

---

# 全国社会保険労務士会連合会認証局

## 認証業務規程

第2.1版

平成22年5月19日

全国社会保険労務士会連合会

## 変更履歴

版数	承認日	内容	作成者	承認者
1.0	2003/6/10	初版作成	河端 祐一	中井 敏夫
1.1	2003/9/10	G P K I 相互認証接続申請に伴う変更修正	河端 祐一	中井 敏夫
1.2	2004/6/10	電子証明書プロファイルの記載方法を変更	河端 祐一	中井 敏夫
1.2.1	2004/11/1	事務所移転に伴い連絡先所在地等を変更	河端 祐一	中井 敏夫
1.3	2005/6/8	利用者による発行申請書の修正方法を追加	河端 祐一	中井 敏夫
1.4	2006/6/5	「誤字俗字・正字一覧表」を最新版に修正	河端 祐一	中井 敏夫
1.5	2006/10/6	証明書利用用途に電磁的記録の保存を追加	小室 理恵子	中井 敏夫
1.6	2007/4/2	誤記訂正	小室 理恵子	中井 敏夫
1.7	2007/11/2	有効期間満了に伴う更新期間を3ヶ月から5ヶ月に修正	飯倉 裕基	加藤 光昭
1.8	2008/4/1	証明書格納媒体をFDからUSBメモリに変更	飯倉 裕基	加藤 光昭
1.9	2008/5/29	事務所名等を社会保険労務士名簿から転載することを明示	飯倉 裕基	加藤 光昭
1.10	2009/2/27	配達記録郵便の廃止に伴う変更修正	飯倉 裕基	奥田 久美
1.11	2009/3/26	認証局の義務に、新旧自己署名証明書、リンク証明書のフィンガープリントを公開することに修正	飯倉 裕基	奥田 久美
1.12	2009/3/26	認証局が損害賠償責任を負う場合の上限額の明示	飯倉 裕基	奥田 久美
1.13	2009/5/22	戸籍謄本等の名称変更等に伴う修正	飯倉 裕基	奥田 久美
2.0	2009/11/2	連絡先にかかる担当部署名を変更	飯倉 裕基	奥田 久美
2.1	2010/5/19	電子証明書のプロファイルの項目名を修正	飯倉 裕基	奥田 久美

1	はじめに	1
1.1	概要	1
1.2	識別	1
1.3	コミュニティと適応性	2
1.3.1	認証業務規程の適用範囲	2
1.3.2	認証局	2
1.3.3	発行局 (IA)	2
1.3.4	登録局 (RA)	3
1.3.5	利用者	3
1.3.6	検証者	3
1.3.7	リポジトリ	3
1.3.8	利用者証明書の適用範囲	3
1.3.9	電子署名法における属性についての証明	3
1.4	連絡先の詳細	3
2	一般的な規定	5
2.1	義務	5
2.1.1	認証局の義務	5
2.1.2	IA の義務	5
2.1.3	RA の義務	6
2.1.4	利用者の義務	6
2.1.5	検証者の義務	7
2.1.6	リポジトリの義務	8
2.2	責任	8
2.2.1	認証局の責任	8
2.2.2	IA の責任	8
2.2.3	RA の責任	8
2.2.4	利用者の責任	8
2.2.5	検証者の責任	8
2.2.6	リポジトリの責任	8
2.3	財務上の責任	8
2.3.1	損害賠償	8
2.4	人事管理と事務取扱要領などの規程	9
2.4.1	独立性、第三者性	9
2.4.2	専門性	9
2.4.3	組織体制	9
2.4.4	人事管理	10
2.4.5	事務取扱要領等の規程	10
2.5	解釈及び執行	10
2.5.1	準拠法	10
2.5.2	認証業務規程の可分性	10
2.5.3	効力の存続	10
2.5.4	認証業務規程の完全性	10
2.5.5	連絡	10
2.5.6	紛争解決手続き	10
2.6	料金	10
2.7	公開とリポジトリ	10
2.7.1	認証局の情報の公開	10
2.7.2	公開の頻度	11

2.7.3	アクセスコントロール	11
2.7.4	リポジトリ	11
2.8	準拠性監査	11
2.8.1	準拠性監査の頻度	11
2.8.2	監査人の任命	11
2.8.3	監査人の監査される主体との関係	11
2.8.4	監査テーマ	12
2.8.5	監査指摘事項への措置	12
2.8.6	監査結果の公開	12
2.9	秘密情報	12
2.9.1	秘密情報の種類	12
2.9.2	個人情報の取扱い	13
2.9.3	電子証明書の失効情報の公開	13
2.9.4	法執行機関への情報開示	14
2.9.5	民事手続き上の開示	14
2.9.6	利用者証明書名義人の要請に基づく開示	14
2.9.7	秘密情報として取扱わない情報	14
2.10	知的財産権	14
3	識別と本人確認	14
3.1	初期登録（発行申請）	14
3.1.1	名前の型	15
3.1.2	名前の意味に関する要件	15
3.1.3	名前形式を解釈するための規則	16
3.1.4	名前の一意性	16
3.1.5	名前に関する紛争の解決手段	16
3.1.6	商標の認識・認証・役割	16
3.1.7	秘密鍵の所有を証明するための方法	16
3.1.8	本人確認	16
3.2	利用者証明書の更新	17
3.3	利用者証明書失効後の再発行	17
3.4	利用者証明書の失効申請	17
3.4.1	失効申請者の真偽確認	17
4	運用上の要件	18
4.1	電子証明書発行申請	18
4.1.1	利用者による申請	18
4.1.2	発行申請書類	18
4.1.3	代理人による申請	19
4.1.4	利用者本人による申請の審査	19
4.1.5	申請の登録	19
4.2	電子証明書の発行	19
4.3	秘密鍵及び電子証明書の受領	19
4.4	電子証明書の更新申請	20
4.5	電子証明書の失効申請	20
4.5.1	失効申請方法	20
4.5.2	失効申請書類	20
4.5.3	利用者証明書の失効	21
4.5.4	失効申請者への通知	21
4.5.5	認証局による失効	21

4.5.6	一時停止	22
4.5.7	失効リスト (CRL・ARL)	22
4.5.8	失効情報及び有効性確認情報に関する要件	22
4.5.9	認証局秘密鍵の危殆化に関する特別要件	22
4.6	セキュリティ監査手続き	22
4.6.1	記録されるイベント	22
4.6.2	監査の頻度	22
4.6.3	監査ログの保存期間	22
4.6.4	監査証跡の保護	22
4.6.5	監査証跡のバックアップ手順	22
4.6.6	監査証跡の記録システム	23
4.6.7	問題の原因となるイベントの通知	23
4.7	記録のアーカイブ	23
4.7.1	申請に係るデータ	23
4.7.2	組織関係データ	24
4.7.3	設備及び安全対策措置に関するデータ	24
4.7.4	アーカイブデータの保護	24
4.7.5	アーカイブデータのバックアップ	25
4.7.6	アーカイブ情報の保管	25
4.7.7	関係書類及び記録の破棄	25
4.8	鍵の更新	25
4.9	危殆化と災害の復旧	25
4.10	特定認証業務の終了	26
5	物理的、手続的、要員のセキュリティ統制	26
5.1	物理的セキュリティ統制	26
5.1.1	登録用端末設備室のセキュリティ	26
5.1.2	認証設備室のセキュリティ	26
5.2	手続きのセキュリティ統制	27
5.3	要員のセキュリティ統制	27
6	技術的セキュリティ統制	28
6.1	鍵ペアの生成とインストール	28
6.1.1	鍵ペアの生成	28
6.1.2	利用者証明書発行者への利用者公開鍵の引渡し	28
6.1.3	利用者への自己署名証明書の配送	28
6.1.4	利用者への鍵配送	28
6.1.5	鍵のサイズ	28
6.1.6	ハードウェア/ソフトウェアでの鍵生成	28
6.1.7	鍵の使用目的	28
6.2	認証局秘密鍵の保護	29
6.2.1	認証局秘密鍵の複数人管理	29
6.2.2	秘密鍵の寄託	29
6.2.3	認証局秘密鍵のバックアップ	29
6.2.4	認証局秘密鍵の暗号モジュールへの格納	29
6.2.5	認証局秘密鍵をアクティブにする方法	29
6.2.6	認証局秘密鍵を非アクティブにする方法	29
6.2.7	認証局秘密鍵の破棄	29
6.3	ネットワークセキュリティ	29
6.4	暗号化モジュールのセキュリティ	29

7	電子証明書と CRL・ARL のプロファイル	30
7.1	電子証明書のプロファイル	30
7.1.1	電子証明書の様式	30
7.1.2	電子証明書拡張様式	30
7.1.3	認証局鍵識別子 (authorityKeyIdentifier)	30
7.1.4	所有者鍵識別子 (subjectKeyIdentifier)	30
7.1.5	鍵用途 (keyUsage)	30
7.1.6	証明書ポリシー (certificatePolicies)	30
7.1.7	所有者別名 (subjectAltName)	30
7.1.8	発行者別名 (issuerAltName)	30
7.1.9	ポリシーマッピング (policyMappings)	30
7.1.10	基本制約 (basicConstraints)	31
7.1.11	ポリシー制約 (policyConstraints)	31
7.1.12	失効リスト配布点 (cRLDistributionPoints)	31
7.1.13	電子署名方式	31
7.1.14	名前の形式	31
7.1.15	名前の制約	31
7.1.16	発行番号	31
7.1.17	有効期間	31
7.2	CRL・ARL プロファイル	31
7.2.1	CRL・ARL の様式	31
7.2.2	失効に関する情報	31
8	仕様管理	32
8.1	認証業務規程の仕様変更手続き	32
8.1.1	実務上の最新情報とお知らせ	32
8.1.2	修正への同意	32
9	電子証明書詳細プロファイル	33
10	CRL・ARL 詳細プロファイル	41

## 1 はじめに

### 1.1 概要

全国社会保険労務士会連合会（以下「連合会」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全国社会保険労務士会連合会認証サービス（以下「連合会認証サービス」という。）を提供する。

連合会認証サービスは、電子署名法の認定制度における認定を受けた特定認証業務であり、また、政府認証基盤ブリッジ認証局（以下「ブリッジ認証局」という。）と相互認証することにより、民側の申請者と官側の処分権者との間で相互に電子証明書を検証するための認証パスを構築する。

全国社会保険労務士会連合会認証局認証業務規程（以下「認証業務規程」という。）は、連合会が運営する連合会認証サービスの業務に関する規程である。

### 1.2 識別

連合会及び連合会認証サービスに関連するオブジェクト識別子を表 1-1 に示す。

表 1-1 連合会におけるオブジェクト識別子とオブジェクトの内容の対応

オブジェクト識別子	オブジェクトの内容
0.2.440.200129	全国社会保険労務士会連合会
0.2.440.200129.8.5.1.1.0	全国社会保険労務士会連合会認証局相互認証テスト用証明書ポリシー
0.2.440.200129.8.5.1.1.10	全国社会保険労務士会連合会認証局相互認証証明書ポリシー及び全国社会保険労務士会連合会認証局利用者証明書ポリシー

### 1.3 コミュニティと適応性

認証業務規程において、全国社会保険労務士会連合会認証局（以下「連合会認証局」という。）の運営体制と各要素の適応性を定める。

#### 1.3.1 認証業務規程の適用範囲

認証業務規程の適用範囲は、図 1-1 に示す連合会認証局により実施される電子証明書発行業務、失効業務、認証業務の運用に付帯する業務及び業務における各種用語等の定義とする。連合会認証局より社会保険労務士に対して発行する社会保険労務士電子証明書（以下「利用者証明書」という。）、連合会認証局が自らに対して発行する電子証明書（以下「自己署名証明書」という。）、連合会認証局の自己署名証明書の新旧世代のリンクを取るための電子証明書（以下「リンク証明書」という。）、連合会認証局がブリッジ認証局と相互認証を行うための電子証明書（以下「相互認証証明書」という。）及び連合会認証局が発行するその他の電子証明書には、全て認証業務規程を適用する。

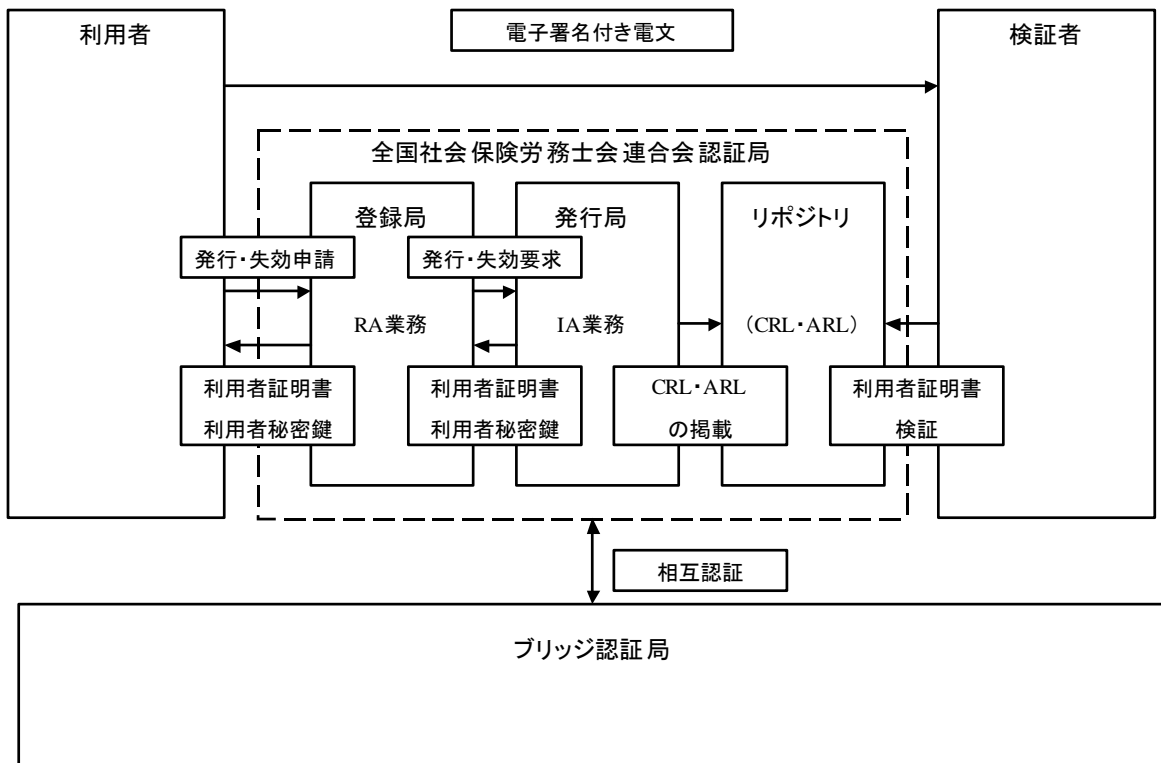


図 1-1 連合会認証局に係るコミュニティ

#### 1.3.2 認証局

連合会認証局は、発行局（以下「IA」という。）、登録局（以下「RA」という。）及びリポジトリをもって構成し、連合会がこれを運用する。連合会は、連合会認証サービスを提供する連合会認証局の運営管理主体であり、その業務を統制、管理する認証業務規程を策定し、これを公開する。連合会認証局は、認証業務規程の遵守を条件に認証業務の一部を外部委託することができる。

#### 1.3.3 発行局 (IA)

IA は、連合会認証局における発行業務を行う。IA は、認証業務規程に従い連合会認証局の秘密鍵（以下「認証局秘密鍵」という。）の生成、管理、廃棄、電子証明書の発行処理、失効処理及び CRL・ARL の発行処理を行う。利用者証明書に関しては、登録局 (RA) からの発行要求及び失効要求に基づ

