

TDB 電子認証サービス TypeA 運用規程

Ver. 1.70

2010. 1. 5

株式会社 帝国データバンク

改訂履歴

Version	変更内容	変更日付	変更者	承認者
1.00	初版発行	2003/2/5	伊藤 正剛	臼井 治彦
1.01	ブリッジ認証局との相互接続実施に関する記載事項の修正。 在職証明書記載事項の修正。	2003/5/30	伊藤 正剛	臼井 治彦
1.02	本人限定受取郵便(特例型)対応実施に関する記載事項の修正。 利用申込書記載事項の修正。	2003/8/1	伊藤 正剛	臼井 治彦
1.03	連絡先窓口変更による修正。 初期不良申請時の提出書類の追加。 失効申請書に関する修正。 セキュリティ監査実施に関する修正。	2003/10/1	伊藤 正剛	臼井 治彦
1.04	利用申込書の変更による修正。	2003/10/27	伊藤 正剛	臼井 治彦
1.10	公開情報の URI の修正。 情報の開示について手順を追加。 uid の説明を追加。 IC カード初期不良申請書の送付を FAX 等に修正。 RA 発行業務室、IA 認証設備室の入退室の日常確認を追加。 相互認証証明書のプロフィールを修正。 各電子証明書プロフィールを追加。 用語の統一。	2004/1/27	伊藤 正剛	臼井 治彦
1.11	電子証明書を利用した利用申込、及びオンラインによる受領書送信に関する記述の追加。 用語の統一。	2004/12/13	伊藤 正剛	臼井 治彦
1.20	本人確認手順の明確化による修正。 用語の統一。 誤記の修正。	2005/1/26	伊藤 正剛	臼井 治彦
1.21	利用者の電子証明書プロフィールにおける、Subject 及び SubjectAltName の cn について追記。	2005/2/9	伊藤 正剛	臼井 治彦
1.22	所属組織等の確認書類の追加。 誤記の修正。	2005/6/3	伊藤 正剛	臼井 治彦
1.23	連絡先窓口変更による修正。	2005/10/3	小林 由里子	伊藤 正剛

1.24	失効情報の公開方法追加、及び利用者の電子証明書プロフィール変更に関する記述の変更。	2005/12/20	小林 由里子	伊藤 正剛
1.30	誤記の修正。 開示請求手順の一部を追加。	2006/1/17	内山 愛	伊藤 正剛
1.31	誤記の修正。	2006/3/6	内山 愛	伊藤 正剛
1.32	失効通知書の送付方法変更による修正。	2006/5/24	内山 愛	伊藤 正剛
1.33	受領書用紙の送付方法変更による修正。 初期不良時の提出書類の変更による修正。	2006/9/4	内山 愛	伊藤 正剛
1.40	用語の統一。 誤記の修正。 利用者鍵ペアの生成の作業場所名を修正。 発行者署名符号の破棄方法について追記。 アクティベーションデータの生成の作業場所名を修正。	2007/1/18	内山 愛	伊藤 正剛
1.41	用語の統一。 失効申請書(所属組織請求)の添付書類変更に伴う修正。	2007/4/2	内山 愛	伊藤 正剛
1.42	利用申込書記載事項の一部修正。	2007/8/6	内山 愛	伊藤 正剛
1.43	利用申込書記載事項の一部追加。 本認証局より発行する利用者の電子証明書の有効期間を追加。	2007/9/3	内山 愛	伊藤 正剛
1.44	リンク証明書、及びリンク証明書のフィンガープリントの公開について一部修正。	2007/10/31	内山 愛	伊藤 正剛
1.50	個人情報の取扱について一部修正。 個人事業者で商業登記をしていない場合の提出書類を一部修正。 表現の修正。	2008/1/8	内山 愛	浅海 輝一
1.60	失効通知書送付に関する記載の明確化による修正。 表現の修正。	2009/1/19	内山 愛	浅海 輝一
1.61	連絡先窓口変更による修正。	2009/4/1	内山 愛	浅野 敬
1.70	受領書データまたは受領書の督促開始日を修正。 表現の修正。 誤記の修正。	2010/1/5	内山 愛	浅野 敬

1.	はじめに.....	10
1.1.	概要.....	10
1.2.	識別名.....	10
1.3.	コミュニティと適用可能性.....	11
1.3.1.	本認証局運用規程の適用範囲.....	11
1.3.2.	関連する登場者.....	12
1.3.2.1.	認証局.....	12
1.3.2.2.	登録局.....	12
1.3.2.3.	発行局.....	12
1.3.2.4.	リポジトリ.....	12
1.3.2.5.	利用者.....	12
1.3.2.6.	所属組織.....	12
1.3.2.7.	署名検証者.....	13
1.3.2.8.	BCA.....	13
1.3.3.	電子証明書の適用範囲.....	13
1.3.4.	電子署名法に関する特別な要件.....	13
1.3.4.1.	属性等についての証明.....	13
1.3.4.2.	虚偽の申込みに対する罰則.....	14
1.3.4.3.	電子署名の法的効力.....	14
1.4.	連絡先の詳細.....	14
2.	一般条項.....	15
2.1.	義務.....	15
2.1.1.	認証局の義務.....	15
2.1.2.	登録局の義務.....	15
2.1.3.	発行局の義務.....	16
2.1.4.	リポジトリの義務.....	16
2.1.5.	利用者の義務.....	16
2.1.6.	所属組織の義務.....	17
2.1.7.	署名検証者の義務.....	17
2.2.	責任.....	18
2.2.1.	認証局の責任事項.....	18
2.2.2.	登録局の責任事項.....	18
2.2.3.	発行局の責任事項.....	18
2.2.4.	リポジトリの責任事項.....	19
2.2.5.	利用者の責任事項.....	19
2.2.6.	所属組織の責任事項.....	19
2.2.7.	署名検証者の責任事項.....	19

2.3.	財務上の責任	19
2.3.1.	賠償責任について.....	19
2.3.2.	利用者のコンピュータシステムの損害に関する免責について	19
2.3.3.	失効申請に関する免責について.....	19
2.3.4.	失効情報の発行周期に関する免責について.....	20
2.3.5.	本認証局廃止に関する免責について	20
2.3.6.	その他の免責事項.....	20
2.4.	解釈、及び執行.....	20
2.4.1.	準拠法.....	20
2.4.2.	分割、存続、合併、及び通知	20
2.4.3.	紛争の解決手順	21
2.5.	手数料.....	21
2.6.	公開、及びリポジトリ.....	21
2.6.1.	本認証局の情報の公開	21
2.6.2.	公開頻度	22
2.6.3.	アクセス管理	22
2.6.4.	リポジトリ.....	22
2.7.	準拠性監査.....	22
2.7.1.	本認証局に対する準拠性監査の頻度	22
2.7.2.	監査人の選任.....	22
2.7.3.	監査人と監査対象者の関係.....	23
2.7.4.	監査項目	23
2.7.5.	監査指摘事項への対応	23
2.7.6.	監査結果報告	23
2.8.	機密事項	23
2.8.1.	機密情報の種類	24
2.8.2.	個人情報の取扱	24
2.8.3.	電子証明書失効情報の公開.....	24
2.8.4.	法執行機関への情報開示.....	24
2.8.5.	民事開示手続きの上の情報開示.....	24
2.8.6.	情報の主体者の申請による情報開示	24
2.8.7.	その他の情報開示.....	25
2.9.	知的財産権.....	25
3.	本人確認、及び認証.....	26
3.1.	初期登録（利用申込）.....	26
3.1.1.	名前の意味に関する要件.....	26
3.1.2.	名前形式を解釈するための規則.....	26
3.1.3.	名前の一意性.....	28

3.1.4.	名前に関する紛争の解決手段	28
3.1.5.	商標の認識・認証・役割.....	28
3.1.6.	署名符号の所有の確認	28
3.1.7.	所属組織等の確認.....	28
3.1.8.	利用申込者の確認.....	28
3.2.	電子証明書の更新	30
3.3.	失効申請	30
3.3.1.	利用者の電子証明書の失効.....	30
3.3.2.	相互認証証明書の失効	31
4.	運用に関する要件	32
4.1.	電子証明書利用申込み.....	32
4.1.1.	申込み方式.....	32
4.1.2.	利用申込書類一式.....	33
4.1.3.	利用申込書記載事項	34
4.2.	電子証明書の発行	36
4.3.	電子証明書の受け取り.....	37
4.4.	IC カード初期不良時の対応	37
4.5.	ロック解除用 PIN.....	38
4.6.	電子証明書の失効と一時停止.....	38
4.6.1.	失効事由	38
4.6.1.1.	利用者の電子証明書の失効事由	38
4.6.1.2.	相互認証証明書の失効事由	39
4.6.2.	利用者または所属組織による失効	39
4.6.3.	相互認証先による失効	42
4.6.4.	本認証局による失効.....	42
4.6.5.	失効情報の発行頻度.....	42
4.7.	セキュリティ監査の手順.....	43
4.7.1.	記録するイベントの種類.....	43
4.7.2.	記録の監査の頻度.....	43
4.7.3.	監査用記録の保管期間	43
4.7.4.	監査用記録の保護.....	43
4.7.5.	監査用記録のバックアップ手順.....	43
4.7.6.	監査用記録システム	43
4.7.7.	問題の原因となるイベントの通知	44
4.7.8.	脆弱性の評価	44
4.8.	記録のアーカイブ	44
4.8.1.	アーカイブの対象.....	44
4.8.2.	アーカイブの保管期間	45

4.8.3.	アーカイブの保護.....	45
4.8.4.	アーカイブのバックアップ手順.....	45
4.8.5.	アーカイブの保管方法	45
4.9.	本認証局の鍵更新.....	45
4.10.	危殆化、及び災害への対応.....	45
4.10.1.	災害等における障害対策.....	46
4.10.2.	発行者署名符号の危殆化.....	46
4.11.	本認証サービスの廃止.....	46
5.	物理面、手続き面、及び人事面のセキュリティコントロール.....	48
5.1.	物理面のコントロール.....	48
5.1.1.	サイト、及び建物.....	48
5.1.2.	物理的アクセス	48
5.1.3.	災害対策.....	49
5.1.4.	メディアの保管	49
5.1.5.	廃棄物処理.....	49
5.1.6.	オフサイトバックアップ.....	50
5.2.	手続き面のコントロール.....	50
5.2.1.	信用に関わる役割.....	50
5.2.2.	タスクごとの人数.....	50
5.2.3.	権限の割当と認証.....	50
5.3.	人事面のコントロール.....	51
5.3.1.	経歴、資格、経験、及び必要条件	51
5.3.2.	人員配属に関する規定事項.....	51
5.3.3.	トレーニング要件.....	51
5.3.4.	権限のない行為に対する制裁	51
6.	技術的なセキュリティコントロール.....	52
6.1.	署名符号の生成、及びインストール.....	52
6.1.1.	署名符号の生成	52
6.1.2.	利用者への署名符号の配送.....	52
6.1.3.	本認証局への利用者署名検証符号の配送	52
6.1.4.	利用者への発行者署名検証符号の配送.....	52
6.1.5.	署名検証者への発行者署名検証符号の配送.....	52
6.1.6.	鍵のサイズとアルゴリズム.....	52
6.1.7.	ハードウェア/ソフトウェアでの鍵ペアの生成.....	53
6.1.8.	発行者署名符号の使用目的.....	53
6.2.	署名符号の保護.....	53
6.2.1.	暗号モジュールの基準	53

6.2.2.	署名符号の複数人管理	53
6.2.3.	署名符号のエスクロー	53
6.2.4.	署名符号のバックアップ.....	53
6.2.5.	署名符号のアーカイブ	53
6.2.6.	署名符号の暗号モジュールへの格納	54
6.2.7.	署名符号をアクティブ・非アクティブにする方法.....	54
6.2.8.	署名符号の破棄方法.....	54
6.3.	署名符号に対するその他の事項	54
6.3.1.	署名符号の使用期間.....	54
6.4.	アクティベーションデータ	54
6.4.1.	アクティベーションデータの生成、及びインストール	54
6.4.2.	アクティベーションデータ保護.....	55
6.4.3.	アクティベーションデータに関するその他の要件.....	55
6.5.	ネットワークセキュリティコントロール	55
6.6.	暗号モジュールの技術コントロール.....	55
7.	電子証明書、及び失効情報のプロファイル.....	56
7.1.	電子証明書のプロファイル	56
7.1.1.	バージョン番号	56
7.1.2.	拡張領域.....	56
7.1.2.1.	発行者鍵識別子 (AuthorityKeyIdentifier)	56
7.1.2.2.	主体者鍵識別子 (SubjectKeyIdentifier)	57
7.1.2.3.	鍵用途 (KeyUsage)	57
7.1.2.4.	証明書ポリシー (certificatePolicies)	57
7.1.2.5.	ポリシーマッピング (PolicyMappings)	58
7.1.2.6.	主体者別名 (SubjectAltName)	58
7.1.2.7.	発行者別名 (IssuerAltName)	58
7.1.2.8.	基本制約 (BasicConstraints)	58
7.1.2.9.	名前制約 (NameConstraints)	59
7.1.2.10.	ポリシー制約 (PolicyConstraints)	59
7.1.2.11.	失効情報配布点 (CRLDistributionPoints)	59
7.1.3.	暗号アルゴリズムの OID.....	59
7.1.4.	名前の形式.....	59
7.1.5.	各種の有効期間	60
7.2.	失効情報のプロファイル.....	60
7.2.1.	バージョン番号	60
7.2.2.	拡張領域.....	60
7.2.2.1.	失効理由 (reasonCode)	61
7.2.2.2.	発行者鍵識別子 (AuthorityKeyIdentifier)	61

7.2.2.3.	CRL 番号 (cRLNumber)	61
7.2.2.4.	配布点 (issuingDistributionPoint)	61
7.2.3.	発行頻度	62
8.	本認証局運用規程の仕様管理	63
8.1.	本認証局運用規程の変更	63
8.2.	本認証局運用規程の公表、及び通知	63
8.3.	本認証局運用規程の承認手続き	63
Appendix 1 .	自己署名証明書プロファイル	
Appendix 2 .	リンク証明書プロファイル	
Appendix 3 .	相互認証証明書プロファイル	
Appendix 4 .	利用者の電子証明書プロファイル	
Appendix 5 .	CRL プロファイル	
Appendix 6 .	ARL プロファイル	
Appendix 7 .	original_CRL プロファイル	

1. はじめに

1.1. 概要

株式会社帝国データバンク（以下、TDB という）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、電子署名法という）により規定された特定認証業務の認定の基準に適合した認証サービスを提供する。TDB は、本サービスを「TDB 電子認証サービス TypeA」（以下、本認証サービスという）と命名する。本認証サービスは、電子署名法に規定された認定を、2003 年 2 月 5 日に付与されている。また、本認証サービスにおいて TDB が運用する認証局（以下、本認証局という）は、行政機関と民間認証局等との間の信頼関係を仲介するために政府が運営するブリッジ認証局（以下、BCA という）との相互認証を実施する。

本認証サービスでは、法人もしくはこれに相当する組織に所属する個人に対して電子証明書を発行する。本認証サービスにより電子証明書の発行を受けた個人（以下、利用者という）は、当該電子証明書を、電子署名において利用することができる。本認証サービスでは、電子署名の狭義の用途を定めない。電子署名の用途の一例としては、政府、地方自治体を実施する電子入札、電子調達、電子申請等の行政手続き等が挙げられる。

本文書「TDB 電子認証サービス TypeA 運用規程」（以下、本認証局運用規程という）は、本認証局が行う電子証明書の発行、失効、及びその他の本認証局業務の運用管理に関する諸手続と、認証局を中心とする公開鍵基盤（PKI:Public Key Infrastructure、以下 PKI という）の要素である発行局、登録局、リポジトリ、利用者、及び署名検証者等の責任について規定した文書である。

本認証局運用規程は、IETF(Internet Engineering Task Force)が提唱する「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework（インターネットにおける X.509 公開鍵基盤証明書ポリシーと認証実践の枠組み）」(RFC2527)に準拠して構成されている。

1.2. 識別名

本認証サービスの名称は「TDB 電子認証サービス TypeA」とし、本認証サービスを実現する本認証局の名称を「TDB 電子認証局 TypeA」とする。また、本文書の名称は「TDB 電子認証サービス TypeA 運用規程」と定める。

