ISSN 0917-3668
2001. 3. 15

KUINSニュース

No. 34

京都大学学術情報ネットワーク機構
http://www.kuins.kyoto-u.ac.jp/

2000 年京都電子図書館国際会議：研究と実際

目　　次

「２０００年京都電子図書館国際会議：研究と実際」

情報学研究科と附属図書館は，我が国初となる電子図書館国際会議を英国・図書館 BL，米国・国立科学財団 NSF と共催で，11 月 13 日 (月) から同月 16 日 (木) までの 4 日間に渡り，欧米，アジア各国の研究者や図書館関係者約 200 人の参加を得て，附属図書館を会場に開催した．国際会議では，長尾総長，上林情報学研究科教授の基調講演や，各国各機関で取り組んでいる最新の電子図書館システムや著作権問題，国際協力の在り方等に関し，100 件を超える研究発表とパネル討論が行われた．

また，13 日に行われた電子図書館に関する図書館長会議においては，世界の電子図書館の健全な発展を目途とする行動要綱作成の呼びかけがあり，14 日のパネル討論の中で，相互協力と情報交換のためのネットワーク作り，　メタデータに関する国際標準の作成努力，著作権に係る権利制限範囲の拡大のアピール，財政的支援の強化要請，電子図書館が広く使われるため積極的な普及活動を行う，を内容とする「電子図書館京都コミュニケ」(全文は，附属図書館ホームページ URL: `http://www.kulib.kyoto-u.ac.jp` に掲載) が採択された．

なお，本会議は「研究と実際」という趣旨にもみられるように，情報学研究科のコーディネート，附属図書館を構成員として実施されたものであり，研究者と実務者が同じテーマで一堂に会したという点でも意義がある．

計算機不正利用に対する防止対策徹底のお願い

学術情報ネットワーク機構

これまでに，KUINS ニュース等で計算機に対する不正利用防止策の徹底のお願いを繰り返してきましたが，相変わらず本学の計算機を発信源とする不正アクセスへの苦情が多数届いています．中には,「直ちに対処しなければ，当方の国内法に基づき，京都大学もしくは当該計算機の管理責任者を相手取って損害賠償の訴訟を起こす.」との警告文も届いています．

本号にも掲載しております「コンピュータ不正アクセス対応連絡要領」(平成 12 年 10 月 16 日付け経情所第 72 号) にもありますように，不正利用の防止対策を徹底し，万一，不正利用を発見あるいは不正利用の報告を受けたしたときは速やかに対処できる体制を整えていただくようお願いします．

苦情の中では，以前に比べれば数は減りましたが，スパムメールの不正中継が相変わらず目立っています．全国紙の新聞で，ある国立機関の計算機がスパムメール不正中継に悪用されたとの記事が掲載されたり，スパムメールによる推定被害額の報道もなされるようになり，スパムメールは一般的な社会問題として認識されております．

本学でも，現状の放置は許されるわけはなく，早急な対策の必要性に迫られています．

そこで，スパムメール不正中継の防止策として，次の対策をお願いします．

1. 各ノードごとにスパムメール対策を講じた計算機 (SMS) を設置し，学外とのメールの送受信は SMS を介して行うようにしてください．

2. SMS 以外の計算機には学外からメールが直接届かないように，フィルタリングの届けを出してください．
3. SMS が接続されていないノードに関しても，「**SMS は存在しない**」旨を届け出てください．

また，最近では，bind (DNS サーバ)，ttdbserver (CDE)，ftpd，sshd，apache (Web サーバ)，php，IIS (Microsoft Internet Information Server) などの幾つかのバージョンでセキュリティホールが多数発見されており，その悪用方法の情報も用意に入手できる状態となっております．本学においても，これらのセキュリティホールを悪用されて，管理者 (root) 権限を乗っ取られた事例が発生しております．

