パブリックサーバ証明書発行プロジェクトのご案内

2007年10月25日

情報基盤センター PKIプロジェクト

西村　健

内容

- プロジェクト概要
  - 背景
  - 現状
- UTnetとの連携
- 実際の手続き等

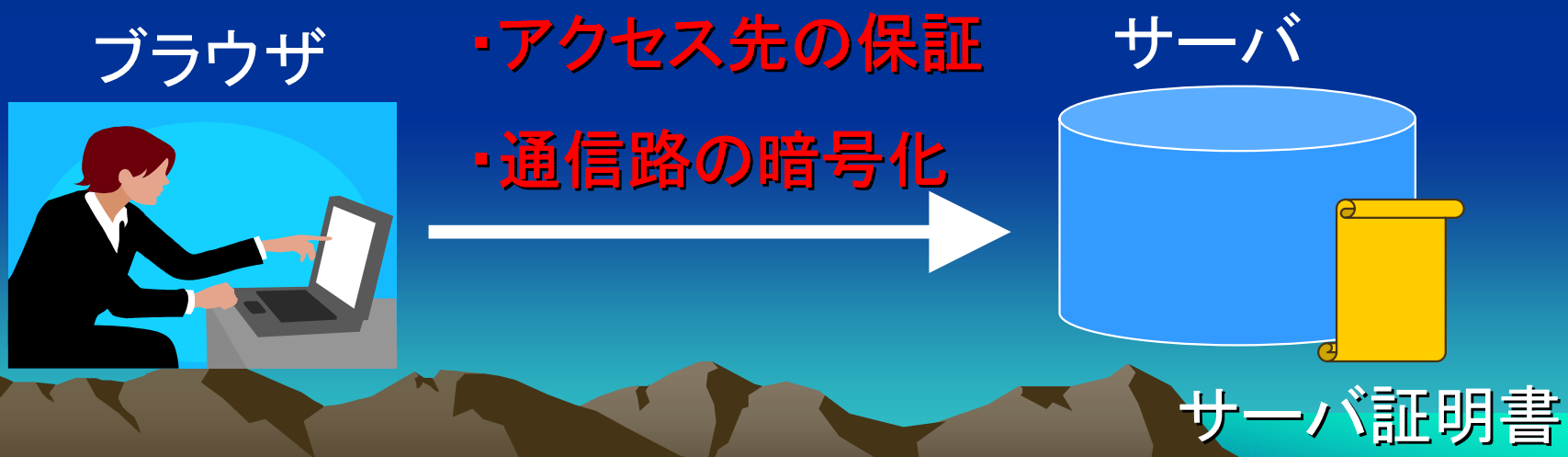
プロジェクト概要

- プロジェクト名を元にした説明

パブリック な サーバ証明書 を 発行 する

「サーバ証明書」

- （主にWebブラウザから）サーバへのアクセスの際にアクセス先を保証するためのもの
- （ついでに）暗号化も可能
  - 通信路の暗号化を行なうためにはサーバ証明書が不可欠



「パブリック」

- 世の中にあるブラウザにあらかじめ発行元認証局が登録されているということ

→これがないと初期状態でアクセス先を確認することができない！

⇔プライベート認証局

  - 利用場面にもよるが、Web利用者へのコスト増、リテラシーの面からあまり好ましくない

「発行」

- 実は東大内からの申請のとりまとめ役
- 背景：国立情報学研究所(NII)が全国の大学を対象にサーバ証明書を（今のところ）無料で発行している
- UTnetの組織に協力していただく形で実現する

プロジェクトの目標

- 業務的側面
  - パブリックサーバ証明書を安価に提供
  - 潜在的需要の開拓
  - 利用者の意識向上
- 実験的側面
  - 東大内での厳格な審査・発行体制の確立
  - 審査手続きの効率化

