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

Background(平成20年度以前)

複数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で認証し、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. . .

- 学生の視点では

1)多数あるサービスのパスワードを覚えておくのは大変である

2)忘れないように複数のサービスを利用するときにも全て同じパスワードを用い、覚えやすい脆弱なパスワードになりがちである

3) 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手間がかかる

- 教職員の視点では

1)学生がパスワードを忘れる場合が多く、再発行の際に職員の手間がかかる

2)一部共通のアカウント・パスワードを利用しているが、その他は分かれている等統一性がないため学生に説明しにくい

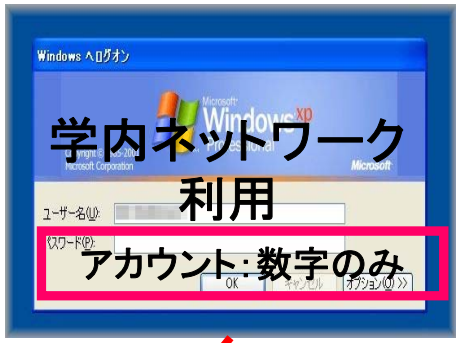
3)成績情報等を見ることができる学務情報システムやE-learningシステムを学外からでもAccess可能にしているが、個人情報が掲載されているため厳重なパスワード管理、強固なパスワードの設定をお願いしているにもかかわらずパスワードが記載されたアカウント通知書の置き忘れ、脆弱なパスワードの設定がされていることが多い

4)授業が始まってからパスワードを忘れたので対処して欲しい、という依頼の際、パスワードの処理担当者が席を外していることがあり、常に迅速な対応をすることは難しい

本学学生利用システムの状況（平成20年度以前）

アカウント：英数字混在

アカウント：英数字混在

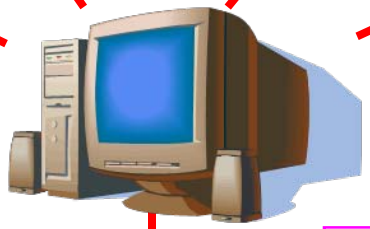


アカウント：数字のみ

アカウント：数字のみ

システム毎に違うユーザ名・パスワード入力が必要

E-learningサーバは外部認証機能があるためWebMailサーバに認証を依頼（NIS）



PC

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の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。

Background(平成20年度)

すべてのシステムでアカウント・パスワードを同じにした。

- 学生の視点では

  1)1つのパスワードを覚えるのみでいいため、パスワードを忘れにくくなった

  2)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

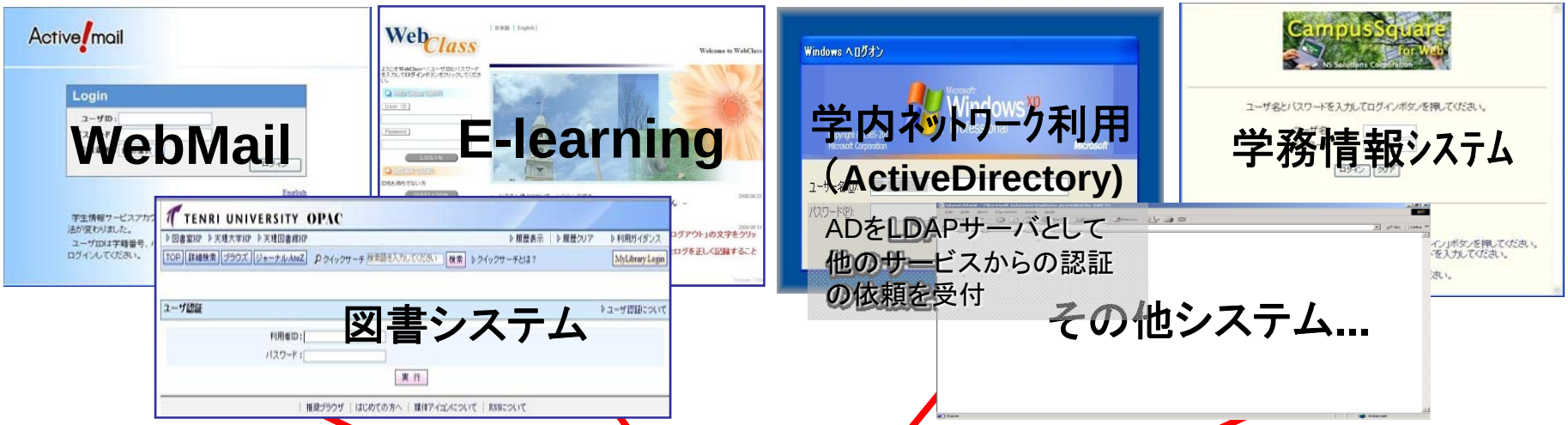
  3)同じアカウント・パスワードではあっても多数あるサービスごとにユーザアカウント・パスワードを入力する手間がかかる

