第5章 CP/CPS 策定に関する検討

内容

- CP/CPS 策定の方針
  - CP/CPS の検討
  - 本検討と RFC3647 について

5. CP/CPS 策定に関する検討

5.1. 本章の目的

本章は、認証局の証明書ポリシ及び運用実施規定である CP/CPS（Certificate Policy and Certification Practice Statement）の策定を目的とし、記述すべき項目及び IP アドレス認証局の業務に則した記述内容の検討を行うものである。

5.2. 概要

IP アドレス認証局のあり方に関する調査を 2002 年度に実施し、セキュリティを考慮した運用要件の検討を進めてきたわけであるが、今回の検討では、セキュリティ要件の他に運用体制等実際の運用を考慮し検討を行った。CP/CPS の記述内容の検討、考察については 5.4.節に記述している。

本報告書上、継続検討課題としている部分も存在する。過度なセキュリティ要求とならないように考慮して検討を進めたが、更にシステムの詳細等が明らかになった時点で、CP/CPS の改善を行っていくものとする。

作成された IP アドレス認証局の CP/CPS（ドラフト版）を Appendix.1 として本報告書に添付する。また一連の検討の過程で必要とされた JPNIC ルート認証局の CP/CPS（ドラフト版）を Appendix.2 として本報告書に添付する。どちらの文書も、公開のときに利用される URL などを含めて改定される可能性がある。

5.3. RFC3647 について

RFC2527 は多くの認証局の CP/CPS 作成時のフレームワークとして利用されてきたが、今般 2003 年 11 月に RFC2527 を引き継ぐ新しい CP/CPS フレームワークとして RFC3647 が公表された。本報告書のための検討を行った時点において、RFC3647 はまだ公表されていなかったため、本報告書 5.4.節においては、RFC2527 のフレームワークにて記述している。なお、RFC2527 と RFC3647 の相違点及び追加検討事項は本報告書 5.5.節で述べるものとする。

5.4. CP/CPS の検討

本節においては、認証局の CP/CPS のフレームワークである RFC2527 の項目にそって、検討すべき項目、検討内容等を記述していく。なお、本報告書 5.4.1.項から 5.4.8.項において記述されている見出しの前の［X］、［X.X］、［X.X.X］の括弧書きの数値は RFC2527 における章、節、項の番号を示している。

5.4.1. ［1］はじめに

5.4.1.1. ［1.1］概要

CP/CPS の 1.1 節では、JPNIC IP アドレス認証局（以下、本認証局と呼ぶ）がどのような認証局であるのか（主体者、発行する証明書等）に関して、その概要を記述することとなる。また、CP/CPS が準拠する文書又は関連する文書があれば、それら文書との関係を記述することとなる。

検討項目としては、次の項目があげられる。

- どこが誰に対して、どのような証明書を発行するのか
- 本 CP/CPS が準拠又は関連する文書には、何があるか
- CP と CPS とを分離して記述するか

（1） 主体者及び発行する証明書について

本認証局における証明書の発行主体は JPNIC となる。JPNIC が、レジストリシステムにおけるユーザ認証及びメッセージ認証の機能を実現するための証明書を、IP アドレス管理業務をする者に対して発行するものと考えられる。また、レジストリシステムにおいてユーザがサーバの認証をするために、JPNIC は当該サーバに対してサーバ証明書を発行するものと考えられる。

このほか、JPNIC は、本認証局の運用に必要な各種の運用用証明書[1]を発行するが、当該証明書は、JPNIC で別途定める運用規則に則り、厳格な手続きのもとに発行されることから、以降、本報告書においては詳細な記述はしないこととする。

（2） 本 CP/CPS が準拠又は関連する文書について

CP/CPS を策定するうえで最初に、CP と CPS を一体のものとして記述するか、独立したものとして記述するかの検討が必要である。独立したものと記述した場合には、CP/CPS の 1.1 節において CP と CPS の位置付け及び優先関係を規定する必要がある。CP と CPS とを分離して記述するかについては、後述する本報告書 5.4.1.1.（3）にて検討を行う。

CP/CPS の記述構成としては、RFC2527 に依拠することとするのが一般的であるが、2003 年 11 月に RFC2527 を引き継ぐ新しい CP/CPS フレームワークとして RFC3647

[1]本認証局の運用上、認証業務を担う各役割（認証局管理者、登録局管理者、セキュリティ管理者、ローカル登録局管理者等）を認証するために必要な証明書として、認証局管理者(CAO)証明書、登録局管理者(RAO)証明書、セキュリティ管理者証明書、ローカル登録局(LRA)管理者証明書等がある。これら、認証業務を担う各役割については本報告書 5.2. 手続管理にて述べる。

が正式にリリースされた。今後、策定される CP/CPS は RFC3647 に準拠するケースが増えると考えられ、現段階から RFC3647 準拠としておくことが望ましいと考えられる。ただし、本報告書 5.3.節にて述べたとおり、本報告書については RFC2527 のフレームワークにて記述している。

また、RFC2527 と RFC3647 は、相互にマッピング可能であるため、検討段階では RFC2527 のフレームワークに準拠するものの、最終的な CP/CPS は RFC3647 のフレームワークに準拠することが望まれる。

次に、WebTrust 基準[2]等、本認証局が準拠すべき基準があれば、本節に記述するのが一般的である。現段階では、本認証局は所定の基準に準拠することは予定しておらず、また、「電子署名及び認証業務に関する法律」における特定認証業務の認定の適用も想定していないが、将来的には何らかの基準への準拠が要求される可能性がある。したがって、以降各所の検討においては、各種の基準が示すレベルを参考にするものとし、現段階で準拠しなければならない基準については特定せず、CP/CPS の 1.1 節に記述しないものとする。

その他、関連する文書として、証明書所有者同意書、検証者同意書、その他の契約関連規程があるのであれば、これらとの関係を記述するのが一般的である。ここで、前述した規程のうち検証者同意書の必要性について、次に検討する。

本 CP/CPS は、JPNIC と IP アドレス管理指定事業者との間のレジストリ管理業務を適用対象としており、証明書を検証する者は、証明書を発行されている者と同一範囲に限定されると考える。したがって現段階では、証明書所有者同意書の中で検証者としての事項を併せて規定すれば、検証者同意書を別途規定する必要はないと考えられる。

前述のように、証明書所有者同意書が存在し、その他の契約関連規程がないものとすると、CP/CPS 及び証明書所有者同意書の関係を記述すればよいこととなる。本認証局においては、CP/CPS と証明書所有者同意書の内容に齟齬がある場合は、現段階では、証明書所有者同意書が優先して適用されるものとする。

（3） CP と CPS とを分離して記述するか

ここでは、JPNIC が発行する証明書に関わるポリシ（CP）並びに JPNIC が適用する認証業務規定（CPS）を一体として記述するか、独立（分離）して記述するかについて検討する。

CP と CPS を独立して記述する場合、CP と CPS はその目的は異なり、別々の観点から記述することができる。認証局の設備、システム及び運用等証明書をどのように

[2] WebTrust Program for Certification Authorities V1.0（2000 年 8 月 25 日）、AICPA/CICA

発行するのかについてはCPS に記述し、どのような証明書を発行するのかに関わる規則やプロファイルについてはCP に記述することになる。

一般的に、CP と CPS は、表裏一体の関係にあり、相補的なものと言われている。したがって、CP と CPS を一体化した場合においても、十分にその両方の機能を満たす記述ができること、また効率的な作成及び管理ができること、利用者にとっても理解しやすいこと等のメリットがある。特に、発行する証明書の種類が固定的であり、かつ証明書の適用範囲及び認証局の運用体制についても固定的である場合には、一体型での記述で問題がないと考えられる。

また、本認証局の場合は、次の特徴がある。

- 本認証局が発行する証明書は、種類がほぼ固定的であり、本認証局の認証業務及びシステムの変更又は拡張も、少ないと考えられる。
- JPNIC と IP アドレス管理指定事業者等との間における適用範囲が限定されたコミュニティでの運用であり、パブリックサービスの場合と比較して、CP/CPS の改訂があったとしても利用者に及ぼす影響が少ない。

前述から、本認証局の CP/CPS は、一体型としての記述が良いのではないかと考えられる。そこで、本報告書では、CP/CPS を一体型として記述するものとして、CP/CPS の各章・節・項の検討を行うこととする。

「1.1.概要」記述案

本 CP/CPS は、社団法人 日本ネットワークインフォメーションセンター（以下、JPNIC と呼ぶ）と IP アドレス管理指定事業者等との間における、IP アドレス及び AS 番号に関する各種管理業務に用いる証明書を発行する JPNIC IP アドレス認証局の認証業務に関する運用規則を定める。

JPNIC IP アドレス認証局は、本 CP/CPS に基づき、IP アドレス管理指定事業者に所属し、各種申請処理業務を行う者（以下、ホストマスタと呼ぶ）等に証明書を発行する。また、安全な通信を実現するため、レジストリシステムの各種サーバに対してサーバ証明書を発行する。

本 CP/CPS の構成は、IETF PKIX が提唱する RFC2527「証明書ポリシと認証実践の枠組み（Certificate Policy and Certification Practices Statement Framework）」に準拠している。

JPNIC IP アドレス認証局は、CP（証明書ポリシ）及び CPS（認証実施規程）をそれぞれ独立したものとして定めず、本 CP/CPS として証明書ポリシ及び運用規程を定めるものとする。

JPNIC は、本認証業務の提供にあたり、自らのポリシ、証明書所有者及び検証者の義務等を、本 CP/CPS、証明書所有者同意書によって包括的に定める。なお、本 CP/CPS と証明書所有者同意書の内容に齟齬がある場合は、証明書所有者同意書が優先して適用されるものとする。

本 CP/CPS は、証明書所有者及び検証者がいつでも閲覧できるように JPNIC のホームページ上（URI は決定後に記述される）に公開される。

(1)CP/CPS

CP/CPS は、証明書の目的、適用範囲、証明書プロファイル、本人認証方法及び証明書所有者の鍵管理並びに本認証業務に関わる一般的な規定を記述した文書である。本 CP/CPS は、必要に応じて証明書所有者同意書を参照する。

(2)証明書所有者同意書

証明書所有者同意書は、認証サービスの内容や証明書所有者の義務等、証明書所有者と JPNIC 間における、認証サービス利用上の諸規則を記述した文書である。

5.4.1.2. ［1.2］識別

CP/CPS の 1.2.節では、CP/CPS の正式名称及び証明書ポリシ（CP）のオブジェクト識別子（OID）を記述することとなる。これは、証明書拡張の CertificatePolicies 属性において、OID による制御を行う場合等に重要な意味を持つ。その他、CP の OID に限らず、関連する OID があれば本節に記述することとなる。

検討項目としては、次があげられる。

- 発行する証明書に割り当てられる OID について
- その他、関連する OID について

（1） 発行する証明書に割り当てられる OID

OID は、組織や文書等一つ一つのオブジェクトを区別するために、各オブジェクトに一意になるよう割り振られた識別子であり、階層構造で管理される。

本認証局の場合、証明書の発行組織である JPNIC の他、本 CP/CPS 並びに本 CP/CPS に基づいて発行される EE 証明書（ホストマスタ証明書及びサーバ証明書）のポリシに対して OID を割り当てることができる。本節では、このように割り当てた OID を列記するのが一般的である。

また、証明書拡張の CertificatePolicies 属性において、CP の OID を記述することで、その証明書がどの CP に基づいて発行されたかを示すことができる。証明書に CP の OID を含めるべきか否かであるが、OID を含める場合には、証明書の利用を OID

によってきめ細かに制御することが可能となる一方、検証アプリケーション側での実装が必要となるという問題がある。

本認証局の場合、証明書の利用に際し、次の特徴がある。

- 証明書の利用用途が主に SSL/TLS 及び S/MIME での利用と想定されていること。
- サーバ側では、識別名（DN：Distinguished Name）[3]によるアクセスコントロールが可能であること。
- 原則として、EE 間でのやり取りは発生しないとしていること。

前述から、本 CP/CPS に基づき発行される証明書内には、OID を含める必要性は必ずしもないと考えられる。

（2） その他、関連する OID

JPNIC 以外の主要なインターネットレジストリ（APNIC、RIPE NCC、ARIN 等）のうち、APNIC、RIPE NCC においては既に認証局運用に関するプロジェクトが開始しており、その他のインターネットレジストリにおいても、今後、レジストリシステムのセキュリティ確保のために認証局を構築する動きがでてくるものと思われる。その際、本認証局と、他の認証局との相互接続が検討され、本 CP/CPS にて相互認証証明書ポリシ等の OID を記述することになると考えられる。しかし当面、本認証局に APNIC 等との相互接続が予定されていないことから、現段階では、他の認証局に関連する OID の記述はせず、他の認証局との相互接続が決まった段階で、関連する OID の記述を検討するものとする。

「1.2.識別」記述案

本 CP/CPS の正式名称は「JPNIC IP アドレス認証局 認証業務規程」という。

JPNIC 及び JPNIC IP アドレス認証局に関連するオブジェクト識別子を､次に示す。

1.2.392.00200175　社団法人 日本ネットワークインフォメーションセンター

1.2.392.00200175.2.（OID は決定後に記述される） JPNIC IP アドレス認証局 認証業務規程（CP/CPS）

[3]識別名（DN：Distinguished Name）については、本報告書 5.4.3.1. 新規発行時での利用者の本人確認方法を参照のこと。

1.2.392.00200175.2.（OID は決定後に記述される） EE 証明書ポリシ

5.4.1.3. ［1.3］コミュニティと適用性

CP/CPS の 1.3 節では、証明書の利用目的、制限事項、利用環境、適用範囲、発行対象等を記述する。

CP/CPS 1.3 節の記述は、本認証局が発行する証明書をどのような目的で、どのような組織、人、物に対して流通させるのかという重要な要素を含んでいる。流通させる適用範囲が明確でないと、本人認証手段、証明書の検証手続きき等にも影響する。また、適用範囲、使用目的が明らかでないと、証明書に関する事故、訴訟への発展も危惧されるので十分な検討が必要と思われる。

検討項目としては、次があげられる。

- 証明書の流通するコミュニティ（組織、人、物）
- 証明書の適用範囲
- 証明書が適合する又は使用が制限されるアプリケーション
- 証明書の使用が禁止される用途
- 証明書の相互運用性

（1） 証明書の流通するコミュニティ（組織、人、物）

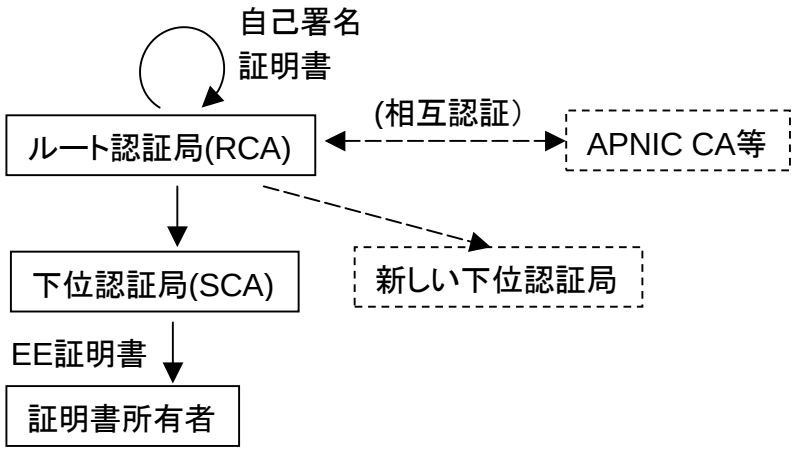
証明書の流通するコミュニティを検討する前に、本認証局を単独の認証局とするか、階層構造を持った複数の認証局の一部（下位認証局）とするかの検討が必要である。各々のメリット・デメリットを表 5-1 に示す。

表 5-1 認証局の構成比較

ケース	メリット	デメリット
単独型認証局	認証局構築・運用コストの低減が図ることができる。	システムの拡張性・応用性が制限される。他の認証局と接続する場合、要件により認証局を再構築する必要がある。
階層型認証局	新たな用途のための認証局追加が比較的容易、かつ既存の認証局に影響を与えない。また、ルート認証局の相互認証により、他との信頼関係の確立が容易となる。	複数の認証局を運営するための、運用負荷・コストが増加する。※ただし、製品の仕様及びライセンス体系に依存する。

本認証局の場合、当面、証明書の適用範囲として、レジストリシステムにおけるメ

ッセージ認証及びクライアント認証を想定しているが、将来的には、インターネットを通じて接続を受け付けるためのゲートウェイを認証する等、証明書の多面的な応用を検討している。その際、新しい用途の認証局を構築することが想定されるため、階層型認証局の構成を取っておくことが望ましいと考えられる（図 5-1)。この場合、新たに追加する下位認証局についてもルート認証局の認証を受けることで、互いの認証局ドメイン間での信頼関係確立が容易となる。また、APNIC CA 等との相互接続はルート認証局だけが行うことで、相互認証が可能となる。ただし、相互認証を行う場合には、相互認証証明書のプロファイルについて調整を行わなければならないと思われる。



RCA: Root Certification Authority, SCA: Subordinate Certification Authority

図 5-1　階層型認証局

次に、コミュニティを構成する認証局、EE 等の登場者の基本的な関係を図 5-2 に示す。JPNIC IP アドレス認証局は、登録局（RA)、発行局（IA）及びリポジトリから構成されるとして扱うのが一般的である。

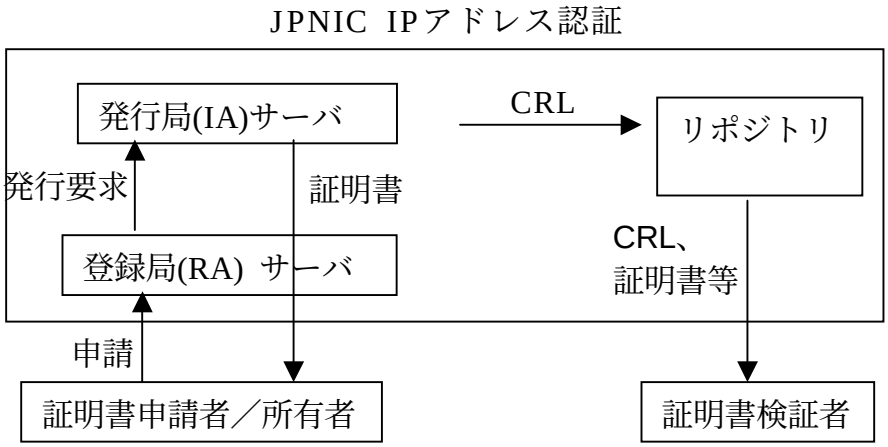


図 5-2　認証局、EE 等の登場者の関係

ここで、主たる証明書所有者は IP アドレス管理指定事業者に所属するホストマスタとなるが、JPNIC が個々のホストマスタに対して証明書の発行業務をすることは、人的業務量が膨大となり非現実的である。そこで、JPNIC は、JPNIC との契約において関連付けられた日本国内の IP アドレス管理指定事業者（以下、LRA[4]と呼ぶ）の管理者（以下、LRA 管理者と呼ぶ）のみを認証し、LRA 管理者が個々のホストマスタ個人を認証する仕組みとする（図 5-3）。

[4] LRA: Local Registration Authority

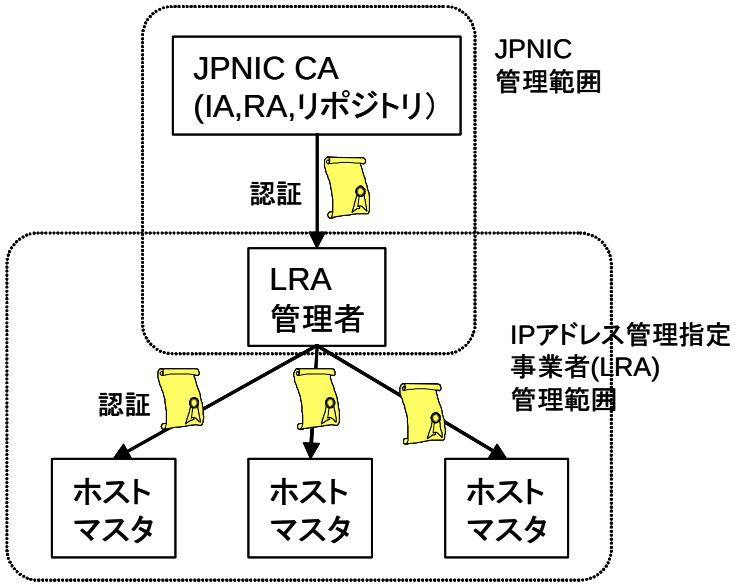


図 5-3　LRA による個人認証モデル

CP/CPS 1.3 節においては、前述したような、証明書の流通するコミュニティに関係する登場者と役割をまとめて記述するのが一般的である（表 5-2）。

表 5-2　コミュニティに関係する登場者と役割

登場者	略称	役割、説明
ホストマスタ		IP アドレス及び AS 番号の割当て・返却等のレジストリ業務を行う者
サーバ		レジストリ業務に用いる JPNIC 内のサーバのうち、証明書が発行されるもの
ホストマスタ証明書		ホストマスタに対して発行される証明書
サーバ証明書		JPNIC の各種サーバに対して発行される証明書
LRA 管理者証明書		本認証局の認証業務に必要な運用用証明書の一つ。ホストマスタへの証明書発行時の LRA 管理者の認証に必要な証明書であり、その取扱いについては運用規則に則って厳格に管理・運用されるものとする。
エンドエンティティ	EE	証明書の発行対象である、ホストマスタ及び各種サーバの総称

エンドエンティティ証明書	EE 証明書	ホストマスタ証明書及びサーバ証明書の総称
証明書申請者	申請者	EE 証明書を申請中の者
証明書所有者	所有者	証明書発行申請を行い、自ら鍵を生成し、認証局により証明書を発行される主体をあらわす。本 CP/CPS では、EE 証明書を所有している者又はサーバの管理者となる。
証明書検証者	検証者	証明書を受け取る者で、その証明書を用いて検証することにより、その証明書及び/又はディジタル署名に依拠して行動する者
JPNIC 発行局	JPNIC IA	JPNIC ルート認証局内の発行局及び JPNIC IP アドレス認証局内の発行局の総称。JPNIC ルート認証局及び JPNIC IP アドレス認証局で発行業務をつかさどる組織。RA より依頼された証明書の発行を行う。 認証局（CA）の内、証明書の発行、失効等の証明書管理機能を表す場合に使用。
JPNIC 登録局	JPNIC RA	証明書発行の申請者の本人を確認し、主として登録業務・失効業務をつかさどる組織。証明書の所有者の本人確認と認証に責任を持っている。
認証局管理者	CAO	認証局サーバ、ディレクトリサーバ等認証局システムの運用管理をする者。
登録局管理者	RAO	登録局（RA）を管理し運営する者。証明書発行、失効の登録作業を行う。
リポジトリ		認証局が署名した証明書及び CRL 等を格納し公表するデータベース。
JPNIC ルート認証局		JPNIC が運営を行う認証局全体のルート認証局。JPNIC における認証階層経路の最上位に位置し、自己署名し、かつ配下にある下位認証局（IP アドレス認証局）の証明書に電子署名を行う。
JPNIC IP アドレス認証局		JPNIC が運営を行う IP アドレスの管理業務に関連する証明書の発行を行う認証局。JPNIC IP アドレス認証局証明書は、JPNIC ルート認証局により電子署名される。
JPNIC 認証局		JPNIC が運営を行う認証局の総称。JPNIC ルート認証局、JPNIC IP アドレス認証局、JPNIC 登録局及びリポジトリから構成される。

運営委員会		JPNIC の理事により構成される会議であり、JPNIC 認証局の運営方針の決定等を行う。運営委員会は、JPNIC の約款に従って運営される。
ローカル登録局	LRA	証明書を発行する組織とは異なる別組織であり、RA 業務において、本人の確認・審査、証明書発行申請処理及び証明書失効申請処理を行う組織。JPNIC 認証局の場合、IP アドレス管理指定事業者が、LRA となる。
ローカル登録局責任者	LRA 責任者	IP アドレス管理指定事業者の中における、LRA 業務の責任者。LRA 管理者の任命・解任を行う。
ローカル登録局管理者	LRA 管理者	IP アドレス管理指定事業者の中で、ホストマスタのメンバー管理と認証及びホストマスタ証明書の発行申請操作を行う。

（2） 証明書の適用範囲

ここでは、発行する証明書の用途について記述することとなる。本認証局の発行する証明書は、JPNIC の行う IP アドレス管理業務における各種申請、連絡等に使用するものであり、IP アドレス管理業務に関係しない使用、特に商取引での使用等には利用できないとするのが妥当である。

具体的には、前述した目的のもと、EE 証明書（サーバ証明書及びホストマスタ証明書）は、レジストリシステムにおけるサーバ及びクライアント（ユーザ）間の相互認証並びにメッセージ認証に用いる。また、本証明書の否認防止目的での使用は想定しないものと考えられる。

（3） 証明書が適合する又は使用が制限されるアプリケーション

ここでは、発行する証明書が適合するアプリケーション及び使用が制限されるアプリケーションがあれば、該当するアプリケーションの一覧を記述することとなる。

本認証局で発行する証明書は、主に SSL/TLS 及び S/MIME での利用を想定している。ただし、現段階では、適合する具体的なアプリケーションについては絞り込めていない状況である。また、既存の CP/CPS においても、適合するアプリケーションについて明記していないのが一般的であるため、本 CP/CPS においても現段階では、記述しないものとする。一方、使用を制限するアプリケーションについても現段階では特に該当するものがないため、記述しないものとする。

（4） 証明書の使用が禁止される用途

ここでは、本認証局の発行する証明書の使用を禁止すべき用途があれば、記述することとなる。

本認証局の発行する証明書は、JPNIC の行う IP アドレス管理業務における各種申請、連絡等に使用するものである。したがって、IP アドレス管理業務に関係しない使用、とりわけ商取引での使用等については禁止することが妥当と思われる。

また、IP アドレス管理業務における各種申請及び連絡等は、JPNIC と IP アドレス管理指定事業者のホストマスタ等との間でなされるものであるから、JPNIC を介さないホストマスタ間での連絡等への使用は、証明書の適用範囲からは外れるものと考えられる。しかし JPNIC として、当該証明書のホストマスタ間での使用を禁止するというのは行き過ぎであると思われ、CP/CPS 上は、ホストマスタ間での証明書使用を禁ずるものではないが、JPNIC が責任を持たないこととするのが妥当であると考える。

（5） 証明書の相互運用性

ここでは、本認証局が発行する証明書の相互運用性等について記述するか否かについて検討する。

本認証局では、前述のとおり、階層型認証局での運用を想定しているが、現段階では他認証局との相互接続等は具体的には予定されていない。ただし将来的には、APNIC CA 等との相互接続が考えられるため、CP/CPS 上は、「JPNIC 認証局は、他の認証局と相互認証を行うことがあるものとする」といった記述にとどめることとする。

「1.3. コミュニティと適用性」記述案

（1） コミュニティにおける登場者と役割

本認証局が発行する証明書の流通するコミュニティには、表 5-2 に示す複数の登場者が含まれる。

（表 5-2 が記述される）

（2） 証明書の適用範囲

本 CP/CPS に基づき発行される証明書は、JPNIC の行う IP アドレス管理業務における各種の申請及び連絡等を目的として、レジストリシステムにおけるユーザ認証及びメッセージ認証のために使われるものとする。

（3） 証明書が適合する又は使用が制限されるアプリケーション

規定しない。

（4） 証明書の使用が禁止される用途

本 CP/CPS に基づき発行される証明書は、JPNIC における各種申請処理業務等に利用することを意図するものであり、電子商取引での利用に意図されているものでも、認められているものでもない。また JPNIC は、IP アドレス管理指定事業者のホストマスタ相互間での証明書の使用を制限するものではないが、本使用に対して、なんら責任を負うものではない。

（5） 証明書の相互運用性

JPNIC 認証局は、他の認証局と相互認証を行うことがあるものとする。

5.4.1.4. ［1.4］連絡先

CP/CPS 1.4 節では、本 CP/CPS の登録、維持管理及び解釈に責任を負う機関の名前と住所を記述することとなる。また、本 CP/CPS に関する連絡先の担当者の名前、電子メールアドレス 電話番号、FAX 番号を記述することとなる。

各種基準では、認証局の管理組織の連絡先として組織名、責任者、住所、電話番号、FAX 番号、電子メールアドレスの明確化及び開示を求めている。

また通常、連絡先の情報として、住所、担当窓口名、電話番号、FAX 番号、電子メールアドレスを記載する他、問い合わせ受付時間を営業時間に限定する場合には、営業日及び営業時間も明記するのが一般的である。

一方で、認証局の所在地等を詳細に開示することが、セキュリティ上の問題を引き起こすとも考えられるため、詳細な連絡先を記述しないこともある。

JPNIC の場合、IP アドレス管理業務の重要性及び認証局のセキュリティを重視して、所在地等の明示は行わないことが望ましいと考えられる。ただし、一定の情報公開の責任はあるため、必要最小限の連絡窓口情報は記述するのが妥当である。

