Appendix 2

IP アドレス認証局（認証）

認証業務規程（CPS）

新旧比較表

新：JPNIC 資源管理認証局認証業務規定(CPS)	旧：JPNIC IP アドレス認証局認証業務規定 (CP/CPS)
1.1.概要 本 JPNIC 資源管理認証局 認証業務規定(以下、CPS という）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 という）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 資源管理認証局（以下、本認証局という）の認証業務に関する運用規則を定める。 本認証局は、本 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、ホストマスタという）等に証明書を発行する等の認証サービスを提供する。また、安全な通信を実現するため、JPNIC の各種サーバに対してサーバ証明書を発行する。 本 CPS の構成は、IETF PKIX WG において標準化されている RFC3647「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。	**1.1. 概要** 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（以下、本認証局と呼ぶ）の認証業務に関する運用規則を定める。 本認証局は、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等の認証サービスを提供する。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 RFC3647「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。 → 本項以降、全て「CP/CPS」を「CPS」に置き換え
1.2.文書の名前と識別 本 CPS の正式名称は「JPNIC 資源管理認証局 認証業務規程」という。 JPNIC 及び本認証局に関連するオブジェクト識別子を表 1-1 に示す。 表 1-1 JPNIC 及び JPNIC 資源管理認証局に関連するオブジェクト識別子 オブジェクト：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 → オブジェクト識別子：1.2.392.200175 オブジェクト：JPNIC 資源管理認証局 認証業務規程（CPS） → オブジェクト識別子：1.2.392.200175.1.2.1（OID の詳細は決定後に記述される） オブジェクト：EE 証明書ポリシ → オブジェクト識別子：1.2.392.200175.1.2.1（OID の詳細は決定後に記	**1.2. 文書の名前と識別** 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 及び本認証局に関連するオブジェクト識別子を表 1-1 に示す。 表 1-1 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 オブジェクト：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 → オブジェクト識別子：1.2.392.00200175 オブジェクト：JPNIC IP アドレス認証局 認証業務規程（CP/CPS） → オブジェクト識別子：1.2.392.00200175.2（OID は決定後に記述される） オブジェクト：EE 証明書ポリシ → オブジェクト識別子：1.2.392.00200175.2（OID は決定後に記述される）

述される）	→ 本項以降、全て「IP アドレス認証局」を「資源管理認証局」に置き換え
1.3.1.認証局、登録局、所有者及び検証者 表 1-2 コミュニティに関係する登場者と役割 ・ メンバ管理者証明書…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メンバ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、メンバ管理者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)…EE に発行される証明書の総称 ・ 証明書申請者…証明書を申請中の者 ・ JPNIC 発行局(JPNIC IA) …JPNIC ルート認証局内の発行局及び JPNIC 資源管理認証局内の発行局の総称。JPNIC ルート認証局及び JPNIC 資源管理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 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（資源管理認証局）の証明書に電子署名を行う。 ・ JPNIC 資源管理認証局…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 資源管理認証局証明書は、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 資源管理認証局、JPNIC 登録局及びリポジトリから構成される。 ・ LRA…証明書を発行する組織とは異なる組織若しくは団体であり、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。	**1.3.1.認証局、登録局、所有者及び検証者** 表 1-2 コミュニティに関係する登場者と役割 ・ 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(追加)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…EE 証明書を申請中の者 ・ 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 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。 ・ ローカル登録局(LRA)…証明書を発行する組織とは異なる組織若しくは団体であり、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。

・ 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。メンバ管理者の任命・解任を行う。 ・ メンバ管理者(メンバ管理者)…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。	・ 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。
1.3.2.その他の関係者 規定しない。	(新設)
1.4.1 適切な証明書の使用 本 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がユーザ及びメッセージを検証する為に使われるものとする。	**1.4.1 適切な証明書の使用** 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。
1.4.2 禁止される証明書の使用 本 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る。(削除) 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。	**1.4.2 禁止される証明書の使用** 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。
1.5.2.CPS のポリシ適合性を決定する者 本 CPS が、本認証局の運営方針として適切か否かの判断は、JPNIC の認証業務に関する運営委員会（以下、運営委員会という）が行う。	**1.5.2.CP/CPS のポリシ適合性を決定する者** 本 CP/CPS が、本認証局の運営方針として適切か否かの判断は、JPNIC の認証業務に関する運営委員会（以下、運営委員会と呼ぶ）が行う。
2.1 リポジトリ 本認証局は、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。リポジトリには証明書リポジトリと情報公開用リポジトリがある。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。	**2.1.リポジトリ** 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。(追加)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。
2.2.証明情報の公開 次の情報を情報公開用リポジトリ上に公開する。 ・CPS また次の情報を証明書リポジトリ上に公開する。 ・EE 証明書	**2.2.証明情報の公開** 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）

