「AOSign サービス運用規程」

AOSign Service Certificate Policy And Certification Practice Statement

Ver8.00

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

制定日：2002. 8.29
改訂日：2018. 3.19

目　次

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	2002.08.29	・初版発行
1.01	2002.09.20	・GPKI 接続に関する記述の修正 ・問い合わせ先(FAX 番号)の変更
1.02	2002.12.16	・代理人を受取代理人と明確に表示
1.03	2003.06.20	・相互認証証明書のプロファイル変更に係る修正
1.04	2003.07.08	・利用者が企業等に所属していることを証明する書類につき、一部を明示して追加 ・自己署名証明書のフィンガープリントの改ざん検知・防止措置に関する記述を追加 ・書類およびデジタルデータの保存に関し、解りやすく表示 ・本人限定受取郵便の採用形式を明示
1.05	2003.07.31	・表現および用語の整理・統一 ・全般的に解りやすい表現に修正 ・誤記の訂正
1.10	2003.10.24	・動作確認前の受領書返送を可能とした。 ・誤記の訂正
1.20	2003.11.04	・本部マシン室要員別権限表における業務運用者権限を個別付与とした。
2.00	2004.01.08	・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の取扱を追加
2.10	2004.01.20	・利用者等の申込による失効の場合の失効事由の表現を一部修正 ・第三者の失効申込の場合の失効事由の表現を一部修正 ・誤記の訂正
2.20	2004.02.23	・電子証明書に記載される利用者情報の一部追記 ・PIN の受領について郵送方法を変更
2.21	2004.04.01	・誤記の訂正

Ver.	日付	改版内容
2.22	2004.06.25	・表現および用語の整理・統一 ・解りやすい表現に修正 ・誤記の訂正
2.30	2004.08.13	・表現および用語の整理・統一 ・解りやすい表現に修正 ・誤記の訂正、追記 ・真偽の確認方法、電子証明書記載事項の登録の追記
2.40	2004.08.20	・利用者手交時における電子証明書記載事項の確認方法の明示
3.00	2004.12.24	・個人情報保護一部追記 ・発行申込の審査において不備があった書類の取扱について明示 ・手交場所の明示
3.10	2005.02.08	・利用者を確認するための書類について明示 ・表現および用語の整理・統一
3.20	2005.03.01	・企業等に関する情報を確認するための書類について明示
3.30	2005.04.19	・個人情報の取扱いについて整理・修正
3.40	2005.07.29	・表現および用語の整理・統一等 ・本人限定受取郵便上の受取代人について明示 ・市町村合併における確認書類を明示
3.50	2005.10.11	・電子証明書用途範囲の追記 ・継続案内時の取扱について一部追記 ・電子証明書に住所を記載しない場合の一部追記 ・真偽の確認方法、電子証明書記載事項の登録の追記
4.00	2006.01.13	・受領書について、電気通信回線を通じた受付方法を追記 ・企業等に関する情報を確認するための書類について一部追記
4.01	2006.06.07	・用語の整理・統一
4.10	2006.07.26	・表現および用語の整理・統一 ・解りやすい表現に修正
4.20	2006.09.01	・利用者証明書の有効期間改訂
4.21	2007.06.13	・表現および用語の整理・統一
4.22	2007.07.23	・誤記の訂正および表現の整理・修正
5.00	2008.06.23	・自己署名証明書に関する記述の修正 ・リンク証明書についての記述の追加
5.01	2008.06.23	・表現および誤記の修正

Ver.	日付	改版内容
5.02	2008.07.22	・新世代の自己署名証明書、リンク証明書、これら証明書のフィンガープリントについて、運用・公開開始時期を追記
5.03	2008.08.01	・新世代の自己署名証明書等の運用開始に伴い、運用・公開開始時期についての記述を削除
5.10	2008.08.11	・用語の整理 ・解りやすい表現に修正
5.20	2009.01.21	・ＩＣカードを代理人に郵送・手交する際のＰＩＮ送付方法の変更時期を追記
5.21	2009.04.28	・利用者に関する情報を確認するための書類について一部追記 ・ＩＣカードを代理人に郵送・手交する際のＰＩＮ送付方法の変更時期を削除 ・誤記の修正
5.22	2009.06.08	・相互認証証明書を失効させる場合について表現の修正と一部追記
5.30	2009.08.13	・旧姓を利用者の固有名称とする申込での真偽確認方法について追記 ・代理人による利用申込について追記
5.40	2009.12.28	・利用者住所(ローマ字)の電子証明書への記載について追記
5.50	2010.07.21	・認証局終了の際の手続きについて一部追記 ・誤記の修正
5.60	2012.07.06	・郵便為替を普通為替または定額小為替に修正 ・外国人の定義について追記 ・利用者に関する情報を確認するための書類について一部追記 ・表現および用語の整理・修正、誤記の訂正
5.70	2012.07.09	・外国人の定義について一部削除 ・利用者に関する情報を確認するための書類について一部削除
5.80	2012.10.09	・利用者に関する情報を確認するための書類の記述について修正 ・デジタルデータとしてアーカイブする情報の追記
6.00	2013.02.03	・センタ変更に伴う修正
6.01	2013.04.30	・誤記の修正
6.10	2013.07.04	・失効申込に係る記述の修正 ・用語の整理
6.20	2013.12.24	・失効に係る手続きの変更 ・認証業務規程の体系変更に伴う修正
6.30	2014.02.25	・表現および誤記の修正

6.31	2014.03.24	・表現の統一
6.32	2014.04.10	・認証業務規程の構成変更に伴う修正
7.00	2014.08.01	・AOSignG2 認証局設立に伴う追記
7.10	2014.10.08	・AOSign 認証局の受付停止に伴う修正
7.11	2015.03.23	・表現および誤記の修正
7.12	2016.03.22	・表現および誤記の修正
7.20	2016.08.05	・人的セキュリティ管理に係る記述の修正
7.30	2016.11.01	・電子証明書の有効期間の追加に伴う修正
7.40	2017.04.17	・手続的セキュリティ管理に係る記述の修正
8.00	2018.03.19	・発行申込方法の追加に伴う修正 ・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、CALS/EC(Continuous Acquisition and Life-cycle Support／Electronic Commerce：公共事業支援統合情報システム)および e-Japan 重点計画に基づく電子政府・電子自治体の推進に対する貢献等を通じてインターネット社会の健全な発展に寄与することを目的として、電子認証サービスである AOSign サービス(以下、「本サービス」という。)を提供する。

(2) 本サービスに属する認証業務はそれぞれの認証局(以下、「認証局」という。)により運営する。NDN は、認証局の運営を通してインターネット社会の中で電子認証が一般的に広く普及し、これにより安全な電子商取引や電子申請等の確保が促進されるよう、電子認証事業の普及発展に努力する。

(3) 本サービスに属する認証業務は、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、本サービスの内容には、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。

(4) 本サービスにおける利用者は、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、本サービスが、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、本サービス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。

(5) NDN は、本サービス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。)および認証業務ごとに運用規程(以下、「個別 CPS」という。)を定めて公開する。同一の条項において、共通 CPS および個別 CPS それぞれに記述がある場合、両方の記述に従う。
共通 CPS および個別 CPS は、認証局に関係する登場者に適用され、また本サービスで発行する電子証明書から参照され関連付けられる。
その他、本サービスの運営のため、共通 CPS および個別 CPS に基づいて「AOSign サービス業務取扱要領」(以下、「業務取扱要領」という。)および関連手順書を定める。

(6) 本サービスで発行する電子証明書を利用する者は、共通 CPS および利用する認証業務の個別 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認証業務ごとに定める利用規約(以下、「利用規約」という。)のうち利用する認証業務の利用規約に、電子証明書を受信する検証者は認証業務ごとに定める検証者同意書(以下、「検証者同意書」という。)のうち利用する認証業務の検証者同意書に同意しなくてはならない。

(7) 共通 CPS および個別 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。

(8) 認証局はブリッジ認証局(BCA)と相互認証を行う。

1.3 正式名称

NDN の名称以下、本サービスおよび共通 CPS 等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	Nippon Denshi Ninsho Co.,Ltd.
1.2.392.200122.1	AOSign Service
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
1.2.392.200122.1.11	AOSign Service G2 CPS
1.2.392.200122.1.12	AOSign Service G2 Policy for certificates
1.2.392.200122.1.13	AOSign Service G2 Policy for cross-certificate between BCA
1.2.392.200122.1.14	AOSign Service G2 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

本サービスに属する認証業務の名称を以下のとおり定める。

(1)「AOSign サービス」(AOSign Service)

(2)「AOSign サービス G2」(AOSign Service G2)

1.3.2 規程の名称

共通 CPS および個別 CPS の正式名称を以下のとおり定める。

(1) 共通 CPS

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

(2) AOSign サービスの個別 CPS

AOSign サービスの個別 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。

(3) AOSign サービス G2 の個別 CPS

AOSign サービス G2 の個別 CPS の正式名称は、「AOSign サービス運用規程(AOSignG2

認証局編)」(AOSign Service Certificate Policy And Certification Practice Statement(AOSign G2 Certification Authority Version))と称する。

1.3.3 認証局の名称

認証局の名称を以下のとおり定める。

(1) AOSign サービスを運営する認証局の名称
「AOSign 認証局」(AOSign Certification Authority)

(2) AOSign サービス G2 を運営する認証局の名称
「AOSignG2 認証局」(AOSign G2 Certification Authority)

