東京工科大学
博士学位論文

公開鍵基盤に基づくトラストサービスの日米欧間比較と相互承認の研究

東京工科大学
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

平成 30 年 3 月

濱口 総志

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。

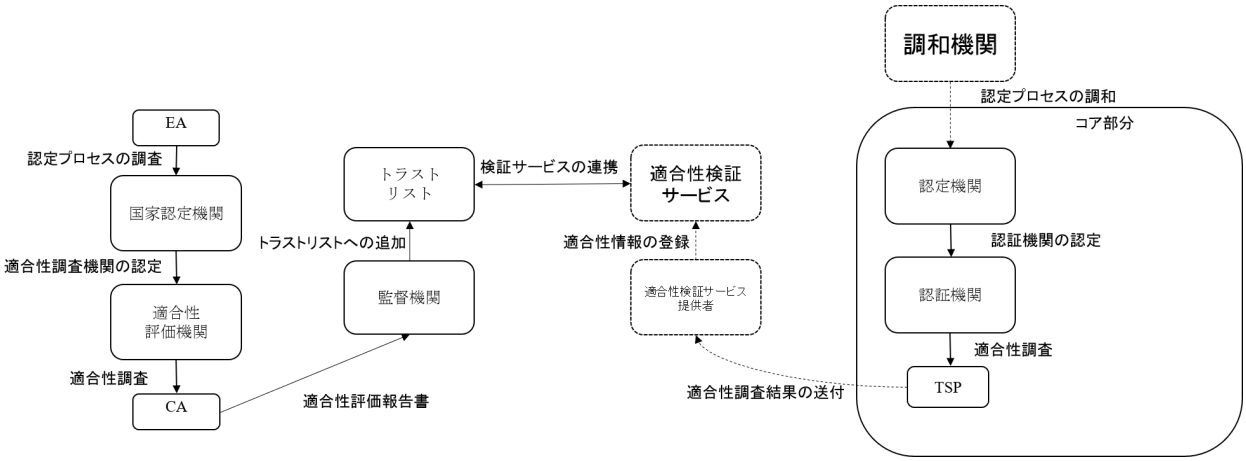

図 1　トラストモデル案と eIDAS 規則の相互承認モデル

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。

内　　容

1. 序論

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[1]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[2]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。

2. 用語

依拠当事者（relying party）： トラストサービスに依拠する者

加入者（subscriber）： トラストサービスプロバイダとの契約によって加入者義務を負う法人又は自然人。

トラストサービス（trust service）： 次のいずれかに関する電子サービス：

- デジタル署名及び関連する証明書の生成、検証、及び妥当性の確認
- タイムスタンプ及び関連する証明書の生成、検証、及び妥当性の確認
- e デリバリー及び関連する証明書
- ウェブ認証のための証明書の生成、検証、及び妥当性の確認
- これらのサービスに関連するデジタル署名又は証明書の保管

トラストサービスプロバイダ（trust service provider）： トラストサービスを提供する事業者

証明書（certificate）： ユーザの公開鍵であり、他の情報と合わせ、発行した認証局の秘密鍵で暗号化することによって偽造不可能にされているもの

証明書ポリシー（Certification Policy, CP）： 特定コミュニティ及び/又は共通のセキュリティ要件を有するアプリケーションへの証明書の適用可能性を示す規則の集合

証明書失効リスト（Certificate Revocation List, CRL）： 証明書発行者が既に有効ではないとみなされる証明書一式を示す署名済みリスト

認証局（Certification Authority, CA）： １人以上のユーザが証明書の作成及びアサインすることを信頼されている当局

認証局失効リスト（Certification Authority Revocation List, CARL）： 証明書発行者が既に有効ではないとみなす認証局に対して発行された CA 証明書のリストを含む失効リスト

認証局運用規定（Certification Practice Statement, CPS）： 証明書の発行、管理、失効、更新またはリキーにおいて、認証局が用いる運用規定

相互認証（Cross Certificate）： 二つの認証局間の信頼関係を構築するために使われる証明書。

電子署名（electronic signature）：電子データに添付されている又は論理的に関係している電子形式のデータであり、署名者が署名する為に使用するもの

デジタル署名（digital signature）： データユニットの受信者によるデータユニットの発信元及び完全性の証明と、受信者などによる偽造の防止を可能にする、追加データ又はデータユニットの暗号変換

タイムスタンプ（Timestamp）：データがその時間に存在していた証拠を確立し、他の電子データを特定の時間と結びつける電子形式のデータ

ハイセキュリティゾーン（High Security Zone）： ルート CA の鍵が保管されているセキュリティゾーン

パブリック証明書（Publicly-Trusted Certificate）： ルート証明書がトラストアンカーとして広く利用可能なアプリケーションソフトウェアで配布されているということから、信頼されている証明書

登録局（Registration Authority）： 主に証明書のサブジェクトの識別及び承認について責任を負うエンティティ

ルート CA（root CA）： TSP のドメイン内で最高位の CA であり、下位 CA の署名に使用する認証局。

セキュアゾーン（secure zone）： TSP が使用するシステムの機密性、完全性及び可用性を適切に保護する、物理的及び論理的制御により保護されている（物理的又は論理的）エリア。

主体者(subject)： 証明書に記載の公開鍵と関連する秘密鍵の所有者として証明書に明記されたエンティティ

下位 CA（subordinate CA）： ルート CA 又はその他の下位 CA によって署名された証明書をもつ認証局

トラストアンカー（trust anchor）： 依拠当事者によって信頼され、認証パスにおける証明書を検証するために使用されるエンティティ

ハードウェアセキュリティモジュール（Hardware Security Module, HSM）：FIPS140-2 或いはコ

モンクライテリア認証を取得した暗号モジュール

適格電子署名生成装置（Qualified Signature Creation Device, QSCD）： 署名者の秘密鍵を保護し、セキュアな署名プロセスを可能にするコモンクライテリア評価を受けた装置。

3. 法制度

3.1 欧州の法制度 － eIDAS 規則

eIDAS 規則は 1999 年に発効された従来の電子署名指令に代わるものであり、EU 加盟各国の電子署名法を上書きする規則である。また、電子署名指令とは異なり、電子署名以外のトラストサービスを新たに定義し、加えて eID のオンライン認証結果の相互承認まで含む。これにより、電子署名指令で実現しきれなかった電子取引における信頼性の構築と加盟国間の相互承認の実現を目的としている。トラストサービスについては、ETSI TS 119 612[3]においても定義されており、eIDAS 規則と ETSI TS 119 612 におけるトラストサービスの定義を以下の図 3.1 に示す。ETSI TS 119 612 における定義は、eIDAS 規則の定義と比較してより広義であり、特に、公開鍵暗号方式の利用を前提としていない。一方で、eIDAS 規則においては、下位規則においてトラストサービスが満たすべき技術規格が指定されており、公開鍵暗号方式の利用が前提となっている。

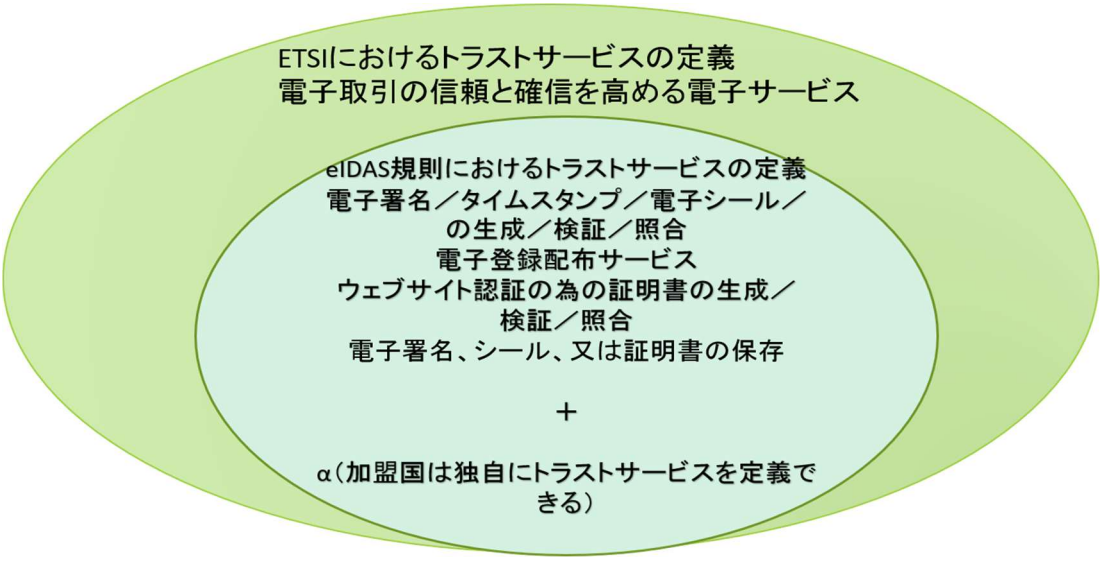

図 3.1 トラストサービスの定義

また、トラストサービスには、適格トラストサービスと適格でない通常のトラストサービスがあり、適格でない通常のトラストサービスについても法的効力は否定されていないが、適格トラストサービスについては明確に法的効力が承認されている。

本論文が研究対象としているトラストサービスは電子署名とウェブサイト認証の 2 つである。

3.1.1 eIDAS 規則における電子署名、ウェブサイト認証の定義

eIDAS 規則では、電子署名について以下の 3 種類が定義されている。

1）電子署名

電子データに添付されている又は論理的に関係している電子形式のデータであり、署名者が署名する為に使用するもの。

2）先進電子署名

先進電子署名とは、以下の要件を満たす電子署名である。

a）署名者に一意的にリンクしている

b）署名者を識別することができる

c）署名者が、本人単独の管理のもとに、高いレベルの信頼を持って使用することができる電子署名生成データを使って作成されている

d）その後のデータへの変更を検知できる方法で署名されたデータにリンクされている

3）適格電子署名

適格電子署名生成装置を利用して生成され、電子署名の為の適格証明書に順ずる先進電子署名をいう。

先進電子署名の要件については、eIDAS 規則の下位規則である EU 委員会の実施決定(EU)2015/1506[4]によって PAdES[5]、XAdES[6]などの署名フォーマットの技術標準が指定されており、実質的に先進電子署名は PKI ベースの電子署名であり、そのうえで、ETSI 規格の技術要件を満たすものである。

適格電子署名は、先進電子署名に包含される電子署名であるが電子証明書を発行する認証局に対してより厳しい要件が課されおり、また、秘密鍵の管理と署名生成は適格電子署名生成装置によって安全性が確保されることを求めている。適格電子署名生成装置はコモンクライテリア認証を取得した製品が前提であり、現在のところ IC カードのようなハードウェアトークン以外のコモンクライテリア認証取得製品は存在しないため、適格電子署名にはハードウェアトークンの利用が必須である。以下の図 3.2 は、eIDAS 規則における電子署名の定義を整理したものである。

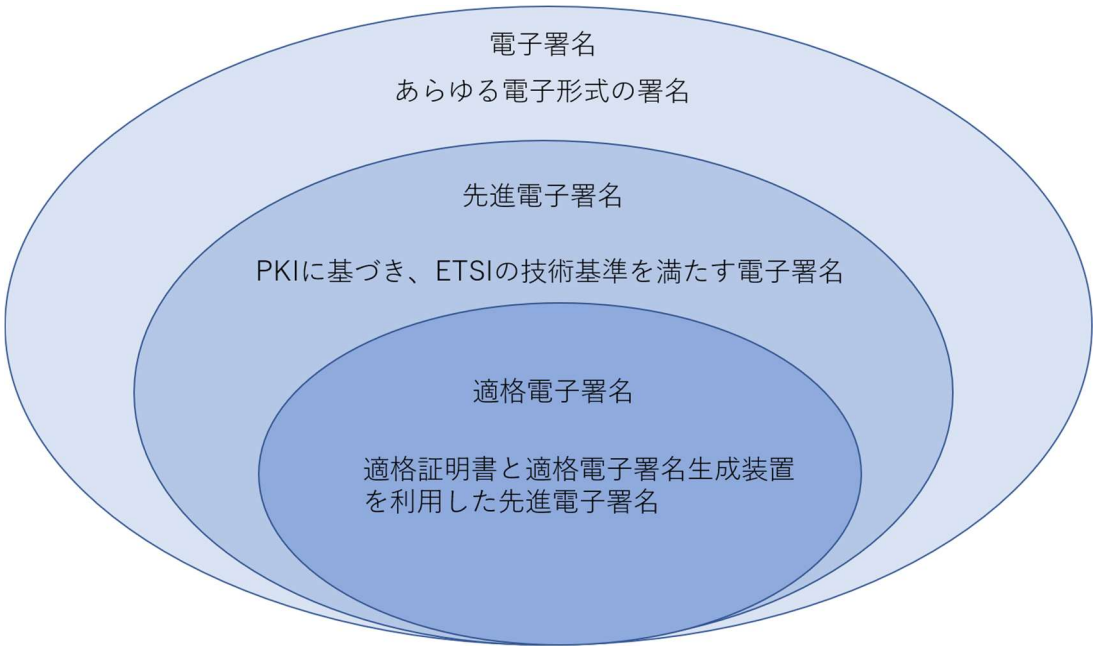

図 3.2　eIDAS 規則における電子署名の定義

ウェブサイト認証とはウェブサイトその管理主体を電子証明書によって認証する仕組みである。ウェブサイトをサポートする合法的な実体があることを、ウェブサイト訪問者が確信できる手段を提供することで、認証を受けたウェブサイトに対してユーザが信頼できるようになりオンライン取引における信頼や信用構築に寄与することが目的である。

eIDAS 規則では適格ウェブサイト認証と、適格でない通常のウェブサイト認証が定義されている。

3.1.2 eIDAS 規則における電子署名、ウェブサイト認証の法的効力

eIDAS 規則では、電子署名の法的効力について以下の様に定められている。

電子署名は、それが電子形式である、又は適格電子署名の要求事項を満たさないという理由だけで、法的効力及び法的手続きにおける証拠としての能力を否定されないこと。適格電子署名は、手書き署名と同等の法的効力をもつこと。

適格電子署名以外の電子署名についても法的効力は否定されていないが、適格電子署名については明確に手書きの署名と同等の法的効力を持つと定めている。適格でない電子署名については、その法的効力について疑義が生じた際は裁判でその妥当性を検証することが必要になる。

ウェブサイト認証の法的効力については、ウェブサイト認証によって何らかの電子取引が実現されるわけではなく、ウェブサイトとその管理主体を結びつきの信頼性を高めるサービスであるため規定されていない。

3.1.3 eID と電子署名の比較

eIDAS では eID によるオンライン認証という今までの電子署名指令になかった概念が定義されている。この eID によるオンライン認証と今までの電子署名との違いを纏めると以下の表 3.1 のようになる。

表 3.1　電子署名と eID の比較

	電子署名	eID
用途	法的拘束力を伴う取引(契約書へ署名 等	ID 認証, オンラインでの本人確認
比較対象	手書き署名と同等	免許証等による本人確認と同等
検証者	誰でも検証可能	限定された第三者が検証可能
検証可能期間	暗号強度によるが, 後からでも，何度でも検証可能	認証時一度のみ

電子署名とは、その名の通り電子的な署名であり、署名者が署名すると言う意思の元行われる。比較対象は手書きの署名であり、手書きの署名と同じように、署名後に署名者の検証が可能である。一方 eID によるオンライン認証は、本人確認と対応するものであり、オンライン上での本人確認を実現する。これは、運転免許証や旅券等の提示を要求する本人確認と同等であり、その本人確認の結果は、オンライン認証時の一度のみ有効であり、また、署名のように署名者の意思が反映されるものではない。

3.2　米国の法制 - ESIGN 法、統一電子取引法及び州法

米国の連邦法である ESIGN 法[7]でも電子署名や電子契約について電子形式であることを理由にその法的効力が否定されることがないことが定められている。ただし、例えば、EU における適格電子署名のように、どのような要件を満たせば、手書き署名や紙の契約書同じレベルの法的効力が保証されるかは定められていない。また、連邦法としての ESIGN 法に

加えて、米国は 50 の州で構成される合衆国であり、各州にはその州内でのみ有効な州法が存在するため、各州法に一貫性を持たせる目的で統一電子取引法（Uniform Electronic Transaction Act : UETA）[8]が定められている。統一電子取引法でも ESIGN 法と同様に電子署名や電子契約について、電子形式であることを利用にその法的効力が否定されることがないように定めているが、ESIGN 法に加えて、電子署名された電子データから署名者が特定できる形式での電子署名を求めている。

イリノイ州とワシントン州では、統一電子取引法を採用しておらず独自の州法[9][10]を定めている。両州法では電子署名に加えて、公開鍵暗号方式に基づくデジタル署名をより安全な電子署名として定めており、認証局や署名アルゴリズムに対する独自の要件を満たしたデジタル署名を安全な電子署名として手書きの署名と同等であることを認めている。

3.3　日本の法制度

日本では契約書や役所への申請書等の正式な文書には、署名と押印を行うことが一般的であり、これは、民事訴訟法第 228 条 4 項においても「*紙に記載され、押印もしくは、署名された文書等(契約書等の文書、議事録等等)は、真正に成立すると推定される*」とその法的効力が規定されている。一方で、電子的に作成された文書については改竄が容易であり、2000 年に電子署名及び認証業務に関する法律によって、この第三条「電磁的記録の真正な成立の推定」にて、一定条件を満たす電子署名を行うことによる電子形式のデータの真正な成立が認められている。この一定条件とは、署名に用いる秘密鍵そのトークンが適正に管理されている場合に、その電子署名によって署名者を特定できる形式であることである。

一方でこの法律の中では、署名者による秘密鍵及びトークンの管理方法について明確な要求が定められておらず、ハードウェアトークンの利用は前提となっていない。 これは、日本では従来署名だけでなく押印を行う商慣習があり、この印鑑の管理については押印者が適切に管理していることを前提としており、その管理方法までは定められていないことと同じ方式を電子署名の秘密鍵の管理にも適応したと考えられる。

電子署名及び認証業務に関する法律ではまた、署名者を特定できる電子署名のための認証業務として特定認証業務を定めており、また、特定認証業務を提供する事業者は主務大臣に認定を受けることができるとしている。電子署名及び認証業務に関する法律施行規則の第 2 条によってこの特定認証業務は公開鍵暗号方式に基づくこととされている。したがって日本における電子署名は、電子署名、特定認証業務に基づく電子署名、認定認証業務に基づく電子署名の 3 種類あることが分かる。

3.4　CA/B Forum

日本と米国ではウェブサイト認証について特に法的に要件が定められていないが、

Google、Microsoft や Mozilla 等のブラウザベンダーとウェブサイト認証の証明書を発行する認証事業者によって構成される CA/B Forum では、各ブラウザによって証明書が信頼されるための共通の条件を定めている。この共通の条件を満たした第三者監査として、ETSI EN 319 411[12]を用いた ETSI 認証と、WebTrust for CA を用いた公認会計士による監査の結果を受け入れており、Google クロームや、Internet Explore 等のブラウザに信頼できる証明書として登録する際に必須の要件となっている。

