「AOSign サービス運用規程(AOSign 認証局編)」

AOSign Service Certificate Policy And Certification Practice Statement
(AOSign Certification Authority Version)

Ver2.00

日本電子認証株式会社
Nippon Denshi Ninsho Co.,Ltd.

制定日：2013.12.24
改訂日：2018.03.19

目　次

目　次 **2**

1　はじめに **6**

1.1　改訂履歴 6
1.2　概要 7
1.3　正式名称 7
1.3.1　認証業務の名称 *8*
1.3.2　規程の名称 *8*
1.3.3　認証局の名称 *8*
1.4　コミュニティと適応可能性 8
1.4.1　登場者と機能に応じた相関関係 *8*
1.4.2　認証業務の形態 *8*
1.4.3　電子証明書の用途範囲 *8*
1.4.4　業務運用関連法令に対する遵法精神 *8*
1.4.5　電子署名法の認定対象外事項の証明に対する宣言 *8*
1.5　連絡先の詳細 8

2　一般的な規定 **9**

2.1　義務 9
2.1.1　発行局(IA)の義務 *9*
2.1.2　登録局(RA)の義務 *9*
2.1.3　利用者の義務 *9*
2.1.4　利用者の所属する企業等の義務 *9*
2.1.5　検証者の義務 *9*
2.1.6　リポジトリの義務 *9*
2.2　責任 9
2.3　財務責任 9
2.3.1　賠償責任 *9*
2.3.2　信頼関係 *9*
2.3.3　会計原則 *9*
2.4　解釈および執行 9
2.4.1　準拠法 *9*
2.4.2　分離、存続、合併、通知 *9*
2.4.3　紛争解決手続 *9*
2.5　料金 9
2.6　公開およびリポジトリ 9
2.6.1　情報の公開 *9*
2.6.2　公開の頻度 *9*
2.6.3　アクセスコントロール *9*
2.6.4　リポジトリ *9*
2.7　準拠性監査 9

2.7.1 監査の頻度 9
2.7.2 監査人の身元保証・資格 9
2.7.3 被監査部門と監査人の関係 9
2.7.4 監査の対象となるトピック 9
2.7.5 監査指摘事項に対する措置 9
2.7.6 監査結果の報告 9
2.8 秘密保持 9
2.8.1 秘密が保たれる情報 9
2.8.2 秘密とみなされない情報 9
2.8.3 失効情報の公開 10
2.8.4 捜査機関等への開示 10
2.8.5 民事手続上の開示 10
2.8.6 電子証明書名義人の要請に基づく開示 10
2.8.7 委託先への情報の開示 10
2.9 知的財産権 10
2.10 個人情報保護 10
2.11 詳細規定 10
3 識別と本人認証 11
3.1 初期登録(発行申込) 11
3.1.1 電子証明書に記載される利用者情報 11
3.1.2 名称の意味に関する要件 11
3.1.3 名称の一意性 12
3.1.4 名称要求の紛争決着の手順 12
3.1.5 企業等の名称の認識・認証・役割 12
3.1.6 秘密鍵の所有を証明する方法 12
3.1.7 発行申込権者および発行申込時に必要な書類 12
3.1.8 利用者の真偽の確認 15
3.1.9 企業等の商号・名称、住所、代表者および法人番号の確認 16
3.1.10 企業等に所属していることの確認 16
3.1.11 受取代理人の真偽の確認 16
3.2 電子証明書の継続に伴う鍵の更新 17
3.3 失効後の電子証明書の鍵の更新 17
3.4 失効申込・失効届出 17
3.4.1 失効申込権者・失効届出権者 17
3.4.2 失効申込者・失効届出者の真偽の確認 17
4 運用の要件 19
4.1 電子証明書の発行申込 19
4.1.1 発行申込のパターン 19
4.1.2 発行申込の受付 19
4.1.3 発行申込の審査 19
4.2 電子証明書の発行 20
4.2.1 電子証明書記載事項の登録 20

4.2.2 電子証明書の発行指示 21
4.2.3 鍵ペアの生成と電子証明書の作成 21
4.2.4 電子証明書および秘密鍵の IC カードへの格納等 21
4.2.5 BCA に対する相互認証証明書の発行 21
4.3 IC カード(電子証明書および秘密鍵)および PIN の受領 21
4.4 電子証明書の失効 23
4.4.1 利用者の申込による失効 23
4.4.2 本認証局の判断に基づく失効 23
4.4.3 失効申込・失効届出のパターン 24
4.4.4 失効申込・失効届出の審査 24
4.4.5 失効データの登録および失効 25
4.4.6 失効申込者・失効届出者への通知 25
4.5 電子証明書失効リスト(CRL/ARL) 25
4.5.1 CRL の更新周期 25
4.5.2 相互認証証明書の失効 25
4.6 セキュリティ監査手続 25
4.7 アーカイブ 26
4.7.1 紙で保存する書類 26
4.7.2 デジタルデータとしてアーカイブする情報 27
4.8 鍵の更新 28
4.9 危殆化と災害からの回復 28
4.10 本認証局の終了(認証業務の終了) 29
5 物理的、手続的、人的なセキュリティ管理 30
5.1 物理的セキュリティ管理 30
5.2 手続的セキュリティ管理 30
5.3 人的セキュリティ管理 30
6 技術的なセキュリティ管理 31
6.1 鍵ペアの生成と組み込み 31
6.1.1 認証局(自己署名 CA) 31
6.1.2 利用者 31
6.2 電子証明書署名鍵(秘密鍵)の保護 31
6.2.1 暗号化装置標準 31
6.2.2 電子証明書署名鍵の複数人制御 31
6.2.3 電子証明書署名鍵のエスクロウ 31
6.2.4 電子証明書署名鍵のバックアップ 31
6.2.5 電子証明書署名鍵のアーカイブ 31
6.2.6 電子証明書署名鍵の暗号化装置へのエントリ(バックアップリカバリ) 31
6.2.7 電子証明書署名鍵を活性化させる方法 31
6.2.8 電子証明書署名鍵を非活性化させる方法 31
6.2.9 電子証明書署名鍵を破壊する方法 31
6.3 鍵ペア管理のその他の面 31
6.3.1 公開鍵のアーカイブ 31

6.3.2 公開鍵と秘密鍵の使用期間 31
6.3.3 CA 属性を持つ電子証明書の有効期間 31
6.4 活性化データ 31
6.4.1 活性化データの生成と組み込み 31
6.4.2 活性化データの保護 31
6.5 コンピュータのセキュリティ管理 31
6.6 ライフサイクルの技術的な管理 31
6.6.1 システム開発の管理 31
6.6.2 セキュリティマネジメント管理 31
6.7 ネットワークのセキュリティ管理 31
6.8 暗号化装置の技術的管理 31

7 電子証明書ならびに CRL/ARL プロファイル 32

7.1 電子証明書プロファイル 32
7.1.1 バージョン番号 32
7.1.2 電子証明書拡張部 32
7.1.3 アルゴリズム OID 32
7.1.4 名称形式 32
7.1.5 名称制約 32
7.1.6 電子証明書ポリシーOID 32
7.1.7 ポリシー制約(policyConstraints)拡張の使用 32
7.1.8 ポリシー修飾子(policyQualifiers) 32
7.1.9 電子証明書プロファイル 32
7.2 CRL/ARL プロファイル 42
7.2.1 バージョン番号 42
7.2.2 CRL/ARL エントリ拡張 42
7.2.3 CRL/ARL プロファイル 42

8 仕様管理 45

8.1 仕様変更の手続きに関するポリシー 45
8.2 公表および通知に関するポリシー 45
8.3 仕様認可の手続き 45
8.4 CPS の保存 45

1　はじめに

1.1　改訂履歴

改訂履歴を表 1-1 に示す。

表 1-1 改訂履歴

Ver.	日付	改版内容
1.00	2013.12.24	・初版発行
1.10	2014.02.25	・表現および誤記の修正 ・利用者が使用できる署名アルゴリズムについて追記
1.11	2014.03.24	・表現の統一
1.12	2014.04.10	・認証業務規程の構成変更に伴う修正
1.20	2014.10.08	・本認証業務の受付停止を追記
1.21	2015.03.23	・表現および誤記の修正
1.30	2015.11.20	・利用者を確認するための書類について追記
1.31	2016.03.22	・表現および誤記の修正
1.40	2016.11.01	・電子証明書の有効期間の追加に伴う修正
1.50	2017.02.06	・電子証明書に記載する法人番号について追記
1.60	2017.07.07	・誤記の修正
1.70	2017.10.27	・企業等に関する情報を確認するための書類について追記
2.00	2018.03.19	・失効に係る手続きについて追記 ・表現および誤記の修正

1.2 概要

(1) 日本電子認証株式会社(以下、「NDN」という。)は、AOSign 認証局(以下、「本認証局」という。)の認証業務として AOSign サービス(以下、「本認証業務」という。)を提供する。本認証業務は、NDN の電子認証サービスである「AOSign サービス」に属する認証業務の一つである。

(2) 本認証業務は、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。)第 2 条第 3 項に規定する特定認証業務であり、同法第 4 条第 1 項に基づき主務大臣の認定を受けている。ただし、本認証業務の内容には、電子署名法の認定対象外事項として、利用者が企業等に所属していることおよび企業等の属性情報を確認する部分も含まれている。

(3) 本認証業務における利用者は、主に企業等に所属している個人を対象としている。これは、本認証業務が、企業等の組織に所属する個人がその代表者として、あるいは代表者から権限の委任を受けて取引を行う場合に利用されることを想定していることによっている。そのため、本認証業務を利用しようとする個人は、所属する企業等の同意を得て申込みを行う。

(4) NDN は、本認証業務の適正な運営を行うため AOSign サービス運用規程(以下、「共通 CPS」という。)1.2 節(5)に規定する認証業務ごとに定める運用規程として AOSign サービス運用規程(AOSign 認証局編)(以下、「本 CPS」という。)を定めて公開する。同一の条項において、共通 CPS および本 CPS それぞれに記述がある場合、両方の記述に従う。

(5) 本認証業務で発行する電子証明書を利用する者は、共通 CPS および本 CPS のすべての条項に同意しなくてはならない。また、利用者および利用者の所属する企業等は、共通 CPS1.2 節(6)に規定する認証業務ごとに定める利用規約のうち AOSign サービス利用規約(以下、「利用規約」という。)に、電子証明書を受信する検証者は、共通 CPS1.2 節(6)に規定する認証業務ごとに定める検証者同意書のうち AOSign サービス検証者同意書(以下、「検証者同意書」という。)に同意しなくてはならない。

