

KUINS ニュース

No. 45

京都大学学術情報メディアセンター
情報サービス部ネットワーク担当
<http://www.kuins.kyoto-u.ac.jp/>



マルチメディア遠隔講義システムを利用した講義風景

目 次

| | |
|---|-----|
| マルチメディア遠隔講義システムの運用開始について | 544 |
| ネットワークセキュリティ講習会を開催 | 544 |
| 新規着任教職員のための KUINS 利用方法に関するガイダンスを開催 | 545 |
| 「京都大学情報ネットワーク危機管理委員会要項」の制定について | 545 |
| 「京都大学情報資産利用のためのルール」について | 545 |
| HUB や無線 LAN 接続装置等を KUINS 接続する際の注意事項 | 546 |
| フレッツグループによる遠隔地への KUINS-III 接続サービスの開始 | 546 |
| 安全な通信方式での接続方法 (その 1) - PuTTY で SSH 接続 - | 547 |
| KUINS 会議日誌 | 556 |
| お知らせ | 556 |

マルチメディア遠隔講義システムの運用開始について

桂キャンパスの設置に伴い、桂キャンパス検討作業部会情報ネットワークWGと学術情報メディアセンターとが協力して、新たな遠隔講義システムを構築しました。平成16年4月より運用を開始し、前期は週に6コマの遠隔講義を実施しています。

このシステムの特徴は、2つの高精細カメラと2枚の高解像度プロジェクタからなる高精細映像伝送装置を備えていることです。1280×960画素の解像度で黒板・講師映像、書画カメラ映像、パソコン画面映像を伝送することができます。理工系の特徴である数式も鮮明に遠隔教室に写し出すことができます。また、遠隔教室の様子が講師側教室の後ろに大きく映し出されるため、受講学生の様子を確認しながら講義を進めることができます。

このシステムは、以下の6教室に設置されています。

- 桂 A2 棟 1 階 (化学系) セミナー室 (A2-123)
- 桂 A1 棟 1 階 (電気系) 中講義室 (A1-131)
- 吉田 工学部 4 号館 1 階 高分子化学第 1 講義室
- 吉田 工学部 電気総合館 3 階 中講義室
- 吉田 学術情報メディアセンター北館 3 階 大会議室
- 宇治 生存圏研究所大会議室 (旧、宙空電波科学研究センター 1F 会議室)

これら6教室の間は自由な接続が可能であり、講義担当講師がどの教室からでも講義を発信することができます。これにより、教員や学生が分散キャンパス間を移動する時間と労力が軽減され、専攻や研究科の枠を越えた講義をより開講・受講しやすくなります。

なお、利用、見学を希望される方、また、資料を希望される方は、下記までご連絡下さい。

学術情報メディアセンター 情報サービス部ネットワーク情報システム担当

連絡先：学内共同利用掛 (南館)

tel: 075-753-9000 fax: 075-753-9001

e-mail: distlearn@media.kyoto-u.ac.jp

<http://www.media.kyoto-u.ac.jp/distlearn/service/>

ネットワークセキュリティ講習会を開催

平成16年3月19日に、学術情報メディアセンター南館2階202号室にてネットワークセキュリティ講習会を開催しました (参加者数87名)。

本講習会では、ネットワークセキュリティにおいて、我が国のセキュリティ分野の第一線でご活躍のお二人 (野川裕記大阪大学講師、西本逸郎株式会社ラック取締役) を講師としてお招きし、大学におけるネットワークセキュリティについてお話をしました。

野川裕記大阪大学講師より、「セキュリティ分野における人材育成：大阪大学の試み」と題して、大阪大学におけるネットワークセキュリティ教育への取り組み方やその問題点等、具体的な例を挙げた講演がありました。また、西本逸郎株式会社ラック取締役からは、「大学で意識すべき情報セキュリティ」と題しまして、ネットワークウイルスの最近の動向やその対策について講演がありました。

講演の後、活発な質疑・応答がなされ、京都大学におけるネットワークセキュリティを考える上で、大変に役立つ情報が得られました。

新規着任教職員のための KUINS 利用方法に関するガイダンスを開催

平成 16 年 4 月 26～28 日に、4 月から新規に京都大学に着任した教職員を対象に京都大学学術情報ネットワークシステム (KUINS) の利用に関する講習会を開催しました。今回は、吉田キャンパス、宇治キャンパス、桂キャンパスと 3 箇所で行いました (参加者合計: 54 名)。

