# 国立情報学研究所　情報処理軽井沢セミナー　研修報告
# 平成20年度テーマ：認証技術を知る　　～学内認証局の構築～

天理大学　情報センター

前芝　志保

## １．セミナー課題発表タイトル

「Single Sign-On 認証システム構築」

## ２．セミナー課題発表内容の概要

別添ファイルをご参照願います。

## ３．セミナーで学んだ技術及び知識

Ⅰ.　学内認証局構築の構築・運用にむけて　～概要および基礎知識～

1) 概要：認証技術の活用事例

- 大学間認証連携（UPKI）
- 認証局構築支援
- オープンドメインサーバ証明書発行
- 無線 LAN ローミング

2) PKI による認証基盤構築のための基礎知識

- 信頼性の確保
- 証明書の概要
- 認証局の運用

Ⅱ. UPKI 共通仕様の活用について　～CP/CPS ガイドライン詳細解説～

Ⅲ. 認証局構築実習

- NAREGI-CA のインストール
- 証明書の発行
- 証明書の利用（シングルサインオン）
- 証明書の検証

Ⅳ. 認証局を実際に運用するには

Ⅴ. グリッドの認証と CSI の活用

## ４．セミナーの成果

- 認証局構築の実習や認証局を実際に運用するための講義を受けることにより、所属機関での学内認証局構築に向けての指針を得ることができたと思う。
- PKI CP/CPS ガイドラインについてのモデルを示して頂けたことで、所属機関でのガイドライン作成について大変参考になったと思う。
- SSL/TLS 認証の仕組みなどを分かりやすく講義して頂けたことにより、理解が深まったと思う。

## ５．セミナー参加にあたり、参考になった URL と内容

「暗号と認証」　日経 BP 社

## ６．事前準備として知っておいた方が良かったと思われること

PKI の基本となる鍵の作成方法から証明書の取得、サーバへのインストールなど一連の流れは所属機関にて担当していたため理解していたが、所属機関の問題点について事前にもっと掘り下げてから参加した方がより発想が広がったように思われる。

## ７．セミナーの感想

- PKI の講義については、普段の業務では定型的に行っている部分があるため、基礎から分かりやすく説明して頂き、整理ができたように思う。
- UPKI については、今まで利用したことがなかったため、今後所属機関でどのように活かすかを考える機会となり良かったと思う。

## ８．　その他

- 集中して学ぶことができるとてもよい環境であったと思います。
- 他大学での導入済機器についての評価や苦労話など、かなり詳しく情報交換させて頂くことができ、大変有益であったと思います。
- セミナー期間中、快適に過ごせるようご配慮頂いた国立情報学研究所のスタッフの皆様に感謝致します。

# Single Sign-On 認証システム構築

国立情報学研究所　情報処理軽井沢セミナー
＝認証技術を知る-学内認証局の構築-＝

於軽井沢国際高等セミナーハウス
2008年9月5日

天理大学　情報センター
前芝　志保

# はじめに　（Single Sign-On導入検討の背景）

## H20以前の本学の問題点

複数のシステムが時期を違えて導入されたため、認証は2つのシステムでのみ共通で他は別々の内部認証システムを持っていた。またアカウント・パスワードもそれぞればらばらであった。そのため…

| 学生の視点 | 教職員の視点 |
| --- | --- |
| 多数あるサービスのパスワードを覚えておくのは大変 | 学生のパスワード忘れが多い<br>サービス数も多数になるため、パスワード忘れ・再発行対応が煩雑 |
| 複数のサービスを利用するときにも覚えやすい脆弱なパスワード/全て同じパスワードを設定しがち | 個人情報が掲載されたサービスになるため、複数のどのサービスに対しても強固なパスワード設定を望むが困難 |
| パスワードが一部共通・他は初期値のみ共通し変更後はばらばら→仕組みが分かりにくい | パスワードが一部共通・他は初期値のみ共通し変更後はばらばら→学生に説明しにくい |
| 多数あるサービスごとにユーザアカウント・パスワードを入力する必要がある | 多数あるサービスのユーザ情報のメンテナンス箇所を統合させたいがばらばらである |

