

キャンパスネットワークへのSSO 機能の適用

西村 浩二

広島大学 情報メディア教育研究センター

学術認証フェデレーション及びSINETサービス説明会(広島)

2009年12月4日

本報告の内容

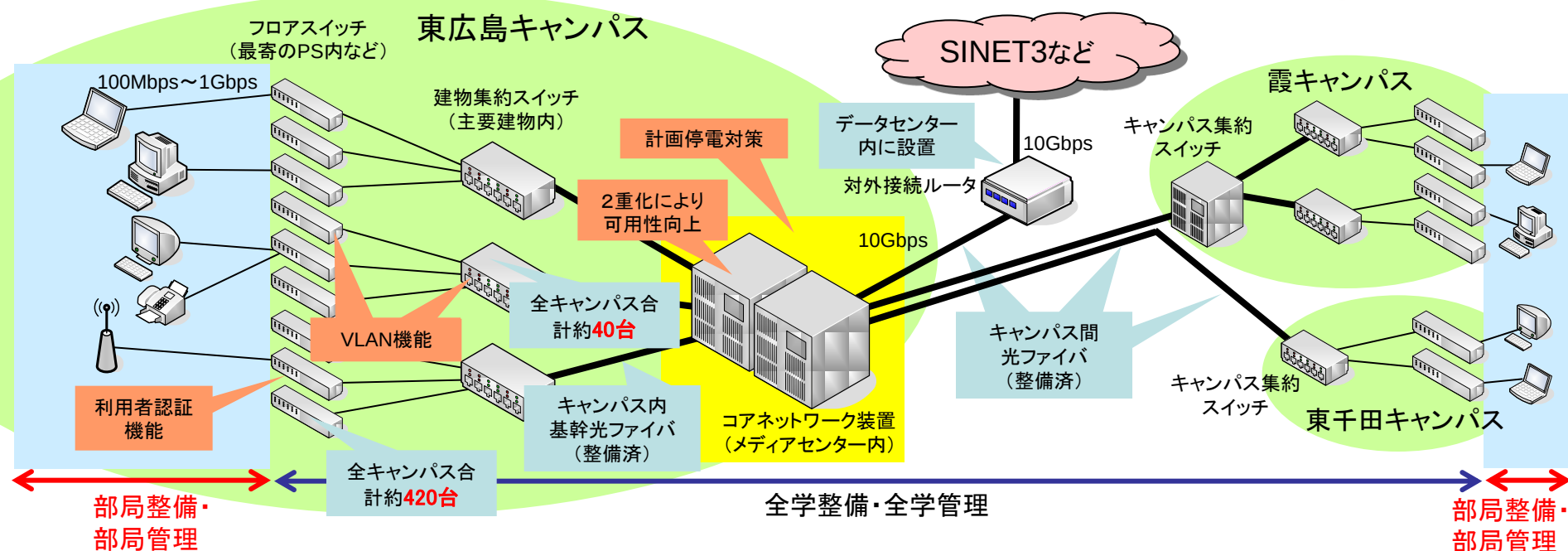
- ・ HINET2007の概要
 - － 全学規模でのセキュリティレベルの向上
- ・ HINET2007へのSSO機能の適用
 - － 増大する認証機会への対応
 - － セキュリティ上好ましくない無理な認証連携の解消

効能

- ・ 認証ネットワークの導入戦略
 - － エッジスイッチでの認証はセキュリティの水際対策
 - － 一手間(認証)の必要性への理解がネック
 - ・ 面倒くさい？それだけ？
 - － SSOとの組合せで利便性を損なうことなく導入が可能に

- ・ HINET2007
 - Hiroshima univ. Information NETwork system 2007
 - ・ 2007年度に整備計画された広島大学情報ネットワークシステム
 - 第4世代(HINET93→HINET95→HINET2001→HINET2007)
 - 全学規模でのセキュリティレベル向上を目的
 - ・ 利用者認証必須、IPアドレス単位の管理

