Vol.2013-IOT-20 No.10
2013/3/14

岡山大学における大規模認証ネットワークの運用と課題 *1

山井 成良[1,a)]　岡山 聖彦[1]　大隅 淑弘[1]　藤原 崇起[1]　河野 圭太[1]　稗田 隆[1]

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，「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の運用方法を報告し，また運用の過程で明らかになった課題を議論する．

キーワード：
キャンパスネットワーク，認証ネットワーク，動的 VLAN

Operation Issues of Large Scale Authentication Network in Okayama University

Nariyoshi Yamai[1,a)]　Kiyohiko Okayama[1]　Yoshihiro Ohsumi[1]　Takaoki Fujiwara[1]
Keita Kawano[1]　Takashi Hieda[1]

Abstract:
We replaced Okayama University Campus Information Network in 2009 fiscal year, and have operated the new network called ODnet2010 since June 2010. ODnet2010 not only improves its bandwidth and reliability, but also provides some new functions such as user authentication by floor switches, location-free function for VLANs. In this paper, we explain the operation of authenticated location-free VLANs called "Living Networks", and discuss some issues experienced during the operation.

Keywords: campus network, authentication network, Dynamic VLAN

1. はじめに

岡山大学（以下，本学）は学生数約 14,000 人，教職員数約 2,600 人，11 学部を擁する，地方大学としては比較的大規模の総合大学である．主要なキャンパスとしては岡山市内の津島キャンパス（医療系を除く学部，情報統括センター，事務局など），鹿田キャンパス（医療系学部，岡山大学病院など），東山キャンパス（教育学部附属学校園），倉敷市の倉敷キャンパス（資源植物科学研究所など），鳥取県三朝町の三朝キャンパス（地球物質科学研究センター，岡山大学病院三朝医療センター）がある．

本学では，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 では旧ネットワークで問題となっていた (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) 利便性の向上の 4 項目を目標に掲げて設計を行った．特に (3)，(4) については Web 認証に基づいてアクセス制御機能を行い，また認証されたユーザの属性に応じて接続先 VLAN を動的に決定するようなネットワーク（生活系ネットワーク）を導入し，ロケーションフリー，すなわちキャンパス内ではユーザの場所に依存しないで同一の条件で利用できるアクセス環境の提供

[1] 岡山大学情報統括センター
Center for Information Technology and Management, Okayama University
3-1-1, Tsushima-naka, Kita, Okayama 700–8530, Japan
[a)] yamai@okayama-u.ac.jp

を目指した [1].

現在，ODnet2010 では従来の認証を要しないネットワークから新しいネットワークへの移行を進めている最中である．しかし移行過程において，スケーラビリティを十分に考慮して設計していなかった，機器や端末の動作を十分に理解していなかった，あるいは機器や端末の持つ脆弱性が顕在化したなどの理由により，導入当初には想定していなかった様々なトラブルが露見するようになった．これらのトラブルには設計や運用の見直しにより対処できたものもあれば，未だに原因が不明であるものや，原因は判明しているものの対処方法が不明であるものが多数存在する．

そこで本稿では ODnet2010 の設計や運用を示したうえで，現在までに発生している様々なトラブルを示し，把握している範囲でその原因や対策手法を紹介する．なお，誌面の都合上，主要なトラブルのうちのいくつかについては稿を改めて紹介する．

2. ODnet2010 の構成と運用

2.1 ODnet2010 の概要

ODnet2010 の物理構成を**図 1** に示す．前節で述べた 4 つの目標を実現するため，ODnet2010 では以下のような構成を採用した．

まず，ネットワークの高速化を図るため，ODnet2010 では基幹ネットワークのうちコアスイッチと他の機器との間（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），それ以外の建物集線スイッチ・フロアスイッチ間は 2Gbps（1Gbps × 2 回線）とし，従来の 1Gbps と比較するとそれぞれ 20 倍，2 倍の帯域を実現した．また，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，従来の 100Mbps の 10 倍の帯域を実現した．

次に，信頼性の向上を図るため，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を行い，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．また，津島・鹿田キャンパス間の接続回線も二重化されているほか，図 1 には示されていないが，従来から津島・三朝キャンパス間接続や SINET との接続も二重化されている [2].