CA/B Forum が定めた要件を満たすウェブサイト認証の証明書を Extended Validation SSL サーバ証明書と言い、これはいわば業界統一の標準であるといえる。以下の図 3.3 は、実際の Extended Validation SSL サーバ証明書が実装されたサーバと SSL 通信が確立されていることをブラウザが表示している例である。このように安全な証明書が実装されていることがユーザに対して視覚的に認識されやすいように、各ブラウザによって異なるが、グリーンバーを表示する、南京錠のアイコンを表示する等の工夫がなされており、ほかの証明書の実装との区別が明確になっている。

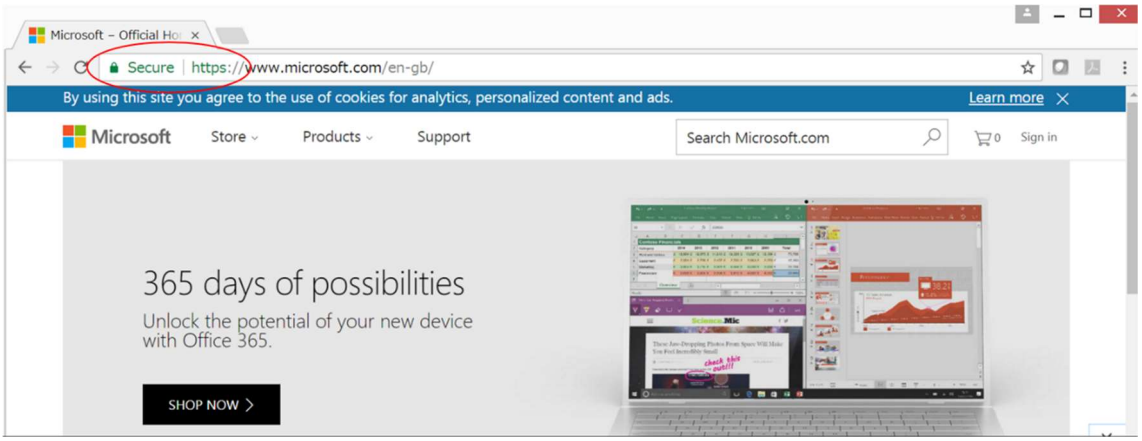

図 3.3 ウェブサイト認証

3.5 日米欧法制度の比較

日米欧の電子署名法制度を比較すると、一般に電子署名には法的に手書き署名と同等といえる電子署名と、他の方式と比べて署名者を技術的に特定できる電子署名とそれ以外の電子署名の 3 種類に分けられることが分かる。欧州では、適格電子署名が法的に手書き署名と同等といえる電子署名であり、先進電子署名が、署名者を技術的に特定できる電子署名であるといえる。米国においては、ESIGN 法及び統一電子取引法では、法的に手書き署名と同等とするための要件は定められていないものの、イリノイ州とワシントン州の州法で安全な電子署名としてのデジタル署名を定めており、その中で要件を満たすものを手書きの署名と同等と定めている。日本でも、電子署名について、認定認証業務に基づく電子署名、特定認証業務に基づく電子署名及びそれ以外の電子署名の 3 種類に分けることができ、認

定認証業務に基づく電子署名を最も信頼性の高い電子署名と位置付けており、署名押印と同レベルとしている。

以下の表 3.2 は日米欧の電子署名法制度をこの 3 段階の観点から分類した表となる。

表 3.2　日米欧電子署名法の整理

国	日	米	欧
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

日米欧の電子署名に関する法律には、以下の共通点がある。

① あらゆる形式の電子署名は電子形式であることを理由にその法的有効性が否定されていない

② 公開鍵暗号方式に基づく電子署名、すなわちデジタル署名は、署名者を技術的に特定できる電子署名である

③ デジタル電子署名の中でも要件を満たした署名を手書きの署名（日本の場合署名及び押印）と同等の法的効力を持つ電子署名とする

一方で日米欧の電子署名に関する法律には、以下の差異がある。

① 欧州では、適格電子署名に対して IC カードのようなハードウェアトークンの利用を前提としているが、日本及び米国では署名鍵の管理は署名者の責任で適切に管理されていることを前提としている。

以上のことから、日米欧間において、電子署名の法的効力、要件、定義について大きな差異は無く、法的効力の観点で相互承認に向けて大きな問題となりうるのはハードウェアトークン利用の有無だけであることが分かる。

4. 技術要件

4.1 欧州の技術要件 ― ETSI EN 規格

eIDAS 規則では、適格トラストサービスの法的要件を定めているが、その技術的詳細については、技術規格としての ETSI 規格によって定められている。認証局に対する要件としては ETSI EN 319 401[11], 411-1[12], 411-2[13]の 3 規格が整備されており、それぞれ、トラストサービスを提供する事業者の一般要求、証明書を発行する事業者の要件、適格証明書を発行する事業者の要件を定めており、各規格は以下の図 4.1 に示す通り、上位の規格を参照しており、例えば EN 319 411-2 の要件を満たすためには、EN 319 411-1, 401 の要件もそれぞれ満たす必要がある。

図 4.1 認証局向けの ETSI EN 規格の関連

また、EN 319 411-1 及び EN 319 411-2 では電子署名のための電子証明書を発行する認証局の要件のほかにもウェブサイト認証のための電子証明書を発行する認証局の要件等複数の証明書ポリシーが定められているが、本研究が研究対象とする証明書ポリシーは以下の 3 つである。

- QCP-n Policy for EU qualified certificate issued to a natural person
- QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD
- QCP-w Policy for EU qualified certificate issued to a natural or legal person and linking the website to that person

QCP-n 及び QCP-n-qscd はともに適格電子署名のための適格電子証明書を発行する認証局の技術的要件を定めており、QCP-w はウェブサイト認証のための適格証明書を発行する認証局の技術的要件を定めている。QCP-w には、CA/B Forum が定める EV 証明書の共通要

件である Extended Validation Guideline[14]、Baseline Requirement[15]及び Network and Certificate System Security Requirements[16]が盛り込まれており、これらの要件への適合性は QCP-ｗへの適合性を確保することで自動的に満たされる。

また、欧州では、適格電子署名については適格電子署名生成装置(QSCD)の利用を前提としている。QSCD とはコモンクライテリア認証を取得した安全なハードウェアトークンのことであり、このハードウェアトークン内で署名用秘密鍵を管理することが求められている。

4.1.1 ETSI EN 319 401

ETSI EN 319 401 は電子署名やウェブ認証だけでなく、すべてのトラストサービスを提供する事業者に対する一般的なポリシー要件である。この技術標準の要求事項は主として 3 つに分類できる。1 つ目はリスクアセスメントであり、トラストサービスプロバイダがトラストサービスを提供上でのリスクを識別／分析／評価し、そのリスクに対する適切な対策の実施と残存リスクの承認を求めている。また、リスクアセスメントを定期的に見直すことが求められている。2 つ目はトラストサービスの運用に係る規定とトラストサービス利用に関する条件の公開と、情報セキュリティポリシーの作成／維持／実施である。3 つ目はトラストサービスプロバイダの管理／運営に係る要件である。詳細は付録 1 に示すが、本項では各 3 点について解説する。

- **リスクアセスメント**

一般的なマネジメントシステムに要求されるリスクアセスメントの要件である。トラストサービスを提供する上で存在するリスクの識別、分析と評価し、各リスクに対して対策を講じることが求められる。また、リスクアセスメントは定期に見直さなければならない。

- **ポリシー及び運用**

トラストサービスが運用規定の公開が求められているが、これはつまり CP 及び CPS のことである。CP、CPS の作成及び公開と、主体者、加入者に対するサービス利用条件を公開することが求められている。また、情報セキュリティ方針文書を作成し維持することが求められている。

- **TSP の管理及び運営**

TSP のマネジメントシステム及び、技術的、組織的要件が定められており、以下の 14 項目に分類できる。

1. 組織の信頼性

財政的要件と公平性に関する要件が定められている。TSP は財政的に安定しており、また、保険に加入することが求められている。

2. 職務の分離

最小特権の原則に従った職務分掌権限規定を定めること。

3. 人的資源

また役割につく要員については、専門性、信頼性、経験及び資質を管理することが求められている。また、職務に違反した際の罰則を定めることが要求されている。

4. 資産管理

資産表の管理と記憶メディアの取り扱い

5. アクセスコントロール

不正アクセス保護対策、内部不正対策及び削除済みファイルによる漏洩への対策

6. 暗号管理

暗号鍵と暗号装置の管理

7. 物理的セキュリティ

物理アクセスの制限

8. 運用セキュリティ

セキュリティバイデザインの要件及びシステムの構成管理と完全性の保護。重要なイベントに対する手順の確立（認証局の場合、キーセレモニーや CA 鍵のバックアップ等）

9. ネットワークセキュリティ

論理ネットワークを複数のセキュリティレベルのゾーンに分けて管理すること。及び運用ネットワークとテスト環境、システム管理ネットワークの分離と通信チャンネルの保護。定期的に IP アドレスの脆弱スキャンと侵入試験を行うことが定められている。

10. インシデント管理

セキュリティ事故を予防、検出するためのイベント管理とログの監視及び、インシデント発生時の手順書を定めることが求められている。

11. 記録の管理
法的手続きに利用できるように TSP の業務に関する記録を管理すること。
12. BCM
事業継続計画を策定及び維持すること。

13. TSP の終了計画
業務終了時の計画書に関する要件。

14. コンプライアンス
法令への適合と個人情報の安全な取り扱い

4.1.2 ETSI EN 319 411-1

EN 319 411-1 はトラストサービスプロバイダの中でも、電子証明書を発行する認証業務を提供するプロバイダに関する要件を定めている。尚、本技術標準は、複数の証明書ポリシーがサポートされているが、本研究では、適格証明書を発行する際に要求事項となる NCP かつ、自然人を対象とした要件を調査比較対象としている。

EN 319 411-1 では、EN 319 401 のポリシー及び運用に関する要件と、TSP の管理及び運用に関する要件を認証局に対する要件となるように詳細化している。リスクアセスメントについては、EN 319 401 の要件がそのまま適用される。
まず、ポリシー及び運用に関する要件としては、CP、CPS を RFC 3647 に従った構成で定めることが求められている。また、CA の階層構造の説明と使用する署名アルゴリズムや鍵長等認証局特有の情報を含めることが求められている。
次に、TSP の運用について、以下の 9 項目の分類で要件が記述されている。

1. 公開と保管の責任
証明書使用に関する条件の常時（24 時間×7 日）公開及び、証明書の公開に関する要件

2. 本人確認
初回登録時の本人確認方法とその記録の保管、また証明書失効要求の受付に関する要件

3. 証明書ライフサイクル
証明書申請、発行、配布から失効までの証明書のライフサイクルを通じた要件。要件は以下に分類される。

- 証明書の発行申請

- 主体者の鍵ペアを認証局で生成しない場合、秘密鍵が主体者の管理下にあることを確認すること
- 登録システムと発行システム間のセキュア通信

- 証明書の発行
  - 主体者鍵生成プロセスにおける機密性の保護（証明書の偽造対策)、証明書に記載される識別名の一意性また、法人の属性を含む場合、証明書の識別子は法人を代表する自然人であること
  - ポリシー識別子を利用すること
- 証明書の受領
  - ユーザに対する証明書の使用条件および責任関して通知すること
  - 加入者との契約書の保管すること
- 鍵ペア及び証明書の使用

主体者及び加入者の義務として以下が定められている。

- 正確な情報の提出
- 鍵ペアの使用制限の遵守
- 秘密鍵の不正使用防止
- 鍵生成を主体者が実施する場合の安全性
- 鍵生成を主体者が実施する場合の単独管理の維持
- 秘密鍵の署名生成装置内での使用
- 秘密鍵の署名生成装置内での生成
- 秘密鍵の危殆化及び証明書の内容に変更がある場合の即時通知
- 危殆化時の鍵使用の中止
- 証明書失効あるいは認証局危殆化の連絡を受けた場合の鍵使用の中止

- 証明書の更新
  - 証明書の更新に過去の本人確認資料を用いる場合、更新する証明書の有効性と本人確認情報の有効性検証を行う。TSP の条件に変更があった場合の通知が必要で

ある。基本的には初回本人確認時の要求事項が適用される。

- 証明書の変更
  - 認証された本人確認情報に変更がある、或いは証明書が失効している場合、初回本人確認時の要件に従って登録情報を検証／記録する
- 失効及び停止
  - 証明書ステータスに変更があった場合の主体者／加入者への通知
  - 完全に失効された証明書の復旧防止
  - CRL の 24 時間毎の公開
    - 予定されている CRL 発行時刻の提示
    - CRL の署名
  - CARL の 1 年毎の更新
  - 相互認証がある場合、CARL の 31 日毎の更新
- 証明書ステータスサービス
  - 失効ステータスの可用性（24 時間 365 日）の保証と、失効ステータス情報の完全性及び真正性保護
  - 発行した証明書の有効期限切れまで、ステータス情報を提供すること
  - OCSP と CRL サポート（OCSP のサポートは推奨条件である)、両方がサポートされる場合、OCSP と CRL 間の情報の同一性を確保すること
- 鍵供託と鍵回復。

複製鍵の保護及び、主体者のソールコントロールの保証。鍵が暗号化によって保護される場合、HSM 内における安全性と同等の手段が講じられる必要がある。

4. 施設と運用管理

認証局の物理的セキュリティ要件して、認証局システムの物理的保護と入退室管理、機器及び記憶メディアの持ち出し制限、及びルート認証局の秘密鍵の隔離が定められている。手順管理としては、認証局の重要イベント（CA 鍵ペア生成、バックアップ、復旧等）の二重管理の要件が、監査ログの要件としては、全セキュリティイベント、CA 鍵関連のイベント、証明書ライフサイクル関連のイベントを監査ログの対象とし、記録の要件としては、証明書の有効期限から少なくとも 7 年間の記録保持を義務づけている。災害復旧に関しては、

5. 技術的セキュリティ管理策

以下の 7 の観点から、技術的セキュリティ要件が定められている。

- 鍵ペア生成とインストール

鍵ペアの生成アルゴリズムは、ETSI 規格で認められたアルゴリズムを利用すること。主体者の鍵の署名に使用する CA 鍵証明書の有効期限が切れる前に新しい CA 鍵証明書を生成すること。CA 鍵ペア生成手順の文書化し、キーセレモニー関連の役割と職務及びセレモニーの証拠の要件(ルート鍵の生成には第三者の立ち合いと署名が必要)を含めること。

- 鍵の安全な先生
  - CA 公開鍵の完全性を保証と CA 署名検証鍵の公開
  - 主体者の鍵生成への適切なアルゴリズムの使用
  - 主体者鍵の安全な生成と保管
  - 主体者の秘密鍵の安全な送付
  - 主体者秘密鍵の全てのコピーの削除
  - 署名生成装置の安全な交付
- 秘密鍵の保護及び暗号モジュールの技術管理
  - CA 鍵ペアの生成は HSM 内で行う
  - CA の秘密鍵は HSM 内で保持する
  - HSM 外で保管する場合、HSM 内と同等の保護レベルで保管すること
  - CA 秘密鍵のバックアップ、保管、復号は安全な環境で二重管理の下行われる
  - CA 秘密鍵のコピーは、使用されている鍵と同等のセキュリティレベルで管理されること
  - CA 秘密鍵及びコピーが専用の HSM 内で保管されている場合、鍵が暗号装置外で使用されないこと
  - HSM は輸送中に改ざんされないこと

- HSM は保管中に改ざんされないこと
- HSM は正しく機能すること
- HSM 廃棄時の、装置内秘密鍵の破棄

- 鍵ペア管理のその他の側面
  - CA 署名鍵の使用用途の制限
  - CA 証明鍵の物理的に安全な環境での使用
  - CA 秘密鍵の使用は証明書生成に使用される鍵長、署名アルゴリズム、ハッシュアルゴリズムと互換性があること
  - CA 署名鍵のライフサイクル終了時の全てのコピーの廃棄
  - CA がセルフサインする場合、証明書の属性は ITU-T 勧告 X.509[36]の Key usage に適合すること
- アクティベーションデータ
  - HSM での CA 鍵のインストール及び復旧は二重管理の下行われること
  - 主体者の署名生成装置の安全なディアクティベーション及びリアクティベーション
  - 主体者の署名生成装置のアクティベーションデータは署名生成装置とは別の手段で主体者に送付されること
- コンピュータセキュリティ管理
  - ローカルネットワークコンポーネントは物理的及び論理的に安全な環境で保持され、定期的に設定が見直されること
  - 証明書発行に直接かかわるすべてのアカウントは多要素認証を行う
  - 配布アプリケーションは証明書の追加、変更などの試みに対してアクセスコントロールを実施すること
  - 失効ステータスアプリケーションは、失効スタータス情報にアクセスコントロー

ルを実施すること

- 不正な試みに対して継続的な監視とアラーム設備を備えること

- ライフサイクルセキュリティ管理
  - 容量需要を監視し、適切な処理能力、容量を保証する
- ネットワークセキュリティ
  - 全ての CA システムを少なくともセキュアゾーンで保護し、セキュアゾーン及びハイセキュアゾーン間の通信を保護すること
  - 使用していないすべてのアプリケーション、アカウント、サービス、プロトコル、ポートを削除／停止すること
  - セキュアゾーン及びハイセキュアゾーンのアクセスコントロール
  - ルート CA システムはハイセキュアゾーンで維持すること

6. 証明書プロファイル

- 証明書
  - ETSI EN 319 412-2[13]に従うこと
- CRL
  - ITU-T 勧告 X.509[36]又は IETF RFC 5280[37]に従うこと
- OCSP
  - IETF RFC 6960[38]に従うこと

7. 適合性監査

ETSI EN 319 403 の要件にあった外部適合性監査を受けること。

8. 法的責任

- 個人情報の保護と登録データの機密性と完全性の保護
- 表明及び保証
  - TSP の一部が業務委託されていても TSP が本ポリシーへの充足に対して責任を持

つ

- CPS と一貫した認証サービスを提供する

9. その他の規定

組織の規定として、TSP の独立性及び公平性を保証すること。また、TSP が発行するすべての証明書を第三者がテストできること、そして、テスト用証明書はテスト用であることが明記されること。

4.1.3 ETSI EN 319 411-2

ETSI EN 319 411-2 は適格証明書を発行するトラストサービスプロバイダに要求される技術標準である。本標準も複数の証明書ポリシーを備えているが、本研究では、自然人に対して適格証明書を発行し、適格電子署名のためのポリシーである QCP-n-qscd を調査比較対象とする。EN 319 411-2 は、証明書を発行する認証局の要件である EN 319 411-1 について、eIDAS 規則に適合する場合の追加の要件を定めている。主な要求は以下の 6 つに分類することができ、それぞれについて説明する。