1.4 コミュニティと適応可能性

1.4.1 登場者と機能に応じた相関関係

本サービスは、表 1-3 の登場者が存在し、図 1-1 において登場者の機能に応じた関連を示す。

表 1-3 登場者とその役割

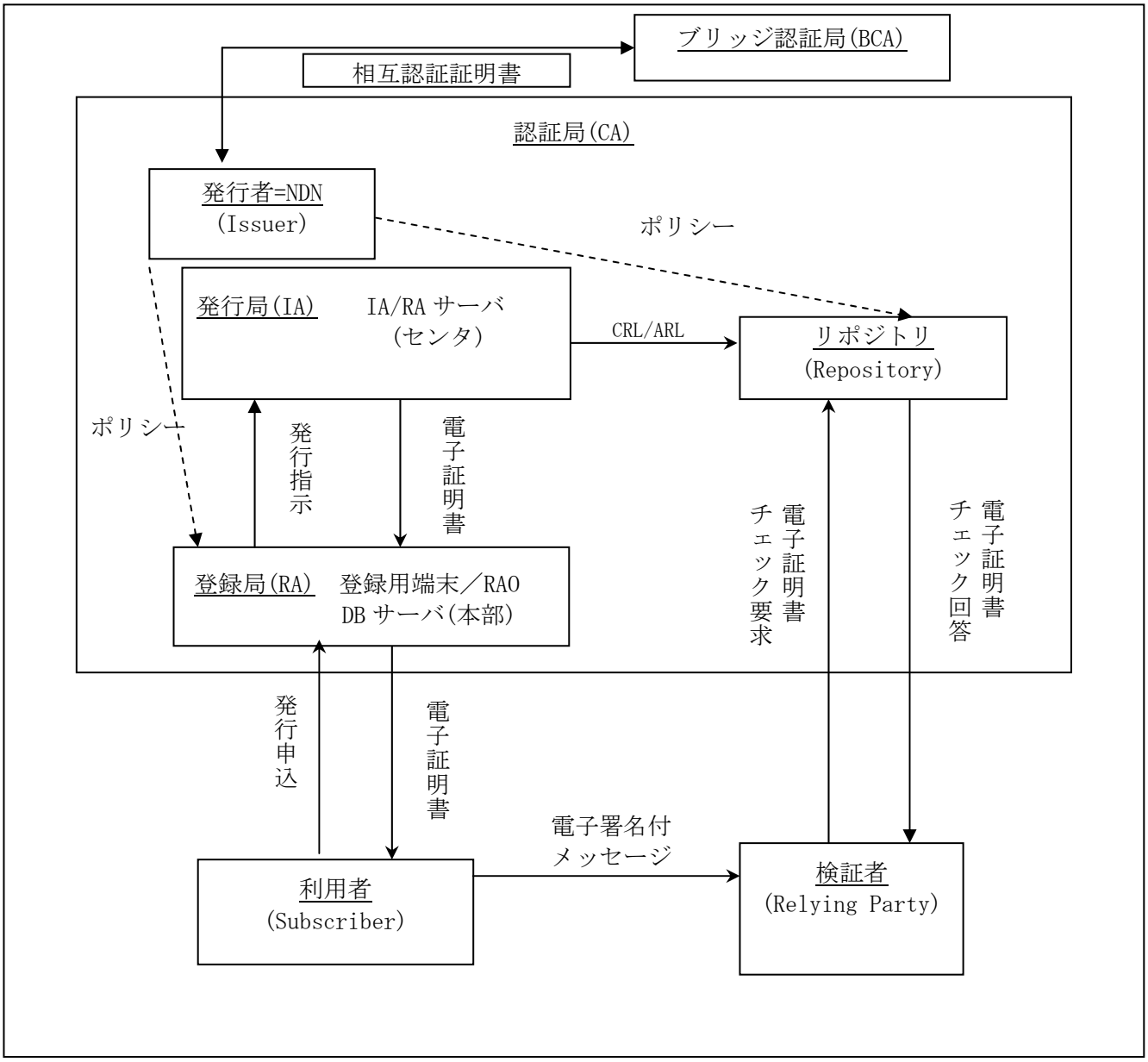
登場者	役　割
個人	国、社会または組織を構成する個々の人。 自然人として法律上の権利義務の主体となり、本サービスにおける電子証明書の利用者となり、検証者となる。 個人は、NDN の規定する共通 CPS、個別 CPS および利用規約に同意の上、利用者となった場合は、利用者としての義務を負い、検証者同意書に同意した場合は検証者としての義務を負う。
利用者 (Subscriber)	NDN と契約を交わし、電子証明書を発行される者 電子証明書の中で、本人の公開鍵と本人の名前を結合される個人 利用者は、NDN の規定する共通 CPS、利用する認証業務の個別 CPS および利用規約に同意し、共通 CPS の利用者の義務に関する条項を遵守しなければならない。
受取代理人	IC カード(電子証明書および秘密鍵)(以下「IC カード」という。)の受取りに関し、利用者からの委任を受ける者。認証局は、AOSign サービス委任状(認証局所定の様式)および受取代理人の印鑑登録証明書の提出を受けることにより受取代理人を名宛人として IC カードを本人限定受取郵便(基本型)にて送付、または手交する。
受取代人	本人限定受取郵便上の受取代人で、名宛人(利用者)に代わって IC カードの受取りができる者。認証局は、委任状(様式不問。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を要件とする。)の提出を受けることにより名宛人を利用者としたうえで、受取代人氏名および住所を併記し、IC カードを本人限定受取郵便(基本型)にて送付する。この場合、郵便局からの通知は利用者本人宛となる。

所有者 (Subject)	本サービスで発行する利用者の電子証明書のプロファイル内の Subject に記載される個人。電子証明書を発行された利用者は、所有者と同義である。
企業等	個人が所属する会社等法人、各種団体および個人企業を総称しての呼称。企業等は、所属する個人に対して、NDN への電子証明書発行申込に同意を行い、共通 CPS、利用する認証業務の個別 CPS および利用規約に基づき、権利を取得し義務を負う。
企業等代表者	利用者の所属する企業等の代表者
検証者 (Relying Party)	利用者の電子証明書を受信して利用者の電子署名を検証する者 本サービスの検証者は、NDN が定める検証者同意書に同意し共通 CPS の検証者の義務に関する条項を遵守しなければならない。
認証局 (CA*[1])	認証局は、発行者、発行局、登録局、リポジトリから構成される。 NDN が運営する認証局の最高責任者は NDN 社長である。 *[1]CA: Certification Authority
電子証明書 (Electronic Certificate)	本人の公開鍵と本人が結合されることを証明する電磁的データ 共通 CPS においては、利用者に対し認証局が発行する Electronic Certificate を電子証明書と呼称している。 なお、本サービスでは、認証局が利用者以外に発行する電子証明書として次のものがある。 ※自己署名証明書：自己署名 CA の電子証明書。旧世代の自己署名証明書を OldWithOld、新世代の自己署名証明書を NewWithNew と呼ぶ。 ※相互認証証明書：ブリッジ認証局と相互認証を行うための電子証明書 ※リンク証明書　：自己署名証明書の新旧世代のリンクを取る電子証明書。新世代から旧世代へのリンクに用いるリンク証明書を OldWithNew と呼び、旧世代から新世代へのリンクに用いるリンク証明書を NewWithOld と呼ぶ。 ※業務運用者用証明書：RAO 証明書 個別 CPS7 章では、これらを含めて証明書と呼称している。
発行者 (Issuer)	NDN は、認証局の運営責任者であり発行者(Issuer)である。 利用者の電子証明書を発行するため、電子証明書署名鍵を発行局に預ける。 実際の発行処理は発行局で行われる。 電子証明書は、利用者、認証局、ブリッジ認証局に発行される。
発行局 (IA*[2])	発行者から委託されて電子証明書署名鍵を預かり、発行者名義の電子証明書および CRL*[3](ARL*[4] を含む。)を発行する。 発行局は、登録局から電子証明書発行の指示を受領して電子証明書を発行する。発行局の運営責任者は NDN 社長である。また、発行局の業務運用上の統括責任者は、運用責任者である。 発行局のコンピュータシステムは、認証局のセンタに設置される FIPS140-2 レベル 3 相当の暗号化装置が接続された IA/RA サーバから構成される。 *[2]IA: Issuing Authority *[3]CRL: Certificate Revocation List ： 電子証明書失効リスト。 CA が発行する失効(無効化)した電子証明書の一覧。検証者は、電子証明書の有効性検

	証の一環としてこのリストを参照し、検証対象電子証明書が無効化していないか確かめなければならない。 *4ARL: Authority Revocation List
IAO*5	IA を管理し運営する者。　　*5IAO: IA Officers
登録局 (RA*6)	登録局は、電子証明書の発行に関連する次の機能を実行する。 ・電子証明書発行申込受付 ・利用者の真偽確認 ・企業等の真偽確認 ・IA に電子証明書発行の指示 ・電子証明書と秘密鍵の利用者への発行 ・電子証明書失効決定 ・IA へ電子証明書失効処理の指示 登録局のコンピュータシステムは、仮想専用線を使用して発行局と閉域網接続される。 登録局の業務運用上の統括責任者は、業務運用管理者である。 *6RA: Registration Authority
自己署名 CA	証明階層経路の頂点に位置し、自己署名し、電子証明書の発行を行う CA 本サービスでは認証局が BCA と相互認証をする。
業務運用者 (RAO*7)	電子証明書発行または失効の指示操作および相互牽制にて承認する者 *7RAO: RA Officers
リポジトリ (Repository)	CRL、ARL および本サービスに関連するその他の情報を保管するディレクトリや Web の総称 検証者や利用者の便宜に供す。
ブリッジ認証局 (BCA*8)	行政機関側認証局と民間側認証局との中間に位置し、それぞれと相互認証をする政府により運営されるブリッジ認証局 *8BCA: Bridge CA