例えば，Common Desktop Environment (CDE) で利用されている ttdbserver のセキュリティホールは SunOS 4.1.3U1 から Solaris 7 (x86 を含む) までの全てバージョンの Solaris，SGI の IRIX (該当するバージョンは不明)，HP の HPUX 10.x と 11.0 などさまざまな OS に存在します．

さらに，Linux 等の一部の PC Unix では，bind 等の全てのサービスデーモンをインストール直後からディフォルトで稼働させるような仕様となっているため，当該計算機の管理者ですら何がバックグラウンドで稼働しているのか把握できていない状況となっています．このため，インストール後，数ヵ月が経過してサービスデーモンにセキュリティホールが発見されても，そのまま放置されてしまっています．実際に，本学における最近の不正利用としては，このようなセキュリティホールの放置を原因とするものが大多数を占めております．

このような事態を防止するため，

(1) 常に最新の情報を入手し，安全なバージョンの維持に努める．

(2) 使用していないサービスデーモンは起動しないようにする．

(1) に関しては，最新バージョンが必ずしも安全であるとは言えないため，最新バージョンの公開後，直ちにバージョンを上げずに，しばらく様子を見る必要もあります．セキュリティ情報全てを網羅しているわけではありませんが，情報処理振興事業協会 (`http://www.ipa.go.jp/secuirty/`) などを参照されることをお勧めします．

(2) に関して，スパムメール不正中継で頻繁に発生している事例ですが，計算機の起動後，手動でサービスデーモンを止めることで「対処済み」回答されている場合が多いようです．このような対処では，停電からの復旧後に手動停止を忘れていて，再びスパムメールをばらまくというイタチごっこが続いています．不要なサービスは，`/etc/rc` 等を編集し，起動させない設定にしてください．

さらに，本号別記事にありますように，postmaster 宛のメールは当該計算機の管理者に確実に届くように設定してください．

また，これらの不正利用は，やはり本号別記事で説明されているように，当該計算機あるいは当該計算機の所属するサブネット全体の通信強制遮断の対象となりますので，ご注意ください．

コンピュータ不正アクセス等への対応について

経理部情報処理課

標記のことにつきましては，平成１２年１０月１６日付け経情処第７２号で通知しました，下記「コンピュータ不正アクセス対応連絡要領」に沿って対応方お願いいたします.

記

コンピュータ不正アクセス対応連絡要領

（趣旨）

第１　本学に設置されたコンピュータへの不正侵入（データ破壊，ホームページ改ざん，メール不正中継（スパムメール）等）やコンピュータウィルス等により，被害が発生（以下「不正アクセス」という。）した場合において，連絡体制を整備することにより被害拡大の防止を計る等必要な措置を講ずるために「不正アクセス対応連絡要領」（以下「要領」という。）を定めるものである。

（被害発生時の連絡）

第２　不正アクセス（不正アクセスか否か判断できない場合も含む。）があった場合は，発見者，又はサーバー機管理者等被害状況を把握できる者が大型計算機センター（ネットワーク掛）及び当該部局連絡責任者に連絡するとともに迅速に適切な措置を講ずるものとする。

