2009年1月29日
サイエンティフィック・システム研究会
2008年度システム技術分科会第2回会合

日本最大規模のキャンパス認証ネットワーク ～HINET2007の構築と運用～

西村 浩二，相原 玲二，近堂 徹，大東 俊博，
田島 浩一，岸場 清悟，岩田 則和

広島大学 情報メディア教育研究センター

広島大学

本報告の内容

広島大学

- HINET2007の構築と運用
  - 導入の背景
  - 概要と特徴
  - 管理・運用・移行の方針
  - 設計・構築のポイント
  - 移行の支援体制とシステム
  - 移行の進捗状況

大学等のネットワークに対する要求

広島大学

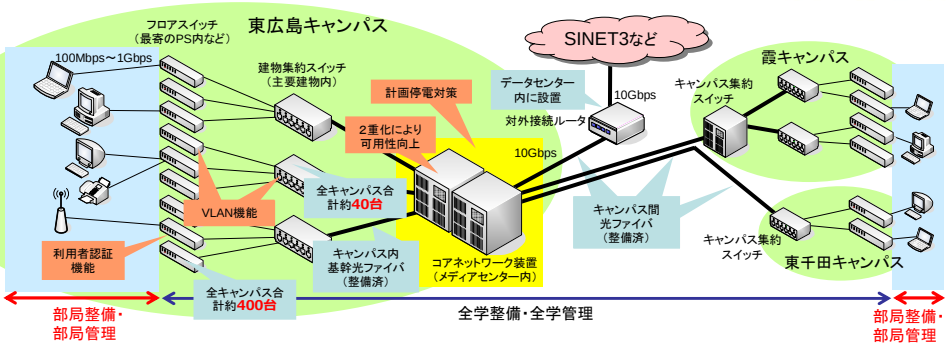
- 高度で柔軟なキャンパスネットワーク
  - 学部、学科、研究室等の単位でサブネット構築
  - 目的に応じて比較的自由な運用

ネットワークのライフライン化
セキュリティインシデントの多発

- 管理方針の根本的な見直し
  - 研究室は独立した企業活動（教員は社長）
  - しかし、外部からは同一組織とみなされる
  - さらに、経営の効率化を求められる

キャンパス情報ネットワーク HINET2007

広島大学



・2008年5月から本格移行開始
・規模
  - 主要3キャンパス（東広島、霞、東千田）、附属学校、小規模遠隔部局（東京，福山，尾道，竹原，呉，宮島）
・ 教員約1,800人、職員約3,300人、学生15,000人
・ フロアスイッチ約450台（約14,000ポート）を全学整備

HINET2007の特徴

広島大学

- 全学的な一元管理体制
  - ボランティアベースによるサブネット管理体制の破綻
  - 各フロアに設置するスイッチまで全学で一元管理
- VLANによる柔軟な仮想配線の提供
  - 同一研究室（グループ）が異なる建物等に分散する場合に対応
  - 学外向けサーバの設置、JGN2plusなどの利用に対応
- 個別ファイアウォール機能の提供
  - 全学ファイアウォール（対学外）のみでは不十分
  - ブロードバンドルータ相当の機能を教員数程度（約2,000個）提供
- すべての接続場所において利用者認証を要求
  - 多様な機器に対応するためWeb／MACアドレス認証を採用
  - 認証後はワイヤレートでの通信が必要

「ゾーン」の導入

広島大学

ゾーン名 略称	グローバルゾーン ゾーンA	ファイアウォール ゾーン ゾーンB	ローカルゾーン ゾーンC	公衆ゾーン ゾーンD
主な用途	**学外向けサーバ接続**	**学内共有サーバ接続**	**一般クライアント接続**	**オープンスペース**
外部IPアドレス	グローバル　固定割当	グローバル　固定割当	グローバル　固定割当	グローバル　DHCP割当
内部IPアドレス	外部IPアドレスと同じ	外部IPアドレスと同じ	プライベート（NAPT） DHCPまたは固定割当	外部IPアドレスと同じ
ゾーン外からの アクセス	学内外とも制限なし	学外から不可 ゾーンAを除く 学内から可	同一ローカルゾーン以外 から不可	学外から不可 ゾーンAを除く 学内から可
学外への アクセス	制限なし	制限なし	原則制限なし （NAPTによる 制限あり）	制限なし
端末認証	MACアドレス認証	MACアドレス認証	Web認証または MACアドレス認証	Web認証

