

政府認証基盤 (GPKI)

官職認証局 CP/CPS

平成 19 年 7 月 6 日

平成 21 年 5 月 25 日改定

平成 24 年 3 月 23 日改定

平成 27 年 3 月 27 日改定

平成 30 年 12 月 26 日改定

令和 3 年 3 月 1 日改定

行政情報システム関係課長連絡会議了承

令和 3 年 9 月 30 日改定

デジタル社会推進会議副幹事会了承

令和 3 年 12 月 9 日改定

令和 3 年 12 月 23 日改定

デジタル社会推進会議関係課長等連絡会議了承

1. はじめに.....	1
1.1 概要.....	1
1.2 文書名と識別.....	1
1.3 PKI の関係者.....	2
1.3.1 デジタル社会推進会議関係課長等連絡会議.....	2
1.3.2 発行局 (IA) 及び登録局 (RA)	2
1.3.3 府省等登録局 (LRA)	3
1.3.4 証明書利用者.....	3
1.3.5 証明書検証者.....	3
1.3.6 その他関係者.....	3
1.4 証明書の用途.....	3
1.4.1 適切な証明書の用途.....	3
1.4.2 禁止される証明書の用途.....	4
1.5 ポリシ管理.....	4
1.5.1 文書を管理する組織.....	4
1.5.2 連絡先.....	4
1.5.3 ポリシ適合性を決定する者.....	4
1.5.4 承認手続.....	4
1.6 定義と略語.....	4
2. 公表とリポジトリの責任.....	13
2.1 リポジトリ.....	13
2.2 証明情報の公表.....	13
2.3 公表の時期又は頻度.....	13
2.4 リポジトリへのアクセス管理.....	13
3. 識別と認証.....	14
3.1 名前決定.....	14
3.1.1 名前の種類.....	14
3.1.2 名前が意味を持つことの必要性.....	14
3.1.3 証明書利用者の匿名性又は仮名性.....	14
3.1.4 様々な名前形式を解釈するための規則.....	14
3.1.5 名前の一意性.....	14
3.1.6 認識、認証及び商標の役割.....	14
3.2 初回の識別と認証.....	14
3.2.1 秘密鍵の所持を証明する方法.....	14
3.2.2 組織の認証.....	15
3.2.3 個人の認証.....	15

3.2.4	検証されない証明書利用者の情報	15
3.2.5	権限の正当性確認	15
3.2.6	相互運用の基準	15
3.3	更新申請時の識別と認証	15
3.3.1	通常の新規時における識別と認証	15
3.3.2	証明書失効後の更新時における識別と認証	15
3.4	失効申請時の識別と認証	15
4.	証明書のライフサイクルに対する運用上の要件	16
4.1	証明書申請	16
4.1.1	証明書申請者	16
4.1.2	登録手続及び責任	16
4.2	証明書申請手続	17
4.3	証明書の発行	17
4.4	証明書の受領	18
4.5	鍵ペア及び証明書の使用	19
4.5.1	証明書利用者の秘密鍵及び証明書の使用	19
4.5.2	証明書検証者の公開鍵及び証明書の使用	19
4.6	証明書の更新	19
4.7	鍵更新を伴う証明書の更新	19
4.8	証明書の変更	20
4.9	証明書の失効と一時停止	20
4.9.1	証明書失効事由	20
4.9.2	証明書失効の申請者	22
4.9.3	失効申請手続	22
4.9.4	失効申請の猶予期間	23
4.9.5	認証局が失効申請を処理しなければならない期間	23
4.9.6	失効調査の要求	23
4.9.7	CRL/ARL の発行頻度	24
4.9.8	CRL/ARL の発行最大遅延時間	24
4.9.9	オンラインでの失効/ステータス確認の可用性	24
4.9.10	オンラインでの失効/ステータス確認を行うための要件	24
4.9.11	利用可能な失効情報の他の形式	24
4.9.12	鍵の危殆化に対する特別要件	24
4.9.13	証明書の一時停止事由	24
4.9.14	証明書一時停止の申請者	24
4.9.15	証明書の一時停止申請手続	24

4.9.16 一時停止を継続できる期間.....	24
4.10 証明書のステータス確認サービス.....	25
4.11 登録の終了.....	25
4.12 秘密鍵の預託と回復.....	25
5. 設備上、運営上、運用上の管理.....	26
5.1 物理的管理.....	26
5.1.1 立地場所及び構造.....	26
5.1.2 物理的アクセス.....	26
5.1.3 電源及び空調.....	26
5.1.4 水害対策.....	26
5.1.5 地震対策.....	26
5.1.6 火災防止及び火災保護対策.....	26
5.1.7 媒体保管.....	27
5.1.8 廃棄処理.....	27
5.1.9 オフサイトバックアップ.....	27
5.2 手続的管理.....	27
5.2.1 信頼すべき役割.....	27
5.2.2 職務ごとに必要とされる人数.....	29
5.2.3 個々の役割に対する本人性確認と認証.....	30
5.2.4 職務分割が必要となる役割.....	30
5.3 人事的管理.....	30
5.4 監査ログの手続.....	30
5.4.1 記録されるイベントの種類.....	30
5.4.2 監査ログを処理する頻度.....	30
5.4.3 監査ログの保管期間.....	30
5.4.4 監査ログの保護.....	31
5.4.5 監査ログのバックアップ手続.....	31
5.4.6 監査ログの収集システム.....	31
5.4.7 イベントを起こした者への通知.....	31
5.4.8 脆弱性評価.....	31
5.5 記録の保管.....	31
5.5.1 アーカイブの種類.....	31
5.5.2 アーカイブ保管期間.....	31
5.5.3 アーカイブの保護.....	31
5.5.4 アーカイブのバックアップ手続.....	32
5.5.5 記録にタイムスタンプを付与する要件.....	32

5.5.6	アーカイブ収集システム	32
5.5.7	アーカイブの検証手続	32
5.6	鍵の切り替え	32
5.7	危殆化及び災害からの復旧	32
5.7.1	事故及び危殆化時の手続	32
5.7.2	ハードウェア、ソフトウェア又はデータが破壊された場合の手続	32
5.7.3	エンティティの秘密鍵が危殆化した場合の手続	32
5.7.4	災害後の事業継続性	33
5.8	認証業務の終了	33
6.	技術的セキュリティ管理	34
6.1	鍵ペアの生成及びインストール	34
6.1.1	鍵ペアの生成	34
6.1.2	証明書利用者に対する秘密鍵の配付	34
6.1.3	CA への公開鍵の配付	34
6.1.4	証明書検証者への CA 公開鍵の配付	35
6.1.5	鍵のサイズ	35
6.1.6	公開鍵パラメータの生成及び品質検査	35
6.1.7	鍵の用途	35
6.2	秘密鍵の保護及び暗号モジュール技術の管理	35
6.2.1	暗号モジュールの標準及び管理	35
6.2.2	秘密鍵の複数人管理	36
6.2.3	秘密鍵の預託	36
6.2.4	秘密鍵のバックアップ	36
6.2.5	秘密鍵のアーカイブ	36
6.2.6	秘密鍵の暗号モジュールへの又は暗号モジュールからの転送	36
6.2.7	暗号モジュールへの秘密鍵の格納	36
6.2.8	秘密鍵の活性化方法	37
6.2.9	秘密鍵の非活性化方法	37
6.2.10	秘密鍵の破棄方法	37
6.2.11	暗号モジュールの評価	38
6.3	鍵ペアのその他の管理方法	38
6.3.1	公開鍵のアーカイブ	38
6.3.2	秘密鍵及び公開鍵の有効期間	38
6.4	活性化データ	38
6.4.1	活性化データの生成及び設定	38
6.4.2	活性化データの保護	39

6.4.3	活性化データの他の考慮点	39
6.5	コンピュータのセキュリティ管理	39
6.5.1	コンピュータセキュリティに関する技術的要件	39
6.5.2	コンピュータセキュリティ評価	40
6.6	ライフサイクルセキュリティ管理	40
6.6.1	システム開発管理	40
6.6.2	セキュリティ運用管理	40
6.6.3	ライフサイクルセキュリティ管理	40
6.7	ネットワークセキュリティ管理	40
6.8	タイムスタンプ	40
7.	証明書、証明書失効リストのプロファイル	41
7.1	証明書プロファイル	41
7.2	CRL/ARL プロファイル	41
8.	準拠性監査と他の評価	42
8.1	監査の頻度	42
8.2	監査者の身元／資格	42
8.3	監査者と被監査者の関係	42
8.4	監査で扱われる事項	42
8.5	不備の結果としてとられる処置	42
8.6	監査結果の開示	42
9.	他の業務上及び法的事項	43
9.1	料金	43
9.2	財務的責任	43
9.3	情報の機密性	43
9.3.1	機密情報の範囲	43
9.3.2	機密情報の範囲外の情報	43
9.3.3	機密情報を保護する責任	43
9.4	個人情報の保護	43
9.5	知的財産権	43
9.6	表明保証	44
9.6.1	IA 及び RA の表明保証	44
9.6.2	LRA の表明保証	44
9.6.3	証明書利用者の表明保証	45
9.6.4	証明書検証者の表明保証	45
9.6.5	他の関係者の表明保証	45
9.7	無保証	45

9.8 責任の制限	45
9.9 補償	45
9.10 有効期間と終了	45
9.10.1 有効期間	45
9.10.2 終了	45
9.10.3 終了の効果と効果継続	46
9.11 関係者間の個別通知と連絡	46
9.12 改定	46
9.12.1 改定手続	46
9.12.2 通知方法及び期間	46
9.12.3 オブジェクト識別子を変更されなければならない場合	46
9.13 紛争解決手続	46
9.14 準拠法	46
9.15 適用法の遵守	46
9.16 雑則	46
9.17 その他の条項	47

1. はじめに

本 CP/CPS は、国民等と行政機関等との間の申請・届出等手続の電子化を実現するため、デジタル庁が運営するブリッジ認証局（以下「BCA」という。）と相互認証を行い、官職の証明書等を発行する官職認証局（以下「官職 CA」という。）の認証業務に関する運営方針を定める。

なお、本 CP/CPS の構成は、IETF PKIX による RFC3647「Certificate Policy and Certification Practices Statement Framework」に準拠している。

1.1 概要

官職 CA は、官職等に対して官職証明書、利用者証明書及び暗号化通信用等証明書を発行し、BCA と相互認証証明書を取り交わす。

官職 CA は、CP（証明書ポリシー）及び CPS（認証実施規程）をそれぞれ独立したものとして、本 CP/CPS を官職 CA の認証業務に関する運営方針として位置付ける。

1.2 文書名と識別

官職 CA の証明書ポリシーは、官職 CA の相互認証証明書ポリシー、官職 CA の相互認証テスト用証明書ポリシー、官職証明書用の証明書ポリシー、利用者証明書用の証明書ポリシー及び暗号化通信用等証明書の証明書ポリシーであり、識別子は、それぞれ次のとおりとする。

