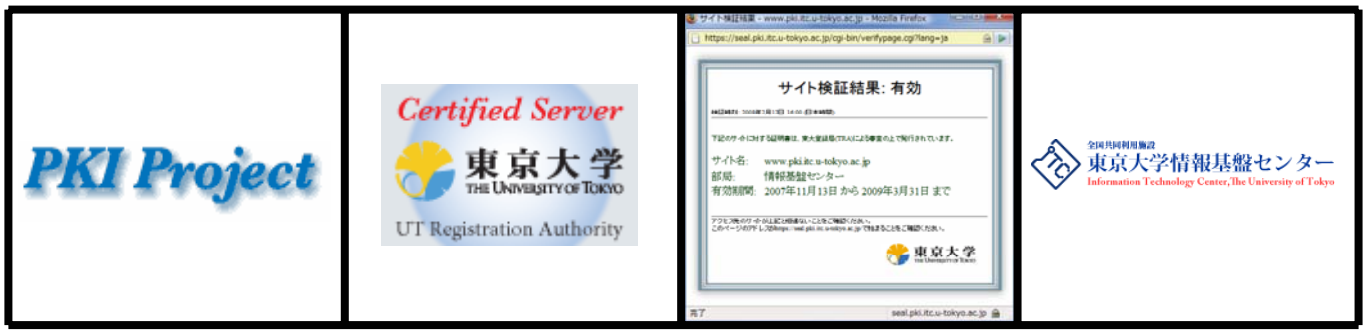
東京大学におけるパブリックサーバ証明書発行プロジェクトについて



大島大輔（発表者）・西村健・佐藤安一郎・佐藤周行
東京大学情報基盤センターPKIプロジェクト

2008年3月10日（月）
平成19年度核融合科学研究所技術研究会
第四分科会<計算機・データ処理>
岐阜県土岐市・セラトピア土岐

概要

- 情報基盤センターPKIプロジェクトは，国立情報学研究所(NII)主催の「サーバ証明書発行プロジェクト*」に参加しています
- PKIプロジェクトが本学の受け口となり，東大ドメイン(u-tokyo.ac.jp)のサーバに対してパブリックなサーバ証明書の審査・発行を担当しています
- 本セッションでは，PKIプロジェクトが行っているサーバ証明書の審査・発行業務，および2008年2月から開始したサービス（東大シール）についてお知らせします

本セッションのキーワード

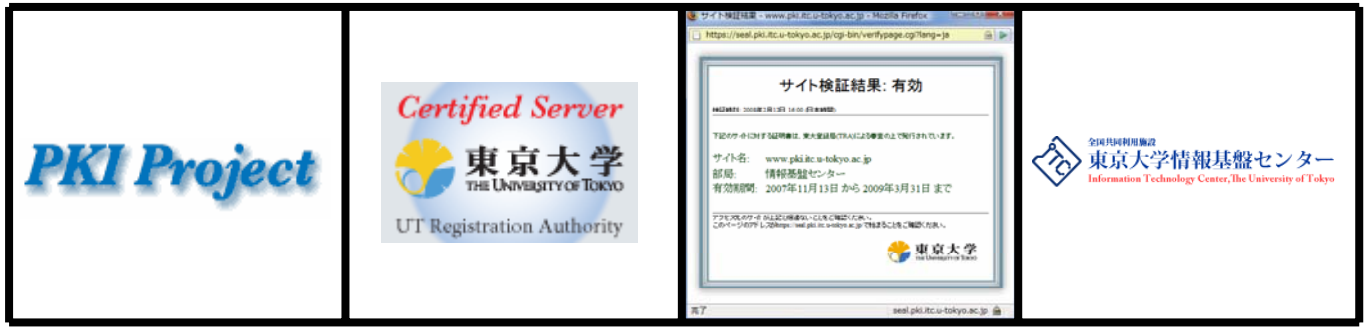
「サーバ証明書」
「PSC(パブリックサーバ証明書発行プロジェクト)」
「東大シール」