き、発行処理及び失効処理を行う。また、IA は CRL・ARL を定期的にリポジトリに公開し、リポジトリの管理を行う。

#### 1.3.4 登録局 (RA)

RA は、連合会認証局における登録業務を行う。利用者証明書の発行に関しては、RA は、認証業務規程に従い利用者証明書の発行申請者の真偽及び発行申請者が社会保険労務士法（昭和 43 年 6 月 3 日法律第 89 号）第 2 条に定める事務に従事する社会保険労務士であることを社会保険労務士名簿で確認後、登録用端末設備室の専用の登録用端末から RA サーバへ安全な通信方法を介して利用者証明書の登録申請情報を送信するとともに、認証設備室の専用の登録用端末から RA サーバへ安全な通信方法を介して利用者証明書の発行申請情報を送信し、RA サーバから IA への利用者証明書の発行要求をオンラインで行い、生成された利用者秘密鍵及び利用者証明書等の利用者への送付を行う。利用者証明書の失効に関しては、RA は、認証業務規程に従い利用者証明書の失効申請者の真偽及び失効申請者が失効申請対象の利用者証明書の利用者本人であることを確認後、登録用端末設備室の専用の登録用端末から RA サーバへ安全な通信方法を介して利用者証明書の失効申請情報を送信し、RA サーバから IA サーバへの利用者証明書の失効要求をオンラインで行う。利用者証明書に係る情報の開示に関しては、RA は、認証業務規程に従い開示申請者の真偽及び開示申請者が開示申請対象の利用者証明書の名義人であることを確認後、開示書類の利用者証明書名義人への送付を行う。

#### 1.3.5 利用者

連合会認証局の利用者とは、連合会認証局に利用者証明書の発行申請を行い、利用者証明書を取得し、利用者証明書を利用する主体とし、利用者証明書の中で本人が所有する秘密鍵（以下「利用者秘密鍵」という。）の対となる公開鍵（以下「利用者公開鍵」という。）と氏名の結びつきを証明され、連合会の社会保険労務士名簿に登録された社会保険労務士法第 2 条に定める事務に従事する社会保険労務士であることを証明された者とする。利用者は、全国社会保険労務士会連合会認証サービス利用規約（以下「サービス利用規約」という。）に同意し、認証業務規程の利用者の義務に関する条項を遵守しなければならない。

#### 1.3.6 検証者

連合会認証局の検証者とは、利用者証明書を信頼し利用する者とする。検証者は、認証業務規程の検証者の義務に関する条項を遵守し、認証業務規程の内容について理解し承諾した上で、連合会認証局が発行した電子証明書を利用しなければならない。

#### 1.3.7 リポジトリ

連合会認証局において、連合会認証局が発行した電子証明書の検証に必要な情報の公開はリポジトリにより行う。

#### 1.3.8 利用者証明書の適用範囲

社会保険労務士に対して利用者証明書を発行し、USB メモリに格納して利用者へ送付する。利用者証明書は、利用者である社会保険労務士が、社会保険労務士法第 2 条に定める事務として行政への電子的な申請及び届出、並びに同法同条及び第 19 条に定める事務として保存を行うために使用するものとする。利用者証明書の有効期間は、利用者証明書を有効とする日から起算して 3 年を経過した日の属する月の翌月以降初めての誕生月の 1 日までとする。（当該 3 年を経過した日（以下「3 年経過日」という。）の前に 3 年経過日の属する暦年の誕生月が経過している場合にあっては翌年の誕生月とする。）

#### 1.3.9 電子署名法における属性についての証明

利用者証明書に記載される利用者の属性については、認証業務規程「3.1.2 名前の意味に関する要件」に定める。利用者証明書に記載される事項で電子署名法の認定対象となっているのは、利用者の氏名であり、その他の利用者の属性については、認定対象外である。

#### 1.4 連絡先の詳細

連合会認証サービスの内容については、以下のとおり問い合わせを受付ける。

問い合わせ先 : 全国社会保険労務士会連合会  
所在地 : 〒103-8346 東京都中央区日本橋本石町3丁目2-12 社会保険労務士会館  
代表者 : 全国社会保険労務士会連合会会長  
担当部署 : 全国社会保険労務士会連合会業務部業務課電子情報係  
連絡先住所 : 〒103-8346 東京都中央区日本橋本石町3丁目2-12 社会保険労務士会館  
連絡担当窓口 : 全国社会保険労務士会連合会業務部業務課電子情報係  
TEL : 03(6225)4869  
FAX : 03(6225)4871  
メールアドレス : cainfo@shakaihokenroumushi.jp  
対応時間 : 午前9時30分～午後5時30分  
(正午から午後1時までの休憩時間及び休日(土曜日、日曜日)、祝日、年末年始(12/29～1/3)を除く。)

## 2 一般的な規定

### 2.1 義務

認証業務規程において、連合会認証サービスにおける認証局、IA、RA 及びリポジトリとしての義務並びに利用者及び検証者の義務を定める。

#### 2.1.1 認証局の義務

連合会認証局は、認証業務規程で規定する利用者、検証者及びブリッジ認証局に対して、次の義務を負う。

- (1) 認証業務規程に基づき連合会認証局の運用を行うこと
- (2) 認証局秘密鍵が危殆化（盗難、漏洩等の事由で他人により使用され得る状態になることをいう。以下同じ。）しないように保護すること
- (3) 利用者及び検証者に対し、連合会認証局により発行された利用者証明書に記載される属性には、電子署名法の認定制度における認定の対象外である内容を含むことを表示すること
- (4) 「1.4 連絡先の詳細」に示す対応時間に問い合わせを受付けること
- (5) 連合会が公開するホームページ（以下「連合会ホームページ」という。）で認証業務規程を公開すること
- (6) システム保守による一時停止及び緊急時等の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、連合会認証局が発行した電子証明書の有効期間の間、公開すること
- (7) 定期的に監査を実施し、監査報告に基づき必要と認められた場合は、認証業務に関する改善を行うこと
- (8) 自己署名証明書 (OldWithOld、NewWithNew)、リンク証明書 (OldWithNew、NewWithOld) 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。）を記録し公開すること
- (9) ブリッジ認証局との相互認証申請時に正確な情報を提示すること
- (10) 認証局秘密鍵の危殆化もしくは、その恐れのある場合は、速やかに主務大臣に通報するとともにブリッジ認証局に報告すること

#### 2.1.2 IA の義務

連合会認証局の IA は、認証業務規程で規定する利用者、検証者及び RA に対して、次の義務を負う。

- (1) 認証業務規程に基づき運用を行うこと
- (2) 認証業務規程に従い認証局秘密鍵を生成し、危殆化する恐れのないように管理すること
- (3) RA の要求に従い、利用者証明書発行要求内容を正確に反映した利用者証明書を発行すること
- (4) RA の要求に従い、利用者証明書の失効処理を行うこと
- (5) 認証業務規程に従い、CRL・ARL を発行しリポジトリに登録すること
- (6) IA 業務に関する監査ログ及びアーカイブを、改竄、毀損、滅失及び漏洩のないように保管すること
- (7) 連合会認証局の指示による監査を実施し、監査報告に基づき IA 業務の改善を行うこと

### 2.1.3 RA の義務

連合会認証局の RA は、認証業務規程で規定する利用者、検証者及び IA に対して、次の義務を負う。

- (1) 認証業務規程に基づき運用を行うこと
- (2) 利用者証明書の発行申請を適正に審査し、利用者の真偽確認を確実に行うこと
- (3) 利用者証明書の発行申請の審査後、利用者の鍵ペア（公開鍵と秘密鍵の対のことをいう。以下同じ。）の生成を適切に行い、IA に対して利用者証明書の発行要求を行うこと
- (4) 利用者からの利用者証明書失効申請を適正に審査し、失効請求者の真偽確認を確実に行うこと
- (5) 利用者からの利用者証明書失効申請の審査後、IA に対して利用者証明書の失効要求を行うこと
- (6) 利用者証明書の名義人からの当該利用者証明書に係る情報の開示申請を適正に審査し、開示請求者の真偽確認を確実に行うこと
- (7) 利用者証明書の名義人からの当該利用者証明書に係る情報の開示申請の審査後、当該名義人への開示書類の送付を行うこと
- (8) 利用者から入手した情報で、利用者証明書に記載しない情報は秘密情報として取扱うこと
- (9) RA 業務に関する監査ログ及びアーカイブを、改竄、毀損、滅失及び漏洩のないように保管すること
- (10) 利用者証明書の失効処理を行う事由を連合会認証局において確認した場合は、遅滞なく失効事由の審査を確実にし、IA に失効要求を行うこと
- (11) 連合会認証局の指示による監査を実施し、監査報告に基づいた RA 業務の改善を行うこと
- (12) 利用者秘密鍵及びパスフレーズ（利用者秘密鍵、利用者証明書及び自己署名証明書を暗号化した所定形式（PKCS#12）を活性化するための文字列のことをいう。以下同じ。）の安全な生成及び管理を行い、USB メモリに格納した後、利用者秘密鍵の生成に係る認証設備から、利用者秘密鍵及びパスフレーズ等の利用者秘密鍵に関連する情報を、速やかに完全消去すること
- (13) 利用者秘密鍵、利用者証明書、自己署名証明書及びパスフレーズを格納した USB メモリの安全な配送を行うこと

### 2.1.4 利用者の義務

連合会認証局が発行した利用者証明書を利用者が使用するにあたり、利用者は連合会認証局が提示するサービス利用規約、重要事項説明書及び認証業務規程に同意し、以下の事項について遵守する義務を負う。なお（1）に関連して、虚偽申請を行い、利用者について不実の証明を連合会認証局にさせた者は、電子署名法第 41 条の規定により罰せられる。

- (1) 利用者証明書発行の申請にあたり、社会保険労務士電子証明書発行申請書（以下「発行申請書」という。）の各記入事項につき真実を記載すること
- (2) 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ため、自らの利用者秘密鍵について危殆化しないよう十分注意して扱うこと

- (3) 利用者秘密鍵を安全に管理し、利用者本人以外に使用及び複写させないこと
- (4) 利用者秘密鍵を含む所定形式 (PKCS#12) を活性化するとき求められるパスフレーズ等の情報を利用者本人以外に知られないように安全に管理すること
- (5) 利用者以外の者が利用者秘密鍵の使用及び複写などを行ったことが判明した場合は、直ちに連合会認証局に利用者証明書の失効申請を行うこと
- (6) 利用者秘密鍵に危殆化 (盗難、漏えい等により他人によって使用され得る状態になること) した場合又はその恐れがある場合は、直ちに連合会認証局に利用者証明書の失効申請を行うこと
- (7) 利用者証明書に記載されている事項に関して変更が生じた場合又は利用者証明書の使用を中止する場合は、直ちに連合会認証局に利用者証明書の失効申請を行うこと
- (8) 認証業務規程で規定された利用用途 (1.3.8 利用者証明書の適用範囲参照) 以外の目的で利用者証明書を使用しないこと
- (9) 発行された利用者証明書の記載内容を利用者証明書取得時に確認すること
- (10) 利用者証明書の記載事項に誤りがあることを認識した場合は、直ちに連合会認証局に利用者証明書の失効申請を行うこと
- (11) 認証業務規程に定められた個人情報の取扱い及び利用者証明書への記載範囲の内容について承諾すること
- (12) 電子署名を行う場合のアルゴリズムは、SHA-1withRSA 方式で、鍵長が 1024bit のものを用いること

### 2.1.5 検証者の義務

検証者は、連合会認証局が発行した電子証明書を利用するにあたり、以下の事項を確認する義務を負う。

- (1) 連合会認証局が発行した電子証明書が認証業務規程 (連合会認証局が発行した電子証明書に記載されている公開先より取得) に規定している使用目的及び制限の範囲内で利用されていること
- (2) 自己署名証明書及び必要に応じリンク証明書を確実に入手し、電子署名が行われた情報を検証すること
- (3) 利用者証明書から検証者の信頼する認証局の電子証明書までの認証パスに含まれる全ての電子証明書への電子署名が正しく行われ、改竄されていないこと (当該電子証明書の発行者の電子証明書をを用いた当該電子証明書の検証による)
- (4) 利用者証明書から検証者の信頼する認証局の電子証明書までの認証パスに含まれる全ての電子証明書が有効期間内であること
- (5) 利用者証明書から検証者の信頼する認証局の電子証明書までの認証パスに含まれる全ての電子証明書が失効されていないこと (連合会認証局が発行した電子証明書に関しては、当該電子証明書に記載された CRL・ARL の登録サイトから CRL・ARL を取得することで確認)
- (6) 利用者証明書から検証者の信頼する認証局の電子証明書までの認証パスが有効であること

- (7) 利用者証明書の記載事項のうち、利用者の氏名以外の属性については電子署名法の認定制度における認定の対象外であること
- (8) 入手した自己署名証明書及び必要に応じ入手したリンク証明書から生成したハッシュ値と連合会認証局が連合会ホームページ上でSSLを介して公開するフィンガープリントとが一致すること

### 2.1.6 リポジトリの義務

連合会認証局のリポジトリは、認証業務規程で規定する利用者及び検証者に対して次の義務を負う。

- (1) 認証業務規程に基づき運用を行うこと
- (2) 連合会認証局のリポジトリの保守による一時的な停止又は災害や障害等のやむを得ない場合の停止を除き、検証者が連合会認証局の発行した電子証明書の有効性を検証できるようにCRL・ARLを定期的に更新し、常時公開すること
- (3) 連合会認証サービスに関する情報を認証業務規程の「2.7 公開とリポジトリ」に従い公開すること
- (4) 連合会認証局のリポジトリを改竄されないよう不正アクセスの防止措置を行うこと

## 2.2 責任

### 2.2.1 認証局の責任

連合会認証局は、認証業務規程に従い連合会認証サービスを提供する。また、認証局秘密鍵を適切に運用管理し、連合会認証局が発行する電子証明書の信頼性を確保する。

### 2.2.2 IAの責任

IAは、認証業務規程に従い運用し、RAの要求等に基づき電子証明書の発行及び失効を適切に行い連合会認証局が発行する電子証明書に係る情報の信頼性を確保する。

### 2.2.3 RAの責任

RAは、認証業務規程に従い、利用者の真偽確認及び利用者の鍵ペアの生成を適切に行い、IAに対して電子証明書の発行及び失効の適切な要求を行うとともに、提供された利用者の個人情報の適切な保護を行う。

### 2.2.4 利用者の責任

利用者は、認証業務規程に従い連合会認証サービスを利用する。

### 2.2.5 検証者の責任

検証者は、認証業務規程に従い利用者証明書を検証する。

### 2.2.6 リポジトリの責任

リポジトリは、認証業務規程に従い、連合会認証局が発行した電子証明書の有効性を検証するために必要な情報の公開を適切に行う。

## 2.3 財務上の責任

連合会は、連合会認証局の運営を維持し、かつその義務を履行するために十分な財政的基盤を確保する。

### 2.3.1 損害賠償

認証業務規程において、連合会認証サービスに係る損害賠償要件発生時の対応について、以下のとおり定める。

- (1) 連合会認証局が認証業務規程「2.2.1 認証局の責任」に定める責任に違反して損害賠償責任

を負う場合は、1,000,000円を上限とする。いかなる場合においてもこの賠償額の上限を超える請求には応じない。ただし、連合会認証局の責任に帰することができない事由から生じた損害、連合会認証局の予見の有無を問わず特別の事情から生じた損害についての賠償責任は負わない。

