

「GoSign サービス 2 運用規程」

GoSign Service 2 Certificate Policy And Certification Practice Statement

Ver. 1. 70



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

制定日 : 2014. 03. 25
改訂日 : 2023. 11. 01

目次	
1 はじめに	- 1 -
1.1 概要	- 1 -
1.2 識別	- 1 -
1.3 運営体制と証明書の適用範囲	- 1 -
1.3.1 CAの組織	- 1 -
1.3.2 証明書の目的と適用範囲	- 3 -
1.4 CP/CPSに関する担当組織	- 3 -
1.4.1 管理担当部署	- 3 -
1.4.2 照会窓口	- 3 -
2 一般規定	- 4 -
2.1 義務	- 4 -
2.1.1 CA業務に関する義務	- 4 -
2.1.2 RA業務に関する義務	- 4 -
2.1.3 証明書申込者の義務	- 4 -
2.1.4 証明書利用者の義務	- 4 -
2.1.5 証明書検証者の義務	- 4 -
2.1.6 リポジトリに関する義務	- 5 -
2.2 CAの責任	- 5 -
2.3 財務上の責任	- 5 -
2.3.1 賠償責任	- 5 -
2.3.2 信頼関係	- 5 -
2.4 解釈および執行	- 6 -
2.4.1 準拠法	- 6 -
2.4.2 分割、存続、合併および通知	- 6 -
2.4.3 紛争解決の手続き	- 6 -
2.5 料金	- 6 -
2.6 公開とリポジトリ	- 6 -
2.6.1 CAに関する情報の公開	- 6 -
2.6.2 公開の頻度	- 6 -
2.6.3 アクセス制御	- 6 -
2.6.4 リポジトリ	- 6 -
2.7 準拠性監査	- 6 -
2.7.1 監査頻度	- 6 -
2.7.2 監査人の身元・資格	- 7 -
2.7.3 監査人と被監査部門の関係	- 7 -
2.7.4 監査テーマ	- 7 -
2.7.5 監査指摘事項への対応	- 7 -
2.7.6 監査結果	- 7 -
2.8 秘密保持	- 7 -
2.8.1 秘密扱いとする情報	- 7 -
2.8.2 秘密扱いとしない情報	- 7 -
2.8.3 証明書失効情報の公開	- 7 -
2.8.4 法執行機関への情報開示	- 8 -
2.8.5 民事手続き上の情報開示	- 8 -
2.8.6 証明書利用者の要求に基づく情報開示	- 8 -
2.8.7 その他の理由に基づく情報開示	- 8 -
2.9 知的財産権	- 8 -

2.10	個人情報保護	- 8 -
3	識別と認証	- 9 -
3.1	初期登録	- 9 -
3.1.1	名前の型	- 9 -
3.1.2	名前の意味に関する要件	- 9 -
3.1.3	名前形式を解釈するための規則	- 9 -
3.1.4	名前の一意性	- 9 -
3.1.5	名前に関する紛争の解決手順	- 9 -
3.1.6	商標の認識・認証・役割	- 9 -
3.1.7	秘密鍵の所有を証明するための方法	- 9 -
3.1.8	組織の認証	- 9 -
3.1.9	職責の認証	- 9 -
3.2	証明書の更新	- 9 -
3.3	証明書失効後の再発行	- 9 -
3.4	証明書の失効申込	- 9 -
4	運用要件	- 10 -
4.1	証明書の発行申込	- 10 -
4.2	証明書の発行	- 10 -
4.3	証明書の受入れ	- 10 -
4.4	証明書の失効と一時停止	- 10 -
4.4.1	証明書の失効理由	- 10 -
4.4.2	証明書の失効申込者	- 10 -
4.4.3	証明書の失効申込および失効処理手順	- 10 -
4.4.4	失効における猶予期間	- 11 -
4.4.5	一時停止	- 11 -
4.4.6	一時停止申込者	- 11 -
4.4.7	一時停止手順	- 11 -
4.4.8	一時停止期間の制限	- 11 -
4.4.9	CRL/ARL の発行周期	- 11 -
4.4.10	CRL/ARL の確認	- 11 -
4.4.11	オンライン有効性確認の可能性	- 11 -
4.4.12	オンライン失効確認要件	- 11 -
4.4.13	その他利用可能な有効性確認手段	- 11 -
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	- 11 -
4.4.15	秘密鍵の危殆化に関する特別な要件	- 11 -
4.5	セキュリティ監査の手順	- 11 -
4.5.1	監査ログに記録する情報	- 11 -
4.5.2	監査ログの検査周期	- 12 -
4.5.3	監査ログの保管期間	- 12 -
4.5.4	監査ログの保護	- 12 -
4.5.5	監査ログのバックアップ手順	- 12 -
4.5.6	監査ログの収集システム	- 12 -
4.5.7	監査ログの検査の通知	- 12 -
4.5.8	脆弱性の評価	- 12 -
4.6	アーカイブ	- 12 -
4.6.1	アーカイブデータの種類	- 12 -
4.6.2	アーカイブデータの保管期間	- 12 -
4.6.3	アーカイブデータの保護	- 13 -

