第5章 IP アドレス認証局のマネジメントに関する検討と構築

内容

- 認証情報の検討
- 認証業務の設計
- システム構成
- 業務フロー
- 画面イメージ

第5章　IP アドレス認証局のマネジメントに関する検討と構築

本年度の調査研究は、2003 年度、2002 年度の調査研究をもとに IP アドレス認証局の構築を行い、更に実験的に運用を行った。

IP アドレス認証局の構築あたり、はじめにマネジメントの形態の検討を行い、次に認証業務の設計と構築を行った。

5.1. 認証情報の検討

インターネットレジストリにおける登録者の認証情報は、割り振りを行ったアドレス資源の情報と関連する形で保持している必要がある。本調査研究では、認証業務の検討に先立ち、資源管理情報を管理する IP レジストリシステムにおいて証明書の情報を含む認証情報をどのように格納すべきかについて検討を行った。

本節では認証情報をまとめ、資源管理情報と関連させる”メンテナー”のあり方について述べる。ここでいうメンテナーは RIPE NCC 等で利用されている RPSL（Routing Protocol Specification Language）で使われている概念とは若干異なり、日本の資源管理の形態に合わせて設計しなおしたものである。

本節は現状調査と各モデルの不具合を洗い出しながら、クライアント証明書の扱いに最も適するメンテナーのモデルについて述べる。

5.1.1. 現状の IP レジストリシステム上の認証

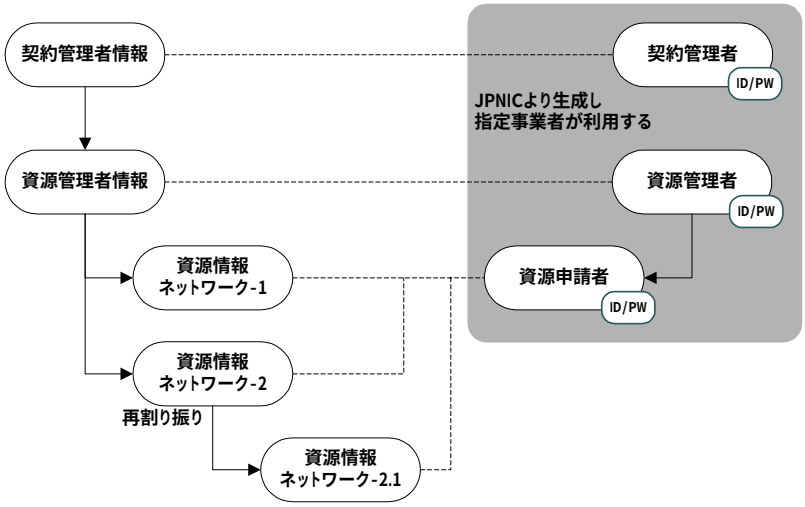
契約が成立した指定事業者には、JPNIC より表 5.1.2.1.-1、図 5.1.2.1.-2 にて業務に応じた３通りの権限に応じた認証を提供している。これは、対象となる業務申請権限となり、各種申請の正当性を図る目的がある。

表 5.1.2.1-1　主な業務毎の処理実施可否について

主な業務名称	契約管理者	資源管理者	資源申請者
指定事業者契約関連	○	×	×
資源管理情報関連	○	○	×
資源情報関連	×	×	○

- 契約管理者：契約情報の保守及び、配下の資源管理者に対しての請求先情報の保守も可能となる。
- 資源管理者：資源情報（割り振り/割り当てアドレス）を統括する管理者情報の保守が可能となる。
- 資源申請者：資源情報（割り振り/割り当てアドレス）の申請業務が可能となる。

図 5.1.2.1-2　IP レジストリデータと利用権限の関連図



5.1.2. メンテナー情報の導入目的

指定事業者で管理している割り振り/割り当てアドレス情報（以下、資源情報）全体に対して、申請権限があるが、指定事業者内の部署別利用制限や、ダウンストリーム（二次指定事業者以降）の利用制限をすることで、より細かな申請制限が必要と考えられてきた。また、現状の認証 ID/パスワードに加え、IP アドレス認証局によるクライアント証明書を導入する事で、更なる情報の安全性に繋がるものとする必要がある。

これらを踏まえて、現状の認証 ID/パスワード及び、クライアント証明書を権限グループとして管理するメンテナー情報を設け、操作対象単位に連結する事により実現させる事となる。

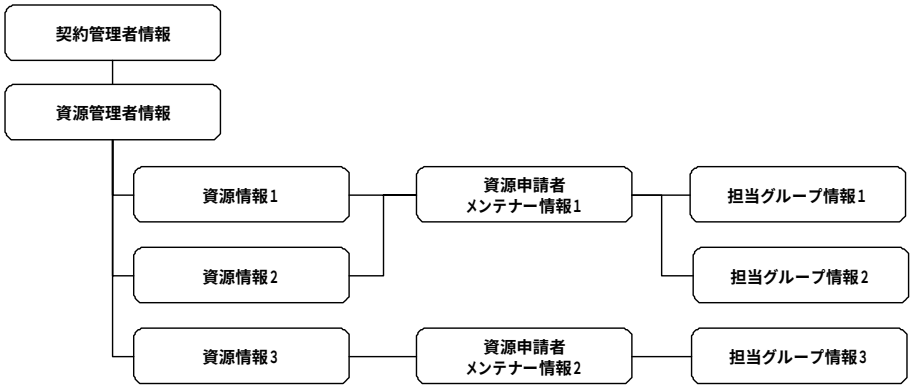
JPNIC のデータには、担当グループ情報が存在する。これは、各種資源情報に、1 担当者の連絡先連絡先となる担当者情報が別に設けており、何らかの問い合わせをする際に利用されている。担当者が所属する指定事業者の組織名や住所等の変更により、関わる膨大な担当者情報変更申請を指定事業者がおこなう必要があった。

そこで、次期 IP レジストリシステムでは、連絡先となる情報を部署単位に設定する担当グループ情報を新たに設置し対処する考えで進められている。

この担当グループ情報には､メンテナー情報のグループの考えと一致していた事から､図 5.1.2.1-3 に示しているデータ構成が考えられる。

メンテナー情報内の組織名・住所等の変更で、属する担当グループ情報にも反映される。これにより、指定事業者の情報変更申請への手間を軽減する事に繋がるものと考えられてきた。また、メンテナー情報導入目的にもある、クライアント証明書を担当グループ単位に設定する事により、認証管理及び指定事業者内の所属管理にも繋がると考えられる。

図 5.1.2.1-3　担当グループ情報とメンテナー情報の関連図



しかし、担当グループ情報は、指定事業者情報つまり資源管理者情報とは無関係となっている為に、組織部署単位に登録が出来たとしても、その情報と指定事業者との関わりが安易な情報と捕らえられる。また、他組織の資源情報についても連結が可能となっており、柔軟なデータ構成で利用するユーザにとって扱い易い反面、メンテナー情報と連結し認証情報を付加させるには、問題があると想定される。その結果、担当グループ情報については、考慮せず検討を進めて行くこととなる。

5.1.2.1. メンテナー情報と認証ID/パスワードについて

現状の認証 ID/パスワードを次期 IP レジストリシステムでもそのまま引継ぎ、利用している指定事業者に対して、無用な混乱をさける必要があると考えられる。図 5.1.2.1.-4 で、メンテナー情報への移行方法を記載している。各情報は権限（契約管理者・資源管理者・資源申請者）の識別子も移行対象となる。移行されたメンテナー情報を直接的に、指定事業者が保持している資源情報と連結する事により、現状のデータ構成と変わりなく利用可能となる。

