KHAN2009の導入 –学長表彰特別賞受賞 –

情報基盤センター 鳩野逸生，伴好弘，佐々木博史, 北内一行

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]．2010年10月に，KHAN2009導入に関する功績が認められ，学長表彰特別賞が授与された．2009年度に導入されたKHAN2009は，神戸大学の教育・研究・大学運営を支える最重要な情報基盤の一つであるが，当グループは，KHAN2009の企画・文部科学省への概算要求および予算要求，仕様策定，導入を一貫して担当し，旧ネットワークより高性能で信頼性の高いネットワークを非常に安価に導入することに成功した．さらに，KHAN2009の一環として，全学認証無線LANシステムを導入し，神戸大学構成員のネットワーク利用の利便性を大幅に向上させたことが評価されたものである．以下に，KHAN2009の概要および導入の経緯について紹介する．

2. KHAN2009導入の経緯

旧神戸大学情報ネットワークKHAN2001が導入されて4年が経過した 2005-6年頃から次期ネットワークシステム導入の必要性は当時の学術情報基盤センター内で認識されていた．しかし，当時はネットワークのような「基盤的なシステム」は文部科学省における「概算要求」の対象にならず，また学内で予算が捻出される見通しもなかった．その後，平成18年に神戸大学ICT戦略が策定され，ネットワーク更新はその中で最優先の課題に位置付けられた．

その後，2007年頃になって基盤的なシステムに関する概算要求も認められるようになったのを契機に2007年，2008年に次期情報ネットワーク更新に対する概算要求が作成され，文部科学省に提出された．2007年には認められなかったが，2008年に，2009年度の予算としてネットワーク更新費が認められた．これは，当時の執行部が概算要求が認められない場合でも2009年度にネットワーク更新を行うことを決定したことで，更新予算において「総額の半分以上の自己負担分」が入った計画であったことが功を奏したものと思われる[2]．

3. 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．

---

[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

[2]概算要求が認められる以前に導入手続きを開始していた．

- **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**

  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．

4. 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) を整備した．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

5. KHAN2009 の構成

5.1 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．

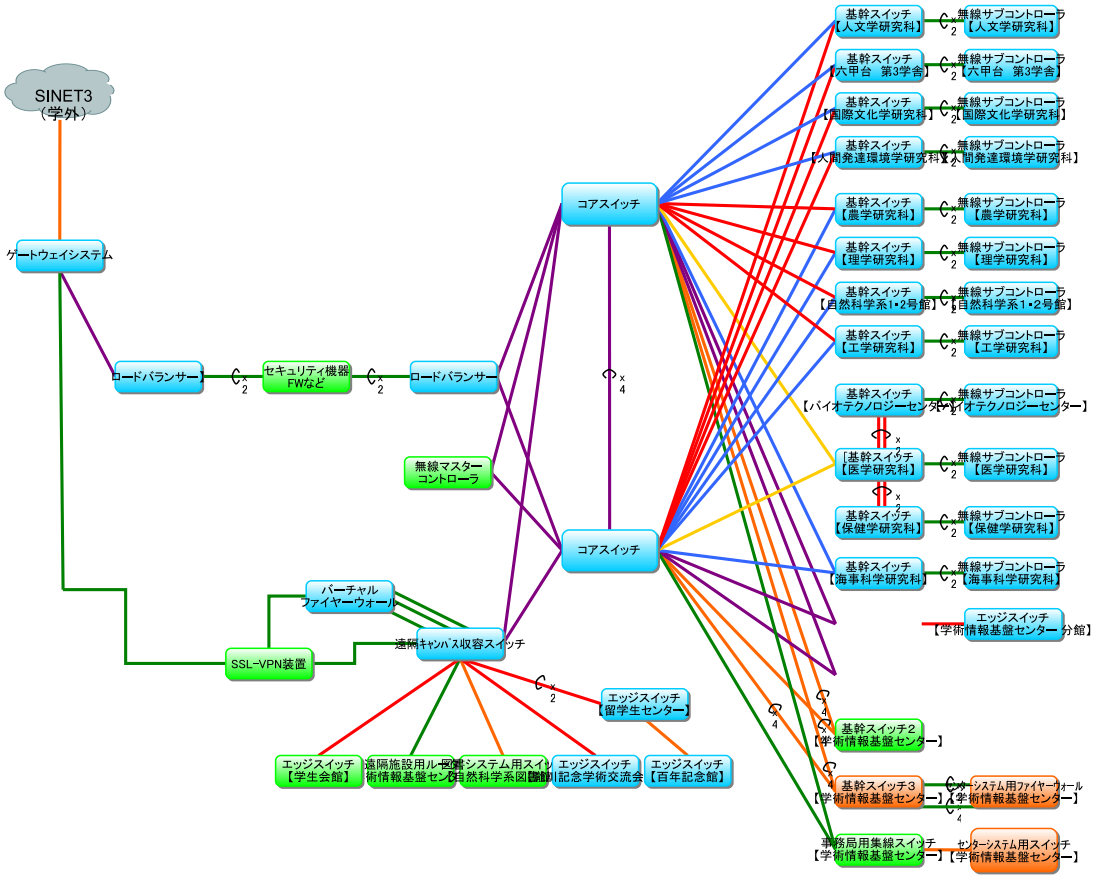

図 1: KHAN2009 の物理構成

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 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．

5.2 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)[1] 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)[2] 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．

