[Work in Progress] 研究報告

学術研究機関から構成されるPKIトラストフェデレーションにおける認証局統合モデルの検討

坂根 栄作[1,a)]　西村 健[1,b)]　合田 憲人[1,c)]

A Study of Certification Authority Integration in an Academic PKI Trust Federation

学術研究機関から構成されるPKIトラストフェデレーションのなかには，いわゆるGrid PKI層で組織されるものがある [1]．代表的なものとして，IGTF[*1] (Interoperable Global Trust Federation) は，相互運用可能な世界的規模の信頼関係を確立するのに役立つ共通の方針や指針を制定している．そのようなPKIトラストフェデレーションの構成員である認証局の運用形態の特徴の1つに，認証局を構成する機器や装置は，運用主体である学術研究機関が自前で整備していることが挙げられる．例えば，IGTFの定める認証局運用要件では，高水準の認証局装置および物理的セキュリティ管理を規定している．認証局の信頼性を担保するためには，そのような設備維持および運用要員確保が必要となり，結果として運用経費がかさむことになる．したがって，認証局運用業務が本来の業務ではないはずの研究機関にとって，高価な運用経費の負担は切実な問題であり，運用効率化による運用経費削減は重要な課題である．

本論文では，単一の認証局に閉じた運用効率化ではなく，複数の認証局を統合することにより同一フェデレーション内の認証基盤全体での運用効率化を議論する．認証局統合手法には，統合前の認証局をそれぞれ中間認証局とするようなルート認証局を新規に構築するものがある [2]．この手法はルート証明書管理を効率化できる長所があるものの，統合前後で各認証局業務はそのままであるために，運用効率化の観点からは逆に負担増になる可能性がある．また，異なる学術研究コミュニティに跨がるルート認証局を新規に構築・運用するには，抜本的な改革の後押しがなければ現実的ではないと考えられる．

実現性の観点から，認証局統合における課題を以下のように設定する：

(1) 可能な限り新規の設備投資を抑える．
(2) 各々の認証局の運用体制に対して抜本的な改編を必要としない．
(3) 各々の認証局の従来の証明書ポリシを可能な限り引き継ぎ共存させる．

これらの課題を解決する手法として，本論文では，認証局の主要な構成要素である発行局および登録局に着目し，2つの認証局（甲・乙）の発行業務を統合し，利用者登録業務を従来どおり各運用機関が実施する統合モデルを提案する．この提案手法における発行業務の統合とは，例えば認証局（乙）は発行業務を終止し，それを認証局（甲）が担うこととして全体の発行業務の効率化を図るものである．また，登録業務は従来どおり各登録局が実施するために，証明書利用手続き等にほとんど変更はなく利用者を混乱させることもない．

上述の統合モデルの基本的着想に基づき，統合された発行局（甲）と登録局（乙）との接続形態を検討する．さらに，統合後の登録局（乙）が受理し審査した申請者の証明書発行依頼に対し，統合後の発行局（甲）がその要求に応じた証明書の発行を可能とするような証明書ポリシの共存手法について，従来の認証局運用要件の適用可能性およびそれらの拡張とともに議論する．

[1] 国立情報学研究所
National Institute of Informatics
[a)] sakane@nii.ac.jp
[b)] takeshi@nii.ac.jp
[c)] aida@nii.ac.jp
[*1] https://www.igtf.net

参考文献

[1] 島岡政基，谷本茂明，片岡俊幸，峯尾真一，曽根原登，寺西裕一，飯田勝吉，岡部寿男：大学間連携のための全国共同電子認証基盤UPKIにおける認証連携方式の検討，情報処理学会研究報告, 2006-QAI-019， Vol. 2006, No. 55, pp. 13–18 (2006).
[2] 古賀　聡，櫻井幸一：認証局の統合と分散の定式化とその考察，情報処理学会研究報告, 2002-CSEC-020， Vol. 2003, No. 18, pp. 155–160 (2003).