

政府認証基盤（GPKI）

ブリッジ認証局CP / CPS

平成13年4月25日

行政情報化推進各省庁連絡会議幹事会了承

平成15年2月28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
1.1.1 相互認証.....	1
1.1.2 CPとCPS.....	1
1.2 識別.....	1
1.3 運営体制と証明書の適用範囲.....	2
1.3.1 CAの組織.....	2
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.....	4
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.....	5
2.6.3 アクセス制御.....	5
2.6.4 リポジトリ.....	5
2.7 準拠性監査.....	5
2.7.1 監査頻度.....	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 監査テーマ.....	5
2.7.5 監査指摘事項への対応.....	6
2.7.6 監査結果.....	6

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開示.....	6
2.8.7	その他の理由に基づく情報開示.....	7
2.9	知的財産権.....	7
3	識別と認証.....	8
3.1	初期登録	8
3.1.1	名前の型.....	8
3.1.2	名前の意味に関する要件.....	8
3.1.3	名前形式を解釈するための規則.....	8
3.1.4	名前の一意性.....	8
3.1.5	名前に関する紛争の解決手順.....	8
3.1.6	商標の認識・認証・役割.....	8
3.1.7	秘密鍵の所有を証明するための方法.....	8
3.1.8	組織の認証.....	8
3.1.9	個人の認証.....	8
3.2	証明書の更新	9
3.3	証明書失効後の再発行	9
3.4	証明書の失効申請	9
4	運用要件.....	10
4.1	証明書の発行申請	10
4.2	証明書の発行	10
4.2.1	審査.....	10
4.2.2	発行.....	10
4.3	証明書の受入れ.....	10
4.4	証明書の失効と一時停止.....	10
4.4.1	証明書の失効事由.....	10
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.....	11
4.4.4	失効における猶予期間.....	11
4.4.5	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	12
4.4.13	その他利用可能な有効性確認手段	12
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	12
4.4.15	秘密鍵の危殆化に関する特別な要件	12
4.5	セキュリティ監査の手順	12
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	13
4.5.6	監査ログの収集システム	13
4.5.7	監査ログ検査の通知	13
4.5.8	脆弱性の評価	13
4.6	アーカイブ	13
4.6.1	アーカイブデータの種類	13
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	レコードのタイムスタンプに関する要件	14
4.6.6	アーカイブデータの収集システム	14
4.6.7	アーカイブデータの検証	14
4.7	鍵更新	14
4.8	危殆化と災害からの復旧	14
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	14
4.8.2	証明書を失効する場合の要件	14
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	15
5	物理面、手続面及び人事面のセキュリティ管理	16
5.1	物理的管理	16
5.1.1	施設の位置と建物構造	16
5.1.2	物理的アクセス	16
5.1.3	電源設備と空調設備	16
5.1.4	水害対策	16
5.1.5	地震対策	16
5.1.6	火災対策	16

5.1.7	媒体管理.....	16
5.1.8	廃棄物処理.....	17
5.1.9	オフサイトバックアップ.....	17
5.2	手続面の管理.....	17
5.3	人事面の管理.....	19
6	技術的セキュリティ管理.....	20
6.1	鍵ペア生成とインストール.....	20
6.1.1	鍵ペア生成.....	20
6.1.2	証明書利用者への秘密鍵配付.....	20
6.1.3	公開鍵の受領.....	20
6.1.4	CA 公開鍵の配付.....	20
6.1.5	鍵のサイズ.....	20
6.1.6	公開鍵パラメータの生成.....	20
6.1.7	公開鍵パラメータの品質の検査.....	20
6.1.8	鍵を生成するハードウェア/ソフトウェア.....	20
6.1.9	鍵の利用目的.....	20
6.2	秘密鍵の保護.....	20
6.2.1	暗号モジュールに関する基準.....	20
6.2.2	秘密鍵の複数人制御.....	21
6.2.3	秘密鍵の預託.....	21
6.2.4	秘密鍵のバックアップ.....	21
6.2.5	秘密鍵のアーカイブ.....	21
6.2.6	暗号モジュールへの秘密鍵の格納.....	21
6.2.7	秘密鍵の活性化方法.....	21
6.2.8	秘密鍵の非活性化方法.....	21
6.2.9	秘密鍵の破棄方法.....	21
6.3	公開鍵の履歴保管と鍵ペアの有効期間.....	21
6.3.1	公開鍵の履歴保管.....	21
6.3.2	公開鍵と秘密鍵の有効期間.....	21
6.4	活性化データ.....	22
6.4.1	活性化データの生成とインストール.....	22
6.4.2	活性化データの保護.....	22
6.5	コンピュータセキュリティ管理.....	22
6.5.1	コンピュータセキュリティ機能要件.....	22
6.5.2	コンピュータセキュリティ評価.....	22
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.....	22
6.6.1	システム開発面における管理.....	22
6.6.2	システム運用面における管理.....	22
6.6.3	セキュリティ評価の基準.....	22

