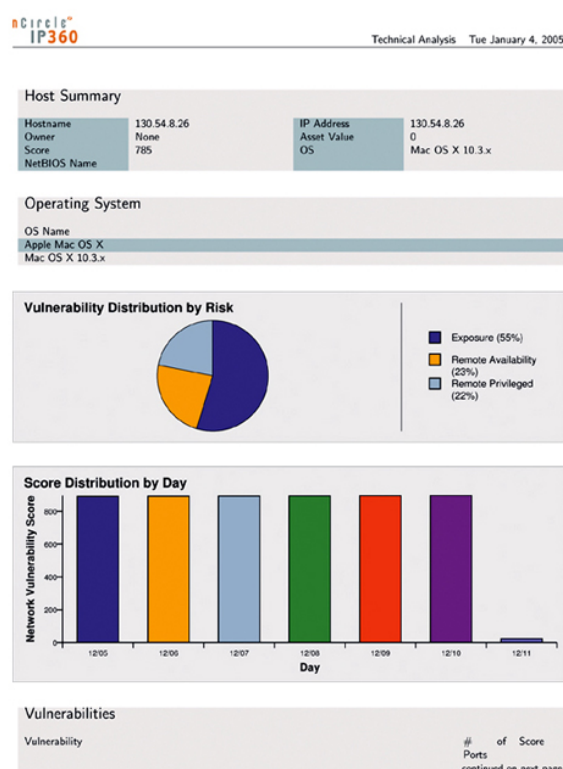


# KUINS

ニュース

No. 47

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/>



脆弱性診断システム (左: システム本体, 右: 診断結果例)

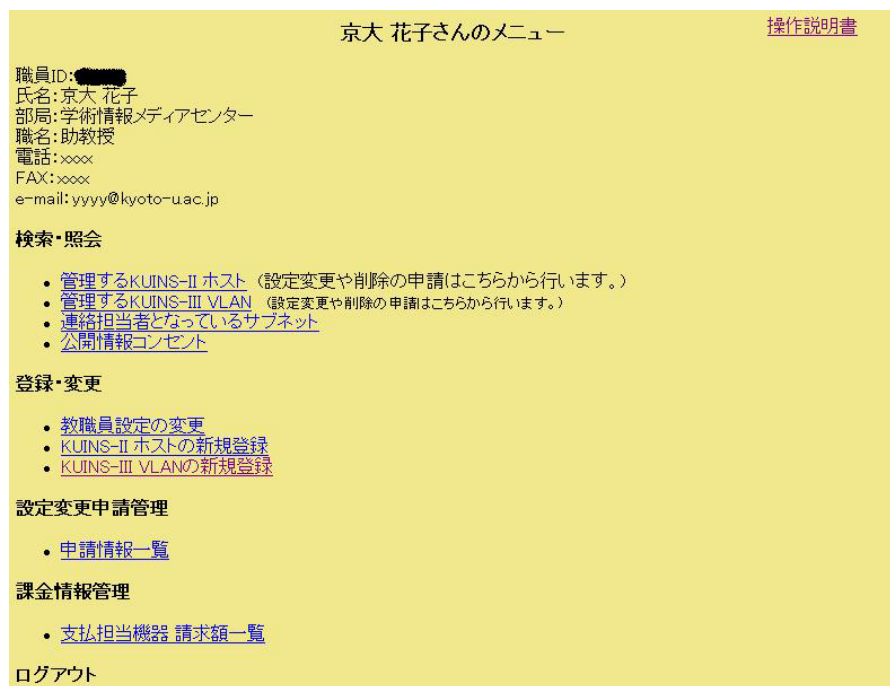
## 目 次

KUINS-III データベースの移行及び概要に関するお知らせ	572
ネットワークセキュリティ講習会のご案内	575
基幹スイッチ障害対応による KUINS 緊急停止のお知らせ	575
KUINS-II ATM ハブノードの利用について	576
遠隔研究支援システムのサポート終了について	576
脆弱性診断システム運用開始について	577
ウィルスチェック機能つきメールサーバの増強について	578
KUINS-II 接続ホストの DNS 登録の整備について	578
PuTTY で鍵交換方式による SSH 接続	579
みあこネット実証実験終了について	586
KUINS 会議日誌	586
お知らせ	586

## KUINS-III データベースの移行及び概要に関するお知らせ

KUINS-III データベースの移行を昨年 12 月中に行うよう、前号の KUINS ニュースでご案内致しましたが、作業が遅れております。1 月中に移行を完了させる予定ですので、何卒ご容赦の程、お願い致します。本号では、新しいデータベースの検索画面や申請画面などをご紹介します。(詳しい操作説明は、別途 WEB で用意し、データベースの画面からリンクさせます。)

図 1 は、現在稼働中の KUINS-II データベースにログインした直後の画面です。「管理する KUINS-III VLAN」と「KUINS-III VLAN の新規登録」はこれまでリンク先がありませんでしたが、ここから KUINS-III VLAN の照会、設定変更申請、新規登録申請ができるようになります。



京大 花子さんのメニュー [操作説明書](#)

職員ID: [REDACTED]  
氏名: 京大 花子  
部局: 学術情報メディアセンター  
職名: 助教授  
電話: xxx  
FAX: xxx  
e-mail: yyyy@kyoto-u.ac.jp

**検索・照会**

- 管理する KUINS-II ホスト (設定変更や削除の申請はこちらから行います。)
- 管理する KUINS-III VLAN (設定変更や削除の申請はこちらから行います。)
- [連絡担当者となっているサブネット](#)
- [公開情報コンセント](#)

**登録・変更**

- 教職員設定の変更
- [KUINS-II ホストの新規登録](#)
- [KUINS-III VLAN の新規登録](#)

**設定変更申請管理**

- [申請情報一覧](#)


**課金情報管理**

- [支払担当機器 請求額一覧](#)

