ISSN 0917-3668
2001.8.6

KUINS ニュース

No. 35

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

京都大学入学式ネット中継の模様

目　　次

卒業式・入学式のネット中継の報告 432
ネット中継機器の貸出しについて 432
KUINS-I 基幹ループ LAN ノード全面停止に関するお知らせ 433
KUINS の Web でセキュリティ情報を提供 434
スパムメール不正中継対策徹底のお願い 434
KUINS-III の概要説明 435
KUINS-III の IP アドレス 439
総合情報メディアセンター新棟の館内ネットワークについて 440
KUINS 接続状況 448
KUINS 関連メールアドレス一覧 449
KUINS 会議日誌 450
お知らせ 450

卒業式 ・入学式のネット中継の報告

学術情報ネットワーク機構では，前年度の京都大学学位授与式，卒業式 (平成 13 年 3 月) 及び本年度の入学式 (平成 13 年 4 月) を学内ネットワークを介して，学内に限定してネット中継を行いました．中継当日に機器等の不良の為に途中で中継が中断される状態となり，大変ご迷惑をおかけしましたが，卒業式が 55 人，入学式が 48 人の方に視聴していただきました．今回使用した機器のシステム構成は図 1 に示す通りです．

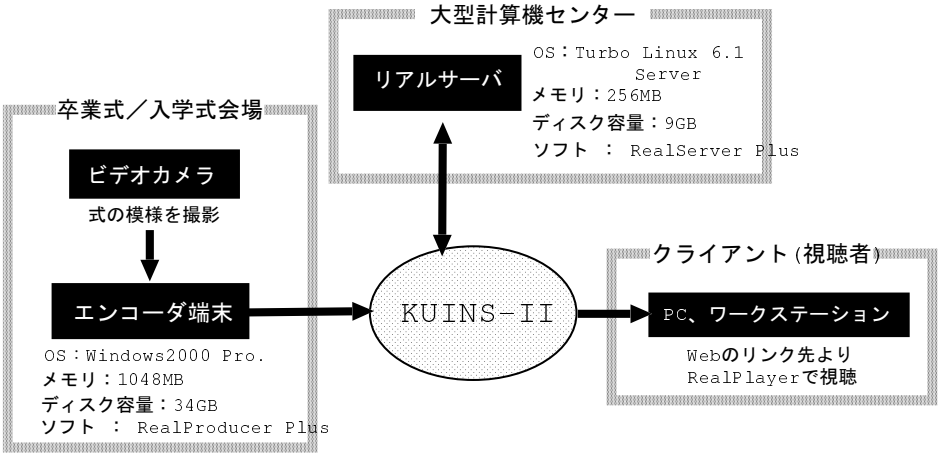

図 1: 中継のシステム構成図

ネット中継機器の貸出しについて

学術情報ネットワーク機構では，インターネットを経由して講演等をリアルタイム中継を行ったり，映像ライブラリとして配信する映像ファイルを作成する為の機器を貸出しを行います．貸出し機器 (ビデオカメラ，エンコーダ端末) は図 1 の通りです．インターネット経由の際のデータ転送方式は，ダウンロード方式によらないストリーミング方式でリアルタイムに転送します．

尚，機器の貸出しを受ける場合，以下の条件を必ず守ってください．

(1) 貸出し担当掛より，リアルサーバアクセス用のユーザアカウントとパスワードの発行を受ける．

(2) 機材の貸出し期間は，貸出し日を含めて 7 日間までとする．

(3) 映像ファイル配信の場合は，ファイルの保存期間をファイル作成日より 1ヶ月間とする (保存期間を過ぎた時点でファイルを削除しますので，後にそのファイルが必要の場合は，事前に各自の端末にダウンロードしておいて下さい．)

(4) 作成できる配信ファイルの全容量は総計 1GB までとする.

(5) エンコーダ端末の設定は必要以外に変更しないで下さい. 故意による過失の場合は元の状態に回復してから返却して戴きます.

図 1: 貸出機器一式

機器の利用方法は, 以下の流れになります.

- 中継を行う場合
  ビデオカメラで撮影して, 講演等の中継映像を, エンコーダ端末中の RealProducer Plus でエンコードしながら大型計算機センターに設置しているリアルサーバに転送し, そこで映像配信を行います.

- 映像ライブラリを作成する場合
  使用者は映像メディアソースをエンコーダ端末でエンコードしてリアルサーバに転送して, 映像ライブラリを作成します.

機器の使用方法及びリアルサーバへのアクセス方法等の詳細については, 機器貸出しの際に「利用の手引き」をお渡ししますので, そちらをご参照下さい. 貸出し希望の連絡先は, 以下の通りです.

問合わせ先 : 大型計算機センター等ネットワーク掛
電話 : 075-753-7432
電子メール : stream@kuins.kyoto-u.ac.jp

KUINS-I 基幹ループ LAN ノード全面停止に関するお知らせ

学術情報ネットワーク機構事務室

昭和 63 年度より 13 年間運用してきました KUINS-I の基幹ループ LAN ノードを, 今年度導入される KUINS-III の運用開始に伴い, 平成 13 年 7 月 27 日 (金) をもって停止し, 全て撤去することになりました.

長い間, 基幹ループ LAN を利用していただき, 有り難うございました.

