

KUINS ニュース No. 59

京都大学 情報環境機構 KUINS 運用委員会

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



電話交換機 (PBX) 更新のための電話庁舎工事の様子

目 次

耐震改修工事に対する KUINS の対応について	718
大型計算機システム電子メールサービス sakura での fml 利用方法 (2)	718
spam メールの学外転送制限におけるメールサーバの新規設置	720
認証つき送信用メールサーバ運用開始のお知らせ	721
エラーメールに偽装した spam メールについて	724
送信ドメイン認証の影響について	725
教育用コンピュータシステムの利用コード (アカウント) について	726
国立大学法人等における情報セキュリティポリシー策定について	730
平成 19 年度情報セキュリティ講習会の開催について	730
本部地区電話交換機 (PBX) 更新について	731
KUINS 会議日誌	732
お知らせ	732

耐震改修工事に対する KUINS の対応について

京都大学では、昨年度から全学的に大規模な耐震改修工事が行われています。

昨年度は、農学部総合館，理学部 3 号館，工学部 3 号館，工学部 4 号館，吉田南総合館北棟・東棟や吉田南 1 号館などについて実施されました。また，今年度は，理学部 1 号館をはじめ，理学部 5 号館，農学部総合館，工学部 5 号館，工学部 7 号館，工学部 9 号館，吉田南総合館，医学部 D 棟，医学部図書館，RI センター，医学部保健学科，宇治研究所本館，遠隔地では，霊長類研究所，原子炉実験所など数多くの建物にて工事が行われています。

KUINS では，これらの大規模な耐震改修工事に伴う情報環境整備につきまして，設置していたネットワーク機器の撤去をはじめとして，改修工事後のネットワークの設計，機器類の設置及び VLAN の設定等，皆様方が引越しと同時にネットワークが利用できるよう実施しております。しかし，工事スケジュールの関係や工事完了時期の重なりにより，遅れが生じることがあります。あらかじめご了承くださいますよう御願います。

なお，耐震改修工事だけでなく，今後，大規模な改修を予定されている場所がありましたら，早めに御連絡いただきますよう，御願います。

大型計算機システム電子メールサービス sakura での fml 利用方法 (2)

学術情報メディアセンター
大型計算機システムメールサービス担当

KUINS ニュース No.58 において，大型計算機システム電子メールサービス sakura 上での fml 利用方法を紹介しました。今回はインストールの方法と基本的操作を紹介しましたが，本稿では引き続き，便利な利用方法を御紹介します。今回は，**メーリングリストへの投稿可能者設定**，**メンバーの自動登録**，**Subject ヘッダのナバリング**について紹介します。

ここでは，前回と同じ例を用いて説明します。すなわち，x12345 というアカウントを持っている人が，hoge hoge というメーリングリストを作成し，作られたメーリングリストのアドレスが hoge hoge@x12345.sakura.kudpc.kyoto-u.ac.jp であるものとします。

まず，以下の設定方法において，コマンドラインからの設定変更を使いますので，その方法を簡単に説明しておきます。インストール時に作った fml というディレクトリで，以下のコマンド（以降，**config コマンド**と呼びます）を実行します。（KUINS ニュース No.58 の最後で，誰からもメールを受け付ける設定にした時のコマンドと同じです。）

```
x12345@sakura ~/fml % ./makefml config hoge hoge
```

これ以降，対話形式による設定変更が開始されます。問い合わせに対して，該当する番号を入力して行くことになります。なお，設定を全て終了して config コマンドから抜けないと，設定内容は反映されませんので，ご注意ください。

投稿可能者設定

メーリングリストへの投稿可能者を設定することができます。config コマンドを実行した後，以下を実行して下さい。

- ・メニューの中の「1 POLICY OF ACCESS (WHO CAN POST AND USE COMMANDS)」を選ぶ.
- ・メニューの中の「1 PERMIT_POST_FROM」を選ぶ.

ここで、「1 members_only」(メンバーのみ投稿可)または「2 anyone」(誰でも投稿可)を選びます。(「3 moderator」はここでは説明しません.) スпамメールを流される可能性が大いにあるので、「2 anyone」はお勧めできません.

また、「1 members_only」(メンバーのみ投稿可)を選んだ場合に、メンバー以外からの投稿があった際の動作を設定することができます. 上と同様に、config コマンドを実行して下さい. そして、以下を実行して下さい.

- ・メニューの中の「1 POLICY OF ACCESS (WHO CAN POST AND USE COMMANDS)」を選ぶ.
- ・メニューの中の「2 WHEN_POST_FROM_NOT_MEMBER」を選ぶ.

ここで、「1 reject」を選ぶと、「メンバーでないため、メールはメーリングリストには配布されなかった」旨のメッセージが、送信者へ返ります. また、「3 ignore」を選ぶと、メッセージは返らず、単に投稿が無視されるだけです. 「2 auto_subscribe」は、自動登録に関係しますので、次項で説明します.

メンバーの自動登録

メーリングリストのメンバーは、管理者が手動で登録しますが (KUINS ニュース No.58 参照)、管理の手間を省くため、登録希望者からのメールにより自動登録をすることが出来ます. 上述した設定項目「1 POLICY OF ACCESS (WHO CAN POST AND USE COMMANDS)」において、「1 PERMIT_POST_FROM」を「members_only」に、「2 WHEN_POST_FROM_NOT_MEMBER」を「auto_subscribe」にしておきます. また、同じ項目の「3 PERMIT_COMMAND_FROM」を「anyone」に、「4 WHEN_COMMAND_FROM_NOT_MEMBER」を「reject」に設定しておきます.

config コマンドを実行した後、以下を実行して下さい.