- (2) 利用者が、認証業務規程に定める義務を履行しないこと又は認証業務規程の「2.2.4 利用者の責任」に定める責任に違反したことにより、連合会認証局が損害を被った場合は、連合会認証局は利用者に対し、当該損害の賠償を請求することができる。
- (3) 利用者が、認証業務規程で定める利用者証明書の用途以外に利用者証明書を使用した結果生じた障害については、利用者が一切の責任を負うものとし、当該障害により連合会認証局が損害を被った場合は、利用者は連合会認証局に対して当該損害を賠償する。
- (4) 利用者が、認証業務規程の「2.1.4 利用者の義務」に定める失効申請において、利用者が失効申請の義務を怠ったことにより生じた第三者によるなりすまし及び検証者の誤った判断等の障害により連合会認証局が損害を被った場合は、利用者は連合会認証局に対して当該損害を賠償する。
- (5) 利用者による電子証明書の使用にあたり利用者自身のシステムに起因するあらゆる損失、損害又は費用に関しては、連合会認証局は免責される。
- (6) 利用者秘密鍵の危殆化に起因するあらゆる損失、損害又は費用について、連合会認証局は免責される。
- (7) 検証者が提示された電子証明書の有効性の確認を行わずに電子証明書を使用した結果被った損害については、連合会認証局は何ら賠償責任を負わない。
- (8) 連合会認証局は、郵便事業株式会社の提供する郵便の役務における事故により生じた損害について責任を負わない。
- (9) 連合会認証局は、以下の事由による連合会認証サービスの停止により利用者あるいは検証者が損害を受けた場合は、一切賠償責任を負わない。
  - ・ 地震、水害、噴火、津波等の天災
  - ・ 火災、停電等
  - ・ 戦争、動乱、騒乱、暴動、労働争議等
  - ・ その他連合会認証局が技術的あるいは運用上緊急に連合会認証サービスを停止する必要があると判断した場合

## 2.4 人事管理と事務取扱要領などの規程

### 2.4.1 独立性、第三者性

連合会認証局は、認証局秘密鍵の運用管理、連合会認証サービスの電子証明書発行及び失効の運用管理等、連合会認証局の業務の一部を信頼性のある第三者に委託することができる。連合会認証局が認証業務の一部を委託した場合は、委託先は認証業務規程を遵守して業務を行う。

### 2.4.2 専門性

連合会認証局は、認証業務規程に従い、認証局としての信頼性を維持するため、専門性を持つ要員によりRA、IA及びリポジトリを構築し、運用する。

### 2.4.3 組織体制

連合会認証局は、認証業務規程に従い、認証局としての信頼性を維持するため、必要な組織体制を構築し、運用する。

#### 2.4.4 人事管理

連合会認証局は、認証業務規程に従い、認証局としての信頼性を維持するため、必要な人事管理を行う。

#### 2.4.5 事務取扱要領等の規程

連合会認証局は、認証業務規程に従い、認証局としての信頼性を維持するため、必要に応じ認証業務に関する全国社会保険労務士会連合会認証局事務取扱要領（以下「事務取扱要領」という。）等の内部規程を定める。認証業務規程の改訂を行う場合は、必要に応じ事務取扱要領等の内部規程を速やかに改訂する。なお、事務取扱要領等の内部規程は非公開とする。

### 2.5 解釈及び執行

#### 2.5.1 準拠法

当事者間の契約又は他の準拠法を選択する旨の規定の有無に係らず、認証業務規程の解釈及び有効性等は日本国内法により判断される。連合会認証局と関係者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によるものとする。

#### 2.5.2 認証業務規程の可分性

連合会認証局の認証業務規程等の一部の規定又はその適用が、何らかの理由により、また、いかなる程度でも、無効又は執行不可能であるとされた場合においても、連合会認証局の認証業務規程等のその他の部分の規定は有効とする。

#### 2.5.3 効力の存続

連合会認証局が、連合会認証サービスを廃止もしくは終了した場合においても認証業務規程の「2.9 秘密情報」の効力は持続する。

#### 2.5.4 認証業務規程の完全性

連合会認証局の権利義務に直接影響する認証業務規程の規定は、認証業務規程に別段の定めがある場合を除いて、口頭で修正、放棄、追加、変更又は終了することができない。

#### 2.5.5 連絡

利用者及び検証者が、認証業務規程に対して何らかの通知、請求及び依頼をする場合の連絡は、文書で行うものとする。

#### 2.5.6 紛争解決手続き

全ての当事者は、認証業務規程又は連合会認証局が発行した電子証明書に関して生じた紛争についての専属的合意管轄裁判所を東京地方裁判所とすることで合意するものとする。認証業務規程及び契約書に定められていない事項やこれらの文書の解釈に関して疑義が生じた場合は、各当事者はその課題を解決するために誠意を持って協議するものとする。

### 2.6 料金

連合会認証サービスに係る利用者が負担する料金、利用者証明書の有効期間及びその支払い方法は、連合会ホームページ上の料金表に提示する。利用者は提示された支払い方法に従い提示された料金を支払わなければならない。一度支払われた料金は、発行申請が不承認となった場合を除いていかなる理由があっても一切払い戻ししない。

### 2.7 公開とリポジトリ

#### 2.7.1 認証局の情報の公開

連合会認証局が公開する情報を以下に定める。

##### (1) 連合会認証局のリポジトリ上での公開

連合会認証局は、次の情報を複製し、連合会認証局のリポジトリに渡し、LDAP (Lightweight Directory Access Protocol) を介して公開する。LDAP の使用については、政府認証基盤相互

運用性仕様書に従っている。

- ・ 自己署名証明書 (属性名: cACertificate)
- ・ リンク証明書 (属性名: cACertificate)
- ・ 相互認証証明書 (属性名: crossCertificatePair)
- ・ CRL (属性名: certificateRevocationList)
- ・ ARL (属性名: authorityRevocationList)

本認証業務の場合、上位認証局からの認証を受けていない為、属性名が cACertificate の電子証明書に関しては、認証局鍵識別子と所有者鍵識別子が同じ場合が自己署名証明書、異なる場合がリンク証明書となる。これらの情報を公開する連合会認証局のリポジトリの URI は、以下の通りである。

<ldap://repository.shakaihokenroumushi.jp/ou=All%20Japan%20Federation%20of%20Shakaihokenroumushi%20Associations%20CA,o=AJFCSILCA,c=JP>

また、連合会認証局はフィンガープリントをリポジトリより SSL を介して公開する。リポジトリにおいては、公開するフィンガープリントの改竄防止措置を行っている。フィンガープリントを公開する連合会認証局のリポジトリの URI は、以下の通りである。

<https://repository.shakaihokenroumushi.jp/fingerprint.html>

## (2) 連合会ホームページ上での公開

連合会認証局は、次の情報を連合会ホームページ上で公開する。

- ・ 認証業務規程
- ・ 連合会認証サービスに関する重要な公開情報

これらの情報を公開する連合会ホームページの URI は、以下の通りである。

<http://www.shakaihokenroumushi.jp/>

### 2.7.2 公開の頻度

認証業務規程に関しては、「8 仕様管理」に従い変更履歴を含む最新の認証業務規程を連合会ホームページを通じて公開する。

CRL・ARL は 24 時間ごとに IA から発行し、リポジトリに登録する。

その他連合会認証サービスに関する情報は、連合会の判断で連合会ホームページを通じて適宜公開する。

### 2.7.3 アクセスコントロール

連合会認証局は、公開可能な連合会認証サービスに関する情報について、連合会ホームページを通じて公開する。利用者及び検証者は、連合会認証局が発行した電子証明書に関する公開情報を、リポジトリを通じて入手することができる。ただし、利用者及び検証者は、これらに修正を加えてはならない。

### 2.7.4 リポジトリ

リポジトリ及び連合会ホームページは 1 日 24 時間、1 週 7 日間運用する。ただし、システムの保守などの場合は、連合会認証局は、利用者及び検証者に予め通知し、リポジトリ及び連合会ホームページを一時停止することができる。なお、緊急時等やむを得ない場合は、この規定を適用しない。

## 2.8 準拠性監査

### 2.8.1 準拠性監査の頻度

連合会認証局は、監査基準を定め、それによって年に一回以上の定期監査を実施する。また、必要に応じて、不定期な監査を実施する。

### 2.8.2 監査人の任命

監査人には、準拠性監査において十分な知識を持った者を任命する。

### 2.8.3 監査人の監査される主体との関係

監査人は、連合会認証局の認証業務に係る要員以外から選定する。

#### 2.8.4 監査テーマ

監査は、連合会認証局が運営する全ての認証業務及び設備を対象とする。当該認証業務の一部を外部に委託する場合は、その委託先の委託業務及び委託先の設備を含む。定期監査では、連合会認証局が運営する IA、RA 及びリポジトリが、認証業務規程、認証業務規程に基づいた事務取扱要領及び事務取扱要領以下の規程類を遵守して運営されているかを監査する。主な監査項目は、以下のとおりとする。

- ・ IA、RA 及びリポジトリの運用業務
- ・ 連合会認証局が発行した電子証明書のライフサイクル管理
- ・ 認証局秘密鍵の管理
- ・ ソフトウェア、ハードウェア及びネットワーク
- ・ 物理的環境及び設備

#### 2.8.5 監査指摘事項への措置

連合会認証局は、監査報告書での指摘事項及びセキュリティ対策技術の最新の動向を踏まえ、業務及び設備の見直しを含む対策を講じ、必要な場合には、認証業務規程を改訂する。

#### 2.8.6 監査結果の公開

連合会認証局は、監査結果をブリッジ認証局へ報告することを除き、その他外部への公開もしくは開示を行わない。ただし、指定調査機関からの監査結果の開示要求があった場合及び公的機関などから法律に基づく開示要求があった場合は、その指示に従いこれを開示する。

### 2.9 秘密情報

連合会認証サービスの業務を通じて知り得る連合会認証局のシステム、ネットワーク及び詳細な認証手順などの公開されない秘密情報に関しては、連合会認証局は連合会認証局の定める規定に従い、その内容を連合会認証局の業務に係る要員の役割に応じて理解される限度に維持されるよう措置を講じることとする。

#### 2.9.1 秘密情報の種類

連合会認証局は、「2.9.7 秘密情報として取扱わない情報」に掲げる情報を除く次に掲げる情報等を秘密情報として取扱い、第三者に開示、漏洩しないとともに、連合会認証サービスを提供するために必要な範囲を越えて使用しない。

- ・ 申請に係る情報（連合会認証局が発行した電子証明書または CRL・ARL に記載された情報、認証業務規程に規定する情報及び公開情報に記載された情報を除く。）
- ・ 連合会認証局が発行した電子証明書の発行申請記録、失効申請記録及び開示申請記録（連合会認証局が発行した電子証明書または CRL・ARL に記載された情報を除く。）
- ・ トランザクションの記録（記録全て及びトランザクションの監査証跡）（連合会認証局が発行した電子証明書または CRL・ARL に記載された情報及び公開情報に記載された情報を除く。）
- ・ 連合会認証局が作成又は保管する監査証跡の記録（連合会認証局が発行した電子証明書または CRL・ARL に記載された情報及び公開情報に記載された情報を除く。）
- ・ 監査人が作成する監査報告書
- ・ 不測の事態に対応する計画及び災害時における回復措置（認証業務規程に規定する情報及び公開情報に記載された情報を除く。）
- ・ ハードウェア及びソフトウェアの運用並びに連合会認証局の運営についてのセキュリティ対策（認証業務規程に規定する情報及び公開情報に記載された情報を除く。）
- ・ 業務手順を記述した書類とその変更に関する記録（認証業務規程に規定する情報及び公開情報に記載された情報を除く。）
- ・ 業務に従事する者の組織、体制、責任及び権限並びに指揮命令系統に関する書類（認証業務規程に規定する情報及び公開情報に記載された情報を除く。）
- ・ 連合会認証サービスの業務に関する記録（連合会認証局が発行した電子証明書または CRL・ARL に記載された情報、認証業務規程に規定する情報及び公開情報に記載された情報を除く。）

## 2.9.2 個人情報の取扱い

連合会認証局は、利用者証明書の発行申請時に発行申請者から提供される情報、利用者証明書の失効申請時に失効申請者から提供される情報及び開示申請時に開示申請者から提供される情報を個人情報として扱い、またその収集を連合会認証サービスを提供するために必要な範囲を越えて行なわず、利用しない。また、その取扱いと保護については以下に従い、連合会認証局の認証業務に係る全ての要員に、それぞれの役割に応じた教育・訓練計画を策定し、それに則って教育訓練を実施する。

### (1) 個人情報の位置付け

連合会認証局が、利用者証明書発行申請、失効申請及び開示申請にあたって利用者から提供された全ての情報及び連合会認証局が利用者以外から提供された利用者に係る情報は、個人情報として扱う。連合会認証局は、利用者証明書の発行申請、失効申請及び開示申請時に提出された申請書類の原本を返還しない。

利用者から提供された個人情報は以下のものを意味する。

- ・ 利用者からの利用者証明書の発行申請、失効申請及び開示申請に関して提出された申請書及び申請書に添付された書類の記載情報

連合会認証局が利用者以外から提供を受けた利用者に係る個人情報は以下のものを意味する。

- ・ 社会保険労務士名簿に記載された利用者に関する情報

### (2) 使用目的の特定

連合会認証サービスを利用者に提供するために必要な個人情報を連合会認証サービスの提供の目的のみに利用する。また、連合会認証サービスの目的と相当の関連性を有すると合理的に認められる範囲を越えて、個人情報の利用は行わない。

### (3) 使用目的による制限

前項の目的以外に個人情報を使用しない。また、第三者から目的外利用を求められた場合は、法令に定められた場合を除き、一切これに応じない。

### (4) 適正な取得

不正な手段により個人情報を取得しない。

### (5) 取得に際しての使用目的の通知

利用者証明書の発行申請、失効申請及び開示申請における個人情報の取得に際しては、使用目的を認証業務規程「2.9.6 利用者証明書名義人の要請に基づく開示」、「3.1 初期登録（発行申請）」及び「3.4 利用者証明書の失効申請」に記載し、公開する。

### (6) 安全管理措置及び要員、委託先の監督

利用者から取得した個人情報に対して、情報を取扱う要員及び委託先の監督も含め、施錠された場所に保管し、許可された者以外がアクセスできないよう措置する等、その改竄、漏洩、滅失及び毀損の防止措置を講ずる。

### (7) 保有個人情報に関する事項の公開

個人情報の使用目的及び開示等について、認証業務規程「2.9.2 個人情報の取扱い」、「2.9.4 法執行機関への情報開示」、「2.9.5 民事手続き上の開示」及び「2.9.6 利用者証明書名義人の要請に基づく開示」の規定に従い公開する。

### (8) 開示

利用者証明書の名義人から申し出があった場合は、認証業務規程の規定に従い利用者本人の個人情報の開示請求を受付ける。ただし、他の法令に別段の定めがある場合はこの限りでない。

## 2.9.3 電子証明書の失効情報の公開

連合会認証局は、失効した電子証明書に関して、リポジトリにおいてCRL・ARLを公開する。CRL・ARLに含まれる情報は秘密情報として取扱わず、全ての検証者に公開する。その他の失効に関する詳

細な情報は、秘密情報とし、開示しない。

#### 2.9.4 法執行機関への情報開示

連合会認証局は、捜査機関、裁判所、その他法律上権限を有するものから強制力を伴う照会があった場合は、法令に従い法執行機関へ利用者に関して保有している秘密情報を開示することができる。

#### 2.9.5 民事手続き上の開示

連合会認証局は、調停、起訴、その他の法的、裁判上又は行政手続きの過程において、秘密情報を開示することができる。

#### 2.9.6 利用者証明書名義人の要請に基づく開示

連合会認証局は、利用者証明書の名義人から権利、利益を侵害又は侵害される恐れがあるとの申し出を受けた場合は、当該申請者が利用者証明書の名義人であることを確認し、開示申請者に対し以下の書類を開示する。