これまでのサブネット構成とは異なる

HINET2007 / HINET2001間のアクセス

広島大学

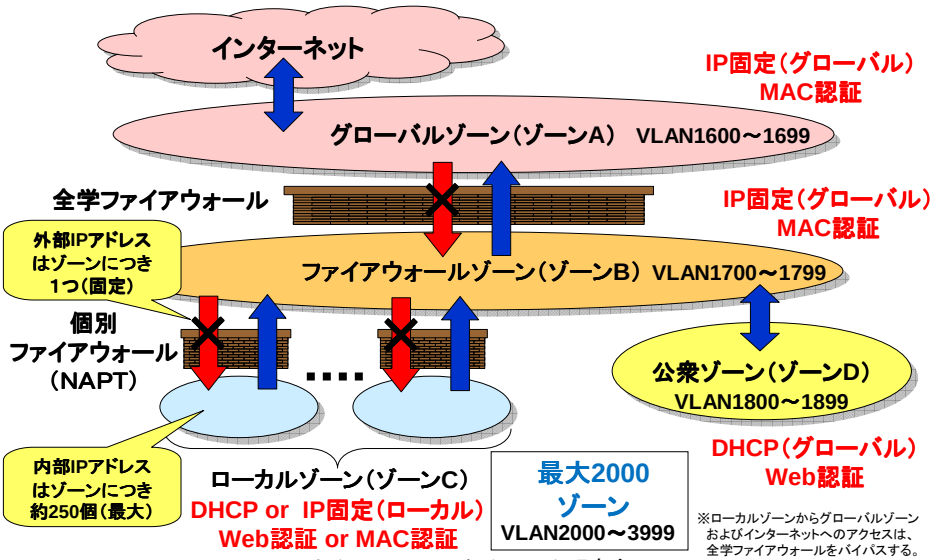
X → Y 方向のアクセス可否　　△：同一ゾーンC内ではアクセス可、異なるゾーンC間ではアクセス不可

X ＼ Y	ゾーンA	ゾーンB	ゾーンC	ゾーンD	全学サーバ	2001 Global	2001 FW	学外
ゾーンA	○	×	×	×	○	○	×	○
ゾーンB	○	○	×	○	○	○	○	○
ゾーンC	○	○	△	○	○	○	○	○
ゾーンD	○	○	×	○	○	○	○	○
全学サーバ	○	○	×	○	○	○	○	○
HINET2001 Global	○	○	×	○	○	○	○	○
HINET2001 FW	○	○	×	○	○	○	○	○
学外	○	×	×	×	○	○	×	—

全学サーバ：全学電子認証システムなど全学的サーバ接続用
HINET2001 Global：HINET2001の全学ファイアウォールに入っていないサブネット
HINET2001 FW：HINET2001の全学ファイアウォールに入っているサブネット

ゾーン種別とアクセス制限

広島大学



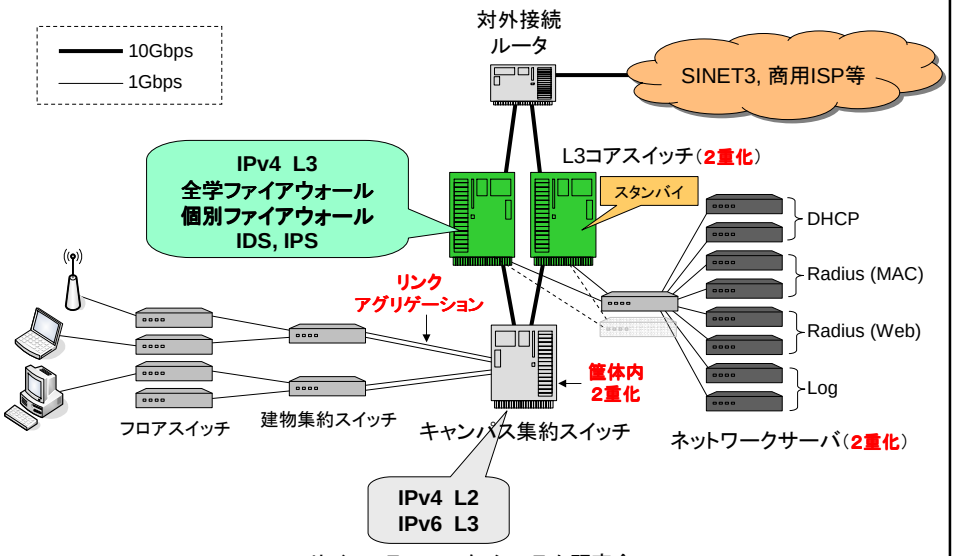
運用と移行の方針

広島大学

- 運用方針
  - 個別ファイアウォールの例外設定は行わない
    - テレビ会議装置はグローバルゾーン（ゾーンA）に置く、など
    - 利用者が適切なゾーンを選択し、自己責任で守る
  - 個別ファイアウォールのローカル側／グローバル側のＩＰアドレスの希望は受け付けない（メディアセンターが指定）
  - 希望すればスイッチの下流ポートへVLANをTaggedで提供（ただしVLAN IDはメディアセンターが指定）
    - 仮想ポート（1本の物理配線に複数のゾーンを載せることが可能）
- 移行方針
  - 移行期間は平成20年度末（2009年3月末）まで
    - 期間中はHINET2001とHINET2007を並行運用
  - IPアドレスのリナンバーが必要
    - 移行はポート単位で可能

