地方公共団体による公的個人認証サービス

ブリッジ認証局　運用規程

Ver.1.2

2014 年 4 月 1 日

公的個人認証サービス共通基盤事業運用会議

改訂履歴

Ver	日付	改版内容
1.0	2004 年 1 月 29 日	初版発行
1.1	2008 年 7 月 29 日	認証局の秘密鍵更新に伴う改訂
1.2	2014 年 4 月 1 日	公的個人認証サービス共通基盤事業運用会議発足に伴う改正

1. はじめに

本運用規程は、地方公共団体における公的個人認証サービス（以下「公的個人認証サービス」という。）における公的個人認証サービスブリッジ認証局(以下「個人認証 BCA」という。)の認証業務に関する運用規程である。

なお、本運用規程の構成は、IETF(Internet Engineering Task Force)においてPKIX(Public-Key Infrastructure X.509) Working Group による RFC(Request For Comments) 2527 「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。

本運用規程の記述においては、RFC2527 で定める項目のすべてを記載する。ただし、他の規程等を参照する場合には、見出しだけを残し、参照内容を明示することとする。

１-１概要

１-１-１証明書の種類

個人認証 BCA は、個人認証 BCA に認証を要求し、個人認証 BCA と相互認証を行う認証局(以下「相互認証 CA」という。)に対し、認証を行い、相互認証証明書を発行する。

個人認証 BCA は、相互認証 CA に対し認証を要求し、相互認証証明書を受け取る。

個人認証 BCA は、公的個人認証サービスの運用に必要な SSL 証明書／コードサイニング証明書を発行する。

１-１-２ＣＰとＣＰＳ

個人認証 BCA は、CP(証明書ポリシー)および CPS（認証実施規程）をそれぞれ独立したものとせず､本運用規程を個人認証 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

個人認証 BCA の証明書ポリシーの識別子は、次のとおりとする。

個人認証 BCA 相互認証証明書ポリシー

（以下で特に指定の無い証明書は全てこのポリシーを適用する。）

1.2.392.200149.8.5.1.1.10

個人認証 BCA 相互認証テスト用証明書ポリシー

1.2.392.200149.8.5.1.0.10

SSL 証明書ポリシー

1.2.392.200149.8.5.1.100

テスト用 SSL 証明書ポリシー

1.2.392.200149.8.5.1.0.100

コードサイニング証明書ポリシー

1.2.392.200149.8.5.1.４00

１-３運用体制と証明書の適用範囲

１-３-１運用体制

⑴意思決定組織

個人認証 BCA の運営に関する意思決定は、公的個人認証サービス共通基盤事業運用会議（以下「運用会議」という。）が行う。運用会議は、次に挙げる事項の決定及び承認を行う。

・本運用規程
・相互認証
・個人認証 BCA の秘密鍵の危殆化時の対応
・災害発生等による緊急時の対応
・その他個人認証 BCA の一元的な運営の実現に関する重要事項

⑵運用組織

個人認証 BCA の運用は、運用会議が選定し委託する者が行う。委託された者は、認証業務の実施に関する事務を行う。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手続は、本運用規程「５-２　手続面のセキュリティ管理」において定める。

１-３-２適用性・適用環境など

個人認証 BCA は、相互認証を行なうために、相互認証先の CA と相互認証証明書を取り交わす。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。

また、個人認証 BCA が発行する SSL 証明書/コードサイニング証明書は運用に係るサーバー等に適用する。

なお、個人認証 BCA が発行する SSL 証明書／コードサイニング証明書をインターネット上で使用する場合の有効期間は、証明書を有効とする日から起算して１年とする。