- ・ 官職 CA 相互認証証明書ポリシー
 - 0.2.440.100145.8.3.1.1.110（sha256WithRSAEncryption の官職証明書用）
 - 0.2.440.100145.8.3.1.21.130（sha256WithRSAEncryption の利用者証明書用）
- ・ 官職 CA 相互認証テスト用証明書ポリシー
 - 0.2.440.100145.8.3.1.1.100（sha256WithRSAEncryption の官職証明書用）
 - 0.2.440.100145.8.3.1.21.100（sha256WithRSAEncryption の利用者証明書用）
- ・ 官職証明書ポリシー
 - 0.2.440.100145.8.3.1.1.110（sha256WithRSAEncryption の官職証明書用）
- ・ 利用者証明書ポリシー
 - 0.2.440.100145.8.3.1.21.130（sha256WithRSAEncryption の利用者証明書用）
- ・ 暗号化通信用等証明書ポリシー
 - 0.2.440.100145.8.3.1.21.150（sha256WithRSAEncryption の暗号化通信用等証明書用）

1.3 PKI の関係者

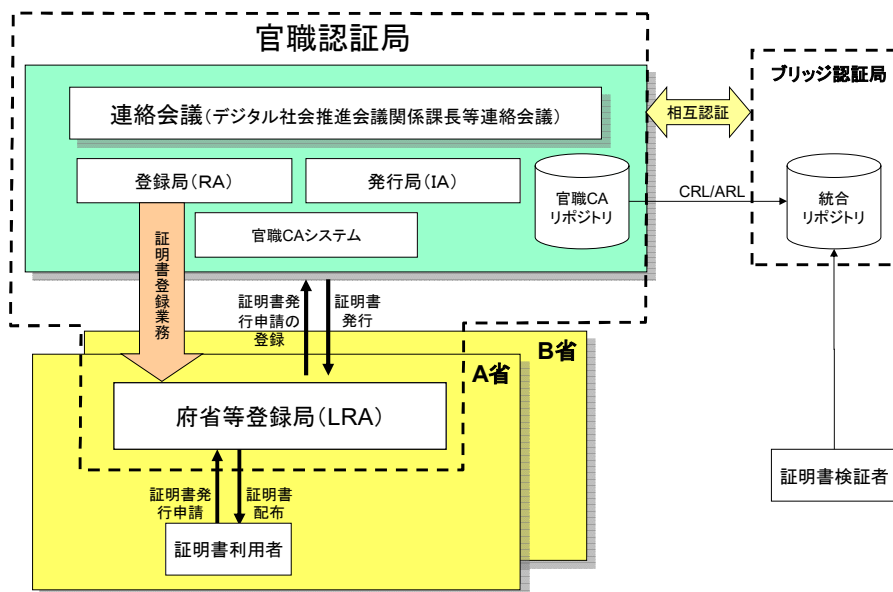


図 1-1 組織体制図

1.3.1 デジタル社会推進会議関係課長等連絡会議

官職 CA の運営に関する意思決定は、デジタル社会推進会議関係課長等連絡会議（以下「連絡会議」という。）が行う。

官職 CA の運営に関する連絡会議の機能は、次のとおりとする。

- ・ 官職 CA の CP/CPS に関する決定
- ・ 相互認証に関する決定
- ・ CA 秘密鍵危殆化時の対応に関する決定
- ・ 災害発生等による緊急時の対応に関する決定
- ・ 府省等登録局（以下「LRA」という。）の設置及び廃止に関する決定
- ・ その他官職 CA の運営に関する重要事項の決定

1.3.2 発行局 (IA) 及び登録局 (RA)

BCA への相互認証申請及び相互認証証明書の発行、更新、失効、CA 秘密鍵の管理、LRA の設置及び廃止に関する運營業務は、運営責任者、IA 鍵管理者、受付担当者及び審査担当者が行う。

運営責任者は、デジタル庁統括官付参事官を充てる。

また、システムオペレーション、システムの維持管理、証明書の発行、更新、失効等の運用業務は、運用責任者、運用責任者補佐、上級 IA 操作員、一般 IA 操作員及び監査ログ検

査者が行う。それぞれの業務については、「5.2 手続的管理」において定める。

1.3.3 府省等登録局（LRA）

連絡会議の承認を受け、原則として府省等単位で設置される組織であり、証明書利用者からの証明書発行、更新及び失効に関する申請の受付と審査を行う。

要員として、LRA 管理者、LRA 操作員、LRA 受付担当者及び LRA 審査担当者を配置する。それぞれの業務については、「5.2 手続的管理」において定める。

1.3.4 証明書利用者

官職 CA が発行する証明書を管理し、本 CP/CPS に従い証明書を利用する。

1.3.5 証明書検証者

自己署名証明書、リンク証明書、官職証明書、利用者証明書、暗号化通信用等証明書及び相互認証証明書の失効情報を公表する失効リスト（以下「CRL/ARL」という。）により証明書の有効性を確認する。

1.3.6 その他関係者

規定しない。

1.4 証明書の用途

1.4.1 適切な証明書の用途

相互認証証明書は、国民等と行政機関等との間の申請・届出等手続の電子化を実現するため、BCA との相互認証で使用される。相互認証証明書の有効期間は、証明書を有効とする日から起算して 5 年以内とする。

官職証明書は、府省等における官職等を示す証明書であり、国民等と行政機関等との間の申請・届出等手続の電子化及び行政機関等内での手続の電子化等で使用する。官職証明書（sha256WithRSAEncryption）の有効期間は、証明書を有効とする日から起算して 5 年とする。

利用者証明書は、府省等の官職等を示す証明書であり、府省等が運用する情報システムの認証等に使用する。利用者証明書（sha256WithRSAEncryption）の有効期間は、証明書を有効とする日から起算して 5 年とする。

暗号化通信用等証明書は、情報提供ネットワークシステム、マイナポータル（省庁等連携機能）及びこれらのシステムの少なくとも一方に接続する電子計算機並びにその使用者を示す証明書であり、通信データの署名及び暗号化に使用する。暗号化通信用等証明書（sha256WithRSAEncryption）の有効期間は、証明書を有効とする日から起算して 5 年と

する。

1.4.2 禁止される証明書の用途

官職 CA が発行する証明書は「1.4.1 適切な証明書の用途」以外の目的に利用してはならない。

1.5 ポリシ管理

1.5.1 文書を管理する組織

本 CP/CPS の変更、更新等に関する事務は、デジタル庁が行う。

1.5.2 連絡先

本 CP/CPS に関する照会は、デジタル庁を窓口とする。

窓口の連絡先は、以下の URL に掲示する。

URL : <https://www.gpki.go.jp/>

1.5.3 ポリシ適合性を決定する者

官職 CA の CP/CPS の適合性を決定する者は、連絡会議とする。

1.5.4 承認手続

官職 CA の CP/CPS は、連絡会議の決定をもって有効なものとする。

1.6 定義と略語

<A~Z>

- ・ ARL (Authority Revocation List : 認証局失効リスト)

証明書の有効期間中に、CA 秘密鍵の危殆化、相互認証基準違反等の事由により失効された自己署名証明書及び相互認証証明書のリスト。このリストには、失効した証明書を発行した CA の署名が付与される。

- ・ BCA (Bridge CA)

国・地方公共団体等の官職等を認証する認証局と国民等を認証する認証局との間の相互認証を行う認証局。

- ・ CA (Certification Authority : 認証局)

証明書の発行・更新・失効、CA 等秘密鍵の生成・保護及び証明書利用者の登録を行う機関。単に CA という場合は証明書発行業務及び登録業務を含む。

- CP/CPS (Certificate Policy : 証明書ポリシー/Certification Practices Statement : 認証実施規程

CP : CA が証明書を発行する際の運用方針を定めた文書。

CPS : CA の信頼性、安全性を対外的に示すために、CA の運用、証明書ポリシー、鍵の生成・管理、責任等に関して定めた文書。証明書ポリシーが何を運用方針にするのかを示すのに対して、認証実施規程は運用方針をどのように適用させるのかを示す。

- CRL(Certificate Revocation List : 証明書失効リスト)

証明書の有効期間中に、CA 秘密鍵の危殆化等の事由により失効された官職証明書、利用者証明書及び暗号化通信用等証明書のリスト。このリストには、失効した証明書を発行した CA の署名が付与される。

- FIPS 140-1 (2) (Federal Information Processing Standard)

NIST(National Institute of Standards and Technology : 米国標準技術研究所)が策定した米国連邦情報処理標準のうち、暗号技術に関するセキュリティ要件を規定しているもの。コンピュータと通信システムの暗号モジュールに対して暗号技術に関する汎用要件を網羅しており、最低レベル 1 から最高レベル 4 までのセキュリティレベルが設定されている。

レベル 1 : FIPS で定義している最低限のセキュリティレベル。一般的な PC に適用されているような暗号モジュールに適用されているレベル。

レベル 2 : 暗号モジュールに、不正アクセスされた場合に、侵入の痕跡を残せるような仕組みを備えているレベル。

レベル 3 : 暗号モジュールに、不正アクセスされた場合に、侵入の痕跡を残せるような仕組みを備えている。レベル 2 に比べ、痕跡をより厳密に追跡できるような仕組みを備えているレベル。特殊なハードウェア装置を使い、侵入があった場合にはデータを消去するような仕組みを持つ。

レベル 4 : FIPS で定義している最高のセキュリティレベル。温度の変化や電流の変化等の環境の変動も検知できるような仕組みを導入しているレベル。

- GPKI (Government Public Key Infrastructure : 政府認証基盤)

国民等と行政機関等との間の申請・届出等手続の電子化及び行政機関等の間、同一組織内等での手続の電子化等における電子文書について、その文書が真にその名義人によって作成され、内容に改変がないことを相互に確認するための仕組み、基盤。具体的には、公開鍵暗号方式による署名を用いた国の行政機関の認証システムであり、BCA と行政機関等側 CA から構成される。

- ・ **HSM (Hardware Security Module)** : ハードウェアセキュリティモジュール)
ハードウェアによる秘密鍵の管理装置。
- ・ **IA (Issuing Authority)** : 発行局)
CA の業務のうち、証明書発行業務を行う機関。「IA 操作員」とは、証明書の発行を主業務とする者で、官職 CA では権限分離の観点から「上級 IA 操作員」と「一般 IA 操作員」に分ける。
- ・ **IETF (Internet Engineering Task Force)**
インターネットの技術的活動部会。インターネットにおけるプロトコルの技術開発、標準化を主な目的としている。作成された仕様は RFC (Request For Comments) と呼ばれる。
- ・ **ISO(International Organization for Standardization)**
国際標準化機構。電気分野を除くあらゆる分野において、国際的に通用する規格・標準類の制定を目的としている。
- ・ **ITU (International Telecommunication Union)**
国際連合(UN)の専門機関の 1 つである国際電気通信連合。電気通信の改善、合理的利用を目的としている。
- ・ **ITU-T(International Telecommunication Union - Telecommunication Standardization Sector)**
国際電気通信連合の電気通信標準化部門。
- ・ **LRA (Local Registration Authority)**
府省等单位で設置される組織。証明書利用者からの証明書の発行、更新及び失効申請の受付と審査を行う。
- ・ **OID (Object Identification)** : オブジェクト識別子)
世界で一意となる値を登録機関 (ISO、ITU) に登録した識別子。PKI で使うアルゴリズム、証明書内に格納する名前 (subject) のタイプ (Country 名等の属性) 等は、オブジェクト識別子として登録されているものが使用される。
- ・ **PIN (Personal Identification Number)**
個人識別番号。証明書利用者へ配付する IC カードの活性化に用いるパスワード及び証明書利用者が鍵ペアを生成した場合に設定する秘密鍵保護に用いるパスワード等を指す。

