エンドエンティティは、証明書所有者と署名検証者（以下、検証者）から構成される。

証明書所有者とは、証明書発行申請を行い、CA により証明書を発行される個人あるいは組織をさす。証明書所有者の範囲は次の通りとする。

XXX における事業活動、及び研究活動に関与する個人あるいは組織

1.3.4. 適用範囲

署名検証用証明書：XXX における事業活動及び研究活動に関与する個人あるいは組織
認証用証明書　　：XXX における事業活動及び研究活動に関与する個人あるいは組織

1.4. 問合せ先

1.4.1. 主管部署

XXX　管理部

1.4.2. 照会窓口

XXX　管理部

1.4.3. 電子メールアドレス

1.5. 用語集

- 患者／保健医療福祉サービス利用者(patient/consumer)
  医療健康関連サービスを受給する人と医療健康情報システム関係者。(ISO/TS17090-3 3.1.6)

- 検証者(relying party)
  証明書を受け取る者で、その証明書を用いて検証することにより、その証明書及び、又はディジタル署名に依拠して行動する者。(ISO/TS17090-3 3.3.21)

・ 非専門職（非公的資格ヘルスケア専門職(non-regulated health professional)）
　ヘルスケア組織に雇われている人で、ヘルスケア専門資格者でない人。例として、予約を処理する受付係又は秘書、あるいは患者の健康保険を確認する責任を負っている業務管理者。(ISO/TS17090 3.1.5)

・ 公的資格専門資格者(regulated health professional)
　国家レベルで認定された団体により、あるヘルスケアサービスを行う資格を与えられた人。(ISO/TS17090-3 3.1.8)

・ CA(Certification Authority)　：　“認証局”

・ CP(Certificate Policy)　：　“証明書ポリシ”

・ CPS(Certification Practices Statement)：“認証実施規程”

・ CRL(Certificate Revocation List)　：　“証明書失効リスト”、失効リスト”

・ hcRole(health care Role)　：　保健医療福祉分野での役割、資格。

・ RA(Registration Authority)　：　“登録局”

・ IA（IssuingAuthority）：
　”発行局”CA の内、証明書の発行、失効等の証明書管理機能を表す場合に使用。

2. 一般条項

2.1. 義務

2.1.1. 認証局の義務

本 CA は、登録プロセス、証明書に含まれる情報の検証、証明書の作成、発行、失効、停止、及び更新の管理を含めて、証明書の発行と管理のすべての局面に責任がある。本 CA は、本 CA のサービスと運用のすべての局面が CP の要件、表現、及び保証と本 CPS に従って行われることを保証する責任がある。なお、本 CA では証明書の停止は行わない。

本 CA のサービスを以下に列挙する。

2.1.1.1. 証明書の発行及び失効の通知

IA は、証明書所有者の識別名を持つ証明書が発行されるときには、各証明書所有者に通知するものとする。

IA は、証明書所有者の識別名を持つ証明書が失効されるときには、証明書所有者に通知するものとする。

IA は、本 CPS 4.4. に従って、検証者が証明書失効リスト（CRL）を入手できるようにするものとする。

2.1.1.2. CA の表現の正確性

IA が証明書を発行するとき、証明書所有者に証明書を発行したことと、証明書に記載されている情報が CP 及び本 CPS に従って検証されたことを本 CA が保証する。証明書所有者に対して証明書を活性化するデータを安全に送付した時点で、このような検証が行われたことの通知とする。

本 CA は、CP 及び本 CPS に基づく証明書所有者の権利と義務を、各証明書所有者に通知するものとする。この通知は、証明書所有者の同意書をもって代替するものとする。この通知は、この CP に基づいて発行された証明書の許される用途、証明書所有者の鍵の保護に関する責任、及びサービス提供の変更又は本 CPS の変更の伝達も含めて、証明書所有者と CA 及び RA 間の通信手続きの記述を含む。

