電子認証登記所（CRCA）

政府認証基盤(GPKI)ブリッジ認証局（BCA）との相互認証業務に関するCP/CPS

（Ver. 5.0）

令和元年11月29日

法　務　省

改　版　履　歴

版 数	日 付	改　版　内　容
1.0	2001/5/25	○ 初版発行
2.0	2003/11/4	○ 相互認証証明書の有効期間を2年から1年としたことによる変更 ○ 相互認証証明書，リンク証明書等をCRCAリポジトリから統合リポジトリへオンラインで複製することとしたこのによる変更 ○ 開発，修正又は変更したシステムの導入の承認をする権限を電子認証登記所の登記官が有する旨を明記 ○ 用語の整理等
3.0	2007/5/15	○ 会社法の施行に伴う整備法による商業登記法の改正による変更 ○ 自己署名証明書の失効情報の公表方法を明記 ○ 運用履歴ログの検査周期を明記 ○ 登記所職員の業務を明記 ○ 業務運用者及びオペレータの業務内容の分類を整理 ○ 用語の整理等
4.0	2014/12/13	○ 暗号アルゴリズム変更に伴う修正
5.0	2019/11/29	○ 暗号アルゴリズム移行完了に伴う修正 ○ 相互認証証明書の有効期間を1年から3年としたことによる変更 ○ CRCAの鍵ペアを更新する期間を1年から3年としたことによる変更 ○ CAの公開鍵と秘密鍵の有効期間を39月から72月としたことによる変更

政府認証基盤ブリッジ認証局との相互認証業務に関するCP/CPS

1．はじめに

本CP/CPSは、ブリッジ認証局（以下「BCA」という。）と相互認証を行う電子認証登記所（以下「CRCA」という。）の相互認証業務の運営に関する方針を定めることを目的とする。
本CP/CPSに定める事項は、CRCAが商業登記法その他関係法令に基づき実施すべき事項に変更を加えるものではない。
なお、本CP/CPSにおいては、CRCAが法令に基づき実施する事項のうち本CP/CPSの内容を理解する上で参考となると思われる事項を、※印を付して記す。
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、具体的な記述においては、「府省認証局CP/CPSガイドライン」（平成17年9月1日行政情報化推進各省庁連絡会議基本問題専門部会了承）の項目内容を基礎としている。

1．1 概要

CRCAは、商業登記法その他関係法令等に定めるところにより「電子証明書」の発行等に係る認証事務を処理するほか、本CP/CPSに定めるところにより、当該「電子証明書」取得者（以下「利用者」という。）と政府との間の申請・届出等手続の電子化に資するため、BCAとの間で相互認証証明書を取り交わす。
CRCAは、BCAとの相互認証業務に関して、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をその運営に関する方針として位置付ける。

1．2 識別

CRCAの証明書ポリシは、次の識別子で示される。

CRCA相互認証証明書ポリシ：
1.2.392.100300.1.3.3(SHA-256用)
CRCA相互認証テスト用証明書ポリシ：
1.2.392.100300.1.3.96(SHA-256用)

※「電子証明書」ポリシ：
商業登記法第12条の2第9項及び第148条（他の法令において準用する場合を含む。以下同じ。）の法務省令に定めるところによる。

1．3 運営体制と証明書の適用範囲

1．3．1 CAの組織

（1） 相互認証業務の運営組織

相互認証業務に係るCRCAの運営は、電子認証登記所(東京法務局)の登記官（電子認証管理官）が行う。
なお、政府の方針として実施する相互認証業務に係るCRCAの運営の方針は、法務省民事局商事課において決定する。法務省民事局商事課は、組織上の権限に基づき、電子認証登記所の登記官が行うCRCAの運営に関して、必要な助言、指導等を行う。

※認証に係る方針及びその実施に必要な事項は関係法令に定めるところにより、実施方針等の変更には、当該法令の改正を要する。

（2） 電子認証登記所の登記官

相互認証業務は、本CP/CPSに基づき、電子認証登記所の登記官が行う。

※商業登記法第12条の2の規定（他の法令において準用する場合を含む。以下同じ。）による認証事務は、法務大臣の指定を受けた電子認証登記所の登記官が行う。
電子認証登記所のCAシステム運営に携わる要員とその役割については、「5.2 手続面の管理」において定めるところによる。

