要　旨

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、また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障害となるのはセキュリティの欠如だけでなく、信頼性の欠如が大きな要因となっている。欧州では 2014 年に eIDAS 規則を施行し、電子商取引における信頼性向上に寄与するサービスとして、電子署名やタイムスタンプ、ウェブサイト認証等のトラストサービスを定義し、トラストサービスに法的効力を与えるとともに、その法的及び技術的要件を定めている。日本でも 2001 年に施行された電子署名法によって電子署名に関する法的効力が定められているが、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。日欧間の相互運用性及び相互承認に向けた取り組みは本年から、少しずつ開始されており、2017 年 7 月 4 日は日欧インターネットトラストシンポジウムが開催され、主として民間レベル、技術レベルでの相互運用性に向けた議論が行われ、また、第六回日 EU・ICT 戦略ワークショップでは政府レベルでの法的効力の相互承認に向けた議論が開始されている。一方で、欧米間では医薬品業界におけるトラストサービスの相互承認に向けた取り組みとして、米国 SAFE-BioPharma と独 TeleTrust の European Bridge CA がパートナーシップ契約を結んでいる。

また、トラストサービスの一つであるウェブサイト認証と、そのトラストフレームワークについては、ブラウザベンダーと認証局事業者から構成される CA/Browser フォーラムと各ブラウザベンダーのルート CA プログラムのデファクトスタンダードとしての影響力が非常に強く、トラストアンカーを民間事業者（ブラウザーベンダー）が担っている状況にある。このような状況下で、ウェブサイト認証のための証明書を発行する認証局はブラウザベンダーの要求する基準を満たすことを信頼できる第三者監査を受けることで証明することが求められているが、この第三者監査の結果についても相互承認を検討していくことが必要である。

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。

日米欧はトラストサービスについて、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。そのためには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する必要がある。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、共通機能を洗い出す必要がある。

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する。

日米欧の電子署名に関連する法律を比較すると、電子署名に関しては日本と欧州は同じ 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　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

法律が手書きの署名と同等と定めている電子署名と、公開鍵基盤に基づく技術的に署名者を特定できるデジタル署名及び、それ以外の方式の３段階である（表1)。

欧州では手書き署名と同等と認められる適格電子署名の要件として、コモンクライテリア認証を取得したセキュアなハードウェアトークンの利用を求めており、日本において秘密鍵の管理が署名者の責任にゆだねられていることと対象的である。米国でもハードウェアトークンの利用を明示的に求めている法律はなく、イリノイやワシントン等の一部の州法による安全な電子署名としての公開鍵基盤に基づくデジタル署名と、その安全な運用方法が規定されているにとどまっている。本研究では、現在日本でもガイドラインが検討されているリモート署名が、これらの差異を解消するのではないかと提案している。

表２　日米欧のトラストモデル

	eIDAS	**ETSI Certification**	**WebTrust for CA**	**日本の電子署名法**
法律	eIDAS 規則	N/A	N/A	電子署名及び認証業務に関する法律
目的	トラストサービスの法的効力の承認による電子取引の活性化	技術的相互運用性、第三者監査、CA/B Forum の要件への適合	技術的相互運用性、第三者監査、CA/B Forum の要件への適合	電子署名の円滑な利用の保証による電子文書の普及
政府機関	EU 委員会	N/A	N/A	経済産業省、 総務省、 法務省
調和機関	EA	EA	N/A	N/A
認定機関	加盟国の国家認定機関	加盟国の国家認定機関	AICPA/CIPA	経済産業省、 総務省、 法務省
認証機関	監督機関	国家認定機関の認定を受けた認証機関	公認会計士	経済産業省、 総務省、 法務省
適合性評価機関	国家認定機関の認定を受けた適合性調査機関	認証機関が認める評価機関	公認会計士	指定調査機関
技術気基準	ETSI 規格	ETSI 規格	WebTrust Criteria	認定基準
保証レベル	法的有効性及び技術的適合性	技術的適合性	技術的適合性	法的有効性及び技術的適合性