# SSO導入スケジュール

## 2ステップに分けての導入を検討

一度にシングルサインオン（SSO）を実現することは難しいため、
第一段階としてアカウントの統合、第二段階としてSSO導入を検討

| | 第１ステップ | | 第2ステップ | |
|---|---|---|---|---|
| 導入の検討<br>平成18年～ | アカウント統合準備<br>平成19年～ | 第1次運用開始<br>平成20年～ | SSO導入準備<br>平成21年～ | 第2次運用開始<br>平成22年（予定） |
| ・現在の学生Webサービスの分析<br>・今後の仕様検討 | ・全てのサービスで学籍番号をアカウントとして統合<br>・ADを中心とした各種サービスのLDAP認証への変更作業<br>(上記の作業内容の詳細は右記) | ・第2ステップの仕様検討 | ・システム選定詳細検討<br>・各プログラムのカスタマイズ<br>・必要機器の見積 | ・導入後の運用に関する担当者への教育やフォロー |

※ **S**ingle **S**ign-**O**n （SSO）とは

たった1回のユーザ認証で、異なるシステムやアプリケーションに一度にアクセスできるシステムのことを「シングルサインオン(Single Sign-On＝SSO)」と言う。

## ■第1ステップでの作業内容

● WebMailアカウントの変更
‥OSの制限で頭2文字を英字にして利用
→Webメールサーバのリプレイス
→学籍番号をアカウント名へ利用可能に
→旧アドレスのメールは新アドレスへ転送することで対応

● WebMailのバージョンアップ
‥旧バージョンではLDAPに対応していないため対応している最新Verへ変更

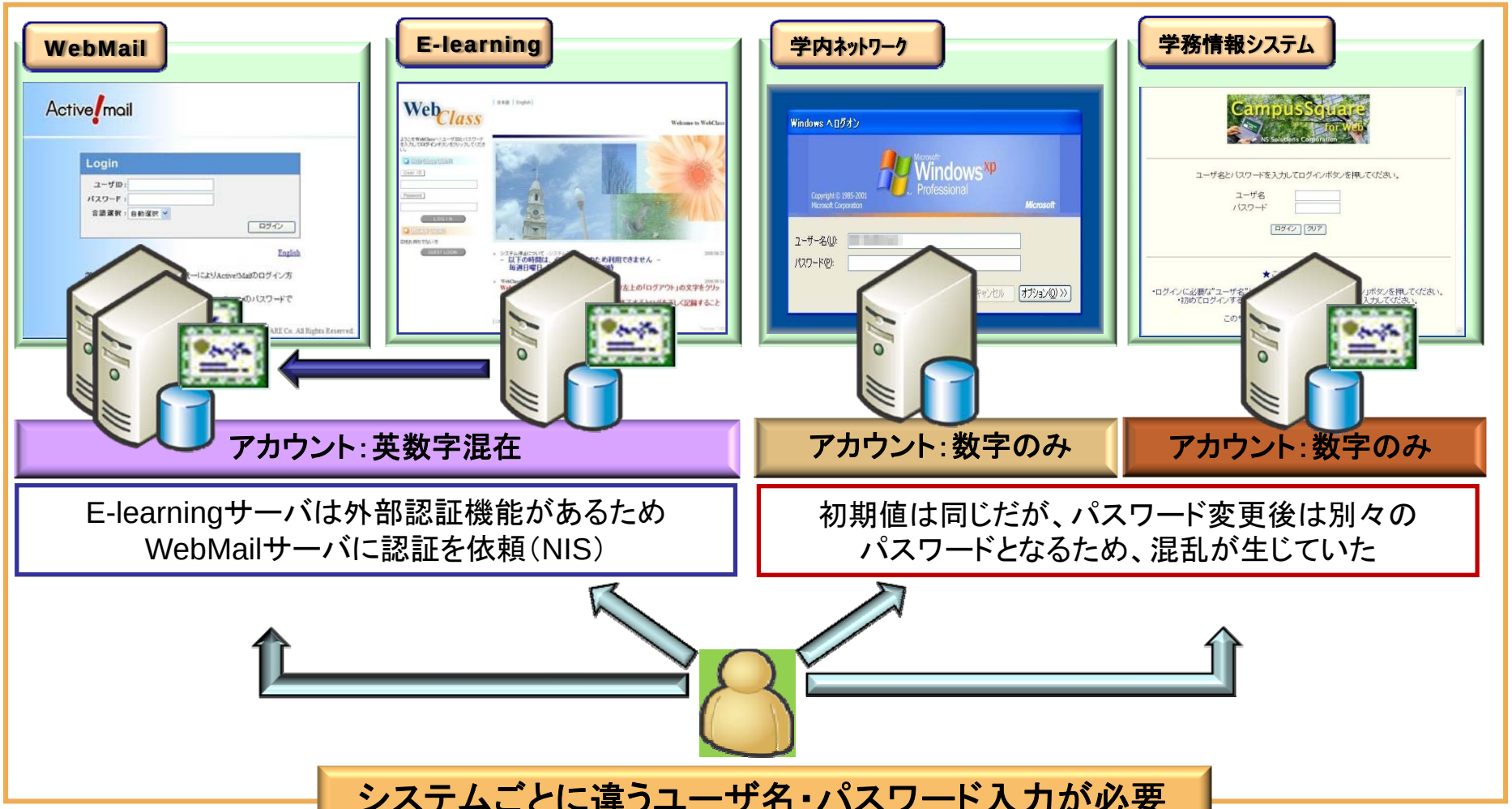
● E-learningサービスの外部認証先を変更
‥NISでWebMailサーバでの認証
→LDAPでADサーバでの認証

