ISSN 0917-3668
2013.12.10

KUINSニュース No.83

京都大学 情報環境機構 KUINS 運用委員会
http://www.kuins.kyoto-u.ac.jp/

iPad を使った会議システム

目　　次

京都大学情報環境機構講習会開催報告

平成 25 年 10 月 11 日 (金) に，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．講習を行なった内容は以下の通りです．

- 「情報環境機構の提供するサービス」
- 「教職員グループウェアについて」
- 「教育に関する情報環境」
- 「学術情報ネットワーク (KUINS) の運用とサービスについて」
- 「京都大学の情報セキュリティ対策について」

今回は，希望があった熊取地区へ遠隔配信を行ないました．参加者数は，合計 15 名 (吉田 14 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．

また，これらの内容のビデオをサイバーラーニングスペース（研修用 Sakai) (https://cls.iimc.kyoto-u.ac.jp/) でも御覧になることが出来ます．都合により受講できなかった方は，こちらを是非御覧ください．

第 9 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 25 年 10 月 4 日 (金)，百周年時計台記念館国際交流ホールにおいて KUINS 利用負担金検討委員会が開催されました．本委員会では，KUINS 利用負担金規程を審議することを目的とし，予算，運用方針の審議や KUINS の現状報告などが行なわれます．

本年度も，KUINS の接続状況や今後展開するプランの説明，ネットワークサービスの実施状況報告，平成 24 年度決算報告，平成 25 年度予算執行計画報告が行なわれました．

各報告後，平成 26 年度利用負担金額についての審議がなされました．平成 25 年度の負担金検討委員会において，OPEN スペース設定情報コンセントに対する利用負担金導入の検討が提案されておりました（詳しくは KUINS ニュース No.79 を参照）が，今回の委員会においてその導入が承認されました．従いまして，平成 26 年度から，OPEN スペース設定情報コンセントに対しても月額 300 円の利用負担金が発生します．また，「KUINS-II でも KUINS-III でもない KUINS 利用をしている情報コンセント」については，これまで利用負担金が免除されておりましたが，平成 26 年度から，同様に月額 300 円の利用負担金が発生します．OPEN スペース設定の課金免除が廃止されることになった主な理由は以下の通りです．

OPEN スペース設定 VLAN は，主に公共の場でネットワーク利用を提供することに使われておりましたが，平成 24 年度 KUINS 利用負担金検討委員会にて，OPEN スペース設定情報コンセントの情報セキュリティポリシー上の問題点が指摘されました．これは，OPEN スペース設定 VLAN の管理責任者が利用者を把握することが困難であるため,「利用者が VLAN 管理責任者の同意を得る」というプロセスの遂行が困難であるというものです．一方，KUINS が運用開始しました「情報コンセント Web 認証サービス」では，対応する VLAN の管理責任者は情報環境機構であり，また，利用者が経なければならない認証の主体も情報環境機構であるため，

認証を行なうことで VLAN 管理責任者の同意を得ることが出来，上記の問題を解決できます．また，OPEN スペース設定情報コンセントの本来の用途である「公共性のあるスペースでは，認証を経ることによりインターネットアクセスを許可する」という利用は，Web 認証用情報コンセントで代替することが出来ます．従いまして，これまで OPEN スペース設定の KUINS-III を利用していた場所は，Web 認証用情報コンセントへ置き換えることで，上記の問題を解決していきます．例えば研究室などで「認証することにより VLAN 利用を許可する」という運用ポリシーも考えられますので，OPEN スペース設定 VLAN の運用は続けますが，OPEN スペース設定 VLAN を利用され続ける場合は CLOSED スペース設定 VLAN と同様の利用負担金を頂くという結論に至りました．

上述のように，OPEN スペース設定 VLAN の情報コンセントには利用負担金が発生することになりますが，web 認証用情報コンセントは情報環境機構の管理になりますので，利用者の方に対しては負担金が発生しません．この機会に OPEN スペース設定情報コンセントを web 認証用情報コンセントへと変更希望される方は，本号別記事「情報コンセント Web 認証サービスの運用開始について」を御覧下さい．上述しましたように，Web 認証用情報コンセントは公共性の高い場所についてのみ設置しますので，全ての申請が認められる訳ではありません．申請に対し，調査の上 KUINS 運用委員会で審議し可否を決定します．

