国税庁認証局運用管理規程

Ver 1.0

令和元年 10 月 1 日

国税庁

改定履歴

版数	日付	内容
1.0	令和元年 10 月 1 日	初版発行

目次

1　はじめに

1.1　概要

国税庁認証局運用管理規程（以下、「CP/CPS」という）は、国税庁（以下、「当庁」という）が運営する「国税庁認証局」（以下、「本認証局」という）の CP（Certificate Policy）及び CPS（Certification Practice Statement）であり、証明書発行（失効も含む）に関して「適用範囲」、「セキュリティ基準」、「審査基準」等の一連の規則を定めるものである。本認証局が発行した電子証明書は、当庁が運営する「免税販売管理システム」（消費税法令に基づき輸出物品販売を経営する事業者等から購入記録情報を受け付けるシステム）に対するアクセスに利用することができる。

本 CP/CPS は、インターネットについて、その仕様等の標準化活動を行なっている組織（IETF：Internet Engineering Task Force）におけるインターネット X.509 PKI 証明書ポリシと認証実施フレームワーク「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」（RFC3647）に従い、利用者証明書の発行、失効及びその他の運用管理等の手続きについて規定した本認証局最高位の規程であり、公開文書である。また、公開鍵基盤（PKI：Public Key Infrastructure。以下「PKI」という。）の構成要素である認証局、利用者及び検証者の義務と責任について規定する。

1.2　文書の名前と識別

本認証局に係るオブジェクト識別子（OID）を表 1.1 に示す。

表 1.1　本認証局に係るオブジェクト識別子

OID	オブジェクト
1.2.392.200127.100.1	国税庁認証局
1.2.392.200127.100.1.1	国税庁認証局運用管理規程（CP/CPS）

1.3　PKI の関係者

1.3.1　認証局

本認証局は、発行局（IA)と当庁（RA）により構成される。

1.3.2　当庁

当庁は、証明書の発行及び失効についての管理を行い、証明書の発行及び失効その他の情報を発行局へ連絡する。

1.3.3　発行局

発行局は当庁からの連絡に基づき証明書の作成、発行、失効及び失効情報の開示及び保管の各業務を行う。

但し、発行局は本 CP/CPS の遵守及び個人情報の厳正な取り扱いを条件に、契約を取り交わすことで業務の一部又は全部を外部に委託することができる。

1.3.4　利用者

利用者とは、証明書を所持し、免税販売管理システムへのアクセスに利用する者である。

1.3.5　検証者

検証者とは、利用者からのアクセスの際に証明書の有効性を確認する者である。

1.3.6　その他の関係者

規定しない。

1.4　証明書の使用方法

1.4.1　適切な証明書の使用

本 CP/CPS で定める証明書は、免税販売管理システムへアクセスする機器を認証するために利用者により使用される。利用者は、利用者自身が適切に管理する機器にのみ証明書をインストールし、証明書を利用するものとする。

1.4.2　禁止される証明書の使用

本認証局より発行される証明書は、本 CP/CPS「1.4.1　適切な証明書の使用」に規定する用途のみに使用するものとする。証明書が用途以外の目的で使用された場合は、本認証局は一切の責任を負わないものとする。

1.5　ポリシ管理

1.5.1　本ポリシを管理する組織

本 CP/CPS の管理組織は、国税庁とする。

1.5.2　問い合わせ先

本 CP/CPS に関する問い合わせ先を以下のように定める。

【問い合わせ先】
窓口：国税庁課税部消費税室
住所：〒100-8978　東京都千代田区霞が関 3-1-1
電話番号：03-3581-4161

1.5.3　CPS のポリシ適合性を決定する者

本 CP/CPS の適合性を決定する者は「1.5.1 本ポリシを管理する組織」の規定に従うものとする。

1.5.4　CPS 承認手続き

規定しない。

1.6　定義と略語

（あ～ん）

- アーカイブ（Archive）
  電子証明書の発行・失効に関わる記録や、認証局のシステム運用に関わる記録等を保管すること。

- 暗号アルゴリズム（Algorithm）
  暗号化／復号には、対になる 2 つの鍵を使う公開鍵暗号と、どちらにも同じ鍵を用いる共通鍵暗号（秘密鍵暗号）がある。前者には RSA、ElGamal 暗号、楕円曲線暗号などがあり、後者には米国政府標準の DES や近年新しく DES の後継として決まった AES などがある。

- 暗号モジュール（Security Module）
  私有鍵や証明書等を安全に保管し、鍵ペア生成や署名等の暗号操作を行うハードウェア又はソフトウェアのモジュール。

- エンドエンティティ（EndEntity）
  証明書の発行対象者の総称。公開鍵ペアを所有している実体（エンティティ）で、利用者証明書を利用するもの。（個人、組織、デバイス、アプリケーション

など）なお、認証局はエンドエンティティには含まれない。

- オブジェクト識別子（Object Identifier）
  オブジェクトの識別を行うため、オブジェクトに関連付けられた一意な値。

- 鍵長（Key Length）
  鍵データのサイズ。鍵アルゴリズムに依存する。暗号鍵の強度は一般に鍵の長さによって決まる。鍵長は長ければ長いほど解読困難になるが、署名や暗号メッセージを作成する際の時間もかかるようになる。情報の価値を見計らって適切な鍵長を選択する必要がある。

- 鍵の預託（Key Escrow）
  第三者機関に鍵を預託すること。

- 鍵ペア（Key Pair）
  私有鍵とそれに対応する公開鍵の対。

- 活性化（Activate）
  鍵を署名などの運用に使用することができる状態にすること。逆に、使用できなくすることを非活性化という。

- 危殆化（Compromise）
  私有鍵等の秘密情報が盗難、紛失、漏洩等によって、その秘密性を失うこと。

- 検証者（Relying Party）
  文書の署名を利用者証明書の公開鍵で検証する者。

- 公開鍵（Public Key）
  私有鍵と対になる鍵で、署名の検証に用いる。公開鍵はたとえ公開されても秘密の私有鍵を類推することが困難である。

- 公開鍵証明書（Public Key Certificate）
  利用者の名義と公開鍵を結合して公開鍵の真正性を証明する証明書で、印鑑登録証明書に相当する。電子証明書あるいは単に証明書ともいう。公開鍵証明書には、公開鍵の利用者情報、公開鍵、認証局の情報、その他証明書の利用規則等が記載され、認証局の署名が付される。

- 自己署名証明書（Self Signed Certificate）
  認証局が自身のために発行する電子証明書。発行者情報と利用者情報が同じである。

- 失効（Revocation）
  有効期限前に、何らかの理由（盗難・紛失など）により電子証明書を無効にすること。基本的には、本人からの申告によるが、緊急時には認証局の判断で失効されることもある。

- 私有鍵（Private Key）
  公開鍵と対になる鍵。公開せず、他人に漏れないように鍵の利用者だけが管理する。私有鍵で署名したものは、それに対応する公開鍵でのみ検証が可能である。

- 証明書失効リスト（Certificate Revocation List、Authority Revocation List）
  失効した電子証明書のリスト。エンドエンティティの証明書の失効リストをCRL といい、認証局の証明書の失効リストを ARL という。

- 証明書配付システム
  利用者私有鍵及び利用者証明書をインターネット経由で利用者に配付するためのシステム。利用者の本人確認のため認証機能を有している。

- 証明書発行要求（Certificate Signing Request）
  請者から認証局に電子証明書発行を求めるための要求。電子証明書を作成するための元となる情報で、その内容には、手続者の固有の ID、公開鍵などの情報が含まれる。

- 証明書ポリシ（Certificate Policy：CP）
  共通のセキュリティ要件を満たし、特定のコミュニティ及び／又はアプリケーションのクラスへの適用性を指定する、名前付けされた規定の集合。

- 手続者（Applicant）
  認証局に電子証明書の発行の手続を行う主体のこと。

- 電子署名（Digital Signature）

電子文書の正当性を保証するために付けられる署名情報。公開鍵暗号などを利用し、相手が本人であることを確認するとともに、情報が送信途中に改ざんされていないことを証明することができる。公開鍵暗号方式を用いて生成した署名はデジタル署名ともいう。

- 当庁（Registration Authority：RA）
  国税庁。

- 登録審査室
  認証業務用設備のうち、登録業務用設備のみが設置された室をいう。

- 認証局（Certification Authority：CA）
  電子証明書を発行する機関。認証局は、公開鍵が間違いなく本人のものであると証明可能にする第三者機関で、公正、中立な立場にあり信頼できなければならない。