6.7	ネットワークセキュリティ管理	23
6.8	暗号モジュールの技術管理	23
7	証明書とCRL/ARLのプロファイル.....	24
7.1	証明書のプロファイル	24
7.2	CRL/ARLのプロファイル	24
8	CP/CPS の管理.....	25
8.1	CP/CPS の変更	25
8.2	CP/CPS の公表と通知.....	25
8.3	CP/CPS の決定	25
9	用語集.....	26

1 はじめに

本 CP/CPS は、国民等と行政との間の申請・届出等手続の電子化を実現するため、行政機関側認証局と民間側認証局（以下、それぞれ「行政機関側 CA」、「民間側 CA」という。）との間の相互認証を行うブリッジ認証局（以下「BCA」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 RFC 2527「Certificate Policy and Certification Practices Statement Framework」に準拠している。

1.1 概要

1.1.1 相互認証

BCA は、BCA に相互認証を要求し、BCA との相互認証のための要件を満たす行政機関側 CA 及び民間側 CA と相互認証を行う。

なお、BCA は、行政機関側 CA と民間側 CA との間の相互認証のために運営するものであり、民間側 CA 間の相互認証を行うことを目的としていない。

1.1.2 CP と CPS

BCA 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 BCA 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

BCA の証明書ポリシーは、相互認証本番用の証明書ポリシー及び相互認証実施前に行う接続テスト用の証明書ポリシーの 2 つであり、識別子は、それぞれ次のとおりとする。

BCA 相互認証証明書ポリシー：

0 . 2 . 4 4 0 . 1 0 0 1 4 5 . 8 . 1 . 1 . 1 . 1 0

BCA 相互認証接続テスト用証明書ポリシー：

0 . 2 . 4 4 0 . 1 0 0 1 4 5 . 8 . 1 . 1 . 1 . 0

1.3 運営体制と証明書の適用範囲

1.3.1 CAの組織

(1) 意思決定組織

BCA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。

BCAの運営に関する連絡会議の機能は、次のとおりとする。

- ・BCA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BCAの運営に関する重要事項の決定

(2) BCA運営組織

相互認証申請の受付及び審査並びに相互認証証明書の発行、更新、失効等の運営業務は、BCA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。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、BCA運用責任者、上級IA操作員、一般IA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

相互認証を行う行政機関側CA及び民間側CA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年以内とする。

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、総務省行政管理局行政情報システム企画課が行う。

1.4.2 照会窓口

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。

2 一般規定

2.1 義務

2.1.1 CA 業務に関する義務

BCA は、CA 業務に関して次の義務を負う。

- ・相互認証を行う行政機関側 CA 及び民間側 CA に対して相互認証証明書を発行する。
- ・証明書の失効処理を行い、有効期間 4 8 時間の失効リスト（以下「CRL/ARL」という。）を 2 4 時間ごとに発行する。
- ・CA 秘密鍵を安全に管理する。
- ・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は、2 4 時間 3 6 5 日体制で行う。

