

高速キャンパスネットワークシステムの更新

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に提供するネットワークサービスは、学生や教職員の教育・研究・事務等の活動の基礎となるものである。したがって、それを構成するネットワーク機器等の設備の重要性は非常に高い。ここでは、その基幹部分等を2014年度更新の情報環境システムに含まれる高速キャンパスネットワークシステムとして調達し、更新を行ったことについて報告する。

1. 情報環境システムとネットワーク

情報社会基盤研究センターで調達、導入、運用、管理を行っている情報環境システムは、

- 仮想デスクトップ環境や端末機器
- ファイルサーバ等のストレージ
- ルータやスイッチ、無線LAN設備等からなるネットワーク機器
- 高速な演算性能を有する並列計算機群

等からなる総合的なシステムである。情報環境システムは契約期間が4年間のシステムであるが、規模が大きいため全体の4分の1ずつを毎年更新している。2014年度更新の情報環境システムにおいては、ネットワーク関連機器の一部も更新対象となった。

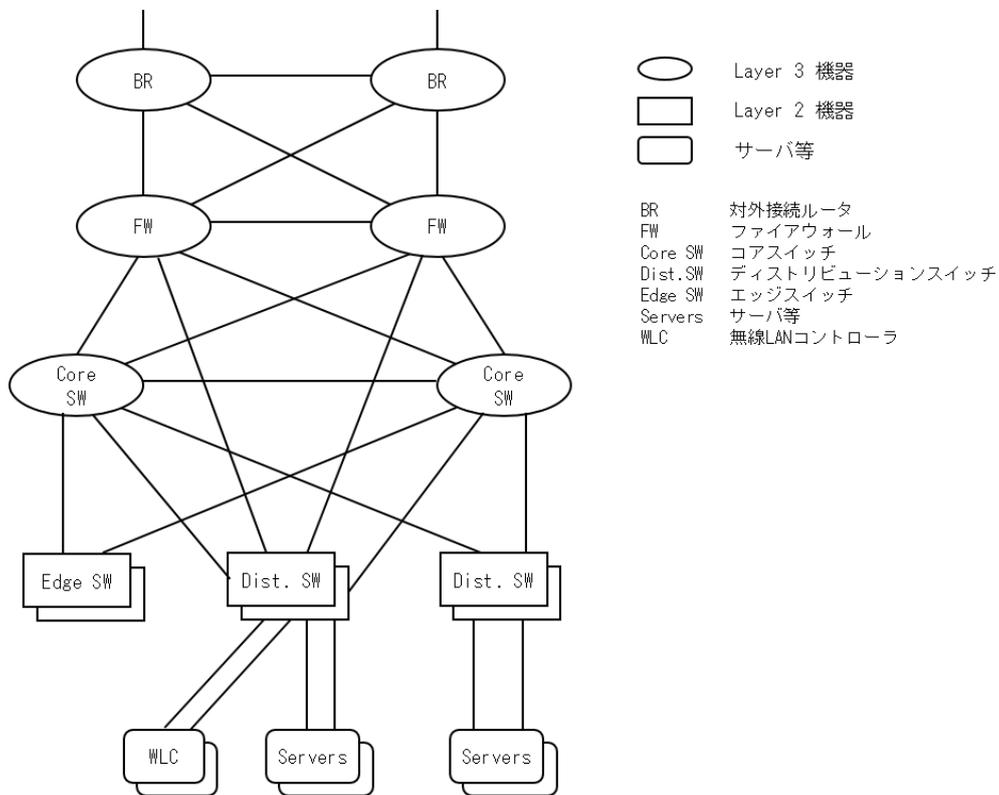


図1. 本学ネットワーク構成の概略図（更新前）

2. 学内ネットワークの概要

情報社会基盤研究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、および無線 LAN を制御する無線 LAN コントローラ等で構成されている。機器間の多くは 10 ギガビットイーサネット接続され、一部については 40 ギガビットイーサネットを用いている。

(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 Communications Systems 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。下流方面に対してはコアスイッチと接続されている。

(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 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、待機系共に 10GbE にて接続される。また、サーバや他のエッジスイッチ等を収容するディストリビューションスイッチとも 40GbE、10GbE、1GbE のいずれかで接続される。なお、常用系コアスイッチには Cisco Systems 社 Nexus7710 を、待機系コアスイッチには Arista Networks 社 7504 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コアスイッチの下流に設置された L2 スイッチである。ファイルサーバやプライベートクラウド基盤などの学内主要サーバを直接収容し、広帯域で快適にアクセスするためのデータセンタスイッチや、サテライトキャンパスや図書館、学生寄宿舎等、学内の研究科フロア以外の各所への接続を一手に収容するためのスイッチ等が該当する。機種や年式、および上流との接続は、用途や重要度に応じて様々なものが混在している。

