セコム認証サービス

セコムパスポート for G-ID
認証運用規定（Certification Practice Statement）

2016年7月29日
Version 11.20

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
V1.00	2002.7.4	初版発行
V1.50	2003.5.27	相互認証業務に関する記述の追記
V1.60	2003.8.18	フィンガープリントの公開に関する追記 fullCRL について追記 その他、用語の整理
V1.70	2004.6.24	情報開示申請手続に関する記述の追記 仕様変更手続きを変更 その他、用語の整理、表現の修正
V1.80	2005.5.23	リポジトリに公開する情報の URL 修正 RA 室における入退室管理
V1.90	2005.6.16	リポジトリに公開に関する修正 認証業務の終了に関する記述の追記 開示要求について
V1.91	2005.6.20	開示要求について、表現の修正
V2.00	2006.5.22	会社統合に伴い、会社名“セコムトラストネット”を“セコムトラストシステムズ”に変更 “セコムトラストネットセキュリティポリシ委員会”を“認証サービス改善委員会”に変更 CA 証明書の公開 URL の記載変更
V2.10	2006.6.7	表現の修正
V3.00	2006.7.3	加入者同意文書の変更 加入者の鍵ペア生成、送付手続きに IC カードシリーズを追加 文言修正
V4.00	2007.5.7	代理受取人について変更 証明書記載情報の拡張について変更 サポート窓口電話番号の変更 従事者適用基準の変更
V4.10	2007.6.21	文言修正 監査人の身分と資格、被監査対象との関係について記述修正
V4.20	2007.9.27	提出書類の追加（郵政民営化に伴う修正）
V4.30	2008.4.25	鍵の更新時期の修正
V4.40	2008.6.25	信頼される役割の修正 主な監査内容の修正
V4.50	2009.2.28	連絡先の変更 鍵更新後の自己署名証明書に関する記述の追記 生体認証設備を虹彩認証から静脈認証へ変更 PIN コード送付方法を配達記録郵便から簡易書留郵便へ変更 住民票の写しと同等とみなす証明書として「住民票記載事項証明書」を追加 文言変更
V4.60	2009.6.16	リンク証明書に関する記載の追記 自己発行証明書に関する記述の追記 リポジトリに公開する情報の追記 CRL に関する説明の追記 セキュリティオフィサの役割を追加 自己署名証明書に関する記載の変更 文言変更

V5.00	2010.12.3	行政書士電子証明書追加 外国人の登録の追加(行政書士電子証明書のみ) 旧姓での登録の追加 文言修正
V5.10	2011.1.27	変更履歴欄の文言修正
V6.00	2011.10.20	司法書士電子証明書追加
V6.10	2011.10.20	ダウンロードシリーズの加入者鍵ペアの削除の記載修正 人事上のセキュリティ管理に関する「社員」の記載修正
V6.20	2012.6.8	文言修正 連絡先 FAX 番号追加 用語追加
V6.30	2012.7.9	外国人の真偽確認書類変更 文言修正
V7.00	2012.8.5	税理士用電子証明書追加
V8.00	2012.10.26	社会保険労務士電子証明書追加
V8.10	2013.6.18	「住民票の写し」、「住民票記載事項証明書」又は「広域交付住民票」に文言統一 「戸籍全部事項証明書」、「戸籍個人事項証明書」、「戸籍謄本」又は「戸籍抄本」に文言統一 取消申請時の第三者からの届出の文言修正
V8.20	2013.11.8	登記を必要としない法人の提出書類を追加
V9.00	2014.3.30	タイプ A の削除 バックアップセンターの設置 ARL の発行頻度の変更 第三者からの届出の手続きの修正
V9.10	2014.4.19	システム更改に伴う修正
V9.20	2014.5.22	CA の鍵の更新間隔の修正
V9.30	2014.7.3	参照する CP の目次番号の修正
V10.00	2014.9.5	土地家屋調査士電子証明書追加 加入者の真偽の確認方法の追加
V11.00	2014.10.16	暗号アルゴリズム移行に伴う修正 タイプ B の IC カードシリーズの削除 「2.10 個人情報保護」の修正 「自己発行証明書」を「リンク証明書」に文言修正 他文言修正
V11.10	2016.7.6	「情報開示要求申請書」を「開示申請書」に修正 開示申請書への自署を削除 電子署名法施行規則第五条第一項第一号イの身分証明書を提示する方法による開示要求を削除 個人番号（マイナンバー）の扱いについて追記 文言修正
V11.20	2016.7.29	司法書士電子証明書にて開示申請書の実印を利用申込時と同一の印章に変更

セコムパスポート for G-ID 認証運用規定（Certification Practice Statement、以下、「本 CPS」という）は、Network Working Group Request for Comments:2527“Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”に準拠した構成で記述される。

「1. はじめに」では、セコムパスポート for G-ID サービスの概要を記述する。

「2. 一般規定」では、電子証明書の登録、発行、使用にかかわる一般的な条項を記述する。

「3. 識別と認証」に関する事項はセコムパスポート for G-ID 証明書ポリシ(Certificate Policy、以下、「CP」という)に記述する。

「4. オペレーション要件」では、電子証明書の発行、取消等に関する手続きを中心に記述する。

「5. 物理的、手続き上、人事上のセキュリティ管理」では、入退管理、鍵管理及び発行機関を運用する要員の人事面の管理を中心に記述する。

「6. 技術的セキュリティ管理」では、セコムパスポート for G-ID サービスで使用される CA の鍵に関する技術的側面を記述する。

「7. 電子証明書と CRL のプロファイル」に関する事項は CP に記述する。

「8. 仕様の管理」では、本文書の変更に係る手続き等を記述する。

1.はじめに

1.1 概要

1.1.1 認証機関と運用規定

本 CPS は、認証機関（Certification Authority：以下、「CA」という）が行う電子証明書の発行、取消、電子証明書を基礎とする公開鍵インフラストラクチャ（PKI：Public Key Infrastructure）の運用維持に関する諸手続きを規定したものである。

本 CPS は、セコムトラストシステムズ株式会社（以下、「セコムトラストシステムズ」という）が提供するセコム認証サービスのうち、「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）の特定認証業務の認定を取得した業務（以下、「認定認証業務」という）を行うセコムパスポート for G-ID サービス（以下、「本サービス」という）の CPS である。

本サービスの加入者は、CP、本 CPS 及び加入者利用規定の内容を加入者自身の利用目的に照らして評価し承諾する必要がある。また、利用者は、利用者利用規定、CP、本 CPS の内容を利用者自身の利用目的に照らして評価する必要がある。

本 CPS は、技術面、サービス面の発展や改良に伴い、それらを反映するために必要に応じ改訂されるものとする。

1.1.2 CP、CPS、加入者利用規定及び利用者利用規定

セコムトラストシステムズは、本サービスの提供にあたり、自らのポリシ及び保証並びに加入者又は利用者の義務等を、CP、本 CPS、加入者利用規定及び利用者利用規定によって包括的に定める。なお、それぞれの文書間で内容が抵触する場合は、CP、本 CPS、加入者利用規定又は利用者利用規定の順に優先して適用されるものとする。

これらの文書は、加入者、利用者及び BCA がいつでも閲覧できるように本サービスのリポジトリに公開する

http://repository.secomtrust.net/PassportFor/G-ID/
https://repository.secomtrust.net/PassportFor/G-ID/

(1) CP

CP は、電子証明書の目的、適用範囲、電子証明書プロファイル、本人確認方法及び加入者の鍵管理に関する事項を中心に記述した文書である。

(2) CPS

本 CPS は、本サービスの運用に係る事項及び認証業務にかかわる一般的な規定を記述し

た文書である。本 CPS の記述は RFC2527 に準拠し、必要に応じて、CP、加入者利用規定及び利用者利用規定を参照する。

(3) 加入者利用規定

加入者利用規定は、サービス内容や加入者の義務など、加入者とセコムトラストシステムズ間の契約内容を記述した文書である。

(4) 利用者利用規定

利用者利用規定は、利用者が本サービスで発行された電子証明書を信頼して利用するにあたっての規定を記述した文書であり、利用者に適用される。

1.2 正式名称

本 CPS の正式名称は「セコムパスポート for G-ID 認証運用規定」という。本サービスの運営母体であるセコムトラストシステムズには、ISO 割当に従ったオブジェクト識別子(以下、「OID」という)が割り当てられている。

組織名	OID
セコムトラストシステムズ株式会社（SECOM Trust Systems Co.,Ltd.）	1.2.392.200091

本 CPS は、次の OID により識別される。

CPS	OID
セコムパスポート for G-ID 認証運用規定	1.2.392.200091.100.601.1

本 CPS は、本サービスの CP に適用されると共に、これをサポートしている。本サービスの CP については、本 CPS「2.6.4 リポジトリ」に記載された URL から最新版を入手できる。

本 CPS がサポートする CP とその OID は、次のとおりである。本サービスが電子証明書発行サービスを追加した場合は、CP とその OID が追記される。

CP	OID
セコムパスポート for G-ID 証明書ポリシ① (署名アルゴリズム：Sha1WithRSAEncryption)	1.2.392.200091.100.621.1
セコムパスポート for G-ID 証明書ポリシ② (署名アルゴリズム：Sha256WithRSAEncryption)	1.2.392.200091.100.621.11

1.3 本サービスの関係者

1.3.1 CA

本サービスのシステムには、Entrust 社の PKI システムを採用する。本サービスのシステムは、CA サーバー、RA 端末、受付サーバー及びリポジトリから構成される。電子証明書発行のための加入者情報の登録や発行、取消の処理は、RA 端末から Entrust PKI インタフェースを通じて安全に CA サーバーにオンラインでアクセスして行われる。受付サーバーは、加入者の鍵ペアを生成した後、CA に加入者証明書発行を要求するインタフェースの役割をもつ。本サービスにおいてこれらの機能の運用に従事する関係者は、サービス責任者、サービス運用管理者、CA 管理者、RA 担当者、ログ検査者及び業務の一部を委託する場合には委託先の業務の要員等である。それぞれの役割については本 CPS「5.2.1 信頼される役割」において記述される。

1.3.2 加入者、利用者及び所属組織

(1) 加入者

加入者とは、本サービスを利用し、CA から秘密鍵の生成、加入者証明書の発行を受ける個人をいう。加入者は、加入者自身の秘密鍵及び加入者証明書の管理責任を負う。

(2) 利用者

利用者とは、加入者証明書を信頼して利用する者をいい、署名検証者と同義である。利用者は、CP、本 CPS 及び利用者利用規定の内容を利用者自身の利用目的に照らして評価したうえで利用しているとみなされる。

