NRA-PKI 統合認証基盤

認証局運用規程

(Certification Practice Statement)

Version 1.20

2018 年 11 月 27 日

変更履歴

バージョン	日付	改訂事由
1.10	2011/10/01	初版
1.20	2018/11/27	仕様変更

目　　次

１．　はじめに

１．１　目的

本認証局運用規程（以下、「本 CPS」という。）は、日本 RA 株式会社（以下、「日本 RA」という。）が提供する NRA-PKI 統合認証基盤サービス（以下、「統合認証基盤サービス」という。）に関し、日本 RA 認証局（以下、「本認証局」という。）が発行する電子証明書の適切な運用・管理に資することを目的とする。

１．２　概要

日本 RA は、本認証局を設置し、同社が提供する統合認証基盤サービスを利用者（本 CPS １．４．４に定義する。）が利用するために必要な電子証明書（以下、「証明書」という）の発行と管理を行う。

本 CPS は、本認証局が認証業務を行う際の運用に関する規程であり、発行局および登録局を含む本認証局の運用方針、利用者と本認証局との関係、本認証局が利用者に対して発行する電子証明書の取り扱い等を定めている。証明書の取り扱いには、申請・登録・発行・更新・再発行・失効・有効期間満了に関する記述、および証明書の発行方針と利用に関連する要件が含まれる。

また、日本 RA は、IETF PKIX ワーキンググループが定める RFC3647「Certificate Policy and Certification Practices Framework」のフレームワークに準じて本 CPS を記載し、当該フレームワークのうち本認証局に適用されない事項については、「規定しない」と記載する。

なお、本 CPS は、本認証局が発行する証明書のプロファイルについても定める。本認証局は、証明書毎の証明書ポリシー（以下、「CP」という。）を個別に定めず、本 CPS が各 CP を包含するものとする。

１．３　文書名称と識別

本 CPS の正式名称は、「NRA-PKI 統合認証基盤認証局運用規程（Certification Practice Statement)」とする。

１．４　PKI の関係者

本 CPS に記述される PKI の関係者を以下に定める。各関係者は、本 CPS の内容に同意し、本 CPS の定める義務を遵守しなければならない。

１．４．１　認証局

本認証局は、発行局および登録局から構成される。本認証局は本 CPS５．２．１　に定める認証局責任者が統括し、認証局責任者が本 CPS を承認し、本認証局が認証業務を行う際の運用に関する規定として本 CPS を採用する。統合認証基盤サービスの認証局は、ルート認証局と中間認証局で構成され、本 CPS では利用者の証明書を発行する中間認証局を認証局として記述する。

認証局は、以下に示す発行局および登録局からなる。

- **発行局**

  登録局からの指示に基づき、電子証明書利用者（以下、「利用者」という。）の鍵ペアの生成、および証明書の発行・失効を行う。また、CRL（失効リスト）の生成・公開を行う。また、本 CPS に基づき、本認証局の秘密鍵を管理する。

- **登録局**

  証明書の発行・失効に係る審査・登録、および発行局に対する証明書の発行・失効指示、および発行された証明書の利用者への提供を行う。また、必要に応じ、問い合わせ対応窓口を設け、利用者からの証明書の申請・発行・失効等に関する問い合わせへの対応を行う。また、統合認証基盤サービスに加入するサービス提供会社およびこれが提供するサービスを審査する。本認証局は、登録局が許可したサービスの利用者に対してのみ、証明書を発行することができる。

１．４．２　利用者管理組織

利用者管理組織は、サービス提供会社が統合認証基盤サービスの利用を許可した組織であり、(i)利用者管理組織は、証明書の発行を申請するため、本 CPS および本 CPS２．２　２．１に定める関連諸規定に同意の上、(ii)利用者管理組織が申込責任者として選任した利用者管理組織に属する個人（以下、「申込責任者」という。）が、証明書の利用申請をサービス提供会社に対し申請する。利用者管理組織は、証明書の利用に際して、自らが管理する利用者および信頼当事者に対して、本 CPS および関連諸規定に同意させ、これらを遵守させる。

また、利用者管理組織は、証明書の紛失などの緊急時に対し、証明書の失効を行うことができる統合認証基盤のインターフェースを利用する権利を有する。

なお、利用者が利用者管理組織を有する法人等に属さない場合、サービス提供会社は利用者管理組織の加入審査と同等の審査を行うこととし、利用者はサービス提供会社へ証明書の発行を申請することができる。

１．４．３　サービス提供会社

サービス提供会社は、利用者管理組織を審査し、申込責任者からの利用申請の可否を判断する。利用者が利用者管理組織を有する法人等に属さない場合には、利用者について、利用者管理組織の審査と同等の加入審査を行い、利用申請を判断する。

また、サービス提供会社は本認証局が発行する証明書および CRL を信頼し、本認証局が発行する証明書を、認証基盤サービスに登録した自らのサービスにおいて、本 CPS１．５．２　に定める用途に限り利用することができる。

１．４．４　利用者

統合認証基盤における利用者とは、サービス提供会社がサービス利用を許可した利用者管理組織の管理の下にある個人、もしくは個人であり、本認証局が発行する証明書の所有者をいう。

１．４．５　信頼当事者

信頼当事者は、サービス提供会社もしくは利用者管理組織の指示または定める事項に従い、本認証局および利用者の証明書の有効性について検証を行う組織または個人である。

１．４．６　その他の関係者

規定しない。

１．５　証明書の用途

１．５．１　証明書の種類

本認証局は、以下の証明書を発行する。

(1)　ルート認証局証明書

ルート認証局証明書は、ルート認証局の自己署名証明書であり、ルート認証局は自身の公開鍵に対して自身の秘密鍵で電子署名をしている。ルート認証局の秘密鍵は、認証局失効リスト（以下、「CRL」という。）と中間認証局の公開鍵に対する電子署名の用途に使用される。

(2)　認証局証明書

認証局証明書は、本認証局自身の証明書であり、本認証局の公開鍵に対してルート認証局の秘密鍵で電子署名されている。本認証局の秘密鍵は、利用者に配付される証明書および CRL への電子署名の用途に使用される。

(3)　利用者証明書

個人に対して発行される証明書であり、信頼当事者のネットワーク機器間における SSL、IPSec、IEEE802.1x 等のネットワークアクセス認証を実現する。本認証局は、本認証局の判断および管理の下、動作確認等を目的とした証明書の発行・失効を行えるものとする。

１．５．２　正規の証明書用途

証明書および対応する鍵ペアは、以下の用途で使用できる。

- サービスにおけるクライアント認証
- SSL(TLS)・VPN 通信等における認証やアクセスコントロール
- Windows ドメイン環境に対する利用者認証
- その他、本認証局が認定する用途
- 電子署名

１．５．３　禁止されている証明書用途

本認証局は、本 CPS １．５．２　に定める用途以外での利用を禁止する。

１．６　ポリシー管理

１．６．１　文書の管理組織

本 CPS は、本認証局により管理される。

１．６．２　連絡窓口

本認証局は、日本 RA が提供するアプリケーションおよび本 CPS 等に関する照会を以下の連絡先にて受け付ける。

窓口：日本 RA 株式会社　サポート窓口
受付時間：10:00～12:00 13:00～17:00
お問合せ：support@nrapki.jp

住所：〒105-0021　東京都港区東新橋 2-1-6 プリプラビル

１．６．３　ポリシーに対する本 CPS の準拠性調査担当者

規定しない。

１．６．４　適合性の承認手続き

規定しない。

２．　公開とリポジトリの責任

２．１　リポジトリ

本認証局は、以下に示す本認証局に関する重要事項等の情報を目的別に日本 RA の Web に公開する。

(1)　本 CPS
(2)　関連諸規定（日本 RA との間の利用契約書に規定される諸規定を含む。以下同じ。）
(3)　信頼者による証明書検証に際しての注意事項等

また、上記の他、CRL を公開する。

(4)　CRL：証明書の CDP（CRL 配布ポイント）欄に URL を記載

上記については、常時参照可能とする。但し、保守作業等により、一時的に利用できないことがある。

２．２　認証情報の公開

規定しない。

２．３　公開の時期と周期

本 CPS が改訂され承認された場合、新しい CPS の有効開始日と共に速やかにこれを公開する。

CRL については、本 CPS ４．９．７　による周期で更新、公開する。

２．４　リポジトリに対するアクセスコントロール

本認証局は、リポジトリに対する情報セキュリティ対策以外の目的で特段のアクセスコントロールは行わない。

３．　本人性確認と認証

３．１　名称

３．１．１　名称のタイプ

利用者は、証明書の中の X.500 識別名 Distinguished Name（以下、「DN」という。）で、一意に識別される。

３．１．２　名称の意味に関する要件

証明書中の DN に含まれる固有名称 Common Name（以下、「CN」という。）には、利用者を識別するために利用者の氏名（英字表記）を記載する。また、Organization Unit（以下、「OU」という。）には、本認証局が同一の利用者に対し複数の証明書を発行することを可能とするために、統合認証基盤が採番する値を記載する。

３．１．３　利用者の匿名・仮名についての要件

本認証局は、原則として本名で CN を記載する。

３．１．４　様々な名称形式を解釈するためのルール

本認証局が発行する証明書の DN の形式は、X.500 に従う。

３．１．５　名称の一意性

本認証局が発行する証明書は、証明書中の別名(SubjectAltName) 中に含まれる E-Mail アドレスと OU に記載された値により利用者を一意に割り当てる。

また、証明書の固有名称(CN)には、同姓同名への対策は講じない。

３．１．６　商標等の認識、認証および役割

本認証局は、サービス提供会社およびサービスの登録、利用者の証明書の発行に際し、著作権、営業秘密、商標権、実用新案権、特許権その他の知的財産権（特許その他の知的財産を受ける権利を含むがこれらに限られない。）については、審査で確認しない。

３．２　初回の利用者の本人性確認

３．２．１　秘密鍵の所有を検証する方法

本認証局は、利用者の秘密鍵が発行局内で生成され、PKCS#12 形式にて配送されるため、同配送をもって、利用者が秘密鍵を所有したものとみなす。

３．２．２　利用者の確認

本認証局は、登録局が許可したサービス提供会社が、当該サービスを利用する利用者管理組織もしくは利用者本人からの利用申請を許可することで、利用者の確認とする。

３．２．３　確認しない利用者情報

本認証局は、利用者の CN および Organization に記載される法人等の名称については、サービス提供会社に対し、その値の真正性または正確性の確認を求めない。ただし、異なる利用者において、同一の法人等の名称が確認された場合はこの限りではない。

３．２．４　権限の正当性確認

本認証局は、登録局による本 CPS３．２．２　に定める確認をもって、当該利用者が証明書の発行をうける権限を有することの確認とする。

３．２．５　相互運用性基準

規定しない。

３．３　鍵（証明書）更新申請時の本人性確認と認証

３．３．１　鍵（証明書）定期更新時の本人性確認と認証

当該サービスを利用する利用者管理組織もしくは利用者本人が秘密鍵を所有していることをもって、利用者の本人性確認とする。

３．３．２　失効後の鍵（証明書）再発行時の本人性確認と認証

本 CPS ３．２．２　を準用する。

３．４　失効申請時の本人性確認と認証

本認証局は、登録局が利用者管理組織から失効が必要となる利用者のリストを受け取ることをもって、失効申請時の確認とする。
また、法人等に所属しない利用者に対しては、サービス提供会社からの失効申請依頼をもって、失効申請時の確認とする。

