e シールに係る認証業務の認定に関するガイドライン

令和７年４月 24 日時点版

１．はじめに

通信インフラの高度化やデジタルサービスの普及・多様化により、我が国のネットワーク上でのデータ流通量は飛躍的に増大している。特に、Society5.0 においては、実空間とサイバー空間が高度に融合し、実空間での紙や対面に基づく様々なやりとりを、サイバー空間においても電子的に円滑に実現することが求められている。

このような中、電子データを安心・安全に流通できる基盤が不可欠であり、電子データの改ざんや送信元のなりすまし等を防止する仕組みであるトラストサービスの活用が期待される。とりわけ、企業等が発行する電子データが増大する中、業務効率化や生産性向上の観点からも、企業等が発行する電子データの発行元を証明する「e シール」の活用が期待される。

このような背景から、総務省では、令和３年６月に、e シールに係る技術や運用等に関する一定の基準を示した「e シールに係る指針」を策定した。令和５年９月からは「e シールに係る検討会」を開催し、e シールの更なる普及や活用を促す観点から、総務大臣による e シールに係る認定制度を創設することが適当との結論を得た。

以上を踏まえて、総務省は「e シールに係る認証業務の認定に関する規程」（令和７年３月 31 日総務省告示第 113 号）（以下「告示」という。）の施行により認定制度の運用を開始するとともに、制度運用に必要な関係規程として、令和７年３月に「e シールに係る認証業務の認定に関する実施要項」（以下「実施要項」という。）及び「e シールに係る認証業務の認定に関するガイドライン」（以下「ガイドライン」という。）を策定した。

本ガイドラインは、総務大臣による e シールに係る認証業務の認定を受けようとする者を対象として、実施要項の逐条解説を示すとともに、認定を受けるために遵守することが求められる技術・運用・設備の基準を定めるものである。

総務大臣による e シールに係る認証業務の認定制度を通じて、e シールの更なる普及や活用が促進されることによって、電子データを安心・安全に流通できる社会的基盤の構築が進むことで、その便益が国民一人一人に還元される社会が実現することを期待する。

なお、本ガイドラインの内容に関する事項について、御不明な点がある場合は、総務省に相談するようにしてください。

２．本書の構成

本ガイドラインは、「１．はじめに」、「２．本書の構成」、「３．用語定義」、「４．実施要項の逐条解説」、「５．技術・運用・設備の基準」により構成されている。

「１．はじめに」では、総務大臣によるｅシールに係る認証業務の認定制度の創設に至る背景と検討の経緯等について説明する。

「２．本書の構成」では、本ガイドラインの目次構成と各章で記載される内容について説明する。

「３．用語定義」では、本ガイドラインに用いられる専門用語の定義について記載する。

「４．実施要項の逐条解説」では、実施要項の規定において、ｅシールに係る認証業務を実施するに当たって、留意すべき事項について解説を行う。

「５．技術・運用・設備の基準」では、総務大臣によるｅシールに係る認証業務の認定を受けようとする者が、認定を受けるために遵守することが求められる事項等について規定する。

３．用語定義

用　語	定　義
Archived Certified Products	情報機器や情報システムなどのセキュリティを評価するための基準を定めた国際規格である ISO/IEC 15408 による認証を受けた製品のうち認証の有効期間が満了した製品を指す。なお、ISO/IEC 15408 は Common Criteria（以下「CC」という。）とも呼ばれる。
CA	Certification Authority の略であり、e シールに係る電子証明書の発行・失効、認証局の秘密鍵の生成・保護及び利用者の登録を行う機関のことを指す。一般に CA は、利用者の審査・登録を行う登録局（RA）、e シールに係る電子証明書の発行・更新・管理を行う発行局（IA）、e シールに係る電子証明書の失効情報などを公開するリポジトリなどにより構成される。
Certified Products	ISO/IEC 15408 による認証を受けた製品のうち、CC 認証証明書が有効期間内である製品のことを指している。
CP/CPS	CP は Certificate Policy の略であり、証明書ポリシーのことを指す。証明書ポリシーは認証局が電子証明書を発行する際の運用方針を定めた文書である。他方、CPS は Certification Practice Statement の略であり、認証業務運用規程のことを指す。認証業務運用規程は認証局の信頼性、安全性を対外的に示すために、認証局の運用、鍵の生成・管理、責任等に関して、運用方針をどのように適用させるのかを定めた文書である。
CRYPTREC	Cryptography Research and Evaluation Committees の略であり、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトのことである。デジタル庁、総務省及び経済産業省が共同で運営する暗号技術検討会と、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で運営する暗号技術評価委員会及び、暗号技術活用委員会で構成されている。
EAL	Evaluation Assurance Level の略であり、評価保証レベルのことを指す。CC の認証において、どの程度まで評価が行われたか、その深さと厳密さを示す尺度である。このような評価保証レベルは、EAL1～EAL7 の 7 段階で定義されており、このうち EAL4 では、EAL3 の保証に加えて、より多くの設計記述、ソースコードなどのセキュリティ機能のすべての実装表現、開発時の評価対象の改ざんを防止する向上されたメカニズムや手続きが要求される。EAL4＋では、EAL4 の保証に加えて、テストとレビューにおいて脆弱性分析の要求を加味することが要求される。

EN	European Norm の略であり、欧州域内における EU 加盟国間の技術基準として制定された統一規格である。
e シールに係る共通証明書ポリシーOID	トラストサービスの種別や認定有無等を機械的に判別可能とするために、e シールに係る電子証明書の証明書ポリシー欄に格納されるオブジェクト識別子（OID：Object Identifier）のことである。
e シールに係る電子証明書失効リスト（CRL）	e シールに係る電子証明書の有効期間中に、e シールに係る電子証明書の記載内容の変更、秘密鍵の紛失・盗難等の事由により、発行した e シールに係る電子証明書を失効した際に、認証局が公表する e シールに係る電子証明書の失効を示す情報のリストである。e シールに係る電子証明書失効リストには、失効した e シールに係る電子証明書の番号、失効日時、失効事由などが記載されている。このリストには、失効した e シールに係る電子証明書を発行した認証局の署名が付与される。CRL は Certificate Revocation List の略である。
e シールに係る電子証明書失効リストの開示先（CRL Distribution Point）	e シールに係る電子証明書失効リスト（CRL）が開示されているウェブページの URL のことである。当該 URL は e シールに係る電子証明書の拡張領域において「CRL 配布ポイント」欄に格納される。
FIPS	Federal Information Processing Standard の略であり、米国国立標準技術研究所(NIST)が制定している標準規格である。その中でも FIPS 140 については、暗号モジュールに関する標準規格を指しており、FIPS 140 のバージョンである FIPS 140-2 、FIPS 140-3 の認証を受けた製品は、「Active」、「Historical」、「Revoked」といった検証証明書の 3 つのステータスによって管理されている。
ISO/IEC	ISO は International Organization for Standardization（国際標準化機構）の略であり、電気・通信及び電子技術分野を除く全産業分野（鉱工業、農業、医薬品等）に関する国際規格の作成を行っている団体である。IEC は International Electrotechnical Commission（国際電気標準会議）の略であり、電気及び電子技術分野に関する国際規格を作成している団体である。
ITU-T	International Telecommunication Union Telecommunication Standardization Sector（電気通信標準化部門）の略であり、電気通信の良好な運用により諸国民の間の平和的関係及び国際協力並びに経済的及び社会的発展を円滑にする目的を持って設立された国際連合の専門機関である ITU の下部組織の 1 つである。通信網の技術・運用方法に関する国際標準の策定や、技術的な検討を行っており、策定された国際標準を勧告として公表している。
OCSP（オンライン証明書状態プロトコル）	Online Certificate Status Protocol の略であり、オンライン証明書状態プロトコルのことを指す。OCSP は電子証明書が失効しているかどうかを確認するためのオンラインによる電子証明書検証手順であり、サーバ

	（OCSP レスポンダ）に対して、クライアント（OCSP リクエスタ）から電子証明書が失効しているかを問い合わせ、サーバから回答を受け取る。
PIN	Personal Identification Number の略であり、日本語では個人識別番号とも表される。本識別番号は、ネットワーク上に流れることはなく、入力端末等に保存されている番号と突合することで認証を行う二要素認証の形態をとっており、一般的にセキュリティレベルがパスワードより高いという特徴がある。一方、パスワードとは、入力した情報がネットワークを通じてサーバに通信され、その中に保存されているパスワード情報と突合することで認証するものである。
Transport Layer Security（TLS）Protocol	インターネット上での通信を保護するために、通信相手を認証するとともに、通信を暗号化するプロトコルの１つである。Secure Socket Layer（SSL）Protocol を元にして、改良が加えられており、インターネット技術タスクフォース（IETF）が定める国際標準規格となっている。
UN/EDIFACT	United Nations/Electronic Data Interchange for Administration, Commerce and Transport の略であり、国際連合欧州経済委員会（UNECE）が定める行政手続き、商流、物流に係る電子データ交換（EDI）に関する規則である。
UPS	Uninterruptible Power System の略であり、蓄電池等により、停電時に切れ目なく電力を供給することのできる無停電電源装置のことを指す。
X.509	ITU-T の認証フレームワークに関する規格（Information Technology－Open Systems Interconnection－The Directory：Authentication Framework）であり、電子証明書フォーマットについて定義している。
暗号技術	文書や画像等のデータを通信及び保管する際に、第三者による情報の窃取を防ぐことを目的として、規定された手順に従いデータを変換し、秘匿化する技術のことである。
鍵長	データの暗号化又は復号に使用する暗号鍵の大きさを示すパラメータのことである。暗号鍵の鍵長が必要以上に長くなるとシステムの処理効率などに悪影響が出る可能性がある。反対に暗号鍵の鍵長が短くなると十分なセキュリティ強度を確保できなくなる可能性がある。
活性化	ハードウェア・セキュリティ・モジュール（HSM）、システム、装置等を起動することをいう。活性化する際には、防護される必要のあるデータ値で鍵以外のもの（例：PIN、パスフレーズなど）が要求され、このような活性化データをアクティヴェーションデータとも呼ぶ。
監査実施記録	認証事業者が自らの認証業務の運用の適正性を評価するために実施する監査の実施結果を記録する書類のことである。
危殆化	盗難、漏えい等、他人によって使用され得る状態になることである。
公開鍵基盤（PKI）	公開鍵と秘密鍵のペアからなる公開鍵暗号方式を用いて電子認証を実現する基盤をいう。本基盤で使用される秘密鍵・公開鍵の２つの鍵はペ

	アとなっており、片方の鍵（秘密鍵）で暗号化したものについては、もう一方の鍵（公開鍵）でしか復号できない仕組みとなっている。なお、公開鍵については広く一般に公開される鍵であるが、秘密鍵については本人だけが使用できるように厳重な管理が求められる。
後方互換性	古い製品やシステムにおいて定義された仕様や実装された機能が、同じ系列でリリースされた新しい製品やシステムにおいても全て使用できる状態のことである。
シグネチャ	マルウェアの帰属を特定・判別するために用いられるマルウェア検知用データのことである。シグネチャは、マルウェア検体を解析し、固有のファイルサイズやコード、ハッシュ値などを抽出して作成されている。
証明書署名要求（CSR）	電子証明書を発行する際の元となるデータのことである。証明書署名要求には、電子証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して電子証明書を発行する。データ形式として、PKCS#10 などがある。CSR は Certificate Signing Request の略である。
生体認証装置	指紋や顔、虹彩、静脈、声紋など、人間の身体や行動の特徴を読み取り、あらかじめ登録したデータと照合することで個人を認証する装置のことである。
電子政府推奨暗号リスト	CRYPTREC を構成する暗号技術検討会及び関連委員会により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストのことである。
登記事項証明書	登記所が登記事務に用いる登記記録が登録されたコンピュータシステムを利用して登記記録に記録されている事項の全部又は一部を証明するために発行する書類のことである。
登録用端末設備	専ら電子証明書の利用者を登録するために用いられる設備のことである。
認証設備室	認証業務用設備を設置する部屋のことである。ただし、認証業務用設備のうち、登録用端末設備のみが設置されている部屋を除く。
ハッシュ値	元データについて一定の長さのデータに変換する手順をハッシュ関数と呼び、それによって出力された値をハッシュ値という。一方向性と衝突発見困難性を満たすハッシュ関数は、暗号学的ハッシュ関数と呼ばれる。ハッシュ関数のアルゴリズムはハッシュ値の長さによって SHA-1、SHA-2、SHA-3 に大別されており、例えば SHA-224、SHA-256、SHA-384、SHA-512 は SHA-2 に分類される。ハッシュ値が長くなるのに伴い、セキュリティ強度が上がるという特徴がある。
ハードウェア・セキュリティ・モジュール（HSM）	暗号鍵等の生成、保管、利用などにおいて、セキュリティを確保する目的で使用するハードウェア（暗号モジュール）のことである。不正アク

	セスに備えるための機能(耐タンパ機能)を備えている。HSM は Hardware Security Module の略である。
ファイアウォール	外部のネットワークと内部のネットワークを結ぶ箇所に導入することで、外部からの不正な侵入を防ぐことができるシステム、又はシステムが導入された機器である。ファイアウォールには防火壁の意味があり、火災のときに被害を最小限に食い止めるための防火壁から、このように命名されている。
フィンガープリント	電子証明書の正当性を証明するデータのことである。電子証明書内のフィンガープリント（拇印）と別途認証局側で公開しているフィンガープリントを照合し一致すれば正しい証明書と確認できる。
ブランク	業務やシステム等の稼働が途切れている期間や状態のことを指す。
プレフィクス	接頭辞とも呼ばれ、語構成要素の一つであり、単独で用いられることがなく、常に他の語に付いて、それにある意味や用法を添加するために用いられる接辞のうち、語の構成上の基幹的な要素である語基よりも前に付く文字列のことである。本ガイドラインにおいては、e シールに係る電子証明書に格納される、発行元組織を一意に特定するための法人番号等の組織識別子の接頭辞（NTRJP 等）を指す。
フロアレスポンス	建築物の地盤に地震波が作用したときに、建築物はその振動特性に応じた応答を示すが、その応答加速度の最大値を各階床ごとに算定したものである。
プロトコル	「規約」、「議定書」といった意味があり、通信でいうところの「プロトコル」とは、異なる通信機器等がネットワークを介して信号やデータ、情報を互いに送受信可能なよう、あらかじめ決められた約束事や手順のことである。
マクロ機能	ソフトウェアやプログラムにおいて、繰り返し使用する複数の操作や命令等を１つにまとめ、必要に応じて呼び出せるようにする機能のことである。
モーションセンサー	物体の加速度や傾き、方向などを検出する装置のことである。
ライフサイクル管理	製品やシステム等の構想から廃棄に至るまでのプロセス全体を管理することである。
乱数生成アルゴリズム	ランダム特性に優れ、十分な長さを持つ乱数を自動的に生成することのできる計算式のことである。
リポジトリサーバ	認証局の電子証明書とそのハッシュ値、電子証明書失効リスト（CRL）、認証局証明書失効リスト（ARL）等を格納し公表するデータベースは「リポジトリ」と呼ばれ、このようなリポジトリを提供するサーバのことを指す。

リモートｅシールサービス提供事業者	クラウド等において、ｅシール生成者の秘密鍵の管理を行い、ｅシール生成者の指示に基づいてｅシールを生成するリモートｅシールサービスを提供する事業者のことである。
リモートｅシール方式	ｅシール生成者がクラウド等のリモート環境に秘密鍵の管理を委ね、リモート環境にアクセスしてｅシールを生成する方式である。例えば、ｅシール生成者が、リモートｅシールサービスを提供する事業者が管理するクラウド等に秘密鍵の管理を委ね、同クラウドにアクセスしてリモート環境でｅシールを生成するといったことが想定されている。
利用者識別設備	専ら利用者情報及び利用者識別符号を識別するために用いられる設備のことである。
利用者識別符号等受信設備	利用者ｅシール検証符号、利用者情報及び利用者識別符号を電気通信回線を通じて受信するために用いられる電子計算機のことである。
ローカルｅシール方式	ｅシール生成者の管理下にある環境で秘密鍵を保持し、この環境でｅシールを生成する方式である。鍵ペア（秘密鍵と公開鍵）の生成される場所によって更に幾つかのパターンに分かれる。例えば、認証局でｅシール生成者の鍵ペア及び当該公開鍵を生成し、秘密鍵と公開鍵に対して発行されたｅシールに係る電子証明書をｅシール生成者に送付するパターンや、ｅシール生成者が自ら鍵ペアを生成した後に認証局が当該公開鍵に対して発行したｅシールに係る電子証明書をｅシール生成者に送付するパターンが想定されている。

用語の定義を作成するにあたり、引用元・参照元として活用した文献、ウェブページを以下に示す。

- Common Criteria Portal ホームページ, https://www.commoncriteriaportal.org/index.cfm
- 「電子署名・認証業務関連 法令集」（一般財団法人日本情報経済社会推進協会）
- CRYPTREC ホームページ, https://www.cryptrec.go.jp/
- 独立行政法人情報処理推進機構（IPA）ホームページ, https://www.ipa.go.jp/
- 一般財団法人日本情報経済社会推進協会（JIPDEC）「用語集ホームページ」, https://www.jipdec.or.jp/library/word/index.html
- 米国国立標準技術研究所（NIST）「Cryptographic Module Validation Program（CMVP）ホームページ」, https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules
- 日本産業標準調査会（JISC）ホームページ, https://www.jisc.go.jp/
- 「行政手続きにおけるオンラインによる本人確認の手法に関するガイドライン」（2019 年（平成 31 年）2 月 25 日各府省情報化統括責任者（CIO）連絡会議決定）, https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/f1be078e/20220422_resources_standard_guidelines_guideline_07.pdf

- 国際連合欧州経済委員会（UNECE）「UN/EDIFACT ホームページ」，
  https://unece.org/trade/uncefact/introducing-unedifact
- 「暗号鍵設定ガイダンス～暗号鍵の鍵長選択方法と運用方法～」（独立行政法人情報処理推進機構セキュリティセンター），
  https://www.ipa.go.jp/security/crypto/guideline/gmcbt80000005ua7-att/000099765.pdf
- 「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（令和５年３月 30 日、デジタル庁・総務省・経済産業省），https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022r1.pdf
- 「ハッシュ関数の安全性に関する技術調査報告」（平成 18 年 2 月（平成 18 年 5 月改訂）、ハッシュ関数・暗号モード利用調査 WG），https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2005.pdf

