JASDEC 認証局証明書準則
(Certificate Policy)

Version1.32

2021 年 4 月 30 日

株式会社 証券保管振替機構

株式会社　ほふりクリアリング

改版履歴		
版数	日付	内容
1.00	2008/7/9	初版発行
1.10	2008/9/12	「Target 保振サイトを通じた残高証明書等の交付等に係るリハーサル」に関する改訂
1.20	2009/1/05	「Target 保振サイトを通じた残高証明書等の交付」の開始に関する改訂
1.21	2009/5/20	証明書のプロファイルに記載する CPS のアドレス等に関する変更
1.22	2013/12/2	定義と略語に関する変更
1.30	2014/1/6	署名アルゴリズムを SHA-1 から SHA-2 に、加入者証明書の鍵長を 1024bit から 2048bit に変更
1.31	2014/6/23	本 CP に関する照会窓口を株式会社証券保管振替機構システム開発部に変更
1.32	2021/4/30	本 CP に関する照会窓口を株式会社証券保管振替機構情報システム開発部に変更

目次

1. はじめに 1
1.1 概要 1
1.2 文書名と識別 1
1.3 PKI の関係者 1
1.3.1 認証局 1
1.3.2 登録局 1
1.3.3 証明書利用者 2
1.3.4 検証者 2
1.4 証明書の用途 2
1.4.1 適切な証明書の用途 2
1.4.2 禁止される証明書の用途 2
1.5 ポリシ管理 3
1.5.1 文書を管理する組織 3
1.5.2 連絡先 3
1.5.3 ポリシ適合性を決定する者 3
1.5.4 承認手続 3
1.6 定義と略語 3
2. 公開とリポジトリの責任 7
2.1 リポジトリ 7
2.2 証明情報の公開 7
2.3 公開の時期又は頻度 7
2.4 リポジトリへのアクセス管理 7
3. 識別と認証 8
3.1 名前の決定 8
3.1.1 名前の種類 8
3.1.2 名前の記載 8
3.1.3 加入者の匿名性又は仮名性 8
3.1.4 様々な名前形式を解釈するための規則 8
3.1.5 名前の一意性 8
3.1.6 認識、認証及び商標の役割 8
3.2 初回の本人性確認 8
3.2.1 私有鍵の所持を証明する方法 8
3.2.2 組織の認証 9
3.2.3 個人の認証 9
3.2.4 検証されない加入者の情報 9

3.2.5 権限の正当性確認 9
3.2.6 相互運用の基準 9
3.3 鍵更新申請時の本人性確認と認証 9
3.3.1 通常の鍵更新時における本人性確認と認証 9
3.3.2 証明書失効後の鍵更新時における本人性確認と認証 9
3.4 失効申請時の本人性確認と認証 9
4. 証明書のライフサイクルに対する運用上の要件 10
4.1 証明書申請 10
4.1.1 証明書申請を提出することができる者 10
4.1.2 登録手続及び責任 10
4.2 証明書申請手続 10
4.2.1 本人性確認と認証の実施 10
4.2.2 証明書申請の承認又は却下 10
4.2.3 証明書申請の処理時間検証者 10
4.3 証明書の発行 10
4.3.1 証明書発行時の処理手続 10
4.3.2 証明書利用者（機構加入者等である場合に限る。）への証明書発行通知 11
4.4 証明書の受領確認 11
4.4.1 証明書の受領確認手続 11
4.4.2 認証局による証明書の公開 11
4.4.3 他のエンティティに対する認証局の証明書発行通知 11
4.5 鍵ペア及び証明書の用途 11
4.5.1 証明書利用者の私有鍵及び証明書の用途 11
4.5.2 信頼者の公開鍵及び証明書の用途 11
4.6 証明書の更新 11
4.6.1 証明書の更新事由 11
4.6.2 証明書の更新を申請することができる者 11
4.6.3 証明書の更新申請の処理 11
4.6.4 加入者に対する新しい証明書発行通知 12
4.6.5 更新された証明書の受領確認の行為 12
4.6.6 認証局による更新された証明書の公開 12
4.6.7 他のエンティティに対する認証局の証明書発行通知 12
4.7 鍵更新を伴う証明書の更新 12
4.7.1 証明書の更新 12
4.7.2 新しい証明書の申請を行うことができる者 12
4.7.3 更新申請の処理 12

4.7.4 証明書利用者（機構加入者等である場合に限る。）に対する新しい証明書の通知 12
4.7.5 鍵更新された証明書の受領確認手続き 12
4.7.6 認証局による鍵更新済みの証明書の公開 12
4.7.7 他のエンティティに対する認証局の証明書発行通知 12
4.8 証明書の変更 13
4.8.1 証明書の変更 13
4.8.2 証明書の変更を申請することができる者 13
4.8.3 変更申請の処理 13
4.8.4 証明書利用者（機構加入者等である場合に限る。）に対する新しい証明書発行通知 13
4.8.5 変更された証明書の受領確認の行為 13
4.8.6 認証局による変更された証明書の公開 13
4.8.7 他のエンティティに対する認証局の証明書発行通知 13
4.9 証明書の失効と一時停止 13
4.9.1 証明書失効事由 13
4.9.2 証明書失効を申請することができる者 14
4.9.3 失効申請手続 14
4.9.4 失効申請の猶予期間 14
4.9.5 認証局が失効申請を処理しなければならない期間 14
4.9.6 失効調査の要求 14
4.9.7 証明書失効リストの発行頻度 14
4.9.8 証明書失効リストの発行最大遅延時間 14
4.9.9 オンラインでの失効/ステイタス確認の適用性 15
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 15
4.9.11 利用可能な失効情報の他の形式 15
4.9.12 鍵の危殆化に対する特別要件 15
4.9.13 証明書の一時停止事由 15
4.9.14 証明書の一時停止を申請することができる者 15
4.9.15 証明書の一時停止申請手続 15
4.9.16 一時停止を継続することができる期間 15
4.10 証明書のステイタス確認サービス 15
4.10.1 運用上の特徴 15
4.10.2 サービスの利用可能性 15
4.10.3 オプショナルな仕様 15
4.11 加入（登録）の終了 16

