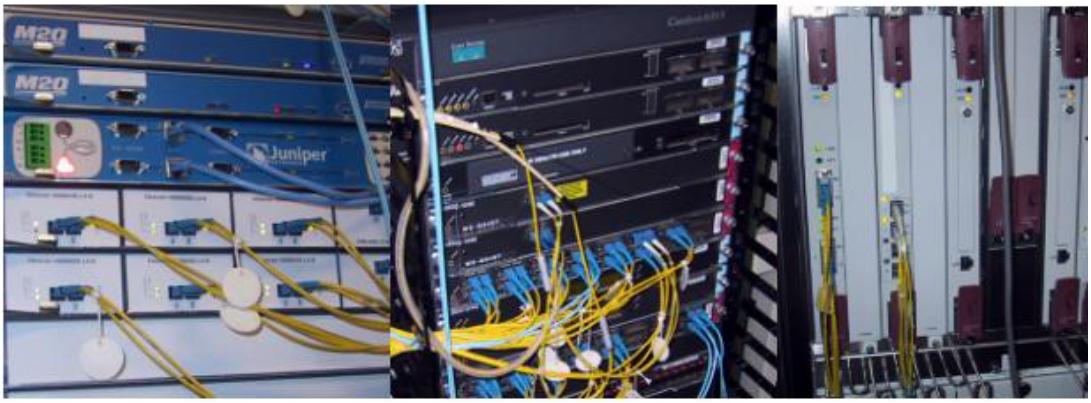
ISSN 0917-3668
2002. 9. 16

KUINSニュース

No. 38

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



KUINS-III 導入ルータ機器類

目　　次

学術情報ネットワーク機構と学術情報メディアセンター

学術情報メディアセンター
センター長　松山隆司

京大広報 No.569(2002 年 6 月) でお知らせしましたように，本年 4 月 1 日より，大型計算機センターと総合情報メディアセンターを廃止，統合して学術情報メディアセンターが設置されました．センターの使命や構成，研究目標などについては，広報に書かせて頂きましたので，ここでは，学術情報ネットワーク機構 (以下，KUINS 機構) とセンターとの関係について，現状および今後の展望を述べさせて頂きます．

KUINS 機構 (機構長：総長) は本学の学術情報ネットワークの整備・管理・運用を行うための学内組織として 1990 年に設置され，以来本学の情報ネットワークの整備，拡充に大きな貢献をしてきました．しかし，この機構には専任の教官，技官，事務官がおらず，学内関連部局の教職員の兼務によってその活動が支えられてきたのが現状で，これからの学術情報ネットワークの大規模化，高機能化，さらには情報セキュリティに関する問題の深刻化に対応するには体制の見直しが強く望まれるようになっていました．

こうした状況を踏まえ，学術情報メディアセンターの設置に際しては，研究開発部に高機能ネットワーク研究分野 (岡部教授) およびセキュリティ研究分野 (北野教授，併任) からなるネットワーク研究部門を置き，ネットワーク研究の専門家集団を組織するとともに，情報サービス部にネットワーク担当を設け，教官・技官の連携によるネットワークサービス業務の強化を図りました．さらに，今後は外部委託による派遣技術者を組織して，日常的なネットワーク管理やセキュリティ・モニタリング，利用者に対するコンサルタントを行う情報拠点の設置も検討しています．

一方，KUINS 機構は，当初の案ではセンター設置に合わせて廃止される予定でしたが，今後の本学の情報基盤を支える全学的体制としては，センターだけでなく他の情報関連部局をも含めたより広汎な組織 (「情報環境機構 (仮称)」) を整備する必要があるとの意見が出され，当分の間現在の KUINS 機構を存続させることになりました．この結果，現在本学の学術情報ネットワークは，全学組織である KUINS 機構と学術情報メディアセンターの両者が管理・運営するという多少分かりにくい状況になっています．ただ，こうした体制はあくまでも経過措置的なもので，近い将来には明確な全学的体制が整備されるものと考えています．

センター設置以来半年が過ぎ，徐々にネットワークの管理・運用体制が整ってきていますが，センターの設置と時期を合わせて KUINS-III の導入・運用が行われることになったため，利用者の方々には色々な面でご迷惑をお掛けすることになってしまいました．本学のネットワークの規模および利用者が要望されている多様な情報サービスの種類からすると現在のセンターの人員は決して十分なものとは言えませんが，安全で快適なネットワーク環境を構築し，運用することは本センターに与えられた重要な使命と思っており，教職員一同精一杯の努力を続けておりますので，何卒ご支援のほど宜しくお願い致します．

KUINS-III 運用に関するおわび

KUINS の新しいキャンパスネットワークシステム「KUINS-III」は，平成 14 年 1 月からテスト運用，平成 14 年 4 月から本運用の予定で，システムの設定作業等を進めてきました．しかし，設定作業が予定よりも大幅に遅れたため 4 月 1 日に全構内で運用を開始することが出来ず，平成 14 年 6 月初めに全構内にて本格的に運用開始となりました．

しかし運用開始以来，通信が止まるなどネットワークの状態が安定せず，トラブルも多数発生し，また設定に関しても「ユーザの意図通りになっていない」などのご指摘を受け，現在も随時修正している状況です．これらにつきましては，ユーザの皆様に大変ご迷惑をかけたことを改めてお詫び申し上げます．

KUINS-III の運用に関しては学術情報メディアセンターとしまして，一日も早い安定稼働を目指しまして努力いたしますので、皆様方のご協力よろしくお願いいたします．

