e-Probatio PS2 サービス 証明書ポリシ（CP）

バージョン 6.3

2011 年 12 月

株式会社エヌ・ティ・ティ ネオメイト

改訂履歴

版数	改訂日	内容	作成者	承認者
1.0	2005/11/ 9	初版作成	池本 恭英	白子 匡博
1.1	2006/02/24	特定するサービスの追加	池本 恭英	白子 匡博
2.0	2006/07/24	・特定するサービスの追加 ・利用者証明書に記載される氏名漢字表記については「戸籍法施行規則(昭和 22 年 12 月 29 日司法省令第 94 号) 別表第二 漢字の表」に基づき記載する場合があることを追記 ・インターネットからの利用申込書作成支援について記載 他	内田 充典	白子 匡博
2.1	2006/08/21	個人事業主の場合の申込書必須記入欄の変更	内田 充典	白子 匡博
2.2	2007/02/28	CA 秘密鍵の鍵更新に関する記述の変更	谷 秀明	白子 匡博
3.0	2007/06/06	発行室新設に伴う変更	谷 秀明	白子 匡博
3.1	2008/01/15	利用者証明書に記載される氏名漢字表記については「法務省 戸籍統一文字情報」に基づき記載する場合があることを追記	谷 秀明	岩崎 千明
4.0	2008/03/07	・利用者証明書及び利用者秘密鍵の有効期間として 3 年 1 ヶ月、4 年 1 ヶ月を追加 ・特定するサービスとして、「IT 書面一括法で定められる文書保存に係わるシステム」を追加	谷 秀明	岩崎 千明
4.1	2008/06/12	利用申込書住所フリガナ欄の記載条件の変更	谷 秀明	岩崎 千明
4.2	2008/08/22	・特定するサービスとして、「不動産業界における有印文書の電子化に係わるシステム」を追加 ・公的書類の名称を修正	谷 秀明	岩崎 千明
4.3	2008/09/05	利用申込書及び失効申込書の必須記入項目を変更	谷 秀明	岩崎 千明
4.4	2008/10/29	・署名検証者からの失効に関する問合わせに対する認証局の対応を修正 ・認証局が発行する電子証明書および CRL/ARL の形式を追記 ・認証業務運営に必要な電子署名に関する誤記を修正 ・改訂履歴欄の様式変更(改訂日・作成者に統一)	中浦　修	岩崎　千明

4.5	2008/12/24	・事前承諾の自筆自署欄廃止に伴う関連記述の削除	中浦　修	岩崎　千明
4.6	2009/01/21	・3 月 1 日付での配達記録郵便廃止に伴い、郵送方法に簡易書留郵便を追記	中浦　修	岩崎　千明
5.0	2009/03/17	・利用者本人の死亡事実確認書類の規定を追加 ・ARL 及び CRL プロファイルにおいて、設定しないプロファイルの Critical フラグを削除	中浦　修	岩崎　千明
5.1	2009/06/08	・利用者申込書に記載される記入項目のひらがな又はカタカナへの置換え基準を追記 ・商業登記に関する必要書類の明確化 他	中浦　修	岩崎　千明
5.2	2009/10/26	・フィンガープリントの表現変更 ・姓名の文言修正 ・誤字修正 他	中浦　修	寺田　博志
5.3	2009/11/16	・受取代人委任状兼承諾書の廃止 ・会社代表者以外の利用者の所属確認における規定の見直し	中浦　修	寺田　博志
6.0	2010/07/01	認証局運営会社を株式会社 NTT アプリエから株式会社エヌ・ティ・ティ ネオメイトに変更	播岡　俊彦	土屋　直広
6.1	2010/10/18	・誤字修正 ・RFC3280 に合わせて、表記を統一	播岡　俊彦	土屋　直広
6.2	2011/10/18	・誤字修正 ・分かりにくい記載箇所の修正	播岡　俊彦	清水　仁志
6.3	2011/12/01	・利用者本人の死亡事実確認書類に除籍謄本等を追加	播岡　俊彦	清水　仁志

― 目次 ―

1　はじめに

本 e-Probatio PS2 サービス証明書ポリシ（以下、本 CP と呼ぶ。）は、株式会社エヌ・ティ・ティ ネオメイト（以下、NTT ネオメイトと呼ぶ。）が運営する e-Probatio 認証局（以下、認証局と呼ぶ。）における e-Probatio PS2 サービス（以下、本サービスと呼ぶ。）の認証業務に関する規程である。

本 CP の構成は、Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC2527「Certificate Policy and Practice Statement Framework」に準拠する。また、本 CP の記述においては、RFC2527 で定められる項目の全てを記述し、他の規程等を参照する場合には、項目だけを残し、参照内容を明示することとする。

1.1 概要

本 CP では、本サービスにおける電子証明書の目的、適用範囲、電子証明書プロファイル、本人確認方法及び鍵管理に関する事項について記述している。

本サービスは、認証局が下記で特定するサービス（以下、特定サービスと呼ぶ。）に使用される利用者の電子証明書（以下、利用者証明書と呼ぶ。）を発行するサービスである。特定サービスは、認証局の情報公開 WEB サイトにも公開する。

- ●（財）日本建設情報総合センター（通称「JACIC」）及び（財）港湾空港建設技術サービスセンター（通称「SCOPE」）電子入札コアシステム
- ●電子入札・開札システム及び電子申請・届出システム
- ●国税電子申告・納税システム（ｅ－Ｔａｘ）
- ●地方税ポータルシステム（ｅＬＴａｘ）
- ●電子契約システム
- ●e-文書法（※1）で定められる文書保存に係わるシステム
- ●IT 書面一括法（※2）で定められる文書保存に係わるシステム
- ●不動産業界における有印文書の電子化に係わるシステム

（※1）「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」および「同法律の施行に伴う関係法律の整備等に関する法律」の 2 つをさす。

（※2）「書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律」をさす。

本サービスは、利用者証明書の他に、認証局の電子証明書（以下、CA 証明書と呼ぶ。）、認証局の公開鍵・秘密鍵の更新のための電子証明書（以下、リンク証明書と呼ぶ。）、政府認証基盤ブリッジ認証局との相互接続のための電子証明書（以下、相互認証証明書と呼ぶ。）を発行する。

1.1.1 関連規程

認証局は、認証局の全ての認証業務に関して e-Probatio 認証局 認証業務規程（CPS）を定め、認証局が提供するサービスに係わらず認証局で共通する事項について規定する。

認証局は、e-Probatio 認証局 認証業務規程（CPS）及び本 CP（以下、本 CP 等と呼ぶ。）に基づく業務手順の詳細を事務取扱要領として規定し、認証局に従事する者は、本 CP 等及び事務取扱要領に従って業務を実施している。なお、本 CP の改訂が行われた場合は、CPS、事務取扱要領及び関係書類についても必要な改訂を実施する。

1.2 識別

e-Probatio PS2 サービスのオブジェクト識別子を表 1.2 に示す。また、本 CP を公開している情報公開 WEB サイトは利用者証明書の「certificatePolicies」内に記載される。

表 1.2　e-Probatio PS2 サービスのオブジェクト識別子

	オブジェクト名	オブジェクト識別子
認証業務提供主体	e-Probatio CA	0.3.4401.4.1
認証業務規程	e-Probatio CPS	0.3.4401.4.1.1
証明書ポリシ	e-Probatio PS2 CP	0.3.4401.4.1.1.2

1.3 関係主体と電子証明書の適用範囲

1.3.1 本 CP の適用範囲

本 CP は、以下の図 1.3 に示す認証局により実施される電子証明書発行及び失効業務に適用される。本サービスより発行される全ての電子証明書には、本 CP が適用される。

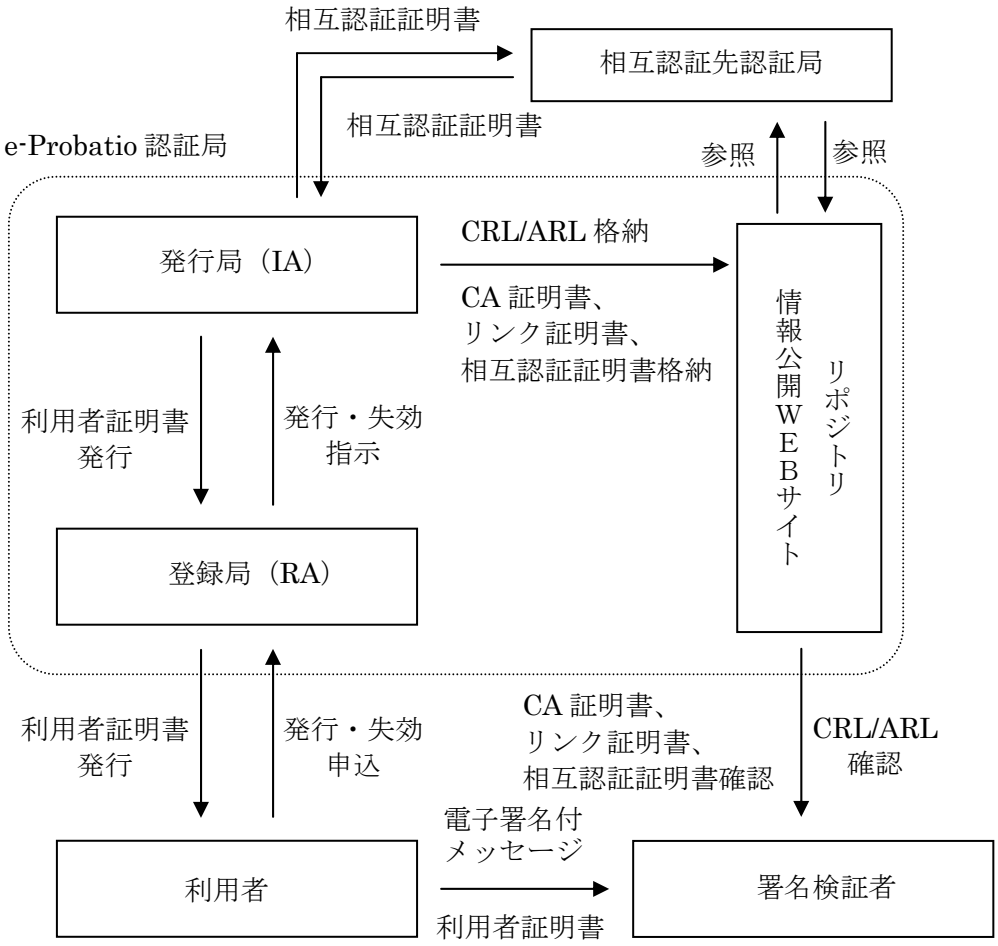

図 1.3 e-Probatio 認証局のコミュニティ

(1) 認証局

本 CP「1.1.1 関連規程」に示す CPS に規定する。

(2) 発行局（IA）

本 CP「1.1.1 関連規程」に示す CPS に規定する。

(3) 登録局（RA）

認証局は、利用者署名符号（以下、利用者秘密鍵と呼ぶ。）及び利用者公開鍵の鍵ペアの生成を登録局（RA）（以下、RA と呼ぶ。）で行う。また、RA は、生成した利用者秘密鍵

と利用者証明書を IC カードに格納し利用者への送付を行う。

その他については、本 CP「1.1.1 関連規程」に示す CPS に規定する。

(4) 利用者

利用者とは、認証局に利用者証明書の利用申込みを行い、利用者証明書を取得し、利用する主体である。また、利用者は、利用者本人が所有する利用者秘密鍵の対になる公開鍵と利用者本人の氏名が結びついている利用者証明書によって、利用者秘密鍵を用いて行われた電子署名が本人の作成に係るものである事を証明される者である。

電子証明書を発行する相手（利用者）は、法人の会社代表者又は法人に所属する個人、商業登記又は商号登記されていない個人事業主、あるいは省官庁／地方公共団体に在籍する個人とする。

(5) 署名検証者

署名検証者とは、電子証明書を信頼し、利用する者である。署名検証者は、本 CP 等の内容について理解し、承諾した上で利用するものとする。

(6)相互認証先認証局

相互認証先認証局とはブリッジ認証局であり、行政機関の認証局と民間機関の認証局との間にあり、各々の認証局間の信頼を橋渡しするために、各々と相互認証する認証局である。