本認証サービスと関連するオブジェクト識別子（OID）を下表にまとめる。

表 1-1 本認証サービスに関連するオブジェクト識別子 (OID)

項番	オブジェクト識別子 (OID)	オブジェクトの内容
1	1.2.392.200101	株式会社帝国データバンク
2	1.2.392.200101.1	ポリシー
3	1.2.392.200101.1.0	証明書ポリシー
4	1.2.392.200101.1.0.4	TDB 電子認証局 TypeA(本認証局)
5	1.2.392.200101.1.0.4.1	TDB 電子認証局 TypeA(本認証局)における利用者の電子証明書

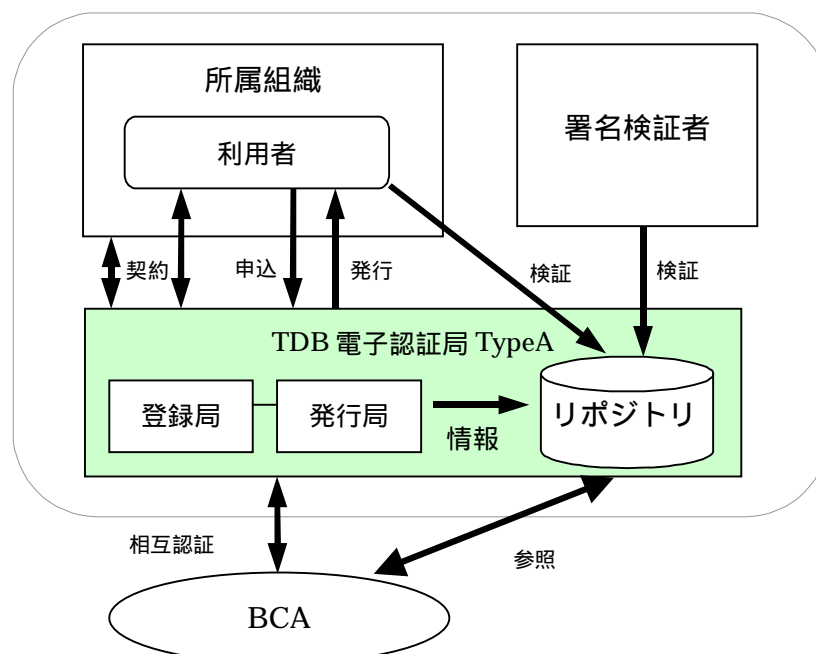
1.3. コミュニティと適用可能性

1.3.1. 本認証局運用規程の適用範囲

本認証局運用規程は、以下の図に示す本認証局により実施される電子証明書発行、失効業務に適用される。本認証局より発行される電子証明書には、全て本認証局運用規程が適用されるものとする。

また、本認証局が認める電子証明書の利用用途は、本認証局運用規程「1.3.3電子証明書の適用範囲」にて規定されるものとする。

図 1-1 本認証局運用規程の適用範囲



1.3.2. 関連する登場者

1.3.2.1. 認証局

本認証局は、登録局と発行局、及びリポジトリから構成され、TDB により運用される。本認証局では業務の一部を外部に委託することが出来る。

1.3.2.2. 登録局

本認証サービスにおいて、正当な利用申込みに対して、電子証明書利用申込者の審査、本人確認を確実にを行い、発行局に対して発行指示を行う。また、利用者署名符号の生成、及び IC カードへの格納を行い、安全な方法で利用者に送付する組織である。利用者の真偽確認と電子証明書の発行、及び失効の指示を行う RA 認証業務と、利用者の署名符号を作成し発行局に対して電子証明書の発行を要求する RA 発行業務、及び登録局で利用する申請管理システムの管理を行う RA システム管理業務の三つの業務内容から構成されている。

1.3.2.3. 発行局

本認証サービスにおいて、本認証局の発行者署名符号の管理を行い、各種電子証明書の発行、失効を行う。発行、及び失効を行う電子証明書には、本認証局自身の電子証明書（以下、自己署名証明書という）、リンク証明書、相互認証証明書、利用者の電子証明書が含まれる。

1.3.2.4. リポジトリ

利用者や署名検証者等に対して、本認証局運用規程、及び電子証明書の失効情報等を提供する LDAP サーバや WWW サーバの総称である。

1.3.2.5. 利用者

本認証サービスで電子証明書の発行対象となる利用者とは、法人、個人事業者、地方公共団体等の役員または従業員で、本認証局に対し本認証サービスの利用を申し込んだ者に限定する。利用者は、TDB との間で「TDB 電子認証サービス TypeA 利用規約」（以下、利用規約という）に基づく契約を締結し、本認証局運用規程、及び利用規約に定められた義務と責任を負う。

1.3.2.6. 所属組織

利用者が所属する、法人、個人事業者、地方公共団体等を総称して所属組織と呼ぶ。所属組織は、所属する利用者が電子証明書の利用を申込み時点で、TDB と所属組織との間

で、利用規約に基づく契約を結ぶものとする。また、所属組織は、所属する利用者が電子証明書を本認証局運用規程、及び利用規約に規定された利用用途に限り、電子証明書を利用するよう管理するとともに、必要に応じて失効の実施を行う義務と責任を負う。

1.3.2.7. 署名検証者

署名検証者とは、利用者の電子証明書を信頼して利用する者をいう。署名検証者は、本認証局運用規程が自己の利用用途に合致していることを確認し、本認証局運用規程の内容について理解し承諾した上で、電子証明書を利用するものとする。

1.3.2.8. BCA

行政機関の認証局と民間の認証局等との間の信頼関係を仲介するために政府が運営する認証局である。本認証局は BCA と相互認証接続を実施する。

1.3.3. 電子証明書の適用範囲

本認証サービスでは、所属組織に所属する個人に対して電子証明書を発行する。利用者は、当該電子証明書を電子署名において利用することができる。本認証サービスでは、電子署名の狭義の用途を定めない。電子署名の用途の一例としては、政府、地方自治体が発行する電子入札、電子調達、電子申請等の行政手続き等が挙げられる。

上記以外において利用された場合、本認証局は一切の責任を負わないものとする。なお、本認証サービスは、BCA との相互接続を実施する。

1.3.4. 電子署名法に関する特別な要件

本認証サービスは、電子署名法に規定された認定制度において、主務大臣より「特定認証業務」の認定を受けたサービスである。本認証サービス、及びその適用を受けるものは、いかなる場合でも本認証局運用規程「2.4.1準拠法」に掲げる当該法、及び関連政省令の定めに従わなければならない。また、以下の項目については特に留意すべきである。

1.3.4.1. 属性等についての証明

電子署名法に規定された認定制度では、認定の対象となる利用者の属性が、氏名、住所、及び生年月日の証明に限定されている。そのため、本認証局が発行する利用者の電子証明書に記載される利用者に関わる上記以外の属性（所属組織名、所属組織の所在地等）についての証明は、電子署名法における認定の対象外となる。

なお、利用者の電子証明書に記載される利用者の属性については、本認証局運用規程「3.1.1名前の意味に関する要件」を参照すること。

1.3.4.2. 虚偽の申込みに対する罰則

虚偽の利用申込みを行い、利用者について不実の証明をさせたものは、電子署名法第四十一条の規定により罰せられる。

1.3.4.3. 電子署名の法的効力

本認証局によって発行された電子証明書に関わる電子署名は、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。従って、利用者は自身の署名符号の取扱に充分留意し、秘匿性を維持しなければならない。

1.4. 連絡先の詳細

本認証サービスに関する問合せは、郵送、電話、FAX もしくは電子メールにて受け付ける。窓口は次の通りである。

窓口 : 株式会社帝国データバンク 営業推進部 営業開発課
営業日 : 月曜日～金曜日（祝祭日、年末年始 12月30日～1月4日を除く）
営業時間 : 9:00～12:00 13:00～17:00
住所 : 〒107-8680 東京都港区南青山 2-5-20
TEL : 03-5775-3134
FAX : 03-5775-3128
Eメール : certinfo@mail.tdb.co.jp

2. 一般条項

2.1. 義務

2.1.1. 認証局の義務

本認証局は、本認証局運用規程で規定する利用者、所属組織、及び署名検証者に対し、次の義務を負う。

- (1) 本認証局運用規程に基づき本認証局の運用を行う。
- (2) 本認証サービスの全ての責任を負う。
- (3) 発行者署名符号が危殆化（盗難、漏洩等により、その機密性を失うこと）することのないように保護する。
- (4) 利用者、所属組織、及び署名検証者に対し、本認証サービスによって発行された電子証明書には、特定認証業務の認定の範囲外である内容を含むことを公開する。
- (5) 本認証局運用規程に従い、本認証局の営業日の営業時間（本認証局運用規程「1.4 連絡先の詳細」参照のこと）に問合せを受け付ける。
- (6) リポジトリにて本認証局運用規程を公開する。
- (7) 24 時間毎に電子証明書の失効情報（original_CRL: original Certificate Revocation List、以下 original_CRL という、CRL: Certificate Revocation List、以下 CRL という、及び ARL: Authority Revocation List、以下 ARL という）を作成しリポジトリに公開する。
- (8) 定期的に、かつ 1 年以内の間隔で監査を実施し、監査報告に基づいて改善を行う。
- (9) 認証業務に関して、本認証局運用規程に基づいた事務取扱要領を規定する。
- (10) 相互認証の実施、及び終了についての判断を行う。なお、接続の実施にあたっては、相互接続先との調整のもと合意した手順に従って適切に各所（発行局、リポジトリ等）に指示を行う。

2.1.2. 登録局の義務

登録局は、本認証局運用規程で規定する利用者、所属組織、署名検証者、及び発行局に対し、次の義務を負う。

- (1) 本認証局運用規程に基づき登録局の運用を行う。
- (2) 本認証局運用規程、及び本認証局運用規程に基づいた事務取扱要領に従い、正当な利用申込みに対して、電子証明書利用申込者の審査、本人確認を確実にを行い、発行局に対して発行指示を行なう。
- (3) 本認証局運用規程、及び本認証局運用規程に基づいた事務取扱要領に従い、利用者署名符号の生成、及び IC カードへの格納を行い、安全な方法で利用者に送付する。
- (4) 本認証局が指定した機器を使用する。

- (5) 本認証局運用規程、及び本認証局運用規程に基づいた事務取扱要領に従い、利用者の電子証明書を失効する必要がある場合、速やかに電子証明書の失効申請を受け付け、審査を行った上、発行局に対して失効の指示を行う。
- (6) 個人情報、秘密情報、申込書類等を適切に取扱い、保管する。
- (7) 利用者の電子証明書を失効した場合は、その旨を利用者に通知する。
- (8) 電子証明書の名義人から申請情報等の開示請求があった場合は開示をする。

2.1.3. 発行局の義務

発行局は、本認証局運用規程で規定する利用者、所属組織、署名検証者、及び登録局に対し、次の義務を負う。

- (1) 本認証局運用規程に基づき発行局の運用を行う。
- (2) 本認証局の指示に従って、自己署名証明書、リンク証明書、相互認証証明書等の発行、及び失効を行う。
- (3) 発行者署名符号の管理、発行者署名符号のライフサイクル管理を行う。
- (4) 登録局から提供される情報を誤りなく電子証明書に反映させ、電子証明書を発行する。
- (5) 登録局からの失効申請に基づき、電子証明書の失効を行う。
- (6) 本認証局運用規程、及び本認証局運用規程に基づいた事務取扱要領に従い、original_CRL、及びCRL/ARLを作成する。

2.1.4. リポジトリの義務

リポジトリは、以下の義務を負う。

- (1) 本認証局運用規程の公開を行う。
- (2) 自己署名証明書（発行者署名符号更新時には新旧 2 種類）、リンク証明書（OldWithNew 及び NewWithOld）、相互認証証明書の公開を行う。
- (3) original_CRL、及びCRL/ARLの公開を行う。
- (4) 改ざん防止措置を行っている環境で自己署名証明書のフィンガープリント（自己署名証明書をSHA-1で変換したハッシュ値）、及びリンク証明書のフィンガープリント（リンク証明書をSHA-1で変換したハッシュ値）の公開を行う。
- (5) 本認証サービスに係わるその他の情報の公開を行う。

2.1.5. 利用者の義務

利用者は、次の義務を負う。

- (1) 電子証明書の利用申込にあたり、本認証局運用規程、及び利用規約の内容を理解し同意する。
- (2) 電子証明書の利用申込にあたり、本認証局に正確な情報を提供する。
- (3) 電子証明書に利用者の氏名、住所等の情報が記載されることを承認する。
- (4) 発行された電子証明書の記載内容を受領時に確認する。

- (5) 電子証明書受領時にその記載内容が利用申込み内容と相違がある場合、電子証明書の記載内容に変更が生じた場合、電子証明書の利用を中止する場合は、本認証局に対し直ちに電子証明書の失効申請を行う。
- (6) 本認証局運用規程、及び利用規約に規定された利用用途に限り、電子証明書を利用する。
- (7) 利用者署名符号の盗難や紛失、他者による不正利用等に十分な注意を払い、秘匿性を維持する。
- (8) 利用者署名符号を格納した IC カードをアクティベートするための IC カード用 PIN (以下、PIN という)、及び IC カードロック解除用 PIN (以下、ロック解除用 PIN という) の盗難や紛失、他者による不正利用等に十分な注意を払い、秘匿性を維持する。
- (9) 利用者署名符号が危殆化もしくは危殆化のおそれがある場合、本認証局に対し直ちに電子証明書の失効申請を行う。
- (10) 所属組織により当該電子証明書の失効申請が行われることがあることを承認する。
- (11) 電子証明書を使用して電子署名を行う場合のアルゴリズムは「SHA-1withRSA Encryption」とする。

2.1.6. 所属組織の義務

所属組織は、次の義務を負う。

- (1) 利用者が所属組織の代表者から権限を委託された者である場合、利用者が所属していることを証明する書類等 (以下、在職証明書等という) を提出するとともに、その記載内容を保証する。
- (2) 利用者の TDB 電子証明書 TypeA 利用申込書 (以下、利用申込書という) 及びその添付書類に記載された事項 (企業名、組織名等) が、電子証明書に転載されることを承認する。
- (3) 電子証明書の失効が必要となった場合、利用者に失効するように勧奨する。
- (4) 在職証明書等で届出た利用者が、電子証明書の利用を中止する場合、所属組織の所属者としての地位を失う等電子証明書の使用が適切でないと判断した場合、本認証局に当該利用者の電子証明書の失効申請を行う。
- (5) 利用者の電子証明書に記載されている事項が事実と異なることを発見した場合、又は係る事項に変更が生じた場合、電子証明書の失効申請を行わなければならない。
- (6) 利用者に、本認証局運用規程、及び利用規約に規定された利用用途の範囲以外で電子証明書を利用させてはならない。

2.1.7. 署名検証者の義務

署名検証者は、次の義務を負う。

- (1) 本認証局運用規程に規定された利用用途に限り、電子証明書を利用する。

- (2) 本認証局の発行者署名検証符号を取得し、信頼すべきかどうかを判断する電子証明書について、以下の内容を確認する。
- ・電子証明書が本認証局から発行されたものであること。
 - ・電子証明書が改竄されていないこと。
- 本認証局の発行者署名検証符号は、本認証局が発行する本認証局自身を示す自己署名証明書、リンク証明書 (OldWithNew 及び NewWithOld)、あるいは本認証局と相互認証を行った接続先が発行する本認証局に対する相互認証証明書に記載されている。また、本認証局の自己署名証明書、リンク証明書についてのフィンガープリントは、本認証局運用規程「2.6.1本認証局の情報の公開」に記述された場所に掲載されている。署名検証者は、必要に応じて、上記の各電子証明書、及びフィンガープリントを入手し、取得した発行者署名検証符号が本認証局のものであることを確認しなければならない。
- (3) 信頼すべきかどうかを判断する電子証明書について、その有効期間中であるかどうかを検証する。
- (4) 信頼すべきかどうかを判断する電子証明書について、リポジトリに公開されている original_CRL、または CRL/ARL により、その電子証明書が失効されていないかどうかを確認する。
- (5) 電子証明書の利用に際しては、本認証局運用規程「2.3 財務上の責任」に記述された免責事項について承諾する。

