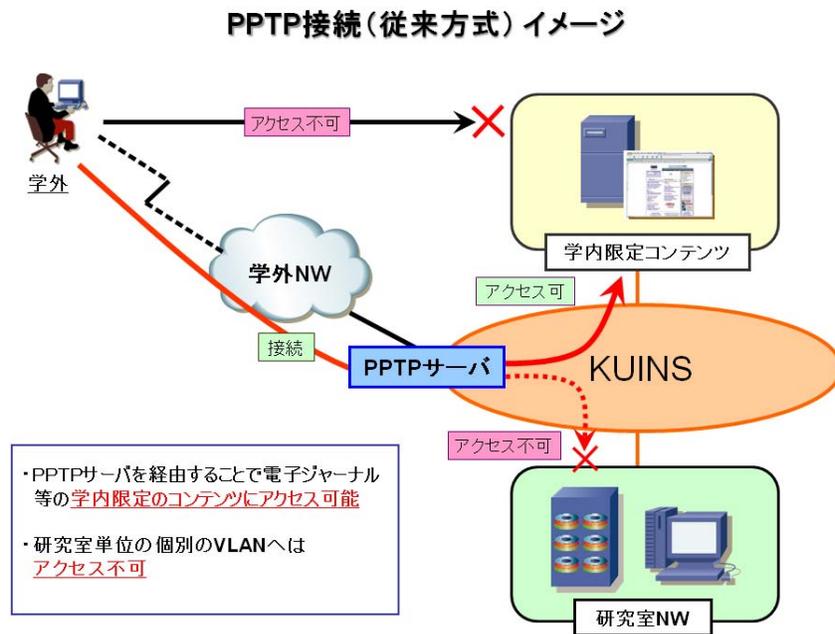


図 1. 従来の PPTP 接続のイメージ

PPTP-VLAN 固定接続 (図 2) では以下のような方法で個別の VLAN へ接続します。

- ・ 利用者の端末から、学内の指定された PPTP サーバへ接続する
- ・ PPTP サーバから認証サーバへアカウント情報 (ECS-ID もしくは SPS-ID) を問い合わせる
- ・ 認証成功後、PPTP 接続専用の KUINS-III VLAN の IP アドレスを割り振る
- ・ IP filter(NAT) 設定スクリプトにより、VLAN 固定接続用の登録リストファイルを参照する
- ・ 登録リストでの認証が成功すると、リストの情報を元に NAT アドレスが設定され、接続先 VLAN のプライベート IP で通信が可能になる

このように、NAT インターフェースを介することで、通信時に [PPTP 接続専用 VLAN の IP アドレス] が [個別の研究室・部局の VLAN の IP アドレス] に変換され、接続した VLAN 内への外部からのアクセスが可能となります。ただし、この方法を利用するためには 4. の VLAN 固定接続用の登録リストに「VLAN の ID」と「ECS-ID もしくは SPS-ID」がセットで登録されている必要があります。