HINET2007の概要

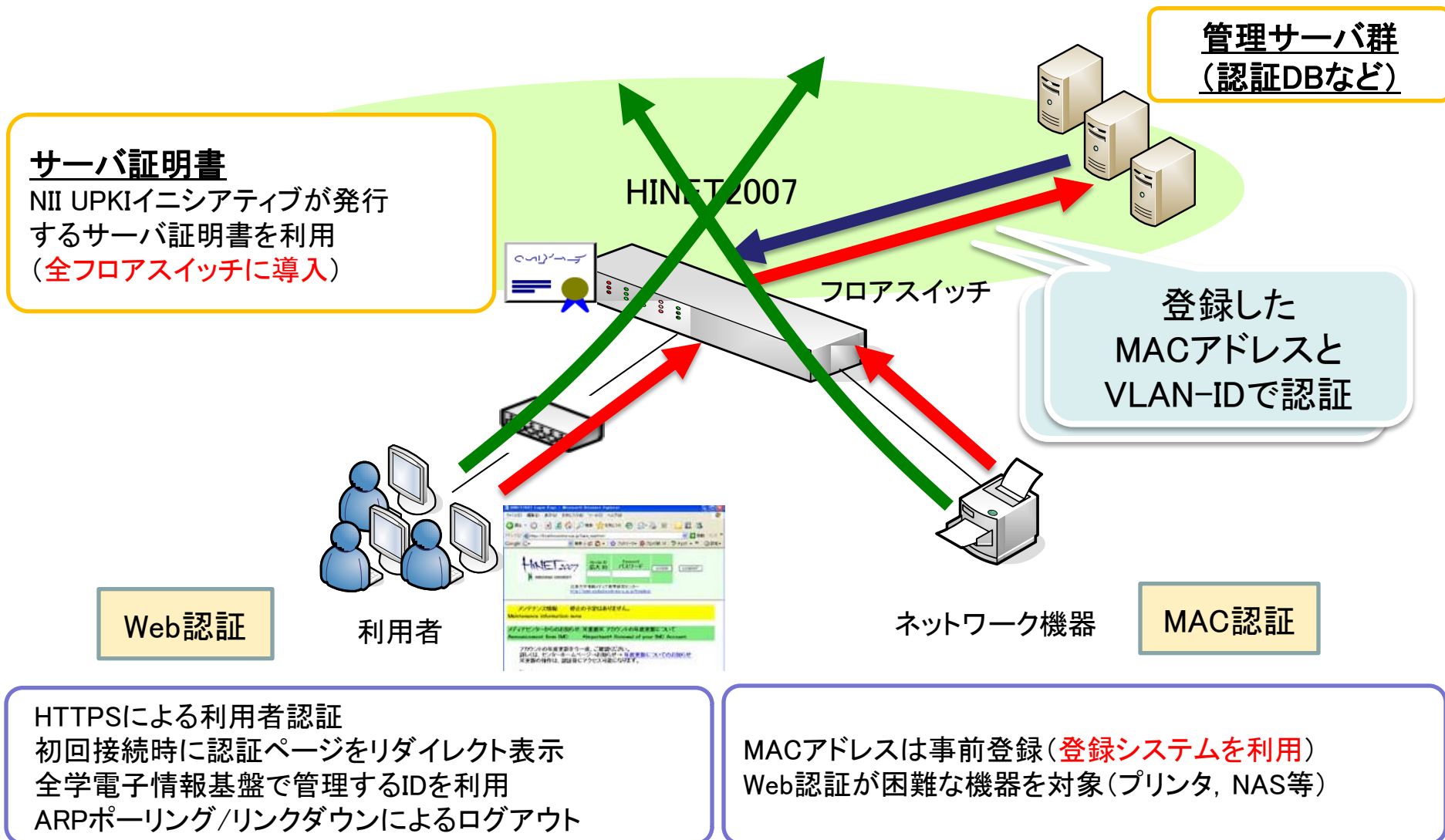


- ・2008年5月から本格移行開始、2009年3月末完全移行
- ・規模
 - － 主要3キャンパス(東広島、霞、東千田)、附属学校、小規模遠隔部局(東京, 福山, 尾道, 竹原, 呉, 宮島)
- ・教員約1,800人、職員約3,300人、学生15,000人
- ・認証スイッチ約460台(約14,000ポート)を全学に整備

