神戸大学キャンパスネットワークにおける仮想化技術について

神戸大学 情報基盤センター
伴　好弘，佐々木博史，鳩野逸生

1 はじめに

大学 ICT を推進するにあたり，キャンパスネットワークは通信基盤を支える物として今までに以上に必要不可欠なシステムとなっている．神戸大学でもそのような背景から，従来より運用されている教育研究系ネットワークの他に，事務システムネットワークや，その他の専用ネットワークが敷設されてきた．しかしこの状況は，アドホックにネットワークが増殖してきていることを意味しており，結果としてシステム全体の複雑化を招き，管理を難しくさせたり，特定個所に未使用ポートの多い機材が複数設置されるなど，消費エネルギー的，場所的，コスト的な観点で効率的とはいえなかった．だた逆に，同じ物理ネットワークを共有するとしても，ネットワーク中を通過する情報の質の違い常に意識する必要があり，拡張性の維持が困難になりがちであった．そこで，これら性質の違う複数のネットワークを仮想化することで機材共有化をできるようにネットワークの更新を行った．本稿ではキャンパスネットワークに対して仮想化技術をどのように利用したのかについて述べる．

2 導入の背景

2.1 更新直前の既存ネットワークについて

前節で述べたように，更新前の神戸大学で運用されているネットワークは，主に以下に示すような物理的・論理的ネットワークが存在していた．今後の利用状態を考慮すると，これ以上の独立したネットワークの増設は，経路の確保や，それぞれのネットワークの安定維持が困難になるという状況が生まれつつあった．

- 教育研究系ネットワーク
- 事務システムネットワーク
- 図書館業務系ネットワーク
- 教育研究用計算機システム用ネットワーク
- SINET の孫請け機関向けネットワーク
- 遠隔キャンパスとの拠点間ネットワーク

この状況に加えて，教育研究系ネットワークに使用していた機器の運用期間が７年を超える物も出始めていたため，機材の保守や修理が受けられないという，ネットワークそのものの維持が困難になりかねない問題も生じ始めていた．

2.2 更新時の制約条件

以上のような状況もあるため，これらの条件に合致するようなネットワークの構成方法の模索を続けていた．

- 冗長化をできる限り低コストで実現すること
- 物理的な構成を単純化および標準化すること
- 管理コストの軽減ができること
- 新規のネットワークを容易に拡張できること

この検討途中に，論理ネットワークを仮想的に扱うことで，それぞれの独立性を保ったまま物理経路を共有する機能が，特定の機材メーカに偏らずに実現できそうだということが分かり，関連する情報の収集を行っていた．幸運にして２００９年度にキャンパスネットワークの更新を実施できるまたとない機会を得ることができた．それに合わせ前年度の２００８年度にこれらのネットワークを含めた具体的な導入検討に入った．

3 ネットワークの仮想化にあたって

ネットワークの更新にあたり，予算的な要請から，従来通りの手法で既存ネットワークの全機能を維持しつつ更新することは不可能であったため，検討中のネットワークの仮想化を視野に入れることとした．

3.1 仮想化の実現方法について

複数のネットワークを束ねて機材の効率的な利用を推し進めようとする際に，対象となるネットワークの論理的な構造をいかにして維持するかが，導入後の運用や拡張の際に大きく影響することは容易に推測がつく．以下の二つがその当時利用できる候補として存在していた．

1. MPLS[1]を使用する
2. VRF[2] を使用する

１．については，IP 以外のプロトコルも共存できるという特徴があるものの，この機能が利用できるネットワーク機器が製品的に上位機種に限られており，総コスト的に無理があった．また，従来の IP ネットワーク的な観点とは違った側面からの理解が必要なため，運用時の問題切り分け作業等に影響が生じる懸念があった．

２．は検討当時まだ機能的に相互接続性や想定通りの動作ができるのかなど，はっきりとしないところがあったものの，価格的に既存のバーチャルルータ機能を有するネットワーク機器と比べ極端な金額差が少なかったため，導入時のハードルが幾分低いことが優位であると考えた．

