[全国共同利用情報基盤センター研究開発論文集 No.30]より

EtherIP を用いたセンター管理型キャンパス無線 LAN

大和 純一　若山 永哉　後藤 英昭　曽根 秀昭

東北大学 サイバーサイエンスセンター

1　はじめに

近年の無線 LAN 機器の普及に伴い，キャンパス内で学生や教職員などが各自の PC を無線 LAN で学内ネットワークに接続して，授業や研究に役立てたいといった要望が増加している．

無線 LAN では，キャンパス内のどこでも同じようにできることが望ましいが，無線 LAN 用のアクセスネットワークをキャンパス全体に新規に敷設することはコストが問題となる．また敷設済みの有線ネットワークを無線 LAN に利用する場合，無線 LAN と既存 LAN の通信が同一 LAN 上に混在することによるセキュリティ面での問題等が生じえる．さらに，管理面からはセンターで無線 LAN を集中管理することが望ましい．

そこで我々は，既設 LAN 上に EtherIP[1]を用いて無線 LAN 専用のアクセスネットワークを構築し，センター管理型のキャンパス無線 LAN を実現した．本稿では EtherIP を用いたキャンパス無線 LAN 用アクセスネット構築手法について報告する．

2　既設 LAN を活用した無線 LAN 用アクセスネットワークの提案

キャンパスネットワークの状況としては，既設の有線ネットワークの管理が部局単位での管理の部分とセンターでの管理の部分が混在し，構成も NAT/NAPT 等が使用されている場合や，機器の VLAN の使用可否等，構成・機器・管理体制が複雑になっている．このような状況でネットワークの管理コストを考慮した上で，学生・教職員がキャンパス内のどこからでも同じように無線 LAN を使用できるようにするためには，センターによる一元管理の無線 LAN 用アクセスネットワークを構築することが望ましい．

無線 LAN 用アクセスネットワークのために，新規の有線ネットワークを敷設することは，敷設工事・機器導入等の初期コストが問題となり実現が困難である．また，既設の有線ネットワークを活用し，VLAN を用い無線 LAN 用アクセスネットワークを実現する方法もあるが，VLAN 対応機器へのリプレースによる機器導入費用は避けがたい．また，既設の有線ネットワークを活用する場合，使用されているネットワーク環境の変更はユーザへの影響が大きく，そのため導入のハードルは高い．以上から，既設の有線ネットワークの使用法・機器・設定を変更せずに，無線 LAN 用アクセスネットワークを構築する方法が望まれる．

一方，学内全ての無線 LAN 機器をセンターで管理することを考えると，末端の機器の設定変更を行わず，センター内に設置した機器の変更のみで運用できることが管理コスト面からは望ましい．さらに，個々の機器の設定変更を要する場合でも，センターからリモートで設定変更が行えることが必須であろう．なお，学内への無線 LAN の導入手順としては，図 1に示すように，センターは導入機器の初期設定のみを行い，設置についてはサービスエリアを管理する部局に一任し，かつ，部局が行う設置作業も最小限となる方法を提案する．

