岡山大学における認証・ロケーションフリーネットワークの構築

Construction of Location-free Network with Authentication in Okayama University

岡山 聖彦, 山井 成良, 大隅 淑弘, 河野 圭太, 藤原 崇起, 稗田 隆

Kiyohiko Okayama, Nariyoshi Yamai, Yoshihiro Oosumi, Keita Kawano, Takaoki Fujiwara, Takashi Hieda

{okayama,yamai,oosumi,keita,hieda-t}@cc.okayama-u.ac.jp
fujiwara-t4@adm.okayama-u.ac.jp

岡山大学情報統括センター
Center for Information Technology and Management, Okayama University

概要

岡山大学では，2009 年度に旧キャンパス情報ネットワークを更新し，2010 年 6 月から新ネットワーク (ODnet2010) の運用を開始した．ODnet2010 では，ネットワークの高速化・高信頼化に加え，新機能としてフロアスイッチにおけるネットワーク認証とロケーションフリー (認証 VLAN) 機能を導入している．本稿では，セキュアネットワークへの移行の第一段階として構築した，「生活系ネットワーク」と称する認証・ロケーションフリーネットワークについて報告する．生活系ネットワークは，本学の全構成員が利用可能な共通的なネットワークであり，主に講義室や会議室などの共用スペースでの利用を想定している．

キーワード

認証スイッチ, ロケーションフリー, Web 認証, MAC アドレス認証

1 はじめに

岡山大学 (以下，本学という) では，キャンパス情報ネットワークを更新し，2010 年 6 月から新ネットワーク (以下，ODnet2010 という) の運用を開始した．

旧ネットワークは 2002 年 1 月から稼働を開始したものであるが，導入から 8 年が経過して老朽化が進み，ネットワーク機器の故障が頻発するようになっていた．また，旧ネットワークは基幹 1Gbps・支線 100Mbps のネットワークであるが，クライアント PC のネットワークインタフェースがギガビット化し，上位の SINET が 10Gbps 化しようとしている状況では，教育研究を支えるインフラとしての性能不足も懸念されるようになってきた．さらに，旧ネットワークは基本的にグローバル IP アドレスで運用しており，ネットワーク機器が認証機能を持たないため，ネットワークの不正利用や学外からの攻撃に対して無防備であることも問題であった．

このような状況を受け，ODnet2010 では，以下に示す 4 つの目標を掲げて導入を進めた．

1. ネットワークの高速化
2. 信頼性の向上
3. セキュリティの強化
4. 利便性の向上

これらのうち，ネットワークの高速化と信頼性の向上については物理的な特性であり，基幹に 10GbE（支線は 1GbE）を導入し，さらに，ネットワーク機器および回線の冗長化を図っている．

また，セキュリティの強化については，機器をネットワークに接続する際の認証機能を備えたフロアスイッチや，仮想網によるネットワークの分割機能を持つコア

スイッチなど，不正利用を防止とセキュリティインシデントの局所化が可能な機器を導入した．一方，セキュリティの強化はユーザから見ると利便性の低下に繋がるため，本学で導入している統合認証基盤システムとの連携による認証 VLAN 機能や，SSL-VPN サーバの導入により，学内外を問わずロケーションに依存しないアクセス環境の実現を目指した．

フロアスイッチを利用したネットワーク認証機能およびロケーションフリー機能の導入は，本学では初の試みである．ネットワークに接続する際に，ユーザ名およびパスワードの入力が必要であったり，事前に MAC アドレスを登録する必要があったりするなど，従来の利用方法と大きく異なるため，各部局が使用する従来のネットワーク（以下，既設研究系ネットワークという）に全面展開しようとすると，大きな混乱が生じる可能性がある．このため，我々は，本学の構成員全員が利用可能な (共通的な) ネットワークを用意して，講義室や会議室などの共用スペースと，当センターが管理する全学無線 LAN に適用すること移行の第一段階とした．このネットワークは，ある程度の制約があっても，メールや WWW などの一般的なサービスを安心・安全に利用することを想定したものであり，研究のために自由度の高い環境を用意するものではないことから,「生活系ネットワーク」と称している．

一方，生活系ネットワークの適用場所として共用スペースを選んだのは，旧ネットワークでは必ずしも共用スペースの情報コンセントが活用されていなかったためである．旧ネットワークでは，部局からの要望に応じて，建物の各居室のみならず多くの共用スペースにもフロアスイッチからの事前配線（以下，情報コンセントという）を施している．共用スペースの情報コンセントは部局管理としたが，これを教職員や学生などに安全に利用させようとすると，別途認証システムの導入が必要となるなど，情報コンセント活用の妨げとなっていた．このような情報コンセントに対して生活系ネットワークを適用すれば，クライアント PC の接続時にフロアスイッチで認証を行うため，部局から見て余計なコストをかけることなく共用スペースの情報コンセントを利用者に開放することができる．