- ・ 利用者証明書に係る発行申請書及び利用者の真偽確認のために提供を受けた書類
- ・ 利用者証明書の記載事項

開示の申請において、開示申請者は、必要事項を記入し印鑑登録済みの印鑑（以下「実印」という。）を押印した社会保険労務士電子証明書発行申請書類開示申請書（以下「開示申請書」という。）及び押印した印に係る開示申請書郵送用封筒に押印された消印の日もしくは手交受取日から3か月以内に発行された印鑑登録証明書を、簡易書留もしくは特定記録郵便による郵送又は窓口への持参により提出する。また、利用者証明書発行申請時から住所もしくは氏名に変更があり提出された書類によって発行申請時の情報が確認できない場合は、住所については発行申請時の住所が記載された住民票の写し又は住民票に記載をした事項に関する証明書（以下「住民票の写し等」という。）、登録原票の写し又は登録原票に登録した事項に関する証明書（以下「登録原票記載事項証明書等」という。）又は戸籍の附票の写しを提出し、氏名については発行申請時の氏名が記載された戸籍謄本又は全部事項証明書もしくは戸籍抄本又は個人事項証明書（以下「全部／個人事項証明書」という）又は登録原票記載事項証明書等を提出する。開示申請者の真偽確認は、開示申請者から受理した開示申請書に記載されている内容と利用者証明書発行申請時の発行申請書に記載されている内容（住所・氏名・生年月日・社会保険労務士登録番号（以下「登録番号」という。））の一致の確認と開示申請書に押印された印とその印鑑に係る印鑑登録証明書との照合により行う。本人確認の結果、承認と判断された場合は、開示資料の写しに社会保険労務士電子証明書発行申請書類開示申請承認通知書を同封し、開示申請書記載の住所に、電子署名法施行規則第5条第1項第3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（基本型）」（以下「本人限定受取郵便」という。）で送付することにより開示する。

#### 2.9.7 秘密情報として取扱わない情報

連合会認証局は、以下の情報を秘密情報として取扱わない。

- ・ 連合会認証局が発行した電子証明書またはCRL・ARLに記載された情報
- ・ 認証業務規程に規定する情報
- ・ 公開情報に記載された情報

#### 2.10 知的財産権

連合会認証局は、以下の情報資料及びデータを、別段の合意のなされない限り連合会認証局に帰属する知的財産として取扱う。

- ・ 連合会認証局が発行した電子証明書
- ・ 認証業務規程
- ・ 認証局秘密鍵及び連合会認証局の公開鍵（以下「認証局公開鍵」という。）

### 3 識別と本人確認

#### 3.1 初期登録（発行申請）

利用者証明書の発行申請の手続きは、認証業務規程に規定する。RAは、利用者の真偽確認を適切に

行わなければならない。なお、利用者が申込みできるのは、唯一の所有者名を持つ利用者証明書のみとし、利用者証明書の有効期間満了の前5ヶ月の更新期間を除いて、1枚のみとする。

### 3.1.1 名前の型

連合会認証局が発行する電子証明書の発行者名 (Issuer) 及び所有者名 (Subject) は、ITU X.500 識別名 (DN:Distinguished Name) の形式に従い設定する。

### 3.1.2 名前の意味に関する要件

利用者証明書に記載する名称 (DN) には、RA が利用者の真偽確認の際に利用者から提出される発行申請書及び添付書類に記載されている内容と社会保険労務士名簿に記載されている情報を含める。

利用者証明書に記載する利用者情報の識別名と連合会認証局での取扱いについては以下のとおりとする。(9. 電子証明書詳細プロファイル参照)

#### (1) 基本領域

- ・ 国名 (Country Name)

利用者の居住する国名とし、“JP” (日本国) で固定する。

- ・ 組織名 (Organization)

Issuer、Subject とも、連合会認証局の運用組織である連合会の英語表記の略称、“AJFCSILCA” で固定する。なお、組織名の証明は電子署名法の認定制度における認定の対象外である。

- ・ 組織単位名 (Organizational Unit)

利用者の所属する社会保険労務士会の都道府県名のローマ字表記を設定する。なお、組織単位名の証明は電子署名法の認定制度における認定の対象外である。

- ・ 一般名 (Common Name)

連合会認証局の運用組織である連合会の英語表記の略称、“AJFCSILCA”、発行申請書に記入されている利用者氏名の日本語呼称のローマ字表記、登録番号 (8 桁の数字) 及び利用者の社会保険労務士会員種別 (1: 開業、2: 社員、3: 勤務 (社会保険労務士法人・開業社会保険労務士の使用人)、0: 勤務) を 1 桁めに示した付加情報に対応するコード (8 桁の英数字) を “AJFCSILCA, 付加情報, 利用者氏名, 登録番号” の形式で設定する。

また、旧姓もしくは外国人登録法 (昭和 27 年法律第 125 号) 第 4 条の 3 に規定する登録原票記載事項証明書等に記載されている通称名を併記する場合には、利用者氏名の後ろに括弧で括って記載し、“AJFCSILCA, 付加情報, 利用者氏名 (旧姓もしくは通称名), 登録番号” の形式で設定する。なお、連合会の英語表記の略称、登録番号及び付加情報の証明は電子署名法の認定制度における認定の対象外である。

#### (2) 拡張領域

- ・ 国名 (Country Name)

利用者の居住する国名とし、“JP” (日本国) で固定する。

- ・ 組織名 (Organization)

連合会認証局の運用組織である、“全国社会保険労務士会連合会” で固定する。なお、組織名の証明は電子署名法の認定制度における認定の対象外である。

- ・ 組織単位名① (Organizational Unit)

利用者の所属する社会保険労務士会の都道府県名を設定する。なお、組織単位名の証明は電子署名法の認定制度における認定の対象外である。

- ・ 組織単位名② (Organizational Unit)

利用者の事務所名、法人名もしくは事業所名を設定する。なお、組織単位名の証明は電子署名法の認定制度における認定の対象外である。

なお、利用者の事務所名、法人名もしくは事業所名については、社会保険労務士名簿から利用者証明書に転載する。

また、利用者の事務所名、法人名もしくは事業所名が 21 文字を超える場合は一部省略した名称

とする。

- 一般名 (Common Name)

利用者の社会保険労務士会員種別（1：開業、2：社員、3：勤務（社会保険労務士法人・開業社会保険労務士の使用人）、0：勤務）を1桁めに示した付加情報に対応するコード（8桁の英数字）、発行申請書に記入されている利用者氏名の日本語呼称の日本語表記及び登録番号（8桁の数字）を“付加情報,利用者氏名,登録番号”の形式で設定する。

また、旧姓もしくは登録原票記載事項証明書等に記載されている通称名を併記する場合には、利用者氏名の後ろに括弧で括って記載し、“付加情報,利用者氏名(旧姓もしくは通称名),登録番号”の形式で設定する。なお、登録番号及び付加情報の証明は電子署名法の認定制度における認定の対象外である。

### 3.1.3 名前形式を解釈するための規則

名前形式の解釈は、ITU X.500 識別名 (DN: Distinguished Name) の規定に従う。

### 3.1.4 名前の一意性

利用者証明書に記載する名称 (DN) は、連合会認証局が発行した利用者証明書において利用者毎に一意に割り当てる。

### 3.1.5 名前に関する紛争の解決手段

名前に関する紛争は、利用者証明書に記載する利用者の識別名に係る、不正発行、商標権侵害、不正競争、不正目的利用等の紛争を意味する。利用者証明書に記載する利用者の識別名に係る紛争は、連合会認証局と利用者間での解決を原則とする。

### 3.1.6 商標の認識・認証・役割

商標は、連合会認証局が発行する利用者証明書に記載する利用者の識別名に含めない。

### 3.1.7 秘密鍵の所有を証明するための方法

連合会認証局は、RA で利用者公開鍵及び利用者秘密鍵を生成し、生成した利用者公開鍵に対して IA から発行する利用者証明書及び利用者秘密鍵を自己署名証明書と合わせて暗号化し、所定形式 (PKCS#12) のファイルを USB メモリに格納し、利用者に本人限定受取郵便を用いて郵送する。このため、利用者が当該利用者秘密鍵を保持することを別途確認しない。

なお、ブリッジ認証局に対する相互認証証明書の発行においては、ブリッジ認証局から送付された電子証明書発行要求の署名検証により、ブリッジ認証局が該当する秘密鍵を保持していることを確認する。

### 3.1.8 本人確認

連合会認証局は、利用者証明書の発行に先立ち、RA において利用者の真偽確認及び申請情報の真正性確認を行う。発行申請書及び添付書類を受理した RA は、利用者の真偽確認を次の手順で行う。

#### (1) 意思確認

- 必要事項が全て記入され利用者の実印の押印のある発行申請書、住民票の写し等もしくは登録原票記載事項証明書等及び発行申請書に押印した印鑑に係る印鑑登録証明書が全て提出されていることを確認する。なお、利用者が利用者証明書において旧姓を使用することを希望する場合は、これらの書類とともに全部／個人事項証明書（旧姓が記載されているもの）が提出されていることを確認する。
- 住民票の写し等もしくは登録原票記載事項証明書等及び印鑑登録証明書に記載されている利用者の住所、氏名及び生年月日が発行申請書に記載されている住所、氏名及び生年月日と同一であること及び住民票の写し等もしくは登録原票記載事項証明書等及び印鑑登録証明書の記載内容及び形式が正しく、公的機関から発行されたことを証明する印が押印されていることを確認する。また、住民票の写し等もしくは登録原票記載事項証明書等及び印鑑登録証明書が、発行申請書郵送用封筒に押印された消印の日もしくは手交受取日か

ら3か月以内のものであることを確認する。なお、利用者が利用者証明書において旧姓を使用することを希望する場合は、全部／個人事項証明書に関しても、記載内容及び形式が正しく、公的機関から発行されたことを証明する印が押印されていることを確認し、発行申請書郵送用封筒に押印された消印の日もしくは手交受取日から3か月以内のものであることを確認する。

- ・ 発行申請書に利用者の実印が押印されていることを確認する。

(2) 実在性の確認

- ・ 発行申請書に記載されている利用者の住所、氏名及び生年月日が住民票の写し等もしくは登録原票記載事項証明書等に記載されている住所、氏名及び生年月日と同一であることを確認する。ただし、利用者が利用者証明書において旧姓を使用することを希望する場合は、全部／個人事項証明書に記載されている旧姓と同一であることを確認する。また、利用者が利用者証明書において通称名を使用することを希望する場合は、登録原票記載事項証明書等に記載されている通称名と同一であることを確認する。

(3) 本人確認

- ・ 発行申請書に押印されている実印の印影と提出された印鑑登録証明書の印影とを照合し、同じであることを確認する。

(4) 社会保険労務士法第2条に定める事務に従事する社会保険労務士であることの確認

- ・ 発行申請書に記入されている氏名、生年月日及び登録番号が社会保険労務士名簿の記載内容と合致し、社会保険労務士名簿に社会保険労務士法第2条に定める事務に従事する社会保険労務士であることが記載されていること、利用者が社会保険労務士名簿から抹消されていないこと及び利用者が社会保険労務士業務の禁止等の処分を受けていないことを確認する。

以上の審査において全ての確認が正しく検証できた場合を真偽確認が真であるとし、いずれかの確認において異常が検出された場合を真偽確認が偽であるとする。もし、審査過程において、提出書類の不備や記載内容の不備などにより疑義が生じた場合は、連合会認証局は、利用者に真偽確認ができなかった理由を通知し、必要書類の再提出を要請する。

なお、連合会認証局は、利用者氏名の読み方（フリガナ）については、住民票の写し等もしくは登録原票記載事項証明書等に記載されている氏名から通常導きうる読み方の範囲を限度として真偽確認を行う。連合会認証局は、これらを超える真偽確認の義務を負わない。

### 3.2 利用者証明書の更新

連合会認証局は、利用者証明書の更新に関する審査を新規発行時と同様に「3.1 初期登録（発行申請）」乃至「3.1.8 本人確認」において定める手続きに基づき行う。

### 3.3 利用者証明書失効後の再発行

連合会認証局は、利用者証明書失効後の再発行に対する審査を新規発行時と同様に「3.1 初期登録（発行申請）」乃至「3.1.8 本人確認」において定める手続きに基づき行う。

### 3.4 利用者証明書の失効申請

#### 3.4.1 失効申請者の真偽確認

連合会認証局は、利用者本人から社会保険労務士電子証明書失効申請書（以下「失効申請書」という。）及び失効申請書に押印した印鑑に係る印鑑登録証明書の提出を受け、失効申請書に記載されている内容と利用者証明書発行申請時の発行申請書に記載されている内容（住所・氏名・生年月日・登録番号）が一致し、失効申請書に押印されている印影が失効申請書とともに提出された印鑑登録証明書の印影と一致する場合に、利用者本人からの申請であると判断する。

なお、発行申請時と住所又は氏名が異なる場合は、全部／個人事項証明書又は登録原票記載事項証明書又は戸籍の附票の写しに記載された以前の住所を確認し一致する場合に、利用者本人からの申請

であると判断する。

## 4 運用上の要件

### 4.1 電子証明書発行申請

認証業務規程において、利用者からの利用者証明書発行申請の手続きについて定める。

なお、ブリッジ認証局からの相互認証証明書の発行申請の受付及びブリッジ認証局への相互認証証明書の発行申請は、ブリッジ認証局の定める手続きに従い実施する。

#### 4.1.1 利用者による申請

利用者証明書の発行申請をする利用者は、連合会ホームページにおいて発行申請書とともに公開されている認証業務規程、サービス利用規約及び重要事項説明書を入手するか、発行申請書、認証業務規程、サービス利用規約及び重要事項説明書を窓口へ出向いて受取るか郵送によって取寄せるか、連合会認証局発行物に含まれる発行申請書、認証業務規程、サービス利用規約及び重要事項説明書を用いて、内容を確認した上で同意するとともに、重要事項説明書における説明に従い個人情報を取扱うこと及び発行申請書の記載事項の一部が利用者証明書に記載されることに同意することを要する。連合会認証局は、発行申請書への実印の押印をもって、認証業務規程、重要事項説明書及びサービス利用規約を理解した上で同意したものとみなす。連合会認証局は、簡易書留もしくは特定記録郵便による郵送又は窓口への持参による利用者からの申請を受け、これ以外の方式による申請は受け付けない。

連合会認証局は、利用者から委託された代理人による申請を受け付けない。また、利用者により、記載内容を訂正する場合には、該当箇所を修正の上、実印による押印を行う。

#### 4.1.2 発行申請書類

利用者は、次の申請書類を連合会認証局に提出しなければならない。

##### (1) 発行申請書

利用者は、発行申請書に実印を押印しなければならない。発行申請書に押印された実印の印影は、発行申請書に添付された印鑑登録証明書に証明されている印影と一致しなければならない。

発行申請書は、以下の記載事項を含む様式とする。

- ・ 申請年月日
- ・ 利用者の氏名
- ・ 利用者氏名のローマ字表記
- ・ 利用者証明書記載用の利用者の氏名
- ・ 利用者の住所
- ・ 利用者の生年月日
- ・ 利用者証明書の用途
- ・ 社会保険労務士登録番号
- ・ 利用者の連絡先
- ・ 利用者の実印の押印

利用者証明書記載する「利用者氏名のローマ字表記」は、旅券法施行規則第5条第2項の所定の形式に従いへボン式ローマ字で本人の氏名（フリガナ）を記述する。

発行申請書の「利用者証明書記載用の利用者の氏名」の欄には、氏名、旧姓又は通称名の記入欄が用意されており、以下のいずれかに該当する場合にのみ記述する。

##### (i) 利用者証明書記載用の旧姓を記載する場合（日本国籍を持つ場合）

本人確認において、住民票の写し等に記載された氏名と全部／個人事項証明書記載された氏名の両方を確認するため、「利用者の氏名」に住民票の写し等に記載された氏名を記述し、「利用者証明書記載用の利用者の氏名」に全部／個人事項証明書記載された旧姓を含んだ氏名を記述する。なお、旧姓が(ii)に相当する場合は、「利用者証明書記載用の利用者の氏名」には旧姓を含んだ氏名を、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）（以下「誤字俗字・正字一覧表」という。）に従い置き換えた略字を用いて記述する。

##### (ii) 氏名に、旧字体等の理由から電子証明書記載することができない漢字がある場合

All rights reserved Copyright(C) 2010 全国社会保険労務士会連合会

本人確認用に「利用者の氏名」に住民票の写し等もしくは登録原票記載事項証明書等に記載された氏名を記述し、「利用者証明書記載用の利用者の氏名」に誤字俗字・正字一覧表に従い置き換えた略字を用いた氏名を記述する。