4.6.4	アーカイブデータのバックアップ手順	- 13 -
4.6.5	レコードのタイムスタンプに関する要件	- 13 -
4.6.6	アーカイブデータの収集システム	- 13 -
4.6.7	アーカイブデータの検証	- 13 -
4.7	鍵更新	- 13 -
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	- 13 -
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	- 13 -
4.8.2	証明書を失効する場合の対処	- 13 -
4.8.3	秘密鍵が危殆化した場合の対処	- 13 -
4.8.4	災害等発生時の設備の確保	- 13 -
4.8.5	その他運営困難な場合の対応	- 13 -
4.9	認証業務の終了	- 14 -
5	物理面、手続面および人事面のセキュリティ管理	- 15 -
5.1	物理的管理	- 15 -
5.1.1	施設の位置と建物構造	- 15 -
5.1.2	物理的アクセス	- 15 -
5.1.3	電源設備と空調設備	- 15 -
5.1.4	水害対策	- 15 -
5.1.5	地震対策	- 15 -
5.1.6	火災対策	- 15 -
5.1.7	媒体管理	- 15 -
5.1.8	廃棄物処理	- 15 -
5.1.9	オフサイトバックアップ	- 15 -
5.2	手続面の管理	- 15 -
5.3	人事面の管理	- 17 -
6	技術的セキュリティ管理	- 18 -
6.1	鍵ペア生成とインストール	- 18 -
6.1.1	鍵ペア生成	- 18 -
6.1.2	証明書利用者への秘密鍵配付	- 18 -
6.1.3	公開鍵の受領	- 18 -
6.1.4	電子証明書署名鍵の公開鍵の配付	- 18 -
6.1.5	鍵のサイズ	- 18 -
6.1.6	公開鍵パラメータの生成	- 18 -
6.1.7	公開鍵パラメータの品質の検査	- 18 -
6.1.8	鍵を生成するハードウェア/ソフトウェア	- 18 -
6.1.9	鍵の利用目的	- 18 -
6.2	電子証明書署名鍵（秘密鍵）の保護	- 19 -
6.2.1	暗号化装置標準	- 19 -
6.2.2	電子証明書署名鍵の複数人制御	- 19 -
6.2.3	電子証明書署名鍵のエスクロウ	- 19 -
6.2.4	電子証明書署名鍵のバックアップ	- 19 -
6.2.5	電子証明書署名鍵のアーカイブ	- 19 -
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）	- 19 -
6.2.7	電子証明書署名鍵を活性化させる方法	- 19 -
6.2.8	電子証明書署名鍵を非活性化させる方法	- 19 -
6.2.9	電子証明書署名鍵を廃棄する方法	- 19 -
6.3	公開鍵の履歴保管と鍵ペアの有効期間	- 19 -
6.3.1	公開鍵の履歴保管	- 19 -