講習内容は、学術情報メディアセンターと KUINS システムに関する概要と KUINS の具体的な利用方法に関する説明を行い、また KUINS におけるセキュリティについて講習も行いました。

なお、講習会の資料等は、

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

でご覧になることができます。

「京都大学情報ネットワーク危機管理委員会要項」の制定について

情報環境部

平成 16 年 3 月 30 日開催の全学情報セキュリティ委員会及び同日開催された部局長会議において、京都大情報ネットワーク危機管理委員会要項が了承されました。

従来情報ネットワーク危機管理委員会は、京都大学学術情報ネットワーク機構 (いわゆる KUINS 機構) のもとに設置されており、内規が定められていましたが、昨年 10 月 21 日開催の部局長会議において「京都大学の情報セキュリティ対策に関する規程」(平成 15 年 10 月 21 日達示第 43 号) が了承され、京都大学に最高情報セキュリティ責任者を置き、そのもとに情報ネットワーク危機管理委員会が設置されることになったことを受け、新しく要項として制定されたものです。

なお、要項は京都大学ホームページの下記のページに掲載されています。

http://www.kyoto-u.ac.jp/top_b/cin2/c-in14.htm

「京都大学情報資産利用のためのルール」について

情報環境部

平成 16 年 3 月 30 日開催の全学情報セキュリティ委員会及び同日開催された部局長会議において、「京都大学情報資産利用のためのルール」が了承されました。

情報倫理に関しては難しい問題があることもあり、これまで京都大学には、学内ネットワークや京都大学の各種情報資産利用にあたって学内構成員が守るべき取り決めは何もありませんでした。しかし、本ルール前文にあるように、京都大学の構成員は、本学の情報資産を利用するに当たり、教育・研究の自由と自主を基礎とした高い倫理性と社会に対する強い責任感が求められることから、本ルールが制定されました。

なお、要項は、京都大学ホームページの下記のページに掲載されています。

http://www.kyoto-u.ac.jp/top_b/cin2/c-in14.htm

HUB や無線 LAN 接続装置等を KUINS 接続する際の注意事項

最近の HUB や無線 LAN アクセスポイント等に、DHCP サーバ機能が搭載された機器が多く存在しています。これらの機器を KUINS に接続する場合、KUINS 側に DHCP サーバ機能が影響しないように設定してくださいようお願いいたします。これを怠りますと、自分たちの VLAN が使用できなくなるだけでなく、KUINS 全体に影響を及ぼす場合がありますので、設置には十分ご注意ください。

フレッツグループによる遠隔地への KUINS-III 接続サービスの開始

KUINS ニュース No.44 でご案内いたしましたように、学術情報メディアセンターでは、NTT 西日本が提供する B フレッツやフレッツ ADSL 等のアクセス回線を利用した、遠隔地での KUINS-III 接続サービスを平成 16 年 4 月より開始しました。接続には、遠隔地において NTT 西日本による B フレッツやフレッツ ADSL 等のアクセス回線への加入が必要となります。このサービスを利用して接続する場合は、次の手順にて申請及び機器の設置をお願いします。

ただし、接続を希望される場合は、事前に学術情報メディアセンター情報サービス部 (内線 7841 or 7432) までご相談下さい。

1. KUINS への申請は、通常の KUINS-III 接続申請により行って下さい (クローズ設定 or オープン設定)。申請方法は、次の URL (<http://www.kuins.kyoto-u.ac.jp/applications/k3vlan/>) の、VLAN 新規設定申請書をメールで送って下さい。
尚、オープン設定・クローズ設定の違いは、次の通りです。
 - オープン設定：講義室などの不特定多数の出入りする部屋で VLAN から外へのアクセスを制限する設定
 - クローズ設定：鍵のかかる部屋で、開室中は常時、教職員が在室していて、ある程度自由に VLAN から外へアクセスできる設定
2. 接続回線 (B フレッツ、フレッツ ADSL 等) は、部局にて申請・設置してください。通常は、プロバイダ契約が必要となりますが、KUINS-III への接続の場合にはフレッツグループ (ビジネスメニュー) というサービスを利用していますので、プロバイダ契約等の別途契約は不要です。
3. リモート (遠隔地側) ルータは、接続予定部局が購入して下さい。ルータの選定は、PPPoE によるグローバル固定複数アドレスの割当に対応し、かつスタティックなルーティングに対応していることなどいくつかの要件があります。設定管理はセンター側にお任せいただく形になりますので、ご購入前にセンターにご相談ください。
現在動作実績があるのは、NEC 製 IX201x および YAMAHA 製 RTX1000 です。
4. リモート (遠隔分室側) ルータの設定は、学術情報メディアセンターにて実施しますので、学術情報メディアセンターネットワーク掛まで送付して下さい。
5. リモート (遠隔分室側) ルータは、日程を相談の上設置して下さい。場合により、学術情報メディアセンターで設置することもあります。

