DIACERT-PLUS サービス
運用規程

（Ver 1. 08）

2018 年 2 月 6 日

ジャパンネット株式会社

目次

改訂履歴

Version	作成内容／改訂内容	作成日/改訂日	作成者/改訂者	承認日	承認者
1.00	初版	2015/01/21	合田　悠資	2015/01/21	角野　章之
1.01	失効申請の必須項目を改訂 認証業務停止を伴う災害時の対応を規程 利用者氏名のフリガナの規程を改訂 個人番号の取扱いについて規定	2015/12/08	室田　邦雄	2015/12/08	角野　章之
1.02	問合せ先変更	2016/03/14	合田　悠資	2016/03/14	角野　章之
1.03	記録媒体の保管庫の名称を変更	2016/12/08	室田　邦雄	2016/12/08	角野　章之
1.04	個人情報保護に関する規程追記	2017/04/10	室田　邦雄	2017/04/10	角野　章之
1.05	法人番号に関する規程追加	2017/05/19	室田　邦雄	2017/05/19	角野　章之
1.06	利用者住所に関する規程追加	2017/08/01	室田　邦雄	2017/08/01	角野　章之
1.07	旧姓の利用に関する規程の追加 問い合わせ先訂正 証明書情報の公開方法修正 利用者住所の記載に関する規程改訂 失効に関する規程の改訂 記録の保存に関する規程の改訂 利用者情報プロファイル修正 誤記訂正	2017/12/28	室田　邦雄	2017/12/28	角野　章之
1.08	利用者氏名のローマ字に関する規程の改訂	2018/02/06	室田　邦雄	2018/02/06	角野　章之

1 はじめに

ジャパンネット株式会社は、「DIACERT-PLUS 認証局」（以下、「本認証局」という。）を設置し、「DIACERT-PLUS サービス電子証明書」（以下、「利用者証明書」という。）を利用者に対して発行する。

1.1 概要

本文書は、本認証局が「DIACERT-PLUS サービス」（以下、「本サービス」という。）として認証業務を行なう際の運用に関する規程（CPS: Certification Practice Statement、以下、「本規程」という。）である。

本規程は、利用者証明書の発行、失効及びその他の運用管理等の手続きについて規定する。また公開鍵インフラストラクチャ（PKI: Public Key Infrastructure、以下、「PKI」という。）の構成要素である認証局、及び利用者と署名検証者の義務責任について規定する。

本サービスは、「電子署名及び認証業務に関する法律」（平成 12 年 5 月 31 日法律第 102 号、以下、「電子署名法」という。）の規定に基づく認定を受けた特定認証業務である。

また本認証局は政府が運営するブリッジ認証局（以下、「BCA」という。）との相互接続を行う。

1.2 文書名と識別

本規程の名称は、「DIACERT-PLUS 認証局運用規程」とする。

本サービスに係るオブジェクト識別子（OID）を、表 1-1 に示す。

表 1-1 本サービスに係る OID とオブジェクト

OID	オブジェクト
1.2.392.200127.10.	DIACERT-PLUS サービス
1.2.392.200127.10.1.1	DIACERT-PLUS 証明書ポリシー（利用者証明書）
1.2.392.200127.10.1.2	DIACERT-PLUS 相互認証証明書用ポリシー（BCA用）

本サービスでは DIACERT-PLUS （電子入札用電子証明書）の利用者証明書を取り扱う。

1.3 PKI の関係者

本サービスに係る関係者とその役割を、表 1-2 に示す。

表 1-2 関係者とその役割

関係者	役割

利用者	日本在住の日本人及び日本に居住する日本国籍を持たない外国人（住民基本台帳法第 30 条の 45 に規定される外国人住民（以下、「外国人」という））で以下の者。 ・法人を代表する個人 ・法人を代表する個人から入札などに関する権限を委任された者 ・個人事業主 ・個人事業主から入札などに関する権限を委任された者 本認証局に対し、利用者証明書の利用申込みを行い、利用者証明書を受領する。 利用者は本規程に同意し、本規程の利用者の義務を遵守しなければならない。
署名検証者	利用者証明書を信頼し、利用する者。 署名検証者は、本規程内容について理解し同意した上で、利用者証明書を利用しなければならない。
認証局 （CA*1）	本サービスの認証業務を行う。 審査登録局、発行局及びリポジトリから構成される。 BCA と相互認証する。 *1:Certification Authority
審査登録局 （RA*2）	利用者から受け付けた利用者証明書の利用申込み又は、利用者証明書の失効申請について真偽確認を行い、許可した利用者証明書の発行要求又は、失効要求を発行局に対して行う。 RA のコンピュータシステムは、利用者情報登録と発行および失効要求を行う登録用 RA 端末と RA 端末から入力されたデータを蓄積する IA/RA サーバから構成される。 *2:Registration Authority
発行局 （IA*3）	審査登録局からの証明書発行要求又は、証明書失効要求に基づき、CA 証明書、リンク証明書、相互認証証明書及び利用者証明書の発行又は、失効を行う。 証明書失効リスト（以下、「CRL*4 /ARL*5/fullCRL*6」という。）の発行を行う。 利用者秘密鍵、利用者公開鍵のペアの生成、PIN*7 コードの生成及び IC カードの利用者秘密鍵と利用者証明書の格納を行う。 発行局より発行された IC カードを利用者に安全に発送する。 本認証局の CA 秘密鍵の生成から廃棄までのライフ管理及び運用管理を行う。 IA のコンピュータシステムは、証明書を発行するための発行用 RA 端末、IA/RA 端末と IA/RA サーバから構成される。 *3:Issuing Authority *4:Certificate Revocation List *5:Authority Revocation List *6: full Certificate Revocation List *7: Personal Identification Number
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 が電子署名を付与することでその公開鍵の正当性を保証する。 本サービスが発行する証明書としては下記のものがある。 ・CA 証明書 ・リンク証明書 ・相互認証証明書 ・利用者証明書
リポジトリ	本規程、CRL/ARL/fullCRL の情報、CA 証明書、リンク証明書、相互認証証明書、CA 証明書のフィンガープリント、DIACERT-PLUS サービス利用規約（以下、「利用者同意書」という。）、DIACERT-PLUS サービス署名検証者同意書（以下、「署名検証者同意書」という。）、その他、本サービスの情報等を保管し、公開する。
企業等	利用者の所属する法人、個人事業主を総称したもの。
組織等	利用者の所属する、法人、商業登記していない団体、個人事業主を総称したもの。
ブリッジ認証局 （BCA*8）	行政機関の認証局、民間の認証局との間に相互認証証明書を発行して、認証基盤の要としての役割を果たす認証局。 *8:Bridge CA

1.4 証明書の用途

(1) 本サービスにより発行される利用者証明書は電子入札コアシステム等の政府・地方自治体が実施する電子入札（電子調達を含む）及び電子申請の電子署名の用途において使用しなければならない。

利用者証明書が用途以外の目的で使用された場合、本認証局は一切の責任を負わない。本サービスで使用する証明書の有効期間は、以下のとおりとする。

① CA 証明書：10 年
② リンク証明書（NewWithOld）：新 CA 証明書の開始日から旧 CA 証明書の終了日まで
③ リンク証明書（OldWithNew）：旧 CA 証明書の開始日から旧 CA 証明書の終了日まで
④ 相互認証証明書：5 年以内
⑤ 利用者証明書：1 年、2 年、3 年、4年 10 ヶ月

利用者証明書の有効期間満了日時は、発行日から選択した期間後の月末日の 23 時 59 分 59 秒迄である。本認証局は有効期間が満了する前の本認証局指定期日迄に、有効期間が切れる旨の通知を利用者宛に行うが、当該利用者証明書の自動更新及び自動継続は行わない。

(2) BCA との相互認証により、利用者と行政機関側の処分権限者との間で相互に証明書を検証するための認証パスを構築できるようにする。

1.5 ポリシー運用管理

1.5.1 ポリシーを管理する組織

本認証局は、本規程に定めた仕様を変更する権利を有する。本認証局は、利用者や署名検証者に事前の了解を得ることなく本規程に定めた仕様の変更をすることが出来る。仕様変更の内容は、認証業務審議会での審議を経て、電子認証局責任者が変更承認する。

1.5.2 問い合わせ先

利用者は、本サービスに関するサービス内容について、電話、FAX 又は、電子メールにて問い合わせることができる。

本サービスに関する問合せ先は、次のとおりである。

［問合せ先］
窓口： ジャパンネット株式会社 営業部
住所： 〒108-0023 東京都港区芝浦 4-16-36 住友芝浦ビル 7F
電話： 03-6771-5109
FAX： 03-6771-5017
電子メールアドレス：japannet.info@mind.co.jp
受付日：月曜日から金曜日（祝祭日、当社休業日※を除く）
受付時間：9:00～12:00 13:00～17:00（日本時間）

※ 当社休業日はホームページ（http://www.diacert.jp/plus/）で公開する。

1.5.3 CPS のポリシー適合性を決定する者

本規程「1.5.1 ポリシーを管理する組織」の規定に従うものとする。

1.5.4 CPS 承認手続き

本規程は、認証業務審議会が承認する。

1.6 用語

表 1-3 文書内の略称及びその内容

用 語	正式名	内 容
ARL	Authority Revocation List	CA 証明書、リンク証明書及び相互認証証明書の失効情報を格納する失効リスト。
BCA	Bridge CA	行政機関の認証局及び民間の認証局との間に相互認証証明書を発行して、認証基盤の要としての役割を果たす認証局。
CA	Certification Authority	認証局（Certification Authority）の略。電子入札、電子商取引等で使われる電子的な身分証明書を発行・管理する機関。RA、IA 及びリポジトリで構成する。
CRL	Certificate Revocation List	その認証局が発行した利用者証明書のうち、利用者証明書の有効期間内に失効された利用者証明書の情報を格納した利用者証明書の一覧。利用者証明書の有効性検証を行う場合には、利用者証明書の署名の検証を行うとともに、この失効リストに検証すべき利用者証明書が掲載されていないかを確認する。
fullCRL	full Certificate Revocation List	その認証局が発行した有効期間内に失効されたすべての CA 証明書、リンク証明書及び相互認証証明書、ならびに利用者証明書の一覧。issuingDistributionPoint のフィールドは使用しない。
GPKI	Government Public Key Infrastructure	行政手続きの電子化で基盤となる政府公開鍵暗号を用いた社会基盤システム。
IA	Issuing Authority	RA からの証明書発行請求又は証明書失効請求に基づき、証明書及び失効リストの発行を管理する機関。証明書の発行及び証明書の失効処理を行い、失効した証明書を失効リストとしてリポジトリへ掲載する。
RA	Registration Authority	利用者から受付けた利用申込み又は失効申請等について真偽確認を行い、許可した利用者証明書の発行請求を IA に対して行う又は利用者証明書の失効を行う機関。利用者

		証明書の利用者情報を管理する。
PIN コード	利用者証明書の Personal Identification Number	利用者証明書を保護する暗証番号。
リポジトリ	―	本規程、利用者同意書、署名検証者同意書、CA 証明書、CA 証明書のフィンガープリント等の利用者等に公開する情報及び署名検証のために必要な情報を掲載する Web サーバ並びに証明書の失効情報（CRL/ARL/fullCRL）、CA 証明書、リンク証明書及び相互認証証明書を掲載するディレクトリサーバ等の総称。
フィンガープリント	―	「拇印」という意味で、デジタル証明書及びメッセージが改ざんされていないことを証明するためにデジタル証明書並びにメッセージ本文にハッシュ関数をかけて得られたハッシュ値。
リンク証明書	―	CA 証明書の更新の際に発行される証明書。
相互認証証明書	―	本認証局と他の認証局が互いに認証するときに発行される証明書。

2　公開とリポジトリの責任

2.1 リポジトリ

リポジトリは、24 時間 365 日利用可能とする。ただし、システムの保守などの理由により、利用者及び署名検証者に予め通知した上で、一時的にリポジトリを停止することができる。

2.2 証明書情報の公開

本認証局は、本サービスに係る情報をリポジトリにて公開する。公開される情報及び公開方法を、表 2-1 に示す。

本認証局は、CA 証明書のフィンガープリントなどを公開するサーバについては、通信路の暗号化、及び情報の改ざん検知・防止措置を施している。

表 2-1 リポジトリの内容

情報	対象	公開方法
本規程	関与する者全員	https://www.diacert.jp/plus/repository/repository01.html
利用者同意書	利用者	https://www.diacert.jp/plus/repository/repository01.html
署名検証者同意書	署名検証者	https://www.diacert.jp/plus/repository/repository01.html
CA 証明書（OldWithOld、NewWithNew）	関与する者全員	ldap://ldap.diacert.jp/OU=DIACERT-PLUS%20Service,O=DIACERT-PLUS%20CA,C=JP?caCertificate https://www.diacert.jp/plus/repository/
リンク証明書（OldWithNew、NewWithOld）	関与する者全員	ldap://ldap.japannet.jp/OU=DIACERT-PLUS%20Service,O=DIACERT-PLUS%20CA,C=JP?caCertificate https://www.diacert.jp/plus/repository/
相互認証証明書	関与する者全員	ldap://ldap.diacert.jp/OU=DIACERT-PLUS%20Service,O=DIACERT-PLUS%20CA,C=JP ?crossCertificatePair
CRL	利用者及び署名検証者	ldap://ldap.diacert.jp/OU=DIACERT-PLUS%20Service,O=DIACERT-PLUS%20CA,C=JP ?certificateRevocationList
ARL	利用者及び署名検証者	ldap://ldap.diacert.jp/OU=DIACERT-PLUS%20Service,O=DIACERT-PLUS%20CA,C=JP?authorityRevocationList
fullCRL	利用者及び署名検証者	ldap://ldap.diacert.jp/OU=DIACERT-PLUS%20Service,O=DIACERT-PLUS%20CA,C=JP? certificateRevocationList http://www.diacert.jp/plus/rlist/crl.crl http://www.diacert.jp/plus/rlist/arl.crl
CA 証明書及びリンク証明書のフィンガープリント	利用者及び署名検証者	https://www.diacert.jp/plus/repository/
本認証局からのお知らせ（料金、その他情報）	関与する者全員	http://www.diacert.jp/plus/

2.3 公開の頻度

本認証局が公開する情報の公開頻度は、下記のとおりとする。

(1) 本規程の公開については、本規程「9.11.2 通知方法と期間」に規定する。

(2) CRL/ARL/fullCRL については、発行した CRL/ARL/fullCRL の有効期間を 48 時間とし、24 時間ごとに更新する。

(3) 利用者同意書、署名検証者同意書は変更の都度、更新する。

(4) CA 証明書、及び CA 証明書のフィンガープリント、並びにリンク証明書、相互認証証明書は、発行及び更新の都度、リポジトリに登録し、公開する。

(5) 次に示す GPKI 接続要件に従う。

① リンク証明書、相互認証証明書及びその ARL/fullCRL は、発行及び更新の都度、公開する。

② 相互認証先認証局の名称及び相互認証を取消した認証局の名称は、電子認証局代表者による決定の都度、公開する。

2.4 リポジトリへのアクセス管理

本認証局は、リポジトリで公開する情報に関して、特定のアクセス制御は実施せず、すべての関与者に当該リポジトリの情報への読取り専用のアクセスを提供する。また、本認証局は、CA 証明書及び CA 証明書のフィンガープリントを公開するサーバについては、公開情報に対する不正アクセスや改ざん防止のために、通信路の暗号化及び情報の改ざん検知等の防止措置を施す。

3　本人の確認と認証

3.1 名前の決定

3.1.1　　名称のタイプ

本サービスで使用する名称は、ITU X.500 シリーズ定義の識別名（DN: DistinguishedName）の形式に従う。

3.1.2　　名称の意味に関する要件

本サービスにおいて発行する利用者証明書に記載される証明書所有者情報（subject）の識別名（DN）、並びに subjectAltName に記載する証明書所有者の所属する組織に関する情報の識別名（DN）は、利用申込み時に提出される「利用者証明書の DIACERT-PLUS 利用申込書（もしくは電子入札コアシステム用電子証明書利用申込書）（以下、「利用申込書」という。）」、並びに公的証明書の記載内容に基づき、本認証局側で設定する。詳細は、表 3-1、表 3-2 に示す。

利用申込書に記入されている内容を転記し設定値とする場合、利用者から提出された公的証明書を用いて、利用申込書の真正性を確認した上で、利用者氏名及び利用者住所については利用申込書に記入されている内容を、会社名については公的証明書に記載されている内容を転記する。

利用者証明書への氏名の記載に関して利用者が旧姓の記載を希望する場合は、利用者氏名については DIACERT-PLUS 旧姓利用申込書に記入されている利用者氏名（旧姓）の内容を転記する。

ただし DIACERT-PLUS 旧姓利用申込書は、DIACERT-PLUS 申込書と併せて申込まなければならない。DIACERT-PLUS 旧姓利用申込書だけでの申込みは受け付けない。

なお、本サービスで使用する文字は JIS 第 1 水準及び第 2 水準にて規定される文字で、これに規定されていない文字は、カナで入力する。また、公的証明書に記載されている文字が旧字体等の理由から本認証局において「誤字俗字・正字一覧表（平成 16 年 10 月 14 日付け法務省民一第 2842 号民事局長通達）」にしたがい置き換える場合は、この限りではない。

表 3-1 証明書所有者情報(subject)

属性	値	使用言語	利用申込書及び添付書類との対応	電子署名法の対応*1
c（国名） 「OID:2.5.4.6」 countryName	“c=JP”で固定（Printable）	日本を示す左記の国名を設定する。(英語)	なし	○
o（組織名） 「OID:2.5.4.10」 organizationalName	“o=DIACERT-PLUS CA”で固定（UTF-8）	本認証局を示す左記を設定する。(英語)	なし	×
ou（組織単位名） 「OID2.5.4.11」 organizationalUnitName	“ ou=DIACERT-PLUS Service” で固定（UTF-8）	本サービスを示す左記を設定する。(英語)	なし	×
st(s) （都道府県名）*2 「OID:2.5.4.8」 stateOrProvinceName	例 “st(s)＝Tokyo” （UTF-8）	ローマ字(英語)	利用者住所(都道府県)のローマ字（ヘボン式）を設定する。	○
l（市区町村名）*2 「OID:2.5.4.7」 localityName	例 “l=Minato-ku, Shibaura 4-16-36” （UTF-8）	ローマ字(英語)	利用者住所(市区町村以下)のローマ字（ヘボン式）を設定する。	○
ou（組織単位名） 「OID2.5.4.11」	例 “ou=D130921P000001”	14 桁の英数字(英語)	証明書番号を設定する。本認証局が割り当てる利用者証明書	×

organizationalUnitName	（UTF-8）		を識別する14桁の英数字を設定する。	
cn（一般名）*3*4 「OID：2.5.4.3」 commonName	例“cn=Ichiro Nippon” （UTF-8）	ローマ字(英語)	利用申込書に記入されている利用者氏名ローマ字*5*6 を転記する	○

*1 電子署名法の認定対象外×、対象○

*2 利用者が利用者住所の記載を希望する場合のみ、利用申込書に記入されている利用者住所をもとに本認証局がヘボン式ローマ字表記に変換し設定する。

*3 日本に居住する外国人の場合、住民票の写し、住民票記載事項証明書又は、広域交付住民票で証明されている氏名（以下、「本名」という。）又は、通称名のどちらか一方（利用申込書に記入された利用者氏名）を記載する。

*4 利用者が旧姓の記載を希望する場合、戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本又は、戸籍抄本で証明されている旧姓の氏名を記載する。

*5 利用者氏名のローマ字表記については、先頭を大文字、以下小文字とし、利用申込書に記入されている利用者氏名（ローマ字表記）が上記法則と異なる場合、本認証局にて先頭を大文字、以下小文字に変換し設定する。

*6 利用者氏名はヘボン式ローマ字で記載する。ただし、利用者がヘボン式以外のローマ字で利用者氏名の記載を求める場合、利用者本人のパスポートのコピーによりローマ字の表記が正しいことを確認する。（ただし、利用者氏名にヘボン式以外のローマ字を使用した電子証明書は、電子入札コアシステムの仕様とは異なるため、電子入札コアシステムでの署名に使用できない可能性がある。）

