



e-Probatio 認証局 認証業務規程 (CPS)

バージョン 7.2

2011年10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 版	2002/11/20	初版作成	池本 恭英	小南 勝信
1.1 版	2002/12/04	OID の変更修正	池本 恭英	小南 勝信
1.2 版	2003/03/05	GPKI 相互認証接続申請に伴う 変更修正	池本 恭英	小南 勝信
1.3 版	2003/06/18	NTT-MS 本社移転に伴う住所変更 個人事業主への証明書発行を追加 利用者証明書の有効期間の変更	池本 恭英	小南 勝信
1.4 版	2003/08/28	相互認証証明書プロファイル変更	池本 恭英	小南 勝信
1.5 版	2003/11/10	情報公開 WEB サイトに公開する 情報の CA 証明書および CA 証明 書のフィンガープリントの追記 他	池本 恭英	小南 勝信
1.6 版	2004/03/22	特定サービスの追加 IC カード及び PIN 送付に伴う変 更修正 他	池本 恭英	小南 勝信
1.7 版	2004/11/20	商業登記簿謄本と呼ぶ書類の明確 化 他	池本 恭英	白子 匡博
1.8 版	2004/12/28	利用者証明書名義人の請求に基づ く情報の開示について詳細を追記	池本 恭英	白子 匡博
1.9 版	2005/01/18	特定サービスの追加	池本 恭英	白子 匡博
2.0 版	2005/03/10	認証業務規程の体系を変更 具体的には、認証局共通事項を認 証業務規程にサービス固有事項を 証明書ポリシーに記載	池本 恭英	白子 匡博
2.1 版	2005/03/25	社名変更に関する連絡を追記	池本 恭英	白子 匡博
3.0 版	2005/04/01	認証局運営会社をエヌ・ティ・テ ィ・メディアサプライ株式会社から 株式会社 NTT アプリエに変更	池本 恭英	白子 匡博
3.1 版	2005/10/14	オブジェクト識別子の変更 他	池本 恭英	白子 匡博
3.2 版	2005/12/12	GPKI 相互認証接続申請に伴う改 訂	池本 恭英	白子 匡博
4.0 版	2006/07/24	PS2 サービスに関する審査担当者 及び登録担当者の役割の変更	内田 充典	白子 匡博
4.1 版	2007/02/28	CA 秘密鍵の使用期間に関する変 更	谷 秀明	白子 匡博
5.0 版	2007/06/06	発行室新設に伴う変更	谷 秀明	白子 匡博
6.0 版	2008/03/07	PS2 サービスの利用者証明書の有 効期間及び利用者秘密鍵の利用期 間に 3 年 1 ヶ月、4 年 1 ヶ月を追 加	谷 秀明	岩崎 千明
6.1 版	2008/08/18	監査結果の通知先としてブリッジ 認証局を明記	谷 秀明	岩崎 千明

6.2 版	2008/10/29	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
6.3 版	2009/08/11	PS サービス廃止に伴う改訂	中浦 修	寺田 博志
6.4 版	2009/10 /26	文書表現の変更	中浦 修	寺田 博志
7.0 版	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
7.1 版	2010/10/18	・誤字修正 ・システムログの検査周期を修正	播岡 俊彦	土屋 直広
7.2 版	2011/10/18	・誤字修正	播岡 俊彦	清水 仁志

— 目次 —

1	はじめに.....	1
1.1	概要.....	1
1.1.1	関連規程.....	1
1.2	識別.....	1
1.3	関係主体と電子証明書の適用範囲.....	2
1.3.1	本 CPS の適用範囲.....	2
(1)	認証局.....	2
(2)	発行局 (IA).....	2
(3)	登録局 (RA).....	3
(4)	利用者.....	3
(5)	署名検証者.....	3
(6)	相互認証先認証局.....	3
1.3.2	電子証明書の適用範囲.....	3
1.3.3	電子署名法に関する特別な要件.....	3
(1)	属性等についての説明.....	3
(2)	虚偽の利用申込みに対する罰則.....	3
(3)	電子署名の法的効果.....	3
(4)	利用者証明書の失効申込について.....	4
(5)	電子署名に使用するアルゴリズム.....	4
1.4	CPS 管理.....	4
1.4.1	管理組織.....	4
1.4.2	対応窓口.....	4
1.4.3	CPS 責任者.....	5
2	一般規定.....	6
2.1	義務.....	6
2.1.1	IA の義務.....	6
(1)	利用者に対する義務.....	6
(2)	相互認証先認証局に対する義務.....	6
(3)	署名検証者に対する義務.....	6
2.1.2	RA の義務.....	6
2.1.3	利用者の義務.....	6
(1)	正確な利用申込み内容の提示.....	6
(2)	利用者証明書の利用制限.....	7
(3)	IC カードと IC カード PIN の管理義務.....	7
(4)	利用者証明書記載事項の管理.....	7

(5) 速やかな利用者証明書失効申込み	7
(6) 署名アルゴリズム	7
2.1.4 署名検証者の義務	7
(1)利用者証明書の利用制限	7
(2)電子証明書の有効性確認	7
2.1.5 リポジトリの義務	7
2.2 責任	7
2.2.1 認証局の責任	7
2.2.2 利用者の責任	8
2.2.3 署名検証者の責任	8
2.3 財務上の責任	8
2.4 解釈及び執行	8
2.4.1 準拠法等	8
2.4.2 分割、存続、合併及び通知	8
2.4.3 紛争解決の手続	8
2.5 料金	9
2.6 公開とリポジトリ	9
2.6.1 認証局に関する情報の公開	9
(1)リポジトリに公開する情報	9
(2) 情報公開 WEB サイトに公開する情報	9
2.6.2 公開の頻度	9
2.6.3 アクセスコントロール	9
2.6.4 リポジトリ	10
(1)リポジトリの URL	10
(2) 情報公開 WEB サイトの URL	10
2.7 準拠性監査	10
2.7.1 監査頻度	10
2.7.2 監査人の身元/資格	10
2.7.3 被監査部門と監査人の関係	10
2.7.4 監査項目	10
2.7.5 監査指摘事項への対応	10
2.7.6 監査結果の通知	11
2.8 機密保持	11
2.8.1 機密情報	11
2.8.2 機密情報対象外の情報	11
2.8.3 電子証明書失効リストの開示	11

