2009年11月27日

広島大学における セキュリティ対策事例

～セキュリティ対策とキャンパスネットワーク更新～

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

広島大学 情報メディア教育研究センター
情報基盤研究部門

広島大学

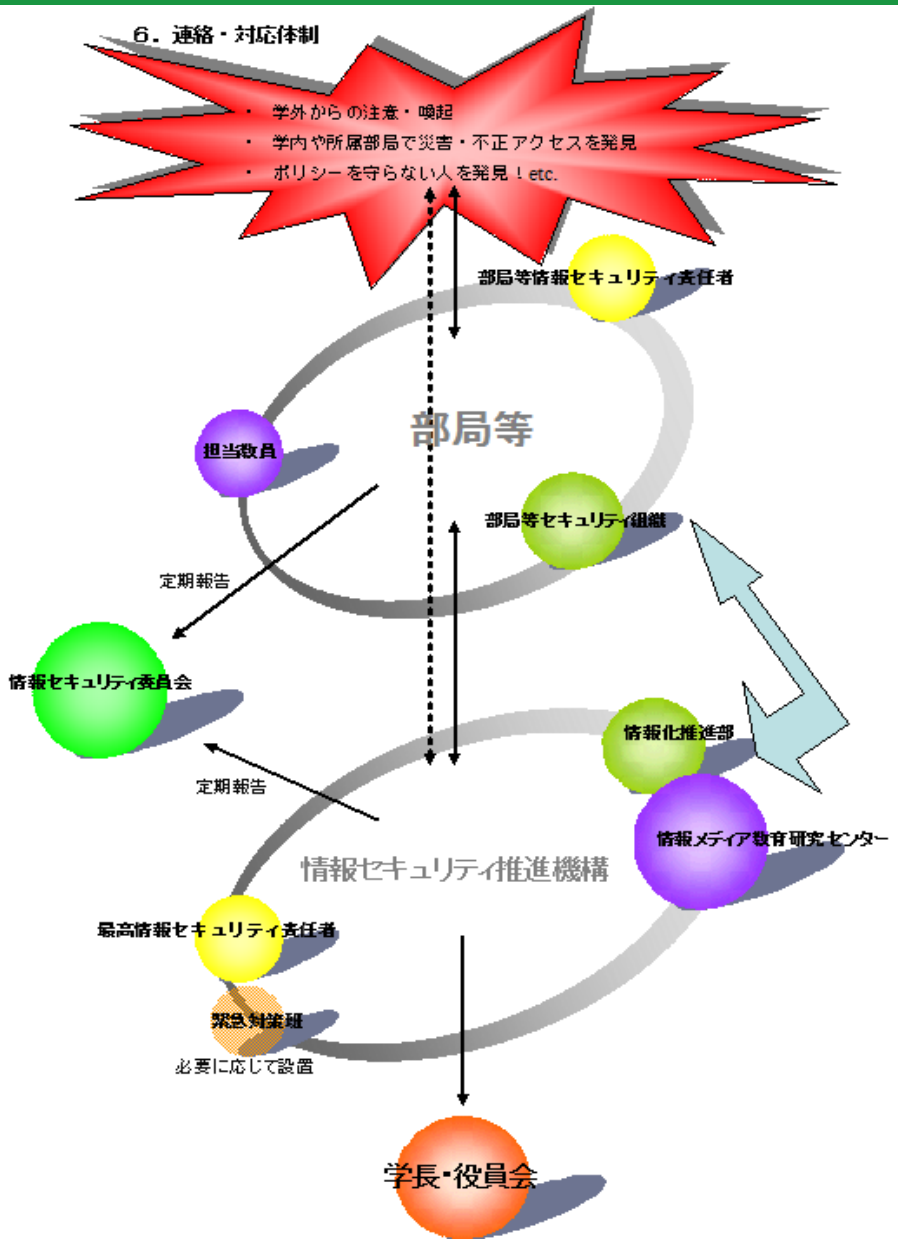
内容

- セキュリティ対応の組織・体制
- 学内インシデントへの対応
- キャンパスネットワークでの対応

↓

- 新ネットワーク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
  - 既存ネットワークよりの移行、支援体制とシステム
- 新ネットワークの導入後
  - シングルサインオン（SSO)対応

学内インシデント対応　組織体制



セキュリティ　教育・講習

情報セキュリティ　～管理者入門コース～

- 外部の講師による年2回程度実施
  - 主要キャンパス1回、他1回
- 対象は主に管理者で、新規採用教員・職員など、毎回30～40名程度
- テキスト
  - IPA作「情報セキュリティ読本」情報セキュリティ教育のための教科書
  - 比較的簡易な表現、コンピュータのユーザとして知っておいてほしい内

他に、オンラインでのセキュリティ講座
WEB-CTで開講

セキュリティポリシー

- テンプレートをベースに、学部・部局毎に作成
- 必要時に随時更新、今年度はUSBメモリ等携帯型の扱いなど
- 年1回の自己点検と結果の報告（の義務）
- 項目例
  - 実施手順の周知状況
  - ウィルス対策のインストール状況
  - OS、アプリケーション等の更新状況
  - 情報システムの管理、パスワード管理　など

セキュリティインシデントに対する メディアセンター行動指針（策定中）

広島大学

- 概略
  - 不正利用の発見（学内外からの指摘、システムログ、入退室記録や監視カメラなどについて）
  - 緊急を要する場合の措置（緊急を要すると判断された場合は、センタースタッフ（複数）の判断による必要な措置について）
  - アカウントの停止、ネットワーク通信遮断（別途の等利用規則※1に基づく停止など）

※1 広島大学情報システム等利用規則
広島大学情報メディア教育研究センター利用内規

インシデント例

- アカウントが不正利用される
- 原因は安易なパスワード
- 該当アカウントで学外のネットワーク攻撃
- 被害の概要
  - bash（ログインシェル）のヒストリ（コマンド履歴）に一部残る。
  - CPUアーキテクチャとOSが特殊→攻撃ツールコンパイル失敗→各種のツール実行は失敗。
  - その後で、スクリプト　perl の簡単な攻撃スクリプトで次のサイト検索に使われた模様

インシデント対応

- 概要
  - 年間件数20～30
  - 外部組織からのクレーム
    - ウィルス、踏み台、不適切な情報発信
  - センター独自で発見
    - Windowsワーム対策
- 不正アクセスの提供情報は、
  - 送信元IPアドレス（学内のIP）、時刻
  - インシデントの内容

↓

迅速な対応には、上記内容より利用者、該当端末の特定

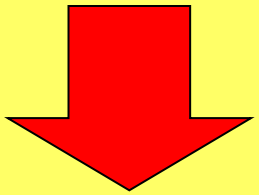
新キャンパスネットワーク完成まで

広島大学

- HINET2007構築推進会議
  - 基本方針では認証が必須
  - サブネットでの管理の廃止
  - ホスト単位での管理を可能とする
- 完全導入まで約2年半
  - 建物内フロア配線調査、追加配線工事検討
  - ネットワークエッジスイッチ設置希望調査
  - 管理者向け説明会
  - 一般利用者向け広報活動
  - あわせて、調達仕様策定～導入～移行

大学等のネットワークに対する要求

- 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



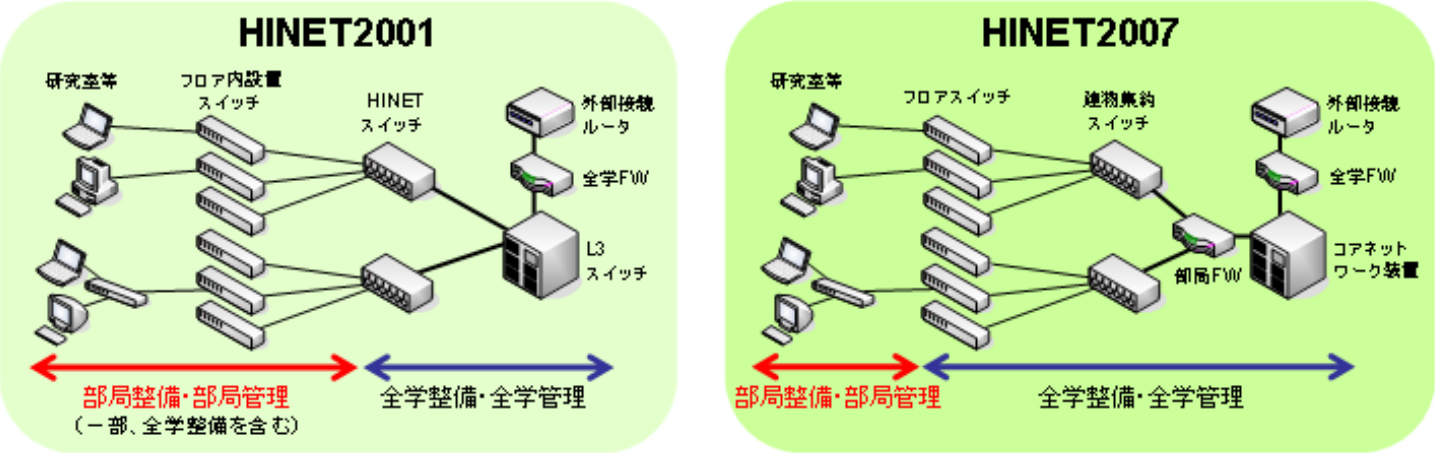
ネットワークのライフライン化
セキュリティインシデントの多発

- 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

ネットワーク管理体制の変更

広島大学

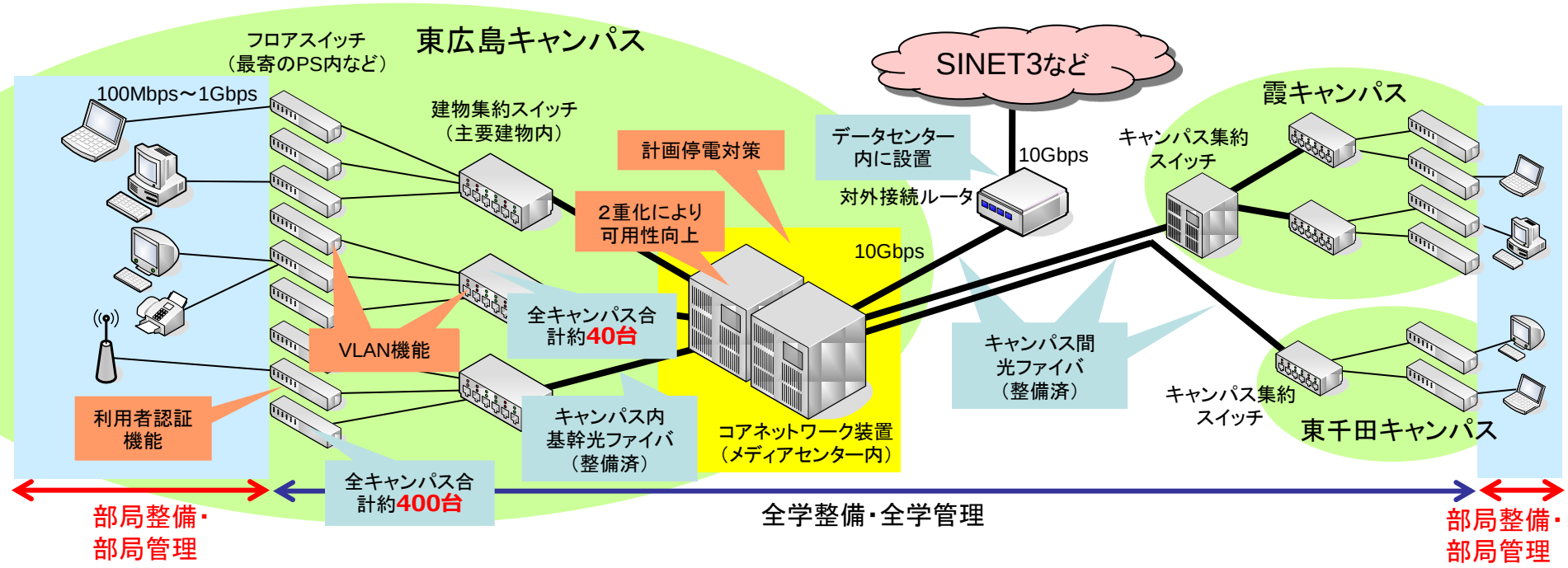
整備・管理区分と管理体制（HINET2001との比較）



	HINET2001	HINET2007
管理単位	**サブネット**	**ローカルゾーンまたはホスト**（原則）
管理者	部局等情報セキュリティ責任者	ローカルゾーン管理者、ホスト管理者
IPアドレス管理	部局等情報セキュリティ責任者	IMC（DHCPまたはIPアドレス固定）
フロア間配線	部局等	IMC（基幹部分からフロアスイッチまで）
フロア内配線	部局等	部局等
ネットワーク障害問合せ先	サブネット管理者 または IMC	IMC
IMC等からの連絡先	部局等情報セキュリティ責任者（原則）および サブネット管理者	機器利用者（原則）および ローカルゾーン管理者、ホスト管理者

