博士学位論文審査結果要旨

平成30年2月28日

研究科、専攻名　バイオ・情報メディア研究科　コンピュータサイエンス専攻

学位申請者氏名　濱口 総志

和 文 題 目　公開鍵基盤に基づくトラストサービスの日欧間比較と相互認証の研究

英 文 題 目　Comparison and possibility of mutual recognition of Trust Services based on Public Key Infrastructure among Japan, US and Europe

審査結果の要旨

研究の背景として、オンライン環境における脅威への対策として既に様々なセキュリティ技術が開発され実装されてきているが、市民や企業が新たな電子サービスやソリューションを利用する際には、セキュリティだけでなく信頼性の確保も重要である。技術の発展によって、ビジネスや市民活動が急速にグローバル化している現在では、オンライン環境における信頼性を向上するトラストサービスについて、国境を越えた相互運用性と相互承認の枠組みの構築が強く求められている。このような背景の中で、公開鍵基盤に基づくトラストサービスについて、日米欧間の制度、法律および技術要件を比較し、その差異を分析し、相互承認に向けた研究を行うことは、市民活動、経済活動の電子化及び効率化の促進に大きく資することができると考えられる。

一方、日米欧はトラストサービスについてそれぞれ独自の法律と技術的要件及び監査要件を定めているが、日米欧のトラストサービスの相互承認を実現するには、先ず各国のトラストサービスに関連する制度、要件を比較可能にする必要がある。そのために各国のトラストサービスに関わるトラストフレームワークを分析し、どのような要素でトラストフレームワークが構成されているかを明らかにし、トラストフレームワークに共通する構成要素に関してその用語と定義を整理した。また、監査結果の効率的な相互承認のためには、各技術要件の比較だけでなく、トラストサービスプロバイダの構成要素を整理し、共通機能の洗い出しを行った。

表１　日米欧電子署名法の整理

適合条件	日本	米国	欧州
法適合（手書き署名と同等と認められる電子署名）	認定認証業務の証明書に基づく電子署名	要件を満たしたデジタル署名	適格電子署名
技術適合（署名者を特定できる技術を用いた電子署名）	特定認証業務に基づく電子署名	デジタル署名	先進電子署名
それ以外の電子署名	電子署名	電子署名	電子署名

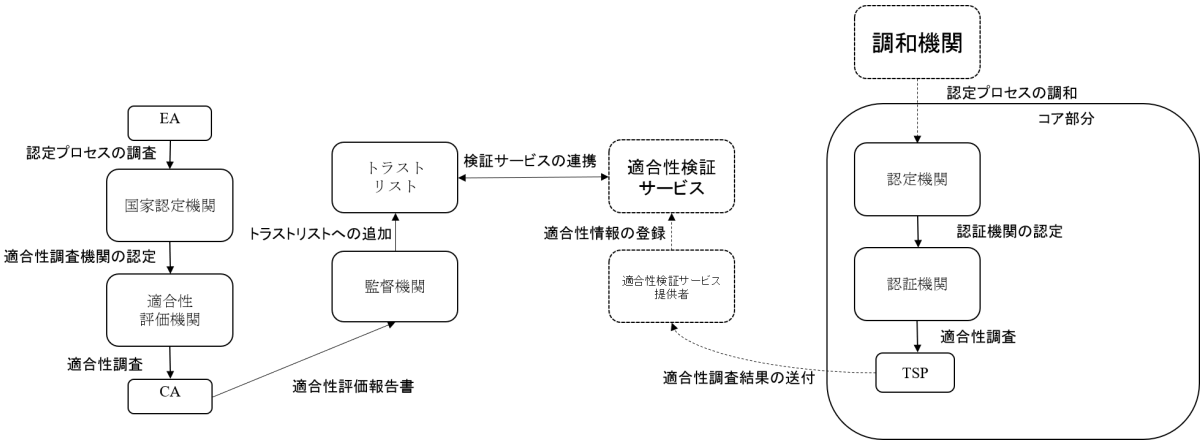

図1　トラストモデル案とeIDAS規則の相互承認モデル

本研究では日米欧のトラストサービスに関わるトラストフレームワークを比較することで、相互承認に向けて障害となりうる差異を分析した。まず日米欧の電子署名に係る法的要件を比較整理し、法的要件の側面から相互承認が実現可能か分析した。日米欧の電子署名に関連する法律を比較すると、電子署名に関して日本と欧州は同じ 3 段階の定義を持っている一方で、ハードウェアトークンの利用について差異があることが分かった（表 1)。

トラストモデルについては、eIDAS 規則、ETSI 認証、WebTrust for CA 及び日本の電子署名法の 4 つについて比較し、共通点と差異を分析した。トラストフレームワークによって法的効力を保証する場合は、法律による裏付けと政府機関による統治がなされていることが解る。

これらの 4 つのモデルと相互承認可能なトラストモデル案を提案した（図 1)。これにより相互承認において重要なお互いのサービスを検証可能にすることができる。欧州ではトラストリストを用いており、加盟国毎に適格トラストサービスのリストを保持しているが、日本の電子署名法のトラストモデルでは、他のトラストモデルがトラストサービスを検証する手段を提供していないため、トラストリストやブリッジ認証局等の相互認証の仕組みを構築する必要性があることが分かった。

本研究をまとめると、公開鍵基盤に基づくトラストサービスについて、日米欧間の制度、法律および技術要件を比較してその差異を分析し、相互承認の実現可能性に見通しを付けた。次に日米欧の代表的な 4 つのトラストモデルについて共通点と差異を分析し、これらの 4 つのモデルと相互承認可能なトラストモデル案を提案した。提案の特徴は、互いのサービスを相互に検証可能にしたことにある。これらの既存モデルの分析とそれに基づいたモデル案の提案は、学位申請者本人が各国の認証機関、認証ユーザにヒアリングし、また国内の政府委員会の委員を務めるなどしてトラストサービスの現場で直接情報収集した結果に基づいており、極めて信頼性と応用性の高い研究である。

また学位審査公聴会なのでおける発表、および質疑応答は妥当なものであり、審査員会は本論文の著者に対して博士（コンピュータサイエンス）の学位を授けるのに十分な能力と学識、語学力を有していることを認めるものである。

審査委員　主査

東京工科大学大学院　教授　　木下 俊之　　印