環境省認証局運用管理規程（ＣＰ／ＣＰＳ）

平成１５年　２月２１日
環境省認証局運営委員会
（最終改正　平成20年　7月　2日）

目次

1. はじめに

本CP／CPSは、国民等と環境省との間の申請･届出等手続の電子化を実現するため、総務省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環境省認証局（以下「環境省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

環境省ＣＡは、官職に対して官職証明書を発行するとともにその他環境省ＣＡの運用に必要な証明書を発行し、ＢＣＡと相互認証証明書を取り交わす。

環境省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を環境省ＣＡの認証業務に関する運営方針として位置付ける。

1.2 識別

環境省CAの証明書ポリシの識別子は、次のとおりとする。

環境省CA相互認証証明書ポリシ：	0.2.440.100195.8.5.1.1.10
環境省CA相互認証テスト用証明書ポリシ：	0.2.440.100195.8.5.1.1.0
環境省CA官職証明書ポリシ：	0.2.440.100195.8.5.1.1.10

1．3 運営体制と証明書の適用範囲

1．3．1 CAの組織

環境省CAの運営体制は、図1．3－1のとおりである。

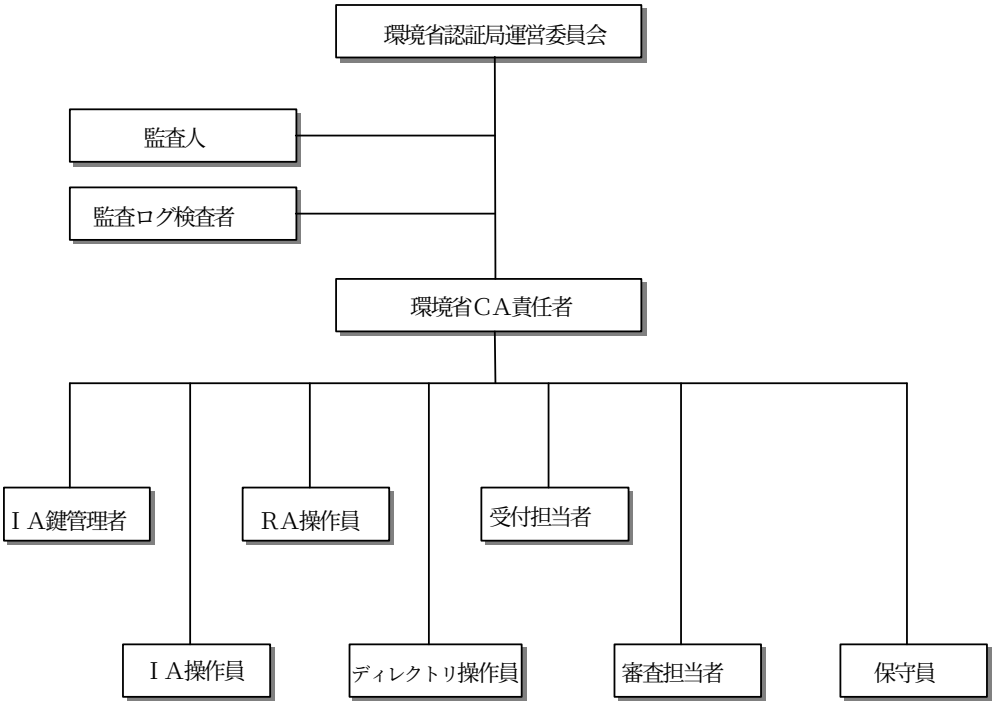

図1．3－1 環境省CAの運営体制

(1) 意思決定組織

環境省CAの運営に関する意思決定は、環境省CA運営委員会が行う。

環境省CA運営委員会の機能は次のとおりとする。

・ 環境省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
・ その他環境省CAの運営に関する重要事項の決定

(2) 環境省ＣＡ組織

BCAへの相互認証申請、環境省における官職証明書発行申請の受付及び審査並びに相互認証証明書、官職証明書等の発行、更新、失効等の運営業務は、環境省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。

