# 東京大学におけるキャンパスPKIの配備に向けて

**東京大学　情報基盤センター**
**PKIプロジェクト**
**佐藤周行　西村健**

# はじめのはじめに（今後ふれません）

- UPKI
- **消費者･調達者としての大学**
- **問題生産者としての大学**

- **東大は、パブリックサーバ証明書のための審査体制を作っていますが、それはまた別の機会に**（RAじゃないし）**。今日の話は人間が対象。**

# http://www.jnsa.org/では

- 東京大学では、2005年度から教職員証と学生証がスマートカード化され、その上の有力なアプリケーションとしてPKIの配備が計画されました。しかし、PKIの配備にはRPの育成と収容など、技術的な問題とともに、管理コストの最適化をはじめとする（この規模の大学にありがちな）財政的・政治的な問題の解決が求められます（ことをいまさらながら痛感しています）。
  この発表では、
  ・東大でのPKI配備に関する技術的・または非技術的背景
  ・管理コスト最適化の試み
  ・証明書活用に関する大学のワークフローとの齟齬などの解決
  の検討を行い、一部実施した結果を報告します。

# Agenda

1. 東大がPKI配備を計画するまでの経緯
    1. PKI配備に関する技術的な背景
    2. PKI配備に関する非技術的な背景
2. 管理コスト最適化の試み
    1. 大学のワークフローへのはめ込みの試み
3. アプリケーションの問題
    1. 問題の発見
    2. 解決策の提示

# PKI配備を計画するまでの経緯

- 2004**年秋プレスリリース**

  **職員証と学生証のスマートカード化**

  **スマートカードにのせるアプリケーションとしてクレジットカード機能、**SafetyPass**機能を発表**
- **プレスリリース内で「将来の**PKI**のメディアとしての利用」をうたう**
- 2005**年**1**月、当時のセンター長の指令で**PKI**プロジェクトを設置**

# PKI配備を計画するまでの経緯

- **全学規模でのスマートカードの導入に際し、解決を要する問題は実は山積み**
  - **カードの発行／運用体制の構築**
  - **全学規模での採番体制の構築　＝　全学規模でのID管理の必要性**
  - **管理運用コストの最適化**
- **本部事務局の努力によって、運用は軌道に乗っている**

# PKI配備に関する技術的・非技術的な背景

- PKIの配備を要求する技術が東大内にあるか？
  - 「作っては見たものの…」では最悪
- PKIの配備は技術的に可能か？
  - この規模の配備はスケールするよね、という確認
- PKIの配備は運用的に可能か？
  - 働くことを期待されているスタッフにそっぽを向かれるのが最悪

# PKIの配備を要求する技術ー需要

- **プローブ先はいくつかある**
  - A**学科**、B**課**、**情報基盤センター**、…
- **困っていそうなところがいくつかある**
  - Critical servers**は、そのほとんどがパスワード認証に加えて**IP**アドレス認証を行なっている**
  - **ファイルにパスワードをかけることが多くなってきた**

