Vol.2010-IOT-10 No.2
2010/7/16

福井大学学内ネットワークシステムの設計と構築

大垣内 多徳[†2,†1] 半田憲嗣[†1] 澤田雅子[†1]
福井一俊[†3,†1] 山下芳範[†2,†1]

福井大学では 2003 年の旧福井大学と旧福井医科大学の統合後，初のネットワークの更新を行った．更新を機会に医学部附属病院を含む全学のネットワークを総合情報基盤センターで一括して運用管理を行うこととし，各部局のセキュリティポリシーを考慮しつつ，高可用性と低運用コストを実現するようなネットワークの設計を行い運用を開始したので報告する．

Campus Network System in the University of Fukui

Tatoku Ogaito,[†2,†1] Noritsugu Handa,[†1]
Masako Sawada,[†1] Kazutoshi Fukui[†3,†1]
and Yoshinori Yamashita[†2,†1]

The University of Fukui has finished the first Campus LAN update after the integration of the former Fukui University and Fukui Medical University. We think this update is an opportunity for changing the campus LAN management policy and the Center for Information Initiative (CII) takes the responsibility of managing the whole campus LAN including the University Hospital. We have designed the new network system with following points: 1) Taking account of the security policy of each faculty. 2) Keeping high availability as an information infrastructure. 3) Keeping management cost as low as possible. In this paper, we introduce our new campus LAN system and some evaluation after the implementation.

1. はじめに

福井大学は，教育地域科学部，工学部からなる旧福井大学と医学系単科大学であった旧福井医科大学が 2003 年 10 月に統合した，2 キャンパス合わせて学生数 5,000 人，職員数 2,700 人 (医学部附属病院職員を含む) を擁する地方大学である．

統合後も，学内ネットワークは，文京キャンパス (旧福井大学) は 2001 年に，松岡キャンパス (旧福井医科大学) は 2002 年に更新されていたため，キャンパスごとに異なる運用形態を継続していた．

文京キャンパスでは，総合情報基盤センターは各建物に設置されている L3 スイッチまでの幹線だけを管理しており，それ以外のネットワーク配線，機材や，IP アドレスやホスト名の資源管理は各部局で行われていた．一方，松岡キャンパスでは元々が医学系単科大学であったこともあり情報処理センター (当時) が附属病院内を含む各部屋設置の情報コンセントまでのキャンパス内のネットワーク全体を管理していた．

しかし，文京キャンパス内の多くの部局からネットワークの運用管理に費やす人的コストの負担低減を求められたこともあり，2009 年度に行った全学キャンパスネットワーク更新のタイミングで，総合情報基盤センターが全学ネットワークの資源管理および，各部屋の情報コンセントまでの配線/機材管理を行うよう運用方針を変更した．

これにより，利用者の負担低減をはかるとともに，学内全てに対して同等な品質によるネットワークサービスの提供を実現している．

本稿では，高可用性と低運用コストを同時に実現するための設計と構築について概説し，現在までの運用について評価する．

2. 情報基盤としてのネットワーク (冗長構成)

今回のネットワーク構築にあたり，学内のコンピュータネットワークを，研究・業務を遂行するために必要不可欠な情報基盤としてとらえ，重点目標の一つとして無停止運用を実現するための冗長化設計をおこなった．(図 1)

†1 福井大学総合情報基盤センター
Center for Information Initiative, University of Fukui
†2 福井大学医学部附属病院医療情報部
Department of Medical Informatics, University of Fukui Hospital
†3 福井大学工学研究科電気・電子工学専攻
Electrical and Electronics Engineering, Graduate Schoold of Engineering, University of Fukui

Vol.2010-IOT-10 No.2
2010/7/16

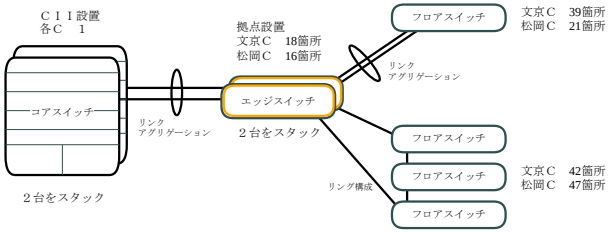

図 1　冗長化構成

幹線については総合情報基盤センターに設置するコアスイッチおよび各拠点に置かれるエッジスイッチについては機能をすべて冗長化する事，さらに運用面を考慮して冗長化を構成する物理的に複数の機材は論理的には一台として取り扱えることを仕様として要求した．入札の結果，コアスイッチとしては Cisco 社の Catalyst 6509 2 台を VSS(Virtual Switching System) を用いて 1 式の仮想スイッチとしたものが，エッジスイッチとしては Allied Telesis 社の AT-X900-12XT/S 2 台を VCS(Virtual Chassis Stacking) を用いて 1 式の仮想スイッチとしたものが導入された．これらの技術を利用した仮想スイッチ構成では，物理的に異なる筐体に属するポート間でリンクアグリゲーション (IEEE 802.3ad) を行うことが可能であるため，拠点との経路については関係するスイッチもしくはケーブルのいずれか一つが動作しなくなった場合でも，通信断は発生しない．