（大型計算機センターの対応）

第３　大型計算機センターにおいて，次の措置を行うものとする。

（１）被害状況の把握

（２）復旧等の技術的支援

（３）経理部情報処理課へ状況報告

（各部局の対応・連絡責任者）

第４　各部局は，不正アクセスがあった場合の連絡・周知が速やかに行える体制を講ずるものとし，併せて連絡責任者を置くものとする。

２　連絡責任者は，次の措置を行うものとする。

（１）発見者からの被害状況の把握

（２）経理部情報処理課へ被害・復旧状況等の報告

（３）経理部情報処理課から情報の提供を受けたときの関係部署への通知

３　連絡責任者は，特別の理由がないかぎり中央事務室の職員を選任して，官職，氏名，電話番号，メールアドレスを書面で経理部情報処理課へ通知する。

また，交替があった場合も同様とする。

４　被害・復旧状況等は，次の事項を書面にして情報処理課まで提出するものとする。

（１）発見者と発見日時

（２）不正アクセスされた期間

（３）被害状況（リスト等があれば添付すること。）

（４）被害を受けたサーバー機等の設置状況（設置場所，管理者，使用 OS，セキュリティ対策）

（５）被害を受けたサーバー機等の主たる使用目的，影響を受ける者の範囲

（６）復旧に要する費用及び時間

（７）その他必要事項

（経理部情報処理課の対応）

第５　経理部情報処理課は，大型計算機センター及び当該部局からの報告により，次の措置を行うものとする。

（１）文部科学省への報告

（２）学術情報ネットワーク機構への報告

（３）各部局への情報提供

（その他）

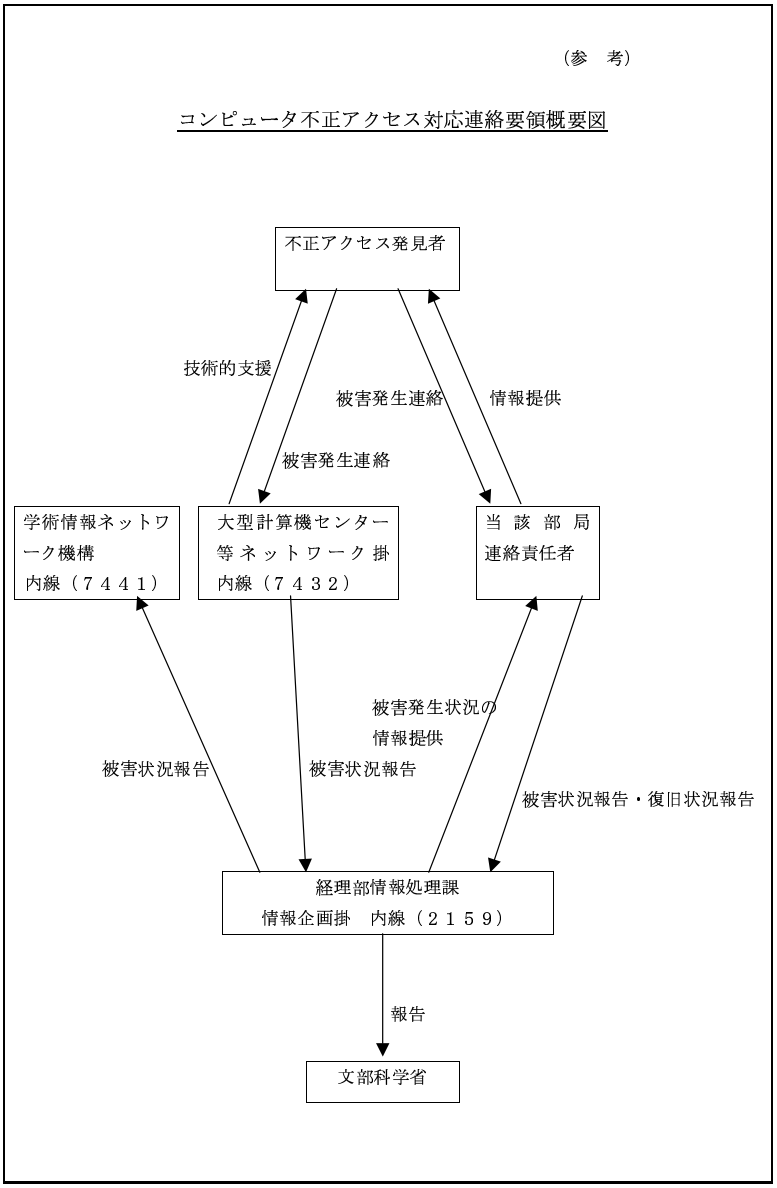
第６　この要領に定めるもののほか，実施に関し必要な事項は，別に定める。

附　則

この要領は，平成１２年１０月１６日から実施する。

（参　考）

コンピュータ不正アクセス対応連絡要領概要図



postmaster 宛メールの到達性確保のお願い

学術情報ネットワーク機構

ネットワーク接続されたホストの設定不良や不正利用などが原因で，学内外に迷惑行為を行ったり，セキュリティ上の脅威を与えてしまうといった事象が報告された場合，当該ホストやドメインの管理者へ迅速に連絡を取ることが重要となります.