2.8.4	法執行機関への開示	11
2.8.5	民事上の手続き	11
2.8.6	利用者証明書名義人の請求に基づく情報の開示	11
2.8.7	その他の事由に基づく情報公開	12
2.9	知的財産権	12
2.10	個人情報保護	12
3	識別と認証	13
3.1	初期登録	13
3.1.1	名前の型	13
3.1.2	名前の意味に関する要件	13
3.1.3	様々な名前形式を解釈するための規則	13
3.1.4	名前の一意性	13
3.1.5	名前に関する紛争の解決手段	13
3.1.6	商標の認識・認証・役割	13
3.1.7	秘密鍵の所有を証明するための方法	13
(1)	相互認証先認証局	13
(2)	利用者	13
3.1.8	組織の認証	13
3.1.9	個人の認証	13
3.2	電子証明書の更新	14
(1)	相互認証証明書	14
(2)	利用者証明書	14
3.3	電子証明書失効後の再発行	14
3.4	電子証明書の失効要求	14
4	オペレーション要件	15
4.1	電子証明書の発行申請	15
4.1.1	電子証明書の発行要求	15
(1)	相互認証証明書	15
(2)	利用者証明書	15
4.1.2	要求データの送付手段	15
(1)	相互認証証明書	15
(2)	利用者証明書	15
4.2	電子証明書の発行	15
4.2.1	審査	15
4.2.2	電子証明書の発行	15
(1)	相互認証証明書	15

(2) 利用者証明書	15
4.3 電子証明書の受入れ	15
(1) 相互認証証明書	15
(2) 利用者証明書	15
4.4 電子証明書の一時停止と失効	16
4.4.1 電子証明書の失効事由	16
(1) 相互認証証明書	16
(2) 利用者証明書	16
4.4.2 失効申込者	16
(1) 相互認証証明書	16
(2) 利用者証明書	16
4.4.3 失効処理手順	16
(1) 相互認証証明書	16
(2) 利用者証明書	16
4.4.4 失効における猶予期間	16
4.4.5 電子証明書の一時停止事由	16
4.4.6 一時停止申請者	16
4.4.7 一時停止手順	16
4.4.8 一時停止期間の制限	16
4.4.9 CRL/ARL 発行周期	17
4.4.10 CRL/ARL の確認要件	17
4.4.11 オンライン有効性確認の可用性	17
4.4.12 オンライン失効確認要件	17
4.4.13 その他利用可能な有効性確認手段	17
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	17
4.4.15 CA 秘密鍵の危殆化に関する特別な要件	17
4.5 セキュリティ監査	17
4.5.1 記録されるイベントの種類	17
(1) 監査対象システムのログ検査	17
(2) リポジトリのシステムログ検査	18
4.5.2 システムログの検査周期	18
4.5.3 システムログの保存期間	18
4.5.4 システムログの保護	18
4.5.5 システムログのバックアップ手順	18
4.5.6 システムログの収集	18
4.5.7 イベントを引き起こした人への通知	18

4.5.8 脆弱性の評価	18
4.6 帳簿の保存	19
4.6.1 保存する帳簿の種類	19
(1) 利用者証明書の利用申込みに関する次の文書	19
(2) 利用者証明書の失効に関する次の文書	19
(3) 認証局の組織管理に関する次の文書	19
(4) 設備及び安全対策措置に関する次の文書	19
4.6.2 帳簿の保管期間	19
(1) 4.6.1(1)～(3)の文書	19
(2) 4.6.1(4)の文書	19
4.6.3 帳簿の保護	20
4.6.4 帳簿の保存媒体	20
4.6.5 帳簿の時にに関する要件	20
4.6.6 電子媒体の可読性維持	20
4.6.7 保存状態の確認と検証の手順	20
4.7 鍵更新	21
4.8 危殆化と災害からの復旧	21
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	21
4.8.2 電子証明書の失効処理の特別な対処	21
4.8.3 CA の秘密鍵が危殆化した場合の対処	21
4.8.4 災害等発生後の安全な設備の確保	21
4.9 CA 業務の終了	21
5 物理的、手続上、人事上のセキュリティ管理	22
5.1 物理的セキュリティ	22
5.1.1 サイトの位置と建物構造	22
5.1.2 物理アクセス	22
(1) 認証設備室	22
(2) 登録端末室	22
(3) 発行室	22
5.1.3 電源設備と空調設備	23
5.1.4 水害対策	23
5.1.5 地震対策	23
5.1.6 火災対策	23
5.1.7 媒体管理	23
5.1.8 廃棄物処理	23
5.1.9 オフサイトバックアップ	24

5.2 手続上の管理.....	24
5.2.1 信頼される役割.....	24
5.2.2 役割毎の必要人員.....	25
5.2.3 役割毎の識別と認証.....	25
5.3 人事管理.....	25
5.3.1 経歴、適正、経験、信頼性の要件.....	25
5.3.2 経歴審査手順.....	26
5.3.3 トレーニングの要件.....	26
5.3.4 再トレーニングの周期と要件.....	26
5.3.5 配置転換の周期と順序.....	26
5.3.6 許可されていない行動に対する罰則.....	26
5.3.7 個人との契約要件.....	26
5.3.8 要員に提供される文書.....	26
6 技術的セキュリティ管理.....	27
6.1 鍵ペア生成とインストール.....	27
6.1.1 鍵ペア生成.....	27
6.1.2 利用者への利用者秘密鍵送付.....	27
6.1.3 CA への公開鍵送付.....	27
6.1.4 利用者への CA 証明書送付.....	27
6.1.5 鍵のサイズ.....	27
6.1.6 公開鍵パラメータの生成.....	27
6.1.7 公開鍵パラメータの品質の検査.....	27
6.1.8 ハードウェア/ソフトウェアの鍵生成.....	27
6.1.9 鍵の利用目的.....	27
6.2 秘密鍵の保護.....	27
6.2.1 暗号装置に関する基準.....	27
6.2.2 秘密鍵の複数人制御.....	27
6.2.3 秘密鍵の預託.....	28
6.2.4 秘密鍵のバックアップ.....	28
6.2.5 秘密鍵のアーカイブ.....	28
6.2.6 暗号装置への秘密鍵の登録.....	28
6.2.7 秘密鍵の活性化方法.....	28
6.2.8 秘密鍵の非活性化方法.....	28
6.2.9 秘密鍵の破棄方法.....	28
6.3 鍵管理のその他の側面.....	28
6.3.1 公開鍵の履歴保管.....	28