図 1-1 登場者の機能関連図

認証局のスキーム



1.4.2　認証業務の形態

本サービスに属する認証業務の概要を以下の表 1-4 および表 1-5 に示す。

表 1-4　AOSign サービスの形態

項　　目				内　　容
サービス名称				AOSign サービス
NDN との契約者				利用者および所属する企業等
認定認証事業者				NDN
電子証明書	識別名（属性）	利用者	氏名	必須
			住所	原則必須(※)
		企業等名称		必須
	鍵の使用目的	電子署名		必須
		否認防止		必須
		鍵暗号化		不可
		データ暗号化		不可
		鍵共有		不可
認証サービスの運営	認証局	発行者		NDN
	発行局	発行局コンピュータ運用		委託先ベンダ
		電子証明書署名鍵生成、管理		委託先ベンダ
	登録局	登録局コンピュータ運用		委託先ベンダ
		真偽確認		NDN
		発行指示/失効指示		NDN
	認定にかかわる書類の管理			NDN＋委託先ベンダ

※　ただし、利用者より申し出があった場合は電子証明書に記載しない。

表 1-5　AOSign サービス G2 の形態

項　　目				内　　容
サービス名称				AOSign サービス G2
NDN との契約者				利用者および所属する企業等
認定認証事業者				NDN
電子証明書	識別名（属性）	利用者	氏名	必須
			住所	任意(※)
		企業等名称		必須
	鍵の使用目的	電子署名		必須
		否認防止		必須
		鍵暗号化		不可
		データ暗号化		不可
		鍵共有		不可
認証サービスの運営	認証局	発行者		NDN
	発行局	発行局コンピュータ運用		委託先ベンダ
		電子証明書署名鍵生成、管理		委託先ベンダ
	登録局	登録局コンピュータ運用		委託先ベンダ
		真偽確認		NDN
		発行指示/失効指示		NDN
	認定にかかわる書類の管理			NDN＋委託先ベンダ

※　利用者より届出があった場合は電子証明書に記載する。

1.4.3　電子証明書の用途範囲

(1) 本サービスで発行する電子証明書は、利用者が利用者の所属する企業等の命令を受けて電子的な取引や電子的記録の通信を行うためにある。
具体的には、電子調達、電子申請、電子商取引、電子文書保存を行うときに使用する。

(2) 本サービスでは、政府が運営する BCA と相互認証することにより、民側の利用者と官側の権限者との間で相互に電子証明書を検証するための電子証明書パスを構築できるようにする。

(3) 利用者は、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を確認して、本サービスから発行する電子証明書の適否を判断する必要がある。用途範囲外の使用に対しては、本サービスの責任対象外である。

1.4.4　業務運用関連法令に対する遵法精神

本サービスで提供する認証業務は、電子署名法に基づく認定認証業務である。同法令の立法趣旨を踏まえて、インターネット社会の通信基盤として安全かつ確実なサービスを提供する。

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

本サービスにおいて、利用者の電子証明書に記載する利用者の属性情報(住所・氏名を除く。)は、電子署名法の認定対象外である。

1.5　連絡先の詳細

共通 CPS および個別 CPS は、リポジトリにて公開される。利用者は、定期的にアクセスし、新規サービス内容や仕様変更について把握し、承知しなければならない。
利用者は、本サービスの内容について知りたいとき、電話等を使って問い合わせることができる。

［問い合わせ先］

日本電子認証株式会社
住所　：〒104-0045
　　東京都中央区築地 5-5-12 浜離宮建設プラザ
名称　：ヘルプデスク
受付時間：9:00～17:00(土曜日、日曜日、祝日、年末年始を除く。)
※ 年末年始の休業日は Web にて掲示する。
　URL：http://www.ninsho.co.jp/aosign/
TEL　：0120-714-240
FAX　：03-5148-5695
E-mail：toiawase@ninsho.co.jp

2　一般的な規定

2.1　義務

NDN は、本サービスに属する認証業務における発行者として、各登場者の義務を以下のとおり定める。

2.1.1　発行局(IA)の義務

IA は、以下に示す原則の下、共通 CPS および実施する認証業務の個別 CPS に従って運用する。

(1) 電子署名法の定めに従い、電子証明書署名鍵をセキュアな環境で生成し、管理する。
(2) RA の発行指示に基づき利用者の電子証明書を発行する。
(3) RA と協調して電子証明書ライフサイクル管理(発行から失効までの一貫した管理)を行う。
(4) RA の失効指示に基づき利用者の電子証明書を失効させ、CRL を発行する。
(5) IA/RA サーバを電子署名法の定めるセキュアな環境に設置し運用する。
(6) システムの稼動監視を行う。
(7) 本サービスでは、これに加えて以下の GPKI(Government Public Key Infrastructure)接続要件に従うものとする。
①BCA への相互認証申請に際して、正確な情報を提示する。
②共通 CPS に基づき、自己署名証明書、リンク証明書、相互認証証明書の発行および失効を行う。相互認証証明書の取り交わしに関しては、BCA の定める手続に従う。
③GPKI 接続要件に従って、CRL に加えて ARL を発行する。
④電子証明書署名鍵の危殆化(盗難、漏えい等により他人によって使用され得る状態になることをいう。以下同じ。)の際、すみやかに BCA 運営組織にも報告する。
⑤電子証明書の発行、失効等に関する監査ログおよびアーカイブデータ(Archive Data)については個別 CPS の定めに従い、保管する。

2.1.2　登録局(RA)の義務

RA は、以下に示す原則の下、共通 CPS および実施する認証業務の個別 CPS に従って運用する。

(1) 個別 CPS3 章および 4 章の規定に従い電子証明書の発行、失効等に係る処理を適正に行う。
(2) 個別 CPS7 章で規定されたプロファイル(Profile)に定義された名称については、実体を適切に表示していることを確認する。
(3) 利用者の公開鍵と秘密鍵を生成後、IC カードに電子証明書と秘密鍵を格納し、利用者に安全かつ確実に IC カードを配付する。
(4) 個別 CPS の定めに従い、発行申込書に記述されている利用者が本人であることの真偽の確認を行う。
(5) 利用者の電子証明書を失効させる場合、失効の妥当性の確認を行う。
(6) 発行申込書の記載情報は、個人情報、秘密情報として取扱う。

(7) IA と協調して電子証明書ライフサイクル管理を行う。
(8) 電子証明書発行に関連するその他の情報をすみやかにリポジトリにて公開する。
(9) 本サービスでは、これに加えて以下の GPKI 接続要件に従うものとする。
①BCA からの相互認証証明書発行要求に含まれる公開鍵が確実に BCA の公開鍵であり、かつ BCA がこの公開鍵に対応する秘密鍵を保有していることを確認する。

2.1.3 利用者の義務

利用者は、共通 CPS、利用する認証業務の個別 CPS および利用規約に同意し、以下の義務を負う。

(1) 企業等の同意を受けた発行申込
利用者は、企業等の同意に基づき電子証明書の発行申込を行う。また AOSign サービス G2 において、利用者が現に有している電子証明書を利用して新たに発行申込を行う場合には、利用者は電子証明書記載事項の内容に変更がないことを確認し、所属する企業等の同意を得た上で申込む。

(2) 正確な発行申込内容の提示
電子証明書の発行申込を行う際、申込内容を正確に提示しなければならない。
虚偽の発行申込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 条の規定により罰せられる。

(3) 利用制限
電子証明書はその用途範囲、損害賠償等を記載した共通CPSに基づき発行される。
利用者は、その範囲外の用途に電子証明書を利用してはならない。

(4) 検証者による利用
利用者の電子証明書を検証者が利用することに関して、その電子証明書がどのような取引において使用されるか、また特定の用途、局面に適合しているか等の審査、確認を NDN は行わないことについて、利用者は承知しなければならない。

(5) IC カード等の秘匿管理
電子署名は、自署や押印に相当する法的効果が認められ得るものであるため、利用者は、電子証明書および秘密鍵が格納されている IC カードおよび IC カードを使用する際に求められる PIN(本人識別のキーコード、Personal Identification Number の略称。以下同じ。)の情報を他人に知られないように、充分な注意をもって管理しなければならない。
したがって、IC カードを他人に貸与、譲渡または質入れなどの行為を絶対にしてはならない。

(6) 電子証明書記載事項の管理
利用者は発行された電子証明書の記載事項を受領時に確認し、かつその後も使用前に随時、利用者の現状に照らして確認しなければならない。
利用者は電子証明書受領時にその記載事項が利用者の現状に合わなかった場合、または電子証明書受領後にその記載事項が利用者の現状に合わなくなった場合は、失効申込を行わなければならない。

(7) 迅速な失効申込
利用者は、秘密鍵が危殆化した場合、もしくは危殆化したおそれがある場合、電子証明書の記載内容に変更が生じた場合および電子証明書の利用を中止する場合においては、遅滞なく電子証明書の失効申込を行わなければならない。

(8) 企業等もしくは第三者による失効届出に対する同意
やむを得ない理由により利用者が失効申込をできない事象が発生した場合、企業等もしくは第三者が失効届出をすることに対し、予め同意しなければならない。
(9) 署名アルゴリズム
①AOSignサービスの署名アルゴリズム
AOSignサービスで提供する署名アルゴリズムは、sha1WithRSAEncryptionである。利用者はこれを承知しなければならない。また、利用者が用途範囲で用いる署名アルゴリズムは「sha1WithRSAEncryption」、「sha256WithRSAEncryption」、「sha384WithRSAEncryption」または「sha512WithRSAEncryption」とする。
②AOSignサービスG2の署名アルゴリズム
AOSignサービスG2で提供する署名アルゴリズムは、sha256WithRSAEncryptionである。利用者はこれを承知しなければならない。また、利用者が用途範囲で用いる署名アルゴリズムは「sha1WithRSAEncryption」、「sha256WithRSAEncryption」、「sha384WithRSAEncryption」または「sha512WithRSAEncryption」とする。
(10)認証局への確認
利用者は、上記各事項に係る解釈については認証局の判断に従わなければならない。したがって、利用者は認証局へ必要に応じて確認する必要がある。

