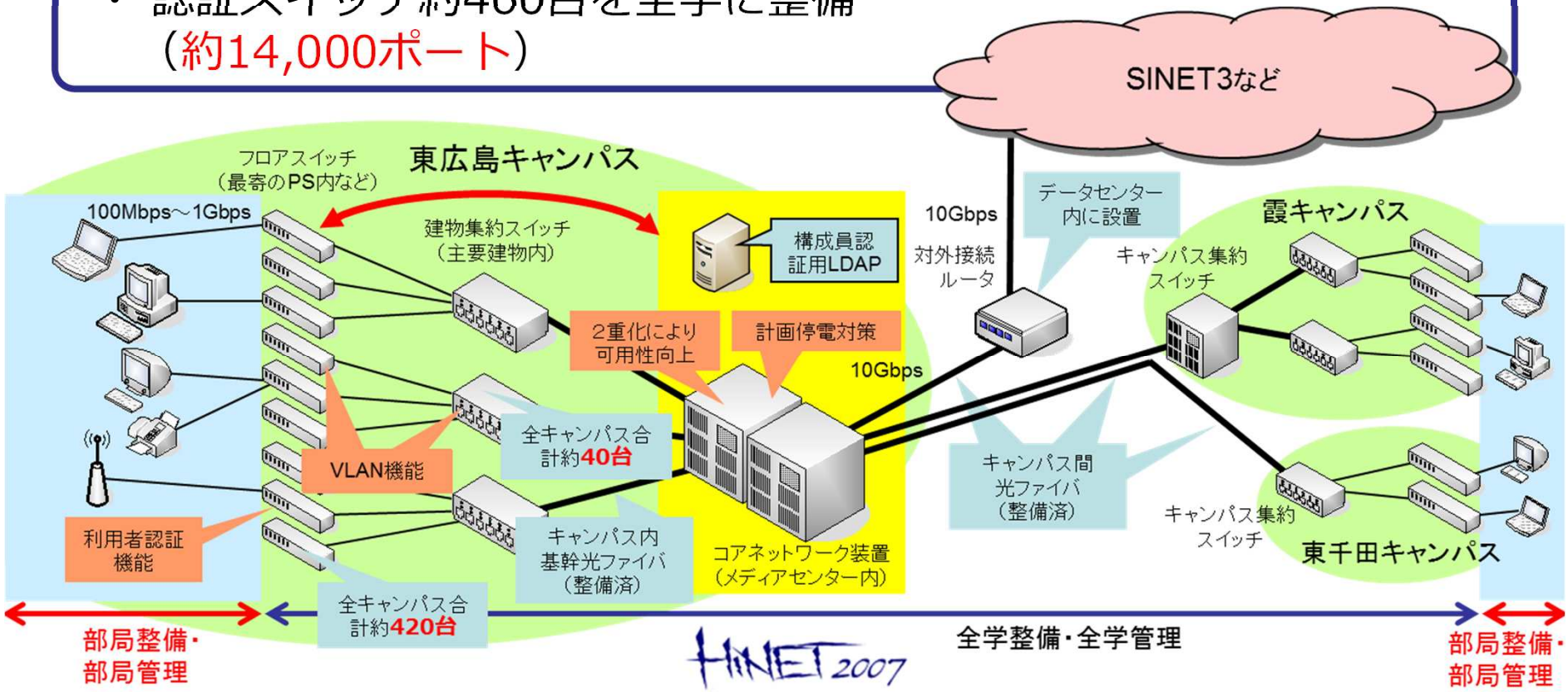
学認を利用した
キャンパスネットワークの利用者認証

広島大学 情報メディア教育研究センター
西村 浩二
kouji@hiroshima-u.ac.jp

広島大学

HINET2007の概要

・2008年5月から本格移行開始、2009年3月末完全移行
・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
・ 認証スイッチ約460台を全学に整備
　（約14,000ポート）

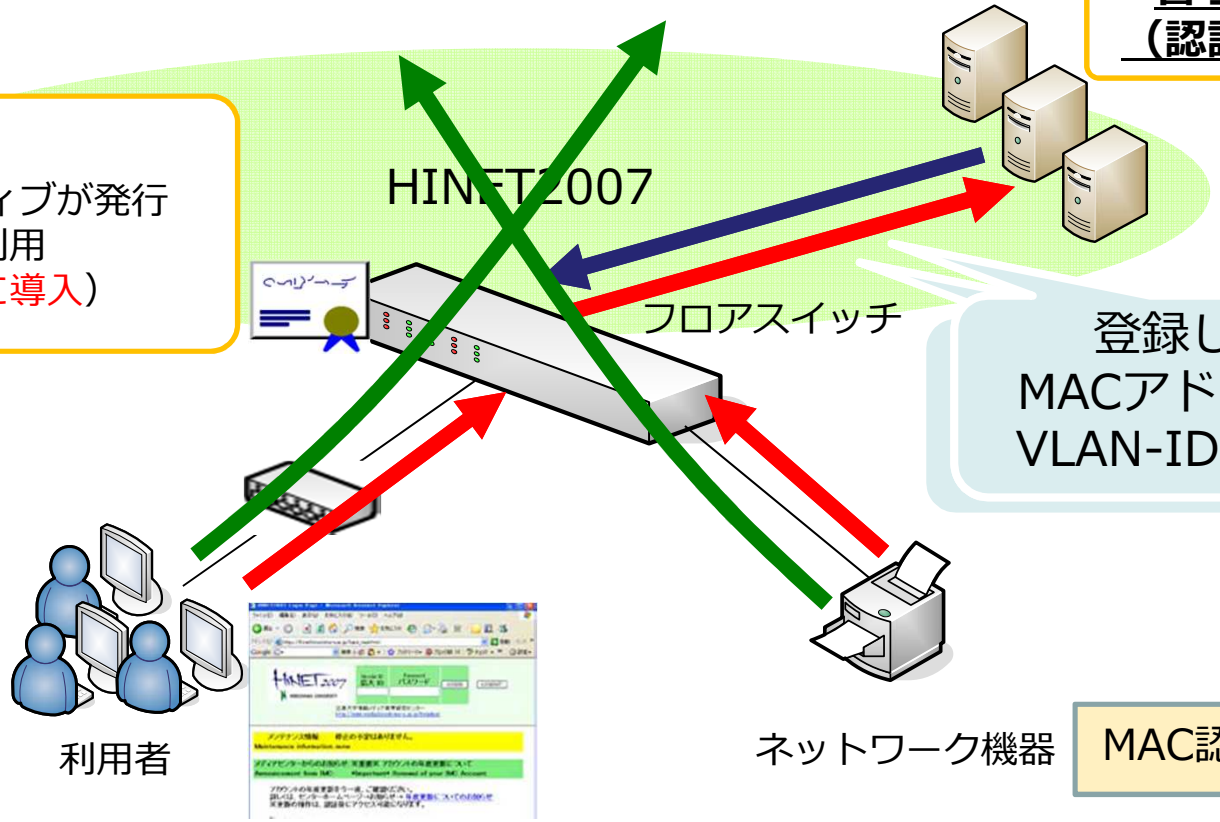


HINET2007の特徴

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一元的に管理
- 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、SINET3, 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