４．実施要項の逐条解説

第４条（e シールの安全性の基準）

（e シールの安全性に係る基準）

第４条　告示第３条第１項第１号の「十分な安全性を有する暗号技術」については、e シールの安全性確保のために用いる公開鍵暗号（署名）が「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（令和５年３月 30 日デジタル庁・総務省・経済産業省策定）（注）のうち、「電子政府推奨暗号リスト」に記載された暗号技術に該当することとする。ただし、やむを得ない事情①がある場合に限り、総務大臣は該当する暗号技術を指定することができるものとする。

（注）CRYPTREC 暗号リストについては、最新更新版を参照することとする。

（１）概要

本条文では、告示第３条第１項第１号の基準として、e シールの安全性を確保するために用いる暗号技術に講ずるべき事項について規定している。

（２）条文解説

①「やむを得ない事情」

電子政府推奨暗号リストに記載されている暗号方式について、CRYPTREC の「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（令和４年３月デジタル庁・総務省・経済産業省策定）に記載されている移行完遂期間内に、認定事業者が発行する e シールに係る電子証明書を利用するシステムベンダー等の暗号移行対応が困難であるなど、認証事業者側の責任に帰さない事由についてはやむを得ない事情として判断することが可能であると解され得る。したがって、単に危殆化や後方互換性の欠如等といった理由はあくまで認証事業者側の都合であり、これに当たらないと解され得る。なお、やむを得ない事情については、総務省が個別具体的な状況に応じて判断する場合がある。

第６条（利用者の真偽の確認の方法）

（利用者の真偽の確認の方法）

第６条　告示第３条第１項第３号の「適切な方法」については、次のとおりとする。

一　利用者が実在することを確認するため、次のイからハまでに掲げる方法により確認を行うものとする。

イ　我が国の法令に規定された証明書の提出を求め確認する方法又はその他同等なものとしてみなすことができる方法。

ロ　利用申込者が申込時に申告した本店又は主たる事務所の住所とイで提出した証明書に記載された本店又は主たる事務所の住所が同一であることを確認する方法又はその他同等なものとしてみなすことができる方法。

ハ　利用者が自らの事業を継続的に運営していることを確認する方法。

二　利用申込者が申込みを行うための正当な権限を有することを確認する。

三　前号の規定において、認証業務の利用の申込み又は申込みの事実の有無を照会する文書の受取

り①を代理人が行うことを認めた認証業務を実施する場合においては、当該代理人に対し、その権限を証する利用申込者本人の署名及び押印（押印した印鑑に係る印鑑登録証明書が添付されている場合に限る。）がある委任状（利用申込者本人が国外に居住する場合においては、これに準ずるもの）又はその他同等なものとしてみなすことができるものの提出を求め、かつ、我が国の法令に規定された証明書等により、当該代理人の真偽の確認を行うものとする。

（1）概要

本条文では、告示第３条第１項第３号についての方法として、e シールに係る認証業務における利用者の真偽の確認を行う方法について規定している。

（2）条文解説

①「申込みの事実の有無を照会する文書の受取り」

認定事業者が行う利用申込者の本人確認の方法として、利用申込者から申請のあった住所に対して、書留郵便又は本人限定受取郵便により、申込みの事実の有無を照会する文書を送付し、これに対する返信を受領するものを指している。なお、上記については、実施要項第３条（電磁的記録による作成等）の規定により、当該文書に係る電磁的記録の作成や、電磁的記録の作成を行ったものの電子メール等による送付についても認められている。

第７条（その他の業務の方法）

（その他の業務の方法）

第７条　告示第３条第１項第４号の「必要な措置」については、次のとおりとする。

一　利用申込者に対し、書類の交付その他の適切な方法により、e シール付与の方法及び認証業務の利用に関する重要な事項について説明を行うこと。

二　利用申込者の申込みに係る意思を確認するため、利用申込者に対し、その署名又は押印（押印した印鑑に係る印鑑証明書が添付されている場合に限る。）のある利用の申込書その他の書面の提出又は利用の申込みに係る情報（電子署名及び認証業務に関する法律（平成十二年法律第百二号。以下「電子署名法」という。）に基づく認定を受けた認証業務又はこれに準ずるものに係る電子証明書により確認される電子署名が行われたものに限る。）の送信を求めること。

三　利用者 e シール符号を認証事業者が作成する場合においては、当該利用者 e シール符号を安全かつ確実に利用者等①に渡すことができる方法により交付し、又は送付し、かつ、当該利用者 e シール符号及びその複製を直ちに消去すること。

三の二　利用者 e シール符号を利用者等が作成する場合において、当該利用者 e シール符号に対応する利用者 e シール検証符号を認証事業者が電気通信回線を通じて受信する方法によるときは、あらかじめ、利用者識別符号を安全かつ確実に当該利用者に渡すことができる方法により交付し、又は送付し、かつ、当該利用者の識別に用いるまでの間、当該利用者等以外の者が知り得ないようにすること。

四　e シールに係る電子証明書の有効期間は、５年を超えないものであること。

五　e シールに係る電子証明書には、次の事項が記録されていること。

イ　当該ｅシールに係る電子証明書の発行者の名称及び発行番号

ロ　当該ｅシールに係る電子証明書の発行日及び有効期間の満了日

ハ　当該ｅシールに係る電子証明書の利用者の名称

ニ　当該ｅシールに係る電子証明書に係る利用者ｅシール検証符号及び当該利用者ｅシール検証符号に係るアルゴリズムの識別子

ホ　当該ｅシールに係る電子証明書の利用者の組織識別子（公的機関が発行する番号体系に基づくもの）

ヘ　当該ｅシールに係る電子証明書の証明書ポリシーの識別子

ト　当該ｅシールに係る電子証明書のｅシールに係る共通証明書ポリシーOID

チ　利用者ｅシール符号の利用目的の制限を示す情報

六　ｅシールに係る電子証明書には、その発行者を確認するための措置であって第４条の基準に適合するものが講じられていること。

七　認証業務に関し、利用者その他の者が認定認証業務（以下「認定業務」という。）と他の業務を誤認することを防止するための適切な措置を講じていること。

八　ｅシール検証者が発行者署名検証符号その他必要な情報を容易に入手することができるようにすること。

九　ｅシールに係る電子証明書の有効期間内において、利用者からｅシールに係る電子証明書の失効の請求があったとき又はｅシールに係る電子証明書に記録された事項に事実と異なるものが発見されたときは、遅滞なく当該ｅシールに係る電子証明書の失効の年月日その他の失効に関する情報を電磁的方法により記録すること。

十　ｅシールに係る電子証明書の有効期間内において、ｅシール検証者からの求めに応じ自動的に送信する方法②その他の方法③により、ｅシール検証者が前号の失効に関する情報を容易に確認することができるようにすること。

十一　第９号の規定によりｅシールに係る電子証明書の失効に関する情報を記録した場合においては、遅滞なく当該ｅシールに係る電子証明書の利用者にその旨を通知すること。

十二　認証事業者の連絡先、業務の提供条件その他の認証業務の実施に関して、告示第６条第１項に規定する規程を適切に定め、当該規程を電磁的方法により記録し、利用者その他の者からの求めに応じ自動的に送信する方法その他の方法により、利用者その他の者が当該規程を容易に閲覧することができるようにすること。

十三　ｅシールに係る電子証明書に利用者として記録されている者から、権利又は利益を侵害され、又は侵害されるおそれがあるとの申出があった場合においては、その求めに応じ、遅滞なく当該ｅシールに係る電子証明書に係る利用者に関する第８条第２項第１号ロ及びハに掲げる書類を当該申出を行った者に開示すること。

十四　次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。

イ　業務の手順

ロ　業務に従事する者の責任及び権限④並びに指揮命令系統

ハ　業務の一部を他に委託する場合においては、委託を行う業務の範囲及び内容並びに受託者による当該業務の実施の状況を管理する方法その他の当該業務の適切な実施を確保するための方

法

ニ　業務の監査に関する事項

ホ　業務に係る技術に関し充分な知識及び経験を有する者の配置

ヘ　認定業務に際して知り得た情報の目的外使用の禁止及び第８条第２項各号に掲げる帳簿書類の記載内容の漏えい、滅失又は毀損の防止のために必要な措置

ト　危機管理に関する事項

十五　認証業務用設備により行われる認証業務の重要度に応じて、当該認証業務用設備が設置された室への立入り及びその操作に関する許諾並びに当該許諾に係る識別符号の管理が適切に行われていること。

十六　複数の者による発行者署名符号の作成及び管理その他当該発行者署名符号の漏えいを防止するために必要な措置が講じられていること。

十七　告示第５条第３項に規定する廃止時等において利用者及び検証者の利益を保護するために 60 日前までにその旨を通知又は連絡すること（告示第９条第１項の規定により認定を取り消された場合等、やむを得ない場合はこの限りでない。）及び認定に係る業務を廃止する日までに利用者に対して発行したｅシールに係る電子証明書について失効の手続を行うことが含まれるものとする。

十八　認証業務に関する帳簿書類として第８条の規定に従い、帳簿書類を作成し、これを保存すること。

（１）概要

本条文では、告示第３条第１項第４号についての基準として、e シールに係る認証業務の方法について規定している。

（２）条文解説

①「利用者等」

実施要項第２条第５号では、「利用者」の定義について、自らが行う e シールの付与又は関連付けについて認証業務を利用する者（法人等をいう。）と定めている。

e シールの付与又は関連付けの方式については、利用者自らが行うローカル e シール方式以外に、利用者から秘密鍵の管理を委ねられたリモート e シールサービス提供事業者が行うリモート e シール方式も存在するため、本ガイドラインにおいては「利用者」という表現ではなく、「利用者等」という表現を用いている。

②「e シール検証者からの求めに応じ自動的に送信する方法」

認証事業者は、e シールに係る電子証明書の失効情報を記載したｅシールに係る電子証明書失効リスト（CRL）を作成し更新している。

CRL に対応した検証ツールから、e シールに係る電子証明書に記載された「e シールに係る電子証明書失効リストの開示先（CRL Distribution Point)」という項目で指定された URL へ自動的にアクセスして、CRL をダウンロードする方法を利用することができる。

上記以外にも、電子証明書が失効されていないかをリアルタイムで確認するプロトコル（OCSP）があり、OCSP に対応した検証ツールから、e シールに係る電子証明書に記載された「オンライン証明書状態プロトコル」という項目で指定された OCSP サーバの URL へ自動的にアクセスする方法を利用することができる。

③「その他の方法」

認証事業者が提供するリポジトリに記録されている e シールに係る電子証明書の失効情報を確認する方法や、認証事業者のホームページで公表されている e シールに係る電子証明書の失効情報を確認する方法等を利用することができる。

④「認証業務に従事する者の責任及び権限」

e シールに係る認証業務に従事する者の責任及び権限の定め方の例示は以下が考えられる。

ア．セキュリティ責任者:セキュリティ対策の実装を管理する責任を有する者

イ．システム管理者:認証設備室内の CA システム（e シールに係る認証業務用設備のうち電子証明書の作成又は管理に用いる情報システム、以下「CA システム」という。）のインストール、構成管理、保守及び障害等からの復旧の権限を有する者

ウ．システム運用担当者:CA システムの運用に関する責任を有し、システムバックアップの権限を有する者

エ．監査者:e シールに係る認証業務や CA システムが適切に運用されていることを、アーカイブや監査ログにより確認する権限を有する者

第８条（帳簿書類の作成及び保存）

（帳簿書類の作成及び保存）

第８条　認定事業者は、その認定に係る業務に関する帳簿書類を作成し、これを保存しなければならない。

２　第１項で定める業務に関する帳簿書類は、次のとおりとする。

一　認証業務の利用の申込みに関する帳簿書類で次に掲げるもの

イ　第７条第１号の説明に関する記録

ロ　利用の申込書

ハ　第６条で定める利用者の真偽の確認のために認証事業者に提出された書類及び提示された証明書等の写し

ニ　利用の申込みに対する諾否を決定した者①の氏名

ホ　利用の申込みに対する承諾をしなかった場合においては、その理由を記載した書類

ヘ　e シールに係る電子証明書及びその作成に関する記録

ト　認証事業者が利用者 e シール符号を作成したときは、当該利用者 e シール符号の作成及び廃棄に関する記録並びに利用者等からの受領書

二　発行者署名符号に関する帳簿書類で次に掲げるもの

イ　発行者署名符号の作成及び管理に関する記録

ロ　発行者署名検証符号に係る電子証明書の作成及びリポジトリ等における公開に関する記録

ハ　リポジトリ等に公開されている発行者署名検証符号に係る電子証明書を格納するサーバ上や当該発行者署名検証符号に係る電子証明書を送信する通信路上において改ざん防止措置を講じ、改ざん検知時のアラート通知の受信記録等の当該措置が正常に機能していることの記録

三　e シールに係る電子証明書の失効に関する帳簿書類で次に掲げるもの

イ　e シールに係る電子証明書の失効の請求書その他の失効の判断に関する記録

ロ　e シールに係る電子証明書の失効を決定した者の氏名

ハ　e シールに係る電子証明書の失効の請求に対して拒否をした場合においては、その理由を記載した書類

ニ　第７条第９号の失効に関する情報及びその作成に関する記録

四　認証事業者の組織管理に関する帳簿書類で次に掲げるもの

イ　第７条第 12 号の規程及びその変更に関する記録

ロ　第７条第 14 号イの事項及びその変更に関する記録

ハ　第７条第 14 号ロの事項及びその変更に関する記録

ニ　認証業務の一部を他に委託する場合においては、委託契約に関する書類

ホ　第７条第 14 号ニの監査の実施結果に関する記録

五　設備及び安全対策措置に関する帳簿書類で次に掲げるもの

イ　第５条第１号の措置に関する記録（映像によるものを除く。）

ロ　第５条第２号の措置に関する記録（不正なアクセス等があったときのものに限る。）

ハ　第５条第３号の認証業務用設備の動作に関する記録

ニ　第７条第 15 号の許諾に関する記録

ホ　認証業務用設備及び第５条各号の基準に適合するために必要な設備の維持管理に関する記録

ヘ　事故に関する記録

ト　帳簿書類の利用及び廃棄に関する記録

３　前項第１号から第４号までに掲げる帳簿書類は、当該帳簿書類に係る e シールに係る電子証明書の有効期間の満了日から 10 年間保存しなければならない。

４　第２項第５号に掲げる帳簿書類は、作成した日から認定の更新の日まで保存しなければならない。

５　第２項各号に掲げる帳簿書類（利用者又はその代理人の署名又は押印がない書類に限る。）は、電磁的方法による記録に係る記録媒体により保存することができる。

６　第２項各号に掲げる帳簿書類（前項に規定する書類を除く。）は、その原本を保存しなければならない。

（１）概要

本条文では、e シールに係る認証業務のうち帳簿書類の作成及び保存の方法について規定している。

（２）条文解説

①「利用の申込みに対する諾否を決定した者」

認証事業者において申込みの確認や処理に係る手続きを機械化・自動化している場合、利用の申込み

に対する諾否の決定に人間が直接関わらない形態も採り得るが、そのような形態においても、諾否を決定した者として、諾否の決定に関わる責任者を明確化する必要がある。

第 15 条（認定効力延長の特例措置）

（認定効力延長の特例措置）

第 15 条　「やむを得ない理由がある場合」とは、大規模な災害の発生<u>その他認定業務の運営又は社会経済情勢の重大な変化①</u>があり、これに対応して認定効力の延長が必要と総務大臣が認める場合に限る。

（1）概要

本条文では、総務大臣が認定効力の延長が必要であると認める場合に適用される特例措置について規定している。

（2）条文解説

①「その他認定業務の運営又は社会経済情勢の重大な変化」

認定を受けたｅシールに係る認証業務（以下「認定業務」という。）の運営又は社会経済情勢において、認定効力延長の特例措置により利用者及び検証者の保護が必要となるような重大な変化が発生することを想定している。具体的には、例えば、紛争、テロ行為、電力調達不能に陥るような発電所の事故、争議行為等の予測困難な又は発生を回避できない危機に直面して、認定業務や調査業務を実施できなくなる事態を指す。

第 25 条（相続による承継の報告）

（相続による承継の報告）

第 25 条　認定事業者の地位を承継しようとするとき（<u>相続①</u>による場合に限る。）は、認定事業者の地位を承継した者は次に掲げる事項を記載した文書を総務大臣に提出して報告を行うものとする。

一　相続人及び被相続人の氏名（相続人が法人又は団体であるときは、その名称及び代表者の氏名）及び住所並びに承継される認定事業者の電子証明書のハッシュ値

二　相続人が事業を相続する年月日

三　事業の相続の理由

四　認定事業者の地位の承継を必要とする理由

五　相続に係る認定業務の名称及び内容並びに当該業務に用いられる設備・システムの概要

六　相続人が告示第３条第１項第６号の規定に該当しないことの証明

２　前項の文書には、次に掲げる文書を添付するものとする。

一　事業の相続に関する契約書の写し

二　相続人が法人であるときは、その定款又は寄附行為及び登記事項証明書（相続人が法人でないときは、これらに準ずるもの）

三　相続人が二人以上ある場合において、認定事業者の地位を承継すべき相続人を定めたときは、他の相続人がこれを同意した事実を証する文書

四　相続人が定める CP 及び CPS
五　利用者及び検証者が第７条第９号及び第 11 号に掲げる検証を適切に行うに当たり必要な情報

（１）概要

本条文では、相続人が認定事業者の地位を継承しようとする場合に、相続人から総務大臣へ提出及び報告が必要となる文書について規定している。

（２）条文解説

①「相続」

認証事業者の相続は、認定事業者が株式会社である場合における株式の相続のことを指している。株式会社の株主が死亡すると、当該株主が所有していた株式は相続の対象となるため、相続により当該株式を取得した者が議決権のある発行済株式の一定数以上を確保した場合、当該株式会社の経営権を引き継ぐことができる。