※サブネット単位で移行する場合は、サブネット管理者等による管理体制の構築（維持）が必要。
※セキュリティポリシーの水準維持のため、部局等情報セキュリティ責任者（部局セキュリティ組織等を含む）は今後とも必要。

キャンパス情報ネットワークでの対策



- 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

新ネットワークの特徴

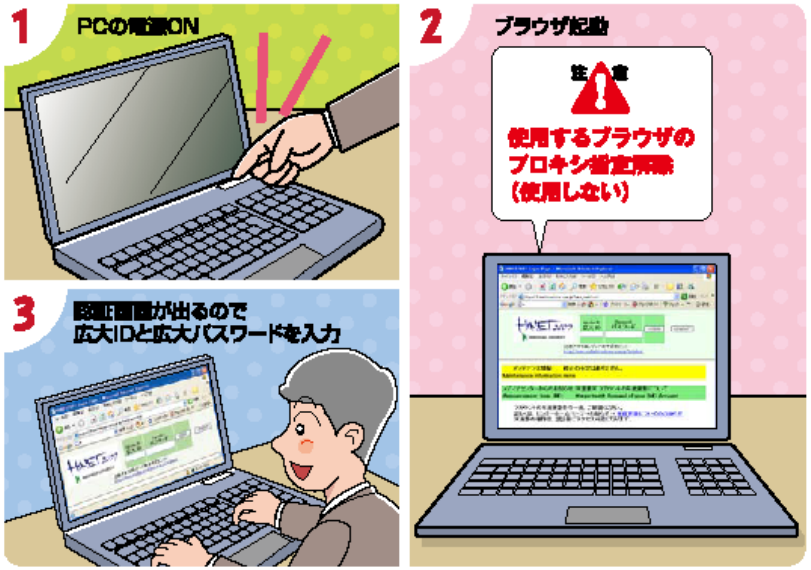
- 全学的な一元管理体制
  - ボランティアベースによるサブネット管理体制の破綻
  - 各フロアに設置するスイッチまで全学で一元管理
- VLANによる柔軟な仮想配線の提供
  - 同一研究室（グループ）が異なる建物等に分散する場合に対応
  - 学外向けサーバの設置、JGN2plusなどの利用に対応
- 個別ファイアウォール機能の提供
  - 全学ファイアウォール（対学外）のみでは不十分
  - ブロードバンドルータ相当の機能を教員数程度（約2,000個）提供
- すべての接続場所において利用者認証を要求
  - 多様な機器に対応するためWeb／MACアドレス認証を採用
  - 認証後は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

新ネットワーク利用案内（配布物）

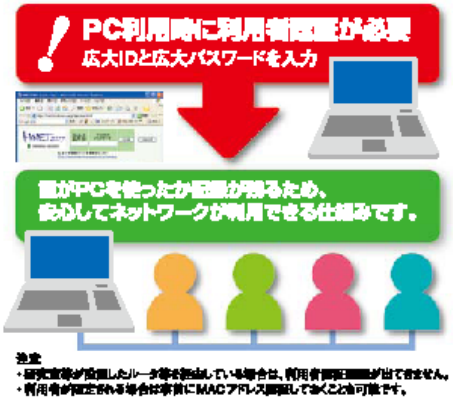
広島大学

HINET2007の使い方

PCの場合



※プロキシとは、WWW閲覧のために、HTTPによる接続を中継するサーバなどを使用すること

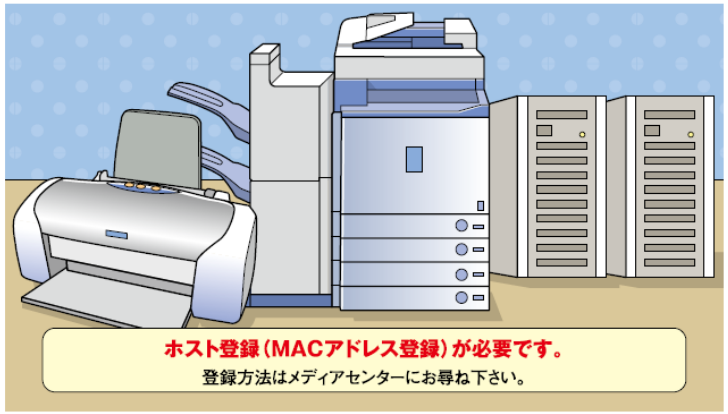


注意
・研究室等が設置したルータ等を接続している場合は、利用者認証画面が出てきません。
・利用者が特定される場合は事前にMACアドレス登録しておくことも可能です。

広島大学

管理者の方へ

プリンタやサーバの場合



※MACアドレスとは、ネットワーク上で、ネットワーク機器を識別するために設定されているLANカードなどのハードウェア固有の情報

注意 ブロードバンドルータ等の利用

●部局等で設置したルータ（ブロードバンドルータ、ファイアウォール等）を経由すると、利用者認証ができなくなります。
●利用者の把握（利用記録の保存等）は、ルータの管理者（設置者）が責任もって行って下さい。

ブロードバンドルータ等の利用にはホスト登録（MACアドレス登録）が必要です。
登録方法はメディアセンターにお尋ね下さい。

注意 無線LANの利用

●部局等で無線LAN装置（無線アクセスポイント、無線LAN機能付ブロードバンドルータ等）を設置する場合、暗号化機能（WEP、WPA等）を設定し、暗号鍵の管理を厳格に行って下さい。
●近隣の無線LANアクセスポイント等との干渉が発生しないよう、設置の際はご配慮をお願いします。（原則、該当の部屋の中のみで利用できるよう調整して下さい）
●ルータ機能の付いた無線LAN装置を使用すると、接続したPCで利用者認証ができなくなります。ルータ機能使用の有無を設定できる装置の場合、ルータ機能を停止すると利用者認証ができるようになります。（こちらを推奨します）

