名古屋工業大学情報基盤システム

情報基盤センター

センター長　松尾啓志

旧情報メディア教育センター、旧情報ネットワークセンターと情報基盤センターの業務について

情報メディア教育センター

組織の役割	業務
(1)情報処理教育	情報技術I（1部　4コマ（1コマ約130～180人））
(2)計算機保守管理	情報技術Ⅱ(1部　4コマ（1コマ約130～170人）)
	情報技術I（2部　1コマ（150人））
	情報技術Ⅱ(2部　1コマ（150人）)

情報ネットワークセンター

組織の役割	業務
MAINSの保守、運用、管理	MAINSの運用、保守、管理

合併、および**組織役割の変更**

情報基盤センター

部門	業務(助教授、助手、技術職員)
データベース部門**(新規)**	学内統合データベースの構築**(新規)**
	事務のIT化システムの運用**(新規)**
	ワークフローシステムの開発、運用**(新規)**
	学内システムの統合ソフトウエア開発**(新規)**
	事務局用PCの管理、運用**(新規)**
コースマネージメントシステム部門**(ミッション変更)**	ICカードによる出欠システムの開発**(新規、概算要求事項)**
	"学びの場"関連システム開発**(新規、概算要求事項)**
	CMSシステムの運用、新しいソフトウエア開発**(新規)**
	CMSシステム利用法の教員への助言、講習**(充実)**
	教育用計算機の管理、運用
	情報技術I, IIの授業補助
ネットワーク・セキュリティ部門**(ミッション拡大)**	MAINSの運用、保守、管理
	学内統一認証システムの開発、運用**(新規)**
	セキュリティ講習**(新規)**、対策
	次世代MAINSの調査、開発**(新規)**

教育支援

教務学生委員会
e-education部会
各教育類
リテラシイ教育

情報基盤センターをIT基盤を常時見直すことのできる技術力を持った組織とすることにより、大学内の迅速な業務改善、学生、教職員間のコミュニケーションの効率化を目指す。

認証基盤を前提としたシステム

- 学生側
  - 学生用PCへのスマートカードログイン
  - コースマネージメントシステムのための認証と、ICカードによる出欠管理システム
  - 学生用ポータルサイトへの認証
    - Webメール
    - VPN
  - 印刷管理システム
  - 図書館との連携（同一システムとして入札）
  - （学内福利厚生施設のキャッシュレス化）
- 教職員
  - 職員用PCのシンクライアント化とスマートカードログイン
  - 教職員用ポータルへの認証とSSO
    - 事務統合DB、統合ファイルサーバのための認証
  - 事務届けで処理のワークフロー化における電子認証
    - 物品購入と出張届けから始める。
    - 頻繁に行う手続きは電子化を行う（数年計画）。

電子認証基盤をどう選んだか？

- ICカードの種類は？
- ICカード上のOSは？
- シングルサインオンとの親和性？
- スマートカードログインとの親和性？
- ICカードの導入コスト、維持コストは？　コスト（悪魔）は細部に宿る。
- PKIはインハウス？アウトソース？、PKI認証運用時のノウハウは？
- 出席管理用ICカードリーダの選択

ICカードの種類

- 接触型
  - 利点：PKI認証ができる。安い。
  - 欠点：耐久性の問題（通常2000回程度）
- 非接触型
  - 欠点：PKI認証ができない。
- ハイブリッド型
  - 接触型＋非接触型　ただし独立
- デュアルインターフェース型
  - 接触側からも非接触側からもPKI認証が可能