本 CA は、鍵の危殆化のおそれ、証明書又は鍵の更新、サービスの取消し、及び紛争解決を処理するための手続を証明書所有者に通知する。

2.1.1.3. 証明書の申請から発行までの期間

本 CA は、証明書所有者が鍵活性化物を生成後、鍵活性化プロセスを完了するまでに、最大で２週間を必要とするものとする。

2.1.1.4. 証明書の失効と更新

IA は、証明書の期限切れ、失効、及び更新のいかなる手続も、CP 及び本 CPS の該当する条項に従っていることを保証しなければならない。CRL 配付点のアドレスは、証明書に記述する。

2.1.1.5. 私有鍵の保護

CA は自身が保有又は格納する私有鍵及び活性化データが本 CPS 6.2、6.3、及び 6.4 に従って確実に保護されていることを保証するものとする。

2.1.1.6. CA 私有鍵の使用制限

本 CA は、CA の証明書署名用私有鍵が、証明書及び証明書失効リストに署名するためだけに使用されることを保証する。本 CA は、CA 運用に必要な操作のためだけに CA 職員に発行した私有鍵が、この目的のためだけに使用されることを保証する。

2.1.2. 登録局の義務

RA は、最初の登録の際の証明書所有者の身元とヘルスケア上の役割の検証を行わなければならない。

また、RA は、証明書失効申請及び認証局失効申請を正確かつタイムリーに CA に渡していることを信頼されなければならない。

RA は、次のことを行うものとする。

1. RA がオンラインでその責務を果たしている場合は、その署名私有鍵が証明書申請に必要な行為のためだけに使用されることを保証する。
2. 証明書所有者の身元を認証したことを証明する。
3. 証明書申請情報等を署名暗号電子メール等の安全な方法により IA に伝送し、申請書類、登録記録等を安全な方法により保管する。
4. （証明書失効申請を行う場合は）CP 及び本 CPS 3.4.2 に従って失効申請を開始する。

2.1.2.1. 証明書の失効申請

RA は、証明書失効申請の取り扱いを行うことができる。RA は、失効申請者の身元及び失効理由を確認し、それが妥当なものであると判断した場合には、CA に対し、証明書失効を要求することができる。

2.1.2.2. 監査

RA の信頼性に対する保証を提供するため、及び内部監査を実施する職員に情報を提供するために、RA は監査可能でなければならない。そのために、RA の作業履歴を残さなければならない。

2.1.2.3. 保管

将来の検証に備え、証明書がどのように、また、なぜ生成されたかを管理できるように、本 CA 内の RA は、証明書の作成要求又は失効要求などのイベントを、該当する証明書の有効期間満了後、10 年間保管するものとする。

2.1.3. 証明書所有者の義務

証明書所有者は、次のことを行うものとする。

1. 証明書申請の記述の正確さを保証し、証明書を受け入れることによって、証明書に含まれている情報のすべてが真実であることを承認する。
2. 私有鍵及び（適用可能な場合は）鍵トークン（鍵配付媒体）を保護し、それらの紛失、開示、変更、又は無許可使用を防止するために妥当な措置をすべて取る。
3. 自分の私有鍵の紛失、開示、又は無許可使用を防止するためにあらゆる努力を払う。
4. 自分の私有鍵の実際の紛失、開示、又はその他の危殆化、又はそれらが疑われるときには、直ちに RA に通知する。
5. 証明書情報、システムの管理責任者、組織所在地などの変更を RA に通知する。
6. CP 及び本 CPS、又は証明書所有者の責任を平易なことばで明瞭に述べた PKI 開示文書を読む。
7. CP 及び本 CPS に従って鍵ペアを使用する。
8. 本 CA より証明書の発行を受ける証明書所有者は、事前の取決めに従い、義務・責任を負い、すべての取決め事項に同意する。

2.1.4. 検証者の義務

本 CA により発行される証明書の検証者は、次の場合に限り、証明書に依拠する権利を保有する。

1. 証明書が使用される目的が、CP 及び本 CPS の下で適切であった場合
2. 信頼することが信頼の時点で、検証者に知られているすべての状況を考慮に入れて、妥当であり、誠意によるものである場合
3. 証明書が失効又は停止されていないことを確認することによって、検証者が証明書の現在の有効性を確認した場合
4. 適用可能な場合は、検証者がデジタル署名の現在の有効性を確認した場合
5. 責任と保証の適用限界を承認した場合