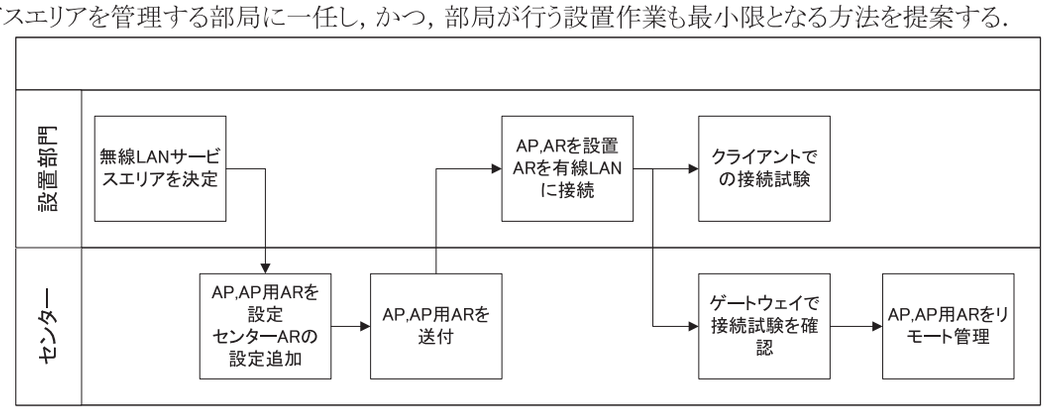

図 1 設置部局とセンターの役割分担

以上述べたような環境を考慮し，容易に導入できる無線 LAN 用アクセスネットワークの構築手法を提案する．提案する構築手法の要件を下記に示す．

- 既設有線ネットワークを活用し，既存のネットワークの使用方法・機器・設定の変更をせずに，無線 LAN 用アクセスネットワークを構成
- 無線 LAN 用アクセスネットワークは，センターで一元管理し，無線 LAN のサービスエリアの開設は，末端機器の設置は各部局に一任
- 無線 LAN サービスエリア開設にあたり，センターで機器の初期設定を行い，部局は最小限の作業で設置が可能
- 無線 LAN サービスエリアに設置する機器は，有線ネットワークの構成変更等の影響を受けず，リモート管理ができ，無線 LAN 用アクセスネットワークの設定変更は基本的にセンター内の機器の設定変更のみで実現

3　EtherIP

我々は，既設の有線ネットワークを活用し，既存のネットワークの使用方法・機器・設定の変更を要さない，無線 LAN 用アクセスネットの実現方法として L2VPN に着目した．L2VPN では，MAC フレームを IP パケットにカプセル化し，VPN のノード間で送受信を行う．

L2VPN を用いることで，IP 等の layer3 のプロトコルを限定せずに無線 LAN 用のアクセスネットワークを実現することが可能である．既設の有線 LAN に導入した場合，L2VPN で接続されたノード間で IP パケットの送受信が行えればよく，サービスエリアとセンターを L2VPN で接続する場合には，既存ネットワークの設定変更も少なく，既設有線 LAN としては，トラフィックの増加以外の影響がないと考えられる．

また，IEEE 802.1Q の VLAN-tag を透過させられる L2VPN 装置を使用することで，部局単位の無線 LAN や，学内共通の無線 LAN や，eduroam[2][3][4]のようなキャンパスネットワークローミングも，一台の無線アクセスポイント(以下，AP)で同時にサービスすることが可能である．この構成では 802.1Q 対応し複数の SSID をあつかい，SSID 毎に VLAN-tag を割り当てられる AP を用いる．

我々は L2VPN として EtherIP を選択した．

4　EtherIP を用いた無線 LAN 用アクセスネットワークの構成

次に，無線 LAN 用アクセスネットワークをセンターで一元管理するための構成について説明する．

無線 LAN サービスエリアとセンターを EtherIP で接続することで，無線 LAN サービスエリアで行われる無線 LAN を介した通信は，センターに全て転送される． さらに，キャンパスネットワークと無線 LAN 用アクセスネットワークとの接続を，センター内のゲートウェイで行うことで，ルーティングおよびフィルタリングを，センター内で一元的に管理する．これにより，キャンパスネットワークの利用ポリシーが変わった際，センター内のゲートウェイの設定変更により無線 LAN アクセスネットワークの利用ポリシーへの対応が可能となる．また，無線 LAN の利用状況をセンターで把握することも容易である．