1. 本人確認

本人確認はフェイストゥフェイスで行う或いは、同等の方法と認められた手段に限る。

2. 証明書ライフサイクル

加入者が同意を電子的に示す場合、先進電子署名或いは先進 e シールを行うことが望ましい。

- 鍵ペア及び証明書の使用

鍵ペアは署名生成装置の中でのみ使用され、秘密鍵は主体者の単独管理の下維持する。鍵ペアは電子署名にのみ使用することが望ましい。

- 証明書失効ステータスサービス

失効ステータスは証明書の有効期限が切れた後も利用可能であること。失効ステータスの可用性について TSP の終了も含み正確に文書化すること

3. 施設と運用管理

監査ログについて以下の追加要件が定められている。

- QSCD の準備に係るすべてのイベントログ
- TSP は適格証明書の発行、生成、配布及び失効管理、QSCD の準備に係るイベントをログし、送受信データを記録すること
- TSP の終了後も法的要件を満たす目的で情報を管理すること
- 情報へのアクセス方法の文書化
- TSP は運用規定で情報の保管期間を正確に文書化し、終了計画により移譲される情報を示すこと

4. 技術的セキュリティ管理策

鍵ペア生成及びインストールについて、以下が定められている。

- 署名生成装置が認証製品であることを検証すること
- 署名生成装置が別の第三者の TSP により準備される場合、TSP はこの第三者の TSP が要求事項を満たしていることを検証すること
- 証明書要求プロセスは認証対象である公開鍵が署名生成装置によって生成された鍵ペアのものであることを確認すること
- 主体者の鍵ペアを TSP が生成し、署名生成装置にインポートする場合は、TSP が認証取得署名生成装置の想定環境を満たすこと
- TSP は署名生成装置証明書ステータスを証明書の有効期限が終わるまで監視し、ステータスに変更が生じる際は CPS に文書化された適切な措置をとる

5. 証明書プロファイル

- 証明書には ETSI EN 319-412-5[40]で規定される QC 宣言を含むこと
- 証明書には ETSI EN 319-412-5[30]で規定される QSCD 宣言を含むこと

- 証明書にはポリシー識別子を含むこと
- TSP が割り当てた OID のみが含まれる場合、どの証明書ポリシーをベースとしているか明示すること

6. その他の規定

証明書ポリシーには適格証明書のポリシーであること、QSCD の使用を要求することを明示すること及び、PKI 開示規定がサポートされていること。

4.2 WebTrust for CA

WebTrust for CA は、CA/B Forum が認める認証局の監査スキームであり、ウェブサイト認証ための電子証明書を発行する認証局の要件を定めた以下の 3 つの基準を定めている。

- Principals and Criteria for Certification Authorities[17]
- Principals and Criteria for Certification Authorities – Extended Validation Audit Criteria[18]
- SSL Baseline Requirements Audit Criteria[19]

これらの 3 基準もまた、CA/B Forum が定める Extended Validation Guideline、Baseline、Requirements 及び Network and Certificate System Security Requirements と整合の取れた基準となっている。

以下に WebTrust for CA の内容を説明する。

CA 業務規程の開示

認証局は RFC3647、RFC2527 の要求事項について認証局運用規定で開示すること。証明書ポリシーについては、RFC3647、RFC2527 の要求事項について開示すること。

CA 業務規程管理

- 認証局は証明書ポリシーのマネジメントプロセスが効果的であること保証する管理策を維持する

- 認証局は認証局運用規定のマネジメントプロセスが効果的であること保証する管理策を維持する
- 認証局は認証局運用規定が証明書ポリシーに含まれる内容に対応していることを保証する管理策を維持する

CA 環境の管理

CA 環境の管理に関する要件はさらに以下の 10 項目に分類される。

1. セキュリティ管理

セキュリティ管理に関しては、認証局は以下の保証する管理策を維持することが求められている。

- セキュリティの計画と管理
- セキュリティリスクの識別と管理
- CA 設備、CA システム、第三者がアクセスする情報のセキュリティ維持
- CA 機能が外部委託された場合の加入者及び依拠当事者の情報のセキュリティ

2. 資産の管理

リスクと規定に基づいた認証局の資産と加入者及び依拠当事者情報を適切に保護すること。

3. 要員のセキュリティ

要員のセキュリティについては、CA の運用をサポートする要員の管理策を設けることが要求されている。

4. 物理的セキュリティとネットワークセキュリティ

物理セキュリティについて、認証局は以下を保証する管理策を維持すること。

- CA 設備の物理アクセスのコントロール及び二重管理による運用
- CA 設備及び機器の環境災害からの保護
- 資産の損失、危殆化、業務継続への影響からの保護

- 情報及び情報機器の危殆化からの保護

5. 運用規定

情報システムの運用規定としては以下の要件がある。

- CA の情報システムの安全な運用
- CA システム障害リスクの最小化
- ウイルス及び悪意のあるソフトウェア対策
- インシデント報告及びインシデント管理策による損失、無効化リスクの軽減
- メディアの保護

6. システムアクセス管理

アクセスコントロールについて、認証局システムへのアクセスが許可されたものに限定されていること保証する管理策を維持すること。

- あらかじめ規定された権限者による OS 及びデータベースへのアクセス
- CA システムのネットワークセグメントへのアクセスは許可された要員、アプリケーションおよびサービスに限定されていること。
- CA アプリケーションの使用は許可された要員に限定されていること。

7. システムの開発と保守

システム開発及び保守について、システムの開発と保守は文書化され、試験され、許可されており、CA システムの完全性を維持するために実施されていること。

8. ビジネス継続性の管理

BCM について、災害時にも事業継続を保証する管理策を維持すること。

- CA の重要コンポーネントの災害復旧計画の開発維持
- 暗号製品の代替保管場所の規定
- 遠隔のバックアップシステムと、バックアップサイトの可用性保護

9. モニタリングと遵守

また、不正検知と CSR について、認証局は以下の保証する管理策を維持すること。

- 関連法律および契約の要求事項への適合
- CA セキュリティポリシーと手順への適合
- システム監査プロセスの効果の最大化とシステム監査プロセスによる悪影響の最小化
- 不正な CA システムの使用の検知

10. 監査ログ

監査ログについては以下の要件が定められている。

- CA の重要環境、鍵管理、証明書管理イベントはログされていること
- 監査ログの機密性と完全性の保証
- 公開されている業務規程に沿った監査ログの保存
- 許可された要員による監査ログの定期的なレビュー

CA 鍵ライフサイクル管理

認証局は CA の鍵ペアが公開されている業務規程及びキーセレモニースクリプトに定められている手順にしたがって生成されていること保証する管理策を維持すること。

認証局の公開される業務規程には以下を含むこと。

- CA の鍵生成は物理的に安全な環境で実施されること
- CA の鍵生成は信頼できる要員による二重管理の下実施される
- CPS に定められている適切な HSM を利用して CA 鍵生成が行われる
- CA 鍵生成がログされている

キーセレモニースクリプトは以下を含むこと。

- 参加者の役割と責任の定義
- キーセレモニー実施の承認
- 暗号ハードウェアと活性化キー
- キーセレモニーで実施される特定の手順
- セレモニールームの物理セキュリティ要件
- キーセレモニー後の暗号装置と活性化キーの保管場所
- キーセレモニーがスクリプト通り実施されたことに対する参加者及び立会人の署名
- キーセレモニースクリプトからのあらゆる差異の記述

CA 秘密鍵の機密性と完全性の保護。CA 秘密鍵のバックアップ及び復旧は、物理的に安全な環境で二重管理の下実施される。CA 公開鍵の完全性と真正性の保証。CA 鍵はあらかじめ定められた場所で、意図した目的にのみ使用されること及び、認証局は以下の保証する管理策を設ける。

- 保存された CA 鍵の機密性が保持され、プロダクションサイトには戻されないこと
- CA の公開された業務規程に従って、CA 鍵がライフサイクルの終わりに破棄されること

CA 鍵の危殆化の際にも CA の運営が継続され、危殆化した鍵で署名されたすべての証明書が失効され再発行されること

HSM に関して、認証局は以下を保証する管理策を維持する

- 秘密鍵の保管、復旧に使用されるデバイスは使用の前に完全性確認のためにテストされること
- HSM へのアクセスは許可されたものに限定されており、二重管理が実施されていること
- HSM が正しく動作していること

加入者鍵ライフサイクル管理

認証局は以下の保証する管理策を維持すること

- 加入者の鍵が公開されている CA の業務規程及びリスク分析に沿って安全な暗号ハードウェアによって生成されていること
- 生成された加入者の鍵が安全に配布されること

加入者鍵の保管と普及については、認証局は以下の保証する管理策を維持すること。

- CA に保管される加入者の秘密鍵の機密性及び完全性の維持
- CA に供託される加入者秘密鍵の機密性維持
- 鍵ライフサイクルの終了と共に CA が保管する加入者秘密鍵の安全な廃棄

署名性装置については、認証局は以下の保証する管理策を維持する

- IC カードの調達、準備、初期化が安全に管理されていること
- IC カードのアプリケーションデータファイルが安全に管理されていること
- IC カードの使用が認証局によって可能になっていること
- IC カードのディアクティベーションとリアクティベーションが安全に管理されていること
- IC カードが安全に保管され配布されること
- IC カードが安全に交換されること
- 返却された IC カードが適切に処理されること

加入者鍵管理について、認証局は以下の保証する管理策を維持する

- 加入者鍵保護の要件が適切に加入者に伝えれること
- CA の公開する業務規程の要件に沿った加入者鍵の管理ツールの提供

証明書ライフサイクル管理

加入者の登録にういて、認証局は以下の保証する管理策を維持する

- 加入者は正確に識別されていること
- 加入者の証明書発行要求は正確であり完全であり認められていること
- 証明書更新については、証明書更新要求は正確であり完全であり認められていること

証明書発行の際に、証明書は公開されている CA の業務規程に従って生成され発行されていることが要件となる。また証明書を配布する際には、公開されている CA の業務規程に沿って発行された証明書が加入者及び依拠当事者にわたること。公開されている CA の業務規程に定められている期間で証明書が、認められ、検証された失効要求に従って失効されること、公開されている CA の業務規程に定められている期間で証明書が、認められ、検証された停止要求に従って停止されること。公開されている CA の業務規程にそって、正確な証明書ステータス情報が関係者に公開されること。

下位認証局ライフサイクル管理

位認証局は以下の保証する管理策を維持すること。

- 下位認証局の証明書要求が正確で認められたものであること
- 下位認証局の証明書更新要求が正確で認められており、完全であること
- CA の業務規程に従って下位認証局のリキー、更新或いは新規証明書が発行されること
- CA の業務規程に従って、発行された証明書が下位認証局にわたること
- 下位認証局の証明書は許可され、検証された失効要求によって失効される
- CA の業務手続きに従って、正確で完全な証明書ステータス情報が全ての関係者に公開される

4.3 技術要件の詳細度

第三者監査の基準について議論となる点として、技術基準に記載されている要件の詳細度がある。要件が詳細であるほど監査結果の再現性は高くなり、監査会社、監査員毎の結果に差異が生じにくくなるが、一方でより形式的な監査となってしまい、監査員の本質的実質的な見地からの適合性判断を阻害しかねない。Thijs R. Timmerman らは、WebTrust for CA の基準と ETSI 規格を比較し、WebTrust for CA がより詳細度の高い要件となっていると結論付けたが[20]、このことから ETSI 規格が WebTrust for CA と比較して劣った基準であるとは言えない。

4.4　日本の技術要件

日本においては、電子署名のための証明書を発行する認証局の技術要件として、以下の法律施行規則、指針、方針が定められている。

- 電子署名及び認証業務に関する法律施行規則[21]
- 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針[22]
- 電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針[23]

法律施行規則、指針、方針の関係性は、施行規則を詳細化したものが指針であり、また、指針への適合判断をより詳細化したものが方針であるといえる。

また、認証業務の特定性を調査する指定調査機関である一般財団法人 情報経済社会推進機構の電子署名･認証センターから､特定認証業務の認定に係る調査表[24]が策定されおり、この調査表の中では、上記方針の内容をより具体化したものを「適合例」として記載している。

以下に日本の技術要件を説明する。日本の技術要件は、認証局設備に関する基準、本人確認に関する基準、その他業務に関する基準及び記録に関する基準の 4 分類で構成されている。

認証局設備に関する基準では入退室管理、物理的セキュリティ対策、ネットワークセキュリティ、アクセスコントロール、暗号装置及び災害防止に関する要件が定められている。

入退室管理

- 生体認証と二重管理による認証室への入退室管理
- 入室権限者の設定と識別／認証
- 入退室の人数管理とアラームシステムの連携
- 設定された入退室時間の超過によるアラーム
- カメラ、センサーなどによる自動的／継続的監視
- 登録端末、主体者識別設備が設置された部屋は施錠されること

ネットワークセキュリティ

- 認証業務用設備がネットワークにつながる場合、ファイアフォールや不正なアクセスを検知するシステムを備えること
- 認証業務用設備が 2 つ以上の部屋に設置され、互いにネットワークにより接続されている場合、セキュアな通信チャンネルの利用
- 主体者が主体者署名鍵を生成する場合において、主体者署名鍵を認証局が受信する際は、受信機の誤認及び盗聴等から保護すること

アクセスコントロール

- 認証業務設備は個人単位でアクセスコントロールを実施すること
- 利用前に識別／認証すること
- あらかじめ主体者ごとにアクセス権限を定めること
- 主体者署名鍵を主体者が生成する場合において、主体者情報及び主体者証明書によって自動的に認証業務用設備を作動させる場合、あらかじめ主体者情報及び主体者証明書を設定しておくこと
- 主体者証明書等受信装置は鍵などが取り付けられた部屋に備えれており、無人の際は施錠されること
- 電子証明書の発行及び失効の要求等の管理に必要な登録用端末設備以外はネットワークを通じた遠隔操作が不可能となるように設定すること
- 認証業務用設備の所在を明らかにしないこと
- 各イベントのログをとる監視機能を備えること
- 監視機能は操作者ごとに履歴を確認できること

暗号装置

FIPS140-2 相当の HSM の使用

災害防止

- 耐震措置

- 水害防止措置
- 認証設備質の隔壁
- 自動火災検知器と消火器の設置
- 認証設備室は防火区域ないであること
- 停電対策
- 安定した地盤であること
- 耐震性のある建物であること
- 準耐火建物であること

本人確認に関する基準では認証業務の主体者の本人確認を行う際に必要な本人確認資料について主に定められている。有効な本人確認資料は以下のとおりである。

- 印鑑証明
- 公的個人認証
- 住民票の写し
- 戸籍謄本
- 住民票記載事項証明書等

これらの本人確認資料の有効性を確認することが求められている。

その他業務に関する基準は以下の 14 項目の基準に分類されている。それぞれについて説明する。

- 主体者の責任に関する説明責任

  主体者に以下の事項の説明すること。

  - 虚偽の申し込みによる不実の証明となった場合、罰せられること
  - 電子署名の法的有効性と署名鍵の安全な管理
  - 危殆化の際の失効要求
  - 指定する署名アルゴリズムの利用

- 主体者申し込み書の記載事項

  主体者申し込み書は以下の情報を満たすことが求められる。

  - 利用用途
  - 主体者指名のローマ字表記
  - 自署または印鑑証明書を本人確認に用いた場合、当該印鑑による押印
  - 代理人が申し込む際には代理の理由及び代理人の自署名または押印

- 主体者の鍵ペア生成
  - 主体者署名鍵を認証局が生成する場合は、安全に主体者に送信し、当該署名鍵のコピーをすべて削除すること
  - 主体者署名鍵を主体者が生成する場合において、当該主体者公開鍵をネットワークを通じて認証局が受信する場合、あらかじめ主体者証明書を安全な形で主体者に送付し、また、当該主体者の識別に用いるまで、第三者に知られないようにすること

- 電子証明書の要件
- 電子証明書の有効期間は 5 年を超えないものとする
  - 電子証明書には以下の情報を含む
    - 発行者の名称及び発行番号
    - 発効日及び有効期限
    - 証明書主体者の氏名
    - 主体者公開鍵及びアルゴリズム識別子
  - 電子証明書発行に係る電子署名方式は以下のいずれかとする
    - SHA-1, 256, 384, 512, かつ鍵長 1024bit 以上 RSA 方式
    - SHA-1, 256, 384, 512 かつ鍵長 1024bit 以上 RSA PSS 方式
    - SHA-1, 256, 384, 512　かつ鍵長 160　bit 以上 ECDSA 方式

- ✧ SHA-1, かつ鍵長 1024bit 以上 DSA 方式

- 認証業務の誤認防止
  - 認証業務に関して主体者が認定認証業務とその他認証業務を誤認する措置を講じること
  - 発行者電子署名鍵を認定認証業務にのみ使用すること
  - 発行者公開鍵に係る電子証明書の値を SHA-1,256, 384, 512 のいずれかで変換した値で認定認証業務を特定すること
- 電子証明の属性情報

  役職等の属性情報は認定対象外であることを電子証明書に明示すること
- 検証情報の提供
  - 署名検証者が検証に必要な発行者公開鍵その他情報を署名検証者に公開すること
  - 証明書ステータス情報の公開
  - 証明書利用目的と利用制限の通知
- 電子証明書の失効
  - 主体者から電子証明書の失効要求を受けた或いは、電子証明書の内容に変更があった場合は失効に関する情報を記録すること。
  - 失効要求の真偽確認方法、記録手続きを定めていること
  - CRL、OCSP 等による失効情報の提供
  - 失効した旨を遅延なく主体者に通知すること
- 認証業務の実施規定

  以下を認証業務規程に含めること
  - 認証事業者の連絡先（住所、電話番号、ファクシミリ番号及びメールアドレス）を認証業務規程に明示すること
  - 電子証明書発行対象

- 電子証明書の使用目的、制限
- 主体者の属性情報が認定対象外であること
- 認定事業者の保証と責任
- 保証及び面積範囲
- 利用申込必要書類
- 主体者の真偽確認方法、本人確認資料
- 電子証明書失効に係る情報
- 電子証明書失効情報確認に係る情報
- セキュリティに関する事項
- 個人情報の取り扱いに関する事項
- 料金に関する事項
- 認証業務において保存する帳簿書類の保存期間、保存方法等
- 業務の廃止時の発行済み電子証明書の失効方法、主体者への通知方法
- 適用法令及び管轄裁判所の情報
- 規定の改訂とその通知方法に係る事項

● 認証業務の廃止

- 廃止の 60 日前までに主体者に通知すること
- 発行済み電子証明書が失効されることの通知

● 主体者情報の開示

電子証明書の名義人からの申し出に応じて当該電子証明書に係る主体者に関する書類を開示すること

● 組織及び体制

以下の事項を定めること

- 業務の手順

- 職務分掌権限規定
- 指揮命令系統
- 業務委託時の受託者による適切な管理の実施を確保する方法
- 業務の監査に係る事項
- 要員の知識／経験
- 個人情報保護
- 危機管理に関する事項