1．3．2 証明書の適用範囲

BCAに対して相互認証証明書を発行する。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年とする。

官職に対して官職証明書を発行する。官職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 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、環境省大臣官房総務課環境情報室が行う。

1．4．2 照会窓口

本CP／CPSに関する照会は、環境省大臣官房総務課環境情報室を窓口とする。

2. 一般規定

2.1 義務

2.1.1 CA業務に関する義務

環境省CAは、CA業務に関して次の義務を負う。

- BCAへの相互認証申請に際して、正確な情報を提示する。
- 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、官職証明書等を発行する。
- 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。
- 証明書の失効処理を行い、有効期間48時間の失効リスト（以下「CRL／ARL」という。）を24時間ごとに発行する。
- CA秘密鍵を安全に管理する。
- CA秘密鍵が危殆化した場合は、速やかにBCA運営組織に報告する。
- 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データを必要な期間保管する。
- システムの稼動監視を行う。

2.1.2 RA業務に関する義務

環境省CAは、RA業務に関して次の義務を負う。

- 環境省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。
- 官職証明書の発行等の申請手続が適切に行われていることを確認する。

2.1.3 証明書利用者の義務

官職証明書の利用者は、次の義務を負う。

- 官職証明書は、法令に基づき本CP／CPSに従って利用する。
- 官職証明書及び官職の秘密鍵を安全に管理する。
- 官職証明書の管理は、環境省が規定する文書管理規程又は公印規程等に基づいて行う。
- 秘密鍵が危殆化した場合は、速やかに環境省CA組織に報告する。

2.1.4 証明書検証者の義務

官職証明書の証明書検証者は、次の義務を負う。

- 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

証する。

2.1.5 リポジトリに関する義務

環境省CAに関する情報のうち公表する情報は、BCAによって運用される統合リポジトリに複製する。

2.2 CAの責任

環境省CAは、自己署名証明書、リンク証明書、相互認証証明書、官職証明書等の発行、更新、失効、保管及び公表に当たっては、BCA、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

環境省CAに関する情報は、BCAの統合リポジトリ及びWeb上で公表する。

(1) BCAの統合リポジトリ上での公表

環境省CAは、環境省CAリポジトリに保有する次の情報をBCAの統合リポジ

トリに複製し、統合リポジトリ上で公表する。

・ 環境省CAが発行した自己署名証明書、リンク証明書、相互認証証明書、官職証明書等及びそのCRL／ARL

（2） Web上での公表

環境省CAは、次の情報をWeb上で公表する。

・ 環境省CAと相互認証したCAの名称及び相互認証を取消したCAの名称
・ 環境省CAが認証した官職の名称及び認証を取消した官職の名称
・ CA秘密鍵危殆化に関する情報
・ 本CP／CPS

2．6．2 公表の頻度

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、官職証明書等及びそのCRL／ARLは、発行及び更新の都度
・ 環境省CAと相互認証したCAの名称及び相互認証を取消したCAの名称は、環境省ＣA運営委員会による決定の都度
・ 環境省CAが認証した官職の名称及び認証を取消した官職の名称は、環境省ＣA運営委員会による決定の都度
・ 本CP／CPSの変更の都度

2．6．3 アクセス制御

環境省CAリポジトリから複製したBCAの統合リポジトリ上で公表する情報及びWeb上で公表する情報は、インターネットを通じて提供する。

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

環境省CAリポジトリに保有する情報のうち、「2 ．6 ．1 CAに関する情報の公表 （1） BCAの統合リポジトリ上での公表」において定める情報をBCAの統合リポジトリに複製し公表する。

2．7 準拠性監査

2．7．1 監査頻度

環境省CA組織は監査人による監査を年1回定期的に実施する。また、環境省CA組織は、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

環境省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

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

2．7．4 監査テーマ

認証業務が本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、並びに外部からの不正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を中心に監査を実施する。

2．7．5 監査指摘事項への対応

環境省CAは、重要又は緊急を要する監査指摘事項について、環境省CA運営委員会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、環境省CAの運用を停止するか否かは環境省CA運営委員会が決定する。また、環境省CA運営委員会は、監査指摘事項に対して環境省CAが対策を実施したことを確認する。

