ISSN 0917-3668
2008. 8. 31

KUINS ニュース No. 62

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

フィールド科学教育研究センター芦生研究林 (左) とルータ (右)

目　　次

学術情報メディアセンター汎用コンピュータシステム更新・基盤コンピュータシステムの導入に伴う KUINS サービス関連機器の更新について

KUINS は，平成元年に導入された光基幹ループ LAN を中核に，全学の利用者をつなぐ「京都大学統合情報通信システム」として，平成 2 年 4 月から本格運用が開始されました．次いで平成 8 年に「超高速情報ネットワークシステム」として ATM ネットワークが導入され，従前のシステムを **KUINS-I**，新システムを **KUINS-II** と呼ぶようになりました．また，平成 11 年には KUINS-I と KUINS-II の連携を強化するバックボーン ATM ネットワーク接続装置が導入されました．さらに平成 13 年秋には，セキュリティ対策に主眼を置く「安全なギガビットネットワークシステム」(**KUINS-III**) が導入され，平成 14 年から運用を開始し現在に至っています．

KUINS-III の導入から約 7 年が経過しましたが，その間，学内 LAN 設備への大規模な投資は（桂キャンパスへの KUINS-III の展開や耐震改修関係を別として）行われていません．老朽化著しい ATM ネットワークシステムは平成 19 年度までに順次停止されましたが，学内バックボーン部分を KUINS-III として導入された機器で担い，その下流に接続された ATM 時代の旧式のルータが KUINS-II サービスを提供しているのが現状です．また SPAM 判定とウイルスチェックを行っている電子メール配送サーバ，KUINS-III を支えるプロキシサーバなどのサーバ類も，老朽化著しい上に昨今のトラフィック量増に追従できずご迷惑をおかけしてきました．

このような状況から，学術情報メディアセンターの全国共同利用システムである「汎用コンピュータシステム」が更新時期を迎えるのにあわせ，KUINS サービスで運用しているサーバの多くを同システムでのホスティングに移行することで安定かつ高性能な運用に切り替えます．また同時期に導入される「基盤コンピュータシステム」において，ファイアウォールルータ，センタールータ，基幹スイッチ，構内スイッチ等の KUINS-III バックボーンを支える重要度の高い機器が導入されます．

更新の具体的な内容は以下の通りです．

〔**ネットワーク系**〕各機器の性能向上や IPv6 への対応と同時に，消費電力の削減を図ります．

ファイアウォールルータ： 本学の主接続先である SINET3 の 10Gbps 化に対応します．

センタールータ： キャンパス内バックボーンの 10Gbps 化を行います．

基幹スイッチ： 吉田地区に 2 台，宇治地区および桂地区にそれぞれ 1 台ずつ設置し，現在帯域不足が顕在化している KUINS-II(グローバル IP アドレス系) の広帯域化を行います．

構内スイッチ： 北部構内，本部北構内 (2 カ所)，本部南構内，吉田南構内，医学部構内，病院構内，薬学部構内，宇治キャンパス，および，桂キャンパスにそれぞれ 1 台ずつ設置し，今後の帯域不足が懸念される KUINS-III(プライベート IP アドレス系) の広帯域化を行います．

〔**サーバ系**〕

プロキシサーバ： ピーク時の性能不足が顕在化しているプロキシサーバの性能向上を行います．

電子メール系： アンチウィルス，アンチスパム，および，メール配送サーバを更新することにより，電子メールの配送能力を強化します．

この他に，現在提供中のサービスの機能強化のため，PPTP サーバ，NAT サーバ，DHCP サーバ，DNS サーバ，NTP サーバ，不正アクセス検知装置を更新します．またあわせて KUINS サービスの全学統合認証システムとの連携を強化します．

これらにより，館内スイッチ，末端スイッチを除く KUINS サービス関連機器について，中長期的にわたって持続的に整備を行うことができるようになります．なお，残る館内スイッチ，末端スイッチについても，その多くが導入後約 7 年を経過していることから，平成 21 年度概算要求などにより早期の更新に向けて努力していきます．

更新に伴う切り替えは，本年 11 月頃から来年 3 月末に向けて予定しています．ネットワークの停止などを伴いますが，ご理解とご協力をお願いします．新しいシステムは，切り替え当初は現在の KUINS-II/III の構成および運用方針を踏襲しますが，切り替えが完了した平成 21 年度以降には，新しいサービスを段階的に展開していきたいと考えております．今後，詳細が決まり次第 KUINS ニュース等で広報いたします．