2.1.5. リポジトリの義務

証明書は検証者にとって入手可能であるものとする。

CRL は、本 CPS 4.4.9 の要件に従って、検証者にとって入手可能であるものとする。

2.2. 責任

2.2.1. 認証局の責任

本 CA の責任は、CA 部門の怠慢行為及び CA が CP 及び本 CPS の条項に従わなかったことが原因で検証者がこうむった直接損害のみに限定する。

本 CA は、以下のことに対して責任を持つ。

1. 鍵配付プロセス中の私有鍵の危殆化。
2. 身元確認と認証に関する文書化されたポリシ及び手続が遵守されたことが証明できない限り、個人の身元とそれに関連付けられたデジタル署名及びその他の認定情報との誤った結合。

   この責任は、CA が結合に誤りがあることを知っていたか疑っていた状況、又は知っているべきか疑うべき状況にも及ぶ。
3. CA は、その失効ポリシに従って証明書を失効しなかったこと。
4. CA は、その失効ポリシで規定されていない理由のために証明書を失効したこと。
5. 私有鍵の証明書所有者による紛失。

   特に、次の場合には、CA には責任がないとみなす。
6. 私有鍵が CA において危殆化したこと、または鍵生成プロセス中に、文書化されたポリ

シ及び手続きが遵守されなかったことで、私有鍵がより危殆化されやすくしたか、私有鍵の実際の発覚をもたらしたことが証明されないばあいにおいて、CA が生成する私有鍵が危殆化したこと。

7. 文書化されたポリシ及び手続きが遵守されなかったことが偽造をもたらしたか、ポリシ及び手続きが偽造を許したことを示すことができた場合を除いた、偽造された署名。

2.2.2. 登録局の責任

RA の責任は、RA 部門の怠慢行為に限定する。

RA の責任は、次のことに関しては限定されるものではない。

1. RA は、身元確認と認証に関する文書化されたポリシ及び手続が遵守されたことが証明できない限り、個人のアイデンティティとそれに関連付けられたデジタル署名及びその他の認定情報との誤った結合に責任がある。この責任は、RA が結合されたサブジェクト情報が誤りであると知っていたか、疑っていた状況又は知っているべきか疑うべき状況にも及ぶ。
2. RA は、その失効ポリシに従って証明書を失効しなかったことに対して責任がある。
3. RA は、その失効ポリシで規定されていない理由のために証明書を失効したことに対して責任がある。

2.3. 財務上の責任

CAは、その運営を維持し、且つその義務を履行するために十分な財務的基盤を有するものとする。

2.4. 解釈及び執行

2.4.1. 準拠法

本認証局運用規程は、日本国内の法律及び規制に基づいて、解釈される。また、本CPSはISO 17799:2000に準拠している。

2.4.2. 分割、存続、合併及び通知

本 CPS は、CPS のひとつのセクションが正しくないか無効であると判断した場合でも、

更新されるまで、他のセクションは事実上有効に存続するものとする。

2.4.3. 紛争解決の手続

本認証サービスの利用について、CP及び本CPSの解釈、有効性及び本CAが行なう認証書発行サービスに関わる紛争については、神戸地方裁判所を第一審の専属管轄裁判所とする。

2.5. 手数料

原則無償提供とするが、IC カードの紛失に伴う再発行処理については、別途定める再発行手数料を徴収するものとする。

2.6. 情報の公表とリポジトリ

2.6.1. CA に関する情報の公開

CA は、次のものを証明書所有者と検証者にとって入手可能にするものとする。

1. CA によって、又は CA に代わって管理され、適用する本 CPS を含んでいる利用可能な Web サイトの URL 等
2. 本 CPS の下に発行された各証明書（証明書所有者の証明書を公開する場合）
3. 本 CPS の下で発行された各証明書の現在の状態
4. CA が運営の基準としている認定又はライセンス基準（CA が運営されている管轄区域でそれらの認定又はライセンス基準が適用可能な場合）

