MCS専用認証局

認証業務規程

Version　1.1

株式会社　日本電子公証機構

改訂履歴

Version	変更内容	日付	変更者/作成者	日付	承認者
1.0	初版作成	2017/4/28	大久保	2017/4/28	牛川
1.1	3.2.3 発行審査に関する特記事項を追加 4.2.3 電子証明書申し込みの処理時間の文言を修正	2017/6/1	大久保	2017/6/5	牛川

目次

1. はじめに 8
1.1. 概要 8
1.2. 文書の名前と識別 8
1.3. PKI の関係者 8
1.3.1. 認証局（Medical Care Station CA） 8
1.3.2. 登録局（RA） 9
1.3.3. 発行局（IA） 9
1.3.4. リポジトリ 9
1.3.5. 利用者 9
1.3.6. 依拠当事者 9
1.3.7. その他関係者 9
1.4. 電子証明書の利用方法 9
1.4.1. 適切な電子証明書の利用 9
1.4.2. 禁止される電子証明書の利用 9
1.5. ポリシー管理 9
1.5.1. 文書を管理する組織 10
1.5.2. 連絡先 10
1.5.3. CPS のポリシー適合性を決定する者 10
1.5.4. CPS 承認手続き 10
1.6. 定義と略語 10
2. 公開とリポジトリの責任 12
2.1. リポジトリ 12
2.2. 認証情報の公開 12
2.3. 公開の時期または頻度 12
2.4. リポジトリへのアクセス管理 12
3. 識別および認証 13
3.1. 名前決定 13
3.1.1. 名前の種類 13
3.1.2. 名前の意味に関する要件 13
3.1.3. 利用者の匿名性または仮名性 13
3.1.4. 名前形式を解釈するための規則 13
3.1.5. 名前の一意性 13
3.1.6. 認識、認証および商標の役割 13
3.2. 初回の本人性確認 13
3.2.1. 秘密鍵の所持を証明する方法 13
3.2.2. 組織の認証 13
3.2.3. 個人の認証 14
3.2.4. 確認しない利用者の情報 15
3.2.5. 権限の確認 15
3.2.6. 相互運用の基準 15
3.3. 鍵更新申請時の本人性確認と認証 15
3.3.1. 通常の鍵更新時の本人性確認と認証 15
3.3.2. 電子証明書失効後の鍵更新の本人性確認と認証 15
3.4. 失効請求時の本人性確認と認証 15
4. 電子証明書のライフサイクルに関する運用上要件 16
4.1. 電子証明書発行申請 16
4.1.1. 電子証明書の発行申請を行うことができる者 16
4.1.2. 電子証明書発行申請手続きおよび責任 16
4.2. 電子証明書申請の処理 16
4.2.1. 本人性確認と認証機能の実行 16
4.2.2. 電子証明書発行申請の承認または否認 16
4.2.3. 電子証明書申し込みの処理時間 16

4.3. 電子証明書の発行 16
4.3.1. 電子証明書の発行過程における認証局の行為 16
4.3.2. 利用者に対する認証局による電子証明書の発行通知 17
4.4. 電子証明書の受領 17
4.4.1. 電子証明書の受領確認行為 17
4.4.2. 認証局による電子証明書の公開 17
4.4.3. 第三者に対する電子証明書発行通知 17
4.5. 鍵ペアと電子証明書の用途 17
4.5.1. 利用者の秘密鍵及び電子証明書の使用 17
4.5.2. 依拠当事者による公開鍵および電子証明書の使用 17
4.6. 電子証明書の更新 18
4.7. 電子証明書の鍵更新 18
4.8. 電子証明書の変更 18
4.9. 電子証明書の失効 18
4.9.1. 電子証明書の失効ケース 18
4.9.2. 電子証明書の失効を請求することができる者 19
4.9.3. 失効請求手続き 19
4.9.3.1. 失効請求者 19
4.9.3.2. 失効手続き 19
4.9.4. 失効請求の猶予期間 20
4.9.5. 認証局が失効申請を処理しなければならない時間 20
4.9.6. 依拠当事者の失効調査要求 20
4.9.7. 電子証明書失効リストの発行頻度 20
4.9.8. 電子証明書失効リストの発行最大遅延時間 20
4.9.9. オンラインでの失効/ステイタス確認の適用性 20
4.9.10. オンラインでの失効/ステイタス確認を行うための要件 20
4.9.11. 利用可能な失効通知の他の形式 20
4.9.12. 電子証明書の一時停止（保留） 20
4.9.13. 鍵危殆時の特別要件 20
4.10. 電子証明書のステイタス確認サービス 21
4.11. 加入の終了 21
4.12. キーエスクローと鍵回復 21
5. 設備上、運営上、運用上の管理 22
5.1. 物理的な管理 22
5.1.1. 立地場所および構造 22
5.1.2. 物理的アクセス 22
5.1.3. 電源および空調 22
5.1.4. 水害 22
5.1.5. 火災防止および保護対策 22
5.1.6. 媒体保管場所 22
5.1.7. 廃棄処理 22
5.1.8. 施設外のバックアップ 22
5.2. 手続き的管理 23
5.2.1. 信頼すべき役割 23
5.2.2. 職務ごとに必要される人数 23
5.2.3. 個々の役割に対する本人性確認と認証 23
5.2.4. 職務分割が必要となる役割 23
5.3. 人事的管理 24
5.4. 監査ログの手続き 24
5.4.1. 記録されるイベントの種類 24
5.4.2. 監査ログを確認する頻度 24
5.4.3. 監査ログを保持する期間 24
5.4.4. 監査ログの保護 24
5.4.5. 監査ログのバックアップ手続き 24
5.4.6. 監査ログの収集システム 24

5.4.7. イベントを起こしたサブジェクへの通知 24
5.4.8. 脆弱性評価 25
5.5. 記録の保管 25
5.5.1. アーカイブされる記録の種類 25
5.5.2. アーカイブの保持期間 25
5.5.3. アーカイブの保護 25
5.5.4. アーカイブのバックアップ手続き 25
5.5.5. 記録にタイムスタンプをつける要件 26
5.5.6. アーカイブの収集システム 26
5.6. 鍵の切り替え 26
5.7. 危殆化および災害からの復旧 26
5.7.1. 事故および危殆化の取扱手続き 26
5.7.2. コンピュータの資源または、ソフトウェアデータが破損した場合 26
5.7.3. 利用者の秘密鍵が危殆化した場合の手続き 26
5.8. 認証局の終了 26
6. 技術的セキュリティ管理 28
6.1. 鍵ペアの生成およびインストール 28
6.1.1. 鍵ペアの生成 28
6.1.2. 利用者に対する秘密鍵、公開鍵の交付 28
6.1.3. 依拠当事者に対する認証局の公開鍵交付 28
6.1.4. 鍵サイズ 28
6.1.5. 公開鍵のパラメータ生成および品質検査 28
6.1.6. 鍵用途の目的 28
6.2. 秘密鍵の保護および暗号モジュール技術の管理 28
6.2.1. 暗号モジュールの標準および管理 28
6.2.2. 秘密鍵の"n out of m"による複数人管理 29
6.2.3. 秘密鍵のエスクロー 29
6.2.4. 秘密鍵のバックアップ 29
6.2.5. 秘密鍵のアーカイブ 29
6.2.6. 秘密鍵の暗号モジュールへのまたは暗号モジュールからの転送 29
6.2.7. 暗号モジュールでの秘密鍵格納 29
6.2.8. 秘密鍵の活性化方法 29
6.2.9. 秘密鍵の非活性化方法 29
6.2.10. 秘密鍵の破棄方法 29
6.2.11. 暗号モジュールの評価 29
6.3. その他鍵ペア管理 29
6.3.1. 公開鍵のアーカイブ 29
6.3.2. 電子証明書の運用上の期間および鍵ペアの使用期間 29
6.4. 活性化データ 30
6.4.1. 活性化データの生成およびインストール 30
6.4.2. 活性化データの保護 30
6.4.3. 活性化データの他の考慮点 30
6.5. コンピュータのセキリティ管理 30
6.6. ライフサイクルの技術上の管理 30
6.7. ネットワークセキュリティ管理 30
6.8. タイムスタンプ 30
7. 電子証明書、CRL のプロファイル 31
7.1. 電子証明書のプロファイル 31
7.1.1. バージョン番号 31
7.1.2. 電子証明書の拡張子 31
7.1.3. アルゴリズムのオブジェクト識別子 31
7.1.4. 名前の形式 31
7.1.5. 名前制約 31
7.1.6. 電子証明書ポリシーオブジェクト識別子 31
7.1.7. ポリシー制約拡張子の使用 32

