

政府認証基盤（GPKI）

アプリケーション認証局 CP/CPS

平成 19 年 7 月 6 日

平成 21 年 5 月 25 日改定

行政情報システム関係課長連絡会議了承

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 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.....	3
1.5 ポリシ管理.....	3
1.5.1 文書を管理する組織.....	3
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.....	12
2.1 リポジトリ.....	12
2.2 証明情報の公表.....	12
2.3 公表の時期又は頻度.....	12
2.4 リポジトリへのアクセス管理.....	12
3. 識別と認証.....	13
3.1 名前決定.....	13
3.1.1 名前の種類.....	13
3.1.2 名前が意味を持つことの必要性.....	13
3.1.3 証明書利用者の匿名性又は仮名性.....	13
3.1.4 様々な名前形式を解釈するための規則.....	13
3.1.5 名前の一意性.....	13
3.1.6 認識、認証及び商標の役割.....	13
3.2 初回の識別と認証.....	13
3.2.1 秘密鍵の所持を証明する方法.....	13
3.2.2 組織の認証.....	14

3.2.3	個人の認証	14
3.2.4	検証されない証明書利用者の情報	14
3.2.5	権限の正当性確認	14
3.2.6	相互運用の基準	14
3.3	更新申請時の識別と認証	14
3.3.1	通常の更新時における識別と認証	14
3.3.2	証明書失効後の更新時における識別と認証	14
3.4	失効申請時の識別と認証	14
4.	証明書のライフサイクルに対する運用上の要件	15
4.1	証明書申請	15
4.1.1	証明書申請者	15
4.1.2	登録手続及び責任	15
4.2	証明書申請手続	15
4.3	証明書の発行	16
4.4	証明書の受領	16
4.5	鍵ペア及び証明書の使用	16
4.5.1	証明書利用者の秘密鍵及び証明書の使用	17
4.5.2	証明書検証者の公開鍵及び証明書の使用	17
4.6	証明書の更新	17
4.7	鍵更新を伴う証明書の更新	17
4.8	証明書の変更	17
4.9	証明書の失効と一時停止	18
4.9.1	証明書失効事由	18
4.9.2	証明書失効の申請者	18
4.9.3	失効申請手続	19
4.9.4	失効申請の猶予期間	19
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	19
4.9.6	失効調査の要求	19
4.9.7	CRLの発行頻度	20
4.9.8	CRLの発行最大遅延時間	20
4.9.9	オンラインでの失効/ステータス確認の可用性	20
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	20
4.9.11	利用可能な失効情報の他の形式	20
4.9.12	鍵の危殆化に対する特別要件	20
4.9.13	証明書の一時的停止事由	20
4.9.14	証明書の一時的停止の申請者	20

4.9.15	証明書の一時停止申請手続	20
4.9.16	一時停止を継続できる期間	20
4.10	証明書のステータス確認サービス	21
4.11	登録の終了	21
4.12	秘密鍵の預託と回復	21
5.	設備上、運営上、運用上の管理	22
5.1	物理的管理	22
5.1.1	立地場所及び構造	22
5.1.2	物理的アクセス	22
5.1.3	電源及び空調	22
5.1.4	水害対策	22
5.1.5	地震対策	22
5.1.6	火災防止及び火災保護対策	22
5.1.7	媒体保管	23
5.1.8	廃棄処理	23
5.1.9	オフサイトバックアップ	23
5.2	手続的管理	23
5.2.1	信頼すべき役割	23
5.2.2	職務ごとに必要とされる人数	25
5.2.3	個々の役割に対する識別と認証	26
5.2.4	職務分割が必要となる役割	26
5.3	人事的管理	26
5.4	監査ログの手続	26
5.4.1	記録されるイベントの種類	26
5.4.2	監査ログを処理する頻度	26
5.4.3	監査ログの保管期間	26
5.4.4	監査ログの保護	27
5.4.5	監査ログのバックアップ手続	27
5.4.6	監査ログの収集システム	27
5.4.7	イベントを起こした者への通知	27
5.4.8	脆弱性評価	27
5.5	記録の保管	27
5.5.1	アーカイブの種類	27
5.5.2	アーカイブ保管期間	27
5.5.3	アーカイブの保護	27
5.5.4	アーカイブのバックアップ手続	28

