デジタル世界の身分証明書その５ー情報基盤センターPKI プロジェクトー

概要

今回はPKI プロジェクト[1]が新しく始めるサービスである、サーバシール[1]（図 1）の試行サービスについてお知らせします。サーバシールとはホームページを閲覧する利用者に対して、

(1)その Web サーバの実在性、つまり○○という組織の下にある正当なサーバであり、偽装されたものでないこと

(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こと

を可視化するものです。可視化というと大げさですが、サーバの信頼性を「見える化」するサービスといえます。本稿ではサーバシールの役割の紹介とともに、サーバシールの東大版「東大シール（仮）」(図 1)サービス開始に向けて PKI プロジェクトが準備してきたことをお知らせします[2]。

図１　本稿の中心となるロゴ（東大シール（仮））

サーバシールの前に

サーバシールの説明をする前に、まずは Web サーバの実在性を証明するサーバ証明書についてご説明します。

ホームページアドレス（URL）は通常「http://～」から始まりますが、そこで使われている「http(Hypertext Transfer Protocol)」とはテキストデータを Web サーバと利用者(クライアント)間でやり取りするための取り決め（規約）です。http では誰も Web サーバの実在性を証明していません。一方、実在性が証明されたホームページもあります。「https://～」から始まるホームページです。「https://～」から始まるホームページにするにはサーバ証明書というものが必要になります。

サーバ証明書は、Web サーバを運営しているサーバ管理者が信頼された認証局[3]に申請を行い、認証局の審査を経て発行されます。信頼された認証局からサーバ証明書が発行されたということは、Web サーバの実在性が証明されたということになります。なお、https とは http に「Security」の「s」がつくことでデータの暗号化通信に対応したホームページになるのですが、データの暗号化については本稿では触れません。また、本稿でいうサーバ証明書とは信頼された認証局から発行されたものを指し、いわゆる自己証明書は含みません。

---

1 「サーバシール」という用語は一般的ではないですが、このサービスを総称する用語がないため、本稿では便宜上サーバシールという用語を使います。

2 毎回ご説明していますが、この原稿は分かりやすく書くことを目的としておりますので、やや正確さを欠く表現があると思います。その点ご理解のうえお読みください。

3 本稿の「信頼された認証局」の定義は、主な Web ブラウザの証明書ストアに認証局証明書がインストールされている認証局のことをいいます。

少々分かりづらい説明が続きましたので、Web ブラウザの Internet Explorer 7（IE7）を例にサーバ証明書について具体的に説明します。

https://～から始まるホームページは、URL の横に図 1 の南京錠のような鍵マークが表示されます。その鍵マークをクリックすると図 2 のような画面が表示されます。さらに図 2 の下の方にある「証明書の表示」をクリックしてください。図 3 の「証明書」が表示されます。図 3 の証明書を検証することで「www.itc.u-tokyo.ac.jp」という Web サーバは認証局から認証（つまり証明）されたものということが確認できます。

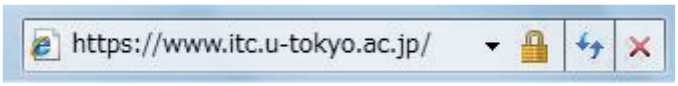

図 1　鍵マーク

図 2　Web サイトの識別

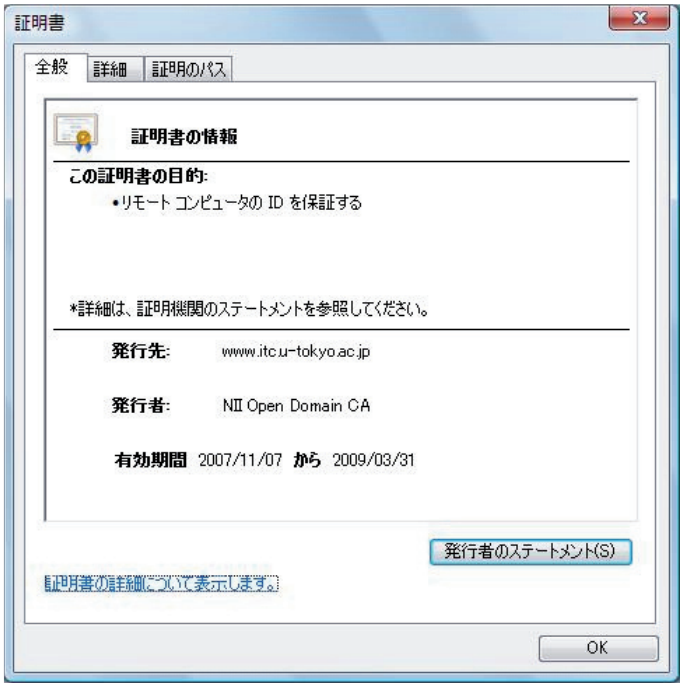

図 3　サーバ証明書の表示

ただし、この確認方法は一般的には分かりやすいとはいえません。そこで、PKI プロジェクトでは簡単に Web サーバの実在性を確認できるサービスを開始することにしました。

東大シール(仮)

さて、前置きが長くなりましたがここからが今回お伝えする話題の中心です。PKI プロジェクトは、サーバシールの試行サービスを開始することを決定しました。名称を仮に東大シールとします。

Web サーバの実在性を検証してみましょう

それでは実際に東大シールをクリックして、Web サーバの実在性を検証してみましょう。まずは https://www.pki.itc.u-tokyo.ac.jp/ にアクセスしてみてください。図 4 のような画像（東大シール）があると思います。その東大シールをクリックすると図 5 のサーバ検証結果が表示されます。その内容を見てサーバの実在性を確認します。

