日本税理士会連合会電子認証局

税理士証明書発行サービス

認証業務運用基準（ＣＰ／ＣＰＳ）

Ver. 2.92

平成２４年１０月１５日

日本税理士会連合会

改版履歴

バージョン	改版日付	改版内容	作成者	承認者
１．０	2004.1.16	初版発行	金田 好史	森 金次郎
１．１	2005.1.20	・用語統一 ・誤記訂正 ・運営委員会の構成人数を変更 ・1.1 概要で加入者証明書に記載される氏名がローマ字であることを明確に表示 ・2.1.6 加入者の義務で加入者証明書に記載される氏名がローマ字であることを明確に表示 ・2.1.6 加入者の義務で加入者証明書に通称名または旧姓が記載される場合を明確に表示 ・2.1.7 検証者の義務で加入者証明書に記載される氏名がローマ字であることを明確に表示 ・2.1.7 検証者の義務で加入者証明書に通称名または旧姓が記載される場合を明確に表示 ・3.1.2 名称の意味に関する要件で加入者証明書に通称名または旧姓が記載される場合を明確に表示 ・4.1.2 発行申請の審査に「利用の申込みに対する諾否」で「否」の判断がされた場合、発行申請書類一式を返却しないことを追加 ・5.1.2 認証設備室の(2)災害対策でＵＰＳを備えていることを追加 ･3.1.7IC カード及び PIN 情報の郵送先を明確に表示 ・4.2 IC カード及び PIN 情報の郵送先を明確に表示 ･6.2.13 IC カード及び PIN 情報の郵送先を明確に表示	金田 好史	森 金次郎

バージョン	改版日付	改版内容	作成者	承認者
１．２	2005.4.21	・審査手順の統一 ・2.1.6 PIN の変更間隔を変更 ・2.7.1 認証局情報の公開に各種案内書類を追加 ・2.11 個人情報保護で代理人からの開示の求めを受領するように変更。 ・2.11 個人情報保護で個人情報の訂正、消去についての記述を追加 ・3.4.1 開示申請者の確認で代理人が申請を行ってきた場合に申請者を確認する手順を追加 ・4.3 加入者証明書及び秘密鍵の受領で利用者が郵送または持参する印鑑登録証明書の有効期限を明確に表示 ・4.6.1 加入者情報の開示で開示申請を代理人が行う場合の手順を追加 ・4.6.1 加入者情報の開示で申請者が郵送または持参する書類（印鑑登録証明書、住民票の写し、登録原票記載事項証明書、戸籍抄本または個人事項証明書）の有効期限を明確に表示 ・4.6.2 加入者情報の開示で開示申請が適当でないと判断する適用例を変更 ・4.7.1 加入者証明書の失効請求で請求者が郵送または持参する書類（印鑑登録証明書、住民票の写し、登録原票記載事項証明書、戸籍抄本または個人事項証明書）の有効期限を明確に表示 ・6.4.2 PIN の変更間隔を変更	金田 好史	森 金次郎
１．３	2005.12.22	・9.1 本基準の変更手続きで本基準の改訂内容を運営委員会委員長が承認後に遅滞なく改訂を行うことを追加	中島　宏夫	森 金次郎
１．４	2007.5.9	・3.1.9 加入者の本人性の確認で税理士資格の有効性確認時に税理士業務が禁止となっていないことを確認することを追加 ・3.5.1 失効請求者の確認で電子証明書失効請求書の失効事由が[税理士登録の抹消]または[税理士業務の停止・禁止]の場合は、税理士資格の有効性の確認を行わないことを追加。	中島　宏夫	森 金次郎

バージョン	改版日付	改版内容	作成者	承認者
		・4.7 加入者証明書の失効請求に加入者証明書の失効事由として税理士業務の禁止処分を追加 ・4.7.5 電子認証局の判断による加入者証明書の失効に加入者証明書の失効事由として税理士業務の禁止処分を追加		
２．０	2008.3.25	・誤記訂正 ・システム運用要員を削除 ・1.3.1 登場者とその役割で HSM 鍵管理者の役割を変更 ・1.3.1 登場者とその役割でシステム管理要員の役割を変更 ・1.3.1 登場者とその役割にセキュリティセンタの要員を追加 ・1.4 連絡先に直通の電話番号を追加 ・2.6 加入者証明書の有効期間を変更 ・3.1.9 加入者の本人性の確認で公的機関から発行された書類の発行日が電子証明書発行申請書兼利用同意書の記入年月日より前後３ヶ月以内に発行されたものであることを確認するように変更 ・3.4.1 開示申請者の確認で公的機関から発行された書類の発行日が電子証明書発行申請書兼利用同意書の記入年月日より前後３ヶ月以内または前後１ヶ月以内に発行されたものであることを確認するように変更 ・3.5.1 失効請求者の確認で公的機関から発行された書類の発行日が電子証明書発行申請書兼利用同意書の記入年月日より前後３ヶ月以内に発行されたものであることを確認するように変更 ・4.1 申請者へ送付する電子証明書発行申請書兼利用同意書から氏名の印刷を削除 ・4.1.2 発行申請の審査において書類不備及び記載事項不備の場合は、発行申請書類一式を不備内容が記載された申請書類再提出のお願いと合わせて返送することに変更 ・4.1.2 発行申請の審査において「利用の申込みに対する諾否」で「諾否」の判断がされた場合は、発行審査結果通知書を送付することに変更 ・4.1.3 電子証明書記載内容の登録作業は審査登録作業室で行うことに変更	中島　宏夫	池田 隼啓

バージョン	改版日付	改版内容	作成者	承認者
		・4.6.1 加入者情報の開示申請で加入者情報開示申請書の必要事項に開示対象の電子証明書を追加 ・4.7.1 加入者証明書の失効請求で電子証明書失効請求書の必要事項から氏名ローマ字を削除 ・4.7.1　電子証明書失効請求書の必要事項に失効対象の電子証明書を追加 ・4.7.2　電子証明書失効請求書と電子証明書発行申請書兼利用同意書の一致確認は税理士登録番号だけでなく電子証明書失効請求書に記載された内容で確認するよう記載を変更 ・4.9 自己署名証明書の更新期間を変更 ・4.12 委託先要員の教育訓練を変更 ・6.2.6 加入者の秘密鍵を取り出す要員をセキュリティセンタシステム担当者に変更 ・6.3.2 CA 秘密鍵の有効期間を変更 ・6.3.2 相互認証証明書の有効期間を変更 ・6.4.1 CA 秘密鍵を活性化するための PIN 情報の設定をセキュリティセンタシステム担当者及び HSM 鍵管理者が行うように変更 ・6.4.1 加入者の秘密鍵を活性化するための PIN 情報を取り出す要員をセキュリティセンタシステム担当者に変更		
２．１	2008.10.16	･2.1.1 電子認証局の義務に IC カード作成後直ちに当該加入者の秘密鍵及び IC カードの PIN 情報を設備、あるいはシステム上より完全に消去することを明記。	中島　宏夫	池田 隼啓
２．２	2009.5.25	・4.1.1 申請に発行申請書類が郵送または持参以外の方式で提出された場合は、書類一式を郵送で返却することを追加。	中島　宏夫	池田 隼啓
２．３	2009.9.25	・用語の定義 「発行申請者」を定義。 ・用語の明確化 「加入者」と「発行申請者」の用語の使い分けを明確化。 ・誤記訂正 2.6 旧電子証明書の発行に係る表現を過去形に修正。 ・更新認定調査の指摘に基づく変更 4.10CA 秘密鍵が危殆化した場合、危殆化した虞がある場合には、CA 秘密鍵及びバックアップ媒体の完全な初期化又は物理的に	中島　宏夫	池田　隼啓

		破壊することとし、自己署名証明書は失効しないよう修正		
２．４		＜該当なし＞		
２．５	2010.7.20	＜誤記訂正＞ ・1.3.1 表 1-3 の発行審査担当者の役割にある「加入者」の表記を「発行申請者」に訂正 ・2.1.3「発行申請者」の表記を追加 ・2.1.6「加入を希望する者」の表記を追加、「発行申請者」の表記を「加入を希望する者」に訂正 ・2.3.2 中にある「2.1.6 加入者の義務」の表記を「2.1.6 加入を希望する者及び加入者の義務」に訂正 ・4.1.2 中にある「3.1.9 加入者の本人性の確認」の表記を「3.1.9 発行申請者の本人性の確認」に訂正 ＜送付書類の追加＞ ・4.1 送付物に「氏名ローマ字表記を変更される場合の注意事項」を追記 ＜加入者情報の開示の手続きの見直し＞ ・1.5 用語に「元加入者」の定義を追加 ・加入者情報の開示手続きに「元加入者」を追加	中島　宏夫	池田　隼啓
２．６	2010.9.17	＜用語の定義を修正＞ ・1.5 で規定されている「元加入者」の定義について有効期限切れを想定した文言に修正 ＜誤記訂正＞ ・目次中にある「2.9.4 加入者の申請による機密情報の開示」を「2.9.4 開示申請による機密情報の開示」に訂正 ・2.1.6 中にある「電子証明書発行申請書兼利用者同意書」を「電子証明書発行申請書兼利用同意書」に訂正 ・4.1.2 中にある「本基準 3.1.9（加入者の本人性の確認)」を「本基準 3.1.9（発行申請者の本人性の確認)」に訂正	中島　宏夫	池田　隼啓
２．７	2011.7.25	＜誤記訂正＞ ・6.2.1 中にある「FIPS140-1 レベル 3」を「FIPS140-2 レベル 3」に訂正 ＜実態に即するための変更＞ ・Copyright の取得年を 2004 年に変更	樋口　久倫	池田　隼啓

		・表 1-3 の発行審査担当者の役割中にある加入者証明書の開示を行おうとする者に「元加入者」を追記 ・2.1.6 に電子証明書受領書を返送する場合は、電子証明書発行申請書兼利用同意書に使用した印鑑を押印することを義務化 ・2.11 の個別通知を行わない者に「元加入者」、「代理人」を追記 ・4.3、4.6.1、4.7.1 に郵送または持参以外の方式で提出された場合の対応方法を明記		
２．８		＜該当なし＞		
２．９	2012.7.31	＜審査登録作業室の廃止＞ ・審査登録作業室を廃止し、登録局の機能をアーカイブ室に統合することによる関係箇所の修正 ＜サービス廃止時の CRL について取扱いを明確化＞ ・4.11 に発行した全ての加入者証明書の期限が満了している場合は、サービス廃止後に CRL/ARL の公開はしないことを明記	樋口　久倫	池田　隼啓
２．９１	2012.8.9	＜登録原票記載事項証明書の廃止に伴う修正＞ 登録原票記載事項証明書が廃止されることに伴い、外国人の実在性を証する書面として「住民票の写し又はそれに準ずるもの」の提出を求めるよう関係箇所を修正 ＜ARL の公開＞ 4.11 に発行した全ての加入者証明書について有効期限が過ぎている場合に本サービスを廃止するときに ARL の公開はしないと規定されていたものを「一定期間公開する」と修正	樋口　久倫	池田　隼啓
２．９２	2012.10.15	＜住民票の写しに準ずる書類の削除＞ 登録原票記載事項証明書が廃止されることに伴い、経過措置として外国人の実在性を確認する書面として「住民票の写し又はそれに準ずるもの」の提出を求めていたが、登録原票記載事項証明書の廃止から 3 ヶ月を経過することから、当該経過措置を廃止する。	樋口　久倫	池田　隼啓

目　次

1　はじめに

1.1 概要

日本税理士会連合会（以下、「日税連」という。）は、税理士法（昭和２６年6月１５日法律第二百三十七号）の規定に従って日税連に備える税理士名簿（以下、「税理士名簿」という。）に登録された者（以下、「税理士」という。）に対して公開鍵暗号技術に基づく電磁的記録（以下、「加入者証明書」という。）を発行するために日本税理士会連合会電子認証局（以下、「電子認証局」という。）を組織する。

電子認証局は、その認証業務として税理士証明書発行サービス（以下、「本サービス」という。）を税理士に対し提供する。税理士は、任意に加入者証明書の発行を申請することができ、加入者証明書の発行を受けた税理士は、電子認証局の加入者となる。

なお、各加入者に対して有効な加入者証明書は、複数枚発行しない（加入者証明書の更新期間を除く）。

本サービスは、「電子署名及び認証業務に関する法律（平成１２年５月３１日法律第百二号）」（以下、「電子署名法」という。）の規定に基づき主務大臣の認定を受けた特定認証業務である。

本サービスは、加入者証明書に記載された所有者に関する情報が、税理士名簿に登録された本人の情報と一致すること、すなわち加入者証明書に記載された公開鍵情報と対になる秘密鍵情報の所有者が税理士であることを第三者に対して証明するものである。ただし、加入者証明書に記載されている氏名（ローマ字）以外の情報は、電子署名法上の認定対象外の事項である。

本サービスは、電子申告など電子化された行政手続きにおいて利用可能とするため、政府認証基盤（以下、「ＧＰＫＩ」という。）との接続を行うものである。

この文書は、本サービスの運用にあたって重要となる以下の事項について規定した認証業務運用基準（ＣＰ／ＣＰＳ）（以下、「本基準」という。）である。

- 電子認証局が行う加入者証明書の発行、失効及びその他本サービスの運用管理に関する諸手続き
- 電子認証局を中心とする公開鍵基盤（ＰＫＩ：Public Key Infrastructure）の要素である電子認証局、加入者及び検証者の義務及び責任

本基準は、本サービスに関する最上位の規定であり、公開文書である。また、本サービスの手順の細目は、本基準に基づいて事務取扱要領等に規定される。

1.2 名称

本サービスの名称、本基準及び関連する組織に対して割り当てられたオブジェクト識別子（ＯＩＤ）は表 1-1 の通りである。

表 1-1 税理士証明書発行サービス関連オブジェクト識別子

ＯＩＤ	オブジェクト
1.2.392.200151	Japan Federation of Certified Public Tax Accountants' Associations
1.2.392.200151.1	Japan Federation of Certified Public Tax Accountants' Associations CA
1.2.392.200151.1.1	Certification Service for Public Tax Accountants
1.2.392.200151.1.1.1	Certification Service for Public Tax Accountants Policy & CPS
1.2.392.200151.1.1.2	Certification Service for Public Tax Accountants (For GPKI TEST)

1.3 コミュニティと適応可能性

1.3.1 登場者と役割

本サービスに関連する要素の機能関連を図 1-1 に示す。また、登場者とそれぞれの役割を表 1-2 に示す。

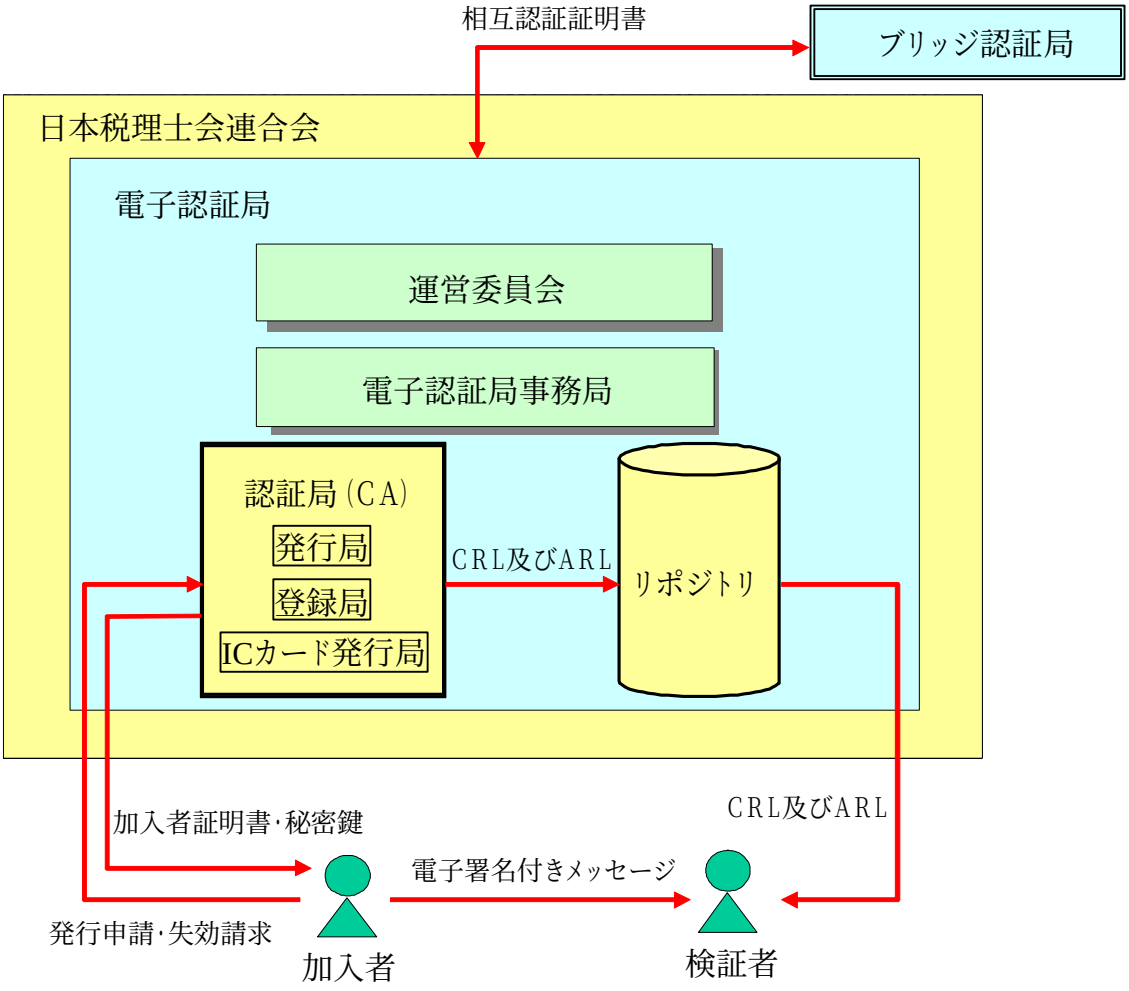

図 1-1 電子認証局機能関連図

表 1-2 登場者とその役割

（網掛け部分は機能要素をあらわす）

登場者	役割
日本税理士会連合会	・ 発行申請書類の発送業務 ・ 監査人の選任 ・ 電子証明書発行取扱規程の改定
電子認証局	・ 本サービスの運営主体 ・ 運営委員会、運営責任者、運用要員（本基準 1.5 用語参照）及び委託先要員（本基準 1.5 用語参照）により運営される。 ・ 本基準及び事務取扱要領の改訂
運営委員会	・ 認証業務の開始と終了に係る事項、相互認証の開始、更新、失効に係る事項及びその他電子認証局の運営に関する重要な事項について決定し、運営責任者からの承認または決定依頼要請に対し、承認または決定する。 ・ 運営委員会は、運営委員会委員長及び委員４名以内で構成する。 ・ 運営委員会委員長は、運営責任者に対する指揮監督、運営責任者及び運用要員の任免並びに準拠性監査実施の指示を行う。
電子認証局事務局	・ 運営責任者の指揮命令のもとで、電子認証局の日常的な業務運用を行う。
認証局（ＣＡ）	・ 発行局、登録局及びＩＣカード発行局から構成されるシステム
発行局	・ 発行局は、加入者の鍵ペア及びＰＩＮ情報の生成を行う。 ・ 発行局は、加入者証明書に関する失効リスト（ＣＲＬ、以下「ＣＲＬ」という。）と電子認証局に関する失効リスト（ＡＲＬ、以下「ＡＲＬ」という。）を発行する。 ・ 発行局は、ＧＰＫＩと接続するため、ブリッジ認証局との間で相互認証証明書の発行及び失効を行う。 ・ 発行局は、登録局の指示により、加入者証明書の発行を行う。
登録局	・ 登録局は、ＲＡ登録操作員が登録した加入者情報または失効情報を管理し、発行局に対して加入者証明書またはＣＲＬの発行を要求する。 ・ 登録局は、加入者証明書の発行、開示に関する申請情報及び失効請求の真偽の審査を行う。
IC カード発行局	・ ＩＣカード発行局は、加入者の秘密鍵及び加入者証明書のＩＣカードへの格納から加入者への配布までを行う。
リポジトリ	・ 電子認証局の運営に関する情報、自己署名証明書等の電子証明書情報、ＣＲＬ及びＡＲＬ等を保管してインターネット上に公開する。 ・ 電子証明書情報、ＣＲＬ及びＡＲＬを公開するディレクトリサーバと本基準等を公開するＷｅｂサーバからなる。
加入者	・ 加入者証明書に記載された公開鍵情報と対になる秘密鍵情報の所有者であり、税理士名簿に登録された税理士である。 ・ 加入者証明書の発行を受けるためには、別に定める電子証明書発行申請書兼利用同意書により、電子認証局に対して加入者証明書の発行申請を行う。
検証者	・ 加入者の加入者証明書と電子認証局を信頼して加入者の作成した電子署名情報の正当性を検証する者である。
ブリッジ認証局（ＢＣＡ）	・ 日本政府により運用される認証局であり、行政機関認証局と民間認証局との中間に位置し、それぞれと相互認証を行う。

