my 電子証明書
認証局運用規程

Version4.0.0

2025 年 4 月 25 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	2022/9/20	高澤 敦紀	連絡窓口の住所に詳細を追記 情報開示の開示方法・開示証明書について追記 6.5.2 の帳簿書類の保存期間に関する記載を修正 利用者 1 人に対する証明書発行枚数の変更に伴い、11.1.1 の記載を変更。 LRA 管理者の役割の記載を修正。 VA の証明書情報のうち、Subject Public Key Info の記載を修正 OCSP アルゴリズムのうち「Signature Algorithm」の記載を修正 証明書の 2 枚発行に係る失効処理の手順について追記。
1.2	2022/10/20	高澤 敦紀	利用者の証明書プロファイルのうち、生年月日に係る記載を追記。 証明書プロファイル（CA 証明書・リンク証明書・VA 証明書）の suject の規定内容について修正
1.3	2023/2/10	高澤 敦紀	本 CA の実施する内部監査について追記。
1.4	2023/9/8	高澤 敦紀	利用可能なマイナンバーカードの電子証明書の種別について、個人番号カード用である旨等を追記。 「認証業務用設備」に記載を統一
1.5	2023/12/13	高澤 敦紀	「利用申請情報」に記載を統一 「復号」に記載を統一 5.2.1 項 表 5-1 について、以下の点を修正。 ・ RA 管理者の役割に関する記載を変更 ・ RA オペレータを新設 ・ LRA 管理者の役割関する記載を変更

			5.2.2 について、RA オペレータの必要人数及要員数について追記 9.12.2 について記載を修正
1.6	2023/12/13	高澤　敦紀	1.5.2 について連絡担当者の受付日時を変更
1.7	2024/3/19	高澤　敦紀	1.5.2 について連絡担当者の住所を変更
3.0.0	2024/10/2	高澤　敦紀	11.1.1 について、以下を修正 ・電子証明書（基本型）及び電子証明書（属性型）のプロファイルのうち、OU の説明を変更 ・「Not　Before」について、電子証明書の有効期限開始日に関する説明を追記 ・ライブラリ対応利用者端末アプリに関する記載を追記
3.1.0	2024/10/2	高澤　敦紀	11.1.1、②について証明書情報の Subject の内容を変更
4.0.0	2025/4/25	高澤　敦紀	5.1.1 項について、myJPKI サービスの運用に関する記載を追記 5.2.1 項について、myJPKI サービスの要員権限との関係性に関する記載を追記 5.2.3 項について、myJPKI サービスのシステム権限との関係性に関する記載を追記 11.1.1 目について、ライブラリで発行した電子証明書（基本型）及び電子証明書（属性型）について、証明書バージョンの記載を修正。

1. 前書き

1.1 概要

本認証局運用規程（Certification Practice Statement：以下、「CPS」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運用及び手順を規定するものである。

なお、CP と CPS の間に齟齬がある場合には、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 my 電子証明書（以下、「本認証サービス」という）を提供する。本 CPS は、my FinTech が提供する本認証サービスのうち、電子署名法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。

各種要件における運用規程を本 CPS に明記する上で、本 CPS は RFC3647 における Certificate Policy and Certification Practices Framework を採用する。 なお、本 CPS 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 CPS の正式名称は「my FinTech 認証局運用規程」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。

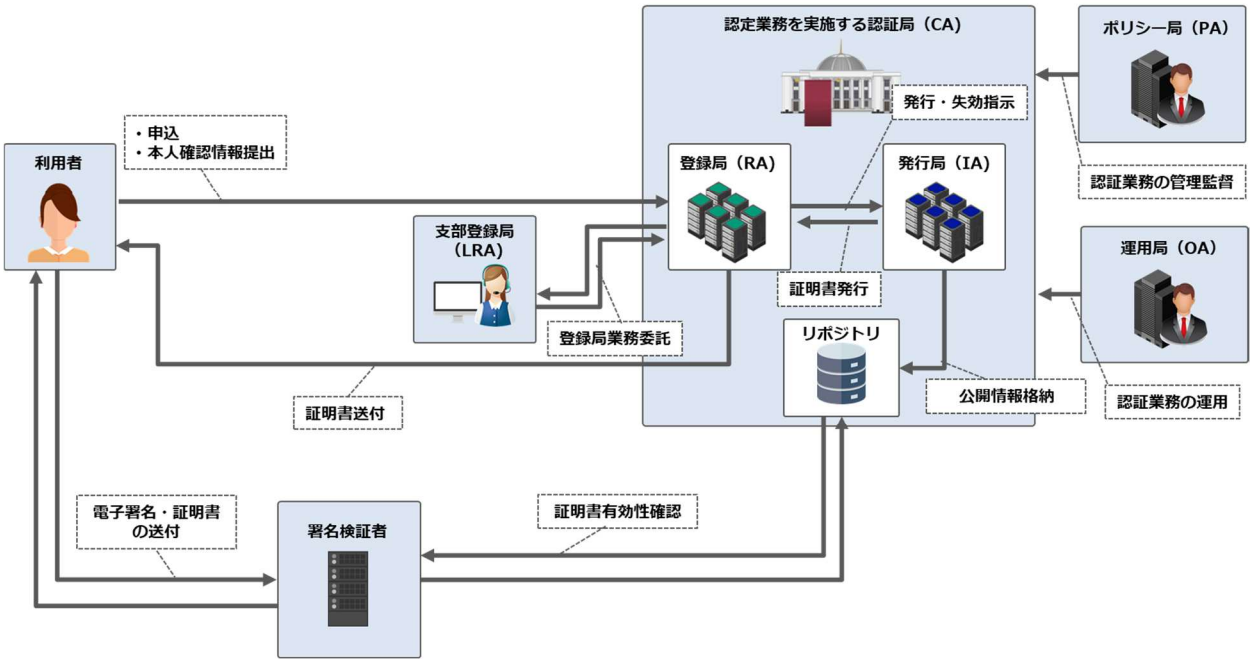
表 1-1 文書名と割り当てられる OID

文書名	OID
my 電子証明書 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 CPS 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）

CP 1.3.1 項に規定のとおり。以下、「PA」という。

1.3.2　運用局（OA）

CP 1.3.2 項に規定のとおり。以下、「OA」という。

1.3.3　認証局（CA）

CP 1.3.3 項に規定のとおり。

1.3.4　発行局（IA）

CP 1.3.4 項に規定のとおり。以下、「IA」という。

1.3.5　登録局（RA）

CP 1.3.5 項に規定のとおり。以下、「RA」という。

1.3.6 支部登録局（LRA）

CP 1.3.6 項に規定のとおり。以下、「LRA」という。

1.3.7 利用者

CP 1.3.7 項に規定のとおり。

1.3.8 署名検証者

CP 1.3.8 項に規定のとおり。

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

CP 1.4.1 項に規定のとおり。

1.4.2 禁止される証明書の用途

CP 1.4.2 項に規定のとおり。

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。

- CP
- 本 CPS
- CP を参照する本認証サービスの利用規約
- CP を参照する本認証サービスの関連諸規定
- 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 CPS 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（メール）：9:00－18:00（日本時間）
- 受付時間（電話）：11:00－18:00（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 CPS の管理者

本 CPS は PA が管理者となる。

1.5.4 CPS の承認手続き

本 CPS 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 CPS 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

CP 2.1 節に規定のとおり。

2.2 公開情報

CP 2.2 節に規定のとおり。

2.3 公開の方法（公開期間や更新タイミング）

CP 2.3 節に規定のとおり。

2.4 リポジトリの参照方法

CP 2.4 節に規定のとおり。

3. 識別と認証

3.1 識別名

3.1.1 識別名タイプ

CP 3.1.1 項に規定のとおり。

3.1.2 識別名の意味付け

CP 3.1.2 項に規定のとおり。

3.1.3 匿名や仮名の利用

CP 3.1.3 項に規定のとおり。

3.1.4 識別名の解釈規則

CP 3.1.4 項に規定のとおり。

3.1.5 識別名の一意性

CP 3.1.5 項に規定のとおり。

3.1.6 商標等について

CP 3.1.6 項に規定のとおり。

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

CP 3.2.1 項に規定のとおり。

3.2.2 利用者の所属組織の確認方法

CP 3.2.2 項に規定のとおり。

3.2.3 利用者本人の確認方法

CP 3.2.3 項に規定のとおり。

3.2.3.1 個人利用者の本人確認

CP 3.2.3.1 目に規定のとおり

3.2.4 確認できない利用申請情報

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

CP 3.3.1 項に規定のとおり。

3.3.2 失効後の鍵更新に対する本人確認と認証

CP 3.3.2 項に規定のとおり。

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

CP 3.4.1 項に規定のとおり。

4. 証明書のライフサイクル運用要件

4.1 証明書の申請

CP 4.1 節に規定のとおり。

4.1.1 利用申請者

CP 4.1.1 項に規定のとおり。

4.1.2 利用申請者の役割と責任

CP 4.1.2 項に規定のとおり。

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、本 CPS 3.2.3.1 目の方法に従う。

4.2.2 証明書申請の諾否

CP 4.2.2 項に規定のとおり。

4.2.3 証明書申請審査にかかる時間

CP 4.2.3 項に規定のとおり。

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

CP 4.3.1 項に規定のとおり。

4.3.2 証明書発行に関する利用者への通知

CP 4.3.2 項に規定のとおり。

4.4 証明書の受領確認

4.4.1 証明書の受領確認方法

CP 4.4.1 項に規定のとおり。

4.4.2 IA による CA の証明書の公開

CP 4.4.2 項に規定のとおり。

4.4.3 IA から RA などへの証明書発行通知

CP 4.4.3 項に規定のとおり。

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

CP 4.5.1 項に規定のとおり。

4.5.2 署名検証者における公開鍵と証明書の用途

CP 4.5.2 項に規定のとおり。

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

CP 4.6.1 項に規定のとおり。

4.6.2 証明書更新申請者

CP 4.6.2 項に規定のとおり。

4.6.3 証明書更新業務

CP 4.6.3 項に規定のとおり。

4.6.4 証明書更新に関する利用者への通知

CP 4.6.4 項に規定のとおり。

4.6.5 更新された証明書の受領確認方法

CP 4.6.5 項に規定のとおり。

4.6.6 IA による更新された CA の証明書の公開

CP 4.6.6 項に規定のとおり。

4.6.7 IA から RA などへの証明書更新通知

CP 4.6.7 項に規定のとおり。

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

CP 4.7.1 項に規定のとおり。

4.7.2 証明書再発行申請者

CP 4.7.2 項に規定のとおり。

4.7.3 証明書再発行業務

CP 4.7.3 項に規定のとおり。

4.7.4 証明書再発行に関する利用者への通知

CP 4.7.4 項に規定のとおり。

4.7.5 再発行された証明書の受領確認方法

CP 4.7.5 項に規定のとおり。

4.7.6 IA による再発行証明書の公開

CP 4.7.6 項に規定のとおり。

4.7.7 IA から RA などへの証明書再発行通知

CP 4.7.7 項に規定のとおり。

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

CP 4.8.1 項に規定のとおり。

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

CP 4.9.1 項に規定のとおり。

4.9.2 証明書失効申請者

CP 4.9.2 項に規定のとおり。

4.9.3 失効申請手続

CP 4.9.3 項に規定のとおり。

4.9.4 失効申請の猶予期間

CP 4.9.4 項に規定のとおり。

4.9.5 失効処理に要する時間

CP 4.9.5 項に規定のとおり。

4.9.6 署名検証者による失効情報確認

CP 4.9.6 項に規定のとおり。

4.9.7 証明書失効リスト（CRL）発行頻度（CRL 発行時）

CP 4.9.7 項に規定のとおり。

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）

CP 4.9.8 項に規定のとおり。

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

CP 4.9.9 項に規定のとおり。

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

CP 4.9.10 項に規定のとおり。

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

CP 4.9.12 項に規定のとおり。

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

CP 4.10.1 項に規定のとおり。

4.10.2 オンライン証明書有効性確認サービスの利用

CP 4.10.2 項に規定のとおり。

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

CP 4.11 節に規定のとおり。

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

本 CA では認証業務の種別毎に施設及び部屋が区画されており、それぞれの部屋には異なるセキュリティレベルを設定している。本 CA に関する設備を設置する部屋には、認証設備室、LRA 業務室がある。以下がそれぞれの部屋区設定するセキュリティレベルとなる。