2．7．6 監査結果

環境省CAの監査結果は、監査人から環境省CA組織に対して監査報告書として提出される。環境省CA組織は、環境省CA運営委員会及びBCA運営組織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

環境省CAは、漏えいすることによって環境省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。機密扱いとする情報は、当該情報を含む書類及び記憶媒体の管理責任者を定め、安全に保管管理する。

2．8．2 機密扱いとしない情報

環境省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

環境省CAは、自己署名証明書、リンク証明書、相互認証証明書、官職証明書等の失効情報を公表する。

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

環境省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、府省、認証局、官職等の名称とする。

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、BCAの定める規則に従う。

3.1.4 名前の一意性

環境省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

環境省CA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。

官職証明書発行手続においては、環境省CA側で秘密鍵と公開鍵が対応する鍵ペアを生成する。

3.1.8 組織の認証

環境省CA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を運営する者の真偽を確認する。

3．1．9 個人の認証

環境省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と認証は、「3 ．1 初期登録」において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と認証は、「3 ．1 初期登録」において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と認証は、「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

(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。

(2) 官職証明書

官職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

(1) 相互認証証明書

環境省CA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

環境省CAは、環境省CA側で生成した公開鍵に、自CAの署名を付して官職証明書を発行する。

4.3 証明書の受入れ

(1) 相互認証証明書

環境省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

環境省CAは、発行した官職証明書を、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。この受領確認をもって官職証明書の受入れの完了とする。

4．4 証明書の失効と一時停止

4．4．1 証明書の失効理由

(1) 相互認証証明書

環境省CAは、環境省CA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

環境省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
・ CA秘密鍵の紛失、危殆化
・ 官職名の変更、廃止

4．4．2 証明書の失効申請者

(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から環境省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

環境省CAからBCAに対する失効申請は、環境省CAの責任者が行う。

(2) 官職証明書

官職証明書の失効申請は、官職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) 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

「3．1．8 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

官職証明書の失効申請を受け取った環境省CAは、そ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うえで、要求された官職証明書を失効し、CRLをBCAの統合リポジトリに複製する。

4.4.4 失効における猶予期間

環境省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 一時停止

環境省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

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。

4.4.10 CRL／ARLの確認

証明書検証者は、環境省CAの発行する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。環境省CAは、この確認が行えるようBCAの統合リポジトリ上でCRL／ARLを公表する。

4.4.11 オンライン有効性確認の可用性

統合リポジトリは、BCAが維持管理する。

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、環境省ＣＡシステム及び環境省CAリポジトリ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

環境省CAシステム及び環境省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）

4.5.2 監査ログの検査周期

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月次で行う。

4.5.3 監査ログの保管期間

監査ログは3年間保管する。

4．5．4 監査ログの保護

監査ログは、改ざん防止対策を施し、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、四半期ごと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

監査ログは日次でバックアップし、四半期ごとで外部記憶媒体に取得する。

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。

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

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、該当する証明書の有効期間満了日から10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、アクセス制御を施すとともに、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、四半期ごとで外部記憶

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、日次でバックアップし、四半期ごとで外部記憶媒体に取得する。

4．6．5 レコード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

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。

4．7 鍵更新

5年ごとにCA鍵ペアの更新を行う。

ただし、公開鍵と秘密鍵の有効期間内に環境省CAを廃止する場合は、この限りではない。

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、BCAの統合リポジトリ上で公表する。

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 証明書を失効する場合の要件

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、危機管理計画に基づいて認証業務を停止し、次の手続を行う。

・ 相互認証証明書、官職証明書等の失効手続
・ 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。

4．8．4 災害等発生時の設備の確保

災害等により環境省CAの設備が被害を受けた場合は、予備機を確保しバックアップデータを用いて運用を行う。

4．9 認証業務の終了

環境省ＣＡ運営委員会において、環境省CAの認証業務の終了が決定した場合は、業務終了の事実、並びに業務終了後の環境省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。

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

環境省CA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

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 手続面の管理」において定める各要員の業務に応じて環境省CA責任者が付与する。

