

セコムあんしんエコ文書サービス
証明書運用規定（建築士版）
（LRA 運用基準）

第 1.0 版

セコムトラストシステムズ株式会社

改版履歴			
版数	日付	内容	担当
V.1.00	2018/7/2	初版作成	STS

目次

1.	はじめに	5
1.1.	目的	5
2.	証明書利用開始の流れ.....	6
3.	RA 業務の運用について.....	7
3.1.	業務の役割	7
3.2.	運用の記録	7
4.	証明書の管理	8
4.1.	証明書の有効期間、記載事項.....	8
4.2.	証明書の利用制限	8
5.	証明書発行手続き.....	9
5.1.	組織および利用者の認証	9
5.1.1.	組織の申請書類一覧および提出方法.....	9
5.1.2.	真偽確認事項	9
5.1.3.	利用者の申請書類一覧および提出方法.....	10
5.1.4.	真偽確認事項	11
5.2.	証明書発行	11
5.3.	証明書の受領確認	11
6.	証明書失効手続き.....	12
6.1.	失効理由.....	12
6.2.	利用者の認証（失効）	12
6.2.1.	失効申請の提出書類および提出方法.....	12
6.2.2.	書類提出を伴う真偽確認事項.....	13
6.2.3.	書類提出を伴わない真偽確認事項.....	13
6.3.	責任者からの失効申請	14
6.3.1.	責任者からのユーザ削除申請の提出書類.....	14
6.3.2.	真偽確認事項	14
6.4.	証明書失効	14
7.	証明書更新手続き.....	15
7.1.	署名用証明書の更新.....	15
7.2.	認証用証明書の更新.....	15
7.3.	証明書の有効期間通知	15
8.	審査業務環境のセキュリティ対策	16
9.	利用者への周知	17
9.1.	利用者への告知事項.....	17
10.	情報管理	18
10.1.	書類・帳票の保管期間・保管方法.....	18
10.2.	書類・帳票の廃棄.....	18
11.	監査.....	19
11.1.	証明書発行取消処理結果の確認.....	19

11.2.	本書の準拠性監査.....	19
12.	署名用証明書プロファイル	20
13.	認証用証明書プロファイル	21

1. はじめに

1.1. 目的

証明書運用規定(以下、本書)はセコムあんしんエコ文書サービス(以下、エコ文書サービス)の電子証明書(以下、証明書)発行対象者の審査、発行対象者情報の登録、証明書の発行、失効等の認証業務の基準について定義したものです。

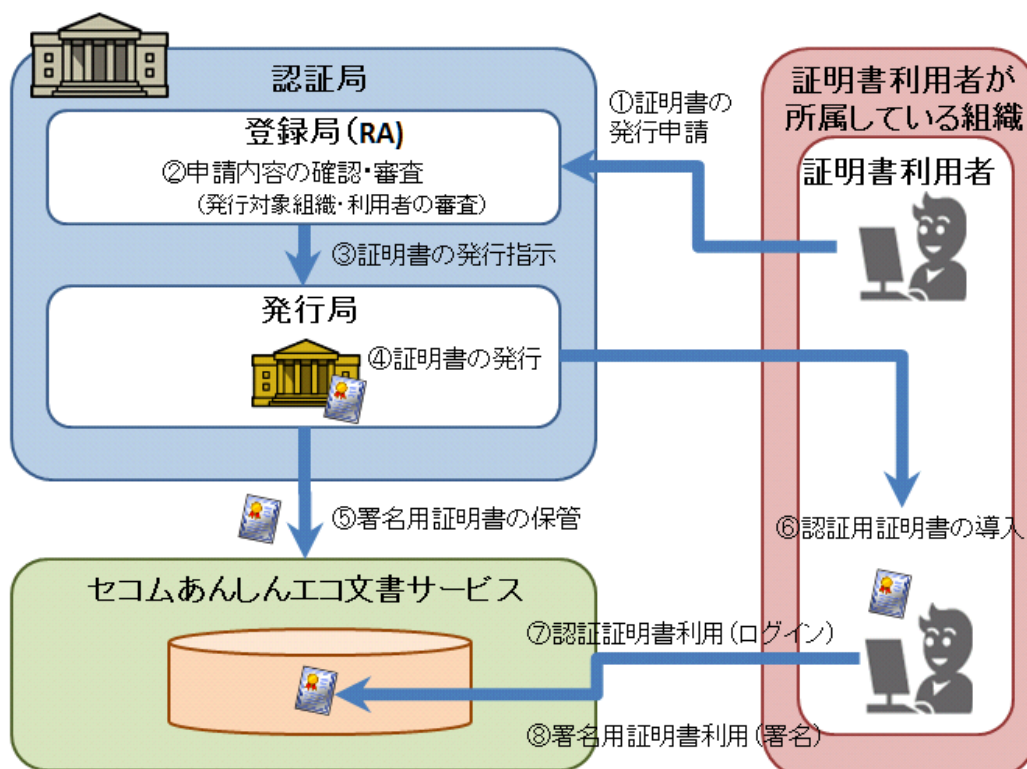
なお、詳細な手順及び管理方法等については、本書に準拠した手順書を作成し、運用を行うものとします。

