eシール解説
～実用化に向けて～

バージョン1.0
(2022.9)

デジタルトラスト協議会（JDTF）

1.はじめに

新型コロナウイルス感染拡大に伴い、テレワークの推進が一層求められ、インターネット上で官民や民間同士の様々なやり取りを電子的に完結可能な環境の需要が高まっている。
特に企業において、契約に基づき発生する請求書・領収書等の紙処理は依然として多く、押印手続きだけのために出社を余儀なくされていることが深刻な課題となっている。
また、ペーパーレス化は徐々に浸透しているが、紙をデータに置換した際に必要となる、送信元のなりすましや電子データの改ざん、ねつ造等を防止する手段であるトラストサービスが、今後重要な役割を果たすと期待されている。

欧州連合(以下、EUという。)では、eIDAS規則[1]において、電子文書の発信元の組織を示す目的で行われる暗号化等の措置（以下、eシールと呼ぶ）を含む複数のトラストサービスが法制度化済みである。さらに、トラストサービスの第三国との相互承認の検討が進められている。一方で、日本では「電子署名及び認証業務に関する法律」[2]により、自然人による電子署名の措置は制度化されているものの、EUにおけるeシールに相当する「組織が電子的に発行したことを簡便に保証する」制度は2022年9月現在で存在しない。
このような状況を踏まえると、電子データの発信元組織を明示し、発信元のなりすましや電子データの改ざん等を防止する仕組みであるeシールの早期導入を図ることが必要である。

総務省では、2020年に「組織が発行するデータの信頼性を確保する制度に関する検討会」[3]を立上げ、eシールに関し、一定の基準に基づく民間の認定制度の創設に向けて、ユースケースについて幅広く調査し、2021年6月に「eシールに係る指針」[4]を公表した。

上記背景を踏まえ、「eシールに係る指針 」を参考にしながら、特に公開鍵基盤(以下、PKIと呼ぶ)に基づくeシールを実用化し、より広範に活用するために必要となる様々な事項について、技術的・運用上の観点から幅広く検討した結果を解説としてまとめた。日本版eシールが民間認定制度として立ち上がり、ひいては国際連携を見据えた国の認定制度へと繋がっていくことを期待するものである。

2. 本書目的

本書では、eシールに関する様々な事項を解説(定義、対象、用途、システムモデル、実用化の課題や論点)することを目的とし、以下を想定読者としている。

---

[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
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[2] https://elaws.e-gov.go.jp/document?lawid=412AC0000000102

[3] https://www.soumu.go.jp/main_sosiki/kenkyu/data_organization/index.html

[4] https://www.soumu.go.jp/main_content/000756907.pdf

- eシールに関わるサービスやシステムを提供する事業者
  認証局、eシール対応の製品やシステムの開発・SIベンダー、リモートeシールサービス
- eシールを生成あるいは検証したい企業や組織

3. 用語定義

用語・略称	説明
CA	Certification Authority: 署名鍵(秘密鍵)と対になる公開鍵に対する公開鍵証明書(以下、証明書と呼ぶ)を発行する機関。
CP/CPS	Certificate Policy/Certification Practice Statement: CPは証明書ポリシーで発行する証明書の利用目的や適用範囲などの適用方針を定めた文書。CPSは認証局運用規定でCPの適用手順を示したもの。
CSR	Certificate Signing Request: 証明書の発行要求であり、証明書の発行要求者の公開鍵とその公開鍵等のデータに対し、発行者の署名を含むデータである。データ形式として、PKCS#10などがある。
EE証明書	エンドエンティティ証明書: PKIを利用するユーザーやシステムに対し、発行する証明書。リーフ証明書とも言う。
eIDAS規則	EU市場における電子商取引のための電子識別およびトラストサービスに関する規則。
HSM	Hardware Security Module: ハードウェアの暗号モジュールであり、ハードウェア内で鍵を保管し、暗号化機能や署名機能を有する装置。
JT2A	日本トラストテクノロジー協議会: 電子署名・証明書や電子認証などのトラストテクノロジーに関連する事業者及び利用者が主体となり、産学官及び国内外の関連団体と連携して信頼性を担保するための技術等の検討を行うことで、より信頼できる電子社会の促進に寄与することを目標とする団体。
QSCD	Qualified Signature/Seal Creation Device: 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装置で、欧州eIDASによる基準への適合性の評価を受け認証されたもの。
SCAL	署名者単独管理保証レベル(Sole Control Assurance Level): リモート署名において、署名者の単独管理の下、リモート署名が生成されたことを保証するレベルを表し、低レベルのSCAL1と適格電子署名、適格eシールを要求するSCAL2がある。CEN 41

	9 241-1にて規定されている。
クレデンシャル	サービスやシステムの利用時に認証に用いるための資格情報。例えば、ID/パスワード、公開鍵証明書と秘密鍵の組合せ、認証デバイス(FIDOトークン、認証ドングル等)、他の資格情報とワンタイムパスワードの組合せなどがある。
コードサイニング (コード署名)	実行ファイル、ソフトウェアライブラリ、ソフトウェアパッケージ、ソフトウェア更新に付与するデジタル署名。ソフトウェアの発行元や非改ざん性を保証するために利用される。
署名検証サービス	電子署名データ、eシールデータを検証するサービス。
セキュアエレメント	耐タンパ性、すなわち外部から内部のデータを解析、不正読み取り、改ざんできず、またそのような攻撃に対して証跡を残す機能を持ち、共通鍵や秘密鍵、証明書データ等を安全に格納できる半導体製品。
先進電子署名	Advanced Electric Signature (AdES): PKIを使用して作成された電子署名であり、デジタル証明書と署名者の同一性を確認、署名者が制御可能な署名生成を用いて作成、署名後の改ざんが検知できるデータ。ISO(ETSI)規格で定義された署名フォーマット(PAdES/XAdES/CAdES/ASiC)のデータ。
中間CA	Intermediate CA: 自らの証明書は他の認証局から発行され、対となる秘密鍵を用いて認証業務(サービス)を提供する認証局。
適格電子署名	Qualified Electric Signature (QES): 欧州において自然人が手書き署名を行ったのと同等の法的効力をもつ電子署名。適格電子署名では、適格トラストサービスプロバイダーによって発行された適格証明書とQSCDに基づき、先進電子署名を作成することが求められる。
秘密鍵活性化	秘密鍵アクティベーションとも言う。秘密鍵を使用可能な状態にすること。例えば、セキュアエレメント等で管理された秘密鍵を使用する際に、パスワード入力を求めることで、秘密鍵が必要となる瞬間のみ秘密鍵の活性化を行うことができる。

4. eシールの定義

デジタルデータは複製、転送、変更が容易である反面、何ら対策を講じないと、発出元が作成したデジタルデータが転送過程で改ざんされ、受信者側ではその痕跡すら検知できないような状況が生じうる。このような場合、受信者側は受信したデジタルデータに改ざんがあり得ることや発出元が成りすましをしている可能性を考慮しなければならない。また、実際には改ざんがなかった場合であっても、発出元が転送したデータの内容を事後に否認するこ

と、あるいは、転送過程で改ざんがあったと主張することや、発出元ではないと主張することが考えられ、いずれにおいても、そのデジタルデータに基づいて重要な判断を行うことには大きなリスクを伴うことになる。

eシールは、検証処理を実行することでデジタルデータの起源(発出元)と完全性(非改ざん性)を確認可能とするために、デジタルデータに添付あるいは論理的に関連付けられたデータあるいはそのデータを生成し付与する措置をいう(「eシールに係る指針」では「措置」と定義されているが、本書では誤解を生じない限り、「データ」と捉えて記す)。電子署名は自然人が生成主体となるのに対し、eシールは 法人や組織等(以下、法人等と表す)が生成主体となる。

電子署名が自然人の意思を表すものである一方、eシールは法人等の意思を表すものではないと解釈するのが一般的である(法人等自体には意思表示ができないため)。そのため、欧州では一部の国(ベルギー等)を除き、意思に基づく「契約」に対してeシールの効果を認めていない。

eシール用証明書は、eシールを検証するためのデータ(公開鍵等)を法人等のeシールの生成主体にリンクし、その法人等を確認可能とするデータである。

eシールを実現するためには、一般にPKIに基づくデジタル署名技術が利用される。この場合、eシール用証明書は公開鍵証明書となり、デジタルデータの発出元と非改ざん性を証明可能となる。

電子署名、eシールとも、事後の否認を防止し、責任の所在を明確にすることを目的としている。PKIに基づく十分に新しい暗号技術と十分な厳密性を持った運用(身元確認や鍵管理等)を適用することにより、責任の所在の確実な特定が可能となる。

5. 本書が扱うeシールのスコープ

4章の定義によりeシール用証明書の発行対象は法人、組織、法人や組織が提供するサービスや装置等といった非自然人になりえる。eシールの議論が始まる以前より、例えば、Webサイト証明書に代表されるように、特定の用途に対して非自然人に対する証明書発行は行われており、その用途ごとに対象の確認や証明書の発行といった運用方法や、証明書の記載事項を定めたプロファイルが規定されてきた。eシールを非自然人に対する証明書として広義にとらえれば、こうした従来の非自然人向け証明書もeシールの概念に含まれることとなる。これから新たに議論を始めるeシールの意義は、組織から発するデータを組織や国境、業界等を超えて相互運用することにあるが、その一方で、eシールの登場によって、Webサイト証明書やデバイス証明書など既存の非自然人向け証明書の運用を妨げてはならない。そこで、本書で整理したeシールのスコープは以下のものとした。

- eシールの対象をデジタルドキュメントやデータとする。

- eシールの新たなユースケース、または、ドメインを超えた相互運用が必要となるユースケースに対して適用できる共通的な運用や証明書プロファイルを主な対象とする。
- 特定用途の非自然人向け証明書として従来から存在する運用やプロファイルの規定については、新たな規定の上書きや再定義をすることは求めない。本書が詳細化する対象外とし、従来の規定に従うものとする。
    - 詳細化の対象外の例としては、Webサイト証明書、プラットフォームで要求されるコードサイニング証明書、S/MIME証明書がある。
    - タイムスタンプ局証明書などトラストサービス向け証明書についても、トラストサービスの適格性を認定するという組織等の存在証明以上の意義があるため、本書の詳細化の対象外とする。
    - 装置、システム、サービスに対する証明書発行においては、個々の機器を識別し発行されているデバイス証明書との違いを認識する。

eシールの対象を整理する観点として例えば以下がある。

- eシール用証明書の発行対象
    - 法人、組織
    - 法人/組織内の部門、事業所など
    - 法人/組織内で管理される装置、システム、サービス
- パブリックな相互接続や相互運用を想定したユースケース
- プライベートな環境に限定されるユースケース

6. eシールのユースケース例

法人および法人内組織が発出する情報は様々である。ここでは、法人および組織が発出するデジタル情報の信頼性を確保することを前提にしたeシールの適用先として考えられる例を記載する。

適用先の大きな分類として、既存の人手を介した業務プロセスの過程で作成や送受、保存等が行われる紙文書類をデジタルに置き換えたドキュメントと、ITシステムを前提としたシステムやデバイス等において機械的に処理されるデジタルデータがある。

それぞれの分類において、eシールの適用先の例を以下に示す。

- ドキュメントの例
    - 組織間取引で交換される文書類
      例：契約書、受発注情報、申込書、請求書、領収書
    - 組織が公開する文書類
      例：ニュース、プレスリリース、官報、約款、カタログ、取扱説明書

    - 組織が発する証明書類
      例：保証書、在籍証明、ライセンス(資格)証明
    - 官に関連するもの
      例：官報、申請、入札
    - 監査関係資料
      例：IR情報、残高証明
    - その他
      例：電子メール、知財機密情報

- デジタルデータの例
    - デバイスやシステムからの発出データ
      例：カメラの画像や動画、センサーデバイスによる測定データ、POSシステムの売上情報
    - サービス間で交換されるデータ
      例：決済サービスの取引データ、eデリバリーサービス、
    - プログラムコード
      例：プログラム実行ファイル、ソフトウェアパッケージ、ライブラリ、マクロ

利用目的によって電子署名とeシールの使い分けを検討する必要もあるだろう。4章で述べたように、電子署名ではなくeシールであるという理由のみでデータに対する否認防止効果が否定されるわけではないが、eシールの適用を検討している対象が法令等により電子署名が求められる、あるいは、電子署名がより適しているものもある。実際にeシールの適用を考える場合には、既存の法令等も含めて検討することが必要である。

7. eシールのシステムモデル

7.1 本章の概要

本章では、eシールの利用イメージを具体化するために、eシール用証明書やeシール署名鍵の管理方法、利用方法などの観点で数種類のシステム構成例を例示する。7.2節ではeシール用証明書発行対象のバリエーションを例示し、7.3節以降では今後想定されるeシール利用方法を分類し、それぞれのシステムモデルについて解説する。

7.2 eシール用証明書の発行対象のバリエーション

eシール用証明書の共通的な発行対象は法人や組織である。6章で例示した様々なユースケースには、法人や組織に関するより詳細な情報が求められるものもあり、それらの情報をeシール用証明書に記載したいという要求も考えられる。例えば以下のものが考えられる。

- 法人/組織名
- 法人/組織の事業所名
- 法人/組織内の部署名
- 法人/組織が提供するサービス名
- 法人/組織が提供/管理するシステムやアプリケーションの名称等

上記を発行対象とする場合や、発行対象(法人や組織)に関連した属性情報としてeシール証明書に記載する場合には、それら情報に対して認証局が行う審査方法と共に検討を行う必要がある(8章を参照のこと)。上記におけるシステムやアプリケーションは法人/組織の業務や事業の一部として機能するものとし、その業務や事業の目的のために発行された証明書を用いることを想定する。