情報コンセント Web 認証サービスの運用開始について

KUINS ニュース No.79 にて，情報コンセント Web 認証サービスのテスト運用の御案内をしておりましたが，この度本格運用に入りましたので，お知らせ致します．情報コンセント Web 認証サービスとは，認証用に設定された情報コンセント（以下「認証コンセント」という）に PC を接続し，Web ブラウザを立ち上げることにより認証画面が表示され，認証に成功するとインターネットが利用できるというサービスです．このサービスでは SPS-ID，ECS-ID，KUINS ビジター用アカウント，eduroam アカウントが使用できます．

利用するには，使用する情報コンセントを事前に認証用コンセントに設定する必要があります．利用を希望する場合は，部局情報セキュリティ技術責任者の方より「Web 認証サービス設定依頼書」を q-a@kuins.kyoto-u.ac.jp まで送ってください．また，サービス内容は KUINS ホームページ上にも書かれておりますので，ご参照下さい．

「京都大学情報環境機構サブドメイン利用内規」及び「京都大学情報環境機構サブドメイン利用に関する申し合わせ」の制定について

KUINS ニュース No. 80 において御案内しましたように，kyoto-u.ac.jp 配下のサブドメイン運用を明確化すべく，規程類の整備を行なって参りましたが，平成 25 年 2 月 20 日付けで「京都大学情報環境機構サブドメイン利用内規」及び「京都大学情報環境機構サブドメイン利用に関する申し合わせ」が制定され，これに基づいて運用を開始しておりますので，お知らせいたします．サブドメインの運用につきましては，KUINS のホームページ内にある当該ページを御覧下さい．

この運用における最大のポイントは，各サブドメインに「サブドメイン管理部局」および「サブドメイン管理責任者」を割り当て，責任を明確化することです．KUINS では平成 25 年 8 月までに，各部局にお問い合わせをかけ，既存の各サブドメインの管理部局と責任者を調査致しました．調査に御協力頂いた皆様には，この場をお借りして御礼申し上げます．

今後は，上記内容を KUINS 接続機器登録データベースに反映させ，サブドメインの管理も KUINS-DB 上で行なえるようにして参ります．

KUINS-DB 上でのサブドメイン管理責任者の作業内容について

本号別記事「『京都大学情報環境機構サブドメイン利用内規』及び『京都大学情報環境機構サブドメイン利用に関する申し合わせ』の制定について」にありますように，今後各サブドメインと管理部局や管理責任者の対応を，KUINS 接続機器登録データベース（KUINS-DB）上で管理することにしています．これに伴い，サブドメインを利用する新規ホスト申請や DNS レコードの変更を含む申請が行われた場合には，当該サブドメイン管理責任者に KUINS-DB 上で承認作業を行なって頂くことになりますので，よろしくお願い致します．また，当該サブドメイン直下に A レコード以外のレコードを設定する場合，サブドメイン管理責任者から KUINS-DB 上で申請して頂く必要があります．

また，これまでは，DNS レコードの変更作業は土日や夜間には行なっておりませんでしたが，土日や夜間にサーバ移行を行う等で DNS レコードの変更が必要な場合のために，KUINS を通らず，申請者が KUINS-DB から直接レコードを変更することも可能となりました．

詳細につきましては，下記のマニュアルを参照ください．

`https://db.kuins.kyoto-u.ac.jp/manual/user/part2/part2_13.html`
`https://db.kuins.kyoto-u.ac.jp/manual/user/part2/part2_15.html`

SSH Brute Force 攻撃への対策

理学研究科 学術推進部 情報技術室長
片桐 統

1. はじめに

Brute Force 攻撃とは，日本語ではパスワード総当り攻撃や辞書攻撃などと言われ，ID とパスワードの対をめったやたらに試してみて，どれかが当たると成功という攻撃です．もちろん，こんな攻撃を手動で行ってもなかなか当たるものではありませんが，コンピュータを利用すれば短時間でかなりの ID とパスワードの組み合わせを試すことができます．

シンプルでわかりやすい攻撃である分，攻撃ツール作成なども非常に簡単に行え，成功すれば即 ID の乗っ取りが完了しますので，脅威度としては非常に高い攻撃です．今回は，この Brute Force 攻撃のうち，SSH サーバに対して行う対策法をお示しします．なお本文の SSH サーバの環境は，Debian Wheezy を想定していますが，多少の違いはあるにせよ，UNIX 系 OS（Mac OS X を含む）なら同様の対策が可能です．

