my 認証
証明書ポリシー

Version1.4

2024 年 3 月 19 日

my FinTech 株式会社

目次

変更履歴

バージョン	日付	更新者	概要
1.0	2021/11/10	林 昌孝	初版
1.1	2021/10/20	高澤 敦紀	フッターのタイトルを修正。 証明書に記載される情報に関する記載を修正。 連絡窓口の住所に詳細を追記。 アルゴリズムの記載を修正。 鍵用途について修正。 証明書の値・発行可否判断日・再発行要件について修正。 CSR の電子署名の検証に係る記載を修正。 表 3-2 の記載を修正。 利用者 1 人あたりの証明書の発行枚数の変更に伴い、1.4, 4.9.1 の記載を修正。 利用者が鍵ペアの生成を行う暗号モジュールのセキュリティレベルの取捨選択に関する記載を修正。 2.3 の CP/CPS,その他本認証サービスに係る文書の公開頻度について修正。 4.1 の利用者端末アプリの記載を修正。 9.12.2 における本 CP 等の改訂内容の公開に関する記載を修正。 9.12.3 の誤字を修正
1.2	2023/12/13	高澤 敦紀	1.3.5 の登録局（RA）の業務内容の変更 1.5.2 連絡担当者の受付日・受付時間について修正 3.2.3.1 の本人確認方法の記載を変更。

			3.3.1 の有効期間満了に伴う鍵更新時の本人確認方法について記載を変更。 4.1 の証明書の申請プロセス概要について記載を変更 4.2.3 の証明書発行期限の短縮 4.7.1 の証明書再発行申請方法の変更
1.3	2024/2/19	高澤 敦紀	4.3.1 証明書発行業務時の手続きや確認事項について証明書受領確認に係る記載を削除 4.4.1 証明書の受領確認方法について規定を削除
1.4	2024/3/19	高澤 敦紀	1.5.2 my 電子証明書サポートセンターの住所を変更

1. 前書き

1.1 概要

本証明書ポリシー（Certificate Policy：以下、「CP」という）は、my FinTech 株式会社（以下、「my FinTech」という）が運営する、「電子署名及び認証業務に関する法律」（以下、「電子署名法」という）による認証業務を実施する認証局（Certification Authority：以下、「CA」という）について、利用用途、適用範囲、セキュリティ基準、証明書の発行等に係る基準等をポリシーとして規定するものである。また、本 CP に基づき、認証局運用規程（Certification Practice Statement：以下、「CPS」という）が規定される。なお、本 CP と CPS の間に齟齬がある場合には、本 CP が優先される。

my FinTech が運営する CA は、認証機関として鍵管理を行い、証明書の発行等を行うための電子証明書サービス（以下、「本認証サービス」という）を提供する。本 CP は、my FinTech が提供する本認証サービスのうち、「電子署名および認証業務に関する法律（以下、「電子署名法」という）第 2 条第 3 項に規定する特定認証業務（以下、「特定認証業務」という）に関する業務に基づいて発行された証明書に適用する。当該 CA における証明書の発行は、本認証サービス利用者の証明書のみに限定し、利用者への X.509 証明書の発行を可能にする。本認証サービスで発行する証明書は、個人とその公開鍵が一意に関連づけられることを証明する。

なお、本認証サービスは、my FinTech が別途提供する、「電子署名および認証業務に関する法律（以下、「電子署名法」という）の特定認証業務の認定を取得した業務（以下、「認定認証業務」という）に基づく my 電子証明書（以下、「my 電子証明書サービス」という。）とは異なるものであることに留意するものとする。

各種要件を本 CP に明記する上で、本 CA は RFC3647 における Certificate Policy and Certification Practices Framework を採用する。 なお、本 CP は、CA に係るセキュリティ面、技術面、サービス面または認証業務の発展及び改良に伴い、必要に応じて改訂されるものとする。

本規程の作成及び改定に関する業務の責任者は、CA 責任者と規定する。

1.2 ドキュメント体系（名称等）

本 CP の正式名称は「my 認証 証明書ポリシー」とし、次のオブジェクト識別子（OID）が割り当てられ、発行された証明書に記載される。

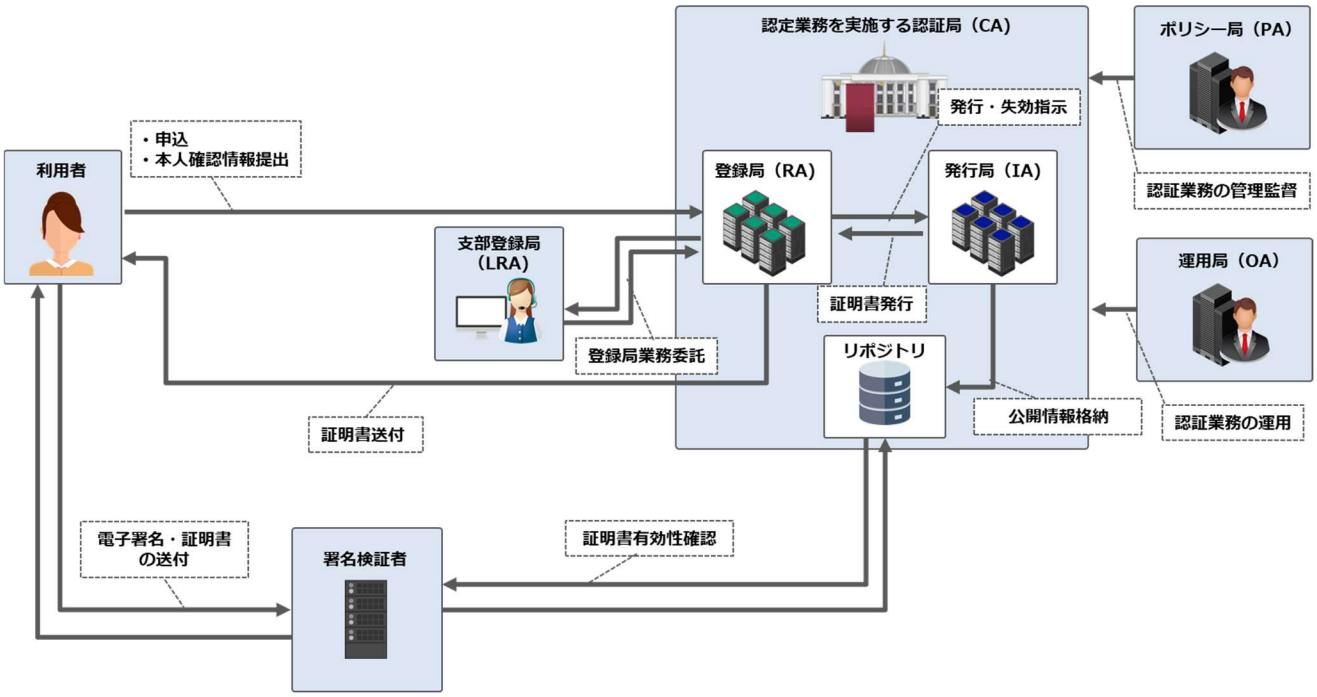
表 1-1 文書名と割り当てられる OID

文書名	OID
my 電子証明書 証明書ポリシー（本 CP）	1.3.6.1.4.1.56986.1.100.1.1
my 電子証明書 認証局運用規程（CPS）	1.3.6.1.4.1.56986.1.100.2.1

1.3 PKI コミュニティの関係者

本 CP は、以下図 1 に示す CA により証明書の発行及び失効業務等が行われる。

図 1　PKI の関係者概要図



1.3.1　ポリシー局（PA）

本 CA は、CA と利用者との信頼関係を確立するため、本 CP 及び CPS 等のポリシーの決定、認証業務の管理監督を適切に実施するためのポリシー局（Policy Authority：以下、「PA」という）を運営している。PA に関わる要員は、my FinTech における社員・役員またはグループ社員でなければならない。

PA は以下の業務、管理、監督を実施する。

- 本 CP に基づいて発行される証明書が CP における要件を充足し続けることの保証
- 本 CP のレビュー、承認、改訂
- 認証局運用規程（CPS）のレビュー、承認、改訂
- 本 CP 及び CPS、本 CP を参照する本認証サービスの利用規約・関連諸規定等のレビュー、承認、改訂
- 本 CP に基づいて発行される証明書における CA の監査レポートのレビュー、承認
- 支部登録局（Local Registration Authority：以下、「LRA」という）において実施される登録業務の一部の監査・監督

1.3.2 運用局（OA）

本 CP では、CA の運用に係る業務、監査に係る業務等を担う運用局（Operation Authority：以下「OA」という）を運営している。OA に関わる要員は、my FinTech における社員・役員またはグループ社員でなければならない。

OA は以下の業務、管理を実施する。

- 本 CP 及び CPS、本 CP を参照する本認証サービスの利用規約・関連諸規定等の作成
- 本 CA システムの保守・管理業務
- 本 CP に基づいて発行される証明書における監査に関する情報の作成
- 本 CA が委託する監査人への監査に関する情報の提供

1.3.3 認証局（CA）

本 CP における CA は、my FinTech が運営し、電子署名法の特定認証業務の認定を取得した業務を行う CA をいう。本 CA は登録局（Registration Authority：以下、「RA」という）及び発行局（Issuing Authority：以下、「IA」という）から構成され、1.3.1 項で定める PA が管理・監督する。

1.3.4 発行局（IA）

IA は my FinTech が運営し、RA の指示に基づき、利用者の証明書の発行または失効を行う。また、CPS に基づき、本 CA の秘密鍵を管理する。IA に関わる要員は、my FinTech における社員・役員またはグループ社員でなければならない。