(6) 本 CPS の構成は、IETF(Internet Engineering Task Force)の Public-Key Infrastructure(X.509)Working Group が提唱する「電子証明書ポリシーと認証実践の枠組み(Certificate Policy and Certification Practices Framework)」(RFC 2527)を参考としている。

1.3 正式名称

本認証業務に割り当てたオブジェクト識別子(OID)を表 1-2 に示す。

表 1-2 OID とオブジェクトの対応表

OID	オブジェクト
1.2.392.200122.1.1	AOSign Service CPS
1.2.392.200122.1.2	AOSign Service Policy for certificates

1.2.392.200122.1.3	AOSign Service Policy for cross-certificate between BCA
1.2.392.200122.1.4	AOSign Service Policy for cross-certificate between BCA while testing
1.2.392.200122.1.50	AOSign Service Common CPS

1.3.1　認証業務の名称

本認証業務の正式名称は、「AOSign サービス」(AOSign Service)と称する。

1.3.2　規程の名称

本 CPS の正式名称は、「AOSign サービス運用規程(AOSign 認証局編)」(AOSign Service Certificate Policy And Certification Practice Statement(AOSign Certification Authority Version))と称する。

1.3.3　認証局の名称

本認証局の正式名称は、「AOSign 認証局」(AOSign Certification Authority)と称する。

1.4　コミュニティと適応可能性

以下の条項について、本 CPS1.2 節(4)に示す共通 CPS に規定する。

1.4.1　登場者と機能に応じた相関関係
1.4.2　認証業務の形態
1.4.3　電子証明書の用途範囲
1.4.4　業務運用関連法令に対する遵法精神
1.4.5　電子署名法の認定対象外事項の証明に対する宣言

1.5　連絡先の詳細

本 CPS1.2 節(4)に示す共通 CPS に規定する。

2　一般的な規定

以下の条項について、本 CPS1.2 節(4)に示す共通 CPS に規定する。

2.1　義務

2.1.1　発行局(IA)の義務
2.1.2　登録局(RA)の義務
2.1.3　利用者の義務
2.1.4　利用者の所属する企業等の義務
2.1.5　検証者の義務
2.1.6　リポジトリの義務

2.2　責任

2.3　財務責任

2.3.1　賠償責任
2.3.2　信頼関係
2.3.3　会計原則

2.4　解釈および執行

2.4.1　準拠法
2.4.2　分離、存続、合併、通知
2.4.3　紛争解決手続

2.5　料金

2.6　公開およびリポジトリ

2.6.1　情報の公開
2.6.2　公開の頻度
2.6.3　アクセスコントロール
2.6.4　リポジトリ

2.7　準拠性監査

2.7.1　監査の頻度
2.7.2　監査人の身元保証・資格
2.7.3　被監査部門と監査人の関係
2.7.4　監査の対象となるトピック
2.7.5　監査指摘事項に対する措置
2.7.6　監査結果の報告

2.8　秘密保持

2.8.1　秘密が保たれる情報
2.8.2　秘密とみなされない情報

2.8.3　失効情報の公開
2.8.4　捜査機関等への開示
2.8.5　民事手続上の開示
2.8.6　電子証明書名義人の要請に基づく開示
2.8.7　委託先への情報の開示
2.9　知的財産権
2.10　個人情報保護
2.11　詳細規定

3　識別と本人認証

3.1　初期登録(発行申込)

3.1.1　電子証明書に記載される利用者情報

本認証業務で使用する名称は、ITU X.500 シリーズ定義の識別名(DistinguishedName)の規定に従い指定される(詳細は本 CPS7 章を参照)。所有者別名(subjectAltName)の詳細については本 CPS7 章を参照のこと。

以下に、本認証業務における電子証明書に記載される所有者(subject)の識別名(DistinguishedName)の種類と取扱を定める。

なお、本認証業務で発行される電子証明書の記述に使用する言語は、英数字および日本語である。

(1) 国名(本 CPS7 章プロファイル表示: C=JP　CountryName のこと)
利用者の居住する国名である。「JP」(日本国)固定である。

(2) 住所 1: 都道府県(本 CPS7 章プロファイル表示: S=XXX　stateOrProvinceName のこと)
利用者の居住する住所の都道府県名をヘボン式ローマ字で指定する。
なお、本名称の確認は電子署名法の認定対象である。

(3) 住所 2: 郡、市区町村以下(本 CPS7 章プロファイル表示: L=XXX　localityName のこと)
利用者の居住する住所の郡、市区町村名以下をヘボン式ローマ字で指定する。
なお、本名称の確認は電子署名法の認定対象である。

(4) 固有名称(本 CPS7 章プロファイル表示: CN=XXX　CommonName のこと)
利用者の呼称(フリガナ)を、ヘボン式ローマ字で指定する。ただし、ヘボン式ローマ字にて記載しがたい場合は、発行申込書に記載されている呼称のローマ字表記をそのまま記載するが、呼称との大幅な乖離(例えば、ニックネーム)は許されない(旧姓および住民票の写しまたは住民票記載事項証明書記載の通称等は、この固有名称に設定可能である。)。
なお、本名称の確認は電子署名法の認定対象である。

(5) 利用者識別子(本 CPS7 章プロファイル表示: UID　UserIdentifier のこと)
利用者に配付した IC カードの識別番号である。本認証局にて割り当てを行う。

ただし、利用者より電子調達、電子申請、電子商取引、電子文書保存のアプリケーションごとに指定される電子証明書要件に基づき、上記(2)住所 1 および(3)住所 2 について電子証明書に記載しないことの申し出があった場合は両住所とも電子証明書に記載しない。

3.1.2　名称の意味に関する要件

本認証業務で使用する識別名には、本 CPS3.1.1 項で規定した種類とそれに対応する意味があり、さまざまな名称の形式を解釈するためのルールは、前述の ITU X.500 シリーズ定義の識別名の規定および GPKI 相互運用性仕様書に規定される電子証明書プロファイルに従うものである。

なお、電子証明書に記載される識別名は、本認証局が本人性確認の際に利用者から提

出された発行申込書に記載されている内容から国名および利用者識別子を除き転記したものである(詳細は本 CPS7 章を参照)。

3.1.3　名称の一意性

電子証明書に記載される識別名は、本認証業務で発行する電子証明書において利用者に対し一意である。

3.1.4　名称要求の紛争決着の手順

名称要求の紛争とは、本認証業務で発行する電子証明書に記載される利用者の識別名に係る何らかの紛争を意味する(不正発行、商標権侵害、不正競争、不正目的使用等)。

利用者の固有名称(CommonName)および利用者ローマ字表記住所 1、2(stateOrProvinceName、localityName)に係る紛争(不正発行)は本認証局と利用者間での解決を原則とする。

3.1.5　企業等の名称の認識・認証・役割

本認証業務で発行する電子証明書における所有者別名(subjectAltName)は、企業等の名称を含む。

本認証業務では、利用者の所属する企業等の名称を本 CPS3.1.7 項(5)の書類(登記事項証明書等)で確認する。

3.1.6　秘密鍵の所有を証明する方法

(1) 利用者の秘密鍵の証明

本認証業務では、本認証局において公開鍵と秘密鍵を生成し、電子証明書と秘密鍵を IC カードに格納し、これを使用する際に求められる PIN とともに安全かつ確実に利用者に配付する。秘密鍵の格納された IC カードおよび PIN を本人限定受取郵便(基本型)または本認証局が対面にて本人性の確認を行ったうえで手交する方法により確実に配付し、秘密鍵受取および所有の証として利用者の自署(手交の場合のみ)または記名押印(実印)された受領書もしくは IC カードに格納されている秘密鍵にて電子署名を行った受領書データ(以下、「受領書データ」という。)を回収する。

なお、利用者が外国人であって、個人の実印を所有していない場合は、押印欄に利用者が自署を行った受領書または受領書データを回収する。

(2) BCA の秘密鍵の証明

GPKI との相互認証手続において、BCA から提出された電子証明書発行要求の電子署名の検証を行い、含まれている BCA 公開鍵に対応する BCA 秘密鍵で電子署名されていることを確認する。また、電子証明書発行要求のフィンガープリントを確認し、BCA 公開鍵の所有者を特定する。

3.1.7　発行申込権者および発行申込時に必要な書類

発行申込権者は利用者のみとし、代理人による発行申込は認めない。ただし、当社窓口に申込書を持参する者は、利用者以外でも構わない。

利用者は、電子証明書の発行申込にあたり、以下の書類一式を提出する。

(1) 発行申込書

本認証局所定の様式により、利用者の記名押印(実印)されていることを必須とし、以下の事項を含むものとする。

なお、利用者が外国人であって、個人の実印を所有していない場合は、発行申込書の押印欄に、自署が行われていることを必須とする。

- 利用者氏名(旧姓および住民票の写しまたは住民票記載事項証明書記載の通称等を含む。)、住所、生年月日
- 電子証明書の用途(電子調達、電子申請、電子商取引、電子文書保存)
- 利用者氏名のローマ字表記
- 利用者住所のローマ字表記

また、本認証業務では利用者が企業等に所属することを前提に電子証明書を発行する。本申込書には、利用者の所属する企業等が「本申込について同意する」旨の確認条項が明示してあり、企業等の記名押印(企業等代表者印)されていることが必須である。ただし、この取扱は電子署名法の認定対象外である。

なお、本認証局は、押印に使用する印鑑を実印(商業登記のない法人の場合は、当該法人が公的機関に届け出た書類または公的機関が発行した書類(公示を含む。)に押印した印を含む。以下、同じ。)に限り、利用者および企業等の意思表示の証としてこれを求める。

(2) 利用者を確認するための書類

印鑑登録証明書および住民票の写しまたは住民票記載事項証明書(いずれも利用者のもので当社受付時点で発行日から 3 ヶ月以内のもの。また、住民票の写しまたは住民票記載事項証明書については、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年 5 月 31 日法律第 27 号）第 2 条第 5 項に規定する個人番号の記載がないものとするが、当該番号の記載がある場合には、本認証局が墨塗りを行うことに同意する。)を提出する。

なお、利用者が外国人であって、個人の実印を所有していない場合は、印鑑登録証明書の提出は省略可とし、本認証局から本人限定受取郵便(基本型)を用いて送付された発行申込意思確認書を、利用者が自筆署名したうえで提出する。旧姓を利用者の固有名称とする場合、旧姓と現姓の関係を証明する戸籍謄本(戸籍全部事項証明書)または戸籍抄本(戸籍個人事項証明書)を上記の書類に加えて提出する。