(特に学外の) 発見者からの第一報的な連絡には電子メールが用いられる事が多く，宛先には通常 postmaster が用いられます．この宛先を持つメールが実際の管理者に届いていないと，すばやい対策ができなくなる恐れがありますので，メールサーバとして機能する全てのホストにおいて'postmaster@ホスト名' 宛てのメールが必ずそのホストの管理者宛に届くよう設定をお願いします．また，全てのサブドメイン，サブサブドメインにおいて，'postmaster@ドメイン名' のメールがドメインの管理者に届くよう設定してください．管理者の異動などにさいしては，必ず新しい管理者への引き継ぎをお願いします.

postmaster 宛のメール連絡が取れない典型的な例は，root 等，実際に管理する人間に対応しないアカウントに転送されており，徒にホストのディスクにスプールされるだけで，誰もそのメールを読まないというケースです．ご注意ください.

入口ルータでの強制遮断について

学術情報ネットワーク機構

KUINS では 2000 年 4 月よりスパムメール不正中継対策を順次実施しておりますが，前記事にありますようにフィルタリング対策そもそもを未施行，あるいはサーバ設定が不十分で，意図に反して不正中継を行ってしまう例が散見されます.

また，スパム中継に限らず，学内のホストが様々な不正行為の踏み台になっていると疑われるような事象も頻発しており，学術情報ネットワーク機構にも苦情が多く寄せられるようになってきております.

このような苦情を受けた場合，あるいは疑わしい事象が発覚した場合，機構では通常，当該ホストの管理者 (ワークステーション接続届けによる) に連絡を行い調査を依頼しますが，連絡先が分からない場合や管理者への通知に手間取る事が多く，対応に苦慮しております．一方で，仮に不正侵入が実際に行われていればその間も不正行為が続けられ，被害がさらに広がる可能性が増大することになります.

そこで，ホストからの不正行為に関して何らかの報告があり，かつその接続届けが出されていない場合，あるいは管理者不在で連絡がとれない場合には，当該サブネットのノード管理者に連絡の上，入口ルータにおいてそのホストへの学外からの IP 到達性を一切遮断する措置を取ることとします.

また最近では，空きの IP アドレスを複数用いて攻撃を行うパターンの不正行為も広がっているようです．同一サブネットの複数アドレスからの不正行為に関して何らかの報告があ

り，その事象の原因が特定されることなく度重なるようであれば，ノード管理者に連絡の上サブネット全体への到達性を遮断する措置を取る場合もありますのでご承知おきください．

サーバとして機能させることできる OS (Linux, UNIX, Windows NT, 2000 等) を搭載したホストの安全には，(実際にサーバとして利用していない場合でも) 常に注意を払い，最新のセキュリティ情報に基づいた管理を行っていただくようお願いします．また，ワークステーション接続届けを必ず提出するよう重ねてお願いします．

OpenSSH と SSH の相互運用

沢田篤史，赤坂浩一 （大型計算機センター）

1. はじめに

前号では，暗号技術を用いた安全な通信方式として SSH について解説しました．さて，この SSH のバージョン 2 (SSH2) はライセンスに制限があり，副業やアルバイトの場で必ずしも自由に利用できないという問題があります．

一方，SSH プロトコルを実現するソフトウェアとしては，SSH の他にも OpenSSH[1] があり，こちらは目的の制限なく利用することができます．最近では，この OpenSSH のパッケージが FreeBSD や Linux のディストリビューションにデフォルトで組み込まれた形で提供されるようになっており，これらのオペレーティングシステムをインストールするだけで利用可能となっています．