* NIIのプロジェクト正式名称：「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」

アジェンダ

1. サーバ証明書とは？
2. パブリックサーバ証明書発行プロジェクト発足の背景と目的
3. プロジェクトが実施してきたこと
4. 東大シール
5. プロジェクトの課題と今後

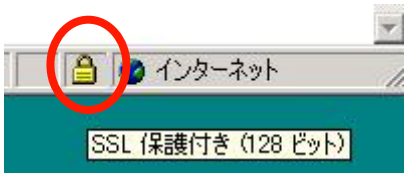
1．サーバ証明書とは？



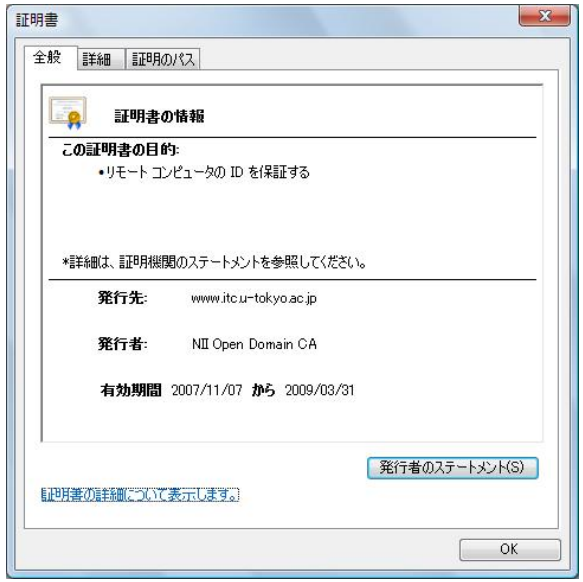
サーバ証明書とは？

1. サーバが実在しているということを証明するもの

IE7の場合



←IE6の場合はウインドウの右下に鍵がある



2. データを暗号化し，通信路上での盗聴・なりすましがないことを保証するもの

サーバ証明書の確認方法（IE7編）

1.

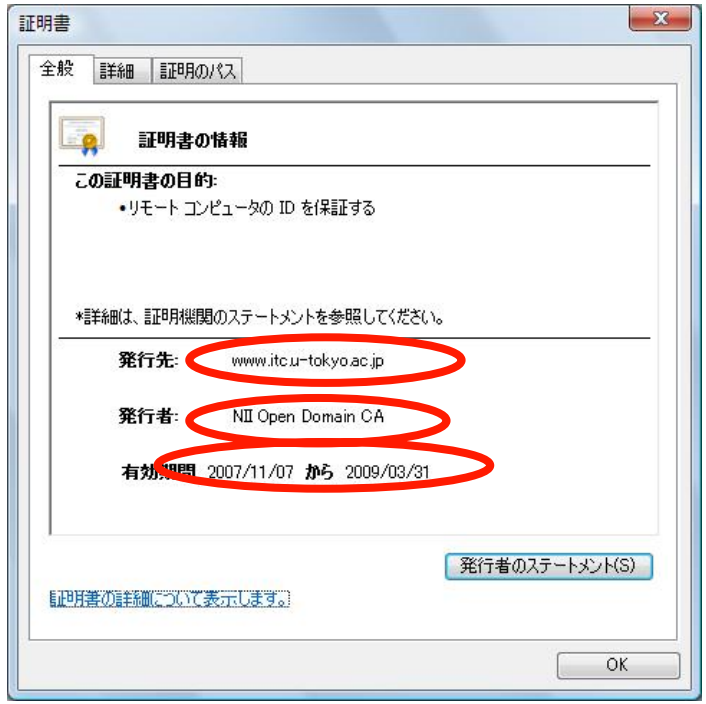
サーバ証明書がインストールされているWebページにアクセスし，南京錠のような鍵マークをクリック

2.

図の1番下にある，「証明書の表示」をクリック

3.

