保健医療福祉分野PKIサービス
認証局運用規定

Healthcare PKI Service
Certification Practice Statement

2005 年 9 月
(Version 1.0)

セコムトラストネット株式会社

改訂履歴

版数	日付	内容
初版	平成１７年　９月	初版発行

－目次－

1　はじめに

1.1　概要

本文書「保健医療福祉分野PKIサービス認証局運用規定」（以下、本CPS）は、保健医療福祉分野PKIサービス（以下、本サービス）にて証明書申請者（以下、加入者）の公開鍵証明書（以下、電子証明書、または、証明書）を発行する認証局の運用方針、諸手続きを定める運用規程です。本CPS で対象とする電子証明書は、否認防止を目的とする電子署名にのみ用いる「署名用証明書」とシステムへの認証や通信の暗号化に用いる「認証用証明書」の2種類の証明書があります。署名用の証明書は、厚生労働省の「保健医療福祉分野PKI 認証局 証明書ポリシ」（以下、署名用CP）に基づいて発行され、認証用の証明書は、財団法人医療情報システム開発センター（以下、MEDIS-DC）の認証用の証明書ポリシ（以下、認証用CP）に基づいて発行されます。本CPSで規定する認証局（以下、本CA）は、署名用証明書を発行するCAと認証用証明書を発行するCAの2つのCAを対象とします。また、その運営は本CPSに準拠しセコムトラストネット株式会社（以下、STN）が担当します。なお、本CPSが上記CPに抵触する場合には、各CPの内容が優先されて運営されます。本CPS の変更は、STNの判断によって時宜公表され、その公表をもって発効するものとします。したがって、加入者が、証明書を使用する場合または証明書利用者（以下、検証者）が証明書を信頼して利用する場合において、本CPS の最新の内容を確認することが必要です。本CPSは、STNのWebサイトから入手することができます。本CPS は、インターネットX.509 公開鍵基盤証明書ポリシおよび認証運用フレームワークであるIETF PKIX RFC3647 に準拠しています。

また、本CPS は以下の文章を参照します。

a) IETF/RFC 3280 Internet X.509 Public Key Infrastructure : Certificate and CRL Profile
b) 保健医療福祉分野PKI 認証局 証明書ポリシ（平成17年4月 厚生労働省）
c) MEDIS認証局 認証用 証明書ポリシ（平成17年9月 財団法人 医療情報システム開発センター）

1.2 文書の名前と識別

本ポリシの名称を「保健医療福祉分野PKI サービス認証局運用規定」とします。

また、本CPSで定めるOIDを表1.2に示します。

表 1.2 本 CPS で定める OID

名称	オブジェクト識別子
保健医療福祉分野PKIサービス認証局運用規定	1.2.392.200091.110.111.1

1.3 PKI の関係者

1.3.1 認証局

認証局（CA）は、証明書発行局（IA）と登録局（RA）により構成されます。また、本CAは、本CPSが参照するCPに準拠する他の認証局と相互認証を行うことがあります。

発行局は証明書の作成、発行、失効および失効情報の開示および保管の各業務を行います。証明書発行、失効の受付は所定のRAが行います。

但し、本CAは本CPSの遵守およ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を外部に委託することができるものとします。

1.3.2 登録局

RAは加入者からの証明書の発行申込等を受け付けて、申込内容の審査を行います。申込内容について問題がない場合、申込情報をもとにCAに対して証明書発行要求等を行います。発行済み証明書に対しては、加入者からの失効の申し込み申込みを受付けてCAに対して失効要求を行います。また、RAでは、証明書および私有鍵のICカードの格納、加入者への送付も業務として実施することがあります。

1.3.3 ローカル登録局

認証局は本CPSの遵守およ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RA業務の一部を外部に委託することができるものとします。その場合、医療機関の管理者や医療従事者団体の代表者（以下、医療機関等の管理者）等に、ローカルRA（LRA）として当該組織に所属する個人へ証明書を発行する際の審査業務を委託することがあります。この場合、該当するCPもしくは本CPSに則った自然人の本人性、実在性、申請意思確認、国家資格所有者の資格所有の事実および組織の所属属性の確認をLRA管理者の責任のもと実施するものとします。

また、認証局とLRAの間で委託に係わる契約を取りわし、委託された業務に関してRAに課せられると同等の責任および義務を負うことを定めるものとします。

なお、本CPSでRAと表記する場合は、LARも含めるものとします。

1.3.4 加入者

加入者とは、証明書所有者のことです。証明書所有者とは、認証局により証明書を発行される個人または組織をさします。加入者は証明書に対応した私有鍵を使い、電子署名、認証応答などの処理を行います。

証明書所有者の範囲は次のとおりとします。

署名用証明書の場合、署名用CP「1.3.3 加入者」の規定の通り、以下とします。

a) 保健医療福祉分野サービス提供者および利用者

上記の提供者である以下の者はその資格、役割を証明書内に記載することができます。

b) 保健医療福祉分野に関わる国家資格所有者

c) 医療機関等の管理者

認証用証明書の場合、認証用CP「1.3.3 加入者」の規定の通り以下とします。

d) 組織およびその所属職員

e) 保健医療福祉分野サービス提供者および利用者

上記の提供者である以下の者はその資格、役割を証明書内に記載することができます。

f) 保健医療福祉分野に関わる国家資格所有者

g) 医療機関等の管理者

1.3.5 検証者

検証者とは、加入者の証明書や署名を検証する者をさします。

1.3.6 その他の関係者

規定しません。

1.4 証明書の使用方法

1.4.1 適切な証明書の使用

本CPSでは、否認防止を目的とした署名用証明書と、証明書を所有する加入者の認証や否認防止を目的としない署名検証、加入者宛のデータ暗号化のための秘密鍵の配送など複数の用途に利用できる認証用証明書の2種類の証明書の発行を規定します。それぞれの種類の証明書は別々のCAから発行され、それぞれのCPに規定されている用途で利用されなければなりません。

なお、認証用証明書は、広く一般の認証用アプリケーションでの利用される事を目的としています。認証用証明書はMEDIS-DCの認証用のOIDをそのまま使用します。したがって、限定された組織内での認証に、この認証用証明書を用いる際にはOIDのみによるアクセスコントロールは不適切となります。その場合少なくともSubjectDNの組

織名等を用いたアクセスコントロールを行う事が必要となります。

1.4.2 禁止される証明書の使用

署名用証明書の場合、署名用CPの同章、認証用証明書の場合、認証用CPの同章の定めのとおりとします。

1.5 ポリシ管理

1.5.1 本ポリシを管理する組織

本CPSの管理組織は、STNで設置する「セキュリティポリシ委員会」（以下、ポリシ委員会）とします。

1.5.2 問い合わせ先

本CPSに関する問い合わせ先を以下のように定めます。

【問い合わせ先】
窓口： セコムトラストネット（株）
受付時間：9 時～18 時
e-mail アドレス：hpki-support@ml.secomtrust.net

1.5.3 CPS のポリシ適合性を決定する者

本CPSの内容が、これに準拠し運用する認証局の運営方針として適切か否かの判断はポリシ委員会が行います。

1.5.4 CPS 承認手続き

本CPSは、STN所定の手続きによってポリシ委員会が行います。

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また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、公開鍵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。
- 活性化（Activate） 鍵をシステムへの認証や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。
- 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。
- 加入者（Subscriber） 認証局から電子証明書を発行され、電子証明書内に記載された公開鍵に対応する私有鍵を用いて署名や認証等の操作を行う者。
- 加入者証明書認証局から加入者に対して発行された公開鍵証明書のこと。
- 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。
- 公開鍵（Public Key） 私有鍵と対になる鍵で、私有鍵で暗号化された情報の復号化に用いる。この仕組みを利用し、本人の認証や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） 加入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、公開鍵の加入者情報、公開鍵、CAの情報、その他証明書の利用規則等が記載され、CA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。発行者名と加入者名が同じである。
- 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CAの判断で失効されることもある。
- 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と呼び、CAの証明書の失効リストをARLと呼ぶ場合があるが、本CPSでは、これらを総称してCRLと呼ぶ。
- 証明書発行要求（Certificate Signing Request） 申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、申請者の所在地、サーバアドレス、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および／また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。
- 申請者認証局に電子証明書の発行を申請する主体のこと。
- 検証者（Relying Party） 証明書の信頼性を受け入れて利用する者のことで，受け取った証明書を検証したり，文書の署名を公開鍵証明書の公開鍵で検証する者。
- 電子署名（Electronic 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。

- RA（Registration Authority：RA） 電子証明書発行の申請者の本人を審査・確認し、主として登録業務を行う機関。RAは、認証局の機能のうち、一部の業務を行う。認証する加入者の識別と本人性認証に責任を負うが、電子証明書に署名したり、発行したりはしない。RA業務を外部に委託する場合、その委託先をLAR（Local Registration Authority）と呼ぶ。
- 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。
- 認証実施規程（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。
- 登録設備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。登録業務用設備とは、加入者の登録用端末や、加入者が初めて証明書をダウンロードする際に１ 度限り使用されるＩＤ、パスワード等を識別する為に用いる設備をいう。
- 認証設備室認証業務用設備（電子証明書の作成また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。
- 私有鍵（Private Key） 公開鍵と対になる鍵で、公開鍵で暗号化された情報の復号化に用いる。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。公開せず、他人に漏れないように鍵の所有者だけが管理する。
- 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および拡張領域の利用方法を定めたもの。
- リポジトリ（Repository） 電子証明書および証明書失効リストを格納し公開するデータベース。
- リンク証明書 CA鍵を更新する際に、新しい自己署名証明書（NewWithNew） と古い世代のCA鍵と新しい世代のCA鍵を紐付けるために発行される電子証明書。リンク証明書によって、世代の異なるCAから電子証明書を発行された加入者間での証明書検証が可能となる。リンク証明書には、新しい公開鍵に古い私有鍵で署名した証明書（NewWithOld） と、古い公開鍵に新しい私有鍵で署名した証明書（OldWithNew）がある。
- ルートCA（Root CA） 階層型の認証構造において、階層の最上位に位置する認証局のこと。下位に属する認証局の公開鍵証明書の発行、失効を管理する。

（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
  認証局に対して発行された電子証明書。
- CP（Certificate Policy）
  証明書ポリシを参照のこと。
- CPS（Certification Practice Statement）
  認証実施規程を参照のこと。
- 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、加入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） RAおよびLRAのこと。（RAを参照）
- 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。
- SHA1（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。
- 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およ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 公開およ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と失効情報および加入者の失効情報を保持します。

本CAは、Webサーバにてリポジトリを提供します。

2.2 証明書情報の公開

本CAは、次の内容をリポジトリに格納し、加入者および検証者がインターネット経由で閲覧できるようにします。

＜検証者に公開する事項＞

a) 本CAの公開鍵証明書
b) 本CPSの最新版
c) 本CPSが準拠するCPまたはその参照先
d) CRL
e) 検証者の表明保証に関する文書
f) 本CAの自己署名証明書の値をSHA-1で変換した値（フィンガープリント）

＜加入者に公開する事項＞

検証者に公開する事項に以下を加えたものを公開します。

g) 認証局の定める加入者に関する各種規定/基準

上記リポジトリにて公開する情報のうち、a,dについては、LDAPディレクトリサービスでのアクセスも可能とします。

2.3 公開の時期またはその頻度

本CAが公表する情報について、公表の時期またはその頻度は次のとおりとします。

a) CRLは、発行の都度公表します。
b) 本CAの自己署名証明書は、発行および更新の都度公表します。
c) 本CPS の最新版は、改訂の都度公表します。

2.4 リポジトリへのアクセス管理

CP、本CPS「2.2 証明書情報の公開」に記載の情報は、リポジトリ上で加入者および検証者に対しては読み取り専用として公開します。

3 識別および認証

3.1 名前決定

3.1.1 名前の種類

すべての識別名は、X.500 識別名（DN :Distinguished Name）の基準を採用します。

CAの識別名は、以下の相対識別名（RDN : Relative Distinguished Name） の並びで構成します。

認証用証明書を発行するCAの識別名：
C JP (固定)