ログアウト

図 1: KUINS-II データベースにログインした直後の画面

「管理する KUINS-III VLAN」をクリックすると、図 2 の画面が現れます。ここに、ご自分が管理責任者となっている KUINS-III VLAN のリストが現れます。



**VLAN(サブネット)リスト** [操作説明書](#)

検索件数: 2件  
ページ: 1 / 1  
並び順: VID順  
表示件数: 100件 ▼

1)

	VID	ネットワークアドレス	管理責任者	
<a href="#">詳細</a>	11111	10.10.10.0/26	京大 花子	<a href="#">ホスト一覧</a>
<a href="#">詳細</a>	22222	10.20.0.0/26	京大 花子	<a href="#">ホスト一覧</a>

[メニューに戻る](#) [前画面へ戻る](#)

図 2: VLAN(サブネット) リスト

「詳細」をクリックすると、図 3 に飛び、VLAN の詳細情報が現れます。この VLAN の設定を変更したいときは、「設定を変更する」を押して下さい。申請画面に飛びます。また削除したいときは「VLAN を削除する」を押します。

VLAN情報 [操作説明書](#)

VID	11111
ネットワークアドレス	10.10.10.0/26
サブネットマスク	255.255.255.192
DHCPアドレス	10.10.10.10～10.10.10.20
固定アドレス	10.10.10.21～10.10.10.30
ゲートウェイアドレス	
ブロードキャストアドレス	
部屋種別	CLOSE
課金区分	課金する
一般公開	公開可

管理責任者

氏名	部局	職名	電話	FAX	e-mail
京大 花子	学術情報メディアセンター	助教授	xxxx	xxxx	yyyy@kyoto-u.ac.jp

連絡担当者

氏名	部局	職名	電話	FAX	e-mail
京大 花子	学術情報メディアセンター	助教授	xxxx	xxxx	yyyy@kyoto-u.ac.jp

支払責任者

氏名	部局	職名	電話	FAX	e-mail
京大 太郎	学術情報メディアセンター	教授	xxxx	xxxx	xxxx@kyoto-u.ac.jp

支払費目	区分	請求先部局
研究経費(教育研究事業費)	1	支払責任者の所属部局

経理責任者

氏名	電話	FAX	e-mail

情報コンセントリスト

建物名	情報コンセント名	末端スイッチ名	ポート番号	課金区分
本部北構内				
学術情報メディアセンター北館(旧大型計算機センター)	sample1-G	FSc2-sample-1	FastEthernet0/1	課金する
学術情報メディアセンター北館(旧大型計算機センター)	sample2-G	FSc2-sample-1	FastEthernet0/3	課金する
学術情報メディアセンター北館(旧大型計算機センター)	sampleA-G	FSc2-sample-2	FastEthernet0/1	課金する
学術情報メディアセンター北館(旧大型計算機センター)	sampleB-G	FSc2-sample-2	FastEthernet0/3	課金する

備考:

更新情報

登録日時: 2005-01-05 13:49:19.05658+09

最終更新日時: 2005-01-05 13:49:19.05658+09

設定を変更する VLANを削除する

メニューに戻る 前画面へ戻る

図 3: VLAN 情報

図 1 の画面から「KUINS-III VLAN の新規登録」を押すと、図 4 へ飛びます。

VLAN新規入力-構内選択 [操作説明書](#)

新規で登録するVLANが所属する構内を選択してVLAN新規作成ボタンを押下してください。

構内名

本部北構内

VLAN新規作成

メニューに戻る

図 4: VLAN 新規入力 -構内選択

ここで新規に作成する VLAN のキャンパスを選んで、「VLAN 新規作成」を押して下さい。すると、図 5 へ飛びます。必要事項を入力して「申請」を押すと、申請が完了します。

VLAN新規登録申請

操作説明書

登録内容の入力

登録したいVLANの情報を入力してください。

最新の情報を取得するときや簡単な入力のチェックを行なう場合は、更新ボタンを押下してください。

更新

申請

（簡単な入力内容のチェックをします。実際の申請は行なわれません。）

（入力した内容で実際に申請を行います。）

管理責任者

ID	氏名	部局	職名	電話	FAX	e-mail
	京大 花子	学術情報メディアセンター	助教授	xxxx xxxxx		yyyy@kyoto-u.ac.jp

連絡担当者

ID	氏名	部局	職名	電話	FAX	e-mail

追加

支払責任者

ID	氏名	部局	職名	電話	FAX	e-mail

経理情報

支払費目

区分

請求先部局

研究経費(教育研究事業費)

区分無し

☒ 支払責任者の所属部局

☐ 支払責任者とは異なる部局

(請求先: 事務局)

アドレス空間(マスクビット数):

26

固定アドレス数

0

部屋種別

☒ OPEN

☐ CLOSE

☐ KUINS-IIとして設定

☐ その他(KUINS-II, KUINS-III以外)

備考

一般公開

☒ 可

☐ 不可

VLAN間通信対象のVLAN

VID	管理責任者	部局	職名

追加

情報コンセンストリスト

建物名	情報コンセントID	末端スイッチ名	ポート番号
本部北楼内			
学術情報メディアセンター北楼(旧大型計算機センター)			/

追加

補足事項:上記の申請について、補足説明があれば記入してください。

更新

申請

（簡単な入力内容のチェックをします。実際の申請は行なわれません。）

（入力した内容で実際に申請を行います。）

メニューに戻る

新画面へ戻る

図 5: VLAN 新規登録申請

図 1 から「支払担当機器 請求額一覧」をクリックすると、これまでの II の支払額一覧に加えて、KUINS-III の支払額一覧も表示されるようになりました (図 6)。

課金対象機器一覧

操作説明書

自分が支払責任者となっているホスト/VLANの情報を表示します。

KUINS-III VLAN

	VID	ネットワークアドレス	課金区分	課金対象情報コンセント数	支払費目	支払区分	請求月額
詳細	22222	10.20.0.0/26	課金する	5	一般管理費(教育研究事業費)	区分無し	1,500

