既存ネットワーク環境へのIPv6導入のポイント
- 広島大学におけるIPv6への取り組み -

広島大学情報メディア教育研究センター
近堂 徹
(tkondo@hiroshima-u.ac.jp)

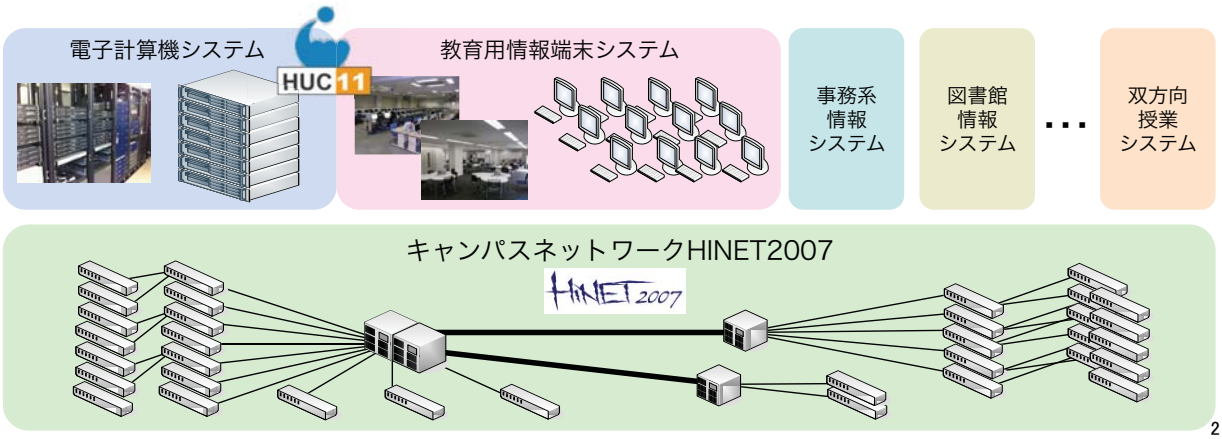
SS研システム技術分科会 2012年度第1回会合

広島大学

本日の内容：3つのIPv6への取り組み

広島大学

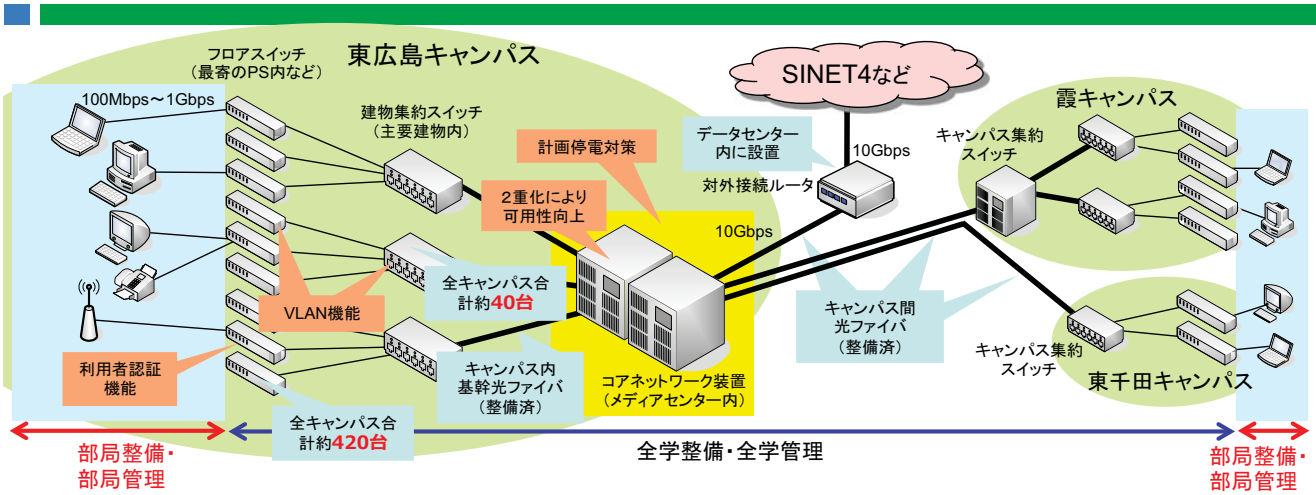
- **全構成員が利用するネットワーク基盤のIPv6化**
  - キャンパス情報ネットワーク HINET2007
- **全学情報サービスのIPv6化**
  - 電子計算機システム HUC11
- **全学で1144台展開する教育用情報端末のIPv6化**
  - 教育用情報端末システム ICE



