# 複数 VLAN の動的切り替えネットワークの構築について

久長 穣[1]　北上 悟史[2]　渡邊 孝博[3]　棚田 嘉博[3]　井上裕二[4]
[1]山口大学総合情報処理センター
[2]富士通サポートアンドサービス株式会社
[3]山口大学工学部
[4]山口大学医学部附属病院

一般にセキュリティポリシーの異なるネットワークは，それぞれのネットワークの利用目的に応じて端末を設置し，物理的に独立した形態で利用，運用されている．このような環境では，端末の設置場所や維持するための経費が余分に必要となる．また，利用目的に応じてネットワークを選択せざるを得ない．

これらの問題点を解決するため，スイッチング・ハブを用いてひとつの物理ネットワークとして構成し、それぞれのネットワークを VLAN として構成し、利用者の要求に応じて VLAN を動的に切換えることにより，未登録の第三者による不正アクセスや異なるネットワーク間での情報の漏洩を防止し，事前に登録された利用者および端末のみが複数ネットワークを統一的に利用できるネットワークを構築した．

ネットワークを構築し、実験を行った結果，認証せずにネットワークにアクセスすることやユーザ端末間において不正アクセスすることは不可能であり，利用者が希望したネットワーク選択して通信できることが確認できた．

# A Construction of Dynamic Selected Network out of VLAN's

Yutaka HISANAGA[1] Satoshi KITAGAMI[2] Takahiro WATANAME[3] Yoshihiro TANADA[3] Yuji INOUE[4]
[1]Integrated Information Processing Center, Yamaguchi University
[2]Fujitsu Support and Service Inc.
[3]Faculty of Engineering Yamaguchi University
[4]Yamaguchi University School of Medicine

There are some networks which security policy is different. The each network is respectively constructed physical network and connected exclusive terminals. The user necessary chose each terminals corresponding to the user purpose.

We construct the physical network with switching HUB. The network has some logical networks as Virtual LANs. The VLAN is dynamically selected out of these VLAN for the user's requirement, if the user is a registered member and users terminal is corrected.

We show the outline the network system and the performance of dynamically selected VLAN.

## 1. はじめに

近年, 処理の分散化と資源の効率化を目的とし，情報システムのネットワーク化が進み，ほぼすべての端末は，ネットワークに接続されている．これらの端末は，ネットワークの利用目的，また，セキュリティレベル等のポリシーに応じて，物理的に独立したネットワーク形態で利用，運用されている．そのため，1 つの組織内にポリシーの異なったネットワークが複数存在するようになってきた．

一般に，ポリシーの異なるネットワークへのア

クセスに対しては, セキュリティを保つためにIPアドレスによるフィルタやファイアーウォール等を設置し, アクセス制限をかけて運用されている. また, セキュリティレベルの高いネットワークから低いネットワークにはアクセスできるが, その逆ができないといったような, 一方向の通信でセキュリティを維持するといったものが一般的である.

このような環境では, 次のような問題点があげられる.

1. ネットワークの利用目的に応じて, そのネットワークに接続されている端末を利用しなければならない.
2. Web やメールは利用できるが, それ以外のネットワークサービスを使用して外部との通信ができないなど, 利用可能なサービスが限定される.
3. 管理者側において, ネットワーク毎に端末を設置しなければならないため, 端末の設置場所や維持するための経費が余分に必要となる.
4. 誰がいつ, どこから, どのような端末を用いて, どのネットワークを利用しているかを, 統一的に管理することが困難な状況である.

これらの問題を解決するために, 複数ネットワークそれぞれのセキュリティポリシーを保ちつつ, 統一的に利用することができる環境を構築し, ネットワーク及び計算機資源を有効利用する必要がある.

正規の利用者が単一のネットワークではあるがネットワークを自由に使用できる環境について他大学においても様々な研究が行われている[1][2].

本稿では, 複数のネットワークをあらかじめ登録された端末であれば、利用者が自由に切り替えて利用できるネットワークを構築したので、その概要および VLAN の動的選択に関する性能について評価する.