- PKCS (Public Key Cryptography Standards) #10

PKCS とは、米国 RSA Data Security 社による公開鍵暗号方式を実現するための技術標準。その1つである PKCS #10 は、CA に対する証明書発行要求メッセージの構文 (Certification Request Syntax Standard) に関する規格。

- PKI (Public Key Infrastructure : 認証基盤)

公開鍵の正当性を保証する公開鍵証明書を利用するための基盤。

- PKIX(Public-Key Infrastructure (X.509))

IETF セキュリティ分野の1つの作業部会。証明書及び CRL/ARL のプロファイル、CP と CPS のフレームワーク等の制定を目的としている。

- RA (Registration Authority : 登録局)

CA の業務のうち、登録業務を行う機関。主な業務は、証明書発行に必要な情報の登録、CA に対する証明書発行要求等である。

- RFC3647 (Request For Comments3647)

RFC とは、インターネットに関する標準文書の総称。その1つである RFC3647 は、CP 又は CPS を作成するためのフレームワーク及びガイドラインを提供している。

- RSA

公開鍵暗号方式で利用する暗号アルゴリズムの1つ。十分に大きな2つの異なる素数を掛け合わせた整数の素因数分解が困難であることに安全性の根拠をおく。

- X.500 識別名(DN:Distinguished Name)

X.500 とは、名前及びアドレスの調査から属性による検索まで広範囲なサービスを提供することを目的に ITU が開発したディレクトリ標準。X.500 識別名は、X.509 の発行者名及び主体者名に使用される。

- X.509

ITU-T が定めた証明書及び CRL/ARL のフォーマット。X.509 v3(Version 3)では、任意の情報を保有するための拡張領域が追加された。GPKI では、証明書は X.509 v3、CRL/ARL は X.509 v2 を使用する。

<あ〜ん>

- アーカイブ

証明書の発行履歴、失効履歴等を長期間保管すること。

- アクセス制御

コンピュータ等、情報の供給源への不正アクセスを防止するための制御機能。アクセス者を識別し、本人であることを確認した上で、あらかじめ設定してある権限（読み出し、書込み等）の操作を可能にする。

- アルゴリズム

計算や問題を解決するための手順、方式。

- 暗号モジュール

暗号化、復号、デジタル署名、認証技術、乱数生成などの暗号化機能を実装したハードウェア、ファームウェア、ソフトウェア及びその組合せ製品。

- 改ざん

データの内容を書き換えられること。

- 鍵のサイズ（鍵長）

暗号の強度を決定する要素の1つ。鍵の長さをビット数で表したものが鍵のサイズであり、鍵のサイズが大きいほど暗号の強度は増す。

- 鍵ペア

公開鍵暗号方式における公開鍵と秘密鍵のペア。一方の鍵から他方の鍵を導き出せない性質を持つため、一方（秘密鍵）を秘密にすることで、他方（公開鍵）を公開することができる。

- 活性化

システム、装置等を使用可能な状態にすること。

- 活性化データ

システム、装置等を活性化するために必要となるデータ（パスワード等）。

- 官職 CA リポジトリ

官職 CA が発行する証明書及び CRL/ARL を格納するリポジトリ。「リポジトリ」参照。

- 管理鍵

HSM の機能を制御する鍵。

- ・ 危殆化

信頼性が喪失された可能性のある事態の発生をいう。CA の場合、CA 秘密鍵が危殆化することによって、発行した全ての証明書の信頼性が失われる。

- ・ 公開鍵

公開鍵暗号方式において用いられる鍵ペアの一方。秘密鍵に対応する、公開されている鍵。

- ・ 公開鍵暗号方式

メッセージを暗号化した鍵と異なる鍵を用いて復号する暗号方式。代表的なものに RSA 暗号方式がある。

- ・ 公開鍵パラメータ

楕円曲線暗号等を利用するに当たって、証明書所有者及び証明書検証者が共通に用いる。楕円曲線暗号においては、計算の基盤となる曲線のパラメータを指す。

- ・ コンピュータセキュリティ

コンピュータシステムを中心とした情報処理活動に関する資産を、それを取り巻く脅威から保護し、情報の機密性、完全性及び可用性を満たすための対策。

- ・ 自己署名証明書

自 CA の公開鍵に対して、自 CA の秘密鍵で署名した証明書。自 CA の公開鍵の正当性を保証する。

- ・ 失効情報

証明書の有効期間中に、記載内容の変更に伴う証明書の更新、CA 秘密鍵の危殆化等の事由により、発行した証明書を失効する際に、CA が公表する証明書の失効を示す情報。

- ・ 失効リスト

「CRL」及び「ARL」参照。

- ・ 主体者名

証明書を所有し、証明書に格納されている公開鍵に対応する秘密鍵を所有している証明書利用者を識別する名前。

- ・ 証明書（公開鍵証明書）

ある公開鍵を、記載されたものが保有することを証明する電子的文書。CA が記載内容を確認の上、CA の署名を付与することで、その公開鍵の正当性を保証する。

- ・ 証明書検証者

証明書の有効性を検証する者（ソフトウェアを含む）。

- ・ 証明書発行要求（CSR : Certificate Signing Request）

証明書を発行する際のもとのデータファイル。CSR には証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して証明書を発行する。GPKI では PKCS#10 に従う。

- ・ 証明書利用者

証明書の発行対象（相互認証先 CA 等）。

- ・ 署名（デジタル署名）

公開鍵暗号方式の秘密鍵を利用した、メッセージの完全性を保証する仕組み。メッセージの送信者が保有する秘密鍵でメッセージのハッシュ値を暗号化し、メッセージに付与すること。メッセージ受信者側は、署名者の公開鍵を用いて、送信者の本人確認及びメッセージの改ざん検知を行う。

- ・ セキュリティ監査

セキュリティを重点テーマとして実施する監査。

- ・ 相互認証基準

BCA と相互認証する相互認証先 CA が満たすべき要件。技術基準と運用基準から構成される。

- ・ 相互認証証明書

2つの異なる認証ドメインの CA がお互いを認証したことを示すために、相互に発行する証明書。GPKI では、行政機関等側 CA 又は国民等側 CA と BCA の間で相互認証証明書が発行される。

- ・ 操作鍵

HSM の操作をする際に必要となる鍵。

- ・ タイムスタンプ

信頼できる時刻管理機器によって管理される時刻を基に、ログ等に記録される事象の発生時刻を示す値。

- ・ 楕円曲線暗号方式

楕円曲線上で定義された加減演算を使用して計算を行う暗号方式。パラメータを変えることにより、強度を保つ必要がある。

- ・ 統合リポジトリ

BCA リポジトリ及び官職 CA リポジトリが保有する情報のうち、証明書の有効性検証に必要な証明書及び CRL/ARL を格納し、公表するリポジトリ。BCA が運営する。「リポジトリ」参照。

- ・ 認証ドメイン

特定の証明書ポリシーの下に運営する CA が発行する証明書の適用範囲。

- ・ 認証パス

自己の証明書を発行した CA から相手の証明書を発行した CA までをたどる検証の道筋。

- ・ 発行者名

証明書を発行し署名を施した CA を識別する名前。

- ・ ハッシュ関数

異なる2つの入力値から同じ出力値を算出することが困難な関数。また、出力値から入力値を逆算することも困難である。

- ・ ハッシュ値

ある値に対するハッシュ関数の出力値。「ハッシュ関数」参照。

- ・ 非活性化

システム、装置等を使用不可能な状態にすること。

- ・ 秘密鍵

公開鍵暗号方式において用いられる鍵ペアの一方。公開鍵に対応する、本人のみが保有する鍵。

- 秘密鍵の預託
本人しか持ち得ない署名用の秘密鍵を第三者に預けること。
- フィンガープリント
任意のメッセージに対するハッシュ値。GPKI では、公開鍵に対するハッシュ値を指す。ハッシュ関数の性質で一意に決まることからフィンガープリント（指紋）と呼ばれる。「ハッシュ関数」参照。
- プロファイル
証明書及び CRL/ARL に含まれるデータの内容を定義したもの。RFC5280 により証明書及び CRL/ARL のプロファイルについて定義されている。
- リストア
バックアップデータを復元すること。
- リポジトリ
証明書及び CRL/ARL を格納し公表するデータベース。
- リンク証明書
CA の鍵更新に伴い同時に存在することとなる新しい CA 鍵ペアと古い CA 鍵ペアの関係を保証するための証明書。
- ログ
コンピュータ上で行った操作及び処理を記録したファイル。

2. 公表とリポジトリの責任

2.1 リポジトリ

官職 CA に関する情報は、統合リポジトリ及び Web 上で公表する。

2.2 証明情報の公表

(1) 統合リポジトリ上での公表

官職 CA は、官職 CA リポジトリに保有する次の情報を統合リポジトリに登録し、公表する。

- ・ 官職 CA の自己署名証明書
- ・ リンク証明書
- ・ 相互認証証明書
- ・ CRL/ARL

(2) Web 上での公表

官職 CA は、次の情報を Web 上で公表する。

- ・ 官職 CA の自己署名証明書及びそのフィンガープリント
- ・ 官職 CA と相互認証した CA の名称及び相互認証を取り消した CA の名称
- ・ CA 秘密鍵危殆化に関する情報
- ・ 本 CP/CPS 及びその改定履歴

2.3 公表の時期又は頻度

公表する情報の更新頻度は次のとおりとする。

- ・ 自己署名証明書、リンク証明書、相互認証証明書及び CRL/ARL は、発行及び更新の都度
- ・ 官職 CA と相互認証した CA の名称及び相互認証を取り消した CA の名称は、連絡会議による決定の都度
- ・ 本 CP/CPS は、本 CP/CPS の変更の都度