(3) 企業等の意思を確認するための書類

この取扱は電子署名法の認定対象外である。

①利用者の所属する企業等が商業登記をしている法人の場合は、当該法人の印鑑証明書(当社受付時点で発行日から 3 ヶ月以内)を提出する。商業登記のない法人の場合は、当該法人が公的機関に届け出た書類または公的機関が発行した書類(公示を含む。)で印影の確認が可能な書類とする。

なお、地方自治法等の特別法に基づく法人については、次の書類とする。

1)当該法人の公印規程(印影つき)。　公印規程に印影のない場合は、公印規程に加え当該法人の発行する公式文書(発番ならびに日付および公印が確認される対外文書(写し可))。

②個人企業の場合は代表者個人の印鑑登録証明書(当社受付時点で発行日から 3 ヶ月以内)を提出する。

(4) 利用者が企業等に所属していることを証明する書類
企業等が、発行申込書に企業等代表者の実印(地方自治法等の特別法に基づく法人の場合は、当該法人の代表者の公印)を押印することにより利用者が当該企業等に所属していることを証明する。
ただし、この取扱は電子署名法の認定対象外である。

(5) 企業等に関する情報を確認するための書類
利用者の所属する企業等および代表者を確認するための書類である。以下の場合において、各書類のうちいずれか一つを提出する。
ただし、この取扱は電子署名法の認定対象外である。
①法人の場合
●商業登記をしている場合は、登記事項証明書(履歴事項全部証明書または現在事項全部証明書)(当社受付時点で発行日から 3 ヶ月以内)
●商業登記のない法人の場合は、当該法人の存在を証明する公的書類
地方自治法等の特別法に基づく法人については、次の書類とする。
1)当該法人を設置する法令
例えば、地方自治法第 4 条の「地方公共団体の位置を定める条例」の制定がある場合は、当該条例の写し。当該条例の制定がない場合は、「部制条例」等の組織を定める規程等の写し。
2)当該団体の代表者氏名が公示されている当該法人発行文書の写し(公報等)
②個人企業の場合
ア)商業登記をしている場合は、登記事項証明書(履歴事項全部証明書または現在事項全部証明書)(当社受付時点で発行日から 3 ヶ月以内)
イ)商業登記をしていない場合は、商号・名称、住所および公的機関またはこれに準ずる機関の印影が確認できる書類(直近年のもの)とする。
例)経営事項審査の結果通知書の写し(国土交通省または都道府県が発行したもの)
例)税務申告書の写し
ただし、電子申告の場合は、『「受信通知」および「申告データ出力分」』を収受日付印のある税務申告書の写しとみなす。
例)国や地方公共団体等との公共工事請負契約書、業務委託契約書の写し

(6) 代理人を確認するための書類
本認証業務は、受取代理人への IC カードの送付または手交を可とする。この場合、利用者は以下の書類を提出する。
①利用者から受取代理人への委任状
提出を求める委任状(本認証局所定の様式)には、利用者が受取代理人に対し IC カードの受取りを委任する旨が記載されている。
当該委任状の利用者氏名および実印は、発行申込書の利用者氏名および実印と合致するものであることを要する。
なお、利用者が外国人であって、個人の実印を所有していない場合は、当該委任状の押印欄に自署されていることを要する。
②受取代理人の印鑑登録証明書
ただし、IC カードの受取りを本人限定受取郵便の代人制度に基づく受取代人とす

る場合には、利用者から利用者氏名、利用者住所、利用者押印(実印)、受取代人氏名、受取代人住所、IC カードの受取について委任する旨の記載があることの要件を満たす委任状(様式不問)の提出を求める。この場合、受取代人の印鑑登録証明書の提出は不要とする。

3.1.8 利用者の真偽の確認

本認証局は、利用者が本人であることの真偽確認を以下の手順で行う。

(1) 発行申込書および添付書類の確認

①発行申込書において以下の同意がなされていること

- ●利用規約に対する同意
- ●利用者情報が電子証明書に記載されることに対する同意

②発行申込書に記名押印(実印)されていること

なお、利用者が外国人であって個人の実印を所有していない場合は、押印欄に自署が行われていること

③添付書類が「様式」、「記載内容」および「有効期限」等において真正な書類であること

(2) 添付書類による利用者の真偽の確認

①真偽の確認にあたっては、発行申込書に記載されている利用者氏名(旧姓および住民票の写しまたは住民票記載事項証明書記載の通称等を含む。)、住所および生年月日が、住民票の写しまたは住民票記載事項証明書、戸籍謄本(戸籍全部事項証明書)、戸籍抄本(戸籍個人事項証明書)に記載されている内容と一致すること。ただし、発行申込書記載の文字と住民票の写しまたは住民票記載事項証明書、戸籍謄本(戸籍全部事項証明書)、戸籍抄本(戸籍個人事項証明書)記載の文字が異なる場合であっても、「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)」等に従い同等と判断できるときは、一致しているものとする。また、発行申込書記載の住所表記の丁目番地等が、ハイフン等で表記されている場合も一致しているものとする。

②電子証明書に記載する利用者氏名および住所のローマ字表記が、日本語呼称(フリガナ)から大きく乖離していないこと

③印鑑登録証明書に証明されている印影と発行申込書に押印された印鑑の印影が一致すること

なお、利用者が外国人であって、個人の実印を所有していない場合は、以下のとおり取扱う。

- ・本認証局は、利用者が申込書記載の住所に居住しているかおよび当該発行申込が利用者本人の申込意思に基づくものであるかを確認するため、発行申込意思確認書を本人限定受取郵便(基本型)にて利用者本人宛に送付する。
- ・発行申込意思確認書を受領した利用者は、当該申込が利用者本人によるものである場合は、同確認書に申込意思を明示し自署の上、本認証局宛に郵送する。
- ・本認証局は、郵送されてきた発行申込意思確認書の受領により利用者の真偽の確認を行い、併せて自署の確認も行う。発行申込意思確認書の発送から 40 日以内に、同確認書が本認証局へ到達しない場合または同確認書により申込意思のないことが確認された場合は、当該申込にかかる利用者の真偽確認は

できなかったものとする。

④旧姓を利用者の固有名称とする申込が行われた場合、旧姓と現姓の関係を証明する戸籍謄本(戸籍全部事項証明書)または戸籍抄本(戸籍個人事項証明書)等の公的書類(当社受付時点で発行日から 3 ヶ月以内)が添付されていること

3.1.9　企業等の商号・名称、住所、代表者および法人番号の確認

(1) 商号・名称、住所、代表者の確認

企業等の商号・名称、住所および代表者の確認は、本 CPS3.1.7 項(5)の書類(登記事項証明書等)によって行う。

当該確認書類については、「様式」、「記載内容」および「有効期限」等において真正な書類であることを確認のうえ、発行申込書の記載内容が同書類に一致していることを確認する。ただし、企業等の商号・名称について、「株式会社」等を「(株)」等に省略して表記されている場合も一致しているものする。

また、発行申込書記載の文字と本 CPS3.1.7 項(5)の書類(登記事項証明書等)に記載の文字が異なる場合は、本CPS3.1.8項(2)①ただし書きに準ずるものとする。

なお、市町村合併等によって企業等の住所変更が行われた場合に、本 CPS3.1.7 項(5)の書類(登記事項証明書等)が合併前の住所であるときには、企業等住所の確認ができないため、市町村役場から発行される合併証明書等または新住所が表記されている印鑑証明書など合併後の新住所を確認できる書類を求め、企業等の住所を確認する。

(2) 法人番号の確認

会社法その他の法令の規定により設立の登記をした法人においては、登記事項証明書に記載された会社法人等番号を基礎とし財務省令で定められた算式によって算出することにより確認する。それ以外の法人等においては、「国税庁法人番号公表サイト」を参照することにより確認する。

3.1.10　企業等に所属していることの確認

本認証業務では、利用者が企業等に所属しているという確認は、発行申込書に企業等代表者の実印が押印されていることおよび印影を確認することにより行う。ただし、この取扱は電子署名法の認定対象外である。

3.1.11　受取代理人の真偽の確認

本認証業務では、受取代理人の真偽の確認および利用者から委任を受けていることの確認を受取代理人の印鑑登録証明書および委任状により行う。

当該確認は、「様式」、「記載内容」、「有効期限」等において真正な書類であることを確認した上で、以下の通り行う。

受取代理人の真偽の確認は、委任状に記載された受取代理人の情報および押印された印鑑の印影が受取代理人の印鑑登録証明書の情報および印鑑の印影と一致することを確認することによる。

利用者から IC カードの受取りに係る委任を受けていることの確認は、委任状の利用者本人の氏名を確認するとともに利用者の印鑑登録証明書に証明されている印影と委任状に押印された利用者の印鑑の印影が一致することを確認することによる。

3.2　電子証明書の継続に伴う鍵の更新

電子証明書の有効期間満了にともなう発行申込(本認証局が既申込情報を利用し印字、送付した電子証明書発行申込書によるものを含む。)は、初期登録に同じ手続を取る。

3.3　失効後の電子証明書の鍵の更新

電子証明書の失効後の発行申込は、一度失効した電子証明書を再度有効化するものではなく、初期登録に同じ手続を取る。

なお、本認証局は、前回失効事由が当該発行に適切でないと判断する場合は発行申込を受付けない。

3.4　失効申込・失効届出

電子証明書の失効申込または失効届出受付、受付内容の確認(失効申込者または失効届出者の真偽の確認を含む。)、失効審査および失効操作は、本認証局が行う。

3.4.1　失効申込権者・失効届出権者

失効申込権者は利用者のみとする。

失効届出権者は利用者の所属する企業等とする。利用者の死亡または利用者の所属する企業等の倒産等やむを得ない場合は、例外的に、第三者が届出を行うことも可能とする。

3.4.2　失効申込者・失効届出者の真偽の確認

本認証局は、原則として失効申込書の内容(利用者の氏名および印影)が当該電子証明書の発行申込書と一致する場合に、利用者の失効申込と判断する。

失効申込書に記載されている利用者氏名が改名等により電子証明書発行申込書に記載された利用者氏名と異なる場合は、戸籍謄本(戸籍全部事項証明書)または戸籍抄本(戸籍個人事項証明書)を求め、利用者氏名の一致を確認する。また、失効申込書に押印されている印影が電子証明書発行申込書に押印された印影と異なる場合は、本 CPS3.1.7 項(2)の印鑑登録証明書を求め、印影の一致を確認する。ただし、最新の発行申込時 (AOSignG2 認証局分を含む。)に添付された書類により確認する場合には、重複提出は求めない。

利用者が外国人であって、個人の実印を所有していない場合、本 CPS3.1.8 項(2)③なお書きに準じ、失効申込意思確認書を本人限定受取郵便(基本型)により送付することにより取り扱う。