6.3.2	公開鍵と秘密鍵の有効期間	- 19 -
6.4	活性化データ	- 20 -
6.4.1	活性化データの生成とインストール	- 20 -
6.4.2	活性化データの保護	- 20 -
6.5	コンピュータセキュリティ管理	- 20 -
6.5.1	コンピュータセキュリティ機能要件	- 20 -
6.5.2	コンピュータセキュリティ評価	- 20 -
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	- 20 -
6.6.1	システム開発面における管理	- 20 -
6.6.2	システム運用面における管理	- 20 -
6.6.3	セキュリティ評価の基準	- 20 -
6.7	ネットワークセキュリティ管理	- 20 -
6.8	暗号モジュールの技術管理	- 20 -
7	証明書と CRL/ARL のプロファイル	- 21 -
7.1	証明書のプロファイル	- 21 -
7.2	CRL/ARL のプロファイル	- 25 -
8	CP/CPS の管理	- 27 -
8.1	CP/CPS の変更	- 27 -
8.2	CP/CPS の公開と通知	- 27 -
8.3	CP/CPS の決定	- 27 -
8.4	CP/CPS の保存	- 27 -
	改訂履歴	- 28 -

1 はじめに

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)を始めとした e-Japan 重点計画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、GoSign サービス 2（以下、「本サービス」という。）を提供する。

本規程は、職責の認証書等を発行する GoSign2 認証局（以下「本認証局」という。）の認証業務に関する運営方針を定める。

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、職責または役職に対して職責証明書を発行する。

本認証局は、CP（証明書ポリシー）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、本サービスは、職責または役職に対して職責証明書を発行するため、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ーの識別子は、次のとおりとする。

表 1-1 NDN および GoSign サービス 2 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.
1.2.392.200122.12	GoSign Service 2
1.2.392.200122.12.1	GoSign Service 2 CPS
1.2.392.200122.12.2	GoSign Service 2 Policy for certificates

1.3 運営体制と証明書の適用範囲

1.3.1 CA の組織

本認証局の運営体制は、次図のとおりである。

図1-1 GoSign2認証局の運営体制

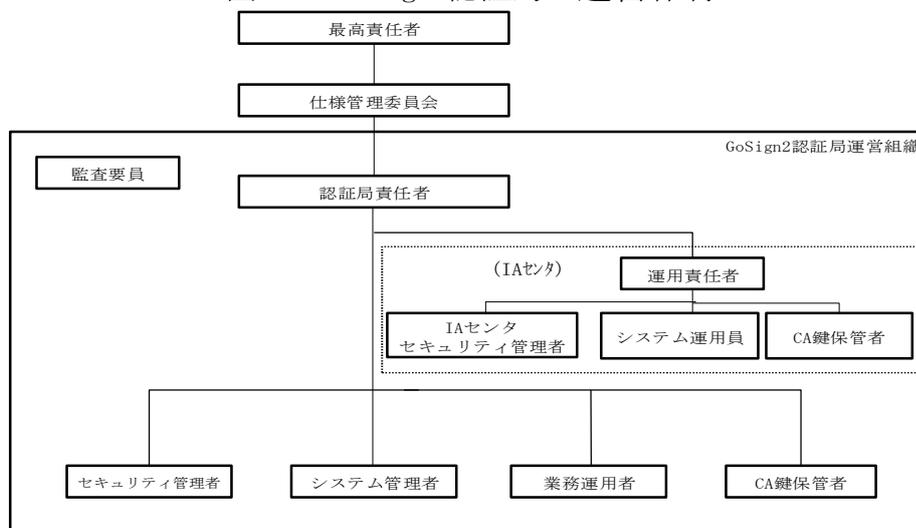


表 1-1 組織・職務とその役割

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	GoSign サービス 2 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 (受付担当、審査担当、登録担当、発行承認担当、失効承認担当)	証明書の発行または失効という認証業務（カッコ内の職務分類）の遂行
業務運用者 B (受付担当、審査担当)	証明書の発行または失効という認証業務（カッコ内の職務分類）の遂行
業務運用者 C (ヘルプデスク担当)	証明書の発行または失効という認証業務のうち、申込に関する説明
CA 鍵保管者	CA 鍵の保管管理
監査要員	定期監査
運用責任者	IA センタ運用における責任
IA センタ セキュリティ管理者	IA センタのシステム操作権限の管理
システム運用員	IA センタのシステム操作権限の登録、削除 IA センタの設備の保守