1.3.2 電子証明書の適用範囲

認証局が発行する利用者証明書は、特定サービスでのみ使用する事が出来る。利用者証明書が特定サービス以外の用途で使用された場合、認証局は一切の責任を負わないものとする。

また、認証局は、利用者証明書への署名以外に、認証業務運営に必要な以下の電子証明書への電子署名も行う。

- 他の特定認証業務の認定を受けた認証業務又は認定認証業務と同等の公の認証業務との相互接続を行うための相互認証証明書 への電子署名
- CA 証明書への電子署名（自己署名）
- CA 証明書更新のためのリンク証明書への電子署名
- CRL/ARL への電子署名
- 認証設備を操作する認証局員用の電子証明書への電子署名
- 認証設備のサーバ用の電子証明書（以下、サーバ証明書と呼ぶ。）への電子署名
- 失効結果報告書への電子署名

1.3.3 電子署名法に関する特別な要件

認証局は、「電子署名及び認証業務に関する法律（平成 12 年 5 月 31 日法律第 102 号）」（以下、電子署名法と呼ぶ。）において、主務大臣より「特定認証業務」の認定を受けた認証業務を行う。特に留意すべき項目を以下に記す。

(1) 属性等についての説明

利用者証明書に表示される情報のうち、利用者が利用者証明書に記載された利用者本人である事については、電子署名法に定める認定認証業務における認定の対象として確認及び表示が行われるが、利用者の氏名、住所及び生年月日以外の情報（属性）の確認及び表示については、同法に定める認定の対象外となる。利用者は、この事を十分理解し、これを承認した上で利用者証明書を利用するとともに、認証局は署名検証者に対し誤認を与える恐れのある表示、説明等を行ってはならないものとする。

(2) 虚偽の利用申込みに対する罰則

利用者は、正確、最新かつ真実の情報を e-Probatio PS2 サービス電子証明書利用申込書（以下、利用申込書と呼ぶ。）類に記載し、申込む必要がある。虚偽の申込みをして、利用者について不実の証明をさせた者は、電子署名法第 6 章第４１条に基づいて罰せられる。

(3) 電子署名の法的効果

利用者は、IC カードに格納された利用者秘密鍵を用いて、認証局所定の署名アルゴリズムを用いて特定サービスに関するデジタルデータに電子署名を行った場合、当該電子署名は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。そのため、利用者は利用者秘密鍵が格納されている IC カード及び IC カードを使用する際に必要となる IC カード PIN を十分な注意をもって秘匿性を維持して管理しなければならない。

(4) 利用者証明書の失効申込について

利用者秘密鍵が危殆化（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事をいう。以下同じ。）、又は危殆化した恐れがある場合、あるいは利用者証明書に記録されている事項に変更が生じた場合、又は利用者証明書の利用を中止する場合においては、遅滞なく利用者証明書の失効申込みを行わなければならない。

(5) 電子署名に使用するアルゴリズム

利用者が本認定認証業務に係る利用者証明書を使用する場合における電子署名のためのアルゴリズムは、「2.1.3　利用者の義務（6）署名アルゴリズム」で指定したものを使用しなければならない。

1.4　CP 管理

1.4.1 管理組織

本 CP「1.1.1 関連規程」に示す CPS に規定する。

1.4.2 対応窓口

本 CP「1.1.1 関連規程」に示す CPS に規定する。

1.4.3 CP 責任者

本業務の本 CP に対する適合性に関しては、認証業務運営検討会が審査し、e-Probatio 認証局の代表者(以下、認証局代表者と呼ぶ。) が最終的な決定及び責任を負う。

2　一般規定

2.1 義務

2.1.1 IA の義務

(1) 利用者に対する義務

IA は利用者に対して、以下の情報を公開する義務を負う。

- CA 証明書（OldWithOld、NewWithNew）およびリンク証明書(OldWithNew、NewWithOld)を SHA-1 でハッシュ化した値（フィンガープリントという）

その他については、本 CP「1.1.1 関連規程」に示す CPS に規定する。

(2) 相互認証先認証局に対する義務

IA はブリッジ認証局に対して、以下の各項目の義務を負う。

- ブリッジ認証局との相互認証申請に際して、正確な情報を提示する
- 認証設備又は運用に変更が生じた場合は、ブリッジ認証局の定める手続きをとる
- CA 秘密鍵が危殆化又は危殆化の恐れが生じた場合は、速やかにブリッジ認証局運営組織に報告する

(3)署名検証者に対する義務

IA は署名検証者に対して、以下の情報を公開する義務を負う。

- CA 証明書（OldWithOld、NewWithNew）、リンク証明書(OldWithNew、NewWithOld)
- CA 証明書（OldWithOld、NewWithNew）、リンク証明書(OldWithNew、NewWithOld)を SHA-1 でハッシュ化した値（フィンガープリント）
- 相互認証証明書
- CRL/ARL
- 本 CP 等

2.1.2 RA の義務

RA は利用者に対して、以下の各項目の義務を負う。

- 本 CP 等及び別途定める事務取扱要領に従い、利用者からの利用申込書類の確認及び審査、本人確認を行い、利用者鍵ペアの生成を行う。また利用者証明書の発行を IA に指示する。
- 利用者秘密鍵を IC カードに格納した後、利用者秘密鍵の生成に係わった認証局の設備等から利用者秘密鍵及び関連情報等を直ちに廃棄する。
- 利用申込みを拒否する場合、認証局は、発行不受理事由を書面にし速やかにこれを利用申込者に通知する。

- 利用者に IC カードを交付する際に設定する IC カード PIN を利用者本人以外には隠蔽して印刷した後、IC カード PIN の生成から印刷までに係わった認証局の設備等から IC カード PIN 及び関連情報等を直ちに廃棄する。
- 利用者証明書を交付する。
- IC カードを利用者へ安全かつ確実に提供するため、電子署名及び認証業務に関する法律施行規則（平成 13 年総務省、法務省、経済産業省令第 2 号）第五条第一項第一号ハで定める「その取扱いにおいて名あて人本人若しくは差出人の指定した名あて人に代わって受け取ることができる者に限り交付する郵便」に相当する郵便事業株式会社が提供する「本人限定受取郵便」により、当該利用者の住民票の写しまたは住民票記載事項証明書または登録原票記載事項証明書の記載住所に送付する。尚、受取代人が指定されていない場合は、「本人限定受取郵便」（基本型）を用い、受取代人が指定されている場合は、「本人限定受取郵便」（特例型）を用いることとする。
- IC カード PIN の送付は、IC カードの送付において、受取代人が指定されていない場合は IC カードと同封し、受取代人が指定されている場合は、「簡易書留郵便」により別送し、当該利用者の住民票の写しまたは住民票記載事項証明書または登録原票記載事項証明書の記載住所に送付する。
- 利用者証明書の失効を行う場合、利用者証明書の失効を IA に指示し、失効を行った事を e-Probatio PS2 サービス失効通知書により利用者に通知する。
- 利用者本人から権利又は利益を侵害され、又は侵害される恐れがあるとの申し出があった場合には、その求めに応じ、遅滞なく名義人の利用申込書一式の写し及び利用者証明書の写しを開示する。

その他については、本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.1.3 利用者の義務

利用者は、e-Probatio PS2 サービス利用申込み（以下、利用申込みと呼ぶ。）手続きの中で認証局より提供される重要事項説明資料（「e-Probatio PS2 サービス利用約款（以下、利用約款と呼ぶ。）」、「e-Probatio PS2 サービス重要事項説明書（以下、重要事項説明書と呼ぶ。）」及び本 CP 等）を理解し同意しなければならないものとする。

利用者は、IC カード受領後、同封された受領書を IC カード発送日より 15 営業日以内に利用者の実印による押印をして認証局に返送しなければならない。

また、「利用約款」に明記されているとおり、利用申込みと IC カード（利用者証明書及び利用者証明書に記載された利用者公開鍵に対する利用者秘密鍵）及び IC カード PIN の使用及び管理について以下の義務がある。

(1) 正確な利用申込み内容の提示

利用者は、利用申込書類に最新であり正確かつ真実を記載し、申込む必要がある。それ

に加え、利用者自身の本人性を証明するために認証局が定める所定の書類を提出しなければならない。

(2) 利用者証明書の利用制限

利用者証明書はその用途範囲、損害賠償などを記載した本 CP 等に基づいて発行されている。利用者はその範囲外の用途で利用者証明書を使用してはならない。

(3) IC カードと IC カード PIN の管理義務

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、充分な注意をもって利用者秘密鍵を格納した IC カード及び IC カード PIN の管理を行い、秘匿性を維持しなければならない。

(4) 利用者証明書記載事項の管理

利用者は発行された利用者証明書の記載事項を受領時に確認し、記載事項に誤りがあった場合には、直ちに認証局へ連絡をしなければならない。また、利用者証明書受領後にその記載事項が利用者の現状に合わなくなった場合は、速やかに失効申込みを行わなければならない。

(5) 速やかな利用者証明書失効申込み

本 CP「4.4.1　電子証明書の失効事由（2）利用者証明書（ｉ）利用者による失効事由」に規定している事項が発生した場合には、利用者は速やかに失効申込みを行わなければならない。

(6) 署名アルゴリズム

利用者秘密鍵を使用して電子署名を行う場合の署名アルゴリズムは、「sha1WithRSAEncryption（オブジェクト識別子：1.2.840.113549.1.1.5)」を使用しなければならない。

2.1.4 署名検証者の義務

認証局が発行した利用者証明書の署名検証者は、情報公開 WEB サイトに公開される「e-Probatio PS2 サービス署名検証者同意書（以下、署名検証者同意書と呼ぶ。)」に同意しなければならない。「署名検証者同意書」に明記されているとおり、以下の各事項の義務を負う。

(1)利用者証明書の利用制限

署名検証者は、利用者から提示された利用者証明書を、本 CP に記載されている使用目的である特定サービスでのみ使用する事を理解し、その使用範囲内で利用しなければなら

ない。

(2)電子証明書の有効性確認

署名検証者は、利用者証明書を検証する際に以下の内容を含む有効性の確認を行わなければならない。

- CA 証明書、リンク証明書、相互認証証明書を本 CP 等で指定する配布方法により確実に入手する
- 信頼するか否かを判断する CA 証明書のフィンガープリントを情報公開 WEB サイトから入手する(必要な場合はリンク証明書を含む)
- 信頼するか否かを判断する CA 証明書のフィンガープリントと入手したフィンガープリントに相違がないかどうかを確認する(必要な場合はリンク証明書を含む)
- 信頼するか否かを判断する電子証明書の署名を検証する
- 信頼するか否かを判断する電子証明書が有効期間内である事を確認する
- 信頼するか否かを判断する電子証明書が失効されていないかどうかを確認する

2.1.5 リポジトリの義務

認証局は、本 CP「2.6 公開とリポジトリ」の規定に従う。

2.2 責任

2.2.1 認証局の責任

- 認証局は、利用者の取得した IC カードによる特定サービスの手続きを、全て当該利用者の意思により行われたものとみなす
- NTT ネオメイトは、本 CP 等及び利用約款の条項及び利用者証明書に記載された NTT ネオメイトの名義にかかわらず、以下に定める事由のいずれかに該当する場合には、一切責任を負わないものとする

① 利用者が認証局に届け出た事項が真実と相違しており、認証局が利用者から提出を受けた資料を相当な注意をもって照合しても当該相違を発見できなかったとき

② 利用者が IC カード、IC カード PIN 又は利用者秘密鍵を漏洩したとき、又は利用者秘密鍵が利用者以外の者によって不正使用されたとき

③ 利用者の使用するソフトウェア、ハードウェア、システム、ネットワーク等に瑕疵、障害その他の問題又は誤操作等が生じたとき

④ 署名検証者が本 CP 等に定める利用者証明書を利用する際に電子証明書の有効性確認を怠ったとき、又は正しくこれらの確認を行わなかったとき

⑤ 本 CP 等に定める利用者証明書の失効事由に該当しているにもかかわらず、利用者

が失効申込手続きを怠ったとき

⑥ 認証局が利用者証明書の失効事由に該当している事を知った後、遅滞なく失効情報を CRL に登録し、これを公表したにもかかわらず、当該公表前に利用者証明書が署名検証者に送付されたとき