1.3.5 登録局（RA）

RA は my FinTech が運営し、利用者からの証明書に係る申請において、申請内容及び本人確認に不備がない場合、IA に対し証明書の発行もしくは失効の登録を行う。申請内容及び本人確認情報に不備がある場合は、利用者に対し申請の修正要求を行う。RA に関わる要員は、my FinTech における社員・役員またはグループ社員でなければならない。

本 CA における RA 業務においては、業務の一部を LRA が実施することができる。

当該登録の内容に瑕疵がないことの確認の業務は RA で実施または LRA へ依頼し、RA での登録業務は、RA または LRA での確認結果に基づいて自動処理される。自動処理によって行われた登録業務は、定期的な監査によって、その処理に瑕疵がないことを確認する。

1.3.6 支部登録局（LRA）

LRA は、RA における RA 業務の一部を実施することができる。LRA が実施できる業務は以下のとおりである。

① 利用者の証明書に係る申請の審査業務

② 利用者の本人確認業務

③ 利用者の証明書に係る申請の承認業務

④ 本認証サービスに係る利用者からの問い合わせの対応業務

⑤ 帳簿の保存業務

RA は、LRA に対し、①、②、③、④、⑤の業務を依頼し、LRA は①、②、③、④、⑤の業務のみを実施する。LRA が実施した①、②、③の業務の結果に基づき、RA で登録業務が自動処理によって実施される。

LRA に係る業務の一部は、外部企業が提供するサービスを利用し、実施する場合がある。

LRA に係る業務は、my FinTech が他の企業に業務委託する場合がある。また、LRA に関わる要員は、my FinTech における社員・役員またはグループ社員、業務委託先の要員でなければならない。

1.3.7 利用者

利用者は、本 CP に従い本 CA へ証明書の申請を行う個人をいう。利用者が証明書の申請を行う際には、本 CP、CPS、及び利用規約に同意を行う。

利用者は本 CP に従い、鍵と証明書を利用する。

1.3.8 署名検証者

署名検証者は利用者証明書を信頼し、利用する者をいう。署名検証者は、本 CP、CPS、サービス利用規約及び署名検証者同意書の内容について理解し同意した上で、利用者の証明書を利用しなければならない。

本 CA は署名検証者への証明書の失効情報の提供を行う。署名検証者は、本 CA 及び利用者の証明書の認証パスを利用して、以下の検証を行う。

- 証明書の認証パスを利用し、CA の証明書の署名検証を行う。
- 利用者が秘密鍵を利用し、生成した電子署名の検証を行う。
- CA のリポジトリへ証明書の失効情報の確認を行う。

1.3.9 その他関係者

規定しない。

1.4 証明書の用途

1.4.1 証明書の用途の範囲

本 CP で規定する利用者の証明書は、特定認証業務に基づいて発行される。発行の対象者は個人の利用者に限定される。当該証明書の用途は、電子的な取引等におけるデータの非改ざん性の担保および本人性の確認のために電子署名を行うことである。また、署名検証者においては、当該電子署名の検証にのみ証明書を利用するものとする。なお、証明書の発行枚数は各利用者につきそれぞれ 1 枚に限定する。

本 CA は CA の鍵の更新と同時に、リンク証明書を発行する。リンク証明書は CA の鍵更新に伴い同時に存在することとなる新しい鍵ペアと古い鍵ペアの関係を保証するための証明書であり、古い秘密鍵で新しい公開鍵を電子署名した CA の証明書（NewWithOld）及び新しい秘密鍵で古い公開鍵を電子署名した証明書（OldWithNew）が発行される。

本 CA は失効情報を CRL 及び OCSP を用いて提供を行う。OCSP による提供は検証局（Validation Authority：以下、「VA」という）によって行われる。VA は失効情報の提供機能を持つサーバであり、本 CA は VA に対して証明書を発行する。

本 CA が取り扱う証明書における有効期限は以下のとおりである。

CA の証明書：証明書の発行可否判断日から最大 180 ヶ月（15 年）

利用者の証明書：証明書の発行可否判断日から 1824 日（5 年後の 1 日前まで）

リンク証明書（NewWithOld）： CA の新しい証明書の開始日から CA の古い証明書の終了日まで

リンク証明書（OldWithNew）： CA の古い証明書の開始日から CA の古い証明書の終了日まで

VA の証明書：10 年

なお、本 CA は、CA の証明書の発行可否判断日について、本 CA が証明書を発行した日と定義するとともに、利用者の証明書の発行可否判断日について、LRA で利用者からの発行依頼を承認した日と定義する。

1.4.2 禁止される証明書の用途

本 CP の 1.4.1 項に基づき、利用者による電子署名以外で証明書を利用することを禁止する。

1.5 ポリシー管理

1.5.1 文書を管理する組織

PA は以下の文書を管理する。

- 本 CP
- CPS
- 本 CP を参照する本認証サービスの利用規約
- 本 CP を参照する本認証サービスの関連諸規定
- 本 CP を参照する本認証サービスに係るその他文書

1.5.2 連絡担当者

本 CP に関する質問は以下が対応し、連絡先を下記に示す。

- 窓口：my 電子証明書サポートセンター
- 住所：東京都港区虎ノ門４－１－２８　虎ノ門タワーズオフィス 23F
- 電話：0120-059-745
- FAX：050-3852-3740
- 電子メールアドレス：ca-support@myfintech.co.jp
- 受付日：平日
- 受付時間（電話）　　：11:00－18:00（日本時間）
- 受付時間（メール・FAX）：9:00－18:00（日本時間）
- 受付日及び受付時間の臨時の変更等における情報は https://www.myfintechtrust.jp/上の「お知らせ」にて公開する。

1.5.3 CP の管理者

本 CP は PA が管理者となる。

1.5.4 CP の承認手続き

本 CP における適合性の決定についての承認は、PA 及び my FinTech によって行われる。

1.6 用語の定義

本 CP 10.1 節及び 10.2 節に規定する。

2. 公開とリポジトリ

2.1 リポジトリ

本 CA は、リポジトリを 24 時間 365 日利用できるように維持管理を行う。ただし、利用可能な時間内においても、システム保守等により利用できない場合がある。

2.2 公開情報

本 CA は以下の情報を https://repository.myfintechtrust.jp/public/index.html の URI にて公開する。

- 本 CP
- CPS
- その他 CA のサービスに係る文書

以下の情報を https://vaauth.myfintechtrust.jp/crl/crl_auth.crl の URI にて公開する。

- 本 CA が発行する証明書失効リスト（Certificate Revocation List：以下、「CRL」という）
- 本 CA の CRL Distribution Points

CRL Distribution Points については、CPS11.1.1 に規定する。

以下の情報を https://repository.myfintechtrust.jp/public/ca_certificate.html の URI にて公開する。

- 本 CA の証明書

また、本 CA は失効情報の提供に際し、Online Certificate Status Protocol（以下、「OCSP」という）によるオンラインチェック方法を署名検証者に提供する。

OCSP による、オンラインチェックは、https://vaauth.myfintechtrust.jp/ocsp/の URI で実施できる。

2.3 公開の方法（公開期間や更新タイミング）

本 CA が公開する情報について、公開の頻度は以下のとおりである。ただし、利用可能な時間内においても、システム保守等により利用できない場合がある。

- 本 CP、CPS、その他の本認証サービスに係る文書については、改訂の都度、PA での承認後に公開される
- CRL は本 CP4.9.7 項で規定された周期で更新を行い、公開される。
- 本 CA の証明書、CA の証明書のフィンガープリント、リンク証明書については、証明書の有効期間中において公開される。

2.4 リポジトリの参照方法

利用者はリポジトリの公開情報に関し、随時、リポジトリを参照することができる。リポジトリの公開において、特定のアクセス制御は実施せず、全ての関与者に当該リポジトリ情報へのアクセスを提供する。リポジトリはインターネットを介し、一般的な Web インターフェースを通じて公開する。

3. 識別と認証

3.1 識別名

3.1.1 識別名タイプ

利用者は CA の発行する証明書の中に記載されるサブジェクト識別名（DistinguishedName：以下、「DN」という）により識別される。証明書の形式は、X.509 ver3 の形式に従い設定されるものとする。

3.1.2 識別名の意味付け

本 CA において取り扱う CA の証明書、リンク証明書、利用者の証明書に記載する DN に関する識別名の意味づけに係る情報は以下のとおりである。

表 3-1 CA の証明書、リンク証明書における識別名の意味づけ

領域名	意味
Issuer	国名（countryName）を示す。
	組織名（organizationalName）を示す。CA の証明書の発行者（以下、「RootCA」という）。
	組織名単位名（organizationalUnitName）を示す。CA の証明書を発行した RootCA の名前を示す値。
	名前（commonname） CA の証明書を発行した RootCA のサービスを示す。
Subject	国名（countryName）を示す。
	組織名（organizationalName）を示す。本 CA の運営者。
	組織名単位名（organizationalUnitName）を示す。本 CA の名前を示す値。
	名前（commonname） 本認証サービスを示す。

表 3-2 利用者の証明書における識別名の意味付け

領域名	意味
Issuer	国名（countryName）を示す。発行者の住所の国を示す。
	組織名（organizationalName）を示す。本 CA の運営者。
	組織名単位名（organizationalUnitName）を示す。本認証サービスを示す値。
Subject	ou（organizationalUnit）を示す。本認証サービスが割り当てる利用者の証明書を識別する 12 桁の数字及び当該利用者の証明書の発行回数を示す記号(G+発行回数を示す数字)。 ※利用者の証明書の発行回数は、初回申請時と同じ端末を使用して、改姓、改名、電話番号の変更のない場合の再発行申請に限定されるものとする。