2.2. 責任

2.2.1. 認証局の責任事項

本認証局は、本認証局運用規程に従い本認証サービスを提供する。また、発行者の署名符号を適切に運用管理し、電子証明書の信頼性を確保する。

2.2.2. 登録局の責任事項

登録局は、本認証局運用規程に従い、電子証明書の利用申込者の本人確認、及び利用者署名符号の生成を適切に行い、発行局に対して電子証明書の発行、及び失効の適切な指示を行うことで、本認証局が発行する電子証明書に係る情報の信頼性を確保する。

2.2.3. 発行局の責任事項

発行局は、本認証局運用規程に従った運用を行い、登録局の指示に基づき、電子証明書の発行、失効を適切に行うことで、本認証局が発行する電子証明書に係る情報の信頼性を確保する。

2.2.4. リポジトリの責任事項

リポジトリは、original_CRL、及び CRL/ARL を公開することで、利用者、所属組織、及び署名検証者が電子証明書の失効状況を検証できるようにする。また、本認証局運用規程等の本認証サービスに係わる情報を公開することで、利用者、所属組織、及び署名検証者が本認証サービスに必要な諸手続き等を把握できるようにする。

2.2.5. 利用者の責任事項

利用者は、本認証局運用規程、及び利用規約に従い、本認証サービスを利用する。

2.2.6. 所属組織の責任事項

所属組織は、所属する利用者が電子証明書の利用を申込み時点で、TDB と所属組織との契約を結ぶ。所属組織は、所属する利用者が本認証局運用規程、及び利用規約に規定された利用用途に限り、電子証明書を利用するよう管理するとともに、必要に応じて失効の実施を行う義務と責任を負う。

2.2.7. 署名検証者の責任事項

署名検証者は、本認証局運用規程に従い、利用者の電子証明書を利用する。

2.3. 財務上の責任

2.3.1. 賠償責任について

本認証局は、本認証局に責を帰すべき事由のない行為によって発生した損害については、一切損害賠償責任を負わないものとする。

本認証局に責を帰すべき事由がある場合、本認証局は、別途利用規約に定める範囲で損害賠償を行うものとする。

2.3.2. 利用者のコンピュータシステムの損害に関する免責について

利用者の電子証明書取得または利用により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または障害が発生しても、本認証局は一切賠償責任を負わないものとする。

2.3.3. 失効申請に関する免責について

利用者や所属組織からの失効申請に伴う失効処理が、正当な事由により遅延した場合、これにより発生した損害については、本認証局は一切損害賠償責任を負わないものとする。

2.3.4. 失効情報の発行周期に関する免責について

original_CRL、及び CRL/ARL の発行周期が原因となって、利用者が何らかの損害を受けた場合には、本認証局は一切賠償責任を負わないものとする。

2.3.5. 本認証局廃止に関する免責について

本認証局の業務を停止することにより発生した損害については、本認証局は一切損害賠償責任を負わないものとする。

2.3.6. その他の免責事項

本認証局は、以下の事由による本認証サービスの停止によって利用者、署名検証者、所属組織が損害を受けた場合、一切賠償責任を負わないものとする。

- (1) 地震、水害、噴火、津波等の天災
- (2) 火災、停電等
- (3) 戦争、動乱、騒乱、暴動、労働争議等
- (4) その他、本認証局が技術的あるいは運用上緊急に本認証サービスを停止する必要があると判断した場合

2.4. 解釈、及び執行

2.4.1. 準拠法

本認証局運用規程は、日本国内の法律、及び規則、また以下の法令等に基づいて、解釈される。

- ・「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)

2.4.2. 分割、存続、合併、及び通知

本認証局運用規程の中で定められている事項もしくはその適用が、何らかの理由で、無効もしくは執行不可能であるとされた場合でも、残余の事項については、当事者の意思に最も合理的に合致するように解釈される。

また、無効もしくは執行不可能とされた事項について、他の当事者への適用もしくは異なる状況下での適用についても、当事者の意思に最も合理的に合致するように解釈される。

2.4.3. 紛争の解決手順

本認証サービスの利用に関し、本認証局に対して訴訟、仲裁を含む解決手段に訴えようとする場合、本認証局、利用者、所属組織、及び署名検証者の所在地にかかわらず、本認証局運用規程の解釈、有効性、及び本認証局が行う本認証サービスに関わる紛争については、東京地方裁判所を第一審の専属管轄裁判所とする。

2.5. 手数料

本認証サービスにかかわる料金は、下記 URL にて提示する。

<http://www.tdb.co.jp/typeA/>

2.6. 公開、及びリポジトリ

2.6.1. 本認証局の情報の公開

本認証局は、次の内容をリポジトリに掲載し、下記の URI にて公開する。

- ・ 本認証局運用規程：

<http://www.tdb.co.jp/typeA/>

- ・ 利用規約：

<http://www.tdb.co.jp/typeA/>

- ・ 発行者署名検証符号を含んだ発行者の電子証明書（自己署名証明書）：

<ldap://dir.tdb.ne.jp/ou=TDB%20CA%20TypeA,o=TEIKOKU%20DATABANK%5c%2cLTD.,c=JP?caCertificate>

<https://cert.tdb.ne.jp/TypeA/>

- ・ 発行者署名符号更新時におけるリンク証明書：

<ldap://dir.tdb.ne.jp/ou=TDB%20CA%20TypeA,o=TEIKOKU%20DATABANK%5c%2cLTD.,c=JP?caCertificate>

<https://cert.tdb.ne.jp/TypeA/>

- ・ 自己署名証明書、及びリンク証明書のフィンガープリント：

<https://cert.tdb.ne.jp/TypeA/fingerprint.html>

- ・ 相互認証証明書：

<ldap://dir.tdb.ne.jp/ou=TDB%20CA%20TypeA,o=TEIKOKU%20DATABANK%5c%2cLTD.,c=JP?crossCertificatePair>

- ・相互認証されている認証局の一覧：
<https://cert.tdb.ne.jp/TypeA/crosscert.html>
- ・本認証局が発行する利用者の電子証明書の失効情報(CRL)：
<ldap://dir.tdb.ne.jp/ou=TDB%20CA%20TypeA,o=TEIKOKU%20DATABANK%5c%2cLTD.,c=JP?certificateRevocationList>
- ・本認証局が発行する認証局関連の電子証明書の失効情報(ARL)：
<ldap://dir.tdb.ne.jp/ou=TDB%20CA%20TypeA,o=TEIKOKU%20DATABANK%5c%2cLTD.,c=JP?authorityRevocationList>
- ・CRL、及び ARL を含む失効情報(original_CRL)：
<https://cert.tdb.ne.jp/CRL/LatestCRL.crl>

なお、本認証局においては、利用者の電子証明書は公開しない。

2.6.2. 公開頻度

本認証局運用規程は、本認証局運用規程「8. 本認証局運用規程の仕様管理」に従い、公開する。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、及び更新の都度公開する。original_CRL、及び CRL/ARL は、24 時間毎に発行し公開する。その他の本認証サービスに係わる情報は、TDB の判断により適宜公開する。

2.6.3. アクセス管理

本認証サービスは、公開可能な電子証明書関連情報について、リポジトリを利用する全ての人に参照権限のみ割り当てて公開している。

2.6.4. リポジトリ

リポジトリは 1 日 24 時間、1 年 365 日利用可能とする。但し、定期保守作業等により、一時的にリポジトリを利用できない場合もある。

リポジトリに公開されている内容の変更は、電子認証局責任者の指示のもとで行われる。

2.7. 準拠性監査

2.7.1. 本認証局に対する準拠性監査の頻度

本認証局が本認証局運用規程に準拠して運営されていることを確認するために、少なくとも年に一度定期監査を実施する。また、電子認証局責任者が必要と認めた場合は、不定期に監査を実施する。

2.7.2. 監査人の選任

電子認証局責任者の指示に基づいて、選任される。

2.7.3. 監査人と監査対象者の関係

監査人は独立性を確保するために監査対象の部門外の者または外部監査人とする。

2.7.4. 監査項目

定期監査では、本認証局が運営する登録局、発行局、及びリポジトリが、本認証局運用規程、及び本認証局運用規程に基づいた事務取扱要領を遵守して運営されているかを監査する。主な監査項目は次の通りである。

- (1) 登録局、発行局、及びリポジトリの運用業務
- (2) 電子証明書ライフサイクルの管理
- (3) 発行者署名符号の管理
- (4) ソフトウェア
- (5) ハードウェア
- (6) ネットワーク監視システム
- (7) 物理的環境、及び設備
- (8) 相互認証に係わる事項
- (9) 外部委託先管理

不定期監査は、電子認証局責任者が必要と認めた場合に、電子認証局責任者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に関しては、電子認証局責任者がこれを是正するための対応を決定する。電子認証局責任者は、問題が解決されるまでの暫定的な対応策も含め、セキュリティ対策技術の最新の動向を踏まえ、設備及び規程等の見直しを含む対応措置を遅滞なく決定し、各担当者に実施の指示を行う。また、対応措置の実施結果について評価を行い、必要に応じて対応措置の見直しを行う。

2.7.6. 監査結果報告

監査報告書は、監査人から電子認証局責任者に提出される。電子認証局責任者は、監査結果を、関係する電子証明書の有効期間満了後 10 年間保管する。

2.8. 機密事項

本認証サービスの業務を通じて知り得る本認証局のシステム、ネットワーク、詳細な手順等の公開されていない情報の機密保持に関して、原則として、本認証局の定めた規定に則り、その内容が本認証局業務に関わる就業者の役割に応じて理解され、かつ維持されるようにする。

2.8.1. 機密情報の種類

本認証局が保有する情報のうち、リポジトリに公開されている情報を除き、全て機密保持対象として扱われる。本認証局は、法の定めによる場合を除いて、原則としてこれらの情報を公開しない。

2.8.2. 個人情報の取扱

電子証明書の利用申込み時、電子証明書の失効申請時、開示請求時、及びその他の事務連絡時に利用者または各申請者から提出される個人情報は、電子証明書に記載する等、本電子認証業務の用に供する以外は使用しない等の取扱いについて、「本認証局運用規程」「TDB 電子認証サービス TypeA 個人情報の取扱いについて」を規定し、かつその内容が維持されるようにする。また、その内容が、本認証局の業務に係わる全ての就業者の役割に応じて理解されるようにする。

2.8.3. 電子証明書失効情報の公開

電子証明書が失効された場合、original_CRL、及びCRL/ARLに失効された電子証明書のシリアル番号（userCertificate）、失効日時（revocationDate）、及び失効理由（reasonCode）が記載される。original_CRL、及びCRL/ARLに記載されたシリアル番号（userCertificate）、失効日時（revocationDate）、及び失効理由（reasonCode）の情報は機密とみなされない。また、失効に関するその他の詳細情報は原則として非公開とする。

2.8.4. 法執行機関への情報開示

本認証局で取扱う情報に対し、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、本認証局は法の定めに従い法執行機関へ情報を開示する。

2.8.5. 民事開示手続きの上の情報開示

本認証局は、調停、訴訟、その他の法的、裁判上または行政手続の過程において、機密保持対象である情報を開示することができるものとする。

2.8.6. 情報の主体者の申請による情報開示

利用者、及び利用者として登録された者から、権利または利益を侵害され、あるいはその恐れがあるとして個人情報の開示を求められた場合には、本人による開示要求であることを確認した後に、本認証局が保有している申込書類一式（添付書類を含む）及び電子証明書に記載されている個人情報の開示を当該申請者に行う。

開示請求者は、電子証明書利用申込書類開示請求書（以下、開示請求書）の送付を本認証局に依頼する。開示請求書を記入し実印を押印し、印鑑登録証明書を添付し本認証局宛に郵送もしくは、TDB 事業所へ持参し提出する。

本認証局は、印鑑登録証明書が少なくとも記載内容、形式、有効期限等において真正な

ものであることを確認する。また、開示請求書に押印された印鑑の印影と、利用申込書に押印された印鑑の印影が印鑑登録証明書に証明されている印影と一致することで真偽の確認を行う。実印の変更により利用申込書に押印された印鑑と印影が異なる場合は、開示請求書に押印された印鑑の印影と、印鑑登録証明書に証明されている印影と一致することと、その他の詳細な情報（生年月日等）を確認することで真偽の確認を行う。確認した後、以下の請求された書類を作成し、開示請求者へ書留郵便で送付、または手交する。

- ・当該電子証明書に係わる利用申込書
- ・利用者の真偽の確認のために提供を受けた書類
- ・利用者の電子証明書の記載データ

2.8.7. その他の情報開示

本認証局は、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

本認証局と利用者との間で別途合意がなされない限り、次の情報資料、及びデータは、本認証局に帰属する知的財産とする。

- (1) 本認証局より発行された全ての電子証明書
- (2) 本認証局により作成された original_CRL、及び CRL/ARL
- (3) 本認証局運用規程

3. 本人確認、及び認証

3.1. 初期登録（利用申込）

電子証明書の初期登録（利用申込）の手順については、本認証局運用規程にて規定される。登録局は、利用申込者の本人確認、及び利用者署名符号の生成を適切に行なわなければならない。

なお、利用申込者は複数枚の電子証明書の申込みを行うことが出来るが、その枚数が明らかに過大な枚数であると判断した場合には、登録局は電子証明書の枚数の制限または申込みの拒否を行うことが出来るものとする。

3.1.1. 名前の意味に関する要件

本認証局では、ITU-T X.509 勧告に準拠した電子証明書を発行する。本認証局が発行する各種電子証明書に記載される発行者名(issuer)、主体者名(subject)、発行者別名(IssuerAltName)、主体者別名(SubjectAltName)においては、ITU-T X.500 に規定された識別名(DN:Distinguished Name)を利用する。

3.1.2. 名前形式を解釈するための規則

本認証局では、利用者が申込み時に提出した利用申込書と添付書類、及び本認証局が独自に割り当てる情報を用いて、利用者の電子証明書に記載される主体者名(subject)及び主体者別名(SubjectAltName)を決定する。

利用者の電子証明書に記載される主体者名、及び主体者別名について以下に整理する。

表 3-1 利用者の電子証明書における主体者名(subject)

項番	属性の名称	値あるいは意味	電子署名法の対応(1)
1	国名 OID= 2.5.4.6 (countryName, c=)	日本を示す以下の値で固定。 “ c=JP ”	-
2	組織名 OID= 2.5.4.10 (organizationName, o=)	TDB を示す以下の値で固定。 “ o=TEIKOKU DATABANK,LTD. ”	-
3	組織内の部署名 OID= 2.5.4.11 (organizationalUnitName, ou=)	本認証局を示す以下の値で固定。 “ ou=TDB CA TypeA ”	-
4	都道府県名 OID= 2.5.4.8 (stateOrProvinceName, st=)	利用者の住所の都道府県名のローマ字表記。利用申込書に記入されている内容を転記する。 例: “ s=tokyo ”	
5	市町村名	利用者の住所の市町村名以下部分	

	OID= 2.5.4.7 (localityName, l=)	のローマ字表記。利用申込書に記入されている内容を転記する。 例: “ l=minato-ku, ... ”	
6	固有名称 OID= 2.5.4.3 (commonName, cn=)	利用者の氏名のローマ字表記。利用申込書に記入されている内容を転記する。(名、姓の順で記載される。) 例: “ cn=Ichiro Teikoku ”	
7	ユーザ識別子 OID= 0.9.2342.19200300.100.1.1 (userid, uid=)	利用者に配布される IC カードの識別番号である IC カード ID が uid の値として記載される。なお、IC カード ID は、本認証局にて割当てを行う。 例: “ uid=1234567890000000 ”	-

- 1 電子署名法に規定された認定制度における認定の対象かどうかを示す。 :対象 - :対象外
2 電子証明書において、項番 1 は PrintableString、これ以外については UTF8String で記載を行う。

表 3-2 利用者の電子証明書における主体者別名(SubjectAltName)

項番	属性の名称	値あるいは意味	電子署名法の対応(1)
1	国名 OID= 2.5.4.6 (countryName, c=)	日本を示す以下の値で固定。 例: “ c=JP ”	-
2	都道府県名 OID= 2.5.4.8 (stateOrProvinceName, s=)	利用者が所属する組織の住所の都道府県名。提出された公的書類(登記事項証明書(商業登記簿謄本)等)に記載された内容を転記する。 例: “ s=東京都 ”	-
3	市町村名 OID= 2.5.4.7 (localityName, l=)	利用者が所属する組織の住所の市町村名以下部分。提出された公的書類(登記事項証明書(商業登記簿謄本)等)に記載された内容を転記する。 例: “ l=港区南青山, ... ”	-
4	組織名 OID= 2.5.4.10 (organizationName, o=)	利用者が所属する組織の名称。提出された公的書類(登記事項証明書(商業登記簿謄本)等)に記載された内容を転記する。 例: “ o=株式会社帝国データバンク ”	-
5	固有名称 OID= 2.5.4.3 (commonName, cn=)	利用者の氏名。提出された住民票の写し(登録原票記載事項証明書)に記載された内容を転記する。(姓名の順で記載される。) 例: “ cn=帝国 一郎 ”	