セキュリティの強化については，フロアスイッチに Web 認証，MAC アドレス認証などの認証機能を有する機器（認証スイッチ）を導入して，ネットワーク利用時に必ず端末認証を行わせるようにした．また，レイヤ 3 スイッチは津島，鹿田，倉敷，三朝，東山の各キャンパスに導入しているが，そのうち津島，鹿田キャンパスのコアスイッチには仮想網によるネットワークの分割機能（VRF: Virtual Routing and Forwarding）を有する機器を導入し，各サブネットの利用目的に応じて他のネットワークと分離できるようにしている．

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（ロケーションフリーネットワーク）の実現を目指した．また，ロケーションフリーネットワークのうち，主として講義室や会議室などの共用スペースや情報統括センター（以下，センター）が管理する全学無線 LAN など，構成員全員が利用する可能性があるサブネットや，特に文系学部のように専らユーザ端末を接続するためのサブネットについては，センターがユーザの属性（所属や身分）に応じたプライベートネットワークを「生活系ネットワーク」として提供し，ユーザ認証時のデフォルトネットワークとして利用できるようにしている．また，生活系ネットワーク以外のネットワーク（研究系ネットワーク）にも VLAN 番号を認証時に「user@VLAN-ID」の形式で指定することにより接続できるようにしている．

2.2 認証ネットワークの運用

前節で述べたように，ODnet2010 では生活系ネットワークと呼称する認証ネットワークを導入している．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．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．設定された VLAN は生活系ネットワークだけで 450 種類以上になる．さらに，電子ジャーナルなど場所に応じたサービスを提供するために，倉敷，三朝，東山キャンパスの生活系ネットワーク用 VLAN は VLAN-ID 変換を行ったうえで津島キャンパスのレイヤ 3 スイッチに収容されており [3]，研究系ネットワークを含めると各スイッチには仕様上利用可能な 4096 のうちの大半が設定されている．