「1.4.連絡先」記述案

本 CP/CPS に関する問い合わせ先を次に定める。

社団法人 日本ネットワークインフォメーションセンター

受付時間：月～金 （年末年始／祝祭日は除く） 10:00～18:00

電子メールアドレス：（電子メールアドレスは決定後に記述される）

［1.5］用語

CP/CPS 1.5 節では、本 CP/CPS の内容を正しく理解するうえで必要となる用語の解説を記述することとなる。

用語の解説については、RFC2527 及び各種基準ともに、記述することを要求していないが、CP/CPS の理解を容易にするために、一般的な用語については解説しておくことが望ましいと思われる。ただし、本 CP/CPS 1.3 節において、本認証局に関係する登場者について記述するため、登場者等に関する別途ここでの解説は不要であると考える。そこで、CP/CPS 1.5 節では表 5-3 に示すような、CP/CPS にて記述される一般的な用語についてのみ、解説するものとする。なお、解説する用語が多数となる場合、本節に記述するのではなく、CP/CPS の最後に別章を設けて記述する場合もある。

表 5-3 用語

用語	略称	説明
電子証明書	証明書	ある公開鍵を、記載されたものが保有することを証明する電子的文書。認証局が電子署名を施すことで、その正当性が保証される。本 CP/CPS では、特に断らない限りホストマスタ証明書、サーバ証明書及び運用用証明書を総称して「証明書」と呼ぶ。
認証局	CA	証明書の発行・更新・失効、認証局等私有鍵の生成・保護及び証明書申請者の登録を行う機関。本 CP/CPS 内で、単に認証局という場合は証明書の発行業務及び登録業務を含む。
RFC2527		Request For Comments 2527 認証局 や PKI のための CP/CPS の執筆者を支援するフレームワーク。
オブジェクト識別子	OID	Object Identifier 世界で一意となる値を登録機関（ISO、ITU）に登録した識別子。PKI で使うアルゴリズム、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。
X.509		ITU-T が定めた証明書及び証明書失効リストのフォーマット。X.509 v3 では、任意の情報を保有するための拡張領域が追加された。
公開鍵		公開鍵暗号方式において用いられる鍵ペアの一方。私有鍵に対応する、公開されている鍵。
私有鍵		公開鍵暗号方式において用いられる鍵ペアの一方。公開鍵に対応する、本人のみが保有する鍵。秘密鍵と呼ぶこともある。
証明書発行要求	CSR	Certificate Signing Request 証明書を発行する際のもととなるデータファイル。CSR には証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して証明書を発行する。

CRL		Certificate Revocation List 証明書の有効期間中に、認証局私有鍵の危殆化等の事由により取消された EE 証明書及び運用用証明書の失効リスト。
PIN		Personal Identification Number 個人を識別するための情報。

「1.5.用語」記述案

（表 5-3 が記述される）

5.4.2. ［2］一般条項

5.4.2.1. ［2.1］義務

［2.1.1］JPNIC 発行局の義務

CP/CPS 2.1.1 項では、主に発行局が発行局自身やリポジトリの信頼性と安全性を確保するための義務を規定する。

その他の検討項目として、次のものがあげられている。

- 発行した証明書の申請者への発行通知
- 申請者以外への発行通知
- 証明書失効後の所有者への失効通知又は停止された証明書の所有者への通知
- 証明書失効後の所有者以外への失効通知又は停止した証明書の所有者以外への通知

JPNIC 発行局自身やリポジトリの信頼性・安全性確保や、所有者・検証者に対する適切な情報提供を保証するために、JPNIC 発行局が JPNIC 登録局や発行する証明書やリポジトリに対して負う義務を検討しなければならないと思われる。

その一つとして、JPNIC 発行局から発行された証明書であることを証明するための JPNIC 発行局の証明書署名鍵を安全に生成し、確実な管理を行うことや、問題がないことを証明する情報を公表する義務があると考えられる。なぜなら、この署名鍵が改ざん又は漏えいすることがあれば、JPNIC 発行局が発行した全ての証明書の信頼性が損なわれるからである。

また JPNIC 登録局からの申請を正確に受付け、正確な処理が行われるよう JPNIC 発行局のシステム稼動を監視し、正常な動作を保つ義務があると考える。

今回の検討では、認証局が EE に対して証明書の発行に必要な情報を送付し、EE 自身が鍵ペアを生成し、証明書の発行に必要な情報とともに認証局システムへアクセスすることにより、証明書をその場で受け取ることができる仕組みを想定している。ゆえに、EE は証明書の発行操作時点で証明書が発行されたことを認識できる。また、リポジトリにおいても確認ができるので、発行した証明書の申請者への発行通知は不要と考える。

申請者以外への発行通知に関しては、一般的には特に申請者以外に知らせる必要はないと思われる。証明書失効後の所有者への失効通知又は停止された証明書の所有者への通知に関しては、JPNIC が必要と考える特別な事情のもとで強制的に失効させることがない限り、所有者又は LRA 担当者からの失効申請に基づいて失効が行われ、CRL へ反映されるため、これをもって所有者への通知と考えられる。また、JPNIC の決定のもとで EE の証明書が失効させられた場合には、所有者への通知を直接又は LRA を介して行う義務があると考える。JPNIC 認証局では証明書の停止を行わない

ため、これに関する義務はないと考える。

証明書失効後の所有者以外への失効通知又は停止した証明書の所有者以外への通知に関しては、一般的には特に申請者以外に知らせる必要はないと思われる。証明書の失効に関する情報は、CRL に開示することで通知されているものと考えることとした。ただし、CRL をいつでも確認できるようにリポジトリを維持管理する義務が発生する。ここで、これらの義務の詳細な検討については JPNIC 発行局のサービスレベルによって大きく影響されるため、特に具体的な数値や可用性、規定すべき内容の表現等は JPNIC 発行局のサービスレベル決定後に再度検討する必要がある。

前述の検討内容を踏まえた CP/CPS 記述案を次に示すが、最低限必要であると思われる一般的な規定内容を示す。

「2.1.1.JPNIC 発行局の義務」記述案

JPNIC 発行局は JPNIC 発行局の業務を遂行するにあたり次の義務を負う。

- JPNIC 発行局の証明書署名鍵のセキュアな生成・管理
- （本 CP/CPS、証明書所有者同意書、証明書検証者同意書、JPNIC ルート認証局の自己署名証明書・自己発行証明書、CRL）の値を（SHA-1（仮のアルゴリズム））で変換した値の公開
- JPNIC 登録局からの申請に基づいた証明書の正確な発行・失効管理
- JPNIC 発行局のシステム稼動の監視・運用
- CRL の発行・公表
- リポジトリの維持管理
- JPNIC の判断によって EE 証明書を失効させた場合の当該証明書の所有者への通知
- 本 CP/CPS に従った受付時間内の問合せ受付

［2.1.2］JPNIC 登録局の義務

CP/CPS 2.1.2 項では、登録局が発行局・LRA・申請者等に対して負う義務を規定する。

JPNIC が JPNIC 登録局自身の信頼性・安全性確保を保証するために、JPNIC 登録局が JPNIC 発行局･LRA･申請者に負う義務として次のようなことが考えられる。

- JPNIC 登録局の端末を不正に操作され、不正な証明書の発行・失効が行われるということがない環境の構築や、端末の運用
- 証明書の発行・失効申請において、JPNIC 発行局へその正確な申請を行うこと
- 失効申請があった場合は、証明書有効性と関わりがあるため、速やかに正確

な失効申請処理を行うこと
等

ここで、JPNIC 登録局にて証明書の発行・失効申請を受付ける時間帯を限定するか 24 時間とするかを検討する必要があると思われる。特に失効申請受付時間帯に関しては証明書有効の確実性と関わりがあるため、この時間帯を明確にし、JPNIC 登録局がこの決定に沿った運用を行うことが義務になると考えられる。ただし、受付時間については、運用体制やコストに大きく影響するため、次のような検討を行った。

証明書の発行・失効申請を受け付ける時間帯を限定せず 24 時間対応とすれば、緊急の失効申請に対しても受付可能であるため、証明書の信頼性が高くなる一方、時間外に受付要員を配置する必要があり、運用体制及び人件費コスト等の問題が生じる。

一般的に証明書の失効処理が即時に行えるということは、証明書の信頼性を高めることになると考えられるため、極力 24 時間の受付を行うことが望ましい。このためには要員の対応だけでなく、システム面での 24 時間対応の検討も必要である。24 時間対応としない場合には、時間外に失効申請が受付けられない際に生じる損害を考慮しつつ、受付時間帯を検討しなければならない。しかし現段階では、詳細な検討ができず、後述の記述案においては、JPNIC 登録局の受付時間に関する義務は規定しないものとする。

前述の検討内容及び一般的な CP/CPS の例を踏まえ CP/CPS 記述案を次に示すが、CP/CPS への記載内容は JPNIC 登録局のサービスレベルや運用手順によって大きく影響されるため、実際の利用組織である IP アドレス管理指定事業者と協議を行ったうえで再度規定内容を検討する必要があると思われる。

「2.1.2.JPNIC 登録局の義務」記述案

JPNIC 登録局は、JPNIC 登録局の業務を遂行するにあたり次の義務を負う。

- 登録端末のセキュアな環境への設置・運用
- 証明書発行・失効申請における JPNIC 発行局への正確な情報伝達
- 証明書失効申請における JPNIC 発行局への運用時間中の速やかな情報伝達

［2.1.3］ローカル登録局の義務

CP/CPS 2.1.3 項では、LRA が登録局・申請者・所有者等に対して負う義務を規定する。

主な検討項目として次のものが考えられる。

- 証明書発行申請を行う前に確実な本人確認の実施
- 申請情報の登録局への正確な伝達

その他にも、LRA 自身の信頼性や安全性確保を保証するための義務を規定する。

前述の各検討項目に対応した LRA の義務を次のように検討した。

証明書発行申請を行う前に確実な本人確認の実施に関しては、申請者が証明書申請書類上の本人であることを LRA 管理者が確実に認証し、JPNIC 登録局へ LRA 管理者が正確に発行申請する義務があると考える。

申請情報の登録局への正確な伝達に関しては、申請者から提出され、審査が終了した申請書類の情報に基づいて LRA 管理者がそれらを正確に JPNIC 登録局へ伝達する義務があると考える。

LRA 自身の信頼性や安全性確保を保証するために、LRA が JPNIC 登録局や申請者や所有者に負う義務を検討しなければならないと思われる。

その一つとして、LRA には、JPNIC との間で取り交わされた契約に基づいてその業務を行う義務があると考えられる。なぜなら、その契約の中で JPNIC 認証局と LRA のそれぞれの業務における責任の所在を明確に分離するために、責任について詳細な規定が行われると考えられるからである。

また LRA には、証明書利用上の注意事項に関して、ホストマスタに徹底させる義務があると考えられる。なぜなら、ホストマスタは LRA 業務を行う IP アドレス管理指定事業者の一員であるため、各 LRA にて所属するホストマスタへの教育を行うべきであると考えられるからである。

現段階では、JPNIC と IP アドレス管理指定事業者との間で行われる契約や義務等に関する協議が行われていないので、協議後に改めて規定内容を検討する必要がある。よって、CP/CPS の記載内容として最低限必要と思われる記述案を次に示す。

「2.1.3.ローカル登録局の義務」記述案

LRA は LRA 業務を遂行するにあたり次の義務を負う。

- 申請書類上の所有者と申請者が同一であることの検証
- JPNIC 登録局への正確な申請情報の伝達
- 証明書利用におけるホストマスタの教育
- 正当な申請者への確実な証明書配布（鍵ペアの受渡しについては生成システムに依存するため、後日の要検討内容）
- 証明書失効の妥当性の確認
- その他、JPNIC との契約に準拠した運用の厳守

［2.1.4］証明書所有者の義務

CP/CPS 2.1.4 項では、所有者が LRA や各自の証明書等に対して負う義務を規定する。

RFC2527 では主な検討項目として次のものがあげられている。

- 証明書アプリケーションを用いた証明書記載内容正確性の確認
- 各自の私有鍵の防護
- 私有鍵と証明書使用についての制限厳守
- 私有鍵改ざんについての LRA への通知

前述の各検討項目に対応する JPNIC 認証局が発行する証明書の所有者の義務を次のように検討した。

証明書アプリケーションを用いた証明書記載内容正確性の確認に関しては、JPNIC 発行局から発行された証明書に記載されている内容が、自らの申請内容と同一であることを確認する義務があると考えられる。また記載内容に誤りがある場合には、速やかに LRA へ申告する義務もあると考えられる。

各自の私有鍵の防護に関しては、他人への貸与を行わないことや他人によって不正に使用されないよう管理する義務があると考えられる。もし CP/CPS に規定された証明書の失効申請を行うべき条件に該当する事象が生じた場合には、速やかに LRA へ失効申請を行う義務もあると考えられる。

私有鍵と証明書使用についての制限厳守に関しては、所有者は CP/CPS に規定されている内容を理解し、所有者本人による使用であっても CP/CPS に規定された利用範囲を超えて使用しないことを厳守する義務があると考えられる。

私有鍵改ざんについての LRA への通知に関しては、所有者の私有鍵が改ざんされた場合又はそのおそれがある場合には、速やかに LRA へ失効申請を行うこと義務があると考えられる。同様に私有鍵が漏えいした場合又はそのおそれがある場合にも、速やかに LRA へ失効申請を行う義務があると考えられる。

その他にも証明書申請時の所有者による正確な情報の提示等を保証するために JPNIC が所有者に課す義務を検討しなければならないと思われる。

ただし、これらの義務に関しては CP/CPS 上で詳細に記載するのではなく、別途“ 証明書所有者同意書 ” を作成しその中で詳細に規定することも考えられる。公開する CP/CPS 上にて所有者の義務の詳細な記述を行うことは困難であっても、証明書所有者同意書として別途、所有者の義務や責任を詳細に記述し、申請者から証明書所有に関する詳細な同意を得ることが可能である。また CP/CPS 上に記載するより内容の改

定手続きが容易となると考えられる。

一方、証明書所有者同意書を作成すると、管理すべき書類（同意書の改版や同意後の書類等）の増加や、申請者との間での同意書授受処理を行う必要が生じると考えられる。

一般的に、CP/CPS 上には基本的な方針を記載するべきであって、詳細な規定を記述するべきではないと思われる。JPNIC 認証局運営における、所有者義務内容の変更に留意し、証明書所有者同意書のような規定を別途作成し、証明書所有者に対して理解と承諾を求めることが望ましい。

前述の検討内容を踏まえた記述案を次に示すが、詳細な規定内容は所有者同意書に記述されることを前提として、一般的な規定内容を示す。

「2.1.4.証明書所有者の義務」記述案

所有者は証明書所有にあたって、次の義務を負うものとする。

- 本 CP/CPS 及び（証明書所有者同意書以外にも必要な書類があれば記載する）の理解と承諾
- 証明書所有者同意書の理解と、証明書所有者同意書への署名
- 証明書の記載内容の受領時確認と誤記内容の申告
- 私有鍵の盗難・漏えい・紛失・他者による不正利用等を防ぐことへの十分な注意と管理
- 鍵の危殆化又はその可能性がある場合の速やかな失効申請
- 利用目的の確認と利用目的内での利用
- 証明書申請内容の正確な提示
- 私有鍵の秘匿管理や私有鍵と公開鍵の対応管理

［2.1.5］証明書検証者の義務

CP/CPS 2.1.5 項では、検証者が証明書を信頼するにあたって証明書に対して負う義務を規定する。

RFC2527 では主な検討項目として次のものがあげられている。

- 証明書が使用される目的確認と承諾
- 署名検証
- 失効と停止の確認

前述の各検討項目に対応して JPNIC 認証局が発行する証明書の検証者の義務を次に検討する。

証明書が使用される目的確認と承諾に関しては、検証者がその証明書を信頼するに先立って証明書の使用目的を理解し、その内容に承諾していることを認識する義務があると考えられる。

署名検証に関しては、検証者がその証明書を信頼する根拠として、JPNIC 認証局による有効期限以内の有効な署名が付与されていることを確認する義務があると考えられる。

失効と停止の確認に関しては、検証者がその証明書を信頼する根拠として、CRL 上に当該証明書の登録が存在しないことを確認する義務があると考えられる。

その他にも検証者による証明書の適切な利用を保証するために、JPNIC が検証者に課す義務を検討しなければならないと考えられる。

その一つは、証明書を信頼する根拠として前述の義務以外に、証明書の有効期限と記載項目の確認を確実に行う義務があると考えられる。当該証明書が CRL に記載されていないとしても、証明書生成時に設定された有効期限を過ぎていることが考えられる。

「2.1.5.証明書検証者の義務」

検証者は証明書を信頼するにあたって次の義務を負わなければならない。

- 証明書を信頼する時点で、本 CP/CPS の理解と承諾
- 証明書の利用目的と自己の利用目的が合致していることの承諾
- 証明書に行われた電子署名の検証と発行者の確認
- 証明書の有効期間や記載項目の確認
- CRL に基づいて、証明書が失効していないことの確認
- 証明書パス上の全証明書の改ざん、有効期間、失効、使用目的の確認

［2.1.6］リポジトリの義務

CP/CPS 2.1.6 項では、リポジトリが検証者等に対して負う義務を規定する。

RFC2527 では、主な検討項目として次のものがあげられている。

- 証明書と失効情報の適時な公表

JPNIC 発行局によってリポジトリに登録された証明書の失効情報が、遅滞なく検証者による参照を可能とする義務がリポジトリにはあると考えられる

その他にも証明書利用目的や方法を踏まえてリポジトリの利用可能時間を検討する必要があると考え、次の検討を行った。

証明書有効性検証等のためのリポジトリ参照の利用可能期間を、JPNIC 認証局運営費用の削減等の理由により限定するなら、リポジトリの通常運用時間に関して次の点を検討する必要がある。

- 1 日の何時から何時まで運用するか
- 1 週間の何曜日に運用するか
- 1 年間を通して特別に運用を停止する時（年末年始等）があるか

しかし、一般的には任意のタイミングでリポジトリへのアクセスを許容するため、リポジトリの 24 時間サービス提供が原則と考えられる。24 時間のリポジトリサービス提供を行う場合は、24 時間提供することを明記するかどうかを検討しなければならないと思われる。明記することで、サービス利用者にサービスに対する信頼感を与えることができる一方、24 時間運用が義務化されるためにシステムの冗長化及び運用体制の強化等を行う必要がある。

ここで、既存の CP/CPS の多くはリポジトリの常時利用可能を前提条件としているが、「24 時間のリポジトリサービスを目指す。ただし、保守・緊急対応の必要性が発生した場合は除く。」といった柔軟な対応を許容する規定が一般的であり、これと同様な記述をすることが適当であると思われる。

「2.1.6.リポジトリの義務」記述案

JPNIC はリポジトリ運用を次のように行う。

- 所有者証明書やサーバ証明書の失効があった場合、直ちに当該証明書失効の公表をリポジトリにて行う
- CRL 等の必要情報を常時確認可能とする。ただし、保守・緊急対応の必要性等が発生した場合は除く

5.4.2.2. ［2.2］責任

CP/CPS 2.2 節中の各項では、発行局・登録局・LRA が取るべき責任について規定する。

RFC2527 では検討項目として次のものがあげられている。

- 権利と権利についての限度
- 補償される被害の種類と適用除外者
- 証明書ごと、若しくはトランザクションごとの賠償限度
- 天災や他の主体が負うべき責任等の例外事項

前述の各項目に基づいて JPNIC 発行局・JPNIC 登録局・LRA が他に対して取るべき責任を規定しなければならない。ただし、この責任の節は CP/CPS の義務及び賠償の節と重複する内容が多いため簡素な記述にまとめられることもある。

今回の検討では、前述の賠償限度、適用除外等の賠償、補償に関わる事項は CP/CPS 2.3 節に記述する。

［2.2.1］JPNIC 発行局の責任

本報告書 5.4.2.2.を踏まえた記述案を次に示す。

「2.2.1.JPNIC 発行局の責任」記述案

JPNIC 発行局は本 CP/CPS 2.1.1 項に従った運用及び 2.1.6 項に示されたリポジトリに関する管理に責任を負う。

［2.2.2］JPNIC 登録局の責任

本報告書 5.4.2.2.を踏まえた記述案を次に示す。

「2.2.2.JPNIC 登録局の責任」記述案

JPNIC 登録局は本 CP/CPS 2.1.2 項に従った運用を行う責任を負う。

［2.2.3］ローカル登録局の責任

本報告書 5.4.2.2.を踏まえた記述案を次に示す。

「2.2.3.ローカル登録局の責任」記述案

LRA は本 CP/CPS 2.1.3 項に従った運用を行う責任を負う。

5.4.2.3. ［2.3］財務上の責任

CP/CPS 2.3 節中の項では、認証局の責任を遂行するための財務上の責任について規定する。

RFC2527 では主な検討項目として次のものがあげられている。

- 補償の範囲
- 補償時の原資の調達先又は企業賠償責任保険への加入
- 補償金額上限

ここで、CP/CPS では JPNIC 認証局が発行する証明書の商用利用を目的としておらず、かつ閉じた領域で使用されるため、CP/CPS 2.2 節の責任に対する賠償の必要性があるかどうかを検討する必要がある。その検討結果として賠償する必要がないと結論付けられるなら、前述の各検討項目について考慮する必要はないと思われる。

一般的に損害賠償責任について、CP/CPS 上に明確に記述されることは少ない。よって、この項では、保証内容及び免責内容について検討した。

JPNIC によって管理し得ない原因によって生じる損害を免責内容とするのがよいと思われる。具体的に免責内容とすることが妥当と思われる状況を次に示す。

- 緊急的な保守時（リポジトリの停止等）
- 火災・停電等の発生時
- 自然災害発生時
- 戦争、テロリズム等の人的災害発生時
- 予想を超えた暗号解読技術の向上時
- LRA の責で生じた時

更にこれらの免責事項に該当しない場合でも、JPNIC は発生した損害の直接的な部分のみを賠償するとし、次に示す損害は免責内容とするのが良いと思われる。

- 間接損害
- 特別損害
- 付随的損害
- 派生的損害

「2.3.賠償」記述案

JPNIC は本 CP/CPS に規定した内容を遵守して認証業務を提供し、認証局私有鍵の信頼性を含む認証業務の信頼性の確保を保証する。JPNIC がこの保証に違反して損害賠償を負う場合には、LRA との契約における該当条項に従う。

［2.3.1］依存する主体による賠償

ここでは、証明書検証者が適切に失効情報を調べることなく行った証明書の使用、又は認証局の許可の範囲外の目的での証明書の使用により、認証局が被った損失について証明書検証者が認証局に対し賠償する義務があることを定める協定を認証局が使用する旨定めることができる。

「2.3.1.依存する主体による賠償」記述案

規定しない。

［2.3.2］様々な主体との間の受託関係

CP/CPS 2.3.2 項では、様々な主体との間の受託関係についてその有無を規定する。

JPNIC に他との受託関係や親子関係等がないのであれば規定する必要性はないと考えられる。

「2.3.2.様々な主体との間の受託関係」記述案

規定しない。

［2.3.3］管理的手続き

CP/CPS 2.3.3 項では、課金や監査等の管理的手続きについて規定する。

この項の規定がある CP/CPS では企業会計原則等が記述されていることがある。一般的には特に記述不要と考えられる。

「2.3.3.管理的手続き」記述案

規定しない。

5.4.2.4. ［2.4］解釈及び執行

［2.4.1］適用される法律

CP/CPS の 2.4.1 項では、適用対象となる CP/CPS 又は協定の解釈と執行を一定の司法権 に属する法に準拠する旨の記述及び関係者が適用法を遵守する要件、例えば、

輸出規制の適用を受ける暗号ハードウェア及びソフトウェアに関連する法律等、に関して規定をすることができる。

今回の CP/CPS においては、本認証局の所在地は日本国であり、かつ証明書の発行対象となる EE は、JPNIC との契約において関連付けられた日本国内の IP アドレス管理指定事業者の組織から任命された者及び JPNIC 内で使用されるサーバであるため、日本国の法令を適用する旨の記述が妥当と考えられる。また、輸出規制や関連する法律を遵守する旨を記述する。

「2.4.1.適用される法律」記述案

本認証局を含む JPNIC 認証局、証明書所有者及び証明書検証者の所在地に関わらず、本 CP/CPS の解釈、有効性及び本認証局の証明書発行に関わる紛争については、日本国の法令が適用される。また、本認証局は、国内における各種輸出規制を遵守し、暗号ハードウェア及びソフトウェアを取扱うものとする。

［2.4.2］分割、存続、合併及び通知

CP/CPS の 2.4.2 項では、CP/CPS、協定等の可分性、効力の継続性、サービスの統合等により CP/CPS に変更が発生する場合に対する方針を記述する。

一般的な記述としては、認証局の示す CP/CPS や協定等の一部の条項について、法律等により有効でないとされた場合においても、その他の条項については、有効性が存続する旨の記述がなされる。また、サービスの統合等により CP/CPS に変更が発生する場合の方針については、統合前の合意事項に責任を持ち続けることに最善を尽くす又は責任を持ち続ける旨の記述がなされる。

「2.4.2.分割、存続、合併及び通知」記述案

本 CP/CPS 及び本認証局より示す協定等において、その一部の条項が有効でないと判断された場合においても、他の条項については有効に存続するものとする。

また、本認証局は、サービスの統合等により CP/CPS に変更が発生する場合においても、統合前の合意事項に責任を持ち続けることに最善を尽くすものとする。

［2.4.3］紛争解決の手続き

CP/CPS の 2.4.3 項では、本認証局が行う証明書発行に関わる紛争について、訴訟、仲裁における手続きについての記述を行う。

「2.4.3.紛争解決の手続き」記述案

本認証局が発行する証明書に関わる紛争について、JPNIC に対して、訴訟、仲裁等を含む法的解決手段に訴えようとする場合は、JPNIC に対して事前にその旨を通知するものとする。仲裁及び裁判地は東京都区内における紛争処理機関を専属的管轄とすることに、全ての当事者は合意するものとする。また、CP/CPS、契約書にて定められていない事項やこれらの文書の解釈に関し疑義が生じた場合は、各当事者はその課題を解決するために誠意を持って協議するものとする。

5.4.2.5. ［2.5］料金

CP/CPS の 2.5 節では、認証局、リポジトリ又は登録局によって課される料金に関して規定する。例えば、証明書の発行又は更新料、証明書へのアクセス料金、失効又はステータス情報へのアクセス料金、関連する CP/CPS へのアクセスを提供するといったその他のサービスに対する料金、払戻しに関する方針について記述することとなる。

本認証局の場合、一般個人、法人に証明書を発行する商用認証局とは異なるので、公開する CP/CPS 上に料金等を示さないのが一般的と思われる。また、今回の検討においては、料金等に関し検討は行われていないため、次のような記述案とする。

「2.5.料金」記述案

本認証局が発行する証明書に関わる発行料金、更新料金、利用料金等は、別途定められるものとし、事前に関係者に周知されるものとする。

5.4.2.6. ［2.6］情報の公表とリポジトリ

［2.6.1］認証局情報の公表

CP/CPS 2.6.1 項では、リポジトリに公表する認証局情報に関して記述する。

公表する情報としては、

- 自己署名証明書
- リンク証明書
- 相互認証証明書
- 下位認証局証明書
- EE 証明書

- CRL/ARL
- CP/CPS
- 証明書所有者/検証者同意書

等が考えられる。

認証局の構成、リポジトリの構成により発行する若しくは公表する証明書は異なるものとなるが、今回の検討においては、JPNIC ルート認証局と下位認証局である JPNIC IP アドレス認証局の構成とし、リポジトリに関しては、ルート認証局と下位認証局は同一のリポジトリを使用するものとして記述を行う。

検討項目として、CP/CPS、EE 証明書を公開するか否かがあげられる。

今回のような適用範囲が限定された利用においては、CP/CPS、EE 証明書を公開しない場合もありうる。

認証局は、関係者に対して義務等の周知及び認証局自体を紛争から守る意味での認証局の要件の周知を CP/CPS、契約書等にて行う必要がある。周知の一般的な方法として、CP/CPS をリポジトリに公開することが妥当と思われる。

EE 証明書については、リポジトリ上に公開することにより、証明書上の個人情報が広く知られることとなり、好ましくない場合もありうる。適用範囲が限定された利用においては、お互いの証明書を交換することが可能であり、証明書をリポジトリに公開しないで PKI を利用することが可能となる。継続的な検討課題として、EE 証明書をリポジトリに公開するか否かについては、今回の PKI 利用に関係する組織と業務上の利便性や個人情報保護の考え方等を踏まえ、更に検討するものとする。

「2.6.1.認証局情報の公表」記述案

本認証局を含む JPNIC 認証局は、次の情報を、JPNIC 認証局のリポジトリ上に公開する。

- 自己署名証明書（JPNIC ルート認証局）
- リンク証明書（JPNIC ルート認証局）
- 下位認証局証明書（JPNIC ルート認証局）
- EE 証明書（JPNIC IP アドレス認証局）＊公表時のみ
- CRL（JPNIC ルート認証局、JPNIC IP アドレス認証局）
- CP/CPS（JPNIC ルート認証局、JPNIC IP アドレス認証局）

リポジトリの URI は次のとおりである。

（URI は決定後に記述される）

また、JPNICが運営する認証局は、フィンガープリントを、リポジトリよりSSL/TLSを使用して公開する。フィンガープリントを公開するリポジトリのURIは次のとおりである。