表 3-2 証明書所有者の所属する組織に関する情報（subjectAltName）

属性	値	使用言語	利用申込書及び添付書類との対応	電子署名法の対応*1
c（国名） 「OID：2.5.4.6」 countryName	“c=JP”で固定(Printable)	英語	なし	×
st(s)（都道府県名）*2 「OID：2.5.4.8」 stateOrProvinceName	例 “st(s)=東京”（UTF-8）	日本語	公的証明書に記入されている会社住所（本店（都道府県））を転記する。	×
l（市区町村名）*3 「OID：2.5.4.7」 localityName	例 “l=港区芝浦4丁目16番36号” (UTF-8)	日本語	公的証明書に記入されている会社住所（本店（市区町村以下））を転記する。	×
o（組織名） *4 「OID：2.5.4.10」 organizationalName	例 “o=ジャパンネット株式会社” (UTF-8)	日本語	公的証明書に記入されている会社名（商号・名称）を転記する。	×
OID.2.5.4.97（法人番号）*5*6 「OID: 2.5.4.97」 organizationIdentifier	例 “OID.2.5.4.97=JCN7010001003845” (UTF-8)	英語	国税庁の「法人番号公表サイト」において公開されている法人番号を転記する。	×
cn（一般名） 「OID：2.5.4.3」 commonName	例 “cn=日本 一郎” (UTF-8)	日本語	利用申込書に記入されている利用者氏名を転記する。	○

*1 電子署名法の認定対象外×、対象○

*2、3、4、5 利用者の所属する企業等が、商業登記されていない個人事業主の場合には記載しない。

*6 電子証明書への法人番号の記載は、2017 年 5 月 22 日以降に受領した利用申込みを対象とする。

電子証明書に記載する法人番号には、法人番号であることの識別のためプレフィックスとして「JCN」を先頭に付記する。

3.1.3 利用者の匿名性又は仮名性

利用者氏名は、本人確認において使用する公的証明書に記載されている氏名を記載し、これ以外は許可しない。ただし、利用者が旧姓の記載を希望する場合は、「DIACERT-PLUS 旧姓利用申込書」に記入されている利用者氏名（旧姓）を記載する。

3.1.4 名称形式を解釈するための規則

本認証局が発行する電子証明書に記載される名称は、ITU-T X.500 識別名（DN）の規定及び本規程「3.1.2 名称の意味に関する要件」の規程に従うものとする。

また、利用者証明書においては、利用者氏名及び利用者住所が電子署名法に規定する認定対象である。本認証局は、電子署名法に規定する基準を満たす利用者本人であることの真偽確認手続きを実施し、真正性が確認された利用者氏名及び利用者住所を利用者証明書に記載する。 なお、利用者住所は、利用者が利用申込書の「利用者住所の記載」に記入し、利用者住所の記載を希望する場合のみ利用者証明書に記載する。

利用者証明書に記載される利用者の属性情報（所属組織に関連する情報）は、電子署名法に規定する認定の対象外であり、登記事項証明書の内容に基づき情報の真正性を確認し、利用者証明書に記載する。

3.1.5 名称の一意性

利用者証明書に記載される利用者情報（subject）の識別名（DN）は、本認証局が発行した利用者証明書において一意である。

3.1.6 認識、認証及び商標の役割

商標使用の権利は、商標所持者が全ての権利を保有するものとする。本認証局は、商標について、確認及び認証を行わない。

3.2 利用者の本人性確認

3.2.1 秘密鍵の所有を証明するための方法

本認証局は、本認証局にて利用者鍵ペアを生成し、利用者証明書とともに IC カードに格納して利用者本人に送付するため、利用者秘密鍵の所有を証明する必要はない。

本認証局は、BCA との相互認証手続きにおいては、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 BCA 公開鍵に対する BCA 秘密鍵で署名されていることを確認する。

3.2.2 組織の確認

3.2.2.1 組織名称の確認

subjectAltName に含まれる利用者の所属する企業等が法人又は、商業登記されている個人事業

主の場合には、利用者が利用申込書に添付する登記事項証明書により組織の確認を行う。但し、subjectAltName に含まれる利用者の所属する企業等が商業登記されていない個人事業主の場合には、別紙 3 に示す事業を営んでいることを証明する書類のうちいずれか 1 つにより組織の確認を行う。

3.2.2.2 組織への所属確認

利用者が提出する利用申込書の中に記載の次の情報により、利用者の当該組織への所属を確認する。

(1) 利用者の所属する企業等が法人又は、商業登記されている個人事業主の場合

利用申込書に押印された利用者の所属する企業等代表者印を、当該組織の代表者の印鑑証明書で確認することにより、当該組織の代表者の意思確認を行なう。なお、所属する企業等によって商業登記を本部組織でのみ行ない、登記事項証明書が本部組織のみを証明している場合において、利用者の申し入れに従い、利用申込書に当該企業の地方組織の名称を追記し、利用者の所属する企業等代表者印が地方組織の名称を確認の上押印している場合は、審査登録局責任者の判断により、当該企業の地方組織の名称を企業等として証明書に記載することを可能とする。

(2) 利用者の所属する企業等が、商業登記されていない個人事業主の場合

利用申込書に押印された利用者の所属する企業等代表者個人の印を、当該組織の代表者個人の印鑑登録証明書で確認することにより、当該組織の代表者の意思確認を行なう。

上記の組織の確認と当該組織への所属確認を通して正しく検証できた場合、利用者が当該組織に所属していると判断する。

3.2.2.3 法人番号の確認

利用者が提出する利用申込書の中に記載の次の情報により、利用者が所属する組織の法人番号を確認する。利用者が所属する組織の法人番号が確認できない場合は、法人番号は証明書に記載しない。

(1) 利用者の所属する企業等が法人又は、商業登記されている個人事業主の場合

利用申込書に記載された会社名（商号・名称）及び会社住所（本店）から、国税庁の「法人番号公表サイト」を利用して確認を行なう。

(2) 利用者の所属する企業等が、商業登記されていない個人事業主の場合

法人番号の確認は行わない。また、電子証明書に法人番号の記載は行わない。

3.2.3 個人の確認

利用申込みを行う者が利用者本人であることの真偽の確認は、RA の受付審査担当者が、以下に定める方法によって行う。以下「3.2.3.1 利用者の真偽確認」事項の審査をもって、利用申込みを行う者が利用者本人であると判定する。なお、審査は複数人により行う。

3.2.3.1 利用者の真偽確認

利用者の真偽確認は、以下の方法により行なう。利用者が日本に居住する外国人である場合、住民票の写し、住民票記載事項証明書又は、広域交付住民票で証明されている本名又は、通称名を利用者証明書に記載することを求めることができる。このため、利用申込書の氏名欄に記入されている利用者氏名が通称名で記入されていれば利用者証明書に通称名での記載を求めたものとして扱う。利用申

込書の氏名欄に記入されている利用者氏名が本名で記入されていれば、利用者証明書に本名での記載を求めたものとして扱う。但し、利用申込書の氏名欄に住民票の写し、住民票記載事項証明書又は、広域交付住民票で証明されている本名と通称名が併記してある場合、本名、通称名のどちらを利用者証明書に記載すればよいかの判断が出来ないため、利用申込書の訂正あるいは再提出を求める。また、利用者が旧姓の記載を希望する場合、利用申込書の提出時に「DIACERT-PLUS 旧姓利用申込書」を添付することで、旧姓の氏名を利用者証明書に記載することができる。その場合、旧姓の確認のため、戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は戸籍抄本のいずれかの提出を利用者に求める。

(1) 記載内容、形式、有効期限等の確認

利用者の真偽確認のために使用する「表 3-3 利用申込みに必要な書類」の記載内容、形式等が真正なものであり、「表 3-4 利用申込みに必要な書類の有効期間」内であることを確認し、これらの書類と利用申込書の記入内容が一致することを確認する。利用者が利用者証明書にヘボン式以外のローマ字で利用者氏名の記載を求める場合は、利用者から参考資料として提出されたパスポートのコピーの記載内容、形式等が真正なものであり、有効なものであることを確認する。さらに、パスポートのコピーに記載されている「生年月日/Date of birth」が利用申込書に記入されている生年月日と一致することを確認する。また、利用者が日本に居住する外国人であり、住民票の写し等に本名の記載がなく、利用者証明書に本名の記載を求める場合は、利用者から参考資料として提出されたパスポートのコピー（顔写真が記載されているページ）、特別永住者証明書又は、在留カードのコピー（裏表両面）の記載内容、形式等が真正なものであり、有効なものであることを確認する。さらに、パスポート、特別永住者証明書又は、在留カードのコピーに記載されている「生年月日/Date of birth」が利用申込書に記入されている生年月日と一致することを確認する。また、利用者が旧姓の利用を希望する場合は、戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は戸籍抄本の記載内容、形式等が真正なものであり、有効なものであることを確認する。さらに、戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は戸籍抄本に記載されている利用者の現姓の氏名及び生年月日が住民票の写し、住民票記載事項証明書、又は広域交付住民票に記入されている氏名、及び生年月日と一致することを確認することにより、戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は、戸籍抄本が利用者のものであることを確認する。

(2) 住民票の写し、住民票記載事項証明書又は、広域交付住民票による確認

利用申込書に記入されている利用者の氏名、生年月日及び住所が、利用者の住民票の写し、住民票記載事項証明書又は、広域交付住民票に記載されている氏名、生年月日及び住所と一致することを確認する。利用者が日本に居住する外国人の場合は、利用申込書に記入されている利用者の氏名（本名又は、通称名）、生年月日、住所が利用者の住民票の写し、住民票記載事項証明書又は、広域交付住民票に記載されている氏名（本名又は、通称名）、生年月日、住所と一致することを確認する。（住民票の写し等に本名の記載がなく、利用者証明書に本名の記載を求める場合、本名の読み方が分からないため、利用者から提出されたパスポート、特別永住証明書又は、在留カードのコピーを参考に確認する。）利用者が旧姓の利用を希望する場合は、利用申込書に添付されるDIACERT-PLUS 旧姓利用申込書に記入されている利用者氏名（旧姓）が、戸籍全部事項証明書、

戸籍個人事項証明書、戸籍謄本、又は戸籍抄本に記載されている利用者の旧姓の氏名と一致することを確認する。

(3) 登記事項証明書等による確認

① 利用者の所属する企業等が法人又は、商業登記されている個人事業主の場合

利用申込書の会社名（商号・名称）、会社住所（本店）、代表者氏名が登記事項証明書に記載されている商号（会社名）、本店（会社住所）、代表者氏名と一致することを確認する。

② 利用者の所属する企業等が、商業登記されていない個人事業主の場合

利用申込書に記入されている利用者の氏名、屋号・雅号および会社住所が別紙３に示す事業を営んでいることを証明する書類のうちいずれか1つに記載されている氏名、屋号・雅号および会社住所と一致することを確認する。ただし、提出された別紙 3 に示す事業を営んでいることを証明する書類に屋号・雅号、会社住所が記載されていない場合は、一致しているものとみなす。

(4) 印鑑登録証明書による確認

利用申込書に利用者の氏名が記入されていること、及び利用者が市区町村に登録した印鑑（以下、「実印」という。）により押印されていることを確認し、利用申込書の実印の印影が、利用者本人の印鑑登録証明書に証明されている印影と一致することを確認する。利用者が旧姓の利用を希望する場合は、利用申込書に添付される DIACERT-PLUS 旧姓利用申込書に利用者の氏名が記入されていること、及び実印により押印されていることを確認し、DIACERT-PLUS 旧姓利用申込書の実印の印影が、利用者本人の印鑑登録証明書に証明されている印影と一致することを確認する。

(5) 印鑑証明書（代表者印）

（利用者の所属する企業等が商業登記されていない個人事業主の場合には、当該個人事業主の代表者個人の印鑑登録証明書をもって代替する）

利用申込書に利用者の所属する企業等代表者印又は、利用者の所属する企業等代表者個人の印が押印されていることを確認する。さらに、利用申込書に押印されている利用者の所属する企業等代表者印又は、利用者の所属する企業等代表者個人の印の印影が、添付されている印鑑証明書又は、印鑑登録証明書（利用者の所属する企業等が商業登記されていない個人事業主の場合）で証明されている印影と一致することを確認する。

3.2.3.2 利用者証明書の受取りを受取代理人に委任する場合

利用者が利用者証明書の受取を受取代理人に委任する場合、以下の(1)～(4)全ての項目が正しく検証できた場合、受取代理人が利用者に代わり利用者証明書を受取ることを承諾したことの意思確認とする。

(1) 利用申込書の受取代理人欄に受取代理人の氏名、住所が記入されていること。

(2) 利用申込書の受取代理人欄に受取代理人が登録した実印により押印されていること。

(3) 受取代理人欄に押印された実印の印影が、添付されている受取代理人の印鑑登録証明書に証明されている印影と一致すること。

(4) 受取代理人欄に記載の受取代理人の氏名、住所が受取代理人の印鑑登録証明書の氏名、住所と一

致すること。

3.2.3.3 利用申込みを行った者に対する疑義

本規程「3.2.3.1 3.2.3.1 利用者の真偽確認」及び「4.2.4(2) 利用者が利用者証明書の受取を受取代理人に委任する場合」の審査において、利用申込みに係る書類の不備や記載内容に疑義があった場合、本認証局は利用申込みを行った者に対し、定められた手順に従って利用申込書の訂正あるいは再提出を求める。20 日以内に再提出が確認できなかった場合は、本認証局は電話等による連絡および確認を行う。

3.2.3.4 必要書類一覧

利用申込みをする際に必要な書類について、表 3-3、表 3-4 に示す。

表 3-3 利用申込みに必要な書類

書類名	利用者の所属する企業等	
	法人	個人事業主
利用申込書	○	○
登記事項証明書	○	○*1
利用者本人の印鑑登録証明書	○	○
住民票の写し*8、住民票記載事項証明書又は、広域交付住民票	○*2*3	○*2*3
印鑑証明書(代表者印)	○	○*4
受取代理人の印鑑登録証明書	△*5	△*5
電子入札用電子証明書変更同意書	△*6	△*6
DIACERT-PLUS 旧姓利用申込書	△*7	△*7
戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は戸籍抄本	△*7	△*7

○:必須、△:省略可能

*1 利用者の所属する企業等が、商業登記されていない個人事業主の場合には、登記事項証明書の代替として別紙３に示す事業を営んでいることを証明する書類のうち、いずれか１つが必要となる。

*2 利用者が日本に居住する外国人であり、住民票の写し等に本名の記載がなく、利用者証明書に本名の記載を求める場合は、参考資料として利用者本人のパスポート、特別永住者証明書又は、在留カードのコピーが追加で必要となる。

*3 利用者がヘボン式以外のローマ字で利用者氏名の記載を求める場合は、参考資料として利用者本人のパスポートのコピーが追加で必要となる。

*4 利用者の所属する企業等が、商業登記されていない個人事業主の場合、当該個人事業主の代表者個人の印鑑登録証明書をもって代替する。但し、利用者が当該個人事業主の代表者である場合は、同一の印鑑登録証明書となるため、印鑑登録証明書の提出は 1 枚でよい。

*5 利用者が利用者証明書の受取を受取代理人に委任する場合のみ必要となる。本審査後に利用者

証明書の受取を受取代理人に委任する場合は、受取代理人申請書が追加で必要となる。

*6 利用申込書が「電子入札コアシステム電子証明書利用申込書」である場合のみ必要となる。

*7 利用者が旧姓の記載を希望する場合のみ必要となる。DIACERT-PLUS 旧姓利用申込書は DIACERT-PLUS サービスのホームページからダウンロード、もしくは郵送で利用者に送付する。

*8 住民票の写しは個人番号が省略されたものでなくてはならない。個人番号が記載されている住民票の写しが提出された場合は、認証局で当該箇所のみ墨塗りを実施する。

表 3-4 利用申込みに必要な書類の有効期間

	有効期間
登記事項証明書*1	本認証局が受領した日から遡って 3ヶ月以内
利用者本人の印鑑登録証明書	本認証局が受領した日から遡って 3ヶ月以内
住民票の写し、住民票記載事項証明書又は、広域交付住民票*2*3	本認証局が受領した日から遡って 3ヶ月以内
印鑑証明書(代表者印)*4	本認証局が受領した日から遡って 3ヶ月以内
受取代理人の印鑑登録証明書	本認証局が受領した日から遡って 3ヶ月以内
戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は、戸籍抄本	本認証局が受領した日から遡って 3ヶ月以内

*1 利用者の所属する企業等が、商業登記されていない個人事業主の場合に登記事項証明書の代替として必要となる事業を営んでいることを証明する書類の有効期間は別紙 3 に定めた通りとする。

*2 日本に居住する外国人で、住民票の写し等に本名の記載がなく、利用者証明書に本名の記載を求める場合に参考資料として必要となる利用者本人のパスポート、特別永住者証明書又は、在留カードのコピーが、有効なものであること。

*3 利用者がヘボン式以外のローマ字で利用者氏名の記載を求める場合は、参考資料として利用者本人のパスポートのコピーが、有効なものであること。

*4 利用者の所属する企業等が商業登記されていない個人事業主の場合に、印鑑証明書(代表者印)の代替として必要となる当該個人事業主の代表者個人の印鑑登録証明書の有効期間は、本認証局が受領した日から遡って 3ヶ月以内とする。

3.2.3.5 利用申込書の記載事項

日本に居住する外国人の場合、利用者氏名には住民票の写し、住民票記載事項証明書又は、広域交付住民票で証明されている本名又は、通称名のどちらか一方(利用者証明書に記載する利用者氏名)を記載する。本サービスで使用する文字は JIS 第 1 水準及び第 2 水準にて規定される文字で、これに規定されていない文字は、カナで入力する。さらに、住民票の写し、住民票記載事項証明書、又は、広域交付住民票(利用者が旧姓の利用を希望する場合は、戸籍全部事項証明書、戸籍個人事項

証明書、戸籍謄本、又は戸籍抄本）に記載されている文字が旧字体等の理由から、本認証局において電子証明書に記載される漢字を置き換える場合、「誤字俗字・正字一覧表（平成 16 年 10 月 14 日付け法務省民一第 2842 号民事局長通達）」にしたがって置き換えられる。

利用申込書には、利用者証明書の用途として「CPS 及び利用者同意書の内容に同意の上、電子入札コアシステム並びに CPS に記載されているサービスの用途にのみ利用する電子証明書の発行を下記の通り申し込む。」旨を明確に記載している。また利用申込書は受取代理人の委任状を兼ねており、利用申込書に受取代理人の委任範囲を明確に記載している。

利用申込書には次の記載が必要である。

（○：必須項目、△：基本的には必須項目であるが、利用者の所属する企業等が、商業登記されていない個人事業主の場合のみ省略可能）

(1) 利用者氏名（○）、利用者住所（○）、生年月日（○）
(2) 利用者氏名のフリガナ
(3) 利用者氏名のローマ字表記（○）
(4) 利用者本人の印鑑登録証明書で証明されている印鑑による押印（○）
(5) 利用者の所属する企業等の会社住所（本店住所）（○）、会社名、（△）
(6) 利用者の所属する企業等の代表者氏名（○）
(7) 利用者の所属する企業等代表者の印鑑証明書で証明されている印鑑による押印又は、利用者の所属する企業等代表者個人の印鑑登録証明書（利用者の所属する企業等が、商業登記されていない個人事業主の場合）で証明されている印鑑による押印（○）
(8) 連絡先会社名、連絡先会社住所、連絡先担当者名、連絡先部署名
(9) 連絡先電話番号、連絡先 FAX 番号、連絡先メールアドレス
(10) 利用を申し込む利用者証明書の有効期間（○）
(11) 受取代理人を指定する場合には、受取代理人の氏名、住所、受取代理人本人の印鑑登録証明書で証明されている印鑑による押印（受取代理人を指定する場合は必須）
(12) 請求先会社名、請求先会社住所、請求先部署名
(13) 利用者住所記載の確認

3.2.4 確認しない利用者の情報

規定しない。

3.2.5 機関の正当性確認

規定しない。

3.2.6 相互運用の基準

本認証局は、BCA との相互認証を行い、相互認証基準を満たすものとする。相互認証業務の実施及び終了については、相互認証先との調整のもとに、合意した手順に従い適切に判断し、処理を行う。

3.3 鍵更新申請時の本人性確認と認証

3.3.1 通常の鍵更新の本人性確認と認証

本認証局は、利用者証明書の有効期限切れが近づいた時期に、その旨を通知する。利用者は、その後、利用申込みを行うものとする。この場合、利用者証明書の利用申込みに関する本人性確認は、新規発行時と同様とし、本規程「3.2 利用者の本人性確認」の規定に従い行う。

