# 東大におけるパブリックサーバ証明書発行体制の運用

2007/09/03

情報基盤センター
PKIプロジェクト
佐藤周行

# 内容

- 発行の背景
  - 大学における利用シーン
  - 現状
  - 国立情報学研究所のプロジェクト
    - 方針
    - 発行される証明書の利用
- 体制の構築と運用の実際
  - 体制構築に当たっての方針
  - TRA（東大登録局）のポリシー
  - TLRA（部局登録局）の設置

# 発行の背景　－大学における利用シーン

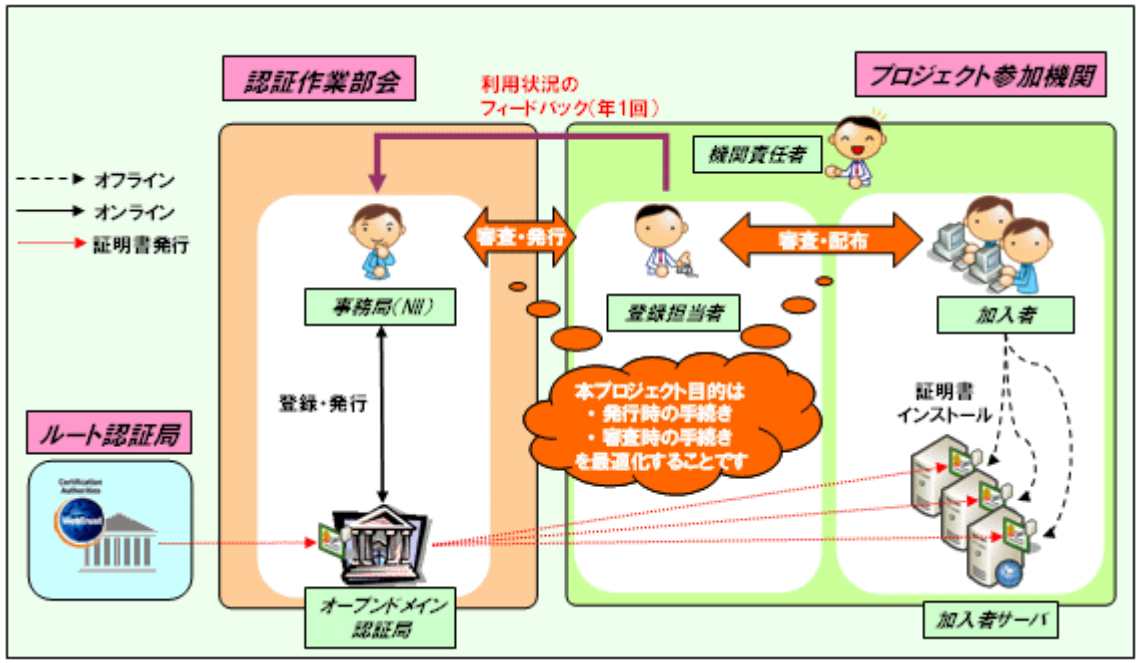
- サーバ証明書で何ができるか
  - SSL暗号路の設定
  - FQDN（ホスト名）で指定したシステムがドメインの管理下のもとに実在する。
- 利用シーン
  - マシンの身元確認が強く求められるとき
    - 例：Phishing対策
    - 例：オフィシャルサイトからのオフィシャルアナウンス（注意：オフィシャルアナウンスの内容を保証するのは別問題）
  - 暗号路の設定が強く求められるとき
    - 例：成績報告、成績閲覧などの教務関係
    - 例：財務管理
    - 例：人事関係教授会資料の閲覧など

# 発行の背景　－現状

- 必要な部局が、個々に証明書を取得
  - ドメインu-tokyo.ac.jp全体の統制なし
  - （証明の強さによって金額に差はあるが）微妙に負担にならない額になっている。
- 自己署名のサーバは（あるのだろうけど）特に目立つわけではない
  - それなりに良好な状態
  - 自己署名のサーバを設置し、学生に使わせているところは、すぐこのパブリックサーバ証明書に移行を！（リテラシー上問題が大きい）
- しかし、必要なところに必要な分だけ証明書が発行されているかどうかについてはよくわからない

# 発行の背景　ー国立情報学研究所のプロジェクト

- https://upki-portal.nii.ac.jp/cerpj/
- 「無料」でサーバ証明書を発行する
- プロジェクトの目的は「発行の手続き・審査の手続き」の最適化