KUINS の Web でセキュリティ情報を提供

学術情報ネットワーク機構

学術情報ネットワーク機構では，KUINS に接続し安全にインターネットを利用するために，最低限必要となる対策や，参考となる情報の提供を KUINS の Web にて行っています．URL は次の通りで，KUINS のトップページからもたどることができます．

`http://www.kuins.kyoto-u.ac.jp/security_index.html`

内容は，推奨するウィルス対策，セキュリティホールとパッチの情報，CERT Advisory[1] の概略などで，各機関が発行する情報へのリンクが主となっています．

計算機のセキュリティに対する認識の甘さから不正アクセスの被害に遭う事例が実際に報告され，その数・頻度は増加傾向にあります．KUINS に接続しインターネットを利用する計算機の管理者は，最新の情報に基づいた対策を行うべきであり，このページはその手助けを目的としてボランタリーに運営されております．

なお，このページにはできるだけ正しい内容を迅速に収集し提供するよう努力しておりますが，情報の利用やパッチの適用にあたっては管理者の判断と責任において行ってくださるようお願いします．

また，万一不幸にして不正アクセスやウィルスの被害にあってしまった場合には，平成 12 年 10 月 16 日付け経情処第 72 号「コンピュータ不正アクセス対応要領」[2]に沿って，確実に対処していただくようお願いします．

スパムメール不正中継対策徹底のお願い

学術情報ネットワーク機構

学術情報ネットワーク機構では，2000 年 4 月よりスパムメールの不正中継対策を行い，2001 年 7 月までに約 150 のサブネットにおいてフィルタの設置を完了しております．

しかしながら，一部のサブネットでは，対外メールサーバそのものが存在しない，関係する利用者間の調整がつかないなどの理由で，フィルタの設定希望の回答がない状態のまま放置されております．その数はおおよそ 80 にのぼります．このようなサブネットに不用意に接続されたサーバが不正中継の踏み台となってしまい，いまだに機構宛ての苦情がなくなることはありません．

そこで，学術情報ネットワーク機構では **2001 年 9 月末まで** にスパム不正中継対策済の届け出がないサブネットに関しては，対外メールサーバが存在しないものとして，各サブネッ

[1] `http://www.cert.org/advisories/`
[2] `http://www.kuins.kyoto-u.ac.jp/news/34/fusei.html`

トの入口ルータにおいて一切の **SMTP (25/tcp)** 接続を遮断するフィルタを設置いたしますのでご承知おきください.

この件に関する連絡先は次の通りです.

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)
spamfilt@kuins.kyoto-u.ac.jp

KUINS-III の概要説明

学術情報ネットワーク機構

現在，KUINS-III の個々の情報コンセント，VLAN，VLAN 間ルーティング等の調査を行っております．KUINS-III では一つ一つの情報コンセント単位でアクセス制御を行うため，調査項目が多岐かつ膨大になりお手間をお掛けしていると思いますが，これからも京都大学がインターネットへの接続を続けるには必要となる作業ですので，ご協力いただくようよろしくお願いします.

まず，KUINS-III の論理構成を図 1 に示します．図にも含まれていますが，KUINS-III の特徴としては以下のものがあります.

- プライベート IP アドレスを利用
  10.224.0.0〜10.255.255.255 を利用することで学外と直接通信できなくなるのと引き換えに，利用できる IP アドレス数が増えます．本ニュース No.34 でもお願いしています通り，現在上記のプライベート IP 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.

  後述する VLAN 一つあたり最小で 64 個の IP アドレスが利用できます (実際には，ネットワーク制御用に最大 9 個利用しますので，55 個となります)．必要があれば現状の 1.5 倍程度の IP アドレスを利用できます．また，直接学外からアクセスできませんので，セキュリティホールへの攻撃による不正アクセスを受けたり，ウィルスや攻撃ソフトに感染した計算機が学外に対して攻撃を行う危険性がかなり小さくなります.

- DHCP による IP アドレス発行
  KUINS-III では DHCP による IP アドレス発行を標準とします．従って，KUINS-II のように接続届けを出さずにネットワークを利用できます．また，自宅からノートパソコンを持ち込む際に，ネットワークの設定を変更する手間が省けます．ただし，ファイルサーバやプリンタのように固定された IP アドレスが必要な場合は，DHCP 割り当ての対象外としますので，その台数を申請してください.

- VLAN の導入 (原則として，同一建物内に限る)
  標準として，各部屋に 2 個ずつ情報コンセントが設置されます．VLAN によって，分散した部屋の情報コンセントを仮想的に統合し，一つの LAN として利用できます．例えば，2 階と 3 階に研究室が分散していても，同じ部屋のネットワークにつながっている感覚で計算機等が利用できます．また，VLAN の最小単位は一つの情報コンセントとなりますので，部屋毎に独立した (例えば，隣の部屋から誤ってプリントアウトされることのない) ネットワークを構築することも可能です．

- KUINS-III から外へのアクセス制御
  KUINS-III ではプライベート IP アドレスを利用するため，学外へアクセスすることはできません．Web や ftp に関しては KUINS 機構側で proxy サーバを設置しますので，学外へアクセス可能です．ただし，後述しますが，不特定多数の人が出入りする部屋については，proxy サーバの利用はできません．また，KUINS-III から KUINS-II へのアクセスは可能ですが，通信可能なプロトコルも部屋ごとに異なります．

- VLAN 間ルーティングにより通信を制御
  KUINS-III では原則として VLAN 間の通信はできません．ただし，研究科事務 VLAN と専攻事務 VLAN でファイル共有をしたい，個々の研究室 VLAN から専攻共有のプリンタに印刷したい場合，レイヤー 3 ルーティングによって VLAN 間の通信が可能となります．レイヤー 3 ルーティングですので，通信可能なプロトコルも制限することが可能です．