環境省CA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 電源設備と空調設備

環境省CA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

環境省CA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

環境省CA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 火災対策

環境省CA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 媒体管理

アーカイブデータ、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･記憶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

重要なデータ等の媒体を別地保管するに当たっては、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は環境省CAの施設と同等のセキュリティ対策を講ずる。

5．2 手続面の管理

相互認証証明書、官職証明書等の発行、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、環境省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) 環境省ＣＡ責任者

環境省ＣＡ責任者は、環境省CAの運営に関する責任者であり、次の業務を行う。

- 環境省CA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
- IA操作員、ＲＡ操作員等への作業指示及び作業結果の確認
- その他環境省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。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。）の保管管理
- 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のHSMに対する鍵操作
- CA秘密鍵の更新時におけるHSMに対する鍵操作
- 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、官職証明書等の発行申請の受付、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、官職証明書等の発行申請の審査業務を行う。

(5) IA操作員

IA操作員は、環境省CA責任者の指示により、CA秘密鍵を使用する業務、および環境省CAシステムの設定と管理に係わる次の業務を行う。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
- 環境省CAシステムの起動･停止
- 環境省CAシステムの動作に関する設定変更管理
- 環境省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
- 証明書ポリシの設定登録、変更
- 自己署名証明書、リンク証明書、相互認証証明書の発行、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

(6) RA操作員

RA操作員は、環境省CA責任者の指示により、環境省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RA操作員が行う。

- 官職証明書等の発行、更新及び失効処理

(7) ディレクトリ操作員

ディレクトリ操作員は、環境省CAリポジトリの設定管理に関する業務を行う。

(8) 監査ログ検査者

監査ログ検査者は、環境省CAシステム及び環境省CAリポジトリのログ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

5．3 人事面の管理

環境省CA要員の適格性審査、教育、配置転換等については、国家公務員法等人事関係法令等に基づいて運用する。また、すべての要員には、環境省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

(1) CA鍵

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を用いて生成する。

(2) 官職証明書鍵

官職証明書の鍵ペアは、RA操作員が環境省CAシステムのソフトウェアを用いて生成する。

6.1.2 証明書利用者への秘密鍵配付

官職証明書の秘密鍵は、「6．2．1 暗号モジュールに関する基準」において定める暗号モジュールに格納し、所定の手続に基づいて配付する。

6.1.3 公開鍵の受領

環境省CA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。

6.1.4 CA公開鍵の配付

環境省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

(1) CA鍵

RSA2048ビットの鍵を使用する。

(2) 官職証明書鍵

RSA1024ビットの鍵を使用する。

6.1.6 公開鍵のパラメータの生成

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／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

(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。

6．2 秘密鍵の保護

6．2．1 暗号モジュールに関する基準

(1) CA鍵

CA秘密鍵は、FIPS140-1 レベル3 相当の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、FIPS140-1 レベル2 相当以上のICカードにより保護する。

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。

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。

HSMからバックアップしたCA秘密鍵は、暗号化して複数に分割し、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

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

(1) CA鍵

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。

(2) 官職証明書鍵

官職証明書の秘密鍵は、RA操作員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

(1) CA鍵

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。

(2) 官職証明書鍵

官職証明書の秘密鍵は、官職証明書の管理者によりPIN（Personal Identification Number）を用いて活性化する。

6．2．8 秘密鍵の非活性化方法

(1) CA鍵

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。

(2) 官職証明書鍵

官職証明書の秘密鍵は、官職証明書の管理者がICカードリーダからICカードを抜き出すことにより非活性化する。

6．2．9 秘密鍵の破棄方法

(1) CA鍵

HSM内の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。なお、初期化したHSMを室外に持ち出す場合は、物理的に

HSMを破壊する。

また、バックアップ媒体内のCA秘密鍵の破棄は、複数人のIA鍵管理者が媒体を初期化することによって行う。なお、初期化したバックアップ媒体を室外に持ち出す場合は、物理的にバックアップ媒体を破壊する。