(1) 意思決定組織

本認証局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 本認証局の規程に関する検討
- ② 本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 その他本認証局の運営に関する重要事項の検討

(2) 本認証局運営組織

本認証局は、職責証明書発行申込の受付、審査を行い、職責証明書の発行、失効等の運営業務を行う。

本認証局運営組織には、本認証局責任者、セキュリティ管理者、システム管理者、業務運用者、CA 鍵保管者、保守要員、運用責任者、IA センタセキュリティ管理者、システム運用員および監査要員を置く。それぞれの業務については、本規程 5.2 節において規定する。

本認証局の運営は、NDN が行う。

1.3.2 証明書の目的と適用範囲

職責証明書は、利用者が所属する組織から発信される文書に電子署名を行うことを目的として、職責または役職に対して発行される。職責証明書の有効期間は、申込み時に指定された期間とし、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、ヘルプデスクを窓口とする。

[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 : ヘルプデスク

E-mail : NDN ホームページの問い合わせフォームより送信

FAX : 03-5148-5695

TEL : 0120-714-240

(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、職責証明書等を発行する。
- ② 証明書の失効処理を行い、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、速やかに申込者に報告する。
- 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 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、職責情報等の申込手続きが適正に行われていることを確認する。

2.1.3 証明書申込者の義務

職責証明書の申込者は、次の義務を負う。

- ① 利用者に対して、申込者および利用者の所属する組織内規程に定める範囲に限定して職責証明書を利用させる。
- ② 利用者に対して、本規程および GoSign サービス 2 利用規約（以下「利用規約」という。）に記載している事項を遵守させる。
- ③ 利用者に対して、職責証明書および利用者の秘密鍵を安全に保管し、適切に管理させる。
- ④ 利用者の秘密鍵が危殆化した場合は、直ちに当該職責証明書の失効申込みを行う。
- ⑤ 利用者が利用者の義務に違反した場合は、直ちに当該職責証明書の失効申込みを行う。
- ⑥ 申込書に記載する職責の名称が変更または廃止された場合は、直ちに当該職責証明書の失効申込みを行う。

2.1.4 証明書利用者の義務

職責証明書の利用者は、次の義務を負う。

- ① 職責証明書は、利用者の所属する組織内規程に定める範囲に限定して利用する。
- ② 本規程および利用規約に記載している事項を遵守する。
- ③ 職責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申込者に届け、または失効申込みを行う。

2.1.5 証明書検証者の義務

職責証明書の検証者は、職責証明書検証の際に、職責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

職責証明書はその目的、適用範囲、組織および職責の認証方法、損害賠償等を記述した本規程に基づいて運用されており、検証者はこれらを理解し、承認したうえで職責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職責証明書の利用目的に疑義があると判断する場合、職責証明書を受け入れてはいけず、転用してはいけず。

(2) 有効性確認義務

電子署名の検証等、職責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 提示された職責証明書の記載項目(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

2.1.6 リポジトリに関する義務

本認証局に関する情報のうち公開する情報は、リポジトリにて公開する。

2.2 CA の責任

本認証局は、自己署名証明書、職責証明書等の発行、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。

2.3 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) 申込者および利用者の賠償責任

申込者が、本規程 2.1.3 項に規定する申込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 は申込者に対し当該損害の賠償を請求することができる。また、利用者が本規程 2.1.4 項に規定する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 は申込者および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、申込者または利用者が失効申込手続き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、申込者および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 は申込者および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 2.1.5 項に規定する職責証明書の利用制限において、検証者が利用目的の範囲をこ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 2.1.5 項に規定する検証者による職責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。

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 紛争解決の手続き

申込者、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

本サービスの料金は別途定める。

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

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 項に規定する情報はリポジトリにて公開する。

2.7 準拠性監査

2.7.1 監査頻度

本認証局は、監査人による監査を年 1 回定期的実施する。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