2. 証明書利用開始の流れ

証明書の利用開始の流れは次の通りです。

- ① 証明書利用者（以下、利用者）は登録局に証明書の発行申請を実施。
（「5 証明書発行手続き」参照）
- ② 登録局は利用者が所属している組織と利用者について審査を実施。
（「5.1 組織の認証」参照）
- ③ 登録局は発行申請の真偽確認実施後、発行局に対して証明書の発行を指示。
（「5.2 証明書発行」参照）
- ④ 発行局は署名用証明書及び認証用証明書を発行。
- ⑤ 発行局より発行された署名用証明書をエコ文書サービスに保管。
署名用証明書は、利用者本人の認証用証明書によってのみ利用可能となる。
- ⑥ 発行局より発行された認証用証明書は専用サイトから証明書利用者がダウンロードしご利用 PC に導入。
- ⑦ 利用者のご利用 PC に導入した認証用証明書を用いてエコ文書サービスにログイン。
- ⑧ 利用者はエコ文書サービスに対して保管された署名用証明書を用いて電子署名を実施。

図 1 証明書利用開始の流れ



3. RA 業務の運用について

RA(Registration Authority)とは証明書に関する申請の審査や、発行・失効の登録業務を行う組織のことをいい、これらの業務を RA 業務とといいます。

3.1. 業務の役割

RA 業務の役割を以下に定めます。

1. 業務責任者

<主な業務>

- ・ RA 業務全般の手続変更・承認を含む RA 業務の全般管理、統括に関する業務
- ・ 審査担当者、登録担当者の任命、解任
- ・ 他の役割との兼務は不可

2. 審査担当者

<主な業務>

- ・ 証明書発行等に関わる審査業務全般
- ・ 利用者からの問い合わせ対応
- ・ 登録担当者との兼務は可能

3. 登録担当者

<主な業務>

- ・ 証明書発行等に関わる登録業務全般
- ・ 利用者からの問い合わせ対応
- ・ 審査担当者との兼務は可能

3.2. 運用の記録

利用者から提出された書類の審査と真偽確認、申請の登録申請、利用者の証明書の失効申請、それら業務の管理・監査等に必要となる業務について、次のような実施記録を残すものとします。

- ・ 業務種別
- ・ 実施日
- ・ 業務実施者名
- ・ 実施承認者名
- ・ 実施内容／結果
- ・ 受領／利用書類名
- ・ 完了承認者名

4. 証明書の管理

4.1. 証明書の有効期間、記載事項

証明書の有効期間は、5年未満です。なお、証明書の記載事項は「12. 証明書プロフィール」に記載のとおりとします。

4.2. 証明書の利用制限

認証用証明書は利用者がエコ文書にログインする際の利用者認証の用途でのみに使用するものとします。署名用証明書は、利用者がエコ文書にアップロードされた電子文書に電子署名を行う用途でのみに使用するものとします。