・CRL ただし EE 証明書と CRL は検証者のみに公開する。	・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）
また本認証局は、自己署名証明書のフィンガープリントを情報公開用リポジトリより http 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、CPS 及び認証局に関する重要情報は、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）	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）
2.3.公開の時期又は頻度 本認証局が公開する情報について、公開の時期及び頻度は次のとおりである。	**2.3.公開の時期又は頻度** 本認証局を含む JPNIC 認証局が公開する情報について、公開の時期及び頻度は次のとおりである。 → 本項以降、全て「本認証局を含む JPNIC 認証局」を「本認証局」に置き換え
2.4.リポジトリへのアクセス管理 本認証局は公開情報に関して、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。認証に使われる EE 証明書の証明書検証者は JPNIC であるとする。従って基本的に証明書リポジトリは JPNIC に向けて提供される。	**2.4.リポジトリへのアクセス管理** 本認証局を含む JPNIC 認証局は、公開情報に関して、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。
3.1.2 名前が意味を持つことの必要性 証明書に記載される名前は、個人名、組織名、役割名、および機器名をあらわすものである必要がある。	**3.1.2.名前が意味を持つことの必要性** 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がある。
3.1.3.所有者の匿名性 証明書には、個人、組織、役割、および機器が特定できる名前であれば、実名を使用する必要はない。	**3.1.3 所有者の匿名性又は仮名性** 証明書に記載される名前として匿名又は仮名を使用することはできない。
3.2.2.組織の認証 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 IP 指定事業者でなければならない。	**3.2.2.組織的本人性の認証** 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。
3.2.3. 個人の認証 JPNIC は、メンバ管理者証明書の申請者の発行登録を行う際に、所定の手続きに従ってメンバ管理者証明書の申請者の証明を行うこととする。 メンバ管理者は、ホストマスタ証明書の申請者の発行登録を行う際に、所定の手続きに従って干すとマスタ証明書の申請者の認証を責任を持って行うこととする。	**3.2.3. 個人的本人性の認証** (追加) LRA 管理者は、ホストマスタ証明書発行対象者の発行登録を行う際に、人事情報 DB、雇用契約等本人を特定できる情報を用いて発酵対象者の本人確認を行う。また、証明書発行対象者が、LRA 責任者より証明書の発行の許可を受けている者であることを認識する。
3.2.5.権限の正当性確認 本認証局は、メンバ管理者からホストマスタ証明書の申請登録を受け付けるにあたって、当該メンバ管理者の正当性を確認する。	**3.2.5.権限の正当性確認** 本認証局は、LRA 管理者からホストマスタ証明書の申請登録を受付けるにあたって、当該 LRA 管理者の正当性を確認する。
3.4.失効申請時の本人性確認と認証 JPNIC は、メンバ管理者証明書に対する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。 メンバ管理者は、ホストマスタ証明書に対する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。	**3.4.失効申請時の本人性確認と認証** 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。
4.1.1.証明書申請を提出することができる者 メンバ管理者証明書の申請を行うことができる者は、IP 指定事業者に所属する者とする。 ホストマスタ証明書の申請を行うことができる者は、認証されたメンバ管理者とする。	**4.1.1.証明書申請を提出することができる者** ホストマスタ証明書の申請を行うことができる者は、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 が指定した者とする。
4.1.2.登録手続及び責任 メンバ管理者証明書の申請者は、JPNIC により事前に周知された方法に従い、JPNIC に対して証明書の発行申請を行う。メンバ管理者は申請書の記載によって役割を確認される。 ホストマスタ証明書の申請者は、メンバ管理者により事前に周知された方法に従い、メンバ管理者に対して証明書の発行申請を行う。また、証明書申請者は、本認証局より鍵ペア生成及び証明書発行に必要な 2 種類の情報が通知されたならば、鍵ペアを生成し、本認証局へ PKCS#10 等の証明書発行要求のデータ形式に従った電子署名のされた証明書発行要求	**4.1.2.登録手続及び責任** （追加） 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、LRA 管理者に対して証明書の発行申請を行う。また、証明書申請者は、本認証局より鍵ペア生成及び証明書発行に必要な 2 種類の情報が通知されたならば、鍵ペアを生成し、本認証局へ PKCS#10 に従った電子署名のされた証明書発行要求をセキュアなオンライン通信を介して

