# 日本銀行外為法手続きオンラインシステム用認証局

# Certification Practice Statement

バージョン 3.1

2024 年 9 月 26 日

日本銀行

目次

**1 はじめに ..... 6**

1.1 概要 ..... 6
1.2 オブジェクト識別子の割り当て ..... 6
1.3 証明書発行等サービスの関係者 ..... 6
1.3.1 認証局 ..... 8
1.3.2 登録局 ..... 8
1.3.3 発行局 ..... 8
1.3.4 システム利用者 ..... 8
1.3.5 依拠当事者 ..... 8
1.4 クライアント証明書の使用方法 ..... 8
1.4.1 適切なクライアント証明書の使用 ..... 8
1.4.2 禁止されるクライアント証明書の使用 ..... 9
1.5 ポリシー管理 ..... 9
1.5.1 文書を管理する組織 ..... 9
1.5.2 連絡担当者 ..... 9

**2 公開とリポジトリ ..... 10**

2.1 リポジトリ ..... 10
2.2 情報の公開 ..... 10
2.3 公開の時期または頻度 ..... 10
2.4 リポジトリへのアクセス管理 ..... 10

**3 識別および認証 ..... 11**

3.1 初期発行 ..... 11
3.1.1 名前の種類 ..... 11
3.1.2 削除 ..... 11
3.1.3 唯一の名称 ..... 11
3.1.4 名称に関する紛争解決手続き ..... 11
3.1.5 個人の認証 ..... 11
3.2 定期的なリキー ..... 12
3.2.1 クライアント証明書の定期的なリキーに関する確認 ..... 12
3.3 取消し要求 ..... 12
3.4 取り消し後のリキー ..... 12

**4 クライアント証明書のライフサイクルに対する運用上の要件 ..... 13**

4.1 クライアント証明書発行申請を行うことが出来る者 ..... 13
4.2 クライアント証明書の利用者 ..... 13

4.3 本人性確認と認証機能の実施 13
4.4 証明書申請の承認もしくは拒絶 13
4.5 証明書申請の処理時間 13
4.6 認証局の利用者に対する証明書発行通知 13
4.7 クライアント証明書の受領となる行為 14
4.8 利用者の秘密鍵及びクライアント証明書の使用 14
4.9 クライアント証明書が変更される場合 14
4.10 クライアント証明書の変更申請の手続き 14
4.11 利用者に対する新しいクライアント証明書発行通知 14
4.12 変更されたクライアント証明書の受領確認の行為 14
4.13 失効が行われる場合 15
4.14 クライアント証明書の失効申請手続き 15
4.15 認証局が失効申請を処理しなければならない期間 15
4.16 利用の終了 15

**5 設備上、運営上、運用上の管理 16**

5.1 設備管理 16
5.2 手続的管理 16
5.2.1 信頼すべき役割 16
5.2.2 職務ごとに必要とされる人数 16
5.3 人事的管理 17
5.4 監査ログの手続 17
5.4.1 記録されるイベントの種類 17
5.4.2 監査ログを検査する頻度 17
5.4.3 監査ログを保持する期間 18
5.4.4 監査ログの保護 18
5.4.5 監査ログのバックアップ手続 18
5.4.6 監査ログの収集システム 18
5.4.7 イベントを発生させたサブジェクトに対する通知 18
5.5 危殆化および災害からの復旧 18
5.5.1 危殆化および被災時の取扱手続き 18
5.5.2 コンピュータの資源、ソフトウェア、またはデータが破損した場合 18
5.5.3 クライアント証明書秘密鍵が危殆化した場合の手続 19
5.5.4 災害後の事業継続能力 19
5.6 認証局サービスの終了 19

**6 技術的セキュリティ管理 20**

6.1 鍵ペアの生成およびインストール 20
6.1.1 鍵ペアの生成 20
6.1.2 システム利用者に対する秘密鍵の交付 20

6.1.3 鍵ペアのサイズ ..... 20
6.1.4 鍵の用途 ..... 21
6.2 秘密鍵の保護および暗号モジュール技術の管理 ..... 21
6.2.1 暗号モジュールの管理 ..... 21
6.2.2 秘密鍵の"n of m"による複数人管理 ..... 21
6.2.3 秘密鍵のバックアップ ..... 22
6.2.4 秘密鍵の暗号モジュールへの転送または暗号モジュールからの転送 ..... 22
6.2.5 秘密鍵の活性化方法 ..... 22
6.2.6 秘密鍵の非活性化方法 ..... 22
6.2.7 秘密鍵の破棄方法 ..... 22
6.2.8 暗号モジュールの評価 ..... 22
6.3 その他の鍵ペア管理 ..... 23
6.3.1 公開鍵のアーカイブ ..... 23
6.3.2 証明書の運用上の期間および鍵ペアの使用期間 ..... 23
6.4 活性化データ ..... 23
6.4.1 活性化データの生成および設定 ..... 23
6.4.2 活性化データの保護 ..... 23
6.5 コンピュータのセキュリティ管理 ..... 23
6.5.1 コンピュータのセキュリティに関する技術的要件 ..... 24
6.5.2 コンピュータセキュリティ評価 ..... 24
6.6 ライフサイクルの技術上の管理 ..... 24
6.6.1 システム開発 ..... 24
6.6.2 セキュリティ運用 ..... 24
6.7 ネットワークセキュリティ管理 ..... 24
**7 証明書プロファイル ..... 25**
7.1 証明書プロファイル ..... 25
7.1.1 ルート認証局証明書 ..... 25
7.1.2 クライアント証明書 ..... 26
**8 準拠性監査とその他の評価 ..... 28**
**9 他の業務上および法的問題 ..... 29**
9.1 料金 ..... 29
9.2 業務において機密として取り扱う情報の管理 ..... 29
9.2.1 機密として取り扱う情報の範囲 ..... 29
9.2.2 機密として取り扱わない情報 ..... 29
9.2.3 機密として取り扱う情報の保護 ..... 29
9.3 個人情報保護 ..... 29
9.4 知的財産権 ..... 30