- ・メニューの中の「2 REGISTRATION METHOD TYPE」を選ぶ.
- ・メニューの中の「1 AUTO_REGISTRATION_TYPE」を選ぶ.

「1 AUTO_REGISTRATION_TYPE」の設定により、4 種類の自動登録方法がありますが、それを以下で説明します.

(1) 「AUTO_REGISTRATION_TYPE」を「1 confirmation」とする場合

登録希望者は、メーリングリスト (hogehoge@x12345.sakura.kudpc.kyoto-u.ac.jp) 宛にメールを送ります. そのメールには、本文に 1 行、「subscribe Taro Yamada」とだけ書きます. (ただし Taro Yamada は、登録希望者の本名.) メーリングリストの管理者から、登録意志確認のメールが登録希望者宛に (自動で) 送られて来ます. その内容に従って、再度メールを送れば、その送信アドレスがメーリングリストに登録されます.

(2) 「AUTO_REGISTRATION_TYPE」を「2 body」とする場合

登録希望者は、メーリングリスト (hogehoge@x12345.sakura.kudpc.kyoto-u.ac.jp) 宛にメールを送ります. そのメールには、本文に 1 行、「subscribe」とだけ書きます. 即座にアドレスがメーリングリストに登録されます. ところが、subscribe の後にメールアドレスを書くと、そのメールアドレスが自動的に登録されてしまいます. このように、他人のメールアドレスや、実在しないメールアドレスをも登録できますので、この方法はお勧めできません.

(3) 「AUTO_REGISTRATION_TYPE」を「3 subject」とする場合

上記 (2) と同様の動作をします. ただし、(2) において本文中に書いていた記述を、メールの Subject 行に書くことになります.

(4) 「AUTO_REGISTRATION_TYPE」を「4 no-keyword」とする場合

上記 (2) と同様の動作をします. ただし、登録希望メールは空メールで結構です (Subject や本文に何か書いてあっても構いません). 送信者を自動登録しますが、From 行を偽ることにより、上記と同様の悪戯が可能です. ですので、これもお勧めできません.

Subject ヘッダのナンバリング

メーリングリストに投稿されたメールの Subject 行に、通し番号を付けることができます。config コマンド実行後、

「5 HEADER CONFIGURATIONS」

「1 SUBJECT_TAG_TYPE」

と進んで下さい。ここで、番号を付ける形式を選択します。番号選択リストがそのままサンプルになっているので、希望するものを選択します。(番号が付かず、メーリングリスト名だけのものもあります。) 次に「5 HEADER CONFIGURATIONS」へ戻り、メニューの中の「2 SUBJECT_TAG_FIGURE」を選んで下さい。ここでは、Subject に付く番号の桁数を選択します。(1 桁を選んだからと言って、10 通までしか送れない訳ではありません。桁数が小さい時に、上位桁に 0 を幾つ加えるかと言う選択です。)

spam メールの外転送制限におけるメールサーバの新規設置

KUINS ニュース No.58 でお知らせしましたように、KUINS のスパムチェックサーバによりスパムと判定されたメールは、KUINS メールサーバでは学外への転送を禁止するという運用を、2007 年 11 月 1 日より開始しました。本運用では、原則として、KUINS メールサーバはスパム判定済メールは受けとらないという設定になっています。従いまして、部局のメールサーバや個人の環境において、11 月 1 日以降もスパム判定済メールをフィルタせず転送する設定にしていると、拒否されたメールが溜るなどして、サーバやパソコンの負荷が上がってしまう可能性があります。

これを緩和するために、スパム判定済メールの転送を拒否するのではなく、一旦受け取った上で捨てる動作をするメールサーバを用意しました。すなわち、拒否されて元のメールサーバにメールが戻されることがなくなります。この新しいメールサーバの名前は、sc-filt.kuins.net です。このメールサーバは、学内のみからしか利用できませんので、ご注意下さい。利用方法は以下の通りです。

部局のメールサーバから利用する場合

メールの送信先にこのサーバを指定して下さい。設定方法は、例えば 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」の (2) を参考にして下さい。

個人で利用する場合

自分宛にきたメールを、現在例えば foo@bar.com というメールアドレスに転送しているとします。このメールアドレスの「@」を「%」に変更した上で、@sc-filt.kuins.net を後ろに付け足したメールアドレス foo%bar.com@sc-filt.kuins.net に転送するよう設定して下さい。sc-filt.kuins.net でフィルタ作業をした後、問題のないメールのみを foo@bar.com に転送します。

認証つき送信用メールサーバ運用開始のお知らせ

KUINS ニュース No.58 でお知らせしましたように、KUINS の送信用メールサーバが、SPAM 転送サーバとしてブラックリストに登録され、送信したメールが拒否あるいは遅配される問題が発生しています。これは、主に、受信した SPAM メールを学外へそのまま転送することが原因であり、KUINS 利用者が発信するメールによる問題は少ないと考えられます。

そこで、KUINS では、上記の影響を受けないように、専用の中継サーバを別に用意致しました。サーバ名は smtp-auth.kuins.kyoto-u.ac.jp です。このサーバが不正中継に利用されることを防ぐために、利用者に SMTP AUTH 認証を課すことにしました。認証用のアカウントとパスワードは、教育用計算機システム利用のものと同じです。

なお、このサーバを利用して送ることの出来るメールのサイズは 50MB 以下です。これを超えるメールは拒否します。また、このサーバはウイルスチェックを行います。次のような場合にはウイルスチェックを行いませんので、端末側でウイルスチェックを必ず行うようお願い致します。

