

よんでん電子入札対応認証サービス 認証業務規程

Ver.2.16

四国電力株式会社

改訂履歴

| Version | 変更内容 | 日付 | 変更者/ 作成者 | 日付 | 承認者 |
|---------|--|------------|-------------|------------|------|
| 1.00 | 初版制定 | 2003.10.02 | 真鍋紳一 | 2003.10.02 | 仲田俊輔 |
| 1.01 | ブリッジ認証局との相互認証接続申請に伴う変更修正 | 2003.12.08 | 真鍋紳一 | 2003.12.08 | 仲田俊輔 |
| 2.00 | RA 認証業務室要件の変更に伴う修正(変更認定) | 2004.06.18 | 真鍋紳一 | 2004.06.18 | 仲田俊輔 |
| 2.01 | 以下の項目について表現の見直し ・利用者の義務 ・発行申込手続き ・発行申込書類 ・発行申込の審査と承認 ・失効事由 ・失効手続き ・利用者への署名鍵の送付 ・仕様変更の手続き | 2004.10.02 | 真鍋紳一 | 2004.10.02 | 仲田俊輔 |
| 2.02 | 以下の項目について表現の見直し ・個人情報の取扱い | 2005.10.02 | 真鍋紳一 | 2005.10.02 | 井上哲司 |
| 2.10 | 認証局署名鍵更新に伴う修正(変更認定) | 2008.07.30 | 真鍋紳一 | 2007.07.30 | 小延隆弘 |
| 2.11 | 以下の項目について表現の見直し ・コミュニティと適用範囲 ・名前の意味に関する要件 ・署名鍵の所有を証明するための方法 ・利用組織の認証 ・利用者の認証 ・利用者証明書の失効 ・失効手続き ・電子証明書及び失効情報プロファイル ・商業登記簿謄本を登記事項証明書(商業登記簿謄本)に見直し | 2008.9.19 | 真鍋紳一 | 2008.9.19 | 小延隆弘 |
| 2.12 | 以下の項目について表現見直し ・認証局関連情報のリンク先 | 2008.11.07 | 真鍋紳一 | 2008.11.07 | 小延隆弘 |
| 2.13 | 配達記録郵便廃止に伴う修正 | 2009.03.02 | 真鍋紳一 | 2009.03.02 | 小延隆弘 |
| 2.14 | 発行申込受付停止予定の追加に伴う修正 | 2009.07.21 | 真鍋紳一 | 2009.07.21 | 小延隆弘 |
| 2.15 | 以下の項目について表現の見直し ・料金掲載の URI ・外国人の実在性の確認事項 ・在職証明書兼同意書の記載事項 | 2009.09.08 | 真鍋紳一 | 2009.09.08 | 小延隆弘 |

| | | | | | |
|------|---|-----------|------|-----------|------|
| | ・戸籍謄本を戸籍全部事項証明書(戸籍謄本)に、戸籍抄本を戸籍個人事項証明書(戸籍抄本)に見直し | | | | |
| 2.16 | 連絡先部署名の変更 | 2011.6.29 | 畔地宙彦 | 2011.6.29 | 真鍋紳一 |

目次

| | | |
|-------|---------------|----|
| 1 | はじめに | 8 |
| 1.1 | 概要 | 8 |
| 1.2 | 識別 | 8 |
| 1.3 | コミュニティと適用範囲 | 9 |
| 1.3.1 | 認証局 | 9 |
| 1.3.2 | 発行局 (IA) | 9 |
| 1.3.3 | 登録局 (RA) | 9 |
| 1.3.4 | 利用者 | 10 |
| 1.3.5 | 利用組織 | 10 |
| 1.3.6 | 検証者 | 10 |
| 1.3.7 | BCA | 10 |
| 1.3.8 | 電子証明書の適用範囲 | 10 |
| 1.4 | 連絡先 | 10 |
| 2 | 一般的な規定 | 12 |
| 2.1 | 義務 | 12 |
| 2.1.1 | 認証局の義務 | 12 |
| 2.1.2 | 利用者の義務 | 13 |
| 2.1.3 | 利用組織の義務 | 14 |
| 2.1.4 | 検証者の義務 | 15 |
| 2.2 | 責任 | 15 |
| 2.2.1 | 認証局の責任 | 15 |
| 2.2.2 | 利用者の責任 | 16 |
| 2.2.3 | 利用組織の責任 | 16 |
| 2.3 | 財務上の責任 | 16 |
| 2.3.1 | 賠償責任 | 16 |
| 2.3.2 | 免責事項 | 16 |
| 2.4 | 解釈及び執行 | 17 |
| 2.4.1 | 準拠法 | 17 |
| 2.4.2 | 分離、存続、合併、通知 | 17 |
| 2.4.3 | 紛争解決の手順 | 17 |
| 2.5 | 料金 | 17 |
| 2.6 | リポジトリにおける情報公開 | 17 |
| 2.6.1 | 認証局情報の公開 | 17 |
| 2.6.2 | 公開情報の更新頻度 | 18 |
| 2.6.3 | アクセス管理 | 18 |
| 2.6.4 | リポジトリの運用 | 18 |
| 2.7 | 準拠性監査 | 18 |
| 2.7.1 | 準拠性監査の実施頻度 | 18 |
| 2.7.2 | 監査人の選任 | 18 |
| 2.7.3 | 監査人と監査対象者の関係 | 19 |
| 2.7.4 | 監査項目 | 19 |
| 2.7.5 | 監査指摘事項への措置 | 19 |

| | | |
|-------|-----------------------|----|
| 2.7.6 | 監査結果の公開..... | 19 |
| 2.8 | 秘密情報..... | 19 |
| 2.8.1 | 秘密情報の種類..... | 19 |
| 2.8.2 | 個人情報の取扱いについて..... | 19 |
| 2.8.3 | 秘密とみなされない情報..... | 19 |
| 2.8.4 | 電子証明書失効情報の公開..... | 20 |
| 2.8.5 | 法執行機関への情報開示..... | 20 |
| 2.8.6 | 民事手続き上の情報開示..... | 20 |
| 2.8.7 | 名義人の申込による情報開示..... | 20 |
| 2.8.8 | その他の情報開示..... | 20 |
| 2.9 | 知的財産権..... | 20 |
| 3 | 本人の識別と認証..... | 21 |
| 3.1 | 利用者証明書の発行..... | 21 |
| 3.1.1 | 名前の型..... | 21 |
| 3.1.2 | 名前の意味に関する要件..... | 21 |
| 3.1.3 | 名前形式を解釈するための規則..... | 22 |
| 3.1.4 | 名前の一意性..... | 22 |
| 3.1.5 | 名前に関する紛争の解決手順..... | 22 |
| 3.1.6 | 商標の認識・認証・役割..... | 22 |
| 3.1.7 | 署名鍵の所有を証明するための方法..... | 23 |
| 3.1.8 | 利用組織の認証..... | 23 |
| 3.1.9 | 利用者の認証..... | 23 |
| 3.2 | 利用者証明書の更新..... | 24 |
| 3.3 | 利用者証明書失効後の再発行..... | 24 |
| 3.4 | 利用者証明書の失効..... | 24 |
| 4 | 運用上の要件..... | 26 |
| 4.1 | 利用者証明書の発行申込..... | 26 |
| 4.1.1 | 発行申込手続き..... | 26 |
| 4.1.2 | 発行申込書類..... | 26 |
| 4.1.3 | 発行申込の審査と承認..... | 28 |
| 4.2 | 利用者証明書の発行..... | 28 |
| 4.3 | 署名鍵及び利用者証明書の受領..... | 29 |
| 4.4 | 電子証明書の失効..... | 29 |
| 4.4.1 | 失効事由..... | 29 |
| 4.4.2 | 失効要求を行う者..... | 30 |
| 4.4.3 | 失効手続き..... | 30 |
| 4.4.4 | CRL/ARLの更新頻度..... | 33 |
| 4.4.5 | CRL/ARL確認の要件..... | 34 |
| 4.4.6 | 一時停止..... | 34 |
| 4.5 | セキュリティ監査手続き..... | 34 |
| 4.5.1 | 記録されるイベント..... | 34 |
| 4.5.2 | 監査の頻度..... | 34 |
| 4.5.3 | 監査証跡の保存期間..... | 34 |
| 4.5.4 | 監査証跡の保護..... | 34 |

| | | |
|-------|-----------------------------|----|
| 4.5.5 | 監査証跡のバックアップ手順 | 34 |
| 4.5.6 | 監査証跡の記録システム | 34 |
| 4.6 | 記録のアーカイブ | 35 |
| 4.6.1 | アーカイブの対象 | 35 |
| 4.6.2 | アーカイブ情報の保管期間 | 35 |
| 4.6.3 | アーカイブデータの保護 | 36 |
| 4.6.4 | アーカイブデータのバックアップ | 36 |
| 4.7 | 署名鍵の更新 | 36 |
| 4.8 | 危殆化と災害の復旧 | 36 |
| 4.9 | 認証業務の廃止 | 37 |
| 5 | 物理的、手続き的及び人員のセキュリティ管理 | 38 |
| 5.1 | 物理的セキュリティ管理 | 38 |
| 5.1.1 | 建物及び立地条件 | 38 |
| 5.1.2 | 物理的なアクセス制御 | 38 |
| 5.1.3 | 電源及び空調 | 38 |
| 5.1.4 | 防水対策 | 38 |
| 5.1.5 | 防火対策 | 39 |
| 5.1.6 | 地震対策 | 39 |
| 5.1.7 | 媒体の保護 | 39 |
| 5.1.8 | 廃棄物処理 | 39 |
| 5.2 | 手続き的セキュリティ管理 | 39 |
| 5.2.1 | 権限の割当て | 39 |
| 5.2.2 | 複数人による作業の実施 | 39 |
| 5.2.3 | 人員配置 | 39 |
| 5.3 | 人員のセキュリティ管理 | 40 |
| 5.3.1 | 教育 | 40 |
| 6 | 技術的セキュリティ管理 | 41 |
| 6.1 | 鍵ペアの生成とインストール | 41 |
| 6.1.1 | 鍵ペアの生成 | 41 |
| 6.1.2 | 利用者への署名鍵の配送 | 41 |
| 6.1.3 | 本認証局への検証鍵の配送 | 41 |
| 6.1.4 | 利用者への認証局検証鍵の配送 | 41 |
| 6.1.5 | 鍵長 | 41 |
| 6.1.6 | ハードウェア/ソフトウェアでの鍵の生成 | 41 |
| 6.1.7 | 鍵の使用目的 | 41 |
| 6.2 | 署名鍵の保護 | 42 |
| 6.2.1 | 暗号モジュールの標準 | 42 |
| 6.2.2 | 署名鍵の管理 | 42 |
| 6.2.3 | 署名鍵のエスクロー | 42 |
| 6.2.4 | 署名鍵のバックアップ | 42 |
| 6.2.5 | 署名鍵のアーカイブ | 42 |
| 6.2.6 | 署名鍵の暗号モジュールへの格納 | 42 |
| 6.2.7 | 署名鍵をアクティブにする方法 | 43 |
| 6.2.8 | 署名鍵を非アクティブにする方法 | 43 |

| | | |
|-------|-----------------------------|----|
| 6.2.9 | 署名鍵を破棄する方法..... | 43 |
| 6.3 | 検証鍵に関するその他の管理..... | 43 |
| 6.4 | アクティベーションデータ..... | 43 |
| 6.4.1 | アクティベーションデータの生成及び管理..... | 43 |
| 6.4.2 | アクティベーションデータの保護..... | 43 |
| 6.4.3 | アクティベーションデータに関するその他の要件..... | 44 |
| 6.5 | 電子計算機のセキュリティ管理..... | 44 |
| 6.6 | ネットワークのセキュリティ管理..... | 44 |
| 6.7 | 暗号モジュールの管理..... | 44 |
| 7 | 電子証明書及び失効情報プロファイル..... | 45 |
| 7.1 | 電子証明書プロファイル..... | 45 |
| 7.1.1 | バージョン番号..... | 45 |
| 7.1.2 | 拡張領域..... | 45 |
| 7.1.3 | アルゴリズムの OID..... | 47 |
| 7.1.4 | 名前形式..... | 47 |
| 7.1.5 | 名前制約..... | 48 |
| 7.1.6 | 証明書ポリシーの OID..... | 48 |
| 7.1.7 | ポリシー制約..... | 48 |
| 7.1.8 | 有効期間..... | 48 |
| 7.2 | 失効情報プロファイル..... | 48 |
| 7.2.1 | バージョン番号..... | 49 |
| 7.2.2 | 拡張領域..... | 49 |
| 8 | 仕様管理..... | 50 |
| 8.1 | 仕様変更の手続き..... | 50 |
| 8.2 | 公表及び通知..... | 50 |
| | 付録..... | 51 |

1 はじめに

1.1 概要

四国電力株式会社(以下、四国電力という)は、「電子署名及び認証業務に関する法律」(平成12年法律第102号、以下、電子署名法という)の規定に適合する認証サービスである「よんでん電子入札対応認証サービス」(以下、本認証サービスという)を提供する。本認証サービスは、電子署名法に規定された認定制度における認定を受けた特定認証業務である。また、本認証サービスにおいて四国電力が運用する「よんでん電子入札対応認証局」(以下、本認証局という)は、政府が運営するブリッジ認証局(以下、BCAという)との相互認証を行う。

本認証サービスでは、四国電力と本認証サービスの利用契約を締結した法人もしくはこれに相当する組織(以下、利用組織という)に所属する個人(以下、利用者という)に対して、当該利用者の認証を行い、電子証明書(以下、利用者証明書という)を発行する。利用者は、当該利用者証明書を電子署名のために利用することができる。本認証サービスにより発行された利用者証明書をを用いた電子署名は、自署や押印に相当する法的効果が認められ得るものである。本認証サービスでは、電子署名の用途を定めない。電子署名の用途の一例としては、政府、地方自治体が実施する電子入札、電子調達、電子申込等の行政手続き等が挙げられる。また、本認証サービスでは、電子署名付き電子文書の受領者(以下、検証者という)に対して、利用者が施した電子署名の有効性を確認するために必要な情報を提供する。ただし、民間と民間の間における取引等を目的とした電子署名の検証は、BCAを介して行うことはできない。(BCAを介せず、有効性確認のための情報を得る場合は、この限りではない)
利用者証明書の発行申込受付は平成21年9月15日までとし、平成21年9月16日以降は発行申込受付を停止する。

本文書「よんでん電子入札対応認証サービス認証業務規程」(以下、本CPSという)は、本認証局が行う電子証明書の発行、失効及びその他の本認証局業務の運用管理に関する諸手続と、認証局を中心とする公開鍵基盤(PKI:Public Key Infrastructure、以下PKIという)の要素である認証局、利用者及び利用組織等の義務及び責任について規定した文書である。

本CPSは、本認証サービスに関する最上位の規程文書であり、公開文書である。また、本認証業務の手順の細目に関しては、本CPSに基づいて事務取扱要領等に規定される。

本CPSは、IETF(Internet Engineering Task Force)のPKIX(Public-Key Infrastructure X.509) Working Group が提唱する「電子証明書ポリシーと認証実践の枠組み (Certificate Policy and Certification Practices Framework)」(RFC2527) に準拠したものである。

1.2 識別

本認証局に関連するオブジェクト識別子(OID)は、次の通りとする。

表1-1 OIDとオブジェクト対応表

| OID | オブジェクト |
|----------------------|--------------------------|
| 1.2.392.200146 | 四国電力株式会社 |
| 1.2.392.200146.1 | よんでん電子認証サービス |
| 1.2.392.200146.1.1 | よんでん電子入札対応認証サービス |
| 1.2.392.200146.1.1.1 | よんでん電子入札対応認証サービス 証明書ポリシー |

1.3 コミュニティと適用範囲

以下の図に本認証サービスを取り巻くコミュニティを示す。コミュニティは、認証局、利用者、利用組織、検証者及びBCAから構成される。認証局は、発行局(以下、IAという)と登録局(以下、RAという)から構成され、また利用者は利用組織に所属している。

