「CI-Standard サービス 2 運用規程」

CI-Standard Service 2 Certificate Policy And Certification Practice Statement

Ver.1.60

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

制定日：2016.04.25
改訂日：2023.11.01

目　次

1　はじめに

日本電子認証株式会社(以下、「NDN」という。)は、CI-Standard2 認証局を設置し、プライベート型認証サービスとして、CI-Standard サービス 2 を提供する。

本規程は、CI-Standard2 認証局(以下、「本認証局」という。)が CI-Standard サービス 2(以下、「本サービス」という。)を提供する際の運営方針を定めたものである。

なお、本規程の構成は、IETF PKIX による RFC3647「Certificate Policy and Certification Practices Statement Framework」に準拠している。

1.1　概要

本認証局は、以下の 2 種類の電子証明書を発行する。

タイプ A・・・標準企業コードを識別情報として、一般財団法人建設業振興基金(以下、「基金」という。)が申込受付(RA 業務)を行い、企業および企業内部門・部署の利用者に対して発行する CI-NET 用電子証明書。

タイプ B・・・NDN が申込受付(RA 業務)を行い、企業および企業グループ内部門・部署の利用者に対して発行するプライベート電子証明書。

本認証局は、CP(証明書ポリシ)と CPS(認証実施規定)をそれぞれ独立したものとせず、本規程を本認証局の認証業務に関する運営方針として位置付ける。

なお、本認証局の業務は、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)第 2 条第 3 項に規定する特定認証業務には該当しない。

1.2　識別

本認証局の証明書ポリシの識別子は、次のとおりとする。

表 1-1 NDN および 本サービス等の OID とオブジェクト対応表

OID	オブジェクト
1.2.392.200122	Nippon Denshi Ninsho Co.,Ltd.
1.2.392.200122.14	CI Service
1.2.392.200122.14.2	CI Service Policy for CI-Root2CA Certificate
1.2.392.200122.14.11	CI-Standard Service 2
1.2.392.200122.14.11.1	CI-Standard Service 2 CPS(本規程)
1.2.392.200122.14.11.2	CI-Standard Service 2 Policy for CI-Standard Service 2 Certificate
1.2.392.200122.14.11.3	CI-Standard Service 2 Policy for CI-Standard Service 2 EE TypeA Certificate
1.2.392.200122.14.11.4	CI-Standard Service 2 Policy for CI-Standard Service 2 EE TypeB1 Certificate
1.2.392.200122.14.11.5	CI-Standard Service 2 Policy for CI-Standard Service 2 EE TypeB2 Certificate

1.3　運営体制と証明書の適用範囲

1.3.1　CA の組織

本サービスの運営体制は、次図のとおりである。

図 1-1　CI-Standard サービス 2 の運営体制

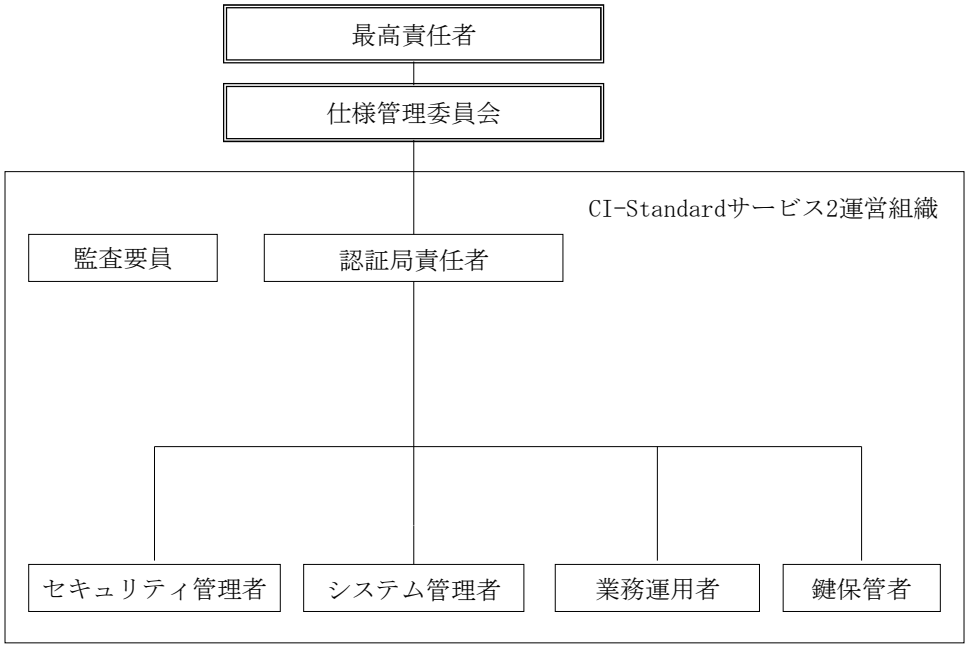

表 1-1　組織・職務とその役割

組織・職務	業務・役割
最高責任者	業務運用に関わる責任者の任命
仕様管理委員会	各種規程類の仕様変更時における妥当性の検討 危殆化、および災害時等の緊急時対応方針の検討
認証局責任者	本サービスの遂行に関する責任
セキュリティ管理者	認証局各施設の物理的セキュリティおよび同監査に関する責任 秘密情報の管理 アーカイブデータの管理
システム管理者	情報基盤の構築と維持 認証局運営上のシステム等の開発・運用・保守
業務運用者 A	タイプ A において、業務運用者 D に対する帯同と証明書の発行支援および失効支援 タイプ B において、証明書の申込受付、審査、発行、失効 CA の判断に基づく証明書の失効

業務運用者 D	タイプ A において、証明書の申込受付、審査、発行、失効
鍵保管者	電子証明書署名鍵をバックアップした USB メモリの保管
監査要員	定期監査

(1)　意思決定組織

本サービスの運営に関する意思決定は、仕様管理委員会が検討を行い、最高責任者の承認を得て行う。最高責任者は NDN 社長とする。

本仕様管理委員会の機能は、次のとおりとする。

① 認証局の規程に関する検討
② 認証局秘密鍵危殆化時の対応に関する検討
③ 災害発生等による緊急時の対応に関する検討
④ その他認証局の運営に関する重要事項の検討

(2)　本サービス運営組織

本サービスにおける認証局は、証明書発行データの登録、審査(内容チェック)を行い、証明書の発行、失効等の運営業務を行う。

本サービス運営組織には、認証局責任者、セキュリティ管理者、システム管理者、業務運用者、鍵保管者、保守要員および監査要員を置く。それぞれの権限については、本規程 5.2 節において規定する。

本サービスの運営は、NDN が行う。

1.3.2　CI-Standard サービス 2 の形態

本サービスは CI-Root2CA 認証局をルート認証局とし、配下の中間認証局の証明書に署名している階層型の認証サービスである。

本認証局(CI-Standard2 認証局)は中間認証局として、電子証明書を発行する組織認証プライベート認証局である。

タイプ A 証明書発行業務では、NDN が発行者(CA)となり、基金が登録局(RA)の業務運用者 D として、申込受付、審査、証明書発行要求、証明書発送および失効受付業務を担当する。

タイプ B 証明書発行業務では、NDN が発行者(CA)と登録局(RA)を実施し、業務運用者 A が、申込受付、審査、証明書発行要求、証明書発送および失効受付業務を担当する。