7.1.8. ポリシー修飾子の構文および意味 32
7.1.9. 重要（Critical）とされた電子証明書ポリシー拡張子の処理 32
7.1.10. 有効期間 32
7.2. CRL のプロファイル 32
7.2.1. バージョン番号 32
7.2.2. CRL および CRL エントリ拡張子 32
7.3. OCSP のプロファイル 32
8. 準拠性監査とその他の評価 33
8.1. 評価の頻度または評価が行われる場合 33
8.2. 評価人の身元または資格 33
8.3. 評価人とされるエンティティの関係 33
8.4. 評価で扱われる事項 33
8.5. 不備の結果としてとられる処置 33
8.6. 評価結果の公開 33
9. 他の業務上および法的問題 34
9.1. 料金 34
9.2. 財務上の責任 34
9.3. 秘密情報の保護 34
9.3.1. 秘密として扱う情報の範囲 34
9.3.2. 機密として取り扱わない情報 34
9.3.3. 機密として扱う情報を保護する責任 34
9.4. 個人情報のプライバシー保護 34
9.4.1. 個人情報保護方針 34
9.4.2. 個人情報として取り扱う情報 34
9.4.3. 個人情報とみなされない情報 34
9.4.4. 個人情報を保護する責任 35
9.4.5. 司法手続きまたは行政手続きにもとづく開示 35
9.4.6. その他開示 35
9.5. 知的財産権 35
9.6. 義務と責任 35
9.6.1. 認証局の義務と責任 35
9.6.2. 利用者の義務と責任 35
9.6.3. 依拠当事者の義務と責任 36
9.6.4. 他の関係者の義務と責任 36
9.7. 責任の範囲外 36
9.8. 責任の制限 36
9.9. 補償 36
9.10. 有効期間と終了 37
9.10.1. 有効期間 37
9.10.2. 終了 37
9.10.3. 終了の効果と効力の残存 37
9.11. 関係者間の個別通知と連絡 37
9.12. 改訂 37
9.12.1. 改訂手続き 37
9.12.2. 通知方法および期間 37
9.12.3. オブジェクト識別子が変更されなければならない場合 37
9.13. 紛争の解決 37
9.14. 準拠法 38
9.15. 雑則 38
9.15.1. 完全合意 38
9.15.2. 権利譲渡 38
9.15.3. 分離可能 38
9.15.4. 強制執行 38
9.15.5. 不可抗力 38
9.16. その他条項 38

A.　電子証明書および CRL プロファイル.....39
A.1.　CA 電子証明書プロファイル.....39
A.2.　利用者電子証明書プロファイル.....40
A.3.　CRL プロファイル.....41

1. はじめに

1.1. 概要

本書は株式会社日本電子公証機構（以下「jNOTARY」という）が運営する MCS 専用認証局（以下「本認証局」という）の認証業務規程（Certification Practice Statement、以下「本 CPS」という）です。本 CPS は本認証局が電子証明書の発行、管理、失効及び更新を含む一連のサービスを提供する際に実施する手続を記載したものです。これらのサービスを MCS クライアント認証用電子証明書発行サービス（以下「本サービス」という）と呼びます。本サービスは、株式会社日本エンブレース（以下「エンブレース」という）が運営する医療連携プラットフォームサービス MedicalCareStation（以下「MCS」という）に接続するためのクライアント認証用電子証明書を提供します。

本認証局が発行する電子証明書の利用用途はクライアント認証に制限されます。

なお、本 CPS は、IETF の PKIX WG において標準化されている「電子証明書ポリシーと認証実践の枠組み(Certificate Policy and Certification Practices Framework)」(RFC3647)の構成に従い、記述されています。

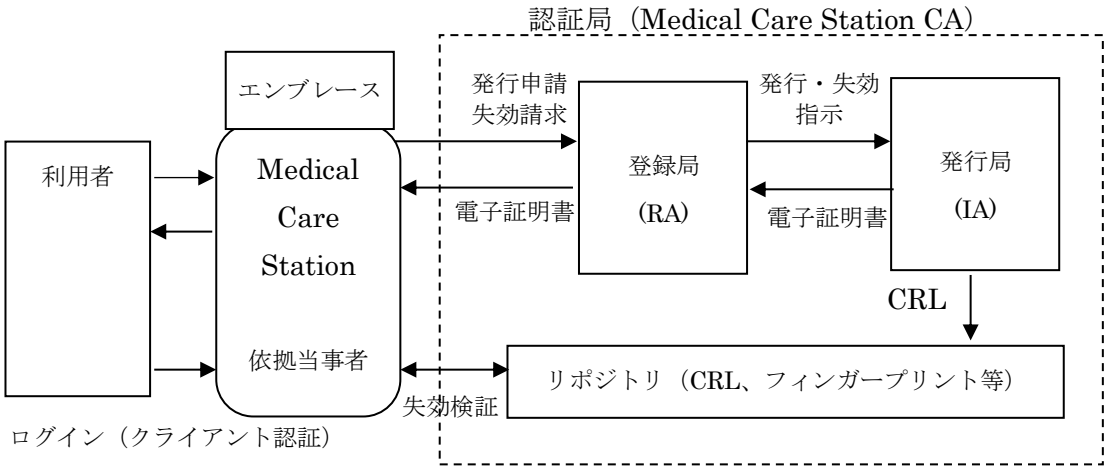
1.2. 文書の名前と識別

本認証局に関連するオブジェクト識別子(OID)は表 1 の通りです。

OID	対象
0.2.440.200148	株式会社日本電子公証機構
0.2.440.200148.1.5	MCS クライアント認証用電子証明書発行サービス
0.2.440.200148.2.2.5	MCS 専用認証局 CPS

1.3. PKI の関係者

以下に本サービスの関係者及びその関係を示します。



1.3.1. 認証局（Medical Care Station CA）

認証局とは、MCS を介して利用者からの電子証明書の発行申請および失効請求を受け付け、必要な審査を行い、電子証明書の発行および失効を行う主体を示します。本認証局は jNOTARY によって運営されます。

1.3.2. 登録局（RA）

本認証局において登録業務はRAによって行われます。RAは、本CPSに従い電子証明書発行申請および失効請求の審査を実施し、IAへの電子証明書の発行指示及び失効指示を行います。

