# 東大におけるパブリックサーバ証明書の発行体制の構築

PKIプロジェクト
佐藤周行

情報基盤センター PKIプロジェクト
UT-CA

# Outline

- NIIのパブリックサーバ証明書発行実験
「サーバ証明書発行・導入における啓発・評価研究プロジェクト」

- サーバ証明書発行の意味

- PKIプロジェクトでの対応

# 「サーバ証明書発行・導入における啓発・評価研究プロジェクト」

- NIIが2008年度末までの時限で実施する
  https://upki-portal.nii.ac.jp/cerpj/
- 5月11日より正式スタート
- 目的は「サーバ証明書発行」に関する手続きの最適化

# 「サーバ証明書発行・導入における啓発・評価研究プロジェクト」

- 実験的なプロジェクトであるが、

- 発行される証明書はパブリックなもの
- かかる費用がゼロ

- 事業の継続について、(ある程度)確固たる意思を持っている

# パブリックサーバ証明書の必要性

- パブリックサーバ証明書　～　各種の代表的なブラウザが信頼するルートを持つCAから発行された証明書

- 必要？（かけたお金に見合うメリットがあるか？）

# 必要となるケース

- 互いに「よく知っている」仲間どうしで運用しているアプリケーション（Web含む）のためのサーバ証明書なら必要ないかも

- 「信頼」と、それに関係する技術について理解していない人たちに「自己責任ね」というのは不親切だろう

# 必要となるケース

- 学内外の一般の人に対してサービスしている（大学内におかれているサーバのブランドを保つ意味からも必要）
  - 全国共同利用のためのサーバ
- 学生に対してサービスしている（セキュリティのレベルを適切に保つ意味からも必要）
  - 学生を対象にした学務関係のサーバ

# NII実験への参加

- PKIプロジェクトは、NIIの実施する発行実験に参加することにした。目的は以下のとおり
  - パブリックサーバ証明書で運用するのが適切なところに、サーバ証明書を配布する（費用ゼロの恩恵）
  - パブリックサーバ証明書がほしいところに適切なセキュリティレベルで審査を行うための体制の構築をはかる

# 体制構築の方針

- 「統制」すべきもの　－　パブリックなものなので、発行に際してはそれなりの保証が必要（ルートのブランドの維持）
  - ドメインが適切に管理されていることの保証
  - 申請が正しい人からあがってくることの保証