フィールド科学教育研究センター芦生研究林の KUINS 接続について

平成 20 年 7 月 3 日 京都府南丹市美山町芦生にありますフィールド科学教育研究センター芦生研究林にて KUINS が利用できるように VPN ルータの設置作業を行いました．芦生研究林では，今まで NTT の ISDN 回線を使ってインターネットに接続していましたが，この度南丹市のプロジェクト「南丹市ケーブルテレビ・インターネット」に変更され通信速度も大幅に向上したことを契機に，研究林全体の KUINS 化を実施する事になりました．この KUINS 化を実施する事により，学内に限定されているサービス (全学グループウエアや財務処理等）へのアクセスや農学研究科教職員用に設置されているメールサーバに直接アクセスできる環境ができ，研究林内教職員だけではなく，研究林を利用する研究者にとっても大変便利になり，大幅に研究も進むという評価を得ています．

遠隔地にとってのネットワーク環境の充実は，事務処理や研究を進めていく上で重要な基盤なのだということを，あらためて感じさせられました．

理学研究科メールシステムにおけるウィルスと SPAM への対策の紹介

理学研究科 総務・学務室 情報管理担当
技術職員 片桐 統

0. はじめに

理学研究科では，以前より専攻・教室や，研究室単位でメールの管理を行ってきました．しかしながら，近年の情報セキュリティリスクの増加などにより，管理コストが大きくなってきて，立ち上げ続けることが経済的又は技術的に困難な状況となるサーバが増えてきました．それに伴い，理学研究科内から，共通のメールサーバや WEB サーバを立ち上げて，管理困難となったサーバの行っているサービスを，継続的に行える基盤が欲しいという要望が多数上がってくるようになりました． そこで，理学研究科情報管理担当は，平成 18 年度よりメールサービスを，平成 19 年度より WEB のサービスを行っており，理学研究科内のドメインの 60%程度を現行のシステムでサービスするようになりました．また，現在は未移行であっても，将来的には移行したいとおっしゃってくださっているドメインもあります． そのような中で，今回 KUINS 運用委員会より KUINS ニュースへの掲載依頼を頂き，理学研究科におけるメールシステムのウィルスや SPAM 対策の取り組みの一端をご紹介できる機会を得たことを大変ありがたく思います．非常に拙い文書で，分かりにくい箇所も多々あろうかとは思いますが，読んでいただいた方々に何かしら参考になれば幸いです．

本文書の構成ですが，まず第 1 節にて理学研究科のメールシステムの構成を簡単に説明します．次に，第 2 節にて SPAM と思しきメールをどういう基準で弾くかを列挙し，ウィルス対策について述べます．その後第 3 節にて救済措置（WhiteList, GreyList, BlackList）について説明します．そして，第 4 節にて現在理学研究科メールシステムが抱える問題点を述べます．

1. 理学研究科のメールシステムの簡単な紹介

理学研究科のメールシステムを簡単に紹介します．機器構成は，表 1-1 のようになっており，それぞれの機器の機能は表 1-2 のようになっています．

表 1-1: 機器構成

受信サーバ	3 台
送信サーバ	1 台
POP サーバ/SMTP サーバ/WEB メール	1 台
データベースサーバ/LDAP サーバ	1 台

表 1-2: 機能説明

受信サーバ (Exim4)	外部からメールを受け取るサーバです．ウィルスとスパムのチェックをここで行います.
送信サーバ (Exim4)	外部へメールを送信するサーバです．受信サーバ同様，ウィルスとスパムのチェックを行っています.
POP サーバ/SMTP サーバ/Web メール (qmail + vpopmail + courier-imap + Squirrelmail)	バーチャルドメイン化されたメールをスプールして，POP サービスを行っています．POP サービスとしては，POP（学内限定），APOP，POP/SSL が利用できます．SMTP サービスとしては，一般的な SMTP 送信（学内限定），SMTP/Auth が利用できます．SMTP サービスは，管理ドメイン宛メールは内部転送を行い，管理外ドメイン宛メールは，送信サーバへ転送します.
データベースサーバ/LDAP サーバ	Greylist 用の SQL サーバ及び Whitelist 用の LDAP サーバが動いています.

管理しているバーチャルドメイン以外（以下,「外部」と書きます）から届くメールの受信は，3 台ある受信サーバで行い，ウィルスチェック，スパムチェックを行い，それらのチェックをパスしたメールが POP サーバに転送されます．POP サーバはバーチャルドメイン化されており，多数のバーチャルドメインを管理しています．平成 20 年 7 月現在，理学研究科のメールシステムで引き受けているバーチャルドメイン数は 28 ドメインで，総アカウント数は 1732 アカウント，転送（ML を含む）は 840 アドレスとなっています．外部へのメールの送信は，SMTP サーバ（POP サーバの別名）にてユーザから受け取ったメールを，送信サーバに転送します．送信サーバでもウィルスとスパムのチェックを行い，問題なければ外部へ送信します．管理しているバーチャルドメイン間のメールは，POP サーバのローカル転送となります．簡単な全体構成図を図 1 に示します.

2. 思いっきりはじく

2-1. メールを受け取り拒否する条件

受信サーバおよび送信サーバでは，下記のルールに従って受け取り拒否をします.