2.6.2. 公表の頻度

本 CA は、CA に関する情報が変更されたときにはただちに、その情報を公開するものとする。証明書失効についての情報は、本 CPS4.4 に従うものとする。

2.6.3. 公表される情報に対するアクセス制御

CP、CPS、証明書及びそれらの証明書の現在の状態などの公開情報は、読み取り専用とする。

2.6.4. リポジトリ

本 CA は証明書所有者及び検証者が CRL 情報にアクセスできるようにリポジトリを維持管理する。

なお、リポジトリは常に最新に保たれ（証明書失効から２４時間以内、状況によってはさらに早く更新される）、１日２４時間、１年３６５日利用可能とする。ただし、定期保守業務等により、一時的に利用できない場合がある。

2.7. 準拠性監査

2.7.1. 監査頻度

CP 及び本 CPS に従って証明書を発行する本 CA が、CP 及び本 CPS に完全に従っているかについて、CA 準拠性監査を行う。準拠性監査は、1 年より長くない間隔で、資格を持った独立した第三者によって行われるものとする。

2.7.2. 監査者の身元・資格

本 CA は、CA 業務を直接行っている部門から独立した、PKI に精通した第三者に定期監査を委託するものとする。

2.7.3. 監査者と被監査者の関係

監査者は、本 CA とは別個の組織に属することによって、被監査者から独立しているものとする。監査者は、被監査者に対しての特別な利害関係を持たないものとする。

2.7.4. 監査テーマ

定期監査では、本 CA が CP 及び本 CPS に準拠しているかを監査する。

主な監査項目は以下の通りである。

- IA の業務（証明書の発行、失効／CRL の発行　など）
- RA の業務（登録申請処理　など）
- 鍵管理
- 設備、環境、ネットワーク情報
- ソフトウェアやハードウェアの状況

2.7.5. 監査指摘事項への対応

監査報告書で指摘された事項（通常改善事項又は緊急改善事項）に関しては、セキュリティポリシ委員会（以下、ポリシ委員会）が対応を決定する。この指摘事項に関しては、ポリシ委員会が、セキュリティ技術の最新の動向を踏まえ、問題が解決されるまでの対応策も含め、その措置を本サービスの CA 運用責任者に指示する。

ポリシ委員会はあらかじめ監査事項への具体的対応を CPS により定めておく。

- 危機的

  本 CPS の不可欠なセクションに従っていないことが指摘された場合には、CA は直ちに業務を一時停止し、是正しなければならない。また、CA の証明書は失効され、是正後の監査で許可が出た場合には再び CA 証明書の発行を受け、CA 業務を再開する。
- 重度

  本 CPS の重要な要素に従っていないことが指摘された場合には、CA は指摘後数日以内に是正措置を行わなければならない。改善できなかった場合には、重度から危機的な欠陥への格上げとなる。
- 部分的

  重大な欠陥になる十分な可能性はないが、CA 運用の完全性に影響を与える可能性がある指摘事項の場合には、CA は 30 日以内に是正措置を取らなければならない。この期間で是正できなかった場合には、重度の欠陥へ格上げされる。
- 軽度

  CA 運用の完全性に対する全体的な影響を軽減するために対処すべき指摘事項の場合には、CA は、次の定期監査までに是正措置を取らなければならない。この期間で是正できなかった場合には、部分的な欠陥へ格上げされる。

講じられた対策の結果はポリシ委員会、及び、その関連組織に報告され、評価されるとともに、次の監査において確認するものとする。

2.7.6. 監査結果の通知

監査者によって証明書の信頼性に影響する重大な欠陥が発見された場合には、本 CA 又は RA は、証明書所有者及び検証者に直ちに通知するものとする。また、本認証局のルート認証局の認証局業務責任者にも通知するものとする。