- KUINS-II から KUINS-III のアクセス禁止
  理由は後述しますが，KUINS-II から KUINS-III へのアクセスできません．

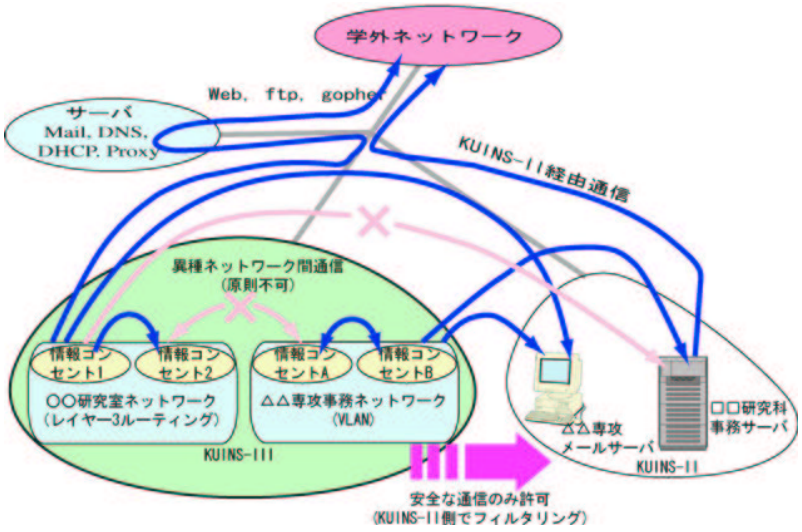

図 1: KUINS-III の論理構成

KUINS-III の主目的は学内全体の高いセキュリティレベルの確保です．このため，不正アクセスを行っている VLAN は発見次第 KUINS-II および学外への接続を遮断させていただきます．さらに，不正アクセスが当該 VLAN からルーティングで到達可能な VLAN や KUINS-II サブネットに及んでいる場合，これらも遮断の対象となり得ます．建物全体で一つの VLAN，研究科全体で VLAN 間ルーティングを行うような大雑把な設計をされますと，どこかで 1 台のパソコンが不正アクセスを行っただけで，研究科全体の KUINS-II および III が通信遮断となる可能性があります．このため，VLAN のサイズおよび VLAN 間ルーティングの範囲はできるだけ小さくしてください．

KUINS-III のもう一つの特徴として，それぞれの VLAN によって利用できるサービス (通信プロトコル) を細かく設定できる点があります．これは，VLAN に属する部屋によってセキュリティのレベルが異なり，KUINS-III 全体のセキュリティレベルを維持するためには，そのレベルに応じてアクセスを制御する必要があるためです．セキュリティレベルの高い VLAN からは比較的自由に KUINS-II へアクセスできます．一方，セキュリティレベルの低い VLAN では KUINS-II へのアクセスを制限を受けますし，さらには KUINS-III で提供する proxy サーバも利用できない場合があります．

個々の VLAN のセキュリティレベルを定めるには，まず，当該 VLAN の特性に応じた物理的セキュリティ，人的セキュリティ，技術的セキュリティの組み合わせ考えていただきます．

まずは，VLAN に所属する個々の部屋ごとに以下のセキュリティを考えてください．

- 物理的セキュリティ
  建物や部屋の入出制限 ･施錠方針，つまり，そこに入出する人が限定されているかなどによってそのレベルが定義されます．

- 人的セキュリティ
  各部屋に入出する人の中で，もっとも低いセキュリティ意識を持つ人にそのレベルを合わせます．

KUINS 機構では部屋のセキュリティレベルの典型として図 2 に示す 3 種類を想定しております．まず，事務室と教官室については，空室時に施錠され，かつ，人の出入りがある程度限定されていると考えられます．また，その部屋に居る人のセキュリティ意識も比較的高いものと期待しております．一方，学生部屋については，その部屋に入出する人が当該研究室の学生だけでない場合があるなどの理由で，物理的セキュリティは若干低く想定しておりますが，その部屋に居る人のセキュリティ意識は事務室と同等に比較的高いものと期待しております．三つ目の講義室 (一般に公開された部屋を意味します) ですが，未使用時の施錠や人の出入りが制御できない場合，最低レベルの人が特定できませんので，人的セキュリティは確保できないと判断してください．さらに，学生部屋ではあるが，講座単位で管理していない大部屋であるなど，人の出入りが制御しにくい場合は，講義室と同等のセキュリティレベルと判断してください．

VLAN としてのセキュリティレベルは，当該 VLAN に属する部屋の内，最もレベルの低いものと同一となります．例えば，教官室と学生部屋で一つの VLAN を構成する場合，VLAN のセキュリティレベルは学生部屋として考えてください．

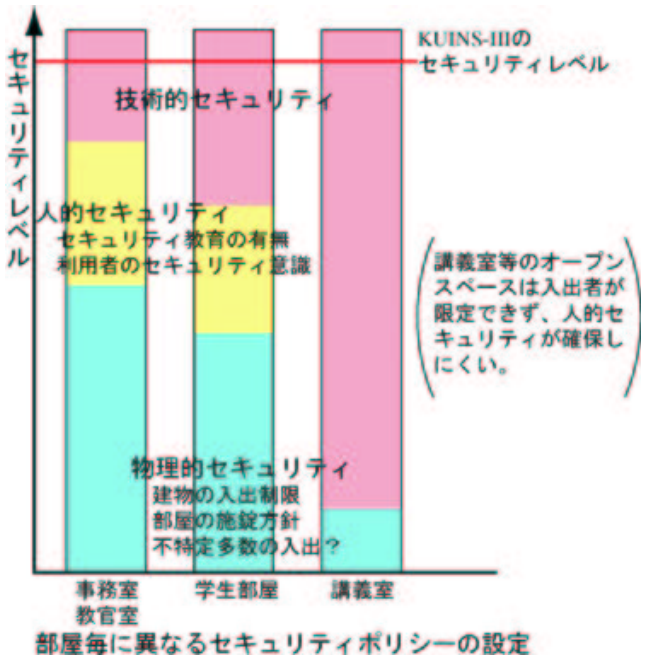

図 2: セキュリティポリシーの概念

物理的セキュリティと人的セキュリティでは KUINS-III のセキュリティレベルに達しない分を技術的セキュリティ，つまり，KUINS-II および学外へのアクセス制御で補うことになります．

