

UPKI 共通仕様 利用の手引き

初版 (ver1.0)

国立情報学研究所
学術情報ネットワーク運営・連携本部
認証作業部会

2007 年 6 月 6 日

1. 利用の手引き

(1)はじめに

本 UPKI 共通仕様(「キャンパス PKI CP/CPS ガイドライン」、「キャンパス PKI 調達仕様ガイドライン」)は UPKI 上で大学間連携サービスを実現するための基盤となるキャンパス PKI を、将来の連携性確保や構築コスト削減などの観点も含めて、構築するための指針となることを目的としている。

本 UPKI 共通仕様(アウトソースモデル)を策定するにあたり、キャンパス PKI を先行して構築済みの 2 大学(以下「先行大学」)の CP/CPS 及び調達仕様書を参考にするとともに、これら先行大学に対してのヒアリングを実施し、さらに RFC3647 と先行大学仕様との比較を実施した。ヒアリング項目数は全 39 項目で、比較項目数は全 73 項目である。これらの結果得られた先行大学に共通する項目、異なる項目を抽出・分析することで、キャンパス PKI として共通に必要な事項について洗い出しを行い、その結果をガイドラインとしてまとめた。具体的には、各大学がキャンパス PKI を構築する際に必要となる「キャンパス PKI CP/CPS ガイドライン」及び「キャンパス PKI 調達仕様ガイドライン」を作成した。なお、両ガイドラインは、原則、厳格な運用を前提として策定を行った。

(2)本仕様の構成

本 UPKI 共通仕様は、「キャンパス PKI CP/CPS ガイドライン」、「キャンパス PKI CP/CPS テンプレート」、「キャンパス PKI 調達仕様ガイドライン」、「キャンパス PKI 調達仕様テンプレート」から構成されている。これらの文書を雛型とすることで、各大学の容易なキャンパス PKI 構築に資することを想定している。また、参考資料として先行大学の CP/CPS と RFC3647 との比較結果を別紙に添付する。

(3)本仕様の利用法

本 UPKI 共通仕様は、各大学がキャンパス PKI を構築するにあたり必要とする CP/CPS 及び調達仕様書の指針となるものである。利用方法として「キャンパス PKI CP/CPS テンプレート」、「キャンパス PKI 調達仕様テンプレート」に記述された内容を各大学にて編集し利用することを想定している。また、テンプレートとして、フルアウトソースモデル、IA アウトソースモデルの 2 種類用意している。フルアウトソースモデルは認証局(CA)を全て外部委託するものであり、IA アウトソースモデルは発行局(IA)を外部委託し、登録局(RA)を学内にて構築するものである。各大学はこれらのモデルから各大学の運用方針に適するものを選択して用いることとする。具体的なテンプレートの利用方法としては、認証局構築モデルを選択後、各テンプレート内の空欄を認証局の運用方針、予算、証明書利用用途に従い項目毎に取捨選択及び空欄を補充することとする。各大学において本「キャンパス PKI CP/CPS テンプレート」、「キャンパス PKI 調達仕様テンプレート」の改変は自由に行えるが、将来の大学間連携を見据えて、認証局のポリシーレベルを合わせる観点からも、各大学では最小限の改変に留めることを推奨する。

以上