１-４運用規程に関する連絡先

１-４-１管理組織

本運用規程の変更及び更新等に関する事務は、運用会議が行う。

１-４-２連絡先

本運用規程に関する照会は、運用会議を窓口とする。

２一般規定

２-１義務

２-１-１認証局業務に関する義務

個人認証 BCA は、認証局業務に関して次の義務を負う。

・相互認証 CA に対して、相互認証証明書を発行する。

・本運用規程に基づき、自己署名証明書、リンク証明書、SSL 証明書／コードサイニング証明書を発行する。

・証明書の失効処理を行い、有効期間 72 時間の失効記録（CRL/ARL）を 24 時間ごとに発行する。

・個人認証 BCA の秘密鍵を安全に管理する。

・個人認証 BCA の秘密鍵が危殆化した場合には、速やかに相互認証 CA 運営組織に報告する。

・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データを必要な期間保管する。

・システムの稼動監視は常時的確に行い、24 時間の安定的な運用を目標とする。

・相互認証 CA への相互認証申請に際して、正確な情報を提示する。

・相互認証証明書の取り交わしに関しては、相互認証 CA との間で合意した手続に従う。

・相互認証証明書等の発行、更新及び失効申請に際して、本運用規程の規定に従い、受付及び審査を行う。

・相互認証証明書等の発行要求に含まれる公開鍵が、確実に相互認証 CA 等の公開鍵であり、かつ、相互認証 CA 等がこの公開鍵に対する秘密鍵を保有していることを確認する。

・相互認証 CA に対する相互認証証明書の発行及び失効の要求を行う。

・発行する証明書プロファイル情報の定義及び保管を行う。

・発行申請情報の保管、発行情報の改ざん防止対策を行う。

２-１-２証明書利用者の義務

(1)相互認証証明書

相互認証 CA は、次の義務を負う。

・相互認証証明書は所定の手続に基づき、本運用規程に従って利用する。

・相互認証証明書及びその CA の秘密鍵を安全に管理する。

・個人認証 BCA の秘密鍵が危殆化した場合は、速やかに本運用規程「1-3-1　運用体制」で定める組織及び相互認証 CA の運営組織に報告する。

・相互認証証明書は、本運用規程「1-3-2 適用性・適用環境など」で定める目的以外で適用しない。

(2) SSL 証明書／コードサイニング証明書

SSL 証明書／コードサイニング証明書の利用者は、次の義務を負う。

・SSL 証明書／コードサイニング証明書は、所定の手続に基づき本運用規程に従って、利用する。
・SSL 証明書／コードサイニング証明書及びその秘密鍵を安全に管理する。
・秘密鍵が危殆化した場合は、速やかに本運用規程「1-3-1　運用体制」で定める組織及び相互認証 CA の運営組織に報告する。
・SSL 証明書／コードサイニング証明書は、本運用規程「1-3-2 適用性・適用環境など」で定める目的以外で適応しない。

２-１-３証明書検証者の義務

証明書検証者は次の義務を負う。

・個人認証 BCA から発行された証明書の検証（当該証明書が有効期間内にあるかどうか、個人認証 BCA から発行されたものであるかどうか、当該証明書が失効していないかどうか)。

２-１-４リポジトリの義務

リポジトリは、次の義務を負う。

・本運用規程「2-6-1　個人認証 BCA に関する情報の公開」で規定される情報の開示を行う。
・原則として、24 時間 365 日の安定的な運用を行う。
・登録された情報の保護を行う。

２-２責任

２-２-１個人認証 BCA の責任

個人認証 BCA は、自己署名証明書、リンク証明書、相互認証証明書、SSL 証明書／コードサイニング証明書等の発行、更新、失効、保管及び公表を、本運用規程に基づいて適切に行う。個人認証 BCA は、発行した証明書について、内容を発行した時点において確認する責任を持つ。個人認証 BCA は、これらの情報には署名を付与しているが、第三者による改ざん及び攻撃法の発見などによる署名アルゴリズムの陳腐化があった場合には、その内容は保証できない。