- 認証局運用管理規程（Certification Practice Statement：CPS）
  証明書ポリシに基づいた認証局運用についての規定集。認証局が電子証明書を発行するときに採用する実践に関する表明として位置付けられる。

- 認証設備室
  認証業務用設備（電子証明書の作成又は管理に用いる電子計算機その他の設備）が設置された室をいう。ただし、登録業務用設備のみが設置される場合を除く。

- 発行局（Issuer Authority）
  電子証明書の作成・発行を主として発行業務を行う機関。発行局は、認証局の機能のうち、一部の業務を行う。

- ハッシュ関数（Hash Function）
  任意の長さのデータから固定長のランダムな値を生成する計算方法。生成した値は「ハッシュ値」と呼ばれる。ハッシュ値は、ハッシュ値から元のデータを逆算できない一方向性と、異なる 2 つのデータから同一のハッシュ値が生成される衝突性が困難であるという性質を持つ。この性質からデータを送受信する際に、送信側の生成したハッシュ値と受信側でデータのハッシュ値を求めて両者を比較し両者が一致すれば、データが通信途中で改ざんされていないことが確認できる。

- プロファイル（Profile）
  電子証明書や証明書失効リストに記載する事項及び拡張領域の利用方法を定めたもの。

- リポジトリ（Repository）
  電子証明書及び証明書失効リスト、その他公開文書を公開するシステム。

- 利用者（Subscriber）
  証明書の発行を受け、証明書を利用して免税販売管理システムにアクセスする者

- 利用者証明書
  認証局から利用者に対して発行された公開鍵証明書のこと。

（A～Z）

- ARL（Authority Revocation List）
  認証局の証明書の失効リスト、証明書失効リストを参照のこと。

- CA（Certification Authority）
  認証局を参照のこと。

- CA 証明書
  自己署名証明書を参照のこと。

- CPS（Certification Practice Statement）
  認証局運用管理規程を参照のこと。

- CRL（Certificate Revocation List）
  エンドエンティティの証明書の失効リスト、証明書失効リストを参照のこと。

- CRL 検証
  証明書失効情報が、認証局が発行する CRL に記載されているかを確認すること。

- CSR（Certificate Signing Request）
  証明書発行要求を参照のこと。

- DN（Distinguished Name）
  X.500 規格において定められた識別名。X.500 規格で識別子を決定することによって、利用者の一意性を保障する。

- FIPS 140-2（Federal Information Processing Standard）
  FIPS とは米国連邦情報処理標準で、FIPS140-2 は暗号モジュールが満たすべきセキュリティ要件を規定したもの。各セキュリティ要件に対して 4 段階のセキュリティレベル（最低レベル 1～最高レベル 4）を定めている。

- IA（Issuer Authority）
  発行局を参照のこと。

- OID（Object ID）
  オブジェクト識別子を参照のこと。

- PKI（Public Key Infrastructure）
  公開鍵基盤。公開鍵暗号化方式という暗号技術を基に認証局が公開鍵証明書を発行し、この証明書を用いて署名／署名検証、暗号／復号、認証を可能にする仕組み。

- RA（Registration Authority）
  登録局を参照のこと。

- RSA
  公開鍵暗号方式の一つ。Rivest、Shamir、Adleman の 3 名によって開発され、その名前をとって名付けられた。巨大な整数の素因数分解の困難さを利用したもので、公開鍵暗号の標準として普及している。

- SHA-1（Secure Hash Algorithm 1）
  ハッシュ関数の一つ。任意の長さのデータから 160bit のハッシュ値を作成する。

- SHA-256（Secure Hash Algorithm 256）

ハッシュ関数の一つ。任意の長さのデータから 256bit のハッシュ値を作成する。

- X.500
  ITU-T/ISO が定めたディレクトリサービスに関する国際基準。

- X.509
  ITU-T/ISO が定めた電子証明書及び証明書失効リストに関する国際標準。
  X.509v3 では、電子証明書に拡張領域を設けて、電子証明書の発行者が独自の情報を追加することができる。

2　公開及びリポジトリの責任

2.1　リポジトリ

リポジトリは認証局の証明書及び利用者証明書の失効情報を保持し、24 時間 365 日利用可能とする。ただし、システムの保守などの理由により、一時的にリポジトリを利用できない場合もある。

2.2　証明書情報の公開

本認証局は、以下の情報を検証者と利用者が入手可能とする。

- 本認証局の CA 証明書
  https://www.eppcert.jp/ntaca/repository/
- CRL
  http://www.eppcert.jp/ntaca/rlist/ntacag1.crl

2.3　公開の時期又はその頻度

認証局は、認証局に関する情報が変更された時点で、その情報を公開するものとする。証明書失効についての情報は、本 CP/CPS「4.9　証明書の失効と一時停止」に従うものとする。

2.4　リポジトリへのアクセス管理

リポジトリに公開する情報へのアクセス制御は行なわない。

3　識別及び認証

3.1　名称決定

3.1.1　名称の種類

本認証局が発行する電子証明書の発行者名（Issuer Name）及び利用者名（Subject Name）は、国際電気通信連合（ITU：International Telecommunication Union）で標準化されているディレクトリに関する一連の規格 X.500 識別名（DN：Distinguished Name）の形式に従い設定する。

3.1.2　名称が意味を持つことの必要性

本 CP/CPS により発行する証明書の相対識別名は、検証者によって判別できるよう意味のあるものとする。証明書に設定されている内容の詳細を表 3.1 に示す。

表 3.1　免税販売管理システム用クライアント証明書の利用者情報（subject）

属性	値	説明	備考
c（国名） 「OID：2.5.4.6」 countryName	“c=JP”で固定 （Printable）	日本を示す先の国名を設定する。（英字）	―
o（組織名） 「OID：2.5.4.10」 organizationalName	“o=Tax Exemption Management System” （Printable）	免税販売管理システムの名称を設定する（英字）	必須
ou（組織単位名） 「OID：2.5.4.11」 organizationalUnitname	例 “ou=NTAE1234567890” （Printable）	証明書固有番号を設定する。（英数字）	必須
cn（一般名） 「OID：2.5.4.3」 commonName	例 “cn=123456789012300000000” （Printable）	利用者が有する識別符号を設定する。（数字）	必須

3.1.3　利用者の匿名性又は仮名性

本認証局が発行する利用者証明書には利用者が有する識別符号のみが設定されている。

3.1.4　種々の名称形式を解釈するための規則

本認証局が発行する利用者証明書に記載される名称は、ITU-T X.500 識別名（DN）

の規定及び本 CP/CPS「3.1.2　名称が意味を持つことの必要性」の規定に従うものとする。

3.1.5　名称の一意性

利用者証明書に記載される利用者情報（subject）の識別名（DN）は、本認証局が発行した利用者証明書において一意に割り当てる。

3.1.6　認識、認証及び商標の役割

規定しない。

3.2　初回の本人性確認

3.2.1　私有鍵の所持を証明する方法

本認証局は、発行局にて利用者鍵ペア及び利用者証明書を生成し、利用者鍵ペア及び利用者証明書を証明書配付システムに格納する。利用者鍵ペア及び利用者証明書は、利用者が、当庁に届け出た情報及び当庁から通知を受けた識別符号情報を認証情報として証明書配付システムから取得する方法により、利用者へ発行する。このため、利用者私有鍵の所持確認については行なわない。

3.2.2　利用者の認証

本認証局は、当庁において証明書の発行及び失効その他に係る届出等を受け付けた際に、当庁がこれに応ずるか判断する。

3.2.3　利用者の個人の認証

本認証局は、個人事業者に対して証明書の発行を行う場合があるが、利用者証明書の発行及び失効その他に係る届出等に応ずるかの判断は、個人及び法人で区別しない。

3.2.4　確認しない利用者の情報

規定しない。

3.2.5　機関の正当性確認

本 CP/CPS「3.2.2　利用者の認証」で規定された利用者の確認を実施することにより、正当性確認を行う。

3.2.6　相互運用の基準

規定しない。

3.3　鍵更新手続時の本人性確認及び認証

3.3.1　通常の鍵更新時の本人性確認及び認証

本認証局は、利用者証明書の鍵更新時において、当該組織が有効な利用者証明書を保有している場合は、本人性確認及び認証を省略することができる。当該組織が有効な利用者証明書を保有していない場合は、初回の本人性確認と同様の手順とする。