図 5.1.2.1-4　認証 ID/パスワードとメンテナー情報への移行図

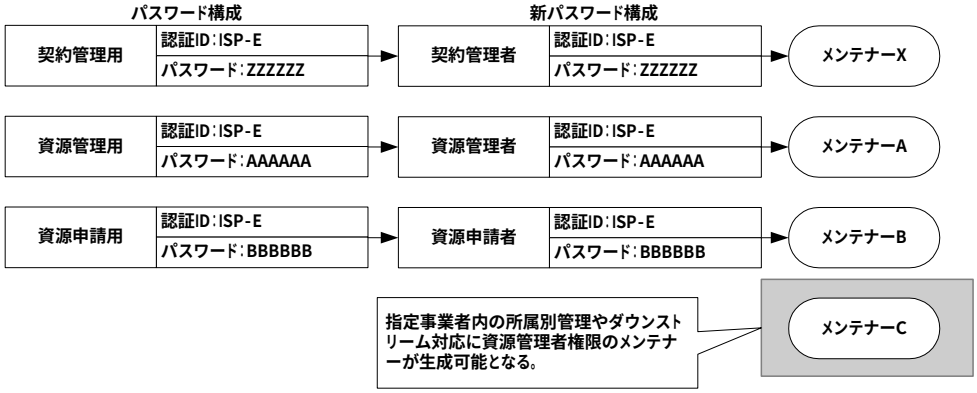
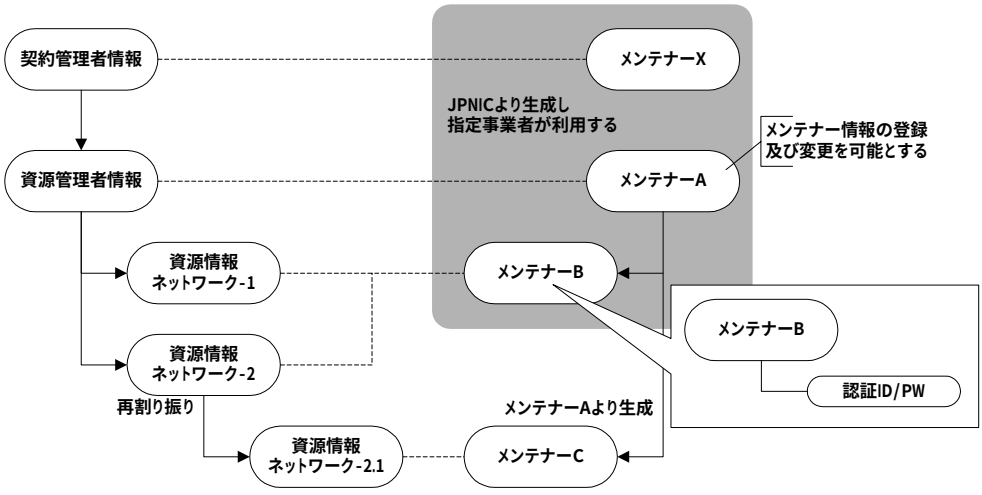


図 5.1.2.1.-5 では､IP レジストリデータとメンテナー情報との関連を記載している。資源管理者メンテナー（図中のメンテナーA）が、必要に応じて資源申請者メンテナー（図中のメンテナーC）を生成し、対象資源情報へ連結する事により、メンテナー情報導入目的にもある、指定事業者内の部署別利用制限や、ダウンストリーム（二次指定事業者以降）の詳細的な利用制限が実現する事になる。

図 5.1.2.1.-5　IP レジストリデータとメンテナー情報の関連図



5.1.2.2. メンテナー情報とクライアント証明書について

既に、個々の資源情報へ連結されているメンテナー情報に対して、クライアント証明書を付加させる事により、権限識別が含まれたクライアント証明書が利用可能となる。

図 5.4.2.2.-1 において、資源申請者メンテナー毎にクライアント証明書を設置した場

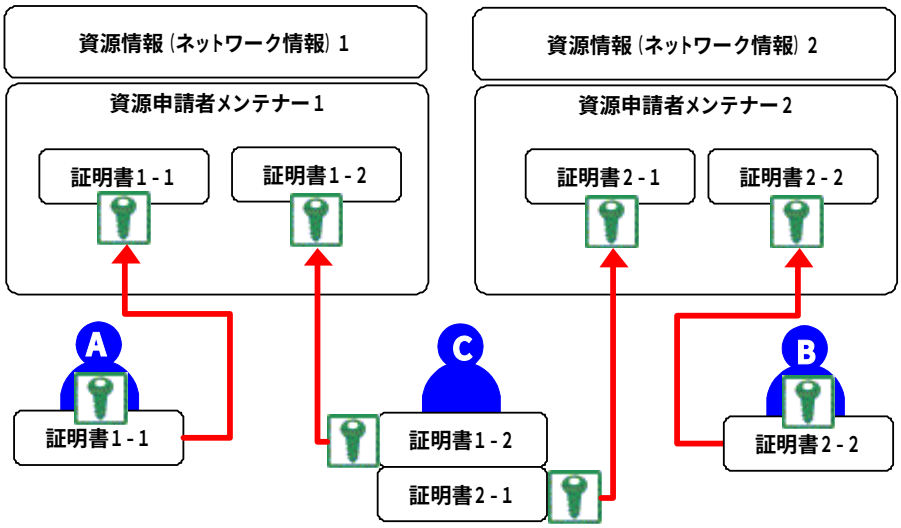
合に、図中の A が保持している証明書１－１で資源情報１へのアクセスが可能となる。また、図中の B においても同様の方法で資源情報２へアクセス可能となる。

しかし、資源情報１と資源情報２へ、それぞれに対してアクセスしたい図中の C については、メンテナー単位にクライアント証明書が異なる為に、必要に応じて利用するクライアントへの取り込む必要があり、その保守対象となる資源情報別に使い分けをする必要がある。また、クライアント証明書を管理する上で、どの証明書を無効にするべきか判断する必要があり、何らかのトラブルで特定クライアントまで追う事が出来ず、他のクライアントにも影響があると考えられる。