なお、本サービスを利用するための負担金については現在検討中ですが、当面は試験運用として無償提供を予定しています。詳しくは情報サービス部ネットワーク担当までお問い合わせ下さい。

安全な通信方式での接続方法 (その1) -PuTTYでSSH 接続-¹

赤坂 浩一 浅岡 香枝 平野 彰雄
(学術情報メディアセンターコンピューティング掛)

1. はじめに

従来、リモート計算機への接続の際には、telnet や ftp を使うことが主でした。しかし、telnet や ftp では、ユーザ認証を行なうために入力した ID やパスワードが、そのまま平文 (暗号化されない文字列) としてネットワーク上に流れていくため、途中の経路で ID やパスワードを盗聴することが容易になります。盗聴された ID やパスワードが悪用されると、計り知れない被害が発生するかも知れませんので、近年は、telnet や ftp による接続を禁止し、暗号技術を用いた安全な通信方式である SSH (Secure SHell) による接続に移り変わってきています。

SSH による接続を行なうためには、お使いのマシン (UNIX・Windows・Macintosh) に SSH クライアントプログラムを用意する必要があります。UNIX 系 OS の場合、OpenBSD や FreeBSD、Linux の様々なディストリビューションには、標準で SSH クライアントプログラムの OpenSSH が用意され、Macintosh の場合、最新の MacOS X には、標準で OpenSSH が用意されていますので、これらのマシンをお使いの方は、そのまま SSH による接続が行なえます。

Windows の場合、95, 98, Me, NT, 2000, XP のどれでも、各自で SSH クライアントプログラムを用意する必要があり、Macintosh の MacOS X より前の OS、UNIX 系 OS の Solaris も、各自で SSH クライアントプログラムを用意する必要があります。今回は、利用者の多くが使用されている Windows マシンに対応した SSH クライアントプログラムで端末エミュレータの機能を持つ PuTTY を紹介します。

なお、SSH には、バージョン 1 とバージョン 2 の二種類が存在しますが、バージョン 1 にはセキュリティ上の問題が指摘されていますので、必ずバージョン 2 の SSH を利用するようにしてください。

2. PuTTY とは

これまで紹介した Windows マシンに対応した SSH クライアントプログラムとしては、SSH Communications Security 社の SSH Secure Shell for Workstations やフリーソフトウェアの TeraTermPro に SSH クライアント機能を拡張する TTSSH などがありました。有料のソフトウェアである SSH Secure Shell for Workstations は、英語版は非商用での利用に限り無償で利用できますが、日本語版は正規品を購入するしかありませんでした。一方、フリーソフトウェアの TeraTermPro+TTSSH は、日本語環境での使用も満足できますが、バージョン 2 の SSH に対応しておらず、セキュリティの面で少し不安が残りました。

今回、紹介する Simon Tatham 氏らによって開発された PuTTY は、MIT ライセンスで商用・非商用を問わずどなたでも無料で使用できるフリーソフトウェアであり、バージョン 2 の SSH にも対応しており、また、Hideki EIRAKU 氏が、PuTTY で日本語を扱えるようにするパッチを作成し公開されています。

それでは、PuTTY の入手と Windows マシンへのインストール、リモートの計算機にログインするための設定について紹介します。

3. PuTTY の入手とインストール方法

PuTTY の入手は、PuTTY のホームページから行ないます。URL は、以下の通りです。

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

¹本稿は、京都大学学術情報メディアセンター全国共同利用版 広報, Vol.3, No.2, pp.77-86 (2004.03) の解説記事に、KUINS-III から学外の SSH サーバへの接続について加筆を行ったものです。

PuTTY のダウンロードページには、バイナリ形式のプログラムやソースコードなどが公開されていますが、インストーラー付きの実行ファイルを手に入れてください。本稿執筆中 (2004 年 6 月 15 日時点) では、`putty-0.54-installer.exe` が最新版となっていますが、各自がダウンロードするときには、なるべく最新版を手に入れるようにしてください。ダウンロードしたインストーラー付きファイルを実行 (マウスでダブルクリック) するとインストールプログラムが起動しますので、**Next** をクリックしてインストールを開始します。

