jNOTARY BusinessCA
運用規定

Version 1.0

株式会社　日本電子公証機構

改訂履歴

Version	日付	変更内容
1.0	2012.4.1	初版作成

目次

1 はじめに

1.1 概要

jNOTAR BusinessCA 運用規定(Certification Practice Statement:以下、「本 CPS」という)は、株式会社日本電子公証機構(以下、「jNOTARY」という)が運用する jNOTARY BusinessCA(以下、「本 CA」という)が電子証明書(以下、「証明書」という)の発行・失効と管理に関するサービス(以下、「本サービス」)に適用する。本 CPS は、jNOTARY BusinessCA リポジトリに掲載し、適宜更新する。

本 CA の証明書発行における申込・審査・発行手続は、使用する証明書に応じた証明書ポリシ(Certificate Policy:以下「CP」という)によって規定される。利用者は jNOTARY によって発行された証明書を利用する際には、本 CPS および CP の内容を利用者自身の利用方法に照らし、評価する必要がある。

1.2 識別

本 CA の証明書ポリシの識別子（OID）は 0 2 440 200148 2 2 4 です。本 CPS は証明書にも公開されている場所が記載される。

1.3 コミュニティと適応可能性

1.3.1 本 CPS の適用範囲

本 CPS は、本 CA により実施される証明書発行及び失効業務に適用されます。本 CA より発行される証明書には、全て本 CPS が適用される。

1.3.2 認証局(CA)

本 CA は、登録局（以下、「RA」という）と発行局（以下、「IA」という）から構成され、jNOTARY により運用される。証明書の発行、失効、失効情報の開示および保管等の統制、管理を行う。

1.3.3 発行局(IA)

本 CA において発行は IA によって行われる。IA は本 CPS に従い証明書の発行処理、失効処理および失効リスト（以下、「CRL」という）の発行処理を行う。

1.3.4 登録局(RA)

本 CA において登録は RA によって行われる。RA は証明書申請者となる個人、組織、団体からの証明書発行、失効等の要求に対して実在性の確認、本人性確認、運用規定の審査等を行う。

1.3.5 申請者

申請者とは、自ら鍵ペアを生成し、本 CA からの証明書の発行を受ける組織または団体の代表者（または代表権を有するもの）をいう。

1.3.6 申請担当者

申請担当者とは、申請者から任命、委任または委託を受けたものであり、jNOTARY との窓口になる担当者をいう。

1.3.7 利用者

利用者とは、本 CA が発行した証明書を信頼して利用する者をいう。

1.4 証明書の使用方法

利用者は当該証明書の信頼性を本 CA の証明書によって検証することができる。

1.5 ポリシ管理

1.5.1 CPS を管理する組織

本 CPS の維持・管理は、jNOTARY が行う。

1.5.2 連絡先

本 CPS に関する問い合わせ窓口は次のとおりである。

[問い合わせ先]

窓口：株式会社日本電子公証機構　jNOTARY BusinessCA サービス窓口

住所：〒130-0013　東京都墨田区錦糸二丁目 14 番地 6 号　エニイビル

営業日：月曜から金曜日（祝日と年末年始の 12 月 30 日～1 月 5 日を除く）

受付時間：午前 10 時から午後 5 時

電話：03-5819-3871

電子メール：info@jnotary.com

1.5.3 CPS 承認手続

本 CPS は、jNOTARY の認証局検討委員会による承認のもと、作成および変更がなされ、リポジトリに公開される。

2．公表とリポジトリの責任

2.1 リポジトリ

本 CA は、申請者および利用者が常時 CRL にアクセスできるようリポジトリを維持管理する。リポジトリへのアクセスに用いるプロトコルは、HTTP,HTTPS とする。リポジトリの情報は、一般的な Web インターフェースを通じてアクセス可能である。

2.2 証明書情報の公開

本 CA は、次の内容をリポジトリに格納し、申請者および利用者がオンラインによって閲覧できるようにする。

・本 CPS および CP に基づく全ての失効情報を含む CRL
・本 CA の自己署名証明書
・最新の本 CPS および CP
・本 CA が発行する証明書に関するその他関連情報