（URI は決定後に記述される）

なお、CP/CPS 及び認証局に関する重要情報は、JPNIC の次に示す URI のホームページにおいても公開される。

（URI は決定後に記述される）

［2.6.2］公表の頻度

CP/CPS 2.6.2 項では、公表する情報の公表頻度、時期について記述を行う。

CRL/ARL の公表時期、頻度については、認証局の運用形態、システムにより左右されるが、24 時間以内での更新が一般的と思われる。

「2.6.2.公表の頻度」記述案

（1） CP/CPS の公表については、本 CP/CPS 8 章にて規定される。

（2） 自己署名証明書、リンク証明書、下位認証局証明書については、発行及び更新の都度公表する。

（3） CRL については、24 時間以内に定期的に更新が行われ、証明書の失効が行われた場合は即時に更新が行われる。

（4） 認証局に関する重要情報若しくはその他情報は、JPNIC 認証局の判断により適宜更新が行われる。

（5） EE 証明書については、発行及び更新の都度公表される。＊公表時のみ

［2.6.3］アクセスコントロール

CP/CPS 2.6.3 項では、CP/CPS、証明書のステータス及び失効リストを含む公開情報へのアクセス管理について記述する。

「2.6.3.アクセスコントロール」記述案

本認証局を含む JPNIC 認証局は、公表情報に関して、読み取り専用の制御以外に特段のアクセスコントロールは行わない。証明書所有者及び証明書検証者は、JPNIC が運営する認証局が発行した証明書に関する公開情報を、リポジトリを通じて入手することができる。

［2.6.4］リポジトリ

CP/CPS 2.6.4 項では、認証局又は他の独立主体によって運用されているリポジトリの利用に関する要件について記述する。

「2.6.4.リポジトリ」記述案

本認証局を含む JPNIC 認証局は、リポジトリを一日 24 時間、一週 7 日間利用できるように維持管理を行う。システムの保守等において、一時的に停止を行う必要がある場合は、証明書所有者、証明書検証者及び関係者に対して、事前に通知若しくはホームページ上で公表するものとする。ただし、災害、事故、障害発生時等やむを得ない事態が発生した場合はこの限りではない。

5.4.2.7. ［2.7］準拠性監査

［2.7.1］各主体に対する準拠性監査の頻度

CP/CPS 2.7.1 項では、CP/CPS に基づいて、評価されるべき個々のエンティティに対する準拠性監査又は他の評価を行う頻度又は評価を行うきっかけとなる状況について記述することとなる。

準拠性監査は、一般的に最低でも毎年実施することが必要と思われる。また、定期的な監査のほかに、運営責任者や運営委員会が必要と判断した場合は、即時に行われることが必要と考える。

「2.7.1.各主体に対する準拠性監査の頻度」記述案

本認証局を含む JPNIC 認証局は、毎年一回以上、認証局運用についての準拠性監査を実施する。また、必要に応じて、不定期な監査を実施する。

［2.7.2］監査者の身元・資格／認定にかかる事項

CP/CPS 2.7.2 項では、監査又は他の評価を行う担当者の身元、資格について記述を行う。

ここでは、

- 外部監査とするか
- 内部監査とする場合、内部監査組織は存在するか若しくは組織するか
- 監査する者の身元、資格を規定するか

等の検討が必要となる。

認証局の監査については、一般的な情報システム監査のほかに認証局特有の注意点（認証局鍵管理、暗号アルゴリズム、厳密性等）があり、認証業務に精通した監査者が望まれる。

現状、JPNIC の組織において、システム監査に関する内部監査組織は組織されておらず、また、現段階での検討においては、内部監査組織を組織化するのか又は外部監査の利用するのかについて定まっていないため、CP/CPS の記述上、運営委員会が指定する認証業務に精通した監査者により行われる旨の記述にとどめることとした。

「2.7.2.監査者の身元・資格／認定にかかる事項」記述案

JPNIC は、認証局の準拠性監査を、運営委員会が選定する認証業務に精通した監査者により実施する。

［2.7.3］監査者と被監査部門の関係

CP/CPS 2.7.3 項では、監査者の独立性の程度、監査者と被監査部門との関係を記述することとなる。

監査者は、監査する業務を客観的に評価する必要があり、被監査部門から独立していることが望まれる。

「2.7.3. 監査者と被監査部門の関係」記述案

JPNIC は、監査者を本認証局を含む JPNIC 認証局の認証業務に関わる要員以外から選定する。

［2.7.4］監査テーマ

CP/CPS 2.7.4 項では、評価又は評価を行うために使用された評価方法に関する事項に関して記述する。

認証局の準拠性監査は、認証局の運営が CP/CPS を遵守して運営されているかを確認するものである。監査項目としては、

- 認証局の業務担当者の業務運用
- 認証局私有鍵の管理
- 証明書のライフサイクル管理
- ソフトウェア、ハードウェア、ネットワーク
- 物理的環境及び設備
- セキュリティ技術の最新動向への対応
- 規定等の妥当性評価

等が考えられる。

また、運営委員会が必要と認めた監査目的による監査の実施も必要と考えられる。

「2.7.4.監査テーマ」記述案

本認証局を含む JPNIC 認証局の準拠性監査は、認証局の運営が CP/CPS 及び関連する規定を遵守して運営されているかを監査するものである。

主な監査項目として、

- 認証局の業務担当者の業務運用
- 認証局私有鍵の管理
- 証明書のライフサイクル管理
- ソフトウェア、ハードウェア、ネットワーク
- 物理的環境及び設備
- セキュリティ技術の最新動向への対応
- 規定等の妥当性評価

等の監査を行う。

また、運営委員会が必要と認めた場合、運営委員会が指定する監査目的による監査を実施する。

なお、JPNIC は LRA の監査を行う権利を有する。

［2.7.5］監査指摘事項への対応

CP/CPS 2.7.5 項では、監査において発見された不備等の指摘事項への対応について記述する。例としては、指摘事項が改められるまでの運用の一時的な停止、不正な証明書の失効、人事の変更、特別な調査の実施又は準拠性監査周期の変更及び不正を起こした要員に対する損害賠償請求等があげられる。

指摘事項に対する詳細な対応事項をもれなく列挙するのは難しく、損害賠償請求、証明書の失効等の詳細な記述はせず、認証局として、どのような方針で対応するのかの概要を示すことにとどめる。

「2.7.5.監査指摘事項への対応」記述案

本認証局を含む JPNIC 認証局は、監査報告書で指摘された事項に対して、運営委員会がその対応を決定する。運営委員会は、指摘事項に関して、セキュリティ技術の最新動向も踏まえ、問題が解決されるまでの対応策も含め、その措置を JPNIC 認証局の運営責任者に指示する。講じられた対応策は、運営委員会に報告され、評価されるとともに、次の監査において確認される。監査において発見された不備等の指摘事項への対応をしない場合は、運営委員会によって予め定められた罰則が課される。

［2.7.6］監査結果の通知、開示等

CP/CPS 2.7.6 項では、監査結果を誰が、誰に、どのように通知若しくは開示するのかを記述する。

検討点として、

- 公開文書とするのか
- 関連組織である LRA の要求があった場合、開示するか
- 開示する場合の手続きは

が、考えられる。

監査報告は、認証局の運用状態等が把握でき、セキュリティ上公開文書とするのは好ましくないと考えられる。また、内容によっては認証局としての信頼性の低下を引き起こす可能性のあるセンシティブな情報を含むことがあり、原則は、外部への開示は行わないとすることが良いと思われる。

「2.7.6.監査結果の通知、開示等」記述案

監査結果の報告は監査者から運営委員会に対して行われる。本認証局を含む JPNIC 認証局は、法律に基づく開示要求があった場合以外は、監査結果を外部へ開示しない。

なお、監査報告書は、JPNIC 認証局運営責任者により最低 5 年間保管管理される。

5.4.2.8. ［2.8］秘密保護ポリシ

［2.8.1］秘密扱いとする情報

CP/CPS 2.8.1 項では、秘密扱いとする情報について記述する。

秘密扱いとする情報については、

- 申請に関わる情報
- 証明書の発行申請記録、失効申請記録、開示申請記録
- 監査ログを含む各種トランザクションの記録
- 監査の記録、監査報告書
- 不測の事態に対応する計画、災害時の復旧計画
- 認証局運用業務のセキュリティ対策
- 業務に関する、規定、手順書、マニュアル等
- 業務に関する記録

等が考えられる。

記述方法として、詳細にそれぞれの情報を記述するのか又は前述の CP/CPS 2.6 で公表すると定めた情報以外と記述するかの選択がある。今回の記述においては、公表すると定めた情報以外については、秘密情報として扱うこととする。

「2.8.1.秘密扱いとする情報」記述案

本認証局を含む JPNIC 認証局が保持する情報は、本 CP/CPS 2.6 節で公表すると定めた情報、本 CP/CPS の一部として明示的に公表された情報、ホームページで公表している情報を除き、秘密扱いとする。JPNIC 認証局は、本 CP/CPS 2.8.3 項から 2.8.7 項に定められた方法を除いてこれらの情報を開示しない。

証明書所有者の私有鍵は、その所有者によって秘密扱いとされる情報とする。

なお、個人情報の保護に関する取扱は、本 CP/CPS 2.10 節に定める。

［2.8.2］秘密扱いとしない情報

CP/CPS 2.8.2 項では、秘密扱いとしない情報について記述する。

前述の CP/CPS 2.8.1 項以外に、次のような情報が考えられる。

- JPNIC の過失によらず知られるようになった情報
- JPNIC 以外の出所から、機密保持の制限なしに JPNIC に知られるようになった情報
- JPNIC によって独自に開発された情報
- 開示対象の情報に関連する人、組織により承認を得ている情報

ここでは、JPNIC 認証局の範囲ではなく、JPNIC においての情報として範囲を広げて記述を行うこととした。

「2.8.2.秘密扱いとしない情報」記述案

本 CP/CPS で公表すると定めた情報、本 CP/CPS の一部として明示的に公表された情報、ホームページ等で公表している情報は秘密扱いとしない。その他、次の状況におかれた情報は秘密扱いとしない。

- JPNIC の過失によらず知られるようになった情報
- JPNIC 以外の出所から、機密保持の制限なしに JPNIC に知られるようになった情報
- JPNIC によって独自に開発された情報
- 開示対象の情報に関連する人、組織により承認を得ている情報

［2.8.3］証明書失効及び停止情報の開示

CP/CPS 2.8.3 項では、証明書の失効及び停止情報に関する取扱いに関して記述する。

なお、JPNIC 認証局では、業務の煩雑さ等を考慮し、停止は行わないこととした。

「2.8.3.証明書失効及び停止情報の開示」記述案

本認証局を含む JPNIC 認証局は、証明書を失効する場合、その証明書の発行者である認証局情報、失効日時を含む CRL を開示する。失効理由及び失効に関するその他の詳細情報は原則として開示しない。

［2.8.4］法的執行機関への情報開示

CP/CPS 2.8.4 項では、法執行機関からの命令による情報開示への対応を記述する。

本検討では、法的な権限に基づく開示請求については、開示できる旨の記述を基本とした。

「2.8.4.法的執行機関への情報開示」記述案

本認証局を含む JPNIC 認証局で取扱う情報に関して、捜査機関、裁判所その他法的権限に基づいて情報を開示するように請求があった場合、JPNIC は法の定めに従って法執行機関へ情報を開示することができる。

［2.8.5］民法上の要求にともなう開示

CPS 2.8.5 項では、調停、訴訟、仲裁、裁判上行政手続きにおける開示請求に対する対応を記述する。

「2.8.5.民法上の要求にともなう開示」記述案

本認証局を含む JPNIC 認証局で取扱う情報に関して、調停、訴訟、仲裁、その他の法的、裁判上又は行政手続きの過程において、裁判所、弁護士、その他の法律上の権限を有する者から任意の開示要求があった場合、当該要求情報に関し開示することができる。

［2.8.6］加入者からの要求に基づく開示

CP/CPS 2.8.6 項では、加入者（一般的には証明書所有者）から、加入者に関する登録情報の開示要求があった場合の対応を記述する。

本認証局の場合、サーバ証明書を除き、JPNIC と利用契約を結んだ、LRA が属する組織から任命された個人に証明書を発行する形態であり、加入者は JPNIC と利用契約を結んだ組織と考えられる。また、その組織は、LRA 管理者に対し、その組織で利用する証明書の管理する権限を与えていると考えられる。ゆえに、開示要求者は証明書にて証明された証明書所有者個人ではなく、LRA 管理者であると考える。

「2.8.6.加入者からの要求に基づく開示」記述案

本認証局では、LRA 管理者から、LRA 管理者の管理する証明書所有者に関連する

情報について、権利、利益を侵害又は侵害するおそれがあるとの申出を受けた場合、LRA 管理者の本人確認及び開示要求の対象情報との関連を確認のうえ、LRA 管理者から受領した証明書所有者に関する情報及び証明書記載情報を開示することができる。

［2.8.7］その他の理由に基づく開示

CP/CPS 2.8.7 項では、前述で示した以外の理由による開示要件を記述する。

一般的には、CP/CPS 2.8.4 項～2.8.7 項で示す要件以外の開示はしない旨の記述又は規定していない場合が多い。

「2.8.7.その他の理由に基づく開示」記述案

本認証局を含む JPNIC 認証局は、証明書検証者からの証明書所有者情報開示要求には、本 CP/CPS 2.8.4 項、2.8.5 項に規定する場合を除いて、応じない。

JPNIC 認証局は、業務の一部を委託する場合、秘密情報を委託先に開示することがある。ただし、その委託契約においては秘密情報の守秘義務を規定する。

5.4.2.9. ［2.9］知的財産権

CP/CPS 2.9 節では、CP/CPS、証明書、名前、ライセンス若しくは関係者からのライセンスの対象となる著作権、特許、商標又は企業秘密等の知的財産権について記述する。

「2.9.知的財産権」記述案

別段の合意がなされない限り、知的財産権の扱いは次に従うものとする。

- JPNIC 認証局の発行した証明書、CRL は JPNIC に帰属する財産である
- 本 CP/CPS は JPNIC に帰属する財産である
- JPNIC 認証局の私有鍵及び公開鍵は JPNIC に帰属する財産である
- JPNIC 認証局から貸与されたソフトウェア、ハードウェア、その他文書、情報等は JPNIC に帰属する財産である

5.4.2.10. ［2.10］個人情報保護方針

RFC2527 において、個人情報保護方針を記述項目としていないが、個人情報保護法の制定、個人情報保護に関する関心の高まりにより、個人情報保護方針について、追

加的に記述する場合が増えている。今回の検討においても個人情報保護方針について記述することが望ましいと考え、JPNIC 認証局における個人情報保護方針として、検討及び記述を行うこととした。

ここでは、

- 個人情報をどのように取扱うのか

を検討することとなる。

日本の場合、個人情報保護法において、個人情報取扱事業者に課せられる個人情報保護義務が定められている。これは、「プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告」の 8 原則（いわゆる OECD8 原則）[5]を考慮したものであり、JPNIC 認証局においても、本法の保護義務を遵守することが望ましい。

現在、JPNIC では、IP アドレスに関連する個人情報の取扱いに関するポリシとして、「JPNIC におけるドメイン名情報および IP アドレスの取扱いについてのポリシー」、「ドメイン名情報および IP アドレス情報の取扱い等に関する規則」、「IP アドレス割り当て等に関する規則」第 18 条を規定している。しかし、JPNIC 認証局においては業務の種類と目的が異なるため、既存のポリシとは別に新たなポリシを規定する必要があると思われる。

ただし、JPNIC 全体におけるプライバシポリシは統一して決められている必要がある。

「2.10.個人情報保護方針」記述案

本認証局を含む JPNIC 認証局は個人情報保護の重要性を認識し、個人情報を次のように取扱う。

（1） 管理責任者を置き、個人情報の適切な管理を行う。

（2） 個人情報を収集する場合、収集目的を知らせた上で、必要な範囲の情報のみを適法かつ公正な手段で収集する。

（3） 証明書所有者から提出を受けた個人情報は、次の目的にのみ使用する。

- IP アドレス管理業務の潤滑な運用を行うため
- 証明書における、本サービス上の責任を果たすため
- その他認証業務に関連した目的のため

[5]OECD8 原則と個人情報取扱事業者の義務規定の対応
http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/pdfs/03.pdf

（4） 証明書所有者の同意がある場合及び法令に基づく場合を除き、個人情報を業務委託先以外の第三者に開示することはしない。業務委託先に開示する場合は、当該業務委託先に対し本書と同等の条件を義務付けるものとする。

（5） 個人情報の管理責任者は、適切な安全対策を講じて、個人情報を不正アクセス、紛失、破壊、改ざん及び漏えい等から保護する責任を持ち、これに努めている。

（6） 証明書所有者自身の個人情報について開示を求められた場合、第三者への個人情報の漏えいを防止するため、証明書所有者自身であることが JPNIC 認証局において確認できた場合に限り、JPNIC 認証局において保管している証明書所有者の個人情報を本人に開示する。また、証明書所有者の個人情報に誤りや変更がある場合には、証明書所有者からの申出に基づき、合理的な範囲で速やかに、不正確な情報又は古い情報を修正又は削除する。証明書所有者は JPNIC 認証局に開示を求める場合、JPNIC 認証局により定められた方法により申請を行うものとする。

（7） JPNIC 認証局は、認証局業務に従事する職員に対して個人情報保護の教育啓蒙活動を実施する。

（8） 証明書所有者の個人情報に関して適用される法令、規範を遵守するとともに、適切な個人情報保護を維持するために、個人情報保護方針を適宜見直し、改善を行う。

5.4.3. ［3］識別と認証

5.4.3.1. ［3.1］新規発行時での利用者の本人確認方法

［3.1.1］サブジェクトに割り当てられた名前の形式

CP/CPS 3.1.1 項では、X.500 識別名、RFC-822 名前（インターネットメールアドレス）及び X.400 名前（X.400 形式のアドレス）といった、サブジェクトに割り当てられた名前の形式について記述する。ITU-T によって証明書の規格として標準化された X.509 では、エンティティを識別するために X.500 に基づいた名前空間（X.500 識別名）を利用する。したがって、証明書形式として X.509 を利用する場合は、X.500 の識別名の規定に従う旨を記述する。ちなみに X.509 は、S/MIME や SSL/TLS 等の多くのセキュリティプロトコルで利用されており、デファクトスタンダードとなっている。

「3.1.1.サブジェクトに割り当てられた名前の形式」記述案

証明書発行者の名前と発行対象の名前は、X.500 シリーズ定義の識別名の規定に従って設定する。

［3.1.2］名前が意味を持つ必要があるか否か

CP/CPS 3.1.2 項では個人名・組織名に意味を持たせる必要性の検討を行う。また、利用者は匿名又は仮名を用いることができるかどうか、そして、もしできるならいかなる名前が匿名希望の利用者に割り当てられ、使用されうるのかを検討する。

証明書の用途が JPNIC のアドレス資源管理業務におけるホストマスタの認証であるため、証明書に記載される名前はホストマスタ個人名及び所属組織名をあらわすものである必要があると思われる。なお、具体的に X.500 識別名の各属性値をどのような値とするかについては、CP/CPS 7 章にて記述するため、本項では大まかな記述にとどめる。

「3.1.2.名前が意味を持つ必要があるか否か」記述案

証明書に記載される名前は、個人名、組織名及びその個人、組織が管理する機器名をあらわすものである必要である。

［3.1.3］様々な名前の形式を解釈するルール

CP/CPS 3.1.3 項では、様々な名前の形式を解釈するルールについて記述する。CP/CPS 3.1.1 項及び CP/CPS 3.1.2 項では名前の形式及びその意味について規定しており、ここではそれらに従って解釈する旨を記述する。

「3.1.3.様々な名前の形式を解釈するルール」記述案

様々な名前の形式を解釈するルールは、X.500 シリーズ定義の識別名の規定に従う。

［3.1.4］名前が一意である必要があるか否か

CP/CPS 3.1.4 項では、名前が一意である必要性について検討を行い、一意とするか否かを記述する。

一意であるとする場合は、名前が一意である範囲を予め規定しておくことが望ましい。一意とする範囲は、例えば、認証局の発行する全証明書内、認証局の発行する同一ポリシの全証明書内、といったように規定する。今回の場合は、一意とする範囲を「本認証局が発行する同一ポリシの証明書内」と規定することが適当と思われる。

また、同一組織の同姓同名の申請者に対して証明書を発行する場合や、証明書更新時に同一主体者に対して新旧の証明書が存在する場合等を想定して、名前を一意とする方法を検討する必要がある。名前を一意とする方法としては、末端の相対識別名（RDN[6]）に EE の名前（commonName）だけでなく、serialNumber 属性を使用して LRA によって一意に管理されるシーケンシャルな番号を追加することが考えられる。

「3.1.4.名前が一意である必要があるか否か」記述案

証明書に記される名前は、本認証局が発行する同一ポリシの証明書において一意とする。

［3.1.5］所有者の名前を決定する際の紛争解決手続き

CP/CPS 3.1.5 項では、証明書に記載される名前に関して認証局が責任を持つのか、また、証明書所有者間で紛争が発生した場合に認証局が関与するのか及び紛争解決の手続きについて検討を行う。

[6] RDN: Relative Distinguished Name

紛争に関しては、認証局は関与せず当事者間で解決するよう規定するのが一般的である。ただし、発行業務を円滑に進めるうえで次のような規定を設けることが必要と思われる。

- 最終的な名前の決定権は認証局が持つこと
- 認証局は紛争を理由に申請を却下できること

また、証明書上の名前は、サイバー空間上で用いられる登録制の名前という点でドメイン名と同様の性格を持つことから、JPNIC の定めるドメイン名紛争処理方針（JP-DRP）[7]に準ずると規定してもよいと思われる。

「3.1.5.所有者の名前を決定する際の紛争解決手続き」記述案

本認証局が発行する証明書に記される主体者名に関する異議申し立てについては、本認証局の責めに帰すべき事由がない場合、本認証局は全ての決定を行う権利を留保する。また、主体者相互間の紛争発生時には、まず当事者間での解決を図るものとし、これにより解決できない場合、本認証局が最終決定者となる。紛争の当事者はこの裁定に拘束される。

［3.1.6］商標の認識・認証・役割

CP/CPS 3.1.6 項では、商標の取扱いについて記述する。なお、日本法において、名前に含まれる可能性のある知的財産権として、商標のほか、商号、ドメイン名等もあり、これらについても本項での記述対象となると思われる。

JPNIC 認証局の場合、想定している証明書の用途においては、名前の誤認混同等の損害による紛争発生の恐れはないと思われる。したがって、本項については規定する必要はないと考える。

「3.1.6.商標の認識・認証・役割」記述案

規定しない。

［3.1.7］公開鍵に対応する私有鍵の所有を証明する方法

CP/CPS 3.1.7 項では、証明書主体者が登録された公開鍵に対応する私有鍵を所持し

[7] JP ドメイン名紛争処理方針
http://www.nic.ad.jp/ja/drp/index.html

ていることを証明しなければならない場合とその方法を記述する。

申請者は、公開鍵に対応する私有鍵を所持していることを、証明書が生成される前に証明しなければならない。私有鍵の所持を証明する方法については、次の点を考慮のうえで検討を行う。

- 鍵ペア生成を行う主体は申請者と認証局のどちらか又は第三者機関を利用するのか
- 証明書の生成はオンラインかオフラインか

鍵ペアを申請者側で生成する場合には、例えば PKCS[8]#10 形式の電子署名が付された証明書リクエストを申請者が送付する方法がある。また、鍵ペアを認証局側で生成する場合には、例えば暗号化された証明書及び私有鍵を PKCS#12 形式で認証局が送付する方法がある。

なお、今回の検討においては、鍵ペアの生成は申請者側で行うこととした。

オンラインで証明書の発行を行う場合は、SSL/TLS 等のセキュアな通信方式を用いる必要がある。オフラインで証明書の発行を行う場合は、上記ファイルを送付するにあたって、本人限定受取郵便等の安全・確実な送付手段の検討が必要である。

「3.1.7.公開鍵に対応する私有鍵の所有を証明する方法」記述案

本認証局は、証明書申請者が私有鍵を所有していることを、PKCS#10 に従った電子署名のされた証明書リクエストの利用、その他本認証局が認めた方法を通じて、確認する。

［3.1.8］サブジェクトの組織（法人）としての識別のための認証要件

CP/CPS 3.1.8 項では、組織の認証を行うための要件を記述する。

組織の認証の例として、設立登記、法的にサインされた会社の決議、社印、その他正式なものと証明された文書がある。また、日本国内の場合には、代表者の印鑑証明がある。

LRA を設置する場合は、LRA の組織認証を行う必要があると思われる。

[8] PKCS: Public-Key Cryptography Standards, http://www.rsa.com/rsalabs/pkcs/index.html

「3.1.8.サブジェクトの組織（法人）としての識別のための認証要件」記述案

本認証局は、LRA に対して組織若しくは団体の認証を行う。LRA としての認証を受けようとする組織若しくは団体は、登記簿及び代表者の印鑑証明、その他本認証局が必要と認める書類を本認証局に提出し、審査を受けなければならない。

［3.1.9］個人の認証要件

CP/CPS 3.1.9 項では、証明書発行時における、個人の本人確認の要件を記述する。

RFC2527 では、検討ポイントとして次の項目をあげている。

- 要求される識別証の数
- どのように認証局若しくは登録局が提供された識別証を認証するか
- 個人は本人認証を行う認証局若しくは登録局に出頭しなければならないか
- どのように個人が組織の一員として本人確認されるか

個人の本人確認を行う目的は、次の 2 点を確認することであるといえる。

- 申請書に記載された名前と一致する個人が実在するか
- その個人が存在するとして、申請者はその個人本人か

したがって、個人の本人確認要件は、架空の人物をでっちあげた不正な申請や、なりすましによる不正な申請を見分けられるものである必要がある。

個人の本人確認の方法には様々なものがあるが、例えば次のようなものがある。

- 認証局（登録局）への出頭並びに 1 種類の写真付き証明書若しくは複数種類の身分証明書の提示を求める
- 1 種類若しくは複数種類の身分証明書を郵送等にて受付け、証明書記載住所に確認書類を送付する
- 個人信用情報機関のような個人情報を収集する組織のデータベースと比較する
- 証明書の申込みをした本人しか知らない機密情報（PIN 等）を提示させる
- メールアドレスを確認する

身元確認に利用することができる身分証明書としては、次のものが考えられる。

- 住民票
- 戸籍謄本
- パスポート

- 運転免許証
- 健康保険証
- 組織（法人）が発行する ID バッヂ

ここで、ID バッヂは社員証のような本人を確認できるものであるとする。

なお、どの程度の要件を規定するかについては、証明書とビジネスモデルに要求される厳密性のレベルを考慮のうえ、適切な要件を検討する必要がある。例えば FBCA では、証明書の保証レベルごとに次の要件が規定されている。

- 初期： 電子メールアドレス
- 基本： データベースとの照合、監督者又は本人による身分証明
- 中位： 登録局又は代理店への出頭及び身分証の提示
- 高位： 登録局又は代理店への出頭及び政府発行の識別書類を最低 2 種類提示（少なくとも 1 種類は写真つきの身分証であること）

LRA を設置する場合、個人の本人確認を LRA にて実施することにより認証局の業務量を削減することが可能である。この場合、LRA における本人確認要件を認証局側で規定するかどうかを検討する必要がある。

本人確認の要件を認証局側で規定する場合、本人確認に関して一定の厳密性を確保することが可能である。ただし、その要件は各 LRA の運営内容を考慮したものである必要がある。また、要件が守られていることを何らかの形で確認する必要があると思われる。一方、本人確認の要件を LRA に任せる場合、各 LRA の実情に合わせた運用が可能となるが、本人確認の厳密性は各 LRA に依存することになるので、本人確認に関して LRA が責任を持つことを規定する必要があると思われる。

ここで、本認証局が本人確認を行うべき申請者数の検討を行う。IP アドレス管理指定事業者ごとに LRA 管理者を 1 名ないし 2 名設置した場合、IP アドレス管理指定事業者の数が 300 程度であることから、LRA 管理者の数は 300 人～600 人である。一方、ホストマスタの人数は 1000 人程度であり、仮にホストマスタについても本認証局が本人確認するとした場合、対象となる人数が 1300 人～1600 人となるため、本人確認に関わる業務量は 3～4 倍になる。業務量の観点から言えば、ホストマスタの本人確認は LRA 業務に関する契約を結ぶ IP アドレス管理指定事業者にて実施することが望ましい。

発行される証明書は、本認証局と IP アドレス管理指定事業者間での申請業務に使われる、クローズドな利用を前提としたものである。証明書の発行対象であるホストマスタは、LRA 組織である IP アドレス管理指定事業者が任命する者であり、その本人確認は IP アドレス管理指定事業者において確実に行うことができると考えられる。したがって、ホストマスタの本人確認を LRA 業務に関する契約を結ぶ IP アドレス管理

指定事業者にて実施するとしても、本人確認における厳密性が損なわれることはないと考えられる。

ホストマスタの本人確認要件については、完全に LRA に任せるのではなく、JPNIC 側で最低限の規定を設けることは必要と思われる。

なお、LRA が行った本人確認及び発行申請等の証明書の管理に関する LRA の責任は、LRA との間で結ばれる契約書に記述されるものと考える。

「3.1.9.個人の認証要件」記述案

LRA 管理者は、証明書発行対象者の証明書発行登録に際し、人事情報 DB、雇用契約等本人を特定できる情報の確認を行う必要がある。また、証明書発行対象者が、LRA 責任者より許可された証明書の発行の許可を受けているものであるかの確認を行う必要がある。