4.12 キーエスクローと鍵回復 16
5. 設備上、運営上、運用上の管理 17
5.1 物理的管理 17
5.1.1 立地場所及び構造 17
5.1.2 物理的アクセス 17
5.1.3 電源及び空調 17
5.1.4 水害対策 17
5.1.5 火災防止及び火災保護対策 17
5.1.6 媒体保管 17
5.1.7 廃棄処理 17
5.1.8 オフサイトバックアップ 17
5.2 手続的管理 17
5.2.1 信頼すべき役割 17
5.2.2 職務ごとに必要とされる人数 17
5.2.3 個々の役割に対する本人性確認と認証 18
5.2.4 職務分割が必要となる役割 18
5.3 人事的管理 18
5.3.1 資格、経験及び身分証明の要件 18
5.3.2 背景調査 18
5.3.3 教育要件 18
5.3.4 再教育の頻度及び要件 18
5.3.5 仕事のローテーションの頻度及び順序 18
5.3.6 認められていない行動に対する制裁 18
5.3.7 独立した契約者の要件 18
5.3.8 要員へ提供される資料 18
5.4 監査ログの手続 18
5.4.1 記録されるイベントの種類 18
5.4.2 監査ログを処理する頻度 19
5.4.3 監査ログを保持する期間 19
5.4.4 監査ログの保護 19
5.4.5 監査ログのバックアップ手続 19
5.4.6 監査ログの収集システム 19
5.4.7 イベントを起こした者への通知 19
5.4.8 脆弱性評価 19
5.5 記録の保管 19
5.5.1 アーカイブの種類 19

5.5.2 アーカイブ保存期間 19
5.5.3 アーカイブの保護 19
5.5.4 アーカイブのバックアップ手続 19
5.5.5 記録にタイムスタンプを付与する要件 19
5.5.6 アーカイブ収集システム 20
5.5.7 アーカイブの検証手続 20
5.6 鍵の切り替え 20
5.7 危殆化及び災害からの復旧 20
5.7.1 事故及び危殆化時の手続 20
5.7.2 ハードウェア、ソフトウェア又はデータが破損した場合の手続 20
5.7.3 エンティティの私有鍵が危殆化した場合の手続 20
5.7.4 災害後の事業継続性 20
5.8 認証局又は登録局の終了 20
6. 技術的セキュリティ管理 21
6.1 鍵ペアの生成及びインストール 21
6.1.1 鍵ペアの生成 21
6.1.2 証明書利用者に対する私有鍵の交付 21
6.1.3 認証局への公開鍵の交付 21
6.1.4 検証者への CA 公開鍵の交付 21
6.1.5 鍵サイズ 21
6.1.6 公開鍵のパラメータの生成及び品質検査 21
6.1.7 鍵の用途 21
6.2 私有鍵の保護及び暗号モジュール技術の管理 21
6.2.1 暗号モジュールの標準及び管理 21
6.2.2 私有鍵の複数人管理 22
6.2.3 私有鍵のエスクロー 22
6.2.4 私有鍵のバックアップ 22
6.2.5 私有鍵のアーカイブ 22
6.2.6 私有鍵の暗号モジュールへの又は暗号モジュールからの転送 22
6.2.7 暗号モジュールへの私有鍵の格納 22
6.2.8 私有鍵の活性化方法 22
6.2.9 私有鍵の非活性化方法 22
6.2.10 私有鍵の破棄方法 22
6.2.11 暗号モジュールの評価 22
6.3 鍵ペアのその他の管理方法 22
6.3.1 公開鍵のアーカイブ 22

6.3.2 私有鍵及び公開鍵の有効期間 23
6.4 活性化データ 23
6.4.1 活性化データの生成及び設定 23
6.4.2 活性化データの保護 23
6.4.3 活性化データの他の考慮点 23
6.5 コンピュータのセキュリティ管理 23
6.5.1 コンピュータセキュリティに関する技術的要件 23
6.5.2 コンピュータセキュリティ評価 23
6.6 ライフサイクルセキュリティ管理 23
6.6.1 システム開発管理 23
6.6.2 セキュリティ運用管理 23
6.6.3 ライフサイクルセキュリティ管理 23
6.7 ネットワークセキュリティ管理 24
6.8 タイムスタンプ 24
7. 証明書及び証明書失効リストのプロファイル 25
7.1 証明書のプロファイル 25
7.2 CRL のプロファイル 29
8. 準拠性監査と他の評価 30
9. 他の業務上及び法的事項 31
9.1 料金 31
9.2 財務的責任 31
9.3 企業情報の機密性 31
9.3.1 機密情報の範囲 31
9.3.2 機密情報の範囲外の情報 31
9.3.3 機密情報を保護する責任 31
9.4 個人情報の保護 31
9.5 知的財産権 31
9.6 表明保証 31
9.6.1 認証局の表明保証 32
9.6.1.1 IA の表明保証 32
9.6.1.2 RA の表明保証 32
9.6.2 証明書利用者（機構加入者等である場合に限る。）の表明保証 32
9.6.3 検証者の表明保証 32
9.6.4 他の関係者の表明保証 33
9.7 無保証 33
9.8 責任の制限 33

9.9 補償 33
9.10 有効期間と終了 34
9.10.1 有効期間 34
9.10.2 終了 34
9.10.3 終了の効果と効果継続 34
9.11 関係者間の個別通知と連絡 34
9.12 改訂 34
9.12.1 改訂手続 34
9.12.2 通知方法及び期間 34
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 34
9.13 紛争解決手続 34
9.14 準拠法 35
9.15 適用法の遵守 35
9.16 雑則 35
9.17 その他の条項 35

1. はじめに

1.1 概要

JASDEC 認証局証明書準則（以下「本 CP」といいます。）は、株式会社証券保管振替機構及び株式会社ほふりクリアリング（以下「ほふり等」といいます。）が認証局（以下「本 CA」といいます。）として発行する証明書に関するポリシ及びこのポリシを運用するための方針、諸手続を定めます。

なお、本 CP は、IETF が認証局運用のフレームワークとして提唱する RFC3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠しています。

1.2 文書名と識別

本 CA では、発行する証明書の種類及び発行基準に応じて一意となるオブジェクト識別子（以下「OID」という。）が割り当てられ、各証明書内に示されます。本 CA が本 CP に基づき発行する証明書、対応する OID 及び本 CP が参照する CPS の OID を次に示します。

CP/CPS	OID
JASDEC 認証局証明書準則	1.2.392.200091.110.161.1
セコム電子認証基盤認証運用規程	1.2.392.200091.100.401.1

1.3 PKI の関係者

1.3.1 認証局

本 CA は、IA（Issuing Authority：発行局）及び RA（Registration Authority：登録局）によって構成されます。IA は、証明書の発行、取消、CRL（CertifiCAte RevoCAtion List：証明書失効リスト）の開示等を行います。また、RA は、証明書の発行、取消を申請する申請者の実在性確認、本人性確認の審査及び証明書を発行、失効するための登録業務等を行います。