領域名	意味

3.1.3 匿名や仮名の利用

本 CA は、匿名の証明書を発行する。

3.1.4 識別名の解釈規則

本 CA が発行する証明書に記載される名称は、X.509 ver3 の形式に従い設定されると共に、3.1.2 項に規定する要件に従うものとする。なお、本 CA の発行する証明書においては、特定認証業務に基づき発行されるものであり、証明書が利用者のものである本人性及び真正性を担保するために、利用者の名前を証明書に記載する。

3.1.5 識別名の一意性

証明書に記載される subject の DN は本 CA が発行した証明書において一意の値となる。

3.1.6 商標等について

本 CA は利用者の証明書の発行に際し、商標権・著作権・特許権・その他知的財産等については認証しない。

3.2 新規登録時の利用者本人確認

3.2.1 秘密鍵の所有確認方法

本 CA では、利用者自身が生成する方法を用いて、秘密鍵の所有を証明する。

本 CA においては、秘密鍵の生成・保管において一定のセキュリティレベルを担保するため、利用者に対し、証明書の申請、証明書の発行プロセスにおける鍵ペアの生成、CSR の生成、証明書のダウンロード機能等を搭載したアプリケーションソフトウェア（以下、「利用者端末アプリ」という）を提供している。利用者は利用者端末アプリを利用し、自ら秘密鍵の生成を行い、自ら CSR を生成するとともに、電気通信回線を通じて、RA に証明書の発行を依頼するものとする。RA は CSR を受領後、IA に対して CSR を送付するとともに、IA において CSR 自体の電子署名の検証を行い、内容が改ざんされていないこと及び含まれている公開鍵と対になる秘密鍵で電子署名してあることを確認するとともに、指針第 3 条に適合する電子署名の方式（ECDSA prime 256v1）であること及び鍵長（256bit）を確認する。

また、本 CA では、利用者が指針第 3 条に適合する電子署名の方式を利用しているか（当社の指定する ESDSA 方式）の確認及び利用者の証明書に記録する利用者署名検証符号が利用者署名符号に対応するものであるか（方針第 4 の 3 への対応）どうかについて、以下の確認を行う。

- 利用者の電子証明書の発行後、利用者は電子署名を行い、電気通信回線を通じて、当該電子署名を RA に送信する。その後、RA にて当該電子署名の検証処理を行い、利用者本人の電子署名であることの確認を行う方法

3.2.2 利用者の所属組織の確認方法

本 CA では組織に対する証明書を発行しない。

3.2.3 利用者本人の確認方法

本 CA に対して利用の申し込みを行うものが利用者本人であることの真偽の確認は RA が以下 3.2.3.1 目に定める方法によって行う。

3.2.3.1 個人利用者の本人確認

利用者の真偽確認は、RA および LRA により以下の方法により行われる。

- my 電子証明書サービスにて発行された署名用電子証明書の電子署名により当該利用申請者の真偽の確認を行う方法

利用者は、自身の電気通信回線に接続された端末（スマートフォン等）を用いて証明書の申請を行う。申請に際して、CA が利用者に対して提供している利用者端末アプリを利用する。

利用者端末アプリは、本 CA が web 上で公開する URL にアクセスするとダウンロードすることができる。なお、利用者端末アプリは、利用者が扱う端末の種別により異なるものであり、端末の種別に応じた利用者端末アプリの URL を公開している。利用者は自身が扱う端末機種別に応じた URL にアクセスし、ダウンロードを行う。

利用者は、利用者端末アプリを使い、利用者の顔写真を撮影し、端末内に格納された利用者のマイナンバーカードの券面事項記載情報（氏名、住所、生年月日、性別、顔画像のデータ）と共に利用申請情報として扱う。

なお、利用者端末内に利用者のマイナンバーカードの券面事項記載情報が格納されていない場合、利用者端末アプリでマイナンバーカードの IC チップを読取り、マイナンバーカードの券面事項入力補助機能を使い券面事項記載情報を取得する。

また、当該利用者申請情報においては、利用申請の同意に係る情報と利用の申し込みをする電子証明書の用途についての記載事項が含まれるものとする。

利用者は、利用者端末アプリを用いて、my 電子証明書サービスにて発行された署名用電子証明書により、当該利用者情報の電子署名処理を行う。当該電子署名、利用者情報、my 電子証明書にて発行された署名用電子証明書は利用者端末アプリから電気通信回線を経由して RA に送付され、利用者の証明書の申請は完了となる。

RA は、利用者端末アプリから送付された my 電子証明書サービスに係る電子署名の真正性の検証、及び利用者の撮影した顔写真とマイナンバーカードの券面事項記載情報の顔画像データとの一致確認を行う。これらの結果に基づき、RA は申請の諾否を決定し、利用者の本人確認が完了する。

利用申請について否認である場合、RA は利用者端末アプリに当該結果を通知する。また、通知内容には申請の再審査の説明を記載する。

電子署名の真正性に不備がある場合、利用申請情報の再入力を実施し、再審査を申請する。この時の再審査のプロセスは、新規発行時と同様である。

利用者の撮影した顔写真とマイナンバーカードの券面事項記載情報の顔画像データとの一致確認のみ不備がある場合、利用者の撮影した顔写真のみ再撮影を行い、前回送信した利用申請情報と併せて再審査を申請する。再度、顔画像の一致確認のみ不備となった場合、以降の再審査の申請では、顔画像の一致確認を RA にて実施するか、LRA にてオペレータの目視により実施するかを利用者が選択することができる。

なお、証明書の申請に係る情報の不備や記載内容に疑義があった場合、本 CA は証明書の申請を行った者に対し、利用者端末アプリにて不承認通知を通知する。

利用者端末アプリによる利用申し込みについて、申請に係る電子データが破損していた場合は、当該申請を受領しなかったものとして扱い、当該データを破棄した上で再送付の通知を行う。

なお、本 CA が指定した以外の方法による申請は受け付けず、規定していない方法によって送付された申請はすべて破棄し、申請情報の保管は行わないものとする。

3.2.4 確認できない利用者情報

規定しない。

3.2.5 利用者の資格や権利に関する確認期間

規定しない。

3.2.6 相互運用に関する要件

規定しない。

3.3 鍵更新時の利用者本人確認

3.3.1 有効期間満了に伴う鍵更新時の利用者本人の確認

本 CA は利用者の証明書の有効期限が近付いた時期に、その旨を利用者に通知する。利用者はその後、証明書の申請を行うものとする。この場合、利用者の証明書の申請に関する本人確認は証明書の再発行時と同様とし、4.7.1 節の規定に従い行う。

3.3.2 失効後の鍵更新に対する本人確認と認証

一度失効してしまった証明書は、使用することができなくなる。失効後に再度、証明書を利用する場合は、証明書の申請を行うものとする。この場合、利用者の証明書の申請に関する本人確認は、証明書の新規発行時と同様とし、3.2 節の規定に従い行う。

3.4 失効申請時の利用者本人の確認

3.4.1 失効申請者本人の確認方法

証明書の失効については、失効申請時に利用者の本人確認を行う。また、my 電子証明書サービスにて発行された署名用電子証明書の失効申請時に行われる本人確認をもって、本認証サービスにおける本人確認が完了したものとみなす。

本認証サービスの証明書の失効については、my 電子証明書サービスにて発行された署名用電子証明書の失効申請に基づき実施される。当社は、my 電子証明書サービスにて発行された署名用電子証明書の失効申請に際し、my 電子証明書サービスの重要事項の説明にて当該記載を明記しており、本重要事項に対し利用者が同意したことをもって、利用者が本認証サービスの失効についても同様に同意したものと見なし、my 電子証明書サービスにて発行された署名用電子証明書の失効申請の受理と同時に本認証サービスの失効手続きを進めるものとする

4. 証明書のライフサイクル運用要件

4.1 証明書の申請

証明書の利用を希望する者は、本 CA が利用を希望する者に提供する利用者端末アプリを利用して証明書の申請を行う。

以下に、証明書の申請プロセスの概要を示す。

1. 利用者端末アプリを利用して、証明書の申請を開始する。
2. 利用者は、利用者端末アプリを用いて自身の顔を撮影する。
3. 利用者端末アプリに利用者のマイナンバーカードの券面事項記載情報が格納されていない場合に限り、利用者端末アプリでマイナンバーカードの IC チップを読取り、マイナンバーカードの券面事項入力補助機能を使い券面事項記載情報を取得する。
4. 利用者は、my 電子証明書サービスのパスワードを入力し、署名用電子証明書に基づく秘密鍵を用いて利用申請情報に係る電子署名を作成する。
5. 利用者は利用申請情報及び、電子署名を RA へ送付する。
6. RA にて送付された署名用電子証明書の電子署名の検証と利用者の顔容貌の一致確認が完了するまで、本人確認結果を待つ状態となる。

上記の利用者端末アプリによる証明書の申請方法以外の申込は受付けない。

なお、利用者端末アプリにおける利用者情報申請フォームに表示される申請情報と実際に送信される送信データの対応については、以下のようになる。

表 4-1 利用者情報申請フォームの画面表示と申請情報の送信データの対応

申請フォームの項目	申請フォームの項目に含まれる内容	送信データの項目	送信データ項目に含まれる値	値のデータ型	電子署名対象 (対象：○、対象外：―)
氏名	氏名 （例：認証 太郎）	name	申請フォームの項目内容と同じ	String	○
住所	住所 （例：北海道江別市２条５丁目９－２）	address	申請フォームの項目内容と同じ	String	○
生年月日	誕生日 （例 1990 年 1 月 1 日）	birthday	申請フォームの項目内容と同じ（yyyyMMdd 形式）	String	○
性別	性別 （例：男性、女性）	gender	“MALE” または”FEMALE”	String	○
マイナンバーカードの顔画像	マイナンバーカードの券面事項に記載された利用者の顔画像	card_picture	マイナンバーカードから読み取った顔写真 を URL-Safe	String	○