5.4.3.2. ［3.2］通常の更新

CP/CPS 3.2 節では、通常の鍵更新時における本人性確認及び認証に対する要件について述べる。ここで検討すべきポイントは次の 2 点である。

- 本人性確認及び認証の必要性
- 新規発行時の認証要件との違い

証明書の更新を要求できる者は、証明書の新規発行を要求できる者と同様、原則として証明書の所有者本人に限定するべきであると思われる。したがって、第三者による不正な更新要求を排除するために、本人性確認及び認証を行う必要がある。

本人性確認及び認証の要件としては、CP/CPS 3.1.9 項にて規定した要件のほかに、次のようなものがあげられる。

- 証明書中の公開鍵に対応する私有鍵による署名
- 証明書発行時に通知された PIN の提示
- 予め登録しておいた符丁（キーワード等）の使用

私有鍵に危殆化のおそれがないならば、私有鍵による署名ができるのは証明書所有者本人だけであるため、私有鍵による署名付きのメール等により本人性確認を行うことができる。また、証明書発行時に認証局より通知された PIN は、証明書所有者本人だけしか知り得ない情報であるため、PIN の提示により本人性確認をできるものと思われる。また、証明書の申請時等に符丁（キーワード等）を認証局に登録しておき、

証明書所有者が更新要求を行うときにこの符丁を使用して本人性確認を行う方法も考えられる。

上述した 3 つの要件は、いずれも証明書所有者本人だけが、私有鍵、PIN、符丁といった秘密情報を保持していることを前提としている。3 つの要件の中から複数を組み合わせた場合も同様である。万一、これら秘密情報が第三者に知られてしまった場合は、不正に証明書更新が行われるおそれがあるため、これら秘密情報の管理は厳密に行われなければならない。

本認証局においては、証明書は LRA 契約を結んだ IP アドレス管理指定事業者の従業員若しくは LRA が指定した者に発行されるものである。したがって、証明書の発行要求は、IP アドレス申請業務の業務担当者としての任命に基づくものであり、発行対象者である証明書所有者自身の判断によるものではない。ゆえに、あくまでも、LRA である IP アドレス管理指定事業者から IP アドレス申請業務の業務担当者としての任命又は任命継続が必要であり、新規発行時と同様な手続きが必要と考えられる。

「3.2.通常の更新」記述案

新規発行手続きと同様とする。

5.4.3.3. ［3.3］失効後の更新－鍵が危殆化していない場合

CP/CPS 3.3 節では、証明書失効後の鍵更新における本人性確認と認証に対する要件について述べる。ここで検討すべきポイントは次の 2 点である。

- 本人性確認及び認証の必要性
- 新規発行時の認証要件との違い

証明書の更新を要求できる者は、証明書の新規発行を要求できる者と同様、原則として証明書の所有者本人に限定するべきであると思われる。したがって、第三者による不正な更新要求を排除するために、本人性確認及び認証を行う必要がある。

証明書が失効した以上、公開鍵が証明書所有者のものであることを保証しうるものは存在しないことになるため、たとえ危殆化していなかったとしてもその公開鍵に対応する私有鍵が証明書所有者のものであることは保証できない。したがって、本人性確認及び認証の要件としては、CP/CPS 3.1.9 項にて記述される新規発行時の本人確認及び認証の要件と同様とすることが良いと思われる。

本認証局においては、本報告書 5.4.3.1.で検討したように、ホストマスタの認証は LRA にて実施することが望ましく、本認証局ではホストマスタの本人確認等は行わない。この場合、本認証局がホストマスタを認証する手段は証明書以外に存在しないた

め、証明書が失効したならば、新規発行時と同様な手続きが必要と考えられる。

「3.3.失効後の更新－鍵が危殆化していない場合」記述案

新規発行手続きと同様とする。

5.4.3.4. ［3.4］証明書の失効申請

CP/CPS 3.4 節では、失効申請時の申請者本人の認証方法について述べる。

本認証局では、ホストマスタの本人認証を LRA にて実施する。したがって、詳細な手続きは LRA ごとに相違していることが予想される。しかし、本認証局としてのホストマスタの認証方法についての基本方針を記述する必要があると思われる。なお、LRA 管理者から本認証局への EE 証明書若しくは LRA 管理者証明書の失効登録の際には、LRA 管理者証明書による本人確認が行われる必要がある。

「3.4.証明書の失効申請」記述案

LRA 管理者は、ホストマスタから署名付き電子メールによる失効申請を受付けた場合には、その署名を検証する。また署名付き電子メールによらないその他の失効申請の場合は、LRA が事前に定め、本認証局から承認を受けた方法によって申請者の本人確認を確実に行うものとする。

LRA 管理者は、失効申請者の本人確認を行った後、本認証局の定めた方式により、本認証局に失効登録を行うものとする。なお、LRA 管理者の本人確認は本認証局により、LRA 管理者証明書をもって確認される。

5.4.4. ［4］運用上の要件

CP/CPS の 4 章では、様々な運用要件に関して、認証局、証明書所有者に課せられる要件について記述する。

本認証局では、EE 証明書としてホストマスタ証明書とサーバ証明書の 2 種類を発行する。ホストマスタ証明書に関しては、その申請、発行、受理及び失効の各手続きについて CP/CPS 上に明確な規定を行う必要がある。

サーバ証明書に関しては、発行対象となるサーバが JPNIC 内部のものであり、関係者は JPNIC 内部に限定される。したがって、発行に係わる手続きの詳細は JPNIC 内部で検討するものとし、CP/CPS 上では簡潔な記述にとどめるものとする。

なお、LRA 管理者証明書に関しては、運用証明書の一つとして位置づけられるものであるから、本報告書 5.4.1.3.で述べたように JPNIC の運用規定に則って管理・運用されるものとし、CP/CPS 上には運用上の要件を記述しないものとする。

5.4.4.1. ［4.1］証明書の申請

CP/CPS の 4.1 節では、証明書申請を提出することができる者、例えば、証明書のサブジェクト又は認証局等について記述する。

本報告書 5.4.1.3.で述べたように、本認証業務における主たる証明書所有者は IP アドレス管理指定事業者に所属するホストマスタとなるが、本認証局が個々のホストマスタに対して証明書の発行業務をすることは、人的業務量が膨大となり非現実的である。そこで、本認証局においては、ホストマスタ証明書の発行に関する審査、登録及び証明書管理等の業務を各 LRA にて実施することが妥当と思われる。

ホストマスタ証明書の申請を行う者は、LRA 契約を結んだ IP アドレス管理指定事業者の従業員若しくは LRA が指定した者である。彼らは、IP アドレス申請業務の業務担当者への任命に基づいて、LRA 管理者に対して証明書の発行申請を行う。このように、証明書の申請に関わる手続きは、各 LRA において組織的な管理のもと実施されるものである。したがって、証明書の申請に関わる要件は、本認証局が一律に規定するという性格のものではなく、各 LRA においてその業務の実態に即した形で定められるべきものであると考える。

ただし、次にあげる要件は証明書申請における最低限の要件として規定する必要があると思われる。

- 証明書申請者が CP/CPS の内容を承諾していること
- 申請者がアドレス申請業務担当者に任命されていることに関して LRA 管理者が確認を行うこと

LRA 管理者証明書に関しては、LRA 組織の責任者より LRA 管理者として任命された者が、本認証局に対して発行申請を行うものと考えられる。本認証局において、申請を受付けるにあたって確認すべき要件としては、次の項目が考えられる。

- 申請者が組織若しくは団体の責任者より LRA 管理者として任命されていること
- 本人からの申請であること
- 申請内容に虚偽がないこと

サーバ証明書に関しては、サーバ管理者がレジストリシステム責任者に対して発行申請を行い、申請を受けたレジストリシステム責任者が本認証局に対してあらためて発行申請を行う、という手順が考えられる。

「4.1.証明書の申請」記述案

ホストマスタ証明書の申請者は、LRA 管理者により事前に周知された方法に従い、証明書の発行申請を行う。申請者は、証明書の発行申請を行うにあたり、本 CP/CPS の内容を承諾しているものとする。申請者の本人確認及び証明書にて証明される者の各種申請業務担当者としての資格確認審査は LRA 管理者により実施される。

サーバ証明書に関しては、サーバ管理者がレジストリシステム責任者を通じて本認証局に対し発行申請を行うものとする。

5.4.4.2. ［4.2］証明書の発行

CP/CPS の 4.2 節では、証明書の発行と、申請者への発行通知に関する要件を記述する。

前項で述べたとおり、本認証局が、LRA 組織に所属するホストマスタ等に対して証明書を発行する場合には、LRA 管理者からの申請登録に基づき証明書を発行するものとする。証明書所有者の本人確認等は LRA 管理者の責任において実施されるものとし、本認証局では本人確認等は行わないこととする。

ここで、証明書の発行対象としては、役割に対するものと個人に対するものの 2 通りが考えられる。

証明書を役割に対して発行する場合には、担当者が変わっても引き続き証明書を利用することが可能であり、LRA にとってはコストを低く抑えることができる。ただし、鍵ペア生成者と証明書使用者が異なるため、LRA 管理者と担当者との間での権限分離

があいまいになるおそれがある。また、LRA 管理者が全ての証明書を管理することが予想されるため、LRA 管理者が EE 証明書を使用できないことを確実にする仕組みが必要である。また、証明書の不正使用があった場合に、使用した個人を特定するため、証明書使用記録を詳細に記録しておく必要があると思われる。

証明書を個人に対して発行する場合には、担当者が変更になる都度、証明書を申請しなおす必要があり、LRA にとっては発行コストの増加を招くこととなる。しかし、鍵ペア生成者と証明書使用者が同一であるため、LRA 管理者と担当者との間での権限分離を確実に行うことができる。ただしこの場合、LRA 管理者は担当者に対し、私有鍵の管理義務を徹底させる必要がある。証明書の不正使用に対しては、個人と証明書とが 1 対 1 で対応するため個人の特定が容易である。

本認証局においては、証明書所有者の個人特定が容易である点、また、LRA 管理者と証明書使用者との間の権限分離が確実に実施できる点から、証明書は個人に対して発行すべきであると思われる。

また、鍵ペアの生成主体としては、本認証局、LRA 管理者、申請者の三者が考えられるが、本認証局に課せられる業務量、また私有鍵の秘匿性の観点から、申請者自身が鍵ペアを生成することが良いと思われる。

これらの検討に基づき、一連の証明書発行手順（証明書の申請、発行及び受領）の一例を図 5-4 に示す。

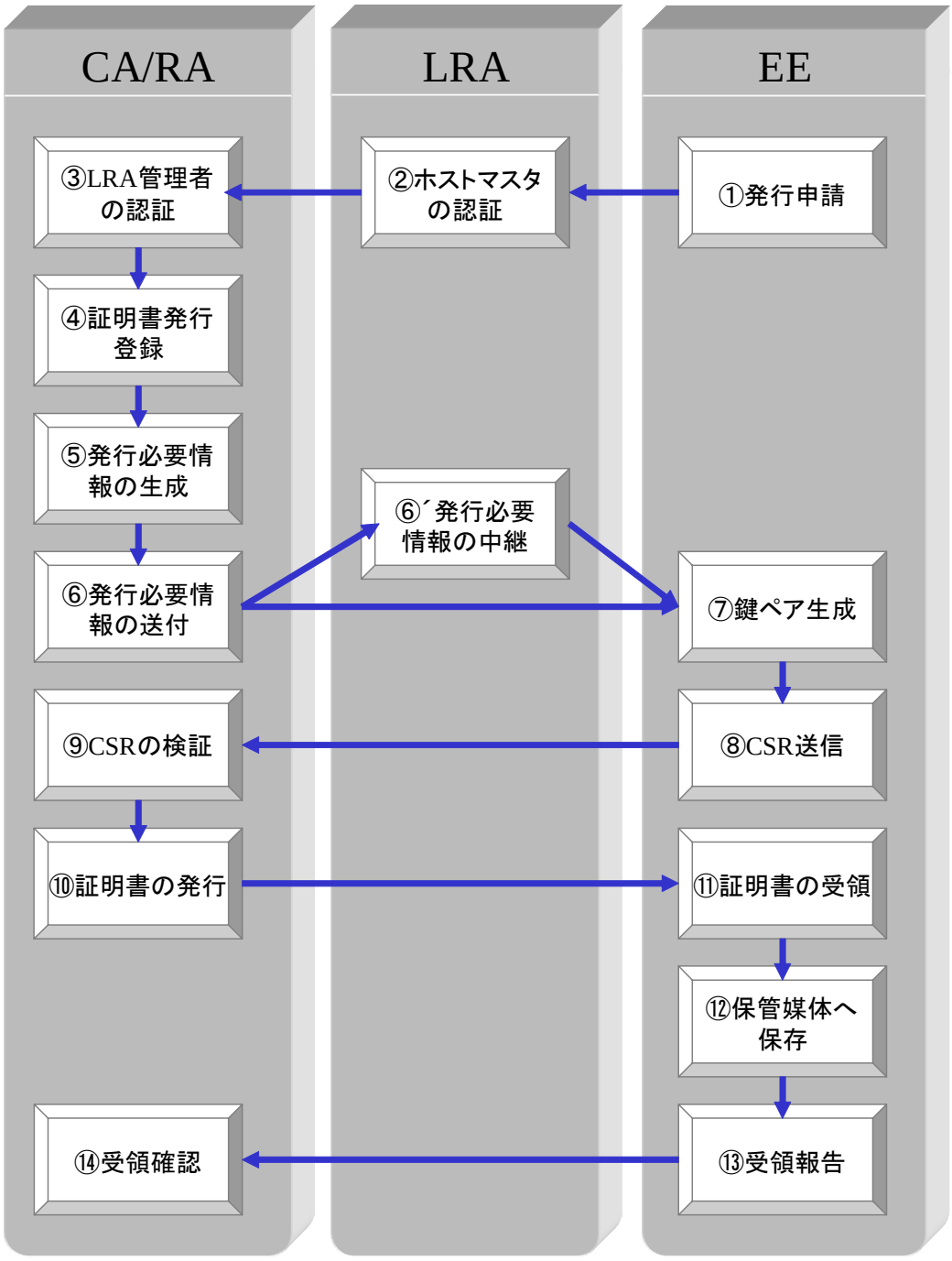


図 5-4　ホストマスタ証明書の発行手順

手順①：ホストマスタは、LRA 管理者に対してホストマスタ証明書の発行申請を行う。

手順②：LRA 管理者は、CP/CPS 3 章で定める個人の認証要件に基づき、ホストマ

スタの本人確認を行い、本認証局に対して証明書の発行申請登録を行う。

手順③：本認証局は、発行申請登録を行った者が真正な LRA 管理者であることの確認を行う。

手順④：本認証局は申請された証明書の発行登録を行う。

手順⑤：本認証局は、証明書の発行要求を受付ける際にホストマスタを識別するための情報を生成する。

手順⑥、⑥´：本認証局は、生成した発行対象者識別情報をホストマスタに送付する。このとき、必要な情報を 2 種類用意し、1 つは直接ホストマスタに、もう 1 つは LRA 管理者経由とすれば、安全かつ確実に情報を渡すことができる。

手順⑦：発行対象者識別情報を受け取ったホストマスタは鍵ペアを生成する。

手順⑧:ホストマスタは、発行必要情報と CSR を本認証局に対して送信する。なお、証明書に記載される情報は、この前の段階で決められている。

手順⑨：本認証局は CSR の検証を行う。

手順⑩：本認証局が証明書を発行する。

手順⑪：ホストマスタが発行された証明書を受領する。

手順⑫：ホストマスタは証明書及び生成した鍵を保管媒体に保存する。

手順⑬：ホストマスタは証明書の内容を確認した後、本認証局に対して受領報告を行う。

手順⑭：本認証局は、申請者からの受領報告をもって証明書の受領を確認する。

上述した一連の手続きは、本認証局側の手続きをシステムによって自動化することにより、証明書の申請から発行、受領までを一貫してオンラインで実施することが可能である。またこの場合、証明書のダウンロードをもって申請者は証明書の受領を完了したとみなすことができ、図 5-4 における手順⑬の受領報告及び手順⑭の受領確認は不要である。

したがって、本認証局側の手続きはシステムによる自動化が望ましいが、詳細はシステム、運用要件の決定によって定められるものである。このため、CP/CPS の記述上は、手作業、システムによる自動処理のどちらになったとしても、問題ない程度の記述内容とする。

LRA 管理者証明書に関しては、本報告書 5.4.4.1.で述べたような要件を確認した後、発行手続きを行う。証明書の発行方式としては、オンラインとオフラインが考えられる。オンラインで発行する場合は、ホストマスタ証明書と同様な発行手続きが考えら

れる。オフラインで発行する場合は、認証局にて鍵ペアを生成し、暗号化された証明書及び私有鍵を PKCS#12 形式でフロッピーに格納するか、若しくは IC カード等の媒体に格納するかして、申請者に送付する方法が考えられる。

サーバ証明書に関しては、レジストリシステム責任者からの発行申請を受けて、本認証局がサーバ管理者に対し証明書を発行するものとする。

「4.2.証明書の発行」記述案

LRA 管理者は、本 CP/CPS 3.1.9 項に基づいて申請者の本人確認及び審査を行い、本認証局に対し申請登録を行う。本認証局は、申請登録を行った LRA 管理者の本人確認を行った後、鍵ペア生成及び証明書発行に必要な 2 種類の情報を生成し、2 系統の経路で申請者へ通知する。証明書はセキュアな通信プロトコルを使用し発行される。

サーバ証明書に関しては、レジストリシステム責任者からの発行申請を受けて、本認証局がサーバ管理者に対し証明書を発行するものとする。

5.4.4.3. ［4.3］証明書の受理

CP/CPS の 4.3 節では、発行された証明書の受領に関する要件を記述することとなる。

証明書の信頼性を確保するために、証明書の受理の際には受領確認を行うことが望ましい。ECOM ガイドライン[9]でも、証明書の送付に関して、受取りの確認ができる手段を利用することを推奨している。また、受領確認がない場合には、証明書を失効させる等の手続きを検討する必要がある。

証明書をサーバからダウンロードする形式であれば、ダウンロードした時点で受領したものとみなすこととができると考えられる。証明書をフロッピーディスク等の記録媒体に格納して送付する場合は、受領確認のメールや証明書の使用をもって受領したとみなすことが可能である。なお、送付の手段としては、開封が検知できる手段を講じたうえで、本人限定受取確認郵便等の確実に申請者本人が受け取ることのできるサービスを利用することが望ましい。

なお、今回の検討では、サーバ証明書を除く EE 証明書の発行はオンラインによる方法を想定している。

一方、申請者は、証明書の受理の際に内容の検証を行うべきである。内容に不備がある場合は直ちに本認証局に通知することが望ましい。

---

9 「認証局運用ガイドライン V1.0 版」、電子商取引実証推進協議会（ECOM）、平成 10 年 3 月

LRA 管理者証明書の場合も同様である。

サーバ証明書の受領確認方法については、上述の検討を踏まえ、証明書の発行方法（オンラインかオフラインか）に応じて適切な方法を別途検討する。

「4.3.証明書の受理」記述案

本認証局は申請者に対し証明書発行に必要な情報を送付する。申請者は送付された証明書発行に必要な情報を用いて、本認証局とセキュアなオンライン通信を行う。本認証局はセキュアなオンライン通信を介して証明書を発行する。申請者がその証明書を受け取った時点で、その証明書を受領したものとする。

なお、申請者は証明書ファイルが自身の PKI 環境で利用可能であること、証明書の記載内容が正しいことを確認しなければならない。

サーバ証明書に関しては、サーバ管理者から本認証局への報告をもって、受領の確認を行うものとする。

5.4.4.4. ［4.4］証明書の停止と失効

CP/CPS の 4.4 節では､証明書の停止及び失効に関する運用要件について記述する。RFC2527 によると、本節で記述されるべき要素には次のものがある。

- 証明書が失効される理由
- 証明書の失効要求の主体者
- 証明書失効要求の手続き
- 失効要求の有効期間
- 証明書の停止理由
- 証明書の停止要求の主体者
- 証明書の停止要求の手続き
- 停止が継続する期間
- CRL の発行頻度
- 検証者における CRL をチェックする要件
- オンラインの失効／ステータスチェックの利用可能性
- 検証者におけるオンラインの失効／ステータスチェックを行う要件
- 利用可能なほかの形態の失効情報
- 検証者におけるほかの形態の失効情報をチェック要件
- 鍵の危殆化に関する特別な要件

上述した各々の要素について、記述すべき内容の検討を行う。

なお、サーバ証明書に関しては、サーバ管理者がレジストリシステム責任者に対して失効申請を行い、申請を受けたレジストリシステム責任者が認証局に対してあらためて失効申請を行うものとする。

［4.4.1］証明書が失効される理由

CP/CPS の 4.4.1 項では、証明書が失効される状況として、証明書を失効させることができる場合及び証明書を失効させなければならない場合について記述することとなる。証明書が失効される状況として、例えば、加入者の雇用期間の終了、暗号トークンの紛失又は私有鍵危殆化のおそれ等の場合がある。

証明書の信頼性を保つために、私有鍵が危殆化した場合、証明書記載事項に変更が生じた場合、虚偽の申請が発覚した場合等は証明書を失効させるべきである。一般的には、次のような失効事由が定められる。

- 証明書所有者の私有鍵が危殆化した（またはそのおそれがある）場合
- 証明書所有者本人の請求があった場合
- 証明書所有者が使用を停止する場合
- 証明書所有者が CP/CPS、その他契約、規則、法律に従わない場合
- 証明書の記載事項が事実と異なる又は変更がある場合
- 認証局の私有鍵が危殆化した（またはそのおそれがある）場合
- 認証局がサービスを停止する場合
- JPNIC 認証局と IP アドレス管理指定事業者との間の LRA に関する契約が解除された場合
- LRA が JPNIC 認証局との契約における義務を果たさなかった場合

また、証明書をサーバからダウンロードさせる場合は、申請者による証明書ダウンロードの失敗も失効事由として検討する必要がある。

LRA 管理者証明書に関しても、同様な要件が該当すると思われる。

サーバ証明書に関しては、次のような失効事由が考えられる。

- サーバの使用を停止する場合
- サーバの私有鍵が危殆化した（またはそのおそれがある）場合
- サーバ管理者の請求があった場合
- サーバ管理者が CP/CPS、その他契約、規則、法律に従わない場合
- 証明書の記載事項が事実と異なる又は変更がある場合
- 認証局の私有鍵が危殆化した（またはそのおそれがある）場合
- 認証局がサービスを停止する場合

「4.4.1.証明書が失効される理由」記述案

LRA 組織に所属する証明書所有者は、LRA が別途定める基準に基づき、LRA 管理者に証明書の失効申請を行わなければならない。

本認証局は、証明書所有者及び LRA 管理者からの失効申請のほかに、次の項目に該当すると認めた場合、証明書の失効処理を行うことができる。

- 本認証局を廃止する場合
- 認証局私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書記載事項が事実と異なる場合
- 証明書所有者の私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書の不正使用、若しくはそのおそれがある場合
- 証明書所有者が本 CP/CPS に違反した場合
- 証明書所有者あるいは LRA が、本 CP/CPS 又はその他の契約、規則、法律に基づく義務を履行していない場合
- JPNIC 認証局と IP アドレス管理指定事業者との間の LRA に関する契約が解除された場合
- その他本認証局が失効の必要があると判断した場合

サーバ証明書に関しては、サーバ管理者は次の項目に該当する場合に本認証局に対し失効申請を行わなければならない。

- サーバの使用を停止する場合
- サーバの私有鍵が危殆化した（またはそのおそれがある）場合

また、本認証局は、サーバ管理者からの失効申請のほかに、次の項目に該当すると認めた場合、サーバ証明書の失効処理を行うことができる。

- 本認証局を廃止する場合
- 認証局私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書記載事項が事実と異なる場合
- サーバの私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書の不正使用、若しくはそのおそれがある場合
- サーバ管理者が本 CP/CPS 又はその他の契約、規則、法律に基づく義務を履行していない場合
- その他本認証局が失効の必要があると判断した場合

［4.4.2］証明書の失効要求の主体者

CP/CPS の 4.4.2 項では、誰が証明書の失効を要求することができるかについて記

述する。失効要求の主体者は、一般に、証明書所有者本人と証明書を発行する認証局である。証明書が役割に対して発行される場合等においては、発行対象の組織の人事部等の場合がある。また、申請者及び証明書所有者が個人で証明書の発行を受けている場合においては、証明書所有者が死亡した場合等において、第三者による申請を受付ける必要がある。ただしこの場合は、失効申請を行う法律上の正式な代理人に対して、事由を明示する書類（死亡届等）の提出を義務付ける等の検討が必要であると思われる。

本認証局の場合、JPNIC に対して各種申請業務を行う役割を LRA 組織が個人に対して任命するものであり、失効申請をできるものは証明書にて証明された個人とは限らないと思われる。LRA 組織が任命しているので LRA 組織の責任者からの指示により、LRA 管理者が失効登録するということも考えられる。今回の検討では、LRA 組織の業務を画一的に決定できないため、CP/CPS 上ではホストマスタ証明書の失効要求は、証明書所有者が LRA 管理者に失効要求を行い、要求を受けた LRA 管理者が、本認証局に対し当該証明書の失効申請登録を行う若しくは LRA 責任者の指示に基づき LRA 管理者が、本認証局に対し当該証明書の失効申請登録を行うものとする。

この他に、前項で述べたとおり、CP/CPS 4.4.1 項に基づいて、本認証局は失効要求を行うことができる。

LRA 管理者証明書に関しては、LRA 管理者本人、組織の責任者、本認証局が失効要求可能な者として想定される。

サーバ証明書に関しては、サーバ管理者と本認証局が失効要求可能なものとして想定される。

「4.4.2.証明書の失効要求の主体者」記述案

証明書の失効要求ができる者は、次のとおりである。

- 証明書所有者
- 証明書所有者の法律上の正式な代理人
- 証明書所有者が所属する組織の LRA 責任者、LRA 管理者
- 本認証局

サーバ証明書に関しては、サーバ管理者と本認証局が失効要求を行うことができるものとする。

［4.4.3］証明書失効要求の手続き

CP/CPS の 4.4.3 項では、証明書失効要求に使用される手続きについて記述する。

検討すべきポイントは、次の点である。

- 失効の申請先
- 失効の申請手段

ホストマスタがホストマスタ証明書の失効申請を行う申請先として、LRA 管理者と本認証局とが考えられる。申請先を LRA 管理者とする場合、LRA 管理者から本認証局に対してあらためて失効申請を行う必要があり、本認証局にて失効処理を開始するまでに遅れが生じる。しかし、失効申請者の本人確認を LRA にて実施するため、本認証局における業務負担は少なく、失効処理そのものは迅速に行うことができる。LRA 管理者の本人確認をシステム化することにより、本認証局における失効処理を自動化することも可能である。一方、申請先を本認証局とする場合、LRA 管理者が不在等のケースでも失効処理を開始することが可能であるが、本認証局において申請者の本人確認を行う必要があり、認証局側の業務負担は大きいものとなる。

証明書の新規発行及び更新時のホストマスタの本人確認を LRA にて実施するならば、失効時におけるホストマスタの本人確認も LRA にて実施することが妥当であり、ホストマスタの失効申請先は LRA 管理者とするべきである。また、本認証局における業務量の観点からも、LRA 管理者を失効申請先とすることが望ましい。

失効申請の手段は、その要求が正当な人物によってなされたものであることを確認できる必要がある。失効の要求を行う手段としては、一般に、署名付きメール、書面、FAX、電話といった手段が考えられる。

次に、これらの手段について検討を行う。

【署名付きメール】

署名検証の結果問題がなければ、本人確認を行う必要なく、失効処理を行ってよいと考えられる。なぜなら、署名ができるのは私有鍵の所有者だけであるから、要求を行っているのは所有者本人であると推定されるからである。仮に第三者が所有者の私有鍵を使って失効要求をしてきたのであれば、第三者が使用している時点で既に鍵は危殆化しているといえるので、本人確認を行うまでもなく当然失効させなければならない。

【書面】

本人確認を行う必要がある。証明書の発行申請時に提出した個人認証情報、若しくはそれと同等な情報の提出を求めなければならない。

【FAX】

失効申請を行う際に、証明書の発行申請時に提出した個人認証情報を同時に送信する等、本人確認を実施できるよう要件を課す必要がある。

【電話】

本人確認が困難であるため、失効要求の手段としては原則不可とするべきと思われる。電話による失効要求を認める場合は、パスワードやキーワードを事前に設定する、コールバックを行う等、何らかの形で本人確認ができる運用を検討する必要がある。

本認証局においては、ホストマスタの失効申請先は LRA 管理者であることが望ましく、したがって、失効申請の手段は、各 LRA において適切な手段を検討するよう規定することが妥当であると思われる。また、本認証局が必要と認める場合には本認証局の判断により失効処理ができる旨を規定することが必要であると思われる。

