4. 無線LANによる移動体通信の事例

1 モバイルIPを用いた安全なキャンパスワイド無線LANインフラ構築事例

Case Study of Secure Mobile Campus Network using Mobile IP Technology

岡村 耕二
九州大学情報基盤センター
oka@ec.kyushu-u.ac.jp

九州大学では，2003年にモバイルIPを用いた無線LANインフラを全学的に整備した．無線LANは一般に便利である反面，単純なブリッジとして利用する際，その設定が不十分であるとセキュリティホールになりやすいという欠点がある．それに対して，九州大学では認証機能が強化されたモバイルIPを利用することで，無線LANをキャンパスネットワークの一部として安全に運用している．本稿では九州大学に導入したキャンパスワイドのモバイルIPによる無線 LANインフラの構築方法を紹介し，導入の際の問題点などを考察する．

モバイルIP導入の背景

近年，大学において，セキュリティに関する政策の検討が研究者からボトムアップではなく，大学の上層部からトップダウンに進められるようになってきた．特に，2001年には文科省から全国の大学に対して，それぞれ各大学固有のセキュリティポリシーの策定を求める勧告があったのは記憶に新しいことであると思う．一方で，無線LANの普及もこの時期非常に盛んであり，無線LAN用のブリッジ製品も低価格化が進んでいたことから，大学としてではなく，研究室あるいは個人ベースでの導入が多数行われていた．

無線LANはいうまでもなく非常に便利である反面，特にブリッジ接続として利用する際に設定方法を誤るとセキュリティ的な問題が多く，本学でセキュリティポリシーの策定が全学的に行われていたのとは裏腹に，無線LANに関するトラブルが多数発生していた．しかし，教育的な観点から見るとe-Learningを始めとして，いわゆる教育のIT化が加速していたのもこの時期で，従来は卒業研究に着手する前の学生が情報処理演習といった講義以外でパーソナルコンピュータを利用する機会は多いとはいえなかったのが，この時期くらいから急速に一般学生からの個人のパーソナルコンピュータをキャンパスで利用したいという需要が増え出した．もちろん，その需要とは，キャンパスネットワークに接続して，インターネットにアクセスしたいというものである．

本学では，九州大学が利用できるクラスBのグローバルアドレスは，サブネット化して各部局に配布し，その利用と責任は部局に一任している．そのため，通常はこれらの卒業研究にまだ着手していない一般学生は，たとえ自分が所属している部局であったとしても，その部局が管理しているIPアドレスを利用するのは困難な状況であった．そこで，結局，便利な無線LANを利用した，全学的なアクセス網を整備して欲しいという要望は自然と情報基盤センターに寄せられてきた．

このような状況で，無線LANを利用した，全学的なアクセス網の構築には，セキュリティ対策は不可欠であった．さらに，情報基盤センターは前述した全学的なセキュリティポリシー策定の責任部局であったため，なおさらである．そこで，本学ではセキュリティ機能が強力である，モバイルIPシステムを導入することとした．モバイルIPシステムは，その接続の際に強力な認証処理が入るので，無線LANの利用を九州大学の構成員だけに限定できることと，各利用者には固有のIPアドレスを割り当てられるので，キャンパスワイドなハンドオーバーといった，ネットワークの新しい利用が期待できる．たとえば，ある場所で遠隔にある他の端末に接続して，そのセッションを保持したままキャンパスを移動できるので，利用者が移動しながら，VoIP (Voice over IP) によるインターネット電話などのマルチメディア通信を行ったり，UNIXなどのマルチユーザタイプの計算機を遠隔に利用したりすることを強力に支援することが期待できる．

システム設計

モバイルIPを全学的に導入するためにはいくつかの方法が考えられる．たとえば，フリーソフトウェアのモバイルIPのスタックなどを利用したり，モバイルIPシステムを一式で購入するなどである．本学での導入は，

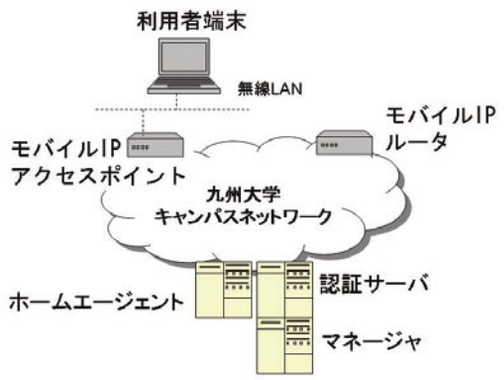

図-1　SISシステムの基本構成

全学的なサービスが目的であったため，メーカサポートが期待できる後者を採用することとした．製品としては，ルート株式会社からSIS（Secure IP Solution）システムを購入し，これを利用することにした．しかし，製品を購入しても，実際に利用するためにはカスタマイズが必要である．また，カスタマイズといっても，それはシステムのほとんどの部分を占めるので，結局，システムの設計と同じである．本章では，そのシステム設計について説明する．