- 認証設備室

  認証設備室は、RA の登録業務に係る機器の設置及び IA の発行業務における認証業務用設備が設置される部屋である。認証設備室は、以下の建築構造となる。

  - 地震、火災、水害、及びその他の災害による影響を容易に受けない施設内に設置される。
  - 外部からの侵入が容易にできないようにセキュリティが確保された施設の内部に設置される。
  - 施設の内部の個室に設置され、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。
  - 認証設備室が設置される施設の内外に認証業務用設備の所在に関わる情報は一切表示しない。

なお、当社は、公的個人認証法第十七条第一項第四号に掲げるものとして、当社 SP 事業者（当社に対して電子署名等確認業務を委託し、かつ認定認証業務に係る署名検証者に該当する者をいう）に対し、マイナンバーカードの電子証明書に関する情報提供を行うサービス（以下、「myJPKI サービス」という）を提供する。当該サービスは、認証設備室内に設置された“RA の登録業務に係る機器”にて運用を行うものとする。

- LRA 業務室

  LRA 業務室は、RA における RA 業務の一部を実施する部屋であり、my FinTech が業務委託した企業の要員が業務を行う。登録用端末設備及び利用者識別設備が設置される部屋である。LRA 業務室は、認証設備室が設置される施設とは異なる施設に設置される。LRA 業務室は、以下の建築構造となる。

  - 地震、火災、水害、及びその他の災害による影響を容易に受けない施設内に設置される。
  - 外部からの侵入が容易にできないようにセキュリティが確保された施設の内部に設置される。
  - 施設の内部の個室に設置され、関係者以外が用意に侵入することができない安全な環境において運用する。
  - LRA 業務室が設置される施設の内外に LRA 業務室の所在に関わる情報は一切表示しない。

  なお、当社は、my 電子証明書サービスの他に、myJPKI サービスを提供しており、当該サービスに関する顧客管理業務等については、LRA 業務室内の登録用端末設備から実施するものとする。

5.1.2 物理的アクセス

本 CA の認証設備室については、以下の物理的なアクセス制限を実施する。

- 認証設備室は、隔壁により区画されている部屋であり、あらかじめ PA により許可された要員のみが入室できることとし、入退室の際には、要員の認証を行い、不正な侵入を防止する。
- 認証設備室は、入退室管理装置により業務を実施する要員の入退室管理が行われる。入室する権限を持つ要員が認証設備室へ入出する場合については、入退室の履歴が記録される。

- 認証設備室の入室は、入室する複数人による認証の操作が必要とする。
- 認証設備室の入退室時の認証は、入退室用 IC カード認証、生体認証、その他の実装可能な技術手段における認証が行われ、セキュリティレベルに応じて入退室時の認証が 1 つの場合、複数の場合に分けられる。
- 認証設備室の入室及び退室については、2 名による操作が必要となる。
- 認証設備室の入退室時の認証において、入室操作の時間（認証設備室の扉の解錠時間）が規定の時間を超えた場合、アラームが発生する。
- 認証設備室の退室完了後、認証設備室内はモーションセンサを働かせるなどで、無人の認証設備室内で動きを検出した場合に警報が発せられる。
- 認証設備室は監視システムにより 24 時間 365 日の監視が行われ、要員の入退室並びに認証業務設備室での作業等の活動が記録される。
- 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される。また、入退室については、月に 1 度正しく入退室が実施されているか確認を行う。

本 CA における LRA 業務室については、以下の物理的なアクセス資源を実施する。

- LRA 業務室は、間仕切りで仕切られた部屋であり、あらかじめ PA により許可された要員のみが入室できることとし、入退室の際には、要員の認証を行い、不正な侵入を防止する。
- LRA 業務室は、入退室管理装置により業務を実施する要員の入退室管理が行われる。入室する権限を持つ要員が LRA 業務室へ入出する場合については、入退室の履歴が記録される。
- LRA 業務室における入退室時の認証は、入退室用 IC カード認証における認証が行わる。
- LRA 業務室は、入退室時の認証において、入室操作の時間（LRA 業務室の扉の解錠時間）が規定の時間を超えた場合、アラームが発生する。
- LRA 業務室は監視システムにより 24 時間 365 日の監視が行われ、要員の入退室並びに LRA 業務室での作業等の活動が記録される。

5.1.3 電源と空調

本 CA の認証設備室については、以下の電源と空調の確保を行う。

- 認証設備室は、認証業務用設備、監視システム、入退室管理装置等の安定運用のために、必要かつ十分な容量の電源の確保ができる施設を利用する。
- 認証設備室は、認証業務用設備、監視システム、入退室管理装置等の安定運用のために、空調設備を設置、稼働させ、設備の温度や湿度制御を行う。
- 認証設備室は、認証業務用設備、監視システム、入退室管理装置等の地震、火災、水害、及びその他の災害の影響による瞬断や停電への対策として、無停電電源装置及び自家発電装置からの給電が可能な状態を維持する。

本 CA における LRA 業務室については、以下の電源と空調の確保を行う。

- LRA 業務室は、監視システム、入退室管理装置等の安定運用のために、必要かつ十分な容量の電源の確保ができる施設を利用する。
- LRA業務室は、登録用端末設備及び利用者識別設備と要員の作業環境を適切に維持するため、空調設備を設置、稼働させ、温度や湿度制御を行う。

- LRA 業務室は、監視システム、入退室管理装置等の地震、火災、水害、及びその他の災害の影響による瞬断や停電への対策として、無停電電源装置からの給電が可能な状態を維持する。

5.1.4 水害防止対策

本 CA の認証設備室については、以下の水害防止対策を実施する。

- 認証設備室は、漏水検知器を設置し、洪水等の水害が生じた際に速やかに対応が可能な態勢とする。
- 認証設備室は、洪水等の水害の対策として、浸水防止の措置が行われており、また排水管等の漏水防止措置が行われている施設に設置する。
- 認証設備室は、建物の二階以上に設置する。

本 CA における LRA 業務室については、以下の水害防止対策を実施する。

- LRA 業務室は、建物の二階以上に設置する。

5.1.5 防火対策

本 CA の認証設備室については、以下の防火対策を設置する。

- 認証設備室は、建築基準法に適合した耐火建築物に設置する。
- 認証設備室は、建築基準法に適合した防火区画内に設置され、自動火災報知器及び消火設備を設置する。

本 CA における LRA 業務室については、以下の防火対策を設置する。

- LRA 業務室は、建築基準法に適合した耐火建築物に設置する。
- LRA 業務室は、建築基準法に適合した防火区画内に設置され、自動火災報知器及び消火設備を設置する。

5.1.6 媒体等の災害対策

本 CA に係る全ての媒体は、キャビネット、金庫等の施錠されたセキュリティが確保された場所で管理される。また、当該キャビネット、金庫等が設置される場所については、許可された要員のみが入室でき、入退室管理装置により、セキュリティレベルに応じた入退室管理が行われる。入室する権限を持つ要員が認証設備室へ入出する場合については、入退室の履歴が記録される。

5.1.7 廃棄処理

本 CA に係る全ての媒体は、以下の方法により廃棄処理を行う。

- 文書等の紙媒体については、シュレッダーにより裁断の上、内容が確認できない状態とし、廃棄する。
- コンピュータ機器等の電子的媒体については、初期化により記録された電子的記録を完全に消去し、内容を復元できない状態とし、廃棄する。
- 本 CA の秘密鍵が格納された電子媒体及び本 CA の秘密鍵のバックアップが格納された電子的媒体については、初期化により内容を復元できない状態とすることで破棄が許可される。なお、内容を復元できない状態とすることが不能な場合は、物理的に当該電子媒体を破壊する。

5.1.8 オフサイトバックアップ

本 CA の秘密鍵及びシステムの復旧上重要なデータ、ソフトウェアアプリケーション、その他認証業務用設備は、遠隔地にバックアップ認証設備室を構築し、データの欠損・消失が行われない様に管理する。バックアップ認証設備室は本施設と同等のセキュリティ及び設備基準を持つ施設を選定する。

上記のバックアップは、本施設とバックアップ認証設備室の間において、安全な通信路を介して行われる。通信路の安全性は、バックアップ装置と CA との間で、閉域網を構築し、暗号化及び情報の改ざん検知・防止措置を施すことで担保される。

5.2 手続的管理

5.2.1 各要員の役割

本 CA の運営に携わる要員とその役割を以下の表に示す。

表 5-1 本 CA の要員の役職と役割

要員の役職	役割	所属
CA 責任者	• 本 CA のすべてを総括する • 本 CA に関わる全ての要員について役割を任命する • 本 CA の監査について、管理監督する • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応を決定する • 災害、事故等の緊急事態時における対応を決定する	—
PA 管理者	• CP/CPS に基づいて発行される証明書が CP/CPS における要件を充足し続けることの保証 • CP/CPS のレビュー、承認、改訂 • CP/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 • CP/CPS 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 • LRA において実施される登録業務の一部の監査・監督 • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応を行う • 災害、事故等の緊急事態時における対応を行う	PA
PA 事務員	• CP/CPS のレビュー、承認、改訂についての補助を実施する • CP/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、改訂についての補助を実施する • CP/CPS 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、承認についての補助を実施する • LRA において実施される登録業務の一部の監査・監督についての補助を実施する • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応を行う • 災害、事故等の緊急事態時における対応を行う	PA