LRA 管理者証明書に関しては、失効申請先は本認証局となる。申請手段については上述の検討内容と同様なことがいえる。

サーバ証明書に関しては、サーバ管理者がレジストリシステム責任者に対して失効申請を行い、申請を受けたレジストリシステム責任者が本認証局に対してあらためて失効申請を行う、という手順が考えられる。

「4.4.3.証明書失効要求の手続き」記述案

LRA 組織に所属する証明書所有者若しくは LRA 責任者は、LRA 組織により定められた手続きによって、LRA 管理者に失効申請を行う。LRA 管理者は失効要求の正当性を確認のうえ、本認証局に証明書失効登録を行う。

なお、「4.4.1.証明書が失効される理由」にて列挙する項目に該当すると本認証局が認めた場合には、本認証局が自身の判断により証明書の失効登録を行うことがある。

サーバ証明書に関しては、サーバ管理者がレジストリシステム責任者を通じて本認証局に対し失効申請を行うものとする。

なお、サーバ証明書に関しても、「4.4.1.証明書が失効される理由」にて列挙する項目に該当すると本認証局が認めた場合には、本認証局が自身の判断により証明書の失効登録を行うことがある。

［4.4.4］失効要求の有効期間

CP/CPS の 4.4.4 項では、サブジェクトにとって利用可能な失効要求の有効期間について記述する。

一般に、CP/CPS 4.4.1 項で定めた証明書の失効事由に該当することがわかった場合、証明書の信頼性を保つために、CP/CPS 4.4.3 項で定める手続きにより、可及的速やかに失効要求を送信するべきであると考えられる。

LRA 管理者証明書、サーバ証明書に関しても同様である。

また、失効要求を受付けた認証局においても要求を受付けてから処理を完了するまでの時間は、できる限り短いことが望まれる。しかし、処理可能な時間についてはシステム及び運用体制等に依存するものであり、現状では具体的な処理時間が確定しないため、「速やかに失効処理を行う」旨の記述が妥当であると考えられる。運用体制等の確定後、別途、処理可能な時間について定めることとする。

「4.4.4.失効要求の有効期間」記述案

証明書の失効要求は、失効すべき事象が発生した場合、可能な限り速やかに行われるものとする。また、本認証局における証明書の失効処理は、失効申請の受付後、速やかに（[決定後に記述される] 時間以内に）行われる。失効処理の結果は CRL に反映される。

サーバ証明書に関しても、同様である。

［4.4.5］証明書の停止理由

CP/CPS の 4.4.5 項では、証明書が停止される状況について記述する。

認証局において証明書の停止をサポートするメリットとしては、EE の私有鍵に危殆化のおそれがある場合、逡巡することなく証明書を停止することができるため、鍵の危殆化への速やかな対応が可能となる。一方、デメリットとしては、失効手続きとは別に、停止業務及び停止解除業務が発生し、これにともなうシステムの拡張が必要であり、業務量及びコストの増大となる。

本認証局では、JPNIC における業務量増大及びシステム対応を考慮し、証明書の停止はサポートしないこととする。

「4.4.5.証明書の停止理由」記述案

本認証局は、発行した証明書の一時停止を行わない。

［4.4.6］証明書の停止要求の主体者

CP/CPS の 4.4.6 項では、誰が証明書の停止を要求することができるかについて記述する。証明書の一時停止を申請することができる者には、例えば、所有者、LRA 管理者又は本認証局等が考えられる。

CP/CPS 4.4.5 項で定めたとおり、本認証局では証明書の一時停止を行わないため、本項は規定しないものとする。

「4.4.6.証明書の停止要求の主体者」記述案

規定しない。

［4.4.7］証明書の停止要求の手続き

CP/CPS の 4.4.7 項では、証明書停止を要求するための手続きについて記述する。停止要求手続きには、例えば、所有者若しくは認証局からの署名付メッセージ、又は認証局からの電話等がある。

CP/CPS 4.4.5 項で定めたとおり、本認証局では証明書の一時停止を行わないため、本項は規定しないものとする。

「4.4.7.証明書の停止要求の手続き」記述案

規定しない。

［4.4.8］停止が継続する期間

CP/CPS の 4.4.8 項では、証明書の停止が継続する期間について記述する。

CP/CPS 4.4.5 項で定めたとおり、本認証局では証明書の一時停止を行わないため、本項は規定しないものとする。

「4.4.8.停止が継続する期間」記述案

規定しない。

［4.4.9］CRL の発行頻度

CP/CPS の 4.4.9 項では、CRL の発行頻度について記述する。

各種の基準によると、ECOM ガイドライン、電子署名法、WebTrust いずれも、CRL を定期的に発行することを要求しており、週次、日次というように定期的に発行することが望ましい。また、発行間隔はより短い方が、検証者にとって安全性が高いと思

われる。更に、定期的な CRL 発行のほか、証明書の失効が発生した場合には、即時に CRL を更新することが望まれる。

CRL の発行間隔の規定例としては、証明書の種類によらず、全証明書一律 24 時間以内と規定する場合、FBCA-CP における規定のように、証明書の保証レベル別に規定する場合（規定なし、週に 1 度、1 日に 1 度、12 時間に 1 度）等がある。

本認証局においては、発行する証明書の保証レベルは単一であるため、CRL 発行の時間間隔としては適当な時間間隔を 1 種類規定すればよいと思われる。

「4.4.9.CRL の発行頻度」記述案

CRL は証明書失効の有無に関わらず、24 時間以内に更新される。証明書の失効が申請された場合は、失効手続きが完了した時点で更新される。

［4.4.10］検証者における CRL をチェックする要件

CP/CPS の 4.4.10 項では、検証者における CRL をチェックする要件について記述する。

証明書の検証を正確に実施するために､検証者に常に最新の CRL を参照するよう要求する必要があると思われる。また、CRL に関する検討事項として、CRL の公開場所をどこに記載するか、また有効期限の切れた証明書を含めるか、といったことがある。後者については、有効期間内に署名された証明書が、検証者のもとに届いたときには期限が切れていた、といった事態が起こりうるため、有効期限の切れた証明書の失効情報についても、CRL に残しておくこと望ましいと思われる。ただし、これはシステムの容量、機能等により別途、決定されるものと考える。したがって本項では、有効期限の切れた失効情報の CRL 上の扱いについては記述せず、下記のとおり、一般的な記述にとどめることとする。

「4.4.10.検証者における CRL をチェックする要件」記述案

本認証局は、CRL を定期的に更新し、証明書に記載されたリポジトリに公開する。検証者は、証明書の有効性を確認するにあたって、最新の CRL を参照し、当該証明書の失効処理が行われているか否かを確認しなければならない。

［4.4.11］オンラインの失効／ステータスチェックの利用可能性

CP/CPS の 4.4.11 項では、オンラインの失効／ステータスチェックの利用可能性に

ついて記述する。この手段として、例えば、ステータスについての問い合わせを受けられる OCSP（オンライン証明書状態確認プロトコル）等がある。

本認証局では、現段階において OCSP 等の利用を想定していない。このため、次のような記述案とする。

「4.4.11.オンラインの失効／ステータスチェックの利用可能性」記述案

OCSP 等のオンラインの失効／ステータスチェックの機能はサポートしない。

［4.4.12］検証者におけるオンラインの失効／ステータスチェックを行う要件

CP/CPS の 4.4.12 項では、オンラインでの失効／ステータス確認を行うために検証者に課せられる要件について記述することとなる。

しかし、CP/CPS 4.4.11 項で定めたとおり、本認証局においては OCSP 等の機能はサポートしないため、本項は規定しないものとする。

「4.4.12.検証者におけるオンラインの失効／ステータスチェックを行う要件」記述案

規定しない。

［4.4.13］利用可能な他の形態の失効情報

CP/CPS の 4.4.13 項では、利用可能な失効通知の他の形式があれば、その失効通知形式について記述することとなる。

一般的に、CRL、OCSP 以外の形式による失効情報の通知手段としては、証明書検証サーバがある。本サーバの導入には、コスト面及び技術的負担面での検討が必要であり、現段階では導入の予定がされていない。したがって、本項では特に規定しないものとする。

「4.4.13.利用可能な他の形態の失効情報」記述案

規定しない。

［4.4.14］検証者における他の形態の失効情報をチェック要件

CP/CPS の 4.4.14 項では、検証者における他の形態の失効情報をチェックする要件について記述することとなる。

しかし、CP/CPS 4.4.13 項で定めたとおり、現段階では本認証局においては証明書検証サーバ等の利用は想定していないため、規定しないものとする。

「4.4.14.検証者における他の形態の失効情報をチェック要件」記述案

規定しない。

［4.4.15］鍵の危殆化に関する特別な要件

CP/CPS の 4.4.15 項では、証明書の一時停止又は失効が、私有鍵の危殆化によって生じた場合の CP/CPS 4.4 節の規定に関する変更について、一時停止又は失効が他の理由で生じた場合と対比して記述することとなる。

認証局私有鍵の危殆化に関する検討項目として、次の項目があげられる。

- 危殆化時に認証局は何を行うか
- 危殆化のおそれに対して何を行うか
- 危殆化時の通知を、誰が、誰に、いつ、どのように行うのか

本認証局の私有鍵が危殆化した場合は、本認証局が発行した全証明書の信頼性が確保できなくなるため、直ちに全証明書を失効させ、CRL を発行すべきと思われる。

本認証局の私有鍵の危殆化のおそれに対しては、JPNIC 認証局内に専門チームを設置し、対策を検討するよう規定することが望まれる。

JPNIC 認証局以外の関係者が本認証局の私有鍵の危殆化に気づいた場合は、直ちに、JPNIC 認証局に通知するよう義務付けることが望まれる。

なお、相互認証を行う場合には、相手認証局が JPNIC 認証局に対して発行する証明書を無効にしてもらうよう相手認証局に要請する旨の記述が必要となると思われるが、今回は相互認証を行わないため、記述は不要とする。

「4.4.15.鍵の危殆化に関する特別な要件」記述案

本認証局は、本認証局の私有鍵に危殆化又は危殆化のおそれがある場合は、直ちに全ての証明書の失効処理を行い、CRL に登録し、証明書所有者に対してメール等の手

段で本認証局の私有鍵の危殆化等の事実と証明書失効の通知を行う。

5.4.4.5. ［4.5］セキュリティ監査の手続き

CP/CPS の 4.5 節では、認証局のセキュアな環境を維持するために実装されるイベント記録と監査システム及びセキュリティ監査に関して記述することとなる。RFC2527 によると、本節で記述されるべき要素には次のものがある。

- 記録されるイベントの種類
- 監査ログが処理、若しくは監査される頻度
- 監査ログの保存期間
- 監査ログの保護
- 監査ログのバックアップ手続き
- 監査ログの収集システム
- 監査イベントを引き起こした者への監査活動の通知
- セキュリティ対策の見直し（脆弱性評価）

次に、前述の各々の要素について、記述すべき内容を検討する。

［4.5.1］記録されるイベントの種類

CP/CPS の 4.5.1 項では、セキュリティ監査のために記録されるイベントの種類を記述することとなる。

本項は、認証局の完全性を証明するために必要な項目であり、本来であれば取得可能な全てのログを記録することを規定することが望ましいが、認証局のレベルに応じて、妥当なイベントを選択することが必要である。

既存の CP/CPS では、記録するイベントの種類の記述に大きな格差がある。最多のものは FBCA-CP[10]である。FBCA-CP では、4 種の保証レベルごとに、記録すべき具体的なイベントを規定しており、初期レベルの保証レベルでは 14 種類のイベントを記録するとしているが、高位の保証レベルでは、52 種類ものイベントを記録することとしている。ただし、実際に記録できるイベントの種類は認証局システムに依存する場合が多いため、CP/CPS 上は具体的なイベントを記述するのではなく、多少幅をもたせ、「認証局私有鍵の操作、システムの起動･停止、データベースの操作、権限設定の変更履歴、証明書の発行、証明書の失効、CRL/ARL の発行等の操作ログを記録する」程度に記述するのが妥当と考えられる。本考察では一般的な記述にとどめ、認証局システムが明確になった時点で特記すべきイベントがあれば、記録すべきイベントを取

[10]連邦ブリッジ認証機関（Federal PKI BCA）X.509 CP V1.3R

捨選択のうえ、CP/CPS の中で明示することが望まれる。

「4.5.1.記録されるイベントの種類」記述案

本認証局システム上で起こったイベントは、それが手動、自動であるかにかかわらず、日付、時刻、イベントを発生させた主体、イベント内容等が記録される。

認証局システムにおける誤操作、不正操作の検知及び運用の正当性を証明するために必要な監査ログとして、次の操作について履歴を記録する。

- 認証局の私有鍵の操作
- システムの起動･停止
- データベースの操作
- 権限設定の変更履歴
- 証明書の発行
- 証明書の失効
- CRL の発行
- 監査ログの検証　　等

また、次のような認証設備室内のネットワーク機器並びに監視システムについても履歴を記録する。

- 認証設備室への入退室に関する記録
- 認証局設備への不正アクセスに関する記録　　等

［4.5.2］監査ログが処理、若しくは監査される頻度

CP/CPS の 4.5.2 項では、4.5.1 項で記録することを定めたイベント、つまり監査ログをどの程度の頻度で処理又は監査するかについて記述することとなる。

監査ログの処理頻度については、CP/CPS の記述上は必須とはいえないが、実際の運用上は具体的に定めるべきである。運用体制及び運用コスト等に影響されるため、運用体制及び運用コストを検討のうえ、最終決定するものとして、本考察では一般的な記述にとどめる。

FBCA-CP においては、証明書の保証レベルごとに少なくとも 1 週間に一度又は 1 ヶ月に一度を検査頻度としている。その他の、CP/CPS では、「セキュリティ監査は少なくとも毎月行われる」、あるいは「監査ログを定期的に精査する」といった記述もある。

この例のように、監査ログの監査頻度を少なくとも 1 ヶ月に一度というように定めることが望ましいが、検査の頻度は、運用体制又は運用コスト等により左右され

CP/CPS 上で明確に記述するのは困難である。当面、具体的な期間を記述するのではなく、定期的に行うとするのが妥当であると考える。具体的な処理頻度については、運用上の総合的な検討のうえ、後日の決定とする。

「4.5.2.監査ログが処理、若しくは監査される頻度」記述案

本認証局は、監査ログ及び関連する記録を定期的に精査する。

［4.5.3］監査ログの保存期間

CP/CPS の 4.5.3 項では、4.5.1 項で記録することを定めたイベントを、オンサイト若しくはオフサイトにて、どの程度の期間、保存しておくのかに関して記述することとなる。

オンサイト／オフサイト各々の保管方法と保管期間を適切に定める必要がある。

- 各種基準においては、明確な保管方法・保管期間について要求していない。
- PKI Assessment Guidelines[11] （以下、PAG と呼ぶ）においては、運用体制の特性にもよるが、数ヶ月から数年間は監査ログがいずれかの場所で保存されるのが適当だとしている。
- FBCA-CP では、「監査ログは、少なくとも 2 ヶ月間オンサイトで保有される」としている。
- その他、既存の CP/CPS では「監査ログは、最低 6 週間は認証局サーバ内に保持され、その後、外部記憶媒体に最低 10 年間は保持される。」程度の記述もある。

前述のように、オンサイト保管としてサーバ内に 1～2 ヶ月程度、オフサイト保管として外部記録媒体に数年～10 年程度は保管するとするのが望ましいと考えられる。

監査ログは、誤操作、不正操作の検知、記録のほかに、運用の正当性を証明する記録とも考えられるので、帳簿等の重要書類と同様な取扱が必要と思われる。したがって、電子署名法が要求する帳簿の保管期間と同様に 10 年間（オフサイト保管）は保存しておくこと望ましい。ただし、保管地、保管環境、コスト等によって、再度の検討が必要と思われるため、本考察では、一般的な記述にとどめることとする。

[11] PKI Assessment Guidelines, PAG v0.30,Public Draft for Comment,June 18,2001,American Bar Association

「4.5.3.監査ログの保存期間」記述案

監査ログは、最低 2 ヶ月間は認証局サーバ内に保持される。その後、外部記憶媒体に最低 10 年間は保管される。また、認証設備室への入退室に関する記録や不正アクセスに関する記録は、次回の監査終了まで保存されるものとする。

［4.5.4］監査ログの保護

CP/CPS の 4.5.4 項では、記録した監査ログの保護に関して記述する。具体的には、監査ログにアクセスすることが出来る者、並びに監査ログの削除や改ざんができないようにするための要件等を記述することが望ましい。

検討項目としては、次のものがある。

- 誰が監査ログを見ることができるか
- 監査ログの改ざんに対する防護
- 監査ログの削除に対する防護

ECOM ガイドラインでは「監査情報は、そのアクセス権限を明確にし、不正アクセスによる情報の改ざん、消去、漏えい等に対して保護し、必要に応じ適正な期間内に提供可能な状態で保管しておく必要がある。」としている。

WebTrust では、「3.10.12 システム監査ツールへのアクセスは、不正使用や誤用を防ぐように防御する。」としている。

ある民間認証局では、「漏えい、改ざん、滅失及び毀損等の防止処置を施し、監査証跡を保管管理する。」としている。

本認証局の場合も、監査ログのアクセスについては一定の制限を設けるべきである。また、監査ログの改ざん及び削除に対する保護方法について、具体的に規定することが望ましいが、本認証局に係わる施設設備の検討及び決定がされていないので詳細を規定することはできない。したがって、現段階では前述の基準及び CP/CPS 記述例にあるような、一般的な記述にとどめることとする。

「4.5.4.監査ログの保護」記述案

本認証局は、JPNIC によって認可された人員のみが監査ログファイルにアクセスすることができるようにするために権限者を定め、許可されていない者が閲覧、修正又は削除をすることから保護する。監査ログは、改ざん防止対策を施し、かつ改ざん検出を可能とする。また定期的に監査ログのバックアップを外部記憶媒体に取得し、適切な入退室管理が行われている室内において、施錠可能な保管庫に保管する。

［4.5.5］監査ログのバックアップ手続き

CP/CPS の 4.5.5 項では、バックアップが必要な監査ログがある場合、そのバックアップ手続きを記述することとなる。具体的には、バックアップの手順と保管場所に関して、いつ、何に対してバックアップを取り、どこに保管するか、を記述することが望ましい。通常の認証局では、監査ログは、定期的に外部記憶媒体に対してバックアップをとり、安全な施設に保管するとするのが一般的である。また、詳細なバックアップ手続きについて CP/CPS 上に規定できない場合は、バックアップ手順を別途定めて、それに従う旨を記述することでも良いと考えられる。

「4.5.5.監査ログのバックアップ手続き」記述案

監査ログは、認証局サーバのデータベースとともに、事前に定められた手続きに従い、外部記憶媒体に定期的にバックアップがとられ、それらの媒体は安全な施設に保管される。

［4.5.6］監査ログの収集システム

CP/CPS の 4.5.6 項では、監査ログの収集システムが、認証局システムの内部のものであるか、外部のものであるかについて記述することとなる。監査ログは、認証局システムで行われた操作との一貫性が保証されなければならない。監査ログの収集は、認証局システム内にあった方がシステム全体として一貫した収集が可能であり、より安全であるといえる。したがって、監査ログの収集システムは、認証局システムに内在している事が望ましい。しかし、監査ログの収集機能は認証局システムに依存し、前述のように内在させる事ができない場合もあるため、認証局システム構成の決定時点で、再度見直すこととする。

「4.5.6.監査ログの収集システム」記述案

監査ログの収集機能は認証局システムの一機能とて内在しているものとし、セキュリティに関する重要な事象を監査ログとして収集する。

［4.5.7］監査イベントを引き起こした人への監査活動の通知

CP/CPS の 4.5.7 項では、監査イベントの記録に際し、イベントを引き起こした者に対して警告等の通知をするか否かについて記述することとなる。

何らかの操作イベントを引き起こした者に対して、その操作を中止させ、あるいは抑制をさせる必要があるのであれば、何らかの通知を行うための方針を記述することとなる。

しかし、監査イベントを記録していることはセキュアな認証局システムにおいては当然のことと考えられ、あえて監査イベントを記録し保存していることを特別に通知する必要性はないものと思われる。また、全ての監査イベントについて、引き起こした者へ通知することはシステム的対応が困難であり、CP/CPS 上、明確に記述することは難しい。更に、何らかの通知方針を CP/CPS に記述することは、どのような場合に監査ログが記録されるかを外部の攻撃者に知らせることとなり、セキュリティ上も好ましくないと考えられる。前述から、監査イベントを引き起こした者に対して通知しないと記述するのが妥当であり、かつ一般的な記述であると思われる。

「4.5.7.監査イベントを引き起こした人への監査活動の通知」記述案

本認証局では、監査ログの収集を、事象を発生させた人、システム又はアプリケーションに対して通知することなく行う。

［4.5.8］セキュリティ対策の見直し（脆弱性評価）

CP/CPS の 4.5.8 項では、本認証局関連システムの脆弱性及び脅威の評価について記述することとなる。

認証局システムでは、そのセキュリティを確保するために定期的に、運用面及びシステム面におけるセキュリティ上の脆弱性を評価して、必要に応じて関連システムの更新並びに CP/CPS 及び関連する文書の見直しを行うことが望ましい。

しかし、CP/CPS のような開示文書上に、脆弱性の評価内容を具体的かつ詳細に記述することは、外部の攻撃者に対して関連システムの脆弱性の評価方法を詳細に知らせることとなり、セキュリティ上は好ましくないと考えられる。したがって、詳細な記述はすることなく、適宜、関連システムの脆弱性評価と見直しを行う旨の記述にとどめるのが妥当であると考えられる。

「4.5.8.セキュリティ対策の見直し（脆弱性評価）」記述案

本認証業務において用いるハードウェア及びソフトウェアは、監査ログ検査等によるシステム面及び運用面におけるセキュリティ上の脆弱性評価に加え、最新の実装可能なセキュリティ・テクノロジの導入等、セキュリティ対策の向上を図るものとする。

5.4.4.6. ［4.6］記録の保管

CP/CPS の 4.6 節では、認証局における一般的な記録の保管・保持のポリシについて記述することとなる。RFC2527 によると、本節で記述されるべき要素には次のものがある。

- アーカイブ記録の種類
- アーカイブの保存期間
- アーカイブの保護
- アーカイブのバックアップ手順
- 記録に対するタイムスタンプを付ける要件
- アーカイブの収集システム
- アーカイブ情報の入手、検証の手続き

次に、上に示した各要素について、記述すべき内容を検討する。

［4.6.1］アーカイブ記録の種類

CP/CPS の 4.6.1 項では、アーカイブされる記録の種類、例えば、全ての監査データ、証明書申請情報及び証明書申請を補う書類等について記述することとなる。

アーカイブする記録の種類は、主に認証局システムで生成され、電子データとして保存されるもの及び紙媒体（書類）として保存されるものに分類される。電子署名法対応の認証局の場合では、記録されるアーカイブの情報には次のような物が網羅されると考えられる。また、記録の保存にあたっては、情報の漏えい、改ざん、滅失の防止措置を施し、紙媒体については原本を保存するものとする。

- 発行された全ての証明書及び CRL（電子データ）
- CP/CPS、証明書所有者規程及びその変更に関する記録（電子データ、紙媒体）
- 認証業務に従事する者の責任及び権限並びに指揮命令系統に関して記載した文書及びその変更に関する記録（電子データ、紙媒体）
- 証明書の発行、失効時に提出を受ける申請書（電子データ、紙媒体）
- 利用者の真偽の確認のために提出を受けた書類（電子データ、紙媒体）
- 証明書の発行、失効申請に対する諾否を決定した者の氏名の記載した書類及び、申請に対して承諾をしなかった場合においてその理由を記載した書類（電子データ、紙媒体）
- 証明書の発行、失効申請の扱いに際し認証局で記録される電子データ
- 認証業務の手順に関して記載した書類。またその変更に関する記録（電子データ、紙媒体）

- 認証業務の一部を他に委託する場合においては、委託契約に関する書類の原本（紙媒体）
- セキュリティ監査対象イベント（CP/CPS 4.5 節）（電子データ）
- 監査の実施結果に関する記録及び監査報告書（電子データ、紙媒体）
- 手続き的管理（CP/CPS 5 章）で規定する権限付与等の記録（電子データ、紙媒体）
- 認証業務用設備の維持管理に関する記録（電子データ、紙媒体）
- 認証業務における、事故に関する記録（電子データ、紙媒体）
- 帳簿書類の利用及び破棄に関する記録（電子データ、紙媒体）

本認証局の場合、電子署名法対応等所定の基準へ準拠することが求められていないため、上に示したほど CP/CPS 上、詳細にアーカイブ記録を定める必要はないものと考えられる。また一方、前述の情報が電子データで記録されるか、紙媒体で記録されるかは、認証局関連のシステム構成に依存する。現段階では、システム構成が決まっていないため、システム構成決定後に、前述のアーカイブ情報を参考にし、どの情報を記録するのか及び各々の情報を電子データ又は紙媒体として記録するのかについて確定していく必要がある。現段階の記述案では、一般的にどのような記録がアーカイブされるのかについて記述する。

「4.6.1.アーカイブ記録の種類」記述案

本 CP/CPS 4.5.1 項に規定する監査ログに加えて､本認証局は次の記録を保存する。

【認証局システムに記録されるイベント】

- 認証局の署名用鍵ペアの生成
- システムからの加入者の追加や削除
- 証明書の発行や取消を含めた鍵の変更
- RA 担当者権限の追加や変更、削除
- 証明書有効期限の変更等、ポリシの何らかの変更

【紙媒体又は外部記憶媒体として保存するもの】

本認証局は次に掲げる運用関連記録のアーカイブを維持、管理する。

（ ）内は保管期間

- 本 CP/CPS、証明書所有者同意書及びその変更に関する記録（その作成又は変更を行ってから 10 年間）
- 認証業務に従事する者の責任及び権限並びに指揮命令系統に関して記載した文書及びその変更に関する記録（その作成又は変更を行ってから 10 年間）

- 証明書の発行、失効時に提出を受ける申請書（該当する証明書の有効期間の満了日から最低 10 年間）
- 利用者の真偽の確認のために提出を受けた書類（該当する証明書の有効期間の満了日から最低 10 年間）
- 証明書の発行、失効申請に対する諾否を決定した者の氏名の記載した書類及び、申請に対して承諾をしなかった場合においてその理由を記載した書類（該当する証明書の有効期間の満了日から最低 10 年間）
- 認証業務の一部を他に委託する場合においては、委託契約に関する書類の原本（その作成を行ってから 10 年間）
- 監査の実施結果に関する記録及び監査報告書（その作成を行ってから 10 年間）

［4.6.2］アーカイブの保存期間

CP/CPS の 4.6.2 項では、アーカイブされる記録の保存期間について記述することとなる。アーカイブの保存期間の目安として、FBCA-CP では、証明書の保証レベルごとに最低限、次の保存期間を設けることとしている。

- 初期（Rudimentary）レベル　　：7 年 6 ヶ月
- 基本（Basic）レベル　　：10 年 6 ヶ月
- 中位（Medium）レベル　　：20 年 6 ヶ月

本認証局の場合、1 つの証明書保証レベルでの運用を検討しており、証明書の保証レベルごとにアーカイブの保存期間を設定する必要はないと考えられる。

もう一つの目安として、電子署名法における帳簿書類の保存期間が法定されており、証明書申請者本人の署名等のある書類等の原本を、証明の有効期間終了後 10 年間保存しなければならないとしている。

前述から、アーカイブの保存期間については、電子署名法及び FBCA-CP の基本（Basic）レベルを意識して、10 年程度としておくのが妥当であると考えられる。

一方で、個々のアーカイブの種類ごとに、保存期間（起点、終点）に差異を設けるかどうかを検討する必要がある。通常、証明書のライフサイクルに関する記録のアーカイブについては、証明書の有効期間満了日を起点とし最低 10 年間とするのが一般的である。また、監査関連のアーカイブについては、監査終了後から次回の監査日までとするのが一般的である。

本項の記述方針としては、個々のアーカイブ対象の保存期間を明示するために、CP/CPS 4.6.1 項において、アーカイブ対象物を規定すると同時に各々の保存期間を記述するのが望ましい。

アーカイブの保存期間については、保存に要するシステムの容量及び運用コスト等との兼ね合いも問題となる。今後、関連システムの構成等の決定後に、システム容量及びコスト等を勘案のうえ、アーカイブ期間を決定することとする。

「4.6.2.アーカイブの保存期間」記述案

認証局サーバデータベースの履歴及び監査ログファイルの履歴は、最低 10 年は保存される。紙媒体及び外部記憶媒体の保存期間に関しては本 CP/CPS 4.6.1 項のとおりである。

［4.6.3］アーカイブ記録の保護

CP/CPS の 4.6.3 項では、アーカイブ記録の保護のために、アーカイブを見ることができる者、アーカイブの変更・削除に対する防止策及びアーカイブが保存される媒体の品質低下に対する防止策等について記述することとなる。

監査ログの保護については、CP/CPS 4.5.4 項にて検討したとおりである。その他のアーカイブ記録に対しても、記録へのアクセスについては一定の制限を設けるべきであり、また、アーカイブの改ざん防止及び削除防止の方法について具体的に規定することが望ましい。しかし、現段階では、本認証局に係わる施設設備の検討及び決定がされていないため、詳細な規定することはできない。したがって、現段階では次のとおり、一般的な記述にとどめることとする。