以下，本稿では，ODnet2010 の概要について述べた後，我々が構築した生活系ネットワークと，構築にあたって生じた技術的課題とその解決策について述べる．

2 ODnet2010 の概要

ODnet の物理構成を図 1 に示す．この図に示すように，ネットワークの高速化に関しては，基幹ネットワーク（コアスイッチ・建物集線スイッチ間，コアスイッチ・データセンタースイッチ間および津島・鹿田キャンパスコアスイッチ間）は 20Gbps （10Gbps × 2 回線），建物内のフロア間（建物集線スイッチ・フロアスイッチ間）は 2Gbps（1Gbps × 2 回線），フロア内の支線ネットワーク（フロアスイッチ以降）は 1Gbps の帯域を確保した．また，信頼性の向上に関しては，コアスイッチの筐体内モジュールの二重化，建物集線スイッチの二重化，基幹ネットワークおよび建物内のフロア間での回線二重化により，主要箇所での単独故障に耐えうる構成になるように設計を行った．

フロアスイッチはいわゆる認証スイッチであり，Web 認証，MAC アドレス認証，IEEE802.1X 認証の機能を有する．Web 認証は主として利用者が接続する端末を認証する場合に用いる．この場合，利用者名としては「user-ID」あるいは「user-ID@VLAN-ID」の形式を用いることができ，前者の場合には標準の VLAN （多くの利用者に対しては生活系 VLAN），後者の場合には指定された VLAN（選択可能な VLAN は利用者毎に異なる）に接続される．一方，MAC アドレス認証はサーバやプリンタなど Web 認証を行えない機器を認証する場合に用いる．この場合には MAC アドレス毎に指定された VLAN に接続される．なお，現時点では IEEE802.1X 認証は利用していない．

3 生活系ネットワークの構築

3.1 旧キャンパスネットワークの問題点

以前のキャンパスネットワーク OUnet3 では，VLAN 機能こそ利用可能であったが認証機能はなく，また VLAN（サブネット）単位で部局に管理権限を委譲していたため，以下に示すような様々な問題が生じていた．

- 各部屋に設置されている情報コンセントに任意の機器を接続して利用できるため，部外者が施錠されていない部屋に侵入し，無断でネットワークを使用する場合があった．
- 無断使用を防ぐためには VLAN 管理者が認証機器を導入する必要があり，導入コストや管理コストの面で普及が進まなかった．特に，共用スペース（講義室や会議室など）の情報コンセントは部局が管理しており，その多くが事実上利用できないように設定されていた．
- 誰が，いつ，どこから，どのような端末を利用しているかを把握することが困難であったため，インシデントが発生した場合に IP アドレスからトラブル発生源となった端末を特定するのにかなりの時間を要した．