O　　SECOM Trust.net Co. Ltd.
CN　　MEDIS-A01-forAuthentication

署名用証明書を発行するCAの識別名：
C　　JP (固定)
O　　SECOM Trust.net Co. Ltd.
CN　　HPKI-01-MEDIS-A01-forNonRepudiation

加入者の識別名は、以下の相対識別名の並びで構成し、それぞれの属性の値は以下の規則に従います。
C　　JP（固定）
L　　MDS***　ここで*** はRA毎に定めた番号を指定します。
O　　組織の英字名
OU　　管理者の場合は "Director"、それ以外の場合にはRAにて設定される文字列
CN　　加入者氏名、または組織に対して発行される場合は組織名（認証用証明書のみ）のローマ字表記
SerialNumber　RAが定めた記号

3.1.2　名前が意味を持つことの必要性

識別名の構成要素である主体者名（CN: CommonName、以下、主体者名）に反映させる名前として、個人の姓名を用いるものとします。個人の姓名には、ローマ字表記を用い、名、姓という順番で記述します。

3.1.3　加入者の匿名性または仮名性

本CAが発行する証明書の主体者名について匿名や仮名は認められません。

3.1.4　種々の名前形式を解釈するための規則

証明書に記載される名前を解釈するルールは、X.500の基準に準拠適合するものとします。

3.1.5　名前の一意性

本CAが発行する電子証明書の加入者名（subjectDN）は、各CA内で一意にするためにシリアル番号（SN）を含むものとします。また、本CAの名前（issuerDN）は、本CAを一意に指し示すものとします。

3.1.6　認識、認証および商標の役割

商標の取り扱いは、関連する契約書および適用する法律の定めに従うものとします。

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CAが加入者の鍵ペアを生成する場合、加入者が私有鍵所有を証明する必要はありま

せん。加入者自身が鍵ペアを生成する場合、加入者の私有鍵で署名された公開鍵証明書要求データをCAが検証することで、加入者は証明書発行を依頼している公開鍵に対応した私有鍵を所有することを証明できます。

3.2.2 組織の認証

本CAでは、申請者が所属する組織または団体について、その組織の実在性や申請者の組織への所属について、下記申し込み書類にもとづき判断します。

本CAに医療機関等の管理者の証明書を申請する者は、証明書の発行に先立ち、次のいずれかの方法で自身の所属もしくは運営する組織の実在性をRAに立証するものとします。

なお、申請者個人の認証は「3.2.3 個人の認証」に定める方法によるものとします。

また、組織の証明書を申請しようとする者についても、同様に、自身の所属もしくは運営する組織の実在性をRAに立証するものとします。

なお、本CPSで取り扱う組織の認証の対象となる組織は以下とします。

a) 法人組織
b) 個人事業者
c) 中央官庁/地方公共団体の運営する組織
d) 上記 a) から c) までの組織で構成される任意団体

＜法人組織の場合＞

商業登記簿謄本、開設許可証のコピーなど公的機関から発行される証明書、各法等で定められる掲示※のコピーのいずれか。

＜個人事業者の場合＞

商業登記簿謄本、公的機関に提出している開設届のコピー、各法等で定められる掲示※のコピーのいずれか。

＜中央官庁/地方公共団体の運営する組織の場合＞

組織が公的機関の場合には、認証局の定める書類に公印規則に定められているその組織責任者もしくは上位組織の管理者の公印を捺印したものを提出することにより組織の実在性をRAに立証するものとします。また、上位組織の管理者による申請の場合は、当該組織とその上位組織の関連が分かる資料を提出するものとします。

＜組織で構成される任意団体の場合＞

幹事等の代表組織の商業登記簿謄本、開設許可証のコピーなど公的機関から発行される証明書、各法等で定められる掲示※のコピーもしくはそれらに順ずる書類のいずれかを提出することによって代表組織の実在性を立証するものとします。また任意団体のパンフレット、設立趣意書等、その団体の実在性を示す書類を提出することで組織の実在性を立証するものとします。
なお、任意団体の組織の認証は、認証用証明書の発行申請の場合のみ認めます。

※ 「各法等で定められる掲示」とは、以下のようなものを指します。
- 医療法 第14条の2（院内掲示義務）
- 薬事法施行規則 第3条（許可証の掲示）
- 指定居宅サービス等の事業の人員、設備および運営に関する基準 第32条およびその準用条項（掲示）

3.2.3 個人の認証

本CAに証明書を申請しようとする個人は、証明書の発行に先立ち、次のいずれかの方法で自身の実在性、本人性および申請意思をRAに立証するものとします。また、国家資格所有者が国家資格を含んだ証明書、医療機関等の管理者が医療機関等の管理者の証明書や組織証明書を申請しようとする場合は、国家資格所有の事実、管理者であることの事実をRAに立証するものとします。立証に用いる書類については、有効期間外のものや、資格喪失後のものを用いることはできません。

なお、本節の定めは証明書申請者の立証に関わる定めであり、RAが証明書を発行申請する場合は、本節の規定に従い申請者の立証を行わせ、4章の規定に則り申請者の審査および証明書の発行を実施します。

＜持参の場合＞

1. 個人の実在性

証明書を申請しようとする個人は、住民票の写しに添えて、認証局の定める申請書類に当該個人の「氏名、生年月日、性別、住所」（以下、基本4情報）を記入し、RAの窓口に提出することで実在性の立証するものとします。

2. 個人の本人性

証明書を申請しようとする個人は、該当するCPが定める書類をRAの窓口で提示することで本人性の立証をするものとします。

3. 個人の証明書申請の意思

本人がRAの窓口に各種の書類を持参して申請する場合は、実在性および本人性の立証を行えば、申請意思の立証がなされたものとみなします。

代理人が窓口で申請する場合は、印鑑登録証明書を添えて、認証局の定める委任状に申請者の実印を捺印したものを提出することで申請者個人の申請意思を立証するものとします。

4. 国家資格および医療機関等の管理者権限

国家資格所有者が国家資格情報を含んだ証明書を申請する場合は、官公庁の発行した国家資格を証明する書類（以下、国家資格免許証等）の原本をRAの窓口で提示することで国家資格所有の事実を立証するものとします。

医療機関等の管理者が医療機関等の管理者の証明書を申請する場合は、「3.2.2 組織の認証」で定める書類に、申請者本人が管理権限者として記載があれば当該書類をRAの窓口で提示することにより管理権限の事実の立証とみなします。記載がない場合は、申請者本人が管理権限を有すると公に告知している医療機関等のパンフレットなどをRAの窓口で提示することで、管理者であることの事実を立証するものとします。

5. 組織の所属属性（認証用証明書の場合のみ）

証明書を申請しようとする個人で、組織の所属属性を証明書に記載することを希望する者は、組織の管理者の記名、押印があり、所属している組織の名称が記載された在籍証明書を、RAの窓口に提出することで自らの所属属性を立証するものとします。

この際、組織およびその管理者権限の立証は上記４に準じてなされるものとします。

＜郵送の場合＞

1. 個人の実在性

証明書を申請しようとする個人は、住民票の写しに添えて、認証局の定める申請書類に当該個人の基本4情報を記入し、RAに郵送することで実在性を立証するものとします。

2. 個人の本人性

証明書を申請しようとする個人は、該当するCPが定める書類をRAに郵送することで本人性の立証をするものとします。

3. 個人の証明書申請の意思

本人が郵送により申請する場合は、印鑑登録証明書を添えて、認証局の定める書類に実印を捺印することで申請者個人の申請意思を立証するものとします。なお、代理人による郵送での申請意思の立証は認めません。

4. 国家資格および医療機関等の管理者権限

国家資格所有者が国家資格情報を含んだ証明書を申請する場合は、官公庁の発行した国家資格免許証等のコピーをRAに郵送することで国家資格所有の事実を立証するものとします。

この時、国家資格免許証等に本人の顔写真が貼付されていない場合は、国家資格証明書のコピーの余白に実印を捺印して、印鑑登録証明書を添えて郵送するものとします。

医療機関等の管理者が医療機関等の管理者の証明書を申請する場合は、「3.2.2 組織の認証」で定める書類に、申請者本人が管理権限者として記載のある場合は、当該書類をRAに郵送することで管理権限の事実の立証とみなします。記載がない場合は、申請者本人が管理権限を有すると公に告知している医療機関等のパンフレットなどを

RAに郵送することで、管理者であることの事実を立証するものとします。

5. 組織の所属属性（認証用証明書の場合のみ）

証明書を申請しようとする個人で、組織の所属属性を証明書に記載することを希望する者は、組織の管理者の記名、押印があり、所属している組織の名称が記載された在籍証明書を、RAに郵送することで自らの所属属性を立証するものとします。

＜オンラインの場合＞

認証用の証明書を申請しようとする個人は、認証局の定める手続きに従い、厚生労働省が定める「保健医療福祉分野PKI認証局 証明書ポリシ」に準じて発行される署名用の証明書等で署名された申請書を提供することにより、実在性および本人性および申請者個人の申請意思を立証するものとします。

なお、保健医療福祉分野PKIの署名用証明書による電子署名は、当該本人しか実行できないことから、電子署名の提供によりこれらの意思を立証したものとみなします。

また、署名用の証明書の初回のオンライン申請は認めません。

3.2.4 確認しない加入者の情報

認めません。

3.2.5 機関の正当性確認

CAは申請者が本サービスの申込を行うための正当な権限を有しているかを、本CPS「3.2.2 組織の認証」および「3.2.3 個人の認証」にしたがい確認します。

3.2.6 相互運用の基準

規定しません。

3.3 鍵更新申請時の本人性確認および認証

3.3.1 通常の鍵更新時の本人性確認および認証

加入者は、RA所定の手続きにより私有鍵および証明書の更新の申込を行うものとします。加入者の認証は「4.2.1 本人性および資格確認」に基づき証明書が発行または更新された日から5年以内であれば、「3.2.3 個人の認証」で提出した書類またはRAで作成された記録を再び参照することで行えます。

5年を過ぎていた場合、または元の書類もしくは記録が無効になっているか廃棄されていた場合は、初回の証明書発行と同様の手続きで認証を実施します。

3.3.2 証明書失効後の鍵更新の本人性確認および認証

私有鍵および証明書の更新の申込のあったときに証明書が失効している場合、また

は有効期限切れの場合、本CAは、本CPS「3.2.3 個人の認証」と同一の手続きをとるものとします。

3.4 失効申請時の本人性確認および認証

加入者が認証局に失効申請を行うときには、次の手順に従うものとします。

a) 失効を申請する証明書を特定する。
b) 証明書を失効する理由を明らかにする。
c) RAは失効申し込みをおこなっている加入者をRAが定める所定の手続きにしたがい、郵送、電話、または、加入者の私有鍵での署名による失効申請で加入者本人であることを認証します。なお、本人確認にあたっては、郵送、電話での失効受付の場合、最低限、本CAで保存してある「4.2.1 本人性および資格確認」で用いた申請者の各種書類を参照します。

4 証明書のライフサイクルに対する運用上の要件

4.1 証明書申請

4.1.1 証明書の申請者

該当するCPに規定します。

4.1.2 申請手続きおよび責任

該当するCPに規定します。

4.2 証明書申請手続き

4.2.1 本人性および資格確認

本人性および資格の確認については、それぞれ以下の方法により実施します。なお、オンラインによる申請は、申請者があらかじめ「保健医療福祉分野PKIの署名用証明書」を所有している場合に認証用の証明書の発行申請を行う場合に受け付けるものとします。

ただし、署名用の証明書の申請の場合、初回のオンラインによる申請は受け付けません。

＜本人からの申請の場合＞

1. 自然人への証明書発行

本 CA は、自然人への証明書の発行時、本 CPS「3.2.3 個人の認証」に定める申請者の本人性、実在性及び申請意思の立証、並びに組織の所属属性を証明書に記載する場合の所属属性の立証に対して、それぞれ以下の方法で真偽の確認を行います。

(1) 持参の場合

申請者から提示された各種の書類について、記載事項が一致していることの確認や印影が一致していることの確認、貼付された写真と申請者本人との照合などを実施し、本人性、実在性、申請意思を確認します。

