東京大学認証局（UT-CA）構築に向けて

東京大学情報基盤センター
大島　大輔（PKIプロジェクト）

第28回全国共同利用情報基盤センター
研究開発連合発表講演会

2006年11月28日（火）
大阪大学銀杏会館　3階ホール
大阪府吹田市

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

本日の発表内容

1. 認証（PKI）を調査・研究することになった背景
2. 東京大学情報基盤センターPKIプロジェクトが調査・研究してきたこと
3. 東京大学認証局（UT-CA）のデモンストレーション
   - 3.1 なぜデモンストレーションを実施したか
   - 3.2 事前準備およびデモンストレーションで気をつけたこと
   - 3.3 当日の模様
   - 3.4 参加者の感想
   - 3.5 実施してよかったこと，反省が必要なこと
4. 今後の展望
5. おわりに

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

1　認証（PKI）を調査・研究することになった背景

- ここ数年多くの大学，民間企業等では情報システムのデータ漏えい事件や不正アクセスなどの被害を受けている
- それにともない，安全・安心な認証やセキュリティの重要性が高まってきた
- しかし，社会にある様々な情報システムはセキュリティに不安を抱えつつもID+パスワードという認証が一般的
- そこで本センターでは，大学における認証の調査・研究を行うプロジェクト（以下，PKIプロジェクトという）発足させ，認証にPKI（Public Key Infrastructure:公開鍵基盤)を採用することを前提に検討を開始

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

2．東京大学情報基盤センターPKIプロジェクトが調査・研究してきたこと　–その１

- 東京大学における認証の現状の把握
  - 情報システムへのアクセスに関するルールは，システム毎にとりきめられている
  - ID+パスワードが一般的
- 証明書および秘密鍵の格納デバイス検討
  - ICカード型身分証，USBトークン，ハードディスク
  - それぞれのメリットデメリットを検討

各デバイスのメリット・デメリット

	ハードディスク	USBトークン	ICカード型身分証
メリット	・既設のハードディスクに格納するため費用がかからない ・鍵を使用するPCが限定されていれば，携帯しなくてよい	・「鍵」を持つというイメージにあう。デバイス自体が「鍵」を想像させる ・USBポートに挿すだけで使える。ただし，ドライバソフトのインストールは必要	・身分証の中に証明書を格納できる ・既に確立した教職員，学生への配付方法がある ・USBトークンと比較して安価
デメリット	・パソコンの盗難や，ネットワーク経由での不正侵入等の可能性があり，セキュリティ面で不安がある	・常時携帯している身分証の他に携帯しなければならない ・デバイス自体が高価	・ICカードを認識するための読み取り機器が必要 ・券面に個人情報が記載されており，盗難の際紐づけて悪用される恐れがある

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

2．東京大学情報基盤センターPKIプロジェクトが調査・研究してきたこと　–その２

- 認証局運用体制の確立
  - 学部，研究科，附置研究所，全学センター等の各部局に対して登録業務の権限を委譲する分散管理体制
  - 登録，審査業務に関しては相互牽制を行える体制
- コンサルティングの活用
  - 認証（特にPKI）についてのノウハウを持つベンダの意見を参考にしたい
  - PKIプロジェクトが調査・研究してきた内容，方向性の正しさを確認したい

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

3．東京大学認証局（UT-CA）のデモンストレーション

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

3.1 なぜデモンストレーションを実施したか

- **本学の意思決定に関与する方および一般利用者に対してPKIの理解を得るため**
- PKIというイメージしにくいものに対して，SSL-VPNやS/MIMEといったアプリケーションを使って理解していただく
- PKIの根幹となる認証局（CA）というものを寸劇を行い認知していただく
- 認証（PKI）を2005年1月から1年以上調査・研究して構築した成果物（UT-CA）を，学内の方に見ていただき評価を聞きたい

