KS Solutions 証明書発行サービス
認証局運用規則

(KS-SOL 認証局版)

Version 2.0

株式会社オプテージ

改訂履歴

Version	変更内容	日付	作成者/変更者	日付	承認者
1.0	新規作成	2016.03.31	岩佐	2016.03.31	平賀
2.0	・社名変更 ・受領確認時の運用を変更 ・ＵＳＢトークン証明書配布時の運用を追加 ・証明書配送時に関する文言変更 ・発行局業務に関する文言削除	2019.04.01	小谷	2019.04.01	
	・ユーザ証明書インストール時にセキュリティデバイスが接続できない端末を利用する場合の運用を追加	2019.04.01	林	2019.04.01	

商標に関する表示

本文書で使用している社名、製品名等は、各社の登録商標または商標です。

目　次

１．はじめに 7
１．１　概要 7
１．２　識別 8
１．３　参加者と適用範囲 8
１．３．１　認証局 9
１．３．２　発行局 10
１．３．３　登録局 10
１．３．４　利用企業 10
１．３．５　証明書利用者 11
１．３．６　依拠当事者 11
１．３．７　適用可能性 11
１．４　連絡先 12
２．　一般規定 13
２．１　義務 13
２．１．１　認証局の義務 13
２．１．２　発行局の義務 13
２．１．３　登録局の義務 13
２．１．４　利用企業の義務 14
２．１．５　証明書利用者の義務 14
２．１．６　依拠当事者の義務 14
２．１．７　リポジトリの義務 15
２．２　責任 15
２．２．１　認証局の責任 15
２．２．２　利用企業の責任 16
２．２．３　証明書利用者の責任 16
２．２．４　依拠当事者の責任 16
２．３　財務上の責任 16
２．４　解釈、および、執行 16
２．４．１　準拠法 16
２．４．２　分割、相続、合併、および通知 17
２．４．３　紛争解決の手続き 17
２．５　料金 17
２．６　公表およびリポジトリ 17

２．６．１　認証局に関する情報の公表 17
２．６．２　公表の頻度 18
２．６．３　アクセス制御 18
２．６．４　リポジトリ 19
２．７　準拠性監査 19
２．７．１　準拠性監査の頻度 19
２．７．２　監査人の識別／認定 19
２．７．３　監査人と被監査人との関係 19
２．７．４　準拠性監査のトピック 19
２．７．５　監査指摘項目への対応 19
２．７．６　監査結果 19
２．８　機密保持 20
２．８．１　機密扱いとする情報 20
２．８．２　機密扱いとしない情報 20
２．８．３　証明書失効情報の公表 20
２．８．４　法執行機関への情報公開 20
２．８．５　民事手続き上の情報公開 20
２．８．６　ユーザの要求に基づく公開 20
２．８．７　その他の公開条件 21
２．９　知的財産権 21
３．識別と認証 22
３．１　初期登録 22
３．１．１　名称のタイプ 22
３．１．２　名称の意味 25
３．１．３　名称を解釈するためのルール 25
３．１．４　名称のユニーク性 25
３．１．５　名称に関する紛争解決手段 26
３．１．６　商標の認定、認証、役割 26
３．１．７　秘密鍵の所有を証明する方法 26
３．１．８　組織の認証 26
３．１．９　個人の認証 27
３．２　証明書の更新 28
３．３　再発行 28
３．４　失効要求 28
４．運用要件 30
４．１　証明書申請 30

４．２　証明書発行 30
４．３　証明書の受領 31
４．４　証明書失効および一時停止 33
４．４．１　失効条件 33
４．４．２　失効要求者 34
４．４．３　失効手続き 34
４．４．４　失効要求の猶予期間 35
４．４．５　一時停止条件 35
４．４．６　一時停止要求者 35
４．４．７　一時停止手続き 35
４．４．８　一時停止期間の制限 35
４．４．９　失効情報の発行頻度 36
４．４．１０　失効情報の確認要件 36
４．４．１１　オンラインステータスチェック 36
４．４．１２　オンライン失効チェック要件 36
４．４．１３　その他の利用可能な失効情報確認手段 36
４．４．１４　その他の利用可能な失効情報確認手段における要件 36
４．４．１５　危殆化時の特別対応 36
４．５　セキュリティ監査の手順 36
４．５．１　記録される情報のタイプ 36
４．５．２　ログが処理、検査される頻度 37
４．５．３　監査ログの保管期間 37
４．５．４　監査ログの保護 37
４．５．５　監査ログのバックアップ手順 37
４．５．６　監査ログの収集システム 36
４．５．７　監査結果の通知 37
４．５．８　脆弱性評価 37
４．６　記録のアーカイブ 37
４．６．１　アーカイブデータの種類 37
４．６．２　アーカイブデータの保管期間 38
４．６．３　アーカイブデータの保護 38
４．６．４　アーカイブデータのバックアップ手順 38
４．６．５　記録へのタイムスタンピング要件 38
４．６．６　アーカイブデータの収集システム 38
４．６．７　アーカイブデータの入手、検証手続き 39
４．７　鍵更新 39

４．８　危殆化と災害復旧 39
４．９　認証業務の終了 39
５．物理面、手続き面および人事面のセキュリティ統制 40
５．１　物理的統制 40
５．１．１　施設の位置と建物構造 40
５．１．２　物理的アクセス 40
５．２　手続き統制 42
５．３　人事統制 44
６．技術的セキュリティ統制 45
６．１　鍵ペアの生成とインストール 45
６．１．１　鍵ペア生成 45
６．１．２　秘密鍵の配布方法 45
６．１．３　公開鍵の提出方法 45
６．１．４　認証局公開鍵の提供方法 45
６．１．５　鍵長 45
６．１．６　公開鍵パラメータの生成 45
６．１．７　パラメータ品質の検査 46
６．１．８　鍵を生成するハードウェア／ソフトウェア 46
６．１．９　鍵使用目的 46
６．２　秘密鍵の保護 46
６．２．１　暗号モジュールに関する標準 46
６．２．２　秘密鍵の複数人制御 46
６．２．３　秘密鍵の預託 47
６．２．４　秘密鍵のバックアップ 47
６．２．５　秘密鍵のアーカイブ 47
６．２．６　暗号モジュールへの秘密鍵の格納 47
６．２．７　秘密鍵の活性化方法 47
６．２．８　秘密鍵の非活性化方法 48
６．２．９　秘密鍵の破棄方法 48
６．３　鍵ペア管理に関するその他の項目 48
６．３．１　公開鍵のアーカイブ 48
６．３．２　鍵ペアの利用期間 48
６．４　活性化データ 48
６．４．１　活性化データの生成とインストール 48
６．４．２　活性化データの保護 49
６．４．３　活性化データに関するその他の項目 49

６．５　ネットワークセキュリティ統制 49
６．６　暗号モジュールの技術統制 48
７．　証明書と CRL/ARL のプロファイル 50
７．１　証明書のプロファイル 50
７．１．１　バージョン番号 50
７．１．２　拡張領域 50
７．１．３　アルゴリズムのオブジェクト識別子 50
７．１．４　名前の形式 50
７．１．５　名前制約 51
７．１．６　証明書ポリシーのオブジェクト識別子 51
７．１．７　ポリシー制約拡張子の利用 51
７．１．８　ポリシー修飾子の記載と意味 51
７．１．９　クリティカルな拡張フィールドの処理方法 51
７．２　失効情報のプロファイル 51
７．２．１　バージョン番号 51
７．２．２　CRL/ARL およびエントリの拡張子 51
８．仕様管理 52
８．１　仕様の変更手続き 52
８．２　公表と通知に関する方針 52
８．３　CPS の承認 52

１．はじめに

１．１　概要

KS Solutions 証明書発行サービス（以下「本サービス」という）とは、株式会社オプテージ（以下「オプテージ」という）が、本サービスを利用する法人等（以下「利用企業」という）の社員および役員等に対して公開鍵証明書（以下「ユーザ証明書」という）を発行する、もしくは、サーバ等に対して公開鍵証明書（以下「サーバ証明書」という）を発行するサービスである。本文書（以下「本 CPS（Certification Practice Statement）」という）は、オプテージが本サービスを実施するにあたり、基本的なポリシーを定めた規定集である。本 CPS 中の用語に関する説明は、付録 C を参照のこと。

本 CPS は、IETF（Internet Engineering Task Force）の PKIX（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施の枠組み（Certificate Policy and Certification Practices Framework）」（RFC2527）に準拠したものである。

オプテージは、本 CPS に従って、本サービスにおけるルート認証局（以下「KS Solutions ルート認証局」という）、ユーザ証明書を発行する中間認証局（以下「KS Solutions ユーザ証明書認証局」という）、および、サーバ証明書を発行する中間認証局（以下「KS Solutions サーバ証明書認証局」という）を運用する。本 CPS では、KS Solutions ルート認証局、KS Solutions ユーザ証明書認証局、および、KS Solutions サーバ証明書認証局をまとめて「本認証局」という。また、ユーザ証明書とサーバ証明書をまとめて「証明書」という。本 CPS には、本認証局が証明書の発行、管理、失効および更新を含む一連のサービスを提供する際の手続きを記載する。

本認証局は、本認証局の業務の一部を外部に委託する場合がある。業務の一部を委託する場合、本認証局は、委託先が本 CPS に従うよう適切に管理を行う。

KS Solutions ユーザ証明書認証局は、以下の用途の証明書を発行する。

- 利用企業の社員、役員および利用企業との間の契約で定められた者等（以下「外部委託者」という）を対象に、情報システム等へのアクセスコントロールおよび電子メールの署名・暗号化に利用することを目的とする公開鍵証明書

KS Solutions サーバ証明書認証局は、以下の用途の証明書を発行する。

- 利用企業のサーバを対象に、通信の暗号化に利用することを目的とする公開鍵証明書

本認証局に関する階層構造は、図１のとおりとする。

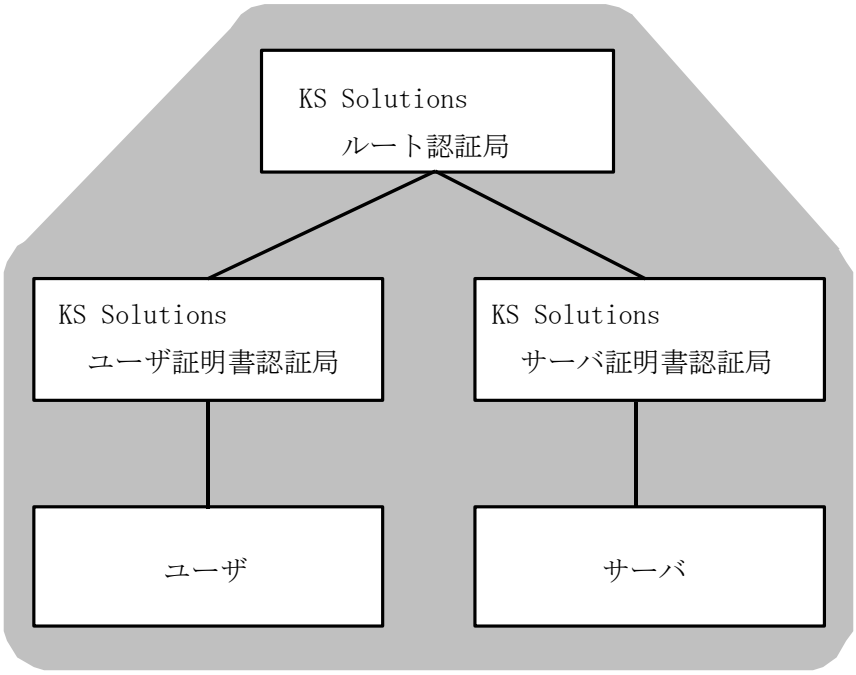

図 1　認証局の階層

１．２　識別

本サービスにおけるオブジェクト識別子（OID）は、表 1のとおりとする。

表 1　本サービスにおけるオブジェクト識別子（OID）

OID	オブジェクト
1.2.392.200174	株式会社オプテージ
1.2.392.200174.2	KS Solutions 証明書発行サービス
1.2.392.200174.2.1	KS Solutions 証明書発行サービス　認証局運用規則
1.2.392.200174.2.1.1	KS Solutions 証明書発行サービス証明書　ユーザ証明書ポリシー
1.2.392.200174.2.2.1	KS Solutions 証明書発行サービス証明書　サーバ証明書ポリシー