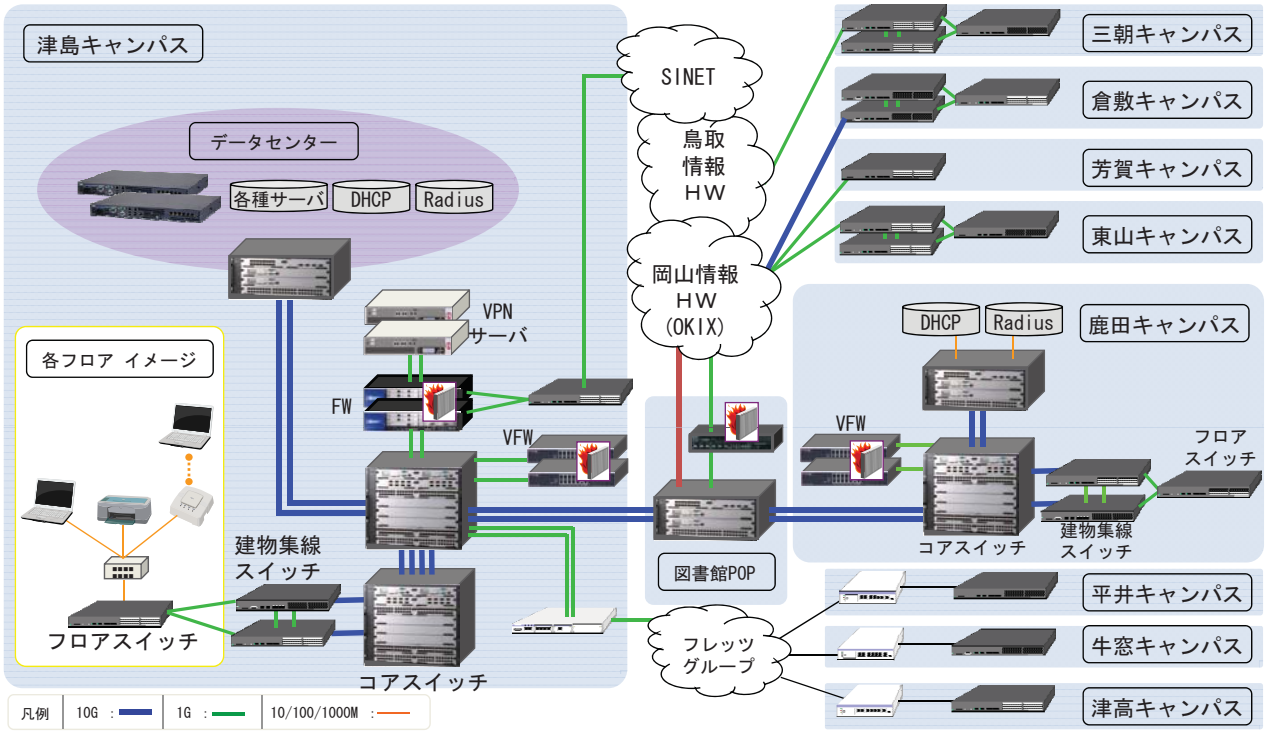

図 1 ODnet2010 の物理構成

生活系ネットワークや研究系ネットワークとは別に，各フロアスイッチには Web 認証を行うための特別の VLAN（認証前 VLAN）が必要である．この VLAN では DHCP により認証用の IP アドレスが一時的に提供される．端末が生活系ネットワークを利用する場合の動作手順を以下に示す．

(1) ユーザ端末はフロアスイッチに接続されると DHCP サーバから認証用 IP アドレスを取得する．
(2) ユーザ端末は Web ブラウザで任意のページにアクセスを行う．フロアスイッチはこのアクセスを Web 認証サーバにリダイレクトする．Web 認証サーバは認証ページを Web ブラウザに表示し，ユーザ名とパスワードの入力を求める．
(3) ユーザはユーザ名とパスワードを入力する．必要であればユーザ名の一部として接続先 VLAN を指定する．Web 認証サーバはユーザ認証を行い，接続先 VLAN が指定されていた場合にはその VLAN へのアクセス権限も確認したうえで，フロアスイッチと協調して指定された VLAN に接続する．接続先 VLAN が明示されていない場合にはユーザの身分や所属に応じた生活系ネットワークに接続する．
(4) ユーザ端末は認証用 IP アドレスのリース切れにより IP アドレスの再取得を試みる．DHCP サーバは新たな VLAN 用の IP アドレスを割り当て，ユーザ端末はこれ以降自由にネットワークにアクセスできるようになる．
(5) ユーザ端末はネットワークから切断する際にログアウト処理を行う．ログアウト処理では端末の 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 アドレスを特定し，さらに認証ログをもとに端末が接続されているレイヤ 2 スイッチを特定したうえで，そのスイッチの認証情報を強制的に無効化する方法を用いている．

3. 大規模認証ネットワーク運用における課題

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．本節では主要な課題とその解決方法について述べる．

3.1 ループ検知設定に伴う通信障害

ODnet2010 では前節で述べたように各スイッチには多数の VLAN が設定されているため，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．そこで，ODnet2010 の当初の設計では，STP（Spanning Tree Protocol）等を用いたループ検知機能を全てのレイヤ 2 スイッチにおいて全ての VLAN に対して有効にしていた．ところがこの設定では各レイヤ 2 スイッチが各 VLAN に関してループ検知フレームを送出するため，全体では（レイヤ 2 スイッチ台数 × VLAN 数）分のループ検知フレームが伝送されることになる．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）に登録されたため，FDB がオーバフローに陥り，他の端末の

MAC アドレスが FDB に登録されなくなって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．

3.2 VLAN 切替え時の問題点

認証ネットワークでは短時間で認証前 VLAN から生活系ネットワークへの切替えが発生する．このことが原因で発生したと思われるトラブルがいくつか散見される．

一部のパーソナルファイアウォールを導入した PC では，時折アクセスが極端に遅くなる現象が発生した．原因が特定できたわけではないが，他のパーソナルファイアウォールに変更したところ現象が収まったため，パーソナルファイアウォールに原因があると思われる．タイミング等の影響を受けるためか，再現性に乏しいが，未確認情報として短期間で端末の IP アドレスが変更されたためにパーソナルファイアウォールが新しいアドレス宛のパケットを攻撃と誤認識し，そのために検査が厳格になった可能性がある．