1.3.3. 発行局（IA）

IAはRAからの発行指示および失効指示にもとづいて、電子証明書の発行および失効を行います。また、証明書失効リスト（CRL）の発行を行います。

1.3.4. リポジトリ

本認証局は、利用者、依拠する当事者（証明書検証者、以下「依拠当事者」という）にCRLおよび本CPS等の必要な情報をリポジトリにて公開します。

1.3.5. 利用者

利用者とは、MCSに参加する資格を持ち、MCSを介して本認証局に電子証明書発行を申請し利用する主体をいいます。

利用者は電子証明書に記載された公開鍵の対となる秘密鍵を管理します。

利用者はMCS接続時のクライアント認証のために本認証局が発行した電子証明書を使用します。

1.3.6. 依拠当事者

依拠当事者とは、本認証局が発行した電子証明書を使用して利用者の認証を行います。本サービスにおける依拠当事者は、MCSを運営するエンブレースが相当します。

1.3.7. その他関係者

規定しません。

1.4. 電子証明書の利用方法

本項では本認証局が発行する電子証明書が利用される範囲を規定します。

1.4.1. 適切な電子証明書の利用

本認証局の発行した電子証明書の利用用途を以下に指定します。利用者は指定された用途以外で電子証明書を利用することはできません。

・ 利用者がMCSにログインするためのクライアント認証のための電子証明書

1.4.2. 禁止される電子証明書の利用

本認証局は1.4.1項で規定されている用途以外での電子証明書の利用を禁止します。

1.5. ポリシー管理

本項では本CPS の管理方法について規定します。

1.5.1. 文書を管理する組織

本 CPS の管理部署は以下の通りです。

・組織：株式会社日本電子公証機構

1.5.2. 連絡先

本 CPS および本サービスについてのお問い合わせ先は以下の通りです。

・お問い合わせ先

株式会社日本電子公証機構

〒130-0013

東京都墨田区錦糸二丁目 14 番地 6 号

Tel: 03-5819-3871、Fax: 03-5819-3873

・お問い合わせ時間

営業日：月曜から金曜日（祝日と年末年始の 12 月 30 日～1 月 5 日を除く）

受付時間：午前 10 時から午後 5 時

1.5.3. CPS のポリシー適合性を決定する者

本 CPS のポリシー適合性を決定する者については、9.12 項にて規定します。

1.5.4. CPS 承認手続き

本 CPS の改訂手続きについては、9.12 項にて規定します。

1.6. 定義と略語

電子証明書	電子データの作成者を検証可能とするための電子的な記録。書面の場合の印鑑に相当する。
秘密鍵	公開鍵暗号方式における鍵の対の一方であり、電子署名を作成するために用いられる鍵。
公開鍵	公開鍵暗号方式における鍵の対のもう一方であり、電子署名を復号するために用いられる鍵。
鍵ペア	対になる秘密鍵と公開鍵の組合せ。
認証局	公開鍵基盤に基づき電子証明書の発行管理を行う機関の総称であり、jNOTARY が運営する。主な内部機能として登録局、発行局により構成される。認証局は、本認証業務規程を策定し管理し、検証者が行う MCS クライアント認証用電子証明書の有効性確認のための情報を提供する。
登録局	登録局は、MCS クライアント認証用電子証明書発行申請の受付、発行申請の審査、発行局に対しての電子証明書発行の指示、電子証明書と秘密鍵の利用者への送付、電子証明書の失効決定、発行局に対しての電子証明書失効の指示を実行する。
発行局	発行局は、登録局からの MCS クライアント認証用電子証明書の発行・失効の指示を受けて、電子証明書の発行・失効をする。また、認証局名義の電子証明書および CRL を発行する。
利用者	実際に MCS クライアント認証用電子証明書の発行申請を行い、電子証明書を利用する者。
依拠当事者	利用者の MCS クライアント認証用電子証明書の有効性を検証する者。
危殆化	秘密鍵、ならびに関連する秘密情報が漏洩、滅失又は毀損すること。

jNOTARY	株式会社日本電子公証機構
本認証局	MCS 専用認証局
本 CPS	MCS 専用認証局の認証業務規定
本サービス	MCS クライアント認証用電子証明書発行サービス
エンブレース	株式会社日本エンブレース
MCS	株式会社日本エンブレースが運営する医療連携プラットフォーム「メディカルケアステーション（Medical Care Station）」のこと

2. 公開とリポジトリの責任

2.1. リポジトリ

本認証局は利用者または依拠当事者に関わる情報を提供するためのリポジトリを運営します。リポジトリは、原則として 365 日 24 時間、運用されます。ただし、システム保守等を実施する場合には予め告知した上でリポジトリの運用を一時停止することがあります。なお、災害あるいは障害等の緊急時には事前に告知することなくリポジトリを停止することがあります。

2.2. 認証情報の公開

本認証局はリポジトリにおいて、以下の情報を公開します。

リポジトリ URL：https://mcs.jnotary.com/

1). 認証業務規程（本 CPS）
2). 電子証明書失効情報（CRL）
3). CA 電子証明書
4). CA 電子証明書のフィンガープリント
5). 本サービスに関するお知らせ等

2.3. 公開の時期または頻度

1). 認証業務規程（本 CPS）
改訂の都度
2). 電子証明書失効情報（CRL）
168 時間（7 日）毎
3). CA 電子証明書
更新の都度
4). CA 電子証明書のフィンガープリント
更新の都度
5). 本サービスに関するお知らせ等
必要に応じて随時

2.4. リポジトリへのアクセス管理

本認証局は、リポジトリで公開する情報の参照についてはアクセス制限を行いません。

3. 識別および認証

3.1. 名前決定

本項では電子証明書に記載される名称について規定します。

3.1.1. 名前の種類

本認証局が発行する電子証明書の発行者名はX.500識別名の形式に従って設定されます。

3.1.2. 名前の意味に関する要件

本認証局は、電子証明書に記載される主体者名（CN:CommonName）に反映される名前として、MCS 会員を一意に特定できる ID（以下「MCSID」という）を用いるものとします。

3.1.3. 利用者の匿名性または仮名性

本認証局が発行する電子証明書に記載する名前はMCSIDであるため、利用者の氏名に関する情報は記載されません。

3.1.4. 名前形式を解釈するための規則

電子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

本認証局は一人の利用者に複数の電子証明書を発行可能としています。
そのため、名前の一意性については規定しません。

3.1.6. 認識、認証および商標の役割

本認証局では、電子証明書に記載する利用者の識別名をMCSIDとするため、利用者の識別名に商標を含むことを想定していません。

3.2. 初回の本人性確認

本項では、電子証明書を発行する際の認証ポリシーについて規定します。

3.2.1. 秘密鍵の所持を証明する方法

本認証局が鍵ペアを生成し利用者に配布するため、利用者による秘密鍵の所持の証明は行いません。

3.2.2. 組織の認証

利用者はMCSへの参加資格を持つ者でなければなりません。
本認証局では、MCSを介して利用者からの申請情報を受け取ることで、上記資格を持つ者であること、および申請の意思を確認します。また、エンブレースは電子証明書発行の

ため、申請を行った利用者に関する以下の情報（以下、「申請情報」という）を本認証局に提出しなければなりません。

・MCSID
・氏名
・メールアドレス（PIN コード通知用）
・その他、本認証局が必要と認める情報

3.2.3. 個人の認証

1). 申請対象者

MCS の参加資格を持つ者。

本認証局は、代理人による申請を認めません。

2). 申請方法

利用者自身が MCS の電子証明書発行申請サービスより行う。

本認証局は上記以外の方法による申請を認めません。

3). 提出書類

申請時に必要な書類は以下とする

	必要な書類	補足
1 点でよいもの	・運転免許証 ・パスポート ・住民基本台帳カード（写真付き）	写真及び氏名等の文字情報が鮮明で判別できること
2 点必要なもの	・健康保険証 ・医療機関等、利用者の所属する組織が発行した顔写真入りの ID カード、入館証等	

・ 利用者は上記の書類を画像ファイルとして、電子証明書発行申請時に添付して MCS に提出します。
・ 本認証局はエンブレースから利用者の申請情報と上記の書類の提出を受け、電子証明書の発行審査（利用者の本人確認を含む）を行います。

4). 審査方法

①.必要な申請情報が揃っていることの確認
②.必要な書類が提出されていることの確認
③.提出された書類が判別可能であることの確認
④.提出された書類が有効期限内であることの確認
（有効期限が記載されている書類の場合）
⑤.提出された書類の記載事項と申請情報に相違がないことの確認
確認する項目
・氏名

■発行審査についての特記事項

発行審査については、事前に本認証局とエンブレースとの間で合意があれば、3.2.3.4) に規定されていない審査を実施することがあります。

その際の審査方法については、事務取扱要領で規定します。

5). 審査結果

本認証局では、申請情報および提出書類について 3.2.3.4)の①～⑤に従って電子証明書発行申請の審査を行います。

①.疑義が生じた場合

審査結果を「不承認」とする。

②.疑義が生じなかった場合

審査結果を「承認」とする。

利用者は MCS のサービスに接続し MCS を介して審査結果を確認します。審査結果が不承認の場合、利用者は不承認の理由を確認し、改めて発行申請と必要書類を提出する必要があります。

3.2.4. 確認しない利用者の情報

本認証局は、利用者の氏名、利用者の実在確認以外の確認は行いません。

3.2.5. 権限の確認

規定しません。

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と認証

本項では電子証明書の更新申請時に行われる認証手続きについて規定します。

3.3.1. 通常の鍵更新時の本人性確認と認証

本認証局は、電子証明書の有効期間が満了時にのみ適用される特別な規定を定めません。電子証明書の有効期間が満了する場合、 利用者は 3.2 項の規定にしたがい、新たな電子証明書発行の申請を行います。

3.3.2. 電子証明書失効後の鍵更新の本人性確認と認証

本認証局は、電子証明書の失効時にのみ適用される特別な規定を定めません。何らかの理由により電子証明書が失効された場合、 利用者は 3.2 項の規定にしたがい、新たな電子証明書発行の申請が行えます。

3.4. 失効請求時の本人性確認と認証

本認証局は以下の規定に従い、電子証明書の失効請求に関する認証を行います。

1). 失効請求者と事由

電子証明書の失効が必要となるケース、および各々のケースにおける失効の依頼者の制約条件等については、4.9.1 項および 4.9.2 項の規定に従います。

2). 失効の請求方法

本認証局はMCSからの失効請求、本認証局自身の失効請求により失効を行います。
本認証局は上記以外の失効請求を認めません。

3). 失効請求の審査

本認証局は、失効請求に対して審査を行います。

4). 審査方法

失効請求に必要な情報（失効理由を含む）が揃っていることの確認
MCSもしくは本認証局からの請求であることの確認
対象の電子証明書が有効期間内であることの確認

4. 電子証明書のライフサイクルに関する運用上要件

4.1. 電子証明書発行申請

本項では電子証明書の発行申請について規定します。

4.1.1. 電子証明書の発行申請を行うことができる者

MCSへの参加資格を持つ者。

4.1.2. 電子証明書発行申請手続きおよび責任

電子証明書発行申請を行う者はMCSの提供する電子証明書発行申請サービスより申請を行わなければなりません。
本認証局は、上記以外の発行申請を認めません。
また利用者は発行申請を行う前に、本CPSに同意する必要があります。