例えば，事務室，教官室，学生部屋については KUINS-III から KUINS-II への TCP および UDP アクセス (telnet や ftp) は，よほど危険なものを除き，申請されても問題ないと思われます．ただし，一般的な学生部屋に比べ物理的あるいは人的セキュリティが低い，一部のアクセスで十分であるなどの理由があれば，KUINS-III から KUINS-II へのアクセスに制限を加えることも可能です．

また，講義室については KUINS-III から KUINS-II へのアクセスは ssh のみが可能となります．また，若干安全性は劣りますが，マイクロソフト社製 Windows 系で採用されている PPTP の利用も可能です．つまり，講義室では利用者を特定しにくいため，KUINS-II 側に設置された何らかの計算機で利用者の認証を得ることでセキュリティレベルを高めていただきます．その他の通信については ssh または PPTP のトンネリングを利用してください．さらに，講義室系では，利用者が限定しにくいため，KUINS-III の proxy サーバも利用できませんので，Web を利用される場合もトンネリングが必須となります．もちろん，利用者認証機能やセキュリティ対策を部局によって施した講義室であれば，KUINS-II へのアクセス制限を緩和することはできます．その場合は，セキュリティ確保の具体的な実現手法を KUINS 機構に提示していただくことになります．

また，レイヤー 3 ルーティングで VLAN 間で相互通信を行う場合は，VLAN のセキュリティレベルが同一であることが条件となります．セキュリティレベルが異なる場合は，レベルの高い VLAN から低い VLAN へのアクセスは可能ですが，逆向きはできません．同じ理由で，

KUINS-II は KUINS-III よりもセキュリティレベルが低いため，KUINS-II から KUINS-III へのアクセスはできません．

このように，KUINS-III ではできないことが沢山あります．従って，Web サーバなどのように対外サービスを行う計算機，あるいは，KUINS-III の VLAN やレイヤー 3 ルーティングでは実現できない通信を行う計算機は KUINS-II に残ることになります．このような計算機のセキュリティ確保は，従来通り，それぞれの計算機管理者にご負担いただくことになります．ただし，これらの計算機へのアクセスを許可する KUINS-III VLAN が限定できる場合は，フィルタリングによってその負担を軽減できる可能性がありますので，KUINS 機構までご相談下さい．なお，現在，KUINS-II 上では計算機管理者が不明確なまま稼働している計算機が多数見受けられるため，9 月下旬頃に個々の計算機に関して管理状態の調査を行う予定です．

最後に，注意点ですが，高セキュリティレベルの確保に重点を置いたため，KUINS-III の設置機器はそれほど高性能ではありません．例えば，末端スイッチから情報コンセントまでの配線は 1Gbps での通信が可能ですが，実際には 100/10Mbps での提供となります．情報コンセントの通信速度を上げたい，あるい，館内スイッチをもっと高性能なものに変えたいとの理由で，新たなネットワーク機器を部局で購入される場合もあるかと思います．その際のお願いなのですが，部局で KUINS-III への追加機器の購入を検討される場合，あるいは，建物の新築の際にネットワーク機器を設置される場合は，事前に KUINS 機構に相談してください．

KUINS-III では安全性の確保のため，KUINS-III に接続されているネットワーク機器は様々な方式で，機器の相互認証と異機器の存在の検出を行います．このため，KUINS 機構への事前相談のないまま部局で購入されたネットワーク機器を KUINS-III の一部として設置されますと，その機器から下流へは VLAN やサブネットの設定情報が一切伝わらず，該当するネットワーク全体の通信が途絶するように設計されています．例えば，館内スイッチを無断で取り換えた場合，建物全体の通信が途絶します．

もちろん，情報コンセントから先にハブやスイッチを設置される場合は問題ありませんので，KUINS 機構への事前相談は不要です．

KUINS-III の IP アドレス

本号別掲の記事にもありますように，今年度導入する KUINS-III では各端末の IP アドレスを RFC1918[1] で定められたプライベートアドレスの，次の範囲から採番します．

10.224.0.0 から 10.255.255.255 まで

これは，現在 KUINS が利用可能なグローバルアドレス (クラス B 二つ分) の 16 倍にあたります．

[1] http://www.ietf.org/rfc/rfc1918.txt

なお，KUINS-III に関する経路情報は KUINS-II にも流通させますので，現在 KUINS-II に接続されたファイアウォールの配下などにおいても，この範囲と重複するアドレスの利用は避けなければなりません．

この結果，以前より KUINS ニュース No. 22 でアナウンス[2] しております，

192.168.128.0 から 192.168.255.255 まで

をあわせ，次の二つのプライベートアドレス範囲を学術情報ネットワーク機構で重複が起らないよう管理させていただくことになります．

192.168.128/17 (192.168.128.0 〜 192.168.255.255)
10.224/11 (10.224.0.0 〜 10.255.255.255)

本件に関連して，現在重複するプライベートアドレスをご利用の方は次の連絡先までできるだけ早めにご相談ください．

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)
q-a@kuins.kyoto-u.ac.jp

総合情報メディアセンター新棟の館内ネットワークについて

総合情報メディアセンター　中村素典

1. はじめに

平成 12 年 7 月，総合人間学部構内の南端に総合情報メディアセンターの新棟が竣工し，平成 13 年度より館内の全サービスの提供を開始した．これまで，工学部 1 号館，工学部 10 号館，楽友会館等に分散してサービスを提供していたものがこれにより 1 ヶ所に集まったことになる (図 1)．新棟の各階の構成は次のようになっている．

