

パブリックサーバ証明書発行プロジェクトのご案内

1. はじめに

国立情報学研究所(NII)は全国の大学を対象として、サーバ証明書の普及推進と証明書発行プロセスの研究を行なうためのプロジェクト¹を始め、パブリックなサーバ証明書を無償で配布しています。ただし誰にでも無審査で証明書を発行するわけにはいきませんから、大学内に「正しい」審査機構があることが発行対象の条件となっています。情報基盤センターPKIプロジェクトは、このプロジェクトの東大における窓口となり、東大内のサーバに対するサーバ証明書発行の受け付けを行なっています。

ここで発行される証明書はパブリック、つまり多くのブラウザにルート認証局として登録されている機関から発行されているものです。特に不特定多数の利用者に対して安全・安心なサービスを提供する上で欠かせない、サーバ認証および通信路の暗号化を、利用者をわずらわせることなく実現することができます。

2. サーバ証明書を取得するための2つの方法

プロジェクト理念はともかく、利用者の側から見れば東大の教職員であれば無償でパブリックサーバ証明書の発行を受けられるということになります。ここでその手順を紹介しましょう。

その前に、このプロジェクトで使われる用語の説明を行ないます。図1が構成を示したもので、NII に対する東大の窓口を東大登録局(TRA)と呼んでいます。また、その下に部局によっては東大部局登録局(TLRA)が設置されているところもあります。TLRAの責任者はUTnet部局担当者が兼任しています。

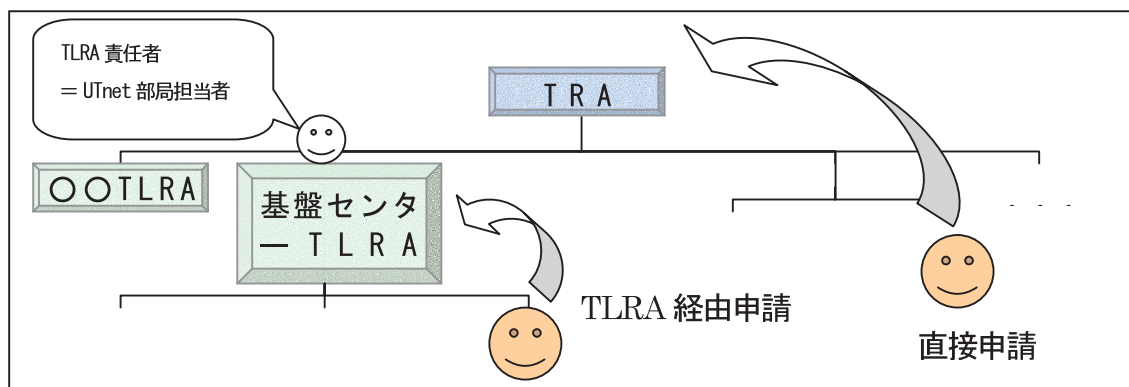


図1 TRA と TLRA、および2種類の申請の方法

¹ プロジェクト名称「サーバ証明書発行・導入の啓発・評価研究プロジェクト」
「4.お問い合わせ」掲載サイト内「関連リンク」を参照のこと。

2.1 TLRA を介した申請

あなたが所属している部局に TLRA が設置されている場合、あなたがやらなければならないことは証明書発行申請書とサーバ上で作成した証明書署名要求(CSR)をフロッピーなどに入れたものを TLRA へ提出することだけです。TLRA 側で申請 FQDN が正しいものであるか審査が行なわれたのち証明書が発行されることとなります。発行された証明書は通常 CSR を格納したメディアに入れて受け渡されます。

ただし、TLRA 毎に審査方法が決められており、発行対象にも制限がある場合がありますので、詳しくは所属部局の TLRA へお問い合わせください。

2.2 TRA への直接申請

あなたが所属している部局にまだ TLRA が設置されていない場合や TLRA がカバーできないドメイン (後述) のサーバにサーバ証明書が欲しい場合、TRA へ直接申請を行なっていただくこととなります。

この場合、TRA が個々のサーバの管理体制を把握するのが難しいため、申請書と CSR に加えて、サーバおよびドメインの管理体制を示す書面を提出していただきます。つまり、サーバが間違いなく申請者が管理するものであることと、そのサーバに申請ホスト名 (FQDN) が割り当てられていることを確認できるものが必要となります (これは TLRA を設置する場合に UTnet 部局担当者に提出をお願いするものと同等のものです)。用意することが困難な場合は TRA による面接等で代替することも可能ですので、詳しくはお問い合わせください。

3. ご注意いただきたいこと

TLRA の体制は既存の UTnet の管理体制を利用したものです。このためドメインの中で TLRA がカバーできない部分が存在します。具体的には、TLRA はその部局に割り当てられたドメイン下のみ発行対象とします (例えば情報基盤センターの場合は itc.u-tokyo.ac.jp)。

また、規則により学生からの申請は受け付けられません。

サーバの管理体制やドメインの管理体制を文書で提出させるなど、面倒とお感じになることがあるかもしれません。しかし我々は、この証明書発行手続きが不正な者による証明書の取得を防ぎ、また将来に渡ってその体制が維持できることを示すために必要と考えております。ご協力いただけましたら幸いです。

最後に、もしあなたがサーバ証明書を取得した場合、その証明書が信頼され続けるためにはサーバ、特にその中に保存されている私有鍵が適切に保護されていることが重要です。くれぐれも不正な者の手に渡ることのないようご注意ください。

4. お問い合わせ

申請書および詳しい情報、問い合わせ先等は以下のサイトをご参照ください。サーバ証明書普及のため、みなさまが抱えている問題や素朴な疑問など何でもお寄せいただきたいと思っております。

また本稿は利用者 (サーバ管理者) を対象としているため TLRA を設置する場合の手続きを意識的に省いてあります。UTnet 部局担当者の方で TLRA 設置を検討される場合もお気軽にお問い合わせください。

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

(西村 健)