ISSN 0917-3668
2005. 3. 18

KUINSニュース No. 48

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/

公衆無線インターネットアクセスポイント用機器

目　　次

KUINS-III データベース運用開始のお知らせ

移行が遅れておりました KUINS-III データベースは，平成 17 年 1 月 31 日より運用を開始致しました．これに伴い，k3-vlan@kuins.kyoto-u.ac.jp に頂いていた VLAN 設定変更などの申請は，データベース上で行って頂きます．これまでお使い頂いていた KUINS-II のデータベースに統合する形となっており，そのURL(https://db.kuins.kyoto-u.ac.jp/) でアクセスできます．データベースへのログインには，これまで KUINS-II の申請で使っていたアカウントとパスワードをご利用下さい．

アカウントに対する詳しい説明は，
http://www.kuins.kyoto-u.ac.jp/announce/local/id-pub.html
をご覧下さい。

データベース利用法の簡単な説明は，KUINS ニュース No.47 に記載しておりますが，詳しい利用法は https://db.kuins.kyoto-u.ac.jp/help/help.html でご覧になれます．

「KUINS 接続機器管理システム」へのメールアドレス・電話番号の登録のお願い

KUINS-II 接続機器の登録及び KUINS-III VLAN 設定申請にて使用していただいている KUINS のアカウントに関しまして，連絡用電話番号やメールアドレス等の記入がないものが多く見られます．**これら連絡用電話番号等は，KUINS からの連絡時に必要となりますので，必ずご記入いただきますようお願いします．**

設定方法は,「KUINS-II 接続機器の登録」あるいは「KUINS-III VLAN 設定申請」をクリックしていただき，KUINS のアカウントとパスワードにてログインし,「教職員設定の変更」をクリックして，メールアドレスや電話番号等の登録をお願いします。

なお，これらの情報は以下の目的に限定して利用させていただきます．

1. KUINS-II 接続機器の登録申請受付
2. KUINS-III VLAN 設定申請受付
3. 申請に対する問い合わせ及び申請結果報告
4. セキュリティ情報の連絡

新しく京都大学に赴任された教職員の方には，KUINS のアカウントを発行しますので以下の項目を記入の上，q-a@kuins.kyoto-u.ac.jp までご連絡下さい．

- 氏名
- 所属部署名
- 電話番号
- メールアドレス

また、自分の KUINS アカウントを忘れられた方も，同じメールアドレスにご連絡くだされば再発行します．

本件に関するお問合わせは，下記にお願いします．

学術情報メディアセンター ネットワーク掛
電話：075-753-7432 または 内線 7432
メール：q-a@kuins.kyoto-u.ac.jp

PPTP 接続サービスの提供について

学術情報メディアセンターでは，学外や学内 KUINS-III オープンスペース設定からの VPN (Virtual Private Network) による安全な接続のためのサービスとして，ポートフォーワード専用 SSH 接続サービスを提供してきましたが，このたび新たに PPTP (Microsoft Point to Pont Tunneling Protocol) による接続サービスを試験的に提供します.

これにより，学外などから KUINS 上に限定して提供されているネットワークサービスに安全にアクセスすることが可能となります．**接続には，学術情報メディアセンター教育用システムのアカウントを利用します．**

Windows XP, Me, 2000 や Mac OS X などでは，PPTP 接続に必要なソフトウェアは OS に標準で組み込まれているため, ドライバのインストールなどは不要です．接続完了後は KUINS-III の標準的なクローズスペース設定の VLAN に接続しているのと同等になります．Web proxy の設定などは KUINS-III への接続に準じてください.

サービス開始は 4 月初旬を予定しています．当面は試験的な運用とし，利用状況を見て同時接続数や接続時間に制限を設ける可能性があります．本件に関するアナウンスは `http://www.kuins.kyoto-u.ac.jp/` に随時掲載いたします.

公衆無線インターネットアクセスポイントの設置について

学術情報メディアセンター研究開発部では，これまで「みあこネット」実証実験に協同し，学内十数箇所に公衆無線インターネットアクセスポイントを設置してきましたが，同実験の終了に伴いそのいくつかを KUINS のサービスとして引き継ぎます.