「4.6.3.アーカイブ記録の保護」記述案

アーカイブデータには、アクセス制御を施すとともに、改ざん検出を可能とする措置を講ずる。アーカイブデータのバックアップは、定期的に外部記憶媒体に取得し、JPNIC の管理部門が許可した以外の者がアクセスできないように、制限された施設に保存される。また、その施設は、温度、湿度、磁気等の環境上の脅威からも保護される。

［4.6.4］アーカイブのバックアップ手順

CP/CPS の 4.6.4 項では、アーカイブのバックアップ手順について記述することとなる。具体的には、アーカイブのバックアップ間隔、バックアップ先、紙等の保管手続きについて記述することが望ましい。

通常、アーカイブのバックアップは日次／週次／月次等、定期的な間隔で、外部記憶媒体に格納されるとするのが一般的である。

また、紙媒体のアーカイブバックアップについては、書類のコピーを施設外の災害復旧施設において保管することが望ましいが、運用上の負荷が極めて高くなるため、CP/CPS 上の記述をしないことも考えられる。ただしこの場合、紙媒体の原本保管を厳重に行う必要があると考えられる。

「4.6.4.アーカイブのバックアップ手順」記述案

認証局サーバデータベースに対して、自動的かつ定期的にサーバ上にバックアップを行う。更に、認証局サーバシステム、監査ログとともに定期的に外部記憶媒体に格納する。

［4.6.5］記録に対するタイムスタンプを付ける要件

CP/CPS の 4.6.5 項では、アーカイブされる種々のデータに対してタイムスタンプを付ける要件について記述することとなる。

認証局においては、例えば、いつ証明書の失効申請が行われたのか、いつ証明書が失効されたのか等の、正確な時刻を記録する必要がある。このため、記録する種々のデータに対し、レコード単位でそのイベントが起きた正確な時刻を記録することが望まれる。また、アーカイブに限定されないが、情報に記録される時間に差異があった場合、情報の整合性が損なわれるので、認証局関連システムの時計は、正確に記録するため時刻の同期化を行う必要があると思われる。そのためには少なくとも、認証局システムの時計は何らかの時刻源から時刻を取得し、各種サーバ間にて時刻の同期化を行う必要がある。更に厳格な時間管理が必要となる場合、又は対外的に法的な時刻証明を必要とする場合は、時刻認証局（TSA：タイムスタンプ局）の利用も考えられる。

現段階では、本認証局において、時刻認証局を利用した時刻証明を行うかどうかの結論はでていない。また、JPNIC におけるレジストリ関連業務においては、トランザクションの前後を厳密に争うことはないと考えられる。したがって、GPS 等を時刻源として、NTP により認証局サーバ等全てのシステム間の時刻を同期させれば十分であると考えられる。将来的に、各種ログデータの原本性保証の要求がある場合には、時刻認証局（TSA）の利用も検討すべきである。

本考察では、次の記述案にとどめ、時刻認証局の利用又は GPS を時刻源としたシステムの構成等が決定された時点で、再度見直しをかけるものとする。

「4.6.5.記録に対するタイムスタンプを付ける要件」記述案

本認証局において使用される認証局システムは、正確な時刻源から時刻を取得し、

NTP（Network Time Protocol）を使用し認証局システムサーバの時刻同期を行ったうえ、本認証局内で記録される重要情報に対してレコード単位にタイムスタンプを付するものとする。

［4.6.6］アーカイブの収集システム

CP/CPS の 4.6.6 項では、CP/CPS 4.6.1 項に規定するアーカイブ記録の収集システムを内部的にするか（システムに内在しているか）、又は外部的にするか及び自動収集できるアーカイブは何かについて記述することとなる。

監査ログに対する収集システムについて、CP/CPS 4.5.6 項にて記述したのと同様に、アーカイブの収集についても、監査ログの収集との一貫性を保持するために、認証局サーバシステムに内在していることが望ましい。ただし、自動収集機能に関してはシステム構成に依存すると考えられるため、システム構成決定後に再度見直すものとする。現段階では、監査ログの収集システムと同等の記述をするものとして、次に記述案を示す。

「4.6.6.アーカイブの収集システム」記述案

認証局サーバデータベース用の履歴収集システムは、認証局サーバシステムに内在している。監査ログファイル用の履歴収集システムについては、本 CP/CPS 4.5.6 項に記述のとおりである。

［4.6.7］アーカイブ情報の入手、検証の手続き

CP/CPS の 4.6.7 項では、アーカイブの情報を入手し、検証する手続きについて記述することとなる。

本認証局においても、適切な権限者がアーカイブを入手し、定期的に可読性の検証を行うことが必要と考えられる。この検証間隔については、可能であれば「年 1 回」というように具体的に定めることが望ましいが、認証局の運用の詳細が確定していない段階では「定期的に」とのみ記述するのが妥当である。

「4.6.7.アーカイブ情報の入手、検証の手続き」記述案

アーカイブデータは、厳格に管理された区画からアクセス権限者が入手し、外部記録媒体の可読性確認を定期的に行う。また必要に応じ、アーカイブデータの完全性及び機密性の維持に留意し、新しい媒体へ複製を行う。保管期間の過ぎた古い媒体は破棄する。

5.4.4.7. ［4.7］鍵の更新（切り替え）

CP/CPS の 4.7 節では、認証局による鍵更新にともなって、認証局の利用者に対して新しい公開鍵を提供する手続きについて記述することとなる。これらの手続きは、現在の鍵を提供した手続きと同じものにすることができる。また、新しい鍵を、古い鍵を使用して署名された証明書の中で認証することもできる。

本認証局の場合、新しい認証局公開鍵は、JPNIC ルート認証局から証明書の発行を受け、次のいずれかの方法により利用者へ提供するものと考えられる。

- セキュアなプロトコルを使って広く公開する方法（Web サイト又はその他のリポジトリにより公開）
- オフラインによる利用者への送付（フロッピーディスクその他の記録媒体に格納し、LRA 管理者経由での手渡）
- オンラインによる利用者への送付（電子メール等への添付）

新しい認証局公開鍵の提供方法を決めるうえで、次の考慮が必要であると考えられる。

- リポジトリ等への公開の場合、証明書の改ざん防止措置等を検討しなければならないこと
- 本認証局の場合、認証局公開鍵の更新は現状 8 年[12]間隔程度と予想され、頻繁に配布するものではないこと
- 今回の認証業務が、適用範囲の限定された環境での運用であることを考慮すると、新しい公開鍵をフロッピーディスク等の外部記憶媒体に格納し、アウト・オブ・バンドで直接配布するのが便利、かつ安全であること

前述の点を考慮すると、本認証局においては、新しい公開鍵は、リポジトリ等上で公開せずに、記録媒体に格納して、LRA 管理者経由で配布することが適当であると考えられる。

ただし、鍵の更新については、認証システム及び利用ユーザのアプリケーションに依存するものと思われる。システムによっては、認証局の鍵の更新を意識せずに利用することも可能である。システム的な対応がない場合は、新規発行時における認証局の公開鍵の提供と同様な手続きになると思われるため、現段階では新規発行時の提供方法と同様の手続きとし、システム構成等の決定後に、再度見直すこととする。

---

[12] 認証局鍵ペアは、その有効期間（10 年）より、EE 証明書の有効期間（2 年）の分だけ前に、更新するのが一般的である。

「4.7.鍵の更新（切り替え）」記述案

本認証局の私有鍵は、その有効期間の残りが EE 証明書の最大有効期間よりも短くなる前に、JPNIC はその鍵による新たな EE 証明書の発行を中止し、新たな認証局鍵ペアを本 CP/CPS 6 章に定める方法で生成する。新たな公開鍵は JPNIC ルート認証局から証明書の発行を受け、本 CP/CPS 6.1.4 項に定めた方法と同様に配布を行う。

5.4.4.8. ［4.8］危殆化と災害からの復旧

CP/CPS の 4.8 節では、危殆化又は災害が起きた際の通知及び復旧手続きに関連する要件について記述することとなる。RFC2527 によると、本節で記述されるべき要素には次のものがある。

- ハードウェア、ソフトウェア又はデータが破壊された場合の対処
- 証明書を失効しなければならない場合の対処
- 私有鍵が危殆化した場合の対処
- 災害等発生時の設備の確保

次に、上に示した各々の要素について、記述すべき内容を検討する。

［4.8.1］ハードウェア、ソフトウェア又はデータが破壊された場合の対処

CP/CPS の 4.8.1 項では、コンピュータの資源、ソフトウェア及び／又はデータが破損した、あるいは破損のおそれがある場合に用いられる復旧手続きについて記述することとなる。

本項では、認証局システムに係わる事故の際の報告先、担当窓口及び手続き等を規定することが望ましいが、一般的に、これら事故時の対応については、CP/CPS 上、詳細な記述をすることが困難と考えられる。JPNIC における前述したような事故の際の体制及び詳細な手続き等については別途、検討するものとして、ここでは一般的な記述案をあげる。

「4.8.1.ハードウェア、ソフトウェア又はデータが破壊された場合の対処」記述案

JPNIC 認証局は、ハードウェア、ソフトウェア又はデータが破壊された場合、事前に定められた復旧計画に従い、バックアップ用のハードウェア、ソフトウェア及びデータにより、速やかに復旧作業に努める。

［4.8.2］証明書を失効する場合の対処

CP/CPS の 4.8.2 項では、EE の公開鍵が失効された場合に使用される復旧手続きについて記述することとなる。

本項では、EE の公開鍵が失効された場合の復旧手続きとして、具体的に、どのように安全な環境が再構築されるのか、どのように新しい公開鍵が EE に提供されるのか、どのように EE は再認証されるのか、について記述することが望ましい。現段階では、EE の証明書を失効した場合に、再度証明書を発行する場合には、初期発行時と同様の手続きをとるとするのが、妥当な対処と考えられる。本考察では、証明書を失効し再発行する場合の一般的な記述案にとどめることとする

「4.8.2.証明書を失効する場合の対処」記述案

発行した証明書の失効処理にあたっては、その失効の取消は行わない。証明書を失効した証明書所有者に対し、再度証明書を発行する場合は、あらためて発行手続きを行う。

［4.8.3］私有鍵が危殆化した場合の対処

CP/CPS の 4.8.3 項では、エンティティの鍵が危殆化された場合に用いられる復旧手続きについて記述することとなる。

本項では、主体の私有鍵が危殆化した場合の復旧手続きとして、前項と同様に、安全な環境がどのように再構築されるのか、サブジェクトはどのように再認証されるのか、等について記述することが望ましい。

認証局の私有鍵が危殆化した場合は、発行した各種証明書の失効手続き、認証局私有鍵の再生成及び各種証明書の再発行手続きをとるのが一般的である。

一方、EE の私有鍵が危殆化した場合は、CP/CPS 4.4 節で定めた手続きをとるのが一般的である。

「4.8.3.私有鍵が危殆化した場合の対処」記述案

認証局私有鍵が危殆化した場合は、予め定めた計画に基づいて認証業務を停止し、次の手続きを行う。

- ホストマスタ証明書、サーバ証明書等の失効手続き
- 認証局私有鍵の廃棄及び再生成手続き
- ホストマスタ証明書、サーバ証明書等の再発行手続き

また、証明書所有者の私有鍵が危殆化した場合は、本 CP/CPS 4.4 節において定める手続きに基づき、証明書の失効手続きを行う。

［4.8.4］災害等発生時の設備の確保

CP/CPS の 4.8.4 項では、自然災害又はその他の災害後、事業継続を保証するエンティティの能力について記述することとなる。

一般の基準によると、WebTrust では、事業継続計画の定期的レビュー及びテスト、バックアップ装置及びバックアップデータの遠隔地保管等を実施することとしている。

本認証局においても、証明書の重要性、補償レベル等に応じて事業継続計画を策定し、バックアップ機器、バックアップデータの遠隔地保管等を考慮する必要があると思われる。しかし、現段階では、事業継続計画及び災害復旧サイトの詳細検討までには至っておらず、詳細確定後に CP/CPS に改善を加えるものとする。

本考察では、本認証局に関連する全てのデータのバックアップを維持し、災害等発生時には予備機等を確保して、事業の継続に努めるものとして、次に記述案を示す。

「4.8.4.災害等発生時の設備の確保」記述案

災害等により JPNIC 認証局の設備が被害を受けた場合は、JPNIC は予備機を確保しバックアップデータを用いて運用の再開に努める。

5.4.4.9. ［4.9］認証局の終了

CP/CPS の 4.9 節では、認証局、登録局の終了と終了の通知のための手続きに関する要件について記述することとなる。

各種基準によると、ECOM ガイドラインでは、認証業務を終了する場合には、そのスケジュールと手続きを決め、その内容を利用者等直接その影響を受けるものに通知する必要があるとしている。利用者への通知スケジュールに関して、署名法では、認証業務終了の 60 日前までに行う必要があるとしている。

本認証局においても、認証業務の終了に際しては、周到な準備と相応の期間が必要であることを認識しておくべきであり、業務終了より相応の期間前までに、関係者に通知することを記述すべきと思われる。

「4.9.認証局の終了」記述案

JPNIC において本認証局の認証業務の終了が決定した場合は、業務終了の事実、並びに業務終了後の本認証局のバックアップデータ、アーカイブデータ等の保管組織及び開示方法を業務終了［日は決定後に記述される］日前までに証明書所有者及び検証者に告知し、所定の業務終了手続きを行う。

5.4.5. ［5］建物・関連設備、運用、要員のセキュリティ管理

CP/CPS 5 章では、認証業務を遂行するために必要とされる非技術的なセキュリティ統制を規定する。非技術的なセキュリティ統制とは、物理的・手続き的・人物的なセキュリティ統制のことである。

これらの規定の検討を行う際に ECOM 作成の認証局運用ガイドライン V1.0、特定認証業務の認定に係る調査表[13]（以下、調査表と呼ぶ）、WebTrust for CA（これらを以下、CP/CPS 策定参考文書と呼ぶ）を参考にする。

なお現段階では、JPNIC 認証局の設置場所等が決まっておらず、また CP/CPS 上に詳細な要件を記述することはセキュリティ上好ましくないため、本報告書上の記述案は、最低限必要と思われる基本的内容についてのみ記述するものとする。

5.4.5.1. ［5.1］建物及び関連設備管理

CP/CPS 5.1 節の各項中では、認証局に要求される物理的な管理に関連することが規定される。

［5.1.1］施設の位置と建物構造

CP/CPS 5.1.1 項では、認証局を設置する建物の立地条件や認証局を設置する区画の条件を物理的なセキュリティの面から規定する。

CP/CPS 策定参考文書によると、次の項目が主な要件としてあげられている。

- 建物の立地条件としては、周辺の火災、電磁界、水害、落雷、空気汚染の自然災害等を受けにくい場所であること
- 建物の条件としては、（準）耐火構造、耐震構造であること
- 認証局を設置する区画条件としては、障壁による区分け、区画への入場資格確認等が行われていること

その他、調査表の中では次のことも規定されている。

- 認証局の所在を公開又はそれを示唆する情報を提示しないこと

前述の内容は、重要な電子計算機設備が設置される建物・区画に関する記述であり、最低でもその概要を記述する必要があると考えられる。

---

[13] 電子署名及び認証業務に関する施行規則及び指定調査機関による特定認証業務調査表

「5.1.1.施設の位置と建物構造」記述案

本認証局に係わる重要な設備については、周辺の火災、電磁界、水害、落雷、空気汚染の自然災害、地震等の影響を受けにくい建物内に設置し、本認証局の設備は、障壁により区画され、入場資格確認等が可能な収納システムの表示のない室に設置する。

［5.1.2］入退管理

CP/CPS 5.1.2 項では、認証局が設置されている区画への入退出を管理・監視するために整備する必要がある環境を規定する。

CP/CPS 策定参考文書によると、次の項目が主な要件としてあげられている。

- 許可された者のみが入室可能となる入退出管理を行うこと
- 認証設備室が無人になる場合にセンサ・カメラによる監視を行うこと
- 窓、扉には防犯装置を講ずること
- 入退出に関する管理規定を整備し、管理責任者を決定すること
- 部外者の認証局区画内への入退出は権限を有する複数名による同行とその日時の記録を行うこと

その他、ECOM ガイドラインや調査表では次の項目も要件として規定されている。

- 2 名以上の生体認証によって入室が可能となること
- 不正な入出操作が行われた際に警報が発せられること
- 監視カメラは死角が出来ないように設置すること
- 装置、情報、ソフトウェアは許可なしで持ち出し出来ないこと

また次のような要件をあげている CP/CPS もある。

- 認証設備室は、天井から床まで設置された 2 重若しくは 3 重の隔壁を持ち、窓がない又は窓に効果的な安全対策が施されている領域に構築すること

「5.1.2.入退管理」記述案

本認証局の認証設備室は、事前に定められた本人の特定及び入室権限の確認を可能とする入退室管理が行われ、監視カメラによる記録が行われる。また認証設備室への立入は、入室権限を有する複数人が同時に操作することにより行われる。

［5.1.3］電源及び空調設備

CP/CPS 5.1.3 項では、認証局運用に必要な電源確保と空調設備設置の要件を検討する。

CP/CPS 策定参考文書によると、次の項目が主な要件としてあげられている。

- 停電対策（UPS、自家発電設備、その他技術的方法から選択）を講じること
- 適切な室内空調を安定して提供できること

その他、ECOM ガイドラインには次の項目が規定されている。

- 電圧、周波数等の安定した電力供給が可能なこと

JPNIC 認証局においても、停電による電力断絶や空調不良によるシステムの温度上昇は業務の停止、システムの故障を起こす要因となるため対策が必要である。

「5.1.3.電源及び空調設備」記述案

JPNIC 認証局における設備は、停電に対する対策を行う。また空調設備は、各種使用する機器に悪影響を与えないよう維持管理される。

［5.1.4］水害及び地震対策

CP/CPS 5.1.4 項では、認証業務を妨げないように水害対策と地震対策の要件を検討する。

CP/CPS 策定参考文書によると、次の項目が主な要件としてあげられている。

- 認証局システムの停止が生じないよう対策が講じられていること
- 災害への対策を規定した文書が作成されていること
- 通常想定される規模の地震によるシステムの転倒及び構成部品の脱落等を防止するための耐震措置が講じられていること

その他、調査表では、水害の防止措置として、直上階からの漏水対策等についても記述されている。

「5.1.4.水害及び地震対策」記述案

漏水等水害に対する措置を講ずる。また地震等により JPNIC 認証局システム等の

機器が転倒、脱落を起こさないように措置を講ずる。

［5.1.5］防火設備

CP/CPS 5.1.5 項では、認証局に設置すべき防火設備の要件について検討する。

ECOM ガイドラインや調査表では次の項目が要件としてあげられている。

- 電源設備や空調設備の防火措置を講ずること
- 認証設備室は防火区画内に設置されること

その他、一般的な CP/CPS では、次のような規定内容も記述されている。

- 自動火災報知器及び消化装置が設置されていること

JPNIC 認証局では前述した項目に従って対策を講じることを CP/CPS 上に規定すれば、一般的な要件レベルを満たしていると考えられる。

「5.1.5.防火設備」記述案

JPNIC 認証局の設備は、防火壁によって区画された防火区画内に設置される。また防火区画内では電源設備や空調設備の防火措置を講じ、火災報知器や消火設備の設置を行う。

［5.1.6］記録媒体の保存

CP/CPS 5.1.6 項では、記録媒体の安全な保管方法を検討する。

調査表で規定されている主な内容として次の項目があげられている。

- 加入者の真偽確認に際して知り得た情報の目的外使用の禁止及び帳簿書類の記載内容の漏えい、滅失又は毀損の防止措置を講じていること

帳簿書類の記載内容の漏えい、滅失又は毀損の防止措置に関しては、紙書類にて保存する情報と電子媒体にて保存する情報を選別・決定し、その保存方法・利用手続きに関してなんらかの規定書上に記載しなければならないと思われる。また電子媒体にて保存される場合には、適切な媒体を検討しなければならないと思われる。

また CP/CPS 上に詳細を記載するかどうかは別として、記録媒体の保管場所を検討しなければならないと思われる。

複製した記録媒体を認証局設備が設置されている場所以外の遠隔地にて保管する場合には、稼動している認証局の所在地にて大規模な災害が発生しても情報の滅失は最小限に抑えられる一方、稼動している認証局から遠隔の保管場所までの安全な輸送方式を確保する必要があり、そのための輸送費用と保管場所確保のためのコストが発生する。

一方、遠隔地保管を行わない場合には、複製した記録媒体の確実な保護のために、各種災害にも耐えられる堅牢な保管設備が必要である。堅牢な保管設備を確保したとしても、稼動している認証局の所在地にて大規模な災害が発生した場合には情報が滅失する可能性があると思われる。そのため、認証局の復旧が困難となり、その結果業務停止となる可能性がある。

稼動している認証局が設置されている場所での記録媒体の保管以外に、稼動している認証局が設置されている地域以外の場所にも保管する方が、災害発生後の復旧を保証する可能性が高くなると考えられる。

「5.1.6.記録媒体の保存」記述案

アーカイブデータ、バックアップデータを含む認証業務を行う上で必要な情報は、適切な入退管理が行われた室内の保管庫に保存されるものとする。

［5.1.7］廃棄物の処理

CP/CPS 5.1.7 項では、情報や設備を破棄する場合の方法を検討する。

WebTrust では、次の項目があげられている。

- 破棄前に機密情報の有無を確認すること
- 機密情報を含む記録媒体は破棄前に完全初期化又は物理的破壊を行うこと

廃棄物からの情報漏えいを防ぐために、前述の項目に対して具体的な対応方法を手順書等に明確に定めておく必要があると思われる。ただし、詳細な対応方法については、公開されることが前提である CP/CPS に記載する必要はないと考えられる。認証局の私有鍵に関する事項は、CP/CPS 6.2.9 項に従うものとする。

「5.1.7.廃棄物の処理」記述案

機密扱いとする情報を含む書類・記録媒体の廃棄については、情報の初期化・裁断等、事前に定められた方法に従い適切に廃棄処理がなされる。

［5.1.8］オフサイト・バックアップ

CP/CPS 策定参考文書の中では、CP/CPS 5.1.8 項に関して特に詳細な規定は行われていない。ただし、サービスレベルを高めるためにはオフサイト・バックアップを用意することが望ましいため、その要件を検討する。なお、記録媒体のオフサイト・バックアップについては前述の CP/CPS 5.1.6 項にて記述している。

オフサイト・バックアップを行うには相当のコストが要求されるため、事業内容を踏まえてその必要性を検討する必要があると思われる。オフサイト・バックアップを行う場合には、稼動している認証局で障害が発生してもオフサイトで引き続きサービス提供を行うことが可能である一方、設備維持や管理要員のコストが増大し、また、サイト間のデータ転送時のセキュリティ対策を厳格に行う必要もある。

一方、オフサイト・バックアップを行わない場合には、特別なコストは要しないものの、稼動している認証局で障害が発生した場合には、復旧完了までサービスを提供することができないという問題が発生する。

コストの点を考慮しないとすると、JPNIC 認証局業務の継続性を保証するためにオフサイト・バックアップを行うことが望ましいと思われる。ここで、オフサイト・バックアップの準備レベルとして次の 3 種があると思われる。

- コールドサイト

JPNIC 認証局の代理運用を可能とする施設のみを事前に確保しておく状態である。代理運用に必要な機器は代理運用が必要となった時点で調達を行うと共に、バックアップからのデータ復旧を行うことによって代理運用可能となる。

- コールドスタンバイ

バックアップからのデータ復旧によって、JPNIC 認証局の代理運用を行うことが可能なだけの設備が整えられている状態である。

- ホットスタンバイ

コールドスタンバイの状態に加え、電源が既に投入されており、バックアップからのデータ投入によっていつでも代理運用可能な状態である。又は JPNIC 認証局システム以外の情報はリアルタイムに更新が行われ、JPNIC 認証局の鍵及び JPNIC 認証局システムの復旧のみによって JPNIC 認証局の代理運用が可能となる状態である。

JPNIC が提供するサービスレベルと許容されるコストをもとに、どの方法を採用するか継続検討課題とし、現段階では規定しないこととする。

「5.1.8.オフサイト・バックアップ」記述案

規定しない。

5.4.5.2. ［5.2］手続き管理

CP/CPS 5.2 節では、認証局を運営するにあたって業務実施上の手続き方法を検討する。

一般的な CP/CPS では、主な規定として次の項目があげられている。

- 認証業務の手順の細目を明確に事務取扱要領に規定し、実施していること
- 業務内容、手順等の変更に伴う事務取扱要領の改訂に関する手順等を明確に規定し、実施していること

またより詳細な規定内容として考えられる項目が、ECOM ガイドラインや WebTrust にて次のように規定されている。

- 役割に応じたアクセスコントロールが行われていること
- 重要な情報にアクセス可能な部署は他から隔離されること
- アクセス権限は定期的にレビューすること
- 事故を予防するために内部牽制が行われること
- 部署外からの監査等のチェック機能が働くこと
- 事故発生時にはその発生源が特定できること

［5.2.1］信頼される役割

CP/CPS 5.2.1 項では、認証業務を担う各役割の決定と要件を規定する。

CP/CPS 策定参考文書によると、次の項目が主な要件としてあげられている。

- 認証局の安全性と信頼性を長期的に確保すること
- 情報セキュリティ技術やシステム監査等の専門家を配置しておくこと
- 指揮命令系統、責任及び権限が文書に明確に定められ、それに従って業務が実施されること
- 全ての就業者の役割に応じて教育・訓練計画等が策定され、それに従って実施されること
- 指揮命令系統、責任及び権限に変更がある場合、規定等の変更手順等が明確に定められ、それに従って変更が行われ、変更に係る教育・訓練が実施されること

一般的にはこの節ではどのような役割があるかについて検討され、教育・訓練については CP/CPS 5.3 節以降で述べられている。ここで、各役割を定めるにあたってセキュアな運用を保証するために、各役割に認められる権限を保有する者を確実に分離する必要がある。権限分離の考慮点としては次のものがある。

- システム操作の承認権限と承認に基づくシステム操作権限を持つ者の分離
- システム管理操作権限と発行・失効操作権限を持つ者の分離
- 運用に携わる権限の付与者と被付与者の分離

前述 3 項目を考慮した役割案を表 5-4 に示す。

表 5-4 名称とその役割

			役割名称又は用語	役割又は用語の説明
			運営委員会	・監査報告確認、承認 ・認証局運営責任者への監査指摘事項対応指示 ・JPNIC 認証局の運営方針の決定 ・証明書ポリシ、運用ポリシ及び運用ポリシ変更の最終承認 ・認証局運営責任者の任命・解任等 ・その他、重要な事項の協議及び決議
運営組織			認証局運営責任者	・サービス及び運用組織の統括 ・監査指摘事項への対応統括 ・運用管理者の任命・解任 ・システム変更及び運用ポリシ変更の承認 ・非常時対応等の指揮、監督
	運用組織		運用管理者	運用組織の統括 ・運用担当者の任命・解任 ・運用担当者の教育計画策定、実施 ・運用担当者の入室権限付与 ・運用担当者の作業報告確認 ・認証局私有鍵の活性化操作、非活性化操作の立会い（生成、削除操作ではない） ・非常時の対応指示 ・作業報告書、貸出簿等、運用記録の保管・管理等 ・その他運用全般の管理 （認証局の運用で使用するパスワード、PIN の管理等を含む。）
		運用担当者	ログ検査者	・監査ログ、入退室ログ等の検査
			鍵管理者	・キーセレモニ時の認証局鍵生成作業立会い ・認証局鍵廃棄時の立会い ・バックアップ私有鍵の管理
			セキュリティ管理者	・認証局システムのセキュリティ設定、変更 ・キーセレモニ時の RAO の登録、発行
			認証局管理者	・認証局サーバ、ディレクトリサーバ等認証局システムの運用管理
			登録局管理者	・証明書発行、失効の登録作業 ・登録局の管理運営

			審査者	・証明書（LRA 管理者証明書）発行申請の受付け ・証明書発行にかかる審査 ・承認者への、LRA 管理者証明書の発行依頼
			承認者	・審査結果の承認 ・発行登録作業承認
			保守員	ネットワーク技術者、システム技術者及び監視技術者の総称 ・ネットワークの設定、維持管理等 ・システム技術サポート（認証局システム、RA システム等）、サーバの設定・維持管理等 ・監視（不正侵入検知連絡、システム状況監視等）
			ベンダー保守員	・各種機器の故障等の対応
	ローカル登録局		ローカル登録局	・証明書を発行する組織とは異なる別組織であり、RA 業務において、本人の確認・審査、証明書発行申請処理及び証明書失効申請処理を行う組織 ・JPNIC 認証局の場合、IP アドレス管理指定事業者が、LRA となる
			ローカル登録局責任者	・IP アドレス管理指定事業者の中における、LRA 業務の責任者 ・LRA 管理者の任命・解任を行う。
			ローカル登録局管理者	・IP アドレス管理指定事業者の中で、ホストマスタのメンバー管理と認証及びホストマスタ証明書の発行申請操作を行う