9.5 表明保証 ..... 30
9.5.1 認証局の義務と責任 ..... 30
9.5.2 利用者の義務と責任 ..... 30
9.6 保証の否認 ..... 30
9.7 責任の制限 ..... 31
9.8 有効期間と終了 ..... 31
9.8.1 有効期間 ..... 31
9.8.2 終了 ..... 31
9.8.3 終了の効果と効果の残存 ..... 31
9.9 改訂 ..... 31
9.9.1 改訂手続き ..... 31
9.10 紛争解決手続 ..... 31
9.11 準拠法 ..... 32
9.12 雑則 ..... 32
9.12.1 分離可能性条項、残存規定条項、完全合意性条項、通知条項 ..... 32

# 1　はじめに

## 1.1　概要

日本銀行は、日本銀行外為法手続きオンラインシステム用認証局（以下「オンラインシステム用認証局」という）として認証機関の機能を果たし、日本銀行外為法手続きオンラインシステム（以下「オンラインシステム」という）の利用者（以下「システム利用者」という）に対して証明書の発行、更新、取消しおよび管理を含む一連のサービス（以下「証明書発行等サービス」という）を提供します。

「オンラインシステム用認証局」は、システム利用者がオンラインシステムにアクセスする際のユーザ認証（以下「クライアント認証」という）に使用する証明書（以下「クライアント証明書」という）を発行します。

日本銀行は、その他の用途に使用する証明書を発行しないものとします。

本書は、本サービスを提供するために日本銀行が運営する「オンラインシステム用認証局」のCPS（Certification Practice Statement）（以下「本書」という）です。

なお、日本銀行が発行する証明書に関する利用者向けの利用規約は、日本銀行が制定した「日本銀行外為法手続きオンラインシステム用認証局が発行する証明書に関する利用規約」（以下「オンラインシステム用認証局の利用規約」という。日本銀行のホームページおよびオンラインシステムで公開している。）を使用します。

「オンラインシステム用認証局の利用規約」は、日本銀行とシステム利用者の間で締結される利用規約です。

なお、本書内の専門的な用語の定義や略語については、巻末の用語集を参照してください。

## 1.2　オブジェクト識別子の割り当て

日本銀行は、本書によって規定されるポリシーに対してオブジェクト識別子の割り当てを行いません。

## 1.3　証明書発行等サービスの関係者

証明書発行等サービスは、PKI（Public Key Infrastructure）サービスを利用しています。図 1に本サービスの参加者とその関係を示します。各参加者の定義は本節内の各項の内容をご参照下さい。

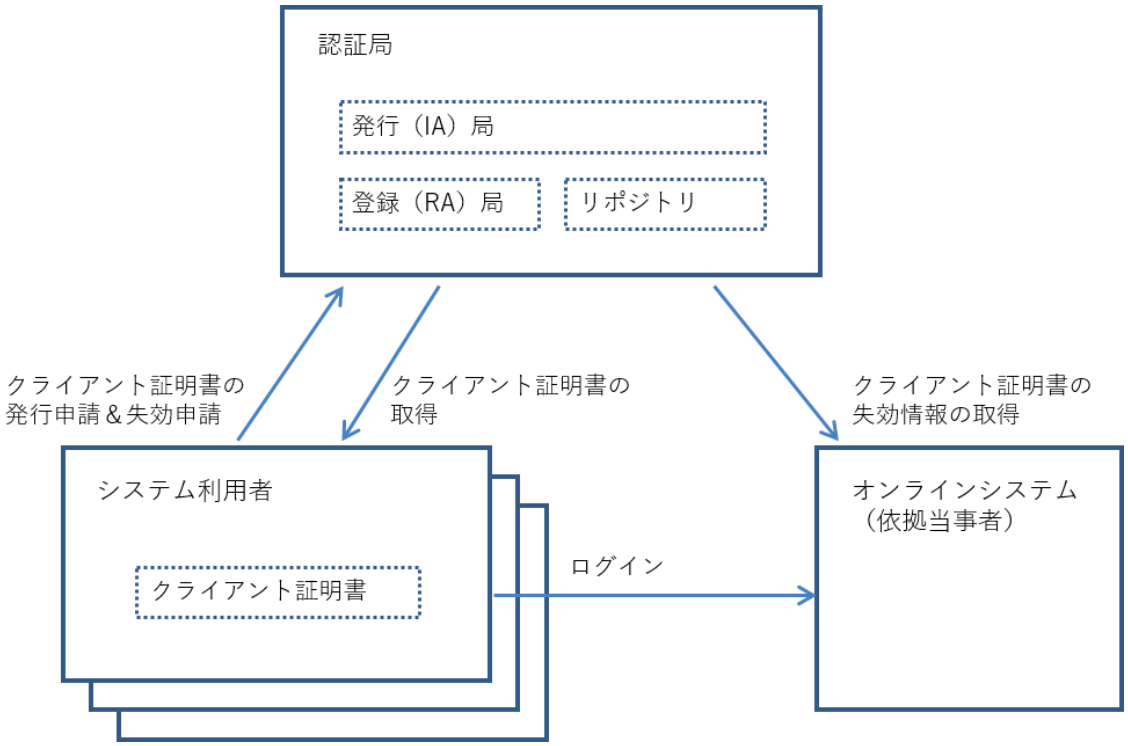


図 1　本サービスの参加者

### 1.3.1　認証局

本書において認証局とは、利用者申し込み（失効にかかる申し込みも含む）から申請を受け付け、必要な審査を行い、適切と認められた利用申込者に対してクライアント証明書を発行する（または失効させる）主体となります。

認証局は、登録局（Registration Authority）、発行局（Issuing Authority）、およびリポジトリ（Repository）を含む総称となります。登録局は 1.3.2、発行局は 1.3.3、リポジトリは 2.1 から 2.4 でそれぞれ規定します。

日本銀行ルート認証局は本認証局の最上位の認証局であり、システム利用者に対してクライアント証明書の発行を行う認証局です。

### 1.3.2　登録局

登録局は、システム利用者からの窓口の役割を果たし、クライアント証明書の発行申請の審査及び承認、失効申請の審査及び承認等を行い、発行局に対してクライアント証明書の発行、失効等の指示を行う機関です。

### 1.3.3　発行局

発行局は、システム利用者のクライアント証明書を発行（生成）する機関です。

発行局は、本認証局の秘密鍵の管理をし、登録局からの指示に従ってクライアント証明書の発行および失効を行う機関です。また、発行局は、CRL（失効情報リスト）の生成も行います。