設定方法は、その装置を購入した販売店にお尋ね下さい。

問い合せ先：http://www.media.hiroshima-u.ac.jp/helpdesk/

「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

いわゆる平坦なサブネットでの構成とは異なる

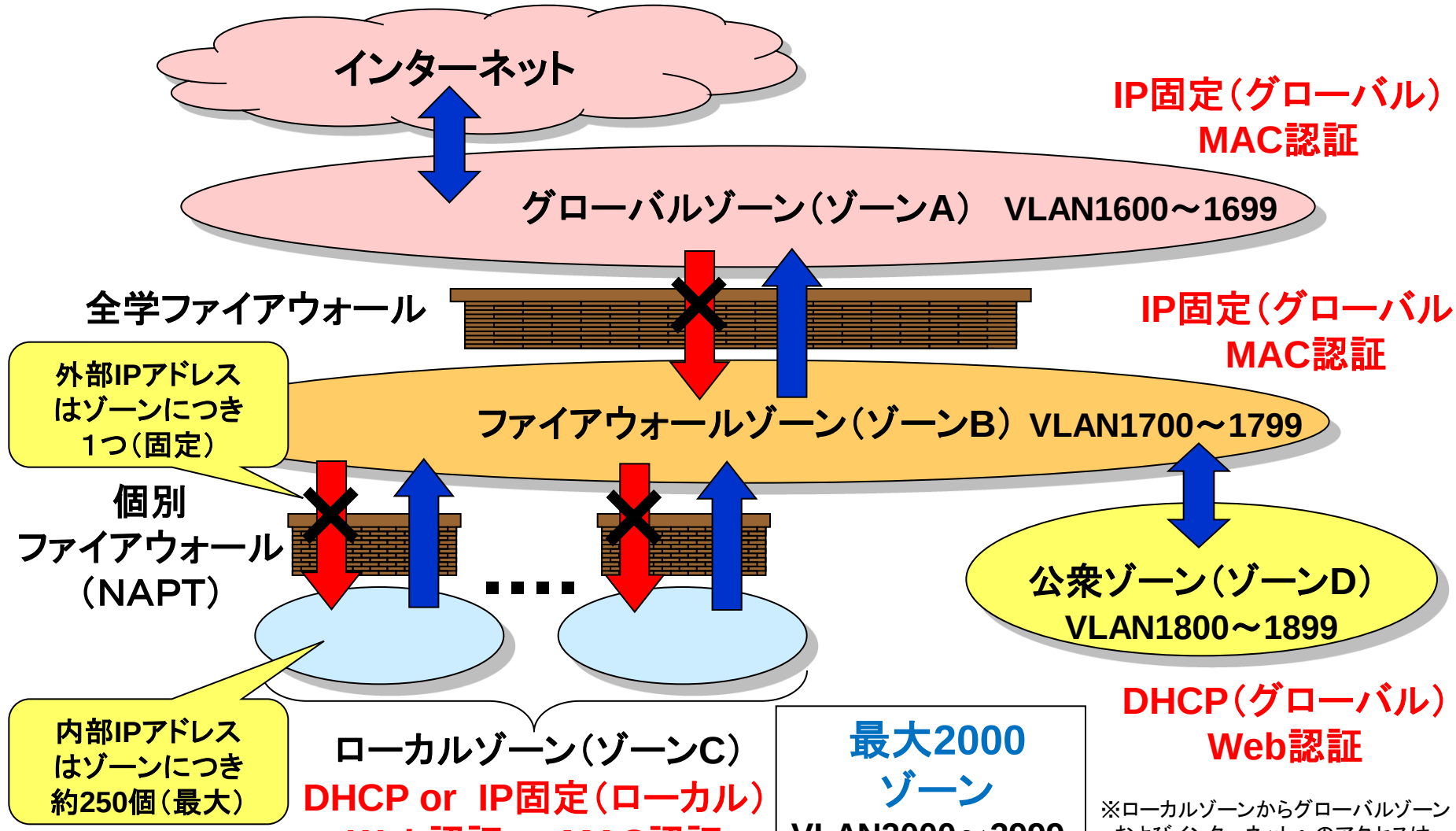
新旧のネットワーク間でのアクセス

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	○	×	×	×	○	○	×	ー

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

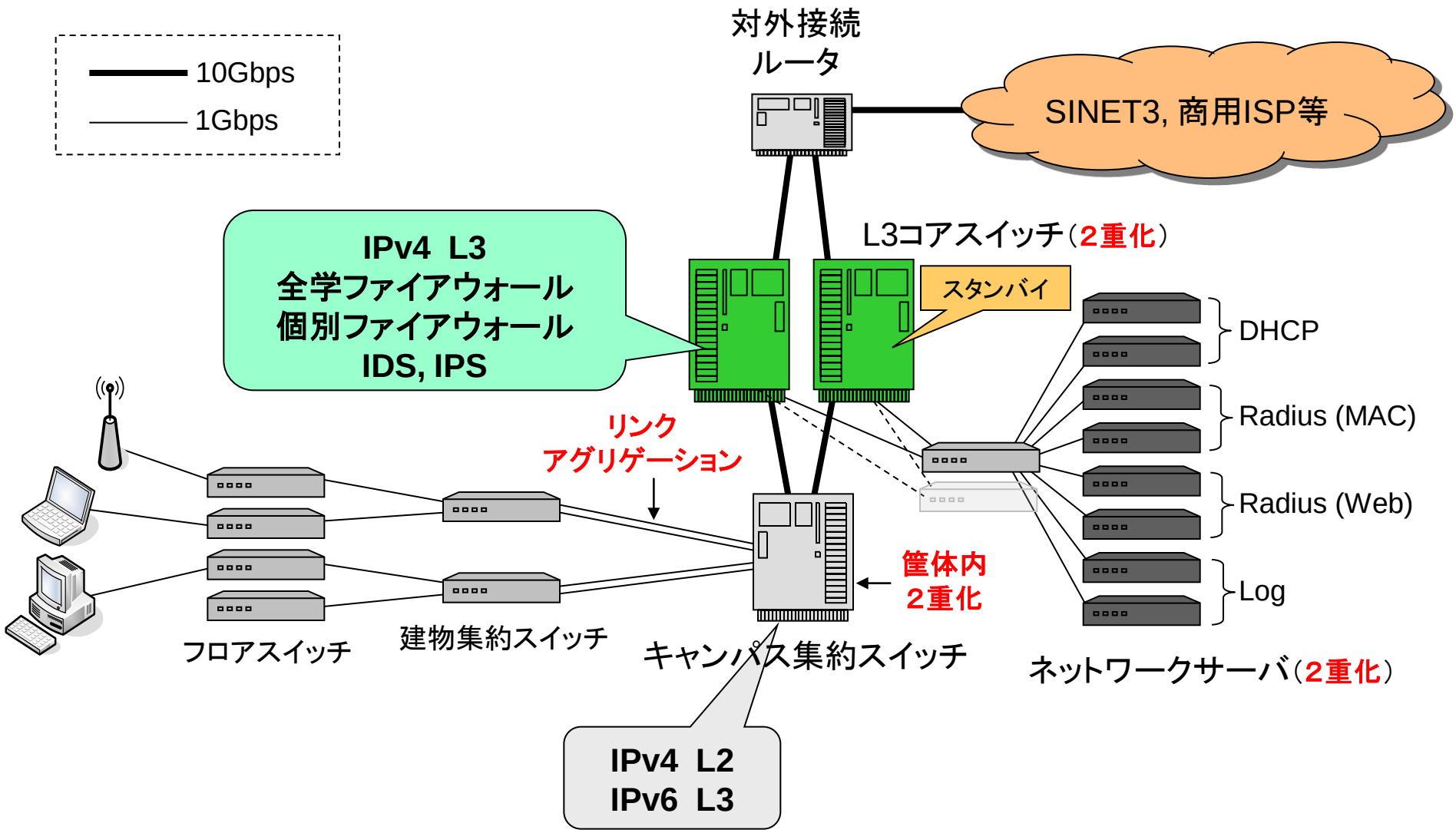
ゾーン種別とアクセス制限



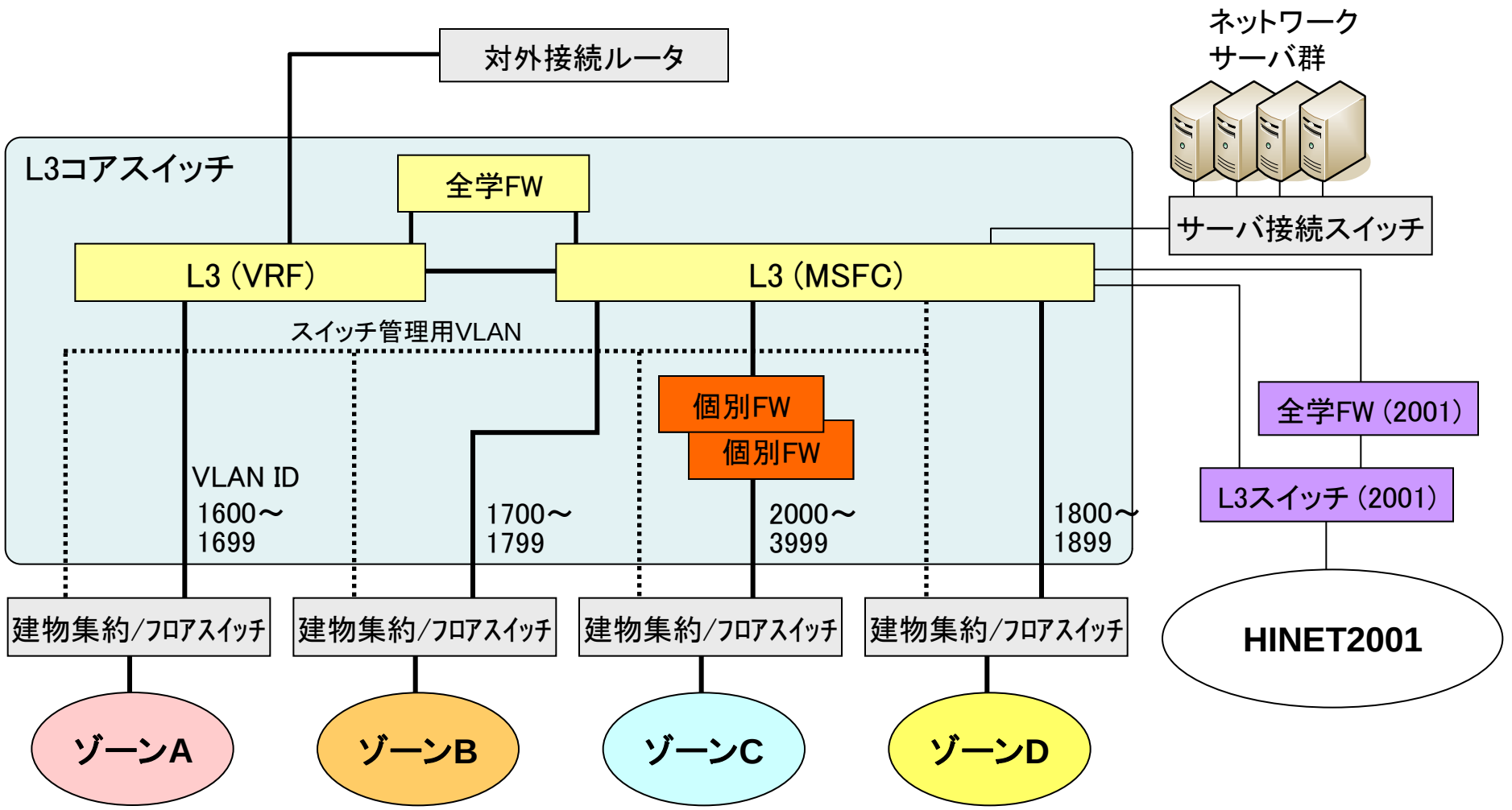
運用と移行の方針

- 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