これらの懸念していた問題点を、回避する為に以下のモデル案を検討してきた。

- メンテナー情報のグループ管理モデル
- メンテナー情報での共有利用モデル

図 5.4.2.2.-1　メンテナー情報内のクライアント証明書



5.4.2.2.1. メンテナー情報のグループ管理モデル

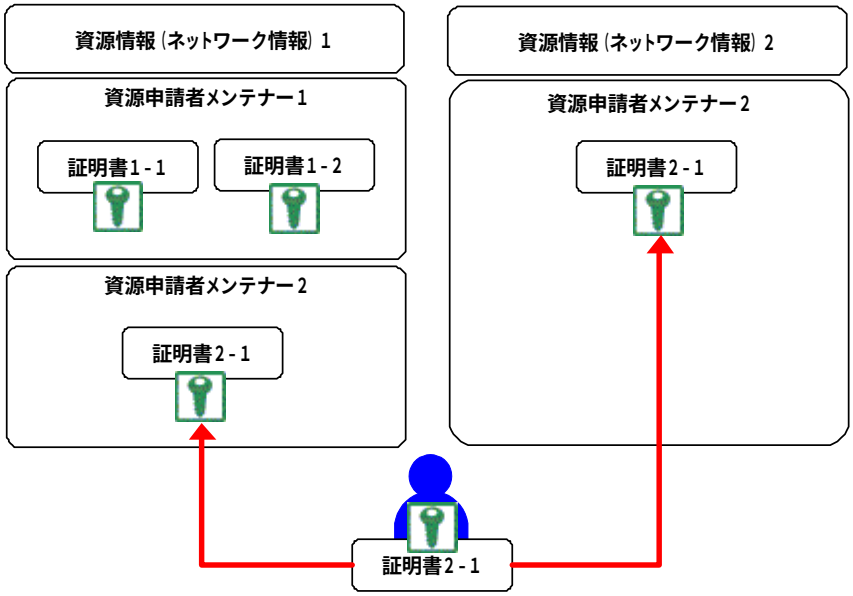
図 5.4.2.2.1.-1 では、資源情報に応じて資源申請メンテナーが異なりそのクライアント証明書もまた違う。ある一定のグループに集約し、資源申請者メンテナー単位に資源情報へ連結するモデルである。

利用するクライアントには、既に取り込まれている単一のクライアント証明書で簡略化されるが、資源情報には複数の資源申請者メンテナーを連結させる必要があり、その管理が必要と考えられる。また、クライアント証明書を別の資源申請者メンテナーへ移す場合に、保守可能な資源情報の把握が必要となる。それは、図中の証明書２－１を資源申請者メンテナー１へ移した場合、資源情報２の保守が不可能となる。

当モデルは、利用する側を考慮した場合であり、そのクライアント証明書や保守可能

となる資源情報との管理が必要である。回避策としては、資源情報に属するメンテナー管理及びメンテナー内のメンバ管理を容易におこなう管理者用機能を提供する事が考えられる。

図 5.4.2.2.1.-1　メンテナー情報単位のグループ管理モデル案



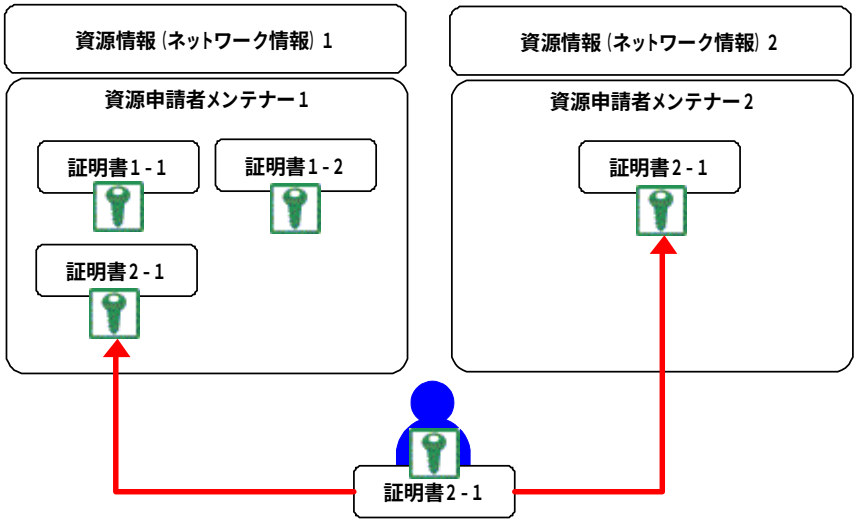
5.4.2.2.2. メンテナー情報での共有利用モデル

図 5.4.2.2.2.-1 では、クライアント証明書を各資源申請者メンテナーで共有利用をおこなうモデルである。

既に利用されるクライアントに取り込まれている為に、資源申請メンテナーのメンバ変更をおこなうだけで簡略化できる。また、失効手続きについても、単一クライアント証明書さえ把握していれば、最小限の対応で回避出来ると考えられる。

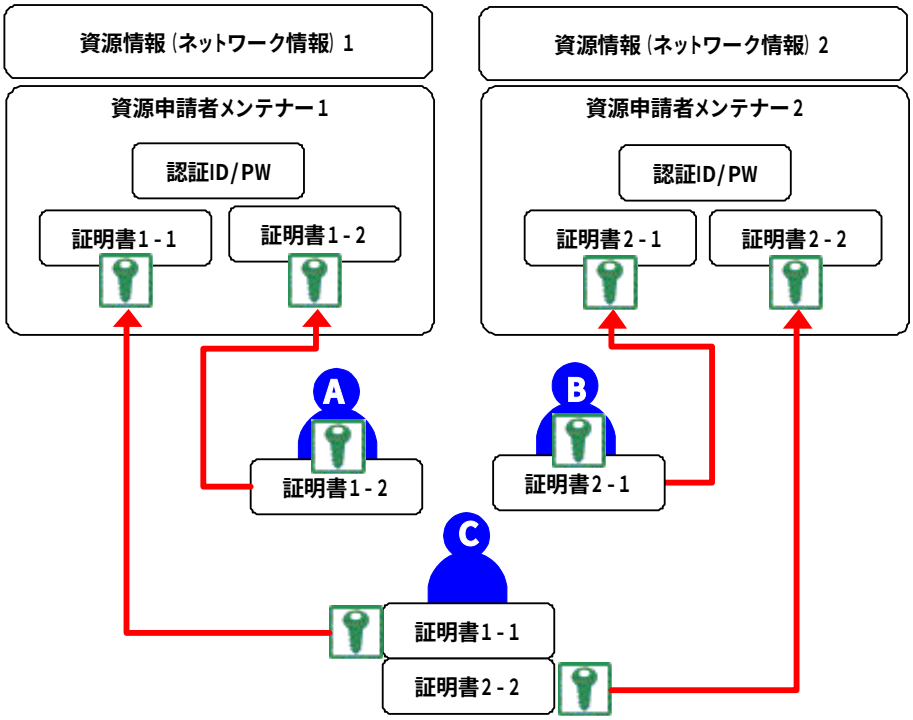
しかし、資源申請者メンテナーに対して、どのクライアント証明書が設定されているのか情報管理が困難と考えられる。

図 5.4.2.2.2.-1　クライアント証明書共有利用モデル案



5.4.2.2.3. クライアント証明書の扱い

これらの検討結果により、クライアント証明書の管理を複雑におこなうよりも、簡略的に対応するのが望ましいと考えられる。そこで、懸念していた状態（図中の C）は、それぞれのメンテナー情報に設定されているクライアント証明書を使い分けて利用することとし、今後の利用状況に応じて改良する事となる。