本認証局は、原則として失効届出書の内容(企業等の名称ならびに代表者氏名および印影)が当該電子証明書の発行申込書と一致する場合に、企業等からの失効届出と判断する。

失効届出書に記載されている企業等名称、代表者氏名が電子証明書発行申込書に記載された内容と異なる場合は、本 CPS3.1.7 項(5)の書類(登記事項証明書等)を求め、企業等名称、代表者氏名の一致を確認する。また、失効届出書に押印されている印影が電子証明書発行申込書に押印された印影と異なる場合は、本 CPS3.1.7 項(3)の印鑑証明書等を求め、印影の一致を確認する。ただし、最新の発行申込時(AOSignG2 認証局分を含む。)

に添付された書類により確認する場合には、重複提出を求めない。
　なお、第三者の失効届出の場合は失効届出者の確認を要しない。ただし、失効事由(本人死亡、企業等の倒産等)を明らかとする公的証明書等の添付を要する。

4　運用の要件

4.1　電子証明書の発行申込

本認証局は、あらかじめ利用者に共通 CPS、本 CPS、利用規約、発行申込書および申込に必要な関係書類等をホームページ(共通 CPS、本 CPS および利用規約はリポジトリ)にて公開する。利用者は、共通 CPS、本 CPS、利用規約および個人情報の取扱(利用者氏名(ローマ字、漢字)、利用者自宅住所(ローマ字)、企業等商号・名称(漢字)、企業等の本店住所(漢字)、法人番号の項目について、電子証明書に記載されること)に同意し、かつ企業等の同意を得て申込む。利用者または企業等が同意できない場合は、申込手続を中止しなければならない。

なお、GPKI との相互認証手続において、BCA から本認証局への相互認証証明書の発行要求および本認証局から BCA への相互認証証明書発行申請は、BCA の定める手続により行われる。

本認証業務の発行申込受付は、平成 26 年 10 月 8 日以降停止する。

4.1.1　発行申込のパターン

発行申込は、郵送申込および対面申込とし、他の方法は認めない。

利用者は、申込にあたり、発行申込書の記載内容および添付書類に不備のないことを確認し、利用者および企業等代表者の記名押印(実印)のうえ、本認証局へ申込む。

なお、利用者が外国人であって、個人の実印を所有していない場合は、発行申込書の押印欄への自署のうえ、本認証局に申込む。

4.1.2　発行申込の受付

(1) 郵送申込

業務運用者は、発行申込書類(添付書類を含む。)が封緘された郵便物を開封した時点で受付ける。

(2) 対面申込

当社窓口での対面申込は、業務運用者が 2 名体制で、発行申込書類(添付書類を含む。)を受理した時点で受付ける。

当社窓口以外での対面申込は、業務運用者が 2 名体制で、封緘された発行申込書類(添付書類を含む。)を受理し、開封することなく鞄等に入れ施錠後、常時携帯し当社まで搬送し、開封した時点で受付ける。

4.1.3　発行申込の審査

業務運用者は、受付けた発行申込書類(添付書類を含む。)に対し、本 CPS3.1.8 項～3.1.11 項に規定する手続を行う。審査の結果、不備がある場合は、利用者に対し「書類不備のお知らせ」を送付し、郵送にて書類の再提出または追加提出を求める。

なお、利用者が、不備のある申込書類または不要な添付書類等の返却を希望する場合には返却することができる。この場合、利用者は、電子証明書発行申込書において指定された連絡先経由で利用者に必要な連絡をすることおよび必要な書類を送付することに同意しなければならない。ただし、本認証局が不正な申込であると判断した場合には返却はしない。再提出または追加提出後は、提出された当該申込書類を原本として取扱い、

本 CPS3.1.8 項～3.1.11 項の手続きを行う。
また、電子証明書発行申込書に不備がある場合、業務運用者が不備の状況により判断した、次の(1)～(3)のいずれかの方法により再提出または追加提出の依頼を行う。ただし、いずれの場合であっても利用者が新たに電子証明書発行申込書の様式を入手し、記入および押印したものを追加提出することを妨げない。

(1) 利用者が提出済み電子証明書発行申込書の控えを訂正、押印する方法
(2) 業務運用者が送付した電子証明書発行申込書を利用者が訂正、押印する方法
(3) 業務運用者が添付書類に基づいて印字作成し、送付した電子証明書発行申込書を利用者が内容を確認、訂正、押印する方法

(2)、(3)の場合に、業務運用者が電子証明書発行申込書を利用者に送付するときは、利用者本人を確認のうえ、以下(a)～(c)のとおり FAX、メールまたは郵送のいずれかの方法により、「書類不備のお知らせ」とともに安全に送付する。

(a) 電子証明書発行申込書連絡先記載の FAX 番号に送付する方法。なお、業務運用者が FAX で返送したものを利用者が追加提出した電子証明書発行申込書の様式、記載内容が不鮮明である場合は、不備として扱い、再度提出していただくものとする。
(b) (a)が困難な場合、電子証明書発行申込書連絡先記載のメールアドレスにメールする方法
(c) (a)、(b)が困難な場合、電子証明書発行申込書連絡先記載の住所に郵送する方法

4.2 電子証明書の発行

業務運用者は、発行申込の受付が完了し、利用者の真偽の確認の結果、真正であると判断された申込に対し、本節の手順で当該利用者の秘密鍵および公開鍵、電子証明書を生成し、安全かつ確実な方法で発行手続を行う。発行される電子証明書の有効期間は発行日より 1 年 30 日、2 年 30 日、3 年 30 日、4 年 30 日、5 年とし、発行の可否判断を行った日から起算して 5 年を超えることのないよう措置している。
なお、発行手続は業務運用者 2 名以上による相互牽制の下に行われる。

4.2.1 電子証明書記載事項の登録

(1) 利用者氏名(ローマ字、漢字)、利用者自宅住所(ローマ字)、企業等商号・名称(漢字)、企業等の住所(漢字)の登録
業務運用者は、登録事務用端末において発行申込書類に基づき、利用者氏名(ローマ字、漢字)、利用者自宅住所(ローマ字)、企業等商号・名称(漢字)、企業等の住所(漢字)の登録を行う。また、発行申込書記載内容のうち、企業等の商号・名称、住所について、「株式会社」等を「(株)」等に省略して記載されていたり、丁目番地等が、ハイフン等で記載されている場合も、本 CPS3.1.7 項(5)の書類(登記事項証明書等)に記載されている内容と一致しているものと判断される場合には、当該登記事項証明書等から登録するものとする。ただし、発行申込書類記載の文字が JIS 第一水準、第二水準の範囲外である場合、JIS 第一水準、第二水準の範囲内

の文字であって、「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)」等に従い置き換えられた文字で登録するものとする。これに該当する文字がないときは、ひらがなまたはカタカナで登録するものとする。ただし、利用者が企業等代表者の場合に限り、利用者氏名を本 CPS3.1.7 項(5)の書類(登記事項証明書等)記載の文字にて上記手順に従い登録する(利用者が企業等代表者の場合は、当該登記事項証明書等で利用者氏名の確認を行えるため)。

(2) 法人番号の登録
業務運用者は、登録事務用端末において本 CPS3.1.9 項の確認方法に基づき、法人番号の登録を行う。確認ができなかった場合は登録しない。

4.2.2 電子証明書の発行指示

業務運用者は、電子証明書記載事項をセンタの IA/RA サーバに送信し、電子証明書の発行指示を行う。

4.2.3 鍵ペアの生成と電子証明書の作成

センタは、電子証明書の発行指示を受信すると同時に正当な指示であることを確認し、以下の処理を行う。

(1) 利用者の秘密鍵と公開鍵ペアの生成
(2) 公開鍵と電子証明書記載事項をあわせ、電子証明書を作成
(3) 電子証明書署名鍵による電子証明書への電子署名
(4) 作成した電子証明書に対する秘密鍵との対応付け、所定形式(PKCS#12)のファイルへの格納、パスワードによる暗号化および MAC(Message Authentication Code)の付与

4.2.4 電子証明書および秘密鍵の IC カードへの格納等

業務運用者は、電子証明書および秘密鍵の IC カードへの格納等を以下のとおり行う。

(1) 電子証明書および秘密鍵をセンタの IA/RA サーバからダウンロードして PKCS#12 形式ファイルから PKCS#11 形式ファイルに変換して、IC カードに格納する。
(2) PIN の印刷を漏洩しないよう行う。
(3) IC カードおよび PIN を安全に封緘する。

なお、作業の終了後、記録されているすべての秘密鍵および PIN のデータを、認証業務用設備およびその関連装置より担当者が目視することなく完全に削除する。

4.2.5 BCA に対する相互認証証明書の発行

本認証業務での BCA に対する相互認証証明書の発行は、BCA の定める手続完了後、BCA から発行された電子証明書発行要求に対し、相互認証証明書を電子証明書署名鍵により電子署名、発行することにより行う。

4.3 IC カード(電子証明書および秘密鍵)および PIN の受領

利用者は、IC カードおよび PIN の受領を以下のとおり行う。なお、本認証業務では、確実な受領を確認するため、IC カードおよび PIN を受領した証として、利用者から受領

書または受領書データを回収する期限(IC カードの発送日から数えて 30 日)を明示している。

受領書および受領書データが重複して本認証局に返送または送信された場合は、先に受付けたものを登録する。後に到着したものも保存する。

(1) 本人限定受取郵便による受領

利用者は、IC カードおよび PIN を本人限定受取郵便(基本型)で受領する。

利用者は IC カードおよび PIN を受領後、発行通知書により電子証明書記載事項を確認の上、受領書に記名押印(実印)して本認証局に返送するか、受領書データを送信しなければならない。なお、利用者が外国人であって、個人の実印を所有していなかった場合の受領書には、実印による押印に代えて利用者の自署が行われていることを必須とする。

当該受領書の記名および実印による押印の確認（利用者が外国人であって、個人の実印を所有していなかった場合は自署の確認）または受領書データの電子署名、電子証明書の確認をもって IC カードおよび PIN は、利用者に確実に受領されたものとする。

本認証業務は、代理人(本人限定受取郵便上の受取代人を含む。)が IC カードを受領する事を認めている。ただし、その場合の PIN は、利用者宛に簡易書留郵便で別送する。代理人は、IC カードを受領した場合、当該郵便物を開封することなく直ちに、利用者へ届けなければならない。