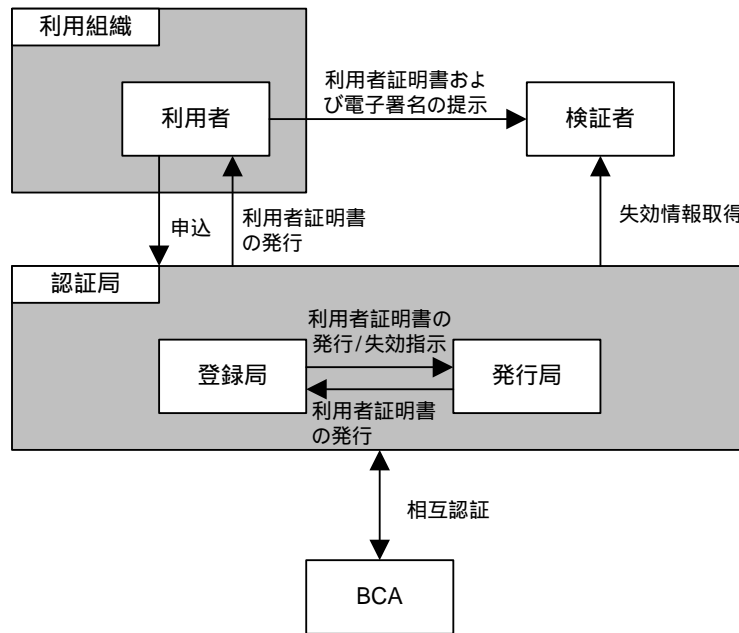


図1-1 本認証サービスを取り巻くコミュニティの概略

1.3.1 認証局

認証局は、IAとRAから構成され、四国電力により運用される。本認証局では、本CPSの遵守を条件に業務の一部を外部委託することができる。また、本認証局はBCAとの相互認証接続を実施する。

1.3.2 発行局(IA)

本認証サービスにおいて、IA業務を実施する。IA業務は、本認証局の認証局署名鍵の管理を行い、各種電子証明書の発行処理、失効処理及び電子証明書の失効リスト(以下、CRL/ARLという)の発行処理を行う。

1.3.3 登録局(RA)

本認証サービスにおいて、RA業務を実施する。RA業務は、利用者からの利用者証明書の申込に対して、申込の正当性、申込者の審査及び利用組織への所属確認を確実にし、IAに対して利用者証明書の発行及び失効の指示を行う。また、利用者署名鍵の生成及びICカードへの格納を行い、安全な方法で利用者へ送付する。RA業務は、その業務内容により二種類(RA認証業務とRA登録業務)に分類される。RA認証業務は、申込の審査を行い、RA登録業務は、RA認証業務からの指示に従い利用者証明書の登録と失効を実施する。

1.3.4 利用者

利用者とは、本認証局に利用者証明書の発行の申込を行い、本認証局により利用者証明書が発行された個人である。利用者証明書には利用者の情報が記載されており、利用者は利用者証明書に対応する利用者署名鍵を用いて電子署名を行う。利用者は、本CPSの利用者の義務に関する条項を遵守し、本CPSの内容について理解し承諾した上で、利用者証明書を利用する。

1.3.5 利用組織

利用組織とは、四国電力と本認証サービスの利用契約を締結した商業登記された法人、商業登記された個人事業者(及びその組織)及び商業登記されていない個人事業者(及びその組織)である。利用組織は、当該組織に所属する利用者が、本認証サービスを利用することを承認し、本認証局に対して利用者が利用組織に属していることを証明する。利用組織は、本CPSの利用組織の義務に関する条項を遵守し、本CPSの内容について理解し承諾した上で、利用者証明書の利用を管理する。

1.3.6 検証者

検証者は、利用者証明書を信頼し利用する者である。検証者は、本CPSの検証者の義務に関する条項を遵守し、本CPSの内容について理解し承諾した上で、利用者証明書を利用する。

1.3.7 BCA

BCAは、行政機関認証局と民間認証局等との相互認証を実現するために政府が運営する認証局である。本認証局はBCAとの相互認証接続を実施する。

1.3.8 電子証明書の適用範囲

本認証サービスにおいて発行する利用者証明書は、電子署名において利用することができる。本認証サービスでは、電子署名の用途を定めない。

民間と民間の間における取引等を目的とした電子署名の検証は、BCAを介して行うことはできない。(BCAを介せず、有効性確認のための情報を得る場合は、この限りではない)

本認証サービスは、電子署名法に規定された認定制度において、主務大臣より「特定認証業務」の認定を受けたサービスである。電子署名法では、利用者証明書に記載された事項において、認定の対象となりえる範囲を、利用者の氏名、住所及び生年月日に限定している。このため、利用者証明書の記載事項のうち利用者氏名、住所のみが認定の対象である。

1.4 連絡先

本認証サービスの内容については、電話、FAX 又は Email にて問い合わせることができる。

問い合わせ先: 四国電力株式会社
所在地: 〒760-8573 香川県高松市丸の内2番5号
担当部署: 情報通信部電子認証事業プロジェクト
連絡先住所: 〒760-8573 香川県高松市丸の内2番5号
連絡担当窓口: よんでん電子認証サービス窓口
営業日: 日曜日、土曜日、祝祭日、年末年始(12月29日から1月3日まで)
及び四国電力の創立記念日(5月1日)を除く

受付時間: 営業日の午前9時から午後5時(正午から1時までの休憩時間を除く)まで
電話番号: 087-887-2389
FAX: 087-825-3022
Email: pki-info@yonden.co.jp

2 一般的な規定

2.1 義務

本認証局、利用者、利用組織及び検証者が有する義務について、以下に規定する。

2.1.1 認証局の義務

本認証局は、本CPSに規定した利用者、利用組織及び検証者に対して、以下の義務を負う。

(1) 本認証局の運用

本認証局は、本CPSに基づき本認証局の運用を行う。

(2) 認証局署名鍵の保護

本認証局は、本認証局の署名鍵が危殆化(盗難、漏えい等により他人に使用され得る状態になること)しないように保護を行う。

(3) 電子証明書の発行及び失効

本認証局は、本CPSに基づき各種電子証明書の適切な発行及び失効を行う。

(4) 利用者署名鍵の扱い

本認証局は、本CPSに基づき利用者署名鍵及び当該利用者署名鍵を格納するICカードのパスワード(以下、ICカードPINという)を適切に取り扱う。本認証局は、利用者署名鍵の生成からICカードへの格納までを適切に行い、安全かつ確実な方法で利用者に利用者署名鍵を送付する。また、ICカードPINの生成から印刷までの作業を適切に行い、利用者署名鍵とは別に安全かつ確実な方法で利用者にICカードPINを送付する。本認証局は、利用者署名鍵及びICカードPINの保管を行わない。本認証局の設備、あるいはシステム上に利用者署名鍵及びICカードPINが一時的に保管される場合には、当該利用者署名鍵及びICカードPINの管理を厳重に行い、かつ必要がなくなった段階で当該利用者署名鍵及びICカードPINを設備、あるいはシステム上より確実に消去する。

(5) 問い合わせの受付

本認証局は、本CPS1.4節(連絡先)に記載された営業日の受付時間に問い合わせを受付ける。

(6) リポジトリの公開

本認証局は、リポジトリにて本CPSを含む本認証局に関する情報、本認証局の自己署名証明書(更新時はOld With Old及びNew With New)、及び更新時にはリンク証明書(Old With New及びNew With Old)を公開し、またそれらの値をSHA-1で変換した値(以下、フィンガープリントという)を公開する。リポジトリの公開情報の詳細は、本CPS 2.6.1項(認証局情報の公開)において示す。

(7) 失効情報の公開

本認証局は、設備、あるいはシステム保守による一時停止、緊急時など、やむを得ない場合の停止を除き、CRL/ARLを作成し定期的にリポジトリに登録し、電子証明書の失効情報を公開する。

(8) 開示要求への対応

本認証局は、本CPSに基づき各種の情報開示を適切に行う。

(9) 秘密情報の取扱い

本認証局は、本CPSに基づき秘密情報を適切に取り扱う。

(10) 監査の実施

本認証局は、定期的に本認証局が実施する全ての認証業務について監査を実施し、監査報告に基づいて必要と認められた場合は、認証業務の改善を行う。

2.1.2 利用者の義務

利用者は、本認証局によって発行された利用者証明書を利用するに際して、以下の義務を負う。

(1) 本CPS及びサービス約款の承諾

利用者は発行申込に際して、本CPS、よんでん電子入札対応認証サービス約款(以下、サービス約款という)及び重要事項説明書を理解し、承諾する。

(2) 正確な情報の提示

利用者は、利用者証明書の発行申込に際し、各記入事項について真実を記載する。利用者は、虚偽の申込をして、不実の証明をさせた場合には、電子署名法第四十一条の規定により罰せられる。

(3) 利用者署名鍵及びICカードPINの管理

利用者は、電子署名が自署や押印に相当する法的効果が認められ得るものであることを承知し、利用者署名鍵及びICカードPINを適切に管理しなければならない。本認証局では、利用者証明書の発行時において、利用者署名鍵と利用者証明書をICカード内に格納し、これを利用者へ送付する。利用者は、当該ICカードの取扱いに十分留意し、秘匿性を維持し、利用者本人以外によって使用されることを防止する。ICカードPINには、ICカード利用者PINとICカード管理PINの2種類がある。

(4) 利用者情報記載の承諾

利用者は、電子証明書発行申込の書類及びその添付書類に記載された内容の内、利用者氏名(漢字、英字)、利用者住所、利用組織商号・名称及び利用組織本店住所が利用者証明書に登録されることについて承諾する。また、利用者住所については、利用者住所のフリガナを認証局がヘボン式ローマ字表記に変換して利用者証明書に登録すること(ヘボン式で表記できない場合は、別途定める申込手順書の記載方法による。)、利用者名、利用組織名、利用組織住所にJIS第1、第2水準以外の漢字が使用されている場合は、認証局が申込書に記載されているフリガナ(カタカナ表記)を利用者証明書に登録することについて承諾する。

(5) 利用者署名鍵の危殆化等に伴う失効申込

利用者は、利用者署名鍵が危殆化した場合、若しくは危殆化したおそれがある場合、本認証局に遅滞なく利用者証明書の失効申込を行う。

(6) 利用者証明書の記載内容変更に伴う失効申込

利用者は、利用者証明書に記載されている事項に変更が生じた場合、本認証局に遅滞なく利用者証明書の失効申込を行う。

(7) 利用者証明書の利用中止に伴う失効申込

利用者は、利用者証明書の利用を中止する場合、本認証局に遅滞なく利用者証明書の失効申込を

行う。

(8) 利用者署名鍵と利用者証明書の使用の制限

利用者は、本CPS 1.3.8項(電子証明書の適用範囲)に規定された用途以外の目的で利用者署名鍵及び利用者証明書を使用しない。

(9) 利用者証明書記載事項の確認

利用者証明書の発行時において、利用者は、ICカードを受領した後に、利用者証明書の記載内容を確認し、その内容が申込内容と相違ないことを確認する。利用者は、利用者証明書の記載事項が申込書に記載の内容と相違する場合は、受領書にその旨を記載し、本認証局に提出する。

(10) 受領書の送付

利用者証明書の発行時において、利用者は、ICカードを受領した後に、ICカードが正常稼動することを確認し、ICカード到着後2週間以内に本認証局に受領書を提出する。

(11) 利用組織及び本認証局による失効

利用者は、利用組織からの申込及び本認証局の判断により利用者証明書が失効されることがあることを承諾する。

(12) 指定された電子署名アルゴリズムの使用

利用者は、本認証局が指定するアルゴリズムを利用して電子署名を行う。本認証局が指定するアルゴリズムは、「SHA1 with RSA」で、鍵長は1024ビットである。

2.1.3 利用組織の義務

利用組織は、当該組織に所属する者が本認証局によって発行された利用者証明書を利用するに際して、以下の義務を負う。

(1) 本CPS及びサービス約款の承諾

利用組織は利用者の発行申込に際して、本CPS、サービス約款及び重要事項説明書を理解し、承諾する。

(2) 正確な情報の提示

利用組織は、利用者証明書の発行申込に際し、在職証明書に記載される利用組織名、利用組織住所等の情報を十分に確認し、真実を記載する。利用組織は、虚偽の申込が成されることの無いように、適切に利用者を管理する。

(3) 利用者署名鍵の管理

利用組織は、利用者が利用者署名鍵の保全に努めるよう、適切に利用者を管理する。利用組織は、利用者以外の者が、当該利用者の利用者署名鍵を利用しないように、適切な管理を行う。

(4) 利用組織情報記載の承諾

利用組織は、利用者証明書に利用組織の情報(組織名、住所)が記載されることを承諾する。

(5) 利用者署名鍵の危殆化等に伴う失効申込

利用組織は、利用者署名鍵が危殆化した場合、若しくは危殆化したおそれがある場合、本認証局に遅滞なく利用者証明書の失効申請を行う。

(6) 利用者証明書の記載内容変更に伴う失効申請

利用組織は、利用者が当該組織の所属者でなくなった場合、あるいは利用者証明書に記載されている事項に変更が生じた場合、本認証局に遅滞なく利用者証明書の失効申請を行う。

(7) 利用者証明書の利用中止に伴う失効申請

利用組織は、利用者証明書の利用を中止する場合、本認証局に遅滞なく利用者証明書の失効申請を行う。

(8) 利用者署名鍵と利用者証明書の使用の制限

利用組織は、利用者が本CPS 1.3.8項(電子証明書の適用範囲)に規定された用途以外の目的で利用者署名鍵及び利用者証明書を使用することの無いように、適切に利用者を管理する。

2.1.4 検証者の義務

検証者は、本認証局によって発行された電子証明書(利用者証明書、相互認証証明書、リンク証明書を含む)を利用するに際して、以下の義務を負う。

(1) 本CPS及びサービス約款の承諾

検証者は本認証局によって発行された電子証明書を利用するに際して、本CPS、サービス約款及び重要事項説明書を理解し、承諾する。検証者は、本CPSに記載された利用目的の範囲内でのみ電子証明書を利用する。

(2) 電子証明書の有効性の確認

検証者は、本認証局が発行する自己署名証明書及び必要に応じてリンク証明書をリポジトリから入手し、利用対象の電子証明書に施された電子署名が本認証局署名鍵で正しく行われていること、及び当該電子証明書が改竄されていないことを確認する。また、検証者はフィンガープリントをリポジトリから入手し、自己署名証明書及び必要に応じてリンク証明書から作成したフィンガープリントと一致することを確認することにより、取得した自己署名証明書が本認証局のものであることを確認する。

(3) 電子証明書の有効期間の確認

検証者は、利用対象の電子証明書が有効期間内であることを確認する。

(4) CRL/ARLの確認

検証者は、電子証明書の失効情報(CRL/ARL)をリポジトリから取得し、利用対象の電子証明書が失効されていないことを確認する。

2.2 責任

本認証局、利用者及び利用組織が有する責任について、以下に規定する。

2.2.1 認証局の責任

本認証局は、本CPSに従い本認証サービスを提供する。また、認証局の署名鍵を適切に運用管理し、

電子証明書の信頼性を確保する。本認証局は、本 CPS に従い、利用者証明書の利用申込者の本人確認及び利用者署名鍵の生成を適切に行う。本認証局は、CRL/ARL を公開することで、利用者、利用組織及び検証者が電子証明書の失効状況を検証できるようにする。また、本 CPS 等の本認証サービスに係わる情報をリポジトリにて公開することで、利用者、利用組織及び検証者が本認証サービスに必要な諸手続き等を把握できるようにする。

2.2.2 利用者の責任

利用者は、本CPS及びサービス約款に従って利用者証明書を利用する。利用者は、本CPSに基づき利用者証明書の失効が必要と判断される場合には、速やかに利用者証明書の失効申請を行う。

2.2.3 利用組織の責任

利用組織は、本CPS及びサービス約款に従って利用者証明書が利用されるように、当該組織に所属する利用者を適切に管理する。利用組織は、本CPSに基づき利用者証明書の失効が必要と判断される場合には、速やかに利用者証明書の失効申請を行う。