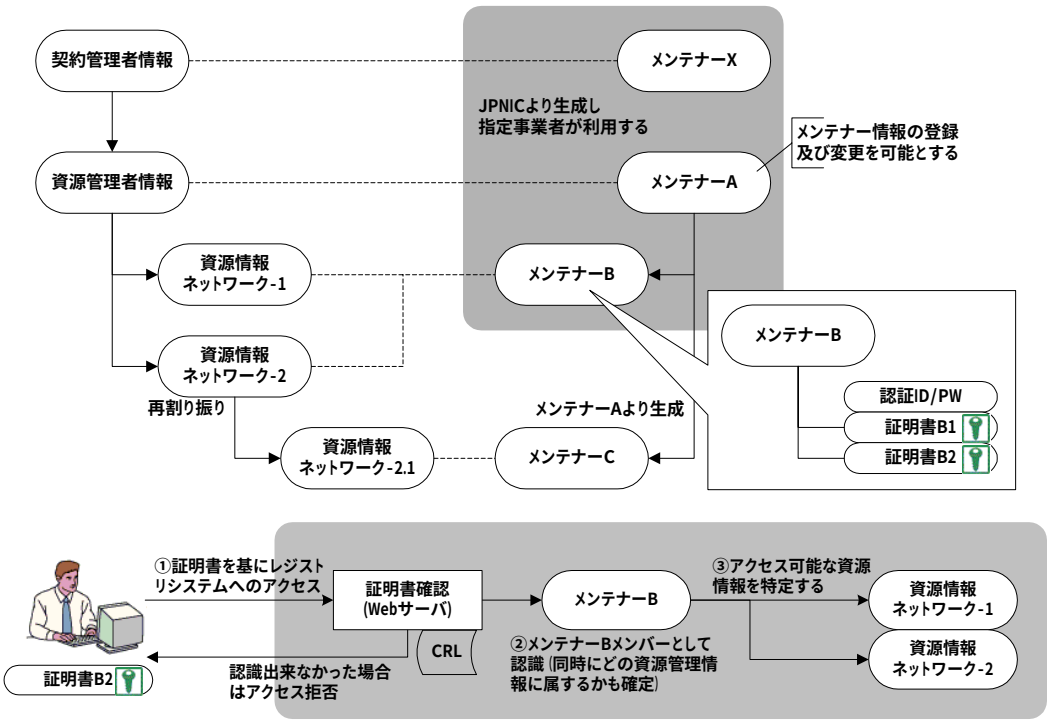
5.1.2.3. IPレジストリシステムとクライアント証明書の関連について

図 5.4.2.3.-1 でメンテナー情報内には、認証 ID/パスワードと複数のクライアント証明書が権限グループとなり管理され、連結されている資源情報のみ保守可能となる。

認証 ID/パスワード又は、クラアント証明書にてアクセスされたら、メンテナー情報を特定し、そのメンテナー情報が保守可能となる資源情報へ紐づく事になる。

クライアント証明書が漏洩した場合の対応策としては、特定のメンテナー又はクライアント証明書を無効化にする管理機能を提供し、被害は最小限に抑える事が可能となる。

図 5.1.2.3.-1　IP レジストリデータとメンテナー情報の関連図



5.2. 認証業務の設計

IP アドレス認証局は役割ごとに認証局を設け、それぞれの認証局の構築が行われた。IP アドレス認証局は、JPNIC ルート認証局、IP アドレス認証局（認証）、IP アドレス認証局（証明）の三つである。2003 年度に行った業務モデルは、IP アドレス認証局（認証）に適用された。

IP アドレス認証局（認証）は、IP レジストリシステム等における認証を目的とした証明書を発行する認証局である。アドレス資源管理におけるユーザの定義に合わせて設計しつつ、クライアント証明書を用いることのメリット（強い認証と個別の有効性管理）を生かす設計を行った。

なお、下記に述べる設計および業務フローは 2004 年度の調査研究を行っている段階のものであり、基本的な設計方針は変わらないものの実際の業務とは異なることがある。

5.2.1. IP アドレス認証局の要求仕様

IP アドレス**認証局**の設計および構築に先立って、IP アドレス認証局の機能を実現する「認証局システム」の要求仕様の明確化を行った。この要求仕様を以下に述べる。

5.2.1.1. 目的

当センターでは、認証局の運用実験を計画している。開発中の IP レジストリシステムにおける利用者認証に SSL/TLS クライアント認証を用いるため、当センターの契約者に証明書を発行する認証局と、それに付随する WEB 申請受付けサーバの開発を行なう。また、実証実験向けの認証局として IP アドレス認証局（証明）を構築し、RFC3779 で提案されているフィールドをもつ証明書の発行を行なう。

5.2.1.2. 基本方針

認証局に関する要件として、ルート認証局である「JPNIC ルート認証局」の構築、その下位の認証局である「IP アドレス認証局（認証）」「IP アドレス認証局（証明）」の構築、さらに IP アドレス認証局（証明）の下位の認証局である「実証実験向け LIR 認証局」の構築を行なう。このうち、JPNIC ルート認証局と IP アドレス認証局（認証）を運用環境用として運用し、IP アドレス認証局（証明）と実証実験向け LIR 認証局を実証実験環境として運用することを目的とする。

それぞれの認証局には証明書を出力するリポジトリが必要であり、運用向けと実証実験向け環境にそれぞれハードウェアを用意し、LDAP サーバをリポジトリとして運用する。

IP レジストリシステムとの連携により発生する業務は以下の通りである。

(1) JPNIC 業務管理者認定業務

IP アドレス認証局（認証）を構築後、CA 管理ツール（GUI）を使用して JPNIC 業務管理者に対して証明書を発行する。発行した証明書は直接 JPNIC 業務管理者に手渡す。

(2) 内向き用（JPNIC 業務管理者）申請受付業務
業務管理者は、業務担当者に対して証明書の発行、更新、失効操作を行なう。

(3) 内向き用（JPNIC 業務担当者）申請受付業務
業務担当者は、契約者（メンバ管理者）のリスト表示と、新規契約者に対して証明書の発行、契約者に対して証明書の更新、失効操作を行なう。

(4) 外向き用（メンバ管理者）申請受付業務
IP レジストリシステムと連携し、メンバ管理者によるメンバの追加とメンバの削除業務を行なう。メンバの追加を行なうと、ライセンス ID の表示と登録完了通知メールの送信が行われる。

(5) 外向き用（ホストマスタ）申請受付業務
メンバ管理者からライセンス ID を受け取り、この ID を使用してメンテナー申請者自身が使用する証明書の申請を行なう。

これらの業務が行なえるように、CGI モジュールの開発を行なっていく。

5.2.1.3. システム構築の要求事項

前節で定義した認証局と認証局システムの構成に対し、仕様上、それぞれに要求される事項をいかに満たすかという検討を行った。

（1） 認証局の役割の実現

	要求事項	内容	対応方針
1	運用向け CA 構成	「JPNIC ルート認証局」「IP アドレス認証局（認証）」の認証局を構成する。	JPNIC ルート認証局と IP アドレス認証局（認証）を構築し、HSM を付加する。
2	実証実験向け CA 構成	「IP アドレス認証局（証明）」「実証実験向け LIR 認証局」の認証局を構成する。	IP アドレス認証局（証明）と実証実験向け LIR 認証局を構築する。
3	ルート認証局	「JPNIC ルート認証局」は、「IP アドレス認証局（認証）」「IP アドレス認証局（証明）」の認証局証明書の発行と管理を行なう。	JPNIC ルート認証局にて Sub-CA のプロファイルを適用した証明書発行が可能である。鍵ペアの生成と下位 CA 証明書の発行を行ない、それぞれ下位の CA に対して PKCS#12 ファイルを提供できる。

