Vol.2018-IOT-43 No.4
Vol.2018-SPT-30 No.4
2018/9/27

神戸大学におけるキャンパスネットワークの更新および全学無線LANサービスと統合した研究室向けプライベートネットワークの導入

鳩野 逸生[1,a)]　伴 好弘[1]　伊達 浩典[1]　北内 一行[1]

概要：神戸大学では, 2018 年 1 月にキャンパスネットワークネットワークの全面更新を実施した．本稿では，キャンパスネットワーク (Kobe University Hyper Academic Network: KHAN 2017) の構成について概説するとともに，新しく導入した教育研究用プライベートネットワークと全学無線 LAN システムとの統合について述べる．

1. はじめに

神戸大学では 2009 年 10 月にネットワークを更新 (KHAN2009)[1][*1]を行って以来，7 年以上が経過し，エッジスイッチ, ファイアウォール，基幹ルータの一部機器のサポートが終了し，安定稼働に支障が生じている状況であった．

一方で，2009 年度の更新時から，情報セキュリティに関する環境や，大学内の組織構造が激変し, KHAN2009 におけるネットワークの設計では対応が困難になって来ていた．2017 年度における更新 (KHAN2017) においては，ネットワークの L2 化，教育研究用のプライベートネットワークの導入，および全学無線 LAN と教育研究用プライベートネットワークとの統合を主な柱として更新を実施した．

本稿では，KHAN2017 の設計方針，構成について述べるとともに，教育研究用プライベートネットワークの導入，および全学無線 LAN との統合について述べる．

2. 旧ネットワーク (KHAN2009) の状況

旧ネットワーク (KHAN2009) の物理構成を 図 1 に示す．KHAN2009 におけるルーティングは，学部間のルーティングをコアスイッチ, 各学部内ルーティングを，各学部の入り口に配置した L3 スイッチで行う L3 構成のネットワークであり，IP アドレスは，原則的に基本的に各部局

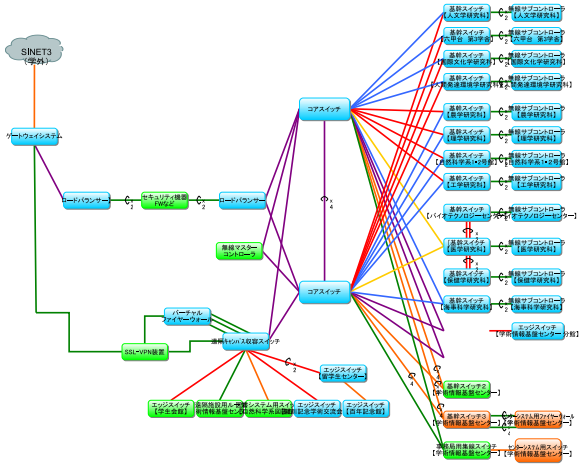


図 1　KHAN2009 の物理構成

の建物毎に異なったグローバルアドレスのセグメントを割り付ける構成となっており，IP アドレスの割付に関しては，各部局に委託，という形式を取っていた[*2]．

このような情況の下で，更新前のネットワークにおいては, 少なくとも 1,000 台以上の小規模なルータあるいは無線ルータが接続されていると推測され [2]，以下のような問題を引き起こしていた．

- ユーザによって設置されたルータ機器の老朽化によるネットワーク障害の多発
- ルータの LAN 側に接続された PC 上で発生した情報セキュリティインシデント発生時の原因特定までの長期間化

一方で，大学内で組織の再編が進み，新しい研究科や研

[1] 神戸大学
Kobe Univ., 1-1 Rokko-dai, Nada, Kobe 657-8501, Japan
[a)] hatono@kobe-u.ac.jp

[*1] 神戸大学のキャンパスネットワークは，KHAN(Kobe Hyper Academic Network) と命名され，ネットワーク整備年度により，KHAN XXXX (XXXX: 年度) と呼ばれている．