2.3 財務上の責任

四国電力は、本認証局を運営し、本CPSに規定された義務及び責任を果たすために必要な財政的基盤を有する。本認証局が負う財務上の責任について、以下に規定する。

2.3.1 賠償責任

本認証局は、本認証局の責に帰さない事由によって発生した損害については、一切損害賠償責任を負わないものとする。

本認証局の責に帰すべき事由によって損害が発生した場合、本認証局は、別途サービス約款に定める範囲で損害賠償を行うものとする。

利用者による利用者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、本認証局は利用者に対して賠償を請求する場合がある。

- ・ 利用者、利用組織の虚偽の申告に伴う損害。
- ・ 利用者、利用組織の故意又は過失による事実の不開示に伴う損害。
- ・ 利用者自身の瑕疵による利用者署名鍵の危殆化に伴う損害。
- ・ 利用者、利用組織及び検証者が、本CPS及びサービス約款の規定遵守を怠ったことに伴う損害。
- ・ 利用者による利用者署名鍵の目的外使用に伴う損害。

2.3.2 免責事項

本認証局は、次の各項に起因する損失、損害又は費用について、一切賠償責任を負わないものとする。

- ・ 利用者証明書を使用するにあたっての利用者、利用組織及び検証者自身のシステムの障害。
- ・ 利用者自身の瑕疵による利用者署名鍵の危殆化に伴う損害。
- ・ 地震、水害、噴火、津波などの天災によるサービス停止。
- ・ 火災、停電などの広域災害によるサービス停止。
- ・ 戦争、動乱、騒乱、暴動、労働争議などによるサービス停止。
- ・ その他の不可効力によるサービス停止。
- ・ 利用者、利用組織及び検証者が本CPS及びサービス約款の規定遵守を怠ったことに伴う、利用

者、利用組織及び検証者が受ける損害。

- ・ 本認証局が失効処理を規定の期日に行ったにもかかわらず、当該失効情報が掲載されたCRLの公開前に電子署名付電子文書が検証者に送付された結果、発生する損害。
- ・ その他、本認証局が緊急にサービスを停止する必要があると判断した場合

2.4 解釈及び執行

本CPSの解釈及び執行について、以下に規定する。

2.4.1 準拠法

本CPSは、日本国内法に基づき解釈される。また、本認証局と関係者間で係争が生じた場合に適用される法令は、日本国内法とする。

2.4.2 分離、存続、合併、通知

本認証局が、本認証局を廃止した場合においても、本CPS2.8節(秘密情報)の効力は存続する。本CPSの規定又はその適用が、何らかの理由により無効又は執行不可能であるとされた場合における、当該事項については、本認証局の意思に合理的に合致するよう解釈され、当事者間にて調整を図る。無効又は執行不可能であるとされた場合における、残余の事項については、なお有効である。

2.4.3 紛争解決の手順

本認証局は、紛争発生時の専属的合意管轄裁判所を高松地方裁判所とする。全ての当事者は、これに同意するものとし、本CPS又は本認証局が発行する電子証明書に関して紛争が発生した場合には、誠意を持ってその解決に向けて協議を行うものとする。

2.5 料金

本認証局にかかわる料金は、下記のURIに提示する。

<http://www.yonden.co.jp/business/ninsho/index.html>

2.6 リポジトリにおける情報公開

本認証局が運営するリポジトリについて、以下に規定する。

2.6.1 認証局情報の公開

本認証局は、次の内容を下記のURIにおいて開示する。

- ・ よんでん電子入札対応認証サービス認証業務規程
<http://www.yonden.co.jp/business/ninsho/document/gyoumu.pdf>
- ・ サービス約款
<http://www.yonden.co.jp/business/ninsho/document/yakkan.pdf>
- ・ その他の認証局関連情報
<http://www.yonden.co.jp/business/ninsho/index.html>
- ・ 自己署名証明書
<ldap://repository.ynss.yonden.co.jp/ou=YONDEN%20CA%20for%20Electronic%20Bidding%20System,o=Shikoku%20Electric%20Power%20Co.%5C%20Inc.,c=JP?cAcertificate>

- <http://www.yonden.co.jp/business/ninsho/prove.html>
- 自己署名証明書のフィンガープリント
<https://repository.ynss.yonden.co.jp/fp1.pdf>
- 相互認証証明書
<ldap://repository.ynss.yonden.co.jp/ou=YONDEN%20CA%20for%20Electronic%20Bidding%20System,o=Shikoku%20Electric%20Power%20Co.%5C%2CInc.,c=JP?crossCertificatePair>
- リンク証明書
<ldap://repository.ynss.yonden.co.jp/ou=YONDEN%20CA%20for%20Electronic%20Bidding%20System,o=Shikoku%20Electric%20Power%20Co.%5C%2CInc.,c=JP?cAcertificate>
<http://www.yonden.co.jp/business/ninsho/prove.html>
- リンク証明書のフィンガープリント
<https://repository.ynss.yonden.co.jp/fp1.pdf>
- 利用者証明書の失効リスト(CRL)
<ldap://repository.ynss.yonden.co.jp/ou=YONDEN%20CA%20for%20Electronic%20Bidding%20System,o=Shikoku%20Electric%20Power%20Co.%5C%2CInc.,c=JP?certificateRevocationList>
- 各種認証局の電子証明書の失効リスト(ARL)
<ldap://repository.ynss.yonden.co.jp/ou=YONDEN%20CA%20for%20Electronic%20Bidding%20System,o=Shikoku%20Electric%20Power%20Co.%5C%2CInc.,c=JP?authorityRevocationList>

2.6.2 公開情報の更新頻度

CRL/ARLは、24時間毎に発行される。その他の公開情報については、公開内容の変更が成される都度に更新される。

2.6.3 アクセス管理

本認証局のリポジトリは、リポジトリを利用する全ての人に参照権限のみ割り当てる。

2.6.4 リポジトリの運用

本認証局は、1日24時間、1年365日間利用可能な運用体制を事務取扱要領等に規定し、リポジトリを運用する。ただし、設備、あるいはシステム保守などが必要となった場合に、予め通知したうえでリポジトリを一時停止することがある。なお、緊急時等のやむを得ない場合には、事前通知せずにリポジトリを停止することがある。

2.7 準拠性監査

本認証局が行う準拠性監査について、以下に規定する。

2.7.1 準拠性監査の実施頻度

本認証局は、年に1回以上の定期監査を実施する。また、認証局責任者が必要と認めた場合は、不定期な監査を実施する。

2.7.2 監査人の選任

監査人は、準拠性監査において十分な知識を持った者が認証局責任者により選任される。

2.7.3 監査人と監査対象者の関係

監査人は、認証業務部門以外から選定される。

2.7.4 監査項目

本認証局は、本認証局の運営が、本CPS及び事務取扱要領等に準拠して行われていることの確認を目的とした監査を実施する。本認証局が運営する全ての業務、システム及び設備を当該監査の対象とする。当該業務の一部を外部委託する場合には、委託先の業務、システム及び設備が監査対象に含まれる。

2.7.5 監査指摘事項への措置

本認証局は、監査結果での指摘事項及びセキュリティ対策に関する最新の技術動向を踏まえて、業務、システム及び設備の見直し、改善を行い、必要である場合は、本CPSの改訂を行う。業務、システム及び設備の見直し、改善を行った場合は、認証業務の実施結果について評価を行う。

2.7.6 監査結果の公開

本認証局は、監査結果の外部への公開を行わない。ただし、以下の場合においては監査結果を開示する場合がある。

- ・ 電子署名法に規定された認定に係る指定調査機関から監査結果の開示要求があった場合
- ・ 公的機関などから法律に基づく開示要求があった場合
- ・ 相互認証接続先の認証局の規定により開示が要求されている場合
- ・ 本認証局責任者が必要と判断した場合

2.8 秘密情報

本認証局の秘密情報について、以下に規定する。

2.8.1 秘密情報の種類

秘密情報の種類には、認証業務に関連して利用者又は利用組織から提示される個人情報、本認証局の設備仕様、システム仕様、ネットワーク仕様、詳細な業務手順などが含まれる。本認証局は、本項に別段の規定がある場合を除き、原則としてこれらの秘密情報を公開しない。本認証局は、本認証サービスを提供するために必要な範囲を超えて、これらの秘密情報を使用しない。

2.8.2 個人情報の取扱いについて

本認証局は、利用者又は利用組織から提示される個人情報の取扱いの詳細について事務取扱要領に定め、個人情報の収集、利用及び提供を制限し、本認証サービスにおける個人情報の適切な保護を実践する。本認証局は、個人情報の収集を本認証サービスに必要な範囲を超えて行わない。本認証局は、個人情報を電子証明書に記載する等、本サービスの用に供される以外の目的に使用しない。本認証局は個人情報を記録した書類、電子媒体を施錠された場所に保管し、許可された者以外が個人情報にアクセスできないような措置を講ずる。本認証局は、個人情報の取扱い及び保護に関して、全ての就業者を対象とした、役割に応じた教育・訓練計画が策定され、教育・訓練等が同計画に沿って実施される。

2.8.3 秘密とみなされない情報

本認証局は、本認証局が発行する電子証明書に記載される情報、CRL/ARLに記載される情報及びリ

ポジトリに公開される情報を秘密情報とみなさない。

2.8.4 電子証明書失効情報の公開

本認証局は、電子証明書が失効された場合、CRL/ARLに含まれる情報として、当該電子証明書のシリアル番号、失効日時及び失効事由(ReasonCode)を公開する。本認証局は、これらを除く電子証明書失効処理に係る情報は、秘密情報としてこれを開示しない。

2.8.5 法執行機関への情報開示

本認証局は、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には、法執行機関への情報開示を行う場合がある。

2.8.6 民事手続き上の情報開示

本認証局は、民事手続き上の要請に基づく情報開示を行う場合がある。民事手続きには、調停、起訴、法的手続き、裁判上手続き及び行政手続き等が含まれる。

2.8.7 名義人の申込による情報開示

本認証局は、利用者証明書の名義人から、当該利用者証明書にかかわる情報の開示の要求があった場合、これらの情報の開示を行う。

情報の開示にあたって、本認証局は、開示申込者から、所定の開示申込書の郵送による提出を受けつける。本認証局は、当該申込書上の記載事項(氏名、押印の印影等)と、当該利用者証明書の発行時の申込書類との比較を行い、開示の要求者が、当該利用者証明書の名義人本人であることを確認する。本認証局は、上記作業において開示申込者の真正を判断できない場合、これを確認するため、開示申込者に対して追加の書類の提出を求める場合がある。開示が認められた場合、本認証局は、開示対象となる情報を、郵送によって、開示の要求者に提示する。

開示対象となる情報は、以下の通りである。

- ・ 利用者証明書に係る申込書及び利用者の真偽を確認するために提供を受けた書類
- ・ 利用者証明書の記載内容

2.8.8 その他の情報開示

本認証局は、本業務の一部を外部に委託する場合、当該業務を実施するために必要な範囲内において、当該外部委託先に対して情報の開示を行う場合がある。情報の開示を実施する場合には、当該情報が本CPS 2.8.1項(秘密情報の種類)の規定に適合した取扱いをされるように、適切な委託契約を締結する等、外部委託先の管理を行う。

2.9 知的財産権

本認証局は、以下の情報資料及びデータを、本認証局に帰属する知的財産とみなす。

- ・ 本認証局の署名鍵及び署名検証鍵
- ・ 本認証局から発行された電子証明書
- ・ 本認証局により作成されたCRL/ARL
- ・ 本CPS及びその他の公開情報

3 本人の識別と認証

3.1 利用者証明書の発行

本認証局が行う利用者証明書の発行について、以下に規定する。

3.1.1 名前の型

本認証局では、ITU-T X.509 勧告に準拠した利用者証明書を発行する。本認証局が発行する利用者証明書に記載される発行者名(issuer)、主体者名(subject)、主体者別名(subjectAltName)、発行者別名(issuerAltName)においては、ITU-T X.500シリーズで規定された識別名(DN:Distinguished Name)を利用する。

3.1.2 名前の意味に関する要件

本認証局では、利用者が提出する電子証明書発行申込書(以下、発行申込書という)の記載事項、添付書類の記載事項及び本認証局が独自に割当てする事項を用いて、利用者証明書に記載される主体者名(subject)及び主体者別名(subjectAltName)を決定する。

利用者証明書に記載される主体者名及び主体者別名について、以下に規定する。

利用者は、利用者証明書の発行申込の際に本認証局に提出した以下の情報が利用者証明書に記載されることを予め承諾しなければならない。

表 3-1 利用者証明書における主体者名(subject)

| 項番 | 名前の属性 | 値あるいは意味 | 電子署名法の対応 |
|----|------------------------------------|---|----------|
| 1 | 国名 (countryName, c=) | 日本を示す以下の値で固定。 “c=JP” | |
| 2 | 都道府県 (stateOrProvinceName, st=) | 利用者住所の都道府県のへボン式ローマ字表記。申込書類の記載事項をもとに本認証局が設定する。 例: “st=kagawa” | |
| 3 | 市町村 (localityName, l=) | 利用者住所の市町村以下のへボン式ローマ字表記。申込書類の記載事項をもとに本認証局が設定する。 例: “l=takamatsu-shi, ...” | |
| 4 | 固有名称 (commonName, cn=) | 利用者氏名のへボン式ローマ字表記。申込書類の記載事項をもとに本認証局が設定する。 例: “cn=Ichiro Tanaka” | |
| 5 | ユーザ識別子(お客さま ID) (userid, uid=) | 利用者に配付されるIC カードの識別番号。本認証局が設定する。 例: “uid=03100101-001” | - |

「 」: 属性の証明が電子署名法の認定制度における証明の対象内

「 - 」: 属性の証明が電子署名法の認定制度における証明の対象外

項番 1(countryName, c=)は PrintableString で記述、これ以外は UTF8String で記述する。

項番 3へボン式ローマ字表記ができない文字は、申込手順書に従い本認証局で変換する。申込手順書に規定されていない文字の変換は、利用者に承諾を得て変換する。

表 3-2 利用者の電子証明書における主体者別名(subjectAltName)

| 項番 | 属性の名称 | 値あるいは意味 | 電子署名法の対応 |
|----|-------------------------------------|---|----------|
| 1 | 国名 (countryName, c=) | 日本を示す以下の値で固定。 “c=JP” | - |
| 2 | 都道府県名 (stateOrProvinceName, st=) | 利用者が所属する組織の住所の都道府県名。 申込書類の記載事項をもとに本認証局が設定する。 例: “st=香川県” | - |
| 3 | 市町村名 (localityName, l=) | 利用者が所属する組織の住所の市町村名以下部分。 申込書類の記載事項をもとに本認証局が設定する。 例: “l=高松市...” | - |
| 4 | 組織名 (organizationName, o=) | 利用者が所属する組織の名称。 申込書類の記載事項をもとに本認証局が設定する。 例: “o=四国電力株式会社” | - |
| 5 | 固有名称 (commonName, cn=) | 利用者の氏名。 申込書類の記載事項をもとに本認証局が設定する。 例: “cn=田中 一郎” | - |

「 」:属性の証明が電子署名法の認定制度における証明の対象内

「 - 」:属性の証明が電子署名法の認定制度における証明の対象外

項番 1(countryName, c=)は PrintableString で記述、これ以外は UTF8String で記述する。

項番 2、3、4 については、利用者が商業登記をしていない利用組織に所属する場合には記載しない。

項番 3、4、5 において、利用者名、利用組織名、利用組織本店住所に誤字俗字が使用されている場合は、「誤字俗字・正字一覧表(平成 16 年 10 月 14 日付け法務省民一第 2842 号民事局長通達)」等に基づき置き換えられた JIS 第 1、第 2 水準の範囲内の文字で登録する。これに該当する文字がない場合は、その文字を発行申込書に記載されているフリガナ(カタカナ表記)に変換する。