6.3.2	秘密鍵の使用期間.....	28
6.4	活性化データ	29
6.4.1	活性化データの生成とインストール	29
6.4.2	活性化データの保護.....	29
6.4.3	活性化データのその他の要件.....	29
6.5	コンピュータセキュリティ管理	29
6.5.1	特定のコンピュータセキュリティ技術要件.....	29
6.5.2	コンピュータセキュリティ評価	29
6.6	セキュリティ技術のライフサイクル管理.....	29
6.6.1	システム開発管理	29
6.6.2	セキュリティマネジメント管理	30
6.6.3	セキュリティ評価のライフサイクル	30
6.7	ネットワークセキュリティ管理	30
6.8	暗号装置の技術管理.....	30
7	電子証明書と CRL (ARL) のプロファイル	31
7.1	電子証明書のプロファイル	31
7.2	CRL/ARL のプロファイル.....	31
8	仕様の管理	32
8.1	仕様の変更手順.....	32
8.2	ポリシーの公表と通知.....	32
8.3	CPS の承認手順.....	32

1 はじめに

本 e-Probatio 認証局認証業務規程（以下、本 CPS 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。）の全ての認証業務に関する規程である。

本 CPS の構成は、Internet Engineering Task Force (IETF) Public Key Infrastructure X. 509 (IETF PKIX) による RFC2527 「Certificate Policy and Practice Statement Framework」に準拠する。また、本 CPS の記述においては、RFC2527 で定められる項目の全てを記載し、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。

なお、従来認証局を運営していたエヌ・ティ・ティ・メディアサプライ株式会社の電子認証サービス事業部が平成 17 年 4 月 1 日をもって NTT アプリエに営業譲渡され、その後、NTT アプリエは、平成 22 年 7 月 1 日をもって NTT ネオメイトと合併したため、認証局の運営は平成 22 年 7 月 1 日から NTT ネオメイトが行っている。

1.1 概要

本 CPS では、公開鍵インフラストラクチャ（PKI : Public Key Infrastructure）の構成要素である認証局、利用者及び署名検証者の責任について記述している。また、本 CPS は、認証局が発行する全ての電子証明書に関する内容を定めている。

1.1.1 関連規程

認証局は、認証局が提供するサービスごとに証明書ポリシー（以下、CP と呼ぶ。）を定め、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規定する。

認証局は、本 CPS 及び各 CP（以下、本 CPS 等と呼ぶ。）に基づく各々の業務手順の詳細を事務取扱要領及び関係書類として規定し、認証局に従事する者は、本 CPS 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 CPS 等の改訂が行われた場合は、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

認証業務規程及び認証業務提供主体のオブジェクト識別子を表 1.2 に示す。また、本 CPS 等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 認証業務規程及び認証業務提供主体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

1.3 関係主体と電子証明書適用範囲

1.3.1 本 CPS の適用範囲

本 CPS 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。認証局により発行される全ての電子証明書には、本 CPS が適用される。

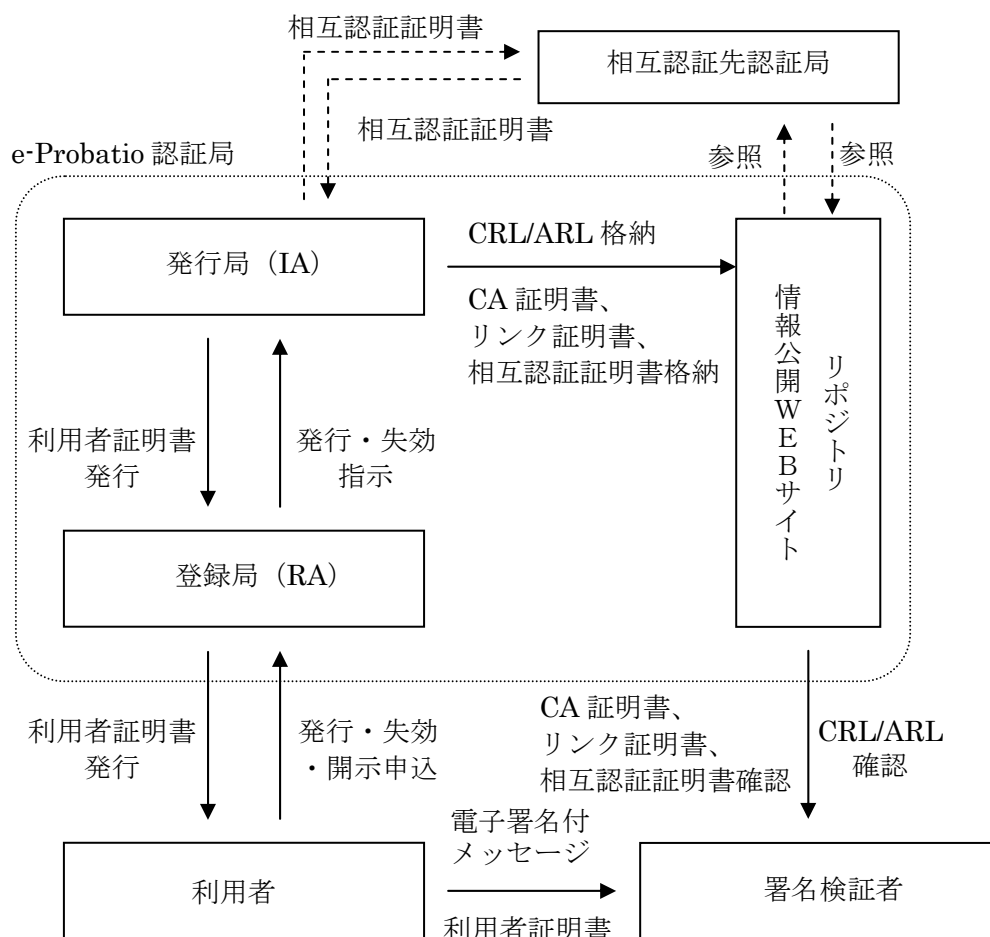


図 1.3 e-Probatio 認証局のコミュニティ

(1) 認証局

認証局は、発行局 (IA) と登録局 (RA) で構成され、NTT ネオメイトにより運用される。但し、本 CPS の遵守を条件に、認証業務の一部を外部委託する事ができる。

(2) 発行局 (IA)

認証局は、発行業務を発行局 (IA) (以下、IA と呼ぶ。) で行う。発行業務とは、本 CPS に従い、登録局からの発行指示により電子証明書の発行処理、失効処理及び電子証明書失効リスト (以下、CRL/ARL と呼ぶ。) の発行処理を行う事をいう。また、認証局署名符号 (以

下、CA 秘密鍵と呼ぶ。)の生成、維持等の管理も行う。なお、リポジトリの管理は IA が行う。

(3) 登録局 (RA)