無線 LAN 用アクセスネットワークのシステム構成を図 2に示す．

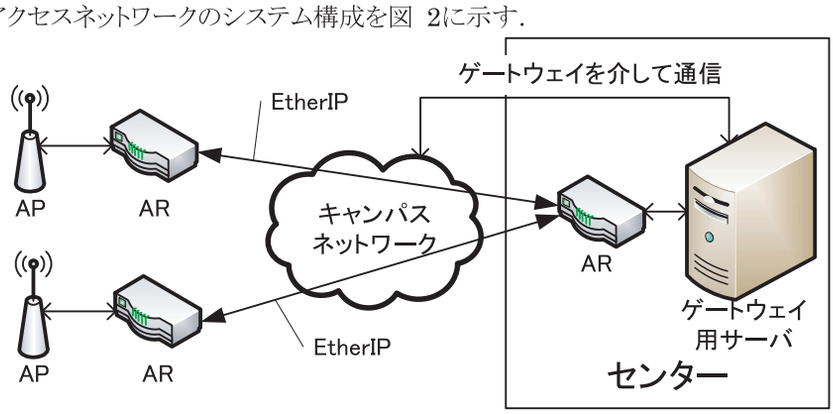

図 2 システム構成

なお，AP として 802.1Q に対応し，複数の SSID に柔軟にセキュリティ設定ができることからアライドテレシス社の AT-TQ2403 を使用した．この AP は EtherIP に対応していないため EtherIP が使用できるアクセスルータ(以下，AR)として，NEC 社の UNIVERGE IX2000/IX3000 シリーズを使用した．

4.1　センター用 AR

センター用 AR は，複数の AP 用 AR と接続する構成とし，大容量のもの（UNIVERGE IX3010 + 2GE-T カード）を使用した．

EtherIP のトンネルが使用するポートには，キャンパスネットのどこからでもアクセスできる固定の IP アドレスを設定し，キャンパスネットワークに接続した．また，ゲートウェイ用サーバとセンター用 AR の他のポートを直結した．センター用 AR では，各 AP 用 AR の IP アドレスを指定し，EtherIP のトンネルを設定し，ゲートウェイ用サーバと接続したポートと，これらトンネル群とをブリッジ接続するように AR を設定した．この構成により AP 用 AR とセンター用 AR を EtherIP で接続し，AP 群から送られてきた全パケットがゲートウェイ用サーバに送られ，ゲートウェイ用サーバから送られてきた全パケットが AP 群に送られる．

4.2　AP 用 AR

AP 用 AR としては設置の自由度を考慮し，小型の AR（UNIVERGE IX2005）を使用した．

EtherIP のトンネルが使用するポートは，センター用 AR と通信可能なように固定の IP アドレスを設定し，キャンパスネットワークに接続した．また，AP と AP 用 AR の他のポートを直結した．センター用 AR の IP アドレスを指定し，EtherIP のトンネルを設定し，AP と接続したポートと EtherIP のトンネルとをブリッジ接続するように AR を設定した．

なお，使用した AR は，内部のブリッジ設定に仮想インターフェースを割り当てる機能があり，これを使用することでセンターから EtherIP のトンネルを経由し，AP 側 AR を管理することが可能である．また， AP に無線 LAN 用アクセスネットからアクセス可能な，IP アドレスを設定することで，センターから EtherIP のトンネルを経由し，AP を管理することも可能である．

なお，図 2では AP 用 AR には 1 台の AP しか接続していないが，1 台の AR に複数の AP を接続することも可能である．

4.3　ゲートウェイ用サーバ

EtherIP を用いて形成した無線 LAN 用アクセスネットワークと，キャンパスネットワークを接続する本構成の要となるゲートウェイについて説明する．

無線 LAN 用アクセスネットワークと，キャンパスネットワークとのゲートウェイは，Linux が動作するサーバを用いて実現した．ゲートウェイ用サーバでは，キャンパスネットワークの運営方針に合わせたパケットのフィルタリングと，dhcp によるクライアントへの IP アドレス払い出しを基本機能として持つ．Linux サーバを使用することでさまざまな機能をゲートウェイ上に実現することが容易である．

また，今回実現した構成では，クライアントへ払い出す IP アドレスに private アドレスを使用し，無線 LAN 用アクセスネットワークとキャンパスネットワークは，NAPT を介して接続している．