# 発行の背景　－プロジェクトの特徴

- 証明書発行ベンダーのおこなっている「Managed PKI Service」のNII版と考えてよい
  - NIIは、発行審査の実質を参加機関にほぼ完全に移譲する方針を立てている
  - 東大は情報基盤センターPKIプロジェクトが移譲先になった
- 証明書の有効期限は2009年3月31日まで
  - それ以後については公式にはノーコメントであるが、非公式には「ポジティブに考える」旨の発言をしている
  - 2009年度以降も何らかの形で継続すると考えてよい（主催者、形態、料金その他については変更があるかも）

# 発行の背景　－発行される証明書の利用

- NIIの正式なアナウンスは以下のとおり
  - サーバ
    - APACHE > 1.3.33 + SSL 1.55
    - IIS  5.0, 6.0
    - IBM HTTP Server > 6.0.2
    - Jakarta Tomcat 4.1.31, 5.0.30
  - ブラウザ
    - IE > 5.5(Windows) > 5.2(Mac)
    - Firefox > 1.0
    - Safari > 1.2
    - Opera > 7.6
- 正式でない場合（たとえば携帯）は相談してください

# 体制の構築と運用の実際（全体方針）

- 体制構築に当たっての方針
  - 審査の権限と責任は情報基盤センターPKIプロジェクトが負う
    - サーバ（責任者）の実在性確認
    - ドメインが合理的な統制の下にあることの確認
  - 実際には、UTnetの組織に乗っかる
- 必要に応じて権限の委譲を行なう
  - 部局には部局のロジックがあり、それでUTnetがつつがなく運用され続けている
  - 特にサーバの実在性確認の審査については、部局に積極的に委譲する