HINET2007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

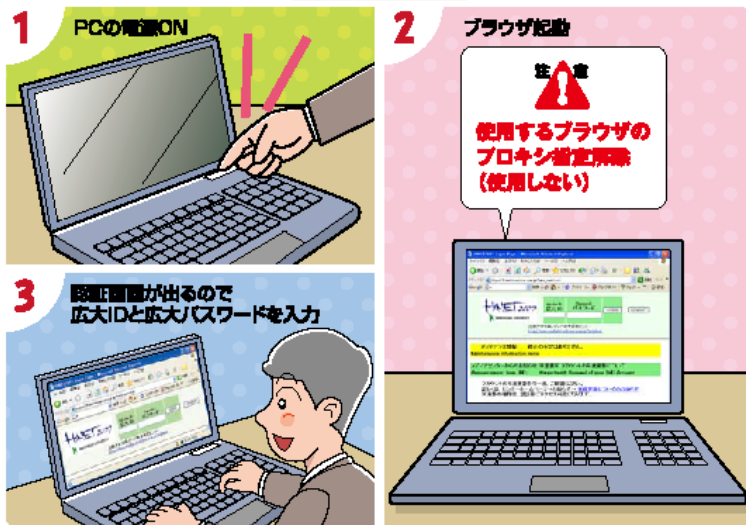
利用者認証の概要



HINET2007の使い方(配布物)

HINET2007の使い方

PCの場合



※ブラウザは、WWW画面の左側にHTTPによる接続を推奨するサーバを指定すること



注意
・研究室等に設置したルータ等が接続している場合は、利用者認証画面が出てきません。
・利用者の設定がある場合は事前にMACアドレス登録しておく必要があります。

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。

問い合わせ先: <http://www.media.hiroshima-u.ac.jp/helpdesk/>

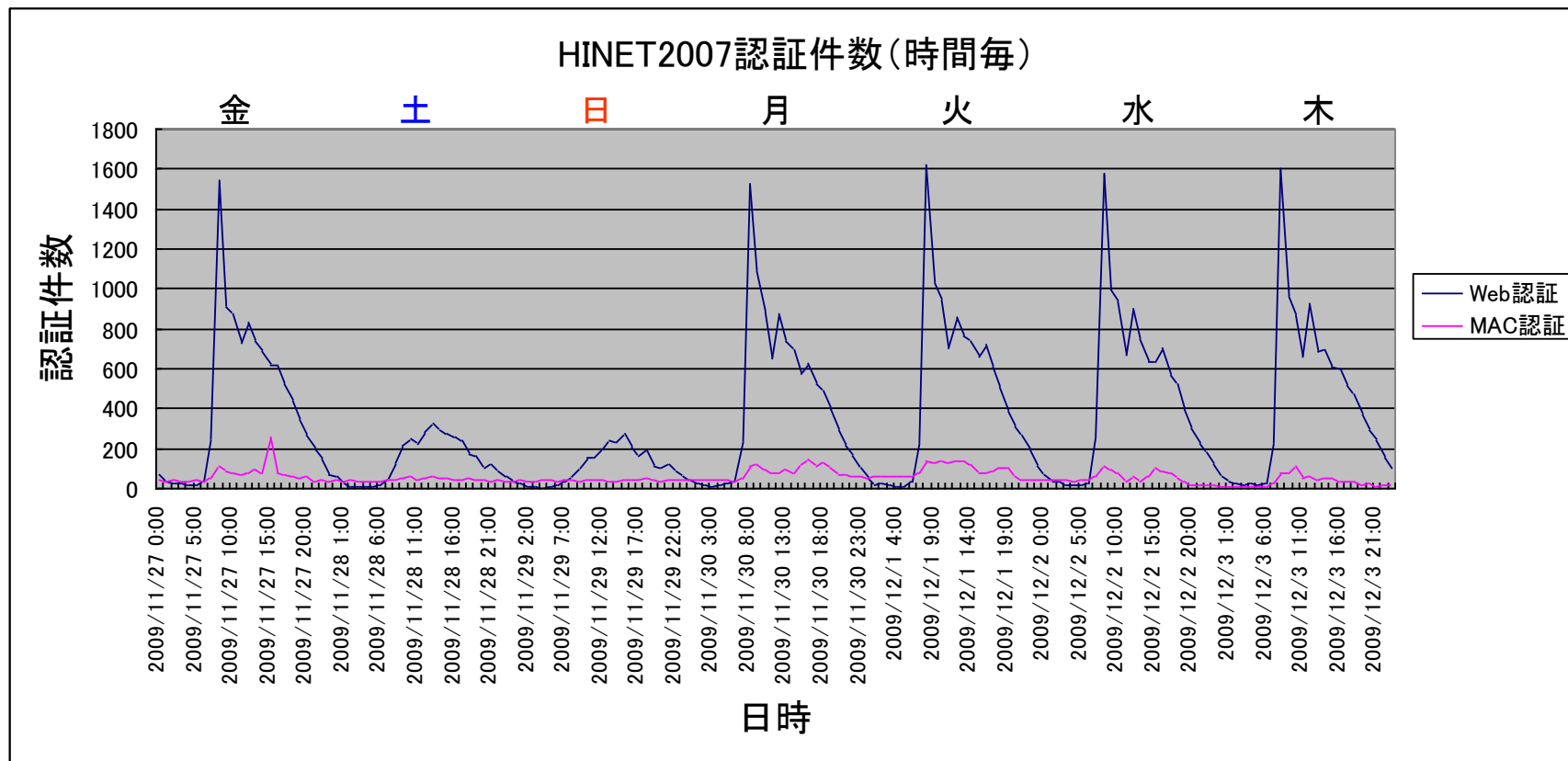
背景(つづき)