利用に際しては，PPTP または SSH で接続できるサーバが必要です．本学構成員の方については学術情報メディアセンターの SSH ポートフォーワードサービスまたは，PPTP 接続サービスが利用できます.

アクセスポイントの設置場所は以下の通りです．今後順次増設を予定しています.

- 学術情報メディアセンター北館 (1 階)
- 学術情報メディアセンター南館 (2 階)
- 時計台記念館
- 正門前
- 吉田南 1 号館
- 総合博物館
- ルネ (1 階，2 階)
- 国際交流会館修学院本館，宇治分館，おうばく分館
- 女子寮，室町寮

NAT 装置の運用について

学術情報メディアセンターでは，KUINS-III のクローズ設定の VLAN に接続されているコンピュータを対象として，NAT 装置による学外への中継サービスを準備しております.

機器の制約上，中継可能な通信はメール受信用の pop3(TCP 110 番)，pop3s(TCP 995 番)，imap4(TCP 143 番)，imaps (TCP 993 番)，および whois(TCP43 番) に限定させて頂きます．

なお，障害調査等に備え中継記録をログとして記録させて頂きますことをご了解願います．また，本サービスで学外からメールを受信される場合は，学術情報メディアセンターのウィルス検知サーバーを利用できませんので，それぞれのコンピュータでウィルス検知ソフトウェアをご使用頂くなどの対策を講じられるようお願い致します.

IP ネットワーク連絡会議および第 13 回 NCA5 総会開催報告

平成 17 年 2 月 10 日に，京都大学学術情報メディアセンター (南館) で，IP ネットワーク連絡会議および第 13 回 NCA5 総会が開催され，NCA5 加入・接続機関 (39 機関 63 名) から多数のご参加をいただきました．

本会では，はじめに NCA5 事務局からの現況報告，新規加入機関についての報告がありました．次に話題提供として，本センターの美濃教授より，コンテンツ作成支援として e-Learning: 情報技術と教育についての説明があり，情報技術を利用した教育を今後どう行っていくかについての講演があり，さらに高倉助教授より，大学における個人情報保護についての説明があり，4 月から始まる個人情報保護法に対する京都大学としての現状について報告がありました．また，KUINS におけるフレッツグループを利用した遠隔地との接続についての説明，及びフレッツグループ導入の経緯および現状についての報告を行いました．

最後に参加機関の方々より，最近のネットワーク状況についての報告があり，参加者間で活発な議論が行われました．

部局管理サーバにおける各種設定確認のお願い

KUINS ニュース No.47 でお知らせしましたようにウィルスチェック機能つきメールサーバの増強に伴う設定作業が 3 月上旬より順次行われていますが，それに伴う設定変更により，ユーザからいくつかの不具合が報告されております．このような不具合が今後は生じないようにするために，各部局で運用しているサーバにおきまして，以下の点について確認していただき，各種設定変更をよろしくお願いします．

1. 今後，KUINS 側で更なるメールサーバの増設や障害時の代替機運用などを実施することがあり，その際にサーバの IP アドレスの変更を伴う場合があります．それにより，部局管理機器で IP アドレスによるフィルタリング設定を行っていることで不具合が生じる可能性があります．そのため，IP アドレスによるフィルタリングの設定については KUINS では推奨できませんので，見直しをご検討いただけるようお願いします．IP アドレスによるフィルタリングがどうしても必要な場合は，KUINS のサーバセグメント全体に対して接続を許可する設定にしてください．具体的な設定の詳細については，`q-a@kuins.kyoto-u.ac.jp` にご相談ください．

2. DNS サーバを部局で独自に運用している場合，KUINS-III 関係のドメイン **(kuins.net)** を参照できるように設定されていないと，KUINS-III においてプライベート IP アドレスを使用しているサーバのアドレス解決ができないため，メールの送受信等に支障がでます．この不具合は学外の DNS サーバを直接参照する設定をしている場合も生じます．そういった不具合を回避するために，

   - **KUINS 内におけるネームサーバの設定に関するお願い**
     `http://www.kuins.kyoto-u.ac.jp/announce/local/dns.html`