本 CA は、本 CP 及び本 CA の認証局の基盤を構築するセコムトラストシステムズ株式会社が管理するセコム電子認証基盤認証運用規程（以下「CPS」という。）に定めるところにより運営されます。

1.3.2 登録局

「1.3.1.認証局」に含みます。

1.3.3 証明書利用者

証明書利用者とは、本 CA から証明書の発行を受け、本 CA が発行する証明書を利用する業務を行う者のことであり、機構加入者等及び機構が認める者とします。証明書利用者は、本 CP 及び CPS に記載される証明書利用者の義務を遵守するものとします。

1.3.4 検証者

検証者とは、電子署名の付されたメッセージ等について、その電子署名が間違いなく証明書利用者によって行われているということを検証する者をいいます。

1.4 証明書の用途

1.4.1 適切な証明書の用途

本 CA が発行する証明書の用途は、本 CA が発行する証明書を利用するほふり等の業務に関するものとします。

1.4.2 禁止される証明書の用途

本 CA が発行する証明書の用途は「1.4.1 適切な証明書の用途」のとおりであり、証明書をそれ以外の目的に利用することはできないものとします。

1.5 ポリシ管理

1.5.1 文書を管理する組織

本 CP の変更、更新等に関する事務は、ほふり等が行います。

1.5.2 連絡先

本 CP に関する照会は、株式会社証券保管振替機構情報システム開発部を窓口とします。

1.5.3 ポリシ適合性を決定する者

本 CP の内容について、ほふり等のポリシ承認機関が適合性を決定します。

1.5.4 承認手続

本 CP は、ほふり等のポリシ承認機関の承諾によって発効されます。

1.6 定義と略語

「あ」～「ん」

アーカイブ

履歴の保存を目的に取得する情報のことをいいます。

エスクロー

第三者に預けること（寄託）をいいます。

鍵ペア

公開鍵暗号方式において、私有鍵と公開鍵から構成される鍵の対のことをいいます。

監査ログ

認証局システムへのアクセスや不正操作の有無を検査するために記録される認証局システムの動作履歴やアクセス履歴等をいいます。

機構加入者等

株式等振替制度、一般債振替制度、短期社債振替制度及び投資信託振替制度の機構加入者、外国株券等保管振替決済業務の外国株券等参加者又は一般振替DVP決済のDVP参加者のことをいいます。

公開鍵
公開鍵暗号方式において用いられる鍵ペアの一方をいい、私有鍵に対応し、通信相手の相手方に公開される鍵のことをいいます。

私有鍵
公開鍵暗号方式において用いられる鍵ペアの一方をいい、公開鍵に対応する本人のみが保有する鍵のことをいいます。

申請 CSV
証明書の利用者が証明書の発行・更新・失効を申請するために、機構に提出する CSV 形式の電子データのことをいいます。

タイムスタンプ
電子ファイルの作成日時やシステムが処理を実行した日時等を記録したデータのことをいいます。

証明書
ある公開鍵を、記載された者が保有することを証明する電子データのことをいいます。CA が電子署名を施すことで、その正当性が保証されます。

リポジトリ
CA 証明書及び CRL 等を格納し公表するデータベースのことをいいます。

「A」～「Z」

CA（Certification Authority）：認証局
証明書の発行・更新・失効、CA 私有鍵の生成・保護及び証明書利用者の登録等を行う主体のことをいいます。

CP（ Certificate Policy）：認証局証明書準則
CA が発行する証明書の種類、用途、申込手続等、証明書に関する事項を規定する文書のことをいいます。

CPS（Certification Practices Statement）：認証運用規程
CA を運用する上での諸手続、セキュリティ基準等、CA の運用を規定する文書のことをいいます。

CRL（Certificate Revocation List）：証明書失効リスト
証明書の有効期間中に、証明書記載内容の変更、私有鍵の紛失等の事由により失効された証明書情報が記載されたリストのことをいいます。

FIPS140-2
米国 NIST（National Institute of Standards and Technology）が策定した暗号モジュールに関するセキュリティ認定基準のことをいいます。

HSM（Hardware Security Module）
私有鍵の生成、保管、利用などにおいて、セキュリティを確保する目的で使用する耐タンパー機能を備えた暗号装置のことをいいます。

IA（Issuing Authority）：発行局
CA の業務のうち、証明書の発行・更新・失効、CA 私有鍵の生成・保護、リポジトリの維持・管理等を行う主体のことをいいます。

OID（Object Identifier）：オブジェクト識別子
ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいいます。

PKI（Public Key Infrastructure）：公開鍵基盤
電子署名、暗号化、認証といったセキュリティ技術を実現するための、公開鍵暗号方式という暗号技術を用いる基盤のことをいいます。

RA（登録局）（Registration Authority）：登録機関
CA の業務のうち、申込情報の審査、証明書発行に必要な情報の登録、CA に対する証明書発行要求等を行う主体のことをいいます。

RFC3647（Request For Comments 3647）
インターネットに関する技術の標準を定める団体である IETF（The Internet Engineering Task Force）が発行する文書であり、CP/CPS のフレームワークを規定した文書のことをいいます。

RSA

公開鍵暗号方式として普及している最も標準的な暗号技術のひとつです。

SHA-1・SHA-256（Secure Hash Algorithm）

電子署名に使われるハッシュ関数（要約関数）のひとつである。ハッシュ関数とは、与えられた原文から固定長のビット列を生成する演算手法をいいます。
データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができます。

2. 公開とリポジトリの責任

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います。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ります。

2.2 証明情報の公開

本 CA は、証明書失効リスト（以下「CRL」といいます。）をリポジトリ上に公開し、証明書利用者及び検証者がオンラインによって閲覧できるようにします。

2.3 公開の時期又は頻度

本 CA は、24 時間ごとに新たな CRL を発行し、リポジトリ上に公開します。また、証明書の失効が行われた場合には、即時に新たな CRL を発行し、リポジトリ上に公開します。また、証明書の有効期間を過ぎた場合には、CRL から削除されます。

2.4 リポジトリへのアクセス管理

本 CA は、リポジトリでの公開情報に関して、特段のアクセスコントロールを行いません。証明書利用者及び検証者は、本 CA の CRL を、リポジトリを通じて入手することが可能です。リポジトリへのアクセスは、一般的な Web インターフェースを通じて可能とします。