なお、利用者証明書の有効期限切れが近づいた時期に、本認証局からその旨を通知する場合がある。

3.3.2　証明書失効後の鍵更新の本人性確認及び認証

初回の本人性確認と同様の手順とする。

3.4　失効手続時の本人性確認及び認証

初回の本人性確認と同様の手順とする。

4　証明書のライフサイクルに対する運用上の要件

4.1　証明書発行手続

4.1.1　証明書の利用者となる者

証明書の利用者は、次の事業者のうち本 CP/CPS に、同意した者とする。

- 輸出物品販売場を経営する事業者のうち証明書の利用を希望する者
- 臨時販売場を設置する事業者のうち証明書の利用を希望する者
- 承認送信事業者
- その他証明書の利用が必要である者

4.1.2　証明書の発行を受けるための手続

証明書の発行を受けるための手続は、次の手続による。

- 輸出物品販売場における購入記録情報の提供方法等の届出手続（変更手続を含む）
- 承認送信事業者承認申請手続
- その他証明書の利用のために当庁が定めた手続

なお、本 CP/CPS で規定する内容に同意したうえでこれらの手続を行うものとする。

4.2　証明書の発行を受けるのための手続の内容

4.2.1　本人性及び資格確認

証明書の発行を受けるための手続を行った者の本人性及び資格確認は、当庁が定める事務手続により当庁の担当者が行う。発行局は、本人性及び資格確認は、一切行わない。

4.2.2　証明書の発行手続の却下

当庁は、証明書の発行を行わない場合は、手続を行った者に対して手続の取り下げを求め、又は、手続の効力がないことを連絡する。

4.2.3　証明書発行手続き期間

規定しない。

4.3　証明書発行

4.3.1　証明書発行時の認証局の機能

1. 本認証局は、当庁が、証明書の発行に必要な情報を発行局に連絡する。
2. 発行局は、認証設備室にて当庁から連絡を受けた発行に必要な情報を CA システムに登録し、利用者鍵ペア、利用者証明書を生成し、生成した利用者の秘密鍵と利用者証明書を PKCS#12 形式で証明書配付システムに登録する。このとき生成された利用者の秘密鍵は証明書配付システムに登録後、CA システムから完全に削除される。

4.3.2　証明書発行後の通知

本認証局は、利用者へ新証明書を発行したことの通知は行わない。

4.4　証明書の受取

4.4.1　証明書の受取

本認証局は、証明書配付システムに登録した利用者証明書が、取得されたことをもって証明書の受取が正常に行われたものとみなす。

4.4.2　認証局による証明書の公開

本認証局は、利用者証明書の公開は行わない。

4.4.3　他のエンティティに対する認証局による証明書発行通知

本認証局は、他エンティティに対する証明書発行通知は行わない。

4.5　鍵ペアと証明書の利用目的

4.5.1　利用者の私有鍵と証明書の利用目的

利用者は、私有鍵を本 CP/CPS「1.4.1　適切な証明書の使用」に規定する用途のみに使用できる。また、本認証局は、利用者証明書が用途以外の目的で使用された場合には、一切の責任を負わない。

4.5.2　検証者の公開鍵と証明書の利用目的

検証者は、利用者の認証を行う用途で公開鍵と証明書を利用する。

4.6　証明書更新

本 CP/CPS に則り認証局から発行される証明書は、鍵更新を伴う更新のみを許可する。従って、鍵の更新を伴わない証明書更新は行わない。

4.7　証明書の鍵更新（鍵更新を伴う証明書更新）

4.7.1　証明書鍵更新の要件

本認証局が発行する利用者秘密鍵は、自動的に更新されない。利用者証明書の有効期間が切れると同時に、鍵も無効となる。

但し、利用者証明書及び鍵の更新が必要な場合は、初回の証明書発行手順と同様に CA システムを使用して利用者鍵ペア、利用者証明書を生成し、生成した加利用者の秘密鍵と利用者証明書を PKCS#12 形式で証明書配付システムに登録することができる。

4.7.2　鍵更新手続者

本 CP/CPS「4.1.1　証明書の利用者となる者」と同様とする。

4.7.3　鍵更新手続の処理手順

本 CP/CPS「4.2.1　本人性及び資格確認」に定める本人性確認並びに資格確認を行う。なお、利用者が有効な証明書を保有している場合、本人性確認並びに資格確認を省略することができる。

4.7.4　利用者への新証明書発行通知

本認証局が利用者へ新証明書を準備したことを通知することを妨げない。

4.7.5　鍵更新された証明書の受取

鍵更新された証明書の受取については本 CP/CPS「4.4.1　証明書の受取」に同じとする。

4.7.6　認証局による鍵更新証明書の公開

本認証局は、利用者証明書の公開は行わない。

4.7.7　他のエンティティへの証明書発行通知

本認証局は、他エンティティに対する証明書発行通知は行わない。

4.8　証明書変更

本 CP/CPS に則り認証局から発行される利用者証明書は、証明書変更を行わない。

4.9　証明書の失効と一時停止

4.9.1　証明書失効の要件

認証局は、次の場合に証明書を失効するものとする。

＜利用者による失効手続＞

利用者による失効手続は次の場合に行うものとする。

- 輸出物品販売場の廃止や、購入記録情報の提供方法等の変更等の理由により、利用者証明書の利用を停止する場合
- 利用者私有鍵の紛失、盗難、不正使用、危殆化又は危殆化の恐れ等の理由により、利用者が利用者証明書を失効させる必要があると判断した場合

本認証局は、利用者からの失効手続があった場合は、理由の如何に関わらず証明書の失効を行う。

＜認証局による失効の場合＞

認証局による利用者証明書の失効については、次の場合に行う。

- 利用者が、本 CP/CPS に従って証明書を利用していないと認証局が判断した場合
- 利用者私有鍵の危殆化が認識されたか、その疑いがある場合
- 本 CP/CPS に従って利用者証明書が適切に発行されなかったと認証局が判断した場合
- 利用者の特定ができない場合で、緊急に失効する必要があると認証局が判断した場合
- 認証局の私有鍵が危殆化又は、危殆化の恐れがある場合
- 認証局のオペレーションミスにより証明書の記載事項に誤りがあった、もしくは証明書の不具合により証明書が使用できない場合
- その他の事由により証明書の記載事項に誤りがあった場合
- 認証局が認証業務を廃止する場合

4.9.2　失効手続者

利用者とする。

4.9.3　失効手続

失効手続きは、以下のとおりとする。

＜利用者からの失効手続の場合＞

利用者からの失効手続は次の手続による。

- 輸出物品販売場廃止届出手続
- 輸出物品販売場における購入記録情報の提供方法等の変更届出手続
- 承認送信事業者不適用申請手続
- 臨時販売場を設置する事業者の不適用届出手続

＜認証局による失効の場合＞

本認証局は「4.9.1　証明書失効の要件」の中の認証局からの失効の場合は、当該証明書を特定し、失効の事由の真偽の確認を実施する。また、失効事由が真実であった場合は速やかに証明書を失効させることがある。

4.9.4　失効における猶予期間

「4.9.1　証明書失効の要件」に規定されている事由が発生した場合であっても、認証局の判断により、失効まで一定の猶予期間を設けることを妨げない。

4.9.5　認証局による失効手続の処理期間

規定しない。

4.9.6　検証者の失効情報確認の要件

検証者は､被認証者の公開鍵を使う時に有効な CRL を使用して失効の有無を確認し、証明書状態の確認を行うものとする。

4.9.7　CRL 発行頻度

本認証局は、CRL の発行頻度を決定し、決定した頻度に従い CRL の更新を行う。

1. CRL の有効期間を 60 日とし、24 時間ごとに毎日午前 3 時に更新する。
2. 利用者証明書の失効を行った場合、即時に CRL の更新は行わず、次回更新時（午前 3 時）に CRL を更新する。

3. 認証局私有鍵が危殆化し、又はその恐れがある場合は、発行した全ての証明書を失効させ、CRL を発行する。

4.9.8 CRL/ARL が公開されない最大期間

規定しない。

4.9.9 オンラインでの失効／ステータス情報の入手方法

規定しない。

4.9.10 オンラインでの失効確認要件

規定しない。

4.9.11 その他利用可能な失効情報確認手段

規定しない。

4.9.12 鍵の危殆化に関する特別な要件

規定しない。

4.9.13 証明書一時停止の要件

一時停止は行わない。

4.9.14 一時停止手続者

一時停止は行わない。

4.9.15 一時停止手続の処理手順

一時停止は行わない。

4.9.16 一時停止期間の制限

一時停止は行わない。

4.10 証明書ステータスの確認サービス

4.10.1 運用上の特徴

規定しない。

4.10.2 サービスの利用可能性

規定しない。

4.10.3　オプショナルな仕様

規定しない。

4.11　利用の終了

利用者が、証明書の利用を終了する場合、本 CP/CPS「4.9　証明書の失効と一時停止」に規定する失効手続きを行うものとする。

4.12　私有鍵預託と鍵回復

規定しない。

4.12.1　預託と鍵回復ポリシ及び実施

規定しない。

4.12.2　セッションキーのカプセル化と鍵回復のポリシ及び実施

規定しない。

5　建物・関連設備、運用のセキュリティ管理

5.1　建物及び物理的管理

5.1.1　施設の位置と建物構造

本認証業務のための設備を維持・運用するための場所である認証設備室については、以下のセキュリティを確保する。

1. 認証設備室は、外部からの侵入が容易にできないようセキュリティが確保された建物の内部に、物理的な仕切りに囲まれた区画（「サイト」ともいう。）の施設とし、物理的な階層構造の中に設置する。
2. 認証設備室については、独自のセキュリティ基準を設けることにより、認証業務用設備が物理的に安全な環境において運用する。
3. 認証設備室及び認証設備室が設置された建物等には、その施設に認証業務用設備があることを示す掲示及びパンフレット等への記載を一切行わない。