5.5.5	記録にタイムスタンプを付与する要件	28
5.5.6	アーカイブ収集システム	28
5.5.7	アーカイブの検証手続	28
5.6	鍵の切り替え	28
5.7	危殆化及び災害からの復旧	28
5.7.1	事故及び危殆化時の手続	28
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	28
5.7.3	エンティティの秘密鍵が危殆化した場合の手続	28
5.7.4	災害後の事業継続性	29
5.8	認証業務の終了	29
6.	技術的セキュリティ管理	30
6.1	鍵ペアの生成及びインストール	30
6.1.1	鍵ペアの生成	30
6.1.2	証明書利用者に対する秘密鍵の配付	30
6.1.3	認証局への公開鍵の配付	30
6.1.4	証明書検証者への CA 公開鍵の配付	30
6.1.5	鍵のサイズ	30
6.1.6	公開鍵パラメータの生成及び品質検査	30
6.1.7	鍵の用途	31
6.2	秘密鍵の保護及び暗号モジュール技術の管理	31
6.2.1	暗号モジュールの標準及び管理	31
6.2.2	秘密鍵の複数人管理	31
6.2.3	秘密鍵の預託	31
6.2.4	秘密鍵のバックアップ	31
6.2.5	秘密鍵のアーカイブ	31
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	32
6.2.7	暗号モジュールへの秘密鍵の格納	32
6.2.8	秘密鍵の活性化方法	32
6.2.9	秘密鍵の非活性化方法	32
6.2.10	秘密鍵の破棄方法	32
6.2.11	暗号モジュールの評価	33
6.3	鍵ペアのその他の管理方法	33
6.3.1	公開鍵のアーカイブ	33
6.3.2	秘密鍵及び公開鍵の有効期間	33
6.4	活性化データ	33
6.4.1	活性化データの生成及び設定	33

6.4.2 活性化データの保護.....	34
6.4.3 活性化データの他の考慮点.....	34
6.5 コンピュータのセキュリティ管理.....	34
6.5.1 コンピュータセキュリティに関する技術的要件.....	34
6.5.2 コンピュータセキュリティ評価.....	34
6.6 ライフサイクルセキュリティ管理.....	34
6.6.1 システム開発管理.....	34
6.6.2 セキュリティ運用管理.....	34
6.6.3 ライフサイクルセキュリティ管理.....	35
6.7 ネットワークセキュリティ管理.....	35
6.8 タイムスタンプ.....	35
7. 証明書、証明書失効リストのプロファイル.....	36
7.1 自己署名証明書.....	36
7.2 サーバ証明書.....	37
7.3 コード署名証明書.....	40
7.4 CRL.....	42
8. 準拠性監査と他の評価.....	44
8.1 監査の頻度.....	44
8.2 監査者の身元／資格.....	44
8.3 監査者と被監査者の関係.....	44
8.4 監査で扱われる事項.....	44
8.5 不備の結果としてとられる処置.....	44
8.6 監査結果の開示.....	44
9. 他の業務上及び法的事項.....	45
9.1 料金.....	45
9.2 財務的責任.....	45
9.3 情報の機密性.....	45
9.3.1 機密情報の範囲.....	45
9.3.2 機密情報の範囲外の情報.....	45
9.3.3 機密情報を保護する責任.....	45
9.4 個人情報の保護.....	45
9.5 知的財産権.....	45
9.6 表明保証.....	46
9.6.1 IA 及び RA の表明保証.....	46
9.6.2 LRA の表明保証.....	46
9.6.3 証明書利用者の表明保証.....	47

9.6.4 証明書検証者の表明保証 .....	47
9.6.5 他の関係者の表明保証 .....	47
9.7 無保証.....	47
9.8 責任の制限 .....	47
9.9 補償 .....	47
9.10 有効期間と終了 .....	47
9.10.1 有効期間 .....	47
9.10.2 終了.....	47
9.10.3 終了の効果と効果継続.....	47
9.11 関係者間の個別通知と連絡.....	48
9.12 改訂 .....	48
9.12.1 改訂手続 .....	48
9.12.2 通知方法及び期間 .....	48
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 .....	48
9.13 紛争解決手続.....	48
9.14 準拠法.....	48
9.15 適用法の遵守 .....	48
9.16 雑則 .....	48
9.17 その他の条項.....	48

## 1. はじめに

本 CP/CPS は、府省等利用機関の業務サーバの暗号化通信、ソフトウェアへの署名等を実現するため、サーバ証明書及びコード署名証明書を発行するアプリケーション認証局（以下「アプリケーション 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