KUINS-II ホスト

該当するデータはありません。

メニューに戻る

図 6: 課金機器対象一覧

## ネットワークセキュリティ講習会のご案内

京都大学学術情報メディアセンターでは、下記の通り講習会を開催します。本講習会では、我が国のネットワークセキュリティ分野の第一線でご活躍のお二人を講師としてお招きし、ネットワークセキュリティについて、特に個人情報保護の観点からお話し頂きます。木村氏は宇治市の個人情報漏洩事件の当時、担当課長として最前線に対応された方です。また、上原氏は地方自治体のセキュリティポリシーや個人情報保護ガイドラインの策定に奔走されておられる方です。

本講習会は大学関係者を対象としていますが、企業の方でも、大学でのネットワーク管理業務等に従事する方はご参加頂けます。受講を希望される方は、氏名、所属、身分を明記の上、下記宛先までお申し込み下さい。

締め切りは、3月10日（木）午後5時とします。なお、定員になり次第、締め切らせて頂きます。

日時： 平成17年3月17日（木）13時30分～17時00分  
 場所： 京都大学学術情報メディアセンター 南館2階202号室  
 定員： 100名  
 講師： 木村 修二 氏（財団法人 関西情報・産業活性化センター）  
 上原 哲太郎 氏（京都大学 大学院工学研究科 附属情報センター）

[申し込み先]：

学術情報メディアセンター ネットワーク掛

電話：内線 7432 または 7841

電子メール：kousyukai@kuins.kyoto-u.ac.jp

## 基幹スイッチ障害対応による KUINS 緊急停止のお知らせ

日頃より学内ネットワーク KUINS の運用にご協力いただき有難うございます。さて、KUINS が各構内に設置しています基幹スイッチの ATM モジュールに障害が発見されました。つきましては、下記の日程にて基幹スイッチのモジュール交換を実施しますので、ご協力の程、よろしくお願いします。

なお、モジュール交換作業時に1時間程度ネットワークが停止しますのでご了承下さい。

日時	構内
平成17年1月6日7時30分～8時30分	本部北構内
平成17年1月11日7時30分～8時30分	京大外との通信停止
平成17年1月13日7時30分～8時30分	北部構内
平成17年1月18日7時30分～8時30分	桂構内
平成17年1月20日7時30分～8時30分	本部南構内
平成17年1月24日7時30分～8時30分	宇治構内
平成17年1月26日7時30分～8時30分	吉田南構内
平成17年1月28日7時30分～8時30分	医学部構内
平成17年1月31日7時30分～8時30分	病院構内
平成17年2月2日7時30分～8時30分	薬学部構内

## KUINS-II ATM ハブノードの利用について

KUINS ニュース No.46 にてお知らせしましたが、接続機器の著しい減少や老朽化に伴い、未使用の ATM ハブノードを撤去することになりました。そのため、サテライトルータ、エッジルータ及び届出済みの ATM 機器が接続されていない ATM ハブノードは、順次撤去作業を行う予定です。

現在、届出なしに ATM ハブノードを接続されている場合で、今後も引き続き利用を希望される場合は、1 月末までに

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

にて、接続申請を行って下さい。接続申請がない場合は利用予定がないものとみなし、撤去対象になりますのでご注意ください。

撤去の手順として、以下の手順で進めていきます。

1. ハブノードの接続確認を事前に実施する。
2. 通信の形跡が無いハブノードの電源を切る。
3. 1 週間待ち、問題が無ければ撤去する。
4. ハブノードを置いているラックは、相談の上撤去する。

---

## 遠隔研究支援システムのサポート終了について

KUINS では、学内で行われる各種打ち合わせに学内の離れた場所から参加することが可能な「遠隔研究支援システム」を平成 10 年度より提供してきました (KUINS ニュース No. 27 「遠隔研究支援システムの導入」参照)。このシステムも、導入より 6 年が経過し納入業者による保守が困難になったこと、さらに同時期に導入され、遠隔研究支援システムの基盤である KUINS-II のバックボーン ATM ネットワーク接続装置も、主としてハブノードの保守期間が満了を迎えつつあります。また、使用している OS(WindowsNT 4.0) に対して、セキュリティ面のサポートができなくなる等の理由により、遠隔研究支援システムの継続的なサポートが困難になりつつあります。

このようなことから、遠隔研究支援システムの提供を平成 16 年度末で終了させて頂くこととなりました。部局設置の端末については、KUINS で回収させて頂きます。引き取り日程等につきましては、別途「運用責任者」にご連絡いたします。

なお、システム単体として継続的な利用を希望されます場合は、その旨をお知らせください。移管の手続きをさせて頂きます。その場合は、端末のセキュリティ対策等 (OS の入れ替えなど) についても全て部局側にて実施して頂くことになりますので、よろしくお願いいたします。

本件に関するお問い合わせは、q-a@kuins.kyoto-u.ac.jp までお願いいたします。

## 脆弱性診断システム運用開始について

この度、学術情報メディアセンターでは、商用の脆弱性診断サービスに採用されているシステムの一つである nCircle 社製 IP360 の運用を開始致します。当センターで行った試験運用では、IP360 により

- 繰り返し診断により、単発の診断では判明しなかった脆弱性の発見
- 管理者の意図しないライブラリのダウングレード
- 管理者の意図しないサーバプログラムの稼働
- ファイアウォールの設定ミス

等が発見できました。また、脆弱性の解説およびその対処法は日本語レポートとなります（ただし、最新の脆弱性で日本語訳が間に合わないものについては英語となります）。

一方で、診断は「寸止め」による疑似攻撃を行うため、ごくわずかですが

- 脆弱すぎる機器の場合、疑似攻撃により当該機器がダウンする可能性があります。
- 診断は「攻撃」として機器のログに保存されますので、ディスク容量に余裕が無い機器では、ディスク溢れによりシステムが不安定な状態に陥る可能性があります。