要員の役職	役割	所属
OA 管理者	• CP/CPS、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 • CP/CPS 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 • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応を行う • 災害、事故等の緊急事態時における対応を行う	OA
OA 事務員	• CP/CPS、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についての補助を実施する • 本 CA システムの保守・管理業務についての補助を実施する • CP/CPS 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についての補助を実施する • 本 CA が委託する監査人への監査に関する情報の提供についての補助を実施する • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応を行う • 災害、事故等の緊急事態時における対応を行う	OA
CA システム 管理者	• CA 責任者の管理の下、CA のシステムの維持管理を行う • RA システム・IA システム・リポジトリのハードウェア・ソフトウェアのセットアップ、保守を行う • RA システム・IA システム・リポジトリの動作状況の監視を行う • RA システム・IA システム・リポジトリの監査ログの採取及び検査を行う • RA システム・IA システム・リポジトリのハードウェア・ソフトウェアの機能強化を行う • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応を行う • 災害、事故等の緊急事態時における対応を行う	OA

要員の役職	役割	所属
CA システム 保守員	• RA システム・IA システム・リポジトリのハードウェア・ソフトウェアのセットアップ、保守の補助を行う • RA システム・IA システム・リポジトリの動作状況の監視補助を行う • RA システム・IA システム・リポジトリの監査ログの採取及び検査補助を行う • RA システム・IA システム・リポジトリのハードウェア・ソフトウェアの機能強化の補助を行う • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応の補助を行う • 災害、事故等の緊急事態時における対応の補助を行う	OA
CA システム 開発者	• CA に係るシステムの開発を行う • CA に係るシステムの改善を行う • CA に係るシステムの検証を行う • CA に係るシステムの品質保証を行う	OA
IA 管理者	• CA 責任者の管理の下、CA の IA 業務を管理する • IA オペレータを任命する • IA オペレータの管理を行う • CA 秘密鍵の生成・バックアップ • CA 秘密鍵の廃棄 • CA システムの起動及び停止 • 証明書の発行及び失効処理 • CRL の生成 • CA システムのバックアップ • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応を行う • 災害、事故等の緊急事態時における対応を行う	IA
IA オペレータ	• CA システムの起動及び停止 • 証明書の発行及び失効処理 • CRL の生成 • CA システムのバックアップ • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応を行う • 災害、事故等の緊急事態時における対応を行う	IA

要員の役職	役割	所属
RA 管理者	• CA 責任者の管理の下、CA の RA 業務を管理する • LRA 管理者及び RA オペレータを任命する • LRA 管理者及び RA オペレータの管理を行う • RA システムのソフトウェアのセットアップ、保守作業を行う。 • RA システムのソフトウェアの監査ログの採取及び検査を行う • RA システムのソフトウェアの機能強化を行う • 利用者識別符号の生成に関する管理を行う • 利用者識別符号の生成等の RA 業務に係る帳簿書類の保管 • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応を行う • 災害、事故等の緊急事態時における対応を行う	RA
RA オペレータ	• RA システムのソフトウェアのセットアップ、保守作業を行う。 • RA システムのソフトウェアの監査ログの採取及び検査補助を行う • RA システムのソフトウェアの機能強化の補助を行う • 利用者識別符号の生成に関する補助を行う。 • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応を行う • 災害、事故等の緊急事態時における対応を行う	RA
LRA 管理者	• LRA 業務の管理・監督を行う • LRA オペレータの管理を行う • LRA オペレータを任命する • LRA 業務の一部を業務委託する場合は、業務委託契約に基づき委託会社の管理を行う • LRA オペレータの審査記録の確認、管理を行う • 利用申し込み、証明書発行依頼に対し、受領を行うとともにその管理責任を有する • 本人確認を行い、結果の記録を行う • 証明書の発行を承認する • 証明書の申請における審査状況・審査結果を利用者に通知する • 証明書の利用者の情報の照会を行う • 本認証サービスに係る利用者からの問い合わせの対応を行う	LRA

要員の役職	役割	所属
LRA オペレータ	• 本人確認を行い、結果の記録を行う • 証明書の発行を承認する • 証明書の申請における審査状況・審査結果を利用者に通知する • 証明書の利用者の情報の照会を行う • 本認証サービスに係る利用者からの問い合わせの対応を行う • 暗号モジュール等の利用者への発送業務を行う	LRA
LRA システム 管理者	• LRA 業務に必要な端末機器の管理を行う • LRA 業務室におけるセキュリティ機器の管理を行う • LRA 業務に必要な端末機器のセットアップ、保守を行う • LRA 業務に必要な端末機器の動作状況の監視を行う • LRA 業務に必要な端末機器の監査ログの採取及び検査を行う • LRA 業務に必要な端末機器の機能強化を行う • 本 CA の秘密鍵が危殆化、または危殆化したと疑われる状況時の対応を行う • 災害、事故等の緊急事態時における対応を行う	LRA

また、当社が別途提供する myJPKI サービスに関する運用業務については、以下の役職員が実施するものとする。

- myJPKI サービス 関連システムの維持管理：RA 管理者又は RA オペレータ
- myJPKI サービスにおける顧客管理業務：LRA 管理者又は LRA オペレータ

5.2.2 各要員の必要人員

本 CA の運営における各要員の人員数は、以下のとおりである。

- CA 責任者 ：1 名
- PA 管理者 ：1 名
- PA 事務員 ：1 名以上
- OA 管理者 ：1 名
- OA 事務員 ：1 名以上
- CA システム管理者 ：1 名
- CA システム保守員 ：1 名以上
- IA 管理者 ：1 名以上
- IA オペレータ ：2 名以上
- RA 管理者 ：1 名
- RA オペレータ ：2 名以上

- LRA 管理者 ：1 名
- LRA オペレータ ：2 名以上
- LRA システム管理者 ：1 名以上
- CA システム開発者 ：1 名以上

IA 管理者は 1 名以上の要員を配置する。

IA オペレータ、RA オペレータ及び LRA オペレータは相互牽制の必要から 2 名以上の要員を配置する。

ただし、セキュリティ上問題ないと判断された場合には、1 名の要員が複数の役割を兼務する場合がある。

また、利用者からの証明書の申請件数の増加により、要員を増員する場合がある。

LRA オペレータについては業務委託先企業が選定した要員を任命することができる。

5.2.3 各要員の本人確認と認証

認証設備室及び認証業務用設備の利用に際し、各要員の役割に応じて、入退室権限及びシステムの操作権限を定める。認証設備室及び認証業務用設備の利用時においては、入退室 IC カード、生体認証、電子証明書、ID 及びパスワード等の単体での認証、または複数での認証により要員の本人確認を行う。

なお、myJPKI サービスに関する基盤システム（認定認証業務用 RA システム内に搭載）、及び顧客管理用インターフェース（登録用端末設備からアクセス）についても、システムの操作権限を定め、電子証明書、ＩＤ及びパスワード等の単体での認証、または複数での認証により要員の本人確認を行うものとする。

5.2.4 要員の権限分割

本 CA の運営において、セキュリティ上問題ないと判断された場合には、1 名の要員が複数の役割を兼務する場合がある。

また、利用者からの証明書の申請件数の増加により、要員を増員する場合がある。

5.3 要員管理

5.3.1 要員の資格・経歴・身分証明

本 CA の運営に携わる者は、my FinTech における一人の社員・役員またはグループ社員でなければならない。

なお、LRA オペレータは my FinTech が業務委託する企業（以下、「LRA 業務委託先企業」という）が選定する適切な能力を持つ従業員を割り当てることができる。

5.3.2 経歴の確認方法

本 CA の運営に携わる者については、my FinTech が定める採用基準に基づき、就業前の身元調査が行われるものとする。LRA の業務に関わる LRA 運営企業の従業員に関しても、同様に my FinTech が確認する。

5.3.3 教育訓練

my FinTech は、本 CA の運営に携わる者に対し（LRA の業務の業務委託企業の従業員は除く）、教育及び訓練を実施する。教育及び訓練には、CP、CPS、CP を参照する本認証サービスの関連文書についての教育の他、各役割に応じた必要な教育及び訓練を実施する。

LRA の業務に関わる LRA 運営企業の従業員の管理者に関しても、同様に my FinTech が教育訓練を行う。LRA の業務の業務委託企業の従業員への教育は、業務委託企業の管理者の監督のもとで my FinTech が行う場合がある。

5.3.4 再教育訓練の実施頻度と要件

my FinTech は、本 CA の運営に携わる者（LRA の業務の業務委託企業の従業員は除く）に対し、再教育及び再訓練を定期的に実施する。LRA の業務に関わる LRA 運営企業の従業員の管理者に関しても、同様に my FinTech が教育訓練を行う。

なお、以下の状況が発生した場合、再教育及び再訓練が行われる。

- CP 及び CPS が改訂され、PA、CA 責任者、IA 責任者、RA 責任者のいずれかの者が必要と判断した場合
- CA のシステムが変更され、PA、CA 責任者、IA 責任者、RA 責任者のいずれかの者が必要と判断した場合
- その他、PA、CA 責任者、IA 責任者、RA 責任者のいずれかの者が必要と判断した場合

5.3.5 要員ローテーションの頻度と方法

my FinTech は、本 CA の運営に携わる要員（LRA の業務に関わる LRA 運営企業の従業員を含む）のローテーションを実施しない。

5.3.6 要員の罰則規定

my FinTech は、本 CA の運営に携わる要員（myFinTech における社員、役員、グループ社員）に対し、与えられた権限を逸脱した行為を行った場合において、故意か過失かに関わらず、定められた就業規則による罰則を適用する。

なお、与えられた権限を逸脱した行為を行った者が業務委託契約による外部企業の要員である場合は、当該要員は、今後一切、本認証業務に携わることができないものとする。また、my FinTech と当該外部企業との業務委託契約に定められた損害賠償が適用されるものとする。

5.3.7 委託契約の要件

LRA 等の業務委託により雇用された要員は、CP 及び CPS の 5.3 節の規定に準じる。

5.3.8 要員への配布資料

本 CA の運営に携わる全ての者（LRA の業務に関わる LRA 運営企業の従業員を含む）は、役割及び許可された権限に応じて、本 CA に関する文書を参照することができる。

5.4 監査ログ

5.4.1 記録するイベント

my FinTech は、CP 及び本 CPS の準拠とセキュリティを評価するため、監査ログとして以下の記録を収集する。

- 本 CA に係るシステムの稼働ログ及び機能、設定等変更時の操作ログ
- IA 業務・RA 業務・LRA 業務における証明書の発行申請、失効申請、証明書の生成、証明書の失効処理に関連するイベントログ及び操作ログ
- リポジトリにおける公開情報の変更に関連するログ
- 本 CA に係るシステムにおけるネットワークのセキュリティに関連するログ
- 本 CA に係るシステムにおける障害及び復旧に関連するログ
- 本 CA に係るシステムにおける保守及び点検に関連するログ
- 本施設及び認証設備室への入退室・監視システムに関連する記録

記録するログについては、イベントの種類、イベント要求の発行先、イベントの発生日時、処理の成功または失敗等の結果、要員の操作が関連する処理に関しては要員を識別する ID が含まれるものとする。

5.4.2 監査ログの確認頻度

本 CA は監査ログの監査を 1 年に一度以上の頻度で行う。本 CA のシステムにおいて不正・事故などが疑われる状況である場合は、速やかに監査ログの検査を行う。

5.4.3 監査ログ保存期間

RA 及び LRA による監査ログについては、1 年間は保管する。ただし、認証設備室の監視カメラの映像記録は除き、当該監視カメラの映像記録の保存期間は 1 週間とする。