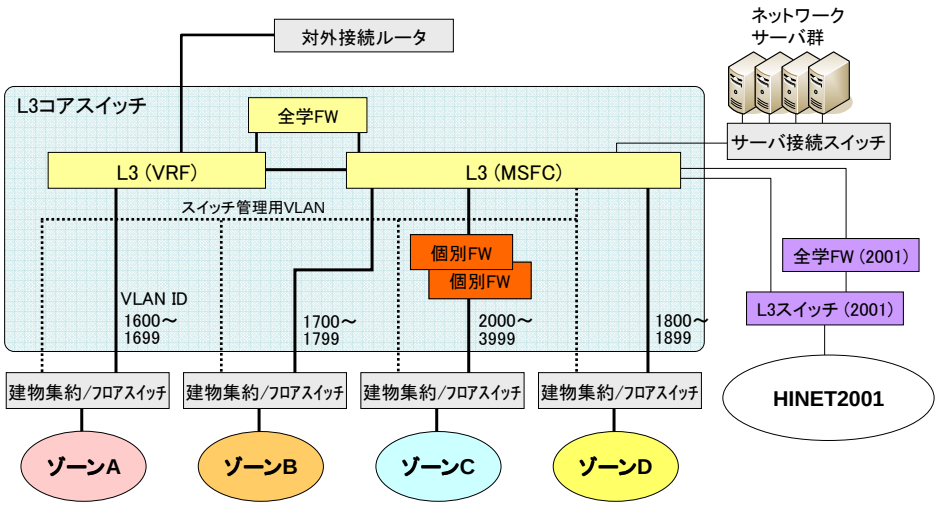
基幹ネットワークの物理構成

広島大学



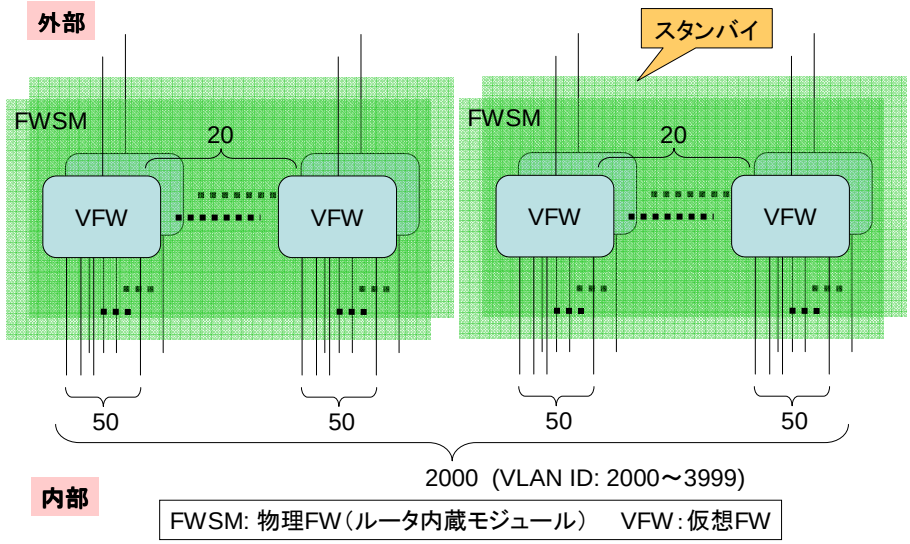
L3コアスイッチの設定

広島大学



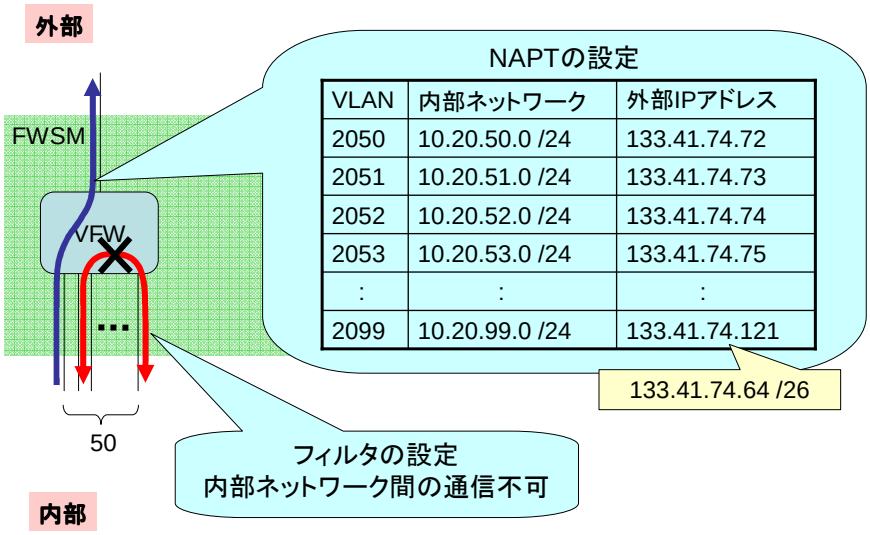
個別ファイアウォールの構成

広島大学



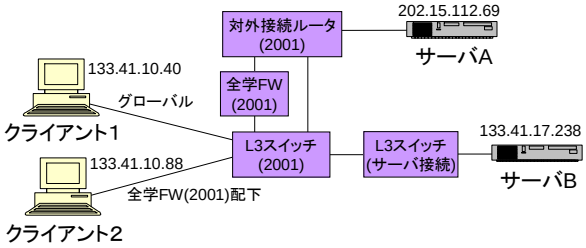
仮想ファイアウォールの設定

広島大学



移行前（HINET2001）の通信性能測定

広島大学

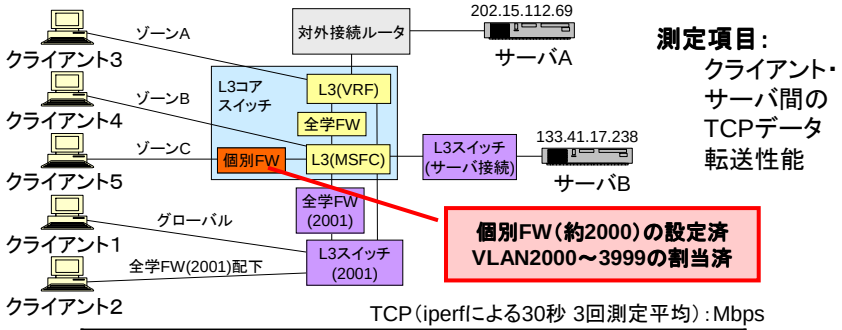


測定項目：
クライアント・サーバ間のTCPデータ転送性能

TCP（iperfによる30秒 3回測定平均）：Mbps

	サーバA		サーバB	
	送信	受信	送信	受信
クライアント1	505	444	672	620
クライアント2	--	360	680	645