2.4 リポジトリへのアクセス管理

官職 CA リポジトリから登録した統合リポジトリ上で公表する情報及び Web 上で公表する情報については、特段のアクセス制御は行わない。

3. 識別と認証

3.1 名前決定

3.1.1 名前の種類

官職 CA が発行する証明書の発行者名及び主体者名は、X.500 識別名 (DN:Distinguished Name) の形式に従って設定する。

3.1.2 名前が意味を持つことの必要性

発行する証明書において使用する名前は、認証局、官職等の名称とする。

3.1.3 証明書利用者の匿名性又は仮名性

「3.1.2.名前が意味を持つことの必要性」のとおりとする。

3.1.4 様々な名前形式を解釈するための規則

名前の形式を解釈するための規則は、BCA の定める規則に従う。

3.1.5 名前の一意性

官職 CA の発行する証明書の主体者名は、一意に割り当てる。

3.1.6 認識、認証及び商標の役割

規定しない。

3.2 初回の識別と認証

3.2.1 秘密鍵の所持を証明する方法

IA 及び RA は、相互認証手続において、BCA から提出された証明書発行要求の署名の検証を行い、含まれている CA 公開鍵に対応する CA 秘密鍵で署名されていることを確認する。また、証明書発行要求のフィンガープリントを確認し、CA 公開鍵の所有者を特定する。

官職証明書及び利用者証明書の申請手続において、IA 及び RA 側で秘密鍵と公開鍵が対応する鍵ペアを生成する。証明書利用者が鍵ペアを生成する場合には、IA 及び RA は、証明書発行要求の署名の検証を行い、含まれている公開鍵に対応する秘密鍵で署名されていることを確認する。

暗号化通信用等証明書の申請手続において、IA 及び RA は、証明書発行要求の署名の検証を行い、含まれている公開鍵に対応する秘密鍵で署名されていることを確認する。

3.2.2 組織の認証

IA 及び RA は、相互認証手続において、所定の手続に基づき、相互認証先の CA を運営する組織の真偽を確認する。

LRA は、官職証明書、利用者証明書及び暗号化通信用等証明書の申請手続において、所定の手続に基づき、証明書利用者の属する組織の真偽を確認する。

3.2.3 個人の認証

IA 及び RA は、相互認証手続において、所定の手続に基づき、相互認証証明書の発行申請を行う者の真偽を確認する。

LRA は、官職証明書、利用者証明書及び暗号化通信用等証明書の申請手続において、所定の手続に基づき、証明書利用者の真偽を確認する。

3.2.4 検証されない証明書利用者の情報

規定しない。

3.2.5 権限の正当性確認

権限の正当性確認は、「3.2.2 組織の認証」及び「3.2.3 個人の認証」において定める手続に基づいて行う。

3.2.6 相互運用の基準

相互認証の基準は、BCA の定めによるものとする。

3.3 更新申請時の識別と認証

3.3.1 通常の新規申請時における識別と認証

証明書更新時における識別と認証は、「3.2 初回の識別と認証」において定める手続に基づいて行う。

3.3.2 証明書失効後の更新時における識別と認証

証明書失効後の再発行時における識別と認証は、「3.2 初回の識別と認証」において定める手続に基づいて行う。

3.4 失効申請時の識別と認証

証明書の失効時における識別と認証は、「3.2.2 組織の認証」及び「3.2.3 個人の認証」において定める手続に基づいて行う。

4. 証明書のライフサイクルに対する運用上の要件

4.1 証明書申請

4.1.1 証明書申請者

(1) 相互認証証明書

BCA に対する相互認証証明書の発行申請を行う者は、BCA の定めによるものとする。

(2) 官職証明書

LRA に対する官職証明書の発行申請を行う者は、証明書利用者又は証明書利用者と同一の組織に属する者とする。

IA 及び RA に対する官職証明書の発行申請は、LRA が行う。

(3) 利用者証明書

LRA に対する利用者証明書の発行申請を行う者は、証明書利用者又は証明書利用者と同一の組織に属する者とする。

IA 及び RA に対する利用者証明書の発行申請は、LRA が行う。

(4) 暗号化通信用等証明書

LRA に対する暗号化通信用等証明書の発行申請を行う者は、証明書利用者又は証明書利用者と同一の組織に属する者とする。

IA 及び RA に対する暗号化通信用等証明書の発行申請は、LRA が行う。

4.1.2 登録手続及び責任

(1) 相互認証証明書

IA 及び RA は、BCA に対して正確な情報を申請する。

(2) 官職証明書

証明書申請者は、LRA に対して正確な情報を申請するものとする。

LRA は、所定の手続に基づき審査を実施し、IA 及び RA に対して正確な情報を申請するものとする。

(3) 利用者証明書

証明書申請者は、LRA に対して正確な情報を申請するものとする。

LRA は、所定の手続に基づき審査を実施し、IA 及び RA に対して正確な情報を申請するものとする。

(4) 暗号化通信用等証明書

証明書申請者は、LRA に対して正確な情報を申請するものとする。

LRA は、所定の手続に基づき審査を実施し、IA 及び RA に対して正確な情報を申請するものとする。

4.2 証明書申請手続

(1) 相互認証証明書

BCA に対する相互認証証明書の発行申請は、BCA の定める手続に基づいて行う。

IA 及び RA は、所定の手続に基づき、BCA からの相互認証証明書の発行申請を処理する。

(2) 官職証明書

証明書申請者は、所定の手続に基づき、LRA に対して官職証明書の発行申請を行う。

LRA は、所定の手続に基づき審査を実施し、IA 及び RA に対して官職証明書の発行申請の登録を行う。

IA 及び RA は、所定の手続に基づき LRA から登録された申請内容が適切であることを確認する。

(3) 利用者証明書

証明書申請者は、所定の手続に基づき、LRA に対して利用者証明書の発行申請を行う。

LRA は、所定の手続に基づき審査を実施し、IA 及び RA に対し利用者証明書の発行申請の登録を行う。

IA 及び RA は、所定の手続に基づき LRA から登録された申請内容が適切であることを確認する。

(4) 暗号化通信用等証明書

証明書申請者は、所定の手続に基づき、LRA に対して暗号化通信用等証明書の発行申請を行う。

LRA は、所定の手続に基づき審査を実施し、IA 及び RA に対し暗号化通信用等証明書の発行申請の登録を行う。

IA 及び RA は、所定の手続に基づき LRA から登録された申請内容が適切であることを確認する。

4.3 証明書の発行

(1) 相互認証証明書

IA 及び RA は、BCA の定める手続に基づく接続テスト完了後、BCA から提出された証明書発行要求に対し、自 CA の署名を付して相互認証証明書を発行する。

(2) 官職証明書

IA 及び RA は、IA 及び RA で生成した公開鍵、又は所定の手続で登録された公開鍵に対し、自 CA の署名を付して官職証明書を発行する。

IA 及び RA は、発行した官職証明書を、所定の手続に基づき LRA に配付する。

LRA は、官職証明書を、所定の手続に基づき証明書利用者又は証明書申請者に配付する。発行の通知は、官職証明書の配付によって行う。

(3) 利用者証明書

IA 及び RA は、IA 及び RA で生成した公開鍵に対し、自 CA の署名を付して利用者証明

書を発行する。

IA 及び RA は、発行した利用者証明書を、所定の手続に基づき LRA に配付する。

LRA は、利用者証明書を、所定の手続に基づき証明書利用者又は証明書申請者に配付する。発行の通知は、利用者証明書の配付によって行う。

(4) 暗号化通信用等証明書

IA 及び RA は、登録された公開鍵に対し、自 CA の署名を付して暗号化通信用等証明書を発行する。

IA 及び RA は、発行した暗号化通信用等証明書を、所定の手続に基づき LRA に配付する。

LRA は、暗号化通信用等証明書を、所定の手続に基づき証明書利用者又は証明書申請者に配付する。発行の通知は、暗号化通信用等証明書の配付によって行う。

4.4 証明書の受領

(1) 相互認証証明書

官職 CA は、発行した相互認証証明書を、所定の手続に基づき、BCA に渡し受領書を受け取る。この受領確認をもって相互認証証明書の受入れの完了とする。

(2) 官職証明書

証明書利用者は、遅滞なく証明書の内容を確認し、問題があれば、LRA に申し出るものとする。

LRA は、所定の手続に基づき、証明書利用者からの受領の連絡を確認する。LRA は、証明書利用者からの受領の連絡の確認後、IA 及び RA に対して受領の登録を行うものとする。この受領の確認をもって官職証明書の受入れの完了とする。

なお、証明書利用者で秘密鍵を生成した場合、証明書利用者は、遅滞なく証明書の内容を確認する。証明書利用者は、問題があれば、LRA に申し出るものとする。LRA は、証明書利用者からの申し出がない場合、官職証明書の受入れが完了したものとする。

(3) 利用者証明書

証明書利用者は、遅滞なく証明書の内容を確認し、問題があれば、LRA に申し出るものとする。

LRA は、所定の手続に基づき、証明書利用者からの受領の連絡を確認する。LRA は、証明書利用者からの受領の連絡の確認後、IA 及び RA に対して受領の登録を行うものとする。この受領の確認をもって利用者証明書の受入れの完了とする。

(4) 暗号化通信用等証明書

証明書利用者は、遅滞なく証明書の内容を確認し、問題があれば、LRA に申し出るものとする。

LRA は、証明書利用者からの申し出がない場合、暗号化通信用等証明書の受入れが完了したものとする。

4.5 鍵ペア及び証明書の使用

4.5.1 証明書利用者の秘密鍵及び証明書の使用

証明書利用者は、秘密鍵及び証明書を利用するにあたり、次の義務を負う。

- ・ 官職証明書は、府省等が定める電子署名規程等及び本 CP/CPS に従って、利用・管理する。
- ・ 利用者証明書及び暗号化通信用等証明書は、本 CP/CPS に従って利用する。
- ・ 官職証明書、利用者証明書及び暗号化通信用等証明書並びに証明書に対応する秘密鍵を安全に管理する。
- ・ 秘密鍵が危殆化した場合は、直ちに LRA に報告する。

4.5.2 証明書検証者の公開鍵及び証明書の使用

官職証明書、利用者証明書及び暗号化通信用等証明書の証明書検証者は、公開鍵及び証明書を信頼し利用するにあたり、次の義務を負う。

- ・ 官職証明書、利用者証明書及び暗号化通信用等証明書の利用目的を確認する。
- ・ 官職証明書、利用者証明書及び暗号化通信用等証明書が改ざんされていないことを確認する。
- ・ 官職証明書、利用者証明書及び暗号化通信用等証明書の有効性及び認証パスの有効性について検証する。

4.6 証明書の更新

(1) 相互認証証明書

相互認証証明書の有効期限が近づいた場合等、相互認証証明書の更新を行う場合は、IA 及び RA は、BCA の定める手続に基づき、BCA から提出された証明書発行要求に対し、自 CA の署名を付して新たな相互認証証明書を発行する。