サーバ証明書の確認



ただし，この確認方法では分かりづらい！！
⇒後ほど，分かりやすいサーバ証明書の確認方法について，本プロジェクトの新サービスをご紹介します

なぜサーバ証明書が必要か？

- 利用者（Webページ閲覧者）に対してWebページの実在性を証明し，安心して利用してもらうため
- 世の中には，フィッシング（※）目的の悪意のあるWebページが多数あり，それを見極めるため

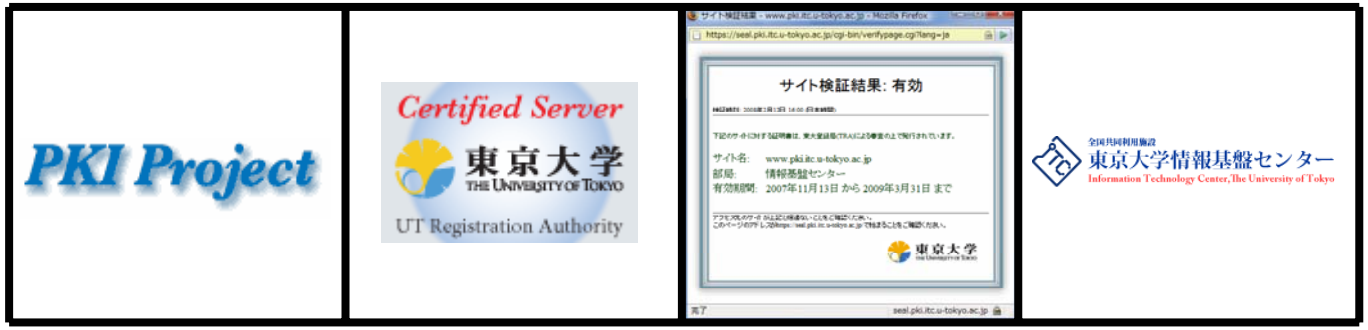
・・・などといった理由が挙げられる

※主に個人情報を詐取する目的で作成されたWebサイト

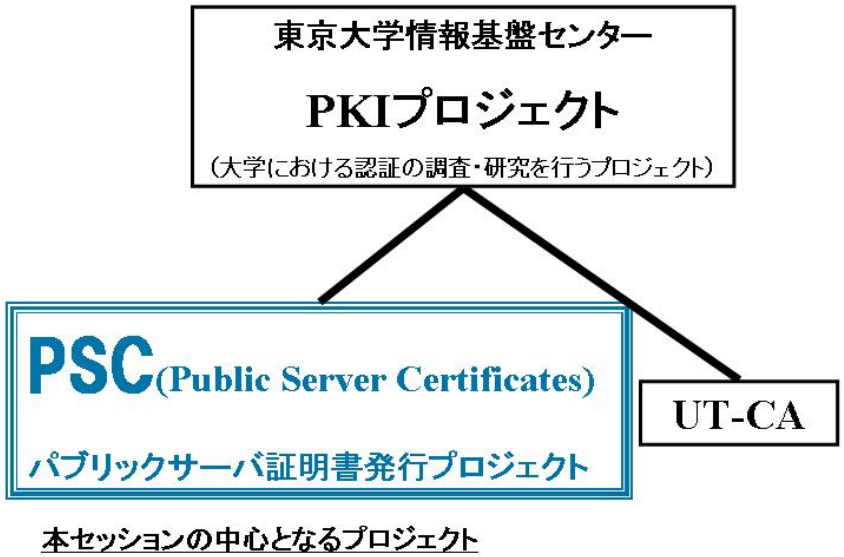
フィッシングサイト事例

- 某大手都市銀行のオンラインバンキングサイトを偽装（2005年）
- 某大手オークションサイトを偽装（2007年）

2．パブリックサーバ証明書発行プロジェクト 発足の背景と目的