3.3.2 証明書失効後の鍵更新の本人性確認と認証

一旦失効した利用者証明書については、使用できない。失効後に再度、利用者証明書を利用する場合は、新規に利用者証明書の利用申込みを行う。

3.4 失効申請時の本人確認と認証

3.4.1 失効申請者の真偽確認

利用者本人が失効申請を行う場合は、利用者本人であることの真偽確認を行なう。

利用者本人の所属している企業等からの失効依頼である場合には、失効対象となる利用者の所属する企業等であることの真偽確認を行なう。

(1) 利用者本人による失効申請の場合

DIACERT-PLUS 失効申請書（以下、「失効申請書」という）に利用者の氏名が記入されていること、及び利用申込書と同じ実印が押印されていることが必要である。但し、利用者の実印が変更されている場合には、利用者本人の印鑑登録証明書の添付が必要である。旧姓を記載した利用者証明書を失効する場合は、利用者証明書の発行時に提出された DIACERT-PLUS 旧姓利用申込書の利用者氏名（旧姓）と同じ氏名が失効申請書に記入されている必要がある。

(2) 利用者が属する企業等による失効依頼の場合

失効依頼書には、利用申込書と同じ利用者の所属する企業等代表者印又は、利用者の所属する企業等代表者個人の印（利用者の所属する企業等が商業登記されていない個人事業主の場合）が押印されていることが必要である。但し、利用者の所属する企業等代表者印が変更されている場合には、当該企業等代表者の印鑑証明書の添付が必要であり、利用者の所属する企業等代表者個人の印（利用者の所属する企業等が商業登記されていない個人事業主の場合）が変更されている場合には、利用者の所属する企業等代表者個人の印鑑登録証明書の添付が必要である。旧姓を記載した利用者証明書を失効する場合は、利用者証明書の発行時に提出された DIACERT-PLUS 旧姓利用申込書の利用者氏名（旧姓）と同じ氏名が失効依頼書に記入されている必要がある。

(3) 利用者の親族による失効依頼の場合

利用者が商業登記していな個人事業主で、利用者が死亡した場合、利用者の親族からの失効依頼を受け付ける。利用者の親族による失効依頼の場合、失効依頼書には利用者の親族の実印が押印されている必要がある。また、失効依頼書に押印された実印と同じ印影の印鑑登録証明書の添付が必要である。旧姓を記載した利用者証明書を失効する場合は、利用者証明書の発行時に提出された DIACERT-PLUS 旧姓利用申込書の利用者氏名（旧姓）と同じ氏名が失効依頼書に記入されている必要がある。

3.4.2 必要書類一覧

失効申請及び失効依頼をする際に必要な書類及び有効期間については、表 3-5 及び表 3-6 に示す

ものとする。

表 3-5 失効申請／失効依頼に必要な書類

書類名	失効申請		失効依頼	
	実印が変更されていない	実印が変更されている	実印が変更されていない	実印が変更されている
失効申請書	○	○	―	―
失効依頼書	―	―	○	○
印鑑登録証明書	―	○	○※	―
印鑑証明書	―	―	―	○

※利用者の親族による失効依頼の場合のみ親族の印鑑登録証明書が必要

表 3-6 失効申請／失効依頼に必要な書類の有効期間

書類名	有効期間
印鑑登録証明書	本認証局が受領した日から遡って 3ヶ月以内
印鑑証明書	本認証局が受領した日から遡って 3ヶ月以内

3.5 本審査後の受取代理人申請

3.5.1 本審査後の受取代理人を申請できる期間

本審査後に利用者本人が入院するなどして、証明書を受け取ることが困難になり、電子認証局責任者がそれを認める場合においてのみ、本審査後の受取代理人指定を認める。本審査後の受取代理人指定は、利用者証明書が発行されており、その受領書を受領していないもののみ申請を受け付ける。ただし、本審査後に受取代理人を指定した場合でも、4.4.1⑧で示す受領期限は変更されない。

3.5.2 利用者および受取代理人の真偽確認

以下の(1)～(7)の項目を検証し、利用者および利用者に委任された受取代理人であることの真偽確認を行う。

(1) 受取代理人申請書の利用者欄に利用者の氏名、住所、生年月日が記入されていること。
(2) 受取代理人申請書の利用者欄の氏名、住所、生年月日が、利用申込書に記入された利用者氏名、住所、生年月日と一致すること。
(3) 受取代理人申請書の利用者欄に利用者証明書の利用申込書に押印されたものと同じ印影の実印により押印されていること。
(4) 受取代理人申請書の受取代理人欄に受取代理人の氏名、住所が記入されていること。
(5) 受取代理人申請書の受取代理人欄に受取代理人が登録した実印により押印されていること。
(6) 受取代理人欄に押印された実印の印影が、添付されている受取代理人の印鑑登録証明書に証明されている印影と一致すること。
(7) 受取代理人欄に記載の受取代理人の氏名、住所が受取代理人の印鑑登録証明書の氏名、住所と一致すること。

3.5.3 本審査後の受取代理人指定の利用申込みを行った者に対する疑義

本審査後の受取代理人指定の審査において、申請に係る書類の不備や記載内容に疑義があった場合、本認証局は申請を行った者に対し、定められた手順に従って受取代理申請書の訂正あるいは再提出を求める。

3.5.4 必要書類一覧

申請を行なう際に必要な書類について、表 3-7 に示す。

表 3-7 本審査後の受取代理人申請に必要な書類の有効期間

	有効期間
受取代理人申請書	―
受取代理人の印鑑登録証明書	本認証局が受領した日から遡って 3ヶ月以内

4　証明書のライフサイクルに対する運用上の要件

4.1 証明書の利用申込み

利用者証明書の利用を希望する者は、本認証局の申込窓口に対して証明書の利用申込みを行う。利用者証明書の利用申込みの詳細については、以下の URL に掲載する。利用者証明書の利用を希望する者は、以下の URL に掲載されている本規程及び利用者同意書に、同意しなければならない。

http://www.diacert.jp/plus/

(1) 利用者は DIACERT-PLUS 利用申込書に記載されている、「本規程及び利用者同意書に同意の上申込む。」旨の記述（電子入札コアシステム用電子証明書利用申込書を使用して DIACERT-PLUS 電子証明書を発行する場合には、利用者は電子入札用電子証明書変更同意書に記載されている「本規程及び利用者同意書に同意の上申込む。」旨の記述）を確認の上、利用申込書に利用者の印鑑登録証明に係わる実印を押印する。この押印によって、本認証局は利用者が本規程、及び利用者同意書に記載された事項について承諾したものと判断する。同時に、本規程「3.1.2 名称の意味に関する要件」で規定されるように、利用者氏名（ローマ字表記を含む）が利用者証明書に記載されること及び本規程「9.4 個人情報の保護」で規定されるように個人情報が取扱われることについて同意されたものと判断する。また、利用者住所を利用者証明書に記載することを希望した場合は、利用者住所（ローマ字表記のみ）が利用者証明書に記載されること及び本規程「9.4 個人情報の保護」で規定されるように個人情報が取扱われることについて同意されたものと判断する。

なお本サービスで使用する文字は JIS 第 1 水準及び第 2 水準にて規定される文字で、これに規定されていない文字は、カナで入力することについて承諾するものとする。さらに、住民票の写し、住民票記載事項証明書又は、広域交付住民票（利用者が旧姓の記載を希望する場合は、戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は戸籍抄本）に記載されている文字が旧字体等の理由から、本認証局において電子証明書に記載される漢字を置き換える場合、「誤字俗字・正字一覧表（平成 16 年 10 月 14 日付け法務省民一第 2842 号民事局長通達）」にしたがって置き換えられることについて承諾するものとする。

(2) DIACERT-PLUS の利用者証明書の利用申込みを希望する場合は、企業等は利用申込書に記載されている、「1.当企業は本件申込について同意します。」「2.当企業は上記利用者が当企業に所属する者であることを認めます。」旨の記述を確認の上、利用申込書に利用者の所属する企業等代表者印又は、利用者の所属する企業等代表者個人の印（利用者の所属する企業等が商業登記されていない個人事業主の場合）を押印することにより、本認証局は、企業等が本規程、及び利用者同意書に記載された事項について承諾の上、当該利用者が利用者証明書を申込むことに同意したものと判断する。同時に、本規程「3.1.2 名称の意味に関する要件」で規定されるように、会社名（商号・名称）、会社住所（本店）が利用者証明書に記載されることについて同意されたものと判断する。但し、利用者の所属する企業等が、商業登記されていない個人事業主の場合には会社名（商号・名称）、会社住所（本店）を利用者証明書に記載しないこととする。

(3) 利用者は、過去に本サービスへの利用申込があり、住民票の写し、住民票記載事項証明書又は、広域交付住民票（利用者が旧姓の記載を希望する場合は、戸籍全部事項証明書、戸籍個人事項証明

書、戸籍謄本、又は戸籍抄本）に記載されている文字が旧字体等の理由から、電子証明書に記載される漢字を本認証局にて置き換えている場合、利用申込書に置き換えられた漢字が印字されることを承諾するものとする。さらに、置き換えられた漢字により住民票の写し、住民票記載事項証明書又は、広域交付住民票（利用者が旧姓の記載を希望する場合は、戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は戸籍抄本）との真偽確認が実施されることを承諾するものとする。また真偽確認の際には、置き換えられた漢字が「誤字俗字・正字一覧表（平成 16 年 10 月 14 日付け法務省民一第 2842 号民事局長通達）」等にしたがって住民票の写し、住民票記載事項証明書又は、広域交付住民票に記載されている漢字の正字であることを確認されることを承諾するものとする。

(4) 利用者は、利用申込書作成支援システム(https://wizard.diacert.jp/default.aspx?type=ebid)により利用申込書を作成した場合、旧字体等のシステムが出力することのできない漢字はすべて正字に置き換えられることを承諾するものとする。さらに、置き換えられた漢字により、住民票の写し、住民票記載事項証明書又は、広域交付住民票（利用者が旧姓の記載を希望する場合は、戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は戸籍抄本）との真偽確認が実施されることを承諾するものとする。また、真偽確認の際には、置き換えた漢字が「誤字俗字・正字一覧表（平成 16 年 10 月 14 日付け法務省民一第 2842 号民事局長通達）」等にしたがって住民票の写し、住民票記載事項証明書又は、広域交付住民票（利用者が旧姓の記載を希望する場合は、戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は戸籍抄本）に記載されている漢字が正字であることを確認することを承諾するものとする。

4.1.1 利用申込みの申請者

利用者証明書の利用申込みは、利用者本人が行わなければならない。本認証局は、代理人による利用申込みは受付けない。

4.1.2 利用申込みの方法

利用者証明書の利用申込みについては、以下の 2 つの方法によるものとする。

① 本認証局の申込窓口への直接申込み

② 本認証局の申込窓口への郵送申込み

上記以外の方法による申込みは、受付けない。

4.2 利用者証明書の利用申込み手続き

4.2.1 本人性確認と資格確認

本認証局では、利用申込書、住民票の写し等の利用申込みに必要な書類一式が揃っていることの確認及び本規程「3.2 利用者の本人性確認」で規定する審査及び利用申込みの意思確認を行う。

4.2.2 証明書利用申込みの承認又は却下

RA は、利用申込みに対する審査において疑義がないことを確認できた場合は、利用申込みを承認し、IA に対し利用者情報の登録及び利用者証明書の発行を要求する。

RA は、利用申込みに対する審査において疑義が認められた場合は、記載されている内容に不備が発見された書類の訂正又は再提出を求める。訂正又は再提出の通知手段は郵便、電話、電子メール等

により利用申込者に対して通知する。

通知を受けた利用者は、通知後 20 日以内に不備のあった書類の訂正又は再度用意の上、本認証局に再提出しなければならない。

本認証局は、利用申込みに対する審査の結果、利用者証明書の発行ができないと判断したときは、不受理の理由及びその旨を郵便、電話、電子メール等の手段により利用者に通知する。

4.2.3 証明書利用申込みの処理時間

本認証局は、利用申込書類の受付け後、真偽確認及び本人の実在性確認を行い、発行の可否判断を30 日以内に行う。

4.2.4 証明書利用申込みの手続きの詳細

(1) 利用者が利用者証明書を自分自身で受け取る場合

利用申込書に必要事項を記入し、利用者本人の実印を押印し、かつ利用者の所属する企業等代表者印又は、利用者の所属する企業等代表者個人の印を押印する。

利用申込書に加え、以下の書類を添付する。但し①、③、④、⑤、⑥、⑦、⑧の添付書類は、本認証局がそれらを受領した日から遡って 3 ヶ月以内のものとする。

① 登記事項証明書(履歴事項全部証明書、あるいは現在事項全部証明書)(利用者の所属する企業等が法人又は、商業登記されている個人事業主の場合)
② 別紙 3 に示す事業を営んでいることを証明する書類のうち、いずれか 1 つ。(利用者の所属する企業等が、商業登記されていない個人事業主の場合)
③ 利用者本人の印鑑登録証明書
④ 利用者本人の住民票の写し、住民票記載事項証明書又は、広域交付住民票
⑤ 利用者の所属する企業等代表者の印鑑証明書(利用者の所属する企業等が、商業登記されていない個人事業主の場合を除く)又は、利用者の所属する企業等代表者個人の印鑑登録証明書(利用者の所属する企業等が、商業登記されていない個人事業主の場合)
⑥ 利用者本人のパスポート、特別永住者証明書又は、在留カードのコピー(日本に居住する外国人で、住民票の写し等に本名の記載がなく、利用者証明書に本名の記載を求める場合)
⑦ 利用者本人のパスポートのコピー(利用者がヘボン式以外のローマ字で利用者氏名の記載を求める場合)
⑧ 利用者の戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は、戸籍抄本(利用者証明書に旧姓の氏名の記載を求める場合)
⑨ 電子入札用電子証明書変更同意書(利用申込書が「電子入札コアシステム電子証明書利用申込書」である場合)
⑩ DIACERT-PLUS 旧姓利用申込書(利用者証明書に旧姓の氏名の記載を求める場合)

(2) 利用者が利用者証明書の受取を受取代理人に委任する場合

利用者が利用者証明書の受取を受取代理人に委任する場合は、上記の本規程4.2.4(1)に加えて、以下が必要である。

① 受取代理人の実印の印鑑登録証明書（但し、本認証局がそれらを受領した日から遡って 3 ヶ月以内のもの）

② 受取代理人申請書（本審査後に受取代理人を指定する場合）

(3) 一人の利用者が複数の利用者証明書を申込む場合

一人の利用者が複数の利用者証明書を申込む場合、利用申込書は利用者証明書1件につき 1 枚ずつ必要である。それぞれの利用申込書の添付書類が同一である場合には、各利用申込書に対して、添付書類は1式で可とする。但し、各利用申込書と添付書類 1 式は同封されて、申込む必要がある。

4.2.5 利用申込みの受付けと審査

4.2.5.1 利用申込みの受付け

利用者証明書の利用申込みは、「1.5.2 問い合わせ先」に示す[問合せ先]への郵送、あるいは[問い合わせ先]の窓口への直接持参でのみ受付ける。利用者証明書の利用申込みは、利用者本人が行なわなければならない。代理人による利用申込みは受付けない。

4.2.5.2 利用申込みに対する審査

(1) 本認証局では、利用申込書、住民票の写し、住民票記載事項証明書又は、広域交付住民票など利用申込みに必要な書類一式が揃っていること、並びに「3.2.3 個人の確認」で規定する審査及び利用申込みの意思確認を行う。

(2) 利用申込みに対する審査において問題が無いことを確認できた場合は、RA が利用申込みを承認し、IA に利用者証明書の発行を要求する。RA は、IA に利用者証明書の発行を要求することと併せて、利用者情報を本認証局に登録する。

(3) 利用申込みに対する審査において疑義が認められた場合は、本認証局は記載されている内容に不備が発見された書類の訂正あるいは再提出を依頼する。訂正あるいは再提出の通知手段は郵便等により利用申込者に対して通知する。

4.3 証明書の発行

4.3.1 利用者証明書の発行時の認証局の機能

(1) IA は、真正な利用者情報が登録された利用者について、RA から利用者証明書の発行を要求されると、認証設備室で複数操作員による相互牽制の下、利用者鍵ペア、利用者証明書及び PIN コードを生成し、生成した利用者秘密鍵と利用者証明書を IC カードに格納する。このとき生成された利用者秘密鍵及び PIN コードは、IC カードに格納後、認証業務用設備から完全に削除される。

(2) IA は IC カード及び PIN コードを安全に利用者へ配送するため、電子署名及び認証業務に関する法律施行規則（平成 13 年総務省、法務省、経済産業省令第 2 号）第 5 条第 1 項第1号ハで定める「その取扱いにおいて 名宛人本人若しくは差出人の指定した名宛人に代わって受け取ることができる者に限り交付する郵便」に相当する郵便事業株式会社が提供する「本人限定受取郵便（基本型）」（以下、「本人限定受取郵便（基本型）」という。）にて、住民票の写し、住民票記載事項証明書又は、広域交付住民票に記載された利用者の住所に郵送する。

(3) 利用者が本審査前に利用申込書への受取代理人欄への記載をもって、利用者証明書の受領を受取代理人に委任している場合、もしくは利用者が本審査後に受取代理人申請書をもって、利用者証明

書の受領を受取代理人に委任している場合は、IC カードを受取代理人宛に「本人限定受取郵便（基本型）」で送付する。受取代理人は当該郵送物を開封することなく直ちに利用者に引き渡す。PIN コードは、利用者の住民票の写し、住民票記載事項証明書又は、広域交付住民票に記載された利用者本人の住所宛に簡易書留にて郵送する。

(4) 本認証局は、利用者からの実印を押印した「DIACERT-PLUS 受領書」（以下、「受領書」という。）をRAが受領することをもって、利用者本人に確実に IC カードと PIN コードが渡ったことを確認する。

4.3.2 BCA に対する相互認証証明書の発行

(1) BCA に対する相互認証証明書の発行については、BCA の定める相互認証に関する手続きが終わった後、BCA よりオフラインで提示される証明書発行要求に対して、本認証局にて署名検証を行なった後、相互認証証明書を発行し、オフラインにて BCA へ提出する。

(2) 本認証局は、相互認証証明書をリポジトリに公開する。

4.3.3 証明書の利用者に対する証明書発行通知

証明書の利用者に対する証明書発行通知は、下記のとおりとする。

(1) 利用者証明書の発行通知

利用者への利用者証明書の発行通知は、IC カード及び PIN コードを発送することにより行う。

(2) BCA に対する相互認証証明書の発行通知

BCA への相互認証証明書の発行通知は、相互認証証明書をオフラインで提出することにより行う。

4.4 証明書の受領

4.4.1 証明書の受領

(1) 利用者証明書の受領

① 利用者は、IA から発送された IC カードを、本人のみが受取ることのできる「本人限定受取郵便（基本型）」で受領する。

② 「本人限定受取郵便（基本型）」が到着した旨の連絡を郵便局から受けた利用者又は、受取代理人は、郵便局に出向き、自身を証明する証明書を提示して「本人限定受取郵便（基本型）」（IC カード、PIN コード及び受領書が同封されたもの）を受領する。但し受取代理人が受領する場合は「本人限定受取郵便（基本型）」には PIN コードは同封されず、本認証局より利用者本人宛に、別途、PIN コードを簡易書留にて送付する。

③ 受取代理人が受け取った場合には、受領した「本人限定受取郵便（基本型）」（IC カード及び受領書が同封されたもの）を開封せず、そのまま利用者本人に手渡されなければならない。

④ 利用者は利用者証明書が格納された IC カードと PIN コードを受領した場合には、直ちに利用者証明書の内容を確認し、その後、速やかに自身の氏名を記入し、利用申込書に押印された実印で押印した受領書を本認証局の申込窓口へ返送しなければならない。

⑤ 利用者が複数枚の利用者証明書を申込んだ場合には、本認証局は、申込まれた各利用申込書単位に IC カードと PIN コードを利用者宛に送付する。このため利用者は個々の利用者証明書に対応する受領書に、自身の氏名を記入し、利用申込書に押印された実印で押印の上、本認証局宛に返送しなければならない。

⑥ 本認証局は、受領書を受取ることにより、利用者本人に利用者証明書が渡ったことを確認する。

⑦ 本認証局は、受領書を受取ることにより、利用者本人に利用者証明書が渡ったことを確認する。利用者は交付された利用者証明書の内容に疑義がある場合は、本認証局から発送後 20 日以内に「1.5.2 問い合わせ先」に示す[問合せ先]に対して連絡しなければならない。この場合、受領書を本認証局に返送してはならない。