2.3 公開の時期および頻度

本 CPS および CP は、更新の都度、リポジトリに公開される。
リポジトリは 1 日 24 時間、1 週 7 日間運用される。ただし、CA システムの保守などにより予め通知し、一時停止することがある。

2.4 リポジトリへのアクセスコントロール

申請者および利用者は、随時、リポジトリを参照できる。

1) CPS
https://www.jnotary.com/home1/jNOTARY%20BusinessCA%20CPS.pdf
2) CP
https://www.jnotary.com/home1/jNOTARY%20BusinessCA%20CP.pdf
3) CA 証明書
https://www.jnotary.com/home1/jNOTARY%20BusinessCA.cer
4) CRL
http://www.jnotary.com/Cert/Cert/jNOTARY%20BusinessCA.crl
5) フィンガープリント
https://www.jnotary.com/home1/jNOTARY%20BusinessCA%20FP.pdf

３．識別と確認

3.1 名前

CP に規定する。

3.2 新規の識別と認証

CP に規定する。

3.3 更新申請時の識別と認証

CP に規定する。

3.4 失効請求時の識別と認証

CP に規定する。

4．証明書の運用要件

4.1 証明書発行申請

CP に規定する。

4.2 証明書発行申請手続

CP に規定する。

4.3 電子証明書発行

CP に規定する。

4.4 電子証明書の受領

CP に規定する。

4.5 鍵ペアと証明書の用途

CP に規定する。

4.6 証明書の更新

CP に規定する。

4.7 鍵更新を伴う証明書の更新

CP に規定する。

4.8 証明書の変更

CP に規定する。

4.9 証明書の取消および一時停止

CP に規定する。

5．物理的、手続き的、要員的なセキュリティ管理

5.1 物理的セキュリティ管理

5.1.1 立地および建物構造

本 CA システムを設置する施設は、通常想定される災害に対しては十分耐え得る建築構造物内に設置する。また、施設内において使用する機器等を、災害および不正侵入防止策の施された安全な場所に設置する。

5.1.2 物理的アクセス

本 CA のハードウェアおよびソフトウェアには、物理的なアクセスおよび電子的なアクセス制御を組み合わせた適切なセキュリティコントロールを装備する。ハードウェアおよび CA サービスを提供するソフトウェアへのアクセスは、システム管理者の承認を必要とする。

5.1.3 電源管理および空調管理

本 CA システムを設置する室は、本 CA システムの運用のために十分な容量の電源を確保するとともに、UPS を備え停電時対応する。また本 CA システムは、適切な温度、湿度を一定に保った環境下に設置される。

5.1.4 火災防止

本 CA システムを設置する室は、防火壁によって区画された防火区画内とし、火災報知器および消火設備を設置する。

5.1.5 地震対策

本 CA システムを設置する室は、機器・什器の転倒および落下を防止するために必要な対策を講ずる。

5.1.6 媒体管理

アーカイブデータ、バックアップデータを含む重要な媒体は、安全な保管場所に保存される。

5.1.7 廃棄処理

CA 秘密鍵、機密情報を含む紙面の文書および磁気媒体等の廃棄方法は、CA 秘密鍵やバックアップ媒体等は完全な初期化を行うかまたは物理的な破壊を行い、文書等の紙媒体はシュレッダーにかけて廃棄を行う。

5.2 手続上の管理

5.2.1 信頼される役割

証明書の登録、発行、失効業務の携わる者は、本 CPS および CP 上信頼される役割を担っている。本 CA 業務における役割を表「5.2 信頼される役割表」に示す。

5.2 信頼される役割表

役割名称	主な職務内容
認証局検討委員会	・本 CPS および CP の策定、改廃に関する承認 ・監査指摘事項への対応指示
認証局責任者	・本 CA 運用の統括 ・本 CA システム変更、運用の変更等の承認
システム管理者	・本 CA システムの運用全般の管理
IA 業務担当	・証明書の登録作業、発行作業 ・証明書の失効作業
RA 業務担当	・証明書申請の受付 ・申込書類の審査