２-２-２RA の責任

個人認証 BCA は、RA 業務において、審査、申請を適切に実施する。

２-２-３証明書利用者の責任

利用者は、本運用規程に従い、本サービスを利用する。

２-２-４証明書検証者の責任

証明書検証者は、本運用規程に従い、本サービスを利用する。

２-２-５リポジトリの責任

リポジトリは、本運用規程によって規定された運用時間において、正当な情報検索要求に対する応答を返却する。

２-３財務上の責任

規定しない。必要な場合には、追加規定する。

２-４解釈と実行

本運用規程に基づく認証業務から生ずる紛争については、「電子署名に係る地方公共団体の認証業務に関する法律」（以下「根拠法」という。）を適用する。

２-５料金

規定しない。

２-６公開とリポジトリ

２-６-１個人認証 BCA に関する情報の公開

個人認証 BCA に関する情報は、公的個人認証サービスのリポジトリ及び Web 上で公表する。

⑴リポジトリ上での公表

個人認証 BCA は、公的個人認証サービスのリポジトリ上で、次の情報を公開する。
自己署名証明書、相互認証証明書、リンク証明書及び自己署名証明書、相互認証証明書、リンク証明書、SSL 証明書／コードサイニング証明書の失効記録（CRL/ARL）。

⑵Web 上での公表

個人認証 BCA は、次の情報を Web 上で公開する。

- 個人認証 BCA と相互認証した CA の名称及び相互認証を取り消した CA の名称
- 個人認証 BCA の秘密鍵の危殆化に関する情報
- 相互認証証明書プロファイル
- 本運用規程
- SSL 証明書／コードサイニング証明書プロファイル
- 個人認証 BCA の自己署名証明書
- 個人認証 BCA のフィンガープリント

２-６-２公開の頻度

公表する情報の更新頻度は、次のとおりとする。

・全ての証明書及びその失効記録（CRL/ARL)は、発行及び更新の都度
・個人認証 BCA が相互認証した CA の名称及び相互認証を取り消した CA の名称は運用会議による決定承認の都度
・本運用規程変更の都度

２-６-３公開情報へのアクセスコントロール

リポジトリ及び 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リポジトリに関する要件

本運用規程「２−１−５リポジトリの義務」において定める。但し、定期保守作業等により、一時的にリポジトリを利用できない場合もある。

２-７準拠性監査

２-７-１準拠性監査の頻度

運用会議は、監査人による監査を年一回定期的に実施する。また定期監査以外に随時監査を必要に応じて実施する。

２-７-２監査人の識別及び資格

個人認証 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監査人及び被監査者との関係

個人認証 BCA の監査を実施する監査人は、個人認証 BCA と利害関係を有しない者を選定する。

２-７-４監査項目

認証業務が、根拠法及び関連法令並びに本運用規程等に準拠して実施さ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

運用組織は、監査指摘事項を確認し、重要又は緊急を要する監査指摘事項について、運用会議の決定の基づき速やかに対応する。個人認証 BCA 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。重要または緊急を要する監査指摘事項が改善されるまでの間、個人認証 BCA の運用を停止するか否かは運用会議が決定する。また、運用会議は、監査指摘事項に対して運用組織が対策を実施したことを確認する。

２-７-６監査結果の取扱い

監査人は、監査を終了したとき、監査報告書を作成し運用会議に提出しなければならない。運用会議は、運用組織に監査結果を通知する。また、相互認証 CA から報告を求められた場合は、運用会議の指示により、運用組織が監査結果を報告する。監査報告書は、１０年間保管する。

２-８機密保持と個人情報保護

２-８-１機密扱いとする情報と個人情報の取扱い

個人認証 BCA は、漏えいすることによって個人認証 BCA 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

個人認証 BCA が保有する情報のうち、自己署名証明書、リンク証明書、相互認証証明書、SSL 証明書／コードサイニング証明書、その他業務運用に必要な証明書及びそれらの証明書の失効記録（CRL/ARL)並びに本運用規程等、公表する情報として明示的に示すものは機密扱いにしない。

２-８-３証明書失効情報の公表

個人認証 BCA は、発行する証明書の失効情報を開示する。失効理由の詳細は開示しない。

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証明書利用者の請求に基づく情報開示

相互認証 CA が個人認証 BCA に提示した情報について、当該相互認証 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名称の型

個人認証 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名称の意味に関する要件

個人認証 BCA が発行する相互認証証明書において使用する名前は、地方公共団体が定める名称、他相互認証 CA の名称とする。また SSL 証明書／コードサイニング証明書に関しては別途所定の手続にて定める。