運営責任者、運用要員（電子認証局事務局）及びセキュリティセンタの要員を表 1-3 に示す。

表 1-3 運営責任者、運用要員（電子認証局事務局）及びセキュリティセンタの要員とその役割

登場者	役割
運営責任者	・ 電子認証局の運営事務に関する責任者 ・ 電子認証局の運営事務について運用要員を指揮命令し、本基準及び事務取扱要領等に則り適正な運営を行う。 ・ ＧＰＫＩに接続するため、相互運用性仕様書に基づいてブリッジ認証局との相互認証を実施する。 ・ 本サービスの実施に当たって本基準を作成し、運営委員会委員長の承認を得た後公開する。 ・ 運営責任者は、本基準を遵守することを条件として、電子認証局の業務の一部を外部に委託することができる。
ＨＳM鍵管理者	・ 秘密鍵管理装置（以下、「ＨＳＭ」という。）の操作を行うための物理鍵 B を保管する金庫のＰＩＮを管理する。 ・ ＣＡ秘密鍵のバックアップ媒体を安全に保管する。 ・ セキュリティセンタシステム担当者の作業においてＨＳＭの操作が必要なときは、これに立会う。 ・ ＨＳＭの操作を行うための物理鍵 A を管理する。 ・ ＣＡ秘密鍵の活性化・非活性化を行う。 ・ ＣＡ秘密鍵の生成、バックアップ、リカバリ及び廃棄を行う。
システム管理要員	・ アーカイブ室に設置するシステムについて、運用要員のアカウントの管理、その他システムの維持を行う。 ・ ＣＡ秘密鍵の生成、バックアップ、リカバリ、廃棄及びブリッジ認証局との相互認証に立会う。 ・ 加入者情報の開示において、加入者証明書のハードコピーを作成する。
発行審査担当者	・ 発行申請者からの加入者証明書発行申請を受け付け、別に定める必要書類等の確認と税理士名簿の確認を行い、当該申請者に加入者証明書を発行する事が妥当であるかを審査する。 ・ 加入者情報の開示を行おうとする加入者、元加入者または代理人（以下、「開示申請者」という。）からの加入者情報開示申請を受け付け、別に定める必要書類等の確認を行い、開示申請者に開示情報を開示することが妥当であるかを審査する。 ・ 加入者証明書の失効請求を行おうとする加入者（以下、「失効請求者」という。）からの加入者証明書失効請求を受け付け、別に定める必要書類等の確認を行い、当該加入者の加入者証明書を失効することが妥当であるかを審査する。
ＲＡ登録操作員	・ 加入者情報を登録局に登録するために、専用端末（以下、「ＲＡ操作端末」という。）を操作し、加入者証明書の発行を要求する。 ・ 加入者証明書の失効審査が完了した後、専用のＲＡ操作端末を使用して登録局に対して失効情報を登録し、加入者証明書の失効を要求する。
セキュリティセンタ責任者	・ セキュリティセンタの全責任者 ・ ＨＳＭ操作を行うための物理鍵 B を保管する金庫の物理鍵を管理する。
セキュリティセンタ運用員管理者	・ 電子認証局のサーバ機器が設置され運用される認証設備室への入室権限と入退室記録を管理する。

登場者	役割
	・ 入退室記録を日常チェックする。 ・ 認証設備室の設備維持。 ・ 操作員の認証に用いる電子証明書の発行、失効操作を行う。 ・ 認証設備室に設置するシステムについて、運用要員及びセキュリティセンタの要員のアカウントの管理を行う。 ・ 認証設備室に設置するシステムについて、電子認証局の運営にあたって必要となるシステム管理（起動、停止、バックアップ、リストア、監視ログの保管、アーカイブログの保管及びパッチ適用）を行う。 ・ リポジトリに関する登録更新操作を行う。 ・ ＨＳＭの操作を行うための物理鍵 B を管理する。 ・ ＣＡ秘密鍵の活性化・非活性化に立会う。 ・ ＣＡ秘密鍵の生成、バックアップ、リカバリ及び廃棄を行う。
セキュリティセンタシステム担当者	・ 認証設備室内のインターネット側に設置したファイアウォールのメンテナンス。 ・ 加入者証明書に記載された公開鍵情報、それと対になる秘密鍵情報及びＰＩＮ情報をＩＣカードに格納するため、発行局からの取り出しと運搬を行う。 ・ 本サービスにおいて、発行する加入者証明書に記載するプロファイル情報の登録変更管理を行う。 ・ ＧＰＫＩと接続するための相互認証証明書の発行、更新、失効等の操作を行う。 ・ 自己署名証明書の更新、失効及びリンク証明書の発行、更新、失効等の操作を行う。 ・ ＣＡ秘密鍵の生成、バックアップ、リカバリ及び廃棄を行う。
セキュリティセンタ監視担当者	・ 電子認証局のサーバ設備、ネットワーク設備、その他建屋の設備について日常的に運用状況を監視し、障害等が検知された場合は電子認証局事務局に通報する。

1.3.2　加入者証明書に記載される属性の取り扱い

電子署名法では、加入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、加入者の氏名、住所及び生年月日に限定している。このため、本サービスで発行された加入者証明書の記載事項のうちローマ字の氏名以外は認定の対象外である。加入者の税理士登録番号は、当該加入者の属性情報であり電子署名法における認定制度の対象外である。

1.3.3　加入者証明書の用途

本サービスにおいて発行される加入者証明書の用途は、以下の事務を電子的に行う場合に限定する。

① 税理士法第二条に定める事務
② 自己の租税に係る行政機関への申告、申請、届出等（ただし、加入者証明書に記載する氏名が旧姓の場合を除く。）
③ 日税連または税理士会への申請、届出等

1.3.4　ＣＡ秘密鍵の用途

ＣＡ秘密鍵の用途は、本サービスにおいて発行する加入者証明書への電子署名に使用される。
上記以外にＣＡ秘密鍵を使用する場合は、以下の用途に限定される。

① ブリッジ認証局に対して発行する相互認証証明書への電子署名
② 本電子認証局の自己署名証明書への電子署名
③ ＣＡ秘密鍵の更新処理のためのリンク証明書への電子署名
④ 操作員（ＲＡ登録操作員、システム管理要員及びセキュリティセンタシステム担当者）認証のための電子証明書への電子署名
⑤ ＣＲＬ及びＡＲＬへの電子署名
⑥ ＷｅｂＲＡサーバ証明書への電子署名

1.4 連絡先

本サービスに関する問い合わせは、電話、ＦＡＸまたは電子メールにより受け付ける。

認証事業者の名称	：日本税理士会連合会
所在地	:〒１４１－００３２　東京都品川区大崎１－１１－８　日本税理士会館８階
代表者	：日本税理士会連合会会長
担当部署	：日本税理士会連合会電子認証局事務局
対応時間	：１０時～１２時及び１３時～１７時（土日祝祭日、１2/２９～1/3を除く）
電話番号	：０３－５４３５－０９４０（直通）　０３－５４３５－０９３１（代表）
ＦＡＸ	：０３－５４３５－０９４１
電子メール	：ca-info@nichizeiren.jp

1.5 用語

本基準で使用する用語を以下に定義する。

ＡＲＬ：Authority Revocation List
電子証明書の有効期間中に何らかの理由により失効された電子認証局の電子証明書を示す失効リスト

ＣＡ秘密鍵
電子認証局が電子証明書とＣＲＬ及びＡＲＬを発行する際に用いる署名用の鍵

ＣＲＬ：Certificate Revocation List
電子証明書の有効期間中に何らかの理由により失効された電子認証局以外の電子証明書を示す失効リスト

ＧＰＫＩ：Government Public Key Infrastructure
政府認証基盤

ＨＳＭ：Hardware Security Module
タンパフリーな秘密鍵管理装置で、ＣＡ秘密鍵を格納

ＩＣカード
タンパフリーな秘密鍵格納媒体で、加入者の秘密鍵と電子証明書を格納

ＰＩＮ情報：Personal Identification Number Information
本電子認証局では、数字からなる暗証情報

委託先要員
　　ＩＣカード発行局の要員、セキュリティセンタの要員及び保守員の総称

運用要員
　　HSM 鍵管理者、システム管理要員、発行審査担当者及び RA 登録操作員の総称

鍵ペア
　　秘密鍵と公開鍵の対

発行申請者
　　加入者証明書の発行申請をしようとする者

加入者
　　有効な税理士資格を有し、加入者証明書の発行を受けている税理士

加入者証明書
　　税理士に発行する電子証明書

自己署名証明書
　　ルートとなる電子認証局が用いる電子認証局自身の電子証明書

相互認証証明書
　　ＣＡ間で信頼を確立するために、相手のＣＡ公開鍵に対し発行する電子証明書

フィンガープリント
　　電子認証局の自己署名証明書の値を SHA１で変換した値

ブリッジ認証局
　　行政機関のＣＡ、民間のＣＡとの間に相互認証証明書を発行して、認証基盤の要としての役割を果たすＣＡ

本人限定受取郵便（基本型）
　　電子署名法第五条第一項第三号で定める「その取扱いにおいて名あて人本人若しくは差出人の指定した名あて人に代わって受け取ることができる者に限り交付する郵便」に相当する郵便事業株式会社が提供する「本人限定受取郵便」の基本型

元加入者
　　加入者証明書の発行を受けたが、現在有効な加入者証明書を持たない者

要員
　　運用要員及び委託先要員の総称

リポジトリ
　　電子証明書や失効リストやフィンガープリント等を保管し、これらの開示や配布のサービス

を提供するシステム

リンク証明書

新しい自己署名証明書(NewWithNew)と、古い自己署名証明書（OldWithOld）を紐付ける電子証明書（OldWithNew、NewWithOld）

旧電子証明書

有効期限が平成 20 年 9 月 30 日の加入者証明書

新電子証明書

有効期限が平成 25 年 3 月 31 日の加入者証明書

2　一般規定

2.1 義務

本サービスにおける電子認証局、発行局、登録局、ＩＣカード発行局及びリポジトリとしての義務ならびに加入者及び検証者の義務を定める。

2.1.1　電子認証局の義務

電子認証局は、加入者及び検証者に対して次の義務を負う。

(1) 本基準に基づき、電子認証局及び本サービスを適切に運営すること。
(2) ＣＡ秘密鍵が危殆化（盗難、漏洩等により他人に使用され得る状態になること）しないよう厳重に保護すること。
(3) 本基準を適切に維持管理するとともにリポジトリにおいて公開すること。
(4) 定期的（２４時間毎）にＣＲＬ及びＡＲＬを作成し、リポジトリに登録し、電子証明書の失効情報を公開すること。
(5) 本基準を含む電子認証局に関する情報、フィンガープリントをリポジトリにおいて公開すること。
(6) 電子認証局が実施するすべての認証業務について、定期的に監査人による監査を実施し、改善事項が指摘された場合には、速やかに改善措置を行うこと。
(7) ブリッジ認証局が相互認証を行うための技術要件に関し定めている相互運用性仕様書の規定に従ってＧＰＫＩとの相互運用性を維持すること。
(8) 加入者の秘密鍵の扱い（加入者の秘密鍵、ＩＣカードのＰＩＮ情報について、その生成から加入者への送付の扱い）をセキュアな環境で行うこと。
　・電子認証局は、本基準に基づき加入者の秘密鍵及び当該加入者の秘密鍵を格納するＩＣカードのＰＩＮ情報を適切に取り扱うこと。
　・電子認証局は、加入者の秘密鍵の生成から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加入者に加入者の秘密鍵を送付すること。
　・電子認証局は、ＩＣカードのＰＩＮ情報の生成から印刷までの作業を適切に行い、加入者の秘密鍵と共に安全かつ確実な方法で加入者にＩＣカードのＰＩＮ情報を送付すること。
　・電子認証局は、加入者の秘密鍵及びＩＣカードのＰＩＮ情報の保管を行わないこと。電子認証局の設備、あるいはシステム上に加入者の秘密鍵及びＩＣカードのＰＩＮ情報が一時的に保管される場合には、当該加入者の秘密鍵及びＩＣカードのＰＩＮ情報の管理を厳重に行い、ＩＣカード作成後直ちに当該加入者の秘密鍵及びＩＣカードのＰＩＮ情報を設備、あるいはシステム上より完全に消去すること。
(9) 本基準に基づいて、電子証明書の適切な発行及び失効を行うこと。
(10) 問合せの受付を行うこと。
(11) 開示申請への対応を行うこと。
(12) 発行申請者からの発行申請､加入者等からの失効請求及び開示申請に含まれる個人情報を始め、本基準 2.9.1(機密情報として取り扱う情報)に定める機密情報の取り扱いをセキュアな環境で管理すること。
(13) その他電子署名法の規定に基づく義務。

2.1.2　発行局の義務

発行局は、加入者及び検証者に対して次の義務を負う。

(1) 発行局を本基準に基づき適切に運営すること。
(2) 電子署名法の規定に従ってＣＡ秘密鍵を安全に生成し、維持管理すること。

(3) 登録局の加入者証明書発行指示に基づき加入者の秘密鍵及び公開鍵の対を安全に生成し、加入者証明書を発行すること。
(4) 登録局の加入者証明書失効指示に基づき、加入者証明書を失効させＣＲＬに記載すること。
(5) 定期的（２４時間毎）にＣＲＬ及びＡＲＬをリポジトリに登録すること。

2.1.3　登録局の義務

登録局は、発行申請者、加入者及び検証者に対して次の義務を負う。

(1) 登録局を本基準に基づき適切に運営すること。
(2) 登録局は、発行申請者からの加入者証明書発行申請を適正に審査し、発行申請者の本人性の確認と発行の意思確認を厳密に実施すること。
(3) 登録局は、失効請求者からの加入者証明書失効請求を適正に審査し、失効請求者の本人性の確認と失効の意思確認を厳密に実施すること。
(4) 登録局は、開示申請者からの開示申請を適正に審査し、加入者本人からの申請であることの確認を厳密に実施すること。

2.1.4　ＩＣカード発行局の義務

ＩＣカード発行局は、加入者及び検証者に対して次の義務を負う。

(1) ＩＣカード発行局を本基準に基づき適切に運営すること。
(2) 発行局が生成した加入者の秘密鍵と加入者証明書をＩＣカードに格納し、安全かつ確実な方法で該当する加入者に配布すること。

2.1.5　リポジトリの義務

電子認証局は、リポジトリにおいて常時（２４時間、３６５日）本基準 2.7.1（認証局情報の公開）に定める情報を公開すること。

ただし、リポジトリを含む認証局設備の一時的な停止または災害等による止むを得ない停止の場合を除くものとする。

2.1.6　加入を希望する者及び加入者の義務

加入を希望する者は、加入者証明書の発行を申請するに先立って重要事項説明書及び本基準を熟読し、本サービスの利用手続き、加入を希望する者及び加入者の義務を理解し、同意すること。電子認証局は、押印された電子証明書発行申請書兼利用同意書を受領確認することで、発行申請者が重要事項説明書及び本基準を理解し同意したものと見なす。なお、重要事項説明書は、電子証明書発行申請書兼利用同意書等とともに日税連から送付される。

次の事項は、重要事項説明書にも掲載される。

(1) 正確な申請

加入者証明書の発行を申請する場合、電子証明書発行申請書兼利用同意書に発行申請者の現状における真実を記入すること。

虚偽の発行申請を行って加入者についての不実の証明をさせた者は電子署名法第四十一条の規定により罰せられる。

(2) 記載事項の承諾

発行申請者は、電子証明書発行申請書兼利用同意書に記載した、税理士登録番号及び以下の発行申請者の氏名（ローマ字）が加入者証明書に記載されることを承諾すること。

- 発行申請者の住民票の写しに記載されている氏名
- 発行申請者が日本に居住する外国人の場合、住民票の写しに記載されている氏名又は通称

名

・　発行申請者が日税連に旧姓使用承認申請書を提出し、旧姓使用の承認を受けた場合、戸籍抄本又は個人事項証明書記載の氏名（旧姓）

(3) 加入者証明書の内容確認

加入者証明書の発行時において、加入者は、ＩＣカードを受領した後、加入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こと。相違があった場合は、直ちにその加入者証明書の失効を請求すること。

(4) 電子証明書受領書の提出

加入者証明書の発行時において、加入者は、ＩＣカード到着後、ＩＣカードが正常に稼動することを確認し、電子証明書受領書に電子証明書発行申請書兼利用同意書で使用した印鑑を押印し、速やかに電子認証局へ郵送または持参（封入・封緘したもの）により提出すること。

(5) 加入者証明書の利用制限

本基準に定められた目的（本基準 1.3.3（加入者証明書の用途）を参照）以外の用途で加入者証明書を使用しないこと。

(6) 秘密鍵の安全な管理

加入者が本人の所有する加入者秘密鍵によって作成する電子署名は、電子署名法の規定により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。従って、加入者は、自らの加入者秘密鍵について加入者本人以外による使用や複写、バックアップ等が行われないよう十分な注意を払い秘匿性を維持して管理すること。また、加入者の秘密鍵を活性化するためのＰＩＮ情報を加入者本人以外に知られることのないよう十分な注意を払い秘匿性を維持して管理すること。加入者の秘密鍵を活性化するためのＰＩＮ情報は、定期的に変更すること。