[*2] 事務系のネットワークは例外で，プライベートアドレスを利用していた．

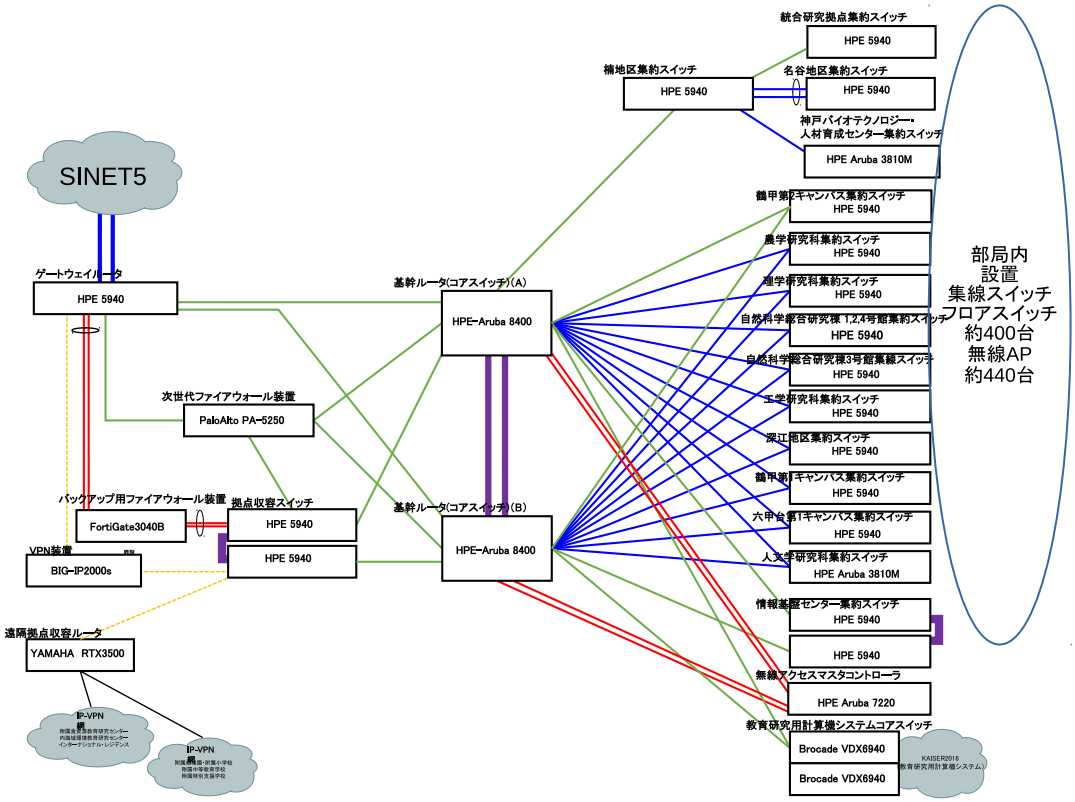


図 2　KHAN2017 の物理構成

究センターが設立されたが，スタッフは，多くの場合既存の研究科との兼任であり，研究実行上の組織と，所属組織，研究室が存在する建物の管理部局が必ずしも一致しない状況が数多く発生していた．同一の研究室が，他部局が管理する建物に分散して配置されているという場合もある．この場合，研究室内で NAS(Network Attached Storage) などを共有するには，グローバルアドレス上に接続する必要があるなど，セキュリティ管理上問題がある状態となっていた．

3. KHAN2017 の設計方針

前節で述べた問題に対処するため，KHAN2017 においては，以下の方針でネットワークを構築した．

(1) **ルータを集約した L2 構成の採用 (一部例外)**
- 全学の任意のフロアスイッチのポートに任意の VLAN を設定可能とする運用開始
- フロアスイッチ設定管理システムの開発
- 医学研究科地区のみ例外としてルータを配置 (停電時の最低限の通信確保のため)

(2) **全学無線 LAN サービスの維持**
- KHAN2017 における全学無線 LAN サービスは維持 [1]

(3) **基幹ネットワーク側によるプライベートネットワークの導入 (教育研究向け)**
- ローカルに設置されたルータの代替となることが目標
- 1,000–2,000 セグメントを想定
- 全学無線 LAN のアクセスポイントからのプライベートセグメントの利用
- VPN サービス (学外からの接続) からのプラベートセグメントへの利用