	接触型	非接触型	ハイブリッド型	デュアル インタフェース型
簡易認証方式への対応	対応可	対応可	対応可	対応可
PKI認証方式への対応	接触型インタフェースからのみ利用 △	不可 ×	接触型インタフェースからのみ可 △	接触型，非接触型，両インタフェースから利用可 ○
接触型インタフェース耐久性	2000回程度の挿抜 ×		2000回程度の挿抜 ×	通常，接触型インタフェースは，使用しない.
非接触型インタフェース耐久性		5～10年程度	5～10年程度	5～10年程度
ICカードのコスト	1000～1500円／枚 ◎	1500円程度／枚 ○	3500円程度／枚 △	3500円程度／枚 △
ICカードリーダのコスト	1500円／台 程度 ◎	3000円／台 程度 ○	1500円／台 3000円／台 場所によって，両方を用意する必要がある. △	3000円／台程度 非接触用リーダのみでよい. ○

非接触ICカード

カードタイプ	FeliCa	TypeB
特徴	交通系・電子マネーで デファクトスタンダード	大容量・高度な暗号演算が可能 （チップ種類による）
国内導入実績	Suica、PiTaPa、Edy,様々な社員証・学生証 おサイフケータイ	住基カード、免許証 東京大学ICカード
対応ベンダー	様々なベンダー、様々な機能・機器が対応	ベンダー、対応機器共に限定される
PKI	演算機能がないため不可 （チップには鍵、PCで演算するタイプ有）	非接触エリアのみでは不可
将来性	様々な分野で活用されており、発行枚数は確実に増加。	大容量を活用するアプリケーションが少ない。対応ベンダーが増えるかがポイント

ICカードのOS

- 特にPKI認証の際の速度が問題だという噂（スマートカードログインに30秒以上かかる）をたくさん聞いていた。
  - JavaOS <=特にこちら
  - Multos OS
  - Native OS
- 実際にJavaOS上でのスマートカードログインをデモしてもらいました。最近のドライバでは実用上問題なし。

シングルサインオンとの親和性

- Active Directory + Windows を前提にしたSSOはかなり構築事例がある。
- 大学環境では
  - Windows だけでなく、最低　Mac OS X、できればLINUXもサポートする必要有り。
  - ブラウザもIE だけではなく、Mozilla 系のブラウザも重要となる。
- 従って、
  - クライアント証明書はPKCS#12に準拠
  - ICカードのドライバがMAC,LINUXをサポートしているか？　＝＞意外と少ない（というか事実上選択肢はほとんどない）。世の中は

ICカード導入コスト

- １枚当たりいくら？
  - 通常はベース金額＋枚数x１枚あたりのコスト
  - ベース金額と1枚あたりのコストは業者によって異なる。
  - 一括発注できる枚数により、安い業者が異なる。
- 隠れコストに注意
  - 通常の見積もりでは基本機能だけというのが多い
  - PKI実現時には、さまざまなオプションを追加する必要が
- ど
  - どこも組まない
  - 信販会社（同窓会カード？　あまり成功例がない）。
  - 信販会社＋α

公開鍵証明書と秘密鍵の発行形態

- PKI，電子認証を行うためにはICカード内に秘密鍵および公開鍵証明書を格納する必要がある。
- グローバル証明書の必要性？
  - そもそもアプリケーションがない。
    - S/MIME
    - UPKI
- ローカル証明書を前提に導入する。

公開鍵証明書の発行形態

- アウトソースモデル
  - グローバル証明書を部分的にでも用いる場合には、この形態しかない。
    - 有効期限に注意：学生書の場合は1年では足りない。
    - コストに関しては、交渉の余地有り
- インハウスモデル
  - 学内で公開証明書の発行を行う。
    - ソフトウエア、ハードウエアとも整備されつつある。
    - 暗号化ハードウエア(HSM: Hardware Security Module,)も安くなってきた。
    - 発行のノウハウに関して注意が必要。
- プレインストールモデル
  - ICカード購入時に、秘密鍵、公開鍵を書き込み済みにする。
    - 導入コストはアウトソースモデルと同じ
    - 個人情報と公開鍵証明書を関連づける学内作業が必要ない。
- 一括請負モデル
  - ICカードを発行する企業に一括して委託する方式
  - 基本的にアウトソースモデルと同様であるが、学内作業量が少なくなる。

