Vol.2009-IOT-7 No.1
2009/10/9

神戸大学におけるネットワークシステムの構築

鳩 野 逸 生[†1]　　伴 好弘[†1]　　佐々木 博史[†1]

神戸大学では，2009 年に，神戸大学キャンパスネットワークシステムの更新を行った．本ネットワークは，部局間接続に 10GbE を採用するとともに，VRF を用いて複数の論理ネットワークに分けた構成となっている．本稿では，旧ネットワークシステムにおけるネットワーク運用の問題点について考察するとともに，問題点を踏まえたネットワークの設計方針について述べる．さらに実際に拘置したネットワークの物理構成および論理構成について概説する．

Deveopment of a Network System in Kobe University

Itsuo Hatono,[†1] Yoshihiro Ban[†1]
and Hiroshi Sasaki[†1]

This paper describes a development of campus network system in Kobe University. In the network, 10GbE Layer 3 switches are used for the connections between the faculties in Kobe University. For the security reason, the physical network is devided into several logical networks. The VRF technique is introduced to realize the logical networks. In this paper, first, the issues of network managent structures in Kobe Univ are discussed. Furthremore, the physical and logical structure of the network are described.

1. はじめに

神戸大学におけるキャンパスネットワークの整備は，1993 年，1995 年, 2001 年に実施されている[⋆1]．ネットワークのトポロジ，機器・技術を以下に示す[1)]．

†1 神戸大学大学 学術情報基盤センター
Information Science and Technology Center, Kobe University

⋆1 神戸大学のキャンパスネットワークは，KHAN(Kobe Hyper Adacemic Network) と命名され, 整備年度により，それぞれ KHAN94, KHAN96, KHAN2001 と呼ばれている

KHAN94　(1993 年度)
　基幹ネットワーク主要技術： FDDI/ATM(OC3)
　ユーザ利用ポート速度： 10Base2/10Base5
KHAN96　(1995 年度) 主要技術：ATM(Lan Emulation)
　基幹ネットワーク主要技術： FDDI/ATM(OC-3/OC-12)
　ユーザ利用ポート速度： 10Base2/10Base5/10Base-T(ごく一部 100Base-TX)
KHAN2001　(2001 年度)
　基幹ネットワーク主要技術： GbE(1Gbps)
　ユーザ利用ポート速度： 100Base-T(ごく一部 1000Base-TX/SX)

この間，KHAN94 以前は学内で接続された計算機は, 数百台であったが，2009 年 3 月現在，ネットワーク利用ユーザは，20,000 名を超えるとともに，10,000 台を超える計算機が学内ネットワークに接続されていると推定される[⋆2]．

2. 現状のネットワーク運用形態

KHAN2009 構築にあたり，現ネットワーク (KHAN2001) で発生しているネットワーク運用およびセキュリティ管理上の問題点をネットワーク構成と運用で整理した．以下に, 詳細について述べる．

- **部局・学科設置 Firewall(以下，FW) 未設置**
  運用状況　グローバル IP 利用. IP 割当，接続機器管理は部局管理者.
  利点　ネットワーク機器の性能を最大限に利用可能
  問題点　部局ネットワーク管理者の労力大. 結果としてセキュリティ対策はユーザ依存.
- **部局設置 FW(部局基幹スイッチに接続)**
  運用状況　グローバル IP 利用. IP 割当，接続機器管理は部局管理者担当.
  利点　FW の内側においてネットワークの性能を最大限に利用可能. FW によるユーザのセキュリティリスクの軽減
  問題点　FW の運用・設定の管理コスト. FW の性能によるネットワーク性能の律速. 基幹ネットワーク側からの IP による接続機器の調査・切断に FW による制約が発生.
- **部局全域 NAT FW 利用**

⋆2 学外向け通信でユニークな IP 数が約 9,000 であった事実より推定している．

運用状況　プライベートアドレスを利用，IP 配布は部局管理者担当.