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、3年とする。

※商業登記法第12条の2に定めるところによる。
なお、「電子証明書」の有効期間（証明期間）は、同条第1項第2号の期間をいう。

1．4 CP/CPSに関する連絡先

1．4．1 管理担当部署

法務省民事局商事課

1．4．2　照会窓口
管理担当部署に同じ。

2．一般規定
2．1　義務
2．1．1　CA業務に関する義務
相互認証業務に関し、CRCAは、次の義務を負う。
・本CP/CPSに基づき、相互認証証明書、リンク証明書等を発行する。
なお、これら証明書に係るCRCAの自己署名証明書は、商業登記法第12条の2の規定により発行する「電子証明書」に係るそれと同一とする。
・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。
・BCAとの相互認証に際して、正確な情報を提示する。

・BCAの定めた手続に従い、相互認証証明書等の失効処理を行う。
・商業登記法12条の2第8項の有効性に係る証明と同一の方法により、相互認証証明書等の有効性について照会に応じる。失効リストは発行しない。
・CRCAの秘密鍵を安全に管理する。
・CRCAの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、失効等に関する運用履歴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。

※商業登記法第12条の2に定めるところによる。

2．1．2　RA業務に関する義務
CRCAは、RA業務に関して次の義務を負う。
・CRCA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。
・相互認証証明書の発行要求に係る手続が適切に行われていることを確認する。

※商業登記法第12条の2及び第148条の法務省令に定めるところによる。

2．1．3　※「電子証明書」利用者の義務
※商業登記法12条の2参照

2．1．4　※「電子証明書」検証者の義務
※商業登記法12条の2及び後記「4．4．10　CRL/ARLの確認」参照

2．1．5　リポジトリに関する義務
CRCAが相互認証業務に関して発行する自己署名証明書、リンク証明書及び相互認証証明書は、BCAの定めるところに従い、BCAの統合リポジトリに複製する。

2．2　CAの責任
CRCAは、BCA及び利用者に対し、本CP/CPSに基づく相互認証業務を適切に行う。

※商業登記法12条の2に定めるところによる。

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に基づく相互認証業務から生じる紛争については、日本国の法令を適用する。

※商業登記法その他の日本国の法令

2．4．2　分割、存続、合併及び通知
規定しない。

※日本国の法令に定めるところによる。

2．4．3　紛争解決の手続
規定しない。

※日本国の法令に定めるところによる。

2．5　料金
規定しない。

※商業登記法13条第1項の政令に定めるところによる。

2．6　公表とリポジトリ
2．6．1　CAに関する情報の公表
CRCAの相互認証に関する情報の公表は、BCAの統合リポジトリ、法務省のWeb等において公表する。
（1）BCAの統合リポジトリ上での公表
CRCAが保有する次の情報は，BCAの統合リポジトリに複製し、BCAの定めるところに従い，統合リポジトリ上で公表される。
・ 相互認証業務に関し、CRCAが発行した自己署名証明書、リンク証明書及び相互認証証明書

（2）CRCAによる情報提供
相互認証業務に係る相互認証証明書、リンク証明書等の有効性に関する情報は、商業登記法第12条の2第8項の証明と同一の方法により提供する。

（3）Web上での公表
CRCAは、次の情報を法務省のWeb上で公表する。
・ CRCAと相互認証するCAの名称及び相互認証を取り消したCAの名称
・ CA秘密鍵危殆化に関する情報の通知
・ 本CP/CPS

※CRCAに関する情報の公表は、次のとおり、官報、法務省のWeb等において公表する。

・CRCAの業務に係る根拠法令は、官報において公示されるほか、その主要なものを法務省のWeb上で公表する。
・「電子証明書」の利用に関して留意すべき事項その他制度の概要は、法務省のWeb上で公表する。
・CRCAが発行する「電子証明書」等による証明は、商業登記法第12条の2に定めるところによる。リポジトリによる公表は行わない。
・CRCAの自己署名証明書のメッセージ・ダイジェストは、法務省のWeb等において公表する。