アプリケーション CA は、府省等利用機関に対してサーバ証明書及びコード署名証明書を発行する。

アプリケーション 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せず、本 CP/CPS をアプリケーション 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

アプリケーション CA の証明書ポリシーは、アプリケーション CA のサーバ証明書用の証明書ポリシー及びコード署名証明書用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。

- サーバ証明書ポリシー：0.2.440.100145.8.4.1.11.10
- コード署名証明書ポリシー：0.2.440.100145.8.4.1.1.20

### 1.3 PKI の関係者

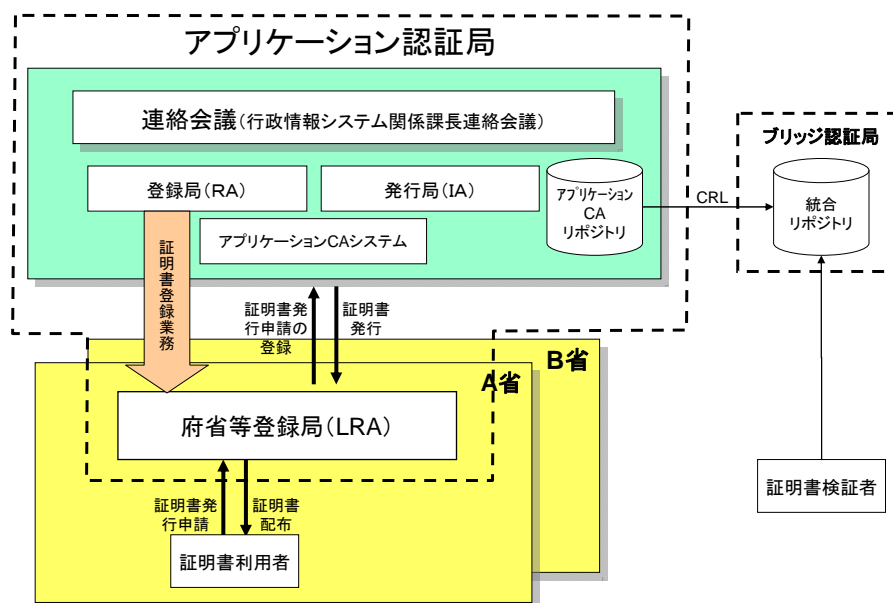


図 1-1 組織体制図

#### 1.3.1 連絡会議

アプリケーション CA の運営に関する意思決定は、行政情報システム関係課長連絡会議（以下「連絡会議」という。）が行う。

連絡会議の機能は、次のとおりとする。

- ・ アプリケーション CA の CP/CPS 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
- ・ その他アプリケーション 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）

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、総務省行政管理局行政情報システム企画課情報システム管理室長を充てる。

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

検査者等が行う。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

アプリケーション 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、サーバ証明書及びコード署名証明書の失効情報を公表する失効リスト（以下「CRL」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

サーバ証明書は、府省等が運営するサーバの実在性証明及び暗号化通信に使用する。サーバ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3年とする。

コード署名証明書は、府省等から国民・企業等へ配付されるソフトウェアへの署名に使用する。コード署名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3年とする。

### 1.4.2 禁止される証明書の用途

アプリケーション 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、総務省行政管理局行政情報システム企画課が行う。

### 1.5.2 連絡先

本 CP/CPS に関する照会は、総務省行政管理局行政情報システム企画課を窓口とする。  
窓口の連絡先は、以下の URL に掲示する。

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

### 1.5.3 ポリシ適合性を決定する者

アプリケーション 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

アプリケーション 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>

- 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/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、鍵の生成・管理、責任等に関して定めた文書。証明書ポリシ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サーバ証明書及びコード署名証明書のリスト。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もつ。

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、アプリケーション 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。
- ・ 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 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。

- SSL (Secure Socket Layer)

サーバとクライアント間の通信の暗号化と認証を行い、安全にデータをやりとりするプロトコル。

- 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 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 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うえで、予め設定してある権限（読出し、書込み等）の操作を可能にする。

- アプリケーション CA リポジトリ

アプリケーション CA が発行する証明書及び CRL を格納するリポジトリ。「リポジトリ」参照。

- 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み合わせ製品。

- ・ 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）。

- ・ 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、発行したすべ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値。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」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うえ、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元となるデータファイル。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（Web サーバ、その管理者等）。

- ・ 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。

- ・ 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 リポジトリ及びアプリケーション 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 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。