4.2. 電子証明書申請の処理

4.2.1. 本人性確認と認証機能の実行

本認証局は、MCSから提供された利用者の申請情報、提出書類をもとに電子証明書発行の審査を行います。
審査方法については、3.2.3.4).に規定します。

4.2.2. 電子証明書発行申請の承認または否認

電子証明書発行申請の審査結果を登録します。
利用者はMCSを介して、発行申請の審査結果を確認します。
審査方法および審査結果については、3.2.3.4).に規定します。

4.2.3. 電子証明書申し込みの処理時間

本認証局は発行申請を受け付け発行申請の審査を行い、審査結果を登録します。審査により電子証明書の発行が承認された場合、申請受付の翌日から3営業日以内に電子証明書の発行を行います。

4.3. 電子証明書の発行

4.3.1. 電子証明書の発行過程における認証局の行為

電子証明書の発行が承認された場合、本認証局は電子証明書発行に必要な情報の登録を行い、電子証明書を発行します。作成された電子証明書は本認証局の外部から直接アクセスできない環境で保管します。

4.3.2. 利用者に対する認証局による電子証明書の発行通知

本認証局は利用者に対して、主体的に電子証明書の発行通知を行いません。

利用者はMCSを介して電子証明書が発行されたことを確認することができます。電子証明書発行が確認できた場合、利用者はMCS経由で電子証明書のダウンロードを行います。

本認証局は電子証明書のインストールに必要なPIN番号をメールもしくはSMSで利用者に通知します。

4.4. 電子証明書の受領

4.4.1. 電子証明書の受領確認行為

利用者は電子証明書をダウンロードした後、4.3.2項のメールのPIN番号を使用して電子証明書のインストールを行います。

電子証明書のインストール後、利用者は電子証明書が正しくインストールできたこと、電子証明書の内容に誤りがないことを確認しなければなりません。

電子証明書が正しくインストールできなかった場合、あるいは電子証明書の記載内容が正しくない場合、MCSを介して本認証局にその旨を通知しなければなりません。

4.4.2. 認証局による電子証明書の公開

本認証局は利用者の電子証明書の公開を行いません。

4.4.3. 第三者に対する電子証明書発行通知

本認証局は第三者に対して主体的に電子証明書の発行通知を行いません。

ただし、エンブレースはMCSを介して電子証明書の発行有無を確認することができます。

4.5. 鍵ペアと電子証明書の用途

4.5.1. 利用者の秘密鍵及び電子証明書の使用

利用者は、1.4項で規定され許可された用途にのみ、電子証明書および秘密鍵を利用することができます。利用者は、自らの秘密鍵を適切に管理しなければならず、電子証明書の有効期間が満了した場合、または電子証明書が失効された場合は、当該電子証明書および秘密鍵を利用してはなりません。

4.5.2. 依拠当事者による公開鍵および電子証明書の使用

依拠当事者は、本認証局で発行された電子証明書を信頼し利用するにあたって、以下の事項を確認する義務を負います。

1). 依拠当事者は電子証明書の利用目的、使用範囲を理解し承認しなければなりません。

2). 依拠当事者は、本認証局の CA 公開鍵を用いて利用対象となる電子証明書に施された電子署名を検証することにより、当該電子証明書が本認証局により発行されていることを確認しなければなりません。

3). 依拠当事者は、リポジトリに掲載された CA 電子証明書のフィンガープリントを確認し、本認証局の CA 電子証明書であることを確認しなければなりません。

4). 依拠当事者は、CA 電子証明書が有効期間内であることを確認しなければなりません。

5). 依拠当事者は、利用対象となる電子証明書が、有効期間内であることを確認しなければなりません。

6). 依拠当事者は、CRL を取得し、利用対象となる電子証明書が失効されていないことを確認しなければなりません。

4.6. 電子証明書の更新

本サービスでは、電子証明書の発行を受けた利用者が電子証明書の更新を希望する場合、新たに電子証明書を発行することで対応します。

4.7. 電子証明書の鍵更新

本サービスでは、電子証明書の発行を受けた利用者が鍵ペアの更新を希望する場合、新規に電子証明書を発行することで対応します。

発行済み電子証明書の有効期間が満了になっていなければ、利用者は当該電子証明書の失効を行わなければなりません。

4.8. 電子証明書の変更

本サービスでは、電子証明書の発行を受けた利用者が電子証明書の変更を希望する場合、新規に電子証明書を発行することで対応します。

発行済み電子証明書の有効期間が満了になっていなければ、利用者は当該電子証明書の失効請求を行わなければなりません。

4.9. 電子証明書の失効

本項では電子証明書の失効の手続きについて規定します。

4.9.1. 電子証明書の失効ケース

1). 利用者による事由

- 利用者の秘密鍵が危殆化した、もしくはその恐れがある場合
- 利用者がデバイスを変更した場合
- 利用者が MCS を退会する場合
- 電子証明書の記載事項に変更が生じた、または誤りがある場合
- 何らかの理由により利用者が正常に電子証明書をインストールできなかった場合
- 何らかの理由により利用者が電子証明書の利用を中止したい場合

2). エンブレースによる事由

- 利用者の秘密鍵が危殆化した、もしくはその恐れがある場合

・ 利用者がMCSを退会した場合
・ 利用者が死亡した場合
・ エンブレースが利用者のMCSへの参加資格を取り消した場合
・ エンブレースがMCSを終了した場合
・ 何らかの理由によりエンブレースが電子証明書の失効を必要と判断した場合

3). 本認証局による事由
・ 利用者の秘密鍵が危殆化した、もしくはその恐れがある場合
・ 電子証明書の記載事項に誤りがある場合
・ 何らかの理由により利用者が正常に電子証明書をインストールできなかった場合
・ 利用者が電子証明書発行後、一定期間電子証明書をダウンロードしなかった場合
・ 何らかの理由により利用者が正常に電子証明書をインストールできなかった場合
・ 利用者が本CPS で規定する用途以外で電子証明書を使用した場合
・ 利用者が電子証明書インストール前にPIN番号を紛失した場合
・ 認証局秘密鍵が危殆化した、もしくはその恐れがある場合
・ 本サービスを終了する場合

4.9.2. 電子証明書の失効を請求することができる者

電子証明書の失効請求ができる者は以下の通りとします。

1). 利用者

4.9.1.1).項の事由に相当する場合

利用者はMCS（エンブレース）に対して失効請求を行い、本認証局はエンブレースから失効請求を受け取ります。

2). エンブレース

4.9.1.2).項の事由に相当する場合

3). 本認証局

4.9.1.3).項の事由に相当する場合

4.9.3. 失効請求手続き

4.9.3.1.失効請求者

1). 利用者

MCSの電子証明書失効請求サービスから失効請求を行う。

2). エンブレース

エンブレースからMCSを介して本認証局へ失効請求を行う。

この場合、利用者への事前の通知を行わず利用者の電子証明書を失効します。

3). 本認証局

本認証局の認証局責任者による指示。

4.9.3.2.失効手続き

3.4 項の規定に従い失効請求の審査を行い、失効請求が承認された場合、直ちに電子証明書の失効を行います。

4.9.4. 失効請求の猶予期間

4.9.2 項に規定された者は、 4.9.1 項の失効事由に該当したことに気付いた場合、 遅滞無く本認証局に失効の請求を行わなければなりません。

4.9.5. 認証局が失効申請を処理しなければならない時間

本認証局は、原則として本認証局の業務時間内において、失効に関する処理を遅滞無く実施します。当該処理の内容には、失効依頼の受け付け、審査と承認、およびシステムへの登録作業等が含まれます。

4.9.6. 依拠当事者の失効調査要求

依拠当事者は、電子証明書に依拠する前に当該電子証明書が失効されていないことを調査しなければなりません。本サービスにおいては、電子証明書の失効に関する情報は CRL に記録され、リポジトリにて公開されます。