本認証局では、発行局業務の実施にあたり、株式会社エヌ・ティ・ティ・データ（以下「NTT データ」という）が提供する PKI サービスを利用します。

### 1.3.4　システム利用者

本認証局は、日本銀行が認めるシステム利用者に対し、クライアント証明書を発行します。

クライアント証明書はオンラインシステムのシステム利用者のために発行されます。

### 1.3.5　依拠当事者

本サービスにおける依拠当事者は、日本銀行（日本銀行外為法手続きオンラインシステム）です。

## 1.4　クライアント証明書の使用方法

本節では日本銀行が発行するクライアント証明書が利用される範囲について規定します。

### 1.4.1　適切なクライアント証明書の使用

日本銀行が発行するクライアント証明書は、クライアントの認証に利用されることを目的としています。

### 1.4.2　禁止されるクライアント証明書の使用

システム利用者は、日本銀行が発行したクライアント証明書を、本書の 1.4.1 で規定した用途以外に使用してはなりません。

## 1.5　ポリシー管理

本書の管理方法について規定します。

### 1.5.1　文書を管理する組織

本書についての管理部署は、日本銀行のホームページおよびオンラインシステムに掲載します。

### 1.5.2　連絡担当者

本書についての照会先は、日本銀行のホームページおよびオンラインシステムに掲載します。

## 2　公開とリポジトリ

### 2.1　リポジトリ

日本銀行は､証明書発行等サービスの運用を円滑に行うために本サービスに関わる各種情報を保管・管理します。また、日本銀行は当該情報を公開するためにリポジトリを運営します。リポジトリは 365 日×24 時間運用されます。ただし、保守などの理由により、一時的に運用を停止する場合があります。

### 2.2　情報の公開

日本銀行は、本書およびオンラインシステム用認証局の利用規約を、日本銀行のホームページおよびオンラインシステムにて公開します。

### 2.3　公開の時期または頻度

日本銀行は、本書またはオンラインシステム用認証局の利用規約を変更した場合には、本書 2.2 に従い、最新版を公開します。

### 2.4　リポジトリへのアクセス管理

本書およびオンラインシステム用認証局の利用規約は、公にアクセス可能なものです。当該情報の参照にはアクセス制限はかけません。

# 3　識別および認証

## 3.1　初期発行

### 3.1.1　名前の種類

日本銀行が提供する証明書発行等サービスのルート認証局証明書の識別名（Subject フィールド）は表 3-1 の通り規定します。

**表 3-1　ルート認証局証明書**

| No. | 属性 | 値（または例） | 説明 |
|---|---|---|---|
| 1 | C | JP | 日本を示す。 |
| 2 | O | Bank Of Japan | 日本銀行の英語名称を示す。 |
| 3 | CN | Gaitame CA – G5 | 日本銀行のルート証明書のサービス名を示す。 |

### 3.1.2　削除

### 3.1.3　唯一の名称

日本銀行は、クライアント証明書に記載される名称（DN）の一意性の確保を行います。

### 3.1.4　名称に関する紛争解決手続き

システム利用者等は、クライアント証明書の申請において、他社の知的財産権を侵害するような名称等を使用してはなりません。日本銀行は、システム利用者等が申請した名称について、当該申請者が申請された名称等の知的財産権を有しているかの確認を行いません。

また、ドメイン・ネーム、商号、商標、サービスマークに関する紛争を仲裁、調停、その他の方法で解決するものではありません。日本銀行は、システム利用者等に何等の責任を負うことなく、上記の紛争を理由としてクライアント証明書の申請を拒絶し、また、発行された当該クライアント証明書を失効する権利を有します。

### 3.1.5　個人の認証

日本銀行は、クライアント証明書の発行において、次の確認を行います。

- システム利用者が提出した、オンラインシステムの利用申込書の内容が正確であること。
- システム利用者がオンラインシステムの正当な利用権限を有していること。

## 3.2　定期的なリキー

### 3.2.1　クライアント証明書の定期的なリキーに関する確認

日本銀行は、発行したクライアント証明書の更新において、以下のいずれかの方法で本人確認を実施します。

- 発行済みの有効なクライアント証明書を用いた電子署名による確認
- 本書 3.1.5 に定める方法

## 3.3　取消し要求

日本銀行は、発行したクライアント証明書の取消しにおいて、別途定める方法を用いて本人確認を実施します。

## 3.4　取り消し後のリキー

システム利用者は、取消し後のリキーを行うことはできません。日本銀行は、クライアント証明書の失効が発生した場合におけるクライアント証明書の再発行時の認証を、新規発行時と同様の手続きに基づき実施します。

# 4　クライアント証明書のライフサイクルに対する運用上の要件

## 4.1　クライアント証明書発行申請を行うことが出来る者

オンラインシステムのシステム利用者になることを希望する者（以下「申請者」という）は、クライアント証明書の発行申請を行うことが出来ます。

## 4.2　クライアント証明書の利用者

申請者は、クライアント証明書の発行申請において、以下の申請手続きを実施するものとします。

- 申請者は、クライアント証明書発行申請において、正しく情報を提供すること。
- 申請者は、鍵ペアを生成し、公開鍵を発行局へ正しく引き渡すこと。
- 申請者は、Web を用いたクライアント証明書の発行申請の前に、オンラインシステムの利用申込書を日本銀行に提出し、審査を受けること。

## 4.3　本人性確認と認証機能の実施

日本銀行は、本書 3.1.5 に規定される方法で申請者の全情報の確認および認証を行います。

## 4.4　証明書申請の承認もしくは拒絶

日本銀行は、本書 3.1.5 に規定される方法で確認および認証が問題なく完了した場合、クライアント証明書の発行申請を承認します。

## 4.5　証明書申請の処理時間

日本銀行は、申請から妥当な時間内にクライアント証明書発行申請の手続きを開始します。オンラインシステム用認証局の利用規約および本書に別段の定めがない限り、申請処理を完了するまでの時間に関する規定は定めません。そのクライアント証明書発行申請は、拒絶されるまで有効です。

## 4.6　認証局の利用者に対する証明書発行通知

日本銀行は、クライアント証明書の発行申請を承認された申請者に対して、クライアント証明書の発行申請に必要な情報を通知します。

### 4.7　クライアント証明書の受領となる行為

日本銀行が提供する証明書発行等サービスでは、申請者による Web を用いたクライアント証明書の発行申請の後に、当該申請者のクライアント証明書の生成を行います。クライアント証明書が生成され次第、申請者はクライアント証明書をダウンロードして受領します。