なお，以下に各構内の運用開始日を記載しておきます．

構内名	運用開始日
北部構内、本部北構内、本部南構内、宇治地区	平成 14 年 4 月 1 日
総合人間学部構内	平成 14 年 4 月 9 日
薬学部・病院西構内	平成 14 年 4 月 12 日
医学部構内	平成 14 年 4 月 19 日
病院東構内	平成 14 年 4 月 25 日
熊取地区・犬山地区・大津地区	平成 14 年 5 月 10 日

KUINS の新しい体制について

(1) はじめに

今年４月に学術情報メディアセンターが発足し，旧 大型計算機センター，旧 総合情報メディアセンター，および学術情報ネットワーク機構（KUINS 機構; 学内措置）の業務は新しいセンターに引き継がれました．

KUINS（学術情報ネットワークシステム）関係は，新センターの「情報サービス部ネットワーク担当」の所管となりました．情報サービス部ネットワーク担当は KUINS のいわゆるインフラをサービスする担当者として教官 5 名 (うち 1 名は併任)，技官・事務官 6 名が配置されています．

(2)“ 安全なネットワーク ”KUINS-III

従来本学で運用されてきたキャンパスネットワークは，平成 7 年度導入の ATM ネットワークをバックボーンとし，平成 10 年度導入の ATM ルータに各建物のサブネットがつながるのが基本の構成となっています．これを便宜的に KUINS-II と呼びます．

従来の KUINS-II の問題は，KUINS 機構が管理するのは建物の入り口となるルータまでで，その先の建物内配線は部局任せであったことです．すなわち，ネットワークのトラブルが生じたときでも，KUINS 機構側では障害が建物内で発生しているというところまでしか掴めませんでした．建物内の配線がきちんと工事され，図面が保管されているような場合にはよいのですが，教官や学生が手作業で引いた線に頼っていて当事者の転出により状況をわかっている人がいなくなっているケースも稀ではありません．このことは障害の切り分けやセキュリティ対応を著しく困難にします．また，改組や建物の建て替えにより，一つのサブネットに複数の部局の構成員が雑居しているケースもあり，サブネットを単位としてポリシーを統一しセキュリティレベルを高めて行くことが困難でした．

そこで，全学のセキュリティレベルの向上を主目的とする KUINS-III では，原則として既設の配線には頼らず，新しいネットワーク KUINS-III を新規に配線することにし，各部屋の情報コンセントまで KUINS が管理することにしました．そして，各コンセントを VLAN と呼ばれる論理的なサブネットに割り当てて，VLAN ごとにポリシーを決定できるようにしました．さらに，KUINS-III では DHCP により個々の端末に対する登録手続きなしで使用できるようにしました．その代わり，KUINS-III に接続された端末からは，学外との直接の (すなわち IP レベルの) 接続性はないものとし，学外との通信はすべてアプリケーションゲートウェイを介することにしました．

あわせて従来の KUINS-II は，厳格な登録制に移行し，計算機ごとの管理責任者を明確化することにしました．ルータでのフィルタリングにより未登録端末からの利用を排除し，特に，従来なし崩し的に利用がなされてきた KUINS-II における DHCP の利用を禁止する (正確には，IP アドレスと MAC アドレスの対応関係を事前登録しての運用のみ認める) ことにしました．

(3)KUINS の利用負担金

前述の通り，従来の KUINS-II では建物の入り口までとしていた KUINS とユーザとの責任分界点を KUINS-III では各部屋に設置された情報コンセントまでとしました．すなわち従来は，全学で高々百数十箇所の接続端子を管理しておればよかったものが，KUINS-III では一万六千ポートの情報コンセントについて責任が及ぶことになりました．また，5000 を超える VLAN を情報コンセントに対応づけ，かつ VLAN ごとにきめ細かなポリシ設定ができるようにしたこと，KUINS-II も端末ごとの厳格な登録性とし各ルータでフィルタ設定を管理する必要が生じたことなど，業務量は従前の何倍にもなっています．

さらに，昨今の不正アクセスの急増にともない，セキュリティに関する監視や緊急対応の業務も増加しています．KUINS では，平成 11 年より IDS（侵入検知装置) を運用してきましたが，KUINS-III の導入とあわせてそれを強化した結果，警報数は 10 倍以上にもなって

います．加えてネットワークの障害に際して現場での障害切り分けに加えさまざまなコンサルタント業務を行うことも，検討されてきました．

以上は新センターへの改組に伴う定員増では対応不可能であり，業務の外注を前提としてきたことです．その一方で，これまで KUINS がもつ財源は，ハードウェア保守契約のための費用のみでした．KUINS の運用のための財源をどうするかは，昨年度，新センター設立の準備と並行して学術情報システム整備委員会で検討され，KUINS-II についてはホスト単位，KUINS-III については情報コンセント単位での利用負担金の形でユーザにも負担を求める方針が打ち出されています．さらに，その検討はセンターの学内共同利用運営委員会に引き継がれ，現在は，KUINS-II において提供するサービスの明文化と今年度の KUINS-II の負担金について素案がまとまったところです．

これまで 9 月中を目処に KUINS-III への移行を進めていただいてきました．10 月からは，オンラインデータベースにより KUINS-II に残る端末の接続登録をお願いすることになります．また，10 月以降，遅くとも年内に，準備のできたサブネットから，KUINS-II での未登録ホストの接続遮断の設定を追加していきます．負担金については，正式に決まり次第，文書にて各部局にお知らせいたしますとともに，KUINS のホームページ等で広報致します．検討中の今年度の KUINS-II の負担金案については，部局選出の本センター学内共同利用運営委員の方にお尋ねいただくか，`q-a@kuins.kyoto-u.ac.jp` までメールでお問い合わせください．