⑧ 利用者は、本認証局が「本人限定受取郵便(基本型)」で発送後、20 日以内に受領書を本認証局宛てに返送する必要がある。本認証局はこの期間内に受領書の返送がない場合は、利用者に対し受領書を本認証局宛に返送するように督促する。督促後、10 日を経過しても受領書の返送がない場合は、利用者証明書の受領が行われなかったものとみなし、当該利用者証明書を失効させる。

⑨ 受領書の返送が郵送の都合等により遅延することを考慮し、失効処理期限前に本認証局より、電話、電子メール等の手段で、利用者に対して受領書の返送に関する状況を確認する。受領書を郵送済、もしくは、受領書は未返送ながら受領書を返送する明確な利用者の意思を確認した場合には、本認証局は利用者証明書の失効処理期限を延長することがある。

(2) BCA からの相互認証証明書の受領

本認証局は、BCA の定める手続きに基づき、発行した相互認証証明書の受領書による受領確認をもって、相互認証証明書の受領完了とする。

4.4.2 認証局による証明書の公開

本認証局は、利用者証明書の公開は行わない。ただし、自己署名証明書、リンク証明書及び相互認証証明書についてはリポジトリ上で公開する。

4.5 鍵ペアと証明書の用途

4.5.1 利用者秘密鍵及び証明書の利用目的

本サービスにより発行される利用者証明書は、本規程「1.4 証明書の用途」に規定する用途のみに使用できる。また、本認証局は、利用者証明書が用途以外の目的で使用された場合には、一切の責任を負わない。

4.5.2 署名検証者の公開鍵及び証明書の利用目的

署名検証者は、電子署名の検証用に利用者の公開鍵及び利用者証明書を利用する。利用に際しては、本規程「9.6.5 署名検証者の責任及び義務」に規定する内容を承諾しなければならない。

4.6 証明書の更新

(1) 利用者証明書の更新

本認証局が発行する利用者証明書は、自動的に更新されない。利用者証明書の有効期間が切れると同時に、鍵も無効となる。利用者は、利用者証明書及び鍵の更新が必要な場合は、再度、利用申込みを行わなければならない。

(2) CA 証明書の更新

本認証局の CA 証明書の更新は、必ず証明書の鍵更新を伴うものとし、本規程「4.7.1(2) CA 証明書

の鍵の更新」に規定する。

4.7 証明書の鍵更新

証明書の鍵更新に関する要件は、下記のとおりとする。

(1) 利用者証明書の鍵の更新

本認証局が発行する利用者秘密鍵は、自動的に更新されない。利用者証明書の有効期間が切れると同時に、鍵も無効となる。利用者は、利用者証明書及び鍵の更新が必要な場合は、再度、利用申込みを行わなければならない。

(2) CA 証明書の鍵の更新

本認証局の CA 秘密鍵更新は、5 年に一度行われ、その際本認証局は、新しい CA 証明書及びリンク証明書を発行し、リポジトリに公開する。旧 CA 証明書については、有効期限までリポジトリへ公開する。旧 CA 秘密鍵については完全に廃棄する。

4.8 証明書の変更

本認証局は、発行した証明書の変更は行わない。利用者は、利用者証明書の変更が必要な場合は、失効申請後、再度、利用申込みを行わなければならない。

4.9 証明書の失効

4.9.1 証明書の失効事由

利用者は、以下の事項に該当する事由が生じた場合は、直ちに本認証局に対し利用者証明書の失効を申請しなければならない。

(1) 利用者証明書の記載事項が事実と異なる場合
(2) 利用者証明書の記載事項に変更が生じた場合
(3) 電子証明書を紛失あるいは破損した場合
(4) 電子証明書の盗難あるいは不正使用などを知った場合
(5) PIN の紛失の場合
(6) PIN の漏洩による電子証明書の不正使用などを知った場合
(7) PIN の入力ミスで電子証明書が利用できなくなった場合
(8) 利用者秘密鍵が危殆化又は、危殆化の恐れがある場合
(9) 利用者証明書の利用を中止する場合
(10) 利用者が当該企業等に属さないこととなった場合
(11) 利用者が利用者証明書を利用して権限を行使することができなくなった場合
(12) その他、利用者が利用者証明書を失効させる必要があると判断した場合

4.9.2 失効申請者

本認証局は、利用者本人が申請する場合に限り、利用者証明書の失効申請を受付けるものとする。但し、利用者の所属する企業等の組織が利用者に変わって、失効依頼書を提出することにより、認証局事由に拠る失効を行うことが出来る。

4.9.3　　失効申請手続

利用者証明書の失効申請については、本認証局の申込窓口への郵送申込みまたは持込み以外の方法による場合は、受付けない。ただし、緊急かつやむを得ない事情がある場合には、FAX でも受付ける。この場合、事後であっても失効申請書の提出は必ず必要となる。

4.9.3.1 失効申請に必要な書類

利用者証明書の失効申請に際しては、失効申請書を提出する。但し、利用者の実印が変更されている場合には失効申請書と利用者本人の印鑑登録証明書を提出する。

また、企業等からの失効依頼に際しては、失効依頼書を提出する。但し、利用者の所属する企業等代表者が変更されている場合は失効依頼書と当該企業等代表者の印鑑証明書を提出する。また、利用者の所属する企業等代表者個人の印（利用者の所属する企業等が商業登記されていない場合）が変更されている場合には、失効依頼書と利用者の所属する企業等代表者個人の印鑑登録証明書を提出する。

利用者が商業登記していない個人事業主で、利用者が死亡した場合、利用者の親族からの失効依頼を受け付ける。親族からの失効依頼の場合、失効依頼書と親族の印鑑登録証明書の提出と、失効依頼書に親族の実印による押印を求める。

4.9.3.2 失効申請書

失効申請書に必要事項を記入し、利用申込書に押印した印と同じ実印で押印する。また、利用者の属する企業等による失効依頼においては、利用申込書と同じ利用者が属する企業等代表者印又は、利用者の所属する企業等代表者個人の印で押印する。利用者の死亡等による利用者の親族の失効依頼においては、依頼を行なう親族個人の実印で押印する。

但し、実印が変更されている場合又は、親族からの失効依頼の場合には、印鑑登録証明書の添付が必要である。

4.9.3.3 失効申請書/失効依頼書の記載事項

失効申請書には次の記載が必要である。（○は必須項目、△：基本的には必須項目であるが、利用者の所属する企業等が、商業登記されていない個人事業主の場合のみ省略可能）

利用者が旧姓を記載した利用者証明書を発行していた場合は、失効申請書、又は失効依頼書の利用者氏名には旧姓を記載する。

(1) 利用者の所属する企業等が利用者本人に代わって失効依頼する場合

① 会社名（商号・名称）（△）
② 代表者氏名（○）
③ 会社住所（本店）（○）
④ 利用者の所属する企業等代表者印、利用者の所属する企業等代表者個人の印又は、利用者の親族の個人の印による押印（○）、
⑤ 連絡先担当者名（○）、連絡先会社住所（○）

⑥ 担当者所属部署名
⑦ 連絡先 e-mail アドレス、FAX 番号
⑧ 連絡先電話番号
⑨ 利用者氏名（○）、住所（○）、生年月日（○）
⑩ 証明書番号（○）
⑪ 失効事由（○）

(2) 利用者本人が失効申請する場合

① 利用者氏名（○）、住所（○）、生年月日（○）
② 利用者本人の印鑑登録証明書で証明される印鑑による押印（○）
③ 会社名（△）
④ 部署名
⑤ 連絡先 e-mail アドレス、FAX 番号
⑥ 連絡先電話番号
⑦ 証明書番号（○）
⑧ 失効事由（○）

4.9.3.4 失効申請の受付けと審査

(1) 失効申請の受付け

利用者証明書の失効申請は、本認証局の申込窓口への郵送または申込窓口への持込みにて受付ける。

(2) 失効申請に対する審査

① 本認証局では、失効申請書など失効申請に必要な書類一式が揃っていることならびに「3.4.1 失効申請者の真偽確認」で規定する審査及び失効申請の意思確認を行う。
② 失効申請に対する審査において問題が無いことを確認できた場合は、RA は利用者証明書を失効する。

4.9.3.5 緊急的な失効申請への対応

本認証局では、利用者証明書の緊急的な失効申請においては、郵送での受付け及び審査に先立ち、FAX による失効申請の受付けを可能とする。ただし、その場合において、本認証局はコールバックにより、本人確認と意思確認を行う。

失効申請を行った者は、失効申請に必要な書類（前項に記載の失効申請書）一式を後日、本認証局に提出する。

4.9.3.6 証明書の失効

(1) 利用者証明書の失効

① RA は利用者証明書を失効させる。
② RA は失効申請を行った者ならびに利用者本人へ失効手続きの完了を知らせる通知書（以下、「失効

完了通知書」という。）を発送する。失効申請を行った者ならびに利用者本人への失効完了通知書は、郵送によって行なう。

(2) BCA に対する相互認証証明書の失効

本認証局は、本認証局もしくは BCA に、次の相互認証証明書失効事由が発生した場合、相互に相互認証証明書を失効させる。

① CA 秘密鍵の危殆化又は、危殆化の恐れがある場合
② 相互認証基準違反
③ 相互認証業務の終了
④ 相互認証証明書の更新

本認証局からの BCA に対する失効申請は、電子認証局代表者が行なう。

BCA からの失効申請は、BCA の責任者から行われたものに対し、組織の認証において定める手続きを行った上で、直ちに相互認証証明書の失効処理を行う。相互認証証明書の失効については、本規程「4.9.7 CRL/ARL/fullCRL の発行頻度」に従い ARL/fullCRL を更新し、リポジトリに公開する。

4.9.3.7 本認証局による失効要求

本認証局は、以下の事項に該当する事由が生じた場合は、利用者からの失効申請によらず、その利用者証明書の失効を行う。

(1) 電子証明書を発送後、30 日を過ぎても受領書が返送されなかった場合
(2) 利用者の秘密鍵が危殆化した又は、危殆化の恐れがある場合
(3) 利用者証明書が不正使用された、もしくはその恐れがある場合
(4) 利用者証明書の記載事項が事実と異なる場合
(5) 本認証局の CA 秘密鍵が危殆化又は、危殆化の恐れがある場合
(6) 利用者が CPS 及び利用者同意書に違反した場合
(7) 本認証局の責めに帰すべき事由により利用者証明書の誤発行等を行なった場合
(8) 本認証局業務を終了する場合
(9) その他、本認証局が必要と判断した場合
(10) 企業等から依頼を受けた場合（利用者が当該企業等に属さないこととなった）
(11) 企業等から依頼を受けた場合
（利用者が利用者証明書を利用して権限を行使することができなくなった）
(12) 企業等から依頼を受けた場合（企業名又は、企業住所（本店）に変更が生じた）
(13) 企業等から依頼を受けた場合（利用者が死亡した）
(14) 企業等から依頼を受けた場合（その他、利用者証明書を失効させる必要があると判断した場合）

本認証局は、利用者証明書を失効させた時には速やかに利用者に失効通知を郵送により通知する。ただし、利用者に通知することが不可能な場合にはこの限りではない。

4.9.4 失効申請の猶予期間

利用者は、本規程「4.9.1 証明書の失効事由」に規定する事由が発生した場合は、直ちに、本規程「4.9.3 失効申請手続」に規定する手続きにより、当該証明書の失効申請をしなければならない。

4.9.5 認証局が失効申請を処理しなければならない期間

本認証局は失効申請書を受付けた場合は本規程「4.9.3 失効申請手続」に規定する手続きを行い利用者証明書の失効を行う。さらに失効後、24 時間以内に CRL/fullCRL にその情報を格納し、公開する。

4.9.6 失効情報及び有効性確認情報に関する要件

本認証局は、利用者証明書、リンク証明書及び相互認証証明書の失効情報、CA 証明書及び有効性確認情報を、リポジトリで公開する。

署名検証者は、本認証局のリポジトリに格納された CRL/ARL/fullCRL によって、検証しようとする証明書の有効性を確認しなければならない。

4.9.7 CRL/ARL/fullCRL の発行頻度

本認証局は CRL/ARL/fullCRL の発行頻度を決定し、その頻度に従い、下記により CRL/ARL/fullCRL の更新を行う。

(1) CRL/ARL/fullCRL の有効期間を 48 時間とし、24 時間ごとに更新する。
(2) 利用者証明書の失効を行った場合には、24 時間以内に CRL/fullCRL を更新する。
(3) CA 秘密鍵が危殆化し、又は危殆化の恐れがある場合は、直ちに、発行した全ての利用者証明書、相互認証証明書及びリンク証明書を失効させ、CRL/ARL/fullCRL を発行する。
(4) CA 証明書の更新、相互認証証明書の更新等を行なった場合は、直ちに ARL/fullCRL を更新する。

4.9.8 証明書失効リストの発行最大遅延時間

本認証局は、発行した CRL/ARL/fullCRL を 24 時間以内にリポジトリに格納する。ただし、CRL/ARL/fullCRL の更新が 24 時間を越えて停止した場合、これを CRL/ARL/fullCRL 有効期限内に BCA 及び署名検証者に対し、リポジトリ（Web ページ）又は電子メール等で通知する。また、CRL/ARL/fullCRL 有効期限内に BCA 及び署名検証者に通知することができず、7 日以上 CRL/ARL/fullCRL の更新を行えなかった場合には、重大障害として、主務大臣へ報告する。

4.9.9 利用可能な失効通知の他の形式

本認証局は、リポジトリに掲載した CRL/ARL/fullCRL 以外の失効リスト検査手段を提供しない。また、本認証局は、有効期間の満了した利用者証明書、リンク証明書及び相互認証証明書の失効情報については提供しない。

4.9.10 証明書の一時停止

本認証局は、利用者証明書の一時停止を行わない。

4.10 認証局へのサービス加入の終了

本認証局は、特定認証業務の認定の更新を受けない場合を含めて、本サービスを廃止することができるものとし、廃止する場合には、下記の方法にて行う。

(1) 本認証業務の廃止日までに有効期間の残っている全ての利用者証明書及び相互認証証明書を失効し、その全証明書の有効期間が満了するまでの間、CRL/ARL/fullCRL をリポジトリに公開する。

(2) 本サービスを廃止する場合には、廃止日の 60 日前までに、利用者及び BCA に書面で通知するとともに、リポジトリにその旨を公開する。

(3) 廃止時には、CA 秘密鍵を完全に初期化し、そのバックアップ媒体を物理的に完全に破壊する。

4.11 キーエスクローと鍵回復

本認証局は、CA 秘密鍵及び利用者秘密鍵のエスクロー(第三者寄託)を行わない。

4.12 本審査後の受取代理人申請

本審査後の受取代理人申請を希望する者は、本認証局の申込窓口に対して申請を行う。

4.12.1 申請に必要な書類

本審査後の受取代理人の申請に際しては、「受取代理人申請書」と「受取代理人の印鑑登録証明書」を提出する。

4.12.2 受取代理人申請書の記載事項

受取代理人申請書には次の記載が必要である。

(○:必須項目、△:基本的には必須項目であるが、利用者の所属する企業等が、商業登記されていない個人事業主の場合のみ省略可能)

(1) 利用者氏名(○)、利用者住所(○)、生年月日(○)

(2) 利用者本人の印鑑登録証明書で証明されている印鑑による押印(○)

(3) 利用者の所属する企業等の会社名(△)

(4) 利用者証明書の証明書番号

(5) 受取代理人氏名(○)、受取代理人住所(○)

(6) 受取代理人本人の印鑑登録証明書で証明されている印鑑による押印(○)

(7) 連絡先担当者名、連絡先会社住所(○)

(8) 連絡先電話番号

(9) 連絡先 FAX 番号、連絡先メールアドレス、連絡先部署名

4.12.3 本審査後の受取代理人申請の受付け

本審査後の受取代理人の申請は、「1.5.2 問い合わせ先」に示す[問合せ先]への郵送、あるいは直接申込にて受付ける。

4.12.4　本審査後の受取代理人申請の審査

(1) 本認証局では、受取代理人申請書および受取代理人の印鑑登録証明書が揃っていること、並びに「3.5.2 利用者および受取代理人の真偽確認」で規定する審査及び本審査後の受取代理人申請の意思確認を行う。

(2) 利用申込みに対する審査において問題が無いことを確認できた場合は、RA は当該利用者証明書の本人限定受取郵便を開封し、受取代理人を指定して出しなおす。その際、本人限定受取郵便に PIN コードが同封されていた場合は、利用者本人の住所宛に簡易書留にて郵送する。

(3) 申請に対する審査において疑義が認められた場合、本認証局は記載されている内容に不備が発見された書類の訂正あるいは再提出を依頼する。訂正あるいは再提出の通知手段は、郵送により利用申込者に対して通知する。

5　物理的、手続き的、人的セキュリティ管理

5.1 物理的セキュリティ管理

5.1.1　　認証設備室及び建物

本サービスのための設備を維持・運用するための場所である認証設備室については、次のセキュリティを確保する。

(1) 認証設備室は、外部からの侵入が容易にできないようセキュリティが確保された建物の内部に、物理的な仕切りに囲まれた区画(「サイト」ともいう。)の施設とし、物理的な階層構造の中に設置される。

(2) 認証設備室については独自のセキュリティ基準を設けることにより、認証業務用設備が物理的に安全な環境において運用する。

(3) 認証設備室及び認証設備室が設置された建物などには、その施設に認証業務用設備があることを示す掲示を一切行わない。

5.1.2　　物理的アクセス

認証業務用設備が設置されている室への入退室においては、次のセキュリティを確保する。

(1) 認証設備室への入室においては、あらかじめ許可された要員の生体と入室しようとする要員の生体を認証することにより、許可されない者が室内に不正侵入できないようにする。さらに、入室する要員については、2 名の要員の生体認証が行われ、要員が単独で室内に入室できないようにする。

(2) 認証設備室への入室においては、入室操作の時間と入室操作の試行回数をチェックすることにより、許可されない者が室内に不正侵入できないようにする。また、そのチェックにより検知した異常については、24時間監視を行っている監視室へ警告される。入室権限者が認証設備室へ入室する場合については、認証業務責任者が日常の入退室チェックと作業毎の入退室記録の確認を行う。日常の入退室チェックの方法は、アラームが発生した場合に、直接現場に行き入退室のチェックを行う方法を取る。

(3) 認証設備室からの退室においては、入室した要員の人数と退室する要員の人数が同じであることをチェックすることにより、入室した要員が室内に無用に残留できないようにする。

(4) 認証設備室が無人の(要員が完全に退室した)状態においては、モーションセンサーにより、室内の状況を常時監視し、何らかの動きを検知できるようにする。

(5) 認証設備室の入室及び退室ならびに認証設備室内での作業については、監視カメラにより、運営要員の活動が記録される。

(6) CA 秘密鍵の生成/リストア、認証業務用設備の補修工事等に際し、入室権限を有する要員以外の者が認証設備室へ入室しなければならないような場合、認証業務責任者の事前の許可を得て、入室権限を保有する作業監督者 2 名が同行し、監督することにより、認証設備室への入室を可能とする。非入室権限者の認証設備室への入退室時には非入室権限者が別途定める電子認証局アクセス管理規程に従い、入退室したことを認証業務責任者(認証業務責任者不在の場合は、上級 IA 操作員)が対面にて確認を行う。

(7) 認証局事務室(利用者証明書の発行情報を生成する設備である DIACERT-PLUS 証明書管理システムが設置される室)の出入り口には錠が取り付けてあり、入退室以外は常時施錠されている。

(8) 認証局事務室は他の区画と区分することにより、関係者以外が容易に設備に触れることができない。

5.1.3 電源及び空調の維持

認証設備室内の認証業務用設備、映像監視装置及び入室管理装置については商用電源が断たれた場合、認証システムの異常停止やサービスの中断を防止するために、設置された UPS（Uninterruptible Power Supply：無停電電源装置）及び自家発電装置からの給電を行う。また認証設備室は、専用の空調システムにより温度や湿度制御が行われる。

5.1.4 水害及び耐震

認証設備室は、建物の 2 階以上に設置され、洪水・津波などの水害から守られる。また、漏水対策も施される。また、認証設備室は、耐震対策を講じた建物に設置されるとともに、認証設備室に設置される機器については、地震による移動及び転倒などを防止する措置を講じる。

5.1.5 防火

認証設備室が設置される建物は、建築基準法に適合した耐火建物である。また、認証設備室は、建築基準法に適合した防火区画に設置され、自動火災報知器及び消火設備が設置される。