(3) 所属組織

所属組織とは、加入者の所属する組織をいう。

1.3.3 ブリッジ認証局

行政機関の認証局と民間の認証局との中間に位置し、政府認証基盤（Government Public Key Infrastructure：以下、「GPKI」という）のもとに政府により運営される CA である。本サービスでは、ブリッジ認証局（Bridge CA：以下、「BCA」という）との相互認証を行う。

1.4 連絡先

本 CPS の維持・管理は、セコムトラストシステムズの認証サービス改善委員会が行う。CP、本 CPS、加入者利用規定及び利用者利用規定に関する問い合わせ窓口は次のとおりである。

認証事業者　　：名称　セコムトラストシステムズ株式会社
　　住所　〒150-0001　東京都渋谷区神宮前 1-5-1

連絡先
本サービス窓口　：名称　セコムトラストシステムズ株式会社　CA サポートセンター

　　：住所　〒181-8528　東京都三鷹市下連雀 8-10-16 セコム SC センター

受付時間　　：営業日のみ　9:00～12:00　13:00～17:00
　　営業日＝土曜、日曜、祭日及び年末年始休暇
　　（12 月 31 日から 1 月 3 日）を除く、平日
電話　　：0422-76-2072
FAX　　：0422-76-2407　※受信のみ
電子メールアドレス：gid-support@ml.secom-sts.co.jp

2. 一般規定

2.1 義務

2.1.1 CA の義務

セコムトラストシステムズは本サービスの提供にあたり、加入者、利用者及び BCA に対して次の義務を負う。

- CP 及び本 CPS に記述したポリシと手順に従い、電子証明書の発行、取消の管理を行うこと。
- 加入者に対して、加入者証明書に関する申請に際し、正確な情報の提供を求めること。
- BCA に対して、相互認証証明書に関する申請に際し、BCA の定める手続きにより正確な情報の提供を求めること。
- 加入者証明書の利用申込の際に、加入者から提供される情報を誤りなく加入者証明書に反映すること。
- 相互認証証明書の申請の際に、BCA から提供される情報を誤りなく相互認証証明書に反映すること。
- 加入者に対して、虚偽の利用申込により不実の証明をした場合は、電子署名法第 41 条により罰せられることを周知すること。
- CP 及び本 CPS に記述したポリシと手順に従い、電子証明書発行、取消をする CA サーバーを 1 日 24 時間、1 週間 7 日運用すること。ただし、保守等を行うために CA サーバーを停止する場合を除く。
- CP 及び本 CPS に記述したポリシと手順に従い、利用者が CRL/ARL/fullCRL を参照するためのディレクトリサーバーを 1 日 24 時間、1 週間 7 日運用すること。ただし、保守等を行うためにディレクトリサーバーを停止する場合を除く。
- CP 及び本 CPS に記述したポリシと手順に従い、本 CPS「1.4 連絡先」に記載した受付時間に問い合わせを受け付けること。
- CRL/ARL/fullCRL の発行及び公表は、本 CPS「2.6 公表とリポジトリ」に基づいて行うこと。
- CP、本 CPS、加入者利用規定、利用者利用規定、CA の自己署名証明書、リンク証明書、相互認証証明書、CRL/ARL/fullCRL 及び CA の自己署名証明書とリンク証明書の値を SHA-1 又は SHA-256 で変換した値（以下、「フィンガープリント」という）を公開し、公開するフィンガープリントには改ざん防止措置を施すこと。なお、CA の自己署名証明書は、CA の鍵更新後、新旧 2 枚存在する。

2.1.2 加入者の義務

加入者は、本サービスにおいて次の義務を負う。

・ 加入者は、本サービスの加入者証明書に関する申請をする時点で、CP、本 CPS 及び加入者利用規定のすべての内容を理解し、承諾していること。
・ 発行された加入者証明書を利用目的外に使用しないこと。
・ 加入者は、電子署名が自署や押印に相当する法的効果を認められ得るものであることを承知し、秘密鍵が危殆化しないよう、秘密鍵及びそれに係る PIN コードの盗難、紛失、他者による不正利用等を防ぐことに対し十分な注意を払い、安全に管理すること。
・ 加入者の秘密鍵が盗難、漏えい、紛失、他者による不正利用等により加入者証明書の信頼性を喪失した可能性がある場合、加入者の秘密鍵が危殆化し機密性が失われた場合又はその可能性がある場合、加入者証明書の記載情報に変更が生じた場合、加入者証明書の記載情報・利用目的が正しくない場合、加入者証明書の利用を中止する場合は、速やかに加入者証明書の取消をセコムトラストシステムズに申請すること。なお、退職、異動、死亡などの理由により、加入者本人が加入者証明書の取消を申請出来ない場合は、第三者からその旨を届け出ること。
・ 加入者証明書の利用申込の際、利用目的を確認し、利用申込の内容は正確な情報を申告すること。なお、虚偽の利用申込をして、不実の証明をさせた場合には罰せられる。
・ 発行された加入者証明書の記載情報、利用目的を受領時に確認し、かつその後も随時確認することで、その加入者証明書の記載情報、利用目的がすべて正しいことを加入者自らが保証すること。
・ 加入者が加入者証明書を利用する場合における電子署名方式は、ハッシュアルゴリズムとして SHA-1、SHA-256、SHA-384 又は SHA-512 を用いた RSA 方式とすること。
・ 加入者は所属組織に対して、加入者証明書の記載情報に変更が発生し、加入者からの取消申請が困難な場合は、所属組織からセコムトラストシステムズに通知するように説明をし、促すこと。

2.1.3 利用者の義務

利用者は、本サービスにおいて次の義務を負う。

・ 加入者証明書を信頼する時点で、CP、本 CPS 及び利用者利用規定のすべての内容を理解し、承諾していること。
・ 加入者証明書を信頼する時点で、その加入者証明書の利用目的が自己の利用目的に合致していることを承諾していること。
・ 加入者証明書を信頼する前に、CA の自己署名証明書及び必要に応じてリンク証明書を用いて、当該加入者証明書に行われた電子署名を検証することにより、当該加入者証明書の発行者を確認すること。
・ 加入者証明書を信頼する前に、フィンガープリントを確認し、本サービスの CA の自己署

名証明書及び必要に応じてリンク証明書であることを確認すること。
・ 加入者証明書を信頼する前に、その加入者証明書の有効期間の確認を行うこと。
・ 加入者証明書を信頼する前に、その加入者証明書が取消されていないことを CRL 又は fullCRL によって確認すること。

2.2 CA の責任

2.2.1 保証

セコムトラストシステムズは、CP 及び本 CPS に規定した内容を遵守して電子証明書の発行、取消を含む認証サービスを提供し、CA 秘密鍵の信頼性を含む認証業務の信頼性の確保を保証する。

2.2.2 一定の損害に対する免責

セコムトラストシステムズは、本 CPS「2.2.1 保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害又は派生的損害に対する責任を負わず、また、いかなる逸失利益、データの紛失又はその他の間接的若しくは派生的損害に対する責任を負わない。ただし、セコムトラストシステムズに故意又は重大な過失がある場合はこの限りではない。

2.2.3 免責

本 CPS「2.2.1 保証」の内容に関し、次の場合、セコムトラストシステムズは責任を負わないものとする。ただし、セコムトラストシステムズに故意又は重大な過失がある場合はこの限りではない。
・ セコムトラストシステムズに起因しない不法行為、不正使用並びに過失等により発生する一切の損害
・ 加入者、利用者又は BCA が自己の義務の履行を怠ったために生じた損害
・ 加入者、利用者又は BCA のシステムに起因して発生した一切の損害
・ 加入者、利用者のソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
・ 加入者が契約に基づく契約料金を支払っていない間に生じた損害
・ セコムトラストシステムズの責に帰することのできない事由で電子証明書及び CRL/ARL/fullCRL に公開された情報に起因する損害
・ セコムトラストシステムズの責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
・ 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害

・ 天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、CA 業務停止を含む本サービスの業務停止に起因する一切の損害

2.2.4 損害賠償及びその制限

本サービスの電子証明書又は本サービスの電子証明書に関連して発生する取引の件数、電子署名の数、損害を被った加入者や利用者の人数、あるいは訴訟の原因に関係なく、一枚の電子証明書に起因する当社の賠償限度額は、金 1,000,000 円を超えないものとする。

2.3 取引にかかわる法律上の責任

電子証明書を使用した取引にかかわる法律上の責任は、取引の当事者である加入者又は利用者が負うものとし、セコムトラストシステムズは一切の責任を負わないものとする。

2.4 解釈及び執行

2.4.1 準拠法及び管轄等

CA、加入者及び利用者の所在地にかかわらず、CP、本 CPS、加入者利用規定及び利用者利用規定の解釈、有効性及び本サービスにかかわる紛争については、日本国の法律が適用される。仲裁及び裁判地は東京都区内における紛争処理機関を専属的管轄とする。

2.4.2 一部無効、存続、包括的合意、通知

(1) 一部無効

CP、本 CPS、加入者利用規定及び利用者利用規定の一部の条項が無効であったとしても、当該文書に記述された他の条項は有効であるものとする。

(2) 存続

加入者とセコムトラストシステムズとの間で本サービス利用契約を終了する場合であってもその性質上、存続されるべき条項は終了の事由を問わず加入者とセコムトラストシステムズに適用されるものとする。

(3) 包括的合意

セコムトラストシステムズは、本サービスの提供にあたり、自らのポリシ及び保証並びに加入者又は利用者の義務等を CP、本 CPS、加入者利用規定及び利用者利用規定によって包括的に定め、これ以外の口頭や書面を問わず、いかなる合意も効力を有しないものとする。

(4) 通知

本サービスは、加入者及び利用者に対する必要な通知をホームページ上、電子メール又は書面によって行う。

2.4.3 紛争解決手続き

本サービスの利用に関し、セコムトラストシステムズに対して訴訟、仲裁を含む解決手段に訴えようとする場合、セコムトラストシステムズに対して事前にその旨を通知するものとする。