5.4.4 監査ログの保存方法

監査ログは許可された要員のみが閲覧できるよう、閲覧権限の設定を行う。監査ログが物理的な文書である場合、保管された保管庫への入退室権限を設ける。監査ログが電子媒体での保管である場合、ファイルストレージへのシステムアクセス権限を設ける。

5.4.5 監査ログのバックアップ手続

my FinTech は監査ログについて、定期的なバックアップを実施する。

5.4.6 監査ログシステムの設置場所（内部と外部）

セキュリティ監査イベントの収集機能は、本 CA の CA システム、リポジトリの機能、ネットワークシステム、入退室管理装置の機能として、業務及びセキュリティに関する重要な事象をイベントとして収集する。

5.4.7 イベント実施者への通知

本 CA の監査ログはイベント実施者への通知を行わない。

5.4.8 脆弱性評価

本 CA のシステムにおいて、リポジトリ等のインターネットに公開されるサーバについては、定期的に脆弱性評価を行い、不正な侵入、攻撃に対して対策措置を講じる。

5.5 帳簿書類

5.5.1 保存する帳簿書類

本 CPS 5.4.1 項に定める監査ログ情報の他、以下の書類及び電子的な記録を含めた帳簿書類を保存する。保存する帳簿書類は電子署名法に準拠する。

① 証明書の発行の申請に関連する帳簿書類及び電子的記録

- 利用の申請に係る電子的記録
- 電子署名法施行規則第六条第一号の説明に関する電子的記録
- 利用者の本人確認に用いる、利用者が現に有している電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（以下、「公的個人認証法」という）第三条第一項に規定する個人番号カード用署名用証明書に係る電子署名の電子的記録
- 利用の申請に対する諾否を決定した要員の氏名及び要員を特定する ID の電子的記録
- 利用の申請に対する承諾をしなかった場合においては、その理由を記載した電子的記録
- 電子証明書及びその作成に関する記録
- 登録業務に関する電子的記録
- 発行業務に関する電子的記録
- 利用者識別符号の受領に関する電子的記録
- 利用者の公開鍵

② 証明書の失効の申請に関連する帳簿書類及び電子的記録

- 失効の申請に係る書類
- 代理人による失効の依頼に係る書類
- 失効の申請に係る電子的記録
- 失効に関する情報及びその作成に関する記録
- 失効申請における重要事項説明に関する電子的記録
- 利用者の本人確認に用いる情報の電子的記録
- 利用者の本人確認に用いる書類
- 代理人の本人確認に用いる書類
- 失効の申請に対する諾否を決定した要員の氏名及び要員を特定する ID の電子的記録
- 失効の申請に対する承諾をしなかった場合においては、その理由を記載した電子的記録
- 登録業務に関する電子的記録
- 証明書の失効業務に関する電子的記録

③ 証明書の開示の申請に関連する帳簿書類及び電子的記録

- 開示の申請に係る書類
- 開示の申請に係る電子的記録
- 開示に関する情報及びその作成に関する記録
- 利用者の本人確認に用いる情報の電子的記録
- 利用者の本人確認に用いる書類
- 開示の申請に対する諾否を決定した要員の氏名及び要員を特定する ID の電子的記録
- 開示の申請に対する承諾をしなかった場合においては、その理由を記載した電子的記録

④ 組織管理に関連する帳簿書類及び電子的記録

- 本 CPS 5.4 に規定する監査ログ
- CP、本 CPS、CP に関連する契約文書及びその改訂記録
- 業務手順に関する規定及びその改訂記録
- 委託契約に関する書類及びその改訂記録
- 業務に従事する者の責任及び権限並びに指揮命令系統に関する書類
- 準拠性監査の実施結果に関する記録

⑤ 本 CA の鍵及び CRL に関する帳簿書類及び電子的記録

- 本 CA の公開鍵
- 本 CA の秘密鍵の生成及び管理に関する記録
- CRL

⑥ 設備及び安全対策措置に関連する帳簿書類及び電子的記録

- 認証設備室への入退室の記録及び入室権限を持たない者の入室時の記録
- 不正なアクセス等が発生した場合におけるセキュリティ監査イベントとしての記録
- 認証業務用設備の障害及び復旧に関する記録
- 認証業務用設備の保守、点検に関する記録
- 帳簿書類及び電子的記録の利用、廃棄に関する記録
- 認証設備室に設置した監視カメラによる映像記録
- 認証業務用設備の動作に関する記録
- 認証設備室への入退室及びその操作の許諾に関する記録
- 事故に関する記録

5.5.2 帳簿書類の保存期間

本 CA は本 CPS の 5.5.1 項に規定される記録①-⑤について、当該帳簿書類に係る証明書の有効期間の満了日から少なくとも 10 年間は保管する。

また、記録①-⑤において、帳簿書類が電子データであるものに関してはサーバ上に保管され、当該帳簿書類に係る証明書の有効期間の満了日から少なくとも 10 年間は保管する。

なお、本 CPS5.5.1 項に規定される記録⑥（認証設備室に設置した監視カメラによる映像記録を除く）については、作成された日から少なくとも次回の特定認証業務の認定更新を経るまでの間（1 年間）保管するものとする。

5.5.3 帳簿書類の保存方法

保存する帳簿書類及び電子的記録は許可された要員のみが閲覧できるよう、閲覧権限の設定を行う。保存する帳簿書類及び物理的な文書である場合、保管された保管庫への入退室権限を設ける。保存する帳簿書類が電子媒体での保管である場合、ファイルストレージへのシステムアクセス権限を設ける。

5.5.4 帳簿書類のバックアップ

本 CA は、保存する帳簿書類の紙の原本について厳重に管理を行い、毀損の無いように保存する。電子的記録については、定期的なバックアップを実施する。

5.5.5 帳簿書類に対するタイムスタンプ

本 CA は保存する帳簿書類及び電子的記録について、処理を行った日付を記録する。帳簿書類が物理的な文書である場合、処理を担当する要員が、日付及び時刻を記録する。電子的記録である場合、CA システムにより自動的に処理を行った日付及び時間を記録する。

5.5.6 帳簿書類システムの設置場所（内部又は外部）

帳簿書類及び電子的記録の保存に関しては、帳簿書類が紙媒体である場合、CA の要員が収集し所定の保管場所に格納する。電子的記録である場合、CA の要員が収集し所定の保管場所に格納するか、または、本 CA のシステムが自動的に収集しファイルストレージへ保管する。

5.5.7 帳簿書類の確認方法

記録の取得及び閲覧が認められる者として、本 CA の要員、監査人及び PA が認めた者に限定する。

なお、本 CA は、電子媒体で保存される帳簿書類について、HDD を用いたファイルストレージを用いて保管を行う。

当該ファイルストレージは、保存された帳簿書類の可読性を保証するため、動作状況について定期的に確認を実施すると共に HDD の故障などに備え RAID1 相当の構成にて運用する。

5.6 CA の鍵更新

本 CA の秘密鍵の更新は、CA の証明書の残存有効期限が利用者の証明書の有効期間よりも短くなる前に実施される。CA の秘密鍵の更新を行った後、利用者に CA の公開鍵を公開する方法は、本 CPS 6.1.4 項に規定する。

5.7 危殆化や災害時の対応

5.7.1 危殆化時の対応手順

本 CA の秘密鍵の危殆化、または危殆化が疑われる状況となった場合の対応手順を以下に示す。また、本 CA は危殆化、または危殆化が疑われる状況となった場合、以下の手順を速やかに実行する。

① 当該秘密鍵を用いた認証業務の停止

② 当該秘密鍵を用いて発行した全ての証明書の失効及び失効情報のリポジトリの公開

③ 当該秘密鍵が危殆化した事実の利用者及び署名検証者への通知

④ 当該秘密鍵及び秘密鍵のバックアップの廃棄

⑤ 当該秘密鍵が危殆化した事実の主務大臣への通知

⑥ 当該秘密鍵が危殆化した原因の調査

⑦ 再発防止策の策定並びに PA による再発防止策の評価・承認

⑧ 当該秘密鍵が危殆化した原因調査結果及び再発防止策の主務大臣への報告

危殆化、または危殆化が疑われる状況となった場合の対応を実行した後、本 CA における認証業務の継続が可能である場合には、新たに CA の秘密鍵を生成し、CA の証明書の発行を行い、本認証サービスの継続に最善を尽くすものとする。

また、本 CA では、緊急事態（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、地震、火災、水害等の自然災害やパンデミック新型感染症の発生等）においても、従業員およびその家族の安全を確保しながら当社の認定認証事業を適切に継続・運営することを目的として、事業継続基本計画書（BCP）を別途規定している。

本項目における具体的な復旧手順については、BCP において詳細を記載する。

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

本 CA の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、または重大障害が疑われる状況となった場合の対応手順を以下に示す。また、本 CA は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、または重大障害が疑われる状況となった場合、以下の手順を速やかに実行する。

① 被害状況を調査の上、対策を実施し、バックアップデータによる回復措置を行う

② 被害の状況、原因及び復旧の見通しを利用者及び署名検証者に対し、リポジトリに公開し通知する

③ 調査の結果、原因が判別した後、対策を講じ、再発防止策を立てる

④ OCSP サーバが停止し、CRL の有効期限内に復旧の目途が立たない場合、その旨を CRL の有効期限内リポジトリに公開し、利用者及び署名検証者に通知する。また、CRL の有効期限内に利用者及び署名検証者に通知することができず、7 日以上 CRL の更新が行えなかった場合には、重大障害として、障害の内容、発生日時、措置状況等を主務大臣へ報告する

本項目における具体的な復旧手順については、BCP において詳細を記載する。

5.7.3 利用者の秘密鍵の危殆化時の対応手順

CP 5.7.3 項に規定のとおり。また、本項目における具体的な復旧手順については、BCP において詳細を記載する。

5.7.4 災害時の認証業務の継続について

本 CA が認証業務の停止を伴う災害を受けた場合の対応手順を以下に示す。また、本 CA は認証業務の停止を伴う災害を受けた場合以下の手順を速やかに実行する。

① 被害状況の調査

② 被害状況の原因調査

③ 被害状況、原因、復旧の見通しについての利用者及び署名検証者への通知

本 CA が新型感染症やパンデミック等の影響により、政府、自治体等により本認証サービスの停止の要請を受けた場合の対応手順を以下に示す。

① 新型感染症やパンデミック等による本認証サービスへの影響についての調査

② 政府、自治体等による本認証サービス停止の要請への諾否の検討

③ 本認証サービスの停止、再開の見通しについての利用者及び署名検証者への通知

本項目における具体的な復旧手順については、BCP において詳細を記載する。

5.8 認証業務の廃止について

本 CA が認証業務を廃止する場合、以下のことを行う。

① 本 CA の認証業務廃止日までに有効期限が残っている全ての証明書を失効し、リポジトリに公開する

② 本 CA の認証業務を廃止する場合には、廃止日の 60 日前までに利用者に通知する

③ 本 CA の認証業務廃止時に、CA の秘密鍵及び秘密鍵のバックアップは完全に初期化し、その保存媒体を物理的に破壊・破棄する

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

CP 6.1.1 項に規定のとおり。

6.1.2 利用者の秘密鍵の安全な配付方法

CP 6.1.2 項に規定のとおり。

6.1.3 利用者の公開鍵の CA への配付方法

CP 6.1.3 項に規定のとおり。

6.1.4 CA の公開鍵の検証者への配付方法

CP 6.1.4 項に規定のとおり。

6.1.5 鍵サイズ

CP 6.1.5 項に規定のとおり。

6.1.6 公開鍵暗号方式のパラメーター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）

CP 6.1.7 項に規定のとおり。

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

CP 6.2.1 項に規定のとおり。

6.2.2 秘密鍵の複数人制御

本 CA の秘密鍵の生成、管理は、本 CA の鍵の管理を担う複数の要員の合議制操作によって認証設備室にて行われる。

6.2.3 秘密鍵のキーエスクロー（鍵供託）

本 CA は本 CA 及び利用者の秘密鍵の預託を行わない。

6.2.4 秘密鍵のバックアップ

本 CA の秘密鍵のバックアップは、IA 管理者及び IA オペレータが行う。HSM からバックアップされた秘密鍵は、バックアップ用の HSM を個別に用意し、保管される。