なお、NDN は登録局用の登録用端末を第 2 登録室にて提供する。

図 1-2 認証局階層

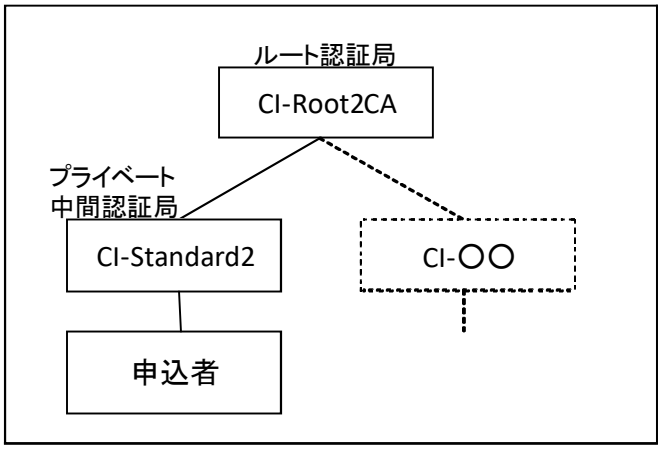

図 1-3 関係者と CI-Standard サービス 2 機能フロー

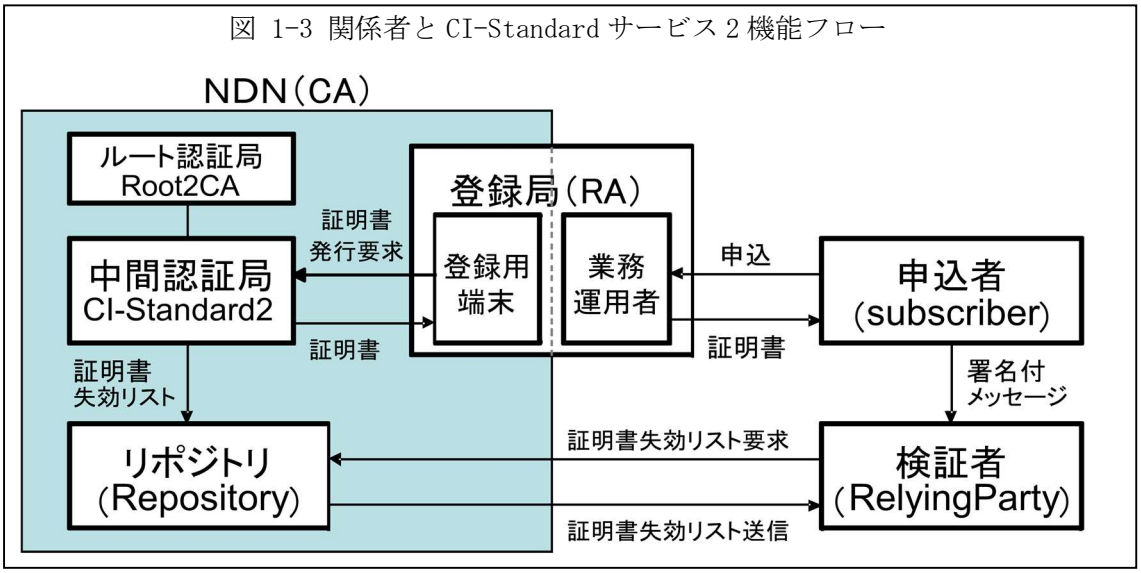

図 1-3 における業務運用者は、タイプ A では基金、タイプ B では NDN が担当する。

1.3.3 証明書の目的と適用範囲

タイプ A 証明書は、利用者が所属する組織から発信される電子商取引用電子文書に電子署名を行うことを目的として、企業または企業内部門・部署の職務権限者に対して発行される。

タイプ B 証明書は、利用者が所属する組織が認める文書への電子署名、暗号化、利用者認証を目的として、企業または企業内部門・部署の責任者からの申込に基づき発行される。

なお、タイプ B 証明書のうち、電子署名用途で用いるもの(keyUsage の nonRepudiation が ON)をタイプ B1、電子署名用途で用いないもの(keyUsage の nonRepudiation が OFF)をタイプ B2 とする。

証明書の有効期間は、証明書を有効とする日から起算して 5 年以内とする。

1.4 CP/CPS に関する担当組織

1.4.1 管理担当部署

本規程の変更、更新等に関する事務は、NDN が行う。

1.4.2 照会窓口

本規程に関する照会は、CI-Standard 係を窓口とする。

［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　：CI-Standard 係

TEL　：03-5148-5206

FAX　：03-5148-5207
　　（9:00～17:00 土曜日、日曜日、祝日、年末年始を除く。）

2　一般規定

2.1　義務

2.1.1　CA 業務に関する義務

本認証局は、CA 業務に関して次の義務を負う。

① 本規程に基づき、自己署名証明書、利用者証明書等を発行する。
② RA の要求に基づき証明書の失効を行い、失効リスト(以下、「CRL/ARL」という。)を定期的に発行する。
③ 電子証明書署名鍵を安全に管理する。
④ 電子証明書署名鍵が危殆化した場合は、速やかに RA に報告する。
⑤ 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を必要な期間、保管する。
⑥ CA システムの稼動監視を行う。

2.1.2　RA 業務に関する義務

本認証局は、RA 業務に関して、申込書記載および確証情報等整合性に関する申込手続が適正に行われていることを確認する。

2.1.3　証明書利用者の義務

証明書の利用者は、次の義務を負う。

① 利用者は利用者の所属する組織内規程に定める範囲に限定して証明書を利用する。
② 本規程および利用規約・利用約款(以下、「利用規約」という。)に記載している事項を遵守する。
③ 証明書および利用者の秘密鍵を安全に保管し、適切に管理する。
④ 利用者の秘密鍵が危殆化した場合は、直ちに失効申込を行う。
⑤ 利用者の義務に違反した場合は、直ちに当該証明書の失効申込を行う。
⑥ 証明書の記載事項に誤りがある場合や証明書の受領後に変更または廃止された場合は、直ちに当該証明書の失効申込を行う。

2.1.4　証明書検証者の義務

証明書の検証者は、証明書検証の際に、証明書の有効性および認証パスの有効性について検証する。

(1) 利用制限

証明書はその利用目的、適用範囲、組織の認証方法、損害賠償等を記述した本規程(利用規約を含む)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証明書の利用目的に疑義があると判断する場合、証明書を受け入れてはいけないし、転用してもいけない。

(2) 有効性確認義務

電子署名の検証等、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 認証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
・ 利用目的が正しいこと
② 提示された証明書の記載項目(特に subject および subjectAltName 項

目)が、本規程 7 章の規定に一致していること

2.1.5 リポジトリに関する義務

本認証局は CRL の作成後、リポジトリにて公開し利用者および検証者が利用者証明書の失効状況を検証できるようにする。

また、ルート認証局証明書およびこれのフィンガープリント、中間認証局証明書およびこれのフィンガープリントを公開する。

2.2 責任

本認証局は、自己署名証明書、利用者証明書等の発行、更新、失効、保管および公開に当たっては、利用者および検証者に対し、本規程に基づく認証業務を適切に行う。

2.2.1 CA の責任

(1) CA は本認証局業務につき、以下の責任を負う。

① RA からの証明書発行要求内容を正確に反映した利用者証明書を発行する責任を負う。

② 利用者証明書発行と同時に、RA に証明書発行情報を提供する責任を負う。

③ 本規程 4 章に従い、CRL をシステム保守等による一時停止、やむを得ない場合の停止を除き、失効後、定期的にリポジトリに登録し、失効対象の証明書の有効期間が満了するまで公開し続ける責任を負う。