(2) 官職証明書鍵

官職証明書の秘密鍵は、所定の手続に従い破棄する。

6．3 公開鍵の履歴保管と鍵ペアの有効期間

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」において定める期間、保管する。

6．3．2 公開鍵と秘密鍵の有効期間

(1) CA鍵

環境省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、公開鍵と秘密鍵の有効期間内に環境省CAを廃止する場合は、この限りでない。

また、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、HSMに入力する。

(2) 官職証明書鍵

官職証明書の秘密鍵を格納するICカードの初期PIN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) 官職証明書鍵

官職証明書の秘密鍵を格納するICカードの活性化に必要なPINは定期的に変更し、安全に保管する。

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機能要件

環境省CA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 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

環境省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、環境省CA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 システム運用面における管理

環境省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。

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

環境省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。

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

⑴ 自己署名証明書

表7－1 自己署名証明書

領域名	ｸﾘﾃｨｶﾙﾌﾗｸﾞ	値(例)	説明
version (バージョン番号)		2	v3、整数
serial Number (シリアル番号)		10001(例)	証明書のシリアル番号、整数
signature algorithm ID (署名アルゴリズム)			環境省 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="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	環境省CA発行者識別名(DN)、英語表記 UTF8String(Country 属性は PrintableString)
validity period (証明書有効期間)			証明書の有効期間
notBefore (発行日)		YYMMDDHHMMSSZ 010401000000Z	証明書の発行日 UTCTime
notAfter (終了日)		YYMMDDHHMMSSZ 110401000000Z	証明書の終了日 UTCTime
subject name (主体者名)		ou="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	環境省CA発行者識別名(DN)、英語表記 UTF8String(Country 属性は PrintableString)
subject public key info (主体者公開鍵情報)			環境省CA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	環境省CA公開鍵アルゴリズム識別子、RSAEncryption
parameter (パラメータ)		NULL	RSAの場合値なし
public key (公開鍵)		BIT STRING	環境省CA公開鍵の値、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	環境省CAの公開鍵のsha-1ハッシュ値
subjectKeyIdentifier (主体者鍵識別子)	FALSE	OCTET STRING	主体者公開鍵のsha-1ハッシュ値
keyUsage (鍵用途)	TRUE		鍵用途の目的を指定
keyCertSign		1	証明書の署名検証用
cRLSign		1	失効情報の署名検証用
issuerAltName (発行者代替名)	FALSE	ou=環境省認証局, ou=環境省, o=日本国政府, c=JP	環境省CAの日本語表示名を示す。 UTF8String(Country 属性はPrintableString)
subjectAltName (主体者代替名)	FALSE	ou=環境省認証局, ou=環境省, o=日本国政府, c=JP	環境省CAの日本語表示名を示す。 UTF8String(Country 属性はPrintableString)
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する
cA		cA=TRUE	
cRLDistributionPoints (CRL配布点)	FALSE	cn=arl, ou="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	directoryNameにてCRL/ARLの配布点を指定 UTF8String(Country 属性はPrintableString)
issuer's signature (発行者署名)			環境省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)		

⑵ 相互認証証明書

表7－2 相互認証証明書

領域名	ｸﾘﾃｨｶﾙﾌﾗｸﾞ	値(例)	説明
version (バージョン番号)		2	v3、整数
serial Number (シリアル番号)		10002(例)	証明書のシリアル番号、整数
signature algorithm ID (署名アルゴリズム)			環境省 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="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	環境省CA発行者識別名(DN)、英語表記 UTF8String(Country 属性はPrintableString)
validity period (証明書有効期間)			証明書の有効期間
notBefore (発行日)		YYMMDDHHMMSSZ 010401000000Z	証明書の発行日 UTCTime
notAfter (終了日)		YYMMDDHHMMSSZ 060401000000Z	証明書の終了日 UTCTime
subject name (主体者名)		ou="Bridge CA", o="Japanese Government", c=JP	BCA識別名(DN)、英語表記 証明書発行要求に指定された値とエンコードタイプ
subject public key info (主体者公開鍵情報)			BCA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	BCA公開鍵アルゴリズム識別子、RSAEncryption
parameter (パラメータ)		NULL	RSAの場合値なし
public key (公開鍵)		BIT STRING	BCA公開鍵の値、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	環境省CAの公開鍵のsha-1ハッシュ値
subjectKeyIdentifier (主体者鍵識別子)	FALSE	OCTET STRING	BCA公開鍵のsha-1ハッシュ値