(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。研究科の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。

(6) 無線 LAN アクセスポイントと無線 LAN コントローラ

無線 LAN アクセスポイント（以下、無線 AP）は、学内の約 380 か所に設置され、学内のほぼ全域に対して無線 LAN サービスを提供している。無線 LAN コントローラは、数多くの無線 AP を効率よく制御するために不可欠な装置である。これにより、無線 LAN の SSID 追加削除等の設定変更作業やバージョンアップ等を個別にではなく一括で行える。無線 LAN コントローラはディストリビューションスイッチに接続されている。

3. 今回の更新対象機器と構成の検討

今回の更新対象機器は、4 年のレンタル期間を満了する、対外接続ルータ 2 台、ファイアウォール 2 台、

無線 LAN コントローラ 2 台である。また、既設の無線 AP 約 380 台のうち一部を今回新たに情報環境システムとして導入して更新することとした。これに基づいて構成を次のように検討した。

対外接続ルータ 2 台については、(1)それぞれが SINET4 と WIDE に接続されインターネット接続を担うこと、(2)一方のルータの障害時もサービスを継続できること、(3)同時のソフトウェア障害発生を防止するため 2 台は互いに異なる OS で動作すること、(4)ポート当たりの帯域幅は従来の 10Gbps を維持すること、等の要件を満たすものを導入することとした。

ファイアウォール 2 台については、(1)一方の機器障害時には他方に機能およびセッションを自動的に引き継いでサービスを継続できること、(2)ファイアウォールとして高いスループットを有すること、(3)ポート当たりの帯域幅は従来の 10Gbps を維持すること、等の要件を満たすものを導入することとした。

また、ファイアウォールの出力するログをもとに 24 時間 365 日体制でセキュリティ監視・分析を行うサービスを新たに導入し、セキュリティレベルの向上を図る。

無線 LAN コントローラ 2 台については、(1)既設の無線 AP を制御できること、(2)約 380 台ある無線 AP すべてを 1 台の無線 LAN コントローラで収容できること、(3)一方の障害時には他方に機能を自動的に引き継ぎ、サービスを継続できること、(4)ネットワークインタフェースは 10Gbps とすること、等の要件を満たすものを導入し、帯域幅の面や、冗長構成の面、あるいは管理運用面での改善を図ることとした。

無線 AP については、IEEE802.11ac の高速通信規格に対応した製品を導入し、主に速度面での改善を図ることとした。設置場所については、(1)研究科で最も古い無線 AP が設置されているマテリアルサイエンス研究科 1,2,3,4 棟、(2)利用者が多いと考えられる、講義棟と学生会館、情報科学研究科 1,2,3 棟の連絡通路である 2 階、コラボレーションルーム等のある情報科学研究科 3 棟 5 階を今回のものを更新することとし、調達台数を 80 台とした。