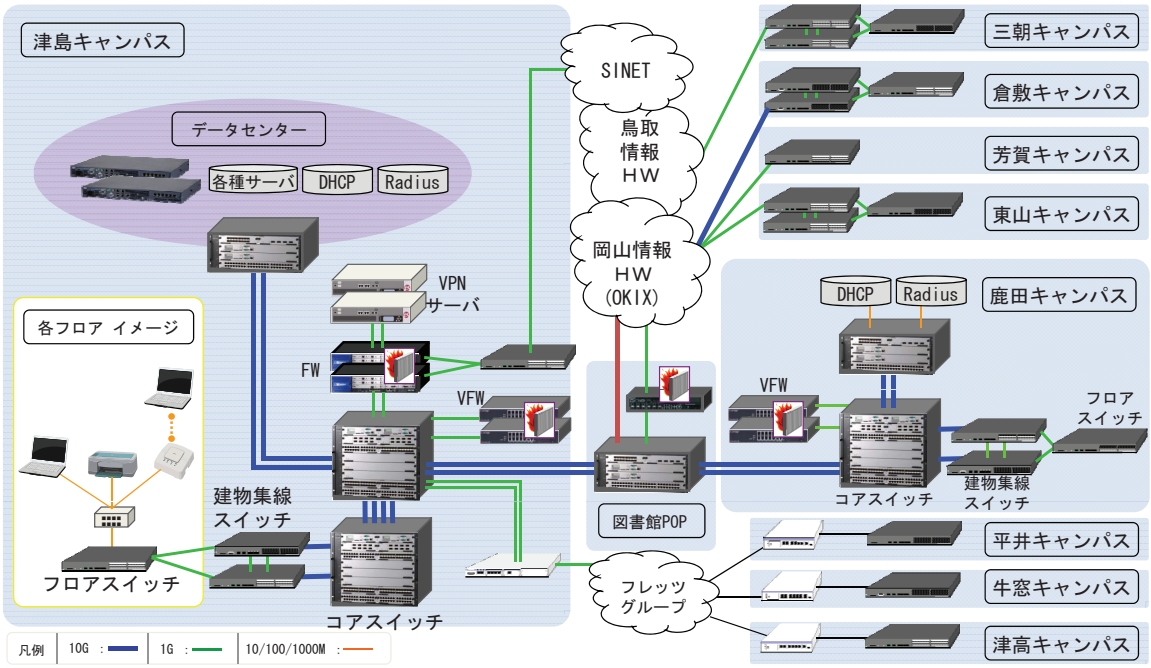

図- 1: ODnet2010 の物理構成

- 基本的に各サブネットにはグローバル IP アドレスを配布していたため，学外から利用者端末に直接アクセスすることができ，ファイアウォール機器があるとはいえ攻撃の対象になっていた．
- 外部からの攻撃に対する安全性を高めるため，部局が独自に NAT ルータを導入してプライベート IP アドレスで運用する場合が増加した．その結果，インシデントが発生した場合に IP アドレスからトラブル発生源となった端末を特定することがさらに困難になった．

これらの問題は，特に管理者がそれほどネットワークに精通していない部局では顕著であり，しばしば問題を引き起こしていた．

3.2 生活系ネットワークの設計

前節で述べた問題点を解決するために，ODnet2010 では新たに生活系ネットワークを構築することにした．生活系ネットワークはプライベート IP アドレスで運用し，IP アドレスは DHCP で自動的に割り当てられる．したがって，生活系ネットワークは部局のネットワーク管理者が関与することなく利用できるようになっている．部局のネットワーク管理者の唯一の役割は，どの部屋で生活系ネットワークを利用できるようにするかを決定することである．

生活系ネットワークでは 10.0.0.0/8 のプライベート IP アドレス空間を用い，次の 4 つのカテゴリーのネットワークを用いている．

- 教員用ネットワーク
- 学生用ネットワーク
- ゲスト用ネットワーク
- 学内共通ネットワーク

これらのうち，教員用ネットワーク，学生用ネットワーク，およびゲスト用ネットワークでは Web 認証が必要で，アクセス可能範囲をキャンパスネットワーク管理者がカテゴリー単位で設定できるようになっている．また，これらのカテゴリーでは利用者の身分および所属により認証後に接続される VLAN が決定されるようになっている．したがって，IP アドレスを見ればサーバではクライアント PC 利用者の所属を判別でき，サーバ側で所属に応じた細かなアクセス制御を行うことができる．

従来の OUnet3 では部外者向け情報コンセントシステム [1] を用い，部外者に対する学内限定情報へのアクセス制御機能を提供していた．これに対して，ODnet2010 では同様の機能をネットワーク側で提供し，生活系ネットワークが利用できる部屋であればどこでも同様のサービスを提供できるようになっている．ただし，従来の部外者向け情報コンセントシステムではクライアント IP アドレスが学内用（150.46.0.0/16）かどうかで学内からのアクセスかどうか判定していたため，サーバの設定は原則として変更する必要がなかったが，ODnet2010 ではどのプライベート IP アドレスがどの身分・所属に対応しているかをサーバ管理者が把握し，適切なアクセス許可範囲になるように設定を変更する必要がある．

一方，学内共通ネットワークはサーバやプリンタなど，Web 認証が困難な機器を収容するもので，MAC アドレス認証を用いる．このネットワークでは接続される機器に応じた VLAN が提供され，たとえばプリンタが接続されている VLAN ではプリンタとは無関係の通信が制限されるなど，機器に応じたアクセス制御が行われる．

4 構築にあたっての課題と解決方法

ODnet2010 の構築にあたり，特に生活系ネットワークが関連する課題がいくつか発生した．本章では主要な課題とその解決方法について述べる．

4.1 ループ検知設定に伴う通信障害

ODnet では生活系ネットワークとして多数の VLAN がキャンパス全体で利用されているため，一部の VLAN でループ接続が発生すると影響がネットワーク全体に波及する可能性が高い．そのため，STP (Spanning Tree Protocol) 等を用いたループ検知機能を活用する必要がある．