4	IP アドレス認証局（認証）	IA、RA、PA の機能、および開発を伴った Web インタフェースと連携するための機能。	IA、RA については 1 つの CA サーバがこれらの代用として動作する。PA については項番 5「運用向けリポジトリ」を参照のこと。Web インタフェースの開発については、項番 7「内向き用申請受付けサーバ」、項番 8「外向き用申請受付けサーバ」を参照のこと。
5	運用向けリポジトリ	「JPNIC ルート認証局」「IP アドレス認証局（認証）」のリポジトリを構成する。	JPNIC ルート認証局と IP アドレス認証局（認証）のリポジトリを構成する。リポジトリのプロトコルには LDAP を使用する。
6	実証実験向けリポジトリ	「IP アドレス認証局（証明）」「実証実験向け LIR 認証局」のリポジトリを構成する。	IP アドレス認証局（証明）と実証実験向け LIR 認証局のリポジトリを構成する。リポジトリには LDAP を使用する。
7	内向き用申請受付けサーバ	JPNIC 業務担当者による申請を受付けるサーバ。Web ブラウザによりアクセス可能であり、申請者「契約管理者/資源管理者」「JPNIC 業務担当者」向けの証明書を発行する。	Web エンロール CGI プログラムがあり、CA サーバに対してリモートで証明書の発行を要求できる。これをベースに申請受け付け用 CGI プログラムの開発を行なう。
8	外向き用申請受付けサーバ	「契約管理者/資源管理者」は WEB ブラウザにてアクセスし、認証コードの発行を行なう。認証コードをメンテナー申請者に渡し、メンテナー申請者は自身で証明書の発行を要求する。	ユーザ情報を入力し、認証コードを発行する CGI プログラムを開発する。また、WEB エンロール CGI プログラムを修正し、認証コードでユーザ認証後に LDAP からユーザ情報を取得し証明書を発行する CGI プログラムの作成を行なう。
9	全ての認証局	全ての認証局はソフトウェア的に分離している必要がある。	1 つのサーバに複数の CA を構成することができ、それぞれの CA はソフトウェア的に分離している。
10	全ての認証局	それぞれが独立して秘密鍵を管理する必要がある。	1 つのサーバに複数の CA を構成することができ、それぞれの CA の秘密鍵は独立して管理される。
11	ハードウェア	「IP アドレス認証局（証明）」は「IP アドレス認証局（認証）」と、ハードウェア的に独立している。	項番 1「運用向け CA 構成」と項番 2「実証実験向け CA 構成」の通り、これらの CA はハードウェア的に分離して運用される。

12	リポジトリ	「JPNIC ルート認証局」「IP アドレス認証局(認証)」「IP アドレス認証局(証明)」「実証実験向け LIR 認証局」はそれぞれ異なるリポジトリが必要。	項番 5「運用向けリポジトリ」と項番 6「実証実験向けリポジトリ」の通り、2 台のハードウェアにて構成し、CA のサブジェクトにより異なるエントリ以下に独立したリポジトリを構成する。
13	IP アドレス認証局(証明)	「IP アドレス認証局（証明)」は、プロファイルの柔軟な変更、証明書とプロファイルデータの分析・保管、他認証局との相互認証の機能が必要。	柔軟なプロファイル管理機能を有しており、証明書と共にこれを保管・分析することが可能である。また、相互認証の機能も持っており、Cross CertificatePair ファイルの出力も可能である。
14	ユーザ利用端末	ユーザが利用する端末は開発対象ではない。	開発は行なわない。

（2） 運用上の役割の実現

15	JPNIC 登録局と発行局	外向き／内向き申請受付けサーバからの申請を受付け、証明書の発行、失効、CRL の発行が必要。	リモートからの証明書発行要求を受付け、アクセス制限の元で即時に証明書の発行が可能である。また定期的な CRL の発行が可能である。
16	JPNIC 登録局と発行局	証明書の管理業務を行なう GUI が必要。それらとは独立した運用担当者のユーザインタフェースが必要。	業務担当者は項番 7 の通り Web 画面を通じて証明書の管理が行なえる。これとは独立して、CA 運用の GUI が用意される。
17	リポジトリ	管理に必要なデータを格納する。IP レジストリシステムからの参照要求を受付け、返答を行なう。LDAP と HTTP（参照のみ）を用いる。	リポジトリには LDAP を使用しユーザ管理情報を保管する。アクセス時には認証を行ない、適切なアクセス制御を施す。
18	リポジトリ	内向き申請受付けサーバ、外向き申請受付けサーバ等の他のサーバとはハードウェア的に独立している必要有り。	項番５、項番６の通り、独立したハードウェアにて運用する。

（3） IP レジストリシステムとの連携

項番７、項番８に従い、IP レジストリシステムとの連携を行う為の開発を行なう。また IP レジストリシステムの開発プロジェクトと並行して開発を行う為、依存度に関しては疎な関係を保つよう留意する。従って二つのシステム間での登録データの矛盾を防ぎまたは解消する機構を持つ。

（4） IP アドレス認証局（証明）および LIR 認証局

19	実証実験向け認証局機能	「IP アドレス認証局（証明）」「実証実験向け LIR 認証局」は、RFC3779 に準拠したフィールドを扱うことができ、プロファイルの変更を行える必要がある。	作成した DER バイナリを証明書拡張情報としてプロファイルに取り込むことが可能である。設定されたプロファイルをもとに証明書を発行できる。
20	実証実験向け認証局機能	「IP アドレス認証局（証明）」「実証実験向け LIR 認証局」は、RIR またはアジア太平洋地域の NIR 等との相互認証証明書の発行が可能でなければならない。	CrossCertificatePair ファイルの出力も可能である。

(5) セキュリティの機能

21	セキュリティ	不正な操作の防止／抑止を行なうために、運用における記録や作業者の操作内容を保管する機能が必要である。	CA サーバには、発行ログ、アクセスログ、エラーログを出力する機能がある。また、開発を行なう CGI モジュールにおいても、これらのログ出力機能を持たせる。
22	セキュリティ	「JPNIC ルート認証局」は、FIPS140-2 レベル 2 に準拠した HSM を使用する必要がある。	項番 1 にある通り、ルート認証局には HSM を使用する。
23	セキュリティ	契約管理者/資源管理者と JPNIC 業務管理/担当者はハードウェアトークン（IC カード、USB トークン等）を使用する必要がある。秘密鍵を取り出すのが困難である。	ハードウェアトークンを使用して各 Web サイトにアクセス、もしくは証明書の発行を行なう。

(6) 環境の変更

24	環境の変更	障害が起きた場合、ハードウェアが変更されることを前提として構成される必要がある。ただし、HSM についてはこの限りではない。	CA フォルダと証明書ストアのバックアップが行われていれば、このデータを新たなマシンにリストアし、自動起動設定を行なうことでシステムの復旧が可能である。

(7) シンプルな構成

25	シンプルな構成	要求システムは、シンプルなシステムを実現することが望まれる。	CA はシンプルかつ少ないリソースで動作が可能である。また、リポジトリと連携しシンプルな証明書発行管理のシステムを開発する。