広島大学におけるIPv6導入の主な流れ

年月	導入内容
2004年　4月	[SuperCSI] SINETよりIPv6アドレス (2001:2f8:1c0::/44) を割当
2004年　5月	[SuperCSI] SINETと接続
2004年 11月	SuperCSIよりIPv6アドレス (2001:2f8:1c1::/48) を割当
2004年 11月	広島大学のキャンパスネットワーク(HINET2001)と接続 以降，情報メディア教育研究センターサーバ接続用途で利用
2008年　4月	HINET2007 運用開始 グローバルゾーンでIPv6接続提供開始
2009年　3月	HINET2007 ファイアウォールゾーン, ローカルゾーン(一部のみ), 公衆ゾーンでIPv6接続提供開始
2010年　9月	電子計算機システム(HUC11), 教育用情報端末(ICE)運用開始 教育用情報端末約1200台へのIPv6アドレス付与
2011年　6月	メディアセンターウェブページのIPv6対応 World IPv6 Dayへの参加
2011年 11月	HUC11基幹サーバのIPv6対応開始 以降，順次対応作業を実施
2011年 12月	教育用情報端末に対する学外IPv6アクセス対応
2012年　6月	World IPv6 Launch

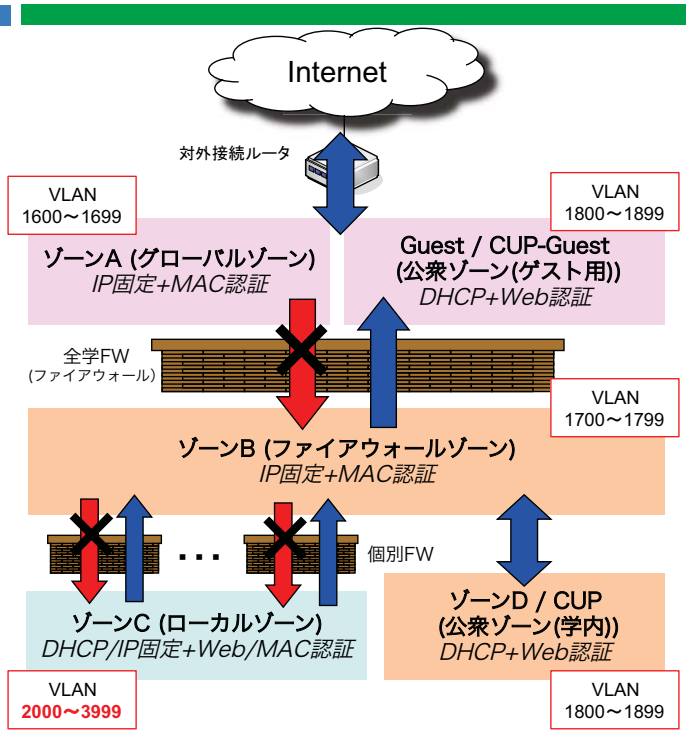
キャンパス情報ネットワーク HINET2007



HINET (Hiroshima univ. Information NETwork system)

- ✓ 2008年5月から稼働開始
- ✓ 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）を接続
- ✓ 教員約1800人, 職員約3300人，学生15000人
- ✓ フロアスイッチとして認証スイッチ約460台（約14000ポート）を全学整備