5. 証明書発行手続き

5.1. 組織および利用者の認証

5.1.1. 組織の申請書類一覧および提出方法

利用者が所属する組織名等の組織属性を記載した証明書の利用を申請する際の提出書類は持参、郵送、または電子文書送信による方法により受領するものとします。書類の提出先は申請書等に定めるものとします。

以下、申請する組織の代表者が提出する申請書類の一覧です。

表 1 組織の申請書類一覧

区分	提出書類
共通	ユーザ登録申請書
法人の場合	所属する組織の建築士事務所登録証明書、または印鑑登録証明書(発行日が受領日から6ヵ月以内) ※1
個人事業主の場合	個人事業主自身の建築士事務所登録証明書、または印鑑登録証明書

※1 信頼できる第三者機関のデータベース(東京商工リサーチ (TSR)、帝国データバンク (TDB) 等)を用いて代替可能

なお、エコ文書サービスを契約している組織と利用者が所属する組織間で、他サービス契約等により印鑑登録証明書(またはそれに変わる書面等)を受領済みであり、組織の実在性、信頼性が担保される場合は、印鑑登録証明書の提出を免除することも可とします。

5.1.2. 真偽確認事項

以下、申請する組織の代表者から提出された申請書類の真偽確認事項です。

<真偽確認事項>

(共通)

- ・ ユーザ登録申請書の必要項目がすべて記載されていることを確認
- ・ ユーザ登録申請書に契約申込者の署名があることを確認
- ・ ユーザ登録申請書に代表者の署名があることを確認
- ・ ユーザ登録申請書に代表者印が押印されていることを確認

(法人の場合)

- ・ 所属する組織の印鑑登録証明書について、記載内容及び形式が真正なものか確認
- ・ 所属する組織の印鑑登録証明書の発行日が受領日から 6 ヶ月以内か確認
- ・ ユーザ登録申請書に記載されている組織名と所属する組織の印鑑登録証明書の組織名が一致しているか確認
- ・ ユーザ登録申請書に押印されている代表者印の印影と所属する組織の印鑑登録証明書の印影が一致しているか確認

(個人事業主の場合)

- ・ 個人事業主自身の印鑑登録証明書に発行している公的機関の押印があり、記載内容及び形式が真正なものか確認
- ・ 個人事業主自身の印鑑登録証明書の発行日が受領日から 6 ヶ月以内か確認
- ・ ユーザ登録申請書に押印されている印影と個人事業主自身の印鑑登録証明書の印影が一致しているか確認

5.1.3. 利用者の申請書類一覧および提出方法

証明書を発行する際の提出書類は持参、郵送、または電子文書送信による方法により受領するものとします。書類の提出先は申請書等に定めるものとします。

以下、利用者が提出する申請書類の一覧です。

表 2 利用者の申請書類一覧

区分	提出書類
共通	ユーザ登録申請書
建築士の場合	①「建築士免許証」もしくは「カード型建築士免許証明書」のコピーまたは、スキャナー、デジタルカメラ等で撮影した画像ファイル※2 ②「建築士登録証明書」の提出
個人の場合	運転免許書のコピー

※2 スキャン画像はフルカラー、200dpi 以上の解像度のもの。

なお、利用者の所属組織が建築士事務所登録を行っている場合は、その代表者または代表者が指定する者による代理申請も可能とします。この場合、建築士事務所の社内規定により、あらかじめ所属する建築士の「建築士免許証」もしくは「カード型建築士免許証明書」を確認し、その写しが保存されており、かつ法令に基づく建築士名簿が適切に作成管理されている場合には、認証

局は当該建築士事務所登録証明書、および社内規程等を確認のうえ、建築士名簿を受領することにより、上記②の「建築士免許証」もしくは「カード型建築士免許証明書」の写しの受領に代えることができますものとしてします。