(4) おわりに

4 月からこれまでに，KUINS-III 運用開始が遅れ，さらに安定運用までに時間を要してしまいました．その上利用者の方々との連絡に抜けや遅れも目立ち，さらに不信を招いてしまいました．また，KUINS-III という新しいコンセプトのネットワークであるにもかかわらず，KUINS-III への移行の具体的な方法や KUINS-II と KUINS-III の使い分けについての広報活動が十分でなかったことも反省点です．そのような状況で負担金とはなにごとか，とのお怒りがまったくごもっともであること承知しておりますが，以上のような状況をご賢察の上，負担金導入についてのご理解とご協力をお願いします．至らぬ点については遠慮なくご叱責下さい．

KUINS 接続機器データベース登録認証用アカウント情報の配布について

KUINS では，ネットワークの円滑な運用とセキュリティ強化のため，KUINS-II に接続される計算機に関する情報を必ず登録して頂くようにかねてよりお願いしておりますが，平行して皆様からの情報の登録を確実かつ迅速に行うために新たなデータベースシステムの準備を進めております．

これまで，このデータベースに皆様からの情報を安全に登録する方法について検討を行っ

ておりましたが，個人毎に設けたアカウントを利用して登録して頂く結論に達しました．つきましては，各自でご利用になる計算機をデータベースに登録して頂くためのアカウント情報 (アカウント名およびパスワード) をお送り致しますのでご確認頂きますようお願い致します (ご利用になる計算機のデータベースへの登録方法等については改めてご案内致します)．

一方，KUINS-III に関しても，現在の各部局の VLAN 設定情報 (情報コンセントの情報，通信可能な KUINS-II セグメント及び KUINS-III VLAN) についてもオンラインで閲覧可能となりました (URL は，`http://webdb.kuins.kyoto-u.ac.jp/KUINS-III/` です)

本件に関するお問合わせは以下にお願いします．

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

KUINS-III 運用開始に伴う部局運用のサーバ設定変更のお願い

KUINS-III 運用開始以来，KUINS-III に接続されている端末から各部局で運用している KUINS-II に接続されている各種サーバへのアクセスの際に様々な不具合が指摘され，利用者の皆様にご迷惑をおかけしております．

これに伴い，KUINS-III から円滑なアクセスが可能になるように，KUINS 管理の機器類につきましては設定変更を行っておりますが，それと同時に，各部局で運用されている各種サーバにて，下記の設定変更を行っていただく必要があります．

(1)DNS サーバの設定変更について

KUINS では，KUINS ニュース No.35 でお知らせしましたように，RFC1918 で定められたプライベートアドレスの一部を学内で重複なく利用できるように管理させて頂いており，KUINS-III に接続される計算機に割り当てを始めています (KUINS-III に接続される計算機には，管理上，原則として **kuins.net** ドメインにて対応付けを行っています)．

プライベートアドレスを利用する KUINS-III では，従前の KUINS-II(KUINS-I は KUINS-II に収容済み) との間で，割り当てられたプライベートアドレスを用いて相互に通信できるようになっていますが (KUINS-III の VLAN 申請時に通信不可を要求した場合を除く)，通信開始時やアクセス制限時等には KUINS-II 側の計算機において，**kuins.net** ドメイン配下のホスト名を指定したり，KUINS-III 側からのアクセスを，IP アドレスからホスト名への 逆引きによって確認したりできるようにしておくことも必要であると考えます．

しかし，プライベートアドレスを利用する **kuins.net** ドメインの情報は，学内に閉じた情報であるため，これらの情報を参照するためには，KUINS-II 側の計算機が参照するネームサーバに，KUINS-III 側の情報を持つネームサーバを登録しておく必要があります． 逆に，

KUINS-II 側のネームサーバに，KUINS-III 側の情報を持つネームサーバを 登録せずにおくと，解決不能な問い合わせがインターネットに流出してしまい，インターネットに無駄なトラフィックを発生させることになります.

そこで、各部局で独自に運用して頂いている DNS(ネーム) サーバの管理者の方々には,

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

に掲載されている設定変更を実施していただくことをお願いします.

(2)WWW サーバの設定変更について

KUINS-III では、 Web 閲覧用として Web プロキシサーバを運用していますが、平成 14 年 7 月現在，プロキシを自動設定で利用する際には，学内及び学外のページとも，プロキシ経由でアクセスするような設定になっておりました．そのため部局限定の Web ページにアクセスできない問題が生じ，利用者の皆様に御迷惑をおかけしている現状でした.

そこで学内のホームページ (*****.kyoto-u.ac.jp**) については，プロキシを経由せずに直接アクセスするよう、自動設定ファイル (proxy.pac) の設定を 8 月 1 日より変更しました.

それに伴い，各部局で運用している WWW サーバの管理者の方々には,

- 学内限定の Web ページについて，KUINS-III の IP アドレス (10.224/11) に対してアクセス許可の設定を追加して下さい.
- 該当部局の KUINS-III VLAN からアクセス可能にする場合については該当部局で使用している KUINS-III のアドレス範囲を追加して下さい。また，KUINS のホームページの「KUINS-III に接続された計算機に付与される IP アドレスの DNS 逆引について」にあるドメイン名でもアクセス制限は可能になります.

設定方法の詳細につきましては，以下の URL を参照下さい.

`http://www.kuins.kyoto-u.ac.jp/announce/local/proxy-modify.html`
(KUINS-III Web プロキシサーバの設定切替えに伴う設定変更のお願い)

`http://www.kuins.kyoto-u.ac.jp/announce/local/rev-dns.html`
(KUINS-III に接続された計算機に付与される IP アドレスの DNS 逆引について)

Super SINET に接続切替

この度，KUINS ではスーパー SINET(`http://www.sinet.ad.jp/s_sinet/index.html`) との接続を完了し，6 月 12 日より利用を開始しました．スーパー SINET は，10Gbps の大容量バックボーンを中心に国内の大学等の研究拠点を最低でも 1Gbps の速度で結ぶネットワークで，文部科学省国立情報学研究所が平成 14 年 1 月より運用を開始しました.