5.1.2　物理的アクセス

認証設備室への入退室においては、以下のセキュリティを確保する。

1. 認証設備室への入室においては、入室を許可されない者の不正侵入を防止するため、入室を許可された運営要員の生体をあらかじめ生体認証装置に登録し、生体が登録された運営要員の生体認証が行なわれることにより、入室を可能とするとともに、生体認証装置により入室の記録が行われる。
2. 認証設備室への入室においては、入室操作の時間と入室操作の試行回数をチェックすることにより、許可されない者が室内に不正侵入できないようにする。また、そのチェックにより検知した異常については、24 時間監視を行っている監視室へ警告する。
3. 認証設備室の入室及び退室並びに認証設備室内での作業については、監視カメラにより、運営要員の活動を記録する。
4. 認証業務用設備の補修工事等に際し、入室権限を有する運営要員以外の者が認証設備室へ入室しなければならない場合は、IA 責任者の事前の許可を得て、入室権限を有する作業監督者が同行し監督することにより、認証設備室への入室ができるものとする。

5.1.3　電源及び空調設備

認証業務用設備については、商用電源が断たれた場合に CA システムの異常停止又は

サービスの中断を防止するために、設置された無停電源装置（UPS：Uninterruptible Power Supply）及び自家発電装置からの給電を行う。また、認証設備室は、空調システムにより温度及び湿度の制御を行う。

5.1.4　水害及び地震対策

認証設備室は、建物の 2 階以上に設置され、洪水・津波等の水害から守り、漏水対策も施す。また、耐震対策を講じた建物に設置するとともに、認証設備室に設置される機器については、地震による移動及び転倒等を防止する措置を講じる。

5.1.5　防火設備

認証設備室は、建築基準法に適合した耐火建物の中に設置する。また、認証設備室は、建築基準法に適合した防火区画に設置し、自動火災報知器及び消火設備を設置する。

5.1.6　記録媒体

アーカイブデータ、バックアップデータを含む媒体は、施錠された安全な保管場所で管理する。

5.1.7　廃棄物の処理

機密扱いとする情報を含む書類・記録媒体の廃棄については、情報の漏洩がないよう、以下の方法で行う。

1. 紙等に記録された情報
   - 文書等については、シュレッダー等により、記載された内容を確認できないよう処理する。
2. 補助記録媒体等に記録されたデータ
   - 磁気テープ等については、無効データの上書き等を行なった上で完全消去する等により、記録されたデータを確認できないよう処理する。また、補助記録媒体の物理的な破壊により、記録されたデータを復元できないよう処理する。
3. コンピュータ機器等に記録されたデータ
   - コンピュータディスク、暗号化装置等については、完全な初期化を行うことにより、記録されたデータを確認できないよう処理する。また、本認証局の CA 私有鍵のバックアップが格納された記録媒体については、物理的な破壊により、記録されたデータを復元できないよう処理する。

5.1.8　施設外のバックアップ

規定しない。

5.2　手続的管理

5.2.1　信頼すべき役割

本認証業務に携わる運営要員とその業務は、表 5.1 に示す。

表 5.1　本認証局の運営要員の役割

運営要員の区分	業務
認証局責任者	・　認証局運営方針の決定及び運営方針変更の決定 ・　CP/CPS の開示及び変更の承認 ・　本認証局の監査実施の指示 ・　CA 秘密鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における対応の統括・最終決定
当庁責任者	・　受付審査担当者の事務処理の監督・指導 ・　CA 秘密鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における作業指示
受付審査担当者	・　発行手続、失効手続に関する書類の受付及び審査 ・　発行局に連絡する利用者情報の管理
IA 責任者	・　IA 操作員との合議制操作による CA 秘密鍵の生成 ・　生成された CA 秘密鍵のバックアップの保管 ・　IA 操作員との合議制捜査による CA 秘密鍵のバックアップ及びバックアップからのリストア ・　IA 操作員に対する CA 証明書及び利用者証明書の発行及び失効指示 ・　認証設備室の維持管理及び認証設備室のセキュリティ監査イベント（アーカイブ）の採取及び検査 ・　CA 秘密鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における対応
IA 操作員	・　IA 責任者との合議制操作による CA 秘密鍵の生成 ・　生成された CA 秘密鍵のバックアップの保管 ・　IA 責任者との合議制操作による CA 秘密鍵のバックアップ及びバックアップからのリストア ・　CA システムの起動及び停止 ・　利用者情報の取得及び CA システムへの登録 ・　CA 証明書、利用者証明書の発行処理及び失効処理

運営要員の区分	業務
	・ CA システムのバックアップ ・ CA 秘密鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における対応
システム保守員	・ 生成された CA 秘密鍵のバックアップの保管 ・ CA システムのハードウェアの管理 ・ CA 秘密鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における対応

5.2.2 職務ごとに必要とされる人数

本認証業務に携わる運営要員の最低限必要な人数は、各運営要員 1 人とする。

5.2.3 個々の役割に対する本人性確認と認証

CA システムへのアクセスには、運用関係者に発行された電子証明書を使用した本人しか持ち得ない私有鍵を用いた強固な認証を行う。

5.2.4 職務分轄が必要になる役割

CA 私有鍵について、本 CP/CPS「表 5.1　本認証局の運営要員の役割」に示す運営要員が実施する重要操作においては、適切な複数人による管理を採用する。

5.3 要員管理

信頼される役割を担う者は、認証局の業務に関して、操作や管理の責務を負う。認証局の運営においては、これら役割の信頼性、適合性及び合理的な職務執行能力を保証する人事管理がなされ、そのセキュリティを確立するものとする。

5.3.1 資格、経験及び身分証明の要件

認証局の業務運営に関して信頼される役割を担う者は、認証局運営組織の採用基準に基づき採用された職員とする。CA システムを直接操作する担当者は、専門のトレーニングを受け、PKI の概要とシステムの操作方法等を理解しているものを配置する。

本認証局の業務の一部を外部委託する場合、又は本認証局の一部を外部のサービスを利用して実現する場合の、外部委託先の要員に関する要件は本書では規定しない。

5.3.2 研修要件

信頼される役割を担う者は、その業務を行うための適切な教育を定期的に受け、以降必要に応じて再教育を受けなければならない。

5.3.3　再研修の頻度及び要件

規定しない。

5.3.4　職務のローテーションの頻度及び要件

規定しない。

5.3.5　認められていない行動に対する制裁

認証業務に携わる者が、定められた権限を逸脱し認められていない行動を行った場合、その行為が故意か過失かに関わらず、定められた罰則が適用されるものとする。

5.3.6　独立した契約者の要件

規定しない。

5.3.7　要員へ提供する資料

認証業務に携わる者は、次の文書にアクセスすることができる。ただし、その文書については、認証業務に携わる者の役割に応じてアクセスできる者を定めるとともに、定められた者のみがアクセスできるよう制限された場所に保管されるものとする。

1. 本 CP/CPS を含む認証局の運用に関する規程
2. 事務取扱要領などの手順書
3. 認証設備に関する仕様書および操作マニュアル
4. CA システムに関する仕様書および操作マニュアル

5.4　監査ログの取扱い

5.4.1　記録するイベントの種類

本認証局は、CA システム、リポジトリ及び認証設備室内のネットワーク機器に関する記録である監査イベントを監査ログとして記録する。監査ログには、以下のものが含まれる。また、イベントを起こした者への通知は行わない。

1. CA システムの起動・停止等の稼動ログ及び機能変更等の操作ログ
2. CA システムにおける利用者の登録、利用者証明書の発行要求及び失効要求並びに利用者証明書の生成処理及び失効処理に関するログ
3. リポジトリにおける掲載情報の変更記録