PPTP接続 (VLAN固定方式) イメージ

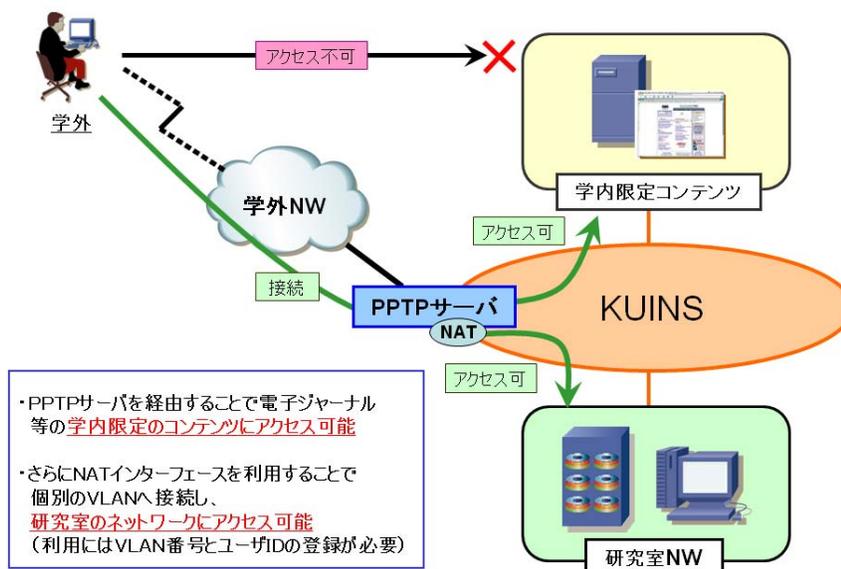


図2. PPTP-VLAN 固定接続のイメージ

サービスの申請方法

PPTP-VLAN 固定接続を利用したい VLAN の管理責任者より、下記の情報を明記したメールを q-a@kuins.kyoto-u.ac.jp 宛に送信してください。メールの件名は「PPTP-VLAN 固定接続 利用申請」にしてください。このサービスは、ここで申請した VLAN と利用者 ID の組み合わせでのみ利用可能です。

- ・ VLAN が属する構内
- ・ VLAN 番号 (VID)
- ・ VLAN 管理責任者名
- ・ 利用者全員の SPS-ID もしくは ECS-ID
- ・ このサービスの利用に関する担当者名と連絡先

登録及び PPTP サーバへの反映は毎週 1 回行ないます。VLAN と利用者 ID の登録が完了次第、管理責任者及び担当者へメールで連絡します。申請は、KUINS 接続機器登録データベースに登録されているメールアドレスから送っていただきますようお願いいたします。

セキュリティ上、利用者の選定は慎重にお願いします（必ず VLAN 管理責任者の承認のもと行って下さい）。VLAN 固定接続をすることによって、VLAN 間通信を設定している VLAN にもアクセスできるようになりますので注意が必要です。利用者の ID は年度末ごとにリセットして、登録解除します。引き続き利用される場合は、継続申請を出していただく必要がありますので、その際にはまた案内を出します。

すでに登録された VLAN に利用者を追加する場合は、メールの件名に「PPTP-VLAN 固定接続 利用者追加申請」と明記の上、VLAN 番号 (VID)、VLAN 管理責任者名、利用者の SPS-ID もしくは ECS-ID を送信してください。利用者を削除する場合は、件名を「PPTP-VLAN 固定接続 利用者削除申請」としてください。

なお、これらの利用申請は、将来的には KUINS 接続機器登録データベースから行えるようにする予定です。

本サービスの提供範囲

北部構内、本部北構内、本部南構内、吉田南構内、医学部構内、病院構内、薬学部・病院西構内、宇治地区、桂地区の 9ヶ所の構内に属する KUINS-III VLAN への接続が可能です。

PC の設定方法

PC 端末の設定方法は従来方式の PPTP 接続とほぼ同様ですが、「サーバホスト名」と接続時の「ログイン ID」が異なります。登録完了時に発送するメールにてそれぞれお知らせします。

是非、PPTP-VLAN 固定接続サービスを研究活動にご活用下さい。本サービスに関する情報は KUINS ニュース及び、KUINS ホームページの「PPTP-VLAN 固定接続」のページでお知らせします。

認証付き情報コンセントサービスのご案内

KUINS ニュース No.70 でお伝えした新サービスの一つ「アクセスネットワークにおける Web 認証サービス・MAC アドレス認証サービス」について、名称を改め「認証付き情報コンセントサービス」としました。本記事ではそのサービス内容についてご案内致します。

現在、講義室や会議室など学内のオープンスペースでのインターネット接続は、OPEN 設定の情報コンセントや無線 LAN アクセスポイント機器を介して、PPTP 接続で利用していただいております。この度 PPTP 接続に代わる接続方法として、認証付き情報コンセントを用いた接続サービスを開始することになりましたので、お知らせいたします。このサービスは、教職員、学生、学外利用者の方にご利用いただけます。

接続方法は 2 つあります。どちらの接続方法も、セキュリティ上の問題から有線のみサービスを提供させていただきます。

1. 貸出スイッチによる接続 (図 1 左)：機構からスイッチを貸し出します。そのスイッチを認証付き情報コンセントに接続し、そのスイッチの下流に端末をつないで頂くと、あらかじめ設定された KUINS-II サブネットまたは KUINS-III VLAN に接続されます。
2. Web 認証による接続 (図 1 右)：認証付き情報コンセントに直接端末を接続します。web ブラウザを立ち上げると、自動的に認証用画面が開きます。そこに、後述の ID とパスワードを入力すると、VLAN に接続されます。