● 学務情報システムのカスタマイズ
‥標準では外部認証機能を持っていない
→カスタマイズで対応。また、LDAPサーバのパスワード変更画面も作成
→サービス毎にあったパスワード変更画面を一つの画面でのみ変更可能に
→シンプルで分かりやすくなった

● ADサーバで証明書を発行し、学務情報システムサーバへインストール
→ADの仕様でLDAP経由でパスワード変更するにはLDAPSで接続する必要があるため　　などなど…

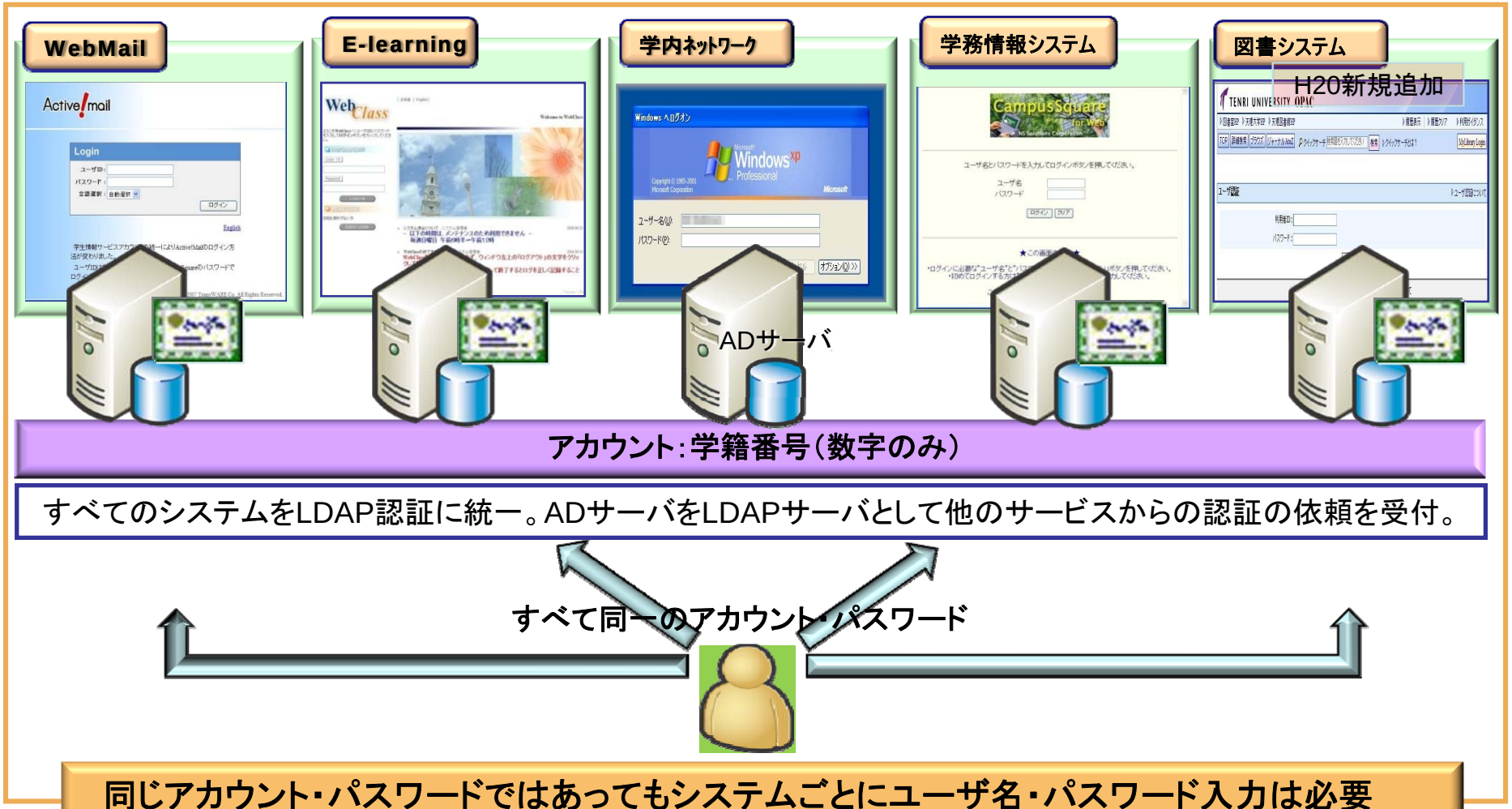
# 学生用システムの状況図①（第1ステップ以前）

それぞれのシステムが時期を違えて　導入されたため、2つのシステムのみ共通にNISで認証し、他は別々の内部認証システムを持っている。またアカウント・パスワードもばらばら。証明書もサーバ毎に必要。



# 学生用システムの状況図②（第1ステップ）

パスワードの変更画面は学務情報システムのメニューからのみ変更可能としたため、シンプルになった。ただし、システムごとにユーザ名・パスワード入力は必要。また証明書も各サーバ毎に必要。




**同じアカウント・パスワードではあってもシステムごとにユーザ名・パスワード入力は必要**

# 現在（第1ステップ段階）の学生用システムの問題を解決し、メリットを生むには…　（第2ステップへの展望）

（現在の問題点）
多数あるサービスごとにユーザアカウント・パスワードを入力するのは手間がかかる。

→セキュアな環境を実現し、かつ一度のユーザアカウント・パスワード入力だけで学内の様々なアプリケーションにアクセス可能にしたい！！

⇒ **シングルサインオンの導入を検討**

→費用面でのメリットはあるか？