2.1.2 RA 業務に関する義務

BCA は、RA 業務に関して次の義務を負う。

- ・相互認証の新規申請に際して、相互認証証明書の発行申請を行う CA（以下「申請 CA」という。）を審査する。
- ・相互認証の更新申請、失効申請に際して、既に相互認証している CA（以下「相互認証先 CA」という。）を審査する。
- ・BCA は、相互認証証明書発行要求に含まれる公開鍵が確実に申請 CA 又は相互認証先 CA の公開鍵であり、かつ申請 CA 又は相互認証先 CA 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。

2.1.3 証明書利用者の義務

申請 CA 又は相互認証先 CA は、BCA との相互認証に関して次の義務を負う。

- ・相互認証申請に際して、正確な情報を提示する。
- ・システム又は運用に変更が生じた場合は、BCA の定める手続をとる。
- ・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。

2.1.4 証明書検証者の義務

規定しない。

2.1.5 リポジトリに関する義務

証明書検証者が公開鍵及び CRL/ARL を参照するための統合リポジトリを原則 2 4 時間 3 6 5 日運用する。ただし、保守等により一時的に運用を停止する場合がある。

2.2 CAの責任

BCAは、自己署名証明書、相互認証証明書の発行、更新、失効、保管及び公表に当たっては、申請CA又は相互認証先CA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

BCAに関する情報は、統合リポジトリ及びWeb上で公表する。

(1) 統合リポジトリ上での公表

BCAは、次の情報を統合リポジトリ上で公表する。

- ・BCA リポジトリに保有する自己署名証明書、リンク証明書、相互認証証明書及びそのCRL/ARL
- ・相互認証した行政機関側CAのリポジトリに保有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

(2) Web上での公表

BCAは、次の情報をWeb上で公表する。

- ・BCAと相互認証した行政機関側CAの名称、民間側CAの名称及び相互認証を取消したCAの名称
- ・CA秘密鍵危殆化に関する情報
- ・相互認証基準及び相互運用性仕様書

- ・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、相互認証証明書及びその CRL/ARL は、発行及び更新の都度
- ・相互認証先 CA の名称及び相互認証を取消した CA の名称は、連絡会議による決定の都度
- ・本 CP/CPS の変更の都度

2.6.3 アクセス制御

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

統合リポジトリは、BCA リポジトリの情報及び相互認証した行政機関側 CA のリポジトリの情報の複製情報を保有し公表する。

2.7 準拠性監査

2.7.1 監査頻度

BCA 運営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、BCA 運営組織は、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

BCA 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

BCA の監査を実施する監査人は、BCA 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

BCA 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、BCA 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 BCA が対策を実施したことを確認する。

2.7.6 監査結果

BCA の監査結果は、監査人から BCA 運営組織に対して監査報告書として提出される。BCA 運営組織は、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。

2.8 機密保持

2.8.1 機密扱いとする情報

BCA は、漏えいすることによって BCA 及び相互認証先 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。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

BCA 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

BCA は、自己署名証明書、リンク証明書及び相互認証証明書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

相互認証した民間側 CA が BCA に提示した情報について、当該民間側 CA から開示要求が行われた場合は開示する。

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

BCA 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

行政機関側 CA に発行する相互認証証明書において使用する名前は、府省及び認証局の名称とする。民間側 CA に発行する相互認証証明書において使用する名前についての規則は、相互運用性仕様書に定める。

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、相互運用性仕様書に定める。

3.1.4 名前の一意性

BCA の発行する相互認証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

BCA は、相互認証手続において、申請 CA 又は相互認証先 CA 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。

3.1.8 組織の認証

BCA は、相互認証手続において、所定の手続に基づき、申請 CA 又は相互認証先 CA を運営する者の真偽を確認する。

3.1.9 個人の認証

規定しない。

3.2 証明書の更新

相互認証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

相互認証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

相互認証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」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