現状の利用状況から，IP 以外のプロトコルの利用は可能性が低い事と，規模的な観点から１でネットワークを構築するのは過剰なものと考え，２の VRF を用いてネットワークの多重化と経路制御の複雑化を避ける事を目指した．

3.2 VRF 機能について

前節で出てきた VRF は Virtual Routing and Forwarding の略称で，一種のバーチャルルータとして機能する転送テーブルの一種である．通常のバーチャルルータ機能は，使用する機器内で閉じた利用となる．一方 VRF は広域ネットワーク等で，複数の VPN を同じ物理経路に共有させる時に併用される事を想定して作られている．このテーブルに記述された経路（ここでは VRF パスと呼ぶ）内のネットワークは定義された VRF パス毎に独立しており，その経路情報が他の VRF パス内に混入する事は基本的に無いという特徴を持つ．その特徴を生かす事で，それぞれ違った経路情報や，アドレス体系を持つネットワークを混在させた際の，各ネットワーク機器内での転送ルールの記述が構造化でき，見通しをよくする事が可能となる．

3.3 VRF の適応範囲

VRF の利用が今回の利用目的に合致する状況ではではあるが，やはりコストの面では普通のレイヤー３スイッチよりは高価であるため，範囲を限定する必要がある．そこで，ルーティング処理を行うバックボーンに相当するコアスイッチと，その直下に接続される拠点スイッチ（基幹スイッチと呼んでいる）を対象に VRF 機能を有する装置を選定する事とした．図 1 にバックボーン部分の基本構成図を示す．この部分は，OSPF（v2, v3）による動的経路制御を行い，各物理経路のコスト設定により冗長化行っている．また図 2 は VRF を用いたネットワークの関係について示したものである．物理経路的に一番広範囲に利用される事となる教育研究系ネットワークは VRF 化せず，それ以外の独立した経路制御が必要なネットワークを VRF 化して収容する構成としている．