3. 識別と認証

3.1 名前の決定

3.1.1 名前の種類

本 CA が発行する証明書に記載される発行者及び証明書利用者の名前は、X.500 シリーズの識別名規定に従って設定します。

3.1.2 名前の記載

本 CA が発行する証明書利用者の証明書に記載される名前として、ほふり等が管理するコード、組織名又は担当者名を記載します。

3.1.3 加入者の匿名性又は仮名性

証明書利用者の名前に関する要件は、3.1.1 及び 3.1.2 のとおりとします。

3.1.4 様々な名前形式を解釈するための規則

様々な名前の形式を解釈する規則は、X.500 シリーズの識別名規定に従います。

3.1.5 名前の一意性

証明書に記載される名前は、本 CA が発行する全証明書内において一意とします。

3.1.6 認識、認証及び商標の役割

規定しません。

3.2 初回の本人性確認

3.2.1 私有鍵の所持を証明する方法

CA 証明書、電子署名用証明書及びクライアント認証用証明書の発行手続においては、本 CA が証明書利用者の鍵ペアを生成することにより、公開鍵と私有鍵との対応を結びつけます。ファイル暗号用証明書の発行手続においては、本 CA は、証明書利用者（機構加入者等である場合に限る。）からオンラインによって受け付けた証明書発行要求（Certificate Signing Request「以下「CSR」といいます。）の署名の検証を行い、当該 CSR が、証明書利用者（機構加入者等である場合に限る。）が所有する私有鍵で署名されていることを確認します。

3.2.2 組織の認証

本 CA は、証明書利用者（機構加入者等である場合に限る。）が行った口座開設等の所定の手続によりその真偽を確認します。

3.2.3 個人の認証

規定しません。

3.2.4 検証されない加入者の情報

規定しません。

3.2.5 権限の正当性確認

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

3.3.1 通常の鍵更新時における本人性確認と認証

鍵更新時における証明書利用者（機構加入者等である場合に限る。）の本人性確認及び認証は、「3.2 初回の本人性確認」と同様とします。

3.3.2 証明書失効後の鍵更新時における本人性確認と認証

証明書失効後の鍵更新時における証明書利用者（機構加入者等である場合に限る。）の本人性確認及び認証は、「3.2 初回の本人性確認」と同様とします。

3.4 失効申請時の本人性確認と認証

失効申請時における証明書利用者（機構加入者等である場合に限る。）の本人性確認及び認証は、「3.2 初回の本人性確認」と同様とします。

4. 証明書のライフサイクルに対する運用上の要件

4.1 証明書申請

4.1.1 証明書申請を提出することができる者

証明書の発行申請を行うことができる者は、証明書利用者とします。

4.1.2 登録手続及び責任

証明書の発行申請を行う者は、本 CA に対して正確な情報を提出するものとします。申請は、申請 CSV の提出により行うものとします。

本 CA は、証明書の発行申請に関する情報を審査し、問題がなければ申請情報に従って証明書の発行登録を行います。

4.2 証明書申請手続

4.2.1 本人性確認と認証の実施

本 CA は、Target 保振サイトの認証情報により、証明書の発行申請を行う者が機構加入者等であることを確認します。

4.2.2 証明書申請の承認又は却下

本 CA は、審査の結果、承認を行った申請について証明書の発行登録を行います。

不備がある申請については、申請を却下し、申請者に対して申請 CSV の再提出を依頼します。

4.2.3 証明書申請の処理時間検証者

本 CA は、承認を行った申請について、適時証明書の発行登録を行います。

4.3 証明書の発行

4.3.1 証明書発行時の処理手続

本 CA は、発行申請を受け付けた後に、証明書の発行登録作業を行います。発行登録作業によって、証明書発行用 Web サイトの URL 及びパスワードを発行します。発行した URL 及びパスワードは、電子メールにより、証明書利用者（機構加入者等である場合に限る。）に対して送付します。