３-１-３名称形式を解釈するための規則

X.500 識別名の規定に従う。

３-１-４名称の一意性

個人認証 BCA が発行する証明書の主体者名は、一意に割り当てる。

３-１-５名称に関する係争の解決手段

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秘密鍵の所有証拠の確認手段

個人認証 BCA は、相互認証手続において相互認証 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 の公開鍵とペアとなる CA の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 の公開鍵の所有者を特定する。

SSL 証明書／コードサイニング証明書に関しては別途所定の手続にて確認手段を定める。

３-１-８組織的な識別

個人認証 BCA は、相互認証証明書等の申請手続において、相互認証 CA 等を運営する組織の真偽を確認する。

３-１-９個人の識別

規定しない。

３-２証明書の更新

個人認証 BCA が発行する証明書更新時における識別及び認証は、本運用規程「3-1 初期登録」において定める手続に基づいて行う。

３-３失効後の再発行

個人認証 BCA が発行する証明書失効後の再発行時における識別及び認証は、本運用規程「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

個人認証 BCA が発行する証明書の失効時における識別及び認証は、本運用規程「3-1-8 組織的な識別」において定める手続に基づいて行う。

４運用要件

４-１証明書適用

(1) 相互認証証明書

相互認証証明書の発行申請は、相互認証 CA と合意した手続に基づいて行う。

(2) SSL 証明書／コードサイニング証明書

SSL 証明書／コードサイニング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

個人認証 BCA は、相互認証 CA と合意した手続に従い、当該相互認証 CA から提出された証明書発行要求に対し、自己の署名を付して相互認証証明書を発行する。

(2) SSL 証明書／コードサイニング証明書

SSL 証明書／コードサイニング証明書の発行は、所定の手続に基づいて行う。

４-３証明書受入れ

(1) 相互認証証明書

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

(2) SSL 証明書／コードサイニング証明書

個人認証 BCA は、発行した SSL 証明書／コードサイニング証明書を所定の手続に基づき、安全かつ確実な方法で配付し受領書を受け取る。この受領の確認をもって SSL 証明書／コードサイニング証明書の受入れの完了とする。

４-４証明書失効と一時停止

４-４-１失効要件

個人認証 BCA は、個人認証 BCA 又は相互認証 CA に、以下の相互認証証明書失効事由が発生した場合は、相互認証証明書を失効する。また SSL 証明書／コードサイニング証明書の失効要件は別途所定の手続にて定める。

・個人認証 BCA 又は相互認証 CA の秘密鍵の危殆化
・相互認証基準違反
・相互認証の終了
・相互認証更新

４-４-２失効申請者

(1) 失効申請を受ける場合

相互認証 CA から個人認証 BCA に対する失効申請は、相互認証 CA が行う。
また SSL 証明書／コードサイニング証明書の失効申請は別途所定の手続にて定める。

(2) 失効申請を行う場合
個人認証 BCA から相互認証 CA に対する失効申請は、個人認証 BCA が行う。
また SSL 証明書／コードサイニング証明書の失効申請は別途所定の手続にて定める。

４-４-３失効要求手続

(1) 相互認証証明書

・失効申請を受ける場合
本運用規程「3-1-8 組織的な識別」で規定された手続により、要求された相互認証証明書を失効し、失効記録（ARL）をリポジトリに登録する。

・失効申請を行う場合
所定の手続に従い、失効申請を行う。相互認証 CA との相互認証証明書を失効し、失効記録（ARL）をリポジトリに登録する。

(2) SSL 証明書／コードサイニング証明書
個人認証 BCA は、所定の手続に基づき、要求された証明書を失効し失効記録（CRL）をリポジトリに登録する。

４-４-４失効猶予期間

個人認証 BCA は、失効申請手続の終了後、直ちに失効処理を行う。

４-４-５一時停止要件

個人認証 BCA が発行する証明書の一時停止は行わない。

４-４-６一時停止申請者

規定しない。

４-４-７一時停止要求手続

規定しない。

４-４-８一時停止期間

規定しない。

４-４-９失効記録（CRL/ARL）発行頻度

有効期間 72 時間の失効記録（CRL/ARL)を 24 時間ごとに発行する。ただし、個人認証 BCA の秘密鍵の危殆化等が発生した場合には、失効記録（CRL/ARL)を直ちに発行する。

