京都女子大学におけるネットワーク機器の更新 — 安全・快適なネットワークを目指して —

宮 下 健 輔[†1]

京都女子大学では学内ネットワークシステムを構成するサーバ群を2006年度に更新したのに続き，2007年8月にネットワーク機器群の更新も行なった．新しい学内ネットワークでは，幹線経路の広帯域化と耐故障性の向上，安全性の向上という3点を実現することで，より安全で快適な学内ネットワークを構築することを目標とした．

本稿では，このネットワーク機器群の更新について，それまでの経緯と新しい学内ネットワークの実現方法，機器更新後の経過などについて報告する．

Renewal of Network System in Kyoto Women's University — Toward a Secure and Agreeable Network —

KENSUKE MIYASHITA[†1]

In Kyoto Women's University, network equipment have been renewed in August 2007, and that follows renewal of servers in 2006. There are three goals in new network system. The bandwidth of main routes aims at being more wider, a better extent of fault-tolerance will be realized and the new network system is supposed to be more secure. Then, the new network system should be a secure and agreeable one.

In this paper, I report the circumstances about this renewal of network system, how to realize the new network system and the progress after renewal.

1. はじめに

京都女子大学では，2000年度から運用してきた学内ネットワークシステム（Kyoto Women's university Integrated Information Network System, 以下KWIINSという）のサーバ群を2006年4月に更新し[1),2)]，続いて2007年8月にネットワーク機器群を更新した．

これはKWIINSで運用中のネットワーク機器と現行製品との間の性能の差が著しくなってきたことや故障への不安が大きくなってきたことなど，機器の老朽化によって発生する問題に対応するためだけでなく，より安全・快適な学内ネットワークの構築・運用を目指して行なわれたものである．

具体的には，新しい学内ネットワーク（以下KWIINS 2.0という）の目標として掲げられたものは次の3点である．

- より広帯域な幹線経路をもつこと（1Gbpsから2Gbpsへ）
- より高い耐故障性を実現すること（基幹経路とL3スイッチの二重化）
- ユーザの利便性を考えつつ安全性の向上を実現すること（ネットワークアクセス制御と脅威検知装置の導入）

以下，ネットワーク更新までの経緯，KWIINS 2.0の特徴と実現方法，更新後の経過などについて具体的に記述する．

2. KWIINS

この節では，まずKWIINSについて説明する．

2.1 経緯と運用体制

KWIINSは2000年4月に運用を開始した．[3),4)] それまで京都女子大学には全学規模のネットワークがなく，図書館と一部の研究室のみがインターネットに接続されており，コンピュータ教室の端末も室内のネットワークにのみ接続されていた．

KWIINSは，同じく2000年度に発足した情報システムセンターという事務部署が管轄している．筆者はそのネットワーク運用責任者という立場にあり，他にネットワーク管理責任者（教員1名）がある．KWIINSは，情報システムセンターとネットワーク運用責

†1 京都女子大学現代社会学部
Faculty for the Contemporary Society, Kyoto Women's University

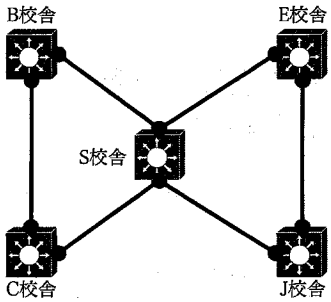

図 1　KWIINS の基幹経路

任者が日常の運用業務を行なうが，運用管理体制としてはネットワーク管理責任者が委員長を務める情報システム運営委員会がその責任を負う．

2.2　範囲と特徴

KWIINS の範囲は，学外との接続に用いているルータからサーバ群を経て各研究室や教室，事務室にある情報コンセントまでとしている．つまり，研究室内に教員が設置した装置や端末等は管轄外である．ただしコンピュータ教室[*1]は KWIINS と同じく情報システムセンターの管轄なので，コンピュータ教室内のネットワーク機器や端末等は KWIINS と同様に情報システムセンターが管理している．