2.1.4 利用者の所属する企業等の義務

利用者の電子証明書の発行申込に同意した企業等は、以下の義務を負う。
(1) 利用者が電子証明書の申込を行うことに対して同意した企業等は、その証として発行申込書に利用者とともに記名押印(代表者印)する。
(2) 企業等は、共通 CPS、利用する認証業務の個別 CPS および利用規約を遵守しなくてはならない。
(3) 企業等は、原則として本サービスに係る費用を支払う。
(4) 電子証明書の失効申込について、やむを得ない理由により利用者が失効申込をできない事象が発生した場合、企業等が失効届出を行う義務を負う。
(5) AOSign サービス G2 において、利用者は現に有している電子証明書を利用して継続・追加に伴う発行申込を行うことができる。当社は、当該方法で行われた発行申込については企業等の同意が得られているものとみなす。企業等は、その事に対して予め同意しなくてはならない。

2.1.5 検証者の義務

検証者は、利用する認証業務の検証者同意書に同意しなければならない。検証者同意書の URL は、電子証明書の certificatePolicies 項目に表示する。検証者同意書に記述されているように、検証者は、取引相手である利用者の電子証明書の有効性について確認しなければならない。また、電子証明書の有効性確認に当たり必要な情報(CRL、自己署名証明書(OldWithOld または NewWithNew)およびそのフィンガープリント、必要に応じリンク証明書(OldWithNew または NewWithOld)およびそのフィンガープリント)をリポジトリから入手しなければならない。URL については、共通 CPS2.6.4 項を参照。
(1) 利用制限
電子証明書はその使用目的、用途範囲、利用者の真偽の確認方法、損害賠償等を

記述した共通 CPS および利用する認証業務の個別 CPS に基づいて運用されており、検証者はこれらを理解し、承認したうえで電子証明書を利用しなければならない。検証者は、利用者から提示された電子証明書の使用目的に疑義があると判断する場合、電子証明書を受け入れてはならない。また転用してもならない。

(2) 有効性確認義務

電子署名の検証等、電子証明書を利用する際には有効性確認を行わなければならない。有効性確認内容には以下を含まなければならない。

①電子証明書パス上のすべての証明書について以下を確認すること

- すべての証明書が改ざんされていないこと
- 有効期間内であること
- 失効していないこと
- 利用者の電子証明書の電子署名を検証すること

②提示された電子証明書の記載項目(特に subject および subjectAltName 項目)が、個別 CPS7 章の規定に一致していること

2.1.6 リポジトリの義務

認証局は、検証者が電子証明書の有効性検証ができるよう CRL/ARL を公開し、電子証明書発行に関連するその他の情報を公開する義務を負う。

CRL/ARL および電子証明書発行に関連するその他の情報は、共通 CPS2.6.4 項に基づきリポジトリにて公開され、認証局は同リポジトリを運営する。

2.2 責任

(1) NDN は、認証局の運営責任者として、利用者および企業等に対しては、共通 CPS、個別 CPS および利用規約に基づいて、また検証者に対しては、共通 CPS、個別 CPS および検証者同意書に基づいて、それぞれ以下のとおり本サービスを提供する責任を有する。

①電子証明書の発行申込に対して、利用者の真偽の確認を実施すること

②電子証明書の発行申込内容を正確に記載した電子証明書を発行すること

③秘密鍵と公開鍵ペアを生成後、電子証明書(公開鍵を含む。)と秘密鍵を格納した IC カードを利用者に安全かつ確実に配付すること

④本サービスで発行する CRL/ARL について、システム保守等の理由による一時停止、やむを得ない場合の停止を除き、作成後、定期的にリポジトリに登録し、電子証明書の有効期間が満了するまで公開し続けること

⑤失効申込または失効届出を確認・受理した場合、失効申込または失効届出対象の電子証明書について確実に失効処理を行うこと

⑥共通 CPS5 章および 6 章の規定に従い、電子証明書発行システムを運用し、電子証明書署名鍵について、危殆化することがないように管理すること

⑦電子証明書、CRL/ARL の形式が、それぞれの発行時点において個別 CPS7 章の規定に一致していること

⑧利用者の真偽の確認のため使用した書類を含む各種の帳簿書類を、漏えい、滅失またはき損、改ざん等のおそれのない方法で、電子署名法の定める期間保管すること

(2) NDN は、以下のいずれかの場合には、利用者、企業等および検証者に通知することなく、一時的に本サービスの全部または一部の提供を中断することができる。
①本サービス用の設備につき、緊急に保守を行う場合
②火災、停電等により本サービスの提供ができなくなった場合
③地震、噴火、洪水、津波等の天災により本サービスの提供ができなくなった場合
④戦争、動乱、暴動、騒乱、労働争議等により本サービスの提供ができなくなった場合
⑤電気通信事業者が電気通信サービスを中断又は中止した場合
⑥その他、運用上、技術上または契約の履行上、NDN が本サービスの提供を一時中断する必要があると判断した場合
(3) 本サービスでは、これに加えて以下の GPKI 接続要件に従うものとする。
①自己署名証明書、リンク証明書、相互認証証明書等の発行、更新、失効、保管および公開にあたっては、BCA、利用者および検証者に対し、共通 CPS および個別 CPS に基づく認証業務を適切に行う。
②BCA に対する相互認証証明書の発行にあたっては、「政府認証基盤におけるブリッジ認証局の相互認証基準について」(平成 13 年 4 月 25 日行政情報化推進各省庁連絡会議幹事会了承)に定める基準に適合し、BCA の意思決定組織による相互認証実施の決定に基づく。

2.3 財務責任

NDN は、本サービスの提供が電子社会における重要なセキュリティ基盤事業の遂行であることを自覚し、利用者等に対し安心および信頼を与え続けることのできる経営内容を堅持し、常に健全な財務を維持する責任を負っている。

2.3.1 賠償責任

(1) NDN の賠償責任
NDN が共通 CPS2.2 節に規定する責任に違反して損害賠償責任を負う場合は、利用者および企業等に対しては別途利用規約で定める金額を、また検証者に対しては検証者同意書で定める金額を上限とする。
ただし、NDN の責に帰すことができない事由から生じた損害、NDN の予見の有無を問わず特別の事情から生じた損害、逸失利益については、賠償責任を負わない。
なお、本サービスは、GPKI における BCA との相互認証を行うものであり、官職を有する検証者(官側の処分権者)に対し NDN が損害賠償の責任を負う場合の損害賠償額については共通 CPS を適用しない。
(2) 利用者の賠償責任
共通 CPS2.1.3 項(3)に規定する利用者による電子証明書利用制限において、利用者が範囲外の用途に電子証明書を利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し、当該トラブルにより NDN が損害を被った場合は、NDN は、利用者に対し当該損害の賠償を請求することができる。
また、共通 CPS2.1.3 項(7)に規定する失効申込において、利用者が失効申込義務を怠ったことにより生じた第三者によるなりすまし、検証者による誤判断等のト

ラブルについては、利用者が一切の責任を負うものとし、当該トラブルにより NDN が損害を被った場合は、NDN は利用者に対し当該損害の賠償を請求することができる。

(3) 企業等の賠償責任

企業等が、共通 CPS2.1.4 項(4)に規定する失効に関する義務を履行しなかったことにより、NDN が損害を被った場合、NDN は企業等に対し当該損害の賠償を請求することができる。

(4) 検証者に対する賠償責任

共通 CPS2.1.5 項(1)に規定する電子証明書利用制限において、検証者が使用目的外で電子証明書を使用した結果被った損害については、検証者が一切の責任を負うものとし、NDN は何ら賠償責任を負わない。

また、共通 CPS2.1.5 項(2)に規定する検証者による電子証明書の有効性確認は、一般的には使用するソフトウェアにより自動的に行われるものであるが、最終判断は検証者の責任であり、検証者が有効性を確認できないにもかかわらず取引等した結果被った損害については、NDN は何ら賠償責任を負わない。

2.3.2 信頼関係

NDN は、公共工事の前払金保証事業会社(北海道建設業信用保証株式会社、東日本建設業保証株式会社、西日本建設業保証株式会社)、金融機関、建設企業および IT ベンダから出資を得ている。

また、NDN は日本電気株式会社に業務の一部を委託している。

2.3.3 会計原則

日本国商法に基づく企業会計原則による。

2.4 解釈および執行

2.4.1 準拠法

共通 CPS および個別 CPS は、日本国内法令に基づき解釈される。

2.4.2 分離、存続、合併、通知

本サービスが、細分化されたり、他サービスを統合したり、または他サービスに統合される場合、NDN は本サービスを実質的に継続すべく最善を尽くす。

上記に伴い共通 CPS および個別 CPS の変更が必要とされる場合には、共通 CPS8 章の規定に従う。

2.4.3 紛争解決手続

利用者、企業等または検証者と NDN 間に訴訟や法的行為が起こる場合、東京地方裁判所を専属的合意管轄裁判所とする。

共通 CPS、個別 CPS、利用規約および検証者同意書に定められていない事項やこれらの文書の解釈に関し疑義が生じた場合、各当事者はその課題を解決するために誠意をもって協議する。

2.5 料金

NDN は、本サービスに属する認証業務の基本料金を NDN のホームページに掲載し、所定の料金を電子証明書発行毎に徴収する。ただし、利用状況によっては、一定の割引を行うことができる。