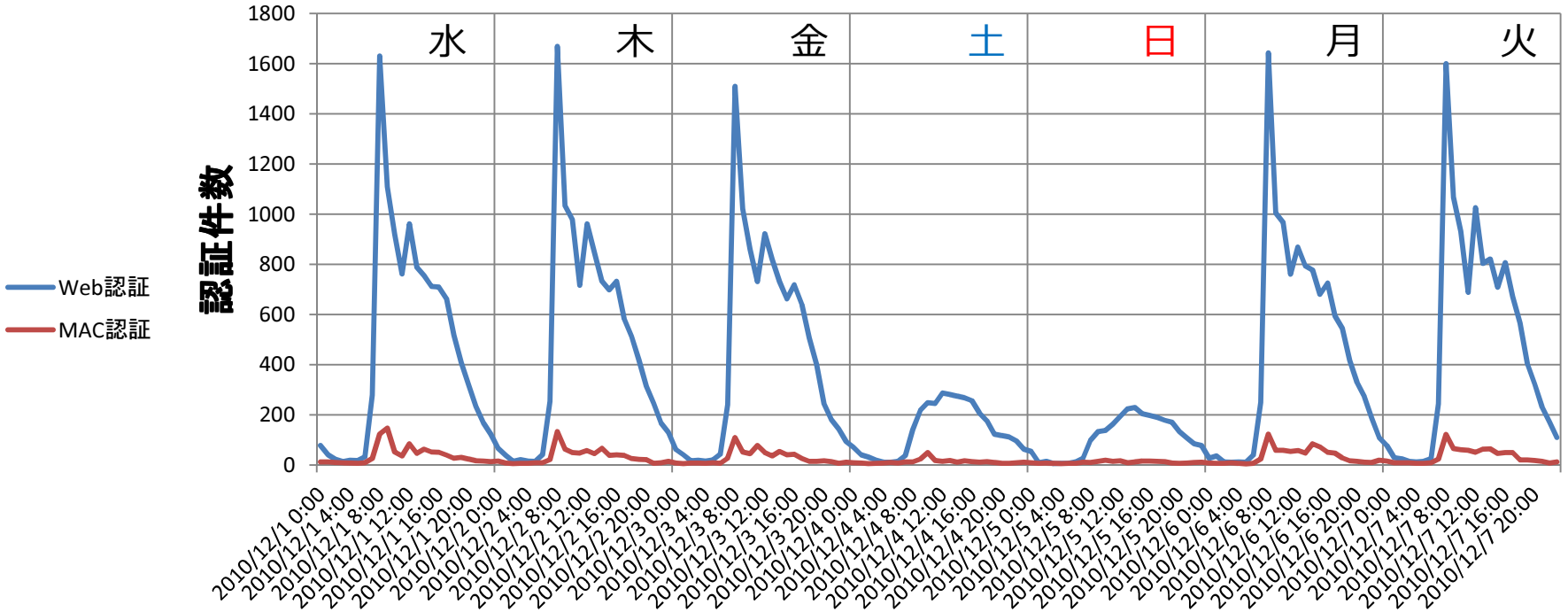
利用者認証の概要



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認証件数（時間毎）



	2010-12-01	2001-12-02	2010-12-03	2010-12-04	2010-12-05	2010-12-06	2010-12-07
Web認証延べ件数	**11,278**	**11,199**	**10,636**	**3,346**	**2,654**	**11,065**	**11,364**
Web認証実数	6,058	6,032	5,830	2,040	1,646	6,003	6,067
MAC認証延べ件数	914	756	687	309	259	821	812
MAC認証実数	326	267	261	94	69	271	322

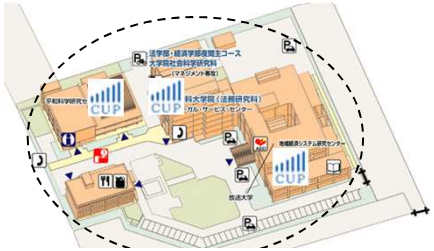
→ 毎日6,000名超の構成員にSSOの利用機会がある

SSO機能追加の背景

広島大学

- 大学におけるWebサービスの普及
  - 充実した学習環境の提供や情報システムの活用による業務作業のサポート
    - 学習支援（電子ジャーナル、WebCT）、学生・教職員ポータルサイト、Webメールなど…
  - サービス間での認証連携
    - 認証連携されていない（利用者はサービス毎に認証を要求される）
    - 無理な認証連携（パスワードとIDをサービス間で直接やり取り）
  - ★ ゲスト向けサービス
    - キャンパス・ユビキタス・プロジェクト（CUP）
    - 来訪者に対するネットワーク接続環境の提供

広島大学公式無線LANアクセスポイント



学内専用AP

フレッツスポット用AP併設

設置AP数：175（2010年12月現在）

アカウントの種別と利用可能サービス

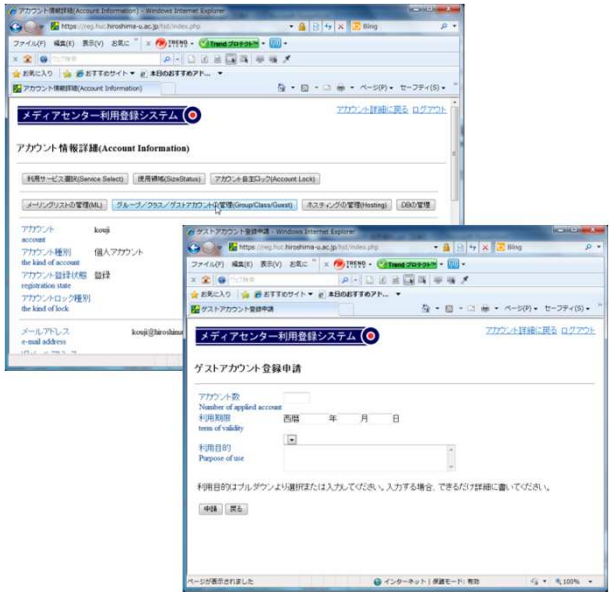
広島大学

機能	個人アカウント		グループアカウント	クラスアカウント	ゲストアカウント
取得可能な方	学生、教職員	学外者、名誉教授	常勤の教職員	常勤の教職員(*1)	常勤の教職員(*1)
利用可能期間	在籍期間中	広大IDの有効期限内	所有者の在籍期間中	申請期間中	申請期間中
年度更新手続き	必要	必要	必要	不要	不要
メール送受信	○	○	○	○	×
アカウント登録時のメールアドレス	アカウント名@hiroshima-u.ac.jp(*3)				×
メールアドレス変更(*2)	○	○	○	×	×
ホームディレクトリ容量	1 GB		10 GB	1 GB	×
印刷可否	○	×	×	○	×
ホームページ公開	○	○	○	○	×
アカウント登録時のURL	http://home.hiroshima-u.ac.jp/アカウント名(*3)				×
URLの変更(*2)	○	○	○	×	×
センター端末利用	○	×	×	○	×
HPC利用	○	○	×	○	×
フレッツ接続、VPN接続	○	○	×	○	×
情報コンセント利用	○	○	×	○	○
HINET2007ウェブ認証	○	○	×	○	○
複数メンバでの利用	×	×	○	×	×