4. ファイアウォール等の認証設備室内のネットワークログ
5. 認証設備室の入退室管理装置の動作ログ及び監視カメラの映像記録

5.4.2 監査ログを処理する頻度

本認証局は、監査ログを必要に応じて適宜検査する。

5.4.3 監査ログを保存する期間

監査ログ（認証設備室の監視カメラの映像記録を除く）は、1 年間保存する。

5.4.4 監査ログの保護

認証局は、認可された人員のみが監査ログにアクセスすることができるよう、適切なアクセスコントロールを採用し、権限を持たない者の閲覧や、改ざん、不正な削除から保護する。

5.4.5 監査ログのバックアップ手続

監査ログは、月 1 回の頻度でバックアップする。

5.4.6 監査ログの収集システム（内部対外部）

規定しない。

5.4.7 イベントを起こしたサブジェクトへの通知

規定しない。

5.4.8 脆弱性評価

規定しない。

5.5 記録の保管

5.5.1 アーカイブ記録の種類

本認証局は、認証業務に関わる以下の書類及び情報をアーカイブする。

- 本認証局から発行する証明書の発行/失効に関する処理履歴
- CRL の発行に関する処理履歴
- CA 証明書
- 利用者証明書

- 証明書発行要求に関わる書類
- 証明書失効要求に関わる書類
- CA 証明書の発行、更新及び失効に関わる書類

5.5.2　アーカイブを保存する期間

アーカイブする情報は、記録が作成されてから最低 10 年間は保存する。

5.5.3　アーカイブの保護

アーカイブ情報の収められた媒体は物理的セキュリティによって保護され、許可された者しかアクセスできないよう制限された施設に保存され、権限を持たない者の閲覧や持ち出し、改ざん、消去から保護する。また、自然災害、火災及び盗難などから保護された場所に保存する。

5.5.4　アーカイブのバックアップ手続

アーカイブは、月 1 回の頻度でバックアップを実施する。

5.5.5　記録にタイムスタンプをつける要件

本 CP/CPS「5.5.1　アーカイブ記録の種類」で規定する情報の記録時間は、処理を行った日付を記録する。

5.5.6　アーカイブ収集システム（内部対外部）

アーカイブの収集機能は、本認証局の CA システム及びリポジトリの機能とし、業務及びセキュリティに関する重要な事象をアーカイブとして収集する。

5.5.7　アーカイブ情報を入手し、検証する手続

本 CP/CPS「5.5.1　アーカイブ記録の種類」で規定する情報については、本 CP/CPS「5.5.3　アーカイブの保護」で規定する方法により、可用性と完全性が確保された形で安全に保管される。

5.6　鍵の切り替え

規定しない。

5.7　危殆化及び災害からの復旧

5.7.1　災害及び CA 私有鍵危殆化からの復旧手続き

本認証局は、想定される以下の脅威に対する復旧手順を規定し、関係する認証局運営要員全員に適切な教育・訓練を実施する。

- CA 私有鍵の危殆化
- 火災、地震、事故等の自然災害
- システム（ハードウェア、ネットワーク等）の故障

5.7.2　コンピュータのハードウェア、ソフトウェア、データが破損した場合の対処

ハードウェア、ソフトウェア、データが破壊又は損傷した場合、バックアップ用のハードウェア（保守)、ソフトウェア、バックアップデータを用いて、速やかに復旧作業を行い、合理的期間内に認証局業務を再開する。また、障害発生時の際には、可能な限り速やかに、利用者、検証者にリポジトリにより通知する。

5.7.3　CA 私有鍵が危殆化した場合の対処

CA 私有鍵が危殆化又その恐れが生じた場合は、認証局責任者の判断により、速やかに認証業務を停止するとともに、認証局で規定された手続きに基づき、全ての利用者証明書の失効を行い、CRL を開示し、CA 私有鍵を廃棄する。更に、原因の追求と再発防止策を講じる。

5.7.4　災害等発生後の事業継続性

災害などにより、認証施設及び設備が被災し、通常の業務継続が困難な場合には、認証局で規定された手続きに基づき、利用者及び検証者に情報を公開する。

5.8　認証局又は登録局の終了

以下のとおり規定する。

1. 本認証局の廃止日までに有効期間の残っている全ての利用者証明書を失効し、その失効リストはリポジトリに 3 ヶ月公開する。
2. 本認証局を廃止する場合、廃止日の 90 日前までに利用者にその旨をお知らせするよう努めるとともに、リポジトリに廃止理由を公開する。
3. 廃止時には、CA 私有鍵を完全に初期化し、そのバックアップ媒体を物理的に完全に破壊する。

6　技術的なセキュリティ管理

6.1　鍵ペアの生成と実装

6.1.1　鍵ペアの生成

本認証局の鍵ペアは、認証設備室内で、複数人の立会いのもと、権限を持った者による操作により生成される。

利用者の鍵ペアは、厳重な管理のもと認証設備室で生成され、証明書配付システムに登録する。証明書配付システムに登録後利用者の鍵ペアは、本認証局内の設備より削除する。

6.1.2　利用者への私有鍵の送付

利用者の私有鍵は認証局で生成されるため、証明書配付システムによって、利用者に引き渡されるものとする。なお、認証局の判断によりその他の方法を採ることを妨げない。

6.1.3　認証局への公開鍵の送付

利用者の公開鍵は本認証局で生成するため、利用者から本認証局へ配送されない。

6.1.4　検証者への CA 公開鍵の配付

CA 公開鍵は、検証者によるダウンロードを可能とするために、本認証局のリポジトリにて公開するものとする。

6.1.5　鍵のサイズ

本認証局で生成する鍵のサイズは、以下のとおりとする。

- 本認証局の鍵のサイズは、RSA アルゴリズムの 2,048 ビット
- 利用者証明書の鍵のサイズは、RSA アルゴリズムの 2,048 ビット

6.1.6　公開鍵のパラメータ生成及び品質検査

公開鍵パラメータは、信頼できる暗号モジュールによって生成される。公開鍵パラメータの品質検査も暗号モジュールにより行うものとする。

6.1.7　鍵の利用目的

鍵の利用目的は以下のとおりとする。

- 本認証局の鍵について、keyUsage は keyCertSign 及び cRLSign のビットを使用する。
- 「免税販売管理システム用クライアント証明書」の鍵について、keyUsage は digitalSignature 及び keyEncipherment のビットを使用し、extendKeyUsage には clientAuth、smartCardLogon を使用する。

6.2 私有鍵の保護及び暗号モジュール技術の管理

6.2.1 暗号モジュールの標準及び管理

CA 私有鍵の格納モジュールは、US FIPS 140-2 レベル 3 相当の暗号化装置によって生成、保存等の管理を行う。

6.2.2 私有鍵の複数人による管理

本認証局の CA 私有鍵の生成及び管理は、本認証局の鍵の管理を担う複数人の運営要員よって行われる。

6.2.3 私有鍵のエスクロー

本認証局は、CA 私有鍵及び利用者私有鍵のエスクローを行わない。

6.2.4 私有鍵のバックアップ

本認証局の CA 私有鍵は、本認証局の鍵の管理を担う複数人の運営要員よって行われ、かつ、そのうちの 1 名だけではできない方法によって認証設備室内でバックアップされ、複数に分割されたバックアップ用の鍵として保管する。バックアップ用の鍵の個々については、一つずつ権限を有する者以外が触れることができないアクセス制御などの措置がされ、耐火等の防災措置がとられた異なる場所に施錠して保管する。

6.2.5 私有鍵のアーカイブ

認証局は CA 私有鍵をアーカイブしない。

6.2.6 暗号モジュールへの私有鍵の格納と取り出し

本認証局の CA 私有鍵をバックアップ用の鍵からリストア（復元）する場合は、本認証局の鍵の管理を担う複数の運営要員によって認証設備室にて行う。

6.2.7 暗号モジュールへの私有鍵の格納

CA 私有鍵は、FIPS 140-2 レベル 3 相当の暗号化装置によって生成し、暗号化して暗号化装置内に保存する。

6.2.8　私有鍵の活性化方法

CA 私有鍵の活性化の方法は、認証局室内において本 CP/CPS「6.2.2　私有鍵の複数人による管理」と同じく、複数名の権限を有する者を必要とする。

6.2.9　私有鍵の非活性化方法

CA 私有鍵の非活性化の方法は、認証局室内において本 CP/CPS「6.2.2　私有鍵の複数人による管理」と同じく、複数名の権限を有する者を必要とする。

6.2.10　私有鍵の廃棄方法

CA 私有鍵を破棄しなければならない状況の場合、認証局室内で本 CP/CPS「6.2.2　私有鍵の複数人による管理」と同じく、複数名の権限を有する者によって、私有鍵の格納された HSM を完全に初期化、又は物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続きによって破棄する。