申請フォームの項目	申請フォームの項目に含まれる内容	送信データの項目	送信データ項目に含まれる値	値のデータ型	電子署名対象 (対象：○、対象外：―)
			Base64 エンコードした文字列		
顔写真	利用者が撮影した顔写真	face_picture	アプリで撮影した顔写真イメージ(PNG)を URL-Safe Base64 エンコードした文字列	String	○
スマホの種類	申請端末の種類 （例：Android、iOS）	terminal_type	“ANDROID”または”IOS”	String	―
重要事項及び利用者規約の同意	証明書発行に関する重要事項及び利用規約に同意し発行申請を行います	user_consent	“証明書発行に関する重要事項及び利用規約に同意し発行申請を行います”	String	―
my 認証の用途	利用者認証での利用	Certificate_usage	“Digital Signature&Non Repudiation& Key Encipherment& Data Encipherment”	String	○

なお、利用者端末アプリに表示される「電子署名の実施方法及び認証業務の利用に関する重要な事項」は、以下の内容を含むものとする。

- 認定認証業務においては、虚偽の証明書の申請をして、利用者について不実の証明をさせた者は、 法第四十一条の規定により罰せられること。
- 利用者の秘密鍵が危殆化（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、又は危殆化したおそれがある場合、電子証明書に記録されている事項に変更が生じた場合又は電子証明書の利用を中止する場合においては、遅滞なく電子証明書の失効の請求を行わなければならないこと。
- 特定認証業務に係る電子証明書を使用する場合における電子署名のためのアルゴリズムは、認証事業者が指定したものを使用する必要があること。

4.1.1 利用申請者

証明書の申請は、利用者本人が行わなければならない。本 CA は代理人による証明書の申請は受け付けない。

4.1.2 利用申請者の役割と責任

利用者は、本 CP、CPS、その他の本認証サービスに係る契約文書に同意の上、証明書の申請を行う。申請に際し、利用者には真正かつ正確な情報を本 CA へ提供する責任がある。

なお、利用者が証明書の発行を申請した時点で、my FinTech と利用者間の利用契約が発効するものとする。

4.2 証明書申請審査（登録業務）

4.2.1 利用者本人の確認業務

本 CA では証明書を発行する前に利用者の本人確認を行う。本人確認方法は、3.2.3.1 目の方法に従う。

4.2.2 証明書申請の諾否

RA 及び LRA は、証明書の申請を承認または却下できる。

RA 及び LRA は、証明書の申請に対する審査において疑義が認められた場合は、記載されている内容に不備が発見された内容の訂正または再提出を求める。訂正または再提出を求める通知手段は、利用者端末アプリによる方法がある。

本 CA は証明書の申請に対する審査の結果、証明書の発行ができないと判断したときは、不受理の理由及びその旨を利用者端末アプリによって通知する。

なお、利用者が申請内容の訂正または再提出を行う場合、4.1 節の申請手順と同様に、利用者端末アプリで申請内容を訂正または再提出を行う必要がある。

4.2.3 証明書申請審査にかかる時間

証明書の申請が承認された場合、本人確認後 24 時間以内に証明書が発行されなければならない。

4.3 証明書発行業務

4.3.1 証明書発行業務時の手続きや確認事項

RA は 3.2.3.1 目に基づき、証明書の申請における本人確認が完了した後、IA に対し、利用者の証明書の発行を登録する。IA は証明書を発行し、RA へ証明書を送付する。RA は 4.3.2 項に規定する通知及び証明書の送付、を利用者端末アプリに対し行う。

4.3.2 証明書発行に関する利用者への通知

本 CA は証明書の発行後速やかに、証明書が発行された旨と利用者が証明書を受領するために必要な手続きについて、利用者に通知する。通知手段は、利用者端末アプリによる通知方法がある。

4.4 証明書の受領確認

4.4.1 証明書の受領確認方法

規定しない。

4.4.2 IA による CA の証明書の公開

本 CA は利用者の証明書を公開しない。ただし、本 CA の証明書及びリンク証明書についてはリポジトリ上で公開する。

4.4.3 IA から RA などへの証明書発行通知

IA にて証明書の発行が完了した後、証明書は RA を経由して利用者端末アプリに送付される。IA から RA に証明書が送付される処理は認証業務用設備のアプリケーションソフトウェアにより自動的に行われるものであり、特定の通知は行わない。

4.5 利用者及び署名検証者における鍵ペアと証明書の用途

4.5.1 利用者における秘密鍵と証明書の用途

利用者は、1.4.1項に定める用途に限り秘密鍵及び証明書を利用するものとし、その他の用途での利用は認められない。また、利用者の秘密鍵は、利用者のみが利用できるものとし、利用者は第三者に対してその利用を許諾してはならない。なお、秘密鍵と証明書の利用に関するその他の利用者の義務は、9.6.3項に定める。

4.5.2 署名検証者における公開鍵と証明書の用途

署名検証者は、利用者が本 CP の 1.4.1 項に定める用途で利用する証明書について、自らの責任で証明書の有効性について確認する。 なお、署名検証者に対しての利用者の公開鍵と証明書の利用に関するその他の義務は、9.6.4 項に定める。

4.6 鍵の更新を伴わない証明書の更新

4.6.1 証明書更新の要件

本CAは、鍵の更新を伴わない証明書の更新を受け付けない。

4.6.2 証明書更新申請者

規定しない。

4.6.3 証明書更新業務

規定しない。

4.6.4 証明書更新に関する利用者への通知

規定しない。

4.6.5 更新された証明書の受領確認方法

規定しない。

4.6.6 IA による更新された CA 証明書の公開

規定しない。

4.6.7 IA から RA などへの証明書更新通知

規定しない。

4.7 鍵の更新を伴う証明書の再発行

4.7.1 証明書再発行の要件

本 CA は、利用者の証明書の有効期限が近付いた時期、または利用者の秘密鍵が利用できなくなった場合、鍵の更新を伴う証明書の再発行を受け付ける。

再発行申請時の利用者の真偽確認は、RA および LRA により以下の方法により行われる。

- my 電子証明書サービスにて発行された署名用電子証明書の電子署名により当該利用申請者の真偽の確認を行う方法

利用者は、自身の電気通信回線に接続された端末（スマートフォン等）を用いて証明書の申請を行う。申請に際して、CA が利用者に対して提供している利用者端末アプリを利用する。

利用者は、利用者端末アプリを使い、利用者の顔写真を撮影し、端末内に格納された利用者のマイナンバーカードの券面事項記載情報（氏名、住所、生年月日、性別、顔画像のデータ）と共に利用申請情報として扱う。

なお、利用者端末内に利用者のマイナンバーカードの券面事項記載情報が格納されていない場合、利用者端末アプリでマイナンバーカードの IC チップを読取り、マイナンバーカードの券面事項入力補助機能を使い券面事項記載情報を取得する。

また、当該利用者申請情報においては、利用申請の同意に係る情報と利用の申し込みをする電子証明書の用途についての記載事項が含まれるものとする。

利用者は、利用者端末アプリを用いて、my 電子証明書サービスにて発行された署名用電子証明書により、当該利用者情報の電子署名処理を行う。当該電子署名、利用者情報、my 電子証明書にて発行された署名用電子証明書は利用者端末アプリから電気通信回線を経由して RA に送付され、利用者の証明書の申請は完了となる。

RA は、利用者端末アプリから送付された my 電子証明書サービスに係る電子署名の真正性の検証、及び利用者の撮影した顔写真とマイナンバーカードの券面事項記載情報の顔画像データとの一致確認を行う。これらの結果を LRA にて確認を実施し、利用者の本人確認が完了する。

証明書の申請について否認である場合、利用者端末アプリに当該結果を通知する。また、通知内容には申請の再審査の説明を記載する。

電子署名の真正性に不備がある場合の再審査は、新規発行時の本人確認業務と同様のプロセスで行う。

利用者の撮影した顔写真とマイナンバーカードの券面事項記載情報の顔画像データの一致確認のみ不備がある場合の再審査は、券面事項記載情報の顔画像データとの一致確認のみ不備がある場合、利用者の撮影した顔写真のみ再撮影を行い、前回送信した利用申請情報と併せて再審査を申請する。再申請では署名用電子証明書の電子署名の検証及び、顔画像の一致確認を RA にて実施し、その結果を LRA にてオペレータの目視により確認する。

なお、証明書の申請に係る情報の不備や記載内容に疑義があった場合、本 CA は証明書の申請を行った者に対し、利用者端末アプリにて不承認通知を通知する。

利用者端末アプリによる利用申し込みについて、再発行の申請に係る電子データが破損していた場合は、当該申請を受領しなかったものとして扱い、当該データを破棄した上で再送付の通知を行う。

なお、本 CA が指定した以外の方法による再発行の申請は受け付けず、規定していない方法によって送付された申請はすべて破棄し、申請情報の保管は行わないものとする。

4.7.2 証明書再発行申請者

本CPの4.1.1項に準じる。

4.7.3 証明書再発行業務

証明書の再発行に関しては、新たな証明書の登録業務、証明書の発行業務を実施した上で、古い証明書の失効業務を行う。

証明書の再発行業務の内、登録業務は本CPの4.2節に準じる。

証明書の再発行業務の内、発行業務は本CPの4.3節に準じる。

証明書の再発行業務の内、失効業務は本CPの4.9節に準じる。

4.7.4 証明書再発行に関する利用者への通知

本CPの4.3.2項に準じる。

4.7.5 再発行された証明書の受領確認方法

本 CP の 4.4.1 項に準じる。

4.7.6 IA による再発行証明書の公開

本 CP の 4.4.2 項に準じる。

4.7.7 IA から RA などへの証明書再発行通知

本 CP の 4.4.3 項に準じる。

4.8 証明書記載情報の変更による証明書変更

4.8.1 証明書変更の要件

本 CA は既に発行された証明書の変更の申請を受け付けないものとする。

利用者は証明書情報に変更が生じる場合、本 CA に対し、遅延なく当該証明書について失効を申請しなければならない。

4.8.2 証明書変更申請者

規定しない。

4.8.3 証明書変更業務

規定しない。

4.8.4 証明書変更に関する利用者への通知

規定しない。

4.8.5 変更された証明書の受領確認方法

規定しない。

4.8.6 IA による変更された証明書の公開

規定しない。

4.8.7 IA から RA などへの証明書変更再発行通知

規定しない。

4.9 証明書の失効と一時停止

4.9.1 証明書失効の要件

本 CA において、利用者は自らの判断に基づいて証明書の失効申請を行うことができる。当社は、my 電子証明書サービスにて発行された署名用電子証明書の失効申請をもって本認証サービスの失効申請に同意したものと見なし、署名用電子証明書の失効申請の受理と同時に本認証サービスの失効手続きを進めるものとする。