- 1 電子署名法に規定された認定制度における認定の対象かどうかを示す。 :対象 - :対象外
2 電子証明書において、項番 1 は PrintableString、これ以外については UTF8String で記載を行う。
3 項番 2, 3, 4 については、公的書類が提出されない場合において記入を行わないことがある。

3.1.3. 名前の一意性

電子証明書に記載される識別名は、本認証局が発行した電子証明書において一意（ユニーク）とする。

3.1.4. 名前に関する紛争の解決手段

本認証サービスの利用者の電子証明書に記載された識別名に関する紛争については、本認証局において協議し、本認証局が全ての決定を行う。

3.1.5. 商標の認識・認証・役割

本認証サービスで発行される電子証明書に記載される利用者の識別名に商標を含む場合、本認証局は商標権の帰属や商標登録の有無を確認しない。

電子証明書に記載された識別名が、利用者または所属組織に帰属しない商標が含まれていることにより、損害を被る者が発生した場合は、本認証局は責任を負わず、当該所属組織または当該利用者が自己の負担と責任の下で解決するものとする。

3.1.6. 署名符号の所有の確認

本認証局では、利用者の署名符号を生成し、ICカードに格納後これを利用者本人に送付する。このため、利用者が当該署名符号を保持することを別途確認しない。

相互認証証明書の発行においては、相互認証先から提出された電子証明書発行要求（PKCS#10 フォーマット）の署名検証を行うことで、相互認証先が該当する署名符号を保持していることを確認する。

3.1.7. 所属組織等の確認

利用者が所属する所属組織の確認は、利用者が利用申込時に本認証局へ提出する登記事項証明書（商業登記簿謄本）によって行う。但し、当該組織が個人事業者で商業登記をしていない場合、税務署への開業届、所得税の青色申告申請書の表紙等、当該の個人事業者が事業を行っていることを確認できる資料の写しにて代替する。

また、登記を行わない公法人（地方公共団体等）の場合は、当該の法人が官公庁等に提出した書類、もしくは公文書等で当該の法人が事業を行っていることを確認できる資料にて代替する。

3.1.8. 利用申込者の確認

利用申込者が本人であることの真偽の確認は、登録局において、以下に定める方法により行うこととする。

（１）確認方法

【住民票の写しによる利用申込者の真偽確認】

住民票の写しによって利用申込者の真偽を確認するにあたっては、住民票の写しに代替するものとして、住民票記載事項証明書の提出も認める。また、利用申込者が

国内に居住する外国人である場合、外国人登録の登録原票記載事項証明書を用いる。本認証局運用規程の以下の項目において、特に断りのない場合はすべてこのルールを適用する。住民票の写しによる利用申込者の真偽の確認にあたっては、それらの書類が少なくとも記載内容、形式、有効期限等において真正なものであることを確認し、それらの書類と利用申込書の記載内容が一致することを確認する。住民票の写しと利用申込書の記載内容が異なる場合、「誤字俗字・正字一覧」「漢和辞典」等を用いて対応する文字を確認する。

【印鑑登録証明書による利用申込者の真偽の確認】

印鑑登録証明書によって利用申込者の真偽を確認するにあたっては、印鑑登録証明書が少なくとも記載内容、形式、有効期限等において真正なものであることを確認し、かつ、利用申込書に実印が押印され、利用申込書に押印された実印の印影と利用申込書に添付された印鑑登録証明書に証明されている印影が一致することを確認する。

【登記事項証明書（商業登記簿謄本）等による所属組織の真偽の確認】

登記事項証明書（商業登記簿謄本）によって所属組織が、登記事項証明書（商業登記簿謄本）に記載されている会社法人であることの真偽を確認するにあたっては、登記事項証明書（商業登記簿謄本）が少なくとも記載内容、形式、有効期限等において真正なものであることを確認し、かつ、登記事項証明書（商業登記簿謄本）と利用申込書の記載内容が一致することを確認する。

当該組織が個人事業者で商業登記をしていない場合、当該の個人事業者が事業を行っていることを確認できる、以下を満たすいずれかの資料の写しにて代替する。

- ・行政機関から発行された資料（発行印、発行日付があるもの）の写し
- ・行政機関に提出し受理された資料（受領印、受領日付があるもの）の写し

また、登記を行わない公法人（地方公共団体等）の場合は、当該の法人が官公庁等に提出した書類、もしくは公文書等で当該の法人が事業を行っていることを確認できる資料にて代替する。本認証局運用規程の以下の項目において、特に断りのない場合はすべてこのルールを適用する。

【在職証明書等による利用者の所属組織への所属に関する真偽の確認】

在職証明書等によって、利用者が所属組織に所属していることの真偽を確認するにあたっては、在職証明書等に押印された所属組織の代表者印とそれに係る印鑑証明書に証明されている印影が一致していることを確認する。

当該組織が個人事業者で代表者印が存在しない場合、代表者個人の印鑑登録証明書にて代替する。また、登記を行わない公法人（地方公共団体等）の場合、当該の法人が官公庁等に提出した書類、もしくは公文書等で当該の法人代表者印の印影が確認できる資料にて代替する。本認証局運用規程の以下の項目において、特に断りのない場合はすべてこのルールを適用する。

(2) 必要書類一覧

本認証局運用規程「4.1.2.利用申込書類一式」を参照のこと。

(3) 真偽確認の手順

2人の担当者がそれぞれ別々に真偽確認を行い、その結果を踏まえてRA認証業務責任者が、発行の承認を行う。

(4) 疑義が生じた場合

利用者の真偽の確認を行うにあたって疑義が生じた場合は、定められた業務手順に従って、利用申込書の再提出や返却、追加書類の提出要求等を行う。

3.2. 電子証明書の更新

本認証サービスでは、電子証明書の更新を規定しない。利用者は、電子証明書の失効もしくは有効期間の満了時に、新たに電子証明書の発行の申込を行う。

3.3. 失効申請

電子証明書の失効申請方法は、本認証局運用規程、及び本認証局運用規程に基づいた事務取扱要領にて規定される。また、本認証局では、本認証局運用規程において規定された失効事由に適合する事象が発生したと判断した場合、利用者の電子証明書、及び相互認証証明書等の失効を行う。なお、利用者の電子証明書の失効にあたっては所定の様式の電子証明書失効申請書（以下、失効申請書という）を用いなければならない。

3.3.1. 利用者の電子証明書の失効

利用者本人による失効申請の場合、電子証明書失効申請者が利用者本人であることの確認を適切に行う。また、所属組織による失効申請の場合には、失効申請を行った所属組織が、失効対象となる電子証明書の利用者が所属する組織であることの確認を適切に行う。

【利用者本人による失効申請の場合】

利用者は、電子証明書の利用申込時に本認証局に届け出た印鑑（以下、届出印という）届け出た実印（以下、届出実印という）もしくは届出実印が変更となった場合は実印を失効申請書に押印しなければならない。利用者が届出印、もしくは届出実印を利用しない場合、当該印鑑に係る印鑑登録証明書の提出も必要である。

本認証局では、届出印、届出実印が押印されている場合には、当該利用者の利用申込書に押印されたものと印影が同一であることを確認する。実印が押印されている場合には、

添付された印鑑登録証明書が少なくとも記載内容、形式、有効期限等において真正なものであることを確認し、失効申請書に押印された実印の印影と印鑑登録証明書に証明されている印影が一致することを確認する。

【所属組織による失効申請の場合】

所属組織は、電子証明書の利用申込時に本認証局に届け出た当該組織における代表者印（以下、届出代表者印という）もしくは届出代表者印が変更となった場合は所属組織の代表者印を失効申請書に押印しなければならない。所属組織が届出代表者印を利用しない場合、当該印鑑に係る印鑑証明書の提出も必要である。

本認証局では、届出代表者印が押印されている場合には、当該利用者の在職証明書に押印されたものと印影が同一であることを確認する。所属組織の代表者印が押印されている場合には、添付された印鑑証明書が少なくとも記載内容、形式、有効期限等において真正なものであることを確認し、失効申請書に押印された所属組織の代表者印の印影と印鑑証明書に証明されている印影が一致することを確認する。

当該組織が個人事業者で代表者印が存在しない場合、代表者個人の実印を押印し、当該印鑑に係る印鑑登録証明書を本認証局に提出しなければならない。また、登記を行わない公法人（地方公共団体等）の場合は、当該の法人代表者印を押印し、当該の法人が官公庁等に提出した書類、もしくは公文書等で当該の法人代表者印の印影が確認できる資料を本認証局に提出しなければならない。本認証局運用規程の以下の項目において、特に断りのない場合はすべてこのルールを適用する。

3.3.2. 相互認証証明書の失効

本認証局では、相互認証先より書面にて相互認証証明書の失効の申請が行われた場合、認証業務検討委員会の検討及び、承認のもと失効を実施する。

4. 運用に関する要件

4.1. 電子証明書利用申込み

電子証明書の発行を希望する者は、本認証局に対して電子証明書の利用申込みを行う。電子証明書の利用申込みについては、本認証局運用規程、及び利用規約が本認証局より提示されるので、電子証明書の発行を希望する者は電子証明書の利用申込時に、利用者に明示された個人情報の取扱方法及び電子証明書への記載事項を承認した上で、利用申込を行わなくてはならない。

利用申込み方法の詳細については以下の URL に掲示する。

<http://www.tdb.co.jp/typeA/>

また、相互認証の開始時においては、本認証局における最高意思決定機関である認証業務検討委員会にて検討、及び承認を行った上で、相互認証証明書の発行を行う。相互認証の開始手続きの詳細については、相互認証先と相談の上、安全な手順を決定し実施するものとする。

4.1.1. 申込み方式

電子証明書の発行を申し込む場合は、TDB のホームページにアクセスし、電子証明書発行申込画面に従って必要事項を入力する。(必要事項については、本認証局運用規程「4.1.3 利用申込書記載事項」を参照すること)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を印刷し、押印してから、所属組織の代表者印が押印された在職証明書、及び他の申込み書類を全て取りそろえて本認証局に申込みを行う。申込みについては、以下の2つの方式によるものとする。

(a) TDB 事業所への持参による申込み(窓口申込み)

TDB 事業所の窓口で利用申込書類を受け取り、未開封のまま本認証局に郵送する。利用申込受付日は、本認証局が利用申込書類を受領した時点とする。

(b) 本認証局への郵送による申込み(郵送申込み)

本認証局に郵送された利用申込書類を受領する。利用申込受付日は、本認証局が利用申込書類を受領した時点とする。

上記以外の方法による利用申込みについては受け付けない。

Web サーバに申込み情報を入力後、90 日以内に利用申込書類が本認証局で受領されない場合、申込みの意思がないものとみなし、原則として当該申込み情報を削除するものとする。

本認証サービスでは、利用者本人による申込みのみを許可し、代理人による申込みを認めない。

4.1.2. 利用申込書類一式

利用申込書類は、以下の通りとする。

表 4-1 利用申込書類一覧

項番	書類名	利用申込者の所属組織			備考
		一般法人	個人事業者	公法人 (地方公共団体等)	
1	TDB 電子証明書 TypeA 利用申込書				利用申込者の実印、届出印(1)が押印されたもの(届出印は必須ではない)
2	利用申込者の住民票の写し(登録原票記載事項証明書)(2)				発行日から3ヶ月以内のもの
3	利用申込者の印鑑登録証明書				発行日から3ヶ月以内のもの
4	所属組織代表者印の印鑑証明書		(3)	(4)	発行日から3ヶ月以内のもの
5	在職を証明する書類(在職証明書等)			(4)	利用申込者の所属組織の代表者印が押印されたもの(5)
6	利用申込者の所属組織の登記事項証明書(商業登記簿謄本)		(6)	(4)	発行日から3ヶ月以内のもの

印：必須 無印： 示された指示に従う。

- 1 利用申込時に押印することで、失効申請時等に利用することが可能となる。
- 2 住民票の写しに代替するものとして、住民票記載事項証明書の提出も認める。日本国籍を持たない外国人の場合は、住民票の写しの代わりに登録原票記載事項証明書を用いる。
- 3 商業登記を行っていない個人事業者については、代表者印が存在しないため、代表者個人の印鑑登録証明書をもって代替する。
- 4 登記を行わない公法人(地方公共団体等)に所属する利用申込者からの申込みに関わる属性証明部分で用いる真偽確認資料は、当該の法人が官公庁等に提出した書類、もしくは公文書等の資料にて代替する。
- 5 商業登記を行っていない個人事業者については、代表者印が存在しないため、代表者個人の実印を押印する。また、登記を行わない公法人(地方公共団体等)については、当該の法人が官公庁等に提出した書類、もしくは公文書等で印影確認が可能な法人代表者印を押印する。本認証局運用規程の以下の項目において、特に断りのない場合はすべてこのルールを適用する。
- 6 商業登記を行っていない個人事業者については、事業を行っていることを確認できる、所属組織名、本店所在地、代表者名の記載がある、以下を満たすいずれかの資料の写しにて代替する(2種類以上の書類の組合せも可とする)

・行政機関から発行された資料(発行印、発行日付があるもの)の写し

- ・行政機関に提出し受理された資料（受領印、受領日付があるもの）の写し
- 例：税務署への開業届、所得税の青色申告申請書の表紙等

4.1.3. 利用申込書記載事項

(1) TDB 電子証明書 TypeA 利用申込書

【利用者本人についての項目】

表 4-2 利用申込書の記載事項（利用者本人）

項番	項目	入力方法	入力者	省略可否	備考
1	IC カードの有効期間	画面入力	利用申込者	必須	
2	IC カードの申込枚数	画面入力	利用申込者	必須	
3	利用者名（漢字）	画面入力	利用申込者	必須	申込画面制御にて JIS 第一及び第二水準外の文字を禁止する
		電子証明書のデータを入力（1）	利用申込者確認		
4	利用者名（カナ）	画面入力	利用申込者	必須	
5	利用者名（ローマ字）	利用者名（カナ）より自動生成（2）	利用申込者確認（修正可能）	必須	
		電子証明書のデータを入力（1）	利用申込者確認		
6	住所（漢字）	画面入力	利用申込者	必須	
7	住所（カナ）	画面入力	利用申込者	必須	
8	住所（ローマ字）	住所（カナ）より自動生成（2）	利用申込者確認（修正可能）	必須	
		電子証明書のデータを入力（1）	利用申込者確認		
9	生年月日	画面入力	利用申込者	必須	
10	実印	押印	利用申込者	必須	
11	届出印	押印	利用申込者	省略可	
12	IC カード受取代理人の氏名	画面入力	利用申込者	省略可	
13	IC カード受取代理人の住所	画面入力	利用申込者	省略可	

- 1 既に IC カードを所有している利用者が申込みの場合、IC カードに格納されている電子証明書に記載されている利用者のデータを利用し申込みを行うことができる。
その場合、電子証明書の内容が電子証明書発行申込画面に自動表示され、利用申込者による修正は行えない。
 - 2 各項目のカナより自動生成されるが、利用申込者により修正することも可能である。
 - 3 2007 年 9 月 3 日以降に、2007 年 8 月 31 日までの旧利用申込書を使用し、「IC カード申込枚数」欄の右に「有効期間 年」の追記、及び追記場所に利用申込者の実印または届出印を押印された利用申込書が到着した場合、2007 年 8 月中に発送したと判断できる場合には、本認証局で受領する。
- なお、利用申込書には、利用申込みをする電子証明書の用途が記載されている。

【所属組織についての項目】

表 4-3 利用申込書の記載事項（所属組織）

項番	項目	入力方法	入力者	省略可否	備考
1	所属組織名（漢字）	画面入力	利用申込者	必須	
		電子証明書のデータを入力（ 1 ）	利用申込者確認		
2	所属組織名（カナ）	画面入力	利用申込者	必須	
3	代表者名（漢字）	画面入力	利用申込者	必須	
4	代表者名（カナ）	画面入力	利用申込者	必須	
5	事業所名・支店名	画面入力	利用申込者	必須	
6	担当部署名	画面入力	利用申込者	必須	
7	所在地	画面入力	利用申込者	必須	
8	申込担当者名（漢字）	画面入力	利用申込者	必須	
9	申込担当者名（カナ）	画面入力	利用申込者	必須	
10	連絡先電話番号	画面入力	利用申込者	必須	
11	連絡先 FAX 番号	画面入力	利用申込者	必須	