PKIプロジェクトとパブリックサーバ証明書発行プロジェクト(PSC)の位置付け



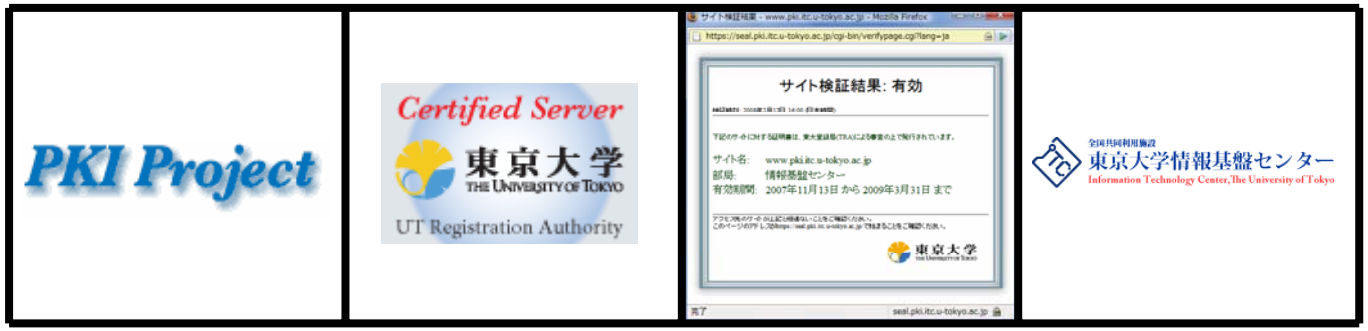
情報基盤センターでは，大学における認証の調査・研究を行うプロジェクト（PKIプロジェクト）を2005年1月に立ち上げ，そのサブプロジェクトとして，PSCを2007年5月に開始した

パブリックサーバ証明書発行プロジェクト発足の背景と目的

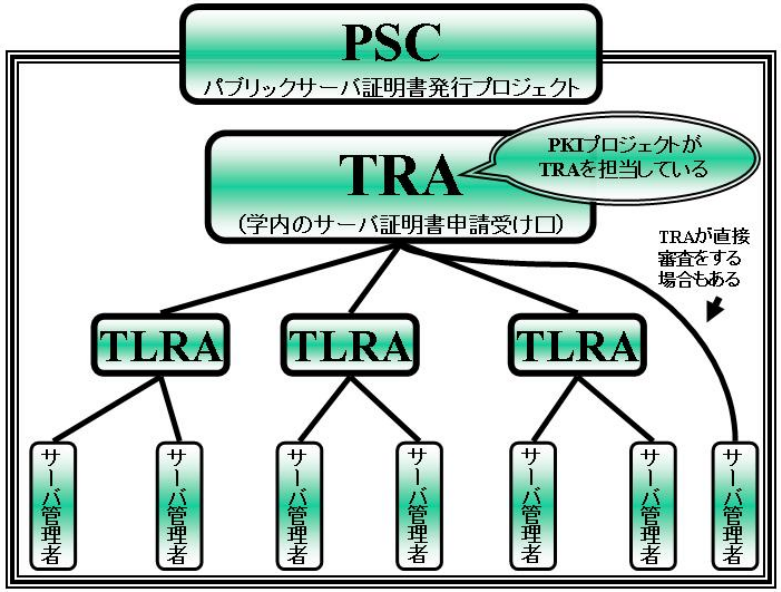
- **背景**
  - 本学では部局（学部，研究科，研究所，全学センター等）や研究室ごとにサーバを管理しており，パブリックなサーバ証明書を必要とする場合も部局のサーバ管理者が商用認証局に直接申請している
  - 部局によっては，パブリックなサーバ証明書を必要としている場合も，予算面等の理由で取得していない場合がある（発行する会社によって違うが，サーバ証明書1枚で数万円から数十万円の費用がかかる）