４-４-１０失効記録（CRL/ARL）の発行最大遅延時間

最後に発行した失効記録（CRL/ARL）の有効期間が満了する前に新たな失効記録（CRL/ARL）を発行する。

４-４-１１失効記録（CRL/ARL)の確認

証明書検証者は、個人認証 BCA の発行する失効記録（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。また個人認証 BCA はこの確認が行えるように、個人認証 BCA のリポジトリ上で失効記録（CRL/ARL)を公表する。

４-４-１２オンライン有効性確認の可用性

本運用規程「２-１-５リポジトリの義務」において定める。

４-４-１３オンライン有効性検証・状態検証要件

規定しない。

４-４-１４失効を公表する他の手法

規定しない。

４-４-１５失効を公表する他の手法の検証要件

規定しない。

４-４-１６秘密鍵の危殆化による特別な要件

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

４-５セキュリティ監査手続

内部監査者（本運用規程「５-２-１高い信頼性が要求される要員とその役割」を参照）は、個人認証 BCA システム及び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

個人認証 BCA システム及びリポジトリにおけるセキュリティに関する重要な事項を対象に、アクセスログ及び操作ログ等監査ログを記録する。

・発行手続に関する操作・稼動ログ
・失効手続に関する操作・稼動ログ
・有効性確認に関するすべてのアクセス・稼動ログ
・個人認証 BCA の鍵ペア生成に関する操作ログ
・システム、各種帳簿等に対するアクセスログ
・個人認証 BCA の設備への入退室記録　　等

監査ログには、次の情報を含める。

・事象又は処理の種類
・発生日時

・処理の結果
・事象の発生元の識別情報（操作員 ID、システム名等）

４-５-２監査ログの検査周期

内部監査者はセキュリティ監査を週次で行う。

４-５-３監査ログの保管期間

1 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す。

監査ログのバックアップは、月次で外部記憶媒体等に取得し、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、内部監査者が行う。

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、月次で外部記憶媒体等に取得する。

４-５-６監査ログの収集システム

監査ログの収集機能は、個人認証 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、その事象を発生させた者に通知することなく行う。

４-５-８脆弱性の検証

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。

・発行した証明書
・失効記録（CRL/ARL)の発行履歴
・個人認証 BCA システムの起動及び停止履歴
・個人認証 BCA システム操作履歴　等

４-６-２アーカイブデータの保管期間

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、改ざん防止対策を施す。アーカイブデータは、月次で外部記憶媒体等に取得し、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、月次で外部記憶媒体等に取得する。

４-６-５アーカイブデータに付与するタイムスタンプの要件

アーカイブデータには、タイムスタンプ（時刻情報）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等の可読性の確認を、年１回行う。

４-７鍵の更新

(1) 個人認証 BCA の鍵ペア

５年以内に鍵ペアの更新を行う。

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

(2) SSL 証明書／コードサイニング証明書の鍵ペア

個人認証 BCA が発行する SSL 証明書/コードサイニング証明書は、インターネット上で使用する場合、1 年以内に鍵ペアの更新を行う。インターネット上以外で使用する場合、5 年以内に鍵ペアの更新を行う。

４-８鍵の危殆化と災害復旧

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には、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証明書が失効した場合の復旧手段

発行した相互認証証明書等の失効処理に当たっては、その失効の取消は、行わない。相互認証証明書等を失効した相互認証 CA 等に対し、再度、相互認証証明書等を発行する場合には、改めて発行手続を行う。

４-８-３秘密鍵が危殆化した場合の復旧手段

秘密鍵が危殆化した場合には、所定の手続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

・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 CA 等の秘密鍵が危殆化した場合には、本運用規程「4-4　証明書失効と一時停止」において定める手続に基づき、相互認証証明書等の失効手続を行う。

４-８-４災害発生時の設備の確保

災害等により個人認証 BCA の設備が被害を受けた場合には、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個人認証 BCA 業務の終了