(4) **IDS の導入/ネットワーク利用記録収集の強化**
- 次世代 Firewall の導入
- ログ収集サーバの大容量化と収集接続記録の拡大

図 2 に KHAN2017 の物理構造を示す．

基幹ルータ，無線コントローラ, および主要ネットワーク機器には HPE 社の製品を採用している．

4. 教育研究用プライベートネットワーク

4.1 教育研究用プライベートネットワークの構造

神戸大学内におけるネットワークの運用状況から無理なくプライベートネットワークに移行することを目指し，以下の 3 種類の属性を持つプライベートネットワークを定義した．

(1) **クライアント用プライベートセグメント**
- ユーザ設置のルータの代替を意図
- 他のプライベートからの通信は遮断

(2) **グループ (部局) 公開用プライベートセグメント**
- グループ (部局) 内[*3]で共有する機器を接続用のセグ

[*3] 規則上に定義された部局には 1 対 1 対応はさせず，一体運用されていると思われる部局をまとめてグループと称している．

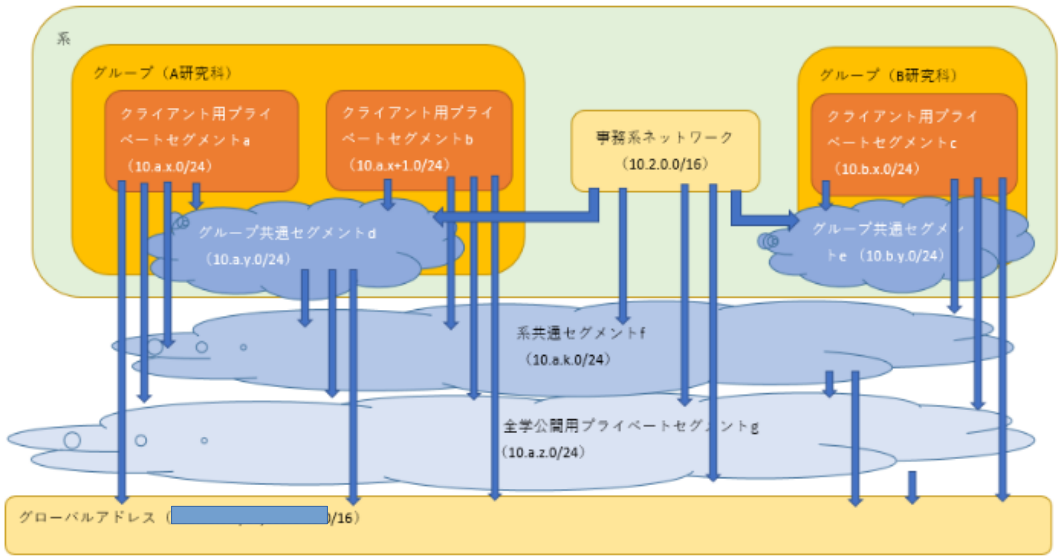


図 3 教育研究用プライベートネットワークのアクセス許可の構造

メントを意図

- 同グループ内のクライアント用プライベートセグメントおよび事務系プライベートセグメントから通信可能

(3) **系共通プライベートセグメント**

- 自然科学系，人文科学系，など複数の部局で共有する場合に利用するセグメント．同一の「系」のプライベートセグメントからの通信を許可

(4) **全学公開用プライベートセグメント**

- 全学のプライベートセグメントから通信可能．
- 全学へ公開する必要があるが，グローバルに配置する必要がない機器を接続するために設置することを意図．

図 3 に教育研究用プライベートネットワークのアクセス許可の構造を示す．

各セグメント間の通信制御は，基幹ルータ (コアスイッチ) における ACL(Access Control List) によって行っている．基幹ルータに設定可能な ACL の数には上限があるため，各セグメントに対するプライベートアドレスの割当てに際しては，各 ACL においてネットマスクによる表現が可能なように割当てている．

グローバルネットワークへ出る際の NAT 処理は，KHAN2017 で導入した次世代 Firewall において，NAT 用の仮想 Firewall を設定することにより実施している．NAT 処理後の通信は，KHAN2017 グローバルネットワークに折り返され，再び Firewall を通過して学外へ通信される．KHAN2017 におけるネットワークサービスの分割とルーティングの概要を**図 4** に示す．