2.8. 機密保持

2.8.1. 秘密扱いとする情報

1. 証明書所有者の個人情報で、RA が本人確認の目的で収集をしたが、証明書に含まれない情報は、秘密に保たれるものとする。（身分証明書、経歴調査、自宅住所、連絡先の詳細など）この情報の一部は、証明書所有者の同意を得て、その証明書所有者のディレクトリリスティングに含めることがある。
2. 私有鍵

2.8.2. 秘密扱いとしない情報

1. 公開鍵
2. 本認証局認証実施規程
3. ヘルスケア専門資格者と非公的資格ヘルスケア専門職の役割
4. ヘルスケア上の専門性

2.8.3. 証明書失効及び一時停止情報の開示

本 CA は、証明書所有者の証明書失効の理由、及び証明書所有者の証明書失効の理由に関する情報を秘密に保つものとする。なお、本 CA は、一時停止は行わないため、一時停止情報は開示しない。

2.8.4. 法的執行機関への情報開示

秘密情報は、証明書所有者の明白な同意に基づいて、または法律の下での要求にしたがってだけ公開されるものとする。

2.8.5. 民事手続上の情報開示

秘密情報は、証明書所有者の明白な同意に基づいて、又は法律の下で認められた法廷からの命令の提示によってだけ公開されるものとする。

2.8.6. 証明書所有者の要求に基づく情報開示

秘密情報は、要求している証明書所有者からの（証明書所有者のデジタル署名のある）認

証された電子メール、又は署名付き文書による要求に従って、証明書所有者によって指名された関係者に開示されるものとする。

2.8.7. その他の理由に基づく情報開示

CAは、前述した以外の事由に基づく情報開示を一切行なわないものとする。また、秘密情報は、法律により認められた方法による要求に従ってのみ開示されるものとする。

2.9. 知的財産権

本CPSでは、規定をしない。

3. 所有者の識別方法と本人確認方法

3.1. 新規発行時での所有者の本人確認方法

3.1.1. 名前の形式

適用する CP に従う。

3.1.2. 名前を意味あるものとする必要性

証明書を効果的に使用するには、証明書に現れる相対識別名が検証者によって理解され、試用される必要がある。これらの証明書で使用される名前は、それらが割り当てられた証明書所有者を意味のある方法で識別できるものとする。

3.1.3. 各種の名前形式を解釈するための規則

認証書に記載される名前（DN）は、登録局が本人確認の際に、添付された公的証明書に記載されている内容に、認証局側で独自に採番するID を付加したものとする。

3.1.4. 名前の一意性

証明書に記載されるサブジェクト識別名は、あいまいさがなく、個別の証明書所有者に一意であるものとする。

3.1.5. 所有者の名前を決定する際の紛争解決手続き

証明書申請者の名前（DN）に関する紛争が発生した場合については、ポリシ委員会が全ての決定を行なうものとする。また、その解決手段の詳細については、ポリシ委員会において協議するものとする。

3.1.6. 登録商標の認識・認証・役割

登録商標使用の権利については、登録商標所持者が全ての権利を留保するものとする。

3.1.7. 私有鍵の所有を証明するための方法

CA に対し証明書発行要求を行う際には、公開鍵証明書と私有鍵との対応を証明するために、CA からのチャレンジに署名を行い、私有鍵の所有を証明するものとする。

3.1.8. 組織の認証

適用する CP に従う。

3.1.9. 個人の認証

適用する CP に従う。

3.2. 通常の更新

3.2.1. CA の通常更新

CA 情報の通常の鍵更新は、元の記録が作成されたときに使用された元の文書に基づいて行われるものとする。

3.2.2. RA の通常更新

RA 情報の通常の鍵更新は、元の記録が作成されたときに使用された元の文書に基づいて行われるものとする。

3.2.3. 証明書所有者の通常更新

証明書所有者情報の通常更新は、元の記録が作成されたときに使用された元の文書または記録を再び参照することによって行われるものとする。元の文書が無効になっているか破棄されていた場合は、元の文書相当の証明書所有者を特定できる代替文書を使用するものとする。

