

Title	基幹ネットワーク構成の変更
Author(s)	岡本, 忠男
Citation	国立大学法人北陸先端科学技術大学院大学技術サービス部業務報告集 : 平成24年度: 33-36
Issue Date	2013-08
Type	Others
Text version	publ isher
URL	http://hdl.handle.net/10119/11901
Rights	
Description	

基幹ネットワーク構成の変更

岡本 忠男

情報社会基盤研究センター

概要

情報社会基盤研究センターが全学向けのサービスを提供する各種サーバは、基幹ネットワークに接続されている。その構成は近年のサーバ仮想化の進展等により、物理的にも論理的にも複雑さを増しており、今後の情勢変化に対応することが難しくなりつつある。そこで、この状況を改善すべく基幹ネットワーク構成の変更を実施したのでここに報告する。

1 はじめに

1.1 学内ネットワークの概要

情報社会基盤研究センター（以下、情報センター）が学内各所に整備しているネットワーク環境は、本学構成員に対して学内の各サーバへのアクセスとインターネットへの接続を提供している。本学のネットワークシステムは図 1 に示すように、対外接続ルータを頂点に、以下、ファイアウォール、コアスイッチ、ディストリビューションスイッチ、エッジスイッチ等で構成されている。機器間には必要に応じて 10 ギガビットイーサネットを用いている。

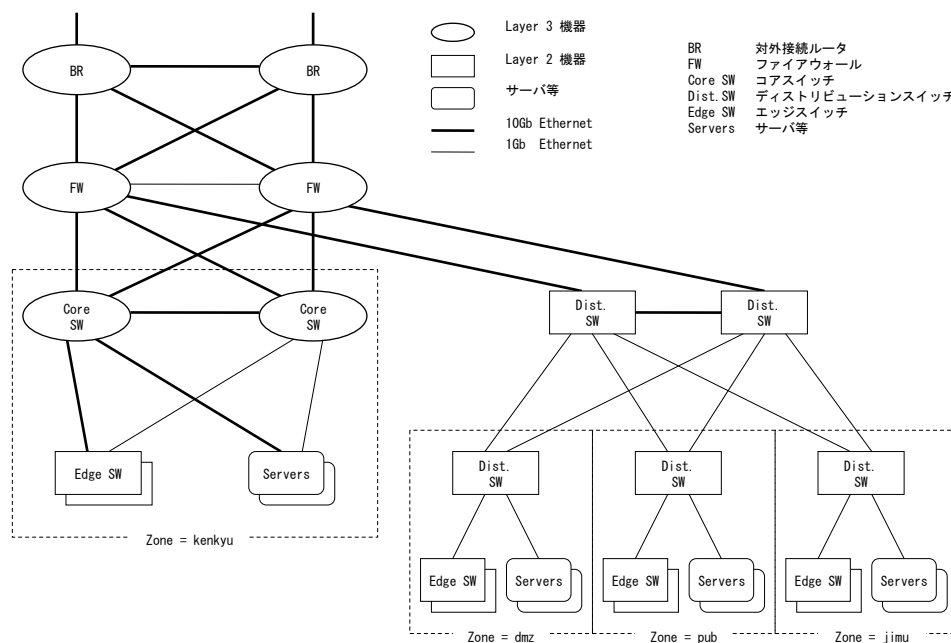


図 1. 本学ネットワーク構成の概略図

1.2 ネットワーク機器の概要

(1) 対外接続ルータ

対外接続ルータは、学内ネットワークの最も上流に位置し、学外ネットワークと学内ネットワークとを接続するための機器である。学内方面に対してはファイアウォールと接続されている。Juniper Networks 社の

MX80 と、Brocade Networks 社の XMR4000 の 2 台による冗長構成を採用している。

(2) ファイアウォール

ファイアウォールは、対外接続ルータの下流に配置され、ポリシーに従って通信の許可および遮断を行う、いわゆるパケットフィルタリングを担う。本学では 2 台の Fortinet 社 FortiGate3950B による冗長構成を採用している。

ファイアウォールにはゾーンと呼ばれる、サブネットの集合から成る論理的なグループがあり、ポリシーは任意のゾーン間に対して定義される。本学の主なゾーンには、各研究室のフロアや全学サービスのサブネットを主とする kenkyu、学外からのアクセスを前提としたサービスのサブネットを主とする dmz、事務局フロアのサブネットを主とする jimu 等がある。