をセキュアなオンライン通信を介して送付する。証明書発行要求の電子署名は検証される。	送付する。 （追加）
4.2.1 本人性確認と認証機能の実行 メンバ管理者証明書の申請者の本人性確認はJPNIC の登録局管理者が行う。 ホストマスタ証明書の申請者の本人性確認はメンバ管理者が行う。メンバ管理者は、本 CPS「1.1.1.個人の認証」に基づき、ホストマスタ証明書の申請者の本人確認を実施する。メンバ管理者は、ホストマスタ証明書の申請者の本人確認に関して責任を負うものとする。	**4.2.1.本人性確認と認証機能の実行** （追加） ホストマスタ証明書の申請者の本人性確認は LRA 管理者が行う。LRA 管理者は、本 CP/CPS「3.2.3.個人的本人性の認証」に基づき、ホストマスタ証明書の申請者の本人確認を実施する。LRA 管理者は、ホストマスタ証明書の申請者の本人確認に関して責任を負うものとする。
4.2.2.証明書申請の承認又は却下 メンバ管理者はホストマスタ証明書の申請者からの申請に対し、予め規定された審査基準に基づき、証明書申請の諾否を決定する。申請を承諾した場合は、本認証局に対し証明書の申請登録を行う。メンバ管理者は申請の審査に関して責任を負うものとする。 JPNIC の登録局管理者はメンバ管理者証明書の申請者からの申請に対し、予め規定された審査基準に基づき、証明書申請の諾否を決定する。申請を承諾した場合は本認証局に対し証明書の申請登録を行う。JPNIC の登録局管理者は申請の審査に関して責任を負うものとする。 なお、本認証局は、ホストマスタ証明書の申請登録を行うメンバ管理者の本人性確認を行った後、証明書の発行手続を開始する。	**4.2.2.証明書申請の承認又は却下** LRA 管理者は、ホストマスタ証明書の申請者からの申請に対し、予め規定された審査基準に基づき、証明書申請の諾否を決定する。申請を承諾した場合は、本認証局に対し証明書の申請登録を行う。LRA 管理者は、申請の審査に関して責任を負うものとする。 (追加) なお、本認証局は、ホストマスタ証明書の申請登録を行う LRA 管理者の本人性確認を行った後、証明書の発行手続を開始する。
4.2.3.証明書申請の処理時間 メンバ管理者は、ホストマスタ証明書の申請者からの発行申請を受理した場合、速やかに証明書の発行申請登録を行う。 JPNIC の登録局管理者はメンバ管理者証明書の申請者からの発行申請を受理した場合、速やかに証明書の発行申請登録を行う。 本認証局は、メンバ管理者又は JPNIC の登録局管理者からの発行申請登録を受理した場合、速やかに証明書の発行を行う。	**4.2.3.証明書申請の処理時間** LRA 管理者は、ホストマスタ証明書の申請者からの発行申請を受理した場合、速やかに証明書の発行申請登録を行う。 (追加) 本認証局は、LRA 管理者からの発行申請登録を受理した場合、速やかに証明書の発行を行う。
4.3.1.証明書の発行過程における認証局の行為 本認証局は、メンバ管理者からのホストマスタ証明書の発行申請登録を受け付けるにあたって、予め定められた方法によりメンバ管理者の権限確認を行う。またメンバ管理者証明書の発行申請登録を受け付けるにあたって、予め定められた方法によりメンバ管理者の権限確認を行う。本認証局は、申請登録	**4.3.1.証明書の発行過程における認証局の行為** 本認証局は、LRA 管理者からのホストマスタ証明書の発行申請登録を受付けるにあたって、予め定められた方法により LRA 管理者の本人性確認を行う。 (追加) 本認証局は、申請登録の真正性を確認した後、ホス