5.2.2 必要とされる人数

本 CA 業務の運用に必要な人員を確保し、作業は複数人によって行われる。

5.2.3 権限分離が必要な役割

本 CA では、権限を特定の個人に集中させず権限を分離することで、権限集中による不正行為等の防止を図る。

5.3 要員的なセキュリティ管理

本 CA 業務に従事する者は入社前・入社後の経歴や経験等を踏まえ、従事するのに適格であるかどうかの確認を行った上で、任命・配置が行われる。また、役割毎に必要な知識・経験、教育訓練計画、最低必要人員が規定されており、この規定に従って人員の配置や教育訓練が行われる。

個人情報の取扱いと保護、本 CA 秘密鍵の危殆化及び災害等による障害発生など不測の事態に対する対応策の教育訓練も含め、本 CA は業務従事者の信頼性、適格性及び業務遂行能力の維持・向上に努める。

5.4 セキュリティ監査の手順

5.4.1 記録されるイベントの種類

本 CA では、本 CA システム、リポジトリシステム、本 CA に関連するネットワークデバイスの監査証跡やイベントログを、手動あるいは自動で取得する。

5.4.2 監査ログの処理頻度

本 CA では、監査ログを定期的に精査する。

5.4.3 監査ログの保存期間

監査ログの保存期間は、10 年とする。

5.4.4 監査ログの保護

本 CA、許可された者のみが監査ログにアクセスすることができるよう、適切なアクセスコントロールを行う。

5.5 記録の保管

5.5.1 アーカイブの種類

本 CA のアーカイブには、次の情報が含まれる。

・証明書の発行／失効に関する処理履歴
・CRL の発行に関する処理履歴
・申請者の証明書
・CRL
・本 CA の自己証明書

5.5.2 アーカイブの保存期間

アーカイブする情報の保管期間は、10 年間とする。

5.5.3 アーカイブの保護

アーカイブ情報の収められた媒体は物理的に保護され、許可された者しかアクセスできないよう制限された施設において保管される。

5.5.4 アーカイブのバックアップ手順

証明書発行、失効または CRL の発行等、本 CA に影響のある重要なデータに変更がある場合は、都度バックアップを正副取得する。

5.5.5 アーカイブの検証

アーカイブ情報は、定期的に保管状況を確認する。必要に応じて新しい媒体へ複製を行う。

5.6 鍵の切り換え

本 CA の秘密鍵の有効期間は 20 年とし、対応する証明書の有効期間を 20 年とする。

本 CA の秘密鍵の有効期間が満了した時点で、新しい秘密鍵が生成され、その後は、新しい秘密鍵を使って証明書および CRL が発行される。

5.7 信頼性喪失や災害からの復旧

5.7.1 事故および危殆化の対応手順

本 CA 秘密鍵が危殆化または危殆化のおそれがある場合および災害等により本サービスの中断、停止につながるような状況が発生した場合には、予め定められた計画、手順に従い、安全にサービスを再開させる。

5.7.2 ハードウェア、ソフトウェアまたはデータが破損した場合の手続き

本 CA は、ハードウェア、ソフトウェアまたはデータが破損した場合、バックアップ用に保管しているハードウェア、ソフトウェアまたはデータを使用して、速やかにシステムの復旧を行う。

5.7.3 申請者の秘密鍵が危殆化した場合の手続き

申請担当者は、申請者の秘密鍵が危殆化したまたは危殆化のおそれがあると判断した場合、本 CA に対して速やかに証明書の失効申請を行わなければならない。

5.8 認証業務の終了

jNOTARY が本サービスを終了する場合、サービス終了の 60 日前までに申請者その他の関係者にその旨を通知する。

また、廃止日までに本 CA にて発行した全ての有効な証明書を失効し、失効した証明書に記載されている有効期間満了日まで有効な CRL を発行し、有効期間が切れるまでリポジトリに公開する。