まず始めに、PuTTY のインストール先を尋ねてきます。差し支えなければ、デフォルトのインストール先である

`C:\Program Files\PuTTY`

にしておきましょう。**Next** をクリックして進みます。

次に、スタートメニューに登録するときの名前を入力します。これもそのまま先に進んでかまいません。インストーラーが日本語対応していないので、日本語のスタートメニューがあった場合文字化けして表示されることもあります。登録に支障はありませんので、**Next** をクリックして進みます。

次のステップでは、スタートメニューに登録するか、デスクトップにショートカットを作るか、PPK という拡張子を持つファイルを Pageant というプログラムに関連づけるか、などを指定します。デフォルトでは、全てにチェックが付いています。ここも変更せず、**Next** をクリックして進みます。図 1 のように、インストール先やオプションの確認を行なったら、**Install** をクリックし必要なファイルのコピーを開始します。

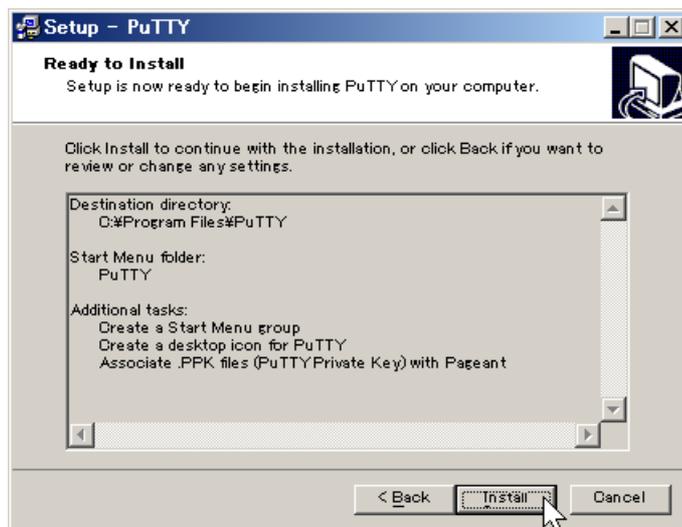


図 1: インストール先やオプションの確認

インストールが終了したことを知らせるウィンドウが表示されたら、**Finish** をクリックして完了です。PuTTY がインストールできました。

4. PuTTY の日本語対応化

続いて、PuTTY で日本語を扱えるようにするパッチを次の URL から入手します。

<http://hp.vector.co.jp/authors/VA024651/download.html>

上記のホームページでは、日本語を扱えるようにするパッチを適用した実行ファイルと日本語メニュー用ファイルとマニュアルファイルの三つのファイルが、ZIP 形式の圧縮ファイルで公開されており、ダウンロードするファイルは、`executable_files` (実行ファイル) にリンクされている ZIP 形式の圧縮ファイルの `puttykjbin.zip` です。本稿執筆中 (2004 年 6 月 15 日時点) では、PuTTY version 0.54 にパッチを適用したものが最新版のようです。

Windows Me,XP をお使いの場合は、標準で ZIP 形式のファイルを解凍 (展開) する機能がありますが、それ以外の Windows 95,98,NT,2000 の場合は、あらかじめ解凍ツールを用意しておいてください。

ZIP 形式の圧縮ファイル (`puttykjbin.zip`) を解凍 (展開) すると、図 2 のように `puttykjbin` という名前のフォルダの中に、`puttyjp.exe`、`puttyjp.lng`、`readme2.html` の三つのファイルに展開されます。

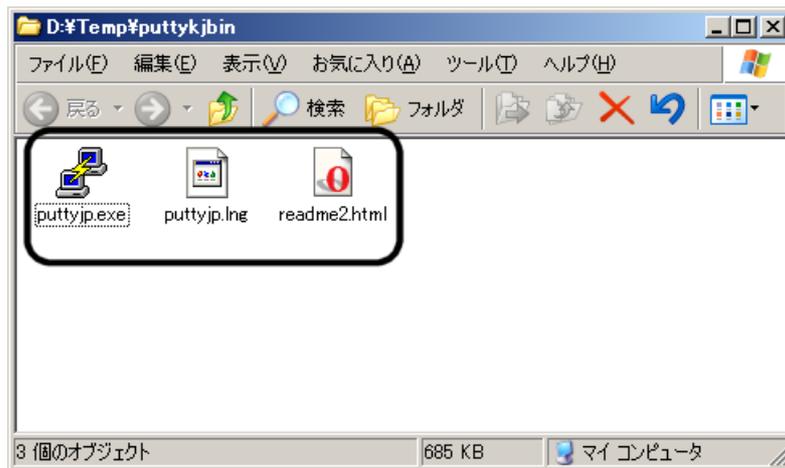


図 2: 日本語パッチが適用されたファイル

上記の三つのファイルは、PuTTY をインストールしたフォルダ (`C:\Program Files\PuTTY`) にコピーします。既に作成されているデスクトップの PuTTY アイコンやスタートメニューに登録されている PuTTY のプログラムのプロパティのリンク先を図 3 のように編集して、日本語パッチの適用されている実行ファイル (`puttyjp.exe`) を起動するように変更しておきます。