これはNIIのプロジェクト全体の目的でもある

現状

- 個々に商用認証局に申請

もしくは

- 自己署名証明書、プライベート認証局からの証明書で運用
  - あなたの部局にそんなサーバはありませんか？

問題設定

- なるべく少ないコストで
- 厳密な審査を行なう
  - 何か問題が起きれば「ブランド」の失墜につながる

証明書発行時に確認すべきこと

（括弧内は例）

- 申請者の本人確認
  - （職員証による対面での本人確認）
  - （申請者が申請資格を持っていることの確認）
- FQDN(ホスト名）で示されるサーバが組織に属し実在するものであることの確認
  - （ドメインの統制が取れていることを書類をもって確認する）

UTnetとの連携

- 東大規模の組織で、申請者・サーバの審査を一ヶ所で行なうのは非現実的
- 既存の組織であるUTnetの部局担当者に審査を委譲する形態をとる
  - カバーできる範囲は一部（後述）
  - 特にサーバの実在性確認の審査については積極的に委譲する

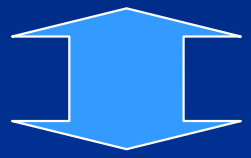
ネットワーク管理とドメイン管理

- UTnetはネットワークを管理する組織である
  - 部局主体
- ドメイン管理のための組織は存在しない！
  - UTnetと重複する部分も多いかもしれないが