2.5 料金

タイプ B 及び行政書士電子証明書の料金に関しては、セコムトラストシステムズホームページ（http://www.secomtrust.net/service/ninsyo/forgid.html）及び加入者利用規定に定める。

司法書士電子証明書、税理士用電子証明書、社会保険労務士電子証明書及び土地家屋調査士電子証明書の料金に関しては、日本司法書士会連合会（以下、「日司連」という）、日本税理士会連合会（以下、「日税連」という）、全国社会保険労務士会連合会（以下、「社労士会連合会」という）及び日本土地家屋調査士会連合会（以下、「日調連」という）の各連合会のホームページに掲載する。

2.6 公表とリポジトリ

2.6.1 リポジトリに公表する情報

CA は次の内容をリポジトリに格納し、加入者及び利用者等がオンラインによって閲覧できるようにする。

- 電子証明書取消リスト（CRL/ARL/fullCRL）
- CA の自己署名証明書
- リンク証明書
- 相互認証証明書
- CP、本 CPS、加入者利用規定及び利用者利用規定
- 相互認証した CA の名称及びその他関連情報
- CP 及び本 CPS に基づく電子証明書に関するその他関連情報
- フィンガープリント

2.6.2 公表の頻度

本 CPS は、本 CPS「8. 仕様の管理」に記述されているとおり随時変更の都度公表される。

CRL/ARL/fullCRL は発行の都度、リポジトリに公表される。CRL/ARL/fullCRL の発行の頻度は、本 CPS「4.5.3 CRL/ARL/fullCRL の発行頻度」で規定される。

自己署名証明書、リンク証明書及び相互認証証明書は、発行及び更新の都度、リポジトリに公表される。

2.6.3 アクセスコントロール

リポジトリは加入者及び利用者に対して 1 日 24 時間、1 週間 7 日参照可能とする。ただし、保守等を行うためにリポジトリを停止する場合を除く。

2.6.4 リポジトリ

本サービスは、CRL/ARL/fullCRL 情報にアクセスできるようにリポジトリを維持管理する。リポジトリは Web、及び X.500 ディレクトリシステムを使用しており、アクセスに用いるプロトコルは HTTP（HyperText Transfer Protocol)、HTTPS（HTTP に SSL によるデータの暗号化機能を付加したプロトコル）又は LDAPv3（Light Weight Directory Access Protocol バージョン(3)）を用いる。リポジトリ内の情報は EntrustPKI アプリケーション又は Web インタフェース等を通じてアクセス可能である。なお、本サービスは、加入者証明書を公開しない。

表 2.6-1 リポジトリに公開する情報

リポジトリ	・ https://repository.secomtrust.net/PassportFor/G-ID/
CP	・ https://repository.secomtrust.net/PassportFor/G-ID/repository/CP.pdf
CPS	・ https://repository.secomtrust.net/PassportFor/G-ID/repository/CPS.pdf
CA 証明書（自己署名証明書)	・ https://repository.secomtrust.net/PassportFor/G-ID/repository/g-idca02.crt（第二世代） ・ https://repository.secomtrust.net/PassportFor/G-ID/repository/g-idca03.crt（第三世代） ・ ldap://repository.secomtrust.net/ou=SECOM%20Passport%20for%20G-ID,o=SECOM%20Trust.net%20Co.%2c%20Ltd.,c=JP?cACertificate
フィンガープリント	・ https://repository.secomtrust.net/PassportFor/G-ID/fingerprint.html
リンク証明書	・ https://repository.secomtrust.net/PassportFor/G-ID/repository/g-idca03-NewWithOld.crt（第二、三世代間の NewWithOld） ・ https://repository.secomtrust.net/PassportFor/G-ID/repository/g-idca03-OldWithNew.crt（第二、三世代間の OldWithNew） ・ ldap://repository.secomtrust.net/ou=SECOM%20Passport%20for%20G-ID,o=SECOM%20Trust.net%20Co.%2c%20Ltd.,c=JP?cACertificate
相互認証証明書	・ ldap://repository.secomtrust.net/ou=SECOM%20Passport%20for%20G-ID,o=SECOM%20Trust.net%20Co.%2c%20Ltd.,c=JP?crossCertificatePair

加入者利用規定	・ https://repository.secomtrust.net/PassportFor/G-ID/repository/kanyusya.pdf ・ https://repository.secomtrust.net/PassportFor/G-ID/repository/kanyusya_shiho.pdf（司法書士電子証明書） ・ https://repository.secomtrust.net/PassportFor/G-ID/repository/kanyusya_zei.pdf（税理士用電子証明書） ・ https://repository.secomtrust.net/PassportFor/G-ID/repository/kanyusya_sharo.pdf（社会保険労務士電子証明書） ・ https://repository.secomtrust.net/PassportFor/G-ID/repository/kanyusya_tochi.pdf（土地家屋調査士電子証明書）
利用者利用規定	・ https://repository.secomtrust.net/PassportFor/G-ID/repository/riyosya.pdf
CRL	・ldap://repository.secomtrust.net/cn=CRL<n>※1,ou=SECOM%20Passport%20for%20G-ID,o=SECOM%20Trust.net%20Co.%2c%20Ltd.,c=JP?certificateRevocationList
ARL	・ldap://repository.secomtrust.net/cn=CRL1,ou=SECOM%20Passport%20for%20G-ID,o=SECOM%20Trust.net%20Co.%2c%20Ltd.,c=JP?authorityRevocationList
fullCRL	・ http://repository.secomtrust.net/PassportFor/G-ID/repository/CRL.crl （第二世代の CA 秘密鍵で署名した CRL） ・ http://repository.secomtrust.net/PassportFor/G-ID/repository1/CRL.crl （第三世代の CA 秘密鍵で署名した CRL） ・ ldap://repository.secomtrust.net/ou=SECOM%20Passport%20for%20G-ID,o=SECOM%20Trust.net%20Co.%2c%20Ltd.,c=JP?certificateRevocationList

※1 エントリ数が一定量増えるたびに、CRL1,CRL2,CRL3,…,CRL<n>と n の値も増える。

2.7 準拠性監査

2.7.1 監査の頻度

セコムトラストシステムズは、本サービスが CP 及び本 CPS に準拠して運営されているかに関して、年に１回以上の定期監査を行う。また、認証サービス改善委員会が必要と認めた場合は、不定期に監査を実施する。

2.7.2 監査人の身分と資格

準拠性監査は、十分な監査経験を有する監査人が行うものとする。

2.7.3 監査人と被監査対象との関係

監査人は、監査に関する事項を除き、被監査部門の業務から独立した外部監査人又は、社内監査部門等とする。監査の実施にあたり、被監査部門は監査に協力するものとする。

2.7.4 監査対象

定期監査では、本サービスの CA が CP 及び本 CPS に準拠して運営されているかを中心に監査する。主な監査内容は、次のとおりである。

- 本 CPS「5.2.1 信頼される役割」で登場する担当者の業務運用
- CA 秘密鍵の管理
- 加入者証明書の発行・取消
- ソフトウェアの機能
- ハードウェアプラットフォーム及びネットワーク監視システム
- 物理的環境
- セキュリティ技術の最新動向を踏まえた設備、規定等の妥当性評価等

不定期監査は、認証サービス改善委員会が必要と認めた場合に、認証サービス改善委員会の定めた監査目的に基づいて実施する。

2.7.5 監査指摘事項への対応

監査報告書で指摘された事項（通常改善事項又は緊急改善事項）に関しては、認証サービス改善委員会が対応を決定する。この指摘事項に関しては、認証サービス改善委員会が、セキュリティ技術の最新の動向を踏まえ、問題が解決されるまでの対応策も含め、その措置を本サービスのサービス運用管理者に指示する。講じられた対策の結果は認証サービス改善委員会に報告され、評価されるとともに、次の監査において確認される。

2.7.6 監査結果の報告

監査報告書は、監査人から認証サービス改善委員会に提出される。監査報告書の開示は、認証サービス改善委員会の判断によるものとする。

2.7.7 監査調書及び監査報告書の保存

定期及び不定期監査の実施に係る監査調書及び監査報告書は、保管管理者を定め、許可されたものだけがアクセスできるよう保管管理する。監査報告書の保管期間は関連する電子証明書の有効期間の満了から 10 年とする。

2.8 機密保持

2.8.1 機密情報の保護

セコムトラストシステムズが保持する本サービスに係る加入者及び BCA の情報は、電子証明書、CRL/ARL/fullCRL、CP、本 CPS、加入者利用規定及び利用者利用規定の一部として明示的に公表されたものを除き、機密保持対象として扱われる。セコムトラストシステムズは、法の定めによる場合又は個人の書面による事前の承諾を得た場合を除いてこれらの情報を社外に開示しない。係る法的手続き、司法手続き、行政手続きあるいは法律で要求されるその他の手続きに関連してアドバイスする法律顧問及び財務顧問に対し、セコムトラストシステムズは機密保持対象として扱われる情報を開示することができる。また、会社の合併、買収あるいは再編成に関連してアドバイスする弁護士、会計士、金融機関及びその他の専門家に対しても、セコムトラストシステムズは機密保持対象として扱われる情報を開示することができる。

加入者の秘密鍵は、その加入者によって機密保持すべき情報である。本サービスは、これらの鍵へのアクセス手段を保有せず、いかなる場合でもこれらの鍵へのアクセス手段を提供していない。

監査ログに含まれる情報及び監査報告書は、機密保持対象情報である。セコムトラストシステムズは、本 CPS「2.7.6 監査結果の報告」に記載されている場合及び法の定めによる場合を除いて、これらの情報を社外へ開示しない。

2.8.2 機密保持対象外の情報

電子証明書及び CRL/ARL/fullCRL に含まれている情報は機密保持対象外として扱う。その他、次の状況におかれた情報は機密保持対象外とする。

- セコムトラストシステムズの過失によらず知られた、あるいは知られるようになった情報
- セコムトラストシステムズ以外の出所から、機密保持の制限無しにセコムトラストシス

テムズに知られた、あるいは知られるようになった情報
- セコムトラストシステムズによって独自に開発された情報
- 開示に関して加入者又はBCAによって承認されている情報

2.8.3 電子証明書取消情報の開示

加入者証明書が取消される場合、取消された加入者証明書の取消事由、取消日時がCRL/fullCRL 情報に含まれる。相互認証証明書が取消される場合は取消事由、取消日時がARL/fullCRL情報に含まれる。この取消事由のコードは機密とみなされず、加入者、利用者及びBCAに公開される。取消に関するその他の詳細情報は原則として開示しない。