5.1.4. 真偽確認事項

以下、利用者から提出された発行申請書類の真偽確認事項です。

<真偽確認事項>

①申請意思確認

- ・ ユーザ登録申請書の必要項目がすべて記載されていることを確認
- ・ ユーザ登録申請書に利用者の署名（自書）があることを確認

②実在性確認

- ・ ユーザ登録申請書に代表者印があるか確認

5.2. 証明書発行

以下、真偽確認実施後に実施する証明書発行処理の手続きです。

1. 審査担当者は真偽確認実施後、確認結果を業務責任者に報告します。
2. 業務責任者は真偽確認結果を承認し登録担当者に対して証明書の発行作業を指示します。
3. 登録担当者は発行局に対して証明書の発行依頼を行います。
4. 登録担当者は発行依頼を完了後、結果を業務責任者に報告します。
5. 業務責任者は発行依頼の結果を確認し、承認します。
6. 登録担当者は、エコ文書サービスのユーザ登録機能を用いて署名用証明書及び認証用証明書を発行します。署名用証明書は、エコ文書サービス内の証明書ストアに格納されます。エコ文書サービスより認証用証明書のダウンロードに必要となる情報をeメールで通知します。
7. 利用者は、eメールに記載されている情報を基に利用者本人の操作により取得します。

5.3. 証明書の受領確認

利用者は、認証用証明書を用いて、エコ文書サービスにログインを行い、署名用証明書のPIN（エコ文書サービスでは、暗証コード）を設定します。この操作により、エコ文書サービスは利用者本人が受領したことを確認します。

6. 証明書失効手続き

6.1. 失効理由

利用者の秘密鍵が危殆化(※1)した場合や、利用者が利用者である要件を満たさなくなった場合等、証明書の信頼性を喪失する／した場合は、証明書を失効する必要があります。

証明書の失効が必要なケースは次のとおりです。特に、証明書の信頼性を著しく低下させる事態（秘密鍵及び PIN(※2)の盗難・紛失等）が発生した場合は、速やかに証明書失効処理を行う必要があります。

なお、署名用証明書と認証用証明書は個別または、双方合わせて失効する場合があります。

※1 証明書にセキュリティ上の問題が発生した場合をいいます。

※2 証明書のパスワードです。エコ文書サービス上では暗証コードと呼ばれます。

①利用環境が変わった場合

- (1)利用している PC を交換する場合
- (2)利用している PC から認証用証明書を削除した場合
- (3)認証用証明書が何らかの理由により破損し、利用できなくなった場合

②証明書の信頼性を低下させる次の事態が発生した場合

- (1) 利用している PC が盗難・紛失した場合（認証用証明書の場合）
- (2) 証明書(秘密鍵)を紛失・盗難・漏洩した、またはその疑いがある場合
- (3) その他、証明書の信頼性を著しく低下させる事態が発生した場合
- (4) 証明書の失効を必要とする障害があった場合
- (5) 業務責任者やセコムが証明書の失効を必要と判断した場合

③利用者が発行対象者要件を満たさなくなった場合

- (1) 利用者が休職もしくは、退職する場合
- (2) 証明書を利用しなくなった場合
- (3) 証明書の内容に変更が発生した場合

6.2. 利用者の認証（失効）

利用者からのユーザ削除申請は、持参、郵送により受け付けます。緊急時などには FAX、電話によっても受け付けます。

なお、証明書のユーザ削除申請は利用者自身、または利用者が所属する組織の責任者から行うことができます。

6.2.1. 失効申請の提出書類および提出方法

証明書の失効を申請する際の提出書類は持参または郵送による方法により受領するものとします。書類の提出先は申請書等に定めるものとします。

以下、失効申請の提出書類です。

表 3 失効申請提出書類一覧

区分	提出書類
削除	ユーザ削除申請書（署名用証明書の場合）
変更	ユーザ変更申請書（署名用証明書の場合）

※利用者のご利用 PC 変更等の事由による、認証用証明書の失効・更新を行う場合は、申請書の提出は求めず、電話または e メールにて依頼を受け、本人確認を実施の上対応します。