- DNS にきちんと登録されていないマシンから送られてくるメール
- HELO/EHLO をしゃべらないマシンから送られてくるメール
- SPF(Sender Policy Framework) のおかしいメール， SPF で fail となるメール
- MAIL FROM:(envelope-from) のアドレスへエラーメールが送れないメール
- RCPT TO:(envelope-to) アドレスの @ の前に特殊記号があるメール
- 転送先のマシンで受けとってもらえないメール
- 受けとるように設定されていないドメイン宛てのメール
- ヘッダの構文がおかしいメール
- ヘッダの送信者がおかしいメール
- Date: ヘッダ，もしくは To: ヘッダが無いメール
- 禁止している拡張子の添付ファイル付きのメール

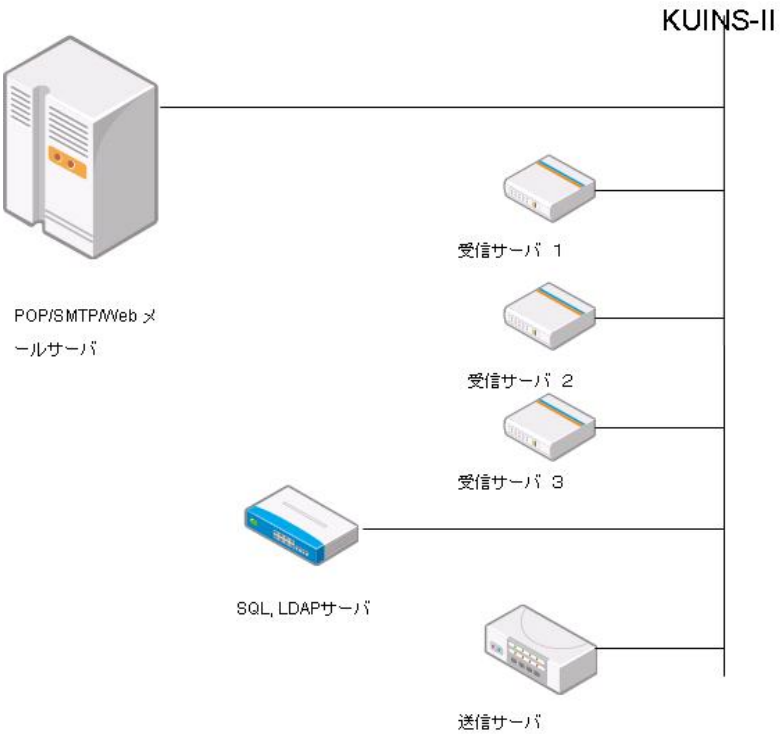


図 1: 理学研究科メールシステム構成図

・アンチウィルスソフト（ClamAV）でウィルスだと判定されたものを含むメール
・スパム対策ソフト（SpamAssassin）で SPAM とマーク（X-Spam-Status: Yes）され，受信者の意思により自動削除と設定されたメール（ルールは，ゆるい目です）

※厳密にいうと，SMTP コネクション段階ではじくものと，受け取ってから廃棄するものがありますが，ユーザが受け取らないという意味で全部「受け取りを拒否する」という表現をしています.

2-2. ウィルス対策について

理学研究科メールシステムのウィルス対策は，受信サーバ及び送信サーバにおいて，フリーのアンチウィルスソフト ClamAV を導入し，届いたメールを clamd に渡してチェックしています.

3. WhiteList, GreyList, BlackList

「2. 思いっきりはじく」で示したとおり理学研究科の受信サーバは，いろいろな条件をつけて，かなりのメールを弾き飛ばします．この弾き飛ばしたメールすべてが，本当に不要で邪魔なスパムメールだったら問題はありません．しかし現実には，正当な組織からの重要なメールにもかかわらず設定が不完全な場合や，レンタルサーバで DNS が不完全なサーバなどが少なからず存在します．これら不完全なサーバからのメールをそのまま弾き飛ばしては，教育・研究に不都合が生じます．したがって，これらを救う手段として，Whitelist, Greylist を用意しています．逆に正しい顔をしてスパムを送りつけてくるようなホストを強制的に排除できるように，BlackList も用意しました.

3-1. WhiteList は LDAP で実現

WhiteList には，正しい送信元にも関わらず，技術的な理由でメールを弾いてしまう場合で，送信元サーバの管理者との交渉が困難な場合や，送信元ポリシー等により送信元の設定変更が叶わない場合に設定しま

す．WhiteList は，LDAP を用いてスタティックに指定しており，手動で LDIF を書いて登録しています (表 3-1)．WhiteList は，送信元の「IP アドレス」ごとに設定します．また，WhiteList により受け取ったメールは，Subject に [wl] という文字列を追加して，チェックを飛ばして受け取っているとわかるようにしています．WhiteList への登録は，ユーザからの依頼による場合の外に，後述の GreyList で同じところが多数あがってきた場合に，手動で設定することもあります．