なお、本認証局は、有効期間の満了した電子証明書の情報についてのお問合せには応じません。

4.9.7. 電子証明書失効リストの発行頻度

本認証局は CRL を 1 週間に 1 回以上の頻度で更新します。

4.9.8. 電子証明書失効リストの発行最大遅延時間

規定しません。

4.9.9. オンラインでの失効/ステイタス確認の適用性

本認証局は、オンラインによる失効情報の提供を行いません。

4.9.10. オンラインでの失効/ステイタス確認を行うための要件

規定しません。

4.9.11. 利用可能な失効通知の他の形式

規定しません。

4.9.12. 電子証明書の一時停止（保留）

本認証局は、電子証明書の一時停止（一時保留）を行いません。

4.9.13. 鍵危殆時の特別要件

1). 利用者の秘密鍵危殆時

本認証局では、利用者の秘密鍵が危殆化したことを発見した場合、またはそう信じるに足る合理的な理由がある場合、当該電子証明書を失効し CRL に掲載します。

MCS は当該秘密鍵を管理する利用者の電子証明書が失効されことを確認できます。

2). 本認証局の秘密鍵危殆時

本認証局は、認証局自身の秘密鍵が危殆化した場合、または危殆化した恐れがある場合、認証局責任者の判断により本認証局のサービスを停止し、直ちに利用者と認証局電子証明書を失効します。電子証明書の失効及び CRL の登録を完了した後、CA 秘密鍵を直ちに廃棄します。

4.10. 電子証明書のステイタス確認サービス

本認証局では、電子証明書の失効について、CRL により情報提供を行います。

4.11. 加入の終了

MCS への参加資格を失った利用者は、発行されている有効な電子証明書を失効する必要があります。失効については、MCS（エンブレース）から失効請求されるものとします。

4.12. キーエスクローと鍵回復

本認証局の生成した秘密鍵はすべて、キーエスクローの対象とはしません。

5. 設備上、運営上、運用上の管理

5.1. 物理的な管理

5.1.1. 立地場所および構造

本認証局は、火災、水害、自身等による災害の被害を受ける恐れの少ない場所に設置し、災害対策を講じます。また、サービスに利用する機器、設備類を災害、不正侵入から防護された安全な場所に設置します。

5.1.2. 物理的アクセス

本認証局の認証設備はデータセンターに設置します。データセンターへの入館および認証設備室への入室は、データセンターの規定に従い、入退館および入退室が管理・記録されています。データセンターにするためには、事前に入館申請が必要であり、入館申請には業務責任者もしくは設備責任者の承認が必要となります。

5.1.3. 電源および空調

本認証局はシステム運用のために充分な要領の電源を確保し、UPS 等を設置し災害発生時の緊急電源の確保に努めます。

5.1.4. 水害

本認証局で利用する設備の設置場所は水害防止等の措置を講じます。

5.1.5. 火災防止および保護対策

本認証局で利用する設備の設置場所は、消火器等を設置し火災防止等の措置を講じます。

5.1.6. 媒体保管場所

アーカイブデータ、バックアップデータは鍵付きのロッカーに保管します。ロッカーの鍵は認証局責任者が管理し、鍵の貸し出しは管理簿により管理されます。

5.1.7. 廃棄処理

本サービスに関連する文書、機器、媒体等を破棄する場合、次の通りとします。

1). 文書

断裁して破棄、もしくは溶解します。

2). 機器

ハードディスクを初期化します。

3). 媒体

物理的に破壊して破棄します。

5.1.8. 施設外のバックアップ

規定しません。

5.2. 手続き的管理

5.2.1. 信頼すべき役割

本認証局は、本認証局の業務を適切に実施するために必要な運用体制を構築します。本認証局の運用体制は、個々の職務内容および責任を定め、各担当者の権限（システムへのアクセス）および指揮命令系統を規定します。

本認証局の業務を実施する担当者の職務は以下の通りです。

1). 認証局責任者

- 認証局運営全体統括
- 認証業務従事者の選任・配置

2). 業務責任者

- RA 業務統括
- RA 業務担当者の業務管理および、RA 業務の承認
- IA 業務統括
- IA 業務担当者の業務管理および、IA 業務の承認

3). RA 業務担当者

- RA 業務（発行申請および失効請求の審査）実施

4). IA 業務担当者

- IA 業務（電子証明書発行および失効）実施
- CRL 発行実施

5). 設備責任者

- 本認証局（RA および IA）の業務用設備（ハードウエアおよびソフトウエア）のセキュリティ維持管理
- 設備担当者の作業内容承認

6). 設備担当者

- RA および IA 業務用設備（ハードウエアおよびソフトウエア）の設定、変更および維持管理

5.2.2. 職務ごとに必要される人数

各担当者は最低 1 名とし、原則として各職務の兼任は行わないこととします。

5.2.3. 個々の役割に対する本人性確認と認証

電子証明書発行（失効）業務の実施者には、各個人にアクセスに必要な ID、パスワードを割り振り、これにより認証を行う。

ID、パスワードの設定は設備担当者が実施し、同時に職務に応じた権限も設定する。

5.2.4. 職務分割が必要となる役割

以下の業務については、権限分離と相互牽制の観点から複数人の体制で実施する。

RA 業務

- 発行審査およびその承認
- 失効審査およびその承認

IA 業務

・ 電子証明書発行指示、およびその承認
・ 電子証明書失効指示、およびその承認

5.3. 人事的管理

本サービスに関わる要員の任命、教育、配置転換等については、jNOTARY の内部規程に基づいて運用します。また、すべての要員には、運営を行うために必要な知識及び技術を習得するための教育訓練を行います。

5.4. 監査ログの手続き

5.4.1. 記録されるイベントの種類

本認証局は以下のものを監査用記録として取得し保管します。

・ 電子証明書の発行および失効に関わる記録
・ 電子証明書の発行および失効に関わるシステムの操作記録
・ 認証設備システムへの不正アクセスの記録
・ 認証設備システムの動作記録
・ 認証設備システムのメンテナンス作業に関する記録

5.4.2. 監査ログを確認する頻度

監査ログの確認は適切と考えられる頻度で定期的に実施します。

5.4.3. 監査ログを保持する期間

電子証明書の発行および失効に関する記録は、電子証明書の有効期間満了日から 1 年間保持します。

上記以外の記録については、最低 1 年間保持することとします。

5.4.4. 監査ログの保護

本認証局は、各監査ログについて、改ざん、破壊、漏えいが行われないよう厳重に保管します。

5.4.5. 監査ログのバックアップ手続き

本認証局は、システム内で管理している各種ログについて必要と判断したものは、適切な手順を定め、これに従いバックアップを作成し保存します。

5.4.6. 監査ログの収集システム

各種記録については、システムによる自動処理もしくは本認証局担当者による手作業により収集します。

5.4.7. イベントを起こしたサブジェクへの通知

本認証局では、各記録の確認時に調査の必要性がある事象を検出した場合、当該事象の発

生者に通知なく調査を行う場合があります。

5.4.8. 脆弱性評価

規定しません。

5.5. 記録の保管

5.5.1. アーカイブされる記録の種類

本認証局では以下のデータおよび記録を保存します。

業務関連

・ 電子証明書の発行申請および失効請求の情報、およびその添付資料
・ 電子証明書の発行申請および失効請求の審査、承認等、実施についての記録
・ 本認証局の認証局電子証明書、およびその作成、管理に関する記録
・ 業務実施に関わる記録で本認証局が必要と途判断した記録

組織関連

・ 本 CPS、およびその改訂に関する記録
・ 本認証局の業務実施の手順等を記した文書、およびそれらの改訂に関する記録
・ 本認証局の組織体制に関わる文書、およびそれらの改訂に関する記録
・ 利用者および依拠当事者に関する規約、およびそれらの改訂に関する記録
・ 監査に関わる記録
・ 本認証局の運営に関わる記録で本認証局が必要と途判断した記録

設備関連

・ システム動作に関する記録
・ システム、設備の保守および変更に関する記録
・ 各システムのアカウントおよび権限の追加、変更、削除に関する記録
・ 障害および事故に関する発生および対応の記録
・ 本認証局の設備に関わる記録で本認証局が必要と判断した記録

5.5.2. アーカイブの保持期間

業務関連

・ 当該記録に関わる利用者の電子証明書有効期間の満了日から 1 年間

組織関連

・ 作成もしくは改訂から 1 年間

設備関連

・ 次回の監査まで

5.5.3. アーカイブの保護

本認証局は取得したデータもしくは書類について、漏えい、破壊、改ざん、などが発生しないように管理します。

5.5.4. アーカイブのバックアップ手続き

本認証局は、バックアップが必要と判断したデータについて、適切なバックアップ手順を定め、これに従い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