● 認証業務設備の操作権限

認証設備室へのアクセスコントロールの実施

- 二重管理
- アクセス権限の登録

やむを得ず、権限のないものがアクセスする場合は権限のあるものが複数同行すること

システム管理者の証明書の厳重な管理

● CA 鍵の漏洩防止

- 発行者署名鍵の生成は二重管理の下実施される
- 発行者署名鍵は認証設備室内で HSM を用いて生成される
- 発行者署名鍵のバックアップ及び復帰は二重管理の下実施される
- バックアップの適切な保護
- 発行者署名鍵の状態変更は認証設備室内で二重管理のもと実施される
  - ✧ 発行者署名鍵の使用を終了する場合、二重管理の下物理的に破壊、或いは完全な初期化を行う、またコピーされた鍵も同時に廃棄する

記録に関する要件は、認証業務利用申請関する記録、電子証明書の失効に関する記録、認証事業者の組織に関する記録、設備及びセキュリティに関する記録の 4 つに分類される。

認証業務利用申請に関する記録

認証業務の利用申し込みに関する帳簿書類で次に掲げるものは、電子証明書の有効期限満了から 10 年間保存する

- 主体者申込書
- 本人確認資料
- 申込の諾否を決定したものの氏名
- 承認されなかった場合その理由
- 電子証明書作成に係る記録
- 発行者公開鍵
- 発行者署名鍵の作成／管理に関する記録
- 認証事業者が主体者署名鍵を生成した場合、主体者からの主体者署名鍵の受領書

電子証明書の失効に関する記録

電子証明書の失効に関する帳簿書類で次に掲げるものは、電子証明書の有効期限満了から 10 年間保存する

- 失効請求書及び失効判断に係る記録
- 失効を決定したものの氏名
- 失効拒否となった場合その理由
- 全ての失効情報

認証事業者の組織に関する記録

認証業務の組織管理に関する帳簿書類で次に掲げるものは、電子証明書の有効期限満了から 10 年間保存する

- CP、CPS
- 業務手順の変更記録
- 職務分掌権限規定、組織図などの変更記録

- 業務委託契約書
- 監査実施記録

設備及びセキュリティに関する記録

認証業務の利用申し込みに関する帳簿書類で次に掲げるものは、作成日から認定の更新日まで保存する

- 入退室に関する記録
- 不正アクセスの記録
- 認証業務用設備の動作記録
- 許諾記録
- 認証業務用設備関連の維持記録
- 障害と復旧に関する報告書
- 帳簿書類の利用と廃棄に関する記録

4.5 技術要件の比較

ここまでで、欧州には電子署名とウェブサイト認証に対する技術要件が ETSI 規格として整備されており、日本では電子署名に関する技術要件だけが、法律施行規則、指針として定められていることが分かった。また、米国では WebTrust for CA というウェブサイト認証の為の証明書発行する認証局のための監査スキームがあるので、本研究では技術要件に関して、日欧の電子署名に関する技術要件の比較と、欧米のウェブサイト認証に対する技術要件を比較する。

4.5.1 日欧電子署名技術要件の比較

下の表 4.1 は電子署名に関する日欧の技術要件の項目を洗い出したものである。日本の秘術要件と比較して ETSI 規格の特徴としては以下があげられる。

- マネジメントシステムベースの規格である
  リスク分析を前提としており ISO27000 シリーズの概念が盛り込まれている

- デモンストレーションの確認

現地監査時は、過去の履歴を中心に調査するのではなく、実際に証明書の発行プロセスをデモンストレーションさせ、運用方法に問題がないかを確認する

- 要員の信頼性に対する厳しい要件

雇用時に過去の犯罪歴などを確認するバックグラウンドチェックの要件や、故意の規定違反または重大な過失に対する罰則規定が求められている

- 財務上の要求

信頼できる組織の要件として、財政的に安定している組織であることが求められている

- 廃局時の要求

何らかの事情により、業務を終える際に他サービスへの引継ぎなどが求められている

表 4.1 日欧電子署名技術要件の範囲

EN 319 411-1,2		
5 認証業務運用規定及び証明書ポリシーに関する一般規定	施行規則	指針
6 トラストサービスプロバイダの運用	1. 業務の用に供する設備の基準	1.1 認証設備室への入出場を管理するために必要な措置
6.1 公開及び保管の責任	2 利用者の真偽の確認の方法	1.2 認証業務用設備への不正なアクセス等を防止するために必要な措置
6.2 識別及び認証	3 その他の業務の方法	1.3 正当な権限を有しない者による認証業務用設備の作動を防止するための措置等
6.3 証明書のライフサイクル運用要件	4 帳簿書類	1.4 発行者署名符号の生成管理に使用する暗号装置
6.4 施設、管理、及び運用管理		1.5 認証業務用設備等の災害の被害を防止するために必要な措置
6.5 技術的セキュリティマネジメント		
6.6 証明書、CRL、及びOSCPプロファイル		2.1 認証業務の利用申込み等
6.7 適合性の監査及びその他の評価		2.2 利用者の真偽の確認方法等
6.8 その他の事業及び法的事項		
6.9 その他の規定		3.1 利用申込者に対する説明事項
		3.2 利用申込書等の記載事項等
		3.3 利用者署名符号及び利用者識別符号の生成等
		3.4 電子証明書に係る事項
		3.5 認定認証業務と他の業務との誤認を防止するための措置
EN 319 401		3.6 電子証明書への属性の記録
5 リスクアセスメント		3.7 署名検証者への情報提供
6 ポリシー及び運用		3.8 電子証明書の失効に係る事項
6.1 トラストサービス運用規定		3.9 認証業務の実施に関する規程
6.2 契約条件		3.10 認証業務の廃止
6.3 情報セキュリティポリシー		3.11 電子証明書名義人への情報の開示
7 TSPの管理及び運営		3.12 認証業務実施のための組織及び体制等
7.1 内部組織		3.13 認証業務用設備の操作等に関する許諾等
7.2 人的資源		3.14 発行者署名符号の漏えいを防止するために必要な措置
7.3 資産管理		
7.4 アクセスコントロール		4.1 認証業務利用申込に関する帳簿書類関係
7.5 暗号管理		4.2 電子証明書の失効に関する帳簿書類関係
7.6 物理および環境セキュリティ		4.3 認証事業者の組織管理に関する帳簿書類関係
7.7 運用セキュリティ		4.4 設備及び安全対策措置に関する帳簿書類関係
7.8 ネットワークセキュリティ		
7.9 インシデント管理		
7.10 証拠の収集		
7.11 事業継続マネジメント		
7.12 TSPの終了および終了計画		
7.13 コンプライアンス		

一方で、日本の技術要件には、欧州の技術要件と比較して以下の差異を見つけることができた。

- 適合例の明示

調査表の中に、具体的な適合例が明示されており、要件だけが規定されている ETSI 規格と比較し、より解りやすい

- 暗号モジュールに対する詳細な要件

暗号モジュールについて ETSI 規格では他の技術規格を参照しているが、日本の技術要件では参照できる規格が存在しないため、詳細に規定されている。技術的には米国の FIPS140-2[25]を意識した記述となっており、コモンクライテリア認証を前提としている ETSI 規格と差が生じている

- サンプルチェック

調査時には、発行された証明書の数から妥当なサンプル数を抽出し、証明書の発行プロセスに問題がなかったか確認する

技術要件として大きな違いは暗号モジュールの評価に関する点と、罰則規定、バックグラウンドチェック、財務の安定性等日欧の文化、商慣習の違いから生じていると考えられる部分にある。暗号モジュールに関しては、ベンダーが限られており、実質的に、ベンダーの主力製品は FIPS140-2 とコモンクライテリアの両方の認証を取得することが想定され、日本の認証局がこれらの主力製品を導入している場合は差異が生じないが、仮にそうでない場合、相互承認には、日本の技術要件にコモンクライテリア認証を盛り込む必要性が生じる。一方でコモンクライテリアの認証結果を受け入れる相互認証の枠組みである Common Criteria Recognition Agreement(CCRA)[26]によると、現在の相互承認の範囲は評価保証レベル 2 までとされており、欧州が暗号モジュールに対して求める EAL4 以上の認証については CCRA の相互承認の範囲外となっており、コモンクライテリアを要件とすることについては障害が大きいと考えられる。

文化、商慣習の違いに起因すると感がられる罰則規定、バックグラウンドチェック、財務の安定性について、特に難しいと考えられる点はバックグラウンドチェックである。日本には雇用時に、個人の犯罪履歴等を確認する仕組みが非常に限られており、実質的に民間サービスである認証局がバックグラウンドチェックを行うのは非現実的である。この点については、2017 年 7 月 4 日の日欧インターネットトラストシンポジウムでも問題提起しており、今後の重要な論点となると思われる。

4.5.2 ウェブサイト認証の為の技術要件比較

ETSI 規格も WebTrust for CA もそれぞれ CA/B Forum が定める共通要件を反映した基準となっており、また、現在のところのこの ETSI 規格と WebTrust for CA を利用した第三者監査のみが CA/B Forum で信頼できるルート証明書の登録時に受け入れられる監査として定められていることから、監査結果のブラウザ登録への利用という観点では相互承認が可能であると思われる。また、Thijs R. Timmerman らの研究によれば少なくとも ETSI 規

格と WebTrust for CA は同じ分野の要求事項を持っていることが分かる。下の図 4.2 は、ETSI 規格と WebTrust Fro CA について、要求事項の関係性を示した図である。共通の要件として、CA/B Forum からの要求である Network and Certificate System Security Requirements、Baseline Requirements、Extended Validation Guideline が盛り込まれており、また、非共通部分についても、少なくとも同じ分野、範囲について要件が定められていることが分かる。

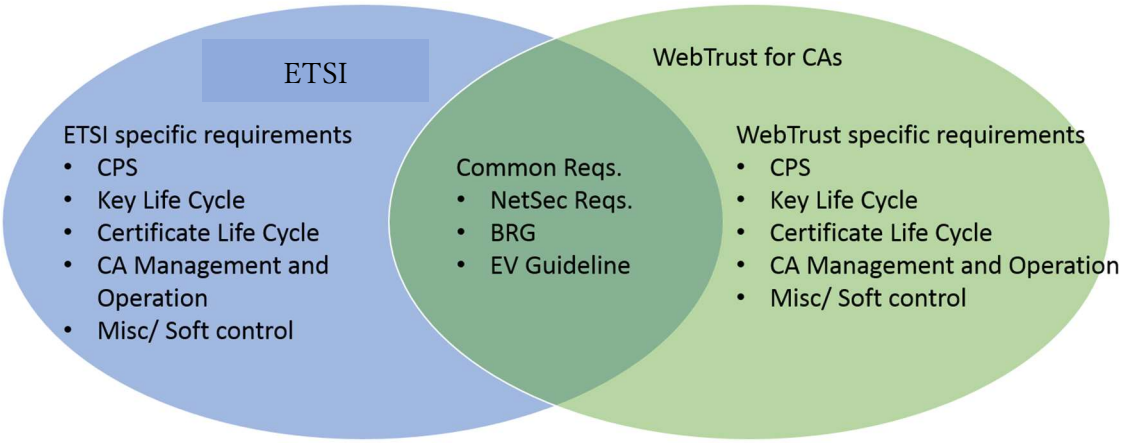

図 4.2 ウェブサイト認証の為の技術要件の比較

5. 最低技術要件

4 章で比較した技術要件から共通要件を導出し、最低技術要件を以下に定める。

1　リスクアセスメント

認証局は認証業務を提供する上でのリスクアセスメントを実施しなくてはならない。リスクアセスメントの結果は少なくとも年に一度見直しを行うこと。

2　CA の文書

認証局はその業務に係る以下の文書を定め、その文書に従って運営されなければならない。

2.1　ポリシー文書

認証局は、RFC 3647 の構成で証明書ポリシーを規定し公開しなければならない。

2.2　認証業務規程

認証局は認証業務規程（CPS）を規定し、公開しなければない。

2.3　情報セキュリティポリシー

認証局は、リスクアセスメントを基に、情報セキュリティポリシーを規定しなければならない。

2.4　条件の公開

認証局は、そのサービスを利用する、あるいはそのサービスに依拠する際の条件及び注意事項を公開しなければない。

3　認証局の運用

3.1　組織の要件

3.1.1 信頼性

認証局は、公正、公平及び中立でなければならない。また、財政的に安定していること。

3.1.2 職務分掌

認証局に必要な役割及びその責任を文書化すること。役割と責任が適切に分離されていること。

3.1.3 要員

雇用時、及び役割に付く際には、要員の経験、知識、資質を評価し適切な教育を実施すること。

3.2 資産管理

認証局は資産表を作成し、リスク評価と併せた資産の管理を実施すること。

3.3 セキュリティ管理

3.3.1 物理的セキュリティ

認証局の重要設備はすくとも二重管理下の安全な環境に設置すること。安全な環境の実現には、アラームやアクセス制御による保護を用いること。

3.3.2 ネットワークセキュリティ

ネットワークをゾーン別に管理し、ゾーン間の通信には暗号通信を用いること。ネットワークには定期的な脆弱性スキャンと、侵入試験を実施すること。また、運用環境と試験環境は分離すること。業務に不要なアプリケーション、ポート、プロトコル、サービスはすべて削除或いは停止し、セキュリティソフトを最新の状態に更新しておくこと。

3.3.3 アクセスコントロール

認証局は不正アクセスから保護する手段を講じること。システムアカウントはすべて個別に識別／認証され、権限のある者のみが許可されたデータ、システム、領域へアクセスできること。権限については定期的に見直しを実施し、不要なアカウントに権限が残らないように注意すること。証明書発行に係るすべての要員は多要素認証によってログインすること。

3.3.4 ログ

認証局はセキュリティイベントのログを記録し、定期的に見直すことで、インシデントの発生を予防する或いは、インシデントの影響を最小化する措置を講じること。また、すべての証明書及び鍵ライフサイクルイベントはログの対象とすること。認証局は保管されているログの完全性と可用性を確保しなければならない。

3.4 認証業務

3.4.1 本人確認

本人確認は、フェイストゥフェイスでの実施或いは、信頼性の高い認証手段を用いること。本人確認資料には、適切で認められた資料を用いなければならない。

3.4.2 証明書ライフサイクル

3.4.2.1 発行

認証局は、本人確認結果に基づき、一意な鍵ペアの生成と証明書を発行しなければならない。

3.4.2.2 配布

発行された鍵ペア及び、証明書は主体者に安全な手段で配布されること。

3.4.2.3 失効

認証局は証明書の失効リクエストを受けた際に、失効リクエストの確認を行い、確認結果に応じて、証明書の失効を実施しなければならない。

3.4.3 証明書ステータス

認証局は証明書の失効情報を少なくとも CRL によって公開しなければならない。失効情報には認証局の署名を施すことにより、完全性と真正性を保証することが必要となる。失効ステータスは証明書の有効期限切れ後も利用可能であるものとし、また、認証局がその業務を終了する際には第三者に引き継ぐ取り決めを保持しておくこと。

3.5 鍵ライフサイクル

3.5.1 CA 鍵

CA 鍵の使用及び管理はすべて安全な環境下で且つ、認められた要員による二重管理の下、実施されること。キーセレモニーについては、事前にキーセレモニープロトコルを作成し、プロトコルに沿って実施されること。また、その際は外部監査員の立ち合いの下、実施されること。キーセレモニーのプロトコルにはすべての参加者の自筆署名を付すこと。CA 鍵は有効期限が切れる十分前に、切り替えを行うこと。

3.5.2 鍵生成

鍵の生成は CC 或いは FIPS140-2 のセキュリティ認証を取得した暗号モジュールによって安全な環境下で実施されること。

3.5.3 秘密鍵の保護

主体者秘密鍵の全てのコピーは削除されること。鍵のバックアップを行う場合は、暗号モジュール内で保管される場合と同等の保証レベルの暗号を用いること。

3.5.4 鍵のバックアップと復旧

CA 鍵のバックアップ及び復旧は安全な環境下で二重管理の下実施されること。

3.5.5 暗号アルゴリズム

認証局は適切な暗号アルゴリズムを鍵生成に用いること。常に推奨アルゴリズムの動向を予測し、鍵のライフサイクルにわたってアルゴリズムの危殆化を避けること。

3.6 外部監査

認証局は、その運用は適切な法令及び本規定に遵守していることを信頼できる第三者機関による監査によって保証しなければならない。監査は毎年一度実施するものとする。

3.7 その他の要求

3.7.1 個人情報保護と法令順守

認証局は個人情報の取り扱い及びその他の業務について、関連法令を遵守しなければならない。

3.7.2 認証局の業務終了

認証局は業務の終了する際の計画書を定めなければならない。

3.7.3 災害復旧

認証局は災害リスクを考慮し、システムのバックアップを講じなければならない。バックアップサイトについては、想定される同一災害で被害を受けない場所を選定すること。

3.7.4 記録の管理

本人確認資料、証明書ライフサイクル記録、鍵ライフサイクル記録、その他セキュリティログについて、法令が定める年数保持しなければならない。

6. トラストフレームワーク

6.1 トラストモデル

本研究では PKI に基づくトラストサービスをテーマとしており、トラストのモデルについても PKI を前提としているが、PKI とは違う仕組みトラストモデルとしてブロックチェーンがある。ブロックチェーンは特定の権威に依拠せずにトラストを確立するモデルであり、PKI におけるトラストモデルでは必ずトラストを保証するトラストアンカーが存在することに比べて対象的である。以下の図 6.1 は、PKI の電子署名におけるトラストモデルである。この場合、認証局（CA）がトラストアンカーとなり、署名に使用された鍵がアリスの秘密鍵であることを保証している。

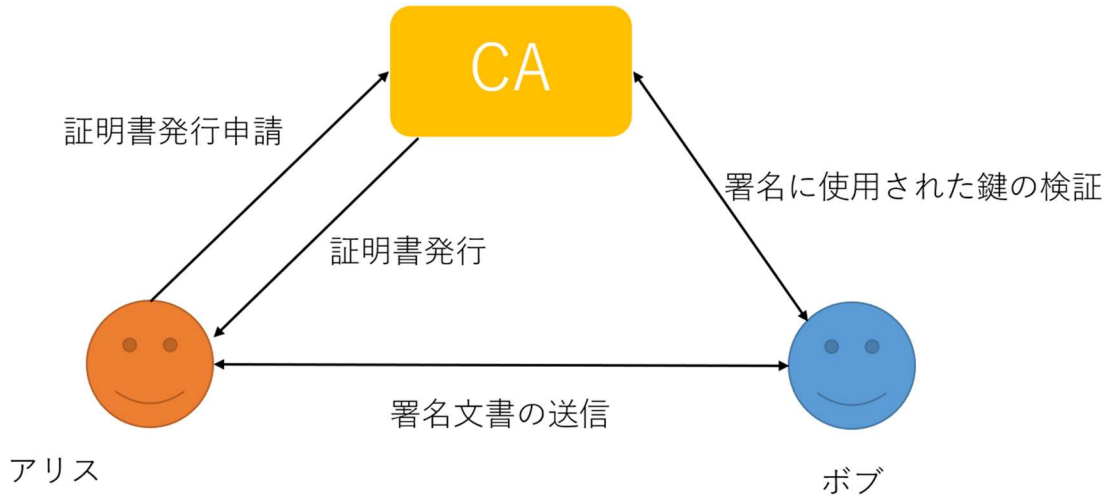

図 6.1　PKI のトラストモデル

ブロックチェーンのトラストモデルでは、PKI における認証局のようなトラストアンカーは存在せずに、ネットワーク上で台帳を共有する個人個人の集合によりトラストを形成する。この台帳にはこれまでの取引履歴が記録されており、これによって不正や改竄を検知する仕組みであり、不正利用や改竄の為には、ネットワーク上の多数の台帳を攻撃する必要がある。