これまで，KUINS と SINET との間は 100Mbps の FDDI で接続されていましたが，スーパー SINET との接続により，回線容量が 1Gbps にまで増強されています.

KUINS-III における NAT の利用

KUINS-III では，学外との接続性を持たないプライベート IP アドレスを用い，学外との通信は，例えば Web の場合には HTTP プロキシサーバを介して行うようになっています．一方，家庭でも普及しつつある ADSL や CATV インターネットなどの広帯域インターネット接続では，いわゆるブロードバンドルータを介してパソコン側にはプライベート IP アドレスが割り当てられるのが普通ですが，家庭の外と特別な設定なく通信できます．これは，ブロードバンドルータが NAT(Network Address Translation) とよばれるプライベート IP アドレスとグローバル IP アドレスの変換の処理を行ってくれているからです．

本稿では，KUINS-III ではなぜ NAT が提供されていないのか，では部局側で KUINS-III に NAT の機能を持つルータ (NAT ルータ) を導入するにはどうすればよいかについて解説します．

NAT とセキュリティ

そもそもなぜ KUINS-III ではプライベート IP アドレスを採用したのでしょうか．これは，グローバル IP アドレスが不足していて， KUINS-III のような新しい空間に割り当てるだけの余裕がなかったからにすぎません．

プライベート IP アドレスを用いると，外部との直接の接続性が無くなってセキュリティ面で優れているという解説がされることがありますが，これは必ずしも本当ではありません．グローバル IP アドレスを用いても，対外接続ルータのところで外部との接続をフィルタリングしてやれば，ほとんど同じことだからです．

プライベート IP アドレスを用いて外部との接続に NAT を介することにすることは，直接グローバル IP アドレスで接続するのに比べ，プライバシーの観点からは優れています．すなわち，外部には NAT ルータの IP アドレスから接続しているようにしか見えないので，NAT ルータの内側にどのような機器があってそのうちどの機器から接続されてきたかということが，外側からは知る方法がないのです．

このことは，家庭などでネットワークを構成する場合にはメリットですが，大学のようなところで NAT ルータを導入する場合には注意しなければなりません．例えば，もし NAT の内側でウイルスに感染したパソコンが外に対して不正アクセスを繰り返しているような状況になったとしましょう．外からは，不正アクセスはすべて NAT ルータから行われているとしかわからず，NAT の内側でどのパソコン (1 台とは限りません) が不正アクセスを行っているかを特定するまでは，NAT ルータそのものを停止して配下の全端末の通信を停止せざるを得ないようなことも起こります．

なぜ KUINS-III では NAT を提供しないのか

KUINS-III の設計段階において，NAT の機能を提供するかどうかは慎重に検討され，結論としては見送られました．

第一の理由は，NAT の処理はルータに取って負荷の重い処理であることです．KUINS での利用においては百歩譲っても 10Mbps 以上の性能が必須と考えられますが，KUINS-III の

設計時点では，その性能を実現できる NAT ルータは非常に高価で，比較的安価なものは数 Mbps が限界でした．さらに，後述のように NAT 処理ごとのログを取ることにするとさらに厳しくなります．しかし，家庭へのブロードバンドサービスの普及とともに，この状況は変わってきています．

第二に，KUINS-III のハードウェア構成との親和性の問題があります．KUINS-III では，機器のコストおよび管理のコストを削減するために，ルーティングの処理を，全学で 8 台の基幹スイッチとよばれる高速の L3 スイッチに集約せざるを得ませんでした．これに NAT の処理を加えるためには，基幹スイッチ自体に NAT 処理をやらせるか，基幹スイッチの周りに VLAN の数だけ NAT ルータを並べるかのいずれかになりますが，前者は性能的に無理があり，後者は機器の管理ができなくなります．

第三に，ログの管理の問題があります．前節で述べたように，NAT ルータを介して外部に不正アクセスがあった場合に問題のある機器を特定できるようにするには，すべての通信に対して NAT によるアドレス変換がどのように行われたかをログとして記録しておくことが必須です．ログの保存期間について法律上の明確な定めはありませんが，最低 3ヵ月は保存しておくことが必要と言われています．KUINS において全通信でそのようなログを取ると膨大な量になり，現実的ではありません．

以上のことから，KUINS-III においては，NAT ではなくアプリケーションゲートウェイを介して学外と通信することを基本とし，KUINS として **Web プロキシサーバ，メールサーバ，SOCKS プロキシサーバ等**を提供することにしました．これに加え，部局で準備するアプリケーションサーバや，SSH によるユーザレベルでのポートフォーワーディングによりほとんどのアプリケーションは KUINS-III においても利用できるようになります (図 1).

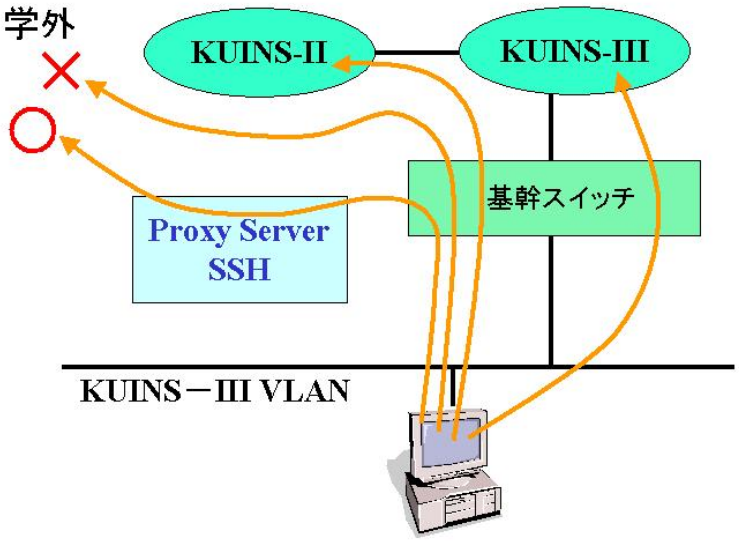


図 1: KUINS-III の通常の利用

部局での NAT ルータの設置

しかし，アプリケーションあるいは OS によっては，アプリケーションゲートウェイではどうしても対応できないものがあります．KUINS ではそのような場合に部局で KUINS-II と KUINS-III を橋渡しするように NAT ルータを設置することを禁止はしません．