(2) 官職証明書

規定しない。

(3) 利用者証明書

規定しない。

(4) 暗号化通信用等証明書

規定しない。

4.7 鍵更新を伴う証明書の更新

(1) 相互認証証明書

規定しない。

(2) 官職証明書

官職証明書の有効期限が近づいた場合等、官職証明書の更新を行う場合は、対応する秘密鍵を新たに生成することとし、その手続は「4.2 証明書申請手続」及び「4.3 証明書の発行」と同様の手続とする。

(3) 利用者証明書

利用者証明書の有効期限が近づいた場合等、利用者証明書の更新を行う場合は、対応する秘密鍵を新たに生成することとし、その手続は「4.2 証明書申請手続」及び「4.3 証明書の発行」と同様の手続とする。

(4) 暗号化通信用等証明書

暗号化通信用等証明書の有効期限が近づいた場合等、暗号化通信用等証明書の更新を行う場合は、対応する秘密鍵を新たに生成することとし、その手続は「4.2 証明書申請手続」及び「4.3 証明書の発行」と同様の手続とする。

4.8 証明書の変更

(1) 相互認証証明書

相互認証証明書の情報に変更が生じる場合は、IA 及び RA は、BCA の定める手続に基づき、BCA から提出された証明書発行要求に対し、自 CA の署名を付して新たな相互認証証明書を発行する。変更に伴う発行済証明書の失効は、「4.9.3 失効申請手続」と同様とする。

(2) 官職証明書

証明書情報に変更が生じる場合は、「4.2 証明書申請手続」及び「4.3 証明書の発行」と同様の手続により、証明書を発行するものとする。変更に伴う発行済証明書の失効は、「4.9.3 失効申請手続」と同様とする。

(3) 利用者証明書

証明書情報に変更が生じる場合は、「4.2 証明書申請手続」及び「4.3 証明書の発行」と同様の手続により、証明書を発行するものとする。変更に伴う発行済証明書の失効は、「4.9.3 失効申請手続」と同様とする。

(4) 暗号化通信用等証明書

証明書情報に変更が生じる場合は、「4.2 証明書申請手続」及び「4.3 証明書の発行」と同様の手続により、証明書を発行するものとする。変更に伴う発行済証明書の失効は、「4.9.3 失効申請手続」と同様とする。

4.9 証明書の失効と一時停止

4.9.1 証明書失効事由

(1) 相互認証証明書

IA 及び RA は、IA 及び RA 又は BCA に次の相互認証証明書失効事由が発生した場合、

相互認証証明書を失効する。

- ・ CA 秘密鍵の危殆化
- ・ 相互認証基準違反
- ・ 相互認証業務の終了
- ・ 相互認証更新

(2) 官職証明書

官職 CA は、次の官職証明書失効事由が発生した場合、官職証明書を失効する。

- ・ 官職証明書の秘密鍵の紛失、危殆化
- ・ 証明書の再発行
- ・ 証明書記載事項の変更
- ・ CA 秘密鍵の紛失、危殆化
- ・ 官職名の変更、廃止
- ・ 証明書利用者又は LRA による本 CP/CPS に定める義務違反等、連絡会議が必要と判断した場合
- ・ LRA からの要請に基づき、運営責任者が必要と判断した場合
- ・ 官職 CA の責めに帰すべき事由による証明書の誤発行等、運用責任者が必要と判断した場合

(3) 利用者証明書

官職 CA は、次の利用者証明書失効事由が発生した場合、利用者証明書を失効する。

- ・ 利用者証明書の秘密鍵の紛失、危殆化
- ・ 証明書の再発行
- ・ 証明書記載事項の変更
- ・ CA 秘密鍵の紛失、危殆化
- ・ 官職名の変更、廃止
- ・ 証明書利用者又は LRA による本 CP/CPS に定める義務違反等、連絡会議が必要と判断した場合
- ・ LRA からの要請に基づき、運営責任者が必要と判断した場合
- ・ 官職 CA の責めに帰すべき事由による証明書の誤発行等、運用責任者が必要と判断した場合

(4) 暗号化通信用等証明書

官職 CA は、次の暗号化通信用等証明書失効事由が発生した場合、暗号化通信用等証明書を失効する。

- ・ 暗号化通信用等証明書の秘密鍵の紛失、危殆化
- ・ 証明書の再発行
- ・ 証明書記載事項の変更
- ・ CA 秘密鍵の紛失、危殆化

- ・ 証明書の利用停止
- ・ 証明書利用者又は LRA による本 CP/CPS に定める義務違反等、連絡会議が必要と判断した場合
- ・ LRA からの要請に基づき、運営責任者が必要と判断した場合
- ・ 官職 CA の責めに帰すべき事由による証明書の誤発行等、運用責任者が必要と判断した場合

4.9.2 証明書失効の申請者

(1) 相互認証証明書

ア BCA から相互認証証明書失効申請を受ける場合

BCA から官職 CA に対する失効申請は、BCA の責任者が行う。

イ BCA に相互認証証明書失効申請を行う場合

官職 CA から BCA に対する失効申請は、官職 CA の運営責任者が行う。

(2) 官職証明書

LRA に対する官職証明書の失効申請を行う者は、証明書利用者又は証明書利用者と同一の組織に属する者とする。

IA 及び RA に対する官職証明書の失効申請は、LRA が行う。

(3) 利用者証明書

LRA に対する利用者証明書の失効申請を行う者は、証明書利用者又は証明書利用者と同一の組織に属する者とする。

IA 及び RA に対する利用者証明書の失効申請は、LRA が行う。

(4) 暗号化通信用等証明書

LRA に対する暗号化通信用等証明書の失効申請を行う者は、証明書利用者又は証明書利用者と同一の組織に属する者とする。

IA 及び RA に対する暗号化通信用等証明書の失効申請は、LRA が行う。

4.9.3 失効申請手続

(1) 相互認証証明書

ア BCA から相互認証証明書失効申請を受ける場合

「3.2.2 組織の認証」において定める手続を行ったうえで、相互認証証明書を失効し、ARL を統合リポジトリに登録する。

イ BCA に相互認証証明書失効申請を行う場合

BCA との相互認証証明書を失効し、ARL を統合リポジトリに登録する。

(2) 官職証明書

証明書申請者は、所定の手続に基づき、LRA に対し官職証明書の失効申請を行う。

LRA は、所定の手続に基づき審査を実施し、IA 及び RA に対し官職証明書の失効申請の

登録を行う。

IA 及び RA は、LRA からの失効申請に基づき、官職証明書の失効処理を行い、CRL を統合リポジトリに登録する。

LRA は、官職証明書の失効完了を確認し、当該証明書利用者又は証明書失効の申請者に通知する。

(3) 利用者証明書

証明書申請者は、所定の手続に基づき、LRA に対し利用者証明書の失効申請を行う。

LRA は、所定の手続に基づき審査を実施し、IA 及び RA に対し利用者証明書の失効申請の登録を行う。

IA 及び RA は、LRA からの失効申請に基づき、利用者証明書の失効処理を行い、CRL を統合リポジトリに登録する。

LRA は、利用者証明書の失効完了を確認し、当該証明書利用者又は証明書失効の申請者に通知する。

(4) 暗号化通信用等証明書

証明書申請者は、所定の手続に基づき、LRA に対し暗号化通信用等証明書の失効申請を行う。

LRA は、所定の手続に基づき審査を実施し、IA 及び RA に対し暗号化通信用等証明書の失効申請の登録を行う。

IA 及び RA は、LRA からの失効申請に基づき、暗号化通信用等証明書の失効処理を行い、CRL を統合リポジトリに登録する。

LRA は、暗号化通信用等証明書の失効完了を確認し、当該証明書利用者又は証明書失効の申請者に通知する。

4.9.4 失効申請の猶予期間

失効の申請は、失効すべき事象が発生してから速やかに行わなければならない。

4.9.5 認証局が失効申請を処理しなければならない期間

IA 及び RA は、失効申請手続の終了後、直ちに失効処理を行う。

なお、発行した証明書の失効処理に当たっては、その失効処理の取消しは行わない。証明書を失効した証明書利用者に対して再度証明書を発行する場合は、あらためて発行手続を行う。

4.9.6 失効調査の要求

証明書検証者は、CRL/ARL によって証明書の有効性を確認しなければならない。IA 及び RA は、この確認が行えるよう統合リポジトリ上で CRL/ARL を公表する。

4.9.7 CRL/ARL の発行頻度

有効期間 48 時間の CRL/ARL を 24 時間ごとに発行する。ただし、CA 秘密鍵の危殆化等が発生した場合は、CRL/ARL を直ちに発行する。

4.9.8 CRL/ARL の発行最大遅延時間

IA 及び RA は、発行した CRL/ARL を速やかに官職 CA リポジトリ及び統合リポジトリに反映させる。

4.9.9 オンラインでの失効/ステータス確認の可用性

統合リポジトリは、BCA が維持管理する。

4.9.10 オンラインでの失効/ステータス確認を行うための要件

規定しない。

4.9.11 利用可能な失効情報の他の形式

規定しない。

4.9.12 鍵の危殆化に対する特別要件

BCA において CA 秘密鍵の危殆化が発生した場合は、直ちに IA 及び RA に報告する。IA 及び RA は直ちに失効処理を行い、連絡会議に事後報告を行う。

証明書利用者の秘密鍵が危殆化した場合、証明書利用者は、直ちに LRA に報告する。LRA は、直ちに失効申請手続きを行う。IA 及び RA は、LRA からの失効申請に基づき、直ちに失効処理を行う。

4.9.13 証明書の一時停止事由

IA 及び RA は、証明書の一時停止を行わない。

4.9.14 証明書一時停止の申請者

規定しない。

4.9.15 証明書の一時停止申請手続

規定しない。

4.9.16 一時停止を継続できる期間

規定しない。

4.10 証明書のステータス確認サービス
規定しない。

4.11 登録の終了
規定しない。

4.12 秘密鍵の預託と回復
秘密鍵の預託は行わない。

5. 設備上、運営上、運用上の管理

5.1 物理的管理

5.1.1 立地場所及び構造

IA 及び RA の施設は、水害、地震、火災その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震又は免震、耐火及び不正侵入防止のための対策を講ずる。また、使用する機器等を災害及び不正侵入から防護された安全な場所に設置する。

5.1.2 物理的アクセス

IA 及び RA の施設内の各室内において行われる認証業務の重要度に応じ、複数のセキュリティレベルで入退室管理を行う。認証は、操作権限者が識別できる IC カード及び生体認証装置により行う。

各室への入退室権限は、「5.2 手続的管理」において定める各要員の業務に応じて運営責任者が付与する。

IA 及び RA の施設は、監視員を配置して監視システムにより 24 時間 365 日監視を行う。

5.1.3 電源及び空調

IA 及び RA は、機器等の運用のために十分な容量の電源を確保するとともに、瞬断、停電、電圧・周波数の変動に備えた対策を講ずる。商用電源が供給されない事態においては、一定時間内に発電機による電源供給に切り換える。