5.1.6 記録媒体の保管

本サービスに係る全ての媒体は、キャビネット又は、金庫などの施錠された安全な保管場所で管理される。

5.1.7 廃棄物処理

本認証局が保持する情報を廃棄する場合は、情報の漏洩が無いよう、次の方法で行う。

(1) 紙などに記録された情報

文書などについては、シュレッダーなどにより、記載された内容を確認できないよう処理する。

(2) 補助記録媒体などに記録されたデータ

磁気テープや運用で用いるICカードなどについては、無効データの上書き等を行なった上で完全消去するなどにより、記録されたデータを確認できないよう処理する。又は、補助記録媒体の物理的な破壊により、記録されたデータを復元できないよう処理する。

(3) コンピュータ機器などに記録されたデータ

コンピュータディスクや暗号化装置などについては、完全な初期化を行なうことにより、記録されたデータを確認できないよう処理する。また、本認証局の CA 秘密鍵のバックアップが格納された記録媒体については、物理的な破壊により、記録されたデータを復元できないよう処理する。

5.1.8 施設外のバックアップ

本認証局は、施設外へのバックアップは行わない。

5.2 手続き的セキュリティ管理

5.2.1 信頼すべき役割

本サービスに携わる運営要員とその役割を、表 5-1 に示す。

表 5-1 本認証局の運営体制

要員区分	役割
電子認証局代表者	① 新規の相互認証、相互認証の変更及び更新、相互認証の終了に関する決定 ② 本認証局運営の責任者である電子認証局責任者の任命、解任 ③ 本認証局の監査実施の指示 ④ CA 秘密鍵に危殆化が生じた場合の対応に関する決定 ⑤ 災害などによる緊急事態における対応に関する決定
電子認証局責任者	① CPS の策定、開示及び変更管理（含む承認） ② 新規相互認証、相互認証の変更及び更新、相互認証終了に関する審査 ③ 本認証局運用に係る要員の任命、解任及び人事管理 ④ 生成された CA 秘密鍵のバックアップの保管 ⑤ 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(立会) ⑥ CA 秘密鍵の初期化とバックアップ媒体の破壊(立会) ⑦ 認証業務に関わる規程など機密文書の保管 ⑧ 監査指摘事項への対処指示及び結果確認、並びに監査記録文書等の保管 ⑨ 鍵の危殆化や災害などの緊急時における対応の統括
審査登録業務責任者	① 受付審査担当者、RA 操作員、システム保守員への作業指示及び結果確認 ② 受付審査担当者、RA 操作員、システム保守員への業務記録の作成指示および管理 ③ 利用者証明書の利用申込及び失効申請、開示申請、受取代理人申請に係る審査結果の検認 ④ IA への利用者証明書の発行要求及び失効要求 ⑤ 審査結果など審査登録業務に関わる書類（アーカイブ）の保管 ⑥ 生成された CA 秘密鍵のバックアップの保管 ⑦ 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(立会) ⑧ CA 秘密鍵の初期化とバックアップ媒体の破壊(立会)
受付審査担当者	① 利用申込及び失効申請、開示申請、受取代理人申請に係る書類の受付け及び審査 ② 審査登録業務責任者への審査結果の報告 ③ 利用者情報の入力 ④ 利用者証明書の発行状況・有効期間の管理と利用者への通知 ⑤ 受領書の受取りと利用者情報との照合 ⑥ 利用者への失効通知、開示情報の送付、利用申込時の不備通知
RA 操作員	① 利用申込み、失効申請及び開示申請に関する書類の受付け及び審査 ② 利用者情報の入力、更新処理（立会） ③ CA システム（RA システム）への登録情報及び失効情報の生成（立会） ④ 利用申込みが許可された利用者情報の CA システム（RA システム）への登録 ⑤ CA システム（RA システム）への利用者証明書失効処理 ⑥ CA 秘密鍵が危殆化し、又は危殆化の恐れがある場合や災害等の緊急時における対応
認証業務責任者	① 上級 IA 操作員、一般 IA 操作員、システム保守員への作業指示と結果確認 ② 上級 IA 操作員、一般 IA 操作員、システム保守員の業務記録の管理 ③ 生成された CA 秘密鍵のバックアップの保管 ④ 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

要員区分	役割
	⑤ CA 秘密鍵の初期化とバックアップ媒体の破壊 ⑥ CA 秘密鍵の廃棄 ⑦ 証明書（CA 証明書、相互認証証明書、リンク証明書、PKI 運用関係者証明書を含む）の発行指示及び失効指示 ⑧ 認証設備室の維持管理、及び認証設備室のセキュリティ監査イベント（アーカイブ）の採取及び検査 ⑨ CA システムのセキュリティ監査イベント（アーカイブ）の検査 ⑩ CA 秘密鍵の危殆化や災害発生など緊急時の対応 ⑪ 発行した証明書やセキュリティ監査イベントなどのデータ（アーカイブ）の保管
上級 IA 操作員	① CA サーバの構築 ② CA 秘密鍵の生成 ③ CA 秘密鍵のアクティベーション及び非アクティベーション ④ CA システムの起動及び停止 ⑤ CA システムのセキュリティ監査イベント（アーカイブ）の採取 ⑥ CA システムの認証機能（セキュリティなどを含む）変更に関する設定変更 ⑦ CA 証明書、相互認証証明書、リンク証明書、PKI 運用関係者証明書の発行処理及び失効処理 ⑧ 利用者証明書の発行処理 ⑨ CRL/ARL/fullCRL の生成 ⑩ CA 秘密鍵の初期化とバックアップ媒体の破壊 ⑪ 利用者鍵ペア、利用者証明書、及び PIN コードの生成 ⑫ 利用者秘密鍵と利用者証明書の IC カードへの格納 ⑬ 利用者への利用者証明書（IC カード）及び PIN コードの発送 ⑭ CA システムのバックアップ
一般 IA 操作員	① CA システムの起動及び停止 ② CA 秘密鍵のアクティベーション及び非アクティベーション ③ 利用者証明書の発行処理 ④ CRL/ARL/fullCRL の生成 ⑤ 利用者鍵ペア、利用者証明書、及び PIN コードの生成 ⑥ 利用者秘密鍵と利用者証明書の IC カードへの格納 ⑦ 利用者への利用者証明書（IC カード）及び PIN コードの発送 ⑧ CA システムのバックアップ
システム保守員	① CA システムのハードウェア・OS などのセットアップ ② リポジトリのハードウェア・OS などのセットアップ ③ リポジトリの更新 ④ リポジトリ、利用者情報のバックアップ ⑤ リポジトリのセキュリティ監査イベント（アーカイブ）の採取及び検査 ⑥ CA システム、リポジトリの稼動状況監視 ⑦ CA システム、リポジトリのハードウェアの保守点検 ⑧ CA システム、リポジトリにおける障害発生時の一次対応ならびに復旧（IA 操作員と共同） ⑨ CA システム、リポジトリのソフトウェア機能強化（IA 操作員と共同） ⑩ リポジトリの機能変更に関する設定変更

5.2.2 業務に必要とされる人数

本認証業務に携わる運営要員の最低限必要な人数は、各運営要員 1 人とするが、発行業務、審査業務など重要な業務においては、合議制操作や相互牽制の必要から 2 名以上の要員を配置する。

5.2.3 個々の役割に対する本人性確認と認証

CA システムへのアクセスには、運営要員に対して発行した、本人しか持ち得ない IC カードの秘密鍵を使用した権限の強固な認証を行う。

5.2.4 職務分割が必要とされる役割

本認証業務に携わる運営要員は、登録局業務と発行局業務等必要に応じて、それぞれ兼務できない役割を別途規定する。

5.3 人的セキュリティ管理

5.3.1 経歴、資格、経験及び必要条件

本サービスに携わる者については、認証システムの開発、運用、コンサルテーションの実務経験を考慮して、採用が行われるものとする。

5.3.2 経歴調査

本サービスに携わる者については、別途定められたセキュリティ審査に従って、就業前の身元調査が行われるものとする。

5.3.3 トレーニング要件

本サービスに携わる者については、別途定められた教育・訓練計画に従って、指揮命令系統、責任と権限等の変更及び業務手順の変更に伴う教育、訓練の実施、並びに災害対応の定期的な教育訓練を実施する。

5.3.4 再トレーニングの頻度及び要件

本認証業務に携わる者については、教育・訓練計画に従って、指揮命令系統、責任と権限等の変更及び業務手順の変更に伴う教育・訓練の実施並びに災害対応の定期的な教育・訓練を実施する。

5.3.5 役職のローテーションの頻度及び要件

規定しない。

5.3.6 権限を逸脱した行為に対する制裁

本サービスに携わる者が、定められた権限を逸脱した行為を行った場合、その行為が故意か過失かに関わらず、定められた罰則が適用されるものとする。

5.3.7 独立した契約者の要件

規定しない。

5.3.8 運営要員が参照できるドキュメント

本認証業務に携わる要員は、業務に関する書類について、その役割及び権限に応じて参照することができるものとする。

5.4 セキュリティ監査イベント手続

5.4.1 セキュリティ監査イベントの種類

本認証局は、本認証局の IA、RA、リポジトリ及び認証設備室内のネットワーク機器並びに監視装置の状況に関する記録であるセキュリティ監査イベントを記録する。セキュリティ監査イベントには、下記のものが含まれる。また、イベントを起こした者への通知は行わない。

(1) CA システムの起動・停止等の稼動ログ及び機能変更等の操作ログ
(2) CA システムにおける利用者の登録、利用者証明書の発行請求及び失効請求並びに利用者証明書の生成処理及び失効処理に関するログ
(3) 利用者鍵ペアの生成及び IC カードへの格納に関するログ
(4) リポジトリにおける掲載情報の変更記録
(5) ファイアウォール、侵入検知システム等の認証設備室内のネットワークの監視ログ
(6) 認証設備室の入退室管理装置の動作ログ及び監視カメラの映像記録

5.4.2 セキュリティ監査イベントに対する検査の頻度

本認証局は、本サービスにおける信頼を維持するために、本認証局の運営に関する状況を記録し、これを定期的に監査する。

5.4.3 セキュリティ監査イベントの保存期間

セキュリティ監査イベント（認証設備室の監視カメラの映像記録を除く）は、1 年間保存する。

5.4.4 セキュリティ監査イベントの保護

セキュリティ監査イベントについては、漏洩、改ざん、毀損及び滅失の防止措置を行い、自然災害、火災及び盗難等から保護された電磁的記録媒体保存用の耐火金庫に保存する。

5.4.5 セキュリティ監査イベントのバックアップ手続

セキュリティ監査イベントは、月次でバックアップを行い記録媒体に保存する。

5.4.6 セキュリティ監査イベントの収集システム

セキュリティ監査イベントの収集機能は、本認証局の CA システム、リポジトリの機能、ネットワークシステム、入退室管理装置の機能として、業務及びセキュリティに関する重要な事象をイベントとして収集する。

5.4.7 イベントを起こしたサブジェクトへの通知

規定しない。

5.4.8 脆弱性評価

認証業務に関連するインターネット公開サーバについては、定期的に脆弱性評価を行う。

5.5 記録の保存

本認証局は、本サービスに関わる以下の書類及び電子的な記録を含め、電子署名法に定められた帳簿類を保存する。

5.5.1 アーカイブ記録の種類

アーカイブ記録の対象は以下のとおりとする。

(1) 利用申込みに伴い提出された利用申込書及び添付資料

① 利用申込書
② 利用者の印鑑登録証明書
③ 利用者の住民票の写し、住民票記載事項証明書又は、広域交付住民票
④ 利用者の所属する企業等の登記事項証明書(利用者の所属する企業等が法人又は、商業登記されている個人事業主の場合)
⑤ 利用者の所属する企業等代表者の印鑑証明書(利用者の所属する企業等が法人又は、商業登記されている個人事業主の場合)
⑥ 利用者の所属する企業等代表者個人の印鑑登録証明書(利用申込みされた利用者の所属する企業等が、商業登記されていない個人事業主であり、利用者が当該個人事業主の代表者である場合)
⑦ 別紙 3 に示す事業を営んでいることを証明する書類(利用申込みされた利用者の所属する企業等が、商業登記されていない個人事業主の場合)
⑧ 利用者本人のパスポート、特別永住者証明書又は、在留カードのコピー(利用者が日本に居住する外国人であり、住民票の写し等に本名の記載がなく、利用者証明書に本名の記載を求める場合)
⑨ 利用者本人のパスポートのコピー(利用者がヘボン式以外のローマ字で利用者氏名の記載を求める場合)
⑩ 戸籍全部事項証明書、戸籍個人事項証明書、戸籍謄本、又は、戸籍抄本(利用者証明書に旧姓の氏名の記載を求める場合)
⑪ 受取代理人の印鑑登録証明書(受取代理人がいる場合)
⑫ 受付審査時に作成した書類
⑬ 発行業務に関する記録
⑭ 受領書
⑮ BCA からの相互認証証明書の発行申請書類(発行に関する記録も含む)
⑯ 電子入札用電子証明書変更同意書(「電子入札コアシステム電子証明書利用申込書」を利用する場合)
⑰ 電子証明書変更同意書(DIACERT-PLUS サービスの公的証明書を DIACERT サービスの申込みに使用する場合)
⑱ DIACERT-PLUS 旧姓利用申込書(利用者証明書に旧姓の氏名の記載を求める場合)

(2) 失効申請に伴い提出された書類

① 失効申請書

② 失効依頼書
③ 印鑑登録証明書及び印鑑証明書
④ 失効審査時に作成した書類
⑤ 失効業務に関する記録
⑥ BCA からの失効申請に関する書類

(3) 開示申請に伴い提出された書類
① 開示申請書
② 印鑑登録証明書及び印鑑証明書

③ 受付審査時に作成した書類
④ 開示業務に関する記録

(4) 受取代理人申請に伴い提出された書類
① 受取代理人申請書
② 受取代理人の印鑑登録証明書

(5) 電子的な記録
① 発行、並びに失効した全ての証明書及びその作成ログ
② 本サービスに関係する全ての証明書
③ CRL/ARL/fullCRL
④ BCA から提供された相互認証証明書発行要求と相互認証証明書

(6) 組織関係の記録
① 本規程及びその改訂記録
② 業務手順に関する規程及びその改訂記録
③ 監査に関する記録(セキュリティ監査を除く)
④ BCA との相互認証に関する記録

(7) その他の記録
① 認証設備室への入退室の記録、及び入室権限を持たない者の入室時の記録
② セキュリティ監査イベントとして採取される記録
③ 認証業務用設備の障害及び復旧に関する記録
④ 認証業務用設備の保守、点検に関する記録
⑤ 帳簿類の利用・廃棄に関する記録

5.5.2 アーカイブ記録の保存期間

本認証局は、本規程「5.5.1 アーカイブ記録の種類」に規定する(1)から(6)の書類等については、当該書類当に係る利用者証明書の有効期間満了後 10 年間保存(書類については原本)するものとする。また、本規程「5.5.1 アーカイブ記録の種類」に規定する(7)については、作成された日から次回の特定認証業務の認定更新を経るまでの間保存するものとする。

5.5.3 アーカイブの保護

アーカイブの対象である書類及びデジタルデータについては、漏洩及び改ざん、毀損、滅失の防止

措置を行う。また、温度、湿度、磁気等環境における要素を考慮した上で保護される。

(1) 全ての情報は、次の条件を満たした本認証局の管理区域内で保管し、保護する。

① 施錠可能な出入り口を有する。

② 自動火災報知器および消火装置を備えている。

③ 直射日光が当たらない。

④ 高温多湿にならないよう空調機能が備えられている。

(2) 利用申込みにおいて利用者から提出された書類など原本性を確保する文書などの情報については、滅失、損傷、漏洩および改ざんを防止するため、管理区域内の文書保存専用のキャビネットに、体系化して保管する。

(3) 証明書など CA システムから出力されたアーカイブ対象である電磁的記録の情報については、記録媒体の変形や劣化を防止するため、管理区域内の電磁的記録媒体保存用の耐火金庫に、体系化して保管し、媒体保護のため、2 世代管理で記録媒体を保存し、かつ年1回以上の周期で媒体交換を実施する。媒体交換をする際には保存内容の完全性・機密性を損なわない方法で行う。

(4) 本規程「6.6.1 システム開発の管理」において、本認証局のシステムについては、電磁的記録で保存される記録の内容が表示できるように、当該システムの機器、OS 及びアプリケーションを維持し、互換性を確保する。

5.5.4 アーカイブのバックアップ手続

バックアップが必要なアーカイブデータについては、別途定められた内部規程に従いバックアップを行う。

5.5.5 記録にタイムスタンプを付ける要件

本規程「5.5.1 アーカイブ記録の種類」で規定する情報の記録時間は、処理を行った日付を記録する。

5.5.6 アーカイブ収集システム（内部又は外部）

アーカイブの収集機能は、本認証局の CA システム及びリポジトリの機能とし、業務及びセキュリティに関する重要な事象をアーカイブとして収集する。

5.6 鍵の更新

5.6.1 利用者の鍵の更新

鍵が自動的に更新されることはない。利用者証明書の有効期間が切れると同時に、鍵も無効となる。利用者は、利用者証明書及び鍵の更新が必要な場合は、再度、利用申込みを行わなければならない。

5.6.2 CA 証明書の鍵の更新

本認証局の CA 秘密鍵更新は、5 年に一度行われ、その際には、本認証局は新しい CA 証明書とリンク証明書を発行し、リポジトリに公開する。旧 CA 証明書については、有効期限までリポジトリへ公開する。旧 CA 秘密鍵については完全な廃棄を行う。

5.7 危殆化及び災害からの復旧

本認証局は、CA 秘密鍵の危殆化又は、危殆化の恐れがある場合や被災時の復旧手順を定め、要員の責任と権限に応じた教育・訓練計画を策定し、教育・訓練を実施する。

5.7.1 CA 秘密鍵が危殆化し、又は危殆化の恐れがある場合の対応

CA 秘密鍵の危殆化又は、危殆化の恐れがある場合、本認証局は次の措置を直ちに行なう。

(1) 証明書発行業務を直ちに中止する。

(2) CA 秘密鍵を使って、発行した全ての利用者証明書、相互認証証明書、リンク証明書を失効させ、CRL/ARL/fullCRL を更新し、リポジトリに公開する。利用者には、CA 秘密鍵危殆化の旨の情報、並びに利用者証明書を失効した旨を書面にて通知する。また CA 秘密鍵危殆化の旨をリポジトリ(Web ページ)に公開することにより、署名検証者へ通知する。その上で、CA 秘密鍵(バックアップを含む)を廃棄する。

(3) CA 秘密鍵が危殆化、又は危殆化の恐れがある場合及び災害、又は認証業務用設備の故障等により署名検証者への CRL/ARL/fullCRL の公開が 7 日間以上に渡り停止し、かつこれを署名検証者に知らせることができなかった場合、重大障害として、直ちに障害の内容、発生日時、処理状況等確認されている事項を主務大臣及び BCA に通報する。

(4) 被害状況の把握並びに、原因調査状況等を直ちに、主務大臣及び BCA へ通報する。また、再発防止策を立てる。

5.7.2 コンピュータのハードウェア、ソフトウェア及びデータが破損した場合の対応

本認証局は、認証業務停止が伴うハードウェア、ソフトウェア及びデータが破壊又は損傷した場合には、下記の措置を行う。

(1) 被害状況を調査の上、対策を実施し、バックアップデータによる回復措置を行う。

(2) 被害の状況、原因及び復旧の見通しをリポジトリに公開し、利用者及び署名検証者に開示する。また、原因別対応策を講じ、再発防止策を立てる。

(3) CRL/ARL/fullCRL の更新が 24 時間を越えて停止した場合、これを CRL/ARL/fullCRL 有効期限内に BCA 及び署名検証者に対し、リポジトリ(Web ページ)又は電子メール等で通知する。また、CRL/ARL/fullCRL 有効期限内に BCA 及び署名検証者に通知することができず、7 日以上 CRL/ARL/fullCRL の更新を行えなかった場合には、原因別対応策を講じ、重大障害として、障害の内容、発生日時、措置状況等確認されている事項を主務大臣へ報告する。

5.7.3 利用者秘密鍵が危殆化した場合の対応

本認証局は、利用者秘密鍵の管理を行わないため、利用者は、自身の秘密鍵が危殆化し、又は危殆化の恐れがある場合は、直ちに、本認証局に対し失効申請を行わなければならない。但し、政府機関に