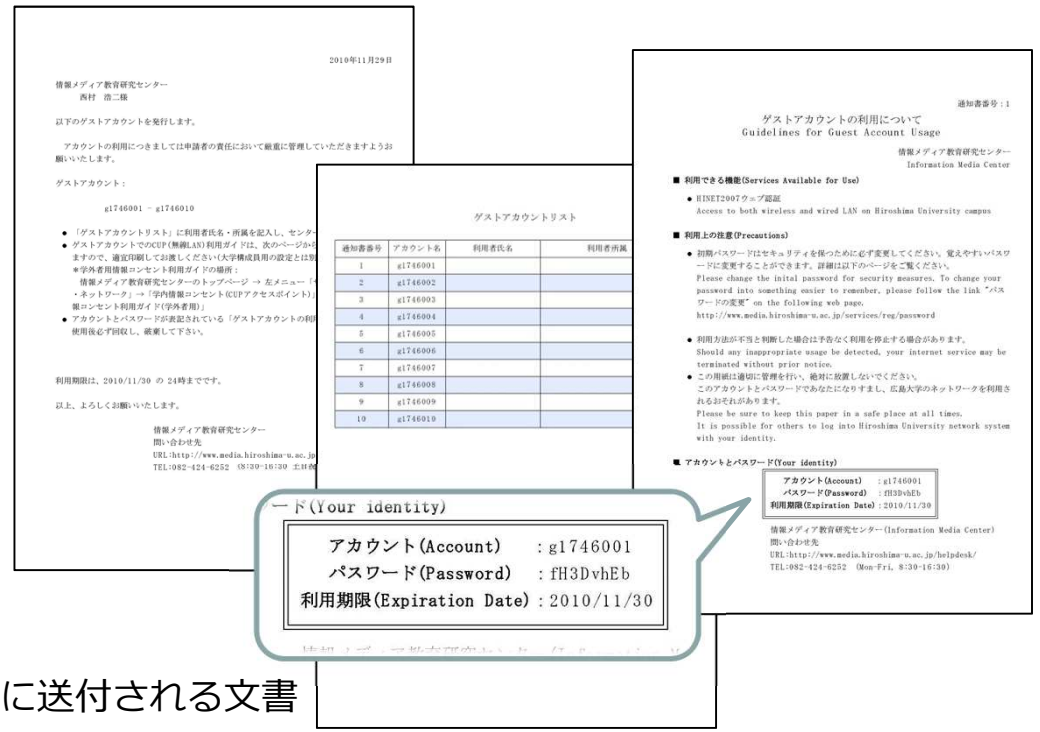
http://www.media.hiroshima-u.ac.jp（ホーム → 提供サービス → メディアセンター利用登録）

認証ネットワークのゲスト利用

- ゲストアカウントの取得
  - 常勤の教職員であれば申請可能
    - メディアセンターで使途等のチェックの後、発行処理
  - 構成員：利用者のセキュリティポリシー遵守の周知・徹底、使用者リストの管理、インシデント発生時の窓口対応等の責任を負う
  - 利用者：複雑なアカウント名とパスワードの入力と管理の責任を負う



申請ページ（利用登録システム）



構成員（申請者）に送付される文書

SSO機能追加の背景

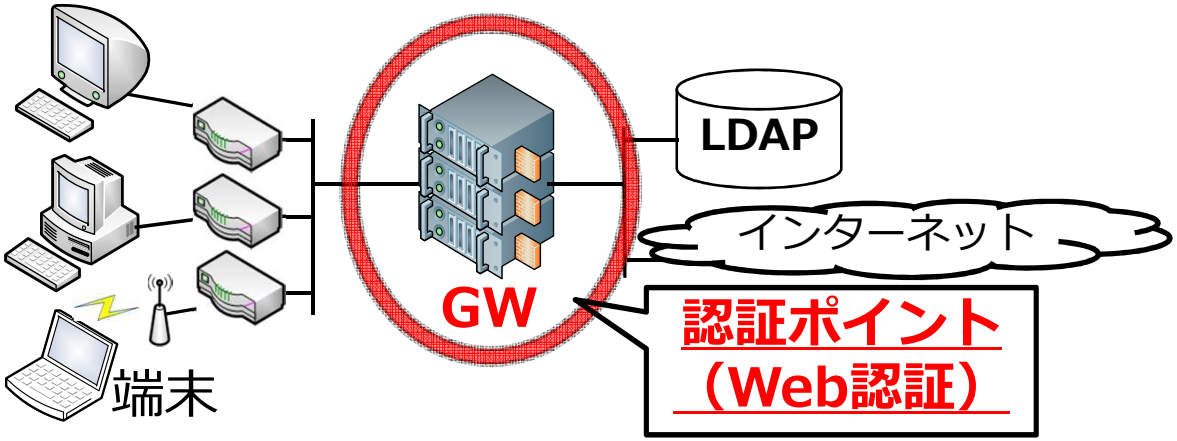
広島大学

- 大学におけるWebサービスの普及
  - 充実した学習環境の提供や情報システムの活用による業務作業のサポート
    - 学習支援（電子ジャーナル、WebCT）、学生・教職員ポータルサイト、Webメールなど…
  - サービス間での認証連携
    - 認証連携されていない（利用者はサービス毎に認証を要求される）
    - 無理な認証連携（パスワードとIDをサービス間で直接やり取り）
  - ★ ゲスト向けサービス
    - キャンパス・ユビキタス・プロジェクト（CUP）
    - 来訪者に対するネットワーク接続環境の提供（ゲストアカウント）
- HINET2007へのSSO機能の追加
  - 増大する認証機会への対応
    - ネットワークとWebサービスの認証連携（利用者の負担軽減）
  - セキュリティ上好ましくない無理な認証連携の解消
    - 適切に管理された環境下での認証連携
  - ゲスト利用者への対応
    - 手続き（構成員）と利用（ゲスト利用者）の煩雑さを解消