KWIINS は主に次のような特徴をもつネットワークシステムである．

- 基幹 L3 スイッチの下流に建物ごとやフロアごとの L2 スイッチ群をもつ
- 基幹 L3 スイッチを結ぶ幹線は 1Gbps（光ファイバ），末端は 100Mbps（UTP）の帯域をもつ
- 学外（SINET および B フレッツ）とは光ファイバで接続し，それぞれ 100Mbps の帯域をもつ

基幹 L3 スイッチは 2000 年度当初は 3 台，その後 1 台ずつ時期をずらして 2 度増えており，B 校舎，C 校舎，E 校舎，J 校舎と S 校舎にそれぞれ設置されている．S 校舎に設置されたスイッチは Cisco 社 Catalyst 6506 であり，その他の校舎は同 4006 および 4506 と Allied Telesis 社 CentreCom 9812T である．基幹 L3 スイッチを結ぶ幹線経路は図 1 のように 2 つのループが S 校舎の L3 スイッチを共有している形状で，RIP による経路制御を行なっている．

3.　ネットワーク機器の更新

今回のネットワーク機器更新計画の概要は以下の通りである．

3.1　背　　景

KWIINS を構成するネットワーク機器の大半は 2000 年度に導入，運用が始まったものであり，その他は KWIINS 以前から運用されているものである．ただし基幹 L3 スイッチのうち 2000 年度に導入されたのは S 校舎のものだけであり，その他はそれ以前から導入されていたのでそれぞれ減価償却時期ごとに更新されている．

ネットワーク機器は本学では電話交換機などと同じ通信機器と見做され，通信機器の耐用年数は 7 年である．そのため，KWIINS を構成するネットワーク機器の大部分を 2007 年度に更新することとなった．

今回の更新は S 校舎の基幹 L3 スイッチと，S 校舎を含むほぼ全学の L2 スイッチが対象である．前述のように導入年度の違いから他の校舎の基幹 L3 スイッチは更新対象とならなかった．また，予算規模を縮小するために配線部材は更新せず，できるだけそのまま流用することとなった．

これらの制約を前提に新しい学内ネットワーク KWIINS 2.0 を構想し（4 節），更新計画を策定した．

3.2　計画策定と更新作業

KWIINS の運用方針は情報システム運営委員会にて決定される．今回の更新計画は，2006 年度当初より同委員会に筆者と情報システムセンターからという形で提案されていた．2006 年度後半にはネットワーク機器更新計画として予算申請を行なうことが同委員会で認められ，その後，理事会において 2007 年度予算として承認された．

2007 年に入ってからは詳細仕様書を作成するための機種選定が本格化し，4 月に詳細仕様書が完成した．引き続き 5 月から 6 月にかけてその仕様書が関係委員会の議を経て承認された．この詳細仕様書をもとに 6 月に業者説明会を開催し，今回の更新作業を請け負う業者が決定した．

更新の際は，一般の利用者が端末の設定等を変更する必要が極力生じないように，つまり KWIINS から KWIINS 2.0 への更新を利用者があまり意識することのないようにした．これは大部分で成功したが，4.4 節で述べるように一部の校舎ではやむを得ず利用者に設定変更を依頼することとなった．

実際の更新作業は 8 月 13 日（月）から 17 日（金）までの間に行なわれた．これは，この週は学内ほぼすべての部署が夏期休業中であり，KWIINS を長期間停止するのに好都合だったためである．作業時間は原則として午前 9 時から午後 5 時までとしたが，それ以降も作業を続けている日が多かった．また，この期間中，S 校舎の L3 スイッチを更新する間だけ学内外の通信が途絶した．これは 8 月 13 日の日中，数時間に及んだが，その後は学外との通信を途絶することなく各校舎ごとに更新作業を行なった．

*1 Windows PC が約 60 台ずつ設置された教室が 9 室，Power Mac G5 が 60 台設置された教室が 1 室ある．

4. KWIINS 2.0

前述のようにKWIINS 2.0の目標は次の3点とした.

- より広帯域な幹線経路をもつこと（1Gbpsから2Gbpsへ）
- より高い耐故障性を実現すること（基幹経路とL3スイッチの二重化）
- ユーザの利便性を考えつつ安全性の向上を実現すること（ネットワークアクセス制御と脅威検知装置の導入）

以下，それぞれの背景と実現方法，発生した問題点などについて述べる.

