平成１9年度軽井沢セミナーレポート

福岡歯科大学　情報図書館課　秋吉　慎仁郎

１．セミナー最終日に発表した課題のタイトル

「学生システムの認証統合及び PKI 導入検討について」

２．１の概要

別添ファイルをご参照ください。

３．セミナーで学んだ技術及び知識

(1)「PKI の基礎」

PKI の基礎知識の再確認ができました。

(2)「UPKI 概要」

大学間連携のための UPKI についての、前提知識、概論（プロジェクト・UPKI の三層アーキテクチャ）及びサーバ証明書の発行・導入・評価研究プロジェクト等についての講義でした。所属する大学でのアカウントを使用して他大学のネットワーク及びサービスに PKI を使用して安全にアクセス可能とすることについて、必要な技術についての解説及び SINET 及び旧制帝大の基盤情報センター等で連携して進めている UPKI プロジェクトについての解説がありました。

(3)「shibboleth の利用及び最新動向」

Shibboleth とは、大学が ID と属性を管理して、SP がこれを使用してシングルサイトオンを可能とするソフトウェアーの講義及び実習でした。

この講義と実習を通じて Federation(属性交換の相互運用に合意した IdP や SP の集合)、SAML(認証情報を安全に交換するための XLM 仕様）及び Grid(プロジェクト内で ID 及び属性を管理せずに Federation と連携することで、IdP による ID 及び属性でログイン可能とする)等の技術について知ることができた。さらに、今後の動向についても知ることができた。

(4)「グリッドでの認証技術の利用」

グリッド利用のための認証（GSI(PKI、X.509 証明書ベースの認証方式)、TLS(TLS/SSL の相互認証プロキシ証明書で認証)やグリッド用認証局の運用についての講義がありました。

４．セミナーの成果

PKI は、クレジットカード等を使用して通信をする時（SSL 通信）には、**エンティティ認証・メッセージ認証**は、使用者のパソコン上のブラウザーとサーバー上ではおこなわれている事ですが、それを他の人に技術的に説明する事や実際にどのように業務に入れてい

くが考える事や運用していく事は私にとっては困難な事と思っていましたが、今回のセミナーを通じ技術的な知識や業務にどのように適用していくかの過程の指針のようなものがわかりました。

とくに、PKI は、難しいがその基礎となる知識がないから難しいのであり、基礎となる知識の積み重ねがあれば PKI は、難しくないと講師の方からお教えいただきましたが、他の情報技術にもそれがあてはまると実感しました。

５．セミナーの事前、事後において、参考になった URL とその簡単な内容紹介

下記の書籍を事前に読んでおきました。

改訂 PKI ハンドブック　ソフトリサーチセンター（ISBN4-88383-205-3）

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

暗号技術と PKI 技術の基礎を知っていたほうが良いと思います。専門用語が講義中にでるのでその知識はあったほうが良いと思います。

７．セミナーの感想

今回のセミナーは、国立情報学研究所の客員教授及び特任準教授の先生から８名の受講者に対してのセミナーであり、少人数で質疑しやすく、かなり興味深い話を聞くことができ、知識や技術の向上に大いに役にたちました。それだけでなく、他大学の情報担当の教職員との交流をもてた事は非常に貴重な体験になりまた。

