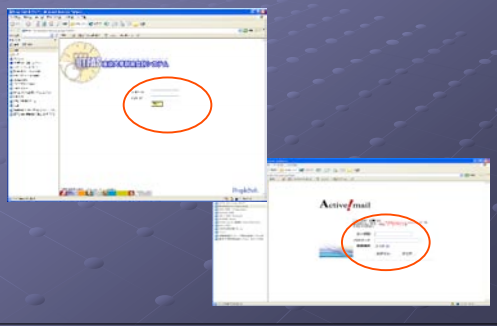
UT-CA（東大認証局）デモ

2006/07/28
情報基盤センター
PKIプロジェクト

「認証」とは何か（1）
ネットワーク上の情報サービス



「認証」とは何か（2）

- 「認証」 ～ 「本人確認」
- 「本人」 ～ ID
- 「本人確認」にパスワードだけで安心か？
  - 内部統制・外部からの攻撃
  - 財産やプライバシーの管理に十分か？
  - 「財務会計システム」「学務システム」…

本日のメニュー

- 「認証基盤」の目指すもの
- 「セキュリティ強化」とPKIの役割
- 大学での利用シナリオ
  ーPKIを使ったアプリケーション
- UT-CAの機能紹介
- UT-CAのデモ

利便性とセキュリティ

- IDは、情報サービスを受けるときの、Digital世界の中での「本人」そのもの。
- 「本人」性の確実な認証はDigital世界では難しい → セキュリティ確保の要請
- 一度、「本人」であることを確認できたら、次からは、その事実を使いたい → 利便性の向上の要請
- → 認証基盤の構築への期待

「セキュリティ強化」とPKIの役割

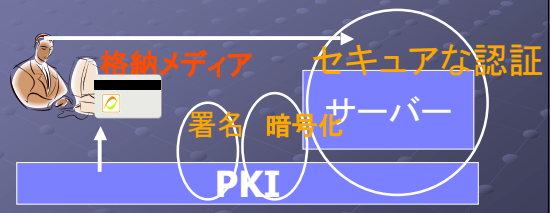
- PKIとは何か

公開鍵暗号技術とX.509証明書

- 現在の技術でもっとも強固なセキュリティを提供できる技術といわれている。

「セキュリティ強化」とPKIの役割

- 認証「基盤」とその全体像



大学での利用シナリオ

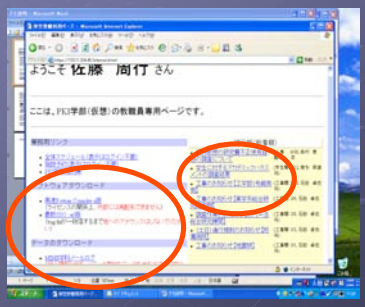
- セキュリティの高い認証 （1）
  - Webにおける認証
- セキュリティの高い認証 （2）
  - アクセスポイントとしてのSSL-VPN
- 機密性・本人署名の必要性
  - s/MIME メール

大学での利用シナリオ

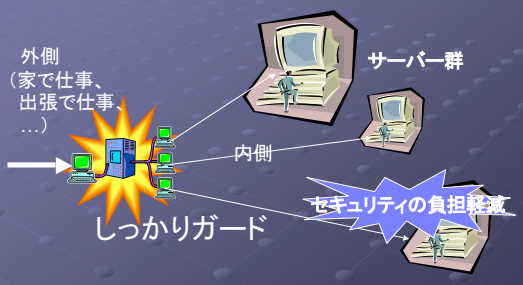
- PKIのご利益
  - 財産、プライバシー、各種法律の強制するセキュリティを実現する
  - 個々のサーバのセキュリティに関する出費の抑制・制限の緩和を可能にする
  - 「なりすまし」「データ偽造」などの情報システムへの攻撃を抑止する

→今まで電子化を妨げていた要因（のいくつか）が取り除かれる

（1）Webページの安全性の高い認証



（2）アクセスポイントの認証強化



（3）暗号化と署名

- メールは、盗聴、改ざんの可能性が否定できない
- 盗聴、改ざんができないメールがあれば、
  - 定期試験問題くらいは、メールで送り付けたい
  - 成績報告をメールでするのは、検討してもよい

大学での利用シナリオ

- これらはすべて、

電子証明書と公開・私有鍵

を利用したアプリケーションプログラム。

実は、世の中にPKI対応のアプリケーションプログラムはそれなりに存在し、すぐに利用可能になっている

大学での利用シナリオ

- これらはすべて以下の了解のもとに可能。
  - 電子証明書と暗号鍵が、「正しく」作成され、
  - 確実かつ安全に本人あてに配布され、
  - 関連する情報が公開され、
  - これら一連のことを皆が「信じている」
- PKIの管理側の負担は、これらの「期待」に応えなければならない。
  - 運用コストの問題

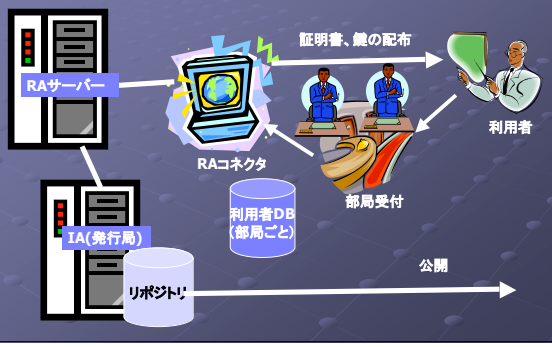
大学におけるPKIの業務

- 「大学」という組織の中で、PKIを実現しようとするときの業務の問題
  - x権限委譲による分散処理の必要性
    （発行業務を中央一か所で統制するのは実情に合わない）
  - xデータの一括、大量処理が必要

UT-CA

- UT-CAは、大学でPKIを運用する場合を想定して、運用コストを最適化するために設計された
  - **利用者の負担軽減のための鍵代理生成・証明書ダウンロード機能**
  - **権限委譲による分散管理**
  - **複数人（2人）による承認・審査体制**
  - **管理側の負担軽減のための機能（例：一括申請・処理）**
  - **監査のためのログ出力**

UT-CAの構成



UT-CAの運用実演

- 証明書発行
  - 職員証・学生証の発行に合わせて、カードに書き込んで配布する
  - 発行後に、ダウンロードの形で配布する。
  - どちらも可能な業務フローを検討した（今回は、ダウンロードのデモを行う）
- 証明書失効

すべてはここからはじまります


PKI 学部
電子証明書発行担当者　殿

複数人操作の強制について

	利用者	審査者	承認者	検査者
利用者申請	→			
申請内容審査		●	×	
審査内容承認		×	●	
証明書発行		●	×	
証明書取得	←			
プロセスの検査				●

時系列

UT-CAの運用実演

- パイロットシステムが完成
- 今後の予定：
  - ロジックの追加
  - 実地での検証（複数の部局に協力を依頼）
  - コストの検証
  - システムの増強

認証基盤研究開発の今後の予定

- PKIの実現で、認証基盤が完了するわけではない
- 大学には、まだ解決を待つさまざまな問題がある
  - **「秘書問題」**
  - **「サイボウズ問題」**
  - **その他**
- コストを意識しながら、解を見つけるための研究開発を進めていく予定