⑦ 認証局が一般的な認証事業者の知見及び技術水準に照らし解読困難とされている暗号その他のセキュリティ手段を用いていたにもかかわらず、当該暗号が解読され、又はセキュリティ手段が破られたとき

⑧ 上記各号の他、利用者もしくは署名検証者が本 CP 等に違反したとき、又は NTT ネオメイトの責めに帰すべき事由がないとき

その他については、本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.2.2 利用者の責任

利用者は、本 CP 等及び利用約款に規定する義務を履行する責任がある。

2.2.3 署名検証者の責任

署名検証者は、本 CP 等及び署名検証者同意書に規定する義務を履行する責任がある。

2.3 財務上の責任

NTT ネオメイトの業務の遂行又は業務の結果に起因して、利用者に損害が生じた場合、NTT ネオメイトが賠償する損害の範囲は予見可能な相当因果関係のある損害のみとする。その賠償額は、当該利用者が NTT ネオメイトに現に支払ったサービス料金を限度とする。

2.4 解釈及び執行

2.4.1 準拠法等

本 CP 等の成立、解釈及び履行、認証局と関係者の間で係争が生じた場合等は全て、次の法令を含む日本国内の法律に準拠するものとする。

- 「電子署名及び認証業務に関する法律」（平成 12 年 5 月 31 日法律第 102 号）
- 「電子署名及び認証業務に関する法律施行令」（平成 13 年 2 月 28 日 政令第 41 号）
- 「電子署名及び認証業務に関する法律施行規則」（平成 13 年 3 月 27 日総務省、法務省、経済産業省令第 2 号）
- 「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」（平成 13 年 4 月 27 日総務省、法務省、経済産業省告示第 2 号）
- 「電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針」（平成 15 年 6 月 2 日 総務省情報通信政策局、法務省民事局、経済産業省商務

情報政策局）

2.4.2 分割、存続、合併及び通知

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.4.3 紛争解決の手続

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.5 料金

利用者が本認証サービスを利用するに当たって必要となる料金、証明対象となる利用者証明書の有効期間及び支払方法等の情報を情報公開 WEB サイトに公開する。

2.6 公開とリポジトリ

2.6.1 認証局に関する情報の公開

リポジトリ及び情報公開 WEB サイトは、以下の情報を公開する。

(1) リポジトリに公開する情報

- CA 証明書
- CRL／ARL
- リンク証明書
- 相互認証証明書

(2) 情報公開 WEB サイトに公開する情報

- 本 CP
- e-Probatio PS2 サービス利用約款
- e-Probatio PS2 サービス署名検証者同意書
- e-Probatio PS2 サービス重要事項説明書
- e-Probatio PS2 サービス電子証明書利用申込書
- e-Probatio PS2 サービス電子証明書失効申込書
- 企業在籍証明書
- 省官庁／地方公共団体在籍証明書
- 料金情報
- CA 証明書（OldWithOld、NewWithNew）およびリンク証明書(OldWithNew、NewWithOld)および当該証明書のフィンガープリント
- IC カードリーダ購入申込書

・ 本サービスに関するお知らせ

その他については、本 CP「1.1.1 関連規程」に示す CPS に規定する。

上記に公開されている内容の変更は、認証局代表者の指示のもとで行われる。

2.6.2 公開の頻度

リポジトリ、情報公開 WEB サイト上に情報を公開するタイミングは、次のとおりである。

- CA 証明書、リンク証明書、相互認証証明書及び CRL／ARL は、発行及び更新の都度、即時公開する。なお、CRL／ARL は、失効情報に変更がない場合でも、情報の適時性を保証するために、24 時間以内に 48 時間有効な CRL／ARL を発行する
- 本 CP 等は改訂の都度公開する。
- 相互認証した認証業務 の名称及び相互認証を取り消した認証業務の名称は認証局による決定の都度公開する

その他については、本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.6.3 アクセスコントロール

認証局のリポジトリ及び情報公開 WEB サイトに公開された情報は、インターネットを介して誰でもアクセスし、参照する事が出来る。

また、CA 証明書及びリンク証明書のフィンガープリントに関しては、改竄の有無を 24 時間監視し、改竄防止措置を講じている。

2.6.4 リポジトリ

リポジトリ及び情報公開 WEB サイトは、以下に示す URL にて、公開される。

(1)リポジトリの URL

ldap://ldap.e-probatio.com/ou=e-probatio%20ps2,o= e-probatio%20ca ,c=jp

(2) 情報公開 WEB サイトの URL

https://www.e-probatio.com/ps2/

2.7 準拠性監査

2.7.1 監査頻度

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.7.2 監査人の身元/資格

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.7.3 被監査部門と監査人の関係

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.7.4 監査項目

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.7.5 監査指摘事項への対応

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.7.6 監査結果の通知

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.8 機密保持

2.8.1 機密情報

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.8.2 機密情報対象外の情報

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.8.3 電子証明書失効リストの開示

認証局は、相互認証証明書及びリンク証明書の失効リスト(ARL)、利用者証明書の失効リスト(CRL)を利用者及び署名検証者に公開する。

電子証明書を失効する場合、失効日時、失効された電子証明書のシリアルナンバが CRL/ARL 情報に含まれる。これらの情報は全ての利用者に共有される。失効に関するその他の詳細情報は原則として開示しないものとする。

2.8.4 法執行機関への開示

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.8.5 民事上の手続き

本 CP「1.1.1 関連規程」に示す CPS に規定する。

2.8.6 利用者証明書名義人の請求に基づく情報の開示

認証局は、利用者証明書に記載される名義人（利用者）から権利又は利益を侵害される、又は侵害される恐れがあるとして、当該証明書の利用者申込みに係る個人情報の開示請求を受けた場合は、これに応ずる。また、名義人（利用者）以外からの個人情報開示請求は受付けない。

名義人（利用者）は、e-Probatio PS2 サービス個人情報開示申込書を記入後、認証局に郵送し、個人情報開示請求を行う。

上記の請求に応じ個人情報を開示する場合には、開示請求人が当該利用者証明書の名義人である事を確認する。具体的には、個人情報開示申込書に記載された内容と、保管してある利用申込書の内容とを比較し、一致した内容で記載されている事を確認する。また、名義人本人による申請である事を確認するために、e-Probatio PS2 サービス個人情報開示申込書に押印された印影と、利用申込書に添付された印鑑登録証明書の印影が一致することを確認する。ただし、利用申込時の印鑑が印鑑登録の変更などにより使用不能の場合は、新しい印鑑登録証明書の提出を求め、その印影が e-Probatio PS2 サービス個人情報開示申込書に押印された印影と一致することを確認し、さらに利用申込書提出後に氏名、住所のいずれかを変更している場合は、変更を証明する公的書類（住民票の写し、戸籍謄本又は戸籍全部事項証明書、戸籍抄本又は戸籍個人事項証明書等）の提出を求め、利用申込書からの変更を確認する。これらの確認を行ったうえで、以下の個人情報の開示を行う。

- 名義人の利用申込書一式の写し
- 利用者証明書の写し(利用者証明書の内容を紙に印刷)

2.8.7 その他の事由に基づく情報公開

認証局は、前述した以外の事由に基づく情報開示を一切行わないものとする。

2.9 知的財産権

IC カード、IC カードに格納された利用者証明書、利用者秘密鍵及び認証局が利用者に対して交付するその他の文書（本 CP 等、利用約款、マニュアルを含む）等の知的財産権は、全て NTT ネオメイトに帰属し、利用者には帰属しないものとする。

2.10 個人情報保護

認証局は、利用約款に定めるとおり、利用者から認証局に提供される個人情報のうち、利用者の氏名、住所、所属組織名、所属組織住所を利用者証明書に記載する。

尚、利用申込書に個人情報の取扱及び利用者証明書に記載される事項について定めた本 CP 等および利用約款に対し、利用者が承諾する際の日付の記入及び実印の押印欄を設けて

いる。認証局における利用者の承諾の確認は、日付の記入及び実印の押印確認により行っている。

その他については、本 CP「1.1.1 関連規程」に示す CPS に規定する。

3　識別と認証

3.1 初期登録

3.1.1 名前の型

認証局の名称及び利用者証明書の名称は X.500 識別名（DN:Distinguished Name）の形式に従って設定する。詳細は、「7.1　電子証明書のプロファイル」の定義に従う。

3.1.2 名前の意味に関する要件

名前の意味は「7.1　電子証明書のプロファイル」に規定される。

3.1.3 様々な名前形式を解釈するための規則

「7.1 電子証明書のプロファイル」に規定される名前形式を解釈するための規則を下表に示す。

表 3.1-1　CA 証明書、リンク証明書の名前解釈の規則

領域名	識別子	名前解釈の規則
issuer subject	c	電子証明書発行者の国名（JP）
	o	電子証明書発行者の組織名のローマ字表記
	ou	電子証明書発行者の部門名のローマ字表記
	（エンコーディング方式） c は PrintableString、その他は UTF8String	
issuerAltName subjectAltName	c	電子証明書発行者の国名（JP）
	o	電子証明書発行者の組織名の日本語表記
	ou	電子証明書発行者の部門名の日本語表記
	（エンコーディング方式） c は PrintableString、その他は UTF8String	

表 3.1-2　相互認証証明書の名前解釈の規則

領域名	識別子	名前解釈の規則
issuer subject	c	電子証明書発行者の国名（JP）
	o	電子証明書発行者の組織名のローマ字表記
	ou	電子証明書発行者の部門名のローマ字表記
	（エンコーディング方式） c は PrintableString、その他は UTF8String	

表 3.1-3　利用者証明書の名前の形式解釈ルール

領域名	識別子	名前解釈のルール
issuer	c	電子証明書発行者の国名（JP）

	o	電子証明書発行者の組織名のローマ字表記
	ou	電子証明書発行者の部門名のローマ字表記
	（エンコーディング方式） c は PrintableString、その他は UTF8String	
subject	c	電子証明書所有者の国名（JP）
	s(st)	電子証明書所有者の居住都道府県名のローマ字表記
	l	電子証明書所有者の居住住所名のローマ字表記 （都道府県名は除く）
	cn	電子証明書所有者の固有名称のローマ字表記
	（エンコーディング方式） c は PrintableString、その他は UTF8String	
issuerAltName	c	電子証明書発行者の国名（JP）
	o	電子証明書発行者の組織名の日本語表記
	ou	電子証明書発行者の部門名の日本語表記
	（エンコーディング方式） c は PrintableString、その他は UTF8String	
subjectAltName	c	電子証明書所有者の所属する会社住所の国名（JP）
	s(st)	・法人の場合 電子証明書所有者の所属する会社住所の都道府県名の日本語表記 ・商業登記または商号登記のない個人企業の場合 半角スペース
	l	・法人の場合 電子証明書所有者の所属する会社住所の日本語表記 （都道府県名は除く） ・商業登記または商号登記のない個人企業の場合 半角スペース
	o	・法人の場合 電子証明書所有者の所属する会社名の日本語表記 ・商業登記または商号登記のない個人企業の場合 半角スペース
	cn	電子証明書所有者の固有名称の日本語表記
	（エンコーディング方式） c は PrintableString、その他は UTF8String	

3.1.4 名前の一意性

認証局は、認証局が発行した電子証明書の subject 及び issuer が一意となる事を保証する。

3.1.5 名前に関する紛争の解決手段

e-Probatio PS2 サービスの利用申込者による名前に関する異議申立てについては、認証局が全ての決定を行う権利を留保する。

名前に関する異議申立ての解決手段については、認証局において協議する。

3.1.6 商標の認識・認証・役割

商標使用の権利については、商標所持者が全ての権利を留保するものとする。但し、認証局は利用申込みの際、利用者に関する情報に商標が含まれていた場合、当該商標を利用者証明書に記載する権利を有するものとする。

