TAINS/G における無線 LAN ローミングシステムの構築について

今野 将、水木 敬明、後藤 英昭、曽根 秀昭
東北大学情報シナジーセンター

1．はじめに

東北大学情報シナジーセンターでは、平成 13 年度末に TAINS/G と呼ばれる学内ネットワークを構築し運用を開始した。現在、この TAINS/G において IEEE802.11 a/b/g 等の無線 LAN システムを利用する場合、大学内の各部局が独自に設置した無線 LAN のアクセスポイントを当該部局の運用ポリシーに従い利用する必要がある。そのため、部局毎に異なるポリシーやサービスの違いによる弊害が多数発生している。具体的には、「部局 A では MAC アドレスによる制限をかけているため、部局 B の利用者が部局 A で無線 LAN を利用するためには部局 A の管理者に許可を得て MAC アドレスの登録をしてもらう必要がある」や、「部局 A の利用者がワーム等に侵されたままの PC を部局 B の無線 LAN システムに接続してしまったため、外部に不正なアクセスを行ってしまったが、苦情が部局 B の管理者にきてしまった」等があげられる。

この問題を解決するための一つの手法として、全学に統一的な無線 LAN システムの敷設が考えられるが、そのためには、多大なコストと各部局の運用ポリシーの差異を吸収する必要がある。そのため、東北大学において統一的な無線 LAN システムの敷設は困難であった。そこで、本稿では、これらの問題を解決した上で、TAINS/G 上に各部局の運用ポリシーを害することの無い無線 LAN ローミングシステムを構築することを考え、その構成について紹介する。

2．無線 LAN ローミングシステム

2.1. システムの概要

東北大学における学内無線 LAN システムは、その多くが部局毎に設定された独自の利用方式（例：認証ゲートウェイ方式、WEP キー制限方式、MAC アドレス制限方式、部局内プライベートネットワーク限定方式、専用クライアントソフトウェア方式等）を用いており、運用ポリシーに関しても部局毎に定められている。そのため、部局 A の利用者が部局 B へ移動した際に、無線 LAN のアクセスポイントはあるのにも関わらず利用することが出来ないことがあり、利用者は不便な思いをしていた（図 1）。また、他部局の利用者が不正アクセスなどの処理を行った場合の責任の所在があやふやになるという管理面での問題点も発生している。

そのため我々は、上記の問題を解決したうえで、

- 利用者の利便性を優先させる
- 部局独自の利用方式への変更を最低限のものとする
- 可能な限り低コストでおこなうものとする
- 不正アクセスが発生した場合の責任の所在をはっきりさせる事を可能とする

という点を考慮した全学的な無線 LAN システムを構築することを考え、図 2 に示すような VPN（Virtual Private Network）を用いる方式を考えた。本方式では、以下のような処理の流れをとることで、利用者にとって利便性の高い無線 LAN ローミングシステムを提供することが可能になる。

