# 総務省運用支援認証局ＣＰ／ＣＰＳ

平成１４年6月２８日

総務省行政情報化推進委員会決定

（最終改正　平成１８年２月２４日）

１．　はじめに　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　1
　１．１　概要　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　1
　１．２　識別　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　1
　１．３　運営体制と証明書の適用範囲　・・・・・・・・・・・・・・・・・・・・・　1
　　１．３．１　総務省運用支援ＣＡの組織　・・・・・・・・・・・・・・・・・・・　1
　　１．３．２　証明書の適用範囲　・・・・・・・・・・・・・・・・・・・・・・・　2
　１．４　ＣＰ／ＣＰＳに関する担当組織　・・・・・・・・・・・・・・・・・・・・　2
　　１．４．１　管理担当部署　・・・・・・・・・・・・・・・・・・・・・・・・・　2
　　１．４．２　照会窓口　・・・・・・・・・・・・・・・・・・・・・・・・・・・　2
２．　一般規定　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　3
　２．１　義務　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　3
　　２．１．１　ＣＡ業務に関する義務　・・・・・・・・・・・・・・・・・・・・・　3
　　２．１．２　ＲＡ業務に関する義務　・・・・・・・・・・・・・・・・・・・・・　3
　　２．１．３　証明書利用者の義務　・・・・・・・・・・・・・・・・・・・・・・　3
　　２．１．４　証明書検証者の義務　・・・・・・・・・・・・・・・・・・・・・・　3
　　２．１．５　リポジトリに関する義務　・・・・・・・・・・・・・・・・・・・・　3
　２．２　ＣＡの責任　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　3
　２．３　財務上の責任　・・・・・・・・・・・・・・・・・・・・・・・・・・・・　4
　２．４　解釈及び執行　・・・・・・・・・・・・・・・・・・・・・・・・・・・・　4
　　２．４．１　準拠法　・・・・・・・・・・・・・・・・・・・・・・・・・・・・　4
　　２．４．２　分割、存続、合併及び通知　・・・・・・・・・・・・・・・・・・・　4
　　２．４．３　紛争解決の手続　・・・・・・・・・・・・・・・・・・・・・・・・　4
　２．５　料金　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　4
　２．６　公表とリポジトリ　・・・・・・・・・・・・・・・・・・・・・・・・・・　4
　　２．６．１　ＣＡに関する情報の公表　・・・・・・・・・・・・・・・・・・・・　4
　　２．６．２　公表の頻度　・・・・・・・・・・・・・・・・・・・・・・・・・・　4
　　２．６．３　アクセス制御　・・・・・・・・・・・・・・・・・・・・・・・・・　4
　　２．６．４　リポジトリ　・・・・・・・・・・・・・・・・・・・・・・・・・・　5
　２．７　準拠性監査　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　5
　　２．７．１　監査の頻度　・・・・・・・・・・・・・・・・・・・・・・・・・・　5
　　２．７．２　監査人の身元・資格　・・・・・・・・・・・・・・・・・・・・・・　5
　　２．７．３　監査人と被監査部門の関係　・・・・・・・・・・・・・・・・・・・　5
　　２．７．４　監査項目　・・・・・・・・・・・・・・・・・・・・・・・・・・・　5
　　２．７．５　監査指摘事項への対応　・・・・・・・・・・・・・・・・・・・・・　5
　　２．７．６　監査結果　・・・・・・・・・・・・・・・・・・・・・・・・・・・　5
　２．８　機密保持　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　6
　　２．８．１　機密扱いとする情報　・・・・・・・・・・・・・・・・・・・・・・　6
　　２．８．２　機密扱いとしない情報　・・・・・・・・・・・・・・・・・・・・・　6
　　２．８．３　証明書失効情報の公表　・・・・・・・・・・・・・・・・・・・・・　6

２．８．４ 法執行機関への情報開示 ・・・・・・・・・・・・・・・・・・・・ 6
２．８．５ 民事手続上の情報開示 ・・・・・・・・・・・・・・・・・・・・ 6
２．８．６ 証明書利用者の要求に基づく情報の開示 ・・・・・・・・・・・・ 6
２．８．７ その他の理由に基づく情報開示 ・・・・・・・・・・・・・・・・ 6
２．９ 知的財産権 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 6
３． 識別と認証 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 7
３．１ 初期登録 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 7
３．１．１ 名前の型 ・・・・・・・・・・・・・・・・・・・・・・・・・・ 7
３．１．２ 名前の意味に関する要件 ・・・・・・・・・・・・・・・・・・・ 7
３．１．３ 名前形式を解釈するための規則 ・・・・・・・・・・・・・・・・ 7
３．１．４ 名前の一意性 ・・・・・・・・・・・・・・・・・・・・・・・・ 7
３．１．５ 名前に関する紛争の解決手順 ・・・・・・・・・・・・・・・・・ 7
３．１．６ 商標の認識・認証・役割 ・・・・・・・・・・・・・・・・・・・ 7
３．１．７ 秘密鍵の所有を証明するための方法 ・・・・・・・・・・・・・・ 7
３．１．８ 組織の認証 ・・・・・・・・・・・・・・・・・・・・・・・・・ 7
３．１．９ 個人の認証 ・・・・・・・・・・・・・・・・・・・・・・・・・ 7
３．２ 証明書の更新 ・・・・・・・・・・・・・・・・・・・・・・・・・・・ 7
３．３ 証明書失効後の再発行 ・・・・・・・・・・・・・・・・・・・・・・ 8
３．４ 証明書の失効申請 ・・・・・・・・・・・・・・・・・・・・・・・・ 8
４． 運用要件 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 9
４．１ 証明書の発行申請 ・・・・・・・・・・・・・・・・・・・・・・・・ 9
４．１．１ 自己署名証明書 ・・・・・・・・・・・・・・・・・・・・・・・ 9
４．１．２ 相互認証証明書 ・・・・・・・・・・・・・・・・・・・・・・・ 9
４．１．３ サーバ証明書及びコード署名証明書 ・・・・・・・・・・・・・・ 9
４．２ 証明書の発行 ・・・・・・・・・・・・・・・・・・・・・・・・・・・ 9
４．２．１ 自己署名証明書 ・・・・・・・・・・・・・・・・・・・・・・・ 9
４．２．２ 相互認証証明書 ・・・・・・・・・・・・・・・・・・・・・・・ 9
４．２．３ サーバ証明書及びコード署名証明書 ・・・・・・・・・・・・・・ 9
４．３ 証明書の受入れ ・・・・・・・・・・・・・・・・・・・・・・・・・・ 9
４．３．１ 自己署名証明書 ・・・・・・・・・・・・・・・・・・・・・・・ 9
４．３．２ 相互認証証明書 ・・・・・・・・・・・・・・・・・・・・・・・ 9
４．３．３ サーバ証明書及びコード署名証明書 ・・・・・・・・・・・・・・ 9
４．４ 証明書の失効及び一時停止 ・・・・・・・・・・・・・・・・・・・・ 9
４．４．１ 証明書の失効理由 ・・・・・・・・・・・・・・・・・・・・・・ 9
４．４．２ 証明書の失効申請者 ・・・・・・・・・・・・・・・・・・・・・ 10
４．４．３ 証明書の失効申請及び失効処理手順 ・・・・・・・・・・・・・・ 10
４．４．４ 失効における猶予期間 ・・・・・・・・・・・・・・・・・・・・ 10
４．４．５ 証明書の一時停止 ・・・・・・・・・・・・・・・・・・・・・・ 11
４．４．６ 一時停止申請者 ・・・・・・・・・・・・・・・・・・・・・・・ 11
４．４．７ 一時停止手順 ・・・・・・・・・・・・・・・・・・・・・・・・ 11