- 1 既に IC カードを所有している利用者が申込みの場合、IC カードに格納されている電子証明書に記載されている利用者のデータを利用し申込みを行うことができる。
その場合、電子証明書の内容が電子証明書発行申込画面に自動表示され、利用申込者による修正は行えない。

(2) 在職証明書

【所属組織についての項目】

表 4-4 在職証明書の記載事項

項番	項目	入力方法	入力者	省略可否	備考
1	所属組織名（漢字）	- (1)	画面制御で自動生成	必須	

		電子証明書のデータを入力 (2)	利用申込者確認		
2	本店所在地 (漢字)	- (1)	画面制御で自動生成	必須	利用申込書には記載されない。
		電子証明書のデータを入力 (2)	利用申込者確認		
3	代表者名 (漢字)	- (1)	画面制御で自動生成	必須	
4	所属組織の代表者印	押印	所属組織の代表者が押印	必須	
5	利用者の住所	- (1)	画面制御で自動生成	必須	
6	利用者名 (漢字)	- (1)	画面制御で自動生成	必須	

- 1 利用申込書のために入力されたデータがそのまま利用される。(在職証明書のみを作成した場合を除く)
- 2 既に IC カードを所有している利用者が申込み場合、IC カードに格納されている電子証明書に記載されている利用者のデータを利用し申込みを行うことができる。その場合、電子証明書の内容が電子証明書発行申込画面に自動表示され、利用申込者による修正は行えない。

4.2. 電子証明書の発行

本認証局は、認証を行った利用申込者に対して電子証明書の発行を行う。本認証局は利用者署名符号、及び発行された当該利用者の電子証明書を、IC カードに格納し、本人限定受取郵便 (特例型) にて利用者の住民票の写しに記載されている住所に送付する。利用者は、本人限定受取郵便 (特例型) の代人受取制度を利用して、IC カードの代人による受け取りを指定することが可能だが、その際は利用申込みにあたり本人限定受取郵便 (特例型) の代人受取申請をしておくことが必要である。また、本認証局は、IC カード用 PIN 通知書 (ロック解除用 PIN を含む、以下、PIN 通知書という) を書留郵便にて利用者の住民票の写しに記載されている住所に送付する。

本認証局より発送した IC カード、または PIN 通知書が、郵便局より本認証局に返送されてきた場合、本認証局は IC カード、または PIN 通知書の再送付をそれぞれの送付方法で 2 回を限度として行う。

また、本認証局より発送された IC カード、または PIN 通知書が郵便局より本認証局に 3 回返送されてきた場合、本認証局は当該利用者の電子証明書に対して失効を行う。

相互認証証明書の発行においては、相互認証先よりオフラインで提示される証明書発行

要求（PKCS#10 フォーマット）について、本認証局において署名検証等を実施後、これをもとに相互認証証明書を発行する。本認証局では、発行を行った相互認証証明書をオフラインにて相互認証先へ提出する。また、相互認証証明書は、リポジトリにて公開を行う。相互認証証明書の発行手順の詳細は、相互認証先との相談のもと決定することとする。

4.3. 電子証明書の受け取り

利用者は IC カード、及び PIN 通知書の受領後、電子証明書の内容確認を行い、問題がなければ当該の IC カードに格納されている電子証明書を利用し電子署名を付した受領書データ（以下、受領書データという）を送信するか、本認証局に TDB 電子証明書 TypeA 受領書用紙（以下、受領書用紙という）の送付を依頼し、本認証局より送付する受領書用紙に、申込書に押印した実印または届出印を押印した受領書（以下、受領書という）を本認証局に送付しなければならない。

なお、受領書用紙は IC カード 1 枚毎に 1 枚送付する。複数枚の IC カードを利用申込みした場合には、その発行枚数分の受領書データまたは受領書を提出する必要がある。

本認証局は、IC カードと PIN 通知書を送付し、利用者の住民票の写しに記載されている住所の最寄の各郵便局に到着後、本人限定受取郵便（特例型）の郵便局での保管期間である 10 日以上経過しても受領書データまたは受領書が到着しなかった場合、利用者もしくは所属組織に対して受領書データまたは受領書の送付を督促する。IC カード送付後 45 日を経過しても、受領書データまたは受領書が到着しなかった場合、本認証局は原則として当該利用者の電子証明書に対して、失効を行う。

相互認証証明書については、オフラインにて相互認証接続先と交換を行うとともに、リポジトリにて公開を行う。

4.4. IC カード初期不良時の対応

IC カードに初期不良が発見された場合、利用者は本認証局に対し IC カード初期不良の連絡をする。本認証局は利用者に対し、IC カード初期不良申請書（以下、初期不良申請書という）を FAX 等にて送付する。利用者は初期不良申請書を受領後、以下の書類を本認証局宛に郵送もしくは、TDB 事業所へ持参し提出する。

- ・ IC カード初期不良申請書
- ・ IC カードの券面コピー

本認証局は、初期不良申請に基づき審査を行い、当該初期不良申請の内容に問題が発見されなかった場合、当該電子証明書を失効するとともに、IC カードの再発行を行う。

4.5. ロック解除用 PIN

利用者が使用している IC カードは、PIN 入力を 5 回間違えるとロックが掛かり利用不能となる設定が施されている。IC カードがロックされた場合、当該利用者はロック解除用 PIN を利用して、IC カードのロックを解除することができる。

ロック解除用 PIN は、PIN 通知書に同封され利用者に届けられる。

4.6. 電子証明書の失効と一時停止

電子証明書の失効は、利用者、所属組織、相互認証先、本認証局のそれぞれの申請、及び事由により実施する。それぞれの失効事由を以下に規定するが、想定されていない事由が発生した場合は、電子認証局責任者の判断に基づき当該電子証明書を失効することができる。

なお、本認証局では、電子証明書の一時停止は行わない。

4.6.1. 失効事由

4.6.1.1. 利用者の電子証明書の失効事由

(1) 利用者による失効事由

利用者による失効の事由は下記のいずれかによるものとする。

- ・ 自らが所有する利用者署名符号が危殆化もしくは危殆化のおそれがある場合。
- ・ IC カードを紛失した場合。
- ・ IC カードの破損等によって IC カードが使用できなくなった場合。
- ・ 電子証明書の記載内容に変更がある場合。
- ・ 電子証明書の利用を中止する場合。
- ・ 利用者が死亡した場合。(失効代理人による失効申請が可能)

(2) 所属組織による失効事由

所属組織による失効の事由は下記のいずれかによるものとする。

- ・ 所属の利用者が所有する利用者署名符号が危殆化もしくは危殆化のおそれがある場合。
- ・ 所属の利用者が IC カードを紛失した場合。
- ・ IC カードの破損等によって所属の利用者の IC カードが使用できなくなった場合。
- ・ 所属の利用者に関する電子証明書の記載内容に変更がある場合。
- ・ 所属の利用者が電子証明書の利用を中止する場合。

- ・所属の利用者が死亡した場合。
- ・所属の利用者が退職した場合。
- ・その他、何らかの理由により所属の利用者の電子証明書の失効が必要になった場合。

(3) 本認証局による失効事由

本認証局による失効の事由は下記のいずれかによるものとする。

- ・利用者署名符号が危殆化もしくは危殆化のおそれがある場合。
- ・郵便局より本認証局に IC カード、または PIN 通知書が 3 回返送されてきた場合。
- ・期日を過ぎても、本認証局に受領書データまたは受領書が到着しない場合。
- ・発行者署名符号が危殆化もしくは危殆化のおそれがある場合。
- ・本認証局が認証業務を廃止する場合。
- ・電子証明書の記載事項に誤りがあった場合。
- ・その他、本認証局が必要と判断した場合。

4.6.1.2. 相互認証証明書の失効事由

(1) 相互認証先による失効事由

相互認証先による失効の事由は下記のいずれかによるものとする。

- ・相互認証を停止する場合。
- ・相互認証先の発行者署名符号が危殆化もしくは危殆化のおそれがある場合。
- ・認証ポリシーの変更がある場合。
- ・その他、相互認証先が必要と判断した場合。

(2) 本認証局による失効事由

本認証局による失効の事由は下記のいずれかによるものとする。

- ・相互認証を停止する場合。
- ・発行者署名符号が危殆化もしくは危殆化のおそれがある場合。
- ・本認証局が業務を廃止する場合。
- ・相互認証先の発行者署名符号が危殆化もしくは危殆化のおそれがある場合。
- ・相互認証基準違反があった場合。
- ・認証ポリシーの変更がある場合。
- ・その他、本認証局が必要と判断した場合。

4.6.2. 利用者または所属組織による失効

利用者または所属組織が何らかの失効事由により、利用者の電子証明書を失効しなければならないと判断した場合、失効申請書を本認証局に提出しなければならない。本認証局は失効申請者の真偽確認の結果、正当であると認められた場合は、失効処理を行う。なお、失効申請書は TDB のホームページ上に掲載公開されており、これを使用する。1 枚の失効申請書で複数枚の IC カード（最大 5 枚）の失効申請ができる。

(1) 失効受付

失効申請は郵送もしくは TDB 事業所の窓口での受付を可能とする。但し緊急の場合は FAX による失効申請を受付けるが、この場合別途定める手順に従い本人確認を行う。

(2) 確認方法

失効申請者の真偽を確認するにあたっては、申請に必要となる書類が全て揃っていること、公的書類については、少なくとも記載内容、形式、公的書類が提出された場合、有効期限等において真正なものであること、失効申請書の記載内容が利用申込書の記載内容と齟齬がないことを確認する。なお、利用者からの申請にあたっては届出印、届出実印、もしくは利用者の実印が利用されるものとする。所属組織からの申請にあたっては、届出代表者印、もしくは所属組織の代表者印が利用されるものとする。

(3) 利用者死亡による失効申請

利用者が死亡した場合は、利用者の失効代理人または所属組織からの失効申請を受け付ける。失効代理人が申請する場合は、失効申請書とともに利用者の死亡が確認できる公的書類（全部事項証明（戸籍謄本）もしくは個人事項証明（戸籍抄本）等）を提出する。

(4) 必要書類一覧

失効申請書類は、以下の通りとする。失効申請者は、以下の必要書類をすべて取りそろえて申請を行うものとする。

【利用者による申請の場合】

表 4-5 失効申請時の提出書類（利用者申請用）

項番	提出書類	備考
1	電子証明書失効申請書（利用者請求）	利用者氏名、IC カード ID、失効事由、押印等が必要
2	【届出印、届出実印が利用されない場合】 利用者の印鑑登録証明書	発行日から 3 ヶ月以内のもの
3	【利用者死亡による失効事由の場合のみ】 利用者の死亡が確認できる公的書類 （全部事項証明（戸籍謄本）もしくは個人事項証明（戸籍抄本）等）	発行日から 3 ヶ月以内のもの

表 4-6 失効申請書の記載事項（利用者申請用）

項番	項目	省略可否	備考
1	申請日	必須	未記入の場合、登録局にて受付日を記入する。 利用者への問い合わせは行わない。
2	利用者名	必須	
3	生年月日	必須	
4	利用者住所	必須	
5	所属組織名	必須	
6	電話番号	必須	

7	FAX 番号	省略可	
8	IC カード ID	必須	5 つまで指定可
9	失効事由	必須	以下より選択する。 紛失・盗難 破損 電子証明書の記載内容の変更 利用中止 その他（具体的に記入）
10	届出実印または届出印(届出実印が変更された場合は印鑑登録証明書添付)	必須	利用申込時の届出印または届出実印：電子証明書利用申込時に押印されたもの 届出実印が変更された場合は、実印

利用者死亡による事由の場合は省略できる。

【所属組織による申請の場合】

表 4-7 失効申請時の提出書類（所属組織申請用）

項番	提出書類	備考
1	電子証明書失効申請書（所属組織請求）	利用者氏名、IC カード ID、失効事由、押印等が必要
2	【届出代表者印が利用されない場合】 所属組織代表者印の印鑑証明書	発行日から 3 ヶ月以内のもの

商業登記を行っていない個人事業者については、代表者印が存在しないため、代表者個人の印鑑登録証明書をもって代替する。

表 4-8 失効申請書の記載事項（所属組織申請用）

項番	項目	省略可否	備考
1	申請日	必須	未記入の場合、登録局にて受付日を記入する。 所属組織の担当者への問い合わせは行わない。
2	利用者名	必須	
3	生年月日	必須	
4	利用者住所	必須	
5	IC カード ID	必須	5 つまで指定可
6	失効事由	必須	以下より選択する。 紛失・盗難 破損 電子証明書の記載内容の変更 利用中止 当該利用者の在職資格の喪失 その他（具体的に記入）
7	所属組織名	必須	
8	申請者連絡先所在地	必須	
9	失効申請者	必須	
10	失効申請者所属部署名	省略可	事業所・支店・担当部署名
11	電話番号	必須	
12	FAX 番号	省略可	
13	届出代表者印	必須	利用申込時の届出代表者印：在職証明書に押印

	(届出代表者印が変更された場合は印鑑証明書添付)		されたもの 届出代表者印が変更された場合は、所属組織の代表者印
--	--------------------------	--	------------------------------------

(5) 失効通知書の送付

当該電子証明書の失効操作が完了した後、電子証明書失効通知書（以下、失効通知書という）を作成し郵便で送付、または手交する。

通知の対象は、当該電子証明書の利用者本人、加えて所属組織によって失効申請が行われていた場合には所属組織の担当者とする。利用者死亡による失効の場合の通知の対象は、利用者に加えて失効申請者とする。

(6) 緊急時の対応

利用者または所属組織は、電子証明書の緊急な失効が必要と判断した場合、これを本認証局に要求することができる。本認証局は、可及的速やかに失効申請者の真偽確認を行い、失効が正当であると認められた場合は、失効処理を行う。

緊急失効時においては、本認証局側からのコールバックにより申請者の本人性を確認する。また、申請にあたっては、FAX により失効申請書を提出できるが、申請者は後日書類の原本を郵送にて本認証局に提出しなければならない。

4.6.3. 相互認証先による失効

本認証局では、相互認証先から、相互認証証明書の失効が申請された場合、失効を実施する。失効申請は、以下の情報が明記された書面にて行われなければならない。

- ・失効対象となる相互認証証明書を一意に識別するための情報
- ・失効事由
- ・失効日時

失効結果については、original_CRL、及び ARL に記載し公表することに加えて、要求元に対して通知を行う。

4.6.4. 本認証局による失効

本認証局が失効事由のいずれかにより電子証明書を失効しなければならないと判断した場合は、当該電子証明書の失効を行う。

当該電子証明書の失効手続き、及び失効操作が完了した後、失効通知書を作成し利用者へ郵便で送付、または手交する。

4.6.5. 失効情報の発行頻度

本認証局は、original_CRL、及び CRL/ARL の発行を 24 時間毎に行う。

但し、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、これに応じない。

4.7. セキュリティ監査の手順

本認証局は、その安全性、及び信頼性を維持するため、PKI の運用に係るイベントを記録し、これを適宜監査するものとする。

4.7.1. 記録するイベントの種類

監査用記録には少なくとも次に挙げるものが含まれる。

- (1) 利用申込み、及び失効申請についての承認・拒否のプロセスにおける記録
- (2) 本認証局の発行者署名符号の生成記録
- (3) 本認証局が発行する各種電子証明書生成・失効記録
- (4) 利用者の署名符号の生成記録
- (5) 利用者の電子証明書発行・失効記録
- (6) 認証設備室への入退室記録、及び入室権限についての承認記録
- (7) 認証設備システムへの不正なアクセスの記録
- (8) 認証設備システムの動作記録
- (9) 帳簿書類へのアクセス、及び帳簿書類の廃棄についての記録

4.7.2. 記録の監査の頻度

監査用記録の監査は、セキュリティを確保する上で、適切と思われる頻度で実施する。

4.7.3. 監査用記録の保管期間

監査用記録はアーカイブデータと同様の手続きで保管される。

本認証局運用規程「4.7.1記録するイベントの種類」(1) ~ (5) の記録については、それに関わる電子証明書の有効期間満了後 10 年間保管されるものとする。