6.2.11　暗号モジュールの評価

CA 私有鍵を格納する暗号モジュールは、FIPS 140-2 レベル 3 相当のものを使用する。

6.3　鍵ペア管理に関するその他の面

6.3.1　公開鍵のアーカイブ

本 CP/CPS「5.5.2　アーカイブを保存する期間」及び「5.5.3　アーカイブの保護」で規定するとおり行う。

6.3.2　利用者証明書の有効期間と鍵ペアの使用期間

私有鍵と公開鍵の有効期間については、表 6.1 に示す。

表 6.1　鍵の有効期間

利用者証明書	私有鍵有効期間	公開鍵有効期間
免税販売管理システム用クライアント証明書	3 年	3 年

本認証局は発行を実施した日時を有効期間の開始日時に設定し、有効期間終了日時を発行日時から起算して有効期間経過後の同月末日の 23 時 59 分 59 秒とする。

6.4　活性化用データ

6.4.1　活性化データの生成とインストール

本認証局において用いられる CA 私有鍵の活性化データは一意で予測不能なものとし、その生成とインストールは定められた規則に従い実施する。

利用者私有鍵の活性化データ（PIN）は認証局側で生成し、本認証局が利用者私有鍵設定する。

本認証局は利用者私有鍵の活性化データ（PIN）を書面等で利用者に通知する。

6.4.2　活性化データの保護

認証局において用いられる CA 私有鍵の活性化データは、権限者の責任で厳重に管理、保護される。

6.4.3　活性化データのその他の要件

規定しない。

6.5　コンピュータのセキュリティ管理

6.5.1　特定のコンピュータのセキュリティに関する技術的要件

認証業務用設備は、ファイアウォールを介して外部ネットワークと接続し、不正アクセスを検知・防止する。本認証業務で用いる暗号化装置は、FIPS140-2 レベル 3 相当の暗号化装置を用いる。

CA システムへのログイン時には、本 CP/CPS「5.2.3　個々の役割に対する本人性確認と認証」で定めるユーザの認証を必須とする。

6.5.2　コンピュータセキュリティ評価

本認証局で使用する製品については、セキュリティに関する情報等を定期的に収集し、最新のセキュリティ技術の最新動向を踏まえて、使用する製品が設けたセキュリティに関する基準を満たすよう維持管理する。

6.6　ライフサイクルの技術的管理

本認証局のハードウェア及びソフトウェアは、適切なサイクルで最新のセキュリティテクノロジを導入すべく、随時本 CP/CPS の見直し及びセキュリティチェックを行う。

6.6.1　システム開発管理

本認証局のシステムは、適切な品質管理が行われた信頼できる組織で開発されたもの

を使用する。

本認証局のシステムについては、電磁的記録で保存される記録の内容が表示できるように、当該システムの機器、OS 及びアプリケーションを維持する。

本認証局のシステムに係る機器、OS 及びアプリケーションを更新する場合は、更新前に試験等を行い、互換性を確保する。

6.6.2 セキュリティ運用管理

本認証局のシステムについては、別に定めるセキュリティに関する規程（以下「セキュリティ規程」という。）の定めに従い、適切な運用を行う。

6.6.3 ライフサイクルのセキュリティ管理

規定しない。

6.7 ネットワークのセキュリティ管理

本認証局のネットワークについては、セキュリティ規程の定めに従い、適切な運用を行う。また、定期的な評価を実施し、ネットワーク運用がセキュリティ規程を満たすよう、以下の措置を行い、維持する。

1. 認証業務用設備を構成するネットワーク及びリポジトリを構成するネットワークに対する不正アクセスを防止するためのファイアウォールによる制御及び監視。また、リポジトリを構成するネットワークに対する不正アクセスを検知するための不正侵入検知システムによる監視
2. 証業務用設備を構成するネットワーク上の通信データの漏洩及び盗聴防止のための暗号化

6.8 タイムスタンプ

本認証局は、正確な時刻源を取得し、NTP（Network Time Protocol）を使用し認証業務用設備の時刻同期を行う。

7　証明書及び失効リスト及び OCSP のプロファイル

7.1　証明書のプロファイル

本認証局が発行する証明書は、X509 Version 3 フォーマット証明書形式により作成され、また証明書は X.500 識別名（Distinguished Name、以下 DN という）により一意に識別されるものとする。

本 CP/CPS に従い発行される CA 証明書のプロファイルは、基本領域のプロファイルを別紙 1　表 A.1 に示し、拡張領域のプロファイルを別紙 1　表 A.2 に示すとおりとする。また、利用者証明書のプロファイルは、基本領域のプロファイルを別紙 1　表 A.3 に示し、拡張領域のプロファイルを別紙 1　表 A.4 に示すとおりとする。

7.1.1　バージョン番号

本認証局が発行する証明書は、X509 Version 3 フォーマット証明書形式により作成されることとする。

7.1.2　証明書の拡張

本認証局が発行する CA 証明書の拡張領域のプロファイルは別紙 1　表 A.2 に示すとおりとする。また、利用者証明書の拡張領域のプロファイルは別紙 1　表 A.4 に示すとおりとする。

7.1.3　アルゴリズムオブジェクト識別子

基本領域の Signature アルゴリズムは以下のとおりとする。

- sha256WithRSAEncryption (1.2.840.113549.1.1.11)

基本領域の subjectPublicKeyInfo アルゴリズムは以下のとおりとする。

- rsaEncryption (1.2.840.113549.1.1.1)

7.1.4　名称の形式

CA 証明書の Issure と Subject の名前の形式は別紙 1　表 A.1 に示される。また、利用者証明書の Issure と Subject の名前の形式は別紙 1　表 A.3 に示される。

7.1.5　名称制約

規定しない。

7.1.6　CP オブジェクト識別子

使用しない。

7.1.7　ポリシ制約拡張

使用しない。

7.1.8　ポリシ修飾子の構文及び意味

規定しない。

7.1.9　証明書ポリシ拡張フィールドの扱い

規定しない。

7.2　証明書失効リストのプロファイル

7.2.1　バージョン番号

認証局が発行する CRL/ARL は、X.509CRL フォーマット形式のバージョン 2 に従うものとする。

7.2.2　CRL と CRL エントリ拡張領域

CRL エントリの基本領域のプロファイル及び拡張領域のプロファイルは別紙 2　表 B.1 のとおりとする。

7.3　OCSP プロファイル

7.3.1　バージョン番号

規定しない。

7.3.2　OCSP 拡張領域

規定しない。

8　準拠性監査とその他の評価

8.1　監査頻度

規定しない。

8.2　監査者の身元・資格

規定しない。

8.3　監査者と被監査者の関係

規定しない。

8.4　監査テーマ

規定しない。

8.5　監査指摘事項への対応

規定しない。

8.6　監査結果の通知

規定しない。

9　その他の業務上及び法務上の事項

9.1　料金

規定しない。

9.2　財務上の責任

9.2.1　保険の適用範囲

規定しない。

9.2.2　その他の資産

規定しない。

9.2.3　エンドエンティティに対する保険又は保証

規定しない。

9.3　企業情報の秘密保護

9.3.1　秘密情報の範囲

本認証局が保有する情報のうち、利用者証明書、CRL、本 CP/CPS 等の公開文書を除いた情報が、秘密情報の対象として扱われる。

9.3.2　秘密情報の範囲外の情報

本認証局は、以下の情報を秘密情報として扱わない。

- 利用証明書、又は CRL に含まれる情報
- 本 CP/CPS 及びその他本認証局の公開文書
- リポジトリで公開される情報
- 本認証局以外の出所から、秘密保持の制限無しに公知となった情報

9.3.3　秘密情報を保護する責任

本認証局は「9.3.1　秘密情報の範囲」で規定された秘密情報を保護するため、内部及び外部からの情報漏洩に係わる脅威に対して合理的な保護対策を実施する責任を負う。

ただし、本認証局が保持する秘密情報を、法の定めによる場合及び利用者による事前の承諾を得た場合に開示することがある。その際、その情報を知り得た者は契約あるいは法的な制約によりその情報を第三者に開示することはできない。にもかかわらず、そ