keyUsage (鍵用途)	TRUE		鍵用途の目的を指定
keyCertSign		1	証明書の署名検証用
cRLSign		1	失効情報の署名検証用
certificatePolicies (証明書ポリシ)	TRUE		パス検証ソフトは、この処理を必須とし、処理が不可能な場合はこの証明書を排除する。
policyIdentifier			OID
certPolicyId		0.2.440.100195.8.5.1.1.10	電子署名ポリシ識別子 id-env-cp-ds.class10
policyQualifiers			ポリシ修飾子(CP/CPSへのポインターまたはユーザ通知情報)
policyQualifierId		id-qt-cps	CP/CPS
qualifier		http://www.env.go.jp	公開するCPSのURI 。IA5ストリング
policyMappings (ポリシマッピング)	FALSE		発行者ポリシと主体者ポリシを等価と見なす。
issuerDomainPolicy		0.2.440.100195.8.5.1.1.10	環境省CAのﾄﾞﾒｲﾝ･ﾎﾟﾘｼOID
subjectDomainPolicy		0.2.440.100145.8.1.1.1.10	BCAのﾄﾞﾒｲﾝ･ﾎﾟﾘｼOID
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する
cA		cA=TRUE	
policyConstraints (ポリシ制約)	TRUE		認証パス処理でポリシマッピング処理をするパス長を指定
requireExplicitPolicy		0	ポリシの明示を要求
inhibitPolicyMapping		1	ポリシマッピング禁止
cRLDistributionPoints (CRL配布点)	FALSE	cn=arl, ou="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	directoryName にて CRL/ARLの配布点を指定 UTF8String(Country 属性はPrintableString)
issuer's signature (発行者署名)			環境省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)		

⑶ 官職証明書

表7－3 官職証明書

領域名	ｸﾘﾃｨｶﾙﾌﾗｸﾞ	値(例)	説明
version (バージョン番号)		2	v3、整数
serial Number (シリアル番号)		10010(例)	証明書のシリアル番号、整数
signature algorithm ID (署名アルゴリズム)			環境省 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="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	環境省CA発行者識別名(DN)、英語表記 UTF8String(Country 属性は PrintableString)
validity period (証明書有効期間)			証明書の有効期間
notBefore (発行日)		YYMMDDHHMMSSZ 010401000000Z	証明書の発行日 UTCTime
notAfter (終了日)		YYMMDDHHMMSSZ 040401000000Z	証明書の終了日 UTCTime
subject name (主体者名)		cn="Chief of Office of Environmental Information", ou="Office of Environmental Information", ou="General Affairs Division", ou="Minister's Secretariat", ou="Ministry of the Environment", o="Japanese Government", c=JP	官職の識別名(DN)、英語表記 cn=役職名,…c=jp (例は大臣官房総務課環境情報室長) UTF8String(Country 属性は PrintableString)
subject public key info (主体者公開鍵情報)			官職証明書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	官職証明書公開鍵アルゴリズム識別子、RSAEncryption
parameter (パラメータ)		NULL	RSAの場合値なし
public key (公開鍵)		BIT STRING	官職証明書公開鍵の値、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	環境省CAの公開鍵のsha-1ハッシュ値
subjectKeyIdentifier (主体者鍵識別子)	FALSE	OCTET STRING	官職証明書公開鍵のsha-1ハッシュ値
keyUsage (鍵用途)	TRUE		鍵用途の目的を指定
digitalSignature		1	デジタル署名検証用
nonRepudiation		1	否認防止
certificatePolicies (証明書ポリシ)	TRUE		パス検証ソフトは、この処理を必須とし、処理が不可能な場合はこの証明書を排除する。
policyIdentifier			OID
certPolicyId		0.2.440.100195.8.5.1.1.10	官職証明書ポリシ識別子 id-env-cp-ds.class10
policyQualifiers			ポリシ修飾子(CP/CPSへのポインターまたはユーザ通知情報)
policyQualifierId		id-qt-cps	CP/CPS
qualifier		http://www.env.go.jp	公開するCP/CPSのURI 。IA5ストリング
issuerAltName (発行者代替名)	FALSE	ou=環境省認証局, ou=環境省, o=日本国政府, c=JP	環境省CAの日本語表示名を示す。 UTF8String(Country 属性はPrintableString)
subjectAltName (主体者代替名)	FALSE	cn=環境情報室長, ou=環境情報室,ou=総務課, ou=大臣官房,ou=環境省, o=日本国政府,c=JP	官職の日本語表示名を示す。(例は大臣官房総務課環境情報室長) UTF8String(Country 属性はPrintableString)
cRLDistributionPoints (CRL 配布点)	FALSE	cn=crl, ou="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	directoryName にてCRL/ARLの配布点を指定 UTF8String(Country 属性はPrintableString)
issuer's signature (発行者署名)			環境省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)		