本認証局運用規程「4.7.1記録するイベントの種類」(6) ~ (9) の記録については、作成された日から次回の特定認証業務の認定更新日まで保管されるものとする。

4.7.4. 監査用記録の保護

監査用記録は、別途事務取扱要領にて定められた手段を用い、流出、改竄、削除等から保護される。

4.7.5. 監査用記録のバックアップ手順

バックアップが必要な監査用記録が存在する場合、別途事務取扱要領に定められた手順を遵守してバックアップを行う。

4.7.6. 監査用記録システム

本認証局では、発行局または登録局のシステムによる自動処理、及びオペレータによる手動での作業を組み合わせ、監査用の記録を収集する。

4.7.7. 問題の原因となるイベントの通知

処理もしくは実行によりセキュリティに関する重大なイベント、または不具合が生じた場合、各担当者は各々の業務責任者に報告する。

4.7.8. 脆弱性の評価

本認証局においては、PKI 全体に影響を与える可能性がある脆弱性が検出された場合、適切な対応を施す。

4.8. 記録のアーカイブ

本認証局は、以下の書類、及び電子的記録を含む電子署名法で定めた帳簿類を保存する。

4.8.1. アーカイブの対象

本認証局は、以下の情報をアーカイブの対象として保管する。

- (1) 電子証明書の申込書、及びその添付書類
- (2) 電子証明書の発行作業指示、作業報告等、発行業務に関する記録
- (3) 登録局システムに登録された申請に関する全ての情報
- (4) 利用者の署名符号の生成、及び廃棄に関する記録
- (5) 利用者から提出される IC カードの受領書（オンライン）（受領書データを出力したもの）または受領書
- (6) 本認証局より発行された各種電子証明書（自己署名証明書、相互認証証明書、利用者の電子証明書等）
- (7) 発行者署名符号の管理に関する記録
- (8) 電子証明書の失効申請書、及びその添付書類
- (9) 電子証明書の失効作業指示等、失効業務に関する記録
- (10) 失効端末による失効操作に関する記録
- (11) 利用者の電子証明書におけるライフサイクル履歴
- (12) 開示業務に関する記録
- (13) 本認証局運用規程とその変更に関する記録
- (14) 業務手順を記述した文書（事務取扱要領等）とその変更に関する記録
- (15) 要員任命、組織管理に関する記録
- (16) 業務委託先の管理に関する記録
- (17) 監査に関する記録
- (18) 検討委員会議事に関する記録
- (19) 認証業務用機器の動作、保守、変更に関する記録

- (2 0) 認証業務用機器への不正アクセスの記録
- (2 1) 認証設備室への入退室に関する記録
- (2 2) 認証設備室への入室権限付与に関する記録
- (2 3) 事故に関する記録
- (2 4) 帳簿書類の管理に関する記録

4.8.2. アーカイブの保管期間

本認証局運用規程「4.8.1アーカイブの対象」の(1) ~ (1 8) の記録については、それに関わる電子証明書の有効期間の満了後 10 年間保管されるものとする。

本認証局運用規程「4.8.1アーカイブの対象」の(1 9) ~ (2 4) の記録については、作成された日から次の特定認証業務の認定更新日まで保管されるものとする。

4.8.3. アーカイブの保護

アーカイブに使用するメディアには、物理的なセキュリティ保護がなされており、漏えい、滅失またはき損防止のための措置が施されている環境で保護されている。また温度、湿度、磁気等環境における要素を考慮した上で保護されている。

4.8.4. アーカイブのバックアップ手順

バックアップが必要なアーカイブデータについては、別途事務取扱要領に定められた手順を遵守してバックアップを行う。

4.8.5. アーカイブの保管方法

本認証局は、アーカイブされた情報が保管期間を通じて読解可能な形式で保管されていることを保証する。

4.9. 本認証局の鍵更新

本認証局は、発行者署名符号の更新にあたり、新旧二つの発行者署名符号の関係をリンク証明書を用いて証明する。このため、発行者署名符号の更新時においては、自己署名証明書の更新に加えて、リンク証明書の発行も必要となる。

自己署名証明書、及びリンク証明書は、リポジトリに公開される。

4.10. 危殆化、及び災害への対応

危殆化、及び災害への対応として、本認証局は、次のことを行う。

- (1) 次の項目を含む詳細な文書を作成し保管する。

鍵が危殆化するような事態、ハードウェア、ソフトウェア、通信に関連する故障や不具合、火災や洪水等の自然災害等を考慮した上での緊急事態や災害に対する対応計画。

- (2) 緊急事態、及び災害に対する復旧計画手順について、関係するスタッフ全員に適切なトレーニングを実施する。

4.10.1. 災害等における障害対策

ハードウェア、ソフトウェアまたはデータの障害が発生した場合、定められた手順に従って速やかに障害個所の特定、及びそれに対する対策が施される。また、その障害の重要度により、利用者への通知、署名検証者への公開、及び相互認証先への連絡を行う。さらに、以下に挙げる状態を「重大な障害」と定義し、該当する場合には主務大臣へ通報する。

「original_CRL、及びCRL/ARLのいずれか、もしくは全ての更新が7日間以上にわたって停止し、かつ利用者への通知、及び署名検証者への公開が出来なかった場合」

4.10.2. 発行者署名符号の危殆化

本認証局は、本認証局自身の発行者署名符号が危殆化した場合は、直ちに危殆化した発行者署名符号を用いて電子署名された電子証明書（利用者の電子証明書、相互認証証明書等）を失効するとともに、original_CRL、及びCRL/ARLを発行し、バックアップを含む全ての発行者署名符号を削除する。

また、発行者署名符号が危殆化のおそれがある場合は、電子認証局責任者の判断により、危殆化のおそれがある発行者署名符号を用いて電子署名された電子証明書（同上）を失効するとともに、original_CRL、及びCRL/ARLを発行し、バックアップを含む全ての発行者署名符号を削除する。

本認証局自身の発行者署名符号が危殆化した場合、または危殆化のおそれがある場合、直ちに利用者への通知、署名検証者への公開、相互認証先への連絡、及び主務大臣への通報を行う。

なお、本認証局は、発行者署名符号が危殆化もしくは危殆化のおそれがある等の事態が起こった場合の対応策をまとめた計画を作成している。

4.11. 本認証サービスの廃止

特定認証業務の認定の更新を受けない場合等を含めて、本認証局が認証業務を廃止する場合には、全ての利用者の電子証明書、及び相互認証証明書を廃止日までに失効し、バックアップを含む全ての発行者署名符号を削除するとともに、廃止日の60日前までに電子証明書の利用者に連絡を行う。また、電子証明書の署名検証者、相互認証先に対しても、同様に認証業務を廃止する旨、及び発行済み電子証明書の失効処理方法等の情報提

供を行う。具体的には以下のいずれかの方法により連絡を行う。

- (1) 認証業務を廃止する通知書類を郵送する。
- (2) TDB のホームページへの掲載で告知する。

なお本認証局では、本認証サービスの廃止時において、それまでに発行した全ての電子証明書の有効期間を包含するのに十分な長さの有効期間を持った original_CRL 、及び CRL/ARL を作成し、リポジトリにて 6 ヶ月間公開する。この際、original_CRL 、及び CRL/ARL の日次での更新は行わない。

5. 物理面、手続き面、及び人事面のセキュリティコントロール

5.1. 物理面のコントロール

5.1.1. サイト、及び建物

登録局、及び発行局は、本認証局全体の信頼性を確保するために、十分考慮された建物内に構築され、不正アクセス等への対策が施されている。

また、登録局、及び発行局の所在を明示または暗示する名称を、看板もしくは表示板等によって建物内外に一切掲示しない。

5.1.2. 物理的アクセス

(1) 登録局

・ RA 認証業務室

RA 認証業務室は専用室で、出入口には生体認証電子ロックが取り付けられており、入室の際は、磁気カード、パスワード、及び生体認証が要求される。また、入退室の際は、RA 認証業務室入退室管理簿への記録が義務づけられている。

なお、入退室時以外は施錠されていることから、入室権限を持つ者以外が容易に RA 認証業務設備に触れることができないようになっている。

・ RA 発行業務室

RA 発行業務室は、入室に際して、あらかじめ許可された 2 人以上の人員による操作が必要であり、入室権限を有する者以外が RA 発行業務設備に容易に触れることができないようになっている。入室権限を有しない者の入室については、定められた手続きを行い 2 人以上の入室権限保有者が帯同する。

また、規定された入室方法、入室手続きで入退室が行われていることを日常確認している。

さらに、RA 発行業務室への入退室については以下の管理が実施されている。

2 人以上での指紋認証装置の操作による入室

試行時間、及び試行回数の制限

不正な操作による開扉があった場合の通報

退室の際、入室者数と同人数の退室を確認

遠隔監視カメラによる継続的な監視の実施、及びその記録

・ RA システム管理業務用設備室

登録局で利用する申請管理システムは、入退室カードによって入退室管理が施された設備室内において、専用のケージの中に設置されている。ケージの扉には錠が取り付けられており、通常時は施錠されている。ケージの扉を開閉するためには、2 種類の異なる鍵が必要であり、これらの鍵は別々の担当者によって管理されている。

(2) 発行局

- ・ 認証設備室

IA 業務用設備が設置される認証設備室へは、入室に際して、あらかじめ許可された 2 人以上の人員による操作が必要である。入室権限を有しない者の入室については、定められた手続きを行い 2 人以上の入室権限保有者が帯同する。

また、規定された入室方法、入室手続きで入退室が行われていることを日常確認している。

さらに、認証設備室への入退室については以下の管理が実施されている。

- 2 人以上での指紋認証装置の操作による入室

- 試行時間、及び試行回数の制限

- 不正な操作による開扉があった場合の通報

- 退室の際、入室者数と同人数の退室を確認

- 遠隔監視カメラによる継続的な監視の実施、及びその記録

5.1.3. 災害対策

登録局、及び発行局は、水害、火災、地震等の災害対策を下記の通り実施している。

- 防水対策

- 洪水等の影響を考慮し、適切な防水対策を施している。

- 火災対策

- 建築基準法に規定する耐火建築物内であり、かつ防火区画内に設置している。

- また、室内には自動火災報知器と、消火装置を設置している。

- 耐震

- 建築基準法に規定されている構造耐力等の基準に適合している。

- 停電対策

- UPS(無停電電源装置)、自家発電装置等による停電対策を施している。

5.1.4. メディアの保管

アーカイブデータ、バックアップデータを含む媒体は、保管場所として十分考慮された室内に設置された施錠可能な場所に保管されるとともに、所定の手続きに基づき適切に搬入出管理を行う。

5.1.5. 廃棄物処理

発行者署名符号、商業的に重要な情報または機密情報を含む紙面の文書、及び電子媒体は、次の方法で安全に破棄される。破棄に関する方法の詳細は、別途手順書に定める。

(1) バックアップを含む関連する全ての発行者署名符号

本認証局では、発行者署名符号の使用を終了する際に、暗号モジュールに格納された当該発行者署名符号をバックアップも含めて完全に消去する。破棄作業はあらかじめ定められた場所、及び複数人で実施する。

(2) 電子媒体の場合

物理的なダメージを与え完全に破壊するか、無効情報の上書き等により完全に消去

する。

(3) 印刷物の場合

確実に断裁破棄するか、溶解処分する外部のサービスによって破棄する。

(4) IC カードの場合

物理的なダメージを与え完全に破壊するか、IC カードライターを使用して IC カードの内容をゼロクリアする。

(5) コンピュータ端末の場合

本認証局で作成した利用者の署名符号、及びアクティベーションデータ (PIN、及びロック解除用 PIN) については、利用者へ送付する IC カードへの格納後、専用のソフトウェアを用いて確実にデータの消去を行う。他のデータについては、専用のソフトウェアの利用やハードディスクのフォーマット、ディスクの物理的な破壊等によって、データの消去を行う。

5.1.6. オフサイトバックアップ

発行者署名符号を含む暗号モジュールについては、オフサイトバックアップを行う場合がある。

5.2. 手続き面のコントロール

5.2.1. 信用に関わる役割

作業を行う者が単独でシステム全体を悪用することを防ぐため、本認証局運用業務の遂行は基本的に複数人管理のもとで行われる。

5.2.2. タスクごとの人数

各役割には、それぞれ別の担当者が配属される。但し、セキュリティ上問題がないと判断された場合には、1人の担当者が複数の役割を兼任することがある。

5.2.3. 権限の割当と認証

認証業務においては、個々の業務について、承認のプロセスが明確化され、どの担当者が何を行うべきかが明確に定められている。

設備のオペレーションについても、担当者とその役割が明確に定められており、システムはオペレーションしようとしているオペレータがあらかじめ設定された適切なオペレータか否かを認証するための仕組みを実装している。

5.3. 人事面のコントロール

本認証局は、以下に示す人事面のコントロールを施す。また、本認証局が業務の一部を外部に委託する場合においても、委託先にて適切な人事面でのコントロールが行われるように、委託先に指示し、管理を行う。

5.3.1. 経歴、資格、経験、及び必要条件

本認証業務の運営に携わる人員は、各ポジションで必要となる経歴、資格、経験、及び必要条件が別途定められ、これらを考慮したうえで配置される。

5.3.2. 人員配属に関する規定事項

本認証サービスに係る人員については、電子認証局責任者により任命される。また、配属される者は、本認証サービスによって知り得た情報に対する機密保持誓約書を電子認証局責任者に提出する。

5.3.3. トレーニング要件

認証業務の遂行に必要な電子署名技術・鍵管理技術・セキュリティ技術等の知識、経験それらを有している技術者を規定し、認証業務に配置する。

認証業務に携わる各担当者に必要な教育訓練計画を別途定め、計画に従って教育訓練を実施する。

指揮命令系統、責任及び権限、業務の手順に変更があった場合、変更後可能な限り速やかに必要な教育訓練を実施する。

5.3.4. 権限のない行為に対する制裁

本認証局業務に携わる各担当者による権限のない行為に対しては、故意、過失に関わらず定められた罰則が適用される。

6. 技術的なセキュリティコントロール

6.1. 署名符号の生成、及びインストール

6.1.1. 署名符号の生成

(1) 本認証局の発行者署名符号生成

発行者署名符号の生成は、複数人の立会いの下、一名の操作ではできない方法により、認証設備室内に設置された専用のハードウェアに接続された暗号モジュールの中で行われる。

(2) 利用者の鍵ペア（利用者署名検証符号 / 利用者署名符号）の生成

利用者の鍵ペアは、利用申込者からの利用申込みの審査・承認後、複数人による牽制の下で RA 発行業務室にて生成され、IC カードに格納される。

利用者署名符号は、IC カードに格納した後、生成から IC カードへの格納までに経過した装置等から完全に廃棄または消去される。

6.1.2. 利用者への署名符号の配送

利用者署名符号は IC カードに格納され、本人限定受取郵便（特例型）で利用者本人へ郵送される。利用者は、IC カードを受け取った後、本認証局に対して受領書データまたは受領書を送付しなければならない。

利用者は、本人限定受取郵便（特例型）の代人受取制度を利用して、代人を指定して IC カードを受け取ることが可能である。その場合、代人は開封せずに利用者本人に IC カードを渡さなければならない。

6.1.3. 本認証局への利用者署名検証符号の配送

利用者の鍵ペアは RA 発行業務において生成されるため、利用者署名検証符号を本認証局へ配送する必要はない。

6.1.4. 利用者への発行者署名検証符号の配送

発行者署名検証符号は、リポジトリで公開する方法により利用者に提供する。

6.1.5. 署名検証者への発行者署名検証符号の配送

発行者署名検証符号は、リポジトリに公開する方法により署名検証者に提供する。

6.1.6. 鍵のサイズとアルゴリズム

発行者署名符号には、以下の仕様に適合する鍵を利用する。

【署名方式】RSA 方式（SHA-1withRSAEncryption、OID は 1 2 840 113549 1 1 5）

【合成数】2048 ビット

利用者署名符号には、以下の仕様に適合する鍵を利用する。

【署名方式】RSA 方式 (SHA-1withRSAEncryption、OID は 1 2 840 113549 1 1 5)