ネットワーク認証方式あれこれ

広島大学

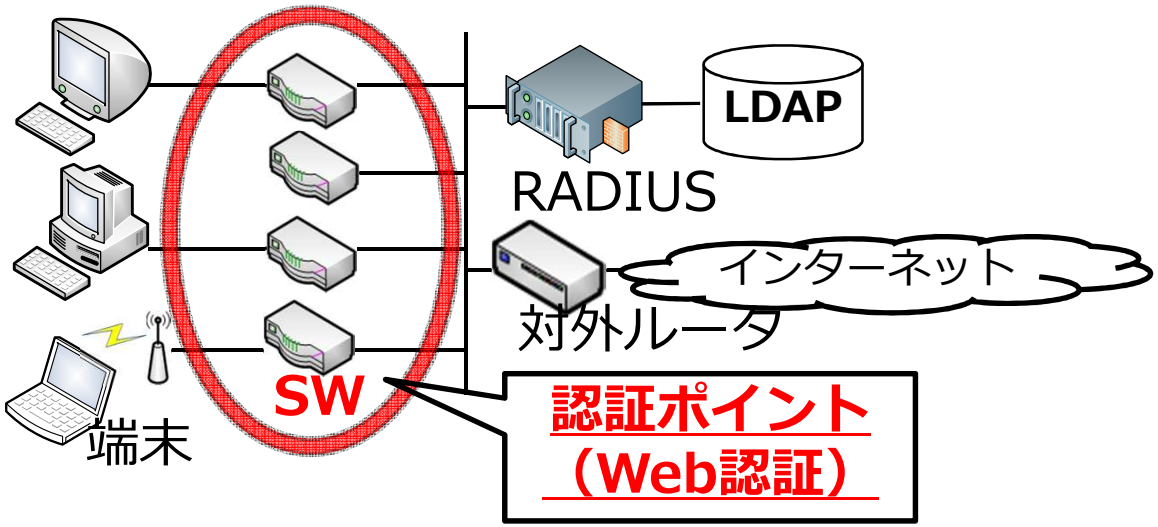
GWベースのネットワーク認証（ex.Opengate@佐賀大）



メリット
- 機能拡張の容易さ
- 機器構成の柔軟さ

デメリット
- ワイヤレートが出ない

SWベースのネットワーク認証（ex.HINET2007@広島大）

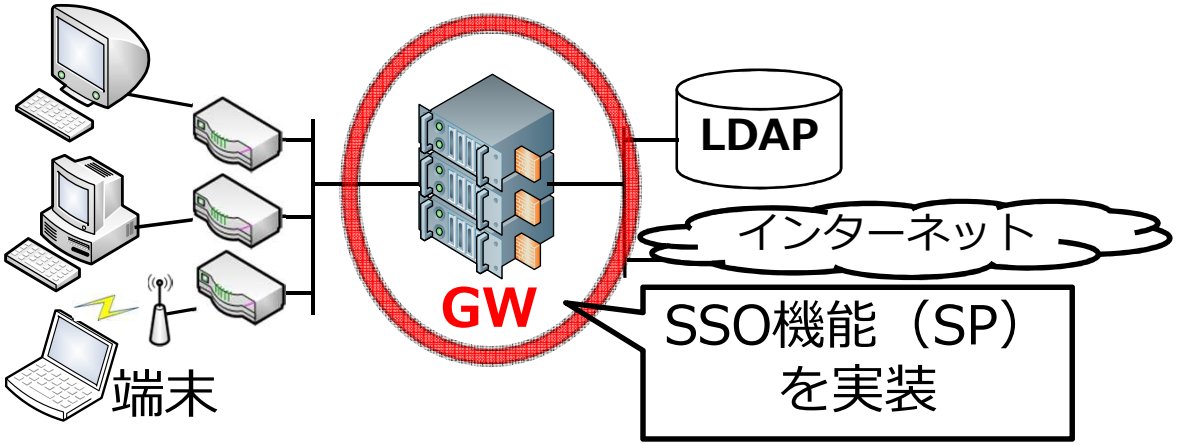


メリット
- 水際対策が可能
- 分散処理が可能

デメリット
- 機能拡張が困難

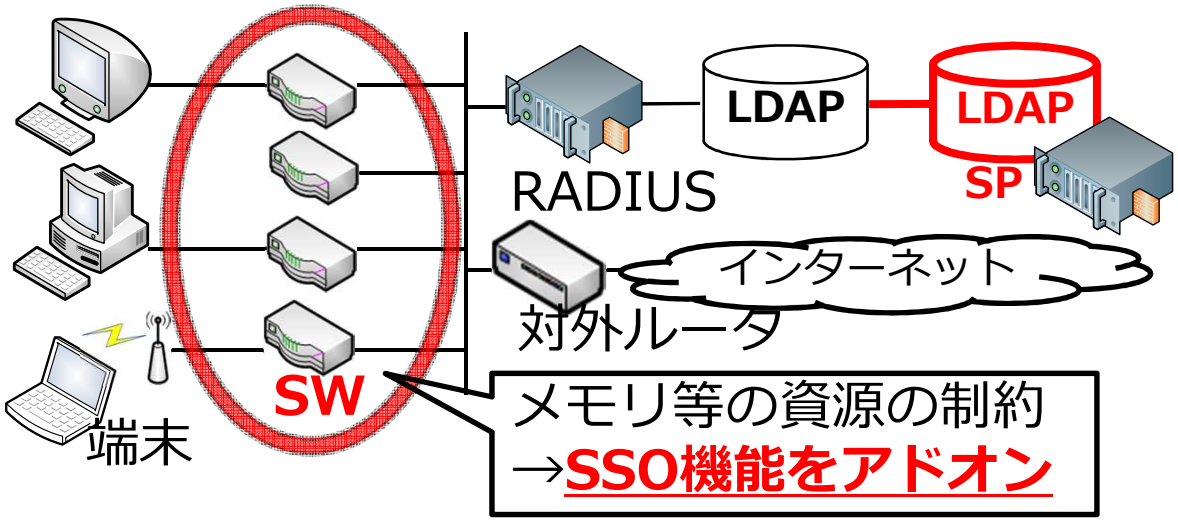
各方式でのSSO対応方法

GWベースのネットワーク認証（ex.SSO-Opengate@佐賀大）