- 4 階: 教育支援部門および開発支援部門の研究室，会議室
- 3 階，2 階:マルチメディア講義室，マルチメディア演習室，語学実習 CALL 室
- 1 階: オープンスペースラボラトリ (自由利用の端末を設置)，運用管理室，事務室
- 地階:計算機室，映像配信室，スタジオ，教材作成室

総合情報メディアセンターのネットワークは，学内の教職員および学生に交付するアカウントで利用可能な教育用計算機システム (新棟では利用者用端末は 1 階から 3 階に設置，また学内の 13 部局にもサテライト演習室を配置) のネットワークと，センター内のスタッフお

[2] http://www.kuins.kyoto-u.ac.jp/news/22/privateIP.html

図 1: 総合情報メディアセンター新棟の外観

よび研究室に配属された学生が研究開発およびシステムを運用するために利用する館内ネットワークの 2 系統から構成されている．

前者は現在利用中のシステムが今年度でレンタル期間を満了し，来年度からサービスを提供する次期システムへのリプレースに向けて作業が進行している．現在のシステムのネットワークについては，すでに KUINS ニュース No.28 等で紹介されているので，そちらをご覧頂きたい．また次期システムについてはサービス開始の準備が整った頃に改めて紹介することになるであろう．今回は後者の館内ネットワークについて紹介する．

2. 館内ネットワークの概要

総合情報メディアセンターの新棟では，最近建築された他部局の新棟と同様に，竣工当初から各部屋には情報コンセントが設けられている．この情報コンセントは各階に設けられた EPS(電気通信用パイプスペース) を経由して地階の計算機室に通じている．しかし，各情報コンセントから計算機室までの配線距離は 100BaseTX 等の規格上の上限である 100 メートルを越えてしまうため，各階の EPS 内に設置したスイッチングハブで一旦中継を行っている．4 階は各分野の研究室があり多数の利用者が居るため，地階から 4 階までは Gigabit Ethernet (1000BaseSX) で接続しているが，それ以外に関してはコストを抑えるため 100BaseTX で接続している (図 2)．

館内ネットワークにおいては，各サブネットの用途に応じて 20 個弱の VLAN を設けている．

- ネットワーク管理用 VLAN(プライベート)
- KUINS との接続用 VLAN(グローバル)
- サーバ用 VLAN(グローバル)

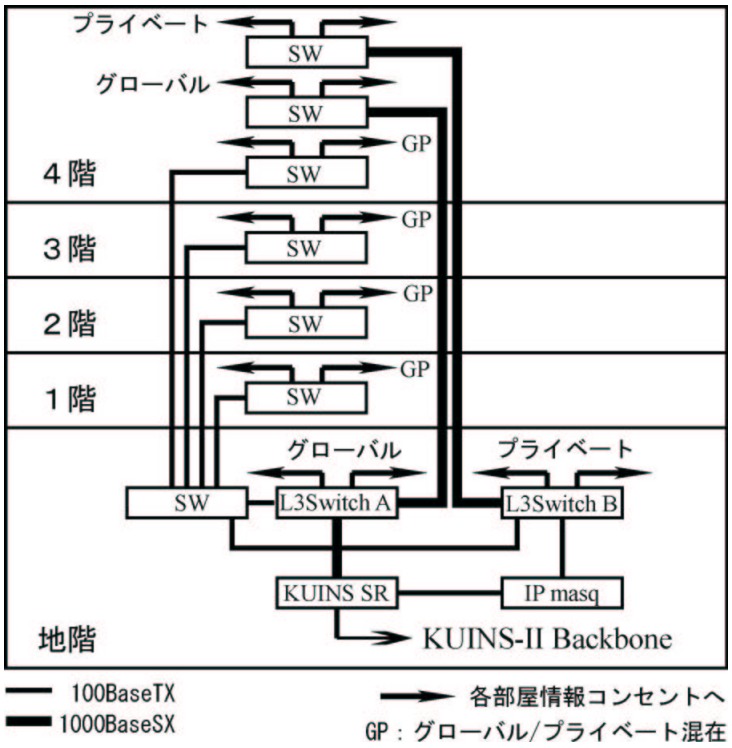

図 2: 館内配線

- 事務用 VLAN(プライベート)
- 運用管理用 VLAN(グローバル/プライベート)
- 遠隔講義用 VLAN(グローバル/プライベート)
- 各研究室用 VLAN(グローバル/プライベート)

運用管理，遠隔講義，各研究室のそれぞれにはグローバルアドレスで利用する VLAN(以下，グローバルサブネットと記す) とプライベートアドレスで利用する VLAN(以下，プライベートサブネットと記す) の両方を用意し，計算機の用途に応じて使い分けることができるようにしている．

ちなみに，一般ユーザから見た場合，サブネット」と VLAN」の 2 つの用語の間に意味的な違いはほとんどない．ポート単位で参加するサブネットを設定変更できたり，1 本の UTP ケーブルに複数のサブネットを設定する (タグ VLAN) ことが可能なスイッチングハブを用いて，サブネットを自由に任意のスイッチの任意のポートに割り当てることができるようにしたものを特に VLAN(Virtual LAN) と呼ぶ (アーキテクチャを示す用語)．この場合，スイッチングハブの内部設定において，それぞれのサブネットを VLAN1，VLAN2 のように区別することも多いため，それぞれのサブネットに相当するものとして VLAN と呼ぶことが多い (サブネットと同義)．メディアセンターの館内ネットワークにおいても，VLAN に対応したスイッチングハブを利用し，少ない台数で多数のサブネットによるネットワークを構成している．

