

## PKI サービス アップデート

情報基盤センターでは、NII の UPKI 電子証明書発行サービスを受ける形でパブリックな電子証明書発行サービスを行っています。サービスの現状のアップデートがありましたのでお知らせします。

### 1. 電子証明書中の DN の扱い変更 (ST=Tokyo の指定と L の廃止)

電子証明書の管理運用の厳格化の流れを受け、2018 年 7 月 9 日発行分より、CSR の中で以下の形式を変更しました。ご注意ください。具体的には ST フィールドに Tokyo を指定するようになり、L フィールドを廃止しました。例として example.itc.u-tokyo.ac.jp のサーバ証明書発行に際して作成する CSR の DN は以下のように変更されます。

(新) CN=example.itc.u-tokyo.ac.jp, OU=Information Technology Center,  
O=The University of Tokyo, ST=Tokyo, C=JP

(旧) CN=example.itc.u-tokyo.ac.jp, OU=Information Technology Center,  
O=The University of Tokyo, L=Academe, C=JP

(下線部が変更部分)

これに伴い、旧型式で発行された電子証明書を更新する場合は、すべて「新規」扱いになります。申請の際にご確認ください。

従来マイクロソフト IIS で運用する証明書では、OpenSSL 等での CSR の作成をお願いしていたわけですが、今後は、IIS 内部で完結することができます。ご利用ください。なお、この変更はサーバ証明書に限らず、コード署名証明書にも適用されます。

### 2. 中間証明書の変更

使用する中間証明書が、2018 年 3 月 26 日以降に発行分より、nii-odca3sha2ct.cer に変更になりました。当分の間旧中間証明書とともに並行運用をお願いします。

### 3. クライアント証明書の発行 (テスト運用)

パブリックなクライアント証明書 (認証用) の発行サービスのための、テスト運用を始めました。テスト運用のために、以下の制限があります。

1. 発行は、当面 TLRA を設置している部局に限ります。
2. クライアント証明書発行申請書とウェブページに掲載している「p12\_一括フォーマット (EXCEL 形式)」を作成し、電子媒体とともに提出してください。DN は以下ようになります。

CN= 共通 ID 下 10 桁, OU=TLRA 設置部局名, O=The University of Tokyo,  
ST=Tokyo, C=JP

詳細は <https://www.pki.itc.u-tokyo.ac.jp/> をご参照ください。

(ネットワーク研究部門 佐藤 周行)  
(ネットワークチーム)