(7) 秘密鍵の危殆化の通知

本人の所有する加入者秘密鍵が危殆化した場合または危殆化した恐れがある場合は、直ちに電子認証局に危殆化の事実を通知し、速やかに加入者証明書の失効手続きを行うこと。

(8) 加入者証明書記載内容の変更に関する通知

加入者証明書の記載内容に変更が生じた場合、速やかに失効手続きを行うこと。

(9) 加入者証明書使用中止に関する通知

加入者証明書の使用を中止する場合、速やかに失効手続きを行うこと。

(10) 加入者証明書失効時のＩＣカードの廃棄

加入者は、加入者証明書の失効手続きが完了した場合、電子認証局の指示に従い、保有するＩＣカードを確実に廃棄すること。ＩＣカードを廃棄する際は、ＩＣカードのチップを切断するようにはさみを入れ、廃棄すること。ただし、ＩＣカードが盗難等により現存しない場合を除く。

(11) 加入者証明書更新時のＩＣカードの廃棄

加入者は、加入者証明書の更新手続きが完了した場合、保有するＩＣカードのチップを切断するようにはさみを入れ、廃棄すること。

(12) 電子認証局判断による加入者証明書の失効

電子認証局の判断（本基準 4.7.5（電子認証局の判断による加入者証明書の失効）を参照）により加入者証明書が失効されることがあることを承諾すること。

(13) 指定された電子署名アルゴリズムの使用

本サービスにより発行した加入者の秘密鍵を使用して電子署名を行う場合のアルゴリズムには、「sha1WithRSAEncryption」を用いること。

2.1.7　検証者の義務

検証者は、電子認証局が発行した加入者証明書を利用するにあたり次の義務を負う。

(1) 本基準及び検証者利用同意書への同意

検証者は、リポジトリにおいて公開される本基準及び検証者利用同意書を理解し、同意したうえで電子証明書を利用すること。また検証者は、電子証明書の利用目的、範囲及びその制限を確認し、信頼すべきか否かの判断を行うこと。

(2) 加入者証明書の有効性確認

検証者は、電子認証局が発行する自己署名証明書をリポジトリから入手し、利用対象の加入者証明書に施された電子署名がＣＡ秘密鍵で正しく行われていること、及び当該加入者証明書が改ざんされていないことを署名検証により確認すること。また、検証者は、電子認証局が発行する自己署名証明書のフィンガープリントをリポジトリから入手して、取得した自己署名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電子認証局のものであることを確認すること。さらに加入者証明書が、有効期間内であることを確認すること。また、検証者は、ＣＲＬ及びＡＲＬをリポジトリから取得し、検証対象の加入者証明書が失効されていないことを確認すること。

なお、加入者証明書に記載される氏名（ローマ字）は以下のいずれかである。

- 加入者の住民票の写しに記載されている氏名をローマ字表記で記載する。
- 加入者が日本に居住する外国人の場合、住民票の写しに記載されている氏名又は通称名をローマ字表記で記載する。
- 日税連に旧姓使用承認申請書を提出し、旧姓使用の承認を受けた加入者は、戸籍抄本又は個人事項証明書記載の氏名（旧姓）をローマ字表記で記載する。

(3) ＧＰＫＩ証明書検証パスの検証

検証者は、ＧＰＫＩを経由して電子証明書の検証を行う場合、電子証明書検証パスに存在する全ての電子証明書について、当該証明書が改ざんされていないこと、有効期間内であること及び失効していないことを確認すること。

(4) 電子認証局証明書の検証

検証者は、電子認証局の自己署名証明書を必要に応じて自身の利用するアプリケーションのTrusted Root 証明書として組み込むことができるが、組み込みを行う際には、組み込む自己署名証明書のフィンガープリントとリポジトリに公開されている自己署名証明書のフィンガープリントとを十分な注意を払い比較検証し、正しい自己署名証明書であることを確認した上で組み込むこと。

2.2 責任

2.2.1 電子認証局の責任

電子認証局は、電子署名法の規定及び本基準に則って認証局を運営するとともに本サービスを提供する。

2.2.2 発行局の責任

発行局は、電子署名法の規定及び本基準に則って電子証明書の発行を行うことにより電子証明書の信頼性を確保する。

2.2.3 登録局の責任

登録局は、電子署名法の規定及び本基準に則って電子証明書の発行申請及び失効請求を取り扱うことにより電子証明書の信頼性を確保する。また、発行申請者からの発行申請、加入者からの失効請求及び開示申請に含まれる個人情報を適切に保護する。

2.2.4 加入者の責任

加入者は、本基準及び重要事項説明書に従って本サービスを利用する。

2.2.5　検証者の責任

検証者は、本基準及び検証者利用同意書に従って加入者の電子署名及び加入者証明書を検証する。

2.3 財務上の責任

2.3.1　認証局の損害賠償責任

電子認証局が本基準 2.2.1（電子認証局の責任）に定める責任に違反したことにより、加入者あるいは検証者が損害を被った場合、加入者あるいは検証者は、電子認証局に対し当該損害の賠償を請求することができる。ただし、この場合の賠償額は５万円を上限とする。

2.3.2　加入者あるいは検証者の損害賠償責任

(1) 加入者が本基準 2.2.4（加入者の責任）に違反したことにより電子認証局が損害を被った場合、電子認証局は、加入者に対して当該損害の賠償を請求することができる。
(2) 加入者が本基準 1.3.3（加入者証明書の用途）に定める加入者証明書の利用制限範囲外の用途に加入者証明書を使用した結果として発生した障害については、加入者が一切の責任を負うものとし、当該障害によって電子認証局が損害を被った場合、電子認証局は、加入者に対して当該損害の賠償を請求することができる。
(3) 加入者が本基準 2.1.6（加入を希望する者及び加入者の義務）に記載する失効手続義務を怠ったことにより生じた第三者による成りすまし及び検証者による電子署名検証の誤判断等の障害については、加入者が一切の責任を負うものとする。当該障害によって電子認証局が損害を被った場合、電子認証局は当該加入者に対して当該損害の賠償を請求することができる。
(4) 検証者が本基準 2.2.5（検証者の責任）に違反したことにより電子認証局が損害を被った場合、電子認証局は、検証者に対して当該損害の賠償を請求することができる。
(5) 検証者が本基準 1.3.3（加入者証明書の用途）に定める加入者証明書の利用制限範囲外の用途に加入者証明書を利用したことにより発生した障害については、検証者が一切の責任を負うものとする。当該障害によって電子認証局が損害を被った場合、電子認証局は検証者に対して当該損害の賠償を請求することができる。

2.3.3　免責

(1) 電子認証局の責めに帰すことが出来ない事由により生じた加入者または検証者に対する損害及び逸失利益について、電子認証局は責任を負わないものとする。
(2) 電子認証局の予見の有無を問わず特別の事情から生じた加入者または検証者に対する損害及び逸失利益について、電子認証局は責任を負わないものとする。
(3) 検証者が厳密な有効性確認を行うことなく電子署名は有効であると認識して電子署名を信頼した結果として損害を被った場合について、電子認証局は責任を負わないものとする。
(4) 加入者の秘密鍵及び加入者証明書を加入者に配布する際の郵便事故または運送機関の事故に伴う損害について、電子認証局は責任を負わないものとする。
(5) 加入者または検証者が本基準 1.3.3（加入者証明書の用途）に定められた用途以外に加入者証明書を使用したことにより生じた損害について、電子認証局は責任を負わないものとする。
(6) 天災によるサービス停止や緊急にサービス停止をする必要があると判断した場合、これに伴う損害について、電子認証局は責任を負わないものとする。
(7) 加入者証明書を使用するにあたっての加入者及び検証者自身のシステムの障害について、電子認証局は責任を負わないものとする。
(8) 加入者自身の瑕疵による加入者秘密鍵の危殆化に伴う損害について、電子認証局は責任を負わないものとする。

(9) 火災、停電などの広域災害によるサービス停止について、電子認証局は責任を負わないものとする。
(10) 戦争、動乱、騒乱、暴動、労働争議などによるサービス停止について、電子認証局は責任を負わないものとする。
(11) 加入者が本基準及び重要事項説明書の規定遵守を怠った場合、あるいは検証者が本基準及び検証者利用同意書の規定遵守を怠った場合に伴う、加入者又は検証者が受ける損害について、電子認証局は責任を負わないものとする。
(12) 電子認証局が失効処理を規定の期日内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きメッセージが検証者に送付された結果、発生する損害について、電子認証局は責任を負わないものとする。

2.4 解釈及び執行

2.4.1 準拠法

本基準は日本国内法及び関連諸規則に基づき解釈されるものとする。また、認証事業者と関係者との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。

関係する法令、規則等には次のものがある。

- 電子署名法（施行令、施行規則を含む）
- 税理士法（施行令、施行規則を含む）
- 日本税理士会連合会会則・規則類

2.4.2 分離、存続、合併、通知

本サービスが細分化、他のサービスと統合、もしくは他のサービスに統合される場合、電子認証局は、実質的に本サービスを継続するように最善を尽くすものとする。これらに伴って本基準が変更される場合には、本基準 9（仕様管理）の規定に従って変更を管理するものとする。この場合においても本基準 2.9（機密情報の取り扱い）の効力は持続する。

2.4.3 紛争解決手続き

全ての当事者は、本基準または電子認証局が発行した加入者証明書に関して生じた紛争についての専属的合意管轄裁判所を東京地方裁判所とすることで合意するものとする。

本基準に定められていない事項やこれらの文書の解釈について疑義が生じた場合、各当事者はその課題を解決するために誠意をもって協議するものとする。

2.5 料金

本サービスの発行手数料及び支払方法は、別途、日税連の「電子証明書発行取扱規程」において定められている。

2.6 加入者証明書の有効期間

本サービスにおいて発行する加入者証明書の有効期間は、発行の可否判断をしてから５年未満とする。具体的には以下の通りである。

平成２０年３月３１日までの間に発行した加入者証明書の有効期間満了日は、全て平成２０年９月３０日とする。

平成２０年４月１日から平成２４年９月３０日までの間に発行する加入者証明書の有効期間満了日は、全て平成２５年３月３１日とする。

2.7 公開とリポジトリ

2.7.1　認証局情報の公開

電子認証局は、認証局の情報として次の内容をリポジトリに格納し、下記のＵＲＬで公開する。

(1) 日本税理士会連合会電子認証局税理士証明書発行サービス認証業務運用基準（ＣＰ／ＣＰＳ）
https://cainfo.nichizeiren.or.jp/ca/

(2) 重要事項説明書
https://cainfo.nichizeiren.or.jp/ca/

(3) 日本税理士会連合会電子認証局自己署名証明書及び自己署名証明書のフィンガープリント
https://cainfo.nichizeiren.or.jp/ca/

(4) 日本税理士会連合会電子認証局自己署名証明書
ldap://ldap.nichizeiren.or.jp/ou%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations%20CA,o%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations,c%3dJP?cACertificate

(5) ＡＲＬ
ldap://ldap.nichizeiren.or.jp/ou%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations%20CA,o%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations,c%3dJP?authorityRevocationList

(6) ＣＲＬ
ldap://ldap.nichizeiren.or.jp/ou%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations%20CA,o%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations,c%3dJP?certificateRevocationList

(7) 相互認証を行った認証局の名称及び相互認証を取り消した認証局の名称
https://cainfo.nichizeiren.or.jp/ca/

(8) ＧＰＫＩとの相互認証証明書ペア
ldap://ldap.nichizeiren.or.jp/ou%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations%20CA,o%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations,c%3dJP?crossCertificatePair

(9) リンク証明書
ldap://ldap.nichizeiren.or.jp/ou%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations%20CA,o%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations,c%3dJP?cACertificate

(10) 検証者利用同意書
https://cainfo.nichizeiren.or.jp/ca/

(11) 各種申請書類（電子証明書失効請求書、加入者情報開示申請書、電子証明書受領書）
https://cainfo.nichizeiren.or.jp/ca/

(12) 各種案内書類（失効請求に関するご案内、開示申請に関するご案内）
https://cainfo.nichizeiren.or.jp/ca/

2.7.2　公開の頻度

本基準の公開は、本基準 9（仕様管理）の規定に従って行われる。

ＣＲＬ及びＡＲＬは、２４時間毎に作成されリポジトリにおいて公開する。

その他の情報については、公開内容の変更がなされる度に更新し、リポジトリにおいて公開する。

2.7.3　アクセスコントロール

電子認証局がリポジトリにおいて公開する認証局の情報は、加入者、検証者を含む全ての関与者が入手可能である。ただし、入手した情報を改ざんしてはならない。

リポジトリへのアクセスは、読み出しのみのアクセスコントロールとする。

2.7.4　リポジトリ

リポジトリは、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、運用する。

ただし、設備あるいはシステム保守などの理由により、事前に通知した上でリポジトリを一時的に停止することがある。なお、緊急の場合は、事前の通知を行わずに一時的にリポジトリを停止することがある。

リポジトリでは、フィンガープリントの改ざん防止措置が講じられている。

2.8 準拠性監査

電子認証局は、本サービスを運用するにあたり、本基準を含む諸規定に準拠して認証業務を行っていることを検証するため、準拠性監査を定期的に実施する。

また、電子署名法の特定認証業務の要件に従って定期的に指定調査機関による調査を受け、認定の更新を受ける。

2.8.1　準拠性監査の頻度

準拠性監査は、監査基準を定め、それに従い定期的に年に1回以上実施することとし、概ね電子署名法の規定に基づく認定更新に先立って実施する。また、運営委員会委員長が必要と認めた場合には、随時準拠性監査を実施する。

なお、セキュリティに関する重要な更改を実施する場合は、当該更改が電子署名法に定める変更の認定を要するか、変更の認定を不要とするかを問わず更改の都度準拠性監査を実施する。

2.8.2　監査人の資格

日税連が選任した準拠性監査を行う監査人は、特定認証業務及び準拠性監査について十分なスキルと経験を有する者とする。

2.8.3　被監査部門と監査人の関係

監査人は、電子認証局における認証業務に携わる者以外から選任する。

2.8.4　監査テーマ

監査は、認証業務が本基準及び事務取扱要領等に準拠して実施されていること、並びに外部からの不正侵入及び内部の不正行為に対する措置が適切に講じられていることを中心に実施する。監査の対象としては、電子認証局が運営するすべての業務、システム及び設備とする。また、当該業務の一部を外部委託にする場合は、委託先の業務、システム及び設備についても監査対象に含まれる。

2.8.5　監査指摘事項に対する措置

電子認証局は、準拠性監査の結果、指摘事項が示された場合には、速やかに改善措置を講じるものとする。また、セキュリティ対策に関する最新技術動向を踏まえた、業務、システム、設備及び規程等の見直し、改善を速やかに行うものとする。業務、システム、設備及び規程等の見直し、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。なお、改善措置を講じる上で必要があれば、本基準の改訂を行う。

2.8.6　監査結果の公開

電子認証局は、準拠性監査の結果を外部に対しては公開しないものとする。ただし、次の場合には運営委員会の承認に基づき、必要な範囲で準拠性監査の結果を開示するものとする。

・ 電子署名法の規定に従って指定調査機関からの監査結果の開示要求があった場合
・ ＧＰＫＩとの接続のため、ブリッジ認証局に監査結果を報告する場合
・ ブリッジ認証局から開示要求があった場合
・ その他運営委員会が必要と認める場合
・ 公的機関等から法律に基づく強制力を伴う開示要求があった場合

2.9 機密情報の取り扱い

電子認証局は、認証業務の運用に関して機密情報として取り扱う情報を明示的に定め、これらの情報が外部に開示、漏洩しないよう運営する。また、電子認証局は、認証業務の運用に関して機密情報として取り扱う情報を本サービスの提供に必要な範囲を超えて使用しないよう運営する。

2.9.1　機密情報として取り扱う情報

次の情報は、機密情報として取り扱う。

(1) 加入者証明書の発行申請に関する記録（本基準 4.1.1（申請）に定める提出書類を含む）
(2) 加入者証明書発行内容の記録（電子証明書自体に記載される情報及びリポジトリに公開される情報を除く）
(3) 開示申請に関する記録（本基準 4.6.1（申請）に定める提出書類を含む）
(4) 加入者証明書の失効請求に関する記録（本基準 4.7.1（請求）に定める提出書類を含む）
(5) 加入者証明書の失効内容の記録（ＣＲＬに記載される情報及びリポジトリに公開される情報を除く）
(6) 電子認証局の運営及び本サービスの提供に関する監査証跡の記録
(7) 監査人が作成する準拠性監査報告書
(8) 電子認証局の設備仕様、システム仕様、ネットワーク仕様
(9) 電子認証局の詳細な業務手順

2.9.2　機密情報として取り扱わない情報

前項の規定に関わらず、次の情報は機密情報としては取り扱わない。

(1) 加入者証明書、ＣＲＬ及びＡＲＬに記載される情報
(2) リポジトリに公開される情報

2.9.3　捜査機関等の請求による機密情報の開示

電子認証局は、公の捜査機関、裁判所等、法律上の権限を有する者から強制力を伴わない任意の情報照会があった場合で、正当防衛、緊急避難等、相当の理由があると運営責任者が判断したときは、照会元に対して機密情報の開示を行うことができるものとする。

2.9.4　開示申請による機密情報の開示

電子認証局は、加入者、元加入者または代理人からの開示申請があった場合、認証局が保管している機密情報のうち当該加入者証明書に対応する次の情報を開示する。

・加入者の真偽を確認した資料
・加入者証明書記載データ
・加入者証明書の発行申請に関する記録

・加入者証明書の発行内容の記録
・加入者証明書の失効請求に関する記録
・加入者証明書の失効内容の記録

2.9.5　業務委託先企業の守秘義務

電子認証局は、認証業務の一部を外部に委託する場合、委託契約において機密情報の取り扱いに関する十分な守秘義務を負わせるものとする。また、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。機密情報の開示を実施する場合には、当該情報が本基準 2.9（機密情報の取り扱い）の規定に適合した取り扱いがなされるように外部委託先の管理を行う。

2.10 知的財産権

本サービスにおいて、日税連の作成物ならびに電子認証局が加入者に貸与するソフトウェア及びドキュメント等著作物の著作権は、日税連に帰属するものとする。

2.11 個人情報保護

電子認証局は、本サービスを提供するために入手する個人情報について、以下の通り取り扱うこととする。

(1) 個人情報の位置付け

電子認証局は、加入者証明書の発行申請、失効請求及び開示申請の手続きについて、発行申請者、加入者、元加入者または代理人から提供を受ける情報を個人情報として取り扱い、十分な注意を払って保護するものとする。

電子認証局は、発行申請者、加入者、元加入者または代理人から提出を受けた申請書類等の原本は、記載内容の不備等がある場合を除いて返却しないものとする。

電子認証局は、発行申請者、加入者、元加入者または代理人から提出される個人情報の取り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、本サービスにおける個人情報の適切な保護を行う。