6．技術的セキュリティ管理

6.1 鍵ペアの生成とインストール

6.1.1 鍵ペアの生成

本サービスでは、本 CA の秘密鍵の生成作業は、システム管理者立会いのもと、複数の権限者による操作によって行われる。

6.1.2 申請者への秘密鍵の送付

申請者の鍵ペアは、申請者自身で生成するため、秘密鍵は申請者のみが保持する。

6.1.3 CA への公開鍵の送付

申請者の公開鍵は、CP に定める手続きにより検証される。

6.1.4 利用者への CA 公開鍵の送付

利用者は、本 CA のリポジトリにアクセスし公開鍵を入手できる。

6.1.5 鍵長

本 CA の電子署名方式を表「6.1 電子署名方式」に示す。

表 6.1 電子署名方式

アルゴリズム	鍵長
Sha256 With RSA Encryption	2048bit

6.1.6 鍵の使用目的

本 CA の秘密鍵は、以下の目的以外に使用されることはありません。

1) 申請者の電子証明書に対する署名
2) CRL への署名

6.2 CA 秘密鍵の保護

6.2.1 秘密鍵の外部公開とバックアップ

本 CA 秘密鍵に、外部の者がアクセスすることはない。

6.2.2 秘密鍵のバックアップ

本 CA 秘密鍵はバックアップされる。

6.2.3 秘密鍵のアーカイブ

本 CA 秘密鍵のアーカイブは行わない。

6.2.4 秘密鍵の廃棄方法

本 CA 秘密鍵を廃棄しなければならない状況の場合、IA 室内にて複数人の権限者によって、秘密鍵を初期化する。同様にバックアップの秘密鍵も同様に手続きにて廃棄する。

6.3 鍵ペア管理のその他の側面

6.3.1 CA 公開鍵のアーカイブ

本 CA 公開鍵のアーカイブは、本 CPS 5.5.1 に含まれる。

6.3.2 CA 鍵ペアの有効期間

本 CA 鍵ペアの有効期間は 20 年とする。

6.4 コンピュータのセキュリティ管理

本 CA のハードウェアは、本 CPS 5.1 に記述される方法により物理的に保護され、ログイン時にユーザ認証を必要とする。

6.5 セキュリティ技術のライフサイクル

本 CA のハードウェアおよびソフトウェアは、適切なサイクルで最新のセキュリティテクノロジーを評価し、必要に応じて、本 CPS および CP の見直しを行う。

6.6 ネットワークセキュリティ管理

本 CA システムは社内および社外の他のシステムとは接続しない。リポジトリシステムは、ファイアウォール、不正侵入検知システム等により、不正アクセスから保護される。

7．証明書と CRL のプロファイル

7.1 証明書のプロファイル

CP に規定する。

7.2 CRL プロファイル

CP に規定する。

8．準拠性監査

8.1 監査の頻度

本サービスが本 CPS および CP に準拠して運用されているかに関して、年に 1 回以上の準拠性監査を行う。

8.2 監査人の身分と資格

運用する本 CA の準拠性監査について CA 業務に精通しているものを監査人として、本サービスの監査を実施する。

8.3 監査人と被監査対象との関係

監査人は、jNOTARY と特別な利害関係のない監査人を選定する。

8.4 監査対象

監査は、本 CA の運用にかかる業務を対象として行う。

8.5 監査指摘事項への対応

jNOTARY は、監査報告書で指摘された事項に関し、速やかに必要な是正措置を行う。

8.6 監査結果の報告

監査報告書は、業務検討委員会に報告される。監査報告書は社内に保管され、公開は行わない。

9 他の業務上および法的問題

9.1 料金

CP に規定する。

9.2 財務的責任

CP に規定する。

9.3 機密保持

CP に規定する。

9.4 個人情報の保護

CP に規定する。

9.5 知的財産権

CP に規定する。

9.6 表明保証

CP に規定する。

9.7 保証の制限

CP に規定する。

9.8 責任の制限

CP に規定する。

9.9 補償

CP に規定する。

9.10 改訂

9.10.1 改訂手続

jNOTARY は、本 CPS の内容変更に際して、変更した本 CPS をリポジトリ上に掲載することにより、申請者および利用者に対して変更の告知を行う。

9.10.2 通知方法および期間

本 CPS を変更した場合、速やかに変更した本 CPS をリポジトリに掲載することにより、申請者および利用者に対しての告知とする。

9.11 紛争解決手段

CP に規定する。

9.12 準拠法

CP に規定する。

9.13 雑則

CP に規定する。