- ・ 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 に含まれるデータの内容を定義したもの。RFC3280 により証明書及び CRL 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 を格納し公表するデータベース。
  
- 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

アプリケーション CA に関する情報は、統合リポジトリ及び Web 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

アプリケーション CA は、アプリケーション 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。

- ・ アプリケーション CA の自己署名証明書
- ・ CRL

#### (2) Web での公表

アプリケーション CA は、次の情報を Web で公表する。

- ・ アプリケーション CA の自己署名証明書及びそのフィンガープリント
- ・ CRL
- ・ CA 秘密鍵危殆化に関する情報
- ・ 本 CP/CPS 及びその改訂履歴

### 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。

- ・ 自己署名証明書及び CRL は、発行及び更新の都度
- ・ 本 CP/CPS は、変更の都度

### 2.4 リポジトリへのアクセス管理

アプリケーション 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 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

アプリケーション 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

###### (1) サーバ証明書

サーバ証明書において使用する名前は、サーバ名とし、絶対ドメイン名 (FQDN:Fully Qualified Domain Name) を設定する。

###### (2) コード署名証明書

コード署名証明書において使用する名前は、アプリケーションを配付する組織の名称とする。

##### 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

様々な名前形式を解釈するための規則は、X.500 シリーズの識別名規定に従う。

##### 3.1.5 名前の一意性

アプリケーション 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、サーバ証明書及びコード署名証明書の申請手続において、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

LRA は、サーバ証明書及びコード署名証明書の申請手続において、申請書に記載された組織等を独立行政法人国立印刷局発行の職員録等と照合することにより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

LRA は、サーバ証明書及びコード署名証明書の申請手続において、申請書に記載された氏名、連絡先等を独立行政法人国立印刷局発行の職員録等と照合することにより証明書利用者の真偽を確認する。

また、LRA は、電話又は対面により申請の意思を確認する。

### 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

規定しない。

## 3.3 更新申請時の識別と認証

### 3.3.1 通常の更新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) サーバ証明書

LRA に対するサーバ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 に対するサーバ証明書の発行申請は、LRA が行う。

##### (2) コード署名証明書

LRA に対するコード署名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 に対するコード署名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) サーバ証明書

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、申請書にサーバ証明書の名義 (cn) として記載されたドメイン名の所有者が、LRA を所管する府省等又はその関連組織であることを第三者機関の提供するデータベース等により確認し、IA 及び RA に対して正確な情報を申請するものとする。

##### (2) コード署名証明書

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、申請書にコード署名証明書の名義 (cn) として記載された組織名称が存在し、かつ LRA を所管する府省等又は府省等に属する庁の最上位の組織名称であることを、府省等が公表している資料に記載の組織名称により確認し、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) サーバ証明書

証明書申請者は、所定の手続に基づき、LRA に対してサーバ証明書の発行申請を行う。

LRA 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き審査を実施し、IA 及び RA に対してサーバ証明書の発行申請の登録を行う。

IA 及び RA は、「3.2.1 秘密鍵の所持を証明する方法」において定める手続の実施及び LRA における審査が完了していることの確認により申請内容が適切であることを確認する。

#### (2) コード署名証明書

証明書申請者は、所定の手続に基づき、LRA に対してコード署名証明書の発行申請を行う。

LRA 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き審査を実施し、IA 及び RA に対してコード署名証明書の発行申請の登録を行う。

IA 及び RA は、「3.2.1 秘密鍵の所持を証明する方法」において定める手続の実施及び LRA における審査が完了していることの確認により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) サーバ証明書

IA 及び RA は、登録された公開鍵に対し、自 CA の署名を付してサーバ証明書を発行する。

IA 及び RA は、発行したサーバ証明書を、安全な通信手段を用いて LRA に配付する。

LRA は、サーバ証明書を、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、サーバ証明書の配付によって行う。

##### (2) コード署名証明書

IA 及び RA は、登録された公開鍵に対し、自 CA の署名を付してコード署名証明書を発行する。

IA 及び RA は、発行したコード署名証明書を、安全な通信手段を用いて LRA に配付する。

LRA は、コード署名証明書を、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、コード署名証明書の配付によって行う。

#### 4.4 証明書の受領

##### (1) サーバ証明書

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、サーバ証明書の受入れが完了したのものとする。

##### (2) コード署名証明書

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、コード署名証明書の受入れが完了したのものとする。

#### 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。

- ・ サーバ証明書及びコード署名証明書は、本 CP/CPS に従って利用する。
- ・ サーバ証明書及びコード署名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