VLAN の概念自体はそんなに新しいものではないが，以前はベンダごとの独自規格で実現されていた．しかし，IEEE 802.1Q 規格が 1998 年に制定されたことで，異なるベンダのスイッチングハブを混在させた VLAN が利用できるようになり，急速に普及しつつある．(しかし，機器によっては VLAN に対応しているといっても 802.1Q 規格に基づいた柔軟な設定に対応できないものもあるので，機器の購入の際には注意が必要である．KUINS-III ではさらにネットワーク管理用の別の仕組みも利用し管理コストを下げる努力をしている．)

用途ごとに分離された各サブネットの間で通信ができるようにするには，それらを接続するためのルーティングが可能な機器 (ルータあるいはレイヤ 3 スイッチ，ほぼ同義だが，後者はハードウェアでルーティングを行うことを明示した用語である) が必要となる．ここでは，次項で述べる IP masqurade 等の利用を考慮して図 3 に示すようなネットワーク設計とした．

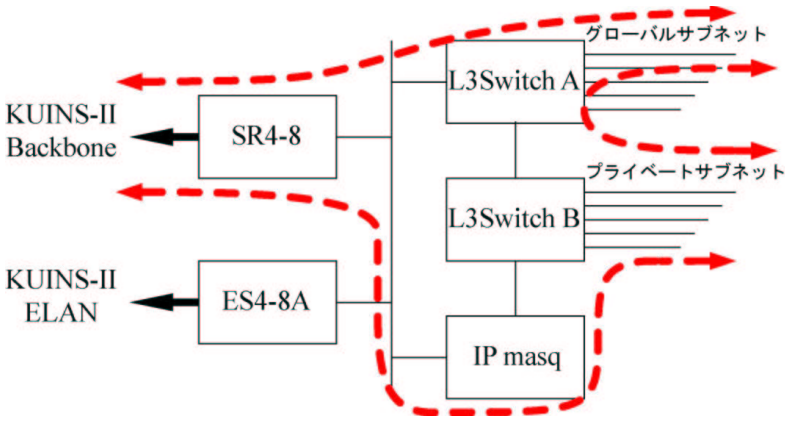

図 3: サブネット間通信の論理設計

このように設計することで，各サブネットにおける通信の際には次のような通信路が利用される．

- グローバルサブネットとプライベートサブネットとの通信は，スイッチ A，スイッチ B を経由
- グローバルサブネットと外部との通信はスイッチ A のみを経由して外へ
- プライベートサブネットと外部との通信はスイッチ B，IPmasq を経由して外へ

これにより，グローバルサブネットとプライベートサブネットとの通信が IPmasq を経由することはなく，両者間で IPmasq の性能に依存しない高速な通信が可能になるとともに (一般に，IP masqurade はソフトウェア処理であるため処理速度はあまり高くない)，個々の計算機を単位とするアクセス制限も可能となる．また，スイッチ A ではグローバルサブネットへの不正アクセスを防止するためのフィルタリング設定を行っている．

ちなみに，スイッチ A および B として当時価格が比較的手頃だった Foundry 社の NetIron Layer3 Stackable Switch および FastIron Workgroup Switch を採用したが (図 4)，このよう

な機器は千差万別なので，スイッチの導入の際にはそれぞれのネットワークにおける要求事項を考慮してよく検討する必要があるだろう．

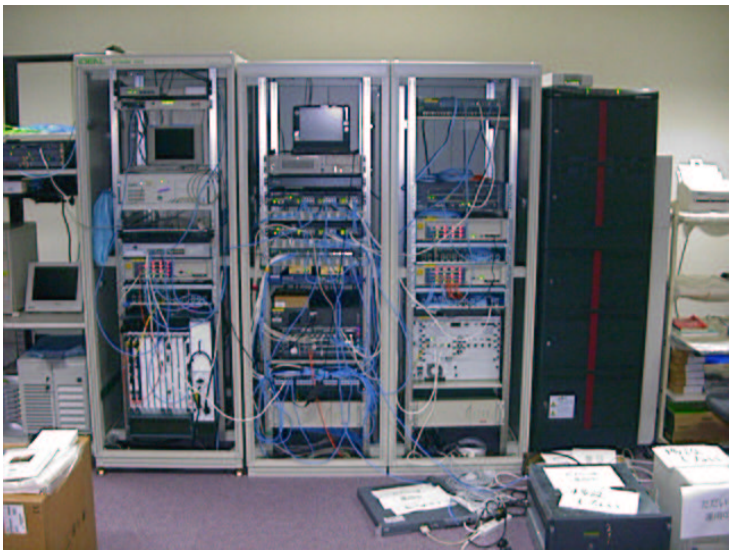

図 4: 構築中の館内ネットワーク (計算機室)

3. IP masqurade

前項で述べたように，館内ネットワークはグローバルサブネットとプライベートサブネットの間は IP masqurade なしに直接通信可能であるが (KUINS-II のグローバルと KUINS-III のプライベートの関係と同じである．なお，館内ネットワークで利用しているプライベートアドレスはメディアセンター内で閉じたものであり，経路情報の KUINS へのアナウンスは行っていない．)，プライベートサブネットと外部との通信のためには，IP masqurade を行う機器を経由することになる．

そもそも，プライベートネットワークから外部へのアクセスするには，IP masqurade 以外にもいくつかの方法が考えられるが，館内ネットワークでは，セキュリティ的に管理が面倒な IP masqurade でどこまでのことができるのかを実際に評価するという観点から IP masqurade を導入することとした．