１．３　参加者と適用範囲

本認証局が提供する本サービスに関する参加者を図 2 に示す。

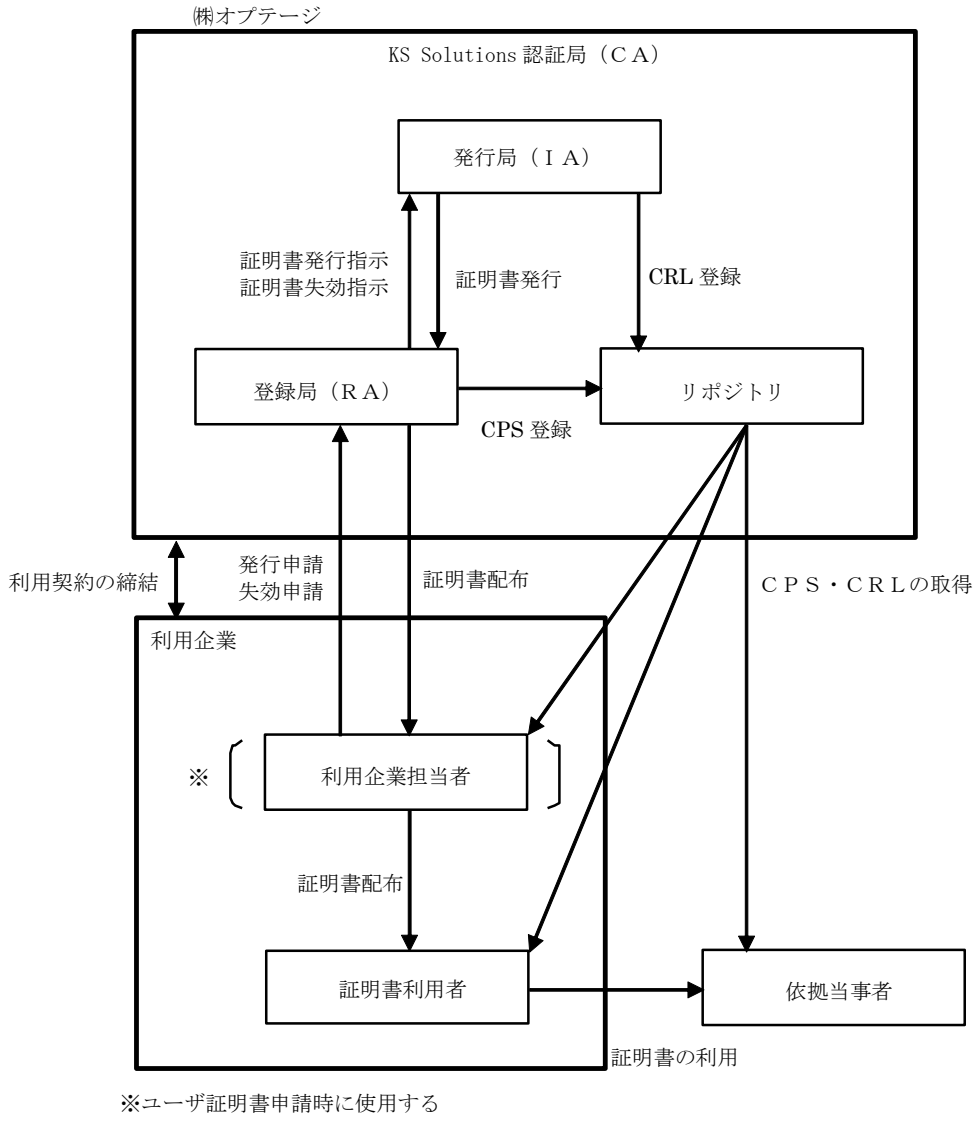

図 2　本サービスにおける参加者

本節では、これら参加者に関する説明と、本サービスにて発行した証明書の適用範囲についての説明を行う。

１．３．１　認証局

認証局（CA：Certification Authority）とは、証明書の発行、管理、失効を行う機関である。本認証局は、オプテージが運営主体となる。本認証局は、発行局（IA：Issuing Authority）、登録局（RA：Registration Authority）およびリポジトリから構成される。発行局に関しては本 CPS 1.3.2、登録局に関しては本 CPS 1.3.3 を参照のこと。本認証局のリポジトリは、登録局が運用する。

本認証局は、本認証局の業務の一部を外部に委託することができる。その場合、本認証局は外部委託先が本 CPS に準拠した運用を行うことを契約、その他の手段により管理する。

１．３．２　発行局

発行局は、認証局の秘密鍵を管理し、登録局から証明書発行データおよび証明書失効データによる発行および失効の指示を受け、証明書発行処理、証明書失効処理および失効情報（CRL（Certificate Revocation List）の発行を行う。発行局に関する設備等については、本 CPS 5 章にて後述するものとする。

１．３．３　登録局

登録局は、証明書の種類により以下の処理を行う。

- ユーザ証明書

  本 CPS1.3.4 に定める利用企業からのユーザ証明書に関する発行および失効の申請に基づき、証明書利用者の鍵ペアを生成し、発行局に対してユーザ証明書に関する発行および失効の指示を行う。また、当該証明書利用者の秘密鍵および発行局から発行されたユーザ証明書をＩＣカード・ＵＳＢトークン等のセキュリティデバイス（以下「セキュリティデバイス」という）に格納し、利用企業へ配布する。但し、証明書インストール時にセキュリティデバイスが接続できない端末を利用する場合は、PKCS#12 形式のデータを用い、ユーザ証明書利用者の秘密鍵とユーザ証明書（以下「ユーザ証明書一式」という）を利用企業へ送付する。

- サーバ証明書

  本 CPS1.3.4 に定める利用企業からのサーバ証明書に関する発行および失効の申請に基づき、発行局に対してサーバ証明書に関する発行および失効の指示を行う。また、発行局から発行されたサーバ証明書を利用企業へ配布する。

登録局は、本 CPS や CRL 等、本サービスに関連する公開情報を保管・公開するために、リポジトリを運用する。

登録局に関する設備等については、本 CPS 5 章にて後述するものとする。

１．３．４　利用企業

利用企業とは、本サービスを利用する企業である。

ユーザ証明書を使用する場合、利用企業は本サービスの利用に先立って、遵守すべき基本規則（以下、「利用法人規約」という）を遵守することを含む契約を、本認証局との間で締結しなければならない。本認証局との各種申請・セキュリティデバイス受領等の窓口業務については、当該利用企業の担当者（以下「利用企業担当者」という）のみが行うものと

する。利用企業は、本サービスを利用して当該利用企業内の社員、役員および外部委託者等のユーザ証明書についての発行および失効の申請を登録局に対して実施する。利用企業は、所属する当該利用企業内の社員、役員および外部委託者等に対して、本 CPS に基づいて認証を行わなければならない。利用企業は、登録局から受領した証明書利用者のセキュリティデバイスもしくはユーザ証明書一式を、確実に当該証明書利用者に配布しなければならない。

また、サーバ証明書を使用する場合、利用企業はサーバ等の証明書についての発行および失効の申請を登録局に対して実施する。利用企業は、登録局から受領したサーバ証明書を、確実に当該証明書利用者に配布しなければならない。

１．３．５　証明書利用者

ユーザ証明書利用者とは、本認証局が発行したセキュリティデバイスもしくはユーザ証明書一式を管理し、使用する者である。本認証局において、ユーザ証明書利用者は利用企業の社員、役員および外部委託者等である。また、サーバ証明書利用者とは、本認証局が発行したサーバ証明書を所持するものである。本認証局において、証明書利用者は利用企業のサーバ等である。ただし、証明書利用者が自然人でない場合、当該利用企業を証明書利用者に含むものとする。

本 CPS では、ユーザ証明書利用者、サーバ証明書利用者をまとめて「証明書利用者（EE：End Entity）」という。

１．３．６　依拠当事者

依拠当事者（RP：Relying Party）とは、証明書利用者が提示した証明書を利用する者あるいは設備である。

１．３．７　適用可能性

証明書利用者は、本サービスで発行する証明書を以下の用途で利用することができる。

・ユーザ証明書
  - 情報システム等への認証によるアクセスコントロール
  - 電子メールへの署名・暗号化

・サーバ証明書
  - 通信の暗号化
  - サーバへの認証

証明書を日本国外で利用する場合は、適用される法令、輸出規制等に従わなければならない。

本サービスで発行する証明書を、以下の用途に利用することは禁止する。

- 原子力の制御、航空管制、重要な交通の制御、医療等の人命の危険を伴う利用

- 障害により、人命や環境が危険にさらされるような重要な状況での利用
- 犯罪行為および公序良俗に反する利用
- 暗号技術を危殆化させるような試みへの利用

１．４　連絡先

本 CPS に関する連絡先は以下のとおりである。

問合せ先：株式会社オプテージ
電子認証業務担当窓口
電話番号：０６－６３５９－６８６６

２．　一般規定

２．１　義務

２．１．１　認証局の義務

本認証局は、本サービスの提供において、以下の義務を負う。

- 本認証局は、本 CPS に基づきサービスを提供する。
- 本認証局は、本 CPS 2.1.2 および本 CPS 2.1.3 に基づき実施される発行局と登録局の業務を統括し、本サービスが円滑に提供されるべく、運営を行う。
- 本認証局は、本サービスに関する本 CPS および関連文書を管理、改廃する。
- 本認証局は、本認証局における業務が適正に実施されることを確認するため、監査を行う。

２．１．２　発行局の義務

発行局は、本サービスの提供において、以下の義務を負う。

- 発行局は、本 CPS に基づき運用する。
- 発行局は、本 CPS に従い認証局の秘密鍵を生成し、危殆化することの無いように厳重に管理する。
- 発行局は、登録局の指示に従い、証明書発行要求の内容を正確に反映した証明書を発行する。
- 発行局は、登録局の指示に従い、証明書の失効を行う。
- 発行局は、24 時間に 1 回の頻度で CRL を更新する。

２．１．３　登録局の義務

登録局は、本サービスの提供において、以下の義務を負う。

- 登録局は、本 CPS に基づき運用する。
- 登録局は、利用企業からの申請に基づいて、発行局に対して証明書の発行指示、失効指示を行う。
- 登録局は、本 CPS に従いユーザ証明書利用者の秘密鍵を生成し、危殆化することのないように厳重に管理する。
- 登録局は、ユーザ証明書一式を生成後、当該秘密鍵を活性化させるための情報（Personal Identification Number、以下「利用者 PIN」という）を適切に設定する。
- 登録局は、セキュリティデバイスもしくはユーザ証明書一式を利用企業に確実に受け渡す。
- 登録局は、ユーザ証明書利用者のユーザ証明書一式を安全な環境で保管する。登録局は、ユーザ証明書の発行から最大 2 ヶ月を経過した時点で、バックアップと