(iii) 利用者証明書に通称名を記載する場合（外国人の場合）

本人確認において、登録原票記載事項証明書等に記載された本名と通称名の両方を確認するため、「利用者の氏名」に登録原票記載事項証明書等に記載された本名を記述し、「利用者証明書記載用の利用者の氏名」に登録原票記載事項証明書等に記載された通称名を記述する。なお、通称名が (ii) に相当する場合は、「利用者証明書記載用の利用者氏名」には通称名を、誤字俗字・正字一覧表に従い置き換えた略字を用いて記述する。

(2) 住民票の写し等又は登録原票記載事項証明書等

住民票の写し等は、利用者の実在性を証明する書類として取扱う。日本国籍をもたない者については、登録原票記載事項証明書等をもってこれに代える。住民票の写し等及び登録原票記載事項証明書等は、発行申請書郵送用封筒に押印された消印の日もしくは手交受取日から3か月以内のものでなければならない。

(3) 印鑑登録証明書

発行申請書に押印した印鑑に係る印鑑登録証明書は利用者の真偽確認を行う書類として取扱う。当該印鑑登録証明書は、発行申請書郵送用封筒に押印された消印の日もしくは手交受取日から3か月以内のものでなければならない。

(4) 全部／個人事項証明書（旧姓が記載されているもの）

利用者が利用者証明書において旧姓を使用することを希望する場合は、全部／個人事項証明書を利用者の旧姓を証明する書類として取扱う。全部／個人事項証明書は、発行申請書郵送用封筒に押印された消印の日もしくは手交受取日から3か月以内のものでなければならない。

4.1.3 代理人による申請

連合会認証局は、利用者から委託された代理人による申請を受付けない。

4.1.4 利用者本人による申請の審査

RA は、複数人の管理のもと認証業務規程「3.1.8 本人確認」に従い利用者の真偽確認及び社会保険労務士法第2条に定める事務に従事する社会保険労務士であることの確認を行った後、不備がなければ、利用者証明書発行申請登録を行う。

4.1.5 申請の登録

RA は、利用者証明書記載情報を登録用端末より RA サーバに送信することで登録を行う。当該登録データは暗号化して送信する。

4.2 電子証明書の発行

RA は、複数人による相互牽制下で、認証設備室内の登録用端末より RA サーバに利用者証明書の発行申請を行う。RA サーバにおいては、利用者の鍵ペアを生成し、IA サーバに利用者証明書の発行要求を送信した後、IA サーバが発行した利用者証明書を利用者秘密鍵及び自己署名証明書とともに暗号化した所定形式 (PKCS#12) のファイルに変換する。この所定形式のファイル及び所定形式のファイルの活性化に必要なパスワードは、USB メモリに格納し本人限定受取郵便を使用して利用者に郵送する。利用者秘密鍵は、生成から利用者証明書の発行までの間、RA サーバ内に保存し、所定形式ファイルの生成後、自動的な処理により完全消去する。

なお、ブリッジ認証局に対する相互認証証明書は、ブリッジ認証局の定める手続きが完了した後、ブリッジ認証局から送付された相互認証証明書発行要求に基づき発行する。

4.3 秘密鍵及び電子証明書の受領

利用者は、利用者秘密鍵、利用者証明書及び自己署名証明書が格納された所定形式のファイル及び

所定形式ファイルの活性化に必要なパスワードが格納されたUSBメモリを受領した後、受領したUSBメモリに利用者秘密鍵と利用者証明書が格納され、利用者証明書の記載内容が正常であることを確認した後、発行申請時に提出した印鑑登録証明書に係る実印を押印した社会保険労務士電子証明書受領確認書（以下、「利用者証明書受領確認書」という。）を郵送もしくは手交により連合会認証局に返信しなければならない。確認結果に問題があった場合は、連合会認証局にその旨を連絡しなければならない。30日以内に利用者証明書受領確認書が郵送もしくは手交により返信されなかった場合は、連合会認証局は当該利用者証明書の失効処理を行う。

なお、ブリッジ認証局に対する相互認証証明書は、ブリッジ認証局の定める手続きに従いブリッジ認証局に渡し、受領書を受取ることにより相互認証証明書の受入れを完了したものとする。

#### 4.4 電子証明書の更新申請

利用者証明書の更新申請は、「4.1 電子証明書発行申請」の規定を準用する。

なお、ブリッジ認証局からの相互認証証明書の更新申請の受付及びブリッジ認証局への相互認証証明書の更新申請は、ブリッジ認証局の定める手続きに従い実施する。

#### 4.5 電子証明書の失効申請

認証業務規程において、連合会認証局が発行した電子証明書の失効申請の手続きについて定める。

##### 4.5.1 失効申請方法

連合会認証局は、簡易書留もしくは特定記録郵便による郵送又は窓口への持参により利用者からの失効申請を受付ける。緊急を要する場合は、FAXによる失効申請を受付けることとし、発行申請書に記載された連絡先に連絡し、利用者の意思確認及び真偽確認を行う。この場合においても利用者は、失効申請書の原本を簡易書留もしくは特定記録郵便による郵送又は窓口への持参により連合会認証局に提出しなければならない。連合会認証局は、これ以外の方式による失効申請を受付けない。

なお、連合会認証局からブリッジ認証局に対する相互認証証明書の失効申請は、認証局責任者が実施し、ブリッジ認証局から連合会認証局に対する失効申請については、ブリッジ認証局の責任者が申請を実施した場合に受付けることとする。

##### 4.5.2 失効申請書類

失効申請をする利用者は、次の申請書類を連合会認証局に提出しなければならない。ただし、発行申請書類も同時に提出する場合に限り、重複する添付書類については提出を不要とする。郵送による申請の場合は、同封されている場合のみ適用できることとする。

###### (1) 失効申請書

利用者は失効申請書に実印を押印しなければならない。

失効申請書は、以下の記載事項欄を含む様式とする。

- ・ 申請年月日
- ・ 申請者（利用者）の氏名
- ・ 申請者（利用者）の氏名のローマ字表記
- ・ 利用者の住所
- ・ 利用者の生年月日
- ・ 社会保険労務士登録番号
- ・ 失効申請の対象となる利用者証明書のシリアル番号
- ・ 発行年月日
- ・ 失効申請事由
- ・ 利用者の実印の押印

###### (2) 印鑑登録証明書

利用者は利用者の真偽証明のために、失効申請書に押印した印鑑に係る印鑑登録証明書を提出しなければならない。印鑑登録証明書は、失効申請書郵送用封筒に押印された消印の日もしくは手交受取日から3か月以内のものでなければならない。

###### (3) 全部／個人事項証明書又は登録原票記載事項証明書等（発行申請時と氏名が異なる場合）

利用者は利用者の真偽証明のために、発行申請時と氏名が異なる場合は発行申請時の氏名が記載された全部／個人事項証明書又は登録原票記載事項証明書等を提出しなければならない。全部／個人事項証明書又は登録原票記載事項証明書等は、失効申請書郵送用封筒に押印された消印の日もしくは手交受取日から3か月以内のものでなければならない。

- (4) 住民票の写し等、登録原票記載事項証明書等又は戸籍の附票の写し（発行申請時と住所が異なる場合）

利用者は利用者の真偽証明のために、発行申請時と住所が異なる場合は発行申請時の住所が記載された住民票の写し等、登録原票記載事項証明書等又は戸籍の附票の写しを提出しなければならない。住民票の写し等、登録原票記載事項証明書等又は戸籍の附票の写しは、失効申請書郵送用封筒に押印された消印の日もしくは手交受取日から3か月以内のものでなければならない。

#### 4.5.3 利用者証明書の失効

利用者は以下に該当する場合は、直ちに連合会認証局に利用者証明書の失効申請を行わなければならない。連合会認証局は、提出された失効申請書と利用者証明書発行申請時の発行申請書に記載されている内容（住所・氏名・生年月日・登録番号）の一致と提出された失効申請書に押印された印影と印鑑登録証明書（発行申請書類も同時に提出する場合は、発行申請書に係る印鑑登録証明書）の印影の一致を確認した後、当該利用者証明書の失効処理を行う。ただし、「4.5.5 認証局による失効」に定める事由が発生した場合は、利用者からの申請を受付けることなく連合会認証局が利用者証明書の失効処理を行う。

- ・ 利用者が利用者証明書の利用を中止する場合
- ・ 利用者の利用者秘密鍵の危殆化、紛失もしくはその恐れのある場合
- ・ 利用者証明書の記載事項が変更された場合
- ・ 利用者証明書記載事項が事実と異なる場合
- ・ 利用者が社会保険労務士でなくなった場合
- ・ 利用者証明書の不正使用もしくは、その恐れのある場合
- ・ その他利用者が失効の必要があると判断した場合

#### 4.5.4 失効申請者への通知

連合会認証局は、利用者証明書の失効処理が完了した後、失効申請者に社会保険労務士電子証明書失効通知書（以下「失効通知書」という。）による失効通知を特定記録郵便による郵送により行う。

#### 4.5.5 認証局による失効

連合会認証局は、利用者からの失効申請の他に、発行した利用者証明書について、以下の項目に該当すると認めた場合は、利用者証明書の有効性が損なわれたと判断し、RA 業務責任者の承認をもって利用者証明書の失効処理を行うことができる。連合会認証局は、当該失効処理が完了した後、利用者に対し失効処理が完了した旨を特定記録郵便による郵送により通知する。

- ・ 連合会認証局を廃止する場合
- ・ 認証局秘密鍵の危殆化もしくは、その恐れのある場合
- ・ 連合会認証局が利用者証明書記載事項の変更があった事実を確認した場合
- ・ 利用者の利用者秘密鍵の危殆化、紛失もしくはその恐れのある場合
- ・ 連合会認証局が利用者証明書送付後 30 日以内に当該利用者の利用者証明書受領確認書を受領しなかった場合
- ・ 利用者が社会保険労務士でなくなった場合
- ・ 利用者が社会保険労務士の業務の停止の処分を受けた場合
- ・ 利用者が会員権の停止の処分を受けた場合
- ・ 利用者証明書の不正使用もしくは、その恐れのある場合
- ・ 利用者が認証業務規程に違反した場合
- ・ その他連合会認証局が失効の必要があると判断した場合

なお、連合会認証局は、ブリッジ認証局に対して発行した相互認証証明書について、以下の項目に該当すると認めた場合は、認証局責任者の承認をもって相互認証証明書の失効処理を行うことができる。

- ・ 連合会認証局又はブリッジ認証局の秘密鍵の危殆化もしくは、その恐れのある場合
- ・ 連合会認証局又はブリッジ認証局が相互認証基準に違反した場合
- ・ 連合会認証局又はブリッジ認証局が相互認証業務を終了する場合
- ・ 連合会認証局又はブリッジ認証局がポリシーを変更した場合
- ・ 連合会認証局とブリッジ認証局の相互認証を更新する場合

#### 4.5.6 一時停止

連合会認証局は、連合会認証局が発行した電子証明書の一時的停止を行わない。

#### 4.5.7 失効リスト (CRL・ARL)

連合会認証局は CRL・ARL を連合会認証局が発行した電子証明書に記載された場所に公開する。CRL・ARL の有効期間は 48 時間とし、発行は 24 時間ごとに行う。CRL・ARL には、連合会認証局が失効処理をした電子証明書で有効期間内のものに関する情報のみを記載する。

#### 4.5.8 失効情報及び有効性確認情報に関する要件

連合会認証局は、CRL・ARL をリポジトリで公開する。検証者は、リポジトリで公開する CRL・ARL を確認し、連合会認証局が発行した電子証明書の失効処理が行われているか否かを確認しなければならない。ただし、連合会認証局は、連合会認証局が発行した電子証明書の中で有効期間を満了した電子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。

#### 4.5.9 認証局秘密鍵の危殆化に関する特別要件

連合会認証局は、認証局秘密鍵に危殆化又は危殆化の恐れがある場合は、連合会認証サービスを停止し、直ちに全ての利用者証明書の失効処理を行い、CRL に登録し、利用者に認証局秘密鍵の危殆化等の事実と利用者証明書失効の通知を行う。その後、相互認証証明書の失効処理を行い、ARL に登録し、CRL・ARL の更新を確認後、認証局秘密鍵の廃棄を行う。

### 4.6 セキュリティ監査手続き

連合会は、連合会認証局を安全に運営するために適切な頻度でセキュリティ上の問題発生の有無について監査を行う。

#### 4.6.1 記録されるイベント

連合会認証局における監査証跡には、以下の事項を含めることとする。

- ・ 連合会認証局が発行した電子証明書の作成及び失効の記録
- ・ 連合会認証局が発行した電子証明書の作成及び失効に係る認証設備システムの操作履歴
- ・ 認証設備室への入退室記録
- ・ 認証設備システムへの不正アクセスの記録
- ・ 認証設備システムの動作に関する記録

#### 4.6.2 監査の頻度

連合会認証局は、連合会認証局のシステムを安全に運営するために適切な頻度で、セキュリティ上の問題発生の有無について監査により監査証跡を残す。

#### 4.6.3 監査ログの保存期間

監査証跡には全て、認証業務規程「4.7.1 申請に係るデータ」及び「4.7.3 設備及び安全対策措置に関するデータ」において定めるデータを含めることとする。監査証跡の保存期間は、認証業務規程「4.7.1 申請に係るデータ」及び「4.7.3 設備及び安全対策措置に関するデータ」に定める。

#### 4.6.4 監査証跡の保護

連合会認証局は、漏洩、改竄、滅失及び毀損等の防止処置を施し、監査証跡を保管管理する。

#### 4.6.5 監査証跡のバックアップ手順

連合会認証局は、バックアップが必要な監査証跡が存在する場合は、別途定めるバックアップ手順

に従い、バックアップを行う。

#### 4.6.6 監査証跡の記録システム

連合会認証局は、IA または RA のシステムによる自動処理及びオペレータによる手動操作を組み合わせ、監査証跡を収集する。

#### 4.6.7 問題の原因となるイベントの通知

IA 又は RA のシステムの処理中又は操作中にセキュリティに関する重大なイベント又は不具合が発生した場合は、その事項を検知したオペレータは、それぞれの業務責任者に報告を行う。報告を受けた業務責任者は、定められた手順に従い当該イベント等を処理する。

#### 4.7 記録のアーカイブ

連合会認証局は、電子署名法の定める書類について、漏洩、改竄、滅失及び毀損の防止処置を施し、電磁的記録媒体により保存するものを除き原本を保管する。

##### 4.7.1 申請に係るデータ

連合会認証局は、以下に定める利用者証明書発行申請時、利用者証明書失効申請時及び利用者証明書に係る情報の開示申請時に利用者から提出された書類及び連合会認証局でその管理上作成した帳簿を、当該帳簿書類に係る利用者証明書の有効期間の満了日から 10 年間保存する。

##### (1) 書類で保管するもの

- 発行申請に関する書類 (RA で保管)
  - ・ 発行申請書
  - ・ 印鑑登録証明書
  - ・ 住民票の写し等
  - ・ 登録原票記載事項証明書等
  - ・ 全部／個人事項証明書
  - ・ 発行申請書の審査時に作成された書類
  - ・ 利用者証明書受領確認書
  - ・ 重要事項説明書
  - ・ サービス利用規約
- 失効申請に関する書類 (RA で保管)
  - ・ 失効申請書
  - ・ 印鑑登録証明書
  - ・ 住民票の写し等
  - ・ 登録原票記載事項証明書等
  - ・ 全部／個人事項証明書
  - ・ 戸籍の附票の写し
  - ・ 印鑑登録証明書のコピー (発行申請書類も同時に提出する場合)
  - ・ 住民票の写し等のコピー (発行申請書類も同時に提出する場合)
  - ・ 登録原票記載事項証明書等のコピー (発行申請書類も同時に提出する場合)
  - ・ 全部／個人事項証明書のコピー (発行申請書類も同時に提出する場合)
  - ・ 失効申請書の審査時に作成された書類
- 開示申請に関する書類 (RA で保管)
  - ・ 開示申請書
  - ・ 印鑑登録証明書
  - ・ 住民票の写し等
  - ・ 登録原票記載事項証明書等
  - ・ 戸籍の附票の写し
  - ・ 全部／個人事項証明書
  - ・ 開示申請書の審査時に作成された書類