ただし次の事由が生じた場合、利用者は CA に対し、速やかに報告すると共に、失効申請を行わなければならない。

・利用者の秘密鍵が危殆化（盗難・漏洩・PIN コード紛失等により他人に使用され得る状態）された、またはその恐れがある場合。

・利用者自身の申し出により、証明書の利用を止める場合。

・証明書を誤って消去し、使用できなくなった場合。

また、次の事由が生じた場合、利用者は本 CA に対し、再発行申請を実施し、本 CA は、証明書の登録業務及び発行業務を実施した上で、古い証明書の失効を行う。

・証明書や秘密鍵が格納された端末等を変更した場合

・証明書の記載情報に変更があった場合。

・証明書の有効期限が近付いた時期に、鍵の更新を伴う証明書の再発行を利用者が申請した場合

さらに、CA が、利用者の証明書に対し次の事由に該当すると判断した場合、証明書の失効を実施する。

・証明書の記載情報に変更があった事実を確認した場合。

・CA 及び利用者の秘密鍵が危殆化（盗難・漏洩・PIN コード紛失等により他人に使用され得る状態）された、またはその恐れがある場合。

・証明書の受領期限を経過しても、利用者から受領報告が得られない場合。

・証明書のダウンロード失敗により、利用者が証明書を正しく受領できない場合。

・利用者が本 CP、CPS、その他契約、利用規約、法律に基づく義務を履行していない場合。

・利用者が暴力団等の反社会的勢力であることが判明した場合。

・利用者が暴力、脅迫、その他犯罪を手段とする要求や法的な責任を超えた不当な要求を行った場合。

・利用者の証明書記載情報に誤りがあった場合。

・利用者が証明書記載情報及び申請情報に虚偽の情報を申告した場合。

・利用者の死亡等の理由により、利用者自身から失効申請が困難な場合。

・my FinTech が本認証サービスを終了する場合。

・利用者の所有する電子証明書のそれぞれにおいて、複数所持が確認された場合。

・その他、my FinTech が失効を必要と判断した場合。

本 CA において、上記の状況のいずれかが発生した際、関連する証明書は失効され、その失効情報が証明書失効リストに登録される。また、証明書の複数所持が確認された場合、当該証明書の保有者が保有していた証明書はすべて失効される。失効した証明書の失効情報は、CRL 及び OCSP にて公開されるものとする。

4.9.2 証明書失効申請者

証明書の失効申請は、証明書の利用者本人、または利用者の代理人から受け付け可能とする。

4.9.3 失効申請手続

利用者が自らの判断に基づいて証明書の失効申請を行う場合、利用者は利用者端末アプリから保有する証明書に関連付けられた秘密鍵を使用し、失効申請情報に電子署名を行い、電気通信回線を通じて失効申請及び電子署名に係る情報の送信を RA に行うものとする。RA において、署名の検証が完了することで、失効申請を受領したものとみなし、IA にて証明書の失効処理が実行される。

なお、4.7節における鍵の更新を伴う証明書の再発行業務は、証明書の失効申請業務を含むものとなるが、その場合は、新たな証明書の登録業務、証明書の発行業務を実施した上で、新たな証明書に関連付けられた秘密鍵を使用し、失効申請情報に電子署名を行い、電気通信回線を通じて失効申請及び電子署名に係る情報の送信をRAに行うものとする。RAにおいて、署名の検証が完了することで、失効申請を受領したものとみなし、IAにて古い証明書の失効処理が実行される。

4.9.4 失効申請の猶予期間

失効申請の猶予期間とは、失効理由の特定後に利用者が失効申請を提出できる期間をいう。

本 CA の場合、本 CP では失効の猶予期間は規定しない。利用者は 4.9.1 項に該当する事由が生じた時は、速やかに失効申請を行うものとする。

4.9.5 失効処理に要する時間

利用者端末アプリによる失効申請の審査については、当社が指定した日を除き、平日・土日祝行うものとする。また、本CAは、利用者による失効申請または失効依頼について、利用者からの提出から1営業日以内に受領し、受領後は遅延なく証明書の失効を処理する。失効申請または失効依頼の受領、及び証明書の失効処理については、CP1.5.2に記載された受付日及び受付時間において実施するものとする

4.9.6 署名検証者による失効情報確認

本 CA は利用者の証明書の失効情報、CA の証明書、リンク証明書、有効性確認情報をリポジトリ上で CRL として公開、または OCSP により署名検証者に提供する。

署名検証者は、本 CA が発行する CRL または OCSP により証明書の失効を確認しなければならない。

OCSP は証明書の現在のステータス（失効されていない証明書であること、失効された証明書であること、該当する証明書がないことに対する応答）を応答するサーバとなる。

なお、有効期間が終了した電子証明書の失効情報は CRL 及び OCSP により公開され、署名検証者の参照可能時間に制限は設けていない（24 時間参照可能）。

4.9.7 証明書失効リスト（CRL）発行頻度（CRL 発行時）

本 CA は CRL を 24 時間以内の周期で発行する。

4.9.8 証明書失効リスト（CRL）発行の最大遅延時間（CRL 発行時）

CRL の有効期間は 48 時間以下である。更新された失効情報を含む CRL は、証明書の失効から 24 時間以内にリポジトリに公開する。なお、有効期間を経過した CRL に関する問い合わせは受け付けない。

4.9.9 オンライン証明書有効性確認サービスの提供について

本CAは、CRLに加えOCSPにより失効情報を提供する。本CAは、48時間以下の有効期間を有するCRLを24時間以内の周期で更新する。本CAのOCSPレスポンスはRFC6960に準拠している。OCSPレスポンスは、VAサーバ内にあるOCSPレスポンダにおいて、VAサーバのHSM内で生成されたOCSP署名用鍵によって署名される。OCSPレスポンダについては、OCSP署名用鍵から作成したCSRをもとにCAが発行した証明書（VA証明書）が格納されている。VA証明書については、OCSPレスポンスに際し、VAサーバ内にあるOCSPレスポンダがOCSPに付する署名に係る証明書となる。

4.9.10 オンライン証明書有効性確認サービス利用の要件

本 CA は利用者の証明書の失効情報、CA の証明書及び有効性確認情報を CRL 及び OCSP により署名検証者に提供する。署名検証者の参照可能時間に制限は設けておらず、24 時間参照可能となる。

本 CA は、OCSP において GET メソッドをサポートする。本 CA の OCSP は、証明書のステータスをリアルタイムで検証するために使用されるプロトコルを指す。OCSP レスポンダは、証明書のステータス要求に応答するために使用され、下記 3 つの応答のいずれかを行うことができる。

・ good（証明書が失効されていないことを示す応答）

・ revoked（失効された証明書であることを示す応答）

・ unknown（該当する証明書がないことに対する応答）

本 CA から VA に利用者証明書データがリアルタイムで同期されており、OCSP は VA に保存された証明書情報を基に認証書ステータスを応答する。なお、発行されていない証明書に対しては、Unknownの値を応答するが、これは証明書の有効性に係る情報ではないことに留意する必要がある。

なお、本 VA は CA から常に最新の失効情報の取得を行い、応答において最新の失効情報を署名検証者に提供する。

4.9.11 その他の証明書有効性確認方法

規定しない。

4.9.12 鍵の危殆時の特別要件

本 CA は、利用者の秘密鍵の危殆化もしくは危殆化の可能性を知り得た場合、3.4.1 項及び 4.9.3 項に基づき失効処理を行う。

4.9.13 証明書一時停止の要件

規定しない。

4.9.14 証明書一時停止申請者

規定しない。

4.9.15 証明書の一時停止申請手続

規定しない。

4.9.16 一時停止可能期間

規定しない。

4.10 オンライン証明書有効性確認サービス

4.10.1 オンライン証明書有効性確認サービスの運用方法

本 CA は利用者の証明書の失効情報、CA の証明書及び有効性確認情報を CRL または OCSP により署名検証者に提供する。

本 CA は CRL 及び OCSP 以外で証明書のステータスを確認できるサービスは提供しない。

CRL または OCSP レスポンスの失効情報は、失効した証明書の有効期限まで削除しないものとする。

4.10.2 オンライン証明書有効性確認サービスの利用

本 CA は、OCSP におけるオンラインでの証明書有効性確認サービスを 24 時間体制で維持するものとする。

4.10.3 追加サービスの提供について

規定しない。

4.11 証明書の利用契約の終了について

本 CA が発行した利用者の証明書は、証明書の失効、有効期限切れ、本認証サービスまたは my 電子証明書のサービスが終了したときに利用契約が終了する。

利用者との証明書の利用契約が終了する事由は、利用規約に定める。

また、利用者は証明書が有効期間中であるにもかかわらず失効を希望する場合、4.9.3 項に基づき、本 CA へ証明書の失効申請を行い、利用契約を終了しなければならない。