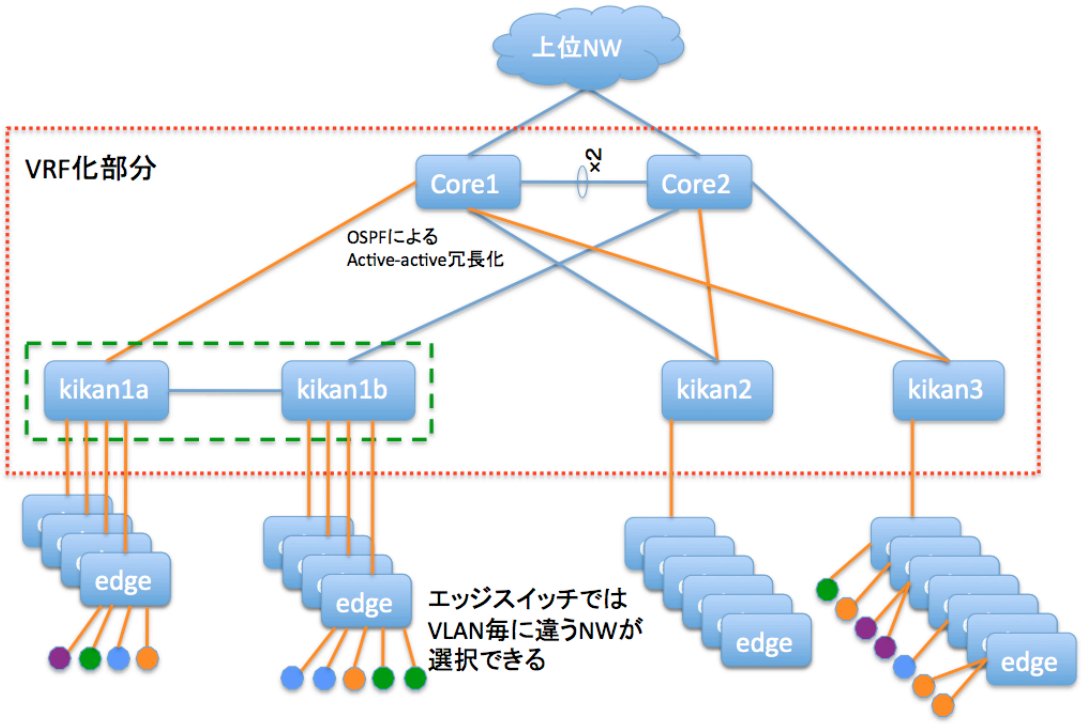

図 1　VRF による多重化

図 2　VRF 化したネットワークの関係

3.4 使用した機材について

使用した機材については，単一メーカではなく，設置箇所と今後の利用状況を極力考慮して，表 1 に示すような複数メーカの製品を使用した．その際に懸念される事項として，相互接続を行った際にうまく動作しないという問題が生じる事があった．そこで，このような可能性を極力最小化するために，メーカ固有の機能を使用せず，IEEE 標準の機能を使用するよう注意を払った．結果として，一部ファームウェアに不具合が見つかったりしたものの，本運用開始時までには VRF を含む機能が正常に動作し，相互接続についての影響は生じなかった．

表 1　VRF 接続で使用した主な機材

製造メーカ	機種名
Brocade	Netiron MLX, CES シリーズ
Juniper	EX4200 シリーズ
Alaxala	AX6700S シリーズ
Cisco	Catalyst3560E シリーズ

3.5 エッジスイッチでの対応

拠点スイッチまでは VRF でネットワーク多重化を行っているが，端末に近いエッジスイッチについては，一般的な Tag VLAN を用いたネットワークとする事で，コストの上昇を抑えつつ，機器の共有化を目指した．図 3 はエッジスイッチでのポートの割当状況の例を示したものであるが，事前に VLAN に割り当てる tag ID をネットワーク毎に重複しないよう統一的に定義し，エッジスイッチのポートでは，この ID 毎に対応するネットワークが割り当てられるような構造をとった．

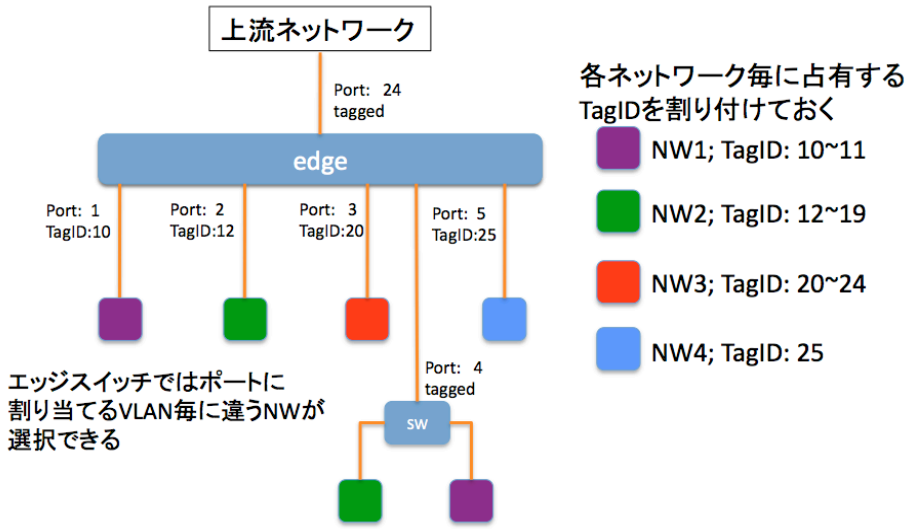

図 3　エッジスイッチでのネットワーク選択

4 更新時の問題とその解決方法

ネットワークを更新する際は，通信途絶状態を極力短時間で確実に終えたいという希望がある．その要望に対して，ネットワーク機材の更新を行う際に，VRF 機能を有効活用させようと活用法を考え，実際に使用してみた．以下に更新に関する内容について述べる．