(2) 対面の手交による受領

対面にて直接 IC カードおよび PIN を手交する場合は、以下のとおり行う。

なお、受取代理人に対する手交は IC カードのみとし、PIN は利用者宛に簡易書留郵便で別送する。

①対面の手交の場合における真偽の確認

当社窓口において利用者または受取代理人に手交する場合、業務運用者は 2 名体制で、利用者または受取代理人に対して本人の運転免許証等公的な写真入りの身分証明書の提示を求め、当該書類が「様式」、「記載内容」および「有効期限」等において真正な書類であることを確認し、利用者または受取代理人であることの確認を行う。受取代理人は、IC カードの入った封筒を受領した場合、当該封筒を開封することなく直ちに、利用者へ届けなければならない。

なお、当社窓口以外に出向き、利用者または受取代理人に手交する場合は、業務運用者が 2 名体制で当社内において IC カード等を鞄等に入れ施錠後、常時携帯、搬送し、利用者の所属企業等安全かつ確実に手渡すことができる場所に出向いて手交を行う。この場合も上記と同様の真偽の確認を行う。

②利用者に手交した場合の受領書の取扱

IC カードおよび PIN を受領した利用者に対し、直ちに発行通知書により電子証明書記載事項を確認させるとともに、受領書に利用者の自署または記名押印(実印)を求め、その場で受領書を回収する。

③受取代理人に手交した場合の受領書または受領書データの取扱

受取代理人へは、手交した証となる対面時受取書(受取代理人自署または記名押印(実印)のある受取り確認書類であるが、受領書ではない。)と引き替えに封緘

されたICカードのみを手交する。受取代理人は、開封することなく直ちに利用者へ届けなければならない。この場合、受取代理人経由でICカードを受領した利用者は、本認証局より別送されてくるPINを受け取り、本項(1)に準じて電子証明書記載事項を確認の上、受領書に記名押印(実印)して本認証局に返送するか受領書データを送信しなければならない。当該受領書の記名押印(実印)の確認または受領書データの電子署名、電子証明書の確認をもって、ICカードおよびPINは、利用者に確実に受領されたものとする。

4.4 電子証明書の失効

電子証明書の有効期間内において、以下の事由が発生したときは、当該電子証明書を失効させる。

4.4.1 利用者の申込による失効

以下の事由が発生した場合、本認証局は利用者の失効申込を受けて電子証明書の失効を行う。

(1) 電子証明書等が格納されたICカードまたはPINの紛失・盗難等の場合
(2) 電子証明書等が格納されたICカードの破損等により機能が損なわれた場合
(3) (1)(2)を除く利用者の秘密鍵の危殆化またはそのおそれのある場合
(4) 電子証明書の記載事項(利用者氏名、利用者自宅住所、企業等の商号・名称、企業等の本店住所、法人番号)の変更
(5) 利用者が当該企業等に属さないこととなった場合
(6) 利用者による使用停止
(7) 企業等の倒産等の場合

4.4.2 本認証局の判断に基づく失効

(1) 企業等からの失効届出を受けて以下の事由が判明した場合、本認証局の判断に基づき電子証明書の失効を行う。ただし、④⑤の場合は第三者が失効届出をすることができる。
①電子証明書の記載事項(利用者氏名、利用者自宅住所、企業等の商号・名称、企業等の本店住所、法人番号)の変更
②利用者が当該企業等に属さないこととなった場合
③利用者による使用停止(人事異動等)
④利用者の死亡
⑤企業等の倒産等の場合
(2) 以下の事由が発生した場合、本認証局の判断に基づき電子証明書の失効を行う。
①期日(ICカードの発送日から数えて30日の受領書回収期限に10日を加算した40日)内に、受領書または受領書データが提出されない場合
②本認証局の責めに帰すべき事由により電子証明書の誤発行等を行った場合
③①、②の他、利用者または利用者の所属する企業等が利用規約に違反する行為を行った場合
④失効申込がないため、第三者に損害を与える等社会的に多大な損害や混乱が生じるもしくはそのおそれのある場合

⑤本認証局の電子証明書署名鍵の危殆化(詳細は本 CPS4.9 節を参照)
⑥本認証局の終了(詳細は本 CPS4.10 節を参照)
なお、②において、利用者が IC カードを受取後、誤発行等が発覚した場合は、利用者は失効の連絡を行う義務を負い、本認証局は誤発行等を確認の上、失効通知書および改めて発行した IC カードを利用者宛に送付する。この場合、発行申込書および添付書類の再提出は不要とする。また、本認証局が IC カードを発送または手交以前に誤発行が発覚した場合は、本認証局内部の手続きにより失効および再度発行業務を行うので、失効通知書の送付は行わない。

4.4.3 失効申込・失効届出のパターン

失効申込は本認証局所定の失効申込書を使用し、利用者からの郵送または対面による申込を原則とする。

ただし、失効事由の重大性や緊急性にかんがみ、FAX による申込も受付けるが、この際本認証局は、失効申込者の意思を電話にて確認する。

なお、失効申込書の原本の提出は、事後であっても必須である。

失効届出は本認証局所定の失効届出書を使用し、企業等もしくは第三者からの郵送または対面による届出により受付ける。

4.4.4 失効申込・失効届出の審査

失効の手続は、通常、失効申込権者が、所定の失効申込書を本認証局に提出する、または企業等もしくは第三者が、所定の失効届出書を本認証局に提出することにより開始される。

失効申込書または届出書の記載内容は以下の事項を含むものとする。

(1) 失効申込書
- 電子証明書カード番号
- 失効理由
- 失効申込者(利用者)の氏名、住所、押印(実印)

※利用者が外国人であって、個人の実印を所有していない場合は、失効申込書の押印欄に、自署が行われていることを必須とする。

(2) 失効届出書(企業等届出用)
- 電子証明書カード番号
- 利用者氏名
- 失効理由
- 失効届出者(企業等)の商号・名称、代表者氏名、本店住所、 押印(企業等の代表者印)

(3) 失効届出書(第三者届出用)
- 電子証明書カード番号
- 利用者氏名
- 失効理由
- 失効届出者の氏名および住所、利用者との関係、押印(認印で可)

業務運用者は、失効申込者または失効届出者の真偽の確認を本 CPS3.4.2 項に基づき行い、失効申込書類または失効届出書類の利用者氏名、失効事由、カード番号(ただし、紛失等によりカード番号が不明な場合は不要)等を確認する。

4.4.5　失効データの登録および失効

失効申込書類または失効届出書類の審査の後、業務運用者は 2 名による相互牽制の下、登録用端末において失効データの登録を行い、IA/RA サーバに対し電子証明書の失効指示を行う。

IA は、失効指示を受信すると同時に正当な指示であることを確認し、電子証明書の失効を行う。

4.4.6　失効申込者・失効届出者への通知

失効処理の完了後、利用者および企業等に対して失効通知書を普通郵便にて送付する。

4.5　電子証明書失効リスト(CRL/ARL)

4.5.1　CRL の更新周期

本認証局は、CRL を定期的に更新し、電子証明書に記載する URL の示すリポジトリに公開する。この更新は原則として 24 時間以内(CRL 次回更新予定時刻は 48 時間後に設定)とする。

CRL として掲載する失効情報は、本 CPS7.2 節の表 7-2(1) CRL プロファイルに規定する。

なお、CRL に掲載する失効情報は、当該電子証明書の有効期間が満了するまで公開し、有効期間の終了した電子証明書については、検証者からの照会には応じない。

4.5.2　相互認証証明書の失効

本認証局または BCA に以下の事象が発生した場合、相互認証証明書を失効させる。

(1) 電子証明書署名鍵の危殆化

(2) 相互認証基準違反

(3) 相互認証業務の終了

(4) 相互認証の更新(本認証局が失効する必要があると判断した場合)

(5) ポリシーの変更

その場合、本認証局からの失効申込は業務運用管理者が行う。BCA からの失効申込は BCA の責任者からのものを組織の認証を実施したうえで受理し、直ちに相互認証証明書を失効させ、その後の最も早い CRL 更新日時に(危殆化の場合は直ちに)ARL を更新し、リポジトリにて公開する。

ARL の発行は CRL と同期して、24 時間以内(ARL の次回更新予定時刻は 48 時間後に設定)とする。

ARL として掲載する失効情報は、本 CPS7.2 節の表 7-2(2)ARL プロファイルに規定する。

4.6　セキュリティ監査手続

本認証局は、安全な環境を維持していくため、本認証局の運営状況を記録し、監査するシステムを以下のように運用する。

(1) 本認証局内の IA/RA サーバ・IC カード印刷機等の機器、センタ認証設備室および本部マシン室内のネットワーク機器、センタ認証設備室および本部マシン室内の

監視装置およびこれらに至る経路上のゲートは監査証跡を残し、定期的にそれをセキュリティ監査する。

(2) 監査証跡には以下が含まれる。

①IA/RA サーバ、IC カード印刷機の操作・稼動ログ

②電子証明書署名鍵管理のログ

③業務運用者用証明書(RAO 証明書)発行のログ

④利用者の電子証明書の登録、発行、失効、各イベントのすべてのログ

⑤ファイアウォール、侵入検知システム、センタ認証設備室および本部マシン室内ネットワークおよびサーバの監視ログ

⑥すべてのパケット、トランザクションに関する記録(主にセンタ側で記録されるもの)

⑦センタ認証設備室および本部マシン室内をカバーするモーションセンサ、監視カメラ・ビデオ、入退室ゲートの各機器の警報発報を含む動作記録。警報発報は以下に記す取扱において異常な記録として扱う。

これらの監査証跡は定期的にセキュリティ監査され、正常と認められた記録は監査記録で置きかえられて抹消される。ただし、入退室ゲートの各機器の警報発報を含む動作記録は、異常正常の区別なく、認定の更新の日まで保存する。

過誤もしくは故意の異常と認められる記録は個別に検証され、必要と認められれば対策がとられる。

この異常と認められた記録等およびとられた対策の記録を含むセキュリティ監査記録は、準拠性監査および電子署名法に則った認定更新までの間、次節に規定する方法で保存され、これらにおいて再度検証される。

セキュリティ監査は少なくとも毎月行われる。

4.7 アーカイブ

本認証業務では、主として電子署名法の要件に基づき、書類およびデジタルデータを保存する。

(1) 保管にあたっては漏えい、滅失またはき損の防止措置をとり、書類については原本を保存する。

(2) 保管場所は、間仕切り、壁等で区分され、防災、防犯、防火、防水、直射日光遮断機能があり、扉が施錠されている。

(3) 共通 CPS2.8.4 項～2.8.7 項の規定による開示要求があった場合は、アーカイブ、保存された情報の規定された範囲の内容を規定された相手にのみ提供する。