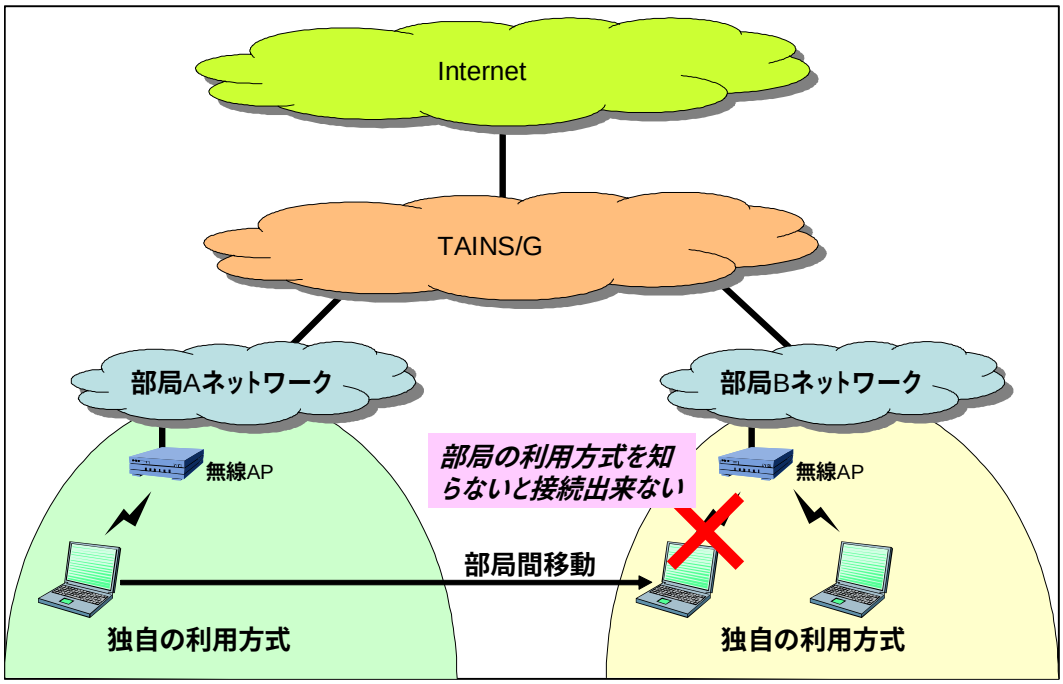

図 1　旧来の学内無線 LAN 環境の概念図

1. 各部局に部局専用の認証＋VPN サーバを設置し、各部局の利用者を登録する（図 2 中の部局専用認証サーバ）
2. 各部局の無線 LAN アクセスポイントにて無線端末⇒認証＋VPN サーバへのアクセスを許可し、利用の際に登録されている認証＋VPN サーバへ接続させる（図 2 の 1）
3. 無線 LAN アクセスポイントに接続した無線端末は所有者の所属する部局の認証＋VPN サーバへ接続し認証を行う（図 2 の 2）
4. 認証に成功したら、認証＋VPN サーバは無線端末に対して部局が保持する IP を振り出し、無線端末⇔認証＋VPN サーバ間で VPN を構成する（図 2 の 3）
5. 無線端末は、所属部局の IP を用いて外部に接続する（図 2 の 4）

2.2. システムの技術的要件

本方式を実現するにあたり、各部局のネットワーク運用管理の担当者を集め意見を聞き、利用者からの利便性や、部局間での相互乗り入れの安全性、構築に関わるコストなどを考慮したうえで、本方式に求められる技術的・機能的な要件として以下に示すものがあげられた。

a. クライアント側では、独自ソフトやドライバは用いずに可能な限りクライアント標準機能を用いる
b. マルチプラットフォーム（Windows、Macintosh、UNIX、PDA）に対応する
c. ゲストユーザによる一時利用も考慮する
d. 無線端末に割り当てる IP アドレスは所属部局が管理する IP アドレスから割り当てるものとする

e. 無線端末のサービス等の制限は所属部局が定めるものを適用する
f. VPN サーバへは、指定した無線端末からのみアクセス可能にする
g. 使い勝手とセキュリティは、システムの性質上使い勝手を“やや”優先させる
h. 基幹ネットワークである TAINS/G への設定変更（VLAN 設定等）は極力避ける
i. 各部局の既存の認証サーバのデータを可能な限り流用する

そして、これらの仕様を充足させるために、我々は本システムに求められる技術として

[P1]認証はローカル認証を基本とし、必要であれば NIS（Network Information Service）、Active Directory、LDAP（Lightweight Directory Access Protocol）に対応させる
[P2]VPN は Windows98 以降において標準実装されている PPTP を用いる
[P3]VPN サーバにて使用可能なサービス等の制限を行う
[P4]認証を通らない限り、VPN 以外のセッションは TAINS/G 内外とも利用できないようにする
[P5]VPN サーバには基本的に TAINS/G 内の無線 LAN アクセスポイント以外からは接続させない

が必要であると考え、各機能・技術の選定を行った。その結果、VPN サーバの OS として PC UNIX を選定し、PPTP サーバには PoPToP [1]を用いてセキュリティも考慮したうえで MSCHAP-V2 に対応した VPN サーバとし、認証は PoPToP 標準のローカル認証とした（P1、P2 に対応）。また、昨今の PC UNIX では標準的な機能である iptables や ipfirewall を用いて各種サービス制限を行う（P3～P5 に対応）こととした。