図 3: リンク先の変更

リンク先のプログラムが、次のように

C:\Program Files\PuTTY\putty.exe

から

C:\Program Files\PuTTY\puttyjp.exe

に変更しています。

5. PuTTY の使い方

デスクトップ上にある PuTTY のアイコンをマウスでダブルクリックすると図 4 のように PuTTY の設定のウィンドウが起動します。例えば、メディアセンター北館に設置のスーパーコンピュータ (以下、HPC2500) にログインする場合は、PuTTY セッションの基本オプションで『ホスト名 (または IP アドレス)』の欄に、ホスト名 (FQDN) の hpc.kudpc.kyoto-u.ac.jp を書き、その下の『プロトコル』から SSH をチェックし、**開く** をクリックします。

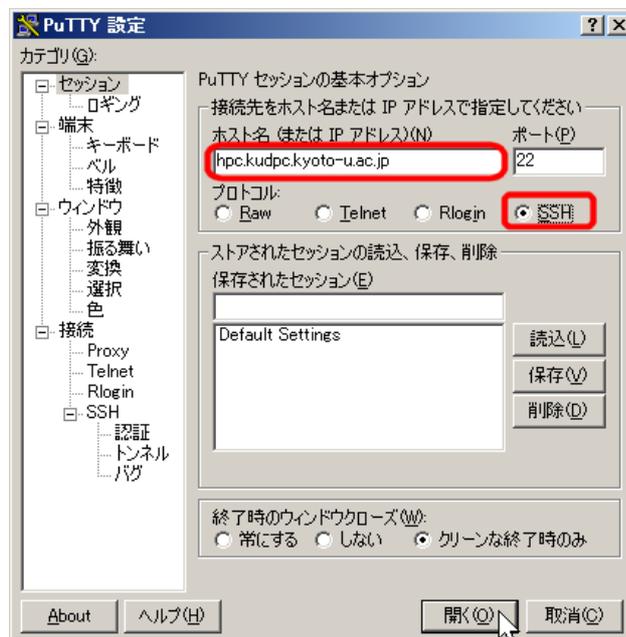


図 4: PuTTY の設定

初めて接続するホストの場合には、図 5 のように接続するホストを信頼するかを確認するウィンドウが表示されます。**はい** をクリックすると、そのホストの鍵を保存しておき、以後の接続時には保存している鍵で接続するホストを検証します。



図 5: 接続するホストの确实性の確認

接続するホストの検証が終わると、図 6 のような PuTTY のウィンドウが表示されます。login as: のプロンプトに対して、HPC2500 のアカウント (user-id) をタイプし、**Enter** キーを押します。

次に、パスワードを尋ねるプロンプトに対して、正しいパスワードをタイプしてください。利用者認証が終わると、ログインが完了します。HPC2500 をログアウトすると PuTTY のウィンドウも閉じます。



図 6: PuTTY のウィンドウ

5.1 セッションの保存

毎回、ホスト名を書き、プロトコルを選択したりするのは、手間なので、何度も接続するホストは、そのセッションに名前を付けて保存しておくのが良いでしょう。

図 7 のように『保存されたセッション』の欄に付けたい名前を書き、**保存** をクリックします。この例では、ホスト名と同じ `hpc.kudpc.kyoto-u.ac.jp` としていますが、自分で覚えやすい名前を付けるのが良いでしょう。これで、保存しておいたセッションを利用した接続が可能となります。



図 7: セッションの保存

名前を付けて保存したセッション設定を図 8 のように選択してマウスでダブルクリックしたり、**開く** をクリックすると、先ほどと同じように図 6 の PuTTY のウィンドウが表示されます。



図 8: 保存したセッションの利用

5.2 PuTTY の詳細な設定

PuTTY を快適に使うために、設定をカスタマイズしてみましょう。PuTTY の設定は、セッション・端末・ウィンドウ・接続といったカテゴリに分けて管理されています。ここでは、ウィンドウと接続の配下にある SSH の箇所を手を加えてみます。