2．6．2　公表の頻度
公表する情報は、内容に変更の生じる都度、更新する。

2．6．3　アクセス制御
「2．6．1　CAに関する情報の提供」の（1）から（3）までに掲げる情報は、インターネット及びその他の方法により提供する。
インターネットを通じて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
「2．6．1　CAに関する情報の公表」の（1）に掲げる情報は、BCAの統合リポジトリに複製し、公表される。

2．7　準拠性監査
2．7．1　監査頻度
CRCAは年1回定期的に監査を実施する。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
CRCAの監査は、監査業務及び認証業務に精通した者によって行う。

2．7．3　監査人と被監査部門の関係
監査は、被監査人と利害関係を有しない者によって行う。

2．7．4　監査テーマ
本CP/CPSのほか所定の監査基準に準拠していることを中心に実施する。

※関係法令のほか所定の監査基準に準拠していることを中心に実施する。

２．７．５　監査指摘事項への対応
監査における緊急を要する重大な指摘事項については、速やかに改善策を講じる。

２．７．６　監査結果
監査結果に係る報告書は、電子認証登記所及び法務省民事局商事課において5年間保管する。また、本CP/CPSの準拠性に関する監査結果を、BCA運営組織に報告する。

２．８　機密保持
２．８．１　機密扱いとする情報
漏えいすることによってCRCA及びBCAの認証業務の信頼性が損なわれるおそれのある情報を、機密情報と位置付ける。機密情報は、安全に保管管理する。

２．８．２　機密扱いとしない情報
「２．６．１　CAに関する情報の公表」に明記するところによる。

２．８．３　証明書失効情報の公表
CRCAは、リンク証明書及び相互認証証明書の失効情報を、商業登記法第１２条の２第９項に定める方法と同一の方法により、証明書検証者に提供する。また、自己署名証明書の失効情報に関する情報の公表は、官報、法務省のWeb等において行う。

※「電子証明書」の失効情報の提供は、商業登記法第１２条の２第８項及び第９項に定めるところによる。

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
CRCAが相互認証業務に関して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。

※商業登記法第１２条の２第９項及び第１４８条の法務省令に定めるところによる。

３．１．２　名前の意味に関する要件
CRCAが相互認証業務に関して発行する証明書に使用する名称は、以下に準ずる。

※商業登記法第１２条の２第９項及び第１４８条の法務省令に定めるところによる。

３．１．３　名前形式を解釈するための規則
CRCAが相互認証業務に関して発行する証明書に使用する名称は、以下に準ずる。なお，名前の形式を解釈するための規則は、BCAの定める規則と適合している。

※商業登記法第１２条の２第９項及び第１４８条の法務省令に定めるところによる。

３．１．４　名前の一意性
CRCAが相互認証業務に関して発行する証明書の主体者名は、一意に割り当てる。

※商業登記法第１２条の２第９項及び第１４８条の法務省令に定めるところによる。

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
CRCA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、含まれている公開鍵に対応する秘密鍵で署名されていることを確認する。また、証明書発行要求のフィンガープリントを確認し、公開鍵の所有者を特定する。
※「電子証明書」発行申請において提出された申請人の公開鍵と署名情報を基に、その公開鍵が署名に使用された秘密鍵と対をなすものであることを確認する。

３．１．８　組織の認証
CRCAは相互認証手続において、所定の手続に基づき、相互認証先がBCAであることを確認する。

※商業登記法第１２条の２第３項の登記事項に基づく。

３．１．９　※個人の認証
※商業登記法第１２条の２及び第２０条に定めるところによる。

３．２　証明書の更新
相互認証業務に係る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
相互認証業務に係る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　証明書の失効要求
相互認証業務に係る証明書の失効要求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。

※商業登記法第１２条の２第７項等に定めるところによる。

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）　※「電子証明書」
※商業登記法第１２条の２第１項から第４項までに定めるところによる。

４．２　証明書の発行
（１）　相互認証証明書
CRCA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）　※「電子証明書」
※商業登記法第１２条の２第５項及び第９項に定めるところによる。

４．３　証明書の受入れ
（１）　相互認証証明書
CRCAは、発行した相互認証証明書を所定の手続に基づいてBCAへ送付し、受領書を受取る。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）　※「電子証明書」
※商業登記法第１２条の２に定めるところによる。