また、認証局は必要に応じて、商標所持者に対し、商標に関する出願等の公的書類の提出を求める事がある。

3.1.7 秘密鍵の所有を証明するための方法

(1) 相互認証先認証局

認証局は、ブリッジ認証局から入手した Certificate Signing Request（PKCS#10）（以下、CSR と呼ぶ。）の署名の検証を行い、内容が改ざんされていない事と CSR に含まれている公開鍵と対になる秘密鍵で署名してある事を確認する。また、CSR のフィンガープリントを確認し、要求先が正しい事及び subject がブリッジ認証局の名称に一致する事の確認を行う。

(2) 利用者

認証局は、認証局で利用者公開鍵と利用者秘密鍵を生成する。その利用者公開鍵を含み、利用者公開鍵に対応する利用者秘密鍵の所有を証明する利用者証明書を生成する。生成された利用者証明書と利用者秘密鍵を IC カードに格納する。

認証局は、正当な利用者に利用者秘密鍵を所有させるため、受取代人が指定されていない場合は、「本人限定受取郵便」（基本型）にて郵送し、受取代人が指定されている場合は、「本人限定受取郵便」（特例型）にて郵送する。また、IC カード PIN の送付は、IC カードの送付において、受取代人が指定されていない場合は IC カードと同封し、受取代人が指定されている場合は、「簡易書留郵便」により別送し、当該利用者の住民票の写しまたは住民票記載事項証明書または登録原票記載事項証明書の記載住所に送付する。

3.1.8 組織の認証

e-Probatio PS2 サービスは、利用者の所属の確認を以下に定める方法により行う。

(1) 法人の場合

①利用者が会社代表者本人である場合

(ｉ)登記事項証明書による代表者の確認

登記事項証明書により会社代表者の確認をするにあたり、登記事項証明書が少なくとも記載内容、形式、有効期限（発行日から 6 ヶ月以内）などにおいて真正である事を確認し、登記事項証明書と利用申込書の記載内容が一致する事を確認する

② 利用者が会社代表者本人でない場合

(ⅰ)登記事項証明書による代表者の確認

利用者が会社代表者である場合と同様に確認を行う

(ⅱ)企業在籍証明書による利用者の所属の確認

企業在籍証明書により利用者の所属の確認をするにあたり、情報公開 WEB サイトから入手した認証局所定様式を用いた企業在籍証明書が少なくとも記載内容、形式、有効期限（発行日から 6 ヶ月以内）などにおいて真正である事を確認し、企業在籍証明書と利用申込書、及び登記事項証明書の記載内容が一致する事を確認する

(ⅲ)「印鑑証明書」による利用者の所属の確認

企業在籍証明書に押印された法人の実印に対応した「印鑑証明書」が少なくとも記載内容、形式、有効期限（発行日から 6 ヶ月以内）などにおいて真正である事を確認し、且つ企業在籍証明書に押印された印影と当該「印鑑証明書」の印影が一致する事を確認する

(2)商業登記または商号登記をしていない個人事業主の場合

青色・白色申告書または許認可証による事業主の確認

青色または白色申告書のコピー（直近年のもの）または官公庁が発行した営業許可証などの事業に係わる許認可証のコピー（直近のもの）により、記載内容、形式、年度などにおいて真正である事を確認し、利用申込書の記載内容と一致することを確認する。
尚、利用者は事業主に限るものとする。

(3) 省官庁/地方公共団体の場合

① 省官庁/地方公共団体在籍証明書による利用者の所属の確認

省官庁/地方公共団体在籍証明書により利用者の所属を確認するにあたり、情報公開 WEB サイトから入手した認証局所定様式を用いた省官庁/地方公共団体在籍証明書が少なくとも記載内容、形式、有効期限（発行日から 6 ヶ月以内）などにおいて真正である事を確認し、省官庁/地方公共団体在籍証明書と利用申込書の記載内容が一致する事を確認する

② 当該省官庁/地方公共団体への確認

当該省官庁/地方公共団体に連絡を取り、利用者が所属している事を確認する

3.1.9 個人の認証

e-Probatio PS2 サービスは、利用者の本人性の確認を以下に定める方法により行う。

(1) 住民票の写しまたは住民票記載事項証明書による利用者の確認

住民票の写しまたは住民票記載事項証明書により利用者を確認するにあたり、住民票の写しまたは住民票記載事項証明書が少なくとも記載内容、形式、有効期限などにおいて真

正である事を確認し、住民票の写しまたは住民票記載事項証明書と利用申込書の記載内容が一致する事を確認する。(但し、利用者が国内に居住する外国人である場合は、住民票の写しまたは住民票記載事項証明書の代わりに外国人登録の登録原票記載事項証明書を用いる。)

なお、住民票の写しまたは住民票記載事項証明書の有効期間は発行日より 3 ヶ月以内とする。但し、発行する地方公共団体が有効期限を設けている場合は、それを優先する。

(2) 印鑑登録証明書による利用者の確認

印鑑登録証明書により利用者を確認するにあたり、印鑑登録証明書が少なくとも記載内容、形式、有効期限などにおいて真正である事を確認し、且つ利用申込書に押印された実印の印影と印鑑登録証明書の印影が一致する事を確認する。なお、印鑑登録証明書の有効期間は発行日より 3 ヶ月以内とする。但し、発行する地方公共団体が有効期限を設けている場合は、それを優先する。

3.2 電子証明書の更新

(1) 相互認証証明書

認証局とブリッジ認証局は、相互に発行された相互認証証明書の有効期間が切れる前までに、新規相互認証時と同様にオフラインによる相互認証証明書を取り交す。 e-Probatio PS2 サービスは、現行の CA 証明書の有効期間が切れる前に、CA 証明書の更新を行い、新規相互認証時と同様にオフラインによる相互認証証明書の取り交しを行う。

(2) 利用者証明書

認証局は、利用者からの利用者証明書の更新手続きを、新規申込みと同じ手続きで行う。

3.3 電子証明書失効後の再発行

利用者証明書失効処理後の再発行は行わない。そのため失効後、利用者証明書を利用したい利用者は、新規申込時と同じ手続きを行う必要がある。

3.4 電子証明書の失効要求

電子証明書失効処理の失効事由及び失効時の手続きは、本 CP「4.4 電子証明書の一時停止と失効」のとおりである。

4　オペレーション要件

4.1 電子証明書の発行申請

4.1.1 電子証明書の発行要求

(1) 相互認証証明書

相互認証証明書の発行要求は、ブリッジ認証局の定めた手続きに基づいて行われる。

(2) 利用者証明書

利用者証明書の利用申込みは、e-Probatio PS2 サービスで定められた手続きに従い、下記の必要書類を認証局へ郵送する。なお、代理人による利用申込みは受付けない。また、利用者は重要事項説明資料（利用約款、重要事項説明書及び本 CP 等）を利用申込みの前に読み、内容を理解し、利用申込みにあたっては、それらに同意した上で申込む必要がある。利用申込みにあたって必要な書類は、情報公開 WEB サイトからダウンロードして入手する事を書類交付の基本とし、電子証明書発行申込画面にしたがって必須事項を入力する。（必須事項については、本 CP4.1.1 ①を参照のこと。ただし、氏名で使用されている漢字が俗字又は旧字等であり電子証明書発行申込画面へ入力できない文字の場合は、印刷された利用申込用紙へ手書きで記入すること。）その後、同画面にて入力した情報が反映された利用申込書等を印刷し、利用者の申込日付の記入及び実印による押印後その他必要書類を全て取り揃えて認証局へ郵送する。（その他必要書類については、本 CP4.1.1②を参照のこと）また、情報公開 WEB サイトにおいて、利用約款、CPS、CP、重要事項説明書をダウンロードした後に、重要事項説明書と利用申込書が一つの PDF 形式のファイルになったものをダウンロードすることもできる。但し、認証局が CD-ROM 媒体又は紙媒体を利用者へ郵送又は手交する場合がある。CD-ROM 媒体配布の際には、同一 CD-ROM 媒体の中に重要事項説明資料と利用申込書が格納されている。また、紙媒体の場合は必ず重要事項説明資料と利用申込書が同封されている。

また、この重要事項説明資料に対する利用者の同意は、利用者が利用申込書に記入する申込日付及び実印により、認証局が確認する。

なお、利用申込書は、本 CP 等で規定された用途で使われる利用者証明書についての申込みが明記された、本業務専用の「e-Probatio PS2 サービス電子証明書利用申込書」を使用する。

「e-Probatio PS2 サービス電子証明書利用申込書」の訂正は、利用者の実印の押印による訂正印を必要とする。

また、利用申込みには、新規・継続・追加の 3 種類があり、それぞれの内容は以下のとおりである。

- 新規：新規の利用者証明書の発行を申込む場合
- 継続：当業務発行の利用者証明書を持っていて、その利用者証明書の有効期間終

了 1 ヶ月前に有効期間開始となる利用者証明書の発行を申込む場合

・ 追加：当業務発行の利用者証明書を持っていて、さらに追加の利用者証明書の発行を申込む場合

① e-Probatio PS2 サービス電子証明書利用申込書

以下の項目を記入し、提出する。

必須記入項目

・ 事前承諾
  －お申込日（承諾日）
・ お申込者様情報
  －姓（住民票の写しまたは住民票記載事項証明書と同じ姓）
  －姓のフリガナ
  －姓のローマ字
  －名(住民票の写しまたは住民票記載事項証明書と同じ名)
  －名のフリガナ
  －名のローマ字
  －生年月日
  －住所(住民票の写しまたは住民票記載事項証明書と同じ住所)
  －住所のフリガナ（ローマ字変換に必要なフリガナ）
  －電話番号
・ 会社情報（商業登記または商号登記をしていない場合は不要）
  －商号又は名称(登記事項証明書記載の商号と同じもの。)
  －住所(登記事項証明書記載の住所と同じもの。若しくは許認可証等記載の住所と同じもの。)
  －代表者名（登記事項証明書記載の代表者名と同じもの。）
  －電話番号
・ その他の情報
  －申込内容(新規/継続/追加のいずれかを○で囲む)
  －IC カード発行枚数
  －証明書有効期間（1 年/2 年/3 年/4 年のいずれかを○で囲む）
  －添付の印鑑登録証明書で証明される利用者本人の実印による押印

任意記入項目

・ お申込者様情報
  －お名前（正字）（住民票の写しまたは住民票記載事項証明書の記載されている文字からの置き換えが、『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)』または、「戸籍法施行規則(昭和 22 年 12 月 29 日司法省令第 94 号) 別表第二 漢字の表」または、「法務省 戸籍統一文字情報」に基づく。これらに該当する文字がないときは、ひらがなまたはカタカナで記載する)

－FAX 番号

・ 会社情報

－電子メールアドレス

－会社 FAX 番号

・ その他の情報

－利用開始希望年月（記載する際は、翌々月から 6 ヶ月後までの期間内を指定する）

更に以下の場合は、必要事項を記入する。

（ｉ）住民票の写しまたは住民票記載事項証明書の記載氏名が旧字体（JIS 第 1 及び第 2 水準以外の文字）の方の場合

－氏名の正字

（ii）IC カードの受取に、受取代人を指定する場合（ただし、受取代人として利用者本人が指定されていた場合は、受取代人を指定しないものとみなす。）

－受取代人氏名

－受取代人住所

（iii）請求書を住民票の写しまたは住民票記載事項証明書とは別の場所への送付を希望する場合

－希望送付先住所

－希望送付先会社名

－希望送付先支店名/部署名

－希望送付先ご担当者名

－希望送付先電話番号

－希望送付先 FAX 番号

なお、必要事項を記入する場合に、住民票の写しまたは住民票記載事項証明書、登記事項証明書等に記載されている俗字又は旧字等からの置き換えは、『誤字俗字・正字一覧表（平成 16 年 10 月 14 日付け法務省民一第 2842 号民事局長通達)』または、「戸籍法施行規則(昭和 22 年 12 月 29 日司法省令第 94 号) 別表第二 漢字の表」または、「法務省 戸籍統一文字情報」（以下、漢字変換規則）に基づく。これらに該当する文字がないときは、ひらがなまたはカタカナで記載する。