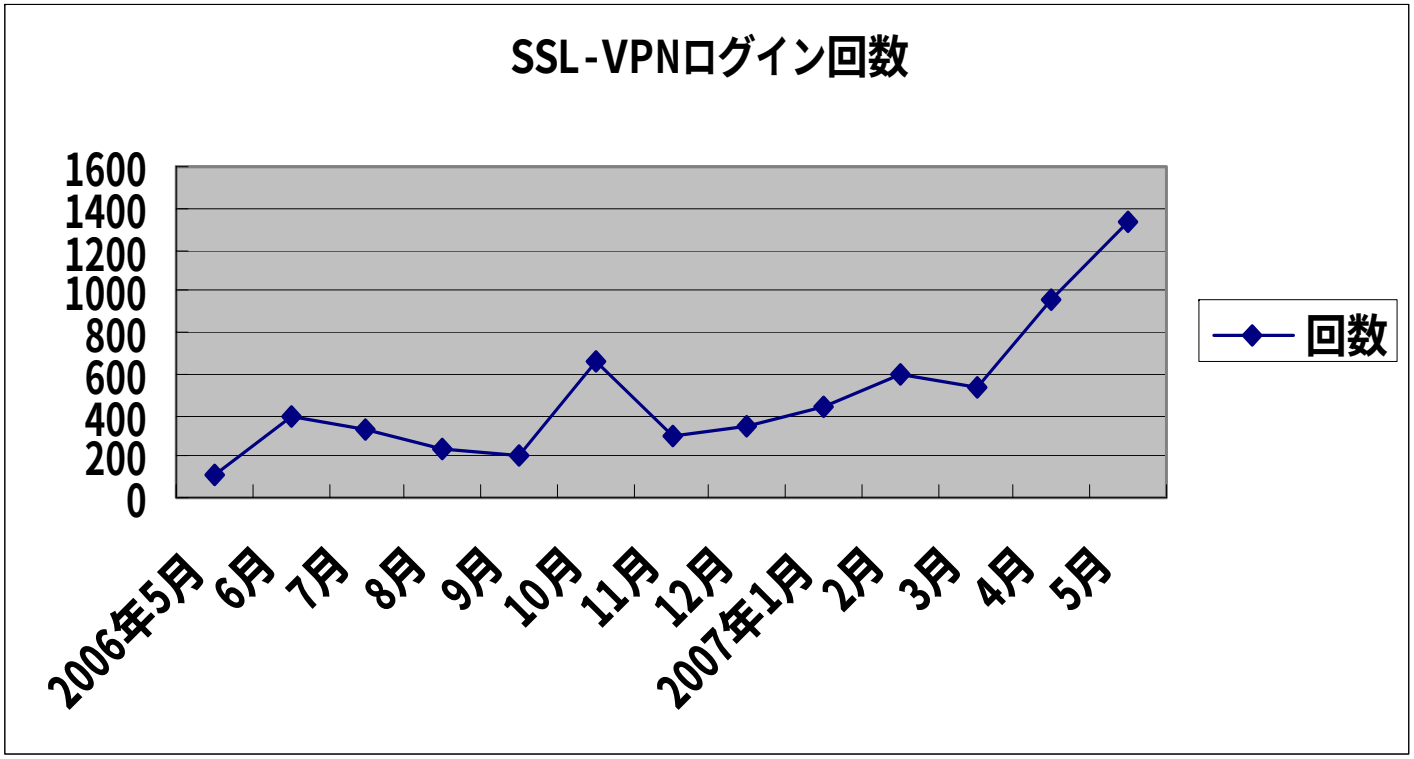
# 潜在的な需要の一例

- **総合図書館によるSSL-VPNサービス**
  - **文献DBのアクセスは出版社との契約により、学内IPアドレスをもっている場所からしかアクセスを許さない**
  - **それにつられて、その制限をかけていないDBへのアクセスにも網をかけている**
  - **認証をしっかりすれば、学外からのアクセスでも大丈夫と思うことにする**

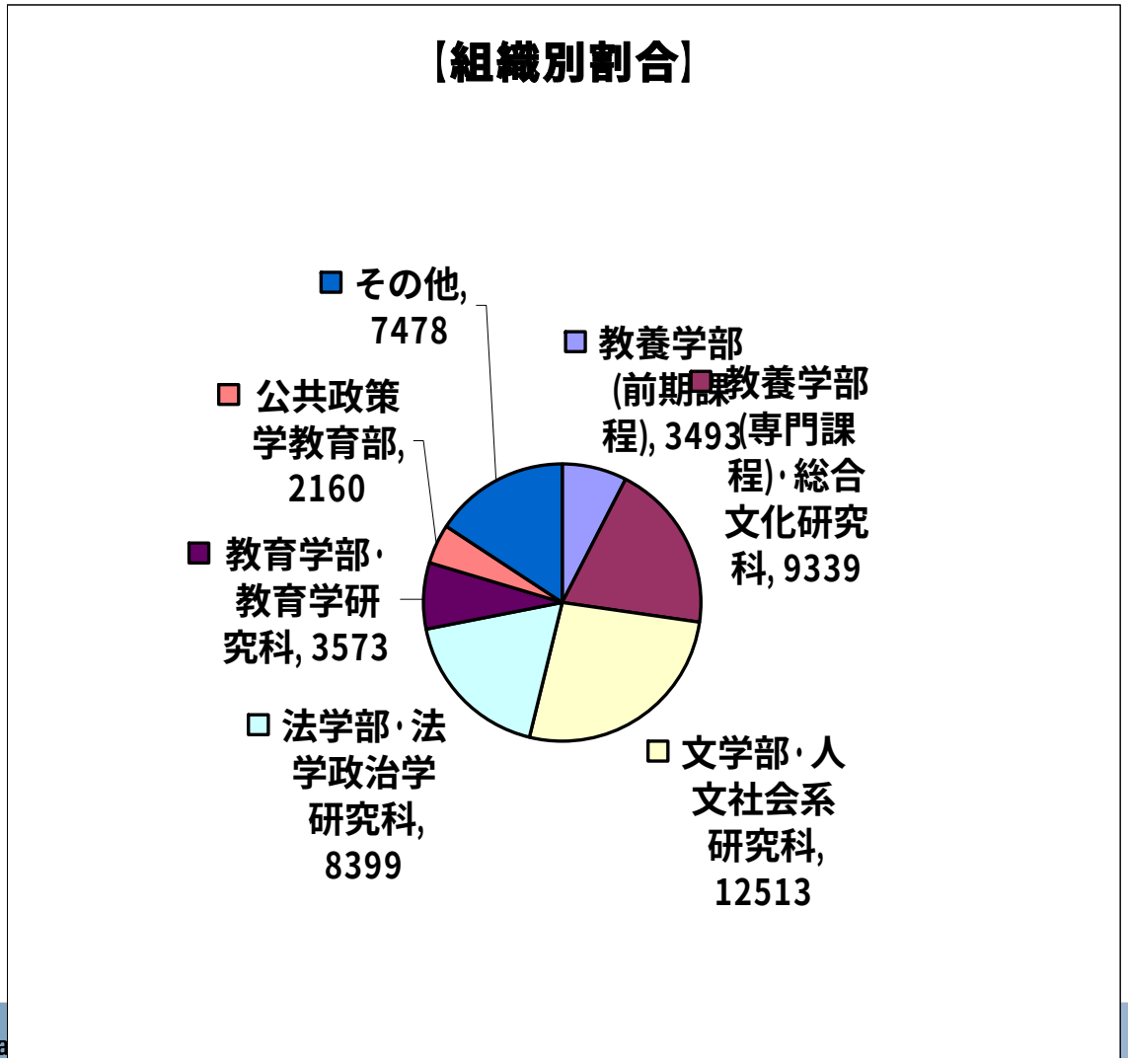
# 総合図書館によるSSL-VPNサービス

- SSL-VPNを認証のGWとして用いる
- ID体系は学内教育用システムが維持管理している
  主に学生･教員を対象としたものを使う
  - おおもとは学籍番号その他。この維持管理は大学（部局）にとって生命線
  - 教育用システムID体系の維持管理には大変なコストと神経を使っている