- 1 通のメール（ヘッダ・本文・添付ファイルの合計）が 50MB を超えている場合（添付ファイルが圧縮されている場合、圧縮前の添付ファイルサイズが合計サイズとしてみなされます）
- パスワード付きの ZIP 形式で圧縮されたファイルなど、解凍が出来ない圧縮ファイル
- 13 回以上多段圧縮されているファイル
- tar, gzip, rar, lzh, lha, cab, arj, zip 以外の形式で圧縮されているファイル
- Base64・uuencode・binhex 以外の形式でエンコードされているファイル

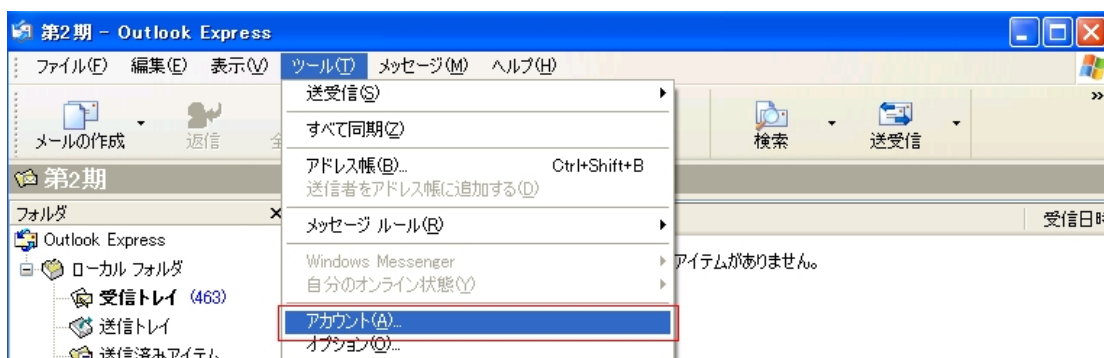
このサーバは、学外からでも利用可能です。特に、KUINS ニュース No.54 「Outbound Port 25 Blocking と MSA (TCP port 587)」で御紹介した「Outbound Port 25 Blocking と MSA (TCP port 587)」における「3. KUINS 内にある MSA 対応のサーバを用いる」に該当するサーバとして利用することができます。また対応プロトコルは、

- MSA (TCP port 587) TLS (Thunderbird など)
- SMTP/SSL (TCP port 465) SSL (Outlook Express)

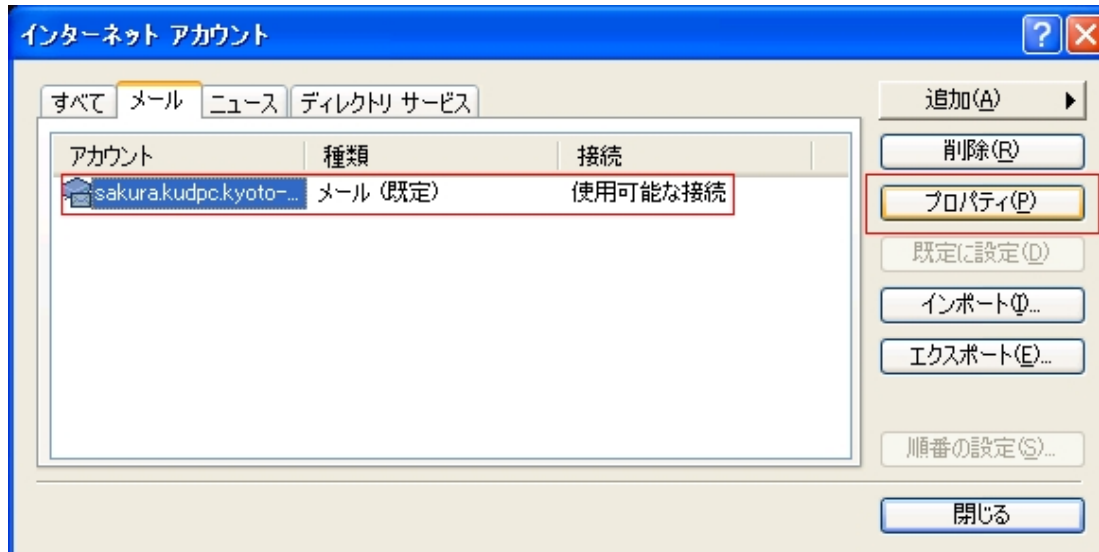
があります。

以下では、Microsoft Outlook Express からの SMTP AUTH サーバ利用のための設定方法を紹介します。Thunderbird の設定例については KUINS ニュース No.54 「大型計算機システムメールサービスの SMTP/TLS および SMTP/SSL 対応について」の (1) を参考にして下さい。