   にある設定を DNS サーバに追加していただくよう，お願いします．

   また，上位の DNS サーバとして，**130.54.8.13** を設定しているサーバが見られますが，

   - **KUINS 接続における DNS サーバの設定について**
     `http://www.kuins.kyoto-u.ac.jp/info/local/resolver-settings.html`

   にありますように，KUINS で推奨している DNS サーバに設定変更していただき，130.54.8.13 は設定から外すようにお願いします **(近日中に 130.54.8.13 は停止する方向で検討しています)**．

ウィルス，ワーム，名前ぐらいは聞いたことあるけど ••

石橋由子
(学術情報メディアセンター教育研究支援掛)

1 はじめに

「ウィルスやワームなんて何のことだかさっぱりわからない」
「仕事でパソコンを使っている（使わされている）けどウィルスって私に関係あるか
どうかもよくわからない」

そのような方に少しでも読んでいただきたく思い，今回の記事を書きました．ウィルスやワームに関してご存知の方は，読み飛ばしていただいてもかまいません．**なお，今回の記事は Windows のユーザを対象にしています．**

2 ウィルスって？ ワームって？

ウィルスはパソコンに勝手に侵入し，他人に大量のメールを送りつけたりシステムを破壊したりします．その特徴から 3 つに分類されます．

ウィルス パソコン上のファイルに寄生して被害をもらたすプログラムです．Word ファイルやテキストファイル，画像ファイルに見せかけた実行ファイルにウィルスがひそんでいる場合もあります．ファイルを開いたり実行すると感染します．以前はウィルスといえばこのタイプのものがほとんどでした．

ワーム ワームは「はいまわる虫」という意味で，ネットワークを通じて自分自身のコピーをあちらこちらに撒き散らして増殖し感染させます．ウイルスと異なり，感染・増殖するためにファイルに寄生しません．ワームのネットワークを使った感染・増殖力は非常に強力です．最近のウイルスの大半がこのワームであるといわれています．

トロイの木馬 便利なプログラムのように見せかけてコンピュータに侵入しシステムを破壊します．

一般的にはこれら 3 つをあわせて**”ウィルス”**と呼ばれています．またこの 3 つの混合タイプのウィルスも作成されています．

2.1 こんなことが起こってるんです

添付ファイルの中にウィルスが潜んでいるメールのほとんどは，送信元メールアドレスが詐称されています．友達から送信されたように見えてもそうとは限らないので，友達にクレームを言っても意味がありません．しかし友達のパソコンがウィルスに感染していてこのような結果を招くこともあり，判断に困ることも多くあります．では，実際によく起こった事例をご紹介します．

(1) エラーメールだと思って読んだだけで...
いつも使っているメールサーバからエラーメールが届きました．**何のメールか確認しようと開けると，それはウィルスでした ••**
メールの Subject（件名）を見てエラーメールとわかるとつい内容を確認してしまいます．人間の弱い部分を逆手にとった手法です．

(2) 友達からのメールだったのでクリックしただけで...
友達からのメールに添付ファイルがついていました．いつもなら怪しいので削除しますが，**友達からだったので開けると，それはウィルスでした ••**
メールに添付されているウィルスは，実行してはじめて感染するものがほとんどです．添付ファイルは

危ないということを多くの人が認識していますので，ウィルスメールの作者にとっては「いかにして添付ファイルを開かせるか」が勝負になります．その手段をいくつかご紹介しておきます．

- エラーメールと同じ Subject（件名）にする
- 添付ファイルをテキストファイルや画像ファイルに見せかけて安心させる
- 添付ファイルの名称を思わずクリックしたくなるような名前にする
- 有名企業や警察からのメールを装う

これらの多くは英語のメールですが，件名が日本語のものもありますのでご注意ください．

(3) Web を見ただけなのに...

Internet Explorer で Web 上のページを見ただけで，勝手にファイルがダウンロードされ実行されました．**実行されたファイルはウィルスでした ••**

Internet Explorer にセキュリティホール[1]が発見されましたが，何もせず放置していた人が，このセキュリティホールを突くウィルスが仕込まれた Web ページを閲覧し，ウィルスに感染したということです．

(4) Outlook Express でメールをプレビューしただけなのに...