さて，前号で説明した SSH2 と OpenSSH バージョン 2 (OpenSSH2) とでは，利用する鍵のフォーマットが若干異なっており，そのままでは相互運用ができません．本稿では，二種類のソフトウェアが混在した環境での運用を想定し，SSH2 のサーバに OpenSSH2 のクライアントでアクセスする場合，逆に OpenSSH2 のサーバに SSH2 のクライアントでアクセスする場合にそれぞれ必要となるユーザ鍵の設定方法について解説します．

2. SSH2 サーバに OpenSSH2 クライアントでアクセス

SSH2 サーバ (ホスト名 `s_serv`) に OpenSSH2 クライアント (ホスト名 `o_clnt`) でアクセスするには，`o_clnt` で作成したユーザの公開鍵を，`s_serv` の `$HOME/.ssh2` ディレクトリにコピーしなければなりません．ここではその手順を，OpenSSH クライアントホスト (`o_clnt`) 側で作業する場合を想定して説明します．

OpenSSH2 でユーザ鍵の生成を行うには，`ssh-keygen` を用います．すでに，ユーザ鍵が生成されている場合にはこの手順を繰り返す必要はありません．

```
o_clnt% ssh-keygen -d -f $HOME/.ssh/id_dsa
```

[1] `http://www.openssh.com/`

を実行し，問い合わせに応じてパスフレーズを二度入力します．二度とも同じパスフレーズを入力すると公開鍵が$HOME/.ssh/id_dsa.pub に格納されますが，これは OpenSSH2 のフォーマットですので，SSH2 サーバで利用するためには次のようにフォーマット変換を行わなければなりません．

```
o_clnt% ssh-keygen -x -f $HOME/.ssh/id_dsa > o_clnt.pub
```

このコマンドを起動し，パスフレーズを入力すると SSH2 形式の公開鍵が o_clnt.pub に出力されます．変換後の鍵を scp コマンドなどで s_serv 上の所定位置にコピーし，アクセス権を正しく設定します．

```
o_clnt% scp o_clnt.pub s_serv:.ssh2/.
o_clnt% ssh s_serv chmod 600 .ssh2/o_clnt.pub
```

次に，転送した公開鍵の情報を s_serv の$HOME/.ssh2/authorization に追加します．

```
o_clnt% echo "Key o_clnt.pub" | ssh s_serv tee -a .ssh2/authorization
o_clnt% ssh s_serv chmod 600 .ssh2/authorization
```

ここまで説明した準備を行うと，SSH2 サーバ (s_serv) において，OpenSSH2 クライアント (o_clnt) の鍵を用いたユーザ認証が可能になります．

3. OpenSSH2 サーバに SSH2 クライアントでアクセス

OpenSSH2 サーバ (ホスト名 o_serv) に SSH2 クライアント (ホスト名 s_clnt) でアクセスするには基本的に前項の逆を行うことになります．ここでは，s_clnt ではユーザ鍵が生成されているものとして，o_serv 側での作業手順を説明します．

OpenSSH2 サーバのデフォルト設定では，まず SSH のバージョン 1 プロトコルで RSA 認証を行うようになっていますが，必要ならば DSA 認証を先に行うように設定します．それには，o_serv の設定ファイル/etc/ssh/sshd_config の Protocol を 2,1 とします．また，X11 のポートフォワーディングはデフォルトで認められない設定となっていますが，利用する場合には ForwardX11 を yes に設定します．

s_clnt のユーザ鍵を o_serv にコピーします．

```
o_serv% scp s_clnt:.ssh2/id_dsa_1024.pub s_clnt.pub
```

次にこの鍵を OpenSSH2 形式に変換するには，ssh_keygen -X を用います．このコマンドにより，標準出力に OpenSSH2 形式の公開鍵が出力されますので，これを OpenSSH2 の公開鍵束ファイル$HOME/.ssh/authorized_keys2 に追加します．このさいには，パスフレーズを要求されることはありません．

```
o_serv% ssh_keygen -X -f s_clnt.pub >> $HOME/.ssh/authorized_keys2
o_serv% chmod 600 $HOME/.ssh/authorized.keys2
o_serv% rm s_clnt.pub
```

ここまでの設定を行うと OpenSSH2 サーバ (o_serv) において，SSH2 クライアント (s_clnt) の鍵を用いたユーザ認証が可能になります.