図 1 . 貸出スイッチによる接続 (左) と Web 認証による接続 (右)

Web 認証の ID と接続先は、以下の通りです。また、表中のユーザはいずれも、認証に失敗すると「MIAKO ネット」へ接続されます。

利用者	ログイン ID	接続先
教職員	SPS-ID	KUINS-III close 設定 vlan
学生	ECS-ID	KUINS-III close 設定 vlan
学外利用者（ゲスト）	eduroam	ゲスト用ネットワーク用 vlan

上記のサービス開始は 2011 年 1 月 20 日頃を予定しております。まずは、百周年時計台記念館、芝蘭会館よりサービスを提供し、順次サービスを拡大していきます。詳細は KUINS 運用委員会ホームページに掲載いたします。

SSL-VPN 接続サービスの試行について

KUINS ニュース No.70 において、SSL-VPN 接続サービスの新規導入を御案内しました。この記事中で、サービス開始予定を 11 月 1 日とお知らせしていましたが、スケジュールが予定より遅れております。12 月 1 日より、SPS-ID 保持者を対象に Windows でのみ試行サービスを開始します。詳細は KUINS ホームページ等で御案内致します。

SSH ポートフォワーディング接続サービスの SPS-ID 対応について

SSH ポートフォワーディング接続サービスは、これまで ECS-ID でのみ接続が可能でしたが、平成 22 年 10 月より SPS-ID (教職員グループウェア利用アカウント) でも利用可能となりましたのでお知らせします。これにより、教職員の方が ECS-ID を取得する必要は、ほぼなくなりました。SPS-ID や ECS-ID については、KUINS ニュース No.66 「全学認証基盤の構築 ～全学 ID と統合ディレクトリ～」を御覧ください。

無線 LAN 基地局に関するお知らせ

KUINS ニュース No.70 以降に新たに追加されました無線 LAN 基地局についてお知らせします。

今回は湯川記念館（1 階 Y105 号室）、理学部 5 号館北棟（セミナー室 1、セミナー室 2）、工学部 2 号館（201 号室）、中央食堂（北、南）、カンフォーラ、楽友会館（1 階会議室、1 階軽ラウンジ、1 階食堂、2 階会議・講演室、2 階会議室 3、会議室 5、桂食堂、2 階名誉教授室）、吉田南食堂（1F、2F）、放射能同位元素総合センター教育訓練棟（3 階講義室）、ウィルス研究所分子生物実験研究棟（129 室）、薬学部本館（3F）、薬学部本館南北棟（4F）、東南アジア研究所本館（4F402 号室）、霊長類研究所本館（2 階東側、3 階東側、4 階西側、4 階東側、5 階東側）、霊長類研究所第 2 キャンパス（小野洞）に設置しました。

さらに、室町寮、熊野寮の基地局リプレイスによる eduroam の提供を計画中です。また、情報学研究科においては、研究科設置の既設基地局をみあこネットおよび eduroam 対応へと切り替えて行きます。なお、KUINS 提供の無線 LAN は、11a および 11g の両規格で、みあこネットおよび eduroam の両方を利用できます。しか

し、情報学研究科既設の無線 LAN 基地局は機種が異なりますので、11g でみあこネットのみ、11a で eduroam のみ、利用可能となります。ご了承下さい。

別記事として、京大生協と楽友会館の無線 LAN 基地局について寄稿いただきましたので、そちらも合わせて御覧下さい。

今まで紹介しております一連の作業は、全学インセンティブ経費 アクセスネットワークによる設置の一環として実施中です。講義室や会議室や共同利用者控室等、公共性の高い空間への設置作業を進めております。御希望のある部局担当者様からの御相談・御質問等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。）

今まで KUINS 側で設置しました場所以外に部局独自で追加設置される場合、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、当該基地局を KUINS 管理に移管することが可能です。なお、現在 KUINS で導入している無線 LAN 基地局は、アライドテレシス製の AT-TQ2403 です。部局での設置を御検討されている場合は、上記同様、導入前に q-a@kuins.kyoto-u.ac.jp まで御連絡下さい。