4.3.2 証明書利用者（機構加入者等である場合に限る。）への証明書発行通知

本 CA は、証明書利用者（機構加入者等である場合に限る。）に対し発行サイトの URL 及びパスワードを通知することによって証明書の発行通知とします。

4.4 証明書の受領確認

4.4.1 証明書の受領確認手続

証明書の受領確認は、証明書利用者（機構加入者等である場合に限る。）が Web サイトより証明書のダウンロードを行ったことを確認することにより行います。

4.4.2 認証局による証明書の公開

本 CA は、証明書利用者の証明書の公開を行いません。

4.4.3 他のエンティティに対する認証局の証明書発行通知

本 CA は、第三者に対する証明書の発行通知を行いません。

4.5 鍵ペア及び証明書の用途

4.5.1 証明書利用者の私有鍵及び証明書の用途

証明書利用者の私有鍵及び証明書の用途は、本 CA が発行する証明書を利用する業務を行うための電子署名、暗号化又は復号とします。

4.5.2 信頼者の公開鍵及び証明書の用途

検証者は、証明書を検証し、発行者を確認します。

4.6 証明書の更新

4.6.1 証明書の更新事由

規定しません。

4.6.2 証明書の更新を申請することができる者

規定しません。

4.6.3 証明書の更新申請の処理

規定しません。

4.6.4 加入者に対する新しい証明書発行通知

規定しません。

4.6.5 更新された証明書の受領確認の行為

規定しません。

4.6.6 認証局による更新された証明書の公開

規定しません。

4.6.7 他のエンティティに対する認証局の証明書発行通知

規定しません。

4.7 鍵更新を伴う証明書の更新

4.7.1 証明書の更新

証明書の更新は、証明書の有効期限の到来に伴い行います。

4.7.2 新しい証明書の申請を行うことができる者

「4.1.1.証明書申請を提出することができる者」と同様とします。

4.7.3 更新申請の処理

「4.3.1.証明書発行時の処理手続」と同様とします。

4.7.4 証明書利用者（機構加入者等である場合に限る。）に対する新しい証明書の通知

「4.3.2.証明書利用者（機構加入者等である場合に限る。）への証明書発行通知」と同様とします。

4.7.5 鍵更新された証明書の受領確認手続き

「4.4.1.証明書の受領確認手続」と同様とします。

4.7.6 認証局による鍵更新済みの証明書の公開

本 CA は、証明書利用者の証明書の公開を行いません。

4.7.7 他のエンティティに対する認証局の証明書発行通知

本 CA は、第三者に対する証明書の発行通知を行いません。

4.8 証明書の変更

4.8.1 証明書の変更

証明書の変更は、証明書の記載内容に変更が発生した場合に行います。

4.8.2 証明書の変更を申請することができる者

「4.1.1.証明書申請を提出することができる者」と同様とします。

4.8.3 変更申請の処理

「4.3.1.証明書発行時の処理手続」と同様とします。

4.8.4 証明書利用者（機構加入者等である場合に限る。）に対する新しい証明書発行通知

「4.3.2.証明書利用者（機構加入者等である場合に限る。）への証明書発行通知」と同様とします。

4.8.5 変更された証明書の受領確認の行為

「4.4.1.証明書の受領確認手続」と同様とします。

4.8.6 認証局による変更された証明書の公開

本 CA は、利用者証明書の公開を行いません。

4.8.7 他のエンティティに対する認証局の証明書発行通知

本 CA は、第三者に対する証明書の発行通知を行いません。

4.9 証明書の失効と一時停止

4.9.1 証明書失効事由

本 CA は、次の事由が発生した場合には、失効申請者からの申請に基づき証明書の失効処理を行います。

- 証明書記載情報に変更があった場合
- 私有鍵の盗難、紛失、漏洩、不正利用等により私有鍵が危殆化した又は危殆化のおそれがある場合
- 証明書の内容が正しくない場合
- 証明書の利用を中止する場合

また、本 CA は、次の事由が発生した場合に、本 CA の判断により証明書利用者の証明

書を失効処理を行います。

- 証明書利用者（機構加入者等である場合に限る。）が本 CP 及び CPS に基づく義務を履行していない場合
- ほふり等が本 CA を終了する場合
- 本 CA の私有鍵が危殆化した又は危殆化のおそれがあると判断した場合
- 本 CA が失効を必要とすると判断するその他の状況が認められた場合

4.9.2 証明書失効を申請することができる者

証明書の失効の申請を行うことができる者は、証明書利用者とします。なお、本 CP「4.9.1. 証明書失効事由」に該当すると本 CA が判断した場合には、本 CA が失効申請者となり得ます。

4.9.3 失効申請手続

失効時の処理手順は、次のとおりとします。

・失効申請者は、本 CP「3.4. 失効申請時の本人性確認と認証」に定める情報を、本 CA へ届け出るものとします。

・本 CA は、所定の手続によって受け付けた情報が有効な失効の申請であることを確認し、証明書の失効処理を行います。

4.9.4 失効申請の猶予期間

失効の申請は、失効すべき事象が発生してから速やかに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期間

本 CA は、有効な失効の申請を受け付けてから速やかに証明書の失効処理を行い、CRL へ当該証明書情報を反映させます。

4.9.6 失効調査の要求

本 CA が発行する証明書には、CRL の格納先である URL が記載されています。CRL へのアクセスは、一般的な Web インターフェースを用いて可能としています。なお、CRL には、有効期限の切れた証明書情報は含ませません。

4.9.7 証明書失効リストの発行頻度

CRL は、失効処理の有無に関わらず、24 時間ごとに更新を行います。証明書の失効処理が行われた場合には、その時点で CRL の更新を行います。

4.9.8 証明書失効リストの発行最大遅延時間

本 CA は、発行した CRL を即時にリポジトリに反映させます。

4.9.9 オンラインでの失効/ステイタス確認の適用性

規定しません。

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 利用可能な失効情報の他の形式

本 CA は、CRL 以外による失効情報の公開を行いません。

4.9.12 鍵の危殆化に対する特別要件

規定しません。

4.9.13 証明書の一時停止事由

一時停止は、実施しません。

4.9.14 証明書の一時停止を申請することができる者

規定しません。

4.9.15 証明書の一時停止申請手続

規定しません。

4.9.16 一時停止を継続することができる期間

規定しません。

4.10 証明書のステイタス確認サービス

規定しません。

4.10.1 運用上の特徴

規定しません。

4.10.2 サービスの利用可能性

規定しません。

4.10.3 オプショナルな仕様

規定しません。

4.11 加入（登録）の終了

証明書の利用を終了する場合には、証明書利用者は、本 CA に対し証明書の失効の申請を行わなければなりません。本 CA は、有効な申請を受け付けた後、証明書の失効を行います。

4.12 キーエスクローと鍵回復

本 CA は、証明書利用者の私有鍵のエスクローを行いません。

5. 設備上、運営上、運用上の管理

5.1 物理的管理

5.1.1 立地場所及び構造
本項については、CPS に規定します。

5.1.2 物理的アクセス
本項については、CPS に規定します。

5.1.3 電源及び空調
本項については、CPS に規定します。

5.1.4 水害対策
本項については、CPS に規定します。

5.1.5 火災防止及び火災保護対策
本項については、CPS に規定します。

5.1.6 媒体保管
本項については、CPS に規定します。

5.1.7 廃棄処理
本項については、CPS に規定します。

5.1.8 オフサイトバックアップ
本項については、CPS に規定します。

5.2 手続的管理

5.2.1 信頼すべき役割
本項については、CPS に規定します。

5.2.2 職務ごとに必要とされる人数
本項については、CPS に規定します。

5.2.3 個々の役割に対する本人性確認と認証

本項については、CPS に規定します。

5.2.4 職務分割が必要となる役割

本項については、CPS に規定します。

5.3 人事的管理

5.3.1 資格、経験及び身分証明の要件

本項については、CPS に規定します。

5.3.2 背景調査

本項については、CPS に規定します。

5.3.3 教育要件

本項については、CPS に規定します。

5.3.4 再教育の頻度及び要件

本項については、CPS に規定します。

5.3.5 仕事のローテーションの頻度及び順序

本項については、CPS に規定します。

5.3.6 認められていない行動に対する制裁

本項については、CPS に規定します。

5.3.7 独立した契約者の要件

本項については、CPS に規定します。

5.3.8 要員へ提供される資料

本項については、CPS に規定します。

5.4 監査ログの手続

5.4.1 記録されるイベントの種類

本項については、CPS に規定します。

5.4.2 監査ログを処理する頻度

本項については、CPS に規定します。

5.4.3 監査ログを保持する期間

本項については、CPS に規定します。

5.4.4 監査ログの保護

本項については、CPS に規定します。

5.4.5 監査ログのバックアップ手続

本項については、CPS に規定します。

5.4.6 監査ログの収集システム

本項については、CPS に規定します。

5.4.7 イベントを起こした者への通知

本項については、CPS に規定します。

5.4.8 脆弱性評価

本項については、CPS に規定します。

5.5 記録の保管

5.5.1 アーカイブの種類

本項については、CPS に規定します。

5.5.2 アーカイブ保存期間

本項については、CPS に規定します。

5.5.3 アーカイブの保護

本項については、CPS に規定します。

5.5.4 アーカイブのバックアップ手続

本項については、CPS に規定します。

5.5.5 記録にタイムスタンプを付与する要件

本項については、CPS に規定します。

5.5.6 アーカイブ収集システム

本項については、CPS に規定します。

5.5.7 アーカイブの検証手続

本項については、CPS に規定します。

5.6 鍵の切り替え

本 CA の私有鍵は、私有鍵に対応する証明書の有効期間が証明書利用者の証明書の最大有効期間よりも短くなる前に新たな私有鍵の生成及び証明書の発行を行います。新しい私有鍵が生成された後は、新しい私有鍵を使って証明書及び CRL の発行を行います。