(2) 使用目的

電子認証局は、個人情報を本サービス提供のためにのみ使用するものとする。

(3) 使用目的の制限

電子認証局は、前項の目的以外に個人情報を使用しない。

また、第三者から個人情報の目的外使用を求められた場合、法令に定めのある場合を除き一切これに応じない。

(4) 適正な取得

電子認証局は、偽りその他不正な手段により個人情報の取得を行わない。電子認証局は、本サービスに必要な範囲を越えて個人情報の収集を行わない。

(5) 取得に際しての使用目的の通知

電子認証局は、個人情報の使用目的を本基準に記載し、リポジトリにおいて公開する。

(6) 安全管理措置及び要員、委託先の監督

電子認証局は、発行申請者、加入者、元加入者または代理人から提出を受けた個人情報について、運用要員、委託先要員の監督を含め、その漏洩、滅失、毀損等の防止措置を講じる。電子認証局は、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及び搬送する場合は、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。電子認証局は、個人情報の取り扱い及び保護に関して、全ての要員を対象とした、役割に応じた教育及び訓練計画を策定し、同計画に沿って実施する。

(7) 保有個人情報に関する事項の開示

電子認証局は、個人情報の取り扱いについては、発行申請者、加入者、元加入者または代理人への個別の通知は行わない。

(8) 開示

電子認証局は、個人情報の開示にあたっては、加入者、元加入者または代理人からの文書による開示申請のみを受け付け、申請者に対して郵送により結果を通知する。

(9) 訂正、消去

発行申請者、加入者、元加入者または代理人から提供を受けた書類は、電子署名及び認証業務に関する法律及び同施行規則の定めにより、記録として一定期間保管を義務付けられるものであり、発行申請者、加入者、元加入者または代理人からの訂正もしくは消去の求めに応じることは出来ない。

電子認証局は、発行申請者、加入者、元加入者または代理人からの訂正もしくは消去の求めがあった場合には、応じることが出来ない旨を発行申請者、加入者、元加入者または代理人に通知する。

2.12 検証者からの問い合わせへの対応

電子認証局は、検証者からの問い合わせについて次の通り取扱う。

リポジトリへのアクセス障害については、直ちに動作確認を行い、必要であれば復旧処置を行う。

(1) 連絡先は、本基準 1.4（連絡先）の通りとする。

(2) 認証局の公開情報は、本基準 2.7.1（認証局情報の公開）に定めるＵＲＬにアクセスして入手する。

(3) 加入者の個人情報及び個別の申請手続に関する機密情報の問い合わせには回答しない。

(4) 個別の加入者証明書の交付依頼には応じない。

(5) 有効期間満了後の加入者証明書及び自己署名証明書に関する問い合せには応じない。

(6) 失効理由（リーズンコード）は、CRL により公開する。しかし、これに係る失効事由は、機密事項とし開示しない。

3　識別と認証

3.1 初期登録

3.1.1　名称のタイプ

本サービスで発行する加入者証明書に記載する名称は、ITU-T X.500 識別名（DN:Distinguished Name）の形式に従って設定する。

3.1.2　名称の意味に関する要件

以下に加入者証明書に記載する加入者情報(subject)の識別名の種類と本サービスにおける取り扱いについて記述する。

(1) 国名(countryName)

加入者が居住する国名である。

“JP”(日本国)で固定である。

(2) 組織名(organizationName)

日本税理士会連合会（” Japan Federation of Certified Public Tax Accountants' Associations”）で固定である。

なお、組織名は電子署名法の認定対象外である。

(3) 税理士登録番号(organizationalUnitName)

加入者に一意に割り当てられた税理士登録番号を記載する。

記載する形式は” Registration Number:xxxxxxx”（xxxxxxx は税理士登録番号）である。

なお、税理士登録番号は電子署名法の認定対象外である。

(4) 固有名称(commonName)

・加入者の住民票の写しに記載されている氏名をローマ字表記で記載する。

・加入者が日本に居住する外国人の場合、住民票の写しに記載されている氏名又は通称名をローマ字表記で記載する。

・日税連に旧姓使用承認申請書を提出し、旧姓使用の承認を受けた加入者は、戸籍抄本又は個人事項証明書記載の氏名（旧姓）をローマ字表記で記載する。

なお、固有名称は電子署名法の認定対象である。

3.1.3　名称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　名称の一意性

本サービスで発行する加入者証明書の記載は、一意になるように設定する。

3.1.5　名称に関する紛争解決

名称に関する紛争とは、本サービスで発行する加入者証明書に記載する加入者の識別名に係る何らかの紛争（不正発行、商標権侵害、不正競争、不明目的使用等）を意味する。

名称に関する紛争は、電子認証局と加入者との間で誠意を持って解決するものとする。

3.1.6　商標の認識、認証及び役割

本サービスで発行する加入者証明書に記載される加入者の識別名は、商標を含まない。

3.1.7　秘密鍵の所有を証明する方法

電子認証局は、発行局において加入者の公開鍵と秘密鍵及び秘密鍵を活性化するためのＰＩＮ情報を生成し、委託先企業においてこれを所定の形式でＩＣカードに格納する。

電子認証局は、加入者に対してＩＣカードとＰＩＮ情報を同一の封筒に梱包し郵送する。

ＩＣカードの受取確認は、加入者から提出される発行申請時に添付された印鑑登録証明書に係る印鑑が押印された電子証明書受領書の受領をもって行う。

「本人限定受取郵便（基本型）」で法令に基づく勤務地の加入者本人宛に配布し、加入者から電子証明書受領書を受け取ることによって、加入者の秘密鍵が本人に渡ったことを確認するものとする。

3.1.8　組織の同一性の確認

電子認証局は、ＧＰＫＩとの相互認証にあたって、ブリッジ認証局の定める手続きに基づき相互認証先となるブリッジ認証局の運営組織を確認する。

3.1.9　発行申請者の本人性の確認

電子認証局は、電子署名法の規定に従い、本基準 4.1.1（申請）に規定する書類の提出を受け、以下の事項に従い発行申請者について確認する。

(1) 本人の申請意思の確認

電子認証局は、電子証明書発行申請書兼利用同意書に発行申請者の押印（押印した印鑑に係る印鑑登録証明書が提出されている場合に限る）を確認することにより発行申請者本人の申請意思があるものと判定する。

(2) 発行申請者が本人であることの確認

電子認証局は、加入者証明書の発行申請者が本人であることの確認を行う。

- 印鑑登録証明書の記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
- 印鑑登録証明書の発行日が電子証明書発行申請書兼利用同意書に記載されている記入年月日より前後３ヶ月以内に発行されたものであることを確認する。
- 電子証明書発行申請書兼利用同意書の記載内容（氏名、生年月日、住所）が、電子証明書発行申請書兼利用同意書に押印した印鑑に係る印鑑登録証明書の記載内容（氏名、生年月日、住所）と同一であることを確認する。
- 電子証明書発行申請書兼利用同意書に押印された印影と印鑑登録証明書に記載されている印影が一致することを確認する。

(3) 発行申請者の実在性の確認

電子認証局は、発行申請者が実在することの確認を行う。

- 住民票の写しの記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
- 住民票の写しの発行日が、電子証明書発行申請書兼利用同意書に記載されている記入年月日より前後３ヶ月以内に発行されたものであることを確認する。
- 電子証明書発行申請書兼利用同意書の記載内容（氏名、生年月日、住所）が、住民票の写しの記載内容（氏名または通称名(日本に居住する外国人の場合)、生年月日、住所）と同一であることを確認する。

(4) 税理士資格の有効性確認

電子認証局は、発行申請者の税理士資格が有効であることの確認を行う。

- 電子証明書発行申請書兼利用同意書に記載された氏名及び住所が税理士名簿の登録内容と一致していることを確認する。
- 発行申請者が税理士法第二十六条第一項の規定により税理士登録が抹消されていないことを確認する。
- 発行申請者が税理士法第四十三条または第四十四条第二号の規定により税理士業務の停止期間中でないこと、もしくは第四十四条第三号の規定により税理士業務が禁止となっていないことを確認する。

(5) 旧姓使用の確認

電子認証局は、日税連から旧姓使用の承認を受けている（税理士名簿に旧姓で登録されている）発行申請者については、以下の確認を行う。

- 戸籍抄本または個人事項証明書の記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
- 戸籍抄本または個人事項証明書の発行日が電子証明書発行申請書兼利用同意書に記載されている記入年月日より前後３ヶ月以内に発行されたものであることを確認する。
- 電子証明書発行申請書兼利用同意書に記載された旧姓が、戸籍抄本または個人事項証明書の記載内容と同一であることを確認する。

3.2 加入者証明書の更新

加入者証明書の更新に関する手続きは、本基準 4.1（加入者証明書の発行申請）に同じである。

3.3 加入者証明書の再発行

加入者証明書の再発行は、行わない。

3.4 加入者情報の開示

電子認証局は、本基準に則って加入者情報の開示手続きを行う。

3.4.1 開示申請者の確認

電子認証局は、本基準 4.6.1（申請）に規定する書類の提出を受け、以下の事項に従い加入者情報開示申請書の申請者が本人または代理人であることを確認する。

(1) 開示申請者が本人の場合

電子認証局は、加入者情報の開示申請者が本人であることの確認を行う。

- 加入者情報開示申請書の記載内容（氏名、生年月日、住所、税理士登録番号）が、加入者証明書発行申請時の電子証明書発行申請書兼利用同意書に記載された内容（氏名、生年月日、住所、税理士登録番号）と同一であることを確認する。
- 加入者情報開示申請書に押印された印影と加入者証明書発行申請時の電子証明書発行申請書兼利用同意書に押印されている印影が一致することを確認する。

電子認証局は、加入者情報開示申請書の記載内容と加入者証明書発行申請時の電子証明書発行申請書兼利用同意書の記載内容に相違がある場合､以下の事項に従い開示申請者の確認を行う。

(a)開示申請者が本人であることの確認

電子認証局は、加入者情報の開示申請者が本人であることの確認を行う。

・印鑑登録証明書の記載内容及び形式が真正なものであり、公的機関から発行されたこと

を証明する印が押されていることを確認する。
・印鑑登録証明書の発行日が加入者情報開示申請書に記載されている記入年月日より前後３ヶ月以内に発行されたものであることを確認する。
・加入者情報開示申請書に押印された印影と印鑑登録証明書に記載されている印影が一致することを確認する。

(b)開示申請者の実在性の確認

電子認証局は、開示申請者が実在することの確認を行う。
・住民票の写しの記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・住民票の写しの発行日が、加入者情報開示申請書に記載されている記入年月日より前後３ヶ月以内に発行されたものであることを確認する。
・加入者情報開示申請書の記載内容（氏名、生年月日、住所）が、住民票の写しの記載内容（氏名または通称名(日本に居住する外国人の場合)、生年月日、住所）と同一であることを確認する。

(c)旧姓使用または氏名変更の確認

電子認証局は、日税連から旧姓使用の承認を受けている（税理士名簿に旧姓で登録されている）または現在の氏名を加入者情報の開示を求める氏名から変更している開示申請者については、以下の確認を行う。
・戸籍抄本または個人事項証明書の記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・戸籍抄本または個人事項証明書の発行日が加入者情報開示申請書に記載されている記入年月日より前後３ヶ月以内に発行されたものであることを確認する。
・加入者情報開示申請書に記載された旧姓が、戸籍抄本または個人事項証明書の記載内容と同一であることを確認する。（旧姓使用の場合）。
・加入者情報開示申請書に記載された開示を求める氏名が、戸籍抄本または個人事項証明書の記載内容と同一であることを確認する。（現在の氏名を加入者情報の開示を求める氏名から変更している場合）

(2) 開示申請者が加入者または元加入者の法定代理人の場合

電子認証局は、以下の事項に従い開示申請者、加入者または元加入者の確認を行う。

(a)加入者または元加入者の実在性の確認

電子認証局は、以下によって加入者または元加入者の実在性の確認を行う。
・加入者情報開示申請書の記載内容（加入者または元加入者の氏名、生年月日、住所、税理士登録番号）が、加入者証明書発行申請時の電子証明書発行申請書兼利用同意書に記載された内容（氏名、生年月日、住所、税理士登録番号）と同一であることを確認する。加入者情報開示申請書の記載内容（加入者の氏名、住所）と加入者証明書発行申請時の電子証明書発行申請書兼利用同意書の記載内容（氏名、住所）に相違がある場合は、以下の確認を行う。
・住民票の写しの記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・住民票の写しの発行日が、加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内に発行されたものであることを確認する。
・加入者情報開示申請書の記載内容（加入者の氏名、生年月日、住所）が、住民票の写しの

記載内容（氏名または通称名(日本に居住する外国人の場合)、生年月日、住所）と同一であることを確認する。
・戸籍抄本または個人事項証明書の記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・戸籍抄本または個人事項証明書の発行日が、加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内に発行されたものであることを確認する。
・加入者情報開示申請書に記載された旧姓が、戸籍抄本または個人事項証明書の記載内容と同一であることを確認する。（旧姓使用の場合）。
・加入者情報開示申請書に記載された開示を求める氏名が、戸籍抄本または個人事項証明書の記載内容と同一であることを確認する。（現在の氏名を加入者情報の開示を求める氏名から変更している場合）

(b)開示申請者が加入者または元加入者の代理人であることの確認

電子認証局は、以下によって開示申請者が加入者または元加入者の代理人であることを確認する。
・登記事項証明書の記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・登記事項証明書の発行日が、加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内に発行されたものであることを確認する。
・住民票の写しの記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・住民票の写しの発行日が、加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内に発行されたものであることを確認する。
・登記事項証明書に記載されている成年後見人、保佐人等の氏名及び住所が、加入者情報開示申請書に記載された代理人の氏名及び住所と同一であることを確認する。
・登記事項証明書に記載されている成年被後見人、被保佐人等の氏名及び住所が、加入者情報開示申請書に記載された加入者または元加入者の氏名及び住所と同一であることを確認する。
・代理人の住民票の写しに記載されている氏名、生年月日及び住所が、加入者情報開示申請書に記載された代理人の氏名、生年月日及び住所と同一であることを確認する。

(c)開示申請者が代理人本人であることの確認

電子認証局は、開示申請者が代理人本人であることの確認を行う。
・印鑑登録証明書の記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・印鑑登録証明書の発行日が、加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内に発行されたものであることを確認する。
・加入者情報開示申請書に記載された代理人の氏名、生年月日及び住所が、代理人から提出された印鑑登録証明書に記載されている氏名、生年月日及び住所と同一であることを確認する。
・加入者情報開示申請書に押印された代理人の印影と代理人から提出された印鑑登録証明書に記載されている印影が一致することを確認する。

(3) 開示申請者が開示申請を行うにつき加入者または元加入者が委任した代理人の場合

電子認証局は、以下の事項に従い開示申請者、加入者または元加入者の確認を行う。

(a)加入者または元加入者の実在性の確認

電子認証局は、以下によって加入者または元加入者の実在性の確認を行う。

・加入者情報開示申請書の記載内容（加入者または元加入者の氏名、生年月日、住所、税理士登録番号）が、加入者証明書発行申請時の電子証明書発行申請書兼利用同意書に記載された内容（氏名、生年月日、住所、税理士登録番号）と同一であることを確認する。加入者情報開示申請書の記載内容（加入者または元加入者の氏名、住所）と加入者証明書発行申請時の電子証明書発行申請書兼利用同意書の記載内容（氏名、住所）に相違がある場合は、以下の確認を行う。
・住民票の写しの記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・住民票の写しの発行日が、加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内に発行されたものであることを確認する。
・加入者情報開示申請書の記載内容（加入者または元加入者の氏名、生年月日、住所）が、住民票の写しの記載内容（氏名または通称名(日本に居住する外国人の場合)、生年月日、住所）と同一であることを確認する。
・戸籍抄本または個人事項証明書の記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・戸籍抄本または個人事項証明書の発行日が、加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内に発行されたものであることを確認する。
・加入者情報開示申請書に記載された旧姓が、戸籍抄本または個人事項証明書の記載内容と同一であることを確認する。(旧姓使用の場合)。
・加入者情報開示申請書に記載された開示を求める氏名が、戸籍抄本または個人事項証明書の記載内容と同一であることを確認する。(現在の氏名を加入者情報の開示を求める氏名から変更している場合)

(b)加入者または元加入者の本人性の確認

電子認証局は、以下によって加入者または元加入者の本人性の確認を行う。

・印鑑登録証明書の記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・印鑑登録証明書の発行日が、加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内に発行されたものであることを確認する。
・委任状に記載されている加入者または元加入者の氏名及び住所が、加入者または元加入者から提出された印鑑登録証明書に記載されている氏名及び住所と同一であることを確認する。
・委任状に押印されている加入者または元加入者の印影と加入者または元加入者から提出された印鑑登録証明書に記載されている印影が一致することを確認する。

(c)開示申請者が加入者または元加入者の代理人であることの確認

電子認証局は、開示申請者が加入者または元加入者の代理人であることを確認する。

・委任状の記載内容及び形式が真正なものであることを確認する。
・委任状の発行日が、加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内に発行されたものであることを確認する。
・委任状に記載されている代理人の氏名及び住所が、加入者情報開示申請書に記載された代理人の氏名及び住所と同一であることを確認する。
・委任状に記載されている加入者または元加入者の氏名及び住所が、加入者情報開示申請書

に記載された加入者または元加入者の氏名及び住所と同一であることを確認する。
・加入者情報開示申請書に記載された代理人の氏名、生年月日及び住所が、代理人の実在性を証明する書類（代理人の住民票の写しに記載されている氏名、生年月日及び住所と同一であることを確認する。

(d)開示申請者が代理人本人であることの確認
電子認証局は、開示申請者が代理人本人であることの確認を行う。
・印鑑登録証明書の記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・印鑑登録証明書の発行日が、加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内に発行されたものであることを確認する。
・加入者情報開示申請書に記載された代理人の氏名、生年月日及び住所が、代理人から提出された印鑑登録証明書に記載されている氏名、生年月日及び住所と同一であることを確認する。
・加入者情報開示申請書に押印された代理人の印影と代理人から提出された印鑑登録証明書に記載されている印影が一致することを確認する。

3.5 加入者証明書の失効
電子認証局は、失効請求者から電子証明書失効請求書を郵送または持参（失効請求書類一式を封入・封緘したもの）で受け付け、失効手続きを行う。
ただし、失効事由の重大性や緊急性に鑑みＦＡＸによる失効請求も受け付ける。この場合、電子証明書発行申請書兼利用同意書に記載されている電話番号に電話をして、本人性、失効の意思、失効の事由を確認する。また、失効請求者は、必ず事後に郵送により押印した電子証明書失効請求書を提出するものとする。
電子認証局の判断で加入者証明書の失効を行う場合は、電子証明書失効指示書により行う。

3.5.1 失効請求者の確認
電子認証局は、本基準 4.7.1（請求）に規定する書類の提出を受け、加入者証明書の失効請求者が正当な者であることを確認する。確認は、以下の事項に従う。