館内ネットワークの構築当時，IP masqurade を行う機器についていくつか調べてみたが，グローバル側およびプライベート側の両方のインタフェースが 100BaseTX になっていて，かつ手頃な価格で入手可能なものはほとんどなかった．UNIX ベースで自作するのはメンテナンスコストの面から避けたかったので，Cisco 2621 (IP Plus Feature Set IOS) を調達することにした．

Cisco 2621 では，プライベートサブネット側の発信元サブネット毎に，異なるグローバル

アドレスを割り当てることができるので，プライベート側のサブネットごとに異なるグローバルアドレスを割り当てることにした．これによって，外部で観測した場合，どのサブネットからのアクセスであるかが容易に判断可能となる．また，この IOS では NetFlow と呼ばれる機能を利用して，通過した通信の記録を収集することが可能である．NetFlow を用いてプライベート側のインタフェースに対して情報を収集した場合，IP masqurade で処理される前の発信元アドレスと目的アドレスの組がポート情報とともに記録できることがわかったが，この機能を利用すれば，アクセスの追跡が必要となった場合にグローバル側のアドレスおよびポートとプライベート側のアドレスおよびポートの関連を把握することが可能となる．もちろん，記録は一定期間保存しておく必要がある．また，プライベート側のサブネットでは，ルータ (レイヤ 3 スイッチ) を定期的に SNMP でアクセスする等して IP アドレスと対応する MAC アドレスの組に関する記録を採っておけば，これだけの記録を突き合わせることで，IP masqurade を経由した通信であっても，通信を行った端末を特定することが可能となる．

Cisco における IP masqurade と NetFlow の設定例を以下に示す．

```
! グローバル側インタフェースの定義
interface FastEthernet0/0
 ip address 130.54.14.XXX 255.255.255.224
 no ip directed-broadcast
 ip nat outside

! プライベート側インタフェースの定義
interface FastEthernet0/1
 ip address 192.168.0.100 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 ip route-cache flow

! flow の情報をホスト 130.54.14.YYY のポート 9999 に送信する
ip flow-export version 6
ip flow-export destination 130.54.14.YYY 9999

! flow の情報を早めに送信するための設定
ip flow-cache timeout active 1

! サブネットごとに異なるグローバルアドレスを割り当てる
ip nat pool NAT11 130.54.14.AAA 130.54.14.AAA prefix-length 27
ip nat pool NAT12 130.54.14.BBB 130.54.14.BBB prefix-length 27
```

```
ip nat inside source list 11 pool NAT11 overload
ip nat inside source list 12 pool NAT12 overload

access-list 11 permit 192.168.11.0 0.0.0.255
access-list 12 permit 192.168.12.0 0.0.0.255

! Cisco 本体へのアクセス制限も忘れずに
access-list 99 permit 130.54.14.0 0.0.1.255

line vty 0 4
 access-class 99 in
```

flow の情報が取得できているかを Cisco 本体上で確認するには，show ip cache flow コマンドを利用する．また，情報は別のホストに送るように設定されているが，ホストでは NetFlow の情報を受信して解析・記録を行うソフトを動作させておく．Cisco のプロダクト以外にもフリーのものがいくつか公開されている．

`http://www.switch.ch/tf-tant/floma/software.html#netflow`

この中から例えば OSU flow-tools を利用すると，次のような情報が記録される．

```
srcIP            dstIP                  prot   srcPort   dstPort   octets   packets
192.168.11.8/17  150.100.3.5/0  (中略)  6      49682     80        2069     12
```

なお，Cisco 2621 の処理能力はあまり大きくはないので，通信トラフィックが増加して処理能力を越えてしまう場合は，上位クラスのハードウェアに交換する等の対策が必要になるであろう．

4. 遠隔講義ネットワーク

館内ネットワークは遠隔講義システムにも関わりがあるので，ここで少し触れておくことにする．

総合情報メディアセンターでは平成 10 年度に学内遠隔講義システムを導入し，学内 13 個所に学内サテライト講義室の整備を行っている．こういった遠隔講義環境をさらに充実させるため，総合情報メディアセンター新棟内の 2 階および 3 階に設置された全ての講義・演習室では遠隔講義が可能となっている．新棟内のそれぞれの講義・演習室は，地下の映像配信室とそれぞれ AV ケーブルで結ばれ，地下の映像配信室で AV スイッチに接続されている．さらに，この AV スイッチには，学内遠隔講義システムや SCS(スペースコラボレーションシステム) 等が接続されている．これにより，AV スイッチを任意に操作することによって様々な部屋およびシステムの組合わせで遠隔講義を行うことが可能となっている．また，各講義・演習室のミキサーは遠隔講義の際に遠隔からでも音声系の制御が可能なようにネットワークに接続されている．

映像配信室からは館内ネットワークや KUINS-II/ATM にアクセスすることができ，学内遠隔講義システムや UCLA との遠隔講義プロジェクトである TIDE プロジェクトで利用さ

れる MPEG2 コーデックが接続されている．このように，映像配信室には映像・音声信号をネットワーク上を流れるストリームに変換するためのコーデック装置が何台も設置され，遠隔講義のいわば中枢となっている (図 5)．

図 5: 映像配信室

5. 余談

毎年，自家用電気工作物保安規定に基づく定期点検が (卒論，修論等で利用率が高くなっている時期に) 実施され，点検の間は停電となる．このような定期点検は通例日曜日に行われるため，メディアセンター棟が停電する場合は，土曜日 (場合によっては金曜日) の夕方から月曜日の早朝までシステムを停止せざるを得ず，毎回皆様にご迷惑をお掛けしている．今年度より新棟を本拠地としてサービスを行うこととなったが，残念ながら電源二重化による無停電化はされていないため，例年通り停電にともなう数日にわたるサービス停止を避けることは難しい．これまでに引き続き利用者の皆様のご理解とご協力をお願いしたい．