の真正性を確認した後、ホストマスタ証明書の申請者に対し、本 CPS「4.3.2.認証局の所有者に対する証明書発行通知」に定められた方法で証明書の発行が許可されたことを通知する。 本認証局は、ホストマスタ証明書の申請者から送付された証明書発行要求の電子署名を検証し、証明書発行要求の真正性を確認した後、セキュアなオンライン通信を介してホストマスタ証明書の申請者に対し証明書を発行する。 本認証局は、メンバ管理者証明書の申請者から送付された証明書発行要求の電子署名を検証し、証明書発行要求の真正性を確認した後、オフラインの手段を介してメンバ管理者証明書の申請者に対し証明書を発行する。	トマスタ証明書の申請者に対し、本 CP/CPS「4.3.2.認証局の所有者に対する証明書発行通知」に定められた方法で証明書の発行が許可されたことを通知する。 本認証局は、ホストマスタ証明書の申請者から送付された証明書発行要求の電子署名を検証し、証明書発行要求の真正性を確認した後、セキュアなオンライン通信を介してホストマスタ証明書の申請者に対し証明書を発行する。 (追加)
4.3.2.認証局の所有者に対する証明書発行通知 メンバ管理者証明書はオフラインの手段により申請者に対し発行通知を行う。 本認証局は、証明書発行に必要な 2 種類の情報を生成し、二つの異なる方法を用いてメンバ管理者経由でホストマスタ証明書の申請者へ通知する。	**4.3.2.認証局の所有者に対する証明書発行通知** （追加） 本認証局は、証明書発行に必要な 2 種類の情報を生成し、一方を（電子メール若しくは郵送：決定後に記述される）を用いて直接ホストマスタ証明書の申請者へ、もう一方を（電子メール若しくは郵送：決定後に記述される）を用いて LRA 管理者経由でホストマスタ証明書の申請者へ通知する。
4.4.1 証明書の受領確認の行為 メンバ管理者証明書に関してはオフラインの手段を使い受領する。証明書に不具合がある場合は JPNIC へ連絡を行う。配達後一週間後までに連絡がない場合は受領したとみなす。 本認証局は、到達確認のできる方法でメンバ管理者の証明書を配達する。ホストマスタ証明書の申請者による証明書のダウンロードし、確認した上で受領するものとする。証明書に不具合がある場合はメンバ管理者を通じて JPNIC へ連絡を行う。ダウンロード後一週間後までに不具合の連絡がない場合は受領したとみなす。	**4.4.1 証明書の受領確認の行為** (追加) 本認証局は、ホストマスタ証明書の申請者による証明書のダウンロードをもって、証明書の受領を確認する。
4.6.1 証明書更新が行われる場合 規定しない。	(新設)
4.6.2 証明書の更新を申請することができる者 規定しない。	(新設)
4.6.3.証明書の更新申請の処理 規定しない。	(新設)

4.6.4 所有者に対する新しい証明書の通知 規定しない。	(新設)
4.6.5.更新された証明書の受領確認の行為 規定しない。	(新設)
4.6.6.認証局による更新された証明書の公開 規定しない。	(新設)
4.6.7.他のエンティティに対する通知 規定しない。	(新設)
4.9.1.証明書失効の場合 ホストマスタ証明書の証明書所有者は、メンバ管理者に証明書の失効申請を行わなければならない。 メンバ管理者証明書の証明書所有者は、JPNIC に証明書の失効申請を行わなければならない。 本認証局は次の項目に該当すると認めた場合、メンバ管理者証明書とホストマスタ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 ・証明書所有者あるいは LRA が、本 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	**4.9.1.証明書失効の場合** 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。 (追加) 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他に、次の項目に該当すると認めた場合、ホストマスタ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
4.9.2.証明書失効を申請することができる者 ホストマスタ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、メンバ管理者 本認証局	**4.9.2.証明書失効を申請することができる者** ホストマスタ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
4.9.3. 失効申請手続	**4.9.3. 失効申請手続**