3.1.3 名前形式を解釈するための規則

ITU-T X.500識別名(DN:Distinguished Name)の規定に従う。

3.1.4 名前の一意性

利用者証明書の主体者名には、本認証局にて一意に割当ててるユーザ識別子(userid, uid=)(以下、お客さま ID という)が含まれ、本認証局が発行する利用者証明書における一意性が確保される。

3.1.5 名前に関する紛争の解決手順

利用者証明書に記載される利用者の識別名に係る紛争は、本認証局と利用者との間での解決を原則とする。

3.1.6 商標の認識・認証・役割

本認証局は、本CPS 4.1.3項(発行申込の審査と承認)に規定された発行申込書及び添付書類の記載事項に基づき、利用者証明書の発行を行う。本認証局は、審査において商標の有無を確認しない。利用者証明書に記載される利用者の識別名(主体者名、主体者別名)は、商標を含む場合がある。このため、利用者証明書上に記載される利用者の識別名について問題が発生した場合は、利用者又は利用組織の責任で対処しなければならない。本認証局は、これらの問題に起因して発生するあらゆる損

害から免責される。

3.1.7 署名鍵の所有を証明するための方法

本認証局は、利用者署名鍵を利用者に送付する手段として、郵便事業株式会社が提供する、郵便物に記載された名あて一人に限って郵便物を渡すサービス(以下、本人限定受取郵便という)を用いる。本認証局は、認証局において利用者署名鍵を生成し、ICカードに格納後、これを本人限定受取郵便(特例型)により利用者本人に送付する。本認証局は、利用者よりICカードの受領書を受領することにより、利用者がICカード及び利用者署名符号を保持することを確認する。

3.1.8 利用組織の認証

本認証局は、利用者証明書の発行時における真偽確認作業の一部として、利用組織に関する以下の認証作業を実施する。本認証局は、2名の担当者が審査を行い、この結果を踏まえて利用者証明書の発行の承認を行う。また、審査において、不合格や疑義が生じた場合には、定められた業務手順に従い、電話、FAX、e-mailまたは郵送により、利用者が所属する組織の連絡担当者に連絡し、内容確認や申込書類の再提出等により対応する。

(1) 利用組織の実在性の確認

当該利用組織が商業登記している企業の場合には、発行申込書記載の利用組織名称及び利用組織本店住所等が、提出された登記事項証明書(商業登記簿謄本)の記載と一致することを確認する。当該利用組織が商業登記していない個人事業者等の場合には、納税証明書等により代替する。なお、登記事項証明書(商業登記簿謄本)などの文字が誤字俗字で記載され、発行申込書記載の文字と異なる場合でも、JIS 第1、第2水準であることと「誤字俗字・正字一覧表(平成16年10月14日付け法務省民一第2842号民事局長通達)」等によって同等の文字であることが確認できる場合は、一致していると判断する。

(2) 利用者の利用組織への所属の確認

発行申込書記載の利用者氏名、利用組織名等が、在職証明書の記載と同一であることを確認する。当該利用組織が商業登記している企業の場合には、在職証明書の押印の印影と、利用組織の印鑑証明書に押印された代表者の印影が一致していることを確認する。当該利用組織が商業登記していない個人事業者等の場合には、利用組織代表者の印鑑登録証明書に押印された印影と照合し一致することを確認することにより、利用者が利用組織に所属していることを確認する。

3.1.9 利用者の認証

本認証局は、以下の審査項目によって利用者の真偽確認を行う。本認証局は、2名の担当者が審査を行い、この結果を踏まえて利用者証明書の発行の承認を行う。また、審査において、不合格や疑義が生じた場合には、定められた業務手順に従い、電話、FAX、e-mailまたは郵送により、利用者に連絡し、内容確認や申込書類の再提出等により対応する。

(1) 申込書類の提出の確認による、申込の意思の確認

本CPS 4.1.2項(発行申込書類)に定める申込書類が全て提出されていることを確認する。申込書類は、記載内容、形式、有効期限等において真正なものであることを確認する。

(2) 住民票の写しを用いた実在性の確認

発行申込書記載の利用者氏名、生年月日及び住所等が、住民票の写しの記載と同一であることを確

認する。利用申込者が国内に居住する外国人である場合、発行申込書記載の利用者氏名、生年月日及び住所等が、外国人登録の登録原票記載事項証明書の記載と同一であることを確認する。また、住民票の写しの代わりに、住民票記載事項証明書を利用することもできる。

なお、住民票の写しもしくは登録原票記載事項証明書の文字が誤字俗字で記載され、発行申込書記載の文字と異なる場合でも、JIS 第1、第2水準であることと「誤字俗字・正字一覧表(平成16年10月14日付け法務省民一第2842号民事局長通達)」等によって同等の文字であることが確認できる場合は、一致していると判断する。

(3) 印鑑登録証明書を用いた本人性の確認

印鑑登録証明書が記載内容、形式、有効期間(発行日より3カ月以内)等において真正なものであることを確認した上で、発行申込書に利用者の押印があり、かつ当該押印の印影が印鑑登録証明書記載の印影と一致することを確認する。また、印鑑登録証明書と発行申込書の記載内容が一致することを確認する。

本認証局では、利用者証明書の発行時においては、当該利用者が発行申込書上に記載された利用組織に所属していることの確認も行う。これについては、本CPS 3.1.8項(利用組織の認証)を参照すること。

3.2 利用者証明書の更新

有効期間の満了に伴う利用者証明書の更新は、新たな利用者証明書の発行により行われる。本認証局は、本CPS 3.1節(利用者証明書の発行)の規定に従って利用者の認証を行った後、利用者証明書の発行を行う。

3.3 利用者証明書失効後の再発行

失効に伴う利用者証明書の再発行は、新たな利用者証明書の発行により行われる。利用者は、利用者証明書の失効後、再発行が必要な場合は、本認証局に対して新たな利用者証明書の発行申込を行わなければならない。本認証局は、本CPS 3.1節(利用者証明書の発行)の規定に従って利用者の認証を行った後、利用者証明書の発行を行う。

3.4 利用者証明書の失効

本認証局は、本認証局が発行した利用者証明書に対して、当該利用者証明書の利用者、あるいは当該利用者証明書の利用者が所属する利用組織からの失効申込を受付ける。本認証局が行う利用者証明書の失効について、以下に規定する。

(1) 利用者の識別と認証

本認証局は、失効申込書に押印された利用者の実印の印影が、発行申込書に押印された利用者の実印の印影と一致し、失効申込書と発行申込書の利用者氏名及び利用者住所等が一致する場合には、失効申込者を利用者本人と認め、失効申込が利用者本人からの要求であると判断する。失効申込書の実印の印影と発行申込書の実印の印影が一致しない場合には、失効申込が利用者本人からの要求であることを証明するために、本CPS4.4.3項(失効手続き)に規定した公的資料の提示を求め、本認証局がこれを判断する。

(2) 利用組織の識別と認証

本認証局は、失効申込書に押印された利用組織の代表印の印影が、当該利用者証明書の発行時に提出された在職証明書に押印された利用組織の代表印の印影と一致し、失効申込書と発行申込書の利用者氏名、利用組織名及び利用組織住所等が一致する場合には、失効申込者が当該利用者の所属する利用組織と認め、失効申込が当該利用者の所属する利用組織からの要求であると判断する。失効申込書の代表印の印影と発行申込書の代表印の印影が一致しない場合には、失効申込が当該利用者の所属する利用組織からの要求であることを証明するために、本CPS4.4.3項(失効手続き)に規定した公的資料の提示を求め、本認証局がこれを判断する。

4 運用上の要件

4.1 利用者証明書の発行申込

本認証局が行う利用者証明書の発行について、以下に規定する。

4.1.1 発行申込手続き

本認証局における発行申込手続きを以下に示す。

- ・ 利用者は、四国電力インターネットホームページから発行申込書類(電子証明書発行申込書、在職証明書兼同意書、代理受領委任状)、本CPS及びサービス約款をダウンロードする。この際、ホームページ上に掲載している重要事項説明書を理解し承諾した上で、ダウンロードする。または、利用者は本認証局からの郵送、あるいは四国電力事業所窓口等より、発行申込書類(電子証明書発行申込書、在職証明書兼同意書、代理受領委任状)、本CPS、重要事項説明書及びサービス約款を入手する。
- ・ 利用者は、発行申込に際して、本CPS、サービス約款及び重要事項説明書を理解し、電子証明書発行申込書への実印の押印をもって、利用者証明書への記載事項及び個人情報の取扱い、その他、本CPS、サービス約款及び重要事項説明書の記載事項について承諾する。
- ・ 利用者は、本CPS 4.1.2項(発行申込書類)に示した発行申込書類を準備する。
- ・ 利用者は、当該利用者が所属する利用組織に対して、発行申込に必要な書類の提供を依頼し、必要書類を準備する。
- ・ 利用者は、全ての発行申込み書類を、本認証局が指定した宛先に一括して郵送する。宛先は、発行申込書類(発行申込手順書)に記載されている。

申込手続きにおいて、発行申込者が注意すべき事項を以下に示す。

- ・ 本認証サービスでは、利用者本人による申込のみを許可し、代理人による申込を認めない。
- ・ 本認証局は、本認証局営業日の営業時間において随時、発行申込みを受付ける。
- ・ 本認証局の非営業日に郵便物が到着した場合は、翌営業日の受領とする。
- ・ 本認証局の営業時間終了後に郵便物が到着した場合は、翌営業日の受領とする。
- ・ 利用者からの発行申込は、郵送でのみ受付け、これ以外の方法では受理しない。
- ・ 本サービスでは、利用者証明書の発行申込受付は平成21年9月15日までとし、平成21年9月16日以降は発行申込受付を停止する。

4.1.2 発行申込書類

発行申込手続きに必要な書類及び主な記載事項を以下に示す。

(1) 発行申込書類

発行申込書類は、以下の通りとする。

表 4-1 発行申込書類一覧

| 項番 | 書類名 | 利用者の所属 | | 備考 |
|----|------------|----------------|--------------------|----|
| | | 企業 (商業登記あり) | 個人事業者等 (商業登記なし) | |
| 1 | 電子証明書発行申込書 | | | |
| 2 | 印鑑登録証明書 | | | |

| | | | | |
|---|------------------|--|--|---|
| 3 | 住民票の写し | | | 1 |
| 4 | 代理受領委任状 | | | 2 |
| 5 | 在職証明書兼同意書 | | | |
| 6 | 印鑑証明書(代表印) | | | |
| 7 | 登記事項証明書(商業登記簿謄本) | | | |
| 8 | 組織代表者の印鑑登録証明書 | | | 3 |
| 9 | 納税証明書または開廃業届の写し | | | 4 |

- 「 」:必須、「 」:場合によって必要、「 」:必要なし
- 1:住民票の写しの代わりとして、住民票記載事項証明書の提出も認める。また、日本国籍を持たない外国人の場合は登録原票記載事項証明書の提出を要する。
 - 2:本人限定受取郵便(特例型)にてICカードの代人受領を利用者が希望する場合に提出する。
 - 3:商業登記を行っていない事業者(個人事業者)については、利用組織代表者の印鑑登録証明書の提出を要する。ただし、個人事業者の代表者1人だけが申込みする場合、印鑑登録証明書の提出は1通でよい。
 - 4:商業登記を行っていない事業者(個人事業者)については、税務署発行の所得税納税証明書又は自治体発行の個人事業税納税証明書を用いて個人事業者の確認を行う。納税証明書の代替として、開廃業届(税務署受付印のある控え)の写し等、個人事業者が事業を行っていることを公的に証明できる書類の提出も受付ける。同一利用組織に所属する複数の利用者が同時に申し込みを行う場合は、項番5、6、7、8、9の資料は一部のみ提出することにより。
- 項番2,3,6,7,8の書類は発行日から3ヶ月以内のものを有効と判断する。

(2) 電子証明書発行申込書

発行申込書は、発行申込者本人が作成し準備する。

表 4-2 電子証明書発行申込書の主な記載事項

| 項番 | 項目 |
|----|------------------------|
| 1 | 利用者氏名 |
| 2 | 利用者氏名(ヘボン式ローマ字表記) |
| 3 | 利用者住所 |
| 4 | 利用者住所(フリガナ) |
| 5 | 利用者生年月日 |
| 6 | 利用組織名 |
| 7 | 利用組織住所 |
| 8 | 利用組織代表者名 |
| 9 | 電子証明書の用途(プレ印刷済み) |
| 10 | ICカード(利用者証明書)の発行枚数 |
| 11 | 利用者の実印(印鑑登録証明書で照合可能な印) |

(3) 在職証明書兼同意書

在職証明書は、利用組織が作成する。

表 4-3 在職証明書兼同意書の主な記載事項

| 項番 | 項目 |
|----|-------|
| 1 | 利用者氏名 |

| | |
|---|------------------------|
| 2 | 利用者住所 |
| 3 | 利用組織名 |
| 4 | 利用組織代表者名 |
| 5 | 利用組織の本店住所 |
| 6 | 利用組織の代表印(印鑑証明書で照合可能な印) |

項番5については、商業登記ありの場合は利用組織の印鑑証明書に押印された代表印、商業登記なしの場合、利用組織代表者の印鑑登録証明書に押印された印、とする。

(4) 代理受領委任状

代理受領委任状は、本人限定受取郵便(特例型)にてICカードの代人受領を希望する場合に、発行申込者本人が作成し準備する。

表 4-4 代理受領委任状の主な記載事項

| 項番 | 項目 |
|----|--------|
| 1 | 利用者氏名 |
| 2 | 利用者住所 |
| 3 | 利用者の実印 |
| 4 | 代人氏名 |
| 5 | 代人住所 |

4.1.3 発行申込の審査と承認

利用者からの発行申込において、本認証局は、発行申込の審査を行う。審査においては、本CPS 4.1.2項(発行申込書類)に定める申込書類が全て揃っていること及び申込書類は、記載内容、形式、有効期限等において真正なものであること等を確認する。本認証局は、電子証明書発行申込書への実印の押印を確認することをもって、利用者証明書への記載事項及び個人情報の取扱について利用者が承諾したことを確認する。本認証局が行う利用者証明書発行申込の審査については、本CPS 3.1.8項(利用組織の認証)及び3.1.9項(利用者の認証)に定めている。

本認証局は、利用者の真偽が確認され、審査に合格した発行申込に対して、責任者が当該発行申込の承認を行う。

4.2 利用者証明書の発行

本認証局は、本認証局が行う発行申込の審査に合格し、かつ本認証局による利用者証明書の発行が認められた者に対して利用者証明書を発行する。本認証局は、利用者署名鍵と利用者検証鍵の対(以下、利用者鍵ペアという)を生成し、当該利用者鍵ペアを利用者署名鍵と利用者証明書としてICカードに格納し、本人限定受取郵便(特例型)にて利用者に送付する。本認証局は、発行申込者が本人限定受取郵便(特例型)におけるICカードの代人受領を希望する場合には、代理受領委任状の提出を受けることにより、これに対応する。また、本認証局は、ICカードPIN(ICカード利用者PINとICカード管理PIN)を記載した通知書(以下、PIN通知書という)をICカードとは別に簡易書留郵便にて発行申込者に送付する。

本認証局は、本認証局より発送したICカード又はPIN通知書が返送されてきた場合には、2回を限度と

して再送付を行う。2回の再送の後に返送されてきた場合には、本認証局は当該利用者証明書の失効を行う。

本認証局は、利用者証明書の他に、BCAと相互接続するための相互認証証明書を発行する。相互認証証明書の発行時において、本認証局は、相互認証先よりオフラインで提示される証明書発行要求(PKCS#10フォーマット)を受取り、署名検証等を行って正当性を確認した後、当該証明書発行要求に対応する相互認証証明書の発行を行う。本認証局が発行した相互認証証明書は、オフラインにて相互認証先へ提出する。相互認証証明書の発行手順の詳細については、相互認証先との協議のもとで決定する。