下流との接続は、kenkyu ゾーンとそれ以外のゾーンの二手に別れ、それぞれコアスイッチとディストリビューションスイッチに向かう。

(3) コアスイッチ

コアスイッチはファイアウォールの下流に設置された、kenkyu ゾーン用の L3 スイッチである。コアスイッチは通常利用される常用系と、常用系の障害時に機能を引き継ぐ待機系の 2 台による冗長構成となっている。コアスイッチは各研究科フロアのエッジスイッチ約 50 台と、常用系は 10GbE、待機系は 1GbE にて接続される。また、ファイルサーバやターミナルサーバ、計算サーバ等の主要サーバを直接収容する。

なお、常用系コアスイッチには Cisco Systems Nexus7018 を、待機系コアスイッチには Alaxala Networks 社の AX6708S（現在はレンタル期間満了による Arista Networks 社の 7504 への更新が完了している）を使用している。

(4) ディストリビューションスイッチ

ディストリビューションスイッチはファイアウォールの下流に設置された、kenkyu ゾーン以外を対象とした L2 スイッチである。ポート数の関係上、多段の構成をとっており、ファイアウォール直下の 2 台のスイッチを除いて、各ゾーン専用のスイッチとして設置されている。

(5) エッジスイッチ

エッジスイッチは、コアスイッチまたはディストリビューションスイッチの下流に位置し、機器を直接収容するための L2 スイッチである。各フロアにおけるエッジスイッチは利用者の端末機器を収容し、サーバ室におけるエッジスイッチは管理用機器や比較的重要度の低いサーバの収容に用いられる。いずれも上流のスイッチと同じゾーンに属し、それに含まれるサブネットのみを扱っている。

1.3 ネットワーク機器の設置場所

対外接続ルータ、ファイアウォール、コアスイッチ、およびディストリビューションスイッチは、情報センター3階のネットワーク室に設置されている。また、各フロア向けのエッジスイッチは学内各所の EPS に、サーバ収容用のエッジスイッチはそのサーバの設置してある部屋またはラック群ごとにそれぞれ設置されている。

2 従来の問題点

2.1 背景

以前、情報センターの管理する各種サーバは学内各所に分散して設置されていた。これは、サーバ室の確保、電源の確保、空調の整備、サーバ機器の総量等の点で課題があり、すべてを 1 箇所に設置することができなかったためである。しかし、

- ・ CVCF の導入（2008 年）
- ・ 情報センター1階倉庫をサーバ室として割り当て（2008 年）

- ・サーバ室の床耐荷重工事（2008 年）
- ・サーバラックおよびエアコンの導入（2008 年，2009 年，2012 年）

等，サーバ室の環境を順次整備したことにより，新規に導入されるサーバ機器はファイルサーバ，ブレードサーバなど規模の大きいものも含め，専ら情報センター1 階のサーバ室に収容できるようになった。また，近年著しく進展したサーバの仮想化により，各所に分散設置されていたサーバのレンタル期間満了を機に後継サーバが仮想化され，同じく情報センター1 階のサーバ室に収容されるようになってきた。このような経緯で，現在は事務局系システム，計算サーバ，およびその他一部のシステムを除き，サーバはそこに集約されつつある。

2.2 問題点

(1) ラック群毎，ゾーン毎にスイッチが必要

仮想化やその他の理由で新たに 1 階サーバ室に入ってきたサーバのゾーンは，kenkyu, dmz, jimu などまちまちである。そして図 1 で見た通り，コアスイッチをはじめディストリビューションスイッチやエッジスイッチはゾーン毎に別のものをを用いている。このため，あるゾーンにわずかな数のサーバを収容する場合でもゾーンの数だけスイッチを用意する必要となってしまう。また，1 階サーバ室では 6-7 台のラックから成るラック群が 6 列あり，広さや配線等の関係上，その 2 列ごとに 3 箇所に分けてスイッチを配置するため，ゾーン単位でのスイッチ設置では柔軟な運用がしにくい。

(2) 3 階と 1 階との間のケーブル数の急増

当初は 1 階サーバ室に設置されるサーバはそれほど多くなかったため，ネットワークケーブルは 3 階ネットワーク室のコアスイッチやディストリビューションスイッチに直接収容する場合が多かった。しかし，サーバが増えるとそれをネットワークに接続するためのケーブル数も当然増え，1 階と 3 階との間に予め敷設しておいた分だけでは不足しかねない。

(3) 帯域利用効率が悪い

これはサーバが一室に集約しつつあることとは無関係であるが，ほとんどのスイッチでは STP(Spanning Tree Protocol)を単一トポロジのモードで使用している。このため，通常稼動時にはそのスイッチのブロッキングポートにはトラフィックが流れることなく待機しており，その分の帯域幅が無駄になっている。