して保管されたユーザ証明書利用者の秘密鍵および利用者 PIN を完全に削除する。
- 登録局は、サーバ証明書を利用企業に確実に受け渡す。
- 登録局は、利用企業から提示される証明書の発行に関する秘密情報を適切に取り扱う。
- 登録局はリポジトリの管理を行う。

２．１．４　利用企業の義務

利用企業は、本サービスの利用にあたり、以下の義務を負う。

- 利用企業は、ユーザ証明書を使用する際は利用法人規約に、サーバ証明書を使用する際は本 CPS に基づき、本サービスを利用する。
- 利用企業は、当該利用企業の証明書利用者に対し、本 CPS もしくは証明書利用者規約（本 CPS 2.1.5 を参照）で規定された証明書利用者の義務・責任を遵守させる。
- 利用企業は、証明書の申請の際に虚偽の申請を行わない。
- 利用企業は、証明書利用者の秘密鍵が危殆化したか、あるいは、そのおそれがある場合に、登録局に対し速やかに失効の申請を行う。
- 利用企業は、本認証局からセキュリティデバイスもしくはユーザ証明書一式および利用者 PIN を、もしくは、サーバ証明書を受け取り、当該証明書利用者に確実に受け渡す。

２．１．５　証明書利用者の義務

本サービスの利用にあたり、ユーザ証明書利用者は利用企業から通知される遵守すべき基本規則（以下「証明書利用者規約」という）に、サーバ証明書利用者は本 CPS に従わなければならない。

- ユーザ証明書利用者は、自身の秘密鍵が危殆化したか、あるいはそのおそれがある場合に、利用企業の担当者に対し速やかに通知しなければならない。
- ユーザ証明書利用者は、セキュリティデバイスもしくはユーザ証明書一式および利用者 PIN を安全に保護しなければならない。
- 証明書利用者は、本 CPS 1.3.7 に規定した用途以外に証明書を利用してはならない。

２．１．６　依拠当事者の義務

依拠当事者は、本サービスのユーザ証明書に依拠する際は、別途定められた遵守すべき基本規則（以下「依拠当事者規約」という）に、サーバ証明書に依拠する際は、本 CPS に従わなければならない。

- 依拠当事者は、依拠しようとする証明書が本認証局から発行され、改ざんされて

いないことを確認しなければならない。
- 依拠当事者は、依拠しようとする証明書が有効期間内であるかどうかを確認しなければならない。
- 依拠当事者は、リポジトリで公開されている CRL を確認し、依拠しようとする証明書が失効されていないことを確認しなければならない。
- 依拠当事者は、依拠しようとする証明書を発行した認証局証明書およびルート認証局証明書が、ルート認証局から発行され、改ざんされていないことを確認しなければならない。
- 依拠当事者は、依拠しようとする証明書を発行した認証局証明書およびルート認証局証明書が、有効期間内であるかどうかを確認しなければならない。
- 依拠当事者は、依拠しようとする証明書が、自己の利用の目的に対して適切であることを自己の判断で確認しなければならない。

２．１．７　リポジトリの義務

リポジトリは、本サービスの提供において、以下の義務を負う。
- リポジトリは、本認証局が発行した証明書に関する CRL を公開する。
- リポジトリは、本 CPS を公開する。
- リポジトリは、上記以外に本 CPS 2.6.1 に挙げられた情報を公開する。
- リポジトリは、1 日 24 時間、年間を通じて運用する。

２．２　責任

２．２．１　認証局の責任

本認証局は、本サービスの提供において、以下の事項を保証する。
- 本認証局が、本 CPS に基づきサービスを提供していること。
- 本認証局が、本 CPS および関連文書を適切に管理していること。

本認証局は、上記で明示している保証以外の一切の保証を行わない。また、以下の損害が発生した場合、本認証局は免責とする。
- 地震、水害、噴火等のあらゆる天災に起因する損害
- 火災、停電等のあらゆる災害に起因する損害
- 戦争、動乱およびその他のあらゆる不可抗力に起因する損害
- 本認証局が、システム障害等やむを得ない事情が発生したことにより、緊急にサービスを停止したことに起因する損害
- 本認証局が、本サービスの一部または全部の終了に起因する損害
- 本認証局が、証明書の失効処理を遅延なく行ったにも関わらず、当該証明書の失効情報が掲載された CRL の公開前に証明書が依拠当事者に送付された結果に起

因する損害
- 利用企業、証明書利用者および依拠当事者が、本 CPS に定められた義務および責任を果たさなかったことに起因する損害
- 証明書利用者および依拠当事者におけるソフトウェア、ハードウェアの誤作動および責任を果たさなかったことに起因する損害
- 本サービスにおいて使用する暗号、署名およびその他セキュリティ手段が、将来において解読や危殆化した結果に起因する損害
- 郵便事故等、配送時に起因する損害

２．２．２　利用企業の責任

利用企業は、本 CPS もしくは利用法人規約で示される義務を遵守しなかった結果によって発生する本認証局、証明書利用者および依拠当事者の損害に対し責任を負うものとする。また、利用企業は、当該利用企業の証明書利用者が、本 CPS もしくは証明書利用者規約に示されている義務を遵守しなかった結果発生する本認証局および依拠当事者の損害に対し連帯して責任を負うものとする。

２．２．３　証明書利用者の責任

証明書利用者は、本 CPS もしくは証明書利用者規約で示される義務を遵守しなかった結果によって発生する本認証局、利用企業および依拠当事者の損害に対し責任を負うものとする。

２．２．４　依拠当事者の責任

依拠当事者は、依拠当事者規約が示す義務を遵守しなかった結果によって発生する本認証局、利用企業および証明書利用者の損害に対し責任を負うものとする。

２．３　財務上の責任

本認証局は、間接損害、特別損害、付随的損害および結果的損害に関しては何ら責任を負わない。また、本認証局が本 CPS にて定める責任事項を全うせず、当該利用企業に対して損害賠償責任を負う場合は、別途その額の上限を定めるものとする。

２．４　解釈、および、執行

２．４．１　準拠法

本 CPS の執行、解釈および有効性は、当事者間の契約や他の準拠法を選択する旨の規定の有無に拘らず、また、日本国に営業上の関連性を有するか否かを問わず、日本国内法および規則に準拠し、同法の適用を受けるものとする。

この準拠法の選択は､証明書利用者と利用企業の住所または証明書の使用場所を問わず、

全関係者において統一的な手続および解釈を確保するためのものであり、証明書利用者の使用するソフトウェア、ハードウェアおよび技術情報の輸出入を制限するものではない。

２．４．２　分割、相続、合併、および通知

本 CPS の規定が、いかなる程度でも無効または執行不可能であるとされた場合であっても、本 CPS の規定の有効性には影響を及ぼさず、本認証局が本来意図する内容に最も合理的に合致するよう解釈されるものとする。

本認証局が廃止され、または本サービスが終了した場合においても、本 CPS 2.8 の効力は存続するものとする。

本サービスの権利義務に直接影響する本 CPS の規定は、本 CPS に別段の定めをしている場合を除き、その変更があった場合、リポジトリで公表する。したがって、口頭で修正、放棄、追加、変更、削除または終了させることはできないものとする。

利用企業や依拠当事者が、本 CPS に対して何らかの通知、請求、依頼をする場合の連絡は、本 CPS で定められた通知先に対し行われるものとする。証明書利用者が、本 CPS に関して本認証局に連絡を行う場合は、利用企業を通じて行うものとする。また、本認証局が利用企業、証明書利用者および依拠当事者に重要な通知を行う場合には、リポジトリ等の手段をもって行うものとする。

２．４．３　紛争解決の手続き

本 CPS および関連文書、あるいは、本認証局が発行した証明書に関して生じた紛争についての専属的合意管轄裁判所は、大阪地方裁判所とする。本 CPS および関連文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て疑義が生じた場合、各当事者は、その課題を解決するために訴訟に先立ち誠意をもって協議するものとする。

２．５　料金

本サービスに関する料金は、別途定めるものとする。

２．６　公表およびリポジトリ

２．６．１　認証局に関する情報の公表

本サービスは、リポジトリにおいて本認証局に関する以下の情報を公開する。

- 本 CPS：
  http://pki3.kanden.ne.jp/repository/KSSOLcps.pdf
- 利用法人規約：
  http://pki3.kanden.ne.jp/repository/KSSOLCorporateAgreement.pdf
- 証明書利用者規約：
  http://pki3.kanden.ne.jp/repository/KSSOLSubscriberAgreement.pdf

- 依拠当事者規約：
  http://pki3.kanden.ne.jp/repository/KSSOLRelyingPartyAgreement.pdf
- KS Solutions ルート認証局証明書のハッシュ値（フィンガープリント）：
  http://pki3.kanden.ne.jp/repository/KSSOLFingerPrint.pdf
- KS Solutions ルート認証局証明書：
  http://pki3.kanden.ne.jp/repository/KSSOLrootCA02.cer
- KS Solutions ユーザ証明書認証局証明書：
  http://pki3.kanden.ne.jp/repository/KSSOLsubCA0201.cer
- KS Solutions サーバ証明書認証局証明書：
  http://pki3.kanden.ne.jp/repository/KSSOLsubCA0202.cer
- CRL（ユーザ証明書）：
  http://pki3.kanden.ne.jp/crl/KSSOLsubCA0201/Latestcrl.crl
- CRL（サーバ証明書）：
  http://pki3.kanden.ne.jp/crl/KSSOLsubCA0202/Latestcrl.crl
- 認証局に関する通知：
  http://pki3.kanden.ne.jp/

２．６．２　公表の頻度

本サービスは、リポジトリにおいて公開する情報を以下の頻度で更新する。

- 本 CPS：改版の都度
- 利用法人規約：改版の都度
- 証明書利用者規約：改版の都度
- 依拠当事者規約：改版の都度
- KS Solutions ルート認証局証明書：発行の都度
- KS Solutions ユーザ証明書認証局証明書：発行の都度
- KS Solutions サーバ証明書認証局証明書：発行の都度
- KS Solutions ルート認証局証明書のハッシュ値（フィンガープリント）：
  KS Solutions ルート認証局証明書の発行の都度
- CRL：発行の都度（24 時間毎に更新される）
- 認証局に関する通知：適時

２．６．３　アクセス制御

リポジトリで公開する情報の閲覧に関しては、アクセスを制限しない。リポジトリで公開する情報に関して修正を行うことができるのは、本認証局において適切な権限を持った者のみとする。

２．６．４　リポジトリ

本サービスでは、リポジトリは 1 日 24 時間、年間を通じて運用される。システムは二重化されており、定期点検時においても原則として停止しない。ただし、システム障害等やむを得ない事情が発生した場合は、事前の通知なしに停止することがある。

２．７　準拠性監査

本認証局は、本認証局が本 CPS に従い適正に業務を行っていることを検証するため、監査基準を定め、定期的に監査を実施する。本認証局は、監査報告に基づいて必要と認められた場合は、業務の改善を行う。