4.3 署名鍵及び利用者証明書の受領

利用者署名鍵及び利用者証明書は、ICカードに格納され、利用者に郵送される。利用者は、ICカード及びPIN通知書の受領後、当該ICカードが利用可能であること、及び利用者証明書の記載内容に誤りがないことの確認を行い、問題がなければICカードと共に送付される電子証明書(ICカード)受領書(以下、受領書という)に押印し、本認証局に郵送する。押印にあたって、利用者は、発行申込書に押印した実印を用いなければならない。

受領書は、ICカード1枚につき1通を提出する。複数枚のICカードの発行を受けた場合には、利用者は、その発行枚数に相当する受領書を提出する。

利用者は、ICカードを送付した際に同封した受領書をICカード到着後2週間以内に認証局へ返送しなければならない。2週間以内に受領書が返送されない場合、認証局は利用者証明書の失効を行う場合がある。

相互認証接続先との相互認証証明書の交換は、オフラインにて行う。

4.4 電子証明書の失効

本認証局が発行する利用者証明書及び相互認証証明書の失効について、以下に規定する。

4.4.1 失効事由

本認証局が発行する利用者証明書及び相互認証証明書の失効事由について、以下に規定する。

(1) 利用者または利用組織に起因する利用者証明書の失効事由

- ・ 利用者署名鍵が危殆化もしくは危殆化のおそれがある場合。
- ・ 利用者がICカードを紛失した場合。
- ・ 破損等によって利用者のICカードが使用できなくなった場合。
- ・ 利用者証明書の記載事項が事実と異なることを発見した場合。
- ・ 利用者証明書の記載事項に変更が生じた場合。
- ・ 利用者証明書の利用を中止する場合。
- ・ 利用者が退職、脱退、死亡等の事由により利用組織に在籍しなくなった場合。
- ・ 利用組織が解散した場合。
- ・ その他、何らかの事由により利用者証明書を失効する必要があると判断した場合。

(2) 本認証局に起因する利用者証明書の失効事由

- ・ 利用者が利用者証明書を格納したICカードを受領後、ICカードを送付した際に同封した電子証

- 明書受領書を本認証局に返送しない場合
- ・ 本人限定受取郵便(特例型)で送付された IC カードを、利用者または利用者の代理人が郵便局での受取審査不合格、もしくは受取り行為をしなかったことにより、郵便局から返送された本人限定受取郵便(特例型)を本認証局が再送したにもかかわらず、3回連続して返送された場合
 - ・ 本認証局が認証業務を廃止する場合
 - ・ 本認証局署名鍵が危殆化もしくは危殆化のおそれがある場合
 - ・ 利用者または利用組織が本CPS及びサービス約款等に違反した場合
 - ・ 利用者署名鍵が危殆化もしくは危殆化のおそれがある場合
 - ・ 利用者証明書の記載事項が事実と異なる場合
 - ・ 利用者証明書の記載事項に変更が生じた場合
 - ・ ICカード発送前に初期不良が発生した場合
 - ・ ICカードの不良により利用者が正しく受領できなかった場合
 - ・ その他、何らかの事由により利用者証明書を失効する必要があると判断した場合
- (3) 相互認証先に起因する相互認証証明書の失効事由
- ・ 相互認証を停止する場合
 - ・ 相互認証先の認証局署名鍵が危殆化もしくは危殆化のおそれがある場合
 - ・ 認証ポリシーの変更がある場合
 - ・ その他、何らかの事由により相互認証先が必要と判断した場合
- (4) 本認証局に起因する相互認証証明書の失効事由
- ・ 相互認証を停止する場合
 - ・ 本認証局の認証局署名鍵が危殆化もしくは危殆化のおそれがある場合
 - ・ 認証ポリシーの変更がある場合
 - ・ 本認証局が業務を廃止する場合
 - ・ 本認証局に相互認証基準違反があった場合
 - ・ その他、何らかの事由により本認証局が必要と判断した場合

4.4.2 失効要求を行う者

本認証サービスにおいて、利用者証明書の失効要求を行う者は、利用者証明書の利用者本人、当該利用者の所属する利用組織及び本認証局である。

本認証サービスにおいて、相互認証証明書の失効要求を行う者は、相互認証先及び本認証局である。

4.4.3 失効手続き

本認証局における失効手続きを、以下に規定する。

(1) 利用者本人による利用者証明書の失効手続き

利用者は、当該利用者証明書の失効申込を行う場合、電子証明書失効申込書を本認証局に郵送で提出しなければならない。電子証明書失効申込書の主な記載事項は、以下の通り。

表 4-5 電子証明書失効申込書の主な記載事項

| 項番 | 項目 |
|----|-------|
| 1 | 利用者氏名 |

| | |
|---|------------------|
| 2 | 利用者住所 |
| 3 | 利用者生年月日 |
| 4 | 電子証明書の失効理由 |
| 5 | お客さまID |
| 6 | 連絡先 |
| 7 | 発行申込書に押印した利用者の実印 |

本認証局は、利用者からの電子証明書失効申込書を郵送で受付、本CPS 3.4節(利用者証明書の失効)に定めた手順に基づき、失効申込の審査を行う。本認証局は、審査に合格し、失効申込が承認された場合に、当該利用者証明書の失効を行う。本認証局は、失効を行った後に、遅滞なく利用者証明書の失効を利用者と利用組織に失効通知書を郵送して通知する。

利用者は、必要に応じて以下の公的書類を電子証明書失効申込書に添付し、本認証局に提出しなければならない。

- ・ 印鑑登録証明書
失効申込書への押印に、発行申込書に押印された利用者の実印を紛失・破損・廃棄等により使用できない場合は、変更された実印を失効申込書に押印し、その実印を証明する印鑑登録証明書の提出が必要となる。
- ・ 住民票の写し又は戸籍の附票の写し
失効申込書への押印に、発行申込書に押印した利用者の実印を使用することができず、なおかつ、利用者が住所を変更した場合は、発行申込書に記載された住所と失効申込書に記載した住所が、ともに利用者本人のものであることを証明する書類として、住民票の写し又は戸籍の附票の写し(日本国籍を持たない外国人の場合は登録原票記載事項証明書)の提出が必要となる(ただし、住民票の写しを提出する場合、変更前の住所として発行申込書に記載された住所が明記されているものに限る)。本認証局では、発行申込時と失効申込時の住所が提出された公的書類に記載されていることを確認する。
- ・ 戸籍全部事項証明書(戸籍謄本)又は戸籍個人事項証明書(戸籍抄本)
失効申込書への押印に、発行申込書に押印した利用者の実印を使用することができず、なおかつ、利用者が氏名を変更した場合は、発行申込書に記載された氏名と失効申込書に記載した氏名が、ともに利用者本人のものであることを証明する書類として、戸籍全部事項証明書(戸籍謄本)又は戸籍個人事項証明書(戸籍抄本)の提出が必要となる。本認証局では、発行申込時と失効申込時の氏名が記載されていることを確認する。

申込手続きにおいて、失効申込者が注意すべき事項を以下に示す。

- ・ 本認証サービスでは、代理人による申込を認めない。
- ・ 本認証局は、本認証局営業日の営業時間において随時、失効申込みを受付ける。
- ・ 本認証局の非営業日に郵便物が到着した場合は、翌営業日の受領とする。
- ・ 本認証局の営業時間終了後に郵便物が到着した場合は、翌営業日の受領とする。

本認証局は、利用者が利用者証明書の緊急な失効が必要と判断した場合には、FAXを用いた失効要求を受付ける。利用者は、本認証局へ電話で連絡した後に、FAXを用いて失効申込書類を本認証局に送付しなければならない。本認証局は、コールバックにより申込の事実及び失効申込者の真偽を確認する。本認証局は、可及的速やかに失効申込者の真偽確認を行い、正当であると認められた場合

は、失効処理を行う。FAXを用いた利用者証明書の失効申込を行った申込者は、1週間以内に本認証局に到着するよう、書類の原本を郵送にて本認証局に提出しなければならない。本認証局は、利用者から郵送で送付された失効申込書類の原本について確認を行う。

(2) 利用組織による利用者証明書の失効手続き

利用組織は、利用者証明書の失効申込を行う場合、電子証明書失効申込書の本認証局に郵送で提出しなければならない。電子証明書失効申込書の主な記載事項は、以下の通り。

表 4-6 電子証明書失効申込書の主な記載事項

| 項番 | 項目 |
|----|------------------------|
| 1 | 利用者氏名 |
| 2 | 電子証明書の失効理由 |
| 3 | お客さまID |
| 4 | 利用組織名 |
| 5 | 利用組織住所 |
| 6 | 利用組織代表者名 |
| 7 | 連絡先 |
| 8 | 在職証明書兼同意書に押印した利用組織の代表印 |

本認証局は、利用組織からの電子証明書失効申込書を郵送で受付、本CPS 3.4節(利用者証明書の失効)に定めた手順に基づき、失効申込の審査を行う。本認証局は、審査に合格し、失効申込が承認された場合に、当該利用者証明書の失効を行う。本認証局は、失効を行った後に、遅滞なく利用者証明書の失効を利用者と利用組織に失効通知書を郵送して通知する。

利用組織は、必要に応じて以下の公的書類を電子証明書失効申込書に添付し、本認証局に提出しなければならない。

商業登記された企業の場合

- ・ 印鑑証明書(代表印)
失効申込書への押印に、在職証明書兼同意書に押印された利用組織の代表印を紛失・破損・廃棄等により使用できない場合は、変更された代表印を失効申込書に押印し、その代表印を証明する印鑑証明書の提出が必要となる。
- ・ 登記事項証明書(商業登記簿謄本)
失効申込書への押印に、在職証明書兼同意書に押印された利用組織の代表印を使用することができず、なおかつ、利用組織名又は利用組織住所を変更した場合は、在職証明書兼同意書に記載された組織名又は住所と失効申込書に記載した組織名又は住所が、ともに利用者が属する利用組織であることを証明する書類として、登記事項証明書(商業登記簿謄本)の提出が必要となる。

商業登記を行っていない事業者(個人事業者)の場合

- ・ 組織代表者の印鑑登録証明書
失効申込書への押印に、在職証明書兼同意書に押印された利用組織の代表印を紛失・破損・

廃棄等により使用できない場合は、変更された代表印を失効申込書に押印し、その代表印を証明する利用組織代表者の印鑑登録証明書の提出が必要となる。

- ・ 当該利用者が属する利用組織であることを証明する書類
失効申込書への押印に、在職証明書兼同意書に押印された利用組織の代表印を使用することができず、なおかつ、利用組織名又は利用組織住所を変更した場合は、在職証明書兼同意書に記載された組織名又は住所と失効申込書に記載した組織名又は住所が、ともに利用者が属する利用組織であることを証明する書類として、失効申込書に記載した組織名、住所を証明する公的書類の提出が必要となる。

申込手続きにおいて、失効申込者が注意すべき事項を以下に示す。

- ・ 本認証局は、本認証局営業日の営業時間において随時、失効申込みを受付ける。
- ・ 本認証局の非営業日に郵便物が到着した場合は、翌営業日の受領とする。
- ・ 本認証局の営業時間終了後に郵便物が到着した場合は、翌営業日の受領とする。

本認証局は、利用組織が利用者証明書の緊急な失効が必要と判断した場合には、FAXを用いた失効要求を受付ける。利用組織は、本認証局へ電話で連絡した後に、FAXを用いて失効申込書類を本認証局に送付しなければならない。本認証局は、コールバックにより申込の事実及び失効申込者の真偽を確認する。本認証局は、可及的速やかに失効申込者の真偽確認を行い、正当であると認められた場合は、失効処理を行う。FAXを用いた利用者証明書の失効申込を行った申込者は、1週間以内に本認証局に到着するよう、書類の原本を郵送にて本認証局に提出しなければならない。本認証局は、利用者から郵送で送付された失効申込書類の原本について確認を行う。

(3) 本認証局による利用者証明書の失効手続き

本認証局は、本認証局が利用者証明書を失効しなければならないと判断した場合には、当該利用者証明書の失効を行う。本認証局は、当該利用者証明書の失効処理及びその確認が完了した後に、遅滞なく失効通知書を作成し利用者と利用組織へ失効通知書を郵送して通知する。

(4) 相互認証先による相互認証証明書の失効手続き

本認証局は、相互認証先から相互認証証明書の失効を申請された場合には、当該相互認証証明書の失効を行う。本認証局は、当該相互認証証明書の失効処理及びその確認が完了した後に、相互認証先へ失効完了の通知を行う。

(5) 本認証局による相互認証証明書の失効手続き

本認証局は、本認証局が相互認証証明書の失効しなければならないと判断した場合には、当該相互認証証明書の失効を行う。本認証局は、当該相互認証証明書の失効処理及びその確認が完了した後に、相互認証先へ失効完了の通知を行う。

4.4.4 CRL/ARLの更新頻度

本認証局は、CRL/ARLを定期的に更新する。CRL/ARLの更新頻度は、24時間毎である。本認証局では、CRL/ARLにおいて、次回更新日(nextUpdate)を、当該更新が行われた時間から48時間後に設定する。本認証局は、失効処理を本認証局の業務時間内に行う。失効処理には、失効申込の受理、失効申込の審査及びシステムへの失効登録作業等が含まれる。本認証局は、失効申込を受理してからリポトリに掲載されるCRL/ARLに失効結果が反映されるまでの、失効処理の待ち時間を含めた遅延時間が最小となるように努める。

4.4.5 CRL/ARL 確認の要件

検証者は、本認証局が発行する最新のCRL/ARLを用いて、電子証明書の有効性を確認しなければならない。本認証局のCRL/ARLは、本CPS 2.6.1項(認証局情報の公開)に定められたリポジトリにおいて公開する。本認証局は、有効期間が満了した電子証明書の失効の問い合わせに応じない。

4.4.6 一時停止

本認証局では、電子証明書の一時停止を行わない。

4.5 セキュリティ監査手続き

本認証局が行うセキュリティ監査の手続きについて、以下に規定する。

4.5.1 記録されるイベント

本認証局における監査証跡には、以下のものが含まれる。

- ・ 電子証明書の発行及び失効に係わる審査の記録
- ・ 電子証明書の発行及び失効の記録
- ・ 電子証明書の発行及び失効に係る操作履歴
- ・ 情報開示に係わる審査の記録並びに情報開示記録
- ・ 認証局署名鍵の管理の記録
- ・ 認証設備室への入退室記録
- ・ 認証設備及び認証システムへの不正アクセスの記録
- ・ 認証システムの動作に関する記録

4.5.2 監査の頻度

本認証局は、本認証局の設備及びシステムを安全に運営するために適切と考えられる頻度で、監査を実施する。

4.5.3 監査証跡の保存期間

監査証跡の保存期間は、本CPS 4.6.2項(アーカイブ情報の保管期間)において定める。

4.5.4 監査証跡の保護

本認証局は、監査証跡を適切に保護し、監査証跡の漏洩、改竄、毀損、滅失を防止する。

4.5.5 監査証跡のバックアップ手順

本認証局は、バックアップが必要な監査証跡に対するバックアップ手順を策定し、当該手順に従いバックアップを行う。

4.5.6 監査証跡の記録システム

本認証局は、本認証局を構成するシステムによる自動処理及びオペレータによる手作業を組み合わせ、監査証跡を記録し収集する。

4.6 記録のアーカイブ

本認証局が行う記録のアーカイブについて、以下に規定する。

4.6.1 アーカイブの対象

本認証局は、以下の記録を含め、電子署名法で定められた記録をアーカイブの対象として保管する。

(1) 業務の実施に係る記録

- ・ 本認証サービスに係る申込書及びその添付資料
- ・ 作業指示、作業報告等の業務に関する記録
- ・ システムに記録された申込書記載事項に該当する情報
- ・ 各種署名鍵の生成、管理及び廃棄に関する記録
- ・ 利用者から提出される受領書等の書類
- ・ 本認証局より発行された各種電子証明書(自己署名証明書、相互認証証明書、リンク証明書、利用者証明書)及びその発行に関する記録
- ・ その他、業務の実施に係る情報

(2) 本認証局の運営に係る記録

- ・ 本CPSとその変更に関する記録
- ・ 本認証局の運営に係る管理書類とその変更に関する記録
- ・ 認証業務を外部に委託する場合の委託契約に関する書類
- ・ 監査に関する記録と監査報告書
- ・ その他、本認証局の運営に係る情報

