

全体運用報告

大島 大輔

東京大学・情報基盤センター・PKIプロジェクト

UT-CA報告会 -東京大学認証局構築に向けて-

2007年4月27日(金)

東京大学農学部弥生講堂・一条ホール



アジェンダ

1. 東京大学情報基盤センターPKIプロジェクトとは？
2. PKIプロジェクトの歩み
3. UT-CA概念図
4. UT-CAの運用説明
5. UT-CAの広報
6. おわりに

PKI

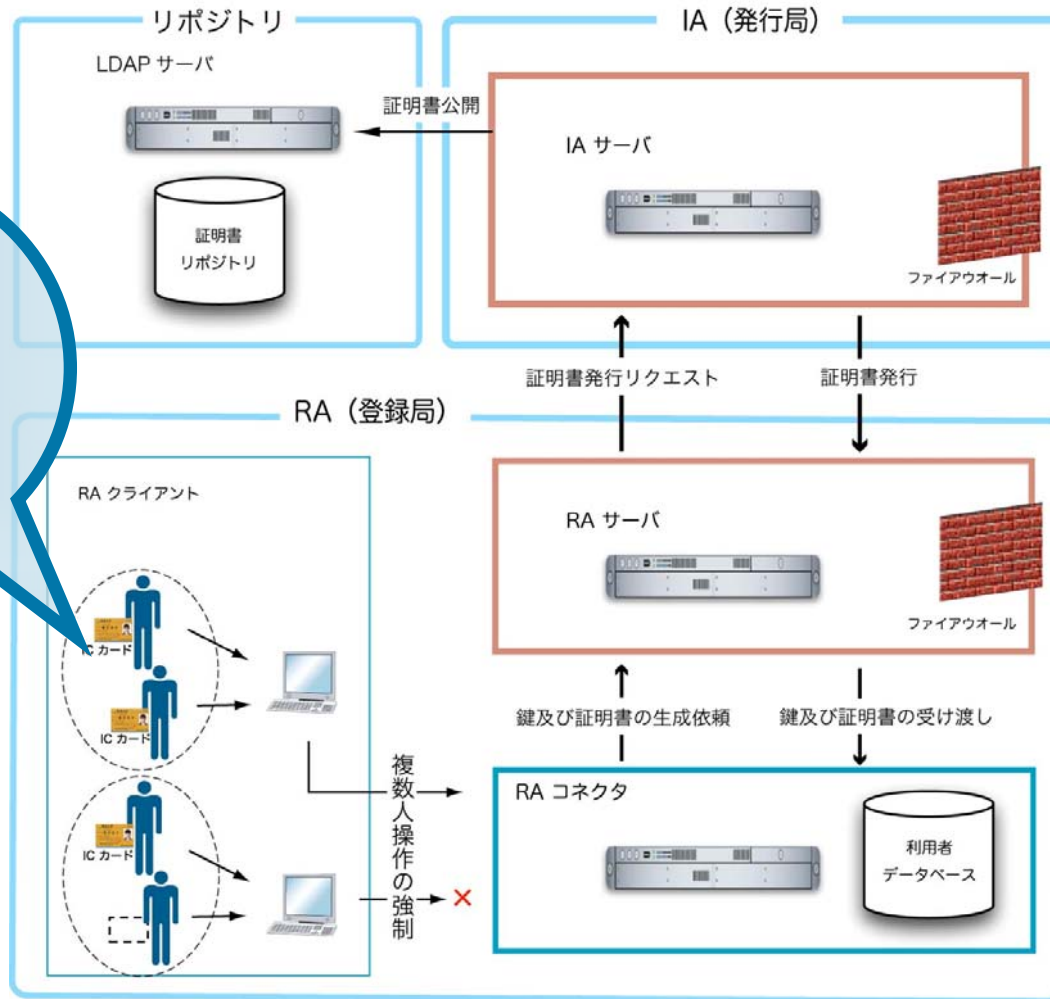
東京大学情報基盤センターPKIプロジェクトとは？

- 部門横断的なプロジェクト
 - 情報メディア教育部門, 図書館電子化部門, キャンパスネットワークキング部門, スーパーコンピューティング部門の教員が参画
- 大学における認証の調査・研究を行うプロジェクト
 - UPKI
 - 認証作業部会(北海道大学, 東北大学, 東京大学, 名古屋大学, 京都大学, 大阪大学, 九州大学, 東京工業大学, 高エネルギー加速器研究機構, 国立情報学研究所)
- PKIアプリケーションの模索
 - SSL-VPN
 - S/MIME
 - SSO (Single Sign-On)
 - デジタル署名(事務ワークフローで利用) など...

PKIプロジェクトの歩み

年 月	摘 要
2005年1月	PKIプロジェクト発足
2005年1月～現在	PKIプロジェクトの運営, PKIアプリケーションの候補, およびその他の議題について月に1回程度の会議を行う
2005年10月～ 2006年3月	プロトタイプのCA(UT-CA)構築を検討および決定→構築に向けて調査・研究の開始