サーバ証明書及びコード署名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。

- ・ サーバ証明書及びコード署名証明書の利用目的を確認する。
- ・ サーバ証明書及びコード署名証明書が改ざんされていないことを確認する。
- ・ サーバ証明書及びコード署名証明書の有効性について検証する。

#### 4.6 証明書の更新

##### (1) サーバ証明書

規定しない。

##### (2) コード署名証明書

規定しない。

#### 4.7 鍵更新を伴う証明書の更新

##### (1) サーバ証明書

サーバ証明書の有効期限が近づいた場合等、サーバ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。

##### (2) コード署名証明書

コード署名証明書の有効期限が近づいた場合等、コード署名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) サーバ証明書

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。

##### (2) コード署名証明書

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) サーバ証明書

IA 及び RA は、次のサーバ証明書失効事由が発生した場合、サーバ証明書を失効する。

- ・ サーバ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
- ・ アプリケーション 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

###### (2) コード署名証明書

IA 及び RA は、次のコード署名証明書失効事由が発生した場合、コード署名証明書を失効する。

- ・ コード署名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
- ・ アプリケーション 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) サーバ証明書

LRA に対するサーバ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 に対するサーバ証明書の失効申請は、LRA が行う。

#### (2) コード署名証明書

LRA に対するコード署名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 に対するコード署名証明書の失効申請は、LRA が行う。

### 4.9.3 失効申請手続

#### (1) サーバ証明書

証明書申請者は、所定の手続に基づき、LRA に対しサーバ証明書の失効申請を行う。

LRA は、申請書に記載された名義(cn)が、発行申請時の申請書に記載された名義(cn)と同一であることを確認し、IA 及び RA に対しサーバ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、サーバ証明書の失効処理を行い、CRL を統合リポジトリ及び Web に登録する。

LRA は、サーバ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。

#### (2) コード署名証明書

証明書申請者は、所定の手続に基づき、LRA に対しコード署名証明書の失効申請を行う。

LRA は、申請書に記載された名義(cn)が、発行申請時の申請書に記載された名義(cn)と同一であることを確認し、IA 及び RA に対しコード署名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、コード署名証明書の失効処理を行い、CRL を統合リポジトリ及び Web に登録する。

LRA は、コード署名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 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及び Web で CRL を公表する。

#### 4.9.7 CRL の発行頻度

有効期間 48 時間の CRL 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 を直ちに発行する。

#### 4.9.8 CRL の発行最大遅延時間

IA 及び RA は、発行した CRL を速やかにアプリケーション CA リポジトリ、統合リポジトリ及び Web 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

統合リポジトリ及び Web 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

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 証明書の一時停止の申請者

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、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、アプリケーション 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
- ・ その他アプリケーション 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、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、アプリケーション 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
- ・ アプリケーション 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
- ・ アプリケーション 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、アプリケーション 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
- ・ アプリケーション CA システムの起動・停止
- ・ アプリケーション CA リポジトリの起動・停止
- ・ アプリケーション CA システムの動作に関する設定変更管理
- ・ アプリケーション 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、アプリケーション 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
- ・ サーバ証明書及びコード署名証明書の失効処理
- ・ 操作員への証明書の発行、更新及び失効処理

- ・ アプリケーション 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、アプリケーション CA システム及びアプリケーション 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
- ・ サーバ証明書及びコード署名証明書の発行、更新及び失効申請の審査結果に対する最終承認
- ・ サーバ証明書及びコード署名証明書の発行、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 へサーバ証明書及びコード署名証明書の発行、更新及び失効申請の登録を行う。

#### (12)LRA 受付担当者

サーバ証明書及びコード署名証明書の発行、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

サーバ証明書及びコード署名証明書の発行、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識別と認証

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

アプリケーション 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、アプリケーション 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

アプリケーション CA システム及びアプリケーション 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アプリケーション 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 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 7 年以内に、CA 鍵ペアの更新を行う。

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
- ・ サーバ証明書、コード署名証明書の失効手続
- ・ CA 秘密鍵の廃棄及び再生成手続

- ・ サーバ証明書、コード署名証明書の再発行手続

また、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。

- ・ 統合リポジトリ及び Web による CRL 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

連絡会議においてアプリケーション 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アプリケーション 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 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 の認定を受けた HSM を用いて生成する。