HINET2007の特徴



ゾーン種別とアクセス制限（概要）

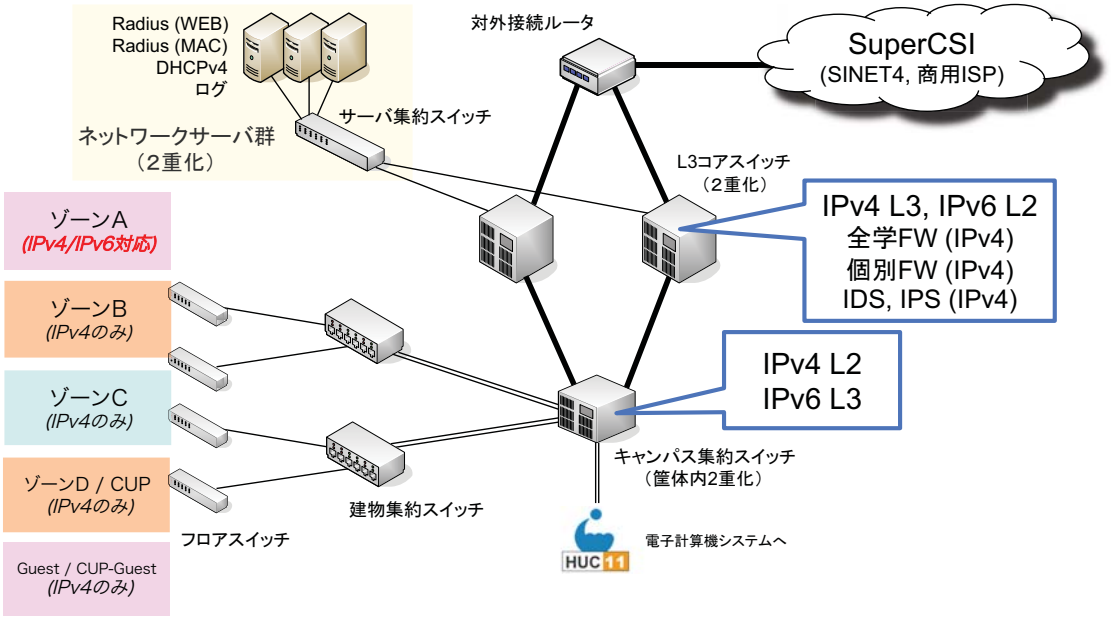
※ CUP (キャンパス・ユビキタス・プロジェクト)
= 全学整備による無線LANアクセスサービス
来訪者に対するネットワーク接続環境の提供

- **ゾーンの導入**
  - ✓ 利用者(教員)の申請に基づき,
    フロアスイッチに各ゾーンを設定
- **個別ファイアウォールの提供**
  - ✓ 各教員単位でのファイアウォール
    - ブロードバンドルータの機能相当
    - NAPT+DHCPを全学的に整備
    - ゾーンC 2,000個 (2,000VLAN)
- **VLANによる柔軟なネットワーク**
  - ✓ キャンパス間をまたがる研究室
    ネットワークにも対応
- **すべての場所で利用者認証**
  - ✓ 多様な機器に対応するために
    Web認証 or MAC認証を利用
    - 接続ゾーンによって異なる