(1) 失効請求者が本人であることの確認
電子認証局は、加入者証明書の失効請求者が本人であることの確認を行う。
・ 電子証明書失効請求書の記載内容（氏名、生年月日、住所、税理士登録番号）が、加入者証明書発行申請時の電子証明書発行申請書兼利用同意書に記載された内容（氏名、生年月日、住所、税理士登録番号）と同一であることを確認する。
・ 電子証明書失効請求書に押印された印影と加入者証明書発行申請時の電子証明書発行申請書兼利用同意書に押印されている印影が一致することを確認する。

(2) 電子証明書失効請求書の記載内容と加入者証明書発行申請時の電子証明書発行申請書兼利用同意書の記載内容に相違がある場合
電子認証局は、以下の事項に従い失効請求者について確認する。
(a) 失効請求者が本人であることの確認
電子認証局は、加入者証明書の失効請求者が本人であることの確認を行う。
・ 印鑑登録証明書の記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。

・ 印鑑登録証明書の発行日が電子証明書失効請求書に記載されている記入年月日より前後３ヶ月以内に発行されたものであることを確認する。
・ 電子証明書失効請求書に押印された印影と印鑑登録証明書に記載されている印影が一致することを確認する。

(b)失効請求者の実在性の確認

電子認証局は、失効請求者が実在することの確認を行う。

・ 住民票の写しの記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・ 住民票の写しの発行日が、電子証明書失効請求書に記載されている記入年月日より前後３ヶ月以内に発行されたものであることを確認する。
・ 電子証明書失効請求書の記載内容（氏名、生年月日、住所）が、住民票の写しの記載内容（氏名または通称名(日本に居住する外国人の場合)、生年月日、住所）と同一であることを確認する。

(c)税理士資格の有効性確認

電子認証局は、失効請求者の税理士資格が有効であることの確認を行う。

・ 電子証明書失効請求書に記載された氏名及び住所が税理士名簿の登録内容と一致していることを確認する。
・ 失効請求者が税理士法第二十六条第一項の規定により税理士登録が抹消されていないことを確認する。
・ 失効請求者が税理士法第四十三条または第四十四条第二号の規定により税理士業務の停止期間中でないことを確認する。

なお、電子証明書失効請求書の失効事由が[税理士登録の抹消]または[税理士業務の停止・禁止]の場合は、税理士資格の有効性の確認を行わない。

(d)旧姓使用の確認

電子認証局は、日税連から旧姓使用の承認を受けている（税理士名簿に旧姓で登録されている）失効請求者または氏名が変更となった失効請求者については、以下の確認を行う。

・ 戸籍抄本または個人事項証明書の記載内容及び形式が真正なものであり、公的機関から発行されたことを証明する印が押されていることを確認する。
・ 戸籍抄本または個人事項証明書の発行日が電子証明書失効請求書に記載されている記入年月日より前後３ヶ月以内に発行されたものであることを確認する。
・ 電子証明書失効請求書に記載された旧姓が、戸籍抄本または個人事項証明書の記載内容と同一であることを確認する。

4　運用要件

4.1 加入者証明書の発行申請

日税連は、税理士名簿に登録されている税理士に対し、以下の書類を送付する。

・電子証明書発行申請書兼利用同意書（フリガナ、住所、生年月日、電話番号、氏名ローマ字、税理士登録番号、電子証明書用途については、印刷済み）
・重要事項説明書
・送付状
・返信用封筒
・送付内容一覧・お申込方法
・住所表記についての注意事項
・氏名ローマ字表記を変更される場合の注意事項

上記に加えて、振込が必要な税理士に対しては、

・電子証明書発行手数料のお支払いについて
・振込用紙

を送付する。

発行申請者は、本基準及び重要事項説明書に同意のうえ、電子証明書発行申請書兼利用同意書と必要な書類（以下「発行申請書類一式」という。）を日税連に提出し発行申請を行う。発行申請書類一式については、本基準 4.1.1（申請）を参照のこと。

なお、加入者証明書の発行申請は、発行申請者本人による申請のみとする。

4.1.1　申請

(1) 提出

発行申請者は、日税連から送付された電子証明書発行申請書兼利用同意書にて申請を行う。なお、提出する書類は、以下のとおり。

・ 電子証明書発行申請書兼利用同意書
　必要事項（記入年月日、氏名、フリガナ、住所、生年月日、電話番号、氏名ローマ字、税理士登録番号、電子証明書用途、旧姓または通称名の使用有無、現姓（旧姓を使用している場合））が全て記入され、かつ発行申請者本人の印鑑登録証明書にて照合可能な印鑑での押印がなされたもの。
　なお、内容に訂正が必要な場合は、発行申請者本人の印鑑登録証明書にて照合可能な印鑑にて訂正印を押印すること。
・ 印鑑登録証明書
　電子証明書発行申請書兼利用同意書に押印された発行申請者の印鑑に係る印鑑登録証明書
・ 住民票の写し
・ 戸籍抄本または個人事項証明書（旧姓を使用している場合）

発行申請書類の提出は、電子認証局への郵送または持参（発行申請書類一式を封入・封緘したもの）とする。郵送または持参以外の方式により提出された場合は、受け付けない。（郵送または持参以外の方式により提出された場合は、書類一式を郵送で返却する。）

(2) 受付

電子認証局へ渡った発行申請書類一式は、アーカイブ室において開封され、この開封によって

受付がなされたものとする。

4.1.2　発行申請の審査

電子認証局は、発行申請書類一式について、本基準 3.1.9（発行申請者の本人性の確認）に従った審査を行う。審査作業は、アーカイブ室において、２名の発行審査担当者により二重の審査を行う。審査で問題のないことを確認後、電子認証局は、電子証明書記載事項の登録作業へ移行する。

審査において書類不備及び記載事項不備が認められた場合には、発行申請書類一式を不備内容が記入された申請書類再提出のお願いと合わせて、発行申請者に返送する。「利用の申込みに対する諾否」で「諾否」の判断がされた以降、発行申請書類一式は発行申請者に返却しない。「利用の申込みに対する諾否」で「否」の判断がされた場合は、審査結果が記入された発行審査結果通知書を発行申請者に送付する。

4.1.3　電子証明書記載内容の登録

電子認証局は、審査結果に基づき、電子証明書記載内容を登録し、加入者証明書の発行要求を行う。

登録作業は、アーカイブ室において、RA 登録操作員２名による相互牽制下で作業を行う。

4.2 加入者証明書の発行

(1) ＩＣカード発行情報の支給

電子認証局は、加入者証明書発行申請を受けて加入者ごとの鍵ペアの生成を行う。鍵ペアは発行局システム内で行われる擬似乱数処理によって生成し、加入者証明書には生成された公開鍵が使用される。

加入者の電子証明書、秘密鍵及び秘密鍵を活性化させるＰＩＮ情報を委託先のＩＣカード発行局へ搬送する。

(2) ＩＣカード発行

委託先であるＩＣカード発行局では、加入者の電子証明書及び秘密鍵をＩＣカードへ登録し、加入者の秘密鍵を活性化させるＰＩＮ情報と共に、加入者に本人限定受取郵便（基本型）にて、法令に基づく勤務地の加入者本人宛に郵送する。

4.3 加入者証明書及び秘密鍵の受領

(1) 加入者証明書に問題がない場合

加入者は、受け取った加入者証明書に問題がないことを確認した後、同封されている電子証明書受領書への受領日及び税理士登録番号の記入と自筆署名及び電子証明書発行申請書兼利用同意書に使用した印鑑にて押印し、速やかに電子認証局へ郵送または持参（封入・封緘したもの）しなければならない。郵送または持参以外の方式により提出された場合は、受け付けない。（郵送または持参以外の方式により提出された場合は、書類一式を郵送で返却する。）このとき使用した印鑑が、電子証明書発行申請書兼利用同意書に使用した印鑑と異なる場合には、電子証明書受領書に押印した印鑑に係る印鑑登録証明書（電子証明書受領書の記入年月日より前後３ヶ月以内に発行されたもの）を添付し郵送または持参（封入・封緘したもの）しなければならない。

なお、電子証明書受領書へ記載した事項に訂正が必要な場合は、加入者本人の印鑑登録証明書にて照合可能な印鑑にて訂正印を押印すること。

電子認証局は、電子証明書受領書を受け取った場合、受領書に押印された印影と電子証明書発行申請書兼利用同意書に押印された印影が一致することを確認する。

電子認証局は、ＩＣカードを郵送してから３０日の期間を経過しても加入者から電子証明書受領書が返送または持参されず、受取の確認ができない場合は、当該加入者に関する加入者証明書を失効させる。

なお、電子署名法に定める「利用者による鍵の確実な受領」の要件は、電子認証局が加入者から郵送または持参される電子証明書受領書の受領をもって満たしたものとする。

(2) 加入者証明書に問題がある場合

加入者は、受け取ったＩＣカードあるいは加入者証明書に問題を見つけた場合、電子証明書受領書にその内容を記入し電子認証局に返送するとともに、電子認証局に対して直ちにその加入者証明書の失効を請求しなければならない。

4.4 加入者証明書の更新申請

加入者証明書の更新申請は、本基準 4.1.1（申請）と同じである。

4.5 加入者証明書の再発行申請

加入者証明書の再発行は、行わない。

4.6 加入者情報の開示

加入者または元加入者は、自身の権利や利益を侵害されているまたはその恐れがある場合、電子認証局に対し加入者情報の開示を申請することができる。なお、加入者情報の開示にあたっては、本人または代理人による申請のみとする。

開示申請者が開示を求めることができる情報は、本基準 2.9.4（開示申請による機密情報の開示）にて規定するもののみである。

加入者または元加入者は、手続きに要する加入者情報開示申請書をリポジトリ（本基準 2.7.1（認証局情報の公開）を参照）からダウンロードすることができる。または、本基準 1.4（連絡先）に示す方法で電子認証局へ依頼することができ、この依頼を受けた電子認証局は、加入者または元加入者に加入者情報開示申請書を送付する。

4.6.1 申請

開示申請者は、加入者情報開示申請書の書類に必要事項を記入し、電子認証局に郵送または持参（開示申請書類一式を封入・封緘したもの）することにより申請を行う。郵送または持参以外の方式により提出された場合は、受け付けない。（郵送または持参以外の方式により提出された場合は、書類一式を郵送で返却する。）

開示を申請できる代理人は、以下である。

・ 加入者または元加入者の法定代理人
・ 加入者情報の開示申請を行うにつき加入者または元加入者が委任した代理人

開示申請に提出を要する書類は、以下の通り。

(1) 加入者または元加入者本人が申請する場合

・ 加入者情報開示申請書

必要事項（記入年月日、氏名、フリガナ、住所、生年月日、税理士登録番号、旧姓・通称名・氏名変更の有無、現姓（旧姓を使用している場合は現姓、氏名を変更している場合は変更後の氏名を記入））、開示対象の電子証明書及び開示事項（開示情報、必要理由）が全て記入されていて、かつ本人の印鑑登録証明書にて照合可能な印鑑にて押印がなされたもの。

なお、内容に訂正が必要な場合は、本人の印鑑登録証明書にて照合可能な印鑑にて訂正印を押印すること。

上記に加えて、加入者情報開示申請書に記入する氏名、住所及び印影のいずれかが、電子証明書発行申請書兼利用同意書と異なる場合は、以下の書類も提出すること。（いずれも加入者情報開示申請書に記載されている記入年月日より前後３ヶ月以内に発行されたもの）

- 印鑑登録証明書
  加入者情報開示申請書に押印された印鑑に係る印鑑登録証明書
- 住民票の写し
- 戸籍抄本または個人事項証明書（旧姓を使用している場合、または現在の氏名を加入者情報の開示を求める氏名から変更している場合）

(2) 加入者または元加入者の法定代理人が申請する場合

以下に掲げる書類で加入者情報開示申請書以外については、発行日が加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内のものとする。

- 加入者情報開示申請書

加入者または元加入者の必要事項（記入年月日、氏名、フリガナ、住所、生年月日、税理士登録番号、旧姓・通称名・氏名変更の有無、現姓（旧姓を使用している場合は現姓、氏名を変更している場合は変更後の氏名を記入））、代理人の必要事項（氏名、フリガナ、住所、生年月日）、開示対象の電子証明書及び開示事項（開示情報、必要理由）が全て記入されていて、かつ代理人本人の印鑑登録証明書にて照合可能な印鑑にて押印がなされたもの。

内容に訂正が必要な場合は、代理人本人の印鑑登録証明書にて照合可能な印鑑にて訂正印を押印すること。

- 法定代理人であることを証明する書類

登記事項証明書

- 法定代理人の実在性を証明するための書類

法定代理人の実在性を証明するために以下の書類を提出すること。

表 4-1 法定代理人の実在性を証明するために必要な書類

		提出が必要な書類
選択	法定代理人が日本人の場合	住民票の写し
	法定代理人が日本に居住する外国人の場合	

- 法定代理人の本人性を証明するための書類

加入者情報開示申請書に押印された代理人の印鑑に係る印鑑登録証明書

- 加入者の実在性を証明するための書類

加入者情報開示申請書に記入する加入者または元加入者の氏名及び住所のいずれかが、電子証

明書発行申請書兼利用同意書と異なる場合は、以下の書類も提出すること。

表 4-2 加入者または元加入者の実在性を証明するために必要な書類

		提出が必要な書類
選択	日本人の場合 日本に居住する外国人の場合	・住民票の写し
	旧姓を使用している場合、または現在の氏名を加入者情報の開示を求める氏名から変更している場合	・戸籍抄本または個人事項証明書

(3) 開示申請を行うにつき加入者または元加入者が委任した代理人が申請する場合

以下に掲げる書類で加入者情報開示申請書以外については、発行日が加入者情報開示申請書に記載されている記入年月日より前後１ヶ月以内のものとする。

・ 加入者情報開示申請書

加入者または元加入者の必要事項（記入年月日、氏名、フリガナ、住所、生年月日、税理士登録番号、旧姓・通称名・氏名変更の有無、現姓（旧姓を使用している場合は現姓、氏名を変更している場合は変更後の氏名を記入））、代理人の必要事項（氏名、フリガナ、住所、生年月日）、開示対象の電子証明書及び開示事項（開示情報、必要理由）が全て記入されていて、かつ代理人本人の印鑑登録証明書にて照合可能な印鑑にて押印がなされたもの。なお、内容に訂正が必要な場合は、代理人本人の印鑑登録証明書にて照合可能な印鑑にて訂正印を押印すること。

・ 代理人であることを証明する書類

委任状

・ 代理人の実在性を証明するための書類

代理人の実在性を証明するために以下の書類を提出すること。

表 4-3 代理人の実在性を証明するために必要な書類

		提出が必要な書類
選択	代理人が日本人の場合 代理人が日本に居住する外国人の場合	住民票の写し

・ 代理人の本人性を証明するための書類

加入者情報開示申請書に押印された代理人の印鑑に係る印鑑登録証明書

・ 加入者の本人性を証明するための書類
委任状に押印された加入者の印鑑に係る印鑑登録証明書

・ 加入者の実在性を証明するための書類
加入者情報開示申請書に記入する加入者または元加入者の氏名及び住所のいずれかが、電子証明書発行申請書兼利用同意書と異なる場合は、本基準 4.6.1（申請 (2)加入者または元加入者の法定代理人が申請する場合 表 4-2）に示す書類も提出すること。

4.6.2 審査

電子認証局は、加入者情報開示申請書について、本基準 3.4.1（開示申請者の確認）に従って審査を行う。審査作業は、２名の発行審査担当者により二重の審査を行う。審査の結果、加入者情報の開示が適当でないと判断した場合には、開示申請者に対して開示審査結果通知書をもって郵送にて通知する。

なお、以下の場合は開示が適当でないと判断する。

・ 開示することにより、本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
・ 開示することにより、電子認証局の業務の適正な実施に著しい支障を及ぼすおそれがある場合
・ 開示することにより、法令に違反することとなる場合

4.6.3 加入者情報の送付

電子認証局は、開示申請者の審査が問題なく済み次第、速やかに開示情報を加入者情報開示通知書と共に開示申請者に送付する。

4.7 加入者証明書の失効請求

加入者は、以下の電子証明書の失効事由が発生した場合、電子認証局に対し加入者証明書の失効を請求しなければならない。なお、加入者証明書の失効請求は、加入者本人による請求のみとする。

・ 加入者証明書の記載内容に変更が発生した場合
・ 加入者証明書の使用を中止する場合
・ ＩＣカードが破損等により使用できない場合
・ 加入者の所有する加入者秘密鍵が危殆化（盗難、漏洩等によりその機密性を失うこと）した場合、または危殆化した恐れがある場合（IC カードの紛失、盗難等）
・ 税理士法第二十六条第一項の規定により税理士登録が抹消された場合
・ 税理士法第四十三条または第四十四条第二号の規定により税理士業務が停止もしくは第四十四条第三号の規定により税理士業務が禁止となった場合
・ その他、何らかの事由により加入者証明書を失効する必要があると判断した場合

加入者は、手続きに要する電子証明書失効請求書をリポジトリ（本基準 2.7.1（認証局情報の公開）を参照）からダウンロードすることができる。または、本基準 1.4（連絡先）に示す方法で電子認証局へ依頼することができ、この依頼を受けた電子認証局は、加入者に電子証明書失効請求書を送付する。

4.7.1 請求

通常の失効請求の手続きは、失効請求者が電子証明書失効請求書に必要事項を記入し、電子認証

局に郵送または持参（失効請求書類一式を封入・封緘したもの）することにより行う。郵送または持参以外の方式により提出された場合は、受け付けない。（郵送または持参以外の方式により提出された場合は、書類一式を郵送で返却する。）

緊急を要する失効請求の場合、加入者本人が電子証明書失効請求書に必要事項を記入し、ＦＡＸにて電子認証局に申し込むことができる。この場合、電子認証局の指示に従い、後日、速やかに電子証明書失効請求書を郵送しなければならない。

提出する書類は以下のとおり。

・ 電子証明書失効請求書

必要事項（記入年月日、氏名、フリガナ、住所、生年月日、電話番号、税理士登録番号、失効対象の電子証明書、失効事由、緊急失効請求日（緊急失効を申請していた場合）、旧姓または通称名または氏名変更の有無、現姓（旧姓を使用している場合は現姓、氏名を変更している場合は変更後の氏名を記入））が全て記入されていて、かつ加入者本人の印鑑登録証明書にて照合可能な印鑑にて押印がなされたもの。

なお、内容に訂正が必要な場合は、加入者本人の印鑑登録証明書にて照合可能な印鑑にて訂正印を押印すること。

上記に加えて、電子証明書失効請求書に記入する氏名、住所及び印影のいずれかが、電子証明書発行申請書兼利用同意書と異なる場合は、以下の書類も提出すること。（いずれも電子証明書失効請求書に記載されている記入年月日より前後３ヶ月以内に発行されたもの）

・ 印鑑登録証明書
　　電子証明書失効請求書に押印された加入者の印鑑に係る印鑑登録証明書
・ 住民票の写し
・ 戸籍抄本または個人事項証明書（旧姓を使用している場合、または氏名が変更となる場合）