5.7 危殆化及び災害からの復旧

本 CA は、本 CA の私有鍵が危殆化した場合又は事故・災害等により本 CA の運用の停止を伴う事象が発生した場合には、速やかに業務復旧に向けた対応を行うとともに、証明書利用者、その他関係者に対し、必要情報を連絡します。

5.7.1 事故及び危殆化時の手続

本項については、CPS に規定します。

5.7.2 ハードウェア、ソフトウェア又はデータが破損した場合の手続

本項については、CPS に規定します。

5.7.3 エンティティの私有鍵が危殆化した場合の手続

本項については、CPS に規定します。

5.7.4 災害後の事業継続性

本項については、CPS に規定します。

5.8 認証局又は登録局の終了

ほふり等は、本 CA を終了する場合には、終了する少なくとも 90 日前までに証明書利用者及び関係者に対して終了の事実を通知又は公表し、所定の終了手続を行います。ただし、緊急やむをえない場合には、この期間を短縮できるものとします。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成及びインストール

6.1.1 鍵ペアの生成

証明書利用者の鍵ペアは、証明書利用者の端末又は本 CA の設備によって生成するものとします。

6.1.2 証明書利用者に対する私有鍵の交付

本 CA が証明書利用者の私有鍵を生成する場合には、鍵ペア及びそれを使用するための PIN を 2 系統によって配付を行います。

6.1.3 認証局への公開鍵の交付

本 CA への証明書利用者（機構加入者等である場合に限る。）公開鍵の送付は、オンラインによって行われます。この時の通信は SSL により暗号化され、通信経路を保護します。

6.1.4 検証者への CA 公開鍵の交付

検証者は、本 CA のリポジトリにアクセスすることにより、CA 公開鍵を入手することができます。

6.1.5 鍵サイズ

証明書利用者の鍵ペアの電子署名方式は、ハッシュアルゴリズムとして SHA-256 を用いた RSA 方式であり、鍵長については 2048 ビットとします。

6.1.6 公開鍵のパラメータの生成及び品質検査

規定しません。

6.1.7 鍵の用途

証明書利用者の KeyUsage は、本 CP「7.1 証明書のプロファイル」に記載します。

6.2 私有鍵の保護及び暗号モジュール技術の管理

6.2.1 暗号モジュールの標準及び管理

本項については、CPS に規定します。

6.2.2 私有鍵の複数人管理

本項については、CPS に規定します。

6.2.3 私有鍵のエスクロー

本項については、CPS に規定します。

6.2.4 私有鍵のバックアップ

本項については、CPS に規定します。

6.2.5 私有鍵のアーカイブ

本項については、CPS に規定します。

6.2.6 私有鍵の暗号モジュールへの又は暗号モジュールからの転送

本項については、CPS に規定します。

6.2.7 暗号モジュールへの私有鍵の格納

本項については、CPS に規定します。

6.2.8 私有鍵の活性化方法

本項については、CPS に規定します。

6.2.9 私有鍵の非活性化方法

本項については、CPS に規定します。

6.2.10 私有鍵の破棄方法

本項については、CPS に規定します。

6.2.11 暗号モジュールの評価

本項については、CPS に規定します。

6.3 鍵ペアのその他の管理方法

6.3.1 公開鍵のアーカイブ

本項については、CPS に規定します。

6.3.2 私有鍵及び公開鍵の有効期間

本項については、CPS に規定します。

6.4 活性化データ

6.4.1 活性化データの生成及び設定

本項については、CPS に規定します。

6.4.2 活性化データの保護

本項については、CPS に規定します。

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ュリティ管理

6.5.1 コンピュータセキュリティに関する技術的要件

本項については、CPS に規定します。

6.5.2 コンピュータセキュリティ評価

本項については、CPS に規定します。

6.6 ライフサイクルセキュリティ管理

6.6.1 システム開発管理

本項については、CPS に規定します。

6.6.2 セキュリティ運用管理

本項については、CPS に規定します。

6.6.3 ライフサイクルセキュリティ管理

本項については、CPS に規定します。

6.7 ネットワークセキュリティ管理

本項については、CPS に規定します。

6.8 タイムスタンプ

本項については、CPS に規定します。

7. 証明書及び証明書失効リストのプロファイル

7.1 証明書のプロファイル

表 7.1-1 CA 証明書のプロファイル

フィールド（基本領域）		内容	critical
Version （X.509 証明書バージョン）		Version 3	-
Serial Number （証明書シリアル番号）		例） 123456789abcdef0	-
Signature Algorithm （署名アルゴリズム）		SHA-256 with RSAEncryption	-
Issuer （発行者）	Country （国）	C = JP	-
	Organization （組織）	O = JASDEC	
	Common Name (CN)	CN = JASDEC CA	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2008/01/01 00:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2028/01/01 00:00:00 GMT ＊20 年以下の有効期間	
Subject （主体者）	Country （国）	C = JP	-
	Organization （組織）	O = JASDEC	
	Common Name (CN)	CN = JASDEC CA	
Subject PublicKey Info （主体者公開鍵情報）		主体者の RSA 公開鍵 (2048bit)	-
フィールド（拡張領域）		内容	critical
Subject Key Identifier （主体者鍵識別子）		主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	N
Key Usage （鍵用途）		keyCertSign (証明書への署名) cRLSign (CRL への署名)	Y
Basic Constraints （基本的制約）		TRUE （CA である）	Y