5　対応環境の拡大

本章では、本構築手法が利用できる環境を拡大するために行った検討について説明する。4章で示した構成方法では，dhcp・NAT/NAPT を使用した環境には対応できず，多数の AP を 1 台のセンター用 AR でまかなう場合フラッディングが発生することが懸念され，クライアントと AP が IEEE 802.1X での認証にキャンパスネットワーク上の RADIUS[5]サーバを使用する場合，RADIUS サーバへのアクセスキーを全 AP で共通にしなければならないという課題がある．以下，各課題の解決策を示す．

5.1　dhcp・NAT/NAPT 対応

まず、dhcp・NAT/NAPT を使用した環境への対応に法ついて説明する。4章で示した構成方法では，

EtherIP のトンネルの設定で相手側の IP アドレスを指定しなければならないため，AP 用 AR も固定 IP アドレスでなければならない．また，EtherIP のトンネルが送信先 IP アドレスに直接パケットを送るため，AP 用 AR はセンター用 AR から直接パケットを受け取れなければならない．そのため dhcp が使用された LAN や，NAT/NAPT の内側の LAN に AP 用 AR を設置することができない．そこで，dhcp・NAT/NAPT 対応させる構成方法を検討した．

使用した AR の EtherIP では，配信プロトコルとして IPSec が使用でき，この IPSec が動的 IP に対応していた．そこで EtherIP + IPSec を用いることで，dhcp 環境に対応可能であった．また，動的 IP 側からコネクションを確立するため NAT/NAPT の内側からコネクションを張ることで，NAT/NAPT の内側の LAN に AP 用 AR を設置することが可能となった．なお，IPSec の通信での暗号化は AR の負荷等を考慮し行わない設定とした．

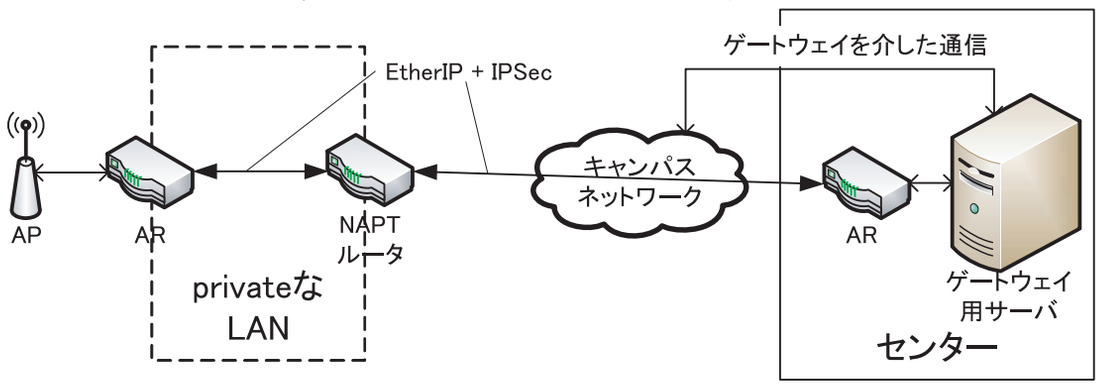

図 3 NAPT 内側に設置

この設定では，下記手順で AP とゲートウェイ用サーバが通信可能となる．すなわち，AP から LAN へのパケット送信を契機に EtherIP が使用可能となる．そのため，EtherIP 用のコネクションが確立していない状況ではセンター側から AP および AP 用 AR にアクセスができない．したがって，センターから無線 LAN が管理できない状態が発生しえる．

1. AP から LAN にパケットを送信
2. EtherIP の接続を開始
3. 無線 AP 側 AR が，センター側 AR と IPSec の接続を要求
4. センター側 AR と無線 AP 側 AR が認証
5. センター側 AR と無線 AP 側 AR で IPSec が確立
6. EtherIP の接続が確立
7. AP とゲートウェイ用サーバが通信可能となる