4.1 幹線経路の広帯域化

前述のようにKWIINSにはB, C, E, J, S各校舎を図1のようなループ状に接続した幹線経路があり，これは光ファイバを用いて1000BASE-SXまたは1000BASE-LXで接続されていた.

学外との接続はS校舎のL3スイッチを介して行なわれ，サーバ群もS校舎に存在する．また，コンピュータ教室はC, J, S各校舎にそれぞれ2教室，2教室，6教室ある．そのため，幹線経路のうち特にC, J校舎とS校舎との間のトラヒックが大きく，また今後も減少することはないと考えられた.

これらのことから，幹線経路の広帯域化を目標に掲げた．しかし，各校舎間の光ファイバを増やすことは電柱への架線状況や予算に鑑みて困難であった.

そこで幹線には波長分割多重方式（Wavelength Division Multiplex，以下WDMという）を採用することとした．WDMであれば既設の光ファイバには手を加えることなく，両端にWDM装置（波長変換システムおよびWDMフィルタ）を設置するだけで広帯域化が可能となる．また，既存のL3スイッチはWDM装置を介して幹線経路に接続すればよく，スイッチ自体には何ら変更を加える必要がないことも好都合である.

WDMで分割，多重化する波は4波とした．それぞれの波を送受信するスイッチには変更がない（S校舎を除く）ので1波あたりの帯域は1Gbpsのままであり，合計で1芯に4Gbpsの帯域を割り当てることとなる．このことにより，幹線経路の帯域はこれまでの1Gbps（全二重）から2Gbps（全二重）に倍増することとなった．今回，WDM装置はNTTエレクトロニクス製のプラスレピータとCWDM 4波フィルタを採用した.

4.2 耐故障性の向上

KWIINSでは幹線経路の断線によってネットワークが停止したことはなく，基幹L3スイッチの故障による停止も運用中の7年間に一度しかなかったが，ネットワーク設計段階でそのような故障に対応できるような工夫を行なうことは一般的である．KWIINS 2.0ではネットワークの耐故障性をより向上させるためにS校舎の基幹L3スイッチを二重化し，それにともなって幹線経路の形状を変更しすべて二重化した.

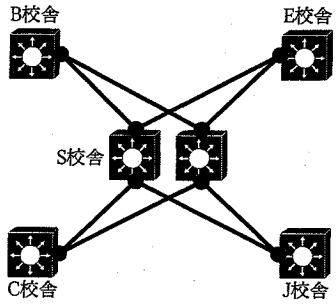

図2 KWIINS 2.0の基幹経路

まずS校舎に設置された基幹L3スイッチの二重化は，予算申請段階の仕様では1つの機器の中でスイッチングモジュールを二重化する方法と機器そのものを2台用意する方法の2種類を併記した．金額は前者の方が安価となるが，耐故障性は後者の方が向上する．結局，予算が許したので後者の方式を採用した．実際にはCisco社Catalyst 6504-Eの2台構成とし，VRRP[5]によって運用することとした.

次に幹線経路の形状は，KWIINSでのループ状からS校舎の基幹L3スイッチを中心としたスター型に変更した（図2）．これはS校舎のL3スイッチが学内のサーバセグメントや学外との通信の要となることから，これを中心としてB校舎，C校舎，E校舎，J校舎をスター状に配置したものである．このとき上述したようにスター型ネットワークの中心が二重化されているので，配線もすべて二重化されることとなる.

この変更によって幹線経路の形状は図1から図2のように変更されることとなる．これは光ファイバを増やすか架け替えるかしなければ実現できないように思えるが，既設光ファイバに空き芯があったことと，各校舎の地理的関係により図1の経路のうちB校舎とC校舎を結ぶもの以外はすべてS校舎の近辺を通過しており，しかもそこでいちど成端されていることから，簡単な工事で図2への形状変更が可能であった.

ネットワーク更新工事の期間中，この幹線経路の運用試験を行なった．これは，S校舎の基幹L3スイッチの更新と幹線経路のWDM化が完了した時点で行ない，二重化したL3スイッチの片方を停止する試験と幹線経路を切断する試験を行なった．その際，停止したスイッチや切断された経路から正常なスイッチ，経路への切替えが瞬時に行なわれることが確認できた.