一方，各フロアに配置されるフロアスイッチとエッジスイッチの間の接続については，フロアスイッチの設置数によって冗長化の方法を選択した．

複数台のフロアスイッチが配置されるフロアについては，任意のフロアスイッチ 1 台もしくは任意のケーブル 1 本が障害をおこし利用不能となっても，稼働中のフロアスイッチはサービスを継続できるよう，リング構成とした．その際，リングの構成管理にはスパニングツリー (IEEE 802.1D) ではなく，EPSR (RFC 3619) を採用した．これは，スパニングツリーでは収束までの時間が比較的長いことと正しく運用管理 (コスト計算) を行う事が可能な人的リソースが不足していたためである．特に医学部附属病院内においては，スパニングツリーが動作した場合の数十秒間のネットワーク停止により，病院情報システムがデータベースロックを起こす等の問題が報告されていた．これと比較して，EPSR では，切替時間が 1 秒未満で済むことや設定方法の大幅な簡素化が実現されている．

他方，もともと 1 台しか配置されないフロアについては，そのフロアスイッチが故障した場合，サービス不能となることに変わりはなく，ケーブル障害に対しての冗長化を考えればよいため，リンクアグリゲーションを用いた．

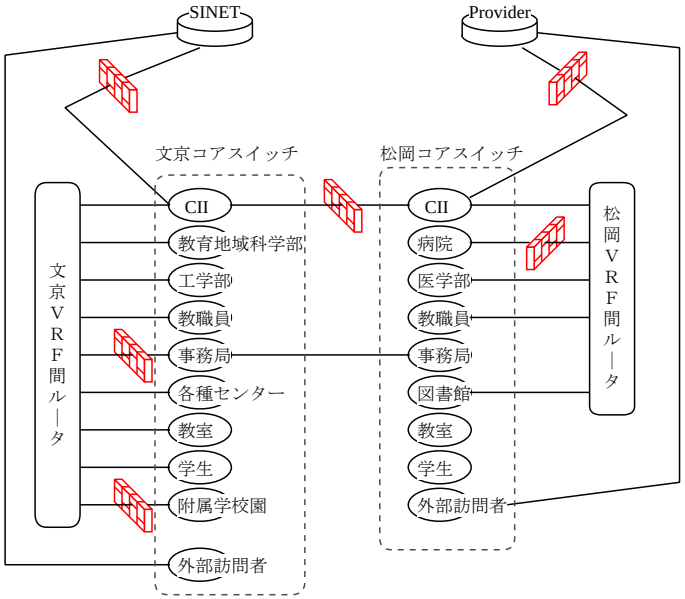

図 2　論理構成

3. 様々な要請に応える論理設計

3.1 センタールーティングへの移行

更新前のネットワーク構成では，両キャンパスの総合情報基盤センターにそれぞれセンタースイッチが，キャンパス内の拠点 (文京キャンパス 18ヵ所，松岡キャンパス 17ヵ所) に L3 スイッチがエッジスイッチが配備されエッジルーティングを行っていた．

エッジルーティングは，その配下で閉じるような通信が多い場合には有効であるが，そうでない場合は結局センタースイッチ位置でのルーティングが必要となることとなる．

一方，運用管理を行う立場からみるとエッジルーティングは，複数拠点にまたがる VLAN のルーティングポイントの選択/設計や，運用開始後の MAC アドレスと IP アドレスの対応確認作業におけるコスト高の原因となる．

そこで，今回のネットワーク設計では，各キャンパスごとにセンタールーティングを行う

ことを基本[*1]とした．

3.2 VRF による論理ネットワークの分割

福井大学では 2009 年度に大学としての指針であるセキュリティポリシーが制定され，現在各部局の特性を考慮した運用規程を作成している．この中で規定されるセキュリティレベルが異なる部局間は直接通信ではなく適切なフィルタリングを行うことが可能である必要がある．つまり，センタールーティングとは言っても，キャンパス内すべての VLAN が相互に無条件で通信できるわけではないため，コアスイッチには「仮想ルータ」機能を仕様として要求した．各キャンパスのコアスイッチ上には，図 2 に示す仮想ルータを VRF(Virtual Routing and Forwarding) を用いて構築している．