4.12 キーエスクロー（鍵供託）と鍵復元

4.12.1 キーエスクローと鍵復元に関する方針と実施手順

規定しない。

4.12.2 セッション鍵のカプセル化と鍵復元に関する方針と実施手順

規定しない。

5. 設備･要員･運用等の管理

5.1 物理的管理

5.1.1 設置場所と建築構造

CPS の 5.1.1 項に規定する。

5.1.2 物理的アクセス

CPS の 5.1.2 項に規定する。

5.1.3 電源と空調

CPS の 5.1.3 項に規定する。

5.1.4 水害防止対策

CPS の 5.1.4 項に規定する。

5.1.5 防火対策

CPS の 5.1.5 項に規定する。

5.1.6 媒体等の災害対策

CPS の 5.1.6 項に規定する。

5.1.7 廃棄処理

CPS の 5.1.7 項に規定する。

5.1.8 オフサイトバックアップ

CPS の 5.1.8 項に規定する。

5.2 手続的管理

5.2.1 各要員の役割

CPS の 5.2.1 項に規定する。

5.2.2 各要員の必要人員

CPS の 5.2.2 項に規定する。

5.2.3 各要員の本人確認と認証

CPS の 5.2.3 項に規定する。

5.2.4 要員の権限分割

CPS の 5.2.4 項に規定する。

5.3 要員管理

5.3.1 要員の資格・経歴・身分証明

CPS の 5.3.1 項に規定する。

5.3.2 経歴の確認方法

CPS の 5.3.2 項に規定する。

5.3.3 教育訓練

CPS の 5.3.3 項に規定する。

5.3.4 再教育訓練の実施頻度と要件

CPS の 5.3.4 項に規定する。

5.3.5 要員ローテーションの頻度と方法

CPS の 5.3.5 項に規定する。

5.3.6 要員の罰則規定

CPS の 5.3.6 項に規定する。

5.3.7 委託契約の要件

CPS の 5.3.7 項に規定する。

5.3.8 要員への配布資料

CPS の 5.3.8 項に規定する。

5.4 監査ログ

5.4.1 記録するイベント

CPS の 5.4.1 項に規定する。

5.4.2 監査ログの確認頻度

CPS の 5.4.2 項に規定する。

5.4.3 監査ログ保存期間

CPS の 5.4.3 項に規定する。

5.4.4 監査ログの保存方法

CPS の 5.4.4 項に規定する。

5.4.5 監査ログのバックアップ手続

CPS の 5.4.5 項に規定する。

5.4.6 監査ログシステムの設置場所（内部と外部）

CPS の 5.4.6 項に規定する。

5.4.7 イベント実施者への通知

CPS の 5.4.7 項に規定する。

5.4.8 脆弱性評価

CPS の 5.4.8 項に規定する。

5.5 帳簿書類

5.5.1 保存する帳簿書類

CPS の 5.5.1 項に規定する。

5.5.2 帳簿書類の保存期間

CPS の 5.5.2 項に規定する。

5.5.3 帳簿書類の保存方法

CPS の 5.5.3 項に規定する。

5.5.4 帳簿書類のバックアップ

CPS の 5.5.4 項に規定する。

5.5.5 帳簿書類に対するタイムスタンプ

CPS の 5.5.5 項に規定する。

5.5.6 帳簿書類システムの設置場所（内部又は外部）

CPS の 5.5.6 項に規定する。

5.5.7 帳簿書類の確認方法

CPS の 5.5.7 項に規定する。

5.6 CA の鍵更新

CPS の 5.6 節に規定する。

5.7 危殆化や災害時の対応

5.7.1 危殆化時の対応手順

CPS の 5.7.1 項に規定する。

5.7.2 コンピュータリソース・ソフトウェア・データ等の重大障害時の対応手順

CPS の 5.7.2 項に規定する。

5.7.3 利用者の秘密鍵の危殆化時の対応手順

利用者は自己の責任により管理する秘密鍵の危殆化もしくは危殆化が疑われる事態が生じた場 合、本 CP 4.9 節に規定された手続きに基づき、証明書の失効手続きを行わなければならない。

5.7.4 災害時の認証業務の継続について

CPS の 5.7.4 項に規定する。

5.8 認証業務の廃止について

CPS の 5.8 節に規定する。

6. 技術的なセキュリティ管理

6.1 鍵ペアの生成及びインストール

6.1.1 利用者の鍵ペアの生成方法

本 CA において、利用者の利用する秘密鍵は、利用者自らが生成する。

本 CA においては、秘密鍵の生成・保管において一定のセキュリティレベルを担保するため、利用者に対し、証明書の発行プロセスにおける鍵ペアの生成、CSR の生成、証明書のダウンロード機能等を搭載した利用者端末アプリを提供している。

利用者は、利用者端末アプリの利用に限り、利用者自身が秘密鍵を生成することが許可される。また、利用者が利用者端末アプリを利用し、秘密鍵の生成を行う際は、利用者端末アプリに対応した以下の表の暗号モジュール、本 CA が指定するセキュリティ機能を備えた端末（スマートフォン等）のいずれかを利用することを義務としている。

表 6-1 利用者が鍵ペアの生成を行う暗号モジュール等

セキュリティレベル	暗号モジュール等
高	FIPS140-2 レベル 3 以上の暗号モジュール
中	FIPS140-2 レベル 2 以上の暗号モジュール
基本	本 CA が指定するセキュリティ機能を備えた端末（スマートフォン等）

セキュリティレベル高における FIPS140-2 レベル 3 以上の暗号モジュールは、利用者の希望に応じ、本 CA から利用者に提供する場合がある。

セキュリティレベル基本における、本 CA が指定するセキュリティ機能を備えた端末（スマートフォン等）については、指定機種情報をリポジトリ上で利用者に公開する。

当該セキュリティレベルは利用者へのセキュリティの説明としての定義を目的としており、法的拘束力はないものとする。

6.1.2 利用者の秘密鍵の安全な配付方法

本 CA では、利用者の秘密鍵を配送しない。利用者の秘密鍵は利用者自らが生成する。

6.1.3 利用者の公開鍵の CA への配付方法

利用者は、CSR データ中に公開鍵を含めた上で、CSR を RA に送付する。なお、CSR の生成は、本 CP 3.2.1 項における利用者端末アプリでのみ生成が可能である。

6.1.4 CA の公開鍵の検証者への配付方法

本 CA は公開鍵をリポジトリ上で公開する。

6.1.5 鍵サイズ

利用者の証明書に係る鍵の署名方式及び最低限の鍵サイズは、ECDSA 暗号方式 256bit 以上のものとする。

6.1.6 公開鍵暗号方式のパラメータ等の鍵ペアの信頼性確保

規定しない。

6.1.7 鍵の用途の目的（証明書記載の鍵用途）

本 CA が発行する利用者証明書の鍵用途は、電子署名、否認防止、鍵暗号またはデータ暗号のみである。

6.2 秘密鍵の信頼性と暗号モジュール

6.2.1 暗号モジュールの技術要件

本 CA の鍵ペアを管理するための暗号モジュールは FIPS140-2 レベル 3 の規格を満たした HSM とする。HSM は IA が管理する。

6.2.2 秘密鍵の複数人制御

CPS の 6.2.2 項に規定する。

6.2.3 秘密鍵のキーエスクロー（鍵供託）

CPS 6.2.3 項に規定する。

6.2.4 秘密鍵のバックアップ

CPS の 6.2.4 項に規定する。

6.2.5 秘密鍵の保管

CPS の 6.2.5 項に規定する。

6.2.6 暗号モジュールにおける秘密鍵の入出力

CPS の 6.2.6 項に規定する。

6.2.7 暗号モジュールにおける秘密鍵の格納

CPS 6.2.7 項に規定する。

6.2.8 秘密鍵の活性化

CPS の 6.2.8 項に規定する。

6.2.9 秘密鍵の非活性化

CPS の 6.2.9 項に規定する。

6.2.10 秘密鍵の廃棄

CPS の 6.2.10 項に規定する。

6.2.11 暗号モジュールの評価

本 CA は、本 CP の 6.2.1 項に定める要件を満たした HSM を使用する。

6.3 その他鍵ペアに関する管理

6.3.1 公開鍵の保存

公開鍵の保存は、それが含まれる証明書を保存することで行う。

6.3.2 証明書の実運用期間と鍵ペアの使用期間

本 CA の証明書及び秘密鍵の有効期間は、証明書の発行可否判断日から最大 180 ヶ月（15 年）に制限するものとする。当該可否判断日については、CA の証明書の発行日と定義する。

OCSP サーバの証明書及び秘密鍵は、最大 10 年間の有効期間を有する。

利用者の証明書及び秘密鍵の使用期間は、証明書の発行可否判断日から 1824 日（5 年後の 1 日前まで）の期間を有する。当該可否判断日については、利用者からの発行依頼に対し、LRA が当該依頼を承認した日と定義する。証明書の有効開始日時は、開始日時の秒数は証明書を発行した秒と設定し、有効終了日時は、終了日時の秒数は開始日時の秒数から 1824 日後と設定する。