8. 感想その他

大変有意義なセミナーでした。セミナーを快適に過ごせるように御配慮いただきました、SINET 基盤企画課の樋口様及び夏目様には、に御礼申し上げます。

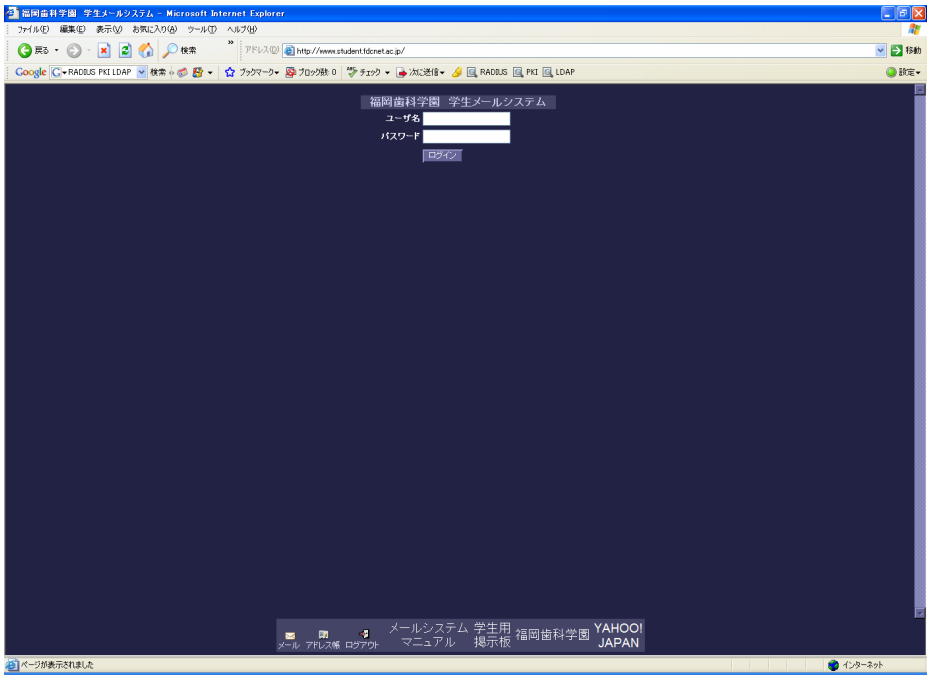
以　上

学生システムの認証統合及びPKI導入検討について

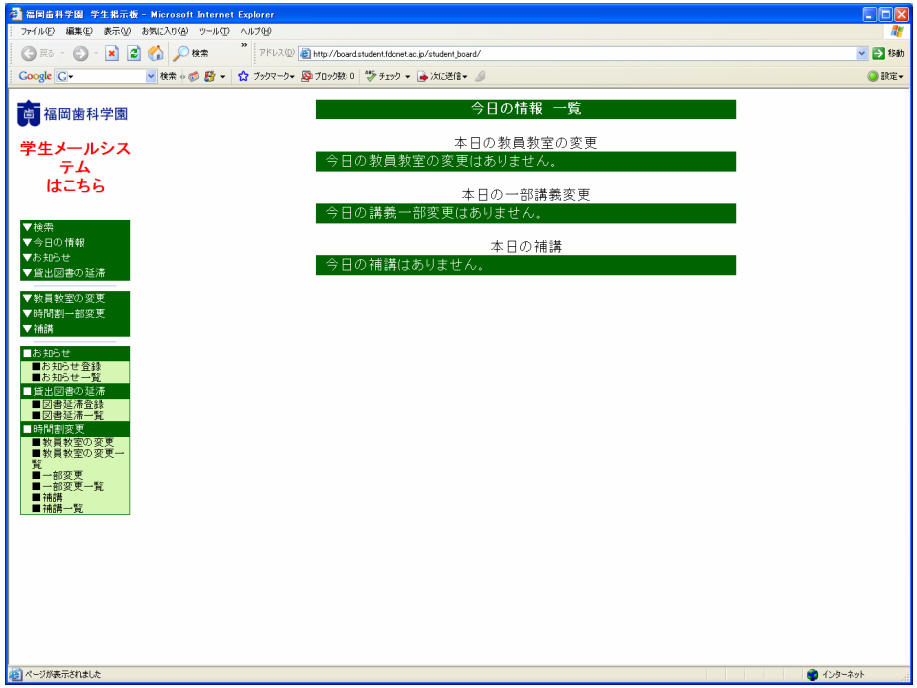
福岡歯科大学　情報図書館課
秋吉　慎仁郎

本学の学生システム

メールシステム



掲示板システム

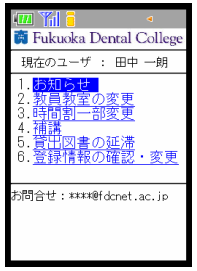


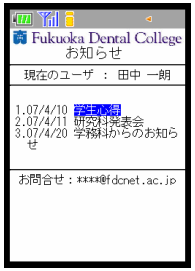
Webシステム

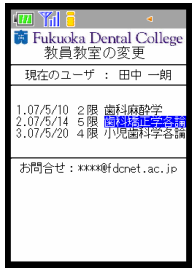
本学の学生システム

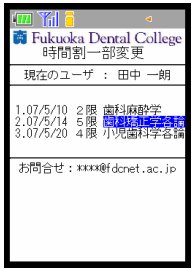
掲示板システム

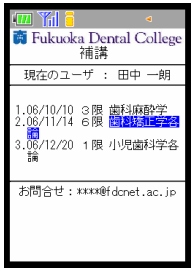
（携帯閲覧画面）

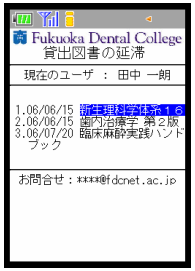