HINET2007移行後の通信性能測定



測定項目:
クライアント・サーバ間のTCPデータ転送性能

TCP(iperfによる30秒 3回測定平均):Mbps

	サーバA		サーバB	
	送信	受信	送信	受信
クライアント1	471	517	704	709
クライアント2	--	365	691	615
クライアント3	637	685	712	878
クライアント4	--	348	696	801
クライアント5	--	292	--	433

利用者認証機能に対する要件(1)

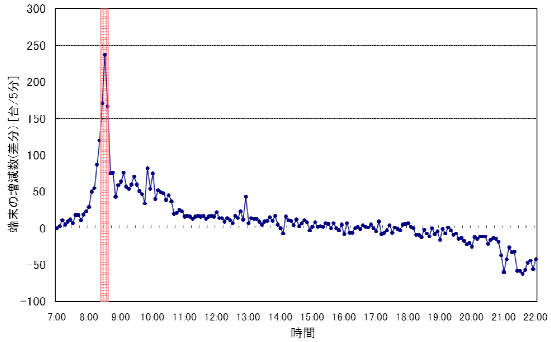
- ネットワークインフラとしての認証ネットワーク
  - 多様な機器に対応
    - 複数OSが混在（Windows, Linux, Mac OS X/9など…）
    - PC以外のネットワーク機器も認証
  - 既存の研究室内ネットワークとの親和性
    - ダムハブなども多数存在
  - 認証後でもワイヤスピードを確保
    - 認証を入れることによるパフォーマンス低下は×