2. 対策の第一歩目は，繋がせないこと

この攻撃が成功するには，当然のことですが，攻撃者がサーバの SSH ポートへ接続可能で，ID とパスワードの入力が可能である必要があります．裏を返せば，対策の第一歩目は,「信用できない IP アドレスからの SSH 接続を拒否する」ことです．方法は，まず/etc/hosts.deny にて，すべての ssh 接続を拒否します．

```
sshd:ALL
```

次に，接続を許可したい IP アドレス等を，/etc/hosts.allow に記載します．

```
sshd:130.54.xxx.xxx                 #単独の IP を指定
sshd:130.54.                         #130.54/16 を指定
sshd:10.226.x.0/255.255.255.192      #10.226.x.0/26 を指定
```

3. パスワード認証をやめて，公開鍵認証にする

上記のとおり，この攻撃が成功するには，ID とパスワードの入力が可能であることが必要です．ということは，パスワードを受け付けなければ，成功しません．このことを踏まえ，パスワード認証を拒否し，公開鍵認証のみにて運用する方法をご紹介します．

公開鍵認証では，SSH サーバにクライアントの公開鍵を保存しておきます．クライアントからの接続要求があると，サーバは乱数を当該ユーザの公開鍵を使って暗号化し，クライアントに送ります．クライアントは自身の秘密鍵を使って復号して，乱数を取り出してハッシュ値をサーバに送付します．サーバで元の乱数のハッシュ値と比較して，一致していたら認証するという方式です．乱数のクライアントへの送付は暗号化されており，クライアントとサーバ間でやりとりされるハッシュ値は毎回異なるため，仮に ID を攻撃者が把握していても，辞書攻撃は非常に困難です．OpenSSH サーバで，パスワード認証をやめて，公開鍵認証にするには，/etc/ssh/sshd_conf の，以下の部分を書き換えて，sshd を再起動してください．

```
# PasswordAuthentication yes    （デフォルトは yes）
 PasswordAuthentication no
```

ユーザの鍵ペアの作り方は，それぞれのクライアントにより異なります．Linux の場合は，ssh-keygen を利用します．

```
$ ssh-keygen -t rsa -f ssh_key
```

これで，カレントディレクトリに ssh_key と ssh_key.pub というファイルが出来上がります．ssh_key が秘密鍵，ssh_key.pub が公開鍵です．この ssh_key.pub をユーザの $HOME/.ssh/authorized_keys に保存すれば，公開鍵認証になります．

4. そして…接続回数制限

ここまで，アクセス元の制限とパスワード認証の制限による対策をお示ししましたが，これでは環境によっては対策が取れない場合があります．そこで，ssh サーバへの単位時間あたりのアクセス回数を制限することで，brute force 攻撃を諦めさせるという方法を紹介します．

単位時間あたりに，同一接続元から多数のアクセスがあった場合，一定時間その接続元からのアクセスを拒否するように iptables に書くのです．ですが，言うは簡単ですが，これを実際に自分で書くとなると非常に難しいです．しかし，世の中には便利なものがあります．Sshguard というツールがあります．これは，導入設定するだけで，自動的に iptables のルールを書き換えてくれます．Debian Wheezy の場合は，オフィシャルパッケージ化されており，インストールは非常に簡単です．

apt-get install sshguard

あとは，/etc/sshguard のホワイトリストを編集（付属ドキュメントをお読みください．わからなければ，デフォルトでも問題ありません）し，sshguard を起動するだけです．接続回数制限をする接続回数や，アクセス拒否する時間の長さなどは，コマンドライン引数で調整します．デフォルトでもとりあえず動作はしますが，詳しい設定方法は，マニュアルをお読みください．

5. おわりに

今回，このような文章を書かせていただこうと思った背景には，身近なサーバにトロイの木馬が仕掛けられ，そのサーバから ssh brute force 攻撃を多数行ったため，学内外に多大なご迷惑をおかけしたことに対する反省から，もし仮に ssh brute force 攻撃が学内外から行われても，被害の発生を少しでも減らせればと考えたからです．その際に，実際に攻撃を受けられた方，対処を頂いた情報セキュリティ対策室の皆様には，この場をお借りして謝罪と感謝をいたします．