- 教職員の視点では

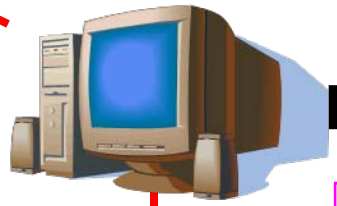
  1)パスワードの変更画面は学務情報システムのメニューからのみ変更可能としたため、シンプルになり説明しやすくなった

  2)パスワード忘れの数が格段に減った。

本学学生利用システムの状況（平成20年度）



アカウント・パスワードを統一！！ただしシステム毎にユーザ名・パスワード入力が必要



PC

LDAP認証に統一。学務情報システムサーバにLDAPサーバのパスワード変更機能を追加し、学生は学務情報システムのメニューでのみパスワード変更を行うよう変更したためシンプルでわかりやすくなった。

シングルサインオン実現へ向けての現時点での問題点(今後の展望)

同じアカウント・パスワードではあっても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手間がかかる

→シングルサインオンを導入したい！！

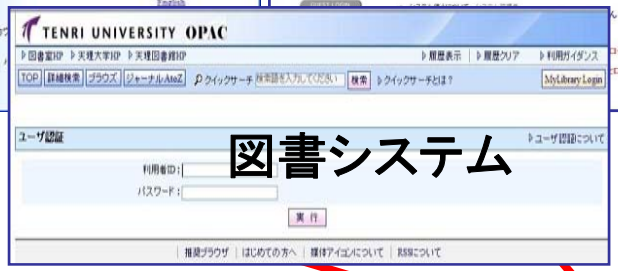
→費用は？

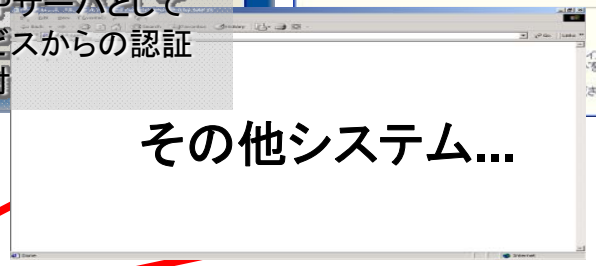
→導入に際する問題点は？

→本学に導入するに適したものは何？

現在の本学学生利用システムの現状（今後の展望）

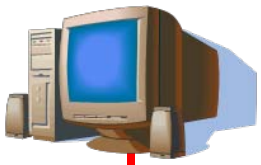
ADをLDAPサーバとして
他のサービスからの認証
依頼を受付





シングルサインオン（一度のログインですべてのサービスの利用が可能に！）

CAS（SSOサーバ）



そのためには...

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

- CAS(Central Authentication Service)とは？その利点とは？
  - 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
  - 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(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
    →コストの削減につながる！！
  - 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
    →CASサーバにのみサーバ証明書が必要
    →現在本学では各サービスに証明書を発行している(年間50万弱)
    →コストの削減につながる！！

今後予想される問題点は？　＆　その対応は？

- 認証DBは現在稼働中のLDAPを利用

  →CASを利用していれば、今後認証DBの形式を変更することがあっても各システムの「認証モジュール」の切り替えを行う必要はなく、CASの認証DBへのアクセスハンドラの置き換えでOK

  →それでもだめな場合は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

- 現在は明確な情報システム利用者の管理規定、運用規定がない。

  (例)いつ利用者の登録作業をするのか。

  どの範囲の利用者までを登録するのか、等

  →現在はそのシステムを主に利用する部署の所属長が判断

  →基準があいまい

  →明確な規定を作成する必要がある

まとめ

（現在）すべてのサービスのアカウントとパスワードが同じになった

（今後）CASを導入し、シングルサインオンの実現に向けて進める

終わり

天理大学　情報センター　前芝　志保