の危険性があります。一方でこのような機器は、学外からの攻撃を受けてもシステムダウンを起こす場合があります。また、システムの不安定化を狙った攻撃により管理者権限を奪取される可能性もあります。診断によるサービス停止の不都合の可能性があることをご了解頂いた上で、事前に脆弱な機器を特定することができるとお考え頂き、是非ご活用ください。

なお、診断装置の物理的制約およびライセンス上の制約により、当面の間、以下の運用方針で脆弱性診断サービスを行わせて頂きます。

- 診断費用は無料です。
- 診断対象は KUINS-II 機器が接続されたサブネットとし、サブネット単位で診断を行います。
- 診断は学術情報メディアセンターの KUINS-II サブネットに設置された診断装置から行い、ファイアウォールの内側のような部局で独自に運用されているネットワークに対しては行いません。
- 部局契約の ISP に設置された機器に対する診断は行いません。
- 診断は部局情報セキュリティ責任者、部局情報セキュリティ幹事、あるいは、サブネット連絡担当者に取りまとめ頂き依頼をしてください。
- 診断期間は 1 週間とします。
- 複数のサブネットを同時に診断することはできますが、同時診断の対象機器は合計で 100 台以下とさせていただきます。
- 診断受付は先着順とさせていただきますので、依頼頂いた後、診断開始日の調整を行わせて頂くことがあります。
- 診断を依頼された方に診断結果の PDF ファイルをお送りします。お手数ですが、診断を依頼された方がそれぞれの機器の管理責任者に診断結果をお渡しください。

脆弱性診断に関するご質問、あるいは、診断の依頼は、q-a@kuins.kyoto-u.ac.jp までお申し出ください。



## ウィルスチェック機能つきメールサーバの増強について

KUINS では、平成 14 年 8 月より、ウィルスチェック機能つきメールサーバの運用を開始し、電子メールに含まれているウィルスの駆除サービスを提供しています (KUINS ニュース No. 38 「ウィルスチェック機能つきメールサーバ運用開始について」 参照)。しかし、最近では、サーバの過負荷等の原因により電子メールの配送に遅延が生じる等の問題が発生するようになってきました。そこで、この対策として、ウィルスチェック機能つきメールサーバの増強を行うこととしました。具体的には、以下のような増強を計画しています。

- ウィルスチェック機能つきメールサーバを 6 台から 8 台に増強し、送信用と受信用を分離
- ウィルスチェックに利用している InterScan のバージョンアップ
- KUINS-III からの送信用メールサーバ (sendmail.kuins.net) の冗長化

各サーバは、学術情報メディアセンター北館および南館に分散配置され、一方が停電等で停止した場合でもサービスが継続して提供できるよう冗長構成をとっています。

増強作業は、平成 17 年 2 月末から 3 月にかけて行う予定ですが、1 月末より DNS の設定内容の調整等の準備作業にとりかかります。日程の詳細については、順次 KUINS の Web ページにてお知らせする予定ですが、作業期間中もサービスは継続して提供する予定ですので、ユーザ側において特に対応して頂く必要はありません。

なお、メールサーバの増強作業によって IP アドレスが一部変更になる予定ですが、ユーザ側においてホスト名を指定して頂いている場合には、特に設定を変更して頂く必要はありません。もし IP アドレスが直接設定されている場合は、増強作業に伴ってメールが送受信できなくなる可能性がありますので、設定の確認をお願いします。また、部局設置のメールサーバにおいてメールの送信元に対するフィルタリングの設定を行っている場合は、一時的にフィルタリングを緩和して頂く必要がありますので、別途お問い合わせ下さい。

### [参考情報]

- KUINS-III 接続ガイド ~ KUINS-III からのメール送受信について ~  
<http://www.kuins.kyoto-u.ac.jp/KUINS3/kuins3-guide/mail.html>
  - KUINS ニュース No. 39 ウィルスチェック機能つきメールサーバの部局サーバからの利用について  
<http://www.kuins.kyoto-u.ac.jp/news/39/virus-mailserv.html>
  - KUINS ニュース No. 40 部局メールサーバの KUINS-III への設置について  
<http://www.kuins.kyoto-u.ac.jp/news/40/kuins3-mserv.html>
- 

## KUINS-II 接続ホストの DNS 登録の整備について

KUINS で管理しているサブドメインの正引き、逆引きの整理を 2005 年 4 月より行います。KUINS-II 接続機器登録データベース (<https://db.kuins.kyoto-u.ac.jp/>) の登録情報を元にデータを変更しますので、登録漏れが無いか確認の方をよろしくお願いします。(特にメールサーバは登録されていなくても使用できている可能性があります)



## PuTTY で鍵交換方式による SSH 接続

### 1. はじめに

KUINS ニュース No.45 で、暗号技術を用いた安全な通信方式の SSH(Secure SHell) を用いて接続ができる 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 の利用方法について紹介しました。その中では、パスワードを用いたユーザ認証によって SSH 接続を実現する設定について記載しましたが、ユーザ認証としてパスワードを利用すると、

- UNIX で用いるパスワードは 8 文字しか有効でないことが多いため、総当たり攻撃や辞書攻撃などに弱く、容易にパスワードを破られる
- 接続しようとするサーバを偽って、偽の SSH サーバに接続させられてしまうことにより、パスワードを盗まれる

などによって、パスワードが第三者によって利用されてしまう「なりすまし」の危険性を回避することはできません。そのため、SSH ではパスワード認証ではなく、公開鍵暗号方式を用いた認証による接続が推奨されています。