４．　証明書のライフサイクル

４．１　証明書申請

４．１．１　証明書の利用申請が認められる者

サービス提供会社とする。

４．１．２　証明書の利用申請方法

サービス提供会社が利用者管理組織における申込責任者（利用者が利用者管理組織を有する法人等に属さない場合には、利用者自身）から利用申請を受理し、利用者管理組織（利用者が利用者管理組織を有する法人等に属さない場合には、利用者自身）を審査の上、登録局に対して利用者のリストを提示するものとする。

４．２　証明書申請プロセス

４．２．１　本人性確認と認証業務の実行

本 CPS３．２．２を準用する。

４．２．２　証明書申請の承認または拒否

本 CPS３．２．２を準用する。

４．２．３　証明書申請プロセスの時間

規定しない。

４．３　証明書の発行

４．３．１　証明書発行時の認証局の行動

登録局は、本 CPS３．２．２　に従い発行局に対し証明書の発行指示を行う。発行局は、指示送信元である登録局の正当性を確認した上で、自動的に利用者の鍵ペアを生成し、対応する証明書を発行する。

４．３．２　認証局から利用者への証明書発行の通知

本認証局による証明書の発行に関する利用者への通知方法について、利用者への証明書の配付方法により、以下のとおり定める。

① 利用者への鍵・証明書の個別配付時
登録局は、利用者が証明書および秘密鍵をダウンロードするために必要な手続きの情報を添えて、当該利用者の電子メールアドレスに対して通知を行う。もしくは、同内容を信書にて利用者もしくは利用者が所属する利用者管理組織に通達する。

② サービス提供会社を経由した鍵・証明書の配付時
本認証局は、登録局が証明書および秘密鍵をサービス提供会社へ受け渡すことをもって通知とみなす。この場合、登録局は、利用者への個別の通知を行わない。

４．４　証明書受領

４．４．１　証明書受領確認手続き

本認証局による、利用者の証明書受領の確認方法について、その配付方法により、以下のとおり定める。

① 利用者への鍵・証明書の個別配付時
利用者は、本 CPS４．３．２　の規定に基づく本認証局から送信された電子メールもしくは信書に記載された通知内容に従い、自ら認証の上、証明書および秘密鍵をダウンロードする。本認証局は、利用者が所定の Web サイトより証明書および秘密鍵をダウンロードしたことをもって、当該証明書に関わる利用者が自ら証明書を受領したものとみなす。

② サービス提供会社を経由した鍵・証明書の配付時
本認証局は、証明書および秘密鍵を、サービス提供会社へ受け渡したことをもって、証明書の受領確認とする。サービス提供会社は、受領した証明書および秘密鍵を確実に利用者に配付しなければならない。

４．４．２　認証局による証明書の公開

本認証局は、利用者の証明書を公開しない。

４．４．３　認証局による他の関係者に対する証明書発行の通知

本認証局は、本 CPS４．３．２　の規定に基づくもの以外への証明書の発行通知を行わない。

４．５　鍵ペアと証明書の利用

４．５．１　利用者による秘密鍵と証明書の利用

利用者は、証明書と秘密鍵の用途について、本 CPS１．５．２　に従うこととし、規定された用途以外に使用してはならない。

また、第三者に使用させてはならない。

なお、秘密鍵をバックアップの目的以外で複写してはならない。

４．５．２　信頼当事者に対する利用者の公開鍵と証明書の利用

信頼当事者は、利用者管理組織の指示または定めに従い、本認証局および利用者の証明書の有効性について検証を行う。

また、利用者の公開鍵と証明書の用途については、本 CPS１．５．２　に従うこととし、信頼当事者は、規定された用途以外に利用者の公開鍵を使用してはならない。

また、信頼当事者は、利用者の公開鍵の使用に際して、CRL によりその時点での有効性の検証を必ず行わなければならない。

４．６　鍵更新を伴わない証明書更新

４．６．１　鍵更新を伴わない証明書更新に関する要件

本認証局は、鍵ペアの更新を伴わない証明書の更新を認めない。

４．６．２　証明書利用申請者

規定しない。

４．６．３　証明書申請プロセス

規定しない。

４．６．４　利用者への新しい証明書発行の通知

規定しない。

４．６．５　証明書受領確認手続き

規定しない。

４．６．６　認証局による新しい証明書の公開

規定しない。

４．６．７　認証局による他の関係者に対する新しい証明書発行の通知

規定しない。

４．７　鍵更新を伴う証明書更新

４．７．１　鍵更新に関する要件

本認証局は、証明書の更新に際して、利用者が保持する既存の鍵ペアの継続利用を認めず、必ず新しい鍵ペアを生成し、その公開鍵に対する新しい証明書を発行する。

証明書の更新は、証明書の有効期間満了に伴う新たな証明書の発行（以下、「更新発行」という。）、および本認証局が許可した証明書失効後の再発行に際して行う。

４．７．２　新しい公開鍵に対する証明書利用申請者

本 CPS ４．１．１　を準用する。

４．７．３　鍵更新における証明書申請プロセス

本認証局は、利用者が有効な証明書を所有していることをもって更新発行を許可する。

４．７．４　利用者への新しい証明書発行の通知

本 CPS ４．３．２　を準用する。

４．７．５　鍵更新された証明書の受領確認手続き

本 CPS ４．４．１　を準用する。

４．７．６　鍵更新された証明書の公開

本 CPS ４．４．２　を準用する。

４．７．７　鍵更新された証明書の他の関係者に対する発行の通知

本 CPS ４．４．３　を準用する。

４．８　証明書の変更

４．８．１　証明書の変更に関する要件

利用者は、証明書の記載内容に変更の必要が生じた場合、利用者管理組織の指示または定めに従うものとする。本認証局は、サービス提供会社からの利用者の証明書に関する変更要請に応じ、適切な内容の証明書を発行する。この場合、変更後の証明書の発行をもって変更前の証明書は失効される。

４．８．２　証明書変更の申請者

規定しない。

４．８．３　証明書変更の申請プロセス

本認証局は、利用者が有効な証明書を所有していることをもって証明書変更を許可する。

４．８．４　利用者への新しい証明書発行の通知

本 CPS４．３．２　を準用する。

４．８．５　変更された証明書の受領確認手続き

本 CPS ４．４．１　を準用する。

４．８．６　変更された証明書の公開

本 CPS ４．４．２　を準用する。

４．８．７　変更された証明書の他の関係者に対する発行の通知

本 CPS ４．４．３　を準用する。

４．９　証明書の失効と一時停止

４．９．１　失効の要件

本認証局は、下記の事由により当該証明書の失効を行う。

(1)　利用者側の事情による失効事由

（ア）　利用者の秘密鍵が危殆化した場合
（イ）　証明書を紛失して一定の時間が経過した場合
（ウ）　証明書の記載内容に変更の必要が生じた場合
（エ）　所属する法人等から退職した場合
（オ）　関連諸規定に規定する場合

(2)　本認証局側の事情による失効事由

（ア）　利用者の秘密鍵が危殆化したことを知り得た場合
（イ）　利用者証明書の記載内容に誤りがある場合
（ウ）　サービス提供会社のサービスが終了した場合
（エ）　サービス提供会社が統合基盤認証サービスを終了した場合
（オ）　統合基盤認証サービスが終了した場合

（カ）　　本認証局の秘密鍵が危殆化した場合
（キ）　　本認証局が認証業務を廃止する場合
（ク）　　関連諸規定に規定する場合
（ケ）　　その他、本認証局が必要と判断した場合

４．９．２　失効申請が認められる者

本 CPS４．９．１　に記載の事由に限り、利用者管理組織もしくは登録局が発行局に対し失効を指示することができる。

４．９．３　失効申請プロセス

証明書の失効申請については、以下の何れかの手続きに従う。

(1)　利用者側の事情による失効事由の手続き
　　利用者管理組織からの登録局への失効対象の証明書のリストの提示、登録局から発行局への失効指示。

(2)　本認証局側の事情による失効事由の手続き
　　登録局から発行局への失効指示。

(1)の場合、登録局は、本 CPS３．４の規定に従って申請の正当性を確認し、失効申請を承認する。但し、定められた変更の申請以外の方法による場合や、申請内容に疑義が生じた場合は、登録局は失効申請を拒否する。また、紛失による失効申請については、一定期間の一時停止をもって失効を行うものとする。

失効申請が承認された場合、発行局は、登録局からの失効指示に基づき、当該利用者の証明書を失効し、必要に応じて当該サービス提供会社に対して通知を行う。

４．９．４　失効申請までの猶予期間

失効申請者は、本 CPS ４．９．１　に定める事由が発生した場合、速やかに申請を行うものとする。

４．９．５　失効申請プロセスの時間

登録局は、失効申請を受領後、遅滞なく当該証明書の失効を発行局へ指示を行う。

４．９．６　信頼者による失効情報確認の要件

信頼当事者は、本認証局が発行する CRL により、証明書の失効を確認することができる。

４．９．７　CRL 発行周期

本認証局は、証明書が失効された時点で CRL を発行する。
また、失効が行われない場合においても、CRL を 24 時間の周期で発行する。

４．９．８　CRL がリポジトリに格納されるまでの最大遅延時間

本認証局は、発行された CRL は遅くとも 1 時間以内にリポジトリにて公開する。

４．９．９　オンラインでの証明書の有効性確認

CRL を証明書の失効情報確認の手段として提供する。また、有効期間の満了した証明書の失効情報確認についての問い合わせには応じない。

４．９．１０　オンラインでの証明書の失効情報確認要件

規定しない。

４．９．１１　その他の利用可能な失効情報確認の手段

CRL 以外の失効情報確認の手段を提供しない。

４．９．１２　鍵の危殆化の特別な要件

規定しない。

４．９．１３　一時停止の要件

下記の事由により当該証明書の一時停止を行う。

(1)　利用者による一時停止事由
　　(ア)　利用者が一定期間、証明書を利用しない場合
　　(イ)　証明書を紛失した場合
　　(ウ)　関連諸規定に規定する場合
(2)　本認証局による一時停止事由
　　(ア)　本認証局が必要と判断した場合
　　(イ)　関連諸規定に規定する場合