ウィンドウでは、PuTTY のウィンドウを管理するオプションの設定を行なうことができます。ウィンドウに関するオプションは、このウィンドウの配下に外観・振る舞い・変換・選択・色に細分化され、設定するようになっていきます。まず、図 9 のウィンドウの箇所では、『ウィンドウのサイズの指定』の枠で行の指定や『ウィンドウ内のスクロールバックの管理』の枠でスクロールバックの行数を指定することができます。実際に指定する値は、各自のお好みで指定して構いません。

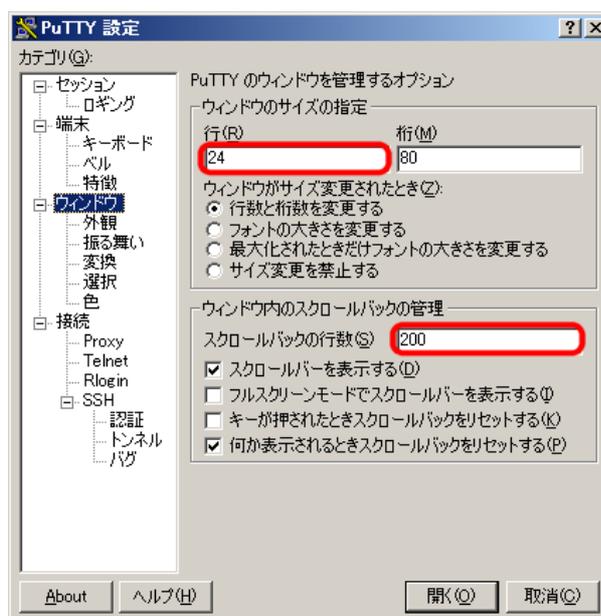


図 9: 『ウィンドウ』での設定

図 10 の外観の箇所では、『端末ウィンドウ内で使われるフォントの設定』の枠で **Change** をマウスでクリックすると、フォントのウィンドウが開きますので、好みに合わせてフォントを選択し、**OK** をクリックしてください。この例では、Terminal,10-point から少しサイズを大きくし、Terminal,14-point に変更してみました。

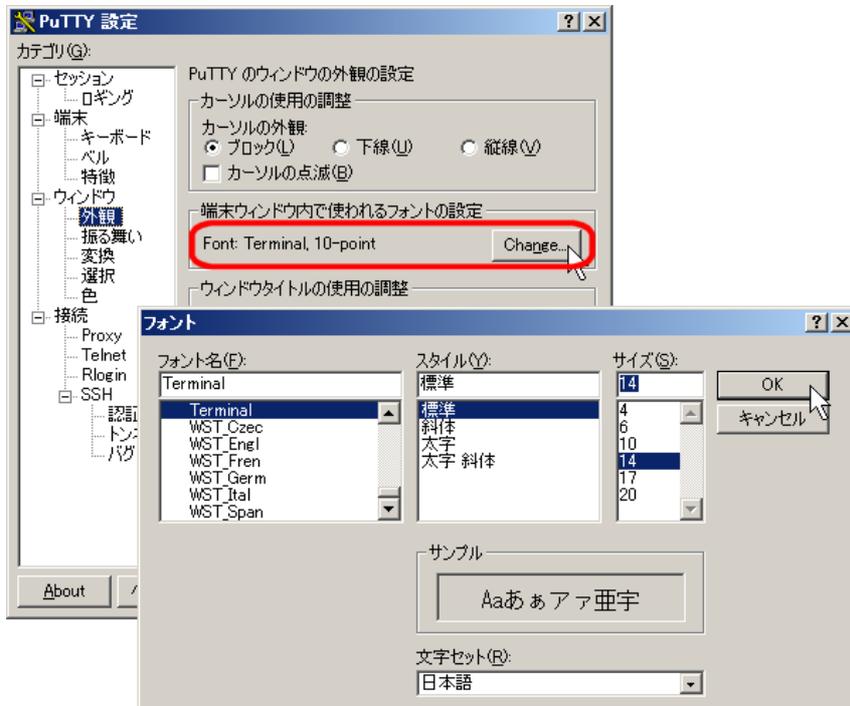


図 10: 『外観』での設定

図 11 の接続の箇所では、接続を管理するオプションの設定が行なえます。『サーバに送られるデータ』の枠で自動ログインのユーザ名の欄に、HPC2500 のアカウント (user-id) を記入しておくと、図 6 の PuTTY のウィンドウで login as: のプロンプトに回答する必要がなくなります。