発行対象の法人や組織等がeシール用証明書を取得した後、法人や組織、事業所、部署といったセクション内で権限を与えられた担当者がeシール生成に関わる管理や操作を行うことになる。本書ではeシール生成に関わる担当者について以下の役割を規定する。

- 管理者
  eシール生成を行う組織内において、eシール署名鍵、eシール署名鍵格納媒体やeシール生成サーバー、eシール署名鍵が組み込まれたシステム等の管理を行う者
- オペレーター
  eシール生成を行う組織内において、eシール署名鍵格納媒体、eシール生成サーバー、リモートeシールサービス等を用いて、与えられた権限の下で対象データに対してeシール生成を行う者

組織内に複数の管理者やオペレーターが存在することもある。リモートeシールサービスを利用する場合、リモートeシールサービスでのユーザー認証やeシール生成の認可を行うためのクレデンシャルを管理者やオペレーターが管理することもある。

7.3 システム構成例の分類

ここではeシール署名鍵の格納方法、eシール用証明書の発行、eシール署名鍵へのアクセス方法、eシール生成方法に関わる論点をより具体的にイメージできるように数種類のシステム構成例を紹介する。eシール署名鍵やeシール用証明書の運用方法の違いにより、以下の分類で整理した。

- 組織内運用
  組織内運用はeシールを組織内で作成した文書やデータに対して生成するものである。eシール署名鍵の管理やeシール生成の運用方法の違いにより、さらに以下に分類できる。
  - 媒体管理型
  - サーバー管理型

    - システム組込み型
- リモートeシールサービス
  第三者機関として各組織のeシール署名鍵の管理を行うもの。
- 機器組込み
  デバイスにeシール署名鍵を搭載し、デバイスからの出力データにeシール生成を行う形態。

7.4節以降では各運用形態の例について解説する。

一般的なeシール生成に至る工程は以下のフェーズで構成される。システム構成や運用方法によって各フェーズで実施される内容の詳細は異なる。

1. eシール署名鍵生成フェーズ
   組織の管理下にある装置、または、組織の要求に基づき認証局やリモートeシールサービスにより、eシール署名鍵を生成する。生成方法にはシステム構成や運用方法によりバリエーションがある。8.4.1節で課題や考え方を示している。
2. eシール用証明書発行フェーズ
   認証局が組織等の存在を確認したうえで、eシール署名鍵に紐づく証明書を発行する。8.3節で組織等の確認や証明書発行に関する課題や考え方を示している。
3. eシール生成フェーズ
   eシール対象データに対して、フェーズ1で生成されたeシール署名鍵を用いて、eシールを生成する。リモートeシールサービスを用いる場合には、リモートeシールサービスが組織を認証(authentication)し、eシール生成の認可を行ったうえで、当該組織のeシールを生成する。8.4.2節でeシール署名鍵の管理や利用に関する課題や考え方を示している。
4. eシール検証フェーズ
   eシールを受領する者がeシールを検証し、eシール対象データを利用する。eシールの検証プロセスはeシール用証明書に含まれる検証鍵(公開鍵)を用いたデジタル署名データの検証、信頼点となる証明書からeシール用証明書に至るパス検証等が含まれる。また、検証プロセスの実行形態としては、検証機能を有したソフトウェアやデバイスやシステム、第三者機関による検証サービス等が考えられる。検証方法に関する考え方は後述する。
5. eシール署名鍵廃棄フェーズ
   組織においてeシール署名鍵の使用を終える場合には、eシール用証明書の失効手続きを行い、署名鍵を廃棄する。8.4.2.2節で失効や廃棄に関する課題や考え方を示している。

eシールの検証方法は従来の電子署名の検証と同様に考えることができる。デジタル署名データの検証や証明書のパス検証といった共通の検証方法(参考：デジタル署名検証ガイドラ

イン[5], ETSI EN規格[6])は電子署名と同じであり、これまで利用されてきた電子署名の検証ソフトウェアやサービス等を活用することが期待できる。また、アプリケーションや適用先の要求に応じて、eシール用証明書や署名フォーマットの記載事項に関する追加の確認が必要となる場合がある。例えば、eシール付きデータの受領者(検証者)が、eシールのデジタル署名としての有効性を検証したうえで、追加の確認として、eシール用証明書に記述されているLEIや法人番号等に基づき、他のデータベースから取得したその組織に関する属性が所定の条件を満たすか等のチェックを行うことが考えられる。このようなアプリケーションに依存する追加の確認事項などの要件はアプリケーション毎に規定する必要がある。

7.4 組織内運用

7.4.1 媒体管理型

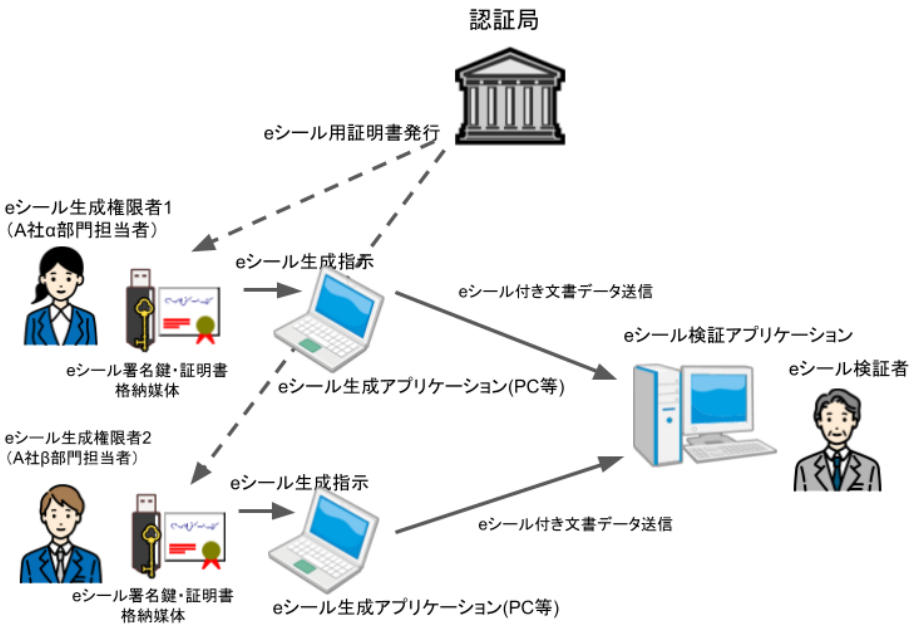

図 7-1 組織内運用(媒体管理型)の例

オペレーターが使用するPCやモバイルデバイスなどのローカル端末にインストールされたeシール生成アプリケーションを用いて、eシール生成を行う(図7-1)。eシール生成アプリケーションは業務アプリケーションと一体になっている場合や、業務アプリケーションと連動する場合もある。業務アプリケーションの機能で作成または受信したドキュメントデータに対してeシール生成アプリケーションの機能でeシール生成を行う。業務アプリケーションはクラウドなどのリモート環境にあり、ローカル端末にあるeシール生成アプリケーションと通信によってドキュメントデータのハッシュ値などのデータをやり取りすることも考えられ

[5] 日本ネットワークセキュリティ協会「デジタル署名検証ガイドライン」https://www.jnsa.org/result/e-signature/2021/index.html

[6] ETSI EN 319 102-1 V1.3.1 (2021-11) 「Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation」

る。生成されたeシール付きドキュメントデータは業務アプリケーション等を通じてeシール検証者に配布される。eシール検証者はeシール検証アプリケーションまたはeシール検証サービスの機能を用いてeシールの検証を行う。

eシール署名鍵の管理や操作方法としては以下のバリエーションが考えられる。

- eシール署名鍵管理デバイス/ハードウェア
  eシール署名鍵が格納された媒体(例えば、耐タンパなICカードやUSBメモリ)をローカル端末に接続し、オペレーターがPIN入力を行う等によってeシール署名鍵を活性化し、eシールの生成を行う。
- ローカル端末での管理
  eシール署名鍵をローカル端末のOSの鍵ストア等にインストールする。eシール生成アプリケーションはその鍵ストア等を通じてeシール署名鍵にアクセスする。eシール署名鍵へのアクセスコントロールとして、eシール署名鍵へアクセスする場合にオペレーターにPIN入力を求める場合もあれば、OSログイン時のアクセスコントロール機能により実現する場合も考えられる。

eシール署名鍵を活性化するためのPIN入力はドキュメントごとに都度入力する場合もあれば、一度のPIN入力によって多数のドキュメントに対してバッチ処理を行う場合もある。

eシール署名鍵生成のバリエーションとしては、オペレーターが属する組織（例えば組織の情報システム担当部門）で署名鍵生成を行い、認証局がその署名鍵に対して証明書を発行する場合もあれば、認証局が署名鍵生成を行い証明書と共に媒体やファイルとして格納してオペレーター（または情報システム担当部門などの関連部門の担当者）に送付する場合も考えられる。

7.4.2 サーバー管理型

組織内にeシール生成サーバーを設置する運用方法である。eシール生成サーバーはeシール署名鍵の管理と、要求されたデータに対してeシール生成を行う機能を有する。他の組織内システムはeシール生成が必要な場合に、eシール生成サーバーと接続し、データに対するeシール生成要求を行う。

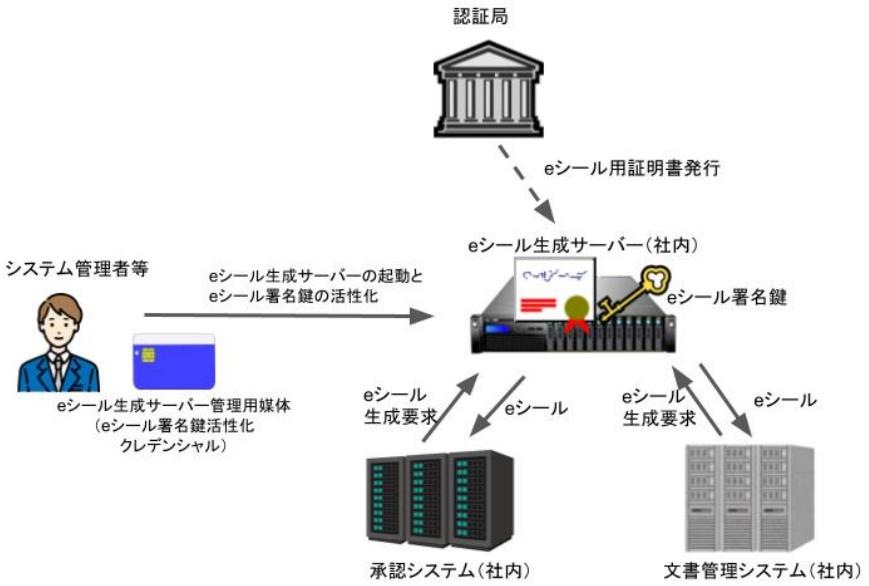

図 7-2 組織内運用(サーバー管理型)の例

eシール生成サーバーの運用形態の一例として、管理者によってeシール生成サーバーの設定や起動が行われた以降は常時稼働する形態が考えられる。その場合、eシール生成要求が、eシール生成サーバーの利用を許可されている特定の社内システムからのものであることを検証し、接続された社内システム（図7-2の例における承認システムや文書管理システム）からの要求に応じて自動的にeシール生成処理が行われることが考えられる。

7.4.3 システム組込み型

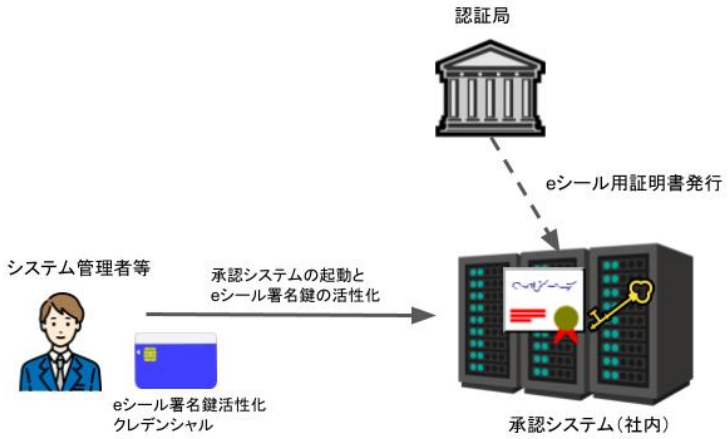

図 7-3 組織内運用(システム組込型)の例

システム組込型はサーバー管理型と同様に社内システム内で活用される運用形態であるが、サーバー管理型とは異なりeシール生成機能が独立しておらず、特定の社内システムに統合された形態となる。例えば、承認システムの内部で処理される承認フローの管理機能としてeシール生成機能を内包しているケースが考えられる。eシール適用範囲が特定の社内システムに限定される場合や、システムの管理や稼働環境などの制約でサーバー管理型の運用が難しい場合などに、システム組込型での運用が想定される。この運用形態ではeシール生成機能やeシール署名鍵などの管理は、対象システムの管理と共に行われることが考えられる。