2.8.4 法執行機関への開示

本サービスで取扱う情報に関して、法的根拠に基づいて情報を開示するように請求があった場合、セコムトラストシステムズは法の定めに従って法執行機関へ情報を開示する。

2.8.5 民事手続き上の開示

セコムトラストシステムズは、調停、訴訟、その他の法的、裁判上又は行政手続きの過程において、裁判所、弁護士その他の法律上権限を有する者から任意の開示要求があった場合、機密保持対象である情報を開示することができる。

2.8.6 加入者証明書の名義人からの要求に基づく開示

セコムトラストシステムズは、加入者証明書の名義人から権利又は利益を侵害される若しくは侵害されるおそれがあるとの申し出があった場合は、本人確認の後、利用申込時に加入者から提出された当該者に係る情報及び加入者証明書の記載情報を郵送により開示する。

開示の申請方法は、開示申請書に自署（※1）、実印（※2）の押印及び必要事項を記載し、郵送又は持参（※3）による申請とする。開示申請書を利用しない開示申請は認めない。利用申込時点から印章の変更があった場合は、実印による押印を行い、「印鑑登録証明書」を添付し申請する。また、利用申込時点から氏名の変更があった場合は、「戸籍全部事項証明書」、「戸籍個人事項証明書」、「戸籍謄本」又は「戸籍抄本」を添付し申請する。なお、外国籍の方で利用申込時点から氏名の変更があった場合は「住民票の写し」（※4）を添付する。

本人確認は開示申請書に押印された印影と利用申込時の利用申込書に押印された印影を比較し確認する。押印された印影が利用申込時と異なる場合、開示申請書に押印された印影と添付された「印鑑登録証明書」の印影の比較、開示申請書に記載された氏名(外国籍の方は氏名又は通称名)と利用申込時の利用申込書に記載された氏名(外国籍の方は氏名又は通称名)の比較により確認する。

（※1）司法書士電子証明書のみ適用。
（※2）司法書士電子証明書では、利用申込時と同一の印章を押印する。
（※3）タイプ B、行政書士電子証明書、土地家屋調査士電子証明書は除く。
（※4）「住民票の写し」は行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成 25 年 5 月 31 日法律第 27 号）の第 2 条第 5 項に規定されている個人番号（マイナンバー）の記載がないものとするが、加入者本人が個人番号（マイナンバー）を記載した住民票を送付した場合には、個人番号（マイナンバー）を復元できない程度にマスキング（墨塗り）した上で保管する。

2.8.7 その他の事由に基づく情報開示

前述した以外のその他の事由に基づく情報開示は行わない。

2.9 知的所有権

セコムトラストシステムズと加入者又は BCA との間で別段の合意がなされない限り、本サービスにかかわる情報資料及びデータは、次に示す当事者の権利に属するものとする。

・加入者証明書	：	セコムトラストシステムズに帰属する財産である
・相互認証証明書	：	セコムトラストシステムズが電子署名を施した相互認証証明書について、セコムトラストシステムズに帰属する財産である
・CRL/ARL/fullCRL	：	セコムトラストシステムズに帰属する財産である
・識別名（DN）	：	加入者証明書に対して対価が支払われている限りにおいて、その名前が付与された者に帰属する財産である
・EntrustPKI	：	ソフトウェア、それに関連する著作権、商標及び特許権はエントラスト社が所有しており、エントラスト社が独占的権利を持つ
・加入者の秘密鍵	：	秘密鍵は、その保存方法又は保存媒体の所有者にかかわらず、公開鍵と対になる秘密鍵を所有する加入者に帰属する財産である
・加入者の公開鍵	：	保存方法又は保存媒体の所有者にかかわらず、対になる秘密鍵を所有する加入者に帰属する財産である
・CP、本 CPS、加入者利用規定及び利用者利用規定	：	セコムトラストシステムズに帰属する財産（著作権を含む）である

CP 及び本 CPS に記載された著作権の表示が CP 及び本 CPS のコピーに維持されており、CP 及び本 CPS が省略されることなく完全にかつ正確に再現されていることを条件に、CP 及び本 CPS を非独占的に複製又は無償で頒布することを許可する。

2.10 個人情報保護

セコムトラストシステムズは、個人情報の重要性を認識し、次のように取扱う。

(1) 個人情報を取扱う部門ごとに管理責任者を置き、個人情報の適切な管理を行う。

(2) 個人情報を収集する場合、収集目的を知らせた上で、必要な範囲の情報のみを適法かつ公正な手段で収集する。

(3) 本サービスにおいて加入者から提出を受けた個人情報は、電子署名法に基づく本サービスを提供するために必要な情報であり、利用目的は以下のとおりである。

- 加入者との契約上の責任を果たすため
- 加入者へよりよいサービスを提供するため
- 加入者へ有用な情報を提供するため
- その他の正当な目的のため

(4) 加入者の同意がある場合及び法令に基づく場合を除き、個人情報を業務委託先以外の第三者に開示することはしない。業務委託先に開示する場合は、当該業務委託先に対し本書と同等の条件を義務付けるものとする。

(5) 個人情報の管理責任者は、適切な安全対策を講じて、個人情報を不正アクセス、滅失、毀損、改ざん、漏えい等から保護する責任を持ち、これに努める。

(6) 加入者自身の個人情報について開示を求められた場合、第三者への個人情報の漏えいを防止するため、加入者自身であることがセコムトラストシステムズにおいて確認できた場合に限り、セコムトラストシステムズにおいて保管している加入者の個人情報を本人に開示する。加入者はセコムトラストシステムズに開示を求める場合、書面による申請を行うものとする。

(7) 加入者の個人情報に誤りや変更がある場合には、加入者からの申し出に基づき、合理的な範囲で速やかに、不正確な情報又は古い情報を修正又は削除する。

(8) セコムトラストシステムズは、社員に対して個人情報保護の教育啓蒙活動を実施する。

(9) 加入者の個人情報に関して適用される法令、規範を遵守するとともに、適切な個人情報保護を維持するために、個人情報保護のポリシを適宜見直し、改善を行う。

2. 11 財務基盤

セコムトラストシステムズは、本サービスの提供にあたり、十分な財務的基盤を維持するものとする。

3 識別と認証

3.1 名前に関する要件

本項は、CP「3.3.2 名前に関する要件」を参照のこと。

3.2 秘密鍵の所有を証明する方法

本項は、CP「3.4 秘密鍵の所有を証明する方法」を参照のこと。

3.3 本人確認

加入者証明書の発行、取消時の本人確認は CP「4.電子証明書の発行、取消」にて記述している方法によって行う。相互認証証明書に係る手続き時の本人確認は、BCA と事前に定める手続きによって行う。

4. オペレーション要件

4.1 通信手段

加入者とセコムトラストシステムズとの間の通信手段は、電子メール、郵便による書面の送付(提出する書類が信書にあたる場合、加入者はセコムトラストシステムズに対して、信書として送付)又は手交を原則とするが、電話やFAXによる通信手段も有効とする。

BCAとセコムトラストシステムズとの間の通信手段は、BCAの定める手続きにより行われる。

4.2 電子証明書の申請

加入者は、CP「4.1.1 申込手続き及び本人確認」に規定された手続きにより加入者証明書の利用申込を行う。加入者は、加入者証明書の利用申込を行うにあたり、CP、本 CPS 及び加入者利用規定の内容を承諾しているものとする。すべての加入者証明書の利用申込は、CP「4.1.1 申込手続き及び本人確認」に規定された手続きによって審査される。

相互認証証明書の発行申請は、CP「4.2.1 相互認証申請」に規定された手続きにより行われる。

4.3 電子証明書発行

セコムトラストシステムズは、申請された加入者証明書を CP「4.1.2 加入者鍵ペア生成と電子証明書発行処理」に規定された手続きにより発行をする。

相互認証証明書の発行は、CP「4.2.2 相互認証証明書の発行」に規定された手続きにより行われる。

加入者証明書及び相互認証証明書の登録情報に関しては、CP「3.3.4 登録情報」にて規定する。

4.4 電子証明書の受領

セコムトラストシステムズで生成された加入者証明書、秘密鍵及びそれに係る PIN コード等は、CP「4.1.2 加入者鍵ペア生成と電子証明書発行処理」に規定された手続きによって加入者に送付される。加入者は、これらを受取った後、CP「4.1.3 電子証明書の受領」に規定された手続きによってセコムトラストシステムズまで受領の報告を行わなければならない。

相互認証証明書の受領は、CP「4.2.3 相互認証証明書の授受」に規定された手続きにより BCA から受領書を受取る。

4.5 電子証明書の取消

4.5.1 電子証明書取消処理

加入者は、CP「4.6 加入者証明書の取消」に規定された手続きによって、セコムトラストシステムズに加入者証明書の取消申請を行う。加入者証明書の取消処理は、セコムトラストシステムズによって行われ、取消処理の結果は CRL/fullCRL に反映される。

相互認証証明書の取消申請は、CP「4.7 相互認証証明書の取消」に規定された手続きにより行われる。相互認証証明書の取消処理の結果は ARL/fullCRL に反映される。

4.5.2 CRL/ARL/fullCRL 確認要件

本サービスによって発行される電子証明書には、電子証明書の検証の際に確認される「CRL 配布点（CRL Distribution Points)」が含まれている。利用者は電子証明書を信頼する前に、その電子証明書が取消されていないことを確認しなければならない。

利用者は、オンラインにおいて、電子証明書の CRL Distribution Points 拡張で識別される現在の CRL/ARL/fullCRL を確認することができる。オフラインで作業している場合、利用者は CRL/ARL/fullCRL の確認を完全に行うことができない。

また、CRL/ARL/fullCRL で確認できる電子証明書の取消情報は、セコムトラストシステムズによって取消を行ったもののみである。なお、本サービスでは有効期間の満了した電子証明書の有効性確認についての問い合わせに対しては応じない。

4.5.3 CRL/ARL/fullCRL の発行頻度

CRL/ARL/fullCRL は前回発行時から 23 時間以上 24 時間以下経過した時点で新たな CRL/ARL/fullCRL が発行される。ただし、加入者証明書の取消処理を行った場合はその時点で新たな CRL/fullCRL が発行される。また、相互認証証明書の取消処理を行った場合はその時点で新たな ARL/fullCRL が発行される。