### 4.8　利用者の秘密鍵及びクライアント証明書の使用

クライアント証明書における公開鍵に対応した秘密鍵の使用は、システム利用者が、オンラインシステム用認証局の利用規約に同意し、クライアント証明書を受領した場合にのみ許可されます。そのクライアント証明書は、オンラインシステム用認証局の利用規約および本書の条件に従って合法的に使用されなければなりません。

### 4.9　クライアント証明書が変更される場合

システム利用者は、既存のクライアント証明書の情報に変更があった場合、クライアント証明書の変更のための再発行申請を行う必要があります。

### 4.10　クライアント証明書の変更申請の手続き

日本銀行は、本書 3.1.5 に規定される方法でクライアント証明書の変更のための再発行申請の確認と認証を行います。

### 4.11　利用者に対する新しいクライアント証明書発行通知

日本銀行は、クライアント証明書の変更のための再発行申請を承認された申請者に対して、クライアント証明書の再発行申請に必要な情報を通知します。

### 4.12　変更されたクライアント証明書の受領確認の行為

日本銀行は、申請者による Web を用いたクライアント証明書の発行申請の後に、当該申請者のクライアント証明書の生成を行います。クライアント証明書が生成され次第、申請者は変更されたクライアント証明書をダウンロードして受領します。

### 4.13　失効が行われる場合

日本銀行は、以下の事由の際に、クライアント証明書の失効（取消し）処理を行います。

- システム利用者がオンラインシステムの利用を取止めるとき
- システム利用者の秘密鍵が危殆化した場合、もしくは、その恐れがあると判断できる場合
- システム利用者等が申請した重要な事実（情報）が虚偽であると判断できる場合
- クライアント証明書に記載された情報に誤りがある場合
- クライアント証明書に記載された情報に変更が発生した場合
- システム利用者、もしくは、利用組織がオンラインシステム用認証局の利用規約に違反したと判断できる場合
- システム利用者との利用規約が解除された場合
- システム利用者、もしくは、利用組織と日本銀行との契約が終了した場合
- システム利用者がクライアント証明書の失効の申請を行った場合
- 日本銀行がクライアント証明書の失効が必要と判断した場合

### 4.14　クライアント証明書の失効申請手続き

クライアント証明書の失効（取消し）を要求しようとするシステム利用者等は、別途定める方法を用いて日本銀行にクライアント証明書の取消しを申請することとします。

### 4.15　認証局が失効申請を処理しなければならない期間

日本銀行は、遅延なく失効申請を処理します。

### 4.16　利用の終了

オンラインシステムの利用を終了するシステム利用者は、別途定める方法を用いて日本銀行にクライアント証明書の取消しを申請することとします。

# 5　設備上、運営上、運用上の管理

本章では、本認証局の設備上、運営上、運用上の管理について規定します。なお、本章では、必要に応じて、登録局、発行局に適用される要件を規定するものとします。

## 5.1　設備管理

発行局の設備管理については、NTT データに委託しており、本書では規定しません。

登録局の設備管理については、一定水準のセキュリティレベルを有する日本銀行において実施します。

## 5.2　手続的管理

本節では本認証局で行われる手続の管理方法について規定します。

### 5.2.1　信頼すべき役割

・登録局

登録局の機能を適切に提供するための体制を整備して、同機能を提供します。また、登録局の機能は、複数の役割によって提供します。

・発行局

発行局の機能を適切に提供するための体制を整備して、同機能を提供します。また、発行局の機能は、以下の役割を含む複数の役割によって提供します。

- キーマネージャー・・・認証局（ルート証明書）秘密鍵の管理を行う要員
- システムアドミンマネージャ・・・発行局のシステム管理に関する要員
- セキュリティーマネージャ・・・発行局のセキュリティ確保に関する要員

### 5.2.2　職務ごとに必要とされる人数

・登録局

登録局の機能は、複数人の関与によって提供します。

・発行局

各職務分掌を確実に実施するための方針と厳格な管理手続きを有しています。認証局用暗号モジュールデバイスおよび関連する秘密鍵関連資料等の最も機密となるものへのアクセスは、複数人の信頼される人物により行われます。

これらの手続きは、物理的または論理的に認証局用暗号モジュールデバイスへアクセスするために最低 2 名の信頼される人物が確実に必要となるようになっています。認証局用暗号モジュールデバイスへのアクセスは、その受け入れから廃棄時の論理的・物理的破壊までのライフサイクルを通じて、複数人の信頼される人物により実施されます。

認証局用暗号モジュールデバイスがサービスに利用されると、当該デバイスに関する一切の操作は、物理的および論理的にも複数人および複数の権限により管理されます。当該デバイスへの物理的なアクセスが出来る人物はシークレット・シェアを保有しておらず、シークレット・シェアを保有する人物は当該デバイスへの物理的なアクセスが出来ません。

## 5.3 人事的管理

・登録局

証明書発行等サービスの運用を行う要員の身元確認を実施します。また、証明書発行等サービスの運用を行う要員に対し、同サービスの運用に必要な知識および技術を習得するための教育訓練を行います。