利点　FW の内側においてネットワークの性能を最大限に利用可能. FW によるユーザのセキュリティリスクの軽減

問題点　FW の運用・設定の管理コスト. FW の性能によるネットワーク性能の律速. 利用グローバル側とプライベート側との通信を対応させることが困難. 結果としてインシデント発生時の調査が困難.

- **小規模 NAT FW 設置 (FW はエッジスイッチに接続)**

運用状況　NAT ルータを利用. 内部はプライベートアドレス利用. IP 配布 (多くは DHCP を利用), 接続危機管理は研究室内.

利点　NAT FW 内と外部を独立に運用可能. NAT ルータにより外部からの接続は遮断されるため, ユーザのセキュリティリスクが軽減.

問題点　基幹ネットワーク管理者の NAT FW 内ネットワークへの関与は困難. 問題発生時の調査はすべて設置組織が担当 (多くは研究室単位). 外部への通信と内部における通信を対応させることは困難.

- **認証付 DHCP 利用全面利用**

運用状況　部局・学科ほぼ全域でセンターの認証付 DHCP を利用. 接続機器管理は一部のプリンタ等のみ.

利点　ユーザ管理は, 神戸大学統合ユーザ管理システムで代替可能. 基幹ネットワークに設置された高速機器が利用可能.

問題点　認証のためのユーザサポートが必要 (場合によっては，ネットワーク利用にソフトウエアのインストールが必要). 利用ポリシーの個別のコントロールが詳細設定が困難. 外部公開サーバは設置不能.

以上のような状況は，KHAN2001 導入以降，セキュリティに関する外部環境およびユーザ意識の変化により発生したものである. この中で，独自で導入した FW 機器を利用している部局においては，運用に問題があると判断される場合が少なくない. また，NAT ルータ配下に PC が多く接続されている場合，インシデント発生時の調査に支障が出た例も存在する. 一方で「認証付 DHCP 利用全面利用」は，神戸大学における文系の学部で大規模に利用されている. 利用部局では，学生のネットワーク利用を認証付 DHCP 接続のみとしており，IP 配布，ユーザ管理などのコスト低減を実現している.

また，教育研究系，事務系，認証付 DHCP 接続などのためのネットワークは，セキュリティ上あるいはネットワーク運用上の観点から，論理的あるいは物理的に分離したネットワーク構成とすることが望ましい. 現状は，物理配線により「物理的」に分離する構成となっているが，配線上の問題から，これ以上物理的に分離することが困難であるという問題があった.

3. 新神戸大学情報ネットワーク (KHAN2009) 構築の基本方針

2009 年には，前回の整備 (2001 年) から 7 年が経過し，機器の老朽化による故障率の増大および基幹ネットワーク機器がメーカによる保守停止年限に達したという問題に直面していた. 一方でネットワークは大学の活動に必要不可欠なインフラであり，安定性・セキュリティ・運用・導入コスト低減への要求が以前と比べて高くなってきている. このような状況の下で，神戸大学では大学予算と概算要求による予算を利用することにより，2009 年度に神戸大学情報ネットワーク (KHAN2009) を整備しつつある[⋆1]. KHAN2009 設計における基本方針を以下に示す. 本方針は, 概算要求を計画していた 2007 年当時に設定したものである.

基本性能

- 安定しておりかつ 5 年間著しく陳腐化しない
- 部局間接続 10Gbps ベース/原則各部屋に 1Gbps を配線

冗長化

- 部局間接続の二重化 (機器の二重化は中心部のみ)

セキュリティ

- 対外接続： Firewall の設置/Mail・Web 通信の保護
- 内部： 部局等の単位の隔離/通信制限/認証ネットワーク

ユビキタス

- 学内認証付無線 LAN/認証付情報コンセントの整備
- 学外接続用 SSL-VPN の整備

4. KHAN2009 の構成

4.1 ネットワーク物理構成

以上のネットワーク設計方針に基づき構成した KHAN2009 の物理構成を**図 1** に示す. 図 1 におけるコアスイッチは，Brocade 社 NetIron MLX-8, 基幹スイッチには，Brocade

⋆1 原稿執筆時 (2009 年 9 月) は構築中である.