前置きが長くなりましたが，KUINS-III に接続された端末から，NAT を介して学外へ接続できるようにするための方法を以下に解説します．部局で NAT ルータを設置する場合には，以下の 2 点に注意していただくことが条件となります．

- **必ず事前に KUINS に相談すること**
- **責任の所在を明確にし，NAT ルータにおけるログの管理をきちんと行うこと**

NAT ルータを不適切な設定で KUINS-III につないでしまうと，うまく通信できないばかりでなく KUINS 全体に波及するトラブルを発生させる可能性があります．事前に調整の上必要な設定項目をご連絡致しますので，接続の前に必ず事前にご相談ください．将来的には簡単な届出のみで NAT ルータの設置ができるようにする予定です．

NAT ルータを設置する際の注意点の第二は，法的責任に関してです．ここで示す方法では，KUINS-III に接続された端末から学外へのアクセスは，すべて NAT ルータの KUINS-II の側の IP アドレスを使って行われます．学外からは NAT ルータの KUINS-II の側の IP アドレスで接続されたということ以上はわかりません．**もし不正アクセスその他法律上の責任が問われるようなことになった場合，実際にそのアクセスがどの端末から行われたかを特定する責任が，NAT ルータの管理者，すなわち KUINS-II 側の IP address について責任者として届け出ている人にかかります．**

したがって，このような NAT ルータを設置する場合には，NAT ルータにおけるアドレス変換毎に，グローバル側とプライベート側での IP アドレスとポート番号の対応関係がきちんとログに取れるようにすることが必要です．また，対象とする KUINS-III 側の VLAN を，責任者が本当に責任が取れる小さな範囲，典型的には研究室単位くらいにしておき，接続される端末の台数も必要以上に増やさないことを強くお勧めします．

NAT ルータの導入方法と製品例

NAT ルータの導入方法としては，次のようになります．まず，NAT ルータの 2 つのネットワークインターフェースのグローバル IP アドレス側に KUIN-II の IP アドレス，プライベート IP アドレス側に接続する KUINS-III の固定 IP アドレスを振ります．また，KUINS-III では KUINS-III 用の DHCP サーバが動作しているため，NAT ルータの DHCP サーバの機能は必ず停止します (図 2)．

KUINS の DHCP サーバは，NAT がない場合と同じように default gateway として KUINS のルータ (基幹スイッチ) の IP アドレスを付与します．KUINS のルータでは，学内向けのパケットは通常通り配送します．一方学外へのパケットは通常であれば，ルータで破棄されるところ，代わりに NAT ルータへ redirect されます (図 3)．

これにより，学外との通信のパケットのみが NAT ルータを通過することになり，NAT の負荷やログの管理の点で有利になります．また万一 NAT ルータが停止しても，学内との通信は (NAT ルータのない) 通常の KUINS-III と同様にできます．