・発行局

発行局は外部へ委託しており、外部委託先の要員に関する要件は本書では規定しません。

## 5.4 監査ログの手続

本節では本認証局で取得される監査ログについて規定します。

### 5.4.1 記録されるイベントの種類

次の重要なイベントについて、種類、日時を記録します。

クライアント証明書のライフサイクル管理に関するイベント

- クライアント証明書新規発行、更新、失効処理
- クライアント証明書および CRL の生成処理

セキュリティに関するイベント

- 発行局が設置された施設への来訪者の入退室記録
- システムへのアクセス記録

### 5.4.2 監査ログを検査する頻度

監査ログの検査は、本システムを安全に運営するために適切と考えられる頻度で実施されます。また、そのために必要な監査ログが記録されます。

### 5.4.3　監査ログを保持する期間

以下の期間、監査ログを保存します。

（1）クライアント証明書のライフサイクル管理に関するイベントは5年間保管されます。

（2）　セキュリティに関するイベントは1年間保管されます。

### 5.4.4　監査ログの保護

監査ログは、漏洩、改ざん、棄損等がないように安全に保管されます。

### 5.4.5　監査ログのバックアップ手続

定められたバックアップ手順に従いバックアップが行われます。

### 5.4.6　監査ログの収集システム

システムの自動処理およびオペレータによる手作業を組み合わせて収集されます。

### 5.4.7　イベントを発生させたサブジェクトに対する通知

監査ログの確認時に、調査の必要性がある事象が検出された場合、当該事象を発生者に対し通知することなく調査を行うことが出来るものとします。

## 5.5　危殆化および災害からの復旧

本節では認証局秘密鍵の危殆化時や認証局設備が被災したときの手続きについて規定します。

### 5.5.1　危殆化および被災時の取扱手続き

発行局では認証局秘密鍵の危殆化または何らかのセキュリティインシデントが発生した場合の手続きを定めており、当該手続きに従い適切に対応します。

### 5.5.2　コンピュータの資源、ソフトウェア、またはデータが破損した場合

・登録局

コンピュータ設備は冗長化されており、ハードウェアが破損した場合、待機系のハードウェアにより業務を継続します。データが破損した場合、バックアップされたデータにより復旧させます。

・発行局

設備は冗長化されており、ハードウェアが破壊した場合、待機系のハードウェアにより業務を継続します。ソフトウェアまたはデータが破壊した場合、バックアップされたソフトウェアまたはデータにより復旧させます。

### 5.5.3　クライアント証明書秘密鍵が危殆化した場合の手続

システム利用者は、クライアント証明書秘密鍵の危殆化を認識した場合またはその疑いがある場合には、直ちにその旨を日本銀行に通知するとともに、クライアント証明書の失効申請を行わなければなりません。

### 5.5.4　災害後の事業継続能力

・登録局

災害時の状況によりサービス運用の継続可否を判断します。

・発行局

充分に遠隔な地域に災害対策用の設備を設けており、災害発生時には、秘密鍵の危殆化の恐れがない場合、災害対策用の設備によりサービス運用を継続します。

## 5.6　認証局サービスの終了

本認証局のサービスを終了する場合、その終了に先立って終了プランを作成します。当該終了プランの作成においては、以下の事項の検討を行います。

- 本認証局の終了を通知するための方法や実施方法
- 発行済みクライアント証明書や CRL の取り扱い
- リポジトリの取り扱い

# 6　技術的セキュリティ管理

本章では、本認証局の技術的セキュリティ管理について規定します。

## 6.1　鍵ペアの生成およびインストール

本節では各鍵ペアに関する要件について規定します。

### 6.1.1　鍵ペアの生成

・ルート認証局証明書の鍵ペア

ルート認証局証明書の鍵ペア生成は、複数人の立会いの下、一名による操作では出来ない方法により、発行局認証設備室内に設置された専用の暗号モジュールデバイスの中で行われます。

・クライアント証明書の鍵ペア

クライアント証明書の鍵ペア生成は、システム利用者が管理するデバイスで行われます。

### 6.1.2　システム利用者に対する秘密鍵の交付

日本銀行が適用する証明書発行等サービスでは、システム利用者の秘密鍵は該当システム利用者自身により生成されます。このため、秘密鍵のシステム利用者への受渡は生じません。

### 6.1.3　鍵ペアのサイズ

日本銀行が提供する証明書発行等サービスでは、使用する鍵ペアのサイズを証明書の種類ごとに以下のとおり規定します。

ルート認証局証明書：暗号アルゴリズムが RSA で、鍵長が 2048bit

クライアント証明書：暗号アルゴリズムが RSA で、鍵長が 2048bit

### 6.1.4　鍵の用途

・ルート認証局証明書の秘密鍵

クライアント証明書に対する電子署名と CRL に対する電子署名

| 証明書の種類 | 証明書のエクステンション |
|---|---|
| ルート認証局証明書 | Certificate Signing, CRL Signing |

・クライアント証明書の秘密鍵

電子署名と鍵の暗号化

| 証明書の種類 | 証明書のエクステンション |
|---|---|
| クライアント証明書 | DigitalSignature,KeyEncipherment |

## 6.2　秘密鍵の保護および暗号モジュール技術の管理

本節では認証局の秘密鍵およびシステム利用者の秘密鍵の管理に関する要件について規定します。

### 6.2.1　暗号モジュールの管理

・ルート認証局証明書の秘密鍵

ルート認証局証明書の秘密鍵は認証局設備内において暗号モジュールデバイス内で保護されています。暗号モジュールデバイスは FIPS 140-1 level 3 相当の暗号モジュールを利用しています。

・クライアント証明書の秘密鍵

システム利用者により適切に保護し管理されます。

### 6.2.2　秘密鍵の"n of m"による複数人管理

・ルート認証局証明書の秘密鍵

機密を要する認証局設備の暗号運用については複数人の信頼出来る要員が関与することを要求する技術的且つ手続的な仕組みを実施しています。ルート認証局証明書の秘密鍵へアクセスするために「シークレット・シェアリング」という仕組みを採用しています。

この仕組みでは、必要な活性化データを「シークレット・シェア」と呼ばれる別々のパーツに分割することで、「シェアホルダー」と呼ばれる必要な訓練を受けた信頼できる要員が保有します。特定のハードウェア暗号モジュールデバイスに保管されているルート認証局証明書の秘密鍵を活性化させるためには、ハードウェア暗号モジュールデバイスに対して生成・分割されたシークレット・シェア総数（m）のうち、一定数（n）の「シークレット・シェア」が必要となります。

・クライアント証明書の秘密鍵
システム利用者により適切に管理されます。

### 6.2.3　秘密鍵のバックアップ

・ルート認証局証明書の秘密鍵
ルート認証局証明書の秘密鍵は、秘密鍵が格納されているハードウェア暗号モジュールデバイスと同等のハードウェア暗号モジュールデバイス間の複製機能によりバックアップを行います。バックアップは複数人の管理の下、発行局設備室内にて行われ、バックアップされたハードウェア暗号モジュールデバイスも安全な場所に保管されます。

・クライアント証明書の秘密鍵
システム利用者により必要に応じてバックアップを行います。

### 6.2.4　秘密鍵の暗号モジュールへの転送または暗号モジュールからの転送

・ルート認証局証明書の秘密鍵
ルート認証局証明書の秘密鍵はハードウェア暗号モジュールデバイスで生成され、バックアップを作成するという特別なケース以外ではハードウェア暗号モジュールデバイスから取り出されることがありません。