４．４．８ 一時停止期間の制限 ・・・・・・・・・・・・・・・・・・・・・・ 11
４．４．９ ＣＲＬ／ＡＲＬの発行周期 ・・・・・・・・・・・・・・・・・・ 11
４．４．１０ ＣＲＬ／ＡＲＬの確認 ・・・・・・・・・・・・・・・・・・・ 11
４．４．１１ オンライン有効性確認の可用性 ・・・・・・・・・・・・・・・ 11
４．４．１２ オンライン有効性確認要件 ・・・・・・・・・・・・・・・・・ 11
４．４．１３ その他利用可能な有効性確認手段 ・・・・・・・・・・・・・・ 11
４．４．１４ その他利用可能な有効性確認手段における確認要件 ・・・・ 11
４．４．１５ 秘密鍵の危殆化に関する特別な要件 ・・・・・・・・・・・・・ 11
４．５ セキュリティ監査の手順 ・・・・・・・・・・・・・・・・・・・・・・ 11
４．５．１ 監査ログに記録する情報 ・・・・・・・・・・・・・・・・・・・ 12
４．５．２ 監査ログの検査周期 ・・・・・・・・・・・・・・・・・・・・・ 12
４．５．３ 監査ログの保管期間 ・・・・・・・・・・・・・・・・・・・・・ 12
４．５．４ 監査ログの保護 ・・・・・・・・・・・・・・・・・・・・・・・ 12
４．５．５ 監査ログのバックアップ手順 ・・・・・・・・・・・・・・・・・ 12
４．５．６ 監査ログの収集システム ・・・・・・・・・・・・・・・・・・・ 12
４．５．７ 監査ログ検査の通知 ・・・・・・・・・・・・・・・・・・・・・ 12
４．５．８ 脆弱性の評価 ・・・・・・・・・・・・・・・・・・・・・・・・ 12
４．６ アーカイブ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 12
４．６．１ アーカイブデータの種類 ・・・・・・・・・・・・・・・・・・・ 12
４．６．２ アーカイブデータの保管期間・・・・・・・・・・・・・・・・・・ 13
４．６．３ アーカイブデータの保護 ・・・・・・・・・・・・・・・・・・・ 13
４．６．４ アーカイブデータのバックアップ手順 ・・・・・・・・・・・・・ 13
４．６．５ アーカイブデータのタイムスタンプに関する要件 ・・・・・・・ 13
４．６．６ アーカイブデータの収集システム ・・・・・・・・・・・・・・・ 13
４．６．７ アーカイブデータの検証 ・・・・・・・・・・・・・・・・・・・ 13
４．７ 鍵の更新 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 13
４．８ 危殆化と災害からの復旧 ・・・・・・・・・・・・・・・・・・・・・・ 13
４．８．１ 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対処 13
４．８．２ 証明書を失効した場合の要件 ・・・・・・・・・・・・・・・・・ 13
４．８．３ 秘密鍵が危殆化した場合の対処 ・・・・・・・・・・・・・・・・ 14
４．８．４ 災害等発生時の設備の確保 ・・・・・・・・・・・・・・・・・・ 14
４．９ 認証業務の終了 ・・・・・・・・・・・・・・・・・・・・・・・・・・ 14
５． 物理面、手続面及び人事面のセキュリティ管理 ・・・・・・・・・・・・ 15
５．１ 物理的管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 15
５．１．１ 施設の位置と建物構造 ・・・・・・・・・・・・・・・・・・・・ 15
５．１．２ 物理的アクセス ・・・・・・・・・・・・・・・・・・・・・・・ 15
５．１．３ 電源設備と空調設備 ・・・・・・・・・・・・・・・・・・・・・ 15
５．１．４ 水害対策 ・・・・・・・・・・・・・・・・・・・・・・・・・・ 15
５．１．５ 地震対策 ・・・・・・・・・・・・・・・・・・・・・・・・・・ 15
５．１．６ 火災防止対策 ・・・・・・・・・・・・・・・・・・・・・・・・ 15

５．１．７ 媒体管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 15
５．１．８ 廃棄物処理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 15
５．１．９ オフサイトバックアップ ・・・・・・・・・・・・・・・・・・・・・ 15
５．２ 手続面の管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 15
５．３ 人事面の管理 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 17
６． 技術的セキュリティ管理 ・・・・・・・・・・・・・・・・・・・・・・・・・ 18
６．１ 鍵ペア生成とインストール ・・・・・・・・・・・・・・・・・・・・・・・ 18
６．１．１ 鍵ペア生成 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 18
６．１．２ 証明書利用者への秘密鍵配付 ・・・・・・・・・・・・・・・・・・・ 18
６．１．３ 公開鍵の受領 ・・・・・・・・・・・・・・・・・・・・・・・・・・・ 18
６．１．４ ＣＡ公開鍵の配付 ・・・・・・・・・・・・・・・・・・・・・・・・・ 18
６．１．５ 鍵のサイズ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 18
６．１．６ 公開鍵パラメータの生成 ・・・・・・・・・・・・・・・・・・・・・ 18
６．１．７ 公開鍵パラメータの品質の検査 ・・・・・・・・・・・・・・・・・・ 18
６．１．８ 鍵を生成するハードウェア及びソフトウェア ・・・・・・・・・・・・ 18
６．１．９ 鍵の利用目的 ・・・・・・・・・・・・・・・・・・・・・・・・・・・ 19
６．２ 秘密鍵の保護 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 19
６．２．１ 暗号モジュールに関する基準 ・・・・・・・・・・・・・・・・・・・ 19
６．２．２ 秘密鍵の複数人制御 ・・・・・・・・・・・・・・・・・・・・・・・・ 19
６．２．３ 秘密鍵の預託 ・・・・・・・・・・・・・・・・・・・・・・・・・・・ 19
６．２．４ 秘密鍵のバックアップ ・・・・・・・・・・・・・・・・・・・・・・・ 19
６．２．５ 秘密鍵のアーカイブ ・・・・・・・・・・・・・・・・・・・・・・・・ 19
６．２．６ 暗号モジュールへの秘密鍵の格納 ・・・・・・・・・・・・・・・・・ 19
６．２．７ 秘密鍵の活性化方法 ・・・・・・・・・・・・・・・・・・・・・・・・ 19
６．２．８ 秘密鍵の非活性化方法 ・・・・・・・・・・・・・・・・・・・・・・・ 19
６．２．９ 秘密鍵の破棄方法 ・・・・・・・・・・・・・・・・・・・・・・・・・ 19
６．３ 公開鍵の履歴保管及び鍵ペアの有効期間 ・・・・・・・・・・・・・・・・ 20
６．３．１ 公開鍵の履歴保管 ・・・・・・・・・・・・・・・・・・・・・・・・・ 20
６．３．２ 公開鍵及び秘密鍵の有効期間 ・・・・・・・・・・・・・・・・・・・ 20
６．４ 活性化データ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 20
６．４．１ 活性化データの生成とインストール ・・・・・・・・・・・・・・・・ 20
６．４．２ 活性化データの保護 ・・・・・・・・・・・・・・・・・・・・・・・・ 20
６．５ コンピュータセキュリティ管理 ・・・・・・・・・・・・・・・・・・・・ 20
６．５．１ コンピュータセキュリティ技術要件 ・・・・・・・・・・・・・・・・ 21
６．５．２ コンピュータセキュリティ評価 ・・・・・・・・・・・・・・・・・・ 21
６．６ システムのライフサイクルにおけるセキュリティ管理 ・・・・・・・・・ 21
６．６．１ システム開発面における管理 ・・・・・・・・・・・・・・・・・・・ 21
６．６．２ システム運用面における管理 ・・・・・・・・・・・・・・・・・・・ 21
６．６．３ セキュリティ評価の基準 ・・・・・・・・・・・・・・・・・・・・・ 21
６．７ ネットワークセキュリティ管理 ・・・・・・・・・・・・・・・・・・・・ 21