認証局は、登録業務を登録局 (RA) (以下、RA と呼ぶ。)で行う。RA は、本 CPS に従い、利用者証明書の利用申込者と失効申込者の本人確認及び IA への利用者証明書発行、利用者証明書失効指示を行う。また、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。利用者証明書発行、利用者証明書失効指示は、安全な通信方法を介して登録端末室に設置した登録端末設備から行う。

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

(4) 利用者

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(5) 署名検証者

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(6) 相互認証先認証局

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

1.3.2 電子証明書の適用範囲

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

1.3.3 電子署名法に関する特別な要件

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(1) 属性等についての説明

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 虚偽の利用申込みに対する罰則

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(3) 電子署名の法的効果

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(4) 利用者証明書の失効申込について

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(5) 電子署名に使用するアルゴリズム

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

1.4 CPS 管理

1.4.1 管理組織

認証局の運営主体は NTT ネオメイトであり、NTT ネオメイトは本 CPS 等に従って、認証局を運営管理する責任を負う。

又、認証局で設置する会議体の名称と役割及び責任を表 1.4 に示す。

表 1.4 会議体の役割と構成員

会議体名称	役割	責任	構成員
経営会議	<ul style="list-style-type: none"> • 認証サービスの存続に関する事項の決定 • 重大な災害・障害等に関する事項の対応 • その他認証局代表者が必要と認めた事項の検討等 	e-Probatio 認証局運営会社である NTT ネオメイトの経営責任	代表取締役社長、本社組織の長
認証業務運営検討会	<ul style="list-style-type: none"> • 通常運営時における最終意思決定 • 認証業務規程 (CPS) 及び証明書ポリシー (CP) の改訂 • 相互認証業務における最終意思決定 	e-Probatio 認証局の運営責任	認証局代表者 業務責任者 設備責任者

1.4.2 対応窓口

本 CPS 等に関する問い合わせは、電話、FAX、E-mail にて受付ける。

【問い合わせ先】

窓口 : 株式会社エヌ・ティ・ティ ネオメイト

電子認証サービス担当

住所 : 〒530-0003 大阪市北区堂島 3-1-21 NTT データ堂島ビル 10 階

営業日 : 月曜日から金曜日 (祝祭日、年末年始を除く)

受付時間 : 9:00~12:00、13:00~17:00 (営業日のみ)

電話 : 06-6348-1015

FAX : 06-6348-1016

E-mail : ninshou@e-probatio.com

1.4.3 CPS 責任者

本業務の本 CPS 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、以下の各項目の義務を負う。

- ・ 認証局の CA 秘密鍵を安全に生成し、危殆化する事のないよう運用管理する
- ・ 本 CPS 等に基づき、IA の運営を行う
- ・ IA 業務に関して、本 CPS 等に基づいた事務取扱要領を規定する
- ・ 責任者を一名配置する
- ・ 本 CPS 等及び別途定める事務取扱要領に基づき、RA からの指示に従って利用者証明書の発行を行う

の発行を行う

- ・ 本 CPS 等及び別途定める事務取扱要領に基づき、RA からの指示に従って利用者証明書

の失効を行う

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

(2) 相互認証先認証局に対する義務

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(3) 署名検証者に対する義務

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

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 CPS 等に基づき、RA の運営を行う
- ・ RA 業務に関して、本 CPS 等に基づいた事務取扱要領を規定する
- ・ 責任者を一名配置する。

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

2.1.3 利用者の義務

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(1) 正確な利用申込み内容の提示

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 利用者証明書の利用制限

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(3) IC カードと IC カード PIN の管理義務

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(4) 利用者証明書記載事項の管理

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(5) 速やかな利用者証明書失効申込み

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(6) 署名アルゴリズム

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

2.1.4 署名検証者の義務

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(1) 利用者証明書の利用制限

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 電子証明書の有効性確認

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

2.1.5 リポジトリの義務

認証局は、本 CPS 「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、本 CPS 等に規定する義務を履行する責任がある。但し、以下を免責事項とする。

利用者の利用者証明書の取得又は利用により、利用者及び署名検証者等が使用するコンピュータシステム等のハードウェア・ソフトウェアに何らかの影響・障害が発生しても、認証局は、その責を一切負わないものとする

NTT ネオメイトは、以下に定める事由のいずれかに起因して利用者が損害を受けた場合

であっても、一切の賠償責任を負わないものとする

- ・地震、噴火、津波、台風等の自然災害に起因して損害が発生した場合
- ・火災、停電、公共サービス機関の業務停止等に起因して損害が発生した場合
- ・戦争、テロ、暴動、変乱、争乱、労働争議に起因して損害が発生した場合
- ・放射性物質、爆発性物質、環境汚染物質に起因して損害が発生した場合
- ・関係法令の制定・改正、又は裁判所もしくは行政庁の処分があった場合
- ・その他、不可抗力により損害が発生した場合

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

2.2.2 利用者の責任

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

2.2.3 署名検証者の責任

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

2.3 財務上の責任

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

2.4 解釈及び執行

2.4.1 準拠法等

本 CPS 等の成立、解釈及び履行、認証局と関係者の中で係争が生じた場合等は全て、日本国内の法律に準拠するものとする。

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

2.4.2 分割、存続、合併及び通知

認証局が業務を終了した場合においても本 CPS 「2.8 機密保持」の効力は存続する。

利用者及び署名検証者が、本 CPS 等 に対して何らかの通知、請求、依頼をする場合の連絡手段は、郵送によって行わなければならない。

また、本 CPS 等内にある項目に誤りがある事が判明した場合、該当部分以外の、他の項目は有効なままとする。本 CPS 等の改訂は、本 CPS 「8 仕様の管理」に規定した手続きに従って行われる。

2.4.3 紛争解決の手続

認証局が発行した電子証明書やサービスに対して、認証局に訴訟や仲裁を含む解決手段に訴えようとする者は、認証局に対して、事前にその旨を通知しなければならない。

認証局が提供するサービスに関するあらゆる紛争を法廷にて解決を図る場合は、大阪地

方裁判所を第一審の専属的合意管轄裁判所とする。

2.5 料金

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

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

認証局は、利用者が認証局を利用する上で必要となるリポジトリ及び情報公開 WEB サイトは、1 日 24 時間、1 週 7 日利用可能とする。但し、システム保守作業などにより予め通知して、一時的に停止する事がある。また、緊急時など止むを得ない場合は、事前に通知できない場合もある。

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

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 情報公開 WEB サイトに公開する情報

- ・ 本 CPS
- ・ e-Probatio 認証局 個人情報取扱要領

その他については、本 CPS 「1.1.1 関連規程」に示す各 CP 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