よるコンテンジェンシープラン発動の指示があった場合には、本認証局は、その指示に従って対応する。

5.7.4 認証業務停止を伴う災害時の対応

本認証局が認証業務停止を伴う災害を受けた場合、次の措置を直ちに行なう。

(1) 被害の状況、原因及び復旧の見通しをリポジトリに公開し、利用者及び署名検証者に開示する。また、原因別対応策を講じ、再発防止策を立てる。

(2) CRL/ARL/fullCRL の更新が 24 時間を越えて停止した場合、これを CRL/ARL/fullCRL 有効期限内に BCA 及び署名検証者に対し、リポジトリ(Web ページ)又は電子メール等で通知する。また、CRL/ARL/fullCRL 有効期限内に BCA 及び署名検証者に通知することができず、7 日以上 CRL/ARL/fullCRL の更新を行えなかった場合には、原因別対応策を講じ、重大障害として、障害の内容、発生日時、措置状況等確認されている事項を主務大臣へ報告する。

5.7.5 CA 秘密鍵の危殆化後の事業継続性

本認証局は、CA 秘密鍵の危殆化時の対応について、本規程「5.7.1 CA 秘密鍵が危殆化し、又は危殆化の恐れがある場合の対応」の規定に従う。その後、事業を継続することが可能である場合には、新たに CA 秘密鍵を生成し、CA 証明書及び相互認証証明書の発行を行う事により、本サービスの継続に最善を尽くすものとする。

5.8 本認証局の廃止

本認証局は、特定認証業務の認定の更新を受けない場合を含めて、本サービスを廃止することができるものとし、次の方法にて行なう。

(1) 本サービスの廃止日迄に有効期間の残っている全ての利用者証明書及び相互認証証明書を失効し、全ての証明書の有効期間満了までの間、CRL/ARL/fullCRL をリポジトリに公開する。

(2) 本サービスを廃止する場合には、廃止日の 60 日前迄に、利用者及び BCA に書面で通知するとともに、リポジトリにその旨を公開する。

(3) 廃止時に、CA 秘密鍵を完全に初期化し、そのバックアップ媒体を物理的に完全に破壊する。

6　技術的セキュリティ管理

6.1 鍵ペアの生成及びインストール

6.1.1　　鍵ペアの生成

(1) 本認証局の鍵生成

本認証局のCA秘密鍵と CA 公開鍵の対である鍵ペア（以下、「認証局鍵ペア」という。）は、認証設備室内の暗号化装置の中で、複数の要員の合議制操作によって生成される。

(2) 利用者の鍵生成

利用者秘密鍵と利用者公開鍵の対である鍵ペア（以下、「利用者鍵ペア」という。）は、認証設備室内の中で、複数の要員によって生成され、利用者に発行されるICカードに格納される。利用者秘密鍵は、その IC カードに格納された後、認証業務用設備から完全に削除される。

6.1.2　　利用者への秘密鍵の配送

利用者秘密鍵は IC カードに格納され、その IC カードは利用者のみが受取れる「本人限定受取郵便（基本型）」にて配布される。本認証局は IC カードを受取った利用者からの受領書の受取をもって、利用者秘密鍵が安全に配付できたことを確認する。

利用者が委任した受取代理人による受取にて利用申込みを行った場合、その IC カードは利用者が委任した受取代理人へ配付され、受取代理人から利用者へ未開封のまま手渡される。但し、この場合においても、本認証局は、IC カードを受取った利用者からの受領書の受取をもって、利用者秘密鍵が安全に配付できたことを確認するものとする。

6.1.3　　本認証局への利用者公開鍵の配送

利用者公開鍵は、利用者鍵ペアとして本認証局で生成されるため、利用者から本認証局へ配送されることはない。

6.1.4　　利用者への CA 証明書の配送

CA 証明書はリポジトリに CA 証明書として公開するとともに、電子媒体に格納して利用者に配布する。

6.1.5　　鍵のサイズ

本認証局で生成される鍵のサイズは、以下のとおりである。

(1) 本認証局の鍵のサイズは、2048 ビットとする。

(2) 利用者の鍵のサイズは、2048 ビットとする。

6.1.6　　ハードウェアあるいはソフトウェアによる鍵の生成

(1) 本認証局の認証局鍵ペアは、暗号化装置（ハードウェア）で生成する。

(2) 利用者鍵ペアは、認証業務用設備内のソフトウェアで生成する。

6.1.7　　鍵の使用目的

(1) 本認証局の鍵は、以下の目的にのみ使用される。

① 利用者証明書に対する電子署名
② 相互認証証明書、及び本認証局の電子証明書発行要求への電子署名
③ CA 証明書に対する電子署名
④ CRL/ARL/fullCRL に対する電子署名
⑤ リンク証明書への電子署名

6.2 秘密鍵の保護

6.2.1 暗号化装置の基準

CA 秘密鍵は、FIPS 140-2 レベル 3 相当の暗号化装置によって生成・保存などの管理が行われる。

6.2.2 秘密鍵の複数人管理

本認証局の CA 秘密鍵の生成、管理は、本認証局の鍵の管理を担う複数の運営要員の合議制操作によって認証設備室にて行なわれる。

6.2.3 秘密鍵のエスクロー

本認証局は、CA 秘密鍵及び利用者秘密鍵のエスクロー(第三者寄託)を行なわない。

6.2.4 秘密鍵のバックアップ

本認証局の CA 秘密鍵は、本認証局の鍵の管理を担う複数の運営要員の合議制操作によって認証設備室内でバックアップされ、複数に分割されたバックアップ用の鍵として保管される。バックアップ用の鍵の個々については、一つずつ異なる場所の施錠等によりアクセス制御が実施されている場所の耐火金庫に保管する。

6.2.5 秘密鍵のアーカイブ

本認証局で生成される秘密鍵は、何れもアーカイブしない。

6.2.6 秘密鍵のエントリー（バックアップからのリストア）

本認証局の CA 秘密鍵をバックアップ用の鍵からリストアする場合は、本認証局の鍵の管理を担う複数の運営要員によって認証設備室にて行なわれる。

6.2.7 秘密鍵のアクティベーション方法

本認証局の CA 秘密鍵のアクティベーションは、認証設備室内において、本認証局の鍵の管理を担う複数の運営要員の合議制操作によって行われる。

6.2.8 秘密鍵の非アクティベーション方法

本認証局の CA 秘密鍵の非アクティベーションは、認証設備室内において、本認証局の鍵の管理を担う複数の運営要員の合議制操作によって行われる。

6.2.9　　秘密鍵の破壊方法

(1) 本認証局のCA秘密鍵の破壊は、鍵の使用期間が満了し更新した場合、もしくは鍵の使用を中止すること(本認証局の廃止など)を決定した場合に行う。

(2) 本認証局のCA秘密鍵の破壊は、本認証局の鍵の管理を担う複数の運営要員の相互牽制によって認証設備室にて行なわれる。

(3) 本認証局の CA 秘密鍵のバックアップ用の鍵については、本認証局の CA 秘密鍵の破壊に係る作業と合わせて遅延なく破壊される。

(4) 本認証局の CA 秘密鍵及びバックアップ用の鍵の破壊方法は、本規程「5.1.7 廃棄物処理」の規定に則り、行う。

6.3 鍵ペア管理に関するその他の要件

6.3.1　　公開鍵のアーカイブ

本規程「5.5 記録の保存」で規定するとおり行う。

6.3.2　　秘密鍵と公開鍵の使用期間

秘密鍵と公開鍵の使用期間については、表 6-1 に示す。

表 6-1 鍵の使用期間

	秘密鍵使用期間	公開鍵使用期間
本認証局	5 年	10 年
利用者	1 年、2 年、3 年、4 年 10 ヶ月	1 年、2 年、3 年、4 年 10 ヶ月

利用者公開鍵(利用者証明書)の使用期間は、1 年、2 年、3 年及び 4 年 10 ヶ月であり、その有効期間の開始は発行日の発行時刻であり、終了は 1 年後、2 年後 3 年後、又は 4 年 10 ヶ月後の月の最終日の 23 時 59 分 59 秒である。

上記により利用者に発行する利用者証明書の有効期間は発行の可否判断日から起算して 5 年未満である。

6.3.3　　CA 属性を持つ証明書の有効期間

CA 属性を持つ証明書の有効期間については、表 6-2 に示す。

表 6-2 CA 属性を持つ証明書の有効期間

証明書の種類	有効期間
自己署名証明書(CA証明書)	10 年
相互認証証明書	5 年以内

6.4 アクティベーションデータ

6.4.1　　アクティベーションデータの生成及びインストール

本認証局内で使用される CA 秘密鍵及び利用者秘密鍵を含む全てのアクティベーションデータは、定められた規則に従って生成及び管理される。

(1) 利用者証明書に対応する利用者秘密鍵と PIN コードについては、認証設備室にて複数の運営要員の相互牽制の下、ランダムに生成される。
(2) 生成された PIN コードは、認証設備室内で IC カードに格納され、格納後、認証業務用設備から完全に削除される。
(3) 本認証局は、利用者証明書を使用するための暗証番号である PIN コードを、IC カードとともに「本人限定受取郵便(基本型)」を使って利用者の住所に郵送する。IC カードの受取りを代理人に委任している場合は、IC カードとは別に PIN コードは利用者の住所に「簡易書留」を使って郵送する。
(4) 利用者は、PIN コードを紛失したり、盗用されたりしないよう一切の管理義務を負うものとする。
(5) 本認証局は、紛失などした PIN コードの再発行を行うことができない。
(6) PIN コードを紛失などした場合には、利用者は、利用者証明書の失効申請手続を行った後、利用者証明書の新規利用申込手続を行わなければならない。
(7) PIN コードを 15 回連続で間違えて入力すると IC カードを利用することが出来なくなる。

6.4.2 アクティベーションデータの保護

本認証局内で使用されるアクティベーションデータは、次の方法によって保護される。
(1) 利用者証明書に対応する利用者秘密鍵と PIN コードは、複数の操作者の相互牽制のもとで生成される。
(2) 操作者も印字内容が認識できない印字方法により PIN コードを印字する。

6.5 セキュリティ管理

6.5.1 セキュリティの要件

認証業務用設備はファイアウォール及びネットワークベースの侵入検知システム(IDS)を介して外部ネットワークと接続し、不正アクセスを検知・防止する。本サービスで用いる暗号化装置は FIPS140-2 レベル 3 の暗号化装置を用いる。

6.5.2 コンピュータセキュリティの管理

本認証局で使用している製品については、セキュリティに関する情報などを定期的に収集し、最新のセキュリティ技術の最新動向を踏まえ、使用する製品が設けたセキュリティに関する基準を満たすよう維持管理する。

6.6 ライフサイクルの技術的な管理

6.6.1 システム開発の管理

本認証局のシステムは、適切な品質管理が行われ、信頼できる組織で開発されたものを使用する。
本認証局のシステムについては、電磁的記録で保存される記録の内容が表示できるように、当該システムの機器、OS 及びアプリケーションを維持する。本認証局のシステムに係る機器、OS 及びアプリケーションを更新する場合は、更新前に試験などを行い、互換性を確保する。

6.6.2 セキュリティ管理

本認証局のシステムについては、別途定めるセキュリティに関する規程に則り、適切な運用を行う。

6.6.3 セキュリティ評価

本認証局のシステムについては、別途定めるセキュリティに関する規程に則り、定期的な評価を実施し、システム運用が定められたセキュリティに関する規程を満たすよう維持する。

6.7 ネットワークのセキュリティ管理

本認証局のネットワークについては、別途定めるセキュリティに関する規程に則り、適切な運用を行う。また、定期的な評価を実施し、ネットワーク運用が定められたセキュリティに関する規程を満たすよう、以下の措置を行い、維持する。

(1) 認証業務用設備を構成するネットワーク、及びリポジトリを構成するネットワークに対する不正アクセスを防止・検知するためのファイアウォール及び不正侵入検知システムによる制御・監視
(2) 認証業務用設備を構成するネットワーク上の通信データの漏洩及び盗聴防止のための暗号化
(3) 認証業務用設備を構成するコンピュータへの不正アクセスを防止するための遠隔操作ができない措置。

6.8 タイムスタンプ

認証業務用設備は、操作記録及び通信記録等に対して正確な時刻を記録するために、タイムサーバによる時間同期を行う。

7　証明書及び CRL/ARL/fullCRL のプロファイル

本認証局が発行する証明書及び CRL/ARL/fullCRL は、次の仕様に従っている。

(1) ITU-T Recommendation　X.509（1997）

(2) IETF RFC5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile

7.1 証明書プロファイル

7.1.1　　バージョン番号

本認証局は、X.509 バージョン 3 に準拠した証明書を発行する。

7.1.2　　証明書エクステンション

本認証局は、X.509 で定められたエクステンションを付加して証明書を発行する。詳細は、「別紙 1. 証明書プロファイル」を参照。

7.1.2.1 本認証局鍵識別子(authorityKeyIdentifier)

本認証局が設定する値を表 7-1 に示す。

表 7-1 本認証局鍵識別子(authorityKeyIdentifier)一覧

証明書種別	値
自己署名証明書	CA 公開鍵の SHA-1 ハッシュ値
リンク証明書（NewWithOld）	OldWithOld の公開鍵の SHA-1 ハッシュ値
リンク証明書（OldWithNew）	NewWithNew の公開鍵の SHA-1 ハッシュ値
相互認証証明書	CA 公開鍵の SHA-1 ハッシュ値
利用者証明書	CA 公開鍵の SHA-1 ハッシュ値

7.1.2.2 所有者鍵識別子(subjectKeyIdentifier)

本認証局が設定する値は、その証明書に含まれる公開鍵の SHA-1 ハッシュ値である。

7.1.2.3 鍵種別（keyUsage）

本認証局が設定する値を表 7-2 に示す。

表 7-2 鍵種別(keyUsage)一覧

証明書種別	用途(値)
自己署名証明書	証明書署名(keyCertSign)、CRL/ARL/fullCRL 署名(cRLSign)
リンク証明書 (NewWithOld、OldWithNew)	証明書署名(keyCertSign)、CRL/ARL/fullCRL 署名(cRLSign)
相互認証証明書	証明書署名(keyCertSign)、CRL/ARL/fullCRL 署名(cRLSign)
利用者証明書	電子署名(digitalSignature)、否認防止(nonRepudiation)

7.1.2.4 証明書ポリシー(certificatePolicies)

本認証局が設定する値を表 7-3 に示す。

表 7-3 証明書ポリシー(certificatePolicies)一覧

証明書種別	値種別	値
自己署名証明書	設定しない	－
リンク証明書 (NewWithOld、OldWithNew)	certPolicyId	2 5 29 32 0(any-policy)
相互認証証明書	certPolicyId policyQualifierId qualifier	1 2 392 200127 10 1 1 1 3 6 1 5 5 7 2 1(id-qt-cps) http://www.diacert.jp/plus/
利用者証明書	certPolicyId policyQualifierId qualifier	1 2 392 200127 10 1 1 1 3 6 1 5 5 7 2 1(id-qt-cps) http://www.diacert.jp/plus/

7.1.2.5 ポリシーマッピング(policyMappings)

本認証局が設定する値を表 7-4 に示す。

表 7-4 ポリシーマッピング(policyMappings)一覧

証明書種別	値種別	値
相互認証証明書	issuerDomainPolicy subjectDomainPolicy issuerDomainPolicy subjectDomainPolicy	1 2 392 200127 10 1 1 BCA 側のポリシーの OID(SHA-2) 1 2 392 200127 10 1 2 BCA 側のポリシーの OID(SHA-1)

7.1.2.6 基本制約(basicConstraints)

本認証局が設定する値を表 7-5 に示す。

表 7-5 基本制約(basicConstraints)一覧

証明書種別	値
自己署名証明書	cA=TRUE
リンク証明書	cA=TRUE

（NewWithOld、OldWithNew）	
相互認証証明書	cA=TRUE

7.1.2.7 名称制約(nameConstraints)

本認証局では、名称制約の設定を行わない。

7.1.2.8 ポリシー制限(policyConstraints)

本認証局が設定する値を表 7-6 に示す。

表 7-6 ポリシー制限(policyConstraints)一覧

証明書種別	値種別	値
相互認証証明書	requireExplicitPolicy inhibitPolicyMapping	0 1

7.1.2.9 CRL 配布点(cRLDistributionPoints)

本認証局が設定する値を表 7-7 に示す。

表 7-7CRL 配布点(cRLDistributionPoints)一覧

証明書種別	値
自己署名証明書	c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）, cn=ARL（UTF8）
リンク証明書 （NewWithOld、OldWithNew）	c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）, cn=ARL（UTF8）
相互認証証明書	c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）, cn=ARL（UTF8）
利用者証明書	c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）, cn=CRL（UTF8）
	http://www.diacert.jp/plus/rlist/crl.crl

表中の（Printable）は、設定された文字列が、printable string の文字コードでエンコードされていることを示す。

表中の（UTF8）は、設定された文字列が、UTF8 string の文字コードでエンコードされていることを示す。

7.1.3 署名アルゴリズム OID

本認証局から発行される証明書と CRL/ARL/fullCRL に使用される電子署名方式は、RSA 公開鍵暗号方式に基づくものを使用し、アルゴリズム OID は、1.2.840.113549.1.1.11(sha256WithRSAEncryption) である。

7.1.4 名前の形式

本サービスで使用する名称は、ITU X.500 シリーズ定義の識別名（DN: DistinguishedName）の形式に従う。自己署名証明書、及び利用者証明書における識別名において、subjectAltName、及び issuerAltName については、日本語、及び英語（アルファベット）を使用する。上記以外の識別名については、英語（アルファベット）のみを使用する。

利用者証明書に記載される利用者情報（subject）の識別名（DN）ならびに subjectAltName に記載する利用者の所属する組織に関する情報の識別名（DN）は、本規程「3.1.2 名称の意味に関する要件」に示される通りである。

本認証局を示す情報（issuer）の識別名ならびに issuerAltName に記載する識別名は下記表 7-8 に示す。

表 7-8 issuer と issuerAltName の名前形式

種別	値
issuer	c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）,
issuerAltName	c=JP(Printable), o=DIACERT-PLUS 認証局（UTF8）, ou=DIACERT-PLUS サービス（UTF8）

表中の（Printable）は、設定された文字列が、printable string の文字コードでエンコードされていることを示す。

表中の（UTF8）は、設定された文字列が、UTF8 string の文字コードでエンコードされていることを示す。

7.1.5 有効期間

本認証局から発行される証明書に記載される有効期間は、本規程「6.3.2 秘密鍵と公開鍵の使用期間」、及び本規程「6.3.3 CA 属性を持つ証明書の有効期間」に示される通りである。

7.2 CRL/ARL/fullCRL プロファイル

ARL にはリンク証明書及び相互認証証明書の失効情報が記載される。CRL には利用者証明書の失効情報が記載される。fullCRL にはリンク証明書及び相互認証証明書の失効情報ならびに利用者証明書の失効情報が記載される。

7.2.1 バージョン番号

本認証局は、X.509 バージョン 2 に準拠した CRL/ARL/fullCRL を発行する。

7.2.2 CRL/ARL/fullCRL 及び CRL/ARL/fullCRL エントリエクステンション

本認証局の CRL/ARL/fullCRL プロファイルについては、本規程「別紙 2. CRL/ARL/fullCRL プロファイル」を参照。

失効理由コード（reasonCode）については RFC5280 で定義されている失効理由コードが記載される。

8　準拠性監査や他の評価

8.1 監査の頻度

監査の頻度は以下の通りとする

(1) 監査は、電子署名法に基づく認定更新に先立って、1 年に一度定期監査として実施する。本認証局は、監査を実施するために、別に「監査規程」を定め、監査計画として監査目的、監査人、スケジュール、監査対象及び作業要領を明確にする。

(2) セキュリティに関する重要な変更などについては、都度、自己監査を実施する。

8.2 監査人の身元・資格

監査人は、本認証局運営部門の要員以外から十分な知識を持った者を電子認証局代表者の指示に基づいて、選定される。

8.3 監査項目

監査項目は、下記の通りとする。

(1) 監査では、本認証業務が本規程及び別に定める諸規程等の基準及び手順に則って実施されていること並びに不正行為等の脅威に対する措置が有効に機能していることを検証する。