Outlook Express でウィルスが添付されたファイルを受信しました．**メールのプレビューを見ただけで感染しました ••**

Outlook Express のプレビューが有効になっている状態で，受信したメールをクリックしてプレビューウィンドウにそのメールの内容が表示されます．このとき，Outlook Expres のセキュリティホールが対策されないまま残った状態にあると，添付ファイルを開く動作をしなくても添付ファイルのウィルスプログラムが実行され感染してしまいます．

2.2 感染したらどうなるの?

最近のウィルスは強力ですので，ひとたび感染してしまうと簡単には復旧できないと考えておいた方がよいと思います．ウィルスに感染すると

- パソコンが起動できなくなる
- パソコンのデータが消える
- ファイルを書き換えられる
- よくわからない画像が画面に表示される
- ファイルをメールで送りつける
- 外部から簡単に侵入できる裏口を作られる
- 他人のパソコンを次々に攻撃してしまう
- ウィルス対策ソフトを削除される

といったことが起こります．自分自身が被害にあうだけでなく，加害者にもなってしまいます．このようなことをぜひとも避けるために，何か挙動がおかしいなと思うことがあったら，直ちに対策をとることが必要です．対策の方法については後で説明します．

2.3 どこから感染したんだろ?

ウィルスの感染ルートはさまざまです．感染例として次のようなことが考えられます．

- 電子メールの添付ファイルをクリックしたら感染した
- HTML 形式のメールを表示させたら感染した
- 友達からもらった CD を読み出したら感染した

[1] システムやソフトウェアのセキュリティ上の欠陥

- Web ページを見ただけで感染した
- パソコンをネットワークに接続しただけで感染した
- ダウンロードしたファイルをクリックしたら感染した

ウィルスはいつでもどこからでも知らないうちにやってきます．すぐに行動を開始するものもあれば，しばらくは身をひそめていてある時間になったら突然動き出すものもあります．

3 ウィルス被害にあわないためには

では，ウィルスにかからないためにはどのようなことに気をつければよいのでしょうか? 一番確実なのはネットワークに接続しないことです．しかし，ネットワークに接続するのは危険なことではありますが，それ以上の必要性や利便性があるからこそ接続するわけです．どうしてこんなにインターネットが普及したのかを考えれば，そのことはすぐにわかります．

ネットワークが危険であることを認識した上で正しい対策をして接続しましょう．それは，あなたを守るためであることはもちろんですが，他人を巻き込まないためにも重要なことなのです．ウィルスに対して安全な接続を確保するのは個々人の責任であるという自覚が必要です．

以降でウィルス被害にあわないために日頃から心がけたいことをあげておきます．

3.1 Windows Update を実行しましょう

Windows のセキュリティ上の弱点であるセキュリティホールは，毎月のように発見されています．その中にはネットワークに接続しただけですぐ感染するような重大なものもあるため，緊急に対処する必要があります．セキュリティホールが発見され，その情報がインターネット上に公開されると，そのセキュリティホールを利用したウィルスが作られます．被害にあわないために Windows Update を使って，パソコンを常に最新の安全な状態にしましょう．

Windows Update で最新の状態にする方法や Windows Update の自動更新の方法について詳しく書かれている Web ページがありますので次の URL をご覧ください．

```
http://www.so-net.ne.jp/security/entry/wup/index.html
```

3.2 ウィルス対策ソフトをインストールしましょう

「ウィルス対策ソフトはどこの会社のものがおすすめですか?」という質問を時々受けます．ウィルスを検出して隔離するという機能については，どこの会社とも大きな差はないと思います．そこで

- 「すぐ手にはいること」
- 「まわりの人と同じものにしておくとアドバイスを受けやすいこと」
- 「更新手続きがしやすいこと」

あたりが購入のポイントになります．

まずはウィルス対策ソフトをインストールしてください．これは基本中の基本です．インストール後，ウィルス対策ソフトがパソコンに常駐するようになります．自分好みの設定に変更することもできますが，設定の意味を理解せずに変更しないようにしてください．

ウィルス対策ソフトは「ウィルス定義ファイル」を参照してウィルスであるかどうか判断しています．毎月のように新しいウィルスが出現していますので，ウィルス定義ファイルも頻繁に更新されています．パソコンのウィルス定義ファイルも常に最新のものにしておく必要があります．多くの場合，ウィルス定義ファイルは自動更新するようになっています．ただし，新種のウィルスに対応するため自動更新だけに頼らず

- 毎朝手動でウィルス定義ファイルを更新する

- 新種のウィルスが出現したら[2]ウィルス定義ファイルを手動で更新する

といった対策を取るとよいと思います.