リポジトリ上に情報を公開するタイミングは、次のとおりである。

- ・ 本 CPS 等の公開タイミングは、本 CPS 「8 仕様の管理」に規定に則り変更され、その都度公開される。同様に他の情報公開 WEB サイトに公開される公開情報に関しても、変更がある度毎に、随時変更、公開される。
- ・ 認証局が提供するサービスの内、e-Probatio PS2 サービスについては CRL/ARL の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。

その他については、本 CPS 「1.1.1 関連規程」に示す各 CP 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。

また情報公開 WEB サイトに関しては、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

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 情報公開 WEB サイトの URL

<https://www.e-probatio.com/> (トップページ)

2.7 準拠性監査

2.7.1 監査頻度

認証局は、認証局代表者の指定する監査人によって、年に 1 回の準拠性監査を実施する。なお、認証局代表者は、必要に応じて準拠性監査以外に個別監査を実施する。定期監査については、監査に係る基準を定めてそれに従って実施する。

2.7.2 監査人の身元/資格

システム監査、PKI 及びシステムセキュリティに関する知識と技能を持ち合わせる者を認証局代表者が監査人に指定する。

2.7.3 被監査部門と監査人の関係

認証局代表者が指定する監査人は、認証局の運用管理部門以外の監査対象領域から独立した者を条件とする。

2.7.4 監査項目

準拠性監査の監査項目は、本 CPS 等及び事務取扱要領に準拠している事を中心に監査を実施する。

2.7.5 監査指摘事項への対応

認証局は、監査における指摘事項に対する改善措置を実施する。改善措置は、認証局代表者の指示のもとに実施する。

また、改善措置は監査における指摘事項だけでなく、セキュリティ対策技術の最新動向も踏まえた上で実施し、併せて改善措置の評価を実施する。

2.7.6 監査結果の通知

監査人は、準拠性監査の結果を報告書として認証局代表者へ提出する。認証局は、監査結果を公表しない。但し、認証局は、認証局の監査人又は法的根拠に基づく開示要求の下での法執行機関、電子署名法における指定調査機関、ブリッジ認証局に対し、監査結果を開示する事もある。

2.8 機密保持

2.8.1 機密情報

認証局は、認証局が保持する情報のうち、リポジトリ及び情報公開 WEB サイトに公開している情報を除いて、全ての情報を機密情報として扱う。個人情報の取扱いについては、本 CPS 「2.10 個人情報保護」にて規定する。

また、認証局は本 CPS 等において開示する事を規定している場合を除いて、原則これらの情報を開示しない。

2.8.2 機密情報対象外の情報

認証局は、次の情報を機密保持対象としない。

- ・ 電子証明書、CRL/ARL に含まれている情報及び本 CPS 等に記載された情報
- ・ 電子証明書の発行対象者以外から、機密条項無しで認証局に知らされた情報
- ・ 本 CPS 等において開示する事を規定している情報

2.8.3 電子証明書失効リストの開示

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

2.8.4 法執行機関への開示

認証局は、法的根拠に基づく裁判所もしくは行政庁の命令、調査その他認証局が情報を開示すべき法的義務を負う場合は、利用者の個人情報その他認証局で取扱う情報を開示する場合がある。

2.8.5 民事上の手続き

認証局は、訴訟等の法的手続において主張・立証の必要が生じた場合には、利用者の個人情報その他認証局で取扱う情報を開示する場合がある。

2.8.6 利用者証明書名義人の請求に基づく情報の開示

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

2.8.7 その他の事由に基づく情報公開

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

2.9 知的財産権

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

2.10 個人情報保護

認証局は認証局が提供する各サービスに対し利用者から提供される個人情報について当該サービスに係わる業務の用に供する目的以外の目的で使用しない。また、個人情報の保護に関する日本の法令その他規範を遵守し、個人情報の収集は当該サービスの提供に必要な範囲を超えて行わない。

認証局は、その取扱いを徹底するために、認証局員を対象とした個人情報の取扱い及び保護に関する教育訓練計画書を策定し、定期的を実施する。

認証局は、「e-Probatio 認証局 個人情報取扱要領」を策定し、それに従い個人情報を取り扱っている。また本要領は情報公開 WEB サイトに公開する。

個人情報の取扱い及び保護として、個人情報を記録した書類、電子媒体を許可された者以外がアクセスできない場所に保管し、滅失、改ざん及び漏洩から保護する。

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

3 識別と認証

3.1 初期登録

3.1.1 名前の型

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

3.1.2 名前の意味に関する要件

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

3.1.3 様々な名前形式を解釈するための規則

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

3.1.4 名前の一意性

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

3.1.5 名前に関する紛争の解決手段

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

3.1.6 商標の認識・認証・役割

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

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

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 利用者

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

3.1.8 組織の認証

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

3.1.9 個人の認証

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

3.2 電子証明書の更新

(1) 相互認証証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 利用者証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

3.3 電子証明書失効後の再発行

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

3.4 電子証明書の失効要求

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

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

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 利用者証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.1.2 要求データの送付手段

(1) 相互認証証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 利用者証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.2 電子証明書の発行

4.2.1 審査

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.2.2 電子証明書の発行

(1) 相互認証証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 利用者証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.3 電子証明書の受入れ

(1) 相互認証証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 利用者証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4 電子証明書の一時的停止と失効

4.4.1 電子証明書の失効事由

(1) 相互認証証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 利用者証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.2 失効申込者

(1) 相互認証証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 利用者証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.3 失効処理手順

(1) 相互認証証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 利用者証明書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.4 失効における猶予期間

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.5 電子証明書の一時的停止事由

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.6 一時的停止申請者

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.7 一時的停止手順

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.8 一時的停止期間の制限

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.9 CRL/ARL 発行周期

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.10 CRL/ARL の確認要件

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.11 オンライン有効性確認の可用性

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.12 オンライン失効確認要件

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.13 その他利用可能な有効性確認手段

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

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

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.4.15 CA 秘密鍵の危殆化に関する特別な要件

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

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

監査対象となるシステム機器毎のアクセスログ、操作ログ、認証ログ（以下システムログと呼ぶ。）を記録する。システムログには、次の項目を含める。

- ・各イベントを起こした者の識別
- ・各イベント要求の発行先
- ・各イベントの種類
- ・各イベント発生日時
- ・各イベントの成否

なお、監査対象となる認証設備の内容は、事務取扱要領に規定する。

(1) 監査対象システムのログ検査

設備責任者は、監査対象となるシステム機器を設置している部屋の入退室を管理する帳簿と、該当する認証設備及びネットワーク設備のシステムログの照合を行い、不正操作の

有無を検査する。また、認証設備及びネットワーク設備のシステムログの確認を行い、運用面、システム面におけるセキュリティ上の脆弱性を検査する。検査結果は記録し、保存する。