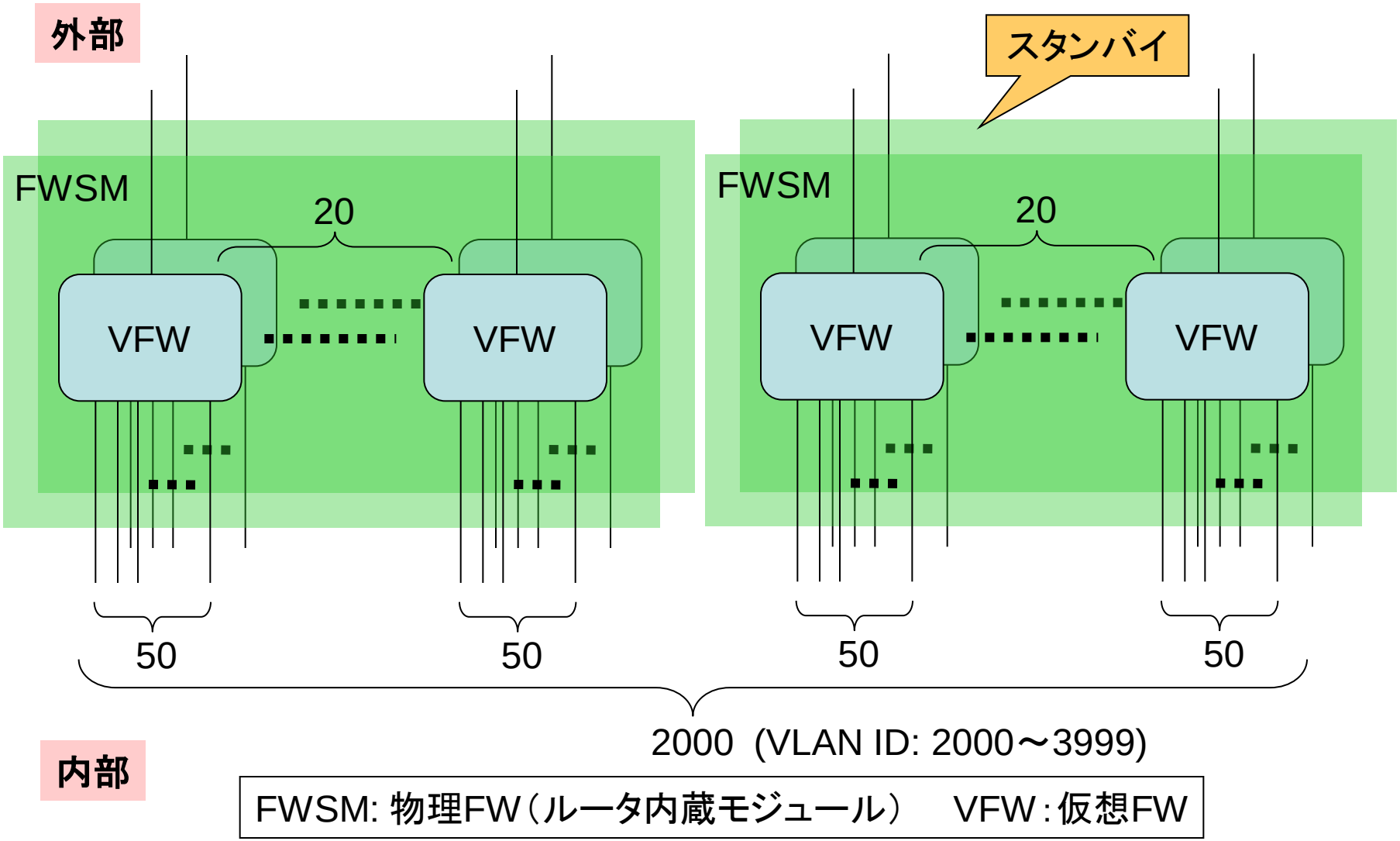
基幹ネットワークの物理構成



L3コアスイッチの設定

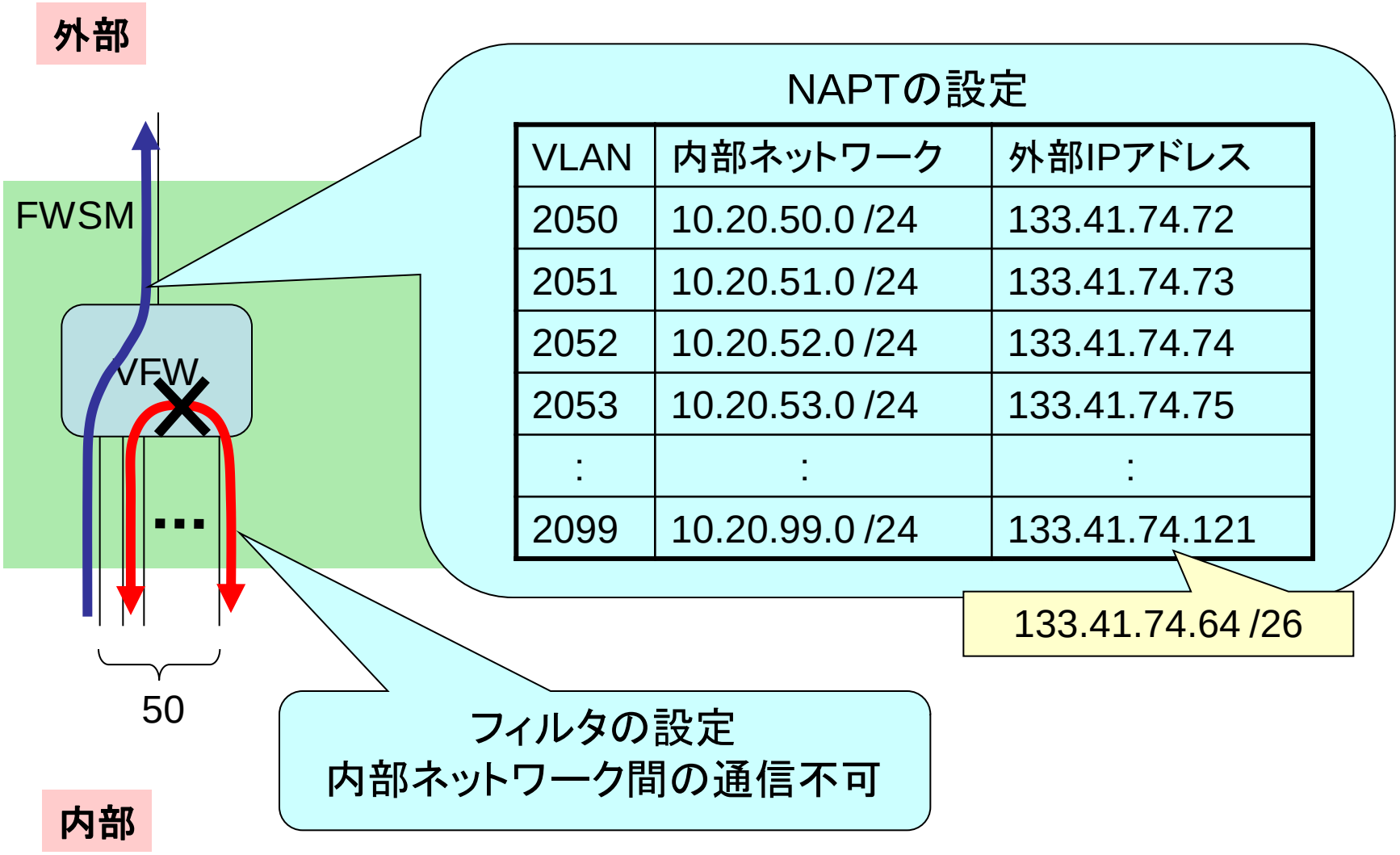


個別ファイアウォールの構成

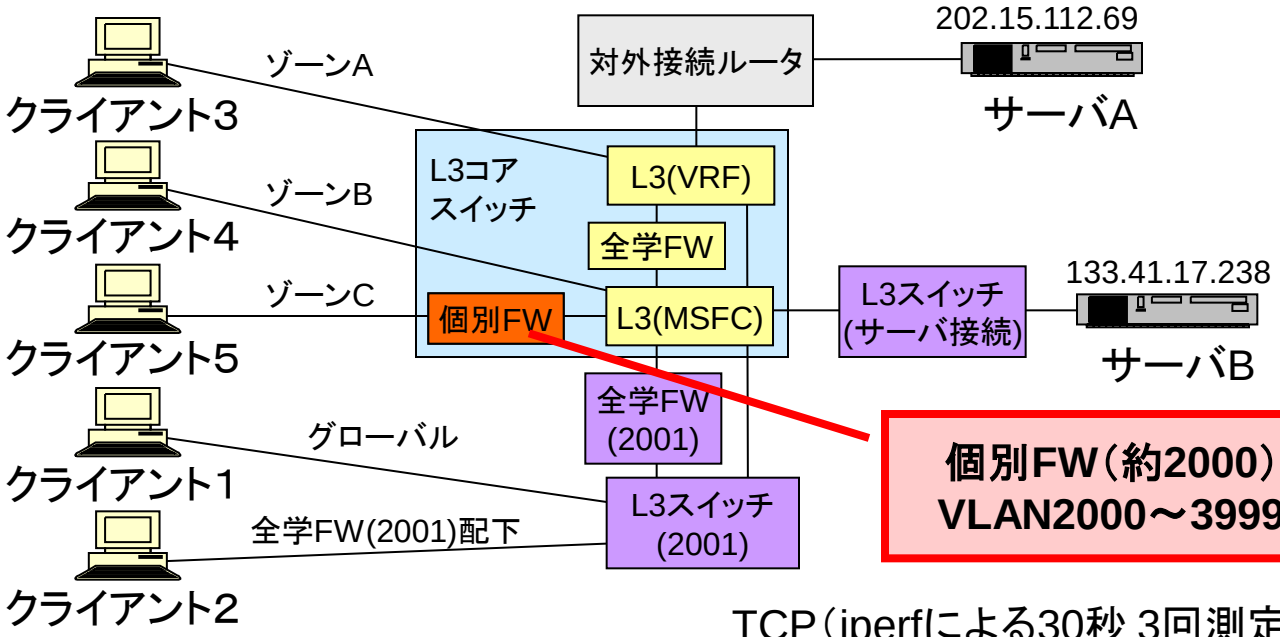


FWSM: 物理FW（ルータ内蔵モジュール）　VFW：仮想FW

仮想ファイアウォールの設定



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

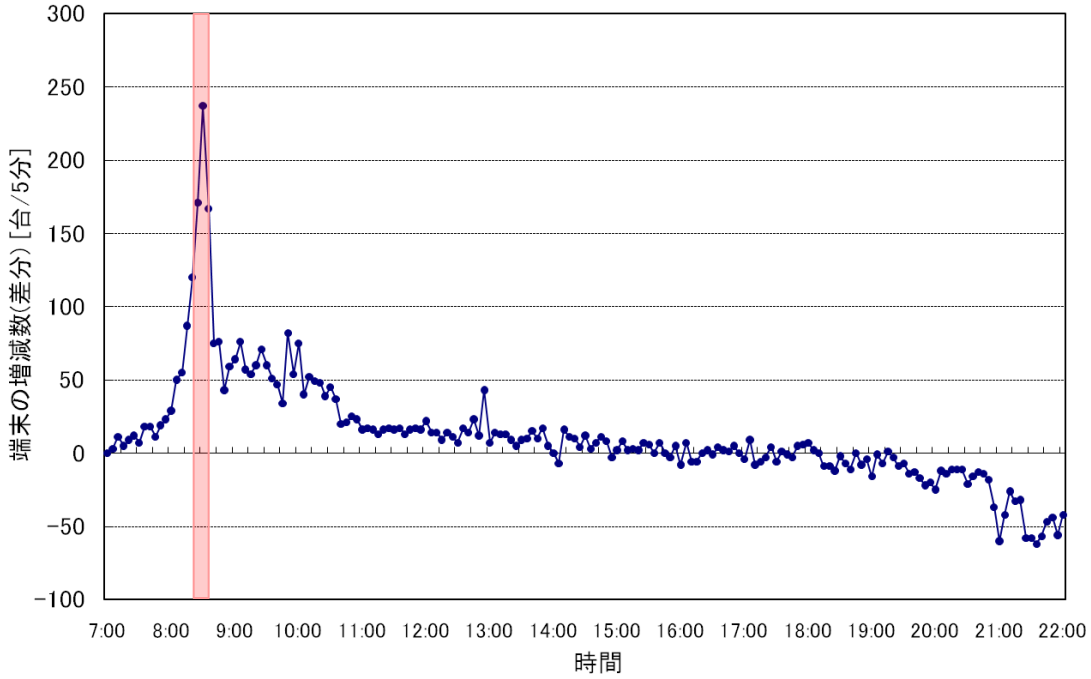
利用者認証機能に対する要件(1)

- ネットワークインフラとしての認証ネットワーク
  - 認証ページ（SSL)で、UPKIオープンドメイン証明書利用
  - 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

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)