前述の役割の位置付け案を図 5-5 に示す。

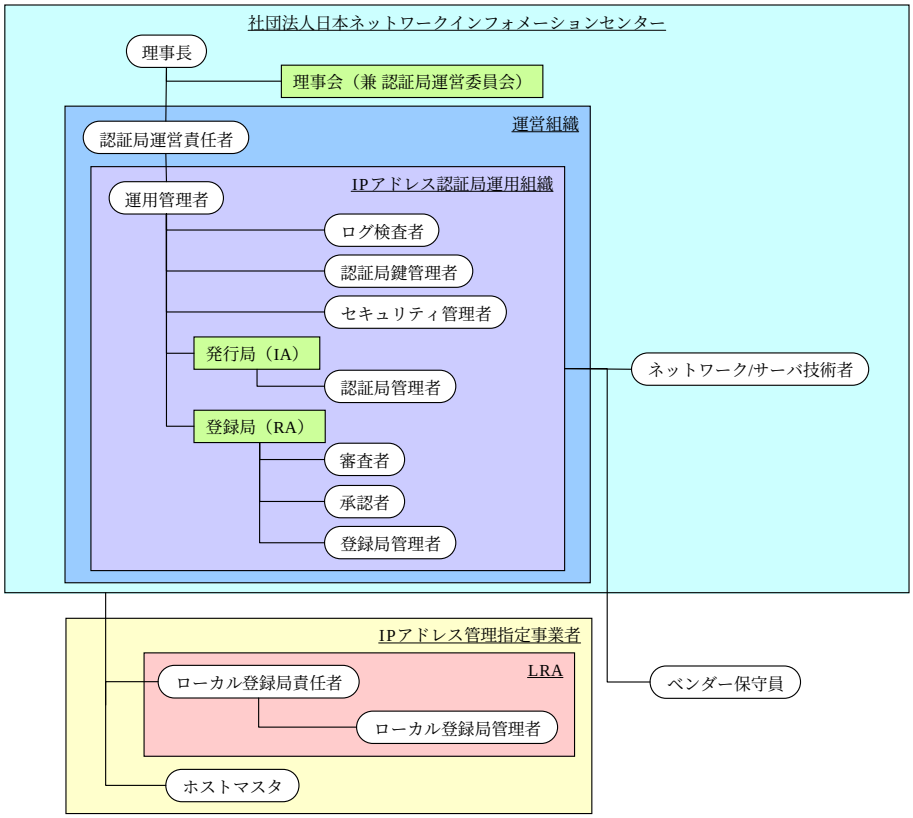


図 5-5　各役割の位置付け

前述の役割の中で兼務可能と考えられる役割について次のように検討した。

- ログ検査者

運用管理者にシステム操作権が認められていないため、ログ検査者は運用管理者と兼務可能と思われる。

- セキュリティ管理者

キーセレモニ時以外はほとんど作業が発生しないため、JPNIC 認証局システムや入退室管理システムによっては複数人操作を前提に、運用管理者と CAO 又は RAO による合同操作にて兼務を可能と思われる。

- 審査者

RAO に申請の承認権がないため、審査者と承認者が兼務されない場合に限って審査者は RAO と兼務可能と思われる。

- 承認者

運用管理者にシステム操作権が認められていないため、承認者がシステム操作を伴わない場合に限って運用管理者と兼務を可能と思われる。

「5.2.1.信頼される役割」記述案

次の表 5-4 に JPNIC 認証局の運営、運用上の役割を示す。

（表 5-4 が記述される）

［5.2.2］必要とされる人数

CP/CPS 5.2.2 項では、各業務において業務を遂行するために必要な要員数に関して規定する。

調査表では各役割の必要要員数を次の視点で検討している。

- 業務遂行上に必要な知識・経験を有している技術者を認証業務に必要数配置する
- 認証設備室への入室が許可される者の指定と登録及び複数人による入室を実施する

また認証業務における重要操作は、複数人で行われるのが通例であると思われる。

これらを考慮した具体的な要員数の構成案を次に示す。

案 1：

- JPNIC 認証局システムサーバの操作は複数人の CAO によって行う
- JPNIC 認証局設備の保守、JPNIC 認証局機器等の故障時対応等において、JPNIC 認証局システムサーバの設置室へ入室権限者以外が入室する必要がある場合は、必ず入室権限者の立会いを必要とする
- JPNIC 登録局の端末を用いた発行・失効操作等は、複数人の RAO によって行う

案 2：

- JPNIC 認証局システムサーバの操作は、複数人の CAO 又は運用管理者立会いのもとで CAO が行う
- JPNIC 認証局設備の保守、JPNIC 認証局機器等の故障時対応等において、

JPNIC 認証局システムサーバの設置室へ入室権限者以外が入室する必要がある場合は、必ず入室権限者が立会いを必要とする

- JPNIC 登録局の端末による発行・失効操作等は、複数人の RAO 又は運用管理者の立会いのもとで RAO が行う

調査表にて認証設備室への立入には複数人を要求しているように、認証局での端末操作のような情報へアクセスする操作に関しても、信頼性を確保するために複数人による相互牽制が可能な人員配置を行う必要があると考えられる。次に、これらの検討をふまえ、各役割の必要要員数を検討した。

案 1 に基づき、兼務を行わない場合と行う場合の必要要員数を考慮すると、次の二つが考えられる。

表 5-5　案 1 に基づいて兼務を行わない場合の必要要員数

役職	人数	備考
運用管理者	2 名	正・副各 1 名。
ログ検査者	2 名	正・副各 1 名。
鍵管理者	2 名	正・副各 1 名。 鍵生成等は CAO、RAO との合議により行う。
セキュリティ管理者	2 名	正・副各 1 名。
CAO	3 名	正 2 名、副 1 名。
RAO	3 名	正 2 名、副 1 名。
審査者	2 名	正・副各 1 名。
承認者	2 名	正・副各 1 名。
人数合計	18 名（正 10 名・副 8 名）	

表 5-6　案 1 に基づいて兼務を行う場合の必要要員数

役職	人数	備考
運用管理者	2 名	正・副各 1 名。
ログ検査者	0 名	運用管理者が兼務。
鍵管理者	2 名	正・副各 1 名。 鍵生成等は CAO、RAO との合議により行う。
セキュリティ管理者	0 名	運用管理者と CAO 又は RAO との合議により行う。
CAO	3 名	正 2 名、副 1 名。
RAO	3 名	正 2 名、副 1 名。
審査者	0 名	RAO が兼務。

承認者	0 名	運用管理者が兼務。
人数合計	10 名（正 6 名・副 4 名）	

案 2 に基づき、兼務を行わない場合と行う場合の必要要員数を同様に考慮すると、次の二つのように考えられる。

表 5-7　案 2 に基づいて兼務を行わない場合の必要要員数

役職	人数	備考
運用管理者	2 名	正・副各 1 名。
ログ検査者	2 名	正・副各 1 名。
鍵管理者	2 名	正・副各 1 名。 鍵生成等は CAO、RAO との合議により行う。
セキュリティ管理者	2 名	正・副各 1 名。
CAO	2 名	正・副各 1 名。 合議操作は運用管理者との合議により行う。
RAO	2 名	正・副各 1 名。 合議操作は運用管理者との合議により行う。
審査者	2 名	正・副各 1 名。
承認者	2 名	正・副各 1 名。
人数合計	16 名（正 8 名・副 8 名）	

表 5-8　案 2 に基づいて兼務を行う場合の必要要員数

役職	人数	備考
運用管理者	2 名	正・副各 1 名。
ログ検査者	0 名	運用管理者が兼務。
鍵管理者	2 名	正・副各 1 名。 鍵生成等は CAO、RAO との合議により行う。
セキュリティ管理者	0 名	運用管理者と CAO 又は RAO との合議により行う。
CAO	2 名	正・副各 1 名。 合議操作は運用管理者との合議により行う。
RAO	2 名	正・副各 1 名。 合議操作は運用管理者との合議により行う。
審査者	0 名	RAO が兼務。
承認者	0 名	運用管理者が兼務。
人数合計	8 名（正 4 名・副 4 名）	

権限分離や複数人制御は、いかに誤用・不正を抑制するかを目的としていると考えられる。できる限り詳細に、権限の分離、操作の複数人制御を行うことが望ましいが、システムのアクセスコントロール設定機能、入退室管理システム機能等により左右される要素が多く、論理的セキュリティや物理的セキュリティと共に検討を行った上で運用体制の決定を行う必要があると思われる。

今回の検討では、一連の業務が単独で行えないことを基本とし、承認者と操作者の分離、権限付与者と付与対象者の分離、役割ごとの操作権限の分離、重要操作の複数人制御を行うものとした。今後も、厳しい条件である案 1 をベースに詳細な運用体制、役割の検討を進める必要があると考えられる。

「5.2.2.必要とされる人数」記述案

- JPNIC 認証局システムサーバの操作は複数人の CAO によって行う
- JPNIC 認証局設備の保守、JPNIC 認証局機器等の故障時対応等において、JPNIC 認証局システムサーバの設置室へ入室権限者以外が入室する必要がある場合は、必ず入室権限者の立会いを必要とする
- JPNIC 登録局の端末を用いた発行・失効操作等は、複数人の RAO によって行う

［5.2.3］役割ごとの識別と本人認証

CP/CPS 5.2.3 項では、認証局設備にアクセスする者の識別条件と権限の確認条件について規定する。

調査表では、主な規定項目として次のものがあげられている。

- 認証局設備を操作する権限を操作者ごとに設定可能であること
- 認証局設備を操作するにあたって操作者と必要権限を確認可能であること

JPNIC 認証局の設備に対するアクセス権のセキュリティ基準を文書化することは必須要件であるが、一般的に CP/CPS 上は詳細な記述がされていないことから、本考察においても詳細な記述は行わず、方針レベルの記述案にとどめることとした。

「5.2.3.役割ごとの識別と本人認証」記述案

JPNIC 認証局の設備へのアクセス管理は、役割ごとの操作権限を操作者ごとに設定できるものとする。また JPNIC 認証局の設備へのアクセス時において、操作者と

必要権限を識別可能とする。

5.4.5.3. ［5.3］要員のセキュリティ統制

［5.3.1］JPNIC 認証局における人事上のセキュリティ管理

CP/CPS 5.3.1 項では、本来、要員の資格、経験及び身分証明の要件を記述することとなっているが、JPNIC 認証局の信頼性を損なわないために、JPNIC 認証局運用に関わる要員の信頼性を保証するための要件を規定することとした。

ECOM ガイドラインでは、規定内容として次の項目があげられている。

- 認証局の役割任命において適切な審査を行うこと
- 運用要員のメンタルヘルス・健康管理・適正な処遇等における継続した人事管理を行うこと

また WebTrust では、規定内容として次の項目があげられている。

- 認証局運用要員は任命時に守秘義務契約に署名すること
- 各役割の要員に欠格事項がないかどうかを継続して定期的に検査すること

CP/CPS 上では基本的な方針を示すべきであり、詳細なセキュリティ管理手順は管理手順書等を別途作成し、これに記載することが適切であると考えられる。よって、本報告書での記述案も基本方針を示す程度とした。

「5.3.1.JPNIC 認証局における人事上のセキュリティ管理」記述案

JPNIC は、職員に認証局の役割を任命する際及びその後定期的に、適切な人物審査を実施のうえ、任命を行う。日常業務においては、メンタルヘルス・健康管理・適正な処遇等における継続した人事管理を行う。また任命前までには、任命者と守秘義務契約を結び、情報の適切な管理を行う。

［5.3.2］背景調査

CP/CPS 5.3.2 項では、認証局運用要員及び認証局以外の関連する従業員（警備員等）を採用する際に行う人物確認の要件を規定する。

人物確認方法として、本人による書類提出が一般的であると考えられる。ここで提出する書類としては次のものが考えられる。

- 最終学歴を証明する書類
- 職歴を表す書類
- 賞罰が記載された書類

これらの書類に基づいて人物確認を行う場合は、その書類の記載内容の真偽及び背景を確認する必要があると考えられる。また採用にあたっては JPNIC 認証局運用要員と同様に、JPNIC 認証局の運用要員以外の者とも守秘義務契約を結ぶことが望ましいと考えられる。

「5.3.2.背景調査」記述案

JPNIC 認証局業務と関連する者を採用するにあたって、JPNIC は予め定めた適切な方法を用いてその人物の背景調査を行う。

［5.3.3］トレーニング要求

CP/CPS 5.3.3 項では、認証局を適切に運用し続けるために運用要員の役割に応じて行うトレーニングの要件を規定する。

調査表では、規定内容として次の項目があげられている。

- 役割に応じた教育・訓練計画を策定し、計画に沿って定期的に教育・訓練を実施すること
- 業務手順に変更がある場合は遅滞なく事務取扱要領の必要箇所を変更し、その変更に関わる教育・訓練を実施すること

また一般的な CP/CPS では、主な規定内容として次の項目もあげられている。

- 運用要員が役割に就く前に、認証局の運用に必要な教育を実施すること

教育・訓練について具体的内容を CP/CPS に記載する必要はなく、教育・訓練の方針を記載するべきであると考えられる。通常時と変更が生じた時の教育・訓練を最低限必要なものとして実施概要を規定するのであれば、前述の項目のようなトレーニング方針を記載することで十分であると考えられる。

「5.3.3.トレーニング要求」記述案

JPNIC 認証局は、運用要員の教育を次のように行う。

- 運用要員が役割に就く前に、認証局の運用に必要な教育を実施する
- 役割に応じた教育・訓練計画を策定し、計画に沿って定期的に教育・訓練を実施する
- 業務手順に変更がある場合は遅滞なく事務取扱要領の必要箇所を変更し、その変更に関わる教育・訓練を実施する

［5.3.4］再トレーニング期間と手続き

CP/CPS 5.3.4 項では、JPNIC 認証局の要員に対する再トレーニングの周期、手続きに関する要件を規定する。

「5.3.4.再トレーニング期間と手続き」記述案

JPNIC は定期的に JPNIC 認証局の要員に対して再トレーニングを行う。また、必要に応じて適時再トレーニングを行う。

［5.3.5］ジョブローテーションの頻度と順序

CP/CPS 5.3.5 項では、各役割間でのジョブローテーションの頻度と順序に関する要件を規定する。

WebTrust では、規定内容として次の項目があげられている。

- 業務運用及びセキュリティが損なわれないよう、職員の退職・解任時には適切な対応を行うこと

「5.3.5.ジョブローテーションの頻度と順序」記述案

JPNIC は、JPNIC 認証局運営が損なわれないよう職員の退職・解任に備えて適切な対策・対応を行う。

［5.3.6］認可されていない行為に対する制裁

CP/CPS 5.3.6 項では、認可されていない行為・認証局の使用・システムの使用についての職員に対する制裁要件を規定する。

WebTrust では、規定内容として次の項目があげられている。

- 許可のない操作、許可のない認証局利用、許可のないシステム利用に対しては制裁規定に従って制裁を実施すること

一般的には CP/CPS 上に具体的な制裁規定が記載されることはなく、別途制裁規定に従って制裁が実施されることを、CP/CPS 上に規定していることが多い。

「5.3.6.認可されていない行為に対する制裁」記述案

JPNIC は、JPNIC 認証局の職員による認可されていない行為に対し、（罰則規定書の名称）に従って制裁を与える。

［5.3.7］契約要員に関する要件

CP/CPS 5.3.7 項では、委託契約を行う際の実施事項について規定する。

調査表では、規定内容として次の項目があげられている。

- 委託契約において、委託業務の内容を明確にするとともに委託者の指示の遵守及び責任分担、保証、違反時の罰則等について明確にすること
- 委託契約において、受託者と守秘義務契約を結ぶこと
- 受託者の業務が適切に行われているかどうかを監督し管理すること

JPNIC の規則上、外部と契約を行う場合に必要な手続き等が前述の項目以外にあるならば併せて規定することが良いと考えられる。

「5.3.7.契約要員に関する要件」記述案

JPNIC は、委託契約において委託業務の内容を明確にするとともに、受託者に対して JPNIC の指示の遵守、責任分担、保証、違反時の罰則等について明確にし、かつ受託者と守秘義務契約を結ぶ。また委託後は受託者の業務が適切に行われているかどうかを監督し管理する。

［5.3.8］要員に提供されるべき文書

CP/CPS 5.3.8 項では、要員に提供されるべき文書に関する要件を規定する。

WebTrust では、規定内容として次の項目があげられている。

- 認証局運営組織によって決定した（CP/CPS、情報セキュリティポリシ、個人情報保護ポリシ、その他認証局の規定等）は全ての運用要員に開示し通知すること

JPNIC 認証局では、各要員に対して要員の役割に応じた義務やセキュリティポリシに関する文書を開示することは、CP/CPS に準拠した認証局運営を行うために必須であると考えられる。またその他、開示する必要があると考えられる文書があるならば併せて開示することが望ましいと思われる。

「5.3.8.要員に提供されるべき文書」記述案

JPNIC 認証局は次の文書を運用要員に開示し、周知する。

- CP/CPS
- 認証局運用に関する諸規程、手続き書、マニュアル、災害復旧計画書等
- 運用要員が遵守しなければならない各種関連規程
- （その他に決定された文書）

5.4.6. ［6］技術的なセキュリティ管理

5.4.6.1. ［6.1］鍵ペアの生成と実装

［6.1.1］鍵ペアの生成主体

各エンティティの鍵ペア生成を誰が行うのか等を記述する。次の項目について検討を行う。

- 誰が鍵ペアの生成を行うのか
- 作業は何人で行われるのか
- どのようなコントロールのもとで生成するのか
- 要件としてどのような基準（ISO 15782-1/FIPS 140-1 又は FIPS 140-2 レベル等）を採用するのか

通常、主に認証局の鍵ペアの生成について記述され、EE 等の鍵ペア生成については、認証局として一定の方法を要求する場合にのみ記述を行うのが一般的であると言える。本認証局では EE 鍵ペアは EE 自身に生成させ、また使用するクライアントアプリケーションを制限しないため、認証局の鍵ペアについてのみ記述する。

認証局の鍵ペア生成は、責任ある役割の者の立会いのもと、適切な権限の与えられた複数名の作業者によって、不正のなされないようなコントロール下で行われることが望ましい。また、高い信頼を得たい場合には、認証局鍵ペアの漏えい、複製等が行われないよう、FIPS 140-1 又は FIPS 140-2 レベル 3 認定若しくはそれ相当の暗号装置の使用が必要と考える。基準を明確に定めない、暗号装置を使用しない場合等においては、CP/CPS 上は誰が、どのように行うのかのコントロールのみを記述することでよいと考える。

本報告書の CP/CPS 記述案では、認証局の鍵ペア生成には安全性の高い暗号化モジュールを含むソフトウェアを使用することを前提とし、要件とする標準については規定しないこととする。

「6.1.1.鍵ペアの生成主体」記述案

本認証局の鍵ペアの生成は鍵管理者立会いのもと、複数人の CAO によって認証設備室内で行われる。本認証局の鍵ペアの生成は、安全性の高い暗号化モジュールを含むソフトウェアを使用して行われる。

［6.1.2］利用者への私有鍵の送付方法

利用者の鍵ペアを利用者自身で生成しない場合の私有鍵の受渡し方法についての検討を行う。利用者自身が鍵ペア生成を行う場合は規定しない。一般的な検討内容として、

- 私有鍵、証明書の受渡し方法（ダウンロード、私有鍵及び証明書の郵送、認証局窓口での手渡し等）
- 私有鍵利用のための PIN の受渡し方法（簡易書留、2 種類のコードの 2 系統配布等）

が考えられる。

本認証局では EE 鍵ペアの生成を行わず、ホストマスタの鍵ペアはホストマスタ自身が、サーバの鍵ペアは当該サーバの管理者が生成を行うため本項の規定は行わない。

「6.1.2.利用者への私有鍵の送付方法」記述案

本認証局は EE 鍵ペアの作成を行わないため、本項の規定を行わない。

［6.1.3］認証局への利用者の公開鍵の送付方法

認証局へ利用者の公開鍵をどのような方法で送付するかを記述する。オフラインで送付する場合には、送付に使用する媒体、送付方法等を記述し、オンラインで送付する場合には通信の保護、改ざん防止の仕組み等を記述する。

運用組織への負荷の軽減、証明書発行までの時間的問題を考慮し、認証局システムによって提供される、オンラインによる署名付証明書発行要求の送付の仕組みを使用することが望ましいと考える。

「6.1.3.認証局への利用者の公開鍵の送付方法」記述案

EE の公開鍵の本認証局への送付は、暗号化された通信下で、PKCS#10 形式のファイルを本認証局へ送付することで行われる。

［6.1.4］利用者への認証局公開鍵の配布

認証局の証明書を利用者へ送付する方法や、改ざんを防止するための仕組み等を検討する。

- セキュアなプロトコルを使用して広く公開する

- オフラインで利用者への送付する
- Web ブラウザへの組み込み

等の方法が考えられる。

本認証局ではオンラインで公開する方法と、オフラインで配付する方法の 2 つの方法を用意し、EE に応じてどちらかより適切な方法を使用することとする。

また、オンラインにて公開する場合には、認証局の証明書フィンガープリントを異なるサーバ上に公開する等置換攻撃への対策を施す必要があると考える。

「6.1.4.利用者への認証局公開鍵の配布」記述案

本認証局の証明書の配布は、次の 2 つの方法のうち EE に応じてどちらかより適切な方法を使用して行う。

- JPNIC 認証局は（URI は決定後に記述される）にて本認証局の証明書を公開する。本認証局の証明書の公開には暗号機能を持つセキュアなプロトコルを使用し、改ざん防止措置をとる。EE は（URI は決定後に記述される）より本認証局の証明書をダウンロードして使用することとする。EE はダウンロードした本認証局の証明書のフィンガープリントと（URI は決定後に記述される）にて公開されているフィンガープリントを比較し、一致していることを確認する。
- サーバ証明書の管理者には RAO が、ホストマスタには LRA 管理者が本認証局の証明書を手渡しする。

［6.1.5］鍵のサイズ

使用する鍵のサイズに関する要件を記述する。

認証局の鍵ペアは RSA 公開鍵暗号方式の 2048 ビット、EE 鍵ペアは RSA 公開鍵暗号方式の 1024 ビットが一般的であると考えられ、またもっとも多くのアプリケーションで利用可能であると考える。

「6.1.5.鍵のサイズ」記述案

本認証局は 2048 ビットの RSA 鍵ペアを使用する。EE については、1024 ビット以上の RSA 鍵ペアを使用することを義務とする。

［6.1.6］公開鍵パラメータの生成主体

公開鍵を生成するためのパラメータに関する要件を記述する。

通常、公開鍵パラメータの生成は鍵ペアの生成で使用する暗号装置若しくは安全性の高い暗号化モジュールを含むソフトウェアにより行われる。

今回の検討においては、鍵ペア生成に安全性の高い暗号化モジュールを含むソフトウェアを使用するとしているので、本項の記述案においてもソフトウェアの使用を前提として記述する。

「6.1.6.公開鍵パラメータの生成主体」記述案

本認証局の鍵ペアを生成するための公開鍵パラメータは、鍵ペア生成に使用される安全性の高い暗号化モジュールを含むソフトウェアに実装された乱数生成モジュール（以下、RNG と呼ぶ）を用いて生成される。

［6.1.7］パラメータ品質の検査方法

公開鍵パラメータの品質チェックに関する要件を記述する。

鍵ペアの生成で使用する暗号装置がどのような規格に合致しているのかを記述することになる。

今回の検討においては、要件とする標準については規定しないものとしているので、本項は規定しないものとする。

「6.1.7.パラメータ品質の検査方法」記述案

規定しない。

［6.1.8］ハードウェア又はソフトウェアによる鍵ペア生成

鍵ペアがハードウェアで生成されるのか若しくはソフトウェアで生成されるかを記述する。

本項の内容は CP/CPS 6.1.1 項にて記述するものとする。

「6.1.8.ハードウェア又はソフトウェアによる鍵ペア生成」記述案

本 CP/CPS 6.1.1 項にて記述する。

［6.1.9］鍵の使用目的

鍵の利用目的や鍵の使用の制限について記述する。またそれらの利用目的が証明書の keyUsage 拡張にどのようにマップされているかを記述する。

「6.1.9.鍵の使用目的」記述案

本認証局の証明書の keyUsage は keyCertSign、cRLSign のビットを使用する。本認証局の私有鍵は EE 証明書、CRL の発行にのみ使用する。

ホストマスタ証明書の keyUsage は digitalSignature、keyEncipherment を使用する。S/MIME、SSL/TLS のクライアント証明書としてのみ使用すること。

サーバ証明書の keyUsage は digitalSignature、keyEncipherment を使用する。SSL/TLS サーバ証明書としてのみ使用すること。

5.4.6.2. ［6.2］私有鍵の保護

［6.2.1］暗号化モジュールに関する標準

認証局で使用する暗号化モジュールに要求する標準について検討する。

暗号化モジュールに関する標準として、ISO 15782-1、FIPS 140-1 又は FIPS 140-2、ANSI X9.66 があげられる。

本認証局の私有鍵については、私有鍵の管理、安全性等を優先的に考慮する場合には、一般的に安全性が高いと言われている FIPS 140-1 又は FIPS 140-2 のレベル 3 以上の認定製品であるハードウェアセキュリティモジュール（以下、HSM と呼ぶ）の使用が妥当と考えられる。

本報告書の CP/CPS 記述案では、要件とする標準については規定しないこととする。

「6.2.1.暗号化モジュールに関する標準」記述案

規定しない。

［6.2.2］複数人による私有鍵の管理

認証局の私有鍵は一般的に厳重に管理するものとされており、どのように管理するかを記述する。

認証局の私有鍵の管理として、権限を複数に分散させ、複数人によって行うことが考えられる。また、権限を有する者のうち、事前に定める人数以上が揃わなければ私有鍵を取り出すことはできないものとすることも考えられる。

「6.2.2.複数人による私有鍵の管理」記述案

本認証局の私有鍵の管理は、複数の CAO に権限を付与し、2 名以上の CAO が揃わなければ本認証局の私有鍵を操作することはできない。

［6.2.3］私有鍵のエスクロー

認証局及び EE の私有鍵の第三者へのエスクローについて記述する。エスクローをする場合には、エスクローする機関、形態等について記述する。

一般的には認証局の私有鍵は認証局自身で厳重に管理されるものと考える。EE の私有鍵は、暗号用として使用される場合は、その用途から認証局におけるエスクローが必要な場合もあると考えられる。ただし、今回の検討においては、認証用として使用することを前提としていることから不要と考える。

なお、エスクローする場合は、次の主たる項目について十分に検討することが必要であると考えられる。

- エスクローする機関
- エスクローする形態（どのような保管をするか等）
- セキュリティ管理
- 責務
- 賠償責任

「6.2.3.私有鍵のエスクロー」記述案

本認証局の私有鍵を第三者に対して委託しない。

EE の私有鍵は EE 自身が生成及び管理する。

［6.2.4］私有鍵のバックアップ

認証局及び EE の私有鍵のバックアップについて、バックアップの方法、管理等について記述する。

障害等に備え、認証局の私有鍵のバックアップは必要と考える。災害等による施設への被害等も考慮し、認証局の私有鍵は稼動中の認証局システムが設置されている場所とは別地に保管することが望ましい。

認証局の私有鍵のバックアップは、複数人の操作を必要とし、鍵管理者の立会い及び複数の CAO による操作を行う必要があると思われる。

私有鍵を管理するソフトウェア若しくはハードウェアにより、バックアップ形態は依存すると考えられることから詳細は決定後記述されるものとする。

また、EE の私有鍵は EE 自身が生成及び管理を行うことから、認証局ではバックアップを行う必要はないと考えられる。

「6.2.4.私有鍵のバックアップ」記述案

本認証局私有鍵は、予め定める外部記憶媒体にバックアップされる。バックアップ作成時も鍵管理者の立会いと複数名の CAO を必要とする。

また、そのバックアップは予め定める保管場所に保管される。

本認証局は、EE の私有鍵のバックアップを行わない。

［6.2.5］私有鍵のアーカイブ

認証局及び EE の私有鍵について、アーカイブを行うか否かを記述する。

一般的には認証局の私有鍵のアーカイブは行われていないことが多いと思われる。

アーカイブを行う場合には、認証局の私有鍵はソフトウェア若しくはハードウェアで生成及び管理されることから、ソフトウェアの場合はアーカイブした記録媒体、ハードウェアの場合はそのハードウェアの管理を行うこととなると考えられる。