5. 全学無線 LAN サービスとの統合

KHAN2017 における教育研究用プライベートネットワークの導入においては，全学に設置されている全学無線 LAN 用アクセスポイントすべてからプライベートセグメントへ直接接続する機能の実装を行った．無線コントローラ (HPE 社製 HPE Aruba 7220 Mobility Controller)[3] および認証サーバの動作は以下のとおりである．

(1) 無線利用ユーザが, 教育研究用プライベートネットワーク用の SSID に接続
(2) 認証サーバにおいて，ID/パスワード認証を実施．
(3) 認証サーバにおいて，LDAP 属性に基づく認可を実施．
(4) 認証サーバにおける認可のマルチソース機能を用い，後述のプライベートネットワーク管理システムへアクセスし，ユーザに割当てる VLAN ID を取得．
(5) 無線コントローラは，ユーザの接続に対して, 認証サーバから取得した VLAN ID を割当てて接続．

本接続サービスにおいては，認証サーバに HPE 社製 ClearPass[4] を用いるとともに，認証には IEEE 802.1x を採用している．なお，ID，パスワードおよび所属等による認可処理には，ClearPass を介して神戸大学における統合ユーザ管理システムが提供する LDAP サービスを利用している．

6. プライベートネットワーク管理システム

前述したように，KHAN2017 で導入するプライベートネットワークは，1,000 セグメント以上設置することが見込まれる上に, 各セグメントの管理者および利用ユーザの変更も頻繁に行なわれることが予想される．従って，すべて手作業による管理は不可能に近いと考えられたため，プ