証明書の交付時、申請者本人が RA に出頭する場合は、電子証明書もしくは

電子証明書を生成する符号を、窓口で交付することにより加入者私有鍵を確実に本人に渡します。
なお、確認に用いた証明書等は RA でコピーを取り、「5.5.2　アーカイブを保存する期間」で定める期間、保存します。

(2) 郵送の場合
申請者から提示された各種の書類について、記載事項が一致していることの確認や印影が一致していることの確認を実施し、実在性、申請意思を確認します。
郵送で証明書を交付する場合は、電子証明書もしくは電子証明書を生成する符号を、申請者本人へ本人限定受取郵便で送付することにより本人性の確認を行うと伴に、加入者私有鍵を確実に本人に渡します。
います。
なお、確認に用いた証明書等は、RA で「5.5.2　アーカイブを保存する期間」で定める期間、保存します。

(3) オンラインの場合
認証用の証明書を申請しようとする個人は、認証局の定める手続きに従い、厚生労働省が定める「保健医療福祉分野 PKI 認証局 証明書ポリシ」に準じて発行される署名用の証明書で署名された申請書を提供することにより、実在性および本人性および申請者個人の申請意思、および組織の所属属性を立証するものとします。
なお、署名用の証明書の初回のオンラインによる申請は受け付けません。
なお、確認に用いた証明書等は、RA で「5.5.2　アーカイブを保存する期間」で定める期間、保存します。

2. 国家資格所有者への証明書発行
認証局は、国家資格所有者への証明書の発行時、「1.　自然人への証明書発行」の方法による申請者の確認に加え、以下の方法により国家資格所有の確認を行います。

(1)　持参の場合
官公庁の発行した国家資格免許証等の原本を要求し、対面により国家資格所有の有無を確認します。
なお、資格確認を実施した国家資格免許証等は RA でコピーを取り、「5.5.2 アーカイブを保存する期間」で定める期間、保存します。

(2)　郵送の場合
官公庁の発行した国家資格免許証等のコピーの郵送を要求し、国家資格所有の有無を確認します。
また、当該国家資格証明書に本人の顔写真が貼付されていない場合は、印鑑登録証明書を添えて、国家資格免許証等のコピーの余白に実印を捺印するものとします。
なお、確認に用いた証明書等は、RA で「5.5.2　アーカイブを保存する期間」で定める期間、保存します。

(3)　オンラインの場合
証明書を申請しようとする個人は、認証局の定める手続きに従い、厚生労働

省が定める「保健医療福祉分野 PKI 認証局 証明書ポリシ」に準じて発行される署名用の証明書等で署名された申請書を提供することにより、国家資格の属性を立証するものとします。

なお、確認に用いた証明書等は、RA で「5.5.2　アーカイブを保存する期間」で定める期間、保存します。

3. 医療機関等の管理者への証明書発行

認証局は、医療機関等の管理者への証明書発行時、「1.　自然人への証明書発行」の方法による申請者の確認に加え、「3.2.2　組織の認証」に定める組織の立証に対して真偽の確認および管理者権限の確認を行います。

署名用証明書の発行申請の場合、組織の立証の真偽の確認をする時は、電話帳などの第 3 者の提供サービスを用いて調査した連絡先若しくは、公知化された連絡先へ問い合わせを実施するか、当該組織を管轄する保健所等へ問い合わせを実施することにより申請機関の実在性確認を行います。

なお、中央官庁・地方公共団体が運営する機関で当該機関の実在性が明らかな場合は、認証局の定める書類に当該機関名を記入し、その組織責任者もしくは上位組織の管理者の公印を捺印したものの提出を求めることで、公印であることを確認し組織の実在性が立証できるものとし、問い合わせによる確認を省略します。

(1) 持参もしくは郵送の場合

申請時に持参もしくは郵送された組織の立証のための書類に記載された代表者の氏名と、「1.　自然人への証明書発行」で確認した書類に記載された氏名が一致することを確認します。

なお、確認に用いた等書類は RA でコピーを取り、「5.5.2　アーカイブを保存する期間」で定める期間、保存します。

(2) オンラインの場合

証明書を申請しようとする個人は、認証局の定める手続きに従い、厚生労働省が定める「保健医療福祉分野 PKI 認証局 証明書ポリシ」に準じて発行される署名用の証明書等で署名された申請書を提供することにより、代表者権限の有無を立証しなくてはならない。

なお、確認に用いた証明書等は、RA で「5.5.2　アーカイブを保存する期間」で定める期間、保存します。

4. 組織に対する証明書

本 CA は、組織への認証用証明書発行時は、「3. 医療機関等の管理者への証明書発行」の手続きに準じます。

なお、組織への署名用証明書の発行申請は受け付けません。

＜組織の代表者による一括申請の場合＞

本 CA は、組織の管理者（代表者）より、その組織およびその組織に所属する個人の認証用証明書の一括申請を受理した場合、組織代表者本人の本人性、実在性、申請意思、資格および組織の所属属性の確認を実施します。

なお、組織の代表者による署名用証明書の一括申請は受け付けません。

1. 証明書をその所属組織で一括申請する場合

本 CA は、その組織および組織に所属する個人への証明書を一括して発行する時、「＜本人からの申請の場合＞ 1.　自然人への証明書発行」の方法による組織代表者

の確認に加え、「3.2.2　組織の認証」に定める組織の立証に対して真偽の確認および代表者権限の確認を行います。

なお、組織に所属する個人の確認は、「＜本人からの申請の場合＞ 1.　自然人への証明書発行」の方法により行います。組織の代表者は、一括申請の対象となる、当該組織に所属する個人の基本 4 情報、および、必要に応じて国家資格、組織の所属属性が記載された名簿を提出するものとします。当該名簿には組織の代表者の記名、押印をし、組織の名称を記載するものとし、組織の代表者はその内容に責任を持つものとします。

組織に所属する個人を確認するための書類は、証明書を申請しようとする組織において、「3.2.3　個人の認証」および「＜本人からの申請の場合＞ 1.　自然人への証明書発行」で定められた内容に準ずる方法によって、事前になされている場合には、その提出を省略することができます。この場合、組織において本人確認に用いた書類は、認証局等から提示の依頼があった場合に提示できるよう、「5.5.2　アーカイブを保存する期間」で定める期間まで保存しておくものとします。

(1) 持参もしくは郵送の場合

申請時に持参もしくは郵送された組織の立証のための書類に記載された代表者の氏名と、「＜本人からの申請の場合＞ 1.　自然人への証明書発行」で確認した書類に記載された氏名が一致することを確認します。

なお、郵送の場合は、その組織の所在地に代表者名で送付します。

(2) オンラインの場合

管理者証明書を申請しようとする組織の管理者（代表者）は、本 CA の所定の手続きに従い、厚生労働省が定める「保健医療福祉分野 PKI 認証局 証明書ポリシ」に準じて発行される署名用の証明書等で署名された申請書を提供することにより、個人および組織の実在性、申請者個人の本人性、申請意思、国家資格の属性、および代表者権限の有無を立証するものとします。

＜代理人からの申請の場合＞

認証局は、代理人からの申請の場合、申請者本人の本人性、実在性、申請意思および資格の確認、委任状による委任の意思確認を実施することに加え、以下の手順により代理人の本人性確認を実施します。

ただし、組織の代表者による一括申請の場合は、代理人からの申請は認めません。

1. 持参の場合

本 CA は、代理人に「3.2.3　個人の認証」の＜持参の場合＞に定める本人性を確認する書類の提示を求め、対面による代理人の本人性の確認を実施します。

この場合も、1 点の書類で確認できる場合と 2 点の書類で確認が必要な場合があり、必要な書類については、「3.2.3　個人の認証」の定めのとおりとします。

2. 郵送の場合

本 CA は、代理人による郵送の申請を認めません。

3. オンラインの場合

本 CA は、電子的に作成された代理人申請書など、本 CA が定める書類に付された「保健医療福祉分野 PKI 認証局 証明書ポリシ」に準じて発行される署名用の証明書でなされた代理人および申請者の電子署名の有効性を確認することにより代理人および申請者の本人性の確認を実施します。

4.2.2　証明書申請の承認または却下

RAは、証明書申請者から提出された申請書類に基づき、申請者の実在性の確認、本人性の確認、申請意思確認、該当CPと本CPSへの同意の確認、国家資格の確認を実施します。またCPにて組織の確認、組織管理者権限の確認、組織の所属属性の確認が必要な場合は、併せてその確認を実施します。その審査過程において疑義が生じた為に発行申請を不受理とする場合は、証明書発行は行わず、郵送、電子メール、または電話等、各RAで定める方法に従い、その理由を申請者宛に連絡します。

4.2.3　証明書申請手続き期間

本CAでは、証明書申請の手続き期間などを情報公開Webサイト等で公開します。また、RAからの申請手続きの案内文に申請手続き期間などを記し、申請者へ送付する場合もあります。

4.3　証明書発行

4.3.1　証明書発行時の認証局の機能

＜認証局が鍵ペアを生成する場合＞

認証局が鍵ペアを生成する場合は、以下の項目を含め運用するものとします。

1. 加入者鍵ペアの生成は、認証設備室と同等の安全性が確保できる環境下で行い、アクセス権限管理、複数人による運用にて内部けん制する等のセキュリティ対策を講じ、その記録を残します。

2. 加入者鍵ペアの転送や出力を行う場合も、加入者鍵ペアの生成時と同様の環境下で作業を行い、アクセス権限管理、複数人による運用等のセキュリティ対策を講じ、その記録を残します。
   また、加入者鍵ペアを転送、出力した後、速やかに加入者鍵ペアを完全に廃棄もしくは消去します。

3. 加入者鍵ペアの活性化に使用する PIN 等の生成、転送、出力等を行う場合も、加入者鍵ペアの生成時と同様の環境下で作業を行い、アクセス権限管理、複数人による運用等のセキュリティ対策を講じ、その記録を残します。加入者鍵ペアの活性化に使用する PIN 等の情報は、加入者を一意に識別でき、また容易に類推できないものとして作成します。
   また、鍵ペアの活性化情報を加入者に通知する際は第三者に渡らないよう安全に通知するものとし、対面で通知する場合以外は、加入者私有鍵の送付とは別に、加入者に安全に送付します。
   なお、PIN 等を生成、転送、出力した後は、速やかに PIN 等を完全に廃棄もしくは消去します。

＜加入者が鍵ペアを生成する場合＞

加入者が鍵ペアを生成し、電気通信回線を通じて受信する場合は、以下の項目を含め運用するものとします。

1. 本 CA は、加入者が鍵ペアを生成する時に用いる 2 つの識別符号を、加入者を一意に識別できるものとして生成し加入者に伝達します。また、識別符号は、容易に類推できないものとします。

2. 加入者の識別符号は、一度利用した後、それ以降の識別処理に用いられないような措置を講じるものとします。

3. 加入者の 2 つの識別符号は、生成した後、手交またはそれぞれ別ルートで加入者以外の第三者に渡らないよう安全に加入者に通知します。また、2 つの識別符号のうちの 1 つは、本人限定受取郵便にて証明書申請者に送付します。なお、認証用証明書の組織による一括申請の場合は組織の代表者に送付します。

4.3.2 証明書発行後の通知

本 CA は、電子証明書を交付することにより電子証明書を発行したことを通知したものとみなします。

4.4 証明書の受理

4.4.1 証明書の受理

＜加入者による証明書内容の確認＞

証明書の内容に誤りがある場合や万一、鍵ペアが正しく機能しない場合には、加入者はその証明書に対応する私有鍵を利用する前にその誤りの修正を RA に対して求めるものとします。証明書内容の修正を行う際は、RA は所定の手続きにしたがって失効、再発行の処理を行います。また、本 CA や RA により証明書を IC カードに格納して配布されている場合は、IC カードを返送いただきます。この際、RA はあらかじめ当該証明書の失効処理を行うものとします。

なお、加入者が対応する私有鍵を利用した場合には、CA は加入者が証明書の内容を承諾したものとみなし、その承諾につき撤回できないものとします。その後の証明書記載内容の変更は証明書失効、再発行手続きによっておこなわれるものとします。