4．4　証明書の失効と一時停止

4．4．1　証明書の失効事由

（1）　相互認証証明書

CRCAは、CRCA又はBCAに以下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の秘密鍵の危殆化
・相互認証基準違反
・相互認証業務の終了
・相互認証更新

（2）　※「電子証明書」

※商業登記法第12条の2第7項及び第8項並びに同法第148条の法務省令に定めるところによる。

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要求を受ける場合

BCAからCRCAに対する失効要求はBCAの責任者が行う。

イ　BCAに相互認証証明書失効要求を行う場合

CRCAからBCAに対する失効要求は電子認証登記所の登記官が行う。

（2）　※「電子証明書」

※商業登記法第12条の2第7項及び第8項並びに同法第148条の法務省令に定めるところによる。

4．4．3　証明書の失効要求及び失効処理手順

（1）　相互認証証明書

ア　BCAから相互認証証明書失効要求を受ける場合

「3．1．8　組織の認証」において定める手続を行った上で、相互認証証明書を失効する。

イ　BCAに相互認証証明書失効要求を行う場合

BCAとの相互認証証明書の失効を要求する。

（2）　※「電子証明書」

※商業登記法第12条の2第7項及び第8項並びに同法第148条の法務省令に定めるところによる。

4．4．4　失効における猶予期間

CRCAは、失効申請手続の終了後、直ちに失効処理を行う。

※商業登記法第12条の2第7項及び第8項並びに同法第148条の法務省令に定めるところによる。

4．4．5　一時停止

CRCAは、相互認証業務に係る証明書の一時停止を行わない。

※商業登記法第12条の2第8項第4号及び第148条の法務省令に定めるところによる。

4．4．6　一時停止申請者

規定しない。

※商業登記法第12条の2第8項第4号及び第148条の法務省令に定めるところによる。

4．4．7　一時停止手順

規定しない。

※商業登記法第12条の2第8項第4号及び第148条の法務省令に定めるところによる。

4．4．8　一時停止期間の制限

規定しない。

※商業登記法第12条の2第8項第4号及び第148条の法務省令に定めるところによる。

4．4．9　CRL/ARLの発行周期
証明書の失効情報の提供は、CRL/ARLを発行する方法によらない。CRCAが相互認証業務に関し発行する証明書の有効性の確認の方法は、商業登記法第12条の2第8項及び第9項に定める方法と同一の方法による。

※CRL/ARLは発行しない。「電子証明書」の有効性は、商業登記法第12条の2第8項及び第9項に定める方法により証明する。

4．4．10　CRL/ARLの確認
証明書の失効情報の提供は、CRL/ARLを発行する方法によらない。CRCAが相互認証業務に関し発行する相互認証証明書及びリンク証明書の検証者は、商業登記法第12条の2第8項及び第9項に定める方法と同一の方法により、当該証明書の有効性を確認しなければならない。

※CRL/ARLは発行しない。「電子証明書」の有効性は、商業登記法第12条の2第8項及び第9項に定める方法により証明する。

4．4．11　オンライン有効性確認の可用性
CRCAが相互認証業務に関し発行する相互認証証明書及びリンク証明書の検証者は、商業登記法第12条の2第8項及び第9項に定める方法と同一の方法により、当該証明書の有効性を確認できる。

※商業登記法第12条の2第8項、及び第9項に定めるところによる。

4．4．12　オンライン有効性確認要件
規定しない。

※商業登記法第12条の2第8項及び第9項に定めるところによる。

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　CAの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
CRCAシステムにおける発生事象を記録したログ（以下「運用履歴ログ」という。）を検査し、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　運用履歴ログに記録する情報
CRCAシステムに関す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、操作ログ等運用履歴ログを記録する。運用履歴ログには、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　運用履歴ログの検査周期
運用履歴ログ検査者は、運用履歴ログの検査を月次、定期監査時及び障害発生等による必要時に行う。

4．5．3　運用履歴ログの保管期間
運用履歴ログは10年間保管する。

4．5．4　運用履歴ログの保護
運用履歴ログは、改ざん防止対策を施し、かつ改ざん検出を可能とする。
運用履歴ログのバックアップは、日次で外部記憶媒体に取得し、適切に入退出管理された室内に設置する施錠可能な保管庫に保管する。