- 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

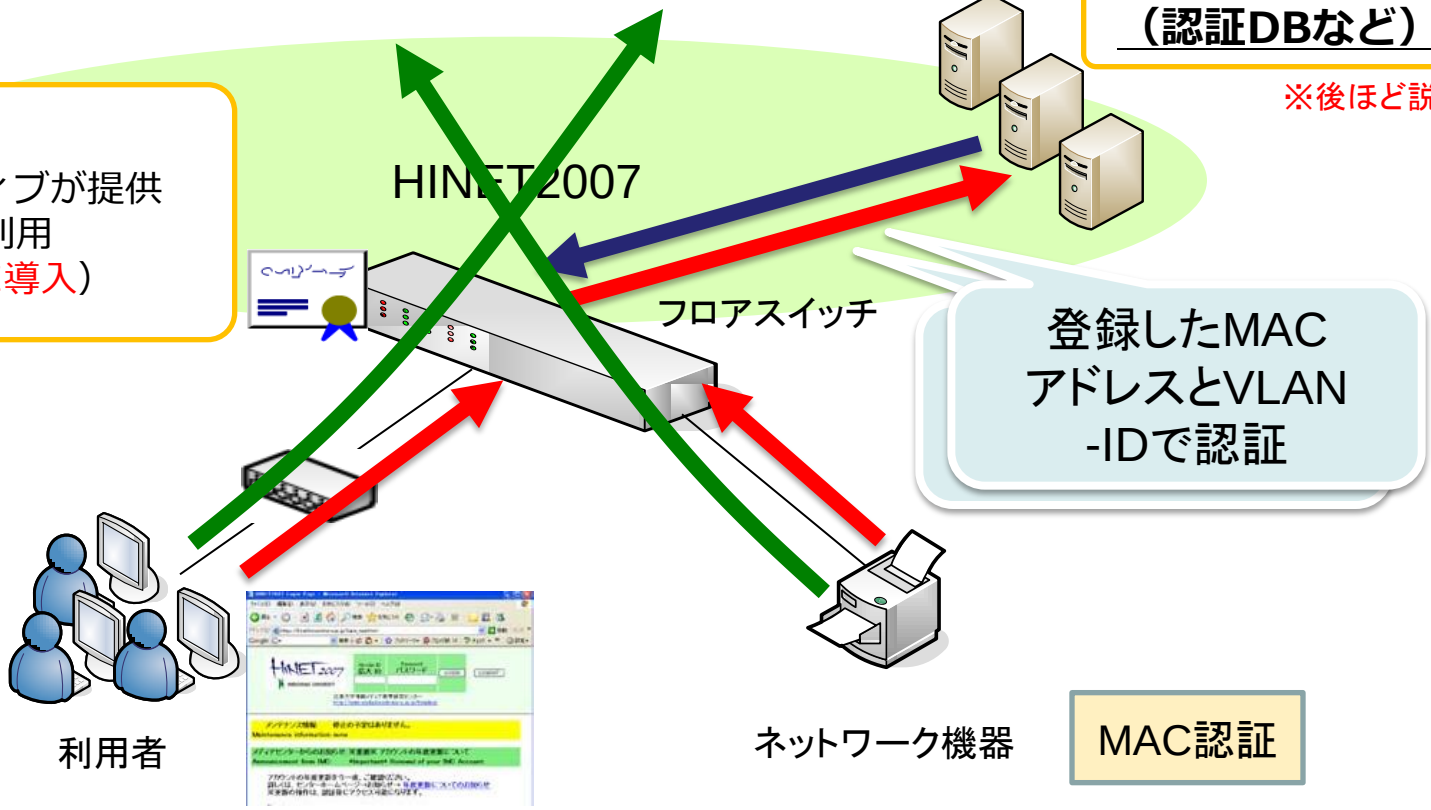


8時20分から35分（15分間）で約600台が稼働

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



中間CA証明書
NII UPKIイニシアティブが提供する中間CA証明書を利用
（全フロアスイッチに導入）

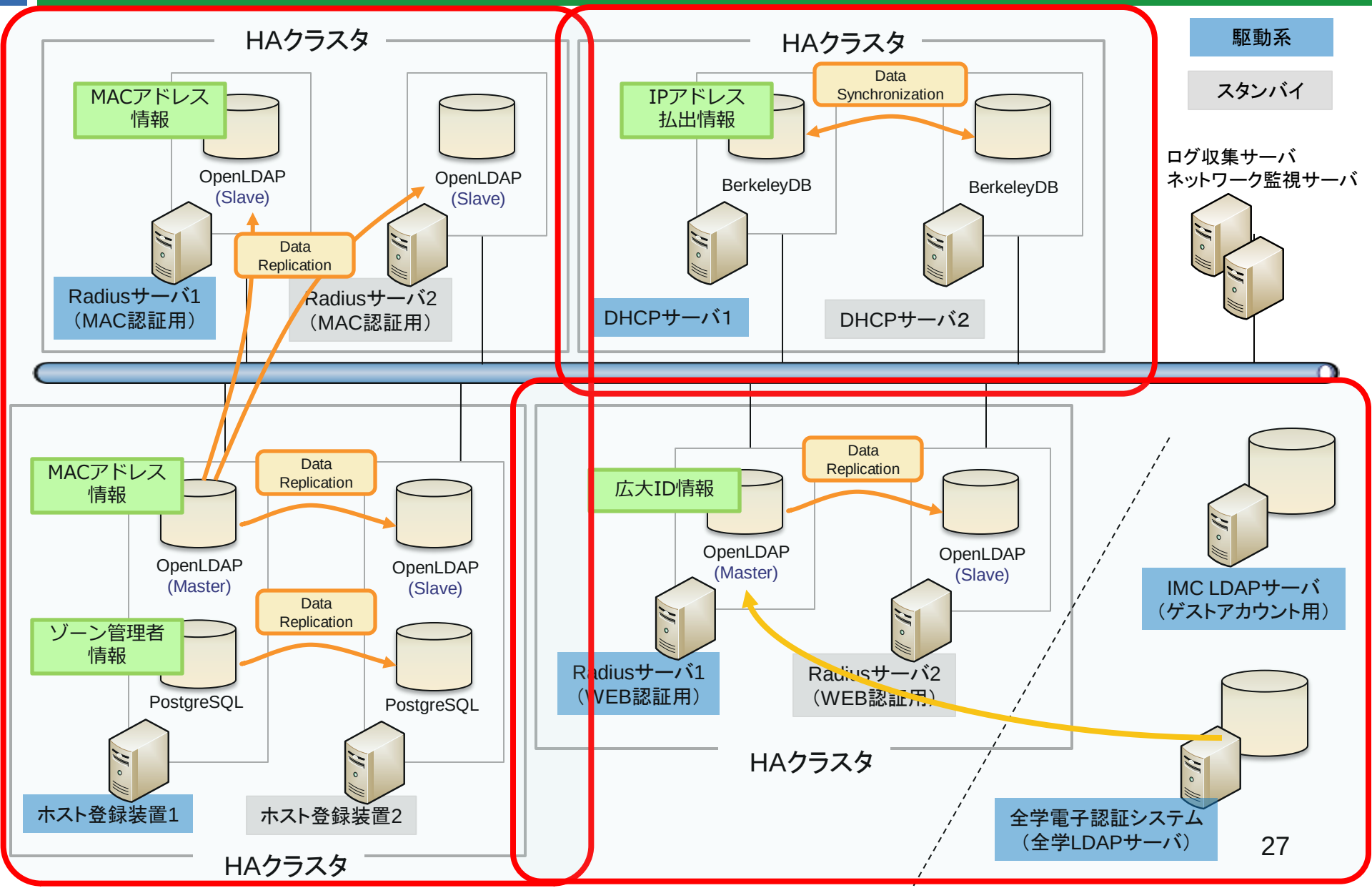
Web認証

MAC認証

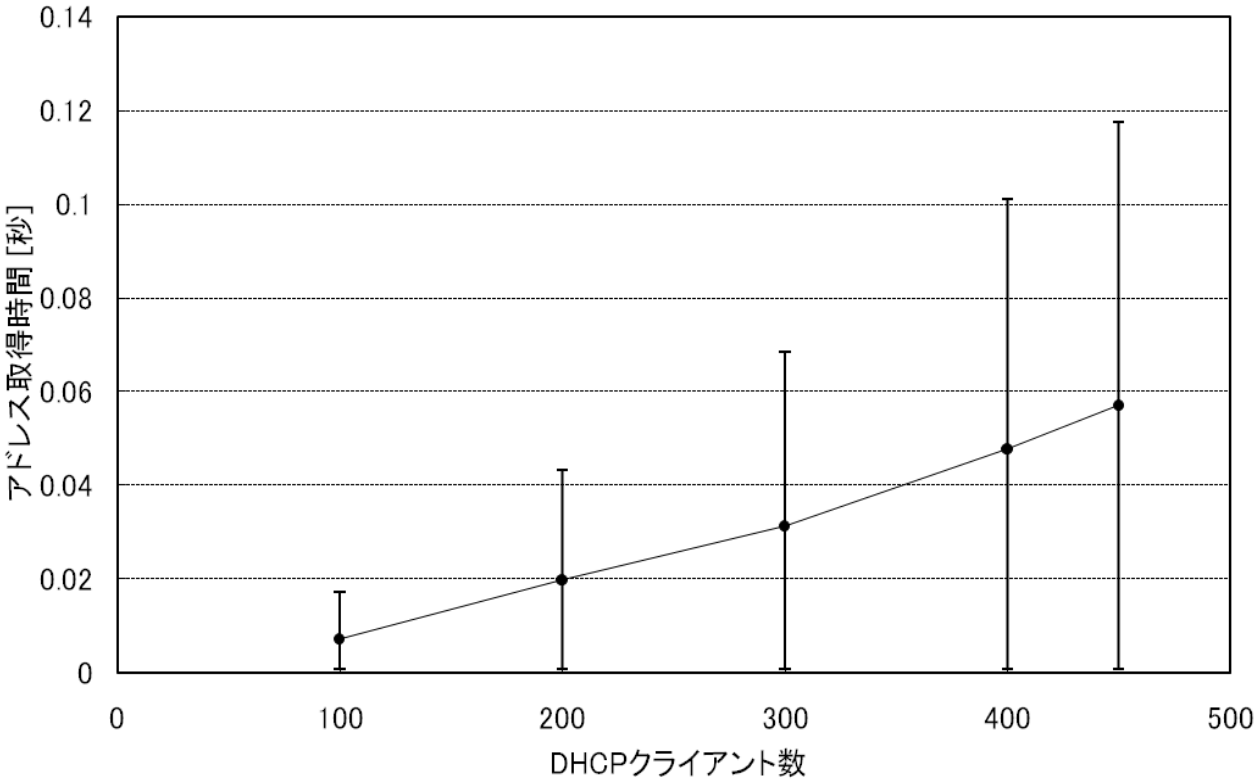
https による利用者認証
初回接続時に認証ページをリダイレクト表示
全学電子情報基盤で管理するIDを利用
ARPポーリング/リンクダウンによるログアウト