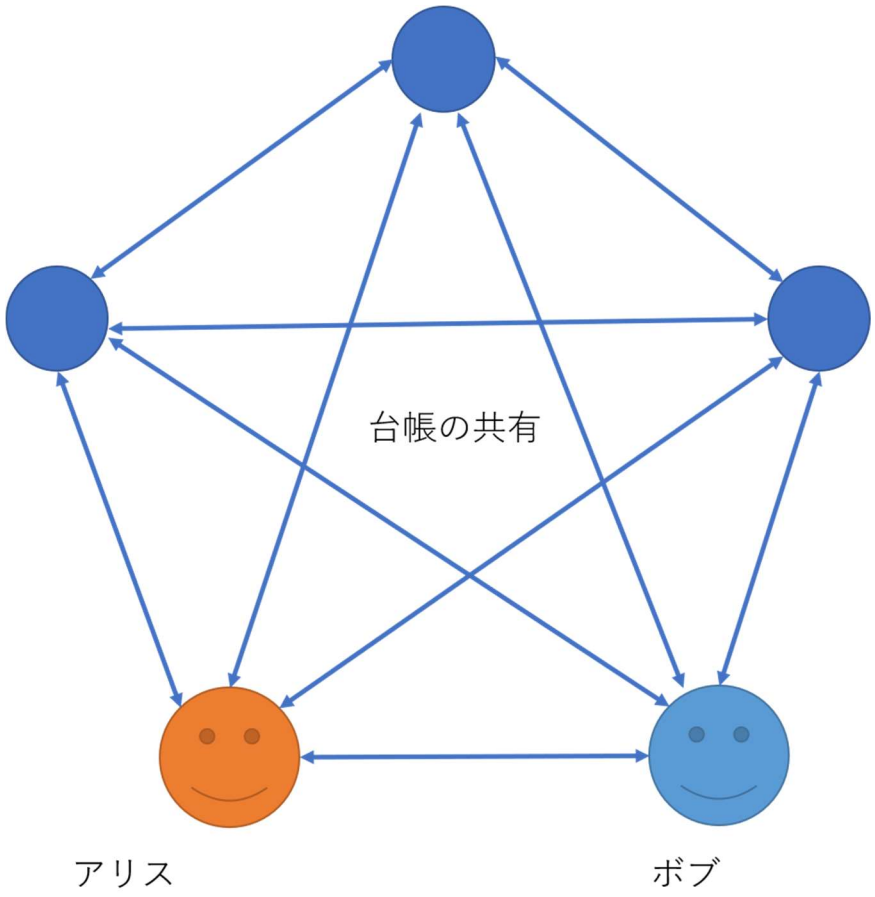

図 6.2 ブロックチェーンのトラストモデル

6.2 eIDAS 規則及び ETSI 認証のトラストフレームワーク

eIDAS 規則では、各加盟国に監督機関と適合性調査機関を指定することを求めている。監督機関は、加盟国内のトラストサービスが eIDAS 規則に従った形で提供されていることを監視する役割があり、また、適合性評価機関からの適合性評価報告書に基づいて、そのトラストサービスの適格性の可否を判断する。監督機関は一般的に国の期間であり、例えばドイツでは連邦ネットワーク庁が担っている。一方適合性評価機関については、その資格を国家認定機関によって認定を受ける必要がある。この認定プロセスについては加盟国間で祖語が生じないように、European Cooperation for Accreditation(EA)と呼ばれる調和機関によって認定スキームの調和が保たれている。監督機関がトラストサービスを適格トラストサービスであると認める場合にはトラストリストに登録することができ、依拠当事者はこのトラストリストを以て、例えば電子署名が適格トラストサービスプロバイダが発行した適格電子証明書に基づく電子証明書であるかを検証することができる。この点において、トラ

ストリストはこのトラストフレームワークにおける信頼の起点、トラストアンカーであるといえる。

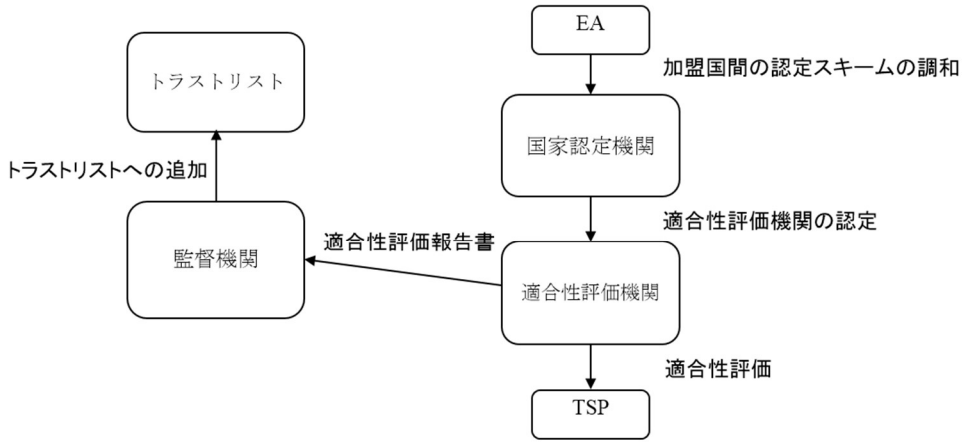

図 6.3　eIDAS 規則のトラストモデル

以下の図 6.4 は、ETSI 認証のトラストモデルであるが、上記図 6 のトラストモデルと酷似していることが分かる。ETSI 認証の場合、監督機関は存在せず、国家認定機関から認定を受ける認証機関が直接適合性評価と、認証の可否を判断することができる。また、必須ではないが、この適合性評価レポートを以て各ブラウザの信頼できるルート証明書プログラムへの登録を申請することができ、各ブラウザベンダーに認められた場合、信頼できるルート証明書の一つとして登録され、発行されるウェブサイト認証の電子証明書がブラウザで自動検証可能となる。このトラストモデルでは、各ブラウザの信頼できるルート証明書のリストが信頼の起点、つまりトラストアンカーであるといえる。

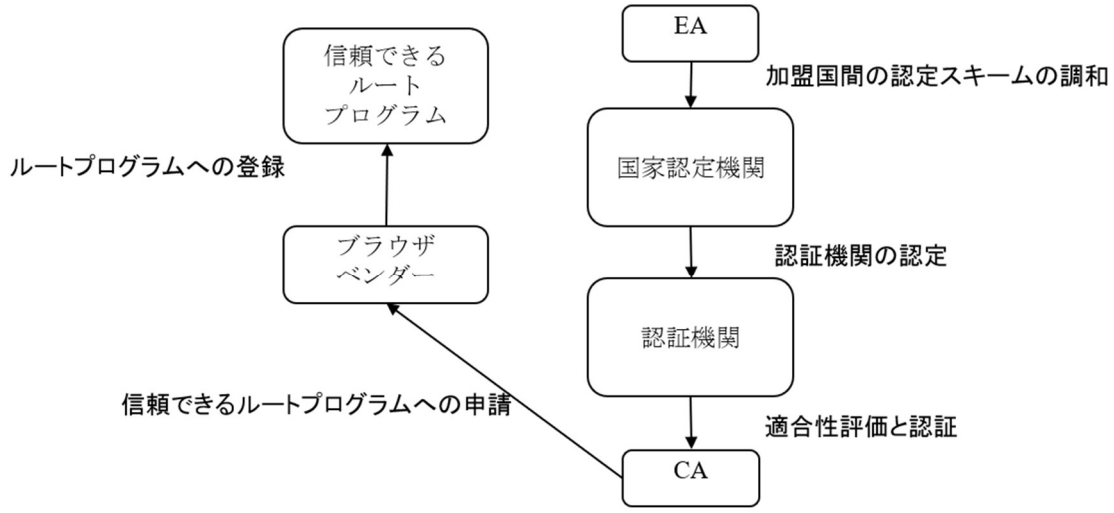

図 6.4　ETSI 認証のトラストモデル

6.3　WebTrust for CA のトラストフレームワーク

WebTrust for CA のトラストモデルは ETSI 認証のトラストモデルに非常に近い。ただし、WebTrust for CA は American Institute for Certified Public Accountant(AICPA)及び Canadian Institute of Chartered Accountants(CICA)が提供しているスキームであり、ETSI 認証のように多数の認定機関を想定しておらず、認定機関の認定プロセスの調和を行う必要がないため、調和機関が存在しない。ETSI 認証と同様に、AICPA 及び CICA から認められた公認会計士の監査結果を以て、各ブラウザのルートプログラムへ登録申請を行うことができる。

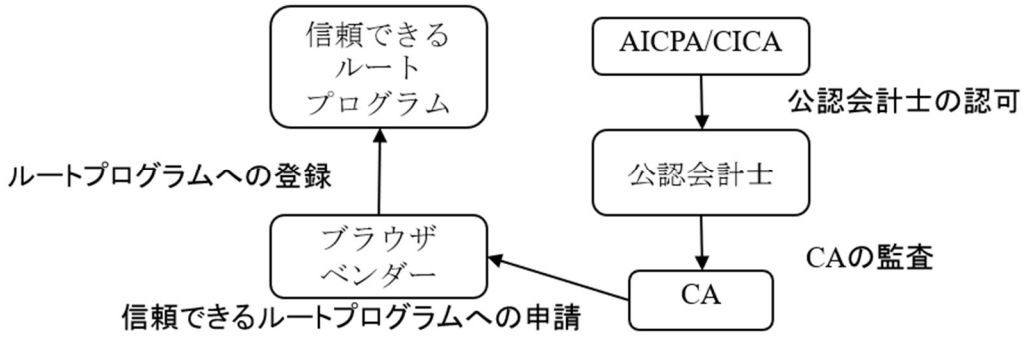

図 6.5 WebTrust for CA のトラストモデル 1

6.4　認定認証業務のトラストフレームワーク

次に日本の電子署名及び認証業務に関する法律におけるトラストフレームワークだが、先ず日本国内でのみ有効なモデルであるため、調和機関は存在しない。主務大臣が指定する指定調査機関が認証局を調査し、その調査結果に基づいて主務大臣が認定の可否を認証局に通知するモデルとなっている。eIDAS 規則におけるトラストリスト、ETSI 認証及び WebTrust for CA におけるルートプログラムの様な自動で有効性検証を行う仕組みをスキームとして持っておらず、認定を受けた事業者のリストが主務三省のウェブページで公開されているだけにとどまっている。

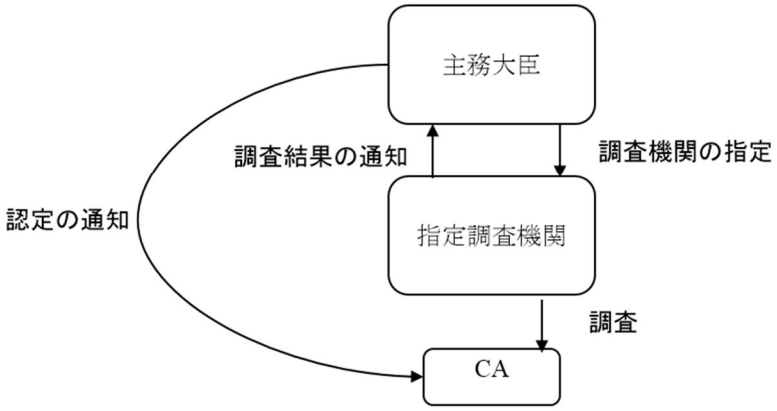

図 6.6 日本の電子署名法におけるトラストモデル

6.5　各トラストフレームワークの比較

以下の表 6.1 に、各トラストフレームワークを比較整理した。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、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。

表 6.1 各トラストフレームワークの比較

	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

7. 相互承認に向けた提案

1章から4章では、日米欧における公開鍵基盤に基づくトラストサービスについて、法的観点、技術的観点、またトラストフレームワークの観点から比較整理を行ったが、5章では、より効率的な監査及び認証と各フレームワークの相互承認に向けた提案を行う。

7.1 フレームワークの整理

相互承認に向けた議論の活性化には、各トラストフレームワークで使用されている用語を整理し、共通の用語を定め、また各フレームワークの共通部分であるコアの要件と、条件によって必要となるオプションの要件を整理することが必要である。

7.2 用語の整理

本研究ではトラストフレームワークの用語として以下を用いる。

トラストモデル： 複数の組織の相互作用によって人、物、組織、サービスに信頼を提供するモデル

トラストアンカー： トラストモデルにおいて信頼の起点となるもの

トラストフレームワーク： トラストモデル及びトラストモデルをサポートする法律、技術規格の枠組み

トラストサービス：電子署名やウェブサイト認証等、電子取引における信頼性を高めるサービス

トラストサービスプロバイダ： トラストサービスを提供する事業者

依拠当事者： トラストサービスの信頼性を依拠する者

監督機関： トラストモデルが法的効力を与える際に必要となる政府機関、トラストフレームワークの監督を行う

調和機関： トラストモデルが国境を越えて信頼を提供する際に必要となる、各国認定機関の認定プロセスの調和を図る機関

認定機関：　適合性調査を行う認証機関の資格認定を行う機関

認証機関：　技術基準、法的要件に従って適合性調査を行う機関
適合性検証サービス：　トラストリスト及びルートプログラム等のトラストサービスのそのトラストモデルへの適合性を検証できるサービス

適合性検証サービス提供者：　適合性検証サービスを提供する事業者

7.3　トラストモデルの整理と提案

5 .2 項の用語及び、4 章でトラストモデルを比較した結果得られた、各モデル共通のコア部分及び、条件によってオプションとなる部分を整理したトラストモデルが以下の図 7.1 である。実線で記述されている部分がコア部分で、点線で記述されている部分がオプションとなる部分である。

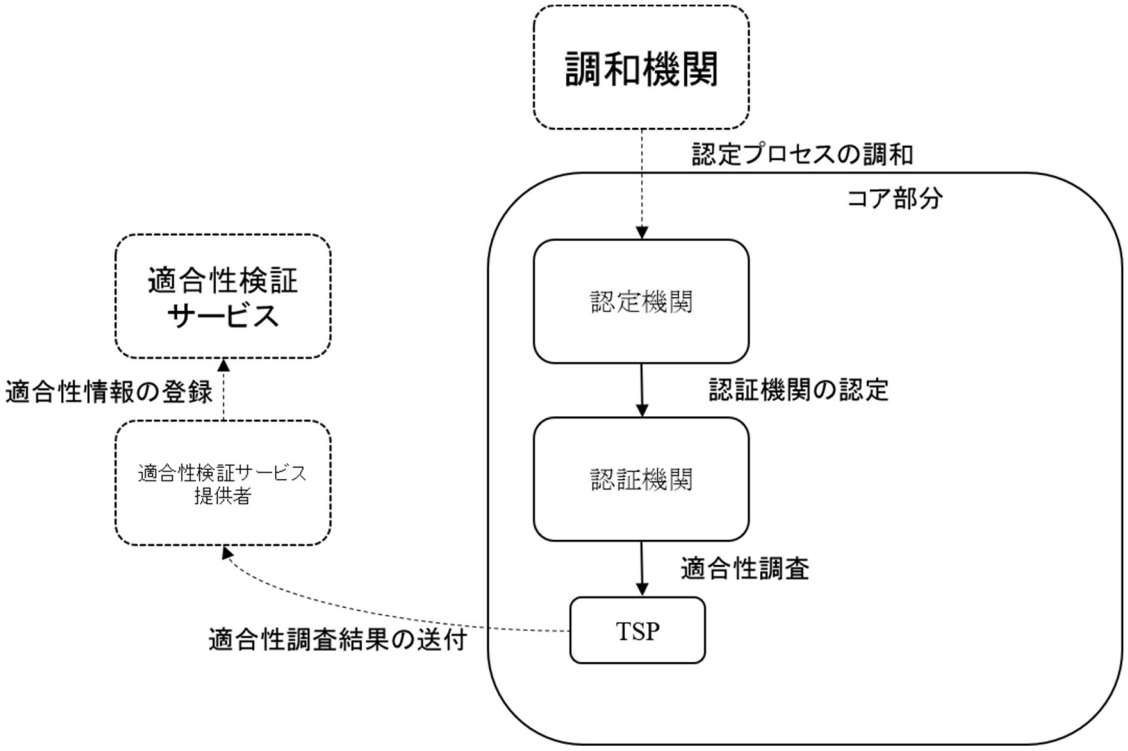

図 7.1 相互承認可能なトラストモデル案

今回比較したトラストモデルの中で最も単純なモデルは日本の電子署名法の認定機関（主務大臣)、認証機関（適合性調査機関)、TSP（認証事業者）の 3 階層のモデルである。これは同時に、他のトラストモデルと比較しても共通の階層構造の部分でもあった。このコ

ア部分に対して、他のトラストモデルとの相互承認を実現するために必要となるオプションの部分が点線部である。

まず調和機関であるが、これは実際に適合性調査を行う認証機関に対してその資格を認定する認定機関のプロセスについて、トラストモデル間で合意が必要であることから必要性が生じる。IAF の場合、調和機関は相互承認に加わるモデルの認定機関によって構成され、それぞれが互いを監督する仕組みとなっている。また、トラストモデル間で脆弱性情報の共有や使用できる暗号アルゴリズムの監視に関する情報の共有が必要となる。

次にお互いのトラストモデルにおける適合性が認められるトラストサービスを検証できる仕組みが必要であり、その仕組みが適合性検証サービス提供者及び適合性検証サービスである。今回のモデル案を用いた欧州 eIDAS 規則におけるトラストモデルとの相互承認のモデルを以下の図 7.2 に示す。