なお、課金体系は、電子証明書発行枚数に単価を乗じて計算することを原則とする。

2.6 公開およびリポジトリ

2.6.1 情報の公開

本サービスに関する情報は、NDN のリポジトリにて公開する。

2.6.2 公開の頻度

(1) 共通 CPS および個別 CPS の公開は、共通 CPS8 章に規定される。
(2) 失効情報については、CRL の形式でリポジトリにて公開する。公開した CRL は、24 時間以内に最新の CRL に更新する。
(3) 失効情報は、電子証明書の有効期間が満了するまでリポジトリにて公開する。
(4) その他の情報については、NDN の判断により、適宜更新される。
(5) 本サービスでは、これに加えて以下の GPKI 接続要件に従うものとする。
①自己署名証明書、リンク証明書、相互認証証明書および CRL/ARL は、発行および更新の都度公開される。
②相互認証した認証局の名称および相互認証を取り消した認証局の名称は、仕様管理委員会による審議を経た決定の都度公開される。

2.6.3 アクセスコントロール

自己署名証明書(OldWithOld、NewWithNew)およびリンク証明書(OldWithNew、NewWithOld)について、電子証明書およびそのフィンガープリントを公開するサーバについては、通信路の暗号化およびフィンガープリントの改ざん検知・防止措置を施し、フィンガープリントの改ざんを検知した場合は、速やかに復旧措置を取る。

2.6.4 リポジトリ

(1) CRL/ARL および本サービスに関連するその他の情報は、認証局毎に定めるリポジトリにて公開される。ただし、利用者の電子証明書は公開されない。
(2) リポジトリへは NDN のホームページからアクセスすることができる。ただし、CRL/ARL については電子証明書記載のアクセス手段およびアドレスによる。
(3) リポジトリは、24 時間運用される。ただし、システムの保守等の理由により、事前に NDN のホームページで告知し、一時停止することがある。なお、やむを得ない場合は、事前に連絡できないことがある。
(4) 本サービスに属する認証業務のリポジトリにて公開される情報およびリポジトリの URL は、表 2-1 および表 2-2 で示す。

表 2-1　AOSign サービスのリポジトリの主な内容

	文書名	対象	公開方法
規約	AOSign サービス運用規程	関与者全員	https
	AOSign サービス運用規程 (AOSign 認証局編)	関与者全員	https
	AOSign サービス利用規約	利用者、企業等	https
	AOSign サービス検証者同意書	検証者	https
電子証明書他	自己署名証明書 (OldWithOld、NewWithNew)	利用者、検証者	LDAP(*2)
			https
	自己署名証明書 (OldWithOld、NewWithNew)の フィンガープリント(*1)	利用者、検証者	https
	リンク証明書 (OldWithNew、NewWithOld)	利用者、検証者	LDAP(*2)
			https
	リンク証明書 (OldWithNew、NewWithOld)の フィンガープリント(*1)	利用者、検証者	https
	相互認証証明書	利用者、検証者	LDAP(*2)
	CRL/ARL	検証者	LDAP(*2)
告知書	NDN からのお知らせ	関与者全員	http

注)リポジトリの URL は、以下のとおりとする。

AOSign サービス運用規程、AOSign サービス運用規程(AOSign 認証局編)の URL	https://rep.ninsho.co.jp/aosign/cps.html
AOSign サービス利用規約の URL	https://rep.ninsho.co.jp/aosign/sa.html
AOSign サービス検証者同意書の URL	https://rep.ninsho.co.jp/aosign/rpa.html

自己署名証明書 (OldWithOld、NewWithNew) の URL(*2)	ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?cACertificate https://rep.ninsho.co.jp/aosign/ca-cert/index.html
自己署名証明書 (OldWithOld、NewWithNew) のフィンガープリントの URL	https://rep.ninsho.co.jp/aosign/ca-cert/index.html
リンク証明書 (OldWithNew、NewWithOld) の URL(*2)	ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?cACertificate https://rep.ninsho.co.jp/aosign/ca-cert/index.html
リンク証明書 (OldWithNew、NewWithOld) のフィンガープリントの URL	https://rep.ninsho.co.jp/aosign/ca-cert/index.html
相互認証証明書の URL(*2)	ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?crossCertificatePair
CRL の URL(*2)	ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?certificateRevocationList
ARL の URL(*2)	ldap://vnec3.jcsinc.co.jp/ou=AOSign%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?authorityRevocationList
NDN ホームページの URL (NDN からのお知らせ)	http://www.ninsho.co.jp

*1　証明書を SHA-1 で変換した値。

*2　LDAP(Lightweight Directory Access Protocol)の使用は GPKI 接続条件である。

表 2-2　AOSign サービス G2 のリポジトリの主な内容

	文書名	対象	公開方法
規約	AOSign サービス運用規程	関与者全員	https
	AOSign サービス運用規程 (AOSignG2 認証局編)	関与者全員	https
	AOSign サービス G2 利用規約	利用者、企業等	https
	AOSign サービス G2 検証者同意書	検証者	https
電子証明書他	自己署名証明書 (OldWithOld、NewWithNew)	利用者、検証者	LDAP(*2)
			https
	自己署名証明書 (OldWithOld、NewWithNew)の フィンガープリント(*1)	利用者、検証者	https
	リンク証明書 (OldWithNew、NewWithOld)	利用者、検証者	LDAP(*2)
			https
	リンク証明書 (OldWithNew、NewWithOld)の フィンガープリント(*1)	利用者、検証者	https
	相互認証証明書	利用者、検証者	LDAP(*2)
	CRL/ARL	検証者	LDAP(*2)
告知書	NDN からのお知らせ	関与者全員	http

注)リポジトリの URL は、以下の通りとする。

AOSign サービス運用規程、AOSign サービス運用規程(AOSignG2 認証局編)の URL	https://rep.ninsho.co.jp/aosign/cps.html
AOSign サービス G2 利用規約の URL	https://rep.ninsho.co.jp/aosign/sa.html
AOSign サービス G2 検証者同意書の URL	https://rep.ninsho.co.jp/aosign/rpa.html

自己署名証明書 (OldWithOld、NewWithNew) の URL(*2)	ldap://ldap.aosign.com/ou=AOSign%20G2%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?cACertificate https://rep.ninsho.co.jp/aosign/ca-cert/index.html
自己署名証明書 (OldWithOld、NewWithNew) のフィンガープリントの URL	https://rep.ninsho.co.jp/aosign/ca-cert/index.html
リンク証明書 (OldWithNew、NewWithOld) の URL(*2)	ldap://ldap.aosign.com/ou=AOSign%20G2%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?cACertificate https://rep.ninsho.co.jp/aosign/ca-cert/index.html
リンク証明書 (OldWithNew、NewWithOld) のフィンガープリントの URL	https://rep.ninsho.co.jp/aosign/ca-cert/index.html
相互認証証明書の URL(*2)	ldap://ldap.aosign.com/ou=AOSign%20G2%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?crossCertificatePair
CRL の URL(*2)	ldap://ldap.aosign.com/ou=AOSign%20G2%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?certificateRevocationList
ARL の URL(*2)	ldap://ldap.aosign.com/ou=AOSign%20G2%20Certification%20Authority,o=Nippon%20Denshi%20Ninsho%20Co.Ltd.,c=JP?authorityRevocationList
NDN ホームページの URL (NDN からのお知らせ)	http://www.ninsho.co.jp

*1　証明書を SHA-256 で変換した値。

*2　LDAP(Lightweight Directory Access Protocol)の使用は GPKI 接続条件である。

2.7　準拠性監査

NDN は、本サービスを運用するに際して、共通 CPS、個別 CPS および業務取扱要領等に準拠して業務が実施されていることを検証するために監査を定期的に行う。

2.7.1　監査の頻度

監査は、以下の時点に実施される。

(1) 年 1 回(電子署名法に基づく認定更新に先立って実施)

(2) セキュリティに関係する重要な更改を行う都度

2.7.2　監査人の身元保証・資格

監査人は、準拠性監査に充分なスキルと経験を有した者を選定する。

2.7.3　被監査部門と監査人の関係

監査人は、認証局運用部門に所属しない者から選定する。

2.7.4　監査の対象となるトピック

(1) NDN は、監査を行うために監査基準、規則と手順を定め、目的、監査組織、スケジュール、監査対象、作業要領、改善状況を明確にする。

(2) 認証業務が共通 CPS、個別 CPS および業務取扱要領等に準拠して実施されていること、ならびに外部からの不正および内部の不正行為に対する措置が適切に講じられていることを中心に監査を行う。

2.7.5　監査指摘事項に対する措置

NDN は、監査の結果、指摘事項があった場合には、可及的すみやかに改善する。

なお、本サービスでは、これに加えて以下の GPKI 接続要件に従うものとする。

(1) 重要または緊急を要する監査指摘事項については、すみやかに対応する。電子証明書署名鍵の危殆化に関する指摘があった場合は緊急事態と位置づけ、緊急時対応の手続をとる。

(2) 重要または緊急を要する監査指摘事項が改善されるまでの間、新たに電子証明書を発行する等の本サービスを中断するか否かは仕様管理委員会で決定する。また NDN は、監査指摘事項に対して対策が実施されたことを確認する。

2.7.6　監査結果の報告

NDN は監査の結果を公表しない。ただし、指定調査機関の求めに応じて、監査結果を開示する。

なお、本サービスでは、GPKI 接続要件に従って、監査結果を BCA 運営組織に報告する。

2.8　秘密保持

2.8.1　秘密が保たれる情報

NDN は、本サービスに関連して相手方から(i)秘密である旨明示された書面によりされ、または(ii)秘密である旨明確に告げられて口頭によりされ、かつ当該後 14 日以内に書面

により確認された秘密情報(利用者に関する情報を含む。)について、相手方の書面による事前の承諾を得ることなく第三者に、漏洩しないとともに、本サービスを提供または利用するために必要な範囲をこえて使用しない。