SISシステムの基本構成

SISシステムの基本構成を図-1 に示す．システムの構成要素として，サーバ系に「ホームエージェント」，「認証サーバ」，「マネージャ」があり，アクセス系としてモバイルIPアクセスポイントがある．動作の概要は以下の通りである．

(0) 利用端末には固有の ホームIPアドレスが静的に付与されている．
(1) 利用端末がモバイルIPアクセスポイントに近付きアソシエイトすると，モバイルIPアクセスポイントが管理する気付アドレスが動的に付与され，通信が可能となる．
(2) 利用端末は認証サーバとやりとりをし，認証に成功すれば正式にインターネットに接続される．
(3) 利用者端末から出力されるパケットは，そのままインターネットに送信される．
(4) インターネットから届くホームIPアドレス宛のパケットは，ホームエージェントがモバイルIPアクセスポイントと経路制御を行い，指定されたホームIPアドレスが付与されている利用者端末に配送される．

なお，上記の説明では触れなかったマネージャは，各利用者端末がどのモバイルIPアクセスポイントに現在接続されているかといった九州大学キャンパスネットワーク内での地理情報やログ情報などの管理をしている．

ホームIPアドレスの割り当て

SISシステムを本学に導入するにあたり，まず，検討する必要があったのは，ホームIPアドレスの割り当てについてである．現在の九州大学の教員，学生，事務その他を含めた全構成員の数は約20,000人である．一方，モバイルIPを使うメリットの1つとして，各利用者端末に固定的なIPアドレスを割り当てることができることがあるので，できれば，グローバルIPアドレスを割り当てたいという希望があった．しかし，九州大学では，現在すでに保有しているクラスBアドレスのうち70 % 以上を利用しており，残念ながら20,000個というアドレスを捻出することは困難であった．また，卒業あるいは修了する学生が本当に卒業，修了することが確定するのは5月以降であり，毎年1学年分のデータが余計に重複する時期が必ず年度始めにあり，実際はその時期に 20,000個以上のアドレスが必要になるため，現在では割り当て済みのアドレスを整理したとしてもやはり固有の固定グローバルアドレスをホームアドレスに利用するのは困難であった．

そこで，九州大学では，ホームアドレスとして，プライベートアドレスを使用することにした．しかし，プライベートアドレスを九州大学の現在のキャンパスネットワーク上で実現するのにはいくつかの問題があった．

利用者端末，モバイルIPアクセスポイントおよびホームエージェントは，これらの機器で九州大学キャンパスネットワーク内にプライベートアドレスネットワークを構成するため，既設の九州大学のキャンパスネットワークとは少なくとも論理的に分離できれば，プライベートネットワークとキャンパスネットワークの接点が1つになるので，外部ネットワークとのアクセスに必要になるプライベートアドレスとグローバルアドレスの変化を行うNAT（Network Address Translate）装置の設置が容易になるはずであった．しかし，モバイルIPアクセスポイントは，全学の各部局の協力によって，大学の各所に設置してあるため，必ずしも，既設のセグメントとモバイルIPのセグメントを論理的に分離できるVLAN（Virtual LAN）の利用できるスイッチングハブに接続できるとは限らなかった．むしろ，ほとんどのケースでは，モバイルIPアクセスポイントが直接接続されているスイッチングハブにはVLANの機能が備わっていなかった．そのため，モバイルIPアクセスポイントは，キャンパスネットワークに対して九州大学のグローバルアドレスで接続し，気付アドレスおよび，ホームアドレスのみプライベートアドレスを使用するという構成をとることにした．ちなみに，将来SISがIPv6に対応し，また，九州大学のキャンパス内ネットワークもIPv6に対応すれば，いずれは，グローバルなIPアドレスをホームアドレスとして利用したいと考えている．