６．８ 暗号モジュールの技術管理 ・・・・・・・・・・・・・・・・・・・・・・ 21
７． 証明書とＣＲＬ／ＡＲＬのプロファイル ・・・・・・・・・・・・・・・・・ 22
７．１ 証明書のプロファイル ・・・・・・・・・・・・・・・・・・・・・・・ 22
７．１．１ 自己署名証明書 ・・・・・・・・・・・・・・・・・・・・・・・ 22
７．１．２ サーバ証明書 ・・・・・・・・・・・・・・・・・・・・・・・・ 24
７．１．３ コード署名証明書 ・・・・・・・・・・・・・・・・・・・・・・ 25
７．２ ＣＲＬ、ＡＲＬのプロファイル ・・・・・・・・・・・・・・・・・・・ 26
７．２．１ ＣＲＬ ・・・・・・・・・・・・・・・・・・・・・・・・・・・ 26
７．２．２ ＡＲＬ ・・・・・・・・・・・・・・・・・・・・・・・・・・・ 27
８． ＣＰ／ＣＰＳの管理 ・・・・・・・・・・・・・・・・・・・・・・・・・ 28
８．１ ＣＰ／ＣＰＳの変更手順 ・・・・・・・・・・・・・・・・・・・・・・ 28
８．２ ＣＰ／ＣＰＳの公表と通知 ・・・・・・・・・・・・・・・・・・・・・ 28
８．３ ＣＰ／ＣＰＳ承認手順 ・・・・・・・・・・・・・・・・・・・・・・・ 28

# １．はじめに

本ＣＰ／ＣＰＳは、国民等と総務省との間で安全な通信を実現するため、総務省認証局（以下「総務省ＣＡ」という。）の機能を補完し、総務省ＣＡの運用を支援するための認証局（以下「総務省運用支援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RFC2527「Certificate Policy and Certification Practices Statement Framework」に準拠している。

## １．１　概要

総務省運用支援ＣＡは、総務省のサイトに対してサーバ証明書を発行し、総務省が提供するプログラムに署名を行うためのコード署名証明書を発行する。

総務省運用支援ＣＡは、ＣＰ（証明書ポリシ）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を総務省運用支援ＣＡの認証業務に関する運営方針として位置付ける。

なお、総務省運用支援ＣＡは、総務省ＣＡと同一の設備及び機器等を使用して構築する。

## １．２　識別

総務省運用支援ＣＡの証明書ポリシを示すオブジェクト識別子は、規定しない。

## １．３　運営体制と証明書の適用範囲

### １．３．１　総務省運用支援ＣＡの組織

(1) 意思決定組織

総務省運用支援ＣＡの運営に関する意思決定は、総務省行政情報化推進委員会（以下「委員会」という。）が行う。

委員会は、総務省運用支援ＣＡの運営に関し、次の事項を行う。

- 総務省運用支援ＣＡのＣＰ／ＣＰＳに関する決定
- 相互認証に関する決定
- ＣＡ秘密鍵の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
- その他総務省運用支援ＣＡの運営に関する重要事項の決定

(2) 運営組織

総務省におけるサーバ証明書等発行申請の受付及び審査並びにサーバ証明書等の発行、更新、失効等の運営業務は、総務省運用支援ＣＡ責任者、ＩＡ鍵管理者、受付担当者及び審査担当者が行う。

また、システムオペレーション、システムの維持管理等の運用業務は、ＩＡ操作員、ＲＡ操作員、ディレクトリ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　手続面の管理」において定める。

なお、総務省運用支援ＣＡの運営組織の要員は、総務省ＣＡの運営組織の要員

をもって充てる。

### １．３．２　証明書の適用範囲

適用範囲は次の証明書及び総務省の事務に必要な証明書とする。

- 総務省運用支援ＣＡに対する自己署名証明書（有効期限：有効とする日から10年）
- 総務省のサイトに対するサーバ証明書（有効期限：有効とする日から３年）
- 総務省が提供するプログラムに署名を行うためのコード署名証明書（有効期間：有効とする日から３年）

## １．４　ＣＰ／ＣＰＳに関する担当組織

### １．４．１　管理担当部署

本ＣＰ／ＣＰＳの変更、更新等に関する事務は、総務省大臣官房企画課情報システム室が行う。

### １．４．２　照会窓口

本ＣＰ／ＣＰＳに関する照会は、総務省大臣官房企画課情報システム室を窓口とする。

## ２．一般規定

### ２．１　義務

#### ２．１．１　ＣＡ業務に関する義務

総務省運用支援ＣＡは、ＣＡ業務に関し次の義務を負う。

- 本ＣＰ／ＣＰＳに基づき、自己署名証明書、サーバ証明書、コード署名証明書その他の証明書の発行を行うこと。
- 証明書の失効処理を行い、速やかに失効リスト（以下「ＣＲＬ／ＡＲＬ」という。）を発行すること。
- 総務省運用支援ＣＡの秘密鍵を安全に管理すること。
- 総務省運用支援ＣＡの秘密鍵が危殆化した場合に速やかに公表すること。
- 証明書の発行、更新、失効等に関する履歴、監査ログ及びアーカイブデータ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。

#### ２．１．２　ＲＡ業務に関する義務

総務省運用支援ＣＡは、ＲＡ業務に関し次の義務を負う。

- サーバ証明書及びコード署名証明書の発行等の申請手続が適正に行われていることを確認すること。

#### ２．１．３　証明書利用者の義務

証明書利用者は、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に従って利用すること。
- サーバ証明書及びコード署名証明書並びにその秘密鍵を適切かつ安全に管理すること。
- サーバ証明書及びコード署名証明書の管理は、本ＣＰ／ＣＰＳに基づいて行うこと。
- 秘密鍵が危殆化した場合、速やかに総務省運用支援ＣＡ責任者に報告すること。