本認証局が､業務の一部を外部に委託する場合､当該業務部分に関する監査については、本 CPS に定められた内容を参考に当該委託先と協議の上、実施することとする。

２．７．１　準拠性監査の頻度

本認証局は、年に 1 度以上の定期監査を行う。

２．７．２　監査人の識別／認定

本認証局は、準拠性監査における十分な知識を持った者を監査人として任命する。

２．７．３　監査人と被監査人との関係

本認証局の監査人は、本サービスの業務と直接関連のない者とする。

２．７．４　準拠性監査のトピック

準拠性監査において実施される監査項目には、以下のものが含まれる。

- 本認証局が運営する業務
- 本認証局が運営するシステム（ハードウェアおよびソフトウェア）およびネットワーク
- 本認証局が運営する設備

２．７．５　監査指摘項目への対応

本認証局は、監査結果での指摘事項に基づき、新技術の動向を考慮して業務および設備の改善を行う。必要である場合は本 CPS を改訂する。

２．７．６　監査結果

本認証局は、監査結果を外部に開示しない。ただし、本認証局の認証局責任者が必要と判断した場合に限り、監査結果を外部に公開することがある。

２．８　機密保持

２．８．１　機密扱いとする情報

本認証局が保有し、機密扱いとする情報は以下のとおりである。

- 証明書の発行および失効の申請に関わる記録（ただし、本 CPS 2.8.2 および 2.8.3 で機密扱いとしないと規定した情報を除く）
- 認証局秘密鍵の作成および管理に関する記録
- 認証局の構築、運用に関する記録およびトランザクションの記録
- 認証局の運用に関する内部規定およびマニュアル
- 監査の結果

２．８．２　機密扱いとしない情報

本認証局が保有し、機密扱いとしない情報は以下のとおりである。

- 証明書に記載される情報
- 失効情報（CRL）に記載される情報
- リポジトリで公開される情報

２．８．３　証明書失効情報の公表

本認証局は、証明書の失効情報に関して以下の情報を機密扱いとしない。

- 失効された証明書のシリアル番号
- 失効された証明書の失効日時

なお、本認証局は、証明書の有効期間が満了した後、当該証明書の失効情報を CRL に記載しない。

２．８．４　法執行機関への情報公開

本認証局は、法的根拠に基づいた情報の開示請求があった際には、法執行機関へ情報（機密情報を含む）の開示を行う場合がある。

２．８．５　民事手続き上の情報公開

本認証局は、民事手続き（調停（仲裁）、起訴、法的手続き、裁判上手続き、行政手続き等）上の要請に基づき情報の開示請求があった際には、情報（機密情報を含む）の開示を行う場合がある。

２．８．６　ユーザの要求に基づく公開

本認証局は、利用企業から当該利用企業に関する証明書にかかわる情報の開示請求があった際には、当該情報の開示を実施する場合がある。また、証明書利用者は、利用企業を

通じて本人の個人情報に関する開示の請求を行うことができる。

２．８．７　その他の公開条件

本認証局は、本サービスの一部を外部に委託する場合、当該業務を実施するために必要な情報を外部委託先に開示する場合がある。情報の開示を実施する場合には、適切な外部委託契約の締結等を実施し、本 CPS 2.8.1 に規定された機密情報を保護する。

本認証局では、取り扱う個人情報については、本認証局が別途定めた個人情報保護の規定に従って適切に管理する。

２．９　知的財産権

以下の情報資料およびデータに関する著作権その他の知的財産権は、本認証局に帰属する。

- 本 CPS
- 本認証局により作成された失効情報（CRL）
- 利用法人規約
- 証明書利用者規約
- 依拠当事者規約
- 本認証局から発行された認証局証明書
- 本認証局から発行された証明書（ただし、証明書利用者の公開鍵情報を除く）
- 本認証局の秘密鍵と公開鍵
- 本認証局に関する通知
- その他リポジトリで公開する情報

本サービスでは、リポジトリで公開される情報の複製を許可する。本認証局が意図していない利用目的のために、無断で転載および再利用等を行うことを禁止する。

３．識別と認証

３．１　初期登録

３．１．１　名称のタイプ

本認証局が発行する証明書の発行者名（issuer）フィールドおよび主体者名（subject）フィールドに含まれる識別名が準拠する規格は、ITU-T Recommendation X.500 形式の識別名（DN：Distinguished Name）である。

KS Solutions ルート認証局、KS Solutions ユーザ証明書認証局、KS Solutions サーバ証明書認証局および証明書利用者についての識別名は、以下のように設定する。

表 2　KS Solutions ルート認証局の発行者名（issuer）フィールド
および主体者名（subject）フィールド

属性名		属性値	備考
発行者名（issuer）			
	国名 （countryName）	c=jp	
	組織名 （organizationName）	o=KandenSystemSolutionsCoInc	
	共通名 （commonName）	cn=KSSOLrootCA02	
主体者名（subject）			
	国名 （countryName）	c=jp	
	組織名 （organizationName）	o= KandenSystemSolutionsCoInc	
	共通名 （commonName）	cn=KSSOLrootCA02	

表 3　KS Solutions ユーザ証明書認証局の発行者名（issuer）フィールド
および主体者名（subject）フィールド

属性名		属性値	備考
発行者名（issuer）			
	国名 （countryName）	c=jp	
	組織名 （organizationName）	o= KandenSystemSolutionsCoInc	
	共通名 （commonName）	cn=KSSOLrootCA02	
主体者名（subject）			
	国名 （countryName）	c=jp	
	組織名 （organizationName）	o= KandenSystemSolutionsCoInc	
	組織単位名 （organizatinalUnitName）	ou=KSSOLsubCA0201	

表 4　ユーザ証明書の発行者名（issuer）フィールド
および主体者名（subject）フィールド

属性名		属性値	備考
発行者名（issuer）			
	国名 （countryName）	c=jp	
	組織名 （organizationName）	o= KandenSystemSolutionsCoInc	
	組織単位名 （organizatinalUnitName）	ou=KSSOLsubCA0201	
主体者名（subject）			
	国名 （countryName）	c=jp	
	組織名 （organizationName）	o=*（利用企業名）*	可変値。値の意味は本 CPS 3.1.2 を参照。
	組織単位名 （organizatinalUnitName）	ou=*（発行回数）*	可変値。値の意味は本 CPS 3.1.2 を参照。
	共通名 （commonName）	cn=*（識別子）*	可変値。値の意味は本 CPS 3.1.2 を参照。

表 5　KS Solutions サーバ証明書認証局の発行者名（issuer）フィールド
および主体者名（subject）フィールド

属性名		属性値	備考
発行者名（issuer）			
	国名 （countryName）	c=jp	
	組織名 （organizationName）	o= KandenSystemSolutionsCoInc	
	共通名 （commonName）	cn=KSSOLrootCA02	
主体者名（subject）			
	国名 （countryName）	c=jp	
	組織名 （organizationName）	o= KandenSystemSolutionsCoInc	
	組織単位名 （organizatinalUnitName）	ou=KSSOLsubCA0202	

表 6　サーバ証明書の発行者名（issuer）フィールド
および主体者名（subject）フィールド

属性名		属性値	備考
発行者名（issuer）			
	国名 （countryName）	c=jp	
	組織名 （organizationName）	o= KandenSystemSolutionsCoInc	
	組織単位名 （organizatinalUnitName）	ou=KSSOLsubCA0202	
主体者名（subject）			
	国名 （countryName）	c=jp	
	州・県名 （stateOrProvinceName）	s=*（都道府県名）*	任意項目。値の意味は本 CPS 3.1.2 を参照。
	所在地名 （localityName）	l=*（市区町村名）*	任意項目。値の意味は本 CPS 3.1.2 を参照。
	組織名 （organizationName）	o=*（利用企業名）*	可変値。値の意味は本 CPS 3.1.2 を参照。
	組織単位名 （organizatinalUnitName）	ou=*（発行回数）*	可変値。値の意味は本 CPS 3.1.2 を参照。
	共通名 （commonName）	cn=*（ドメイン名）*	可変値。値の意味は本 CPS 3.1.2 を参照。

３．１．２　名称の意味

本認証局が発行するユーザ証明書では、その主体者名に関して以下のような意味を持つ。

- 組織名：
  利用企業の正式な英文名称に対して、「 」（スペース）「.」（ピリオド）「,」（カンマ）「-」（ハイフン）を取り除いた値とする。
- 組織単位名：
  組織名と共通名で識別可能な特定の証明書利用者への証明書を発行した回数とする。回数は、発行、更新および再発行によりカウントアップされる。
- 共通名：
  利用企業内で、証明書利用者を一意に識別することが可能な識別子（ユーザ ID 等）とする。

また、本認証局が発行するサーバ証明書では、その主体者名に関して以下のような意味を持つ。

- 組織名：
  利用企業の正式な英文名称に対して、「 」（スペース）「.」（ピリオド）「,」（カンマ）「-」（ハイフン）を取り除いた値とする。
- 組織単位名：
  組織名と共通名で識別可能な特定の証明書利用者への証明書を発行した回数とする。回数は、発行、更新および再発行によりカウントアップされる。
- 所在地名：
  利用企業の市区町村名とする。（任意項目）
- 州・県名：
  利用企業の都道府県名とする。（任意項目）
- 共通名：
  利用企業内で、証明書利用者を一意に識別することが可能な識別子（ドメイン名等）とする。

３．１．３　名称を解釈するためのルール

規定しない。

３．１．４　名称のユニーク性

本認証局が発行する証明書では、証明書の主体者名フィールドの組織名および共通名の組み合わせにより、証明書利用者を一意に特定できる。

３．１．５　名称に関する紛争解決手段

本認証局が本 CPS3.1.2 の名称変換の実施有無に関わらず、名称を変更して作成した識別名によって紛争が発生した場合、本認証局は一切の関与をせず、当該利用企業と識別名に対して異議を主張する第三者との間で紛争解決を図るものとする。また協議の結果、紛争が解決するに至らなかった場合、本認証局は証明書の失効、保留等を行う権利を有する。

３．１．６　商標の認定、認証、役割

本認証局は、証明書に記載する識別名が商標を含むかどうかの確認を行わないため、当該識別名は商標を含む場合がある。証明書に記載された識別名が、商標を含むことにより、損害を被る者が発生した場合は、本認証局は一切の責任を負わず、当該利用企業が自己の負担と責任の下で解決するものとする。

３．１．７　秘密鍵の所有を証明する方法

本認証局は、認証局側においてユーザ証明書利用者の秘密鍵、公開鍵の鍵ペアを生成し、サーバ証明書利用者の秘密鍵、公開鍵については、サーバ証明書利用者側において鍵ペアを生成する。

３．１．８　組織の認証

組織の認証について以下のとおり処理を行う。

ユーザ証明書の場合

本サービスの利用にあたり、利用企業は本認証局と利用法人規約をもって契約の締結を行わなければならない。利用企業は、当該利用企業内の特定の担当者とその連絡先電話番号を、本認証局が別途定める方法で登録しなければならない。登録局では、登録された担当者からの申請のみを受け付ける。

利用企業がユーザ証明書の申請を行う場合、登録局は、利用企業の担当者を以下の方法で確認することによって、申請が当該利用企業からのものであることを認証する。

(1)　利用企業の担当者は、以下の情報を含む発行申請書を登録局に送付する。
- 発行依頼年月日
- 利用企業名
- 担当者所属部署名
- 担当者名
- 印鑑証明書によって照合可能な印（以下、「公印」という）による押印