##### (2) サーバ証明書鍵

サーバ証明書の鍵ペアは、証明書利用者が生成する。

##### (3) コード署名証明書鍵

コード署名証明書の鍵ペアは、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 は、証明書利用者に対する秘密鍵の配付は行わない。

#### 6.1.3 認証局への公開鍵の配付

証明書利用者の公開鍵は、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。

#### 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及び Web 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 による自己署名証明書及び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) サーバ証明書鍵

RSA1024 ビットの鍵を使用する。

##### (3) コード署名証明書鍵

RSA1024 ビットの鍵を使用する。

#### 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) サーバ証明書鍵

サーバの実在性証明及び暗号化通信に用いる。

#### (3) コード署名証明書

プログラム等ソフトウェアへの署名に用いる。

## 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) サーバ証明書鍵

規定しない。

#### (3) コード署名証明書鍵

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) サーバ証明書鍵

規定しない。

##### (3) コード署名証明書鍵

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) サーバ証明書鍵

規定しない。

##### (3) コード署名証明書鍵

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) サーバ証明書鍵

規定しない。

##### (3) コード署名証明書鍵

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) サーバ証明書鍵

規定しない。

##### (3) コード署名証明書鍵

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

アプリケーション 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、7 年以内に鍵更新を行う。

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) サーバ証明書鍵

サーバ証明書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 3 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) コード署名証明書鍵

コード署名証明書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 3 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) サーバ証明書鍵

サーバ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。

##### (3) コード署名証明書鍵

コード署名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) サーバ証明書鍵

サーバ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。

##### (3) コード署名証明書鍵

コード署名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

アプリケーション 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

アプリケーション 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

アプリケーション 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、アプリケーション 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

アプリケーション 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 自己署名証明書

表 7-1 アプリケーション CA 自己署名証明書

領域名	クリティカルフラグ	値	説明
Version (バージョン番号)		2	v3 整数
serial Number (シリアル番号)		例)1	証明書のシリアル番号、整数
signature algorithm ID (署名アルゴリズム)			アプリケーション CA 署名アルゴリズム
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer name (発行者名)		ou=ApplicationCA, o=Japanese Government, c=JP	アプリケーション CA の識別名(DN)、英語表記 Printable スtring
validity period (証明書有効期間)			証明書の有効期間
notBefore (発行日)		例)010401000000Z	証明書有効期間の開始日 YYMMDDHHMMSSZ
notAfter (終了日)		例)110401000000Z	証明書有効期間の終了日 YYMMDDHHMMSSZ
subject name (主体者名)		ou=ApplicationCA, o=Japanese Government, c=JP	アプリケーション CA の識別名(DN)、英語表記 Printable スtring
subject public key info (主体者公開鍵情報)			公開鍵アルゴリズム
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.1	アプリケーション CA 公開鍵アルゴリズム識別子、RSA Encryption
parameter (パラメータ)		NULL	RSA の場合値なし

public key (公開鍵)		BIT STRING	アプリケーション CA 公開鍵、 BIT スtring
extensions (証明書拡張領域)			
subjectKeyIdentifier (主体者鍵識別子)	FALSE	OCTET STRING	主体者鍵識別子
keyUsage (鍵用途)	TRUE		鍵用途の目的を指定
keyCertSign		1	[5]
cRLSign		1	[6]
subjectAltName (主体者代替名)	FALSE	ou=アプリケーション CA, o=日本国政府, c=JP	アプリケーション CA の識別 名 (DN)、日本語表記 UTF8 スtring
basicConstraints (基本制約)	TRUE		CA 証明書とエンド・エンティテ ィ証明書を区別
cA		cA=TRUE	必須(MUST)とする。
issuer's signature (発行者署名)			アプリケーション CA のデジタ ル署名
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
		ENCRYPTED (署名値)	

## 7.2 サーバ証明書

表 7-2 サーバ証明書

領域名	クリティカ ルフラグ	値	説明
version (バージョン番号)		2	v3 整数
serial Number (シリアル番号)		例) 23	証明書のシリアル番号、整数
signature algorithm ID (署名アルゴリズム)			アプリケーション CA 署名ア ルゴリズム

algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer name (発行者名)		ou=ApplicationCA, o=Japanese Government, c=JP	アプリケーション CA の識別 名(DN)、英語表記 Printable スtring
validity period (証明書有効期間)			証明書の有効期間
notBefore (開始日)		例) 010401000000Z	証明書有効期間の開始日 YYMMDDHHMMSSZ
notAfter (終了日)		例) 040401000000Z	証明書有効期間の終了日 YYMMDDHHMMSSZ
subject name (主体者名)		例) cn=xxx.yyy.go.jp, ou=Ministry of Internal Affairs and Communications, o= Japanese Government, c=JP	主体者の識別名(DN)、英語 表記(DN は4つの RDN から 構成)、cn はサーバの FQDN Printable スtring
subject public key info (主体者公開鍵情報)			公開鍵アルゴリズム
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.1	サーバ公開鍵 アルゴリズム 識別子、RSA Encryption
parameter (パラメータ)		NULL	RSA の場合値なし
public key (公開鍵)		BIT STRING	サーバ公開鍵、BIT スtring
extensions (証明書拡張領域)			
authorityKeyIdentifier (認証局鍵識別子)	FALSE		認証局鍵識別子
keyIdentifier		OCTET STRING	アプリケーション CA 鍵識別子
subjectKeyIdentifier (主体者鍵識別子)	FALSE	OCTET STRING	主体者鍵識別子
keyUsage (鍵用途)	TRUE		鍵用途の目的を指定
digitalSignature		1	[0]

keyEncipherment		1	[2]
extendedKeyUsage (拡張鍵用途)	FALSE		拡張鍵用途の目的を指定
KeyPurposeId		id-kp-serverAuth	TLS または SSL によるサーバ認証
certificatePolicies (証明書ポリシー)	FALSE		
policyIdentifier			OID
certPolicyId		0.2.440.100145.8.4.1.11.10	サーバ証明書ポリシーの OID id-apca-cp-tls.server10
policyQualifiers			ポリシー修飾子(CPS へのポインターまたはユーザー通知情報)
policyQualifierId		id-qt-cps	CPS
qualifier		http://www.gpki.go.jp/apca/cpcps/index.html	アプリケーション CACPS の URI、IA5 スtring
issuerAltName (発行者代替名)		FALSE	ou=アプリケーション CA, o=日本国政府, c=JP
cRLDistributionPoints (CRL 配布点)	FALSE		
distributionPoint			配布点
fullName (省略しない名称)		http://dir.gpki.go.jp/ApplicationCA.crl	URIにて CRL の配布点を指定、IA5 String
distributionPoint			DistributionPointName
fullName (省略しない名称)		http://dir.gpki.hq.admix.go.jp/ApplicationCA.crl	URIにて CRL の配布点を指定、IA5 String
issuer's signature (発行者署名)			アプリケーション CA のデジタル署名
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
	ENCRYPTED (署名値)		

### 7.3 コード署名証明書

表 7-3 コード署名証明書

領域名	クリティカルフラグ	値	説明
version (バージョン番号)		2	v3 整数
serial Number (シリアル番号)		例)23	証明書のシリアル番号、整数
signature algorithm ID (署名アルゴリズム)			アプリケーション CA 署名アルゴリズム
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer name (発行者名)		ou=ApplicationCA, o=Japanese Government, c=JP	アプリケーション CA の識別名(DN)、英語表記 Printable スtring
validity period (証明書有効期間)			証明書の有効期間
notBefore (開始日)		例)010401000000Z	証明書有効期間の開始日 YYMMDDHHMMSSZ
notAfter (終了日)		例)040401000000Z	証明書有効期間の終了日 YYMMDDHHMMSSZ
subject name (主体者名)		例)cn= Ministry of Internal Affairs and Communications, ou=Ministry of Internal Affairs and Communications, o= Japanese Government, c=JP	主体者の識別名(DN)、英語 表記(DN は4つの RDN から 構成) Printable スtring
subject public key info (主体者公開鍵情報)			公開鍵アルゴリズム
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.1	コード署名公開鍵アルゴリズム 識別子、RSA Encryption