3.3. 失効後の更新－鍵が危殆化していない場合

3.3.1. CA の失効後の更新－鍵が危殆化していない場合

証明書が鍵危殆化以外の理由で失効された後の鍵の更新は、認証局を認定するために使用された元の情報の再提出を必要とするものとする。

3.3.2. RA の失効後の更新－鍵が危殆化していない場合

証明書が鍵危殆化以外の理由で失効された後の情報更新は、RA を認定するために使用された元の情報の再提出を必要とするものとする。

3.3.3. 証明書所有者の失効後の更新－鍵が危殆化していない場合

証明書所有者の通常の更新は、証明書所有者情報の元の記録が作成されたときに使用された元の文書の提出、または使用された元の記録の参照を必要とするものとする。元の文書が無効になっているか廃棄されていた場合は、元の文書相当の証明書所有者を特定できる代替文書を使用するものとする。

3.4. 失効申請

3.4.1. CA の失効申請

本 CA が失効申請をする場合には、ルート CA に申請する。

1. 証明書を特定する。
2. 証明書が失効されるべき理由を述べる。
3. 申請書に私有鍵で署名して、メッセージを暗号化し、関連するドメイン CA に送信する方法や CA を認証できる方法により行われるものとする。

3.4.2. RA の失効

RA が CA に失効申請を行うときには、次のようにするものとする。

1. 失効を要求する証明書を特定する。
2. 証明書が失効されるべき理由を述べる。
3. 申請書に私有鍵で署名して、メッセージを暗号化し、関連するドメイン CA に送信する方法や失効申請者を認証できる方法により行われるものとする。

3.4.3. 証明書所有者の失効

証明書所有者が本 CA に失効申請を行うときには、以下の手順に従うものとする。

1. 失効を申請する証明書を特定する。
2. 証明書が失効されるべき理由を述べる。
3. 申請に私有鍵で署名して、メッセージを暗号化し、関連したドメイン CA に送信する。

私有鍵を含んでいるトークンが紛失又は盗まれた場合等証明書所有者がデジタル署名付きの要求を開始できない場合は、他の何らかの手段を用い、証明書を取得するために提供したものと同等の本人確認のための書類を添える。

4. 運用上の要件

4.1. 証明書の申請

証明書の発行申請者は、RA に証明書の発行申請を行う。申請に必要な書類を以下に示す。

（1） 組織の場合

・認証局証明書発行申請書
・登記簿謄本又は法人印鑑証明書
・保健医療福祉機関であることを証明する書類（開業届け等の写し）
・申請者（代表者）の本人確認
    1) 住民票の提出
    2) 官公署の発行した資格証明書、運転免許証、旅券その他本人であることを証明できる書面であって、本人の写真を添付してあるものの提示
    3) 本人であることを証明できる 2) 以外の官公庁の発行した書面（各種健康保険の被保険者証、各種年金の年金手帳等）の 2 種類以上の提示

（2） 個人の場合

・認証局証明書発行申請書
・国家資格保有の確認（関係官庁によって発行された職業上の国家資格免許状や身分証明書またはその写し）
・申請者（代表者）の本人確認
    1) 住民票の提出
    2) 官公署の発行した資格証明書、運転免許証、旅券その他本人であることを証明できる書面であって、本人の写真を添付してあるものの提示
    3) 本人であることを証明できる 2) 以外の官公庁の発行した書面（各種健康保険の被保険者証、各種年金の年金手帳等）の 2 種類以上の提示

4.2. 証明書の発行

RA は、CP 及び本 CPS に基づく発行申請者の審査、本人確認を行う。審査適合の場合、RA は IA に発行申請を行う。IA は、RA からの発行申請を受け、証明書所有者の私有鍵、公開鍵を生成、公開鍵証明書を生成する。その後、RA に生成した私有鍵、公開鍵、証明書を送る。