停電と言えば，昨今の省電力化への配慮で，計算機室に設置された空調装置はガスを用いたものとなたのだが，残念ながら瞬間停電が発生した場合に自動復帰するようにはなっていない．幸運にも京都大学では雷雨の度に停電するようなひどい状況ではないが，それでも夜間や休日時の予期せぬ停電が懸念される．また，計算機室の床はフリーアクセスになってはいるが床下空調ではないため，サーバを搭載したラックの冷却効率もあまり良いとは言えない．新しい建物に計算機室を設置される場合は，このあたりについてもよく検討しておかれることをお勧めする．

6. おわりに

本稿では，総合情報メディアセンターの新棟に敷設されている 2 系統のネットワークのうち，新棟への移転の際に設計を行った館内ネットワークの概要について解説した．館内ネットワークでは VLAN の技術を多用し，グローバルアドレスとプライベートアドレスを使い分けているが，これはいわば KUINS-III の設計を先取りしたものと言えるだろう．プライベートへの移行することで安全性が向上するが，その代償としてある程度の利便性が損なわれることは仕方がない．メディアセンターでは，館内ネットワーク向けに独自に IP masqurade を運用し評価を行っているが，このような IP masqurade を全学規模で運用することは容易なことではない．安全性×利便性＝コスト」という式で表されるように，利便性を損なわずに安全性を向上させるためには，それなりのコストが必要となる．総合情報メディアセンターも KUINS の 1 ユーザとして，今後 KUINS-III を利用しながらセキュリティを確保しつつ利便性を向上できるような方法を検討していきたいと考えている．

KUINS 接続状況

学術情報ネットワーク機構

平成 13 年 7 月末現在の，KUINS-II/ATM への端末の接続状況をお知らせします．

吉田地区	13398(425) 端末
宇治地区	1909 (53) 端末
遠隔地 (全て)	821 (10) 端末
(合計)	16128 (488) 端末

( ) 内が IP over ATM での接続数です。

KUINS のネットワークの構成や運用について検討する際に接続申請の情報を参考にしています．従って，接続申請を行わずに端末を接続して，端末の利用に関しては不自由していなくても，部局，建物のネットワークを評価する対象となっていない場合があります．ネットワーク構成や運用について検討する際に不利益とならないよう，正しく接続申請を行っていただくようお願いします．

接続申請や申請様式の取得については次ページに示すメールアドレス，あるいは以下の URL をご参照下さい．

`http://www.kuins.kyoto-u.ac.jp/applications/`

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 (KUINS-III 関係も含む)
    q-a@kuins.kyoto-u.ac.jp
  - KUINS スタッフへの連絡先
    staff@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 に関する問い合わせ先
    atm-tech@kuins.kyoto-u.ac.jp
  - スパムメール不正中継対策に関する問い合わせ先
    spamfilt@kuins.kyoto-u.ac.jp
  - ネームサーバ管理者の連絡先
    ns-admin@kuins.kyoto-u.ac.jp
  - KUINS のネームサーバ管理者全体
    ns-assoc@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 への接続申請関連
  - KUINS-II/ATM へ端末を接続する申請の提出先
    ip-over-atm@kuins.kyoto-u.ac.jp
  - KUINS-II/ATM への端末の接続申請書のフォーマット請求先
    ipoa-request@kuins.kyoto-u.ac.jp
  - elan への端末の接続申請書の提出先
    elan@kuins.kyoto-u.ac.jp
  - elan への端末の接続申請書のフォーマット請求先
    ws-request@kuins.kyoto-u.ac.jp
  - ワークステーション接続届の提出先
    ws@kuins.kyoto-u.ac.jp
  - ワークステーション接続届のフォーマット請求先
    ws-request@kuins.kyoto-u.ac.jp
  - ワークステーション接続届に関する問い合わせ
    ws-trouble@kuins.kyoto-u.ac.jp
  - 新たなサブドメインの申請窓口 (アドレス変わりました)
    domain@kuins.kyoto-u.ac.jp
- User's Group
  - KUINS User's Group
    ug@kuins.kyoto-u.ac.jp
  - KUINS User's Group へ参加したい場合 (学内のみ)
    ug-request@kuins.kyoto-u.ac.jp
  - KUINS Appletalk User's Group
    appletalk@kuins.kyoto-u.ac.jp
  - KUINS Appletalk User's Group へ参加したい場合 (学内のみ)
    appletalk-request@kuins.kyoto-u.ac.jp

KUINS 会議日誌

平成 13 年 3 月 15 日～平成 13 年 8 月 5 日

学術情報システム整備委員会

平成 13 年 3 月 28 日　第 29 回)

- 京都大学情報基盤機構について

平成 13 年 7 月 17 日　第 30 回)

- ネットワーク機構の定員化について
- セキュリティ体制の確立について

学術情報システム整備委員会技術専門委員会

平成 13 年 7 月 27 日　第 51 回)

- KUINS-III の運用方針について
- その他

学術情報ネットワーク機構運営会議

平成 13 年 3 月 30 日

- 桂キャンパスにおける情報ネットワーク整備について
- 京都大学情報基盤機構について
- KUINS-III の進歩状況について
- 平成 13 年度ネットワーク機構運営経費要求について
- 一般に対する物理回線貸出の条件について

学術情報ネットワーク機構課長等連絡会議

平成 13 年 3 月 29 日

- ネットワーク機構運営会議について
- 平成 13 年度ネットワーク機構運営経費要求について
- 一般に対する物理回線貸出の条件について

KUINS ネットグループ連絡会議

平成 13 年 7 月 10 日　第 92 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 (報告)
- 汎用ドメイン名の契約について
- 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))