OpenSSH2 クライアントの使用法は，前号で解説した SSH2 のものと基本的に同じですが，コマンドラインオプションに若干の違いがある場合もあります．利用にあたってはオンラインマニュアルなどを参考にしてください.

4. おわりに

本稿では，SSH2, OpenSSH2 が混在する環境において，クライアントとサーバでソフトウェアの種類が異なる場合の対処方法について解説しました.

なお，OpenSSH のバージョン 2.2.0 と SSH のバージョン 2.3.0 との間では鍵フォーマットの相違以前に，そもそも通信不可能であるという問題があります．この問題は新しいバージョンを利用すると解決されます．本稿執筆時点 (2001 年 2 月) での最新バージョンは，OpenSSH が 2.5.1p1，SSH が 2.4.0 です.

第三期整備計画「安全なギガビットネットワーク」概要

学術情報ネットワーク機構

京都大学学術情報ネットワーク機構 (KUINS) では，平成 13 年度予算において第三期整備計画を実現すべく概算要求を提出しておりましたが，平成 12 年度補正予算としてそれが認められ (昨年秋)，現在政府調達の手続きが進められております．導入は平成 13 年の秋頃の予定で，平成 14 年度初からの本格稼働を目指しています.

第三期整備計画のキーワードは「セキュリティ」であり，研究教育活動を支えるライフラインとしてのキャンパスネットワークの安全を確保することを第一の目的としています.

本計画では，新たなバックボーンネットワーク (KUINS-III) を既存の KUINS-II と並立する形で構築し，学外との間にはファイアウォール装置を設置します．なお KUINS-I の運用は KUINS-III の導入を機に停止し，ノード装置を撤去します.

KUINS-III の物理構成を図 1 に示します．KUINS-III は Ethernet をデータリンクにもつ IP 網です．センタールータ (1 台)，基幹スイッチ (9 台)，館内スイッチ (約 100 箇所)，末端スイッチ (約 700 台) からなる四階層のスター型ネットワークで，末端スイッチからは，研究室，講義室などの各部屋にカテゴリ 5e のツイステドペアケーブルを配線し情報コンセントを設置します．末端に提供する通信速度は 100Mbps となります.

一方，KUINS-III の論理構成を図 2 に示します．センタールータはファイアウォールとして機能し，学外と KUINS-III との間の IP 通信接続が一切遮断されます．結果として KUINS-III にはプライベートアドレス空間[1]を用いることができ，IP アドレスの枯渇問題を回避することができます．また，ファイアウォールを越える通信の仲介を行うサーバ群を提供し，電子メー