5.2　大規模対応

次に大規模環境への対応法を説明する。4章で示した構成方法では，センター用 AR で，全ての EtherIP 用トンネルとゲートウェイ用サーバの接続されたポートを，一つのブリッジとして設定したため，センター用 AR を介して，全ての AP 用 AR に，全てのパケットが送信される．そのため，各 AP 用 AR に不要なパケットが流れ，規模によってはフラッディングが発生しえる．この問題に対する対応策を説明する．

使用した AR では，トンネルのような仮想インターフェースも含めてインターフェース単位にパケットをフィルタリングする機能を持ち，VLAN-tag によるフィルタリングも可能であった．また本構成では，802.1Q 対応の AP を用いることから，AP で使用する VLAN-tag を変え，センター用 AR の各 EtherIP のトンネルに対応する VLAN-tag のみを通過させるフィルタを設定した．この設定により各 AP に関連しないパケットが送信されることを防ぐことが可能となる．なお，VLAN-tag を建物内のフロアーや建物単位で共通化することで，フロアー内の端末や AP が同一 LAN に接続され，情報の共有等が容易となる．

この構成では，ゲートウェイ用サーバも VLAN-tag に対応させ，VLAN-tag で識別できる LAN 単位で dhcp による IP アドレス払い出し，パケットのフィルタリング，NAPT を介したキャンパスネットワークとの接続を行わせた．