なお、譲渡による株式の取得について株式会社の承認を必要とする譲渡制限株式の場合においても、会社法（平成 17 年法律第 86 号）の第 133 条及び第 134 条（株主の請求による株主名簿記載事項の記載又は記録）では、相続その他の一般継承による当該株式の移転は、譲渡制限の対象外であることを規定しているため、当該株式は相続の対象となっている。

５．技術・運用・設備の基準

（１）．e シールの安全性に係る基準関係（実施要項第４条）

（e シールの安全性に係る基準）

第４条　告示第３条第１項第１号の「十分な安全性を有する暗号技術」については、e シールの安全性確保のために用いる公開鍵暗号（署名）が「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（令和５年３月 30 日デジタル庁・総務省・経済産業省策定）（注）のうち、「電子政府推奨暗号リスト」に記載された暗号技術に該当することとする。ただし、やむを得ない事情がある場合に限り、総務大臣は該当する暗号技術を指定することができるものとする。

（注）CRYPTREC 暗号リストについては、最新更新版を参照することとする。

以下の①、②の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① e シールの安全性確保のために用いる公開鍵暗号（署名）は、「電子政府推奨暗号リスト」に記載された暗号技術から選択し、採用していること。
（注）電子政府推奨暗号リストについては、最新更新版を参照することとする。

② 「電子政府推奨暗号リスト」に記載された公開鍵暗号（署名）を利用する際には、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（令和４年３月デジタル庁・総務省・経済産業省策定）をもとに、当該暗号技術において適切なセキュリティ強度を実現するために必要な鍵長及びハッシュ長を選択し、採用していること。
（注）暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準については、最新更新版を参照することとする。

【必要書類】

必要書類	基準の項番
CPS	①～②
事務取扱要領	①～②

【実施要項第４条の逐条解説】
・12 頁参照

（２）．認証設備室への入出場管理関係（実施要項第５条第１号）

（業務の用に供する設備の基準）

第５条　告示第３条第１項第２号の「認証業務を適切に実施するための設備」については、次のとおりとする。

一　申請に係る業務の用に供する設備のうち認証業務用設備は、入出場を管理するために認証業務

の重要度に応じて必要な措置が講じられている場所に設置されていること。

以下の①～⑮の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 認証設備室への入室には、入室する複数人による生体認証装置(身体的特徴を識別する装置)の操作が必要であること。

② 認証設備室への入室は、生体認証装置によりあらかじめ登録された権限者であることが認証・識別される必要があること。

③ 認証設備室への入退室は、入室者と同数の複数人の退室操作で退室完了状態となり、退室者数が入室者数と同人数であることが確認できること。

④ 認証設備室からの退室完了後に無人の認証設備室内で動きを検出した場合(認証設備室内にモーションセンサーを設置する等)警報が発せられること。

⑤ 認証設備室への入室操作に要する時間(扉が開いている時間を含む)及び試行回数を設定し登録していること。
(注)「入室操作に要する時間」とは、例えば認証精度（本人拒否率、他人受入率)、生体認証装置の照合スピード及び認証精度を満たすのに必要な照合処理の試行回数（生体認証の不安定性を考慮して、複数回の試行を許可する必要がある）を考慮した時間（すなわち許容できる入室操作時間）を指している。

⑥ 認証設備室への入室操作において、⑤で設定し登録した時間又は試行回数を超えた場合は、常時(24 時間)人のいる場所に警報を発すること。もしくは入室操作の実施状況を遠隔監視装置で常時(24 時間)モニタリングし、異常な行動が見られた場合にはただちに対応できる体制が整っていること。

⑦ 認証設備室への入退室者及び在室者の撮影に死角ができないような位置に遠隔監視カメラを設置している。やむなく撮影に死角が存在する場合、当該場所に位置しないよう、また当該場所に位置する者がいないことをチェックするよう要員に対する教育を行っていること。

⑧ 認証設備室への入退室を記録する 1 週間分以上の映像が記録できる映像記録装置を設置していること。

⑨ 遠隔監視装置で認証設備室への入退室者及び在室者が常時(24 時間)撮影並びにモニタ表示されていること。又は、侵入検知センサー等と遠隔監視装置を連動させることで、入退室者及び在室者が存在する場合だけを自動的かつ継続的に監視及び記録していること。

⑩　認証設備室への入退室を記録する映像記録装置の記録媒体の交換時におけるブランクが生じないようにしていること。やむを得ない場合、記録媒体の交換を、認証設備室への入室者及び在室者がいないことを確認しながら、速やかに実施していること。

⑪　認証設備室内を記録する遠隔監視カメラで撮影している映像及び記録された映像は被写体が明確に確認できること。

⑫　認証設備室内を記録する遠隔監視装置及び映像記録装置には停電時対応のための UPS 等を設置していること。

⑬　登録用端末設備又は利用者識別設備が設置された室の出入口には錠を取付けてあり、無人の際には施錠されていること。

⑭　登録用端末設備又は利用者識別設備が設置された室においては、登録用端末設備又は利用者識別設備が設置されている場所は間仕切りで登録用端末設備又は利用者識別設備以外の区画と区分する等により関係者以外が容易に登録用端末設備又は利用者識別設備に触れる事ができないような措置を講じていること。

⑮　入退出者の別を考慮して認証設備室への搬入及び搬出可能な物品を定め、それ以外の物品の搬入及び搬出の状況を管理すること。
(注)搬入及び搬出可能な物品には、e シールに係る認証業務用設備のほか、外部記憶媒体、業務用のパソコン、保守用端末、監査用機器、その他日用品（生活必需品や事務用品を含む。但し危険物を除く。）等が含まれる。

【必要書類】

必要書類	基準の項番
CPS	⑬～⑮
事務取扱要領	①～⑮
生体認証装置の機器説明書	①
認証設備室の入退室記録（日時、場所、ID 等）	③
遠隔監視装置の機器説明書(含む監視カメラ及び侵入検知センサー)	⑦
映像記録装置の機器説明書（記録時間表：記録時間間隔×画質モード）	⑧
監視カメラの台数及び映像記録装置の台数	⑧
映像記録の記録媒体の交換記録（時間と実施者）	⑩
認証設備室における単線結線図	⑫

（３）．ｅシールに係る認証業務用設備への不正アクセス対策関係（実施要項第５条第２号）

（業務の用に供する設備の基準）
第５条　（略）
二　認証業務用設備は、電気通信回線を通じた不正なアクセス等を防止するために必要な措置が講じられていること。

以下の①～⑦の事項に関して事務取扱要領等に明確かつ適切に規定し、その規定を満たすｅシールに係る認証業務用設備等を設置していること。

① ｅシールに係る認証業務用設備（登録用端末設備を除く）が外部のネットワークと接続している場合、当該設備は次の要件を満たしていること。
ア．不正アクセス行為を防御するためのファイアウォール機能及びネットワークベースの侵入検知機能を備えた通信機器を有し、それらを介して通信が行われること。
イ．不正アクセス行為の要因となる可能性がある脆弱性の有無について定期的に確認され、対処されていること。

② ファイアウォール機能を備えた通信機器は次の要件を満たしていること。
ア．利用しないプロトコルによる通信を遮断できる。
イ．特定発信元及び特定着信先を指定し、それ以外の通信を遮断できる。
ウ．利用しないネットワークサービスへの通信を遮断できる。
エ．処理する通信の記録ができる。

③ ネットワークベースの侵入検知機能を備えた通信機器は次の要件を満たしていること。
ア．ネットワーク上を流れるパケットをモニタし、不正な侵入あるいはサービス妨害攻撃が検出できること。
イ．検出の基準となる不正侵入パターン(シグネチャ)ファイルを手動で設定ができる、あるいはソフトウェア等のアップデートによって定期的に更新できる機能を有していること。
ウ．不正な侵入又はその兆しを発見した時に、管理者へ報告する機能を備えていること。

④ ｅシールに係る認証業務用設備が２以上の部分から構成され(例えば、発行業務に用いる設備と登録業務に用いる設備に分かれている場合)、外部ネットワークを経由して接続されている場合、当該設備間の通信に関して、各設備の誤認並びに通信内容の盗聴及び改変を防止する措置を講じていること。また、当該設備間の通信には、少なくともTransport Layer Security（TLS）Protocol バージョン1.2以上を用いること。

⑤ ｅシールに係る認証業務用設備が２以上の部分から構成され、同一認証設備室内に設置されている場合、当該設備間の通信に関して、システムの設定、アクセス管理、内部牽制等の運用上の措置により、各設備の誤認並びに通信内容の盗聴及び改変を防止する措置を講じていること。

⑥　利用者ｅシール符号を利用者等が作成する場合において、利用者ｅシール検証符号、利用者情報及び利用者識別符号を電気通信回線を通じて受信するために用いられる電子計算機(以下「利用者識別符号等受信設備」という。)が設置されている場合は、利用者識別符号等受信設備からｅシールに係る認証業務用設備への通信に関して、各設備の誤認並びに通信内容の盗聴及び改変を防止する措置を講じていること。

⑦　ｅシールに係る認証業務用設備において、マルウェアに対するリアルタイムでの検知及びそれに対する保護措置を講じていること。代表的な保護装置には、次のようなものがある。

ア．不要なソフトウェアの削除

イ．マルウェア感染リスクが高い部分（マクロ機能等）が含まれるファイルの無害化

ウ．正常な動作から逸脱を要求する処理の無効化

⑧　マルウェア検知に係る製品は、次の要件を満たしていること。

ア．ｅシールに係る認証業務用設備内のシステム（OS、メモリ、システム構成情報、プログラムを含む）を監視し、マルウェアを検知できること。

イ．検知の基準となるシグネチャ又はマルウェアの可能性がある不正な動作を識別するための閾値について定期的に更新できる機能を有していること。

ウ．マルウェアを検知した時に、管理者へ報告する機能を備えていること。

【必要書類】

必要書類	基準の項番
事務取扱要領	①　～⑧
ｅシールに係る認証業務用設備等のセキュリティ関連文書	①～⑧
論理的ネットワーク構成図	①
物理的ネットワーク構成図	①
ファイアウォールの製品名、使用 OS 名、バージョン情報、機能がわかる文書	②
侵入検知システムの製品名、使用 OS 名、バージョン情報、機能がわかる文書	③
マルウェア検知に係る製品名、バージョン情報、機能がわかる文書	⑦～⑧

（４）．ｅシール認証業務用設備への不正操作対策関係（実施要項第５条第３号）

（業務の用に供する設備の基準）

第５条　（略）

三　認証業務用設備は、正当な権限を有しない者によって作動させられることを防止するための措置が講じられ、かつ、当該認証業務用設備の動作を記録する機能を有していること。

e シールに係る認証業務用設備を操作者によって作動させる場合は、以下の①～③の事項に関して、事務取扱要領等に明確かつ適切に規定し、その規定を満たす e シールに係る認証業務用設備を設置していること。

① e シールに係る認証業務用設備に対するアクセス権限は、操作者単位に設定できること。

② e シールに係る認証業務用設備は、パスワード、電子署名又は生体認証等により操作者の認証が行える機能を備え、あらかじめ設定されたアクセス権限に対応する操作者の特定ができること。

③ 登録用端末設備においては、接続されている e シールに係る認証業務用設備が上記①及び②の機能を備えていること。

利用者 e シール符号を利用者等が作成する場合において、e シールに係る認証業務用設備を利用者情報及び利用者識別符号の識別によって自動的に作動させる場合は、以下の④～⑥の事項に関して、事務取扱要領等に明確かつ適切に規定し、その規定を満たすように e シールに係る認証業務用設備等を設置していること。

④ e シールに係る認証業務用設備において、各利用者に対する利用者識別符号の設定をしていること。

⑤ 利用者識別符号等受信設備が設置された室の出入口には鍵を取付けてあり、無人の際には施錠していること。

⑥ e シールに係る認証業務用設備は、利用者識別符号等受信設備から電気通信回線を通じて送信された当該利用者情報及び当該利用者識別符号を識別する機能を有し、当該利用者情報及び当該利用者識別符号の確認を行う機能を備えていること。

以下の⑦～⑩の事項に関して、事務取扱要領等に明確かつ適切に規定し、その規定を満たす e シールに係る認証業務用設備を設置していること。

⑦ e シールに係る認証業務用設備に対して、登録用端末設備からの e シールに係る電子証明書の発行要求や失効要求等の当該電子証明書の管理に必要な操作のために利用する以外はネットワーク経由の遠隔操作が不可能であるように設定していること。

⑧ e シールに係る認証業務用設備毎に、以下の履歴を記録する機能を有していること。
ア．各イベントの要求者名（操作者によって作動させる場合に限る。）
イ．各イベント要求の発行先（端末 ID など）
ウ．各イベントの種類（ファイルのオープン、クローズ、名前変更、属性変更、削除など）

エ．各イベント発生日時
オ．各イベントの結果

⑨　操作者毎に、e シールに係る認証業務用設備の操作履歴記録が表示できること。

⑩　登録用端末設備、利用者識別設備、リポジトリサーバが接続される内部ネットワークセグメントに外部からアクセスする際には、②で規定する操作者の認証以外に追加の認証要素を加えること。

以下の⑪の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。

⑪　e シールに係る認証業務用設備を収容する建築物の外部及び建築物内に e シールに係る認証業務用設備の所在を明示又は暗示する名称が、以下のような場所において、看板もしくは表示板等によって掲示されていないこと。
ア．e シールに係る認証業務用設備を収容する建築物の外部
イ．e シールに係る認証業務用設備を収容する建築物のエントランス
ウ．e シールに係る認証業務用設備を収容する建築物のエレベータ
エ．認証設備室の入口
オ．受付
カ．その他パンフレット、ホームページ等

【必要書類】

必要書類	基準の項番
事務取扱要領	①　～⑪
e シールに係る認証業務用設備等のセキュリティ関連文書	①～⑪

（５）．発行者署名符号を作成し又は管理する電子計算機関係（実施要項第５条第４号）

（業務の用に供する設備の基準）
第５条　（略）
四　認証業務用設備のうち e シールに係る電子証明書の発行者（認証業務の名称により識別されるものである場合においては、その業務を含む。以下同じ。）を確認するための措置であって第４条の基準に適合するものを行うための発行者署名符号を作成し又は管理する電子計算機は、当該発行者署名符号の漏えいを防止するために必要な機能を有する専用の電子計算機であること。

以下の①の事項に関して、事務取扱要領等に明確かつ適切に規定し、その規定を満たす電子計算機を設置していること。

①　発行者署名符号は、ハードウェア・セキュリティ・モジュール（FIPS 140-2 のレベル 3 以上若し

くはFIPS 140-3のレベル3以上(注)又はISO/IEC 15408 EAL4＋以上（EN 419 221-5に対応するもの）の認証を受けた製品とし、以下「HSM」という。）を用いて保護していること。
(注)HSM選定時には、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準（以下「暗号強度要件設定基準」という。)」(2022年３月デジタル庁・総務省・経済産業省策定）等を踏まえて、暗号アルゴリズムの将来的な危殆化や後方互換性の欠如等の発生可能性、新しい方式への移行見込みを考慮すること。なお、暗号強度要件設定基準は最終更新版を参照することとする。

CMVPによるFIPSの認証を受けたHSMを使用する場合、以下の②～⑤の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。

② HSMの認証ステータスは原則として「Active」であること。

③ 運用中のHSMの認証ステータスが「Historical」に移行した場合においては、その要因が発行者署名符号の保護等に影響を及ぼさないものであることを確認し、確認した事実の証跡として、確認結果を文書化し保存すること。

④ ③において、認証ステータスが「Historical」に移行した要因が発行者署名符号の保護等に影響を及ぼさないことを確認できたHSMを継続的に使用する場合、認証ステータスを常時把握するとともに、定期的に発行者署名符号の保護等に影響を及ぼさないことを確認し、確認した事実の証跡として、確認結果を文書化し保存すること。

⑤ 運用中のHSMの認証ステータスが「Revoked」に移行した場合や「Historical」に移行した要因が発行者署名符号の保護等に影響を及ぼす恐れがある場合、当該HSMを用いて、新規の発行者署名符号を生成しないこと。また、認証ステータスが「Active」であるHSMに移行する計画を立て、当該計画を総務大臣に説明し承認を得ること。

ISO/IEC 15408の認証を受けたHSMを使用する場合、以下の⑥～⑦の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。

⑥ 原則として「Certified Products」の製品リストに登録されているHSMであること。

⑦ 運用中のHSMが「Archived Certified Products」の製品リストに移行した場合、当該HSMを用いて、新規の発行者署名符号を生成しないこと。また、「Certified Products」の製品リストに登録されているHSMに移行する計画を立て、当該計画を総務大臣に説明し承認を得ること。

【必要書類】

必要書類	基準の項番
事務取扱要領	①～⑦

HSM の製品名、ソフトウェア（OS、ファームウェアを含む）名、バージョン情報、機能がわかる文書	①
HSM が FIPS 140-2 のレベル 3 以上若しくは FIPS 140-3 のレベル 3 以上又は ISO/IEC 15408 EAL4＋以上（EN 419 221-5 に対応するもの）の認証を受けていることが確証できる文書	**６**

（６）．e シールに係る認証業務用設備への災害対策関係（実施要項第５条第５号）

（業務の用に供する設備の基準）

第５条　（略）

五　認証業務用設備及び第１号の措置を講じるために必要な装置は、停電、地震、火災及び水害その他の災害の被害を容易に受けないように認証業務の重要度に応じて必要な措置が講じられていること。

認証設備室が設置されている建築物及び認証設備室について、以下の①～㉑の停電、地震、火災及び水害その他の災害への対策に関して、事務取扱要領等に明確かつ適切に規定し、必要な措置を講じていること。