図 4　東大シール

図 5　サーバの検証結果（サーバの実在性の確認）

以上の手順をまとめますと、
(1)　https://www.pki.itc.u-tokyo.ac.jp/　にアクセスする
(2)　図 4 の東大シールをクリックする
(3)　図 5 のサーバ検証結果が表示され中身を見てサーバの実在性を確認したら検証は成功となります。

東大シールをクリックしてサーバの実在性を検証する意味は？

前節で東大シールをクリックしてサーバが実在していることは確認しました。ここで重要なことは、図4の東大シールがホームページ上に表示されているだけでそのサーバが本物だという証明にはならないということです。あなたが見ている東大ドメインのホームページは、もしかしたら悪意のある者が作成した偽のホームページに、偽造した東大シールの画像を貼り付けているだけかもしれません。東大登録局の審査の上で発行されたサーバ証明書であることを確実に検証するには、図4の東大シールをクリックして図5を表示させてからURLが https://seal.pki.itc.u-tokyo.ac.jp/ から始まることを確認する必要があります。seal.pki.itc.u-tokyo.ac.jp というサイトは、間違いなく東大登録局(TRA)が運用しているサイトです。そこからサーバの実在性が検証されたということは、皆さんが閲覧した東大ドメインのホームページも確かに実在するということになります。

また、サーバの実在性を検証することはフィッシング詐欺対策にも有効です。フィッシング詐欺とは、悪意のある者が例えばヤフーに偽装した偽のオンラインショッピングのホームページを作成して、そのホームページにアクセスしてきたユーザに名前、生年月日、電話番号、クレジットカード番号等の情報を入力させ、不正に個人情報を詐取する（フィッシング=釣る）ことをいいます。一般的にフィッシング詐欺をするためのホームページは「http://～」から始まるため、サーバの実在性が確認できません。利用者はホームページに表示されたサーバシールをクリックするなどしてサーバ証明書を検証し実在性を確認すればフィッシング詐欺に引っかかることはありません。

なお、多くの商用サイトでは、東大シールと同様なサービスを提供している商用認証局[4][5]のシール（ステッカーと呼ばれる場合もあり）を表示して、実在性を容易に確認できるようにしています。このような一般の商用サイトについてもサーバシールをクリックし、サーバの実在性をご確認ください。

東大シールを表示するには

現在あなたがサーバ管理者の場合、管理しているWebサーバに東大シールを表示させたい場合は、まずはPKIプロジェクトが立ち上げた東大登録局（TRA）[2]の審査を受けサーバ証明書を取得しなければなりません。サーバ証明書の取得にかかる費用は、2009年3月31日までは無料です。その後は未定ですが、2009年4月1日以降、サーバ証明書の取得に費用がかかるようになっても、東大シールはサーバ証明書に付随するサービスなので、別途費用がかかることはありません。

本稿をご覧になってご関心を持たれた方がいらっしゃいましたら、URL: http://www.pki.itc.u-tokyo.ac.jp/cerpj/ をご覧いただき、電子メールにて（PublicServerCertificates [at]itc.u-tokyo.ac.jp）までご連絡ください。

東大シール実現に向けて

PKIプロジェクトでは東大シール試行サービスに向けて次のような準備をしてきました。

・ハードウェア関係
-専用のサーバを購入し，ドメインを取得すること
-サーバ証明書を取得すること
-電源の二重化を実施すること（予定）

・ソフトウエア関係
-シールのデザインを作成すること
-主なWebブラウザで問題なくシールを検証できることの確認（各ブラウザに対応すること）
-データベースの構築
-検証ページの設計

おわりに

PKIプロジェクトは、国立情報学研究所(NII)の「サーバ証明書の発行・導入における啓発・評価研究プロジェクト」[3](以下、NIIプロジェクトとよぶ)に参加し、東大ドメイン(u-tokyo.ac.jp)のサーバを管理しているサーバ管理者に対してパブリックなサーバ証明書の審査・発行を担当する組織（東大登録局（TRA））を立ち上げました。

今回は紙面の都合上、東大登録局（TRA）については特に説明していませんが、NIIプロジェクトのサーバ証明書を必要とする場合はTRAの審査を受けなければなりません。

「u-tokyo.ac.jp」というドメインは知名度があり、それ自体にブランド力があると考えています。そのためTRAでは、(1)職員証をもとにした本人確認、(2)当該サーバの管理体制の聞き取り、(3)ドメインの管理体制の聞き取りなどといった厳格な審査を行っています。その理由は不適正な管理の下にあるサーバに対してサーバ証明書を発行してしまっては東大全体の信用問題(東大ブランドの失墜)になるからです。

東大登録局（TRA）発行のサーバ証明書をインストールしたWebサーバのすべてに東大シールが表示され、東大ドメインのホームページ利用者が安心して利用できる環境を提供し東大シールが東大ドメインのブランド力向上の一助となるよう、PKIプロジェクトは活動を続けていきます。

参考資料：

[1] 東京大学情報基盤センターPKIプロジェクト　http://www.pki.itc.u-tokyo.ac.jp/
[2] パブリックサーバ証明書発行東大登録局　http://www.pki.itc.u-tokyo.ac.jp/cerpj/
[3] 国立情報学研究所「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」
https://upki-portal.nii.ac.jp/cerpj/
[4] セコムトラストシステムズ株式会社：http://www.secomtrust.net/service/sticker.html
[5] 日本ベリサイン株式会社：http://www.verisign.co.jp/securesite/sitelist.html

（大島大輔）