本認証局の監査を実施する監査人は、本認証局と利害関係をもたない者を選定する。

2.7.4 監査テーマ

本サービスが本規程および別途定める GoSign サービス 2 業務取扱要領（以下、「業務取扱要領」という。）および GoSign サービス 2 事務取扱要領（以下、「事務取扱要領」という。）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

NDN 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、職責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 民事手続き上の情報開示

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

3.1 初期登録

3.1.1 名前の型

本認証局が発行する証明書の発行者名および所有者名は 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。所有者別名 (subjectAltName) の詳細については、本規程 7 章を参照のこと。

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、利用者の属する組織に依存する。

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、ITU X.500 シリーズ定義の識別名の規定に従う。

3.1.4 名前の一意性

規定しない。

3.1.5 名前に関する紛争の解決手順

規定しない。

3.1.6 商標の認識・認証・役割

規定しない。

3.1.7 秘密鍵の所有を証明するための方法

職責証明書発行手続きにおいては、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により、申込者の属する組織を確認する。

3.1.9 職責の認証

申込者から提出された申込書に記載されている職責を別途定める業務取扱要領により確認する。

3.2 証明書の更新

職責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手続きに基づいて行う。

3.3 証明書失効後の再発行

職責証明書失効後の再発行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手続きに基づいて行う。

3.4 証明書の失効申込

職責証明書の失効申込み時における識別と認証は、本規程 3.1.8 項および 3.1.9 項において規定する手続きに基づいて行う。

4 運用要件

4.1 証明書の発行申込

職責証明書の発行申込みは、本規程および利用規約に同意のうえ、申込み関係書類一式を本認証局に提出し発行申込みを行う。

発行申込みに必要な書類は以下のとおりとする。

- ① GoSign サービス 2 電子証明書 発行申込書

※発行申込書は本認証局より入手する。

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職責証明書を発行する。

4.3 証明書の受入れ

本認証局は、発行した職責証明書を、別途定める業務取扱要領により安全かつ確実な方法で申込者に配付し受領書を受取る。この受領確認をもって職責証明書の受入れの完了とする。

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、職責証明書を失効する。本規程 4.4.1 項の①から⑤の場合は失効申込に基づき、⑥から⑨の場合は本認証局の判断により職責証明書の失効処理を行う。

- 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（職責の名称の変更または廃止）
- ⑤ 電子証明書の使用停止
- ⑥ 本認証局の責めに帰すべき事由による電子証明書の誤発行
- ⑦ 利用者の義務違反
- ⑧ 電子証明書署名鍵の危殆化
- ⑨ 本認証局の終了

4.4.2 証明書の失効申込者

職責証明書の失効申込は、職責証明書の申込者が行う。

4.4.3 証明書の失効申込および失効処理手順

職責証明書の失効申込みを受取った本認証局は、その失効申込みが所定の手続きに基づいていることを確認したうえで、申込みされた職責証明書を失効し、CRL をリポジトリに公開する。

なお、申込者が失効申込みすべき場合において、失効申込みがなく、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処理を行うことができる。

失効申込みに必要な書類は以下のとおりとする。

- ① GoSign サービス 2 電子証明書 失効申込書

※失効申込書は本認証局より入手する。

4.4.4 失効における猶予期間

本認証局は、失効申込みの受付完了後、直ちに失効処理を行う。

4.4.5 一時停止

本認証局は、職責証明書の一時的停止を行わない。

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 時間以内に発行する。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職責証明書を直ちに失効する。

4.4.10 CRL/ARL の確認

検証者は、本認証局が発行する CRL/ARL によって職責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、IA センタ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、IA センタ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、職責証明書および 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保管する。

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、事象が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

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**
規定しない。
- 4.7 **鍵更新**
15年ごと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**
発行した職責証明書の失効を行った場合は、当該職責証明書の申込者へ失効を通知する。
なお、発行した職責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。職責証明書を失効した利用者に対して、再度職責証明書を発行する場合は、あらかじめ発行手続きを行う。
- 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、次の手続きを行う。
① 職責証明書の失効手続き
② 電子証明書署名鍵の廃棄および再生成手続き
③ 職責証明書の再発行手続き（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きに基づき、失効手続きを行う。
- 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、予備機を確保しバックアップデータを用いて運用を行う。
- 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