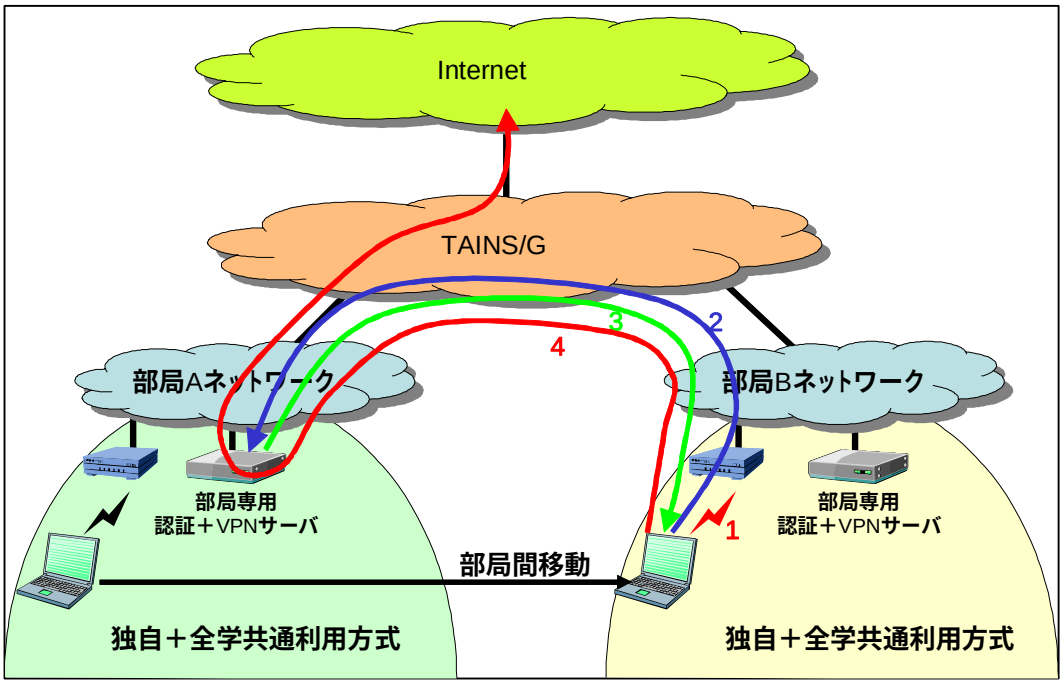

図 2　提案する学内無線 LAN 環境の概念図

3．システムの試作と実験

本稿にて提案しているシステムの実現可能性を検証するために、プロトタイプシステムを構築し動作の検証を行った。プロトタイプシステムは VPN サーバとして Free BSD 4.10 [2]と SUSE Linux 9.0[3]にそれぞれ PoPToP をインストールした 2 種類の VPN サーバを構築した。なお、それぞれの VPN サーバにおける認証方法は、PoPToP の標準的な方法であるローカルファイルによる認証を用いた。そして、それぞれの VPN サーバに対して NAPT（Network Address Port Translation）環境下の端末から接続を試み、VPN サーバにて“接続元クライアントを TAINS/G 内部端末に限定”、“VPN 接続後のアクセスを TAINS/G 内部に限定 or 外部接続の許可”等の制限を排他的に適用し、前節で述べた P1～P5 の実現可能性を検証した。

検証の結果、NAPT 環境を構築するゲートウェイの種類によっては、PPTP 接続時に用いる GRE（Generic Routing Encapsulation）プロトコル（プロトコル番号 47 番）の NAPT 越えに支障が出ることがわかり、PPTP パススルー機能を搭載したゲートウェイ等を用いた適切な NAPT 環境を構築する必要があることが解った。また、P2～P5 の技術的要件に関しては既存の技術を複数用いることでの実現可能性が高いと判断でき、P1 の認証サーバの NIS、Active Directory、LDAP への拡張に関しては、ソフトウェアの改造も視野に入れて検討を行う必要があることが解った。