(8) 拡張性

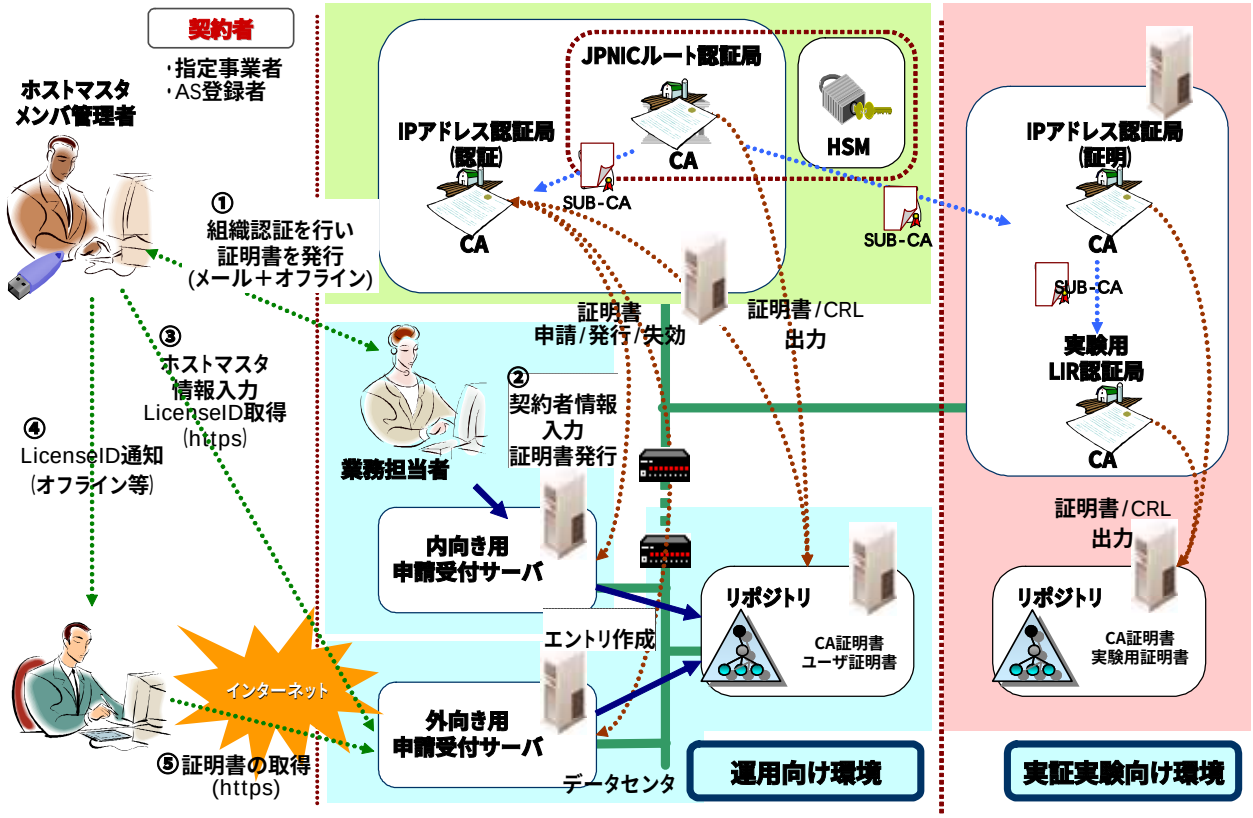
26	拡張性	収容した証明書の世代管理が可能であることが望まれる。複数の証明書プロファイルを切り替えることが望まれる。	1 つのサーバにて複数の CA を同時に運用可能である。CA の中で複数のプロファイルが管理でき、それぞれのプロファイルを適用して柔軟な証明書発行が可能である。
27	HSM の拡張利用	「IP アドレス認証局（認証）」「IP アドレス認証局（証明）」は、HSM を使うことが望まれる。各認証局は独立した秘密鍵の管理ができる。	「JPNIC ルート認証局」には HSM が接続されており、この HSM を「IP アドレス認証局（認証）」にて利用することができる。

(9) 運用管理の GUI

28	JPNIC 登録局と発行局	運用管理のユーザインタフェースには GUI もしくは Web インタフェースが望まれる。証明書管理、運用管理のユーザインタフェースおけるアクセス制御が望まれる。	管理ツールとして GUI のツールが利用可能である。パスワードによる認証や、リモートでは指定した権限によるアクセス制御が可能である。

5.2.2. システム構成

5.2.2.1. システム図



システム構成は、運用向け環境と実証実験向け環境に大別される。運用向け環境では主に 4 つの業務を処理する。（1）業務管理者による業務担当者の情報登録、証明書発行業務、（2）業務担当者による契約者（メンバ管理者）の情報登録、証明書発行業務、（3）メンバ管理者によるメンテナー申請者情報登録、証明書発行用認証 ID の払い出し業務、（4）メンテナー申請者による証明書の申請、発行業務の処理を行なう。これらの業務向けに Web インタフェースが提供され、(1)(2)は内向き用申請受付けサーバ)、（3）（4）は外向き用申請受付けサーバ上で動作する CGI によって処理される。

運用向け環境では、2 つの認証局が運用される。1 つは JPNIC ルート認証局で、下位の認証局に対して証明書を発行する。この認証局からは EE 証明書は発行しない。なお、秘密鍵を HSM に保管することで高い安全性を確保する。もう 1 つの認証局は IP アドレス認証局（認証）と呼ばれ、JPNIC ルート認証局の下位に位置している。この認証局から、JPNIC 業務管理者と JPNIC 業務担当者、契約者（メンバ管理者)、メンテナー

申請者向けの証明書の発行を行なう。これら 2 つの認証局は運用向け認証局サーバにより運営される。このうち、ルート認証局については常時稼動ではなく、必要なときに秘密鍵トークンを起動して動作させるような運用を想定する。

この他、運用環境向けにリポジトリが用意される。このリポジトリには契約者とメンテナー申請者の DN を持つエントリが作成され、証明書の保管が行われる。リポジトリは常時稼動しており、IP レジストリシステムからのアクセスも受付ける。

外向き申請受付けサーバは、インターネットからのアクセスを受付けるため、DMZ に配置され FW 経由で認証局サーバ、リポジトリ、IP レジストリシステムの RDB にアクセスする。

実証実験向け環境では 2 つの認証局が運用される。1 つは IP アドレス認証局（証明）で JPNIC ルート認証局の下位に位置している。この認証局の更に下位に実証実験向け LIR 認証局が存在し、RFC3779 に対応した拡張フィールドを持つ証明書を発行し、実証実験向けに使用する。

5.2.3. 認証局設計

5.2.3.1. JPNICルート認証局

（1） 方針

JPNIC ルート認証局は、下位の認証局に対してのみ証明書を発行するものとする。ルート認証局の鍵アルゴリズムは RSA 公開鍵暗号、鍵長は 2048bit とし、証明書の有効期限は 10 年とする。署名アルゴリズムは sha1WithRSAEncryption とする。CA の名称は「JPNIC ルート認証局」とする。

本来であれば ARL（Authority Revocation List）の発行が必要となるが、ルート認証局は通常非アクティブとして稼動させないため、ARL の発行は行なわないものとする。なお、ルート認証局の秘密鍵が漏洩、もしくは下位の認証局である IP アドレス認証局（認証）の秘密鍵が漏洩するようなインシデントが発生した場合、ルート認証局から CA の再構築を行なう。

（2） CA 証明書プロファイル設計

基本情報を以下に示す。

Field	ルート証明書
version	v3(2)
serialNumber	○
signature	
algorithm	sha1WithRSAEncryption
parameters	NULL
issuer	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	JPNIC Root Certification Authority
validity	20年
notBefore	発行時点
notAfter	指定可能
subject	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	JPNIC Root Certification Authority
subjectPublicKeyInfo	2048bit
algorithm	rsaEncryption
parameters	NULL
subjectPublicKey	○
signatureAlgorithm	
algorithm	sha1WithRSAEncryption
parameters	NULL
signatureValue	○