＜加入者の受領確認＞

RA は、電子証明書を交付した後、加入者が受領した旨を確認します。

受領の確認ができない場合、RA は再度、申請者に連絡を取り、提出書類の記載に誤りがある場合正しい書類の送付を求め、電子証明書若しくは電子証明書を生成する符号を再発送します。また、この際 RA は返送された電子証明書若しくは電子証明書を生成する符号を、加入者の受領を確認するまでの間、安全に保管するものとします。

また、証明書記載内容の変更を伴う場合、当該証明書を失効の上、再発行の処理を行います。

なお、証明書を交付してから一定の期間内に RA が申請者の証明書受領が確認できない場合、CA は RA からの申請に基づき証明書を失効させます。

4.4.2 認証局による証明書の公開

CAは、リポジトリで利用者証明書の公表を行いません。

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CAはRAを通じて加入者に対し証明書発行時の通知を行い、原則として第三者に対しては、発行時の通知は行いません。

4.5 鍵ペアと証明書の利用用途

4.5.1 加入者の私有鍵と証明書の利用用途

加入者は証明書中の鍵使用法拡張（keyUsage）に従った使用をしなければなりません。

＜署名用証明書の場合＞

加入者は、私有鍵を否認防止を目的とする電子署名にのみ利用することができます。

＜認証用証明書の場合＞

加入者は、私有鍵をシステムへの認証、否認防止を目的としない署名、加入者公開鍵で暗号化された暗号鍵の復号化にのみに利用することができます。

4.5.2 検証者による公開鍵と証明書の利用用途

検証者は証明書中の鍵使用法拡張（keyUsage）に従った使用をしなければなりません。

＜署名用証明書の場合＞

検証者は、署名検証の用途で公開鍵と証明書を利用することができます。

＜認証用証明書の場合＞

検証者は、加入者の認証、加入者宛のデータの暗号鍵の暗号化、署名検証の用途で公開鍵と証明書を利用することができます。

4.6 証明書更新（鍵更新を伴わない証明書更新）

本CAから発行される証明書は、鍵更新を伴う更新のみを許可します。したがって、鍵の更新を伴わない証明書更新は行いません。

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CAは、以下の条件を満たす時に証明書の更新申請を受け付けます。

a) 更新対象証明書が存在すること。
b) 証明書が有効期限終了前のものであること。
c) 証明書が失効されていないこと。
d) 有効期限終了前で、RAで別途定める期間の申請であること。

これらの要件を満たせば、申請者は証明書の更新が申請できます。

4.7.2 鍵更新申請者

本CAは、加入者本人若しくはその代理人を鍵更新申請者として受け付けます。

ただし、準拠するCPにて、初回申請時に代理人による申請を認めていない場合には更新申請時も代理人による申請を受け付けません。

4.7.3 鍵更新申請の処理手順

「4.2.1 本人性および資格確認」に定める本人性確認並びに資格確認を行うものとします。但し、RAで「4.2.1 本人性および資格確認」に定める本人確認が完了した日から5年以内の場合は、上記に代わり更新対象となる加入者証明書によるオンライン申請にて本人確認を行うことができます。

4.7.4 加入者への新証明書発行後の通知

本CPS「4.3.2. 証明書発行後の通知」と同様とします。

4.7.5 鍵更新された証明書の受理

本CPS「4.4.1. 証明書の受理」と同様とします。

4.7.6 認証局による鍵更新証明書の公開

本CPS「4.4.2. 認証局による証明書の公開」と同様とします。

4.7.7 他のエンティティに対する証明書発行通知

本CPS「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」と同様とします。

4.8 証明書変更

本CAから発行される証明書は、証明書変更は行いません。失効後新規発行扱いとします。

4.9 証明書の失効と一時停止

4.9.1 証明書失効の要件

本CAは、次の場合に証明書を失効するものとします。

＜加入者、組織の管理者もしくはその代理人から失効申請があった場合＞

加入者、組織の管理者もしくはその代理人からの失効申請と確認された場合は、理由

の如何に関わらず証明書の失効を行います。

＜認証局の職員から失効申請があった場合＞

次の各項に該当する場合、証明書を失効させます。

a) 加入者が、本 CPS、またはその他の契約、規制、あるいは有効な証明書に適用される法に基づく義務を果たさなかった場合。
b) 私有鍵の危殆化が認識されたか、その疑いがある場合。
c) 証明書に含まれる該当の情報が正確でなくなった場合。（例えば、医師資格等の保健医療福祉分野専門資格を喪失した場合）。
d) 本 CPS にしたがって証明書が適切に発行されなかったと本 CA が判断した場合。
e) 加入者の特定ができない場合で、緊急に失効させる必要があると本 CA 判断した場合。
f) 本 CA が、本 CPS「4.4.1. 証明書の受理」に基づく加入者の証明書の受領確認ができなかった場合
g) 加入者に関して、正当な権限を有する第三者により正当かつ適切な当該証明書に関する失効の申込（例えば、裁判所の命令を含みかつそれに限定されないものとします）を本 CA が受領した場合
h) 上記の他、加入者の信用状態、および管理者資格、国家資格の状況に重大な変化が生じたと本 CA が判断した場合
i) 加入者に関して、その所属組織が監督官庁より営業停止の処分を受け、または営業免許もしくは営業登録の取消または一時停止の処分を受けた場合（組織の所属属性が記されている証明書の場合のみ）
j) 加入者に関して、その所属組織が解散その他営業活動を休止した場合（組織の所属属性が記されている証明書の場合のみ）
k) その他、本 CA が、加入者に関して本サービスの継続を困難と認めるとする事実が発生した場合

4.9.2　失効申請者

本CAは、次の1人またはそれ以上の者からの失効申請を受け付ける。

a) 本人の名前で証明書が発行された加入者、組織の管理者もしくはその代理人
b) 本CAの職員

4.9.3　失効申請の処理手順

本CAは、失効申請の受領の判断を「3.4 失効申請時の本人性確認および認証」にしたがって、以下の手順を実施した上で証明書の失効を行います。

＜本人からの失効申請の場合＞

RAは失効の申込を受け付け、失効を要求している申請者が、失効される証明書に記されている加入者であることを確認します。確認にあたっては、加入者の私有鍵での署名による失効申請の場合、その署名を検証します。それ以外の場合は最低限、本CAで保存してある「4.2.1 本人性および資格確認」で用いた申請者の各種書類を

参照します。

＜組織の代表者からの失効申請の場合（認証用証明書のみに適用）＞

失効を要求している申請者が、失効される証明書に記されている組織の代表者であることを確認します。確認にあたっては、最低限、認証局で保存してある「4.2.1 本人性および資格確認」で用いた申請者の各種書類を参照します。

代表者が、その管理する組織に所属する個人への証明書の失効を要求する場合、申請時に「4.2.1　本人性および資格確認 ＜組織の代表者による一括申請の場合＞ 1. 証明書をその所属組織で一括申請する場合」にしたがって提出した名簿を参照します。

代表者が、その管理する組織の証明書の失効を要求する場合、「4.2.1　本人性および資格確認 ＜本人からの申請の場合＞ 4.組織に対する証明書」で用いた申請者の各種書類を参照します。

＜代理人からの失効申請の場合＞

代理人が失効を要求して来た場合は、RAは当該代理人が正当な失効権限を持っていることを確認します。確認にあたっては、加入者の委任状の提出、本人死亡の場合などは、法定代理人と確認できる書類等の提出を求めます。

当該証明書の実際の失効にあたっては、代理人を通じて失効を要求している申請者が、失効される証明書に記されている加入者であることを確認します。確認にあたっては、最低限、本CAで保存してある「4.2.1 本人性および資格確認」で用いた申請者の各種書類を参照します。

RAは上記、それぞれの場合で、証明書の失効理由を確認します。RA は本CAに対して証明書の失効申請を行い、本CAはRAからの失効申請を受付け、当該証明書の失効処理を行います。

＜認証局の職員からの失効申請の場合＞

本CAは「4.9.1 証明書失効の要件」の中の本CAの職員から失効申請があった場合は、速やかに当該証明書を特定し、失効の事由の真偽の確認を実施します。また、失効事由が適正であった場合は速やかに証明書を失効させます。

上記、すべての場合、証明書の失効を実施した場合は、CRLを発行します。また、証明書の失効の事実をCRLの発行をもって申請者に通知します。

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には、速やかに失効申請を行わなければならない。その期限はその事由が発生したことが確認された後、24時間以内とします。

4.9.5　認証局による失効申請の処理期間

証明書の失効要求の結果として取られる処置は、受領後直ちに開始され、本人確認後直ちに失効処理を行います。

4.9.6　検証者の失効情報確認の要件

検証者は、加入者の公開鍵を使う時に有効なCRL、本CAがサイニングを受けている場合、ルートCAのCRLおよび関連する認証局の証明書を使用して失効の有無をチェックし、証明書状態の確認を行うものとします。

4.9.7　CRL 発行頻度

CAは、証明書の失効処理を行った場合、CRLを即時に発行します。これらがない場合も、CRLを48時間ごとに発行し、その有効期間は96時間とします。

また、認証局私有鍵（以下、CA私有鍵）、加入者の私有鍵の危殆化等が発生した場合は、CRLを直ちに発行するものとします。

4.9.8　CRL が公開されない最大期間

CRLは発行後直ちに公開されます。

4.9.9　オンラインでの失効／ステータス情報の入手方法

CAではOCSPレスポンダ等による証明書検証サービスは提供しません。

4.9.10　オンラインでの失効確認要件

CAではOCSPレスポンダ等による証明書検証サービスは提供しません。

4.9.11　その他利用可能な失効情報確認手段

使用しません。

4.9.12　鍵の危殆化に関する特別な要件

本CAは、本CA署名鍵の危殆化の際には関連組織に直ちに通知するものとします。

4.9.13　証明書一時停止の要件

一時停止は行いません。

4.10　証明書ステータスの確認サービス

CAではOCSPレスポンダ等による証明書検証サービスは提供しない。

4.10.1　運用上の特徴

規定しません。

4.10.2　サービスの利用可能性

規定しません。

4.10.3　オプショナルな仕様

規定しません。

4.11　加入の終了

加入者が、証明書の利用を終了する場合、本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します。

4.12　私有鍵預託と鍵回復

CA は加入者の私有鍵のエスクロウを行いません。
また、署名目的の私有鍵の回復も行いません。

5　　建物・関連設備、運用のセキュリティ管理

5.1　建物および物理的管理

5.1.1　施設の位置と建物構造

本CAは、火災、水害、地震等による災害の被害を受けるおそれの少ない場所に位置し、災害対策を講じます。また、本CAは、サービスに利用する機器類（以下、CAシステム）を災害および不正侵入から防護された安全なエリアの内部に設置します。

5.1.2　物理的アクセス

本CAを運用する施設は、認証業務用設備の所在を示す掲示をしません。本CAでは、セキュリティレベルを分けて入退室管理を行います。各室への入室権限は、これらのセキュリティレベルに基づき、各室内で行われる業務あるいは操作に応じて、サービス責

任者が付与します。

CAシステムが設置される室は、セキュリティレベルに応じた認証方式を行うことによりアクセス制御を施し、さらに各室への入室には、サービス責任者の承認を必要とします。機器保守、設備保守等で入室権限が無い者の入室が必要な場合は、サービス責任者が承認し、複数の権限者の立会いを必要とします。また、入退出の記録を残します。

CAサーバの設置された室への入室は、2名の権限者の認証を必要とします。

登録設備室においては、関係者以外が容易に立ち入ることが出来ないようにするための施錠等の措置を講じます。

施設内の様子は監視カメラ、各種センサー、入退室制御を行う装置により常時監視されます。

5.1.3 電源および空調設備

本CAは、CAシステムの運用のために十分な容量の電源を確保し、CVCFを設置するとともに、商用電源が供給されない事態に備え非常用自家発電機を装備しています。また、空調設備を用意し、機器類の動作環境および要員の作業環境を適切に維持します。

5.1.4 水害および地震対策

本CAが設置される建物には漏水検知器を設置し、天井および床には防水対策を講じます。また、本CAが設置される建物は耐震構造とし、機器・什器の転倒、落下防止策を講じます。