- **目的**
  - 部局担当者が直接商用認証局にサーバ証明書を申請する手間を，PKIプロジェクトが代わりに担当する。また，適正な管理をしているサーバに，正しい手順でサーバ証明書を発行することができる体制の構築を目的とする
  - 今回のサーバ証明書は2009年3月までは費用がかからないため，財政的な負担を軽減させることができる。また，信頼できるサーバ証明書を使うことでWebサーバ等の信頼性向上とサーバ管理者やWeb閲覧者のリテラシーを向上させる

3． プロジェクトが実施してきたこと



TRAとTLRAの設置



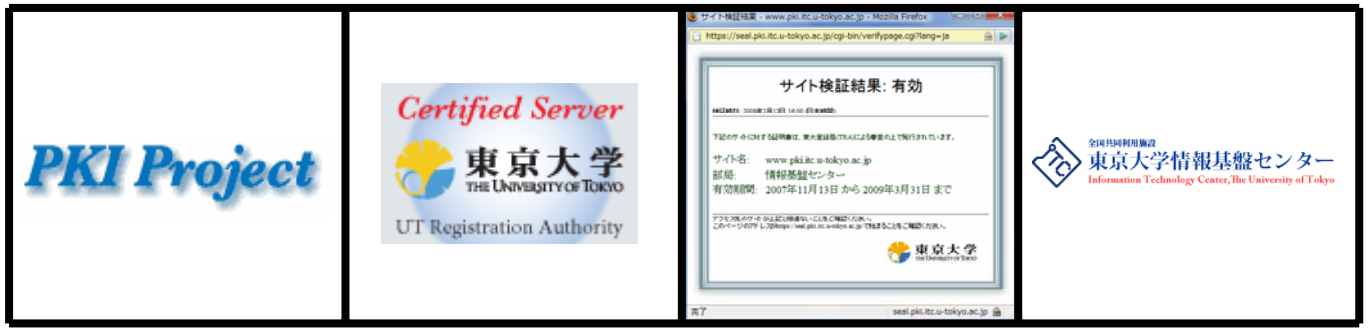
- 学内のサーバ証明書申請受け口として，TRA（東大登録局:The University of Tokyo Registration Authority）を立ち上げた。TRAはPKIプロジェクトが担当している
- ただし，TRAが東大規模のサーバ管理者に対して，個別に審査を行うことは現実的ではないと考え，TRAの支部として，TLRA(東大部局登録局:The University of Tokyo Local Registration Authority)を設置した

サーバ証明書の発行状況および利用している部局

- サーバ証明書発行状況
  - 2008年3月5日現在での申請を含む発行枚数は，65枚
- サーバ証明書を利用している部局（一例）

部局名	ドメイン名	主な利用目的（動機）
史料編纂所	hi.u-tokyo.ac.jp	1. コンテンツの保護 2. 第三者機関からコンテンツの存在を証明して欲しい
新領域創成科学研究科	k.u-tokyo.ac.jp	1. 電子掲示板での利用 2. 学生や教員への公的な連絡手段としての責任