表 3-1: WhiteList 用 LDIF

```
dn: cn=whitelist_hosts, dc=sci, dc=kyoto-u, dc=ac, dc=jp
changetype: modify
add: ipHostNumber
ipHostNumber: xxx.xxx.xxx.xxx
```

3-2. GreyList は SQL を使って動的に

GreyList の導入に至った元々の動機は,「受信者には，どのようなメールが弾かれているかがわからない.」また「必要なメールが弾かれている場合に対応できていない」という受信者の不満を解消するため，受信者自らメールを受け取るか否かを判断できる機会を用意する必要が生じたということです．

GreyList による判断は，以下のような手順になっています．送信元サーバの DNS が不正なメールなど，SPAM の可能性が高いと判断されたメールは，一旦受信サーバで Temporary Error を返して受け取りを拒否し，データベースに情報を書き込みます．表 3-2-1 にデータベースのテーブル定義を，表 3-2-2 に GreyList の登録 SQL 文を示します．

一般的なメール送信サーバでは，Temporary Error を返されると，メールを数日間再送します．しかし，SPAM 送信サーバでは，再送を行わないまたは短い時間しか再送しないことが多いです．この特徴を利用して，ある程度の時間（設定では 3 時間以上，7 時間未満）の間で再送を行ってくるメール送信サーバは，SPAM ではない可能性があるという判断をし，本来の受信者に対して，GreyList から「受け取りますか？」というメールを受信者に送ります．この間受信サーバは，元の送信サーバに対して Temporary Error を返し続けます．

受信者が受け取りたい場合，GreyList からのメールに直接返信します．これが受信者からの「受信許可返信」とみなされます．この受信許可返信があると，当該メールは「受信許可状態」となり，受信者に対して受信許可された旨を通知します．受信許可を受付ける期間は，初めに送信元のサーバより SMTP 接続を受けてから (データベースにデータが記載されてから)，7 日間です．

メールが受信許可状態になると，送信サーバからの次の再送の際，受信サーバはメールを受け取ります．受信サーバからメールを受け取った際には，受信許可状態を以降 36 日間維持します．受信許可状態になっているメールと同一のサーバかつ同一の送信アドレスから同一受信者宛のメールは，自動的に受信されます．そして，受信許可状態がそこからさらに 36 日間延長されます．ひとたび受信許可状態が満了すると，当該エントリはデータベースから削除されますので，仮に一度受信許可が出たメールであっても，再度初めからの受信許可手続きが必要になります．

表 3-2-1: データベースのテーブル定義

Field	Type	Null	Key
id	bigint(20)	NO	PRI
relay_ip	varchar(80)	NO	
sender	varchar(255)	YES	
recipient	varchar(255)	NO	
block_expires	datetime	NO	
record_expires	datetime	NO	
create_time	datetime	NO	
type	SPAM / UNKNOWN / HAM	NO	

id: 通し番号
relay_ip: 送信元 IP アドレス
sender: 送信元メールアドレス (envelope-from)
recipient: 受信者メールアドレス (envelope-to)
block_expires: 再送を遅延する時間（この間の再送は，再送とみなさない）
record_expires: このエントリの有効期限
create_time: 作成日時
type: 状態 (SPAM or UNKNOWN or HAM)

表 3-2-2: GreyList へのデータの登録

```
INSERT INTO GREYLIST_TABLE ( relay_ip, sender, recipient, block_expires,
record_expires, create_time) VALUES ($sender_host_address, $sender_address,
$local_part$ldomain, now()+DELAY, now()+LIFETIME, now() )
```

※$で始まる変数は，Exim4 が受け取ったメールについての情報を格納する変数．
※ DELAY = 3 時間，LIFETIME = 7 時間に設定しています．

3-3. BlackList

BlackList は，WhiteList と設定方法などは同等で，止めるか通すかの違いです．BlackList に記載されたホストからのメールは，無条件に拒否します．現在のところ，BlackList に記載されているホストはありません．

4. 数限りなくある問題

4-1. 受信サーバの悲鳴

まず，ここ数ヶ月の一日あたりのメール受信数の変化を図 4-1 に示します．

この半年で，メールの受信数が倍増しています．これだけだと，受信サーバが 3 台あれば特に問題ないと感じられるかもしれません．しかしこのグラフは，受け取りを拒否したメールについてはカウントしておらず，実際の SMTP コネクションは，これの数倍程度あります．また，実際には一日の間に波があり，ピーク時には，受信サーバの Load Average が 10.0 を超えることも少なくありません．