5.1.5 防火設備

本CAが設置される建物は耐火構造とします。CAシステムを設置する室は防火区画とし、消火設備を備えます。

5.1.6 記録媒体

アーカイブデータ、バックアップデータは、権限者以外が入室できないよう入退室制御された室内の保管庫に安全を確保して保管する。保管場所と遠隔地保管場所の間の媒体搬送は、移送中の安全を確保して行う。

5.1.7 廃棄物の処理

本サービスに関連する重要な文書類、機器類、磁気媒体、HSM等を廃棄する場合の規則は次のとおりとします。

a) 文書類は裁断し廃棄します。
b) 機器類は記録領域を初期化するか、電磁的に破壊するかまたは物理的に破壊し廃棄します。
c) 磁気媒体は初期化するか、電磁的に破壊するかまたは物理的に破壊し廃棄します。
d) HSMは内容を完全に初期化するかまたは物理的に破壊し廃棄します。

なお、私有鍵を含む廃棄物の処理作業は、複数名で行うものとします。

5.1.8 施設外のバックアップ

本CAは、障害、自然災害等によるCAシステムの重要データの喪失に備え、また、業務継続性を確保することを目的に、CAシステムに関する重要なデータを定期的に本CAの施設と同程度の物理的セキュリティを備えた遠隔地保管場所へ保管します。

5.2 手続き的管理

5.2.1 信頼すべき役割

本CAは、セキュリティ確保のため、所定の手続きにより本サービスの業務に従事する者の職務権限を以下のとおり分離し、業務を行う者が単独で不正を行うことができないよう管理を行います。

a) サービス責任者 ― RA担当者、CA管理者の作業承認を行います
b) RA担当者 ― LRAの審査・登録・証明書発行・管理を行います
c) CA管理者 ― CAシステムの運用管理を行います
d) ログ検査者 ― 証明書の発行・失効などの業務が正しくおこなわれたかどうかを、ログをもとに確認します。

本CAがRA業務をLRAに委託する際、LRAについても加入者の証明書、私有鍵の管理においても職務権限を分離し、特定の個人が複数の役割を兼務することがないように管理統制を行います。

5.2.2 職務ごとに必要とされる人数

CAは、CA私有鍵を用いた操作等の重要操作については複数人によって行います。

5.2.3 個々の役割に対する本人性確認と認証

認証局システム、RAシステムへアクセスし、CA私有鍵の操作や証明書発行、失効に係わる操作等の重要操作を行う権限者は、本CAのサービス責任者により任命されます。

証明書の発行等の処理を行うに当たっては、本CPS「5.1.2. 物理的アクセス」の他

に、CAシステムによって操作者の識別と認証を行います。

5.2.4 職務分割が必要になる役割

CA私有鍵の操作やCAシステム管理者、RAシステムを操作するLRA申請業務担当者の登録等の重要操作は、複数人によるコントロールを実施します。このとき、CAシステム管理者、RAシステム管理者の登録に際しては権限付与を承認するものと登録を行う者の職務分離を図ります。同様に、RAで加入者証明書の利用申請の審査業務を行う者とRAシステムを操作し発行入力を行う者は、職務分離を図ります。

5.3 要員管理

CAは、本サービスの運用のセキュリティを確立するため、本CA所定の手続きによって適切な人事管理を行います。

5.3.1 資格、経験および身分証明の要件

本CAの業務運営に関して信頼される役割を担う者は、STN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します。

5.3.2 経歴の調査手続き

信頼される役割を担う者の信頼性と適格性を、本CAの規則の要求にしたがって、任命時および定期的に検証します。

5.3.3 研修要件

CAは、本サービスの業務に従事する者に対し、職務ごとに適切な教育を必要に応じて行うものとします。

5.3.4 再研修の頻度および要件

CAの運用に新たに携わる担当者は、運用の実業務にあたる前に職務に必要となるセキュリティや専門知識に関する新任教育を、また、CAの運用担当者は1年に1回、再教育を、本CAの定める規定に従い受講します。また、新知識、新技術の収得のための教育はこの周期にかかわらず、必要の都度、実施されます。

5.3.5 職務のローテーションの頻度および要件

CAの運用担当者は、複数職務の経験による職務遂行能力や技術向上、等を目的とし、定期的あるいは不定期に配置転換が行われます。また、配置転換の際には新任者に対して適切な期間のOJTや引継等を行い、本サービスの運用に支障をきたさないものとします。

5.3.6 認められていない行動に対する制裁

本CAの運用に従事するものが、業務遂行上重大な過失を犯した場合、別途、本CAの定める規定により相当の処罰をあたえることがあります。

5.3.7 独立した契約者の要件

本CAは、本サービスの運用業務の一部を外部機関に委託する場合、当該業務委託先との契約によって、当該業務委託先のもとで本サービスに従事する者の人事管理が適切に行われていることを確認します。

5.3.8 要員へ提供する資料

本CAは、本サービスに従事する者に対して、本サービスに関し業務上必要な文書のみの閲覧を許可します。

5.4 監査ログの取扱い

5.4.1 記録するイベントの種類

認証局は、CA システム、リポジトリシステム、認証局に関するネットワークアクセスの監査証跡やイベント・ログを監査ログファイル等に記録します。この中には、以下の事象を含みます。

a) CA私有鍵の操作
b) システムの起動・停止
c) データベースの操作
d) 権限設定の変更履歴
e) 証明書の発行
f) 証明書の失効
g) CRLの発行
h) 監査ログの検証
i) RAからの操作ログ
j) 入退室時の認証の記録
k) 不正侵入検知機等の警報ログ

5.4.2 監査ログを処理する頻度

本CAは、監査ログを毎営業日定期的に精査します。

5.4.3 監査ログを保存する期間

CAシステム上で生成される監査ログは、CAシステム上に保管されます。監査ログは、本CPS「5.5.2. アーカイブを保存する期間」 に従い、保管用記録として保存されます。

5.4.4 監査ログの保護

CAシステム上の監査ログは、予め定められた者だけが、調査し、確認することができます。また、監査ログは、権限を持たない者の閲覧や、改ざん、不正な削除から保護されています。

5.4.5 監査ログのバックアップ手続き

監査ログは、CAシステム上のデータと同様の手続きで、バックアップ用の媒体に格納され、安全な保管場所に保管されます。

5.4.6 監査ログの収集システム

監査ログの収集は、本CAが利用するシステムまたはソフトウェアにより自動的に行われます。

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

本CAは、監査ログの検査結果をもとに、必要に応じて運用面およびシステム動作面でのセキュリティ上のぜい弱性の評価を行い、見直しを行います。

5.5 記録の保管

5.5.1 アーカイブ記録の種類

本CAは、以下の情報をアーカイブとして作成し保管します。

a) 発行したすべての証明書
b) 証明書の発行、私有鍵の生成、失効、一時停止等に関する情報（申込書類、審査記録等を含みます）
c) CAの鍵ペアの作成に関する情報
d) CRLおよびその作成に関する記録
e) 本サービスの業務に関する基準および手順を記載した書類およびその変更に関する情報
f) 本CAの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
g) 監査の実施結果に関する記録

5.5.2 アーカイブを保存する期間

アーカイブの保存期間は、10年間または法律で規定された保存期間のどちらか長い期間とします。

5.5.3 アーカイブの保護

本CAは、適切なアクセスコントロールまたは改ざん防止措置等によりアーカイブの保

護を行います。

5.5.4 アーカイブのバックアップ手続き

アーカイブは、本CA所定の手続きによりバックアップを行います。

5.5.5 記録にタイムスタンプをつける要件

規定しません。

5.5.6 アーカイブ収集システム

規定しません。

5.5.7 アーカイブ情報を入手し、検証する手続き

規定しません。

5.6 鍵の切り替え

本CAは、定期的にCA私有鍵の更新を行います。その頻度は、本CPS「6.3.2 私有鍵と公開鍵証明書の有効期間」で規定します。CA私有鍵は、認証設備室内にて、複数人の操作で、専用の暗号モジュール（HSM）を用いて生成されます。

CA私有鍵の更新と共に自己署名証明書の更新も実施される。この更新においてもCA私有鍵生成の場合と同様に、複数人の操作にて実施されます。

5.7 危殆化および災害からの復旧

5.7.1 災害および CA 私有鍵危殆化からの復旧手続き

本CAは、想定される以下の脅威に対し、本CA所定の手続きにより復旧、または停止を行います。また、関係する認証局員全員に適切な教育・訓練を実施します。

a) CA私有鍵の危殆化
b) 火災、地震、事故等の災害
c) 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

システム障害またはデータの破損が発生したもしくは破損されたおそれがある場合、本CA所定の手続きにより本サービスの提供を停止し、被害状況および原因の調査を行います。この場合、本CAは、情報公開用Webサイト等を通じて加入者および検証者に通知または公表します。

5.7.3 CA 私有鍵が危殆化した場合の対処

CA私有鍵が危殆化または危殆化の恐れが生じた場合は、本CAのサービス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、CAは所定の手続きにより、全ての加入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

災害等によって中断した本サービスの再開が可能であると本CAが判断した場合、CA所定の手続きにより可能な限り速やかにシステム復旧を行い、本サービスの提供を再開します。

正常復旧を確認した後、本CAは、情報公開用Webサイト等を通じて加入者および検証者に復旧を通知または公表します。

災害などにより、認証施設および設備が被災し、通常の業務継続が困難な場合には、CA所定の手続きにより、加入者および検証者に被災状況等の情報を公開します。

5.8 認証局または登録局の終了

本CAは、CAの判断により本サービスを終了することができるものとします。この場合、CAは本サービスを終了する少なくとも90日前までに加入者および検証者に対して通知または公表します。

LRAの運用を停止する場合は、LRAの持っている加入者の情報と運営をCAまたは他のLRAに移管し、それを加入者に通知します。なお、LRAは、このような場合にCAや他のLRAに加入者の情報や運営を他のRAに移管することについて、事前に加入者の同意を得るものとします。

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

CA鍵ペアは、FIPS140-2 レベル3準拠のHSMによって生成します。CA鍵ペアの生成手続きは、CAサーバの設置された室において複数名のCA管理者、運用管理者によって行われるものとします。

加入者の鍵ペアをCAで生成する場合には、FIPS 140-2 レベル2準拠のHSMによって生成します。

6.1.2 加入者への私有鍵の送付

＜認証局が鍵ペアを生成する場合＞

加入者私有鍵が認証局で生成される場合は、CAは複数人による運用にて、私有鍵および証明書をICカード等のメディアに格納し、手交または本人限定受け取り郵便にて加入者へ安全に送付します。その後、複数人による運用にてCA内の加入者のすべての私有鍵データを削除し、その記録を残すものとします。

なお、LRAが私有鍵および証明書をICカード等のメディアに格納する場合、認証局は私有鍵生成後、LRAの定められたシステムまたは担当者のみが復号できる形式で暗号化をおこない、証明書を含め、それら暗号化された鍵ペアデータを安全な方法でLRAに送ります。鍵ペアのうち暗号化された私有鍵部分については、LRAへの送付後、すみやかにCAが管理するサーバから削除し、その記録を残すものとします。LRAは、暗号化されているデータを受領後、複数人による運用にて当該データを復号し、私有鍵および証明書をICカードに格納し、そのICカードは手交、または本人限定受取郵便等、各LRAが定めた安全な方法で加入者へ送付されます。その後、LRAは、複数人による運用にて加入者のすべての私有鍵データを削除し、その記録を残すものとします。

＜加入者が鍵ペアを生成する場合＞

CA は、「4.3.1　証明書発行時の認証局の機能　＜加入者が鍵ペアを生成する場合＞」の手順にしたがって、鍵ペアを生成する時に用いる 2 つの識別符号を加入者に通知します。加入者は本 CA の証明書発行サイトにアクセスし、2 つの識別符号を入力することにより、加入者私有鍵、および対応する公開鍵の鍵ペアを生成し、証明書をダウンロードできます。

6.1.3　認証局への公開鍵の送付

エンドエンティティの加入者の公開鍵が加入者により生成される場合は、IETF RFC 2510「証明書管理プロトコル」にしたがってオンライントランザクションで、または同様に安全な方法によって、本CAに引き渡されるものとします。