本認証局は、データのバックアップに際して必要と判断したアーカイブにタイムスタンプを付与します。

5.5.6. アーカイブの収集システム

各種記録については、システムによる自動処理もしくは本認証局担当者による手作業により収集することとします。

5.6. 鍵の切り替え

規定しません。

5.7. 危殆化および災害からの復旧

5.7.1. 事故および危殆化の取扱手続き

災害及び危殆化等により、本サービスの中断、提示につながるような問題が発生した場合、本認証局は本サービスの提供を停止し、被害状況及び原因の調査を行います。

5.7.2. コンピュータの資源または、ソフトウェアデータが破損した場合

システム障害、データの破損が発生し本サービスの提供が困難と思われる問題が発生した場合、本認証局は本サービスの提供を停止し、被害状況及び原因の調査を行います。

5.7.3. 利用者の秘密鍵が危殆化した場合の手続き

利用者は、自身の秘密鍵が危殆化した場合、遅滞なく本認証局に当該電子証明書の失効請求を行わなければなりません。電子証明書の失効請求を受け取った場合、本認証局は適切な審査を実施し、当該電子証明書を直ちに失効します。利用者は MCS を介して電子証明書を失効したことを確認できます。

5.7.4. 災害後の事業継続能力

規定しません

5.8. 認証局の終了

本認証局は、災害等による不測の事態の発生により業務の不履行に至った場合、jNOTARY の事業方針の変更などの場合に本サービスを終了します。

1). 発行済み電子証明書の失効処理方法

認証業務の廃止日迄に、本認証局によって発行された全ての利用者の電子証明書を失効し、失効通知を行います。

2). 利用者への連絡方法、連絡時期等

業務終了の少なくとも 60 日前から本認証局のリポジトリに業務終了の案内を掲載する

と共に、全ての利用者に 60 日前までに何らかの方法（メール、MCS のお知らせ、郵送等）で利用者に通知します。

3). 廃止後の失効情報の公開

失効に伴い本認証局は CRL を更新し、リポジトリに 1 年間公開します。

4). 認証局秘密鍵の処理

本認証局の秘密鍵及びバックアップされた本認証局の秘密鍵全てを復元不可能とします。

6. 技術的セキュリティ管理

6.1. 鍵ペアの生成およびインストール

6.1.1. 鍵ペアの生成

本認証局の CA 鍵ペアは、認証設備室内において、本サービスに関わる複数人の立会いのもと作成するものとします。

6.1.2. 利用者に対する秘密鍵、公開鍵の交付

利用者に対する鍵ペアは認証設備室内において、複数人の承認を経て自動的に生成されます。利用者は指定された方法で MCS を介して秘密鍵を含む電子証明書のダウンロード行います。電子証明書を活性化するための PIN コードは本認証局から利用者にメールまたは SMS で通知します。

6.1.3. 依拠当事者に対する認証局の公開鍵交付

本認証局の公開鍵は CA 電子証明書に記載され、リポジトリにおいて公開します。

6.1.4. 鍵サイズ

・本認証局

2048 ビットの RSA

・利用者

2048 ビットの RSA

6.1.5. 公開鍵のパラメータ生成および品質検査

規定しません。

6.1.6. 鍵用途の目的

本認証局は鍵ペアを以下の目的のために利用します。

・本認証局の CA 電子証明書への署名

・利用者の電子証明書への署名

・CRL への署名

6.2. 秘密鍵の保護および暗号モジュール技術の管理

本項では本認証局の秘密鍵保護方法について規定します。

利用者の秘密鍵保護については規定しませんが、利用者は自身の責任により秘密鍵を管理する必要があります。

6.2.1. 暗号モジュールの標準および管理

本認証局では暗号モジュールを使用しません。

本認証局の認証局秘密鍵は外部から容易にアクセスできない環境で厳重に保管されます。

6.2.2. 秘密鍵の"n out of m"による複数人管理

本認証局の認証局秘密鍵は、認証局責任者を含む複数の者が立ち会いのもと、活性化を行うこととします。

6.2.3. 秘密鍵のエスクロー

本認証局が管理する全ての秘密鍵はエスクローの対象とはなりません。

6.2.4. 秘密鍵のバックアップ

本認証局のバックアップは、認証設備室内において権限を有する担当者により行われ外部からアクセスできない安全な環境に保管します。

6.2.5. 秘密鍵のアーカイブ

本認証局は認証局秘密鍵のアーカイブを行いません。

6.2.6. 秘密鍵の暗号モジュールへのまたは暗号モジュールからの転送

本認証局では暗号モジュールを使用しません。

6.2.7. 暗号モジュールでの秘密鍵格納

本認証局では暗号モジュールを使用しません。

6.2.8. 秘密鍵の活性化方法

6.1.1 で規定しています。

6.2.9. 秘密鍵の非活性化方法

規定しません。

6.2.10. 秘密鍵の破棄方法

規定しません。

6.2.11. 暗号モジュールの評価

本認証局では暗号モジュールを使用しません。

6.3. その他鍵ペア管理

6.3.1. 公開鍵のアーカイブ

本認証局の認証局電子証明書については、本サービスの提供中は認証局内で保管します。利用者の電子証明書については、有効期間満了後 1 年は保管します。

6.3.2. 電子証明書の運用上の期間および鍵ペアの使用期間

規定しません。

6.4. 活性化データ

6.4.1. 活性化データの生成およびインストール

本認証局の秘密鍵の活性化については、6.2.2 項で規定しています。

利用者の秘密鍵については規定しません。

6.4.2. 活性化データの保護

規定しません。

6.4.3. 活性化データの他の考慮点

規定しません。

6.5. コンピュータのセキリティ管理

本認証局は、認証業務に使用するシステムのハードウェア、ソフトウェア等について、最新のセキュリティ技術の動向を踏まえ、必要に応じてパッチ適用を含む適切な対応を行います。

6.6. ライフサイクルの技術上の管理

規定しません。

6.7. ネットワークセキュリティ管理

本認証局は、認証業務に関わるネットワークについては、暗号通信路（SSL を含む)、ファイアウォール等の技術を導入し適切なセキュリティ管理を実施します。

6.8. タイムスタンプ

規定しません。

7. 電子証明書、CRL のプロファイル

7.1. 電子証明書のプロファイル

本項では本認証局の発行する電子証明書およびCRLのプロファイルについて規定します。

7.1.1. バージョン番号

本認証局は、ITU-T Recommendation X.509 バージョン 3 に準拠した電子証明書を発行します。

7.1.2. 電子証明書の拡張子

拡張領域の名称	Critical フラグ	CA 電子証明書	電子証明書（利用者）
SubjectKeyIdentifier (主体者鍵識別子)	FALSE	○	○
AuthorityKeyIdentifier（機関キー識別子）	FALSE	―	○
KeyUsage（鍵使用法）	TRUE	○	○
certificatePolicies (電子証明書ポリシ)	FALSE	―	○
BasicConstraints（基本制約）	TRUE	○	―
CRLDistributionPoints（CRL 配布点）	FALSE	―	○
extKeyUsage（拡張キー使用方法）	FALSE	―	○

”○”：当該電子証明書に含める項目
“―”：当該電子証明書に含めない項目
※1. CA 電子証明書の場合は TRUE、他の場合は FALSE。

7.1.3. アルゴリズムのオブジェクト識別子

本認証局は sha256WithRSAEncryption（オブジェクト識別子：1 2 840 113549 1 1 11）方式を用いて電子証明書に署名し、このアルゴリズムを示すオブジェクト識別子を当該電子証明書に記録します。

7.1.4. 名前の形式

認証局が発行する各種の電子証明書の含まれる識別名には、ITU-T X.500 識別名（DN:Distinguished Name）が用いられます。

7.1.5. 名前制約

電子証明書の記述に使用する言語は英語です。

7.1.6. 電子証明書ポリシーオブジェクト識別子

本サービスを示すオブジェクト識別子は 1.2 項で規定されています。

7.1.7. ポリシー制約拡張子の使用

規定しません。

7.1.8. ポリシー修飾子の構文および意味

規定しません。

7.1.9. 重要（Critical）とされた電子証明書ポリシー拡張子の処理

7.1.2 項を参照してください。

7.1.10. 有効期間

本認証局が発行する各種電子証明書の有効期間は以下の通りです。

電子証明書の種類	有効期間	鍵の更新頻度	電子証明書の 更新（または発行）頻度
CA 電子証明書	10 年	9 年毎	鍵の更新時
電子証明書（利用者）	390 日（約 13 ヶ月）	左記に同じ	鍵の更新時