④ RA からの失効要求を受理した場合、失効の要求があった利用者の証明書について確実に失効を行う責任を負う。

⑤ 本規程 5 章および 6 章に従い、証明書発行システムを運用管理し、すべての認証局の秘密鍵について、公開鍵から類推・算出されるような場合を除き盗難等による危殆化がないよう責任を負う。

⑥ 証明書、CRL の形式、属性がそれぞれの証明書の発行時点において本規程 7 章記載の規定に合致させることに責任を負う。

(2) 上記にかかわらず、NDN は、以下のいずれかの場合には、RA および利用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ものとする。

① NDN が保有する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、労働者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 その他運用上、技術上、NDN が本サービスの提供の一時的な中断が必要と判断した場合

(3) その他、一定期間、本認証局において通常運営が困難となる場合、または、本サービスを停止せざるを得ない場合（政府または地方自治体の要請に基づくものを含む）は、その旨を検証者および利用者へ通知する。

2.2.2 RA の責任

(1) RA は、証明書申込内容の審査と検証(認証)、ならびに証明書記載内容正当性の確認プロセスを正しく構築／運用する責任を負う。

(2) 発行した鍵ペアを、その鍵ペアを所持すべき利用者だけに確実に渡る手段を提供する責任を負う。

(3) RA は、失効申込を受理した場合、速やかに CA に対し該当証明書の失効要求を行

う責任を負う。
(4) RA は、証明書利用者の義務および NDN の責任範囲について、利用者に周知徹底する責任を負う。

2.3 財務上の責任

2.3.1 賠償責任

(1) NDN の賠償責任

NDN が本規程 2.2 節に規定する責任に違反した場合は、損害賠償責任を負う。

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。

(2) 利用者の賠償責任

利用者が本規程 2.1.3 項に規定する証明書利用者の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 は利用者に対し当該損害の賠償を請求することができる。さらに、利用者が失効申込手続の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) 検証者に対する賠償責任

本規程 2.1.4 項に規定する証明書の利用制限において、検証者が利用目的の範囲を越えて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、本規程 2.1.4 項に規定する検証者による証明書の有効性確認は、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、建設企業及び IT ベンダから出資を得ている。

2.4 解釈および執行

2.4.1 準拠法

本サービスから生ずる紛争については、日本国の法令を適用する。

2.4.2 分割、存続、合併および通知

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、本規程の変更が必要とされる場合には、本規程 8 章の規定に従う。

2.4.3 紛争解決の手続

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

本規程、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

本認証局の発行する証明書の料金、およびその他必要な料金について、タイプ A は基金の Web サイトに掲載する。

2.6 公開とリポジトリ

2.6.1 CA に関する情報の公開

本認証局に関して公開する情報は、次のとおりとする。

① ルート認証局の自己署名証明書
② ルート認証局の自己署名証明書のフィンガープリント
③ 本認証局の自己署名証明書
④ 本認証局の自己署名証明書のフィンガープリント
⑤ 証明書の失効情報
⑥ 電子証明書署名鍵の危殆化に関する情報
⑦ 本規程
⑧ 利用規約
⑨ 検証者同意書

2.6.2 公開の頻度

前項の規定により公開する情報の更新頻度は、情報の発行および更新の都度とする。

2.6.3 アクセス制御

リポジトリ上にて公開する情報は、インターネットを通じて提供する。
公開する情報の提供に当たっては、特段のアクセス制御は行わない。

2.6.4 リポジトリ

本規程 2.6.1 項に規定する情報のうち、①～⑦、⑨は NDN のリポジトリにて公開する。⑧は RA(タイプ A は基金、タイプ B は NDN)の Web サイトにて公開する。

2.7 準拠性監査

2.7.1 監査頻度

本認証局は、本運用開始後、監査人による監査を年 1 回定期的に実施する。また、本認証局は、必要に応じて定期監査以外に監査を実施する。

2.7.2 監査人の身元・資格

本認証局の監査は、監査業務および認証業務に精通した者が行う。

2.7.3 監査人と被監査部門の関係

監査人は、本認証局運用部門に所属しない者から選定する。

2.7.4 監査テーマ

本認証局の業務内容が本規程、業務取扱要領および業務手順書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実施する。

2.7.5 監査指摘事項への対応

監査の結果、指摘事項があった場合には、可及的速やかに改善する。また、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。

(1) 重要または緊急を要する監査指摘事項

重要また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。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) 改善までの経過措置

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、本サービスの全部または一部を中断するか否かは、仕様管理委員会で検討し最高責任者が決定する。

2.7.6 監査結果

本認証局の監査結果は、公開しない。

2.8 秘密保持

2.8.1 秘密扱いとする情報

本認証局は、本規程の履行に関連して相手方から開示を受けた情報であって、次項で規定する以外の情報を秘密情報として扱い、第三者に開示または漏洩しないものとする。

2.8.2 秘密扱いとしない情報

秘密扱いとしない情報については次のとおりとする。

① 開示のとき、被開示者が既に保有し、または既に公知であった情報
② 開示後、被開示者の責によらず、公知となった情報
③ 第三者から秘密保持義務を負うことなく適法に入手した情報
④ 開示者が第三者に対し、秘密保持義務を課すことなく開示した情報
⑤ 証明書および証明書の失効情報
⑥ 法令等により開示が義務付けられた情報

2.8.3 証明書失効情報の公開

本認証局は、自己署名証明書および利用者証明書の失効情報を公開する。

2.8.4 法執行機関への情報開示

NDN は、NDN 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に請求があった場合、法の定めに従い法執行機関へ情報を開示する。

2.8.5 民事手続上の情報開示

本規程 2.8.4 項の規定に含まれる。

2.8.6 証明書利用者の要求に基づく情報開示

個人情報の保護に関する法律(平成 15 年 5 月 30 日法律第 57 号)に定める開示の求めについては、NDN 個人情報保護ポリシーの定めに基づき取り扱う。

2.8.7 その他の理由に基づく情報開示

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 本規程、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、本サービスの運営に伴い取得する個人情報について、NDN 個人情報保護ポリシーに基づき取り扱う。

3　識別と認証

NDN は、本サービスにて発行されるすべての証明書に対するルート認証局を運用する。これは、NDN が発行した証明書の内容を最終的には NDN が保証することを意味する。このため、NDN は証明書の真正を適正に検証することを RA に義務付ける。適正な検証には、証明書発行申込を検証するために利用し得る身元情報(所属企業情報)の正確なコンテンツ(以下、「確証情報」という。)と、RA が設計し作成する証明書発行申込内容(申込様式の内容)と確証情報との比較検証(認証)プロセスと、証明書申込者がその要求の中にある企業、および企業内部門・部署に属しているかの検証(識別)プロセスの確立が必須である。

・確証情報として公的書類等の添付
・証明書申込様式
・申込者検証プロセス(認証と識別)における押印等

を正確に設計／構築／運用することが重要であり、RA はこの義務を怠ったことによって発生する事故／紛争に関して責任を負うものとする。

3.1　初期登録(初期申込)

3.1.1　名前の型

本認証局が発行する証明書の発行者名(Issuer)および所有者名(Subject)は ITU X.500 シリーズ定義の識別名(DN:Distinguished Name)の形式に従って設定する。

3.1.2　名前の意味に関する要件

発行する証明書において使用する名前は、RA が管理する名前ルールに従うものとする。

なお、タイプ A 証明書の標準企業コードは、RA が一般財団法人日本情報経済社会推進協会(JIPDEC)の管理する企業識別コードに対し、枝番として申込者が所属する企業内部門・部署コードを付与するものとする。