- ・ HINET2007
 - Hiroshima univ. Information NETwork system 2007
 - ・ 2007年度に整備計画された広島大学情報ネットワークシステム
 - 第4世代(HINET93→HINET95→HINET2001→HINET2007)
 - 全学規模でのセキュリティレベル向上を目的
 - ・ 利用者認証必須、IPアドレス単位の管理
- ・ 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

SSO対応の方針

- ・ HINET2007でのSSO機能の提供
 - － 増大する認証機会への対応
 - ・ Webサービスの利用にはネットワーク認証が必要（利用者の負担増）
 - － 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での認証連携

HINET2007認証件数(SSO利用機会)



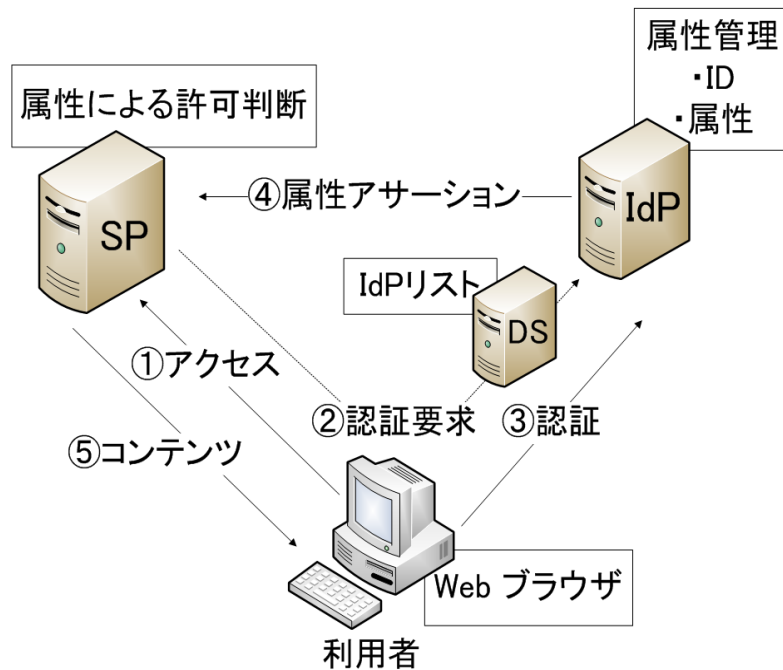
	2009-11-27	2009-11-28	2009-11-29	2009-11-30	2009-12-01	2009-12-02	2009-12-03
Web認証延べ件数	9,960	3,394	2,596	10,253	10,795	10,570	10,177
Web認証実数	5,544	1,976	1,573	5,734	5,837	5,780	5,678
MAC認証延べ件数	1,582	1,028	973	1,863	2,053	1,228	822
MAC認証実数	421	98	61	341	323	269	338