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．

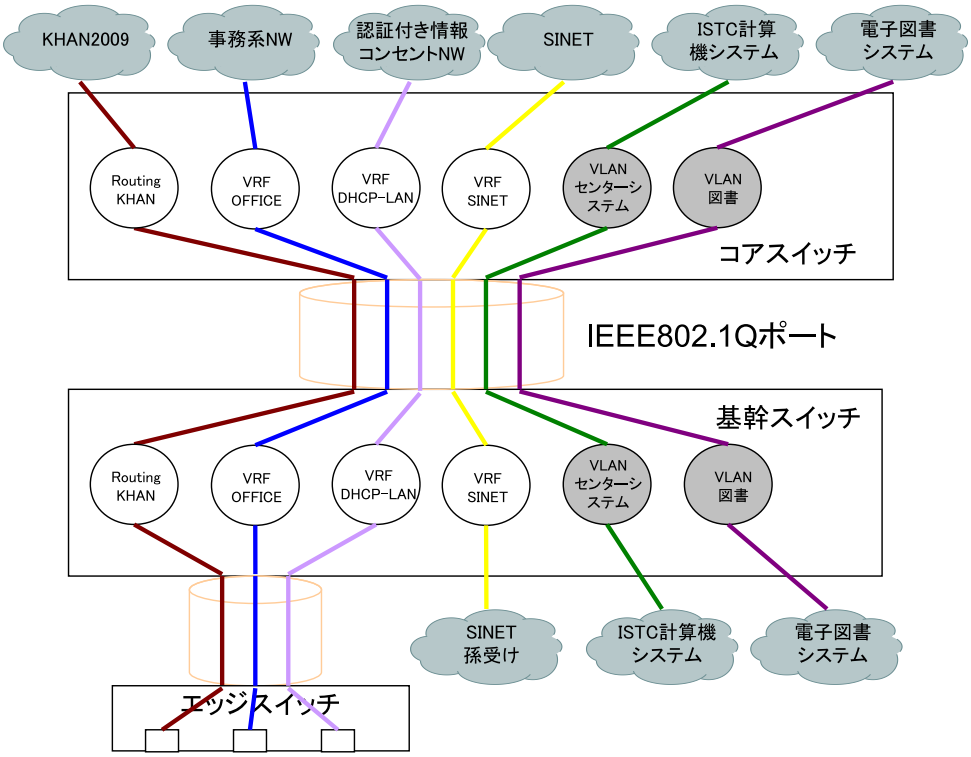

図 2: VRF の構成

6. 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，2011 年 3 月現在，全学の教室・会議室などのパブリック・スペースに約 250 台以上設置されており，学内の教室・会議室のかなりの部分をカバーしている．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．

7. 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

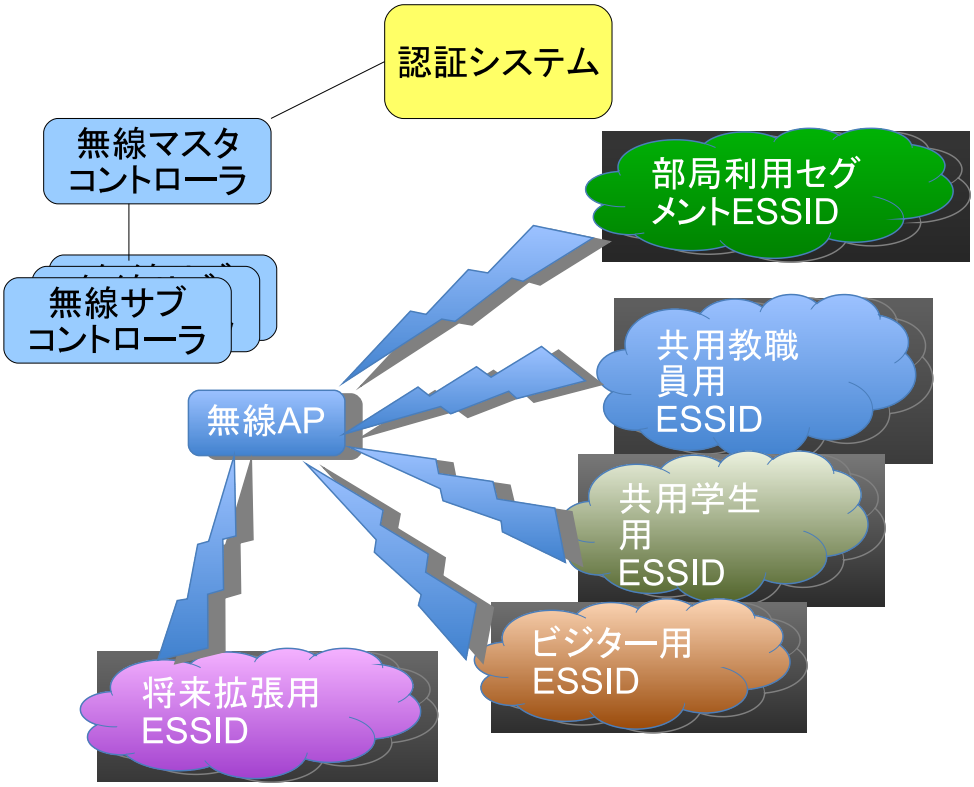

図 3: 認証付無線 LAN システムの構成

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.)[3].

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．

[3]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．

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．KHAN2009 は, 大学における先進的なネットワーク技術の取り組みとして ASCII テクノロジー　2010 年 6 月号, 日経コミュニケーション　2010 年 6 月号に取り上げられるとともに，ベンダーのプレスリリース，ユーザ事例 (ブロケードコミュニケーションシステムズ (株), ブロケードコミュニケーションシステムズ (株) ユーザ事例, Aruba Network 社ユーザ事例など) に取り上げられている．

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．

参考文献

[1] RFC2547 (2003)

[2] RFC 3031 (2001)