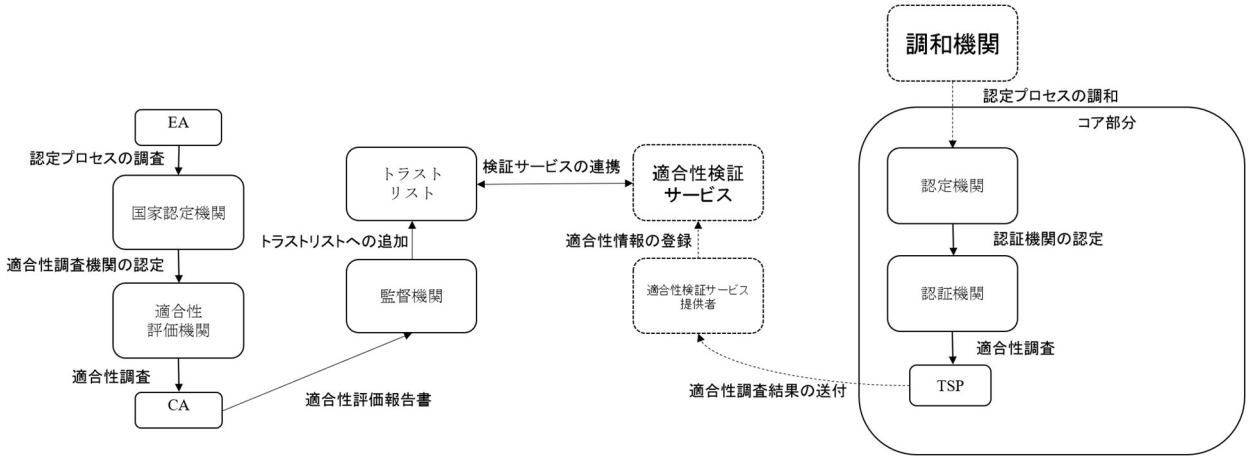

図 7.2　トラストモデル案と eIDAS 規則におけるトラストモデルの相互承認

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。図 10 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。

7.4 トラストモデルの評価

本研究では、いわゆるトラストリスト型の連携方式を提案したが、相互承認の実現のためには、他に以下の方式が考えられる。

① 相手側のトラストフレームワークの中に入る方式

これは例えば、欧州との連携において EU のリストオブトラストリストの中に日本のトラストリストを入れてもらう方式である。対等な意味での相互承認とは言えないかもしれないが、トラストサービスに関する法的効力は日本―欧州間で同等とすることができるであろう。

② ブリッジ認証局型の連携方式

米国の連邦 PKI はブリッジ型の連携方式をとっているが、日本でもブリッジ認証局を設立し、日本で認められたトラストサービスプロバイダと相互認証する形で接続し、このブリッジ認証局が相手側のトラストフレームワークの窓口になる方式である。

③ トラストサービスプロバイダ毎に相手側のトラストフレームに入る方式

この方式では、国家間の相互承認を目指すのではなく、トラストサービスプロバイダの企業努力によって両トラストフレーワークにおける法的効力の承認を得る案である。

それぞれのモデルをコストとフレームワーク内におけるトラストへの影響、他のトラストフレームワークとの接続性、実現期間という観点で以下の表 7.1 に比較する。

表 7.1　各相互承認実現案の比較

方式	コスト	フレームワーク内におけるトラストへの影響	接続性	実現期間
①EU トラストリストのフレームワークに入る方式	トラストリストの運用コスト	欧州のトラストリストの影響を受ける国内の法体系を捨てる必要がある	日本－欧州間のみ 欧州と他のフレームワーク間の相互承認次第	1 年～2 年
②ブリッジ認証局型の連携方式	ブリッジ認証局の設立コスト	なし	ブリッジ型－トラストリスト型の連携課題	2 年～3 年
③TSP 事に相手側のトラストフレームワークに入る方式	TSP 毎に複数の法律／技術規格に適合するコスト	なし	相互承認ではなく、他のトラストフレームワークへの接続性もない	1 年
④日本版トラストリスト方式	トラストリストの運用コスト	なし	ブリッジ型との連携課題	2 年～3 年

相互承認の実現にかかるコストの面で比較すると最も低コストであるのが、①と④である。トラストリストはすでに技術標準が ETSI によって定められており、開発コストを抑えることができる。一方②のブリッジ方式では、新たにブリッジ認証局を設計、設立する必要があり、①、④案と比較すると高コストとなる。③の TSP 毎に現地の法律／技術要件に適合していく方式では、結局のところ 2 つ以上のトラストフレームワーク内でそれぞれのトラストサービスプロバイダが認定を受けていく必要があり、サービスコストが割高になり、長期的に最も高コストな方式となる。

次にフレームワーク内のトラストに与える影響の観点では、②、③及び④の方式では、現状の日本のフレームワークへの悪影響は考えられない。仮に相互承認先のフレームワーク内で重大なインシデントが発生した場合においても、相互承認を切断すれば、国内のトラストフレームへの被害は最小限に抑えることができる。一方で①の方式では、EU 各国のトラストリストをまとめているリストオブトラストリストに日本のトラストリストを入れてもらう方式であり、相互承認を一方的に切断される可能性がある。また、欧州の法体系、技術方式をそのまま受け入れる方式であり、国内の電子署名法等の体系に影響が出ることが想定される。

次に他のフレームワークとの接続性に関する観点では、②と④の方式が最も優れているといえる。②はブリッジ型のモデルであり、すでに米国の連邦 PKI で採用されており、米

国との連携が最も容易なモデルである。一方でブリッジ型のモデルとトラストリスト型のモデルの相互連携には、現状課題が残る。④はトラストリスト型のモデルの採用であり、欧州で採用されているモデルであるため、欧州との連携が容易である。ブリッジ型のモデルとの連携には②と同じく課題がある。①は欧州のフレームワーク内に入るため、他のフレームワークとの相互承認については、欧州と他のフレームワーク間の検討結果に依存するものとなり、日本のトラストフレームワークとしての独立性がない。③はそもそも相互承認の枠組みではないため、接続性はない。

実現期間については、4 案とも相互承認の実現という目標に対してそれほど大きな問題となるとは考えられない。この評価結果を 3 段階評価でまとめると以下の表 7.2 の通りとなり、総合的には、本研究で提案しているトラストリスト型のモデルの採用が最も優れているといえる。

表 7.2 評価結果

方式	コスト	フレームワーク内におけるトラストへの影響	接続性	実現期間
①EU トラストリストのフレームワークに入る方式	○	×	×	△
②ブリッジ認証局型の連携方式	△	○	△	△
③TSP 事に相手側のトラストフレームワークに入る方式	×	○	×	○
④日本版トラストリスト方式	○	○	△	△

7.5 リモート署名

日米欧の電子署名の法的要件の中で、ハードウェアトークンの扱いに差があることは 2 章で明らかになった。欧州では、セキュリティ評価を受けたハードウェアトークンに秘密鍵を格納し、署名生成することが法律で求められているが、日米では、法律上明確なハードウェアトークン利用の要件はなく、現状でも、秘密鍵を PC 上で管理している例も多い。この差異を解消する手段となりえるのがリモート署名である。リモート署名とは、署名者の秘密鍵をサーバ側の暗号モジュールで管理する方式であり、署名者は、リモート署名サーバに対してユーザ認証を行い、その結果サーバ側で署名者の鍵を活性化し、署名生成を行う。eIDAS

規則ではリモート署名であっても一定の要件を満たせば、適格電子署名として認められることが規定されている。日本や米国でも欧州と同等の方式でのリモート署名の要件が整備されれば、より安全で簡便かつ、ハードウェアトークン利用の問題を解消し、欧州と技術的に比較可能な電子署名が可能になる。

リモート署名を実現するために課題となるのが、リモート署名が果たして日本の電子署名法 3 条に記載されている「本人による署名」として認めることができるかという点にある。欧州ではセキュリティ管理により、秘密鍵が署名者の単独の管理にあることが保証されればリモートで適格電子署名を行うことができるとしている。この実現のためには、署名者の認証プロセスと署名鍵の活性化プロセスが非常に重要となる。従って、日本及び米国においてリモート署名の技術要件が欧州の要件と同等のレベルで整備されれば、少なくともリモート署名に関しては、相互承認の可能性が高いと考えられる。

7.6 部分認証

3.5.2 項でウェブサイト認証の技術要件を比較したが、現状欧州の認証局は eIDAS 規則に適合する必要があり、また、米国の認証局は WebTrust for CA を取得しているが、グローバルに活動している認証局は WebTrust for CA と eIDAS 規則の両方に適合するための監査を受けている。認証局は監査費用のみならず、監査の準備、対応には大きなコストを割いているが、本研究ではより効率的な監査の手法として部分認証を提案する。

例えば、図 7.3 のように、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る。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。

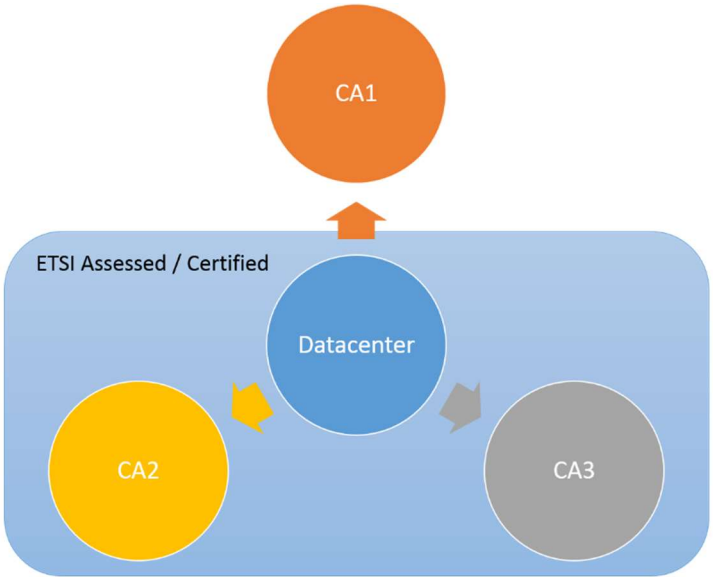

図 7.3 同一のデータセンターを複数の認証局が利用している例

部分認証の結果を流用する際に考慮しなければならない点として、認証結果の有効期限の問題がある。以下の図 7.4 は、認証結果の有効期限の問題を示す。

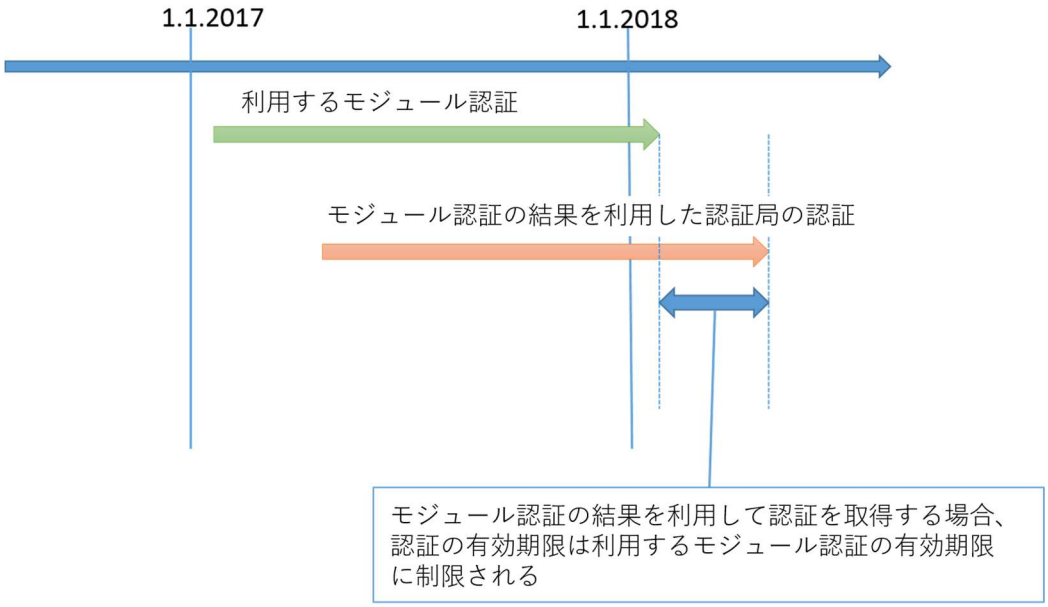

図 7.4 認証結果の有効期限

主要なブラウザベンダーは、信頼できるルートプログラムで、ETSI 規格あるいは WebTrust for CA の監査を 12 か月毎に受けることを要求している為、監査結果の有効期限は信頼できるルートプログラムでの利用では 12 か月であるといえる。この場合、例えば図 12 が示すように、部分認証が 2017 年の 1 月 1 日に発行されており、この認証結果を利用した認証が多とベア 2017 年の 3 月に発行されたとしても、その認証結果の有効期限は部分認証の有効期限である 2018 年 1 月に制限される。

また、データセンターが共有されていたとしても、例えば使用する暗号モジュールや、サーバラックの配線等の認証局固有の実装については確認が必要である。しかしながら、アクセスコントロールや電源供給、空調設備や災害復旧等の多くの点において、適合性評価の工数削減が期待できる。

8 結論

本研究では、電子取引における信頼性を高める電子署名やウェブサイト認証といったトラストサービスについて、市民活動、経済活動がグローバル化された現代では国境を越えて利用できる環境を目指す必要があるという課題に対して、日米欧のトラストサービスに関する法的要件、技術的要件、またトラストモデルを比較整理し、共通点と差異を分析した。

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。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。

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、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。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。

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。これは認証局の実態として、データセンター等の同一のファシリティを共有している例が多く、これらの同一ファシリティに対する監査の重複を回避するものである。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。

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。

今後の研究課題として、本研究での提案に対する定量的な評価分析に取り組みたい。

謝辞

本論文を執筆するにあたって、指導教官である木下俊之教授から、感謝しきれないほど熱心なご指導を賜りました。心から感謝いたします。また、日頃からサポート頂いた木下研究所の皆様にもこの場を借りてお礼を申し上げます。皆様に感謝いたします。

参考文献

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[2] 電子署名及び認証業務に関する法律、平成 12 年 5 月 31 日法律第 102 号

[3] European Telecommunication Standards Institute, ETSI TS 119 612 V2.1.1, Electronic Signature and Infrastructure (ESI); Trusted Lists, July 2015.

[4] COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 Sepctember 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[5] Europen Telecommunication Standards Institute, ETSI EN 319 142-1 V1.1.1, Electronic Signature and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures, April 2016

[6] Europen Telecommunication Standards Institute, ETSI EN 319 132-1 V1.1.1, Electronic Signature and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures, April 2016

[7] Public Law 106-229, 106th Congress, ElECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT

[8] National Commerce of Commissioners on Uniform State Laws, Uniform Electronic Transactions Act, July 1999

[9] The State of Illinoi, The Electronic Commerce Security Act, 5 ICL/1 et seq, July 1998

[10] The State of Washington, Washington Electronic Authentication Act, 1997

[11] European Telecommunication Standards Institute, ETSI EN 319 401 V2.1.1, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, February 2016

[12] European Telecommunication Standards Institute, ETSI EN 319 411-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for

Trust Service Providers issuing certificates; Part 1: General requirements , February 2016

[13]European Telecommunication Standards Institute, ETSI EN 319 411-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, February 2016

[14]Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, V1.0, CA/Browser Forum, November 2011

[15]Guidelines For The Issuance And Management Of Extended Validation Certificates, V1.4, CA/Browser Forum, effective on 29 May 2012

[16]Network And Certificate System Security Requirements, V1.0, CA/Browser Forum, effective on 1/1/2013

[17]CPA Canada, Trust Service Principles and Criteria for Certification Authorities Version 2.0, March 2011

[18]CPA Canada, WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5, April 2014

[19]CPA Canada, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.1, November 2016

[20]Thijs R. Timmerman, Certification Authority Criteria in User Perspective, August 2014

[21]電子署名及び認証業務に関する法律施行規則、平成 13 年総務省・法務省・経済産業省令第 2 号

[22]電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針、平成 13 年 4 月 1 日総務省・法務省・経済産業省

[23]電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針、平成 15 年 6 月 2 日総務省・法務省・経済産業省

[24]特定認証業務の認定に係る調査表の説明と記入例、2004 年 4 月 9 日、一般財団法人情報経済社会推進機構 電子署名・認証センター

[25]FIPS 140-2, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, Information Technology Laboratory National Institute of Standards and Technology, May 25th, 2001

[26]Arrangement on the Recognition of Common Criteria Certificate in the field of Information Technology Security, July 2nd, 2014

[27]Soshi Hamaguchi, Toshiyuki Kinoshita, Ph.D, and Satoru Tezuka, Ph.D " Examination of the Possibilities of Reusing Certification Results between Different Assessment Schemes for Certification Authorities", The 2016 World Congress in Computer Science, Computer Engineering, & Applied Computing, July 25-28, 2016

[28]Soshi Hamaguchi, Toshiyuki Kinoshita and Satoru Tezuka "An Analysis of Trust Models of Public Key Infrastructure", International Journal of Control Theory and Applications Volume 9, Number 43 P395-402, 2016

[29]Soshi Hamaguchi, Toshiyuki Kinoshita, Ph.D, Satoru Tezuka, Ph.D "Comparison of electronic signature between Europe and Japan", The World Congress on Internet Security 2017, December 11-14, 2017

[30]Standards and Industry Regulations Applicable to Certification Authorities, Kirk Hall, Trend Micro, Inc

[31]Federal PKI Management Authority, Federal PKI Trust Infrastructure Overview, V1.0 September 2015

[32]Federal Public Key Infrastructure Policy Authority, Federal Public Key Infrastructure (FPKI) Concept of Operation (ConOps), Version 1.0.0, January 2012

[33]Marc Sel, “A Comparison of Trust Models”, ISSE 2015 pp 206-215.