SSO対応の方針(つづき)

- ・ HINET2007でのSSO機能の提供
 - － 増大する認証機会への対応
 - ・ Webサービスの利用にはネットワーク認証が必要(利用者の負担増)
 - － 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での認証連携
- ・ SSO機能の実装方法
 - － 認証ゲートウェイへのSSO機能の実装
 - ・ SSO-Opengate(佐賀大学)
 - － 認証スイッチへのSSO機能の実装
 - ・ メモリ等のリソースに大きく制約を受けるため困難

→ 認証スイッチへの機能追加を必要としないSSO機能の実現

ShibbolethによるSSOの仕組み



- ① SPへアクセス
- ② IdPでの認証を指示
- ③ IdPで認証
(利用者へ認証チケットが提供される)
- ④ SPへ認証結果(属性)を送信
- ⑤ SPはサービス(コンテンツ)を提供

※チケットの提示で利用権限のあるSPを利用可能

認証とサービスの分離により
サービス提供者に提示する情報の適切な管理が可能

HINET2007へのSSO機能の適用



利用者

- ・ HINET2007はネットワークサービスのプロバイダ (HINET-SP)
- ・ 一度の認証操作で認証スイッチでの認証とIdPでの認証を同時に実施

認証連携

認証スイッチ

認証OK

認証サーバ

コンテンツ

Service

コンテンツ

Service

認証チケット

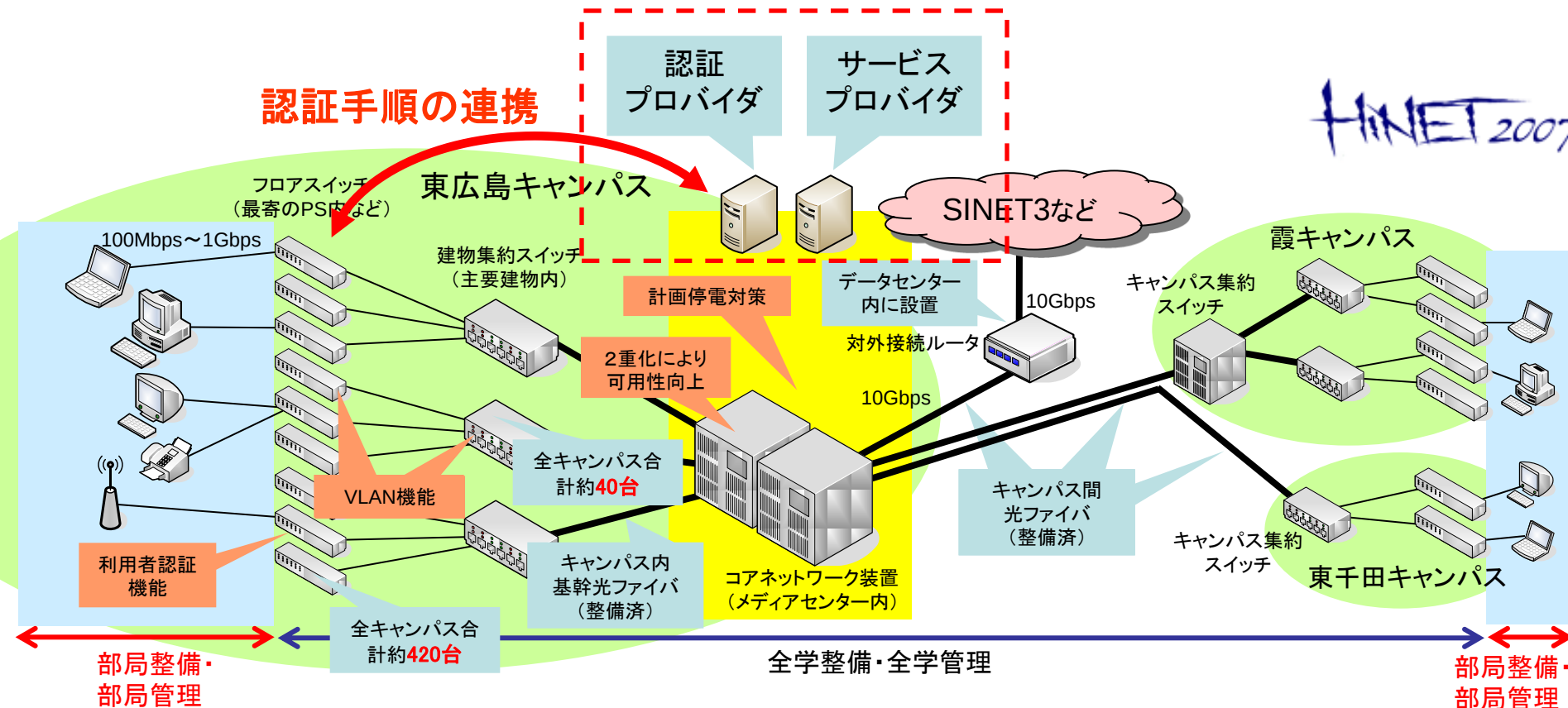
認証サーバ
(shibboleth IdP)