機能拡張の柔軟さを活かし、GWにSPを実装
→SSOに対応した
ネットワーク認証

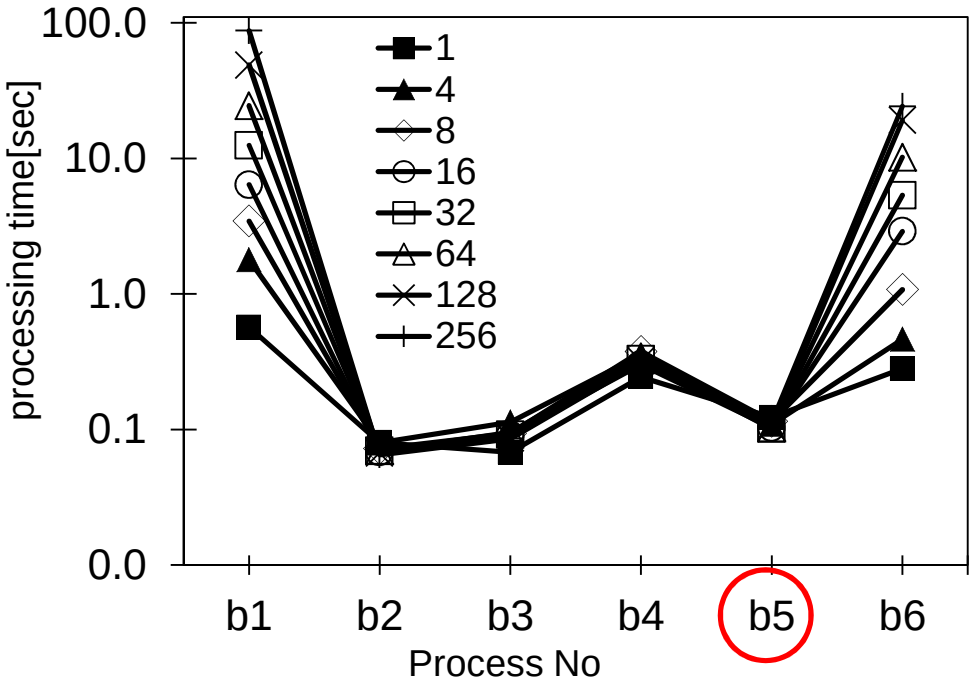
SWベースのネットワーク認証（ex.HINET2007@広島大）

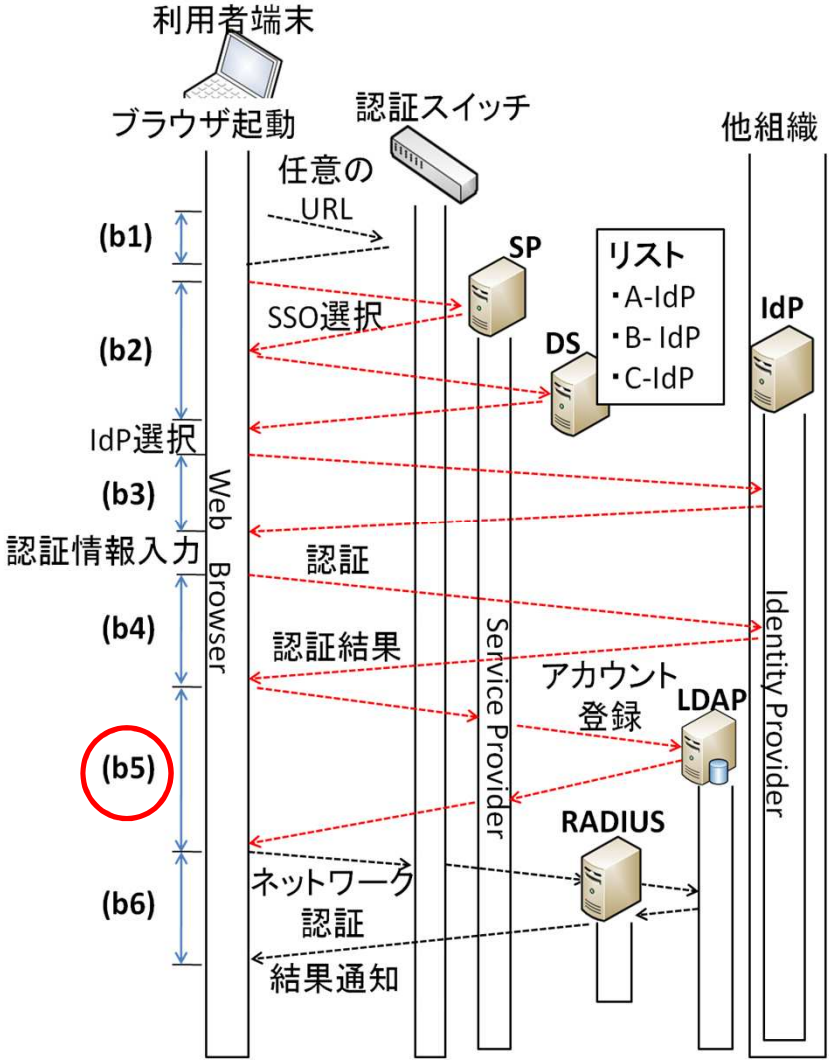


SWの機能拡張に依らないSSO機能の実装
→SWの認証機構と
SSO認証の連携

HINET2007へのSSO機能の追加

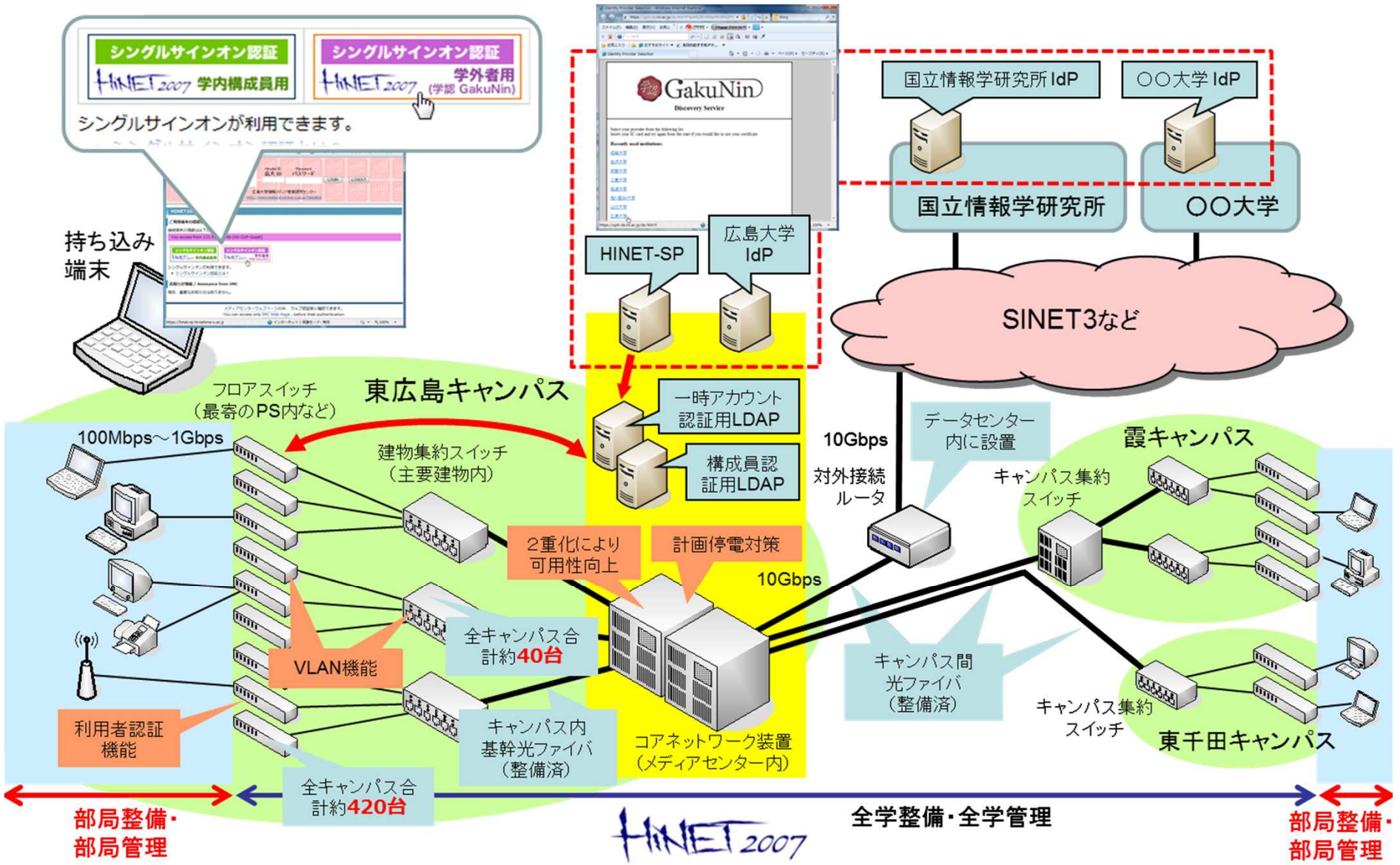
- 認証ステップ
  1. ブラウザでSWにアクセス（SPにリダイレクト）(b1)
  2. SSO認証 (b2～b4)
  3. 一時アカウント登録 (b5)
  4. 一時アカウントでネットワーク認証 (b6)