6.2.5 秘密鍵の保管

本 CA で使用する秘密鍵のアーカイブを行わない。

6.2.6 暗号モジュールにおける秘密鍵の入出力

本 CA で使用する秘密鍵のコピーは、安全な方法でバックアップ用の HSM へ移送する。バックアップ用の HSM 及びバックアップ用認証業務用設備はバックアップ認証設備室に設置される。災害、障害等により HSM の故障等によりメインサイトによる本 CA の秘密鍵の利用ができなくなった場合、IA 管理者は、認証業務をバックアップ認証設備室の利用に切り替え、バックアップ用の HSM での認証業務の運用を実施する。

6.2.7 暗号モジュールにおける秘密鍵の格納

本 CA の秘密鍵は、FIPS 140-2 レベル 3 規格を満たす HSM 内で生成され、暗号化された上で保存される。本 CA の秘密鍵の生成は、認証設備室内に設置された HSM によって行われる。この秘密鍵の生成操作は、認証設備室内において、本 CA の鍵の管理を担う複数の要員の合議制操作によって行われる。

生成された本 CA の秘密鍵は HSM 内で保管される。

6.2.8 秘密鍵の活性化

本 CA の秘密鍵は、認証設備室内において、本 CA の鍵の管理を担う複数の要員の合議制操作によって活性化される。

6.2.9 秘密鍵の非活性化

本 CA の秘密鍵は、認証設備室内において、本 CA の鍵の管理を担う複数の要員の合議制操作によって非活性化される。

6.2.10 秘密鍵の廃棄

本 CA の秘密鍵の破棄については、以下のとおり行う。

- 本 CA の秘密鍵の破棄は、鍵の使用期間が満了し更新した場合、もしくは本 CA の廃止などを決定した場合に行う。
- 本 CA の秘密鍵の破棄は、CA の鍵の管理を担う複数の要員の相互牽制によって認証設備室にて行われる。
- 本 CA の秘密鍵のバックアップ用の鍵については、本 CA の秘密鍵の破棄に係る作業と合わせて遅延なく破棄される。
- 本 CA の秘密鍵及びバックアップ用の鍵の破棄方法は、本 CPS 5.1.7 項の規定に則り、行う。

6.2.11 暗号モジュールの評価

CP 6.2.11 項に規定のとおり。

6.3 その他鍵ペアに関する管理

6.3.1 公開鍵の保存

CP 6.3.1 項に規定のとおり。

6.3.2 証明書の実運用期間と鍵ペアの使用期間

CP 6.3.2 項に規定のとおり。

6.4 活性化データ

6.4.1 活性化データの生成と設定

本認証サービスで使用される CA の秘密鍵及び全ての活性化データの生成とインストールは別途、事務取扱要領に規定され、実施される。

本認証サービスで使用される利用者の秘密鍵及び PIN コードは以下の方法によって生成及び管理される。

- CP 6.11 項に規定するセキュリティレベル高及び中の暗号モジュールを搭載した利用者自身の持つ端末（スマートフォン等）は、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有する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）を搭載し、当該利用者端末アプリによって、利用者の証明書に対応する秘密鍵と PIN コードの生成指示が送信され、暗号モジュール内で秘密鍵と PIN コードを生成する。なお、生成された PIN コードは、暗号モジュール等内に格納され、格納後、利用者端末アプリから完全に削除される。
- CP 6.11 項に規定するセキュリティレベル基本の機能を備えた利用者自身の持つ端末（スマートフォン等）は、利用者端末アプリを搭載し、当該利用者端末アプリによって、利用者の証明書に対応する秘密鍵と PIN コードの生成指示が送信され、利用者自身の持つ端末（スマートフォン等）内で秘密鍵と PIN コードを生成する。なお、生成された PIN コードは、利用者自身の持つ端末（スマートフォン等）内に格納され、格納後、利用者端末アプリから完全に削除される。

6.4.2 活性化データの保護

本認証サービスで使用される CA の秘密鍵及び全ての活性化データの生成とインストールは、事務取扱要領に規定され、これを遵守することで保護される。

本認証サービスで使用される利用者の秘密鍵と PIN コードは以下の方法によって保護される。

- 利用者の秘密鍵は暗号モジュール等内で安全に保管される。
- 利用者自身のもつ端末（スマートフォン等）にインストールした利用者端末アプリでのみ、暗号モジュール等に対する活性化の要求ができる。
- 暗号モジュール等に対し、PIN コードを 5 回連続で間違えて入力すると、暗号モジュール等が利用不可能になる。

- 利用者は PIN コードを紛失、盗用されないように一切の管理義務を負うものとする。

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 認証業務用設備のセキュリティ管理

6.5.1 認証業務用設備に関する特別なセキュリティ要件

認証業務用設備はファイアウォール及びネットワークベースの侵入検知システム（IDS）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。認証業務用設備で用いる HSM は FIPS140-2 レベル 3 の HSM を用いる。

6.5.2 認証業務用設備のセキュリティ評価

本 CA が導入するハードウェア、ソフトウェアに対しては、事前に導入評価を実施する。また、使用するシステムにおけるセキュリティ上の脆弱性に関する情報収集及び評価を継続的に行い、最新のセキュリティ技術の最新動向を踏まえ、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 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

本 CA のシステムは、導入するハードウェア、ソフトウェアに対しては、事前に導入評価を実施する。本 CA 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、更新前に試験などを行い、互換性を確保する。

6.6.2 セキュリティ運用管理

本 CA のシステムは、十分なセキュリティを確保するために必要な設定が行われる。また、セキュリティレベルに則した入退室管理やアクセス権限管理、同システムのウィルス対策等を実施するとともに、セキュリティ上の脆弱性についての情報収集及び評価を継続的に行い、重大な脆弱性が発見された場合には、速やかに必要な対応を行う。

6.6.3 ライフサイクルのセキュリティ管理

本 CA のシステムの開発、運用、変更、廃棄の各工程において責任者を定め、 作業計画または手順を策定・評価し、必要に応じ試験を行う。また、各作業は記録される。

6.7 ネットワークセキュリティ管理

本 CA のネットワークについては、定期的な評価を実施し、ネットワーク運用において以下の措置を実施する。

- 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・検知するためのファイアウォール及び不正侵入検知システムによる制御・監視
- 認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
- 認証業務用設備を構成するコンピュータへの不正アクセスを防止するための遠隔操作ができない措置

6.8 タイムスタンプ

認証業務用設備は、各種ログに対して正確な時刻を記録するために、タイムサーバによる時間同期を行う。

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

CP 7.1.1 項に規定のとおり。

7.1.2 証明書の拡張

CP 7.1.2 項に規定のとおり。詳細は本 CPS の 11.1 節を参照。

7.1.3 アルゴリズムオブジェクト識別子

CP 7.1.3 項に規定のとおり。

7.1.4 識別名の形式

CP 7.1.4 項に規定のとおり。

7.1.5 識別名の制約

CP 7.1.5 項に規定のとおり。

7.1.6 CP オブジェクト識別子

CP 7.1.6 項に規定のとおり。

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

CP 7.1.8 項に規定のとおり。

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

CP 7.2.1 項に規定のとおり。

7.2.2 CRL と CRL entry 拡張

CP 7.2.2 項に規定のとおり、詳細は本 CPS の 11.2 節を参照。

7.3 OCSP プロファイル

7.3.1 バージョン番号

CP 7.3.1 項に規定のとおり。

7.3.2 OCSP 拡張

CP 7.3.2 項に規定のとおり、詳細は本 CPS の 11.2 節を参照。

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

本 CA は年に一度、或いは PA が必要と判断した時期に、本 CA が CP 及び本 CPS に準拠して認証業務を実施しているか、監査人による監査を受けなければいけない（以下、「準拠性監査」という。）。

PA は、CA に係る CP、CPS に記載されているセキュリティ運用及び手順に従って運用されていることを検証するために、定期的及び周期的なコンプライアンス監査又は検査（以下、「内部監査」という。）を本 CA に要求する権利を有するものとする。

8.2 監査人の資格

本CAの監査を行う監査人は、CA責任者の指定する十分な知識をもった監査人でなければならない。

8.3 監査人と認証機関

監査人は、原則として本 CA の業務とは独立している必要があり、中立性を保つ者とする。

8.4 監査事項

内部監査では、被監査部門が本 CPS 及び、CP を参照する全ての規程等の基準及び手順に則って業務を実施していることを精査する。PA は、内部監査の結果をもとに、被監査部門に対してヒアリング又は業務の改善を要請する。また、PA は、監査人に対して、内部監査に関する報告を実施する。

準拠性監査では、当該報告が適正であることを確認するとともに、本 CA に係る業務が本 CPS 及び、CP を参照する全ての規定等の基準及び手順に則って実施されていることを検証する。監査人が監査する監査事項は、下記の通りとする。

- 本 CA が発行した電子証明書のライフサイクル管理
- IA、RA 及びリポジトリの運用業務
- 本 CA の秘密鍵の管理
- ソフトウェア、ハードウェア及びネットワーク
- 物理的環境及び設備
- 電子証明書の複数枚所持の検査結果
- 内部監査に係る報告

8.5 監査結果の対応

本 CA は、監査人が作成する、準拠性監査に係る報告書（以下、「監査報告書」という。）で指摘された事項に関して、速やかに、下記の改善の措置を行う。

- 軽微な監査指摘事項については、改善するための合理的な是正措置を実施する。また、重要事項又は緊急を要する監査指摘事項については、速やかに対応する。
- CA の秘密鍵が危殆化、又は危殆化が疑われる指摘があった場合は、緊急事態と位置付け、緊急時対応の手続きをとる。