- 認証局秘密鍵の生成及び管理に関する書類 (IA で保管)
- 利用者秘密鍵の生成に関する記録 (RA で保管)
- 相互認証手続きに関する書類 (IA で保管)

(2) 電磁的記録媒体に保管するもの

- 連合会認証局が発行した電子証明書及びその作成に関する記録 (IA で保管)
- 自己署名証明書及びリンク証明書 (IA で保管)
- 失効に関する情報及びその作成に関する記録 (IA で保管)
- 利用者秘密鍵の生成及び削除に関する記録 (RA で保管)
- 利用者秘密鍵・利用者証明書・自己署名証明書の PKCS#12 ファイルへの格納及び削除に関する記録 (RA で保管)
- 相互認証手続きに関する記録 (IA で保管)

#### 4.7.2 組織関係データ

連合会認証局は、以下に定める業務遂行上必要とされる組織管理関係帳簿等の原本を、当該帳簿書類に係る利用者証明書の有効期間の満了日から 10 年間保存する。

- 認証業務規程とその変更に関する記録 (RA で保管)
- 業務手順を記述した書類とその変更に関する記録 (RA・IA で保管)
- 業務に従事する者の組織、体制、責任及び権限並びに指揮命令系統に関する書類 (RA・IA で保管)
- 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及び外部のファシリティ設備を利用する場合の利用契約等の書類 (RA で保管)
- 定期的に行う監査に関する記録と監査報告書 (RA・IA で保管)

#### 4.7.3 設備及び安全対策措置に関するデータ

連合会認証局は、その運用に係る設備及びその安全対策措置に関する記録を、監査記録として作成した日から認定の更新日まで保存する。

(1) 書類で保管するもの

- 帳簿書類の利用及び廃棄に関する記録 (RA・IA で保管)
- 認証設備室への入退室時の警報に関する記録 (IA で保管)
- 認証設備の保守及びシステム変更に関する記録 (RA・IA で保管)
- 認証設備の維持管理に関する記録 (RA・IA で保管)
- 認証設備の障害及び復旧に関する記録 (RA・IA で保管)
- 認証設備の事故に関する記録 (RA・IA で保管)
- 入室権限を持たない者を入室させた時の管理記録 (RA・IA で保管)
- 登録用端末設備室への入退室に関する記録 (RA で保管)

(2) 電磁的記録媒体に保管するもの

- 認証設備室への入室権限付与に関する記録 (IA で保管)
- 認証設備室への入退室及び警報に関する記録 (IA で保管)
- 認証設備システムへの不正アクセスの記録 (IA で保管)
- 認証業務用設備の操作記録及び操作時に使用する識別符号の管理記録 (IA で保管)
- 認証設備システムの動作に関する記録 (IA で保管)
- 登録用端末 OS のアカウントログ (RA・IA で保管)

#### 4.7.4 アーカイブデータの保護

連合会認証局は、漏洩、改竄、滅失及び毀損等を防止する安全措置を講じ、温度、湿度、磁気等の環境における要素から保護することを考慮し、自動火災報知器及び消火装置を備え、施錠可能な出入り口を持ち、間仕切りにより区分された常温常湿の部屋に設置された施錠可能なキャビネットにおいて、直接日光の当たらない環境で専用ファイルに綴じ込み帳簿書類の原本及びアーカイブされたデータを記録、保管している電磁的記録媒体を保管管理する。

#### 4.7.5 アーカイブデータのバックアップ

連合会認証局は、バックアップが必要なアーカイブデータが存在する場合は、別途定めるバックアップ手順に従いバックアップを行う。

#### 4.7.6 アーカイブ情報の保管

連合会認証局は、アーカイブされた情報が保管期間を通じて判読可能な状態で保管する。そのため、以下を満たす保管を行う。

- ・ 電磁的記録媒体の内容を表示できるように、機器やアプリケーション等の維持、保存を行う。
- ・ 機器やアプリケーションをバージョンアップ等の機器の変更を行う場合、電磁的記録媒体の判読が可能であるように互換性を保つようにする。もし、互換性を保てない場合は、機器変更後も判読可能な電磁的記録媒体に再記録を行う。
- ・ 年に1度、保管している電磁的記録媒体をサンプリング抽出し、データが読み取り可能である事を確認する。
- ・ 電磁的記録媒体は適切なケース等に保管する。

#### 4.7.7 関係書類及び記録の破棄

連合会認証局は、「4.6.3 監査ログの保存期間」及び「4.7.1 申請にかかるデータ」乃至「4.7.3 設備及び安全対策措置に関するデータ」に定める保存対象の認証業務関係書類及び記録について、その保存期間を経過した場合は当該書類、記録及び電磁的記録につき、確実に破棄する。これら書類及び記録は確実に断裁破棄、電磁的記録は媒体の破壊又は無効情報の上書き等により消去し、破棄した日、処理日等を記録するものとする。

#### 4.8 鍵の更新

##### (1) 連合会認証局鍵ペア

認証局公開鍵の有効期間は、有効とする日から起算して10年とし、連合会認証局は自己署名証明書が残存有効期間が利用者証明書の有効期間より短くなる前に、鍵更新を行う。認証局秘密鍵の有効期間は、有効とする日から鍵更新時までとし、鍵更新時に廃棄する。また、連合会認証局鍵ペア更新時には、古い認証局公開鍵と新しい認証局公開鍵の認証パスを構築するリンク証明書の発行を行う。

##### (2) 利用者鍵ペア

利用者公開鍵と利用者秘密鍵の有効期間は、有効とする日から起算して3年を経過した日の属する月の翌月以降初めての誕生月の1日までとする。(3年経過日の前に3年経過日の属する暦年の誕生月が経過している場合にあっては翌年の誕生月とする。)

#### 4.9 危殆化と災害の復旧

認証局秘密鍵の危殆化、災害等による障害発生などの不測の事態が発生した場合又は発生する恐れのある場合は、連合会は、迅速に次の措置を講じることとする。

##### (1) 認証局秘密鍵に危殆化又は危殆化の恐れがあることが判明した場合

- ・ 連合会認証局の発行業務を直ちに停止する。
- ・ 直ちに自己署名証明書を除く当該認証局秘密鍵を利用して発行した全電子証明書の失効処理を行い、全利用者にその旨を失効通知書の送付により通知するとともに、CRL・ARLを更新し、連合会ホームページを通じて検証者にその旨を公開し、認証局秘密鍵をバックアップも含め完全に破棄する。
- ・ 原因及び被害状況を調査し、対策及び再発防止策を講じ、直ちに障害の内容、発生日時、措置状況等確認済みの事項を主務大臣に通報するとともに、ブリッジ認証局へ報告する。
- ・ 連合会認証サービスを継続するために、再度、主務大臣の認定を受け、利用者が新たな利用者証明書の発行申請を行なえるようにするとともに、ブリッジ認証局との相互認証の手続きを行う。
- ・ その他必要な対策を講じる。

##### (2) 天災事変等の被災、認証業務用設備の故障等により運用を停止した場合

- ・ 被害の事実を全利用者宛て個別にその旨を通知書の送付により通知するとともに、連合

会ホームページを通じて検証者に公開する。

- ・ 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じる。
- ・ 検証者への失効情報の公開が、7日間を超えて停止し、かつ検証者が停止を知る方法がなかった場合は、連合会認証局は直ちに障害の内容、発生日時、措置状況等確認済の事項を主務大臣に通報するとともに、ブリッジ認証局へ報告する。
- ・ 電子署名法で公開及び保管が義務付けられているデータをバックアップをもとに復元する。
- ・ その他必要な対策を講じる。

#### 4.10 特定認証業務の終了

連合会認証局は、災害による不測の事態の発生により業務の不履行に至った場合又は連合会の事業方針の変更などに起因して認定の更新ができなかった場合は以下の手順に従い連合会認証サービスを終了する。

##### (1) 発行済み電子証明書の失効処理方法

連合会認証サービスの廃止日までに、自己署名証明書を除く当該認証業務で発行した全ての電子証明書の失効処理を行う。

##### (2) 連絡方法及び連絡時期等

当該認証業務の終了 60 日前から連合会ホームページに業務終了の案内を掲載するとともに、業務終了 60 日前までに主務大臣への通報及びブリッジ認証局への報告を行い、全利用者に業務終了の通知書を郵送する。

##### (3) 廃止後の失効情報の公開

業務終了に伴い連合会は、CRL・ARL の有効期間を 1 年間に設定して更新し、失効情報をリポジトリに 1 年間公開する。

##### (4) 認証局秘密鍵の処理

連合会認証局は、認証局秘密鍵及びバックアップした認証局秘密鍵の全てを完全に復元不可能な状態にする。

## 5 物理的、手続的、要員のセキュリティ統制

### 5.1 物理的セキュリティ統制

連合会認証局は、認証業務のための設備を、通常想定される災害に対して十分耐え得る建築構造物内に設置し、セキュリティ対策を講じることとする。

#### 5.1.1 登録用端末設備室のセキュリティ

登録用端末設備室は、これを独立した区画とし、無人のときは入退室口を施錠しなければならない。鍵の管理及び授受については予め任命された管理者がその任に就く。入室権限を有しない者の入室は原則として認めないこととする。やむを得ずこれを認める場合は、予め RA 設備責任者の許可を得て、入室権限者同行の上この者を入室させることとする。

#### 5.1.2 認証設備室のセキュリティ

認証設備室を収容する建築構造物に関しては、耐震耐火設計、自動火災報知器と消火装置の設置、防火区画内設置、隔壁による区画、水害防止措置などが、予め十分講じられている等、地震、火災、水害等想定される災害にも耐えうる設備とする。また、当該建築構造物には停電に備えた UPS 及び自家発電機の設置、配置された設備に応じた空調設備の設置等、連合会認証サービスの継続に必要で適切な措置を講じ、複数のセキュリティレベルで区画された場所の中に認証設備室を設置する。

認証設備室への入退室等については、以下のとおり厳重に管理する。

- (1) 厳重に施錠管理し、防護措置としてその入室者の身体的特徴の識別手段を用いた施錠設備による本人確認を行う。

- (2) 予めその資格について審査され指定登録を済ませた 2 名をもって入室可とし、入室者と同数

の者の退出をもって、退出を完了とする。1名のみで在室する状態にならないよう、対策を講じる。なお、入室権限を有しない者の入室は原則として認めない。ただし、やむを得ずこれを認める場合は、予め IA 設備責任者の許可を得て、複数人の入室権限者同行の上この者を入室させる。IA 設備担当者は、以上の入退室管理が実施されているか、日常的にチェックし監督する。

- (3) 入室のための装置操作に不正常な時間を要した場合は、警報が発せられるよう設定を行う。
- (4) 認証設備室への入退室者及び在室者の状況については、遠隔監視、モーションセンサ及び画像記録により、自動的かつ継続的に監視記録する。当該記録は、IA 設備担当者が正確に点検し、定められた期間、安全に保管する。
- (5) 認証設備室の所在及び仕様は、関係者以外には厳重に秘匿する。建物の内外には、認証設備室の所在についての表示を行わない。

## 5.2 手続き的セキュリティ統制

手続き的セキュリティ統制に係る組織体系を表 5-1 に示す。

表 5-1 連合会認証局の各役割の業務と権限

役割	主な業務	設備室等入室権限	設備アクセス権限
組織代表者	連合会の代表	認証設備室：なし 登録用端末設備室及び認証局用倉庫：RA 設備責任者が鍵を貸与	なし
認証局責任者	認証局運営全体統括	認証設備室：なし 登録用端末設備室及び認証局用倉庫：RA 設備責任者が鍵を貸与	なし
RA 登録業務		登録用端末設備室及び認証局用倉庫	
RA 業務責任者	RA 業務統括	RA 設備責任者が鍵を貸与	ユーザ権限
RA 業務担当者	利用者の真偽確認	RA 設備責任者が鍵を貸与	ユーザ権限
RA 端末操作者	利用者情報の登録操作	RA 設備責任者が鍵を貸与	ユーザ権限
RA 設備責任者	登録用端末設備の管理責任	設備室の鍵の管理を行い、自ら管理する鍵を使用	なし
RA 設備担当者	登録用端末設備の管理	RA 設備責任者が鍵を貸与	管理者権限
RA 発行申請業務		認証設備室	
RA 端末操作者	利用者証明書の発行操作	IC カード、生体認証	ユーザ権限
IA 業務		認証設備室	
IA 業務責任者	IA 業務統括	IC カード、生体認証	なし
IA 業務担当者	IA 認証設備の運用	IC カード、生体認証	ユーザ権限
IA 設備責任者	IA 認証設備の管理責任	IC カード、生体認証	なし
IA 設備担当者	IA 認証設備の管理	IC カード、生体認証	管理者権限
IA 鍵操作者	認証局秘密鍵の操作	IC カード、生体認証	ユーザ権限

## 5.3 要員のセキュリティ統制

連合会認証局は、認証業務に係る要員の採用前後の経歴や経験を踏まえ、従事するのに的確であるか否かの確認を行った上で、任命・配置を行い、役割ごとの必要な知識・経験、教育訓練計画、最低必要人員を規定し、この規定に従い人員の配置や教育訓練を行う。

個人情報取扱いと保護、認証局秘密鍵の危殆化及び災害等による障害発生などの不測の事態に対

する対応策及び回復手順に関して認証業務に従事する者の責任と権限に応じた教育・訓練計画を策定し、教育訓練を定期的実施することも含め、連合会認証局は、認証業務に係る要員の信頼性、適格性及び業務遂行能力の維持に努める。

## 6 技術的セキュリティ統制

### 6.1 鍵ペアの生成とインストール

連合会認証局は、連合会認証局鍵ペアを、信頼性あるシステムを用いて生成し、その滅失、毀損、紛失、開示、改変、漏洩あるいは無断使用の防止措置を十分に講じて保護する。

#### 6.1.1 鍵ペアの生成

##### (1) 認証局鍵ペア生成

連合会認証局は、認証設備室内で専用の電子計算機を用いて、複数人の要員により行なわれかつそのうちの1名だけでは生成されない方法によって、暗号モジュール (FIPS140-2 レベル 3 認定済の製品である HSM) 内で連合会認証局の鍵ペアを生成する。

##### (2) 利用者鍵ペア生成

連合会認証局は、利用者証明書発行申請の審査及び承認を行った後、複数人による相互牽制下で認証設備室内の登録用端末より利用者証明書の発行要求を行い、認証設備室内に設置された RA サーバ上で利用者の鍵ペアを生成する。また、当該利用者秘密鍵を IA より発行された利用者証明書及び自己署名証明書とともに所定形式 (PKCS#12) のファイルに登録し、複数人の管理下で USB メモリに格納する。USB メモリに格納するまでに経由した装置における利用者秘密鍵及び所定形式 (PKCS#12) の活性化に必要なパスフレーズ等の利用者秘密鍵に関連する情報は完全に消去する。

#### 6.1.2 利用者証明書発行者への利用者公開鍵の引渡し

利用者の鍵ペアは、連合会認証局において生成するため、利用者は利用者公開鍵の連合会認証局への引渡しを行わない。

#### 6.1.3 利用者への自己署名証明書の配送

連合会認証局は、自己署名証明書を USB メモリに格納し、利用者へ配送する。

#### 6.1.4 利用者への鍵配送

利用者の鍵ペアの配送に関しては、利用者秘密鍵、利用者証明書及び自己署名証明書を登録した所定形式 (PKCS#12) のファイルに変換し、USB メモリに格納した後、本人限定受取郵便を使用して利用者本人に郵送する。