IPv6導入のポイント

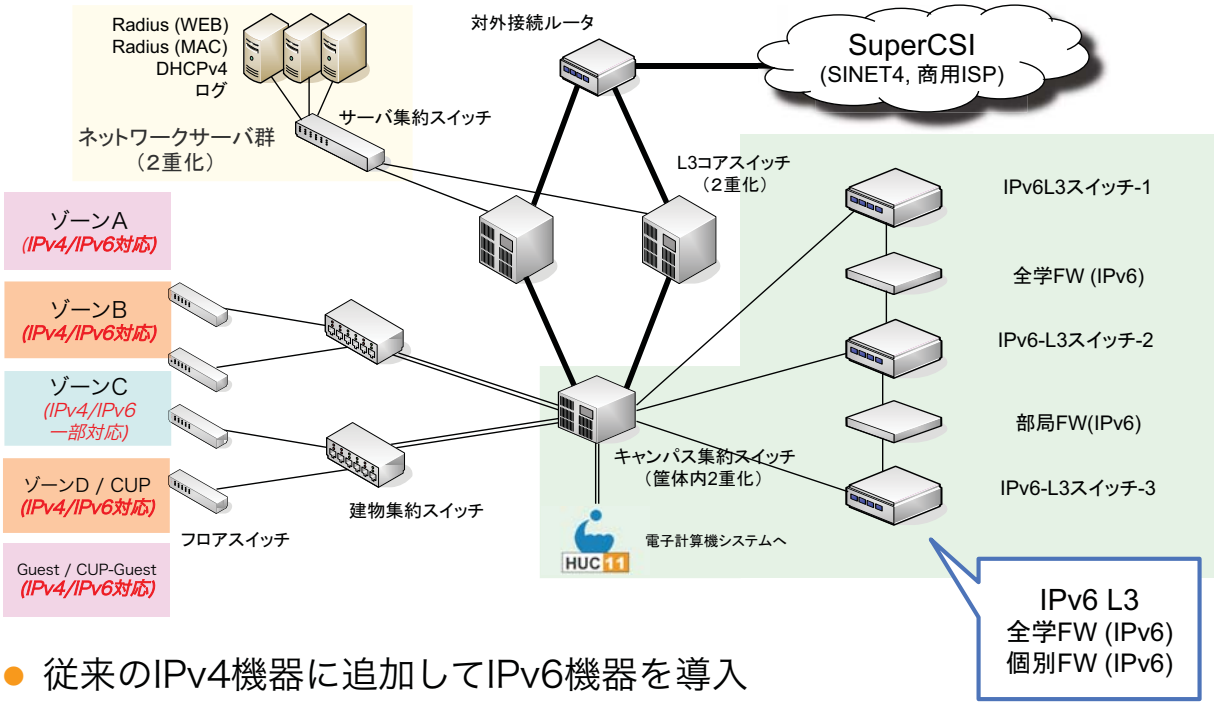
- 段階的な導入を実施
  - 2008年4月
    - HINET2007稼働時にゾーンAのみ提供開始
  - 2009年2月
    - 残りのゾーンでの提供開始
      - ✓ IPv6専用のL3スイッチとトランスペアレント型の
        ファイアウォールを導入
- 既存IPv4ネットワークにIPv6ネットワークを追加
- ゾーン毎に異なる提供方法を採用

基幹ネットワークの物理構成 （2008年4月 HINET2007運用開始当初）



- グローバルゾーン(ゾーンA)のみでIPv6の接続性を提供
  - IPv4との同程度のファイアウォールの提供が困難だったため
- IPv4とIPv6でルーティングポイントが異なる環境

基幹ネットワークの物理構成（2009年3月から現在）

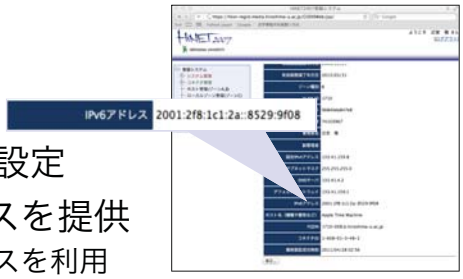


- 従来のIPv4機器に追加してIPv6機器を導入
- 全てのゾーンでIPv4/IPv6デュアルスタック対応
  - 但しゾーンCは**機器の仕様**により対応数に制限あり

HINET2007におけるIPv6提供

広島大学

- ゾーンによって提供方法が異なる
  - ゾーンA, B (サーバ向け)
    - RAによる自動設定なし，固定アドレス設定
    - IPv4アドレスに対応付けたIPv6アドレスを提供
      - ✓ IPv6アドレスの下位32ビットにIPv4アドレスを利用
      - ✓ HINET登録システムで管理



HINET登録システム
（広大IDとパスワードでログイン）

  - ゾーンC, D, CUP, CUP-Guest（クライアント向け）
    - RAによる自動設定
      - ✓ DNSはIPv4DHCPで配布
    - ウェブ認証はIPv4で実施
      - ✓ 認証スイッチはIPv6での認証に未対応

運用における課題と対策

広島大学

- IPv6の仕様に起因する課題
  - Path MTU Discovery Black Hole
    - 通信に必要なICMPv6通信をフィルタ
      - ✓ IPv4と同じポリシーでICMPv6のフィルタを適用
        - » 昨年度のWorld IPv6 Dayの際に外部から指摘

⇒ “Recommendations for Filtering ICMPv6 Messages in Firewalls” (RFC4890) に基づくフィルタリング設定を導入

  - 不正RA対策
    - 意図しない端末からのIPv6アドレス/デフォルト経路の広告
      - ✓ WindowsのICSによる6to4プレフィックスを広告 … [1]
      - ✓ 故意にRAを流す可能性もあり（DHCPv4でも同じ問題あり）… [2]

⇒ ・Router Preference (RFC4191)の設定 （ [1]に対する対策）
・NDP, DHCPモニタリングによる検知 ([2]に対する対策)