４．９．１４　一時停止申請者

本 CPS４．９．２　を準用する。

４．９．１５　一時停止申請の手続き

本CPS４．９．３　を準用する。

４．９．１６　一時停止可能な期間

規定しない。

４．１０　証明書ステータス確認サービス

本認証局は、CRL以外で証明書のステータスを確認できるサービスを提供しない。

４．１０．１　運用上の特徴

規定しない。

４．１０．２　サービスの可用性

規定しない。

４．１０．３　他の要件

規定しない。

４．１１　認証局への登録の終了

利用者は、証明書の利用を終了する場合、自身の証明書を抹消しなければならない。

また、証明書が有効である場合、本CPS４．９．１　に基づく証明書の失効をもって、登録の終了となる。

４．１２　鍵の第三者預託と鍵回復

４．１２．１　鍵預託とリカバリのポリシーと手順

規定しない。

４．１２．２　セッションキーのカプセル化・復旧のポリシーと手順

規定しない。

５．　設備、管理、運用統制

５．１　物理的な管理

５．１．１　施設の所在と構造

本認証局のシステムに係る施設（以下、「本施設」という。）は、地震、火災および水害、その他の災害による影響を容易に受けない施設に設置する。本施設には、建物構造上、耐震、耐火、水害および不正侵入防止の措置を講じる。

また、本施設は、建築物の外部および建築物内に発行局の所在を明示または暗示する名称を看板もしくは表示板等により一切掲示しない。

５．１．２　物理的アクセス

本認証局に係る施設は、入退館等に際して資格確認を行い、識別証等により入退出を管理する。

(1)　登録局

認証業務を行う各室では、業務の重要度に応じたセキュリティレベルを設定し、相応する入退室管理を行う。

(2)　発行局

入退室時の認証には、各室内において行われる認証業務の重要度に応じ、権限保有者であることを確認できる入退室用カードもしくは生体認証等を用いる。

建物内および各室内は、監視システムおよび監視要員による 24 時間 365 日監視を行う。

５．１．３　電源設備と空調設備

本認証局に係る施設は、機器類の運用のために十分な容量の電源を確保し、また、空調設備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。発行局については、瞬断、停電に備えた対策を講じ、商用電源が供給されない事態においては、自家発電機による電源供給に切り換える。また、空調設備は二重化する。

５．１．４　水害対策

本認証局に係る施設は、水害による影響を容易に受けない場所に設置する。発行局については、建物および各室に漏水検知器を設置し、天井、床には防水対策を講じる。

５．１．５　火災に対する予防措置と対策

本認証局に係る施設は、耐火構造とする。発行局については、本認証局に係るシステムを設置する室は防火区画とし、自動ガス消火設備を備える。

５．１．６　地震に対する予防措置と対策

本施設は、現行の建築基準法に規定する構造上の安全を有する。建物は、新耐震規準に基づいた耐震構造にて設計する。また、本認証局のシステム機器および什器には転倒および落下を防止する対策を講じる。

５．１．７　媒体保管場所

本認証局のシステムのバックアップデータが含まれる媒体、審査業務で使用した書類等については、職務上利用することが許可された者のみが入室できる室内に保管する。

５．１．８　廃棄物処理

本施設では、機密情報を含む書類はシュレッダーにより裁断の上、廃棄する。電子媒体については、物理的破壊、初期化、消磁等の措置によって記録されたデータを完全に抹消の上、廃棄する。

５．１．９　オフサイトバックアップ

規定しない。

５．２　職務統制

５．２．１　信頼される役割および人物

本認証局は、認証局を運営するために必要な人員（以下、「認証局員」という。）およびその役割を以下のとおり定める。

(1)　ポリシー承認局

本認証局におけるポリシーの決定、承認、本 CPS 等の重要ドキュメントの変更、承認等を行う最高意思決定機関であり、日本 RA の情報セキュリティ委員会が行う。

(2)　認証局責任者

本認証局を統括し、登録局責任者および発行局責任者を管理する。

(3)　登録局責任者

本認証局の登録局に係る業務を統括し、業務オペレータを管理する。

(4)　登録局オペレータ

本認証局の登録局に係る業務を行う。

証明書に関する窓口として、利用者・信頼者からの問い合わせにも対応する。

(5)　発行局責任者

本認証局の発行局に係る業務を統括し、発行局システムアドミニストレータおよび発行局オペレータを管理する。

(6)　発行局システムアドミニストレータ

発行局システムアドミニストレータは、発行局責任者の管理の下、本認証局のシステムの維持・管理を行う。

(7)　発行局オペレータ

本認証局に係るシステムの運用、保守および鍵管理等を行う。

(8)　業務監査担当者

本認証局とは独立した組織で監査を行う。

５．２．２　役割ごとに必要な人員の数

本認証局は、発行局システムアドミニストレータおよび発行局オペレータについては、2名以上配置する。

５．２．３　各役割における本人性確認と認証

本認証局は、各役割に応じ、認証業務を行う各室の入室権限および本認証局のシステムの操作権限を定める。また、発行局に関する各室への入室時またはシステムの操作時においては、入退室カード、生体認証、電子証明書、ID およびパスワード等の単体または組合せにより、本人性および入室・操作権限の確認ならびに認証を行う。

５．２．４　職務の分離が要求される役割

本認証局は、下記の職務については、兼務することを認めない。

(1)　認証局責任者
(2)　登録局責任者
(3)　登録局オペレータ
(4)　発行局責任者
(5)　業務監査担当者

５．３　人事面の管理

５．３．１　経歴、資格、経験などに関する要求事項

本認証業務に従事する全ての職員については、職務規程に基づき、審査、教育、配置転換等を行う。但し、業務の一部が外部の委託会社に委託される場合、当該委託業務に従事する職員は、当該委託会社の職務規程に基づき審査、教育、配置転換等を行う。

５．３．２　身元調査手続き

規定しない。

５．３．３　教育訓練要件

本認証局は、認証局員として従事するすべての職員に対し、その業務に応じた知識・技術情報の提供または教育訓練等を行う。

５．３．４　教育訓練の周期

本認証局は、認証局員に対する再教育および訓練を適宜実施する。
また、以下の事態が生じた場合には、教育・訓練を実施する。

① 本 CPS、および関連諸規定が改訂され、認証局責任者、発行局責任者、または登録局責任者が必要と判断した場合。
② 本認証局システムを変更する場合であって、認証局責任者、発行局責任者、または登録局責任者が必要と判断した場合。
③ その他、認証局責任者、発行局責任者、または登録局責任者が必要と判断した場合。

５．３．５　ジョブローテーションの周期と順序

本認証局は、必要に応じて認証局員の配置転換を行う。

５．３．６　許可されていない行動に対する罰則

認証局員が過失、故意に関わらず、本 CPS に記載されるポリシーと手続き、もしくは運用手順書に定める手順等に違反した場合、速やかに原因および影響範囲の調査を行った上で、処罰を課す。

５．３．７　職員に対する契約要件

本認証局は、外部の委託会社に委託された業務に係る職員については、就業規則に則った義務を遵守させる。

５．３．８　職員が参照できるドキュメント

本認証局は、認証局員が、運用手順書等、業務に係るドキュメントをその役割に応じて参照できる措置を講じる。

５．４　監査ログの手続き

５．４．１　記録されるイベントの種類

本認証局は、本 CPS の準拠性および情報セキュリティ対策の妥当性を評価するために、本認証局における業務および情報セキュリティに関する重要な事象を対象に、アクセスログや操作ログ等、監査ログを収集する。

５．４．２　監査ログを処理する頻度

本認証局は、認証局運用に疑義が生じた際などにおいて、機能不全、脆弱性または悪意の行動を検出する目的で監査ログを確認する。

５．４．３　監査ログの保持期間

本認証局は、発行した証明書の有効期間満了後の少なくとも 1 年間は監査ログを保管する。他の記録については、当該ログ発生より 3 年間保持する。

５．４．４　監査ログの保護

本認証局は、許可された者のみが閲覧可能となるよう、監査ログへのアクセスコントロールを施す。保管庫への物理的なアクセスコントロール、電子媒体であればフォルダ等への論理的なアクセスコントロールを施す。

５．４．５　監査ログのバックアップ手続き

本認証局は、監査ログに関する電子データを日次でバックアップし取得する。紙媒体については、原本のみを保管する。

５．４．６　監査ログ収集システム

発行局のシステムは、実装された機能により監査ログを自動的に収集する。

５．４．７　当事者に対する通知

本認証局は、イベントを発生させた当事者に通知することなく、監査ログを収集、検査する。

５．４．８　脆弱性評価

本認証局は、本認証局に係るシステムに対し、外部の専門機関による定期的な脆弱性評価を行う。また、その評価結果を文書化し保管する。

５．５　業務記録の保存

５．５．１　保存対象となる業務記録

本認証局は、本 CPS５．４．１　で規定された監査ログのほか、以下の情報を保管する。

(1)　ルート認証局証明書
(2)　認証局証明書
(3)　証明書発行・失効に係る情報
(4)　利用者証明書
(5)　内部監査報告書
(6)　サービス提供会社より受領した統合基盤認証サービスの申請等の書類
(7)　本 CPS および関連諸規定

５．５．２　業務記録の保持期間

本認証局は、本 CPS５．５．１　に規定される記録について、関連する証明書の有効期間を超えて少なくとも 1 年間保管する。

５．５．３　業務記録の保護

本 CPS５．４．４　を準用する。

５．５．４　業務記録のバックアップ手続き

本 CPS５．４．５　を準用する。

５．５．５　業務記録の日付要件

本認証局は、本 CPS５．５．１　に関し、帳票類については起票日もしくは処理した日付を記録する。また、日付のみでは記録としての立証性に欠ける場合は、時刻も記録する。本認証局および利用者の証明書については、発行された日時を記録する。また、本認証局のシステムには、発行する証明書および監査ログに対して正確な日付・時刻を記録するために必要な措置を講じる。

５．５．６　業務記録収集システム

本認証局は、電子データについては本認証局に係るシステムの機能により収集する。その他、紙媒体については、認証局員が収集する。

５．５．７　業務記録の取得と検証手続き

本認証局は、本 CPS５．５．１　に関し、記録の取得および閲覧は、業務監査担当者および認証局責任者が認めた者に限定する。また、記録の可読性に関わる検証は、必要に応じ、実施する。

５．６　認証局の鍵更新

本認証局は、20 年ごとに、認証局の鍵ペアを更新する。

５．７　危殆化および災害からの復旧

５．７．１　認証局秘密鍵の危殆化および災害からの復旧手続き

本認証局は、発行局の責による場合を除き、本認証局の秘密鍵の危殆化による統合認証基盤サービスの停止を不可抗力事項として扱い、同サービス再開に要する時間について保証しない。

本認証局は、以下の措置を実施するとともに、利用者・信頼者への周知を図る。

(1)　危殆化した秘密鍵を用いた認証業務の停止
(2)　全ての証明書の失効
(3)　危殆化の原因調査
(4)　本認証局の新しい鍵ペアの生成と対応する証明書の発行
(5)　本認証業務の再開の妥当性評価
(6)　本認証業務の再開
(7)　新たな鍵ペアの生成および証明書の発行

本認証局が被災した場合には、本 CPS ５．７．４　に基づき、復旧に努める。

５．７．２　ハードウェア、ソフトウェア、データの障害時の手続き

本認証局は、ハードウェア、ソフトウェア、データが破壊された場合には、バックアップ用のハードウェア、ソフトウェア、データにより、遅滞なく復旧作業を行う。

５．７．３　利用者秘密鍵危殆化時の手続き

利用者は、自身の秘密鍵の危殆化または危殆化が疑われる事態が生じた場合、本 CPS４．９．１　に記載されたとおり、当該事態の発生を利用者管理組織に連絡し、利用者管理組織の指示または定めに従うものとする。