6.4 活性化データ

6.4.1 活性化データの生成と設定

CPS の 6.4.1 項に規定する。

6.4.2 活性化データの保護

CPS の 6.4.2 項に規定する。

6.4.3 その他活性化データに関する考慮点

規定しない。

6.5 認証設備のセキュリティ管理

6.5.1 認証設備に関する特別なセキュリティ要件

CPS の 6.5.1 項に規定する。

6.5.2 認証設備のセキュリティ評価

CPS の 6.5.2 項に規定する。

6.6 システムのライフサイクル管理

6.6.1 システム開発管理

CPS の 6.6.1 項に規定する。

6.6.2 セキュリティ運用管理

CPS の 6.6.2 項に規定する。

6.6.3 ライフサイクルのセキュリティ管理

CPS の 6.6.3 項に規定する。

6.7 ネットワークセキュリティ管理

CPS の 6.7 節に規定する。

6.8 タイムスタンプ

CPS の 6.8 節に規定する。

7. 証明書、CRL と OCSP のプロファイル

7.1 証明書のプロファイル

7.1.1 証明書のバージョン番号

本 CA は、X.509 ver3 の証明書形式バージョン基づき発行するものとする。

7.1.2 証明書の拡張

本 CA は、標準の証明書拡張を使用する場合は、RFC5280 に準拠するものとする。

7.1.3 アルゴリズムオブジェクト識別子

本 CA が発行する証明書は、以下表 7-1 のオブジェクト識別子のいずれかを用いて署名アルゴリズムを識別するものとする。

表 7-1 署名アルゴリズム識別子

アルゴリズム識別子	オブジェクト識別子
ECDSA(SHA256)	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}

本 CA が発行する証明書において ECDSA 暗号アルゴリズムを用いる場合、以下の曲線を指定するものとする。

表 7-2 楕円曲線におけるパラメータ

アルゴリズム識別子	オブジェクト識別子
prime256v1	{iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) prime256v1(7)}

本 CA が発行する証明書におけるサブジェクトの公開鍵の暗号アルゴリズムは以下を用いるものとする。

表 7-3 サブジェクトの公開鍵の暗号アルゴリズム

アルゴリズム識別子	オブジェクト識別子
id-ecPublicKey	{iso(1)member-body(2)us(840)ansi-X962(10045)id-publicKeyType(2)1}

7.1.4 識別名の形式

本 CA で使用する識別名は、ITU X.500 シリーズ定義の識別名の形式に従う。識別名は、RFC5280 で特定されているものなど、標準的な属性タイプで構成されるものとする。

7.1.5 識別名の制約

本 CA は、必要に応じて Name Constraints フィールドに名前制約を含めることができる。

7.1.6 CP オブジェクト識別子

CA が発行した全ての証明書は、拡張領域に OID 形式で CP が記載され、OID は 1.2 節に準拠するものとする。

7.1.7 証明書ポリシー制約拡張の使用

規定しない。

7.1.8 証明書ポリシー修飾子の構文及び意味

本CAが発行した証明書には、RFC5280で規定されているポリシー修飾子を含めることができる。

7.1.9 クリティカルな証明書ポリシー拡張

規定しない。

7.2 CRL プロファイル

7.2.1 バージョン番号

CA は、X.509 バージョン 2 の証明書失効リストを発行するものとする。

7.2.2 CRL と CRL entry 拡張

本 CA は、証明書における拡張領域について、CPS の 11.2 節に記載するものとする。

7.3 OCSP プロファイル

7.3.1 バージョン番号

本 CP の下で運用される OCSP は、証明書失効リスト署名用に指定されたアルゴリズムを用いてレスポンスに署名するものとする。なお、OCSP バージョン 1 を使用するものとする。

7.3.2 OCSP 拡張

本 CA は、証明書における拡張領域について、CPS の 11.2 節に記載するものとする。

8. 準拠性監査とその他監査基準

8.1 監査の頻度と実施要件

CPS 8.1 節に規定のとおり。

8.2 監査人の資格

CPS 8.2節に規定のとおり。

8.3 監査人と認証機関

CPS 8.3 節に規定のとおり。

8.4 監査事項

CP S8.4 節に規定のとおり。

8.5 監査結果の対応

CPS 8.5 節に規定のとおり。

8.6 監査結果の公開

CPS 8.6 節に規定のとおり。

9. 他のビジネス及び法的要件

9.1 料金

9.1.1 証明書の発行及び更新料金

CPS の 9.1.1 項に規定する。

9.1.2 証明書のアクセス料金

規定しない。

9.1.3 証明書の失効情報参照料金

CPS の 9.1.3 項に規定する。

9.1.4 その他認証サービスに関連する料金

CPS の 9.1.4 項に規定する。

9.1.5 払戻し方針

CPS の 9.1.5 項に規定する。

9.2 財務的責任

9.2.1 保険範囲

CPS の 9.2.1 項に規定する。

9.2.2 その他の資産について

CPS の 9.2.2 項に規定する。

9.2.3 利用者等への保証

CPS の 9.2.3 項に規定する。

9.3 ビジネス上の秘密情報の管理について

9.3.1 秘密情報の対象事項

CPS の 9.3.1 項に規定する。

9.3.2 秘密情報の対象外事項秘

CPS の 9.3.2 項に規定する。

9.3.3 秘密情報の管理責任

CPS の 9.3.3 項に規定する。

9.4 秘密情報の管理責任

9.4.1 個人情報保護の方針

CPS の 9.4.1 項に規定する。

9.4.2 個人情報保護の対象情報

CPS の 9.4.2 項に規定する。

9.4.3 個人情報保護の対象外情報

CPS の 9.4.3 項に規定する。

9.4.4 個人情報の管理責任

CPS の 9.4.4 項に規定する。

9.4.5 個人情報の利用に関する説明

CPS の 9.4.5 項に規定する。

9.4.6 法的手続による個人情報の公開

CPS の 9.4.6 項に規定する。

9.4.7 その他個人情報公開の要件

CPS の 9.4.7 項に規定する。

9.5 知的財産権

CPS の 9.5 節に規定する。

9.6 責任と義務

9.6.1 IA の責任と義務

my FinTech は、IA における業務の遂行にあたり、以下の義務を負う。

- CA の秘密鍵の安全な管理を行うこと
- RA からの申請に基づく正確な証明書の発行及び失効を行うこと

- CRL の発行及び公開、ならびに OCSP サーバをもって失効情報を提供すること
- システムの監視及び運用を行うこと
- リポジトリの維持・管理を行うこと

9.6.2 RA の責任と義務

my FinTech は、RA における業務の遂行にあたり、以下の義務を負う。

- 本 CP に基づく利用者の審査を行うこと
- IA への証明書発行申請及び失効申請の正確な処理を行うこと
- 本 CP 1.5.2 項に定める問い合わせ受付を行うこと

9.6.3 利用者の責任と義務

利用者は、以下の義務を負うことを表明し、保証する。

- 証明書の発行申請時における真正かつ正確な情報提供を行うこと
- 本 CP 1.4.1 に定める証明書用途を遵守すること
- 秘密鍵及びパスワードの厳重な管理を行うこと
- 本 CP4.9.1 項に定める事由が生じた場合は、速やかな失効の申請を行うこと
- 秘密鍵の危殆化またはその可能性があると判断したときは速やかに失効申請を行うこと
- 有効期間が満了した証明書及び失効された証明書を使用しないこと
- 関連法規制を遵守すること
- 本 CA は、法令で定めるアルゴリズムのうち、利用者が使用する電子署名アルゴリズムとして、ECDSA(SHA256)を指定し、かつ楕円曲線におけるアルゴリズムとして prime256v1 を指定する。利用者は、当該したアルゴリズムを使用すること

9.6.4 署名検証者の責任と義務

署名検証者は、以下の義務を負うことを表明し保証する。

- 証明書が本 CP 1.4.1 項に定める用途で利用されていることの確認を行うこと
- 本 CA が発行した証明書の有効期間と記載項目の確認を行うこと
- 証明書に行われた電子署名の検証と発行者の確認を行うこと
- CRL または OCSP により、証明書の失効の有無について確認を行うこと
- 本項に規定された義務の不履行により発生した事態に対し、法的責任を負うこと

9.6.5 その他コミュニティ関係者の責任と義務

規定しない。

9.7 保証外事項

本 CA は、本 CP 9.6.1 項及び 9.6.2 項に定める保証に関連して発生する直接損害以外の損害については、本 CP に基づく債務不履行に関していかなる責任も負わない。

本 CA は、署名検証者が自らの判断で本 CA 及び利用者の証明書を信頼した結果については、いかなる責任も負わない。

9.8 責任の制限

my FinTech は、本 CP9.6.1 項及び 9.6.2 項の内容に関し、以下の場合に一切の責任を負わないものとする。

- 本 CA が、本 CP、CPS、本 CP 1.1 項に明記する法規制を遵守したにも関わらず発生するいかなる損害
- my FinTech に起因しない、不法行為、不正使用または過失等により発生するいかなる損害
- 利用者または署名検証者が、本 CP 9.6 項の規定に基づきそれぞれが負う義務の履行を怠ったために生じた損害
- 本 CA が発行した証明書に係る鍵ペアが、my FinTech 以外の第三者の行為により漏洩し生じた損害
- 証明書が利用者、署名検証者または第三者の所有する著作権、営業秘密またはその他の知的財産権を侵害したことにより生じる損害
- ハードウェア的またはソフトウェア的な暗号アルゴリズム解読技術が現時点の予想を超えて向上したことに起因する損害
- 本 CP、CPS、利用契約書または関連諸規程に基づく債務不履行もしくは違反について生じる損害のうち、データ消失、間接的損害、派生的損害、懲罰的損害について、本 CA は責任を負わない。

9.9 補償

本 CA が発行した証明書を利用者または署名検証者が受領もしくは利用した時点で、利用者または署名検証者には、自らの為した以下に掲げるいずれかの行為に起因して生じた my FinTech に対する第三者からの請求、訴訟の提起その他の法的措置により my FinTech が被った損害を賠償し、かつ my FinTech に損害を生ぜしめないようにする責任が生じるものとする。