4.7.2　審査

電子認証局は、電子証明書失効請求書について、本基準 3.5.1（失効請求者の確認）に従って審査を行う。審査作業は、２名の発行審査担当者により二重の審査を行う。

電子認証局は、失効請求内容に不備があった場合、失効請求者に対して失効請求を拒否することを失効審査結果通知書にて通知し再提出を求めるものとする。

なお、電子証明書失効請求書に記載された内容と電子証明書発行申請書兼利用同意書の記載内容が一致しない場合の加入者証明書失効の可否は、失効事由の重大性や緊急性に鑑み運営責任者が判断し、失効する場合もある。

4.7.3　加入者証明書の失効

電子認証局は、失効請求者の審査が済み次第、速やかに失効登録を行う。

電子認証局は、ＣＲＬを定期的に更新し、加入者証明書に記載されたＵＲＬに公開する。

ＣＲＬの更新は原則として２４時間毎（ＣＲＬの次回更新予定日時は４８時間後に設定）とする。

なお、ＣＲＬに記載する失効情報は、当該電子証明書の有効期限までの掲載とし、有効期限を越えた電子証明書については、検証者からの照会には応じない。

4.7.4　加入者証明書の失効通知

電子認証局は、加入者証明書を失効させた場合、加入者に対して電子証明書失効通知書の郵送により、遅滞なく電子証明書失効の通知を行う。

4.7.5　電子認証局の判断による加入者証明書の失効

電子認証局は、次の失効事由が発生したことを認めた場合、電子認証局自身の判断で加入者証明書を失効することができる。電子認証局は、加入者証明書を失効させた場合、該当する加入者に対して電子証明書失効通知書の郵送により電子証明書失効の通知を行う。

・税理士法第二十六条第一項の規定により税理士登録が抹消された場合
・税理士法第四十三条または第四十四条第二号の規定により税理士業務が停止もしくは第四十四条第三号の規定により税理士業務が禁止となった場合
・電子証明書の記載内容が事実と異なることが発覚した場合
・電子証明書の記載事項に変更が生じた場合
・ＩＣカードの不良により加入者が正しく受領できなかった場合
・加入者にＩＣカードを送付した後、配達不能で差し戻された場合
・加入者にＩＣカードを送付した後、３０日を経過しても加入者からの電子証明書受領書が返送または持参されず受領の確認が行われない場合
・加入者の所有する加入者秘密鍵が危殆化した場合、または危殆化の恐れがある場合
・ＣＡ秘密鍵が危殆化もしくは危殆化の恐れがある場合
・本サービスを廃止する場合
・その他、何らかの事由により電子証明書を失効する必要があると判断した場合

4.8 記録の保管

本サービスでは、以下の書類、電子データ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。

保管にあたり電子認証局は、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、間仕切りまた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直射日光が当たらないように保管・管理される。

保管庫の出し入れに関しては、帳簿記録により管理する。

電子認証局は、保存期間の過ぎた書類及び電子データを確実な方法により廃棄または消去する。

書類に関しては細かく裁断するなどの措置をとり、電子データは、媒体の破壊もしくは無効情報の上書きにより情報を消去するなどの措置をとる。

電子認証局は、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、アーカイブに使用でき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再記録する等の措置を行う。ただし、その際、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。

電子認証局は、データの重要度に応じて、電子認証局が許可するもの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。

(1) 業務の実施に係る記録（当該記録に係る電子証明書（相互認証証明書、加入者証明書）の有効期間の満了日から１０年間保存）
・電子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、加入者証明書）及びその発行に関する記録のうち紙で管理されるものの原本
・システムに記録された申請書記載事項に該当する情報
・発行申請者からの加入者証明書の発行の申請、加入者からの失効の請求及び開示の申請（元加入者、代理人からの申請を含む）に提出される申請書等の原本

・加入者証明書の発行、失効及び開示の認証業務の記録（帳票等で運用されるものの原本及び電子データで運用されるもの）
・ＣＡ秘密鍵管理（鍵生成、鍵の活性化／非活性化、バックアップ／復元、破棄）の記録（帳票等で運用されるものの原本及び電子データで運用されるもの）
・加入者から提出される電子証明書受領書等の書類の原本
・発行された加入者証明書、ＣＲＬ及びＡＲＬ
・加入者秘密鍵の生成、管理及び廃棄に関し帳票等で運用されるものの原本

(2) 電子認証局の運営に係る記録（当該記録に係る電子証明書（相互認証証明書、加入者証明書）の有効期間の満了日から１０年間保存）
・認証業務の一部を他に委託する場合の業務委託契約書及び関係する書類の原本
・認証業務に関する管理（要員、組織、体制、指揮命令系統など）情報、履歴など紙で運用されるものの原本
・監査記録及び監査報告書の原本
・ブリッジ認証局との相互認証に関する記録（紙で管理されるものの原本及び電子データで管理されるもの）
・本基準とその変更に関する記録（紙で管理されるものの原本及び電子データで管理されるもの）
・電子認証局の運営に係る管理書類の原本とその変更に関する記録
・その他、電子認証局の運営に係る記録（紙で管理されるものの原本及び電子データで管理されるもの）

(3) 設備及び安全対策措置に係る記録（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保存）
・室への入退室及び室の安全対策措置に関する記録（紙で管理されるものの原本及び電子データで管理されるもの）
・設備の保守及び設備の変更に関する記録（紙で管理されるものの原本）
・障害及び復旧に関する記録（紙で管理されるものの原本）
・システムの動作に関する記録（紙で管理されるものの原本及び電子データで管理されるもの）
・その他、設備及び安全対策措置に係る記録（紙で管理されるものの原本及び電子データで管理されるもの）

4.9 鍵の更新

自己署名証明書の有効期間は、有効とする日から起算して 10 年とする。電子認証局は、自己署名証明書の有効期限前に鍵の更新を行う。鍵更新時には、古い鍵と新しい鍵の認証パスを構築するリンク証明書を発行する。電子認証局は、新しい自己署名証明書及びリンク証明書を遅滞なくリポジトリに公開する。

4.10危殆化と災害からの回復

電子認証局の運営中に発生し得る CA 秘密鍵の危殆化、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または生じる恐れのある時には、以下の手順に則り速やかな回復を実現する。

(1) 電子認証局は、ＣＡ秘密鍵の危殆化、もしくは危殆化した恐れがある場合、その鍵で署名した全ての有効な加入者証明書を失効させるものとする。この場合、危殆化したＣＡ秘密鍵でＣＲＬを署名、公開し、加入者証明書を失効した全ての加入者に対して電子証明書失効通知書を郵送する。

また、CA 秘密鍵が危殆化した旨をブリッジ認証局及び主務大臣に対して直ちに通知し、速やかに相互認証証明書の失効手続きを行う。CA 秘密鍵及びそのバックアップ媒体を完全な初期化又は物理的に破壊し使用を中止するが、その CA 秘密鍵に対応する自己署名証明書は失効しない。電子認証局は、本サービスを継続するために再度、主務大臣の認定を受け、加入者が新たな加入者証明書の発行申請を行えるようにする。電子認証局は、本サービスが継続可能となった時点で改めてブリッジ認証局に対して相互認証の申込みを行う。また、原因及び被害の追求と原因別対応策を実施する。

(2) 電子認証局は、災害等により、施設、設備に被害を受けた場合、もしくはその施設、設備に対する物理的または論理的攻撃を受け、認証業務の運用が続けられなくなった場合、新たな施設、設備などを準備し、バックアップデータに基づいて認証業務を再開する。また、バックアップデータから公表及び保管を義務付けられている情報を復元し、さらに保護すべき情報を漏洩させないように努める。なお、電子認証局は、認証業務の運用が続けられなくなった時点で速やかにブリッジ認証局に通知し、相互認証証明書の失効手続きを行う。電子認証局は、認証業務の再開後、改めてブリッジ認証局に対して相互認証の申込を行う。また、原因及び被害の追求と原因別対応策を実施する。

(3) 電子認証局は、ＣＡ秘密鍵の危殆化もしくは被災の事実が生じた場合、電子認証局のホームページ（https://cainfo.nichizeiren.or.jp/ca/）及び日税連のホームページ（http://www.nichizeiren.or.jp/）にて加入者及び検証者に通知する。

(4) 電子認証局は、ＣＡ秘密鍵の危殆化または危殆化の恐れがある場合及び１日以上の停止を伴う重大障害や（被災を含む）、認証業務用設備の故障で検証者への失効情報の提供が４８時間を超えて停止し、かつ検証者がその停止を知る方法がなかった場合、直ちに、電子署名法の定める主務大臣に危殆化の発生または発生しそうな事実、障害の内容、発生日時、被害状況、措置状況等確認されている事実の報告を行う。また、原因及び被害の追求と原因別対応策を実施する。

(5) 電子認証局は、ＣＡ秘密鍵の危殆化もしくは被災の際の復旧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。

4.11 本サービスの廃止

電子認証局は、本基準の改廃及び電子認証局の事業方針の変更や災害等により、止むを得ず本サービスを廃止する場合がある。

本サービスの廃止は、遅くても廃止予定日の６０日前から日税連及び電子認証局のホームページで通知し、廃止後は６ヶ月間にわたり日税連のホームページにて通知する。また、廃止予定日以降に有効な加入者証明書がある場合、その加入者に対して６０日前までに本サービスの廃止を郵送で通知する。

本サービスを廃止する際には、ＣＡ秘密鍵及びそのバックアップ媒体を完全な初期化または物理的に破壊し使用を中止するが、そのＣＡ秘密鍵に対応する自己署名証明書は失効しない。

電子認証局は、本サービスの廃止の際に、新たな加入者証明書の発行を中止し、廃止日までにその時点で有効な全ての加入者証明書を失効し、ＣＲＬを６ヶ月間公開する。ただし、発行した全ての加入者証明書の期限が満了している場合はＣＲＬの公開は行わない。

なお、本サービスを廃止する場合においても、電子認証局は電子署名法に定める帳票類保存期間にわたり、紙及び電子データを保存し続けるよう最善を尽くす。やむを得ず、電子認証局が他者に情報を引き継ぐ場合には、これらの情報の後継管理に係る規定を、本サービス廃止の公表とあわせ

て電子認証局及び日税連のホームページにて通知する。

電子認証局は、本サービスを廃止する場合、廃止予定日の６０日前までにブリッジ認証局及び主務大臣に対して本サービスの廃止を通知し、廃止予定日を待って相互認証証明書の失効手続きを行う。電子認証局は、相互認証証明書失効後、ＡＲＬを６ヶ月間公開する。ただし、発行した全ての加入者証明書の期限が満了している場合は、ＡＲＬの公開は一定期間に留めるものとする。

4.12 教育訓練の実施

電子認証局は、運用要員に対して必ず定められた教育訓練を受けさせなければならない。この場合、すべての運用要員の責任と権限に応じて、下記の項目について必要な教育訓練計画を定め、その計画に従って教育訓練を実施するものとする。

- 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、責任及び権限に関する教育訓練及びその変更に伴う教育訓練
- 認証業務手順及びその変更に伴う教育訓練
- 危機管理に関する教育訓練
- ＣＡ秘密鍵の危殆化または災害等発生に対する対応策や回復手順に関する、責任と権限に応じた教育訓練
- 個人情報の取扱い及び保護に関する教育訓練

運用要員への教育訓練は、運用要員の任命後、業務の開始前に必ず実施し、その都度教育訓練の実施を記録し、証跡資料を残すこととする。責任及び権限の変更が生じた場合も同様である。以降、その任にある間は、1年毎に定められた教育訓練を実施する。なお、認証業務の内容に変更があった場合は、変更業務の開始前に新しい業務内容にあわせた教育訓練を実施する。

運営責任者は、委託業務の開始前に委託先要員が十分な技能を有していることを履歴書にて確認する。従って、委託先要員である保守員に関しては、教育訓練を免除することができる。但し、ICカード発行局の要員については、委託先において、指揮命令系統、責任、権限及び災害などの際の措置について教育が行われることを確認する。

4.13 ブリッジ認証局との相互認証

4.13.1 相互認証証明書の発行及び受領

ブリッジ認証局に対する相互認証証明書の発行は、ブリッジ認証局の定める手続きにより、相互認証証明書発行要求（ＣＳＲ）を受領した後、運営責任者の指示により実施する。

相互認証証明書の受け渡し確認は、ブリッジ認証局の定める手続きにより相互認証証明書受領書を受け取ることにより完了するものとする。

ブリッジ認証局からの相互認証証明書の受領は、運営責任者の指示により開始し、ブリッジ認証局の定める手続きにより相互認証証明書発行要求（ＣＳＲ）を生成してブリッジ認証局に送付し、相互認証証明書を受領する。

相互認証証明書の受け渡し確認は、ブリッジ認証局の定める手続きにより相互認証証明書受領書を送付することにより完了するものとする。

4.13.2 相互認証証明書の失効

電子認証局は、自己またはブリッジ認証局において、次の相互認証証明書失効事由が発生した場合、相互認証証明書を失効させるものとする。

- CA 秘密鍵の危殆化
- 相互認証基準違反

・ 相互認証業務の終了
・ 相互認証の更新
・ ポリシの変更
・ 本サービスの廃止
・ その他ブリッジ認証局から要請があった場合

電子認証局からの失効請求は、運営責任者が実施する。

ブリッジ認証局からの失効請求を受領した場合は、本基準 3.1.8（組織の同一性の確認）を実施した上で受理し、運営責任者の指示により、相互認証証明書を失効させる。

電子認証局は、ＡＲＬを定期的に更新し、相互認証証明書に記載されたＵＲＬに公開する。

ＡＲＬの更新は､原則として２４時間毎（ＡＲＬの次回更新予定日時は４８時間後に設定）とする。

4.13.3 相互認証証明書の更新

相互認証証明書の更新は、ブリッジ認証局の定める手順に従い本基準 4.13.1（相互認証証明書の発行及び受領）に準じて実施する。

4.13.4 相互認証証明書の公開

電子認証局は、相互運用性仕様書に定める仕様に従って、相互認証証明書、自己署名証明書をリポジトリに公開する。

電子認証局は、ＧＰＫＩの統合リポジトリに対する参照情報をリポジトリに設定する。

4.14 有効性確認に関する要件

検証者は、加入者証明書の検証において、電子認証局がリポジトリにて公開するＣＲＬ及びＡＲＬを参照し､当該加入者証明書あるいは電子認証局の自己署名証明書が失効処理済みになっているか否かを調べ、有効性の確認をしなければならない。なお、有効期間を満了した加入者証明書についての検証者からの問い合わせには応じない。

5　物理的、手続き的、人的セキュリティ管理

5.1 物理的セキュリティ管理

電子認証局は、認証業務用設備をアーカイブ室、認証設備室及びＩＣカード発行設備室に設置する。認証設備室は、セキュリティセンタ内に設置される。

それぞれの物理的セキュリティについては、以下に定める。

5.1.1　アーカイブ室

アーカイブ室では、加入者証明書を作成するために必要な、加入者情報の生成及び登録を行う。

(1) 入退室管理

アーカイブ室は、間仕切り及び施錠可能な出入り口により、他の部屋と分離を行う。

アーカイブ室は、入室権限を有する２名以上での入退室とし、無人になる際には、必ず施錠する。

アーカイブ室では、必ず、入室権限を有する者が２名以上在室するものとし、入室権限者は、関係者以外の者が登録用端末設備に触れないよう注意を払う。

(2) 災害対策

火災対策として、自動火災報知器、消火器を備える。

5.1.2　認証設備室

認証設備室では、加入者証明書の発行、ＩＣカード発行用データの作成、リポジトリサーバの運用、ＣＲＬ及びＡＲＬの公開を行う。

(1)入退室管理

認証設備室は、最高セキュリティレベルをもつ区画に設置する。

認証設備室は、入室権限者による認証設備室入退室用ＩＣカード操作及び指紋認証を必須とし、識別、認証の後、電子錠付扉を開錠させるものとする。認証設備室への入室の許可については、セキュリティセンタの委託先要員として任命を受け、セキュリティセンタの入退室に関する管理者により登録された者を入室権限者とする。認証設備室は、入退室装置により有人時には必ず複数名の入室権限者が在室する。

入室権限を有しない者の入室は、セキュリティセンタ責任者が必要性の確認を行い、許可した場合のみ、入室権限を有する２名以上の者が同行することにより可能とする。入室権限を有しない者については、認証設備室入退室管理簿に入退室を記録する。

セキュリティセンタの入退室に関する管理者は、入退室装置のログ、認証設備室入退室管理簿及び認証設備室が設置されているセキュリティセンタの入退室管理簿を確認することにより規定された入室方法、手続きで入室が行われているかについて日常チェックを行う。

監視情報または入退室記録は、監査証跡として監査の対象とする。異常記録は、準拠性監査及び電子署名法にもとづく認定更新までの間保管されるものとする。入退室記録については、正常な記録も含める。

(2) 災害対策

認証設備室においては、災害対策（水害、火災、防火、停電及び耐震）として以下を行うものとする。

- 水設備を設置せず、直上階からの漏水対策を行う。
- 自動火災報知器と消火設備を設置し、設備管理業者による定期点検を行う。
- 防火区画内に設置し、ダクト、ケーブル引き込み口には延焼対策を行う。

・ ＵＰＳ及び自家発電装置を備え、停電時の電源供給が可能とする。
・ 耐震構造をもつ建物に設置し、認証局設備を収納するラックは、ボルト止め等による移動、転倒防止措置を行う。

5.1.3 ＩＣカード発行設備室

ＩＣカード発行設備室では、ＩＣカードの発行及び封入封緘を行う。

(1)入退室管理

ＩＣカード発行設備室は、最高セキュリティレベルをもつ区画に設置する。

ＩＣカード発行設備室は、入室権限者による暗証番号入力操作及び指紋認証を必須とし、識別、認証の後、電子錠付扉を開錠させるものとする。ＩＣカード発行設備室への入室の許可については、ＩＣカード発行局の責任者により、任命を受け、登録された者を入室権限者とする。ＩＣカード発行設備室は、入退室装置により有人時には必ず複数名の入室権限者が在室する。

入室権限を有しない者の入室は、ＩＣカード発行局の責任者が必要性の確認を行い、許可した場合のみ入室権限を有する２名以上の者が同行することにより可能とする。入退室者は、ＩＣカード発行設備室入退室管理簿に入退室を記録する。

ＩＣカード発行局の責任者は、入退室装置のログとＩＣカード発行設備室入退室管理簿を確認することにより規定された入室方法、手続きで入室が行われているかについて日常チェックを行う。

監視情報または入退室記録は、監査証跡として監査の対象とする。異常記録は、準拠性監査及び電子署名法にもとづく認定更新までの間保管されるものとする。入退室記録については、正常な記録も含める。

(2) 災害対策

ＩＣカード発行設備室においては、災害対策（水害、火災、防火、停電及び耐震）として以下を行うものとする。

・ 水設備を設置せず、屋上からの漏水対策を行う。
・ 自動火災報知機、消火器を設置し、これらに関して必要に応じ所轄消防署に設置届出書を提出する。また、年１回の定期検査を実施する。
・ 防火区画内に設置し、ダクト、ケーブル引き込み口には延焼対策を行う。
・ 自家発電装置またはＵＰＳ等を備え、停電時の電源供給が可能とする。
・ 耐震構造をもつ建物に設置し、ＩＣカード発行設備は、耐震粘着ゴム等による移動、転倒防止措置を行う。