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、リポジトリ上にCA公開鍵を公表します。

6.1.5　鍵のサイズ

CA私有鍵の鍵長はRSAの2048 ビットとし、加入者の私有鍵の鍵長は、RSAの1024 ビットとします。

6.1.6　公開鍵のパラメータ生成および品質検査

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ます。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します。

6.1.7　鍵の使用目的

認証局の鍵は、keyCertSignとcRLSignのビットを使用する。

エンドエンティティの鍵は、署名用証明書においてはnonRepudiationのビットを立て、認証用証明書においてはdigitalSignature、keyEnciphermentのビットを立てます。

CA私有鍵は、以下の目的のために利用されます。

a) 加入者の証明書への電子署名
b) CA証明書への電子署名
c) CRLへの電子署名
d) CAシステムに対する証明書への電子署名
e) CAおよびRAシステムを操作する者に対する証明書への電子署名

6.2　私有鍵の保護およ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および管理

CA私有鍵の格納モジュールは、FIPS 140-2　レベル3の認定を取得したHSMを利用します。また、エンドエンティティの加入者私有鍵の格納モジュールは、FIPS 140-2　レベル1 と同等以上の規格に準拠するものとします。

6.2.2　複数人による私有鍵の管理

CA私有鍵の生成は、運用管理者と複数名の権限者によって行われます。また、鍵生成後の私有鍵の操作（活性化、非活性化、バックアップ、搬送、破棄等）においても複数名の権限者によって行われます。

6.2.3　私有鍵のエスクロウ

CAはCA私有鍵および加入者私有鍵のエスクロウを行いません。

6.2.4　私有鍵のバックアップ

CA私有鍵のバックアップは、CAの障害や災害時の復旧を目的として取得します。CA私有鍵のバックアップは、バックアップ作業の権限を有する複数人の立会いのもとで行い、暗号化された状態でCAサーバの設置された室に保管します。

CAは加入者の私有鍵のバックアップは行いません。

6.2.5　私有鍵のアーカイブ

CAは、CA私有鍵および加入者私有鍵のアーカイブは行いません。

6.2.6　暗号モジュールへの私有鍵の格納と取り出し

CA私有鍵のバックアップは暗号化された形式で保管されており、他のHSMでの回復処理には、HSMを操作するための管理者用ICカードが必要となり、所定の手順でのみ回復することができます。

6.2.7　暗号モジュールへの私有鍵の保管

CA私有鍵は、暗号化された状態でCAサーバの設置された室に保管します。

6.2.8　私有鍵の活性化方法

CA私有鍵の活性化は、CAの起動時にHSM を操作するために必要な操作用ICカードに格納されているデータによって活性化させます。以上の操作は複数名のCA管理者によっておこなわれます。

6.2.9　私有鍵の非活性化方法

CA私有鍵の非活性化は、CAを停止させるかもしくはHSM操作用のICカードをスロットから抜くことで非活性化します。以上の操作は複数名のCA管理者によっておこなわれます。

6.2.10　私有鍵の廃棄方法

CA私有鍵を廃棄しなければならない状況の場合は、CA所定の手続きにより、複数名のCA管理者によって完全に初期化または物理的に破壊し、廃棄されるものとします。バックアップについても同様の手続きによるものとします。証明書の有効期間の満了した、または本CPS「4.9.1 証明書失効の要件」により失効された加入者のIC カードは、加入者の責任のもと廃棄するものとします。

6.2.11　暗号モジュールの評価

CAが利用する暗号モジュールの品質基準については、本CPS「6.2.1 暗号モジュールの標準および管理」のとおりとします。

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

CA公開鍵および加入者の公開鍵は、証明書のアーカイブに含まれ、本CPS「5.5.2 アーカイブを保存する期間」において規定された期間保存します。

6.3.2 私有鍵と公開鍵証明書の有効期間

CAは、CA私有鍵の有効期間20年に対して、遅くとも10年が経過する前には新しいCA鍵ペアを生成し、連続性を確保します。ただし、暗号のセキュリティが容認できないほどぜい弱になった場合は、CAの判断により、CA 鍵ペアの更新を行うことができるものとします。

更新前のCA証明書は、その20年の有効期間を満了するまでの間、有効となります。CA私有鍵および証明書の更新は、CA所定の手続きにより安全に行われます。本CAは、常に最新のCA私有鍵を用いて証明書の発行を行います。

署名用証明書の私有鍵および証明書の有効期間は、5年以内とします。その鍵の使用は2年を経過して使用しないものとします。

認証用証明書の私有鍵および証明書の有効期間は、3年と1ヶ月を越えないものとする。

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

CA私有鍵を操作するために必要な活性化データは、複数名のCA管理者によって一意で予測不能なものとして生成され、管理用ICカードに格納されます。
加入者私有鍵の活性化データがCAで生成される場合は、加入者に配付する、ICカードについてのPINコード設定用暗証番号は一意で予測不能なものとし、CAまたはRAが管理する安全な環境においてICカードに対して生成されます。その上で、加入者に安全に伝えられるものとします。

加入者私有鍵の活性化データを加入者が生成する場合は、活性化データは予測不能なものとし、その生成とインストールはRAで定める所定の手順もしくは、加入者が利用するアプリケーションの手順に従い実施されるものとします。

6.4.2 活性化データの保護

CAで使用するHSMの起動は管理用IC カードで行います。管理用ICカードは、HSMと同等の環境において安全に保管管理します。

加入者私有鍵の活性化データが本CAで生成される場合は、活性化データが加入者に伝えられた後は、本CAおよびRAにおいては完全に破棄し保管しません。また、伝えられた活性化データは、加入者により安全に保護するものとします。

加入者私有鍵の活性化データを加入者が生成する場合は、本CAで定められた規定に従い、加入者により安全に保護するものとします。

6.4.3　活性化データのその他の要件

規定しません。

6.5　コンピュータのセキュリティ管理

CAシステムは、物理的に安全な環境に設置され、アクセスコントロール、複数人の立会いによる操作、監査ログの検査等、運用面においても適切なセキュリティ管理を行います。

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

認証業務用設備に対する当該電気通信回線を通じて行われる不正なアクセス等を防御するための対策を実施します。

CAシステムへのログイン時には、本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実施します。

6.5.2　コンピュータセキュリティ評価

CAではＣＡシステムに用いるハードウェア、ソフトウェアのセキュリティ基準を設ける等の対応を行い、客観的に評価を行います。

6.6　ライフサイクルの技術的管理

本CAは、CAシステムの構築およびメンテナンスを安全な設備の中で行います。CAシステムの変更を行う場合は、CA所定の手続きにより安全性を評価、確認するものとします。CAシステムに導入するコンピュータセキュリティ技術の管理においては、最新のセキュリティ技術を導入するために、適切なサイクルでセキュリティチェックを行います。

6.6.1　システム開発管理

情報システムへのセキュリティの組み込みを確実にするために、システム開発時の要件定義にはセキュリティ要件を含めて開発を行います。セキュリティ要件の実装には、必要に応じて暗号技術を含めて実装します。

開発テスト用のシステムが設置されている設備室には物理的なセキュリティを確保し、入退室に関しては関係者以外が容易に立ち入ることが出来ないようにするための措置を講じます。また、開発テスト用のシステムへのネットワークアクセスは、開発に使用を認められた端末以外からのアクセスができないように限定されています。外部に公開するプログラムに関してはセキュリティ上、脆弱なコードがないことを事前に確認します。ソフトウェア開発を外部委託する際には、セキュリティ要件を定め、委託先のセキュリティ確保状況を事前に確認します。

6.6.2　セキュリティ運用管理

＜システムのセキュリティ要求事項＞

情報システムへのセキュリティの組み込みを確実にするために、システム変更時には、セキュリティ要件の検討を実施し、計画に反映されていることを確認します。

＜業務用システムのセキュリティ＞

CAシステムにおける利用者データの消失、変更または誤用を防止するために、CAシステムにおいて、入力データの妥当性、重要データに対する改ざんがないこと、および、出力データの妥当性を確認します。

＜暗号による管理策＞

情報の機密性、真正性または完全性を保護するために、取り扱う情報の重要性に応じ電子署名や暗号化を行います。

＜システムファイルのセキュリティ＞

本CAサービスの業務において、セキュリティが保たれた状態で実施されることを確実にするために、「5.2 手続き的管理」で定めるとおり、業務に従事する者の職務権限を分離し、許可された以外の者がソフトウェアの実行、利用ができないよう管理します。

また、テストを実施する場合には、本番環境より隔離したテスト環境を用いて実施します。

＜開発および支援過程によるセキュリティ＞

CAシステムおよび情報のセキュリティを維持するために、システムの変更においては、作業計画および承認の記録を残します。また、OSのパッチ導入などを適切なタイミングで行います。

＜事業継続管理＞

事業活動の中断に対処するとともに、重大な障害または災害の影響から重要な事務手続きを保護するために、適切なリスク分析の結果に基づく、全社の災害復旧方針を定めます。また、本サービスにおける災害復旧計画を定め、適切な時間内で維持または復旧させるための手順および役割、体制、連絡体制などを定め、定期的に訓練を実施します。

6.6.3　ライフサイクルのセキュリティ管理

「6.6 ライフサイクルの技術的管理」の記述のとおりとします。

6.7　ネットワークのセキュリティ管理

CAシステムへのアクセスは、許可された者だけがアクセスできるように制限されており、外部からのアクセスは認証局のソフトウェアの特性を使用して、真正性が確認さ

れ、暗号化されたセッションだけが、アクセスを許可されます。

6.8 タイムスタンプ

認証設備は、アプリケーション等において正確な日付・時刻を使用することとします。GPSによる時刻同期を行います。

7　証明書、失効リストおよびOCSP のプロファイル

7.1　証明書のプロファイル

本CA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）により一意に識別されるものとする。

CAが発行する証明書のプロファイルの基本領域は、次のとおりである。

証明書シリアル番号： CA毎に一意に識別できる文字列
署名アルゴリズム：「7.1.3 アルゴリズムオブジェクト識別子」で指定する
　　オブジェクト識別子
認証局DN：　「3.1 名前決定」で記述したX.500識別名
Validity (not before)：UTCTimeで表現された時刻
Validity (not after)：UTCTimeで表現された時刻
サブジェクトDN：　「3.1 名前決定」に従ったX.500識別名
サブジェクト公開鍵：RFC3280に従ったエンコード
署名：　RFC3280に従ったエンコード

7.1.1　バージョン番号

本CA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す。

7.1.2　証明書の拡張（保健医療福祉分野の属性を含む）

7.1.2.1　鍵使用法 (keyUsage)

鍵使用法拡張は、CA証明書、加入者証明書ともにクリティカルな拡張です。CA証明書の鍵使用法をあらわすビットとして、certSign, crlSign のビットを立てます。

加入者証明書の鍵使用法については、認証用証明書については digitalSignature、keyEncipherment のビットを立て、署名用証明書には nonRepudiation のビットを立てます。

7.1.2.2　証明書ポリシ拡張

加入者の証明書ポリシ拡張には「7.1.6 CPオブジェクト識別子」で規定するオブジェクト識別子を指定します。CA証明書には証明書ポリシ拡張を持ちません。加入者証明書で証明書ポリシ拡張を設定する場合には、署名用証明書ではクリティカルな拡張とな

り、認証用証明書ではノンクリティカルとなります。

7.1.2.3　サブジェクト別名

加入者の証明書には加入者のインターネット電子メールアドレス(rfc822Mail)を指定することできます。

認証用証明書でS/MIMEに使用する際には電子メールアドレスを必ず指定する必要があります。

メールアドレスが指定されない場合には、証明書中にこの拡張はありません。加入者の証明書のサブジェクト別名拡張はクリティカルな拡張ではありません。　CA証明書はサブジェクト別名拡張を持ちません。

7.1.2.5　基本制約 (basicConstraint)

CA証明書の基本制約拡張はクリティカルな拡張で、CAフィールドがTRUEで設定されています。PathLengthフィールドは指定しません。　加入者の証明書にはこの拡張を含みません。