3.1.3　名前形式を解釈するための規則

名前の形式を解釈するための規則は、RA が管理する名前ルールに従う。

3.1.4　名前の一意性

証明書に記載される名前は、本認証局が発行する証明書内において利用者ごとに一意とする。

なお、タイプ A 証明書の標準企業コード採番において、RA は重複チェックを実施し、一意性を確保する。

3.1.5　名前に関する紛争の解決手順

RA と利用者間において解決するものとする。

3.1.6　企業等の名称の認識・認証・役割

利用者の所属する企業等の名称は、本規程 4.1 節において規程する申込関係書類により確認する。

3.1.7　秘密鍵の所有を証明するための方法

利用者証明書発行手続においては、本認証局側で秘密鍵と公開鍵の鍵ペアを生成する。

3.1.8 組織の認証

申込書を受領する際に別途定める業務取扱要領および業務手順書等により、申込者の属する組織を確認する。

3.2 証明書の更新

利用者証明書の更新時における識別と認証は、本規程 3.1 節において規定する初期登録と同様の手続に基づいて行う。

3.3 証明書失効後の更新

利用者証明書失効後の更新時における識別と認証は、本規程 3.1 節において規定する初期登録と同様の手続に基づいて行う。

3.4 証明書の失効申込

利用者証明書の失効申込時における識別と認証は、RA が業務取扱要領および業務手順書等に基づき実施し、識別と認証の正当性確認後、CA へ失効を要求し、CA は該当証明書の失効と失効通知書の出力、および CRL 公開を実施する。

4　運用要件

4.1　証明書の発行申込

利用者証明書の発行申込は、利用規約に同意のうえ、申込関係書類一式を RA に提出し発行申込を行う。

発行申込に必要な書類は以下のとおりとする。

① 電子証明書発行申込書

② 申込者の所属企業名が明示された公的書類

4.2　証明書の発行

本認証局は、本認証局側で生成した利用者の公開鍵に、本認証局の署名を付して利用者証明書を発行する。

なお、証明書発行方式は一括発行方式とし、証明書発行情報ファイルと共に一括化されて登録用端末に出力される。

一括化出力された利用者証明書は、暗号化記録媒体(セキュリティ USB メモリ)に格納し、RA 事務室に搬送する。

4.3　証明書の配付

RA は、利用者毎の利用者証明書を CD-R 等の電子媒体に書き込んだうえで PIN 通知書と共に本人限定受取郵便(特例型)にて配付する。

4.4　証明書の失効と一時停止

4.4.1　証明書の失効理由

本認証局は、次の失効理由が発生した場合、証明書を失効する。以下の①から⑤の場合は失効申込に基づき、⑥、⑦の場合は RA の判断、⑧から⑪の場合は CA の判断により証明書の失効を行う。

① 電子証明書等が格納された媒体の紛失・盗難等またはそのおそれ
② 電子証明書等が格納された媒体の破損等
③ 利用者の秘密鍵の危殆化またはそのおそれ
④ 本規程 7 章で規定する識別名等の電子証明書の記載事項の変更(組織名称、職責名称、利用者名、標準企業コード、法人番号およびメールアドレス等の変更または廃止)
⑤ 電子証明書の使用停止
⑥ RA の責めに帰すべき事由による電子証明書の誤発行等
⑦ 利用者が利用規約に違反する行為を行った場合
⑧ CA の責めに帰すべき事由による電子証明書の誤発行等
⑨ 利用者の義務違反
⑩ 電子証明書署名鍵の危殆化
⑪ 本認証局の終了

4.4.2　証明書の失効申込者

利用者証明書の失効申込は、証明書の申込者、または証明書の利用者、利用者の代理人が行う。

4.4.3　証明書の失効申込および失効手順

RA はその失効申込が所定の手続に基づいていることを確認したうえで本認証局に対し利用者証明書の失効要求を行う。本認証局は、RA からの要求を受理した後、直ちに申込された利用者証明書を失効し、CRL をリポジトリに公開する。

なお、失効申込者が失効申込すべき場合において、失効申込がなく、かつ当該失効理由が客観的に判明している場合は、本認証局の判断により失効することができる。

失効申込に必要な書類は以下のとおりとする。

① 電子証明書失効申込書(失効申込に係る意思を確認するため、失効申込者の記載および押印欄を設ける。)

4.4.4 失効における猶予期間

本認証局は、RA からの失効要求後、直ちに失効を行う。

4.4.5 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。

4.4.6 一時停止申込者

規定しない。

4.4.7 一時停止手順

規定しない。

4.4.8 一時停止期間の制限

規定しない。

4.4.9 CRL/ARL の発行周期

CRL/ARL を原則として 24 時間ごとに発行する。ただし、電子証明書署名鍵の危殆化等が発生した場合は、本認証局が発行したすべての利用者証明書を直ちに失効する。

4.4.10 CRL/ARL の確認

検証者は、本認証局の発行する CRL/ARL によって利用者証明書の有効性を確認しなければならない。CRL/ARL は、リポジトリにて公開する。

4.4.11 オンライン有効性確認の可能性

適用しない。

4.4.12 オンライン失効確認要件

規定しない。

4.4.13 その他利用可能な有効性確認手段

規定しない。

4.4.14 その他利用可能な有効性確認手段における確認要件

規定しない。

4.4.15 秘密鍵の危殆化に関する特別な要件

規定しない。

4.5 セキュリティ監査の手順

セキュリティ管理者は、本認証局システムにおける発生事象を記録したログ(以下、「監査ログ」という。)に基づきセキュリティ監査を行う。

4.5.1 監査ログに記録する情報

本認証局システムおよびリポジトリにおけるセキュリティに関する重要な事象を対象に、アクセスログ、操作ログ等監査ログを記録する。監査ログには、次の情報を含める。

① 事象の種類
② 事象が発生した日付および時刻
③ 各種処理の結果
④ 事象の発生元の識別情報(操作員名、システム名等)

4.5.2 監査ログの検査周期

セキュリティ管理者は、監査ログの検査を定期的に行う。

4.5.3 監査ログの保管期間

監査ログは、次回準拠性監査実施時まで保管する。

4.5.4 監査ログの保護

監査ログのバックアップには、改ざん防止対策を施す。また、自己署名証明書、利用者証明書および CRL/ARL を発行するソフトウェアが出力する監査ログのバックアップについては、改ざん検出を可能とする。

監査ログのバックアップは、定期的に外部記憶媒体に取得し、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管する。

なお、監査ログの閲覧および削除はセキュリティ管理者が行う。

4.5.5 監査ログのバックアップ手順

監査ログは少なくとも毎月バックアップし、外部記憶媒体に取得する。

4.5.6 監査ログの収集システム

監査ログの収集機能は本認証局システムの一機能とし、セキュリティに関する事象をシステムの起動時から監査ログとして収集する。

4.5.7 監査ログの検査の通知

監査ログの検査は、事象を発生させた者に通知することなく行う。

4.5.8 脆弱性の評価

監査ログ検査することにより、運用面およびシステム面におけるセキュリティ上の脆弱性を評価する。

4.6 アーカイブ

アーカイブは CA サーバを設置したマシン室内で次のとおり行う。

(注)マシン室は、電子署名およ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わる指針第四条第一項に規定する認証設備室に相当する室である。