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トラストモデルの 4 つのトラストモデルを比較し、共通点と差異を分析した（表 2)。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、当然ではあるが、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。また、調和機関についてはトラストフレームワークが多国家にわたって提供される場合に必要であり、例えば ISO における国際認定フォーラム（IAF）のような組織が各フレームワーク間の相互承認には必要と考えられる。

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)。相互承認において重要になるのが、以下に互いのサービスを検証可能にするかである。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。

下記の相互承認モデルでは、適合性検証サービスが連携して互いのサービスを検証可能にするが、現状日本には独自の適合性検証サービスが存在しないため、この実現のために、欧州と同じ方式でトラストリストを公開する方式が現実的である。

また、より効率的な監査の手法として部分認証を提案した。これは、現実に認証業務の提供の際にあるデータセンターを複数の認証局が利用している例があり、このような場合、例えば、このデータセンターの運営事業者は､認証局が eIDAS 規則あるいは WebTrust for CA の監査を受ける都度、監査を受けているのが実態であるが、部分認証とはこのような他の認証局と共通の部分について単体で適合性評価を行い適合性認証することである。

この例の場合、共通部分であるデータセンターをあらかじめ適合性認証しておくことで、別の認証局の適合性評価の際に、このデータセンターについては評価結果を流用することができる。

この手法は､実際に eIDAS 規則に基づく監査の中で採用されており､4 件ほど認証されている。採用された例はすべて、電子証明書を発行する本人確認のプロセスについてである。

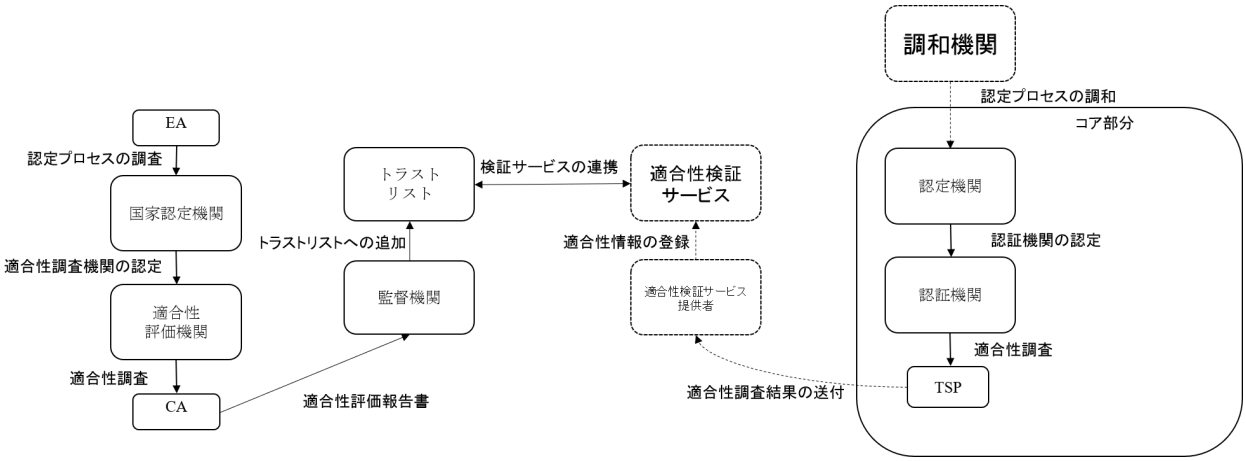

図 1　トラストモデル案と eIDAS 規則の相互承認モデル

トラストサービスの相互承認を実現するためには、互いのトラストサービスの制度に対する相互理解が必要不可欠であるが、諸外国のトラストサービスと日本のトラストサービスを比較分析している資料は少ない。本研究でトラストサービスの相互承認に向けて取り組んでいく中で、本研究で比較分析した結果が利活用されることを期待する。