NDN は、利用者からの発行申込、失効申込等に伴って提供または提示される個人情報を本サービスを提供または利用するために必要な範囲をこえて使用しない。

なお、本サービスでは、これに加えて以下の GPKI 接続要件に従うものとする。

(1) 漏洩することによって本サービスおよび BCA の認証業務の信頼性が損なわれるおそれのある情報を秘密扱いとする。

(2) 本部およびセンタそれぞれで管理者を定め、秘密扱いとする情報を含む書類および記録媒体を、安全に保管管理する。

2.8.2 秘密とみなされない情報

共通 CPS2.8.1 項の規定にかかわらず、以下に定める情報は、秘密情報とはみなされない。

(1) 電子証明書および CRL/ARL に含まれるべき情報。ただし、利用者の電子証明書の利用者識別名(利用者別名情報を含む。)を除く。

(2) 共通 CPS および個別 CPS に含まれる情報

2.8.3 失効情報の公開

電子証明書が失効される場合、CRL には失効理由、失効日時が含まれる。

したがって、この失効理由、失効日時は秘密情報とはみなされず、すべての検証者に公開されることになる。

2.8.4 捜査機関等への開示

NDN は、捜査機関、裁判所、弁護士会その他法律上権限を有する者から強制力を伴わない任意の照会があった場合で、正当防衛、緊急避難にあたると判断したときは、利用者等に関して知りうる秘密情報につき、当該捜査機関等に開示できる。

2.8.5 民事手続上の開示

共通 CPS2.8.4 項の規定に含まれる。

2.8.6 電子証明書名義人の要請に基づく開示

NDN は、電子証明書名義人から名義人自身の権利または利益を侵害されている、もしくはそのおそれがあるとして、開示申込書に現金、普通為替または定額小為替により開示申込手数料(別途定める。)を添えて申込があった場合、電子証明書発行申込書と開示申込書の利用者名および利用者の実印(印影)が一致することを確認したうえで、発行申込時に受付けた申込書類一式および電子証明書記載事項を郵送または対面による手交にて開示する。開示申込書記載の利用者氏名が改名等により電子証明書発行申込書記載の利用者氏名と異なる場合は、利用者に対し、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)の提出を求め、氏名を確認する。また、開示申込書に押印された利用者の実印(印影)が、電子証明書発行申込書に押印された実印(印影)と異なる場合は、利用者に対し、印鑑登録証明書の提出を求め、印影を確認する。なお、利用者が現に有している電子証明書を利用して新たに発行された電子証明書に対して申込があっ

た場合は、個別 CPS3.1 節の初期登録時に受付けた発行申込書類を用いて手続きを行う。この場合、初期登録時に受付けた申込書類一式、開示対象の電子証明書記載事項および発行申込データを開示する。

受付方法は郵送または対面(窓口)とし、オンラインによる方法では受付けない。ただし、申込者が、日本国籍を有しない者で住民基本台帳法第三十条の四十五に定める外国人住民(以下、「外国人」という。)であり個人の実印を所有していない場合は、電子証明書の名義人であることを「個別 CPS3.1.8 項(2)③なお書き」に準じ、開示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扱う。

なお、NDN は共通 CPS2.8.4 項および 2.8.5 項に規定する場合を除き、電子証明書名義人以外からの利用者情報に関する要求には応じない。

2.8.7　委託先への情報の開示

NDN は、業務の一部を委託する場合、秘密情報を委託先に開示することができる。その場合、委託契約にて委託先に守秘を義務付ける。

2.9　知的財産権

以下の資産は、NDN に帰属する知的財産とする。

(1) 共通 CPS、個別 CPS、関係規程および各種様式
(2) その他本サービスに関して NDN が作成したもの

2.10 個人情報保護

NDN は本サービスを行うにあたり、入手する個人情報の保護について、NDN 個人情報保護ポリシーに基づき、以下のとおり取り扱う。

(1) 入手する個人情報の位置づけ
入手する個人情報のうちには、利用者の求めの有無にかかわらず NDN に訂正、追加または削除、利用の停止、消去の措置の権限のないものが存在し、電子署名法に基づく保管を義務付けられるものである。

(2) 利用目的の特定
NDN は、本サービスを利用者に提供するために必要とする利用者の個人情報を本サービス提供の目的(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書類を送付することを含む。)および付随する目的(電子証明書の有効期間満了時期を案内する際に、既申込情報を利用し印字した電子証明書発行申込書を添付することを含む。)の範囲内でのみ利用する。
NDN がこの利用目的を変更する場合、共通 CPS8 章の規定に従って、現利用目的と相当の関連性を有すると合理的に認められる範囲内にあることを検討したうえで行う。

(3) 利用目的による制限
NDN は、(2)の目的以外に個人情報を利用しない。
また、第三者から目的外利用を求められた場合、法令に定められた場合を除き、一切これに応じない。

(4) 適正な取得

NDN は、偽りその他不正な手段により個人情報を取得しない。

(5) 取得に際しての利用目的の通知
申込に伴って個人情報を取得する場合は、あらかじめこれら利用目的を利用規約にて通知し、利用者の同意を得る。

(6) 内容の正確性の確保
NDN は、利用者から直接入手した個人情報を正確かつ最新の内容に保つように努める。

(7) 安全管理措置ならびに要員および委託先の監督
NDN は利用者から入手した個人情報に対して、個別 CPS4.7 節および共通 CPS5 章に規定するとおり、情報を取り扱う要員および委託先の監督を含め、その漏洩、滅失、毀損の防止等の措置をとる。

(8) 第三者提供の制限
NDN は、法令の定めに基づき提供しなければならない場合および、守秘義務を課したうえで本サービスの一部を委託する場合を除き、個人情報を利用者以外の第三者に提供しない。

(9) 保有個人情報に関する事項の公開
NDN は、利用目的を本節(2)に、情報の開示、訂正等の手続きを共通 CPS2.8.6 項および利用規約にてそれぞれ規定し、利用者が知り得るように公開する。
従って、これらについて個別の通知は行わない。

(10)開示、訂正、追加または削除、利用の停止
利用者から開示または訂正、追加または削除、利用の停止の依頼を受けた場合に限り、別途定める業務取扱要領に定める手続きにより結果を通知する。ただし、訂正の内容が電子証明書記載事項にかかる場合は、当該電子証明書の失効を必須とする。

(11)理由の説明、手続、料金
NDN は利用者の要求と異なる措置をとる場合、その理由を利用者に説明する。利用者は各種の要求を、NDN が指定する方法によって行わなければならない。
また、利用者の求めに応じる場合、NDN は所定の料金または実費を請求することができる。

2.11 詳細規定

共通 CPS および個別 CPS に基づき、本部およびセンタそれぞれが業務取扱要領等の詳細規定を定める。

共通 CPS8 章の規定に基づき共通 CPS および個別 CPS の改訂が行われる場合、これに伴って詳細規定も、必要な改訂を行う。

3　識別と本人認証

以下の条項について、共通 CPS1.2 節(5)に示す個別 CPS に規定する。

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
3.1.2　名称の意味に関する要件
3.1.3　名称の一意性
3.1.4　名称要求の紛争決着の手順
3.1.5　企業等の名称の認識・認証・役割
3.1.6　秘密鍵の所有を証明する方法
3.1.7　発行申込権者および発行申込時に必要な書類
3.1.8　利用者の真偽の確認
3.1.9　企業等の商号・名称、住所および代表者の確認
3.1.10　企業等に所属していることの確認
3.1.11　受取代理人の真偽の確認

3.2　電子証明書の継続に伴う鍵の更新

3.3　失効後の電子証明書の鍵の更新

3.4　失効申込・失効届出

3.4.1　失効申込権者・失効届出権者
3.4.2　失効申込者・失効届出者の真偽の確認

4　運用の要件

以下の条項について、共通 CPS1.2 節(5)に示す個別 CPS に規定する。

4.1　電子証明書の発行申込

4.1.1　発行申込のパターン
4.1.2　発行申込の受付
4.1.3　発行申込の審査

4.2　電子証明書の発行

4.2.1　電子証明書記載事項の登録
4.2.2　電子証明書の発行指示
4.2.3　鍵ペアの生成と電子証明書の作成
4.2.4　電子証明書および秘密鍵の IC カードへの格納等
4.2.5　BCA に対する相互認証証明書の発行

4.3　IC カード(電子証明書および秘密鍵)および PIN の受領

4.4　電子証明書の失効

4.4.1　利用者の申込による失効
4.4.2　認証局の判断に基づく失効
4.4.3　失効申込・失効届出のパターン
4.4.4　失効申込・失効届出の審査
4.4.5　失効データの登録および失効
4.4.6　失効申込者・失効届出者への通知

4.5　電子証明書失効リスト(CRL/ARL)

4.5.1　CRL の更新周期
4.5.2　相互認証証明書の失効

4.6　セキュリティ監査手続

4.7　アーカイブ

4.7.1　紙で保存する書類
4.7.2　デジタルデータとしてアーカイブする情報

4.8　鍵の更新

4.9　危殆化と災害からの回復

4.10　認証局の終了(認証業務の終了)

5　物理的、手続的、人的なセキュリティ管理

5.1　物理的セキュリティ管理

NDN は、認証局が設置され運用される室を次のとおり定める。

- センタ認証設備室：IA/RA サーバが設置、運用される室
- 本部マシン室　　：登録用端末および DB サーバならびに ICC(IC カード)印刷機が設置、運用される室
- 登録事務室　　：登録事務用端末が設置、運用される事務室

NDN は、当該室および当該室を含む施設のセキュリティを以下のとおり定める。

(1) センタ認証設備室ならびに本部マシン室および登録事務室を置く建物の内部は複数のセキュリティレベルで区画し、レベルごとおよびレベル間の移動に関するセキュリティ規定を設ける。
センタ認証設備室は、IA/RA サーバ等の認証業務用設備を設置するので最高セキュリティレベルの室とし、本部マシン室は ICC(IC カード)印刷機を設置するので、センタ認証設備室相当のセキュリティレベルの室とし、他の区画と間仕切りにより区分されている。