① 地震に対し e シールに係る認証業務用設備は、以下のいずれかによる移動・転倒防止対策が講じられていること。

ア．認証設備室のフロアレスポンスに応じて、e シールに係る認証業務用設備の製造業者が推奨する設置方式を考慮した移動・転倒防止等の措置が講じられていること。

イ．耐震脚、転倒防止金具等で建物構造体に固定されていること。

ウ．建築物全体、e シールに係る認証業務用設備が設置してある床等が免震構造を持つ、もしくは、e シールに係る認証業務用設備が免震台により支持されていること。

② ラックは例えば建物構造体への固定等により移動、転倒防止措置が講じられていること。

③ e シールに係る認証業務用設備の構成部品は、落下防止金具や耐震バンド等で固定されていること。

④ フリーアクセスフロアは地震で損壊しないようアングルやストリンガー等の補強措置が講じられていること。

⑤ 地震の際に e シールに係る認証業務用設備に被害を与えないよう、認証設備室内の什器・備品等に耐震措置が講じられていること。

⑥ 水害の防止のための措置として、次のいずれかを満足していること。

ア．認証設備室を建築物の 2 階以上に設置すること。または、
イ．認証設備室を建築物の 1 階以下に設置する場合には、水害に対して十分な対策を講じること。特に、過去に水害がある場合又は海抜ゼロメートル地帯等である場合には、浸水対策を講ずること。

⑦ 直上階の床板にアスファルトやウレタン系防水塗料を塗布する等の防水施工を講じている。防水施工が困難な場合は直上階床板下面のはり及び柱の周辺に全面検知型の漏水センサーを設置し、室内に防水カバーを常備していること。

⑧ 認証設備室には流し台、給茶機等の水使用設備は設置しないこと。

⑨ 認証設備室に空気調和機を設置する場合は、空気調和機の周辺に防水提又は水受け皿等を設置し、かつ防水提又は水受け皿等の内側に漏水センサーを設置していること。

⑩ 漏水監視は中央監視盤等により常時行っていること。

⑪ 認証設備室は、容易に破壊されない構造・強度を持った間仕切り壁又は隔壁により認証設備室以外の室と区分されていること。

⑫ 認証設備室は、侵入が可能となるような開口部を設けていないこと。

⑬ 認証設備室には、消防法施行令に規定された自動火災報知器及び消火装置を設置し、消防署等の検査を受け、定期点検を実施していること。

⑭ 認証設備室を含む区画は建築基準法に規定する防火区画であること。

⑮ ケーブルが防火区画を貫通する場合、貫通部分及び貫通部分から両側 1m以内の部分は不燃材料等による延焼防止措置を講じていること。

⑯ 換気、暖・冷房のダクトが防火区画を貫通する場合、ダクトの防火区画を貫通する部分又はこれに近接する部分に防火上有効なダンパーを設けていること。

⑰ 認証設備室において使用される e シールに係る認証業務用設備及び入退室管理装置には UPS(無停電電源装置)又は CVCF(定電圧定周波装置)と蓄電池を設置していること。

⑱ 認証設備室を設置する建築物は、地震による被害の恐れの少ない地域に設置されていること。やむを得ない場合には、パイル打設等の軟弱な地盤に対する不同沈下防止措置を講じていること。不同沈下に対する代表的な対策工法には次のようなものがある。

ア．密度増大工法：コンパクションパイル工法、静的砂杭締固め工法等
イ．固結工法：表層混合処理工法、深層混合処理工法、高圧噴射攪拌工法等
ウ．置換工法：掘削置換え工法等
エ．地下水位低下工法：ディープウェル工法、ウェルポイント工法等
オ．間隙水圧消散工法：バーチカルドレーン工法等
カ．せん断変形抑制工法：地中連続壁工法、矢板工法等
キ．その他：空気注入不飽和化工法等

⑲　認証設備室を設置する建築物は、建築基準法に規定する構造耐力等の基準に適合していること。

⑳　認証設備室を設置する建築物は、建築基準法に規定する耐火建築物又は準耐火建築物の基準に適合していること。

㉑　e シールに係る認証業務で用いる情報、ソフトウェア及びシステムに関するバックアップ媒体を管理する設備は、e シールに係る認証業務用設備と別の場所で、かつ同一の災害による影響を避けられる場所に設置されていること。

【必要書類】

必要書類	基準の項番
事務取扱要領	①～㉑
災害対策に関する文書	①～㉑
免震構造の効力を証明する認定書	①
e シールに係る認証業務用設備の製造業者が推奨する設置方式	①
防水施工図	⑦
消防用設備等検査済証	⑬
定期点検検査報告書	⑬
建築図面（フロアの平面図／防火区画が明記されているもの）	⑭
ダクト配管図	⑯
地盤調査書（地盤の N 値データ、基礎構造、支持層の位置、杭長が記載されているもの）	⑱
確認通知書	⑲～⑳
検査済証	⑲～⑳

（７）．利用者の実在性の確認の方法関係（実施要項第６条第１号）

（利用者の真偽の確認の方法）
第６条　告示第３条第１項第３号の「適切な方法」については、次のとおりとする。
一　利用者が実在することを確認するため、次のイからハまでに掲げる方法により確認を行うもの

とする。

イ　我が国の法令に規定された証明書の提出を求め確認する方法又はその他同等なものとしてみなすことができる方法。

ロ　利用申込者が申込時に申告した本店又は主たる事務所の住所とイで提出した証明書に記載された本店又は主たる事務所の住所が同一であることを確認する方法又はその他同等なものとしてみなすことができる方法。

ハ　利用者が自らの事業を継続的に運営していることを確認する方法。

以下の①～⑥の事項に関して CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 利用者の実在性の確認における実施要項第 6 条第 1 号イの方法については、次のアからエまでに掲げるいずれかの方法により確認すること。

ア. 利用の申込書に付された法人代表者による電子署名（商業登記法（昭和三十八年法律第百二十五号）第十二条の二第一項及び第三項の規定による電子証明書に係る電子署名に限る。）の有効性の確認を行う方法

イ. 利用の申込書に付された組織等の属性情報が格納された電子証明書に係る電子署名の有効性の確認（電子署名及び認証業務に関する法律（平成十二年法律第百二号）第四条の規定による認定認証業務に限る。）を行う方法

ウ. 商業登記法（昭和三十八年法律第百二十五号）第十条第一項の規定による登記事項証明書に証明されている商号又は社名の確認を行う方法

エ. 信頼できる第三者機関が営む法人データベースへの登録状況の確認を行う方法。法人データベースは、以下の要件を満たすデータベースとすること。

・商業登記法（昭和三十八年法律第百二十五号）第六条が定める商業登記簿の情報と照合されていること。

・データベースの内容（正確な場所、連絡先、その他の属性情報）が、トラストサービス業界以外の他の業界（組織間の商取引に際して取引先等の与信管理や信用調査が必要となる業界）においても信頼され、継続的に利用されていること。また、国際標準規格（UN/EDIFACT 3055、ISO/IEC 6523-2 又は ISO/IEC 15459-2 等）の認定を受けた発番機関が発行する企業識別番号（当該企業識別番号とリンクして発番される企業識別番号を含む。）が当該データベースに格納されていること。

・データベース提供事業者によって、データベースの内容が少なくとも年に 1 回更新されていること。

・データベース提供事業者と認定事業者が同一事業者である場合、双方の事業者の業務を区別する方針及び手順を有していること。

② 利用者の実在性の確認における実施要項第 6 条第 1 号ロの方法については、次のアからウまでに掲げるいずれかの方法により確認すること。

ア. 利用の申込書に付された法人代表者による電子署名（商業登記法（昭和三十八年法律第百二十

五号）第十二条の二第一項及び第三項の規定による電子証明書に係る電子署名に限る。）において、電子証明書の記載事項（本店又は主たる事務所の所在地）の確認を行う方法

イ. 商業登記法（昭和三十八年法律第百二十五号）第十条第一項の規定による登記事項証明書に証明されている本店又は主たる事務所の所在地の確認を行う方法

ウ. 信頼できる第三者機関が営む法人データベースへの登録状況の確認を行う方法。法人データベースは、以下の要件を満たすデータベースとすること。

・商業登記法（昭和三十八年法律第百二十五号）第六条が定める商業登記簿の情報と照合されていること。

・データベースの内容（正確な場所、連絡先、その他の属性情報）が、トラストサービス業界以外の他の業界（組織間の商取引に際して取引先等の与信管理や信用調査が必要となる業界）においても信頼され、継続的に利用されていること。また、国際標準規格（UN/EDIFACT 3055、ISO/IEC 6523-2 又は ISO/IEC 15459-2 等）の認定を受けた発番機関が発行する企業識別番号（当該企業識別番号とリンクして発番される企業識別番号を含む。）が当該データベースに格納されていること。

・データベース提供事業者によって、データベースの内容が少なくとも年に 1 回更新されていること。

・データベース提供事業者と認定事業者が同一事業者である場合、双方の事業者の業務を区別する方針及び手順を有していること。

③ 利用者の実在性の確認における実施要項第 6 条第 1 号ハの方法については、次のアからウまでに掲げるいずれかの方法により確認すること。

ア. 利用の申込書に添付された商業登記法（昭和三十八年法律第百二十五号）第十条第一項の規定による登記事項証明書に証明されている設立年月日が、設立から 3 年以上経過していることの確認を行う方法

イ. 信頼できる第三者機関が営む法人データベースへの登録状況の確認を行う方法。法人データベースは、以下の要件を満たすデータベースとすること。

・商業登記法（昭和三十八年法律第百二十五号）第六条が定める商業登記簿の情報と照合されていること。

・データベースの内容（正確な場所、連絡先、その他の属性情報）が、トラストサービス業界以外の他の業界（組織間の商取引に際して取引先等の与信管理や信用調査が必要となる業界）においても信頼され、継続的に利用されていること。また、国際標準規格（UN/EDIFACT 3055、ISO/IEC 6523-2 又は ISO/IEC 15459-2 等）の認定を受けた発番機関が発行する企業識別番号（当該企業識別番号とリンクして発番される企業識別番号を含む。）が当該データベースに格納されていること。

・データベース提供事業者によって、データベースの内容が少なくとも年に 1 回更新されていること。

・データベース提供事業者と認定事業者が同一事業者である場合、双方の事業者の業務を区別する方針及び手順を有していること。

ウ．免許・許可・登録等を受けている金融機関に開設された、利用者が現に有している自らを名義人とする預貯金口座の保有状況の確認を行う方法（弁護士が作成する意見書又は公認会計士等が作成する監査報告書（会計監査報告書を含む。）による証明及び提出を求め、確認を行う方法等）

④ 利用者の真偽の確認において、①のア、②のアの方法を用いる場合には、電子証明書について、少なくとも記載内容、形式、有効期限、失効されていないこと等により電子証明書の有効性を確認していること。かつ、利用の申込みに係る情報に付された当該電子証明書に係る電子署名の有効性を検証していること。

⑤ 利用者の真偽の確認において①のイ、②のイ又は③のアの方法を用いる場合には、登記事項証明書について少なくとも記載内容、形式、有効期限等が真正なものであることを確認していること。

⑥ 利用者の真偽の確認を行うにあたって疑義が生じた場合には、あらかじめ文書をもって定められた手続に従って、利用者の真偽の確認の手続を行うこと。

【必要書類】

必要書類	基準の項番
CPS	①～⑥
事務取扱要領	①～⑥

（８）．利用申込者の権限の確認の方法関係（実施要項第６条第２号）

（利用者の真偽の確認の方法）
第６条　（略）
二　利用申込者が申込みを行うための正当な権限を有することを確認する。

以下の①～④の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① e シールに係る認証業務の利用の申込みにおいて、対面による申込み、郵送による申込み、電気通信回線を通じた安全な申込み等、採用する方式について指定すること。

② 指定した利用申込方式において、実施要項第６条第１項第１号及び第３項で規定する利用者及び代理人の真偽の確認のために使用する資料の種類を指定すること。

③ 指定した利用申込方式以外の方式による利用の申込みがあった場合の取扱や手続きについて定めていること。

④　利用申込者が e シールに係る認証業務を利用する組織等に在籍することを、次のアからウまでに掲げるいずれかの方法により確認すること。

ア. 利用の申込書に付された法人代表者による電子署名（商業登記法（昭和三十八年法律第百二十五号）第十二条の二第一項及び第三項の規定による電子証明書に係る電子署名に限る。）において、電子証明書の記載事項（法人代表者の氏名）の確認を行う方法

イ. 商業登記法（昭和三十八年法律第百二十五号）第十条第一項の規定による登記事項証明書に証明されている法人代表者の氏名の確認を行う方法

ウ. 信頼できる第三者機関が営む法人データベースへの登録状況の確認を行う方法。法人データベースは、以下の要件を満たすデータベースとすること。

・商業登記法（昭和三十八年法律第百二十五号）第六条が定める商業登記簿の情報と照合されていること。

・データベースの内容（正確な場所、連絡先、その他の属性情報）が、トラストサービス業界以外の他の業界（組織間の商取引に際して取引先等の与信管理や信用調査が必要となる業界）においても信頼され、継続的に利用されていること。また、国際標準規格（UN/EDIFACT 3055、ISO/IEC 6523-2 又は ISO/IEC 15459-2 等）の認定を受けた発番機関が発行する企業識別番号（当該企業識別番号とリンクして発番される企業識別番号を含む。）が当該データベースに格納されていること。

・データベース提供事業者によって、データベースの内容が少なくとも年に 1 回更新されていること。

・データベース提供事業者と認定事業者が同一事業者である場合、双方の事業者の業務を区別する方針及び手順を有していること。

【必要書類】

必要書類	基準の項番
CPS	①～④
事務取扱要領	①～④

（９）．代理人の真偽の確認の方法関係（実施要項第６条第３号）

（利用者の真偽の確認の方法）

第６条　（略）

三　前号の規定において、認証業務の利用の申込み又は申込みの事実の有無を照会する文書の受取りを代理人が行うことを認めた認証業務を実施する場合においては、当該代理人に対し、その権限を証する利用申込者本人の署名及び押印（押印した印鑑に係る印鑑登録証明書が添付されている場合に限る。）がある委任状（利用申込者本人が国外に居住する場合においては、これに準ずるもの）又はその他同等なものとしてみなすことができるものの提出を求め、かつ、我が国の法令に規定された証明書等により、当該代理人の真偽の確認を行うものとする。

以下の①～⑦の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 次のアからウまでに掲げる方法のうちいずれか一以上のものにより、代理人の真偽の確認を行うこと。

ア. 出入国管理及び難民認定法（昭和二十六年政令第三百十九号）第二条第五号に規定する旅券、同法第十九条の三に規定する在留カード、日本国との平和条約に基づき日本の国籍を離脱した者等の出入国管理に関する特例法（平成三年法律第七十一号）第七条第一項に規定する特別永住者証明書、別表に掲げる官公庁が発行した免許証、許可証若しくは資格証明書等、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号）第二条第七項に規定する個人番号カード又は官公庁（独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。）、地方独立行政法人（地方独立行政法人法（平成十五年法律第百十八号）第二条第一項に規定する地方独立行政法人をいう。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第一項第八号の規定の適用を受けるものをいう。）を含む。）がその職員に対して発行した身分を証明するに足りる文書で当該職員の写真を貼り付けたもののうちいずれか一以上の提示を求める方法

イ. 利用の申込書に押印した印鑑に係る印鑑登録証明書（利用申込者が国外に居住する場合においては、これに準ずるもの）の提出を求める方法

ウ. その取扱いにおいて名宛人本人若しくは差出人の指定した名宛人に代わって受け取ることができる者（以下「名宛人等」という。）に限り交付する郵便（次に掲げるいずれかの書類の提示を求める方法により名宛人等であることの確認を行うことにより交付するものに限る。）又はこれに準ずるものにより、申込みの事実の有無を照会する文書を送付し、これに対する返信を受領する方法

- アに掲げる書類のいずれか一以上
- 健康保険、国民健康保険、船員保険等の被保険者証（マイナンバーカードを活用した被保険者証も含む。）、共済組合員証（マイナンバーカードを活用した共済組合員証も含む。）、国民年金手帳、基礎年金番号通知書、国民年金、厚生年金保険若しくは船員保険に係る年金証書又は共済年金、恩給等の証書のいずれか二以上
- 上記に掲げる書類のいずれか一以上及び学生証、会社の身分証明書又は公の機関が発行した資格証明書（アに掲げるものを除く。）であって写真を貼り付けたもののいずれか一以上

② 代理人の真偽の確認において①のアの方法を用いる場合には、提示された官公庁が発行した証明書等について少なくとも記載内容、形式、有効期限等が真正なものであることを確認していること。かつ、当該証明書等に貼付してある写真と提示者との照合により真偽の確認を実施していること。

③ 代理人の真偽の確認において①のイの方法を用いる場合には、印鑑登録証明書について少なくとも記載内容、形式、有効期限等が真正なものであることを確認していること。かつ、利用申込書に

代理人の実印が押印され、代理人の真偽の確認資料としてその押印に係る印鑑登録証明書が添付されている場合は、利用申込書に押印された実印の印影と利用申込書に添付された印鑑登録証明書に証明されている印影の写しが一致することを確認していること。

④ 代理人の真偽の確認において①のウの方法を用いる場合には、代理人に確かに交付されたことを示す書類を受領していること。

⑤ 代理人による利用申込み、及び実施要項第６条第１項第３号に規定する申込みの事実の有無を照会する文書の代理人による受取りの場合において提出を求める委任状には、利用者が代理人に対し委任する利用申込みの内容もしくは代理人による受取りが明確に記されていること。

⑥ 代理人による利用申込み、及び実施要項第６条第１項第３号に規定する申込みの事実の有無を照会する文書の代理人による受取りの場合、委任状になされた利用者本人の署名を確認するとともに、同文書に押印された利用者の実印の印影と委任状に添付された印鑑登録証明書に証明されている印影の写しが一致することを確認していること。

⑦ 代理人の真偽の確認を行うにあたって疑義が生じた場合には、あらかじめ文書をもって定められた手続に従って、代理人の真偽の確認の手続を行うこと。

【必要書類】

必要書類	基準の項番
CPS	①～⑦
事務取扱要領	①～⑦

【実施要項第６条の逐条解説】
・12 頁参照

(10). 利用者に対する重要な事項の説明関係（実施要項第７条第１号）

（その他の業務の方法）
第７条　告示第３条第１項第４号の「必要な措置」については、次のとおりとする。
一　利用申込者に対し、書類の交付その他の適切な方法により、e シール付与の方法及び認証業務の利用に関する重要な事項について説明を行うこと。