仮想ルータ間のルーティングについては，別筐体として「VRF 間ルータ」を用意した．これにより，コアスイッチと VRF 間ルータの間に，セキュリティレベルがより高い部局が独自管理のファイアウォールを導入する事を容易としている．

3.3 利用者からの希望に対する柔軟な構成変更

文京キャンパスでは，拠点設置のエッジスイッチより下流側の部局内ネットワークについては，総合情報基盤センターが介入することはなく自由に配線変更や設定変更が行われていた．その結果，ケーブル配線が複雑となり，担当者が離学したような場合後任の担当者が状況把握に手間取り，ときにはネットワーク障害を引き起こす事例も観察された．

今回のネットワークでは，末端のフロアスイッチまで VLAN 機能を有功としたため，物理的な配線変更ではなく論理的な設定変更で対応することが可能となった．利用者としては，センターに依頼するという手続きが新たに必要ではあるが，従来困難であった異なる建物に分散した研究室や実験室であっても同一ネットワークとしての利用が可能となった．

3.4 両キャンパスにまたがる部局の取扱い

従来は各キャンパスは独立して運用していたため，両キャンパスにまたがる部局は相互通信が困難な状態にあった．特に文京キャンパスから松岡キャンパス内に設置されているサーバにアクセスする事は不可能であり，松岡キャンパスから文京キャンパスへのアクセスについても多くの制限が課せられていた．その制限を回避するためだけに，両キャンパス間に VPN 装置を対向で設置するような利用も見られた．

新ネットワークでは，各キャンパス内に構築された VRF 間を相互に接続する事で容易に両キャンパスにまたがる論理ネットワークの構築が可能となった．これにより，統合時より事務局からでていた単一ネットワークでの運用という希望を実現できることとなった．

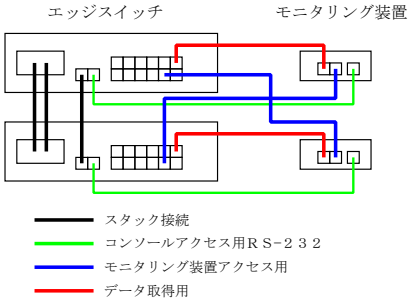

図 3 モニタリング装置の接続

4. 運用コストを低減するために

4.1 スイッチへのアクセス管理

すべてのスイッチは freeRADIUS[1)] を用いて福井大学統一認証システム [9,10)] と連携させ，総合情報基盤センターのネットワーク運用担当関係者のみ login できるように設定してある．これにより，担当者は新たなパスワードを覚える必要がなくなった．さらに，システム管理上も，各人に付与する権限管理が RADIUS サーバ上でできるようになるとともに，人事異動等が発生した場合であっても全スイッチの設定変更を行う必要がなくなるなど運用コストの低減が実現されている．

4.2 リモートコンソール接続/監視端末

従来，障害発生等のネットワーク異常時には，現場に相応の知識を有する担当者が赴き，スイッチ等の設定を確認したり，必要な設定変更を行った上でパケット採取等の作業を行う必要があった．このため，人的資源が不足した状況では，障害発生時に必要な情報収集が行われずに単に機器のリセットを行う等の対処療法的な対応が行われ同様な障害を繰り返す傾向が見られた．

今回我々はすべてのエッジスイッチ位置にモニタリング装置として Plathome 社の OpenBlockS600 を 2 台づつ導入している．OpenBlockS600 では 2 つの NIC および console 用とは異なるシリアルポートが 1 つ利用可能である．これらのポートを図 3 のようにエッジスイッチと接続することで，VCS による仮想スイッチを構成するいずれかの筐体に異常が生じた場合であっても，当該筐体のコンソールにアクセスすることや，任意のポートに流れる

⋆1 AT-X900-12XT/S は IPv4/IPv6 ともルーティングすることが可能である．

パケット採取をリモートから可能なようにしている．また，これらを監視プログラム [6] で監視対象として設定することでエッジスイッチ直下までの可用性について常時把握している．

さらに，ネットワーク障害が重要な影響を与えるような箇所においては各フロアに OpenBlockS600 を 1 台配置し，これらも監視対象として利用することで障害発生から復旧まで対応時間の短縮を目指している．