4．5．5　運用履歴ログのバックアップ手順
運用履歴ログは日次で外部記憶媒体にバックアップを取得する。

4．5．6　運用履歴ログの収集システム
運用履歴ログの収集機能はCRCAシステムの一機能とし、システムの起動時からセキュリティに関する重要な事象を収集する。

4．5．7　運用履歴ログ検査の通知
運用履歴ログの検査は、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
必要に応じて運用履歴ログ等の情報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
・証明書状態DB
・運用履歴ログ

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20年間保管する。ただし、運用履歴ログについては、「4．5．3　運用履歴ログの保管期間」に定めるところによる。

※商業登記法第148条の法務省令参照

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、ディスクから削除する前に外部記憶媒体に取得し、適切に入退出管理された室内に設置する施錠可能な保管庫に保管する。ただし、運用履歴ログについては、「4．5．4　運用履歴ログの保護」に定めるところによる。

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、ディスクから削除する前に外部記憶媒体に取得する。ただし、運用履歴ログについては、「4．5．5　運用履歴ログのバックアップ手順」に定めるところによる。

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、アーカイブする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
3年ごとにCRCAの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、BCAの統合リポジトリ上で公表される。

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、データが損傷した又は無効になった場合の対処
ハードウェア、ソフトウェア、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。失効後に，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。

※同上
なお、失効した「電子証明書」利用者に対し、再発行をする必要がある場合には、当該利用者の申請又はその同意に基づき、新たな「電子証明書」の発行処理を行う。

4．8．3　CAの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、認証業務を停止し、所定の手続に基づき、次の処理を行う。
・証明書の失効処理
・CA秘密鍵の廃棄及び再生成処理
・証明書の再発行手続

※商業登記法第3条及び同法第１４８条の法務省令に定めるところによるほか、「電子証明書」利用者への周知を図り、上記に準じて処理する。
なお、「電子証明書」利用者の秘密鍵が危殆化した場合は、商業登記法第１２条の2第7項の届出をすることができる。

4．8．4　自然災害等発生後の設備の確保
CRCAの施設・設備が罹災した場合には、予備機、バックアップデータ等を用いるなどして速やかに運用を再開する。

4．9　認証業務の終了
CRCAの相互認証業務を終了するときは、業務終了90日前までにその旨、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公表した上で、所定の業務終了手続を行う。

※CRCAの認証業務の終了は法改正による。その内容は、官報において公示される。その他、「2．6．1　CAに関する情報の公表」を参照。

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
CRCAの施設は、水害、地震及び火災その他の災害の被害を容易に受けない場所に設置され、建物構造上、耐震、耐火及び不正侵入防止対策が講じられる。
また、使用する機器、装置類は、災害及び不正侵入から防護された安全な場所に設置される。

5．1．2　物理的アクセス
建物内は入退館等に際して資格審査が行われ、識別証等により入退出が管理される。
CRCA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が行われる。その認証には、各室内において行われる認証業務の重要度に応じ、操作権限者が識別できるICカード及び生体認証等が用いられるほか、権限者のデュアルアクセスが要求される。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、電子認証登記所の登記官が、法務省民事局商事課の承認を得て指定した者に付与される。
建物内及びCRCA施設内は、別個の監視システムにより監視要員によって24時間365日監視が行われる。

5．1．3　電源設備及び空調設備
CRCA施設は、機器類の運用のために十分な容量の電源が確保され、瞬断、停電、電圧・周波数の変動に備えた対策が講じられる。商用電源が供給されない事態においては、自家発電機による電源供給に切り換えられる。
空冷式空調設備により機器類の動作環境及び要員の作業環境は適切に維持される。

5．1．4　水害対策
CRCAの設備が設置される建物及び各室には漏水検知器が設置され、天井、床には防水対策が講じられる。

5．1．5　地震対策
CRCAの設備が設置される建物は強固な支持基盤を有する耐震構造・形状とし、機器･什器類は転倒、落下防止策が講じられる。

5．1．6　火災対策
CRCAの設備が設置される建物は耐火構造、各室は防火区画とし、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、適切に入退出管理された室内に設置する施錠可能な保管庫に保管するとともに、適切に搬入出管理を行う。