[34]EN 419 211-1, Protection Profile for secure signature creation device – Part1: Overview, CEN/TC 224/WG 17, October 8th, 2014

[35]European Telecomunication Standardization Institute, ETSI TS 119 312 V1.1.1, Electronic Signatures and Infrastructures (ESI); Cyptographic Suites, November 2014

[36]ITU-T Recommendation X.509 Information technology – Open Systems Interconnection – The Directory: Public-Key and attribute certificate framework, October 2016

[37]Networking Working Group, RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

[38]Internet Engineering Task Force (IETF), RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013

[39]European Telecommunication Standardization Institute, ETSI EN 319 403 V2.2.2, Electronic Signature and Infrastructure (ESI); Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers, August 2015

[40]European Telecommunciation Standardization Institute, ETSI EN 319 412-5 V2.0.12, Electronic Signature and Infrastructure (ESI); Certificate Profiles; Part5: QCSStatements, June 2015

業績リスト

A. ジャーナル論文

1．Soshi Hamaguchi1, Toshiyuki Kinoshita, and Satoru Tezuka, “An Analysis of Trust Models of Public Key Infrastructure,” International Journal of Control Theory and Applications, Vol. 9, No. 43, pp. 395—402, 2016

2．Soshi Hamaguchi1, Toshiyuki Kinoshita, and Satoru Tezuka, “Comparison of electronic signature between Europe and Japan,” International Journal for Information Security Research (IJISR), Volume 8, Issue 1, 2018

B. 国際学会講演

1．Soshi Hamaguchi1, Toshiyuki Kinoshita, and Satoru Tezuka, “Examination of Possibility on Reuse of Certification Result between Different Assessment Scheme for Certification Authority,” Proceedings of the 2016 International Conference on Security and Management (SAM’16), pp. 362-366, July 2016

2．Soshi Hamaguchi1, Toshiyuki Kinoshita, and Satoru Tezuka, “An Analysis of Trust Models of Public Key Infrastructure,” Proceedings of 5th International Conference on Computing, Engineering and Communication Technologies (ICCECT 2017), March 2017

3．Soshi Hamaguchi1, Toshiyuki Kinoshita, and Satoru Tezuka, “Comparison of electronic signature between Europe and Japan,” Proceedings of World Congress on Internet Security 2017 (WorldCIS 2017), Dec.2017

付　録

以下、論文本中で比較した各技術規格の要件をまとめた表である。

表 1 EN 319 401 の要求

要求範囲	要求項目	要求内容
リスクアセスメント	－	● トラストサービスを提供する上でのリスクの識別、分析及び評価 ● 適切なリスク対策の選択と残存リスクの承認 ● リスクアセスメントの定期的な見直し
ポリシー及び運用	トラストサービス運用規定	● トラストサービス運用規定の作成と公開
	条件	● 加入者及び依拠当事者に対する条件の通知
	情報セキュリティポリシー	● 情報セキュリティポリシーの作成／維持／実施
TSP の管理及び運営	組織の信頼性	● 非差別的であること ● 公開されている条件に合う申請者すべてがサービスにアクセスできること ● 十分な資産と保険への加入 ● 財務上の安定 ● クレームや紛争に対するポリシーと手順を持つこと ● 外部委託時の正当な契約関係
	職務の分離	職務と責任範囲の分離
	人的資源	● 要員採用時の専門性／信頼性／経験／資質管理 ● 専門知識／経験及び能力の充足 ● 違反時の懲戒処分 ● セキュリティに関する役割と責任の文書化と信頼できる役割の区別 ● 職務規定書（責任分散、アクセスレベ

		ル、バックグラウンドチェック等） ● 情報セキュリティ管理手順に従った手続き ● 管理職の知識と経験 ● 公平性の維持 ● 信頼できる役割の責任に関する規定 ● 信頼できる役割の任命及び最小特権の原則 ● 必要な確認の完了前のアクセスの禁止
	資産管理	● 資産表とリスク評価に沿った管理 ● メディアの安全な取り扱いと廃棄
	アクセスコントロール	● 不正アクセスからの保護とファイアウォールの設定 ● オペレータ／管理者／監視アカウントとアクセスの管理 ● アクセスコントロールポリシーに従った規制 ● 各アカウントの識別と認証 ● 要員の活動に関する説明責任（イベントログの保管） ● 削除済みファイル等を介した漏洩対策
	暗号管理	● 暗号鍵、暗号装置のライフサイクルを通した適切なセキュリティ制御
	物理及び環境セキュリティ	● 物理アクセスの制限 ● 情報及び設備の危殆化と盗難に対する管理策 ● 資産の損失、損害に対する管理策 ● 重要コンポーネントの物理保護（アラーム、アクセス制御等）
	運用セキュリティ	● セキュリティバイデザイン ● システムの構成管理と変更管理手順 ● システムの完全性保護 ● メディアの安全な取り扱い ● 記録保管の期間とメディアの陳腐化防止 ● 重要な役割に関する手順の確立と実施

		● セキュリティパッチ適用手順の規定／運用
	ネットワークセキュリティ	● セキュリティのゾーニング ● セキュリティゾーン間のアクセス制限と定期的な見直し ● 重要システムの安全なゾーンでの保持 ● ネットワーク分離（テスト環境、システム管理ネットワーク、運用ネットワーク） ● 信頼できる通信チャンネルによるシステム間通信 ● 必要に応じた外部ネットワーク接続の冗長化 ● IP アドレスの定期的な脆弱性スキャン ● 定期的な侵入テストの実施
	インシデント管理	● 情報の機微性を考慮した監視 ● セキュリティ侵害の可能性の検出及びアラーム ● ログ機能の起動／停止、ネットワーク及びサービスの可用性の監視 ● 迅速なイベント管理とインシデント対応手順 ● 個人情報に影響を与えるインシデントの対応 ● トラストサービス利用者へのインシデント通知 ● 監査ログの定期的なレビューとアラームの自動化 ● 重大な脆弱性への対応 ● 損害を最小限に抑えるインシデント報告と対応手順
	証拠の収集	● 記録の気密性及び完全性の維持 ● 公開されている規定に従った記録の管理 ● 法的手続きのための記録の提供 ● 重要イベントの正確な時間の記録

		● 記録の保管期間 ● イベントログの削除防止
	事業継続マネジメント	● 事業継続計画の規定と維持
	TSP の終了及び終了計画	● 終了計画の保持 ● 業務終了手順 ● 破産時の協定 ● 業務終了時の規定の公開 ● 公開鍵あるいはトラストサービストークンの可用性
	コンプライアンス	● 法律の充足 ● アクセスフリー ● 個人情報の取り扱い

表 2 EN 319 411-1 の要件

要求範囲	要求項目	要求内容
認証業務運用規定及び証明書ポリシーに関する一般規定	認証業務運用規定の要求事項	● IETF RFC 3647 に従った構成 ● CA の階層構造の説明 ● 署名アルゴリズムとパラメータ ● CPS のオンライン公開 ● 証明書、CRL 及び OCSP に署名する鍵に関する規定
トラストサービスプロバイダの運用	公開及び保管の責任	● 証明書の正確な発行と安全な配布 ● 証明書の公開に関する主体者の同意 ● 証明書使用に関する条件の依拠当事者への公開 ● 条件の容易な識別 ● 証明書と使用に関する条件の常時公開（24 時間×7 日） ● 英語での公開
	識別及び認証	● 初回本人確認 ➢ 適切で認可された本人確認資料の使用 ➢ 対面あるいは同等手段での本人確認 ➢ 本人情報の証拠確認 ✧ フルネーム ✧ 生年月日、出生地、ID の参照、その他属性 ➢ 法人と関連する場合の要件 ➢ 本人確認資料の記録 ➢ 主体者以外が加入者である場合の要件 ➢ 加入者との連絡方法の確認 ➢ 登録手続きにおけるデータ保護法令の遵守に関する証拠提供 ➢ 証明書の使用目的に沿った必要最低限の本人確認 ➢ 利益相反の防止 ● リキーリクエストの識別及び認証

		➢ 証明書と本人確認情報の有効性確認 ➢ 条件の変更の通知 ➢ 初回本人確認時の要求事項の適用 ● 失効要求の識別と認証 ➢ 失効手続きの文書化 ✧ 失効リクエストの要求者 ✧ 失効要求方法 ✧ 失効の必要性確認 ✧ 失効あるいは一時停止の理由 ✧ 失効ステータス情報の配布 ✧ 受付から失効／停止判断までの時間 ✧ 失効／停止判断から失効ステータス情報への反映までの時間 ✧ 失効サービスに利用される時間の同期 ➢ 失効リクエストと失効に関連するイベント報告の受領時の処理 ➢ 失効リクエストの真偽確認
	証明書のライフサイクル	● 証明書申請 ➢ 主体者の鍵ペアを認証局で生成しない場合、秘密鍵が主体者の管理下にあることを確認すること ● 証明書申請プロセス ➢ 外部登録局を利用する場合のセキュア通信 ● 証明書発行 ➢ 証明書プロファイル ➢ 主体者鍵生成プロセスにおける機密性の保護（証明書の偽造対策） ➢ 証明書の発行手順と登録手続き、証明書リキー等との安全なリンク ✧ 鍵ペア生成と証明書のリンク ✧ 秘密鍵の主体者への安全な送

		付 ✧ 署名生成装置の安全な送付 ➢ 証明書に記載される識別名の一意性 ➢ 法人の属性を含む場合、証明書の識別子は法人を代表する自然人であること ➢ ポリシー識別子の利用 ● 証明書の受領 ➢ 証明書の使用条件の契約前の通知 ➢ 主体者への責任関する通知 ➢ 通知方法 ➢ 加入者との契約書の保管 ➢ 加入者と主体者が異なる場合の個別の契約書 ● 鍵ペア及び証明書の使用 ➢ 主体者及び加入者の義務 ✧ 正確な情報の提出 ✧ 鍵ペアの使用制限の遵守 ✧ 秘密鍵の不正使用防止 ✧ 鍵生成を主体者が実施する場合の安全性 ✧ 鍵生成を主体者が実施する場合の単独管理の維持 ✧ 秘密鍵の署名生成装置内での使用 ✧ 秘密鍵の署名生成装置内での生成 ✧ 秘密鍵の危殆化及び証明書の内容に変更がある場合の即時通知 ✧ 危殆化時の鍵使用の中止 ✧ 証明書失効あるいは認証局危殆化の連絡を受けた場合の鍵使用の中止 ➢ 依拠当事者への通知

		✧ 現在の失効情報を利用した検証 ✧ 証明書使用に係る制限の考慮 ✧ 契約等で規定される事項への注意 ● 証明書更新 ➢ 更新する証明書の有効性と本人確認情報の有効性検証 ➢ TSP の条件に変更があった場合の通知 ➢ 初回本人確認時の要求事項の適用 ➢ 前回認証された公開鍵を用いた証明書発行 ● 証明書の変更 ➢ 認証された本人確認情報に変更がある或いは署名書が失効している場合、初回本人確認時の要件に従って登録情報を検証／記録する ● 証明書失効及び停止 ➢ 証明書ステータスに変更があった場合の主体者／加入者への通知 ➢ 完全に失効された証明書の復旧防止 ➢ CRL の 24 時間毎の公開 ✧ 予定されている CRL 発行時刻の提示 ✧ CRL の署名 ➢ CARL の 1 年毎の更新 ➢ 相互認証がある場合、CARL の 31 日毎の更新 ● 証明書ステータスサービス ➢ 失効ステータスの可用性（24 時間 365 日） ➢ 失効ステータス情報の完全性及び真正性 ➢ 証明書の有効期限切れまで、ステ

		ータス情報を提供すること ➢ OCSP のサポート ➢ CRL のサポート ➢ OCSP と CRL 間の情報の同一性 ➢ 失効情報の公開 ● 鍵供託と鍵回復 ➢ 複製される鍵のセキュリティ ➢ 必要性最低限の複製 ➢ 秘密鍵に対する主体者の単独管理の保証 ➢ 秘密鍵のその他目的による使用の制限 ➢ 秘密鍵の機密性維持
	施設と管理、運用管理	● 物理的セキュリティ管理 ➢ 証明書生成及び失効管理関連施設の物理的保護環境 ➢ 物理的安全エリアの入退室管理 ➢ 物理的境界線と物理的安全エリアの共有の制限 ➢ システムリソース、設備リソースの保護 ➢ 機器、メディア、情報等の持ち出し制限 ➢ 同一安全エリアにおける TSP 運用のその他機能のサポート ➢ ルート認証局の秘密鍵の隔離 ● 手順管理 ➢ ルート認証局による証明書発行の二重管理 ● 監査ログ ➢ 全てのセキュリティイベントのログ ➢ 登録業務に係る情報の記録 ➢ プライバシーの維持 ➢ CA 鍵ライフサイクル関連イベントのログ

		➢ 証明書ライフサイクル関連イベントのログ ➢ その他 CA が管理する鍵のライフサイクル関連イベントのログ ➢ 失効関連イベントのログ ● 記録のアーカイブ ➢ 証明書の有効期限後少なくとも 7 年間の記録保持 ● 危殆化及び災害復旧 ➢ システムのバックアップ ➢ バックアップ及び復旧プロセスの信頼された要員による実施 ➢ 復旧における二重管理の必要性 ➢ CA 鍵の危殆化を事業継続計画に含めること ➢ 現実的再発防止対策 ➢ CA 鍵危殆化の場合の手続き ✧ 全ての関係者への通知 ✧ CA 鍵を使用した証明書､失効ステータス情報が有効でない旨の表示 ✧ 他の CA の危殆化の場合、危殆化した TSP に対して発行した証明書の失効 ➢ 暗号アルゴリズム或いは関連パラメータの危殆化の場合の手続き ✧ 全ての関係者への通知 ✧ 影響を受ける証明書の失効計画 ● 認証局又は登録局の業務停止 ➢ 登録情報､失効ステータス情報､イベントログの依拠当事者への移譲 ➢ 失効ステータスの引継ぎ ➢ 相互認証した TSP が失効管理を含めた業務を停止した場合の相互認証証明書の失効

	技術的セキュリティ管理策	● 鍵ペア生成とインストール ➢ CA 鍵ペアの生成及び公開鍵の認証は二重管理の下、物理的に安全な環境で行うこと。この職務を負う要因は必要最低限であること。 ➢ CA 鍵ペアの生成は ETSI TS 119 312[35]で規定されているアルゴリズムに従うこと ➢ 主体者の鍵の署名に使用する CA 鍵証明書の有効期限が切れる前に新しい CA 鍵証明書を生成すること ➢ CA 鍵の円滑な切り替え ➢ CA 鍵ペア生成手順の文書化 ✧ キーセレモニー関連の役割と職務 ✧ セレモニーの証拠の要件 ➢ キーセレモニーレポートの作成と署名 ✧ ルート鍵の生成には第三者の立ち合いと署名が必要 ➢ CA 公開鍵の完全性を保証と CA 署名検証鍵の公開 ➢ 主体者の鍵生成への適切なアルゴリズムの使用 ➢ 主体者鍵の安全な生成と保管 ➢ 主体者の秘密鍵の安全な送付 ➢ 主体者秘密鍵の全てのコピーの削除 ➢ 署名生成装置の安全な交付 ● 秘密鍵の保護及び暗号モジュールの技術管理 ➢ CA 鍵ペアの生成は HSM 内で行う ➢ CA の秘密鍵は HSM 内で保持する

		➢ HSM 外で保管する場合、HSM 内と同等の保護レベルで保管すること ➢ CA 秘密鍵のバックアップ、保管、復号は安全な環境で二重管理の下行われる ➢ CA 秘密鍵のコピーは、使用されている鍵と同等のセキュリティレベルで管理されること ➢ CA 秘密鍵及びコピーが専用の HSM 内で保管されている場合、鍵が暗号装置外で使用されないこと ➢ HSM は輸送中に改ざんされないこと ➢ HSM は保管中に改ざんされないこと ➢ HSM は正しく機能すること ➢ HSM 廃棄時の、装置内秘密鍵の破棄 ● 鍵ペア管理のその他の側面 ➢ CA 署名鍵の使用用途の制限 ➢ CA 証明鍵の物理的に安全な環境での使用 ➢ CA 秘密鍵の使用は証明書生成に使用される鍵長、署名アルゴリズム、ハッシュアルゴリズムと互換性があること ➢ CA 署名鍵のライフサイクル終了時の全てのコピーの廃棄 ➢ CA がセルフサインする場合、証明書の属性は ITU-T 勧告 X.509[36] の Key usage に適合すること ● アクティベーションデータ ➢ HSM での CA 鍵のインストール及び復旧は二重管理の下行われること

		➢ 主体者の署名生成装置の安全なディアクティベーション及びリアクティベーション ➢ 主体者の署名生成装置のアクティベーションデータは署名生成装置とは別の手段で主体者に送付されること ● コンピュータセキュリティ管理 ➢ ローカルネットワークコンポーネントは物理的及び論理的に安全な環境で保持され、定期的に設定が見直されること ➢ 証明書発行に直接かかわるすべてのアカウントは多要素認証を行う ➢ 配布アプリケーションは証明書の追加、変更などの試みに対してアクセスコントロールを実施すること ➢ 失効ステータスアプリケーションは、失効スタータス情報にアクセスコントロールを実施すること ➢ 不正な試みに対して継続的な監視とアラーム設備を備えること ● ライフサイクルセキュリティ管理 ➢ 容量需要を監視し、適切な処理能力、容量を保証する ● ネットワークセキュリティ ➢ 全ての CA システムを少なくともセキュアゾーンで保護し、セキュアゾーン及びハイセキュアゾーン間の通信を保護すること ➢ 使用していないすべてのアプリケーション、アカウント、サービス、プロトコル、ポートを削除／停止すること ➢ セキュアゾーン及びハイセキュア

		ゾーンのアクセスコントロール ➢ ルート CA システムはハイセキュアゾーンで維持すること
	証明書、CRL 及び OCSP のプロファイル	● 証明書プロファイル ➢ ETSI EN 319 412-2[13]に従う ● CRL ➢ ITU-T 勧告 X.509[36]又は IETF RFC 5280[37]に従う ● OCSP ➢ IETF RFC 6960[38]に従う
	適合性監査及びその他の評価	ETSI EN 319 403[39]参照
	その他の事業及び法的事項	● 個人情報 ➢ 登録データの機密性と完全性の保護 ● 表明及び保証 ➢ TSP の一部が業務委託されていても TSP が本ポリシーへの充足に対して責任を持つ ➢ CPS と一貫した認証サービスを提供する
	その他の規定	● 組織の規定 ➢ TSP の独立性 ➢ TSP の公平性 ● 追加試験 ➢ TSP が発行するすべての証明書を第三者がテストできること ➢ テスト用証明書はテスト用であることが明記されること

表 3　EN 319 411-2 の要求

要求範囲	要求項目	要求内容
トラストサービスプロバイダの運用	識別及び認証	● 初回本人確認 ➢ 自然人の物理的存在の確認 ➢ 物理的存在の確認と同等レベルの信頼性の確認手法
	証明書のライフサイクル	● 証明書の受領 ➢ 加入者が同意を電子的に示す場合、先進電子署名或いは先進 e シールを行うことが望ましい ● 鍵ペア及び証明書の使用 ➢ TSP が QSCD を管理する場合、秘密鍵は QSCD 内以外で署名のために使用しないこと ➢ TSP が QSCD を管理する場合、秘密鍵は主体者の単独管理の下使用されること ➢ TSP が QSCD を管理する場合、主体者の鍵ペアは電子署名のみに使用されることが望ましい ➢ 加入者の義務 ✧ 秘密鍵は主体者の単独管理の下維持する ✧ 鍵ペアは電子署名にのみ使用することが望ましい ● 証明書失効ステータスサービス ➢ 失効ステータスは証明書の有効期限が切れた後も利用可能であること ➢ 失効ステータスの可用性について TSP の終了も含む正確に文書化すること
	施設、管理及び運用管理	● 監査ログ ➢ QSCD の準備に係るすべてのイベントログ ➢ TSP は適格証明書の発行、生成、