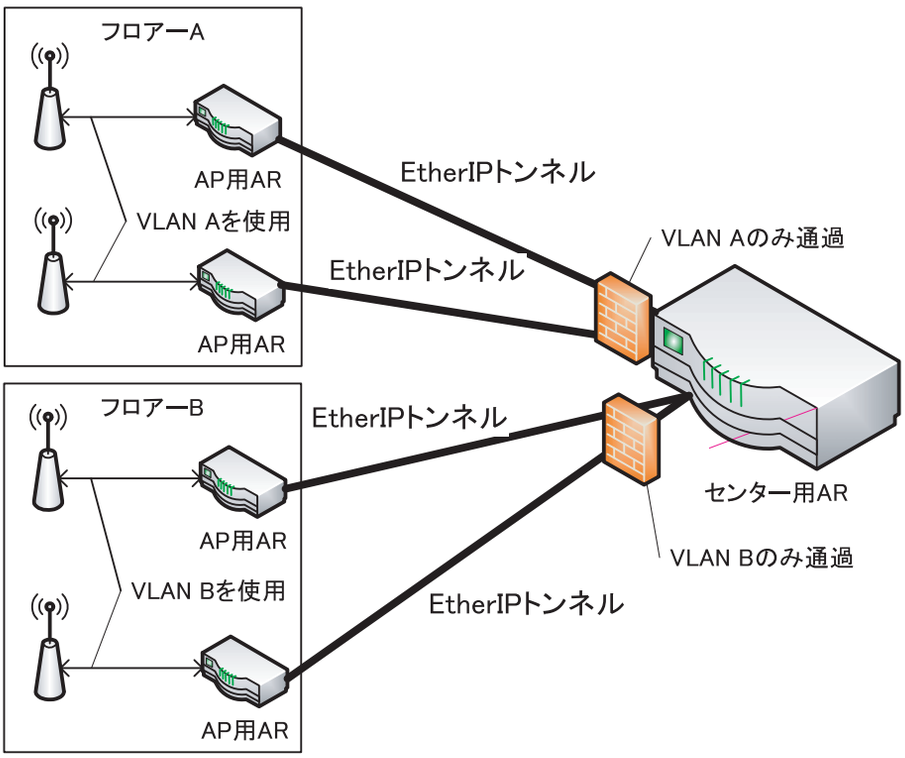

図 4 大規模対応のイメージ

5.3　RADIUS サーバアクセスキーの AP 個別化

最後に RADIUS サーバのアクセスキーを AP 個別に持たせる方法について説明する。4章で示した構成方法では，ゲートウェイ用サーバが NAPT を行っているため，キャンパスネット上からはクライアントや AP を個別に認識することができない．一方，クライアントと AP が IEEE 802.1X を用いた認証を行う場合，RADIUS を使用するが，RADIUS サーバは IP アドレスでクライアントを識別する．そのため，キャンパスネット上の RADIUS サーバを用いる場合，AP を個別に識別することができない．従って，RADIUS サーバにアクセスする際に必要となるアクセスキーを AP で共通化する必要が生じる．アクセスキーを共通化した場合，アクセスキー変更時の作業量が膨大となる．

この課題の対応策の一つとして，ゲートウェイ用サーバで RADIUS サーバを稼動させ，キャンパス内の RADIUS サーバとプロキシー接続し，各 AP はゲートウェイ用サーバの RADIUS サーバにアクセスする方法が考えられる．なお，この方法では，各 AP の RADIUS サーバへのアクセス設定はゲートウェイ用サーバで行うこととなる．

6　事例

現在，学内の一部であるがこの手法で AP を設置し，実際に運用を行っている．本章では，提案した構成法を用いた事例をいくつか紹介する．

6.1　AP 設置作業のセンター省力化（図書館）

まず，図書館に設置した際の事例を紹介する．この事例では，装置を図書館の担当者に送付し，設置と設置場所に合わせた設定を図書館の担当者が実施した．

本設置での役割分担は下記のとおりである．

- センター
  - ➢ dhcp・NAT/NAPT 対応で設定済み AP 用 AR を設定

- dhcp・NAT/NAPT 対応でセンター側 AP の設定を追加
- ゲートウェイ用サーバに図書館用 VLAN の設定(dhcp, フィルタリング)を追加

- 図書館
  - AP および AP 用 AR の設置
  - dhcp が使用されていなかった場合の AP 用 AR のキャンパスネットに接続するポートのネットワーク設定

dhcp・NAT/NAPT 対応で設定済み AP 用 AR を設定することで，センターで設置される有線ネットワークの詳細を把握せずに設置することが可能である．また，使用するネットワークで dhcp が使用されていた場合は，ネットワークケーブルと電源の接続のみで稼動させることが可能である．設置した AP と AR のセットを図 5に示す．

また，使用した AR に web ベースインターフェースがあり，これを用いることでポートのネットワーク設定（IP アドレスとゲートウェイアドレスの設定）が比較的容易であった．そこで，設定マニュアルを作成し，詳細な説明を要さず，AP と AR を設置していただけた．

なお，東北大学では VPN 認証の「どこでも TAINS」[6][7][8]と 802.1X を用いた「eduroam」を展開している．また，eduroam は VPN のみ使用を許可する VPN only ポリシーで運用している．VPN サーバをもたなければアクセスができないため，図書館のようにさまざまな人が使用する場では，無線 LAN の恩恵に預かれる人が限定される．そこで，専用の VPN サーバを用意し，図書館でテンポラリアカウントを払い出し，使用していただけるようにしている．なお，VPN サーバのテンポラリアカウントは VPN サーバの web インターフェースにより図書館員に管理していただいている．