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

3.2 事前準備および当日のデモンストレーションで気をつけたこと –事前準備

事前準備

- 当日の進行に即したリハーサルを必ず行うこと
  - 要所のみのリハーサルを行うと，当日の進行で思わぬトラブルに見舞われる可能性がある
- デモンストレーション会場の広さにかかわらずマイクは使用したほうがよい
  - デモ機（サーバ）がうるさかったり，後ろの方では声が聞こえづらいことがある
- その他の注意点
  - 会場案内板を用意，空調のチェック，パンフレットの用意

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

3.2 事前準備および当日のデモンストレーションで気をつけたこと –当日

当日

- 飽きのこない構成でデモンストレーションを行った
  - 講演者の話を1時間聞いていても飽きるので，PKIのアプリケーション（S/MIMEとSSL-VPN）デモや認証局の役割について寸劇を行った
  - 会場の雰囲気が活発になるよう，デモの最後だけでなく，途中でも質疑応答を行った

- デモンストレーション当日に認証に関するタイムリーな話題を提供できるよう，前日までの報道を注意して見た
  - この時は日本経済新聞の社員が権限のないサーバにアクセスしインサイダー情報を得て，それをもとに株式取引を行い逮捕された話

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

3.3　当日の模様　-その1

日時：2006年7月28日（金）　14:00～15:00
会場：東京大学情報基盤センター別館地下1F

デモンストレーションタイムテーブル

時　間	内　容	備　考
14:00	デモンストレーション開始	PKIの概要を説明後，簡単な質疑応答を行った
14:15	PKIを使ったアプリケーションデモンストレーション	使用アプリケーションはSSL-VPNとS/MIME
14:30	認証局運用体制の説明	配役を決め，それぞれの役割について寸劇を行った
14:50	全体についての質疑応答	
15:00	デモンストレーション終了	