５．７．４　認証局秘密鍵の危殆化および災害後の事業継続性

本認証局は、災害による認証局の停止を不可抗力事項として取扱い、統合認証基盤サービスの再開に要する時間について保証しない。

本認証局は、災害により統合認証基盤サービスが停止した場合、サービス提供会社に当該事実を通知する他、日本 RA の Web サイトにおいても、その旨公開する。サービス提供会社は、日本 RA よりかかる通知を受領した場合には、可及的速やかに当該事実を利用者管理組織に通知するものとする。

本認証局を管理する日本 RA は、以上に掲げる措置を実施するとともに、被災状況の調査を行い、調査結果に基づき、復旧方針を定めるものとし、発行局、登録局は当該復旧方針に従い復旧作業を実施する。

５．８　認証局の業務終了

本認証局は、業務を終了する場合、サービス提供会社および利用者管理組織に事前に通知するほか、日本 RA の Web サイトにおいても、その旨公開する。

本認証局が保有する証明書発行・失効申請に関わる情報については、廃棄するものとし、この旨は業務終了時に日本 RA の Web サイトにて告知する。

６．　技術面のセキュリティ管理

６．１　鍵ペア生成と導入

６．１．１　鍵ペアの生成

本認証局の鍵ペアは､認証局責任者の管理の下､認証局の運用担当者により FIPS 140-1 レベル 4 の秘密鍵管理モジュール（以下､「HSM」という。）を用いて生成する。

利用者の鍵ペアについては、本認証局が定める暗号ライブラリにより生成する。

６．１．２　利用者への秘密鍵の配送

本認証局は、サービス提供会社の依頼に基づき証明書に関わる秘密鍵を生成し、その気密性および完全性を確保する措置を講じた上で、利用者へ配付する。

６．１．３　本認証局への公開鍵の配送

本認証局は、利用者からの公開鍵の配送を受け付けない。

６．１．４　信頼者への認証局公開鍵の配送

本認証局は、信頼当事者に対する本認証局の公開鍵の配送を行わない。本認証局の公開鍵が含まれる認証局証明書は、本認証局のリポジトリにて公開する。

６．１．５　鍵長

本認証局が発行する認証局証明書に係る鍵は、下記の仕様に適合する鍵を利用する。

署名方式　：　　SHA2withRSA

合成数　　：　　2048 bit

利用者証明書に係る鍵は、下記の仕様に適合する鍵を利用する。

署名方式　：　　SHA1withRSA

合成数　　：　　2048 bit

６．１．６　公開鍵パラメータ生成および検査

規定しない。

６．１．７　鍵用途（X.509 v3 key usage フィールド）

本認証局が発行する証明書の鍵用途は、本 CPS１１．　に定める。

６．２　秘密鍵保護と秘密鍵管理モジュール技術の管理

６．２．１　秘密鍵管理モジュールの標準と管理

本認証局の鍵ペアは、FIPS 140-1 レベル 4 の秘密鍵管理モジュール（HSM）にて保護する。上記のモジュールは、発行局オペレータが管理する。

６．２．２　秘密鍵の複数人管理（n out of m）

本認証局の秘密鍵の管理は、常時複数人の発行局システムアドミニストレータが行う。

６．２．３　秘密鍵の預託

本認証局は、本認証局および利用者の秘密鍵の預託を行わない。

６．２．４　秘密鍵のバックアップ

本認証局の秘密鍵のバックアップは、発行局オペレータが行う。HSM からバックアップした本認証局の秘密鍵は、暗号化して複数に分割し、施錠可能な保管庫にて安全に保管する。

６．２．５　秘密鍵のアーカイブ

本認証局は、本認証局の秘密鍵のアーカイブを行わない。

６．２．６　秘密鍵管理モジュールからの秘密鍵の転送

本認証局は、HSM の故障など秘密鍵の復元が必要な場合、発行局責任者の管理・指示の下、発行局オペレータが、バックアップからの秘密鍵の復元を行う。このとき、バックアップデータを本施設外へ移送しない。

６．２．７　秘密鍵管理モジュール内での秘密鍵保存

本認証局の秘密鍵は、HSM 内で生成する。秘密鍵管理モジュール内で秘密鍵は暗号化し保存する。

６．２．８　秘密鍵の活性化

本認証局の秘密鍵は、本認証局起動手順に従い、発行局管理者の管理の下、複数人の発行局システムアドミニストレータが活性化を行う。また、活性化作業の内容を記録する。

６．２．９　秘密鍵の非活性化

本認証局の秘密鍵は、本認証局停止手順に従い、発行局管理者の管理の下、複数人の発行局技術担当者が非活性化を行う。また、非活性化作業の内容を記録する。

６．２．１０　秘密鍵破壊の方法

本認証局の秘密鍵は、認証局責任者の指示を受け、発行局管理者の管理の下、別途規定された手順に基づき、複数の発行局システムアドミニストレータが破壊する。同時に、バックアップされたデータについても、同様の手順に基づき破壊する。また、破壊作業の内容を記録する。

６．２．１１　秘密鍵管理モジュールの評価

本認証局は、本 CPS６．２．１　に定める標準を満たした HSM を使用する。

６．３　鍵ペア管理に関するその他の項目

６．３．１　公開鍵の保存

公開鍵の保存については、それを含む証明書を保存することによって行う。

６．３．２　証明書と鍵ペアの使用期間

証明書の有効期間を次に示す。

(1)　認証局証明書　：　20 年

(2)　利用者証明書　：　5 年以内

６．４　秘密鍵の活性化情報

６．４．１　活性化情報の作成と設定

本認証局内で使用される活性化情報は、容易に推測されないように配慮して生成し、設定する。

６．４．２　活性化情報の保護

本認証局内で使用される活性化情報は、本 CPS５．１　に基づき適切な入退室管理がなされた室内において、施錠可能な保管庫に保管する。

６．４．３　活性化情報に関するその他の項目

規定しない。

６．５　コンピュータセキュリティ管理

６．５．１　特定のコンピュータセキュリティに関する技術的要件

本認証局に係るシステムは、アクセス制御機能、操作者である発行局オペレータの識別と認証機能、システムのバックアップ・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の評価

本認証局に係るシステムは、事前に導入評価を実施し、認証業務開始後もセキュリティ上の脆弱性についての情報収集、評価を継続的に行い、重大な脆弱性が発見された場合には、速やかに必要な対処を行う。

６．６　技術面におけるライフサイクルの管理

６．６．１　システム開発管理

本認証局の構築・修正・変更は、認証局責任者の管理の下、信頼できる組織および環境にて作業を実施する。修正・変更に際しては、テスト環境において検証を行い、認証局責任者の承認を得た上で導入する。ただし、軽微な修正・変更の場合、発行局については発行局責任者の承認の下、登録局については登録局オペレータの判断により、作業を実施する。

６．６．２　セキュリティマネジメント管理

本認証局に係るシステムでは、十分なセキュリティレベルを確保するために必要な設定を行う。また、システムのセキュリティ上の脆弱性についての情報収集、評価を継続的に行ない、重大な脆弱性が発見された場合には、速やかに必要な対処を行う。

６．６．３　ライフサイクルセキュリティの管理

本認証局のシステムの開発、運用、変更、廃棄の各工程において責任者を定め、作業計画または手順を策定・評価し、必要に応じ試験を行う。また、各作業の内容を記録する。

６．７　ネットワークセキュリティ管理

本認証局のシステムとインターネット等の外部システムとは、ファイアウォール等を介して接続し、また侵入検知システムによる監視を行う。

６．８　日時の記録

本認証局に係るシステムには、発行する証明書および監査ログ等に対して正確な日付・時刻を記録するために必要な措置を講じる。

７．　証明書、CRL、OCSP の各プロファイル

７．１　証明書プロファイル

７．１．１　バージョン番号

本 CPS１１．　に定める証明書プロファイルにおいて規定する。

７．１．２　証明書拡張領域

本 CPS１１．　に定める証明書プロファイルにおいて規定する。

７．１．３　アルゴリズムオブジェクト識別子

本 CPS１１．　に定める証明書プロファイルにおいて規定する。

７．１．４　名前の形式

本 CPS１１．　に定める証明書プロファイルにおいて規定する。

７．１．５　名称制約

規定しない。

７．１．６　証明書ポリシーオブジェクト識別子

規定しない。

７．１．７　ポリシー制約拡張の使用

規定しない。

７．１．８　ポリシー修飾子の構文と意味

本 CPS１１．　に定める証明書プロファイルにおいて規定する。

７．１．９　重要な証明書ポリシー拡張についての処理方法

規定しない。

７．２　CRL プロファイル

７．２．１　バージョン番号

本 CPS１１．３　に定める CRL プロファイルにおいて規定する。

７．２．２　CRL、CRL エントリ拡張

本 CPS１１．３　に定める CRL プロファイルにおいて規定する。

７．３　OCSP プロファイル

７．３．１　バージョン番号

規定しない。

７．３．２　OCSP 拡張

規定しない。

８．　準拠性監査とその他の評価

８．１　監査の頻度と要件

本認証局は、認証業務に疑義が生じた場合、発行局および登録局の全部または一部について、本 CPS８．２　に定める監査人による監査を実施することができる。

８．２　監査人の要件

本認証局の監査は、必要な知識と経験を有する者が行う。

８．３　監査人と被監査者の関係

公正な監査を遂行するために、監査人は本認証局から独立していることとする。

８．４　監査の範囲

本認証局の認証業務が、本 CPS に準拠して実施されていることの監査を範囲とする。

８．５　監査における指摘事項への対応

監査により発見された指摘事項は、認証局責任者、発行局責任者および登録局責任者へ報告される。監査人、認証局責任者、発行局責任者、または登録局責任者により是正措置が必要と判断された場合、発行局責任者または登録局責任者の管理の下、是正措置を実施する。

８．６　監査結果の開示

本認証局は、監査結果を利用者および信頼当事者へ開示しない。
本認証局は、本認証局が必要と認めた対象にのみ監査結果を開示する。

９．　他のビジネス的・法的問題

９．１　料金

９．１．１　証明書発行または更新料

規定しない。

９．１．２　証明書へのアクセス料金

規定しない。

９．１．３　失効またはステータス情報へのアクセス料金

規定しない。

９．１．４　その他のサービスに関する料金

規定しない。

９．１．５　払い戻し指針

規定しない。

９．２　金銭上の責任

９．２．１　保険の適用範囲

規定しない。

９．２．２　その他の資産

規定しない。

９．２．３　利用者を保護する保険、保証

規定しない。

９．３　企業情報の秘密性

９．３．１　秘密情報の範囲

本認証局は、発行局、登録局が保有する情報のうち、以下の情報を機密として取り扱う（以下、「機密情報」という。）。

① サービス提供会社からの依頼情報
② 本CPS９．４．２　に定める情報
③ 本認証局の情報セキュリティに関する情報

９．３．２　秘密情報の範囲外の情報

本認証局は、発行局、登録局が保有する情報のうち、以下の情報については機密情報の範囲外とする。

① 本CPS２．２　において公開するものとして定める情報
② 本認証局の過失によらず公知となった情報
③ 本認証局以外のものから機密保持の制限なしに開示された情報
④ 第三者への提供の承諾を得た情報