7.2. CRL のプロファイル

7.2.1. バージョン番号

本認証局は、ITU-T Recommendation X.509 バージョン 2 に準拠した CRL を発行します。

7.2.2. CRL および CRL エントリ拡張子

本認証局が発行する CRL は、下表にしたがい CRL エントリ拡張子（crlEntryExtensions）、CRL 拡張子（crlExtentions）の設定を行います。

【拡張領域（crlEntryExtensions／失効リストエントリ拡張）】

領域名	Critical フラグ	設定値（例）	補足説明
reasonCode (失効理由)	FALSE	…	※ reasonCode は掲載されない場合もあります

【拡張領域（crlExtensions／失効リスト拡張領域）】

領域名	Critical フラグ	設定値（例）	補足説明
AuthorityKeyIdentifier (認証局鍵識別子)	FALSE		
keyIdentifier		…	発行者の鍵の識別子
cRLnumber (CRL番号)	FALSE	…	CRL の番号

7.3. OCSP のプロファイル

本認証局では OCSP は採用しません。

8. 準拠性監査とその他の評価

8.1. 評価の頻度または評価が行われる場合

本認証局が、本 CPS に従って適正な業務を行っていることを確認し維持するために、本認証局の責任者が必要と認めた場合、監査を実施することとします。

8.2. 評価人の身元または資格

監査人は、充分な知識及び経験を持つ者で、本認証局責任者によって指名されます。

8.3. 評価人とされるエンティティの関係

監査人は、本認証局の業務に関わっていない者でなければなりません。

8.4. 評価で扱われる事項

監査は、本認証局が運営する全ての認証業務及び設備を対象とします。監査では、本認証局が運営する IA、RA 及びリポジトリが、本 CPS 及び本 CPS に基づいた各種手順書などを順守して運営されているかを監査します。主な監査項目は次の通りです。

- IA および RA の運用業務
- 電子証明書のライフサイクル管理
- 本認証局の秘密鍵の管理
- ソフトウェア、ハードウェア及びネットワーク
- 認証設備室設備
- リポジトリ

8.5. 不備の結果としてとられる処置

監査結果での指摘事項及び新技術の動向を踏まえ、業務および設備の見直し改善を行い、必要である場合は、本 CPS を改訂し、その結果の評価を行います。

8.6. 評価結果の公開

監査結果の外部への公開もしくは開示は行いません。ただし、公的機関などから法律に基づく開示要求があった場合、もしくは開示が妥当であると本認証局責任者が判断した場合、監査結果を開示することがあります。

9. 他の業務上および法的問題

9.1. 料金

規定しません。

9.2. 財務上の責任

本 CPS では、損害保険加入の有無等財務的な責任については規定しません。

9.3. 秘密情報の保護

本項では、本認証局が管理する秘密情報の取り扱いについて規定します。

9.3.1. 秘密として扱う情報の範囲

・利用者、もしくはエンブレースから提出または提示された電子証明書の発行、失効に関する書類、データ
・本認証局で実行した各種の処理の記録
・本認証局に関わる設備、システム、ネットワーク等の詳細な仕様
・その他本認証局が必要と認めたもの

9.3.2. 機密として取り扱わない情報

本 CPS を含む本認証局のリポジトリで公開している各種情報

9.3.3. 機密として扱う情報を保護する責任

9.4.4 項で規定しています。

9.4. 個人情報のプライバシー保護

9.4.1. 個人情報保護方針

本認証局は本サービスの提供に必要な範囲内でのみ、利用者、エンブレースから提出または提示された個人情報を利用します。個人情報の取り扱いにあたっては jNOTARY の規定を順守します。

jNOTARY の個人情報保護方針は以下で確認することができます。

http://www.jnotary.com/privacy/index.html

9.4.2. 個人情報として取り扱う情報

本サービスでは以下を個人情報として取り扱います。

- 氏名
- メールアドレス
- 発行申請時に添付された本人確認書類

9.4.3. 個人情報とみなされない情報

規定しません。

9.4.4.　個人情報を保護する責任

本認証局は、個人情報の保護を充分に行い、jNOTARY の個人情報保護方針に従って個人情報を取り扱います。

9.4.5.　司法手続きまたは行政手続きにもとづく開示

本認証局は司法機関から法的根拠に基づいて情報を開示するように請求があった場合、当該司法機関に対して個人情報の開示を行う場合があります。また、本認証局は、調停、訴訟、その他の法的、裁判上または行政手続きの過程において個人情報開示を行う場合があります。

9.4.6.　その他開示

電子証明書の利用者は、自身の権利または利益が侵害された場合、またはその恐れがあると判断した場合、本認証局に対して当該電子証明書についての情報開示を請求することができます。

9.5.　知的財産権

別段の合意がなされない限り、以下の情報資料およびデータは本認証局を運営する jNOTARY に帰属する知的財産です。

・本認証局から発行された利用者電子証明書
・本認証局から発行された CA 電子証明書
・本認証局により作成された CRL
・本 CPS
・その他、リポジトリで公開する全ての情報

9.6.　義務と責任

9.6.1.　認証局の義務と責任

本認証局は、本 CPS で規定する利用者、および依拠当事者に対し、次の義務を負います。

1). 本認証局は、本 CPS に基づき本認証局の運営を行います。
2). 本認証局の秘密鍵を適切に運用管理し、電子証明書の信頼性を確保します。
3). 本認証局は、CRL を定期的に作成しリポジトリにて公開します。
4). 本認証局は、MCS クライアント認証のための電子証明書のみを発行し、それ以外の用途の電子証明書の発行は行いません。

9.6.2.　利用者の義務と責任

利用者は、本サービスの利用、あるいは利用申請にあたり、以下の事項に関して義務と責任を負わなければなりません。

1). 電子証明書発行の申請もしくは失効の請求にあたり、登録、提出する情報に誤りがないこと。
2). 電子証明書の使用用途を順守すること。
3). 利用者自身の秘密鍵、秘密鍵を利用するために必要な PIN コード等は、利用者自身が

責任を持って管理すること。

4). 4.9.1 項の電子証明書の失効要件に該当した場合、遅滞なく失効請求を行うこと

5). 本認証局は、本 CPS に従って運営されていることを承認すること。

9.6.3. 依拠当事者の義務と責任

依拠当事者は、電子証明書に依拠するにあたり、以下の事項に関して義務と責任を負わなければなりません。

1). 1.4 節において電子証明書の利用が許された範囲内においてのみ、電子証明書に依拠すること。

2). 本認証局の有効な CA 電子証明書を入手し、利用者の電子証明書に施された電子署名が、本認証局によるものであることを確認すること。また、CA 電子証明書（自己署名電子証明書）の真正性の確認は、本認証局が開示するフィンガープリントを入手し、これを用いて実施すること。

3). 電子証明書の有効性について、本認証局が発行する有効な失効情報（CRL）において、当該電子証明書の失効を示す情報が記録されていないことを確認すること。

4). 電子証明書は、その有効期間内において利用されたものであることを確認すること。

5). 電子証明書に依拠するかどうかの判断は、本 CPS に規定されているとおり、電子証明書の利用の目的、利用および検証の環境、最新の技術の動向等を考慮し、依拠当事者自身によってなされるものであること。

6). 本認証局が本 CPS にしたがって運営されていることを理解し、承認すること。

9.6.4. 他の関係者の義務と責任

規定しません。

9.7. 責任の範囲外

利用者の電子証明書取得または利用によりコンピュータシステム等のハードウェア、ソフトウェアに何らかの影響または障害が発生しても、本認証局は一切賠償責任を負わないものとする。

9.8. 責任の制限

1). 電子証明書を使用するにあたっての利用者自身及び依拠当事者自身のシステムに起因するあらゆる損失、損害または費用について、本認証局は免責されます。

2). 利用者自身の利用者秘密鍵の危殆化に起因するあらゆる損失、損害または費用について、本認証局は免責されます。

3). 利用者による電子証明書の使用から発生する、次の各項に起因する損害について、利用者は本認証局に賠償しなければなりません。

・ 虚偽の申告

・ 故意または過失による事実の不開示

・ 利用者秘密鍵の保護の懈怠

9.9. 補償

1) 本認証局は、本 CPS に定めた責任に違反して損害賠償責任を負う場合は、利用者に対し、支払う賠償額の上限を５０万円とします。いかなる場合においても、この賠償額の上限を超える請求には応じません。また、いかなる場合においても依拠当事者からの損害賠償請求には応じません。