受信した際に，ウィルスチェックを行い，GreyList のデータベース検索を行い，LDAP 接続を行うという処

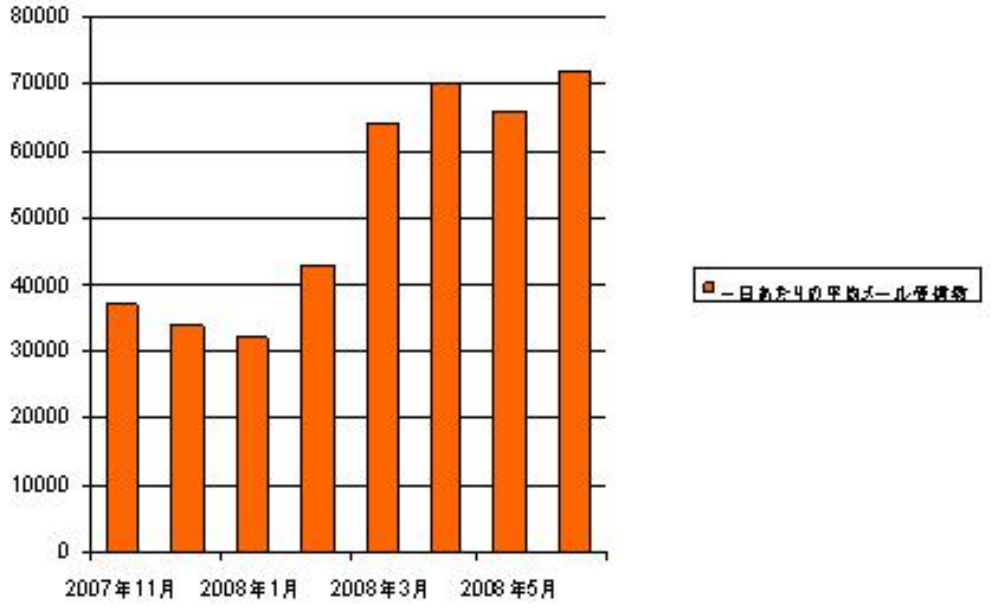


図 4-1: 最近数ヶ月間のメール受信数

理があるために，1 通あたりの負荷が大きくなっていることも，負荷上昇の原因と考えています．

4-2. LDAP, データベースサーバの悲鳴

単位時間当たりのメールが増加すると，チェックのためにデータベースへの接続が増えます．当初，これはそれほどたいした事ないと高を括っていました．しかし，図 4-1 で示したとおりのメールの増加で，消化できなくなってきました．

実は，元々は送信サーバにスペック的な空があったので，受信サーバの片手間に始めたサービスでした．しかし，不幸なことに受信するメールはどんどん増加し，データベースサービスがリソースを圧迫することによって，送信サーバが メールを送信できないという状態になってしまいました．このため，送信サーバを独立させました．

今後，このペースでメール受信が増え続ければ，近いうちにデータベースサーバが破綻することは目に見えていますので，レプリケーション機能を設定し，複数台によるサービスを実施する方針です．

4-3. qmail という選択

qmailadmin というインターフェイスを利用したいという理由で，POP サーバの MTA は qmail を選択していますが，qmail は「存在しないユーザのメールも一度受け取ってからエラーメールを送信する」という問題があります．

これは，SMTP コネクションレベルでエラーとして受け取り拒否してもらえれば，そのまま受信サーバで受け取り拒否が可能なのですが，一度受け取るという動作をするので，受信サーバとしても受け取らなくてはならなくなります．これにより，ウィルスチェックや GreyList といった色々な機能が動作し，余計な負荷が受信サーバにかかります．