4．東大シール



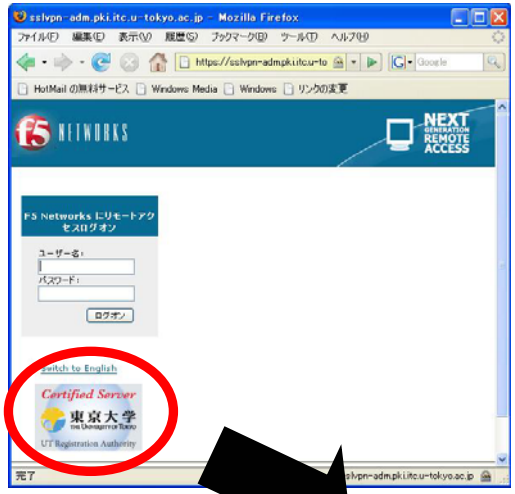
東大シール

- PKIプロジェクトでは，サーバ証明書を可視化（見える化）するサービスを開始しました
- 名称は「東大シール」です

東大シール

どのように利用するか

1.
PSCのサーバ証明書を使用している東大ドメインのサイトは，東大シールを表示することができます



2.
Webサイト閲覧者は，東大シールをクリックしてサーバの実在性を検証します

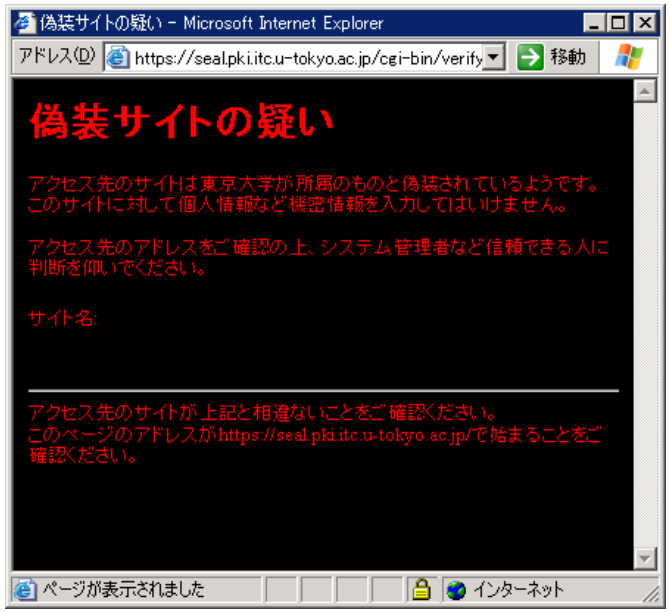
3.
ウインドウがたちあがり，サーバの実在性が検証できました

東大シールの表示方法

- 東大シールの表示方法は非常に簡単です。以下の行をHTMLファイルの適当な位置に挿入するだけです
- ただし，TRAが審査し，サーバ証明書を発行したサーバでなければ，東大シールは正しく表示されません

```
--
<script src="https://seal.pki.itc.u-tokyo.ac.jp/writeseal.js"
type="text/javascript"></script>
<noscript>
<div><a href="https://seal.pki.itc.u-tokyo.ac.jp/cgi-
bin/verifypage.cgi" target="_blank"><img
src="https://seal.pki.itc.u-tokyo.ac.jp/cgi-bin/seal.cgi"
border="0" /></a></div>
</noscript>
--
```