最寄りのフロアスイッチにて利用者/機器認証
WEB（HTTPS）認証とMACアドレス認証をサポート

利用者認証機能に対する要件（2）

広島大学

- 短時間での一斉認証要求への対応
  - 共同利用施設（演習用端末室）や事務職員用端末
    - 広島大学には事務職員用端末が約1,400台存在



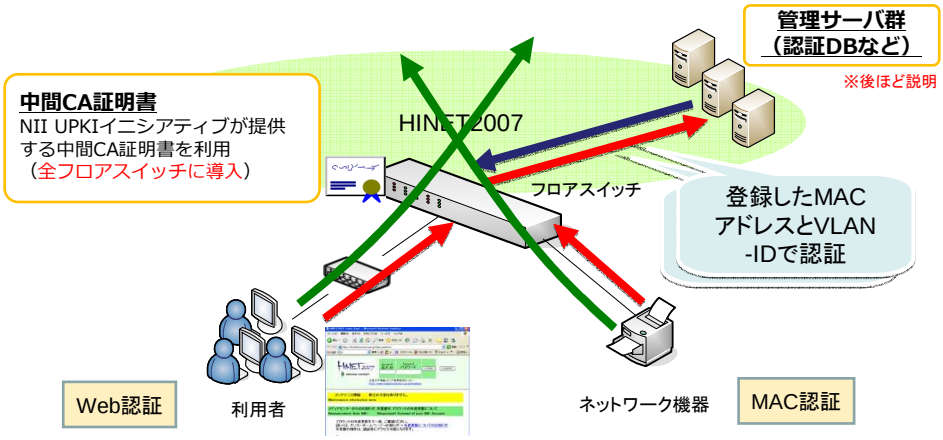
8時20分から35分（15分間）で約600台が稼働

100台からの同時認証を30秒以内で処理できることを条件

HINET2001における端末増減数（５分間隔）※2007年1月29日（月）に採取

利用者認証の概要

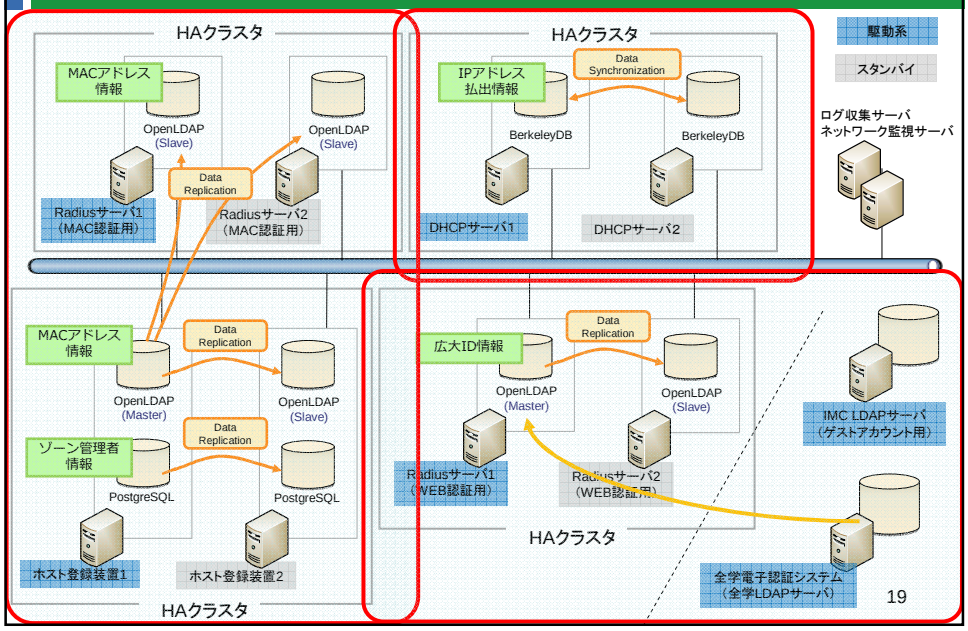
広島大学



https による利用者認証
初回接続時に認証ページをリダイレクト表示
全学電子情報基盤で管理するIDを利用
ARPポーリング/リンクダウンによるログアウト

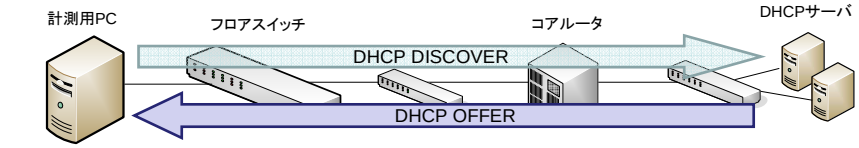
MACアドレスは事前登録（登録システムを利用）
Web認証が困難な機器を対象（プリンタ，NAS等）

HINET2007サーバ群の構成



DHCPサーバのIPアドレス払い出し性能

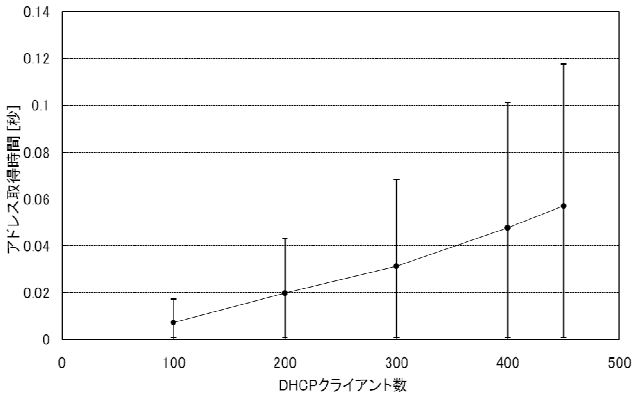
- 実験概要
  - 計測用PCを稼働中のフロアスイッチに接続
  - 複数DHCPリクエストを同時に送信
    - PerlのDHCPクライアントライブラリを利用
    - 異なるMACアドレスでDHCP DISCOVERを送信
  - DHCPリクエストからアドレス取得時間までを計測
    - DHCP-DISCOVER から DHCP-OFFER
    - DHCPサーバのIP払出しDB更新を含む