5．1．8　廃棄物処理
機密情報を含む書類・記憶媒体の廃棄については、適切に廃棄処理を行う。

5．1．9　オフサイトバックアップ
重要なデータを記録する媒体等を別地保管する必要がある場合には、移送方法のセキュリティを確保し、媒体の保管・管理には、CRCAの施設に準じたセキュリティ対策を講じる。

５．２　手続面の管理

CRCAは、CA秘密鍵の保管・生成等に係る操作、相互認証業務に係る証明書の発行・失効等に係る操作等の重要な業務の実施に当たっては、業務の重要度に応じ、複数人の要員の合議操作、責任者の立会等による相互牽制を行う。
要員がシステム操作を行う際、システムは、要員が正当な権限者であることの識別・認証を行う。
各要員の業務の概要は、以下のとおり。この場合において、業務運用者とオペレータは、各2グループから構成され、それぞれに定める業務のうちCA秘密鍵の生成等の業務に携わるグループの要員は、権限上証明書の発行等の業務に携わることはできない。

〇電子認証登記所の登記官
・認証業務の統括
・CA秘密鍵の危殆化時、災害発生時等緊急時における対応の統括
・業務運用者への作業指示及び作業結果の確認
・その他CRCAの運営及び運用に関する統括
・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に対する鍵操作およびCA秘密鍵のバックアップ媒体のセット
・BCAからの相互認証証明書の発行要求の受付及び申請書類等の管理
・相互認証証明書等の発行、失効等の処理
・相互認証証明書、リンク証明書等のCRCAリポジトリから統合リポジトリへの複製

〇登記所職員
・受付
・審査
・RA操作

〇業務運用者
【鍵グループ】
・HSMの機能を制御する鍵の保管管理
・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に対する鍵操作およびCA秘密鍵のバックアップ媒体のセット

【証明書グループ】
・自己署名証明書の発行

【業務運用者共通の作業】
・CAシステムの起動・停止
・CAシステムの動作に関する設定変更管理
・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
・相互認証証明書、リンク証明書等のCRCAリポジトリから統合リポジトリへの複製

【業務運用者要員限定（鍵、証明書の操作にかかわらない者）の作業】
・ログの検査、ログの削除

〇オペレータ
【鍵グループ】
・HSMの機能を制御する鍵の保管管理
・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に対する鍵操作およびCA秘密鍵のバックアップ媒体のセット

【証明書グループ】
・自己署名証明書の発行
※「電子証明書」発行等の権限等については、商業登記法第１２条の２第８項及び同法第１４８条の法務省令に定めるところによる。

５．３　人事面の管理

CRCAの運用を行うすべての要員は、その業務に応じて必要な専門知識及び技術を修得するための教育訓練を受ける。

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 鍵ペア生成

(1)CA鍵
CRCAの鍵ペアは、複数人の鍵管理者の合議によりFIPS140-1レベル3相当のHSMを用いて生成する。

(2)※「電子証明書」鍵
※「電子証明書」の鍵ペアの生成は申請人が行う。その方法には関知しない。

6．1．2 ※証明書利用者への秘密鍵配布

※商業登記法第12条の2第2項参照。CRCAは「電子証明書」利用者に秘密鍵を配布しない。

6．1．3 公開鍵の受領

CRCA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な手段で受け取る。

※「電子証明書」の発行申請時の申請人公開鍵の受領については、商業登記法第12条の2第2項及び同法第148条の法務省令に定めるところによる。

6．1．4 CA公開鍵の配付

商業登記法第12条の2第9項及び第148条の法務省令に定めるところに準じる。

※商業登記法第12条の2第9項及び第148条の法務省令に定めるところによる。

6．1．5 鍵のサイズ

（1） CA鍵
RSA2048ビットの鍵を使用する。

（2） ※「電子証明書」鍵
※商業登記法第12条の2第1項第1号の法務省令に定めるところによる。

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 ハードウェア／ソフトウェアによる鍵生成

「6.1.1鍵ペア生成」において定めるところによる。

6．1．9 鍵の利用目的

（1）CA鍵
CRCAの秘密鍵は、署名に用いる。

（2）※「電子証明書」鍵
※商業登記法第12条の2第1項第1号参照

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
CRCAの秘密鍵は、FIPS140-1レベル3相当のHSM内で保護する。