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

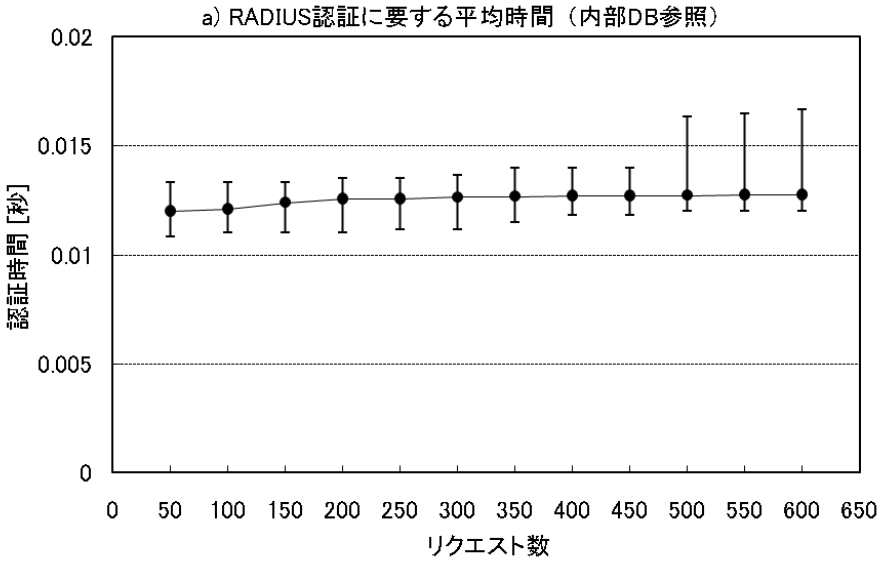


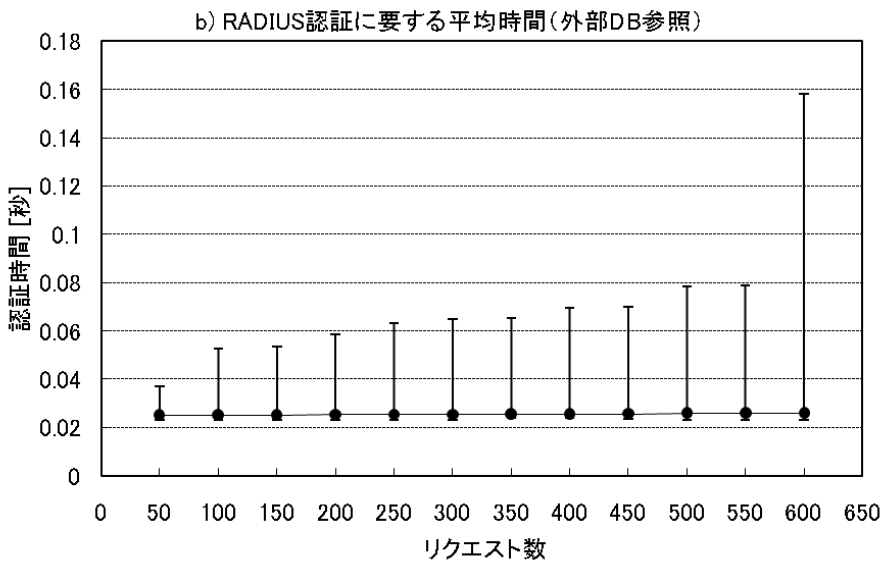
DHCPサーバのIPアドレス払い出し性能



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





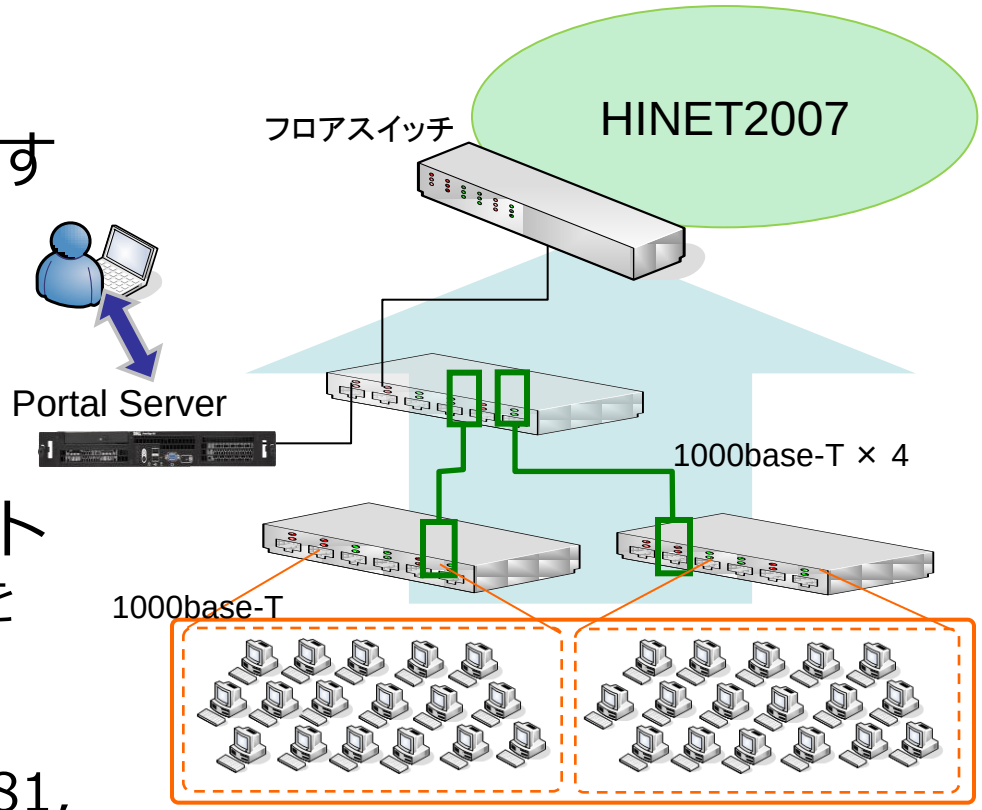
内部DB参照（通常のWeb, MAC認証）

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

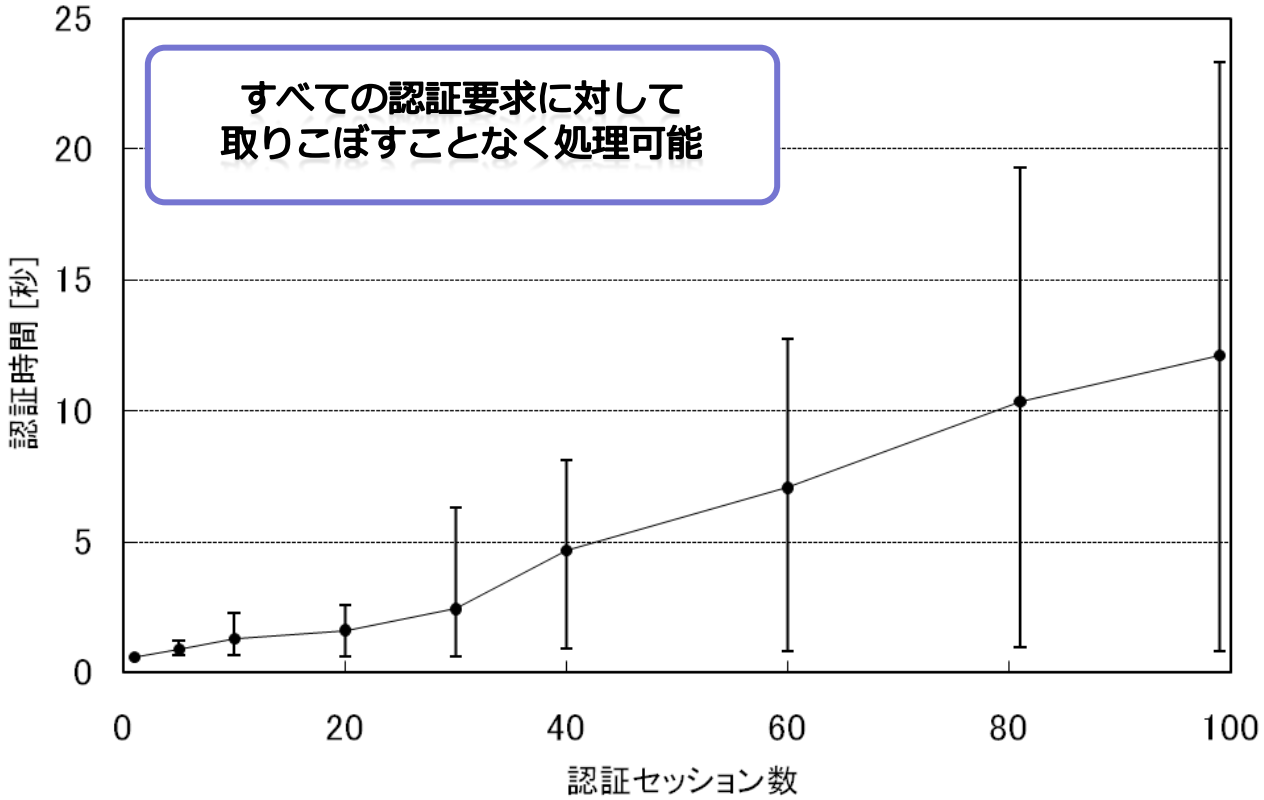
- 実験概要
  - フロアスイッチを経由する同時Web認証性能
  - リダイレクトと認証処理時間の和を計算
  - 100個の個別リクエスト
    - IMCゲストアカウントを利用
  - 同時接続セッション数
    - 1, 5, 10, 20, 30, 40, 81, 99
  - 認証リクエストは1秒以内で同期