本サービスを終了する場合は、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 ヶ月前までに申込者、利用者および検証者に告知し、所定の業務終了手続きを行う。

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。認証は、認定外 IA/RA サーバを設置した認証設備室については生体認証装置により行う。各室への入退室権限は本規程 5.2 節において規定する。

認証設備室は、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

認証設備室には漏水探知機を設置し、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、認証設備室は防火区画とし、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保管するとともに、別途定めるセキュリティ管理要領および事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、別途定めるセキュリティ管理要領および事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、5-2 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	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	なし	・ ID カードシステム
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
システム 管理者	認証局責任者	あり	あり	・ ID カードシステム
業務運用者	認証局責任者	あり	あり	・ ID カードシステム
CA 鍵保管者	認証局責任者	あり	なし	・ ID カードシステム
保守要員 監査要員	—	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

※業務運用者の入室権限および操作権限については、必要に応じて付与する。

表 5-2 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	—
IA センタ セキュリティ 管理者	運用責任者	なし	なし	—
システム 運用員	運用責任者	あり	あり	・ ID カードシステムと生体認証システム
CA 鍵保管者	最高責任者	なし	なし	—

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、各要員に、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十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 鍵ペア生成

(1) 電子証明書署名鍵

電子証明書署名鍵ペアは、CA 鍵保管者立会いの下で、複数人のシステム運用員が生成する。

(2) 職責証明書鍵

職責証明書の鍵ペアは、業務運用者が職責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。

6.1.2 証明書利用者への秘密鍵配付

利用者の秘密鍵は、IC カード等の媒体に格納の上、所定の手続きに基づいて配付する。

6.1.3 公開鍵の受領

規定しない。

6.1.4 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、リポジトリに公開することで行う。

なお、本認証局を信頼する他の認証事業者による本認証局の自己署名証明書の配付は、その者が本サービスを保証するという意味するものではない。

6.1.5 鍵のサイズ

(1) 電子証明書署名鍵

RSA 2,048 ビットの鍵を使用する。

(2) 職責証明書鍵

RSA 2,048 ビットの鍵を使用する。

6.1.6 公開鍵パラメータの生成

規定しない。

6.1.7 公開鍵パラメータの品質の検査

規定しない。

6.1.8 鍵を生成するハードウェア/ソフトウェア

本規程 6.1.1 項において規定する。

6.1.9 鍵の利用目的

(1) 電子証明書署名鍵

電子証明書署名鍵は、署名に用いる。

(2) 職責証明書鍵

利用者の秘密鍵は、署名に用いる。

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

本機能は実装しない。

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 USB メモリに保管し、バックアップ媒体は二重化する。

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 メモリに保管する。CA 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て、CA 鍵保管者の責任において、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操作は、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暗号化装置へのエントリ（バックアップリカバリ）

本機能は実装しない。

6.2.7 電子証明書署名鍵を活性化させる方法

本機能は実装しない。

6.2.8 電子証明書署名鍵を非活性化させる方法

本機能は実装しない。

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、合議制操作により認定外 IA/RA サーバにおいて電子証明書署名鍵を消去する。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 CA 鍵保管者が完全に初期化する。

鍵の廃棄に立会う第三者（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）および CA 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 USB メモリ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年ごとに鍵更新を行う。

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場合がある。

(2) 職責証明書鍵

職責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

本機能は実装しない。

6.4.2 活性化データの保護

本機能は実装しない。

6.5 コンピュータセキュリティ管理

6.5.1 コンピュータセキュリティ機能要件

本認証局システムには、アクセス制御機能、操作員の識別と認証機能、監査ログおよびアーカイブデータの収集機能、電子証明書署名鍵およびシステムのリカバリ機能等を備える。

6.5.2 コンピュータセキュリティ評価

規定しない。

6.6 システムのライフサイクルにおけるセキュリティ管理

6.6.1 システム開発面における管理

本認証局システムの開発、修正または変更に当たっては、所定の手続きに基づき、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、運用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。