CPU: Core2Duo 3GHz
Memory: 4GB
OS: Linux

DHCPサーバのIPアドレス払い出し性能

広島大学

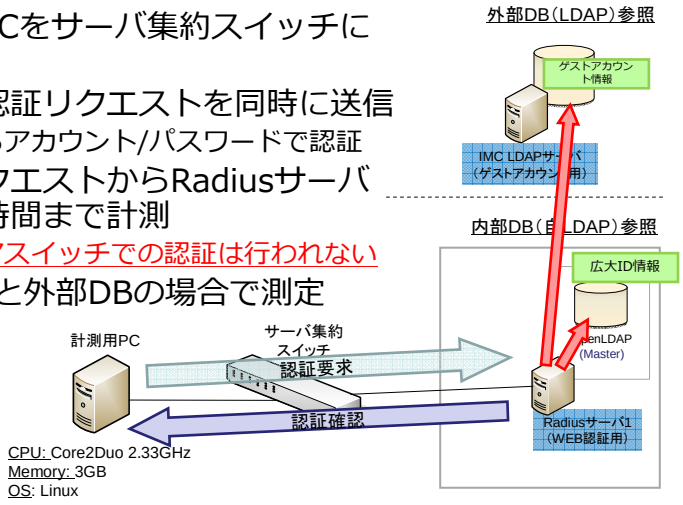


450台のDHCPアドレス取得要求に対して
最大0.12秒以内で処理が完了

Radiusサーバの同時認証性能

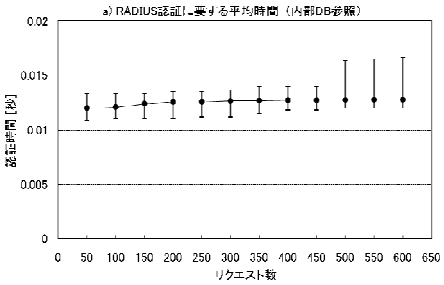
広島大学

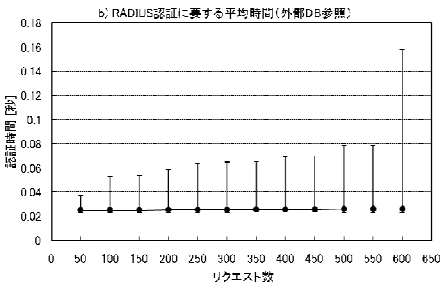
- 実験概要
  - 計測用PCをサーバ集約スイッチに接続
  - 複数の認証リクエストを同時に送信
    - 異なるアカウント/パスワードで認証
  - 認証リクエストからRadiusサーバの応答時間まで計測
    - フロアスイッチでの認証は行われない
  - 内部DBと外部DBの場合で測定



Radiusサーバの同時認証性能

広島大学





内部DB参照（通常のWeb, MAC認証）

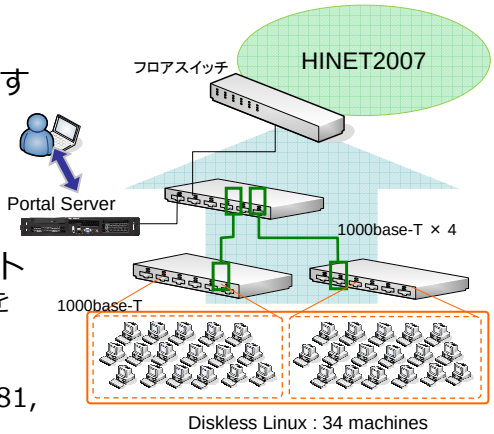
外部DB参照（ゲストのWeb認証）

600台からのRADIUS認証要求に対して
1秒以内に処理可能

認証スイッチの同時認証性能

広島大学

- 実験概要
  - フロアスイッチを経由する同時Web認証性能
  - リダイレクトと認証処理時間の和を計算
  - 100個の個別リクエスト
    - IMCゲストアカウントを利用
  - 同時接続セッション数
    - 1, 5, 10, 20, 30, 40, 81, 99
  - 認証リクエストは1秒以内で同期