- 証明書の不正使用、改ざん、利用時の不実の表明
- 本 CP、利用契約書、または CPS への違反
- 利用者の秘密鍵保全の怠慢

9.10 本規程の効力

9.10.1 本規程の効力有効期間

本 CP は、PA が承認することにより有効となる。また、本 CP 9.10.2 項に定める時点の前に 本 CP が無効となることはない。

9.10.2 本規程の無効

本 CP は、本 CP 9.10.3 項に定める規定を除き、本 CA が業務を終了した時点で無効となる。

9.10.3 本規程の効力継続について

本 CP 9.3、9.4、9.5、9.6、9.7、9.8、9.9、9.10.2、9.10.3、9.13、9.14、9.15、9.16 の規定については本 CP の終了後も存続するものとする。

9.11 コミュニティにおける通知と連絡

my FinTech から利用者に対し個別の通知を行う場合は、利用者端末アプリの送信、書面による手渡し、郵便による配達、電子メールの送信が行われたときをもって通知がなされたものとみなす。また、利用者から my FinTech へのすべての通知は、利用者アプリ、書面の郵便、電子メール、電話または FAX によりなされるものとする。

9.12 改訂

9.12.1 改訂手続

本 CA は、PA の指示に基づき、本 CP の見直しを年 1 回行う。また、適宜、本 CP の改訂を行うことができる。改訂の承認は PA が行う。認証業務の規定や手順等が変更となる場合は、遅延なく本 CP を改訂するものとする。

9.12.2 改訂通知方法と通知時期

本 CA は、本 CP 等について、改訂の都度 Web サイトに公開する。my FinTech から当該改訂の撤回の通知が公表されない限り、当該改訂は PA が別途定める時点をもって発効するものとする。利用者がその発効後 15 日以内に当該電子証明書の失効を請求しない場合、利用者は改訂後の本 CP につき同意したものとみなされる。

9.12.3 CP オブジェクト識別子の変更の要件

本 CP の改訂により、OID の変更が必要となるかは PA が判断し、責任を負うものとする。

9.13 紛争解決手続

CPS の 9.13 節に規定する。

9.14 準拠法

本 CP は、日本国内法及び電子署名法に関する法令等に基づき解釈されるものとする。

9.15 適用法の遵守

本 CP は、下記の法令等を遵守する。

- 電子署名及び認証業務に関する法律
- 電子署名及び認証業務に関する法律施行令
- 電子署名及び認証業務に関する法律施行規則
- 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針

9.16 雑則

9.16.1 完全合意条項

本 CP における合意事項は、特段の定めをしている場合を除き、本 CP が改訂または終了されない限り、他のすべての合意事項より優先される。

9.16.2 権利譲渡条項

利用者は、本 CA の提供する本認証サービスの提供を受ける権利を第三者に譲渡できないものとする。

署名検証者は、署名検証者同意書に基づく契約の契約上の地位またはこれに基づく権利もしくは義務のいかなる一部についても、これを第三者に譲渡することができないものとする。

9.16.3 分離条項

本 CP の一部の条項が、何らかの事由により無効または執行できないと判断された場合においても、その他の条項は有効であるものとする。

9.16.4 強制執行条項（弁護士費用及び権利放棄）

本 CA は、いずれかの当事者の行為に関連して被った損害、損失、及び費用について補償及び弁護士費用の支払を求めることができるものとする。本 CA が本 CP または CPS のいずれかの規定の執行を怠った場合でも、かかる規定を本 CA がその後に執行する権利または本 CP ないし CPS の他のいずれかの規定を執行する権利を本 CA が放棄したものとみなされることはないものとし、本 CA が署名した書面により、権利の放棄が有効となる。

9.16.5 不可抗力

天災地変、裁判所の命令、労働争議、その他本 CA の責に帰さない事由により、本 CP 及び CPS 上の義務の履行が一部または全部を遅延した場合には、my FinTech は当該遅延期間について本 CP 及び CPS 上の義務の履行を免れ、利用者または証明書の全部または一部を信頼し、もしくは利用した第三者に対し、何らの責任をも負担しない。

9.17 その他事項

規定しない。

10. 定義と略語

10.1 定義集

用語	定義
暗号モジュール	セキュリティ機能を実装した、暗号境界内のハードウェア、ソフトウェア、及び／又はファームウェアの集合。
運用期間	証明書の実際に有効な期間。 本 CA の証明書及び秘密鍵の使用期間は、最大 180 ヶ月（15 年）に制限するものとする。 OCSP サーバの証明書及び秘密鍵の使用期間は、最大 1 年間の証明書有効期間を有する。 利用者の証明書及び秘密鍵の使用期間は、1824 日（5 年後の 1 日前まで）の期間を有する。証明書の有効開始日時は、開始日時の秒数は証明書を発行した秒と設定し、有効終了日時は、終了日時の秒数は開始日時の秒数から 1824 日後と設定する。
オブジェクト識別子(OID)	特定のオブジェクト又はオブジェクトクラスを参照するために、ISO 登録規格に基づいて登録された一意の英数字/数字識別子。証明書ポリシーに基づき発行される証明書及びサポートされる暗号アルゴリズムを一意に識別するために使用される。
オンライン証明書ステータスプロトコル(OCSP)	証明書のステータスをリアルタイムで検証するために使用されるプロトコルを指す。OCSP レスポンダは、証明書のステータス要求に応答するために使用され、以下のいずれかを発行できる。 ・ good（証明書が失効されていないことを示す応答） ・ revoked（失効された証明書であることを示す応答） ・ unknown（該当する証明書がないことに対する応答） 上記 3 つの応答のいずれかを行うことができる。OCSP レスポンダは CA から提供された証明書データに基づいた認証書ステータスを応答する。
鍵ペアの生成	2 つの数学的に関連する鍵(秘密鍵とそれに対応する公開鍵)で、以下の性質を持つ ・一方の鍵は、他方の鍵でのみ復号化が可能なように通信を暗号化することができる。 ・いずれかの鍵で暗号化されたテキストが利用可能であるなどの状況が想定されても、一方の鍵を他方の鍵から導出または発見することは、実用的な時間内で計算することは困難である。
公開鍵基盤(PKI)	証明書や公開鍵暗号を採用したセキュリティシステムの運用を支えるアーキテクチャ、技術、実務、手順。
識別名(DN)	ITU/CCITT.500 に基づいたディレクトリ内で利用者を特定できるようにするための一意の識別子。(例えば識別名には次のような属性が含まれる:共通名(cn)、電子メールアドレス(mail)、組織名(o)、組織単位(ou)、ロカリティ(l)、州(st)、国(c))
失効	証明書を特定の時点から永久に無効にすることを指す。証明書が有効期間中であっても、証明書を無効とする措置である。
証明書	証明書は電子記録であり、発行された CA、利用者の名前もしくは身元を特定する情報、利用者の公開鍵、有効期間を含む CA によってデジタル的に署名されたもの。本 CP や適用される規格により有効性が与えられる。

用語	定義
証明書失効リスト(CRL)	有効期間満了前に失効した証明書のリスト。
電子署名	電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。 一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。 二　当該情報について改変が行われていないかどうかを確認することができるものであること。 (電子署名及び認証業務に関する法律第二条より)
CA の証明書	CA が発行した公開鍵の証明書。
CA の秘密鍵	CA 証明書に記載されている公開鍵に対応する秘密鍵。CA 証明書の署名に使用される。
証明書ポリシー(CP)	共通のセキュリティ要件を持つある特定のコミュニティ及び・又はアプリケーションに対し、証明書の適用を示す一連の規則。例えば、ある CP は、特定の価格帯の商品またはサービスの取引のための企業間取引に従事する当事者の認証に対して、適用できる証明書の種類を示している。
秘密鍵	鍵ペアのうち、相手方への譲渡や一般公開を行わず、所有者が管理下において秘匿する必要がある鍵。デジタル署名の作成や、対応する公開鍵を使用して暗号化されたデータを復号化する際に使用される。
リポジトリ	証明書及び付随する情報（証明書の有効性や失効の情報など）を保存及び取得するために、CA によって管理されているオンラインシステム。
利用規約	CA と利用者との間で交わされた合意であり、証明書の発行及び管理に関する当事者の権利と責任とを明確にした規約。
利用者	証明書を発行された証明書の対象者。本 CA における特定認証業務においては、自然人個人が証明書の発行対象となる。
X.500	電子ディレクトリサービスを対象としたコンピューターネットワークの規格。ディレクトリアクセスプロトコル(DAP)、ディレクトリシステムプロトコル(DSP)、ディレクトリ情報シャドーイングプロトコル(DISP)、ディレクトリオペレーショナルバインディング管理プロトコル(DOP)が含まれる。
X.509	公開鍵証明書と認証パスの検証のための標準フォーマットを規定した、PKI のための ITU-T（国際電気通信連合-電気通信標準化セクター）の標準規格。

10.2 略語集

略語	意味
CA	認証局（Certification Authority）
CISA	公認情報システム監査員（Certified Information System Auditor）
CP	証明書ポリシー（Certificate Policy）
CPS	認証局運用規程（Certification Practice Statement）
CRL	証明書失効リスト（Certificate Revocation List）
CSR	証明書署名要求（Certificate Signing Request）
DN	識別名（Distinguished Name）
EC	楕円（Elliptic Curve）
FIPS	連邦情報処理基準（Federal Information Processing Standard）
HSM	ハードウェアセキュリティモジュール（Hardware Security Module）
IA	発行局（Issuing Authority）
LRA	支部登録局（Local Registration Authority）
OA	運用局（Operating Authority）
OCSP	オンライン証明書ステータスプロトコル（Online Certificate Status Protocol）
OID	オブジェクト識別子（Object Identifier）
PA	ポリシー局（Policy Authority）
PKI	公開鍵基盤（Public Key Infrastructure）
RA	登録局（Registration Authority）
RFC	インターネットの技術的仕様（Request for Comment）