また、空調設備を設置することにより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

IA 及び RA の設備を設置する建物、室には漏水検知器を設置し、天井、床には防水対策を講ずる。

5.1.5 地震対策

IA 及び RA の設備を設置する建物は耐震構造又は免震構造とし、機器・什器の転倒及び落下を防止する対策を講ずる。

5.1.6 火災防止及び火災保護対策

IA 及び RA の設備を設置する建物は耐火構造、室は防火区画とし、消火設備を備える。

5.1.7 媒体保管

IA 及び RA は、アーカイブデータ、バックアップデータを含む媒体を、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管するとともに、所定の手続に基づき適切に搬入出管理を行う。

5.1.8 廃棄処理

IA 及び RA は、機密情報を含む書類・記憶媒体の廃棄について、所定の手続に基づき適切に廃棄処理を行う。

5.1.9 オフサイトバックアップ

IA 及び RA は、重要なデータ等の媒体を別地保管するに当たって、移送経路のセキュリティを確保するとともに、媒体の保管のための施設に IA 及び RA の施設と同等のセキュリティ対策を講ずる。

5.2 手続的管理

5.2.1 信頼すべき役割

(1) 運営責任者

運営責任者は、官職 CA の運営に関する責任者であり、次の業務を行う。

- ・ 運営方針の策定
- ・ 認証業務の統括
- ・ CA 秘密鍵の危殆化発生時、災害発生時等緊急時における対応の統括
- ・ その他官職 CA の運営に関する統括

(2) IA 鍵管理者

IA 鍵管理者は、CA 秘密鍵を使用する業務に関する責任者であり、次の業務を行う。

なお、操作は複数人の IA 鍵管理者が行う。

- ・ HSM の機能を制御する鍵（以下「管理鍵」という。）の管理
- ・ CA 秘密鍵のバックアップ媒体の管理
- ・ CA 秘密鍵生成、自己署名証明書発行時の HSM に対する操作の立会い
- ・ CA 秘密鍵の更新時における HSM に対する操作の立会い
- ・ CA 秘密鍵のバックアップ、バックアップからのリストア時の HSM に対する管理鍵操作及び CA 秘密鍵バックアップ媒体のセット

(3) 受付担当者

受付担当者は、BCA からの相互認証証明書の発行要求の受付、LRA の加入及び脱退に関

する申請等の受付並びに申請者との連絡調整業務及び申請書類等の管理を行う。

(4) 審査担当者

審査担当者は、LRA の加入及び脱退に関する申請等の審査業務を行う。

(5) 運用責任者

運用責任者は、官職 CA の運用に関する責任者であり、次の業務を行う。

- ・ 上級 IA 操作員、一般 IA 操作員等への作業指示及び作業結果の確認
- ・ CA 秘密鍵の危殆化発生時、災害発生時等緊急時における初期対応の指示
- ・ 官職 CA の運用に関する管理業務
- ・ HSM の操作をする際に必要となる鍵（以下「操作鍵」という。）の管理

(6) 運用責任者補佐

運用責任者補佐は、運用責任者を補佐する役割であり、次の業務を行う。

- ・ 上級 IA 操作員、一般 IA 操作員等への作業指示及び作業結果の確認代行
- ・ 官職 CA の運用に関する管理業務の代行
- ・ HSM の操作鍵の管理代行

(7) 上級 IA 操作員

上級 IA 操作員は、官職 CA のシステムに関する次の業務を行う。なお、操作は複数人の上級 IA 操作員が行う。

- ・ CA 秘密鍵生成、自己署名証明書発行時の HSM に対する操作鍵の操作
- ・ CA 秘密鍵の更新時における HSM に対する操作鍵の操作
- ・ CA 秘密鍵の活性化・非活性化
- ・ 官職 CA システムの起動・停止
- ・ 官職 CA リポジトリの起動・停止
- ・ 官職 CA システムの動作に関する設定変更管理
- ・ 官職 CA システムのデータベースのバックアップに関する諸設定管理並びにバックアップ、リストア及びアーカイブの操作

(8) 一般 IA 操作員

一般 IA 操作員は、官職 CA システムが発行する証明書に関する次の業務を行う。なお、操作は複数人の一般 IA 操作員が行う。

- ・ 証明書ポリシーの設定登録、変更
- ・ 相互認証証明書等の発行、更新及び失効処理
- ・ 官職証明書及び利用者証明書にかかる秘密鍵の生成及びその証明書の発行、更新及び失

効処理

- ・ 操作員への証明書の発行、更新及び失効処理
- ・ 官職 CA リポジトリの設定管理

(9) 監査ログ検査者

監査ログ検査者は、官職 CA システム及び官職 CA リポジトリにおけるセキュリティに関する重要な事象を記録したログ（以下「監査ログ」という。）に関する次の業務を行う。

- ・ 監査ログの検査
- ・ 不要な監査ログの削除

(10)LRA 管理者

LRA 管理者は LRA の運営に関する責任者であり、次の業務を行う。

- ・ LRA の要員の指名、指名の解除
- ・ 作業計画の立案及び LRA 要員への作業指示
- ・ 官職証明書、利用者証明書及び暗号化通信用等証明書の発行、更新及び失効申請の審査結果に対する最終承認
- ・ 官職証明書、利用者証明書及び暗号化通信用等証明書の発行、更新及び失効申請の審査業務の統括
- ・ 申請書類等の管理
- ・ LRA の内部点検の実施
- ・ 運営責任者への内部点検結果等の報告

(11)LRA 操作員

LRA 管理者の指示に基づき、IA 及び RA へ官職証明書、利用者証明書及び暗号化通信用等証明書の発行、更新及び失効申請の登録を行う。

(12)LRA 受付担当者

官職証明書、利用者証明書及び暗号化通信用等証明書の発行、更新及び失効申請の受付、付随する事務手続や連絡業務を行う。

(13)LRA 審査担当者

官職証明書、利用者証明書及び暗号化通信用等証明書の発行、更新及び失効申請の審査業務を行う。

5.2.2 職務ごとに必要とされる人数

IA 及び RA は、CA 秘密鍵の生成及び自己署名証明書の発行、並びに相互認証証明書の

発行、更新、失効等の重要な業務について複数名の要員で行う。

5.2.3 個々の役割に対する本人性確認と認証

操作員がシステム操作を行う際、システムは、操作員が正当な権限者であることの識別・認証を行う。

5.2.4 職務分割が必要となる役割

重要な業務の指示は、運営責任者から運用責任者に対して行う。

運用責任者は、各要員に対して業務の指示を行う。

重要な業務の実施に当たっては、要員の職務権限を分離し、相互牽制を行う。

LRA における業務の指示は、LRA 管理者が LRA の各要員に対して行う。

5.3 人事的管理

官職 CA の要員の適格性の審査、教育、配置転換、罰則等については、国家公務員法等人事関係法令に基づいて運用する。また、すべての要員には、官職 CA の運営を行うために必要な知識及び技術を習得するための教育訓練を行う。なお、業務の一部を委託する場合は、委託先との間で委託業務に関する機密保持義務等を含む適切な契約を締結する。

5.4 監査ログの手続

監査ログ検査者は、監査ログを業務実施記録等と照合し、不正操作等異常な事象を確認するセキュリティ監査を行う。

5.4.1 記録されるイベントの種類

官職 CA システム及び官職 CA リポジトリにおけるセキュリティに関する重要な事象を対象に、アクセスログ、操作ログ等監査ログを記録する。監査ログには、次の情報を含める。

- ・ 事象の種類
- ・ 事象が発生した日付及び時刻
- ・ 各種処理の結果
- ・ 事象の発生元の識別情報（操作員名、システム名等）

5.4.2 監査ログを処理する頻度

監査ログ検査者は、業務実施記録等と監査ログとの照合を週次で行う。

5.4.3 監査ログの保管期間

監査ログは、3年間保管する。

5.4.4 監査ログの保護

監査ログには、アクセス制御を施すとともに、改ざん検出を可能とする措置を講ずる。

監査ログのバックアップは、週次で外部記憶媒体に取得し、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管する。

なお、監査ログの閲覧及び削除は監査ログ検査者が行う。

5.4.5 監査ログのバックアップ手続

監査ログは日次でバックアップし、週次で外部記憶媒体に取得する。

5.4.6 監査ログの収集システム

監査ログの収集機能は官職 CA のシステムの一機能とし、セキュリティに関する重要な事象をシステムの起動時から監査ログとして収集する。

5.4.7 イベントを起こした者への通知

監査ログの検査は、事象を発生させた者に通知することなく行う。

5.4.8 脆弱性評価

監査ログを検査することにより、運用面及びシステム面におけるセキュリティ上の脆弱性を評価する。

5.5 記録の保管

5.5.1 アーカイブの種類

アーカイブデータは、次のものとする。

- ・ 証明書の発行履歴
- ・ CRL/ARL の発行履歴
- ・ 起動停止ログ
- ・ 操作ログ

5.5.2 アーカイブ保管期間

アーカイブデータは、該当する証明書の有効期間満了後 10 年間保管する。

5.5.3 アーカイブの保護

アーカイブデータには、アクセス制御を施すとともに、改ざん検出を可能とする措置を講ずる。

5.5.4 アーカイブのバックアップ手続

アーカイブデータは日次でバックアップし、月次で外部記憶媒体に取得する。

5.5.5 記録にタイムスタンプを付与する要件

アーカイブデータには、レコード単位でタイムスタンプを付与する。

5.5.6 アーカイブ収集システム

規定しない。

5.5.7 アーカイブの検証手続

アーカイブデータが記録された外部記憶媒体の可読性の確認を、年1回行う。

5.6 鍵の切り替え

有効とする日から起算して5年ごとにCA鍵ペアの更新を行う。

CA鍵ペア更新時には、古いCA公開鍵と新しいCA公開鍵の認証パスを構築するリンク証明書を発行し、統合リポジトリ上で公表する。新しいCA公開鍵を配付する方法は、「6.1.4 証明書検証者へのCA公開鍵の配付」と同様とする。

5.7 危殆化及び災害からの復旧

5.7.1 事故及び危殆化時の手続

IA及びRAは、事故及び危殆化が発生した場合に速やかに業務を復旧できるよう、以下を含む事故及び危殆化に対する対応手続を策定する。

- ・ ハードウェア、ソフトウェア、データ等の破損、故障
- ・ CA秘密鍵の危殆化
- ・ 火災、地震等の災害

5.7.2 ハードウェア、ソフトウェア又はデータが破壊された場合の手続

ハードウェア、ソフトウェア又はデータが破壊された場合、バックアップ用のハードウェア、ソフトウェア又はデータにより、速やかに復旧作業を行う。なお、復旧に必要なソフトウェア及びデータは、定期的又は必要に応じて取得する。