のような情報が漏洩した場合、その責は漏洩した者が負う。

9.4　個人情報の保護

9.4.1　プライバシープラン

本認証局において認証業務の円滑な運営に必要な範囲で、本認証局の利用者の情報を収集する場合がある。収集した情報は利用目的の範囲内で適切に取り扱う。本認証局では、利用者の情報を本認証局での認証業務を円滑に運営するために、利用者の組織確認、及び利用者への連絡先、送付先として利用する。

また、本認証局では、収集した情報について、法令に基づく開示請求があった場合、その他特別な理由のある場合を除き、利用目的以外の目的のために自ら利用、又は第三者に提供しない。更に、本認証局は、収集した情報の漏えい、滅失又はき損の防止その他収集した情報の適切な管理のために必要な措置を講じる。

9.4.2　プライバシーとして保護される情報

認証局は、次の情報を保護すべき個人情報として取り扱う。

- 登録局が本人確認や各種審査の目的で収集した情報の中で、証明書に含まれない情報。例えば、身分証明書、自宅住所、連絡先の詳細など、他の情報と容易に照合することができ、それにより特定の個人を識別することが可能な情報を指す。
- CRL に含まれない利用者の証明書失効又は停止の理由に関する情報。
- その他、認証局が業務遂行上知り得た利用者の個人情報。

9.4.3　プライバシーとはみなされない情報

次の情報は、秘密情報として扱わない。

- 利用者証明書
- CRL に記載された情報

9.4.4　個人情報を保護する責任

認証局は「9.4.2　プライバシーとして保護される情報」で規定された情報を保護するため、内部及び外部からの情報漏洩に係わる脅威に対して合理的な保護対策を実施する責任を負う。

9.4.5　個人情報の使用に関する個人への通知及び同意

認証局は、証明書発行業務及びその他の認証業務の利用目的に限り個人情報を利用する。それ以外の目的で個人情報を利用する場合は、法令で除外されている場合を除き、あらかじめ本人の同意を得るものとする。

9.4.6　司法手続又は行政手続に基づく公開

司法機関、行政機関又はその委託を受けたものの決定、命令、勧告等があった場合は、認証局は情報を開示することができる。

9.4.7　その他の情報開示条件

個人情報を提供した本人又はその代理人から当該本人に関する情報の開示を求められた場合、認証局で別途定める手続きに従って情報を開示する。この場合、複製にかかる実費、通信費用等については、情報開示を求める者の負担とする。

9.5　知的財産権

以下の情報及びデータについての著作権その他知的財産権等の全ての権利は、本認証局に帰属するものとする。

- 本認証局より発行された利用者証明書
- 本認証局より公開された CRL
- 本 CP/CPS

9.6　表明保証

9.6.1　認証局の表明保証

本認証局は、以下の責任及び義務を負う。

1. 提供するサービスと運用のすべてが、本 CPS の要件に従い行う。
2. 本 CP/CPS「5　建物及び関連施設、運用のセキュリティ」及び「6　技術的セキュリティ管理」に従い本認証局を運営する。
3. CA 私有鍵が、利用者証明書及び証明書失効リストに署名するためだけに使用されることを保証する。
4. 利用者が使用する電子署名アルゴリズムとして、法令で定めるアルゴリズムのうち、公開鍵暗号方式については、鍵長 2,048 ビットの RSA 方式を、ハッシュ関数については、SHA-256 方式を指定し、電子署名アルゴリズムは、本認証局が指定するものを使用する。

9.6.2　利用者の表明保証

利用者は、以下の責任及び義務を負う。

1. 利用者証明書の利用に際して、本 CP/CPS に同意し遵守するとともに、本 CP/CPS「1.4.1　適切な証明書の使用」に規定する用途のみに利用する。
2. 利用者証明書に関する手続を行う。
3. 本認証業務によって発行された利用者証明書に対応する私有鍵と PIN を、十分に注意して管理する。
4. 利用者証明書受領時に利用者証明書の記載事項及び有効性等を確認し、記載事項に誤りがあった場合には、直ちに、本認証局へ報告する。
5. 本認証局は、利用者が使用する電子署名アルゴリズムとして、法令で定めるアルゴリズムのうち、公開鍵暗号方式については、鍵長 2,048 ビットの RSA 方式を、ハッシュ関数については、SHA-256 方式を指定する。利用者は、本認証局が指定する電子署名アルゴリズムを使用する。
6. リポジトリを随時閲覧し、本認証局に関する情報を適宜取得する。

9.6.3　検証者の表明保証

検証者は、以下の責任及び義務を負う。

1. 利用者証明書の検証に際して、本 CP/CPS に同意し遵守するとともに、本 CP/CPS「1.4.1　適切な証明書の使用」に規定する範囲のみに利用する。
2. 利用者証明書の利用にあたり、利用者証明書の検証を行なわなければならない。即ち、本認証局の CA 証明書により利用者証明書を署名検証することにより、当該利用者証明書が本認証局の CA 秘密鍵により電子署名されていることを検証する。本認証局の CA 証明書のフィンガープリント（CA 証明書の値を SHA-1 でハッシュ変換した値）を検証することにより、当該 CA 証明書が本認証局の発行したものであることを確認する。
3. 利用者証明書を利用するにあたり、その利用者証明書が有効期間内であること及び失効されていないかどうかを確認する。
4. 利用者証明書を利用するにあたり、本認証局がリポジトリで公開する本認証サービスに関する情報を確認する。

9.6.4　他の関係者の表明保証

規定しない。

9.7　無保証

本認証局は、本 CP/CPS「9.6.1　認証局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害又は派生的損害に対する責任を負わず、いかなる逸失利益、データの紛失又はその他の間接的若しくは派生的損害に対する責任を負わない。

また、本 CP/CPS「9.16.5　不可抗力」で規定される不可抗力による認証業務の停止によって利用者、若しくはその他の第三者において損害が生じた場合、認証局は一切の責任を負わない。

9.8　責任制限

本認証局は、利用者において証明書の利用又は私有鍵の管理その他利用者が注意すべき事項の運用が不適切であったために生じた損害に対して責任を負わない。

また、本認証局の責任は、本認証局の怠慢行為により本 CP/CPS に定められた運用を行わなかった場合に限定する。

なお、本 CP/CPS「9.6　表明保証」に関し、次の場合、本認証局は責任を負わない。

- 認証局に起因しない不法行為、不正使用並びに過失等により発生する一切の損害
- 利用者又は検証者が自己の義務の履行を怠ったために生じた損害
- 利用者又は検証者のシステムに起因して発生した一切の損害
- 利用者又は検証者が使用する端末のソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
- 認証局の責に帰することのできない事由で証明書及び CRL に公開された情報に起因する損害
- 認証局の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
- 証明書の使用に関して発生する業務又は取引上の債務等、一切の損害
- 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害

9.9　補償

規定しない。

9.10　本ポリシの有効期間と終了

9.10.1　有効期間

本 CP/CPS は、作成された後、当庁が承認することによって有効となり、また、本 CP/CPS「9.10.2　終了」に規定する本 CP/CPS の終了まで有効とする。

9.10.2　終了

本 CP/CPS は、「9.10.3　終了の影響と存続条項」で規定する存続条項を除き、当庁が無効と宣言した時点、又は本認証局が本認証業務を終了した時点で無効となる。

9.10.3　終了の影響と存続条項

本認証局が終了した場合であっても、本 CP/CPS「9.3　企業情報の秘密保護」、「9.4 個人情報の保護」、「9.5　知的財産権」、「9.8　責任制限」、「9.9　補償」、「9.10.3　終了の影響と存続条項」、「9.13　紛争解決手続」、「9.14　準拠法」及び「9.15　適用法の遵守」の各規定については、なお、効力を有する。

9.11　関係者間の個々の通知と連絡

関係者間の個別通知と報告は、以下のとおりとする。

1. 本認証局は、本認証局から利用者及び検証者への通知方法として、電子メール、郵便、FAX 及びホームページへの掲示等、本認証局が適当と判断した方法により行う。
2. 電子メールによる通知においては、当該電子メールを本認証局が送信し、送信できたことが確認できた時に通知したものとみなす。
3. 郵便による通知においては、当該郵便の消印日をもって通知したものとみなす。
4. FAX による通知においては、当該 FAX を本認証局が送信し、送信できたことが確認できた時に通知したものとみなす。

9.12　改訂

9.12.1　改訂手続き

本認証局は、本 CP/CPS 及び別に定める諸規程の仕様を変更することができる。また、本認証局は、利用者及び検証者に事前の了解を得ることなく、本 CP/CPS に定めた仕様の変更をすることができる。

9.12.2　通知方法と期間

本認証局は、本 CP/CPS に定めた仕様の変更に関する公開と通知を、以下のとおり行い、変更した本 CP/CPS を公開後 15 日以内に、利用者が自己の利用者証明書の失効手続を行わない場合には、変更に同意したものとみなす。