拡張情報を以下に示す。

Field	ルート証明書
AuthorityKeyIdentifier	non-critical
keyIdentifier	○
authorityCertIssuer	
authorityCertSerialNumber	
SubjectKeyIdentifier	non-critical
keyIdentifier	○
KeyUsage	non-critical
digitalSignature	
nonRepudiation	
keyEncipherment	
dataEncipherment	
keyAgreement	
keyCertSign	○
cRLSign	○
encipherOnly	
decipherOnly	
BasicConstraints	non-critical
cA	○
pathLenConstraint	

拡張情報には、AuthorityKeyIdentifier、SubjectKeyIdentifier、KeyUsage、BasicConstraints の 4 つを設定する。全て non-critical とし、CA 証明書に必要な情報を入力する。

(3)　EE 証明書プロファイル設計

EE 証明書は、IP アドレス認証局（認証）の CA 証明書となる。それぞれの項目を参照のこと。

5.2.3.2. IPアドレス認証局（認証）

（1） 方針

IP アドレス認証局（認証）は、JPNIC 業務管理者と JPNIC 業務担当者、契約者（メンバ管理者）、メンテナー申請者全てに証明書を発行する。CA 証明書の鍵アルゴリズムは RSA 公開鍵暗号、鍵長は 1024bit とし、証明書の有効期限は 10 年とする。署名アルゴリズムは sha1WithRSAEncryption とする。CA の名称は「JPNIC 資源管理認証局」、通称「メンテナー認証局」とする。

EE 証明書の鍵アルゴリズムは RSA 公開鍵暗号、鍵長は 1024bit とし、証明書の有効期限は 3 年とする。署名アルゴリズムは sha1WithRSAEncryption とする。登録担当者とメンバ管理者、メンテナー申請者の証明書について、「証明書プロファイル」という単位にグループ分けし管理する。

IP アドレス認証局（認証）は常時稼動し、CRL の発行も行なう。CRL は定期的に運用向けリポジトリに出力される。出力するリポジトリの DN は CA のサブジェクト DN と同じエントリとする。

（2） CA 証明書プロファイル設計

基本情報を以下に示す。

Field	CA証明書
version	v3(2)
serialNumber	○
signature	
algorithm	sha1WithRSAEncryption
parameters	NULL
issuer	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	JPNIC Root Certification Authority
validity	10年
notBefore	発行時点
notAfter	指定可能
subject	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	Internet Resource Service
organizationalUnitName	JPNIC Resource Service Certification Authority
subjectPublicKeyInfo	1024bit
algorithm	rsaEncryption
parameters	NULL
subjectPublicKey	○
signatureAlgorithm	
algorithm	sha1WithRSAEncryption
parameters	NULL
signatureValue	○

拡張情報を以下に示す。

Field	CA証明書
AuthorityKeyIdentifier	non-critical
keyIdentifier	○
authorityCertIssuer	
authorityCertSerialNumber	
SubjectKeyIdentifier	non-critical
keyIdentifier	○
KeyUsage	non-critical
digitalSignature	
nonRepudiation	
keyEncipherment	
dataEncipherment	
keyAgreement	
keyCertSign	○
cRLSign	○
BasicConstraints	non-critical
cA	○
pathLenConstraint	
certificatePolicies	non-critical
policyIdentifier	CP/CPSのOID
policyQualifiers	
policyQualifierID	CPSUri
qualifier	CP/CPSのURL
cRLDistributionPoint	non-critical
destributionPoint	
destributionPoint	CRLのURL

拡張情報には、AuthorityKeyIdentifier、SubjectKeyIdentifier、KeyUsage、BasicConstraints の 4 つを設定する。全て non-critical とし、CA 証明書に必要な情報を入力する。

(3)　EE 証明書プロファイル設計

JPNIC 業務管理者、業務担当者の基本情報は以下の通りである。

Field	EE証明書
version	v3(2)
serialNumber	○
signature	
algorithm	sha1WithRSAEncryption
parameters	NULL
issuer	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	Internet Resource Service
organizationalUnitName	JPNIC Resource Service Certification Authority
validity	2年
notBefore	発行時点
notAfter	指定可能

Field	EE証明書
subject	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	Internet Resource Service
organizationalUnitName	Secretariat
organizationalUnitName	Administrator
organizationalUnitName	<メンテナーコード>
commonName	JPNIC-AD <JPNIC従業員コード> <NAME>
subjectPublicKeyInfo	1024bit
algorithm	rsaEncryption
parameters	NULL
subjectPublicKey	○
signatureAlgorithm	
algorithm	sha1WithRSAEncryption
parameters	NULL
signatureValue	○

JPNIC 管理者は ou=Administrator、JPNIC 業務担当者は ou=Hostmaster となる。

契約管理者の基本情報は以下の通りである。なお、管理者メンテナーのサブジェクトの OU が Maintainer Administrator となり、契約者メンテナーは Corporate Administrator、メンテナー申請者は Hostmaster を入力する。

Field	EE証明書
version	v3(2)
serialNumber	○
signature	
algorithm	sha1WithRSAEncryption
parameters	NULL
issuer	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	Internet Resource Service
organizationalUnitName	JPNIC Resource Service Certification Authority
validity	2年
notBefore	発行時点
notAfter	指定可能
subject	
countryName	JP
organizationName	<組織名>
organizationName	LIR Corporate Administrator
organizationalUnitName	<メンテナーコード>
commonName	LIR-CO <認証ID> <NAME>
subjectPublicKeyInfo	1024bit
algorithm	rsaEncryption
parameters	NULL
subjectPublicKey	○
signatureAlgorithm	
algorithm	sha1WithRSAEncryption
parameters	NULL
signatureValue	○

拡張情報を以下に示す。

Field	EE証明書
AuthorityKeyIdentifier	non-critical
keyIdentifier	○
authorityCertIssuer	
authorityCertSerialNumber	
SubjectKeyIdentifier	non-critical
keyIdentifier	○
KeyUsage	non-critical
digitalSignature	○
nonRepudiation	
keyEncipherment	○
dataEncipherment	
keyAgreement	
keyCertSign	
cRLSign	
BasicConstraints	non-critical
cA	FALSE
pathLenConstraint	
certificatePolicies	non-critical
policyIdentifier	CP/CPSのOID
policyQualifiers	
policyQualifierID	CPSUri
qualifier	CP/CPSのURL
cRLDistributionPoint	non-critical
destributionPoint	
destributionPoint	CRLのURL
subjectAltName	non-critical
rfc822Name	○

（4） CRL プロファイル設計

CRL の基本情報は以下の通りである。

Field	CRL
version	v2(1)
signature	
algorithm	sha1WithRSAEncryption
parameters	NULL
issuer	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	Internet Resource Service
organizationalUnitName	JPNIC Resource Service Certification Authority
thisUpdate	○
nextUpdate	24時間後
revokedCertificates	
userCertificate	○