【合成数】1024 ビット

6.1.7. ハードウェア/ソフトウェアでの鍵ペアの生成

本認証局の鍵ペアは、暗号モジュール内で生成される。

利用者の鍵ペアは、全てソフトウェアにて生成される。

6.1.8. 発行者署名符号の使用目的

発行者署名符号は、以下の目的に利用する。

- (1) 利用者の電子証明書への電子署名
- (2) 自己署名証明書への電子署名
- (3) 相互認証証明書、及び自己署名証明書発行要求(PKCS#10 フォーマット)への電子署名
- (4) リンク証明書への電子署名
- (5) original_CRL 、及び CRL/ARL への電子署名

6.2. 署名符号の保護

6.2.1. 暗号モジュールの基準

使用する暗号モジュールは、FIPS-140-1Level3 を満たす HSM である。

6.2.2. 署名符号の複数人管理

発行者署名符号の生成・保存・アクティベート、及び非アクティベート等の管理については、認証設備室内において複数人管理の下で行われる。

6.2.3. 署名符号のエスクロー

全ての署名符号について、エスクローの対象とはならない。

6.2.4. 署名符号のバックアップ

発行者署名符号のバックアップは、認証設備室内において複数人によってかつそのうちの 1 名だけでは操作できない方法によって行われる。

バックアップ用の暗号モジュールは、認証設備室と同等のセキュアな環境に保管される。

6.2.5. 署名符号のアーカイブ

本認証局内で生成される署名符号は、何れもアーカイブの対象とはならない。

6.2.6. 署名符号の暗号モジュールへの格納

発行者署名符号は、認証設備室内の暗号モジュール内で生成され、保管される。

6.2.7. 署名符号をアクティブ・非アクティブにする方法

発行者署名符号は、認証設備室、またはこれと同等のセキュリティが確保された室内に設置された暗号モジュール内に格納される。発行者署名符号の状態変更を行う場合には、認証設備室内において、権限を持つ複数名の要員が必ず関与し、相互牽制を行う中で作業を行う。

6.2.8. 署名符号の破棄方法

暗号モジュール内の発行者署名符号を破棄する場合には、別途手順書に定められた手順に従い、認証設備室において、権限を持つ複数名の要員が必ず関与し、相互牽制を行う中で作業を行う。破棄作業の全工程完了後には、発行者署名符号を復旧することはできない方法で行う。

破棄作業は、バックアップ分も含めた全ての暗号モジュールに対して、一連の作業指示において遅滞なく実施する。

6.3. 署名符号に対するその他の事項

6.3.1. 署名符号の使用期間

利用者署名符号は、それに対応する電子証明書の有効期間中のみ使用することが可能である。

自己署名証明書の有効期間は10年とする。但し、発行者署名符号は最初の5年間のみ電子証明書等への電子署名に利用する。

6.4. アクティベーションデータ

6.4.1. アクティベーションデータの生成、及びインストール

発行者署名符号、及び利用者署名符号についてのもを含む、全てのアクティベーションデータは、定められた規則に従って生成、及び管理される。

利用者署名符号のアクティベーションデータ（PIN、及びロック解除用PIN）は、生成からICカードへの格納まで、盗聴、改変等されないよう厳重に管理されたRA発行業務室で安全に行われている。アクティベーションデータは書留郵便にて利用者へ送付され、その後、別途定められた手順に従って本認証局の設備内から完全に削除される。

6.4.2. アクティベーションデータ保護

本認証局内で使用されるアクティベーションデータについては、定められた規則に則って保護される。

利用者署名符号に対するアクティベーションデータ（PIN、及びロック解除用 PIN）は、利用者の責任をもって保護しなければならない。

6.4.3. アクティベーションデータに関するその他の要件

本認証局内でのアクティベーションデータの取扱については、事務取扱要領に記載される。

6.5. ネットワークセキュリティコントロール

本認証局では、ネットワークセキュリティに関して以下の基準を設けている。

- ・外部ネットワークと接続を行う場合、外部ネットワークからの認証設備室と RA 発行業務室に対する不正なアクセスを防止・検知するため、ファイアーウォール、及び不正侵入検知システムを導入する。
- ・認証業務用設備間の通信においては、設備等の認証、盗聴防止、改ざん防止措置を実施する。

登録局、発行局、リポジトリ間の個々の設備、及び通信について、上記基準をもとにその重要性に応じて具体的な措置を決定し実施している。

6.6. 暗号モジュールの技術コントロール

発行者署名符号を管理する暗号モジュールとして、FIPS-140-1Level3 を満たす HSM を使用する。また、その安全性に対する脅威についての情報を常に収集し、問題があればそれに対する対策を行う。

7. 電子証明書、及び失効情報のプロファイル

本認証局が発行する各種電子証明書、及び失効情報(original_CRL、及び CRL/ARL)の形式、属性の仕様は以下の標準に準拠し定義している。

- 1) ITU-T Recommendation X.509 (1997)
- 2) IETF RFC3280 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002

詳細なプロファイルについては、Appendix に記載されている。

7.1. 電子証明書のプロファイル

7.1.1. バージョン番号

本認証局は、X.509 バージョン 3 に準拠した電子証明書を発行する。

7.1.2. 拡張領域

本認証局は、X.509 で定義された拡張領域を利用する。利用する拡張領域を以下に整理する。

表 7-1 電子証明書の拡張領域

項番	拡張領域の名称	Critical	自己署名証明書	リンク証明書	相互認証証明書	利用者証明書
1	AuthorityKeyIdentifier	False				
2	SubjectKeyIdentifier	False				
3	KeyUsage	True				
4	certificatePolicies	True	-			
5	PolicyMappings	False	-	-	-	-
6	SubjectAltName	False		-	-	
7	IssuerAltName	False		-	-	
8	BasicConstraints	True				-
9	NameConstraints	True	-	-	-	-
10	PolicyConstraints	True	-	-		-
11	CRLDistributionPoints	False				

: 当該電子証明書に含める項目、 - : 当該電子証明書に含めない項目

リンク証明書ではcertificatePoliciesのCriticalフラグをFalseに設定する。

また、本認証局で発行する電子証明書において、標準領域の issuerUniqueID と subjectUniqueID は常に利用しない。

7.1.2.1. 発行者鍵識別子 (AuthorityKeyIdentifier)

本認証局では、各種電子証明書において、AuthorityKeyIdentifierとしてkeyIdentifier

のみを設定する。設定値の詳細を以下に示す。

表 7-2 電子証明書の AuthorityKeyIdentifier (keyIdentifier) の設定

項番	電子証明書の種類	設定値
1	自己署名証明書	発行者署名検証符号の SHA-1 のハッシュ値
2	リンク証明書	OldWithNew: 新発行者署名検証符号の SHA-1 のハッシュ値 NewWithOld: 旧発行者署名検証符号の SHA-1 のハッシュ値
3	相互認証証明書	発行者署名検証符号の SHA-1 のハッシュ値
4	利用者の電子証明書	発行者署名検証符号の SHA-1 のハッシュ値

7.1.2.2. 主体者鍵識別子 (SubjectKeyIdentifier)

本認証局では、各種電子証明書において、SubjectKeyIdentifier を以下のように設定する。

表 7-3 電子証明書の SubjectKeyIdentifier の設定

項番	電子証明書の種類	設定値
1	自己署名証明書	発行者署名検証符号の SHA-1 のハッシュ値
2	リンク証明書	OldWithNew: 旧発行者署名検証符号の SHA-1 のハッシュ値 NewWithOld: 新発行者署名検証符号の SHA-1 のハッシュ値
3	相互認証証明書	相互認証先の署名検証符号の SHA-1 のハッシュ値
4	利用者の電子証明書	利用者署名検証符号の SHA-1 のハッシュ値

7.1.2.3. 鍵用途 (KeyUsage)

本認証局では、各種電子証明書において、KeyUsage を以下のように設定する。

表 7-4 電子証明書の KeyUsage の設定

項番	電子証明書の種類	設定値
1	自己署名証明書	KeyCertSign と cRLSign を指定
2	リンク証明書	KeyCertSign と cRLSign を指定
3	相互認証証明書	KeyCertSign と cRLSign を指定
4	利用者の電子証明書	DigitalSignature と nonRepudiation を指定

7.1.2.4. 証明書ポリシー (certificatePolicies)

本認証局では、各種電子証明書において、certificatePolicies を以下のように設定する。

表 7-5 電子証明書の certificatePolicies の設定

項番	電子証明書の種類	設定値
1	自己署名証明書	設定しない。
2	リンク証明書	OID=2.5.29.32.0 (ANY-POLICY) を指定
3	相互認証証明書	OID=1.2.392.200101.1.0.4.1 を指定。また CPSuri として CPS の公開場所を記載する。2.6.1 項参照。

4	利用者の電子証明書	OID=1.2.392.200101.1.0.4.1 を指定。また CPSuri として CPS の公開場所を記載する。2.6.1 項参照。
---	-----------	--

7.1.2.5. ポリシーマッピング (PolicyMappings)

本認証局では、相互認証証明書に PolicyMappings を含める。

7.1.2.6. 主体者別名 (SubjectAltName)

本認証局では、各種電子証明書において、SubjectAltName を以下のように設定する。

表 7-6 電子証明書の SubjectAltName の設定

項番	電子証明書の種類	設定値
1	自己署名証明書	c=JP o=株式会社帝国データバンク ou=TDB 電子認証局 TypeA
2	リンク証明書	設定しない。
3	相互認証証明書	設定しない。
4	利用者の電子証明書	3.1.2 項に記述した通り設定を行う。

“c=JP” のみ PrintableString で記載する。他の項目は UTF8String で記載する。

7.1.2.7. 発行者別名 (IssuerAltName)

本認証局では、各種電子証明書において、IssuerAltName を以下のように設定する。

表 7-7 電子証明書の IssuerAltName の設定

項番	電子証明書の種類	設定値
1	自己署名証明書	c=JP o=株式会社帝国データバンク ou=TDB 電子認証局 TypeA
2	リンク証明書	設定しない。
3	相互認証証明書	設定しない。
4	利用者の電子証明書	c=JP o=株式会社帝国データバンク ou=TDB 電子認証局 TypeA

“c=JP” のみ PrintableString で記載する。他の項目は UTF8String で記載する。

7.1.2.8. 基本制約 (BasicConstraints)

本認証局では、各種電子証明書において、BasicConstraints を以下のように設定する。

表 7-8 各電子証明書の BasicConstraints の設定

項番	電子証明書の種類	設定値
1	自己署名証明書	cA=True と設定する。 PathLenConstraint は指定しない。
2	リンク証明書	cA=True と設定する。 PathLenConstraint は指定しない。
3	相互認証証明書	cA=True と設定する。 pathLenConstraint は指定しない。
4	利用者の電子証明書	設定しない。

7.1.2.9. 名前制約 (NameConstraints)

本認証局では、NameConstraints を含めない。

7.1.2.10. ポリシー制約 (PolicyConstraints)

本認証局では、相互認証証明書には PolicyConstraints を含める。

7.1.2.11. 失効情報配布点 (CRLDistributionPoints)

本認証局では、各種電子証明書において、CRLDistributionPoints を以下のように設定する。

表 7-9 電子証明書の CRLDistributionPoints の設定

項番	電子証明書の種類	設定値
1	自己署名証明書	ARL を公開する場所を URI にて設定する。2.6.1 項参照。
2	リンク証明書	ARL を公開する場所を URI にて設定する。2.6.1 項参照。
3	相互認証証明書	ARL を公開する場所を URI にて設定する。2.6.1 項参照。
4	利用者の電子証明書	original_CRL、及び CRL を公開する場所を URI にて設定する。2.6.1 項参照。

7.1.3. 暗号アルゴリズムの OID

本認証局が発行する各種電子証明書、及び失効情報 (original_CRL、及び CRL/ARL) における署名アルゴリズムは SHA-1withRSAEncryption 方式(OID=1.2.840.113549.1.1.5) である。各電子証明書に記載される主体者の署名検証符号は、RSA 方式 (OID=1.2.840.113549.1.1.1)の鍵を利用する。

また、本認証局より発行される電子証明書を利用する利用者が、電子署名に利用できるアルゴリズムは、SHA-1withRSAEncryption 方式(OID=1.2.840.113549.1.1.5)とする。

7.1.4. 名前の形式

本認証局が発行する各種電子証明書、及び失効情報(original_CRL、及び CRL/ARL)に含まれる各種の識別名は、ITU-T X.500 勧告における識別名 (DN : Distinguished Name) の規定に従い決定する。自己署名証明書、及び利用者の電子証明書における発行者別名 (IssuerAltName)、及び主体者別名 (SubjectAltName) においては、日本語、及び英語 (アルファベット) を利用する。上記以外の各識別名においては英語 (アルファベット) のみを利用する。

利用者の電子証明書における主体者名 (Subject) と主体者別名 (SubjectAltName) については、3.1.2 項を参照すること。

本認証局を示す識別名(DN)は下表の値とする。但し、発行者別名(IssuerAltName)を電子証明書上あるいは失効情報上に記載するかどうかについては、各々のプロファイルの規則に従う。

表 7-10 発行者名(issuer)と発行者別名(IssuerAltName)

項番	種別	設定値
1	発行者名 (issuer)	c=JP o=TEIKOKU DATABANK,LTD. ou=TDB CA TypeA
2	発行者別名 (IssuerAltName)	c=JP o=株式会社帝国データバンク ou=TDB 電子認証局 TypeA

“c=JP”のみPrintableStringで記載する。他の項目はUTF8Stringで記載する。

7.1.5. 各種の有効期間

本認証局が発行する各種電子証明書に記載される有効期間(validity)及び関連する署名符号の利用期間について以下に整理する。

表 7-11 各種電子証明書の有効期間等

電子証明書の種類	有効期間	署名符号更新の頻度	電子証明書の発行頻度
自己署名証明書	10年	5年毎	署名符号更新時
相互認証証明書	5年以下	-	随時
リンク証明書 (OldWithNew)	旧世代の署名符号作成時～ 旧世代の電子証明書有効期限	-	自己署名証明書の 署名符号更新時
リンク証明書 (NewWithOld)	新世代の署名符号作成時～ 少なくとも旧世代の署名符号 で最後に発行した電子証明 書の有効期限	-	自己署名証明書の 署名符号更新時
利用者の 電子証明書	発行日から760日、1,125日、 1,490日、または1,765日	左記に同じ	署名符号更新時 (申込み単位)

7.2. 失効情報のプロファイル

7.2.1. バージョン番号

本認証局は、X.509バージョン2に準拠した失効情報(original_CRL、及びCRL/ARL)を発行する。

7.2.2. 拡張領域

本認証局が発行する失効情報(original_CRL、及びCRL/ARL)における拡張領域を以下

に整理する。

表 7-12 失効情報の拡張領域

項番	拡張領域の名称	Critical	original_CRL	CRL	ARL
crlEntryExtensions					
1	reasonCode	False			
CrlExtensions					
2	AuthorityKeyIdentifier	False			
3	CRLNumber	False			
4	issuingDistributionPoint	True			

: 当該失効情報に含める項目

7.2.2.1. 失効理由 (reasonCode)

本認証局では、original_CRL、及び CRL/ARL に失効された電子証明書の失効理由 (reasonCode) を記載する。

7.2.2.2. 発行者鍵識別子 (AuthorityKeyIdentifier)

本認証局では、失効情報 (original_CRL、及び CRL/ARL) において、AuthorityKeyIdentifier として keyIdentifier のみを設定する。keyIdentifier の具体的な値は、当該失効情報 (original_CRL、及び CRL/ARL) に電子署名を行った発行者署名検証符号の SHA-1 ハッシュ値とする。

7.2.2.3. CRL 番号 (cRLNumber)

本認証局では、失効情報 (original_CRL、及び CRL/ARL) において、cRLNumber を記載する。

7.2.2.4. 配布点 (issuingDistributionPoint)

本認証局では、失効情報 (original_CRL、及び CRL/ARL) において、issuingDistributionPoint を記載する。

表 7-13 失効情報の issuingDistributionPoint の設定

項番	失効情報の種類	設定値
1	original_CRL	DistributionPoint として original_CRL の配布点を URI 形式で指定するとともに、onlyContainsUserCerts、及び onlyContainsCACerts を False とする。2.6.1 項参照。
2	CRL	DistributionPoint として CRL の配布点を URI 形式で指定するとともに、onlyContainsUserCerts を True とする。2.6.1 項参照。