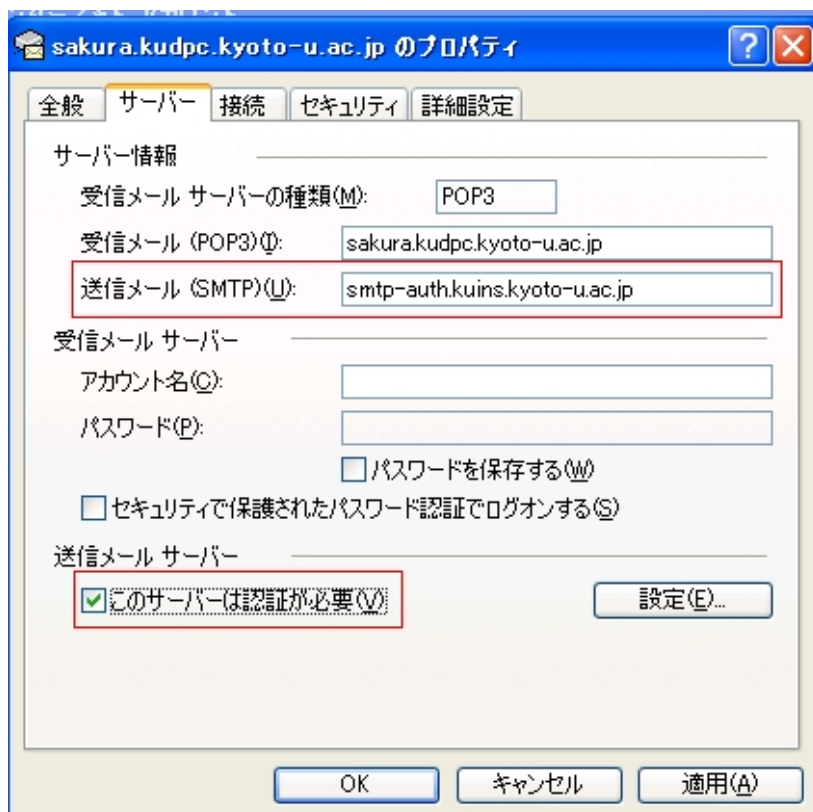
1. メニューの「ツール」, 「アカウント」を選びます。



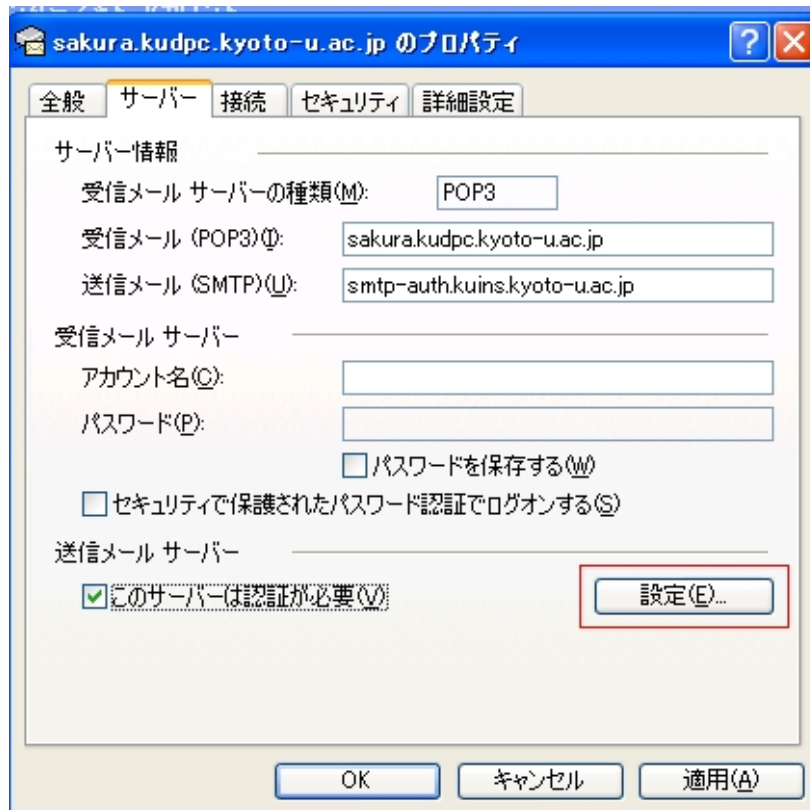
2. この設定を適用するアカウントを選び、「プロパティ」を選択します。



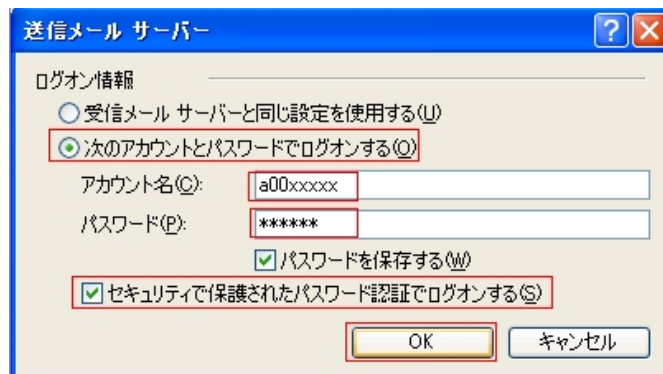
3. 「送信メール」にサーバ名 (smtp-auth.kuins.kyoto-u.ac.jp) を記述します。「このサーバーは認証が必要」にチェックを入れます。



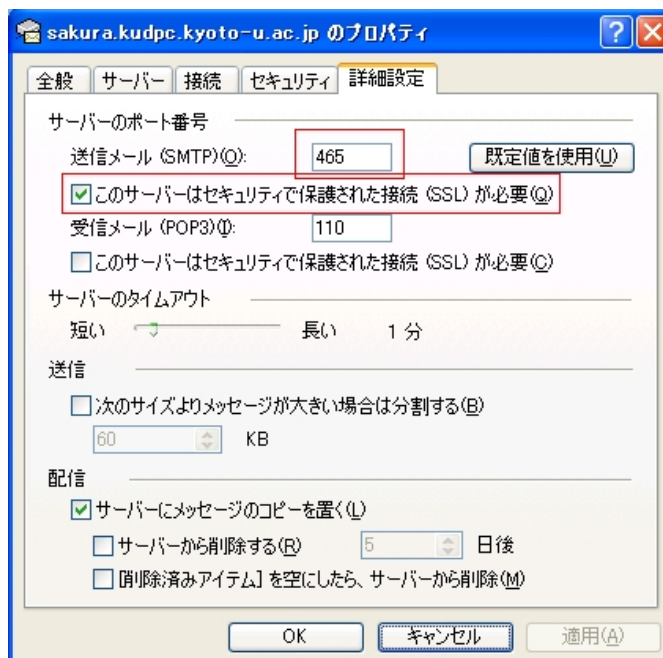
4. 「設定」をクリックします。



5. 「次のアカウントとパスワードでログオンする」をチェックします。教育用計算機システムのアカウントとパスワードを記入します。「セキュリティで保護されたパスワード認証でログオンする」をチェックします。