運用における課題と対策

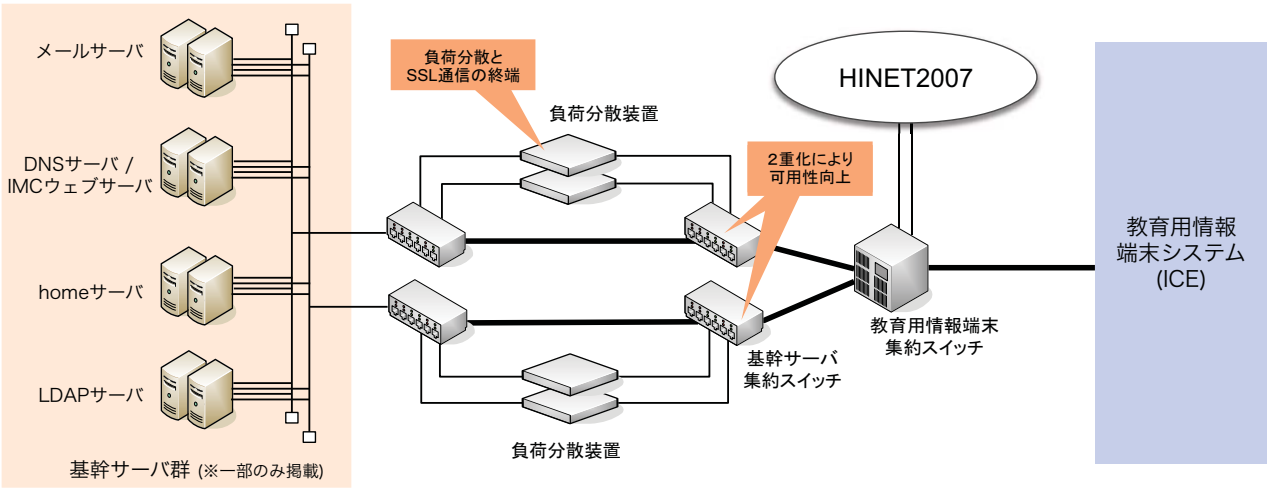
広島大学

- IPv4/v6デュアルスタック運用による課題
  - 障害時の切り分けが複雑化
    - IPv4とIPv6で経路が異なる
    - 利用者の端末も様々　(Windows XP/Vista/7, Mac OS, Linux…)
      - ✓ 利用者はIPv4かIPv6かは気にしない
    - RA自動設定の端末は一時アドレスを利用

⇒ ・ログの統一的な管理
・IPv6の挙動も考慮したトラブル対応の確立

電子計算機システム

広島大学



HUC11 (Hiroshima University Computer system)

- ✓ 2010年8月から稼働開始
- ✓ 広島大学の教育研究を支える情報基盤
- ✓ DNS, 電子メール, ウェブページサービス, HPCグリッド, 教育用情報端末, プリンタなどのサービスを提供
- ✓ ネットワーク2重化, サーバ2重化（一部）による可用性確保

基幹サーバのIPv6導入状況

広島大学

(2012年7月1日時点，主要なサービスのみ掲載)

サーバ	サービス	IPv6対応
DNSサーバ	–	○ (2012/3 対応)
loginサーバ	SSHサービス	○ (2012/3 対応)
	WebDAVサービス	× (2012年度前期対応予定)
homeサーバ	http (ホームページ公開) サービス	○ (2012/8 対応)
受信メールサーバ	POP/IMAPサービス	× (2012年度前期対応予定)
送信メールサーバ	SMTPサービス	× (検討中)
hostingサーバ	SSHサービス	○ (2012/3 対応)
	http (ホームページ公開) サービス	× (2012年度前期対応予定)
	POP/IMAPサービス	× (2012年度前期対応予定)
プロキシサーバ	-	○ (2012/6 対応)
VPNサーバ	-	× (検討中)
センターウェブサーバ	-	○ (2011/5 対応)

- サーバ側でIPv4/IPv6デュアルスタック化
  - IPv4と(できるだけ)同じポリシーでの運用を検討
    - ✓ SSL終端処理ポリシー, アクセス制限ポリシーなど