公開鍵暗号方式とはデータ暗号方式の一つで、ユーザが独自に「公開鍵」と「秘密鍵」と呼ぶ二つの鍵をペアで作成し、それらの鍵を使ってデータの暗号化／復号化を行います。公開鍵は暗号文を作り出す鍵で、通信相手に知らせる鍵としてインターネット上でもやりとりできます。また、だれでもこの公開鍵で暗号文を作成でき、鍵を公開している人に送ることができます。一方、暗号文の受け手は公開鍵とペアになっている本人だけが分かるように厳重に管理された秘密鍵で復号します。暗号化と復号化を同じ鍵で行う共通鍵暗号方式に比べて、公開鍵の共有が容易なことや相手の数に関係なく公開鍵は 1 つでよいなど、鍵の管理が容易で安全性が高いとされています。今回は、PuTTY での鍵交換方式による SSH 接続方法について紹介いたします。

### 2. PuTTY における SSH 鍵生成

まず、自分が使用している PC に PuTTY をインストールされている必要があります。PuTTY がインストールされていない場合は、KUINS ニュース No.45 の記事を参照してインストールを行って下さい。PuTTY で鍵生成を行うプログラムとして、PuTTYgen が付属していますのでこれを利用します。スタートメニューから、「スタート」->「プログラム」->「PuTTY」->「PuTTYgen」とたどることにより、PuTTYgen を起動することができ、図 1 にあるウインドウが表示されます。



図 1: PuTTYgen の起動画面

まず、鍵の生成を行う前に、鍵の種類を設定します。種類は”SSH1 RSA”・”SSH2 RSA”・”SSH2 DSA”の3種類から選べます。ここではSSH2 接続できるように ”SSH2 RSA” を選択してください。(PuTTYgenのHELP ファイルでは、”SSH DSA”よりも”SSH2 RSA”を推奨しています)

次に、`generate` ボタンを押して鍵を生成します。マウスの動きで乱数生成を行いますので、ダイアログ上で適当にマウスを動かしてください(図 2)。

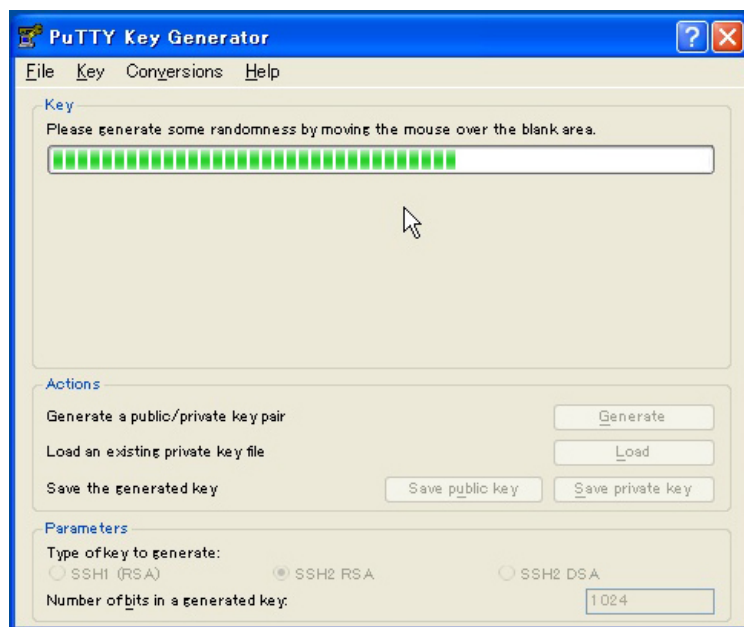


図 2: 鍵生成 (マウスの動きによる乱数作成)

ポインタを動かし続けていると、「Please wait while a key is generated...」とメッセージが変わり鍵が生成されます(図 3)。

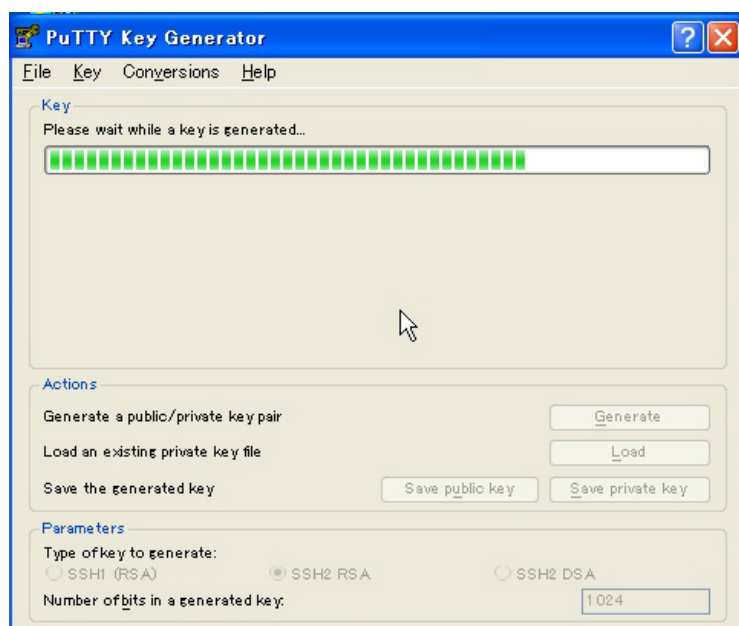


図 3: 鍵生成中の画面

鍵が生成されました，パスフレーズの入力を行います．ウインドウの中央部分にある『Key passphrase』にパスフレーズとして任意の文字列を入力し，確認のためにその下の『Confirm passphrase』に同じパスフレーズを繰り返し入力します(図4)．パスフレーズには文字制限がなく，また空白も含めることが可能です(尚，ここで入力するパスフレーズは，UNIX サーバなどのユーザに対するパスワードとは違うものです)．パスフレーズを入力したら，作成した鍵を保存します．『Save private key』(秘密鍵)，『Save public key』(公開鍵)を順にクリックしてください．それぞれファイル名を決めて保存します．保存先については特に制限はありませんが，本稿では，