7.5 リモートeシールサービス

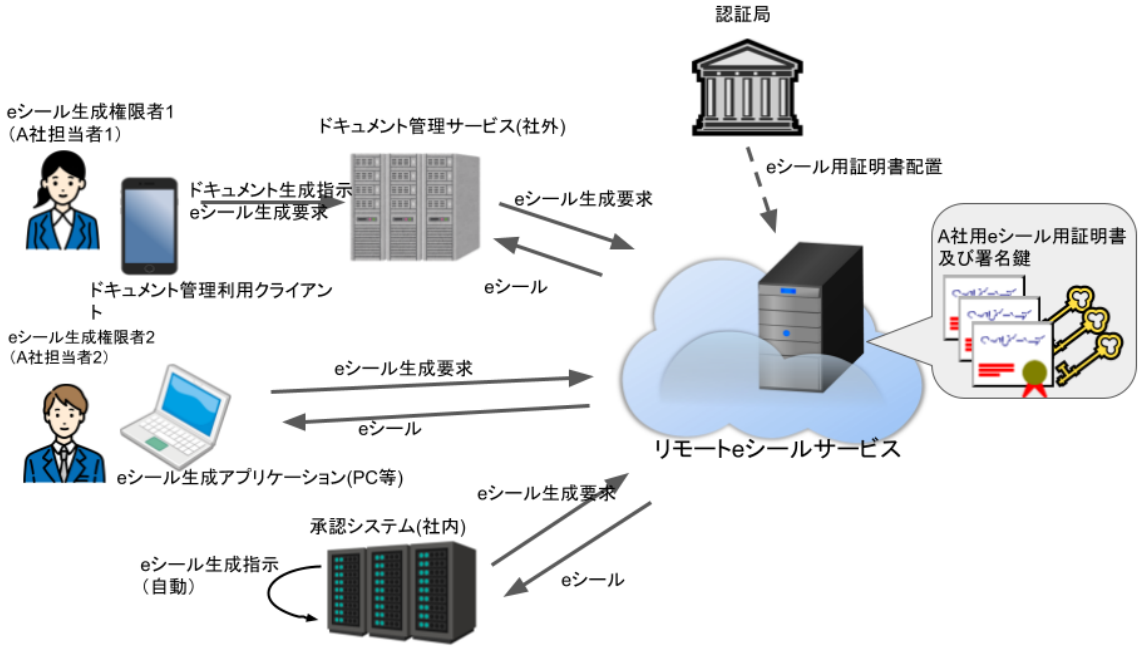

図 7-4のリモートeシールの例

リモート署名サービスのように、第三者機関のリモートeシールサービスが複数の顧客のeシール署名鍵を管理し、リモートでeシールを行う機能を提供する。オペレーターが操作するドキュメント管理アプリやドキュメント管理システム、ドキュメント管理サービスとリモートeシールサービスが連動する。ドキュメント管理システムから提供されるドキュメントデータ（またはハッシュ値）に対して、オペレーターの指示に基づき、リモートeシールサービスがオペレーターのeシール署名鍵を用いてeシール生成を行う(図7-4)。

eシール証明書発行対象の組織内の管理者やオペレーターはeシール署名鍵を直接管理や操作をする必要はないが、リモートeシールサービスへアクセスするための認証用クレデンシャルを安全に管理する必要がある。認証用クレデンシャルの種類はリモートeシールサービスが採用する認証方法に依存する。認証方法としては、例えば、パスワードやワンタイムパスワードなどがあり、端末認証なども組み合わせた多要素認証を求める場合もある。

リモートeシールサービスで求められるeシール署名鍵の管理やアクセス方法、オペレーターへの認証用クレデンシャルの割り当て及びeシール署名鍵との対応関係についてはバリエーションが考えられる。これらの論点は8章で整理する。

リモートeシールサービスを提供する事業者の形態には、例えば以下のようなものが考えられる。

- 認証局事業と共に行っている事業者
  eシール用証明書発行機能と共にeシール署名鍵のリモート管理機能を提供するサービス。
- 認証局事業者とは独立した事業者
  例としてeシール対象データ(または同データのハッシュ値)を受信し、デジタル署名の計算結果を返却するサービスや、汎用的な文書管理サービスと共にeシール生成サービスを提供するもの等が考えられる。
- 特定用途アプリケーション(サービス)と一体の事業者
  特定の業界や用途に特化したサービスにeシール生成機能を有したもの。

7.6 機器組込み

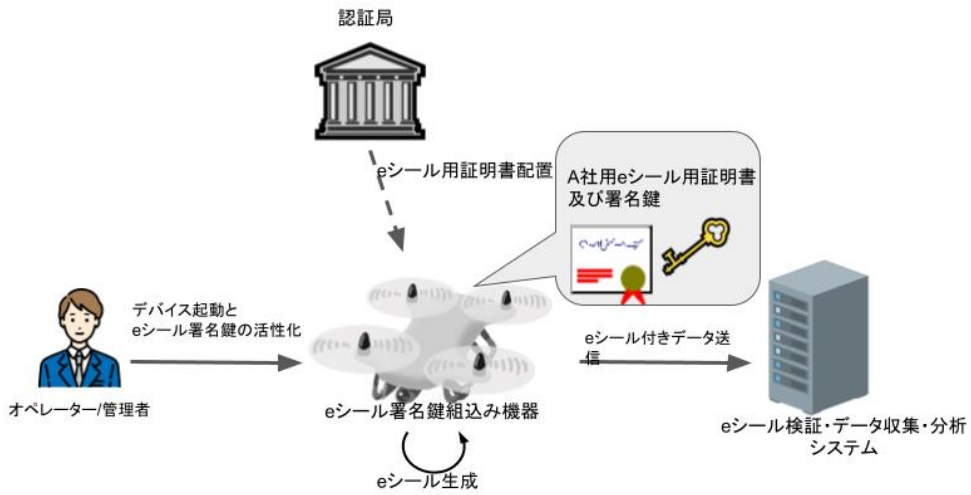

図 7-5の機器組込みの例

機器の種類や提供方法などによって様々な形態が考えられる。

eシールに限らず一般的な署名鍵に関して、機器が署名鍵を扱う分類として以下のものが考えられる。

- ハードウェア
  ハードウェアの製造過程において生成された署名鍵、もしくは、それらの署名鍵と関連して生成された署名鍵を利用するケース。これらの署名鍵はデバイスやチップベンダーの管理下に置かれることが考えられ、署名鍵は半導体チップなどセキュアエレメントによって管理されることが想定される。
- プラットフォーム
  OSなどデバイスを使用するための基本機能を提供するプラットフォームによって管理される署名鍵。これらの署名鍵はプラットフォーム提供ベンダーによって管理されることが考えられ、プラットフォームでサポートしているハードウェア上のセキュアエレメントによって署名鍵が管理されることも考えられる。
- アプリケーションが使用する署名鍵
  ハードウェアに配置されるアプリケーションが使用する署名鍵。これらの署名鍵はアプリケーション自身や、アプリケーション開発元や配布元の組織の管理下にある。特定の機能を有する単独のアプリケーションやサービスと連動して機能を提供するアプリケーションが考えられる。署名鍵はアプリケーションが制御可能なセキュアエレメント上の領域で管理されることも考えられる。

また、利用形態やシステム構成によって署名鍵の生成段階も様々なパターンが考えられる。例えば、以下のようなものが挙げられる。

- 機器製造段階での署名鍵生成
- 機器のプラットフォーム等のセットアップ設定段階での署名鍵生成
- オンライン上で機器管理プラットフォーム(クラウドIoTプラットフォーム等)やサービスに機器が接続しアクティベーション等を行う段階での署名鍵生成
- アプリケーションがインストールされる段階での署名鍵生成

署名鍵生成を機器内で行う場合と、機器外で行う場合等が考えられる。このような署名鍵生成段階のバリエーションと共にeシール用証明書の発行方法にも様々なバリエーションがある。

機器に対して発行される証明書としては、以前よりデバイス向け証明書が存在するが、これらの証明書はデバイスの認証用に用いられることが主眼であると言える。それに対して、機器へeシール署名鍵/eシール用証明書を導入することは、デバイスが発するデータ(乱数ではなく意味を持つデータ)に対する証明を行う目的であり、デバイス認証用途とは区別される。

eシールとして期待される証明の対象にはユースケースに応じて以下のようなものが考えられる。

- 機器の製造元や責任の所在の証明
  例：センサーデバイス、エッジデバイス、ドローン

- 機器上のソフトウェアの開発元や責任の所在の証明
  例：データ処理プログラム、データ整形プログラム
- 機器を構成要素の一つとするクラウドIoTプラットフォームの提供元や責任の所在の証明
- 機器を用いて実施されるサービスの運営主体・責任の所在の証明
  例：センサーネットワークを用いた気象情報サービス等
- 機器の運用・管理の主体となる組織の証明
  例：機器を用いたスマート工場を管理する企業など
- 特定の要件に適合した機器の証明
  例：医療機器、法定計量の対象となる機器
- 機器の製造環境もしくは機器の製造や流通に関わる組織が特定の要件に適合していることの証明
  例：認定製造工場、認定サプライチェーン

上記の対象には組織の存在証明以上の意味を持つものもあり、また、それぞれの機器に対する識別が要求される場合もありえる。eシールとしてどのような範疇を対象とするべきか今後検討が必要となる。

また、上記以外にアプリケーション等へのコード署名が考えられるが、コード署名は開発や配布元となる組織等が署名を行うものであり、署名鍵は開発や配布元となる組織によって管理されるものとなる。したがって、7.4節の組織内運用のケースと同様の運用形態になるものと考えられる。機器自身はコード署名の検証を行うものの、署名鍵は管理しないため、本7.6節の対象外としている。

8. eシールを実用化するための課題

8.1 本章の概要

5章にて解説の通り、eシールを広義でとらえた場合、その利用目的や利用形態は様々である。eシールに関する相互運用性を確保するために、eシール署名鍵やeシール用証明書のフォーマットや運用方法等の様々な課題を検討する必要がある。
なお1章で記載のとおり「eシールに係る指針 」を参考にしながらeシールに関する様々な事項について幅広く検討し、課題や対応策を挙げている。

本章では以下の課題について記述している。

- eシールの保証レベルの考え方(8.2節)
- eシール用証明書の発行(8.3節)
  組織や代表者の確認方法、証明書の記載事項、発行方法、受け渡し方法など認証局に関係する事項が主となる。

- eシール署名鍵の管理(8.4節)
  署名鍵の生成、管理における留意点、証明書の失効と署名鍵の廃棄など認証局やeシール発行対象の組織、リモートeシールサービスに関連する事項となる。
- eシールの国際相互承認(8.5節)
  eシールの国際的な相互承認に向けた制度設計に関連する事項となる。
- eシールの実用化に向けた制度等の全般に関わる課題(8.6節)
  基盤となる組織識別子や登記情報などに関連する課題、eシール普及促進のための制度設計などの全般に関連する事項となる。

8.2 eシールの保証レベルの考え方

eシール署名鍵の生成や管理方法、eシール用証明書の発行方法の違いにより、セキュリティの厳格さも異なる。この厳格さのレベルをここではeシールの保証レベルと呼ぶ。保証レベルが高いほど担保されるセキュリティのレベルは高い一方で、運用コストや導入コストもより高くなる傾向にある。例えば、高額取引も想定されるトランザクションや重要施設/設備から発せられる重要度の高いデータなどのように、適用先のユースケースの重要度により保証レベルの高いeシールが要求されることも考えられる。

EUではeIDAS規則に基づき厳格な適格(Qualified)レベルと、その他の非適格(Non-Qualified)レベルに区分されており、適格eシールの要件は、適格電子署名と同様に署名フォーマット(AdES)、適格電子証明書(QC)、適格署名生成装置(QSCD)の3要素から成り立っている(図8-1)。

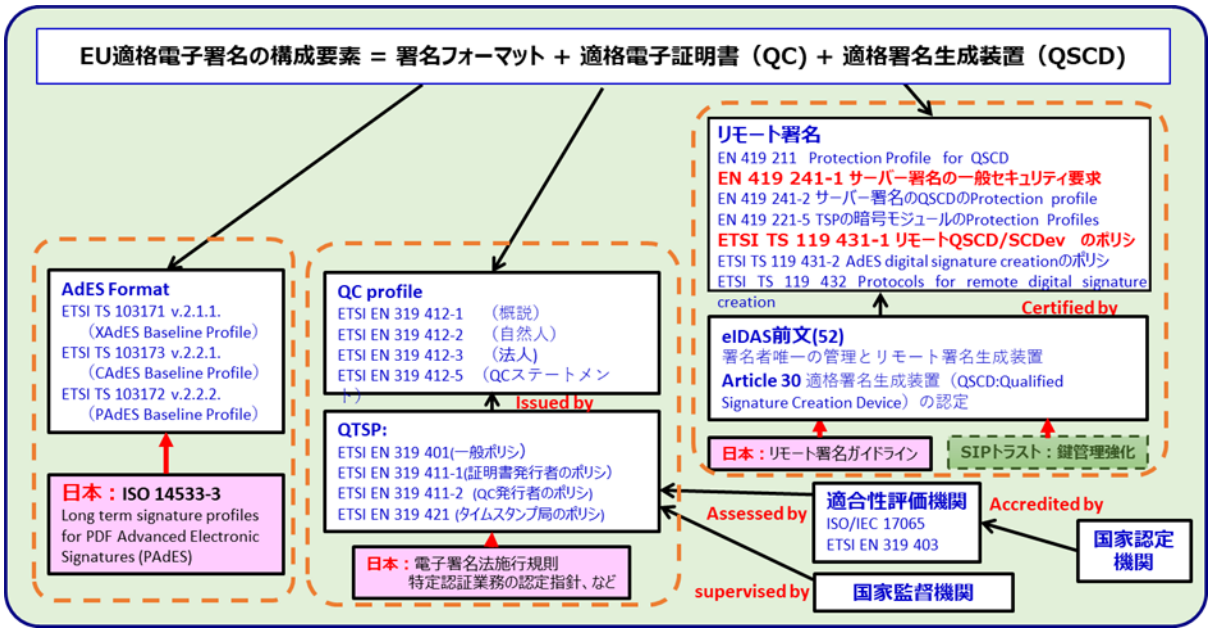

図8-1日欧電子署名関連技術基準

日本におけるeシールの保証レベルを議論する場合、要求レベルの異なる様々な業界やより幅広いユースケースへ対応を想定した基準作りを目指すことが望ましい。特に、eシール用