6.2.2. 書類提出を伴う真偽確認事項

以下、利用者から提出されたユーザ削除申請書類またはユーザ変更申請書の真偽確認事項です。

<真偽確認事項>

①申請意思確認

- ・ ユーザ削除申請書またはユーザ変更申請書に署名（自書）があることを確認

②書類の真正性確認

- ・ ユーザ削除申請書またはユーザ変更申請書に代表者印があるか確認
- ・ ユーザ削除申請書またはユーザ変更申請書の組織名とユーザ登録申請書の組織名が一致しているか確認

6.2.3. 書類提出を伴わない真偽確認事項

以下、書類提出を伴わない場合の真偽確認事項です。

<真偽確認事項>

①申請意思確認

- ・ 利用者から電話または e メールで対応窓口への連絡での意思表示

②申請の真正性確認

- ・ 利用者より提示された「企業名」、「氏名」、「メールアドレス」、「ユーザ ID」のうち 2 点が登録情報と一致するか確認

6.3. 責任者からの失効申請

退職や死亡等の理由により、利用者本人がユーザ削除申請できない場合は、利用者が所属する組織の責任者が代理で申請可能とします。

責任者がユーザ削除申請をする際は、責任者がユーザ削除申請書に必要な事項を記入し、提出します。

6.3.1. 責任者からのユーザ削除申請の提出書類

以下、責任者からのユーザ削除申請の提出書類一覧です。

表 4 責任者からのユーザ削除申請提出書類一覧

区分	提出書類
共通	ユーザ削除申請書

6.3.2. 真偽確認事項

以下、責任者から提出されたユーザ削除申請書類の真偽確認事項です。

<真偽確認事項>

①申請意思確認

- ・ ユーザ削除申請書に責任者の署名（自書）があるか確認

②書類の真正性確認

- ・ 責任者のユーザ削除申請書に代表者印があるか確認
- ・ ユーザ削除申請書の組織名とユーザ登録申請書の組織名が一致しているか確認

6.4. 証明書失効

以下、真偽確認実施後に実施する証明書失効処理の手続きです。

1. 審査担当者は真偽確認実施後、確認結果を業務責任者に報告する。
2. 業務責任者は真偽確認結果を承認し業務責任者は登録担当者に対して証明書の失効作業を指示する。
3. 登録担当者は登録局に証明書の失効依頼を行う。
4. 登録担当者は失効依頼を完了後、結果を業務責任者に報告する。
5. 業務責任者は失効依頼登録結果を確認し、承認する。
6. 発行局は証明書を失効する。

7. 証明書更新手続き

7.1. 署名用証明書の更新

利用者が署名用証明書の有効期間満了後も継続して署名用証明書を必要とする場合には、利用者がエコ文書サービスの画面操作を行い新たな署名用証明書を取得します。

7.2. 認証用証明書の更新

利用者が認証用証明書の有効期間満了後、またはご利用 PC の変更後も継続して認証用証明書を必要とする場合には、登録担当者がエコ文書サービスの画面操作を行い新たな認証用証明書を発行します。

7.3. 証明書の有効期間通知

登録担当者または審査担当者は、発行済み証明書の有効期間を定期的を確認し、証明書の有効期間満了1ヶ月前までに、利用者に対して継続して証明書が必要か否かの確認を行います。

8. 審査業務環境のセキュリティ対策

審査業務で利用する端末（以下、審査業務利用端末）の設置場所は、外部の第三者が無断で入室出来ない区画内とし、次の条件を満たすものとします。

- ・ 審査業務利用端末の保管・運用状態に関し業務責任者が管理すること
- ・ 審査業務利用端末を設置する室が無人の場合は施錠されること
- ・ 審査業務利用端末を設置する室を施錠、開錠出来る鍵を所持する従業員を特定できること
- ・ 審査業務利用端末へのログインには、適切な ID・パスワードによるアクセス制御を施すこと