→導入に際する問題点はないか？
→本学に適したものは何か？（ JOSSO？ Open SSO？…何が適当？）

# SSO実装のためのソフトウェア比較

Webアプリケーションにシングル・サインオン機能を導入するためのソフトウェア比較の参考として
まず、一般的に何が推奨・利用されているかを検討

| | 費用面 | 利用状況 | 備考 | 推奨度 |
|---|---|---|---|---|
| OpenSSO | ◎<br>（オープンソース） | ○<br>（たまに利用される） | ・https://opensso.dev.java.net/<br>・SUNが主導するオープンソース<br>・製品（Sun Java System Access Manager）のSSO部分を公開している ・SSOのコアのみ | 6 |
| JOSSO | ◎<br>（オープンソース） | ×<br>（利用されていない） | ・http://www.josso.org/<br>・The BSD License の元で公開 | 2 |
| CAS | ◎<br>（オープンソース） | ◎<br>（よく利用されている） | ・http://www.ja-sig.org/products/cas/<br>・多くの利用実績（大学が多い）<br>・名古屋大学で拡張したCAS-2がある | 9 |
| opentrust-pam | ◎<br>（オープンソース） | △<br>（あまり利用されていない） | ・http://opentrust-pam.sourceforge.net/<br>・OpenSUSE で利用可能<br>・日本語対応は無し。そもそもフランス語が多い | 2 |