# 実績



# 掘り起こせば需要は必ずある

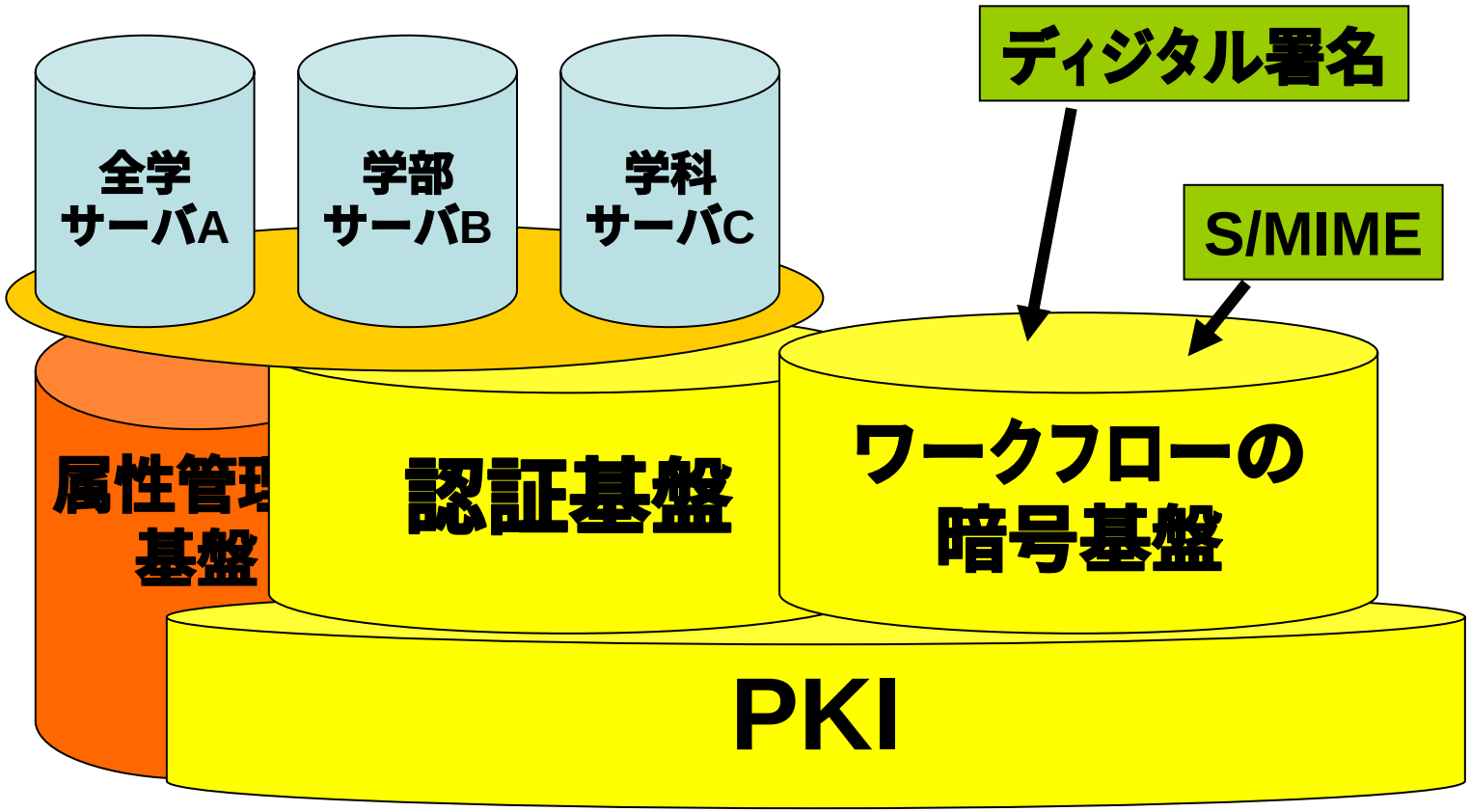


# PKI配備に関する技術的・非技術的な背景

- **PKIの配備を可能にする文化的なバックグラウンドはあるか？**
- **大学という組織の特徴をふまえる**
  - **いろいろな人（身分と属性）がいる。しかも目的を共有している人の集合体としては考えられない**
  - **全体としての組織は大きいが、「学科」相当の小さいコミュニティが作られており、その中ではうまくやっている**
  - **職員の職業に対する倫理は一般に高い**

# 大学にPKIを配備する？

- **目的：何のために？**



# 大学にPKIを配備する目的

- 認証基盤としての期待
  - 正確に言えば、より大きいID基盤・属性管理基盤の整備と、その中のセキュアな部分の整備の一環として
  - 組織のマスターDBの維持管理が生命線
  - 東大は全学的な「共通ID」を採用
  - それからが問題
- ワークフローに使う暗号基盤としての期待
  - 実際に使用を余儀なくされているところがある
  - 半信半疑だが、機能を説明すると期待が膨らむ
  - 実際のワークフローに適用するには、ソフトの熟成その他まだ問題が…