利用者は利用者の鍵ペアを受取った後、連合会認証局に対して利用者証明書受領確認書を送付しなければならない。

#### 6.1.5 鍵のサイズ

連合会認証局で生成する連合会認証局の鍵のサイズと利用者の鍵のサイズは、以下のとおりとする。

連合会認証局：2048bit

利用者：1024bit

#### 6.1.6 ハードウェア/ソフトウェアでの鍵生成

連合会認証局は、連合会認証局の鍵ペアに関しては暗号モジュール (HSM) 内で生成する。また、利用者の鍵ペアに関しては RA サーバ内のソフトウェアで生成する。

#### 6.1.7 鍵の使用目的

連合会認証局で生成する認証局秘密鍵の使用目的及び利用者秘密鍵の使用目的は、以下のとおりとする。

認証局秘密鍵：電子証明書への電子署名、失効情報への電子署名

利用者秘密鍵：電子署名、否認防止

なお、認証局秘密鍵は、利用者証明書への電子署名以外では、以下の用途でのみ使用する。

- ・ ブリッジ認証局との相互認証の実施
- ・ 自己署名証明書への電子署名
- ・ リンク証明書への電子署名
- ・ 認証業務用設備及びそれを操作する者に対して発行する電子証明書への電子署名
- ・ 失効情報への電子署名

## 6.2 認証局秘密鍵の保護

連合会認証局は、認証局秘密鍵の保護につき管理体制を定める。

### 6.2.1 認証局秘密鍵の複数人管理

連合会認証局は、認証局秘密鍵の生成、バックアップ、リカバリ、破棄及び認証局秘密鍵を使用可能もしくは使用不可能にする操作を、認証設備室内において複数人の要員により行ないかつそのうちの1名だけでは操作できない方法によって、実施する。

### 6.2.2 秘密鍵の寄託

連合会認証局が管理する全ての秘密鍵は、寄託の対象としない。

### 6.2.3 認証局秘密鍵のバックアップ

連合会認証局は、認証局秘密鍵のバックアップを、認証設備室内において複数人の要員により行ないかつそのうちの1名だけでは操作できない方法によって、実施する。バックアップ／リカバリに必要となる暗号モジュールの管理鍵は複数に分割し、複数人の要員により管理者となる要員以外が触れることができない施錠等のアクセス制御及び耐火等の防災措置がとられた、それぞれ異なる安全な場所に保管する。

### 6.2.4 認証局秘密鍵の暗号モジュールへの格納

連合会認証局は、認証局秘密鍵を認証設備室内において複数人の要員の相互牽制のもと、暗号モジュール内で生成し、保管する。

### 6.2.5 認証局秘密鍵をアクティブにする方法

連合会認証局は、認証局秘密鍵を認証設備室内において複数人の要員により行ないかつそのうちの1名だけでは操作できない方法によって、使用可能な状態とする。

### 6.2.6 認証局秘密鍵を非アクティブにする方法

連合会認証局は、認証局秘密鍵を認証設備室内において複数人の要員により行ないかつそのうちの1名だけでは操作できない方法によって、使用不可能な状態とする。

### 6.2.7 認証局秘密鍵の破棄

連合会認証局は、認証設備室内において複数人の要員の相互牽制のもと、廃棄対象の認証局秘密鍵を元の状態に戻せないことが保障できる方法によって、認証局秘密鍵を破棄する。また、一連の作業指示において、遅延なくバックアップした認証局秘密鍵を物理的に破棄する。

## 6.3 ネットワークセキュリティ

連合会認証局は、認証設備がインターネット等の外部のネットワークに接続する箇所においては、不正なアクセスを防止するためのファイアウォールを介して接続するとともに不正なアクセスを検知するシステムを設置する。RA、IA 間及び RA サーバ、登録用端末間で行われる通信については、それぞれの危険性に対応して盗聴防止及び改竄防止等のセキュリティ機能をもつアプリケーションを使用し、設備間の認証及び不要な通信データの破棄等の安全を確保するための適切な措置を講じた通信設備を用いる。

## 6.4 暗号化モジュールのセキュリティ

連合会認証局は、認証業務に用いるハードウェアに関して、FIPS140-2 Level3 認定済の製品であ

る暗号モジュールを使用する。

暗号モジュールを管理する電子計算機は、全てのネットワークからの隔離（オフラインの場合）もしくは他の電子計算機でのアクセス制御による外部ネットワークからの隔離（オンラインの場合）等、外部からの不正アクセス対策を施したものを使用することとする。また、連合会認証局は、OS等の安全性に対する脅威についての情報を常に収集し、問題があればメーカ推奨の修正プログラムを適用する等の対策を実施する。

## 7 電子証明書と CRL・ARL のプロファイル

### 7.1 電子証明書のプロファイル

連合会認証局が発行する電子証明書の形式、属性の仕様は、以下に掲げるものに準じたものを使用する。

(1) ITU-T Recommendation X.509

(2) RFC2459 Internet X.509 Public Key Infrastructure and CRL Profile, January 1999

#### 7.1.1 電子証明書の様式

連合会認証局は、「9 電子証明書詳細プロファイル」に定めるとおり X.509 バージョン 3 に準拠した電子証明書を発行する。

#### 7.1.2 電子証明書拡張様式

連合会認証局が発行する電子証明書には、認証局鍵識別子 (authorityKeyIdentifier)、所有者鍵識別子 (subjectKeyIdentifier)、鍵用途 (keyUsage)、証明書ポリシー (certificatePolicies) (自己署名証明書を除く)、所有者別名 (subjectAltName) (相互認証証明書を除く)、発行者別名 (issuerAltName) (相互認証証明書を除く)、基本制約 (basicConstraints) (利用者証明書を除く) 及び失効リスト配布点 (cRLDistributionPoints) を含める。

相互認証証明書には、これらに加えてポリシーマッピング (policyMappings)、ポリシー制約 (policyConstraints) を含める。

#### 7.1.3 認証局鍵識別子 (authorityKeyIdentifier)

認証局公開鍵の sha-1 ハッシュ値を設定する。

#### 7.1.4 所有者鍵識別子 (subjectKeyIdentifier)

自己署名証明書及びリンク証明書においては、認証局公開鍵の sha-1 ハッシュ値を設定し、ブリッジ認証局に対する相互認証証明書においては、ブリッジ認証局の公開鍵の sha-1 ハッシュ値を設定する。利用者証明書においては、利用者公開鍵の sha-1 ハッシュ値を設定する。

#### 7.1.5 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においては、keyCertSign と cRLSign を ON にする。利用者証明書においては、digitalSignature と nonRepudiation を ON にする。

#### 7.1.6 証明書ポリシー (certificatePolicies)

相互認証証明書及び利用者証明書においては、「1.2 識別」に定めるオブジェクト識別子と認証業務規程を公開した URI を設定する。リンク証明書においては、ANY-POLICY を設定する。

#### 7.1.7 所有者別名 (subjectAltName)

自己署名証明書、リンク証明書及び利用者証明書においては、所有者名の別名を設定する。

#### 7.1.8 発行者別名 (issuerAltName)

自己署名証明書、リンク証明書及び利用者証明書においては、発行者名の別名を設定する。

#### 7.1.9 ポリシマッピング (policyMappings)

相互認証証明書においては、連合会認証局のドメインポリシーとブリッジ認証局のドメインポリシーを

等価と設定する。

#### 7.1.10 基本制約 (basicConstraints)

自己署名証明書、リンク証明書及び相互認証証明書においては、認証局証明書と設定する。

#### 7.1.11 ポリシ制約 (policyConstraints)

相互認証証明書においては、認証パス中のポリシの関係の制限を設定する。

#### 7.1.12 失効リスト配布点 (cRLDistributionPoints)

自己署名証明書、リンク証明書、相互認証証明書及び利用者証明書においては、CRL・ARL を公開した場所を設定する。

#### 7.1.13 電子署名方式

連合会認証局は、発行する電子証明書に対して、sha1WithRSAEncryption 方式を用い、2048bit の認証局秘密鍵で電子署名する。また、利用者が使用する利用者秘密鍵のサイズは 1024bit とする。

#### 7.1.14 名前の形式

連合会認証局が発行する電子証明書に含まれる名前については、国名は PrintableString 形式で記載し、それ以外の属性は UTF8String 形式で記載する。ただし、使用できる文字は issuerAltName、subjectAltName を除き、PrintableString で定義されている文字の範囲とする。

#### 7.1.15 名前の制約

issuer、subject は英語、issuerAltName、subjectAltName は日本語で表記する。

#### 7.1.16 発行番号

連合会認証局が発行する電子証明書には、連合会認証局内で一意に特定できる番号を整数形で記載する。

#### 7.1.17 有効期間

- ・自己署名証明書の有効期間は、発行日時より 10 年とする。
- ・相互認証証明書の有効期間は、発行日時より 5 年以内とする。
- ・リンク証明書の有効期間は、OldWithNew に関しては、旧世代の自己署名証明書の開始日から旧世代の自己署名証明書の終了日までとし、NewWithOld に関しては、新世代の自己署名証明書の開始日から旧世代の自己署名証明書の終了日までとする。
- ・利用者証明書の有効期間は、発行日時より起算して 3 年を経過した日の属する月の翌月以降初めての誕生月の 1 日までの期間（当該 3 年を経過した日（以下「3 年経過日」という。）の前に 3 年経過日の属する暦年の誕生月が経過している場合にあつては翌年の誕生月とする。）とする。なお、利用者証明書の有効期間は、最大 3 年と 365 日とし、発行の可否判断日から起算して 5 年未満である。

各証明書の有効期間は、UTCTime 形式で開始日及び終了日を記載することにより表す。

## 7.2 CRL・ARL プロファイル

連合会認証局は発行する電子証明書の形式、属性の仕様は、以下に掲げるものに準じたものを使用する。

- (1) ITU-T Recommendation X.509
- (2) RFC2459 Internet X.509 Public Key Infrastructure and CRL Profile, January 1999

### 7.2.1 CRL・ARL の様式

連合会認証局は、認証業務規程「10 CRL・ARL 詳細プロファイル」に定めるとおり、X.509 バージョン 2 に準拠した CRL・ARL を発行する。

### 7.2.2 失効に関する情報

連合会認証局は、CRL・ARL において失効を行った電子証明書のシリアル番号、失効日時、理由コー

ド及び無効日を記載する。

## 8 仕様管理

### 8.1 認証業務規程の仕様変更手続き

連合会は、本認証業務の仕様変更、あるいは仕様変更に伴い認証業務規程の改訂が必要となった場合、仕様変更に伴う電子署名法の変更認定の必要性について指定調査機関に確認するものとする。

また、認証業務規程の仕様変更にあたっては、事務取扱要領に定める全国社会保険労務士会連合会認証局ポリシー委員会（以下「ポリシー委員会」という。）において、改訂案の検討ならびに確認を行い、誤りがなければ認証局責任者による承認をもって仕様変更に係る作業を行う。

なお、仕様変更については、利用者又は検証者に事前の承諾なしに、随時、連合会はこれを修正することができる。この場合、変更履歴を含む最新の認証業務規程を連合会ホームページに掲載する。

#### 8.1.1 実務上の最新情報とお知らせ

連合会は、変更履歴を含む最新の認証業務規程を連合会ホームページに掲載することにより、利用者及び検証者へ改訂の通知を行う。

連合会ホームページに掲載する変更履歴を含む最新の認証業務規程は、認証業務規程を修正する効力を有し、かかる修正は、認証業務規程の関連する版の相違する認証業務規程及び指定された認証業務規程に優先するものとする。

#### 8.1.2 修正への同意

利用者が、修正の公開後 15 日以内に、自己の利用者証明書の失効申請を行わないときには、修正に同意したものとみなす。

## 9 電子証明書詳細プロフィール

連合会認証局が発行する電子証明書の詳細プロフィールを以下のとおり示す。

(1) 自己署名証明書

自己署名証明書の詳細プロフィールを表 9-1 に示す。

表 9-1 自己署名証明書の詳細プロフィール

領域名	クリティカル フラグ	値(例)	説明
version (バージョン)		2	V3 整数
serialNumber (発行番号)		(例: 013156A400000001)	電子証明書のシリアル番号、整数
signature (署名アルゴリズム)			電子署名のアルゴリズム
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer (発行者名)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	連合会認証局の識別名 (DN) UTF8String (country 属性のみ Printable)
validity (証明書有効期間)			電子証明書の有効期間(10年)
notBefore (開始日)		YYMMDDHHMSSZ (例: 150401000000Z)	電子証明書の開始日 UTCTime
notAfter (終了日)		YYMMDDHHMSSZ (例: 250331235959Z)	電子証明書の終了日 UTCTime
subject (所有者名)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	連合会認証局の識別名 (DN) UTF8String (country 属性のみ Printable)
subjectPublicKeyInfo (所有者公開鍵情報)			連合会認証局の公開鍵アルゴリズム
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.1	認証局公開鍵識別子 RSAEncryption
subjectPublicKey (公開鍵)			認証局公開鍵の値 BIT STRING

領域名	クリティカル フラグ*	値(例)	説明
extensions (電子証明書拡張領域)			
authorityKeyIdentifier (認証局鍵識別子)	FALSE		認証局鍵識別子
keyIdentifier (鍵識別子)			認証局公開鍵の SHA-1 ハッシュ値 OCTET STRING
authorityCertIssuer (発行者証明書発行者)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	UTF8String (country 属性のみ Printable)
authorityCertSerialNumber (発行者証明書シリアルナンバ)		(例 : 013156A400000001)	電子証明書のシリアル番号
subjectKeyIdentifier (所有者鍵識別子)	FALSE		認証局公開鍵の SHA-1 ハッシュ値 OCTET STRING
keyUsage (鍵用途)	TRUE		鍵の使用目的を指定
keyCertSign		1	[5] 電子証明書への電子署名
cRLSign		1	[6] 失効情報への電子署名
subjectAltName (所有者別名)	FALSE	OU=全国社会保険労務士会連合会認証局 O=全国社会保険労務士会連合会 C=JP	連合会認証局の識別名の別名 UTF8String (country 属性のみ Printable)
issuerAltName (発行者別名)	FALSE	OU=全国社会保険労務士会連合会認証局 O=全国社会保険労務士会連合会 C=JP	連合会認証局の識別名の別名 UTF8String (country 属性のみ Printable)
basicConstraints (基本制約)	TRUE		認証局証明書と利用者証明書を区別
cA		cA=TRUE	必須(MUST とする)
cRLDistributionPoints (失効リスト配布点)	FALSE	ldap://repository.shakaihokenroumushi.jp/ ou=All%20Japan%20Federation%20of%20 Shakaihokenroumushi%20Associations%20CA, o=AJFCSILCA, c=JP?authorityRevocationList	配布点の URI

(2) リンク証明書

リンク証明書の詳細プロフィールを表 9-2 に示す。

表 9-2 リンク証明書の詳細プロフィール

領域名	クリティカル フラグ	値(例)	説明
version (バージョン)		2	V3 整数
serialNumber (発行番号)		(例 : 013156A400000002)	電子証明書のシリアル番号
signature (署名アルゴリズム)			電子署名のアルゴリズム
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer (発行者名)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	連合会認証局の識別名 (DN) UTF8String (country 属性のみ Printable)
validity (証明書有効期間)			電子証明書の有効期間
notBefore (開始日)		YYMMDDHHMMSSZ (例 : 150401000000Z)	電子証明書の開始日 UTCTime OldWithNew : 旧世代の自己署名証明書の開始日 NewWithOld : 新世代の自己署名証明書の開始日
notAfter (終了日)		YYMMDDHHMMSSZ (例 : 250331235959Z)	電子証明書の終了日 UTCTime OldWithNew : 旧世代の自己署名証明書の終了日 NewWithOld : 旧世代の自己署名証明書の終了日
subject (所有者名)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	連合会認証局の識別名 (DN) UTF8String (country 属性のみ Printable)
subjectPublicKeyInfo (所有者公開鍵情報)			連合会認証局の公開鍵アルゴリズム
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.1	認証局公開鍵識別子 RSAEncryption
subjectPublicKey (公開鍵)			認証局公開鍵の値 BIT STRING