逆に，端末側が IP アドレスの変更を短期間では行えないために発生したトラブルもある．特に MacOS X では DHCP のリース時間（10 秒）より長い間隔でアドレス更新要求を送信するため，認証成功後に実際にネットワークが利用できるようになるまでしばらく待たされる問題が発生している．また，ODnet2010 では認証時に接続先の VLAN をユーザが選択することができるため，たとえば生活系ネットワークに接続した後，必要に応じて研究系ネットワークに切り替えたい場合がある．ODnet2010 では認証ネットワークのログアウト機能を提供しており，ユーザはこの機能を用いて現在のネットワークから一旦ログアウトしたうえで新しいネットワークに再接続することになる．ところが，一部の端末ではログアウト後に再度認証 VLAN に切り替える際に DHCP により割り当てられた IP アドレスのリース切れ（最大 10 分間）まで認証用 VLAN の IP アドレス割当てを行うことができず，円滑に新しいネットワークにアクセスできないという問題が発生している．これに対してはアドレスの再取得を行うバッチプログラムの配布により対処しているが，機種によってはこのプログラムが利用できず，再起動や LAN ケーブルの抜き差しを必要とするものがある．

この他にも認証ネットワークへの移行に伴い，以下のような問題が発生している．

- Windows7 では Web 認証成功後も「ネットワークと共有センター」のインターネットアイコンの前に×印が表示される現象が時折発生している．ネットワークの利用には支障がないが，原因や対策は現在のところ不明である．
- 一部のプリンタは DHCP で提供するデフォルトゲートウェイが反映されず，これを手作業で設定する必要があった．
- ユーザが認証前に HTTPS で通信を行う場合，認証スイッチが認証ページへのリダイレクトを行うが，その際に認証スイッチ自身が持つ証明書を用いる．この証明書は本来のアクセス先のものとは異なるため，端末側では警告画面が表示され，仕組みをよく理解していないユーザは混乱する．
- Web 認証はフロアスイッチが直接行うのではなく，共通の Web 認証サーバへのリダイレクトを行っているだけである．しかし，フロアスイッチでは端末との間で認証用セッションを維持しているため，特に学会等のイベント開催時に多数の未認証端末から同時に接続があると，セッション数が超過して認証ができなくなる場合がある．これに対しては，セッション維持時間を調整するとともに，リダイレクトを用いずに Web 認証サーバに直接アクセスさせるような手順書を作成して対処した．

3.3 認証スイッチの動作に起因する問題点

認証スイッチは端末が送信するフレームをその MAC アドレスに応じて適切な VLAN に中継するため，異なる VLAN に属する複数の端末を 1 つの物理ポートに接続することができる．ところが，逆に認証スイッチから物理ポートにフレームを送信する場合には，認証スイッチは VLAN を意識しない動作を行う．すなわち，ある VLAN に属するフレームを認証スイッチが物理ポートに送出する場合，そのフレームの属する VLAN がその物理ポートで利用可能であれば，各端末の属する VLAN とは異なる場合でも中継するように動作する．ODnet2010 ではこの動作に起因する多数の問題に遭遇した．

たとえば，端末が認証前 VLAN において認証後に割り当てられる範囲の IP アドレスを手動で設定すると，認証を行っていないにもかかわらず通信が行えるというトラブルが見つかった．これは**図 2** に示すように，端末からの誤った送信元 IP アドレスを持つパケットは L2 スイッチでは認証前 VLAN（VLAN100）経由で L3 スイッチに中継されるが，L3 スイッチからの誤った宛先アドレスを持つパケットは宛先アドレスに対応する VLAN（VLAN200）に送出され，認証スイッチでは端末が接続されている物理ポートにこのパケットを中継する [*1]．このため，往復のパケット

[*1] 実際にはパケット送出前に ARP によるアドレス解決が行われるが，同様に通信が成立する．

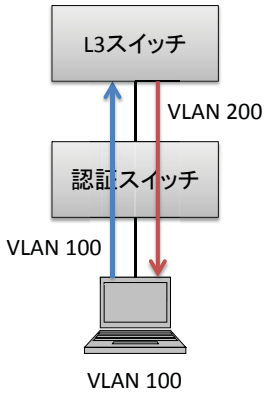

図 2 認証スイッチの中継動作

が経由する VLAN が異なるにもかかわらず，通信が成立する．このような通信を防止するため，L3 スイッチでは各 VLAN に対して誤った送信元アドレスを持つパケットを破棄するような設定を追加している．