# 実例（想像ではない！）

- A課では
  - 全学サーバにおいて、IDの配布と更新に非常に大きい手間をかける
  - 人事異動がスパイクを見せるときが超繁忙期
- B学部では
  - 他人に見られてはいけない資料・身分によって見られるレベルを設定されている資料がある
  - メールの危険性は熟知（盗聴のほかにも、意図的、非意図的な誤配送を制御できないことなど）
  - これらをいちいち印刷して「親展」で送っていたのでは、ワークフローが効率化できない

# PKI配備のバリア

- PKIに対して拒否感を持つ人がいる
  - 新しい（自分の知らない）技術
  - 自分の上にお役所（CA)がかぶさってくる不快さ
  - その他
- 運用の大変さに関するうわさが定着
  - CAの運用コストが大変（人件費含む）ー本能的に警戒
  - CA運用に関して、請負側との責任・仕事の分界点に納得がいかない
  - 今までのワークフローに異質のものが飛び込み、仕事が増えてしまう（外注でも内製でも）

# 情報基盤センターPKIプロジェクト

- PKIの配備に関する運用回りのさまざまなことに関する調査研究
  - PKIが正しく運用されるか
  - PKIが合理的なコストで運用できるか
  - PKIのご利益は投資に見合うものか
  - 解決を待つ研究的課題には何があるか
- 境界条件
  - 学生証、職員証のICカード化
  - スピードが遅れるときっと致命的

# 方針

- **管理エンティティを自前で運用する**
  - **インソースでの運用に係わるさまざまなことを解決する**
  - **ソフトウェアで解決できることと、人的な要素がからんでくることを峻別する**
  - **運用に当たってのコストを評価する**
  - **→UT-CAを構築して運用実験を行う**

# 方針

- **新しい方向を常に向く**
  - **必要なものは自分で作る**
    - Simple SSO on SSLーVPN
  - **ベンダの製品開発力に期待する（要求を正しくあげるのが大切）**
    - Thin Client**認証と事務端末への採用**
  - **周囲との連携に気を配る**
    - **証明書検証、パス構築と相互信頼モデル**
    - UPKI

# 東大情報基盤センターPKIプロジェクト

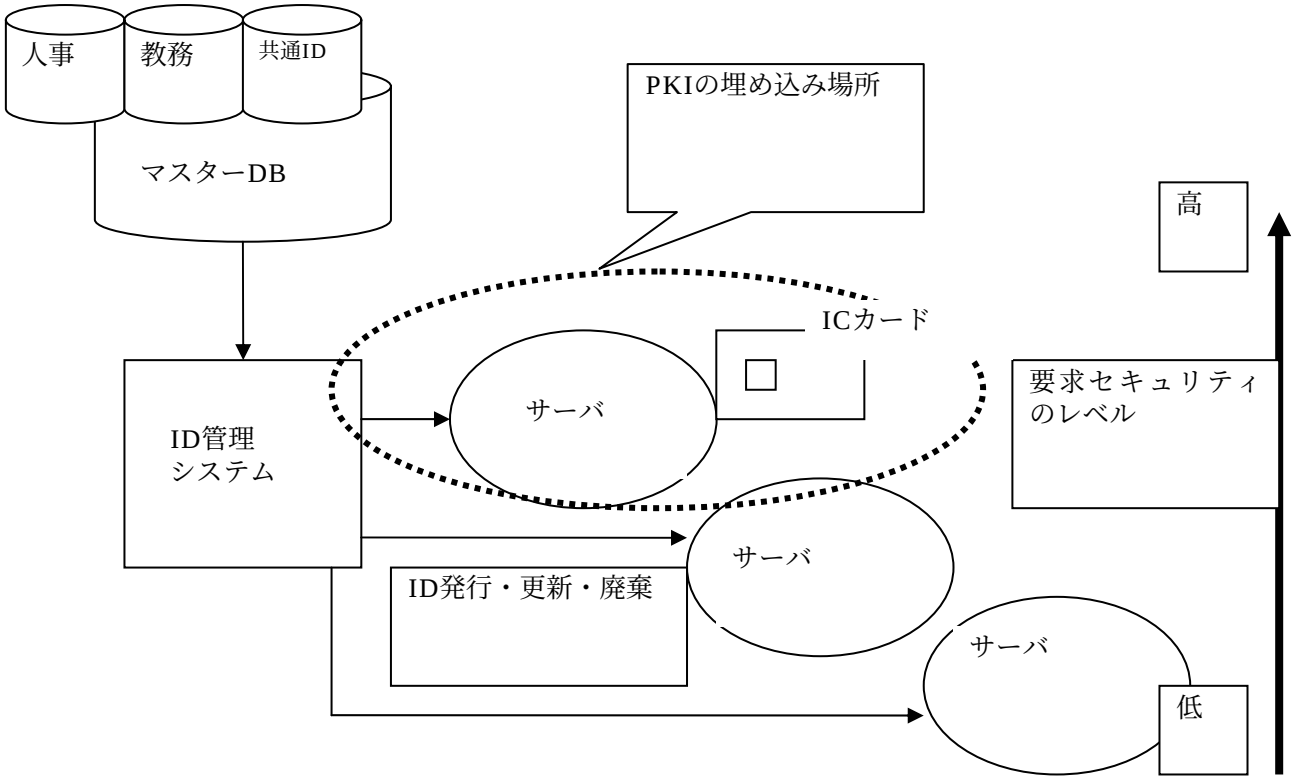
- **東大では、すでにスマートカードはある**
  - **格納メディアに関するコストはとりあえず隠れる**
- **大学の特徴とワークフローを前提とし、それにあわせた運用コストの最適化をさぐる**
  - **研修、試行、デモその他周辺的なことを全部含む**
- **「ご利益」**(Usability) **の提示**
  - Web**認証**、SSL-VPN、S/MIME**など、具体的なアプリケーションの普及と問題点の解決を探る**