② その他の必要書類

（ｉ）法人の場合

利用者が会社代表者である場合は、以下の書類を提出する。

- 「登記事項証明書」（商業・法人登記に関する「履歴事項全部証明書」または「現在事項全部証明書」をさす。その他、法務局から交付される商業・法人登記に関する事項（商号、会社住所、会社代表者名）が記載されている登記事項証明書も可とする。）
- 「印鑑登録証明書」
- 「住民票の写しまたは住民票記載事項証明書（利用者が国内居住の外国人である場合は外国人登録の登録原票記載事項証明書）」

また、利用者が会社代表者以外の場合、更に以下の書類を提出する。

- 「企業在籍証明書」
- 企業在籍証明書に押印された法人の実印に対応した「印鑑証明書」

（ⅱ）商業登記または商号登記をしていない個人事業主の場合

「登記事項証明書または商号登記簿謄本」に代えて以下のいずれかの書類を提出する。

- 「青色または白色申告書のコピー（直近年のもの）」
- 「官公庁が発行した営業許可証などの事業に係わる許認可証のコピー（直近年のもの）」

加えて、以下の 2 つの書類を提出する。

- 「印鑑登録証明書」
- 「住民票の写しまたは住民票記載事項証明書（利用者が国内居住の外国人である場合は外国人登録の登録原票記載事項証明書）」

（ⅲ）省官庁/地方公共団体の場合

利用者が省官庁/地方公共団体に所属する者である場合は、以下の書類を提出する。

- 「省官庁/地方公共団体在籍証明書」
- 「住民票の写しまたは住民票記載事項証明書（利用者が国内居住の外国人である場合は外国人登録の登録原票記載事項証明書）」
- 「印鑑登録証明書」

4.1.2 要求データの送付手段

(1) 相互認証証明書

ブリッジ認証局は、証明書要求データを郵送又は手交によってのみ、認証局に送付する。

(2) 利用者証明書

利用者証明書の申込者は、提出書類一式を、郵送によって、認証局へ送付する。郵送以外の申込みは取り扱わない。

4.2 電子証明書の発行

4.2.1 審査

(1) 相互認証証明書

認証局代表者から相互認証の承認が得られた場合は、要求データを取り交し、認証局はブリッジ認証局から相互認証証明書の CSR を郵送又は手交で受取り、相互認証申込書が受理された後、この申込みに対して、CSR の署名検証を行い、CSR に含まれている公開鍵と対になる秘密鍵で署名してある事を確認する。また、CSR のフィンガープリントを確認し、要求先が正しいか及び subject がブリッジ認証局の名称に一致する事を確認する。

(2) 利用者証明書

e-Probatio PS2 サービスは、限られた特定の場所で郵送されてきた申込書類を開封し、本 CP「 3.1.8 組織の認証」、「3.1.9 個人の認証」に記載した方法で審査を行う。また、受領後は申込書類を利用者へ返却しない。尚、審査において疑義が生じた場合は、事務取扱要領にて規定した方法に従い処理する。

4.2.2 電子証明書の発行

(1) 相互認証証明書

本 CP 「4.2.1 審査」で行った審査の後、ブリッジ認証局から受け取った相互認証証明書の発行要求に基づいて CA 秘密鍵で署名を付して、PKCS#7 フォーマットに従って相互認証証明書を発行した後、外部記憶媒体に格納し、これをブリッジ認証局の指定する方法でブリッジ認証局へ送付する。

(2) 利用者証明書

入力された利用申込みの情報に誤入力が無い事を確認した上で、利用申込書に指定された有効期間（1 年 1 ヶ月／2 年 1 ヶ月／3 年 1 ヶ月／4 年 1 ヶ月）を設定し、利用者証明書の発行指示を行う。なお、利用者証明書の発行指示と同時に利用者鍵ペアは、認証設備室内で生成される。この生成された利用者公開鍵に、CA 秘密鍵で署名を付して利用者証明書を発行する。その後、利用者秘密鍵及び利用者証明書は発行室で IC カードに格納する。なお、IC カード PIN は権限のある操作者が複数人により安全に生成する。

4.3 電子証明書の受入れ

(1) 相互認証証明書

認証局及びブリッジ認証局において、郵送又は手交によって相互に取り交した相互認証証明書を対として、リポジトリに登録する。双方がリポジトリへ登録した事をもって、相互認証が受け入れられたものとする。

(2) 利用者証明書

認証局は、利用者秘密鍵と利用者証明書を格納した IC カードを受取代人が指定されていない場合は、「本人限定受取郵便」（基本型）にて郵送し、受取代人が指定されている場合は、「本人限定受取郵便」（特例型）にて郵送する。また、IC カード PIN の送付は、IC カードの送付において、受取代人が指定されていない場合は IC カードと同封し、受取代人が指定されている場合は、「簡易書留郵便」により別送し、当該利用者の住民票の写しまたは住民票記載事項証明書または登録原票記載事項証明書の記載住所に送付する。

利用者は、IC カード及び IC カード PIN を受領した後、認証局が IC カードを発送した発送日より認証局の 15 営業日以内に実印を押印した受領書を認証局へ送付しなければならない。また、受領書の訂正は、利用者の実印の押印による訂正印を必要とする。

認証局は、受領した受領書の実印の印影と利用申込書の実印の印影との照合を行う。なお、認証局は、発送日より認証局の 15 営業日以内に受領書が返信されなかった場合、当該利用者証明書を失効する権限を有する。

また、IC カードの受取りは、受取代人に委任することも可能である。但し、IC カードを受取代人が受け取る場合は、受取代人が利用者本人から IC カードの受取りを委任されたこと、未開封のまま利用者本人に手渡すことについて承諾したことを示すために、受取代人は利用申込書に認印を押印しなければならない。

4.4 電子証明書の一時停止と失効

4.4.1 電子証明書の失効事由

(1) 相互認証証明書

認証局は、以下のような相互認証証明書の失効事由が発生した場合においては相互認証証明書の失効処理を行うものとする。

- 相互認証証明書の信頼性の低下
- 相互認証基準違反
- 認証局の業務終了
- 相互認証の終了
- 相互認証更新
- CA 秘密鍵の危殆化

・ ポリシの変更

(2) 利用者証明書

（ｉ）利用者による失効事由

利用者は、以下の場合には、直ちにその旨を認証局に報告し、利用者証明書の失効申込みを行わなければならない。

① 利用者秘密鍵が危殆化した場合
② 利用者証明書の内容が事実と異なる事を発見した場合
③ 利用者証明書の内容に変更があった場合
④ 利用者本人が死亡した場合（但し、この場合利用者本人以外による失効要求を受付ける）
⑤ IC カード、又はこれに格納されている利用者証明書もしくは利用者秘密鍵につき、紛失、漏洩、盗難、詐取、横領、偽造、変造その他の不正使用の可能性が生じた場合、又は破損して修復不能となった場合
⑥ 利用者証明書の利用を中止する場合
⑦ その他、利用者が利用者証明書の失効の必要性を判断した場合

（ⅱ）認証局による失効事由

認証局は、以下に定める事由のいずれかが発生した場合は、利用者証明書を失効する権限を有する。

① 利用者が本 CP 等及び利用約款に基づく義務に違反した場合
② 利用者証明書の発行に用いる CA 秘密鍵が危殆化した場合、又はその危険性があると認証局が認めた場合
③ 利用者秘密鍵が危殆化した場合、又はその危険性があると認証局が認めた場合
④ 利用者秘密鍵又は利用者証明書が不正使用された場合、又はその危険性があると認証局が認めた場合
⑤ 利用者証明書を格納した IC カード及び IC カード PIN を発送した日から、15 営業日以内に受領書が認証局に返送されない場合
⑥ 利用者証明書記載の情報に事実との相違があり、又はその情報が変更された事を認証局が確認した場合
⑦ 利用者本人の死亡を認証局が確認した場合
⑧ 利用者証明書の規格変更がなされた場合
⑨ その他、認証局が必要と判断した場合

4.4.2 失効申込者

(1) 相互認証証明書

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込者は、認証局代表者のみ

とする。

(2) 利用者証明書

利用者証明書の失効申込者は、利用者本人とする。但し、利用者が死亡した場合、利用者本人以外による失効要求を受付ける。

なお、本 CP「4.4.1 電子証明書の失効事由　(2) 利用者証明書　（ⅱ）認証局による失効事由」に該当する失効事由が発生した場合のみ、認証局の権限で、利用者証明書の失効処理を行う。

4.4.3 失効処理手順

(1) 相互認証証明書

認証局及びブリッジ認証局は相互の失効要求に基づき、互いの相互認証証明書を失効し、ARL を発行するとともにリポジトリから相互認証証明書ペアを削除する。

(2) 利用者証明書

（ⅰ）失効の申込み

利用者は、利用者証明書の失効を要求する場合、「e-Probatio PS2 サービス電子証明書失効申込書（以下、失効申込書と呼ぶ）」を認証局へ郵送する。緊急を要する失効要求の場合、失効申込書を認証局宛てに FAX し、後日、原本失効申込書を郵送する。なお、失効申込書の訂正は、利用者の実印の押印による訂正印を必要とする。

（ⅱ）失効申込書に記載すべき事項

- お客様情報
  - －姓（住民票の写しまたは住民票記載事項証明書と同じ姓）
  - －名（住民票の写しまたは住民票記載事項証明書と同じ名）
  - －生年月日
  - －住所（住民票の写しまたは住民票記載事項証明書と同じ住所）
- 会社情報
  - －商号又は名称(登記事項証明書記載の商号と同じもの。但し、商業登記または商号登記をしていない個人事業主の場合は不要)
- 利用者証明書情報（シリアル番号）
- 失効事由
- 押印（利用者申込書に添付された印鑑登録証明書で証明される利用者本人の実印）

（iii）失効申込者の本人確認の方法

利用者証明書の失効要求を受け取った認証局は、失効申込書又は FAX に押印されてい

る印影と新規申込み時点の印鑑登録証明書の印影を照合する方法により、失効要求者の本人性を確認する。但し、利用者本人の死亡時は、死亡事実が記載された戸籍謄本、戸籍全部事項証明書、戸籍抄本、戸籍個人事項証明書、除籍謄本、除籍全部事項証明書、除籍抄本、除籍個人事項証明書、履歴事項全部証明書、死亡診断書の写しのいずれかにより確認する。また、利用申込時の印鑑登録証明書の内容に変更があった場合は、印鑑登録証明書の再提出が必要となる。

（iv）失効処理

失効申込者の本人確認を行い、失効要求が失効事由に該当するか確認した上で、利用者証明書の失効登録を行い、CRL を発行するとともにリポジトリに公開する。

また、利用者証明書を失効した場合は、失効した事を遅滞なく当該利用者へ失効通知書を郵送して通知する。

4.4.4 失効における猶予期間

利用者証明書及び相互認証証明書の失効要求を受け取った場合、速やかに失効処理を行う。

4.4.5 電子証明書の一時停止事由

電子証明書の一時停止は行わない。

4.4.6 一時停止申請者

電子証明書の一時停止は行わない。

4.4.7 一時停止手順

電子証明書の一時停止は行わない。

4.4.8 一時停止期間の制限

電子証明書の一時停止は行わない。

4.4.9 CRL/ARL 発行周期

CRL/ARL は失効情報に変更がない場合でも、情報の適時性を保証するために、24 時間以内に 48 時間有効な CRL/ARL を発行する。

4.4.10 CRL/ARL の確認要件

認証局が発行する電子証明書を使用する署名検証者は、認証局が発行する CRL/ARL に署名検証対象の電子証明書のシリアル番号が掲載されていない事及び CRL/ARL に付与さ

れている認証局の署名の有効性及び CRL/ARL の有効期限を署名検証時に確認しなければならない。

なお、利用者証明書の有効期間が終了した場合も当該利用者証明書に係る証明書失効情報は 10 年間 CRL に掲載される。認証局は、署名検証者からの失効に関して問合わせが合った場合は CRL へのアクセスを案内する。