6. 「詳細設定」を選択します。送信メールのポート番号を「465」と記入します。「このサーバーはセキュリティで保護された接続（SSL）が必要」をチェックします。



7. 以上で設定は終了です。「OK」ボタンを押し、設定ウインドウを終了して下さい。

エラーメールに偽装した spam メールについて

最近、エラーメールに偽装した SPAM メールが増えてきています。

本学に届く SPAM メールの何割かは到達不能なアドレス宛のものです。SPAM メールは送信元アドレスも偽装されていることがほとんどです。そのような SPAM メールに対して user unknown のエラーメールを返すことは、無駄なだけでなく、**本学からエラーメールに偽装した SPAM を大量送信していると判断される恐れ**があります。現状、KUINS のメール中継サーバは帯域制限や一時的な受信拒否を大手プロバイダを含むいくつかのメールサーバから受けており、これが原因であることが疑われています。

つきましては、部局で運用されているメールサーバにおいて、送信を KUINS のウイルスチェック機能付メール中継サーバを経由して行っている場合には、受信において SPAM 判定を経由するようにし、SPAM 判定されたメールを学外へは送らないようフィルタする処理（58 号記事ならびに本号別記事も参照）をしていただくだけでなく、**SPAM 判定されたメールについては user unknown を返さないよう設定して**くださるようお願いいたします。

KUINS が提供する SPAM 判定をお使いの場合、X-Kuins-Spam ヘッダのついたメールについて user unknown を返さず捨てるようにする設定は、sendmail の場合は本号の WEB 版 (<http://www.kuins.kyoto-u.ac.jp/news/59/>) のこの記事からリンクを張っておりますので、そちらをご参照下さい。

送信ドメイン認証の影響について

最近、国内外の機関において、メール受信の際に、RFC 4408(<http://www.ietf.org/rfc/rfc4408.txt>), Sender Policy Framework (http://www.openspf.org/SPF_Record_Syntax)に基づく、送信ドメイン認証を行う所が増えてきております。身近な例としては、NTT DoCoMo (http://www.nttdocomo.co.jp/service/mail/imode_mail/sender_id/)において、2007年11月1日より、送信ドメイン認証の運用が始まっております。この影響を受けるのは以下のような場合です。

1. 「送信ドメイン認証に対応していないドメイン」に所属する発信者メールアドレスで、メールを送信する。
2. 学外 (ISP 等) のメールサーバを使用して、発信者メールアドレスが本学の所属であるメール (foo@hogehoge.kyoto-u.ac.jp) を送信する。
3. 本学のメールサーバを使用して、発信者メールアドレスが学外の所属であるメールを送信する。

1 と 2 につきましては各ドメインが定義する認証のポリシーに、3 については学外組織が定義するポリシーに従います。影響は、使用するドメインの認証ポリシー、および、受信先メールサーバの運用ポリシー等によりますが、最悪の場合は、受信拒否を受け、さらには、エラーメールが送信者本人に送られない可能性もあります。現在、本学の大多数のドメインが 1 に該当しております。

送信ドメイン認証を行う相手先にメールを送信することが予想される場合は、送信ドメイン認証に対応する必要があります。一例ですが、送信と受信サーバが同一である場合、

```
hogehoge.kyoto-u.ac.jp. IN TXT "v=spf1 mx ~all"
```

メールの送信に KUINS 運用委員会が提供するメール配送サーバを使用されている場合、

```
hogehoge.kyoto-u.ac.jp. IN TXT "v=spf1 mx ip4:130.54.130.64/27 ip4:192.50.9.0/27 ~all"
```

と DNS 情報に記述することで対応できます。この他の書式が必要な場合は、以下の URL を参考に、SPF レコードを作成ください。

<http://www.openspf.org/>

<http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/default.aspx>

以上の説明は 1 については考慮していますが、2 については対応しておりません。このため、2 のような利用をされる場合は、メールが届かない可能性もある点に注意してください。

また、メールサーバにおいて、

- KUINS-III のプライベート IP アドレスに設置されている
- 学内のメールサーバに直接送信をする

が共に合致し、かつ、受信先メールサーバがドメイン認証を行っている場合も、メールが届かない可能性があります。一つの解決策は、ドメイン認証の情報を、当該サーバの IP アドレスを明記することです。その場合、プライベート IP アドレスの情報を外部に公開するリスクが生じます。一方、受信先側で KUINS-III の IP アドレスに対応するのも管理が複雑になります。このため、送信時に KUINS で運用するメールサーバ `sendmail.kuins.net` に配送を依頼するのが最も簡単な手法です。

教育用コンピュータシステムの利用コード (アカウント) について

情報環境機構
情報教育支援サービス

情報環境機構 教育用コンピュータシステムは、学生の皆様の学習を主な目的として提供されています。利用コード (アカウント) を取得すると、教育用コンピュータシステム提供の PC 端末、電子メール、情報コンセント等を利用することができます。また「2. ご利用いただけるサービス」の表 2 に記載されているサービスを利用する際にも教育用コンピュータシステムの利用コードが必要です。