(3) 設備及び安全対策措置に係る記録

- ・ 帳簿書類へのアクセス及び帳簿書類の管理に関する記録
- ・ 室への入退室及び室の安全対策措置に関する記録
- ・ 設備の保守及び設備の変更に関する記録
- ・ 障害及び復旧に関する記録
- ・ 事故に関する記録
- ・ システムの動作に関する記録
- ・ その他、設備及び安全対策措置に係る情報

4.6.2 アーカイブ情報の保管期間

本認証局は、アーカイブされた記録を、書類の場合は原本で、電磁的方法の場合は読み出しに必要なアプリケーションを残し、保管期間を通じて読解可能な状態で保管する。

(1) 業務の実施に係る記録

本認証局は、当該記録に係る電子証明書(相互認証証明書、利用者証明書)の有効期間の満了日から10年間、業務の実施に係る記録の原本を保存する。

(2) 本認証局の運営に係る記録

本認証局は、当該記録に係る電子証明書(相互認証証明書、利用者証明書)の有効期間の満了日から10年間、本認証局の運営に係る記録の原本を保存する。

(3) 設備及び安全対策措置に係る記録

本認証局は、当該記録を作成した日から電子署名法に規定された特定認証業務の認定の更新日まで、設備及び安全対策措置に係る記録を保存する。

4.6.3 アーカイブデータの保護

本認証局は、アーカイブデータの漏洩、改竄、毀損、滅失を防止するために、アーカイブデータの保護を適切に実施する。アーカイブデータは、施錠可能な入り口を持ち、間仕切り又は壁等によって区分され、自動火災報知器及び消火装置が備えられている室において保管・管理される。本認証局は、アーカイブされた記録が保管期間を通じて読解可能な状態を維持できるように、温度、湿度、磁気などの環境における要素を考慮した上で、アーカイブに使用する媒体を適切に保護する。また、媒体の特徴に合わせて適宜記録し直すなどの措置を行う。ただし、その際、保存内容の完全性・機密性を損なわない方法で作業を実施する。本認証局は、データの重要度に応じて、本認証局が許可する者以外がアーカイブデータを参照及び利用することを禁止するための措置を行う。

4.6.4 アーカイブデータのバックアップ

バックアップが必要なアーカイブデータについては、別途定めたバックアップ手順に従いバックアップを行う。

4.7 署名鍵の更新

本認証局は、認証局署名鍵の更新にあたり、リンク証明書を用いて新旧二つの認証局署名鍵の関係を証明する。このため、認証局署名鍵の更新時においては、自己署名証明書の発行に加えて、リンク証明書の発行も実施する。発行された自己署名証明書及びリンク証明書は、リポジトリにて公開を行う。

4.8 危殆化と災害の復旧

本認証局署名鍵の危殆化、もしくは危殆化した恐れがある場合、認証業務停止が伴う災害等による障害の発生など不測の事態が生じた時又は生じる恐れのある時には、本認証局は対策措置を迅速に行う。本認証局は、鍵の危殆化、もしくは危殆化した恐れがある場合、認証業務停止が伴う災害発生の際の対応策及び回復手順及びこれに係る教育計画を別途定め、計画に従って就業者の役割に応じて、定期的に教育訓練を行う。本認証局は、危殆化と災害の復旧について、以下を規定する。

(1) 本認証局署名鍵の危殆化又は危殆化の恐れがあることが判明した場合

- ・ 危殆化の内容、発生日時、被害状況、対応状況等の確認事項を主務大臣へ通報する。
- ・ 事故発生と事故に対する手続き等を本認証局のリポジトリに掲載し、利用者及び検証者へ通知する。
- ・ 当該署名鍵を用いて発行した全ての電子証明書(利用者証明書、相互認証証明書、リンク証明書)及び当該署名鍵を対象としたリンク証明書の失効を行い、CRL/ARLを更新する。
- ・ 利用者証明書の失効を行ったことを全利用者に宛て個別に郵送で通知するとともに、リポジトリを通じて検証者に公開する。
- ・ 相互接続を実施している接続先認証局に連絡する。
- ・ 認証局署名鍵の危殆化等の原因及び被害状況を調査し、対応策及び再発防止策を講ずる。

(2) 災害発生等により運用を停止した場合

- ・ 災害発生と災害に対する手続き等を本認証局のリポジトリに掲載し、利用者及び検証者へ通知する。
- ・ 検証者への失効情報の開示が7日間を超えて停止し、且つ検証者が停止を知る方法が無かった場合、直ちに障害の内容、発生日時、措置状況等の確認事項を主務大臣へ通報する。
- ・ 相互接続を実施している接続先認証局に連絡し、本認証局の被災状況等を通知する。
- ・ 手順に従い、復旧作業を行う。
- ・ 災害等による障害発生の原因及び被害状況を調査し、対応策及び再発防止策を講ずる。

4.9 認証業務の廃止

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継続が困難となった場合等において、認証業務を廃止する。本認証局は、認証業務の廃止後は新たな電子証明書の発行を行わない。認証業務を廃止する場合には、以下の処置を行う。

- (1) 利用者及び利用組織への連絡
認証業務廃止日の60日前までに、本認証局のリポジトリに業務廃止の案内を掲載すると共に、全ての利用者及び利用組織に業務廃止を知らせる通知書を郵送する。
- (2) 発行済み電子証明書の失効
認証業務廃止日までに、本認証局が発行した全ての利用者証明書、相互認証証明書、リンク証明書を失効する。
- (3) 認証業務廃止後の失効情報の開示
CRL/ARLを更新し、リポジトリに6ヶ月間公開する。この際、CRL/ARLの次回更新日(nextUpdate)は失効対象となった全ての電子証明書の有効期間の満了日以降の日付とする。また、CRL/ARLの日次での更新は行わない。
- (4) 認証局署名鍵の処理
本認証局は本認証局署名鍵(バックアップを含む)を消去し、復元不可能とする。
- (5) 主務大臣への届け出
本認証局は、当該認証業務廃止前に、所定の書式に従って主務大臣に届け出る。

5 物理的、手続き的及び人員的セキュリティ管理

5.1 物理的セキュリティ管理

本認証局が使用するRA認証業務室及び認証設備室の物理的セキュリティ管理について、以下に規定する。RA認証業務室は、利用者からの利用者証明書の発行申込を受付け、審査及び承認を行うための設備を設置した室である。認証設備室は、認証局署名鍵の管理、利用者鍵ペアの生成、利用者証明書を含む各種電子証明書の発行、利用者署名鍵と利用者証明書を格納するICカードの作成、PIN通知書の作成、等を行うための設備を設置した室である。

5.1.1 建物及び立地条件

本認証局は、本認証局全体の信頼性を確保するために、自然災害等を考慮した立地条件のもとに建築された、堅牢な構造を持つ建物内に、認証設備室を設置する。また、本認証局の所在及び仕様は、関係者以外には開示しない。建物の内外において、RA認証業務室、認証設備室の所在について表示しない。

5.1.2 物理的なアクセス制御

RA認証業務室は、RA認証業務に従事する者のみが入室権限を与えられた室で、室内が無人の場合は施錠し、権限を持つ者以外が容易に認証業務用設備に触れることを防止する。RA認証業務室の施錠鍵は、当該業務の責任者により管理され、業務の都度入室権限を持つ者に貸与される。認証設備室は、他の業務を行う室と区別された専用室で、最初の入室及び最後の退室に際しては、予め許可され登録された入室権限者2名による生体認証装置の操作が必要である。これにより、権限を持つ者を含め、認証設備室への単独での入室を防止し、かつ権限を持つ者以外が容易に認証業務用設備に触れることを防止する。認証設備室内で行う業務の権限を割り当てられた者以外の入室は、原則としてこれを禁止する。入室権限を持たない者が入室する場合は、2名以上の入室権限者同行の上この者を入室させることとする。認証設備室の入退室については、上記の運用が確実に行われていることについて、日常的にチェックを行い、適切に監督を実施する。認証設備室の物理的なアクセス制御については、以下の管理等を講じる。

- ・ 不正操作及び不正侵入者に対する警報。
- ・ 遠隔監視カメラ及びモーションセンサーによる室内状況の監視。
- ・ 容易に破壊されない構造・強度を持った壁による、他の室との区分。
- ・ 間仕切り壁等の隔壁は、建屋のスラブに固定され、侵入が可能となるような開口部を設けない。

5.1.3 電源及び空調

認証設備室の電源及び空調には、以下の対策等を講じる。

- ・ 電源は、2系統の受電経路を持つ。
- ・ 非常用自家発電機等を設置する。
- ・ 機器類の廃熱による温度上昇及び冬季の結露等を防止するための空調設備を有する。

5.1.4 防水対策

認証設備室内には、以下の防水対策等を講じる。

- ・ 配管等に漏水センサーを設置する。
- ・ 空調設備に漏水対策を講じる。
- ・ 認証設備室内には流し台、給茶機等の水使用設備を設置しない。

5.1.5 防火対策

RA 認証業務室には、自動火災報知器及び消火装置を備える等、防火措置を講じる。

認証設備室には、以下の防火対策を講じる。

- ・ 煙感知式の火災報知器、ハロン消火設備等を設置し、所轄消防署の定期検査を受ける。
- ・ 認証設備室を含む区画は、建築基準法に規定する防火区画とする。
- ・ ケーブル及び各種ダクトの防火区画貫通部に、延焼防止措置を講じる。

5.1.6 地震対策

認証設備室が設置される建屋は、以下の耐震対策を講じる。

- ・ 建屋は耐震構造を有する。
- ・ ラック等は床に固定され、卓上機器類はベルト等により固定する。

5.1.7 媒体の保護

電子データを保管した媒体を保護するために、以下の対策を講じる。

- ・ 媒体を保管する専用キャビネットは、適切に施錠管理し、権限を持つ者以外が媒体を持ち出すことを防止する。
- ・ 媒体は、管理者を設定して管理する。
- ・ 媒体は、変形防止、あるいは磁気等によるデータ破損防止の対策を講じる。

5.1.8 廃棄物処理

認証局署名鍵、商業的に重要な情報又は機密情報を含む紙面の文書及び電子媒体は、所定の手続きに基づいて安全に破棄される。

5.2 手続き的セキュリティ管理

本認証局が採用する手続き的なセキュリティ管理策について、以下に規定する。

5.2.1 権限の割当て

本認証局は、個々の業務の役割を明確に定め、役割に応じた権限を担当者に対して適切に割り当てる。本認証局は、各担当者に対して適切な設備機器類等の操作権限を明確に定め、操作権限に応じたログインアカウント等を担当者に対して適切に割り当てる。

5.2.2 複数人による作業の実施

本認証局では、本認証局が行う業務を正確に実施することを目的として、本認証局が行う一部の業務において、複数人により作業を実施することを規定し、これに従って作業を実施する。複数人によって実施する作業の範囲は、業務の重要度に応じて決定する。また、これにより、作業を行う者が単独でシステム全体を悪用することを防止する。

5.2.3 人員配置

本認証局における人員の配置は、定められた手順に基づき行う。本認証局は、個々の業務の役割に対して個別に人員を配置する。但し、相互牽制の効果を考慮し、安全性に問題が無いと判断される場合には、兼務を認める場合がある。

5.3 人員のセキュリティ管理

本認証局が採用する人力的なセキュリティ管理策について、以下に規定する。

5.3.1 教育

本認証局は、すべての就業者の役割に応じ、以下の項目についての必要な教育訓練計画を定め、計画に従って教育訓練を実施する。本認証局は、教育訓練の実施を記録し、証跡資料を残す。

- ・ 必要な知識、技術を習得するための教育訓練
- ・ 指揮命令系統、責任及び権限の変更に伴う教育訓練
- ・ 業務手順変更に伴う教育訓練
- ・ 危機管理に関する教育訓練

6 技術的セキュリティ管理

6.1 鍵ペアの生成とインストール

本認証局における署名鍵と検証鍵の対(以下、鍵ペアという)の生成とインストールについて、以下に規定する。

6.1.1 鍵ペアの生成

本認証局の鍵ペアは、認証設備室内において、本認証局の担当者が相互に牽制を行う状態で、担当者一人の操作だけでは実施できない方法により、ハードウェア暗号モジュール(以下、HSMという)の中で生成する。

本認証局の利用者の鍵ペアは、認証設備室内において、本認証局の複数の担当者が相互に牽制を行う状態で、特定の電子計算機の中で生成する。利用者鍵ペアとして生成された利用者署名鍵は、本認証局より発行された利用者証明書とともに IC カードに格納される。本認証局では、IC カードへの登録が完了した利用者署名鍵については、本認証局の管理する全ての装置上から完全に削除を行う。

6.1.2 利用者への署名鍵の配送

本認証局は、利用者署名鍵を、利用書証明書とともにICカードに格納し、本人限定受取郵便(特例型)で利用者本人に送付する。利用者は、本人限定受取郵便(特例型)の代人受取制度を利用してICカードを受領することができる。この場合に、当該郵便を代理受領した受取代理人は、封筒を開封してICカードを取り出してはならない。また、本認証局は、ICカードPIN(ICカード利用者PINとICカード管理PIN)を記載したPIN通知書をICカードとは別に簡易書留郵便にて利用者本人に送付する。

6.1.3 本認証局への検証鍵の配送

利用者鍵ペアは本認証局において生成されるため、利用者検証鍵の本認証局への配送については考慮しない。BCAの検証鍵は、本認証局へオフラインで配送される。

6.1.4 利用者への認証局検証鍵の配送

本認証局の検証鍵は、本認証局が発行する自己署名証明書に含まれ、本認証局署名鍵による電子署名を検証するために利用される。利用者への本認証局検証鍵の配送は、自己署名証明書を利用者が本認証局のリポジトリからダウンロードする方法で行われる他に、媒体(CD-ROM)に格納してICカードとともに本認証局から利用者へ郵送される。

6.1.5 鍵長

本認証局が生成する認証局署名鍵及び利用者署名鍵の鍵長は、以下の通りとする。各々の電子証明書への署名方式は、RSA方式(SHA1withRSA)を採用する。

認証局署名鍵： 2048bit RSA方式

利用者署名鍵： 1024bit RSA方式

6.1.6 ハードウェア/ソフトウェアでの鍵の生成

本CPS 6.1.1項(鍵ペアの生成)に規定する。

6.1.7 鍵の使用目的

本認証局は、認証局署名鍵を以下の目的に使用する。

- ・ 利用者証明書への電子署名

- ・ 本認証局の電子証明書(自己署名証明書(更新時はOld With Old及びNew With New))への電子署名
- ・ 相互認証証明書及び本認証局の電子証明書発行要求(PKCS#10フォーマット)への電子署名
- ・ リンク証明書(Old With New及びNew With Old)への電子署名
- ・ CRL/ARLへの電子署名

本認証局は、利用者署名鍵の使用を利用者に限定し、且つ本CPSの他の項目や契約等の制約によって利用者署名鍵の使用目的を電子署名に限定する。

6.2 署名鍵の保護

本認証局は、定められた手順に基づき、認証局署名鍵を厳重に管理し保護する。

利用者は、本 CPS に基づき、IC カードに格納された利用者署名鍵を、管理し保護しなければならない。

6.2.1 暗号モジュールの標準

本認証局署名鍵を格納する暗号モジュールの標準として、FIPS-140-1Level3を満たすHSMを採用する。

6.2.2 署名鍵の管理

認証局署名鍵の管理は、定められた手順により、認証設備室内において行なわれる。本認証局は、認証局署名鍵の生成、保存、アクティベート、非アクティベート、バックアップ及び廃棄等に係る管理を、権限を持った2名以上の者による相互牽制の下で行う。

利用者署名鍵の管理は、定められた手順により、認証設備室内において行なわれる。本認証局は、利用者署名鍵の生成、廃棄、ICカードへの格納及びICカードの送付に係る管理を、権限を持った2名以上の者による相互牽制の下で行う。本認証局は、ICカードへ利用者署名鍵を格納した後に、すべての装置上から完全に利用者署名鍵を削除する。また、ICカード受領後においては、利用者が責任を持って利用者署名鍵を管理しなければならない。