メンバ管理者は所定の手続きに従って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。 JPNIC は所定の手続きに従って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。	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。 (追加)
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 本認証局における証明書の失効処理は、失効申請の受領後、24 時間以内に行われる。	**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** 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、(時間は決定後に記述される) 時間以内に行われる。
4.9.14.証明書の一時停止を申請することができる者 規定しない。	(新設)
4.9.15 証明書の一時停止申請手続き 規定しない。	(新設)
4.9.16.一時停止を継続することができる期間 規定しない。	(新設)
4.12.キーエスクローと鍵回復 本認証局は私有鍵を第三者に対して寄託しない。 (削除)	**4.12.キーエスクローと鍵回復** 本認証局は私有鍵を第三者に対して寄託しない。 EE は私有鍵を EE 自身で生成及び管理する。
4.12.1 キーエスクローと鍵回復ポリシ及び実施 規定しない。	(新設)
4.12.2 セッションキーのカプセル化と鍵回復ポリシ及び実施 規定しない。	(新設)
5.1.1.立地場所及び構造 本認証局に係わる重要な設備については、火災、(削除)水害、地震、落雷(削除)その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震、耐火及び不正侵入防止のための対策を講ずる。建物の内外には、認証設備室の所在についての表示を行わない。	**5.1.1.立地場所及び構造** 本認証局に係わる重要な設備については、火災、電磁界、水害、地震、落雷、空気汚染その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震、耐火及び不正侵入防止のための対策を講ずる。建物の内外には、認証設備室の所在についての表示を行わない。
5.1.2.物理的アクセス 本認証局は、認証設備室に関して、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を行う。(削除) 本認証局は、入室権限を有しない者の入室を原則として認めない。やむを得ずこれを認める場合は、予め認証局運用管理者の許可を得て、入室権限者同行のうえこの者を入室させることとする。	**5.1.2.物理的アクセス** 本認証局は、認証設備室に関して、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を行い、また監視カメラによる記録を行う。認証設備室への立入には、入室権限を有する複数人が同時に操作する必要がある。本認証局は、入室権限を有しない者の入室を原則として認めない。やむを得ずこれを認める場合は、予め認証局運用管理者の許可を得て、入室権限者同行のうえこの者を入室させることとする。

5.1.4.水害及び地震対策 本認証局の設備を設置する室は防水対策を施し、浸水による被害を最小限に抑える。また、JPNIC 認証局は、地震等による機器及び什器の転倒及び落下を防止する対策を講ずる。	**5.1.4.水害及び地震対策** 本認証局の設備を設置する建物及び室には漏水検知器の設置等、防水対策を施して浸水による被害を最小限に抑える。また、JPNIC 認証局は、地震等による機器及び什器の転倒及び落下を防止する対策を講ずる。
5.1.6 媒体保管場所 アーカイブデータ、バックアップデータを含む媒体は、適切な入退管理が行われた室内の保管庫に保管される。また複製された重要な媒体は、本認証局の設置場所とは別の適切な入退管理が行われた室内の保管庫に保管される。	**5.1.6. 媒体保管場所** アーカイブデータ、バックアップデータを含む媒体は、適切な入退管理が行われた室内の保管庫に保管される。また複製された重要な媒体は、別地の適切な入退管理が行われた室内の保管庫に保管される。
5.2.1. 信頼される役割 証明書の発行、更新、失効等の重要な業務に携わる者は、本 CPS 上信頼される役割を担っている。認証局では、業務上の役割を特定の個人に集中させず、複数人に権限を分離している。 (表 5-1 とともに削除)	**5.2.1.信頼される役割** 証明書の発行、更新、失効等の重要な業務に携わる者は、本 CP/CPS 上信頼される役割を担っている。JPNIC 認証局では、業務上の役割を特定の個人に集中させず、複数人に権限を分離している。JPNIC 認証局運営上の役割を表 5-1 に示す。
5.2.2.職務ごとに必要とされる人員 (削除) 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、認証設備室への入室権限を有しない者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。	**5.2.2.職務ごとに必要とされる人数** 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。また、JPNIC 登録局の端末を用いた発行・失効等の操作は複数人の RAO 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、認証設備室への入室権限を有しない者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。
5.2.3.個々の役割に対する本人性確認と認証 認証局の設備は、操作者及び必要権限を識別する機能を有するものとする。また、認証局設備を操作する権限は、操作者ごとに設定可能であるものとする。	**5.2.3.個々の役割に対する本人性確認と認証** JPNIC 認証局の設備は、操作者及び必要権限を識別する機能を有するものとする。また、JPNIC 認証局設備を操作する権限は、操作者ごとに設定可能であるものとする。
5.2.4.職務分割が必要となる役割 (削除)権限を特定の個人に集中させず複数人に権限を分離することで、単独操作で発生する不正行為等の防止を図る。システム操作、承認行為及び監査に関する権限は分離される。	**5.2.4.職務分割が必要となる役割** JPNIC 認証局では、権限を特定の個人に集中させず複数人に権限を分離することで、単独操作で発生する不正行為等の防止を図る。システム操作、承認行為及び監査に関する権限は分離される。
5.3.2.人員配属に関する規定事項 認証局業務に関わる要員を任命するにあたって、業務の遂行上支障が出ない適切な人員を配置する。配属されるものは機密保持及び内部規定の遵守に対する誓約書を提出する。	**5.3.2.経歴の調査手続** JPNIC 認証局業務に係わる要員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.研修要件	**5.3.3.研修要件**