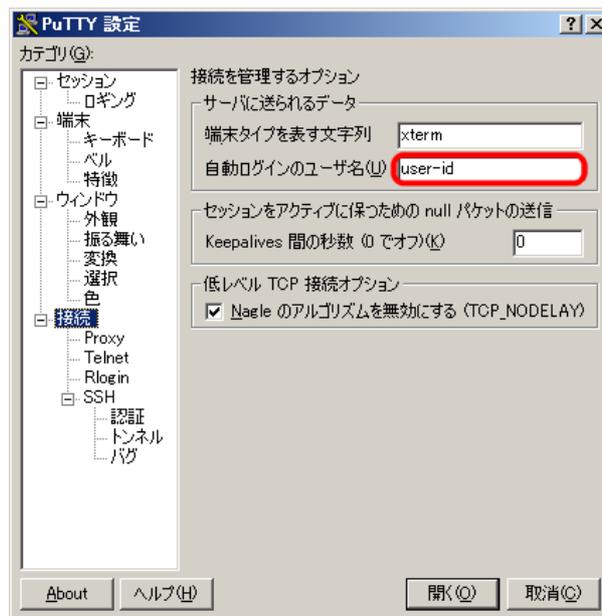


図 11: 『接続』での設定

図 12 の SSH の箇所では、SSH 接続を管理するオプションの設定が行なえます。
『プロトコルオプション』の枠で圧縮を有効にするをチェックすると暗号化通信を圧縮します。優先する SSH プロトコルバージョンには 2 もしくは 2 only をチェックするのが良いでしょう。

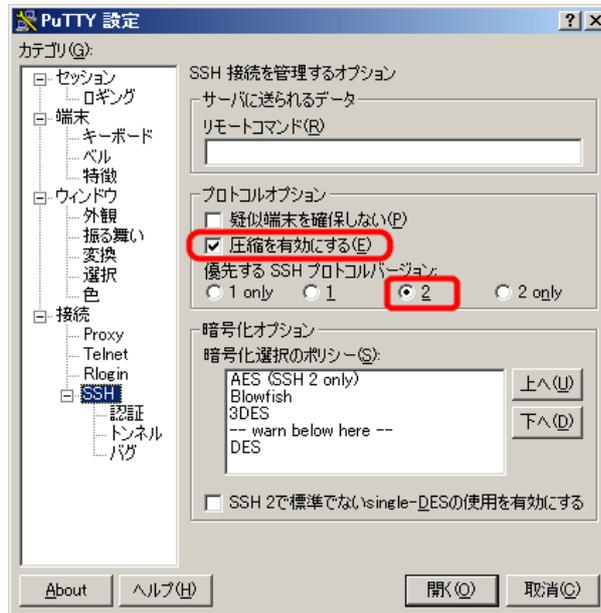


図 12: 『SSH』での設定

図 13 のトンネルの箇所では、SSH トンネリングを管理するオプションの設定が行なえます。『X11 フォワーディング』の枠で X11 フォワーディングを有効にするをチェックしておけば、安全な通信経路で X Window System を利用することができます。また、『ポートフォワーディング』の枠では、リモートマシンとローカルマシンの通信をポートごとに安全な通信経路で行なうように設定することができます。なお、この例では、トンネルの箇所の設定は変更していません。

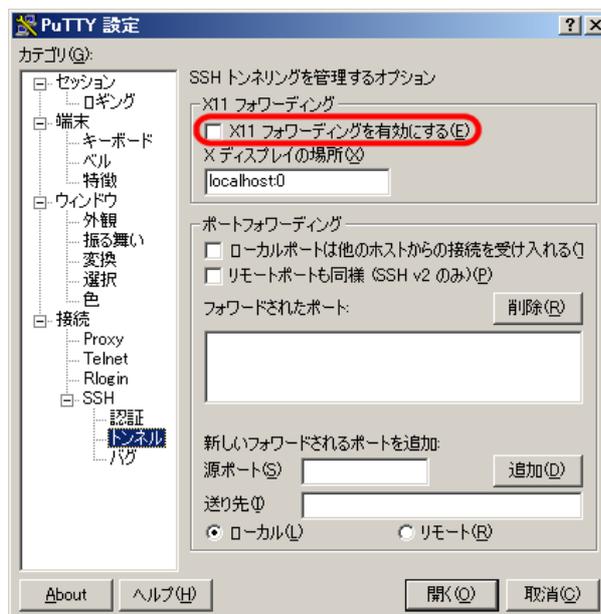


図 13: 『トンネル』での設定

カスタマイズした設定は、忘れないうちに保存しておきましょう。セッションのカテゴリに移動し、図 14 のように、『保存されたセッション』の欄に先ほど付けた名前を書き、『保存』をクリックします。



図 14: カスタマイズした設定の保存

6. socks を利用した学外の SSH サーバとの接続

現在, KUINS-III を利用している場合, 学外の SSH サーバと直接接続することはできません. しかし, KUINS で運用している socks-proxy サーバを経由することで, PuTTY を利用して, 学外と接続することができます. ここで, 設定方法を紹介します.