(2) セキュリティレベルのアクセス権限の付与に関する手続を文書化する。

(3) センタ認証設備室および本部マシン室は、耐震・防火・防水・防犯・空調機能を有す安全な施設に設置する。

(4) センタ認証設備室および本部マシン室間は、仮想専用線を使用して閉域網接続する。

(5) センタ認証設備室および本部マシン室は、ビデオ記録システム、モーションセンサにより常時監視され、不正侵入が検知されると警報が作動する。警報作動の原因はすみやかに確認され、対策が講じられる。

(6) センタ認証設備室および本部マシン室へ入室するときには、生体認証システムにより本人性確認が行なわれ、電子錠付扉が解錠する。入退室には、同時に 2 名の認証を必須とする。

(7) 監視情報、入退室記録は監査証跡として、少なくとも毎月のセキュリティ監査の対象とし、次の電子署名法に基づく認定更新までの間保管される。

(8) 機密性、安全性を保持するために重要となる機器には、停電に備えた措置を取っている。

(9) 登録事務室は、出入口には錠を取付けてあり、無人の際には施錠し、間仕切りで登録事務用端末を設置しない区画と区分する等により、権限を有するもの以外が容易に同端末設備に触れる事ができない措置を講じている。

以上のセキュリティ管理の考え方に準拠して、設備が運営されているか否かを文書化された手順に基づき、少なくとも毎月セキュリティ監査する。

また、登録用端末の運用操作に関するセキュリティを以下のように定める。

(1) 登録用端末から DB サーバを介した IA/RA サーバへのアクセスは、IA/RA サーバによって認証される。

(2) 登録用端末の操作者(業務運用者)の保持するクライアント証明書(業務運用者用証明書)は IC カードに格納され、PIN で保護される。

(3) IC カードごとに業務運用者が定められ、文書に記録される。
(4) 業務運用者の IA/RA サーバへのアクセスは、盗聴防止のために充分な強度の暗号通信が適用される。
(5) 業務運用者のすべての運用操作に合議制操作が適用される。
(6) 業務運用者の IA/RA サーバへのアクセスは監査証跡として、IA/RA サーバに記録される。

5.2 手続的セキュリティ管理

手続的セキュリティに関するセンタ認証設備室および本部マシン室の要員別権限を表 5-1、5-2 に定義する。

表 5-1 センタ認証設備室要員別権限

要員区分	指名	入室権限	操作権限	入室権限についてのアクセス権限チェック方式
運用責任者	最高責任者	なし	なし	・セキュリティシステムへのアクセス権限を有した者の帯同が必要
システム運用員	運用責任者	あり	あり	・ID カードシステム ・生体認証システム
セキュリティ管理者	運用責任者	なし	なし	・セキュリティシステムへのアクセス権限を有した者の帯同が必要
データセンタ責任者	運用責任者	なし	なし	・セキュリティシステムへのアクセス権限を有した者の帯同が必要
データセンタ運用員	データセンタ責任者	あり	あり	・ID カードシステム ・生体認証システム
データセンタセキュリティ管理者	データセンタ責任者	なし	なし	・セキュリティシステムへのアクセス権限を有した者の帯同が必要
データセンタ鍵管理者	データセンタ責任者	なし	なし	・セキュリティシステムへのアクセス権限を有した者の帯同が必要
保守要員等	－	なし	なし	・セキュリティシステムへのアクセス権限を有した者の帯同が必要

表 5-2 本部マシン室要員別権限

要員区分	指名	入室権限	操作権限	入室権限についてのアクセス権限チェック方式
業務運用管理者	最高責任者	あり	なし	・ID カードシステム ・生体認証システム
セキュリティ管理者	最高責任者	あり	なし	・ID カードシステム ・生体認証システム
システム管理者	業務運用管理者	あり	あり	・ID カードシステム ・生体認証システム
業務運用者	業務運用管理者	個別付与	個別付与	・ID カードシステム ・生体認証システム
保守要員等	－	なし	個別付与	・セキュリティシステムへのアクセス権限を有した者の帯同が必要

注)個別付与とは、設備機械ごとに操作権限を付与することをいう。

センタ認証設備室および本部マシン室のセキュリティを確保するために、特定の要員に入室権限を付与し、センタ認証設備室および本部マシン室へのアクセスを制限する。センタ認証設備室は、データセンタ責任者の指示によりデータセンタセキュリティ管理者が各要員に各室への入室権限を付与できる。本部マシン室は、業務運用管理者が各要員に各室への入室権限を付与できる。データセンタセキュリティ管理者および本部のセキュリティ管理者は権限付与を表明した文書に基づき、ID カードシステム、生体認証システムに当該要員の登録または削除を行う。

なお、設備の保守その他業務の運営上必要な事情により、やむを得ず入室権限を有しない者を入室させる場合には、入室権限を有する者(以下、「入室権限者」という。)2 名以上による帯同を必要とする。その際、入室権限者 2 名と帯同された者全員は、入退室に係る管理帳簿に必要事項を記入し、入退室管理の記録とする。また、2 名を超えて入室権限者が同時に入室する場合、入室時の生体認証システムの操作を行わなかった入室権限者も管理帳簿へ記入し、退出時の操作は行わない。

認証業務用設備の運用にかかわるセキュリティを確保するため、装置・機器の操作権限を特定の要員に分散して付与し、可能なアクセスを制限する。センタのセキュリティ管理者および本部の業務運用管理者が、認証設備の操作権限を付与できるものとする。システム運用員または業務運用管理者は権限付与を表明した文書に基づき、アカウント設定(または変更、抹消)を行う。なお、装置・機器のアカウントのうち特権を付与されるものについては、特に厳重に管理する。

入室権限、操作権限付与・抹消の記録は、センタはデータセンタ管理者またはデータセンタセキュリティ責任者により管理され、本部は業務運用管理者により管理される。

これらの権限付与および指揮命令系統の詳細は、別途セキュリティ管理要領にて規定する。業務の一部を委託する場合、委託先に本章の規定の遵守を求め、詳細手順書の作成とこれに沿った運用を求める。なお、運用責任者または業務運用管理者は、各要員の作業ならびに委託先による作業について、共通 CPS に従って適切なセキュリティを維持すべく監督しなければならない。

5.3 人的セキュリティ管理

認証業務の運用に携わる要員の管理を、以下の諸要件に適合するよう実施する。

(1) 各要員に、通常実務(指揮命令系統、責任と権限、認証業務フロー、セキュリティ、個人情報保護)および障害回復の運用に必要な規程、手順などの教育を実施し、これを遵守することの同意をとり、宣誓書に署名させる。この中で特に、鍵または PIN の危殆化、または紛失の重大性について熟知させる。

(2) 電子証明書署名鍵(秘密鍵)の分割保管(共通 CPS6.2 節を参照)において鍵断片(分割鍵)の保管者は、鍵断片(分割鍵)を受け取る前に管理責任を果たすことに同意し文書に署名をする。

なおセンタ要員、本部要員の中に、業務に係る技術に関して充分な知識および経験を有すると認められた者を適宜配置する。技術に関する知識および経験とは、認証システムの開発、運用、コンサルテーションの実務の経験および共通 CPS、個別 CPS ならびにこれに類する規定の開発経験をいう。その所定人員数はセンタおよび本部ごとに定める。

6　技術的なセキュリティ管理

6.1　鍵ペアの生成と組み込み

6.1.1　認証局(自己署名 CA)

(1) 鍵ペアの生成
自己署名 CA として、電子証明書発行者である NDN に対する鍵ペアの生成はセンタ認証設備室で行われる。鍵ペアの生成は、本部の鍵断片(分割鍵)保管者およびセンタ要員の合議メンバが行う。

(2) 電子証明書発行者(Issuer=NDN)に対する公開鍵の配付
認証局は、自己署名 CA として電子証明書発行者である NDN に対し生成した公開鍵は、外部に提出することなくセンタ認証設備室で電子証明書の形式にする。

(3) 鍵のサイズ
RSA 公開鍵暗号方式による 2,048 ビットの鍵を使用する。

(4) 使用するハッシュ関数
①AOSign サービスで使用するハッシュ関数
ハッシュ関数としては、SHA-1 を使用する。
②AOSign サービス G2 で使用するハッシュ関数
ハッシュ関数としては、SHA-256 を使用する。

(5) 利用者に対する自己署名証明書の配付
以下のいずれかの方法で配付する。
①アプリケーション(製品、アプリケーションプログラム)に自己署名証明書をプレインストールして配付する。
②認証局のリポジトリから利用者、検証者にダウンロードしてもらい配付する。
ダウンロードする自己署名証明書の正当性は、リポジトリにて公開されるフィンガープリントから利用者、検証者が確認することを義務付ける。
③利用者の秘密鍵と公開鍵ペアを配付する際に一緒に配付する。

(6) BCA に対する自己署名 CA 公開鍵の発行
相互認証証明書作成要求(PKCS#10 形式)に含めて発行する。

(7) ハードウェア鍵の使用
鍵ペアは、センタ認証設備室内に設置する暗号化装置(ハードウェア)により生成する。なお、生成された秘密鍵はその暗号化装置内でのみ使用する。

(8) 鍵の使用目的
X.509V3 の拡張部を使用して、鍵の使用目的(keyUsage)を利用者の電子証明書、相互認証証明書、リンク証明書および運用証明書、CRL/ARL の署名・検証に限定する。

(9) 鍵ペアの格納
鍵ペアを生成した装置内に格納される。

6.1.2　利用者

(1) 鍵ペアの生成
利用者に対する鍵ペアの生成は、センタ認証設備室で行われる。鍵ペアの生成は、本部業務運用者 2 人の合議制操作による承認をもとに IA/RA サーバで行われる。