(2)　登録局は、利用企業名を上記(１)の申請情報を確認する。

(3)　登録局は、事前に登録された連絡先電話番号へのコールバックを実施し、当該申

請が行われたことについて事前に登録された利用企業担当者に確認する。

サーバ証明書の場合

利用企業がサーバ証明書の申請を行う場合、登録局は、以下の方法で確認することによって、申請が当該利用企業からのものであることを認証する。

(1) 利用企業は、以下の情報を含む発行申請書を登録局に送付する。
- 発行依頼年月日
- 利用企業名
- 担当者所属部署名
- 担当者名
- 印鑑証明書によって照合可能な印（以下、「公印」という）による押印

(2) 登録局は、利用企業名を上記(1)の申請情報を確認する。

(3) 登録局は、コールバックを実施し、当該申請が行われたことについて確認する。

３．１．９ 個人の認証

利用企業は、登録局に対して証明書の申請を行うにあたり、本 CPS、もしくは利用法人規約に基づいて当該証明書利用者を認証しなければならない。登録局では、証明書利用者の個人の認証を行わない。

利用企業が証明書の申請を行う場合、以下の方法で証明書利用者の情報を登録局に受け渡す。

ユーザ証明書の場合

(1) 利用企業の担当者は、以下の情報を含む発行申請書を登録局に送付する。なお、ユーザ ID、ユーザ証明書の有効期限については必須とする。
- ユーザ ID
- ユーザプリンシパル名（UPName）
- 電子メールアドレス（rfc822Name）
- ユーザ証明書の有効期限

(2) 登録局は、本 CPS 3.1.8 に従って利用企業の認証を行う。

(3) 登録局は、発行申請書の情報を用いてユーザ証明書を発行する。

なお、本認証局が承認した利用企業の場合、本認証局より指定した方法でユーザ証明書利用者の情報の受け渡しを行うことができる。

サーバ証明書の場合

(1) 利用企業は、以下の情報を含む発行申請書および、CSR（Certificate Signing

Request）を登録局に送付する。

（2） 登録局は本 CPS3.1.8 に従って利用企業の認証を行う。

（3） 登録局は、発行申請書の情報を用いてサーバ証明書を発行する。

３．２ 証明書の更新

証明書の更新要求は、利用企業が登録局に対して行う。利用企業は、証明書の更新の要求を行うにあたり、当該証明書利用者を本 CPS 3.1.9 に従って認証しなければならない。更新されたユーザ証明書について利用企業は、当該証明書利用者に確実に配布しなければならない。ユーザ証明書利用者が更新の対象となる古いセキュリティデバイスを保有している場合、利用企業は自身の判断によりセキュリティデバイスの回収および破棄を行う。

また、サーバ証明書についても、利用企業は当該証明書利用者に確実に配布しなければならない。

本認証局の認証局証明書の更新については、本 CPS では規定しない。

３．３ 再発行

以下の事由で証明書を失効する場合において、利用企業は、証明書の再発行の要求を行うことができる。

- セキュリティデバイスの盗難
- セキュリティデバイスの紛失
- セキュリティデバイスの破損
- セキュリティデバイス（ＩＣカード）の券面情報の変更
- 証明書利用者の秘密鍵の危殆化およびその恐れがある場合
- ユーザ証明書がインストールされた端末を紛失もしくは破損にて利用できなくなった場合
- その他、利用企業が必要と判断した場合

利用企業は登録局に対して再発行申請書を提出して申請することにより、証明書の再発行要求を行う。利用企業は、再発行の申請を行うにあたり、当該証明書利用者を本 CPS 3.1.9 に従って認証しなければならない。更新後のユーザ証明書は、新たに作成される。

３．４ 失効要求

利用企業は、登録局に対して、本認証局が発行した証明書の失効の要求を行うことができる。利用企業が、失効の要求を行うのは、以下の場合である。

- 退職、退任あるいは契約の解除等の理由により、ユーザ証明書利用者が利用企業の構成員ではなくなった場合
- セキュリティデバイスの盗難

- セキュリティデバイスの紛失
- セキュリティデバイスの破損
- セキュリティデバイス（ＩＣカード）の券面情報の変更
- 証明書利用者の秘密鍵の危殆化およびその恐れがある場合
- サーバ証明書が不要となった場合
- ユーザ証明書がインストールされた端末を盗難、紛失もしくは破損にて利用できなくなった場合
- その他、利用企業が必要と判断した場合

利用企業は登録局に対して失効申請書を提出して申請することにより、証明書の失効要求を行う。利用企業は、失効の申請を行うにあたり、当該証明書利用者を本 CPS 3.1.9 に従って認証しなければならない。

４．運用要件

４．１　証明書申請

利用企業は、証明書の発行申請を行うにあたり、以下のとおり処理を行う。

ユーザ証明書の場合

利用企業は、ユーザ証明書の発行申請を行うにあたり、予め担当者を登録局側で識別できるように事前に手続きを行っておく必要がある。登録局では、事前に登録された担当者以外からのユーザ証明書の発行申請を受け付けない。

ユーザ証明書の発行申請の手続きは、以下のとおりとする。

（1）　利用企業の担当者は、発行申請書を登録局に送付する。
（2）　登録局は、本 CPS 3.1.8 および 3.1.9 に従い、申請内容の審査を行う。
（3）　(2)で問題なく審査が完了した場合、登録局は本 CPS 4.2 に従い、ユーザ証明書の発行の手続きを行う。

サーバ証明書の場合

サーバ証明書発行申請手続きは、以下のとおりとする。

（1）　利用企業は、発行申請書および、CSR を登録局に送付する。
（2）　登録局は、本 CPS 3.1.8 および 3.1.9 に従い、申請内容の審査を行う。
（3）　(2)で問題なく審査が完了した場合、登録局は本 CPS 4.2 に従い、サーバ証明書の発行の手続きを行う。

本認証局が承認した利用企業は､本認証局と利用企業との間で別途合意した方法により、登録局に対して発行申請の情報を受け渡すことができる。

４．２　証明書発行

本認証局において、証明書の発行手続きは、以下のとおりとする。

ユーザ証明書の場合

（1）　本 CPS 4.1 の手続きを実施した登録局は、証明書利用者の鍵ペアを生成する。
（2）　登録局は、発行局に対してユーザ証明書の発行指示を行う。
（3）　発行局は、当該発行指示が登録局からのものであることを確認する。
（4）　発行局は、当該発行指示が正しく確認できた場合、ユーザ証明書を生成する。
（5）　発行局は、登録局に対してユーザ証明書を返送する。
（6）　登録局は、当該ユーザ証明書が発行局からのものであることを確認する。
（7）　登録局は、発行局から発行されたユーザ証明書を受領する。

（8） 登録局は、証明書利用者の秘密鍵とユーザ証明書を PKCS#12 形式で暗号化する。また、PKCS#12 形式のデータを復号化する際に必要となる PIN（PKCS#12 の PIN）は、専用ソフトウェアを用いて安全に生成する。
（9） 登録局は、PKCS#12 形式のデータを用い、ユーザ証明書一式を作成する。
（10） 登録局は、ユーザ証明書一式を本 CPS 4.3 に従って利用企業に送付する。
（11） 登録局は、PKCS#12 形式のデータを、本 CPS 6.2.4 に従って保管する。

本認証局は、ユーザ証明書利用者の秘密鍵とユーザ証明書のセキュリティデバイスへの格納を外部業者に委託することがある。

サーバ証明書の場合
（1） 本 CPS 4.1 の手続きを実施した登録局は、発行局に対してサーバ証明書の発行指示を行う。
（2） 発行局は、当該発行指示が登録局からのものであることを確認する。
（3） 発行局は、当該発行指示が正しく確認できた場合、サーバ証明書を生成する。
（4） 発行局は、登録局に対してサーバ証明書を返送する。
（5） 登録局は、当該ユーザ証明書が発行局からのものであることを確認する。
（6） 登録局は、発行局から発行されたサーバ証明書を受領する。
（7） 登録局は、サーバ証明書を本 CPS 4.3 に従って利用企業に送付する。

４．３ 証明書の配布

本認証局において、発行された証明書の受領手続きは、以下のとおりとする。

ユーザ証明書の場合
(1) セキュリティデバイスがＩＣカードの場合
① ユーザ証明書の発行を完了した登録局は、納品書とともに、セキュリティデバイスを利用企業に送付する。
② 利用企業は、当該セキュリティデバイスの受領および確認を行う。
③ 利用企業は、当該セキュリティデバイスを正当なユーザ証明書利用者に対して確実に配布する。
④ 本認証局は、セキュリティデバイス送付後、所定の手順により受領登録されていることを確認し、ユーザがセキュリティデバイスを受領したとみなす。
⑤ 以下の事由に該当する場合、利用企業は自己の判断において、ユーザ証明書利用者から旧セキュリティデバイスの回収および破棄を行う。但し、盗難･紛失等の理由により、ユーザ証明書利用者が旧セキュリティデバイスを所有していない場合を除く。

・本 CPS3.2 の内容に基づき、本認証局がユーザ証明書の更新処理を実施し、ユーザ証明書利用者が保有している旧セキュリティデバイスの効力が失われた場合。
・本 CPS3.3 の内容に基づき、本認証局がユーザ証明書の再発行処理を実施し、ユーザ証明書利用者が保有している旧セキュリティデバイスの効力が失われた場合。
・本 CPS3.4 の内容に基づき、本認証局がユーザ証明書の失効処理を実施し、ユーザ証明書利用者が保有している旧セキュリティデバイスの効力が失われた場合。

本認証局からセキュリティデバイスを送付後、一定期間を経ても所定の手順により受領登録されていることが本認証局で確認できない場合、送付先の利用企業担当者へ確認の上、当該ユーザ証明書を失効させる場合がある。

(2) セキュリティデバイスが USB トークンの場合

① ユーザ証明書の発行を完了した登録局は、納品書および受領書とともに、セキュリティデバイスを利用企業に送付する。
② 利用企業は、当該セキュリティデバイスの受領および確認を行う。
③ 利用企業は、当該セキュリティデバイスを正当なユーザ証明書利用者に対して確実に配布する。
④ 利用企業は、当該セキュリティデバイスに問題無ければ、受領書に捺印して本認証局へ返送する。
⑤ 以下の事由に該当する場合、利用企業は自己の判断において、ユーザ証明書利用者から旧セキュリティデバイスの回収および破棄を行う。但し、盗難･紛失等の理由により、ユーザ証明書利用者が旧セキュリティデバイスを所有していない場合を除く。
・本 CPS3.2 の内容に基づき、本認証局がユーザ証明書の更新処理を実施し、ユーザ証明書利用者が保有している旧セキュリティデバイスの効力が失われた場合。
・本 CPS3.3 の内容に基づき、本認証局がユーザ証明書の再発行処理を実施し、ユーザ証明書利用者が保有している旧セキュリティデバイスの効力が失われた場合。
・本 CPS3.4 の内容に基づき、本認証局がユーザ証明書の失効処理を実施し、ユーザ証明書利用者が保有している旧セキュリティデバイスの効力が失われた場合。

本認証局からセキュリティデバイスを送付後、一定期間を経ても受領書が返送されていることが本認証局で確認できない場合、送付先の利用企業担当者へ確認の上、当該ユーザ証明書を失効させる場合がある。