4.3 安全性の向上

安全性を向上するための方策として，ネットワーク利用時の認証とコンピュータウイルス等の拡散防止の2点を掲げた.

4.3.1 利用者認証

KWIINS では，利用者がネットワークに機器を接続するとき，その機器が静的 IP アドレスをもつ予定なら機器接続申請を，また動的 IP アドレスでよいなら DHCP 利用申請を行なう必要がある．これは必要事項を紙に記入して情報システムセンターに提出するものであり，正式には情報システム運営委員会の議を経て承認の可否が決まるが，実際には情報システム運営委員会の常任委員会において異議がなければ承認される[*1]．これらの申請は KWIINS 上にアカウントがあれば誰でも可能である．

DHCP 利用の場合は MAC アドレスを申請し，ネットワーク接続時に DHCP サーバにて認証を行なうが，機器接続申請の場合は IP アドレス等のネットワーク情報を申請者に提供するのみでその後の接続は検証していない．すなわち DHCP 利用申請の場合は接続時にその機器（厳密にはネットワークインタフェース）を認証しているが，機器接続申請の場合はなんら認証せずに接続を許していたことになる．

この方式では，どの利用者がいつどのように KWIINS に接続したのかを管理者が把握することが困難である．また申請を紙で行なう必要があり，その承認に日数がかかることから利用者にも不便であると思われる．

そこで，KWIINS 2.0 では紙での申請を原則廃止し，その代わり原則としてすべての機器で接続ごとに利用者認証を行なうことで接続の安全性を高めることとした．ただし，利用者認証を行なうことが不可能な機器（PDA やネットワークプリンタ等）は，従来通り紙による申請を必要とする．

利用者認証は KWIINS 2.0 の末端に配置された L2 スイッチ（エッジスイッチ）で接続のたびに行なう．このときの手段としては IEEE 802.1X を採用することも検討したが，対応する OS が限られることや利用者の教育や通達の煩雑さに鑑みて断念し，利用者の利便性を考えて WWW ブラウザを用いたものとした．これによりネットワーク接続時に利用者を特定することが可能となる．

これらの認証は Apresia 社の L2 スイッチ（2124GT-SS2 など）の NA (Network Authentication) 機能により実現する．今回の更新では同社の L2 スイッチをエッジスイッチとして 80 台弱導入した．このスイッチであれば，利用者認証の他に MAC アドレスによる認証もサポートされており，WWW ブラウザをもたないデバイス等には従来同様 MAC アドレスによる機器認証が可能である．また，エッジスイッチの下流に利用者がハブやスイッチを設置していた場合には，エッジスイッチの 1 つのポートに対して複数の機器からのトラヒックが流れることになるが，上記のスイッチであればその際にもそれぞれの機器に対して別々に利用者認証および MAC アドレス認証を行なうことが可能である．

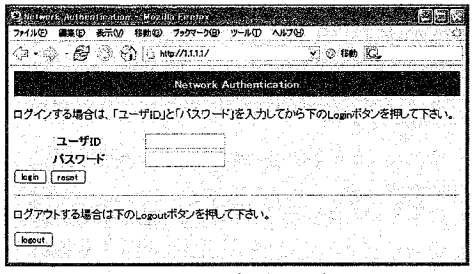

図 3 利用者認証ページ

利用者の機器に表示される認証ページを図 3 に示す．予め周知された特定の URL へ利用者がアクセスすると，図 3 のような利用者認証ページが表示されるので，利用者はここでユーザ名とパスワードを入力する．入力されたデータは Radius サーバにて認証され，ユーザ名とパスワードが正しい組合わせであれば，その機器が接続されたスイッチのポートが利用可能となる．Radius サーバは KWIINS でも利用されていたものを流用した．

このスイッチでは，ネットワークの利用終了を検出するために種々の方法が利用できる．例えば利用時間を予め設定しておくことや ICMP による到達性の監視などである．本稿執筆時点では，接続された機器の無通信時間が予め定めた時間を超えた時点を利用終了と見做して切断する方式を採用している．