(2) 電子証明書の発行

生成した公開鍵を用いて、IA/RA サーバ内で電子証明書を発行する。

(3) 鍵のサイズ

①AOSign サービスで使用する鍵のサイズ

RSA 公開鍵暗号方式による 1,024 ビットの鍵を使用する。

②AOSign サービス G2 で使用する鍵のサイズ

RSA 公開鍵暗号方式による 2,048 ビットの鍵を使用する。

(4) 使用するハッシュ関数

①AOSign サービスで使用するハッシュ関数

ハッシュ関数としては、SHA-1 を使用する。

②AOSign サービス G2 で使用するハッシュ関数

ハッシュ関数としては、SHA-256 を使用する。

(5) ハードウェア鍵の使用

ハードウェア鍵は使用しない。

(6) 鍵の使用目的

鍵の使用目的(keyUsage)は、電子署名(digitalSignature)および否認防止(nonRepudiation)である。鍵の使用目的(KeyUsage)は X.509V3 電子証明書拡張部で設定する。利用者はこの鍵使用目的の範囲内で電子証明書を使用する。

(7) 鍵ペアの格納

鍵ペアは、PIN をパスフレーズとして用いて業務運用者が本部マシン室にて IC カードに格納する。

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

電子証明書署名鍵は FIPS 140-2 レベル 3 相当の暗号化装置によって管理する。

6.2.2 電子証明書署名鍵の複数人制御

電子証明書署名鍵を使用する操作は、複数人による合議制操作(Dual Control)とする。電子証明書署名鍵は分割保管(Secret Share を採用)し、各鍵断片(分割鍵)に付きバックアップ媒体は二重化する。

表 6-1 合議制操作と Secret Share

機　関	合議制操作に必要な人数	SecretShare 分割数	電子証明書署名鍵を復元するために必要な Share 数
自己署名 CA	2	2	2

6.2.3 電子証明書署名鍵のエスクロウ

実施しない。

6.2.4 電子証明書署名鍵のバックアップ

電子証明書署名鍵はセンタ認証設備室内で Secret Share によってトークンに鍵断片(分割鍵)として保管する。鍵断片(分割鍵)保管者は、本部は業務運用管理者が任命し、

センタはデータセンタ責任者が任命し、「鍵管理の宣誓書」に署名したうえでトークンを扱い、トークンは耐タンパ性封筒に封印して、鍵断片(分割鍵)保管者の責任においてそれぞれ異なる場所に安全に保管管理する。

なお、電子証明書署名鍵のバックアップ操作は、合議制操作で行われる。

6.2.5　電子証明書署名鍵のアーカイブ

電子証明書署名鍵はアーカイブしない。

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)

(1) 電子証明書署名鍵のエントリは、センタ認証設備室において合議制操作で行われる。

(2) 電子証明書署名鍵は分割トークンから暗号化装置に投入する。

トークンは「鍵管理の宣誓書」に署名した鍵断片(分割鍵)保管者がシステム運用員の指示に従い操作する。

6.2.7　電子証明書署名鍵を活性化させる方法

電子証明書署名鍵の活性化はセンタ認証設備室において合議制操作で行う。活性化された鍵はハードウェア保守時などを除き常時活性状態に置かれる。

6.2.8　電子証明書署名鍵を非活性化させる方法

電子証明書署名鍵の非活性化はセンタ認証設備室において合議制操作で行う。

6.2.9　電子証明書署名鍵を破壊する方法

電子証明書署名鍵は、鍵の有効期間が満了した場合または鍵の使用を中止した場合(認証局終了時の処置)に破壊する。電子証明書署名鍵の破壊は暗号化装置において完全な初期化を行う。この初期化は、合議制操作で行う。これと同時に、鍵断片(分割鍵)トークンは完全な初期化を行うか物理的に破壊する。作業は第三者組織の立会者のもと、鍵断片(分割鍵)保管者が行う。立会者および鍵断片(分割鍵)保管者は「鍵破壊の宣誓書」に署名する。

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

公開鍵のアーカイブは改ざんを防止する措置をとる。アーカイブ期間については表6-2に示す。

表 6-2 公開鍵のアーカイブ期間

発行機関	アーカイブ種別	アーカイブ期間
自己署名 CA	自己署名証明書	電子証明書有効期間満了から 10 年
	電子証明書、その他自己署名 CA が発行した証明書	電子証明書有効期間満了から 10 年

6.3.2 公開鍵と秘密鍵の使用期間

公開鍵と秘密鍵の使用期間(鍵を使用できる期間)を表 6-3 に記す。

表 6-3 鍵使用期間

電子証明書種類	公開鍵使用期間	秘密鍵使用期間
自己署名証明書	10 年以内	5 年以内
利用者の電子証明書	5 年以内	5 年以内

6.3.3 CA 属性を持つ電子証明書の有効期間

CA 属性を持つ電子証明書の有効期間を表 6-4 に記す。

表 6-4 電子証明書有効期間

発行機関	電子証明書種類	有効期間
自己署名 CA	相互認証証明書	5 年以内
	リンク証明書(NewWithOld)	新自己署名証明書の開始日から旧自己署名証明書の終了日まで
	リンク証明書(OldWithNew)	旧自己署名証明書の開始日から旧自己署名証明書の終了日まで

6.4 活性化データ

認証局のコンピュータシステムを利用するために必要な活性化データは、PIN とパスワードとして管理する。

6.4.1 活性化データの生成と組み込み

PIN、パスワードは英文字と数字を含む一定以上の長さに設定し使用する。

6.4.2 活性化データの保護

パスワードは、システム上に暗号化して保管する。パスワードは有効期間を設定し、定期的にパスワード変更を行う。PIN はハードウェアモジュールやトークン内に保管され、外部へは取り出せない。

6.5　コンピュータのセキュリティ管理

IA、RA が使用するコンピュータシステムは、最新のセキュリティ対策を施している。

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

IA、RA で採用するコンピュータシステムは信頼できる組織で開発、テストされたことが証明できるものを使用する。

6.6.2　セキュリティマネジメント管理

IA、RA では随時ワクチンソフトの適用により、ウイルス感染の検出、回復を行う。

6.7　ネットワークのセキュリティ管理

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をインターネットと接続する場合はファイアウォールを介して行う。 ファイアウォールでは不正アクセスを監査証跡として取得する。なお、センタ認証設備室は、ネットワークベース IDS を使用し不正アクセスを防止する。

6.8　暗号化装置の技術的管理

IA で使用する暗号化装置(ハードウェア)は FIPS140-2 レベル 3 相当の暗号モジュールの基準を満たした装置を用いる。

7　電子証明書ならびに CRL/ARL プロファイル

以下の条項について、共通 CPS1.2 節(5)に示す個別 CPS に規定する。

7.1　電子証明書プロファイル

7.1.1　バージョン番号
7.1.2　電子証明書拡張部
7.1.3　アルゴリズム OID
7.1.4　名称形式
7.1.5　名称制約
7.1.6　電子証明書ポリシーOID
7.1.7　ポリシー制約(policyConstraints)拡張の使用
7.1.8　ポリシー修飾子(policyQualifiers)
7.1.9　電子証明書プロファイル

7.2　CRL/ARL プロファイル

7.2.1　バージョン番号
7.2.2　CRL/ARL エントリ拡張
7.2.3　CRL/ARL プロファイル

8　仕様管理

NDN は、利用者のサービス向上、利用アプリケーションの拡大およびセキュリティ技術の最新動向をふまえて、必要に応じ共通 CPS および個別 CPS の仕様を変更する。

8.1　仕様変更の手続きに関するポリシー

NDN は、利用者や検証者に事前の了解を得ることなく共通 CPS および個別 CPS を変更する権利を保有する。共通 CPS および個別 CPS の変更にあたっては、仕様管理委員会において変更内容を検討し、その妥当性が確認された後、実施される。

(1) 認証局の一部ないし全体が危殆化の恐れがあるなど緊急を要する重要な改訂は、直ちに仕様管理委員会を開催し、最高責任者の承認を得て、共通 CPS および個別 CPS の改訂を行う。

(2) 軽微な変更、認定認証業務の変更認定を必要とする変更など一般的な改訂は、仕様管理委員会の検討後最高責任者の承認を得て、共通 CPS および個別 CPS の改訂を行う。

なお、仕様管理委員会は、最高責任者の下に位置し、別途定める仕様管理委員会運営要領に基づき運営される。

8.2　公表および通知に関するポリシー

共通 CPS および個別 CPS の改訂(以下、本項および次項において改訂を伴わない変更を含む。)の公表は、改訂した共通 CPS および個別 CPS を公開するかまたは変更内容のみを当社リポジトリに公開することで行われる。この公表は、通知と同じ効果を持ち、共通 CPS および個別 CPS の実際の改訂と同じ効果を持つ。共通 CPS および個別 CPS の改訂は共通 CPS および個別 CPS の次版に反映され、改訂履歴を表わすバージョン番号と発行日付により識別される。

共通 CPS および個別 CPS の改訂は、通知後直ちに効力を発する。

8.3　仕様認可の手続き

共通 CPS および個別 CPS の改訂が行われた場合、電子証明書発行時期に関わらず当社リポジトリに掲載されている改訂後の規程が適用される。NDN が行った個々の改訂に対して利用者および企業等は、電子証明書の失効申込または失効届出をしない場合、これに同意したとみなされる。 また、検証者はこれに同意できない場合は、入手した電子証明書の使用を中止する。

8.4　CPS の保存

NDN は、改訂された共通 CPS および個別 CPS の各版および変更履歴を電子証明書の有効期間満了後 10 年間保存する。