1. 利用コードを新規に取得したい場合

教育用コンピュータシステムの利用コードを取得できるのは

- ・ 本学の学生
- ・ 本学の教職員
- ・ その他機構長が特に認めた者

となっています。申請される方の身分により手続き方法が異なります (表 1)。

- (a) **学生の方** (学部生、大学院生、研究生、聴講生、科目等履修生、特別聴講学生、特別研究学生、研修員など)
- (b) **教職員の方** (常勤教職員、非常教勤職員、外国人教師、客員教授、招へい外国人学者、研究員、外国人特別研究員、外国人共同研究者、共同研究者、特別研究員、民間等共同研究員など)、**名誉教授の方**
- (c) **その他の方**

表 1: 申請者の身分ごとの利用コード取得手続き

申請される方	利用コード取得のための手続き
(a) の方	利用コード交付講習会 (注 1) を受講してください。
(b) の方	京大発行の身分証明書を持参の上、窓口 (注 2) にて利用申請を行ってください。お持ちでない方はこの記事の最後に掲載しています問い合わせ先までご連絡ください。
(c) の方	この記事の最後に掲載しています問い合わせ先までご連絡ください。

注 1: 利用コード交付講習会は月に 1 回程度開催しています。多くの新入生を迎える 4 月は 30 回ほど開催しています。利用コード交付講習会の日程は、教育用コンピュータシステムのトップページ (<http://www.iimc.kyoto-u.ac.jp/services/ecs/>)

注 2: 学術情報メディアセンター南館 学内共同利用担当で受付しています。他に、学術情報メディアセンター北館、宇治キャンパス、桂キャンパス、一部の図書室 (医学図書館など) でも申請書を受け付けています。詳細は、教育用コンピュータシステムのトップページ (<http://www.iimc.kyoto-u.ac.jp/services/ecs/>) の「利用コードの取得」をご覧ください。

2. ご利用いただけるサービス

教育用コンピュータシステム提供の PC 端末、電子メール、情報コンセント等を利用することができます。また、表 2 にあげるサービスを利用する際にも教育用コンピュータシステムの利用コードが必要です。

表 2：教育用コンピュータシステムの利用コードが必要な他のサービス

提供組織	サービス	備考
情報環境機構 KUINS 運用委員会	SSH ポートフォワードサービス	注 3
情報環境機構 KUINS 運用委員会	PPTP サービス	注 3
情報環境機構 KUINS 運用委員会	SMTP-Auth サービス	
情報環境機構 セキュリティ対策室	情報セキュリティe-Learning	
情報環境機構 遠隔講義支援サービス	教室予約システム	
図書館機構	MyKULINE	
図書館機構	電子ジャーナル・データベース	注 3

注 3: 利用登録後あるいはパスワード変更後、実際に反映されるまでに約 1 時間ほどお時間をいただいています。

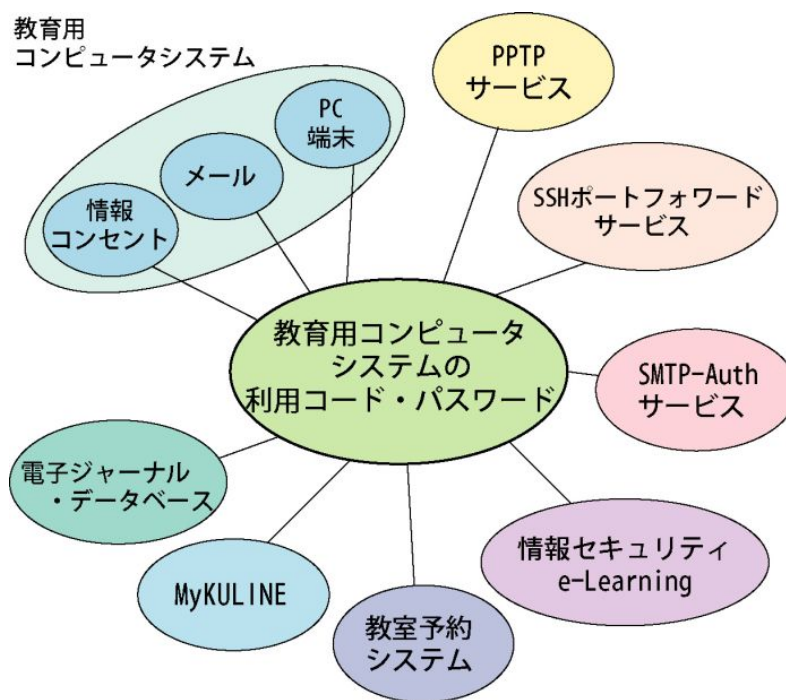


図 1：教育用コンピュータシステムの利用コードが必要なサービス

3. サービスを受けられないとき

表 2 にあげましたサービスの中には PPTP サービスのように事前に設定が必要なものもあります。設定終了後に、利用を開始しようとするとき何らかのエラーが表示され、利用コードあるいはパスワードの入力ミスであるのか、設定ミスなのかがよくわからないことがあります。表示されるエラーメッセージだけが頼りなのですが、理解不能なメッセージが表示されることもあります。これらのサービスで利用コードとパスワードを入力しても正しく利用できない場合、