- 重要事項又は緊急を要する監査指摘事項が改善されるまでの間は、本 CA に係る認証業務を継続するか否かは、PA が決定する。
- 本 CA は、監査指摘事項に対して対策を実施したことを確認し、指摘事項に対して実施した改善結果を評価する。
- セキュリティ技術の最新動向を踏まえて、設備及び本規程等の見直しを含む対応措置を実施する。

8.6 監査結果の公開

準拠性監査結果は、監査報告書にて監査人から PA に報告される。PA は監査結果を承認し、その監査結果に係る証明書の有効期間満了後 10 年間保存する。

準拠性監査結果の開示要求については、電子署名法の認定更新時における指定調査機関からの要求、主務官庁からの要求等に対してのみ応じる。

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

本 CA が発行する証明書の発行及び更新料金は発生しないものとする。発行及び更新料金に変更が生じる場合は、CP2.2 節に規定の my FinTech の Web サイト上、あるいは書面等の利用者が適切に確認できる手段により通知する。

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

本 CA が発行する証明書の失効情報参照料金は、利用者及び署名検証者においては発生しないものとする。

9.1.4 その他認証サービスに関連する料金

本 CA に対する開示申請の請求に係る手数料（1 件につき 600 円）は、利用者が負担するものとする。

9.1.5 払戻し方針

本 CA が発行する証明書に関する払戻し方針について、利用者においては規定しない。署名検証者においては、署名検証者毎に書面等の適切に確認できる手段により通知する。

9.2 財務的責任

9.2.1 保険範囲

my FinTech の責任の範囲は以下のとおりである。

- 本 CA が、CP 及び CPS に定める責任に違反したことにより、利用者及び署名検証者に損害を与えた場合には、その損害の賠償責任を負うものとする。ただし、本 CA の責に帰すことができない事由から生じた損害及び逸失利益については、賠償責任を負わないものとする。
- 利用者が CP 及び CPS で定める範囲以外の用途に証明書を使用した結果生じたトラブルについては、利用者が一切の責任を負うものとする。当該トラブルにより本 CA 及び署名検証者に損害を与えた場合、利用者が本 CA 及び署名検証者に対し、損害賠償を行うものとする。
- 利用者が CP 及び CPS で定める失効申請を怠った結果生じたトラブルについては、利用者が一切の責任を負うものとする。該トラブルにより本 CA 及び署名検証者に損害を与えた場合、利用者が本 CA 及び署名検証者に対し、損害賠償を行うものとする。
- 署名検証者が使用目的の範囲を超えて利用者の証明書を使用した結果被った損害については、署名検証者が一切の責任を負うものとする。

9.2.2 その他の資産について

my FinTech は、CP・CPS に定める内容を遵守のうえ本 CA を運営するために、十分な財務的基盤を維持するものとする。また、賠償責任への対応に備えた財務的基盤の維持を行う。

9.2.3 利用者等への保証

my FinTech が損害賠償責任を負う場合、別途定める利用者同意書、署名検証者同意書に定める範囲とする。

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

my FinTech は以下の情報を秘密情報として取り扱う。

- 利用者からの申請情報
- 利用者、署名検証者、その他第三者より受けた問い合わせ情報
- 本 CA のセキュリティに関する情報

9.3.2 秘密情報の対象外事項

my FinTech が保有する情報のうち、以下の情報は秘密情報の範囲外とする。

- 本 CPS 2.2 節で定める公開するものとして定める情報
- my FinTech の責によらず公知となった情報
- my FinTech 以外のものから秘密保持の制限なしに公知となった情報
- 利用者から事前に開示または提供の合意を得た情報

9.3.3 秘密情報の管理責任

本 CA は、施錠された場所に秘密情報を記録した書類やデータを保存し、本認証業務に関わる許可された要員以外がアクセスできないような措置を講じ、秘密情報への不正アクセス又は漏洩を防止する。

9.4 秘密情報の管理責任

9.4.1 個人情報保護の方針

本 CA が保有する個人情報保護の方針は、別途定める「my FinTech 株式会社 my 電子証明書 個人情報取扱要領」に準拠する。

9.4.2 個人情報保護の対象情報

本 CPS において個人情報とは、利用者の証明書の利用申請、失効申請において、利用者から提出された全ての情報及び本 CA にて作成した利用者を特定する情報をいう。また、認証設備室に入室するために登録される生体情報、及び入室時の映像記録も個人情報として取り扱う。

9.4.3 個人情報保護の対象外情報

本 CPS 9.4.1 項及び 9.4.2 項に規定する個人情報を保護する。

9.4.4 個人情報の管理責任

本 CA が保有する個人情報の保護責任は、本 CPS 9.4.1 項に定めるとおりとする。

9.4.5 個人情報の利用に関する説明

本 CA は、利用者からの証明書の申請をもって、利用者が CP、CPS 及び利用規約に同意したものとみなし、利用者から本認証業務上必要とする個人情報の使用の承認を得たものとする。

また、本 CA は、利用者からの証明書の失効申請をもって、当社が別で営む特定認証業務に基づくサービス（以下、「my 認証サービス」という。）についても利用者は失効申請に同意したものと見なし、本認証サービスの受理と同時に my 認証サービスの失効手続きを進めるものとする。

本 CA は、個人情報を本認証業務以外には使用しない。本 CA のネットワークについて、my 認証サービス等との連携を行う際に、サービスの連携に必要なデータ（利用者 ID 等）の提供が行われる場合がある。

本 CA は、利用者からの証明書の申請に係る情報については、利用者の真偽の確認のため、my FinTech の業務委託先に対して開示することがある。この場合、当該委託に関する契約において、当該委託先に対して機密情報及び個人情報の守秘義務を課すものとする。

9.4.6 法的手続による個人情報の開示

本ＣＡで取扱う個人情報に関して、法的根拠に基づく情報の開示要求があった場合、本 CA は法の定めに従って、法執行機関等へ個人情報を開示する。また、本ＣＡは、調停、訴訟、その他法的手続きにおいて、裁判所、弁護士その他の法律上権限を有する者から任意の開示要求があった場合、個人情報を開示することができる。

9.4.7 その他個人情報開示の要件

本 CA は利用者から、権利または利益を侵害され、または侵害される恐れがあると申し出があった場合において、本 CA が有する利用者についての情報を開示しなければならない。

本 CA が利用者から開示申請を受けた場合、本 CA は開示申請を行った利用者の本人確認を行い、正しく確認できた利用者に対してのみ、これまで利用者へ発行したすべての証明書について以下の情報を開示する。

- 利用の申請時に係る情報（申請時の氏名・住所・性別・生年月日・電話番号・利用者 ID）
- 利用者の証明書の記載事項の一部（シリアル番号・証明書の有効開始日・証明書の有効終了日）

開示申請は本 CA が指定する開示申請書にのみよって受け付ける。利用者は本 CA がリポジトリ上で公開する開示申請書をダウンロードすることができる。開示申請書は、郵便にて提出される。

当該開示申請に係る本人確認は以下の方法により行う。

- 開示申請書に記載される氏名、住所、生年月日と証明書の利用申し込み時の氏名、住所、生年月日と一致すること
- 以下の、利用者本人を証明する書類のコピー
  - プラスチック製 IC カードのマイナンバーカード（以下、「マイナンバーカード」という。）の表面のコピー

- 運転免許証の表面及び裏面のコピー
- 運転免許経歴証明書の表面及び裏面のコピー
- 在留カードの表面及び裏面のコピー
- 特別永住者証明書の表面及び裏面のコピー

なお、マイナンバーカード表面のコピーの提出に際して、マイナンバーカードの裏面（マイナンバーカード及び QR コード記載面）のコピーが含まれる場合、マイナンバーカードの裏面のコピーは廃棄を行った上で、申請者に不備の通知を送付する。

また、情報開示にかかる手数料は利用者が負担するものとし、切手または定額小為替証書を同封される。手数料が送付されていない場合も、申請者に不備の通知を送付する。

9.5 知的財産権

次の情報及びデータについての知的財産権を含む全ての権利は、my FinTech に帰属するものとする。

- 本 CA が発行した証明書
- 本 CA がリポジトリ上で公開する証明書の失効情報
- 本 CA の CP、CPS、CP に関連する全ての文書
- 本 CA の秘密鍵及び公開鍵
- 本 CA が利用者に提供する利用者端末アプリ
- 本 CA が利用者に提供する暗号モジュール

9.6 責任と義務

9.6.1 IA の責任と義務

CP 9.6.1 項に規定のとおり。

9.6.2 RA の責任と義務

CP 9.6.2 項に規定のとおり。

9.6.3 利用者の責任と義務

CP 9.6.3 項に規定のとおり。

9.6.4 署名検証者の責任と義務

CP 9.6.4 項に規定のとおり。

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

CP 9.7 節に規定のとおり。

9.8 責任の制限

CP 9.8 節に規定のとおり。

9.9 補償

CP 9.9 節に規定のとおり。

9.10 本規程の効力

9.10.1 本規程の効力有効期間

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

9.10.2 本規程の無効

本 CPS は、本 CPS 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 CPS 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 CPS 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

CP 9.11 節に規定のとおり。

9.12 改訂

9.12.1 改訂手続

本 CA は、PA の指示に基づき、本 CPS の見直しを年 1 回行う。また、適宜、本 CPS 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 CPS 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 CPS 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、その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 CPS 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 CPS の改訂により、OID の変更が必要となるかは PA 管理者が判断し、責任を負うものとする。

9.13 紛争解決手続

本 CPS、CP に関連して生じたすべての訴訟については、東京地方裁判所を管轄裁判所とする。

9.14 準拠法

本 CPS 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 CPS 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 CPS 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 CPS 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。ただし、CP における合意事項との齟齬がある場合には、CP の合意事項が優先される。

9.16.2 権利譲渡条項

CP 9.16.2 項に規定のとおり。

9.16.3 分離条項

本 CPS 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 CP または本 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 CP ないし本 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、CP 及び本 CPS 上の義務の履行が一部または全部遅延した場合には、my FinTech は当該遅延期間について CP 及び本 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 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、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（証明書が有効であることを示す応答） ・ 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 から提供された利用者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。
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。

用語	定義
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 における認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.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）
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）
SSM	ソフトウェアセキュリティモジュール（Software Security Module）

11. 証明書・失効情報等のプロファイル

11.1 証明書のプロファイル

11.1.1 利用者の証明書

利用者の証明書情報は以下となる。なお、以下①②の証明書情報のうち、Not Before（証明書の有効開始日時）については、すべて実際の発行時間より 10 分前に設定される。

①利用者端末アプリにて発行した証明書情報

・電子証明書（基本型）

領域名	値または内容	規定内容
基本部		
Version	0x2	X.509 ver3 の証明書形式バージョンに基づき発行
Serial Number	※証明書のシリアル番号	電子証明書のシリアル番号
Signature Algorithm	1.2.840.10045.4.3.2	証明書の署名暗号アルゴリズム ECDSA-with-SHA256 を使用
Issuer	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者。 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Validity		
Not Before	※証明書の有効開始日時	証明書の有効開始日時
Not After	※証明書の有効終了日時	証明書の有効終了日時