(3)セキュリティデバイスに格納できない場合

① ユーザ証明書の発行を完了した登録局は、納品書および受領書とともに、ユーザ証明書一式を利用企業に送付する。
② 利用企業は、当該ユーザ証明書一式の受領および確認を行う。
③ 利用企業は、当該ユーザ証明書一式を正当なユーザ証明書利用者に対して確実に配布する。
④ 利用企業は、当該ユーザ証明書一式に問題無ければ、受領書に捺印して本認証局へ返送する。

本認証局からユーザ証明書一式を送付後、一定期間を経ても受領書が返送されていることが本認証局で確認できない場合、送付先の利用企業担当者へ確認の上、当該ユーザ証明書を失効させる場合がある。

サーバ証明書の場合

(1) サーバ証明書の発行を完了した登録局は、サーバ証明書を利用企業に送付する。
(2) 利用企業は、サーバ証明書の受領および確認を行う。
(3) 利用企業は、当該サーバ証明書を該当サーバ等に対して配布する。

４．４　証明書失効および一時停止

４．４．１　失効条件

利用企業は、以下の事由がある場合、証明書の失効を申請しなければならない。

- 証明書利用者のユーザ証明書の秘密鍵が危殆化した場合、もしくは危殆化のおそれがある場合
- 証明書利用者がセキュリティデバイスを紛失した場合、または盗難された場合
- 破損等によって証明書利用者のセキュリティデバイスが使用できなくなった場合
- 証明書利用者のセキュリティデバイスおよび、証明書の記載事項が事実と異なることを発見した場合
- 証明書利用者のセキュリティデバイスおよび、証明書の記載事項に変更が生じた場合
- 証明書の利用を中止する場合
- 証明書利用者である社員の退職、役員の退任、あるいは、外部委託者の利用企業との間の契約の解除が発生した場合

- 証明書利用者が、本 CPS もしくは、証明書利用者規約に違反した場合
- 証明書がインストールされた端末を盗難、紛失もしくは破損にて利用できなくなった場合
- 利用企業が、上記以外の事由により証明書を失効する必要があると合理的に判断した場合

本認証局は、以下の事由がある場合、証明書を失効することができる。

- 本認証局が、利用企業より一定期間を経ても受領書が返送されていないこと、所定の手順により受領登録されていることが確認できなかった場合
- ユーザ証明書利用者のセキュリティデバイスおよびユーザ証明書一式、もしくは証明書の記載事項が事実と異なることを発見した場合
- 利用企業と本認証局との契約が解除された場合
- 利用企業が解散した場合
- ユーザ証明書利用者のセキュリティデバイス発送前に、初期不良が発生した場合
- 本認証局の秘密鍵が危殆化した場合、もしくは危殆化のおそれがある場合
- 本認証局が認証業務を廃止する場合
- 本認証局が、上記以外の事由により証明書を失効する必要があると合理的に判断した場合

４．４．２　失効要求者

本認証局では、本 CPS 4.4.1 の事由において、以下の者が証明書の失効を要求することができる。

- 利用企業
- 本認証局

４．４．３　失効手続き

本認証局における失効手続きは以下のとおり処理する。

ユーザ証明書の場合

本認証局に対するユーザ証明書の失効申請を行うにあたり、利用企業は、予め担当者を登録局側で識別できるように事前に手続きを行っておく必要がある。登録局では、事前に登録された担当者以外からのユーザ証明書の失効申請を受け付けない。

ユーザ証明書の失効申請の手続きは、以下のとおりとする。

（1）　ユーザ証明書の失効を申請する場合、利用企業の担当者は、本 CPS 3.4 に従って登録局にユーザ証明書の失効を申請する。

(2) ユーザ証明書の再発行を伴う失効を申請する場合、利用企業の担当者は、本 CPS 3.3 に従って登録局にユーザ証明書の失効を申請する。
(3) 利用企業は自己の判断において、ユーザ証明書利用者から失効の対象となったユーザ証明書を格納したセキュリティデバイスの回収および破棄を行う。

本認証局が承認した利用企業は、本認証局と利用企業との間で別途合意した方法により、登録局に対して失効申請の情報を受け渡すことができる。

サーバ証明書の場合
サーバ証明書の失効申請の手続きは、以下のとおりとする。

(1) サーバ証明書の失効を申請する場合、本 CPS 3.4 に従って登録局にサーバ証明書の失効を申請する。
(2) サーバ証明書の再発行を伴う失効を申請する場合、本 CPS 3.3 に従って登録局にサーバ証明書の失効を申請する。

４．４．４　失効要求の猶予期間

利用企業は、ユーザ証明書利用者に対して、ユーザ証明書が失効する事由がある場合に速やかに通知するよう義務付けなければならない。利用企業は、証明書利用者から通知があったか、証明書に関する失効の事由を発見した場合、速やかに登録局に対して失効の申請をしなければならない。本認証局では、登録局が利用企業からの失効申請の内容を確認できた時点から原則として 24 時間以内に失効の処理を完了する。

４．４．５　一時停止条件

本認証局では、証明書の一時停止を行わない。

４．４．６　一時停止要求者

規定しない。

４．４．７　一時停止手続き

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　失効情報の発行頻度

本認証局は、証明書に関する CRL を 24 時間毎に発行する。CRL に記載する次回更新日（nextUpdate）は、当該 CRL の発行日時（thisUpdate）から 72 時間後とする。ただし、システム保守による一時停止、緊急時等やむを得ない場合を除く。

４．４．１０　失効情報の確認要件

依拠当事者は、本認証局が発行する最新の CRL を用いて証明書の有効性を確認しなければならない。

最新の CRL は、本 CPS 2.6.1 に定められたリポジトリにおいて公開する。CRL に記載される情報は、本 CPS 2.8.3 に定める。

４．４．１１　オンラインステータスチェック

本認証局では、CRL を除き、オンラインでの証明書ステータス確認の方法を提供しない。

４．４．１２　オンライン失効チェック要件

規定しない。

４．４．１３　その他の利用可能な失効情報確認手段

本認証局では、CRL 以外の失効情報確認手段を提供しない。

４．４．１４　その他の利用可能な失効情報確認手段における要件

規定しない。

４．４．１５　危殆化時の特別対応

本認証局の秘密鍵が危殆化した場合は、本 CPS 4.8 に従うものとする。

４．５　セキュリティ監査の手順

本認証局では、設備やシステムが安全に運用されていることを確認し、維持するためにセキュリティ監査を行う。ただし外部に委託された業務に関する監査については、本 CPS に定められた内容を参考に当該委託先と協議の上、実施することとする。

４．５．１　記録される情報のタイプ

本認証局における監査ログには、以下の情報が含まれる。

- 証明書の作成および失効の記録
- 証明書の作成および失効に係る IA 認証業務用設備および RA 認証業務用設備の操作履歴

- IA 設備室および RA 設備室への入退室記録
- IA 認証業務用設備および RA 認証業務用設備への不正アクセスの記録
- IA 認証業務用設備および RA 認証業務用設備の動作に関する記録

登録局では、上記の監査ログに加えて、以下の記録を保存する。

- RA オペレーション室への入退室記録
- 作業用セキュリティデバイス管理記録

４．５．２　ログが処理、検査される頻度

セキュリティ監査は、本認証局の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する。

４．５．３　監査ログの保管期間

本認証局では、監査ログの保管期間を 6 年間とする。

４．５．４　監査ログの収集とバックアップ

監査ログは、IA 認証業務用設備および RA 認証業務用設備から自動で収集し、定期的保存する。

４．５．５　監査ログの保護

監査ログは、漏えい、改ざん、き損等が行われないように安全に保存、管理される。また作業で使用した電子データは、安全に保存し、書面で保存される帳簿書類については、施錠可能なキャビネット等に保管する。

４．５．６　監査結果の通知

監査ログにおいて、調査の必要性がある事象が検出された場合、本認証局は当該事象の発生者に対しての通知を義務としない。

４．５．７　脆弱性評価

規定しない。

４．６　記録のアーカイブ

本認証局では、記録の保管に関して以下のとおり規定する。

４．６．１　アーカイブデータの種類

本認証局で保管する記録には、以下の帳簿書類等を含むものとする。

(1) 発行処理、失効処理に関するデータおよび認証局でその管理上作成した書類等
- 認証局秘密鍵の作成および管理に関する記録
- 発行された全ての証明書の発行に関する情報およびその作成に関する記録
- 発行された全ての証明書の失効に関する情報およびその作成に関する記録

(2) 業務遂行上必要とされる組織管理関係書類等
- 業務手順を記述した書類とその変更に関する記録
- 業務に従事する者の組織、体制、責任および権限並びに指揮命令系統に関する管理書類
- 認証業務を外部に委託する場合の委託契約に関する書類
- 準拠性監査に関する記録と監査報告書

(3) 本サービス提供に係る設備およびその安全対策措置に関する記録等
- IA 設備室、RA 設備室および RA オペレーション室への入退室に関する記録
- IA 認証業務用設備および RA 認証業務用設備の保守およびシステム変更に関する記録
- IA 認証業務用設備および RA 認証業務用設備の障害および復旧に関する記録
- IA 認証業務用設備および RA 認証業務用設備の事故に関する記録
- IA 認証業務用設備および RA 認証業務用設備の動作に関する記録

４．６．２　アーカイブデータの保管期間
本認証局では、記録の保管期間を 6 年間とする。

４．６．３　アーカイブデータの保護
アーカイブデータは、漏えい、改ざん、き損等が行われないように安全に保存、管理される。電子データの場合、アーカイブデータを定期的に保存する。書面で保存される帳簿書類については、施錠可能なキャビネット等で保管する。

４．６．４　アーカイブデータのバックアップ手順
規定しない。

４．６．５　記録へのタイムスタンピング要件
規定しない。

４．６．６　アーカイブデータの収集システム
記録は、IA 認証業務用設備および RA 認証業務用設備による自動で収集する。

４．６．７　アーカイブデータの入手、検証手続き

規定しない。

４．７　鍵更新

規定しない。

４．８　危殆化と災害復旧

本認証局の秘密鍵が危殆化または危殆化の恐れがあることが判明した場合、あるいは災害による障害発生等の不測の事態が生じた場合には、本認証局は次のとおり対応する。

- 認証局秘密鍵の危殆化または危殆化の恐れがあることが判明した場合
  (1) 本認証局は、本サービスを停止する。
  (2) 本認証局は、利用企業と直ちに協議し、当該認証局秘密鍵を用いて発行した証明書の有効性を取消す処理について、必要な措置を講じる。
  (3) 本認証局は、原因および被害状況を調査し、対応策および再発防止策を講じる。
  (4) 本サービスを継続するために、利用企業と協議し、可及的すみやかに新たな当該認証局秘密鍵を生成する等、対応を講じる。

- 天災事変等の被災、認証業務用設備の故障等により運用を停止した場合
  (1) 本認証局は、災害等による障害発生の原因および被害状況を調査し，対応策および再発防止策を講じる。
  (2) 可能であれば、保管されているデータをバックアップから復元する。

４．９　認証業務の終了

本認証局が認証業務を終了しようとする場合、本認証局は終了計画を作成し、これを実施する。終了計画には、以下の内容を含む。

- 利用企業への連絡方法
- 発行済み証明書の有効性を終了する方法
- 認証業務終了後に失効情報を開示する方法
- 認証局秘密鍵の消去の方法

５．物理面、手続き面および人事面のセキュリティ統制

５．１　物理的統制

５．１．１　施設の位置と建物構造

発行局にて認証局の秘密鍵の管理、証明書発行・失効処理、失効リストの発行等に使用するシステムを IA 業務用設備と呼ぶ。IA 業務用設備が設置された部屋を、IA 設備室と呼ぶ。