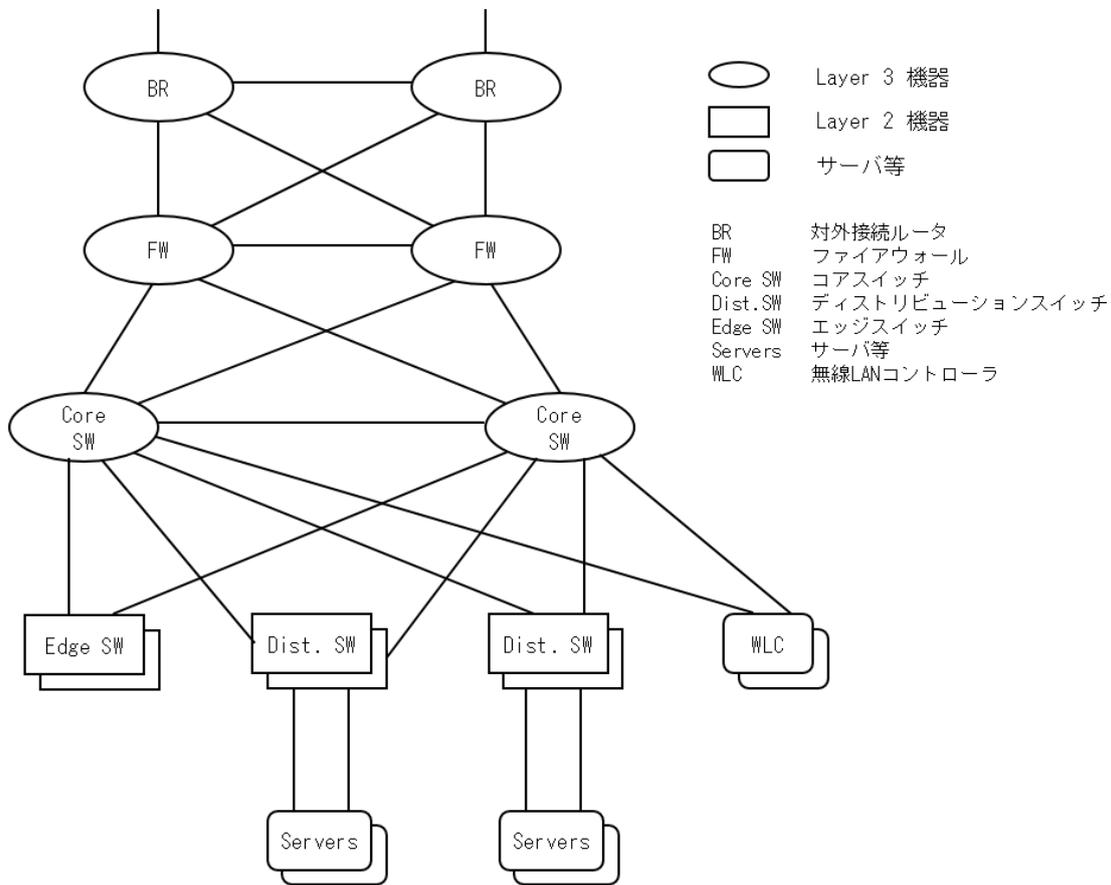


図 2. 本学ネットワーク構成の概略図 (更新後)

その他の構成変更等としては、次の二点について改善を図ることとした。第一に、ファイアウォールとコアスイッチの両方に接続されているディストリビューションスイッチ(Extreme Networks 社 Summit X650)の接続を改めることとした。具体的にはファイアウォールとの接続を切断し、上流との接続をコアスイッチのみとする構成に変更して、管理・運用面での煩雑さを低減することとした。第二に、無線 LAN コントローラの収容先を従来のディストリビューションスイッチから、一段階上流のコアスイッチに変更して可用性の向上を図ることとした。

以上の構成検討を反映したネットワーク概略図は図 2 の通りである。また、次の機器が調達された。

対外接続ルータ 1	Cisco Systems 社 Catalyst 6880
対外接続ルータ 2	Brocade Communications Systems 社 MLXe-4
ファイアウォール	Fortinet 社 FortiGate 3700D
無線 LAN コントローラ	Cisco Systems 社 Cisco 8500
無線 AP	Cisco Systems 社 Cisco Aironet 3702



図 3. 対外接続ルータ

上が Cisco Systems 社 Catalyst 6880
下が Brocade Communications Systems 社 MLXe-4



図 4. 無線 AP

Cisco Systems 社 Cisco Aironet 3702

4. 更新作業計画

ネットワーク機器は全学に常時提供されているサービスであるため、機器更新に際してはなるべく構成員の活動に及ぼす影響を少なくなるように実施する必要がある。

まずは、切替作業に先立ち、各機器の収容内容の決定、トポロジ変更となる部分の設定確認および追加設定作業、不要設定の削除等の事前作業を行った。

続いて、切替作業の日程を作成した。それぞれの機器の切替日当日に要する時間とその時のサービス停止時間は表 5 の通りである。これらの作業はすべて独立して行うことができるため、作業順序は自由に組換え可能である。

表 5. 機器更新時の所要時間とサービス停止時間

更新機器	所要時間	サービス停止時間
対外接続ルータ	5 時間	数 10 秒以内
ファイアウォール	4 時間	15 分間が 1 回, 1 分間が 2 回
無線 LAN コントローラ	3 時間	無線 AP ごとに 30 分間
無線 AP	4 日	無線 AP ごとに 30 分間

この更新作業計画では、サービス停止の影響が最も大きいファイアウォール更新作業の 15 分間の停止時期を、利用者数が少ない早朝の時間帯に組み込み、また、対外接続ルータ更新時間帯には、ある研究室の学外とのテレビ会議使用が行われることになっていたため、その時間帯には作業を一時中断するなど、利用者への影響が総合的に少なくなるよう配慮している。

表 6. 機器更新時の所要時間とサービス停止時間

更新作業日	作業内容
第 1 日から第 4 日	無線 AP の更新
第 5 日 4 時から 7 時	ファイアウォール更新
第 5 日 8 時から 11 時	無線 LAN コントローラ更新
第 5 日 11 時から 18 時	対外接続ルータ更新
第 6 日	予備日

5. 実際の更新作業と今後の予定

更新作業は、無線 LAN コントローラについて問題が発生し作業を予備日に延期した以外は、小さな問題がいくつか発生したもののいずれも短時間で解決し、全体としては概ね順調に進行した。今回調達した機器以外にもネットワーク機器は多い。それらも含めて今後も引き続き安定したネットワーク運用に努めたい。