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

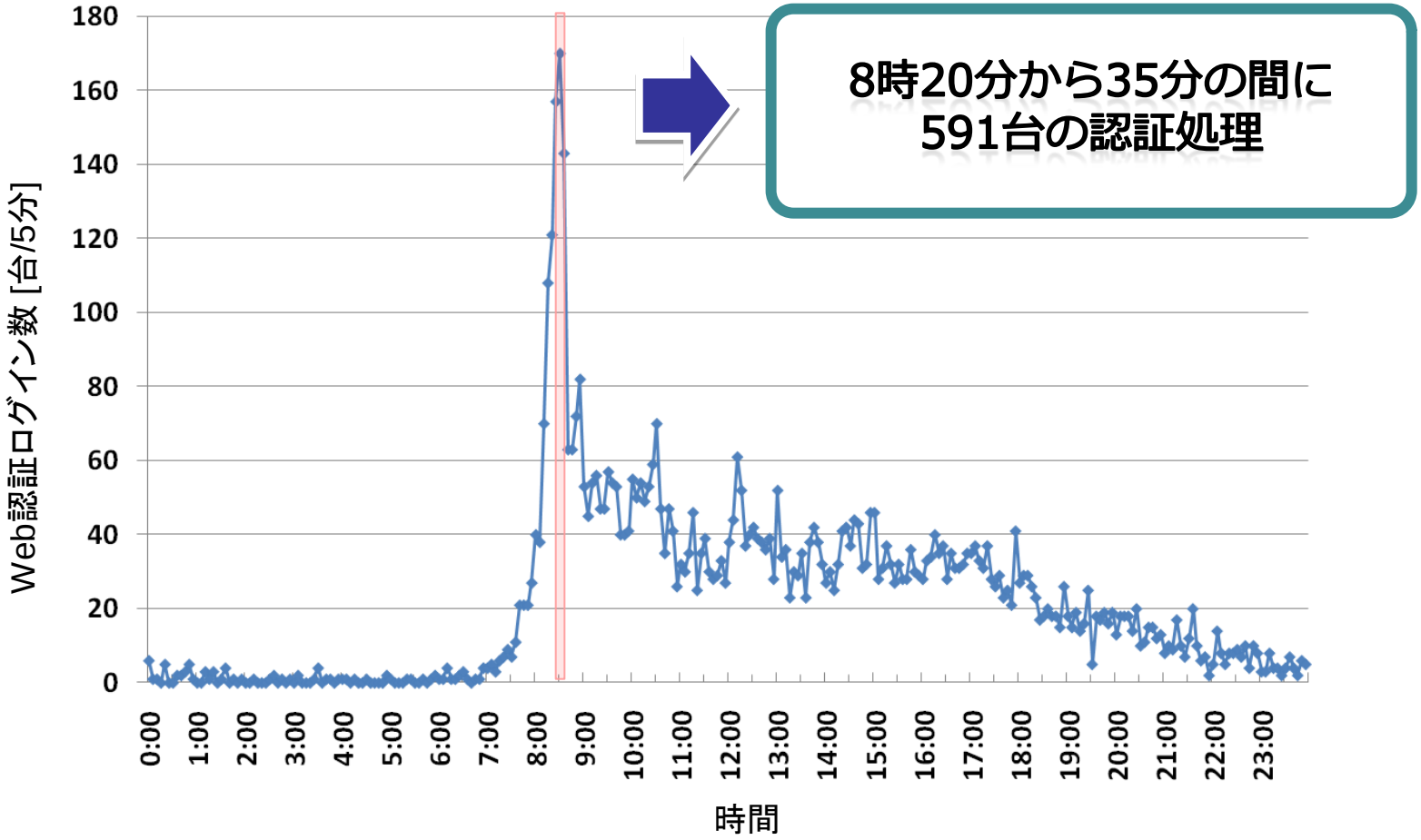


https接続
証明書鍵長 2,048bit

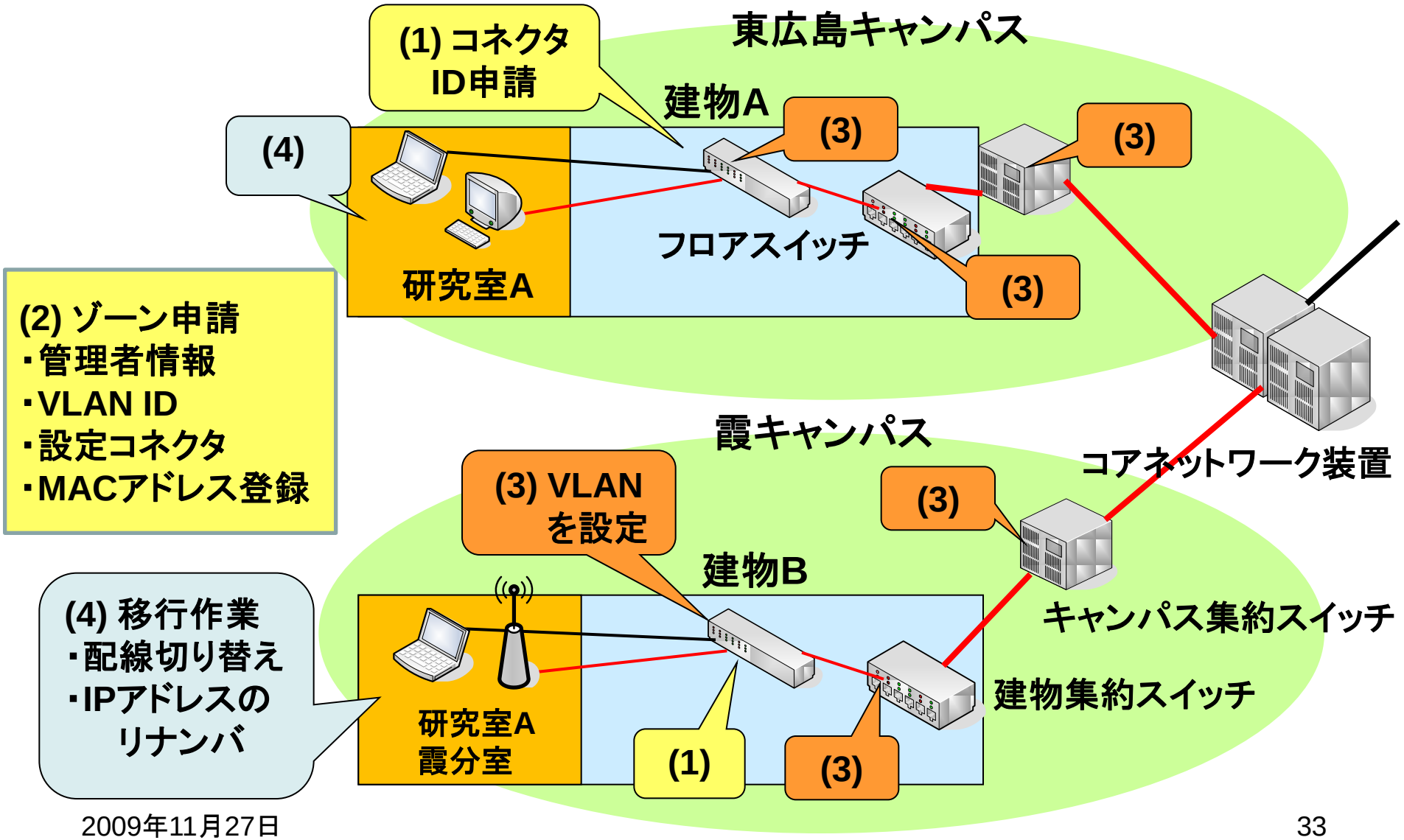
数セッションの同時認証では1秒
100セッションの同時認証でも最大23秒 で処理可能

現在の利用状況

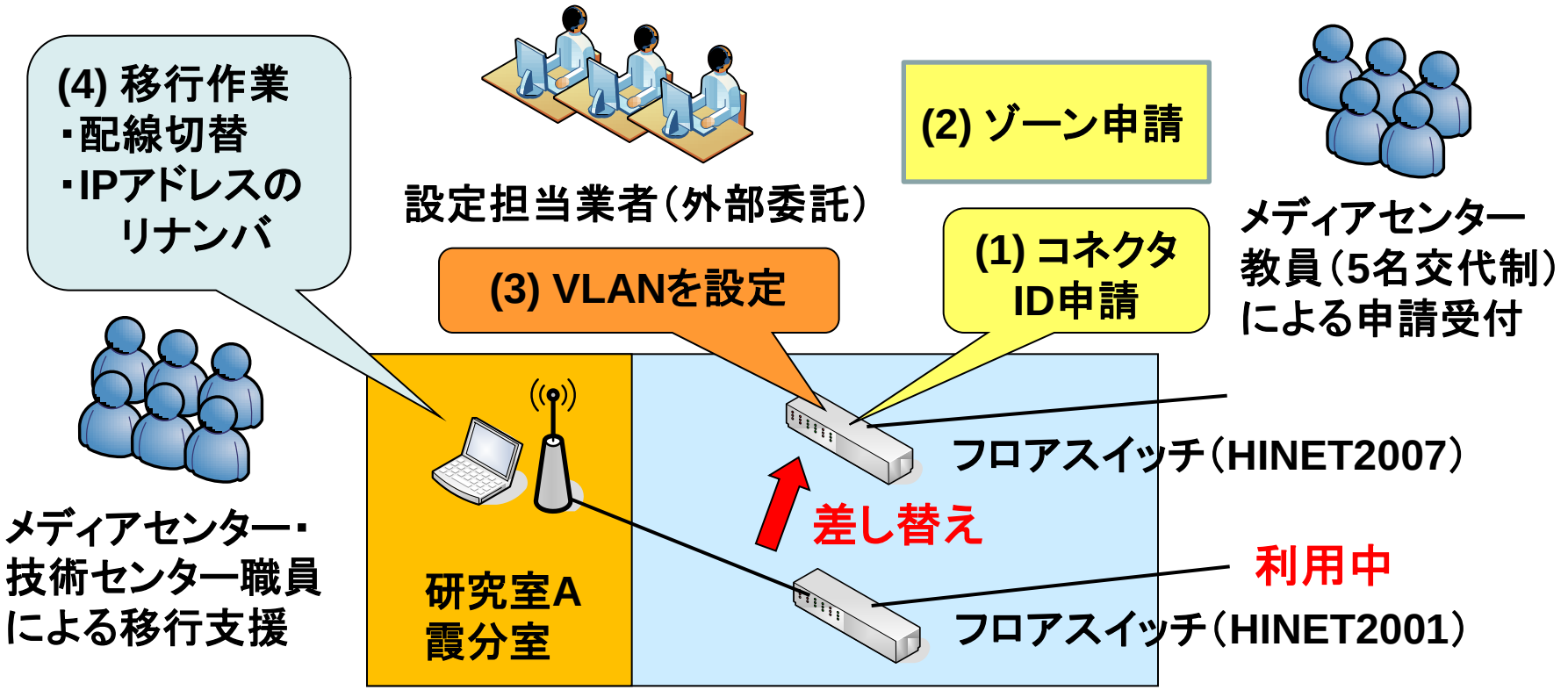
- Web認証の推移（5分間隔のログイン処理数）



ネットワーク移行の概要（移行手順）



ネットワーク移行の概要（支援体制）

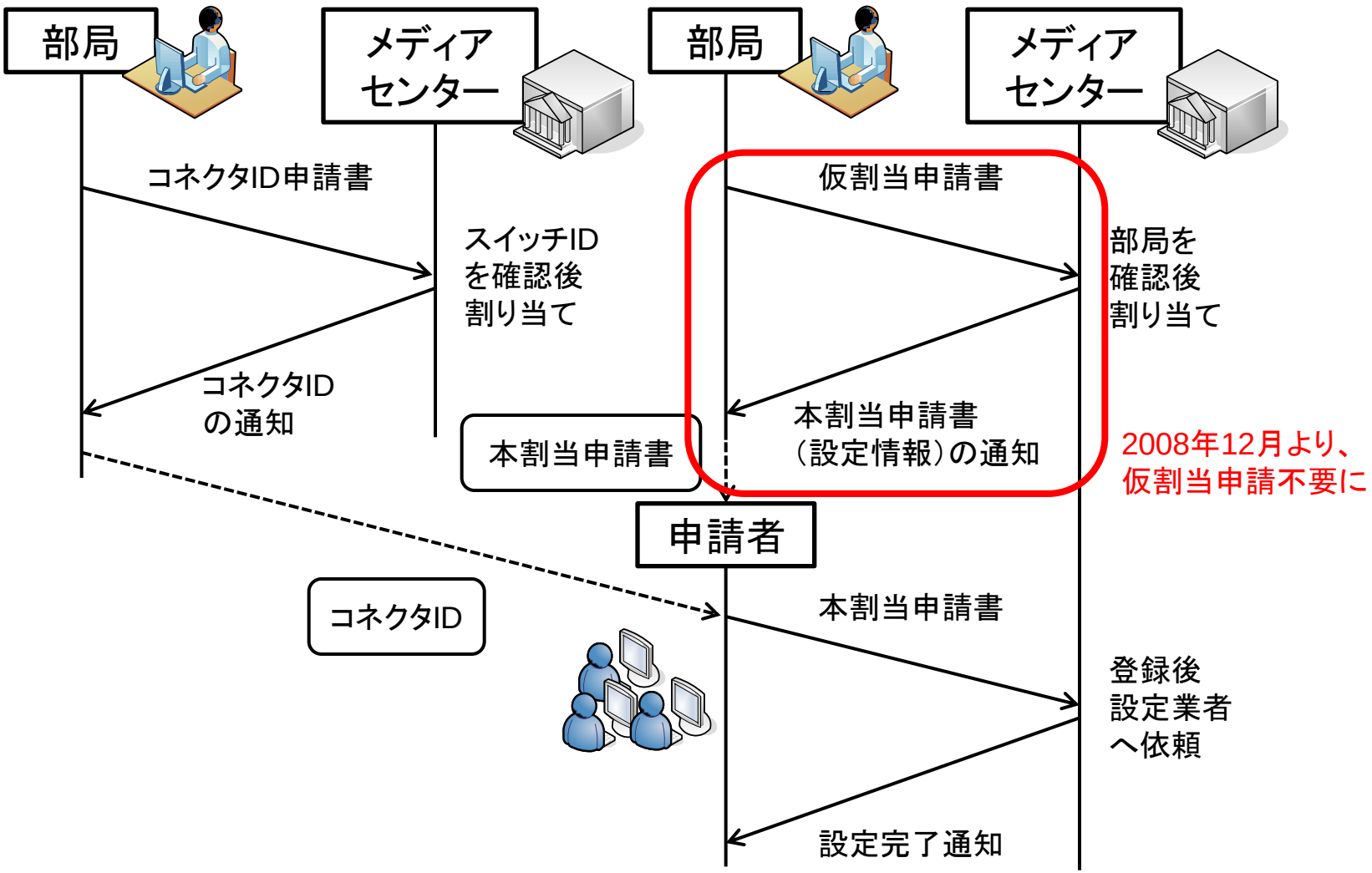


ポイント

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

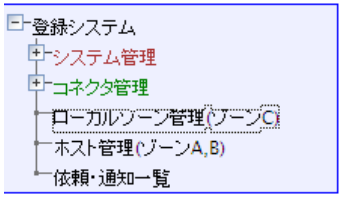
コネクタIDとゾーンCの申請手順

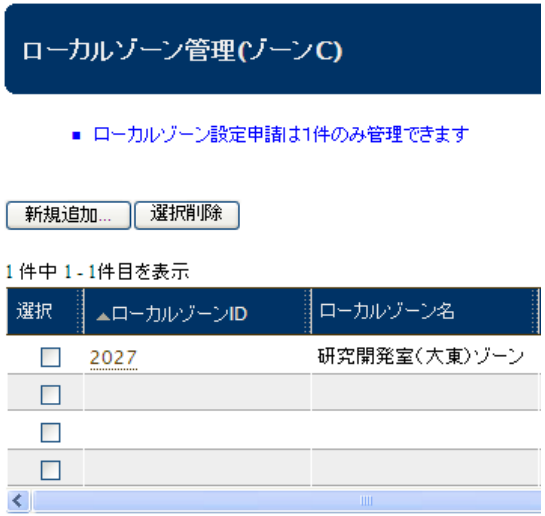


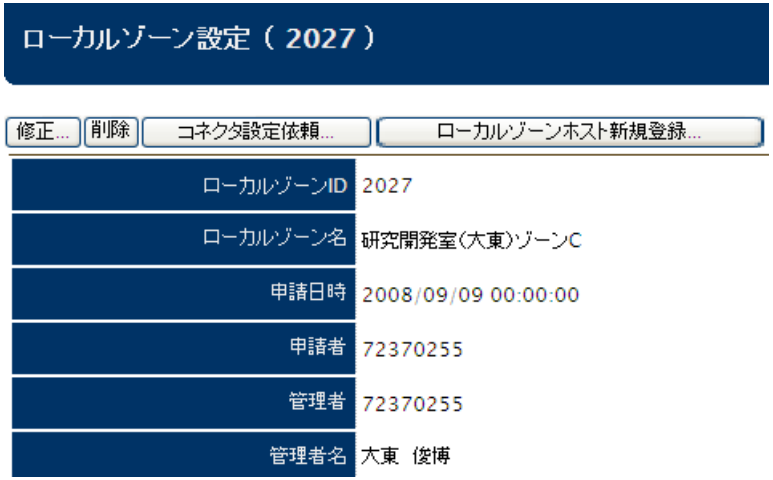
ホスト登録システム

- 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(2009年11月現在)