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

3.3　当日の模様　－その2

PKIの概要を説明

アプリケーションを使ったデモ（SSL-VPN ＆ S/MIME）

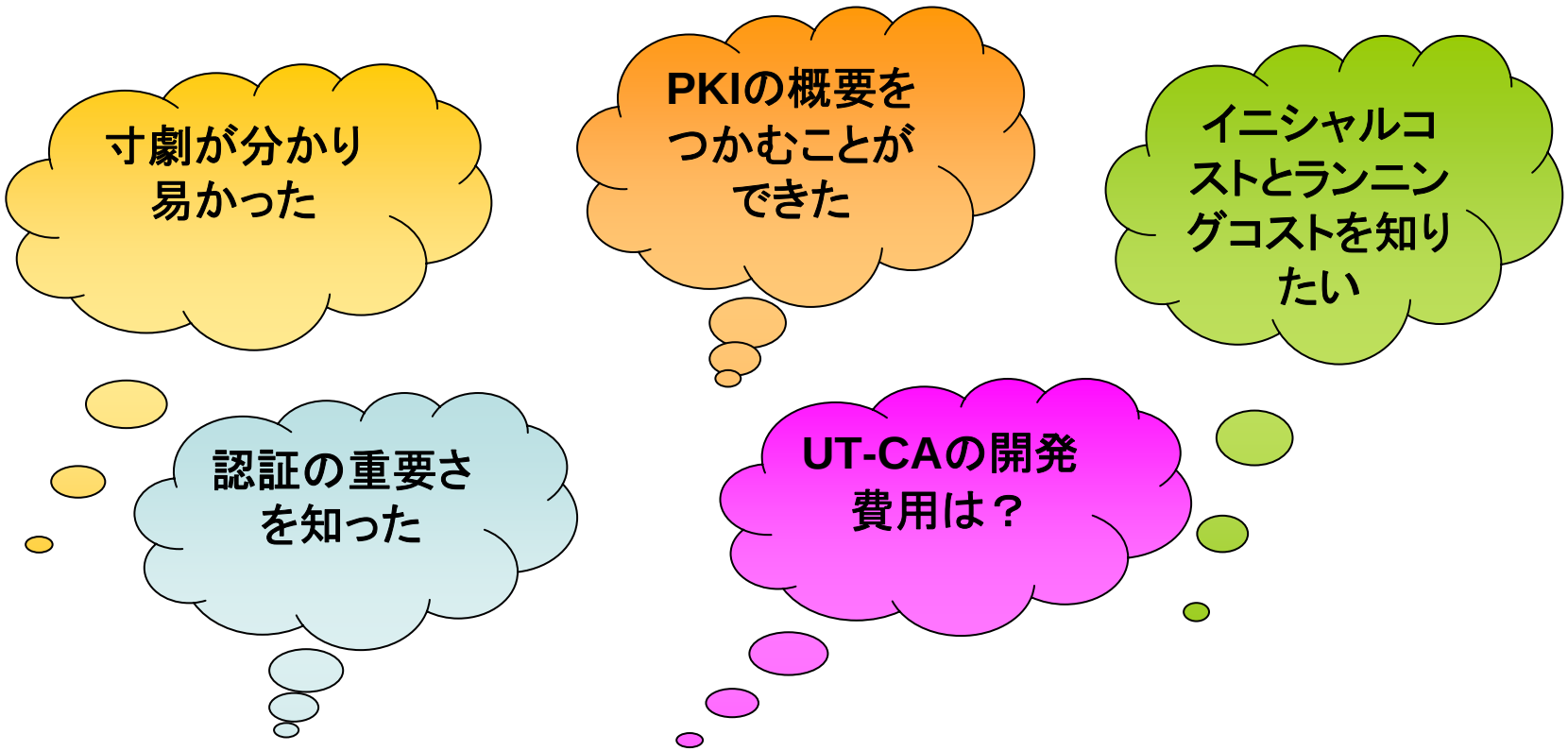
認証局担当者の役割を寸劇で説明

質疑応答

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

3.4　参加者の感想

- 会場でアンケート用紙を配付したわけではなく，デモンストレーション終了後に個人的に聞いたり，人づてに感想を聞いたりした内容です…



Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

3.5　実施してよかったこと，反省が必要なこと

- よかった点
  - まずは認証（PKI）を認知してもらえるだけでも収穫はあった
  - 認証局の役割の理解を助けるための寸劇を行ったことはよかった

- 反省すべき点
  - アプリケーションのデモ時にPINを入力する場面があったが，紛らわしい文字（l(小文字のエル)，1（数字のイチ），|（記号のパイプ））を事前にPINに設定しない等の対策をしなかったため，デモ当日で慌ててしまった

    →リハーサル中に気付いてはいたが，文字の設定に時間がかかると勝手に思い，当日にはなんとかなるだろうということで，そのまま進めてしまった。**トラブルの芽は事前に摘むこと！！**

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

4　今後の展望

- 複数部局とPKIの実証実験を開始します
  - 部局担当者の本務への負荷を調べる
  - 全学規模の展開を想定した技術の検証とノウハウの蓄積
  - 上記2項目はUT-CAに関することだが，実証実験を行うことにより，PKIそのものもの使い心地，メリット，問題点等を洗い出す
- UT-CAの広報
  - 今回行ったデモンストレーションの拡張版として，本郷キャンパスの他，各地に点在するキャンパスに出張し，UT-CAおよびPKIの広報を行う
- CP/CPSの作成
  - 認証局の憲法というべきCP/CPSの作成に向けて鋭意検討中

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.

5　おわりに

- この資料は東京大学情報基盤センターPKIプロジェクトのWebサイト（http://www.pki.itc.u-tokyo.ac.jp/）に公開予定です
- 本日は認証の話を主にしましたが，PKIのもう一つの柱であるデジタル署名を用いたS/MIMEも併せて調査・研究しています
- PKIプロジェクトの成果が表れつつあるので，今後も情報を発信続けていきます

Copyright© 2006 Information Technology Center, The University of Tokyo. All Rights Reserved.