IA 業務用設備を収容する建築構造物（建物および部屋）の立地場所は、地震、水害等の天災を受けにくい場所とする。建築構造物に関しては、耐震耐火設計、自動火災報知器と消火装置の設置、防火区画内への設置、隔壁による区画、水害防止等の措置が予め十分講じられている等、地震、火災、水害等想定される災害に耐えうる設備とする。また、停電に備えた UPS および自家発電機の設置、設備に応じた空調機器の設置等、サービスの継続に必要な適切な措置が講じられている。

登録局において、ユーザ証明書利用者の鍵ペアの生成および発行局に対する証明書の発行・失効指示等に使用されるサーバ機器と通信機器の総称を RA 業務用設備と呼ぶ。

RA 業務用設備が設置された区画を、RA 設備区画と呼ぶ。RA 設備区画に関しては、厳重な施錠管理を施しており、該当する権限を有しない者による物理的アクセスを制御するように、適切な措置を講じている。また、耐震耐火設計、消火装置の設置等により、地震や火災といった災害への対策を施すとともに、停電に備えた CVCF および自家発電機の設置、設備に応じた空調機器の設置等、サービスの継続に必要な適切な措置を講じている。

RA 業務用設備を遠隔操作するための端末およびセキュリティデバイスの発行機が設置された専用の部屋を RA オペレーション室と呼ぶ。RA オペレーション室では、ユーザ証明書利用者の秘密鍵およびユーザ証明書のセキュリティデバイスへの格納、（ＩＣカードの場合、券面印刷等の処理)、発行後のセキュリティデバイス発送準備作業を行う。RA オペレーション室に関しては、消火装置の設置等が予め十分講じられていて、火災等の災害に耐えうる設備とする。

利用企業から送付される申請書等を取り扱う部屋は、RA 業務室と呼ぶ。RA 業務室に関しては、消火装置等の設置が予め十分講じられていて、火災等の災害に耐えうる設備とする。

本認証局において、登録局におけるセキュリティデバイスの発行に関する一部の業務は、外部業者に委託する場合がある。

５．１．２　物理的アクセス

IA 設備室への入退室等については、次により厳重に管理される。

・ IA 設備室は厳重に施錠管理され、その入室は入室者の身体的特徴の識別手段を用い

た施錠設備による本人確認をしてはじめて可能となるよう予め防護措置が講じられる。

- IA 設備室へは、予めその資格について審査され指定登録されている 2 名の者をもって開錠し入室する。退出にあたっては入室者と同数の者の退出をもって退出を完了する。退出完了後、センサーが異常を検出した場合、ならびに入退室に不正常な時間を要した場合には、警報が発せられる。なお、入室権限を有しない者の入室は原則として認められないが、やむを得ずこれを認める場合には、予めＩＡセキュリティマネージャの許可を得、複数の入室権限者同行の上この者を入室させることができる。また、これらの行為はＩＡセキュリティマネージャにより点検される。
- IA 設備室への入退室者および在室者の状況については、遠隔監視装置、センサーおよび映像記録装置等によって自動的かつ継続的に監視記録され、その記録については、定期的に点検され、定められた期間、安全に保存される。
- IA 設備室の所在および仕様は、関係者以外には厳重に秘匿される。建物の内外には IA 設備室の所在については表示されない。

RA 設備区画への施錠、RA オペレーション室および RA 業務室への入退室等については、次により厳重に管理される。

- RA 設備区画、RA オペレーション室、RA 業務室およびこれらを収容する建築構造物は、厳重に入退館管理され、その入館は予め定められた手順に従って許可および本人確認を行った後、はじめて立入可能となるよう防護措置が講じられる。
- RA 設備区画は予めその資格について審査され指定登録されている２名以上の者をもって相互牽制を行い、開錠する。施錠にあたっても相互牽制を実施する。また、これらの行為は RA 責任者により点検される。
- RA オペレーション室へは、予めその資格について審査され指定登録されている２名以上の者をもって相互牽制を行い開錠し入室する。退出にあたっても相互牽制を行い入室者と同数の者の退出をもって完了とする。なお、入室権限を有しない者の入室は原則として認められないが、やむを得ずこれを認める場合には、予め RA 責任者の許可を得、複数の入室権限者同行の上この者を入室させることができる。また、これらの行為は RA 責任者により点検される。
- RA 設備区画の施錠、および RA オペレーション室への入退室の記録については、予め定められた手続きによって記録を行い、その記録については、定期的に点検され、定められた期間、安全に保存される。
- RA 業務室への入室については、予め定められた手順に従って許可および本人確認を行った後、はじめて立入可能となるよう防護措置が講じられる。
- RA 業務室への入室の記録については、電子的に記録を行い、その記録については、定期的に点検され、定められた期間、安全に保存される。

５．２　手続き統制

本認証局の業務の遂行に必要な各役割、その業務内容、各役割を担う者の設備へのアクセス権限は、表 5、表 6および表 7のとおりとする。

各役割に従事する者の任命、物理的な部屋ごとの入室権限の設定、認証業務設備へのシステムごとのアクセス権限の設定は予め定められた手続きに従い、特定の権限者がこれを行う。

表 5　認証局の各役割とその主な業務内容、設備へのアクセス権限

役割	主な業務	入室権限付与	設備へのアクセス権限
認証局責任者	認証局運営全体統括	×	×
発行局責任者	発行局運営統括	×	×
発行局業務責任者	発行局業務統括	○（生体認証）	×
発行ｼｽﾃﾑ管理責任者	発行認証業務設備の管理統括	○（生体認証）	
発行ｼｽﾃﾑ管理担当者	発行認証業務設備の管理	○（生体認証）	
発行ｼｽﾃﾑ運用責任者	発行認証業務設備の運用統括	○（生体認証）	
発行ｼｽﾃﾑ運用者	発行認証業務設備の運用	○（生体認証）	
発行ｼｽﾃﾑ運用監視担当者	発行認証業務設備のログ監査	×	
発行局ｾｷｭﾘﾃｨﾏﾈｼﾞｬｰ	発行認証業務用設備のｾｷｭﾘﾃｨ維持管理、認証設備室の鍵管理	発行局責任者が付与	
登録局責任者	登録局運営統括	×	×
登録局業務責任者	認証・登録業務統括	×	×
登録局認証業務担当者	認証業務の実施（申請受付・審査）	登録局ｾｷｭﾘﾃｨﾏﾈｼﾞｬｰが付与	
登録局登録業務担当者	登録業務の実施（発行局への指示）（ﾃﾞﾊﾞｲｽの発行・発送）	登録局ｾｷｭﾘﾃｨﾏﾈｼﾞｬｰが付与	
登録局設備責任者	登録認証業務用設備の管理統括	登録局ｾｷｭﾘﾃｨﾏﾈｼﾞｬｰが付与	
登録局設備担当者①	登録認証業務用設備の管理	登録局ｾｷｭﾘﾃｨﾏﾈｼﾞｬｰが付与	
登録局設備担当者②	登録認証業務用設備の管理	登録局ｾｷｭﾘﾃｨﾏﾈｼﾞｬｰが付与	
登録局ｾｷｭﾘﾃｨﾏﾈｼﾞｬｰ	登録認証業務用設備のｾｷｭﾘﾃｨ維持管理、認証設備室の鍵管理	登録局責任者が付与	
キーマネジャー	発行局の鍵管理	登録局ｾｷｭﾘﾃｨﾏﾈｼﾞｬｰが付与（生体認証）	

表 6　発行局の各役割とその主な業務内容、設備へのアクセス権限

役割	主な業務	入室権限付与	設備への アクセス権限
IA 責任者	IA 運営統括	なし	なし
IA 業務責任者	IA 業務統括	IA 設備室に関する入室権限を IA セキュリティマネージャが付与 生体認証	なし
IA システム管理責任者	IA 認証業務用設備の管理統括		IA 認証業務用設備の管理者権限
IA システム管理担当者	IA 認証業務用設備の管理		IA 認証業務用設備のユーザ権限
IA システム運用責任者	IA 認証業務用設備の運用統括		IA 認証業務用設備のユーザ権限
IA システム運用担当者	IA 認証業務用設備の運用		IA 認証業務用設備のユーザ権限
IA システム監視担当者	IA 認証業務用設備のログ監査	なし	なし
IA セキュリティマネージャ	IA 認証業務用設備のセキュリティ維持管理、認証設備室の鍵管理	IA 設備室の入室権限を IA 責任者が付与	なし
キーマネージャ	発行局の鍵管理	IA 設備室の入室権限を IA セキュリティマネージャが付与 生体認証	IA 認証業務用設備のユーザ権限
プールＡ	発行局におけるシステムレベルのセキュリティシェアの管理と行使	なし	なし
プールＢ	発行局におけるユーザーレベルのセキュリティシェアの管理と行使	なし	なし
セーフ・コンビネーション	発行局における金庫等の鍵の管理と行使	なし	なし

表 7　登録局の各役割とその主な業務内容、設備へのアクセス権限

役割	主な業務	入室権限付与	設備へのアクセス権限
RA 責任者	RA 運営統括	なし	なし
RA 業務責任者	RA 認証・登録業務統括	なし	なし
RA 認証業務担当者	RA 認証業務の実施（申請受付・審査）	RA オペレーション室への入室権限を RA セキュリティマネージャが付与	RA 端末のユーザ権限
RA 登録業務担当者	RA 登録業務の実施（IA への指示、セキュリティデバイスの発行・発送）	RA オペレーション室への入室権限を RA セキュリティマネージャが付与	RA 端末のユーザ権限
RA 設備責任者	RA 認証業務用設備の管理統括	RA 設備室、オペレーション室への入室権限を RA セキュリティマネージャが付与	RA 認証業務用設備の管理者権限
RA 設備担当者 A	RA 認証業務用設備の管理		RA 認証業務用設備の管理者権限
RA 設備担当者 B			RA 認証業務用設備のユーザ権限
RA セキュリティマネージャ	RA 認証業務用設備のセキュリティ維持管理 RA 設備室、オペレーション室の鍵管理	RA 設備室、オペレーション室への入室権限を RA 責任者が付与	なし

登録局の各役割の者は、RA 業務室への入室権限を有する。

５．３　人事統制

認証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・配置を行う。

本認証局は、全ての就業者の役割に応じ、以下の項目についての必要な教育計画を年度毎に定め、計画に従って教育を実施するとともに、その実施結果について記録し、証跡資料を残す。

- 必要な知識、技術を習得するための教育
- 指揮命令系統、責任および権限の変更に伴う教育
- 業務手順変更に伴う教育
- 危機管理に関する教育

６．技術的セキュリティ統制

６．１　鍵ペアの生成とインストール

本認証局で生成する認証局およびユーザ証明書利用者の鍵ペアは、信頼性あるシステムを用いて生成する。生成された鍵ペアは、漏えい、改変、き損等あるいは無断使用の防止措置を十分に講じて保護する。