ところが，当初の設定では全てのレイヤ 2 スイッチにおいて全ての VLAN に対するループ検知機能を有効化していたため，（レイヤ 2 スイッチ台数× VLAN 数）分のループ検知フレームが全てのレイヤ 2 スイッチに伝送されるようになっていた．その結果，各レイヤ 2 スイッチでは大量のループ検知フレームにより帯域が圧迫されるだけでなく，これらのループ検知フレームの MAC アドレスが全て FDB(Forwarding Database) に登録され，他の端末の MAC アドレスが FDB に登録されなくなり，通信が不安定になる現象が発生した．

この問題に対処するため，我々は当初目標としていた任意箇所でのループの検知を断念し，同一フロアスイッチ内での検知のみを行うように設定した．これにより，ループ検知フレームが他のレイヤ 2 スイッチに中継されないようになり，FDB のオーバフローを抑えることができた．なお，複数のレイヤ 2 スイッチ間を跨ぐループの検知については，STP の代わりにストームコントロール機能を用いて実現している．

4.2 VLAN の切替え

ODnet2010 では前述のように「user-ID@VLAN-ID」の形式で利用者名を指定すると標準以外の VLAN に接続することができる．この機能を有効に活用するには，現在使用している VLAN との接続を一旦終了する機能（ログアウト機能）が必要になる．

ODnet2010 で導入したスイッチでは標準でログアウト機能を有しているため，当初はこの機能をそのまま利用する予定であった．ところが，この機能を利用するには，現在接続している VLAN 内でアクセスできる IP アドレスをスイッチが持つ必要があるにも関わらず，1 台のスイッチで指定できる IP アドレス数に制限があったため，全ての VLAN に IP アドレスを持たせることは不可能であった．

そこで，我々はログアウト専用の Web ページを別に提供することにした．ログアウト処理は以下の手順で行われる．

1. クライアントの IP アドレスをもとに，レイヤ 3 スイッチの ARP テーブルを検索してクライアントの MAC アドレスを特定する．
2. 認証ログをもとに，クライアントが接続されているレイヤ 2 スイッチを特定する．
3. クライアントが接続されているレイヤ 2 スイッチに管理者権限で接続し，当該クライアントの認証を強制的に無効化する．

また，これとは別に，クライアント側ではこれまで割り当てられていた IP アドレスを解放して認証用 VLAN 用の IP アドレスを新たに取得する必要がある．これには利用者側の操作が必要となるが，これを行うプログラムをログアウト用ページで提供し，事前にダウンロードできるようにしている．

4.3 Web 認証と MAC アドレス認証の併用

生活系ネットワークでは特に必要ではないが，研究系ネットワークの中には Web 認証や MAC 認証では不十分で，より強力な認証を必要とするものがある．これは，単なる Web 認証ではパスワードの漏洩に耐性がなく，また単なる MAC アドレス認証では端末を誰が使用したか特定できないためである．そこで，Web 認証と MAC アドレス認証の両方に成功した場合に限りネットワークアクセスを認める認証機構を一部の研究系ネットワークに導入するようにした．

ODnet2010 で導入したレイヤ 2 スイッチではこのような認証（多段認証）に対応できない[1]ことから，我々は認証システムに一部修正を加えてこの機能を実現した．このようなネットワークに接続可能な端末は MAC アドレスの事前登録時に接続先として特別な VLAN を割り当てる．この VLAN は実在しないものであり，結果として MAC アドレス認証には失敗して Web 認証に移行するが，その際に端末の MAC アドレスが認証シス

[1] 最近のレイヤ 2 スイッチでは対応済み

テムに通知される．その後，接続先 VLAN が多段認証を必要とするものであれば，Web 認証時に認証システムが MAC アドレスの照会を行い，接続の可否を決定する．

5　まとめ

本稿では岡山大学新キャンパスネットワーク ODnet2010 において新たに導入した「生活系ネットワーク」の構築方法に関して報告した．生活系ネットワークはキャンパス内のどこからでもアクセスが可能なネットワークであり，身分や所属に応じたキャンパスワイドの VLAN を構成することにより実現している．2011 年 7 月 14 日現在，フロアスイッチのポート数で 501 個のポートが生活系ネットワークに移行しており，これは使用済みポート数の約 1 割にあたる．今後は生活系ネットワークへの移行を進めるとともに，旧研究系ネットワークの移行も順次進めていきたい．

参考文献

[1] 山井成良, 岡山聖彦, 木澤政雄, 土居正行, 河野圭太, 大隅淑弘: 部外者からの組織内限定サービスへのアクセスを保護する LAN アクセス制御システム, 情報処理学会論文誌, vol.48, no.4, pp.1573–1583 (2007-04).