		配布及び失効管理、QSCD の準備に係るイベントをログし、送受信データを記録すること ➢ TSP の終了後も法的要件を満たす目的で情報を管理すること ➢ 情報へのアクセス方法の文書化 ➢ TSP は運用規定で情報の保管期間を正確に文書化し、終了計画により移譲される情報を示すこと
	技術的セキュリティマネジメント	● 鍵ペア生成及びインストール ➢ QSCD が認証製品であることを検証すること ➢ QSCD が別の第三者の TSP により準備される場合、TSP はこの第三者の TSP が要求事項を満たしていることを検証すること ➢ 証明書要求プロセスは認証対象である公開鍵が QSCD によって生成された鍵ペアのものであることを確認すること ➢ 主体者の鍵ペアを TSP が生成し、QSCD にインポートする場合は、TSP が認証取得 QSCD の想定環境を満たすこと ➢ TSP は QSCD 証明書ステータスを証明書の有効期限が終わるまで監視し、ステータスに変更が生じる際は CPS に文書化された適切な措置をとる
	証明書、CRL、及び OCSP プロファイル	● 証明書プロファイル ➢ 証明書には ETSI EN 319-412-5[40]で規定される QC 宣言を含むこと ➢ 証明書には ETSI EN 319-412-5[30]で規定される QSCD 宣言を含むこと

		➢ 証明書にはポリシー識別子を含むこと ➢ TSP が割り当てた OID のみが含まれる場合、どの証明書ポリシーをベースとしているか明示すること
	その他の規定	● 条件 ➢ 証明書ポリシーには適格証明書のポリシーであること、QSCD の使用を要求することを明示すること ➢ PKI 開示規定がサポートされていること

表 4 WebTrust for CA の要件

要求範囲	要求項目	要求内容
CA 業務規程の開示	認証局運用規定	認証局は RFC3647、RFC2527 の要求事項について認証局運用規定で開示すること
	証明書ポリシー	認証局は RFC3647、RFC2527 の要求事項について証明書ポリシーで開示すること
CA 業務規程管理	証明書ポリシー管理	認証局は証明書ポリシーのマネジメントプロセスが効果的であること保証する管理策を維持する
	認証局運用規定の管理	認証局は認証局運用規定のマネジメントプロセスが効果的であること保証する管理策を維持する
	CP 及び CPS の一貫性	認証局は認証局運用規定が証明書ポリシーに含まれる内容に対応していることを保証する管理策を維持する
CA 環境の管理	セキュリティ管理	認証局は以下の保証する管理策を維持する ● セキュリティの計画と管理 ● セキュリティリスクの識別と管理 ● CA 設備、CA システム、第三者がアクセスする情報のセキュリティ維持 ● CA 機能が外部委託された場合の加入者及び依拠当事者の情報のセキュリティ
	資産の分類と管理	識別されたリスクと公開された規定に基づいた認証局資産と加入者及び依拠当事者情報の適切な保護
	人員のセキュリティ	CA の運用をサポートする要員の管理策
	物理的・論理的セキュリティ	認証局は以下の保証する管理策を維持する ● CA 設備の物理アクセスのコントロール及び二重管理による運用

		● CA 設備及び機器の環境災害からの保護 ● 資産の損失、危殆化、業務継続への影響からの保護 ● 情報及び情報機器の危殆化からの保護
	運用規定	認証局は以下の保証する管理策を維持する ● CA の情報システムの安全な運用 ● CA システム障害リスクの最小化 ● ウイルス及び悪意のあるソフトウェア対策 ● インシデント報告及びインシデント管理策による損失、無効化リスクの軽減 ● メディアの保護
	システムアクセス管理	認証局システムへのアクセスが許可されたものに限定されていること保証する管理策を維持する ● あらかじめ規定された権限者による OS 及びデータベースへのアクセス ● CA システムのネットワークセグメントへのアクセスは許可された要員、アプリケーションおよびサービスに限定されている ● CA アプリケーションの使用は許可された要員に限定されている
	システムの開発と保守	システムの開発と保守は文書化され、試験され、許可されており、CA システムの完全性を維持するために実施されていること
	ビジネス継続性の管理	災害時にも事業継続を保証する管理策を維持する ● CA の重要コンポーネントの災害復旧計画の開発維持

		● 暗号製品の代替保管場所 ● 遠隔のバックアップシステム ● バックアップサイトの可用性
	モニタリングと遵守	認証局は以下の保証する管理策を維持する ● 関連法律および契約の要求事項への適合 ● CA セキュリティポリシーと手順への適合 ● システム監査プロセスの効果の最大化とシステム監査プロセスによる悪影響の最小化 ● 不正な CA システムの使用の検知
	監査ログの取得	認証局は以下の保証する管理策を維持する ● CA の重要環境、鍵管理、証明書管理イベントはログされていること ● 監査ログの機密性と完全性の保証 ● 公開されている業務規程に沿った監査ログの保存 ● 許可された要員による監査ログの定期的なレビュー
CA 鍵ライフサイクル管理	CA 鍵の生成	認証局は CA の鍵ペアが公開されている業務規程及びキーセレモニースクリプトに定められている手順にしたがって生成されていること保証する管理策を維持する 認証局の公開される業務規程には以下を含む ● CA の鍵生成は物理的に安全な環境で実施されること ● CA の鍵生成は信頼できる要員による二重管理の下実施される ● CPS に定められている適切な HSM を利用して CA 鍵生成が行われる ● CA 鍵生成がログされている

		キーセレモニースクリプトは以下を含む ● 参加者の役割と責任の定義 ● キーセレモニー実施の承認 ● 暗号ハードウェアと活性化キー ● キーセレモニーで実施される特定の手順 ● セレモニールームの物理セキュリティ要件 ● キーセレモニー後の暗号装置と活性化キーの保管場所 ● キーセレモニーがスクリプト通り実施されたことに対する参加者及び立会人の署名 ● キーセレモニースクリプトからのあらゆる差異の記述
	CA 鍵のストレージ、アックアップと復旧	CA 秘密鍵の機密性と完全性の保護。CA 秘密鍵のバックアップ及び復旧は、物理的に安全な環境で二重管理の下実施される。
	CA 公開鍵の配布	CA 公開鍵の完全性と真正性の保証
	CA 鍵の使用法	CA 鍵はあらかじめ定められた場所で、意図した目的にのみ使用されること
	CA 鍵の保存及び破壊	認証局は以下の保証する管理策を維持する ● 保存された CA 鍵の機密性が保持され、プロダクションサイトには戻されないこと ● CA の公開された業務規程に従って、CA 鍵がライフサイクルの終わりに破棄されること
	CA 鍵の危殆化	CA 鍵の危殆化の際にも CA の運営が継続され、危殆化した鍵で署名されたすべての証明書が失効され再発行されること

	CA 鍵の暗号装置ライフサイクル管理	認証局は以下の保証する管理策を維持する ● 秘密鍵の保管、復旧に使用されるデバイスは使用の前に完全性確認のためにテストされること ● HSM へのアクセスは許可されたものに限定されており、二重管理が実施されていること ● HSM が正しく動作していること
	CA 鍵供託	供託された CA の秘密鍵の機密性が保持されること
加入者鍵ライフサイクル管理	加入者鍵生成	認証局は以下の保証する管理策を維持する ● 加入者の鍵が公開されている CA の業務規程及びリスク分析に沿って安全な暗号ハードウェアによって生成されていること ● 生成された加入者の鍵が安全に配布されること
	加入者鍵の保管と復旧	認証局は以下の保証する管理策を維持する ● CA に保管される加入者の秘密鍵の機密性及び完全性の維持 ● CA に供託される加入者秘密鍵の機密性維持 ● 鍵ライフサイクルの終了と共に CA が保管する加入者秘密鍵の安全な廃棄
	IC カードライフサイクル管理	認証局は以下の保証する管理策を維持する ● IC カードの調達、準備、初期化が安全に管理されていること ● IC カードのアプリケーションデータファイルが安全に管理されていること

		● IC カードの使用が認証局によって可能になっていること ● IC カードのディアクティベーションとリアクティベーションが安全に管理されていること ● IC カードが安全に保管され配布されること ● IC カードが安全に交換されること ● 返却された IC カードが適切に処理されること
	加入者鍵管理	認証局は以下の保証する管理策を維持する ● 加入者鍵保護の要件が適切に加入者に伝えれること ● CA の公開する業務規程の要件に沿った加入者鍵の管理ツールの提供
証明書ライフサイクル管理	加入者の登録	認証局は以下の保証する管理策を維持する ● 加入者は正確に識別されていること ● 加入者の証明書発行要求は正確であり完全であり認められていること
	証明書更新	証明書更新要求は正確であり、完全であり認められていること
	証明書リキー	証明書リキー要求は正確であり、完全であり認められていること
	証明書発行	証明書は公開されている CA の業務規程に従って生成され発行されていること
	証明書配布	公開されている CA の業務規程に沿って発行された証明書が加入者及び依拠当事者にわたること
	証明書失効	公開されている CA の業務規程に定められている期間で証明書が、認められ、検証された失効要求に従って失効されること

	証明書停止	公開されているCAの業務規程に定められている期間で証明書が、認められ、検証された停止要求に従って停止されること
	証明書検証	公開されているCANお業務規程にそって、正確な証明書ステータス情報が関係者に公開されること
下位認証局ライフサイクル管理	下位認証局ライフサイクル管理	上位認証局は以下の保証する管理策を維持する ● 下位認証局の証明書要求が正確で認められたものであること ● 下位認証局の証明書更新要求が正確で認められており、完全であること ● CA の業務規程に従って下位認証局のリキー、更新或いは新規証明書が発行されること ● CA の業務規程に従って、発行された証明書が下位認証局にわたること ● 下位認証局の証明書は許可され、検証された失効要求によって失効される ● CA の業務手続きに従って、正確で完全な証明書ステータス情報が全ての関係者に公開される

表 5 日本の技術要件

要求範囲	要求項目	要求内容
業務の用に供する設備の基準	認証室への入出場を管理するために必要な措置	● 生体認証と二重管理による認証室への入退室管理 ● 入室権限者の設定と識別／認証 ● 入退室の人数管理とアラームシステムの連携 ● 設定された入退室時間の超過によるアラーム ● カメラ、センサーなどによる自動的／継続的監視 ● 登録端末、利用者識別設備が設置された部屋は施錠されること
	認証業務用設備への不正アクセス等を防止するために必要な措置	● 認証業務用設備がネットワークにつながる場合、ファイアフォールや不正なアクセスを検知するシステムを備えること ● 認証業務用設備が 2 つ以上の部屋に設置され、互いにネットワークにより接続されている場合、セキュアな通信チャンネルの利用 ● 利用者が利用者署名符号を生成する場合において、利用者署名符号を認証局が受信する際は、受信機の誤認及び盗聴等から保護すること
	正当な権限を有しない者に認証業務用設備の作動を防止するための措置等	● 認証業務設備は個人単位でアクセスコントロールを実施すること ● 利用前に識別／認証すること ● あらかじめ利用者ごとにアクセス権限を定めること ● 利用者署名符号を利用者が生成する場合において、利用者情報及び利用者識符号によって自動的に認証業務用設備を作動させる場合、あらかじめ利用者情報及び利用者識別符号を設定しておくこと

		● 利用者識別符号等受信装置は鍵などが取り付けられた部屋に備えれており、無人の際は施錠されること ● 電子証明書の発行及び失効の要求等の管理に必要な登録用端末設備以外はネットワークを通じた遠隔操作が不可能となるように設定すること ● 認証業務用設備の所在を明らかにしないこと ● 各イベントのログをとる監視機能を備えること ● 監視機能は操作者ごとに履歴を確認できること
	発行者署名符号の生成管理に使用する暗号装置	● FIPS140-2 相当の HSM の使用
	認証業務用設備等の災害の防止するために必要な措置	● 耐震措置 ● 水害防止措置 ● 認証設備質の隔壁 ● 自動火災検知器と消火器の設置 ● 認証設備室は防火区域ないであること ● 停電対策 ● 安定した地盤であること ● 耐震性のある建物であること ● 準耐火建物であること
利用者の真偽の確認の方法	認証業務の利用申し込み等	● 対面、郵送、或いはネットワークを通じた申請 ● 本人確認資料の指定 ➢ 印鑑証明 ➢ 公的個人認証 ➢ 住民票の写し ➢ 戸籍謄本 ➢ 住民票記載事項証明書等
	利用者の真偽の確認方法等	● 本人確認資料の有効性確認

その他の業務の方法	利用者申し込みに対する説明事項	● 利用者に以下の事項の説明 ➢ 虚偽の申し込みによる不実の証明となった場合、罰せられること ➢ 電子署名の法的有効性と署名符号の安全な管理 ➢ 危殆化の際の失効要求 ➢ 指定する署名アルゴリズムの利用
	利用者申込書等の記載事項等	● 利用用途 ● 利用者指名のローマ字表記 ● 自署または印鑑証明書を本人確認に用いた場合、当該印鑑による押印 ● 代理人が申し込む際には代理の理由及び代理人の自署名または押印
	利用者署名符号及び利用者識別符号の生成等	● 利用者署名符号を認証局が生成する場合は、安全に利用者に送信し、当該符号のコピーをすべて削除すること ● 利用者署名符号を利用者が生成する場合において、当該利用者署名検証符号をネットワークを通じて認証局が受信する場合、あらかじめ利用者識別符号を安全な形で利用者に送付し、また、当該利用者の識別に用いるまで、第三者に知られないようにすること
	電子証明書に係る事項	● 電子証明書の有効期間は 5 年を超えないものとする ● 電子証明書には以下の情報を含む ➢ 発行者の名称及び発行番号 ➢ 発効日及び有効期限 ➢ 証明書利用者の氏名 ➢ 利用者署名検証符号及びアルゴリズム識別子 ● 電子証明書発行に係る電子署名方式は以下のいずれかとする ➢ SHA-1, 256, 384, 512, かつ鍵長 1024bit 以上 RSA 方式 ➢ SHA-1, 256, 384, 512 かつ鍵長

		1024bit 以上 RSA PSS 方式 ➢ SHA-1, 256, 384, 512　かつ鍵長 160　bit 以上 ECDSA 方式 ➢ SHA-1, かつ鍵長 1024bit 以上 DSA 方式
	認定認証業務と他の業務との誤認を防止するための措置	● 認証業務に関して利用者が認定認証業務とその他認証業務を誤認する措置を講じること ● 発行者電子署名符号を認定認証業務にのみ使用すること ● 発行者署名検証符号に係る電子証明書の値を SHA-1,256, 384, 512 のいずれかで変換した値で認定認証業務を特定すること
	電子証明書への属性の記録	● 役職等の属性情報は認定対象外であることを電子証明書に明示すること
	署名検証者への情報提供	● 署名検証者が検証に必要な発行者署名検証符号その他情報を署名検証者に公開すること ● 証明書ステータス情報の公開 ● 証明書利用目的と利用制限の通知
	電子署名の失効に係る事項	● 利用者から電子証明書の失効要求を受けた或いは、電子証明書の内容に変更があった場合は失効に関する情報を記録すること。 ● 失効要求の真偽確認方法、記録手続きを定めていること ● CRL、OCSP 等による失効情報の提供 ● 失効した旨を遅延なく利用者に通知すること
	認証業務の実施に関する規定	● 以下を認証業務規程に含めること ➢ 認証事業者の連絡先（住所、電話番号、ファクシミリ番号及びメールアドレス）を認証業務規程に明示すること ➢ 電子証明書発行対象

		➢ 電子証明書の使用目的、制限 ➢ 利用者の属性情報が認定対象外であること ➢ 認定事業者の保証と責任 ➢ 保証及び面積範囲 ➢ 利用申込必要書類 ➢ 利用者の真偽確認方法、本人確認資料 ➢ 電子証明書失効に係る情報 ➢ 電子証明書失効情報確認に係る情報 ➢ セキュリティに関する事項 ➢ 個人情報の取り扱いに関する事項 ➢ 料金に関する事項 ➢ 認証業務において保存する帳簿書類の保存期間、保存方法等 ➢ 業務の廃止時の発行済み電子証明書の失効方法、利用者への通知方法 ➢ 適用法令及び管轄裁判所の情報 ➢ 規定の改訂とその通知方法に係る事項
	認証業務の廃止	● 廃止の 60 日前までに利用者に通知すること ● 発行済み電子証明書が失効されることの通知
	電子証明書名義人への情報の開示	● 電子証明書の名義人からの申し出に応じて当該電子証明書に係る利用者に関する書類を開示すること
	認証業務実施のための組織及び体制等	● 以下の事項を定めること ➢ 業務の手順 ➢ 職務分掌権限規定 ➢ 指揮命令系統 ➢ 業務委託時の受託者による適切な管理の実施を確保する方法 ➢ 業務の監査に係る事項

		➢ 要員の知識／経験 ➢ 個人情報保護 ➢ 危機管理に関する事項
	認証業務用設備の操作等に関する許諾等	● 認証設備室へのアクセスコントロールの実施 ➢ 二重管理 ➢ アクセス権限の登録 ● やむを得ず、権限のないものがアクセスする場合は権限のあるものが複数同行すること ● システム管理者の識別符号の厳重な管理
	発行者署名符号の漏洩を防止するために必要な措置	● 発行者署名符号の生成は二重管理の下実施される ● 発行者署名符号は認証設備室内でHSM を用いて生成される ● 発行者署名符号のバックアップ及び復帰は二重管理の下実施される ● バックアップの適切な保護 ● 発行者署名符号の状態変更は認証設備室内で二重管理のもと実施される ● 発行者署名符号の使用を終了する場合、二重管理の下物理的に破壊、或いは完全な初期化を行う、またコピーされた符号も同時に廃棄する
帳簿書類	認証業務利用申込に関する帳簿書類関係	● 認証業務の利用申し込みに関する帳簿書類で次に掲げるものは、電子証明書の有効期限満了から 10 年間保存する ➢ 利用者申込書 ➢ 本人確認資料 ➢ 申込の諾否を決定したものの氏名 ➢ 承認されなかった場合その理由 ➢ 電子証明書作成に係る記録 ➢ 発行者署名検証符号 ➢ 発行者署名符号の作成／管理に関する記録

		➢ 認証事業者が利用者署名符号を生成した場合、利用者からの利用者署名符号の受領書
	電子証明書の失効に関する帳簿書類関係	● 電子証明書の失効に関する帳簿書類で次に掲げるものは、電子証明書の有効期限満了から 10 年間保存する ➢ 失効請求書及び失効判断に係る記録 ➢ 失効を決定したものの氏名 ➢ 失効拒否となった場合その理由 ➢ 全ての失効情報
	認証事業者の組織管理に関する帳簿書類関係	● 認証業務の組織管理に関する帳簿書類で次に掲げるものは、電子証明書の有効期限満了から 10 年間保存する ➢ CP、CPS ➢ 業務手順の変更記録 ➢ 職務分掌権限規定、組織図などの変更記録 ➢ 業務委託契約書 ➢ 監査実施記録
	設備及び安全対策措置に関する帳簿書類関係	● 認証業務の利用申し込みに関する帳簿書類で次に掲げるものは、作成日から認定の更新日まで保存する ➢ 入退室に関する記録 ➢ 不正アクセスの記録 ➢ 認証業務用設備の動作記録 ➢ 許諾記録 ➢ 認証業務用設備関連の維持記録 ➢ 障害と復旧に関する報告書 ➢ 帳簿書類の利用と廃棄に関する記録