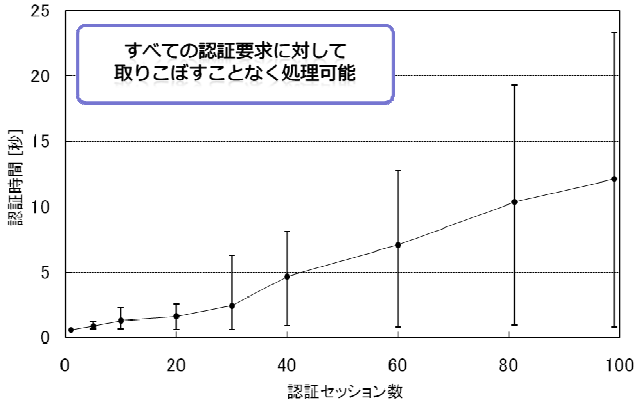


Diskless Linux : 34 machines
CPU: Pen-4 3GHz, Mem: 1GB

近堂ら, "PCクラスタによる認証スイッチの認証評価システム", 2007-DSM-47(5), pp.25--30

認証スイッチの同時認証性能

広島大学



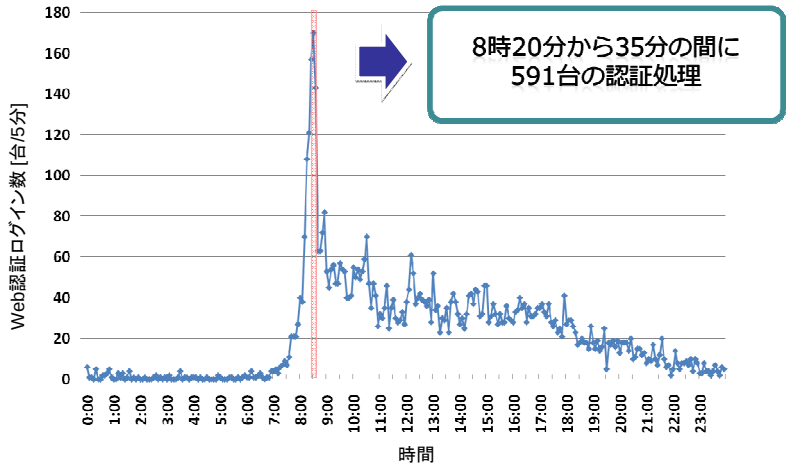
https接続
証明書鍵長 2,048bit

数セッションの同時認証では1秒
100セッションの同時認証でも最大23秒 **で処理可能**

現在の利用状況

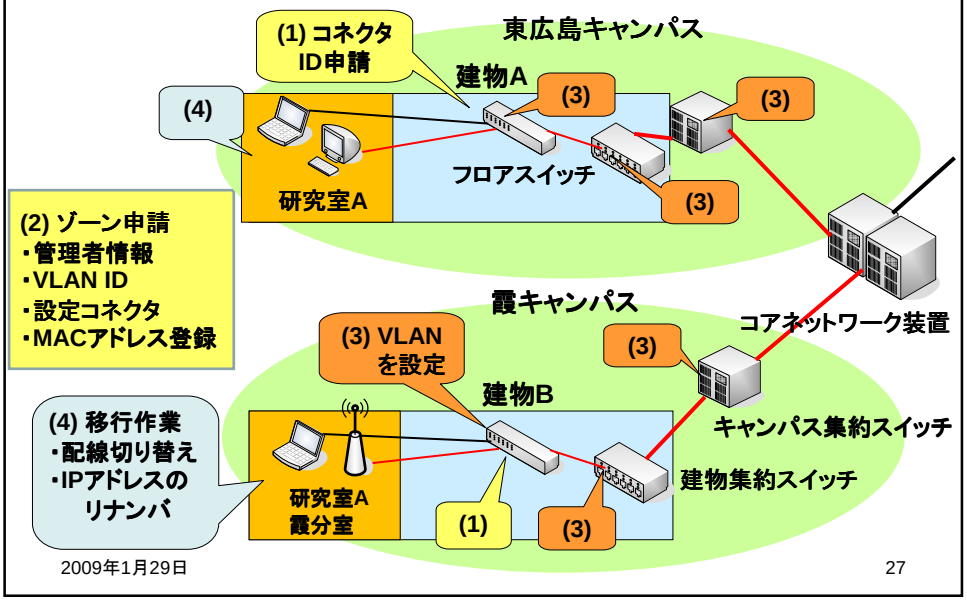
広島大学

- Web認証の推移（5分間隔のログイン処理数）



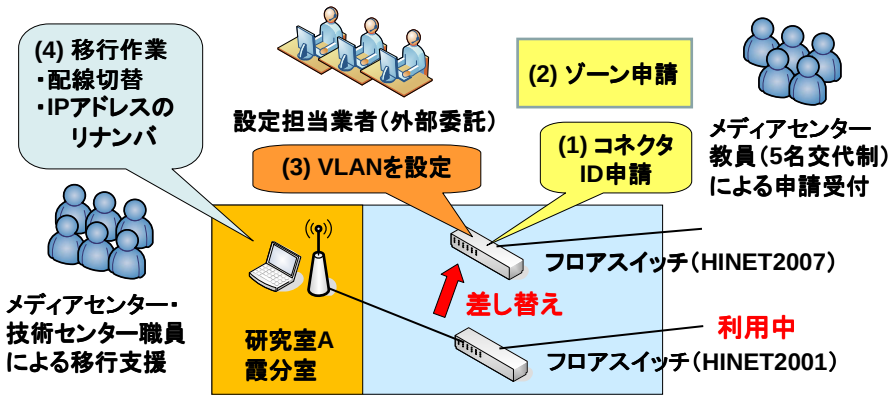
ネットワーク移行の概要（移行手順）

広島大学



ネットワーク移行の概要（支援体制）

広島大学

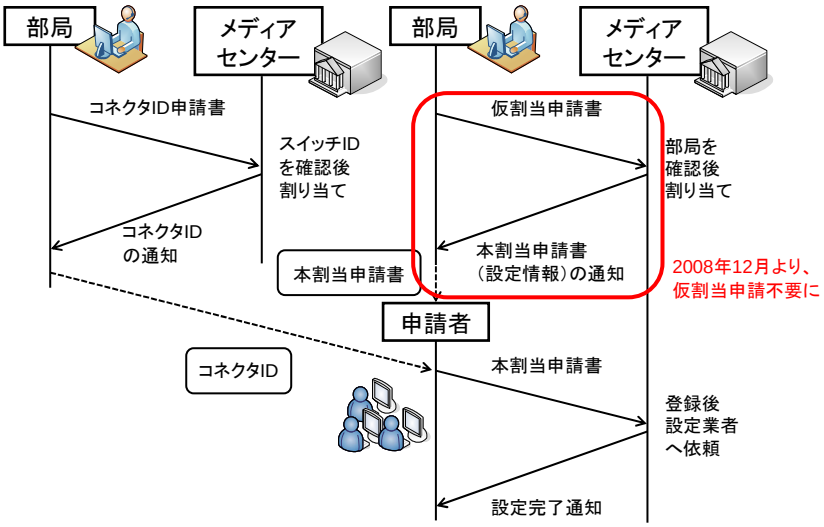


ポイント

HINET2001との並行運用
➡ 利用者の都合が良いタイミングで移行可能

コネクタIDとゾーンCの申請手順

広島大学



ホスト登録システム

広島大学

- Webによる移行申請受付、設定変更の自動化
  - 定常運用時での使用を想定
- 移行初期は人海戦術による手動申請受付
  - 部局で連続したグローバルIPアドレスを取得したい（電子ジャーナル対策）
- 2008年12月より
  一部機能開放
  - 副管理者登録・変更
  - ホスト情報登録・変更
    削除（ゾーンC）
  - MACアドレス登録・
    変更（ゾーンA,B）
  - 年度更新（ゾーンA,B）

ホスト登録システムの画面例

移行進捗状況（2008年12月末現在）

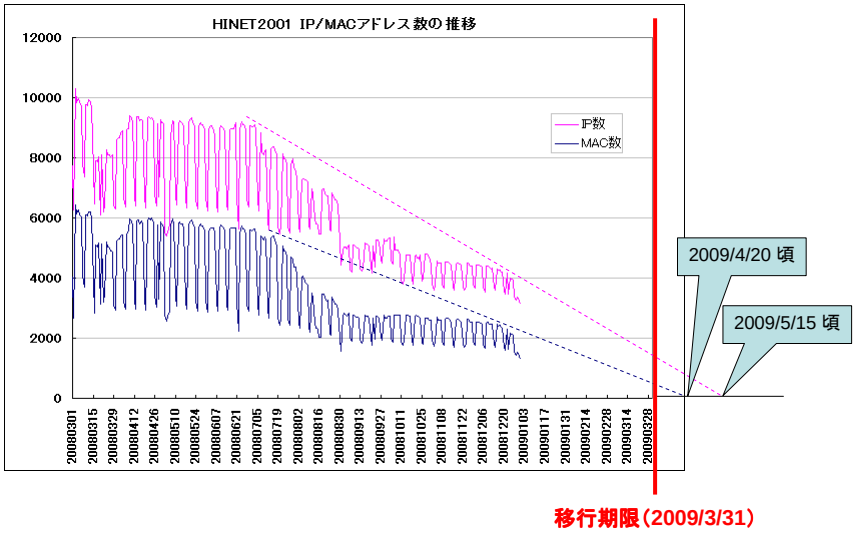
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
申請メール受付数	28	126	100	140	173	183	110	100	126				1086
コネクタID登録数	-	520	95	1215	608	493	230	178	530				3869
コネクタID削除数	-	28	2	1	6	20	14	0	0				71
MACアドレス登録数	-	290	215	1044	745	934	354	173	83				3838