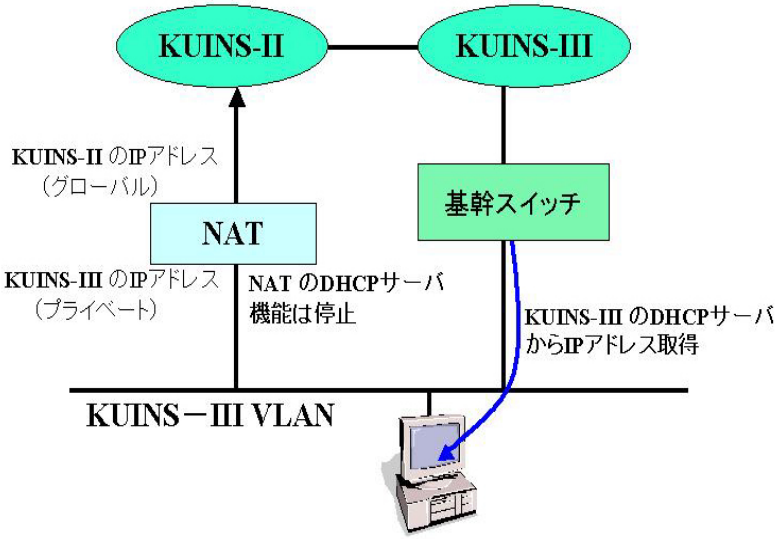


図 2: NAT ルータの導入方法

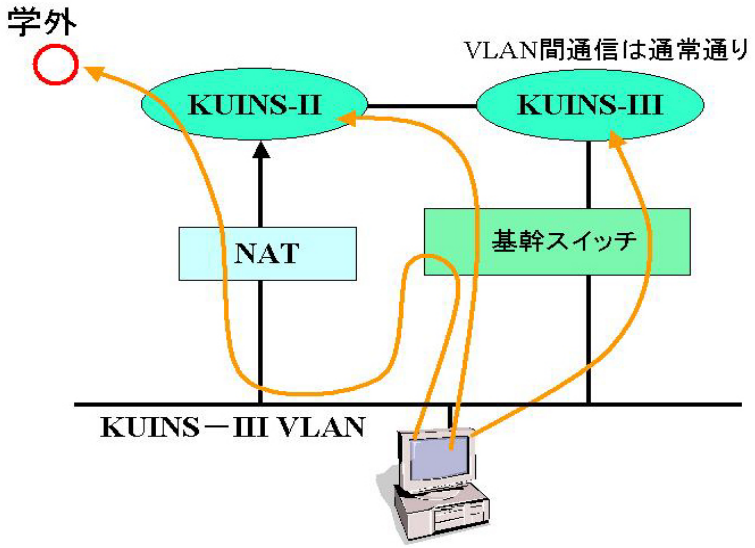


図 3: NAT ルータ使用時の動作

NAT ルータとしては,「ブロードバンドルータ」のような名前で売られている専用のルータを用いる方法と，PC に UNIX あるいは WindowsNT server を載せて動作させる方法があります．プロードバンドルータを利用する場合には，NAT 処理でのアドレス変換毎のグローバル側とプライベート側の IP アドレスとポート番号の対応関係がすべてログに残せることが条件です．また，ブロードバンドルータそのものはハードディスクなどの二次記憶を持たずメモリ容量も限られているため，必ずログを管理するためのサーバを別に用意して，そこへ syslog というプロトコルでログが飛ばせるようになっていることが必要です．

syslog ログ対応とうたっていても，アドレス変換ごとのログがきちんと取れるものは限定されるようです．こちらで確認している製品例としては YAMAHA RTA55i があります．PC やワークステーションに NAT ルータをさせる場合，きめ細かいログが取れること，ログの蓄積もそれ自身が行うことができる点で有利です．ただし，停電などの対策が必要になり長期安定運用のためにはそれなりの手間がかかります．

おわりに

以上，KUINS-II と KUINS-III を NAT ルータでつないで利便性を高くする方法について述べました．しかしながら利便性の向上はセキュリティレベルの低下と表裏一体であることを常に意識しておいてください．

最近の NAT ルータは，UPnP 対応や VPN 対応など高機能を売りにしていますが，これらの機能が予期せぬ不正侵入経路をつくってしまうことが稀ではありません．NAT ルータの設定の際には，使わなさそうな機能，よく理解できない機能はできるだけ停めた状態で運用なさるようご配慮下さい．

ウィルスチェック機能つきメールサーバ運用開始について

KUINS では，8 月 1 日より KUINS-III に接続された計算機から利用可能なメールサーバを正式に運用開始しましたので，お知らせします．

このメールサーバは，ウィルスチェック機能を持っており，ウィルスが検出された場合は，ウィルスの含まれる添付ファイルを削除するとともに，その旨の通知を行います．(脚注: このウィルスの情報は自動的に最新版に更新されるようになってはいますが，削除すべきウィルスに関する情報の更新は，一般にウィルスの発見より必ず後になってしまうため，油断は禁物です．)

送信用サーバとして，このメールサーバを利用する場合は，送信用メールサーバとして，**sendmail.kuins.net** を指定します．このメールサーバは KUINS-III からのみでなく，KUINS-II から発信されたメールの中継も行うように設定されていますので，KUINS-II からも自由に利用して頂けます．なお，すでに sendmail.kuins.kyoto-u.ac.jp という名前で暫定的に送信メールの中継サービスを開始していますが，これについてもウィルスチェック機能を持つサーバに切り替える予定です．

部局にて運用されているメールサーバから，KUINS の提供するウィルスチェック機能つきメールサーバを中継用に利用する方法については別途御相談下さい．

また，KUINS ニュース No. 30 でお知らせしました KUMX についても，今回準備を完了したウィルスチェック機能を持ったサーバによる中継に変更する予定です．もし，中継時のウィルスチェックを希望しない場合は，KUMX を利用しないように設定を変更して頂く必要があります．KUMX によるウィルスチェックの開始は，10 月 1 日を予定しています．

プロキシによるトンネリングについて

現在，KUINS-III のプロキシにおいて，httptunnel または類似のソフトウェア (以下，トンネリングソフトウェアと表記します) による通信が頻繁に記録されています．一般には，ftp やメール送受信を中継するソフトウェアが多いのですが，任意のプロトコルを中継できるものも見られるようなりました．トンネリングソフトウェアの利用により，KUINS-III のプライベート IP アドレス空間に設置された機器 (以下，内側機器と表記します) でも，グローバル IP アドレスを必須とするアプリケーションが利用可能となります．

その仕組みですが，内側機器から送信される通信は，まず，トンネリングソフトウェアにより内側機器で http プロトコルに変換されます．次に，Web プロキシを介して，インターネットに設置されたサーバ (本学のものとは限りません) に送信されます．サーバではトンネリングソフトウェアの逆変換により http プロトコルを元の通信プロトコルに戻し，インターネット上の任意の計算機にアクセスします．内側機器での受信は送信の逆の手順を行います．

この仕組みから，トンネリングソフトウェアの利用には以下の危険性があることが判ります．

- 内側機器は KUINS-III の保護下に置かれないことになります．http プロトコル変換/逆変換により，内側 PC は実質的にインターネットに直結された状態に置かれますので，あらゆる不正アクセスに曝されることとなります．
- その他の機器も KUINS-II/III の保護下に置かれなくなります．内側機器は KUINS-III の裏口となりますので，乗っ取られた場合，その機器が接続されている VLAN，さらにはその VLAN から到達可能な機器 (KUINS-II および KUINS-III VLAN に設置) が不正アクセスを受けることになります．

現在，セキュリティ監視装置において不正アクセスを検出しているトンネリングソフトウェアもあります．このため，トンネリングソフトウェアによる危険な通信を行っていると判断される場合は，VLAN 管理責任者に問い合わせをさせていただきます．

SSH ダウンロードサービスに関するおわび

KUINS ニュース No.33 でもお知らせしていますが，KUINS では京都大学における非営利目的利用に限定した SSH(Secure SHell) のサイトライセンスを取得し，学内向けにダウンロードを可能としました．

しかし，KUINS 側で京都大学向けアカデミックサイトライセンスの取得に手違いがあり，SSH 3.1 以前のプログラムで一部 evaluation licence(評価) 版を配布する事態になり，ユーザに多大なご迷惑をおかけいたしました．

平成 14 年 9 月現在，配布しているバージョン (3.2.0) はアカデミックサイトライセンスを取得しております．

ご使用の際には，お手数をかけることになって大変申し訳ありませんが，現在使用されている以前のバージョン (evaluation license 版も含む) をアンインストールしてから，最新バージョンをインストールして下さい.