4.6.1 アーカイブデータの種類

アーカイブデータは、次のものとする。

① 証明書
② CRL/ARL
③ 起動停止ログ
④ 操作ログ
⑤ 稼動ログ

4.6.2 アーカイブデータの保管期間

証明書は、有効期間満了後 10 年間保管する。

CRL/ARL は、nextUpdate の日時を過ぎた後、その内部に記載された失効証明書の有効期間満了後 10 年間保管する。

その他のアーカイブデータは、少なくとも次回準拠性監査実施時まで保管する。

4.6.3 アーカイブデータの保護

アーカイブデータには、アクセス制御を施すとともに、改ざん検出を可能とする。アーカイブデータのバックアップは、定期的に外部記憶媒体に取得し、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管する。

4.6.4 アーカイブデータのバックアップ手順

アーカイブデータは定期的にバックアップし、外部記憶媒体に取得する。

4.6.5 レコードのタイムスタンプに関する要件

規定しない。

4.6.6 アーカイブデータの収集システム

規定しない。

4.6.7 アーカイブデータの検証

アーカイブデータが記録された外部記憶媒体の可読性の確認を、定期的に行う。

4.7 鍵更新

15 年以内に電子証明書署名鍵ペアの更新を行う。

4.8 危殆化と災害からの復旧およびその他運営困難な場合の対応

4.8.1 ハードウェア、ソフトウェアまたはデータが破壊された場合の対処

ハードウェア、ソフトウェアまたはデータが破壊された場合、バックアップ用のハードウェア、ソフトウェアまたはデータにより、速やかに復旧作業を行う。

4.8.2 証明書を失効する場合の対処

発行した証明書の失効を行った場合は該当証明書の利用者へ失効を通知する。

なお、発行した利用者証明書の失効に当たっては、その失効の取消しは行わない。証明書を失効した利用者に対して、再度証明書を発行する場合は、あらためて発行手続を行う。

4.8.3 秘密鍵が危殆化した場合の対処

電子証明書署名鍵が危殆化した場合は、危機管理計画に基づいて本サービスを停止し、次の手続を行う。

① 発行済有効証明書の失効手続

② 電子証明書署名鍵の廃棄および再生成手続
③ 証明書の再発行手続(電子証明書発行申込書による申込を要する。)

また、利用者の秘密鍵が危殆化した場合は、本規程 4.4 節において規定する手続に基づき、失効手続を行う。

4.8.4 災害等発生時の設備の確保

災害等により本認証局の設備が被害を受けた場合は、代替機を確保しバックアップデータを用いて環境を復旧し運用を継続する。

4.8.5 その他運営困難な場合の対応

その他、一定期間、本認証局において通常運営が困難となる場合、または、本サービスを停止せざるを得ない場合（政府または地方自治体の要請に基づくものを含む）は、その旨を検証者および利用者へ通知する。

4.9 認証業務の終了

本認証局を終了する場合は、業務終了の事実、ならびに業務終了後の本認証局のバックアップデータ、アーカイブデータ等の保管組織および開示方法を業務終了 2 ヶ月前までに、利用者および RA に告知し、以下の業務終了手続を行う。

(1) 本認証局終了の際、電子証明書署名鍵およびそのバックアップ媒体は完全な初期化または物理的に破壊し使用を中止するが、その電子証明書署名鍵に対応する自己署名証明書の失効は行わない。
(2) 本認証局は新たな電子証明書の発行を中止する。
(3) 本認証局終了の時点で発行済みで有効期間の残っている失効されていない電子証明書は、本認証局の終了に伴って一斉に失効される。この一斉失効を追記する最後の CRL 更新を行い、その CRL をリポジトリにて相当の期間公開する。
(4) 本認証局が終了する場合においても、その後、当規程に定める帳票類保存期間に渡り、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。

5　物理面、手続面および人事面のセキュリティ管理

5.1　物理的管理

5.1.1　施設の位置と建物構造

本認証局の施設は、水害、地震、火災その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震、耐火および不正侵入防止のための対策を講ずる。

また、使用する機器等を災害および不正侵入から防護された安全な場所に設置する。

5.1.2　物理的アクセス

施設内の各室内において行われる認証業務の重要度に応じ、複数のセキュリティレベルで入退室管理を行う。CA サーバを設置したマシン室への入退室管理については生体認証装置により行う。

なお、入室権限のない業務運用者 D が第 2 登録室へ入室する際は、本認証局の入室有資格者(業務運用者 A)の帯同を必要とする。

各室への入退室権限は本規程 5.2 節において規定する。

マシン室は、監視カメラにより常時監視を行う。

5.1.3　電源設備と空調設備

本認証局は、機器等の運用のために十分な容量の電源を確保するとともに、瞬断、停電、電圧・周波数の変動に備えた対策を講ずる。

また、空調設備を設置することにより機器類の動作環境および要員の作業環境を適切に維持する。

5.1.4　水害対策

マシン室には漏水探知器を設置し、天井には防水対策を講ずる。

5.1.5　地震対策

本認証局の設備を設置する建物は耐震構造とし、使用する機器等には転倒および落下を防止する対策を講ずる。

5.1.6　火災対策

本認証局の設備を設置する建物は耐火構造であり、マシン室は防火区画とし、消火設備を備える。

5.1.7　媒体管理

アーカイブデータ、バックアップデータを含む媒体は、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管するとともに、業務取扱要領に基づき適切に搬入出管理を行う。

5.1.8　廃棄物処理

秘密扱いとする情報を含む書類・記憶媒体の廃棄については、業務取扱要領に基づいて適切に廃棄処理を行う。

5.1.9　オフサイトバックアップ

規定しない。

5.2 手続面の管理

証明書の発行、更新、失効等の重要な業務の実施に当たっては、要員の職務権限を分離し、相互牽制を行う。

重要な業務の指示は、最高責任者が本認証局責任者に対して行い、本認証局責任者は各要員に指示する。各要員がシステム操作を行う際、システムは、操作員が正当な権限者であることの識別、認証を行う。

各要員別権限を表 5-1 に定義する。

表 5-1　第 2 登録室要員別権限

要員区分	指名	入室権限(a)	入室権限(b)	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
認証局責任者	最高責任者	あり	あり	なし	・(a)については、ID カードシステムと生体認証システム ・(b)については、ID カードシステム
セキュリティ管理者	最高責任者	あり	あり	なし	・(a)については、ID カードシステムと生体認証システム ・(b)については、ID カードシステム
システム管理者	認証局責任者	あり	あり	あり	・(a)については、ID カードシステムと生体認証システム ・(b)については、ID カードシステム
業務運用者 A	認証局責任者	なし	あり	あり	・(b)については、ID カードシステム
業務運用者 D	認証局責任者	なし	なし	あり	・(b)については、登録端末へのアクセス権限を有した者の帯同が必要
鍵保管者	認証局責任者	なし	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
保守要員 監査要員	－	なし	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）入室権限(a)：マシン室
　　入室権限(b)：第 2 登録室