- 従来の学内ネットワーク管理体制
  - UTnetがもっとも適切
  - ただし、ドメインの管理そのものに責任を持っているわけではない

# 体制構築の方針

- 一義的には、PKIプロジェクトが責任を持ってNIIに申請する

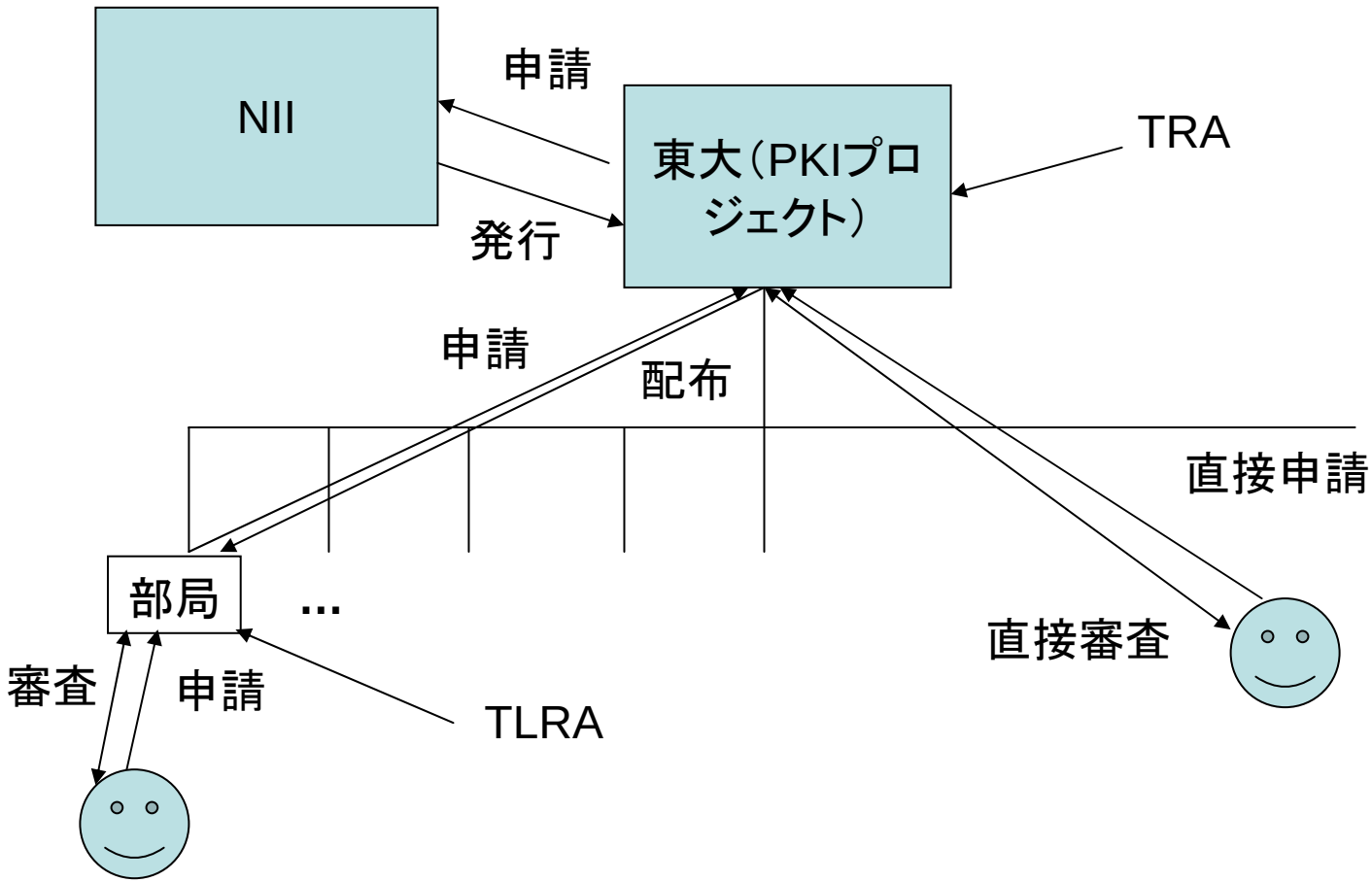
- PKIプロジェクトでカバーできる範囲には限界がある
  - 地理的な限界
  - 人間関係の限界

# 今回の実験での「解」

- Utnetの協力なしには回らない(とりあえずやってみようか)
  - 人の管理　⇔　総務系
  - マシンの管理　⇔　ネットワークの管理をしているところ
- UTnetがいままで築いてきた運用管理体制の上にのっからせてもらう(もし、今後協力を本格的に考えてもらえるのなら感謝！)
- ドメインの管理体制とUTnetの管理体制が(偶然)一致した部分については、信頼できるものと考える

# 今回の実験での「解」

- PKIプロジェクトは、
  - 申請者の本人確認と
  - サーバ(のFQDN)が、その部局に設置するのが適切かどうかの審査をおこなう
  - 東大のもつ「ブランド」の維持
- 審査が同程度に厳密に行われると判断した場合、UTnet部局担当者(が望めば)に委譲することがある
  - 審査に要するコストの最適化
  - 審査の厳密さは保たれる



# 現在のステージ

- TLRA設置のための基準と、ガイド、各種帳票類の作成　ー参加キット
- テスト的に数部局に打診（運用回るかな？）

- NIIの実験正式開始にあわせて、参加キットの公開

# 将来の体制

- 以下の意味で、今回の実験のアウトプットは重要
- パブリックサーバ証明書の需要に応えるために、全学的な組織を作ることの是非については、以下をさらに検討する必要がある
  - バルクで交渉することで、コストがどのくらい安くなるか
  - 「組織」の維持管理にどのくらいコストがかかるか