以下の①、②の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 以下の重要な説明事項について、利用申込者にわかりやすく記述し、利用申込者に説明していること。

ア．当該 e シールに係る認証業務は総務大臣から認定されたものであり、虚偽の申込みをしてはならないこと。

イ．e シールに係る電子証明書を署名用途と混同して使用してはならないこと。

ウ．充分な注意をもって利用者 e シール符号及びその活性化に使用する PIN 等の管理を行い、秘匿性を維持すること。

エ．利用者 e シール符号の複製や利用者 e シール符号を扱うことができる権限者以外の者への共有をしてはならないこと。

オ．利用者 e シール符号が危殆化（盗難、漏えい等により他人によって使用され得る状態になることをいう。以下同じ。）した場合、又は危殆化したおそれがある場合、e シールに係る電子証明書の記載事項に変更が生じた場合及び e シールに係る電子証明書の利用を中止する場合等においては、遅滞なく e シールに係る電子証明書の失効請求を行うこと。

カ．当該 e シールに係る電子証明書に係る署名アルゴリズムは、当該認証事業者が指定するものを用いること。

キ．実施要項第７条第１項第５号チに定める利用者 e シール符号の利用目的の制限に従い、当該 e シールに係る電子証明書を利用すること。

ク．利用申込者から e シールに係る認証業務を利用する担当者への重要な事項の説明を抜け漏れがないように実施し、組織内への浸透を図ること。

② 利用者への重要な説明事項の説明を、以下のいずれかの方法により実施していること。

ア．書類の交付(郵送、手交、電子メール)

イ．対面による説明

ウ．その他ア、イと同等な方法

【必要書類】

必要書類	基準の項番
CPS	①～②
事務取扱要領	①～②

(11)．利用申込者に対する申込みに係る意思の確認関係（実施要項第７条第２号）

（その他の業務の方法）

第７条　（略）

二　利用申込者の申込みに係る意思を確認するため、利用申込者に対し、その署名又は押印（押印した印鑑に係る印鑑証明書が添付されている場合に限る。）のある利用の申込書その他の書面の提出又は利用の申込みに係る情報（電子署名及び認証業務に関する法律（平成十二年法律第百二号。以下「電子署名法」という。）に基づく認定を受けた認証業務又はこれに準ずるものに係る電子証明書により確認される電子署名が行われたものに限る。）の送信を求めること。

以下の①、②の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 利用申込書又は利用の申込みに係る情報に以下の記載事項があること。
ア．利用申込者の氏名、役職
イ．利用申込者が在籍する組織の商号又は社名、本店又は主たる事務所の所在地、法人番号
ウ．利用の申込みをする e シールに係る電子証明書が利用者の意思を確認する用途で用いられないことの確認結果
エ．利用申込者の自筆署名又は印鑑証明書に係る印鑑による押印（利用の申込みに係る情報の送信の場合を除く。）
利用の申込みに係る情報を、電気通信回線を通じて送信する場合は、エに代えて有効な電子署名が付されていること。

② 代理人による申込みの場合においては、利用申込書には①の記載事項に加えて、代理人の氏名及び自筆署名又は印鑑登録証明書に係る印鑑による押印（代理人の真偽の確認の方法として印鑑登録証明書を用いる場合に限る。）並びに代理人による申込み理由の記載があること。

【必要書類】

必要書類	基準の項番
CPS	①～②
事務取扱要領	①～②
利用申込書	①～②

（12）．認証事業者による利用者 e シール符号の作成関係（実施要項第７条第３号）

（その他の業務の方法）
第７条　（略）
三　利用者 e シール符号を認証事業者が作成する場合においては、当該利用者 e シール符号を安全かつ確実に利用者等に渡すことができる方法により交付し、又は送付し、かつ、当該利用者 e シール符号及びその複製を直ちに消去すること。

利用者 e シール符号を認証事業者が生成する場合は、以下の①～⑥の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 利用者 e シール符号の生成を、認証設備室内又は同等の安全性が確保できる環境において、複数人の操作者によって行い、アクセス権限管理、内部牽制等により盗聴、改変防止等の措置を講じていること。

② 利用者 e シール符号の転送又は出力等を行う場合は、生成時と同等の安全性が確保された環境に

おいて、アクセス権限管理、内部牽制等により盗聴、改変防止等の措置を講じていること。また、生成、転送又は出力等に用いた装置等から取り出した後、遅滞なく利用者 e シール符号を完全に廃棄又は消去していること。

③ 利用者 e シール符号は、e シールに係る認証業務を利用する担当者のみが活性化することができるよう、PIN 等を安全に管理していること。

④ 利用者 e シール符号の活性化に使用する PIN 等の生成、転送又は出力等を行う場合は、アクセス権限管理、内部牽制等により盗聴、改変防止等の措置を講じていること。また、生成、転送又は出力等に用いた装置等から取り出した後、遅滞なく利用者 e シール符号の活性化に使用する PIN 等を完全に廃棄又は消去していること。

⑤ PIN の生成に関しては、適切な関数やアルゴリズムを用いた乱数を使用していること。

⑥ 生成された利用者 e シール符号を、安全かつ確実な方法で利用者本人に渡し、利用者から、利用者本人を特定できる自筆署名、印鑑証明書に係る印鑑等利用者本人を特定できる印鑑による押印、電子署名が付された受領書、又は利用者 e シール符号による e シールが付与若しくは関連付けされた受領書を受け取ること。

【必要書類】

必要書類	基準の項番
CPS	①～⑥
事務取扱要領	①～⑥

【実施要項第 7 条の逐条解説】
・13 頁参照

(13). 利用者等による利用者 e シール符号の作成関係（実施要項第７条第３の２号）

（その他の業務の方法）
第７条　（略）
三の二　利用者 e シール符号を利用者等が作成する場合において、当該利用者 e シール符号に対応する利用者 e シール検証符号を認証事業者が電気通信回線を通じて受信する方法によるときは、あらかじめ、利用者識別符号を安全かつ確実に当該利用者に渡すことができる方法により交付し、又は送付し、かつ、当該利用者の識別に用いるまでの間、当該利用者等以外の者が知り得ないようにすること。

利用者ｅシール符号を利用者等が作成し、ｅシールに係る認証業務用設備を利用者情報及び利用者識別符号の識別によって自動的に作動させる場合において、当該利用者ｅシール符号に対応する利用者ｅシール検証符号を認証事業者が電気通信回線を通じて受信を行う場合は、以下の①～⑤の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。但し、④の事項に関しては、ｅシールに係る認証業務用設備を利用者情報及び利用者識別符号の識別によって自動的に作動させない場合も含むものとする。

① 利用者の識別に用いる利用者識別符号は、安全な乱数生成アルゴリズムを用いて生成するものとし、認証設備室又は同等の安全性が確保できる環境において、複数人によって行われていること。

② 利用者識別符号は、安全かつ確実な方法で利用者本人に渡され、かつ、当該利用者へｅシールに係る電子証明書を発行する際には、当該利用者識別符号の受領及び保持の確認が行われていること。

③ 利用者識別符号は、認証設備室又は同等の安全性が確保できる環境に暗号化等の措置を講じて保管されていること。

④ 利用者が利用者識別符号を送信する際には、利用者識別符号を当該利用者の識別に用いる等受信設備の誤認並びに通信内容の盗聴及び改変を防止する措置が講じられていること。

⑤ 利用者の識別に用いた利用者識別符号がそれ以降の識別処理に用いられないような措置（ｅシールに係る認証業務用設備内に設定されている識別された利用者に対応した利用者識別符号を、廃棄又は使用済フラグを立てることなどにより使用できないようにすることなど）が直ちに講じられていること。

【必要書類】

必要書類	基準の項番
CPS	①～⑤
事務取扱要領	①～⑤

（14）．ｅシールに係る電子証明書の有効期間関係（実施要項第７条第４号）

（その他の業務の方法）
第７条　（略）
四　ｅシールに係る電子証明書の有効期間は、５年を超えないものであること。

以下の①の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 利用者に発行するｅシールに係る電子証明書の有効期間はｅシールに係る電子証明書データ作成

日（時、分、秒を含む。）から起算して5年以下であること。

【必要書類】

必要書類	基準の項番
CPS	①
事務取扱要領	①

(15). eシールに係る電子証明書の記録事項関係（実施要項第７条第５号）

（その他の業務の方法）

第７条　（略）

五　eシールに係る電子証明書には、次の事項が記録されていること。

イ　当該eシールに係る電子証明書の発行者の名称及び発行番号

ロ　当該eシールに係る電子証明書の発行日及び有効期間の満了日

ハ　当該eシールに係る電子証明書の利用者の名称

ニ　当該eシールに係る電子証明書に係る利用者eシール検証符号及び当該利用者eシール検証符号に係るアルゴリズムの識別子

ホ　当該eシールに係る電子証明書の利用者の組織識別子（公的機関が発行する番号体系に基づくもの）

ヘ　当該eシールに係る電子証明書の証明書ポリシーの識別子

ト　当該eシールに係る電子証明書のeシールに係る共通証明書ポリシーOID

チ　利用者eシール符号の利用目的の制限を示す情報

以下の①～⑥の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 利用者に発行するeシールに係る電子証明書の形式（ITU-T が定めた公開鍵基盤（PKI）に関する国際規格である X.509 に準拠する必要がある）及び言語を規定し、記載事項には以下の情報が含まれていること。

ア．発行者の名称（複数の認証業務を行っている場合には、業務の種類を含む）

イ．発行番号（認証業務内で重複しない一意の番号であること）

ウ．開始日及び終了日により表される有効期間（時、分、秒を含む）

エ．利用者の名称

オ．利用者eシール検証符号及び当該検証符号に係るアルゴリズム識別子

カ．利用者の組織識別子（公的機関が発行する番号体系に基づくもの）

キ．証明書ポリシーの識別子

ク．eシールに係る共通証明書ポリシーOID

ケ．利用者eシール符号の利用目的の制限を示す情報

② ①のカに規定する当該 e シールに係る電子証明書の利用者の組織識別子（公的機関が発行する番号体系に基づくもの）については、プレフィクス（接頭辞）としての「NTRJP」と、法人番号（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号）第三十九条第四項の規定により、国税庁が公表する法人番号）の体系を組み合わせて表現される利用者の識別子を、当該 e シールに係る電子証明書に記録していること。

③ ①のケに規定する利用者 e シール符号の利用目的の制限を示す情報については、e シールに係る電子証明書の拡張領域に鍵使用目的を記録していること。

④ e シールに係る電子証明書の拡張領域に、e シールに係る電子証明書の失効情報を入手できる e シールに係る電子証明書失効リストの開示先（CRL Distribution Point）として指定された URL 情報又は OCSP で指定された OCSP サーバの URL 情報を記録していること。

⑤ 利用者 e シール符号を利用者等が作成する場合において、①のオに規定する e シールに係る電子証明書に記録する利用者 e シール検証符号は、利用者 e シール符号によって行われた e シールの付与又は関連付けを当該利用者 e シール検証符号を用いて検証する等の方法により、利用者が当該利用者 e シール検証符号に対応する利用者 e シール符号を保有していることを確認していること。また、当該利用者 e シール検証符号を検証する場合は、その鍵長と暗号アルゴリズムが実施要項第４条に対応した基準(e シールの安全性に係る基準関係の基準)を満たすことを確認すること。

⑥ e シールに係る電子証明書に記録される事項の変更に伴い、e シールに係る電子証明書の新たな発行を行う場合、実施要項第７条第１項第３号及び第３の２号の規定を準用し、その基準を満たすこと。また、e シールに係る電子証明書の新たな発行に係る申請及び承認手続きを定め、e シールに係る電子証明書の新たな発行を当該手続きに従い適切に実施していること。

【必要書類】

必要書類	基準の項番
CPS	①～⑥
事務取扱要領	①～⑥

(16). e シールに係る電子証明書の発行者を確認するための措置関係（実施要項第７条第６号）

（その他の業務の方法）
第７条　（略）
六　e シールに係る電子証明書には、その発行者を確認するための措置であって第４条の基準に適合するものが講じられていること。

以下の①、②の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① eシールの安全性確保のために用いる、eシールの付与対象となる電子データのハッシュ値を得るためのハッシュ関数及びeシールの生成に用いる公開鍵暗号（署名）は、「電子政府推奨暗号リスト」に記載された暗号技術から選択し、採用していること。
(注)電子政府推奨暗号リストについては、最新更新版を参照することとする。

② 「電子政府推奨暗号リスト」に記載された公開鍵暗号（署名）及びハッシュ関数を利用する際には、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（令和４年３月デジタル庁・総務省・経済産業省策定）をもとに、当該暗号技術において適切なセキュリティ強度を実現するために必要な鍵長及びハッシュ長を選択し、採用していること。
(注)暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準については、最新更新版を参照することとする。

【必要書類】

必要書類	基準の項番
CPS	①～②
事務取扱要領	**17** ～②

(17). eシールに係る認証業務と他の業務の誤認防止措置関係（実施要項第７条第７号）

（その他の業務の方法）
第７条　（略）
七　認証業務に関し、利用者その他の者が認定認証業務（以下「認定業務」という。）と他の業務を誤認することを防止するための適切な措置を講じていること。

以下の①、②の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 発行者署名符号の用途は e シールに係る認証業務の発行する e シールに係る電子証明書への電子署名のみに使用されること。上記以外に発行者署名符号を使用する場合は、以下の項目内に限定されること。
ア．当該eシールに係る認証業務のeシールに係る電子証明書への電子署名（自己署名）
イ．当該発行者署名符号の更新処理のため、新しい当該 e シールに係る認証業務の e シールに係る電子証明書への電子署名
ウ．当該発行者署名符号の更新処理のため、古い当該 e シールに係る認証業務の e シールに係る電子証明書への電子署名
エ．当該 e シールに係る認証業務用設備及びそれを操作する者に対して発行する電子証明書への電子署名
オ．エの電子証明書を発行するための証明書署名要求（CSR）への電子署名

カ．電磁的に記録する失効に関する情報への電子署名
キ．e シールに係る電子証明書失効情報および当該 e シールに係る認証業務に関する情報等を開示する設備に対して発行する電子証明書への電子署名

② 当該発行者署名符号に対応した発行者署名検証符号に係る e シールに係る電子証明書の値を SHA-256、SHA-384 又は SHA-512 のうちいずれか 1 以上で変換した値（フィンガープリント）を記録し、改ざん防止措置を講じて公開していること。

e シールに係る電子証明書に利用者の属性を記録する場合には、以下の③の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

③ e シールに係る電子証明書に記録された事業所又は営業所その他の利用者の属性（利用者の名称及び当該利用者を識別する情報を除く。）は告示第３条第１項が定める認定の対象外であることを e シールに係る電子証明書に注記している、又は CP 若しくは CPS に記載し、その情報へのリンク先を e シールに係る電子証明書に記録していること。

【必要書類】

必要書類	基準の項番
CPS	①～③
事務取扱要領	①～③
e シールに係る電子証明書の値を SHA-256、SHA-384 又は SHA-512 のうちいずれか 1 以上で変換した値	②
e シールに係る電子証明書	③
CP	③

(18)．e シール検証者による必要な情報の入手関係（実施要項第７条第８号）

（その他の業務の方法）
第７条　（略）
八　e シール検証者が発行者署名検証符号その他必要な情報を容易に入手することができるようにすること。

以下の①～③の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 以下のア～ウの事項を含む e シール検証者に対する説明事項をわかりやすく記述し、e シールに係る電子証明書のリンク先等の場所に掲載していること。
ア．発行者署名検証符号及びフィンガープリントを確実に入手し、e シールに係る電子証明書に行われた発行者による電子署名を検証することにより、e シールに係る電子証明書の発行者を確認

すべきであること。

イ．e シールに係る電子証明書を信頼すべきか否か判断する際は、e シールに係る電子証明書の利用目的もしくは使用範囲又はその制限（利用者に通知した利用条件を含む。）を確認すべきであること。

ウ．認証事業者により提供される適切な手段を用い、e シールに係る電子証明書について失効されていないことを確認すべきであること。

② e シール検証者が、①で記述された各事項を確認するために必要な以下のア～エの情報を、e シールに係る電子証明書に記録されているリンク先等から容易に入手できること。

ア．発行者の e シールに係る電子証明書及びフィンガープリント

イ．e シールに係る電子証明書の利用目的もしくは使用範囲又はその制限（利用者に通知した利用条件を含む。）が記述された文書

ウ．e シールに係る電子証明書の失効情報

エ．実施要項第２条第１項第 16 号で定める CP 及び実施要項第２条第１項第 17 号で定める CPS

③ リンク先等から公開されている②のアで定める情報に対して、改ざん防止措置を講じていること。

【必要書類】

必要書類	基準の項番
CPS	①～③
事務取扱要領	①～③
e シールに係る電子証明書	①～②
e シール検証者への説明事項	①

(19)．利用者による e シールに係る電子証明書の失効請求関係（実施要項第７条第９号）

（その他の業務の方法）

第７条　（略）

九　e シールに係る電子証明書の有効期間内において、利用者から e シールに係る電子証明書の失効の請求があったとき又は e シールに係る電子証明書に記録された事項に事実と異なるものが発見されたときは、遅滞なく当該 e シールに係る電子証明書の失効の年月日その他の失効に関する情報を電磁的方法により記録すること。

以下の①～④の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 利用者等自身の起因による e シールに係る電子証明書の失効事由及び認証事業者自身の起因による e シールに係る電子証明書の失効事由をそれぞれ定めていること。

② 失効請求の方法（失効請求を行うことができる者を含む)、失効申請に必要な書類とその記載事項を定めていること。
（注） 失効請求を行うことができる者は、法人代表者又は法人代表者から委任を受けた者に限定することとする。