5.3 人事面の管理

本サービスの運用に携わる要員のセキュリティ管理を、以下の要件に適合するよう実施する。

① 本サービスの運営に直接携わる要員には、本サービスの運用に必要な規程、手順などのセキュリティ教育を実施し、これを遵守することの同意をとり、宣誓書に署名させる。

なお、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本規程ならびにこれに類する規定の開発経験をいう。

6　技術的セキュリティ管理

6.1　鍵ペア生成とインストール

6.1.1　ルート認証局

(1) 鍵ペア生成

電子証明書署名鍵ペアは、システム管理者 2 人と認証局責任者が指名した鍵保管者2人の合議制操作によりマシン室内のCAサーバの鍵生成機能を用いて生成する。

(2) 公開鍵の受領

規定しない。

(3) 電子証明書署名鍵の公開鍵の配付

利用者および検証者への公開鍵の配付は、本認証局のリポジトリに公開することで行う。

(4) 鍵のサイズ

・電子証明書署名鍵
RSA2,048 ビットの鍵を使用する。

(5) 使用するハッシュ関数

SHA-256 とする。

(6) 公開鍵パラメータの生成

規定しない。

(7) 公開鍵パラメータの品質の検査

規定しない。

(8) 鍵を生成するハードウェア／ソフトウェア

本規程 6.1.1 項(1)において規定する。

(9) 鍵の利用目的

・電子証明書署名鍵
電子証明書署名鍵は、電子証明書への署名、およびCRL/ARL 署名に用いる。

6.1.2　中間認証局

(1) 鍵ペア生成

・電子証明書署名鍵
電子証明書署名鍵ペアは、システム管理者 2 人と認証局責任者が指名した鍵保管者 2 人の合議制操作によりマシン室内の CA サーバの鍵生成機能を用いて生成する。
・利用者証明書鍵
利用者証明書の鍵ペアは、業務運用者が利用者証明書発行時に本認証局システムのソフトウェアを用いて生成する。

(2) 証明書利用者への秘密鍵配付

利用者の秘密鍵は、CD-R 等の電子媒体に格納の上、RA より所定の手続に基づき、

秘密鍵を利用するための活性 PIN と共に本人限定受取郵便(特例型)にて配付する。

(3) 公開鍵の受領

規定しない。

(4) 電子証明書署名鍵の公開鍵の配付

利用者への配付は利用者証明書を発行する際に一緒に配付する。
検証者への公開鍵の配付は、本認証局のリポジトリに公開することで行う。

(5) 鍵のサイズ

・電子証明書署名鍵
RSA2,048 ビットの鍵を使用する。

・利用者証明書鍵
RSA2,048 ビットの鍵を使用する。

(6) 使用するハッシュ関数

SHA-256 とする。

(7) 公開鍵パラメータの生成

規定しない。

(8) 公開鍵パラメータの品質の検査

規定しない。

(9) 鍵を生成するハードウェア／ソフトウェア

本規程 6.1.2 項(1)において規定する。

(10) 鍵の利用目的

・電子証明書署名鍵
電子証明書署名鍵は、電子証明書への署名、および CRL/ARL 署名に用いる。

・利用者証明書鍵
利用者証明書の秘密鍵は、署名、および鍵、機密情報の暗号化に用いる。

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、マシン室内の CA サーバに暗号化して管理する。

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とし、作業報告書を監査証跡として保管する。

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 USB メモリにバックアップし、2 重化記録として保管する。

鍵保管者は「鍵管理の宣誓書」に署名した上でUSBメモリを扱い、USBメモリはタンパーエビデント封筒に封印し、マシン室内耐火金庫に保管する。耐火金庫の物理鍵はセキュリティ管理者の責任において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は、システム管理者 2 人と鍵保管者 2 人の合議制操作により行う。

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エントリ(バックアップリカバリ)

システム管理者 2 人と鍵保管者 2 人の合議制操作により、USB メモリから CA サーバに電子証明書署名鍵を復元する。

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、システム管理者 2 人が合議制操作により行う。

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、システム管理者 2 人が合議制操作により行う。

6.2.9 電子証明書署名鍵を廃棄する方法

電子証明書署名鍵の有効期間が満了した場合または電子証明書署名鍵の使用を中止する場合(認証局終了時の処置)は、第三者組織の立会者(認証局責任者が「鍵廃棄立会者指名通知書」により指名した本認証局の要員以外の者)の立会いのもと、システム管理者 2 人と鍵保管者 2 人の合議制操作により、CA サーバにおいて電子証明書署名鍵を完全に初期化する。また、電子証明書署名鍵の復元のために保管した USB メモリも、鍵保管者が合議制操作により完全に初期化する。

鍵の廃棄に参加した第三者組織の立会者および鍵保管者は「鍵廃棄の宣誓書」に署名する。

なお、電子証明書署名鍵のバックアップを再取得するに伴い、既に保管してあった電子証明書署名鍵を廃棄する場合も本規定を準用する。

6.3 公開鍵の履歴保管と鍵ペアの有効期間

6.3.1 公開鍵の履歴保管

公開鍵は証明書のアーカイブに含まれ、本規程 4.6.2 項において規定する期間、保管する。

6.3.2 公開鍵と秘密鍵の有効期間

(1) 電子証明書署名鍵

電子証明書署名鍵ペアの有効期間は、有効とする日から起算して 20 年とし、15 年以内に鍵更新を行う。

ただし、暗号のセキュリティが脆弱になったと判断した場合は、その時点で鍵更新を行う。

(2) 利用者証明書鍵

利用者証明書鍵ペアの有効期間は、有効とする日から起算して 5 年以内とする。

6.4 活性化データ

6.4.1 活性化データの生成とインストール

電子証明書署名鍵を格納する CA サーバ上署名鍵の活性化に必要なパスワードは、

システム管理者が決定し、マシン室内の CA サーバに直接入力する。

6.4.2 活性化データの保護

電子証明書署名鍵を格納する CA サーバ上署名鍵の活性化に必要なパスワードは、システム管理者が定期的に変更する。

6.5 コンピュータセキュリティ管理

本認証局システムでは、CA、RA システムに対し、最新のセキュリティ対策を施している。

6.6 システムのライフサイクルにおけるセキュリティ管理

6.6.1 システム開発面における管理

本認証局システムの開発、修正または変更に当たっては、所定の手続に基づき、信頼できる組織および環境下において作業を実施する。

開発、修正または変更したシステムは、テスト環境において検証を行い、本認証局責任者の承認を得たうえで導入する。また、システム仕様および検証報告については、文書化し保管する。

6.6.2 システム運用面における管理

随時ワクチンソフトの適用により、ウィルス感染の検出、駆除を行う。

6.7 ネットワークセキュリティ管理

本認証局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アクセスログを取得する。

6.8 暗号モジュールの技術管理

本規程 6.1 節および 6.2.1 項において規定する。

7　証明書と CRL/ARL のプロファイル

7.1　証明書のプロファイル

証明書の形式は X.509 バージョン 3 に従う。以下に自己署名証明書、中間 CA 証明書、利用者証明書のプロファイルを示す。

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

(1) 自己署名証明書

表 7-1　自己署名証明書

名称	クリティカリティ	設定値
証明書基本部		
version(バージョン)	－	V3
serialNumber(シリアル番号)	－	正の整数
Signature(署名)	－	sha256WithRSAEncryption (OID=1 2 840 113549 1 1 11)
Issuer(発行者)	－	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=CI-Root2CA ※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	－	有効期間は 20 年間とする ※UTCtime で設定する
notAfter	－	
subject(所有者)	－	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU= CI-Root2CA ※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)		
PublicKeyAlgorithmIdentifier	－	rsaEncryption(OID=1 2 840 113549 1 1 1)
public key	－	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)	F	公開鍵のフィンガープリント(SHA-1 ハッシュ値)
keyUsage(鍵種別)	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)	―	設定しない
	issuerAltName(発行者別名)	―	設定しない
	basicConstraints(基本制約)	T	
	cA		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)	F	distributionPoint.fullName.URL に以下を設定する。 https://rep.ci-root.com/cis2/cir.crl
	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