(削除)運用要員の教育を次のように行う。	JPNIC 認証局は、運用要員の教育を次のように行う。
5.3.4.再研修の頻度及び要件 JPNIC は定期的に本認証局の要員に対して適切な教育を行い、以降必要に応じて再教育を行う。	**5.3.4.再研修の頻度及び要件** JPNIC は定期的に JPNIC 認証局の要員に対して適切な教育を行い、以降必要に応じて再教育を行う。
5.3.6.認められていない行動に対する処罰 JPNIC は、本認証局の運用要員による認可されていない行為に対し、予め決められた規程に従って処罰する。	**5.3.6.認められていない行動に対する制裁** JPNIC は、JPNIC 認証局の運用要員による認可されていない行為に対し、(罰則規定書の名称は決定後に記述される）に従って制裁を与える。
5.3.8.要員へ提供される資料 運用に必要な文書を運用要員に開示し周知する。 (削除)	**5.3.8.要員へ提供される資料** JPNIC 認証局は次の文書を運用要員に開示し周知する。 ・本 CP/CPS ・認証局運用に関する諸規程、手続書、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、要員に提供されるべき文書があれば決定後に記述される。）
5.4.1.記録されるイベントの種類 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に関する記録 ・証明書の発行及び失効等の作業に関する記録 ・失効情報の作成作業に関する記録 ・監査ログの確認に関する記録 また、認証局設備へのアクセスに関する履歴を記録する。	**5.4.1.記録されるイベントの種類** 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

5.4.3.監査ログを保持する期間 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、外部記憶媒体に一定期間保管される。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。	**5.4.3.監査ログを保持する期間** 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。
5.5.1.アーカイブ記録の種類 本 CPS「5.4.1.記録されるイベントの種類」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】 ・本認証局の署名用鍵ペアの生成 ・システムからの証明書所有者の追加及び削除 ・証明書の発行・失効を含めた鍵の変更 ・登録局管理者権限の追加、変更及び削除 (削除) 【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。 (削除) ・本 CPS、証明書所有者同意書及びその変更に関する記録(削除) ・認証業務に従事する者の責任及び権限(削除)に関して記載した文書及びその変更に関する記録(削除) (削除) ・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(削除) ・監査の実施結果に関する記録及び監査報告書(削除)	**5.5.1.アーカイブ記録の種類** 本 CP/CPS「5.4.1.記録されるイベントの種類」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】 ・本認証局の署名用鍵ペアの生成 ・システムからの証明書所有者の追加及び削除 ・証明書の発行・失効を含めた鍵の変更 ・登録局管理者権限の追加、変更及び削除 ・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） ・証明書申請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）
5.5.2.アーカイブ保持期間	**5.5.2.アーカイブ保持期間**