京都大学生協 食堂施設の無線 LAN 接続環境について

京都大学生協生活協同組合

以前より、多くの組合員（＝学内利用者）から、「生協食堂にも無線 LAN アクセスポイントがほしい。」という声をいただいております。2010 年 8 月に、カンフォーラをはじめ、多くの食堂に、KUINS 提供の無線 LAN アクセスポイントが整備されました。学生の勉学・研究、また、研究室・ゼミ単位でのミーティングなどで、十二分に活用いただけると期待いたします。

生協食堂施設の無線 LAN アクセスポイント設置エリアは、下記の通りです。

- ・カンフォーラ
- ・中央食堂
- ・吉田食堂（1 階，2 階）
- ・北部食堂（1 階，2 階）
- ・宇治食堂
- ・桂食堂
- ・カフェテリアルネ

無線 LAN の導入にご協力頂きました情報環境部ネットワークグループの皆様には、心よりお礼申し上げます。

京都大学楽友会館の無線 LAN アクセスポイントについて

総務部総務課

京都大学楽友会館では、2010 年 10 月に KUINS 提供の無線 LAN アクセスポイントを設置しました。

1925 年に本学吉田南地区の近衛通りに面する一角に建築された楽友会館は、このたび、第二期重点事業実施計画の一環で改修され、情報ネットワーク環境の整備を実施し、無線 LAN（みあこネット方式）の導入を実現しました。

全館無線 LAN アクセスを可能とし、ラウンジ・食堂といった共有スペースをはじめ、各会議室においてネットワークへの接続ができることを特徴としています。このことにより、より多くの教職員の方々の会合開催や福利厚生事業の実施、教育研究活動の促進に役立つものと期待しています。

楽友会館の無線 LAN アクセスポイントの設置エリアは、以下のとおりです。

- ・1階会議室
- ・1階軽ラウンジ
- ・1階食堂
- ・2階会議・講演室
- ・2階会議室 3, 会議室 5
- ・桂食堂
- ・2階名誉教授室

国立情報学研究所の提供するテレビ会議用 MCU 予約サービスとの連携

情報環境機構 情報環境部
統合認証センター

京都大学の組織間認証連携シングルサインオンシステム Shibboleth IdP が、国立情報学研究所 (NII) の提供する MCU の予約サービス FaMCUs と連携しました。MCU とは、複数のテレビ会議システムを繋いで、複数拠点間でテレビ会議を行うために利用する装置です。FaMCUs では MCU の予約を教職員からのみ受け付けています。認証には、SPS-ID(教職員グループウェア用 ID) または ECS-ID(教育用コンピュータシステム利用コード:ただし教職員のみ) を利用できます。MCU 利用時は利用者の制限はなく、接続に必要な情報を共有しているメンバーであれば誰でも接続することができます。

1. 予約可能な MCU 装置

2010 年 11 月の時点では、以下の MCU 装置が利用可能です。

- ・ Polycom RMX 2000 (5 ~ 20 拠点:解像度によって異なります)
- ・ Tandberg Codian MCU 4505 (12 拠点)

Tandberg Codian MCU は Windows 用アプリケーションの ConferenceMe を用いた接続も可能です。Firewall や NAT の内側でもテレビ会議に参加することができます。

2. MCU の予約

FaMCUs のサービスを初めて利用する場合は、IdP での認証を受けた後、自分のメールアドレスを登録する必要があります。メールアドレスが実際に有効であることを確認した後、MCU の予約ができるようになります。

教職員であれば MCU の予約を行うことができます。MCU の空き状況を参考に、利用をする日時を予約してください。

予約の際に入力するのは次の項目です。接続端末数が少なければ、他の利用者が別の会議を同時に実施できるので、必要最小限の端末数を予約するようにしてください。

カンファレンス名	会議の名称を入力します
日付	会議を開始する日を入力します
時刻	会議を開始する時間、および終了する時間を入力します。 (最大 24 時間まで設定可能です)
接続予定端末数	2~10, 最大 (最大を指定すると MCU を占有します)
接続サーバ	利用する MCU を選択します
カンファレンスパスワード	4桁程度の暗証番号を入力できます (省略可)。通常は会議室番号による識別で十分ですが、会議をより安全に開催したい場合に指定します