(2) 中間 CA 証明書

表 7-2　中間 CA 証明書

名称	ｸﾘﾃｨｶﾙ ｶﾘﾃｨ	設定値
証明書基本部		
version(バージョン)	―	V3
serialNumber(シリアル番号)	―	正の整数
Signature(署名)	―	sha256WithRSAEncryption (OID=1 2 840 113549 1 1 11)
Issuer(発行者)	―	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=CI-Root2CA
validity(有効期間)		
notBefore	―	有効期間は 20 年間とする

	notAfter	―	※UTCtime で設定する
subject(所有者)		―	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=CI-Standard2 Certification Authority
subjectPublicKeyInfo (所有者公開鍵)			
	PublicKeyalgorithmIdentifier	―	rsaEncryption(OID=1 2 840 113549 1 1 1)
	public key	―	2048bit の値
証明書標準拡張部			
authorityKeyIdentifier (認証局鍵識別)		―	自己署名証明書(ルート証明書)公開鍵のフィンガープリント(SHA-1 ハッシュ値)
	keyIdentifier		
	authorityCertIssuer		
	authCertSerialNumber		
subjectKeyIdentifier (所有者鍵識別)		F	公開鍵のフィンガープリント(SHA-1 ハッシュ値)
keyUsage(鍵種別)		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)		―	
	policyIdentifier		
	certPolicyId		1.2.392.200122.14.11.2
	policyQualifiers		
	policyQualifierId		pkix-id-qt CPSurl
	Qualifier		https://rep.cistd.com/cis2/cps.html (検証者同意書の URL)
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		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)	F	distributionPoint.fullName.URL に以下を設定する。 https://rep.ci-root.com/cis2/cir.crl
	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

(3) 利用者証明書

表 7-3　利用者証明書(タイプ A)

名称		クリティカリティ	設定値
証明書基本部			
	version(バージョン)	－	V3
	serialNumber(シリアル番号)	－	正の整数
	signature(署名)	－	sha256WithRSAEncryption (OID=1 2 840 113549 1 1 11)
	Issuer(発行者)	－	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=CI-Standard2 Certification Authority
	validity(有効期間)		
	notBefore	－	有効期間は 1 年+30 日、3 年+30 日、5 年のいずれかとする。但し、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	－	
	subject(所有者)	－	C=JP(固定) O=CI-NET(固定) OU①=CPN-英字表記企業名 OU②=CMN-JCNXXXXXXXXXXXXX+XXXXXX (法人番号 13 桁+枝番 6 桁) OU③=CompanyCode-XXXXXXXXXXXX (標準企業コード 12 桁) OU④=TID-,MAC-,IMEI-,ICCID- CN=英字表記利用者名もしくは職責名 E=メールアドレス
	subjectPublicKeyInfo (所有者公開鍵)		
	algorithmIdentifier	－	rsaEncryption(OID=1 2 840 113549 1 1 1)
	public key	－	2048bit の値
証明書標準拡張部			
	authorityKeyIdentifier (認証局鍵識別)	F	
	keyIdentifier		中間 CA 公開鍵のフィンガープリント(SHA-1 ハッシュ値)

	authorityCertIssuer		issuer の DN
	authCertSerialNumber		シリアル番号
subjectKeyIdentifier (所有者鍵識別)		F	公開鍵のフィンガープリント(SHA-1 ハッシュ値)
keyUsage(鍵種別)		T	digitalSignature, keyEncipherment, 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)		T	
	policyIdentifier		
	certPolicyId		1.2.392.200122.14.11.3
	policyQualifiers		
	policyQualifierId		pkix-id-qt CPSurl
	Qualifier		https://rep.cistd.com/cis2/cps.html (検証者同意書の URL)
policyMappings (ポリシーマッピング)		―	設定しない
	issuerDomainPolicy		
	subjectDomainPolicy		
subjectAltName(所有者別名)		T	rfc822Name=メールアドレス
issuerAltName(発行者別名)		F	設定しない
basicConstraints(基本制約)		F	
	cA		
	pathLenConstraint		NULL
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)		F	distributionPoint.fullName.URL に以下を設定する。 https://rep.cistd.com/cis2/cis_crl.crl
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 7-4　利用者証明書(タイプ B1)

名称	クリティカリティ	設定値
証明書基本部		
version(バージョン)	―	V3
serialNumber(シリアル番号)	―	正の整数

signature(署名)		―	sha256WithRSAEncryption (OID=1 2 840 113549 1 1 11)
Issuer(発行者)		―	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=CI-Standard2 Certification Authority
validity(有効期間)			
	notBefore	―	有効期間は1年+30日、3年+30日、5年のいずれかとする。但し、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	―	
subject(所有者)		―	C=JP(固定) O=英数字 OU①=CPN-英字表記企業名 OU②=OFC-英字表記所属もしくは役職 OU③=CMN-JCNXXXXXXXXXXXXX+XXXXXX (法人番号13桁+枝番6桁) OU④=CompanyCode-XXXXXXXXXXX (標準企業コード12桁) OU⑤=TID-,MAC-,IMEI-,ICCID- CN=英字表記利用者名もしくは職責名 E=メールアドレス
subjectPublicKeyInfo (所有者公開鍵)			
	algorithmIdentifier	―	rsaEncryption(OID=1 2 840 113549 1 1 1)
	public key	―	2048bit の値
証明書標準拡張部			
authorityKeyIdentifier (認証局鍵識別)		F	
	keyIdentifier		中間 CA 公開鍵のフィンガープリント(SHA-1 ハッシュ値)
	authorityCertIssuer		issuer の DN
	authCertSerialNumber		シリアル番号
subjectKeyIdentifier (所有者鍵識別)		F	公開鍵のフィンガープリント(SHA-1 ハッシュ値)
keyUsage(鍵種別)		T	digitalSignature, keyEncipherment, 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)		T	
	policyIdentifier		
		certPolicyId	1.2.392.200122.14.11.4
	policyQualifiers		
		policyQualifierId	pkix-id-qt CPSurl
		Qualifier	https://rep.cistd.com/cis2/cps.html (検証者同意書の URL)

	policyMappings (ポリシーマッピング)	―	設定しない
	issuerDomainPolicy		
	subjectDomainPolicy		
	subjectAltName(所有者別名)	T	rfc822Name=メールアドレス
	issuerAltName(発行者別名)	F	設定しない
	basicConstraints(基本制約)	F	
	cA		
	pathLenConstraint		NULL
	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)	F	distributionPoint.fullName.URL に以下を設定する。 https://rep.cistd.com/cis2/cis_crl.crl
	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 7-5　利用者証明書(タイプ B2)

名称		クリティカリティ	設定値
証明書基本部			
	version(バージョン)	―	V3
	serialNumber(シリアル番号)	―	正の整数
	signature(署名)	―	sha256WithRSAEncryption (OID=1 2 840 113549 1 1 11)
	Issuer(発行者)	―	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=CI-Standard2 Certification Authority
	validity(有効期間)		
	notBefore	―	有効期間は 1 年+30 日、3 年+30 日、5 年のいずれかとする。但し、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	―	

	subject(所有者)	―	C=JP(固定) O=英数字 OU①=CPN-英字表記企業名 OU②=OFC-英字表記所属もしくは役職 OU③=CMN-JCNXXXXXXXXXXXXX+XXXXXX (法人番号 13 桁+枝番 6 桁) OU④=CompanyCode-XXXXXXXXXXXX (標準企業コード 12 桁) OU⑤=TID-,MAC-,IMEI-,ICCID- CN=英字表記利用者名もしくは職責名 E=メールアドレス
	subjectPublicKeyInfo (所有者公開鍵)		
	algorithmIdentifier	―	rsaEncryption(OID=1 2 840 113549 1 1 1)
	public key	―	2048bit の値
証明書標準拡張部			
	authorityKeyIdentifier (認証局鍵識別)	F	
	keyIdentifier		中間 CA 公開鍵のフィンガープリント(SHA-1 ハッシュ値)
	authorityCertIssuer		issuer の DN
	authCertSerialNumber		シリアル番号
	subjectKeyIdentifier (所有者鍵識別)	F	公開鍵のフィンガープリント(SHA-1 ハッシュ値)
	keyUsage(鍵種別)	T	digitalSignature, keyEncipherment 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)	T	
	policyIdentifier		
	certPolicyId		1.2.392.200122.14.11.5
	policyQualifiers		
	policyQualifierId		pkix-id-qt CPSurl
	Qualifier		https://rep.cistd.com/cis2/cps.html (検証者同意書の URL)
	policyMappings (ポリシーマッピング)	―	設定しない
	issuerDomainPolicy		
	subjectDomainPolicy		
	subjectAltName(所有者別名)	T	rfc822Name=メールアドレス
	issuerAltName(発行者別名)	F	設定しない
	basicConstraints(基本制約)	F	
	cA		
	pathLenConstraint		NULL