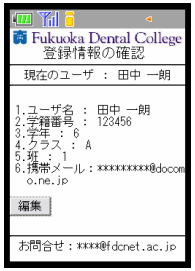


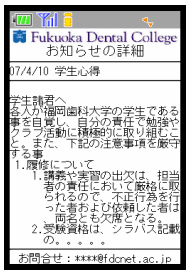


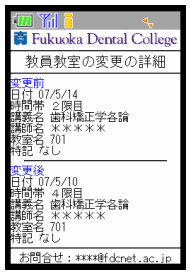


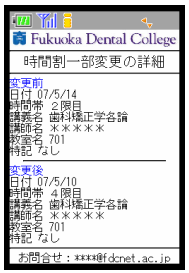


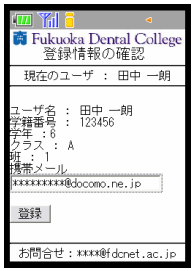












学生システムの認証統合及びPKI導入検討について（経緯）

① パスワードを忘れる場合が多い
② 脆弱なパスワード運用になりがち

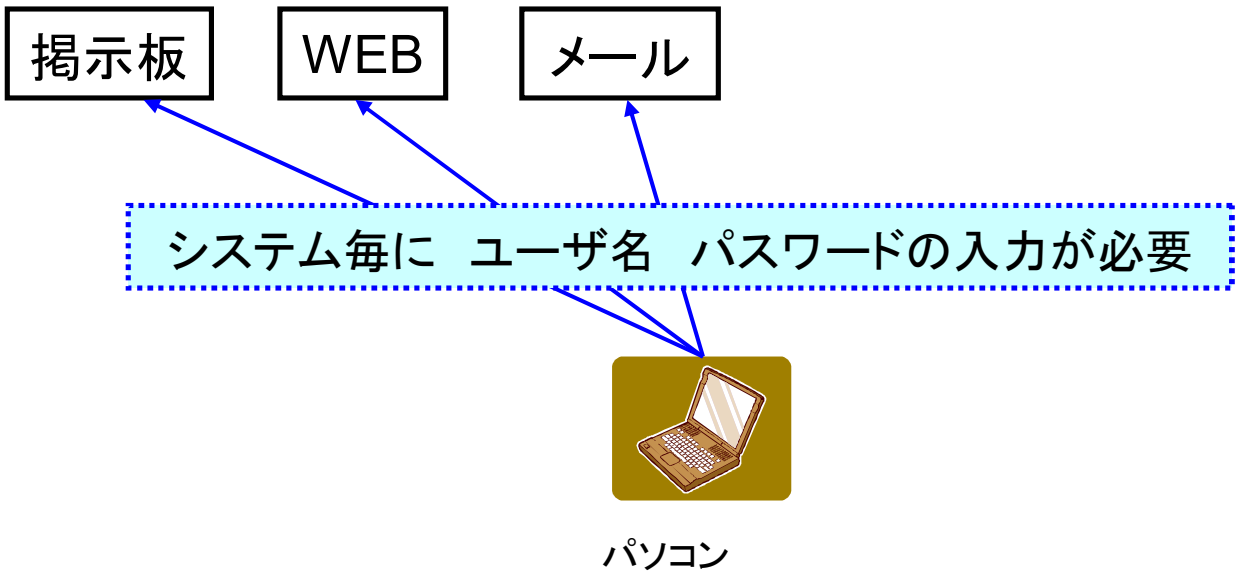
- 学生の立場から
  ・サービス毎にユーザ名とパスワードを入力するのは面倒
  ・サービス毎に覚えておくのは大変
  ・サービス毎に強固なパスワード管理は困難

- 教員の立場から
  ・システムを使用した授業をしたいがその前に パスワードを忘れた学生の対応で講義時間が短くなる。
  ・掲示板等は、重要な事を掲示するので厳重なパスワード管理をしてもらいたい