5.2 手続き的セキュリティ管理

電子認証局の要員は、権限に応じた入退室及び各業務実施時の手続きについて以下の要件に従って管理される。

(1) 運用要員の任命と権限割り当て

電子認証局の運営にかかわる運営責任者及び運用要員は運営委員会委員長が任命し、運用要員への権限割り当ては、運営委員会委員長の指揮及び監督を受ける運営責任者が行う。

(2) アクセスコントロール

運営責任者は、運用要員の業務及び権限をもとに入退室管理や、アカウント管理を実施する。業務委託先の入退室管理や、アカウント管理は業務委託先の責任者が実施する。

(3) 複数人による作業の実施

電子認証局が行う業務を正確に実施することを目的として、電子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。これにより、相互牽制を確立し、単

独で作業を行う者がシステムを悪用することを防止する。

(4) 作業指示と報告

電子認証局におけるすべての業務は、運営責任者の指示によって開始し、運営責任者への報告によって完了するものとする。この指示及び報告には、定められた書式を用いる。

5.3 人的セキュリティ管理

電子認証局の要員の管理は、以下の要件に適合するように実施する。

(1) 運用要員の教育

運営責任者は、運用要員に対し認証業務用設備の運用に必要な規定、手順などの教育訓練を実施する。

(2) システム管理要員の資格

システム管理要員は、業務に係わる技術に関して十分な知識及び経験を有する者とする。

(3) 運用要員の適性判断

運営委員会委員長は、運用要員の経験、知識、スキルをもとに適正を判断し任命する。運営責任者は任命された運用要員に権限を割り当てるとき、教育の必要性を検討し、必要と判断した場合は適切な教育を遅滞なく実行する。運営責任者は、運用要員として適性に問題があると判断した場合、運営委員会委員長へ運用要員の解任を要請する。

(4) 委託先要員の管理

運営委員会委員長は、業務委託先の責任者に対し、提示した経験、知識、スキルをもとにした委託先要員の割り当てを指示する。運営責任者は、業務委託先の責任者から受け取った委託先要員リストによってこれを確認する。

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

6.1.1　認証局の鍵生成

(1) 鍵ペアの生成

鍵ペアの生成は、認証設備室内において、1 名だけでは生成できない方法で行う。

(2) 自己署名証明書の生成

生成した公開鍵は、認証局システム内部で電子証明書の形式にする。

(3) 加入者に対する自己署名証明書の配布

電子認証局は、加入者証明書の格納されたＩＣカードとともに自己署名証明書を配布する。

また、加入者に自己署名証明書を配布する際に、自己署名証明書のフィンガープリントを一緒に配布する。

(4) 鍵のサイズ

ＲＳＡ公開鍵暗号方式による 2048 ビットの鍵を生成する。

(5) ハードウェア鍵の使用

鍵ペアの生成は、ＨＳＭで行う。

6.1.2　加入者の鍵生成

(1) 鍵ペアの生成

鍵ペアの生成は、加入者情報登録後、認証設備室の発行局システム内で疑似乱数処理を組み込んだソフトウェアにより自動生成される。なお、加入者情報の登録は、複数人のＲＡ登録操作員が相互牽制の下で行う。

(2) 加入者証明書の作成

生成した公開鍵は、認証局システム内部で加入者証明書の形式にする。

(3) 鍵のサイズ

ＲＳＡ公開鍵暗号方式による 1024 ビットの鍵を生成する。

(4) ハードウェア鍵の使用

ハードウェア鍵は使用しない。

(5) 加入者からの公開鍵の配送

電子認証局は、発行局システム内で加入者の鍵ペアを生成する。そのため加入者から、加入者の公開鍵が電子認証局に配送されることはない。

6.2 秘密鍵の保護

6.2.1　暗号モジュールに関する基準

HSM は、FIPS140-2 レベル３に基づいて設計された装置を使用する。

加入者の秘密鍵は、ＩＣカードに格納される。

加入者の秘密鍵を発行局システムから取り出す場合は、外部記録媒体の管理を厳密に行い、ＩＣカードに格納した後は速やかに外部記録媒体を破壊し、廃棄する。

6.2.2　秘密鍵の複数人制御

ＣＡ秘密鍵を使用する操作については、認証設備室内において、1 名だけでは操作できない方法で行う。

暗号化された加入者の秘密鍵及びＰＩＮ情報の管理と廃棄は、複数人のＩＣカード発行局の要員が相互牽制下において行う。

6.2.3　秘密鍵のエスクロウ

ＣＡ秘密鍵のエスクロウは、実施しない。

加入者秘密鍵のエスクロウは、実施しない。

6.2.4　秘密鍵のバックアップ

ＣＡ秘密鍵のバックアップ操作は、認証設備室内において、1名だけでは操作できない方法で行う。

ＨＳＭからバックアップしたＣＡ秘密鍵は、複数に分割される。

ＣＡ秘密鍵のバックアップ媒体は、権限を有する者以外が触れることのできない施錠等によるアクセス制御措置及び耐火等の防災措置のとられた保管場所へそれぞれ別に保管される。

加入者の秘密鍵のバックアップは行わない。

6.2.5　秘密鍵のアーカイブ

実施しない。

6.2.6　秘密鍵の取り出し及びＰＩＮ情報の生成

発行局サーバからの加入者の秘密鍵の取り出しは、複数人のセキュリティセンタシステム担当者が行う。作業は、認証設備室において相互牽制の下で行う。その際ＰＩＮ情報も生成し、加入者の秘密鍵と合わせて記録媒体に書き込みを行う。書き込み時に一時的に作成される作業用ファイルは、加入者の秘密鍵とＰＩＮ情報を格納したのち、速やかに完全削除される。

6.2.7　秘密鍵のリカバリ

ＣＡ秘密鍵のリカバリの操作は認証設備室内において、1名だけでは操作できない方法で行う。

6.2.8　秘密鍵の活性化方法

ＣＡ秘密鍵の活性化の操作は、認証設備室内において、1名だけでは操作できない方法で行う。

加入者の秘密鍵活性化の操作は、加入者がＩＣカードと同時に送付されるＰＩＮ情報を入力することによって行う。

6.2.9　秘密鍵の非活性化方法

ＣＡ秘密鍵の非活性化の操作は、認証設備室内において、1名だけでは操作できない方法で行う。

6.2.10　秘密鍵の破棄方法

ＨＳＭ内のＣＡ秘密鍵は、複数人でＨＳＭを完全に初期化する。なお、初期化不能かつＨＳＭを認証設備室外に持ち出す場合は、認証設備室内にて物理的に破壊する。

また、ＣＡ秘密鍵のバックアップ媒体も、一連の操作指示において遅延なく物理的に媒体を破壊する。

6.2.11　秘密鍵の認証設備室からＩＣカード発行局への配送方法

加入者秘密鍵は、複数人の運用要員及び委託先要員の相互牽制により、認証設備室からＩＣカード発行局へ安全に運搬される。要員間での受け渡しの際は、相互に顔写真付き識別証を提示し正当な相手であることを確認する。なお、運搬途中に加入者秘密鍵が危殆化またはその恐れがある場合は、関連する加入者証明書を全て失効する。

6.2.12　ＩＣカード発行局での加入者秘密鍵の取扱方法

ＩＣカード発行局の要員は、暗号化された加入者の秘密鍵及びＰＩＮ情報を格納した記録媒体を

受け取る際に、その運搬経路における危殆化の有無を確認する。また、受領後ＩＣカード発行処理が終了し電子認証局事務局に返却するまでの間、記録媒体をＩＣカード発行局に保管する。
ＩＣカード発行の際に生成される同秘密鍵を含む中間ファイルは、ＩＣカード発行後速やかに消去する。
記録媒体は、ＩＣカード発行局から外部に持ち出す前に物理的に破壊される。

6.2.13　加入者秘密鍵のＩＣカード発行局から加入者への配送方法

加入者の秘密鍵を格納したＩＣカードとＰＩＮ情報は、同一の封筒に梱包して本人限定受取郵便（基本型）を用いて、法令に基づく勤務地の加入者本人宛に郵送する。

6.3 鍵ペアの管理

6.3.1　公開鍵のアーカイブ

公開鍵のアーカイブは改ざんを防止する措置をとる。アーカイブ期間について以下に示す。

表 6-1 公開鍵のアーカイブ期間

種類	アーカイブ期間
ＣＡの自己署名証明書	有効期間満了から１０年
加入者証明書	有効期間満了から１０年

6.3.2　公開鍵と秘密鍵の有効期間

公開鍵と秘密鍵の有効期間を以下に示す。

表 6-2 公開鍵と秘密鍵の有効期間

種類	有効期間
ＣＡ秘密鍵	１０年
ＣＡの自己署名証明書	１０年
リンク証明書	（注１）
相互認証証明書	５年未満
加入者証明書	発行の可否判断をしてから 5 年未満（注２）

（注1）　リンク証明書（OldWithNew、NewWithOld）の有効期間は、それぞれ異なる。OldWithNew の有効期間は、OldWithOld の有効期間と同一である。NewWithOld の有効期間は、NewWithNew の notBefore から OldWithOld の notAfter までである。

（注2）　平成２０年３月３１日までの間に発行する加入者の秘密鍵及び加入者証明書の有効期間満了日は、全ての加入者について平成２０年９月３０日とする。
平成２０年４月１日から平成２４年９月３０日までの間に発行する加入者の秘密鍵及び加入者証明書の有効期間満了日は、全ての加入者について平成２５年３月３１日とする。

6.4 活性化データの管理

6.4.1　活性化データの生成と組み込み

ＣＡ秘密鍵を活性化するためのＰＩＮ情報は、ＨＳＭでのＣＡ秘密鍵生成時に複数人のセキュリティセンタシステム担当者の立会いのもと HSM 鍵管理者が設定する。

加入者の秘密鍵を活性化するためのＰＩＮ情報は、加入者の秘密鍵を発行局システムから取り出すときに生成する。作業は、複数人のセキュリティセンタシステム担当者が相互牽制下で行う。

ＰＩＮ情報は、ＩＣカードと同封して本人限定郵便（基本型）で郵送する。

6.4.2　活性化データの保護

ＣＡ秘密鍵を活性化するためのＰＩＮ情報は、6 ヶ月に一回以上変更を行う。
加入者の秘密鍵を活性化するためのＰＩＮ情報は、定期的に変更する。

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機能

電子認証局が使用する認証業務用設備は、十分な信頼度を有する装置を使用する。

6.5.2　コンピュータセキュリティの評価

電子認証局は、セキュリティ基準を規定し、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 ライフサイクルの技術的な管理

電子認証局で採用するシステムは、信頼できる組織で開発及びテストされたことが証明できるものを使用する。

6.7 ネットワークセキュリティの管理

電子認証局は、必要に応じて以下の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ざんを防止するための装置、あるいはシステムを設置する。

認証業務用設備のネットワークは、ファイアウォールを介して接続する。
ファイアウォールでは、不正アクセスの記録を監査証跡として取得する。
また、必要に応じて外部からペネトレーションテストを実施する。

ＩＣカード発行局のＩＣカード発行システムは、ＩＣカード発行局外の機器とのネットワーク等による接続を行わない。

6.8 セキュリティ監査手続き

セキュリティ監査人は、ネットワークセキュリティの強度が適切に維持されていることを確認し、外部ネットワークからのセキュリティ侵害の有無を確認するためにセキュリティ監査を実施する。

セキュリティ監査は二部から構成されている。

(1) セキュリティ強度診断

ＩＡ／ＲＡサーバ、リポジトリサーバのセキュリティ強度が適切に管理されていることを監査する。

(2) ＩＤＳログ監査

セキュリティセンタに設置された侵入検知装置（ＩＤＳ）のログを監査し、重大なセキュリティ侵害の可能性がないかを監査する。

7　電子証明書とＡＲＬ及びＣＲＬプロファイル

本サービスで発行する電子証明書、ＣＲＬ及びＡＲＬの形式、属性の使用は以下の標準仕様に従って定義する。

(1) ITU-T Recommendation X.509(1997E)
(2) RFC2459 Internet X.509 PKI Certificate and CRL Profile, January1999

これらの標準仕様は現在も改版作業が続けられており、今後決定される標準仕様に対しては、その対応状況を考慮して対応して行く。

7.1 電子証明書のプロファイル

本サービスで発行する電子証明書のプロファイル一覧を表 7-1 に示す。

表 7-1 電子証明書プロファイル

フィールド名	設定				備考
	自己署名証明書	リンク証明書	相互認証証明書	加入者証明書	
電子証明書基本部（Certificate Basic Fields）					
バージョン（version）	○	○	○	○	Version3
シリアル番号（serialNumber）	○	○	○	○	
電子署名アルゴリズム（signature）	○	○	○	○	
発行者（issuer）	○	○	○	○	
有効期間（validity）	○	○	○	○	UTCTime
所有者（subject）	○	○	○	○	
所有者公開鍵（subjectPublicKeyInfo）	○	○	○	○	
発行者一意 ID（issuerUniqueID）	×	×	×	×	
所有者一意 ID（subjectUniqueID）	×	×	×	×	
電子証明書標準拡張部（Certificate Standard Extensions）					
認証局鍵識別（authorityKeyIdentifier）	○	○	○	○	
所有者鍵識別（subjectKeyIdentifier）	○	○	○	○	
鍵種別（keyUsage）	○	○	○	○	
拡張鍵種別（extendedKeyUsages）	×	×	×	×	
秘密鍵有効期間（privateKeyUsagePeriod）	×	×	×	×	
電子証明書ポリシ（certificatePolicies）	×	○	○	○	

ポリシマッピング（policyMappings）	×	×	○	×	
所有者別名（subjectAltName）	×	×	×	×	
発行者別名（issuerAltName）	×	×	×	×	
基本制約（basicConstraints）	○	○	○	×	
名前制約（nameConstraints）	×	×	×	×	
ポリシ制約（policyConstraints）	×	×	○	×	
CRL 分配点（cRLDistributionPoints）	○	○	○	○	
所有者ディレクトリ属性（subjectDirectoryAttributes）	×	×	×	×	

（○：設定する。 ×：設定しない）

7.2 ＣＲＬ及びＡＲＬのプロファイル

本サービスで発行するＣＲＬ及びＡＲＬのプロファイル一覧を表 7-2 に示す。

表 7-2ＣＲＬ及びＡＲＬのプロファイル

フィールド名	設定	備考
CRL 基本部（CRL Basic Fields）		
バージョン（version）	○	Version2
電子署名アルゴリズム（signature）	○	
発行者（issuer）	○	
今回更新日時（thisUpdate）	○	UTCTime
次回更新予定日時（nextUpdate）	○	UTCTime
失効証明書（RevokedCertificates）	○	
証明書シリアル番号(userCertificate)	○	
失効日時(revocationDate)	○	
理由コード(reasonCode)	○	
CRL 拡張部（CRL Extensions）		
認証局鍵識別（authorityKeyIdentifier）	○	
発行者別名（issuerAltName）	×	
CRL 番号（cRLNumber）	○	
デルタ CRL 識別（deltaCRLIndicator）	×	
発行分配点（issuingDistributionPoint）	○	

（○：設定する。 ×：設定しない）

7.3 電子証明書プロファイルの詳細

本サービスで発行する電子証明書プロファイルの詳細を以下に示す。

7.3.1 自己署名証明書

自己署名証明書のプロファイル詳細を表 7-3 に示す。

表 7-3 自己署名証明書プロファイル詳細

(1) 電子証明書基本領域(Basic)

名称	設定値
version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier algorithm parameters	電子証明書への署名に使用された電子署名アルゴリズムの識別子 sha1WithRSAEncryption 電子署名アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 5 電子署名アルゴリズムの引数 型:NULL 値:なし
validity	
validity notBefore notAfter 	電子証明書の有効期間 開始日時 型:UTC Time 値:yymmddhhmmssZ 終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName Type Value 	電子証明書発行者の国名 国名のオブジェクト ID 型:OID 値:2 5 4 6 国名の値 型:PrintableString 値:JP

organizationName	電子証明書発行者の組織名
Type	組織名のオブジェクト ID
	型：OID
	値：2 5 4 10
value	組織名の値
	型：UTF8String
	値(英語)：
	JapanFederationOfCertifiedPublicTaxAccountants’Associations
organizationalUnitName	電子証明書発行者の組織単位名
Type	組織単位名のオブジェクト ID
	型：OID
	値：2 5 4 11
value	組織単位名の値
	型：UTF8String
	値(英語)：
	JapanFederationOfCertifiedPublicTaxAccountants’Associations
	CA
subject	
countryName	電子証明書所有者の国名
Type	国名のオブジェクト ID
	型：OID
	値：2 5 4 6
value	国名の値
	型：PrintableString
	値：JP
organizationName	電子証明書所有者の組織名
Type	組織名のオブジェクト ID
	型：OID
	値：2 5 4 10
value	組織名の値
	型：UTF8String
	値(英語)：
	JapanFederationOfCertifiedPublicTaxAccountants’Associations
organizationalUnitName	電子証明書所有者の組織単位名
Type	組織単位名のオブジェクト ID
	型：OID
	値：2 5 4 11
value	組織単位名の値
	型：UTF8String
	値(英語)：
	JapanFederationOfCertifiedPublicTaxAccountants’Associations
	CA
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報

algorithmIdentifier	暗号アルゴリズムの識別子 RSAEncryption
algorithm	暗号アルゴリズムのオブジェクト ID 型：OID 値：1 2 840 113549 1 1 1
parameters	暗号アルゴリズムの引数 型：NULL 値：なし
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値

(2) 電子証明書標準拡張領域(extensions)

名称	設定値
authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
KeyIdentifier	公開鍵の識別子 SHA-1 160bit 型：OCTET STRING 値：ユニークなバイト列
subjectKeyIdentifier （クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型：OCTET STRING 値：ユニークなバイト列
keyUsage （クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型：BitString 値：000001100(keyCertSign、cRLSign)
basicConstraints （クリティカルフラグ = TRUE)	
basicConstraints	基本的制限
cA	CA かどうかを示すフラグ 型：BOOLEAN 値：TRUE
cRLDistributionPoints （クリティカルフラグ = FALSE)	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
uniformResourceIdentifier	CRL の URI 値： ldap://ldap.nichizeiren.or.jp/ou%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations%20CA,o%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations,c%3dJP?authorityRevocationList

7.3.2　リンク証明書

リンク証明書のプロファイル詳細を表 7-4 に示す。

表 7-4 リンク証明書プロファイル詳細

(1)電子証明書基本領域(Basic)

名称	設定値
version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier	電子証明書への署名に使用された電子署名アルゴリズムの識別子 sha1WithRSAEncryption
algorithm	電子署名アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 5
parameters	電子署名アルゴリズムの引数 型:NULL 値:なし
validity	
validity	電子証明書の有効期間
notBefore	開始日時 型:UTC Time 値:yymmddhhmmssZ
notAfter	終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName	電子証明書発行者の国名
type	国名のオブジェクト ID 型:OID 値:2 5 4 6
value	国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名
type	組織名のオブジェクト ID