③ 失効請求を受理した場合、失効請求者の真偽の確認方法、失効に関する情報の記録の手続き等を定め、失効に関する措置を遅滞なく講じていること。

④ 電磁的に記録する失効情報に関する形式、失効情報の内容及び、更新サイクルを定めていること。

【必要書類】

必要書類	基準の項番
CPS	①～④
事務取扱要領	①～④

(20). e シール検証者による e シールに係る電子証明書の失効確認関係（実施要項第７条第 10 号）

（その他の業務の方法）
第７条　（略）
十　e シールに係る電子証明書の有効期間内において、e シール検証者からの求めに応じ自動的に送信する方法その他の方法により、e シール検証者が前号の失効に関する情報を容易に確認することができるようにすること。

以下の①、②の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① e シールに係る電子証明書に記録されている e シールに係る電子証明書の有効期間の間、e シール検証者が当該 e シールに係る電子証明書の失効情報を容易に確認できるように、以下のいずれかの方法を提供していること。
ア．失効された e シールに係る電子証明書の情報を記載した e シールに係る電子証明書失効リストの開示
イ．OCSP による e シールに係る電子証明書の失効状態の確認
ウ．その他、上記ア、イと同等の機能を有する方法

② 有効期間が終了した e シールに係る電子証明書の失効に関する e シール検証者から問合せへの対応方法を定めていること。

【必要書類】

必要書類	基準の項番

CPS	①～②
事務取扱要領	①～②

【実施要項第７条の逐条解説】
・13 頁参照

(21). 利用者への e シールに係る電子証明書の失効の通知関係（実施要項第７条第 11 号）

（その他の業務の方法）
第７条　（略）
十一　第９号の規定により e シールに係る電子証明書の失効に関する情報を記録した場合においては、遅滞なく当該 e シールに係る電子証明書の利用者にその旨を通知すること。

以下の①の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① e シールに係る電子証明書の失効に際して、遅滞なく当該 e シールに係る電子証明書の利用者にその旨を通知すること。

【必要書類】

必要書類	基準の項番
CPS	①
事務取扱要領	①

(22). 利用者による認証業務規程の閲覧関係（実施要項第７条第 12 号）

（その他の業務の方法）
第７条　（略）
十二　認証事業者の連絡先、業務の提供条件その他の認証業務の実施に関して、告示第６条第１項に規定する規程を適切に定め、当該規程を電磁的方法により記録し、利用者その他の者からの求めに応じ自動的に送信する方法その他の方法により、利用者その他の者が当該規程を容易に閲覧することができるようにすること。

以下の①～⑬の事項に関して、CPS に明確かつ適切に規定し、電磁的方法により記録し公開していること。

① 認証事業者の名称、連絡先及び認定業務名
・認証事業者の名称及び住所（郵便番号、都道府県名、ビル名、階等を含む）

・認定業務名
・連絡担当窓口の名称
・電話番号（事業者番号、市外局番号を含む）
・受付時間
・ファクシミリ番号（事業者番号、市外局番号を含む）（任意）
・電子メールアドレス
・認証事業者が運営するホームページ上の問い合わせフォームの URL 情報（任意）

② 証明の目的、対象及び制限に関する事項
ア．e シールに係る認証業務によって e シールに係る電子証明書を発行する対象
イ．e シールに係る認証業務で発行する e シールに係る電子証明書が使用できる目的、使用に当たっての制限及びそれらの関連事項等
ウ．e シールに係る電子証明書に記録されている事業所又は営業所その他の利用者の属性（利用者の名称及び当該利用者を識別する情報を除く。）は告示第３条第１項が定める認定の対象外であること。

③ 認証事業者が負担する保証、免責について制限を設ける場合にはその範囲
ア．認証事業者の保証又は責任
イ．保証及び免責の制限範囲

④ 利用申込み及び利用者の真偽の確認に関する事項
ア．e シールに係る電子証明書の利用申込み方法及び必要書類
イ．利用者の真偽の確認の方法、真偽の確認に使用する資料等

⑤ e シールに係る電子証明書の失効請求に関する事項
ア．失効の請求の方式
イ．失効の請求書又は請求情報に記載又は記録すべき事項
ウ．e シールに係る電子証明書の失効事由（認証事業者に起因するものを含む。）
エ．請求者の真偽の確認の方法

⑥ e シールに係る電子証明書の失効情報の確認方法及び期間に関する事項
ア．公開される失効に係る情報の内容及び公開の方法、e シールに係る電子証明書の失効情報の更新の周期
イ．失効に係る e シールに係る電子証明書の利用者への通知方法
ウ．有効期間の経過後に e シール検証者からの e シールに係る電子証明書の失効に関する情報について照会を受けた場合の対応方法等

⑦ セキュリティに関する事項

ア. 組織において実施する情報セキュリティ対策の方針や行動指針（情報セキュリティポリシー）
イ．e シールに係る認証業務に係るセキュリティ管理に関する事項
ウ. e シールに係る認証業務の運用に際して知り得た利用申込者をはじめとする者の個人情報の取扱いに関する事項
エ．運用体制、認証整備室のレイアウト、監査情報、e シールに係る認証業務用設備のセキュリティ等の機密情報の取扱いに関する事項
個人情報及び機密情報の取扱いには次のようなものがある。
・個人情報の取得及び利用
・個人情報及び機密情報の管理
・個人情報及び機密情報の保存期間
・個人情報及び機密情報の廃棄
・個人情報及び機密情報の開示

⑧ 料金に関する事項
ア．利用者が e シールに係る認証業務を利用するに当たって必要となる料金及び支払方法等、又はその記載場所

⑨ 帳簿書類の保存に関する事項
ア．e シールに係る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

⑩ 業務の廃止に関する事項
ア．e シールに係る認証業務を廃止する時の、発行済み e シールに係る電子証明書の失効処理方法、利用者への通知の時期及び方法

⑪ 認証事業者と関係者の間で係争が生じた場合に適用される法令及び解決のための手続きに関する事項
ア．e シールに係る認証業務に関して、認証事業者と関係者間で係争が生じた場合に適用される法令（原則日本国内法等）
イ．係争解決のための手続き、係争を取り扱う管轄裁判所等

⑫ HSM を使用する場合の取扱いに関する事項
ア. 輸出貿易管理令（昭和二十四年政令第三百七十八号）等の安全保障貿易管理分野の関係法令に準拠した暗号装置の使用方法
イ．FIPS の認定を受けた HSM の認証ステータスが「Revoked」又は「Historical」に移行した際の対応の方法又は ISO/IEC 15408 の認証を受けた HSM が登録されている製品リストが「Archived Certified Products」に移行した際の対応の方法

⑬ 本規程の改訂及び通知方法に関する事項

ア．本規程の改訂に関する実施及び承認手続き等
イ．本規程の改訂に関する利用者その他の者への通知の方法

【必要書類】

必要書類	基準の項番
CPS	①～⑬

(23)．権利侵害等の申出を行った利用者への必要な情報の開示関係（実施要項第７条第 13 号）

（その他の業務の方法）
第７条　（略）
十三　e シールに係る電子証明書に利用者として記録されている者から、権利又は利益を侵害され、又は侵害されるおそれがあるとの申出があった場合においては、その求めに応じ、遅滞なく当該 e シールに係る電子証明書に係る利用者に関する第８条第２項第１号ロ及びハに掲げる書類を当該申出を行った者に開示すること。

以下の①の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① e シールに係る電子証明書の名義人から権利又は利益を侵害され、又は、侵害されるおそれがあるとの申出を受け、必要な情報を開示する場合について、以下の事項を規定し、実施していること。
ア．申出する際の必要書類と申出方法
イ．申出を受理した時の真偽の確認方法
ウ．開示する情報（当該 e シールに係る電子証明書利用申込書類及び利用者の真偽を確認した資料、e シールに係る電子証明書記載データ等）

【必要書類】

必要書類	基準の項番
CPS	①
事務取扱要領	①

(24)．業務の手順関係（実施要項第７条第 14 号イ）

（その他の業務の方法）
第７条　（略）
十四　次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。
イ　業務の手順

e シールに係る認証業務に従事する者の責任と権限に応じた業務の手順及び、以下の①、②の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。

① e シールに係る認証業務の手順を変更する場合は、遅滞なく関連する事務取扱要領等を改訂していること。

② e シールに係る認証業務の手順について、 e シールに係る認証業務に従事する者の責任と権限に応じた教育・訓練計画を策定し、教育・訓練を実施していること。かつ、e シールに係る認証業務の手順の変更に際しても、適切な教育・訓練を実施していること。

【必要書類】

必要書類	基準の項番
事務取扱要領	①～②
業務手順の規程一覧	①～②
指揮命令系統を含む組織体制図	①～②
教育訓練計画書	②

(25). 業務に従事する者の責任及び権限並びに指揮命令系統関係（実施要項第７条第 14 号ロ）

（その他の業務の方法）
第７条　（略）
ロ　業務に従事する者の責任及び権限並びに指揮命令系統

e シールに係る認証業務に従事する者の責任及び権限並びに指揮命令系統並びに、以下の①、②の事項に関して、内部牽制を考慮した上で、事務取扱要領等に明確かつ適切に規定し、実施していること。

① 責任及び権限並びに指揮命令系統を変更する場合は、遅滞なく関連する事務取扱要領等を改訂していること。

② e シールに係る認証業務に従事する者の責任及び権限並びに指揮命令系統について、e シールに係る認証業務に従事する者の責任と権限に応じた教育・訓練計画を策定し、教育・訓練を実施していること。さらに、e シールに係る認証業務に従事する者の責任及び権限並びに指揮命令系統の変更に際しても、適切な教育・訓練を実施していること。

【必要書類】

必要書類	基準の項番
事務取扱要領	①～②
指揮命令系統を含む組織体制図	①～②

教育訓練計画書	②

【実施要項第７条の逐条解説】
・13 頁参照

(26). 業務の一部の委託関係（実施要項第７条第 14 号ハ）

（その他の業務の方法）
第７条　（略）
ハ　業務の一部を他に委託する場合においては、委託を行う業務の範囲及び内容並びに受託者による当該業務の実施の状況を管理する方法その他の当該業務の適切な実施を確保するための方法

以下の①、②の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。
業務委託する場合、その範囲は業務の一部に限定されること。業務の一部とは、利用者の真偽の確認に係る業務、e シールに係る認証業務の管理・運用に係る業務、帳簿の保存に係る業務等であること。

① 委託契約において、業務委託に係る手続き及び委託業務の内容を明確にするとともに委託元の指示の遵守及び責任分担、保証等について明確にしていること。

② 委託業務に関して委託先からの定期的な報告を受けること等により、業務が適切に行われていることを管理していること。

【必要書類】

必要書類	基準の項番
事務取扱要領	①～②
委託契約書	①～②

(27). 業務の監査関係（実施要項第７条第 14 号ニ）

（その他の業務の方法）
第７条　（略）
ニ　業務の監査に関する事項

以下の①～⑤の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 認定業務が CPS 及び事務取扱要領に沿って適切に運営されていることを確認する監査を計画し、実施していること。

② e シールに係る認証業務に係わる監査基準（実施要項第７条第１項第 12 号に規定する規程及び実施要項第７条第１項第 14 号イに規定する業務の手順等に基づき、適正に業務が運営されていることを確認するための監査に係る基準）を定め、当該基準に従い定期的な監査を毎年 1 回以上実施していること。

③ 監査結果及びセキュリティ対策技術の最新の動向を踏まえ、設備、規程等の見直しを含む対策を講じ、かつその対策の妥当性の評価を実施していること。

④ 保管すべき監査情報と保管期間を定めるとともに、保管に当たってはアクセス権限を明確にし、完全性及び機密性を保つための措置を講じていること。

⑤ 監査実施後に、総務大臣に対して監査結果を速やかに報告していること。また監査の結果として改善その他必要な措置が指摘された場合には、次に掲げる事項について速やかに対処していること。
ア．必要な措置が講じられるまでの運用の停止や利用者及び e シール検証者への通知又は連絡等
イ．必要な措置の実施

【必要書類】

必要書類	基準の項番
CPS	①～⑤
事務取扱要領	①～⑤
監査計画書	①～⑤
監査基準書	②
監査報告書	③～⑤

(28)．技術者の配置関係（実施要項第７条第 14 号ホ）

（その他の業務の方法）
第７条　（略）
ホ　業務に係る技術に関し充分な知識及び経験を有する者の配置

以下の①の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。

① e シール技術、電子署名技術、鍵管理技術、セキュリティ技術等に関する業務遂行上に必要な知識、経験それらを有している技術者の必要数を規定し、e シールに係る認証業務に従事する者として配置していること。

【必要書類】

必要書類	基準の項番

事務取扱要領	①
指揮命令系統を含む組織体制図	①

(29). 個人情報及び機密情報の取扱い関係（実施要項第７条第 14 号へ）

（その他の業務の方法）
第７条　（略）
へ　認定業務に際して知り得た情報の目的外使用の禁止及び第８条第２項各号に掲げる帳簿書類の記載内容の漏えい、滅失又は毀損の防止のために必要な措置

以下の①～⑥の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 個人情報の取扱及び保護に関して規定し、保管場所などの整備や適正な保護のための措置（施錠等）を行い、利用者より提出される個人情報を適切に管理していること。

② e シールに係る電子証明書の利用申込時に、個人情報の取扱いの方法、e シールに係る電子証明書への記載範囲について、利用者に明示し承認を受けていること。

③ 個人情報及びそれを含む書類や記録媒体については、認定業務に直接従事する者を特定した上で、目的外利用や漏えいがないように取扱い方法（廃棄の方法を含む）を定め、それに従った運用を実施していること。

④ 機密情報の取扱及び保護に関して規定し、保管場所などの整備や適正な保護のための措置（施錠等）を行い、機密情報を適切に管理していること。

⑤ 機密情報及びそれを含む書類や記録媒体については、認定業務に直接従事する者を特定した上で、漏えいした際の認定業務への影響度を十分考慮した取扱い方法（廃棄の方法を含む）を定め、それに従った運用を実施していること。

⑥ 個人情報及び機密情報の取扱及び保護に関して、役割に応じた教育・訓練計画を策定し、e シールに係る認証業務に従事する者に教育・訓練等を実施していること。

以下の⑦に関する事項を含む実施要項第８条第２項各号に規定する帳簿書類の保存を、CPS 及び事務取扱要領等に規定し、実施していること。

⑦ 各記録は漏えい、滅失又は毀損防止のため、以下の措置を講じていること。
ア．共通要件
・各記録は、施錠可能な出入口を持ち、間仕切り又は壁等によって区分された室の中に保存す

ること。

・各記録が保存される室には、自動火災報知器及び消火装置が備えられていること。

・各記録は直射日光が直接当たらない場所に保存するか、直射日光が当たらないよう、遮蔽措置を講ずること。

イ．紙媒体により原本で保存される資料等における追加要件

・原本上の記録が判読不能とならない環境を備えていること。

・専用のファイルにとじ込むこと。

ウ．電磁的記録で保存される記録における追加要件

・当該記録媒体の内容を表示することが出来るように、電子計算機その他の機器、オペレーティングシステム及びアプリケーションを維持・保存しておくこと。特に、電子計算機その他の機器、オペレーティングシステム及びアプリケーションを更新する場合は、当該記録媒体との互換性を確保すること等により、表示不能を生じさせないこと。

・記録媒体は、データの表示不能にならないように適切なケース等に保管すること。さらに記憶媒体の特徴に合わせて適宜記録し直すなどの措置が実施されるようになっていること。ただし、その際、保存内容の完全性・機密性を損なわない方法でなされていること。

【必要書類】

必要書類	基準の項番
CPS	①～⑦
事務取扱要領	①～⑦
教育訓練計画書	⑥

(30)．危機管理関係（実施要項第７条第 14 号ト）

（その他の業務の方法）

第７条　（略）

ト　危機管理に関する事項

以下の①～⑥の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 災害等による影響により、CA システム等の運用が中断又は途絶した場合に備えて、CA システム等の継続又は復旧を確実なものにするための対応策や手順、体制等を定めた業務継続計画を策定していること。

② 情報セキュリティインシデントが発生した場合に備えて、情報セキュリティインシデントに対する迅速な対応を確実なものにするための手順、体制等を確立していること。

③ e シールに係る認証業務停止が伴う災害等による障害発生への対応策には、以下の項目が含まれて

いること。

ア．利用者への通知、e シール検証者への開示及びその方法

イ．原因及び被害の追求と原因別対応策

ウ．e シールに係る認証業務で用いる情報、ソフトウェア及びシステムに関する定期的なバックアップを行い、これらのバックアップを e シールに係る認証業務用設備と別の場所で、かつ同一の災害による影響を避けられる場所に保管すること。

④ 発行者署名符号が危殆化し、又は危殆化したおそれがある場合の対応策には、以下の項目が含まれていること。

ア．当該 e シールに係る認証業務によって発行された全ての利用者の e シールに係る電子証明書の失効

イ．上記アの利用者の e シールに係る電子証明書の失効に関する情報の電磁的記録

ウ．利用者への通知、e シール検証者への開示及びその方法

エ．原因及び被害の追求と原因別対応策

⑤ 発行者署名符号が危殆化し、又は危殆化したおそれがある場合及び、災害又は e シールに係る認証業務用設備の故障等により、e シール検証者への失効情報の提供が、CPS にて定める時間を超えて停止し、かつ e シール検証者が停止を知る方法が無かった場合は、直ちに障害の内容、発生日時、措置状況等確認されている事項を総務大臣に通報すること。

⑥ 発行者署名符号の危殆化又は災害等による障害の発生に対する対応策や回復手順に関して、e シールに係る認証業務に従事する者の責任と権限に応じた教育・訓練計画を策定し、教育・訓練を実施していること。

【必要書類】

必要書類	基準の項番
CPS	①～⑥
事務取扱要領	①～⑥
業務継続計画	①、③
情報セキュリティインシデント対応方針	②
教育訓練計画書	⑥

(31)．認証設備室への入室管理及び操作者の権限管理関係（実施要項第７条第 15 号）

（その他の業務の方法）

第７条　（略）

十五　認証業務用設備により行われる認証業務の重要度に応じて、当該認証業務用設備が設置された室への立入り及びその操作に関する許諾並びに当該許諾に係る識別符号の管理が適切に行われ

ていること。

以下の①～⑤の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 認証設備室への入室について、許可されている者の指定、登録及び複数人による入室がなされていること。