3 改善の主な方針

上で述べた問題点を改善するにあたり，次のような方針を定めた。

(1) PVST の適用

STP のモードを，従来の単一トポロジのモードから複数トポロジを持てるモードに変更する。MST(Multiple Spanning Tree)は運用コストが高いため採用せず，PVST(Per Vlan Spanning Tree)等，VLAN 毎にトポロジを持つモードを利用する。これにより，帯域を有効活用可能な構成にすると同時に，以降のネットワーク構成変更を実施しやすくする。

(2) ゾーン別のスイッチ配置を改める

ゾーン毎にスイッチを分ける構成をやめ，任意のゾーンの VLAN を任意のスイッチに出せるようにする。これにより，スイッチ配置の柔軟性が高まり配線のしやすさが向上するなど，より効率的にネットワークを運用できるようにする。

(3) データセンター用スイッチを導入する

1 階サーバ室のラック群 2 列ごとに，冗長性を考慮して 2 台のデータセンター用スイッチを新たに導入し，そのラック群に収容されるサーバを収容する。このスイッチにはそれらを十分に収容できる性能が要求される。それにより，従来コアスイッチに直接収容していた接続をこのデータセンター用スイッチに移行し，3

階と 1 階との間の不必要なネットワークケーブル数を削減する。

4 変更作業の実施

(1) PVST 化の実施

- ・作業手順の検討

STP の設定変更はネットワークサービスへの影響が広範囲に及ぶことがしばしばある。このため、ネットワークへの影響を最小限に留めるためにゾーン単位で順次切替を完了させていく方針とし、その作業手順の検討を行った。それに従って以下のように切替作業を行った。

- ・kenkyu ゾーン以外の PVST 化

kenkyu ゾーン以外においては、下流に位置するエッジスイッチから順に切替を行い、最後にディストリビューションスイッチの切替を行った後、正常に動作していることを確認した。

- ・kenkyu ゾーンフロア用 VLAN は STP を停止

kenkyu ゾーンフロア用エッジスイッチは約 50 セットあり、そこで扱っている VLAN の数はおよそ 100 である。(1)フロア用エッジスイッチの VLAN すべてについて個別にトポロジを持つと負荷の点で懸念があること、(2)フロア用エッジスイッチでは仕様上 PVST を使用できないこと、(3)レイヤ 3 のコアスイッチ 2 台の下にレイヤ 2 のエッジスイッチが 1 台という単純な構成であることを考慮し、これらの VLAN については STP を無効とすることとし、その設定をコアスイッチ 2 台に対して行った。

- ・kenkyu ゾーン PVST 化

kenkyu ゾーンのコアスイッチは 2 台あり、一方のみを PVST 化すると予期せぬブロッキングポートの発生などサービスに少なからず影響を及ぼす恐れがある。そこで今回は、待機系コアルータの全インタフェースを無効化してネットワークから切り離し、両コアルータそれぞれに PVST 化を行った。その後、無効化した待機系コアスイッチのインタフェースを有効化して PVST の動作を確認した。

(2) コアスイッチとディストリビューションスイッチの接続

kenkyu ゾーンとそれ以外のゾーンをレイヤ 2 で互いに接続するために、コアスイッチとディストリビューションスイッチとを直接ネットワークケーブルで接続した。PVST 化が既に完了しており STP の問題は発生していない。

(3) データセンター用スイッチの導入

40GbE インタフェースを搭載したスイッチ、Dell 社の Z9000 と Arista Networks 社の 7050Q の 2 機種用意して 1 階サーバ室に設置した。従来、3 階ネットワーク室のコアスイッチに直接収容されていたブレードサーバ等を新たに収容すると共に、今回導入されたファイルサーバ等の機器も収容している。

5 構成変更の効果

一連の構成変更作業により、各スイッチにおけるゾーンの制約が解消され、任意のスイッチに任意のゾーンのサブネットを設定できるようになった。これは、スイッチの配置に柔軟性をもたらすだけでなく、収容される機器に応じたネットワークの帯域幅や信頼性の提供にも寄与する。また、障害時のみに利用されてきた部分を常時活用することが容易な環境となり、今後のネットワーク帯域の一層の有効活用が見込める。

6 今後の課題

今回は情報環境システムの機器の導入時期が迫っていたため、それに必要な部分を優先して構成変更を行った。ファイアウォールとディストリビューションスイッチとの間の接続をファイアウォールとコアスイッチ間に移行する作業や、ブレードサーバ用のスイッチの収容先変更作業等、変更すべき部分は現在も残っているため、今後順次その作業を進めていく予定である。