なお，本バージョン (3.2.0) では，SSH Secure Shell for Windows Server に関しては，アカデミックサイトライセンスの適用範囲外となっています.

KUINS-III 利用ガイドのホームページ

KUINS-III が本格的に運用開始し，KUINS-II からの移行作業も進みつつある状況かと思いますが，この期間に利用者の皆様から KUIN-III に関する利用方法及び端末の設定方法について，数多くの質問やご指摘をいただきました.

KUINS 側で行った検証や利用者からの数多くの報告を基にして，KUINS-III 利用ガイドを KUINS ホームページ上にて，学内限定で公開しております．URL は以下の通りで，KUINS のトップページからリンクしていますので，ご参照いただければと思います.

`http://www.kuins.kyoto-u.ac.jp/KUINS3/kuins3-guide/`

なお，当ページに関する情報でご不明な点や，追加できる設定情報などがありましたら，`q-a@kuins.kyoto-u.ac.jp` までご連絡をお願いします.

大学における情報セキュリティポリシーの考え方について

近年は大学においても，大学の情報セキュリティ対策の強化が課題となっており，研究，教育，事務活動などのために多数かつ多様な情報を扱うコンピュータが接続されていることから，情報資産のセキュリティ確保に向けた取組の強化が重要とされます.

このほど，全国共同利用大型計算機センター長会議の下,「大学の情報セキュリティポリシーに関する研究会」では，大学の情報セキュリティポリシーの在り方について実践的な研究を行い,「大学における情報セキュリティポリシーの考え方」がまとめられました.

今後， 各大学における情報セキュリティポリシーを策定する際の参考となるように，ご活用願いたく思います.

詳しい情報は以下の URL にあります.

`http://www.kudpc.kyoto-u.ac.jp/Security/`

「京都 ONE」について

京都 ONE(http://www.kyoto-one.ad.jp) は，京都情報基盤協議会が京都市と連携して，京都の情報通信ネットワークの向上を目指し「地域 IX(インターネット・エクスチェンジ)」「iDC（インターネット・データ・センター)」を整備，活用する構想です.

京都地域に開かれた WAN(ワイド･エリア･ネットワーク) を構築し，それを活用した ASP(アプリケーション・サービス・プロバイダ) などの様々なサービスを展開することにより，インターネットと言う共通の基盤の上で，市民生活や産業活動などの京都地域内の活動を一体的に向上させることを目指すものです.

京都 ONE のテーマの一つに,『大学間情報ネットワークの構築』があります．これは，京都に数多く集積する「大学」を高速な情報通信ネットワークで結ぶことにより，大学間連携，学際研究のより一層の促進を図ろうとするものです.

この一貫として，本年 4 月に京都リサーチパーク (KRP) にある (財) 京都高度技術研究所 (ASTEM) と本学吉田キャンパスの間が，ATM OC-12c (622Mbps) で接続されました．さらに，(財) 大学コンソーシアム京都 (http://www.consortium.or.jp) や京都デジタルアーカイブ研究センター (http://www.kyoto-archives.gr.jp) のあるキャンパスプラザ京都と本学との間も，近日中に ATM OC-12c (622Mbps) で接続される予定です.

情報学研究科 無線 LAN の使用について

情報学研究科 計算機委員会

1. 情報学研究科 無線 LAN システム

情報学研究科では，平成 12 年度より「情報学研究科教育計算機システム」の一部として，同研究科の構成員が使用するスペースを中心に無線 LAN システムの設置・運用を行っています．このシステムについて，主に講義室等の公共スペースをカバーするという性質に鑑み，情報学研究科内にとどまらず他部局の方にも利用いただけるよう，セキュリティを考慮したネットワーク設定と公開ポリシー策定とを行いました．新たに無線 LAN アクセスポイントを設置される部局は電波干渉のないようご配慮下さい．本稿では，同無線 LAN システムをご利用いただく際のポリシーと，利用のために必要な諸設定に関して説明いたします．なお，無線 LAN のアクセスポイント設置場所については

http://www.i.kyoto-u.ac.jp/informatics/MUSENAPCH1.PDF

を参照してください．表中「10 号館」などとあるのは「工学部 10 号館」をさします.

2. 公開ポリシー

情報学研究科無線 LAN システムは，以下のポリシーのもとに公開するものです．これらに御同意の上，あくまでも自己責任においてご利用ください.