	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)	F	distributionPoint.fullName.URL に以下を設定する。 https://rep.cistd.com/cis2/cis_crl.crl
	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 のプロファイル

CRL および ARL の形式は X.509 バージョン 2CRL に従う。以下に CRL および ARL のプロファイルを示す。

(1) ルート認証局が発行する CRL/ARL(中間 CA 証明書の CRL)

表 7-4 ルート認証局が発行する CRL/ARL

名称			クリティカリティ	設定値
CRL 基本部				
	version(バージョン)		－	V2
	signature(署名)		－	sha256WithRSAEncryption (OID=1 2 840 113549 1 1 11)
	Issuer(発行者)		－	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=CI-Root2CA
	thisUpdate(今回更新日時)		－	CRL 発行日時(UTCTime で設定する)
	nextUpdate(次回更新予定)		－	CRL の次回更新日時(UTCTime で設定する)
	revokedCertificates (失効証明書)			
		userCertificate	－	証明書シリアル番号
		revocationDate	－	失効日時
CRL 拡張部				
	authorityKeyIdentifier (認証局鍵識別)		F	
		keyIdentifier		自己署名証明書(ルート証明書)公開鍵のフィンガープリント(SHA-1 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)		F	正の整数
	deltaCRLIndicator (デルタ CRL 識別)		－	設定しない

	issuingDistributionPoint (発行分配点)		T	
		distributionPoint		distributionPoint.fullName.URL に以下を設定する。 https://rep.ci-root.com/cis2/cir.crl
		onlyContainsUserCerts		FALSE を設定する
		onlyContainsCACerts		FALSE を設定する
CRL エントリー拡張部				
		reasonCode(理由コード)	F	設定しない

(2) 中間認証局が発行する CRL(利用者証明書の CRL)

表 7-5　利用者証明書の CRL

名称			クリティカリティ	設定値
CRL 基本部				
	version(バージョン)		―	V2
	signature(署名)		―	sha256WithRSAEncryption (OID=1 2 840 113549 1 1 11)
	Issuer(発行者)		―	C=JP,O=Nippon Denshi Ninsho Co.Ltd., OU=CI-Standard2 Certification Authority
	thisUpdate(今回更新日時)		―	CRL 発行日時(UTCTime で設定する)
	nextUpdate(次回更新予定)		―	CRL の次回更新日時(UTCTime で設定する)
	revokedCertificates (失効証明書)			
		userCertificate	―	証明書シリアル番号
		revocationDate	―	失効日時
CRL 拡張部				
	authorityKeyIdentifier (認証局鍵識別)		F	
		keyIdentifier		中間 CA 公開鍵のフィンガープリント(SHA-1 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)		F	正の整数
	deltaCRLIndicator (デルタ CRL 識別)		―	設定しない
	issuingDistributionPoint (発行分配点)		T	
		distributionPoint		distributionPoint.fullName.URL に以下を設定する。 https://rep.cistd.com/cis2/cis_crl.crl
		onlyContainsUserCerts		TRUE を設定する
CRL エントリー拡張部				

		reasonCode(理由コード)	F	理由コードを設定する

(3) 中間認証局が発行する ARL

表 7-6　ARL

名称			クリティカリティ	設定値
CRL 基本部				
	version (バージョン)		―	V2
	signature(署名)			sha256WithRSAEncryption (OID=1 2 840 113549 1 1 11)
	Issuer(発行者)		―	C=JP, O=Nippon Denshi Ninsho Co.Ltd., OU=CI-Standard2 Certification Authority
	thisUpdate(今回更新日時)		―	ARL 発行日時(UTCTime で設定する)
	nextUpdate(次回更新予定)		―	ARL の次回更新日時(UTCTime で設定する)
	revokedCertificates (失効証明書)			
		userCertificate	―	証明書シリアル番号
		revocationDate	―	失効日時
CRL 拡張部				
	authorityKeyIdentifier (認証局鍵識別)		F	
		keyIdentifier		中間 CA 公開鍵のフィンガープリント(SHA-1 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)		F	正の整数
	deltaCRLIndicator (デルタ CRL 識別)		―	設定しない
	issuingDistributionPoint (発行分配点)		T	
		distributionPoint		distributionPoint.fullName.URL に以下を設定する。 https://rep.cistd.com/cis2/cis_arl.crl
		onlyContainsCACerts		TRUE を設定する
CRL エントリー拡張部				
		reasonCode(理由コード)	F	理由コードを設定する

8 CP/CPS の管理

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、必要に応じ本規程の仕様を変更する。

8.1 CP/CPS の変更

NDN は、本規程を変更する権利を保有する。本規程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、最高責任者の承認を得た後、あらかじめ利用者および検証者へ周知してから実施される。

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 CP/CPS の公開と通知

本規程の改訂(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。)の公開は、変更内容をあらかじめ当社のホームページにおいて周知した後、改訂した本規程を公開するかまたは変更内容のみをリポジトリに公開することで行われる。この公開は、通知と同じ効果を持つ。本規程の改訂は本規程の次版に反映され、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。

本規程の改訂は、この通知後直ちに効力を発する。

8.3 CP/CPS の決定

本規程の改訂が行われた場合、利用者証明書発行時期に関わらず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は、利用者証明書の失効申込をしない場合、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、入手した利用者証明書の使用を中止する。

8.4 CP/CPS の保存

NDN は、本サービスを提供している間、改訂された本規程の各版および改訂履歴を保存する。

改訂履歴

Ver.	日付	改版内容
1.00	2016.4.25	初版発行
1.01	2016.8.5	人事面の管理に係る記述の修正
1.10	2016.10.28	運営体制の変更 電子証明書への法人番号記載方法の変更
1.11	2017.3.1	業務取扱要領と業務手順書等に係る記述の修正 利用者証明書プロファイルの subject（所有者）の変更に係る修正
1.20	2017.4.17	要員の入退室権限変更に伴う変更
1.21	2018.10.26	表現および用語の整理・統一
1.22	2019.11.05	誤記・誤字、文書の見直し等
1.30	2020.4.3	通常運営が困難な場合等の対応について追記
1.40	2021.3.16	意思決定組織に関する修正 表現および用語の整理・統一
1.41	2021.11.1	公開情報に関する変更 表現および用語の整理・統一
1.50	2022.4.1	証明書配布方法の変更 民法改正に伴う対応
1.60	2023.11.1	準拠性監査指摘に伴う変更 表現および用語の整理・統一