BCA に対する相互認証証明書の発行申請は、所定の手続に基づいて、申請 CA 又は相互認証先 CA の責任者が BCA 運営組織に行う。

4.2 証明書の発行

4.2.1 審査

BCA は、BCA に対する相互認証証明書の発行申請を受理した後、相互認証基準に基づいて書類審査及び接続テストを行う。

4.2.2 発行

BCA は、申請 CA 又は相互認証先 CA 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。

申請 CA 又は相互認証先 CA においても同様に、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。

4.3 証明書の受入れ

BCA は、発行した相互認証証明書を、所定の手続に基づき、申請 CA 又は相互認証先 CA に渡し受領書を受け取る。申請 CA 又は相互認証先 CA においても同様に、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。双方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。

4.4 証明書の失効と一時停止

4.4.1 証明書の失効事由

BCA は、BCA 又は相互認証先 CA 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

4.4.2 証明書の失効申請者

(1) 相互認証先 CA から相互認証証明書失効申請を受ける場合

相互認証先 CA から BCA に対する失効申請は、相互認証先 CA の責任者が行う。

(2) 相互認証先 CA に相互認証証明書失効申請を行う場合

BCA から相互認証先 CA に対する失効申請は、BCA の責任者が行う。

4.4.3 証明書の失効申請及び失効処理手順

(1) 相互認証先 CA 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。

(2) 相互認証先 CA に相互認証証明書失効申請を行う場合

相互認証先 CA 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。

4.4.4 失効における猶予期間

BCA は、相互認証先 CA との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

BCA は、相互認証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 4 8 時間の CRL/ARL を 2 4 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、BCA 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。BCA は、この確認が行えるよう統合リポジトリ上で CRL/ARL を公表する。

4.4.11 オンライン有効性確認の可用性

BCA は、統合リポジトリを「2.1.5 リポジトリに関する義務」に定めるとおり運用する。

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

相互認証先 CA において CA 秘密鍵の危殆化が発生した場合は、速やかに BCA 運営組織に報告する。BCA は直ちに失効処理を行い、連絡会議に事後報告を行う。

4.5 セキュリティ監査の手順

監査ログ検査者は、BCA システム、BCA リポジトリ及び統合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

BCA システム、BCA リポジトリ及び統合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週次で行う。

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、適切な入退出管理が行われて

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、週次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 BCA 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、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、月次で外部記憶媒体に取得し、適切な入退出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、月次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。

CA 鍵ペア更新時には、古い CA 公開鍵と新しい CA 公開鍵の認証パスを構築するリンク証明書を発行し、統合リポジトリ上で公表する。

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

発行した相互認証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。相互認証証明書を失効した相互認証先 CA に対し、再度相互認証証明書を発行する場合は、あらかじめ発行手続を行う。

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
- ・相互認証証明書等の再発行手続

また、相互認証先 CA の CA 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、相互認証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 BCA 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

連絡会議において BCA 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 BCA のバックアップデータ、アーカイブデータ等の保管組織及び開示方法を業務終了 90 日前までに相互認証先 CA 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

BCA 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 BCA 運営責任者が付与する。

BCA 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

BCA 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

BCA 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

BCA 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

BCA 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、適切な入退出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

規定しない。

5.2 手続面の管理

相互認証証明書等の発行、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、BCA 運営責任者から BCA 運用責任者に対して行い、BCA 運用責任者は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) BCA 運営責任者

BCA 運営責任者は、BCA の運営に関する責任者であり、次の業務を行う。

- ・BCA 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 BCA 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 秘密鍵バックアップ媒体のセット

(3) 受付担当者

受付担当者は、相互認証申請の受付から相互認証の承認・不承認の決定までの事務
手続、申請 CA 又は相互認証先 CA との連絡調整業務を行う。

(4) 審査担当者

審査担当者は、相互認証基準に基づき、申請 CA 又は相互認証先 CA の審査業務を
行う。

(5) BCA 運用責任者

BCA 運用責任者は、BCA 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

(6) 上級 IA 操作員

上級 IA 操作員は、CA 秘密鍵を使用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（HSM）の活性化・非活性化
- ・BCA システムの起動・停止
- ・BCA システムの動作に関する設定変更管理
- ・BCA 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