Vol.2009-IOT-7 No.1
2009/10/9

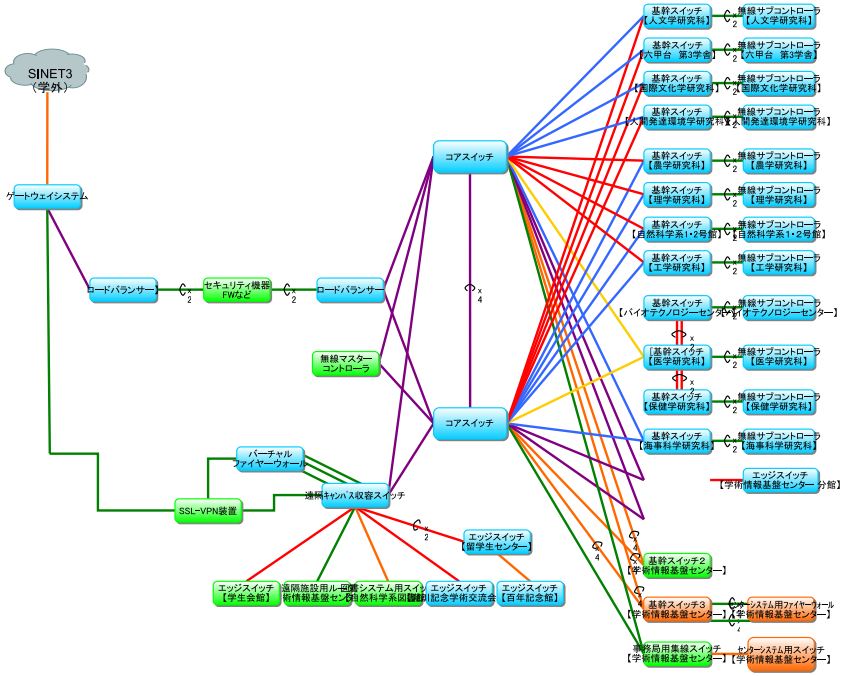

図 1　KHAN2009 の物理構成

社 NetIron CES 2024F/2048FX, Juniper 社製 EX-4200-24F を採用した．また，無線コントローラには, Aruba 社製 Aruba 6000/3400, SSL-VPN 装置には, F5 社製 FirePass 4320, エッジスイッチには，H3C 社製の L2 スイッチを採用した．

4.2　ネットワークの論理構成

KHAN2009 においては，教育研究系ネットワーク，事務系ネットワーク，認証付き DHCP 用ネットワークなど，要求されるセキュリティレベルが大きく異なるため，分離して構成することが妥当であると考えられるネットワーク群を, 図 1 に示す物理構成を，VRF(Virtual Routing and Forwarding)[2] を用いて論理的に分離した構成としている．ネットワークを論理的に分割して構成する技術として，MPLS(Multi Protocal Label Switching)[3] などが知られているが，KHAN2009 においては, 導入コストおよび低コストによるネットワークの拡張性を考慮して VRF を採用した．KHAN2009 における VRF の構成を**図 2** に示す．