### 6.2.5　秘密鍵の活性化方法

・ルート認証局証明書の秘密鍵
ルート認証局証明書の秘密鍵については本書 6.2.2 を参照ください。

### 6.2.6　秘密鍵の非活性化方法

・ルート認証局証明書の秘密鍵
ルート認証局証明書の秘密鍵はシステムの停止、もしくは、ハードウェア暗号モジュールデバイスをデバイスリーダから抜き取ることにより非活性化します。

### 6.2.7　秘密鍵の破棄方法

・ルート認証局証明書の秘密鍵
ルート認証局証明書の秘密鍵の廃棄を行う場合は、専用の機器を用いて、複数人の管理のもと秘密鍵を完全に復元できない方法により行われます。また、バックアップされたハードウェア暗号モジュールデバイス内にある秘密鍵も同じ方法により破棄されます。

### 6.2.8　暗号モジュールの評価

6.2.1 項で規定した通りです。

## 6.3　その他の鍵ペア管理

本節では鍵ペアの管理に関するその他の事項について規定します。

### 6.3.1　公開鍵のアーカイブ

・ルート認証局証明書

ルート認証局証明書は、本サービスが提供されている間はアーカイブされます。

・クライアント証明書

クライアント証明書は、本サービスが提供されている間はアーカイブされます。

### 6.3.2　証明書の運用上の期間および鍵ペアの使用期間

・ルート認証局証明書

規定しません。

・クライアント証明書

３年間とします。

## 6.4　活性化データ

ルート認証局証明書の秘密鍵およびクライアント証明書の秘密鍵を活性化するためのデータに関して規定します。

### 6.4.1　活性化データの生成および設定

・ルート認証局証明書

ルート認証局証明書の秘密鍵は「シークレット・シェア」によって活性化されます。「シークレット・シェア」は、別途定められた方法により生成および配布されます。

### 6.4.2　活性化データの保護

・ルート認証局証明書

ルート認証局証明書の秘密鍵の活性化データは複数人に分割されて管理されています。各活性化データは権限者により厳重に管理されます。

## 6.5　コンピュータのセキュリティ管理

本節では本認証局におけるコンピュータセキュリティについて規定します。

### 6.5.1　コンピュータのセキュリティに関する技術的要件

・登録局

日本銀行の判断に基づき適切なセキュリティを設定します。

・発行局

アクセス制御機能、監査ログ記録機能を持つ信頼性の高いシステムにより運営されます。

### 6.5.2　コンピュータセキュリティ評価

・登録局

使用されるハードウェアおよびソフトウェアについては、セキュリティに関する情報等を必要に応じて収集し、それを評価することにより、適切に維持管理されます。

・発行局

使用されるハードウェアおよびソフトウェアについて、セキュリティに関する情報等を必要に応じて収集し、それを評価することにより、別途定めたセキュリティに関する基準を満たすように維持管理されます。

## 6.6　ライフサイクルの技術上の管理

本節では本認証局のシステムライフサイクルにおけるセキュリティ管理について規定します。

### 6.6.1　システム開発

システム開発およびメンテナンスには、所定の手続きにより、信頼出来る環境下において実施されます。

### 6.6.2　セキュリティ運用

ソフトウェアの設定等は、所定の手順により、その完全性、バージョン、および、その設定等が管理されています。

## 6.7　ネットワークセキュリティ管理

本節では本認証局のネットワークにおけるセキュリティ管理について規定します。

アクセス権限の無い者によるアクセスおよびその他不正な活動を防止するため、所定の手続きに従い、セキュリティの確保されたネットワークを用いています。秘密とすべき情報の通信には、必要に応じて暗号化を用いています。

# 7　証明書プロファイル

## 7.1　証明書プロファイル

### 7.1.1　ルート認証局証明書

| 領域名 | クリティカルフラグ | 値(例) | 説明 |
|---|---|---|---|
| **Version**<br>(バージョン番号) | — | 2 | 証明書のバージョンが X.509 のバージョン 3 であることを示す。INTEGER 型。 |
| **serial Number**<br>(シリアル番号) | — | 0bd0 ee62 879f 1c6c 8826 d82b 41a8 f690 | 証明書のシリアル番号を示す。INTEGER 型。 |
| **signature algorithm ID**<br>(署名アルゴリズム) | — | | ルート認証局が、ルート認証局証明書に署名する際に使用した署名アルゴリズム。 |
| algorithm identifier<br>(アルゴリズム識別子) | | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption を表す OID の値を示す。 |
| **issuer name**<br>(発行者名) | — | CN = Gaitame CA - G5<br>O = Bank Of Japan<br>C = JP | 認証局証明書の識別名 (DN) を示す。英語表記。 |
| **validity period**<br>(証明書有効期間) | — | | 証明書の有効期間を示す。 |
| notBefore<br>(発行日) | | *YYMMDDHHMMSSZ*<br>220304000000Z | 証明書の有効期間開始日を示す。UTCTime 型。 |
| notAfter<br>(終了日) | | *YYMMDDHHMMSSZ*<br>320229235959Z | 証明書の有効期間終了日を示す。UTCTime 型。 |
| **subject name**<br>(主体者名) | — | CN = Gaitame CA - G5<br>O = Bank Of Japan<br>C = JP | 認証局証明書の識別名 (DN) を示す。英語表記。 |
| **subject public key info**<br>(主体者公開鍵情報) | — | | 証明書の公開鍵アルゴリズムを示す。 |
| algorithm identifier<br>(アルゴリズム識別子) | | 1.2.840.113549.1.1.1 | 証明書の公開鍵アルゴリズム識別子である、rsaEncryption を表す OID の値を示す。 |
| Parameter<br>(パラメータ) | | NULL | RSA の場合、本項目には値が設定されない。 |
| public key<br>(公開鍵) | | *BIT STRING* | 証明書の公開鍵の値を示す。BIT STRING 型。 |
| **Extensions**<br>(証明書拡張領域) | | | |
| **basicConstraints**<br>(基本制約) | TRUE | | 認証局証明書であるかどうか、および認証局証明書の階層の制限を示す。 |
| cA | | TRUE | 認証局証明書であることを示す。 |
| pathlen | | 0 | 下位認証局を作成するかを示す。 |
| **keyUsage**<br>(鍵用途) | TRUE | | 鍵の使用目的を設定する。 |
| Certificate Signing | | 1 | 証明書用途であることを示す。 |
| CRL Signing | | 1 | CRL 用途であることを示す。 |
| **subjectKeyIdentifier**<br>(サブジェクトキーの識別子) | FALSE | 674f 2b27 71b1 6645 ecc3 6db4 2d80 c9f1 e732 aa38 | ルート認証局証明書の RSA 鍵ペアを識別する情報を設定する。 |