4.1 コアスイッチ周辺の更新

コアスイッチから対外接続部分の更新については，経路情報の輻輳を避けるため，図 4 左側の様に，新ネットワークは上位ネットワークに接続しない状態で一通りの設定を実施しておき，次節で出てくる遠隔キャンパスを除く各キャンパスの新基幹スイッチとの間で，最低限の経路を作成しておく．移行作業の時間的，対象範囲的な制約から，旧ネットワークを一斉に停止する事は不可能であるため，新ネットワーク内に旧ネットワークを丸ごと収容するための移行用 VRF ネットワークをあらかじめ作成しておく．バックボーン部分の更新時は，図 4 右側のように旧ネットワークを新ネットワークのコアスイッチに設定しておいた移行用のポートに接続替えする．その後，新ネットワークのコアスイッチを上位ネットワークに接続する事で，バックボーン部分について新旧のネットワークが共存する過渡的な状況を作り上げる．まだこの時点では，主要な経路は旧ネットワークへルーティングされるので，旧ネットワークに接続された機器は通信を継続できる．後日実施する基幹スイッチの更新時に経路を新ネットワークの方へ順次変更する事で，バックボーン部分の物理的な接続替えを実施しなくても良い状態にした．

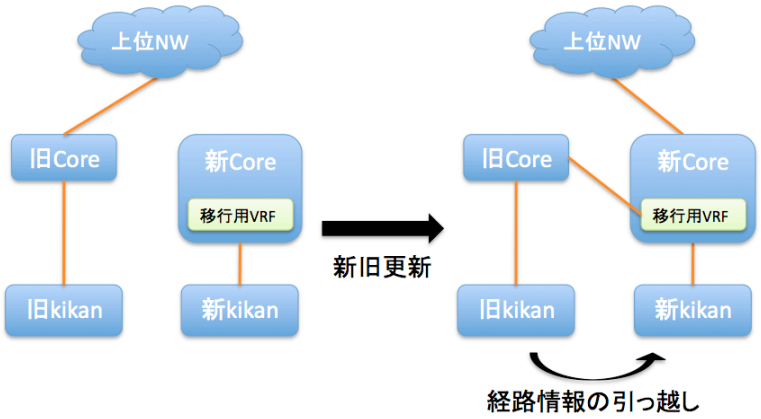

図 4　バックボーン部分の移行手順

4.2 キャンパス内ネットワークの更新

キャンパス内の更新については，従来コアスイッチと基幹スイッチ間に複数本の 1Gpbs 経路を用いたチャネル接続を使用していた．今回の構成では，主経路の 10Gbps 経路と障害時の接続性維持のための 1Gbps 経路という接続形態に変更されるため，利用可能な光ファイバに余裕が生じる事になる．そこで図 5 の様に，更新前段階で事前に旧ネットワークのチャネル接続の経路を縮退させ，新ネットワークの経路を確保する事で，更新時に同じネットワークが新旧のシステムで共存する形をとった．基幹から先も同様に，事前にエッジスイッチを接続できる箇所については新旧の装置を同時に稼働させる事とした．