PKI導入に関して

- MS-CA, ActiveDirectoryとの連動
- キーペアーのバルク発行
- キーペアーのバックアップ
- 特別な知識無しに電子証明書の管理ができる環境の提供
- 明確かつ運用しやすい業務モデルの構築
  - 申請、審査、発行、監査業務を明確に分離する運用モデル

大学にPKIを導入する際の問題点

- IDの統一
- さまざまな雇用形態の人が存在
  - 統一管理がなされていない。
- 新入生の名簿が3月末までFIXできない。FIX後1週間程度で、ICカードの発行＝＞事実上無理がある。
- 紛失時の対応
  - IDm （非接触　簡易認証）
  - 秘密鍵
  - 紐付けデータ
  - マニュアル化が重要
- 厳格な適用を誰が、どこで決定するのか？
  - ICカードがないと業務PCにログインできない（職員）。
  - 出席扱いにならないかも（学生）
- なにに使うかが導入時に明確でない。あとでICカードを更新することは事実上困難。進歩に取り残される危険性もある。待てるのならあと2年は待つべきか？
  - SSFC
  - FCF
  - IDm以外（簡易認証）以外は、配布後の拡張は困難

出席管理用ICカードリーダの選択

- 非接触型ICカードを使った出席管理システムは、既に存在している。
- これらは単に出席を電子的に取るだけ。
- 我々は新しい形の授業支援システムを提案
  - 特別研究経費：充実した「学びの場」の構築ー教員の教育力の向上及び双方向型教育支援システムの整備ー
    - 学生の出席履歴、コースマネージメントシステムによる予習復習履歴、成績を数年にわたり蓄積し、その結果をデータマイニングの手法により解析。その結果早期に授業について行けない学生を発見し、指導。もしくはより高度な教育を行うことのできる学生を発掘。
    - ICカードリーダの双方向化により、単なる学生ポータルサイトの構築だけでは困難なインタラクティブな情報伝達を可能とするシステムの構築。

ICカードリーダのカスタマイズ

- 既存のICカードリーダでは我々の要求は満たされない。
- 選択肢
  - LINUX　BOX　＋　非接触型ICカードリーダ
    - 自由度は高いが、少量発注なので値段も高い。
  - MS　ORIGAMI
    - 値段は安いが、耐久性に疑問
  - タイミング良く使えそうな物が出てきた￥(^0^)￥

某社のICカードリーダ

- OSはWindows CE
- SSFC,FCFにも対応したFerica対応
- タッチパネル、カメラ、スピーカ、マイクなどを標準装備
  - パネル、スピーカは学生への情報伝達に有効
  - マイクやカメラは使うかどうかは分からないけど楽しいそう。
- 無線LAN，有線LAN（PoE対応）
  - 持ち運び可能
- Dual CPU
  - 制御用モジュール搭載。電子錠などのコントロールもできる。
- メモリも大きい。メイン64MB，フラッシュ64MB
  - 出欠システムを構築する際は結構重要
- 我々がプログラム可能
- Toruka, WebTo 対応
  - ICカードの代わりに携帯電話を使った場合は、瞬時に100文字程度の文字データを携帯電話に転送可能。
  - 呼び出しや、ポータルサイトへのアクセス要求、電子メールの着信時連絡にも使える。
- 安い！！！！

最後に

- 学生
  - 個別ポータル
  - スマートカードログイン
  - 双方向型学習支援システム
  - 図書館システムとの結合
- 教職員
  - グループウエア（主に職員、できれば教員も）
  - シンクライアント＋ファイルサーバ
  - 事務作業のワークフロー化＋ペーパーレス
  - 統一データベースの構築
  - 学内既存レガシーシステムとの結合（SOA？）

これらの導入には、数年間の計画で行う予定です。しかし想像もできない困難が待ち受けていることは明らかであり、ある種無謀ともいえるプロジェクトであることは間違いありません。是非ともアドバイスを頂ければ幸いです。