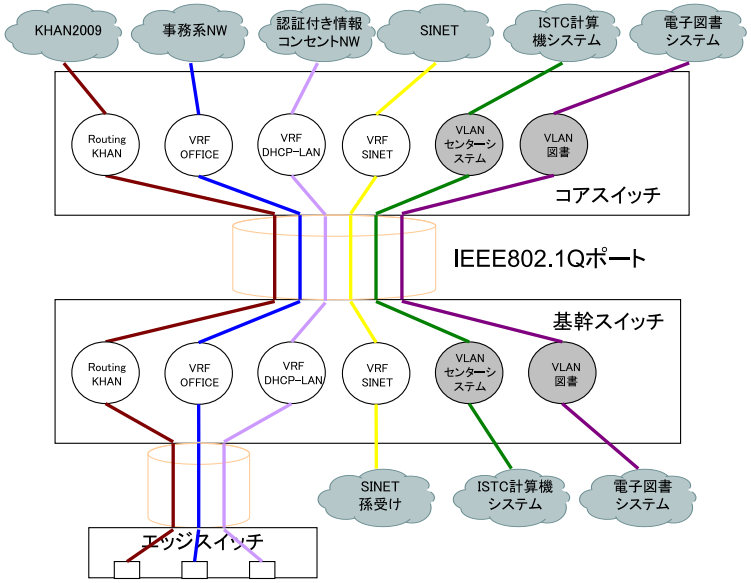

図 2　VRF の構成

論理的に分割された各ネットワークは，Virtual Firewall 装置を介して教育研究系ネットワークと接続されており，それぞれ独立なポリシーで Firewall のルールが設定されている．

5.　認証付無線 LAN システムの導入

KHAN2009 においては，以下に示す機能を持つ認証付無線 LAN システムを導入している．

- ユーザが，無線 LAN を利用するにあたって，統合ユーザ管理システム (神戸大学の全構成員が登録) の認証サーバを用いた認証が実施される．
- 接続する 無線基地曲の SSID により以下に示す異なった利用形態が実現可能である．
  - SSID 毎に利用可能なユーザ種別 (教職員，学生，所属) が指定可能である．
  - ある特定の部局内では，部局内のセグメントに認証付で接続可能である．
  - 認証方式は，Web 認証方式および IEEE 802.1X が可能である．
- 全無線アクセスポイントは，設定および稼働状況に関する集中管理が可能である．

本無線 LAN システムは，全学の教室・会議室などのパブリック・スペースに 200 台以上

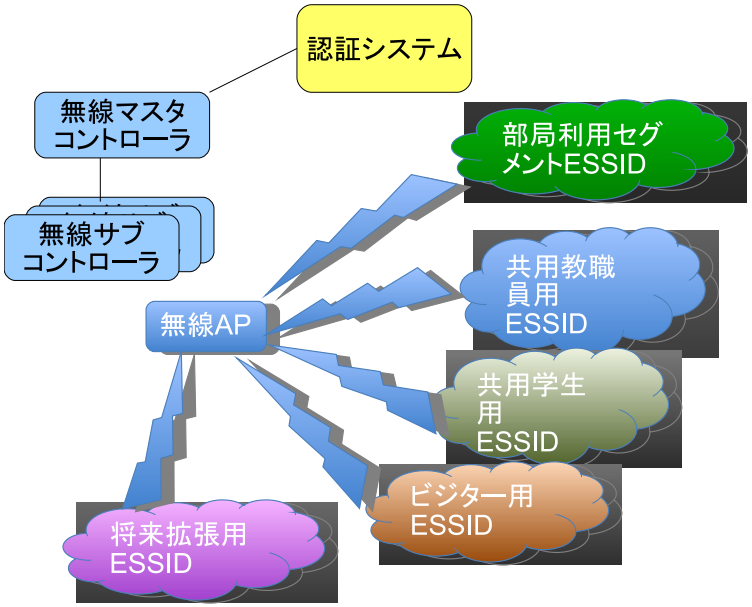

図 3 認証付無線 LAN システムの構成

設置されており，ネットワークの教育・研究利用を促進するとともに，部局におけるネットワークユーザの管理コストの低減に寄与することが期待される．

6. ネットワーク運用

本来，ネットワークセキュリティに関する設定は，ユーザの利用形態によってセキュリティレベルを決定して運用すべきである．しかし，大学内においてこのようなセキュリティレベルの設計・運用ができる人材は極めて限られており，しかも多くの場合はボランティアベースで実施されている．そのため，属人的になりがちであり，どのようなセキュリティレベルに現在のネットワークが設定されているかが失念されるケースも存在する．このような状態では，セキュリティに関する設定・運用を部局にすべて委託するというネットワーク運用では，利便性とセキュリティをバランスさせ，かつ安定した運用を行うことは困難であると考えられる．KHAN2009 においては，セキュリティ上の設定を簡素化し，集中化することを目的として，以下のような設定を導入している．