## 2. 提案手法

セキュリティポリシーの異なる複数ネットワークを統一的に利用するため, 本論文では図１のようなシステムを構築した. ここで、複数ネットワークとはインターネットのつながる学内 LAN、研究室等で利用される研究用 LAN およびもっぱら業務のみで利用される業務LANの３つのLANとした。

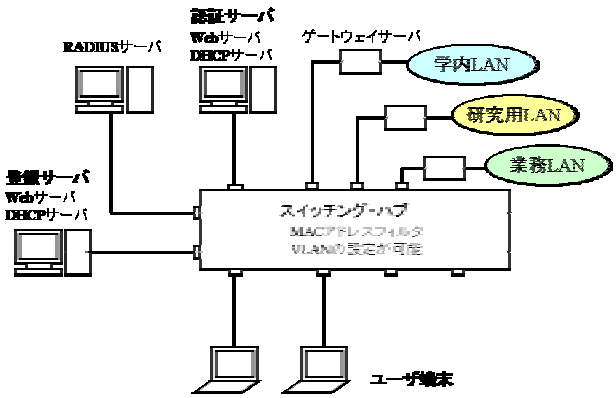


図１　本システムのネットワーク構成図

### 2.1 本システムを実現するために必要な機能

安全性を保ちつつ, 複数のネットワークを統一的に利用できる環境を構築するため, 次の機能が必要となる.

1. ユーザ認証機能
   ネットワークにアクセスしようとしているユーザが, 利用資格を有するかどうかを判断するため, ユーザの認証機能が必要となる.
2. アクセスログ記録機能
   管理者がネットワークの利用状況を把握するため, また, 不正アクセスの検出を行うため, 誰が, いつ, どこで, どの端末を用いて, どのネットワークにアクセス／アクセス終了したかを記録しておく必要がある.
3. ユーザ端末間のセキュリティ機能
   複数の端末をネットワークに接続するためにハブを用いた場合, 相互に通信を行うことが用意である. このため, ユーザ端末のセキュリティを守るためにはインターネットなどの外部からの攻撃を防ぐだけでなく, ユーザ端末間の攻撃を防ぐ必要がある.
4. ユーザ端末の特定
   ユーザの認証を行うだけでは, 認証情報が漏洩した場合, 不正なユーザの侵入を許してしまう. このため, ユーザが利用可能な端末の特定を行う必要がある.
5. ネットワークの動的切り換え
   認証が正しく行われたユーザだけが, 安全に希望したネットワークとアクセスできるように, ネットワークを動的に切り換える仕組みが必要となる.

6. 通信終了のリアルタイム検出
ネットワーク利用を終了した場合，その部分がセキュリティホールとなることを防ぐため，即座にその動向を検出する仕組みが必要となる．

本システムでは，ユーザが複雑なネットワーク設定を行うことなくネットワーク利用ができるよう，DHCP(Dynamic Host Configuration Protocol)[4]サーバを設置した．また，利用制限を行うために必要となる認証情報を格納するデータベースサーバとして，RADIUS(Remote Authentication Dial In User Service)[5]サーバを設置した．

### 2.2 認証機能の条件

本システムでは，ユーザの特定を行うため次の条件を満たす認証サーバを設置した．

・条件 1.端末に特別な認証用のソフトを必要としない
・条件 2.ネットワークの利用状況を把握する
・条件 3.認証が正しく行われるまでは，認証サーバ以外との通信を禁止する
・条件 4.認証が正しければ，ユーザが希望するネットワークとの通信を許可する
・条件 5.ユーザがネットワーク利用を終了後，再び認証サーバ以外との通信を禁止する

本システムにおいて，条件 1，2 を満たすため，認証に Web ブラウザを用い認証時のアクセスログを記録することとした．条件 3～5 を満たすため，スイッチング・ハブの VLAN 設定を動的に切換ることとした．

## 3. 事前登録

安全に本システムを利用するため，事前に RADIUS サーバに認証情報の登録を行う必要がある．どのような登録方法を用いてもかまわないが，登録の増加に伴い，管理者の負担も増加する．本システムでは，管理者の負担を軽減し、管理責任の実体化のため，保証人制度と登録サーバを設置した．

### 3.1 保証人制度

組織の規模，ユーザ数にもよるが，管理者がユーザ全員の登録を行うためには，名簿が存在しての一括登録を除いて，利用者の出入りに伴い個々に対応していたのでは、多くの負担が必要になる．このため，本システムではあらかじめ管理者より適当であると判断された保証人を定め、利用者情報は、その保証人と利用者自身が登録してもらう．また、端末や利用者の管理責任は保証人が負うものとする。大学の場合は、それぞれの教授が適当だと考える。