証明書の基準作成に関しては、組織の確認レベルや認証局の技術・運用レベルを定めることが求められる。

表8-1で本書におけるeシールの保証レベルの考え方を示す。

表8-1　eシールの保証レベルの考え方

	レベル1	レベル2	レベル3
レベル概要	発行元証明に必要とされる最低限の組織確認が行われるレベル。	国並びに国に準ずる機関又は中立・公正な機関が作成した基準に基づく適合性評価を受けたレベル。 日本国内において幅広く利用される。	国際相互承認の対象となる適合性評価を受けたレベル。 厳格な組織確認を必要とする。

eシールにおいては下記の観点に対して、それぞれの技術的対策や運用方法についてレベルの差異が存在しうる。

- eシール用証明書発行対象(法人・組織等)の確認方法
  認証局がeシール用証明書を発行する際に行う、発行対象の存在確認や発行対象に関わる属性等の確認に用いられる方法。
- 認証局の運用方法
  認証局を運用するための体制や手続き、安全対策等。
- eシール署名鍵の生成・管理方法
  eシール署名鍵の生成装置や生成時の運用方法や、eシール用証明書発行対象である法人・組織等によるeシール署名鍵の管理方法。

また、リモートeシールサービスの保証レベルにおいては以下の観点が含まれる。

- リモートeシールサービスの運用方法
- リモートeシールサービスに関わるeシール署名鍵の生成方法・管理方法
- eシール生成要求に関わるユーザーの認証・認可方法

8.3 eシール用証明書の発行に関する課題と対応案

8.3.1 本節について

8.3節では、eシール用証明書の発行時における発行対象の確認方法や、証明書の記載事項、証明書の受け渡し方法に関する課題と対応案を整理する。発行対象の確認方法については8.2節で述べたレベル差異を想定した案を示している。なお、7.4節では発行対象あるいは発行対象に関連した属性についていくつかのバリエーションを例示しているが、8.3節で述べる

発行対象の確認方法と証明書の記載事項は「法人/組織」に焦点を当てている。特に、システムやアプリケーション等については検討対象の中心から除外している。個別の機器を識別して発行されるデバイス証明書との相違も含め今後の検討課題がある。

8.3.2 組織や代表者等の確認方法

ここでは、登記等での扱いと同様に、会社や法人を代表する者を代表者と呼ぶ。実務においては、代表者から権限委譲された者がその権限の範囲で業務を行うことが考えられる。代表者や代表者から委任を受けた者を含めて、本書では代表者等と呼ぶ。
認証局が組織の実在性や代表者のeシール証明書発行申請の意思を確認したうえで、eシール用証明書を発行する。組織や代表者等に関する確認事項として以下の観点で整理を行っている。

- 法的実在確認
  法令に従った登記情報等に当該組織が存在することを確認する。
- 物理的実在確認
  組織の所在を確認する。
- 組織の運営確認
  組織の運営状態を確認する。
- 組織代表者の申請意思確認
  代表者等に対して、eシール用証明書発行申請の意思や内容に関する確認を行う。

これらの確認内容や方法には、厳密さに応じてレベルに違いがあるものと考えられる。表8-2は組織の確認レベルの案を示している。なお、官公庁に関する確認事項については今後の課題とする。

表8-2　組織確認のレベル案

	組織確認レベル１	**組織確認レベル２**	**組織確認レベル3**
対象例	レベル2の対象に加え ・登記されていない組織(任意団体、管理組合など) ・個人事業主	レベル3の対象に加え ・開業届を確認できる個人事業主 ・適格請求書発行事業者登録番号を確認できる事業者	・法人番号を確認できる組織
法的実在確認	－	商業登記されていることを確認[7] ＜確認事項＞ 以下のいずれかの方法によるものとする。 1) 組織の商業登記簿謄本(もしくは抄本)の提出を求める方法、もしくは民間企業概要データベース(商業登記簿を確認しているものに限る)を参照する方	

[7] 参考：「CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates」の「11.2. Verification of Applicant’s Legal Existence and Identity」

		法 2) 法人の代表者の電子署名の有効性を検証する方法(商業登記法第12条の2第1項、同第3項の規定で証明されるものに限定) 3) 組織属性を格納した証明書による電子署名の有効性を検証する方法(電子署名法第4条に基づく認定認証事業者の発行に限定) レベル2で個人事業主の場合は以下全てを確認 1) 利用申込書等に屋号を記載のうえ、当該個人事業主の実印を押印し印鑑登録証明書を添付 2) 利用申込書等に記載の屋号と開業届の屋号を確認 3) 適格請求書発行事業者登録番号を保持している場合は当該番号を利用申込書に記載し、国税庁適格請求書発行事業者公表サイトで確認	
物理的実在確認	―	申請された住所が登記簿やQIISで確認できる住所であることを確認[8]。 QIIS：CA/Browser Forumで用語定義されている認定された独立した組織情報ソース(例.帝国データバンク、東京商工リサーチ)。	
組織の運営確認	―	設立から3年以上経過しているか、QIISに登録があるかの確認[9]。 又は弁護士意見書などを確認。 ＜個別実施事項＞ A. 法人番号を証明書に格納する際には、「証明書に格納された属性情報の信頼性と利用に関するガイドライン[10]」の認証方法に基づく。 B. 英文商号は、定款に記載がある場合は提出を求める(定めがない場合自己申告に基づく) C. QIIS(商業登記簿を確認しているものに限る)を参照して当該民間企業が管理する企業コードを証明書に格納する場合は、オンラインで企業コードを確認する。	
組織代表者の申請意思確認	レベル2に準じた方法を採用する。 求められるレベルに基づき、例えば、以下のような方法が考えられ	以下のいずれかの方法によるものとする。 1) 書類申請 代表者印が押印された発行申請書、および印鑑証	レベル2に加え、厳密な身元確認を求める。詳細は、以下の＜A＞＜B＞＜C＞を全て実施する。 ＜A＞

[8] 参考：「CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates」の「11.4. Verification of Applicant’s Physical Existence」

[9] 参考：「CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates」の「11.6. Verification of Applicant’s Operational Existence」

[10] 電子認証局会議「証明書に格納された属性情報の信頼性と利用に関するガイドライン」 http://www.c-a-c.jp/download/guideline.html

	る。 ・「在職証明」の提出 ・民間企業概要データベース(商業登記簿を確認しているものに限る)を参照した法人電話番号への電話による代表者の在職確認 ・電話帳、電話会社発行の請求書などで確認できる電話番号	明書の提出が必要 個人事業主の場合は利用申込書等に屋号を記載のうえ、当該個人事業主の実印を押印し、開業届および印鑑登録証明書を添付 2) 電子申請(その1) 法人代表者の電子署名(商業登記法第12条の2第1項及び第3項の規定により証明されるものに限る)の付与が必要 3) 電子申請(その2) 法人代表者から委任を受けた者の電子署名(電子委任状の普及の促進に関する法律第5条第1項の認定を受けた電子委任状取扱事業者が発行したもので署名検証できるものに限る)の付与が必要(電子委任状が電子署名法の認定認証業務以外の場合は委任を受けた者の本人性を確認するため、別途住民票の提出を求める) 4) 電子申請(その3) 法人の代表者の電子署名(電子委任状の普及の促進に関する法律第５条第１項の認定を受けた電子委任状取扱事業者が発行したもので、代表者であることの確認、および署名検証できるものに限る)の付与が必要 5) 代表者のマイナンバーカードに格納された署名用証明書による電子署名(「第三者機関が管理するデータベース(商業登記情報等の公的な機関が管理する情報と照合されたものに限る。)に登録されている代表者の住所の一致の確認」が必要)	いずれかの方法によるものとする。 1) 書類申請 代表者印が押印された発行申請書、および印鑑証明書の提出が必要 2) 電子申請(その1) 法人の代表者の電子署名(商業登記法第12条の2第1項及び第3項の規定により証明されるものに限る)の付与が必要 3) 電子申請(その2) 法人代表者から委任を受けた者の電子署名(電子委任状の普及の促進に関する法律第5条第1項の認定を受けた電子委任状取扱事業者が発行したもので検証できるものに限る)の付与が必要(電子委任状が電子署名法の認定認証業務以外の場合は委任を受けた者の本人性を確認するため、別途住民票の提出を求める) 4) 電子申請(その3) 法人の代表者の電子署名(電子委任状の普及の促進に関する法律第5条第1項の認定を受けた電子委任状取扱事業者が発行したもので、代表者であることの確認、および署名検証できるものに限る)の付与が必要 ＜B＞

			必要書類[11](写し)の提出を求める ＜C＞ 代表者等の写真付き身分証明書[12]を持参のうえ、対面(もしくはビデオによる対面)による認証を実施し、認証結果を保存する。 または第三者検証者(弁護士など)による身元確認を実施し確認結果書類(第三者検証者の署名を求める)を保存する。

組織の下で構成される部門や事業所、組織が扱うサービスやシステムの名称など、組織に紐づいてeシール用証明書に記載されうる事項をここでは組織の内部属性と呼ぶことにする。特に保証レベル2や3に関するeシール用証明書に対して、組織の内部属性を記載する場合には、その属性情報に関する確認方法も併せて定めておくことが求められる。表8-3では組織の内部属性に関する確認レベルの案を示している。

表8-3 組織の内部属性に関する確認レベル案

	組織属性確認 レベル1	組織属性確認 レベル2	組織属性確認 レベル3
組織の内部属性 ・部門	規定なし	組織の代表者の宣言	組織の代表者の宣言 ※今後の国際的な議

[11] 【要件】2点必要とし、最低でもAグループから1つが必要。写しの全てにおいて代表者等の本人氏名が確認できること、2点のうちいずれかで住所の確認ができるもの。
【Aグループ】
- 有効期限の記載がある有効期限内のクレジットカード(または同カードの明細書)
- 有効期限記載がある有効期限内の金融機関発行のデビットカード(または同カードの明細書)
- 6ヶ月以内に発行された、認識可能な貸し手からの住宅ローンの明細書
- 規制金融機関発行の銀行の明細書

【Bグループ】
- 直近(6ヶ月以内)公共料金請求書、公益事業会社からの証明書(携帯電話請求書は除く)
- 6ヶ月以内に発行されたリース料支払の明細書
- 6ヶ月以内に発行された出生証明書(日本国内の場合は戸籍謄本もしくは戸籍抄本)
- 直近の課税年度の地方自治体税請求書
- 過去6ヶ月以内に認定された離婚証明書、無効通知書、養子縁組通知書など裁判所発行証明書

[12] 例として以下が挙げられる。
- パスポート
- 運転免許証
- マイナンバーカード

・事業所 ・サービス ・システム等			論の動向をみて再検討する可能性がある

組織や代表者等の確認に関して、以下の課題について留意が必要である。

- 身元確認に関する他の要件との整合性
  現状ではeシールに関連する法制度上の要件は存在しないが、eシールの想定されるユースケースを考慮し、電子署名法や犯罪収益移転防止法、eIDAS等の海外の法規制で定められた身元確認要件との整合性も視野に入れて検討が必要になる可能性がある。
- 登記簿上に記載されていない組織の確認方法
  商業登記等の登記簿など信頼できる情報源に登録されている組織であれば、それらを元に組織の実在性を確認することができるが、それ以外の組織については、別の情報源に基づいて組織の実在性を確認する必要がある。また、個人事業主の屋号をeシール用証明書の対象として扱うべきか、あるいは、電子署名として分類すべきかについては別途議論を要する。
- 組織内の部署、サービス、デバイスなど組織内で管理される対象
  eシール用証明書のユースケースによっては、組織だけでなく組織内の部署や組織が運営するサービスやシステム、デバイスなどを証明書に記載して識別したいケースも考えられる。組織内で管理される部署やサービスやシステム等は登記簿等の外部の信頼できる情報源に登録されるものではないため、組織から認証局へ申告された情報に依るところが大きい。表8-2にあるように組織代表者にeシール用証明書発行のための申請意思の確認を行う場合には、証明書発行対象となる部署等がその証明書によるeシール生成のために必要な権限を有していることの確認が含まれることも考えられる。認証局が確認を行う対象や範囲、確認方法についてはCP/CPSにより明確化する必要がある。
- 組織の内部属性に関わる制限
  他の組織の名称や商標などの権利を侵害するものや、eシールの利用者に誤解を与える情報を組織の内部属性として記述することは避けなければならない。組織の内部属性に対する禁止や制限などの規則について検討する必要がある。

8.3.3 証明書の記載事項に関する論点

8.3.3.1 eシール用証明書のプロファイル要求事項案

eシール用証明書の確認レベルに応じて記載事項が異なることに注意する必要がある。この節では表8-2の組織確認レベルのうちレベル2とレベル３を想定し、組織に発行するeシール用証明書のプロファイルの要求事項の案を示している。表8-3から表8-6において、証明書の各項目に関する要件を定めている。