更新当日は旧ネットワークのエッジスイッチに接続されているケーブルを新エッジスイッチの指定したポートに接続する事で，切り替え時間の短縮を行った．

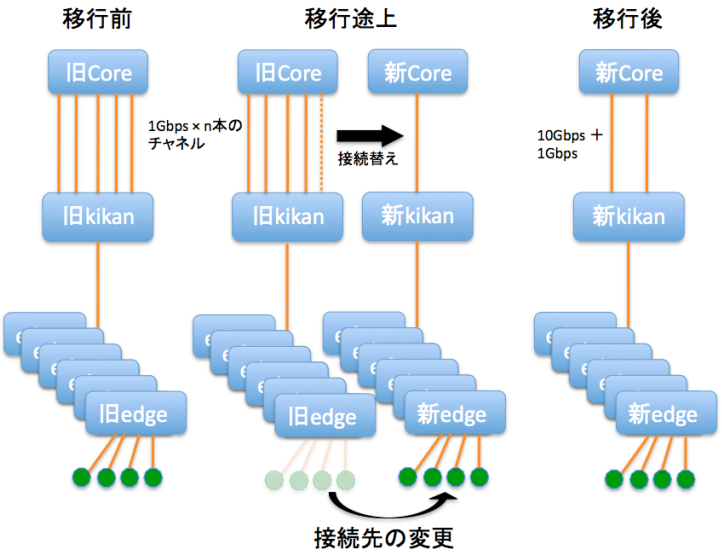

図 5　基幹スイッチ以下の移行手順

4.3 キャンパス間ネットワークの更新

ネットワークの更新を実施する際に，本学の場合，遠隔キャンパスと研究拠点が分散しているため，これらキャンパス間の更新と，各キャンパス内のネットワークの更新という，性格の違う２種類の作業が生じる．幸いな事に主要な遠隔キャンパスは経路が冗長化されているので，それを最大限活用する形で更新作業を進める事とした．移行の順序を図 6 に示す．基本的な手順とし

てはキャンパス内ネットワークの移行手順と似ているものの，多の拠点への中継点にもなるため，それらの移行用のネットワークを仮設する必要がある．

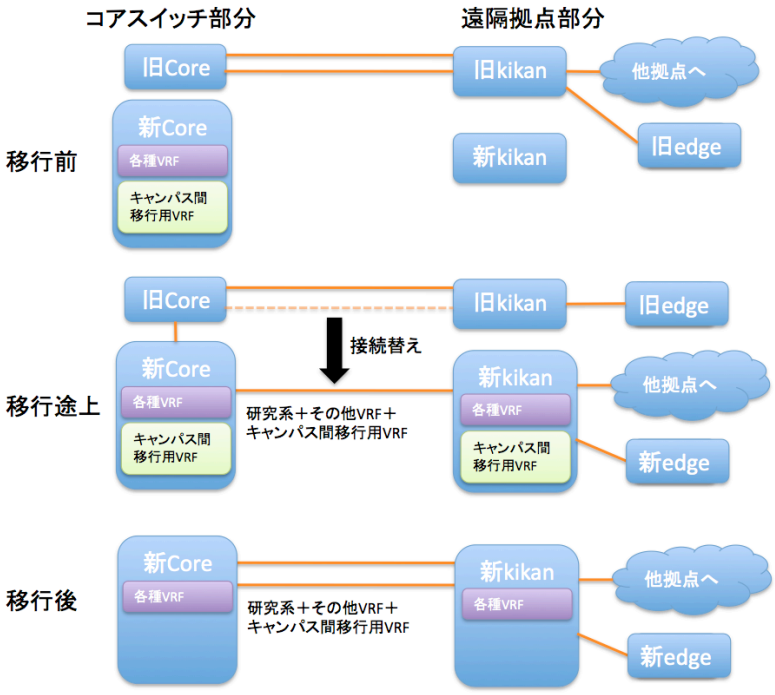

図 6　キャンパス間接続の移行手順

5 まとめ

ネットワークの更新後の経過として，おおむね安定運用できている状況であり，今回統合の対象となった，教育用計算機システムのネットワークの実現もスムーズに移行でき，実稼働に持っていく事ができた．その際に表面化した問題としては以下の項目が挙げられるが，今後ファームウェアの更新などで解消してくと聞いている．

- VRF は実装されているが，DHCP リレーなどの付加機能と VRF をまだ同時利用できない装置がある
- IPv6 について VRF での対応がまだ不完全な機材がある

それと，懸念されていた複数メーカ間での VRF の稼働については，過去に別の機能で経験したような，不可解な動作を示す事も無かったため，その点においても更新がスムーズに行えたという点でよかったと言える．

参考文献

[1] http://datatracker.ietf.org/doc/rfc3031/
[2] Ananda Rajagopal, Building Trusted VPNs with Multi-VRF, Foundry Networks, 2006