この利用者認証をネットワーク更新直後から有効にすることは利用者の混乱を招き，また上述の申請制度を定めている学内ネットワーク運用規則との齟齬も生じる．

そのため，利用者認証は KWIINS 2.0 運用開始後に相当の周知期間を経て導入することとした．これは，大きな変更を複数同時に実施せず段階的に行なうことで，検証を容易にしかし確実に行なうことができるという点からも有効であると考える．

4.3.2 ウイルス等の拡散防止

学内でのコンピュータウイルスやワームの活動を防止するため，KWIINS ではサーバセグメント以外から送信された ICMP echo パケットがセグメントを越えることを禁止し，ウイルスやワームがよく利用するポート番号（137 や 445 など）についても同様にセグメントを越えて通信できないようにしていた．これらは S 校舎 L3 スイッチ（Catalyst 6506）上で access list を記述することで実現していた．

この対策によりウイルスやワームがセグメントを越えて活動することは防げるが，セグメント内での活動は防止できない．また，別セグメントにある機器の

---

*1 常任委員会による決定は，後日，委員長より本委員会に報告される．

ICMP による死活監視や，コンピュータ教室での ping コマンドの実習や経路探索実習[*1]などが不可能になるという弊害があった．

KWIINS 2.0 では，ウイルスやワームなどの振る舞いを検知してこれを管理者に報告し，さらにネットワークから隔離する機能を持つ機器を導入することによって上記の対策を廃止することとした．これにより上述したような問題によってユーザの利便性を損なうことなく，安全性の向上が実現できる．

これは Mirage Networks 社の Mirage CounterPoint という機器を導入することで実現した．CounterPoint は，接続された（複数の）VLAN 上に未使用 IP アドレスを利用した囮ホストを生成し，これらへのポートスキャンや大量の ICMP echo パケットの送信等，ウイルスやワーム，不正利用者などの振る舞いを監視する装置である．そのような振る舞いが観測されたとき，CounterPoint はそのことを管理者に通知するとともに予め定められた対応（例えば当該機器のネットワークからの隔離）を行なう．CounterPoint は 1 台で複数の VLAN を監視でき，KWIINS 2.0 では学内ほぼすべてのセグメントを監視対象とするためにこれを複数台導入することとした．

この CounterPoint の導入によって，KWIINS で行なわれていた通信制限を撤廃できることとなり，これは利用者の利便性を向上することに通じる．また，従来は不可能だったセグメント内でのウイルスやワームの活動の検知・防止や，不正利用者の発見・隔離が可能となり，これらはネットワークの安全性向上につながる．以上のことから，KWIINS 2.0 では KWIINS よりも安全・快適にネットワークを利用することが可能になると期待できる．

4.4 アドレス変更

前述の通り，今回の更新では利用者にはなるべく更新を意識させない，つまり端末の設定変更などを伴わない方法で更新を行なう方針であった．しかし以下で述べる 3 校舎だけはアドレス体系の見直しを行なうこととした．

KWIINS では，B 校舎は建物全体で 1 セグメント（ネットマスク 24bit，以下同様）としていたが，接続端末数が既に 200 近くに達していたため，KWIINS 2.0 ではこれを各階ごとのセグメントに分けることとした．また逆に E 校舎の 4，5 階と J 校舎では各階ごとに 1 セグメントを割り当てていたが，接続端末数が少なく今後大幅に増加する見込みもないことから，前者では 2 階まとめて 1 セグメント，後者では建物全体で 1 セグメントとした．この E 校舎と J 校舎のセグメント縮小は，主に前述の CounterPoint で監視するセグメント数を減少させる（すなわち CounterPoint の導入台数を減らす）目的で行なわれたものである．

これら 3 つの校舎では，セグメント変更に際してネットワークアドレスもすべて KWIINS のものから変更し，更新前後では端末の IP アドレスやデフォルトゲートウェイなどを変更することとした．これは一部だけは KWIINS と同じアドレスを利用するようにすることも可能であり，また前述した更新のポリシー（更新を利用者が意識することのないようにする）と矛盾するが，すべて変更した方が利用者への説明がしやすいことからそのように設定した．