# 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

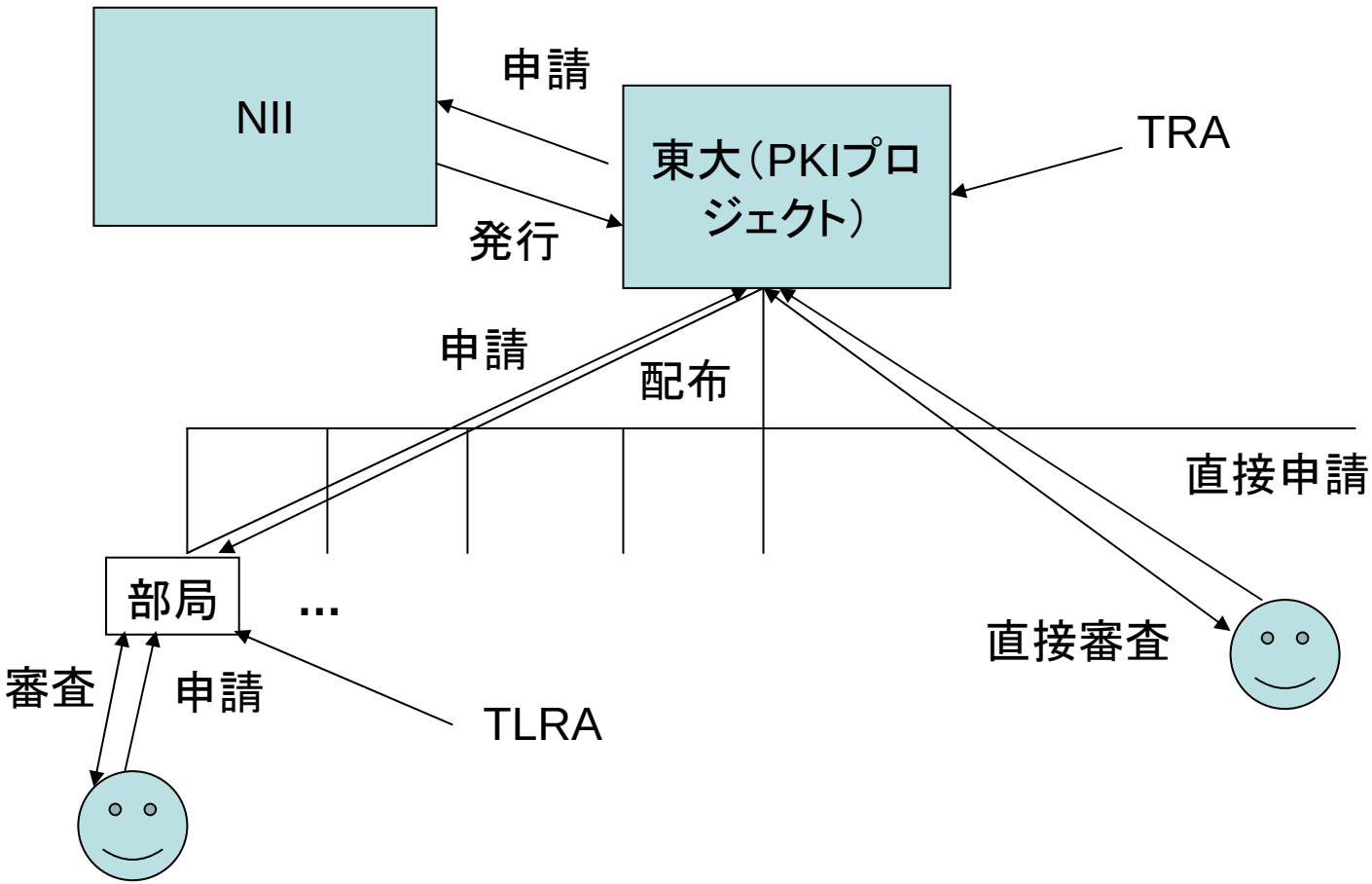
- 一義的には、PKIプロジェクトが責任を持ってNIIに申請する

- 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

# 体制構築の方針

- 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」の維持に注意を払う
- 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ことの保証を求める

# 体制構築の方針



# TRAの運用ポリシー

- http://www.pki.itc.u-tokyo.ac.jp/cerpj/htdocs/document/TRA-CPCPS-1.01.pdf にかいてあるとおり
- 職員証による対面での本人確認
- 申請者が申請資格をもっていることの確認
- ドメインの統制がとれていることの確認

- 以上を、書類、書類がそろわない場合は適宜面接を用いて確認する
- 定期的に検査を行なう

# TLRAの設置

- 部局ごとにきちんと統制が取れていれば、審査を委譲することができる。具体的には

- 部局がそこに属する東大加入者を統制できる体制にあることの審査
- TLRA の審査体制の構築に関する審査
- 部局が東大加入者の属するドメインを統制できる体制にあることの審査
  - DNSの統制の確認

# TLRAの設置

- 証明書取得以外についても（根性論になりますが）以下のご利益があります
  - サーバ管理・運用についてのルールの明確化
  - サーバ管理・運用に携わる人の「棚卸」
  - DNS管理についてのルールの明確化（明文化することをお勧めします）
  - Guru（たち）がいて「その人の主張が絶対」というのは組織としてあまりよくないだろう

# TLRAの設置

- このような場合は、TRA（PKIプロジェクト）に直接相談してください
  - 「部局」でない場合
  - 証明書が1枚程度しか必要でないとき
- このような場合は、TLRAを設置するのが合理的です
  - 証明書が複数枚必要になることがわかっているとき
  - UTnet部局担当者として、DNS等ネットワークの管理を順調にまわしているとき

# TLRAの設置

- 現状では＞10枚証明書を発行し、TRAが直接審査を行なったのは全体の1/3程度

- TLRAは以下に設置されている（証明書がほしい場合は担当者に連絡を）
  - itc.u-tokyo.ac.jp
  - k.u-tokyo.ac.jp
  - hi.u-tokyo.ac.jp
  - adm.u-tokyo.ac.jp

# TLRAの設置

- 今回のセミナーを聞いたならば、具体的な統制のしかたについてはこつがつかめたはずです（特に日々の運用と監査対策について）。
- それでもまだ何か不安だ、という人は以下を参考にすることができます。http://www.pki.itc.u-tokyo.ac.jp/cerpj/htdocs/document/TLRA_example-1.0.pdf
- TRAのCP/CPSにしたがって、年1回以上の内部検査を行ないます

# 書類の提出先

- 審査は現在書面で行なっています
- 必要なフォームはhttp://www.pki.itc.u-tokyo.ac.jp/cerpj/index.html にあります。

- 申請の書類と添付書類は「情報基盤センターPKIプロジェクト」宛に学内便で送ってください。
- 事前相談等、全般については、以下のアドレスで受け付けています

PublicServerCertificates@itc.u-tokyo.ac.jp