5.7.3 エンティティの秘密鍵が危殆化した場合の手続

CA秘密鍵が危殆化した場合は、所定の手続に基づき認証業務を停止し、次の手続を行う。

- ・ 危殆化に関する情報の公表
- ・ 相互認証証明書、官職証明書、利用者証明書及び暗号化通信用等証明書の失効手続

- ・ CA 秘密鍵の廃棄及び再生成手続
- ・ 相互認証証明書、官職証明書、利用者証明書及び暗号化通信用等証明書の再発行手続
また、相互認証先 CA の CA 秘密鍵及び証明書利用者の秘密鍵が危殆化した場合は、「4.9 証明書の失効と一時停止」において定める手続に基づき、証明書の失効手続を行う。

5.7.4 災害後の事業継続性

災害等により IA 及び RA の設備が被害を受けた場合は、バックアップサイトにおいてバックアップデータを用いて運用を行う。バックアップサイトは、メインサイトから適切な距離の場所に設置する。災害時の業務方針を以下に定める。

- ・ 統合リポジトリによる CRL/ARL の公表を最優先として、公表停止から 48 時間以内に公表を再開する。
- ・ 緊急を要する証明書発行及び失効業務は、業務停止より 96 時間以内に再開する。
- ・ 通常業務は、メインサイトの IA 及び RA の設備並びにセキュリティが完全に復旧されたことを確認後に再開する。

5.8 認証業務の終了

連絡会議において官職 CA の認証業務の終了が決定した場合、IA 及び RA は、業務終了の事実、並びに業務終了後の官職 CA のバックアップデータ、アーカイブデータ等の保管組織及び開示方法を業務終了 90 日前までに相互認証先 CA、LRA、証明書利用者及び証明書検証者に告知し、所定の業務終了手続を行う。

6. 技術的セキュリティ管理

6.1 鍵ペアの生成及びインストール

6.1.1 鍵ペアの生成

(1) CA 鍵

CA 鍵ペアは、複数人の IA 鍵管理者立会いのもと、複数人の上級 IA 操作員が FIPS140-2 レベル 3 認定を受けた HSM を用いて生成する。

(2) 官職証明書鍵

IA 及び RA で生成する官職証明書の鍵ペアは、複数人の一般 IA 操作員が安全な環境下において生成する。また、官職証明書の鍵ペアは、証明書利用者においても生成可能とする。

(3) 利用者証明書鍵

IA 及び RA で生成する利用者証明書の鍵ペアは、複数の一般 IA 操作員が安全な環境下で生成する。

(4) 暗号化通信用等証明書

暗号化通信用等証明書の鍵ペアは、証明書利用者が生成する。

6.1.2 証明書利用者に対する秘密鍵の配付

IA 及び RA で生成する官職証明書及び利用者証明書の秘密鍵は、「6.2.1 暗号モジュールの標準及び管理」において定める暗号モジュールに格納し、所定の手続に基づき配付する。

6.1.3 CA への公開鍵の配付

(1) 相互認証証明書

IA 及び RA は、相互認証証明書の取り交わしにおいて、BCA の公開鍵を安全かつ確実に受取る。

(2) 官職証明書

IA 及び RA において証明書利用者の鍵ペアを生成する。

証明書利用者が鍵ペアを生成する場合は、証明書利用者が LRA に安全な方法で送付するものとし、LRA が安全な方法で、IA 及び RA へ送付する。

(3) 利用者証明書

IA 及び RA において証明書利用者の鍵ペアを生成する。

(4) 暗号化通信用等証明書

証明書利用者が LRA に安全な方法で送付するものとし、LRA が安全な方法で、IA 及び RA へ送付する。

6.1.4 証明書検証者への CA 公開鍵の配付

IA 及び RA は、自己署名証明書を統合リポジトリにより公表し、そのフィンガープリントを Web により公表する。Web によるフィンガープリントの公表は、安全な方法により行う。

6.1.5 鍵のサイズ

(1) CA 鍵

RSA2048 ビットの鍵を使用する。

(2) 官職証明書鍵

RSA2048 ビットの鍵を使用する。(sha256WithRSAEncryption)

(3) 利用者証明書鍵

RSA2048 ビットの鍵を使用する。(sha256WithRSAEncryption)

(4) 暗号化通信用等証明書

RSA2048 ビットの鍵を使用する。(sha256WithRSAEncryption)

6.1.6 公開鍵パラメータの生成及び品質検査

規定しない。

6.1.7 鍵の用途

以下に定める利用目的以外には、鍵を利用しないものとする。

(1) CA 鍵

CA 秘密鍵は、署名に用いる。

(2) 官職証明書鍵

官職証明書の秘密鍵は、署名に用いる。

(3) 利用者証明書鍵

利用者証明書の秘密鍵は、認証及び暗号に用いる。

(4) 暗号化通信用等証明書

暗号化通信用等証明書の秘密鍵は、署名及び暗号に用いる。

6.2 秘密鍵の保護及び暗号モジュール技術の管理

6.2.1 暗号モジュールの標準及び管理

(1) CA 鍵

CA 秘密鍵は、FIPS140-2 レベル 3 の認定を受けた HSM により保護する。

(2) 官職証明書鍵

官職証明書の秘密鍵は、耐タンパ性を持つ暗号モジュールにより保護する。

(3) 利用者証明書鍵

利用者証明書の秘密鍵は、耐タンパ性を持つ暗号モジュールにより保護する。

(4) 暗号化通信用等証明書

規定しない。

6.2.2 秘密鍵の複数人管理

CA 秘密鍵の管理に関する操作は、複数人の IA 鍵管理者及び複数人の上級 IA 操作員が行う。

6.2.3 秘密鍵の預託

CA 秘密鍵の預託は行わない。

6.2.4 秘密鍵のバックアップ

CA 秘密鍵のバックアップは、複数人の IA 鍵管理者及び複数人の上級 IA 操作員が行う。

HSM からバックアップした CA 秘密鍵は、複数人の IA 鍵管理者によって安全に保管する。

6.2.5 秘密鍵のアーカイブ

CA 秘密鍵のアーカイブは行わない。

6.2.6 秘密鍵の暗号モジュールへの又は暗号モジュールからの転送

規定しない。

6.2.7 暗号モジュールへの秘密鍵の格納

(1) CA 鍵

CA 秘密鍵は、複数人の IA 鍵管理者及び複数人の上級 IA 操作員が HSM の中で生成し、格納する。

(2) 官職証明書鍵

IA 及び RA で生成する官職証明書の秘密鍵は、複数人の一般 IA 操作員が安全な環境下において生成し、暗号モジュール内に格納する。

証明書利用者で秘密鍵を生成する場合は、安全な環境下で生成し暗号モジュール内に格納するものとする。

(3) 利用者証明書鍵

IA 及び RA で生成する利用者証明書の秘密鍵は、複数人の一般 IA 操作員が安全な環境下において生成し、暗号モジュール内に格納する。

(4) 暗号化通信用等証明書

規定しない。

6.2.8 秘密鍵の活性化方法

(1) CA 鍵

CA 秘密鍵は、複数人の上級 IA 操作員により操作鍵及びパスワードを用いて活性化する。

(2) 官職証明書鍵

官職証明書の秘密鍵は、証明書利用者により PIN を用いて活性化する。

(3) 利用者証明書鍵

利用者証明書の秘密鍵は、証明書利用者により PIN を用いて活性化する。

(4) 暗号化通信用等証明書

規定しない。

6.2.9 秘密鍵の非活性化方法

(1) CA 鍵

CA 秘密鍵は、複数人の上級 IA 操作員によりパスワードを用いて非活性化する。

(2) 官職証明書鍵

官職証明書の秘密鍵は、証明書利用者によりログアウト又は暗号モジュールの取り外し等によって非活性化する。

(3) 利用者証明書鍵

利用者証明書の秘密鍵は、証明書利用者によりログアウト又は暗号モジュールの取り外し等によって非活性化する。

(4) 暗号化通信用等証明書

規定しない。

6.2.10 秘密鍵の破棄方法

(1) CA 鍵

HSM 内の CA 秘密鍵は、複数人の IA 鍵管理者及び複数人の上級 IA 操作員が HSM の機能を用いて消去する。また、CA 秘密鍵のバックアップ媒体を破棄する場合も同様とする。

(2) 官職証明書鍵

官職証明書の秘密鍵の破棄は、所定の手続に基づき破棄する。

(3) 利用者証明書鍵

利用者証明書の秘密鍵の破棄は、所定の手続に基づき破棄する。

(4) 暗号化通信用等証明書

規定しない。

6.2.11 暗号モジュールの評価

「6.1.1 鍵ペアの生成」及び「6.2.1 暗号モジュールの標準及び管理」において定める。

6.3 鍵ペアのその他の管理方法

6.3.1 公開鍵のアーカイブ

公開鍵は証明書のアーカイブに含まれ、「5.5.2 アーカイブ保管期間」において定める期間、保管する。

6.3.2 秘密鍵及び公開鍵の有効期間

(1) CA 鍵

官職 CA の公開鍵と秘密鍵の有効期間は、有効とする日から起算して 10 年とし、5 年ごとに鍵更新を行う。

ただし、暗号のセキュリティが脆弱になったと判断した場合は、その時点で鍵更新を行う場合がある。

(2) 官職証明書鍵

官職証明書 (sha256WithRSAEncryption) の公開鍵と秘密鍵の有効期間は、証明書を有効とする日から起算して 5 年とする。

ただし、暗号のセキュリティが脆弱になったと判断した場合は、その時点で鍵更新を行う場合がある。

(3) 利用者証明書鍵

利用者証明書 (sha256WithRSAEncryption) の公開鍵と秘密鍵の有効期間は、証明書を有効とする日から起算して 5 年とする。

ただし、暗号のセキュリティが脆弱になったと判断した場合は、その時点で鍵更新を行う場合がある。

(4) 暗号化通信用等証明書

暗号化通信用等証明書の公開鍵と秘密鍵の有効期間は、証明書を有効とする日から起算して 5 年とする。

ただし、暗号のセキュリティが脆弱になったと判断した場合は、その時点で鍵更新を行う場合がある。

6.4 活性化データ

6.4.1 活性化データの生成及び設定

(1) CA 鍵

CA 秘密鍵を格納する HSM の活性化に必要な操作鍵とパスワードは、複数人の IA 鍵管

理者及び複数人の上級 IA 操作員が生成し、設定する。

(2) 官職証明書鍵

官職 CA が生成した官職証明書の秘密鍵を格納する暗号モジュールの初期 PIN は、官職 CA が生成し、設定する。

証明書利用者が生成した証明書利用者の秘密鍵を格納する暗号モジュールの初期 PIN は、証明書利用者が生成し、設定する。

(3) 利用者証明書鍵

官職 CA が生成した利用者証明書の秘密鍵を格納する暗号モジュールの初期 PIN は、官職 CA が生成し、設定する。

(4) 暗号化通信用等証明書

暗号化通信用等証明書の秘密鍵の活性化データは、証明書利用者が生成し、設定する。

6.4.2 活性化データの保護

(1) CA 鍵

IA 及び RA は、CA 秘密鍵を格納する HSM の活性化に必要なパスワード及び操作鍵を安全に保管する。

(2) 官職証明書鍵

官職証明書の秘密鍵の活性化に必要な PIN は、証明書利用者自身で定期的に変更し、安全に保管するものとする。

(3) 利用者証明書鍵

利用者証明書の秘密鍵の活性化に必要な PIN は、証明書利用者自身で定期的に変更し、安全に保管するものとする。

(4) 暗号化通信用等証明書

暗号化通信用等証明書の秘密鍵の活性化データは、証明書利用者が安全に保管するものとする。

6.4.3 活性化データの他の考慮点

規定しない。

6.5 コンピュータのセキュリティ管理

6.5.1 コンピュータセキュリティに関する技術的要件

官職 CA のシステムには、アクセス制御機能、操作員の識別と認証機能、データベースセキュリティのための暗号化機能、監査ログ及びアーカイブデータの収集機能、CA 鍵及びシステムのリカバリ機能等を備える。