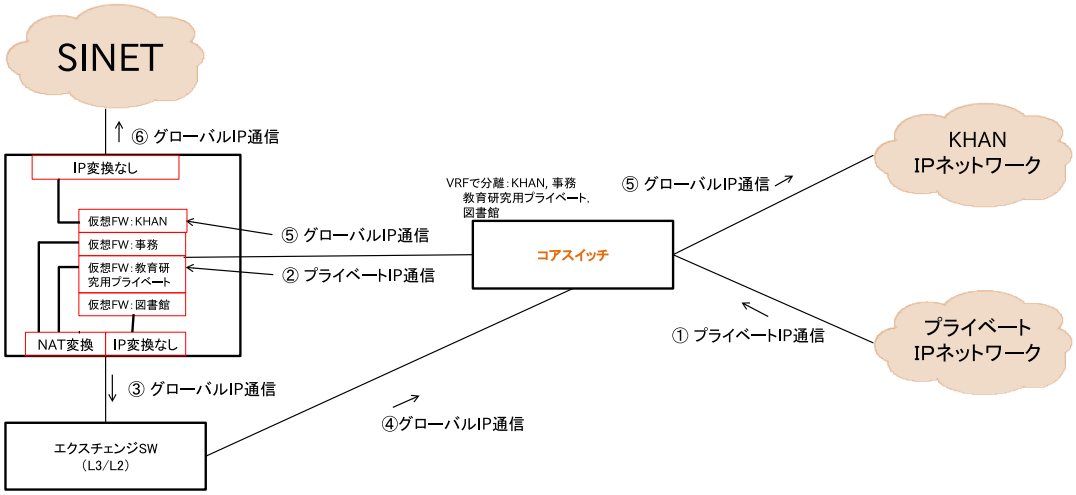


図 4　ネットワークサービス分離と経路制御

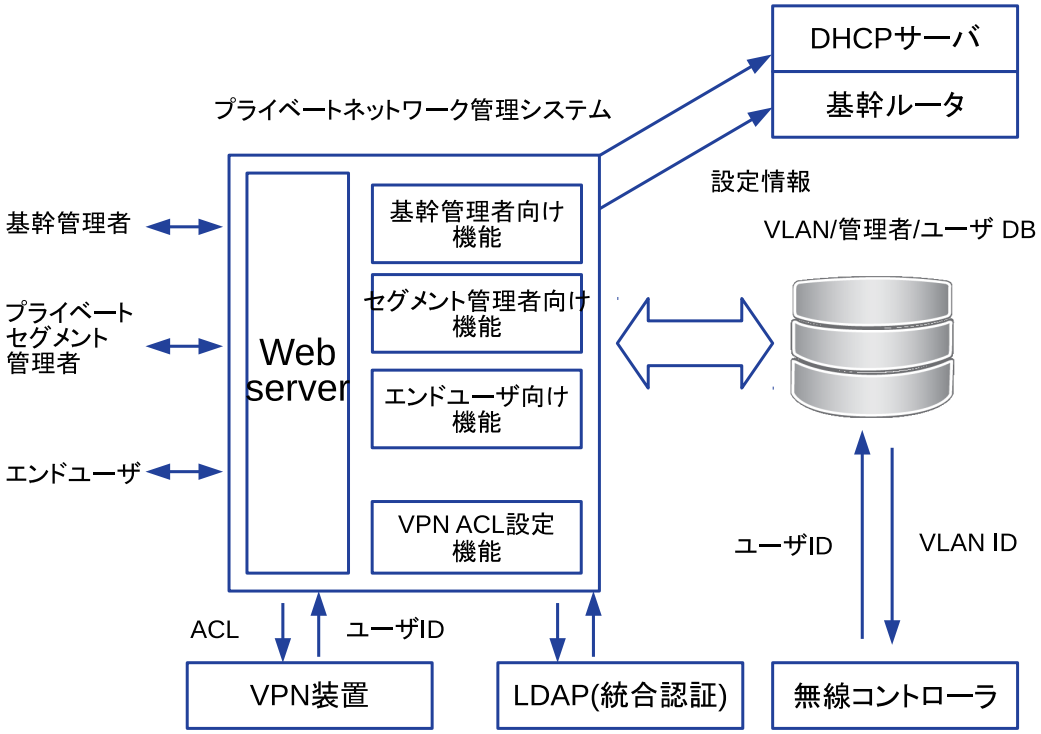


図 5　プライベートネットワーク管理システム

ライベートネットワークを管理システムの開発を行った．主な機能を以下に示す．

- 基幹ネットワーク管理者向け機能
  - プライベートセグメントの登録・削除
    - フォーム入力インタフェース
    - 一定形式の Excel ファイルアップロードによる登録フォーム
    - 登録内容修正フォーム
  - プライベートセグメント管理者登録・編集機能
    - プライベートセグメント登録時からの管理者変更・削除
  - プライベートセグメント登録機能
    - データベースに登録されている情報を用いた基幹ルータおよび DHCP サーバの設定情報の生成・登録・削除
    - 管理者の在籍チェックおよび異動者の通知
- プライベートセグメント管理者向け機能
  - 全学無線 LAN からの接続許可フォーム
  - 情報基盤センター VPN サービスからの接続許可フォーム
  - 全学無線 LAN および VPN へ登録したユーザの在籍確認・自動削除
- ユーザごとのプライベート接続情報提供機能
  - 全学無線 LAN に対して，プライベートセグメント利用者の接続 VLAN ID を応答
  - VPN 装置に対して，接続ユーザ向けのプライベート

表 1　教育研究用プライベートネットワークの登録状況 (2018 年 8 月現在)

クライアント用セグメント	1,182
グループ用セグメント	167
系共通セグメント	30
全学用セグメント	10

セグメントアクセス許可情報を応答

- **エンドユーザ向け機能**
  - 接続可能なプライベートセグメントからの選択機能
  - VPN 接続許可状況確認機能

図 5 に，プライベートネットワーク管理システムの構成を示す．開発には, python3/django/PostgreSQL を用いた．なお，管理者およびユーザの在籍確認は，統合ユーザ管理システムが提供する LDAP サーバに問い合わせることにより実施している．

各プライベートセグメントは，基幹ネットワーク管理者への設置申請により本システムへの登録が実施される．登録後，実際に割り付けられた VLAN 情報を元に，フロアスイッチのポートに対するセグメントの割付申請を受け付ける (現在，フロアスイッチのポート割付管理・登録システムの開発中)．登録後，各プライベートセグメントの管理者は，本システムのプライベートセグメント管理者向け機能が利用可能となり，全学無線 LAN および VPN からの接続許可ユーザを自由に設定することができる．また，5 日以内の許可ユーザの接続状況も確認できる機能も実装している (**図 6**)．