C:\Program Files\PuTTY

に，秘密鍵を id\_rsa.ppk，公開鍵を id\_rsa.pub という名前で保存することにします．

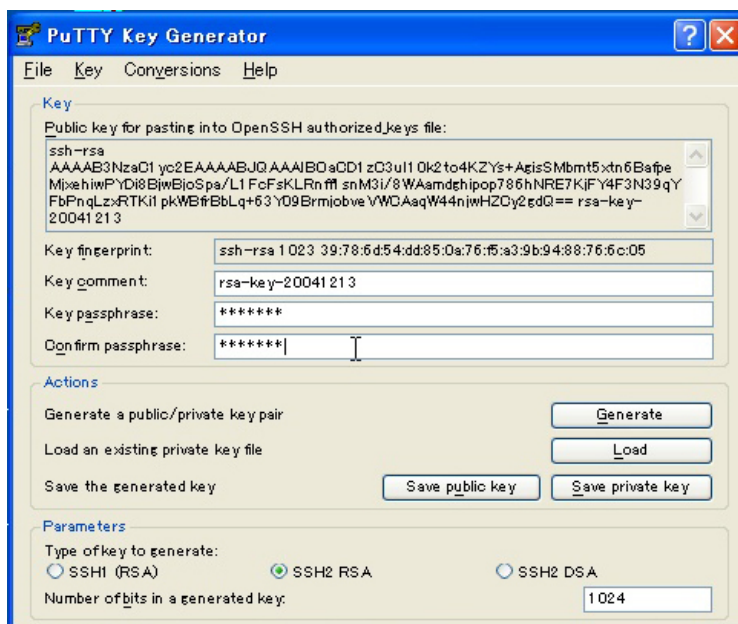


図 4: パスフレーズの入力，秘密鍵，公開鍵の保存

### 3. SSH サーバへ公開鍵の登録

次に，作成した公開鍵を接続する SSH サーバに登録を行います(尚、今回はサーバ側で OpenSSH を用いていると想定しています)．最初に公開鍵を SSH サーバに転送する必要があります．転送方法としては安全に転送を行うために，SCP，SFTP などを使うことで可能ですが，ここでは PuTTY に付属されている pscp コマンドを利用します．本稿では SSH サーバの例として，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)を用います．

まず，コマンドプロンプトを立ち上げて(スタートメニューから「プログラム」->「アクセサリ」)以下のコマンドを実行して，pscp.exe が存在するディレクトリに移動します．

C:\>cd C:\Program Files\PuTTY

そして，以下のコマンドで公開鍵を HPC2500 (FQDN 名:hpc.kudpc.kyoto-u.ac.jp) に転送します．尚，ここではユーザアカウントを user-id としていますが，各自で使用している SSH サーバに登録されている自分のアカウント名，SSH サーバのホスト名に置き換えて下さい．

C:\> pscp id\_rsa.pub user-id@hpc.kudpc.kyoto-u.ac.jp:id\_rsa.pub

次に、転送した公開鍵をサーバに登録を行うために、HPC2500 にログインします。ログインは PuTTY を使用して行うことができます。方法については、KUINS ニュース No.45 の記事を参考にして下さい。

ログインできましたら、登録の前に PuTTYgen で作成した公開鍵を、OpenSSH で使用できるように変換を行う必要があります。変換方法として、ssh-keygen コマンドを用います。以下のコマンドを実行して下さい。

```
% ssh-keygen -i -f id_rsa.pub >> authorized_keys
```

次に、自分のホームディレクトリに .ssh というディレクトリが存在することを確認して下さい。存在しない場合はディレクトリを作成し、またディレクトリのパーミッションを 700 にしておきます。

そして、.ssh ディレクトリに移動します。そのディレクトリに authorized\_keys というファイルが存在していなければ、さきほど変換して作成したファイルをこのディレクトリに移動させます。また、authorized\_keys のパーミッションを 600 にしておきます。以上の作業を、下記のコマンドを実行することで行えます。

```
% cd .ssh
% mv ../authorized_keys .
% chmod 600 authorized_keys
```

authorized\_keys が既に存在している場合は、そのファイルにさきほど変換したファイルの内容を追加して下さい。あと、転送した公開鍵ファイル (id\_rsa.pub) は削除しておいて下さい。

```
% rm ~/id_rsa.pub
```

#### 4. PuTTY の設定

サーバ側での鍵登録が完了しましたら、PuTTY で認証の設定を行います。スタートメニューから、あるいはデスクトップ上にある PuTTY のアイコンをダブルクリックすることにより、PuTTY の設定のウィンドウを起動します。まず、『保存されたセッション』の欄に既に登録されている中で、公開鍵を登録したサーバのセッションを選択し、読みボタンをクリックします。ここでは、サーバのホスト名と同じ hpc.kudpc.kyoto-u.ac.jp のセッションを選択しています (図 5)。



図 5: PuTTY の設定画面

次に、カテゴリの『接続』->『SSH』->『認証』を選択すると、図 6 の画面が表示されます。その中で『認証パラメータ』の『認証のためのプライベートキーファイル』で作成した自分の秘密鍵 (id\_rsa.ppk) を指定します。『参照』ボタンをクリックして、秘密鍵があるフォルダに移動して、使用する秘密鍵ファイルを選択して下さい。設定が完了しましたら、『セッション』のカテゴリに移動し、『保存』をクリックします。