領域名	値または内容	規定内容
Subject	(例) OU=012345678910 G1, (例) CN=Nihontsushin Taro	利用者を識別する情報 OU: 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)を設定する。 CN: 利用者氏名のローマ字を設定する。
Subject Public Key Info		証明書所有者の公開鍵情報
Algorithm	1.2.840.10045.2.1	公開鍵アルゴリズム id-ecPublicKey を使用
Parameters	1.2.840.10045.3.1.7	パラメーター prime256v1
Subject Public Key	※公開鍵値	公開鍵の値

X509v3 Authority Key Identifier (標準拡張領域)

Authority KeyIdentifier		CA の鍵識別子
Key Identifier	※CA の公開鍵のハッシュ値	CA の公開鍵のハッシュ値
Authority Information Access	https://vasign.myfintechtrust.jp/ocsp/	OCSP URI
Certificate Policies		
Policies	1.3.6.1.4.1.56986.1.100.1.1	CP の OID
CPS	https://repository.myfintechtrust.jp/public/index.html	リポジトリの URI
CRL Distribution Points		
Full Name		
URI	https://vasign.myfintechtrust.jp/crl/crl_sign.crl	CRL 配布の URI
CRL Issuer		

領域名	値または内容	規定内容
DirName	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-	
Subject Key Identifier		利用者の鍵識別子
Key Identifier	※利用者の公開鍵のハッシュ値	利用者の公開鍵のハッシュ値
Key Usage	Digital Signature, Non Repudiation	鍵の用途

・電子証明書（属性型）

領域名	値または内容	規定内容
基本部		
Version	0x2	X.509 ver3 の証明書形式バージョンに基づき発行
Serial Number	※証明書のシリアル番号	電子証明書のシリアル番号
Signature Algorithm	1.2.840.10045.4.3.2	証明書の署名暗号アルゴリズム ECDSA-with-SHA256 を使用
Issuer	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者。 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Validity		
Not Before	※証明書の有効開始日時	証明書の有効開始日時

領域名		値または内容	規定内容
	Not After	※証明書の有効終了日時	証明書の有効終了日時
Subject		(例) OU=012345678910 G1, (例) CN=Nihontsushin Taro	利用者を識別する情報 OU: 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)を設定する。 CN: 利用者氏名のローマ字を設定する。
Subject Public Key Info			証明書所有者の公開鍵情報
	Algorithm	1.2.840.10045.2.1	公開鍵アルゴリズム id-ecPublicKey を使用
	Parameters	1.2.840.10045.3.1.7	パラメーター prime256v1
	Subject Public Key	※公開鍵値	公開鍵の値

X509v3 Authority Key Identifier (標準拡張領域)

1.3.6.1.4.1.56986.1.100.100.1	(例)日本通信 太郎	利用者の氏名 姓名の順で表示される。UTF8String で設定する。 JIS 第 1 水準、第 2 水準、補助漢字の範囲での表記とする。
1.3.6.1.4.1.56986.1.100.100.2	(例) 東京都港区虎ノ門四丁目１番２８号	利用者の住所 UTF8String で設定する。
1.3.6.1.4.1.56986.1.100.100.3	(例)20220405	利用者の生年月日 （YYYYMMDD）で表記される。 UTF8String で設定する。 YYYY（西暦年） MM（月） DD（日） ※MM については 1-12, DD については 1-31 までの整数が記載される。

領域名	値または内容	規定内容
Authority KeyIdentifier		CA の鍵識別子
Key Identifier	※CA の公開鍵のハッシュ値	CA の公開鍵のハッシュ値
Authority Information Access	https://vasign.myfintechtrust.jp/ocsp/	OCSP URI
Certificate Policies		
Policies	1.3.6.1.4.1.56986.1.100.1.1	CP の OID
CPS	https://repository.myfintechtrust.jp/public/index.html	リポジトリの URI
CRL Distribution Points		
Full Name		
URI	https://vasign.myfintechtrust.jp/crl/crl_sign.crl	CRL 配布の URI
CRL Issuer		
DirName	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-	
Subject Key Identifier		利用者の鍵識別子
Key Identifier	※利用者の公開鍵のハッシュ値	利用者の公開鍵のハッシュ値
Key Usage	Digital Signature, Non Repudiation	鍵の用途

②ライブラリ対応利用者端末アプリにて発行した証明書情報

・電子証明書（基本型）

領域名	値または内容	規定内容

基本部

Version	0x2	X.509 ver3 の証明書形式バージョンに基づき発行

領域名	値または内容	規定内容
Serial Number	※証明書のシリアル番号	電子証明書のシリアル番号
Signature Algorithm	1.2.840.10045.4.3.2	証明書の署名暗号アルゴリズム ECDSA-with-SHA256 を使用
Issuer	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者。 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Validity		
Not Before	※証明書の有効開始日時	証明書の有効開始日時
Not After	※証明書の有効終了日時	証明書の有効終了日時
Subject	(例) OU=012345678910 L1, (例) CN=Nihontsushin Taro	利用者を識別する情報 OU: 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)を設定する。 CN: 利用者氏名のローマ字を設定する。
Subject Public Key Info		証明書所有者の公開鍵情報
Algorithm	1.2.840.10045.2.1	公開鍵アルゴリズム id-ecPublicKey を使用
Parameters	1.2.840.10045.3.1.7	パラメーター prime256v1
Subject Public Key	※公開鍵値	公開鍵の値

領域名	値または内容	規定内容
X509v3 Authority Key Identifier (標準拡張領域)		
1.3.6.1.4.1.56986.1.100.100.10	(例) V1	証明書バージョン （Ｖ＋バージョン数を表す数字） 2024 年 10 月 2 日よりライブラリ対応利用者端末アプリにて発行された証明書について証明書バージョンをＶ1 として設定する。 証明書のプロファイルに変更が生じる度に、バージョン数を表す数字を 1 ずつ増加させる。
1.3.6.1.4.1.56986.1.100.100.11	(例)mebuku_app	アプリ ID 証明書の発行を申請したライブラリ対応利用者端末アプリを識別するための文字列を設定。
1.3.6.1.4.1.56986.1.100.100.12	certified_id_basic	証明書種別 電子証明書（基本型）を識別するための固定値を設定
Authority KeyIdentifier		CA の鍵識別子
Key Identifier	※CA の公開鍵のハッシュ値	CA の公開鍵のハッシュ値
Authority Information Access	https://vasign.myfintechtrust.jp/ocsp/	OCSP URI
Certificate Policies		
Policies	1.3.6.1.4.1.56986.1.100.1.1	CP の OID
CPS	https://repository.myfintechtrust.jp/public/index.html	リポジトリの URI
CRL Distribution Points		
Full Name		
URI	https://vasign.myfintechtrust.jp/crl/crl_sign.crl	CRL 配布の URI
CRL Issuer		

領域名	値または内容	規定内容
DirName	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-	
Subject Key Identifier		利用者の鍵識別子
Key Identifier	※利用者の公開鍵のハッシュ値	利用者の公開鍵のハッシュ値
Key Usage	Digital Signature, Non Repudiation	鍵の用途

・電子証明書（属性型）

領域名	値または内容	規定内容

基本部

Version	0x2	X.509 ver3 の証明書形式バージョンに基づき発行
Serial Number	※証明書のシリアル番号	電子証明書のシリアル番号
Signature Algorithm	1.2.840.10045.4.3.2	証明書の署名暗号アルゴリズム ECDSA-with-SHA256 を使用
Issuer	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者。 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Validity		
Not Before	※証明書の有効開始日時	証明書の有効開始日時

領域名		値または内容	規定内容
	Not After	※証明書の有効終了日時	証明書の有効終了日時
Subject		(例) OU=012345678910 L1, (例) CN=Nihontsushin Taro	利用者を識別する情報 OU: 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)を設定する。 CN: 利用者氏名のローマ字を設定する。
Subject Public Key Info			証明書所有者の公開鍵情報
	Algorithm	1.2.840.10045.2.1	公開鍵アルゴリズム id-ecPublicKey を使用
	Parameters	1.2.840.10045.3.1.7	パラメーター prime256v1
	Subject Public Key	※公開鍵値	公開鍵の値

X509v3 Authority Key Identifier (標準拡張領域)

1.3.6.1.4.1.56986.1.100.100.1	(例)日本通信 太郎	利用者の氏名 姓名の順で表示される。UTF8String で設定する。 JIS 第 1 水準、第 2 水準、補助漢字の範囲での表記とする。
1.3.6.1.4.1.56986.1.100.100.2	(例) 東京都港区虎ノ門四丁目１番２８号	利用者の住所 UTF8String で設定する。
1.3.6.1.4.1.56986.1.100.100.3	(例)20220405	利用者の生年月日 （YYYYMMDD）で表記される。 UTF8String で設定する。 YYYY（西暦年） MM（月） DD（日） ※MM については 1-12, DD については 1-31 までの整数が記載される。

領域名	値または内容	規定内容
1.3.6.1.4.1.56986.1.100.100.10	(例) V1	証明書バージョン （Ｖ＋バージョン数を表す数字） 2024 年 10 月 2 日よりライブラリ対応利用者端末アプリにて発行された証明書について証明書バージョンをＶ1 として設定する。 証明書のプロファイルに変更が生じる度に、バージョン数を表す数字を 1 ずつ増加させる。
1.3.6.1.4.1.56986.1.100.100.11	(例)mebuku_app	アプリ ID 証明書の発行を申請したライブラリ対応利用者端末アプリを識別するための文字列を設定。
1.3.6.1.4.1.56986.1.100.100.12	certified_id_property	証明書種別 電子証明書（属性型）を識別するための固定値を設定
Authority KeyIdentifier		CA の鍵識別子
Key Identifier	※CA の公開鍵のハッシュ値	CA の公開鍵のハッシュ値
Authority Information Access	https://vasign.myfintechtrust.jp/ocsp/	OCSP URI
Certificate Policies		
Policies	1.3.6.1.4.1.56986.1.100.1.1	CP の OID
CPS	https://repository.myfintechtrust.jp/public/index.html	リポジトリの URI
CRL Distribution Points		
Full Name		
URI	https://vasign.myfintechtrust.jp/crl/crl_sign.crl	CRL 配布の URI
CRL Issuer		

領域名	値または内容	規定内容
DirName	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-	
Subject Key Identifier		利用者の鍵識別子
Key Identifier	※利用者の公開鍵のハッシュ値	利用者の公開鍵のハッシュ値
Key Usage	Digital Signature, Non Repudiation	鍵の用途

11.1.2 CA の証明書

CA の証明書情報は以下となる。

領域名	値または内容	規定内容
基本部		
Version	0x2	X.509 ver3 の証明書形式バージョンに基づき発行
Serial Number	※証明書のシリアル番号	電子証明書のシリアル番号
Signature Algorithm	1.2.840.10045.4.3.2	証明書の署名暗号アルゴリズム ECDSA-with-SHA256 を使用
Issuer	C = JP, O = my FinTech Inc. , OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Validity		
Not Before	※証明書の有効開始日時	証明書の有効開始日時
Not After	※証明書の有効終了日時	証明書の有効終了日時