2006年3月	プロトタイプのCA (UT-CA)完成
2006年5月	SSL-VPN Gateway 試行サービス開始(→清田助教発表)
2006年7月	PKIプロジェクトとして初の報告会を開催
2006年11月	情報学環部局RAを立ち上げる(→原田准教授発表)
2006年12月	運用管理規定(CP/CPS)制定
2006年12月	本部事務局, 情報基盤センター合同RAを立ち上げる(→佐々木職員発表)
2007年1月	東京大学学内広報(No.1350)でUT-CAのフィンガープリントを公開
2007年4月	UT-CA報告会を開催

UT-CA概念図



審査者および承認者の2名が揃わなければ、証明書と鍵は発行できない



UT-CAサーバ群

UT-CAの運用説明 その1

UT-CAの操作

1. 施錠してあるサーバ室に入室→鍵の施錠は鍵管理者
2. 2名の担当者により操作を行う(相互牽制)
3. サーバ室鍵管理者はCAを操作できない

※参考

現在、サーバ室に入る時は鍵を使用しているが、本来はICカード＋生体認証等の組み合わせ、かつ入退室のログを採ることが一般的ではあることはPKIプロジェクトも認識している。ただし、プロトタイプのカということもあり、そこまでの運用は行っていない。

UT-CAの運用説明 その2

部局RAに対して

- 部局責任者に登録局業務委任願を提出させ、それに対しPKIプロジェクトでは、登録局業務委任状と機器貸与通知書を交付する
- 上記のやりとりはやや形式的ではあるが、一般利用者に信頼を得るためには止むを得ない