6.2.3 署名鍵のエスクロー

本認証局は、本認証局が管理する署名鍵の第三者預託(エスクロー)を行わない。

6.2.4 署名鍵のバックアップ

本認証局は、本認証局署名鍵のバックアップを行う。バックアップは、複数人の管理の下、認証設備室内において定められた手順によりHSMの複製機能を使用して行う。バックアップ用の暗号モジュールは、定められた手順に従って認証設備室内の安全な場所に保管を行う。本認証局は、利用者署名鍵のバックアップは行わない。

6.2.5 署名鍵のアーカイブ

本認証局は、本認証局が管理する署名鍵をアーカイブの対象としない。

6.2.6 署名鍵の暗号モジュールへの格納

本認証局署名鍵は、HSM内で生成され、HSMに保管される。

利用者署名鍵は、認証設備室内に設置された特定の電子計算機の中で生成し、ICカードへ格納する。利用者署名鍵は、ICカードへの格納が完了した後に、生成から格納までに経由したすべての装置上

から完全に消去する。

6.2.7 署名鍵をアクティブにする方法

本認証局は、本認証局署名鍵の閉塞状態を解除し、利用可能な状態にする(以下、アクティブにするという)方法として、複数の要員が本認証局署名鍵の活性化のためのデータ(以下、「アクティベーションデータ」という)を入力する方式を採用する。本認証局は、本認証局署名鍵をアクティブにする操作の実施場所を、認証設備室内に限定する。

本認証局は、利用者署名鍵をアクティブにする方法として、PINを入力する方式を採用する。本認証局は、利用者に対してPIN通知書を郵送する。本認証局では、利用者への郵送が完了したICカードPINの情報は保持しない。

6.2.8 署名鍵を非アクティブにする方法

本認証局は、複数の要員の管理下において、本認証局署名鍵を非アクティブにする。本認証局は、本認証局署名鍵を非アクティブにする操作の実施場所を、認証設備室内に限定する。

6.2.9 署名鍵を破棄する方法

本認証局は、本認証局署名鍵の廃棄が必要になった場合、定められた手順に従い本認証局署名鍵の廃棄を行う。署名鍵の廃棄は、相互牽制の下において、鍵を完全に復元できない方法により、HSMの中で行う。また、バックアップされた本認証局署名鍵の廃棄も一連の作業指示で遅延なく実施する。利用者は、利用者署名鍵の廃棄が必要になった場合、利用者署名鍵が格納されたICカードを物理的に破壊する等の方法により確実に廃棄しなければならない。

6.3 検証鍵に関するその他の管理

本認証局では、本認証局の自己署名証明書(認証局検証鍵を含む)を、当該証明書の有効期間の満了日から10年間保管する。また、本認証局では、本認証局が発行した他の電子証明書(利用者証明書、相互認証証明書、リンク証明書)について、当該電子証明書の有効期間の満了日から10年間保管する。

6.4 アクティベーションデータ

本認証局は、本認証局署名鍵の活性化のためのデータを適切に運用管理する。

6.4.1 アクティベーションデータの生成及び管理

本認証局は、別途定められた規則に従って、本認証局署名鍵のアクティベーションデータ及び利用者署名鍵を格納するICカードのPINの生成及び管理を行う。

6.4.2 アクティベーションデータの保護

本認証局は、別途定められた規則に従って、本認証局署名鍵のアクティベーションデータの保護を行う。

本認証局は、ICカードPINの秘匿性を確保するように最善の努力を払いながら、ICカードへのPIN設定及びPIN通知書の作成を行う。PIN通知書を受取った利用者は、本CPSの規定に基づき、当該ICカードPINを保護しなければならない。

6.4.3 アクティベーションデータに関するその他の要件

本認証局は、ICカード及びPIN通知書が作成された後に、本認証局が管理する全ての装置上から、当該PINの情報を完全に消去する。

6.5 電子計算機のセキュリティ管理

本認証局は、電子計算機のセキュリティの脆弱性に関する情報等を常時収集し、問題があればセキュリティ基準を再評価し、必要に応じて是正措置を施す。

6.6 ネットワークのセキュリティ管理

本認証局は、以下の管理基準を設け、必要に応じてネットワークセキュリティの管理策を講じて実施する。

- ・ 不正なアクセス等を防止するための装置、あるいはシステムを設置する。
- ・ 不正なアクセス等を検知するための装置、あるいはシステムを設置する。
- ・ 通信内容の盗聴及び改変を防止するための装置、あるいはシステムを設置する。

6.7 暗号モジュールの管理

本認証局は、本CPS 6.2.1項(暗号モジュールの標準)に規定したHSMを、暗号モジュールとして採用する。本認証局は、暗号モジュールの安全性に対する脅威についての情報を常に収集し、問題があれば対応策を講じる。

7 電子証明書及び失効情報プロフィール

本認証局が発行する電子証明書と失効情報(CRL/ARL)の形式、属性の仕様は、ITU-T X.509 および RFC2459 に従い定義している。

7.1 電子証明書プロフィール

電子証明書のプロフィールについて、以下に規定する。

7.1.1 バージョン番号

本認証局は、ITU-T X.509で規定されるバージョン3に準拠した電子証明書を発行する。

7.1.2 拡張領域

本認証局が発行する電子証明書に記載される拡張領域の範囲を以下に規定する。

表 7-1 電子証明書の拡張領域

| 項番 | 拡張領域の名称 | critical フラグ | 自己署名証明書 | リンク証明書 | 相互認証証明書 | 利用者証明書 |
|----|------------------------|--------------|---------|--------|---------|--------|
| 1 | authorityKeyIdentifier | FALSE | | | | |
| 2 | subjectKeyIdentifier | FALSE | | | | |
| 3 | keyUsage | TRUE | | | | |
| 4 | certificatePolicies | 1 | - | | | |
| 5 | policyMappings | FALSE | - | - | | - |
| 6 | subjectAltName | FALSE | | - | - | |
| 7 | issuerAltName | FALSE | | - | - | |
| 8 | basicConstraints | TRUE | | | | - |
| 9 | nameConstraints | TRUE | - | - | | - |
| 10 | policyConstraints | TRUE | - | - | | - |
| 11 | cRLDistributionPoints | FALSE | | | | |

:当該電子証明書に含める項目

:相互接続先との調整の上決定する項目

- :当該電子証明書に含めない項目

1 リンク証明書は FALSE、相互認証証明書と利用者証明書は TRUE とする。

(1) 認証局鍵識別子 (authorityKeyIdentifier)

本認証局は、authorityKeyIdentifierとしてkeyIdentifierを設定する。

自己署名証明書、相互認証証明書及び利用者証明書の設定値は、認証局検証鍵のSHA-1のハッシュ値とする。

リンク証明書の設定値は、OldWithNew は新認証局検証鍵のSHA-1のハッシュ値とし、NewWithOld は旧認証局検証鍵のSHA-1のハッシュ値とする。

(2) 主体者鍵識別子 (subjectKeyIdentifier)

自己署名証明書の設定値は、認証局検証鍵のSHA-1のハッシュ値とする。

リンク証明書の設定値は、OldWithNew は旧認証局検証鍵のSHA-1のハッシュ値とし、NewWithOld は新認証局検証鍵のSHA-1のハッシュ値とする。

利用者証明書の設定値は、利用者検証鍵のSHA-1ハッシュ値とする。
相互認証証明書の設定値は、相互認証先の検証鍵に係る値とする。

(3) 鍵用途 (keyUsage)

自己署名証明書、リンク証明書及び相互認証証明書の設定値は、以下とする。

keyCertSign
cRLSign

利用者証明書の設定値は、以下とする。

digitalSignature
nonRepudiation

(4) 証明書ポリシー (certificatePolicies)

リンク証明書の設定値は、以下とする。

policyIdentifier: ANY-POLICY (2.5.29.32.0)

相互認証証明書及び利用者証明書の設定値は、以下とする。

policyIdentifier: 本認証局に対応するOIDを設定 (1.2.392.200146.1.1.1)

policyQualifiers: 本CPSの掲載場所を設定 (本CPS 2.6.1項に記載のURI)

自己署名証明書には設定しない。

(5) ポリシマッピング (policyMappings)

本認証局は、相互認証証明書にpolicyMappingsを含める。policyMappingsの具体的な値は、相互接続先との調整の上決定する。

自己署名証明書、リンク証明書及び利用者証明書には設定しない。

(6) 主体者別名 (subjectAltName)

本認証局は、subjectAltNameとしてdirectoryNameを設定する。“c=JP”のみPrintableStringで記載する。他の項目はUTF8Stringで記載する。

自己署名証明書の設定値は、以下とする。

c=JP
o=四国電力株式会社
ou=よんでん電子入札対応認証局

利用者証明書の設定値は、本CPS 3.1.2項 (名前の意味に関する要件) に規定した内容を設定する。

リンク証明書及び相互認証証明書には設定しない。

(7) 発行者別名 (issuerAltName)

本認証局は、issuerAltNameとしてdirectoryNameを設定する。“c=JP”のみPrintableStringで記載する。他の項目はUTF8Stringで記載する。

自己署名証明書及び利用者証明書の設定値は、以下とする。

c=JP
o=四国電力株式会社
ou=よんでん電子入札対応認証局

リンク証明書及び相互認証証明書には設定しない。

(8) 基本制約 (basicConstraints)

本認証局は、basicConstraintsとしてcAを設定する。pathLenConstraintは設定しない。
自己署名証明書、リンク証明書及び相互認証証明書の設定値は、以下とする。

cA: TRUE

利用者証明書は設定しない。

(9) 名前制約 (nameConstraints)

本認証局は、相互認証証明書にnameConstraints を含める場合がある。nameConstraintsの具体的な値は、相互接続先との調整の上決定する。

自己署名証明書、リンク証明書及び利用者証明書は設定しない。

(10) ポリシ制約 (policyConstraints)

本認証局は、相互認証証明書にpolicyConstraints を含める場合がある。policyConstraintsの具体的な値は、相互接続先との調整の上決定する。

自己署名証明書、リンク証明書及び利用者証明書は設定しない。

(11) CRL配布点 (cRLDistributionPoints)

本認証局は、cRLDistributionPointsとしてdistributionPointを設定する。

自己署名証明書、リンク証明書、相互認証証明書には、ARLを公開する場所をURIにて設定する。利用者証明書には、CRLを公開する場所をURIにて設定する。ARL及びCRLを公開する場所は、本CPS 2.6.1項(認証局情報の公開)に規定する。

7.1.3 アルゴリズムの OID

本認証局が発行する各種電子証明書は、SHA1withRSA(OID: 1.2.840.113549.1.1.5)方式を用い、2048bitの本認証局署名鍵で署名される。本認証局が発行する自己署名証明書、リンク証明書、利用者証明書には、RSA方式(OID: 1.2.840.113549.1.1.1)の検証鍵が格納され、当該検証鍵を示すOIDが設定される。相互認証証明書に格納される接続先認証局の検証鍵のアルゴリズムのOIDは、接続先認証局との調整の上決定する。

7.1.4 名前形式

本認証局が発行する各種電子証明書に含まれる各種の識別名は、ITU-T X.500勧告における識別名(DN:Distinguished Name)の規定に従う。自己署名証明書及び利用者の電子証明書における発行者別名(issuerAltName)及び主体者別名(subjectAltName)においては、日本語及び英語(アルファベット)を利用する。上記以外の各識別名においては英語(アルファベット)のみを利用する。

利用者の電子証明書における主体者名(subject)と主体者別名(subjectAltName)については、本CPS 3.1.2項(名前の意味に関する要件)に規定する。

本認証局が発行する電子証明書において、発行者名(issuer)及び発行者別名(issuerAltName)が格納される場合は、以下の値とする。

発行者名(issuer)の設定値は、以下とする。

c=JP

o=Shikoku Electric Power Co.,Inc.

ou=YONDEN CA for Electric Bidding System

発行者別名 (issuerAltName) の設定値は、以下とする。

c=JP
o=四国電力株式会社
ou=よんでん電子入札対応認証局

7.1.5 名前制約

本認証局は、相互認証証明書にnameConstraints を含める場合がある。詳細については、本CPS 7.1.2項(拡張領域)に規定する。

7.1.6 証明書ポリシーの OID

本認証局は、certificatePoliciesを設定する場合がある。詳細については、本CPS 7.1.2項(拡張領域)に規定する。

7.1.7 ポリシ制約

本認証局は、相互認証証明書にpolicyConstraints を含める場合がある。詳細については、本CPS 7.1.2項(拡張領域)に規定する。

7.1.8 有効期間

本認証局が発行する各種電子証明書に記載される有効期間 (Validity) 及び関連する署名鍵の利用期間について以下に整理する。各電子証明書の記載事項はシリアル番号を含み、電子証明書の一意性を確保する。

表 7-2 各種電子証明書の有効期間等

| 電子証明書の種類 | 有効期間 | 署名鍵更新頻度 | 電子証明書発行頻度 |
|---|--|---------|-----------------------|
| 自己署名証明書 (Old With Old及び New With New) | 10年 | 5年毎 | 本認証局署名鍵の更新時 |
| リンク証明書 (OldWithNew) | 旧世代の自己署名証明書の発行日～ 旧世代の自己署名証明書の有効期間の満了日 | - | 本認証局署名鍵の更新時 |
| リンク証明書 (NewWithOld) | 新世代の自己署名証明書の発行日～ 少なくとも旧世代の署名鍵で最後に発行した電子証明書の有効期間の満了日 | - | 本認証局署名鍵の更新時 |
| 相互認証証明書 | 5年以内 | - | 相互認証証明書の有効期間の満了時/失効時等 |
| 利用者証明書 | 発行日を含め761日 | 左記に同じ | 利用者署名鍵の更新時等 |

7.2 失効情報プロファイル

失効情報プロファイルについて、以下に規定する。

7.2.1 バージョン番号

本認証局は、X.509で規定されるバージョン2に準拠した失効情報(CRL/ARL)を発行する。

7.2.2 拡張領域

本認証局が発行するCRL/ARLにおける拡張領域を以下に規定する。

表7-3 CRL/ARLの拡張領域

| 拡張領域の名称 | | criticalフラグ |
|-------------------|--------------------------|-------------|
| CrEntryExtensions | reasonCode | FALSE |
| CrExtensions | authorityKeyIdentifier | FALSE |
| | cRLNumber | FALSE |
| | issuingDistributionPoint | TRUE |

また、本認証局で発行するCRL/ARLにおいて、標準領域のversion、nextUpdateは常に利用する。

(1) 失効理由(reasonCode)

本認証局では、原則としてCRL/ARLにreasonCodeを記載する。

(2) 認証局鍵識別子(authorityKeyIdentifier)

本認証局では、CRL/ARLにおいて、authorityKeyIdentifierとしてkeyIdentifierのみを設定する。

(3) CRL番号(cRLNumber)

本認証局では、CRL/ARLにおいて、cRLNumberを記載する。

(4) 配布点(issuingDistributionPoint)

本認証局は、issuingDistributionPointとしてdistributionPoint、onlyContainsUserCerts又はonlyContainsCACertsを設定する。

CRL/ARLを公開する場所は、本CPS 2.6.1項(認証局情報の公開)に規定する。

CRLの設定値は、以下とする。

distributionPoint: CRL/ARLの配布点をURI形式で設定

onlyContainsUserCerts: TRUE

ARLの設定値は、以下とする。

distributionPoint: CRL/ARLの配布点をURI形式で設定

onlyContainsCACerts: TRUE

8 仕様管理

8.1 仕様変更の手続き

本認証局は、準拠性監査の結果や最新技術の動向を踏まえて業務の改善に努めるとともに、必要ある場合には、遅滞なく本CPSを改訂する。

本認証局は、利用者又は検証者に事前の承諾なしに、随時本CPSを改訂することができる。本認証局は、本CPSに変更が必要と判断される場合には、本認証局の最高意志決定機関にて変更の妥当性を検討し、その実施を判断する。本CPSの変更が発生した場合、本認証局は、本CPSの修正版をリポトリにて遅滞なく公開する。変更後のCPSを承認しない利用者は、修正の公表後15日以内に利用者証明書の失効を要求しなければならない。また、変更後のCPSを承認しない検証者は、証明書の利用を中止しなければならない。