4.6 電子証明書の一時停止

本サービスは、電子証明書の一時停止を行わない。

4.7 電子証明書の一時停止解除

本サービスは、電子証明書の一時停止解除を行わない。

4.8 セキュリティ監査の手順

4.8.1 記録されるイベントの種類

CA サーバー上で起こったイベントは、それが手動、自動であるかにかかわらず、日付、

時刻、イベントを発生させた主体、イベント内容等が監査ログファイルに記録される。

CA システムにおける運用の正当性を証明するために必要な監査ログとして、以下の操作等について履歴を記録する。

・CA 鍵の操作
・システムの起動･停止
・データベースの操作
・権限設定の変更履歴
・電子証明書の発行
・電子証明書の取消
・CRL/ARL/fullCRL の発行
・監査ログの検証
・RA 端末からの操作ログ

また、以下のような入退室や不正アクセスに関する履歴を記録する。

・CA サーバーが設置されている室（以下、「CA 室」という）、CA 関連サーバー等サービスの運用維持に必要なサーバーが設置されている室（以下、「関連サーバー室」という）、電子証明書の登録、取消等の作業を行う端末が設置されている室（以下、「RA 室」という）、CA 室、関連サーバー室及び RA 室に設置している設備と同様の設備を設置したバックアップセンターの室（以下、「BC 認証設備室」という）の入退室に関する記録
・認証業務用設備等への不正アクセスに関する記録

4.8.2 監査ログの処理頻度

セコムトラストシステムズは、監査ログを定期的に精査する。

4.8.3 監査ログの保存期間

監査ログは、最低 6 週間は CA サーバー内に保持される。その後、外部記憶媒体に、該当する電子証明書の有効期間の満了日から最低でも 10 年間は保存される。CA 室、関連サーバー室、RA 室、BC 認証設備室への入退室に関する記録や不正アクセスに関する記録は、次回の認定の更新日まで保存されるものとする。

4.8.4 監査ログの保護

セコムトラストシステムズは、認可された人員のみが監査ログファイルにアクセスすることができるようにするために権限者を定め、許可されていない者が閲覧することから保護する。

4.8.5 監査ログのバックアップ

監査ログは、CA サーバーデータベースとともに、外部記憶媒体にバックアップがとられ、それらの媒体は安全な施設に保管される。

4.8.6 監査ログの収集システム

監査ログの収集システムは、CA サーバーシステムに内在している。

4.8.7 イベントを引き起こした人への通知

本サービスでは、監査ログに記録されたイベントを引き起こした人、システム、又はアプリケーションに対して、一切の通知を行わない。

4.8.8 セキュリティ対策の見直し

本サービスにおいて用いるハードウェア及びソフトウェアは、適切なサイクルで最新のセキュリティテクノロジを導入すべく、必要に応じて随時設備の更新を行い、本 CPS 及び関連する文書の見直しを行う。

4.9 レコードの履歴（アーカイブ）

履歴が保管、記録される対象は、「電子署名法 施行規則第 12 条」の主務省庁で定める業務に関する帳簿書類（利用申込時に提出を受けた書類、監査ログファイル、CA サーバーデータベース等）である。

4.9.1 アーカイブの種類

4.9.1.1 CA システムで生成される電子データとしてアーカイブする情報

監査ログとして記録されるイベントの種類は、本 CPS「4.8.1 記録されるイベントの種類」に記載されている。CA システムで生成され、電子データとしてアーカイブされる情報としては次に挙げる情報がある。

- 監査ログ
- CA データベースのバックアップデータ
- CA 動作設定ファイル

4.9.1.2 紙、外部記憶媒体として保存する物

本サービスでは以下に掲げる運用関連記録のアーカイブを維持、管理する。

（ ）内は保管期間

- 加入者への説明の記録（該当する電子証明書の有効期間の満了日から最低 10 年間）
- 電子証明書の発行、取消時に提出を受ける申請書及び電子データ（該当する電子証明書

の有効期間の満了日から最低 10 年間）

- 加入者の真偽の確認のために提出を受けた書類及び電子データ（該当する電子証明書の有効期間の満了日から最低 10 年間）
- 行政書士電子証明書の発行に際して、加入者の行政書士資格者確認のために日本行政書士会連合会から提出を受けた書類及び電子データ（該当する電子証明書の有効期間の満了日から最低 10 年間）
- 司法書士電子証明書の発行に際して、加入者の司法書士資格が有効であることを日司連に確認した記録（該当する電子証明書の有効期間の満了日から最低 10 年間）。
- 税理士用電子証明書の発行に際して、加入者の税理士資格が有効であることを日税連に確認した記録（該当する電子証明書の有効期間の満了日から最低 10 年間）。
- 社会保険労務士電子証明書の発行に際して、加入者の社会保険労務士資格が有効であることを社労士会連合会に確認した記録（該当する電子証明書の有効期間の満了日から最低 10 年間）。
- 土地家屋調査士電子証明書の発行に際して、加入者の土地家屋調査士資格が有効であることを日調連に確認した記録（該当する電子証明書の有効期間の満了日から最低 10 年間）。
- 相互認証手続きに係る書類（該当する電子証明書の有効期間の満了日から最低 10 年間）
- 電子証明書の発行、取消申請に対する諾否を決定した者の氏名を記載した書類及び、申請に対して承諾をしなかった場合においてその理由を記載した書類（該当する電子証明書の有効期間の満了日から最低 10 年間）
- 発行した全ての電子証明書及びその作成に関する記録（該当する電子証明書の有効期間の満了日から最低 10 年間）
- CA の公開鍵及びその作成に関する記録（該当する電子証明書の有効期間の満了日から最低 10 年間）
- CA の秘密鍵の作成及び管理に関する記録（該当する電子証明書の有効期間の満了日から最低 10 年間）
- 加入者の秘密鍵の作成及び廃棄に関する記録、また、その受領に関する記録（該当する電子証明書の有効期間の満了日から最低 10 年間）
- 電子証明書の取消情報及び取消に関する記録（該当する電子証明書の有効期間の満了日から最低 10 年間）
- CP、本 CPS、加入者利用規定及び利用者利用規定、また、その変更に関する記録（該当する電子証明書の有効期間の満了日から最低 10 年間）
- 業務の手順に関して記載した書類、また、その変更に関する記録（該当する電子証明書の有効期間の満了日から最低 10 年間）
- 業務に従事する者の責任及び権限並びに指揮命令系統に関して記載した書類、また、その変更に関する記録（該当する電子証明書の有効期間の満了日から最低 10 年間）

- 認証業務の一部を他に委託する場合においては、委託契約に関する書類（該当する電子証明書の有効期間の満了日から最低 10 年間）
- 監査の実施結果に関する記録（該当する電子証明書の有効期間の満了日から最低 10 年間）
- 入退室管理装置に関する記録（作成した日から次回更新認定を受けた日まで）
- 不正アクセス防止措置に関する記録（作成した日から次回更新認定を受けた日まで）
- 認証業務用設備の動作に関する記録（作成した日から次回更新認定を受けた日まで）
- 認証業務用設備等への立ち入り及び操作の許諾に関する記録（作成した日から次回更新認定を受けた日まで）
- 認証業務用設備の維持管理に関する記録（作成した日から次回更新認定を受けた日まで）
- 本サービスにおける事故に関する記録（作成した日から次回更新認定を受けた日まで）
- 帳簿書類の利用及び破棄に関する記録（作成した日から次回更新認定を受けた日まで）
- 施設設備の保守管理に関する記録（作成した日から次回更新認定を受けた日まで）

4.9.2 アーカイブの保存期間

CA サーバーデータベースのアーカイブ及び監査ログファイルのアーカイブは、該当する電子証明書の有効期間満了日から最低でも 10 年間保存される。紙及び外部記憶媒体の保存期間に関しては、本 CPS「4.9.1.2 紙、外部記憶媒体として保存する物」のとおりである。

4.9.3 アーカイブの保護

CA サーバーデータベースは、暗号化され保護されている。CA サーバー上の監査ログについては、本 CPS「4.8.4 監査ログの保護」に記述のとおりである。

紙及び外部記憶媒体は物理的セキュリティによって、漏えい、滅失又は毀損等から保護され、セコムトラストシステムズが許可したもの以外アクセスできないように制限された施設に保存される。また、その施設は、温度、湿度、磁気等の環境上の脅威からも保護される。

4.9.4 アーカイブのバックアップ手順

CA サーバーデータベースは、自動的にサーバー上にバックアップがとられる。さらに、CA サーバーシステム、監査ログとともに外部記憶媒体に格納される。

4.9.5 アーカイブの収集システム

CA サーバーデータベース用の履歴収集システムは､CA サーバーシステムに内在している。監査ログファイル用の履歴収集システムについては、本 CPS「4.8.6 監査ログの収集システム」に記述のとおりである。

4.9.6 アーカイブ情報の検証

アーカイブデータは、媒体の耐性を考慮した定期的サイクルで可読性検証を行い、完全性、機密性の維持に留意し、新しい媒体へ複製する。

4.10 鍵の切り替え

CA の鍵の有効期間は 10 年と 30 分とし、CA の鍵の有効期間の残りが加入者証明書の最大有効期間よりも短くなる前に鍵の更新を行う。また、鍵の更新と同時に、リンク証明書を発行する。リンク証明書は、CA の鍵更新に伴い同時に存在することとなる新しい鍵ペアと古い鍵ペアの関係を保証するための電子証明書であり、新しい鍵で古い鍵を電子署名した電子証明書及び古い鍵で新しい鍵を電子署名した電子証明書が発行される。リンク証明書の有効期間は、古い自己署名証明書の残存有効期間までである。

CA 秘密鍵を用いて行う電子署名は、CA 秘密鍵の更新時を除いて、常に最新の鍵によって行われる。また、CA の鍵の切り替えは、自己署名証明書の記載情報変更時、及び上記に定めた更新期日に至った際に行われる。

4.11 信頼性喪失や災害からの復旧

不測の事態が発生した場合に速やかに復旧作業を実施できるよう、予め本サービスに関連するシステムの代替機の確保、復旧に備えたバックアップデータの確保、災害復旧のためのバックアップセンターの設置、復旧手続の策定等、可能な限り速やかに認証業務システムを復旧するための対策を行う。