表 7.1-2 電子署名用証明書のプロファイル

証明書フィールド（基本領域）		内容	critical
X.509 Version （X.509 証明書バージョン）		Version 3	-
Serial Number （証明書シリアル番号）		例） 123456789abcdef0	-
Signature Algorithm （署名アルゴリズム）		SHA-256 with RSAEncryption	-
Issuer （発行者）	Country （国）	C = JP	-
	Organization （組織）	O = JASDEC	
	Common Name (CN)	CN = JASDEC CA	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2008/01/01 12:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2013/01/01 12:00:00 GMT ＊有効期間 5 年以内	
Subject （主体者）	Country （国）	C = JP	-
	Organization （組織）	O = JASDEC	
	Organizational Unit （組織単位）	OU = "組織単位" ＊証明書申請時に値を決定する	
	Common Name （主体者名）	CN = "主体者名" ＊証明書申請時に値を決定する	
Subject PublicKey Info（主体者公開鍵情報）		主体者の公開鍵（2048bit）	-
証明書フィールド（x.509 v3 拡張領域）		内容	critical
Authority Key Identifier （発行者鍵識別子）		発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	N
Subject Key Identifier （主体者鍵識別子）		主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	N
Key Usage （鍵用途）		digitalSignature (ディジタル署名) nonRepudiation (否認防止) keyEncipherment (鍵暗号化) dataEncipherment (データ暗号化)	Y
Certificate Policies （証明書準則）		Policy: 1.2.392.200091.110.161.1 CPS: http://www.jasdec.com/	N
CRL Distribution Points （CRL 配布ポイント）		http://repo1.secomtrust.net/sppca/jasdec/fullcrl.crl ldap://repo1.secomtrust.net/CN=JASDEC%20CA, O=JASDEC,C=JP?certificateRevocationList	N

表 7.1-3 ファイル暗号用証明書のプロファイル

証明書フィールド（基本領域）		内容	critical
X.509 Version （X.509 証明書バージョン）		Version 3	-
Serial Number （証明書シリアル番号）		例） 123456789abcdef0	-
Signature Algorithm （署名アルゴリズム）		SHA-256 with RSAEncryption	-
Issuer （発行者）	Country （国）	C = JP	-
	Organization （組織）	O = JASDEC	
	Common Name (CN)	CN = JASDEC CA	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2008/01/01 12:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2011/01/01 12:00:00 GMT ＊有効期間 3 年以内	
Subject （主体者）	Country （国）	C = JP	-
	Organization （組織）	O = JASDEC	
	Organizational Unit （組織単位）	OU = "組織単位" ＊証明書申請時に値を決定する	
	Common Name （主体者名）	CN = "主体者名" ＊証明書申請時に値を決定する	
Subject PublicKey Info（主体者公開鍵情報）		主体者の公開鍵（2048bit）	-
証明書フィールド（x.509 v3 拡張領域）		内容	critical
Authority Key Identifier （発行者鍵識別子）		発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	N
Subject Key Identifier （主体者鍵識別子）		主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	N
Key Usage （鍵用途）		digitalSignature (ディジタル署名) nonRepudiation (否認防止) keyEncipherment (鍵暗号化) dataEncipherment (データ暗号化)	Y
Certificate Policies (証明書準則)		Policy: 1.2.392.200091.110.161.1 CPS: http://www.jasdec.com/	N
CRL Distribution Points （CRL 配布ポイント）		http://repo1.secomtrust.net/sppca/jasdec/fullcrl.crl ldap://repo1.secomtrust.net/CN=JASDEC%20CA, O=JASDEC,C=JP?certificateRevocationList	N

表 7.1-4 クライアント認証用証明書のプロファイル

証明書フィールド（基本領域）		内容	critical
X.509 Version （X.509 証明書バージョン）		Version 3	-
Serial Number （証明書シリアル番号）		例） 123456789abcdef0	-
Signature Algorithm （署名アルゴリズム）		SHA-256 with RSAEncryption	-
Issuer （発行者）	Country （国）	C = JP	-
	Organization （組織）	O = JASDEC	
	Common Name (CN)	CN = JASDEC CA	
Validity （有効期限）	NotBefore （有効性開始日時）	例） 2008/01/01 12:00:00 GMT	-
	NotAfter （有効性終了日時）	例） 2010/01/01 12:00:00 GMT ＊有効期間 2 年以内	
Subject （主体者）	Country （国）	C = JP	-
	Organization （組織）	O = JASDEC	
	Organizational Unit （組織単位）	OU = "組織単位" ＊証明書申請時に値を決定する	
	Common Name （主体者名）	CN = "主体者名" ＊証明書申請時に値を決定する	
Subject PublicKey Info（主体者公開鍵情報）		主体者の公開鍵（2048bit）	-
証明書フィールド（x.509 v3 拡張領域）		内容	critical
Authority Key Identifier （発行者鍵識別子）		発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	N
Subject Key Identifier （主体者鍵識別子）		主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	N
Key Usage （鍵用途）		digitalSignature (ディジタル署名) keyEncipherment (鍵暗号化)	Y
Certificate Policies (証明書準則)		Policy: 1.2.392.200091.110.161.1 CPS: http://www.jasdec.com/	N
CRL Distribution Points （CRL 配布ポイント）		http://repo1.secomtrust.net/sppca/jasdec/fullcrl.crl ldap://repo1.secomtrust.net/CN=JASDEC%20CA, O=JASDEC,C=JP?certificateRevocationList	N

7.2 CRL のプロファイル

表 7.2-1 CRL プロファイル

フィールド（基本領域）		内容	critical
Version（X.509CRL バージョン）		Version 2	-
Signature Algorithm（署名アルゴリズム）		SHA-256 with RSAEncryption	-
Issuer （発行者）	Country （国）	C = JP	-
	Organization （組織）	O = JASDEC	
	Common Name (CN)	CN = JASDEC CA	
This Update（更新日時）		例） 2008/09/01 00:00:00 GMT	-
Next Update（次回更新予定日時）		例） 2008/09/05 00:00:00 GMT ＊ 実更新間隔 24 時間、有効期間 96 時間	
Revoked Certificates （失効証明書）	Serial Number （失効証明書シリアル番号）	例） 1234567890	-
	Revocation Date （失効日時）	例） 2008/09/01 12:00:00 GMT	
	Reason Code （失効理由）	unspecified(未定義) Key Compromise(鍵危殆化) Affiliation Changed(内容変更) superseded(証明書更新による破棄) cessation of operation(運用停止)	
フィールド（拡張領域）		内容	critical
CRL Number （CRL 番号）		例） 1 （CRL の発行順序を示す整数値）	N
Authority Key Identifier （発行者鍵識別子）		発行者の公開鍵識別子 （公開鍵の SHA-1 ハッシュ値）	N