運用会議において個人認証 BCA の認証業務の終了が決定した場合には、業務終了の事実、並びに業務終了後の個人認証BCAのバックアップデータ及び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 CA、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物理面のセキュリティ管理

５-１-１施設の位置と建築

個人認証 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じる。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

個人認証 BCA の施設内の各室内において行われる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、本運用規程「5-2　手続面のセキュリティ管理」において定める各要員の業務に応じて個人認証 BCA の認証局管理責任者が付与する。

個人認証 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電力と空調

個人認証 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じる。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

個人認証 BCA の設備を設置する建物及び室には漏水探知機を設置し、天井及び床には、防水対策を講じる。

５-１-５地震対策

個人認証 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じる。

５-１-６防火対策

個人認証 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電磁波対策

個人認証 BCA の施設内の各室内において行われる業務の重要度に応じて、電磁波攻撃及び電磁波からの情報漏えいを防ぐ設備を備える。

５-１-８媒体（磁気媒体等）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。

５-１-９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。

５-１-１０オフサイトバックアップ

規定しない。

５-２手続面のセキュリティ管理

５-２-１高い信頼性が要求される要員とその役割

各要員の業務を次のとおり定める。

⑴認証局管理責任者

認証局管理責任者は、個人認証 BCA の運営に関する責任者であり、次の業務を行う。

・認証業務の統括
・個人認証 BCA の秘密鍵の危殆化発生及び災害発生時等緊急時における対応の統括
・要員等への作業指示及び作業結果の確認
・HSM の機能を制御する鍵（以下「管理鍵」という。）の保守管理
・入退室管理
・準拠性監査への対応及びその指摘事項に対する是正実施管理
・その他個人認証 BCA の運営及び運用に関する統括

⑵秘密鍵管理者

秘密鍵管理者は、個人認証 BCA の秘密鍵等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、作業は複数人の秘密鍵管理者が行う。

・個人認証 BCA の秘密鍵等のバックアップ媒体の保管管理
・個人認証 BCA の秘密鍵等生成、自己署名証明書発行時の HSM に対する操作
・個人認証 BCA の秘密鍵等の更新時における HSM に対する操作
・個人認証 BCA の秘密鍵等のバックアップ、バックアップからのリストア時の HSM に対する操作および個人認証 BCA の秘密鍵等のバックアップ媒体のセット

⑶受付担当者

受付担当者は、相互認証証明書等の発行、更新及び失効申請の受付、相互認証 CA 等との連絡調整業務及び申請書類等の管理を行う。

⑷審査担当者

審査担当者は、相互認証証明書等の発行、更新及び失効申請の審査業務を行う。

(5)審査承認者

審査承認者は、審査担当者からの相互認証証明書等の発行申請、更新申請及び失効申請の審査結果に対して承認業務を行う。

(6)上級操作員

上級操作員は、個人認証 BCA の秘密鍵を使用する次の業務を行う。また、作業は複数人の上級操作員が行う。

・HSM の活性化及び非活性化
・自己署名証明書発行、更新、失効処理
・相互認証証明書発行、更新、失効処理
・SSL 証明書／コードサイニング証明書発行、更新、失効処理
・個人認証 BCA 証明書等ポリシーの設定登録及び変更
・その他個人認証 BCA システムの運用管理業務

(7)リポジトリ操作員

リポジトリ操作員は、リポジトリの設定管理に関する業務を行う。

(8)一般操作員

一般操作員は、ネットワーク機器等の運用及び維持管理を行う。

(9)内部監査者

内部監査者は、個人認証 BCA システム及び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
・監査済みログの削除

５-２-２個人認証 BCA における各要員の職務権限の分離と作業の指示方法

相互認証証明書の発行、更新及び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。個人認証 BCA の秘密鍵の操作を行う秘密鍵管理者及び上級操作員等は、複数人任命する。

５-２-３個人認証 BCA における各要員の識別と認証要件

業務の指示は、認証局管理責任者が各操作員に対して指示を行う。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。