日本OSS推進フォーラム サーバ部会セキュリティTF,セキュリティ関連OSSの成熟度評価Ver1.0 平成20年3月 を一部引用

**⇒ 一番利用実績が多いCASの導入を本学でも検討**

# What is CAS? ＆ Profit of SSO using CAS（1）

## ---CAS導入に向けての詳細な検討---

### CAS(Central Authentication Service)とは？その利点とは？(導入面)

- Web Applicationに対するシングルサインオン(SSO)を構築
- Cookie,http direction,javaScriptなどの標準的なWeb技術だけを用いて実装が可能。また、処理が極めて軽くインストールおよび設定が容易
- ユーザインターフェイスとしてWebブラウザを利用
- 通信の暗号化にはSSL(https)を利用している
- 認証DBとは独立であり、DBの形式に依存しない
- 認証DBの安全性が飛躍的に向上する
- Web ApplicationをCAS対応にすることが容易
- 本学においてSSO導入の一番の障壁になると予測されるシステムである学務システムと同じシステムを導入している熊本大学が既にCASでSSO構築済み

# What is CAS? ＆ Profit of SSO using CAS（2）

## ---CAS導入に向けての詳細な検討---

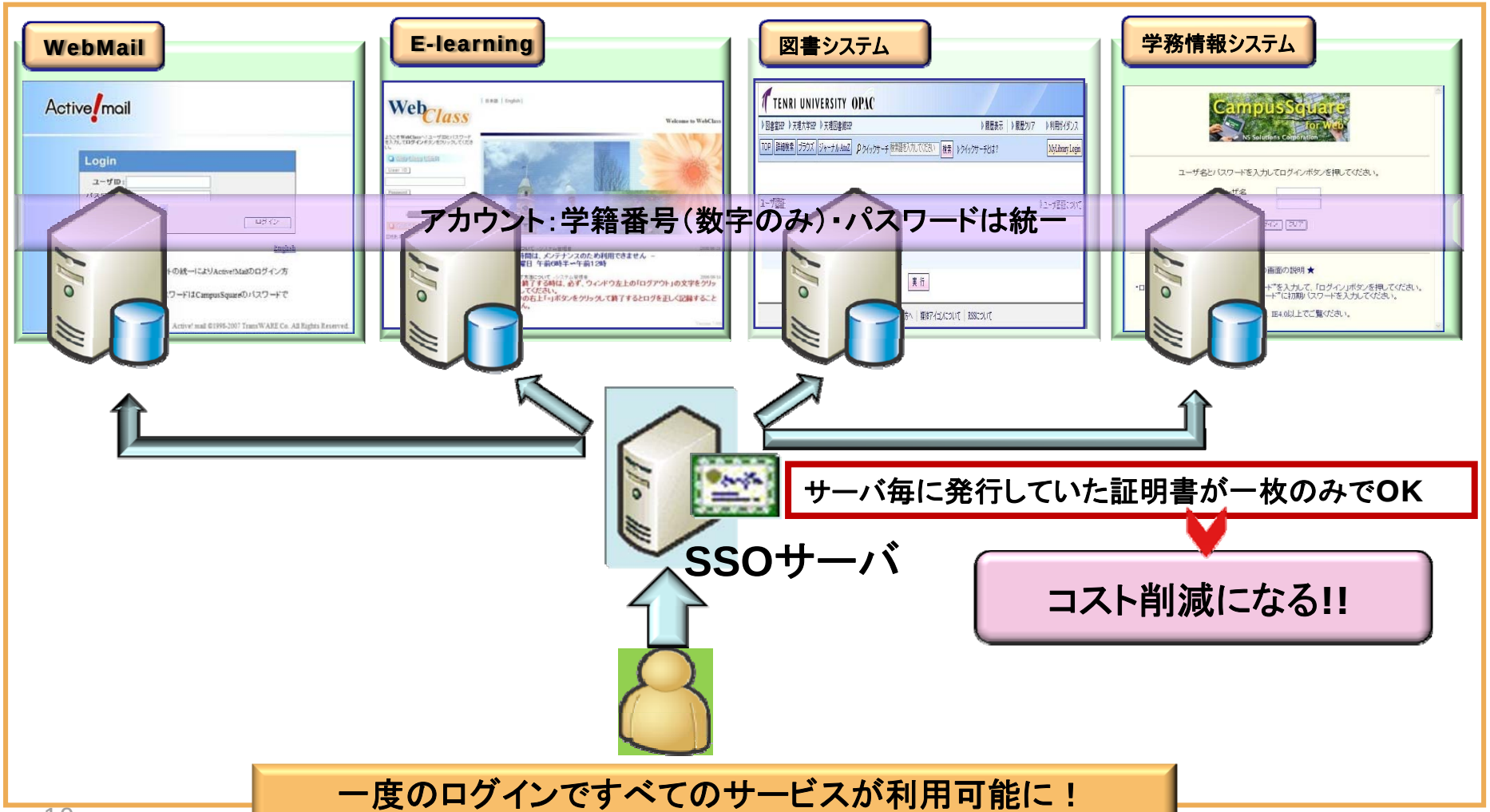
### CAS(Central Authentication Service)とは？その利点とは？（費用面）