5. 多様な利用形態への対応

5.1 IPv6

「次世代ネットワーク」として提唱されている IPv6 についても新ネットワークでは全学を対象としてサービスを開始している．

松岡キャンパスでは早くから導入されているものの，世界的に導入が進んでいないこともあって文京キャンパスでは導入されていなかったが，2011 年度中には新規の割り当てが停止される事が予想されている事もあり，全学でのサービスに踏み切った．

5.2 無線環境の拡大整備

従来，松岡キャンパスでは病院内を中心として無線 LAN サービスが導入され，ベッドサイドにおける患者情報入力等に利用されていた [4,5]．安定した無線 LAN 環境を維持するためには，アクセスポイント間の干渉を考慮した適切なチャネルプランを行う事が必要であるとともに，配置後に実際の無線環境の調査を行い適切な位置へとアクセスポイントを移動させることが重要であった．また，接続機の中にはローミング処理が適切に行われないものもあり，機器の移動により無線接続が切断されるような事象も観測されていた．

今回，両キャンパスにおいて無線サービスを開始/拡充するにあたり，これらの煩雑かつ難度の高い作業を軽減し，安定したサービスを提供するために全てのアクセスポイントが同一周波数で動作し，端末側からはサービス提供範囲で一つの大きなアクセスポイントとして見える Meru 社の MC4100 および AP320 を導入した．端末が送信した無線接続パケットは，その信号を受信した全てのアクセスポイント (AP320) からトンネル接続用 VLAN を通じてコントローラである MC4100 にすべて送信される．その上で，MC4100 が，各 AP が観測した無線強度を比較し，最近接の AP320 からのみ，下りの通信を行うことで，無線利用の最適化を行っている．この際に，用いられる BSS ID は接続している各端末に固有の値を用いるため，端末側はローミング処理が不要となっている．また，複数 SSID をサポートし，各 SSID ごとに，接続する VLAN を変更することができるだけでなく，認証方式や暗号化方法も設定可能である．

学生用 VRF や職員用 VRF へは福井大学統一認証システムのユーザ名/パスワードを用いた認証を経た上で接続させることを検討している．

5.3 DHCP サービスの導入

前述の AP320 の運用を「L3 モード」で行うこととしたため，ネットワークの運用自体に DHCP サーバが必要となることになった．また，文京キャンパスではネットワーク更新と同時に IPv4 アドレスのリナンバリングが行われた事もあり，利用者の設定作業の軽減も実現できるよう，DHCP サービスを開始した．ただし，DHCP サービスでアドレス払出を行うのは，あらかじめ登録された MAC アドレスに対してのみであり，払出アドレスは MAC アドレスについて固定しているため，このサービスの利用は必須ではない．

なお，この DHCP サービス用のサーバは，OS として NetBSD[2] を採用し ISC DHCP[3] を動作させている．

6. 導入後の課題

新ネットワークの導入後に直面し課題として取り上げた事項について以下に述べる．この中には導入前から認識はされていたものの対応に時間を要し，対応できないまま導入を迎えているものも含んでいる．

ネットワーク管理支援システムの更新

従来，おもに松岡キャンパスで用いられていたネットワーク管理運用支援データベース [7] をはじめとする運用支援ツールは，当時の福井医科大学ネットワークの形態に特化しているものが多く，現在の新ネットワークに対応していない．このため，利用者からの問い合わせや障害発生時の対応に従来より時間がかかる状態となっている．現在，おこなっている改修作業が終了すれば，総合情報基盤センターの職員であれば，どちらのキャンパスであっても障害の一時切り分けが可能となり，より高可用性を実現できるものと考えられる．

取扱いが確定していない VRF

図 2 中にもあるように，松岡キャンパス側の学生および教室 VRF はいずれのネットワークとも接続されていない．

設計当初，学生 VRF は文京 VRF 間ルータに，教室用 VRF は松岡 VRF 間ルータに接続する事を検討していたが，想定される利用形態の再検討をおこなった結果，学生であっても，松岡キャンパス内の論理ネットワークへのアクセスが必要である可能性も出てきた．同様の事例として松岡教職員用 VRF から，病院ネットワークへのアクセスを希望するものもあり今後，あらたな VRF の設置とその論理的接続の検討が必要である．

外部訪問者用ネットワーク

無線接続において，導入時の Firmware では，外部訪問者用ネットワークのサービス提供 [8] に支障が生じた．これは，コントローラがパケット送信する際に IPv4 接続については固定のゲートウェイを利用するという制限に基づくものであった．その後，firmware を更新し，訪問者ネットワークの VLAN については，トンネル接続用 VLAN を通してコントローラで処理するのではなく，AP 位置で Visitor VLAN に渡すことでサービス提供を継続している．