表8-3 eシール用証明書プロファイルの要求事項の案

領域名	要求レベル	値	説明
version バージョン番号	必須	値は以下に制限する。 2 (v3)	バージョン3であることを示す
serialNumber シリアル番号	必須	(例) “12ab3456789ef13”	発行時に割り当てる。値はRFC 5280の要件に従う。
signature 署名アルゴリズム	必須	アルゴリズムの選択は電子政府推奨暗号リスト(CRYPTREC暗号リスト)に従う。 https://www.cryptrec.go.jp/list.html (例) 1.2.840.113549.1.1.11 SHA256withRSA	
issuer 発行者名	表8-5 を参照		
validity 証明書有効期間	必須		
notBefore 発行日		値の選択については右記の説明を参照のこと。値は以下の形式となる。 yymmddhhmmssZ	2049年まではUTCTimeで記述
notAfter 終了日		値の選択については右記の説明を参照のこと。値は以下の形式となる。 yymmddhhmmssZ	2049年まではUTCTimeで記述
subject 主体者名	表8-5 を 参照		
subjectPublicKeyInfo 主体者公開鍵情報	必須	アルゴリズムの選択は電子政府推奨暗号リスト(CRYPTREC暗号リスト)に従う https://www.cryptrec.go.jp/list.html	
algorithm 鍵アルゴリズム		(例) 1.2.840.113549.1.1.1 rsaEncryption	
subjectPublicKey 公開鍵		(例) “0382010f3082010a02...”	
issuerUniqueID	禁止		
subjectUniqueID	禁止		
Extensions 拡張領域	表8-4を参照		

表8-4 Extensions(拡張領域)の要求事項の案

Extensions 拡張領域	Critical フラグ	要求 レベル	値	説明

AuthorityKey Identifier 発行者鍵識別子	FALSE	必須	authorityCertIssuer, authorityCertSerialNumberは使用しない	
keyIdentifier			(例) “14c3ef1234567890abcdef9876543210a1cdef17”	RFC 5280に従う
SubjectKey Identifier 主体者鍵識別子	FALSE	必須		
keyIdentifier			(例) “abcdef1234567890abcdef9876543210abcdef12”	RFC 5280に従う
KeyUsage 鍵使用目的	TRUE	必須	値として取り得るフラグの組合せについては表8-6の設定例を参照。 ・nonRepudiation(否認防止) ・digitalSignature(デジタル署名) ・keyEncipherment(RSA鍵の場合に鍵暗号化)もしくはkeyAgreement(EC鍵の場合に鍵交換)	
certificatePolicies 証明書ポリシー	TRUE	必須		PolicyInformationは複数記載可
policy Identifier ポリシー識別子		必須	(例) Qualified Certificates for Electronic Seals (Legal Persons) 欧州適格eシール証明書(発行対象は法人) 0.4.0.194112.1.3	※EUでは電子署名/eシール1/QSCDの有無で証明書ポリシーオブジェクト識別子(OID) 0.4.0.194112.1.xxx が規定されており、日本においても同様な規定の検討が必要
poclicy Qualifier Info[0]		任意	id-qt-unotice (例) explicitText = “for eSeal”	explicitTextフィールドのみをテキストで記載可能
policy Qualifier Info[1]		任意	id-qt-cps (例) https://example.xx.jp/repository/	CP/CPS文書を公開しているURIを記載
SubjectAltName 主体者別名		任意	表8-5 を参照	
IssuerAltName 発行者別名		任意	表8-5 を参照	
CRLDistribution Points CRL配布点	FALSE	必須		
distribution Point			(例) https://rep.example.xx.jp/CRL1.crl ldap://example.xx.jp/ou=XXX%20CA%20 eSeal,o= XXX%5c%2cLTD.,c=JP?cRL	fullNameをURIにて記述

Basic Constraints 基本制約	FALSE	必須		
cA		必須	FALSE	
QCStatements QCステートメント	FALSE	必須	※日本における組織確認レベル2、3の詳細が検討される際に併せて記載事項も設定されるべき。 ※QC Statementの詳細は付録A.1を参照	
Authority InfoAccess		推奨		機関情報アクセス
Access Method		任意	id-ad-ocsp 1.3.6.1.5.5.7.48.1	オンライン証明書状態プロトコルOCSP
Alternative Name			(例) http://ocsp.example.xx.jp	
Acess Method		推奨	id-ad-caIssuers 1.3.6.1.5.5.7.48.2	eシール証明書を発行する認証局証明書
Alternative Name			(例) https://repository.example.xx.jp/ica.crt	証明書DERもしくはP8B形式で公開
LEI 取引主体識別子	FALSE	任意	LEI(Legal Entity Identifier)とは金融商品の取引を行う組織の国際的な識別子である。 (例) 123456XX1X23456XX123	LEI拡張の詳細は「付録A.3 LEI拡張について」を参照。

表8-5 識別名に関する要求事項の案

領域名	要求レベル	属性	値の例	説明
issuer 発行者名 (必須)	必須	C	JP	PrintableStringを使用
	任意	ST	Tokyo	・UTF8StringまたはPrintableStringを使用 ・organizationIdentifierに格納される値は8.6の「組織等の識別子や表記に関する課題」を参照のこと ・左記属性タイプ以外の格納も可能とする(任意)
	任意	L	Chiyoda-ku	
	必須	O	xxx,LTD.	
	必須	CN	xxxCA for eSeal	
	任意	OU	xxxCA	

	任意	organizationIdentifier	NTRJP-987654321098	
subject 主体者名 (必須)	必須	C	JP	PrintableStringで記述
	任意	ST (※2)	Tokyo	・UTF8StringまたはPrintableStringを使用 ・organizationIdentifierの例示は会社法人等番号を記載 ・organizationIdentifierに格納される値は8.6の「組織等の識別子や表記に関する課題」を参照のこと ・左記属性タイプ以外の格納も可能とする(任意) ・主体者の名称、住所はシステムや国際的な相互運用性の観点から英名、半角英数字記号を使用する。和名はsubjectAltNameに記載する。
	任意	L (※2)	Shinjuku-ku	
	必須	O (※1)	YYYYYY, LTD.	
	必須	CN (※1)	YYY	
	任意	OU	ZZ Division	
	必須	organizationIdentifier	NTRJP-1234567890123	
issuer AltName 発行者別名 (任意)	任意	C	JP	
	任意	ST	東京都	・UTF8StringまたはPrintableStringを使用 ・organizationIdentifierを複数格納する場合はissuerAltNameに格納(格納される値は8.6の「組織等の識別子や表記に関する課題」を参照のこと) ・左記属性タイプ以外の格納も可能とする(任意)
	任意	L	千代田区	
	任意	O	ＸＸＸ株式会社	
	任意	CN	ＸＸＸ認証局 for eSeal	
	任意	OU	ＸＸＸ認証局	
	任意	organizationIdentifier	T1:JP-111111111	
subject AltName 主体者別名 (任意)	任意	C	JP	
	任意	ST	東京都	・UTF8StringまたはPrintableStringを使用 ・organizationIdentifierを複数格納する場合は、subjectAltNameに格納(格納される値は8.6の「組織等の識別子や表記に関する課題」を参照のこと ・左記属性タイプ以外の格納も可能とする(任意)
	任意	L	新宿区	
	任意	O	ＹＹＹＹＹＹ株式会社	

	任意	CN	ＹＹＹ	
	任意	OU	ZZ事業部	
	任意	organization Identifier	T1:JP-999999999	

「ETSI EN 319 412-2 V2.2.1 (2020-07), Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons」の「4.3.2 Key usage」では鍵使用目的(KeyUsage)の設定値について説明している。表8-6は同プロファイルで規定している鍵使用目的拡張の設定例のバリエーションを示している。鍵の混在使用を避けるため、タイプA、C、Eのいずれかの型を使用することが望ましい。また、署名済みコンテンツへのコミットメント(否認防止)を検証するために使用する証明書は、タイプ A、B、またはFに限定することが考えられる。下記の注意事項2に示すように、場合によってはタイプAを使用する必要もある。

表8-6：鍵使用目的(KeyUsage)拡張の設定例

型	Non-Repudiation	Digital Signature	Key Encipherment or Key Agreement
A	X(注)		
B	X	X	
C		X	
D		X	X
E			X
F	X	X	X

(注) 証明書検証の実装によってはNon-Repudiationのみの証明書では検証時にエラーとなる場合があり、相互運用性の問題が生じうることも考慮する必要がある。

今後、実際のプロファイル検討を行う場合には、利用目的に応じてさらに以下について考慮することが求められる。

- 組織名のO、CNの英名記載について(※1)
  主体者識別名(subject)のO、CNフィールドにおいて、国際相互運用性、システム相互運用性の観点から組織英名を記載するとしているが、国税庁の法人番号検索では組織名、法人名の和名しか記載がなく、英名については民間の企業データベースや

定款などを確認することとなり、組織英名の正式なデータベースが存在せず、登記で組織和名しか登録していない場合には問題となる。
また、認証局によってはCNに略称(接頭辞や登記された英名からInc. Co,.Ltd.などを除いた物)を記載するケースがある。略称が公式または正式なものであるという判断基準が必要となる。

- 組織の所在地のST、Lの記載について (※2)
  日本における組織の証明書の主体者組織名(subject)ではST(stateOrProvince)では都道府県、L(locality)では市区町村名を記載するのが一般的である。ここで、Lに市までしか記載しないのか、市区まで記載するのか(例 横浜市神奈川区)ガイドライン等で規定する必要がある。また、市区町村名において正式な読み仮名のデータベースが無いために、ローマ字で記載する場合でも揺らぎが発生する恐れがある。
- 他の証明書との識別
  商業登記証明書に限らず、一般の認証局が発行する証明書には従来から組織名称が記載された組織代表者向けのものが存在する。これらの証明書は自然人である組織代表者を対象とした電子署名用途であり、eシール用証明書との混同や誤用を防ぐ必要がある。また、サービスやシステム、デバイス等をeシール用証明書の対象とした場合、サービスやシステム、デバイス等を対象とした認証(authentication)用途の証明書は従来からも使用されており、これらの証明書との誤用を防ぐことも求められる。証明書の相違についてはCP/CPSにより人が判断することはできうるが、検証プログラムによる自動化処理などを想定した場合、証明書プロファイルなどデータ上で識別可能であることが望ましい。8.3.2.2節で、より詳細な論点を整理している。
- 証明書記載事項(例 メールアドレス)に関する制限等
  CAブラウザフォーラムでは、S/MIME Baseline Requirementsにおいて、パブリックなS/MIME用の証明書について厳しい制限事項を課すことを検討している(本書執筆時点)。このような動向を考慮すれば、S/MIMEではないeシール用証明書の利用目的においては、emailAddress(E=)属性タイプの記載を禁止する、または、S/MIMEの目的では使用できなくすることが求められる。また、eシール用証明書へのメールアドレスの記載において、メールアドレスについても認証局の審査が必要となるため、8.3.2節で述べた組織の内部属性の審査方法と共に検討が必要となる。以上の理由から本書の証明書プロファイル案ではemailAddress(E=)を識別名に記載しないこととした。
- 組織内の部署、サービス、デバイスなどの情報の記載方法
- リモートeシールサービスを通じて発出したeシールと各組織が直接生成したeシールの識別方法

8.3.3.2 証明書の記載事項を検討する際の留意点

5章や8.3.3.1節で述べたように、eシールという言葉が登場する以前より、組織を対象とした証明書は活用されていた。以下はその用途の例である。

- 組織が発行する電子文書に対する署名
- 組織が配布するプログラムのコード署名

- 組織が提供するデータに対する署名(設計データ、記録データ、提出データ)
- 組織が発行する広報やお知らせ等のメールへの署名
- 組織が共用する利用者認証/ログイン認証に使われる証明書

8.3.3.1節ではeシール用証明書のプロファイル例が示されているが、これはあくまでも具体的に示した一例である。eシール用証明書としての共通的なプロファイル要件は

- 検証された組織名の記載
- これに加えオプションとして検証された組織に関する属性の記載

である。さらに、eシール用証明書の用途に応じて、その用途に基づく要件により複合的にプロファイル要件が追加される。

6章で述べたようなユースケースの観点に加え、eシールが利用(検証)される環境等についても考慮する必要がある。例えば、以下のような観点がある(これらの観点の中には相互に関係するものもある)。

- Microsoft、Apple、Chrome、Mozilla、Adobe等のルートプログラムに搭載されたパブリックなルートCAが要求されるかどうか
- パブリック/プライベートなドキュメント用途か
- パブリック/プライベートなPDF署名用途かどうか、さらに、パブリックなAdobeのプログラム(AATL)に準拠するPDF署名用途かどうか
- パブリック/プライベートなクライアント認証用途に使用するか
- パブリックなS/MIMEメール用途に使用するか
- CAブラウザフォーラムの各種ガイドラインに従う必要があるか
- Qualified Certificateプロファイルに従う適格証明書かどうか
- 日本の認定認証局または同等のeシール用CAの認定制度に準拠する必要があるかどうか
- eIDAS適格eシール用証明書かどうか
- CRYPTREC暗号リストへの準拠性が必要かどうか
- WebTrust認定をする必要があるかどうか

なお、CAブラウザフォーラムのガイドラインでは、エンドエンティティの証明書だけでなく、ルートCA、中間CAの証明書にも様々な要件が課せられているので、上記のプロファイル要件を考慮してプロファイルの設計を行う必要がある。

CAブラウザフォーラムのガイドラインに準拠したパブリックCAの場合、eシール用証明書で用いられる組織名や組織に紐付く属性情報は、認証局が申請者組織の登記情報等の情報を検証、審査して発行することとなり、証拠が示せず検証できない属性情報は証明書に記載することができない。また、証明書に記載する組織の名称や、組織に紐づく属性情報の確認方法は、現在(2022年6月時点)ドラフトとなっているCAブラウザフォーラムの

Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates が参考になる。
https://github.com/cabforum/smime/blob/preSBR/SBR.md

8.3.3.3 QCStatementsの運用方法について

現在、我が国の電子署名法の認定認証業務から発行される証明書は、証明書プロファイル上は認定以外のものと区別できる項目は無く、官報に公開される認定認証業務を実施する認証局の証明書のハッシュ値により、認定外の証明書と区別している。しかしながら、本来、証明書プロファイル上で区別することができれば、証明書利用者にとってより使い勝手が良くなると考えられる。RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profileでは、そのような認定制度に基づく適格証明書(Qualified Certificate)の証明書プロファイルが定義されており、Qualified Certificate Statements(qcStatement)拡張の中で証明書が特定の法制度に基づき適格証明書として発行されることを発行者が表明することを可能としている。また、欧州の「ETSI EN 319 412-5 Electronic Signatures and Infrastructures(ESI); Certificate Profiles;Part 5: QCStatements」では、QCStatementについて下記などの記載事項が示されている。
・eIDAS規則に基づく適格証明書であることの表明
・秘密鍵が適格署名/シール生成装置(QSCD)に存在することの表明
・証明書が電子署名、eシール、またはWebサイト認証の目的の1つとして発行されることの表明
それらの技術規格を参考に、我が国の認定制度に基づいた適格証明書であることを示すQCStatementsの運用が望ましいと考えられる。国内の利用を想定し、適切なCStatementsの規定(拡張等)の検討を行う必要がある。
「付録A.1 QCStatements拡張の要素」において、欧州eIDASの適格証明書のQCStatements拡張の記載内容ついて詳説している。併せて参照されたい。

8.3.4 eシール用証明書等の受け渡し方法に関する論点

7章のシステム構成に応じて例示し、それぞれの課題や要検討項目、論点を示す。

- 組織内管理のケース
  組織代表者(もしくは組織代表者からの受任者)がeシール用証明書やeシール署名鍵を物理的に直接受領する場合は、認証局は本人限定受取郵便を利用するなど、身元確認を確実に行い、且つ第三者に渡ることを防止する。
  また、オンラインによる受け渡しを行う場合には、eシール用証明書やeシール署名鍵を配布するサーバー等のなりすまし対策と、対象組織以外の第三者によるeシール署名鍵の不正取得の防止策が必要となる。配布サーバーに対して適切なサーバー認証(TLS等)を実施し、対象組織の代表者や受任者に配布サーバーへのアクセスに必要な認証クレデンシャルを適切に配布することが求められる。また、より高度な運用方法として、組織内で運用されるeシール生成サーバーと外部の認証局がシステム上

で連携し、オペレーターを介さずにeシール用証明書やeシール署名鍵の配送を行うことも考えられる(特にeシール用証明書の更新など)。このような形態においても、eシール生成サーバーと認証局側のシステムの双方に適切な認証方法を実施することが求められる。

- リモートeシールサービスでeシール生成を実施する場合
  a. eシール署名鍵をリモートeシールサービスが生成する場合
     リモートeシールサービスは対象組織からの要求に応じてeシール署名鍵を生成する。eシール署名鍵の生成方法(乱数生成や鍵生成装置)には十分留意する必要がある。リモートeシールサービスはeシール署名鍵の生成後、外部にある認証局に証明書発行要求(CSR)を発行することとなる。認証局はCSRに基づき証明書を発行する。リモート署名サービスは受領した証明書がCSRに基づき正しく生成されているか確認することが望ましい。
  b. eシール署名鍵を認証局など信頼できる第三者機関が生成する場合
     認証局が生成するeシール署名鍵を、安全にリモートeシールサービスが受領する仕組みが必要となる。リモートeシールサービスは認証局から提供されたeシール署名鍵とeシール用証明書をその対象組織のみが使用できるように適切に受領し管理する仕組みを持つ必要がある。
  c. eシール署名鍵を対象組織が生成してリモートeシールサービスに配置する場合
     リモートeシールサービスは、対象組織が生成したeシール署名鍵を安全に受領する仕組みが必要となる。対象組織を適切に認証し、提供されたeシール署名鍵をその対象組織のみが使用できるように適切に管理することが必要となる。

  上記のパターンはリモートeシールサービスに関する保証レベルの違いにも関連しうる。
- 機器組込みのケース
  7.6節で例示したように機器組込みのケースは多種多様であり、ユースケースによりeシール署名鍵の生成やeシール用証明書の管理に関わる組織や構成、フロー等が異なる。ユースケースに応じて、その対象組織が適切に扱えるようにeシール署名鍵とeシール用証明書の管理方法を検討する必要がある。

8.4 eシール署名鍵の管理について

7章で例示したように、eシールの適用先となるアプリケーションやシステムの形態は様々であり、形態に応じてeシール署名鍵の生成、保管、廃棄などのライフサイクルや鍵管理方法が異なるものと考えられる。

8.4.1 eシール署名鍵生成

7章のシステム構成の分類に応じて、eシール署名鍵の生成に関する考え方や論点、課題を示す。

- 組織内管理のケース
  基本的に従来から運用されてきた電子署名用途の署名鍵生成の考え方に準じるものと考えられる。eシール署名鍵生成をeシール証明書発行対象組織側の環境(システムや媒体)で行うケースと、組織側の要求に基づき認証局側で安全にeシール署名鍵を生成し、その組織に安全に受け渡すケースが考えられる。認証局側でeシール署名鍵生成を行う場合には、当該組織以外の第三者がeシール署名鍵を不正利用できないように、eシール署名鍵の受け渡しを適切に実施することや、認証局側でeシール署名鍵生成後に適切に削除すること等が求められる。
  eシール署名鍵生成を行うプログラムやデバイス等の環境に関して、デバイスや鍵生成プログラムの仕様を確認し、安全な鍵を生成できるかを留意すべきである。8.2節の保証レベル(特にレベル2と3)に応じて、鍵生成を行う暗号モジュールに対する評価や認証(certification)[13]に対して一定の要件を定めることも考えられる。また、レベル3の国際相互承認を想定する場合には、欧州のQSCD相当の暗号モジュールを要件とすることも考えられる。

- リモートeシールサービス
  電子署名用途を想定したJT2Aリモート署名ガイドラインでは3つのレベルを規定しており、そのうちレベル2, レベル3はHSMによる署名鍵管理を求めており、署名生成を行う鍵認可のために署名者の複数要素認証を求めている。さらに、レベル3ではこの鍵認可のための認証処理(署名活性化モジュール)をHSMによって実装することを求めている。レベル3は主にEUの適格電子署名との将来的な相互認証を見据えた内容となっており、適格電子署名で求められるSCAL2に相当するものとなっている。このようにJT2Aリモート署名ガイドラインが定める各レベルの違いは、署名者による自分の署名鍵に対する署名者の単独管理の度合いを示しているとも言える。一方で、eシールの場合では、eシール署名生成を要求するのは組織内で権限を与えられたオペレーターや、管理者により管理されたシステムであり、オペレーターの指示によって生成されたeシールはその組織に属するものであることが分かればよいことが十分なケースが多く、厳格に自然人としての署名者単独管理を維持すべき電子署名とは求められる要件が異なることも考えられる。特に、組織側のシステムがリモートeシールサービスに接続するケース(7.5節の図7-4における承認システムのようなケース)は特徴的なものであり、その要件については留意すべきであろう。リモートeシールサービスについてもユースケースにより求められるサービスのレベルは異なるものと考えられ、8章の保証レベルに応じて適切な要件を検討する必要がある。

- 機器組込みのケース
  8.3.4節と同様に、ユースケースにより多種多様であり、ユースケースに応じて、eシール署名鍵とeシール用証明書の適切な管理方法を検討する必要がある。

[13] certificationとauthenticationの和訳として、同じ「認証」という単語が広く使われている。認証(certification)は、製品、サービス、システム、人員の技能等に対して、ある基準へ適合していることを第三者が評価し証明する仕組みを意味している。一方、認証(authentication)は、人やデバイスやサービス等の対象を確認する行為(その対象が主張する通りのものであることを検証する行為)を意味する。

8.4.2 eシール署名鍵管理における運用上の課題

8.4.2.1 eシール署名鍵管理の考え方

自然人を対象とした電子署名用途の署名鍵は、当該自然人自身のコントロール下において管理することが求められる。一方、eシール署名鍵は組織内のコントロール下で管理されることになり、複数の管理者やオペレーターが関与することも考えられる。管理者やオペレーターにより権限外の利用や複製、窃取、毀損や消滅が無いよう管理することが求められる。

8.4.2.2 eシール署名鍵の管理や利用について

ここでは組織内管理とリモート署名サービスによる管理のケースについて、eシール署名鍵の管理や利用についての基本的な考え方や論点、課題について述べる。機器組込み型についてはユースケースに応じてバリエーションが様々であり、想定したユースケースに応じて検討が必要であると考えられる。

- 組織内管理のケース
  電子署名用途の署名鍵では所有する当人の管理下に置くことが求められるが、eシール署名鍵では組織内で適切に管理することが求められる。組織内で管理者やオペレーターにどのような権限を与え、eシール署名鍵の管理や利用をどのように行うかは基本的に組織内での管理規定を定めることになる。組織構造やシステム構成等により、管理者やオペレーターがeシール署名鍵を扱うバリエーションも様々であると考えられるが、例として以下のようなものが考えられる。

  - ケース1：媒体管理型
    eシール用証明書に対応するeシール署名鍵が格納された媒体を用意し、複数のオペレーターで共有して使用する。組織内で権限を与えられたオペレーターのみがこの媒体が扱えるように適切なアクセスコントロールを実施する。また、利用時の記録を残し監査を行う。
  - ケース2：媒体管理型
    eシール用証明書に対応するeシール署名鍵が格納された媒体をオペレーター毎に用意する。eシール署名鍵の複製が認められない場合には、オペレーター毎に異なるeシール用証明書となりえる。各オペレーターが媒体を管理することが考えられ、適切に管理するための指導やシステム上での対策、管理者による定期的なチェックなどを実施することが考えられる。
  - ケース3：eシール生成サーバー/システム組込み型
    管理者がeシール生成サーバー等を操作しサーバー内でeシール署名鍵を生成する。または、信頼できる認証局への依頼や、外部の安全な署名鍵生成装置等により署名鍵を取得し、システム上に配置する。配置は管理者の人手を介さずにオンラインで自動的に配置する方法もある。eシール署名鍵の生成/配置を完了したのち、管理者がeシール生成サーバーやeシール署名鍵を格納したシステムを起動する。起動時には署名認可用クレデンシャル(eシール署名鍵を活性化するためのクレデンシャル。例えば、認証用の媒体やPINなど)を求めるように設計することもできる。管理者による不正や誤操作等を検知す

るために、操作ログの取得や監査を実施することが考えられる。
eシール生成サーバーやeシール署名鍵を格納したシステムへのeシール生成要求は、ユーザーインターフェースを通じたオペレーターによる操作や、別のシステムによる機械的な処理を通じて行われることが考えられる。システム設置環境に応じて、オペレーターや接続システムの認証を適切に行うことが求められる。

- リモートeシールサービスによる管理のケース
  オペレーターと署名認可用クレデンシャルと署名鍵(証明書)の関係は柔軟な対応が求められる可能性がある。表8-7に想定されるパターンを示し、備考として各パターンの特徴や論点を示す。

表8-7 署名認可クレデンシャルと署名鍵の対応関係の例

署名認可クレデンシャルの割り当て	署名鍵の割り当て方法	備考
複数のオペレーターがオペレーターごとに割り当てられた署名認可クレデンシャルを使用する	署名認可クレデンシャルに対して異なるeシール署名鍵(eシール用証明書)が1対1で紐づく。	リモート署名サービスと同様の署名鍵に対して署名者が単独管理する。リモート署名サービスは電子署名と同じメカニズムでリモートeシールサービスを提供できる。署名鍵生成・管理や証明書発行のコストは電子署名と大きく変わらない可能性もある。
	それぞれの署名認可クレデンシャルが共通の一つのeシール署名鍵(証明書)に紐づく。	リモートeシールサービスは、それぞれの署名認可クレデンシャルを使用するアカウント毎にアクセスログを記録する(これは一般的なリモート署名サービスが行っている事と同じ)。
複数のオペレーターが共通の署名認可クレデンシャルを使用する	署名認可クレデンシャルに一つのeシール署名鍵(証明書)が紐づく。	オペレーターが属する組織内で、署名認可クレデンシャルを適切にアクセスコントロールし、オペレーターの署名認可クレデンシャルの使用記録をとる。アクセスコントロールや使用記録の保持はオペレーターが属する組織のガバナンスに依る。

