東京大学情報基盤センター PKI プロジェクト

UT-CA

東京大学情報基盤センター PKI プロジェクトは，センター内において，認証技術全般の研究開発を行うために, 2005 年 1 月に, センター内の関係する教職員を集めて発足しました。PKI 技術は, 認証技術の重要な要素の一つとして，特に力を入れています。

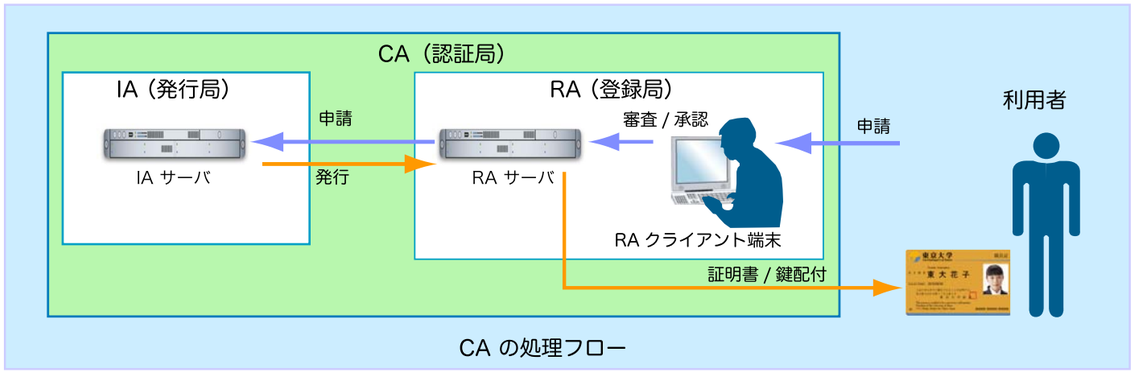
東京大学情報基盤センター
Information Technology Center, The University of Tokyo
〒113-8658　東京都文京区弥生2-11-16
TEL:03-5841-2710　FAX:03-5841-2708(G3)
URL:http://www.itc.u-tokyo.ac.jp/

PKIプロジェクト
URL:http://www.pki.itc.u-tokyo.ac.jp/

東京大学情報基盤センター
Information Technology Center,The University of Tokyo

東京大学情報基盤センター PKI プロジェクト UT-CA

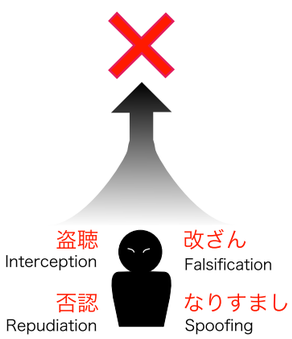
UT-CA は，東大情報基盤センター PKI プロジェクトが，大学における管理運用を想定して設計した，インハウス(学内)用の PKI 業務システムです。UT-CA は, PKI における IA(発行局), RA(登録局)と, リポジトリ(情報公開サーバ)，さらに，これらの運用管理を行う体制を含みます。大学組織における証明書発行業務は，学生，教職員をはじめとした多様な構成員を対象にしなければなりません。しかも，運用においては少ない人員で且つ合理的なコストで利用者管理 / 発行業務が行えること，その際にセキュリティに厳密であることが求められます。UT-CA は，これらの要求に応えるべく設計されました。2006 年度は，実験的な運用を開始し，システムの熟成を図っていこうと考えています。