VRF と直感の乖離

仮想ルータ機能としての VRF について，頭では理解しているものの実際に利用するにあたり，従来の運用と異なるため作業に手間取る場合が見られる．

顕著に見られるのは，ある特定の VLAN における ARP テーブルの調査時である．従来は，当該 VLAN のゲートウェイアドレスにアクセスし，その機器での ARP テーブルを閲覧する事で目的とする情報に到達できた．新ネットワークでは全ての VLAN のゲートウェイアドレスはコアスイッチが保有しているため，同じ操作で目的を達することができない VLAN が多数存在することになる．仮想ルータ名を指定することで，情報に到達する事は可能であるが，直感とは乖離していることや，仮想ルータ名の確認作業に手間取る事は避けられない．

フロアスイッチの冗長化方法

図 1 で示したように，エッジスイッチとフロアスイッチ間の接続は，各フロアに設置されるフロアスイッチの台数によって方法が異なる．一台しか設置されないフロアについては，帯域の有効利用が可能なリンクアグリゲーションを用いたものの，フロアスイッチの増減に対して臨機応変な対応を困難にしている事は否めない．また，日常点検等の通常運用において，いずれの方法による接続であるかを意識する必要があるのも運用コストの面からは問題であると考えている．

そのため，ファームウェア更新等の作業時に，EPSR によるリング構成に統一する事を現在検討中である．

IPv6 通過ルールの検討

IPv6 について，文京キャンパスと学外とのファイアウォールの設定ルールの検討が完了していないため，文京キャンパスから学外への IPv6 通信は現在全て遮断されている．このことにより，dual stack な OS の利用で学外の dual stack サーバへの接続において，IPv6 から IPv4 への fallback に要する時間だけ，利用者にとって接続に時間がかかるように見えている．このことは，十分な知識を持たない利用者にとっては「新ネットワーク」の不具合として捉えられ兼ねないため，早急なルール設定とファイアウォールへの反映を行うことが必要である．

7. おわりに

現在，大学ネットワークの運用のあり方に関する議論が活発におこなわれている．議論の背景には，運用を継続するためのコストの問題や運用にたいして責任を負う組織の明確化/人的資源の確保が困難な現状があると認識している．この様な中で福井大学は，学内ネットワークシステムについて，学内情報基盤として総合情報基盤センターが責任を持って運用するという方針をとることとし，この方針に則った初めてのネットワーク更新を終えたものである．現在までの評価としては，(特に分散管理されていた文京キャンパスにおいて) 従来より安定したネットワーク運用が総合的により低い運用コストで実現できているものと考える．

今後は，総合情報基盤センターが専門家集団として大学全体の情報基盤であるキャンパス LAN を維持するための人的リソースの確保維持の手法について検討していく事が必要であると考えている．

参考文献

(1) The FreeRADIUS Project, http://freeradius.org/.
(2) The NetBSD Project, http://www.NetBSD.org/.
(3) Internet Systems Consortium's DHCP software, http://www.isc.org/software/dhcp/.
(4) 大垣内 多徳，山下 芳範，吉野 孝博，高山 俊一，大谷 孝博，猪島 哲也: 病院内無線 LAN の設計と運用上の影響評価. 医療情報学 (Suppl.), 21, pp732-733 (2001)
(5) 大垣内 多徳，山下 芳範: 病院内無線 LAN 構築における問題と対策. 医療情報学 (Suppl.), 22, pp200–201 (2002)
(6) 大垣内 多徳，山下 芳範，高岡 宏光: マイクロサーバを利用した学内ネットワーク監視システムの構築. 情報処理学会研究報告, 2002-DSM-28, pp.43–48 (2002)
(7) 大垣内 多徳， 山下 芳範: ネットワーク管理運用支援データベースの構築と運用. 情報処理学会研究報告, 2003-DSM-30, pp.1–6 (2003)
(8) 大垣内 多徳，平塚 紘一郎，山下 芳範: 外部訪問者に対する病院内からのネットワーク接続サービス. 医療情報学 (Suppl.), 26, pp331-332 (2006)

Vol.2010-IOT-10 No.2
2010/7/16

(9) 平塚 紘一郎, 大垣内 多徳, 田中 光也: 信頼性の検証が可能な認証システムの設計と運用. 情報処理学会研究報告, 2007-DSM-47, pp.7–12 (2007)
(10) 平塚 紘一郎, 大垣内 多徳, 田中 光也: 長期運用を考慮した認証システムの設計と運用. 情報処理学会研究報告, 2007-DSM-47, pp.13–18 (2007)