認証スイッチのこのような動作により発生したトラブルは他にも以下に示すように多数発生している．

- ある端末が SSDP（Simple Service Dicsovery Protocol）による機器探索用マルチキャストパケットを送出すると，このパケットがその端末の属する VLAN を利用可能な全ての物理ポートに到達する．このパケットは他の VLAN に属する端末でも受信され，その応答についても同様に他の VLAN でも受信できるため，結果としてネットワークコンピュータ及びプリンタ一覧に膨大な機器が表示される．
- Apple 社 Time Capsule や AirMac のうち，未設定状態のものがいずれかの VLAN 上に存在すると，上記と同様の動作により他の VLAN に属する Mac 系端末がこれを検出し，初期セットアップウィザードを表示する．
- 無線ルータを運用しているユーザが認証ネットワークに接続する場合，配下の個々の端末を認証するために無線ルータをブリッジモードで利用する必要がある．しかし，無線ルータをブリッジモードで利用すると，アップリンク（認証スイッチ側）から送られてくる大量のブロードキャスト（マルチキャスト）フレームを受信して送信元 MAC アドレスを学習しようとしてリソース不足になり，正常に動作しなくなる．これは WAN ポートではなく LAN ポートをアップリンクに接続することで回避できるが，無線ルータのデフォルト IP アドレスが重複する，DHCP サーバとして動作した場合に全学に影響を及ぼす，などの問題が新たに発生する．
- 無線ルータの UPnP（Universal Plug and Play）機能が有効になっていると，上記のように他の VLAN を含めてネットワーク上の全ての対象機器を認識し，リソース不足に陥り 10 秒程度の間隔で再起動を繰り返すものがある．
- 実際には運用していないにもかかわらず，IPv6 関連のマルチキャストパケットによるトラフィックが相当量を占めるようになっている．このため，特に無線ルータ配下の端末では動作が遅くなる現象が確認されている．また，実際に IPv6 を運用を開始した場合，端末は各 VLAN に対する RA（Router Advertisement）を全て受信し，それぞれに対して IP アドレスを割り当てるように動作すると予想され，事実上 IPv6 を運用することができない．
- 一部のブロードバンドルータで IPv6 マルチキャストパケットを WAN ポートで受信すると，これを LAN ポートだけでなく WAN ポートにも中継する（折り返す）製品が存在する．このような製品が認証スイッチに接続されると，ある端末が送信した IPv6 マルチキャストパケットが当該製品からも送出され，同一の端末が 2 か所で接続されているように誤認識される場合があった．これにより，この端末でログアウト操作を行っても当該製品が接続されている認証スイッチの認証テーブルがクリアされ，端末では再認証が行えない場合が生じた．

これらの問題に対する対策として，現在のところ認証スイッチにおいて IPv6 パケットのフィルタリングを行っており，一定の効果が得られている．ただし，根本的な解決策ではないため，今後対応策を検討する予定である．

なお，認証スイッチの最新の OS では正当な受信者が存在しない物理ポートへの送出を抑制する機能が追加されており，その機能の導入も検討する予定である．

4. まとめ

本稿では岡山大学における新キャンパス情報ネットワーク ODnet2010 について，特に「生活系ネットワーク」と呼称している認証・ロケーションフリーネットワークの設計と運用を紹介した．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．生活系ネットワークにより利便性が向上した半面，VLAN 数が大きく，また 1 つの VLAN がキャンパス全体にわたって構築されているという特徴に起因して発生した問題も多く経験してきており，一部は未解決の状態である．

現在，ODnet2010 は旧研究系ネットワークから生活系ネットワークへの移行を継続して実行しているが，生活系ネットワークに移行した端末が増加するに従って新たなトラブルが発生している．このようなトラブルについては，稿を改めて紹介するとともに，問題の解決に向けた検討を継続して行っていく予定である．

参考文献

[1] 岡山聖彦, 山井成良, 大隅淑弘, 河野圭太, 藤原崇起, 稗田隆: “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”, 学術情報処理研究, No.15, pp.161–165, 平成 23 年 9 月.
[2] 山井成良, 岡山聖彦, 金勇, 河野圭太, 大隅淑弘: “岡山大学における地域 IX と SINET を利用したネットワーク冗長化”, 情報処理学会インターネットと運用技術研究会研究報告, 2009-IOT-004-20, pp.113–118, 平成 21 年 3 月.
[3] 大隅淑弘, 岡山聖彦, 山井成良, 藤原崇起, 稗田 隆: “電子ジャーナルの地理的なサイトライセンス契約条件に適応するロケーションフリーネットワークシステム”, 情報処理学会インターネットと運用技術研究会インターネットと運用技術シンポジウム 2011 論文集, pp.51–58, 平成 23 年 12 月.