9. 利用者への周知

9.1. 利用者への告知事項

エコ文書サービスを契約している組織は下記の事項を利用者に告知することとします。

- 利用者が提出する書類の種類
- 書類の提出方法
- 証明書の用途（エコ文書サービス上での電子署名の利用）
- 利用者にかかる重要事項
- エコ文書サービスを契約している組織が定める約款等に対する承諾
- エコ文書サービスを利用する上で遵守する規定「セコムあんしんエコ文書サービス利用規約(ご利用者様向け)」に対する承諾

10. 情報管理

10.1. 書類・帳票の保管期間・保管方法

真偽確認のために利用者から収集した書類等の情報や証明書発行、失効に係る作業記録は、書面によるものは200dpi、フルカラーにてスキャンした画像ファイルを、電子データによるものは当該電子データ（PDF形式）をあらかじめ定められたエコ文書サービス上のフォルダにアップロードし業務責任者の電子署名を付与した後、当該証明書の有効期間終了から15年間保管します。ただし、関連する法令等で保管期間が定められている場合はこの限りではありません。

上記のエコ文書サービス上のフォルダにはLRA業務の監査を目的として弊社よりアクセス用のユーザIDの作成とアクセス権の付与をお願いする場合がございます。

表5 書類・帳票の保管期間

No	分類	保管対象	保管期間
1	証明書の発行等に係る書類	ユーザ登録申請書、ユーザ変更申請書、ユーザ削除申請書	エコ文書サービス内で発行した当該電子証明書の有効期間終了日から15年間
2		利用者から提出された真偽確認書類	
3		RA業務の運用記録	

10.2. 書類・帳票の廃棄

保管期間を過ぎた書類及び帳票については、業務責任者による立ち合いのもと、細かく裁断する等の復元困難な状態で廃棄を実施し、廃棄の記録を残すこととします。

11. 監査

11.1. 証明書発行取消処理結果の確認

RA は、利用者以外に証明書が不正に発行されていないことを確認するため、証明書発行申請の記録と証明書失効申請の記録を定期的に（最低 1 ヶ月に 1 回）確認することとします。

実施結果については記録を残し、業務責任者の承認を得ることとします。

11.2. 本書の準拠性監査

RA は、業務品質の維持や組織の信頼性向上の為、RA 業務運用が本書に準拠して行われているかを内部または外部監査により確認するものとします。監査の頻度は、最低 1 年に一回とします。

監査の実施結果を記録し、最低 5 年間、保管することとします。

12. 署名用証明書プロフィール

表 6 署名用証明書プロフィール一覧

フィールド (基本領域)		内容
X.509 Version (X.509 証明書バージョン)		Version 3
Serial Number (証明書シリアル番号)		例) 123456789abcdef0
Signature Algorithm (署名アルゴリズム)		SHA-256 with RSAEncryption
Issuer (発行者)	Country (国)	C=JP
	Organization (組織)	O=SECOM Trust Systems CO.,LTD.
	Organizational Unit (組織単位)	OU=SECOM Passport for Member 2.0 PUB
	Common Name (CN)	CN=SECOM Passport for Member PUB CA" 数字" *"数字"の値は任意
Validity (有効期限)	NotBefore (有効性開始日時)	例) Feb 10 09:55:27 2006 GMT
	NotAfter (有効性終了日時)	例) Feb 10 10:25:27 2007 GMT *有効期間5年以下
Subject (主体者)	Country (国)	C=JP
	Organization (組織)	O="Secom Trust Systems CO. LTD."
	Organizational Unit (組織単位)	OU="Denshi Shoko Service*" *"数字"の値は任意
	Organizational Unit (組織単位)	OU="利用者が所属する会社名"【任意に指定可能】 ※1
	Organizational Unit (組織単位)	OU="資格コード" ※2
	Common Name (主体者名)	CN="利用者名"
	Serial Number (シリアル番号)	SerialNumber="シリアル番号"
Subject PublicKey Info (主体者公開鍵情報)		主体者の公開鍵データ