---

iPad を用いた SaaS 型ペーパレス会議システムの運用開始について

～KUINS 無線 LAN アクセスポイントがあればどこからでも直ぐに利用可能～

情報部

平成 25 年 11 月から，全学で利用出来る「iPad を用いた SaaS（Software as a Service）型ペーパレス会議システム」の運用を開始しています．本システムは，生命科学研究科が中心となってシステムの選定・改修等を行い，全学システムとして情報部から提供することとなりました．会議システムの運用で必要となるサーバは，汎用コンピュータの VM ホスティングサービスにより提供しており，個々に用意する必要がありません．専用の会議 ID によりセキュリティを確保しています．既に生命科学研究科が中心となり，約 1 年間の試行期間を経ております．また，テスト利用を含め 13 部局が導入し，会議進行及び会議準備業務の効率化を図っています．

iPad の会議システムで必須となる無線 LAN 環境では，KUINS 運用委員会の協力により,「学内ユビキタス環境整備 (無線 LAN 環境整備)」の一環として全学に設置されている KUINS 提供の無線 LAN アクセスポイントに新たに設定された事務システム用 ESSID が利用可能となっています．これにより本システムでは，利用部局で新たに無線 LAN 環境を整備する必要がなく，また，全学に設置された約 1,000 台のアクセスポイントを利用できるため，特定の場所に限定されることなくペーパレス会議を行うことが可能です．

その他の特徴としては，

- 議事次第機能や投票機能をはじめ，部局でニーズの高い機能を多数実装
- 高度なセキュリティ対策を実施

等があります．

システムの詳細・導入等に関するお問い合わせは e-office@mail2.adm.kyoto-u.ac.jp までお願い致します．

無線 LAN 基地局に関するお知らせ

KUINS ニュース No. 82 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．今回は次の表に示す 5 部局，計 12 箇所に設置しました．

理学研究科	理学研究科 1 号館	119 号室
工学研究科	工学部 3 号館（西館）	4 階リフレッシュルーム前
	工学部物理系校舎	316 室前廊下，718 室前廊下
	イノベーションプラザ棟	事務室前廊下，セミナー室天井 (2 箇所)，2 階会議室天井，3 階控え室前廊下
防災研究所	宇治地区研究所本館 E 棟	防災研究所特別会議室 (E-320D)
東南アジア研究所	東南アジア研究所東棟	E311 室
生態学研究センター	生態学研究センター研究実験棟	図書室

今まで紹介しております一連の作業は,「学内ユビキタス環境整備 (無線 LAN 環境整備)」の一環として実施中です．講義室や会議室，共同利用者控室等，公共性の高い空間で利用できるように設置作業を進めております．また，部局独自で無線 LAN を追加設置される場合，購入される基地局が現在 KUINS で導入しているアライドテレシス製の AT-TQ2403，AT-TQ2450，AT-TQ3600 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．

無線 LAN についての御相談・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．

KUINS 会議日誌

平成 25 年 8 月 31 日〜平成 25 年 11 月 29 日

情報環境機構 KUINS 運用委員会

平成 25 年 9 月 30 日 (平成 25 年度 第 6 回)

- KUINS 利用負担金検討委員会開催について
- KUINS ニュースについて
- 基盤コンピュータシステム調達について
- KUINS のサービス整備状況について
- KUINS のサービスと現状について
- NII 提供サーバ証明書プロジェクト 2 発行状況
- その他

平成 25 年 10 月 25 日 (平成 25 年度 第 7 回)

- KUINS 利用負担金検討委員会開催について
- KUINS ニュースについて
- 基盤コンピュータシステム調達について
- KUINS のサービス整備状況について
- KUINS のサービスと現状について
- NII 提供サーバ証明書プロジェクト 2 発行状況
- その他

平成 25 年 11 月 25 日 (平成 25 年度 第 8 回)

- KUINS-III 利用負担金改正についての連絡方法の検討
- KUINS 敷設光ケーブルの借用について
- KUINS-DB のパスワード文字列長について
- KUINS ニュースについて
- 公衆無線 LAN 接続にかかる契約書について
- KUINS のサービス整備状況について
- KUINS のサービスと現状について
- NII 提供サーバ証明書プロジェクト 2 発行状況
- 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

情報部 情報基盤課 情報環境支援グループ ネットワーク担当 (075-753-7432)