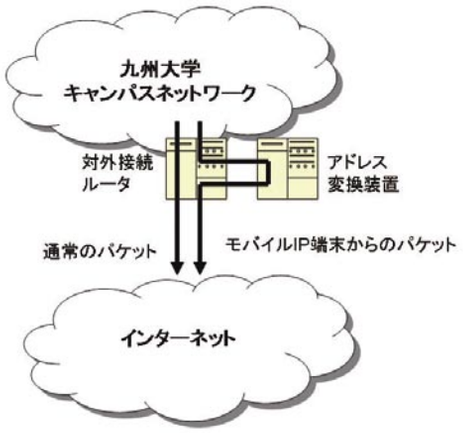

図-2　対外接続部の構成

対外接続部分の経路制御

このような構成では，モバイルIP端末からのソースアドレスとして各利用者のホームIPアドレスがついたパケットと，ソースアドレスとして九州大学のIPアドレスがついたパケットがキャンパスネットワークのネットワーク層で混在するようになった．つまり，既設のキャンパスネットワーク内において，モバイルIPのホームIPアドレスであるプライベートアドレスの経路制御を行うことにした．九州大学で現在対外接続で用いているルータ装置にはNATの機能はないので，プライベートアドレスを用いているモバイルIP端末が，九州大学外部と通信するためには別途アドレス変換が必要となった．しかも，その装置は図-2 のように対外接続ルータに外づけのように接続させる必要があった．つまり，対外接続ルータは，ソースルーティングを行い，ソースアドレスがモバイルIPのホームアドレスであれば，アドレス変換装置に経路制御を行い，アドレス変換装置にてソースアドレスをそのアドレス変換装置のグローバルアドレスに置き換えてインターネットへパケットを送出するようにした．

このようなシステム構成で，九州大学内で安全な無線LANによるモバイルIPの利用が可能になった．

モバイルIPシステムの導入

本章では，実際にシステムを導入し，運用を始めて発生したさまざまな問題点を挙げ，それらについて考察する．

キャンパスへのモバイルIPアクセスポイントの設置

モバイルIPアクセスポイントは九州大学全体で，現在約240台設置されている．九州大学は，箱崎キャンパスを中心に，病院キャンパス，筑紫キャンパス，六本松キャンパス，大橋キャンパスというサテライトキャンパスで構成されているが，それぞれのキャンパスでモバイルIPの利用が可能になっている．詳細な設置情報を紹介することは，本学のセキュリティ上好ましくないため，大雑把な紹介にとどめる．事務局，食堂，課外活動共同施設，いくつかの講義室，図書館，など従来キャンパスネットワークの利用が困難であった個所を中心にモバイルIPアクセスポイントを設置している．特に食堂への設置は，まだ，特定の研究室に所属しない学部学生，文系の学生をターゲットにしている．しかし，基本的には設置する部局の協力ならびに要望に基づいて設置しているので，従来，まったく，学内ネットワークがなかった個所への設置は行っていない．基本的に，近郊に既設の有線の学内ネットワークの機器があり，そこからケーブルが伸ばせる範囲でモバイルIPアクセスポイントを設置している．

屋内に設置できるものは図-3のようなタイプの機器を設置し，また，屋外に設置したものは図-4のような，雨などを防げるハウジングで覆われたタイプのものを設置した．

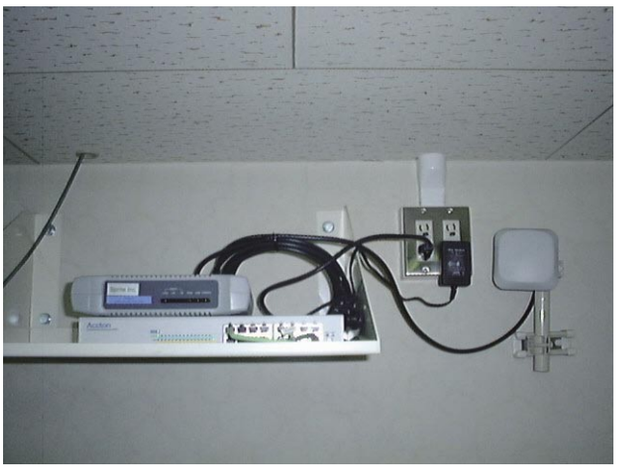

図-3　屋内用 モバイルIPアクセスポイント

図-4　屋外用 モバイルIPアクセスポイント

ID管理

SISシステムの特徴の1つである，認証のためには，利用者 のID管理を行う必要がある．ID管理で特に重要なのは，IDの利用者への配布である．いわゆる商用サー

ビスと異なり，大学でのサービスは，利用者が必要であるという意思表示に無関係に全構成員のIDの作成ならびに配布する準備をする必要がある．これに対して，学生は，4月入学だけではなく9月入学などもあるし，教員ならびに職員は毎月任意に人事異動があるので，九州大学の最新の構成員情報とモバイルIPのID情報を常に同期させることは非常に困難である．