7.1.2.6　CRL配布点

加入者の証明書のCRL配布点には、CAが発行した証明書のすべてのCRLエントリを含んだCRLの配布点をURL形式で指定します。

認証用のCAでは、

'http://repo1.secomtrust.co.jp/sppca/mds1/fullCRL.crl'

'ldap://repo1.secomtrust.co.jp/cn=STN-A01-forAuthentication,o=SECOM Trust.net Co. Ltd.,c=JP?certificateRevocationList'

署名用CAでは、

'http://repo1.secomtrust.co.jp/sppca/mds2/fullCRL.crl'

'ldap://repo1.secomtrust.co.jp/cn=STN-A01-forNonRepudiation,o=SECOM Trust.net Co. Ltd.,c=JP?certificateRevocationList'

また、当該加入者のCRLエントリが入る分割CRLの配布点をX.500識別名で指定します。分割CRLは外部に公開していません。

認証用CA:　CN=CRL<n>, CN=MEDIS-A01-forAuthentication,　O=SECOM Trust.net Co. Ltd.,　C=JP

署名用CA: CN=CRL<n>, CN=MEDIS-A01-forNonRepudiation, O=SECOM Trust.net Co. Ltd., C=JP

CRL配布点拡張はクリティカルな拡張でありません。CA証明書についてはCRL配布点拡張を含みません。

7.1.2.7 機関鍵識別子

CA証明書、加入者証明書ともにRFC3280に準拠した鍵識別子を使用します。機関鍵識別拡張はクリティカルな拡張ではありません。

7.1.2.8 サブジェクト鍵識別子

CA証明書、加入者証明書ともにRFC3280に準拠した鍵識別子を使用します。サブジェクト鍵識別子拡張はクリティカルな拡張ではありません。

7.1.2.9 サブジェクトディレクトリ

加入者証明書のサブジェクトディレクトリ属性には、「保健医療福祉分野PKI認証局証明書ポリシ 7.1.3 保健医療福祉分野の属性(hcRole)」で記述されているhcRole属性を指定します。この拡張は加入者が保健医療福祉分野の該当する国家資格を保有している場合および医療機関の管理責任者の場合は指定し、それ以外の場合は省略します。

本CAでは、国家資格および管理者資格が最大4つまで指定できます。

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通りとします。

sha1WithRSAEncryption (1.2.840.113549.1.1.5)

基本領域のsubjectPublicKeyInfoアルゴリズムは以下の通りとします。

RSAEncryption (1.2.840.113549.1.1.1)

7.1.4 名前の形式

サブジェクトの識別名は 「3.1 名前決定」の命名規則にしたがいます。

7.1.5 名前制約

用いません。

7.1.6 CP オブジェクト識別子

＜署名用証明書の場合＞

表7.1 に示す、「保健医療福祉分野PKI認証局 証明書ポリシ」で定めるOIDを使用する。

表7.1 本CPSで使用する署名用証明書のOID

名称	オブジェクト識別子
HPKI 署名用証明書ポリシ	1.2.392.100495.1.5.1.1.3.1
HPKI 署名テスト用証明書ポリシ	1.2.392.100495.1.5.1.1.0.1

＜認証用証明書の場合＞

表7.2 に示す、「MEDIS認証局 認証用 証明書ポリシ」で定めるOIDを使用する。

表7.2 本CPSで使用する認証用証明書のOID

名称	オブジェクト識別子
MEDIS認証局 認証用証明書ポリシ	1.2.392.200119.2.2.1.1.1.1
MEDIS認証局 認証テスト用証明書ポリシ	1.2.392.200119.2.2.1.0.1.1

7.1.7 ポリシ制約拡張

使用しません。

7.1.8 ポリシ修飾子の構文および意味

証明書ポリシ拡張において、証明書ポリシ修飾子は指定しません。

7.1.9 証明書ポリシ拡張フィールドの扱い

本CPS のOID を格納します。

7.1.10 保健医療福祉分野の属性（hcRole）

該当するCPに準じます。

7.2 証明書失効リストのプロファイル

STNが発行するCRLは、X.509 バージョン2形式で、RFC3280に準拠し作成します。

7.2.1 CRL プロファイル－基本領域

Version	7.2.1 に記述したバージョン番号を指定
署名アルゴリズム	アルゴリズムとしてsha1withRSAEncryption (1 2 840 113549 1 1 5)
発行者	CAの名前を記載します。
thisUpdate	UTCTimeで記載します。
nextUpdate	UTCTimeで記載します。
revokedCertificate	失効した証明書の証明書シリアル番号および失効時刻を記載します。

7.2.2 CRL プロファイル－CRL エントリ拡張

reasonCode	RFC3280で規定された失効理由コードを記載します。

7.2.3 CRL プロファイル－CRL 拡張

authorityKeyIdentifier	CAの公開鍵のSHA1ハッシュ値を記載します
CRLNumber	CA毎のCRLの通し番号で、CRLが発行するたびに増加していく数字が記載されます。

7.3 OCSP プロファイル

OCSPは使用しません。

7.3.1 バージョン番号

規定しません。

7.3.2 OCSP 拡張領域

規定しません。

8　準拠性監査とその他の評価

8.1　監査頻度

CAは、本サービスの運用がこのCPSに準拠して行われていることを、毎年、1年より長くない間隔で監査を行います。但し、移管、譲渡、合併など、認証局の構成に大規模な変更があった場合は直ちに監査を実施するものとします。

8.2　監査者の身元・資格

CAは、認証局業務を直接行っている部門から独立した、適切な能力を有する監査者により定期監査を実施します。

8.3　監査者と被監査者の関係

監査者は、監査に関する事項を除き、CAの被監査部門の業務から独立した立場にあるものとします。監査の実施にあたり、CAの被監査部門は監査に協力するものとします。

8.4　監査テーマ

監査対象は、本サービスの運用がこのCPSに準拠して行われていること、並びに外部からの不正アクセスおよび内部における不正行為に対するコントロールが適切に行われていること等とします。

8.5　監査指摘事項への対応

重要または緊急を要する監査指摘事項に対しては、速やかに是正を行います。その場合、是正されるまでの間、CAは本サービスの提供を停止することがあります

8.6　監査結果の通知

監査結果は、監査者からポリシ委員会に報告されます。この監査結果は、このCPS「5.5.2. アーカイブを保存する期間」に定める期間、保存します。また、監査者によって証明書の信頼性に影響する重大な欠陥が発見された場合は、加入者および検証者および該当するCPが定める外部機関に直ちに通知するものとする。

9　その他の業務上および法務上の事項

9.1　料金

加入者は、本サービスの利用について、CAが別途定める料金をCAまたはCAが指定する組織に支払うものとします。

9.2　財務上の責任

本CAは、その継続的な運営に必要とされる十分な財務的基盤を維持するものとします。

9.2.1　保険の適用範囲

規定しません。

9.2.2　その他の資産

規定しません。

9.2.3　エンドエンティティに対する保険または保証

規定しません。

9.3　企業情報の秘密保護

9.3.1　秘密情報の範囲

本CPSに従うCAが保持する個人および組織の情報は、証明書、CRLの一部として明示的に公表されたものを除き、秘密保持対象として扱われます。CAは、法の定めによる場合および加入者による事前の承諾を得た場合を除いてこれらの情報を外部に開示しません。

加入者の私有鍵は、その加入者によって秘密保持すべき情報であり、CAでは、いかなる場合でもこれらの鍵へのアクセス手段を提供していません。

監査ログに含まれる情報および監査報告書は、秘密保持対象情報です。CAは、本CPS「8.6 監査結果の通知」に記載されている場合、法の定めによる場合、および監査者が監査を行う上で必要な場合を除いて、これらの情報を外部へ開示しません。

ただし、CAは、かかる法的手続き、司法手続き、行政手続きあるいは法律で要求されるその他の手続きに関連してアドバイスする法律顧問および財務顧問に対し、秘密保持対象として扱われる情報を開示することができるものとします。

また組織の合併、買収あるいは再編成に関連してアドバイスする弁護士、会計士、金融機関およびその他の専門家に対しても、CAは秘密保持対象として扱われる情報を開示することができるものとします。

9.3.2 秘密情報の範囲外の情報

証明書およびCRLに含まれている情報は秘密情報として扱わない。その他、次の情報も秘密情報として扱わない。

- 本CA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
- 情報等を取得した際、既に自ら正当に所有していた情報
- 開示に関して加入者によって承認されている情報
- 別途CPに定められた事項

9.3.3 秘密情報を保護する責任

CA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、内部およ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います。

ただし、CAが保持する秘密情報を、法の定めによる場合および加入者による事前の承諾を得た場合に開示することがあります。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ません。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ものとします。

9.4 個人情報のプライバシー保護

9.4.1 プライバシープラン

CAにおける個人情報の取り扱いについては、下記の「個人情報保護方針」を適用するものとする。

「セコムトラストネット株式会社 個人情報保護方針」
(www.secomtrust.net/privacy/index.html)

9.4.2 プライバシーとして保護される情報

CAは、次の個人情報をプライバシーとして保護すべき情報として取り扱います。

a) RA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します
b) CRLに含まれない加入者の証明書失効または停止の理由に関する情報
c) その他、CAが業務遂行上知り得た加入者の個人情報

9.4.3 プライバシーとはみなされない情報

CAは、次の個人情報をプライバシーとして保護すべき情報として取り扱いません。

a) 公開鍵証明書
b) CRLに記載された情報

9.4.4 個人情報を保護する責任

CA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、個人情報の取扱に関するわが国の法令、並びにCA所定の手続きにより適切に収集、利用、管理を行います。内部およ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ものとします。

9.4.5 個人情報の使用に関する個人への通知および同意

CAは、証明書発行業務およびその他の認証業務の利用目的に限り個人情報を利用します。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します。

9.4.6 司法手続きまたは行政手続きに基づく公開

法令、規則、行政庁の命令等により本サービスに関わる個人情報の開示が義務付けられる場合（当局検査を含みます）、CAは加入者の承諾なくして当該法令、規則、命令等の定める手続きに基づいて個人情報を開示することがあります。CAが個人情報を開示したことにより生じた損害について、CAは責任を負いません。

9.4.7 その他の情報開示条件

個人情報を提供した本人また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、CAで別途定める手続きにしたがって情報を開示します。

9.5 知的財産権

CAと加入者との間で別段の合意がなされない限り、CAが提供するサービスに関わる情報、資料、およびデータは、次に示す当事者の権利に属するものとする。

a) 加入者証明書：CAに帰属する財産である
b) 加入者の私有鍵：私有鍵は、その保存方法または保存媒体の所有者に関わらず、公開鍵と対になる私有鍵を所有する加入者に帰属する財産である
c) 加入者の公開鍵：保存方法または保存媒体の所有者に関わらず、対になる私有鍵を所有する加入者に帰属する財産である
d) 本CPS：本CAに帰属する財産（著作権を含む）である

9.6 表明保証

9.6.1 認証局の表明保証

CAは、その運営にあたり、該当するCPおよび本CPSに基づいて、加入者および検証

者に対して次のCAとしての責任を果たすものとする。

a) 提供するサービスと運用のすべてが、該当するCPの要件と本CPSにしたがって行われること。
b) 証明書の発行時に、RAが申請者の申請内容の真偽の確認を確実に行うこと。
c) 本CAが証明書を発行する時は、証明書に記載されている情報が本CPにしたがって検証されたことを保証すること。
d) 公開鍵を含む証明書を加入者に確実に届けること。
e) 失効事由が生じた場合は、CAで定める失効ポリシにしたがって証明書を確実に失効すること。
f) CRLなどの重要事項を本CAの定める方法により、速やかに入手できるようにすること。
g) CAの定める方法で、CPに基づく加入者の権利と義務を各加入者に通知すること。
h) 鍵の危殆化のおそれ、証明書または鍵の更新、サービス内容の変更、および紛争解決をするための手続きを加入者に通知すること。
i) 本CPS「5 建物および関連施設、運用のセキュリティ」および「6 技術的セキュリティ管理」に従い本CAを運営し、私有鍵の危殆化を生じさせないこと。
j) CA私有鍵が、以下の目的で署名するためだけに使用されることを保証すること。
    - 加入者の証明書への電子署名
    - CA証明書への電子署名
    - CRLへの電子署名
    - CAシステムに対する証明書への電子署名
    - CAおよびRAシステムを操作する者に対する証明書への電子署名
k) 申請者の申請内容の真偽の確認において利用した書類を含む、各種の書類の滅失、改ざんを防止し、10年間保管すること。
l) 本CAの発行する証明書の中で、加入者に対して、加入者の名称（subjectDN） の一意性を保証すること。