まず, 図 15 にある接続の箇所にある proxy を選択します. そこで, 『Proxy 必須設定項目』の各欄について, 以下の通りに指定します.

Proxy のタイプ SOCKS
 Proxy ホスト socks-proxy.kuins.kyoto-u.ac.jp
 ポート 1080

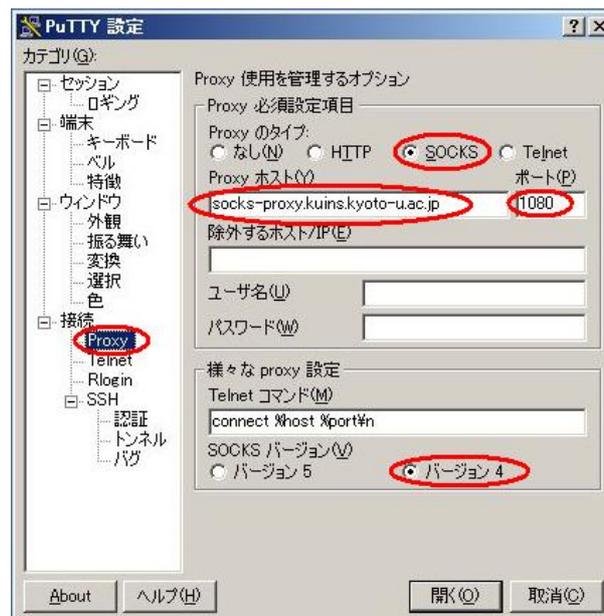


図 15: proxy(socks) の設定

次に、『様々な proxy 設定』で、バージョン 4 を選択します。設定が完了しましたら、「5. PuTTY の使い方」に戻って、順次に設定を行えば、学外の SSH サーバとの接続が可能になります

7. おわりに

以上、PuTTY の入手・インストールと簡単な使い方を紹介しました。この他にも、公開鍵認証に必要な鍵ペア（公開鍵，秘密鍵）を作成するツール（PuTTYgen）や公開鍵認証でリモートホストにログインする場合のパスフレーズの入力を自動化するツール（Pageant）なども用意されていますが、今回は、説明を省きます。

また、安全なファイル転送の protocols として、SFTP (SSH File Transfer Protocol) と SCP (Secure Copy Protocol) の二種類があり、PuTTY では、pscp コマンドや psftp コマンドが用意されています。しかし、どちらもコマンドラインから利用するコマンドなので、使いこなすには、ある程度の慣れが必要となります。

SFTP と SCP によるファイル転送を GUI ベースで実行可能なアプリケーションの一つに WinSCP がありますが、こちらは次号の KUINS ニュースで利用方法について紹介します。

KUINS 会議日誌

平成 16 年 2 月 25 日 ~ 平成 16 年 6 月 24 日

KUINS 運用委員会

平成 16 年 3 月 12 日 (第 28 回)

- KUINS 負担金状況報告
- KUINS データベースシステムについて
- KUINS-II 接続機器のフィルタリングについて
- 広報関係について
- KUINS 関連の講習会開催について
- その他

平成 16 年 4 月 9 日 (第 29 回)

- KUINS 負担金状況報告
- KUINS データベースシステムについて
- 広報関係について
- KUINS-III VLAN の各種申請について
- 遠隔地間との接続について

- その他

平成 16 年 5 月 10 日 (第 30 回)

- KUINS 負担金状況報告
- KUINS データベースシステムについて
- 講習会に関する報告
- KUINS ニュース No.45 の発行について
- フレッツグループによる遠隔地接続について
- その他

平成 16 年 6 月 14 日 (第 31 回)

- KUINS 負担金状況報告
- KUINS データベースシステムについて
- 桂地区ネットワークの状況報告
- NCA5 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

学術情報メディアセンター 情報サービス部ネットワーク担当 ((075) 753-7841)

(学術情報メディアセンター等ネットワーク掛 ((075) 753-7432))