９．３．３　秘密情報の保護責任

本認証局は、機密情報の漏えいを防止する対策を実施する。また、本認証局の運営の用に供する以外には機密情報を使用しない。なお、個人情報の取り扱いは、本CPS９．４　に定める。

９．４　個人情報の保護

９．４．１　プライバシーポリシー

本認証局は、発行局および登録局が保有する情報のうち、本CPS９．４．２　に該当する情報については、本 CPS に定める事項以外の事項に関しては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）、及び日本RAに適用される、行政機関が定める個人情報の保護に関するガイドラインに基づいて取り扱う。

また、日本RAは、本認証局の業務のうち自社が担当する業務については、Web サイトで公開するプライバシーポリシーを遵守する。

９．４．２　個人情報として扱われる情報

本認証局は、サービス提供会社および利用者管理組織から登録局へ証明書の発行または失効の指示等に含まれる、氏名、生年月日、その他の記述等により特定の個人を識別することができるものを個人情報として扱う。

９．４．３　個人情報とみなされない情報

本認証局は、本 CPS９．４．２　に定める情報以外は、個人情報としてみなさない。

９．４．４　個人情報を保護する責任

本認証局が保有する個人情報の保護責任は、本 CPS ９．４．１　に定めるとおりとする。

９．４．５　個人情報の使用に関する個人への通知および承認

本認証局は、証明書の利用申請もしくは失効申請をもって、本認証業務上必要とする個人情報の使用の承認を利用者から得たものとする。

９．４．６　司法手続または行政手続に基づく公開

本認証局で取扱う個人情報に関して、裁判上、行政上その他の法的手続きの過程において情報の開示要求があった場合、本認証局は、当該個人情報を開示することができるものとする。

９．４．７　他の情報公開の場合

本認証局は、業務の一部を外部の委託会社に委託する場合、秘密情報を委託会社に対して開示することがある。この場合、本認証局は、委託会社による情報の漏洩を防ぐため、委託会社との間で秘密保持に関する契約を締結し、守秘を義務づける。

９．５　知的財産権

特段の合意がなされない場合に限り、以下の情報に関わるすべての知的財産権は、日本 RA または本認証局のサービスに関する日本 RA の仕入先またはライセンサーに帰属するものとする。

(1)　本認証局の発行した証明書、証明書の失効情報

(2)　本 CPS およびその他関連文書

(3)　本認証局の公開鍵および秘密鍵
(4)　本認証局から貸与されたソフトウェア、ハードウェア

９．６　表明および保証

９．６．１　発行局の表明および保証

発行局を運営する組織は、本認証局を構成する発行局として発行局の義務の遂行にあたり、以下の義務を負うことを表明し保証する。

(1)　本 CPS に従った認証局秘密鍵の安全な管理を行うこと
(2)　登録局からの指示に基づき正確に証明書の発行および失効を行うこと
(3)　CRL の発行および公開を行うこと
(4)　証明書に記載される情報と、申請にあった情報とが一致していること
(5)　本 CPS に従ったシステムの監視および運用を行うこと

９．６．２　登録局の表明および保証

日本 RA は、本認証局を構成する登録局として登録局の業務の遂行にあたり、以下の義務を負うことを表明し保証する。

(1)　本 CPS および関連諸規定を遵守すること
(2)　発行局への証明書発行および失効の正確な指示を行うこと
(3)　証明書の発行を申請者に正しく通知し、または発行された証明書を正しく配付すること
(4)　本項に規定された登録局の義務、債務の不履行により発生した事態に対し、合理的な範囲で対処すること

９．６．３　利用者の表明および保証

利用者は、以下の義務を負うことを表明し保証する。

(1)　本 CPS および関連諸規定を遵守すること

(2)　本 CPS １．５　で規定された証明書用途を遵守すること

(3)　利用申請にあたり申請者が本認証局に提供する情報が正確であること

(4)　秘密鍵、パスワードについて、紛失、改変、第三者による使用・複製等が行われない様、十分な注意をもって厳重に管理すること

(5)　本 CPS ４．８．１　に示す内容に変更があるとき、本 CPS４．９．３　に従い、遅滞なく失効申請を行うこと

(6)　有効期間が満了した証明書および失効された証明書を使用しないこと

(7)　配付された証明書を許可された情報機器のみにインストールすること

９．６．４　信頼当事者の表明および保証

信頼当事者は、以下の義務を負うことを表明し保証する。

(1)　本 CPS １．５　で規定された証明書用途を遵守すること。

(2)　証明書の有効性の確認等により、証明書を信頼するか否かを判断すること。

(3)　本認証局が発行した証明書の有効期間と記載事項の確認を行うこと

(4)　CRL による失効登録の有無の確認を行うこと

(5)　本項に規定された義務の不履行により発生した事態に対し責任を負うこと

９．６．５　他の関係者の表明および保証

規定しない。

９．７　無保証

本認証局は、本 CPS９．６．１　、９．６．２　に定める保証に関連して発生する直接損害以外の損害については、本 CPS に基づく債務不履行に関していかなる責任も負わない。

９．８　責任制限

９．８．１　利用者の義務違反

本認証局は、利用者が本 CPS ９．６．３に違反したことに起因して生じた損害について、本認証局は、関係者に対し一切の責任を負わない。

利用者が本 CPS９．６．３　に述べる責任・義務に違反していることが明らかな場合、本認証局は利用者への事前の通知を行うことなく、利用者に対して発行した証明書を失効させることができるものとし、これに対し利用者は一切の請求、異議申し立てを行うことができない。

９．８．２　信頼当事者の義務違反

本認証局は、信頼当事者が本 CPS ９．６．４に違反したことに起因して生じた損害について、関係者に対し一切の責任を負わない。

９．８．３　不可抗力等

(1)　証明書や CRL の取得、利用等により利用者もしくは信頼者等のコンピュータシステム等に合理的な管理を超える状況により何らかの影響、障害が生じても、その責任を一切負わない。

(2)　利用者からの失効申請に伴う本認証局内での失効処理が、正当な事由により遅延した場合、これにより発生した損害については、損害賠償責任を一切負わない。

(3)　本認証局の廃止に伴う事前通知を実施し、廃止以降に発生した損害については、損害賠償責任を一切負わない。

(4)　次に掲げる事象または状況によって利用者、その他第三者（信頼者を含むがこれに限らない）に損害が生じた場合でも、その責任を一切負わない。

（ア）　天災：火災、雷、噴火、洪水、地震、嵐、台風、津波等

（イ）　人災：戦争、革命、暴動、内乱、労働争議等

（ウ）　裁判所、政府、行政、省庁等による作為、不作為、命令等

（エ）　電源の供給停止、回線の停止等、本認証局以外のシステムの停止

（オ）　技術上もしくは運用上緊急に本認証局に係るシステムを停止する必要があると本認証局が判断した場合

（カ）　本認証局が、本 CPS に基づく義務を適切に履行したにも関わらず、不完全履行もしくは履行遅滞を生じさせ、かかる結果に至ることとなった事象または状況

（キ）　その他本認証局の責に帰すべからざる事由

９．８．４　賠償

本認証局は、本 CPS に規定された責任を果たさなかったことに起因して、利用者または信頼当事者に対して損害を与えた場合の賠償については、別途定める。

ただし、本認証局側の責に帰さない事由から発生した損害、逸失利益、間接損害、または予見の有無を問わず特別損害、本利用者証明書を提供する際に用いる暗号アルゴリズムの退化による損害、コンピュータが用いられた不測の攻撃による損害およびデータの喪失については、いかなる場合でも一切の責任を負わない。また、本認証局は、本認証局の発行する証明書の不適切な使用に起因して発生した各種損害に対して、利用者、その他第三者（信頼当事者を含むがこれに限らない）に対し、一切の責任を負わない。

９．９　補償

利用者、信頼者の行為に起因して、第三者に損害が生じた場合、本認証局は免責されるものとし、利用者または信頼者は、損害賠償の責めを負う。

９．１０　文書の有効期間と終了

９．１０．１　文書の有効期間

本 CPS は、本 CPS 発効日より有効となる。本 CPS　９．１０．２　で記載する本 CPS の終了以前に本 CPS が無効となることはない。

９．１０．２　終了

本 CPS は、本 CPS ９．１０．３　に掲げる存続条項を除き、本認証局が業務を終了した時点で無効となる。

９．１０．３　終了の影響と存続条項

本 CPS ９．４　、９．５　、９．６　、９．７　、９．８　、９．９　、９．１０．２　９．１０．３　、９．１３　、９．１４　、９．１６　の規定については本 CPS の終了後も、存続するものとする。

９．１１　個々の関係者間に対する通知と連絡

本認証局から利用者に対し個別の通知が必要となった場合、適切な手段をもって行う。

９．１２　改訂

９．１２．１　改訂手続き

本認証局は、認証局責任者の指示に基づき、適宜、本 CPS の改訂を行うことができる。認証局員の評価、または弁護士等外部の専門家または有識者の評価を得た後、認証局責任者が改訂の承認を行う。

９．１２．２　通知方法と期間

本 CPS の内容に変更があった場合は、利用者に対して適宜通知する。

９．１２．３　オブジェクト識別子の変更理由

規定しない。

９．１３　紛争解決手続き

本 CPS に基づく認証業務から生じる紛争については、東京地方裁判所を第一審の専属管轄裁判所とする。

９．１４　準拠法

本 CPS に基づく認証業務から生じる紛争については、日本国の法令を適用する。

９．１５　適用される準拠法

規定しない。

９．１６　その他の条項

９．１６．１　完全合意

本 CPS における合意事項は、特段の定めをしている場合を除き、本 CPS が改訂または終了されない限り、他のすべての合意事項より優先される。

９．１６．２　譲渡

本認証局は、登録局業務において、第三者への譲渡を認めない。

９．１６．３　分離可能性

本 CPS 中のある規定が、何らかの理由により、無効または執行不可能であるとされた場合においても、残余の規定は有効であり、当事者の意思に最も合理的に合致するよう解釈する。

責任制限、保証、免責、または損害の排除等について規定する本 CPS の各条項は、他の規定とは分離し、また、その条項に従って執行可能であることにつき当事者は合意するものとする。

９．１６．４　執行（弁護士費用と権利の放棄）

規定しない。

９．１６．５　事務

規定しない。

９．１６．６　改廃

附則

本 CPS は、2011 年 10 月 1 日から施行する。

１０．　用語集

あ行

- アーカイブ（Archive）
  証明書の発行履歴、失効履歴等を必要に応じて閲覧可能な状態にて長期間保管すること。

- アクセス制御（Access Control）
  ユーザの権限に応じた制御を行う方法。データへのアクセスについて、閲覧が許可されている人に限りアクセスできるように物理的、電子的な手法で制御すること。