- セグメント毎に端末利用 IP レンジ，部局外公開用 IP サーバレンジを設定し，
  - 端末利用 IP レンジに関しては該当する部局外からの通信を遮断するアクセスリストを設定する．
  - 部局外公開用 IP サーバレンジに関しては，アクセスリストを設定しない (サーバ側での制限を想定.)[⋆1]．

ただし，移行措置として，現状端末利用レンジに部局外公開用サーバレンジが存在する場合，１回限りという条件で許可のルールを設定 (該当ルール削除以外の依頼は不許可) している．これにより，旧 KHAN2001 上で設置されていた部局導入 FW の機能を代替することが期待される．

7. 導入および運用上の課題

KHAN2009 の導入にあたっては，2007 年から数年に渡って仕様の検討を行ってきたが，実際に仕様を作成するにあたって課題として認識された事項ををを以下に述べる．

- **ネットワーク利用における SLA(Service Level Agreement)**
  一般に，情報関連のシステム導入を行う際には，SLA を設定した上で設計を行うことが一般的である．学内利用者の要求する SLA には，24 時間 365 日の稼働保障, 機器故障時の即時対応・復旧などがあげられるが，KHAN2009 の導入に当たり，運用予算の確保・体制の整備が出来なかったため，ビジネスアワーの対応とせざるを得なかった．本来は学内で十分に議論するべきである．
- **ネットワーク規模・構成の妥当性評価**
  各部局の人員構成および建物の構成は，大きく異なっている．各部局の教職員数，学生数が異なればネットワークの導入規模が異なることは自明であるが，ほぼ同じ教職員数・学生数であるにもかかわらず，必要となるネットワーク機器の規模が大きく異なる場合が発生した．多くは建物の構成に起因していると思われる．しかし，KHAN2009 は多くを学内予算で賄っているため，学内に適切な投資であることを説明する場合に問題が発生する可能性がある．また，部局から要求が妥当であったかを評価する必要がある．KHAN2009 においては，トラフィックを適切に記録して，次回以降のネットワーク更新の資料とする予定である．
- **ネットワーク運用体制**

⋆1 神戸大学においては，学外へ公開するためには対外 FW 設定のための申請が必要である．

神戸大学学術情報基盤センターが，神戸大学のネットワーク管理を担当しているが，人員が限られているため，IP 割当などのユーザの管理は各部局側で実施することとしている．しかし，部局側のネットワーク管理に対する取り組みは様々なレベルであり，部局側の都合に合わせた機器の導入・設定を行うとコスト高になる．

- **ネットワーク管理人材の不足**
  現在，ネットワーク利用者の「ユーザ化」が急速に進行している．一方でネットワークは複雑化しているため，ネットワーク管理ができる人材が不足するという事態に直面している．ネットワークの構築にあたっては，エンドユーザへのレベルに応じた説明が不可欠であるが，部局によっては管理者がユーザレベルのスキルしか持たない場合もある．このような場合，ネットワーク設定に関する正しい情報が収集できないリスクがある．

8. 終 わ り に

本稿では，2009 年度に導入した神戸大学情報ネットワーク KHAN2009 の設計方針，構成および課題について述べた．今後は，KHAN2009 の構成，機能の周知を計り，神戸大学におけるネットワーク運用の効率化を図るとともに，次期ネットワーク導入 (6 ないし 7 年後を想定) に向けて準備を進めていく予定である．

謝辞 KHAN2009 構築および本稿の執筆にあたっては， KHAN2009 構築を担当した NTTPC コミュニケーションズ (株) 村岡賢二氏並びに NTT 西日本担当者を含む KHAN2009 構築担当者グループに多大なる寄与を頂いたことを附記し，謝意を表する．

参 考 文 献

1) 神戸大学百年史編集委員会編: **神戸大学百年史**, 神戸大学 (2002)
2) RFC2547 (2003)
3) RFC 3031 (2001)