3	ARL	DistributionPoint として ARL の配布点を URI 形式で指定するとともに、onlyContainsCACerts を True とする。2.6.1 項参照。
---	-----	---

7.2.3. 発行頻度

本認証局では、原則として、24 時間毎に失効情報(original_CRL、及び CRL/ARL)の更新を行う。また、失効情報上に記載される次回更新時間(nextUpdate)は、当該失効情報の更新時間(thisUpdate)に 48 時間を加えた値とする。

8. 本認証局運用規程の仕様管理

8.1. 本認証局運用規程の変更

本認証局は、利用者、所属組織、及び署名検証者に事前の了解を得ることなく本認証局運用規程を変更する権利を有する。変更にあたっては、本認証局に設置された認証業務検討委員会にて変更内容を検討し、その妥当性が確認された後、RA 認証業務責任者が変更を行い、電子認証局責任者が承認する。

8.2. 本認証局運用規程の公表、及び通知

本認証局は、本認証局運用規程を変更した場合、速やかに変更した本認証局運用規程をリポジトリに掲載公表することをもって通知とする。

8.3. 本認証局運用規程の承認手続き

利用者、及び所属組織が、変更した本認証局運用規程を公表後 15 日以内に自己の電子証明書失効を要請しない場合、変更に同意したとみなされる。

Appendix 1 . 自己署名証明書プロファイル

領域名	記述例	説明
version (バージョン番号)	2	バージョン3であることを示す
serialNumber (シリアル番号)	"....."	発行時に割当て
signature (署名アルゴリズム)	1.2.840.113549.1.1.5	SHA-1withRSAEncryption
issuer (発行者名)	c=JP o=TEIKOKU DATABANK,LTD. ou=TDB CA TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述
validity (証明書有効期間)		有効期間は10年間
notBefore (発行日)	yymddhmmss	UTCTimeで記述
notAfter (終了日)	yymddhmmss	UTCTimeで記述
subject (主体者名)	c=JP o=TEIKOKU DATABANK,LTD. ou=TDB CA TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述
subjectPublicKeyInfo (主体者公開鍵情報)		
algorithm (アルゴリズム)	1.2.840.113549.1.1.1	RSAEncryption
subjectPublicKey (公開鍵)	"....."	鍵長は2048bit
issuerUniqueId	未使用	
subjectUniqueId	未使用	
Extensions (拡張領域)	Critical フラグ	
AuthorityKeyIdentifier (発行者鍵識別子)	FALSE	
keyIdentifier	"....."	公開鍵のSHA-1ハッシュ値
SubjectKeyIdentifier (主体者鍵識別子)	FALSE	"....." 公開鍵のSHA-1ハッシュ値
KeyUsage (鍵用途)	TRUE	
keyCertSign	1	電子証明書への電子署名
cRLSign	1	CRLへの電子署名
BasicConstraints (基本制約)	TRUE	
Ca	TRUE	CAであることを示す
pathLenConstraints	未使用	
CRLDistributionPoints (失効情報配布点)	FALSE	
distributionPoint	"ldap://dir.tdb.ne.jp/ou=TDB%20CA%20TypeA,o=TEIKOKU%20DATABANK%5c%2cLTD.,c=JP?authorityRevocationList"	fullNameをURIにて記述
IssuerAltName (発行者別名)	FALSE	
directoryName	c=JP o=株式会社帝国データバンク ou=TDB電子認証局TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述
SubjectAltName (主体者別名)	FALSE	
directoryName	c=JP o=株式会社帝国データバンク ou=TDB電子認証局TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述

Appendix 2 . リンク証明書プロファイル

領域名	記述例	説明
version (バージョン番号)	2	バージョン3であることを示す
serialNumber (シリアル番号)	"....."	発行時に割当て
signature (署名アルゴリズム)	1.2.840.113549.1.1.5	SHA-1withRSAEncryption
issuer (発行者名)	c=JP o=TEIKOKU DATABANK,LTD. ou=TDB CA TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述
validity (証明書有効期間)		
notBefore (発行日)	yymmddhhmmss	OldWithNew:旧世代の鍵ペアを作成した日時 NewWithOld:新世代の鍵ペアを作成した日時
notAfter (終了日)	yymmddhhmmss	OldWithNew:旧世代の自己署名証明書の有効期限 NewWithOld:少なくとも旧世代の鍵で最後に発行した証明書の有効期限
subject (主体者名)	c=JP o=TEIKOKU DATABANK,LTD. ou=TDB CA TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述
subjectPublicKeyInfo (主体者公開鍵情報)		
algorithm (アルゴリズム)	1.2.840.113549.1.1.1	RSAEncryption
subjectPublicKey (公開鍵)	"....."	鍵長は2048bit OldWithNew:旧世代の公開鍵 NewWithOld:新世代の公開鍵
issuerUniqueID	未使用	
subjectUniqueID	未使用	
Extensions (拡張領域)	Critical フラグ	
AuthorityKeyIdentifier (発行者鍵識別子)	FALSE	
keyIdentifier	"....."	OldWithNew:新世代の鍵の識別子 NewWithOld:旧世代の鍵の識別子
SubjectKeyIdentifier (主体者鍵識別子)	FALSE	"....."
OldWithNew:旧世代の鍵の識別子 NewWithOld:新世代の鍵の識別子		
KeyUsage (鍵用途)	TRUE	
keyCertSign	1	電子証明書への電子署名
cRLSign	1	CRLへの電子署名
BasicConstraints (基本制約)	TRUE	
cA	TRUE	CAであることを示す
pathLenConstraints	未使用	
CRLDistributionPoints (失効情報配布点)	FALSE	
distributionPoint	"ldap://dir.tdb.ne.jp/ou=TDB%20CA%20TypeA,o=TEIKOKU%20DATABANK%5c%2cLTD.,c=JP?authorityRevocationList"	fullNameをURIにて記述
certificatePolicies (証明書ポリシー)	FALSE	
policyIdentifier	2.5.29.32.0	"ANY-POLICY"を示す

Appendix 3 . 相互認証証明書プロファイル

領域名	記述例	説明
version (バージョン番号)	2	バージョン3であることを示す
serial Number (シリアル番号)	"....."	発行時に割当て
signature (署名アルゴリズム)	1.2.840.113549.1.1.5	SHA-1withRSAEncryption
issuer (発行者名)	c=JP o=TEIKOKU DATABANK,LTD. ou=TDB CA TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述
validity (証明書有効期間)		有効期間は5年以下
notBefore (発行日)	yymmddhhmmss	UTCTimeで記述 (有効期間の開始日が入る)
notAfter (終了日)	yymmddhhmmss	UTCTimeで記述 (有効期間の終了日が入る)
subject (主体者名)	c=JP o=Japanese Government ou=BridgeCA	BCAの識別名
subjectPublicKeyInfo (主体者公開鍵情報)		BCAの公開鍵情報
algorithm (アルゴリズム)	1.2.840.113549.1.1.1	RSAEncryption
subjectPublicKey (公開鍵)	"....."	
issuerUniqueId	未使用	
subjectUniqueId	未使用	
Extensions (拡張領域)	Critical フラグ	
AuthorityKeyIdentifier (発行者鍵識別子)	FALSE	
keyIdentifier	"....."	公開鍵のSHA-1ハッシュ値
SubjectKeyIdentifier (主体者鍵識別子)	FALSE	"....."
SubjectKeyIdentifier		BCA公開鍵のSHA-1ハッシュ値
KeyUsage (鍵用途)	TRUE	
keyCertSign	1	電子証明書への電子署名
cRLSign	1	CRLへの電子署名
BasicConstraints (基本制約)	TRUE	
cA	TRUE	CAであることを示す
pathLenConstraints	未使用	
CRLDistributionPoints (失効情報配布点)	FALSE	
distributionPoint	"ldap://dir.tdb.ne.jp/ou=TDB%20CA%20TypeA,o=TEIKOKU%20DATABANK%5c%2cLTD.,c=JP?authorityRevocationList"	fullNameをURIにて記述
certificatePolicies (証明書ポリシー)	TRUE	
policyIdentifier	1.2.392.200101.1.0.4.1	本認証局に対応するOID
policyQualifiers policyQualifierId qualifier	id-qt-cps (1.3.6.1.5.5.7.2.1) http://www.TDB.co.jp/TypeA	
PolicyMappings (ポリシーマッピング)	FALSE	
issuerDomainPolicy	1.2.392.200101.1.0.4.1	本認証局に対応するOID
subjectDomainPolicy	id-bca-cp-ds.class10(0 2 440 100145 8 1 1 1 10)	BCAのポリシOID
PolicyConstraints (ポリシー制約)	TRUE	
requireExplicitPolicy	0	

Appendix 4 . 利用者の電子証明書プロフィール

領域名	記述例	説明
version (バージョン番号)	2	バージョン3であることを示す
serial Number (シリアル番号)	"....."	発行時に割当て
signature (署名アルゴリズム)	1.2.840.113549.1.1.5	SHA-1withRSAEncryption
issuer (発行者名)	c=JP o=TEIKOKU DATABANK,LTD. ou=TDB CA TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述
validity (証明書有効期間)		有効期間は2年1ヵ月(760日)、3年1ヵ月(1,125日)、4年1ヵ月(1,490日)、4年10ヵ月(1,765日)
notBefore (発行日)	yymmddhhmmss	UTCTimeで記述
notAfter (終了日)	yymmddhhmmss	UTCTimeで記述
subject (主体者名)	c=JP o=TEIKOKU DATABANK,LTD. ou=TDB CA TypeA s=Tokyo l=Minato-ku, Minamiaoyama X-Y-Z cn=Hanako Tanaka uid=1234567890123456	cはPrintableStringで記述 c以外はUTF8Stringで記述 s, l, cnは利用者の住所及び名前を示す cnは名、姓の順で記述 uidは認証局にて割当てを行うICカードの識別番号 uidのOIDには"0.9.2342.19200300.100.1.1"を使用
subjectPublicKeyInfo (主体者公開鍵情報)		
algorithm (アルゴリズム)	1.2.840.113549.1.1.1	RSAEncryption
subjectPublicKey (公開鍵)	"....."	鍵長は1024bit
issuerUniqueID	未使用	
subjectUniqueID	未使用	
Extensions (拡張領域)	Critical フラグ	
AuthorityKeyIdentifier (発行者鍵識別子)	FALSE	
keyIdentifier	"....."	公開鍵のSHA-1ハッシュ値
SubjectKeyIdentifier (主体者鍵識別子)	FALSE	"....."
KeyUsage (鍵用途)	TRUE	
digitalSignature	1	電子署名
nonRepudiation	1	否認防止
certificatePolicies (証明書ポリシー)	TRUE	
policyIdentifier	1.2.392.200101.1.0.4.1	本認証局に対応するOID
policyQualifiers policyQualifierId qualifier	id-qt-cps http://www.tdb.co.jp/typeA	
SubjectAltName (主体者別名)	FALSE	
directoryName	c=JP s=東京都 l=千代田区霞ヶ関A丁目B番C号 o=日本株式会社 cn=田中 花子	cはPrintableStringで記述 c以外はUTF8Stringで記述 s, l, oは利用者が所属する団体の情報(場合により省略される) cnは利用者の名前(姓名の順で記述)
IssuerAltName (発行者別名)	FALSE	
directoryName	c=JP o=株式会社帝国データバンク ou=TDB電子認証局TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述
CRLDistributionPoints (失効情報配布点)	FALSE	
distributionPoint	"ldap://dir.tdb.ne.jp/ou=TDB%20CA%20TypeA,o=TEIKOKU%20DATABANK%5c%2cLTD.,c=JP?certificateRevocationList" "https://cert.tdb.ne.jp/CRL/LatestCRL.crl"	fullNameをURIにて記述

Appendix 5 . CRL プロファイル

領域名		記述例	説明
version (バージョン番号)		1	バージョン2であることを示す
signature (署名アルゴリズム)		1.2.840.113549.1.1.5	SHA-1withRSAEncryption
issuer (発行者名)		c=JP o=TEIKOKU DATABANK,LTD. ou=TDB CA TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述
thisUpdate (今回の更新日)		yymmddhhmmss	UTCTimeで記述 24時間で更新
nextUpdate (次回の更新日)		yymmddhhmmss	UTCTimeで記述 thisUpdate + 48時間とする
revokedCertificates (失効された電子証明書のリスト)			
userCertificate		"....."	失効対象電子証明書のシリアル番号
revocationDate		yymmddhhmmss	失効日
crlEntryExtensions (失効リストエントリ拡張領域)		Critical フラグ	
reasonCode		FALSE	1,2,3,5
1: 秘密鍵の危殆化 2: CAの 秘密鍵の危殆化 3: 記載事項変更による証明書失効 5: 利用の中止			
crlExtensions (失効リスト拡張領域)		Critical フラグ	
authorityKeyIdentifier (発行者鍵識別子)		FALSE	
keyIdentifier		"....."	公開鍵のSHA-1ハッシュ値
CRLNumber (CRL番号)		FALSE	"....."
CRL番号を整数で記述			
issuingDistributionPoint (配布点)		TRUE	
distributionPoint		"ldap://dir.tdb.ne.jp/ou=TDB%20CA%20TypeA,o=TEIKOKU%20DATABANK%5c%2cLTD.,c=JP?certificateRevocationList"	fullNameをURIにて記述
onlyContainsUserCerts		TRUE	

Appendix 6 . ARL プロファイル

領域名		記述例	説明
version (バージョン番号)		1	バージョン2であることを示す
signature (署名アルゴリズム)		1.2.840.113549.1.1.5	SHA-1withRSAEncryption
issuer (発行者名)		c=JP o=TEIKOKU DATABANK,LTD. ou=TDB CA TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述
thisUpdate (今回の更新日)		yymmddhhmmss	UTCTimeで記述 24時間で更新
nextUpdate (次の更新日)		yymmddhhmmss	UTCTimeで記述 thisUpdate + 48時間とする
revokedCertificates (失効された電子証明書のリスト)			
userCertificate		"....."	失効対象電子証明書のシリアル番号
revocationDate		yymmddhhmmss	失効日
crlEntryExtensions (失効リストエントリ拡張領域)		Critical フラグ	
reasonCode		FALSE	1,2,3,5
1: 秘密鍵の危殆化 2: CAの 秘密鍵の危殆化 3: 記載事項変更による証明書失効 5: 利用の中止			
crlExtensions (失効リスト拡張領域)		Critical フラグ	
authorityKeyIdentifier (発行者鍵識別子)		FALSE	
keyIdentifier		"....."	公開鍵のSHA-1ハッシュ値
CRLNumber (CRL番号)		FALSE	"....."
CRL番号を整数で記述			
issuingDistributionPoint (配布点)		TRUE	
distributionPoint		"ldap://dir.tdb.ne.jp/ou=TDB%20CA%20TypeA,o=TEIKOKU%20DATABANK%5c%2cLTD.,c=JP?authorityRevocationList"	fullNameをURIにて記述
onlyContainsCACerts		TRUE	

Appendix7 . original_CRL プロファイル

領域名		記述例	説明
version (バージョン番号)		1	バージョン2であることを示す
signature (署名アルゴリズム)		1.2.840.113549.1.1.5	SHA-1withRSAEncryption
issuer (発行者名)		c=JP o=TEIKOKU DATABANK,LTD. ou=TDB CA TypeA	cはPrintableStringで記述 c以外はUTF8Stringで記述
thisUpdate (今回の更新日)		yymmddhhmmss	UTCTimeで記述 24時間で更新
nextUpdate (次回の更新日)		yymmddhhmmss	UTCTimeで記述 thisUpdate + 48時間とする
revokedCertificates (失効された電子証明書のリスト)			
userCertificate		"....."	失効対象電子証明書のシリアル番号
revocationDate		yymmddhhmmss	失効日
crlEntryExtensions (失効リストエントリ拡張領域)		Critical フラグ	
reasonCode		FALSE	1,2,3,5
1:秘密鍵の危殆化 2:CAの秘密鍵の危殆化 3:記載事項変更による証明書失効 5:利用の中止			
crlExtensions (失効リスト拡張領域)		Critical フラグ	
authorityKeyIdentifier (発行者鍵識別子)		FALSE	
keyIdentifier		"....."	公開鍵のSHA-1ハッシュ値
CRLNumber (CRL番号)		FALSE	"....."
CRL番号を整数で記述			
issuingDistributionPoint (配布点)		TRUE	
distributionPoint		"https://cert.tdb.ne.jp/CRL/LatestCRL.crl"	fullNameをURIにて記述
onlyContainsUserCerts		FALSE	
onlyContainsCACerts		FALSE	