ウィルス対策ソフトには有効期限があります．ほとんどのウィルスソフトは有効期限が迫ってくるとお知らせを表示してくれます．忘れずに有効期限内に更新手続きを行ってください．期限が切れてしまうとウィルス定義ファイルを更新することができなくなり，新種のウィルスに対応できなくなります．これではウィルスソフトを導入していないのとほぼ同じ状態です．ご注意ください.

3.3 HTML メールはやめましょう

HTML メールは背景の画像を指定したり文字の色や大きさを変化させることができます．一方，メールソフトに表示されている URL とは異なるリンクを仕込むことやメールソフトのセキュリティホール悪用するウィルスが仕込むこともできます．これを回避する方法の 1 つとして，HTML 形式のメールは扱わないことです.

Outlook Express 6 の場合は，受信した HTML 形式のメールをテキスト形式で表示することができます. **[ツール] → [オプション] → [読み取り] タブの画面にある「メッセージはすべてテキスト形式で読み取る」にチェックを入れます．**HTML 形式のメールを送信しないためには，**[ツール] → [オプション] → [送信] タブの画面にあるメール送信の形式を「テキスト形式」にチェックを入れます．**

3.4 心がけること

ウィルス被害にあわないために日頃から心がけたいことを再度リストアップしておきます.

- **定期的に Windows Update を実行しましょう**
- **ウィルス対策ソフトをインストールしましょう**
  - **パターンファイルは定期的にアップデートしましょう**
  - **時々ディスク全体をチェックしましょう（フルスキャン）**
  - **ウィルス対策ソフトの更新忘れは入れてないのとほぼ同じです**
- **HTML 形式のメールは取り扱わないようにしましょう**

3.5 添付ファイルの取り扱い

情報処理推進機構（IPA）のまとめた，添付ファイルの取り扱いに関する心得を引用しておきます (次ページ参照).

`http://www.ipa.go.jp/security/antivirus/attach5.html`

3.6 もし感染してしまったら

どうも動作がおかしい，いつもと様子が違う，と感じることがあったら，ただちにネットワークから切り離します．それには，LAN ケーブルを抜いてしまうのが簡単・確実です.

その上で，ウィルス対策ソフトを実行してみます．感染した時点でウィルス対策ソフトの働きを妨害するようなウィルスもありますから，確実とはいえませんが，うまくいけばウィルスを駆除できるかもしれません.

パターンファイルが更新されていない場合には，たとえ妨害されていなくてもウィルスの検出ができない可能性が高くなります．その場合には，別の正常なパソコンを利用して最新のパターンファイルをダウンロードし，フロッピーや USB メモリなどを介して問題のパソコンへ移します．このとき，そのフロッピーや USB メモリにウィルスが感染しては困りますから，**問題のパソコンへ差し込む前に書込み禁止にしておく**ことを忘れないでください．CD-R のように一度しか書き込みができないメディアを使う手もあります.

[2]新種のウィルスが出現するとウィルスソフト会社の Web ページやメーリングリストでアナウンスされることが多い.

メールの添付ファイルの取り扱い 5 つの心得

(IPA によるウィルス対策情報　2001 年 8 月 17 日付)

1. **知らない相手から届いたメールの添付ファイルは開けない**

   見知らぬ相手先から送信されたメールの添付ファイルについては，安全を確認することが難しく，また，ほとんどのケースが自分に必要ないものであるので，無条件に削除することが望ましい．

2. **添付ファイルの見た目に惑わされない**

   テキストファイル（拡張子.txt）や画像ファイル（拡張子.jpg）等の，ウイルスに感染することのないファイルに見せかけた添付ファイルを送りつけるウイルスが発見されており，注意が必要である．添付ファイルは，見た目に惑わされず，プロパティで拡張子を表示する等によりファイル形式を確認し，ファイルを実行するアプリケーションを把握するとともに，自分に必要なものかどうかを判断した上で使用するべきである．