4.3. 証明書の受理

RA は IA より証明書所有者の私有鍵、証明書を受け取り、IC カードに格納する。そして、証明書所有者に直接 IC カードを渡す。

4.4. 証明書の一時停止と失効

4.4.1. 証明書の失効事由

IA は、次の場合に証明書を失効するものとする。

1. 証明書所有者が、CP、本 CPS、又はその他の契約、規制、あるいは、有効な証明書に適用される法に基づく義務を満たさなかった場合
2. 私有鍵の危殆化が認識されたか、妥当な疑いがある場合
3. 証明書に含まれる該当のサブジェクト情報が正確でなくなった場合
4. 証明書所有者の所属組織が変更された場合（例えば、ヘルスケア専門資格者が特定の組織から退職した場合）
5. CA が、CP 及び本 CPS に従って証明書が適切に発行されなかったと決定した場合。
6. いかなる理由でも、証明書所有者または認定ヘルスケア提供者の認定者の要求があった場合。

証明書所有者、RA 及び認定者は、証明書のサブジェクト情報が不正確であることに気づいた場合には、CA に知らせる義務がある。

4.4.2. 証明者の失効申請が出来る者

証明書の失効は、次の 1 人又はそれ以上の者によって要求されるものとする。

1. その人の名前で証明書が発行された証明書所有者
2. IA の職員
3. IA と連携している RA の職員

4.4.3. 失効要求手続き

証明書失効手続きは以下のように行うものとする。

1. 失効要求者は証明書失効申請書を RA に提出する。

2. RA は、失効を要求しているエンティティが、本 CPS4.4.2.で規定された範囲の者であることを確認する。
3. 要求者が証明書所有者の代理人として行動している場合は、要求者が失効をもたらすに十分な権限を持っていることを確認する。
4. 失効事由を確認し、それが真実であると実証された場合は、RA は CA に失効申請を行う。
5. CA は、RA からの失効申請に基づき、証明書失効を行い、CRL を発行する。

4.4.4. 失効要求の猶予期間

証明書の失効要求の結果として取られる処置は、受領後直ちに開始されるものとする。

4.4.5. 一時停止事由

本 CA は、一時停止を行わないものとする。

4.4.6. 一時停止を申請できる者

本 CA は、一時停止を行わないものとする。

4.4.7. 証明書の一時停止手続き

本 CA は、一時停止を行わないものとする。

4.4.8. 一時停止期間の限度

本 CA は、一時停止を行わないものとする。

4.4.9. 失効リスト発行の頻度

証明書の失効を行った場合、又は、本 CA の私有鍵に危殆化等が発生した場合は、証明書失効リストを即時に発行する。証明書失効があるなしにかかわらず、証明書失効リストは 1 日に 1 回発行する。

ただし、CA 私有鍵の危殆化等が発生した場合は、CRL/ARL をただちに発行するものとする。

4.4.10. 失効リスト確認の必要性

検証者は、別のエンティティの公開鍵を使い始めるときは常に、CRL/ARL をチェックすべきである。検証者は、CRL/ARL を少なくとも毎日、失効の有無をチェックし証明書状態の確認を行うものとする。

4.4.11. オンラインでの失効確認に対する可用性

本 CA は、保守等にてシステムを停止する以外においては、検証者に対して、CRL のチェックを可能とする。

4.4.12. オンラインでの失効確認の必要性

署名して応答する機能を備えたオンライン証明書状態チェックのサーバを利用しオンライン失効チェックを可能とする場合は、サーバと証明書所有者が安全な通信を確立できるようにするものとする。証明書の真正性の検証は CA のリポジトリに格納されている CRL にて確認するものとする。

4.4.13. その他利用可能な失効確認公表手段

本 CA ではその他の失効確認公表手段は用いない。

4.4.14. その他利用可能な失効確認公表手段における確認要件

本 CA ではその他の失効確認公表手段は用いない。

4.4.15. 鍵の危殆化に関する特別な要件

CA 署名鍵の危殆化の際には、CA はルート CA 及び関連組織に直ちに通知するものとする。

4.5. セキュリティ監査の手続き

4.5.1. 記録するイベントの種類