勝手にソースを貼り付けられても



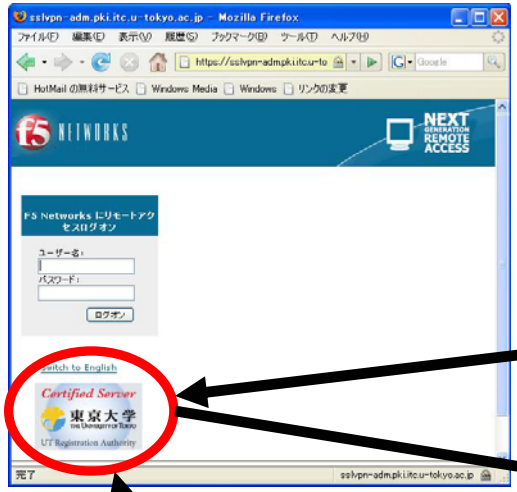
② ①をクリックしてもサイトは検証できない

1. シールサーバが実在性を確認していないサーバについては，東大シール表示用のソースを貼り付けても図（①）のとおり東大シールは表示されません

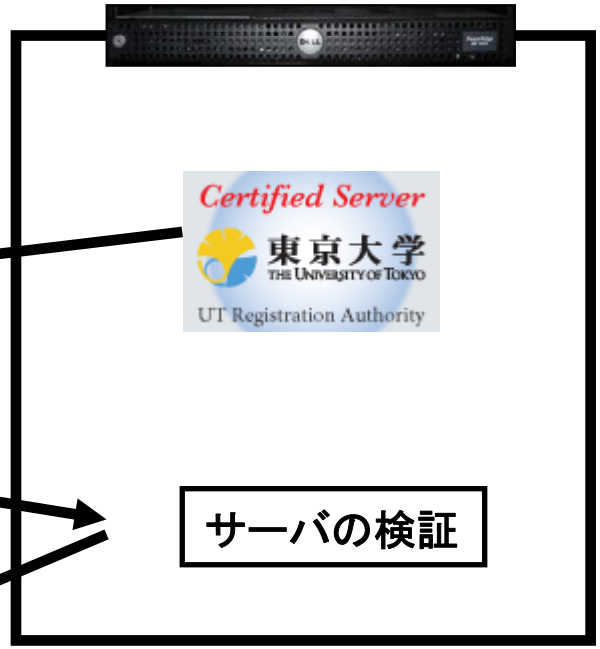
2. さらに①の画像をクリックしても，別ウインドウがポップアップして「偽装サイトの疑い」（②）と表示されるだけです

運用概念図（サービスの構成・アクセス図）

本プロジェクトのサーバ証明書を使用
しているサーバ（Webサイト）



PKIプロジェクトが運用する
シールサーバ

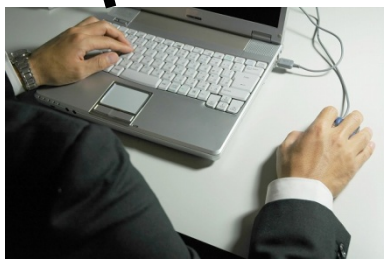


⓪ 東大シールを表示

②

①

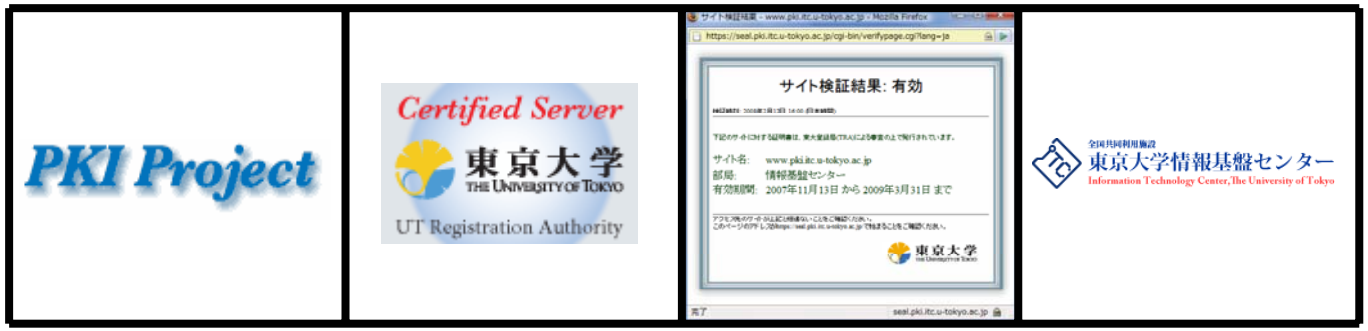
閲覧者



③

サーバの検証結果

5．プロジェクトの今後とまとめ



プロジェクトの課題と今後

- **課題**
  - TLRAのさらなる設置
    - TLRAはまだ少数の部局にしか設置されていないが，各部局サーバ管理者のためにもさらに設置しなければならない課題がある（⇒末端のサーバ管理者に近い存在であるTLRAが増えることで，サーバ管理者はサーバ証明書の申請がしやすくなる）

- **今後（実現したいこと）**
  - 学内向けのコンサルティング
    - 様々な申請事例を審査しサーバ証明書の発行フローのノウハウを蓄積して，サーバ管理者などに対して学内のコンサルティング業務などを行いたい
  - 東大シールが表示されているWebサイトを増やす
    - PSCのサーバ証明書を利用しているサーバ（Webサイト）に東大シールが表示され，東大ドメインのWebサイトを閲覧している利用者が安心して利用できる環境を提供したい