### 3.2 登録サーバ

本システムでは，管理者の負担を軽減させるため，ユーザ自身に RADIUS サーバに対して認証情報の登録を行ってもらう．RADIUS には登録を行うためのコマンドが用意されているが，これを実行するのはユーザにとって負担が大きい．登録作業を円滑に行うため，Web サーバ，DHCP サーバ，RADIUS クライアントとして機能する登録サーバを設置した．

ユーザ認証情報の登録手順は，あらかじめ登録された保証人の保証人と利用者が２人で利用予定の端末を用いて行うものである．また，登録だけでなく，認証情報の削除や変更も可能である．

## 4. 本システムの利用制限

### 4.1 VLAN による利用制限

本システムでは，異なるネットワーク間の情報の漏洩および VLAN の動的選択のために，VLAN の方式として、ポートベース VLAN 方式と IEEE802.1Q 規格の VLAN Tagging 方式[6]を利用した．

### 4.2 認証による利用制限

本システムでは，ユーザが希望したネットワークとアクセスするために，以下に示す３つの認証を行っている．

・ユーザ認証による利用制限
ユーザ名，パスワードによるユーザ認証を行うことで，本システムを利用することができる正規ユーザかどうかの判断を行う．
・グループ属性による利用制限
本システムでは，図２に示す関係で，ユーザを学生，研究生，職員というグループに分け，接続先ネットワークを学内 LAN，研究用 LAN，業務 LAN とし，事前に登録されたユーザに対しても，アクセス可能なネットワークを制限する．
・ユーザ端末のＭＡＣアドレスによる利用制限

ユーザ認証を行うだけでは，認証情報が漏洩した場合，不正なユーザの侵入を許してしまう．このため，端末のネットワーク機器が持つ MAC アドレスによる制限をすることにより，ユーザが利用可能な端末かどうかの判断を行う．

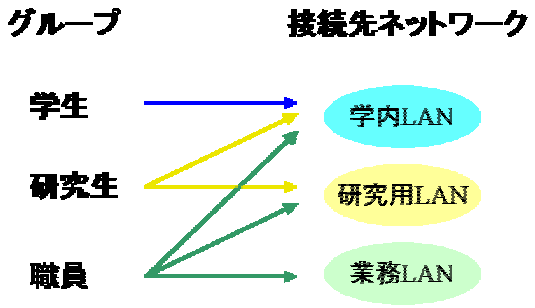


図２　各グループと接続先ネットワークの関係

## 5. 本システムのネットワーク利用方法

### 5.1 本システムの VLAN 初期状態

本システムの VLAN 初期状態として，ユーザ側の各ポートに VLAN を 1 つずつ設定し，認証サーバが接続されているポートに VLAN Tagging の設定を行う(図３参照)．こうすることにより，認証が正しく行われるまでは，ユーザ端末は認証サーバとしか通信が行えず，ユーザ端末間同士の不正アクセスを防止することができる．

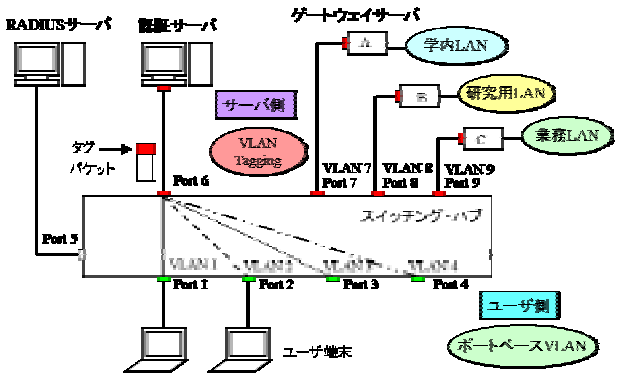


図３　VLAN 設定の初期状態

本システムでは，サーバ側のポートには VLAN Tagging を用い，タグ付きパケットが流れるため，これを処理する必要がある．認証サーバ，ゲートウェイサーバ共に，このタグ付きパケットを処理できるように設定した．

### 4.3 ネットワーク利用手順

本システムにおいて，ネットワークを利用するための手順を以下に示す．また，切り替え後の状態を図４に示す．なお，ユーザの認証情報，ユーザ端末の MAC アドレスはあらかじめ RADIUS サーバに登録されているものとし，ユーザは，接続先ネットワークとして研究用 LAN を選択したものとする．