#### ２．１．４　証明書検証者の義務

証明書検証者は、証明書検証の際に、証明書の有効性及び認証パスの有効性について検証しなければならない。

#### ２．１．５　リポジトリに関する義務

規定しない。

### ２．２　ＣＡの責任

総務省運用支援ＣＡは、自己署名証明書、サーバ証明書等の発行、更新、失効、保管及び公表に当たっては、証明書利用者及び証明書検証者に対し、本ＣＰ／ＣＰＳに

基づく認証業務を適切に行う。

２．３　財務上の責任

規定しない。

２．４　解釈及び執行

２．４．１　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。

２．４．２　分割、存続、合併及び通知

規定しない。

２．４．３　紛争解決の手続

規定しない。

２．５　料金

規定しない。

２．６　公表とリポジトリ

２．６．１　ＣＡに関する情報の公表

総務省運用支援ＣＡは、次の情報をＷｅｂ上で公表する。

- 自己署名証明書のフィンガープリント
- 証明書の失効情報
- ＣＲＬ／ＡＲＬ
- 総務省運用支援ＣＡが認証し、又は認証を取り消したサイト及びコード署名者の名称
- 総務省運用支援ＣＡの秘密鍵の危殆化に関する情報
- 本ＣＰ／ＣＰＳ

２．６．２　公表の頻度

総務省運用支援ＣＡに関する公表情報の更新頻度は、次のとおりとする。

- 自己署名証明書のフィンガープリント　発行及び更新の都度
- 証明書の失効情報　総務省運用支援ＣＡ責任者の決定の都度
- ＣＲＬ／ＡＲＬ　発行の都度
- 総務省運用支援ＣＡが認証し、又は認証を取り消したサイト及びコード署名者の名称　総務省運用支援ＣＡ責任者の決定の都度
- 本ＣＰ／ＣＰＳ　変更の都度

２．６．３　アクセス制御

Ｗｅｂ上で公表する情報は、インターネットを通じて提供される。公表情報を提供するに当たっては、特段のアクセス制御は行わない。

### ２．６．４　リポジトリ

規定しない。

## ２．７　準拠性監査

### ２．７．１　監査の頻度

総務省運用支援ＣＡの監査は、監査人により年１回定期的に行う。また、必要に応じて定期監査以外に監査を実施する。

### ２．７．２　監査人の身元・資格

総務省運用支援ＣＡの監査は、監査業務及び認証業務に精通した者が行う。

### ２．７．３　監査人と被監査部門の関係

監査人は、総務省運用支援ＣＡと利害関係を有しない者を選定する。

### ２．７．４　監査項目

総務省運用支援ＣＡの監査は、次の項目を中心に実施する。

- 認証業務が本ＣＰ／ＣＰＳ、運用マニュアル等に準拠して実施されていること。
- 外部及び内部の不正行為に対する措置が適切に講じられていること。

### ２．７．５　監査指摘事項への対応

総務省運用支援ＣＡは、監査人による監査結果に対し、次のとおり対応する。

- 重要又は緊急を要する監査指摘事項について、委員会の決定に基づき速やかに対応する。
- 総務省運用支援ＣＡの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、総務省運用支援ＣＡの運用を停止するか否かは委員会が決定する。
- 委員会は、監査指摘事項に対して総務省運用支援ＣＡが対策を実施したことを確認する。

### ２．７．６　監査結果

総務省運用支援ＣＡの監査結果は、監査人から総務省運用支援ＣＡ責任者に対して監査報告書として提出される。総務省運用支援ＣＡ責任者は、委員会に監査結果を報告する。

監査報告書は、５年間保管する。

## ２．８　機密保持

### ２．８．１　機密扱いとする情報

総務省運用支援ＣＡは、漏えいすることによって総務省運用支援ＣＡの認証業務の信頼性が損なわれるおそれのある情報を機密扱いとする。機密扱いとする情報は、当該情報を含む書類及び記録媒体の管理責任者を定め、安全に保管管理する。

### ２．８．２　機密扱いとしない情報

総務省運用支援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。

### ２．８．３　証明書失効情報の公表

総務省運用支援ＣＡが発行した証明書失効情報のうち公表するものは、次のとおりである。

- 自己署名証明書の失効情報
- サーバ証明書の失効情報
- コード署名証明書の失効情報

### ２．８．４　法執行機関への情報開示

規定しない。

### ２．８．５　民事手続上の情報開示

規定しない。

### ２．８．６　証明書利用者の要求に基づく情報の開示

規定しない。

### ２．８．７　その他の理由に基づく情報開示

規定しない。

## ２．９　知的財産権

規定しない。

## ３．識別と認証

### ３．１　初期登録

#### ３．１．１　名前の型

総務省運用支援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　名前の意味に関する要件

発行する証明書において使用する名前は、省、外局、部局又は機関、ドメインと名等が識別できる名称とする。

#### ３．１．３　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、原則として、ブリッジ認証局の定める規則を準用する。

#### ３．１．４　名前の一意性

総務省運用支援ＣＡの発行する証明書の主体者名は、一意に割り当てる。

#### ３．１．５　名前に関する紛争の解決手順

規定しない。

#### ３．１．６　商標の認識・認証・役割

規定しない。

#### ３．１．７　秘密鍵の所有を証明するための方法

総務省運用支援ＣＡは、サーバ証明書等を発行する場合、ＲＡにおいてサーバ証明書等用鍵ペアを生成し、可逆性非対称アルゴリズムを用いてサーバ証明書等を作成し、当該サーバ証明書等及び秘密鍵の対応関係に矛盾を生じさせず、外部記憶媒体に格納する。

#### ３．１．８　組織の認証

総務省運用支援ＣＡは、所定の手続に基づき、証明書の発行申請を行う者の所属する組織の真偽を確認する。

#### ３．１．９　個人の認証

総務省運用支援ＣＡは、所定の手続に基づき、証明書の発行申請を行う者の真偽を確認する。

### ３．２　証明書の更新

証明書更新時における識別及び認証は、「３．１　初期登録」に定める手続に基づいて行う。

３．３　証明書失効後の再発行

証明書失効後の再発行時における識別及び認証は、「３．１　初期登録」に定める手続に基づいて行う。

３．４　証明書の失効申請

証明書の失効時における識別及び認証は、「３．１．８　組織の認証」及び「３．１．９　個人の認証」において定める手続に基づいて行う。

## ４．運用要件

### ４．１　証明書の発行申請

#### ４．１．１　自己署名証明書

総務省運用支援ＣＡ責任者が、ＩＡ鍵管理者に対し発行指示を行う。

#### ４．１．２　相互認証証明書

規定しない。

#### ４．１．３　サーバ証明書及びコード署名証明書

サーバ証明書及びコード署名証明書の発行申請は、所定の手続に基づいて行う。

### ４．２　証明書の発行

#### ４．２．１　自己署名証明書

総務省運用支援ＣＡは、生成したＣＡ公開鍵に、自ＣＡの署名を付して自己署名証明書を発行する。

#### ４．２．２　相互認証証明書

規定しない。

#### ４．２．３　サーバ証明書及びコード署名証明書

総務省運用支援ＣＡは、生成したＣＡ公開鍵又は証明書発行要求に基づき発行するサーバ証明書にあっては当該証明書発行要求に含まれている公開鍵に、自ＣＡの署名を付してサーバ証明書等を発行する。