8.4.2.2 eシール用証明書の失効とeシール署名鍵の廃棄について

ここではeシール用証明書の失効とeシール署名鍵の廃棄に関する論点を整理する。

- 組織内管理のケース
  eシール署名鍵の使用を終了し廃棄するには、認証局に対して当該eシール用証明書の失効申請を行うと共に、廃棄後にeシール署名鍵を不正利用されないように適切な廃棄処理を行う必要がある。eシール署名鍵の廃棄方法としては物理的な破壊や論理的な完全消去がある。ICカードのような媒体に格納されている場合には、はさみ等で破砕し処分することが考えられるが、HSMなどの鍵管理装置の場合は、実装されている鍵消去機能を利用し、署名鍵データを完全消去する。それ以外の記憶媒体で物理的な破壊が難しい場合には、Gutmannなどの完全消去アルゴリズムを用いた方法で消去することも考えられる。
- リモートeシールサービスによる管理のケース
  上記と同様にeシール用証明書の失効とeシール署名鍵の廃棄を行うこととなる。eシール用証明書の失効、eシール署名鍵の廃棄に関わる告知を当該利用者に適切に行い、廃棄処理を確実に行うことが重要となる。
- 機器組込みのケース
  組織内管理やリモート署名サービスのケースとは異なり、機器の種類によってはオフライン環境下で運用される場合や、常時人手による操作を行うことは困難な環境にある場合もありえる。失効や廃棄だけでなく、署名鍵の更新を行うことを想定した場合には、機器の制約上アップデートが困難なケースもありえる。このような環境下で利用される機器に適用されるeシール用証明書やeシール署名鍵の運用方法は組織内管理のケースやリモート署名サービスのケースとは異なる考え方が求められる。ユースケースに応じて、有効期限や失効、鍵更新の考え方について検討することが求められる。

8.5 eシールの国際相互承認

8.5.1 本節について

8.5節では、eシールの国際的な相互承認の必要性と、そのために必要となる技術以外の観点も含めた課題の整理、その課題への取り組みに関する考え方を示している。本書の目的に従いeシールの課題として言及しているが、8.5節で述べているいずれの考え方や課題は、eシール以外のトラストサービス全般に共通するものである。

8.5.2 国際相互承認の必要性

- 国際社会での「信頼ある自由なデータ流通: Data Free Flow with Trust」の拡大

Society5.0の実現に向け、ヒト、モノ、システム間での高度な情報連携が進みAI含めデ

ータの自動連携が社会システムの基盤となり、デジタル経済を支える信頼ある自由なデータ流通(DFFT)が国際社会の中で拡大することが予想されている。

「デジタル社会の実現に向けた重点計画」(2022年6月18日閣議決定)[14]の「包括的データ戦略」では、DFFT 推進 に向けた国際連携の中で、「信頼性のある情報の自由かつ安全な流通の確保を図るため、データ流通に関連する国際的なルール作りや討議等を通じて、 DFFT を推進し続ける必要がある。」とされ「有志国による国際連携、貿易、プライバシー、セキュリティ、トラスト基盤、データ利活用、次世代データインフラといった 政策分野に応じて責任を 持ちつつ、連携して検討・遂行する。」と示されている。

● DFFTを支えるトラストサービスの国際相互承認の必要性

「包括的データ戦略」では、データのトラストの3要素「意思表示の証明(電子署名等)」、「 発行元証明(eシール等)」、「存在証明(タイムスタンプ等)」の国際的な相互承認の必要性について、「国際的な相互承認を得るにあたっては、トラストアンカーの確認、トラストアンカー間の接続の仕組み、 及び 技術基準の整合性の確保のみならず、監督・適合性評価のレベルや関連の国内制度の整合性も確認する必要性が想定される。このため、国内のトラストサービス認定のフレームワーク では、国際的な同等性等を配慮した国際相互承認を検討段階から 念頭に置くことが必要である。」と述べられている。

● 国連国際商取引法委員会(UNCITRAL)での電子商取引におけるID管理とトラストサービスに関するモデル法[15]

国際商取引の場面における障害となっている法的な不調和を調和させ、国際商取引を発展させることを目的として議論しているUNCITRALにて、①民間における電子取引においてID管理とトラストサービスについて基準を整理して効力があることとし、②法的には各国主権があることを前提に、ID管理とトラストサービスのモデル法が整理され、採択された(2022年7月)。モデル法では、電子取引の確からしさを判断する事後的要件と、それを推定可能とする事前信頼性指定が整理されている。

eシールは、トラストサービスのひとつとして、Article17に規定され、その議論背景情報として付録に6項目が記載されている。内容の解釈を間違わないよう、以下に原文を引用する。

> Article 17. Electronic seals

[14] https://www.digital.go.jp/policies/priority-policy-program/

[15] https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/acn9-1112-e.pdf

Where the law requires a legal person to affix a seal, or provides consequences for the absence of a seal, that requirement is met in relation to a data message if a method is used:

(a) To provide reliable assurance of the origin of the data message; and

(b) To detect any alteration to the data message after the time and date of affixation, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display.

5. Article 17. Electronic seals

189. Electronic seals provide assurance of the origin and integrity of a data message that originates from a legal person. In practice, they combine the function of a generic electronic signature with respect to origin, and that of certain types of signature, typically based on the use of cryptographic keys, with respect to integrity. The existence of such electronic signatures is reflected in 6(3)(d) MLES. Accordingly, the description of the integrity requirement contained in article 17 is based on article 6(3)(d) MLES.

190. Article 17 is inspired by regional legislation, according to which “In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers.” (eIDAS Regulation, recital 65).

191. The assurance of the origin of the data message may be achieved by establishing its provenance, which, in turn, requires identification of the legal person originating the data message. The method used for the identification of the legal person affixing the seal is the same used for identifying a signatory, and UNCITRAL provisions on electronic signatures have usually been enacted as applicable to both natural and legal persons.

192. Moreover, provisions contained in UNCITRAL texts require integrity to achieve functional equivalence of the paper-based notion of “original”. In particular, article 6(3)(d) MLES refers to the notion of “integrity” where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates.

193. In light of the above, it is possible that jurisdictions that have already enacted UNCITRAL provisions on electronic signatures that provide assurance as to integrity may not distinguish between the functions pursued with the use of an electronic signature and those pursued with the use of

an electronic seal. This may also reflect the business practice of using hybrid methods combining electronic signatures and electronic seals.

Integrity

194. Integrity is an essential component of electronic seals and of electronic archiving and may be an optional component of other trust services. In earlier UNCITRAL texts, integrity is a requirement to achieve functional equivalence with the paper-based notion of "original" (article 8 MLEC). Articles 17 and 19 are inspired by article 8(3) MLEC with respect to requirements for ensuring integrity.

8.5.3 国際相互承認のために必要な項目

- 内閣官房トラストに関するワーキンググループでの論点

内閣官房 IT総合戦略室　第１回トラストに関するワーキングチーム(2021年4月8日)の「資料7データのトラストの枠組み検討の主な論点」[16]ではトラストサービスの国際相互承認について、以下のように示されている。図8-2は認証局に関して米国と欧州の相互承認を行うイメージであり、同ワーキングチームの資料7からの引用である。

「国際間の利用者が相互に適格性を確認できるように、以下の項目の同等性などを検討し、相違点を補完する仕組みが必要ではないか。」とし、以下の観点を挙げている。

1. 法制度
2. 監督・適合性評価
3. 技術標準(可能な範囲で技術規格をそろえるが、必ずしも同一である必要はない)
4. トラストアンカーの確認、トラストアンカー間の接続の仕組み

[16] https://warp.ndl.go.jp/info:ndljp/pid/11740658/www.kantei.go.jp/jp/singi/it2/dgov/trust_wt/dai1/gijisidai.html

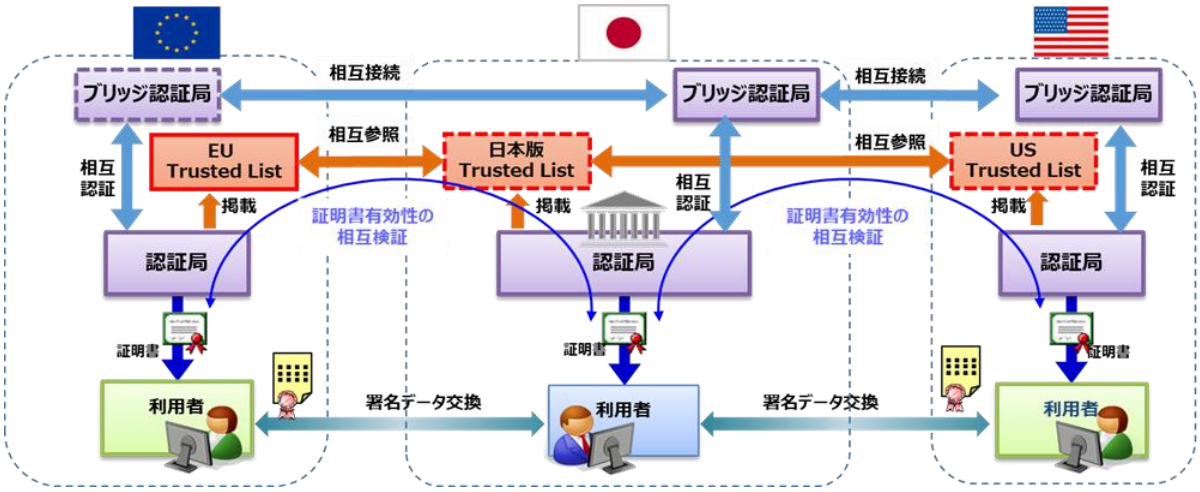

図8-2 トラストサービスの国際相互承認のイメージ

- 欧州eIDASにおける第三国との相互承認の考え方

  欧州eIDASでは、トラストサービスの第三国との相互承認についてArticle 14に記載されており、eIDAS2.0(プロポーザル)において以下の改訂案が示されている。

  1. 委員会は、第48条第(2)項に従って、その地域に設立されたトラストサービス事業者及びそれらが提供するトラストサービスに適用する条件と同等とみなすことができる第三国の要件を定め、その施行規則を制定することができる。

  2. 委員会が第1項に従って施行法を制定した場合、又はEU 運営条約(AEUV条約)第218条によりトラストサービスの相互承認に関する国際協定を締結した場合、第三国に設立された事業者が提供するトラストサービスは、連合で設立された適格トラストサービス事業者が提供する適格なトラストサービスと同等とみなす。

  即ち、EU以外のTSP/TS要件とeIDASとの間の同等性に関する条件を設定する必要があり、これは「法的効果」、「監督・監査制度」、「技術標準」、「トラストアンカーの開示」の 4つの柱(4 pillars)による同等性の確認が必要とされている(図8-3)。

2019 Trust Services Forum：Arno Fiedler（Vice-Chair ETSI ESI） 発表資料より

図8-3 eIDASに関して同等性が求められる4つの柱

8.5.4 国際的な相互運用への配慮

8.5節のこれまでの節で述べたトラストサービスの国際相互承認の観点以外にも、eシールのユースケースに応じて証明書の国際的な相互運用性を意識してプロファイルや運用方法を検討することが求められる(8.3.2.2節参照)。検討を行うためには、証明書に関わる国際的な標準化の動向についても注視する必要がある。例えば、Webサイト証明書に関する要件の策定・改訂を行ってきたCA/Browser Forumでは、コードサイニング証明書ワーキンググループ及びS/MIME証明書ワーキンググループが新たに創設され、各々の証明書について、証明書プロファイル(記載情報、鍵使用目的、証明書有効期間等)、鍵ペアの生成、鍵管理、証明書発行対象の認証手続き、証明書ステータス情報の提供、監査等々を含む要件の策定・改訂を行っている。このように様々な証明書に関する標準化が進められており、その議論の中には組織を対象とする証明書という観点でeシール用証明書とも関係するものもある。様々な証明書との運用を阻害しないためにも、国際的な動向を踏まえながら、eシール用証明書に関する検討を行う必要がある。

8.6 eシールの実用化に向けた制度等の全般に関わる課題

この節では、eシールの実用化と利用促進、ユースケースの拡大を図るために必要な環境や制度等に関連する課題を列挙している。

- 指針やガイドライン、認証制度等に関する課題
    - 保証レベルに応じて、証明書プロファイルの要件や認証局運用規程基準を作成することが望ましい。

- 保証レベルに対する具体的な要件は今後の検討課題であるが、一定の保証レベルについては適合性を評価する認証制度が必要である。また、認証制度では適合性評価機関に対する要件・基準も必要となる。
- eシールをより安全に容易に扱えるように、組織内でeシール署名鍵の管理やeシール生成などの管理や運用に関するガイドを作成することが望ましい。
- 機器組込みについては様々なユースケース、バリエーション、業界も多様であるため分野や業界の枠を超えて一般モデル化を行うことは難しい。業界横断型にeシールが活用されることが想定され、相互運用性の確保が重要となる分野については、ユースケースに応じて証明書プロファイルや運用方法、管理方法に関するガイドライン等を定めることが望ましい。

- 組織等の識別子や表記に関する課題
  - 組織の識別子として格納される番号体系として複数の候補が存在する。OrganizationIdetifier[17]に格納する際のプレフィクスを日本国内で統一的に決めることで、検証側で機械可読が実現できる。さらに、国際的な相互運用を考えた場合、他の国から簡単に参照可能であることが望ましい。
  - eシールの業界横断的な活用や国際的な相互運用を想定し、OrganizationIdentifierのプレフィックス管理は、国の基準として決めることが望ましい。(欧州eIDASにおけるOrganizationIdentifierのプレフィクスについては付録A.2 参照)
  - 国際的な利用においては、法人名の英語表記が必要となる。現状の登記制度では法人の英名は確認できない。eシールの検証者や検証処理を行うプログラムがeシール用証明書に記載されている英名表記の確認を行うことを考えた場合、登記等のベースレジストリに英文による名称や組織情報が登録され、それらの情報が参照可能であることが望ましい。
  - 個人事業主の屋号をeシール用証明書の記載対象として扱うべきか検討が必要である。