8. 準拠性監査と他の評価

ほふり等は、ほふり等が定期的に行う内部監査により、本 CA の準拠性監査を行います。

9. 他の業務上及び法的事項

9.1 料金

規定しません。

9.2 財務的責任

規定しません。

9.3 企業情報の機密性

9.3.1 機密情報の範囲

ほふり等が保持する本 CA に係る個人情報及び組織情報は、証明書及び CRL の一部として明示的に公開されたものを除き、機密保持対象として扱います。

9.3.2 機密情報の範囲外の情報

証明書及び CRL に含まれている情報は、機密保持対象外として扱います。その他、次の状況におかれた情報は、機密保持対象外とします。

- ほふり等の過失によらず知られた、又は知られるようになった情報
- ほふり等以外の出所から、機密保持の制限なしにほふり等に知られた、又は知られるようになった情報
- ほふり等によって独自に開発された情報
- 開示に関して証明書利用者によって承認されている情報

9.3.3 機密情報を保護する責任

ほふり等は、法の定めによる場合には、機密情報を開示することがあります。

9.4 個人情報の保護

ほふり等の個人情報保護方針については、ほふり等の Web サイトにより公開しています。

9.5 知的財産権

本 CP は、著作権を含み、ほふり等の権利に属するものとします。

9.6 表明保証

9.6.1 認証局の表明保証

9.6.1.1 IA の表明保証

ほふり等は、認証業務を遂行するにあたり次の義務を負うものとします。

・CA 私有鍵のセキュアな生成・管理
・RA からの申請に基づいた証明書の正確な発行・失効管理
・IA のシステム稼動の監視・運用
・CRL の発行・公表
・リポジトリの維持管理

9.6.1.2 RA の表明保証

ほふり等は、RA の業務を遂行するにあたり次の義務を負うものとします。

・登録端末のセキュアな環境への設置・運用
・証明書発行・失効申請における IA への正確な情報伝達
・証明書失効申請における IA への運用時間中の速やかな情報伝達

9.6.2 証明書利用者（機構加入者等である場合に限る。）の表明保証

証明書利用者（機構加入者等である場合に限る。）は、次の義務を負うものとします。

・私有鍵を紛失から防止し、第三者に対する開示又は危殆化を防止すること。
・証明書に格納されたデータや情報を修正し、変更し、又は改変しないこと。
・私有鍵の危殆化又はそのおそれが生じた場合、直ちに本 CA に失効の申請を行うこと。
・証明書に記載されているデータ又は情報に変更がある場合、本 CA に対し、直ちに失効申請を行うこと。
・証明書に対応する私有鍵を利用する前に、証明書の記載内容に誤りがないということを確認すること。
・証明書を利用する場合における電子署名方式は、ハッシュアルゴリズムとして SHA-256 を用いた RSA 方式であって、鍵長については 2048 ビットとすること。

9.6.3 検証者の表明保証

検証者は、次の事項を前提として利用する証明書を利用するものとします。

・検証者の責任において、証明書を信頼することを決定する前に、証明書利用者を適切に評価し、合理的な判断を行うこと。
・証明書の利用目的が、自己の利用目的に合致していることを承諾していること。
・CA 公開鍵を用いて振替口座簿記録事項証明書等に行われた電子署名を検証することにより、振替口座簿記録事項証明書等の発行者を確認すること。
・フィンガープリントを確認し、CA 証明書であることを確認すること。

・証明書の有効期限が満了していないことを確認すること。
・証明書が失効していないことを CRL によって確認すること。

9.6.4 他の関係者の表明保証

規定しません。

9.7 無保証

ほふり等は、本 CP「9.6.1 認証局の表明保証」の内容に関し発生した損害については、ほふり等に故意又は重過失がある場合を除き、一切の責任を負わないものとします。

9.8 責任の制限

ほふり等は、本 CP「9.6.1 認証局の表明保証」の内容に関し、次の場合には、責任を負わないものとします。

・ほふり等に起因しない不法行為、不正使用又は過失等により発生する一切の損害
・証明書利用者（機構加入者等である場合に限る。）が自己の義務の履行を怠ったために生じた損害
・証明書利用者（機構加入者等である場合に限る。）のシステムに起因して発生した一切の損害
・ほふり等、証明書利用者（機構加入者等である場合に限る。）のハードウェア、ソフトウェアの瑕疵、不具合又はその他の動作自体によって生じた損害
・ほふり等の責に帰することのできない事由で証明書及び CRL に公開された情報に起因する損害
・ほふり等の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
・証明書の使用に関して発生する取引上の債務等、一切の損害
・現時点の予想を超えた、ハードウェア的又はソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
・天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、ほふり等の業務停止に起因する一切の損害

9.9 補償

本 CA が発行する証明書を申請、受領、信頼した時点で、証明書利用者（機構加入者等である場合に限る。）には、本 CA 及び関連する組織等に対する損害賠償責任及び保護責任が発生するものとします。当該責任の対象となる事象には、損失、損害、訴訟、あらゆる種類の費用負担の原因となるようなミス、怠慢な行為、各種行為、履行遅滞、不履行等の各種責任が含まれます。

9.10 有効期間と終了

9.10.1 有効期間

本 CP は、ほふり等のポリシ承認機関の承諾により有効となります。

9.10.2 終了

本 CP は、本 CA の終了と同時に無効となります。

9.10.3 終了の効果と効果継続

証明書利用者（機構加入者等である場合に限る。）とほふり等との間で利用契約等を終了する場合、又は、本 CA 自体を終了する場合であっても、その性質上存続されるべき条項は、終了の事由を問わず証明書利用者（機構加入者等である場合に限る。）及びほふり等に適用されるものとします。

9.11 関係者間の個別通知と連絡

ほふり等は、証明書利用者（機構加入者等である場合に限る。）及び関係者に対する必要な通知をホームページ上、電子メール又は書面等によって行います。

9.12 改訂

9.12.1 改訂手続

本 CP は、本 CA の判断によって適宜改訂され、ほふり等のポリシ承認機関の承認によって発効するものとします。

9.12.2 通知方法及び期間

本 CP を変更した場合には、速やかに変更した本 CP を通知することにより、証明書利用者（機構加入者等である場合に限る。）及び関係者に対して知らせるものとします。

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 紛争解決手続

証明書の利用に関し、ほふり等に対して訴訟、仲裁を含む解決手段に訴えようとする場合には、ほふり等に対して事前にその旨を通知しなければなりません。なお、仲裁及び裁判地は東京都区内における紛争処理機関を専属的管轄とします。

9.14 準拠法

ほふり等又は証明書利用者（機構加入者等である場合に限る。）の所在地にかかわらず、本 CP の解釈、有効性及び証明書の利用にかかわる紛争については、日本国の法律が適用されるものとします。

9.15 適用法の遵守

規定しません。

9.16 雑則

規定しません。

9.17 その他の条項

規定しません。