現在，qmail から exim4 への乗換えを検討中ですが，管理用インターフェイスが用意できていないため，移行が思うように進んでいません．

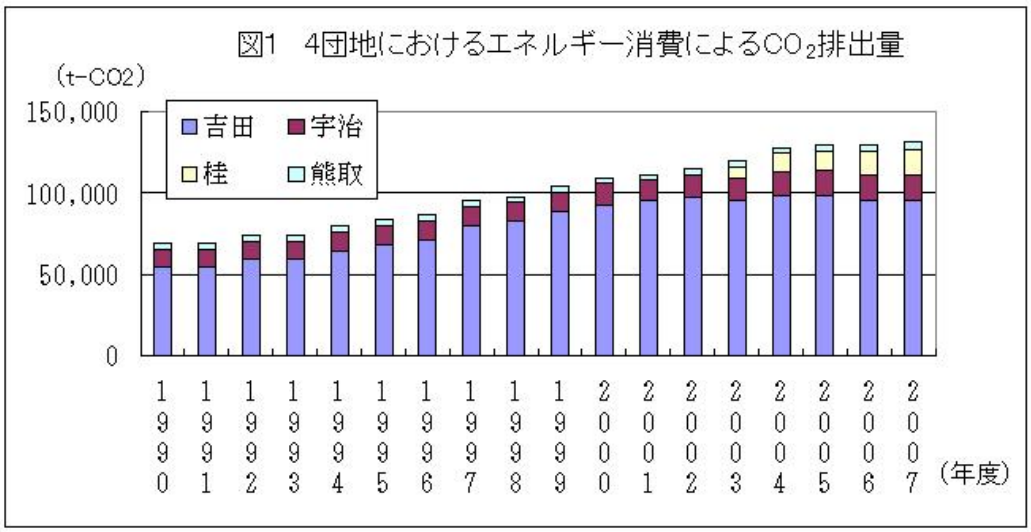
5. おわりに

簡単に，理学研究科のメールシステムからウィルス及びSPAMメールの対策をご紹介させていただきました．最近のSPAMメール受信の急速な伸びに対して，受信するサーバの能力が追いつかないのが現状です．このままの伸び率でSPAMメールが増加すれば，いずれ破綻してしまいます．常に，先手を打った対策が必要とされています．最後になりますが，平素より理学研究科メールシステムの運用・管理にご協力いただいております，KUINS及び理学研究科の構成員の皆さまに感謝申し上げます．また，理学研究科メールシステムの管理・運用にご尽力いただき，本稿の作成にもお手伝いいただきました，寺崎彰洋技術職員に心より感謝いたします．

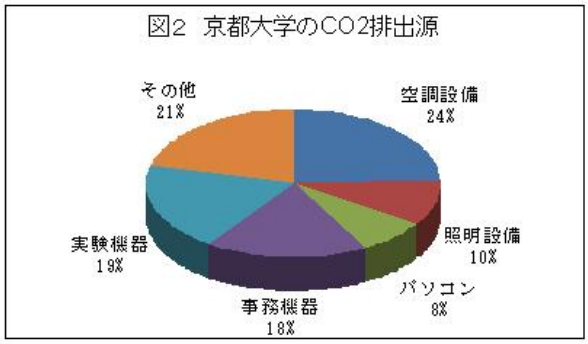
CO_2削減のために，まず私から ～パソコン省エネ設定の奨め～

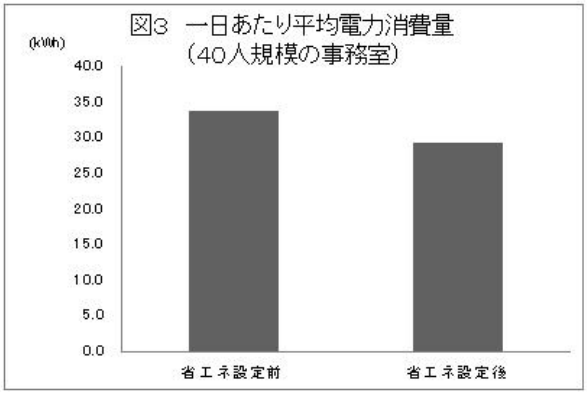
環境安全衛生部

京都大学のCO_2排出量は1990年比でおよそ90%増加しています(図1参照)．その原因を考えたとき，情報関連機器の発展は無視できない要素です．1990年当時はパソコンが現在ほど普及していませんでした．それが今では構成員一人一人が少なくともパソコン一台を使用していると考えられます．現在では，パソコンの電力消費に起因するCO_2排出量は大学全体の約9%を占めると推定されており，空調や照明に続く非常に大きなCO_2発生源となっています(図2参照)．



そこで環境安全衛生部では，空調や照明などとともに，情報関連機器，とくにパソコンを最重要項目としてCO_2排出量削減に向けた取り組みを進めています．まず着目したのは，ほとんどのパソコンに搭載されている省エネ機能です．調べたところ，この機能を充分に活用している人はあまりいないことが判ってきました．そこで，ある事務室の協力を得てこの機能の設定を行ったところ，10%を超える電力消費，CO_2排出量が削減できたのです(図3参照)．この機能は設定を行うだけですので，費用もかかりませんし，簡単に今すぐ出来て効果も期待できます．以下の設定方法を参考に，まず自分から始めてみませんか．

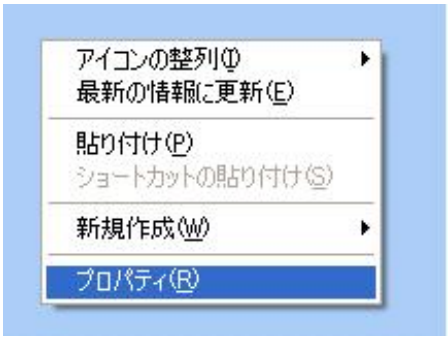




■パソコン省エネ設定の方法

設定の方法は OS の種類によって若干違います．下記の設定方法は Windows XP におけるものです．

1. デスクトップ上で右クリックをし，一番下の「プロパティ(R)」をクリックして下さい．

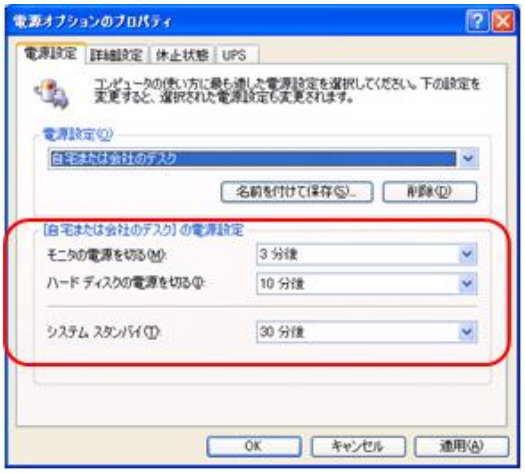


2. 画面のプロパティが出てきます．

「スクリーンセーバー」のタブをクリックして下さい．一番下にある「モニタ電源」の項目にある「電源 (O)」ボタンをクリックして下さい．

3. 電源オプションのプロパティが出てきます.「電源設定」のタブ内にある電源設定を以下のように変更して下さい．

「モニタの電源を切る」→ 3 分後
「ハードディスクの電源を切る」→ 10 分後
「システムスタンバイ」→ 30 分後
各項目の意味については，設定画面で右上の「？」を押した後に項目をクリックすると，説明が現われます.