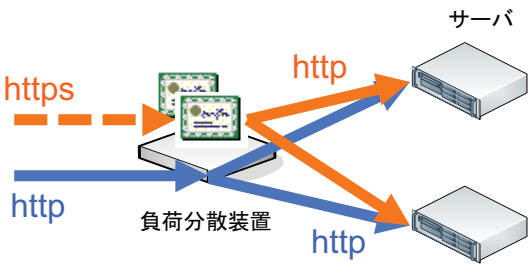
導入に際して直面した問題（1）

広島大学

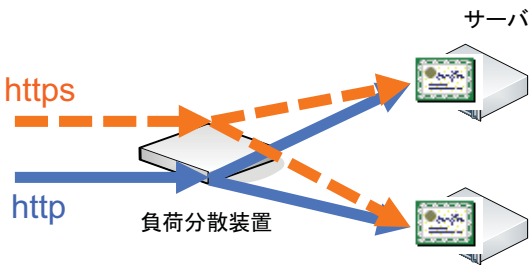
■負荷分散装置の影響

- 構成が装置の仕様に左右される
  - –IPv4と同じ構成にするのが難しい
    - ✓例) IPv6の場合，負荷分散措置でのSSL終端ができない

ファームウェアの
バージョンアップ
で対応予定



IPv4の場合　負荷分散装置でSSL終端可能



IPv6の場合　サーバ側で終端させる必要あり

導入に際して直面した問題（2）

広島大学

- アクセス制限(.htaccess)の表記
  - ホームページ公開(http)サービス
    - 利用者がpublic_html配下にコンテンツを自由に設置することができるサービス
    - 利用者の都合で学内限定公開を選択できる
      - ✓ .htaccessをシステムで自動作成，かつ利用者が自由に変更することも可能
    - 旧システムではIPv4アドレスでのみ制限
  - サーバのIPv6対応により意図しないアクセス制限が発生
    - Orderディレクティブの指定方法により挙動が異なる

➡ システム側での一括変更および該当者への周知で対応

導入に際して直面した問題（3）

広島大学

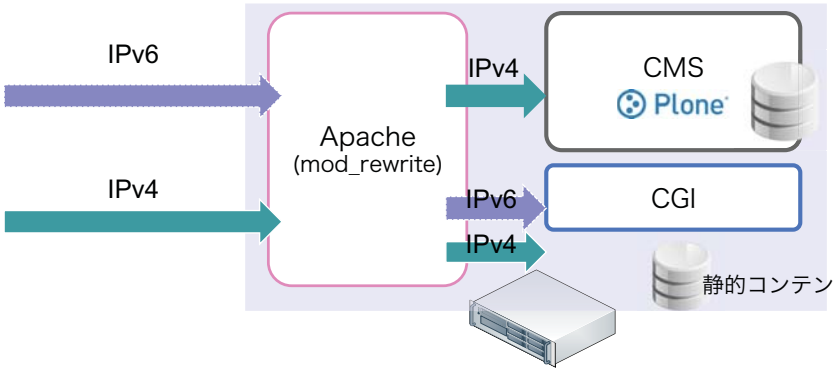
- サーバ監視
  - (導入している)監視ソフトウェアがIPv6未対応

➡ NagiosでIPv4とIPv6でサービス毎に監視，通知
(IPv6 Readyな外部ホスティングサービスからの監視も実施)

※Nagios - オープンソースの監視ソフトウェア
http://www.nagios.org

- IPv6未対応のCMSやサービスへの対応
  - ウェブアプリケーションで稼働するCMS
    - メディアセンターの場合はPloneを利用
  - 単体ではIPv6に対応することができない