表 7 署名用証明書拡張領域一覧

フィールド (x.509 v3 拡張領域)	内容
-----------------------	----

Authority Key Identifier (発行者鍵識別子)	発行者の公開鍵識別子 (発行者公開鍵の 160bit SHA-1 ハッシュ値)
Subject Key Identifier (主体者鍵識別子)	主体者の公開鍵識別子 (主体者公開鍵の 160bit SHA-1 ハッシュ値)
Key Usage (鍵用途)	digitalSignature (デジタル署名) Non Repudiation (否認防止)
Certificate Policies (証明書ポリシー)	Policy: 1.2.392.200091.100.381.4 CPS: https://repol.secomtrust.net/spcpp/pfm20pub/
CRL Distribution Points (CRL 配布ポイント)	<a fullcrl.crl"="" href="http://repol.secomtrust.net/spcpp/pfm20pub/ca" 数字"="">http://repol.secomtrust.net/spcpp/pfm20pub/ca"数字"/fullCRL.crl *"数字"の値は任意 ldap://repol.secomtrust.net/"IssuerDN"?certificateRevocationList

※1 証明書申請毎に設定の有無を変えられる項目です。

※2 「設計図書の電磁的記録による作成と保存のガイドライン」(公益社団法人、日本文書情報マネジメント協会(JIIMA))にて規定される建築士の資格種別と登録番号をあらわす情報を設定します。

13. 認証用証明書プロファイル

表 8 認証用証明書プロファイル一覧

フィールド (基本領域)		内容
X.509 Version (X.509 証明書バージョン)		Version 3
Serial Number (証明書シリアル番号)		例) 123456789abcdef0
Signature Algorithm (署名アルゴリズム)		SHA-1 with RSAEncryption
Issuer (発行者)	Country (国)	C=JP
	Organization (組織)	O=SECOM Trust Systems CO., LTD.
	Organizational Unit (組織単位)	OU= SECOM Passport for Member 2.0 PUB
	Common Name (CN)	CN=SECOM Passport for Member PUB CA"数字" *"数字"の値は任意
Validity (有効期)	NotBefore (有効性開始日時)	例) Feb 10 09:55:27 2006 GMT

限)	NotAfter (有効性終了日時)	例) Feb 10 10:25:27 2007 GMT *有効期間 5 年以下
Subject (主体者)	Country (国)	C=JP
	Organization (組織)	O="Secom Trust Systems CO. LTD."
	Organizational Unit (組織 単位)	OU="Denshi Shoko Service *" *"数字"の値は任意
	Organizational Unit (組織 単位)	OU="ECO"
	Common Name (主体者名)	CN="S47xxxxxx(サービス内で採番)"
	Serial Numbewr (シリアル 番号)	SerialNumber="シリアル番号"
Subject PublicKey Info (主体者公開鍵情報)	主体者の公開鍵データ	

表 9 認証用証明書拡張領域一覧

フィールド (x.509 v3 拡張領域)	内容
Authority Key Identifier (発行者鍵識別子)	発行者の公開鍵識別子 (発行者公開鍵の 160bit SHA-1 ハッシュ値)
Subject Key Identifier (主体者鍵識別子)	主体者の公開鍵識別子 (主体者公開鍵の 160bit SHA-1 ハッシュ値)
Key Usage (鍵用途)	digitalSignature (デジタル署名) Key Encipherment (鍵暗号)
Certificate Policies (証明書ポリシー)	Policy: 1.2.392.200091.100.381.4 CPS: https://repol.secomtrust.net/spcpp/pfm20pub/
CRL Distribution Points (CRL 配布ポイント)	http://repol.secomtrust.net/spcpp/pfm20pub/ca数字/fullCRL.crl *"数字"の値は任意 ldap://repol.secomtrust.net/IssuerDN?certificateRevocationList

本書は、セコムパスポート for Member 2.0 PUB 証明書ポリシー (以下、CP) 及びセコム電子認証基盤認証運用規程 (以下、CPS) に基づき作成されたものです。CP および CPS は (<https://repol.secomtrust.net/spcpp/pfm20pub/>) に公開されています。