② 規定された入室方法、手続きで入室が行われているかを日常チェックしていること。

③ 設備の保守その他の業務の運営上必要な事情により、やむを得ず入室権限を有しない者を入室させる場合には、入室の必要性を確認していること。また、入室時には、入室権限を有する複数人による同行がなされていること。

④ 規定された入室方法、手続きで入室権限を有しない者の入室が行われているかを日常チェックしていること。

⑤ 認証設備室の入退室記録を作成し、次回の更新認定を受ける日まで保存していること。

e シールに係る認証業務用設備へのアクセス管理がパスワードを用いてなされる場合は、以下の⑥の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。

⑥ パスワードの設定、変更等の手続きや管理が行なわれている。例えば、十分な長さがあり、容易に推測されない等の、十分に複雑で使い回しのないパスワードを設定し、アカウント流出等のおそれがあった際や、業務に従事する者の退職等アクセス権限に変更が生じた際は、直ちに変更していること。また、e シールに係る認証業務用設備にデフォルトのパスワードが設定されている場合、初回アクセス時に変更していること。さらに、パスワードファイル等、電磁的方法によるパスワードの記録は暗号化されており、これらへのアクセスは、権限を有する者のみが可能であること。

【必要書類】

必要書類	基準の項番
CPS	①～⑤
事務取扱要領	①～⑥

(32). 発行者署名符号の作成及び管理関係（実施要項第７条第 16 号）

（その他の業務の方法）
第７条　（略）
十六　複数の者による発行者署名符号の作成及び管理その他当該発行者署名符号の漏えいを防止す

るために必要な措置が講じられていること。

以下の①～⑪の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 発行者署名符号の生成及び活性化は、複数人によって行われかつその内の１名だけでは操作されない方法によって行われていること。

② 発行者署名符号の生成は、認証設備室内で、実施要項第５条第１項第４号に規定する HSM を用いて行われていること。

③ 発行者署名符号のバックアップ及び回復は当該 e シールに係る認証業務を行う認証設備室内で、複数人によって行われかつそのうちの１名だけでは操作できない方法によって行われていること。

④ 発行者署名符号のバックアップが、実施要項第５条第１項第４号に規定する HSM 自体の複製機能を使用して行われる場合は、以下の要件を満たすものであること。
ア．バックアップされた HSM を、認証設備室もしくはそれと同等の安全性を有する場所に保存していること。

⑤ 発行者署名符号のバックアップに実施要項第５条第１項第４号に規定する HSM 自体の複製機能を使用しない場合は、認証設備室内で発行者署名符号に関する情報を分割し、複数の者が異なる安全な場所に分散して保管する方法（発行者署名符号を再生する場合には、複数の者が集合することを要するものに限る。）が用いられ以下の要件を満たすものであること。
ア．分散された発行者署名符号は、権限を有する人間以外が触れることのできない施錠等によるアクセス制御及び耐火等の防災措置がとられた場所に保管されること。
イ．分散された発行者署名符号は、それぞれが異なる場所に保管されること。

⑥ 発行者署名符号の使用を可能とし、又は不可能とする状態変更を、以下の条件で行っていること。
ア．状態変更を認証設備室内で実施していること。
イ．状態変更を、複数人により行いかつその内の１名だけの操作ではできない方法によって実施していること。

⑦ 発行者署名符号の使用を終了する場合、発行者署名符号（バックアップも含む）の廃棄を、以下のいずれかの方法を用いて、いずれも複数人によって行い、元の状態に戻せない事を確認すること。
ア．物理的破壊
イ．完全な初期化
ウ．その他、廃棄対象の発行者署名符号のすべての部分が元の状態に戻せないことが保証できる方法

⑧ 発行者署名符号の廃棄及びバックアップされた発行者署名符号（複製および分散された発行者署名符号を含む）の廃棄を一連の作業指示において遅延なく実施していること。

⑨ 実施要項第５条第１項第４号で定める発行者署名符号を作成し又は管理する HSM は、初期導入時において使用する機能が正しく動作することをテストにより確認していること。

⑩ 実施要項第５条第１項第４号で定める発行者署名符号を作成し又は管理する HSM について、使用を終了する場合には、⑦を含め HSM の廃棄を安全かつ確実な方法で実施していること。

⑪ 発行者署名符号を使用する CA システム等について、企画、要件定義、調達、構築、運用、保守、更改、廃棄等のライフサイクル全般を通して、必要となる情報セキュリティ対策を定め、管理していること。必要となる情報セキュリティ対策には次のようなものがある。

ア．企画及び要件定義時：実施体制の確保、セキュリティ要件の策定等

イ．調達及び構築時：機器等の納入時の検査、システムの受入時の検査、設定のミスや不備の確認等

ウ．運用及び保守時：機器等の脆弱性対策、アクセス権限の管理、バックアップの取得及び保存等

エ．更改及び廃棄時：機器等の変更管理、記録されている情報の完全な抹消等

【必要書類】

必要書類	基準の項番
CPS	①～⑪
事務取扱要領	①～⑪

(33)．廃止時の利用者及び検証者への通知関係（実施要項第７条第 17 号）

（その他の業務の方法）

第７条　（略）

十七　告示第５条第３項に規定する廃止時等において利用者及び検証者の利益を保護するために 60 日前までにその旨を通知又は連絡すること（告示第９条第１項の規定により認定を取り消された場合等、やむを得ない場合はこの限りでない。）及び認定に係る業務を廃止する日までに利用者に対して発行した e シールに係る電子証明書について失効の手続を行うことが含まれるものとする。

以下の①～④の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 認定の更新を受けない場合等を含め、 認定業務を廃止する場合には、廃止する日の 60 日前までに、認定業務を廃止する旨を利用者等及び検証者に通知すること。

② 利用者等及び検証者への通知は、電話や電子メール、ホームページ等の日常的に利用でき、かつ広く周知を図ることができる方法により行うこと。

③ 廃止時において利用者等及び検証者の利益を保護するために必要な事項として、次のア～カに掲げる事項について通知又は連絡するよう努めること。

ア．廃止しようとする認定業務の内容

イ．廃止しようとする年月日

ウ．廃止の理由

エ．廃止しようとする認定業務に関する利用者等及び検証者からの苦情又は相談に応ずる営業所又は事務所の連絡先

オ．廃止しようとする認定業務に係る役務の代替となる役務（当該認定業務に係る役務と当該代替となる役務との比較検討が可能となる情報を含む。）

カ．廃止しようとする認定業務に係る役務に関する利用者等及び検証者の被害の発生又は拡大の防止に資する情報

④ 認定業務の廃止日までに、当該認定業務によって発行された全ての利用者の e シールに係る電子証明書を失効すること、及び廃止後の失効に関する情報の確認方法を規定し、実施すること。

【必要書類】

必要書類	基準の項番
CPS	①～④
事務取扱要領	①～④

(34)．帳簿書類の作成及び保存関係（実施要項第７条第 18 号）

（その他の業務の方法）

第７条　（略）

十八　認証業務に関する帳簿書類として第８条の規定に従い、帳簿書類を作成し、これを保存すること。

以下の①の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① e シールに係る認証業務に関する帳簿書類の作成又は保存を、実施要項第８条の規定に従い、実施していること。

【必要書類】

必要書類	基準の項番

CPS	①
事務取扱要領	①

(35). 帳簿書類の作成及び保存関係（実施要項第８条第１項）

（帳簿書類の作成及び保存）
第８条　認定事業者は、その認定に係る業務に関する帳簿書類を作成し、これを保存しなければならない。

以下の①の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 認定に係る業務に関する帳簿書類を作成し、これを保存していること。

【必要書類】

必要書類	基準の項番
CPS	①
事務取扱要領	**36**

(36). e シールに係る認証業務の利用の申込みに関する帳簿書類関係（実施要項第８条第２項第１号）

（帳簿書類の作成及び保存）
第８条　（略）
２　第１項で定める業務に関する帳簿書類は、次のとおりとする。
一　認証業務の利用の申込みに関する帳簿書類で次に掲げるもの
イ　第７条第１号の説明に関する記録
ロ　利用の申込書
ハ　第６条で定める利用者の真偽の確認のために認証事業者に提出された書類及び提示された証明書等の写し
ニ　利用の申込みに対する諾否を決定した者の氏名
ホ　利用の申込みに対する承諾をしなかった場合においては、その理由を記載した書類
ヘ　e シールに係る電子証明書及びその作成に関する記録
ト　認証事業者が利用者 e シール符号を作成したときは、当該利用者 e シール符号の作成及び廃棄に関する記録並びに利用者等からの受領書

以下の①～⑪の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。

① 実施要項第７条第１項第１号（利用申込者に対し、書類の交付その他の適切な方法により、e シールの付与又は関連付けの方法及び e シールに係る認証業務の利用に関する重要な事項について説

明を行うこと。）の説明に関する記録を作成し、保存していること。
上記に関する記録には、その実施の日付及び実施した者の識別に関する情報が関連づけられて記録されていること。

② 利用者又はその代理人により提出された利用の申込書に関する書類又はその情報（電子署名及び認証業務に関する法律（平成十二年法律第百二号）に基づく認定を受けた認証業務又はこれに準ずるものに係る電子証明書により確認された電子署名が行われているものに限り、その電子署名の有効性を確認した記録も含む。）を保存していること。
上記の書類又は情報には、受領の日付及び受領した者の識別に関する情報が関連づけられて記録されていること。

③ 利用者の真偽の確認のために提出された書類及び提示された証明書の写し又はその情報（電子署名及び認証業務に関する法律（平成十二年法律第百二号）に基づく認定を受けた認証業務又はこれに準ずるものに係る電子証明書により確認された電子署名が行われているものに限り、その電子署名の有効性を確認した記録も含む。）を保存していること。
上記の書類又は証明書の写し、又はその管理に係る帳簿等には、受領の日付及び受領した者の識別に関する情報が関連づけられて記録されていること。

④ 代理人の真偽の確認のために提出された書類及び提示された証明書の写し又はその情報（電子署名及び認証業務に関する法律（平成十二年法律第百二号）に基づく認定を受けた認証業務又はこれに準ずるものに係る電子証明書により確認された電子署名が行われているものに限り、その電子署名の有効性を確認した記録も含む。）を保存していること。
上記の書類又は証明書の写し、又はその管理に係る帳簿等には、受領の日付及び受領した者の識別に関する情報が関連づけられて記録されていること。

⑤ 利用の申込みに対する諾否を決定した者の氏名及び決定した日付を記録し、保存していること。

⑥ 利用の申込みに対する承認をしなかった場合においては、その理由を記載した書類を作成し、保存していること。

⑦ e シールに係る電子証明書及びその作成に関する記録を作成し、保存していること。
上記の記録には、当該 e シールに係る電子証明書の作成を実施した日付並びに実施した者及び当該 e シールに係る電子証明書の作成について責任を有する者の識別に関する情報が関連づけられて記録されていること。

⑧ 認証事業者が利用者 e シール符号を作成したときには、当該利用者 e シール符号の作成及び廃棄に関する記録を作成し、保存していること。
上記の記録には、当該利用者 e シール符号の作成及び廃棄を実施した日付並びに実施した者及び

当該利用者 e シール符号の作成及び廃棄について責任を有する者の識別に関する情報が関連づけられて記録されていること。

⑨ 認証事業者が利用者 e シール符号を作成したときには、実施要項第 7 条第 1 項第 3 号に対応する基準（認証事業者による利用者 e シール符号の作成関係の基準）のうち、⑥の基準が定める利用者からの受領書又はその情報（電子署名及び認証業務に関する法律（平成十二年法律第百二号）に基づく認定を受けた認証業務又はこれに準ずるものに係る電子証明書により確認された電子署名が行われているものに限り、その電子署名の有効性を確認した記録も含む。）を保存していること。上記の記録には、その受領の日付及び受領した者の識別に関する情報が関連づけられて記録されていること。

【必要書類】

必要書類	基準の項番
事務取扱要領	①～⑨
利用者への説明の実施記録 【参考例】 ・利用者同意書 ・説明事項同意書	①
利用の申込書に関する書類又はその情報 【参考例】 ・利用申込書（代理人による申込の場合は委任状を含む） ・電子署名付き利用申込情報及び有効性確認記録	②
利用者の真偽確認の提出書類 【参考例】 ・登記事項証明書 ・利用者の真偽の確認作業管理簿 ・電子署名に用いた電子署名及び認証業務に関する法律（平成十二年法律第百二号）に基づく認定を受けた認証業務又はこれに準ずるものに係る電子証明書及び有効性確認記録 ・弁護士が作成する意見書又は公認会計士等が作成する監査報告書（会計監査報告書を含む）の写し	③
代理人の真偽確認の提出書類 【参考例】 ・印鑑登録証明書 ・代理人の真偽の確認作業管理簿 ・電子署名に用いた電子署名及び認証業務に関する法律（平成十二年法律第百二号）に基づく認定を受けた認証業務又はこれに準ずるものに係る電子証明書及び有効性確認記録	④

申込み諾否を決定した者の氏名 【参考例】 ・e シールに係る電子証明書発行指示書	⑤
承認しなかった理由を記載した帳簿 【参考例】 ・e シールに係る電子証明書発行指示書 ・発行拒否理由通知書の写し	⑥
e シールに係る電子証明書及び e シールに係る電子証明書の発行管理簿	⑦
利用者 e シール符号生成・廃棄に係る帳簿 【参考例】 ・利用者 e シール符号生成・廃棄管理簿	⑧
利用者からの受領書 【参考例】 ・受領書 ・受領書管理簿	⑨

【実施要項第８条の逐条解説】
・16 頁参照

(37)．発行者署名符号に関する帳簿書類関係（実施要項第８条第２項第２号）

（帳簿書類の作成及び保存）
第８条　（略）
二　発行者署名符号に関する帳簿書類で次に掲げるもの
イ　発行者署名符号の作成及び管理に関する記録
ロ　発行者署名検証符号に係る電子証明書の作成及びリポジトリ等における公開に関する記録
ハ　リポジトリ等に公開されている発行者署名検証符号に係る電子証明書を格納するサーバ上や当該発行者署名検証符号に係る電子証明書を送信する通信路上において改ざん防止措置を講じ、改ざん検知時のアラート通知の受信記録等の当該措置が正常に機能していることの記録

以下の①～③の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。

① 発行者署名符号の作成及び管理に関する記録を作成し、保存していること。発行者署名符号の作成及び管理に関する記録とは、以下に関するものを含む。
ア．発行者署名符号の使用範囲の規定
イ．発行者署名符号の生成、保存（バックアップに関するもの）
ウ．発行者署名符号の使用を可能とし、又は不能とする e シールに係る認証業務用設備の設定の変更
エ．発行者署名符号のバックアップ

オ．発行者署名符号の復元
カ．発行者署名符号の廃棄
上記の記録（但し①は除く）には、当該発行者署名符号の作成及び管理を実施した日付並びに実施した者及び当該発行者署名符号の作成及び管理について責任を有する者の識別に関する情報が関連づけられて記録されていること。

② 発行者署名検証符号に係る電子証明書の作成及びリポジトリ等における公開に関する記録を保存していること。
上記の記録には、当該発行者署名検証符号に係る電子証明書の作成及びリポジトリ等における公開を実施した日付並びに実施した者及び当該発行者署名検証符号に係る電子証明書の作成及びリポジトリ等における公開について責任を有する者の識別に関する情報が関連づけられて記録されていること。

③ リポジトリ等に公開されている発行者署名検証符号に係る電子証明書を格納するサーバ上や当該発行者署名検証符号に係る電子証明書を送信する通信路上において講じる改ざん防止措置の改ざん検知時におけるアラート通知の受信に関する記録を作成し、保存していること。
上記の記録には、当該発行者署名検証符号に係る電子証明書を格納するサーバ上や当該発行者署名検証符号に係る電子証明書を送信する通信路上における改ざん防止措置の改ざん検知時におけるアラート通知を受信した日付並びに受信した者及び当該改ざん防止措置の運用時におけるアラート通知の受信について責任を有する者の識別に関する情報が関連づけられて記録されていること。

【必要書類】

必要書類	基準の項番
事務取扱要領	①～③
発行者署名符号の生成及び管理に関する記録 【参考例】 ・発行者署名符号生成･管理に関する帳簿	①
発行者署名検証符号に係る電子証明書の作成及びリポジトリ等における公開の記録 【参考例】 ・発行者署名検証符号に係る電子証明書生成指示書(作成依頼と受信) ・発行者署名検証符号に係る電子証明書生成作業管理簿	②
発行者署名検証符号に係る電子証明書を格納するサーバ上や当該発行者署名検証符号に係る電子証明書を送信する通信路上における改ざん防止措置の改ざん検知時におけるアラート通知の受信記録 【参考例】 ・改ざん防止措置におけるアラート通知の受信記録簿	③

(38). e シールに係る電子証明書の失効に関する帳簿書類関係（実施要項第８条第２項第３号）

（帳簿書類の作成及び保存）
第８条　（略）
三　e シールに係る電子証明書の失効に関する帳簿書類で次に掲げるもの
イ　e シールに係る電子証明書の失効の請求書その他の失効の判断に関する記録
ロ　e シールに係る電子証明書の失効を決定した者の氏名
ハ　e シールに係る電子証明書の失効の請求に対して拒否をした場合においては、その理由を記載した書類
ニ　第７条第９号の失効に関する情報及びその作成に関する記録

以下の①～④の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。

① e シールに係る電子証明書の失効の請求書その他の失効の判断に関する記録（e シールに係る電子証明書の失効の請求者の真偽の確認に使用した資料を含む。）を保存していること。上記の記録には、失効事由を含むこと。
上記の e シールに係る電子証明書の失効の請求書又はその情報（電子署名及び認証業務に関する法律（平成十二年法律第百二号）に基づく認定を受けた認証業務又はこれに準ずるものに係る電子証明書により確認された電子署名が行われているものに限り、その電子署名の有効性を確認した記録も含む。）その他の失効の判断に関する記録については、その受領の日付及び受領した者の識別に関する情報が関連づけられて記録されていること。