(2) リポジトリのシステムログ検査

設備責任者は、リポジトリのシステムログと実際の運用状況の照合を行い、運用面、システム面におけるセキュリティ上の脆弱性、不正操作の有無を検査する。検査結果は記録し、保存する。

4.5.2 システムログの検査周期

システムログの検査周期は、月に一回以上である。

4.5.3 システムログの保存期間

システムログは、生成又は追記した日から1年間保存する。但し、保存期間終了後も必要に応じてシステムログを保存する事がある。

4.5.4 システムログの保護

システムログは、定期的に改ざんが困難な媒体に保存され、保護される。システムログのバックアップは、施錠可能な書庫に施錠し、保管する。また、権限者以外は、システムログの閲覧及び削除はできない。

4.5.5 システムログのバックアップ手順

システムログは、別媒体でバックアップし、認証設備室の書庫に保管する。なお、認証設備のバックアップの方法については、事務取扱要領に規定し、実施する。

4.5.6 システムログの収集

認証設備はシステムログを記録する。設備責任者によってシステムログを別媒体に収集する。

4.5.7 イベントを引き起こした人への通知

イベントを引き起こした人への通知は行わない。

4.5.8 脆弱性の評価

設備責任者は、システムログ検査の結果から、運用面、システム面でのセキュリティ上の脆弱性がないか評価する。

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

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(2) 利用者証明書の失効に関する次の文書

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

(3) 認証局の組織管理に関する次の文書

本 CPS 等及びその改訂に関する記録

e-Probatio 認証局 個人情報取扱要領

認証局員任命解任記録

e-Probatio 認証局監査計画書兼実施記録簿

e-Probatio 認証局改善報告書

事務取扱要領等、認証局の組織管理における内部文書及び内部処理の記録

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

(4) 設備及び安全対策措置に関する次の文書

認証設備室入退室記録

登録端末室入退室記録簿

障害及びその復旧に関する記録

システムログ検査管理簿

生体認証装置への権限者登録記録等

認証局の設備や安全対策に関する内部処理の記録

その他については、本 CPS 「1.1.1 関連規程」に示す各 CP 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

当該帳簿書類に係る利用者証明書の有効期間が満了してから 10 年間。

(2) 4.6.1(4)の文書

生成又は追記した日から 1 年間保存する。但し、保存期間終了後も必要に応じて保存する事がある。

4.6.3 帳簿の保護

- ・ 認証局は、帳簿の滅失・毀損及び情報の漏えいを防止するために、次の措置を講じている。
- ・ 帳簿は、直射日光が当たらないように書庫に保管する
- ・ 書庫は施錠可能な室内に設置する
- ・ 書庫は防火区画内に設置する
- ・ 害虫対策を施す
- ・ 紙媒体で保存される帳簿は、ファイルに綴じる
- ・ 電子媒体（光媒体及び磁気媒体）で保存される帳簿は、その媒体を適切なケースに格納する
- ・ 磁気媒体で保存される帳簿は、その媒体を防磁ケースに格納する又は防磁された場所に保管する
- ・ 帳簿保存する室には、自動火災報知器及び消火装置を設置する
- ・ 帳簿保存する室は、間仕切り等で区分された室である
- ・ 原本で保存される資料等について、原本上の記録が判読不能とならない環境を備えている

4.6.4 帳簿の保存媒体

認証局は、帳簿の保存対象となる文書であって、利用者又は認証局員等の署名又は押印が付されていないものは、電子媒体で保存することができる。認証局は、各帳簿に応じた保存媒体を別途定める事務取扱要領で特定し、それに従って保存する。

4.6.5 帳簿の時に関する要件

帳簿の保存対象となる文書であって、日時の記録が必要なものは、日本標準時を基に記録する。

4.6.6 電子媒体の可読性維持

認証局は、電子媒体で保存される帳簿書類に対し、その可読性を保証するために、当該電子媒体の内容を表示できる機器、ソフトウェアを保持する。機器・ソフトウェアの保持が困難な場合は、当該電子媒体の内容を表示が可能な新しい電子媒体へ移す事によって可読性を維持する。この複製の作成にあたっては、セキュリティ上安全な場所にて複数人で実施し、複製情報の完全性及び機密性を維持する。

4.6.7 保存状態の確認と検証の手順

認証局は、帳簿書類の滅失、毀損及び情報の漏えい防止を予防するため、年1回、数点の帳簿書類をサンプリングする事により、帳簿の保存状態を検査する。

4.7 鍵更新

認証局が提供するサービスの内、e-Probatio PS2 サービスについては、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。

同時に CA 証明書の更新も実施され、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。

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

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

認証局にかかわるハードウェア、ソフトウェア、データが損傷又は滅失された場合、バックアップ用のハードウェア、バックアップデータによって、できるだけ迅速に復旧作業を行う。

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

4.8.2 電子証明書の失効処理の特別な対処

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.8.3 CA の秘密鍵が危殆化した場合の対処

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.8.4 災害等発生後の安全な設備の確保

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

4.9 CA 業務の終了

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

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

認証局の施設は、想定される火災、水害、震災に対して十分な措置が講じられた施設内に設置する。また、施設は独自の防犯設備を備えており、不正侵入から防護された安全な施設内に設置する。

5.1.2 物理アクセス

施設は入退室管理上、複数のセキュリティレベルに分かれている。認証局に関する機器を設置する部屋には、認証設備室、登録端末室、発行室等がある。また、それぞれの部屋は区画されており、異なるセキュリティレベルを設定している。

(1) 認証設備室

認証設備室は、電子証明書の生成・管理を行う最も重要な機器が設置される部屋である。火災、水害、震災への措置及び、空気調和機や無停電電源 (UPS と自家発電装置)、モーションセンサ、監視モニタを設置する。

入退室については生体認証装置で管理し、権限のある者の2名以上の認証で入室可能となっている。止むを得ず権限が無いものが入室する場合は、事前に設備責任者が許可した者のみ、複数人の入室権限者と同伴で入室を認める。

また、入室権限者複数名による入室および入室権限を持たない者の入室について、入室権限者により日常チェックを行っている。

(2) 登録端末室

登録端末室は、登録端末設備が設置される部屋で、利用者証明書の発行・失効に関わる重要な操作を行う部屋である。

登録端末室の出入り口は錠を取付け、無人の際には施錠する。業務責任者が鍵を管理し、権限のある者が2名以上でしか入室できない。また、1名で在室することが無いように運用にて管理している。止むを得ず権限が無いものが入室する場合は、事前に業務責任者が許可した者のみ、入室権限者と同伴で入室を認める。