(2) 本認証局が発行した電子証明書のライフサイクル管理

(3) IA、RA 及びリポジトリの運用業務

(4) CA 秘密鍵の管理

(5) ソフトウェア、ハードウェア及びネットワーク

(6) 物理的環境及び設備

8.4 監査指摘事項への対応

本認証局は、監査結果である監査報告書で指摘された事項に関して、速やかに、下記の改善の措置を行う。

(1) 軽微な監査指摘事項については、改善するための合理的な是正措置を実施する。また、重要事項又は緊急を要する監査指摘事項については、速やかに対応する。

(2) CA 秘密鍵が危殆化し、又は危殆化の恐れに関する指摘があった場合は、緊急事態と位置付け、緊急時対応の手続きをとる。

(3) 重要事項又は緊急を要する監査指摘事項が改善されるまでの間は、本サービス又は相互認証を継続するか否かは、認証局代表者が決定する。

(4) 本認証局は、監査指摘事項に対して対策を実施したことを確認し、指摘事項に対して実施した改善結果を評価する。

(5) セキュリティ技術の最新動向を踏まえて、設備及び本規程等の見直しを含む対応措置を実施する。

8.5 監査結果の報告

監査結果は、監査報告書にて監査人から電子認証局代表者へ報告される。電子認証局代表者は、監査結果を承認し、その監査結果に係る証明書の有効期間満了後 10 年間保存する。

本認証局は、監査結果の開示要求については、電子署名法の認定更新時における指定調査機関からの要求、主務官庁からの要求などに対してのみ応じる。また、BCA に対しては、開示要求の有無に係らず相互認証業務等に関する監査結果の報告を行う。

9 他の業務事項と法的事項

9.1 料金

本サービスに係る料金は、本認証局の Web サイト（下記）に掲載する。

http://www.diacert.jp/plus/

(1) 利用申込者もしくは企業等は、利用者証明書の発行手数料として、別途定める金額を所定の方法で指定する期日までに本認証局に支払うものとする。

(2) 指定する期日までに支払いがない場合、本認証局は利用者への事前通知なしに、発行済の利用者証明書を失効させることができるものとする。

9.2 財務上の責任

9.2.1 責任範囲

本認証局の責任の範囲は、下記のとおりとする。

(1) 本認証局は、本認証局が本規程に定める本認証局の責任に違反したことにより、利用者及び署名検証者に損害を与えた場合には、その損害の賠償責任を負うものとする。ただし、本認証局の責に帰すことができない事由から生じた損害及び逸失利益については、賠償責任を負わないものとする。

(2) 利用者が本規程で定める範囲以外の用途に利用者証明書を使用した結果生じたトラブルについては、利用者が一切の責任を負うものとする。当該トラブルにより本認証局及び署名検証者に損害を与えた場合、利用者が本認証局及び署名検証者に対し、損害賠償を行なうものとする。

(3) 利用者が本規程で定める失効申請を怠った結果生じたトラブルについては、利用者が一切の責任を負うものとする。当該トラブルにより本認証局及び署名検証者に損害を与えた場合、利用者が本認証局及び署名検証者に対し、損害賠償を行なうものとする。

(4) 利用者の所属する企業等が、本規程に定める失効に関する義務を履行しなかったことにより本認証局が損害を被った場合、本認証局は当該企業等に対し当該損害の賠償を請求することができる。

(5) 署名検証者が使用目的の範囲を超えて利用者証明書を使用した結果被った損害については、署名検証者が一切の責任を負うものとする。

9.2.2 利用者に対する保証

本認証局が損害賠償責任を負う場合、別途定める利用者同意書、署名検証者同意書に定める範囲とする。

9.2.3 分割、存続、合併に対する保証

本認証局は、ジャパンネット株式会社の分割、合併等が行なわれる場合においても、本サービスを継続すべく最善を尽くす。

9.3 業務情報の秘密保護

9.3.1 秘密情報の範囲

(1) 本認証局が保有する情報のうち、CA 証明書、利用者証明書、CRL/ARL/fullCRL、本規程等の公開文書を除いた情報が、機密保持の対象として扱われる。

(2) 本認証局は、法的根拠に基づいて情報を開示するよう請求があった場合、もしくは利用者から書面による事前の承諾を得ている場合を除いて、本規程において機密保持の対象として扱われる情報を開示しない。

(3) 次に示す GPKI 接続要件に従う。

① 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。

② 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。

9.3.2 秘密情報の範囲外の情報

本認証局が保有する情報のうち、利用者証明書、CRL/ARL/fullCRL 及び本規程などの公開文書は秘密情報として取扱わない。

9.3.3 秘密情報を保護する責任

本認証局は、施錠された場所に秘密情報を記録した書類やデータを保存し、許可された者以外がアクセスできないような措置を講じ、秘密情報への不正アクセス又は漏洩を防止する。

9.4 個人情報の保護

9.4.1 個人情報の種類

本規程において個人情報とは、利用者証明書の利用申込み、失効申請及び開示申請等にあたって、利用者から提出された全ての情報及び本認証局にて作成した利用者に関する全ての特定の利用者を識別できる情報をいう。また、認証設備室に入室するために登録される生体情報、及び入室時の映像記録も個人情報として取り扱う。

9.4.2 個人情報とは見なされない情報

本規程「9.4.1 個人情報の種類」に規定する情報以外については、個人情報とみなさない。

9.4.3 個人情報を保護する責任

本規程「9.4.1 個人情報の種類」に規定された情報は、本認証業務の用に供する以外は使用しないこと及び本認証業務に必要な範囲を越えて収集を行わないこと等の個人情報の取扱いについて、別に定めるアクセス管理規程に従い、その機密が保持されるようにする。

本認証局は、施錠された場所に個人情報を記録した書類を保存することで、許可された者以外がアクセスできないような措置を講じ、個人情報への不正アクセス又は漏洩を防止する。また、個人情報の取扱いについては、運営要員を対象とし、各運営要員の役割に応じた教育・訓練計画を策定し、教育及び訓練を行う。

9.4.4　　個人情報の使用に関する個人への通知及び同意

本認証局は、利用者からの証明書の申込をもって、利用者が本規程及び利用者同意書に同意したものとみなし、利用者から本認証業務上必要とする個人情報の使用の承認を得たものとする。

本認証局は、個人情報を本認証業務以外には使用しない。

9.4.5　　司法手続又は行政手続きによる情報開示

本認証局は、本認証局で取扱う情報に対し、法的根拠に基づいて情報を開示するよう請求があった場合は、法の定めに従い、法執行機関等へ情報を開示する。また、本認証局は、調停、訴訟、その他法的手続き又は行政手続の過程において、機密保持対象である情報を開示することができるものとする。

9.4.6　　利用者の要請による情報開示

(1) 利用者は、本認証局が有する利用者についての情報の開示を求める権利を有する。但し、本認証局は電子署名法第 11 条の要件に基づき、保管義務のある申請書類等の訂正又は削除の要求には応じることができない。

(2) 本認証局は、発行した利用者証明書の利用者から、権利又は、利益を侵害される又は、侵害されるおそれがあると申し出があった場合、申し出たものが当該利用者証明書の利用者であることを確認した上で、本認証局が保有する次の情報を開示する。

① 利用申込書ならびに添付書類の写し

② 利用者証明書の記載事項の写し

(3) 本認証局は、情報の開示を行うにつき、開示に要する費用を請求することができる。

(4) 本認証局は、利用者が開示申請を行った場合、DIACERT-PLUS 開示申請書（以下、「開示申請書」という。）を郵送でのみ受付ける。開示申請者の真偽確認を行い、正しく確認できた開示申請者へ情報を開示する。

(5) 開示申請者の真偽確認は、下記の手段により行う。

① 開示申請書に証明書番号が記載されていること。証明書番号とは利用者証明書を一意に指定するために利用者証明書の格納された IC カードの表面に印刷されている 14 桁の英数字のことである。

② 開示申請書に記載された氏名、住所、生年月日及び実印の印影が該当する証明書番号の利用申込書に記載されている利用者の氏名、住所、生年月日及び実印の印影と一致すること。

本認証局は開示申請者に対して、本人限定受取郵便（基本型）にて、開示情報を送付する。

9.4.7　　その他の情報開示

本サービスの一部を外部の業者に委託する場合は、業務に係って委託先に開示する情報の機密性を確保するために、守秘義務を定めた委託契約を委託業者との間で締結する。

9.4.8　　生体情報及び映像情報の取扱い

電子署名法施行規則の要件に基づき、認証設備室に入室するための要員の生体情報が入退室管

理装置に記録され、入退室の記録が一定期間保存される。また、認証設備室に入室した要員や非入室権限者の映像情報が映像記録装置に記録され、一定期間保存される。

9.5 知的財産権

次の情報及びデータについての著作権、その他知的財産権など全ての権利は、本認証局に帰属するものとする。

(1) 本認証局より発行された利用者証明書
(2) 本認証局より公開された CRL/ARL/fullCRL
(3) 本規程
(4) 本サービスに関するマニュアル

9.6 責任及び義務

9.6.1 認証局の責任及び義務

本認証局は以下の義務を負う。

(1) 本規程に基づき本認証局の運用を行い、業務の運用に関する詳細を規定した下位文書を定める。
(2) 本認証局の CA 秘密鍵が危殆化、又は危殆化の恐れが生じないように保護する。
(3) 利用者及び署名検証者に対し、本サービスによって発行された利用者証明書には、電子署名法の認定対象外の情報を含むことを本規程に記載し、公開する。
(4) 本認証局は、本規程に従い、受付日の受付時間内に問合せを受付ける。
(5) 本認証局は、本規程をリポジトリにて公開する。
(6) 本認証局は、CRL/ARL/fullCRL の有効期間を 48 時間、更新を 24 時間毎とし、一時停止、緊急時などのやむを得ない停止を除き、リポジトリに公開する。
(7) 本認証局（IA、RA 及びリポジトリを含む）は、電子認証局代表者の指示に基づく監査を定期的に年 1 回実施し、監査報告に基づいて改善を行う。
(8) BCA との相互認証申請に際して、正確な情報を提示する。BCA との相互認証証明書の取り交わしについては BCA の定めた手続きに従う。また、BCA 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 がこの公開鍵に対する BCA の秘密鍵を保有していることを確認する。

9.6.2 IA の責任及び義務

本認証局を構成する IA は、次の義務を負う。

(1) 本規程及び下位文書に基づき、IA の運用を行なう。
(2) IA の責任者を 1 名配置する。
(3) 本認証局の CA 秘密鍵を安全に生成し、管理する。
(4) RA からの証明書の発行要求に基づき、誤りのない証明書の発行を行う。
(5) 利用者公開鍵、利用者秘密鍵及び PIN コードを安全に生成する。
(6) 利用者秘密鍵と利用者証明書を安全に IC カードに格納し、IC カードと PIN コードを正当な利用者へ安全、確実に配布する。
(7) RA からの証明書の失効要求に基づき、証明書の失効を行う。

(8) 証明書等の情報、及びその他の情報を安全に保管する。
(9) CRL/ARL/fullCRL の更新を行う。

9.6.3 RA の責任及び義務

本認証局を構成する RA は、次の義務を負う。
(1) 本規程及び下位文書に基づき、RA の運用を行なう。
(2) RA の責任者を 1 名配置する。
(3) 利用申込書を審査し、申込者の真偽確認及び利用組織への所属等の属性の確認を確実に行う。
(4) 利用者証明書の発行を IA に要求する。
(5) 利用者証明書の失効を行う。
(6) 利用者証明書を失効した場合は、その旨を利用者に通知する。
(7) 失効申請書を審査し、失効申請者（利用者本人、利用者の所属する企業等）の真偽確認を確実に行う。
(8) 個人情報保護、秘密情報の保護、利用申込書類の管理・保管を適切に実施するとともに、開示請求への対応を行なう。

9.6.4 利用者の責任及び義務

利用者は、次の義務を負う。
(1) 利用者証明書の利用に際しては、本規程及び利用者同意書に同意し遵守するとともに、本規程記載の用途でのみ利用者証明書を利用しなければならない。
(2) 利用者証明書の利用申込みに際しては、利用者の所属する企業等の同意を得なければならない。
(3) 利用者証明書の利用申込みに際しては、利用者本人が正確な利用申込み内容を本認証局に提出しなければならない。虚偽の利用申込みをして利用者について不実の証明をさせた者は、電子署名法第 41 条により罰せられる。
(4) 日本に居住する外国人の利用者は、在留期間が満了した場合は、本認証局に遅滞なく利用者証明書の失効申請を行わなければならない。
(5) 利用者は、電子署名が自署や押印に相当する法的効果を認められ得るものであることを承知しなければならない。利用者は、本サービスによって発行された利用者証明書に対応する利用者秘密鍵と PIN コードを、十分に注意して管理し、秘匿し続けなければならない。
(6) 利用者は、IC カード受領時に利用者証明書の記載事項、有効性等を確認し、記載事項に誤りがあった場合には、直ちに「1.5.2 問い合わせ先」に示す［問合せ先］へ連絡しなければならない。
(7) 利用者は、発行された利用者証明書が危殆化し、又は危殆化の恐れがある場合、本認証局に遅滞なく利用者証明書の失効申請を行わなければならない。また、利用者証明書に記録されている事項に変更が生じた場合、もしくは利用者証明書の利用を中止する場合においても、遅滞なく利用者証明書の失効申請を行わなければならない。
(8) 本認証局は、利用者が使用する電子署名アルゴリズムとして、法令で定めるアルゴリズムのうち、SHA1withRSA、SHA256withRSA、SHA384withRSA または、SHA512withRSA を指定する。利用者は、本認証局が指定する電子署名アルゴリズムを使用しなければならない。
(9) 利用者は、署名検証者が利用者証明書を利用することに関し本認証局は責任を負わないことを、承

知しなければならない。

(10) 利用者は、リポジトリを随時閲覧し、本サービスに関する情報を適宜取得しなくてはならない。

(11) 利用者は、本認証局が利用者の所属する企業等の依頼に基づき当該利用者証明書を失効させる場合があることに同意する。

9.6.5 署名検証者の責任及び義務

署名検証者は、次の義務を負う。

(1) 利用者証明書の利用においては、本規程及び署名検証者同意書に同意し遵守するとともに、本規程記載の用途でのみ利用者証明書を利用しなければならない。

(2) 署名検証者は利用者証明書の利用にあたり、利用者証明書の検証を行なわなければならない。即ち本認証局の CA 証明書、リンク証明書により利用者証明書を署名検証することにより、当該利用者証明書が本認証局の CA 秘密鍵により電子署名されていることを検証する。本認証局の CA 証明書のフィンガープリント(CA 証明書の値を SHA256 でハッシュ変換した値)、リンク証明書のフィンガープリント(リンク証明書の値を SHA256 でハッシュ変換した値)と、リポジトリに公開しているフィンガープリントとを 比較検証することにより、当該 CA 証明書、リンク証明書が本認証局の発行したものであることを確認する。

(3) 利用者証明書について、その利用者証明書が有効期間内であること、失効されていないかどうかを確認する。

(4) 利用者証明書を利用するにあたり、本認証局がリポジトリで公開する本サービスに関する情報を確認しなければならない。

9.6.6 リポジトリの責任及び義務

リポジトリは、下記の責任及び義務を負う。

(1) 本規程を公開する。

(2) CRL/ARL/fullCRL により、失効した証明書の情報を遅滞なく公開し、その証明書の有効期間が満了するまで公開し続ける。

(3) 利用者同意書及び署名検証者同意書の公開を行う。

(4) CA 証明書、リンク証明書及び相互認証証明書の公開を行う。

(5) CA 証明書のフィンガープリント、及びリンク証明書のフィンガープリントの公開を行う。

(6) その他本認証業務に関する情報の公開を行うことで、利用者、利用者の所属する企業等、及び署名検証者が本サービスの利用に必要な諸情報、諸手続き等を把握できるようにする。

9.6.7 企業等の責任及び義務

利用者が利用者証明書の利用申込みを行うことに同意した企業等は、次の義務を負うものとする。

(1) 企業等は本規程及び利用者同意書に同意し、遵守する。

(2) 下記に示す、企業等が利用者証明書を失効すべき事由が発生した場合は、利用者に利用者証明書の使用を中止させ、利用者証明書の失効依頼を行なわなければならない。ただし、企業等は利用者自身が失効すべき事由においては失効依頼を行なうことはできない。

・ 利用者が当該企業等に属さないこととなった場合
・ 利用者が利用者証明書を利用して権限を行使することができなくなった場合
・ 企業名又は、企業住所（本店）に変更が生じた場合
・ 利用者が死亡した場合
・ その他、利用者証明書を失効させる必要があると判断した場合

9.7 責任の制限

9.7.1 利用者の義務違反

本認証局は、利用者が本規程「9.6.4 利用者の責任及び義務」の規定に違反したことが原因で生じた損害については、関係者に対し一切の責任を負わない。

また、利用者が本規程「9.6.4 利用者の責任及び義務」に規定する責任又は義務に違反していることが明らかな場合は、利用者への事前の通知を行うことなく、利用者に対して発行した電子証明書を失効させることができるものとし、利用者は、これに対し一切の請求又は異議申し立てを行うことができないものとする。

9.7.2 署名検証者の義務違反

本認証局は、署名検証者が本規程「9.6.5 署名検証者の責任及び義務」の規定に違反したことが原因で生じた損害については、関係者に対し一切の責任を負わない。

9.7.3 不可抗力

不可抗力による免責は、下記のとおりとする。

(1) 本認証局は、利用者又は署名検証者が、利用者証明書を利用する際に発生したコンピュータシス テム等のハードウェア又はソフトウェアへの障害については、一切の賠償責任を負わない。

(2) 本認証局は、下記の事由による本サービスの全部又は一部の停止によって被った利用者及び署名検証者の損害については、一切の損害賠償責任を負わない。

① 火災又は停電等
② 地震、噴火、洪水、津波等の天災
③ 戦争、動乱、暴動、騒乱、労働争議等
④ 電気通信事業者が電気通信サービスを中断又は停止した場合
⑤ その他、認証局代表者が運用上又は技術上の事由により本サービスの中断又は停止が必要と判断した場合
⑥ 行政関係システムの不具合

9.8 免責事項

(1) 本認証局は、利用者又は、署名検証者が本規程「1.4 証明書の用途」で定める用途以外に利用者証明書を使用することに対して、一切の責任を負わない。

(2) 本認証局は、IC カードならびに IC カードに格納されている利用者秘密鍵の盗難、不正使用などによって、利用者又は、署名検証者が被った損害に対して、一切の責任を負わない。

(3) 本認証局は、利用者の PIN コードの盗難、不正使用などによって、利用者又は、署名検証者が被っ

た損害に対して、一切の責任を負わない。

(4) 本認証局は、証明書の失効申請ならびに失効依頼に対し、遅滞なく失効をおこなった場合、リポジトリへの CRL/ARL/fullCRL の公開前に発生した利用者又は、署名検証者の被害に対し、一切責任を負わない。

(5) 本認証局は、利用者又は、署名検証者が、利用者証明書を利用する際に発生したコンピュータシステムなどのハードウェアもしくはソフトウェアへの障害について、一切の賠償責任を負わない。

(6) 本認証局は、以下に定める事由による本サービスの全部又は、一部の停止によって被った利用者又は、署名検証者の損害については、一切の損害賠償責任を負わない。

① 火災、停電等
② 地震、噴火、洪水、津波などの天災
③ 戦争、動乱、暴動、騒乱、労働争議等
④ 電気通信事業者が電気通信サービスを中断又は、停止した場合
⑤ その他、運用上あるいは技術上、本サービスの中断又は、停止が必要と判断した場合

(7) 電子署名法の認定対象外となる属性情報が原因となって受けた利用者又は、署名検証者の損害について、本認証局は一切の賠償責任を負わない。

(8) 本認証局は、その他本認証局の責に帰すべきでない事由から生じた利用者又は、署名検証者の損害については、一切の損害賠償責任を負わない。

9.9 本ポリシーの有効期間と終了

9.9.1 有効期間

本規程は、作成された後、認証業務審議会が承認することによって有効となり、また、本規程「9.9.2 終了」に規定する本規程の終了まで有効とする。

9.9.2 終了

本規程は、本規程「9.9.3 終了の影響と存続条項」に規定する存続条項を除き、認証業務審議会が無効とした時点又は本認証局が本認証業務を終了した時点で無効となる。

9.9.3 終了の影響と存続条項

本認証局が終了した場合であっても、本規程「9.4 個人情報の保護」、「9.5 知的財産権、「9.6 責任及び義務」、「9.7 責任の制限」、「9.8免責事項」、「9.9.3 終了の影響と存続条項」、「9.12 管轄裁判所」、「9.13 準拠法」、「9.14 適用法の遵守」及び「9.15 その他の条項」の各規程については、なお、効力を有する。