# Agenda

1. 東大がPKI配備を計画するまでの経緯
   1. PKI配備に関する技術的な背景
   2. PKI配備に関する非技術的な背景
2. 管理コスト最適化の試み
   1. 大学のワークフローへのはめ込みの試み
3. アプリケーションの問題
   1. 問題の発見
   2. 解決策の提示

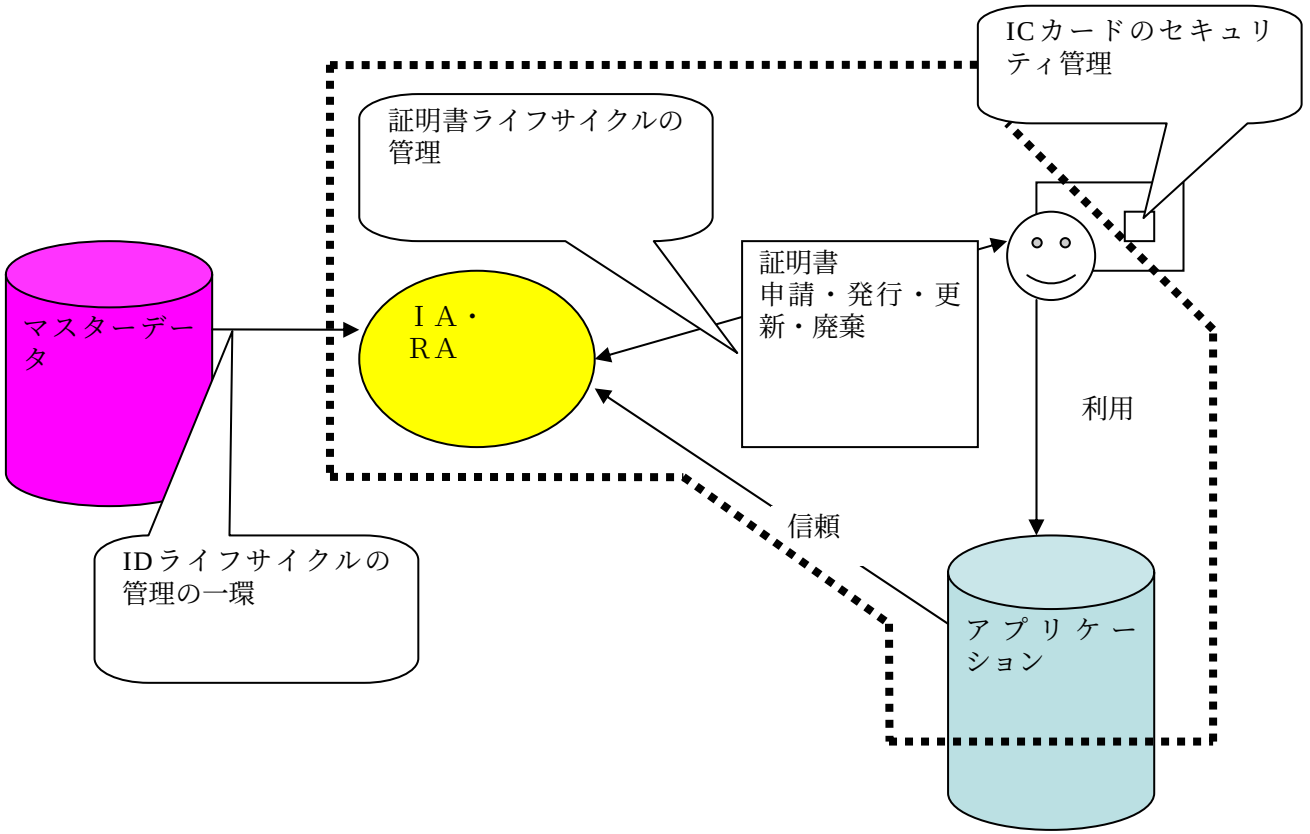
# PKIプロジェクトの立ち位置

- **まずは認証からやる　ーUTーCAの構築**




図．ID管理の枠組とPKIの位置づけ

# 実験範囲



# UT-CA実験の時系列

- 2005.11　UT-CA**設計　発注**
  -- 2006.03 **コンサルティング**
- 2006.07 UT-CA**お披露目デモ**
- 2006.10 S/MIME**対応用にプロファイル変更。主要**MUA**対応確認**
- 2006.11 A**学部**　RA**開設**
- 2006.12 **学内広報に**IA**拇印公開**
- 2006.12 **センター合同**RA**開設**
- 2006.12 CP/CPS**公開**
- 2007.03 **運用の一年延長決定**
- 2007.04 **運用の検査検討と予備検査**