(7) 一般 IA 操作員

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

- ・証明書ポリシーの設定登録、変更
- ・相互認証証明書等の発行、更新及び失効処理
- ・操作員への証明書の発行、更新及び失効処理

(8) ディレクトリ操作員

ディレクトリ操作員は、BCA リポジトリ及び統合リポジトリの設定管理に関する業
務を行う。

(9) 監査ログ検査者

監査ログ検査者は、BCA システム、BCA リポジトリ及び統合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

BCA の要員の適格性の審査、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に基づいて運用する。また、すべての要員には、BCA 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 を用いて生成する。

6.1.2 証明書利用者への秘密鍵配付

規定しない。

6.1.3 公開鍵の受領

BCA は、相互認証証明書の取り交わしにおいて、相互認証先 CA 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

規定しない。

6.1.5 鍵のサイズ

RSA 2048 ビットの鍵を使用する。

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/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

CA 秘密鍵は、FIPS140-1 レベル 3 相当の HSM 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

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、複数人の上級 IA 操作員により管理鍵を用いて活性化する。

6.2.8 秘密鍵の非活性化方法

CA 秘密鍵は、複数人の上級 IA 操作員により管理鍵を用いて非活性化する。

6.2.9 秘密鍵の破棄方法

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、破棄する CA 秘密鍵のバックアップ媒体を室外へ持ち出す場合も、物理的に媒体を破壊する。

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

BCA の公開鍵と秘密鍵の有効期間は、有効とする日から起算して 10 年とし、5 年ごと

に鍵更新を行う。

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

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

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 に直接入力する。

6.4.2 活性化データの保護

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。

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

BCA 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

BCA 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、BCA 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 システム運用面における管理

BCA 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

BCA リポジトリは、ファイアウォールを介して統合リポジトリに接続する。

統合リポジトリはインターネットに接続し、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 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

自己署名証明書、リンク証明書、相互認証証明書等のプロファイルは、相互運用性仕様書に定める。

7.2 CRL/ARL のプロファイル

CRL/ARL のプロファイルは、相互運用性仕様書に定める。

8 CP/CPS の管理

8.1 CP/CPS の変更

連絡会議は、本 CP/CPS を必要に応じて変更する。

8.2 CP/CPS の公表と通知

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。

8.3 CP/CPS の決定

BCA の CP/CPS は、連絡会議の決定をもって有効なものとする。

9 用語集

< A ~ Z >

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

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

・ BCA リポジトリ

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

・ 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官職証明書等のリスト。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(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 : 暗号化モジュールに、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 : 暗号化モジュールに、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)

国民等と行政との間でインターネット等を利用してやり取りされ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行政機関側の認証システムであり、BCAと各府省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。「暗号モジュール」参照。

・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、BCA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。

- ・ 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/ARL のプロファイル、CP と CPS のフレームワーク等の制定を目的としている。

- ・ RA (Registration Authority : 登録局)

CA の業務のうち、登録業務を行う機関。主な業務は、証明書発行対象者の本人確認、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。

- ・ RFC2527 (Request For Comments 2527)

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 RFC2527 は、CP 又は CPS を作成するためのフレームワーク及びガイドラインを提供している。

- ・ RSA

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

- ・ X.500 識別名(DN:Distinguished Name)

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

- ・ X.509

ITU - T が定めた証明書及び CRL/ARL のフォーマット。X.509 v3(Version 3)では、任意

の情報を保有するための拡張領域が追加された。GPKI では、証明書は X.509 v3、CRL/ARL は X.509 v2 を使用する。

< あ ~ ん >

- ・ アーカイブ

証明書の発行履歴、失効履歴等を長期間保管すること。

- ・ アクセス制御

コンピュータ等、情報の供給源への不正アクセスを防止するための制御機能。アクセス者を識別し、本人であることを確認したうえで、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