メディアセンターウェブサイトの場合

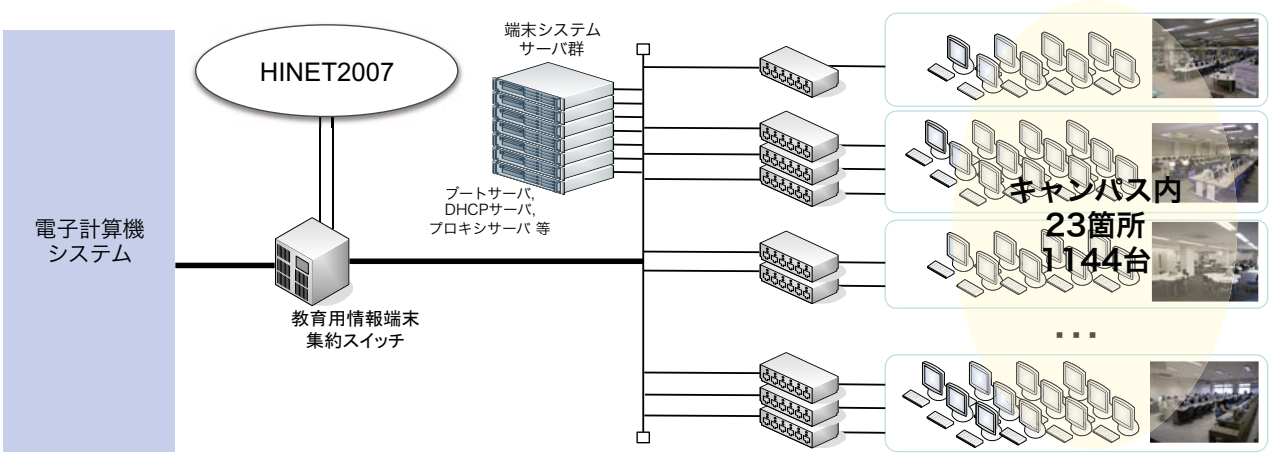


- リバースプロキシを利用してCMSをIPv6対応
  - フロントエンドにApache, mod_rewriteモジュールを利用
  - 静的コンテンツのオフロード，CGIとの連携を考慮

【課題】

  - CMSからみると，クライアントのIPアドレスがみえなくなる
    - ✓ (IPアドレスによる)アクセス制限を行う場合はフロントエンド側で制御
  - 障害時の切り分けが複雑化

教育用情報端末システム (ICE)



ICE (Information system for Communication and Education)

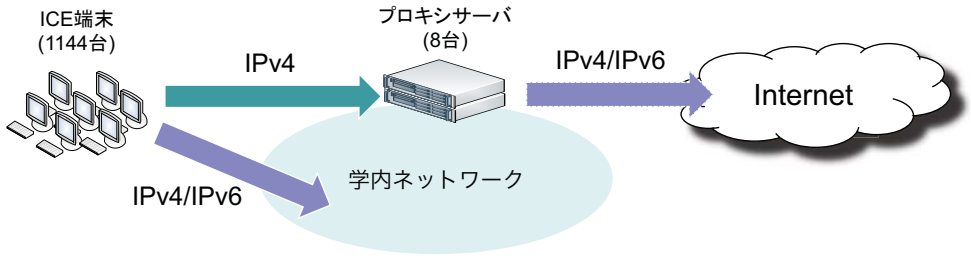
- ✓ 情報科目の授業や演習，自主学習の目的で利用
- ✓ 東広島，霞，東千田地区あわせて23箇所，1144台を整備
- ✓ 情報メディア教育研究センターが管理
- ✓ Windows/Linuxのデュアルブート，ネットブート方式を採用
- ✓ 外部へのウェブアクセスはプロキシサーバを経由

ICE端末におけるIPv6利用

広島大学

- 全端末にIPv6アドレスを付与
  - RAによる自動設定
    - 通信には一時アドレスを利用
  - DNSはIPv4DHCPで配布

- プロキシサーバのIPv6対応 (2012年1月)
  - 端末⇔プロキシ間はIPv4を利用
    - アクセスログの可読性を考慮
  - 学内のIPv6対応サイトへは直接IPv6通信



まとめと今後の展開

広島大学

- 広島大学におけるIPv6への取り組みについて紹介
  - 導入を通じて感じること
    - IPv6導入の障壁は確実に下がってきている
      - ✓ ネットワーク機器の実装，クライアントOSの実装
    - …が，頭では理解していても動かしてみないと分からない部分も多い
    - 運用に関する経験，ノウハウの共有が重要！
- 今後の展開
  - デュアルスタック運用時の影響を見極めながら展開
    - クライアント環境に対するIPv6環境の充実
      - ✓ DHCPv6の運用，RA/NDP監視体制の強化
    - 各種サーバのIPv6対応
  - トラブルシューティング，ユーザサポート体制の確立