### ４．３　証明書の受入れ

#### ４．３．１　自己署名証明書

規定しない。

#### ４．３．２　相互認証証明書

規定しない。

#### ４．３．３　サーバ証明書及びコード署名証明書

総務省運用支援ＣＡは、発行したサーバ証明書及びコード署名証明書を所定の手続に基づき安全かつ確実な方法で申請者に配付し、受領書を受け取る。

### ４．４　証明書の失効及び一時停止

#### ４．４．１　証明書の失効理由

(1) 自己署名証明書

総務省運用支援ＣＡは、次の事由が発生した場合には、自己署名証明書を失効させる。

・　ＣＡ秘密鍵の紛失及び危殆化
・　自己署名証明書の更新（「４．７　鍵の更新」において定めるＣＡ鍵ペアの更新に伴うものを除く。）

(2) サーバ証明書及びコード署名証明書

総務省運用支援ＣＡは、次の事由が発生した場合には、サーバ証明書及びコード署名証明書を失効させる。

・　当該証明書の秘密鍵の紛失及び危殆化
・　ＣＡ秘密鍵の紛失及び危殆化
・　認証基準違反
・　サイトのドメイン名その他証明書記載事項の変更及び廃止
・　プログラムの変更及び廃止

４．４．２　証明書の失効申請者

(1) 自己署名証明書

自己署名証明書の失効申請は、総務省運用支援ＣＡ責任者が行う。

(2) 相互認証証明書

規定しない。

(3) サーバ証明書及びコード署名証明書

サーバ証明書及びコード署名証明書の失効申請は、当該証明書の管理者が行う。

４．４．３　証明書の失効申請及び失効処理手順

(1) 自己署名証明書

自己署名証明書を失効させ、ＡＲＬを発行し、ＡＲＬ及び自己署名証明書の失効情報をＷｅｂ上で公表する。

(2) 相互認証証明書

規定しない。

(3) サーバ証明書及びコード署名証明書

サーバ証明書及びコード署名証明書の失効申請が所定の手続に基づいていることを確認した後、当該証明書を失効させ、ＣＲＬを発行し、並びにＣＲＬ及び失効情報をＷｅｂ上で公表する。

当該証明書の管理者は、所定の手続に基づき、証明書を破棄するものとする。

４．４．４　失効における猶予期間

総務省運用支援ＣＡは、失効申請手続の終了後、直ちに失効処理を行う。

４．４．５　証明書の一時停止

総務省運用支援ＣＡは、証明書の一時停止を行わない。

４．４．６　一時停止申請者

規定しない。

４．４．７　一時停止手順

規定しない。

４．４．８　一時停止期間の制限

規定しない。

４．４．９　ＣＲＬ／ＡＲＬの発行周期

ＣＡ秘密鍵の危殆化等が生じた場合はＣＲＬ／ＡＲＬを直ちに発行する。

４．４．１０　ＣＲＬ／ＡＲＬの確認

証明書検証者は、総務省運用支援ＣＡの公表する失効情報によって証明書の有効性を確認しなければならない。このため、総務省運用支援ＣＡは、Ｗｅｂ上にＣＲＬ／ＡＲＬを公表する。

４．４．１１　オンライン有効性確認の可用性

規定しない。

４．４．１２　オンライン有効性確認要件

規定しない。

４．４．１３　その他利用可能な有効性確認手段

規定しない。

４．４．１４　その他利用可能な有効性確認手段における確認要件

規定しない。

４．４．１５　秘密鍵の危殆化に関する特別な要件

規定しない。

４．５　セキュリティ監査の手順

監査ログ検査者は、総務省運用支援ＣＡシステムにおける発生事象を記録したログ（以下「監査ログ」という。）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。

４．５．１　監査ログに記録する情報

総務省運用支援ＣＡシステム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、操作ログその他の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と時刻
・　各種処理事象の成功／失敗
・　事象発生元（オペレータ名、システム名等）

４．５．２　監査ログの検査周期

監査ログ検査者は、監査ログ及び業務実施記録等の照合を月次で行う。

４．５．３　監査ログの保管期間

監査ログの保管期間は、３年とする。

４．５．４　監査ログの保護

監査ログは、改ざん防止対策を講じ、かつ改ざん検出を可能とする。

監査ログのバックアップは、月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。

４．５．５　監査ログのバックアップ手順

監査ログは、日次でＣＡシステムのハードディスクに自動的にバックアップし、月次でこれを外部記憶媒体に手動により取得する。

４．５．６　監査ログの収集システム

監査ログの収集機能は、ＣＡ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。

４．５．７　監査ログ検査の通知

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。

４．５．８　脆弱性の評価

監査ログ検査者は、監査ログの検査結果から、運用面及びシステム面でセキュリティ上の脆弱性を評価する。

４．６　アーカイブ

４．６．１　アーカイブデータの種類

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
・　アクセスログ

４．６．２　アーカイブデータの保管期間

アーカイブデータは、30年間保管する。

４．６．３　アーカイブデータの保護

アーカイブデータには、アクセス制御を行うとともに、署名付与等の改ざん検出を可能とする措置を講ずる。

アーカイブデータのバックアップは、月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。

４．６．４　アーカイブデータのバックアップ手順

アーカイブデータは、日次でＣＡシステムのハードディスクに自動的にバックアップし、月次でこれを外部記憶媒体に手動により取得する。

４．６．５　アーカイブデータのタイムスタンプに関する要件

アーカイブデータには、レコード単位でタイムスタンプ（システムの日付と時刻）を付与する。

４．６．６　アーカイブデータの収集システム

規定しない。

４．６．７　アーカイブデータの検証

年１回、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行う。

４．７　鍵の更新

ＣＡ鍵ペアの更新間隔は、５年間とする。

ただし、公開鍵と秘密鍵の有効期間内に総務省運用支援ＣＡを廃止する場合は、この限りでない。

４．８　危殆化と災害からの復旧

４．８．１　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対処

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。

４．８．２　証明書を失効した場合の要件

発行した証明書の失効処理に当たっては、その失効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、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。

### ４．８．３　秘密鍵が危殆化した場合の対処

ＣＡ秘密鍵が危殆化した場合は、別に定めるところにより認証業務を停止し、次の手続を行う。

- サーバ証明書、コード署名証明書等の失効手続
- ＣＡ秘密鍵の廃棄及び再生成手続
- サーバ証明書、コード署名証明書等の再発行手続

また、証明書利用者の秘密鍵が危殆化した場合は、「４．４　証明書の失効及び一時停止」において定める手続に基づき、証明書の失効手続を行う。

### ４．８．４　災害等発生時の設備の確保

総務省ＣＡに準じる。

### ４．９　認証業務の終了

委員会において総務省ＣＡ又は、総務省運用支援ＣＡの認証業務の終了が決定した場合は、業務終了の90日前までに、証明書利用者及び証明書検証者に対し、業務終了の事実並びに業務終了後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告知し、所定の業務終了手続を行う。