サーバ証明書利用者の鍵ペアは、利用企業において作成されるため規定しない。

６．１．１　鍵ペア生成

認証局の鍵ペアは、IA 設備室内に設置された暗号装置内で、発行局の複数要員により、一人の操作だけではできない方法により生成される。

ユーザ証明書利用者の鍵ペアは、RA 設備室において、本認証局の複数の担当者が相互に牽制を行う状態で、特定の電子計算機の中で生成する。

６．１．２　秘密鍵の配布方法

ユーザ証明書利用者の秘密鍵は、本 CPS 4.2 および 4.3 に従って、証明書利用者に配布される。

６．１．３　公開鍵の提出方法

ユーザ証明書利用者の鍵ペアは本認証局において生成されるため､本項目は規定しない。

６．１．４　認証局公開鍵の提供方法

本認証局の公開鍵は、認証局証明書を本認証局のリポジトリで公開することで、証明書利用者および依拠当事者に提供される。本認証局では、認証局の証明書が正当であることを確認する手段として、KS Solutions ルート認証局証明書のハッシュ値を提供する。

６．１．５　鍵長

本認証局に関する RSA 鍵ペアの鍵長は以下のとおりとする。

- KS Solutions ルート認証局： 2048 ビット
- KS Solutions ユーザ証明書認証局： 2048 ビット
- KS Solutions サーバ証明書認証局： 2048 ビット
- ユーザ証明書： 2048 ビット
- サーバ証明書： 2048 ビット

６．１．６　公開鍵パラメータの生成

規定しない。

６．１．７　パラメータ品質の検査

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

本認証局の鍵ペアは、専用の暗号装置内で生成される。ユーザ証明書利用者の鍵ペアは、RA 設備室内の専用のソフトウェアで生成される。

６．１．９　鍵使用目的

KS Solutions ルート認証局の秘密鍵は、原則として以下の目的以外に使用されない。

- KS Solutions ユーザ証明書認証局証明書への電子署名
- KS Solutions サーバ証明書認証局証明書への電子署名
-

KS Solutions ユーザ証明書認証局の秘密鍵は、原則として以下の目的以外に使用されない。

- ユーザ証明書への電子署名
- CRL への電子署名

ユーザ証明書利用者の秘密鍵は、以下の目的以外に使用してはならない。

- 情報システム等への認証によるアクセスコントロール
- 電子メールへの署名・暗号化

KS Solutions サーバ証明書認証局の秘密鍵は、原則として以下の目的以外に使用されない。

- サーバ証明書への電子署名
- CRL への電子署名

６．２　秘密鍵の保護

６．２．１　暗号モジュールに関する標準

ユーザ証明書利用者の秘密鍵は、セキュリティデバイスに格納し、保護する。

サーバ証明書利用者の鍵ペアは利用企業において作成されるため、規定しない。

６．２．２　秘密鍵の複数人制御

本認証局の秘密鍵は、その使用にあたり活性化される必要がある。秘密鍵の生成および活性化については、複数人の管理の下、IA 設備室内において定められた手順により行われる。

本認証局は、ユーザ証明書利用者の秘密鍵の生成、廃棄、セキュリティデバイスへの格納およびセキュリティデバイスの送付に係る管理を、複数人の管理の下、RA オペレーション室内において定められた手順により行う。

６．２．３　秘密鍵の預託

本認証局では、秘密鍵の預託を行わない。

６．２．４　秘密鍵のバックアップ

本認証局は、認証局の秘密鍵のバックアップを行う。バックアップは、複数人の管理の下、IA 設備室内において定められた手順により行われ、バックアップ用の外部媒体は、定められた手順に従って IA 設備室内もしくは IA 設備室と同等のセキュリティが施された安全な場所に保存される。

登録局で生成したユーザ証明書利用者の秘密鍵と PKCS#12 の PIN は、セキュリティデバイスの初期不良等による交換に対応するため、セキュリティデバイスを利用企業に送付後、登録局で最大２ヶ月間保管する。その際、ユーザ証明書利用者の秘密鍵は暗号化を行い、ユーザ証明書利用者の秘密鍵と PKCS#12 の PIN は別の機器に保管する。

６．２．５　秘密鍵のアーカイブ

本認証局では、秘密鍵のアーカイブを行わない。

６．２．６　暗号モジュールへの秘密鍵の格納

本認証局の秘密鍵は、専用のサーバで生成され、当該サーバはオフラインで運用される。本認証局の秘密鍵は、本 CPS 6.2.4 で規定したバックアップ作成時を除き、外部に取り出されることはない。

ユーザ証明書利用者の秘密鍵は、RA 設備室内に設置された特定の電子計算機の中で生成し、RA オペレーション室でセキュリティデバイスへ格納する。ユーザ証明書利用者の秘密鍵は、セキュリティデバイスへの格納が完了した後に、本 CPS 6.2.4 で規定したバックアップを除き、生成から格納までに経由したすべての装置上から消去する。

６．２．７　秘密鍵の活性化方法

認証局の秘密鍵は、認証設備室内において、複数人の要員がサーバをオフラインすることで活性化される。

ユーザ証明書利用者の秘密鍵は、セキュリティデバイスに設定された利用者 PIN を入力することにより活性化される。

６．２．８　秘密鍵の非活性化方法

認証局の秘密鍵は、認証設備室内において、複数人の要員が非活性化作業を行うことにより非活性化される。

ユーザ証明書利用者の秘密鍵は、セキュリティデバイスを取り外すこと等により非活性化される。

６．２．９　秘密鍵の破棄方法

本認証局の秘密鍵の廃棄は、定められた手順に従い専用の機器を用いて、複数人の管理の下、鍵を完全に復元できない方法により行われる。また、バックアップされた秘密鍵も一連の作業指示において遅延なく完全に破棄される。

利用企業は、ユーザ証明書利用者の秘密鍵の破棄が必要になった場合、自己の判断において、証明書利用者から当該秘密鍵が格納されたセキュリティデバイスの回収および破棄を行う。

６．３　鍵ペア管理に関するその他の項目

６．３．１　公開鍵のアーカイブ

本認証局の公開鍵は、本 CPS2.6.1 に示すリポジトリにて公開する。ユーザ証明書利用者の公開鍵は定められた手順に従い、本認証局内で保管されており、原則として非公開とする。

サーバ証明書利用者の鍵ペアは利用企業において作成されるため、規定しない。

６．３．２　鍵ペアの利用期間

本認証局の鍵ペアの利用期間は、以下のとおりとする。

- KS Solutions ルート認証局： 30 年
- KS Solutions ユーザ証明書認証局： 30 年
- KS Solutions サーバ証明書認証局： 30 年

ユーザ証明書利用者の鍵ペアの利用期間は、本認証局と利用企業との間で合意された期間とする。ただし、利用企業の定めた時期に一括して鍵ペアの更新を行うことがある。

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

本認証局の秘密鍵に関する活性化データは、複数の担当者が相互に牽制を行う状態で、安全に生成、インストールされる。

ユーザ証明書利用者の秘密鍵を格納したセキュリティデバイスの利用者 PIN は、利用企業と登録局の間で別途合意した方法で設定するものとする。

サーバ証明書利用者の鍵ペアは利用企業において作成されるため規定しない。

６．４．２　活性化データの保護

本認証局の秘密鍵に関する活性化データは、複数の担当者が相互に牽制を行う状態でなければ利用できないよう、安全に保護される。

本認証局は、ユーザ証明書利用者のセキュリティデバイスの利用者 PIN を、利用企業と登録局との間で別途合意した方法で設定する。利用企業は、ユーザ証明書利用者に対してセキュリティデバイスの利用者 PIN を保護することを義務付けなければならない。

本認証局は、ユーザ証明書利用者の秘密鍵のバックアップを消去する際、同時に本認証局が管理する全ての装置上から、PKCS#12 の PIN の情報も消去する。

６．４．３　活性化データに関するその他の項目

規定しない。

６．５　ネットワークセキュリティ統制

IA 認証業務用設備と RA 認証業務用設備は、外部からの不正なアクセスを防止するためのファイヤーウォールを備えている。

IA 認証業務用設備と RA 認証業務用設備との間で行われる通信に関しては、送信をした設備の誤認、通信内容の盗聴および改変を防止するセキュリティ機能を持ったアプリケーションが使用される。

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

７．１．１　バージョン番号

本認証局は、ITU-T Recommendation X.509 で規定されたバージョン 3 の仕様に準拠した証明書を発行する。

７．１．２　拡張領域

本認証局が発行する証明書は、拡張領域を含む場合がある。表 8に各証明書における拡張領域の利用方法についてまとめる。各拡張子の詳細については、付録 A に記述する。

表 8　証明書の拡張領域

項番	拡張領域の名称	Critical フラグ	KSS ルート認証局 証明書	ユーザ証明書認証局 証明書	ユーザ証明書	サーバ証明書認証局 証明書	サーバ証明書
1	AuthorityKeyIdentifier	FALSE	○	○	○	○	○
2	SubjectKeyIdentifier	FALSE	○	○	○	○	○
3	KeyUsage	TRUE	○	○	○	○	○
4	ExtendedKeyUsage	FALSE	－	－	○	－	－
5	CertificatePolicies	FALSE	－	－	○	－	○
6	SubjectAltName	FALSE	－	○	○	○	○
7	BasicConstraints	TRUE	○	○	－	○	－
8	CRLDistributionPoints	FALSE	○	○	○	○	○
9	NetscapeCertType	FALSE	－	○	○	○	○

※1　本表に記載のない拡張領域については利用しない。

７．１．３　アルゴリズムのオブジェクト識別子

本認証局では、オブジェクト識別子が 1.2.840.113549.1.1.11 で識別される sha-256WithRSAEncryption 方式のアルゴリズムを用いて、証明書に電子署名を行う。

７．１．４　名前の形式

本認証局は、本 CPS 3.1 に従い、各種証明書に発行者名（issuer）および主体者名（subject）を設定する。また、拡張子である subjectAltName、issuerAltName については、本 CPS 7.1.2 の内容に従って設定を行う。

７．１．５　名前制約

規定しない。

７．１．６　証明書ポリシーのオブジェクト識別子

本認証局は、証明書の証明書ポリシー拡張子フィールドにおいて、本 CPS 1.2 で定義するオブジェクト識別子（OID）を設定する。

７．１．７　ポリシー制約拡張子の利用

規定しない。

７．１．８　ポリシー修飾子の記載と意味

規定しない。

７．１．９　クリティカルな拡張フィールドの処理方法

規定しない。

７．２　失効情報のプロファイル

７．２．１　バージョン番号

本認証局は、X.509 で規定されるバージョン 1 に準拠した失効情報（CRL）を発行する。

７．２．２　CRL およびエントリの拡張子

本認証局が発行する失効情報は、拡張領域を含まない。詳細については、付録 B に記述する。

８．仕様管理

８．１　仕様の変更手続き

本認証局は、利用企業、証明書利用者、または、依拠当事者による事前の承諾なしに、随時本 CPS を変更することができる。本 CPS の改訂は、本認証局における最高意思決定機関である情報セキュリティ委員会における承認を必要とする。

本認証局は、本 CPS の変更を実施した場合、本 CPS の修正版、または変更箇所についての説明をリポジトリ上にて公開する。

８．２　公表と通知に関する方針

本認証局は、本 CPS および本 CPS の改訂に関する履歴を本 CPS 2.6 に定義されたリポジトリにて公開する。また、本認証局の運用に関する各種規定については、リポジトリにて公開されたものを除き、原則として非公開とする。

８．３　CPS の承認

本認証局では、証明書ポリシー（Certificate Policy、以下「CP」という）を別途定めておらず、本 CPS の CP に対する承認プロセスは存在しない。

本 CPS は本 CPS 8.1 の内容に基づき改訂、承認される。