② e シールに係る電子証明書の失効を決定した者の氏名及び失効の決定日付を記録し、保存していること。

③ e シールに係る電子証明書の失効の請求に対して拒否をした場合においては、その決定した者の氏名、失効請求拒否の決定日付及びその理由を記載した書類を作成し、保存していること。

④ 実施要項第７条第９号（e シールに係る電子証明書の有効期間内において、利用者から e シールに係る電子証明書の失効の請求があったとき又は e シールに係る電子証明書に記録された事項に事実と異なるものが発見されたときは、遅滞なく当該 e シールに係る電子証明書の失効の年月日その他の失効に関する情報を電磁的方法（電子的方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。以下同じ。）により記録すること。）の失効に関する情報及びその作成に関する記録を作成し、保存していること。
上記の記録には、当該 e シールに係る電子証明書の失効に関する情報の作成を実施した日付並びに実施した者及び当該 e シールに係る電子証明書の失効に関する情報の作成について責任を有する者の識別に関する情報が関連づけられて記録されていること。

【必要書類】

必要書類	基準の項番
事務取扱要領	①～④
失効の請求書その他の失効の判断に関する記録(失効事由を含む) 【参考例】 ・e シールに係る電子証明書失効請求書 ・利用者および代理人の真偽の確認用資料 ・電子署名付き電子証明書失効請求情報 ・電子署名に用いた電子署名及び認証業務に関する法律（平成十二年法律第百二号）に基づく認定を受けた認証業務又はこれに準ずるものに係る電子証明書及び有効性確認記録 ・失効請求、真偽の確認の実施管理簿（確認書） ・失効指示書	①
失効を決定した者の氏名 【参考例】 ・失効指示書 ・失効処理管理簿	②
失効の請求に対して拒否をした理由 【参考例】 ・失効拒否決定書 ・失効処理管理簿 ・失効拒否理由通知書写し	③
全ての失効情報(CRL 等) 【参考例】 ・失効指示書 ・失効処理管理簿	④

(39). 認証事業者の組織管理に関する帳簿書類関係（実施要項第８条第２項第４号）

（帳簿書類の作成及び保存）

第８条　（略）

四　認証事業者の組織管理に関する帳簿書類で次に掲げるもの

イ　第７条第 12 号の規程及びその変更に関する記録

ロ　第７条第 14 号イの事項及びその変更に関する記録

ハ　第７条第 14 号ロの事項及びその変更に関する記録

ニ　認証業務の一部を他に委託する場合においては、委託契約に関する書類

ホ　第７条第 14 号ニの監査の実施結果に関する記録

以下の①～⑥の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。

① 実施要項第７条第 12 号(認証事業者の連絡先､業務の提供条件その他の認証業務の実施に関して、告示第６条第１項に規定する規程を適切に定め､当該規程を電磁的方法により記録し､利用者その他の者からの求めに応じ自動的に送信する方法その他の方法により、利用者その他の者が当該規程を容易に閲覧することができるようにすること｡）の規程及びその変更に関する記録を作成し、保存していること。
上記の記録には、当該 e シールに係る認証業務の実施に関する規程の作成及び変更を実施した日付並びに実施した者及び当該 e シールに係る認証業務の実施に関する規程の作成及び変更について責任を有する者の識別に関する情報が関連づけられて記録されていること。

② 実施要項第７条第 14 号イ（業務の手順）の事項及びその変更に関する記録を作成し、保存していること。
上記の記録には、当該業務の手順に関する事項の作成及び変更を実施した日付並びに実施した者及び当該業務の手順に関する事項の作成及び変更について責任を有する者の識別に関する情報が関連づけられて記録されていること。また､当該業務の手順に関する事項の作成及び変更のうち確認を要する業務については､上記の記録の中に､確認した事実の証跡として､確認結果を文書化した記録が含まれていること。

③ 実施要項第７条第 14 号ロ（業務に従事する者の責任及び権限並びに指揮命令系統）の事項（e シールに係る認証業務に従事する要員に関する組織図又は体制図を含むもの｡）及びその変更に関する記録を作成し、保存していること。
上記の記録には、当該業務に従事する者の責任及び権限並びに指揮命令系統に関する事項の作成及び変更を実施した日付並びに実施した者及び当該業務に従事する者の責任及び権限並びに指揮命令系統に関する事項の作成及び変更について責任を有する者の識別に関する情報が関連づけられて記録されていること。

④ e シールに係る認証業務の一部を他に委託する場合においては、委託契約に関する書類を作成し、保存していること。
上記の記録には、当該委託契約を実施した日付並びに実施した者及び当該委託契約について責任を有する者の識別に関する情報が関連づけられて記録されていること。

⑤ 実施要項第７条第 14 号ニ（業務の監査に関する事項）の監査の実施結果に関する次の記録を作成し、保存していること。
ア．監査実施記録（不定期に実施される監査を含む｡）
イ．監査報告書（定期的に実施される監査に関するもの｡）
ウ．監査結果に基づく是正処置報告書
上記の記録には、当該監査を実施した日付並びに実施した者及び当該監査の実施について責任を

有する者の識別に関する情報が関連づけられて記録されていること。

⑥　情報セキュリティ対策のうち脆弱性が発見された場合の対策等において、是正を必要としない旨の決定を行った場合は、決定の理由及びその根拠についても記録されていること。

【必要書類】

必要書類	基準の項番
事務取扱要領	①～⑥
CPS 及び CPS 変更記録	①
業務手順の変更記録 【参考例】 ・事務取扱要領及びそれ以下の規程文書（改訂記録を含む） ・文書管理規程（文書体系を含む）	②
業務責任などの変更記録 【参考例】 ・指揮命令系統を含む組織図 ・指揮命令系統を含む組織図の変更記録 ・業務責任及び権限規程並びにそれらの変更記録 ・業務発令及び解任発令記録	③
業務委託契約書及び附属覚書	④
監査実施記録 【参考例】 ・監査基準・手順 ・監査事項・内容書 ・質問書等 ・監査実施記録 ・監査報告書 ・是正処置報告書	⑤
監査実施記録 【参考例】 ・是正を必要としない旨の決定に関する記録	⑥

（40）．設備及び安全対策措置に関する帳簿書類関係（実施要項第８条第２項第５号）

（帳簿書類の作成及び保存）

第８条　（略）

五　設備及び安全対策措置に関する帳簿書類で次に掲げるもの

イ　第５条第１号の措置に関する記録（映像によるものを除く。）

ロ　第５条第２号の措置に関する記録（不正なアクセス等があったときのものに限る。）
ハ　第５条第３号の認証業務用設備の動作に関する記録
ニ　第７条第 15 号の許諾に関する記録
ホ　認証業務用設備及び第５条各号の基準に適合するために必要な設備の維持管理に関する記録
ヘ　事故に関する記録
ト　帳簿書類の利用及び廃棄に関する記録

以下の①～⑦の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施していること。

① 実施要項第５条第１号（申請に係る業務の用に供する設備のうち e シールに係る認証業務用設備は、入出場を管理するために e シールに係る認証業務の重要度に応じて必要な措置が講じられている場所に設置されていること。）の措置に関する次の項目を記録し、保存していること。
ア．入退室の日時及び場所
イ．入退室者の識別に関する情報
ウ．入退室に係る装置の操作の記録
エ．警報に関する記録

② 実施要項第５条第２号（e シールに係る認証業務用設備は、電気通信回線を通じた不正なアクセス等を防止するために必要な措置が講じられていること。）の措置に関する次の項目を記録し、保存していること。
ア．ファイアウォール及び侵入検知システムの履歴のうち、異常の状態を示す記録（異常発生の日時、送信元電子計算機の IP アドレス、宛先電子計算機の IP アドレス、使用した通信プロトコル等）
イ．マルウェア検知に係る製品の履歴のうち、マルウェアの検知を示す記録（検知日時、検出元、感染ファイル等）

③ 実施要項第５条第３号（e シールに係る認証業務用設備は、正当な権限を有しない者によって作動させられることを防止するための措置が講じられ、かつ、当該 e シールに係る認証業務用設備の動作を記録する機能を有していること。）の e シールに係る認証業務用設備の動作に関する次の項目を記録し、保存していること。
ア．e シールに係る認証業務用設備の動作に関する記録のうち、通常の業務に係る操作以外の操作に関する記録及び障害に関するもの。

④ 実施要項第７条第 15 号（e シールに係る認証業務用設備により行われる認証業務の重要度に応じて、当該 e シールに係る認証業務用設備が設置された室への立入り及びその操作に関する許諾並びに当該許諾に係る識別符号の管理が適切に行われていること。）の許諾に関する次の項目を記録し、保存していること。
ア．許諾の態様ごとに作成された許諾に係る規定に基づく権限管理の実施の記録を含むもの。

上記の記録には、その実施の日付並びに当該業務を実施した者及び当該業務について責任を有する者の識別に関する情報が関連づけられて記録されていること。

⑤　e シールに係る認証業務用設備及び実施要項第５条各号の基準に適合するために必要な設備及びシステムのライフサイクル管理に関する次の項目を記録し、保存していること。

ア．設備の設置から廃棄に至るライフサイクル管理に関する記録及びシステムの企画から廃棄に至るライフサイクル管理に関する履歴を含むもの。

上記の記録には、その実施の日付並びに当該業務を実施した者及び当該業務について責任を有する者の識別に関する情報が関連づけられて記録されていること。

⑥　事故に関する次の項目を記録し、保存していること。

ア．認証設備室への不正な侵入、e シールに係る認証業務用設備の停止若しくは不正な操作及び認証設備室の入退室管理装置の停止若しくは不正な操作に関する記録（ファイアウォール、侵入検知システム及びマルウェア検知に係る製品の履歴のうち、異常な状態を示す記録を除く。）、それらの障害に関する報告書（障害発生日時を含む障害状況）及びその復旧に関する報告書（復旧日時及び復旧実施者を含む復旧実施結果）を含むもの。

上記の記録には、その実施の日時並びに当該業務を実施した者及び当該業務について責任を有する者の識別に関する情報が関連づけられて記録されていること。

⑦　帳簿書類の利用及び廃棄に関する記録を作成し、保存していること。

上記の記録には、その実施の日付並びに当該業務を実施した者及び当該業務について責任を有する者の識別に関する情報が関連づけられて記録されていること。

【必要書類】

必要書類	基準の項番
事務取扱要領	①～⑦
入退室に関する記録 【参考例】 ・認証設備室の入退室管理記録 ・警報に関する記録 ・非権限者の入退室記録	①
不正アクセスの記録 【参考例】 ・ファイアウォールの設定情報及び異常ログ ・侵入検知システムの異常ログ（異常と判断した理由を含む、管理者への通知メール） ・マルウェア検知に係る製品のマルウェア検知ログ ・セキュリティ監査記録	②

e シールに係る認証業務用設備の動作記録 【参考例】 ・異常操作及び障害に関する記録	③
許諾記録(許諾決定者を含む) 【参考例】 ・権限付与に係る帳簿　(生体認証装置への情報記録、パスワード管理記録等を含む)	③
e シールに係る認証業務用設備関連のライフサイクル管理記録 【参考例】 ・e シールに係る認証業務用設備の保守の記録 ・e シールに係る認証業務用設備の変更履歴 ・バックアップ設備への移行記録 ・施設の保守・管理記録 ・認証設備室の保守・管理記録	⑤
障害及び復旧に関する報告書 【参考例】 ・e シールに係る認証業務用設備の障害及びその復旧に係る報告書 ・入退室管理装置の障害及びその復旧に係る報告書 ・登録用端末設備の障害及びその復旧に係る報告書	⑥
帳簿書類の利用及び廃棄に関する記録 【参考例】 ・CPS、利用者同意書、署名検証者同意書、個人情報保護規程及び事務取扱要領以下の規程文書の利用及び廃棄に関する記録	⑧

(41). e シールに係る認証業務の利用の申込みに関する帳簿書類等の保存期間関係（実施要項第８条第３項）

（帳簿書類の作成及び保存）
第８条　（略）
３　前項第１号から第４号までに掲げる帳簿書類は、当該帳簿書類に係る e シールに係る電子証明書の有効期間の満了日から 10 年間保存しなければならない。

以下の①の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 実施要項第８条第２項第１号から第３号までに掲げる帳簿書類を、当該帳簿書類に係る e シールに係る電子証明書の有効期間の満了日から 10 年間保存していること。

【必要書類】

必要書類	基準の項番
CPS	①
事務取扱要領	①

(42). 設備及び安全対策措置に関する帳簿書類の保存期間関係（実施要項第８条第４項）

（帳簿書類の作成及び保存）
第８条　（中略）
４　第２項第５号に掲げる帳簿書類は、作成した日から認定の更新の日まで保存しなければならない。

以下の①の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 実施要項第８条第２項第４号に掲げる帳簿書類を、作成した日から認定の更新の日まで保存していること。

【必要書類】

必要書類	基準の項番
CPS	①
事務取扱要領	①

(43). 電磁的方法による記録に係る記録媒体による帳簿書類の保存関係（実施要項第８条第５項）

（帳簿書類の作成及び保存）
第８条　（略）
５　第２項各号に掲げる帳簿書類（利用者又はその代理人の署名又は押印がない書類に限る。）は、電磁的方法による記録に係る記録媒体により保存することができる。

以下の①の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 実施要項第８条第２項各号に掲げる帳簿書類（利用者又はその代理人の署名又は押印がない書類に限る。）を電磁的方法による記録に係る記録媒体により保存する場合、記録媒体のライフサイクル管理に関する次の項目を記録し、保存していること。
ア．記録媒体の取得から廃棄に至るライフサイクル管理に関する記録を含むもの。
上記の記録には、その実施の日付並びに当該業務を実施した者及び当該業務について責任を有する者の識別に関する情報が関連づけられて記録されていること。

【必要書類】

必要書類	基準の項番

CPS	①
事務取扱要領	①
記録媒体のライフサイクル管理記録	①

(44). 帳簿書類の原本の保存関係（実施要項第８条第６項）

（帳簿書類の作成及び保存）
第８条　（略）
６　第２項各号に掲げる帳簿書類（前項に規定する書類を除く。）は、その原本を保存しなければならない。

以下の①の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 実施要項第８条第２項各号に掲げる帳簿書類（電磁的方法による記録に係る記録媒体により保存された帳簿書類を除く。）の原本は、権限管理、内部牽制等により改ざんやすり替え等の防止措置を講じて保管されていること。

【必要書類】

必要書類	基準の項番
CPS	①
事務取扱要領	①

(45). 経理的基礎関係（実施要項第９条第１項第１号）

（経理的基礎）
第９条　経理的基礎について、財政の状況（過事業年度に係るものを含む財産目録、貸借対照表、損益計算書、事業計画書等）は次の各号に掲げる要件を満たすこととする。
一　継続的な債務超過がないなど、認定業務の継続的かつ安定した遂行が担保できること。

① 法人設立の日以降の経過年数が３か年以上である場合、過事業年度に係る貸借対照表を用いて、資産の合計額が負債の合計額よりも多い状態が直近３か年以上継続していることを示すこと。

② 法人設立の日以降の経過年数が２か年以上３か年未満である場合、過事業年度に係る貸借対照表を用いて、資産の合計額が負債の合計額よりも多い状態が直近２か年以上継続していることを示すこと。

③ 法人設立の日以降の経過年数が２か年未満である場合、中小企業診断士又は公認会計士等が作成する経営診断書を提出すること。

【必要書類】

必要書類	基準の項番
過事業年度に係るものを含む財産目録、貸借対照表、損益計算書、事業計画書等	①～②
中小企業診断士又は公認会計士等が作成する経営診断書	③

(46). 経理的基礎関係（実施要項第９条第１項第２号）

（経理的基礎）
第９条　（略）
二　賠償責任保険に加入しているなど、損害賠償請求をされた場合に対応できる能力があること。

① 認証事業者の免責や認証事業者が負う損害賠償金支払額について、利用規約等に定めていること。

② ①で定めた規約等に基づいて算出される最大賠償金額に対して、事業計画等におけるサービス対価に基づく収入予測や貸借対照表等で示される資産等で支払うことができることを示すこと。なお、賠償責任保険によって当該損害賠償金の全部又は一部を支払う場合においては、認定を受けようとする e シールに係る認証業務に当該保険が適用されることや実際に保険が支払われる際の金額等について示し、最大賠償金額を支払うことができることを示すこと。

【必要書類】

必要書類	基準の項番
利用規約	①
過事業年度に係るものを含む財産目録、貸借対照表、損益計算書、事業計画書等	②
加入している賠償責任保険の内容（被保険者、保険期間、補償内容、保険金の支払い内容及び保険金支払額等）がわかる文書、賠償責任保険証明書の写し	②

(47). 経理的基礎に係る情報の公表関係（実施要項第９条第２項）

（経理的基礎）
第９条　（略）
２　前項第１号に係る情報については、認定事業者において公表することとする。

① 認証事業者が株式会社である場合、会社法（平成 17 年法律第 86 号）第 440 条第１項及び第２項が定める貸借対照表の公告及び会社法（平成 17 年法律第 86 号）第 939 条第１項に基づき定款で

定めた公告方法により、少なくとも年に１回、財務状況を決算として公表していること。なお、認証事業者が株式会社ではない場合も同様の公告方法により、少なくとも年に１回、財務状況を決算として公表していること。

【必要書類】

必要書類	基準の項番
貸借対照表、損益計算書を含む決算が分かる文書	①

(48). 技術的能力関係（実施要項第 10 条）

（技術的能力）

第 10 条　技術的能力については、e シールに係る認証業務に従事するために必要な技術に関する専門性の優れた要員を配置し、認定業務を継続的に安定して遂行するための教育訓練を行い、それを記録することとする。

以下の①の事項に関して、CPS 及び事務取扱要領等に明確かつ適切に規定し、実施していること。

① 関係要員に対するｅシール技術、電子署名技術、鍵管理技術、セキュリティ技術等に関する業務遂行上に必要な知識、経験を身に付けるための教育訓練については、任命時及び少なくとも年に１回以上の頻度で定期的に実施していること。その教育訓練の記録を作成し、保存していること。

【必要書類】

必要書類	基準の項番
CPS	①
事務取扱要領	①