### 7.1.2　クライアント証明書

| 領域名 | クリティカルフラグ | 値(例) | 説明 |
|---|---|---|---|
| Version<br>(バージョン番号) | ― | 2 | 証明書のバージョンが X.509 のバージョン 3 であることを示す。INTEGER 型。 |
| serial Number<br>(シリアル番号) | ― | 362b 8aa7 181b ecb4 9952 009d d1ce 27 (例) | 証明書のシリアル番号を示す。INTEGER 型。 |
| signature algorithm ID<br>(署名アルゴリズム) | ― | | 認証局証明書を用い、クライアント証明書に署名する際に使用した署名アルゴリズム。 |
| algorithm identifier<br>(アルゴリズム識別子) | | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption を表す OID の値を示す。 |
| issuer name<br>(発行者名) | ― | CN = Gaitame CA - G5<br>O = Bank Of Japan<br>C = JP | 認証局証明書の識別名 (DN) を示す。 |
| validity period<br>(証明書有効期間) | ― | | 証明書の有効期間を示す。 |
| notBefore<br>(発行日) | | *YYMMDDHHMMSSZ*<br>130511000000Z(例) | 証明書の有効期間開始日を示す。UTCTime 型。 |
| notAfter<br>(終了日) | | *YYMMDDHHMMSSZ*<br>160510235959Z(例)　*※3 年間* | 証明書の有効期間終了日を示す。UTCTime 型。 |
| subject name<br>(主体者名) | ― | ※日本銀行が作成した命名規則（非公表）に基づき、システム利用者を識別できる識別名を設定する。 | システム利用者の識別名 (DN) を示す。CN と C は PrintableString、メールアドレスは IA5STRING、その他は T61String を使用。<br>*※斜字箇所はポリシー設定による。* |
| subject public key info<br>(主体者公開鍵情報) | ― | | 証明書の公開鍵アルゴリズムを示す。 |
| algorithm identifier<br>(アルゴリズム識別子) | | 1.2.840.113549.1.1.1 | 証明書の公開鍵アルゴリズム識別子である、rsaEncryption を表す OID の値を示す。 |
| Parameter<br>(パラメータ) | | NULL | RSA の場合、本項目には値が設定されない。 |
| public key<br>(公開鍵) | | *BIT STRING* | 証明書の公開鍵の値を示す。BIT STRING 型。 |
| Extensions<br>(証明書拡張領域) | | | |
| basicConstraints<br>(基本制約) | FALSE | | 認証局証明書であるかどうか、および認証局証明書の階層の制限を示す。 |
| cA | | FALSE | 認証局証明書ではなく、エンド・エンティティ証明書であることを表す。Internet Explorer では「Subject Type=End Entity」と表示される。 |
| Pathlen | | NULL | 下位認証局を作成するかを示す。 |

| 領域名 | クリティカルフラグ | 値(例) | 説明 |
|---|---|---|---|
| **keyUsage**<br>(鍵用途) | FALSE | | 鍵の使用目的を設定する。 |
| digitalSignature | | 1 | 署名に使用することを表す。 |
| KeyEncipherment | | 1 | 共通鍵の暗号化に使用することを表す。 |
| **cRLDistributionPoints**<br>(CRL 配布点) | FALSE | URL=https://www.ccissue.opencanvas.ne.jp/crl/0000-0C000000001C/0000-0C0000001C.crl | CRL の配布点を、URI と fullName を使用して示す。 |

## 8　準拠性監査とその他の評価

本認証局は発行局の業務を NTT データが提供する PKI サービスを利用して実現しています。発行局の監査については、本認証局の運営主体と NTT データとのサービス利用契約に基づくものとし、本書では規定しません。

登録局の監査については、日本銀行によって適切に実施します。

# 9　他の業務上および法的問題

## 9.1　料金

日本銀行は、システム利用者に対し、証明書発行等サービスに関し、手数料を請求しません。

## 9.2　業務において機密として取り扱う情報の管理

本節では、日本銀行が証明書発行等サービスで機密として取り扱う情報について規定します。

### 9.2.1　機密として取り扱う情報の範囲

日本銀行では、以下の情報を機密として取扱います。

- クライアント証明書の発行申請時にシステム利用者から提出された情報
- クライアント証明書の失効申請時にシステム利用者から提出された情報
- クライアント証明書の発行申請や失効申請の各種処理の記録
- 日本銀行に対する個別の問い合わせの内容
- 日本銀行が活用するハードウェア、ソフトウェア、ネットワーク等の詳細
- 災害復旧計画
- 監査の記録

ただし、9.2.2 において明示的に秘密としてみなされないと規定されている情報については、機密として取り扱いません。

### 9.2.2　機密として取り扱わない情報

日本銀行では、9.2.1 で明示的に機密として取り扱うと規定された情報以外は機密として取り扱いません。また、日本銀行が発行するクライアント証明書に記載されている情報、CRL に記載されている情報、並びに、リポジトリで公開される情報については機密としてみなされません。

### 9.2.3　機密として取り扱う情報の保護

日本銀行では、機密として取り扱う情報の保護を充分に行います。本サービスの運営上必要となる範囲以外に機密として取り扱う情報の利用を行いません。

## 9.3　個人情報保護

日本銀行では、システム利用者から受領する個人情報の保護について、重要性を充分に認識し、保護を適切に行います。

## 9.4　知的財産権

本サービスに関してシステム利用者へ提供される資料等の知的財産権については、日本銀行に帰属します。

## 9.5　表明保証

本節では本サービスの関係者における保証について規定します。

### 9.5.1　認証局の義務と責任

日本銀行はシステム利用者に対して、次の事項を保証します。

- クライアント証明書に記載される事実には、日本銀行が知り、またはそこから生じる重要な不実の記載は存在しないこと。
- クライアント証明書中の情報には、日本銀行が、クライアント証明書の発行申請の取扱において合理的注意を用いることを怠ったことにより生じた誤りが存在しないこと。
- システム利用者よりクライアント証明書の取消し申請があった場合には、取消し申請の審査および取消し手続きに相当な注意を払い、取消し対象のクライアント証明書を取消すこと。
- クライアント証明書が本書に定める全ての重要な要件に合致していること。