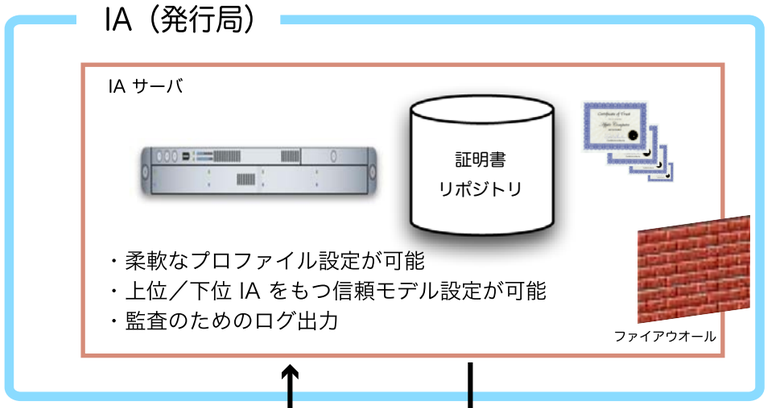


CA の処理フロー

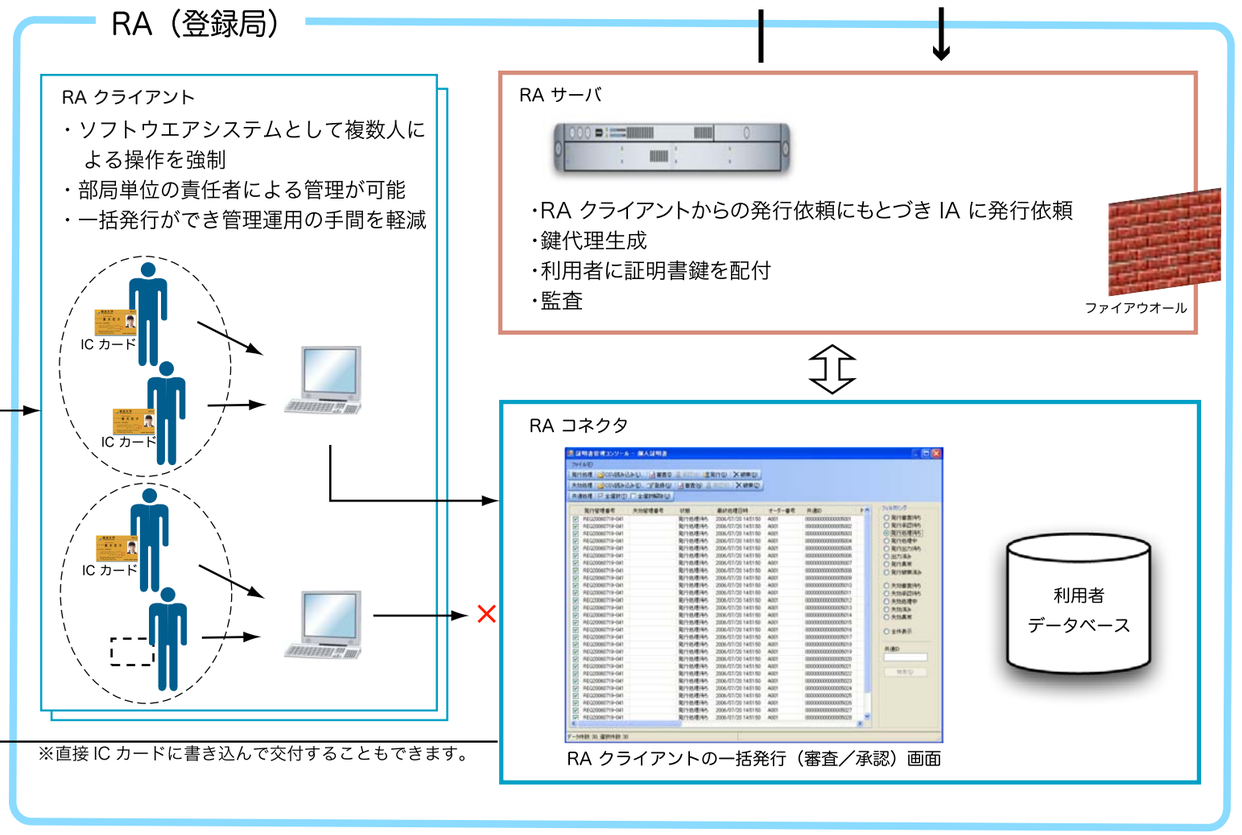
多様な利用シーン

- セキュアなログイン方法の提案
  - SSO，SSL-VPN
- データの暗号化
- 事務の電子化
  - デジタル署名，S/MIME メール



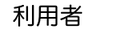


証明書発行リクエスト　証明書発行



※直接 IC カードに書き込んで交付することもできます。

RA クライアントの一括発行（審査／承認）画面

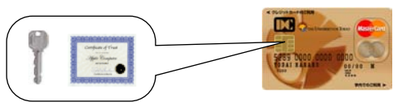


申請

証明書ダウンロード Web 画面

交付

鍵・証明書の書き込み



運用体制

UT-CA は，それを運用する体制の提案を含んでいます。運用体制の実現にあたっては，現状，大学で行われている業務が基づく権限の階層，さらに具体的な事務の流れにはめ込めるようなものにしなければなりません。加えて，PKI に関係する業務が従来の業務を圧迫しないという実地の証明が重要です。われわれは，発行業務に際して，大きめの単独部局，または部局の集合体を想定し，最少人数で運用が可能で，しかも規則に外れた一人の暴走を防ぐ体制を提案しています。また，本格的な運用を前に，実験的な運用をして，提案する運用体制が合理的であることの検証をすることが不可欠であると考えています。