このアドレス変更と同時に，これらの校舎では利用者認証をネットワーク更新直後から有効にすることとした．これは，利用者にアドレス変更の必要性を認識させる（KWIINS のときと同じネットワーク設定の端末が KWIINS 2.0 に接続されるのを防ぐ）ためであるのと同時に，利用者認証の先行実験を行なうためである．

これらの校舎ではアドレス変更の経緯や端末の設定変更方法，利用者認証の方法などを記した案内を配布した．

5. 更新作業後の状況

ネットワーク更新作業が終了した翌週（8 月 20 日）から次々と各部署の夏期休業が明け，また教員が出勤したり学生が登校したりして，一般の利用者が KWIINS 2.0 を利用し始めた．

前述のアドレス変更を行なった校舎にある研究室や事務室からは多くの問い合わせや苦情が寄せられたが，それ以外は全体として特に大きな問題もなく KWIINS 2.0 の運用を開始できた．

5.1 運用規則の改正

前述（4.3.1 節）の通り，KWIINS 2.0 で導入する利用者認証方式は KWIINS での申請制度を原則不要とするものであり，この申請制度を定めているネットワーク運用規則を改正してから運用しなければならない[*2]．本稿執筆時点では，この規則改正のための議論を行なっているところである．

規則改正の方針は以下の通りである．

(1) ネットワーク接続時に WWW による利用者認証を行ない，動的 IP アドレスを利用する機器については申請することなく KWIINS 2.0 に接続できる
(2) WWW による利用者認証が不能な機器は MAC アドレスを申請する必要がある
(3) 静的 IP アドレスを利用する機器は機器接続申請が必要である

まず (1) では接続のたびに利用者認証が行なわれるので，その都度利用者を特定することができ，その接

*1 Windows 上の tracert コマンドは ICMP パケットを利用している．

*2 4.4 節で述べた校舎については，情報システム運営委員会で「例外」として先に認められていた．

続に対する責任は利用者が負うことをはっきりさせることが可能になる．また (2) では接続のたびに MAC アドレスを認証することとなり，これは利用者ではなく機器（厳密にはネットワークインタフェース）を認証することになるので，接続に対する責任は MAC アドレスを申請した者が負うこととなる．最後の (3) では従来通り何ら認証を行なわないので，管理者が割り振った IP アドレスによってなされた通信はすべて機器接続申請を行なった者が責任を負うこととなる．ネットワーク利用の責任をより明確にするという方針とともに，以上の事柄を利用者に浸透させる必要があると考えている．

規則改正には理事会による承認と毎月発行の学園報による公布が必要であるため，本稿執筆時点では，2007 年 12 月中に規則改正を行ない，本年末に利用者認証を有効にする予定である．それまでの期間は，前述した B 校舎，E 校舎，J 校舎を利用してログや問い合わせ事例を収集し，本格運用に役立てたいと考えている．

6. おわりに

本稿では京都女子大学における学内ネットワークの更新について，その経緯と新しい学内ネットワークでの目標や実現方法，ネットワーク更新後の状況などについて報告した．前述のように，本稿執筆時点ではネットワーク更新からまだ日も浅く今回の更新についての問題点がすべて表出していないと思われる．今後，相当期間の運用を経た後にもう一度今回のネットワーク更新についてまとめと考察を行なう必要があると考える．

本稿がこれからネットワークを更新しようと考える機関において何らかの参考になれば，筆者の喜びとするところである．

参考文献

1) 宮下健輔，水野義之：京都女子大学における情報機器更新計画，情報処理学会研究報告，No.DSM-39, pp.25–30 (2005).
2) 宮下健輔：Mac OS X Server を利用した Windows ドメイン運用，信学技報，No.TM2006-2, pp.7–12 (2006).
3) 宮下健輔：京都女子大学ネットワーク構築記，*UNIX MAGAZINE*, Vol.15, No.10, pp.104–118 (2000).
4) 水野義之，宮下健輔：京都女子大学における情報教育環境の構築と運用，SSS2002 情報教育シンポジウム論文集，IPSJ Symposium Series, No.12, pp.151–154 (2002).
5) Hinden, R.: *Virtual Router Redundancy Protocol (VRRP)*, RFC3768 (2004).