MACアドレス削除数	-	8	11	16	9	32	34	10	2				122
ゾーンC割り当て数	76	322	56	36	154	61	42	33	52				832

コネクタID　最大14,000ポート ⇒ 3,798ポート割当

ゾーンC　最大2,000ゾーン ⇒ 832ゾーン割当

HINET2001 IP/MACアドレス数の推移

広島大学



2009/4/20 頃

2009/5/15 頃

移行期限(2009/3/31)

まとめ

広島大学

- HINET2007の概要
  - 特徴
    - 全学的な一元管理体制
    - VLANによる柔軟な仮想配線の提供
    - 個別ファイアウォール機能の提供
    - すべての接続場所において利用者認証を要求
  - 管理・運用・移行の方針
  - 設計・構築のポイント
    - 個別ファイアウォール機能の実現
      - スループット測定
    - 利用者認証機能の実現
      - DHCPサーバのIPアドレス払い出し性能
      - Radiusサーバの同時認証性能
      - 認証スイッチの同時認証性能
  - 移行の支援体制とシステム
  - 移行状況

広島大学

使用した機器の名称または仕様

装置	機器の名称または仕様
フロアスイッチ	Alaxala AX2430S
建物集約スイッチ	
サーバ集約スイッチ	
Radiusサーバ	CPU: Xeon X5355 2.66GHz x 2, Memory: 4GB FreeRADIUS 1.1.7, OpenLDAP 2.3.41
DHCPサーバ	CPU: Xeon X5355 2.66GHz x 2, Memory: 4GB ISC-DHCP 3.05
L3コアスイッチ（2007）	Cisco Catalyst 6509 w/ FWSM x 3, IDSM x 2
対外接続ルータ（2007）	Alaxala AX6304S
L3スイッチ（サーバ接続）	Cisco Catalyst 6506
L3スイッチ（2001）	Cisco Catalyst 6509
全学ファイアウォール（2001）	Alteon Switched Firewall Director/Accelerator Checkpoint Firewall-1
対外接続ルータ（2001）	Hitachi GR2000-BH
サーバA, B	CPU: Pentium4 3.06GHz, Memory: 512MB
クライアント1～5	CPU: Pentium4 2.8GHz, Memory: 512MB

広島大学

ご清聴ありがとうございました