⑷ リンク証明書

表7－4 リンク証明書

領域名	ｸﾘﾃｨｶﾙﾌﾗｸﾞ	値(例)	説明
version (バージョン番号)		2	v3、整数
serial Number (シリアル番号)		10002(例)	証明書のシリアル番号、整数
signature algorithm ID (署名アルゴリズム)			環境省 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="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	環境省CA発行者識別名(DN)、英語表記 UTF8String(Country 属性は PrintableString)
validity period (証明書有効期間)			証明書の有効期間
notBefore (発行日)		YYMMDDHHMMSSZ 010401000000Z	証明書の発行日。 UTCTime OldWithNew:旧世代の鍵ペアを作成した日時 NewWithOld:新世代の鍵ペアを生成した日時
notAfter (終了日)		YYMMDDHHMMSSZ 060331000000Z	証明書の終了日。 UTCTime OldWithNew:旧世代の自己署名証明書の有効期限 NewWithOld:少なくとも旧世代の鍵で最後に発行した証明書の有効期限
subject name (主体者名)		ou="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	環境省CA発行者識別名(DN)、英語表記 UTF8String(Country 属性は PrintableString)
subject public key info **(主体者公開鍵情報)**			環境省CA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	環境省CA公開鍵アルゴリズム識別子、RSAEncryption
parameter **(パラメータ)**		NULL	RSAの場合値なし
public key **(公開鍵)**		BIT STRING	環境省CA公開鍵の値、BITストリング OldWithNew:旧世代の公開鍵 NewWithOld:新世代の公開鍵

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	OldWithNew：新世代の鍵の識別子、sha-1ハッシュ値 NewWithOld：旧世代の鍵の識別子、sha-1ハッシュ値
subjectKeyIdentifier (主体者鍵識別子)	FALSE	OCTET STRING	OldWithNew：旧世代の鍵の識別子、sha-1ハッシュ値 NewWithOld：新世代の鍵の識別子、sha-1ハッシュ値
keyUsage (鍵用途)	TRUE		鍵用途の目的を指定
keyCertSign		1	ビット5、証明書の署名検証用
cRLSign		1	ビット6、失効情報の署名検証用
certificatePolicies (証明書ポリシ)	FALSE		証明書ポリシ
policyIdentifier			OID
certPolicyId		2.5.29.32.0	ANY-POLICY
issuerAltName (発行者代替名)	FALSE	ou=環境省認証局, ou=環境省, o=日本国政府, c=JP	環境省CAの日本語表示名を示す。 UTF8String(Country 属性はPrintableString)
subjectAltName (主体者代替名)	FALSE	ou=環境省認証局, ou=環境省, o=日本国政府, c=JP	環境省CAの日本語表示名を示す。 UTF8String(Country 属性はPrintableString)
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する
cA		cA=TRUE	
cRLDistributionPoints (CRL配布点)	FALSE	cn=arl, ou="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	directoryName にてCRL/ARL の配布点を指定 UTF8String(Country 属性は PrintableString)
issuer's signature (発行者署名)			環境省CAのデジタル署名 OldWithNew：新世代の鍵による署名 NewWithOld：旧世代の鍵による署名
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 CRL／ARLのプロファイル