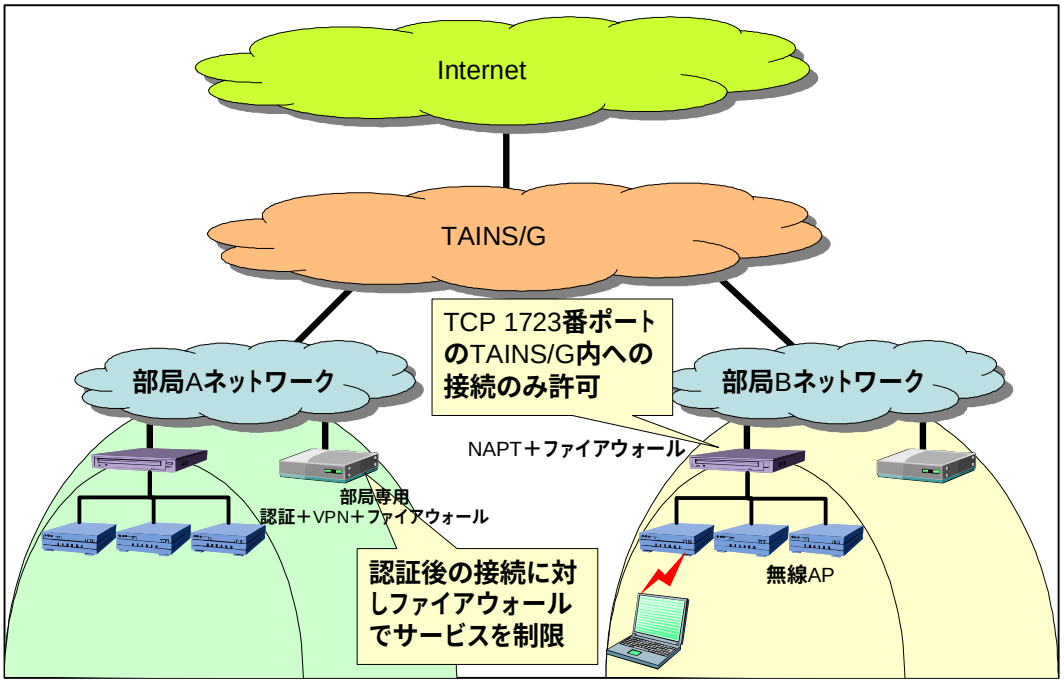

図 3　問題点を解決した学内無線 LAN 環境の概念図

今回の実験環境においては、認証前の端末が NAPT 環境から VPN サーバへ接続するために必要な TCP 1723 番ポートを、NAPT 環境用のゲートウェイにおいて常時開放していたため、TAINS/G 外部の VPN サーバへも接続できてしまう、さらには TCP 1723 番ポートを利用した悪質なプログラムが実行できてしまうという問題点があることがわかった。また、部局の運用ポリシーを反映させるには、各部局がもつ認証＋

VPN サーバにおいて、VPN 接続後の端末のサービス制限を施す事が適切であることがわかった。これらに関して、今後の運用を考えると、図 3 に示すようにクライアント端末側にも NAPT やファイアウォールを設置しクライアントの接続先にも制限を設け、認証＋VPN サーバにもファイアウォール機能を付加し、サービスの制限を行う必要があると考えられる。

4. おわりに

本稿では、東北大学の学内ネットワーク TAINS/G において無線 LAN ローミングシステムの実現方法と設計について述べた。このような、部局間を広くローミングする無線 LAN システムとしては、みあこネット[4]が有名であるが、みあこネットでは本システムが求められているような状況（部局毎のポリシー設定が可能、割り当てられる IP アドレスは所属部局のものであること等）には適応が困難であると考えられる。また、最近では PPTP サーバ機能を搭載したブロードバンドルータも安価に販売されてきている。今後、これらの既存製品の活用も視野に入れ、本システムの試験運用を通して、より要求に合致した無線 LAN ローミングシステムの構築を行ってゆく。

参考文献

[1] Poptop - The PPTP Server for Linux. “http://www.poptop.org/”.
[2] The FreeBSD Project. “http://www.freebsd.org/”.
[3] SUSE Linux.“http://www.suse.com/”.
[4] MIAKO-NET 公衆無線インターネットプロジェクト.“http://www.miako.net/”.