５-３個人認証 BCA における人事面のセキュリティ管理

５-３-１要員の許可手順

所要の審査手順に従い、雇用前に書類（履歴書、推薦状等）検査により経歴調査を実施

する。

５-３-２各要員に対する訓練の手順

教育訓練計画書に従い、各要員に必要な訓練を実施する。

５-３-３要員間の業務交代と頻度、順序

認証局管理責任者が文書により、業務のローテーション方法を規定する。

５-３-４許可されていない行動

各要員が許可されていない行動を行った場合には、あらかじめ定められた懲戒処分を課す。

５-３-５各要員へ提供される文書

各要員は、それぞれのアクセス権に応じて文書（運用手順書、操作手順書等）を閲覧することが可能である。

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鍵ペアを生成する者、生成方法

(1) 個人認証 BCA の鍵ペア

個人認証 BCA の鍵ペアは、複数人の秘密鍵管理者が本運用規程「６-１-８鍵ペアを生成するハードウェア／ソフトウェア」に定める設備を用いて生成する。

(2) SSL 証明書／コードサイニング証明書に係る鍵ペア

SSL 証明書／コードサイニング証明書に係る鍵ペアは、所定の手続に基づいて生成する。

６-１-２秘密鍵の配付

規定しない。

６-１-３相互認証 CA の公開鍵の受領

個人認証 BCA は、相互認証証明書の取り交わしにおいて、相互認証 CA の公開鍵を安全かつ確実に受け取る。

６-１-４個人認証 BCA の公開鍵の配付

個人認証 BCA の自己署名証明書は、本運用規程「2-6-1 個人認証 BCA に関する情報の公開　(2)Web 上での公表」より配布される。

配布された個人認証 BCA の自己署名証明書は、オフライン等で配布されたフィンガープリントによって確認される。

６-１-５鍵長

(1) 個人認証 BCA の鍵長

RSA 暗号方式に基づく 2048 ビットの鍵を使用する。

(2) SSL 証明書／コードサイニング証明書に係る鍵長

RSA 暗号方式に基づく 1024 ビットの鍵を使用する。

６-１-６公開鍵パラメータ

規定しない。

６-１-７公開鍵パラメータの品質検証

規定しない。

６-１-８鍵ペアを生成するハードウェア／ソフトウェア

(1) 個人認証 BCA の鍵ペア

FIPS140-1 レベル 3 相当の HSM。

(2) SSL 証明書／コードサイニング証明書に係る鍵ペア

所定の手続に基づいて生成する。

６-１-９秘密鍵の利用目的

電子署名用とする。

６-２秘密鍵保護

６-２-１秘密鍵の保管について、要求される基準

(1) 個人認証 BCA の秘密鍵

FIPS140-1 レベル 3 相当の HSM により保護する。

(2) SSL 証明書／コードサイニング証明書に係る秘密鍵

所定の手続に基づいて保護する。

６-２-２秘密鍵の複数人制御

(1) 個人認証 BCA の秘密鍵

複数人の秘密鍵管理者により制御する HSM で秘密鍵を保護する。

(2) SSL 証明書／コードサイニング証明書に係る秘密鍵

所定の手続に基づいて保護する。

６-２-３秘密鍵の預託（エスクロー）

秘密鍵の預託は行わない。

６-２-４秘密鍵のバックアップ

(1) 個人認証 BCA の秘密鍵

秘密鍵のバックアップは、複数人の秘密鍵管理者による操作で行う。HSM からバックアップした個人認証 BCA の秘密鍵は､暗号化して秘密鍵管理者によって安全に保管する。但し、秘密鍵管理者は、バックアップ媒体を保管することとされている室の外に持ち出してはならない。