不正アクセスに備えるための機能（耐タンパ機能）を保有した秘密鍵の管理装置。

耐タンパ機能とは 不正アクセスに対してその侵入の痕跡を残したり、データを消去する機能であり、不正アクセスの証拠を残す不正顕示機能、不正アクセスからデータを防護する不正防護機能、不正アクセスに対してデータを消去する対抗動作を行う不正対抗機能等がある。「HSM」参照。

- ・ 改ざん

データの内容を書き換えられること。

- ・ 鍵のサイズ（鍵長）

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

- ・ 鍵ペア

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

- ・ 活性化

システム、装置等を使用可能な状態にすること。

- ・ 活性化データ
システム、装置等を活性化するために必要となるデータ（パスワード等）。
- ・ 官職証明書
ある公開鍵が、記載された官職が使用するものであることを保証する電子的な文書。
- ・ 管理鍵
HSM の操作をする際に必要となる鍵。HSM の機能を制御するために用いる。
- ・ 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。
- ・ 行政機関側 CA
行政機関が運営する CA。官職証明書等を発行する。
- ・ 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」及び「ARL」参照。

- ・主体者名

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

- ・証明書（公開鍵証明書）

ある公開鍵を、記載されたものが保有することを証明する電子的文書。CA が記載内容を確認のうえ、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（相互認証先 CA 等）。

- ・署名（デジタル署名）

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

- ・セキュリティ監査

セキュリティを重点テーマとして実施する監査。

- ・相互運用性仕様書

複数の CA が相互接続する場合に、相手側の CA が発行した証明書を、信頼を保ちつつ相互に利用できるようにするための機能に関する要件を記載した文書。

- ・ 相互認証基準

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

- ・ 相互認証証明書

2 つの異なる認証ドメインの CA がお互いを認証したことを示すために、相互に発行する証明書。GPKI では、府省 CA、民間 CA 又は商業登記 CA と BCA の間で相互認証証明書が発行される。

- ・ 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。

- ・ ディレクトリサーバ

階層の構造を持ち、証明書や失効情報を格納するデータベースサーバ。

- ・ 統合リポジトリ

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

- ・ 認証ドメイン

特定の証明書ポリシーのもとに運営する CA が発行する証明書の適用範囲。

- ・ 認証パス

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

- ・ 発行者名

証明書を発行し署名を施した CA を識別する名前。

- ・ハッシュ関数

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

- ・ハッシュ値

ある値に対するハッシュ関数の出力値。「ハッシュ関数」参照。

- ・非活性化

システム、装置等を使用不可能な状態にすること。

- ・秘密鍵

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

- ・秘密鍵の預託

本人しか持ち得ない署名用の秘密鍵を第三者に預けること。

- ・フィンガープリント

任意のメッセージに対するハッシュ値。GPKIでは、公開鍵に対するハッシュ値を指す。ハッシュ関数の性質で一意に決まることからフィンガープリント（指紋）と呼ばれる。「ハッシュ関数」参照。

- ・府省 CA リポジトリ

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

- ・プロファイル

証明書及び CRL/ARL に含まれるデータの内容を定義したもの。RFC2459により証明書及び CRL/ARL のプロファイルについて定義されている。

- ・民間側 CA

「電子署名及び認証業務に関する法律（平成12年法律第102号）」（電子署名法）に基づき認定された特定認証業務を行う認定認証事業者、「商業登記制度に基礎を置く電子認証制度」に基づく CA を指す。

- ・リストア

バックアップデータを復元すること。

- ・リポジトリ

証明書及び CRL/ARL を格納し公表するデータベース。GPKI ではディレクトリサーバを使用する。

- ・リンク証明書

CA の鍵更新に伴い同時に存在することとなる新しい CA 鍵ペアと古い CA 鍵ペアの関係を保証するための証明書。

- ・ログ

コンピュータ上で行った操作及び処理を記録したファイル。