予約が成立すると、上記で指定した情報の他に次の予約情報が表示され、メールでも通知されます。

会議室 IP アドレス	MCU にテレビ会議端末を接続する際に指定するアドレス
会議室番号	自動的に割り当てられた識別番号
代理アクセス URL	本予約に対する権限を委譲するための URL
カンファレンスミー	Tandberg MCU の ConferenceMe で会議室にアクセスするための URL

予約した人は、その予約に対する権限を他の人に委譲できます。委譲したい人に「代理アクセス URL」を通知してアクセスしてもらおうと委譲手続きが完了します。委譲される人は、教職員には限定していませんので、予約した人の責任で委譲してください。

3. 予約の変更・削除

開催前の会議については自由に変更・削除が可能です。開催中の会議の時間延長は可能です。その他の変更については、制約があります (Polycom は端末数の変更ができない等)。

4. MCU への接続 (会議への参加)

会議の参加者は、必ずしも学術認証フェデレーションに参加する機関に属している必要はありません。参加予定者に、予約情報の会議室 IP アドレス、会議室番号、カンファレンスパスワードを通知して下さい。

MCU では、複数の会議を同時に実施することができるため、会議を識別するための会議室番号 (カンファレンス ID) が、それぞれの会議に割り当てられます。会議に参加する際には、テレビ会議端末において、MCU の IP アドレスとともに会議室番号を指定する必要があります。

4.1. 接続時に会議室番号を指定する方法

Polycom VSX/HDX などでは接続先として指定する IP アドレスに続けて会議室番号を指定することができません (内線番号としての扱い、E.164 アドレス)。

例：150.100.12.113##123 (#2 つで区切る) Tandberg Codian MCU から接続 (カスケード) する場合は “##” の代わりに “!” で区切ります。

4.2. 接続した後に会議室番号を指定する方法

接続時に会議室番号を指定しなかった場合は、MCU への接続が完了すると会議室選択画面が最初に表示されます。テレビ会議端末でリモートカメラ制御の状態にしてから、タッチトーン信号を用いて会議室番号を送出し最後に「#」を送出します。

4.3. カンファレンスパスワードを指定する方法

会議室にカンファレンスパスワード (暗証番号) が設定されている場合は、会議室接続時に暗証番号を送信する必要があります。トーン信号を用いて暗証番号を送出し、最後に「#」を送出します。

4.4. テレビ会議端末ごとのトーン信号の送出方法

テレビ会議室システムによってトーン信号を送出する方法が異なります。

Polycom/Tandberg:

ほとんどの機種で、リモコンの#ボタンを押すとタッチトーンを送出できるようになります

Polycom PVX:

ウィンドウ下側にある「通話制御」をクリックして開き「キーパッド」のタブをクリックします

XMeeting:

Tools の Remote Control を選びます

NEC MediaPoint/VisuaLink:

リモコンのポインタボタンを押します

Sony PCS-1:

リモコンの*ボタンを押します。決定ボタンでメニューが消えます

4.5. Tandberg ConferenceMe (Windows 用アプリケーション) の利用による参加

Tandberg Codiam MCU を予約している場合は、ConferenceMe 機能を利用して会議に参加することが可能です。ConferenceMe では、PC が NAT の配下に接続されていても、双方向のテレビ会議接続が可能になります。まず、カメラとマイクのついた PC を用意し、予約情報で指定された URL にアクセスします。

最初にアクセスしたときは、アプリケーションのインストールを行います。「インストーラをダウンロードするにはここをクリック」からインストーラをダウンロードしてインストールしてください。アプリケーションがインストール済みの場合は、「ConferenceMe でカンファレンスに参加するにはここをクリック」をクリックして開始します。

ConferenceMe を起動する前に、同時にインストールされている「Configure ConferenceMe」で利用したいデバイスをあらかじめ選択しておく必要があります。ウィルスバスター等のセキュリティソフトと相性が合わないことがあります。ConferenceMe を使用する場合、通信遅延が若干長めになるようです。