parameter (パラメータ)		NULL	RSA の場合値なし
public key (公開鍵)		BIT STRING	コード署名公開鍵、BIT ストリング
extensions (証明書拡張領域)			
authorityKeyIdentifier (認証局鍵識別子)	FALSE		認証局鍵識別子
keyIdentifier		OCTET STRING	アプリケーション CA 鍵識別子
subjectKeyIdentifier (主体者鍵識別子)	FALSE	OCTET STRING	主体者鍵識別子
keyUsage (鍵用途)	TRUE		鍵用途の目的を指定
digitalSignature		1	[0]
extendedKeyUsage (拡張鍵用途)	FALSE		拡張鍵用途の目的を指定
KeyPurposeId		id-kp-codeSigning	コード署名
certificatePolicies (証明書ポリシー)	FALSE		
policyIdentifier			OID
certPolicyId		0.2.440.100145.8.4.1.1.20	コード署名証明書ポリシーの OID id- apca-cp-ds.class20
policyQualifiers			ポリシー修飾子(CPS へのポインターまたはユーザー通知情報)
policyQualifierId		id-qt-cps	CPS
qualifier		<a href="http://www.gpki.go.jp/apca/cpcps/index.html">http://www.gpki.go.jp/apca/cpcps/index.html</a>	アプリケーション CACPS の URI、IA5 ストリング
issuerAltName (発行者代替名)	FALSE	ou=アプリケーション CA, o=日本国政府, c=JP	アプリケーション CA の識別名 (DN)、日本語表記 UTF8 ストリング
cRLDistributionPoints (CRL 配布点)	FALSE		
distributionPoint			配布点

fullName (省略しない名称)		http://dir.gpki.go.jp/ApplicationCA.crl	URIにて CRL の配布点を指定、IA5 スtring
distributionPoint			DistributionPointName
fullName (省略しない名称)		http://dir.gpki.hq.admix.go.jp/ApplicationCA.crl	URIにて CRL の配布点を指定、IA5 スtring
issuer's signature (発行者署名)			アプリケーション CA のデジタル署名
algorithm identifier (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
ENCRYPTED (署名値)			

#### 7.4 CRL

表 7-4 失効リスト

領域名	クリティカルフラグ	値	説明
version (バージョン番号)		1	v2 CRL 整数
signature (署名アルゴリズム)			署名アルゴリズム
algorithmIdentifier			アルゴリズム識別子と署名アルゴリズム領域(signatureAlgorithm)は一致させる。
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer (発行者)		ou=ApplicationCA, o=Japanese Government, c=JP	アプリケーション CA の識別名(DN)、英語表記 Printable スtring
thisUpdate (今回の更新日)		例) 010501000000Z	今回の更新日時 YYMMDDHHMMSSZ
nextUpdate (次回の更新日)		例) 010503000000Z	次回の更新日時 YYMMDDHHMMSSZ
revokedCertificates			失効される証明書エントリー

(失効した証明書)			(以下の組のリスト)
userCertificate		例) 10002	失効された証明書を整数で指定
revocationDate		例) 010501000000Z	失効日時 YYMMDDHHMMSSZ
crlEntryExtensions (失効証明書エントリー拡張)	FALSE		(失効証明書ごとの拡張領域)
reasonCode			理由コード
unspecified			[0] 未定義
keyCompromise			[1] 鍵の危殆
cACompromise			[2] CA 鍵の危殆
affiliationChanged			[3] 所属の変更
superseded			[4] 上書き
cessationOfOperation		例) 1	[5] 業務の停止
certificateHold			[6] 証明書の保留
↓			
次の revokedCertificates (失効した証明書)			

拡張領域			
crlExtensions (証明書失効リスト拡張)			
authorityKeyIdentifier (認証局鍵識別子)	FALSE		認証局鍵識別子、証明書拡張と同じにする。
keyIdentifier		OCTET STRING	アプリケーションCA鍵識別子
cRLNumber (CRL 番号)	FALSE	例) 32	シーケンス番号、整数
			ENCRYPTED (署名値)

## 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、アプリケーション 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、アプリケーション 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

アプリケーション CA は、漏えいすることによってアプリケーション CA 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

アプリケーション 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」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、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。

アプリケーション 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な要求があった場合、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アプリケーション 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、サーバ証明書、コード署名証明書、CRL、自己署名証明書及び本 CP/CPS の知的財産権は、アプリケーション CA に帰属するものとする。

ただし、サーバ証明書及びコード署名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。

- 本 CP/CPS に基づき、自己署名証明書、サーバ証明書、コード署名証明書を発行、更新、失効すること
- 「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 を通常運用時には 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には、速やかに危殆化に関する情報を公表すること
- 証明書の発行、更新及び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
- 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アプリケーション 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、又はアプリケーション 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、証明書検証者及びアプリケーション 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、又は許容されるアプリケーション CA に対する通知、請求、要求、依頼その他の連絡は総務省行政管理局行政情報システム企画課を窓口とする。連絡先は「1.5.2 連絡先」に規定する。

#### 9.12 改訂

##### 9.12.1 改訂手続

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の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。