# ＲＡアーキテクチャの検討

- ＣＡの運用では、これが肝心
  - 作業量の観点からも、人の配置の観点からも
  - 「中央に少数のＲＡ」は、大学としては機能しにくい
  - 「小さい単位に多数のＲＡ」はよいアイデアだが、統制がきちんととれることは確認する必要がある。
  - その場合、ＲＡひとつにある程度の人をはりつけるというのは問題外

# 分散ＲＡは機能するか？

- 「統制は十分取れる」ことを推論
- 「作業量」は、従来の仕事にもぐりこませられる（人の管理は学部学科単位で従来から行ってきた）ことから、「隠せる」ことを推論
- 少人数で回す運用モデルをコンサルティングで得て、実地に運用する根拠ができた
  - でも、スマートカードまわりのことを過小評価してしまって…

# 分散RAの設置（現状）

- 組織の数としては3つ。4つめを予定している。実験はそれなりに機能
- うち、2つは合同RA（小規模組織収容のテストを兼ねる）
- RA要員を出してもらって、実際の作業を行なう
- マスタレコードの維持管理は現在手作業

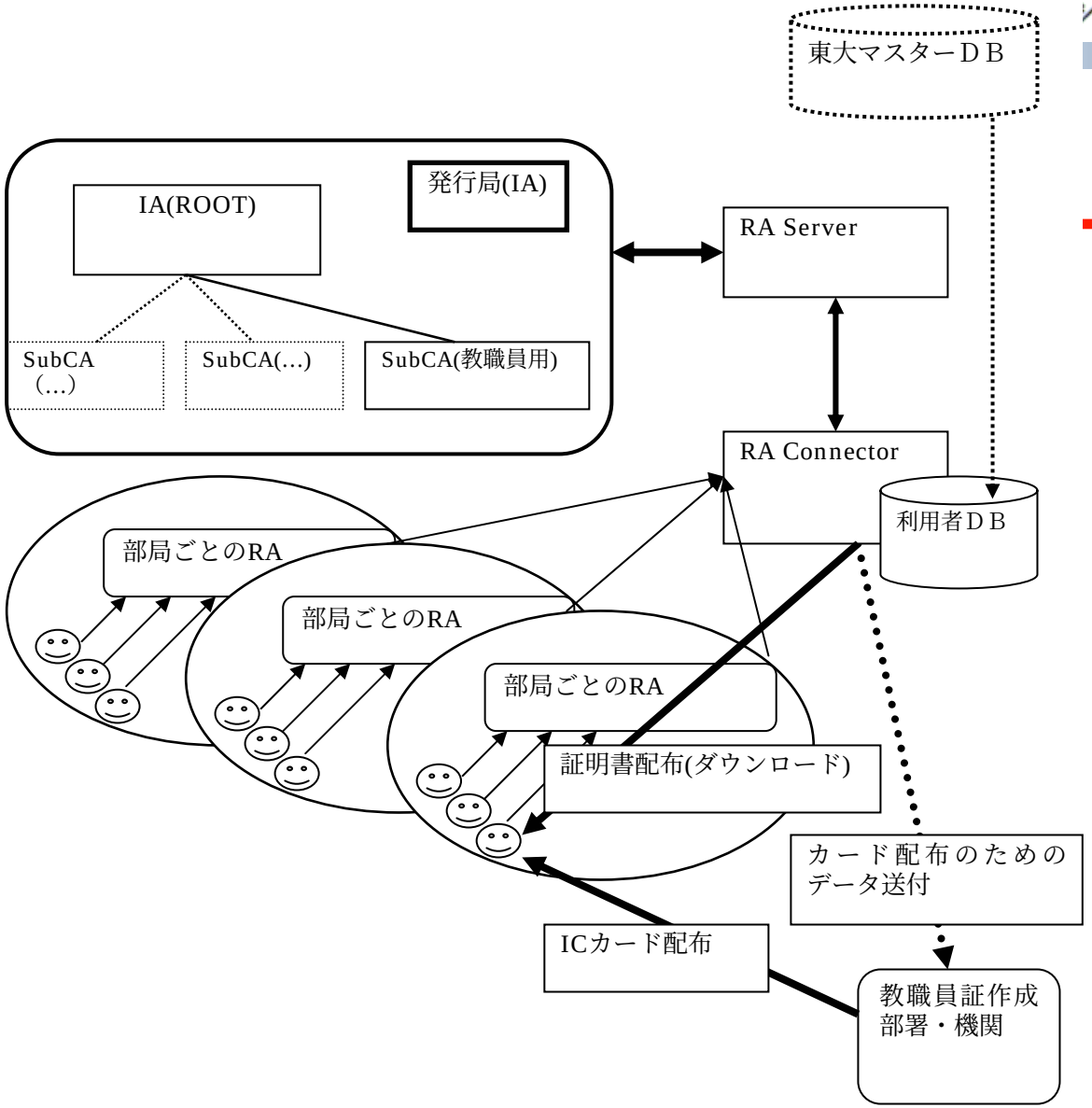



図1. UT-CAのシステムアーキテクチャ

# コンサルティングについてのコメント

- 「コンサルティングは必須」を実感。ただし、する側とされる側に下のような緊張関係が必要

- コンサルティングする側は、大学の内部事情をあまり知らないと理解したうえで、いろいろ聞き出して、解を最適化する努力を。
- コンサルティングされる側は、自らの状況（背景）を丁寧に説明して、丸投げしない覚悟を。