5. Web ブラウザからの MCU 制御

会議の予約者 (権限委譲を受けている者を含む) は Web ブラウザで会議の制御を行えます。MCU の予約画面で、カンファレンス名のリンクを辿ると制御画面が表示されます。なお、制御画面は会議開催中しか表示されません。主な制御は次の通りです。

全端末に対する操作

- ・レイアウト：全ての端末に適用する画面合成のレイアウトを指定します
- ・ビデオミュート：全ての端末からのビデオの受信を停止します
- ・オーディオミュート：全ての端末からの音声の受信を停止します

端末ごとの操作

- ・重要設定：音声切り替えによらず、この端末をレイアウト画面中で大きく表示します
- ・ビデオミュート設定：この端末からのビデオの受信を停止します
- ・オーディオミュート設定：この端末からの音声の受信を停止します

- ・コンテンツチャンネル：この端末に対する映像送信について、カメラ映像か、PC 映像 (H.239) かを切り替えます (端末が H.239 非対応の場合に有効)
- ・切断：この端末との接続を終了します

参加者を追加

- ・IP アドレスとプロトコル (H.323/SIP, 通常は H.323) を指定して、MCU 側からテレビ会議端末を呼び出すことができます。

「livedoor Wireless」の学内実証実験について

学術情報メディアセンター ネットワーク研究部門
高機能ネットワーク研究分野

KUINS ニュース No.70 でお伝えしておりました「livedoor Wireless」の学内実証実験について、以下の場所に対応無線 LAN 基地局が追加されましたので、お知らせいたします。

吉田キャンパス：(本部構内) 中央食堂

桂キャンパス：船井記念講堂，事務管理棟，福利・保健管理棟，プロムナード下，ローム記念館

なお、対応基地局の最新情報は、http://blog.livedoor.jp/ld_wireless2/archives/cat_50051016.html で御覧頂けます。

衛星ブロードバンドシステムを利用した遠隔地接続実証実験

1. はじめに

京都大学には、研究科及び研究所が所有するフィールド観測施設 (以下、遠隔地と呼ぶ) が 70 か所程度設置されています。これら遠隔地の多くは人里から離れており、光ファイバーケーブルはもちろん ADSL 等のブロードバンド回線も使用できません。最近では、一部の遠隔地で地方自治体による CATV (ケーブルテレビ) 回線を利用した接続が行われていますが、未整備箇所が残っています。

しかし、現代社会では、研究や業務の遂行にはインターネット接続は欠かせないものとなっているため、何らかの手立てを講じる必要があります。そこで我々は、インターネットの地上整備の難しい遠隔地でも、衛星を用いた接続は可能ではないかと考え、衛星ブロードバンドシステムを利用した接続実験を行いました。その結果を、ここで簡単に報告いたします。なお、この内容は、平成 22 年 11 月に行われた全国共同利用情報基盤センターの連合発表会で報告しました。その発表原稿に、より詳しい報告がございますので、必要な方はお問い合わせ下さい。

2. ネットワークの構成

使用したのは、2009 年 4 月に日本で利用が開始された IPSTAR 衛星ブロードバンドです。これは、タイ国の衛星を管理運用するタイコム社の子会社である IPSTAR (アイピースター) 社によるサービスで、これまでの衛星通信システムに比べ個人でも手軽に導入が可能な衛星ブロードバンドシステムとなっています。

使用したパッケージは、以下の通りです。

- 契約回線：IPSTAR Pro
- 通信最大速度：ダウンロード 3Mbps/アップロード 1Mbps
- 固定 IP アドレスサービス：IP4(使用可能 IP アドレス 1 個)
- 回線使用料：月額 10,000 円 (税別)
- 固定アドレス使用料：月額 6,000 円 (税別)

3. 実験

実験では、衛星ブロードバンド経由で、(1) インターネットへの直接接続、(2) PPTP 接続、(3) SSH ポートフォワード接続、(4) IPSec-VPN 接続の 4 通りを試しました。これらそれぞれの接続形態に対し、(a) スピード計測サイトへのアクセス速度、(b) 京都大学グループウェアへのアクセス速度、(c) 附属図書館電子ジャーナルへのアクセス状況、(d) H.323 に準拠したテレビ会議システムへの接続状況の 4 つを調べました。