本認証局は、認証局システムのデータベースの履歴及び監査ログファイルの履歴を一定期間保存する。紙媒体及び外部記憶媒体の保存期間に関しては本CPS「5.5.1.アーカイブ記録の種類」に規定する。	本認証局は、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を最低 10 年間保存する。紙媒体及び外部記憶媒体の保存期間に関しては本CP/CPS「5.5.1.アーカイブ記録の種類」に規定する。
5.5.3.アーカイブ保護 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。本認証局は、アーカイブデータのバックアップを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者以外の者がアクセスできないように制限し、温度、湿度（削除）等の環境上の脅威から保護された施設に保管する。	**5.5.3.アーカイブ保護** 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。本認証局は、アーカイブデータのバックアップを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者以外の者がアクセスできないように制限し、温度、湿度、磁気等の環境上の脅威から保護された施設に保管する。
5.5.4.アーカイブのバックアップ手続 本認証局は、認証局システムの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、（削除）監査ログも定期的に外部記憶媒体に格納する。	**5.5.4.アーカイブのバックアップ手続** 本認証局は、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。
5.5.5.記録にタイムスタンプを付ける要件 本認証局は、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。ここでいうタイムスタンプとは暗号技術を用いたものではない。	**5.5.5.記録にタイムスタンプを付ける要件** 本認証局は、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。
5.7.3.エンティティの私有鍵が危殆化した場合の手続 認証局私有鍵が危殆化した場合は、予め定められた計画に基づいて認証業務を停止し、次の手続を行う。 ・ホストマスタ証明書、サーバ証明書等の失効手続 ・認証局私有鍵の廃棄及び再生成手続 ・ホストマスタ証明書、サーバ証明書等の再発行手続 また、証明書所有者の私有鍵が危殆化した場合は、本 CPS「4.9.証明書の失効と一時停止」において定める手続に基づき、証明書の失効手続を行う。	**5.7.3.エンティティの私有鍵が危殆化した場合の手続** 認証局私有鍵が危殆化した場合は、予め定められた計画に基づいて認証業務を停止し、次の手続を行う。 ・ホストマスタ証明書、サーバ証明書等の失効手続 ・認証局私有鍵の廃棄及び再生成手続 ・ホストマスタ証明書、サーバ証明書等の再発行手続 また、証明書所有者の私有鍵が危殆化した場合は、本 CP/CPS「4.9.」において定める手続に基づき、証明書の失効手続を行う。
5.8.認証局又は登録局の終了 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及び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 14 日前までに証明書所有者及び証明書検証者に告知し、所定の業務終了手続を行う。	**5.8.認証局又は登録局の終了** 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及び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証明書検証者に告知し、所定の業務終了手続を行う。
6.1.1.鍵ペアの生成 本認証局の鍵ペアの生成は鍵管理者立会いのもと、	**6.1.1.鍵ペアの生成** 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、FIPS140-1 レベル 3 の暗号化モジュールを使用して行われる。 メンバ管理者証明書の鍵ペアの生成は、FIPS140-2 レベル 3 の暗号化モジュールを使用して行われる。	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。 （追加）
6.1.2.所有者に対する私有鍵の交付 メンバ管理者証明書の鍵ペアの生成は、本認証局において暗号化モジュール内で行われる。生成された鍵ペアは暗号化モジュールを含むハードウェアトークンを使って、メンバ管理者証明書の申請者に交付される。 本認証局はホストマスタ証明書の鍵ペアの作成を行わないため、本項の規定を行わない。	**6.1.2.所有者に対する私有鍵の交付** （追加） 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.証明書発行者に対する公開鍵の交付 ホストマスタ証明書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。	**6.1.3.証明書発行者に対する公開鍵の交付** 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.検証者に対する認証局の公開鍵の交付 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。 ・（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。証明書検証者は（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。証明書検証者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、ホストマスタにはメンバ管理者が本認証局の証明書を手渡しする。	**6.1.4.検証者に対する認証局の公開鍵の交付** 本認証局の証明書の配布は、次にあげる 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。証明書検証者は（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。証明書検証者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。
6.1.7.鍵用途の目的 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、サーバ証明書及び 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、dataencipherment のビットを使用する。S/MIME、SSL/TLS のクライアント証明書としてのみ使用す	**6.1.7.鍵用途の目的** 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（追加）及び 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（追加）のビットを使用する。S/MIME、SSL/TLS のクライアント証明書としてのみ使用するものとする。

るものとする。	
6.2.7.暗号モジュールへの私有鍵の格納 本認証局の私有鍵は、安全性の高い暗号化モジュール内で生成、格納される。 ホストマスタの私有鍵はホストマスタ自身が私有鍵の生成を行い、ホストマスタ自身で格納を行う。メンバ管理者の秘密鍵は JPNIC において、安全性の高い暗号化モジュール内で生成、格納される。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.暗号モジュールへの私有鍵の格納** 本認証局の私有鍵は、安全性の高い暗号化モジュール内で生成、格納される。 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。（追加） 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。
6.2.10.私有鍵の破棄方法 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。メンバ管理者の秘密鍵は基本的に JPNIC において破棄するものとする。ただし、紛失等の場合はこの限りではない。	**6.2.10.私有鍵の破棄方法** 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。（追加）
6.3.1.公開鍵のアーカイブ 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。 （削除）	**6.3.1.公開鍵のアーカイブ** 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。
7.1.2.3.keyUsage ホストマスタ証明書は digitalSignature、keyEncipherment、dataEncipherment を試用する。 サーバ証明書は digitalSignature と keyEncipherment のみを使用する。この拡張は non-critical である。	**7.1.2.3.keyUsage** ホストマスタ証明書、サーバ証明書共に digitalSignature と keyEncipherment のみを使用する。この拡張は critical である。
7.1.6.証明書ポリシ OID ホストマスタ証明書、メンバ管理者証明書、サーバ証明書のいずれも本 CPS「1.2.文書の名前と識別」に定める EE 証明書ポリシの OID を使用する。	**7.1.6.証明書ポリシ OID** ホストマスタ証明書、（追加）サーバ証明書共に本 CP/CPS「1.2.文書の名前と識別」に定める EE 証明書ポリシの OID を使用する。
7.1.9.critical な証明書 certificatePolicies 拡張の処理 表 7-1 JPNIC 資源管理認証局が発行する証明書プロファイル ・keyUsage…n (Field 追加)	**7.1.9.critical な証明書 certificatePolicies 拡張の処理** 表 7-1JPNIC IP アドレス認証局が発行する証明書プロファイル ・ keyUsage…c data Encipherment　ホストマスタ証明書 1 サーバ証明書　0