- アルゴリズム（Algorithm）
  ここにおいては、暗号化アルゴリズムをさす。暗号化アルゴリズムは、情報に対して一連の変換を施して情報を第三者に理解困難な形式にするための数学的に表現した規則の集まりを指す。

- 暗号モジュール（Cryptographic Module）
  暗号鍵等の生成、保管、利用などにおいて、セキュリティを確保する目的で使用されるソフトウェア、ハードウェアあるいはそれらを組み合わせた装置。

- 一時失効（Suspension）
  証明書の有効期間中に証明書を一時的に無効な状態にすること。

か行

- 鍵ペア（Key Pair）
  公開鍵暗号方式における公開鍵およびそれに対応する秘密鍵。２つの鍵は、一方の鍵から他方の鍵を導き出せない性質を持つ。

- 鍵長（Key Length）
  鍵の長さをビット数で表したもの。暗号の強度を決定する要素の１つ。一般に鍵長が長いほど解読がされにくいとされる。

- 鍵の預託（Key Escrow）
  秘密鍵または公開鍵を第三者機関に登録保管すること。

- 活性化（Activation）
  システムや装置等を使用可能な状態にすること。

- 活性化情報（Activation Data）
  システムや装置等を活性化するために必要となるデータ。具体的には、PIN コードやパスフレーズ等を指す。

- 危殆化（Compromise）
  秘密鍵や関連秘密情報等の秘密性が、盗難や漏洩、第三者による解読等によって失われた、もしくは失われた可能性のある事態の発生をいう。認証局の秘密鍵が危殆化した場合、当該認証局から発行された全ての証明書の信頼性が失われる。

- 公開鍵（Public Key）
  公開鍵暗号方式における鍵ペアのうちの一つで、通信相手等の他人に知らせて利用してもらうための鍵。

- 公開鍵暗号方式（Public Key Cryptographic Algorithm）
  関連した２つの鍵（公開鍵と秘密鍵）を使用する非対称暗号方式(asymmetric cryptographic algorithm)の１つであり、一方の鍵（公開鍵）で暗号化したデータは、他方の鍵（秘密鍵）でのみ復号できるようになっている。

さ行

- 自己署名証明書（Self-signed Certificate）
  認証局が、自己を証明するために発行する証明書。証明書に記載される証明書発行主体（Issuer）と被発行者（Subscriber）とが同一になっている。本 CPS ではルート認証局証明書と記載している。

- 失効（Revocation）
  証明書の有効期間内に、秘密鍵が危殆化もしくはその可能性が発生した場合、証明書の記載内容に変更が生じた場合等において、証明書を無効にすること。

- 失効リスト（Certificate Revocation List = CRL）
  失効した証明書のリスト。失効リストには、証明書を発行した認証局による電子署名が付される。

- 証明書（Certificate）
  認証対象者の識別情報と公開鍵とが対応していることを証明する電子文書。認証対象者の識別情報、その公開鍵、鍵の利用目的・範囲、発行認証局名などが含む一連の情報に、認証局の電子署名を付加したもの。

- 証明書ポリシー（Certificate Policy = CP）
  認証局が証明書を発行する際の運用方針を定めた文書。

- 信頼当事者（Relying Party）
  証明書を受け取って、それを信頼して行動する者。

た行

- タイムスタンプ(Time Stamp)
  信頼できる時刻管理機器によって管理される時刻を基に、ログ等に記録される事象の発生時刻を示す値。

- 中間認証局（Intermediate Certificate Authority）
  上位の認証局による認証を受けることにより、自らの正当性を認証する認証局。本 CPS において、利用者の証明書を発行する機関である。

- 登録局（Registration Authority = RA）
  証明書の発行や失効のプロセスにおいて、本人性確認や認証局システムへのデータ登録等の一部機能を認証局の承認を受けて行う組織。登録局は、証明書および失効リストの生成は行わない。

- 電子署名（Electronic Signature）
  間違いなく本人であることを証明する電子的なデータで、広義ではアナログ署名を電子データにしたものも含まれるが、ここでは、デジタル署名(digital signature)の意味で用いる。具体的には、署名対象データのハッシュ値に対して、秘密鍵で暗号化したもの。電子署名の検証は､電子署名を公開鍵で復号した値と元のデータのハッシュ値とを照合することで可能となる。

な行

- 認証局（Certification Authority = CA）
  証明書の発行、失効、失効リストの開示等のサービスを行う信頼された組織。

- 認証局運用規程（Certification Practice Statement = CPS）
  認証局の信頼性、安全性を対外的に示すために、認証局の運用規則、鍵の生成・管理、遵守事項等を文書化したもの。利用者・信頼者等の認証局の外部者に開示されるもの。

は行

- 発行局（Issuing Authority = IA）
  登録局において審査・承認され、送信される証明書の発行指示に対し、電子署名を行い、電子証明書を発行する機関。

- 秘密鍵（Private Key）
  公開鍵暗号方式における鍵ペアのうちの一つで、他人には知られないように秘密にしておく鍵。

- ハッシュ関数（Hash Function）
  データを数学的な操作によって一定の長さに縮小させる関数であり、異なる２つの入力値から同じ出力値を算出することが困難な関数。出力値から入力値を逆算することは不可能。

- ハッシュ値（Hash Value）
  ある値に対するハッシュ関数の出力値。「ハッシュ関数」参照。

- 秘密鍵管理モジュール（Hardware Security Module = HSM）
  暗号モジュールのうちハードウェアにより秘密鍵を安全に管理する装置。主に認証局で使用され、耐タンパ性をもち安全な秘密鍵管理機能を備えた暗号モジュールのこと。「暗号モジュール」参照。

- フィンガープリント（Finger Print）
  自己署名証明書などの証明書が改ざんされていないことを証明するためのデータ（ハッシュ値）のことをいう。その証明書が唯一無二であることを証明できることから、拇印と呼ばれている。SHA-2 ハッシュ関数）により算出したフィンガープリントは、40 桁の 16 進数であり、「0」～「9」及び「A」～「F」の文字の組合せで示される。ただし、フィンガープリントを表示するソフトウェアの種類又はバージョンにより、大文字又は小文字の相違、「:」又は「 」（スペース）の付加等表示方法が異なることがある。

- 複数人管理（Dual Control）
  秘密情報へのアクセス､システム運用・操作等における不正行為を防止する為に、複数の人間に管理機能を分散させ、全員がそれぞれの管理機能を遂行してはじめて所定の機能が働くようにする作業方式または管理方式。

- プロファイル（Profile）
  証明書（自己署名証明書、利用者用証明書）、失効リスト（CRL）等の設定情報のこと。

- ポリシー承認局(Policy Authority = PA)
  本認証局のポリシーの決定や CPS（本 CPS）の承認等を行う、本認証局における意思決定機関。

- 本人性確認（Identification and Authentication）
  個人や機器等の認証対象に関する情報が、本人（本体）のものであることを審査する行為。

ま行

ら行

- ルート認証局（Root Certificate Authority）
  上位の認証局による認証を受けず、自ら正当性を証明する最上位の認証局。自らを認証するルート証明書を発行し、ルート証明書の信頼性は、厳格な監査を受けることや、CPS を公開することなどで示される。

- リポジトリ（Repository）
  証明書や失効リスト、CPS 等を保管し、証明書利用者等に対してこれらの開示等のサービスを提供するシステム。

- 利用者（Subscriber）
  本認証局への申請主体である個人もしくは機器等であり、実際に証明書を利用する者を指す。

- ログ（Log）
  コンピュータの利用状況や通信の記録。操作やデータの送受信等が行われた日時と、操作者、操作内容、通信内容等が記録される。

Ａ－Ｇ

- CA（Certification Authority）
  「認証局」参照。

- CN（Common Name）
  ITU-T（国際電気通信連合－Ｔ）が策定した X.500 勧告において定められた、識別名（Distinguished Name）の中のひとつの属性。通常、一般的な名称（対象が人であれば人名）を表す。

- CP（Certificate Policy）
  「証明書ポリシー」参照。

- CPS（Certification Practices Statement）
  「認証局運用規定」参照。

- CRL（Certificate Revocation List）
  「失効リスト」参照。

- DN（Distinguished Name）
  ITU-T（国際電気通信連合－Ｔ）が策定したX.500 勧告において定められた識別名。C（Country Name = 国名）、O（Organization Name = 組織名）、OU（Organization Unit Name = 組織部局名）、CN（Common Name = 一般名）等の属性で構成される。

- FIPS 140-1（Federal Information Processing Standard 140-1）
  FIPS は商務省連邦情報処理規格を指し、140-1は暗号モジュール用セキュリティ要件を規定している。暗号モジュールは、セキュリティレベルという段階基準があり、どの要件に適合するかにより、最低レベル1 から最高レベル4 のいずれかに当てはめられる。

Ｈ－Ｎ

- HSM（Hardware Security Module）
  「秘密鍵管理モジュール」参照。

- IETF（Internet Engineering Task Force）
  インターネットで利用される技術を標準化する組織。インターネットの標準化を統括するIABの下部機関。ここで策定された技術仕様はRFCとして公表される。

- IPSec（Security Architecture for IP）
  IPパケットの暗号化と認証を行う、TCP/IP環境で汎用的に用いることができるネットワーク層で動作するセキュリティ技術。IETFにより標準化され、フレーム構成、データの暗号化や受信パケットの改ざんチェックなど、暗号通信の基本部分が規定されている。IPSec通信を行う相手との鍵交換方式には、IKE（Internet KeyExchange）が使用される。

- ISO(International Organization for Standardization)
  国際標準化機構。電気分野を除くあらゆる分野において、国際的に通用する規格・標準類の制定を目的としている。

- ITU（International Telecommunication Union）
  国際連合(UN)の専門機関の１つである国際電気通信連合。電気通信の改善、合理的利用を目的としている。

- ITU-T(International Telecommunication Union - Telecommunication Standardization Sector)
  国際電気通信連合の電気通信標準化部門。

- LDAP (Lightweight Directory Access Protocol)
  インターネット、イントラネット等の TCP/IP ネットワークで、ディレクトリデータベースにアクセスするためのプロトコル。

O－U

- OCSP (Online Certificate Status Protocol)
  証明書のステータス(失効・一時停止していないかどうか)をオンラインで問い合わせるプロトコル。OCSP クライアントと OCSP レスポンダ（サーバ）との間の通信方法について取り決めている。OCSP クライアントは、OCSP レスポンダに対して、対象となる証明書のシリアル番号を、電子署名付きで送信する。
  OCSP レスポンダは、問い合わせのあった証明書の状態を電子署名付きで返答する。

- OID (Object Identification：オブジェクト識別子)
  世界で一意となる値を登録機関（ISO、ITU）に登録した識別子。暗号アルゴリズムや証明書内に格納する名前（subject）のタイプ（Country 名等の属性）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。