9.10. 有効期間と終了

本項では、本 CPS の有効期間について規定します。

9.10.1. 有効期間

本 CPS は、本サービスが継続する間有効なものとします。本 CPS の改訂が行われた場合は、最も新しい版が有効とされます。

9.10.2. 終了

本 CPS は、本サービスの終了に従い廃止されるまで有効なものとします。

9.10.3. 終了の効果と効力の残存

9.11. 関係者間の個別通知と連絡

9.12. 改訂

本項では本 CPS の改訂について規定します。

9.12.1. 改訂手続き

本 CPS は利用者、依拠当事者、その他の者に事前の了解を得ることなく改訂を行うことができるものとします。本 CPS の改訂には、本認証局の認証局責任者による承認を必要とします。

9.12.2. 通知方法および期間

本認証局は、本 CPS の改訂が行われた場合、リポジトリにて公開します。また、リポジトリで公開された時点で当該 CPS は有効なものとなります。

9.12.3. オブジェクト識別子が変更されなければならない場合

規定しません。

9.13. 紛争の解決

全ての当事者は、本 CPS または本認証局発行の電子証明書に関して生じた紛争についての専属的合意管轄裁判所を東京地方裁判所とすることで合意するものとします。本 CPS、及び本認証局が発行する他の関連文書に定められていない事項やこれらの文書の解釈に関して疑義が生じた場合、各当事者は、その課題を解決するために誠意をもって協議するものとします。

9.14. 準拠法

当事者間の契約または他の準拠法を選択する旨の規定の有無にかかわらず、本 CPS の解釈及び有効性等は日本国内法によって判断されます。

9.15. 雑則

本項では、本 CPS に関わるその他条項について規定します。

9.15.1. 完全合意

本 CPS は、本 CPS において別段の定めをしている場合を除き、書面によらず口頭での追加、変更、削除、放棄、終了させることはできないものとします。

9.15.2. 権利譲渡

利用者は、この CP/CPS に基づく権利または義務の全部または一部を、本認証局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。

9.15.3. 分離可能

本 CPS、本サービスに関する契約、および合意の一部分の規定が、いかなる程度でも無効または執行不可能であるとされた場合であっても、本 CPS、本サービスに関する契約、および合意のその他の規定の有効性には影響を及ぼさず、当事者の意思に最も合理的に合致するように解釈されるものとします。

9.15.4. 強制執行

規定しません。

9.15.5. 不可抗力

以下の事象が発生し、利用者あるいは依拠当事者が損害を受けた場合、本認証局は一切賠償責任を負いません。

- 地震、水害、噴火、津波などの天災
- 火災、停電など
- 戦争、動乱、騒乱、暴動、労働争議など
- その他、あらゆる不可抗力に起因する損害

9.16. その他条項

規定しません。

A. 電子証明書および CRL プロファイル

A.1. CA 電子証明書プロファイル

【基本領域】

領域名	設定値(例)	補足説明
version (バージョン番号)	2	バージョンが 3 であることを示す
serialNumber (発行番号)	…	ユニークな値
signature (署名アルゴリズム)	1.2.840.113549.1.1.11	Sha256WithRSAEncryption を示す
issuer (発行者名)	cn=" Medical Care Station CA Service" o="Japan Digital Notarization Authority, Inc." c=jp	PrintableString で記載
validity (有効期間)		10 年有効
notBefore (開始日)	YYMMDDHHMMSSZ(年月日時分秒)	UTC 時刻型で記載
notAfter (終了日)	YYMMDDHHMMSSZ(年月日時分秒)	UTC 時刻型で記載
subject (主体者名)	cn=" Medical Care Station CA Service" o="Japan Digital Notarization Authority, Inc." c=jp	PrintableString で記載 issuer と同じ値
subjectPublicKeyInfo (主体者の公開鍵)		
algorithm(アルゴリズム)	1.2.840.113549.1.1.1	rsaEncryption を示す
subjectPublicKey(公開鍵)	…	主体者の公開鍵 2048 ビット長

【拡張領域】

領域名	Critical フラグ	設定値(例)	補足説明
EnrollCerttypeExtension (電子証明書テンプレート)	FALSE	CA	(マイクロソフト拡張)
KeyUsage (鍵使用法)	TRUE	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
BasicConstraints (基本制約)	TRUE		
cA		TRUE	CA であることを示す
SubjectKeyIdentifier (主体者鍵識別子)	FALSE	…	主体者(=CA)の鍵の識別子
caVersion (CA 電子証明書のバージョン)	FALSE	…	CA 電子証明書のバージョン

A.2.　利用者電子証明書プロファイル

【基本領域】

領域名	設定値(例)	補足説明
version (バージョン番号)	2	バージョンが 3 であることを示す
serialNumber (発行番号)	…	ユニークな値
signature (署名アルゴリズム)	1.2.840.113549.1.1.11	Sha256WithRSAEncryption を示す
issuer (発行者名)	cn=" Medical Care Station CA Service" o="Japan Digital Notarization Authority, Inc." c=jp	PrintableString で記載
validity (有効期間)		有効期間は 390 日(約 13 ヶ月)
notBefore(開始日)	YYMMDDHHMMSSZ(年月日時分秒)	UTC 時刻型で記載
notAfter(終了日)	YYMMDDHHMMSSZ(年月日時分秒)	UTC 時刻型で記載
subject (主体者名)	cn= MCSID	PrintableString で記載
subjectPublicKeyInfo (主体者の公開鍵)		
algorithm(アルゴリズム)	1.2.840.113549.1.1.1	rsaEncryption を示す
subjectPublicKey(公開鍵)	…	主体者の公開鍵 2048 ビット長

【拡張領域】

領域名	Critical フラグ	設定値(例)	補足説明
extKeyUsage (拡張キー使用方法)	FALSE	1.3.6.1.5.5.7.3.2	クライアント認証
KeyUsage (鍵使用法)	TRUE	DigitalSignature, keyEncipherment	
certificatePolicies (電子証明書ポリシ)	FALSE		
policyIdentifier		0.2.440.200148.2.2.5	本認証局の電子証明書ポリシ
policyQualifierId		id-qt-cps (1.3.6.1.5.5.7.2.1)	
qualifier		"https://mcs.jnotary.com/documents/MCS_CPS.pdf"	
subjectKeyIdentifier (主体者鍵識別子)	FALSE		
		…	主体者の鍵の識別子
AuthorityKeyIdentifier (認証局鍵識別子)	FALSE		
keyIdentifier		…	発行者の鍵の識別子
CRLDistributionPoints (CRL配布点)	FALSE		
distributionPoint		"http://mcs.jnotary.com/MCSCA.crl"	URI にて記載

A.3. CRL プロファイル

【基本領域】

領域名	設定値(例)	補足説明
version (バージョン番号)	1	バージョンが 2 であることを示す
signature (署名アルゴリズム)	1.2.840.113549.1.1.11	Sha256WithRSAEncryption を示す
issuer (発行者名)	cn=" Medical Care Station CA Service" o="Japan Digital Notarization Authority, Inc." c=jp	PrintableString で記載
thisUpdate (今回の更新日時)	YYMMDDHHMMSSZ(年月日時分秒)	168 時間(7 日)で更新 UTC 時刻型で記載
nextUpdate (次回の更新期限)	YYMMDDHHMMSSZ(年月日時分秒)	thisUpdate+168 時間(7 日間) +公開期間の 10% UTC 時刻型で記載
revokedCertificates (失効した電子証明書のリスト)		
userCertificate (失効した電子証明書)	…	失効した電子証明書の発行番号 (serialNumber)
revocationDate (失効日時)	YYMMDDHHMMSSZ(年月日時分秒)	失効処理が行われた日時 UTC 時刻型で記載

【拡張領域 (crlEntryExtensions/失効リストエントリ拡張)】

領域名	Critical フラグ	設定値(例)	補足説明
reasonCode (失効理由)	FALSE	…	※reasonCode は掲載されない場合もあります

【拡張領域 (crlExtensions/失効リスト拡張領域)】

領域名	Critical フラグ	設定値(例)	補足説明
AuthorityKeyIdentifier (認証局鍵識別子)	FALSE		
keyIdentifier		…	発行者の鍵の識別子
cRLnumber (CRL番号)	FALSE	…	CRL の番号
caVersion (CA電子証明書のバージョン)	FALSE	…	CA 電子証明書のバージョン
crlNextPublish (次のCRL発行)	FALSE	YYMMDDHHMMSSZ(年月日時分秒)	thisUpdate+168 時間(7 日間)