（注意）
上記に示した設定時間は参考値であり，強制するものではありません．業務に支障がない範囲で各自の判断により設定してください．

変更ができましたら右下の「適用 (A)」ボタンを押し,「OK」ボタンをクリックして下さい．これで設定は完了です.

無線 LAN 基地局に関するお知らせ

KUINS ニュース No.61 でもお知らせしましたように，KUINS では吉田・宇治・桂地区（桂地区は既に導入済）での無線 LAN 基地局の整備を今年度から順次進めております．ここではその進捗状況をお知らせ致します.

2008 年 7 月 28 日現在，総合研究 5 号館の一部，ウィルス研究所及び医学研究科人間健康科学系専攻での無線 LAN 基地局設置が完了しました．設置箇所は，以下の通りです．いずれの基地局もみあこネット方式に対応しており，PPTP や SSH port forwad によるサービスを利用することが出来ます．詳細は以下の URL を御参照下さい．http://www.kuins.kyoto-u.ac.jp/KUINS3/kuins3-guide/

基地局新規設置場所

（総合研究 5 号館）

・1 階〜4 階の学術情報メディアセンター側（西側）

（ウィルス研究所）

・図書室 1 階（設置場所は図書室 1 階ですが，図書室 1 階・2 階，隣接するセミナー室でも利用できます.）

（医学研究科人間健康科学系専攻）

・図書室, 高井ホール, 玄関ホール, 会議室 I, 会議室 II, 会議室 III

7 月 29 日に利用者向け説明会が部局内で開催されましたが，詳細に関しては次号にて報告させていただきます．今後，他部局への展開も計画しておりますので，御興味・御関心がおありの担当者様からの御相談を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．(Subject:に【無線 LAN 基地局設置】と記入していただけますと幸いです．)

コンピュータウィルス対策について

情報環境部 情報基盤課
情報セキュリティ対策室

現在，コンピュータウィルスの感染数が増加傾向にあります．最近のウィルスの特徴として以下の 7 点が挙げられます．

1. 本学のみ，あるいは，限られた部局内でのみ感染が広がる
2. 感染時点では，アンチウィルスソフトウェアは検知できない
3. 更新頻度が非常に高い
4. OS 等の設定を参照する
5. 情報盗聴・転送機能を有する場合が多い
6. 一度に複数のインストールを行う
7. 様々な方法で感染拡大を試みる

1 については，一般に，アンチウィルスベンダ各社は，感染が拡大し，ウィルス本体を入手できるようになるまでは，検知パターンを生成することができません．このため，本学限定のような局所的な感染の場合，検知パターンの提供は数ヶ月後，最悪の場合は永遠に受けられないことになります．

2 および **3** については，感染時にはアンチウィルスが効かないため，ほぼ確実に感染します．ウィルスの更新頻度は数分間隔であり，一般的なアンチウィルスの更新頻度 (5 分〜1 時間) を上回っています．このため，アンチウィルスによる駆除は容易ではありません．

4 については，OS 等の設定参照により，プロキシ等の中継サーバを使用できるため，インターネットに直結していないコンピュータであっても，ウィルスの更新が容易に行えます．

5 に関しては，感染コンピュータ内を検索，さらには，感染コンピュータが接続している LAN 内の通信を盗聴し，Web アクセスやメール送信により，入手した情報を学外に転送します．

6 については，一度の更新活動の際に，数個から十数個のファイルをインストールすることで，実際に活動するウィルスを特定し難くしています．さらには，アンチウィルスのスキャンを察知すると，偽ウィルスをインストールして，これを検知させることにより，活動中のウィルスの存在を隠蔽する工作も行います．

最後に **7** は，感染コンピュータから LAN を経由したり，USB メモリやファイルサーバを介して他のコンピュータへの感染拡大を試みるため，感染は一部の部局，あるいは，共同研究グループに集中する傾向が高くなっています．このため，学外からのコンピュータや USB メモリ等の持ち込みにより，感染が始まった事例が増えてきています．

このため，ウィルス感染が疑われる場合，アンチウィルスの「駆除成功」報告を鵜呑みにしないよう心がけてください．また，重要な情報を扱うコンピュータの場合，使用を継続するか否かについては，部局情報セキュリティ責任者の指示を必ず受けてください．