# 運用実績

| | | 発行 | 取得 |
|---|---|---|---|
| A**学部** | RA | 42 | 28 |
| **情報基盤センター合同** | RA | 19 | 12 |
| **合計** | | 61 | 40 |

# 今までの反省

- RAの分散については作業の質・量に関しては理解が得られているようだが、納得するかどうかは、スマートカードに関連する運用管理の最適化にかかっている
- IA,RAの運用は結局はお役所仕事（東大が得意とするところか？）をつつがなくやることが大事だ←ひーひー言いながらこつをつかんだ
- ドキュメントワークが本質的に大変だ←ひーひー言いながら結構大量のドキュメントを書いた

# Agenda

1. 東大がPKI配備を計画するまでの経緯
   1. PKI配備に関する技術的な背景
   2. PKI配備に関する非技術的な背景
2. 管理コスト最適化の試み
   1. 大学のワークフローへのはめ込みの試み
3. アプリケーションの問題
   1. 問題の発見
   2. 解決策の提示

# 問題の発見

- PKIの具体的な応用を見つけることが成功の鍵　ー Usability

- **認証のLOAをあげることについては、すぐにでも適用可能か？**
  - **サーバ側の都合を無視してつっぱしることはできない。サーバ運用側の都合（認証・認可）は実はいろいろある。**

- S/MIMEの需要はどのくらいあるか？
  - **需要はあるが、大学のワークフローにはめこめなければ結局は採用されないだろう**

# First Approach

- **実地に需要を持っている学部のサポート**
  - **証明書発行はUT-CAで引き受けましょう。実際の利用シナリオについて教えてください。というスタンス**
  - Successful
- **既製品をテストする**
- **分野として**
  - **認証**
    - **SSL-VPNサーバを認証GWに用いる　←IPアドレス認証の回避の意味でご利益があがる**
    - **SSOシステムは現在手付かず　←サーバに手を入れられない**
  - S/MIME

# Lessons

- 利用者をかかえている部署との連携は不可欠だと実感した
- 管理側があれこれ考えて、利用シナリオを押し付けてもうまくいかないのではないか
- 利用に当たって問題が生じたら、それを解決すべくいっしょうけんめいにかんがえましょう（解決するのはPKIプロジェクトのミッションのひとつ）

# Usabilityの問題点

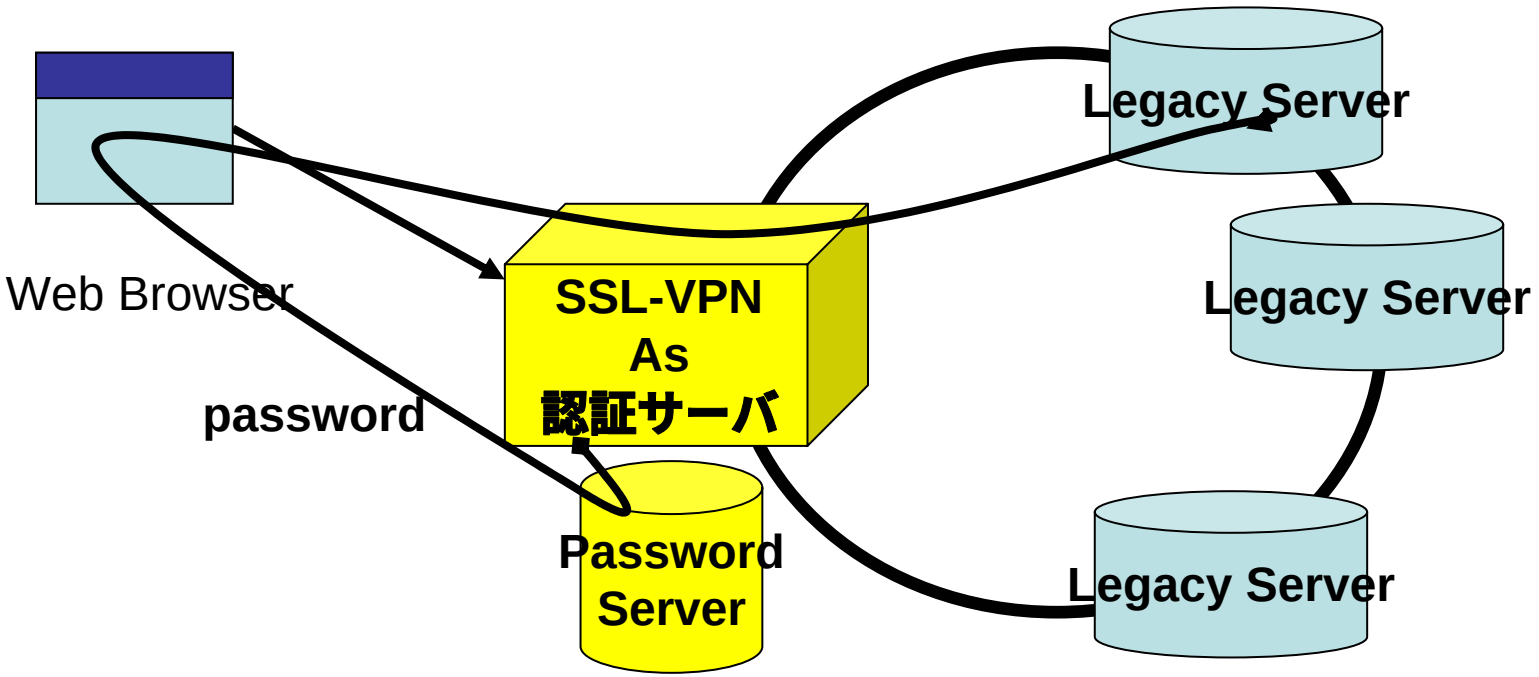
- **署名可能ソフトウェアは、そのままではワークフローを効率化しない**
  - **ワークフロー全体の面倒を見る解の提示**
- **「秘書問題」**
  - **大学のワークフローで本質的な「秘書」を正しく取り扱えないと認証基盤を構築しても役に立たない**
- **「レガシーソフト問題」**
  - Web**認証ができるようになっても、そのままではレガシーソフトの買い替えが進むわけではない**