## ５．物理面、手続面及び人事面のセキュリティ管理

### ５．１　物理的管理

#### ５．１．１　施設の位置と建物構造

総務省ＣＡに準じる。

#### ５．１．２　物理的アクセス

総務省ＣＡに準じる。

#### ５．１．３　電源設備と空調設備

総務省ＣＡに準じる。

#### ５．１．４　水害対策

総務省ＣＡに準じる。

#### ５．１．５　地震対策

総務省ＣＡに準じる。

#### ５．１．６　火災防止対策

総務省ＣＡに準じる。

#### ５．１．７　媒体管理

アーカイブデータ及びバックアップデータを含む媒体は、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　廃棄物処理

機密扱いとする情報を含む書類及び記録媒体の廃棄については、所定の手続に基づいて適切に廃棄処理を行う。

#### ５．１．９　オフサイトバックアップ

規定しない。

### ５．２　手続面の管理

サーバ証明書等の発行、更新、失効等の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。

重要な業務の指示は、総務省運用支援ＣＡ責任者が各操作員に対して作業指示書によって指示する。

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。

各要員の業務を次のとおり定める。

(1) 総務省運用支援ＣＡ責任者

総務省運用支援ＣＡ責任者は、総務省運用支援ＣＡの運営全般に関する責任者であり、次の業務を行う。総務省運用支援ＣＡ責任者は、総務省ＣＡ責任者をもって充てる。

- 総務省運用支援ＣＡ運営方針の策定
- 認証業務運用の統括
- 各種規程及び手続の維持管理
- ＣＡ秘密鍵の危殆化発生時、災害発生等緊急時における対応の統括
- ＩＡ操作員、ＲＡ操作員等への作業指示及び結果確認
- その他総務省運用支援ＣＡの運営及び運用に関する統括

(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。ＩＡ鍵管理者は、総務省ＣＡのＩＡ鍵管理者をもって充てる。なお、操作は複数人のＩＡ鍵管理者が行う。

- 管理鍵の保管管理
- ＣＡ鍵ペアの生成
- ＣＡ秘密鍵のバックアップ媒体の保管管理
- ＣＡ秘密鍵生成、自己署名証明書発行時におけるＨＳＭに対する鍵操作
- ＣＡ秘密鍵のバックアップ及びバックアップからのリストア
- 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に対する鍵操作及びＣＡ秘密鍵のバックアップのセット

(3) ＩＡ操作員

ＩＡ操作員は、総務省運用支援ＣＡシステムに直接ログインする権限を有し、総務省運用支援ＣＡ責任者の指示により、総務省運用支援ＣＡ秘密鍵を用いた次の業務を行う。ＩＡ操作員は、総務省ＣＡのＩＡ操作員をもって充てる。なお、操作は、複数人のＩＡ操作員が行う。

- ＣＡ秘密鍵（ＨＳＭ）の活性化・非活性化
- 総務省運用支援ＣＡシステムの起動及び停止
- 総務省運用支援ＣＡシステムの動作に関する設定変更管理
- 総務省運用支援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及びマニュアル操作によるバックアップ及びリストア
- 自己署名証明書の発行処理
- ＡＲＬの発行処理

(4) 受付担当者

受付担当者は、次の業務を行う。受付担当者は、総務省ＣＡの受付担当者をもって充てる。

- サーバ証明書等の発行申請の受付

・　申請者との連絡調整
・　申請書類等の管理

(5) 審査担当者

審査担当者は、サーバ証明書等の発行申請の審査業務を行う。審査担当者は、総務省ＣＡの審査担当者をもって充てる。

(6) ＲＡ操作員

ＲＡ操作員は、総務省運用支援ＣＡ責任者の指示により、総務省運用支援ＣＡが発行する証明書に関し次の業務を行う。ＲＡ操作員は、総務省ＣＡのＲＡ操作員をもって充てる。なお、操作は複数人のＲＡ操作員が行う。

・　ＲＡサーバの起動及び停止
・　ＲＡサーバの動作に関する設定変更管理
・　サーバ証明書、コード署名証明書等の発行、更新及び失効処理
・　操作員等への証明書の発行、更新及び失効処理
・　ＲＡサーバのバックアップ及びリストア
・　ＣＲＬの発行処理

(7) 監査ログ検査者

監査ログ検査者は、総務省運用支援ＣＡシステムのログに関し次の業務を行う。監査ログ検査者は、総務省ＣＡの監査ログ検査者をもって充てる。

・　監査ログの検査
・　不要な監査ログの削除等

５．３　人事面の管理

総務省運用支援ＣＡの業務に従事する者の適格性の審査、教育、配置転換の実施及び規則違反に対する罰則の適用については、国家公務員法等の人事関係法令に準じて運用する。また、総務省運用支援ＣＡの業務に従事する者には、総務省運用支援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。

## ６．技術的セキュリティ管理

### ６．１　鍵ペア生成とインストール

#### ６．１．１　鍵ペア生成

ＣＡ鍵ペアは、複数人のＩＡ鍵管理者がFIPS140-1レベル3相当のＨＳＭを用いて生成し、サーバ証明書等（証明書発行要求に基づき発行するものを除く。）の鍵ペアは、ＲＡ操作員がＲＡサーバにおいて生成する。

総務省運用支援ＣＡ及びサーバ証明書等の秘密鍵の更新は、同一アルゴリズム及び同一鍵長で鍵生成を行い、変更はアルゴリズム又は鍵長を変更して鍵生成を行う。

#### ６．１．２　証明書利用者への秘密鍵配付

サーバ証明書（証明書発行要求に基づき発行するものを除く。）及びコード署名証明書の秘密鍵は、ＲＡ操作員が外部記憶媒体に格納し、受付担当者が申請者に手渡しで配付する。秘密鍵が記録されるファイルに関しては、ＲＡ操作員が生成する時点で、パスワードを設定する。このとき、媒体を配付した事項に対する履歴を管理する。

#### ６．１．３　公開鍵の受領

総務省運用支援ＣＡは、サーバ証明書発行要求の受領において、サーバ証明書の公開鍵を安全かつ確実に受け取る。

#### ６．１．４　ＣＡ公開鍵の配付

総務省運用支援ＣＡ内の証明書利用者及び証明書検証者に安全かつ確実な手段で配付する。

#### ６．１．５　鍵のサイズ

ＣＡ鍵は、RSA2048ビットの鍵を使用し、サーバ証明書等の鍵は、RSA1024ビットの鍵を使用する。

鍵ペアの生成を伴わない証明書発行要求のために、申請者側で生成する鍵ペアについても、RSA1024ビットで生成する。

#### ６．１．６　公開鍵パラメータの生成

規定しない。

#### ６．１．７　公開鍵パラメータの品質の検査

規定しない。

#### ６．１．８　鍵を生成するハードウェア及びソフトウェア

「６．１．１　鍵ペア生成」において定める。

６．１．９　鍵の利用目的

ＣＡ秘密鍵及びコード署名証明書の秘密鍵は、署名に用いる。

サーバ証明書の秘密鍵は、暗号化通信（ＳＳＬ）に用いる。

６．２　秘密鍵の保護

６．２．１　暗号モジュールに関する基準

ＣＡ秘密鍵は、FIPS140-1レベル3相当以上のＨＳＭにより保護する。また、バックアップ以外の目的でハードディスク等の外部記憶装置への秘密鍵の出力は行わない。

６．２．２　秘密鍵の複数人制御

ＣＡ秘密鍵を使用する操作は、複数人のＩＡ鍵管理者が行う。また、バックアップ等及びリカバリの操作についても同様に複数人のＩＡ鍵管理者が行う。

６．２．３　秘密鍵の預託

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鍵管理者が行う。この場合、ＣＡ秘密鍵を暗号化し、複数に分割した後、複数人のＩＡ鍵管理者によって安全に保管される。