4.4.11 オンライン有効性確認の可用性

利用しない。

4.4.12 オンライン失効確認要件

規定しない。

4.4.13 その他利用可能な有効性確認手段

利用しない。

4.4.14 その他利用可能な有効性確認手段における確認要件

規定しない。

4.4.15 CA 秘密鍵の危殆化に関する特別な要件

認証局は、経営会議の判断により、認証局の CA 秘密鍵が危殆化及び危殆化の疑いがあると判断された場合は、速やかに全ての利用者証明書、相互認証証明書の失効処理を行い、リポジトリに CRL/ARL を公開し、CA 秘密鍵を廃棄する。

4.5 セキュリティ監査

4.5.1 記録されるイベントの種類

本 CP「1.1.1 関連規程」に示す CPS に規定する。

(1) 監査対象システムのログ検査

本 CP「1.1.1 関連規程」に示す CPS に規定する。

(2) リポジトリのシステムログ検査

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.5.2 システムログの検査周期

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.5.3 システムログの保存期間

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.5.4 システムログの保護

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.5.5 システムログのバックアップ手順

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.5.6 システムログの収集

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.5.7 イベントを引き起こした人への通知

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.5.8 脆弱性の評価

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.6 帳簿の保存

4.6.1 保存する帳簿の種類

認証局は、以下の文書を帳簿として保存する。

(1) 利用者証明書の利用申込みに関する次の文書

- e-Probatio PS2 サービス電子証明書利用申込書
- 登記事項証明書または商号登記簿謄本
- 印鑑登録証明書
- 住民票の写しまたは住民票記載事項証明書（但し、利用者が国内に居住する外国人である場合は、住民票の写しまたは住民票記載事項証明書の代わりに外国人登録の登録原票記載事項証明書を用いる）
- 企業在籍証明書
- 「印鑑証明書」
- 青色･白色申告書または許認可証のコピー
- 省官庁／地方公共団体在籍証明書
- 利用者証明書の発行の諾否に関する書類等
- 利用者証明書の発行の際における内部処理の記録及び受領書
- CA 証明書
- CA 秘密鍵生成記録

・ その他、「電子署名及び認証業務に関する法律施行規則（平成 13 年 総務省、法務省、経済産業省令第 2 号)」(以下、施行規則と呼ぶ)「第 12 条第 1 項第 1 号」の規定された文書等

(2) 利用者証明書の失効に関する次の文書

・ e-Probatio PS2 サービス電子証明書失効申込書
・ 利用申込時の印鑑登録証明書の内容に変更があった場合は、印鑑登録証明書も必要である
・ 利用者証明書の失効を決定した者に関する書類等
・ 利用者証明書を失効する際における内部処理の記録
・ その他、施行規則「第 12 条第 1 項第 2 号」の規定された文書等

本人死亡時は、以下の書類も必要である。

・ 戸籍謄本、戸籍全部事項証明書、戸籍抄本、戸籍個人事項証明書、除籍謄本、除籍全部事項証明書、除籍抄本、除籍個人事項証明書、履歴事項全部証明書、死亡診断書の写しのいずれか

(3) 認証局の組織管理に関する次の文書

・ e-Probatio PS2 サービス利用約款
・ e-Probatio PS2 サービス署名検証者同意書
・ その他、施行規則「第 12 条第 1 項第 3 号」の規定された文書等

その他については、本 CP「1.1.1 関連規程」に示す CPS に規定する。

(4) 設備及び安全対策措置に関する次の文書

・ 施行規則「第 12 条第 1 項第 4 号」の規定された文書等

その他については、本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.6.2 帳簿の保管期間

帳簿を保管する期間は次の 2 つである。

(1) 4.6.1(1)～(3)の文書

本 CP「1.1.1 関連規程」に示す CPS に規定する。

(2) 4.6.1(4)の文書

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.6.3 帳簿の保護

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.6.4 帳簿の保存媒体

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.6.5 帳簿の時に関する要件

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.6.6 電子媒体の可読性維持

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.6.7 保存状態の確認と検証の手順

本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.7 鍵更新

認証局は、CA 証明書の残存有効期間が利用者証明書及び相互認証証明書の有効期間よりも短くなる前に、当該 CA 秘密鍵の使用を中止するとともに、CA 秘密鍵の更新を行う。CA 秘密鍵は、認証設備室内の HSM で複数人による操作により生成される。CA 秘密鍵の生成操作は、1 名だけでは行えない。

同時に CA 証明書の更新も実施される。CA 証明書の更新も複数人による操作により行われ、その内の 1 名だけでは実行できない。この更新にあたって、古い CA 証明書と新しい CA 証明書を関連付けるリンク証明書が発行される。このリンク証明書及び新しい CA 証明書を使って、利用者及び署名検証者は古い CA 秘密鍵で署名された電子証明書が検証可能となる。CA 証明書更新実行後、認証局は新しい CA 証明書、リンク証明書、CRL/ARL を速やかにリポジトリで公開するとともに、CA 証明書、リンク証明書及び当該証明書のフィンガープリントを情報公開 WEB サイトで公開する。

4.8 危殆化と災害からの復旧

以下のとおり対処を実施し、個々の教育・訓練も定期的に行う。

4.8.1 ハードウェア、ソフトウェア、データが不正にさらされた時の対処

認証局が 2 ヶ月以上新規の電子証明書を発行できないか、又は 24 時間以上リポジトリを更新できず、ブリッジ認証局、利用者及び署名検証者に周知できなかった場合は、主務大臣に通報する。更に、原因の追求と再発防止策を講じる。

その他については、本 CP「1.1.1 関連規程」に示す CPS に規定する。

4.8.2 電子証明書の失効処理の特別な対処

正規の失効申込手続きに基づく失効処理において認証局のシステム異常などにより認証局で失効登録が行われない場合は、ブリッジ認証局及び利用者に失効した旨及び失効した電子証明書のシリアル番号を書面で通知する。電子証明書の失効登録が可能になったときに、ブリッジ認証局及び利用者に失効実施済みの旨、告知する。

4.8.3 CA の秘密鍵が危殆化した場合の対処

経営会議により、電子署名アルゴリズムの危殆化、HSM の盗難及び HSM 管理カードの紛失等で認証局の CA 秘密鍵が危殆化又は危殆化の恐れがあると判断された場合は、全ての利用者証明書の失効手続きを行い、リポジトリに CRL を公開する。利用者証明書を失効した事を遅滞なく当該利用者へ失効通知書を郵送して通知する。また、相互認証証明書は、ブリッジ認証局に通知し、調整した後、即座にリポジトリから削除する。その後、失効手続きを行い、リポジトリに ARL を公開する。CA 秘密鍵を本 CP「6.2.9　秘密鍵の廃棄方法」に従って廃棄する。CA 秘密鍵の危殆化又は、危殆化の恐れがあると判断され、その対応処理を実施した場合は、直ちに障害の内容、発生日時、措置状況等確認されている事項を主務大臣に通報し、ブリッジ認証局、利用者に対してメール、情報開示 WEB サイトが利用できる場合は、メール及び情報開示ＷＥＢサイトによる通知を行う。メール、情報開示 WEB サイトが利用できない場合は、FAX による通知を実施し、ＦＡＸが利用できない場合は電話による口頭通知を行う。署名検証者に対しては情報公開 WEB サイトにて公開する。尚、署名検証者に対しては署名検証者同意書に示している NTT ネオメイト保有の WEB サイトで公開することもある。更に原因及び被害の追求と原因別対応策を講じる。また、CA 鍵の危殆化による障害の発生等、脅威の種類に応じた対応策や回復手順等について、年 1 回の教育訓練を実施することを規定し、教育・訓練計画を策定して実施している。

4.8.4 災害等発生後の安全な設備の確保

災害などにより、認証局関連施設が被害を受け、通常の業務継続が困難な場合は、事務取扱要領において、定められた手続きにより、主務大臣、ブリッジ認証局、利用者に対してメール、情報開示 WEB サイトが利用できる場合は、メール及び情報開示ＷＥＢサイトによる通知を行う。メール、情報開示 WEB サイトが利用できない場合は、FAX による通知を実施し、ＦＡＸが利用できない場合は電話による口頭通知を行う。署名検証者に対しては情報公開 WEB サイトにて公開する。尚、署名検証者に対しては署名検証者同意書に示している NTT ネオメイト保有の WEB サイトで公開することもある。更に、原因及び被害の追求と原因別対応策を講じる。災害、認証業務用設備の故障等により署名検証者への失効情報の開示が、認証業務規程にて定める時間（24 時間）を超えて停止し、かつ署名検証者

が停止を知る方法が無かった場合は、直ちに障害の内容、発生日時、措置状況等確認されている事項を故障報告書として、主務大臣に対して通報する。

災害等による障害の発生等、脅威の種類に応じた対応策や回復手順等について、年 1 回の教育訓練を実施することを規定し、教育・訓練計画を策定して実施している。

4.9 CA 業務の終了

認証ポリシの大幅な変更や認証局機能の大幅な改良等で、CA 業務を終了する場合は、終了の 60 日前までに主務大臣、ブリッジ認証局及び全利用者に郵送にて通知の上、情報公開 WEB サイトに業務を終了する旨を公開する。また、CA 業務の終了日迄に、当該 CA 業務によって発行された全ての利用者証明書、相互認証証明書を失効し、ブリッジ認証局及び利用者に郵送にて失効済通知を行い、リポジトリに CRL/ARL を公開し、業務終了手続きを取る。なお、業務終了の手続きが完了するまでリポジトリに CRL/ARL を公開する。また、CA 業務終了に伴い、認証局のバックアップデータやアーカイブデータ等の保管組織、開示方法等を認証局から主務大臣に通報するとともに、ブリッジ認証局及び利用者に告知した上で CA 業務の終了日までに、バックアップを含む CA 秘密鍵を完全に破棄する。署名検証者に対しては、情報公開 WEB サイトにて業務終了後 3 カ月間 CRL/ARL を公開する。この際、CRL/ARL は日次での更新は行わない。

5　物理的、手続上、人事上のセキュリティ管理

5.1 物理的セキュリティ

5.1.1 サイトの位置と建物構造

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.1.2 物理アクセス

本 CP「1.1.1 関連規程」に示す CPS に規定する。

(1) 認証設備室

本 CP「1.1.1 関連規程」に示す CPS に規定する。

(2) 登録端末室

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.1.3 電源設備と空調設備

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.1.4 水害対策

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.1.5 地震対策

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.1.6 火災対策

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.1.7 媒体管理

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.1.8 廃棄物処理

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.1.9 オフサイトバックアップ

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.2 手続上の管理

5.2.1 信頼される役割

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.2.2 役割毎の必要人員

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.2.3 役割毎の識別と認証

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.3 人事管理

5.3.1 経歴、適正、経験、信頼性の要件

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.3.2 経歴審査手順

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.3.3 トレーニングの要件

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.3.4 再トレーニングの周期と要件

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.3.5 配置転換の周期と順序

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.3.6 許可されていない行動に対する罰則

本 CP「1.1.1 関連規程」に示す CPS に規定する。

5.3.7 個人との契約要件

本 CP「1.1.1 関連規程」に示す CPS に規定する。

6　技術的セキュリティ管理

6.1 鍵ペア生成とインストール

6.1.1 鍵ペア生成

CA 鍵ペアは、認証設備室内に設置された専用の暗号装置（HSM）を用いて、権限を持った複数人による操作により生成される。また、その内の 1 名だけでは生成できない。

利用者鍵ペアは、認証設備室内に設置された認証設備において、IC カードで認証された複数人の認証局員により生成される。

6.1.2 利用者への利用者秘密鍵送付

認証局で生成した利用者秘密鍵は、安全に IC カードへ格納され、速やかに利用者の住民票の写しまたは住民票記載事項証明書または登録原票記載事項証明書の記載住所へ、受取代人が指定されていない場合は、「本人限定受取郵便」（基本型）にて郵送し、受取代人が指定されている場合は、「本人限定受取郵便」（特例型）にて郵送する。なお、認証局で生成した利用者秘密鍵及び生成に利用した関連情報は、IC カードに格納後、遅延なく認証設備から完全に抹消される。また、IC カード PIN は、利用者本人以外に見られないように印刷された後、認証設備から完全に抹消される。