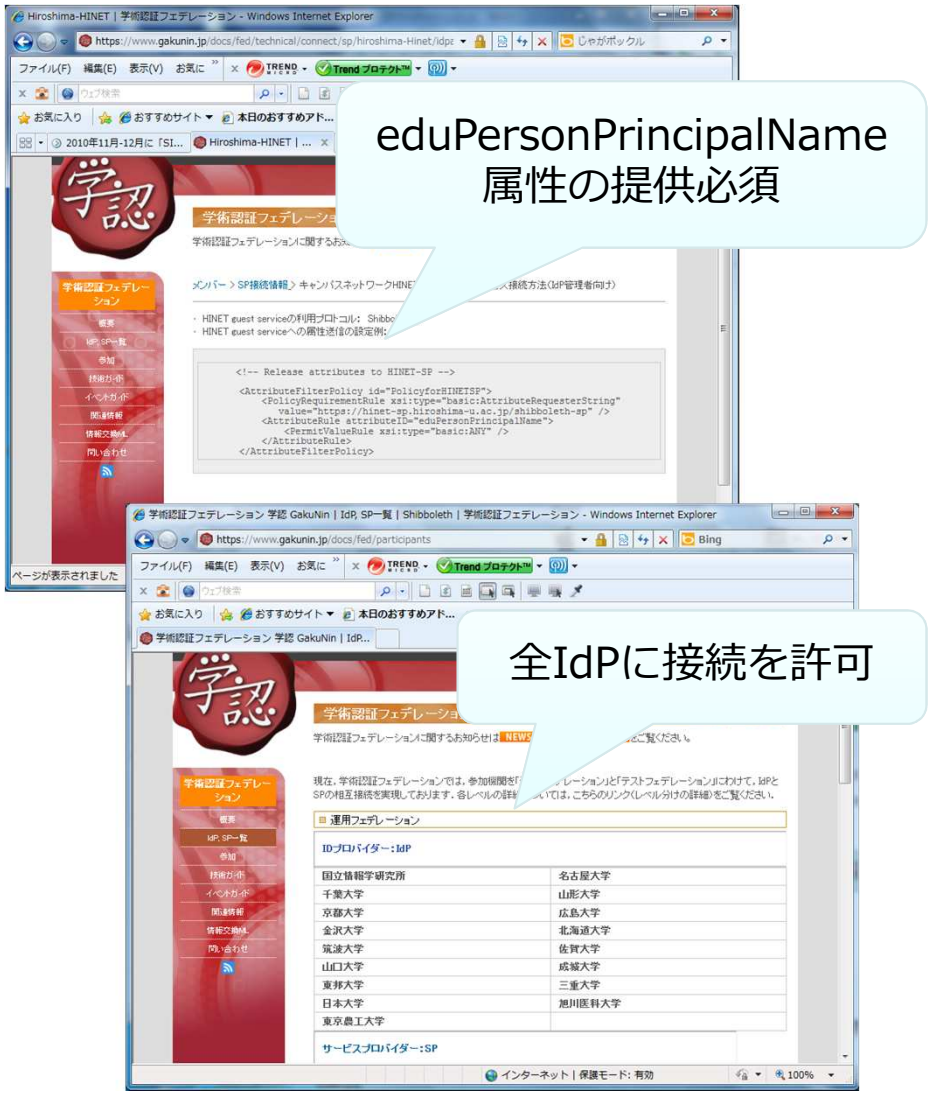
→ SSO認証処理と一時アカウント登録処理の追加による影響小

HINET2007のSSO認証対応

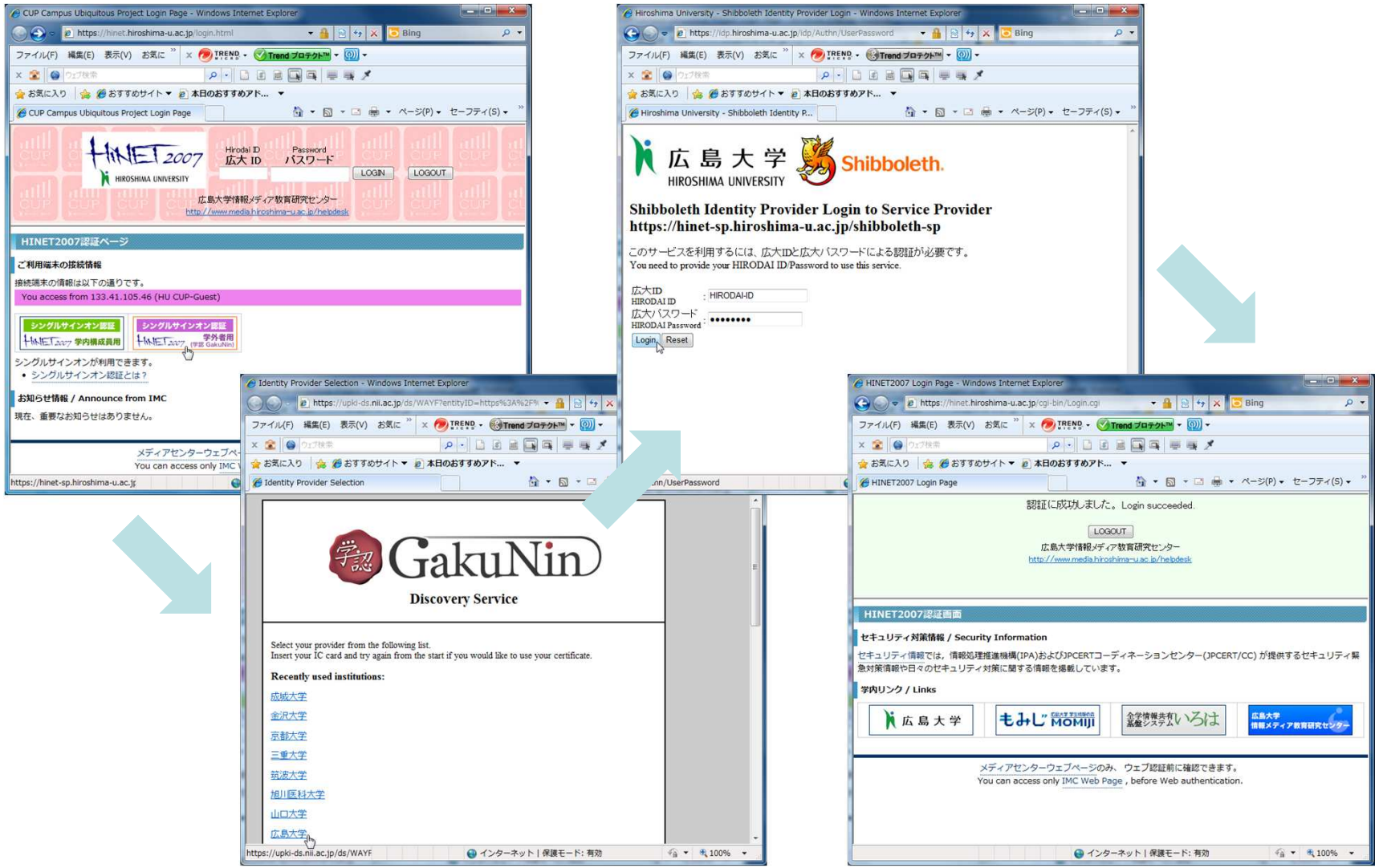


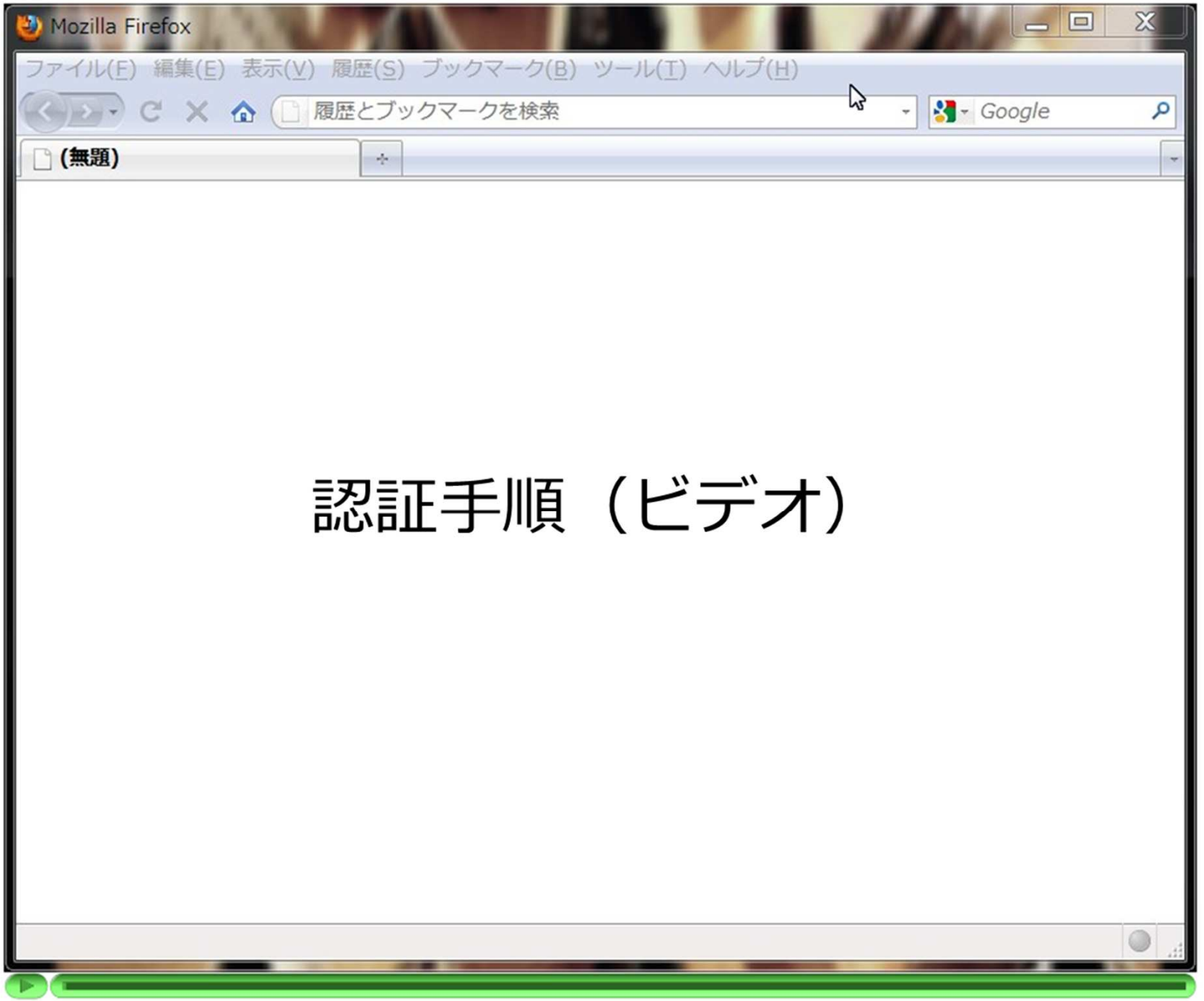
HINET-SP接続情報（11/22公開）

- IdP（学認参加組織）側の設定
  - eduPersonPrincipalName属性の提供必須
    - 他大学と横並びに決定
    - 組織のIDを見せないというSSOのポリシーとの関係は？
- SP（広島大学）側の設定
  - 学認に参加しているIdPを盲目的に設定（接続許可付与）
    - 今後の展開によっては選択の要求があるかも？
    - その場合、登録依頼は組織間で個別に行う？