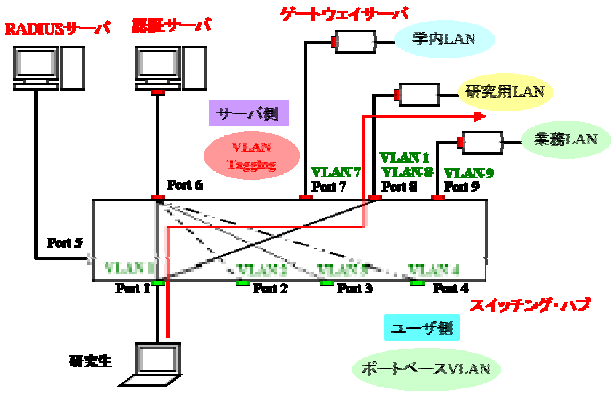


図４　本システムのネットワーク VLAN 切り替え後

処理 1.　利用者がネットワークに端末を接続することにより，端末は DHCP によるネットワークの設定が行われる．

処理 2.　利用者は Web ブラウザを用いて、認証サーバに接続し，ユーザ名，パスワード，利用したいネットワークを入力する．

処理 3.　認証サーバは RADIUS サーバに認証情報の問い合わせを行う．

処理 4.　RADISU サーバは認証サーバに認証許可の通知をおこなう。

処理 5.　認証サーバはグループや MAC アドレスを用いて、利用制限の確認する。

処理 6. 認証サーバは端末が接続されたポートに対して，該当端末の MAC アドレスフィルタの設定する。

処理 7.　認証サーバは VLAN 設定の切り換え，利用者が選択したネットワークへ接続する．

処理 8.　利用者が希望したネットワークと通信可能となる．

また，利用者に権限があれば，同様の手順を行うことにより，研究用の LAN だけでなく，他の LAN にもアクセス可能である．

### 5.3 ネットワーク利用終了手順

本システムにおいて，ネットワーク利用終了手

順を以下に示す.

処理 1.端末がはずされるなどして、該当ポートのリンクがダウンすると、スイッチは認証サーバへ、ネットワーク利用終了を通知する.
処理 2.認証サーバは VLAN 設定を元に戻す.
処理 3.認証サーバは MAC アドレスフィルタの設定を解除する.
処理 4.認証サーバとしか通信できない状態に戻る.

## 6．評価

実際に構築したシステムの動作検証とパフォーマンス測定を行った．ハードウェアおよびソフトウェアは以下のものを用いた.

ハードウェア
スイッチング・ハブ：
Cabletron Systems SSR-2000
サーバ：AT 互換機

ソフトウェア
サーバ OS：FreeBSD-4.2
DHCP：ISC-DHCP-2.0
Web サーバ：Apache-1.3.4
RADIUS サーバ：Radiusd-Cistron-1.6.3

### 6.1 動作検証

VLAN 設定が正常に切換わっているかどうかを調べるため，以下に示す 4 つの状態でユーザ端末から Ping，ARP(Address Request Protocol)コマンドを実行し，通信可能な端末の変化を調べた(表 1 参照).

- VLAN の設定が行われていない状態
- 本システムの VLAN 設定の初期状態
- 認証後，VLAN 設定が切換わった状態
- ネットワーク利用終了後，再び VLAN 設定が切換わった状態

表 1：通信可能な端末の変化

| | 他のユーザ端末 | 認証サーバ | RADIUSサーバ | ゲートウェイサーバA | ゲートウェイサーバB | ゲートウェイサーバC |
|---|---|---|---|---|---|---|
| VLAN設定が行われていない状態 | ○ | ○ | ○ | ○ | ○ | ○ |
| 本システムのVLAN設定初期状態 | × | ○ | × | × | × | × |
| VLAN設定が切換わった状態 | ▲ | ○ | × | △ | △ | △ |
| 再びVLAN設定が切換わった状態 | × | ○ | × | × | × | × |

○ :通信可能　▲ :同じ接続先ネットワークを指定した場合のみ通信可能
× :通信不可　△ :ユーザが接続先ネットワークに指定した場合のみ通信可能

### 6.2 パフォーマンス測定

複数のユーザからの同時アクセスを想定して，認証とスイッチング・ハブの設定変更にかかる時間を接続台数別に測定した(表 2，3 参照).