6.1.3 CA への公開鍵送付

ブリッジ認証局との相互認証証明書の取り交しに際して、認証局はブリッジ認証局から郵送又は手交された証明書発行要求ファイル（PKCS#10 フォーマットに従った公開鍵を含む）を受け取る。

利用者の鍵ペアは認証局が生成するため利用者からの利用者公開鍵の送付は受付けない。

6.1.4 利用者への CA 証明書送付

認証局 は、CA 証明書をリポジトリに格納し、公開する。

また、認証局から CD-ROM により、CA 証明書を配布する事がある。

6.1.5 鍵のサイズ

認証局で生成される鍵のアルゴリズム及びサイズは以下のとおりである。

認証局：RSA（2048bit）

利用者：RSA（1024bit）

6.1.6 公開鍵パラメータの生成

規定しない。

6.1.7 公開鍵パラメータの品質の検査

規定しない。

6.1.8 ハードウェア/ソフトウェアの鍵生成

認証局の CA 鍵ペアは、FIPS PUB 140-2 レベル 3 の認定を取得した暗号装置（HSM）を用いて生成する。

利用者の利用者鍵ペアは、安全なハードウェア、ソフトウェア環境のもと生成する。

6.1.9 鍵の利用目的

本 CP「7.1　電子証明書のプロファイル」の各証明書のプロファイルの「keyUsage」に規定している。

6.2 秘密鍵の保護

6.2.1 暗号装置に関する基準

認証局で使用する暗号装置は FIPS PUB 140-2 レベル 3 の認定を取得した HSM を用いる。利用者秘密鍵は IC カードに格納されており、IC カード PIN を入力する事で、利用者秘密鍵を活性化でき、利用者秘密鍵を使って署名を付与できる。

6.2.2 秘密鍵の複数人制御

CA 秘密鍵の生成・更新・廃棄・活性化・非活性化・バックアップ・リストアは、認証設備室内で複数人による操作で行い、その内の 1 名だけでは実行できない。また、その他 CA 秘密鍵に関する全ての操作についても、複数人による操作が必要であり、その内の 1 名だけでは実行できない。

6.2.3 秘密鍵の預託

CA 秘密鍵の預託は行わない。

6.2.4 秘密鍵のバックアップ

CA 秘密鍵のバックアップは、認証設備室内において複数人立会いのもとで行う。また、バックアップデータは暗号化され、リストアに必要な CA 秘密鍵に関する情報は分散される。各分散された符号は、それぞれ異なる場所にある、権限を有する認証局員のみが開錠できる耐火金庫内に保管される。

6.2.5 秘密鍵のアーカイブ

CA 秘密鍵のアーカイブは行わない。

6.2.6 暗号装置への秘密鍵の登録

CA 秘密鍵は、認証設備室内に設置された HSM 内で生成され、登録される。この操作は、複数人による操作が必要であり、その内の 1 名だけでは実行できない。

6.2.7 秘密鍵の活性化方法

CA 秘密鍵は、認証設備室内に設置された HSM 内で活性化される。この操作は、複数人による操作が必要であり、その内の 1 名だけでは実行できない。

6.2.8 秘密鍵の非活性化方法

CA 秘密鍵は、認証設備室内に設置された HSM 内で非活性化される。この操作は、複数人による操作が必要であり、その内の 1 名だけでは実行できない。

6.2.9 秘密鍵の破棄方法

CA 秘密鍵の廃棄は、複数人立会いのもと復元できない方法により廃棄する。また、CA 秘密鍵のバックアップ媒体は CA 秘密鍵の廃棄作業の一環として、遅滞なく物理的に破壊される。

6.3 鍵管理のその他の側面

6.3.1 公開鍵の履歴保管

認証局及び利用者証明書の公開鍵は、本 CP「4.6.2　帳簿の保管期間」において定義された期間、保管される。

6.3.2 秘密鍵の使用期間

CA 秘密鍵の使用期間は 5 年とする。但し、鍵長に対する暗号セキュリティが容認できないほど脆弱になった場合は、5 年より早く鍵ペアの更新を行う場合がある。

利用者秘密鍵の使用期間は 1 年 1 ヶ月、2 年 1 ヶ月、3 年 1 ヶ月または 4 年 1 ヶ月とする。

また、CA 証明書の有効期間は 10 年間、相互認証証明書の有効期間は 5 年以内、利用者証明書の有効期間は 1 年 1 ヶ月、2 年 1 ヶ月、3 年 1 ヶ月または 4 年 1 ヶ月とする。

6.4 活性化データ

6.4.1 活性化データの生成とインストール

CA 秘密鍵も含め、認証局内で使用される全ての活性化データの生成とインストールは、別途、事務取扱要領に規定され、実施される。

6.4.2 活性化データの保護

認証局内で使用される活性化データは、事務取扱要領にて取扱規則と手順を規定し、これを遵守する事で、保護される。

6.4.3 活性化データのその他の要件

認証局内での活性化データの取扱手順は別途、事務取扱要領に規定され、実施される。

6.5 コンピュータセキュリティ管理

6.5.1 特定のコンピュータセキュリティ技術要件

本 CP「1.1.1 関連規程」に示す CPS に規定する。

6.5.2 コンピュータセキュリティ評価

本 CP「1.1.1 関連規程」に示す CPS に規定する。

6.6 セキュリティ技術のライフサイクル管理

6.6.1 システム開発管理

本 CP「1.1.1 関連規程」に示す CPS に規定する。

6.6.2 セキュリティマネジメント管理

本 CP「1.1.1 関連規程」に示す CPS に規定する。

6.6.3 セキュリティ評価のライフサイクル

本 CP「1.1.1 関連規程」に示す CPS に規定する。

6.7 ネットワークセキュリティ管理

本 CP「1.1.1 関連規程」に示す CPS に規定する。

6.8 暗号装置の技術管理

本 CP「1.1.1 関連規程」に示す CPS に規定する。

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

認証局が発行する電子証明書の形式は ITU-T X.509 バージョン 3 および RFC3280 に従う。以下に CA 証明書（表 7.1）、リンク証明書（表 7.2）、相互認証証明書（表 7.3）及び利用者証明書（表 7.4）のプロファイルを示す。プロファイル中の「×」は設定しない事を表している。

(1) CA 証明書

表 7.1 CA 証明書プロファイル

領域名	OID	Critical	規定内容と設定値
基本部			
version			2（v3）
serialNumber			ユニークな値 (例：01317D2F00000003)
signature			sha1WithRSAEncryption (1.2.840.113549.1.1.5)
validity			証明書の有効期間（10 年有効）
notBefore			有効開始日時（yymmddhhmmssZ）
notAfter			終了日時（yymmddhhmmssZ）
issuer			証明書発行者の国名： c=JP 証明書発行者の組織名： o= e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
subject			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
subjectPublicKeyInfo			証明書所有者の公開鍵に関する情報
algorithm			RsaEncryption (1.2.840.113549.1.1.1)
subjectPublicKey			RSA 公開鍵値：2048bit
issuerUniqueID			×
subjectUniqueID			×

標準拡張領域			
AuthorityKeyIdentifier	2.5.29.35	FALSE	証明書発行者の公開鍵に関する情報
keyIdentifier			CA 公開鍵の SHA1 ハッシュ値
authorityCertIssure			
directoryName			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
authorityCertSerialNumber			CA 公開鍵のシリアル番号
SubjectKeyIdentifier	2.5.29.14	FALSE	証明書所有者の公開鍵に関する情報
keyIdentifier			subjectPublicKey の SHA1 ハッシュ値
KeyUsage	2.5.29.15	TRUE	鍵の使用目的
keyCertSign			1
cRLSign			1
ExtKeyUsageSyntax	2.5.29.37		×
PrivateKeyUsagePeriod	2.5.29.16		×
CertificatePolicies	2.5.29.32		×
PolicyMappings	2.5.29.33		×
IssuerAltName	2.5.29.18	FALSE	証明書発行者の別名
directoryName			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio 認証局 証明書発行者の部門名： ou=PS2 サービス （c は PrintableString、 その他は UTF8String）
SubjectAltName	2.5.29.17	FALSE	証明書所有者の別名
directoryName			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio 認証局 証明書発行者の部門名： ou=PS2 サービス （c は PrintableString、 その他は UTF8String）
BasicConstraints	2.5.29.	TRUE	基本的制限

cA	19		true
pathLenConstraint			NULL
NameConstraints	2.5.29.30		×
PolicyConstraints	2.5.29.36		×
CRLDistributionPoints	2.5.29.31	FALSE	ARL のリポジトリ登録先
distributionPoint			
fullName			
uniformResourceIdentifier			ldap://ldap.e-probatio.com/ou=e-probatio%20ps2,o=e-probatio%20ca,c=jp?authorityRevocationList
SubjectDirectoryAttributes	2.5.29.9		×
AuthorityInfoAccessSyntax	1.3.6.1.5.5.7.1.1		×
独自拡張領域			
なし			

(2) リンク証明書

リンク証明書の New with Old の有効期間開始日は New with New の有効期間開始日、有効期間終了日は Old with Old の有効期間終了日である。また、Old with New の有効期間開始日及び終了日は、ともに Old with Old の有効期間開始日及び終了日となる。

表 7.2　リンク証明書プロファイル

領域名	OID	Critical	規定内容と設定値
基本部			
version			2（v3）
serialNumber			ユニークな値 (例：01317D2F00000003)
signature			sha1WithRSAEncryption (1.2.840.113549.1.1.5)
validity			証明書の有効期間
notBefore			有効開始日時（yymmddhhmmssZ）
notAfter			終了日時（yymmddhhmmssZ）
issuer			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
subject			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
subjectPublicKeyInfo			証明書所有者の公開鍵に関する情報
algorithm			RsaEncryption (1.2.840.113549.1.1.1)
subjectPublicKey			RSA 公開鍵値：2048bit
issuerUniqueID			×
subjectUniqueID			×

標準拡張領域			
AuthorityKeyIdentifier	2.5.29.35	FALSE	証明書発行者の公開鍵に関する情報
keyIdentifier			CA 公開鍵の SHA1 ハッシュ値
authorityCertIssure directoryName			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
authorityCertSerialNumber			CA 公開鍵のシリアル番号
SubjectKeyIdentifier	2.5.29.35	FALSE	証明書所有者の公開鍵に関する情報
keyIdentifier			subjectPublicKey の SHA1 ハッシュ値
KeyUsage	2.5.29.15	TRUE	鍵の使用目的
keyCertSign			1
cRLSign			1
ExtKeyUsageSyntax	2.5.29.37		×
PrivateKeyUsagePeriod	2.5.29.16		×
CertificatePolicies	2.5.29.32	FALSE	
PolicyInfomation			
policyIdentifier			AnyPolicy（2.5.29.32.0）
PolicyMappings	2.5.29.33		×
IssuerAltName	2.5.29.18	FALSE	証明書発行者の別名
directoryName			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio 認証局 証明書発行者の部門名： ou=PS2 サービス （c は PrintableString、 その他は UTF8String）
SubjectAltName	2.5.29.17	FALSE	証明書所有者の別名
directoryName			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio 認証局 証明書発行者の部門名： ou=PS2 サービス （c は PrintableString、 その他は UTF8String）
BasicConstraints	2.5.29	TRUE	基本的制限

cA	9.19		true
pathLenConstraint			×
NameConstraints	2.5.29.30		×
PolicyConstraints	2.5.29.36		×
CRLDistributionPoints	2.5.29.31	FALSE	ARL のリポジトリ登録先
distributionPoint			
fullName			
uniformResourceIdentifier			ldap://ldap.e-probatio.com/ou=e-probatio%20ps2,o=e-probatio%20ca,c=jp?authorityRevocationList
SubjectDirectoryAttributes	2.5.29.9		×
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1		×
独自拡張領域			
なし			