６．２．５　秘密鍵のアーカイブ

秘密鍵のアーカイブは行わない。

６．２．６　暗号モジュールへの秘密鍵の格納

ＣＡ秘密鍵は、複数人のＩＡ鍵管理者が暗号モジュールの中で生成し、格納する。

６．２．７　秘密鍵の活性化方法

ＣＡ秘密鍵は、複数人のＩＡ操作員により管理鍵を用いて活性化する。

サーバ証明書等の秘密鍵は、当該証明書の管理者が所定の方法に従い活性化する。

６．２．８　秘密鍵の非活性化方法

ＣＡ秘密鍵は、複数人のＩＡ操作員により管理鍵を用いて非活性化する。

サーバ証明書等の秘密鍵は、当該証明書の管理者が所定の方法に従い非活性化する。

６．２．９　秘密鍵の破棄方法

ＣＡ秘密鍵の破棄は、複数人のＩＡ鍵管理者がＨＳＭを初期化することによって行う。これを室外に持ち出す場合は、物理的にＨＳＭを破壊する。

また、破棄するＣＡ秘密鍵をバックアップした媒体を室外へ持ち出す場合は、物理的に媒体を破壊する。

サーバ証明書等の秘密鍵の破棄は、所定の手続に従い破棄する。

## ６．３　公開鍵の履歴保管及び鍵ペアの有効期間

### ６．３．１　公開鍵の履歴保管

公開鍵は、証明書のアーカイブに含まれ、「４．６．２　アーカイブデータの保管期間」において定義された期間保管する。

### ６．３．２　公開鍵及び秘密鍵の有効期間

公開鍵及び秘密鍵の有効期間は、次のとおりとする。

- 総務省運用支援ＣＡの公開鍵及び秘密鍵　有効とする日から起算して10年とし、５年ごとに鍵更新。ただし、公開鍵と秘密鍵の有効期間内に総務省運用支援ＣＡを廃止する場合は、この限りでない
- サーバ証明書及びコード署名証明書の公開鍵及び秘密鍵　有効とする日から起算して３年

なお、暗号のセキュリティが脆弱になった場合は、その時点で鍵ペアの変更を行う場合がある。

## ６．４　活性化データ

### ６．４．１　活性化データの生成とインストール

(1) ＣＡ鍵

ＣＡ秘密鍵を格納するＨＳＭの操作は、パスワードと複数の管理鍵により行う。ＨＳＭの操作を行うためのパスワードは、ＩＡ鍵管理者が決定し、入力する。

(2) サーバ証明書鍵及びコード署名証明書鍵

サーバ証明書及びコード署名証明書の秘密鍵を記録するファイルを活性化するためのパスワードは、ＲＡ操作員が設定する。

### ６．４．２　活性化データの保護

(1) ＣＡ鍵

ＣＡ秘密鍵を格納するＨＳＭの活性化に必要なパスワードは、定期的に変更し、管理鍵は安全に保管する。

(2) サーバ証明書鍵及びコード署名証明書鍵

サーバ証明書等の秘密鍵を記録するファイルの活性化に必要なパスワードは、ＲＡ操作員が安全に保持し、申請者にのみ伝達する。

## ６．５　コンピュータセキュリティ管理

### ６．５．１　コンピュータセキュリティ技術要件

総務省運用支援ＣＡシステムには、アクセス制御機能、操作員の識別及び認証機能、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　システムのライフサイクルにおけるセキュリティ管理

### ６．６．１　システム開発面における管理

総務省ＣＡに準じる。

### ６．６．２　システム運用面における管理

総務省ＣＡに準じる。

### ６．６．３　セキュリティ評価の基準

規定しない。

## ６．７　ネットワークセキュリティ管理

規定しない。

## ６．８　暗号モジュールの技術管理

「６．１．１　鍵ペア生成」及び「６．２．１　暗号モジュールに関する基準」において定める。

## ７．証明書とＣＲＬ／ＡＲＬのプロファイル

### ７．１　証明書のプロファイル

各証明書の形式は、X.509 version3 に従う。

#### ７．１．１　自己署名証明書

| 項目 | Critical | 内容 | 備考 |
|---|---|---|---|
| バージョン<br>version | ― | 2 | 2はX.509V3証明書を表す。 |
| 発行番号<br>serialNumber | ― | 例：123456789 | 同一ＣＡが発行する証明書内でユニークな値にしなければならない。 |
| 署名<br>signature | ― | 1.2.840.113549.1.1.5<br>(sha1WithRSAEncryption) | |
| 有効期限<br>validity | ― | NotBefore UTCTime 010331150000Z<br>(例：2001年4月1日(日本時間))<br>NotAfter UTCTime 110331150000Z<br>(例：2011年3月31日(日本時間)) | 2049年まではUTCTime で表現し、2050年以降はGeneralizedTime で表現する。 |
| 発行者名<br>issuer | ― | C = JP<br>O = Japanese Government<br>OU = MPHPT<br>OU = MPHPT Certification Authority | PrintableString により記述する。 |
| 所有者名<br>subject | ― | C = JP<br>O = Japanese Government<br>OU = MPHPT<br>OU = MPHPT Certification Authority | PrintableString により記述する。 |
| 所有者の公開鍵情報<br>subjectPublicKeyInfo | ― | 1.2.840.113549.1.1.1(RSAEncryption)<br>+<br>公開鍵のビット列 | |
| 標準拡張項目 | Critical | 内容 | 備考 |
| 認証局鍵識別<br>authorityKeyIdentifier | FALS | 例：0123456789abcdef0123 | 認証局公開鍵のSHA-1ハッシュ値を表わす。 |
| 所有者鍵識別<br>subjectKeyIdentifier | FALSE | 例：abcdef0123456789abcd | 所有者公開鍵のSHA-1ハッシュ値を表している。 |
| 鍵の利用目的<br>keyUsage | FALSE | keyCertSign,cRLSign | 鍵の用途目的<br>証明書および失効リストの発行 |
| 基本制約<br>basicConstraints | FALSE | CA=TRUE | ＣＡ証明書であることを記載する。 |
| 発行者署名<br>issuer's signature | | 1.2.840.113549.1.1.5<br>(sha1WithRSAEncryption) | 運用支援ＣＡのデジタル署名 |
| 証明書使用目的（ネットスケープ用） | FALSE | Bit-5(SSL　CA)　と　bit-7(Object Signing CA)を1、残りを0 | BIT STRING型 |