平成 21 年度以降の国立情報学研究所によるサーバ証明書発行について

KUINS ニュース No.57 等でお知らせし，本学も参加している国立情報学研究所サーバ証明書プロジェクトによる SSL サーバ証明書の発行は，平成 21 年 3 月末終了とされてきましたが，このたび国立情報学研究所より，平成 21 年度以降についても現行のプロジェクトの後継に当たる新プロジェクトを平成 21 年度〜平成 23 年度の 3 年間の時限プロジェクトとして実施することになったとの通知がありましたのでお知らせいたします．また，新プロジェクトが発行する証明書へのスムーズな切り替えを実現するため，現行プロジェクトの実施期間を 3ヶ月延長し，平成 21 年 6 月末までとするとのことです．

新プロジェクトの詳細につきましてはまだ公表されておりませんが，現プロジェクトと同様に情報環境機構 KUINS 運用委員会の責任でこれまで通り発行できるよう，準備を進めたいと考えています．

なお，現行のプロジェクトで発行した証明書につきましては，証明書の有効期限（KUINS ニュース No.61 でお知らせの通り平成 22 年 6 月 30 日）に関わらず，平成 21 年 9 月末日をもって失効させるとのことですので，予めご了承ください．

平成 20 年度第 2 回 KUINS 講習会の開催案内

平成 20 年度第 2 回目の「KUINS 講習会」を下記日程で開催します．この講習会は，KUINS に関する各種の情報を提供するために開催するもので，新規採用教職員を主な対象としていますが，それに限らず多くの皆様に御参加頂きたい講習です．講習内容は，

・京都大学学術情報ネットワーク (KUINS) の構成，運用体制
・京都大学におけるネットワークセキュリティ対策
・KUINS の利用方法の解説

などです．詳細は KUINS ホームページにてご案内します．多くの方の参加をお待ちしております．

日時： 平成 20 年 10 月 6 日 (月）午前 10 時〜
場所： 学術情報メディアセンター北館 3 階講習室

平成 20 年度情報セキュリティ講習会開催報告

情報環境部 情報基盤課
情報セキュリティ対策室

平成 20 年 5 月 15 日 (木)，今年度新たに本学構成委員となった方々を対象とした情報セキュリティ講習会（入門）を開催しました．この講習会では，本学の構成委員として知っておいて頂きたい情報セキュリティの基本的な事項についての講義をメインに，本学で運用している情報セキュリティe-Learning の使い方と注意点，本学でのソフトウェアの管理上の注意点，CO_2 削減のためのパソコンの省エネ設定の利用 (本号別記事に掲載) についての説明があり，46 名の方々に御参加頂き，熱心に聴講頂きました．また，この講習会の模様は，遠隔会議システムを利用して，宇治地区，桂地区，熊取地区に配信しました．

10 月にも同様の講習会開催を予定しております．詳細が確定しましたら，情報環境機構のホームページ (http://www.iimc.kyoto-u.ac.jp/) の「講習会情報」等でお知らせいたします．

KUINS ニュースアンケートのお願い

KUINS ニュースの読者の皆様の声を取り入れ，KUINS ニュースをより良いものにしていくために，アンケートを実施しております．No.61 のアンケートに回答下さいました皆様には，この場をお借りして厚く御礼申し上げます．

綴じ込みのアンケート用紙に記入し，FAX または学内便，郵送でお送り下さい．または，本号 web 版 (http://www.kuins.kyoto-u.ac.jp/news/62/) の同じ記事から，アンケート用紙の電子ファイル（ワード）にリンクを張っています．ファイルに書き込み，

kuins-news@kuins.kyoto-u.ac.jp

までメールでお送り頂くか，印刷後 FAX または学内便，郵送でお送り下さい．(より詳しい返送方法は，アンケートファイルに記述してあります．) 御協力をよろしくお願い致します．

KUINS 会議日誌

平成 20 年 5 月 31 日〜平成 20 年 8 月 30 日

情報環境機構 KUINS 運用委員会

平成 20 年 6 月 16 日 (平成 20 年度 第 3 回)

- 平成 20 年度 KUINS 概算要求について
- KUINS ニュースについて
- 研究プロジェクトからの光ケーブル使用願いについて
- KUINS 無線 LAN アクセスポイントの状況報告
- kyoto-u ドメイン申請
- KUINS 状況報告
- その他

平成 20 年 8 月 4 日 (平成 20 年度 第 4 回)

- 平成 21 年度概算要求及びアクションプランを含めた予算要求について
- インセンティブ経費要求「アクセスネットワーク整備」について
- 平成 20 年度耐震改修工事について
- KUINS ニュースについて
- KUINS ホームページ移行について
- 学術情報メディアセンター汎用コンピュータシステム・基盤コンピュータシステム 調達結果について
- KUINS 無線 LAN アクセスポイント状況報告
- kyoto-u ドメイン申請
- 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)