- LAN管理室の立場から
  強固なパスワード管理をしてもらいたい
  学生がパスワードを忘れた時の処理が大変（情報処理の実習中など。。。）

認証を統一化。 同じユーザ名、パスワードでログイン可能にするので厳重なパスワードを管理してもらおう （PKIの導入も検討。。。。。）

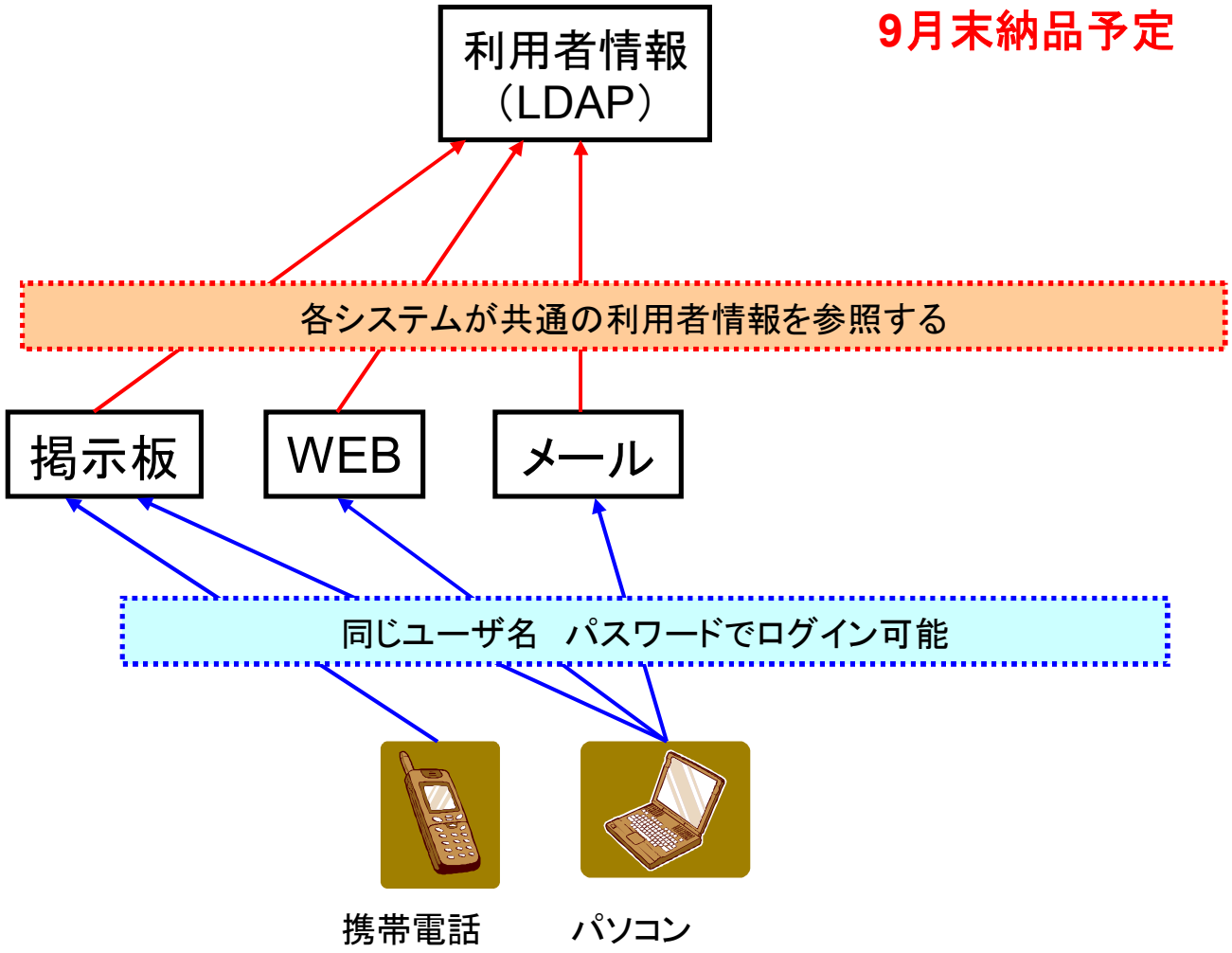
学生システムの認証（平成18年度迄）



学生システムの認証（平成19年度）

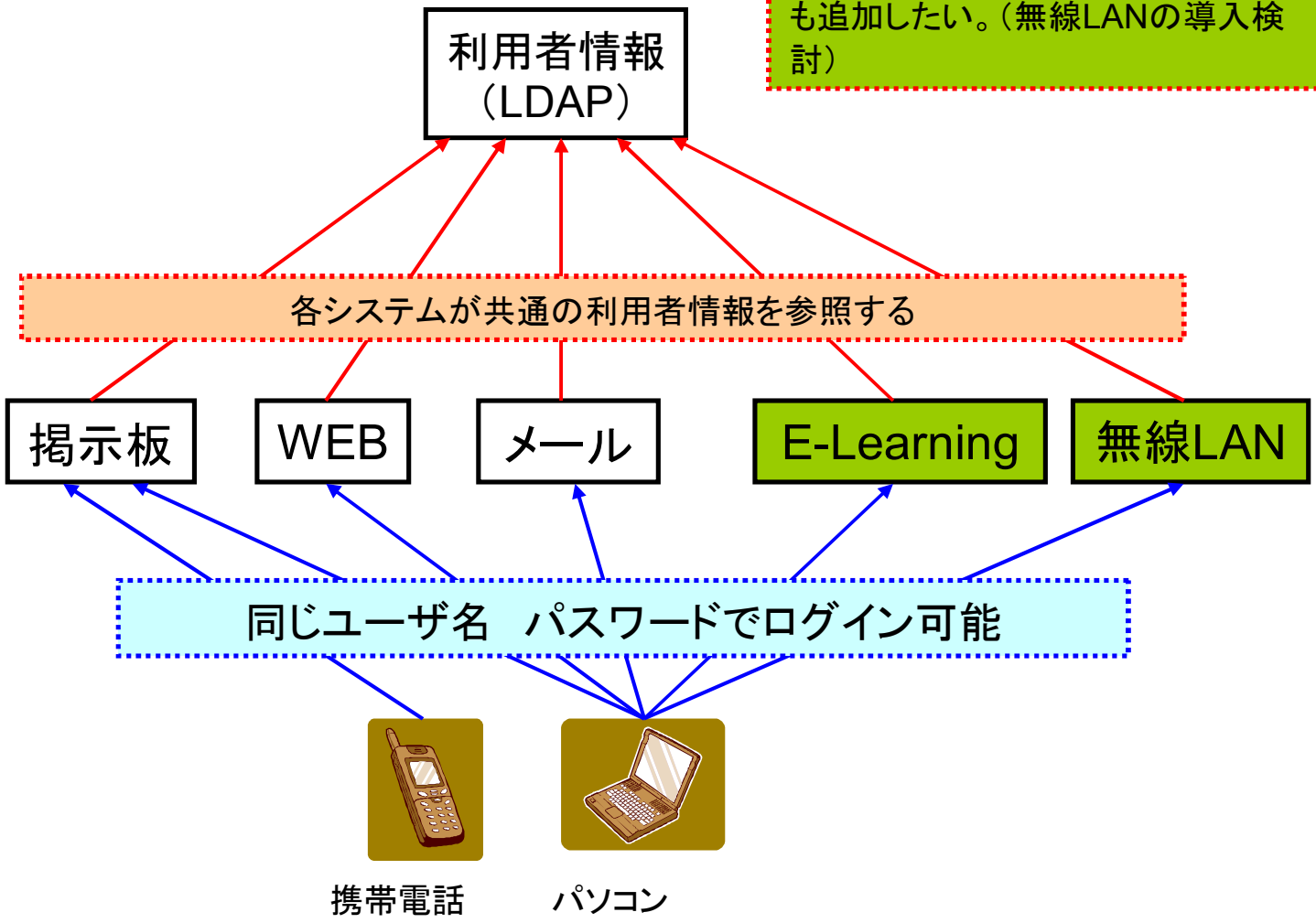
4月発注済み

9月末納品予定



今後予想されるシステムの展開

・E-learningを導入検討中
・これに伴い学生のアクセスポイントも追加したい。（無線LANの導入検討）



学生システムの認証（平成19年度）の システムだけで可能な事

- 今回導入したLDAPの仕様にあった製品を導入すれば、認証統合が可能（無線LAN・ E-Learning)
- 新しいシステム導入では利用者情報側とシステム側で拡張や調整が必要

PKIの導入について(メリット)

- ユーザ名やパスワードのみじゃなくPKIを導入すればよりセキュアになるのでは。
  （→もっと掲示板に色々掲示できる・E-Learningのコンテンツの充実）
- ICカード・USBキーでログインできるようにすれば利便性が向上
- 導入検討中のE-learningシステムでの本人認証
- IEEE802.1XでPKIできるように
  本学ネットワーク機器は、IEEE802.1X 対応
  Cisco Catalyst 4510+Catalyst 2960
  （→Radiusサーバが必要）

PKI導入の前提

- RADIUS及び各サーバーにプライベートCAで作成したサーバー証明書を設置
- 学生にプライベートCA で作成したクライアント証明書を配布
- 学生がSSL通信が可能なアプリケーションを利用できること

前提を実現するための課題

- 導入費用及び運転費用（保守費等）の問題
- 管理・運営がかなり大変そうである。
  （システム担当者は全学で2名）
- クライアント証明書の配布・紛失・再発行の対応？
- 使用者が使えるか　不満がでないか

PKIを導入した場合のシステム展開

認証を証明書で相互に行うため認証の精度が高まる!