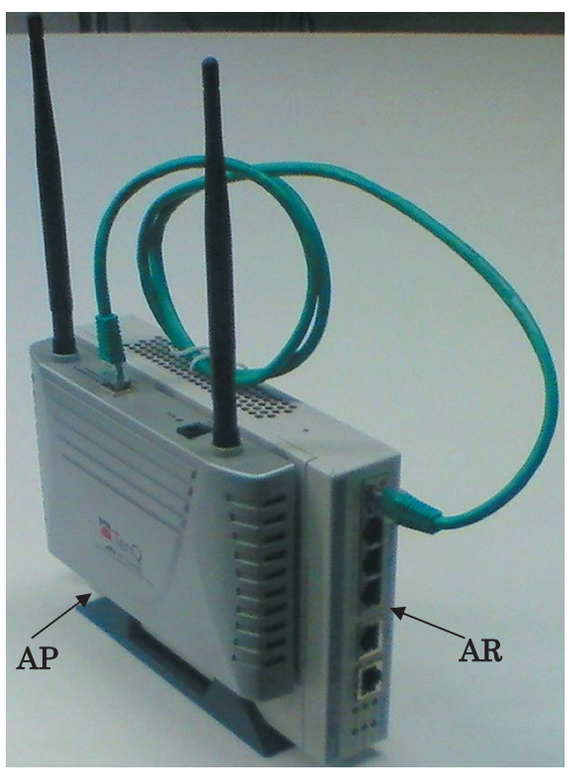

図 5 設置した AP と AR

6.2　VLAN-tag 対応ネットワークでの構築（電気系部局）

次に，電気系部局に設置した際の事例を紹介する．電気系部局では VLAN-tag が使用できるネットワークが構成されていた。

この事例での構成を図 6に示す．VLAN-tag が使用できるエリアに設置する AP 群には，既存のネットワークで使用されていない VLAN-tag を割り当て，1台の AP 用 AR で賄った．

この構成では AP 用 AR を集約でき初期コスト削減が期待できる．

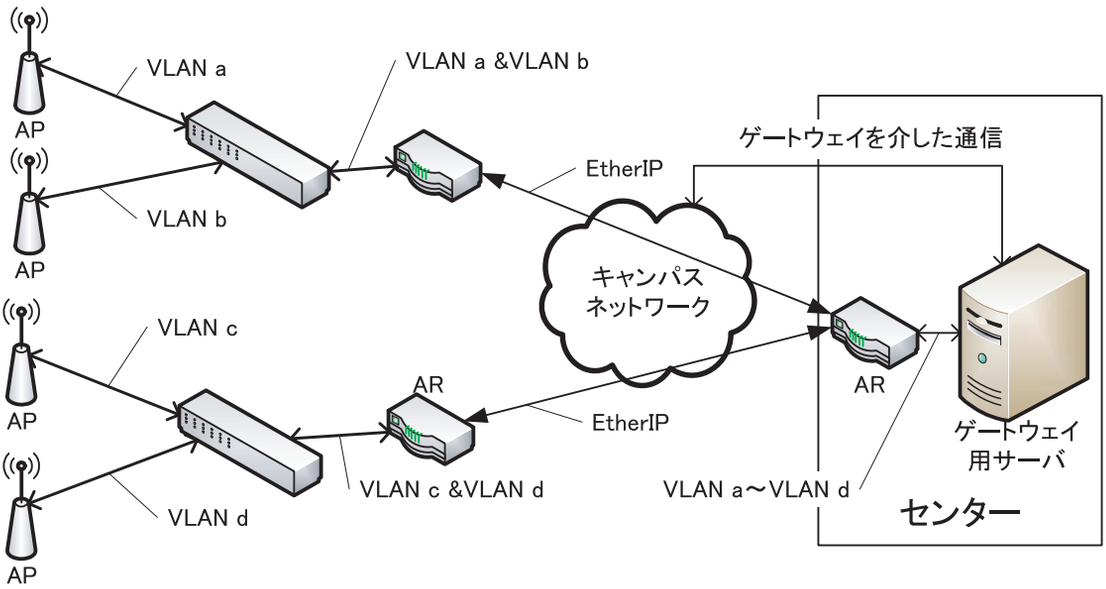

図 6 VLAN 対応 LAN を活用した構成

なお，情報共有等が容易となるため VLAN –tag をフロアー単位で共通化した．

6.3　学外に無線 LAN サービスエリア仮設

本構成の応用事例を紹介する．6.1と同様の構成の AP 用 AR を用い，センター用 AR を The Internet と直接通信できるよう構成することで，学外にある会議場等が有線で The Internet への接続をサービスしていれば，センター管理の無線 LAN サービスエリアを仮設することが可能である．