また，現在，九州大学には全構成員に対する汎用的なID管理システムは存在しないので，学生のIDは，情報基盤センターの教育用システムのIDと連動，教員，職員は，部局単位にID管理係を決めて，部局単位でとりまとめの協力をお願いしている．将来的には九州大学にも，全学的なID管理システムのようなものができあがる予定になっているので，それと連携できれば，教員，職員のID管理のオーバーヘッドも減ることが期待できる．なお，教育用システムのIDとの連動については，頻繁に変更されることが期待されている教育用システムパスワードの性質と，あくまで利用者の認証のための目的であるモバイルIPシステムのパスワードの性質は異なるので，教育用システムのIDそのものをモバイルIPで利用しているわけではない．

導入時あるいは導入後に発生した問題とそれに対する考察

本システムは，情報基盤センターが中心になって導入を進めてきたが，実際の運用を開始する時は，全学的な意見を聞く機会があった．運用をする側としては，安全で便利なインフラが整備されるので，あまり否定的な意見がでることは予想していなかったが，それでも次のような意見が学内から出てきた．ただし，中にはシステムの構成の誤解からくるものもあった．

モバイルIPアクセスポイントの設置と部局のポリシー

モバイルIPアクセスポイントの学内キャンパスネットワーク側のインタフェースには，どうしても，そのアクセスポイントが設置される部局のグローバルアドレスを付与する必要がある．これは前述したように，キャンパスネットワークの末端のスイッチはVLANに対応していないものが多いため，避けることはできなかった．もちろん，同一データリンクセグメントに複数の異なるネットワークを利用することは可能であるので，キャンパスネットワークのルータにもプライベートアドレスを付与すれば，モバイルIPアクセスポイントのすべてインタフェースにプライベートアドレスを付与して運用することは可能である．しかし，これはさすがに運用管理のオーバーヘッドが大き過ぎるので，モバイルIPアクセスポイントにはそのアクセスポイントを設置する部局からアドレスを割り当ててもらいそのアドレスを用いてキャンパスネットワークと接続している．そのため，そのモバイルIPアクセスポイントに，アソシエイトした利用者端末にはその部局のセグメントのIPアドレスがついてしまうと誤解されがちであった．部局のネットワーク担当者の立場からすれば，たとえ，九州大学の構成員であってもその部局のポリシーを知らない利用者によるネットワーク上のトラブルが自分の部局のアドレスで起こされるのはたまらない，という意見であり，それはもっともである．しかし，実際は，先述した通り，どこのモバイルIPアクセスポイントにアソシエイトしても，利用者の端末から発せられるパケットのソースアドレスは，その利用者端末固有のホームIPアドレスとなる．また，そのパケットが学外に出ている時は，そのソースアドレスは，情報基盤センターに設置されたアドレス変換装置のグローバルアドレスに置き換えられるが，そのアドレスは情報基盤センターで管理されているものなので，もしも，モバイルIP利用者がインターネット上でトラブルを起こしたとしても，そのコンタクトは情報基盤センターになる．なお，学内の機器にアクセスする場合は，アドレス変換装置を経由しないので，ソースアドレスは，各利用者に割り当てられたホームIPアドレスのままとなる．そのため，利用者が学内のどこからアクセスしようと，ホームIPアドレスからその利用者を特定できる反面，ソースアドレスがプライベートアドレスであるので，九州大学のクラスBアドレスでアクセス制限を行っているWebサービスのアクセスが拒否されるといった問題が発生した．いずれにしてもこの問題は，本質的にはホームIPアドレスとして，九州大学の持つグローバルIPアドレスが利用できなかったところにある．

いつでもどこでもインターネットが使えることは…

無線LANで，モバイルIPを全学的に利用可能にすることによって，九州大学の各キャンパスでいつでもインターネットの利用が可能になった．また，キャンパスによっては従来インターネットの利用できない講義室でもインターネットアクセスが常時可能となった．しかし，この状況に対して，ある講義担当の先生からは，「講義中に学生がコンピュータでインターネットを閲覧できるのは学生が講義に集中できなくなるので困る」という意見をいただいてしまった．「正規の講義中はモバイルIPの利用を停止してもらえないか」というものである．また，ある部局からは，「モバイルIPアクセスポイントの電波が届けば，パソコンが使えてしまうので，夜中など建物のまわりでパソコンを使う学生が増えてしまいそうなので，夜中はモバイルIPの運用を停止して欲しい」と