| | | | |
|---|---|---|---|
| netscape-cert-type | | | |

７．１．２　サーバ証明書

| 項目 | Critical | 内容 | 備考 |
|---|---|---|---|
| バージョン<br>version | ― | 2 | 2はX.509V3証明書を表す。 |
| 発行番号<br>serialNumber | ― | 例：123456789 | 同一CAが発行する証明書内でユニークな値にしなければならない。 |
| 署名<br>signature | ― | 1.2.840.113549.1.1.5<br>(sha1WithRSAEncryption) | |
| 有効期限<br>validity | ― | NotBefore UTCTime 0103311150000Z<br>(例：2001年4月1日(日本時間))<br>NotAfter UTCTime 0403311150000Z<br>(例：2004年3月31日(日本時間)) | 2049年まではUTCTime で表現し、2050年以降はGeneralizedTime で表現する。 |
| 発行者名<br>issuer | ― | C = JP<br>O = Japanese Government<br>OU = MPHPT<br>OU = MPHPT Certification Authority | PrintableString により記述する。 |
| 所有者名<br>subject | ― | C = JP<br>O = Japanese Government<br>OU = MPHPT<br>CN = xxx.yyy.go.jp | PrintableStringにより記述する。<br>CNは、総務省内Webサイトのドメイン名を示す。 |
| 所有者の公開鍵情報<br>subjectPublicKeyInfo | ― | 1.2.840.113549.1.1.1 (RSAEncryption)<br>+<br>公開鍵のビット列 | |
| 標準拡張項目 | Critical | 内容 | 備考 |
| 認証局鍵識別<br>authorityKeyIdentifier | FALSE | 例：0123456789abcdef0123 | 認証局公開鍵のSHA-1ハッシュ値を表わす。 |
| 所有者鍵識別<br>subjectKeyIdentifier | FALSE | 例：abcdef0123456789abcd | 所有者公開鍵のSHA-1ハッシュ値を表している。 |
| 鍵の利用目的<br>keyUsage | TRUE | DigitalSignature<br>keyEncipherment<br>DataEncipherment | |
| 発行者署名<br>issuer's signature | | 1.2.840.113549.1.1.5<br>(sha1WithRSAEncryption) | 運用支援CAのデジタル署名 |
| 証明書の利用目的(ネットスケープ用)<br>netscape-cert-type | FALSE | bit-1(SSL server)を1、残りを0 | BIT STRING型 |

７．１．３　コード署名証明書

| 項目 | Critical | 内容 | 備考 |
|---|---|---|---|
| バージョン<br>version | ― | 2 | 2はX.509V3証明書を表す。 |
| 発行番号<br>serialNumber | ― | 例：123456789 | 同一CAが発行する証明書内でユニークな値にしなければならない。 |
| 署名<br>signature | ― | 1.2.840.113549.1.1.5<br>(sha1WithRSAEncryption) | |
| 有効期限<br>validity | ― | NotBefore UTCTime 0103311150000Z<br>(例：2001年4月1日(日本時間))<br>NotAfter UTCTime 0403311150000Z<br>(例：2004年3月31日(日本時間)) | 2049年まではUTCTime で表現し、2050年以降はGeneralizedTime で表現する。 |
| 発行者名<br>issuer | ― | C = JP<br>O = Japanese Government<br>OU = MPHPT<br>OU = MPHPT Certification Authority | PrintableString により記述する。 |
| 所有者名<br>subject | ― | C = JP<br>O = Japanese Government<br>OU = MPHPT<br>CN = MPHPT(Soumu-sho) | PrintableString により記述する。 |
| 所有者の公開鍵情報<br>subjectPublicKeyInfo | ― | 1.2.840.113549.1.1.1 (RSAEncryption)<br>+<br>公開鍵のビット列 | |
| 標準拡張項目 | Critical | 内容 | 備考 |
| 認証局鍵識別<br>authorityKeyIdentifier | FALSE | 例：0123456789abcdef0123 | 認証局公開鍵のSHA-1ハッシュ値を表わす。 |
| 所有者鍵識別<br>subjectKeyIdentifier | FALSE | 例：abcdef0123456789abcd | 所有者公開鍵のSHA-1ハッシュ値を表している。 |
| 鍵の利用目的<br>keyUsage | FALSE | DigitalSignature | コード署名用として使用。 |
| 発行者署名<br>issuer's signature | | 1.2.840.113549.1.1.5<br>(sha1WithRSAEncryption) | 運用支援CAのデジタル署名 |
| 証明書の利用目的（ネットスケープ用）<br>netscape-cert-type | FALSE | bit-3(Object Signing)を1、残りを0 | BIT STRING型 |

## ７．２　ＣＲＬ／ＡＲＬのプロファイル

ＣＲＬ／ＡＲＬの形式は、X.509 version2 に従う。

### ７．２．１　ＣＲＬ

| フィールド | 意味 | 備考 |
|---|---|---|
| TbsCertList | | |
| Version | Version2を示す1 | |
| Signature | 署名アルゴリズム | |
| Issuer | CRLの発行者 | |
| ThisUpdate | CRLの発行日時 | 2049年まではUTCTime で表現し、2050年以降はGeneralizedTime で表現する。 |
| NextUpdate | 次回のCRLの発行日時 | 2049年まではUTCTime で表現し、2050年以降はGeneralizedTime で表現する。 |
| RevokedCertificates | 失効証明書 | |
| CertificateSerialNumber | 証明書のシリアル番号 | |
| RevocationDate | 失効日時 | |
| CrlEntryExtensions | 拡張領域 | |
| ReasonCode | 失効理由 | |
| CrlExtensions | 拡張領域 | |
| AuthorityKeyIdentifier | CRLの署名確認に用いる証明書の識別子 | |
| CRLNumber | CRLのシリアル番号 | |
| IssuingDistributionPoint | 発行する配付点 | |

７．２．２　ＡＲＬ

| フィールド | 意味 | 備考 |
|---|---|---|
| TbsCertList | | |
| Version | Version2を示す1 | |
| Signature | 署名アルゴリズム | |
| Issuer | ARLの発行者 | |
| ThisUpdate | ARLの発行日時 | 2049年まではUTCTime で表現し、2050年以降はGeneralizedTime で表現する。 |
| NextUpdate | 次回のARLの発行日時 | 2049年まではUTCTime で表現し、2050年以降はGeneralizedTime で表現する。 |
| RevokedCertificates | 失効証明書 | |
| CertificateSerialNumber | 証明書のシリアル番号 | |
| RevocationDate | 失効日時 | |
| CrlEntryExtensions | 拡張領域 | |
| ReasonCode | 失効理由 | |
| CrlExtensions | 拡張領域 | |
| AuthorityKeyIdentifier | ARLの署名確認に用いる証明書の識別子 | |
| CRLNumber | ARLのシリアル番号 | |
| IssuingDistributionPoint | 発行する配付点 | |

## ８．ＣＰ／ＣＰＳの管理

### ８．１　ＣＰ／ＣＰＳの変更手順

委員会は、本ＣＰ／ＣＰＳを必要に応じて変更する。

### ８．２　ＣＰ／ＣＰＳの公表と通知

委員会は、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。

### ８．３　ＣＰ／ＣＰＳ承認手順

総務省運用支援ＣＡのＣＰ／ＣＰＳは委員会の決定をもって有効なものとする。