- (1) 利用コード・パスワードが間違っている、あるいは無効化されている
- (2) サービスに関して行うべき設定をミスしている

のどちらかが考えられます。(1), (2) を切り分けるために、教育用コンピュータシステムの Web メール (DEEP-Mail) にログインしてみてください。Web メールへは、教育用コンピュータシステムのトップページから「電子メールサービス」をクリックしてログイン画面に進み、利用コードとパスワードでログインしてください。

【Web メールにログインできる場合】

利用コード・パスワードは正しいので、設定に間違いがないか確認してください。不明な場合はそれぞれのサービスの提供元にお尋ねください。その際「教育用コンピュータシステムの Web メール (DEEPMail) にログインできた」ということをお伝えください。

【Web メールにログインできない場合】

- ・利用コードが間違っている
- ・パスワードが間違っている
- ・利用コード、パスワード両方とも間違っている
- ・利用コードが無効になっている

主な原因としてこのようなものが考えられます。いずれも利用者側では対応できませんので、この記事の最後に掲載しています問い合わせ先までご連絡ください。

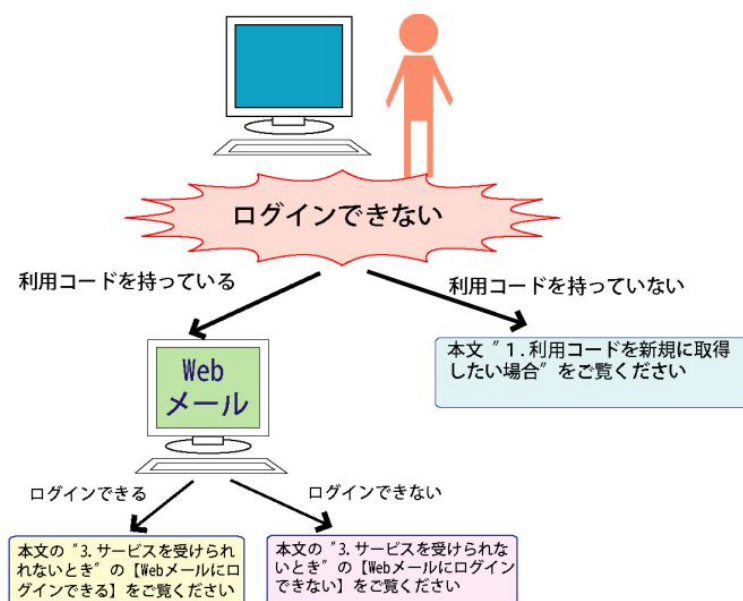


図 2：ログインできないとき

4. 利用コードとパスワードの管理について

利用コードで利用者を特定し、パスワードで利用者が本人であることを証明します。他人に悪意をもって利用コードを使われると、

- ・データやメールの閲覧、消去、改竄
- ・当人になりすまして信用をおとしめるメールなどを発信

ということが可能になります。利用コードとパスワードの適正な管理が必要となります。具体的には、次のようなことに注意してください。

- ・利用コードは不必要に他人に教えない
- ・パスワードは絶対に秘密にする
- ・パスワードは適当な間隔で変更する（できれば半年ごと）
- ・推測されにくいパスワードを使う
- ・ログイン（ログオン）したまま PC を離れない

ログインできない際の問い合わせメール内にパスワードを書いてこられる方がいます。絶対にパスワードをメールに書かないでください。情報環境機構の職員であってもパスワードをお尋ねすることはありません。

自分自身の利用コード・パスワードを適正に管理することはもちろん，他人に利用コードを使用させたり，他人の利用コードを使用することも禁止されており，不正なアクセスとみなされます．十分にご注意ください．

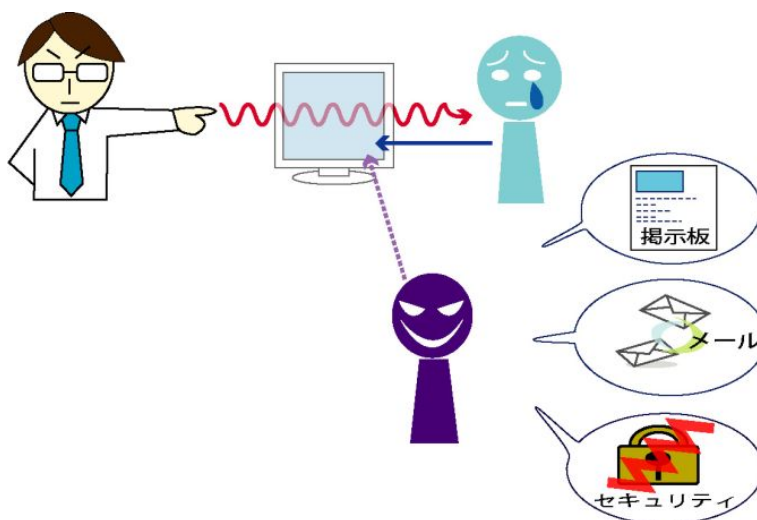


図 3：他人に利用コードを貸してはいけません！

5. 利用コードとパスワードについて特に注意していただきたいこと

例えば，あなたの利用コードとパスワードを他人に教え，他人があなたの利用コードを用いて何らかの不正行為を行うと，その責任は利用コードの持ち主であるあなたが負うことになります．また，PCに利用コードとパスワードを記憶させた状態で，他人があなたのPCとあなたの利用コードを使って何らかの不正行為を行うと，その責任も利用コードの持ち主であるあなたが負うことになります．どのような場合であっても，たとえ非常に短時間であっても，絶対に他人と利用コードを共用しないでください．くれぐれも利用コードとパスワードは適正に，かつ，厳重に管理をお願いします．