なお、本サービスにおいて、CA 秘密鍵の危殆化若しくは危殆化のおそれがある場合及び災害等により利用者へ取消情報の提供が 72 時間を超えて停止する等の場合、障害発生の状況に応じて下記の必要な作業を実行し、安全な環境を修復する。

(1) CA 秘密鍵の危殆化若しくは危殆化のおそれがある場合は、サービスを停止し、被害状況及び原因を調査する。また、直ちに、発行したすべての加入者証明書、相互認証証明書及びリンク証明書について取消の手続きを行う。

(2) 障害発生の事実をリポジトリに掲載し、加入者、利用者に告知する。
なお、以下に挙げる状況が発生した場合においては、直ちに当該障害の内容、発生日時、措置状況等確認されている事項を主務省庁及び BCA に通報する。
- CA 秘密鍵の危殆化若しくは危殆化したおそれがある場合
- 利用者へ取消情報の提供が 72 時間を超えて停止し、利用者に対してその事実を告知できない場合

(3) 発生した不測事態の性質によって、CA 管理者、RA 担当者、セキュリティオフィサ、ログ検査者のパスワードをすべて変更する。

(4) 発生した不測事態の性質によって、入退室権限及び鍵の変更あるいは取消をする。

(5) ディレクトリが使用不能の場合、ディレクトリデータ、当該認定認証業務の運用電子証明書、及び取消情報をリストアする。ディレクトリ破壊の疑いがあった場合、バックアップからリストアする

4.11.1 窓口設置

災害や深刻な信頼性喪失からの復旧を行う場合には、加入者及び BCA に対して状況を通知できる体制をとり、さらに加入者、利用者及び BCA が状況確認を行えるよう専用窓口を設置し、告知する。告知方法は、電子メール若しくは郵便及びリポジトリ上の告知による。

4.11.2 復旧

CA 秘密鍵の危殆化有無の最終判断に従って、あらかじめ検討・準備されている対策、復旧手順を行う。正常な復旧を確認した後、加入者、利用者及び BCA に対して復旧を通知する。通知方法は、電子メール若しくは郵便及びリポジトリ上の告知等による。

4.11.3 電子証明書の再発行

CA の信頼性喪失を理由に取消を行った電子証明書については､CA の信頼性が回復した後、可能な場合は新たに生成された CA の秘密鍵を用いて、電子証明書を再発行する手続きを行う。

4.12 認証業務の終了

セコムトラストシステムズが本サービスによる認証業務を終了する場合には、最低 90 日以上前に加入者、利用者を含むその他の関係者に通知し、主務省庁及び BCA に届出る。本サービスにおいて発行されたすべての加入者証明書及び相互認証証明書は、サービスの終了日までに取消される。すべての加入者証明書及び相互認証証明書を取消した後、セコムトラストシステムズは加入者及び BCA に対して加入者証明書及び相互認証証明書の取消を通知する。また、サービスを終了した場合であっても、加入者証明書及び相互認証証明書は、全ての発行済み電子証明書の有効期間が満了するまでは、電子証明書に記載している CRL 配布点に最新の CRL/ARL/fullCRL の公開を実施する。加入者への終了に関する通知は電子メール又は書面にて行う。また、終了に関する情報をセコムトラストシステムズホームページ上で公表する。CA 秘密鍵及びその複製は、本 CPS「6.2.7 秘密鍵の破棄方法」により、復元不可能な状態にする。

5. 物理的、手続き上、人事上のセキュリティ管理

5.1 物理的管理

本サービスでは、CA のハードウェア及び CA サービスを提供するソフトウェアへの物理的なアクセスを制限する適切なセキュリティコントロールを装備する。そのハードウェアやソフトウェアへのアクセスは、本 CPS「5.2.1 信頼される役割」で記述されるそれぞれの権限者に制限される。アクセスの制御は電子的なアクセス制御方法、物理的なアクセス制御方法を組み合わせる。ハードウェア及び CA サービスを提供するソフトウェアへの物理的アクセスは常時監視され、また、許可されているアクセスについてもサービス運用管理者の承認の下に行われる。

5.1.1 入退室管理

CA 室、関連サーバー室、RA 室内の設備への不正操作によるアクセスを制限するため、CA 管理者は CA 室及び関連サーバー室への入室権限を持ち、RA 担当者は RA 室への入室権限を持つ。なお、BC 認証設備室へは、CA 管理者及び RA 担当者が入室することができる。ただし、設備への不正操作によるアクセスを制限するため、設備は CA 管理者権限のラックと RA 担当者権限のラック内にそれぞれ保管する。

電子証明書の登録業務の一部（以下、「登録局業務」という）を外部に委託する場合には、委託先にて登録局業務を実施する部屋を LRA 室と称する。LRA 室では、加入者の秘密鍵及び加入者証明書は扱わない。

5.1.1.1 CA 室における入退室管理

CA 室は、常時施錠された区画であり、原則として CA 管理者以外の者は入室できないよう制御されている。

CA 室への入室時の認証方式は、生体認証であり、複数人の認証が必要である。CA 室への入室権限の付与及び CA 室内で行う作業の承認はサービス運用管理者が行う。機器保守、設備保守等で入室権限がない者の入室が必要な場合も、サービス運用管理者が承認し、関係者以外の者が設備に触れることが出来ないよう必ず複数名の CA 管理者が立ち会う。入室が許可されている CA 管理者であっても、CA 室へ入室する人数は必ず複数名とし、単独での入室、システム操作は行わない。また、CA 室は監視カメラにより、常時監視される。

CA 室の入退室記録については、毎営業日チェックされ、その他の監査対象の記録とともに保管され、監査対象となる。

5.1.1.2 RA 室における入退室管理

RA 室は、常時施錠された区画であり、原則として RA 担当者以外の者が入室できないよう制御されている。

RA 室への入室時の認証方式は、生体認証であり、複数人の認証が必要である。RA 室への入室権限の付与及び RA 室内で行う作業の承認はサービス運用管理者が行う。機器保守、設備保守等で入室権限がない者の入室が必要な場合も、サービス運用管理者が承認し、関係者以外の者が設備に触れることが出来ないよう必ず複数の RA 担当者が立ち会う。入室が許可されている RA 担当者であっても、RA 室へ入室する人数は必ず複数名とし、単独での入室、システム操作は行わない。また、RA 室への入退室は、監視カメラにより常時監視される。

RA 室の入退室記録については、毎営業日チェックされ、その他の監査対象の記録とともに保管され、監査対象となる。

5.1.1.3 LRA 室における入退室管理

LRA 室は、間仕切りで区分され、外部から容易に侵入できない区画であり鍵付きの扉により出入りを限定している。原則として RA 業務運用者、RA 施設管理者以外の者が入室できないように、入退室時以外常時施錠されており、入室時にはその度に帳簿に記録を残す。関係者以外の者が端末設備に触れることが出来ないように、入室権限のない者の入室が必要な場合、必ず入室権限を有する者の帯同を必要とする。

LRA 室の入退室記録については、RA 施設管理者により日常的にチェックされ、その他の監査対象の記録とともに保管され、監査対象となる。

5.1.1.4 関連サーバー室における入退室管理

関連サーバー室は、常時施錠された区画であり、原則として CA 管理者、監視オペレータ以外の者が入室できないよう制御されている。

関連サーバー室の入室時の認証方式は、IC カード認証であり、複数人の認証が必要である。関連サーバー室への入室権限の付与及び関連サーバー室内で行う作業の承認はサービス運用管理者が行う。機器保守、設備保守等で入室権限がない者の入室が必要な場合も、サービス運用管理者が承認し、関係者以外の者が設備に触れることが出来ないよう必ず複数の入室権限者が立ち会う。入室権限者であっても、関連サーバー室へ入室する人数は必ず複数名とし、単独での入室、システム操作は行わない。また、関連サーバー室への入退室は監視カメラにより、常時監視される。

関連サーバー室の入退室記録については、その他の監査対象の記録とともに保管され、監査対象となる。

5.1.1.5 BC 認証設備室における入退室管理

BC 認証設備室は、常時施錠された区画であり、原則として CA 管理者、RA 担当者以外の

者が入室できないよう制御されている。

BC 認証設備室への入室時の認証方式は、生体認証であり、CA 管理者、RA 担当者それぞれ複数人の認証が必要である。BC 認証設備室への入室権限の付与及び BC 認証設備室内で行う作業の承認はサービス運用管理者が行う。機器保守、設備保守等で入室権限がない者の入室が必要な場合も、サービス運用管理者が承認し、関係者以外の者が端末設備に触れることが出来ないよう必ず複数名の CA 管理者又は RA 担当者が立ち会う。入室権限者であっても、BC 認証設備室へ入室する人数は必ず複数名とし、単独での入室、システム操作は行わない。また、BC 認証設備室は監視カメラにより、常時監視される。

BC 認証設備室の入退室記録については、その他の監査対象の記録とともに保管され、監査対象となる。

5.1.2 電源管理

CA 室、RA 室、関連サーバー室及び BC 認証設備室の電源は、UPS により安定的に供給され、かつ長時間停電時においても自家発電装置より電源供給を受け保護される。

5.1.3 空調管理

CA 室、RA 室、関連サーバー室及び BC 認証設備室は、機器類に最適な温度、湿度を一定に保つことが可能な設備によって保護される。また、CA 室、関連サーバー室及び BC 認証設備室の温度、湿度は常時監視される。

5.1.4 火災防止

CA 室、RA 室、関連サーバー室及び BC 認証設備室は、防火壁によって区画された防火区画内とし、火災報知器及び消火設備を設置する。LRA 室は、火災報知機及び消火装置を設置する。

5.1.5 地震対策

CA 室、RA 室、関連サーバー室及び BC 認証設備室には、次のような地震対策を講ずる。

- CA 室、RA 室、関連サーバー室及び BC 認証設備室内のラックは、転倒防止のため、建物構造体に固定された専用架台にボルトにより固定する。
- 照明器具は、飛散防止対策が施された器具を使用する。
- 重要な電源設備、空気調和設備は建物構造体に固定する。
- 転倒の危険がある什器は転倒防止措置が講じられる。

5.1.6 媒体保管

本サービスでは、すべての磁気媒体は、キャビネット又は金庫に保管され、セキュアな保管場所に保管される。

5.1.7 廃棄

CA 秘密鍵、機密情報を含む紙面の文書及び磁気媒体等の廃棄の方法は、CA 秘密鍵やバックアップ媒体等は完全な初期化を行うか物理的に破壊を行い、紙面･文書等の紙ベースのものはシュレッダーにかけ廃棄を行う。