# Solutions by PKIプロジェクト

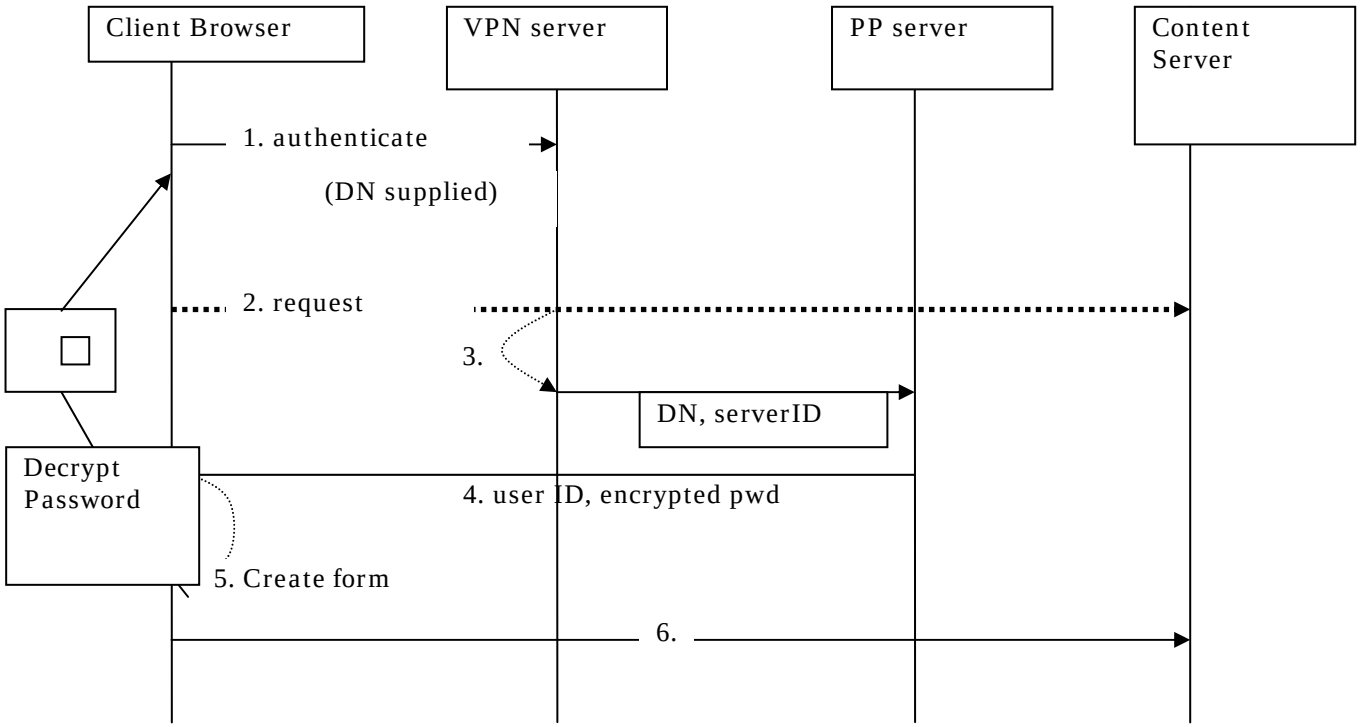
- **「レガシーソフト問題」**
  - **パスワード認証を使うWebソフトに根強い需要**
  - **証明書認証の出る幕なし**
  - SSO**は便利だが、今までの使用ソフトへの対応を間違えると身動きがとれなくなる**
- Solution: Legacy Enabling SSO
  - Client**参加型の**SSO

# LESSO

- 現在、プロトタイプを作成して、テスト中 (もちろん、問題は山積)



# LESSO



# とりあえずのまとめ

- **大学の特徴を前提としたPKI運用の試行**
  - **特徴や需要の調査がとても役立つ**
  - **必要ならコンサルティングを受ける必要**
  - **最適化の余地あり (運用論としておもしろい問題)**
- **Usabilityに配慮したアプリケーションの配備**
  - **必要なら作る覚悟も**