3. **知り合いから届いた少し怪しげなメールの添付ファイル添付ファイル付きのメールは疑ってかかる**

   メールを送信するタイプのウイルスが激増しており，知り合いから送信された添付ファイル付きのメールは，送信者の知らない間にウイルスが送信している可能性がある．巧妙に添付ファイルを開かせるような心理をついてくるので，このような知り合いからのメールこそウイルスの疑いを持って接する必要がある．メールに付帯の情報（メール本文等）もウイルスが作成している可能性があるため，これらの情報も信用せず，例えば先方に問い合わせるなどにより安全を確認してから使用するべきである．

4. **メールの本文でまかなえるようなものをテキスト形式等のファイルで添付しない**

   受信者にウイルス検査の作業負担を生じさせることになり，また，検査を行ったとしても不安感を完全にぬぐいさることはできないので，添付ファイル付きのメール送信は避ける．必要にせまられ添付ファイル付きでメールを送信する場合には，当該ファイルのウイルス検査を行ってから実施するようにし，併せて，メールに付帯の情報（メール本文等）以外で，添付ファイルを付けた旨とその内容を事前に先方に伝えるような配慮が望ましい．一方，このようにして届けられたものでも，受信者はウイルス検査後使用するという用心深さが必要である．

5. **各メーラー特有の添付ファイルの取り扱いに注意する**

   メーラーの設定，メーラーの特殊性などの添付ファイルの取り扱いに関連する事項をよく把握して使用することが重要である．例えば，一部のメーラーでは，受信時に添付ファイルをあらかじめ指定されたフォルダに自動的に展開しファイル保存する．このようなメーラーを使用している場合は，ウイルス検出等でメール本文ごと添付ファイルを削除したときに，保存されている複製も忘れずに削除されるような設定にする必要がある．

大きな被害をもたらしたウィルスに関しては，そのウィルス専用の駆除ソフトをウィルス対策ソフトのメーカが無料で配っていることがあります．どのウィルスに感染したかある程度見当がつく場合には，そういったソフトをダウンロードして利用するのも良いでしょう．その際には，当然上と同様な注意が必要です．

なお，ウィルスを駆除できたとしても，喜んですぐにネットワークに再接続してはいけません．ネットワークを介して自力で繁殖するワームが蔓延している場合には，無防備のままに接続するとすぐにもう一度感染してしまいます．したがって，その前に「パッチ (プログラムの不具合を修正するプログラム)」をあてておかなければなりません．パッチは通常ソフトメーカのサイトからダウンロードできます．繰り返しますが，ダウン

ロードの際は別の対策済みパソコンを使用してください．

この節の内容は，ちょっと難しいなと思われたことでしょう．そうです，一度感染してしまったら復活させるのは困難です．感染しないように予防策をしっかりと取りましょう．

4 おわりに

今回は，ウィルスに感染したらどうなるか，感染しないためにはどうしたらいいかについてご紹介してきました．

パソコンをネットワークに接続する場合「これさえやっておけば大丈夫」という王道はありません．日頃より Windows Update やウィルスチェックソフトの導入，パターンファイルの更新といった必要かつ地道な作業を行い，正しく作業が行われているか定期的にチェックをしてください．それでもなおウィルスに感染することもあります．その場合はあわてず駆除ソフト等で適切な対応をしてください．

参考になる Web サイト

さらに詳しく知りたいときは次にあげる Web サイトを参照してください．

情報処理推進機構 (IPA)	http://www.ipa.go.jp/security/
シマンテック	http://www.trendmicro.co.jp/vinfo/
トレンドマイクロ	http://www.trendmicro.co.jp/vinfo/
マカフィー	http://www.mcafeesecurity.com/japan/security/
BUGLOBE セキュリティ	http://security.biglobe.ne.jp/
so-net セキュリティ通信	http://www.so-net.ne.jp/security/

KUINS 会議日誌

平成 17 年 1 月 17 日〜平成 17 年 3 月 17 日

KUINS 運用委員会

平成 17 年 1 月 26 日 (第 38 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 管理経費について
- その他

平成 17 年 2 月 23 日 (第 39 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.48 発行について
- 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

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)）