- PIN (Personal Identification Number)
  個人識別番号のこと。本認証局においては、利用者の秘密鍵を活性化するための PIN 及び利用者に配付する IC カードの活性化用に用いる IC カード PIN がこれに該当する。

- PKI (Public Key Infrastructure)
  公開鍵暗号方式を用いて情報システム、コミュニケーションシステムのセキュリティを確保するための一連の技術及びサービス。

- RA (Registration Authority)
  「登録局」参照。

- RFC3647 (Request For Comments 3647)
  RFC とは、インターネットに関する標準文書の総称。その１つである RFC3647 は、CP もしくは CPS を作成するためのフレームワーク及びガイドラインを提供している。

- RSA

  Rivest、Shamir、Adelman の 3 人が開発した公開鍵暗号方式の一つ。

- SHA-2 (Secure Hash Algorithm -2)

  電子署名等に使われるハッシュ関数のひとつ。原文から 256 ビットの疑似乱数（ハッシュ値）を発生し、通信経路の両端で比較することで、通信途中で原文が改ざんされていないかを検出することができる。不可逆な一方向関数を含むため、ハッシュ値から原文を再現することはできず、また同じハッシュ値を生成する別のメッセージを作成することは極めて困難である。

- SSL (Secure Socket Layer)

  ネットワーク上の、２つのアプリケーション間の相互認証、通信の暗号化を行うプロトコル。米 Netscape 社が開発した。HTTP、SMTP、POP3 等のアプリケーション層のプロトコルと組み合わせて用いる（それぞれ HTTPS、SSMTP、SPOP3 と呼ぶ）。認証、暗号化に使う方法は通信の両端で打ち合わせて決めるようになっており、一般には、RSA、MD5、DES 等を用いている。

Ｖ－Ｚ

- X.500

  X.500 シリーズは、ITU-T で 1988 年に規格化されたディレクトリ・サービスの勧告（国際標準）であり 1997 年に新しい仕様が加えられている。この仕様には、ディレクトリの概念やその階層構造、サービスやオブジェクトの定義などが含まれる。

- X.509

  ITU-T が定めた、証明書に関する規格。バージョンが 1，2，3 とある。本認証局が発行する証明書はバージョン 3 を用いており、CRL はバージョン 2 を用いている。

- X.509v3

  証明書に関する ITU-T 規格のバージョン 3。既にエクステンション（拡張領域）を含むか、含むことが可能な証明書のこと。

- X.509v3 key usage

  証明書エクステンションの一つで、鍵が利用される目的を設定する項目のこと。電子署名、否認防止等の鍵利用目的がある。

１１．　証明書プロファイル

１１．１　ルート認証局証明書

(1)証明書基本領域(Basic)

Version		**値**
Version	電子証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
serialNumber		**値**
CertificateSerialNumber	電子証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号
Signature		**値**
AlgorithmIdentifier	電子証明書への署名に使用された署名アルゴリズムの識別子 （公開鍵暗号とハッシュ関数）	
Algorithm	署名アルゴリズムのオブジェクト ID 型：OID 値：≪署名アルゴリズム≫	 1.2.840.113549.1.1.11(SHA256withRSA)
Parameters	署名アルゴリズムの引数 型：NULL 値：	 NULL
Issuer		**値**
CountryName	電子証明書発行者の国名	
Type	国名のオブジェクト ID 型：OID 値：２５４６	 2.5.4.6
Value	国名の値 型：PrintableString 値：JP	 JP
OrganizationName	電子証明書発行者の組織名	
Type	組織名のオブジェクト ID 型：OID 値：２５４10	 2.5.4.10

Value	組織名の値	
	型：PrintableString	
	値：<<名称>>	Nippon RA Inc.
CommonName	電子証明書発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString	
	値：<<Root 認証局名称>>	Nippon RA Root Certification Authority
Validity		**値**
Validity	電子証明書の有効期間	20 年
notBefore	開始日時	
	型：UTCTime	＊有効開始日時（例）
	値：yymmddhhmmssZ	yymmddhhmmss
notAfter	終了日時	
	型：UTCTime	＊有効終了日時（例）
	値：yymmddhhmmssZ	yymmddhhmmss
Subject		**値**
CountryName	電子証明書発行者の国名	
Type	国名のオブジェクト ID	
	型：OID	
	値：2 5 4 6	2.5.4.6
Value	国名の値	
	型：PrintableString	
	値：JP	JP
OrganizationName	電子証明書発行者の組織名	
Type	組織名のオブジェクト ID	
	型：OID	
	値：2 5 4 10	2.5.4.10
Value	組織名の値	
	型：PrintableString	
	値：<<名称>>	Nippon RA Inc.
CommonName	電子証明書発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	

	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString	
	値：<<Root 認証局名称>>	Nippon RA Root Certification Authority
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	電子認証書発行者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）	
Algorithm	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY)	
	型：OID	
	値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	署名アルゴリズムの引数	
	型：NULL	NULL
	値：	
subjectPublicKey	公開鍵値	
	型：BIT STRING	
	値：公開鍵値	2048Bit

(2) 証明書標準拡張領域(extensions)

basicConstraints (extnId ::= 2 5 29 19, critical ::= TRUE)		**値**
BasicConstraints	基本的制限	
cA	CA かどうかを示すフラグ	
	型：Boolean	
	値：True（CA である）	TRUE
subjectKeyIdentifier (extnId ::= 2 5 29 14, critical ::= FALSE)		**値**
SubjectKeyIdentifier	電子証明書発行者の公開鍵に関する情報	
keyIdentifier	公開鍵の識別子	
	型：OCTET STRING	
	値:発行者の subjectPublicKey の Hash 値	
keyUsage （extnId ::= 2 5 29 15, critical ::= TRUE)		**値**
KeyUsage	鍵の使用目的	
	型：BitString	
	値：11000110	11000110
	(digitalSignature,NonRepudiation,	

	CertificateSigning,CRLSigning)	

１１．２　認証局証明書

(1)証明書基本領域(Basic)

Version		**値**
Version	電子証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
serialNumber		**値**
CertificateSerialNumber	電子証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号
Signature		**値**
AlgorithmIdentifier Algorithm Parameters 	電子証明書への署名に使用された署名アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 署名アルゴリズムのオブジェクト ID 型：OID 値：≪署名アルゴリズム≫ 署名アルゴリズムの引数 型：NULL 値：	 1.2.840.113549.1.1.11(SHA256withRSA) NULL
Issuer		**値**
CountryName Type Value 	電子証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6 国名の値 型：PrintableString 値：JP	 2.5.4.6 JP
OrganizationName Type 	電子証明書発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10	 2.5.4.10

Value	組織名の値	
	型：PrintableString	
	値：<<名称>>	Nippon RA Inc.
CommonName	電子証明書発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString	
	値：<<Root 認証局名称>>	Nippon RA Root Certification Authority
Validity		**値**
Validity	電子証明書の有効期間	
notBefore	開始日時	ユーザ証明書有効期間＋5 年 1 ヶ月
	型：UTCTime	＊有効開始日時（例）
	値：yymmddhhmmssZ	yymmddhhmmss
notAfter	終了日時	
	型：UTCTime	＊有効終了日時（例）
	値：yymmddhhmmssZ	yymmddhhmmss
Subject		**値**
CountryName	電子証明書発行者の国名	
Type	国名のオブジェクト ID	
	型：OID	
	値：2 5 4 6	2.5.4.6
Value	国名の値	
	型：PrintableString	
	値：JP	JP
OrganizationName	電子証明書発行者の組織名	
Type	組織名のオブジェクト ID	
	型：OID	
	値：2 5 4 10	2.5.4.10
Value	組織名の値	
	型：PrintableString	
	値：<<名称>>	Nippon RA Inc.
CommonName	電子証明書発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	

	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString	
	値：<<証明書発行局名称>>	Nippon RA Certification Authority 1 ～ 4
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	電子認証書発行者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）	
Algorithm	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY)	
	型：OID	
	値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	署名アルゴリズムの引数	
	型：NULL	NULL
	値：	
subjectPublicKey	公開鍵値	
	型：BIT STRING	
	値：公開鍵値	2048Bit

(2) 証明書標準拡張領域(extensions)

basicConstraints (extnId ::== 2 5 29 19，critical ::== TRUE)		**値**
BasicConstraints	基本的制限	
cA	CA かどうかを示すフラグ	
	型：Boolean	
	値：True（CA である）	TRUE
authorityKeyIdentifier (extnId ::== 2 5 29 35，critical ::== FALSE)		**値**
AuthorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報	
keyIdentifier	公開鍵の識別子	
	型：OCTET STRING	
	値：Root 認証局の subjectPublicKey の Hash 値	
subjectKeyIdentifier (extnId ::== 2 5 29 14，critical ::== FALSE)		**値**
SubjectKeyIdentifier	電子証明書発行者の公開鍵に関する情報	
keyIdentifier	公開鍵の識別子	
	型：OCTET STRING	

	値：Root 認証局の subjectPublicKey の Hash 値	
keyUsage （extnId ::= 2 5 29 15，critical ::= TRUE）		**値**
KeyUsage	鍵の使用目的 型：BitString 値：11000110 (digitalSignature,NonRepudiation, CertificateSigning,CRLSigning)	11000110
cRLDistributionPoints (extnId ::= 2 5 29 31，critical ::= FALSE)		**値**
cRLDistributionPoints DistributionPoint fullName	CRL 配付ポイント CRL 配付ポイント CRL を配付する URI 型：IA5 String 値：http URI (ldap URI)	*CRL が配布される URI http://mpkicrl.managedpki.ne.jp/mpki/NipponRARootCertificationAuthority

１１．３　証明書失効リスト

(1)CRL 標準領域(Basic)

Version		**値**
Version	フォーマットのバージョン番号 型：INTEGER 値：1	1 (Ver.2)
Signature		**値**
AlgorithmIdentifier Algorithm	証明書失効リストへの署名に使用された署名アルゴリズムの識別子（公開鍵暗号とハッシュ関数） 署名アルゴリズムのオブジェクト ID 型：OID 値：≪署名アルゴリズ	1.2.840.113549.1.1.5(SHA-256withRSA)

	ム≫	
Parameters	署名アルゴリズムの引数	
	型：NULL	NULL
	値：	
Issuer		**値**
CountryName	証明書失効リスト発行者の国名	
Type	国名のオブジェクト ID	
	型：OID	
	値：2 5 4 6	2.5.4.6
Value	国名の値	
	型：PrintableString	
	値：JP	JP
OrganizationName	証明書失効リスト発行者の組織名	
Type	組織名のオブジェクト ID	
	型：OID	
	値：2 5 4 10	2.5.4.10
Value	組織名の値	
	型：PrintableString or UTF8String	
	値：<<名称>>	Nippon RA Inc.
CommonName	証明書失効リスト発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString or UTF8String	
	値：<<発行局名称>>	Nippon RA Certification Authority 1 ～ 4
thisUpdate		**値**
thisUpdate	有効開始日	
	型：UTCTime	＊有効開始日時
	値：yymmddhhmmss	例 yymmddhhmmss

nextUpdate		**値**
nextUpdate	次回更新予定日時 型：UTCTime 値：yymmddhhmmss	有効開始日から 10 日間後 ＊更新予定日時 例 yymmddhhmmss