[1] RFC1918 参照

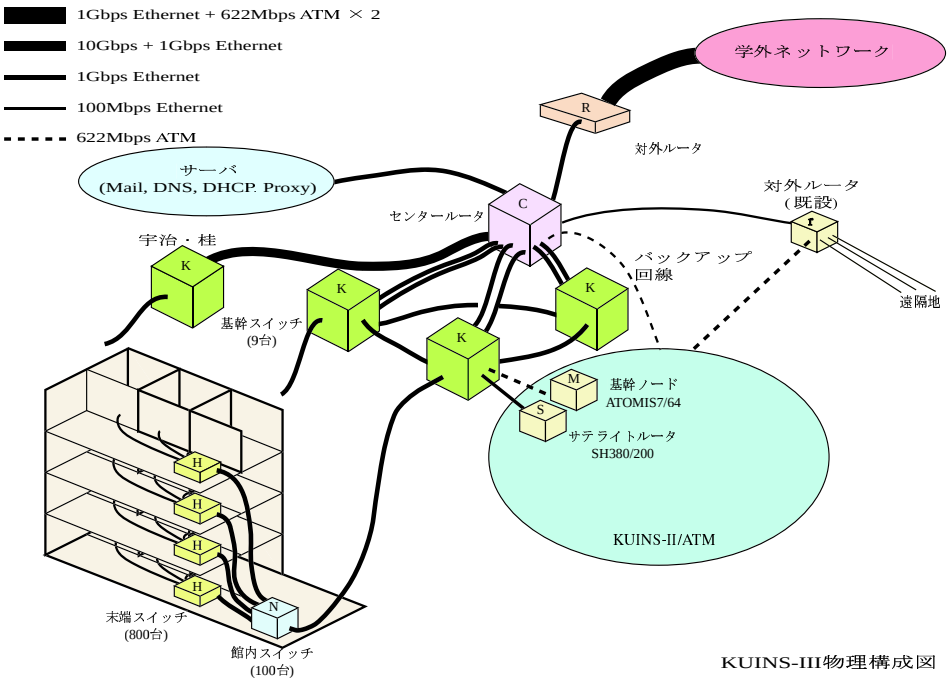


図 1: KUINS-III の物理構成

ルと Web (クライアント), ftp (クライアント) 等の利用を可能とします．電子メールの送受信を仲介するサーバは，いわゆるスパムメールの不正中継を拒否する機能を持ち，KUINS-III を利用するにあたっては，不正中継対策に留意する必要がなくなります．メール中継サーバには通過するメールのウィルスチェックを行う機能があり，希望する部局等には，ウィルスチェックサービスを提供することを検討しております．

また，KUINS-III では，情報コンセントの設置される部屋の種類や使用目的に応じ，論理的なサブネット (VLAN) を設定することができます．この VLAN を例えば研究室のようなグループへ割り当てることになりますが，VLAN をまたいだ通信を基本的に行えない設定とすることにより，仮にあるホストが不正侵入を受けたとしても，その被害が他の VLAN に及ぶことを防ぐことができます．このように，KUINS-III では，メール，Web，ftp など，最低限の情報通信をセキュリティに関する配慮なしに利用することができます．

一方，学外ネットワークとの通信は遮断されており，またアドレス変換を行わないため，KUINS-III 内部から学外へ，例えば telnet, rlogin などの直接通信を行うことはできません．また，KUINS-III 内部から学外への情報サービス (Web, ftp サーバなど) を行うことはできません．外部との直接通信が必要なホストは，KUINS-II を利用していただくことになります．KUINS-III と学外ネットワークとはファイアウォールで遮断されますが，KUINS-II とは基幹スイッチを介して互いの経路情報を流し，KUINS-II と KUINS-III 相互の通信は学外ファイアウォールを経由せずに可能となります．ただし，通信プロトコルは ssh などに限られたもののみ認められます．なお，KUINS-III のプライベートアドレス空間は 10.224/11 より