全学無線 LAN または VPN の利用許可が設定された無線 LAN ユーザは，本システムにアクセスすることにより，自分自身がどのプライベートセグメントに対して許可が設定されているかを確認することが出来る．全学無線 LAN に関しては，同時に 1 つのセグメントにしか接続できないため，複数のプライベートセグメントに対して許可設定されている場合は，本システムを用いてユーザ自身が選択する必要がある (**図 7**)．

現在，KHAN2017 における教育研究用プライベートネットワークは，2018 年 8 月現在，1,000 を越すセグメントが登録されて稼働中である．登録状況を**表 1** に示す．

7. おわりに

本稿では，2018 年 1 月に導入した神戸大学キャンパスネットワーク KHAN2017 の構成の概要および教育研究用プラベートネットワークおよびプライベートネットワーク管理システムの構成と全学無線 LAN システムとの統合について述べた．

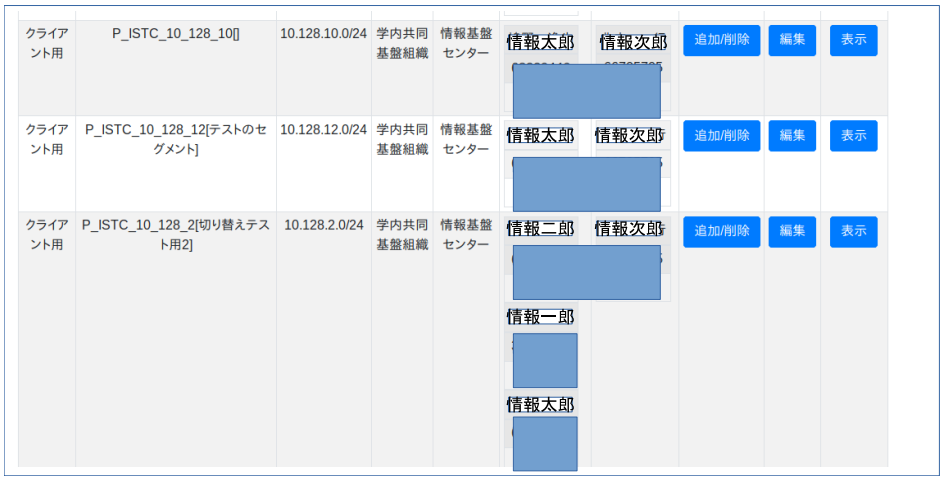
今後は，運用を通じてプライベトーネットワーク管理システムの改善を行う．将来は，有線接続においても全学無線 LAN 接続と同様な Dynamic VLAN による運用にしていく必要があると考えられる．さらに，KHAN2017 では，KHAN2009 に比べて接続された計算機がネットワーク上から見える範囲が広がり，ネットワーク監視の強化が実現できることが期待できる．ネットワーク上で収集した情報から，セキュリティインシデント発生時の情報収集の迅速化とともに，学内の教育研究活動の把握・分析のためのデータソースとして利用することを検討している．

謝辞

KHAN2017 の設計・導入にあたり，詳細な情報提供を頂いた，NTTPC 社村岡 賢二氏をはじめとする, NTTPC 社，HPE 社，NTT 西日本の技術者諸氏に感謝致します．また，KHAN2017 の予算確保および教育研究プライベートネットワークの運用設計に当たっては，情報基盤センター事務部に多大なるご協力を頂いたことに感謝致します．

参考文献

[1] 鳩野逸生，伴好宏，佐々木博史: 神戸大学におけるネットワークシステムの構築, 情報処理学会研究報告，Vol.2009-IOT-7 No 1, pp. 1–5 (2009)
[2] 鳩野逸生: ネットワーク接続記録収集によるネットワーク利用状況把握の試み, 情報処理学会研究報告, 2016-IOT-35, Vol. 2016, No 15, pp. 1–7 (2016)
[3] HPE 社: available from ⟨https://www.arubanetworks.com/ja/products/networking/controllers/7200-series/⟩ (2018 年 8 月現在)
[4] HPE 社: available from ⟨https://www.arubanetworks.com/ja/products/security/network-access-control/⟩ (2018 年 8 月現在)



(a) 管理対象セグメントリスト

(b) アクセス許可設定

図 6 管理者設定画面例

図 7 ユーザ設定管理画面例