8.2 公表及び通知

本認証局は、本CPSを、本CPS 2.6.1項(認証局情報の公開)に規定されたリポトリに掲載し公開する。

付録

(1) 自己署名証明書の詳細プロフィール

| 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 3 を示す |
| serialNumber (シリアル番号) | ... | | 各電子証明書にユニークな整数 |
| signature (署名アルゴリズム) | | | |
| algorithm identifier (アルゴリズム識別子) | 1.2.840.113549.1.1.5 | | Sha-1 With RSA を示す |
| issuer (発行者名) | c=JP o=Shikoku Electric Power Co.,Inc. ou=YONDEN CA for Electronic Bidding System | | "c"は PrintableString、他の項目は UTF8String で記載 |
| validity (証明書有効期間) | | | |
| notBefore (発行日) | YYMMDDHHMMSSZ | | UTCTimeで記載 |
| notAfter (終了日) | YYMMDDHHMMSSZ | | UTCTimeで記載 |
| subject (主体者名) | c=JP o=Shikoku Electric Power Co.,Inc. ou=YONDEN CA for Electronic Bidding System | | "c"は PrintableString、他の項目は UTF8String で記載 |
| subjectPublicKeyInfo (主体者検証鍵情報) | | | |
| algorithm (アルゴリズム識別子) | 1.2.840.113549.1.1.1 | | |
| subjectPublicKey (検証鍵の値) | ... | | 検証鍵の値 |
| extensions (拡張領域) | | | |
| 領域名 | クリティカル フラグ | 設定値(例) | 補足説明 |
| authorityKeyIdentifier (認証局鍵識別子) | FALSE | ... | 認証局検証鍵のSHA-1 ハッシュ値 |
| keyIdentifier | | ... | |
| subjectKeyIdentifier (主体者鍵識別子) | FALSE | ... | 認証局検証鍵の SHA-1 ハッシュ値 |
| keyUsage (鍵用途) | TRUE | keyCertSign cRLSign | |
| subjectAltName (主体者別名) | FALSE | | |
| directoryName | | c=JP o=四国電力株式会社 ou=よんでん電子入札対応認証局 | "c"はPrintableString、他の項目はUTF8Stringで記載 |
| issuerAltName (発行者別名) | FALSE | | |

| | | | |
|---|-------|--|---|
| directoryName | | c=JP o=四国電力株式会社 ou=よんでん電子入札対応認証局 | “c”は PrintableString、他の項目は UTF8String で記載 |
| basicConstraints (基本制約) | TRUE | | |
| cA | | TRUE | |
| cRLDistributionPoints (CRL 配布点) | FALSE | | |
| distributionPoint | | ldap://repository.ynss.yonden.co.jp/ ou=YONDEN%20CA%20for%20E lectronic%20Bidding%20System,o= Shikoku%20Electric%20Power%20 Co.%5C%2CInc.,c=JP?authorityRe vocationList | URI にて記載 |

(2) リンク証明書 (Old With New及びNew With Old) の詳細プロフィール

| 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 3 を示す |
| serialNumber (シリアル番号) | ... | | 各電子証明書にユニークな整数 |
| signature (署名アルゴリズム) | | | |
| algorithm identifier (アルゴリズム識別子) | 1.2.840.113549.1.1.5 | | Sha-1 With RSA を示す |
| issuer (発行者名) | c=JP o=Shikoku Electric Power Co.,Inc. ou=YONDEN CA for Electronic Bidding System | | "c"は PrintableString、他の項目は UTF8String で記載 |
| validity (証明書有効期間) | | | |
| notBefore (発行日) | YYMMDDHHMMSSZ | | UTCTimeで記載 Old With New: 旧世代の自己署名証明書の発行日 New With Old: 新世代の自己署名証明書の発行日 |
| notAfter (終了日) | YYMMDDHHMMSSZ | | UTCTimeで記載 Old With New: 旧世代の自己署名証明書の有効期間の満了日 New With Old: 少なくとも旧世代の署名鍵で最後に発行した電子証明書の有効期間の満了日 |
| subject (主体者名) | c=JP o=Shikoku Electric Power Co.,Inc. ou=YONDEN CA for Electronic Bidding System | | "c"は PrintableString、他の項目は UTF8String で記載 |
| subjectPublicKeyInfo (主体者検証鍵情報) | | | |
| algorithm (アルゴリズム識別子) | 1.2.840.113549.1.1.1 | | |
| subjectPublicKey (検証鍵の値) | ... | | OldWithNew: 旧世代の検証鍵 NewWithOld: 新世代の検証鍵 |
| extensions (拡張領域) | | | |
| 領域名 | クリティカル フラグ | 設定値(例) | 補足説明 |

| | | | |
|--|-------|--|--|
| authorityKeyIdentifier (認証局鍵識別子) | FALSE | ... | OldWithNew: 新世代の認証局検証鍵の SHA-1 ハッシュ値 NewWithOld: 旧世代の認証局検証鍵の SHA-1 ハッシュ値 |
| keyIdentifier | | ... | |
| subjectKeyIdentifier (主体者鍵識別子) | FALSE | ... | OldWithNew: 旧世代の認証局検証鍵の SHA-1 ハッシュ値 NewWithOld: 新世代の認証局検証鍵の SHA-1 ハッシュ値 |
| keyUsage (鍵用途) | TRUE | keyCertSign cRLSign | |
| certificatePolicies (証明書ポリシー) | FALSE | | |
| policyIdentifier | | 2.5.29.32.0 | "ANY-POLICY"を示す |
| basicConstraints (基本制約) | TRUE | | |
| cA | | TRUE | |
| cRLDistributionPoints (CRL 配布点) | FALSE | | |
| distributionPoint | | ldap://repository.ynss.yonden.co.jp/ ou=YONDEN%20CA%20for%20El ectronic%20Bidding%20System,o= Shikoku%20Electric%20Power%20 Co.%5C%2CInc.,c=JP?authorityRe vocationList | URI にて記載 |

(3) 相互認証証明書の詳細プロフィール

| 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 3 を示す |
| serialNumber (シリアル番号) | ... | | 各電子証明書にユニークな整数 |
| signature (署名アルゴリズム) | | | |
| algorithm identifier (アルゴリズム識別子) | 1.2.840.113549.1.1.5 | | Sha-1 With RSA を示す |
| issuer (発行者名) | c=JP o=Shikoku Electric Power Co.,Inc. ou=YONDEN CA for Electronic Bidding System | | "c"は PrintableString、他の項目は UTF8String で記載 |
| validity (証明書有効期間) | | | |
| notBefore (発行日) | YYMMDDHHMMSSZ | | UTCTimeで記載 |
| notAfter (終了日) | YYMMDDHHMMSSZ | | UTCTimeで記載 |
| subject (主体者名) | c=JP o=Japanese Government ou=BridgeCA | | 相互認証先の認証局の名称 左記は設定例である |
| subjectPublicKeyInfo (主体者検証鍵情報) | | | |
| algorithm (アルゴリズム識別子) | 1.2.840.113549.1.1.1 | | |
| subjectPublicKey (検証鍵の値) | ... | | 検証鍵の値 |
| extensions (拡張領域) | | | |
| 領域名 | クリティカルフラグ | 設定値(例) | 補足説明 |
| authorityKeyIdentifier (認証局鍵識別子) | FALSE | ... | 認証局検証鍵のSHA-1 ハッシュ値 |
| keyIdentifier | | ... | |
| subjectKeyIdentifier (主体者鍵識別子) | FALSE | ... | BCA 検証鍵の SHA-1 ハッシュ値 |
| keyUsage (鍵用途) | TRUE | keyCertSign cRLSign | |
| certificatePolicies (証明書ポリシ) | TRUE | | |
| policyIdentifier | | 1.2.392.200146.1.1.1 | 本認証局の証明書ポリシ |
| policyQualifiers policyQualifierId qualifier | | 1.3.6.1.5.5.7.2.1 http://www.yonden.co.jp/business/nisho/document/gyoumu.pdf | id-qt-cps 本認証局のCPS公開場所 IA5Stringで記載 |
| policyMappings (ポリシマッピング) | FALSE | | |

| | | | |
|---|-------|--|---------------|
| issuerDomainPolicy | | 1.2.392.200146.1.1.1 | 本認証局の証明書ポリシー |
| subjectDomainPolicy | | ... | 相互接続先の証明書ポリシー |
| basicConstraints (基本制約) | TRUE | | |
| cA | | TRUE | |
| policyConstraints (ポリシー制約) | TRUE | | |
| requireExplicitPolicy | | 0 | |
| cRLDistributionPoints (CRL 配布点) | FALSE | | |
| distributionPoint | | ldap://repository.ynss.yonden.co.jp/ou=YONDEN%20CA%20for%20Electronic%20Bidding%20System,o=Shikoku%20Electric%20Power%20Co.%5C%2CInc.,c=JP?authorityRevocationList | URI にて記載 |

(4) 利用者証明書の詳細プロフィール

| 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 3 を示す |
| serialNumber (シリアル番号) | ... | | 各電子証明書にユニークな整数 |
| signature (署名アルゴリズム) | | | |
| algorithm identifier (アルゴリズム識別子) | 1.2.840.113549.1.1.5 | | Sha-1 With RSA を示す |
| issuer (発行者名) | c=JP o=Shikoku Electric Power Co.,Inc. ou=YONDEN CA for Electronic Bidding System | | "c"は PrintableString、他の項目は UTF8String で記載 |
| validity (証明書有効期間) | | | |
| notBefore (発行日) | YYMMDDHHMMSSZ | | UTCTimeで記載 |
| notAfter (終了日) | YYMMDDHHMMSSZ | | UTCTimeで記載 |
| subject (主体者名) | c=JP st=kagawa l=takamatsu-shi, ... cn=Ichiro Tanaka uid=03100101-001 | | "c"は PrintableString、他の項目は UTF8String で記載 左記は、c=JP は固定値、他の項目は設定例である |
| subjectPublicKeyInfo (主体者検証鍵情報) | | | |
| algorithm (アルゴリズム識別子) | 1.2.840.113549.1.1.1 | | |
| subjectPublicKey (検証鍵の値) | ... | | 検証鍵の値 |
| extensions (拡張領域) | | | |
| 領域名 | クリティカル フラグ | 設定値(例) | 補足説明 |
| authorityKeyIdentifier (認証局鍵識別子) | FALSE | ... | 認証局検証鍵のSHA-1 ハッシュ値 |
| keyIdentifier | | ... | |
| subjectKeyIdentifier (主体者鍵識別子) | FALSE | ... | 利用者検証鍵の SHA-1 ハッシュ値 |
| keyUsage (鍵用途) | TRUE | digitalSignature nonRepudiation | |
| certificatePolicies (証明書ポリシー) | TRUE | | |
| policyIdentifier | | 1.2.392.200146.1.1.1 | 本認証局の証明書ポリシー |
| policyQualifiers policyQualifierId qualifier | | 1.3.6.1.5.5.7.2.1 http://www.yonden.co.jp/business/nisho/document/gyoumu.pdf | id-qt-cps IA5Stringで記載 本認証局のCPS公開場所 |

| | | | |
|---|-------|--|--|
| subjectAltName (主体者別名) | FALSE | c=JP st=香川県 l=高松市... o=四国電力株式会社 cn=田中 一郎 | "c"は PrintableString、他の項目は UTF8String で記載 左記は、c=JP は固定値、他の項目は設定例である。 利用者が商業登記をしていない利用組織に所属する場合には記載しない。 |
| directoryName | | | |
| issuerAltName (発行者別名) | FALSE | c=JP o=四国電力株式会社 ou=よんでん電子入札対応認証局 | "c"は PrintableString、他の項目は UTF8String で記載 |
| directoryName | | | |
| cRLDistributionPoints (CRL 配布点) | FALSE | ldap://repository.ynss.yonden.co.jp/ou=YONDEN%20CA%20for%20Electronic%20Bidding%20System,o=Shikoku%20Electric%20Power%20Co.%5C%2CInc.,c=JP?certificateRevocationList | URI にて記載 |
| distributionPoint | | | |

(5) ARLの詳細プロフィール

| 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 2 を示す |
| signature (署名アルゴリズム) | | | |
| algorithm identifier (アルゴリズム識別子) | 1.2.840.113549.1.1.5 | | Sha-1 With RSA を示す |
| issuer (発行者名) | c=JP o=Shikoku Electric Power Co.,Inc. ou=YONDEN CA for Electronic Bidding System | | “c”は PrintableString、他の項目は UTF8String で記載 |
| thisUpdate (今回の更新日時) | YYMMDDHHMMSSZ | | UTCTime で記載 |
| nextUpdate (次回の更新日時) | YYMMDDHHMMSSZ | | UTCTime 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シリアル番号 |
| revocationDate (失効日時) | YYMMDDHHMMSSZ | | 失効処理が行われた日時 UTCTime で記載 |
| crEntryExtensions (失効した電子証明書ごとの拡張領域) | | | |
| 領域名 | クリティカル フラグ | 設定値(例) | 補足説明 |
| reasonCode (失効事由) | FALSE | cessationOfOperation | 左記は設定例である |
| crExtensions (拡張領域) | | | |
| 領域名 | クリティカル フラグ | 設定値(例) | 補足説明 |
| authorityKeyIdentifier (認証局鍵識別子) | FALSE | ... | 認証局検証鍵のSHA-1 ハッシュ値 |
| keyIdentifier | | ... | |
| cRLNumber (CRL 番号) | FALSE | 150 | 左記は設定例である |
| issuingDistributionPoint (発行者配布点) | TRUE | | |
| distributionPoint | | ldap://repository.ynss.yonden.co.jp/ou=YONDEN%20CA%20for%20Electronic%20Bidding%20System,o=Shikoku%20Electric%20Power%20Co.%5C%2CInc.,c=JP?authorityRevocationList | URI にて記載 |
| onlyContainsCACerts | | TRUE | |

(6) CRLの詳細プロファイル

| 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 2 を示す |
| signature (署名アルゴリズム) | | | |
| algorithm identifier (アルゴリズム識別子) | 1.2.840.113549.1.1.5 | | Sha-1 With RSA を示す |
| issuer (発行者名) | c=JP o=Shikoku Electric Power Co.,Inc. ou=YONDEN CA for Electronic Bidding System | | "c"は PrintableString、他の項目は UTF8String で記載 |
| thisUpdate (今回の更新日時) | YYMMDDHHMMSSZ | | UTCTime で記載 |
| nextUpdate (次回の更新日時) | YYMMDDHHMMSSZ | | UTCTime 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シリアル番号 |
| revocationDate (失効日時) | YYMMDDHHMMSSZ | | 失効処理が行われた日時 UTCTime で記載 |
| crEntryExtensions (失効した電子証明書ごとの拡張領域) | | | |
| 領域名 | クリティカル フラグ | 設定値(例) | 補足説明 |
| reasonCode (失効事由) | FALSE | cessationOfOperation | 左記は設定例である |
| crExtensions (拡張領域) | | | |
| 領域名 | クリティカル フラグ | 設定値(例) | 補足説明 |
| authorityKeyIdentifier (認証局鍵識別子) | FALSE | ... | 認証局検証鍵のSHA-1 ハッシュ値 |
| keyIdentifier | | ... | |
| cRLNumber (CRL 番号) | FALSE | 160 | 左記は設定例である |
| issuingDistributionPoint (発行者配布点) | TRUE | | |
| distributionPoint | | ldap://repository.ynss.yonden.co.jp/ou=YONDEN%20CA%20for%20Electronic%20Bidding%20System,o=Shikoku%20Electric%20Power%20Co.%5C%2CInc.,c=JP?certificateRevocationList | URI にて記載 |
| onlyContainsUserCerts | | TRUE | |