	型:OID
	値:2 5 4 10
value	組織名の値
	型:UTF8String
	値(英語): JapanFederationOfCertifiedPublicTaxAccountants'Associations
organizationalUnitName	電子証明書発行者の組織単位名
type	組織単位名のオブジェクト ID
	型:OID
	値:2 5 4 11
value	組織単位名の値
	型:UTF8String
	値(英語): JapanFederationOfCertifiedPublicTaxAccountants'Associations CA
subject	
countryName	電子証明書所有者の国名
type	国名のオブジェクト ID
	型:OID
	値:2 5 4 6
value	国名の値
	型:PrintableString
	値:JP
organizationName	電子証明書所有者の組織名
type	組織名のオブジェクト ID
	型:OID
	値:2 5 4 10
value	組織名の値
	型:UTF8String
	値(英語): JapanFederationOfCertifiedPublicTaxAccountants'Associations
organizationalUnitName	電子証明書所有者の組織単位名
type	組織単位名のオブジェクト ID
	型:OID
	値:2 5 4 11
value	組織単位名の値
	型:UTF8String
	値(英語): JapanFederationOfCertifiedPublicTaxAccountants'Associations CA
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子
	RSAEncryption

algorithm	暗号アルゴリズムのオブジェクト ID 型：OID 値：1 2 840 113549 1 1 1
parameters	暗号アルゴリズムの引数 型：NULL 値：なし
subjectPublicKey	公開鍵値 型：BIT STRING 値：公開鍵値

(2) 電子証明書標準拡張領域(extensions)

名称	設定値
authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子 SHA-1 160bit 型：OCTET STRING 値：ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型：OCTET STRING 値：ユニークなバイト列
keyUsage (クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型：BitString 値：000001100(keyCertSign、cRLSign)
certificatePolicies (クリティカルフラグ = FALSE)	
policyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型：OID 値：2 5 29 32 0 ※ AnyPolicy
basicConstraints (クリティカルフラグ = TRUE)	
basicConstraints	基本的制限
cA	CA かどうかを示すフラグ 型：BOOLEAN 値：TRUE
cRLDistributionPoints (クリティカルフラグ = FALSE)	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
uniformResourceIdentifier	CRL の URI 値： ldap://ldap.nichizeiren.or.jp/ou%3dJapanFederationOfCertifiedP

	ublicTaxAccountants'Associations%20CA,o%3dJapanFederation OfCertifiedPublicTaxAccountants'Associations,c%3dJP?authorityRevocationList

7.3.3　相互認証証明書

相互認証証明書のプロファイル詳細を表 7-5 に示す。

表 7-5 相互認証証明書プロファイル詳細

(1)電子証明書基本領域(Basic)

名称	設定値
version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier	電子証明書への署名に使用された電子署名アルゴリズムの識別子 sha1WithRSAEncryption
Algorithm	電子署名アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 5
Parameters	電子署名アルゴリズムの引数 型:NULL 値:なし
validity	
validity	電子証明書の有効期間
notBefore	開始日時 型:UTC Time 値:yymmddhhmmssZ
notAfter	終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName	電子証明書発行者の国名
Type	国名のオブジェクト ID 型:OID 値:2 5 4 6
Value	国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名
Type	組織名のオブジェクト ID

	型:OID 値:2 5 4 10
value	組織名の値 型:UTF8String 値(英語): JapanFederationOfCertifiedPublicTaxAccountants'Associations
organizationalUnitName	電子証明書発行者の組織単位名
Type	組織単位名のオブジェクト ID 型:OID 値:2 5 4 11
value	組織単位名の値 型:UTF8String 値(英語): JapanFederationOfCertifiedPublicTaxAccountants'Associations CA
subject	
	BCAから指定されるDN名 相互認証証明書要求ファイルで指定される
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子 RSAEncryption
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
subjectPublicKey	公開鍵値 型:BIT STRING 値:公開鍵値

(2)電子証明書標準拡張領域(extensions)

名称	設定値
authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier (クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING

	値:ユニークなバイト列
keyUsage （クリティカルフラグ = TRUE）	
keyUsage	鍵の使用目的 型:BitString 値:000001100(keyCertSign、cRLSign)
certificatePolicies （クリティカルフラグ = TRUE）	
policyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型:OID 値:1 2 392 200151 1 1 1
policyQualifiers	ポリシ修飾子
policyQualifierID	ポリシ修飾子のオブジェクト ID 型:OID 値:1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ（URI） 型:IA5String 値:https://cainfo.nichizeiren.or.jp/ca/
policyMappings （クリティカルフラグ = FALSE）	
issuerDomainPolicy	発行者のドメイン・ポリシ OID 型:OID 値:1 2 392 200151 1 1 1
subjectDomainPolicy	相互認証先認証局(GPKI BCA)のドメイン・ポリシ OID
basicConstraints （クリティカルフラグ = TRUE）	
basicConstraints	基本的制限
cA	CA かどうかを示すフラグ 型:BOOLEAN 値:TRUE
policyConstraints （クリティカルフラグ = TRUE）	
requireExplicitPolicy	ポリシの要求 型:INTEGER 値:0
inhibitPolicyMapping	ポリシマッピングの制限 型:INTEGER 値:1
cRLDistributionPoints （クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
uniformResourceIdentifier	CRL の URI 値: ldap://ldap.nichizeiren.or.jp/ou%3dJapanFederationOfCertified PublicTaxAccountants'Associations%20CA,o%3dJapanFederati onOfCertifiedPublicTaxAccountants'Associations,c%3dJP? authorityRevocationList

7.3.4　加入者証明書

加入者証明書のプロファイル詳細を表 7-6 に示す。

表 7-6 加入者証明書プロファイル詳細

(1) 電子証明書基本領域(Basic)

名称	設定値
version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:2
serialNumber	
certificateSerialNumber	電子証明書のシリアル番号 型:INTEGER 値:ユニークな整数
signature	
algorithmIdentifier	電子証明書への署名に使用された電子署名アルゴリズムの識別子 sha1WithRSAEncryption
Algorithm	電子署名アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 5
Parameters	電子署名アルゴリズムの引数 型:NULL 値:なし
validity	
validity	電子証明書の有効期間
notBefore	開始日時 型:UTC Time 値:yymmddhhmmssZ
notAfter	終了日時 型:UTC Time 値:yymmddhhmmssZ
issuer	
countryName	電子証明書発行者の国名
Type	国名のオブジェクト ID 型:OID 値:2 5 4 6
Value	国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名
Type	組織名のオブジェクト ID

	型：OID 値：2 5 4 10
value	組織名の値 型：UTF8String 値(英語)： JapanFederationOfCertifiedPublicTaxAccountants’Associations
organizationalUnitName	電子証明書発行者の組織単位名
Type	組織単位名のオブジェクト ID 型：OID 値：2 5 4 11
value	組織単位名の値 型：UTF8String 値(英語)： JapanFederationOfCertifiedPublicTaxAccountants’Associations CA
subject	
countryName	電子証明書所有者の国名
Type	国名のオブジェクト ID 型：OID 値：2 5 4 6
value	国名の値 型：PrintableString 値：JP
organizationName	電子証明書所有者の組織名
Type	組織名のオブジェクト ID 型：OID 値：2 5 4 10
value	組織名の値 型：UTF8String 値(英語)： JapanFederationOfCertifiedPublicTaxAccountants’Associations
organizationalUnitName	電子証明書所有者の組織単位名
Type	組織単位名のオブジェクト ID 型：OID 値：2 5 4 11
value	組織単位名の値 型：UTF8String 値(英語)：Registration Number:9999999（7 桁固定） ※ 9999999 は、税理士登録番号をゼロパディングした 7 桁の値である。
commonName	電子証明書所有者の固有名称
Type	固有名称のオブジェクト ID

	型:OID 値:2 5 4 3
value	固有名称の値 型:UTF8String 値(日本語):XXXXXXX ※ XXXXXXX は申請者氏名のローマ字表記（アルファベットのみ）であり、電子証明書発行申請書兼利用同意書の申請内容による。
subjectPublicKeyInfo	
subjectPublicKeyInfo	電子証明書所有者の公開鍵に関する情報
algorithmIdentifier	暗号アルゴリズムの識別子 RSAEncryption
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 1
parameters	暗号アルゴリズムの引数 型:NULL 値:なし
subjectPublicKey	公開鍵値 型:BIT STRING 値:公開鍵値

(2) 電子証明書標準拡張領域(extensions)

名称	設定値
authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子　SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
subjectKeyIdentifier （クリティカルフラグ = FALSE)	
subjectKeyIdentifier	電子証明書所有者の公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
keyUsage （クリティカルフラグ = TRUE)	
keyUsage	鍵の使用目的 型:BitString 値:110000000 (digitalSignature、nonRepudiation)
certificatePolicies （クリティカルフラグ = TRUE)	
policyInformation	ポリシに関する情報
policyIdentifier	ポリシのオブジェクト ID 型:OID 値:1 2 392 200151 1 1 1
policyQualifiers	ポリシ修飾子

policyQualifierID	ポリシ修飾子のオブジェクト ID 型：OID 値：1 3 6 1 5 5 7 2 1
qualifier	CPS へのポインタ（URI） 型：IA5String 値：https://cainfo.nichizeiren.or.jp/ca/
cRLDistributionPoints （クリティカルフラグ = FALSE）	
cRLDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
uniformResourceIdentifier	CRL の URI 値： ldap://ldap.nichizeiren.or.jp/ou%3dJapanFederationOfCertified PublicTaxAccountants'Associations%20CA,o%3dJapanFederati onOfCertifiedPublicTaxAccountants'Associations,c%3dJP?cert ificateRevocationList

7.3.5　ＣＲＬ

ＣＲＬのプロファイル詳細を表 7-7 に示す。

表 7-7ＣＲＬプロファイル詳細

(1)基本領域(Basic)

名称	設定値
version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:1
signature	
algorithmIdentifier	電子証明書への署名に使用された電子署名アルゴリズムの識別子 sha1WithRSAEncryption
algorithm	電子署名アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 5
parameters	電子署名アルゴリズムの引数 型:NULL 値:なし
issuer	
countryName	電子証明書発行者の国名
type	国名のオブジェクト ID 型:OID 値:2 5 4 6
value	国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名
type	組織名のオブジェクト ID 型:OID 値:2 5 4 10
value	組織名の値 型:UTF8String 値(英語): JapanFederationOfCertifiedPublicTaxAccountants'Associations
organizationalUnitName	電子証明書発行者の組織単位名
type	組織単位名のオブジェクト ID 型:OID 値:2 5 4 11
value	組織単位名の値

	型:UTF8String 値(英語): JapanFederationOfCertifiedPublicTaxAccountants'Associations CA
thisUpdate	
thisUpdate	電子証明書の更新日 型:UTC Time 値:yymmddhhmmssZ
nextUpdate	
nextUpdate	電子証明書の次回更新日 型:UTC Time 値:yymmddhhmmssZ
revokedCertificates	
userCertificate	電子証明書シリアル番号 型:INTEGER 値:ユニークな整数
revocationDate	失効日 型:UTC Time 値:yymmddhhmmssZ
crlEntryExtensions	失効リストエントリ拡張領域
reasonCode (クリティカルフラグ = FALSE)	理由コード 型:ENUMERATED 値:失効事由(作業指示書(失効)による)に応じて設定

(2)標準拡張領域(extensions)

名称	設定値
authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報
keyIdentifier	公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
cRLNumber (クリティカルフラグ = FALSE)	
cRLNumber	失効リストの番号 型:INTEGER 値:ユニークな整数
issuingDistributionPoint (クリティカルフラグ = TRUE)	
issuingDistributionPoints	CRL 配布点に関する情報
distributionPoint	CRL 配布点
fullName	
uniformResourceIdentifier	CRL の URI 値: ldap://ldap.nichizeiren.or.jp/ou%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations%20CA,o%3dJapanFederati

	onOfCertifiedPublicTaxAccountants'Associations,c%3dJP?certificateRevocationList
onlyContainsUserCerts	ユーザ証明書に対する失効のみかを示すフラグ 型：BOOLEAN 値：TRUE

7.3.6　ＡＲＬ

ＡＲＬのプロファイル詳細を表 7-8 に示す。

表 7-8ＡＲＬプロファイル詳細

(1)基本領域(Basic)

名称	設定値
version	
version	電子証明書フォーマットのバージョン番号 型:INTEGER 値:1
signature	
algorithmIdentifier	電子証明書への署名に使用された電子署名アルゴリズムの識別子 sha1WithRSAEncryption
algorithm	電子署名アルゴリズムのオブジェクト ID 型:OID 値:1 2 840 113549 1 1 5
parameters	電子署名アルゴリズムの引数 型:NULL 値:なし
issuer	
countryName	電子証明書発行者の国名
Type	国名のオブジェクト ID 型:OID 値:2 5 4 6
Value	国名の値 型:PrintableString 値:JP
organizationName	電子証明書発行者の組織名
Type	組織名のオブジェクト ID 型:OID 値:2 5 4 10
Value	組織名の値 型:UTF8String 値(英語): JapanFederationOfCertifiedPublicTaxAccountants'Associations
organizationalUnitName	電子証明書発行者の組織単位名
Type	組織単位名のオブジェクト ID 型:OID 値:2 5 4 11
Value	組織単位名の値

	型:UTF8String 値(英語): JapanFederationOfCertifiedPublicTaxAccountants'Associations CA
thisUpdate	
thisUpdate	電子証明書の更新日 型:UTC Time 値:yymmddhhmmssZ
nextUpdate	
nextUpdate	電子証明書の次回更新日 型:UTC Time 値:yymmddhhmmssZ
revokedCertificates	
userCertificate	電子証明書シリアル番号 型:INTEGER 値:ユニークな整数
revocationDate	失効日 型:UTC Time 値:yymmddhhmmssZ
crlEntryExtensions	失効リストエントリ拡張領域
reasonCode (クリティカルフラグ = FALSE)	理由コード 型:ENUMERATED 値:失効事由(作業指示書(失効)による)に応じて設定

(2)標準拡張領域(extensions)

名称	設定値
authorityKeyIdentifier (クリティカルフラグ = FALSE)	
authorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 SHA-1 160bit 型:OCTET STRING 値:ユニークなバイト列
cRLNumber (クリティカルフラグ = FALSE)	
cRLNumber	失効リストの番号 型:INTEGER 値:ユニークな整数
issuingDistributionPoint (クリティカルフラグ = TRUE)	
issuingDistributionPoints distributionPoint fullName uniformResourceIdentifier	CRL 配布点に関する情報 CRL 配布点 CRL の URI 値: ldap://ldap.nichizeiren.or.jp/ou%3dJapanFederationOfCertifiedPublicTaxAccountants'Associations%20CA,o%3dJapanFederati

	onOfCertifiedPublicTaxAccountants'Associations,c%3dJP?authorityRevocationList
onlyContainsCACerts	CA 証明書に対する失効のみかを示すフラグ 型：BOOLEAN 値：TRUE

8　運営委員会

運営委員会は、以下のとおり運営する。

8.1 運営

運営委員会は、次に掲げる事項を所掌する。

・他の認証局との相互認証の承認及び相互認証の取消しの決定に係る事項
・準拠性監査の結果を開示することについての承認に係る事項
・本基準及び事務取扱要領を制定または改訂することについての承認に係る事項
・ＣＡ秘密鍵の危殆化により、当該秘密鍵で署名した電子証明書を失効することについての決定に係る事項
・その他、認証局の運営に関する事項で運営責任者からの承認または決定の求めに対する承認または決定に係る事項

8.2 構成

運営委員会は、運営委員会委員長及び委員４人以内で構成する。
運営委員会委員長には、日税連の会長を充てる。
委員は、本会専務理事及び総務部長から本会会長が任命する。
運営委員会委員長に事故あるときまたは欠員となったときは、委員の互選により、これを選出する。

8.3 運営委員会の招集及び議長

運営委員会は、運営委員会委員長が招集する。
運営委員会を招集しようとするときは、会日の２週間前までに、会議の日時、場所及び議案を記載した書面を構成員に発送して通知しなければならない。ただし、運営委員会委員長が必要と認めたときは、期間を短縮し、または書面によらない方法で通知することができる。
運営委員会の議長は、運営委員会委員長があたる。

8.4 定足数

会議は、構成員の２分の１以上が出席しなければ、開くことができない。

8.5 議決の要件

運営委員会の議決は、出席委員の過半数で決し、可否同数のときは、議長の決するところによる。

8.6 運営委員会会議議事録

会議の議事については、運営委員会会議議事録を作成し、保存しなければならない。運営委員会会議議事録には、議長及び出席委員２人以上が署名押印しなければならない。

8.7 書面決議

運営委員会委員長が運営委員会に付議すべき事項について会議を招集する必要がないと認めたときは、議案を記載した書面を構成員に送って、当該議案に対する賛否の意見を求め、書面による議決をすることができる。この場合、本基準 8.4（定足数）と本基準 8.5（議決の要件）の規定を準用する。

8.8 運営委員会委員長の職務及び権限

運営委員会委員長は、運営責任者を指揮監督し、認証局の事務の執行を掌理する。
運営委員会委員長は、運営責任者及び運用要員の任命及び罷免を行う。
運営委員会委員長は、運営委員会での決定に基づき本基準及び事務取扱要領の承認を行う。
運営委員会委員長は、必要と認めた場合適宜準拠性監査の指示を行う。
運営委員会委員長は、監査計画の承認を行う。
運営委員会委員長は、監査人から監査報告を受ける。
運営委員会委員長は、監査基準書の制定及び改廃の承認を行う。

9　仕様管理

電子認証局は、準拠性監査の結果やセキュリティ技術等最新の技術動向、ＧＰＫＩの運用方針などを踏まえ、必要に応じて本基準の改訂を行うものとする。

9.1 本基準の変更手続き

電子認証局は、必要に応じて加入者及び検証者等関係者の事前の承諾を得ること無く、本基準の改訂を行うことができるものとする。

本基準の改訂にあたっては、運営委員会において改訂内容を検討し、運営委員会委員長がその妥当性を確認し、承認する。承認後は、遅滞なく改訂を行う。

本基準の改訂により電子署名法に定める変更認定が必要となる場合には、必ず事前に変更認定申請の手続きを行う。

9.2 公表及び通知

電子認証局は、本基準を改訂した場合、本基準 2.7（公開とリポジトリ）に規定するリポジトリにおいて改訂後の本基準を公開する。

加入者及び検証者等関係者への改訂の通知は、リポジトリへの公開をもって行う。

本基準の改訂は、変更履歴を表すバージョン番号と改版日付によって識別される。

9.3 仕様認可の手続き

本基準の改訂が行われた場合、加入者証明書が発行された時期に拘らずリポジトリに掲載されている改訂後の基準が適用される。

電子認証局は、加入者が改訂後の基準について公開後３０日以内に加入者証明書の失効を請求しない限り、改訂に同意したものとみなす。

検証者は、改訂後の基準に同意できない場合、加入者証明書を利用した電子署名の検証を中止しなければならない。

9.4 本基準の保存

電子認証局は、本サービスを継続している間及び当該帳簿書類に係る電子証明書の有効期間の満了日から 10 年間、本基準の変更履歴とそれぞれのバージョン番号の基準を保存するものとする。