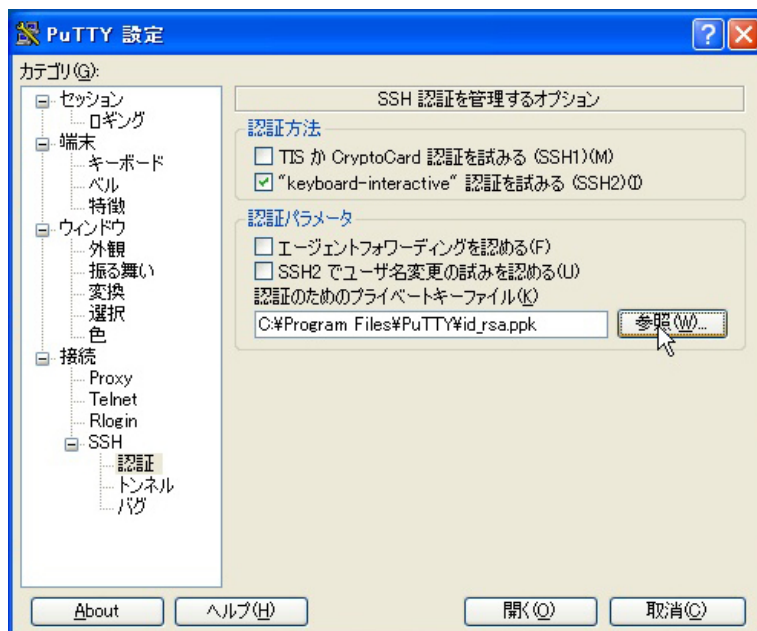


図 6: SSH 認証を管理するオプション

## 5. SSH サーバへのログイン

設定が完了しましたので、実際にサーバにログインをしてみます。さきほど保存したセッションを読み込んで、『開く』のボタンをクリックします。図 7 のような PuTTY のウィンドウが表示されます。パスワード認証の際のログインと異なり、

```
Authenticating with public key "rsa-key-20041213"
Passphrase for key "rsa-key-20041213"
```

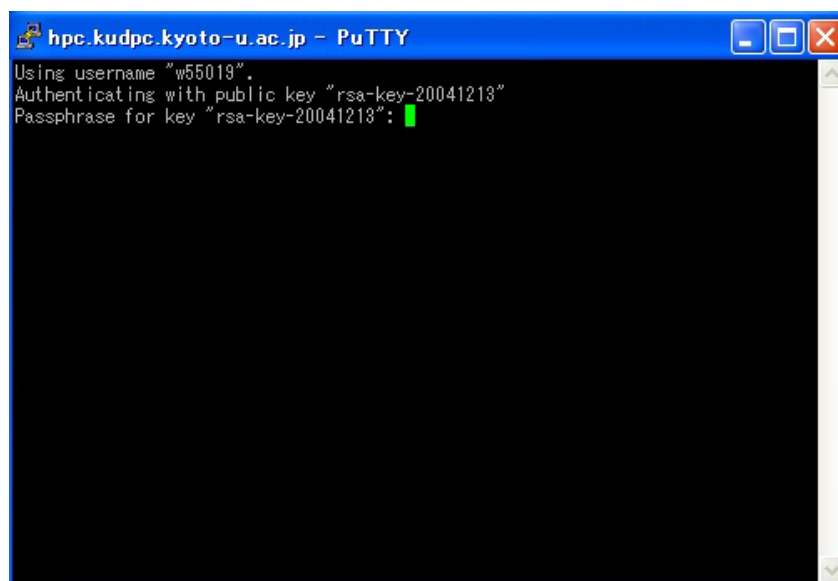


図 7: PuTTY のウィンドウ (パスフレーズ入力を要求)

というメッセージが表示され、パスフレーズの入力を要求されます。(尚、rsa-key-20041213 は、鍵作成の際に設定されているキーメッセージです。) パスフレーズは、鍵作成の際に入力したものをこのウインドウ上に入力します。正しく入力できると、図 8 のように正常にログインが完了します。

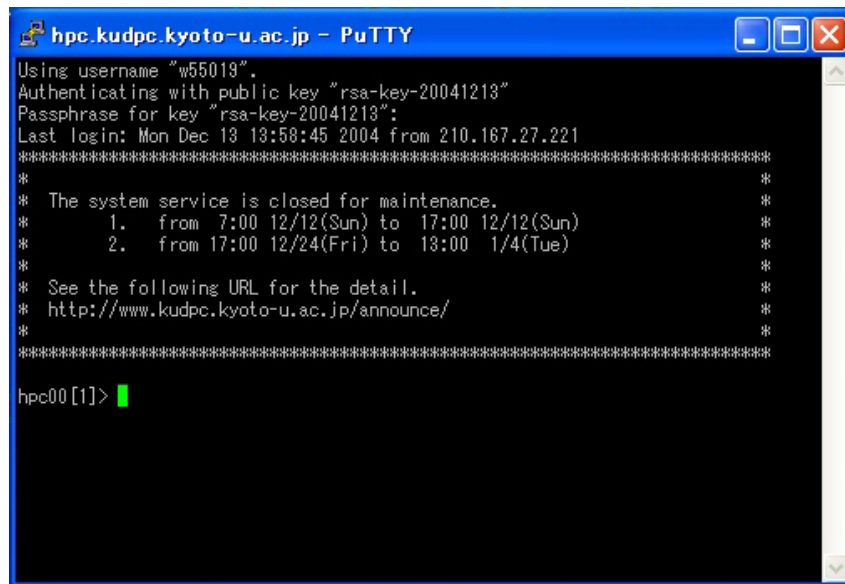


図 8: PuTTY のウインドウ (ログイン完了)

## 6. Pagent の利用

以上の方法で、PuTTY で鍵交換によって ssh サーバにログイン可能になりました。しかしこの方法においてもログインする度に、パスフレーズを入力する作業を行う必要があります。そこで、Pagent を利用することにより、パスフレーズの入力を省略することができます。次に、Pagent の利用方法について紹介します。

スタートメニューから、Pagent を起動します(「スタート」->「プログラム」->「PuTTY」->「Pagent」とたどれます)。起動すると、タスクバー(右下)にアイコンが表示されます(図 9)。そのアイコンをダブルクリックすると、図 10 のウインドウが表示されます。