(4) 保存期間の過ぎた書類およびデジタルデータを確実に消去する。

(5) 書類は細かく裁断する等の措置を、デジタルデータは媒体の破壊もしくは無効情報の上書きにより消去する等の措置をとる。

4.7.1 紙で保存する書類

本認証業務に関する以下の書類は、紙の原本を保存する。文末の( )内は保存期間である。

(1) 認証業務の一部を他に委託する場合の委託契約書および関係する書類の原本(電子証明書の有効期間満了後 10 年間)

(2) 認証業務に従事する要員、組織、体制、主管、指揮命令系統に関する管理情報、履歴のうち紙で運用されるものの原本(電子証明書の有効期間満了後 10 年間)
(3) 内部監査(準拠性監査(詳細は共通 CPS2.7 節を参照))記録および監査報告書の原本(電子証明書の有効期間満了後 10 年間)
(4) 電子証明書署名鍵管理(鍵生成、保管、活性化/非活性化、バックアップ/復元、破棄)および電子証明書署名鍵に対応する自己署名証明書発行に伴い、紙で運用される帳票(電子証明書の有効期間満了後 10 年間)
(5) 利用者からの発行申込に伴い提出される発行申込書原本および添付される書類(電子証明書の有効期間満了後 10 年間)
(6) 受領書(電子証明書の有効期間満了後 10 年間)
(7) 利用者等からの電子証明書失効申込または失効届出に伴い提出される申込書等失効判断に用いた書類一式(電子証明書の有効期間満了後 10 年間)
(8) 電子証明書発行申込、電子証明書失効申込または失効届出を取扱う記録のうち紙で管理されるもの(電子証明書の有効期間満了後 10 年間)
(9) セキュリティ監査対象イベントの記録のうち紙で管理されるもの(内部監査および認定更新を経るまで)
(10) 手続的管理(詳細は共通 CPS5 章を参照)で規定する権限付与、剥奪の記録のうち紙で管理されるもの(内部監査および認定更新を経るまで)
(11) 設備保守、システム保守、変更、障害の記録のうち紙で管理されるもの(内部監査および認定更新を経るまで)
(12) 相互認証手続に関する書類(相互認証証明書の有効期間満了後 10 年間)

4.7.2 デジタルデータとしてアーカイブする情報

以下の情報は、デジタルデータとして電磁的媒体に記録し、電子署名等の改ざん防止措置を施す。なお、可読性を保つために、媒体間での複写を行う場合がある。文末の( ) 内は保存期間である。

(1) 認証業務の一部を他に委託する場合の電子契約にて締結した委託契約書および関係する書類のデジタルデータ(電子証明書の有効期間満了後 10 年間)
(2) 発行されたすべての電子証明書、CRL/ARL、自己署名証明書および関係するすべての電子証明書(電子証明書の有効期間満了後 10 年間)
(3) 共通 CPS、本 CPS、業務取扱要領、関係する詳細手続文書等およびそれらの変更履歴(電子証明書の有効期間満了後 10 年間)
(4) 利用者に公開される利用規約、検証者同意書等およびそれらの変更履歴(電子証明書の有効期間満了後 10 年間)
(5) 認証業務に従事する要員、組織、体制、主管、指揮命令系統に関する管理情報、履歴のうち、デジタルデータで運用されるもの(電子証明書の有効期間満了後 10 年間)
(6) 電子証明書署名鍵管理(鍵生成、保管、活性化/非活性化、バックアップ/復元、破棄)と対応するデジタルデータで運用される帳票(電子証明書の有効期間満了後 10 年間)
(7) 発行申込、電子証明書失効申込または失効届出を取扱う記録のうち、デジタルデータで管理されるもの(電子証明書の有効期間満了後 10 年間)
(8) 受領書データおよび関連データ、それらを取扱う記録のうち、デジタルデータで

管理されるもの(電子証明書の有効期間満了後 10 年間)
(9) セキュリティ監査対象イベントの記録のうち、デジタルデータで管理されるもの(内部監査および認定更新を経るまで)
(10)手続的管理(共通 CPS5 章)で規定する権限付与、剥奪の記録のうちデジタルデータで管理されるもの(内部監査および認定更新を経るまで)
(11)設備保守、システム保守、変更、障害の記録のうちデジタルデータで管理されるもの(内部監査および認定更新を経るまで)
(12)相互認証業務に関する手続文書およびそれらの変更履歴(相互認証証明書の有効期間満了後 10 年間)

4.8 鍵の更新

本認証局の秘密鍵(電子証明書署名鍵)の有効期間の残りが利用者の電子証明書の最大有効期間よりも短くなる前に、本認証局はその鍵による新たな利用者の電子証明書の発行を中止し、新たな署名用鍵ペアを共通 CPS6 章規定の方法で生成する。

鍵の更新を行う本認証局では新たな公開鍵についての自己署名証明書および現存の公開鍵との間のリンク証明書(新しい本認証局の公開鍵に古い本認証局の秘密鍵で電子署名した電子証明書(NewWithOld)と、古い公開鍵に新しい秘密鍵で電子署名した電子証明書(OldWithNew))を発行し、リポジトリにて公開する。

4.9 危殆化と災害からの回復

(1) 電子証明書署名鍵が危殆化または危殆化の恐れが判明した場合、その鍵の不正な複写により新たな利用者の電子証明書が出回り、不正に信頼されることを避けるために、その電子証明書署名鍵を無効なものとして取扱う。
(2) 具体的には、危殆化が発生した鍵にて電子署名したすべての有効な電子証明書(発行した相互認証証明書を含む)を可及的すみやかに失効させ、その CRL/ARL に危殆化した鍵で電子署名して公開し、さらに電子証明書署名鍵を抹消する。検証者および利用者への危殆化の事実等の通知は、ホームページにより行い、電子証明書の失効の通知は、利用者へ郵送で行う。
(3) 本認証局は、天災等により施設、設備に被害を受け、もしくはその施設、設備に対する外部からの物理的または論理的攻撃を受けて、運用を続けられなくなった場合、共通 CPS および本 CPS に基づいて新たな施設、設備等を準備し、バックアップデータに基づいて業務を再開することについて最善の努力をはらう。
(4) 本認証局は可及的すみやかに危殆化もしくは被災の事実を検証者および利用者に NDN ホームページで公開し、原因究明と対策確立のうえ、電子証明書署名鍵の危殆化またはその恐れ、または 72 時間以上の停止を伴う重大障害(被災を含む。)であって検証者が停止を知る方法がなかった場合には、主務大臣および BCA へ通報する。
(5) また、バックアップは、通常のオンサイトバックアップとし、オフサイトバックアップは行わない。なお、電子証明書署名鍵のバックアップについては、鍵断片(詳細は共通 CPS6 章を参照)の所有者により安全な場所に保管される。
(6) 本認証局は危殆化もしくは被災の際の復旧手順について別途定め、計画に従って

教育訓練を行う。

4.10 本認証局の終了(認証業務の終了)

本認証局は、電子署名法関係法令の改訂、共通 CPS2.2 節～2.4 節の規定および本認証局の事業方針の変更等に起因して認証業務を終了することとした場合は、以下の手続きをとるものとする(電子署名法の定める更新を行わないこととした場合を含む。)。

(1) やむを得ない場合を除き、終了の 60 日前から終了の 6 ヶ月後まで本認証局のホームページに公開するとともに、利用者および企業等に終了 60 日前までに終了を通知する。
(2) 本認証局は新たな電子証明書の発行を中止する。
(3) 電子証明書および相互認証証明書を一斉に失効処理し、失効したすべての電子証明書および相互認証証明書に記載されている有効期間満了日まで有効な CRL/ARL を発行し、リポジトリにて有効期間が満了するまで公開する。
(4) 本認証局は、利用者および企業等に対して失効通知書を普通郵便にて送付する。
(5) 電子証明書署名鍵およびそのバックアップ媒体を完全な初期化または物理的に破壊する。
(6) 電子署名法の定める帳票類保存期間にわたり、紙およびデジタルデータの各種書類、データを保存し続けるよう最善を尽くす。やむを得ない場合は、これらの保存された情報の後継管理者を公開する。

5　物理的、手続的、人的なセキュリティ管理

以下の条項について、本 CPS1.2 節(4)に示す共通 CPS に規定する。

5.1　物理的セキュリティ管理

5.2　手続的セキュリティ管理

5.3　人的セキュリティ管理

6　技術的なセキュリティ管理

以下の条項について、本 CPS1.2 節(4)に示す共通 CPS に規定する。

6.1　鍵ペアの生成と組み込み

6.1.1　認証局(自己署名 CA)
6.1.2　利用者

6.2　電子証明書署名鍵(秘密鍵)の保護

6.2.1　暗号化装置標準
6.2.2　電子証明書署名鍵の複数人制御
6.2.3　電子証明書署名鍵のエスクロウ
6.2.4　電子証明書署名鍵のバックアップ
6.2.5　電子証明書署名鍵のアーカイブ
6.2.6　電子証明書署名鍵の暗号化装置へのエントリ(バックアップリカバリ)
6.2.7　電子証明書署名鍵を活性化させる方法
6.2.8　電子証明書署名鍵を非活性化させる方法
6.2.9　電子証明書署名鍵を破壊する方法

6.3　鍵ペア管理のその他の面

6.3.1　公開鍵のアーカイブ
6.3.2　公開鍵と秘密鍵の使用期間
6.3.3　CA 属性を持つ電子証明書の有効期間

6.4　活性化データ

6.4.1　活性化データの生成と組み込み
6.4.2　活性化データの保護

6.5　コンピュータのセキュリティ管理

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
6.6.2　セキュリティマネジメント管理

6.7　ネットワークのセキュリティ管理

6.8　暗号化装置の技術的管理

7　電子証明書ならびに CRL/ARL プロファイル

本章では、本認証業務で発行する電子証明書および CRL/ARL のプロファイルについて記述する。

7.1　電子証明書プロファイル

7.1.1　バージョン番号

本認証業務では、X.509V3 の電子証明書を発行する。

7.1.2　電子証明書拡張部

本認証業務では、発行する電子証明書の種類によって使用する拡張部は異なる。詳細は、本 CPS7.1.9 項に規定される個々の電子証明書プロファイルを参照されたい。

7.1.3　アルゴリズム OID

本認証業務で発行する電子証明書、CRL/ARL で使用されるアルゴリズム名とその OID は以下のとおりである。

(1) 所有者公開鍵(subjectPublicKeyInfo)：RSAEncryption(OID=1 2 840 113549 1 1 1)
(2) 署名(signature)： sha1WithRSAEncryption(OID=1 2 840 113549 1 1 5)