6.5.2 コンピュータセキュリティ評価

規定しない。

6.6 ライフサイクルセキュリティ管理

6.6.1 システム開発管理

官職 CA のシステム開発、修正又は変更に当たっては、所定の手続に基づき、信頼できる組織及び環境下において作業を実施する。開発、修正又は変更したシステムは、テスト環境において検証を行い、運営責任者の承認を得たうえで導入する。また、システム仕様及び検証報告については、文書化し保管する。

6.6.2 セキュリティ運用管理

官職 CA のシステムを維持管理するため、OS 及びソフトウェアのセキュリティチェックを定期的に行う。また、この検証結果を文書化し保管する。また、適宜ウイルス対策及び不正プログラム対策を行う。

6.6.3 ライフサイクルセキュリティ管理

IA 及び RA は、官職 CA のシステム開発、運用、保守が適切に行われていることを監査等を通じて適時評価し、必要に応じ改善を行う。

6.7 ネットワークセキュリティ管理

官職 CA リポジトリに保有する情報のうち公表する情報は、ファイアウォールを介して BCA の統合リポジトリに複製する。LRA との間は、専用線経由の暗号化通信のみとする。また、不正侵入検知等十分なセキュリティ保護対策を行う。

6.8 タイムスタンプ

IA 及び RA は、信頼される時刻源を使用してシステムの時刻同期を行い、システム内で記録される重要な情報に対しレコード単位でタイムスタンプを付与する。

7. 証明書、証明書失効リストのプロファイル

7.1 証明書プロファイル

自己署名証明書、リンク証明書、相互認証証明書、官職証明書、利用者証明書及び暗号化通信用等証明書のプロファイルは、相互運用性仕様書に定める。

7.2 CRL/ARL プロファイル

CRL/ARL のプロファイルは、相互運用性仕様書に定める。

8. 準拠性監査と他の評価

IA 及び RA は、IA 及び RA の業務に関し、「8.1 監査の頻度」から「8.6 監査結果の開示」に規定するとおり監査を実施する。また、IA 及び RA は、LRA に対し、監査を実施する権利を有する。

8.1 監査の頻度

IA 及び RA は、監査人による監査を年 1 回定期的実施する。また、IA 及び RA は、必要に応じて定期監査以外に監査を実施する。

8.2 監査者の身元／資格

IA 及び RA の監査は、監査業務及び認証業務に精通した者が行う。

8.3 監査者と被監査者の関係

IA 及び RA の監査を実施する監査人は、官職 CA と利害関係を有しない者を選定する。

8.4 監査で扱われる事項

IA 及び RA の業務が本 CP/CPS 及び運用マニュアルに準拠して実施されていることの監査を実施する。

8.5 不備の結果としてとられる処置

IA 及び RA は、重要又は緊急を要する監査指摘事項について、連絡会議の決定に基づき速やかに対応する。CA 秘密鍵の危殆化に関する指摘があった場合は緊急事態と位置付け、緊急時対応の手続をとる。重要又は緊急を要する監査指摘事項が改善されるまでの間、官職 CA の運用を停止するか否かは連絡会議が決定する。また、連絡会議は、監査指摘事項に対して IA 及び RA が対策を実施したことを確認する。

8.6 監査結果の開示

監査結果は、監査人から IA 及び RA に対して監査報告書として提出される。運営責任者は、連絡会議及び BCA に監査結果を報告する。

監査報告書は、5 年間保管する。

9. 他の業務上及び法的事項

9.1 料金

規定しない。

9.2 財務的責任

規定しない。

9.3 情報の機密性

9.3.1 機密情報の範囲

官職 CA は、漏えいすることによって官職 CA 及び BCA の認証業務の信頼性が損なわれる恐れのある情報を機密扱いとする。

9.3.2 機密情報の範囲外の情報

官職 CA が保有する情報のうち、証明書、失効情報、本 CP/CPS 等、公表する情報として明示的に示すものは機密扱いとしない。

9.3.3 機密情報を保護する責任

機密情報は、「行政機関の保有する個人情報の保護に関する法律」(平成 15 年法律第 58 号)及び「行政機関の保有する個人情報の保護に関する法律施行令」(平成 15 年政令第 548 号)等に従い、当該情報を含む書類及び記憶媒体の管理責任者を定め、安全に管理する。

官職 CA は、法的根拠に基づいて法律執行機関から情報を開示するように正式に要求があった場合、司法手続若しくは行政手続に基づく要求があった場合、又は証明書利用者が官職 CA に提示した情報について当該証明書利用者から開示要求が行われた場合は、機密情報を開示する。

9.4 個人情報の保護

「行政機関の保有する個人情報の保護に関する法律」及び「行政機関の保有する個人情報の保護に関する法律施行令」等に従い、適切に保護する。

9.5 知的財産権

CA 鍵ペア、官職証明書、利用者証明書、暗号化通信用等証明書、相互認証証明書、CRL/ARL、自己署名証明書、リンク証明書及び本 CP/CPS の知的財産権は、官職 CA に帰属するものとする。

ただし、官職証明書、利用者証明書及び暗号化通信用等証明書の鍵ペア及び主体者名の知

的財産権は、その限りではない。

9.6 表明保証

9.6.1 IA 及び RA の表明保証

IA 及び RA は、認証業務に関して次の内容を表明し、保証する。

- ・ BCA への相互認証申請に際して、正確な情報を提示すること
- ・ 本 CP/CPS に基づき、自己署名証明書、リンク証明書、相互認証証明書、官職証明書、利用者証明書及び暗号化通信用等証明書を発行、更新、失効すること
- ・ 相互認証証明書の取り交わしに関しては、BCA の定めた手続に従うこと
- ・ 「2.2 証明情報の公表」に定める情報を公表すること
- ・ 有効期間 48 時間の CRL/ARL を 24 時間ごとに発行すること
- ・ CA 秘密鍵を安全に管理すること
- ・ CA 秘密鍵が危殆化した場合は、速やかに BCA に報告すること並びに危殆化に関する情報を公表すること
- ・ 証明書の発行、更新、失効等に関する監査ログ及びアーカイブを必要な期間保管すること
- ・ システムの稼動監視を行うこと
- ・ 官職 CA は、BCA からの相互認証証明書発行要求に含まれる公開鍵が確実に BCA の公開鍵であり、かつ BCA がこの公開鍵に対応する秘密鍵を保有していることを確認すること
- ・ LRA の審査を適切に行うこと
- ・ LRA から証明書の発行、更新及び失効等を受け付ける際に、LRA の真偽を確認すること
- ・ 次を含む LRA の基準及び手続を定めること
 - LRA が行う証明書申請審査業務に係る基準及び手続
 - LRA において実施すべきセキュリティ対策に係る基準及び手続
 - LRA において取得すべきログに係る基準及び手続
- ・ LRA における上記基準及び手続の遵守状況を把握すること

9.6.2 LRA の表明保証

LRA は、LRA の業務に関して次の内容を表明し、保証する。

- ・ 証明書利用者からの証明書の発行、更新及び失効申請に際して、受付、証明書利用者の真偽の確認及び申請内容の確認を確実にすること
- ・ IA 及び RA に対して、LRA システムを使用して安全に証明書の発行、更新及び失効申請を行うこと

- ・ 証明書利用者に対して、証明書の発行完了及び失効完了を通知すること
- ・ 各申請手続において入手した証明書利用者情報を安全に保管すること
- ・ IA 及び RA が定める LRA の基準及び手続を遵守すること
- ・ IA 及び RA に対して、LRA における上記基準及び手続の遵守状況を報告すること

9.6.3 証明書利用者の表明保証

証明書利用者は、「4.5.1 証明書利用者の秘密鍵及び証明書の使用」に定める内容及び以下に定める内容を遵守することについて表明し、保証する。

- ・ LRA に対し、証明書を発行、失効するための正確な情報を申請すること
- ・ 証明書を受領する時点で、証明書の情報が正しいことを確認すること
- ・ 証明書の記載事項が変更となる場合は、速やかに LRA に申請すること

9.6.4 証明書検証者の表明保証

証明書検証者は、「4.5.2 証明書検証者の公開鍵及び証明書の使用」に定める内容を遵守することについて表明し、保証する。

9.6.5 他の関係者の表明保証

規定しない。

9.7 無保証

規定しない。

9.8 責任の制限

規定しない。

9.9 補償

規定しない。

9.10 有効期間と終了

9.10.1 有効期間

本 CP/CPS は、連絡会議の承認により有効となる。

「9.10.2 終了」に規定する終了以前に本 CP/CPS が無効となることはない。

9.10.2 終了

本 CP/CPS は、「9.10.3 終了の効果と効果継続」に規定する内容を除き官職 CA を終了し

た時点で無効となる。

9.10.3 終了の効果と効果継続

証明書利用者が証明書の利用を終了する場合、又は官職 CA の業務を終了する場合であっても、「9.3 情報の機密性」、「9.4 個人情報の保護」、「9.5 知的財産権」及び「9.14 準拠法」の条項は終了の事由を問わず証明書利用者、証明書検証者及び官職 CA に適用されるものとする。

9.11 関係者間の個別通知と連絡

本 CP/CPS 上必要とされ、又は許容される官職 CA に対する通知、請求、要求、依頼その他の連絡はデジタル庁を窓口とする。連絡先は「1.5.2 連絡先」に規定する。

9.12 改定

9.12.1 改定手続

連絡会議は、本 CP/CPS を必要に応じて変更する。

9.12.2 通知方法及び期間

連絡会議は、本 CP/CPS を変更した場合、速やかに変更した CP/CPS を公表する。これをもって証明書利用者及び証明書検証者への通知とする。

9.12.3 オブジェクト識別子を変更されなければならない場合

規定しない。

9.13 紛争解決手続

規定しない。

9.14 準拠法

本 CP/CPS に基づく認証業務から生ずる紛争については、日本国の法令を適用する。

9.15 適用法の遵守

規定しない。

9.16 雑則

規定しない。

9.17 その他の条項

規定しない。