何か不明な点がありましたら，ご遠慮なく次の問い合わせ先までご連絡ください．

《問い合わせ先》

Web のお問い合わせフォーム (<http://www.iimc.kyoto-u.ac.jp/services/ecs/contact.php>) より入力してください．

国立大学法人等における情報セキュリティポリシー策定について

情報環境部 情報基盤課
情報セキュリティ対策室

政府機関の情報セキュリティ対策のための統一基準(<http://www.nisc.go.jp/active/general/kijun01.html>)が平成19年6月14日に改訂されました。本学の情報セキュリティポリシーもこれに準拠すべく、全学情報セキュリティ幹事会において、検討中です。

また、統一基準に対応して、国立情報学研究所学術情報ネットワーク運営・連携本部 国立大学法人等における情報セキュリティポリシー策定作業部会および電子情報通信学会 ネットワーク運用ガイドライン検討ワーキンググループにより、平成18年度から検討されてきた「高等教育機関の情報セキュリティ対策のためのサンプル規程集(<http://www.nii.ac.jp/news-jp/2007/11/post.42.shtml>)」が公開されました。

本学においても、本サンプル規程集を参考に情報セキュリティポリシーを改訂する予定です。

平成19年度情報セキュリティ講習会の開催について

情報環境部 情報基盤課
情報セキュリティ対策室

各部署の情報セキュリティ担当者及び情報機器やネットワークの管理担当者を対象とした情報セキュリティ講習会を下記の通り開催します。受講希望者は、所属、氏名、連絡先メールアドレス、連絡用電話番号を情報セキュリティ対策室宛に電子メールでお知らせ願います。

日時：平成20年3月10日(月) 14時～16時30分

場所：京都大学 学術情報メディアセンター 南館2階201, 202号室

定員：200名

プログラム：「情報セキュリティポリシーの見直しについて ―政府統一基準への対応―」

(注) プログラムは変更になることがあります。

受講申込要領

締め切り：平成20年3月5日(水) 17時

受付用メールアドレス：i-s-office@media.kyoto-u.ac.jp

件名に「講習会受講申込」と記載願います

情報環境部情報基盤課 情報セキュリティ対策室

電子メール：i-s-office@media.kyoto-u.ac.jp

電話: 内線 7490, 7491, 7492

本部地区電話交換機(PBX)更新について

情報環境部

本学の吉田地区における電話交換機(以下 PBX)設備は、本部地区と病院地区の2地区から構成されています。本部地区 PBX 設備は、北部構内、本部構内、西部構内、吉田南構内、医学部構内及び薬学部構内へサービスを提供している設備です。

既存の本部地区 PBX 設備は昭和 63 年に導入されてから 20 年が経過しており、現在ではメーカー保守物品が確保できない状態となっています。また、近年の IP 電話等の多様なサービスに対応できない設備もあります。そのため、平成 20 年 2 月 9 日(土)に本部地区 PBX 設備を最新型の IP 対応デジタル交換機設備に更新します。

今回の本部地区 PBX 設備更新は、今後の段階的更新計画の第 1 ステップと考えていて、計画は次の通りとなっています。これらの計画を進めていくことによって業務効率化、経費削減等の手助けになると考えております。

<本部地区 PBX 設備段階的更新計画(3 ステップ)>

(第 1 ステップ)

- ・本部地区 PBX 設備の更新
- ・周辺サーバ(通話料金管理サーバ、ユニファイドメッセージサーバ等)の更新
- ・デジタル電話機の更新

(第 2 ステップ)

- ・本部地区 PBX 設備へ学内 PHS 機能の追加
 - － PHS アンテナ、子機の追加

(第 3 ステップ)

- ・本部地区 PBX 設備へ IP 電話機能の追加
 - － SIP-Phone、無線 LAN の新設

なお、今後の予定は以下の通りとなっています。本部地区新旧 PBX 切替え時、ご不便等をお掛け致しますが、ご協力よろしくお願い致します。

<今後の予定>

○平成 20 年 2 月 9 日(土) 午前 8 時～正午(4 時間)

本部地区新旧 PBX の切替え

- － 吉田地区全内線電話の通信停止(病院地区除く)
- － 各地区間の内線発着信の停止
- － 吉田地区内、新デジタル電話機への取替え(病院地区除く)

KUINS 会議日誌

平成 19 年 10 月 20 日～平成 19 年 12 月 12 日

情報環境機構 KUINS 運用委員会

平成 19 年 11 月 19 日 (平成 19 年度 第 7 回)

- 平成 19 年度第 6 回 KUINS 運用委員会議事録の確認
- KUINS ニュースについて
- 改修工事関係
- 改修工事に伴う移転先のネットワークへの要望 (人文研から)
- 学内の無線 LAN 設置について
- KUINS 運用委員検索用 KUINS アカウントの運用委員会外への発行について
- KUINS 利用負担金免除申請 (報告)
- KUINS 利用負担金の請求処理について
- 負担金検討委員会の開催について
- 平成 20 年度保守点検業務, 運転管理業務の調達について
- KUINS 状況報告

- スпамメール対策について
- その他

平成 19 年 12 月 10 日 (平成 19 年度 第 8 回)

- 平成 19 年度第 7 回 KUINS 運用委員会議事録の確認
- KUINS ニュースについて
- KUINS 利用負担金の請求処理について
- KUINS 運営事業費について
- 負担金検討委員会の開催について
- 平成 20 年度保守点検・運転管理業務の調達について
- KUINS 運用委員検索用アカウントの運用委員会外への発行について
- 教育用コンピュータシステムの認証サーバ利用に関する御願い
- 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)