認証手順


CUP Campus Ubiquitous Project Login Page - Windows Internet Explorer
HINET2007
HIROSHIMA UNIVERSITY
Hirodai ID
広大 ID
Password
パスワード
LOGIN
LOGOUT
広島大学情報メディア教育研究センター
HINET2007認証ページ
ご利用端末の接続情報
You access from 133.41.105.46 (HU CUP-Guest)
シングルサインオン認証
シングルサインオンが利用できます。
お知らせ情報 / Announce from IMC
現在、重要なお知らせはありません。
Hiroshima University - Shibboleth Identity Provider Login - Windows Internet Explorer
広島大学
HIROSHIMA UNIVERSITY
Shibboleth.
Shibboleth Identity Provider Login to Service Provider
https://hinet-sp.hiroshima-u.ac.jp/shibboleth-sp
このサービスを利用するには、広大IDと広大パスワードによる認証が必要です。
You need to provide your HIRODAI ID/Password to use this service.
広大ID
HIRODAI ID
広大パスワード
HIRODAI Password
HIRODAI-ID
Login
Reset
Identity Provider Selection - Windows Internet Explorer
GakuNin
Discovery Service
Select your provider from the following list.
Insert your IC card and try again from the start if you would like to use your certificate.
Recently used institutions:
成城大学
金沢大学
京都大学
三重大学
筑波大学
旭川医科大学
山口大学
広島大学
HINET2007 Login Page - Windows Internet Explorer
認証に成功しました。Login succeeded.
LOGOUT
広島大学情報メディア教育研究センター
HINET2007認証画面
セキュリティ対策情報 / Security Information
セキュリティ情報では，情報処理推進機構(IPA)およびJPCERTコーディネーションセンター(JPCERT/CC) が提供するセキュリティ緊急対策情報や日々のセキュリティ対策に関する情報を掲載しています。
学内リンク / Links
広島大学
もみじ MOMIJI
学術情報共有基盤システム いろは
広島大学 情報メディア教育研究センター
メディアセンターウェブページのみ、ウェブ認証前に確認できます。
You can access only IMC Web Page , before Web authentication.


Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
履歴とブックマークを検索
Google
(無題)
認証手順（ビデオ）

ゲスト(学認)利用者 第1号！

シンポジウム

学術情報流通の危機を考える

電子ジャーナル・出版・機関リポジトリの現在と未来

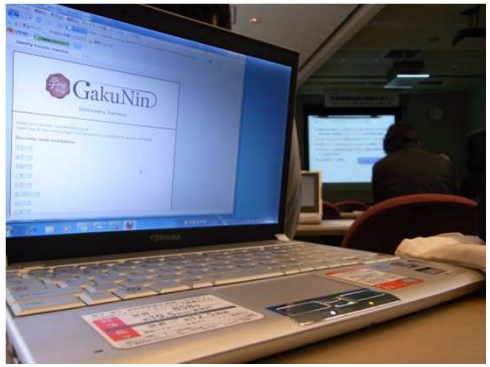
日時：平成22年11月29日（月） 13:00～17:00

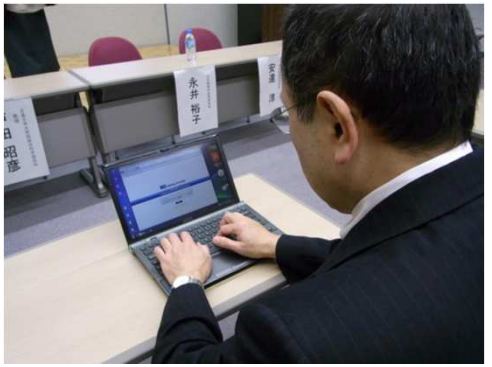
場所：広島大学中央図書館ライブラリホール

学認の認証は１回でできたんだけど、無線LANの接続（WPA2）には２回失敗しちゃったよ。（笑）

広島大学長 浅原 利正

NII 安達 淳 先生





ゲスト利用者の無線LAN接続

広島大学

- 学認の利用によって、学認参加組織の構成員はゲストアカウントの事前取得が不要になったが…
  - ゲスト用設定情報（マニュアル）が必要
  - 土日、休日や夜間の対応窓口が問題
- 対策
  - 接続に最低限必要な情報を、利用可能場所のポスターに表示

ESSID（学外者用）：HU-Guest〇〇
暗号化：WPA2-AES，　認証：PEAP（mschap-v2）を設定
ルート証明機関：「Security Communication RootCA1」を指定
「Windowsのログオン名とパスワードを自動的に使う」はOFFにする
PEAP認証完了後、「ゲストアカウント」または「学認」によるWeb認証が必要

  - PEAP認証の情報もシールにして貼付（年度毎変更）

HU-Guest〇〇には（ID：×××，パスフレーズ：××××）で接続できます。

  - セッション鍵は端末毎に異なるため安全性への影響は最小

無線LANポスター


CUP
HIROSHIMA UNIVERSITY
無線ＬＡＮ
利用できます
「情報コンセント利用ガイド」は
情報メディア教育研究センター
および　利用場所の最寄りの事務室
で配布しています。
ESSID（学外者用）：HU-Guest○○
暗号化：WPA2-AES、 認証：PEAP（mschap-v2）を設定
ルート証明機関：「Security Communication RootCA1」を指定
「Windowsのログオン名とパスワードを自動的に使う」はOFFにする
PEAP認証完了後、「ゲストアカウント」または「学認」によるWeb認証が必要
この場所の ESSID は
HU-CUP20
HU-Guest20
HU-Guest○○には（ID：×××，パスフレーズ：××××）で接続できます。
■情報コンセントの利用方法に関するご質問は
情報メディア教育研究センター
本館　電話：082-424-6252　内線：（東広島）84-6252
霞分室　電話：082-254-5693　内線：（霞）83-6033
URL：http://www.media.hiroshima-u.ac.jp/helpdesk/
■CUP（キャンパス・ユビキタス・プロジェクト）に関するご質問は
業務システム問い合わせ窓口
電話：082-424-5609　内線：（東広島）84-5609
Mail：systemhelp@office.hiroshima-u.ac.jp

まとめ

- HINET2007へのSSO機能の追加
  - 学認によるゲスト利用者のネットワーク認証
- （学認全体として）今後考慮を要する点
  - SP接続情報の交換
    - 要求する属性の妥当性・方針
    - 接続を許可するIdPの登録方法
  - ゲスト利用者に対する無線LAN設定手順の周知方法
- 広島大学でのSSO利用状況
  - HINET2007ネットワーク認証
  - 電子ジャーナル
    - CiNii, CUP, Elsevier, Springer, Thomson Reuters, Ovid
- 今後の対応予定
  - 学内ポータルシステム
    - いろは（教職員用），もみじ（学生用）
  - 情報メディア教育研究センター関連システム
    - ホームページ（対応可能（Plone利用）），利用登録システム（対応済み），Active!Mail（もうすぐ対応？），WebCT6（モジュールに問題あり？情報求む！），ホスト登録システム（対応準備中）