9.10 関係者間の個別通知と報告

(1) 本認証局は、本認証局から利用者への通知方法として、郵便、電子メール又は、ホームページへの掲示など、本認証局が適当と判断した方法により行う。

(2) 第 1 項に定める郵便による通知においては、当該郵便の消印を利用者への到達時とみなす。

(3) 第 1 項に定める電子メールによる通知においては、当該電子メールを本認証局の運営要員が送信し、送信できたことが確認できた時点とみなす。

(4) 第 1 項に定めるホームページへの掲示による通知においては、当該掲示の掲載日を利用者への到達時とみなす。

9.11 改訂

9.11.1 改訂手続

本認証局は、本規程及び別に定める諸規程の仕様を変更することができる。また、本認証局は、利用者及び署名検証者に事前の了解を得ることなく、本規程に定めた仕様の変更をすることができる。仕様変更の内容は、認証業務審議会での審議を経て、認証局責任者が変更を承認する。但し、緊急時等で認証業務審議会が開催できない場合は、認証局責任者が変更内容を審議し、承認する事とする。この場合、認証業務審議会での承認は事後承認とし、その旨を議事録に残す。

なお、主務大臣の認定が必要な事項については、主務大臣の変更認定を得て発効する。

9.11.2 通知方法と期間

利用者、及び利用者の所属する企業等は、変更した本規程を公開後、15 日以内に利用者が自己の利用者証明書の失効申請を行なわない場合には、変更に同意したものとみなす。

(1) 仕様が変更された本規程については、変更後、速やかに、リポジトリにて公開することにより、利用者及び署名検証者へ通知されたものとする。
(2) 仕様が変更された本規程については、仕様が変更された抜粋ではなく、全てを公開する。
(3) 本規程の変更については、バージョン番号及び改訂日により識別する。
(4) 仕様が変更された本規程については、リポジトリによる利用者及び署名検証者への通知をもって、直ちに、有効とする。利用者及び署名検証者は、本認証局のリポジトリを定期的に参照し、本規程の変更について同意するものとする。

9.12 管轄裁判所

利用者もしくは署名検証者と本認証局との間に、訴訟や法的行為が起こる場合、東京地方裁判所を管轄裁判所とする。

9.13 準拠法

本規程は、日本国内法及び電子署名法に関する法令等に基づき解釈されるものとする。

9.14 適用法の遵守

本認証業務は、下記の法令等を遵守する。

(1) 「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)
(2) 「電子署名及び認証業務に関する法律施行令」(平成 13 年政令第 41 号)
(3) 「電子署名及び認証業務に関する法律施行規則」(平成 13 年総務省、法務省、経済産業省令第 2 号)
(4) 「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」(平成 13 年 4 月 27 日 総務省、法務省、経済産業省告示第 2 号)

9.15 その他の条項

9.15.1　　完全合意条項

本規程は、本規程で定められた事項に対して関係者間における完全合意を構成するものであり、本サービスについて本規程より早い時期及び同時期に定められた書面、口頭による意思表示、合意及び表明事項のすべてに優先する。

9.15.2　　権利譲渡条項

規定しない。

9.15.3　　分離条項

本規程は、規定の一部に対し、裁判所又はその他評決機関が何らかの理由により、無効又は執行できないと判断した場合においても、その理由の如何を問わず、その他の部分の規定は、効力を失わないものとする。

別紙 1. 証明書プロファイル

表 A-1 に、自己署名証明書プロファイル、表 A-2 に、リンク証明書（NewWithOld）プロファイル、表 A-3 に、リンク証明書（OldWithNew）プロファイル、表 A-4 に、相互認証証明書プロファイル、表 A-5 に、利用者証明書プロファイルをそれぞれ示す。

凡例

(1) (sha256WithRSAEncryption)及び(rsaEncryption)はそれぞれ、OID に対応づけられた暗号アルゴリズムを示している。

(2) (any-policy)は、OID に対応づけられた、ポリシー識別子を示す。

(3) (id-qt-cps)は、OID に対応づけられた、ポリシー識別子を示す。

(4) （Printable）は、設定された文字列が、printable string の文字コードでエンコードされていることを示す。

(5) （UTF8）は、設定された文字列が、UTF8 string の文字コードでエンコードされていることを示す。

(6) （IA5）は、設定された文字列が、IA5 string の文字コードでエンコードされていることを示す。

表 A-1 自己署名証明書プロファイル

領域名	クリティカルフラグ	規定内容と設定値（○：設定する、×：設定しない）
基本部		
version		2(v3)
serialNumber		1（例）
signature		1.2.840.113549.1.1.11(sha256WithRSAEncryption)
validity		○
notBefore		有効期間は10年に設定（UTCTime で設定する）
notAfter		
issuer		c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）
subject		c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）
subjectPublicKeyInfo		○
algorithm		1 2 840 113549 1 1 1(rsaEncryption)
subjectPublicKey		RSA 公開鍵値(2048bit)
issuerUniqueID		×
subjectUniqueID		×
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		
directoryName		c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）
authorityCertSerial		本証明書の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		本証明書の公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
keyCertSign		○
cRLSign		○
extendedKeyUsage		×
privateKeyUsagePeriod		×
certificatePolicies		×
policyMappings		×
issuerAltName	FALSE	○
directoryName		c=JP(Printable), o=DIACERT-PLUS 認証局（UTF8）, ou=DIACERT-PLUS サービス（UTF8）
subjectAltName	FALSE	○
directoryName		c=JP(Printable), o=DIACERT-PLUS 認証局（UTF8）, ou=DIACERT-PLUS サービス（UTF8）
basicConstraints	TRUE	○
cA		TRUE
pathLenConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		c=JP(Printable), o= DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）, cn=ARL（UTF8）

	distributionPoint		○
	uniformResource Identifier		http://www.diacert.jp/plus/rlist/arl.crl
subjectDirectoryAttr			×
authorityInfoAccess			×
独自拡張領域			×

表 A-2 リンク証明書(NewWithOld)プロファイル

領域名	クリティカルフラグ	規定内容と設定値(○:設定する、×:設定しない)
基本部		
version		2(v3)
serialNumber		1(例)
signature		1.2.840.113549.1.1.11(sha256WithRSAEncryption)
validity		○
notBefore		NewWithNew の validity.notBefore(UTCTime で設定)
notAfter		OldWithOld の validity.notAfter(UTCTime で設定)
issuer		c=JP(Printable), o=DIACERT-PLUS CA(UTF8), ou=DIACERT-PLUS Service(UTF8)
subject		c=JP(Printable), o=DIACERT-PLUS CA(UTF8), ou=DIACERT-PLUS Service(UTF8)
subjectPublicKeyInfo		○
algorithm		1 2 840 113549 1 1 1(rsaEncryption)
subjectPublicKey		RSA 公開鍵値(2048bit)
issuerUniqueID		×
subjectUniqueID		×
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		NewWithNew の公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		OldWithOld の issuer の DN
authorityCertSerial		OldWithOld の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		本証明書の公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
keyCertSign		○
cRLSign		○
extendedKeyUsage		×
privateKeyUsagePeriod		×
certificatePolicies	FALSE	○
policyIdentifier		○
certPolicyId		2 5 29 32 0(any-policy)
policyQualifiers		×
policyQualifierId		×
qualifier		×
policyMappings		×
issuerAltName		×
subjectAltName		×
basicConstraints	TRUE	○
cA		TRUE
pathLenConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		c=JP(Printable), o=DIACERT-PLUS CA(UTF8), ou= DIACERT-PLUS Service(UTF8), cn=ARL(UTF8)
distributionPoint		○

uniformResource Identifier		http://www.diacert.jp/plus/rlist/arl.crl
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		×

表 A-3 リンク証明書(OldWithNew)プロファイル

領域名	クリティカルフラグ	規定内容と設定値(○:設定する、×:設定しない)
基本部		
version		2(v3)
serialNumber		1(例)
signature		1.2.840.113549.1.1.11(sha256WithRSAEncryption)
validity		○
notBefore		OldWithOld の validity.notBefore(UTCTime で設定)
notAfter		OldWithOld の validity.notAfter(UTCTime で設定)
issuer		c=JP(Printable), o=DIACERT-PLUS CA(UTF8), ou=DIACERT-PLUS Service(UTF8)
subject		c=JP(Printable), o=DIACERT-PLUS CA(UTF8), ou=DIACERT-PLUS Service(UTF8)
subjectPublicKeyInfo		○
algorithm		1 2 840 113549 1 1 1(rsaEncryption)
subjectPublicKey		RSA 公開鍵値(2048bit)
issuerUniqueID		×
subjectUniqueID		×
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		NewWithNew の公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		NewWithNew の issuer の DN
authorityCertSerial		NewWithNew の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		本証明書の公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
keyCertSign		○
cRLSign		○
extendedKeyUsage		×
privateKeyUsagePeriod		×
certificatePolicies	FALSE	○
policyIdentifier		○
certPolicyId		2 5 29 32 0(any-policy)
policyQualifiers		×
policyQualifierId		×
qualifier		×
policyMappings		×
issuerAltName		×
subjectAltName		×
basicConstraints	TRUE	○
cA		TRUE
pathLenConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		c=JP(Printable), o=DIACERT-PLUS CA(UTF8), ou=DIACERT-PLUS Service(UTF8), cn=ARL(UTF8)
distributionPoint		○

	uniformResource Identifier		http://www.diacert.jp/plus/rlist/arl.crl
subjectDirectoryAttr			×
authorityInfoAccess			×
独自拡張領域			×

表 A-4 相互認証証明書プロファイル

領域名	クリティカルフラグ	規定内容と設定値（○：設定する、×：設定しない）
基本部		
version		2(v3)
serialNumber		1（例）
signature		1.2.840.113549.1.1.11(sha256WithRSAEncryption)
validity		○
notBefore		有効期間を 5 年間に設定（UTCTime で設定する）
notAfter		
issuer		c=JP(Printable), o= DIACERT-PLUS CA（UTF8）, ou= DIACERT-PLUS Service（UTF8）
subject		BCA から指定された DN
subjectPublicKeyInfo		○
algorithm		1 2 840 113549 1 1 1(rsaEncryption)
subjectPublicKey		RSA 公開鍵値(2048bit)
issuerUniqueID		×
subjectUniqueID		×
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		issuer の DN
authorityCertSerial		CA 証明書の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		本証明書の公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
keyCertSign		○
cRLSign		○
extendedKeyUsage		×
privateKeyUsagePeriod		×
certificatePolicies	TRUE	○
policyIdentifier		○
certPolicyId		1 2 392 200127 10 1 1
policyQualifiers		○
policyQualifierId		1 3 6 1 5 5 7 2 1(id-qt-cps)
qualifier		http://www.diacert.jp/plus/（IA5）
policyIdentifier		○
certPolicyId		1 2 392 200127 10 1 2
policyQualifiers		○
policyQualifierId		1 3 6 1 5 5 7 2 1(id-qt-cps)
qualifier		http://www.diacert.jp/plus/（IA5）
policyMappings	TRUE	○
issuerDomainPolicy		1 2 392 200127 10 1 1
subjectDomainPolicy		BCA 側の OID(SHA-256)

issuerDomainPolicy		1 2 392 200127 10 1 2(GPKI 用)
subjectDomainPolicy		BCA 側の OID(SHA-1)
issuerAltName		×
subjectAltName		×
basicConstraints	TRUE	○
cA		TRUE
pathLenConstraints		×
nameConstraints		×
policyConstraints	TRUE	○
requireExplicitPolicy		0
inhibitPolicyMapping		1
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		c=JP(Printable), o= DIACERT-PLUS CA (UTF8), ou=DIACERT-PLUS Service(UTF8), cn=ARL(UTF8)
distributionPoint		○
uniformResourceIdentifier		http://www.diacert.jp/plus/rlist/arl.crl
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		×

表 A-5 利用者証明書プロファイル

領域名	クリティカルフラグ	規定内容と設定値（○：設定する、×：設定しない）
基本部		
version		2(v3)
serialNumber		1001（例）
signature		1.2.840.113549.1.1.11(sha256WithRSAEncryption)
validity		○
notBefore		有効期間は 1 年、2 年、3 年、4 年 10 ヶ月のいずれかを設定（UTCTime で設定する）
notAfter		
issuer		c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）
subject		c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）, （例） st=Tokyo（UTF8）, （例） l=Minato-ku, Shibaura 4-16-36（UTF8）, （例） ou=D130921P000001（UTF8）, （例） cn=Taro Nippon（UTF8） ＊2017 年 8 月 1 日以降に発行する利用者電子証明書の「st」、「l」については利用者が利用申込書の利用者住所の記載を希望した場合のみ記載する。
subjectPublicKeyInfo		○
algorithm		1 2 840 113549 1 1 1(rsaEncryption)
subjectPublicKey		RSA 公開鍵値(2048bit)
issuerUniqueID		×
subjectUniqueID		×
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）
authorityCertSerial		CA 証明書の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		本証明書の公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
digitalSignature		○
nonRepudiation		○
extendedKeyUsage		×
privateKeyUsagePeriod		×
certificatePolicies	TRUE	○
policyIdentifier		○
certPolicyId		1 2 392 200127 10 1 1
policyQualifiers		○
policyQualifierId		1 3 6 1 5 5 7 2 1(id-qt-cps)
qualifier		http://www.diacert.jp/plus/（IA5）
policyMappings		×
issuerAltName	FALSE	○
directoryName		c=JP(Printable), o=DIACERT-PLUS 認証局（UTF8）, ou=DIACERT-PLUS サービス（UTF8）
subjectAltName	FALSE	○

directoryName		c=JP(Printable), (例) st(s)=東京都(UTF8), (例) l=港区芝浦4丁目16番36号(UTF8), (例) o=ジャパンネット株式会社(UTF8), (例) OID.2.5.4.97=JCN7010001003845(UTF8), (例) cn=日本　太郎(UTF8) ＊利用者の所属する企業等が、商業登記されていない個人事業主の場合には「c」、「cn」以外については記載しない。 ＊「OID.2.5.4.97」の記載は 2017 年 5 年 22 日以降に受領した利用申込みを対象とする。
basicConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		
directoryName		c=JP(Printable), o=DIACERT-PLUS CA(UTF8), ou=DIACERT-PLUS Service(UTF8), cn=CRL(UTF8)
distributionPoint		○
uniformResourceIdentifier		http://www.diacert.jp/plus/rlist/crl.crl
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		×

別紙 2. CRL/ARL/fullCRL プロファイル

表 B-1 に、CRL プロファイル、表 B-2 に、 ARL プロファイル、表 B-3 に fullCRL プロファイルをそれぞれ示す。

表 B-1 CRL プロファイル

領域名	クリティカルフラグ	規定内容と設定値（○：設定する、×：設定しない）
CRL 基本部		
version		1（v2）
signature		1.2.840.113549.1.1.11(sha256WithRSAEncryption)
issuer		c=JP(Printable), o=DIACERT-PLUS CA（UTF8） ou=DIACERT-PLUS Service（UTF8）
thisUpdate		CRL 発行日時（UTCTime で設定する）
nextUpdate		thisUpdate + 48 時間（UTCTime で設定する）
revokedCertificates		○
userCertificate		利用者証明書の serialNumber
revocationDate		失効日時（UTCTime で設定する）
crlEntryExtentions		○
reasonCode	FALSE	RFC5280 で定義される理由コード （本認証局では下記を使用する。） 1：秘密鍵の危殆化 2：CA 秘密鍵の危殆化 3：記載事項変更による証明書失効 5：利用の中止
CRL 拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		c=JP(Printable), o=DIACERT-PLUS CA（UTF8） ou=DIACERT-PLUS Service（UTF8）
authorityCertSerial		CA 証明書の serialNumber
cRLNumber	FALSE	本 CRL のシリアル番号
issuingDistributionPoint	TRUE	○
distributionPoint		c=JP(Printable), o=DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）, cn=CRL（UTF8）
onlyContainsUserCerts		TRUE

表 B-2 ARL プロファイル

領域名	クリティカルフラグ	規定内容と設定値（○：設定する、×：設定しない）
CRL 基本部		
Version		1（v2）
Signature		1.2.840.113549.1.1.11(sha256WithRSAEncryption)
Issuer		c=JP(Printable), o=DIACERT-PLUS CA（UTF8） ou=DIACERT-PLUS Service（UTF8）
thisUpdate		ARL 発行日時（UTCTime で設定する）
nextUpdate		thisUpdate + 48 時間（UTCTime で設定する）
revokedCertificates		○
userCertificate		証明書の serialNumber
revocationDate		失効日時（UTCTime で設定する）
crlEntryExtentions		○
reasonCode	FALSE	RFC5280 で定義される理由コード （本認証局では下記を使用する。） 1：秘密鍵の危殆化 2：CA 秘密鍵の危殆化 3：記載事項変更による証明書失効 5：利用の中止
CRL 拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		c=JP(Printable), o=DIACERT-PLUS CA（UTF8） ou=DIACERT-PLUS Service（UTF8）
authorityCertSerial		CA 証明書の serialNumber
cRLNumber	FALSE	本 ARL のシリアル番号
issuingDistributionPoint	TRUE	○
distributionPoint		c=JP(Printable), o= DIACERT-PLUS CA（UTF8）, ou=DIACERT-PLUS Service（UTF8）, cn=ARL（UTF8）
onlyContainsCACerts		TRUE

表 B-3 fullCRL プロファイル

領域名	クリティカルフラグ	規定内容と設定値（○：設定する、×：設定しない）
CRL 基本部		
version		1（v2）
signature		1.2.840.113549.1.1.11(sha256WithRSAEncryption)
issuer		c=JP(Printable), o=DIACERT-PLUS CA（UTF8） ou=DIACERT-PLUS Service（UTF8）
thisUpdate		fullCRL 発行日時（UTCTime で設定する）
nextUpdate		thisUpdate + 48 時間（UTCTime で設定する）
revokedCertificates		○
userCertificate		証明書の serialNumber
revocationDate		失効日時（UTCTime で設定する）
crlEntryExtentions		○
reasonCode	FALSE	RFC5280 で定義される理由コード （本認証局では下記を使用する。） 1：秘密鍵の危殆化 2：CA 秘密鍵の危殆化 3：記載事項変更による証明書失効 5：利用の中止
CRL 拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		c=JP(Printable), o=DIACERT-PLUS CA（UTF8） ou=DIACERT-PLUS Service（UTF8）
authorityCertSerial		CA 証明書の serialNumber
cRLNumber	FALSE	本 fullCRL のシリアル番号
issuingDistributionPoint	TRUE	×
distributionPoint		×
onlyContainsUserCerts		×

別紙 3. 事業を営んでいることを証明する書類

subjectAltName に含まれる利用者の所属する企業等が商業登記されていない個人事業主の場合、下記 「表 D-1 事業を営んでいることを証明する書類」に示す書類のいずれか1つにより、組織の確認を行なう。

表 D-1 事業を営んでいることを証明する書類

No	書類名	有効期限
1	青色又は白色申告書のコピー	直近年のもの
2	個人事業の開廃業等届出書のコピー	直近のもの
3	所得税の青色申告承認申請書のコピー	直近年のもの
4	建設業の許可申請書または通知のコピー	直近のもの
5	測量業者登録申請書または通知のコピー	直近のもの
6	建築士事務所登録申請書または通知のコピー	直近のもの
7	(産業廃棄物および一般廃棄物) 収集運搬業許可申請書または通知のコピー	直近のもの
8	(産業廃棄物および一般廃棄物) 処分(処理)業許可申請書または通知のコピー	直近のもの
9	貨物自動車運送事業許可申請書または通知のコピー	直近のもの
10	貨物運送取扱事業許可申請書または通知のコピー	直近のもの
11	一般旅客自動車運送事業許可申請書または許可証のコピー	直近のもの
12	特定旅客自動車運送事業許可申請書または許可証のコピー	直近のもの
13	登録証明書等(測量業者登録証明書、建設コンサルタント現況報告書、地質調査業者現況報告書、補償コンサルタント現況報告書、建築士事務所登録証明書、土地家屋調査士登録証明書、計量証明事業者登録証明書、不動産鑑定業者登録証明書、司法書士登録証明書)のコピー	直近のもの
14	納税証明書のコピー	直近年のもの
15	経営規模等評価結果通知書・総合評定値通知書のコピー	直近のもの
16	その他、公的機関またはこれに準ずる機関の印の付いた証明書、許可証等のコピー	直近のもの