- 仕様が変更された本 CP/CPS については、変更後、速やかに、リポジトリにて公開することにより、利用者及び検証者へ通知されたものとする。
- 仕様が変更された本 CP/CPS については、仕様が変更された抜粋ではなく、全てを公開する。
- 本 CP/CPS の変更については、バージョン番号及び改訂日により識別する。
- 仕様が変更された本 CP/CPS については、リポジトリによる利用者及び検証者への通知をもって、直ちに、有効とする。
- 利用者及び検証者は、本認証局のリポジトリを定期的に参照し、本 CP/CPS の変更について同意するものとする。

9.12.3　オブジェクト識別子（OID）の変更理由

規定しない。

9.13　紛争解決手続

利用者又は検証者と本認証局との間に、訴訟又は法的行為が起こった場合は、東京地方裁判所を専属管轄裁判所とする。

9.14　準拠法

本 CP/CPS は、日本国内法及び規則に基づき解釈されるものとする。

9.15　適用法の遵守

規定しない。

9.16　雑則

9.16.1　完全合意条項

本 CP/CPS は、本 CP/CPS で定められた事項に対して関係者間における完全合意を構

成するものであり、本認証業務について本 CP/CPS より早い時期及び同時期に定めれれた書面、口頭による意思表示、合意及び表明事項のすべてに優先する。

9.16.2　権利譲渡条項

規定しない。

9.16.3　分離条項

本 CP/CPS のひとつ又は複数の条項が司法の判断により、無効であると解釈された場合であっても、その他の条項の有効性には影響を与えない。無効と判断された条項は、法令の範囲内で当事者の合理的な意思を反映した規定に読み替える。

9.16.4　強制執行条項（弁護士費用及び権利放棄）

規定しない。

9.16.5　不可抗力

本認証局は、以下に例示されるような通常人の標準的な注意義務を尽くしても、予防・回避できない事象を不可抗力とする。不可抗力によって損害が発生した場合、本 CP/CPS「9.7　無保証」の規定により認証局は免責される。

- 利用者又は検証者が、利用者証明書を利用する際に発生したコンピュータシステム等のハードウェア又はソフトウェアへの障害
- 火災、雷、噴火、洪水、地震、嵐、台風、天変地異、自然災害、放射能汚染、有害物質による汚染、又は、その他の自然現象
- 暴動、市民暴動、悪意的損害、破壊行為、内乱、戦争（宣戦布告されているか否かを問わない）又は革命
- 裁判所、政府又は地方機関による作為又は不作為
- ストライキ、工場閉鎖、労働争議
- 電気通信事業者が電気通信サービスを中断又は停止した場合
- 認証局の責によらない事由で、本 CP/CPS に基づく義務の遂行上必要とする必須の機器、物品、供給物若しくはサービス（電力、ネットワークその他の設備を含むがそれに限らない）が利用不能となった場合

9.17　その他の条項

規定しない。

別紙１　証明書プロファイル

下表に証明書プロファイルを示す。

凡例

(1) (sha256WithRSAEncryption)及び(rsaEncryption)はそれぞれ、OID に対応づけられた暗号アルゴリズムを示している。

(2) (id-kp 1)及び(id-kp 2)は、それぞれ OID に対応づけられた利用目的を示している。

(3) （Printable）は、設定された文字列が、printable　string の文字コードでエンコードされていることを示す。

(4) （IA5）は、設定された文字列が、IA5　string の文字コードでエンコードされていることを示す。

(5) （UTF-8）は、設定された文字列が、UTF-8　string の文字コードでエンコードされていることを示す。

表 A.1　自己署名証明書プロファイル（基本部）

領域名	規定内容と設定値（○：設定する、×：設定しない）
基本部	
Version	2（v3）
serialNumber	1（例）
signature	sha256WithRSAEncryption
validity	○
notBefore	有効期間は 30 年に設定（UTCTime で設定する）
notAfter	
issuer	c=JP（Printable）， o=Japanese Government（Printable）， ou=National Tax Agency（Printable）， cn=National Tax Agency CA - G1（Printable）
subject	c=JP（Printable）， o=Japanese Government（Printable）， ou=National Tax Agency（Printable）， cn=National Tax Agency CA - G1（Printable）
subjectPublicKeyInfo	○
algorithm	rsaEncryption
subjectPublicKey	RSA 公開鍵値（2048bit）
issuerUniqueID	×
subjectUniqueID	×

表 A.2　自己署名証明書プロファイル（拡張部）

領域名	ｸﾘﾃｨｶﾙﾌﾗｸﾞ	規定内容と設定値 （○：設定する、×：設定しない）
標準拡張領域		
subjectKeyIdentifier	FALSE	○
keyIdentifier		本証明書の公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
keyCertSign		1　（証明書署名検証）
cRLSign		1　（CRL 署名検証）
extendedKeyUsage		×
privateKeyUsagePeriod		×
certificatePolicies		×
policyMappings		×
issuerAltName		×
subjectAltName		×
basicConstraints	TRUE	○
cA		TRUE
pathLenConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints		×
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		
なし		

表 A.3　免税販売管理システム用クライアント証明書プロファイル（基本部）

領域名	規定内容と設定値（○：設定する、×：設定しない）
基本部	
Version	2（v3）
serialNumber	1001（例）
signature	sha256WithRSAEncryption
validity	○
notBefore	有効期間は 3 年後の月末を設定（UTCTime で設定する）
notAfter	
issuer	c=JP（Printable）， o=Japanese Government（Printable）， ou=National Tax Agency（Printable）， cn=National Tax Agency CA - G1（Printable）
subject	c=JP（Printable）， o=Tax Exemption Management System（固定,Printable）， ou=NTAE1234567890（証明書固有値英数字,Printable）， cn=012345678901234567890（識別符号数字,Printable）
subjectPublicKeyInfo	○
algorithm	rsaEncryption
subjectPublicKey	RSA 公開鍵値（2048bit）
issuerUniqueID	×
subjectUniqueID	×

表 A.4　免税販売管理システム用クライアント証明書プロファイル（拡張部）

領域名	ｸﾘﾃｨｶﾙ ﾌﾗｸﾞ	規定内容と設定値 （○：設定する、×：設定しない）
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		c=JP（Printable）, o=Japanese Government（Printable）, ou=National Tax Agency（Printable）, cn=National Tax Agency CA - G1（Printable）
authorityCertSerial		CA 証明書の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		本証明書の公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
digitalSignature		1　（電子署名）
keyEncipherment		1　（鍵暗号）
extendedKeyUsage	FALSE	○
keyPurposeId		○
clientAuth		1.3.6.1.5.5.7.3.2
smartCardLogon		1.3.6.1.4.1.311.20.2.2
privateKeyUsagePeriod		×
certificatePolicies	FALSE	○
policyIdentifier		○
certPolicyId		1.2.392.200127.100.1.1
policyQualifiers		1.3.6.1.5.5.7.2.1（id-qt-cps）
qualifier		http://www.eppcert.jp/ntaca/（IA5）
policyMappings		×
issuerAltName		×
subjectAltName		×
basicConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		○
uniformResource Identifier		http://www.eppcert.jp/ntaca/rlist/ntacag1.crl
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		
なし		

別紙２　CRL プロファイル

表 B-1 に、CRL プロファイルを示す。

表 B.1　CRL プロファイル

領域名	ｸﾘﾃｨｶﾙ ﾌﾗｸﾞ	規定内容と設定値 （○：設定する、×：設定しない）
CRL 基本部		
version		1（v2）
signature		sha256WithRSAEncryption
issuer		c=JP（Printable）, o=Japanese Government（Printable）, ou=National Tax Agency（Printable）, cn=National Tax Agency CA - G1（Printable）
thisUpdate		CRL 発行日時（UTCTime で設定する）
nextUpdate		CRL 発行日時+60 日（UTCTime で設定する）
revokedCertificates		○
userCertificate		利用者証明書の serialNumber
revocationDate		失効日時（UTCTime で設定する）
crlEntryExtentions		○
reasonCode	FALSE	RFC2459 で定義される理由コード （本認証局では以下を使用する。） 1：秘密鍵の危殆化 2：CA 秘密鍵の危殆化 3：記載事項変更による証明書失効 5：利用の中止
CRL 拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		c=JP（Printable）, o=Japanese Government（Printable）, ou=National Tax Agency（Printable）, cn=National Tax Agency CA - G1（Printable）
authorityCertSerial		CA 証明書の serialNumber
cRLNumber	FALSE	本 CRL のシリアル番号