(2) CRL 標準拡張領域(extensions)

authorityKeyIdentifier (extnId ::= 2 5 29 35，critical ::= FALSE)		**値**
AuthorityKeyIdentifier keyIdentifier	証明書失効リスト発行者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値:認証局の subjectPublicKey の Hash 値	*認証局の subjectPublicKey の Hash 値
cRLNumber (extnId ::= 2 5 29 20，critical ::= FALSE)		**値**
cRLNumber	CRL の番号 型：INTEGER 値：ユニークな整数	＊CRL の番号

(3) CRL エントリ領域

revokedCertificates		**値**
CertificateSerialNumber	証明書失効リストのシリアル番号 型：INTEGER 値：ユニークな整数	＊シリアル番号
revocationDate	失効日時 型：UTCTime 値：yymmddhhmmss	

(4) CRL エントリ拡張領域

invalidityDate (extnId ::= 2 5 29 24，critical ::= FALSE)		**値**
invalidityDate	無効化日時 型：UTCTime 値：yymmddhhmmss	
cRLReason (extnId ::= 2 5 29 21，critical ::= FALSE)		**値**
cRLReason	失効理由コード	(1) keyCompromise (2) cACompromise (3) affiliationChanged

		(4) superseded (5) cessationOfOperation *unspecified は、cRLReason として出力しない。

１１．４　利用者証明書

１１．４．１　（利用者証明書）

(1) 証明書基本領域(Basic)

Version		**値**
Version	電子証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
serialNumber		**値**
CertificateSerialNumber	電子証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号
Signature		**値**
AlgorithmIdentifier Algorithm Parameters	電子証明書への署名に使用された署名アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 署名アルゴリズムのオブジェクト ID 型：OID 値：≪署名アルゴリズム≫ 署名アルゴリズムの引数 型：NULL 値：	 1.2.840.113549.1.1.5(SHA-256withRSA) NULL
Issuer		**値**
CountryName Type	電子証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6	 2.5.4.6

Value	国名の値	
	型：PrintableString	
	値：JP	JP
OrganizationName	電子証明書発行者の組織名	
Type	組織名のオブジェクト ID	
	型：OID	
	値：2 5 4 10	2.5.4.10
Value	組織名の値	
	型：PrintableString	
	値：<<会社名称>>	Nippon RA Inc.
CommonName	電子証明書発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString	
	値：<<発行局名称>>	Nippon RA Certification Authority 1 ～ 4
Validity		**値**
Validity	電子証明書の有効期間	
notBefore	開始日時	有効期間：1 年～5 年 1 ヵ月
	型：UTCTime	＊有効開始日時
	値：yymmddhhmmssZ	例 yymmddhhmmss
notAfter	終了日時	
	型：UTCTime	＊有効終了日時
	値：yymmddhhmmssZ	例 yymmddhhmmss
Subject		**値**
CountryName	電子証明所有者の国名	
Type	国名のオブジェクト ID	
	型：OID	
	値：2 5 4 6	2.5.4.6
Value	国名の値	
	型：PrintableString	
	値：JP	JP　*固定
OrganizationName	電子証明書所有者の組織名	
Type	組織名のオブジェクト ID	

	型：OID	
	値：2 5 4 10	2.5.4.10
Value	組織名の値	
	型：PrintableString or UTF8String	
	値：<<加入者の会社名称>>	利用法人名称
OrganizationalUnitName	電子証明書所有者の部署名	
Type	部署名のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	部署名の値	
	型：PrintableString or UTF8String	
	値：<<利用者識別子>>	識別番号
CommonName	電子証明書所有者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString or UTF8String	
	値：<<利用者氏名>>	利用者氏名
EmailAddress	電子証明書所有者のメールアドレス	
Type	メールアドレスのオブジェクト ID	
	型：OID	
	値：1.2.840.113549.1.9.1	1.2.840.113549.1.9.1
Value	メールアドレスの値	
	型：IA5 String	
	値：<<利用者のメールアドレス>>	＊利用者のメールアドレス
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	電子証明書所有者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）	
Algorithm	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY)	
	型：OID	
	値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	署名アルゴリズムの引数	
	型：NULL	NULL

subjectPublicKey	値： 公開鍵値 型：BIT STRING 値：公開鍵値	 2048Bit

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (extnId ::= 2 5 29 35，critical ::= FALSE)		**値**
AuthorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値:認証局の subjectPublicKey の Hash 値	 *電子証明書発行者の証明書の subjectPublicKey の Hash 値
subjectKeyIdentifier (extnId ::= 2 5 29 14，critical ::= FALSE)		**値**
SubjectKeyIdentifier keyIdentifier	電子証明書所有者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値:所有者の subjectPublicKey の Hash 値	 *利用者証明書の subjectPublicKey の Hash 値
keyUsage　(extnId ::= 2 5 29 15，critical ::= FALSE)		**値**
KeyUsage	鍵の使用目的 型：BitString 値：101000000 (digitalSignature,keyEncipherment)	 101000000
cRLDistributionPoints (extnId ::= 2 5 29 31，critical ::= FALSE)		**値**
cRLDistributionPoints DistributionPoint fullName	CRL 配付ポイント CRL 配付ポイント CRL を配付する URI 型：IA5 String 値：http URI (ldap URI)	 *CRL が配布される URI http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority1 ～ 4/cdp.crl
extKeyUsage (extnId ::= 2 5 29 37，critical ::= FALSE)		**値**
extKeyUsage KeyPurposeId clientAuth	鍵の使用目的（拡張） 使用目的 ID クライアント認証利用	

	型：OID 値：1 3 6 1 5 5 7 3 2	 1.3.6.1.5.5.7.3.2 (clientAuth)

１１．４．２　（利用者証明書：SCL 利用）

(1) 証明書基本領域(Basic)

Version		**値**
Version	電子証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
serialNumber		**値**
CertificateSerialNumber	電子証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号
Signature		**値**
AlgorithmIdentifier Algorithm Parameters	電子証明書への署名に使用された署名アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 署名アルゴリズムのオブジェクト ID 型：OID 値：≪署名アルゴリズム≫ 署名アルゴリズムの引数 型：NULL 値：	 1.2.840.113549.1.1.5(SHA-256withRSA) NULL
Issuer		**値**
CountryName Type Value OrganizationName Type 	電子証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6 国名の値 型：PrintableString 値：JP 電子証明書発行者の組織名 組織名のオブジェクト ID 型：OID	 2.5.4.6 JP

	値：2 5 4 10	2.5.4.10
Value	組織名の値	
	型：PrintableString	
	値：<<会社名称>>	Nippon RA Inc.
CommonName	電子証明書発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString	
	値：<<発行局名称>>	Nippon RA Certification Authority 1 ～ 4
Validity		**値**
Validity	電子証明書の有効期間	
notBefore	開始日時	有効期間：3 年 1 ヵ月
	型：UTCTime	＊有効開始日時
	値：yymmddhhmmssZ	例 yymmddhhmmss
notAfter	終了日時	
	型：UTCTime	＊有効終了日時
	値：yymmddhhmmssZ	例 yymmddhhmmss
Subject		**値**
CountryName	電子証明所有者の国名	
Type	国名のオブジェクト ID	
	型：OID	
	値：2 5 4 6	2.5.4.6
Value	国名の値	
	型：PrintableString	
	値：JP	JP　*固定
OrganizationName	電子証明書所有者の組織名	
Type	組織名のオブジェクト ID	
	型：OID	
	値：2 5 4 10	2.5.4.10
Value	組織名の値	
	型：PrintableString or UTF8String	
	値：<<利用者の会社名称>>	利用法人名称
OrganizationalUnitName	電子証明書所有者の部署名	

Type	部署名のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	部署名の値	
	型：PrintableString or UTF8String	
	値：<<利用者識別子>>	識別番号
CommonName	電子証明書所有者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString or UTF8String	
	値：<<利用者氏名>>	利用者氏名
EmailAddress	電子証明書所有者のメールアドレス	
Type	メールアドレスのオブジェクト ID	
	型：OID	
	値：1.2.840.113549.1.9.1	1.2.840.113549.1.9.1
Value	メールアドレスの値	
	型：IA5 String	
	値：<<利用者のメールアドレス>>	＊利用者のメールアドレス
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	電子証明書所有者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）	
Algorithm	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY)	
	型：OID	
	値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	署名アルゴリズムの引数	
	型：NULL	NULL
	値：	
subjectPublicKey	公開鍵値	
	型：BIT STRING	
	値：公開鍵値	2048Bit

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (extnId ::= 2 5 29 35，critical ::= FALSE)		**値**
AuthorityKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値:認証局の subjectPublicKey の Hash 値	*電子証明書発行者の証明書の subjectPublicKey の Hash 値
subjectKeyIdentifier (extnId ::= 2 5 29 14，critical ::= FALSE)		**値**
SubjectKeyIdentifier keyIdentifier	電子証明書所有者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値:所有者の subjectPublicKey の Hash 値	*利用者証明書の subjectPublicKey の Hash 値
keyUsage （extnId ::= 2 5 29 15，critical ::= FALSE)		**値**
KeyUsage	鍵の使用目的 型：BitString 値：111000000 (digitalSignature,nonRepudiation, keyEncipherment)	111000000
cRLDistributionPoints (extnId ::= 2 5 29 31，critical ::= FALSE)		**値**
cRLDistributionPoints DistributionPoint fullName	CRL 配付ポイント CRL 配付ポイント CRL を配付する URI 型：OctetString 値：http URI (ldap URI)	*CRL が配布される URI http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority1 ～ 4/cdp.crl
subjectAltName （extnId ::= 2 5 29 17，critical ::= FALSE)		**値**
subjectAltName rfc822Name otherName userPrincipalName type-id	証明書所有者の別名 メールアドレスタイプ 型：IA5String 値：<<証明書所有者メールアドレス>> その他のタイプ UPN (Windows ログオンに使用する名称) オブジェクト ID 型：OID	証明書所有者メールアドレス

	値：1 3 6 1 4 1 311 20 2 3	1.3.6.4.1.311.20.2.3
Value	文字列値	
	型：UTF8String	
	値：<<ユーザプリンシパル名>>	ユーザプリンシパル名
extKeyUsage (extnId ::= 2 5 29 37，critical ::= FALSE)		**値**
extKeyUsage	鍵の使用目的（拡張）	
KeyPurposeId	使用目的 ID	
emailProtection	メール保護利用	
	型：OID	
	値：1 3 6 1 5 5 7 3 4	1.3.6.1.5.5.7.3.4 (emailProtection)
smartCardLogon	Windows スマートカードログオン利用	
	型：OID	
	値：1 3 6 1 4 1 311 20 2 2	1.3.6.1.4.1.311.20.2.2(smartCardLogon)
clientAuth	クライアント認証利用	
	型：OID	
	値：1 3 6 1 5 5 7 3 2	1.3.6.1.5.5.7.3.2 (clientAuth)