広島大学

- 利用状況

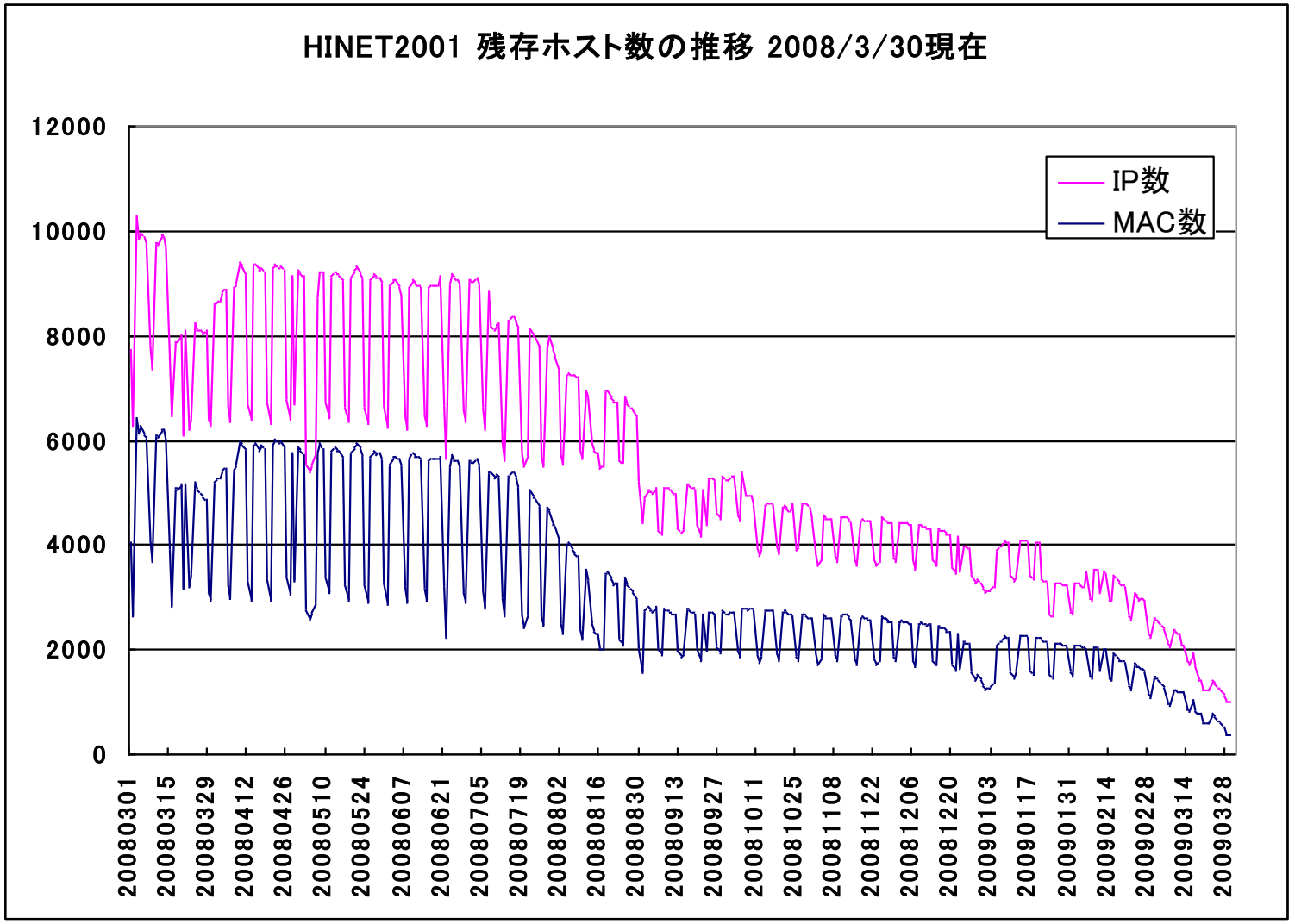
ゾーンA　　297 台

ゾーンB　　338 台

コネクタID　最大14,000ポート　⇒　約6000ポート割当

ゾーンC　　最大2,000ゾーン　⇒　1043ゾーン割当

ネットワーク移行、IP/MACアドレス数の推移



Single Sign-On(SSO)対応

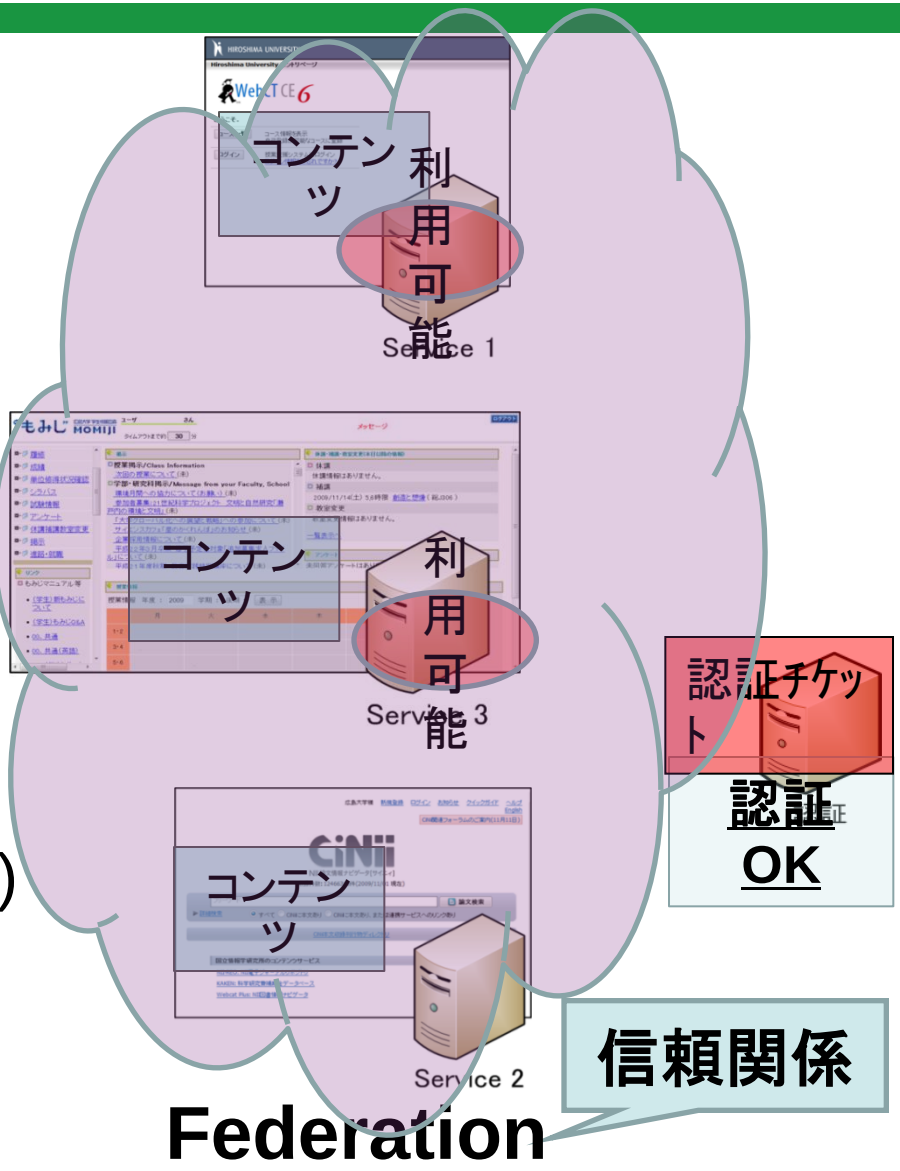
認証(SSO)

↓

認証状態(認証チケット)の保持

↓

認証状態を利用(認証チケットの提示)



利便性⇔セキュリティの解決

実装システム

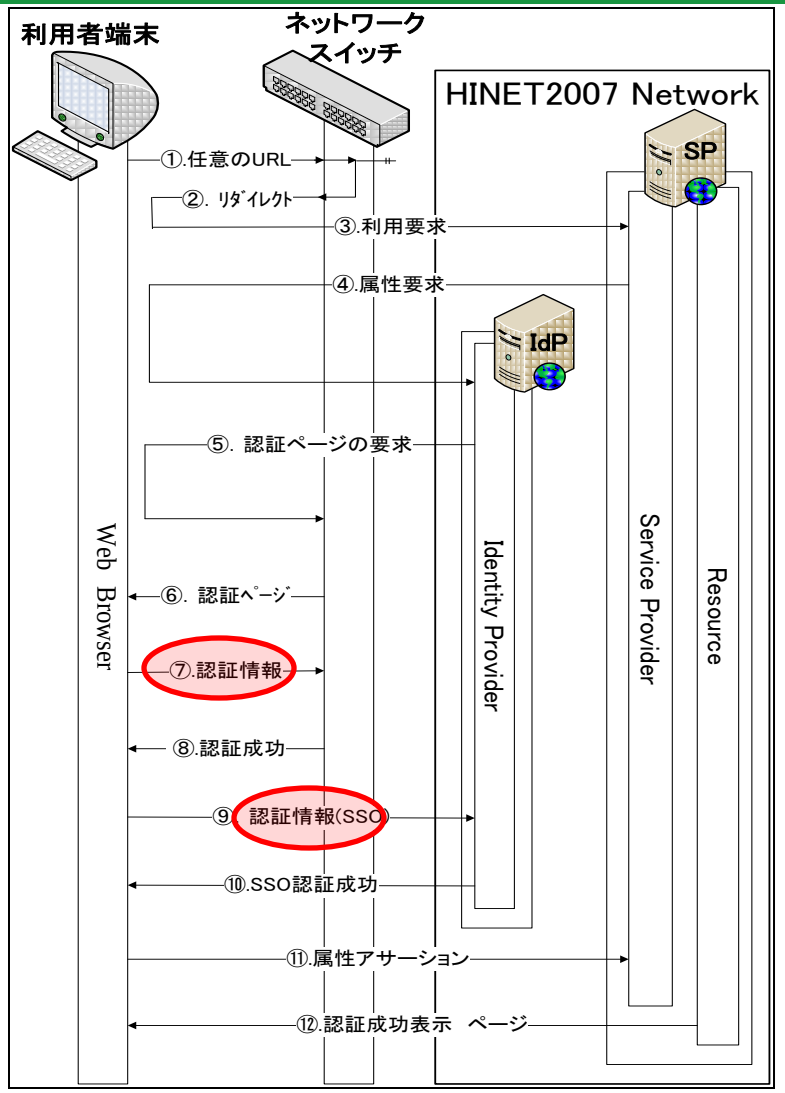
要求条件

1)ネットワーク認証は利用者端末から
　MACアドレスで利用者を特定

2)SSOは利用者端末のWebブラウザから
　認証プロバイダから認証チケット受け取り、サービスプロバイダに提示

3)利用者が行う認証操作は一度だけ
　SSOは一度の認証で許可されるすべての機能が利用できるシステム

認証情報送信を制御する
JavaScriptを開発中



まとめ

- セキュリティ対応の組織・体制紹介
- 学内インシデントへの対応から新キャンパスネットワークへ
- HINET2007（新キャンパスネットワーク）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、設計・構築のポイントについて
    - 個別ファイアウォール機能の実現
    - 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
  - 移行の完了
- SSO認証への対応

使用した機器の名称または仕様

広島大学

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

ご清聴ありがとうございました