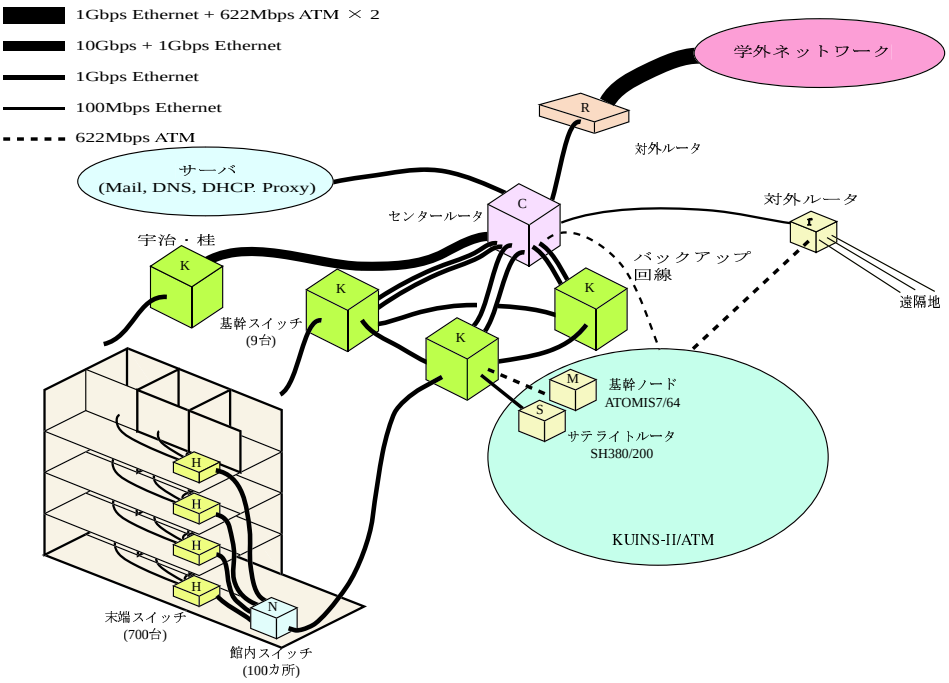


図 2: KUINS-III の論理構成

採番する予定です．現在 KUINS-I, II 配下でこの範囲のプライベートアドレスを利用されている場合には，経路情報の混乱が生じますので，早めに移動していただくようお願いします．

つまり，KUINS-II は，KUINS-III と学外ネットワークの中間に位置し，ユーザが情報サービスのために利用可能な，非武装地帯 (DMZ) ととらえることができます．KUINS-III 導入後も KUINS-II はあくまで「非武装」ですので，個々に安全性を確保していただくことが必須となります．

このように，学外との直接通信や学外への情報発信の必要な利用者は，KUINS-III と KUINS-II とを併用することが必要となります．その具体的な方法については，今後本ニュース等を通じて解説を行う予定です．

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

学術情報ネットワーク機構情報システム管理掛 ((075) 753-7841)
（大型計算機センター等ネットワーク掛 ((075) 753-7432)）

卒業式をネットで生中継

今年度の卒業式・修了式，および来年度の入学式を下記のようにネット中継しますのでぜひご覧下さい.

3 月 23 日 (金) 10:00〜 修士学位授与式
3 月 26 日 (月) 10:00〜 卒業式
4 月 11 日 (水) 入学式
URL = http://www.kuins.kyoto-u.ac.jp/ceremony/222.html

KUINS 会議日誌

平成 12 年 7 月 17 日〜平成 13 年 3 月 14 日

学術情報システム整備委員会

平成 12 年 7 月 17 日（回議）
- 小委員会の再開について

平成 12 年 10 月 26 日（第 26 回）
- データベースの著作権について

平成 12 年 12 月 20 日（第 27 回）
- 「キャンパス情報ネットワーク設備第３期整備計画」- 安全なギガビットネットワークシステム - について

平成 13 年 3 月 12 日（第 28 回）
- 平成 14 年度概算要求について
- 学術情報ネットワーク機構改組構想について

学術情報システム整備委員会技術専門委員会

平成 12 年 9 月 18 日（回議）
- 委員の追加について

平成 13 年 1 月 11 日（第 49 回）
- KUINS-III について
- その他

平成 13 年 2 月 23 日（第 50 回）
- 平成 14 年度概算要求について

KUINS ネットグループ連絡会議

平成 12 年 7 月 26 日（第 89 回）
- 接続端末数について
- 接続状況報告
- KUINS 障害報告
- スパムメール不正中継対策フィルタ設定実施状況について
- KUINS-II ノード機器室の環境整備依頼について

平成 12 年 9 月 27 日（第 90 回）
- 接続端末数について
- 接続状況報告
- KUINS 障害報告
- スパムメール不正中継対策フィルタ設定実施状況について

平成 12 年 10 月 27 日（第 91 回）
- 接続端末数について
- 接続状況報告
- KUINS 障害報告
- スパムメール不正中継対策フィルタ設定実施状況について