- 情報学研究科無線 LAN システムの利用において，利用者は情報学研究科に登録を行うものとする．無線 LAN カードを用いて

http://172.16.7.252/cgi-bin/wireless.cgi
で登録を行なって下さい．なお，未登録の無線 LAN カードは，一定時間を過ぎると利用できなくなります．

- 同システムを用いて生じた一切の不具合について，情報学研究科はその責任を負わない．
- 同システムは利用者にことわりなく停止することがある．
- 端末および無線 LAN カードなどの機材は利用者が準備するものとする．
- 無線 LAN システムから外部への通信は SSH を用いた学内への通信のみを許可する．したがって，Web 閲覧等を行うためには，学内にサーバを設置し，そこでユーザ認証を行った上で，SSH による ポートフォワーディングなどを行う必要がある．
- 上記のポートフォワーディング等を行うのに必要な，SSH サーバやプロクシサーバの類は，利用者の所属部局ないし研究室等において用意するものとする．(情報学研究科として他部局向けにサーバを用意することなどはしない) [1]
- この公開ポリシーは情報学研究科において必要に応じて変更する．

3. 利用方法

情報学研究科無線 LAN システムを利用するにあたっては，以下の機材および設定が必要となります．

機材

- SSH サーバ：学内 (KUINS-II 内) に一つ．
- 端末：ノート PC など．
- 無線 LAN カード：IEEE802.11b に準拠したもの (市販のものの大半は 準拠)．

設定

1. SSH サーバに利用者のアカウントを作成する．方法はサーバを用意した部局・研究室の管理者に問合せる．
2. 無線 LAN カードの設定を行う． 各々の方法は無線 LAN カードおよび端末のマニュアルを参照 [2]
   i. ドライバのインストール．
   ii. SSID の設定：SSID を ”Wireless”(先頭のみ大文字．引用符は含まない) にする．
   iii. 通信モードの設定：”Infrastracture” (または「インフラストラクチャ」) モードでの通信とする．
   iv. 暗号化は使用しない．
3. SSH のポートフォワーディングの設定を行う．
   - SSH によるポートフォワーディングに関する説明は
     http://www.i.kyoto-u.ac.jp/local/manual/ssh/portforwarding.html
     を参照のこと．

[1] 補足：この件については，学術情報メディアセンターの教育用システムのサーバを利用できる可能性が，KUINS-III に関する Q&A http://www.kuins.kyoto-u.ac.jp/KUINS3/Q_and_A.html#Z9
でとりあげられています．ただし，(本稿執筆段階では) サービスはまだ提供されていません．

[2] 情報学研究科で配布された SS Magic 11 の設定については情報学研究科教育計算機システム 機器取扱説明 http://www.i.kyoto-u.ac.jp/informatics/ の「無線 LAN 関係」の項目を参照のこと．

みあこネット

京都街中無線インターネットプロジェクトみあこネット (Mobile Internet Access in KyotO, http://www.miako.net) は，特定非営利活動法人日本サスティナブル・コミュニティ・センター (SCCJ，http://www.sccj.com) を中心に，本学大学院情報学研究科知能情報学専攻，(財) 京都高度技術研究所，モバイルインターネットサービス (株) などが協力して行っている公衆無線インターネットサービスの実験プロジェクトです.

京都駅ビル，四条大橋から鴨川沿い，百万遍交差点付近など京都府下に 150 以上の無線基地局が設置され，実験期間中，ノート PC と無線 LAN カードを用いて無料で無線モバイルブロードバンドの実験サービスを受けられます．利用者一人一人にグローバル固定 IP アドレスを割り当て，Mobile IP の技術を用いて移動透過性を実現していることと，無線環境でも安心して使えるセキュリティ技術が特徴です.

利用には事前のユーザ登録が必要ですが，本学関係者は Web によるオンラインでのアカウント取得が可能です.

http://register.miako.net/kyoto-u/
(本学学内 LAN からのみアクセス可能)

詳しくは同プロジェクトの Web ページを御覧ください.

KUINS 会議日誌

平成 14 年 3 月 25 日〜平成 14 年 9 月 15 日

学術情報システム整備委員会

平成 14 年 5 月 23 日 (第 35 回)

- 学術情報メディアセンター KUINS 利用負担金規程について
- 専門委員会について
- 情報セキュリティポリシー策定について

KUINS 運用委員会

平成 14 年 8 月 20 日 (第 1 回)

- KUINS-II，III 運用状況について
- 学術情報メディアセンターパンフレットについて
- KUINS データベースについて
- 遠隔地の通信状況について
- その他

平成 14 年 9 月 5 日 (第 2 回)

- KUINS ニュース (No.38) 発行について
- 学術情報メディアセンター パンフレットについて
- KUINS-III パンフレットについて
- KUINS のセキュリティ対策について
- その他

吉田構内高圧幹線定期点検に伴う停電のお知らせ

10 月下旬から 12 月上旬にかけての週末に，吉田構内において停電が予定されており，これに伴い，KUINS のネットワークが大規模にわたって停止する恐れがあります．詳細情報につきましては，文書と KUINS のホームページの方で後日アナウンスしますので，ご確認の方をよろしくお願いします．

KUINS 関連メールアドレス一覧

KUINS に関する様々なお問い合わせ等がありましたら、以下のメールアドレスまでご連絡下さい。

問い合わせ窓口

- KUINS に関する総合窓口
  q-a@kuins.kyoto-u.ac.jp
- KUINS のトラブルレポート先
  lan-trouble@kuins.kyoto-u.ac.jp
- KUINS-II/ATM 接続に関する問い合わせ先
  atm-tech@kuins.kyoto-u.ac.jp
- ネット中継機器の貸出しに関する問い合わせ先
  stream@kuins.kyoto-u.ac.jp

KUINS への接続申請に関するアドレス

- KUINS-III VLAN 設定変更申請届の提出先
  k3-vlan@kuins.kyoto-u.ac.jp(アドレス変更になりました)
- メールサーバ申請届の提出先
  spamfilt@kuins.kyoto-u.ac.jp
- 接続機器 DNS 登録申請に関する問い合わせ
  ns-admin@kuins.kyoto-u.ac.jp
- 新たなサブドメインの申請窓口
  domain@kuins.kyoto-u.ac.jp

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)）