⑴ CRL

表7－5 CRL

領域名	ｸﾘﾃｨｶﾙﾌﾗｸﾞ	値(例)	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			
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer (発行者)		ou="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	環境省CA発行者識別名(DN)、英語表記 UTF8String(Country 属性はPrintableString)
thisUpdate (今回の更新日)		YYMMDDHHMMSSZ 010501000000Z	今回の更新日時 UTCTime
nextUpdate (次回の更新日)		YYMMDDHHMMSSZ 010502000000Z	次回の更新日時 UTCTime
revokedCertificates (失効した証明書)			失効される証明書エントリ (以下の組のリスト)
userCertificate		10002 (例)	失効された証明書を整数で指定
revocationDate		YYMMDDHHMMSSZ 010501000000Z	失効日時 UTCTime
crlEntryExtensions (失効証明書エントリ拡張)			(失効証明書ごとの拡張領域)
reasonCode			理由コード
unspecified	FALSE		[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			[5] 業務の停止
certificateHold			[6] 証明書の保留
removeFromCRL			[8] CRLの削除(使用しない)

↓			
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		署名鍵の識別、証明書拡張と同じ形式
keyIdentifier		OCTET STRING	環境省CA公開鍵のsha-1ハッシュ値
cRLNumber (CRL 番号)	FALSE	32 (例)	シーケンス番号、整数
IssuingDistributionPoint (発行する配布点)	TRUE	cn=crl, ou="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	directoryNameにてCRL/ARLの配布点を指定 UTF8String(Country 属性はPrintableString)
onlyContainsUserCerts		TRUE	
	ENCRYPTED (署名値)		

(2) ARL

表7－6 ARL

領域名	ｸﾘﾃｨｶﾙﾌﾗｸﾞ	値(例)	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			
algorithm (アルゴリズム識別子)		1.2.840.113549.1.1.5	sha-1WithRSAEncryption
issuer (発行者)		ou="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government", c=JP	環境省CA発行者識別名(DN)、英語表記 UTF8String(Country 属性はPrintableString)
thisUpdate (今回の更新日)		YYMMDDHHMMSSZ 010501000000Z	今回の更新日時 UTCTime
nextUpdate (次回の更新日)		YYMMDDHHMMSSZ 010502000000Z	次回の更新日時 UTCTime
revokedCertificates (失効した証明書)			失効される証明書エントリ(以下の組のリスト)
userCertificate		10005(例)	失効された証明書を整数で指定
revocationDate		YYMMDDHHMMSSZ 010501000000Z	失効日時 UTCTime
crlEntryExtensions (失効証明書エントリ拡張)			(失効証明書ごとの拡張領域)
reasonCode			理由コード
unspecified	FALSE		[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			[5] 業務の停止
certificateHold			[6] 証明書の保留
removeFromCRL			[8] CRLの削除(使用しない)
↓			
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		署名鍵の識別、証明書拡張と同じ形式
keyIdentifier		OCTET STRING	環境省CA公開鍵のsha-1ハッシュ値
cRLNumber (CRL 番号)	FALSE	32 (例)	シーケンス番号、整数
IssuingDistributionPoint (発行する配布点)	TRUE	cn=arl, ou="ENV Root CA", ou="Ministry of the Environment", o="Japanese Government"", c=JP	directoryNameにてCRL/ARLの配布点を指定 UTF8String(Country 属性はPrintableString)
onlyContainsCaCerts		TRUE	
	ENCRYPTED (署名値)		

8. CP／CPSの管理

8.1 CP／CPSの変更

環境省CA運営委員会は、本CP／CPSを必要に応じて変更する。

8.2 CP／CPSの公表と通知

環境省CA運営委員会は、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の決定

環境省CAのCP／CPSは、環境省CA運営委員会の決定をもって有効なものとする。