

東京大学における CiNII 認証代行応用としての SS0 への参加

東京大学情報基盤センターPKI プロジェクト

佐藤周行・西村健

東京大学で SS0 への参加にあたりたてた方針は以下のとおりである。

- (1) 従来サービスと不整合をおこさないこと
- (2) 提供する ID の品質に責任を持つこと

なお、われわれは、このプロジェクトについて、まずはサービスに対する理解が得やすいように「CiNII 認証代行」を東大の IdP で行なうという図式で臨んでいる。ただし、学内の一部からは大学をまたがるサーバに対する認証の要求も具体的に出ており、SP の整備は今後ゆっくりとではあるが着実に進むであろうことを予想している。この部分の展開については今後のテーマになる。

(1) について述べる。SP として想定された CiNII は、附属図書館においてすでに SSLVPN を通した電子ジャーナルの外部からのアクセスサービスと重複するところが多くある。そこでわれわれは2つのサービスが不整合を起こさないように、両者が利用できる ID 体系を用意することにした。なお、附属図書館側のサービスで利用している ID 体系の品質は非常に高いものがあるが、その情報を学外サービスのために利用するにはプライバシーその他検討を要するところが多くあり、とりあえず PKI プロジェクトで責任を持って運用管理できる学内 CA である UT-CA の情報を利用することにした。

(2) について述べる。SS0 が今回想定するような分散 ID 管理のもとで正しく運用できるためには IdP の統制が必須である。われわれは IdP に ID を提供する LDAP サーバの統制をその上流を含めて検討した。

このプロジェクトでは以下のドキュメントを作成している。

- (1) プロジェクト参加の呼びかけ (<http://www.pki.itc.u-tokyo.ac.jp/>)
- (2) ID Policy/ID Practice Statement の作成
- (3) 2008 年 11 月の中間報告会の際のスライド

この報告では (1) と (3) を添付する。