(2) SSL 証明書／コードサイニング証明書に係る秘密鍵

所定の手続に基づいて行う。

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) 個人認証 BCA の秘密鍵

秘密鍵は、複数人の秘密鍵管理者による操作で HSM の中で生成し、暗号モジュールへ

格納する。

(2) SSL 証明書／コードサイニング証明書に係る秘密鍵

規定しない。

６-２-７秘密鍵の活性化

(1) 個人認証 BCA の秘密鍵

秘密鍵は、複数人の秘密鍵管理者による操作により活性化する。

(2) SSL 証明書／コードサイニング証明書に係る秘密鍵

所定の手続に基づいて行う。

６-２-８秘密鍵の非活性化

(1) 個人認証 BCA の秘密鍵

秘密鍵は、複数人の秘密鍵管理者による操作により非活性化する。

(2) SSL 証明書／コードサイニング証明書に係る秘密鍵

所定の手続に基づいて行う。

６-２-９秘密鍵の破棄

(1) 個人認証 BCA の秘密鍵

暗号モジュール内の秘密鍵の破棄は、複数人の秘密鍵管理者が暗号モジュールを初期化等により完全に利用できない状態にする。なお、暗号モジュールを室外に持ち出す場合には、物理的に暗号モジュールを破壊する。

また、破棄する秘密鍵のバックアップ用暗号モジュールも同様に破棄することとする。

(2) SSL 証明書／コードサイニング証明書に係る秘密鍵

所定の手続に基づいて行う。

６-３鍵ペア生成管理に関する他の局面

６-３-１公開鍵の保管

公開鍵は、証明書のアーカイブに含まれ、本運用規程「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公開鍵及び秘密鍵の使用期間

(1) 個人認証 BCA の公開鍵及び秘密鍵

個人認証 BCA の自己署名証明書の有効期間は 10 年とする。個人認証 BCA の公開鍵及び秘密鍵の使用期間は、鍵を生成した日から起算して5年とし、5年ごとに鍵更新を行う。但し、暗号のセキュリティが脆弱になったと判断した場合には、暗号方式の変更を検討しその時点で鍵更新を行うことがある。

(2) SSL 証明書／コードサイニング証明書に係る公開鍵及び秘密鍵

個人認証 BCA が発行する SSL 証明書/コードサイニング証明書は、インターネット上で使用する場合、有効期間及び秘密鍵の使用期間は 1 年とする。インターネット上以外

で使用する場合、有効期間及び秘密鍵の使用期間は 5 年以内とする。

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) 個人認証 BCA の秘密鍵を格納する HSM の活性化データは、管理鍵により設定する。

(2) SSL 証明書／コードサイニング証明書に係る秘密鍵の活性化データは、所定の手続に基づいて生成、インストールする。

６-４-２活性化データの保護

(1) 個人認証 BCA の秘密鍵を格納する HSM の活性化に必要な管理鍵は、安全に保管する。

(2) SSL 証明書／コードサイニング証明書に係る秘密鍵の活性化データの保護は、所定の手続に基づいて行う。

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

個人認証 BCA に係るシステムには、信頼される OS の使用、アクセス制御機能、各要員の識別と認証機能、監査ログ及びアーカイブデータの収集機能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

システムのセキュリティ評価を随時実施する。

６-６ライフサイクルセキュリティ管理

６-６-１システム開発におけるセキュリティ管理

個人認証 BCA システムの開発、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、認証局システムの評価環境において検証を行い、認証局管理責任者の承認を得た上で導入する。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セキュリティ管理

個人認証 BCA 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

不正アクセスを防止するため、外部ネットワークとの通過を許可するネットワークサービスは必要最小限とする。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。

リポジトリに保有する情報のうち公開する情報はファイアウォールを介して提供する。

６-８暗号モジュールの技術管理

本運用規程「6-1-1 鍵ペアを生成する者、生成方法」及び「6-2-1 秘密鍵の保管について、要求される基準」において定める。

７証明書と失効記録（CRL/ARL)の内容

７-１証明書プロファイル

証明書プロファイルは、プロファイル設計書に定める。

７-２失効記録（CRL/ARL)プロファイル

失効記録（CRL/ARL)プロファイルは、プロファイル設計書に定める。

８運用規程の管理

８-１運用規程変更管理

運用会議は、本運用規程を必要に応じて変更する。

８-２開示及び通知

本運用規程を変更した場合には、運用会議は速やかに変更した運用規程を Web 上で公表する。これをもって、利用者及び証明書検証者への通知とする。

８-３運用規程承認手続

運用会議の決定をもって有効なものとする。