- Yale University,JA-SIGによってオープンソースとして開発されている
  **→コストがかからない！！**

- 認証情報がユーザ・CASサーバ間で通信するため、暗号するべきなのはCASサーバとユーザの間になる
  →現在本学では学生用システムの4つのサービス毎に証明書を発行している
  （大学全体では7つ：年間50万弱。また各サーバの証明書を申請し、セットする手間が7回かかる）
  **→CASサーバにのみサーバ証明書が必要**
  **→4枚分の証明書の費用が1枚分の費用に！！**
  **証明書申請・セットの手間も1回（年間）のみに！！**
  **→コストの削減につながる！！**

# 今後の展望図 （第3ステップへの展望）

一度のアカウント・パスワード入力だけで、他のすべてのシステムを利用可能としたい。また各サーバごとに必要であった証明書も一枚にまとめてコスト削減をはかりたい。



# 今後予想される問題点は？　＆　その対応は？

## 予想される問題

現在認証DBは稼働中のLDAPを利用

→今後認証DBの形式を変更する場合は？

教職員利用システムへ

シングルサインオンを導入する場合は？

## 予想される問題への対応

対応1）CASの認証DBへのアクセスハンドラの置き換えでOK（各システムの「認証モジュール」の切り替えを行う必要はない）

対応2）対応1でだめな場合はCASがアクセスする認証DBを切り替える、または認証DBへのアクセス方法を切り替えればアプリケーション側の本質的な変更はない

学生利用システムは全てWebアプリケーションであるためCAS認証で実現可能だが教職員利用システムには一部Webアプリケーション以外のものが含まれている
→Webアプリケーションに対してはCAS認証を利用し、それ以外のサービスに対しては既存利用の認証方法で提供する

# [参考文献]

[1]名古屋大学のユーザ認証基盤の現状紹介
http://www.ssken.gr.jp/lib/nl/2005/stg/2/02_hirano.pdf

[2]梶田 将司, 内藤 久資, 小尻 智子, 平野 靖, 間瀬 健二 :
CASによるセキュアな全学認証基盤の構築, 情報処理学会DSM研究会研究報告,
2005-39, pp.35-40, 2005
http://www2.itc.nagoya-u.ac.jp
/pub/pdf/pdf/vol04_03/179_187service02.pdf

このPPTはMicrosoftのテンプレートを使用し作成いたしました