CA 秘密鍵の破棄方法に関しては、本 CPS「6.2.7 秘密鍵の破棄方法」で記述される。その他媒体、文書等についても別途定められる。

5.2 手続き上の管理

5.2.1 信頼される役割

本サービスの運用業務に携わるすべての者は、本 CPS で規定された信頼される役割を担っている。信頼される役割を担う者は、次のとおりである。

(1) 認証サービス改善委員会

セコムトラストシステムズが提供する認証機関として最高決定権をもち、認証サービスの監査実施を決定する権限を有する。セコム認証サービスの開始、終了等に係る意思決定を行う権限を有する。直接、サービスの運用を行わない。

(2) サービス責任者

セコムトラストシステムズが提供する認証サービスの統括責任者であり、サービス運用管理者の任命と解任を行う。

(3) サービス運用管理者

セコムトラストシステムズが提供する認証サービスの運用の責任者である。電子証明書の証明書ポリシの設定、管理、CA 管理者、RA 担当者その他の要員の人事管理、入退室制御管理、監査ログによるセキュリティ監査等を行う。サービス運用管理者は、CA 室、RA 室、関連サーバー室及び BC 認証設備室の入室権限やシステムの操作権限を持たない。

(4) CA 管理者

CA 管理者は、CA サーバー、CA 関連サーバー、CA の秘密鍵等の CA 関連システムの操作権限を持ち、構築、運用、管理を行う。

CA 管理者は、加入者の本人確認や、不正に RA 端末を操作して加入者の登録、発行及び取消等が出来ないよう、RA 担当者の持つ権限は持たない。

(5) RA 担当者

RA 担当者は、加入者の本人確認や RA 端末等の操作権限を持ち、加入者の審査、登録、発行及び取消等の処理を行う。

RA 担当者は不正に CA 関連システムを操作し、顧客情報や加入者証明書の改ざんが出来ないよう、CA 管理者の持つ権限を持たない。

相互認証の場合は、BCA への CSR の生成、BCA からの CSR の署名の検証、相互認証証明書の発行等を行う。

(6) ログ検査者

監査ログの抽出、検査、管理を行う。

(7) CA 技術担当者

システムの技術的な部分について、サービス運用管理者、CA 管理者、RA 担当者の補助的な役割を担い、システム評価、検証、障害対応等を行う。CA 技術担当者は必要に応じてサービス運用管理者によって指名され、CA 技術担当者が作業を行う場合は、サービス運用管理者がその作業を承認し、作業内容によっては CA 管理者又は RA 担当者が作業に立ち会う。

(8) 監視オペレータ

関連サーバー室への入室権限を持ち、1 日 24 時間、1 週間 7 日システムの監視を行う。

登録局業務の一部を外部に委託して行う場合には委託先の役割として、次の役割を定める。

(9) RA 責任者

委託先の登録局業務における責任者である。委託先の要員の任命と解任を行う。

(10) RA 業務管理者

委託先の登録局業務の運用の管理者である。RA 業務運用者への作業指示、作業報告の確認を行う。

(11) RA 施設管理者

委託先の登録局業務を行う端末設備の管理者である。LRA 室への入退室の管理と検査を行う。

(12) RA 業務運用者

委託先の登録局業務の運用者である。RA 業務管理者の指示のもと、加入者の審査及び登録の業務を行う。

5.2.2 必要とされる人数

5.2.2.1 CA サーバー及び関連サーバーへのアクセス

CA サーバー及び関連サーバーへのアクセスは、本 CPS「5.1.1 入退室管理」に記述された物理的制限の他に、権限の実行において複数人の立ち会いを必要とし、CA サーバー及び関連サーバーの操作に係る責任は、複数の役割及び人物で共有する。

5.2.2.2 RA 端末へのアクセス

電子証明書の登録、取消等を行う端末へのアクセスは、本 CPS「5.1.1 入退室管理」に記述された物理的制限の他に、権限の実行において複数人の立ち会いを必要とし、審査、登録、取消等において、相互牽制を働かせる。

5.2.3 業務手続きとその変更管理

本 CPS の下に業務手続きを定め文書化し、それに従って業務を実施する。サービス運用管理者は、本 CPS 等の変更に伴い業務手続きの見直しを行い、必要に応じて関連する文書類を改訂する。

5.3 人事上のセキュリティ管理

信頼される役割を担う者は、本サービスに関して、操作や管理の責務を負う。本サービスにおいては、これら担当者の信頼性、適合性、及び合理的な職務執行能力を保証する人事管理がなされ、そのセキュリティを確立するものとする。

5.3.1 CA における人事上のセキュリティ管理

本サービスに関して信頼される役割を担う者は、セコムトラストシステムズ株式会社の採用基準に基づき採用された社員とする。

サービス責任者が、職務遂行能力等を勘案しサービス運用管理者を任命する。

サービス運用管理者が CA 管理者、RA 担当者及びログ検査者をサービスに必要な技術的専門知識等を勘案し任命する。

また、CA 管理者、RA 担当者、ログ検査者は、専門のトレーニングを受け、PKI の概要とシステムの操作方法等を理解している。

5.3.2 委託先業務における人事上のセキュリティ管理

業務の一部を外部に委託して実施する場合には、委託先に本規定の遵守を求め、これに沿った運用を求めるものとする。

5.3.3 トレーニング要求

信頼される役割を担う者は、その業務を行うための適切な教育を定期的に受け、以降必要に応じて再教育を受けなければならない。

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 鍵ペア生成

(1) CA 秘密鍵生成

CA の秘密鍵は、CA サーバーシステムを最初に立ち上げる際に生成される。本サービスでは CA の署名用鍵ペアを FIPS140-2 レベル 3 の認定を取得したハードウェアセキュリティモジュール（Hardware Security Module、以下、「HSM」という）上で生成する。CA の秘密鍵の生成作業は、CA 室又は BC 認証設備室内でサービス運用管理者立会いのもと、複数名の CA 管理者が操作を行うことによって行われる。

(2) 加入者の鍵ペア生成

加入者の鍵ペアとそれに係る暗号化に用いる PIN コードは、RA 室又は BC 認証設備室からの操作により、必ず複数名の RA 担当者が相互にチェックを行いながら生成操作を行い、操作者にその内容を知られないよう安全に生成される。

媒体シリーズの加入者の鍵ペアは、加入者証明書発行後、媒体(CD-R)に格納され、関連する全ての装置から、直ちに完全な消去がなされる。

ダウンロードシリーズの鍵ペアは加入者証明書を発行後、サーバー上に格納され、加入者からのダウンロード実施後 1 時間後に全ての装置から、直ちに完全な消去がなされる。

6.1.2 加入者の秘密鍵及び加入者証明書の送付

加入者の秘密鍵及び加入者証明書の送付に関しては、CP「4.1.2 加入者鍵ペア生成と電子証明書発行処理」に規定された手続きにより行われる。

6.1.3 CA 公開鍵の送付

媒体シリーズの CA 公開鍵は、加入者の秘密鍵及び加入者証明書とともに媒体(CD-R)に保管され、加入者の秘密鍵及び加入者証明書と同様の手段により加入者に送付される。

また、ダウンロードシリーズの CA 公開鍵は加入者の秘密鍵及び加入者証明書とともに加入者の端末にてダウンロードされる。

6.1.4 鍵長

本サービスの電子証明書の発行に利用する電子署名方式及び鍵長は以下のとおりである。

自己署名証明書の発行に利用する電子署名方式は、ハッシュアルゴリズムとして SHA-1 又は SHA-256 を用いた RSA 方式であって鍵長は、2048 ビットである。

加入者証明書、相互認証証明書、リンク証明書の発行に利用する電子署名方式は、ハッシュアルゴリズムとして SHA-1 を用いた RSA 方式であって鍵長は 1024 ビット又はハッシュアルゴリズムとして SHA-256 を用いた RSA 方式であって鍵長は 2048bit である。

6.1.5 公開鍵パラメータの生成

規定しない。

6.1.6 パラメータ品質の検査

規定しない。

6.1.7 ハードウェア/ソフトウェアによる鍵生成

本 CPS「6.1.1 鍵ペア生成」に記述したとおりである。

6.1.8 鍵利用目的

CA 秘密鍵の用途は発行する加入者証明書への電子署名である。これ以外は、次に掲げる使用に限定される。

- 当該認定認証業務の自己署名証明書への電子署名（自己署名）
- CA 秘密鍵の更新処理のため、新しい当該認定認証業務のリンク証明書への電子署名（※１）
- CA 秘密鍵の更新処理のため、古い当該認定認証業務のリンク証明書への電子署名（※１）
- 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
- 認証業務用設備及びそれを操作する者の権限を示す電子証明書への電子署名
- 当該認定認証業務を利用する各コンポーネントに対して発行する電子証明書への電子署名
- 電子証明書取消情報を公開するために発行する CRL/ARL/fullCRL への電子署名
- 相互認証証明書への電子署名

（※１）新旧 2 種類のリンク証明書へ電子署名を行う。

6.2 CA 秘密鍵の保護

6.2.1 暗号モジュール

CA の秘密鍵の生成、保管、署名操作は、FIPS140-2 レベル 3 の認定を取得した HSM を用いて CA 室又は BC 認証設備室で行われる。

6.2.2 秘密鍵の複数人コントロール

CA の秘密鍵の生成を完了するには、サービス運用管理者と複数名の CA 管理者を必要とする。生成後に発生する秘密鍵の更新等の秘密鍵管理についても同様である。

6.2.3 秘密鍵の外部公開とバックアップ

CA の秘密鍵は、条件付であっても、外部の第三者への公開を行わない。CA 秘密鍵は、CA 室内で FIPS140-2 レベル 3 の認定を取得した HSM にバックアップされる。バックアップ作成時も本 CPS「6.2.2 秘密鍵の複数人コントロール」と同じコントロールがなされる。

また、そのバックアップは CA 室及び BC 認証設備室内に保管される。

6.2.4 秘密鍵の暗号化モジュールへの格納

CA 秘密鍵は、HSM の内部で生成され、他のハードウェア及びソフトウェア等がそのモジュールに介入することはない。

6.2.5 秘密鍵の有効化の方法

HSM の有効化は、CA 室又は BC 認証設備室内において本 CPS「6.2.2 秘密鍵の複数人コントロール」と同じく、複数人により管理鍵（電子鍵）を用いて行われる。加入者の秘密鍵に関しては、規定しない。