※2　C=JP, O=（組織名称）, O=Resource Holder, O=LIR Corporate Administrator, OU=（LIR Corporate Administrator、LIR Administrator、LIR Hostmaster のいずれか）, OU=（JPNIC が資源管理の単位ごとに割り当てるメンテナーコード）CN=（LIR-CO、LIR-AD、LIR-HM のいずれか）＋（JPNIC がユーザごとに割り当てる認証 ID）＋（証明書発行対象ホストマスタの名称をアルファベット表記したもの）	※ 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）
7.3.1.バージョン情報 使用しない。	（新設）
7.3.2.OCSP 拡張 使用しない。	（新設）
8.1.評価の頻度又は評価が行われる場合 本認証局は必要に応じて監査を実施する。	**8.1.評価の頻度又は評価が行われる場合** 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。
8.3.評価人と評価されるエンティティとの関係 JPNIC は、本認証局の認証業務に関わる要員以外から監査者を選定する。	**8.3.評価人と評価されるエンティティとの関係** JPNIC は、本認証局を含む JPNIC 認証局の認証業務に係わる要員以外から監査者を選定する。
8.4.評価で扱われる事項 本認証局の準拠性監査は、認証局の運営が本 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。 （削除） 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。	**8.4.評価で扱われる事項** 本認証局を含む JPNIC 認証局の準拠性監査は、認証局の運営が本 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。 主な監査項目は次のとおりである。 ・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 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。
9.2.財務的責任 規定しない。	**9.2.財務的責任** 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、IP アドレス管理指定事業者等との契約における該当条項に従う。
9.3.3.秘密情報を保護する責任	**9.3.3.秘密情報を保護する責任**

本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。また、本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。更に、本認証局では、メンバ管理者から、メンバ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、メンバ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、メンバ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。	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。また、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。更に、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。
9.4.2.プライバシとして扱われる情報 規定しない。	（新設）
9.4.3.プライバシとはみなされない情報 規定しない。	（新設）
9.4.4.個人情報を保護する責任 JPNIC 認証局は、本 CPS「9.4.1.プライバシポリシ」に則って個人情報を保護する責任を負う。	（新設）
9.4.5.個人情報の使用に関する個人への通知及び承諾 規定しない。	（新設）
9.4.6.司法手続又は行政手続に基づく公開 規定しない。	（新設）
9.4.7.他の情報公開の場合 規定しない。	（新設）
9.6.1.発行局の表明保証 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 (削除) ・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	**9.6.1.発行局の表明保証** 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 （削除） ・本 CPS に従った受付時間内の問合せ受付	・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
9.6.3.ローカル登録局の表明保証 LRA は、LRA 業務を遂行するにあたり次の義務を負う。 ・（削除）証明書所有者と証明書申請者が同一であることの検証	**9.6.3.ローカル登録局の表明保証** LRA は、LRA 業務を遂行するにあたり次の義務を負う。 ・申請書類上の証明書所有者と証明書申請者が同一であることの検証
9.12.2 通知方法及び期間 本認証局は、変更された CPS をその改訂が有効になる 10 営業日前までに、変更履歴とともにリポジトリに公開することにより、証明書所有者及び関係者に改訂の通知を行うものとする。	**9.12.2.通知方法及び期間** 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、変更履歴とともにリポジトリに公開することにより、証明書所有者及び関係者に改訂の通知を行うものとする。
9.17.その他の条項 規定しない。	（新設）