なお，これを実現する際には，設置先のネットワークで IPSec が通過できる必要がある．また，The Internet をパケットが通過するため，AP 用 AR とセンター用 AR 間を接続する IPSec に関しては暗号化を行うことが望ましいと考える．

7　課題

提案した構築手法を実施したことで見つかった課題を説明する．

- 設置の自由度が高くない
  AP と AP 用 AR をセットで設置するが，AR が IEEE802.3af PoE(Power over Ethernet)による給電に対応しておらず，AP は PoE 対応であるが，AR から AP に PoE での給電ができないため，設置場所に LAN ケーブルの AP 用と AR 用の電源が必要となる．
- IPSec を使用した場合の管理性低下
  dhcp および NAT/NAPT の内側に AP を設置するために IPSec により AP 用 AR からセンター用 AR にコネクションを張ったが，コネクションが確立していない状態では AP および AP 用 AR にセンターからリモートアクセスを行うことができない．これにより管理性が低下する．
- 規模見積もり
  1 台のセンター用 AR およびゲートウェイ用サーバで実運用可能な AP 数は確認していない．設置する AP 数と必要となるセンター用 AR およびゲートウェイ用サーバ数の見積もり手法が必要である．

また，AP 用 AR を LAN に接続しただけで運用ができるところまでは至っていない．今後，これら課題について検討する予定である．

8　まとめ

EtherIP を用いて既設の有線ネットワークを活用しながら，センターで集中管理できる無線 LAN 用の専用ネ

ットワークの構築手法について報告した. また, この手法で dhcp 環境や NAT/NAPT の内側に AP を設置する方法や, 大規模化への対応方法, および, いくつかの事例も報告した.

今後, センター用 AR およびゲートウェイサーバ一台あたりで実運用可能な AP 数の見積もり手法, AP 用 AR をネットワークに接続するだけで無線 LAN 用アクセスネットワークに組み込むことができる AR の設定手法の改良を行う予定である.

参考文献

[1] R. Housley S. Hollenbeck, ``EtherIP: Tunneling Ethernet Frames in IP Datagrams, '' IETF RFC3378, Sep. 2002.
[2] L. Florio, K. Wierenga, ``Eduroam, providing mobility for roaming users,'' EUNIS 2005, June 2005.
[3] 後藤, 今井, 曽根, ``eduroam とキャンパスユビキタスネットワーク,''東北大学情報シナジーセンター TAINS ニュース Vol.34, 2007. (http://www.tains.tohoku.ac.jp/news/news-34/0508.html)
[4] eduroam.jp ポータルサイト: http://www.eduroam.jp/
[5] C. Rigney, S. Willens, A. Rubens, and W. Simpson, ``Remote Authentication Dial In User Service (RADIUS),'' IETF RFC2865, June 2000.
[6] 今野, 水木, 後藤, 曽根, ``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, `` 東北大学情報シナジーセンター大規模科学計算機システム広報 SENAC, Vol.38, No.1, pp.41-45, 2005. (http://www.cc.tohoku.ac.jp/refer/pdf_data/v38-1p41-45.pdf)
[7] 今野, ``TAINS/G における無線 LAN ローミング「どこでも TAINS」について,'' 東北大学情報シナジーセンター TAINS ニュース vol.33,2005. (http://www.tains.tohoku.ac.jp/news/news-33/0309.html)
[8] 後藤, 水木, 曽根, ``無線・有線 LAN ローミングシステム「どこでも TAINS 2」',東北大学情報シナジーセンター TAINS ニュース Vol.33, 2008. (http://www.tains.tohoku.ac.jp/news/news-35/0507.html)
[9] NEC インフロンティア, 「IX2000/3000 シリーズコマンドリファレンスマニュアル 第5版」, Feb. 2008.