いう意見をいただいた．いずれの意見に対しても，モバイルIPシステムは，キャンパスネットワークと同様に九州大学の全学的なネットワークインフラなので，間欠的なサービスはしたくないと情報基盤センターからは回答したが，モバイルIPアクセスポイントの設置は各部局内にしているので，もしも，部局の方で，電源などを抜いたり，ブレーカーを落としたりされるとこちらは，モバイルIPアクセスポイントの停止は検知できるものの，その復旧までは困難である．なお，SISシステムではシステムスケジュールで，特定のモバイルIPアクセスポイント群のサービス提供の時間的なスケジューリングは可能なので，このような部局からの要望に対応することは可能であった．しかし，情報基盤センターのモバイルIP運用のポリシーとして現状では，常時サービスを提供することにして，このようなネットワークインフラの整備と倫理面から見たパソコン利用の制限とのトレードオフはより高いレイヤで解決を図ることとした．しかし，逆に，情報基盤センターによる整備が不十分であった部局からは自前でモバイルIPアクセスポイントを購入して整備したいという申し入れもあり，それによってモバイルIPアクセスポイントの数が増えた部局もあった．

モバイルIPアドレスとしてグローバルアドレスを利用する

筆者のユーザとしての個人的な感想は，筆者の職場である情報基盤センターにはモバイルIPアクセスポイントが潤沢に設置されていることもあり，職場で利用する分には満足している．しかし，残念ながら筆者がよくでかけるキャンパス内のある建物にはモバイルIPアクセスポイントはまったく設置されていないので，実はその恩恵をあまり得ていない．モバイルIPアクセスポイントの設置については部局に依存するので，その辺り難しいところである．なお，情報基盤センターの利用者のホームIPアドレスは，プライベートアドレスではなく，情報基盤センターの管理下のグローバルアドレスを用いている．そのため，気付アドレスもグローバルアドレスを用いているが，モバイルIPアクセスポイントに対して，ネットワークセグメントの数が少ない，言い替えれば，1つのネットワークセグメントに多数のモバイルIPアクセスポイントが接続されているので，気付アドレスとしてグローバルアドレスを多数割り当てる必要が生じ，全体的にアドレスの効率的な利用ができていないという問題がある．たとえば，ある会議室に設置されているモバイルIPアクセスポイントに割り当てられる気付アドレスは数個なので，同時に10名程度の人数で会議を始めると，気付アドレスが不足するという事態に陥る．そのため，もし，部局からホームアドレスとして，グローバルアドレスの利用の申請があった場合その対応は可能であるが，この気付アドレスの管理の問題は承知してもらう必要がある．

今後の展開

本稿で紹介したようなシステムで，九州大学では現在，モバイルIPを用いた無線LANインフラが全学的に提供されている．本システムの稼働は2003年に始まったばかりで，稼働実績はまだ1年未満であるため，利用者サービスの観点からの定量的な評価はまだ行っていない．現在はシステムの全学的な整備が完了したばかりなので，そのような評価をゆっくりと行える状態ではないというのが実情であるが，今後は利用者数の把握や時間帯をキーにしたさまざまな解析を行っていく予定である．ただ，IPアドレスから利用者が特定できてしまうので，その辺りは情報に適宜匿名性を持たせるなど注意する必要がある．それから，現在ホームIPアドレスとしてプライベートアドレスを利用しているため，出口のところで，モバイルIP端末からのパケットのみをアドレス変換装置を経由させるために対外接続ルータでソースルーティングを行っているが，この処理が実はかなり対外接続の負荷をあげる要因となっている．その辺りの具体的なトラフィックも定量的に測定して，ソースルーティングのオーバーヘッドの見積りなども吟味する必要がある．

現在，情報基盤センターに対する利用に関する問合せはかなり多い方であるので，すでに多くのユーザが利用されていることが予想される．九州大学が採用したSISシステムは，利用者の端末にSISシステム専用のソフトウェアをインストールする必要があるのと，本来このソフトウェアは特定の無線ネットワークカードには依存しない設計であるにもかかわらず，一部動作が安定しない端末があり，ドライバの継続的なバージョンアップが必要である．また，現時点では，利用端末としてマイクロソフト社製のWindows版しか対応できていないが，九州大学では医学部，農学部ではMacユーザが多く，近々完了する予定であると聞いているMacへの対応に期待している．

九州大学でのモバイルIPによる安全な無線LANのインフラは整ったばかりである．今後このインフラを用いた有益なアプリケーションが学内からたくさん出てくることに期待する．また，そのようなアプリケーションをまた報告できる機会があれば，と考えている．

謝辞　九州大学におけるモバイルIPシステムは，情報基盤センターのスタッフならびにモバイルIPアクセスポイントを設置させていただいている部局の協力によって運用されてている．モバイルIPシステムの運用にかかわっているすべての方に感謝いたします．

（平成16年7月1日受付）