6.6.3 セキュリティ評価の基準

規定しない。

6.7 ネットワークセキュリティ管理

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 6.1.1 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

本認証局が発行する証明書の形式は X.509 バージョン 3 に従う。以下に自己署名証明書および職責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 (1) 自己署名証明書プロファイル

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)	—	128bit 以下の正の整数
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=GoSign2 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	—	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=GoSign2 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	—	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 SHA-1 値 (ハッシュ値)
keyUsage (鍵の使用目的)	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)	F	C=JP, O=日本電子認証株式会社, OU=GoSign2 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)	F	C=JP, O=日本電子認証株式会社, OU=GoSign2 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)	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。 ldap://ldap.gosignca.com/ou=GoSign2%20C ertification%20Authority,o=Nippon%20Densh i%20Ninsho%20Co.Ltd.,c=JP?authorityRevoca tionList
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) 職責証明書

表 7-1 (2) 職責証明書プロフィール

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)	—	128bit 以下の正の整数
	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=GoSign2 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	—	有効期間は申込者指定の期間とする。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)	—	職責の DN、英字表記 ※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	—	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		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)	F	公開鍵の SHA-1 値 (ハッシュ値)
	keyUsage (鍵の使用目的)	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)	T	
	policyIdentifier		
	certPolicyId		(OID=1.2.392.200122.12.2)
	policyQualifiers		
	policyQualifierId		(OID=1 3 6 1 5 5 7 2 1) id-qt-cps
	Qualifier		https://rep.ninsho.co.jp/gosign2/rpa.ht ml (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)	F	職責の DN、日本語表記 ※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)	F	C=JP, O=日本電子認証株式会社, OU=GoSign2 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)	F	distributionPoint.fullName.URL に以下を 設定する。 ldap://ldap.gosignca.com/ou=GoSign2%20C ertification%20Authority,o=Nippon%20Densh i%20Ninsho%20Co.Ltd.,c=JP?certificateRevo cationList
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

本認証局が発行する 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) CRL

表 7-2 (1) CRL プロファイル

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=GoSign2 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)	—	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) ※thisUpdate + 14 日間
	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		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)	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)	T	
	distributionPoint		distributionPoint.fullName.URL に以下を 設定する。 ldap://ldap.gosignca.com/ou=GoSign2%20C ertification%20Authority,o=Nippon%20Densh i%20Ninsho%20Co.Ltd.,c=JP?certificateRevo cationList
	onlyContainsUserCerts		TRUE を設定する。
CRL エントリ拡張部			
	reasonCode (理由コード)	F	理由コードを設定する。

(2) ARL

表 7-2 (2) ARL プロファイル

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= GoSign2 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)	—	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) ※thisUpdate + 14 日間
	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		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)	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)	T		
distributionPoint		distributionPoint.fullName.URL に以下を 設定する。 ldap://ldap.gosignca.com/ou=GoSign2%20C ertification%20Authority,o=Nippon%20Densh i%20Ninsho%20Co.Ltd.,c=JP?authorityRevoca tionList	
onlyContainsCACerts		TRUE を設定する。	
CRL エントリ拡張部			
	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、職責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申込者および利用者は、職責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、入手した職責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	2014.03.25	初版発行
1.10	2014.07.08	認証局運営体制の変更等
1.20	2015.02.02	準拠性監査の指摘事項に基づく変更等
1.21	2016.08.05	人事面の管理、CP/CPSの管理に係る記述の修正 表現および用語の整理・統一
1.30	2017.04.17	要員の入退室権限変更に伴う変更
1.31	2018.10.26	表現および用語の整理・統一
1.32	2019.04.17	運営体制および要員別権限の変更
1.33	2019.11.05	誤記・誤字、文書の見直し等
1.40	2020.04.03	通常運営が困難な場合等の対応について追記
1.50	2021.03.16	表現および用語の整理・統一 誤記・誤字、文書の見直し等
1.51	2021.11.01	公開情報に関する変更
1.60	2022.04.01	民法改正に伴う変更
1.70	2023.11.01	準拠性監査の指摘事項に基づく変更