図 9: Pagent のアイコン

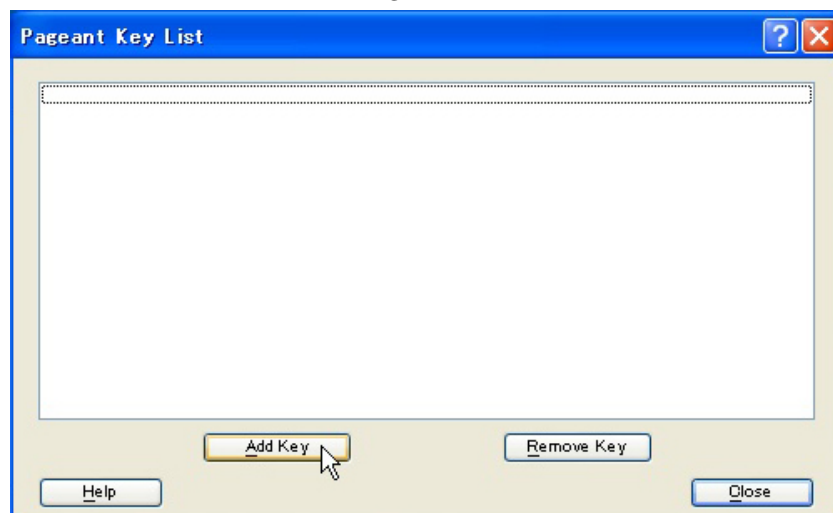


図 10: 秘密鍵登録のウインドウ



そして、**Add Key**をクリックしますと、『Select Private Key File』のダイアログが立ち上がりますので、作成している秘密 (id\_rsa.ppk) のフォルダに移動して選択します。選択しますと、『Pageant: Enter Passphrase』のウィンドウが表示されてパスフレーズを聞かれますので、鍵作成時に設定したパスフレーズを入力して下さい (図 11)。



図 11: パスフレーズの入力

パスフレーズが正しく入力されましたら、図 12 のように登録された秘密鍵が表示されます。登録が確認できたら、**Close** ボタンでこのウィンドウを閉じて、完了です。

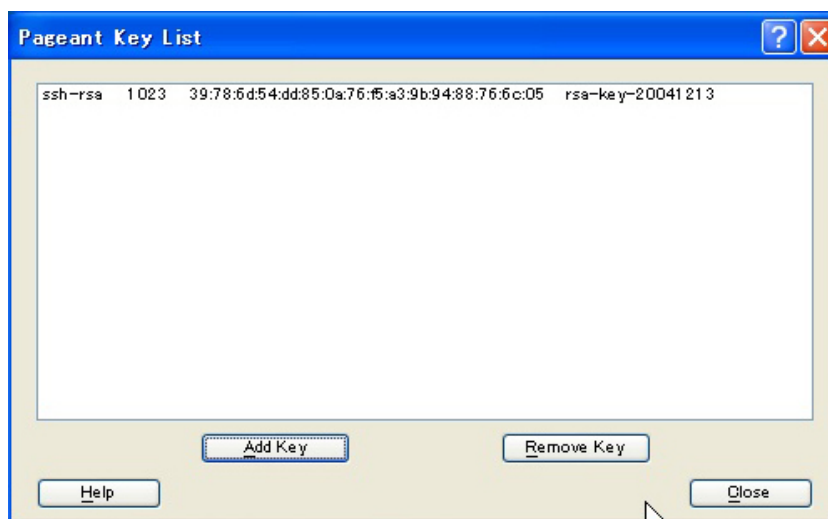


図 12: 秘密鍵登録のウィンドウ (登録完了)

このように、Pageant が常駐している状態 (タスクバーにアイコンが表示されている状態) で PuTTY を起動しますと、パスフレーズを聞かれることなく ssh サーバにログインすることが可能です。但し、Pageant を終了させた場合、もう一度秘密鍵の登録からやり直すことになります。

## 7. おわりに

本稿では、PuTTY を用いた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省略できる (Pageant) について紹介しました。

パスワードを用いたユーザ認証では、パスワードが何らかの形で第三者に漏れると、容易にアクセス可能になってしまう事態を避けられませんので、今回紹介した公開鍵暗号方式での認証への移行をお勧めします。



## みあこネット実証実験の終了について

KUINS ニュース No.38 記事 (<http://www.kuins.kyoto-u.ac.jp/news/38/#miako-net>) で紹介した公衆無線インターネット「みあこネット」(<http://www.miako.net>) 実証実験が、平成 17 年 3 月末で終了します。

みあこネット方式で本学に設置されている無線基地局については、4 月以降、学術情報メディアセンターのサービスとして、これまでと同等の運用が継続できるように調整中です。

なお、本学関係者向けに Web によりオンライン発行されていたアカウントについては、3 月末で失効します。4 月以降のみあこネット方式の無線基地局からの接続については、SSH port forwarding サービス (<http://www.ipse.media.kyoto-u.ac.jp/services/ssh/portfwd.html>) などの SSH トンネリングを用いる方法や、PPTP (Microsoft Point-to-Point Tunneling Protocol) を用いる方法が使えます。PPTP については、学術情報メディアセンターの教育用計算機システムのアカウントで接続できるサービスを準備中です。また、部局等で独自に PPTP サーバを運用することも可能です。KUINS ニュース No.41 記事「mpd を用いた PPTP サーバの構築」<http://www.kuins.kyoto-u.ac.jp/news/41/pptp.html> をご参照ください。

## KUINS 会議日誌

平成 16 年 10 月 20 日～平成 17 年 1 月 16 日

### KUINS 運用委員会

平成 16 年 10 月 26 日 (第 35 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-III フィルタリング設定の見直しについて
- その他

平成 16 年 11 月 29 日 (第 36 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 ニュース No.47 発行について

- メディアセンター汎用機システムリプレースに伴う構成変更について

- その他

平成 16 年 12 月 22 日 (第 37 回)

- KUINS 負担金状況報告
- KUINS データベースシステムについて
- メディアセンター汎用機システムリプレースに伴う構成変更について
- KUINS サービス用サーバのリプレースについて
- 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](mailto: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))