7.1.4　名称形式

本認証業務で発行する電子証明書、CRL/ARL に記載される発行者、所有者の名称とその形式詳細は、本 CPS7.1.9 項および 7.2.3 項を参照

7.1.5　名称制約

本認証業務では、名称制約拡張を使用しない。

7.1.6　電子証明書ポリシーOID

本認証業務で使用する電子証明書のポリシーの OID は、1.2.392.200122.1.2 である。

7.1.7　ポリシー制約(policyConstraints)拡張の使用

本認証業務では、ポリシー制約拡張を、BCA 接続のため発行する相互認証証明書に使用する。詳細は、本 CPS7.1.9 項の表 7-1(3)を参照

7.1.8　ポリシー修飾子(policyQualifiers)

利用者の電子証明書では「検証者同意書」の URL を、また相互認証電子証明書では共通 CPS および本 CPS の URL を格納している。詳細は、本 CPS7.1.9 項を参照

7.1.9　電子証明書プロファイル

本認証業務で発行する電子証明書のプロファイル詳細を表 7-1 に記述する。なお、以降の表で現われる「設定者」と「クリティカリティ」の設定値の意味は以下のとおりである。また、後述の CRL/ARL の表の記述における意味も同一である。なお、電子証明書の記載項目は、特に断りのない限り PrintableString でエンコードされる。

設定者　IA ： IA で値を設定する。
　　RA ： RA で値を設定する。
　　× ： 値を設定しない。

クリティカリティ　T　： TRUE を表す。
　　F　： FALSE を表す。
　　－ ： 設定できない、または設定しない。

表 7-1(1) 自己署名証明書プロファイル

名称	設定者	クリティカリティ	設定値
証明書基本部			
version(バージョン)	IA	－	V3
serialNumber(シリアル番号)	IA	－	128bit 以下の正の整数
signature(署名)	IA	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
issuer(発行者)	IA	－	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=AOSign Certification Authority ※C は PrintableString でエンコードする、 その他は UTF8String でエンコードする。
Validity(有効期間)			
notBefore	IA	－	有効期間は 10 年間とする。
notAfter	IA	－	※UTCtime で設定する。
subject(所有者)	IA	－	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=AOSign Certification Authority ※C は PrintableString でエンコードする、 その他は UTF8String でエンコードする。
subjectPublicKeyInfo (所有者公開鍵)			
algorithmIdentifier	IA	－	rsaEncryption(OID=1 2 840 113549 1 1 1)
public key	IA	－	2048bit の値
証明書標準拡張部			
authorityKeyIdentifier (認証局鍵識別)	×	－	設定しない。
keyIdentifier			
authorityCertIssuer			
authCertSerialNumber			
subjectKeyIdentifier (所有者鍵識別)	IA	F	公開鍵の SHA-1 値(ハッシュ値)
keyUsage(鍵の使用目的)	IA	T	keyCertSign, cRLSign を ON とし、他を OFF とする。
extendKeyUsage(拡張鍵種別)	×	－	設定しない。

privateKeyUsagePeriod (秘密鍵有効期間)	×	―	設定しない。
certificatePolicies (証明書ポリシー)	×	―	設定しない。
policyIdentifier			
certPolicyId			
policyQualifiers			
policyQualifierId			
Qualifier			
policyMappings (ポリシーマッピング)	×	―	設定しない。
issuerDomainPolicy			
subjectDomainPolicy			
subjectAltName(所有者別名)	IA	F	C=JP,O=日本電子認証株式会社, OU=AOSign 認証局 ※C は PrintableString でエンコードする、 その他は UTF8String でエンコードする。
issuerAltName(発行者別名)	IA	F	C=JP,O=日本電子認証株式会社, OU=AOSign 認証局 ※C は PrintableString でエンコードする、 その他は UTF8String でエンコードする。
basicConstraints(基本制約)	IA	T	
cA	IA		TRUE
pathLenConstraint	×		設定しない。
nameConstraints(名称制約)	×	―	設定しない。
policyConstraints (ポリシー制約)	×	―	設定しない。
requireExplicitPolicy			
inhibitPolicyMapping			
cRLDistributionPoints (CRL 分配点)	IA	F	distributionPoint.fullName.URL に以下を設定する。 Ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?authorityRevocationList
subjectDirectoryAttributes (所有者ディレクトリ属性)	×	―	設定しない。
証明書プライベートインターネット拡張部			
authorityInfoAccess (認証局情報アクセス)	×	―	設定しない。

表 7-1(2) 利用者の電子証明書プロファイル

名称	設定者	クリティカリティ	設定値
証明書基本部			
version(バージョン)	IA	－	V3
serialNumber(シリアル番号)	IA	－	128bit 以下の正の整数
signature(署名)	IA	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
issuer(発行者)	IA	－	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=AOSign Certification Authority ※C は PrintableString でエンコードする、その他は UTF8String でエンコードする。
Validity(有効期間)			
notBefore	IA	－	有効期間は 1 年+30 日,2 年+30 日,3 年+30 日,4 年+30 日,5 年のいずれかとする。ただし、開始日時および終了日時(有効期限)は UTCtime 形式により秒単位で設定する。
notAfter	IA	－	
subject(所有者)	RA	－	C=JP, S=XXX, L=XXX, CN=XXX, UID を設定する。(*) ※C は PrintableString でエンコードする、その他は UTF8String でエンコードする。なお、UID は登録局で IC カードに識別子を設定する。
subjectPublicKeyInfo (所有者公開鍵)			
algorithmIdentifier	RA	－	rsaEncryption(OID=1 2 840 113549 1 1 1)
public key	RA	－	1024bit の値
証明書標準拡張部			
authorityKeyIdentifier (認証局鍵識別)	IA	F	
keyIdentifier			公開鍵の SHA-1 値(ハッシュ値)
authorityCertIssuer			issuer の DN
authCertSerialNumber			シリアル番号
subjectKeyIdentifier (所有者鍵識別)	IA	F	公開鍵の SHA-1 値(ハッシュ値)
keyUsage(鍵の使用目的)	IA	T	digitalSignature, nonRepudiation を ON とし、他を OFF とする。
extendKeyUsage(拡張鍵種別)	×	－	設定しない。
privateKeyUsagePeriod (秘密鍵有効期間)	×	－	設定しない。
certificatePolicies (証明書ポリシー)	IA	T	
policyIdentifier			
certPolicyId			(OID=1 2 392 200122 1 2)

policyQualifiers				
	policyQualifierId			(OID=1 3 6 1 5 5 7 2 1) id-qt-cps
	Qualifier			https://rep.ninsho.co.jp/aosign/rpa.html (検証者同意書の URL)
	policyQualifierId			(OID=1 3 6 1 5 5 7 2 2) id-qt-unotice
	Qualifier			Accredited under e-Signature Law(Japan) ※VisibleString でエンコードする。
policyIdentifier				
	certPolicyId			(OID=1 2 392 200122 1 3)
policyQualifiers				
	policyQualifierId			(OID=1 3 6 1 5 5 7 2 1) id-qt-cps
	Qualifier			https://rep.ninsho.co.jp/aosign/rpa.html (検証者同意書の URL)
	policyQualifierId			(OID=1 3 6 1 5 5 7 2 2) id-qt-unotice
	Qualifier			Accredited under e-Signature Law(Japan) ※VisibleString でエンコードする。
policyMappings (ポリシーマッピング)		×	―	設定しない。
	issuerDomainPolicy			
	subjectDomainPolicy			
subjectAltName(所有者別名)		RA	F	C=JP,S=本社住所(都道府県), L=本社住所(郡、市区町村以下), O=企業等名称, organizationIdentifier= JCNXXXXXXXXXXXXX,CN=氏名を設定する。 ※CはPrintableStringでエンコードする、 その他はUTF8Stringでエンコードする。
issuerAltName(発行者別名)		IA	F	C=JP,O=日本電子認証株式会社, OU=AOSign 認証局 ※CはPrintableStringでエンコードする、 その他はUTF8Stringでエンコードする。
basicConstraints(基本制約)		×	―	設定しない。
	cA			
	pathLenConstraint			
nameConstraints(名称制約)		×	―	設定しない。
policyConstraints (ポリシー制約)		×	―	設定しない。
cRLDistributionPoints (CRL 分配点)		IA	F	distributionPoint.fullName.URL に以下を設定する。 Ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?certificateRevocationList
subjectDirectoryAttributes (所有者ディレクトリ属性)		×	―	設定しない。

証明書プライベートインターネット拡張部				
	authorityInfoAccess (認証局情報アクセス)	×	―	設定しない。

＊ 2013 年 2 月 1 日までに発行された証明書は、C=JP, S=XXX, L=XXX, CN=XXX が設定されている。

表 7-1(3) 相互認証証明書プロファイル

名称			設定者	ｸﾘﾃｨｶﾙﾃｨ	設定値
証明書基本部					
	version(バージョン)		IA	―	V3
	serialNumber(シリアル番号)		IA	―	128bit 以下の正の整数
	signature(署名)		IA	―	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
	issuer(発行者)		IA	―	C=JP, O=Nippon Denshi Ninsho Co.Ltd., OU=AOSign Certification Authority ※C は PrintableString でエンコードする、 その他は UTF8String でエンコードする。
	Validity(有効期間)				
		notBefore	IA	―	有効期間は 5 年間以内とする。 ※UTCTime で設定する。
		notAfter	IA	―	
	subject(所有者)		IA	―	BCA から指定される DN ※BCA が指定したエンコードで設定する。
	subjectPublicKeyInfo (所有者公開鍵)				
		algorithmIdentifier	IA	―	rsaEncryption(OID=1 2 840 113549 1 1 1)
		public key	IA	―	2048bit の値
証明書標準拡張部					
	authorityKeyIdentifier (認証局鍵識別)		IA	F	
		keyIdentifier			公開鍵の SHA-1 値(ハッシュ値)
		authorityCertIssuer			issuer の DN
		authCertSerialNumber			シリアル番号
	subjectKeyIdentifier (所有者鍵識別)		IA	F	公開鍵の SHA-1 値(ハッシュ値)
	keyUsage(鍵の使用目的)		IA	T	keyCertSign, cRLSign を ON とし、他を OFF とする。
	extendKeyUsage(拡張鍵種別)		×	―	設定しない。
	privateKeyUsagePeriod (秘密鍵有効期間)		×	―	設定しない。
	certificatePolicies (証明書ポリシー)		IA	T	
		policyIdentifier			
		certPolicyId			(OID=1 2 392 200122 1 3) NDN-GPKI 用

	policyQualifiers			
	policyQualifierId			(OID=1 3 6 1 5 5 7 2 1) id-qt-cps
	Qualifier			https://rep.ninsho.co.jp/aosign/cps.html (CPS の URL)
policyMappings (ポリシーマッピング)		IA	F	
	issuerDomainPolicy			(OID=1 2 392 200122 1 3) NDN-GPKI 用
	subjectDomainPolicy			BCA 側 OID
subjectAltName(所有者別名)		×	ー	設定しない。
issuerAltName(発行者別名)		×	ー	設定しない。
basicConstraints(基本制約)		IA	T	
	cA	IA		TRUE
	pathLenConstraint	×		設定しない。
nameConstraints(名称制約)		×	ー	設定しない。
policyConstraints (ポリシー制約)		IA	T	
	requireExplicitPolicy	IA		0 を設定する。
	inhibitPolicyMapping	IA		1 を設定する。
cRLDistributionPoints (CRL 分配点)		IA	F	distributionPoint.fullName.URL に以下を設定する。 Ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?authorityRevocationList
subjectDirectoryAttributes (所有者ディレクトリ属性)		×	ー	設定しない。
証明書プライベートインターネット拡張部				
authorityInfoAccess (認証局情報アクセス)		×	ー	設定しない。