- 検証環境に関する課題
  - eシールを機械的に検証可能にするため、eシール用証明書に関するルート認証局等のトラストアンカーを確認できるための枠組み(トラステッドリスト)の整備が必要となる。eシールの検証可能性の維持や、保証レベルに応じた適切なeシールの利用といった観点においても重要である。
  - eシール生成と検証を行うリファレンス実装の整備を行うことで、eシールを活用したアプリケーションやシステムの開発をより促すことにつながる。

[17] CABFで議論されているS/MIMEのルールにも考慮が必要となる。(https://github.com/cabforum/smime/blob/preSBR/SBR.md 参照)

9. おわりに

本書ではPKIを用いたeシールを活用したアプリケーションやシステムを導入する際に求められる技術面と運用面における検討課題を整理し解説を行った。eシールには様々なユースケースが想定され、各組織が扱うeシール同士の相互運用性の確保だけでなく、eシールと従来の電子署名や非自然人向けの証明書による様々な用途との相互運用性の確保といった視点も重要となる。本書ではそのような視点に立ち、eシール用証明書プロファイルに関わる課題、法人の実在性確認も含めたeシール用証明書の発行に関わる課題、eシール用証明書の発行を受けた組織によるeシール署名鍵の管理における課題、eシール全般に関わる国際的な相互承認に向けた課題など多岐にわたる事項を俯瞰し、各課題に対する考え方の指針を示している。これらの課題や論点は、eシール用証明書を発行する認証局、eシールに対応したアプリケーションやシステム、リモートeシールサービス等の構築と運用に関する検討を行う上で参考になるものと考えられる。また、課題や論点の中には、業界の様々な関係者と共により詳細な考察を行い、解決策を検討することが必要なものもある。その検討結果を踏まえ、eシールの相互運用性を確保するための規格やガイドライン、そして、実装や運用を支援するガイドブック等の整備していくことは、eシールをより広範な用途での活用に広げ、円滑な導入を促すためにも重要であると考えられる。今後期待されるeシールに関わる様々な規格やガイドライン、ガイドブック等の策定においても、本書の挙げる課題や論点が検討の手引きとなれば幸いである。

付録A：EUにおけるeシール用証明書の記載項目に関する特記事項

A.1 QCStatements拡張の要素

8.3.3.1節「 eシール用証明書のプロファイル要求事項案」にてeシール用適格証明書には、「適格」であることを示すqcStatements拡張が含まれるとし、8.3.3.3節「QCStatementの運用方法について」qcStatements拡張について簡単に触れた。

本節では、EU eIDASの下で発行された適格証明書のqcStatementsにどのような情報が記載可能なのか補足解説する。

QCStatements拡張はRFC 3739で定義された拡張であり、欧州に限らず認定された一定の要件を満たせば、この拡張を含めることができる。ETSI EN 319 412-5 Part 5 QCStatements では欧州eIDASに基づき発行される証明書のQCStatements拡張の予約された要素の型を定めており、その一覧は以下の通りである。eIDASの適格証明書のQCStatementsでは下記の任意の型を含めることができるが、情報収集で得られた数社の欧州TSPの実際の適格証明書よりQCStatement型の利用頻度も記載しておいた。

表 A.1-1 eIDASで使用されるQCStatementsの要素の型の一覧

QCStatementの型	説明	頻度
1.3.6.1.5.5.7.11.2 pkixQCSynatax-v2	[RFC 3739 3.2.6.1] RFC 3739より新たに導入された要素の型(v2)であり、証明書識別名で使用される属性タイプの意味や要件をセマンティックIDとして指定できるようになった。指定可能な値は表 A.1-3に示す。 なお、RFC 3739ではv1とv2の双方が利用可能であるとしている。	中
0.4.0.1862.1.1 id-etsi-qcs-QcCompliance	[Part5 4.2.1] eIDAS規則に基づいて発行された適格証明書であることを示す。	必須
0.4.0.1862.1.2 id-etsi-qcs-QcEuLimitValue	[Part5 4.3.2] 署名等に基づく取引金額もしくは価値の上限を定める。通貨の種類、金額、指数などを指定できる。(価値=金額×10^指数)	極低
0.4.0.1862.1.3 id-etsi-qcs-QcRetentionPeriod	[Part5 4.3.3] 証明書の有効期間後、証明書の信頼情報が何年保管されるかを示す。	低

0.4.0.1862.1.4 id-etsi-qcs-QcSSCD	[Part5 4.2.2] 証明書に紐づく秘密鍵がEUの定める認定リストに記載されたHSM (QSCD) に格納されているかを示す。	中
0.4.0.1862.1.5 id-etsi-qcs-QcPDS	[Part5 4.3.4] 証明書のCP/CPSでは一般的利用者にはわかりにくいため、証明書発行に関する要点、重要周知事項を簡潔に説明する公開文書 PKI Disclosure Statements(PDS)の公開URLと記載言語(enやfr等)を示す。PDSの様式の例はETSI EN 319 411-1 Annex A で示している。	中
0.4.0.1862.1.6 id-etsi-qcs-QcType	[Part5 4.2.3] EU適格証明書の用途種類(署名用/eシール用/ウェブサーバー用)を示す。指定可能な値は表 A.1-2に示す。	高
0.4.0.1862.1.7 id-etsi-qcs-QcCClegislation	[Part5 4.2.4] どの国の規制で証明書が発行されたかを示す2文字国コード(ISO 3166-1 alpha2) (例 DE、ES)	低

EU適格証明書の種類を指定するためにQcTypeを使用することができる。その種類はOIDにより指定することができ、取り得る値は以下の通りである。

表 A.1-2 QcTypeの指定可能な値一覧

QcTypeの値	用途
0.4.0.1862.1.6.1　id-etsi-qct-esign	自然人による署名用証明書
0.4.0.1862.1.6.2　id-etsi-qct-eseal	法人によるeシール用証明書
0.4.0.1862.1.6.3　id-etsi-qct-web	サーバー用証明書

改訂されたRFC 3739より、QCStatementsの新しいシンタックスQCStatementSyntaxV2が導入され、QCStatementsの要素として、V2を使用していることの明示と、セマンティクスIDが導入され指定できるようになった。セマンティクスIDが導入される前は、証明書の識別名の属性タイプと値は、認証局のCP/CPSにより各社の解釈で設定していたが、識別名の取り扱い、意味の解釈を定め、認証局、利用者で共通に利用できるようにしたのがセマンティクスIDである。

QCStatementSyntaxV2の値として指定できるETSI EN 319 412-1で定められたセマンティクスIDは以下の通りである。

表 A.1-3 QCSyntax-v2で指定可能なセマンティクスIDの一覧

セマンティクスID	内容

0.4.0.194121.1.1 id-etsi-qcs-semanticsId-Natural	Semantics identifier for natural person [EN 319 412-1 5.1.2節] 自然人用のセマンティックIDであり、証明書のsubjectフィールド等に個人を特定するIDを属性タイプとして seiralNumber を用い、パスポート(PAS)、国民IDカード(IDC)等、予約された身元確認情報を定められたフォーマットで記載する。
0.4.0.194121.1.2 id-etsi-qcs semanticsId-Legal	Semantics identifier for legal person [EN 319 412-1 5.1.3節] 法人用のセマンティックIDであり、証明書のsubjectフィールド等に法人を特定するIDを属性タイプ として organizationIdentifier を用い、法人納税番号(VAT)、国で定めた商業登録番号(NTR)など、予約された組織確認情報を定められたフォーマットで記載する。
0.4.0.194121.1.3 id-etsi-qcs-semanticsId-eIDASNatural	Semantics identifier for eIDAS natural person [EN 319 412-1 5.1.3節] eIDASに基づく自然人用のセマンティックIDであり、識別名には上記 serialNumber の他に属性タイプとして以下を用いる。 ● surname 姓 (eIDASのFamilyName) ● givenName 名 (eIDASのFirstName) ● dateOfBirth 生年月日 (eIDASのDateOfBirth)
0.4.0.194121.1.4 id-etsi-qcs-semanticsId-eIDASLegal	Semantics identifier for eIDAS legal person [EN 319 412-1 5.1.4節] eIDASに基づく法人用のセマンティックIDであり、識別名には上記 organizationIdentifier の他に属性タイプとして以下を用いる。 ● organizationName 組織名 (eIDASのLegalName)

QCStatementsを用いて日本版の適格eシール用証明書、適格署名用証明書を実装し、相互運用性を確保するためには、本節で紹介したQCStatementsの型やOIDを何らかの標準やガイドラインで規定しなければならない。

また、EUで認定されたHSM(即ちQSCD)を使用していることを示すQcSSCDタイプと同等のものを日本で実装する場合には以下が課題となる。

- EUでは、QSCDとして利用可能な認定されたHSM製品のリストを維持管理している。同等の認定制度が日本でも必要となる。
- 認証局は利用者の鍵がQSCDの要件を満たさないと、QcSSCDタイプをQCStatementsに含めることができない。
    - 認証局が利用者にUSBトークン等で秘密鍵と共に証明書を提供する場合
    - リモートeシール/署名サービスと認証局が同一の組織で運用しており、認定されたQSCDにリモートeシール/署名用の鍵を使っていることの確認、検証が容易である場合

  は、問題にならないが、
    - リモートeシール/署名サービスと認証局が別の事業者である場合

  については、本当に認定されたQSCDに利用者の署名鍵が格納されているかを確認するのは難しく、リモートアテステーションのような方法で技術的に確実に確認する

か、完全ではないにせよリモート署名サービスの認定制度と監査によりこれを保証するか、何らかの確認、検証方法を提供する必要がある。

A.2 組織識別子(organizationIdentifier)の値

EU eIDAS準拠のeシール用証明書の主体者識別名で使用される組織識別子(organizationIdentifier)の値の形式は、付録A.1でも紹介されている、”Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures “, ETSI EN 319 412-1 V1.4.4 (2021-05) の5.1.4節で法人用の証明書のセマンティクスID id-etsi-qcs-SemanticsId-Legal として定められている。

組織識別子の値は具体的には、例えばドイツの付加価値税登録番号の組織IDの場合、VATDE-1234567890のような形式の値であり、以下の値の並びになっている。

1. 法人IDのタイプを表す3文字（VAT、NTR等）
2. ISO 3166-1 [2] による国の二文字コード（例 DE, ES）
3. マイナス記号 ″-″ (0x2D (ASCII), U+002D (UTF-8))
4. 法人IDタイプに従ったID番号（表記方法は法人IDタイプに依存）

eシールのセマンティクスIDでは5種類の法人IDタイプを定義している。

- VAT - 各国の付加価値税登録番号(Value Added Tax)
- NTR - 各国の法人登記番号（日本の場合、法人番号もしくは法人等番号に相当する）
- PSD - 欧州PSD2指令(Payment Service Directive)に基づく各国金融機関の登録番号
- LEI - 金融安定理事会(FSB)が設立した国際団体GLEIFで管理する取引主体識別子(Legal Entity Identifier)番号
- 国ローカルな法人IDタイプは英字2文字とコロンと合わせた3文字で定義できる。(例 “EI:”)

日本版eシール用証明書においても同様に、組織識別子の値のとり得る形式を標準等によりセマンティクスとして規定する必要がある。

A.3 LEI拡張について

LEI(Legal Entity Identifier)は、金融取引を行う組織が持つ20文字の英数字の国際的な識別子(ID)であり、日本では東京証券取引所がIDを発行できる。

本解説書のeシール用証明書プロファイルでは、LEIの値はX.509v3拡張として格納することができ、その形式はISO 17442-2:2020 Financial services - Legal entity identifier (LEI) - Part 2: Applicaiton digital certificates で定義されている。

```
leiExtension   EXTENSION ::= {
   SYNTAX PrintableString(SIZE(20))
   IDENTIFIED BY lei }
Lei   OBJECT IDENTIFIER ::= { 1 3 6 1 4 1 52266 1 }
```

また参考までに、ISO 17442-2 では、組織における役職、肩書きを記載するためのRoleというX.509v3拡張も定義されているが、これは個人に対して付与されるためeシールには不要である。

```
roleExtension   EXTENSION ::= {
   SYNTAX PrintableString(SIZE(1.. ub-leiRole-length))
   IDENTIFIED BY role }
Role   OBJECT IDENTIFIER ::= { 1 3 6 1 4 1 52266 2 }
```

エディター
佐藤雅史 （セコム株式会社 IS研究所）

メンバー(所属名・氏名の五十音順・敬称略)

氏名	所属
新井聡	ＮＴＴビジネスソリューションズ株式会社
奥村美樹	ＮＴＴビジネスソリューションズ株式会社
金谷徹	ＮＴＴビジネスソリューションズ株式会社
執行雄樹	ＮＴＴビジネスソリューションズ株式会社
石橋麻衣子	サイバートラスト株式会社
金子大輔	サイバートラスト株式会社
宿谷昌弘	サイバートラスト株式会社
渡辺弘幸	サイバートラスト株式会社
渋谷憲	株式会社サイバーリンクス
稲葉厚志	GMOグローバルサイン株式会社
漆嶌賢二	GMOグローバルサイン株式会社
新宅友也	GMOグローバルサイン・ホールディングス株式会社
柴田孝一	セイコーソリューションズ株式会社
相良直彦	セコムトラストシステムズ株式会社
小田嶋昭浩	株式会社帝国データバンク
大澤昭彦	一般財団法人日本情報経済社会推進協会(JIPDEC)
臼田昇	一般財団法人日本データ通信協会
伊地知理	一般財団法人日本データ通信協会
齋藤久	一般財団法人日本データ通信協会
田中裕一	一般財団法人日本データ通信協会
西山晃	フューチャー・トラスト・ラボ
宮崎一哉	三菱電機株式会社
山中忠和	三菱電機株式会社