また、EE の私有鍵は EE 自身が生成及び管理を行うことから、認証局ではアーカイブを行う必要はないと考えられる。

「6.2.5.私有鍵のアーカイブ」記述案

本認証局の私有鍵のアーカイブは行わない。

EE の私有鍵についても同様にアーカイブは行わない。

［6.2.6］暗号化モジュールへの私有鍵の格納

認証局及び EE の私有鍵の暗号化モジュールへの格納に関して記述する。

暗号化モジュールへの格納は、認証局の私有鍵を取り扱うことのできる権限を付与された者が複数で行うことが必要と考える。

EE の私有鍵は EE 自身が鍵ペアの生成を行うため、EE 自身が格納を行うものと考えられる。

「6.2.6.暗号化モジュールへの私有鍵の格納」記述案

本認証局の私有鍵は、安全性の高い暗号化モジュールを含むソフトウェアで生成され、他のハードウェア及びソフトウェア等がそのモジュールに介入することはない。

EE の私有鍵は EE 自身が私有鍵の生成を行い、EE 自身で格納を行う。

ただし、サーバにおいてはサーバ証明書の管理者が格納を行う。

［6.2.7］私有鍵の活性化方法

認証局の私有鍵の活性化に関して記述する。

認証局の私有鍵を利用可能状態にする操作は、複数人で行うことが必要と思われる。

「6.2.7.私有鍵の活性化方法」記述案

本認証局の活性化は、認証設備室内において複数名の CAO を必要とする。

EE の私有鍵に関しては、規定しない。

［6.2.8］私有鍵の非活性化方法

認証局の私有鍵の非活性化に関して記述する。

認証局の私有鍵を利用不可能状態にする操作は、複数人で行うことが必要と思われる。

「6.2.8.私有鍵の非活性化方法」記述案

本認証局の私有鍵の非活性化は、認証設備室内において複数名の CAO を必要とし、操作をする者とその監視をする者とに分かれて行われる。

EE の私有鍵に関しては、規定しない。

［6.2.9］私有鍵の破棄方法

認証局及び EE の私有鍵の破棄方法に関して記述する。

認証局の私有鍵の使用終了時には、物理的な破壊、完全な初期化等を行うことが必要と考えられる。その操作は［6.2.7］と同様に複数人によって行われ、私有鍵が復元できないことを確認する。バックアップ、アーカイブを行った私有鍵についても同様な操作が必要と思われる。

EE の私有鍵は、EE 自身で確実に破棄することが必要と考える。

「6.2.9.私有鍵の破棄方法」記述案

本認証局の私有鍵を破棄しなければならない状況の場合は、鍵管理者と複数名の CAO によって、私有鍵の格納されたハードディスクを完全に初期化又は物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続きによって破棄する。

EE の私有鍵は、EE 自身で確実に破棄するものとする。

5.4.6.3. ［6.3］鍵ペア管理に関するその他の面

［6.3.1］公開鍵の保存

公開鍵の保存が必要かどうか、またどのように公開鍵の有効性を確保するかを検討する。

検証者による署名検証の可用性を確保するためには、公開鍵のアーカイブを行うことが必要である。また公開鍵の有効性を確保するため、アーカイブは暗号化し改ざん防止措置をとることが望ましい。

「6.3.1.公開鍵の保存」記述案

本認証局は、本認証局の証明書及び本認証局によって発行される全ての証明書のバックアップを行う。バックアップデータは改ざん防止のため暗号化して保管される。

［6.3.2］私有鍵と公開鍵の有効期間

私有鍵、公開鍵の使用可能期限について検討する。

私有鍵については、暗号化された文書の復号を行うため、有効期間を規定しないことが一般的である。

公開鍵については、有効期間の短いほうがより安全性が高いと言われているが、暗号解読技術の進展等を踏まえた変更が必要になると思われる。

「6.3.2.私有鍵と公開鍵の有効期間」記述案

本認証局の証明書の有効期間は 10 年、私有鍵の有効期間は 8 年とする。本認証局は私有鍵の有効期限前に鍵ペアの更新を行う。

EE 証明書の有効期間は 2 年とする。私有鍵は復号を行う場合においてのみ、2 年を超える使用を認めるものとする。

5.4.6.4. ［6.4］活性化データ

［6.4.1］活性化データの生成と組み込み

暗号化モジュールの起動時に要求される活性化用データについて記述する。

暗号化モジュールの起動時に要求される活性化用データを保護する方法として、パスワードや PIN を使用することが考えられる。

パスワードや PIN に用いる文字及びその長さは、容易に推測できてはならず、十分な長さを使用することで推測を困難なものにすることが可能と考える。

使用する文字は、英大文字、英小文字、数字を全て含むこととし、8 文字以上の長さが妥当であると思われる。

「6.4.1.活性化データの生成と組み込み」記述案

本認証局の私有鍵に対するものを含め、本認証局で使用される PIN やパスワードは、英大文字、英小文字、数字を全て含む 8 文字以上の長さを使用する。

［6.4.2］活性化データの保護

暗号化モジュールの活性化データの保護について記述する。

使用するパスワードや PIN を長期間同一のものを使用することは、悪意のある第三者に対して推測する時間を与えるだけであり、解読されてしまう危険性がともなうことが考えられる。

パスワードや PIN を定期的に変更することが必要と考える。

また、パスワードや PIN の管理及び変更は、事前に権限を付与された者が行う必要があると考える。

「6.4.2.活性化データの保護」記述案

本認証局で使用される PIN やパスワードについては、封印されたうえで運用管理者による管理のもと、保管される。また、CAO によって定期的に変更を行う。

5.4.6.5. ［6.5］コンピュータのセキュリティ管理

［6.5.1］信頼されるコンピューティング基本コンセプト

システムのセキュリティに関する要件及びその対策を記述する。

記述する内容として、

- OS の要塞化
- アクセスコントロール
- パスワードの管理方法
- リソースの常時監視

等が考えられる。

具体的な対策については、実際のシステム構成や使用する OS、ソフトウェアが決定した後に詳細な検討を行わなければならない。記述案では、一般的にどういった項目について対策をとるのかについて記述する。

「6.5.1.信頼されるコンピューティング基本コンセプト」記述案

本認証局のサーバシステムに関わる業務は、原則として複数人の CAO によって行われる。ただし、ハードウェア障害時等に発生する専門的な知識を必要とする作業については、複数人の CAO 立会いのもとで保守員によって行われるものとする。システムに対して行われた重要な操作は、全てログが残るよう設定されている。システム

にアクセスするためのパスワードは、全て適切な管理が行われる。本認証局のサーバシステムは、常時リソース監視が行われ、システムの異常や不正運用を検知し、速やかに適切な対策が行われる。

［6.5.2］コンピュータセキュリティ評価

使用するハードウェア、ソフトウェア及び CP/CPS 6.5.1 項で記述している対策への評価をどのように行うのか検討する。また評価に使用する基準があれば、その基準について記述を行う。

記述内容として、

- クラッキングテスト等を行う
- ISO/IEC15408-3:1999 の EAL4 等の認定を取った製品を使用する

等が考えられる。

具体的な内容については、実際に使用するハードウェア、ソフトウェアを検討する際に採用した基準や運用テストについて記述を行うことが望ましい。

「6.5.2.コンピュータセキュリティ評価」記述案

本認証局は使用する全てのソフトウェア、ハードウェアに対して事前に運用テストを行い、信頼性の確認を行う。

5.4.6.6. ［6.6］ライフサイクルのセキュリティ管理

［6.6.1］システム開発管理

システム開発時における管理について記述する。

システム開発管理においては、一般的なシステム開発時における管理（セキュリティも含む)、成果物のレビュー、導入時の受け入れ試験等を実施し、障害発生率を抑えるとともにセキュリティを保つ必要があると考えられる。

「6.6.1.システム開発管理」記述案

システムの品質及びセキュリティを保つために、開発時における各工程の管理、導入前の評価等を実施する。

［6.6.2］セキュリティ管理統制

セキュリティ運用管理に関して記述する。

国際標準規格である「ISO/IEC 17799:2000（JIS X 5080:2002）」、「ISMS」、経済産業省が推進している「情報セキュリティ管理基準」を参考に、システム開発時にはセキュリティを十分に配慮した管理が必要であると思われる。

検討項目として必要があると考えられるものを次に記す。

- 入退室管理、要員管理（教育を含む）、権限管理等の運用管理の実施及び運用改善
- 不正侵入対策、ウイルス対策等のシステム的なセキュリティ対策
- セキュリティ対策ソフトウェアの適時の改善等の実施

「6.6.2.セキュリティ管理統制」記述案

システムのセキュリティ管理として、入退室管理、教育を含む要員管理、権限管理等の運用管理の実施、不正侵入対策、ウイルス対策等のシステム的なセキュリティ対策、セキュリティ対策ソフトウェアの適時更新等の実施を行うものとする。

［6.6.3］ライフサイクル評価

［6.6.1］、［6.6.2］で記述した管理について、評価を行う。評価結果をもとに分析を行い、管理方法を見直すことも必要である。

また、導入を行ったシステムに関して、最新のセキュリティ上における脆弱性等の情報収集を行い、最新の動向を考慮したシステムへの評価、改善を行うことが必要と考えられる。

「6.6.3.ライフサイクル評価」記述案

規定された管理方法により、システムが管理されているか評価を行う。

本認証局のシステムに対して、セキュリティに関する情報収集を行い、最新の動向を考慮し、適切な評価、改善を行う。

5.4.6.7. ［6.7］ネットワークのセキュリティ管理

ネットワークセキュリティを確保するための対策について記述する。

検討内容としては、

- 利用可能なプロトコルの制限
- ファイアウォールや IDS（Intrusion Detection System）の導入
- ネットワークアタックテストの実施

等が考えられる。

具体的な対策については、実際のネットワーク構成や使用する機器等が決まった後に詳細な検討を行わなければならない。記述案では、一般的にどういった項目について対策をとるのかについて記述する。

「6.7.ネットワークのセキュリティ管理」記述案

本認証局の存在するネットワークはファイアウォールを使用し、ファイアウォール外からのアクセスは必要最低限のプロトコルに制限され、またアクセス可能なホストも限定される。

本認証局の存在するネットワークに対するアクセスは全て監視、記録され、不正なアクセスを早期に発見可能なシステムとする。

5.4.6.8. ［6.8］暗号化モジュールの技術管理

［6.2］と同様であるため、省略する。

5.4.7. ［7］証明書と失効リストのプロファイル

CP/CPS 7 章では、その CP/CPS に従って発行される証明書及び CRL のフォーマット、拡張領域を含む各領域の値について記述する。

証明書及び CRL のプロファイルを検討するうえで、次の項目を前提とした。

- ホストマスタ証明書は S/MIME 及び SSL/TLS、サーバ証明書は SSL/TLS で使用される。
- 可能な限り多くのアプリケーションで使用できるよう、シンプルなプロファイルにする。あるアプリケーションでは使用できないことが判明している拡張領域や値がある場合には極力使用せず、使用する場合には non-critical とする。
- 本認証局が発行する証明書だけでなく、JPNIC ルート認証局が発行する証明書のプロファイルも同時に策定する。
- 可能な限り RFC3280 準拠とする。

また、次の 2 項目については、個別に検討を行った。

- certificatePolicies 拡張の使用について
- 証明書中の DirectoryString のエンコードについて

certificatePolicies 拡張について、RFC3280 準拠とすると critical でなければならないが、一部アプリケーションではこの拡張を解釈できずに証明書の検証に失敗してしまうものがあるため、non-critical で発行することとした。

また、もし証明書ポリシのない PKI ドメインと相互認証を行うことになった場合には、有効なポリシツリーが辿れなくなるおそれがあるため、相互認証相手のドメインより発行される相互認証証明書中の policyIdentifier の値として anyPolicy を入れて発行してもらう等、相互認証証明書のプロファイルについて調整を行わなければならないと思われる。

DirectoryString のエンコードについて、 RFC3280 には「2003 年 12 月 31 日より後に発行する証明書中の DirectoryString は UTF8String でエンコードしなければならない」と記述されているが、PKI で使用する際のエンコードの異なる DirectoryString の一致規則が明確化されておらず、また一部のアプリケーションでは DN が UTF8String でエンコードされている証明書が使用できない等の理由から、DirectoryString のエンコードには PrintableString を使用することとした。実際、第 58 回 IETF ミーティングにおいても UTF8String の導入は先送りされることとなり、PKIX WG にて UTF8String を使用した際の一致規則について仕様を策定することに

なっている。

表 5-9、表 5-10 に本認証局が発行する証明書及び CRL のプロファイル案を記す。

表 5-9　JPNIC IP アドレス認証局が発行する証明書プロファイル

Field	critical flag	ホストマスタ証明書	サーバ証明書
version	NA	2	2
serialNumber	NA	non-negative integer	non-negative integer
signature	NA		
algorithm		sha1withRSAEncryption	sha1withRSAEncryption
parameters		null	null
issuer	NA		
		PrintableString*1	PrintableString*1
validity	NA		
notBefore		UTCTime	UTCTime
notAfter		UTCTime notBeforeの時刻より2年後	UTCTime notBeforeの時刻より2年後
subject	NA		
		PrintableString*2	PrintableString*3
subjectPublicKeyInfo	NA		
algorithm		rsaEncryption	rsaEncryption
parameters		null	null
subjectPublicKey		ホストマスタ公開鍵のBIT STRING	サーバ公開鍵のBIT STRING
authorityKeyIdentifier	n		
keyIdentifier		JPNIC IPアドレス認証局公開鍵の160bit SHA-1ハッシュ値	JPNIC IPアドレス認証局公開鍵の160bit SHA-1ハッシュ値
authorityCertIssuer		使用しない	使用しない
authorityCertSerialNumber		使用しない	使用しない
subjectKeyIdentifier	n	ホストマスタ公開鍵の160bit SHA-1ハッシュ値	サーバ公開鍵の160bit SHA-1ハッシュ値
keyUsage	c		
digitalSignature		1	1
nonRepudiation		0	0
keyEncipherment		1	1
certificatePolicies	n		
policyIdentifier		本CPのOID	本CPのOID
policyQualifiers			
policyQualifierId		CPSUri	CPSUri
qualifier		本CP/CPSを公開するURI	本CP/CPSを公開するURI
subjectAltName	n		
rfc822Name		ホストマスタのメールアドレス	使用しない
cRLDistributionPoints	n		
DistributionPoint			
distributionPoint		JPNIC IPアドレス認証局がCRLを公開するURI	JPNIC IPアドレス認証局がCRLを公開するURI
reasons		使用しない	使用しない
cRLIssuer		使用しない	使用しない

表 5-10　JPNIC IP アドレス認証局が発行する CRL プロファイル

Field	critical flag	証明書失効リスト
version	NA	1
signature	NA	
algorithm		sha1withRSAEncryption
parameters		null
issuer	NA	
		PrintableString*1
thisUpdate	NA	UTCTime
nextUpdate	NA	UTCTime thisUpdateより24時間後
revokedCertificates	NA	
revokedCertificate		
userCertificate		失効された証明書の シリアル番号
revocationDate		UTCTime 証明書の失効された時刻
crlEntryExtensions		
		使用しない
crlExtensions	NA	
cRLNumber	n	non-negative integer
authorityKeyIdentifier	n	JPNIC IPアドレス認証局 公開鍵の160bit SHA-1ハッシュ値

また、本認証局の CP/CPS には記載されない JPNIC ルート認証局が発行する証明書及び CRL のプロファイル案を表 5-11、表 5-12、表 5-13 に記す。

表 5-11　JPNIC IP アドレス認証局の証明書と JPNIC ルート認証局の証明書プロファイル

Field	critical flag	JPNIC IPアドレス認証局 証明書	JPNIC ルート認証局 証明書
version	NA	2	2
serialNumber	NA	non-negative integer	non-negative integer
signature	NA		
algorithm		sha1withRSAEncryption	sha1withRSAEncryption
parameters		null	null
issuer	NA		
		PrintableString*4	PrintableString*4
validity	NA		
notBefore		UTCTime	UTCTime
notAfter		notBeforeの時刻より10年後	notBeforeの時刻より20年後
subject	NA		
		PrintableString*1	PrintableString*4
subjectPublicKeyInfo	NA		
algorithm		rsaEncryption	rsaEncryption
parameters		null	null
subjectPublicKey		JPNIC IPアドレス認証局 公開鍵のBIT STRING	JPNIC ルート認証局 公開鍵のBIT STRING
authorityKeyIdentifier	n		
keyIdentifier		JPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値	JPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値
authorityCertIssuer		使用しない	使用しない
authorityCertSerialNumber		使用しない	使用しない
subjectKeyIdentifier	n	JPNIC IPアドレス認証局 公開鍵の160bit SHA-1ハッシュ値	JPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値
keyUsage	c		
		keyCertSign	keyCertSign
		cRLSign	cRLSign
certificatePolicies	n		
policyIdentifier		本CPのOID	使用しない
policyQualifiers			
policyQualifierId		CPSUri	使用しない
qualifier		本CP/CPSを公開するURI	使用しない
basicConstraints	c		
cA		TRUE	TRUE
cRLDistributionPoints	n		
DistributionPoint			
distributionPoint		JPNIC ルート認証局がCRLを公開するURI	使用しない
reasons		使用しない	使用しない
cRLIssuer		使用しない	使用しない

表 5-12　JPNIC ルート認証局リンク証明書プロファイル

Field	critical flag	JPNIC IPルート認証局リンク証明書OldwithNew	JPNIC ルート認証局リンク証明書NewwithOld
version	NA	2	2
serialNumber	NA	non-negative integer	non-negative integer
signature	NA		
algorithm		sha1withRSAEncryption	sha1withRSAEncryption
parameters		null	null
issuer	NA		
		PrintableString*4	PrintableString*4
validity	NA		
notBefore		UTCTime	UTCTime
notAfter		UTCTime 古い自己署名証明書の notAfter	UTCTime 古い自己署名証明書の notAfter
subject	NA		
		PrintableString*4	PrintableString*4
subjectPublicKeyInfo	NA		
algorithm		rsaEncryption	rsaEncryption
parameters		null	null
subjectPublicKey		古いJPNIC ルート認証局公開鍵のBIT STRING	新しいJPNIC ルート認証局
authorityKeyIdentifier	n		
keyIdentifier		新しいJPNIC ルート認証局 公開鍵の160bit	古いJPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値
authorityCertIssuer		使用しない	使用しない
authorityCertSerialNumber		使用しない	使用しない
subjectKeyIdentifier	n	古いJPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値	新しいJPNIC ルート認証局 公開鍵の160bit
keyUsage	c		
		keyCertSign	keyCertSign
		cRLSign	cRLSign
certificatePolicies	n		
policyIdentifier		anyPolicy	anyPolicy
policyQualifiers			
policyQualifierId		使用しない	使用しない
qualifier		使用しない	使用しない
basicConstraints	c		
cA		TRUE	TRUE
cRLDistributionPoints	n		
DistributionPoint			
distributionPoint		JPNIC ルート認証局がCRLを公開するURI	JPNIC ルート認証局がCRLを公開するURI
reasons		使用しない	使用しない
cRLIssuer		使用しない	使用しない

表 5-13　JPNIC ルート認証局が発行する CRL プロファイル

Field	critical flag	証明書失効リスト
version	NA	1
signature	NA	
algorithm		sha1withRSAEncryption
parameters		null
issuer	NA	
		PrintableString[*4]
thisUpdate	NA	UTCTime
nextUpdate	NA	UTCTime thisUpdateより1年後
revokedCertificates	NA	
revokedCertificate		
userCertificate		失効された証明書の シリアル番号
revocationDate		UTCTime 証明書の失効された時刻
crlEntryExtensions		
		使用しない
crlExtensions	NA	
cRLNumber	n	non-negative integer
authorityKeyIdentifier	n	JPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値

※1　C=JP, O=Japan Network Information Center, OU=Internet Resource Services, OU=JPNIC Resource Service Certification Authority

※2　C=JP, O=Japan Network Information Center, OU=Internet Resource Services, OU=Resource Holder, OU=（JPNIC が LRA 組織に一意に割り当てる ID）（LRA 組織名称）, CN=（証明書発行対象ホストマスタの氏名をアルファベット表記したもの） + serialNumber=（LRA 組織ごとに一意に管理される ID）

※3　C=JP, O=Japan Network Information Center, OU=Internet Resource Services, OU=Resource Management System, CN=（証明書発行対象サーバの FQDN）

※ 4　C=JP, O=Japan Network Information Center, OU=JPNIC Root Certification Authority

5.4.8. ［8］仕様の管理

5.4.8.1. ［8.1］改訂手続き

CP/CPS の 8.1 節では、CP/CPS の改訂に関する手続きを記述することとなる。

検討項目として、

- どのようなときに改訂を行うのか
- 大幅な仕様変更時の扱い
- 改訂に関する関係者の合意
- 改訂にともなう関係機関に確認承認が必要な場合の手続き

について検討を行う。

どのようなときに行うのかについては、認証局の運用、手続きの変更等において、CP/CPS の改訂の最終承認を行う運営委員会が証明書ポリシ及びその履行の保証に著しく影響を与えないと判断した場合に、CP/CPS の改訂を行うものと考えられる。

証明書ポリシ及びその履行の保証、利用者の義務に変更が行われ、証明書を利用する者、検証する者に著しく影響を与える変更等の大幅な仕様変更時の扱いとしては、本来、同一の証明書ポリシでよいのかという検討が必要になる。CP/CPS の最終承認組織である運営委員会は、前述の検討を行ったうえで、CP/CPS の改訂承認、若しくは別の証明書ポリシの策定を指示することが望まれる。

改訂に関する関係者の合意については、改訂が有効になるまでの間に関係者より申出がない場合は合意が得られたと解釈する場合が一般的と思われる。合意が得られず、関係者より申出があった場合の対応であるが、本認証局の場合、LRA との契約を前提としており、本考察では一般的な記述にとどめ、契約関係が明確になった時点で変更を行うものとする。

改訂にともなう関係機関に対する、確認又は承認が必要な場合の手続きについては、今回の JPNIC 認証局は特別な関係機関からの認定等を想定していないので、関係機関に対する確認、承認依頼は不要であると考える。

「8.1.改訂手続き」記述案

本認証局は、証明書ポリシ及びその保証、義務に著しい影響を与えない範囲での CP/CPS 変更の必要性が生じた場合、利用者又は検証者に事前の承諾なしに、随時 CP/CPS の変更することができる。なお、改訂の通知から改訂が有効になるまでの期間に改訂に対する異議の申出がない場合は、改訂に対する合意が得られたものとする。改訂に対し合意できない関係者においては、即時に本認証局から発行された証明書の利用を中止するものとする。

5.4.8.2. ［8.2］公表と通知の手続き

CP/CPS の 8.2 節では、CP/CPS の公表と通知に関する手続きを記述することとなる。

検討項目として、

- 公表、通知の時期、公表頻度
- 公表、通知の方法（公表先、公表場所、通知方法等）
- 変更履歴を公表するか否か

について検討を行う。

公表、通知の時期については、関係者の確認期間を考慮し、その改訂が有効になる一定期間以前に公表、通知が必要と思われる。また公表頻度は常時公表とするのが一般的である。

公表の方法については、認証局のホームページ及びリポジトリへの開示が一般的と考えられる。

通知の方法については、利用者への通知方法を定めている場合はその方法により行うこととなると思われるが、通知業務の負荷等を考え特段の通知方法を定めない場合、ホームページ等への公表をもって通知とすることも一般的な記述として考えられる。

公表先については、証明書の適用範囲を限定している証明書の利用の場合は広く一般には公開せず、証明書の利用者及び関係者等に限定して開示する場合がある。本認証局においても、IP レジストリ業務における利用を前提としており、公表先を一部に限定することも考えられるが、適用範囲外の者からの問い合わせ等を考慮し、広く一般に公開を行うものとする。

変更履歴の公表については、最新の CP/CPS 及び変更履歴についての公表を行うことが一般的であり、変更履歴についても公表を行うものとする。

「8.2.公表と通知の手続き」記述案

本認証局は、変更された CP/CPS をその改訂が有効になる（期間は決定後に記述される）前までに、変更履歴とともに本認証局ホームページに掲載することにより、利用者及び関係者に改訂の通知を行うものとする。

5.4.8.3. ［8.3］承認手続き

CP/CPS の 8.3 節では、CP/CPS の承認に関する手続きを記述することとなる。

一般的な CP/CPS においては、どのような承認が行われるのかが記述される。また、関係者との合意についての記述がなされる場合がある。本報告書では、関係者との合意については、本報告書 5.4.8.1.にて記述しているので、承認者又は承認機関についての記述のみとする。

「8.3.承認手続き」記述案

本規定の改訂は、社団法人日本インターネットインフォメーションセンターの認証業務に関する運営委員会により承認を受けた後に公表されるものとする。

5.5. RFC3647 との相違点及び追加検討事項

5.5.1. RFC2527 と RFC3647 の相違点の概要

新しい CP/CPS のフレームワークである RFC3647 は、RFC2527 においてわかりにくかった説明や内容的に重複している項目に対して補足説明及び整理統合が行われ利用しやすいものとなっている。RFC3647 は RFC2527 に比べ構成の変更及び若干の項目追加が行われているが、記述すべき項目及び内容において、RFC2527 との著しい変更は行われていない。RFC2527 に比べ CP/CPS を検討する者にとって評価できる内容となっていると思われる。

RFC3647 において追加されている項目については、「5.5.2.RFC3647 にて追加された項目及び記述方針」にて述べるものとする。

5.5.2. RFC3647 にて追加された項目及び記述方針

（1） RFC3647　1.3.5 その他関係者

本認証局では、証明書一括発行期間、リポジトリサービス等外部組織の利用を想定しておらず、規定しないと記述するものとする。

（2） RFC3647　1.6.定義と略語

本検討上、RFC2527 のフレームワークにおいても、定義と略語は必要と考え RFC2527 の章構成の 1.5 節に追加記述している。

（3） RFC3647　4.9.5.認証局が失効申請を処理しなければならない期間

証明書の使用者等からの失効申請に対し、認証局が失効を完了させなければならな

い期間の記述をすることとなる。

完了する期間の定めは、休日、夜間の対応等認証局の運用体制に大きく影響するため、実際の認証局の運用体制が定まってから再度検討する必要がある。若しくは、運用によらずシステム的に自動化する等の対応の検討が必要となる。本項については継続的に検討を行うものとし、当初の記述方針とし、

- 証明書の使用者が申請した時点からの完了期間ではなく、申請確認を行った後、完了するまでの期間を記述する
- 完了期間は、速やかに実施するという表現にとどめる

こととする。

（4） RFC3647　4.11.加入の終了

ここでは、加入者が認証局のサービスの登録を終了する場合の手続きを定める。

検討点として、サービスの利用終了と証明書の関係を明確にする。

本認証局で発行する証明書は IP アドレスの管理に関する各種申請業務に使用することを前提にしており、本認証局のサービスの加入者は IP アドレス管理指定事業者となる。IP アドレス管理指定事業者が本認証局のサービスの登録を終了するということは、JPNIC に対する IP アドレスの管理に関する各種申請業務を終了するということになり、継続的に証明書を使用する必要性がなくなる。ゆえに、加入者が本認証局のサービスの利用登録を終了する場合は、加入者に対して発行した証明書を全て失効する旨の内容を記述方針とする。

（5） RFC3647　6.8.タイムスタンプ

タイムスタンプに関する検討は、本報告書の 5.4.4.6.の RFC2527 の文書構成上の「4.6.5.記録に対するタイムスタンプを付ける要件」において記述している。

（6） RFC3647　7.3.1.OCSP プロファイル、7.3.2.OCSP バージョン、7.3.3.OCSP 拡張

OCSP サーバ等を利用する場合、プロファイル、プロトコルのバージョン、拡張の内容を記述する箇所であるが、本認証局では OCSP によるサービスを提供しないこととしているので、記述方針としては、各項目に「OCSP は使用しない。」若しくは「規定しない。」と記述するものとする。

（7） RFC3647　9.4.1.プライバシポリシ

ここでは、関係者の活動に適用されるプライバシポリシの明示及び公開を記述することとなる。

RFC3647 上ではプライバシプランとなっているが、プライバシポリシとして記述する。

JPNIC においては、プライバシポリシをホームページ上で公開しており、JPNIC が扱う個人情報をプライバシポリシの対象としている。本認証局において、この公開されているプライバシポリシを適用するのか、公開されているプライバシポリシを改訂の上使用するのか、新たに認証局のサービスにおけるプライバシポリシを作成するのか等の JPNIC 全体での検討が必要となる。

今回の検討においては、個人情報保護の高まりを考慮し、RFC2527 の追加事項として、RFC2527 の文書構成上の 2.10 節に記述を行っている。

（8） RFC3647　9.4.5.個人情報の使用に関する個人への通知及び承諾

（7）の検討と同様。

（9） RFC3647　9.6.5.他の関係者の表明保証

（1）の検討と同様。

（10） RFC3647　9.10.1.有効期間

ここでは、CP/CPS、契約書、協定等の文書の有効期間について記述することができる。

RFC3647 の説明自体曖昧な感があるが、各種文書は正当な承認手続きにて発行され、正当な承認手続きにて改訂されるまでの間、有効である旨の表記になると考えられる。

（11） RFC3647　9.10.2.終了

ここでは、CP/CPS、契約書、協定等の文書の全部又は一部、若しくは特定の関係者に対して有効でなくなる場合について記述することができる。

RFC3647 の説明自体曖昧な感があるが、各種文書の一部若しくは特定の関係者に対して規定されている条項が無効になった場合、その該当部分についてのみ終了の効果が及ぶといった旨の表記をするものと考えられる。この項においては、「9.10.3.終了の

効果と効果継続」と重複感があり、記述内容について、再度調査を行うものとする。

（12） RFC3647　9.16.2.権利譲渡条項

ここでは、相手方当事者との契約等に基づく自己の権利の譲渡や義務の履行の委任についての制限等を記述することができる。

現時点では各種関係者との契約的な協議は行われておらず、継続検討課題とする。

（13） RFC3647　9.17.その他の条項

ここでは、RFC3647 のフレームワークにあてはまらない追加的な責任等を記述することができる。

この項は、RFC3647 のフレームワーク以外で、特に記述しておきたい事項の記述となるが、現時点では各種関係者との契約的な協議は行われておらず、継続検討課題とする。