(3) 相互認証証明書

相互認証証明書の有効期間は、以下の条件を満たす期間内で、相互接続先との同意の上、決定される。

・ 相互認証証明書の有効期間は 5 年以内であること

表 7.3　相互認証証明書プロファイル

領域名	OID	Critical	規定内容と設定値
基本部			
version			2（v3）
serialNumber			ユニークな値 (例：01317D2F00000003)
signature			sha1WithRSAEncryption (1.2.840.113549.1.1.5)
validity			証明書の有効期間
notBefore			有効開始日時（yymmddhhmmssZ）
notAfter			終了日時（yymmddhhmmssZ）
issuer			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
subject			証明書所有者の国名： c=JP 証明書所有者の組織名： o=Japanese Government 証明書所有者の部門名： ou=BridgeCA （c は PrintableString、 その他は UTF8String）
subjectPublicKeyInfo			証明書所有者の公開鍵に関する情報
algorithm			RsaEncryption (1.2.840.113549.1.1.1)
subjectPublicKey			RSA 公開鍵値：2048bit
issuerUniqueID			×
subjectUniqueID			×

標準拡張領域			
AuthorityKeyIdentifier	2.5.29.35	FALSE	証明書発行者の公開鍵に関する情報
keyIdentifier			CA 公開鍵の SHA1 ハッシュ値
authorityCertIssure			
directoryName			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
authorityCertSerialNumber			CA 公開鍵のシリアル番号
SubjectKeyIdentifier	2.5.29.35	FALSE	証明書所有者の公開鍵に関する情報
keyIdentifier			subjectPublicKey の SHA1 ハッシュ値
KeyUsage	2.5.29.15	TRUE	鍵の使用目的
keyCertSign			1
cRLSign			1
ExtKeyUsageSyntax	2.5.29.37		×
PrivateKeyUsagePeriod	2.5.29.16		×
CertificatePolicies	2.5.29.32	TRUE	
PolicyInfomation			
policyIdentifier			e-Probatio PS2 CP（0.3.4401.4.1.1.2）
policyQualifiers			
policyQualifierId			Id-qt-cps（1.3.6.1.5.5.7.2.1）
CPSuri			https://www.e-probatio.com/ps2/
policyQualifierId			Id-qt-unotice（1.3.6.1.5.5.7.2.2）
UserNotice			
noticeRef			
organization			e-Probatio CA
noticeNumbers			e-Probatio CA（0.3.4401.4.1）
explicitText			Accredited under e-Signature Law (Japan)
PolicyMappings		FALSE	
issuerDomainPolicy			e-Probatio PS2 CP（0.3.4401.4.1.1.2）
subjectDomainPolicy			id-bca-cp-ds.class10
IssuerAltName			×
directoryName			×
SubjectAltName			×
directoryName			×
BasicConstraints		TRUE	基本的制限

cA			true
pathLenConstraint			×
NameConstraints			×
PolicyConstraints		TRUE	ポリシ制約
requireExplicitPolicy			0
CRLDistributionPoints		FALSE	ARL のリポジトリ登録先
distributionPoint			
fullName			
uniformResource Identifier			ldap://ldap.e-probatio.com/ou=e-probatio%20ps2,o=e-probatio%20ca,c=jp?authorityRevocationList
SubjectDirectoryAttributes			×
AuthorityInfoAccess			×
独自拡張領域			
なし			

(4) 利用者証明書

subject 及び subjectAltName に記述されている値は例示（その他パラメータの値は設定値）であるため、利用者毎に異なる値が設定される。

表 7.4 利用者証明書プロファイル

領域名	OID	Critical	規定内容と設定値
基本部			
version			2（v3）
serialNumber			ユニークな値 (例：01317D2F00000003)
signature			sha1WithRSAEncryption (1.2.840.113549.1.1.5)
validity			証明書の有効期間（1 年 1 ヶ月、2 年 1 ヶ月、3 年 1 ヶ月または 4 年 1 ヶ月）
notBefore			有効開始日時（yymmddhhmmssZ）
notAfter			終了日時（yymmddhhmmssZ）
issuer			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
subject			証明書所有者の国名： c=JP 証明書所有者の居住都道府県名： s(st)=Osaka（例） 証明書所有者の居住住所名（都道府県名は除く）： l=Osaka-shi, chuo-ku, uchihonmachi 2-2-5 （例） 証明書所有者の固有名称： cn=Ninsho Taro　（例） （c は PrintableString、 その他は UTF8String）
subjectPublicKeyInfo			証明書所有者の公開鍵に関する情報
algorithm			RsaEncryption (1.2.840.113549.1.1.1)
subjectPublicKey			RSA 公開鍵値：1024bit
issuerUniqueID			×
subjectUniqueID			×
標準拡張領域			
AuthorityKeyIdentifier	2.5.29.35	FALSE	証明書発行者の公開鍵に関する情報
keyIdentifier			CA 公開鍵の SHA1 ハッシュ値

authorityCertIssure directoryName			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
authorityCertSerialNumber			CA 公開鍵のシリアル番号
SubjectKeyIdentifier	2.5.29.35	FALSE	証明書所有者の公開鍵に関する情報
keyIdentifier			subjectPublicKey の SHA1 ハッシュ値
KeyUsage	2.5.29.15	TRUE	鍵の使用目的
digitalSignature			1
nonRepudiation			1
ExtKeyUsageSyntax	2.5.29.37		×
PrivateKeyUsagePeriod	2.5.29.16		×
CertificatePolicies	2.5.29.32	TRUE	
PolicyInfomation			
policyIdentifier			e-Probatio PS2 CP（0.3.4401.4.1.1.2）
policyQualifiers			
policyQualifierId			Id-qt-cps（1.3.6.1.5.5.7.2.1）
CPSuri			https://www.e-probatio.com/ps2/
policyQualifierId			Id-qt-unotice（1.3.6.1.5.5.7.2.2）
UserNotice			
noticeRef			
organization			e-Probatio CA
noticeNumbers			e-Probatio CA（0.3.4401.4.1）
explicitText			Accredited under e-Signature Law (Japan)
PolicyMappings	2.5.29.33		×
IssuerAltName	2.5.29.18	FALSE	証明書発行者の別名
directoryName			証明書発行者の国名： c=JP 証明書発行者の組織名： o= e-Probatio 認証局 証明書発行者の部門名： ou=PS2 サービス （c は PrintableString、 その他は UTF8String）
SubjectAltName	2.5.29	FALSE	証明書所有者の別名

directoryName	9.17		証明書所有者の所属する会社住所の国名： c=JP 証明書所有者の所属する会社住所の都道府県名： s(st)=大阪 （例） 証明書所有者の所属する会社住所（都道府県名は除く）： l=大阪市中央区内本町二丁目２番５号（例） 証明書所有者の会社名： o=株式会社エヌ・ティ・ティ ネオメイト（例） 証明書所有者の固有名称： cn=認証　太朗（例） （c は PrintableString、 その他は UTF8String）
BasicConstraints	2.5.29.19		×
cA			×
pathLenConstraint			×
NameConstraints	2.5.29.30		×
PolicyConstraints	2.5.29.36		×
CRLDistributionPoints	2.5.29.31	FALSE	CRL のリポジトリ登録先
distributionPoint			
fullName			
uniformResourceIdentifier			ldap://ldap.e-probatio.com/ou=e-probatio%20ps2,o=e-probatio%20ca,c=jp?certificateRevocationList
SubjectDirectoryAttributes	2.5.29.9		×
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1		×
独自拡張領域			
なし			

7.2 CRL/ARL のプロファイル

認証局が発行する CRL/ARL の形式は X.509 バージョン 2 および RFC3280 に従う。以下に CRL（表 7.5）及び ARL（表 7.6）のプロファイルを示す。プロファイル中の「×」は設定しない事を表している。

(1) CRL

表 7.5　CRL プロファイル

領域名	OID	Critical	規定内容と設定値
基本領域			
version			V2(1)
signature			CRL への署名に使用された暗号アルゴリズム
algorithm			1.2.840.113549.1.1.5 sha1WithRSAEncription
issuer			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
thisUpdate			当該 CRL の発行日時 （yymmddhhmmssZ）
nextUpdate			次回発行予定日時（yymmddhhmmssZ） 48 時間後
revokedCertificates			
userCertificate			証明書のシリアルナンバ
revocationDate			失効申請実施日時（yymmddhhmmssZ）
crlEntryExtensions			
crlExtensions			
crlEntryExtensions			
CRLReason	2.5.29.21	FALSE	理由コード： [0]unspecified(未定義)
HoldInstructionCode	2.5.29.23		×
InvalidityDate	2.5.29.24		×
CertificateIssuer	2.5.29.29		×

crlExtensions			
AuthorityKeyIdentifier	2.5.29.35	FALSE	CRL 発行者の公開鍵に関する情報
keyIdentifier			CA 公開鍵の SHA1 ハッシュ値
authorityCertIssure			
directoryName			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
authorityCertSerialNumber			CA 公開鍵のシリアル番号
IssuerAltName	2.5.29.18		×
CRLNumber	2.5.29.20	FALSE	ユニークな値（シーケンス番号）
BaseCRLNumber	2.5.29.27		×
IssuingDistributionPoint	2.5.29.28	TRUE	発行者のリポジトリ登録先
distributionPoint			
fullName			
uniformResourceIdentifier			ldap://ldap.e-probatio.com/ou=e-probatio%20ps2,o=e-probatio%20ca,c=jp?certificateRevocationList
onlyContainsUserCerts			TRUE
onlyContainsCACerts			×

(2) ARL

表 7.6　ARL プロファイル

領域名	OID	Critical	規定内容と設定値
基本領域			
version			v2(1)
signature			ARL への署名に使用された暗号アルゴリズム
algorithm			1.2.840.113549.1.1.5 sha1WithRSAEncription
issuer			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
thisUpdate			当該 ARL の発行日時 （yymmddhhmmssZ）
nextUpdate			次回発行予定日時（yymmddhhmmssZ） 48 時間後
revokedCertificates			
userCertificate			証明書のシリアルナンバ
revocationDate			失効申請実施日時（yymmddhhmmssZ）
crlEntryExtensions			
crlExtensions			
crlEntryExtensions			
CRLReason	2.5.29.21	FALSE	理由コード： [0]unspecified(未定義)
HoldInstructionCode	2.5.29.23		×
InvalidityDate	2.5.29.24		×
CertificateIssuer	2.5.29.29		×

crlExtensions			
AuthorityKeyIdentifier	2.5.29.35	FALSE	ARL 発行者の公開鍵に関する情報
keyIdentifier			CA 公開鍵の SHA1 ハッシュ値
authorityCertIssure directoryName			証明書発行者の国名： c=JP 証明書発行者の組織名： o=e-Probatio CA 証明書発行者の部門名： ou=e-Probatio PS2 （c は PrintableString、 その他は UTF8String）
authorityCertSerialNumber			CA 公開鍵のシリアル番号
IssuerAltName	2.5.29.18		×
CRLNumber	2.5.29.20	FALSE	ユニークな値（シーケンス番号）
BaseCRLNumber	2.5.29.27		×
IssuingDistributionPoint	2.5.29.28	TRUE	発行者のリポジトリ登録先
distributionPoint			
fullName			
uniformResourceIdentifier			ldap://ldap.e-probatio.com/ou=e-probatio%20ps2,o=e-probatio%20ca,c=jp?authorityRevocationList
onlyContainsUserCerts			×
onlyContainsCACerts			TRUE

8　仕様の管理

本 CP「1.1.1 関連規程」に示す CPS に規定する。

8.1 仕様の変更手順

8.1.1 重要な変更

本 CP「1.1.1 関連規程」に示す CPS に規定する。

8.1.2 重要でない変更

本 CP「1.1.1 関連規程」に示す CPS に規定する。

8.2 ポリシの公表と通知

本 CP「1.1.1 関連規程」に示す CPS に規定する。

8.3 CP の承認手順

本 CP「1.1.1 関連規程」に示す CPS に規定する。

以　上