（2）※「電子証明書」鍵
※「電子証明書」利用者の秘密鍵の管理には関知しない。

6．2．2 秘密鍵の複数人制御

CA秘密鍵の生成、バックアップ、破棄等の操作は、複数人の鍵管理者の合議により行われる。

6．2．3 秘密鍵の預託

※「電子証明書」利用者の秘密鍵の管理には関知しない。

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、複数人の鍵管理者の合議により行われる。
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、各鍵管理者が安全に保管する。

６．２．５　秘密鍵のアーカイブ
CA秘密鍵のアーカイブは行わない。

６．２．６　暗号モジュールへの秘密鍵の格納
（1）CA鍵
CA秘密鍵は、複数人の鍵管理者の合議により暗号モジュールの中で生成し、格納する。

（2）※「電子証明書」鍵
※「電子証明書」の秘密鍵の生成は申請人が行う。その方法には関知しない。

６．２．７　秘密鍵の活性化方法
（1）CA鍵
CA秘密鍵は、複数人の鍵管理者の合議により行うCA鍵生成手続において指定する日時から自動的に活性化される。
（2）※「電子証明書」鍵
※「電子証明書」利用者の秘密鍵には関知しない。

６．２．８　秘密鍵の非活性化方法
（1）CA鍵
CA秘密鍵は、複数人の鍵管理者の合議により行うCA鍵生成手続において指定したその使用期間の満了又は証明書の失効処理によって非活性化される。

（2）※「電子証明書」鍵
※「電子証明書」利用者の秘密鍵には関知しない。

６．２．９　秘密鍵の破棄方法
（1）CA鍵
CA秘密鍵の削除は、複数人の鍵管理者の合議により行う。HSMから削除後、秘密鍵バックアップ媒体を物理的に破棄する。

（2）※「電子証明書」鍵
※「電子証明書」利用者の秘密鍵には関知しない。

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
公開鍵を含む証明書はアーカイブされ、「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
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72月とし、3年ごとに鍵の更新を行う。ただし、暗号のセキュリティが脆弱になったと判断される場合等においては、その時点で鍵の更新を行う。

（2）※「電子証明書」鍵
※商業登記法第12条の2第1項第2号及び第7項並びに同法第148条の法務省令に定めるところによる。

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
「６．２．７　秘密鍵の活性化方法」参照。

（2）※「電子証明書」鍵
※「電子証明書」利用者の秘密鍵には関知しない。

６．４．２　活性化データの保護
（1）CA鍵
「６．２．７　秘密鍵の活性化方法」参照。

（2）※「電子証明書」鍵
※「電子証明書」利用者の秘密鍵には関知しない。

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

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、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 システム開発における評価

CRCAのシステムの開発、修正又は変更に当たっては、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、法務省民事局商事課及び電子認証登記所の登記官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管理

CRCA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

CRCAとインターネット等の外部システムとは、ファイアウォール等を介して接続される。

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」において定めるところによる。

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

法務省のWeb上で別途公表するところによる。

※商業登記法第12条の2第9項及び第148条の法務省令に定めるところによる。

7．2 CRL/ARLのプロファイル

CRL/ARLは発行しない。証明書の有効性に係る証明のプロファイルについては、法務省Web上で公表するところによる。

※CRL/ARLは発行しない。「電子証明書」の有効性に係る証明の方式については、商業登記法第12条の2及び第148条の法務省令に定めるところによる。

8．CP/CPSの管理

8．1 CP/CPSの変更

法務省民事局商事課は、本CP/CPS（法令に基づき実施する事項を除く。）を必要に応じて変更する。

8．2 CP/CPSの公表と通知

法務省民事局商事課は、本CP/CPS（法令に基づき実施する事項を除く。）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

本CP/CPS（法令に基づき実施する事項を除く。）は、法務省民事局商事課において決定した日又は当該決定において定めた日から有効なものとなる。本CP/CPSを変更する場合も同様とする。