詳しいデータは上述の原稿に掲載していますが、要約すると以下のような結果になりました。(a) 速度計測では、(1) および (3) では、衛星回線提供業者のアナウンス通り、ダウンロード 3Mbps、アップロード 1Mbps の速度が達成できました。(2) および (4) では、この 1/4 程度でした。(b) グループウェアへの接続においては、全ての接続形態において、業務に支障のない程度の速度を達成できました。ただし、Web 会議システムを PPTP 接続で利用した場合には、通信断が頻発し、業務に使用できるものではありませんでした。(c) 電子ジャーナルへの接続は、問題ありませんでした。(d) テレビ会議システムの利用に関しては、1 秒程度の遅延があるものの、映像・音声ともに、途切れることなく通信ができました。

4. おわりに

この実証実験により、衛星ブロードバンドシステムは、インターネット地上整備が難しい遠隔地に対するインターネット接続手段として、大いに期待できる情報インフラであることが実証できました。今回使用した衛星ブロードバンドシステムは、タイ、オーストラリア、ニュージーランド等、アジア・太平洋地域で大きく展開されており、京都大学の海外拠点との接続にも利用できる可能性があると思われます。なお、今回の実験では、大学本部を遠隔地と見立て、そこから衛星ブロードバンドを使い性能を検証しました。今後は、遠隔地の協力を募り、実際に現地からのアクセス実験を実施していきたいと思えます。

桂キャンパスのスイッチ交換について

KUINS-III 導入時のスイッチの老朽化に伴い、平成 20 年度に、本学の「アクションプラン」経費により、本部南構内のスイッチの入れ替えを実施しました。また、平成 21 年度には「アクションプラン」経費に加え、概算要求により獲得した経費で、北部、医学部、病院、病院西、宇治、犬山、熊取、大津の各構内のスイッチを入れ替えました。この結果、残るは桂キャンパスのみとなっていました (KUINS ニュース No.68 参照)。

KUINS ニュース No.70 でお知らせしました通り「平成 22 年度インセンティブ経費」が認められましたので、桂キャンパスに設置している保守期限切れスイッチを交換します。今後、12 月初めから 3 月末にかけて桂キャンパスの館内スイッチ・末端スイッチの入れ換えを順次実施いたします。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。

更新対象スイッチに設定されている VLAN 管理責任者・連絡担当者の皆様には、別途更新実施連絡をします。「KUINS 接続機器登録データベース」のメールアドレス登録情報をもとに連絡しますので、もれなく登録していただきますようお願いいたします。

KUINS 会議日誌

平成 22 年 8 月 31 日 ~ 平成 22 年 11 月 29 日

情報環境機構 KUINS 運用委員会

平成 22 年 9 月 13 日 (平成 22 年度 第 5 回)

- 平成 22 年度予算(案)の補正について
- インセンティブ経費(部局)の要求について
- KUINS ニュースについて
- KUINS の新サービスの進行現状について
- インセンティブ経費による調達経過報告
- SINET4 接続回線共同調達結果について
- 附属病院 (kuhp.kyoto-u.ac.jp) へのメール不達について
- KUINS 無線 LAN アクセスポイントの状況報告
- KUINS 状況報告
- kyoto-u ドメイン申請
- その他

平成 22 年 10 月 6 日 (平成 22 年度 第 6 回)

- 第 6 回京都大学情報環境機構 KUINS 利用負担金検討委員会の開催について
- KUINS ニュースについて
- KUINS の新サービスの進行状況について

- 情報環境機構講習会の開催について
- インセンティブ経費による調達経過報告
- インセンティブ経費(部局)の要求について
- KUINS 無線 LAN アクセスポイントの状況報告
- KUINS 状況報告
- kyoto-u ドメイン申請
- その他

平成 22 年 11 月 5 日 (平成 22 年度 第 7 回)

- 第 6 回京都大学情報環境機構 KUINS 利用負担金検討委員会の議事について
- KUINS の新サービスの進行状況について
- KUINS ニュース No.71 の発行
- 情報環境機構講習会の開催結果
- インセンティブ経費による調達経過報告
- インセンティブ経費(部局)の要求について
- KUINS 無線 LAN アクセスポイントの状況報告
- KUINS 状況報告
- kyoto-u ドメイン申請
- 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 ネットワークグループ (075-753-7841, 7432)