表 7-1(4) リンク証明書(NewWithOld)プロファイル

名称	設定者	クリティカリティ	設定値
証明書基本部			
version(バージョン)	IA	ー	V3
serialNumber(シリアル番号)	IA	ー	128bit 以下の正の整数
signature(署名)	IA	ー	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
issuer(発行者)	IA	ー	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=AOSign Certification Authority ※C は PrintableString でエンコードする、その他は UTF8String でエンコードする。
Validity(有効期間)			

	notBefore	IA	―	NewWithNew の validity.notBefore を UTCTime で設定する。
	notAfter	IA	―	OldWithOld の validity.notAfter を UTCTime で設定する。
Subject(所有者)		IA	―	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=AOSign Certification Authority ※C は PrintableString でエンコードする、その他は UTF8String でエンコードする。
subjectPublicKeyInfo (所有者公開鍵)				
	algorithmIdentifier	IA	―	rsaEncryption(OID=1 2 840 113549 1 1 1)
	public key	IA	―	2048bit の値
証明書標準拡張部				
authorityKeyIdentifier (認証局鍵識別)		IA	F	
	keyIdentifier			OldWithOld の公開鍵の SHA-1 値(ハッシュ値)
	authorityCertIssuer			OldWithOld の issuer の DN
	authCertSerialNumber			OldWithOld のシリアル番号
subjectKeyIdentifier (所有者鍵識別)		IA	F	NewWithNew の公開鍵の SHA-1 値(ハッシュ値)
keyUsage(鍵の使用目的)		IA	T	keyCertSign, cRLSign を ON とし、他を OFF とする。
extendKeyUsage(拡張鍵種別)		×	―	設定しない。
privateKeyUsagePeriod (秘密鍵有効期間)		×	―	設定しない。
certificatePolicies (証明書ポリシー)		IA	F	
	policyIdentifier			
	certPolicyId			(OID=2 5 29 32 0) any-policy
	policyQualifiers	×	―	設定しない。
	policyQualifierId			
	Qualifier			
policyMappings (ポリシーマッピング)		×	―	設定しない。
	issuerDomainPolicy			
	subjectDomainPolicy			
subjectAltName(所有者別名)		×	―	設定しない。
issuerAltName(発行者別名)		×	―	設定しない。
basicConstraints(基本制約)			T	
	cA	IA		TRUE
	pathLenConstraint	×	―	設定しない。
nameConstraints(名称制約)		×	―	設定しない。

	policyConstraints (ポリシー制約)	×	―	設定しない。
	cRLDistributionPoints (CRL 分配点)	IA	F	distributionPoint.fullName.URL に以下を設定する。 Ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?authorityRevocationList
	subjectDirectoryAttributes (所有者ディレクトリ属性)	×	―	設定しない。
証明書プライベートインターネット拡張部				
	authorityInfoAccess (認証局情報アクセス)	×	―	設定しない。

表 7-1(5) リンク証明書(OldWithNew)プロファイル

名称		設定者	クリティカリティ	設定値
証明書基本部				
version(バージョン)		IA	―	V3
serialNumber(シリアル番号)		IA	―	128bit 以下の正の整数
signature(署名)		IA	―	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
issuer(発行者)		IA	―	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=AOSign Certification Authority ※C は PrintableString でエンコードする、その他は UTF8String でエンコードする。
Validity(有効期間)				
	notBefore	IA	―	OldWithOld の validity.notBefore を UTCTime で設定する。
	notAfter	IA	―	OldWithOld の validity.notAfter を UTCTime で設定する。
Subject(所有者)		IA	―	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=AOSign Certification Authority ※C は PrintableString でエンコードする、その他は UTF8String でエンコードする。
subjectPublicKeyInfo (所有者公開鍵)				
	algorithmIdentifier	IA	―	rsaEncryption(OID=1 2 840 113549 1 1 1)
	public key	IA	―	2048bit の値
証明書標準拡張部				
authorityKeyIdentifier (認証局鍵識別)		IA	F	
	keyIdentifier			NewWithNew の公開鍵の SHA-1 値(ハッシュ値)

authorityCertIssuer			NewWithNew の issuer の DN
authCertSerialNumber			NewWithNew のシリアル番号
subjectKeyIdentifier (所有者鍵識別)	IA	F	OldWithOld の公開鍵の SHA-1 値(ハッシュ値)
keyUsage(鍵の使用目的)	IA	T	keyCertSign, cRLSign を ON とし、他を OFF とする。
extendKeyUsage(拡張鍵種別)	×	―	設定しない。
privateKeyUsagePeriod (秘密鍵有効期間)	×	―	設定しない。
certificatePolicies (証明書ポリシー)	IA	F	
policyIdentifier			
certPolicyId			(OID=2 5 29 32 0) any-policy
policyQualifiers	×	―	設定しない。
policyQualifierId			
Qualifier			
policyMappings (ポリシーマッピング)	×	―	設定しない。
issuerDomainPolicy			
subjectDomainPolicy			
subjectAltName(所有者別名)	×	―	設定しない。
issuerAltName(発行者別名)	×	―	設定しない。
basicConstraints(基本制約)	IA	T	
cA	IA		TRUE
pathLenConstraint	×		設定しない。
nameConstraints(名称制約)	×	―	設定しない。
policyConstraints (ポリシー制約)	×	―	設定しない。
cRLDistributionPoints (CRL 分配点)	IA	F	distributionPoint.fullName.URL に以下を設定する。 Ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?authorityRevocationList
subjectDirectoryAttributes (所有者ディレクトリ属性)	×	―	設定しない。
証明書プライベートインターネット拡張部			
authorityInfoAccess (認証局情報アクセス)	×	―	設定しない。

7.2 CRL/ARL プロファイル

7.2.1 バージョン番号

本認証業務では、X.509V2 の CRL/ARL を発行する。

7.2.2 CRL/ARL エントリ拡張

本認証業務では、この拡張に設定が可能な項目のうち、理由コード(reasonCode)のみを使用する。

7.2.3 CRL/ARL プロファイル

本認証業務で発行する CRL/ARL のプロファイル詳細を表 7-2 に記述する。なお、電子証明書の記載項目は、特に断りのない限り PrintableString でエンコードされる。

表 7-2(1) CRL プロファイル

名称	設定者	クリティカリティ	設定値
CRL 基本部			
version(バージョン)	IA	－	V2
signature(署名)	IA	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
issuer(発行者)	IA	－	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=AOSign Certification Authority ※C は PrintableString でエンコードする、 その他は UTF8String でエンコードする。
thisUpdate(今回更新日時)	IA	－	CRL 発行日時(UTCTime で設定する。)
nextUpdate(次回更新予定)	IA	－	thisUpdate＋48 時間(UTCTime で設定する。)
revokedCertificates (失効証明書)			
userCertificate	RA	－	証明書シリアル番号
revocationDate	IA	－	失効日時
CRL 拡張部			
authorityKeyIdentifier (認証局鍵識別)	IA	F	
keyIdentifier			公開鍵の SHA-1 値(ハッシュ値)
authorityCertIssuer			issuer の DN
authCertSerialNumber			シリアル番号
issuerAltName (発行者別名)	×	－	設定しない。
cRLNumber(CRL 番号)	IA	F	128bit 以下の正の整数
deltaCRLIndicator (デルタ CRL 識別)	×	－	設定しない。
issuingDistributionPoint (発行分配点)	IA	T	

		distributionPoint			distributionPoint.fullName.URL に以下を設定する。 Ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?certificateRevocationList
		onlyContainsUserCerts			TRUE を設定する。
CRL エントリ拡張部					
		reasonCode(理由コード)	RA	F	理由コードを設定する。

表 7-2(2) ARL プロファイル

名称			設定者	クリティカリティ	設定値
CRL 基本部					
	version (バージョン)		IA	－	V2
	signature(署名)		IA		sha1WithRSAEncryption (OID=1 2 840 113549 1 1 5)
	issuer(発行者)		IA	－	C=JP, O=Nippon Denshi Ninsho Co.Ltd., OU=AOSign Certification Authority ※C は PrintableString でエンコードする、 その他は UTF8String でエンコードする。
	thisUpdate(今回更新日時)		IA	－	ARL 発行日時(UTCTime で設定する。)
	nextUpdate(次回更新予定)		IA	－	thisUpdate＋48 時間(UTCTime で設定する。)
	revokedCertificates (失効証明書)				
		userCertificate	IA	－	証明書シリアル番号
		revocationDate	IA	－	失効日時
CRL 拡張部					
	authorityKeyIdentifier (認証局鍵識別)		IA	F	
		keyIdentifier			公開鍵の SHA-1 値(ハッシュ値)
		authorityCertIssuer			issuer の DN
		authCertSerialNumber			シリアル番号
	issuerAltName (発行者別名)		×	－	設定しない。
	cRLNumber(CRL 番号)		IA	F	128bit 以下の正の整数
	deltaCRLIndicator (デルタ CRL 識別)		×	－	設定しない。
	issuingDistributionPoint (発行分配点)		IA	T	

		distributionPoint			distributionPoint.fullName.URL に以下を設定する。 Ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?authorityRevocationList
		onlyContainsCACerts			TRUE を設定する。
CRL エントリ拡張部					
		reasonCode(理由コード)	IA	F	理由コードを設定する。

8　仕様管理

以下の条項について、本 CPS1.2 節(4)に示す共通 CPS に規定する。

8.1　仕様変更の手続きに関するポリシー

8.2　公表および通知に関するポリシー

8.3　仕様認可の手続き

8.4　CPS の保存