- 部局に割り当てられたドメイン（1部局1ドメイン）と部局ネットワークを一組にしてUTnet部局担当者に委譲する
  - それ以外の部分は例外として扱う

ドメイン管理体制の明確化（１／２）

- UTnet（の部局担当者）はネットワークに接続されている機器に対する責任は持てるが、ドメイン管理の責任は持てない（原則的に）



- サーバ証明書発行にはドメイン管理も重要

- ドメイン管理体制を明文化して提出いただき、その審査をもって代替とします

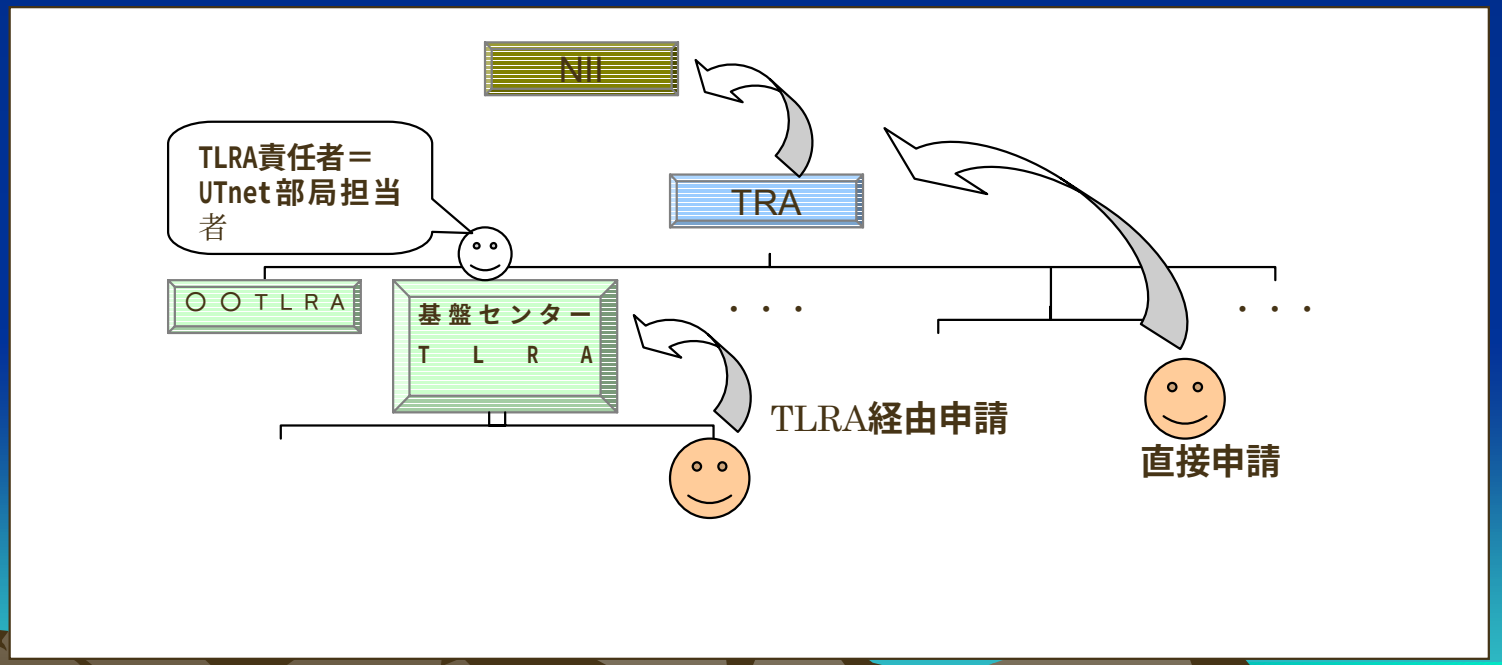
ドメイン管理体制の明確化（2／2）

- 管理体制の明確化とは例えば
  - DNSサーバの管理者権限を持つものは誰か（どのようにして決定されるか）
  - どのような申請の元にどのように登録を行なうか

- 証明書を取得する･しないに関わらず、管理体制を一度明文化してみることをお勧めします！

発行体制の概要

- 実際に証明書を発行する機関 – NII
- 東大での窓口 – TRA
- 部局での窓口 – TLRA
- NII – TRA - TLRAの階層



TLRAの設置手続き

- 以下の書面での提出をお願いしています。
  - 審査委任願
  - TLRA責任者が対象部局のUTnet部局担当者であることを示す文書
  - 対象ドメインが対象部局に割り当てられたものであることを示す文書
  - TLRAが受け付ける申請の申請者の本人確認を行なう体制を示す文書
  - 対象ドメインおよびその下のサブドメインについて、名前付けがその部署の意思を正しく反映できる体制にあるかどうかを審査できる体制にあることを示す文書
    （DNSの管理体制、IPアドレスの管理体制等。管理下にあるサブドメインが全体のうちの一部である場合はその旨明記すること。）
- 書類を用意することが困難な場合は面接で確認します。

商用認証局のアプローチとの比較

- 商用認証局の審査には、組織の実在性から確認するものから、メールの到達性のみで確認するものまで千差万別

  ⇔このプロジェクトではコストを抑えつつかなり厳密に確認できる

- コストの集約化

動作環境

- サーバ
  - Apache（mod_ssl）※1
  - Apache-SSL※1
  - Microsoft Internet Information Server5.0
  - Microsoft Internet Information Server6.0
  - IBM HTTP Server 6.02以上
  - Jakarta Tomcat※2

  ※1 Apache（mod_ssl-2.8.25-1.3.34）、apache_1.3.33 + ssl_1.55で動作を確認
  ※2 Jacarta Tomcat 4.1.31、Jakarta Tomcat 5.0.30で動作を確認
- ブラウザ
  - Netscape Communicator 4.78 以上
  - Netscape Communicator 7 以上
  - Microsoft Internet Explorer 5.5以上
  - Microsoft Internet Explorer（MacOS） 5.2 以上
  - Opera 7.6 以上
  - Firefox 1.0 以上
  - Safari 1.2.2 以上

- アクセスが携帯等の場合はご相談ください。

CP/CPSについて

- 電子証明書発行にあたっての発行対象等を明確化
- 要は「ちゃんと管理すること」が求められている
  - 発行体制（TLRA責任者）に対しても
  - 証明書を導入するサーバ管理者に対しても
- 厳密であるがゆえに長文

すでにいくつかの部局でTLRAが運用されています

（あのサーバも実は･･･）

新たにサーバ証明書を取得する場合や、既存の証明書を更新する場合に、このプロジェクトを検討対象の一つにしていただければ幸いです

お問い合わせ

- http://www.pki.itc.u-tokyo.ac.jp/cerpj/

お気軽にお問い合わせください。