(3) 発行室

発行室は、電子証明書を IC カードや CD-R 等の媒体に格納する発行業務に係わる機器が設置され発行業務を実施する部屋である。

火災、水害、震災への措置及び、空気調和機や無停電電源 (UPS と自家発電装置)、モーションセンサ、監視モニタを設置する。

入退室については生体認証装置で管理し、権限のある者の2名以上の認証で入室可能と

なっている。止むを得ず権限が無いものが入室する場合は、事前に業務責任者が許可した者のみ、複数人の入室権限者と同伴で入室を認める。

また、入室権限者複数名による入室および入室権限を持たない者の入室について、入室権限者により日常チェックを行っている。

5.1.3 電源設備と空調設備

認証局の電源設備は、運用に十分な電源容量を確保した無停電電源装置である。無停電電源装置とは、瞬断しないように電源そのものに UPS の機能が備わっており、かつ電源が供給されない事態に備えて発電機を用意し、一定時間内に発電機による電源供給に切り替える仕組みを持つ装置である。

また、空気調和機を用意し、機器類の動作環境及び要員の作業環境を適切に維持する。

5.1.4 水害対策

認証局の設備は、建物の二階以上に設置する。また、空気調和機には防水堤と漏水検知機を設置する。直上階の床面にも、防水対策を講じている。

5.1.5 地震対策

建物は耐震構造である。また、認証局の機器及び什器には、転倒・落下防止措置を講じている。

5.1.6 火災対策

建物は耐火構造である。認証局の機器は、建物の防火区画内に設置する。また、自動火災報知器や消火設備を備える。

5.1.7 媒体管理

アーカイブデータ、バックアップデータを記録した媒体は、施錠のできる書庫もしくは金庫に保管し、媒体の搬入管理を行う。また、媒体の保管場所には地震、火災、水害対策を講じている。

5.1.8 廃棄物処理

認証局で扱う重要な情報（個人情報、機密情報、秘密鍵、電子証明書）を記録した媒体の廃棄は、以下の方法により復元できないように廃棄する。

①重要な情報を記録した紙

シュレッダーにかけた後、廃棄する

②重要な情報を記録した磁気媒体もしくは光媒体

データ抹消用のアプリケーションを使用し、再び復元できないように情報を抹消するも

しくは、物理的に破壊した後に廃棄する

③重要な情報を記録した IC カード

物理的に破壊した後に廃棄する

④重要な情報を記録したコンピュータ機器

データ抹消用のアプリケーションを使用し、再び復元できないように情報を抹消するもしくは、物理的に破壊した後に廃棄する

5.1.9 オフサイトバックアップ

オフサイトバックアップの施設はない。

5.2 手続上の管理

5.2.1 信頼される役割

認証局は、以下の表 5.2 に示すとおり、認証業務の遂行に必要な認証局員の役割を定めている。各役割に対応する担当者ごとに物理的な部屋毎の入退室権限及び認証設備へのアクセス権限を付与し、アクセスコントロールを行う。また、認証局員の任命、入退室権限の設定、認証設備へのアクセス権限の設定は予め定められた手順に従い、実施する。

表 5.2 認証局員の各役割と本人識別方式

担当名	主な業務	本人識別方式
認証局代表者	<ul style="list-style-type: none"> ・ 認証局の運営・管理と業務の総括 ・ 認証局員の任命・解任及び配置 	—
業務責任者	<ul style="list-style-type: none"> ・ 審査、登録、発行業務の実施と監督 	<ul style="list-style-type: none"> ・ 入退室 ・ 生体認証 ・ IC カード ・ 物理鍵
審査担当者	<ul style="list-style-type: none"> ・ 申込書類一式の書類審査 ・ 利用者証明書発行及び失効情報入力データの確認 (PS2 サービス以外) 	<ul style="list-style-type: none"> ・ 入退室 ・ 物理鍵 ・ 認証設備へのログイン※ ・ IC カード (PS2 サービス以外) ・ ID/パスワード
登録担当者	<ul style="list-style-type: none"> ・ 利用者証明書発行及び失効情報のデータ入力 ・ 利用者証明書発行及び失効情報入力データの確認 (PS2 サービスのみ) 	<ul style="list-style-type: none"> ・ 入退室 ・ 物理鍵 ・ 認証設備へのログイン※ ・ IC カード ・ ID/パスワード
発行担当者	<ul style="list-style-type: none"> ・ IC カード作成に必要なデータ (鍵情報、顧客情報) の取得 ・ 利用者秘密鍵及び利用者証明書情報 	<ul style="list-style-type: none"> ・ 入退室 ・ 生体認証 ・ IC カード

	<ul style="list-style-type: none"> のICカードへの格納とICカード券面印刷 ・ICカードPINの印刷 	<ul style="list-style-type: none"> ・認証設備へのログイン※ ICカード ID/パスワード
設備責任者	<ul style="list-style-type: none"> ・認証設備を含む認証局内全ての設備に対する維持・管理の実施と監督 ・監査ログの収集、検査、保存 	<ul style="list-style-type: none"> ・入退室 生体認証 ICカード ・認証設備へのログイン※ ICカード ID/パスワード
設備担当者	<ul style="list-style-type: none"> ・認証設備の保守運用 ・システム障害対応、分析及び報告 	<ul style="list-style-type: none"> ・入退室 生体認証 ICカード ・認証設備へのログイン※ ICカード ID/パスワード
キーマネージャ	<ul style="list-style-type: none"> ・CA 秘密鍵の生成、更新、廃棄、活性化、非活性化、バックアップ、リストアの実施と監督 ・CA 秘密鍵管理の実施と監督 ・鍵の危殆化対応 	<ul style="list-style-type: none"> ・入退室 生体認証 ICカード ・認証設備へのログイン※ ICカード ID/パスワード

(※) 但し、ログイン方法は認証設備によって、ICカード及びID/パスワードの両方が必要な場合とID/パスワードのみでよい場合がある。

5.2.2 役割毎の必要人員

本CPS「5.2.1 信頼される役割」で述べた各役割に対し、事務取扱要領に規定した必要数の担当者を配属する。但し、セキュリティ上問題が無いと判断された場合には1名の担当者が複数の役割を兼務する場合がある。