領域名	クリティカル フラグ	値(例)	説明
extensions (電子証明書拡張領域)			
authorityKeyIdentifier (認証局鍵識別子)	FALSE		認証局鍵識別子
keyIdentifier (鍵識別子)			認証局公開鍵の SHA-1 ハッシュ値 OCTET STRING OldWithNew: 新世代の鍵の SHA-1 ハッシュ値 NewWithOld: 旧世代の鍵の SHA-1 ハッシュ値
authorityCertIssuer (発行者証明書発行者)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	UTF8String (country 属性のみ Printable)
authorityCertSerialNumber (発行者証明書シリアル番号)		(例 : 013156A400000001)	OldWithNew: 新世代の自己署名証明書のシリアル番号 NewWithOld: 旧世代の自己署名証明書のシリアル番号
subjectKeyIdentifier (所有者鍵識別子)	FALSE		認証局公開鍵の SHA-1 ハッシュ値 OCTET STRING OldWithNew: 旧世代の鍵の SHA-1 ハッシュ値 NewWithOld: 新世代の鍵の SHA-1 ハッシュ値
keyUsage (鍵用途)	TRUE		鍵の使用目的を指定
keyCertSign		1	[5] 電子証明書への電子署名
cRLSign		1	[6] 失効情報への電子署名
certificatePolicies (証明書ポリシー)	FALSE		電子証明書のポリシー情報
policyIdentifier			
certPolicyId		2.5.29.32.0	ANY-POLICY
subjectAltName (所有者別名)	FALSE	OU=全国社会保険労務士会連合会認証局 O=全国社会保険労務士会連合会 C=JP	連合会認証局の識別名の別名 UTF8String (country 属性のみ Printable)
issuerAltName (発行者別名)	FALSE	OU=全国社会保険労務士会連合会認証局 O=全国社会保険労務士会連合会 C=JP	連合会認証局の識別名の別名 UTF8String (country 属性のみ Printable)
basicConstraints (基本制約)	TRUE		認証局証明書と利用者証明書を区別
cA		cA=TRUE	必須(MUST とする)
cRLDistributionPoints (失効リスト配布点)	FALSE	ldap://repository.shakaihokenroumushi.jp/ ou=All%20Japan%20Federation%20of%20 Shakaihokenroumushi%20Associations%20CA, o=AJFCSILCA,c=JP?authorityRevocationList	配布点の URI

(3) 相互認証証明書

相互認証証明書の詳細プロフィールを表 9-3 に示す。

表 9-3 相互認証証明書の詳細プロフィール

領域名	クリティカル フラグ	値(例)	説明
version (バージョン)		2	V3 整数
serialNumber (発行番号)		(例: 013156A400000003)	電子証明書のシリアル番号
signature (署名アルゴリズム)			電子署名のアルゴリズム
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer (発行者名)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	連合会認証局の識別名 (DN) UTF8String (country 属性のみ Printable)
validity (証明書有効期間)			電子証明書の有効期間 (GPKI 定義期間)
notBefore (開始日)		YYMMDDHHMSSZ (例: 150401000000Z)	電子証明書の開始日 UTCTime
notAfter (終了日)		YYMMDDHHMSSZ (例: 200331235959Z)	電子証明書の終了日 UTCTime
subject (所有者名)		OU=Bridge CA O=Japanese Government C=JP	ブリッジ認証局の識別名 (DN)
subjectPublicKeyInfo (所有者公開鍵情報)			ブリッジ認証局の公開鍵アルゴリズム
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.1	ブリッジ認証局の公開鍵識別子 RSAEncryption
subjectPublicKey (公開鍵)			ブリッジ認証局の公開鍵の値 BIT STRING

領域名	クリティカル フラグ	値(例)	説明
extensions (電子証明書拡張領域)			
authorityKeyIdentifier (認証局鍵識別子)	FALSE		認証局鍵識別子
keyIdentifier (鍵識別子)			認証局公開鍵の SHA-1 ハッシュ値 OCTET STRING
authorityCertIssuer (発行者証明書発行者)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	UTF8String (country 属性のみ Printable)
authorityCertSerialNumber (発行者証明書シリアル番号)		(例 : 013156A400000001)	自己署名証明書のシリアル番号
subjectKeyIdentifier (所有者鍵識別子)	FALSE		ブリッジ認証局公開鍵の SHA-1 ハッシュ値 OCTET STRING
keyUsage (鍵用途)	TRUE		鍵の使用目的を指定
keyCertSign		1	[5]電子証明書への電子署名
cRLSign		1	[6]失効情報への電子署名
certificatePolicies (証明書ポリシー)	TRUE		電子証明書のポリシー情報
policyIdentifier			
certPolicyId		0.2.440.200129.8.5.1.1.10	利用者証明書ポリシー識別子
policyQualifiers			ポリシー修飾子 (CP/CPS へのポインタまたは、ユーザ通知情報)
policyQualifierId			CP/CPS
qualifier		http://www.shakaihokenroumushi.jp/	公開する CP/CPS の URI IA5String
policyMappings (ポリシーマッピング)	FALSE		発行者ポリシーと所有者ポリシーを等価と見なす
issuerDomainPolicy		0.2.440.200129.8.5.1.1.10	連合会認証局のドメインポリシー識別子
subjectDomainPolicy		0.2.440.100145.8.1.1.1.10	ブリッジ認証局のドメインポリシー識別子
basicConstraints (基本制約)	TRUE		認証局証明書と利用者証明書を区別
cA		cA=TRUE	必須 (MUST とする)
policyConstraints (ポリシー制約)	TRUE		認証パス処理でポリシーマッピング処理をするパス長を指定
requireExplicitPolicy		0	ポリシーの明示を要求
cRLDistributionPoints (失効リスト配布点)	FALSE	ldap://repository.shakaihokenroumushi.jp/ ou=All%20Japan%20Federation%20of%20 Shakaihokenroumushi%20Associations%20CA, o=AJFCSILCA,c=JP?authorityRevocationList	配布点の URI

(4) 利用者証明書

利用者証明書の詳細プロフィールを表 9-4 に示す。

表 9-4 利用者証明書の詳細プロフィール

領域名	クリティカル フラグ	値(例)	説明
version (バージョン)		2	V3 整数
serialNumber (発行番号)		(例: 013156A400000004)	電子証明書のシリアル番号
signature (署名アルゴリズム)			電子署名のアルゴリズム
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer (発行者名)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	連合会認証局の識別名 (DN) UTF8String (country 属性のみ Printable)
validity (証明書有効期間)			電子証明書の有効期間 3年+誕生月 (当該月1日)
notBefore (開始日)		YYMMDDHHMMSSZ (例: 150410120000Z)	電子証明書の開始日 UTCTime
notAfter (終了日)		YYMMDDHHMMSSZ (例: 180801235959Z)	電子証明書の終了日 UTCTime
subject (所有者名)		(例: CN=AJFCSILCA, 10000000, Shinsei Taro, 12345678 OU=Tokyo O=AJFCSILCA C=JP )	利用者の識別名 (DN) CN= AJFCSILCA, 付加情報, 利用者氏名, 社会保 険労務士登録番号 OU=所属する社会保険労務士会の都道府県名 O= AJFCSILCA C=JP UTF8String (country 属性のみ Printable) ※
subjectPublicKeyInfo (所有者公開鍵情報)			利用者の公開鍵アルゴリズム
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.1	利用者公開鍵識別子 RSAEncryption
subjectPublicKey (公開鍵)			利用者公開鍵の値 BIT STRING

※旧姓もしくは通称名を利用する場合、subject の CN は利用者名の後ろに“(旧姓もしくは通称名)”を加えた形式で記載する。

CN=AJFCSILCA, 10000000, Shinsei Taro (Ninshou), 12345678

OU=Tokyo

O =AJFCSILCA

C =JP

領域名	クリティカルフラグ	値(例)	説明
extensions (電子証明書拡張領域)			
authorityKeyIdentifier (認証局鍵識別子)	FALSE		認証局鍵識別子
keyIdentifier (鍵識別子)			認証局公開鍵の SHA-1 ハッシュ値 OCTET STRING
authorityCertIssuer (発行者証明書発行者)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	UTF8String (country 属性のみ Printable)
authorityCertSerialNumber (発行者証明書シリアル番号)		(例 : 013156A400000001)	自己署名証明書のシリアル番号
subjectKeyIdentifier (所有者鍵識別子)	FALSE		利用者公開鍵の SHA-1 ハッシュ値 OCTET STRING
keyUsage (鍵用途)	TRUE		鍵の使用目的を指定
digitalSignature		1	[0] 電子署名
nonRepudiation		1	[1] 否認防止
certificatePolicies (証明書ポリシー)	TRUE		電子証明書のポリシー情報
policyIdentifier			
certPolicyId		0.2.440.200129.8.5.1.1.10	利用者証明書ポリシー識別子
policyQualifiers			ポリシー修飾子 (CP/CPS へのポインタまたは、ユーザ通知情報)
policyQualifierId			CP/CPS
qualifier		http://www.shakaihokenroumushi.jp/	公開する CP/CPS の URI IA5String
subjectAltName (所有者別名)	FALSE	(例 : CN=10000000, 申請 太郎, 12345678 OU=認証事務所 OU=東京 O=全国社会保険労務士会連合会 C=JP )	CN=付加情報, 日本語氏名, 社会保険労務士 登録番号 OU=事務所名、法人名もしくは事業所名 OU=所属する社会保険労務士の都道府 県名 O=全国社会保険労務士会連合会 C=JP UTF8String (country 属性のみ Printable)
issuerAltName (発行者別名)	FALSE	OU=全国社会保険労務士会連合会認証局 O=全国社会保険労務士会連合会 C=JP	連合会認証局の識別名の別名 UTF8String (country 属性のみ Printable)
cRLDistributionPoints (失効リスト配布点)	FALSE	ldap://repository.shakaihokenroumushi.jp/ ou=All%20Japan%20Federation%20of%20 Shakaihokenroumushi%20Associations%20 OCA, o=AJFCSILCA, c=JP?certificateRevocationList	配布点の URI

※旧姓もしくは通称名を利用する場合、subjectAltName の CN は利用者名の後ろに“(旧姓もしくは通称名)”を加えた形式で記載する。

CN=10000000, 申請 太郎 (認証), 12345678

OU=認証事務所

OU=東京

O =全国社会保険労務士会連合会

C =JP

## 10 CRL・ARL 詳細プロフィール

連合会認証局が発行する CRL・ARL 詳細プロフィールを以下のとおり示す。

(1) CRL

CRL の詳細プロフィールを表 10-1 に示す。

表 10-1 CRL の詳細プロフィール

領域名	クリティカル フラグ	値(例)	説明
version (バージョン番号)		1	V2 整数
signature (署名アルゴリズム)			電子署名のアルゴリズム
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha1WithRSAEncryption
issuer (発行者名)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	連合会認証局の識別名 (DN) UTF8String (country 属性のみ Printable)
thisUpdate (今回の更新日)		YYMMDDHHMMSSZ (例: 030501000000Z)	今回の更新日時、UTCTime で設定する。
nextUpdate (次の更新日)		YYMMDDHHMMSSZ (例: 030503000000Z)	次の更新日時、UTCTime で設定する。 今回の更新日の 48 時間後を設定する。
revokedCertificates (失効した電子証明書)			失効された電子証明書エントリ (以下の組のリスト)
userCertificate		(例: 013156A400000007)	失効された電子証明書をシリアル番号 で指定、整数
revocationDate		YYMMDDHHMMSSZ (例: 010420000000Z)	失効日時、UTCTime で設定する。
crlEntryExtensions (失効証明書エントリ拡張)			(失効証明書ごとの拡張領域)
reasonCode	FALSE		理由コード 下記のいずれかを選択
unspecified		0	未定義、使用しない。
keyCompromise		1	鍵の危殆
cACompromise		2	認証局の鍵の危殆
affiliationChanged		3	所属の変更
superseded		4	更新
cessationOfOperation		5	利用の中止
certificateHold		6	電子証明書の保留、使用しない。
removeFromCRL	8	CRL の削除、使用しない。	
invalidityDate (無効日)	FALSE	YYMMDDHHMMSSZ (例: 010420000000Z)	本認証業務においては使用しない

次の revokedCertificates (失効した電子証明書)

領域名	クリティカル フラグ	値(例)	説明
crlExtensions (電子証明書失効リスト拡張)			
authorityKeyIdentifier (認証局鍵識別子)	FALSE		認証局秘密鍵の識別。電子証明書拡張と同じ形式。
keyIdentifier			認証局公開鍵の SHA-1 ハッシュ値 OCTET STRING
authorityCertIssuer (発行者証明書発行者)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	UTF8String (country 属性のみ Printable)
authorityCertSerialNumber (発行者証明書シリアル番号)		(例 : 013156A400000001)	自己署名証明書のシリアル番号
cRLNumber (CRL 番号)	FALSE	(例 : 013156A400000001)	シーケンス番号、整数
issuingDistributionPoint (発行配布点)	TRUE		
distributionPoint (配布点)		ldap://repository.shakaihokenroumushi.jp/ ou=All%20Japan%20Federation%20of%20Shakaihokenroumushi%20Associations%20OCA, o=AJFCSILCA,c=JP?certificateRevocationList	配布点の URI
onlyContainsUserCerts (利用者証明書のみ)		TRUE	利用者証明書のみを扱う。

(2) ARL

ARLの詳細プロフィールを表 10-2 に示す。

表 10-2 ARLの詳細プロフィール

領域名	クリティカルフラグ*	値(例)	説明
version (バージョン番号)		1	V2 整数
signature (署名アルゴリズム)			電子署名のアルゴリズム
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha1WithRSAEncryption
issuer (発行者名)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	連合会認証局の識別名 (DN) UTF8String (country 属性のみ Printable)
thisUpdate (今回の更新日)		YYMMDDHHMMSSZ (例: 030501000000Z)	今回の更新日時、UTCTime で設定する。
nextUpdate (次回の更新日)		YYMMDDHHMMSSZ (例: 030503000000Z)	次回の更新日時、UTCTime で設定する。 今回の更新日の 48 時間後を設定する。
revokedCertificates (失効した電子証明書)			失効された電子証明書エントリ (以下の組のリスト)
userCertificate		(例: 013156A400000008)	失効されたリンク証明書及び相互認証 証明書をシリアル番号で指定、整数
revocationDate		YYMMDDHHMMSSZ (例: 010420000000Z)	失効日時、UTCTime で設定する。
crlEntryExtensions (失効証明書エントリ 拡張)			(失効証明書ごとの拡張領域)
reasonCode	FALSE		理由コード 下記のいずれかを選択
unspecified		0	未定義、使用しない。
keyCompromise		1	鍵の危殆
cACompromise		2	認証局の鍵の危殆
affiliationChanged		3	所属の変更
superseded		4	更新
cessationOfOperation		5	利用の中止
certificateHold		6	電子証明書の保留、使用しない。
removeFromCRL	8	CRL の削除、使用しない。	
invalidityDate (無効日)	FALSE	YYMMDDHHMMSSZ (例: 010420000000Z)	本認証業務においては使用しない

次の revokedCertificates (失効した電子証明書)

領域名	クリティカル フラグ	値(例)	説明
crlExtensions (電子証明書失効リスト拡張)			
authorityKeyIdentifier (認証局鍵識別子)	FALSE		認証局秘密鍵の識別。電子証明書拡張と同じ形式。
keyIdentifier			認証局公開鍵の SHA-1 ハッシュ値 OCTET STRING
authorityCertIssuer (発行者証明書発行者)		OU=All Japan Federation of Shakaihokenroumushi Associations CA O=AJFCSILCA C=JP	UTF8String (country 属性のみ Printable)
authCertSerialNumber (発行者証明書シリアル番号)		(例 : 013156A400000001)	自己署名証明書のシリアル番号
crlNumber (CRL 番号)	FALSE	(例 : 013156A400000001)	シーケンス番号、整数
issuingDistributionPoint (発行配布点)	TRUE		
distributionPoint (配布点)		ldap://repository.shakaihokenroumushi.jp/ ou=All%20Japan%20Federation%20of%20Shakaihokenroumushi%20Associations%20OCA, o=AJFCSILCA, c=JP?authorityRevocationList	配布点の URI
onlyContainsCACerts (認証局証明書のみ)		TRUE	認証局証明書のみを扱う。