＜CAが加入者の鍵ペアおよび証明書をICカード等に格納する場合＞
CAは上記に加え、以下の責任を果たすものとします。
a) 加入者の私有鍵を複数人による運用にてICカード等に格納し、加入者本人のみに確実に届けること。
b) 加入者の私有鍵を、加入者以外の第三者に漏洩しないこと。
c) ICカード等を発送した後、複数人による運用にて加入者の私有鍵データを消去し、その記録を残すこと。

9.6.2 登録局の表明保証

登録局は、本CAから独立してRAを運営する場合、RAは本CPSに定める事項を遵守し、加入者、検証者、CAに対して次の責任を果たすものとします。また、RAは、CAに代わって果たす行為について個別に責任を負います。

a) 証明書発行にあたり、申請内容の真偽の確認を確実に行い、確認の結果を認証局に対して保証すること。
b) CAの発行する証明書の中で、加入者に対して加入者の名称（subjectDN）の一意性を保証すること。

c) 証明書申請情報を本CAに安全に送付し、登録記録を安全に保管すること。
d) 証明書失効申請を行う場合は、本CPS「4.9.3 失効申請の処理手順」にしたがって失効申請を行うこと。
e) 将来の検証のため、また証明書がどのように、どの申請に基づき生成されたかを管理可能なように、証明書の作成要求または失効要求などの記録を、CAに移管した場合を除き、証明書の有効期間満了後10年間保管すること。
f) 加入者の私有鍵をICカードに格納した場合、ICカードを発送した後、RAは、複数人による運用にて加入者の私有鍵データを消去し、その記録を残すこと。

＜RAが加入者の鍵ペアおよび証明書をICカード等に格納する場合＞
RAは上記に加え、以下の責任を果たすものとします。
a) 加入者の私有鍵を複数人による運用にてICカード等に格納し、加入者本人のみに確実に届けること。
b) 加入者の私有鍵を、加入者以外の第三者に漏洩しないこと。
c) ICカード等を発送した後、複数人による運用にて加入者の私有鍵データを消去し、その記録を残すこと。

9.6.3 加入者の表明保証

本CAの加入者は、本CAに対して次の責任を果たすものとします。

a) 証明書発行申請内容に対する責任
証明書発行申請を行う場合、CAに提示する申請内容が虚偽なく正確であることに対する責任を果たすこと。
b) 証明書の受領時に証明書記載内容を確認する責任
証明書の記載内容について証明書の受領時に確認を行い、申請内容と相違ないかを確認すること。また、記載内容について現状との乖離が発生した場合には、速やかに当該証明書の失効手続きを行うこと。
c) 鍵などの管理責任
私有鍵を保護し、紛失、暴露、改ざん、または盗用されることを防止するために妥当な措置を取ること。
d) 各種の届出に対する責任
私有鍵の紛失、暴露、その他の危殆化、またはそれらが疑われる時には、CAの定めるCPSにしたがって速やかに届け出ること。
また、証明書情報に変更があった場合は、本CPSにしたがって速やかに届け出ること。
e) 利用規定の遵守責任
加入者は、本CPSおよびCAで加入者に対して開示される文章を読み、その利用規定および禁止事項を遵守すること。

9.6.4 検証者の表明保証

本CAから発行した証明書を利用する検証者は以下の責任を果たすものとする。

＜利用規定の遵守責任＞
検証者は、本CPSおよびCAで検証者に対して開示される文章を読み、その利用規定および禁止規定を遵守しなければなりません。また、証明書の利用目的が、自己の利用目的に合致していることを承諾する必要があります。なお、証明書の利用に

際しては信頼点の管理(当該証明書を発行している認証局およびその認証局にサイニングを行う中間認証局やルート認証局を信頼し、各認証局の証明書を受容すること）を確実に行わなければなりません。

＜証明書有効性の確認責任＞

検証者は、証明書を利用する際に、その有効性を確認する責任があります。有効性の確認には、以下の事項が含まれます。

a) 本CAの公開鍵証明書のフィンガープリントを確認し、本CAの証明書であることを確認すること。
b) CA公開鍵を用いて証明書に行われた電子署名を検証することにより、当該証明書の発行者を確認すること。
c) 証明書の有効期限が満了していないことを確認すること。
d) 証明書が失効されていないことをCRLによって確認すること。
e) 証明書の記載事項が、別途定めるCPおよび本CPS「7 証明書および失効リストおよびOCSP のプロファイル」に記述されているプロファイルと合致していること。特に、次の2 点の検証を実施することが重要である。
   - OIDおよびIssuerのCNが該当するCPの規定に一致していること
   - 署名用証明書のkeyUsageは、nonRepudiationのみが立てられていること
   - 認証用証明書のkeyUsageは、DigitalSignatureとKeyEnciphermentのみが立てられていること、
   - hcRole属性のプロファイルの確認

9.6.5 他の関係者の表明保証

規定しません

9.7 無保証

本CAは、本CPS「9.6.1 認証局の表明保証」および「9.6.2 登録局の表明保証」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、付随的損害または派生的損害に対する責任を負わず、いかなる逸失利益、データの紛失またはその他の間接的もしくは派生的損害に対する責任を負わない。

また、本CPS「9.16.5 不可抗力」で規定される不可抗力によるサービス停止によって加入者、もしくはその他の第三者において損害が生じた場合、本CAは一切の責任を負わない。

9.8 責任制限

本CAは、加入者において電子証明書の利用または私有鍵の管理その他加入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CAおよびRAの責任は、CAおよびRAの怠慢行為により本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CPS「9.6 表明保証」に関し、次の場合、CAは責任を負わない。

a) CA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
b) 加入者また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
c) 加入者または検証者のシステムに起因して発生した一切の損害
d) 加入者また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
e) CAの責に帰することのできない事由で電子証明書およびCRLに公開された情報に起因する損害
f) CA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
g) 証明書の使用に関して発生する業務または取引上の債務等、一切の損害
h) 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
i) 加入者が契約に基づく契約料金を支払っていない間に生じた損害
j) 天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、本サービスの業務停止に起因する一切の損害

また、CAは、加入者と第三者間（これには検証者を含みます）における契約その他取引関係については一切関与せず、いかなる責任も負わないものとします。

9.9 補償

本CPSに規定された責任を果たさなかったことに起因して、CAがサービスの加入者に対して損害を与えた場合、加入者が本サービスの対価として本CAに支払った額の直近1年分を上限として損害を賠償します。ただし、CA側の責に帰さない事由から発生した損害、逸失利益、間接損害、または予見の有無を問わず、特別損害については、いかなる場合でも一切の責任を負わず、補償の対象としません。

また、加入者は本CAが発行する証明書を申請した時点で、検証者は証明書を信頼した時点で、「9.6.3 加入者の表明保証」や「9.6.4 検証者の表明保証」で記されたそれぞれの責任を故意または不注意で果たさなかった場合、本CAおよび関連する組織等に対する損害賠償責任が発生します。

9.10 本ポリシの有効期間と終了

9.10.1 有効期間

本CPSは、作成された後、ポリシ委員会により審査、承認されることにより有効となります。また、「9.10.2 終了」で記述する本CPSの終了まで有効であるものとします。

9.10.2 終了

本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、ポリシ委員会が無効と宣言した場合または本CAが運用を終了した場合、無効になります。なお、本CAが運用を終了する場合、加入者に対し90日前までに電子メールまたは書面によりその旨通知するものとし、原則として終了日をもって電子証明書を失効します。

9.10.3 終了の影響と存続条項

文書が終了した場合であっても、「9.3 企業情報の秘密保護」、「9.4 個人情報のプライバシー保護」、「9.5 知的財産権」に関する責務は存続するものとします。また、ポリシ委員会において部分的な存続を定めた場合は、当該存続部分は有効なものとします。

9.11 関係者間の個々の通知と連絡

CAから加入者への通知方法は、別項で特に定めるものを除き、電子メール、リポジトリ上、郵送による書面通知などCAが適当と判断した方法により行うものとします。また、CAから加入者の届け出た住所、FAX番号または電子メールアドレスに宛てて加入者への通知を発した場合には、それらの連絡先が誤りで有ることに起因して当該通知が延着または不着となった場合であっても、通常到達すべき時に到達したものとみなします。

本通知はLRAが代行して行う場合もあります。

9.12 改訂

9.12.1 改訂手続き

本CPSは、CAの判断によって適宜改訂され、ポリシ委員会の承認をもって成立するものとします。加入者、検証者は、公表された内容に同意しない場合には、公表から1週間以上のCAが相当と認める期間内にその旨をCAに通知するものとします。CAがこの変更に同意しない旨の通知を受領しない場合には、変更に同意があったものとみなします。また、変更に同意しない旨の通知があった場合には、CAは本サービスの解約および証明書の失効を行うことができるものとします。

9.12.2 通知方法と期間

本CPSが改訂された場合、情報公開用Webサイト等を通じて、全ての加入者、関連するCAおよび検証者に速やかに公開します。改訂内容の発効期日については公開時に明示するものとし、次のように定めます。

a) 重要な変更は、通知後90日を上限として、通知に定められた告知期間を経て効力を発します。なお、通知後、上記で示した方法に従い通知を行うことにより、変更を中止することもあり得ます。但し、監査指摘事項などによる緊急を要する重要な変更は、通知後、即、効力を発します。
b) 重要でない変更は、通知後直ちに効力を発します。

9.12.3 オブジェクト識別子（OID）の変更理由

規定しません。

9.13 紛争解決手続き

CA、加入者および利用者の所在地に関わらず、本CPS の解釈、有効性およびSTNが行う本サービスに関わる紛争については、日本国の法律が適用されます。調停、仲裁および裁判地は東京都区内における紛争処理機関を専属的管轄とします。

なお、本サービスの利用に関し、STNに対して訴訟、仲裁を含む解決手段に訴えようとする場合、STNに対して事前にその旨を通知しなければならないものとします。

9.14 準拠法

このCPSの効力、履行および解釈に関しては、すべて日本法が適用されるものとします。また、このCPSでの認証業務における個人情報の取扱に関しては「個人情報の保護に関する法律」および関連する日本国内法規に準じます。

9.15 適用法の遵守

本CPSの運用にあたっては、日本国内法および公的通知等がある場合はそれを優先します。

9.16 雑則

9.16.1 完全合意条項

本CPSは、本CPSに定められたサービスに対して当事者間の完全合意を構成し、認証業務について記述された書面または口頭による過去の一切の意思表示、合意または表明事項に取って代わるものです。

9.16.2 権利譲渡条項

関係者は、本CPSに定める権利義務を担保に供することができない。また、次の場合を除き、第三者に譲渡することができない。

- 本CAがRAに本CPに定める業務の委託を行うとき
- 本CAの移管もしくは譲渡を行うとき

加入者は、本CPSに基づく権利または義務の全部または一部を、CAの書面による承諾を得ないで、第三者に譲渡、貸与、質権設定その他担保に供することはできないものとします。

9.16.3　分離条項

本CPSのひとつまた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（弁護士費用および権利放棄）

規定しません。

9.16.5　不可抗力

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します。不可抗力によって損害が発生した場合、本CPS「9.7 無保証」の規定により本CAは免責されます。

- 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、または、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）または革命
- 裁判所、政府または地方機関による作為または不作為
- ストライキ、工場閉鎖、労働争議
- 本CAの責によらない事由で、本CPS に基づく義務の遂行上必要とする必須の機器、物品、供給物もしくはサービス（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

本CAまたはRAが別の組織と合併もしくは別の組織に移管、譲渡する場合、新しい組織は本CPSの方針に同意し責任を持ちつづけるものとします。