表 2：ネットワーク利用時における処理時間

| 処理時間＼接続台数 | 1台 | 2台 | 4台 | 8台 |
|---|---|---|---|---|
| 認証に要する時間(s) | 0.08 | 0.13 | 0.28 | 0.51 |
| SW-HUBの設定が完了するまでの時間(s) | 0.71 | 1.54 | 3.17 | 6.41 |
| 合計(s) | 0.79 | 1.67 | 3.45 | 6.92 |

表 3：ネットワーク利用終了時における処理時間

| 処理時間＼接続台数 | 1台 | 2台 | 4台 | 8台 |
|---|---|---|---|---|
| Link-Downの検出時間(s) | 0.02 | 0.04 | 0.05 | 0.08 |
| SW-HUBの設定が完了するまでの時間(s) | 0.78 | 1.63 | 3.42 | 6.46 |
| 合計(s) | 0.81 | 1.67 | 3.47 | 6.54 |

## 7. 考察

本システムにおいて，DHCP によるネットワークの設定，認証サーバによる利用制限が正常に行われているかどうかは，実際に，異なるのグループ属性を持つ数人の被験者に本システムを利用してもらうことで確認が行えた．また，認証サーバに，ユーザ名，ユーザ端末の IP アドレス，MAC アドレス，ユーザのネットワーク利用時間などの詳細なログが記録できていることも確認できた．以上のことから，ユーザの特定，ユーザ端末の特定，管理者によるネットワークの利用状況が把握できているといえる.

表 1 の結果より，4 つの状態において通信可能な端末が変化していることにより，本システムが正常に動作し，VLAN 設定が動的に切換わっていることが分かる.

本システムにおいて，認証にかかる時間，SW-HUB の設定にかかる時間を測定した結果(表 2，3 参照)，ユーザ 1 人に対して約 0.8 秒でユーザは希望したネットワークにアクセスすることが可能であることが分かった．また，設定を解除する場合も同様に非常に高速に行えることが分かった．更に，ほぼ同時に 8 人が認証サーバにアクセスし，本システムを利用したとしても，全てのユーザが希望したネットワークにアクセスするまで約 7 秒かかるが，問題なく SW-HUB の設定を変更すること

ができた.

## 8. まとめ

本研究では，VLAN 設定を動的に切り換えることにより，事前に登録された正規利用者と端末のみが，複数ネットワークを切り替えて利用できる環境を構築した．また，保証人制度と登録サーバを設置することにより，事前登録時における管理者の負担を軽減した.

今後さらに複雑化するネットワーク管理，セキュリティ問題を考えると，異なるセキュリティポリシーを持つ複数ネットワークを持つようなネットワーク環境において、本システムのように複数ネットワークを動的に切り替えて利用する環境が重要になる.本システムは附属病院内の一部の研究室で試験的に運用を試みている。

今後の課題としては通信データの暗号化および認証時でのデジタル署名の使用などがあげられる。

## 文献


[1] 久長穣,岡田隆,刈谷丈治: 情報コンセントのユーザ認証について,学術情報情報処理究,pp.77-80(1998).

[2] 石橋勇人,山井成良,安部広多,大西克実,松浦敏雄: IP アドレス/MAC アドレス偽造に対応した情報コンセント不正アクセス防止方式,情報処理学会論文誌.pp.4353-4361(1999).

[3] Droms,R.: Dynamic Host Configuration Protocol,RFC2131(1997).

[4] Rigney,C.,Rubens,A.C.,Simpson,W.A. and Willens,S.: Remote Authentication Dial In User Service(RADIUS),RFC2138(1997).

[5] IEEE: 802.1Q-1998 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridge Local Area Networks,IEEE(1998).

[6] J.Postel,J.Reynolds: Telnet Protocol Specification,RFC854(1983).

[7] Case,J.D.,Fedor,M.,Schoffstall,M.L. and Davin,J.R.: Simple Network Management Protocol(SNMP),RFC1157(1990).

[8] 是友: ポイント図解式 VPN/VLAN 教科書,株式会社アスキー(1999).

[9]笠野: インターネット RFC 辞典，株式会社アスキー(1998).