領域名	値または内容	規定内容
Subject	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の主体者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Subject Public Key Info		証明書所有者の公開鍵情報
algorithm	1.2.840.10045.2.1	公開鍵アルゴリズム id-ecPublicKey を使用
Parameters	1.2.840.10045.3.1.7	パラメーター prime256v1
Subject PublicKey	※公開鍵値	公開鍵の値

X509v3 Authority Key Identifier (標準拡張領域)

Authority Key Identifier		CA の鍵識別子
Key Identifier	※CA の公開鍵のハッシュ値	CA の公開鍵のハッシュ値
Authority Information Access	https://vasign.myfintechtrust.jp/ocsp/	OCSP URI
Certificate Policies		
Policies	1.3.6.1.4.1.56986.1.100.1.1	CP の OID
CRL Distribution Points		CRL 配布ポイント
Distribution Point Name		
Full Name	https://vasign.myfintechtrust.jp/crl/crl_sign.crl	CRL 配布ポイントの URI
CRL Issuer		
DirName		

領域名	値または内容	規定内容
Directory Address	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	CRL 発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Subject Key Identifier		本証明書の鍵識別子
Key Identifier	※本証明書の公開鍵のハッシュ値	本証明書の公開鍵のハッシュ値
keyUsage	Digital Signature, Certificate Sign, CRL Sign	鍵の用途

11.1.3 リンク証明書（NewWithOld）

リンク証明書（NewWithOld）情報は以下となる。

領域名	値または内容	規定内容
基本部		
Version	0x2	X.509 ver3 の証明書形式バージョンに基づき発行
Serial Number	※証明書のシリアル番号	電子証明書のシリアル番号
Signature Algorithm	1.2.840.10045.4.3.2	証明書の署名暗号アルゴリズム ECDSA-with-SHA256 を使用
Issuer	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Validity		
Not Before	証明書（NewWithNew）の Validity.notBefore の日時を設定	証明書の有効開始日時
Not After	証明書（OldWithOld）の Validity.notAfter の日時を設定	証明書の有効終了日時

領域名	値または内容	規定内容
Subject	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の主体者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Subject Public Key Info		証明書所有者の公開鍵情報
algorithm	1.2.840.10045.2.1	公開鍵のアルゴリズム id-ecPublicKey を使用
Parameters	1.2.840.10045.3.1.7	パラメーター prime256v1
subjectPublicKey	※公開鍵値	公開鍵の値

X509v3 Authority Key Identifier (標準拡張領域)

Authority Key Identifier		CA の鍵識別子
keyIdentifier	※OldWithOld の公開鍵のハッシュ値	OldWithOld の公開鍵のハッシュ値
Authority Information Access	https://vasign.myfintechtrust.jp/ocsp/	OCSP URI
Certificate Policies		
Policies	1.3.6.1.4.1.56986.1.100.1.1	CP の OID
CRL Distribution Points		CRL 配布ポイント
Distribution Point Name		
Full Name	https://vasign.myfintechtrust.jp/crl/crl_sign.crl	CRL 配布ポイントの URI
CRL Issuer		
DirName		

領域名	値または内容	規定内容
Directory Address	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	CRL 発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Subject Key Identifier		本証明書の鍵識別子
Key Identifier	※NewWithNew の公開鍵のハッシュ値	NewWithNew の公開鍵のハッシュ値
keyUsage	Digital Signature, Certificate Sign, CRL Sign	鍵の用途

11.1.4 リンク証明書（OldWithNew）

リンク証明書（OldWithNew）情報は以下となる。

領域名	値または内容	規定内容
基本部		
Version	0x2	X.509 ver3 の証明書形式バージョンに基づき発行
Serial Number	※証明書のシリアル番号	電子証明書のシリアル番号
Signature Algorithm	1.2.840.10045.4.3.2	証明書の署名暗号アルゴリズム ECDSA-with-SHA256 を使用
Issuer	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Validity		
Not Before	証明書（OldWithOld）の Validity.notBefore の日時を設定	証明書の有効開始日時
Not After	証明書（OldWithOld）の Validity.notAfter の日時を設定	証明書の有効終了日時

領域名	値または内容	規定内容
Subject	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の主体者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Subject Public Key Info		証明書所有者の公開鍵情報
algorithm	1.2.840.10045.2.1	公開鍵のアルゴリズム id-ecPublicKey を使用
Parameters	1.2.840.10045.3.1.7	パラメーター prime256v1
subjectPublicKey	※公開鍵値	公開鍵の値

X509v3 Authority Key Identifier (標準拡張領域)

Authority Key Identifier		CA の鍵識別子
keyIdentifier	※NewWithNew の公開鍵のハッシュ値	NewWithNew の公開鍵のハッシュ値
Authority Information Access	https://vasign.myfintechtrust.jp/ocsp/	OCSP URI
Certificate Policies		
Policies	1.3.6.1.4.1.56986.1.100.1.1	CP の OID
CRL Distribution Points		CRL 配布ポイント
Distribution Point Name		
Full Name	https://vasign.myfintechtrust.jp/crl/crl_sign.crl	CRL 配布ポイントの URI
CRL Issuer		
DirName		

領域名	値または内容	規定内容
Directory Address	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	CRL 発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Subject Key Identifier		本証明書の鍵識別子
Key Identifier	※OldWithOld の公開鍵のハッシュ値	OldWithOld の公開鍵のハッシュ値
keyUsage	Digital Signature, Certificate Sign, CRL Sign	鍵の用途

11.1.5 VA の証明書

VA の証明書情報は以下となる。

領域名	値または内容	規定内容
基本部		
Version	0x2	X.509 ver3 の証明書形式バージョンに基づき発行
Serial Number	※証明書のシリアル番号	電子証明書のシリアル番号
Signature Algorithm	1.2.840.10045.4.3.2	証明書の署名暗号アルゴリズム ECDSA-with-SHA256 を使用
Issuer	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Validity		
Not Before	※証明書の有効開始日時	証明書の有効開始日時
Not After	※証明書の有効終了日時	証明書の有効終了日時

領域名	値または内容	規定内容
Subject	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の主体者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Subject Public Key Info		証明書所有者の公開鍵情報
algorithm	1.2.840.113549.1.1.1	VA の公開鍵のアルゴリズム RSA を使用
Parameters	05 00	RSA の場合 Null を意味する「05 00」が表示される。
subjectPublicKey	※公開鍵値	VA の公開鍵の値

X509v3 Authority Key Identifier (標準拡張領域)

Authority Key Identifier		CA の鍵識別子
keyIdentifier	※CA の公開鍵のハッシュ値	CA の公開鍵のハッシュ値
Authority Information Access	https://vasign.myfintechtrust.jp/ocsp/	OCSP URI
Certificate Policies		
Policies	1.3.6.1.4.1.56986.1.100.1.1	CP の OID
CRL Distribution Points		CRL 配布ポイント
Distribution Point Name		
Full Name	https://vasign.myfintechtrust.jp/crl/crl_sign.crl	CRL 配布ポイントの URI
CRL Issuer		

領域名			値または内容	規定内容
		DirName		
		Directory Address	C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	CRL 発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
Subject Key Identifier				本証明書の鍵識別子
	Key Identifier		※本証明書の公開鍵のハッシュ値	本証明書の公開鍵のハッシュ値
keyUsage			Digital Signature, Certificate Sign, CRL Sign	鍵の用途

11.2 CRL 及び OCSP のプロファイル

11.2.1 CRL

CRL のプロファイル情報は以下となる。

領域名		値または内容	規定内容
CRL 基本部			
Version		0x1	CRL のフォーマットバージョン番号 Ver.2 を使用
Signature Algorithm		1.2.840.10045.4.3.2	証明書の署名暗号アルゴリズム ECDSA-with-SHA256 を使用
Issuer		C = JP, O = my FinTech Inc., OU = my Digital Certificate-SignCA, CN = my Digital Certificate-Sign-G1	証明書の発行者を識別する情報 C：国名（countryName）を示す。利用者の住所の国を示す。国内住居者のみを対象とするため JP で固定とする。 O：組織名（organizationalName）を示す。本 CA の運営者 OU：組織単位名（organizationalUnitName）を示す。本 CA のサービス名。 CN：一般名（commonname）を示す。本 CA の名称。
thisUpdate		※発行日時	CRL の発行日時
nextUpdate		※更新予定日時	CRL の次回発行予定日時
revokedCertificates			失効された証明書情報
	userCertificate	※証明書 serialNumber	当該証明書の serialNumber
	revocationDate	※失効処理日時	当該証明書の失効日時
	reasonCode	※失効理由コード	当該証明書の失効理由

CRL 拡張領域

authorityKeyIdentifier			CRL 発行者の公開鍵に関する情報
	keyIdentifier	※CA の公開鍵のハッシュ値	CA の公開鍵のハッシュ値
cRLNumber		※CRL 番号	CRL 識別番号

11.2.2 OCSP

OCSP については API にて署名検証者へサービス提供を行う。OCSP のリクエスト及びレスポンス構文は以下となる。

リクエスト構文

項目	値	規定内容
OCSP Request Data		
Version	0x0	プロトコルバージョン 1 を示す
Requestor List		OCSP リクエストの内容を示す
Certificate ID		失効確認したい利用者証明書の情報を示す
Hash Algorithm	SHA1	リクエストで用いるハッシュアルゴリズムの指定を示す
Issuer Name Hash	※CA の証明書の DN のハッシュ値	CA の証明書の DN のハッシュ値を示す
Issuer Key Hash	※CA の公開鍵のハッシュ値	CA の公開鍵のハッシュ値を示す
Serial Number	※利用者の証明書のシリアルナンバ	利用者の証明書のシリアルナンバを示す
Request Extensions		
OCSP Nonce	※ノンス値	リクエストにおけるノンスを示す

レスポンス構文

項目	値	規定内容
OCSP Response Data		
OCSP Response Status	0x0	レスポンスの状態を示す successful (0x0)
Response Type	Basic OCSP Response	レスポンスのタイプを示す
Version	0x0	プロトコルバージョン 1 を示す
Responder Id	※VA の公開鍵に紐づく ID の値	VA の識別情報
Produced At	※日時	レスポンスが生成された時間
Responses		OCSP レスポンスの内容を示す
Certificate ID		失効確認した利用者証明書の情報を示す
Hash Algorithm	SHA1	リクエストで用いるハッシュアルゴリズムの指定を示す
Issuer Name Hash	※CA の証明書の DN のハッシュ値	CA の証明書の DN のハッシュ値を示す
Issuer Key Hash	※CA の公開鍵のハッシュ値	CA の公開鍵のハッシュ値を示す
Cert Status	※good、revoked、unknown の何れかの値	失効情報（good、revoked、unknown）
This Update	※日時	失効情報が更新された時間
Revoked Info		

Revocation Time	※日時	利用者証明書が失効された時間
Response Extensions		
OCSP Nonce	※ノンス値	レスポンスにおけるノンスを示す
Signature Algorithm	1.2.840.113549.1.1.11	レスポンスの署名アルゴリズム sha256WithRSAEncryption