登録局業務委任願

情報基盤センターPKIプロジェクト
UT-CA トライアル管理運用組織代表 殿

以下の通り、登録局業務の委任をお願いいたします。

年 月 日

部局名 _____

責任者 _____ 印

操作者名	操作者の共通 ID	操作内容
1		審査者・承認者
2		審査者・承認者
3		審査者・承認者
4		審査者・承認者
5		審査者・承認者

※ 操作内容については該当するものに丸をつけること。審査者と承認者を兼任することはできない。

これより下は記入しないこと

審査



UT-CA トライアル登録局業務委任状

以下の通り、UT-CA トライアル登録局業務を委任する。

年 月 日

情報基盤センターPKIプロジェクト
UT-CA トライアル管理運用組織代表 印

部局名: _____

氏名: _____

共通 ID: _____

審査者・承認者の別: _____ として

貸与する登録局操作者 IC カード
シリアルナンバー: _____
初期 PIN: _____

※ 登録局操作者 IC カードの PIN は、IC カードを受領次第変更すること。



UT-CA トライアル登録局支部機器貸与通知書

以下の通り、UT-CA トライアル登録局支部運用のために使用する機器を貸与する。

年 月 日

情報基盤センターPKIプロジェクト
UT-CA トライアル管理運用組織

貸与先部局名: _____

PKI 証明書登録端末: _____ 台

初期 Windows ログオンパスワード: _____

初期管理者パスワード: _____

初期 PIN ロック解除用管理者パスワード: _____

証明書ダウンロード用端末: _____ 台

初期 Windows ログオンパスワード: _____

初期管理者パスワード: _____

※ 初期設定されているパスワードは、受領次第変更すること。

部局責任者より提出

PKIプロジェクトより交付

UT-CAの広報 その1

- Webページ
 - <http://www.pki.itc.u-tokyo.ac.jp/>

The screenshot shows the homepage of the UT-CA project. At the top, it reads '東京大学情報基盤センター PKI プロジェクト UT-CA'. Below this, there are navigation links for 'UT-CA' (selected), '資料公開', 'PKIプロジェクトについて', '認証リリース', and '研究・教育'. A notice states that the UT-CA report will be published on the website on April 27th. The main content area is titled 'UT-CA(東京大学PKI管理コンプライアンスシステム)' and includes a 'PKIの仕組みを簡単に説明' link. A paragraph of text describes the project's goals and the role of the RA (Registration Authority). Below the text is a diagram titled 'CAの処理フロー' (CA Processing Flow) showing the interaction between the RA (発行者), CA (認証局), and the user (利用者). The RA issues certificates to the CA, which then issues them to the user. The user can also request certificates from the RA. A sidebar on the right lists features like 'セキュアなログイン方法の実装' (Implementation of secure login methods), 'SSO, SSL, VPN' (SSO, SSL, VPN), 'データの暗号化' (Data encryption), and '電子署名' (Digital signature). Below the sidebar, there is a warning icon with a red 'X' and the text '盗難 (Steal) 盗み (Steal) 偽造 (Forgery) なりすまし (Spoofing)'.

- 成果報告
 - 2006年7月28日(金) UT-CAデモンストレーション@情報基盤センターB1F
 - 2007年4月27日(金) UT-CA報告会(本日)@農学部弥生講堂・一条ホール

UT-CAの広報 その2

2006年7月28日(金)

UT-CAデモンストレーション@情報基盤センターB1F



UT-CAの広報 その3

● 研究会等の成果発表

1. [発表1] T. Nishimura, H. Sato, “Authentication with PKI a Case Study in Information Technology Center in The University of Tokyo,” International Symposium on Advanced ICT, pp. 251-255, 2006. 2006年8月8日 電気通信大学
2. [発表2] 大島 大輔,西村 健,佐藤 安一郎,佐藤 周行,“東京大学認証局(UT-CA)構築に向けて,” 第28回全国共同利用情報基盤センター研究連合発表講演会, 研究開発論文集No.28,pp.42-49,2006年11月 2006年11月28日 大阪大学
3. [発表3] 西村 健, 佐藤 周行,“レガシー Web アプリケーションに対応するPKI を用いた簡易 Single Sign-On の実現,” インターネットアーキテクチャ研究会, 電子情報通信学会技術研究報告 Vol.106 No.465, pp. 61-66, 2007年1月 2007年1月19日 広島国際会議場
4. [発表4] 大島 大輔,“東京大学認証局(UT-CA)の構築と普及に向けて,” 平成18年度名古屋大学総合技術研究会, “情報・ネットワーク技術研究会報告集,pp.13-16,2007年3月 2007年3月1日 名古屋大学
5. [発表5] 西村 健, 佐藤 周行,“自律的組織の集合体としての大学におけるPKIの運用,” 情報処理学会全国大会 講演論文集(分冊4), pp. 327-328, 2007年3月 2007年3月6日 早稲田大学

おわりに

- ご意見, ご質問等ございましたら, 下記担当までご連絡お願いいたします



東京大学情報基盤センター
PKIプロジェクト

事務担当: アプリケーション支援係

電話: 03-5841-2739

メール: pki-info@itc.u-tokyo.ac.jp