6.2.6 秘密鍵の無効化の方法

HSM の無効化は、CA 室又は BC 認証設備室内において本 CPS「6.2.2 秘密鍵の複数人コントロール」と同じく、複数人により、操作をする者とその監視をする者とに分かれて行われる。加入者の秘密鍵に関しては、規定しない。

6.2.7 秘密鍵の破棄方法

CA 秘密鍵を破棄しなければならない状況の場合は、CA 室又は BC 認証設備室内で本 CPS「6.2.2 秘密鍵の複数人コントロール」と同じく、複数人によって、秘密鍵の格納された HSM を完全に初期化し、又は物理的に破壊する。同時に、バックアップの秘密鍵に関しても同様の手続きによって破棄する。

詳細な破棄手順に関しては、別途手順書に定められている。

6.3 鍵ペア管理のその他の側面

6.3.1 CA 公開鍵のアーカイブ

CA の公開鍵はアーカイブ対象とする。

6.3.2 CA 鍵ペアの有効期間

CA の鍵の有効期間は 10 年 30 分である。有効期間の変更はできない。

6.4 有効化データ

6.4.1 有効化データの生成とインストール

CA の秘密鍵に対するものを含め、CA で使用される PIN コードやパスワードは、英大文字、英小文字、数字等をすべて含む 8 文字以上の長さを使用する。

加入者秘密鍵に係る PIN コードは、RA 室又は BC 認証設備室から操作者に識別されない方法によって、必ず複数名の RA 担当者が相互に操作確認を行いながら生成される。

6.4.2 有効化データの保護

CA で使用される PIN コードやパスワードについては、封印された上でサービス運用管理者による管理の下、金庫内に保管される。また、その操作権限者によって定期的に変更を行う。

加入者秘密鍵に係る PIN コードについては、運用担当者及び外部に漏れないように厳重に生成及び管理され、加入者宛に秘密鍵とは異なる送付方法によって届けられる。

また、すべてのシリーズの加入者秘密鍵に係る PIN コードは、PIN コード送付票に印刷された後、関連する全ての装置から、直ちに完全な消去がなされる。

6.5 コンピュータセキュリティ管理

CA サーバーのハードウェアは、物理的に本 CPS「5.1 物理的管理」に記述されている対策によって保護される。CA サーバー及び RA 端末へのログイン時には、ユーザーの認証（又は本人認証）が行われる。これらに使用されるパスワードは、入室権限及び操作権限をもたないサービス運用管理者が安全に管理し、サービス運用管理者が作業指示を行う際に、入室権限をもつ RA 担当者、CA 管理者に貸し出すものとする。

CA サーバーデータベースへのアクセスと監査ログへのアクセスは、本 CPS「4.9.3 アーカイブの保護」と本 CPS「4.8.4 監査ログの保護」で記述される制限を受ける。

6.6 セキュリティ技術のライフサイクル管理

本サービスにおいて用いるハードウェア及びソフトウェアは、適切なサイクルで最新のセキュリティ技術を導入すべく、随時、本 CPS の見直し及びセキュリティチェックを行う。

6.7 ネットワークセキュリティ管理

電子証明書発行等で必要なリモートから CA サーバーへのアクセスは、セキュアなプロトコルを利用して保護される。また、ネットワークにはファイアウォール、不正侵入検知システムを導入し、不正アクセス対策を講じる。CA サーバーへのその他のアクセスについては、状態監視等の必要最低限に留める。

6.8 暗号モジュールの技術管理

CA 鍵ペアは、FIPS140-2 レベル 3 の認定を取得した HSM を使用し保護されている。

7. 電子証明書と CRL/ARL/fullCRL のプロファイル

本項の内容は、CP「6.電子証明書と CRL/ARL/fullCRL のプロファイル」に規定する。

8 仕様の管理

8.1 仕様変更手続き

認証サービス改善委員会は、本 CPS の内容変更に際しては、まず主務省庁に変更の認定申請の必要性について確認する。また、BCA に対し申請の必要性について確認する。

8.1.1 変更の申請が必要な変更

本 CPS の内容変更に際して、主務省庁に問い合わせた結果、変更の認定申請が必要であるという回答を得た場合、又は BCA に問い合わせた結果、変更申請が必要であるという回答を得た場合は、変更の認定申請に対する主務大臣の認定の取得、又は BCA の変更の承認を得て変更を実施し、本 CPS のメジャーバージョン番号を更新する。また、速やかに変更した本CPS(本CPSの変更内容と変更実施日を含む)をリポジトリ上に掲載することにより、加入者及び利用者に対して告知する。

8.1.2 変更の申請が必要でない変更

本 CPS の内容変更に際して、主務省庁が認定申請を不要とし、かつ BCA も変更申請を不要とした場合は、本 CPS のマイナーバージョン番号を更新し、変更を実施する。また、速やかに変更した本 CPS（本 CPS の変更内容と変更実施日を含む）をリポジトリ上に掲載することにより、加入者及び利用者に対して告知する。

8.2 公表と告知方法

本 CPS を変更した場合、速やかに変更した本 CPS（本 CPS の変更内容と変更承認日を含む）をリポジトリ上に掲載することにより、加入者及び利用者に対して告知する。加入者は告知日(リポジトリ上に掲載されたリリース日)から一週間の間、異議を申し立てることができ、異議申し立てがない場合、変更された本 CPS は加入者に同意されたものとみなされる。

8.3 CPS の承認手続き

本 CPS とその変更は、認証サービス改善委員会の承認を受けるものとする。また、加入者の異議がないことで同意される。

9. 用語

用語	説明
電子証明書	ある公開鍵を、記載されたものが保有することを証明する電子的文書。CA が電子署名を施すことで、その正当性が保証される。本 CPS では、特に断らない限り加入者証明書、相互認証証明書、自己署名証明書及びリンク証明書を総称して「電子証明書」と呼ぶ。
自己署名証明書	自 CA の公開鍵に対して、自 CA の秘密鍵で署名した電子証明書。自 CA の公開鍵の正当性を保証する。
加入者証明書	特定認証業務の認定を取得した本サービスより個人に対して発行する加入者用の電子証明書。
相互認証証明書	2つの異なる認証ドメインのCAがお互いを認証したことを示すために、相互に発行する証明書。本サービスでは、BCAとの間で相互認証証明書が発行される。
リンク証明書	CA 鍵更新に伴い、同時に存在することとなる新しい CA 鍵ペアと古い CA 鍵ペアの関係を保証するための電子証明書。
CA	電子証明書の発行・取消、CA等秘密鍵の生成・保護及び加入者の登録を行う機関。本CPS内で、単にCAという場合は電子証明書の発行業務及び登録業務を含む。
リポジトリ	CAの自己署名証明書及びCRL/ARL/fullCRL等を格納し公表するデータベースである。
RFC2527	：Request For Comments 2527 CAやPKIのためのCP/CPSの 執筆者を支援するフレームワーク。
オブジェクト識別子（OID）	：Object Identification 世界で一意となる値を登録機関（ISO 、ITU）に登録した識別子。PKI で使うアルゴリズム、電子証明書内に格納する名前（subject）のタイプ（Country名等の属性）等は、オブジェクト識別子として登録されているものが使用される。
X.509	ITU-Tが定めた電子証明書及び証明書失効リストのフォーマット。X.509 v3(Version 3)では、任意の情報を保有するための拡張領域が追加された。
X.500	名前及びアドレスの調査から属性による検索まで広範囲なサービスを提供することを目的にITU-Tが定めたディレクトリ標準。

	X.500識別名は、X.509の発行者名及び主体者名に使用される。
公開鍵	公開鍵暗号方式において用いられる鍵ペアの一方。秘密鍵に対応する、公開されている鍵。
秘密鍵	公開鍵暗号方式において用いられる鍵ペアの一方。公開鍵に対応する、本人のみが保有する鍵。
証明書発行要求（CSR）	：Certificate Signing Request 電子証明書を発行する際の元となるデータファイル。CSRには電子証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して電子証明書を発行する。
本人限定受取郵便	電子署名法で定める「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サービス。
簡易書留	引き受けと配達のみを記録し、万一、郵便物等が壊れたり、届かなかった場合に、原則として5万円までの実損額を賠償する郵便事業株式会社が提供するサービス。
PINコード	：Personal Identification Number 個人を認証するための暗証番号。本サービスでは、秘密鍵を有効化するために用いる。
CRL	：Certificate Revocation List 電子証明書の有効期間中に、CA秘密鍵の危殆化等の事由により取消された加入者証明書のリスト。
ARL	：Authority Revocation List 電子証明書の有効期間中に、CA秘密鍵の危殆化、相互認証基準違反等の事由により取消された自己署名証明書及び相互認証証明書のリスト。
fullCRL	：full Certificate Revocation List 電子証明書の有効期間中に、CA秘密鍵の危殆化、相互認証基準違反等の事由により取消された全ての電子証明書のリスト。
RA	：Registration Authority CAの業務のうち、登録業務を行う機関。主な業務は、電子証明書発行対象者の本人確認、電子証明書発行に必要な情報の登録、CAに対する証明書発行要求等である。
FIPS	：Federal Information Processing Standard NIST（National Institute of Standards and Technology）が

	策定した米国連邦情報処理標準を定めたガイドライン、及び認定を受けた技術や製品に関する文書。そのうち、FIPS140-2は、暗号技術に関するセキュリティ要件を規定している。
電子署名法施行規則第五条第一項第一号イの身分証明書	顔写真付きのものに限る。 (1) 旅券（パスポート） (2) 在留カード (3) 特別永住者証明書 (4) 官公庁が発行した免許証、許可証若しくは資格証明書等（運転免許証、船員手帳、海技免状、小型船舶操縦免許証、猟銃・空気銃所持許可証、戦傷病者手帳、宅地建物取引主任者証、電気工事士免状、無線従事者免許証、認定電気工事従事者認定証、特種電気工事資格者認定証、耐空検査員の証、航空従事者技能証明書、運航管理者技能検定合格証明書、動力車操縦者運転免許証、教習資格認定証、検定合格証） (5) 住民基本台帳カード (6) 官公庁（独立行政法人、地方独立行政法人及び特殊法人を含む）が職員に発行した身分証明書