実装上の要件

- ・ ネットワーク認証は利用者端末から
 - MACアドレスで端末を、利用者IDで利用者を特定
- ・ SSOは利用者端末のWebブラウザから
 - IdPが発行した認証チケット(Cookie)をWebブラウザが受け取る
 - 認証チケットをサービスプロバイダに提示することでサービスが利用できる
- ・ 利用者が行う認証操作は一度だけ
- ・ 認証スイッチへの機能追加は不可

HINET2007へのSSO機能の追加

HINET2007

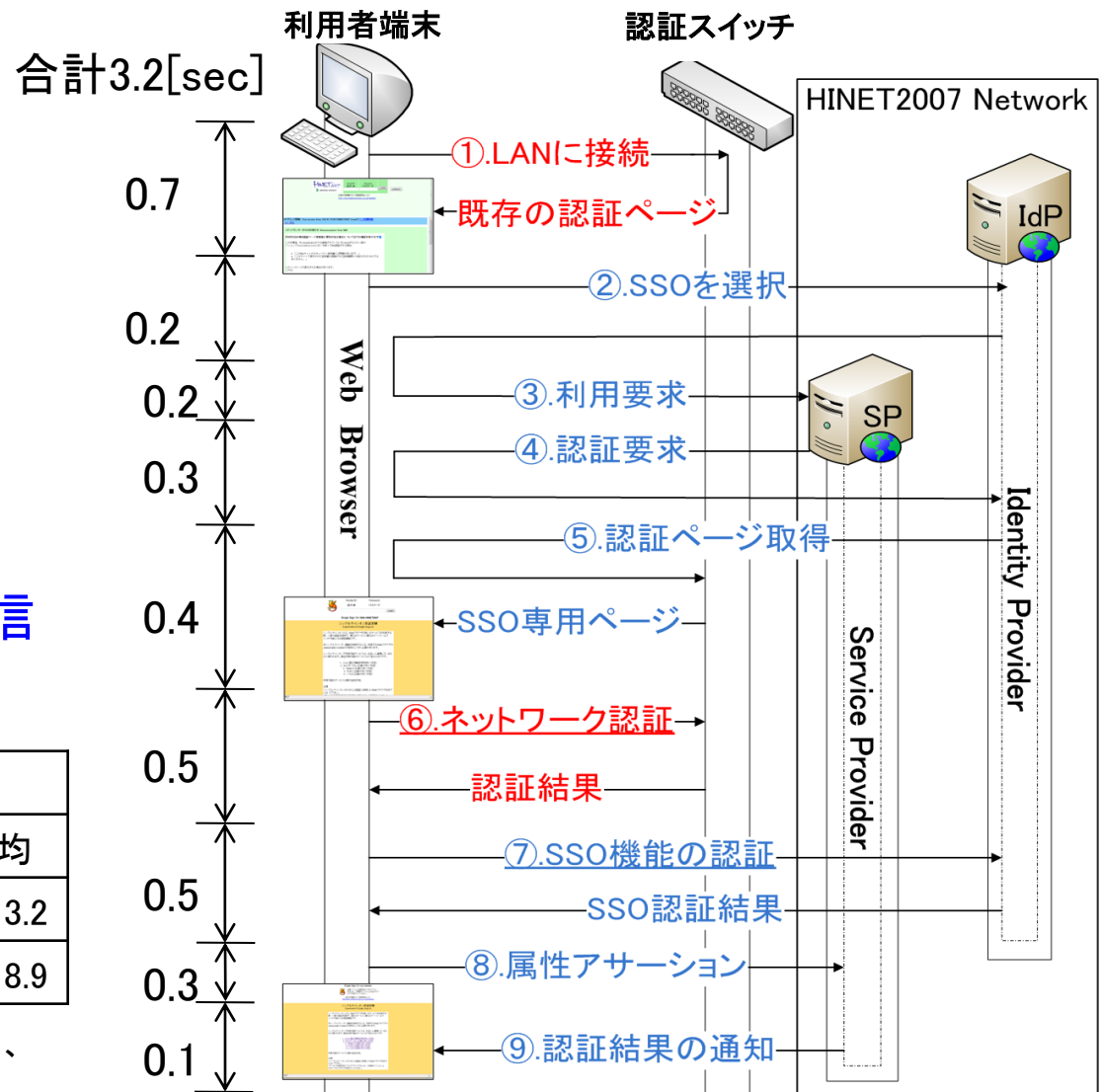


実装システムの動作

- ① LANに接続
- ② SSOを選択
- ③ 利用要求
- ④ 認証要求
- ⑤ 認証ページ取得
- ⑥ ネットワーク認証
- ⑦ SSO機能の認証
- ⑧ 属性アサーションの送信
- ⑨ 認証結果の通知

	SSOなし		SSOあり	
	最大	平均	最大	平均
1台	1.8	1.7	3.5	3.2
10台	8.8	6.3	11.3	8.9

※単位は[sec]。ただし、認証情報の入力時間、Webブラウザのレンダリング時間は含まない。



利用者インタフェース

① HINET2007 認証ページの表示

- 従来の認証方式を選択可能

② SSO専用ページへ移動

- SSOの説明
- 認証情報を入力

③ 認証失敗

- 構成員はネットワーク認証とSSOに同一の認証情報を使用
 - ・ ネットワーク認証に失敗
 - ・ ID／パスワードの間違い

④ 認証成功

- SSO可能な各サービスへのリンク

① HINET2007 認証ページ

SSOの選択



② SSO専用ページ

③ 認証失敗



NG

Link

SSOの説明

OK

④ 認証成功

利用可能サービスのリンク



まとめと今後の予定

- ・ HINET2007の概要
 - － 認証スイッチベースの大規模認証ネットワーク
 - ・ 460台の認証スイッチにサーバ証明書をインストール
 - － Web/MACアドレス認証の利用状況
- ・ HINET2007へのSSO機能の適用
 - － 認証機会増大への対応
 - － セキュリティ上好ましくない認証連携の解消
- ・ 試験運用開始
 - － 実運用に向けた問題点の洗い出し
- ・ SSO機能の全学展開
 - － 運用フェデレーションへの参加
 - － 学内Webサービス(電子ジャーナル、WebCT)のSSO化
- ・ 非構成員によるHINET2007のゲスト利用
 - － 他組織の認証システムとの連携手順の検討