利用規約には、追加の表明と保証を定めることが出来る。

### 9.5.2　利用者の義務と責任

システム利用者は、クライアント証明書の秘密鍵が危殆化した場合（または危殆化する惧れがある場合）、またはその秘密鍵を保護するデータもしくはクライアント証明書中の情報が不正確であるか変更されたという事態が生じた場合には、クライアント証明書の取消し請求を日本銀行に対し速やかに行うこと。

また、システム利用者は、日本銀行に対し、クライアント証明書が、正当で合法的な目的のためにのみ、かつ、本書を遵守した態様によってのみ、使用されることを保証する。

利用規約には、追加の表明と保証を定めることが出来る。

## 9.6　保証の否認

適用される法律上許される範囲内において、オンラインシステム用認証局の利用規約は、日本銀行のその他一切の保証を否定します。

## 9.7　責任の制限

日本銀行は、クライアント証明書の取得、使用等によって生じた損害に対する賠償責任を、一切負いません。

## 9.8　有効期間と終了

本節では、本書の有効期間について規定します。

### 9.8.1　有効期間

本書は、日本銀行のホームページおよびオンラインシステムに掲載されたときに有効になります。本書の変更も、日本銀行のホームページおよびオンラインシステムに掲載されたときに有効になります。

### 9.8.2　終了

本書は、新たな本書が効力を発するまで、有効とします。

### 9.8.3　終了の効果と効果の残存

本書が終了した場合においても、システム利用者は発行したクライアント証明書の残存有効期間中は、本書の条項に拘束されるものとします。

## 9.9　改訂

本節では、本書の改訂手続きについて規定します。

### 9.9.1　改訂手続き

システム利用者の事前の了解を得ることなく、必要に応じて適宜本書の内容を変更することができるものとします。

## 9.10　紛争解決手続

本書のいずれかの事項にかかわる紛争を解決する場合、法的措置を講じる前に、システム利用者は、日本銀行その他の紛争にかかわる当事者に通知して、当事者間で紛争の解決を求めることとします。当事者間で紛争が解決出来なかった場合、当該紛争の解決については東京地方裁判所を第一審の専属管轄裁判所とします。

## 9.11　準拠法

本書は日本法に準拠し解釈されるものとします。

## 9.12　雑則

本節では、本書に関するその他雑則について規定します。

### 9.12.1　分離可能性条項、残存規定条項、完全合意性条項、通知条項

本書の一部分の規定が、いかなる程度でも無効又は執行不可能であるとされた場合であっても、本書のその他の規定の有効性には影響を及ぼさず、当事者の意思に最も合理的に合致するよう解釈されるものとします。

付録　用語集

| 用語 | 定義 |
|---|---|
| 日本銀行外為法手続きオンラインシステム用認証局（オンラインシステム用認証局） | 日本銀行外為法手続きオンラインシステム用認証局は、日本銀行外為法手続きオンラインシステムにおけるクライアント証明書の発行、更新、取消しおよび管理を含む一連のサービスを提供する機関である。なお、日本銀行は、日本銀行外為法手続きオンラインシステム用認証局の運用業務の一部を、NTT データに委託している。 |
| 日本銀行外為法手続きオンラインシステム（オンラインシステム） | 届出・報告（外国為替および外国貿易法において日本銀行が事務委任を受けて受理する届出および報告をいう。以下同じ。）の手続きに係るものを処理するシステムおよび電子届出・報告の手続きを支援するための各種情報等を提供するシステム。 |
| システム利用者等 | 「システム利用者」および「申請者」を示す。 |
| 本書 | 「日本銀行外為法手続きオンラインシステム用認証局<br>Certification Practice Statement」を示す。 |
| Certification Practice Statement | 認証局の信頼性および安全性をシステム利用者が評価できるように、認証局のセキュリティポリシー、責任や義務、約款などに関する詳細を規定した文書。 |
| オブジェクト識別子 | 一意となる値による識別子であり、登録機関に登録される。PKI で利用するアルゴリズム、電子証明書内に格納する名前のタイプ等は、オブジェクト識別子として登録されているものが使用される。 |
| PKI | Public Key Infrastructure の略。<br>公開鍵と秘密鍵の対応関係を、認証局を用いて保証する技術基盤、環境を指す。 |
| 認証局 | 1.3.1 章を参照。 |
| 登録局 | 1.3.2章を参照。 |
| 発行局 | 1.3.3章を参照。 |
| リポジトリ | 本認証局の運用を円滑に行うための各種情報を公開するサイトを示す。 |
| CRL | クライアント証明書の失効情報リストを示す。 |
| 本認証局 | 「日本銀行外為法手続きオンラインシステム用認証局」を示す。 |
| 依拠当事者 | 1.3.5章を参照。 |

| 用語 | 定義 |
| --- | --- |
| ルート認証局証明書 | 本認証局における最上位の認証局証明書を示し、日本銀行の独自ルート証明書となる。 |
| 識別名 | 証明書の所有者や認証局の名前の情報。 |
| リキー | 証明書の更新。 |
| 鍵ペア | 秘密鍵とそれに対応する公開鍵。 |
| 危殆化 | 暗号アルゴリズムの安全性が、計算機能力の向上や暗号解読手法の進歩にともなって次第に低下することを示す。 |
| 暗号モジュール | 暗号機能により安全性を確保したソフトウェアまたはハードウェア。 |
| 監査ログ | 認証局の監査を行う上で監査対象となる証跡。 |
| アーカイブ | 認証局にて保管する文書またはデータ。 |
| 表明保証 | 契約事項が正確であることを表明し、その内容を保証することを示す。 |
| 利用規約 | 「日本銀行外為法手続きオンラインシステム用認証局が発行する証明書に関する利用規約」を示す。 |