5.2.3 役割毎の識別と認証

認証局員任命に際しては、任命される者の本人確認を対面による識別で実施した上で任命する。

5.3 人事管理

5.3.1 経歴、適正、経験、信頼性の要件

認証局の運用に関わる人材の募集要項及び選定基準は役割と責任に応じて、PKI、セキュリティ、電子署名法等、業務遂行に必要な知識、経験を有する者とする。

また、認証局員の任命の際は、本認証業務によって知り得た情報に対する機密保持誓約の承諾を得る。

5.3.2 経歴審査手順

規定しない。

5.3.3 トレーニングの要件

認証局の運用に関わる認証局員全員に対して、事務取扱要領に規定された教育計画に従って教育・訓練を行う。

5.3.4 再トレーニングの周期と要件

認証局は、認証局員に対し、継続的な教育・訓練を実施する。事務取扱要領では、認証局員に対する初期の教育・訓練だけではなく、定期的な教育・訓練の要件についても定める。また、非定期的に業務内容、手順等の変更及び指揮命令系統、責任及び権限の変更等に伴う教育・訓練を実施する。

5.3.5 配置転換の周期と順序

認証局は、必要に応じて、交代制など規則的な配置転換を実施する。

5.3.6 許可されていない行動に対する罰則

認証局員は、故意、過失に関わらず許可されていない行為を行った場合、NTT ネオメイトの就業規則に基づき処罰される。

5.3.7 個人との契約要件

認証局員は必ず、認証局代表者と個人の間で機密保持の誓約を必要とする。

5.3.8 要員に提供される文書

認証局員は、次の文書にアクセスすることができる。

但し、それぞれの文書はアクセスすることができる担当を定めており、アクセスコントロールされている。

- ① 認証局運用に関する以下の文書
 - ・ 運用に関する事務取扱要領等の規定文書
 - ・ 操作マニュアル
- ② ハードウェアやソフトウェア仕様書
- ③ セキュリティ文書

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

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.1.2 利用者への利用者秘密鍵送付

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.1.3 CA への公開鍵送付

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.1.4 利用者への CA 証明書送付

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.1.5 鍵のサイズ

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.1.6 公開鍵パラメータの生成

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.1.7 公開鍵パラメータの品質の検査

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.1.8 ハードウェア/ソフトウェアの鍵生成

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.1.9 鍵の利用目的

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.2 秘密鍵の保護

6.2.1 暗号装置に関する基準

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.2.2 秘密鍵の複数人制御

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.2.3 秘密鍵の預託

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.2.4 秘密鍵のバックアップ

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.2.5 秘密鍵のアーカイブ

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.2.6 暗号装置への秘密鍵の登録

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.2.7 秘密鍵の活性化方法

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.2.8 秘密鍵の非活性化方法

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.2.9 秘密鍵の破棄方法

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.3 鍵管理のその他の側面

6.3.1 公開鍵の履歴保管

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.3.2 秘密鍵の使用期間

認証局が提供するサービスの内、e-Probatio PS2 サービスについては、CA 秘密鍵の使用期間は 5 年間とする。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 年間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。

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

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

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.4.2 活性化データの保護

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

6.4.3 活性化データのその他の要件

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

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

認証設備は、以下の機能を備えている。

認証設備へのアクセスには、ID・パスワードによる操作者の認証又は IC カード、IC カード PIN を用いた電子署名による操作者の認証が行える機能を備え、操作者が特定できる。

また、予め設定されたアクセス権限確認機能を備えている

認証局の発行業務に用いる認証設備と登録業務に用いる認証設備間の通信は、認証設備の設定、アクセス管理、内部牽制等の措置により、各認証設備の認証並びに通信内容の盗聴及び改変を防止する措置を講じている

認証設備のシステムログは、以下の項目を含む事を規定している

- ① 各イベントを起こした者の識別
- ② 各イベント要求の発行先
- ③ 各イベントの種類
- ④ 各イベント発生日時
- ⑤ 各イベントの成否

6.5.2 コンピュータセキュリティ評価

規定しない。

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

認証局内で使用されるソフトウェアは、適切な品質管理のもと、開発している。

6.6.2 セキュリティマネジメント管理

認証設備及びネットワークの新規導入、アップグレードや設定変更を行う場合は、権限のある担当者が事務取扱要領に規定された手続きに従い、履歴を残す。

6.6.3 セキュリティ評価のライフサイクル

認証設備に導入したコンピュータセキュリティ技術について、セキュリティの脆弱性に関する情報等を収集し、適切なサイクルで最新のセキュリティテクノロジーを導入するため、随時セキュリティチェックを行う。セキュリティ上深刻な問題、脆弱性などがないかをテスト環境にて評価し、必要に応じて認証局代表者の承認後、是正措置を実施する。

6.7 ネットワークセキュリティ管理

認証設備及びリポジトリは、インターネットを含むその他のネットワークに対してファイアウォールを介して接続すると共に、不正侵入検知等十分なセキュリティ保護対策を行う。

情報公開 WEB サーバは、公開したフィンガープリントの改ざん防止措置を講じる。

6.8 暗号装置の技術管理

暗号装置の不正な解読等の事前検知と被害防止のために、関連情報の収集と調査分析を行う。暗号強度の評価については、設備責任者がその役割を担う。

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

認証局が提供するサービスの内、e-Probatio PS2 サービスについては、リンク証明書の New with Old の有効期間開始日を New with New の有効期間開始日、有効期間終了日を Old with Old の有効期間終了日とする。また、Old with New の有効期間開始日及び終了日を、ともに Old with Old の有効期間開始日及び終了日とする。
また、相互認証証明書の有効期間を 5 年以内とする。

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

7.2 CRL/ARL のプロファイル

本 CPS 「1.1.1 関連規程」に示す各 CP に規定する。

8 仕様の管理

認証業務運営検討会は、必要に応じて本CPS等を見直し、変更内容に関する審査を行う。

8.1 仕様の変更手順

認証業務運営検討会は、本CPS等の内容変更が利用者、署名検証者又は相互認証先に対し、電子証明書やCRL/ARLを使用する上で明らかに影響すると判断した場合、変更内容の審査過程において関係者から意見を聴取する場合がある。なお、以下の変更を実施する場合には、認定認証業務の変更認定が必要となる場合がある。

- ・ 認証設備、業務手順に関わる重要な変更
- ・ 認証局の責任、義務に関わる変更
- ・ 利用者責任、義務に関わる変更
- ・ 相互認証方針の変更

など

また、本CPS等を変更する場合はバージョン番号を更新する。

8.2 ポリシの公表と通知

認証業務運営検討会は、本CPS等又はその変更を承認した後、速やかに認証局が運営する情報公開WEBサイトに公開し、これをもって署名検証者、利用者及び相互認証先への通知とする。

8.3 CPSの承認手順

本CPS等及びその変更は、認証業務運営検討会が審査し、認証局代表者が承認する。

以上