拡張情報を以下に示す。

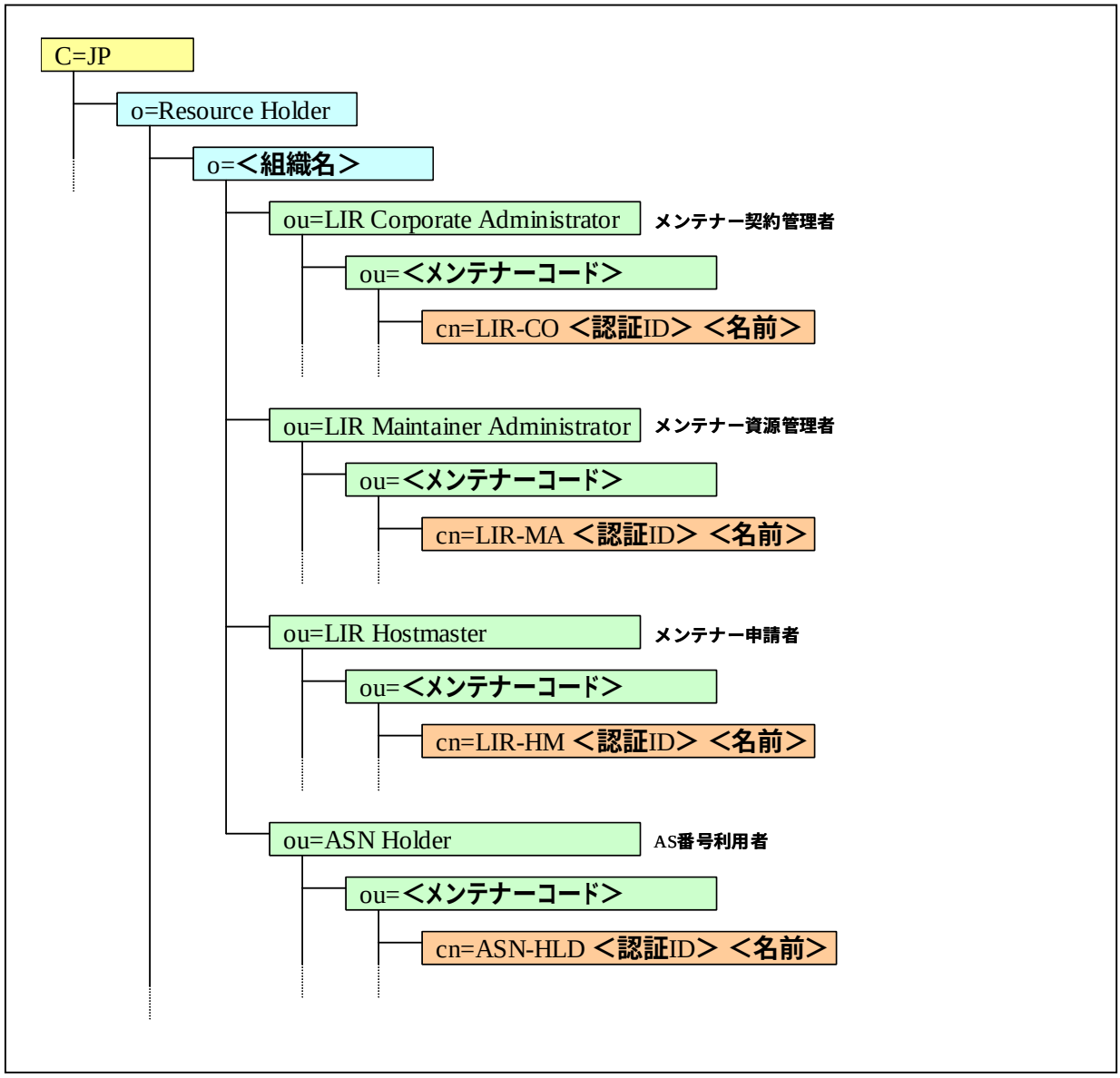
Field	CRL
authorityKeyIdentifier	
keyIdentifier	○
authorityCertIssuer	
authorityCertSerialNumber	
issuerAltName	
cRLNumber	○
deltaCRLIndicator	

5.2.4. リポジトリ設計

5.2.4.1. 指定事業者（組織）情報ツリー

（1） ツリー構成

指定事業者（組織）情報ツリーについては、下図のとおりである。



ツリーの頂点として“ o=Resource Holder,c=JP ”を作成し、この配下に様々なエントリを作成する。

指定事業者（組織）ごとに“ o=＜組織名＞,o=Resource Holder,c=JP ”を作成し、その直下には、“ ou=LIR Corporate Administrator ”、“ ou=LIR Maintainer Administrator ”、“ ou=LIR Hostmaster ”が作成される。

“ ou=LIR Corporate Administrator ”は、メンテナー契約管理者の格納場所である。

この配下に、メンテナーコード別に、証明書格納用エントリ“ cn=LIR-CO ＜認証 ID＞ ＜名前＞ ”を作成する。

“ ou=LIR Maintainer Administrator ”は、メンテナー資源管理者の格納場所である。

この配下に、メンテナーコード別に、証明書格納用エントリ“ cn=LIR-MA ＜認証 ID＞ ＜名前＞ ”を作成する。

“ ou=LIR Hostmaster ”は、メンテナー申請者の格納場所である。この配下に、メンテナーコード別に、証明書格納用エントリ“ cn=LIR-HM ＜認証 ID＞ ＜名前＞ ”を作成する。

“ ou=ASN Holder ”は、AS 番号利用者の格納場所である。この配下に、メンテナーコード別に、証明書格納用エントリ“ cn=ASN-HLD ＜認証 ID＞ ＜名前＞ ”を作成する。

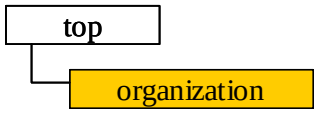
(2)　オブジェクトクラス

指定事業者（組織）情報ツリーで使用するオブジェクトクラスは、以下である。

「使用する属性」は、アプリケーションからの利用に基づいた定義である。そのため、ディレクトリ内における定義とは異なる場合がある。

■ コンテナ用オブジェクトクラス（1）

コンテナを作成するために、organization オブジェクトクラスを使用する。
organization オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成を持つ。



ツリー内における対象オブジェクトは、以下である。

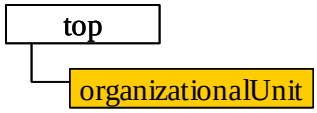
o=Resource Holder
o=**＜組織名＞**

使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名、組織名	o	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	organization

■ コンテナ用オブジェクトクラス（2）

コンテナを作成するために、organizationalUnit オブジェクトクラスを使用する。
organizationalUnit オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成を持つ。



ツリー内における対象オブジェクトは、以下である。

ou=LIR Corporate Administrator
ou=LIR Maintainer Administrator
ou=LIR Hostmaster
ou=ASN Holder
ou=**＜メンテナーコード＞**

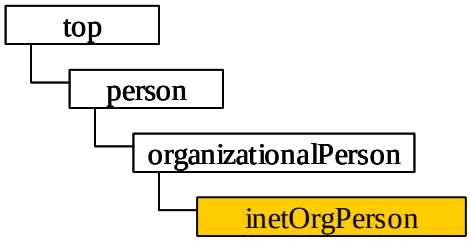
使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名、メンテナーコード	ou	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	organizationalUnit

■ **証明書格納用オブジェクトクラス**

証明書を格納するために、inetOrgPerson オブジェクトクラスを使用する。

inetOrgPerson オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成である。



ツリー内における対象オブジェクトは、以下である。

cn=LIR-CO **＜認証ID＞ ＜名前＞**
cn=LIR-MA **＜認証ID＞ ＜名前＞**
cn=LIR-HM **＜認証ID＞ ＜名前＞**
cn=ASN-HLD **＜認証ID＞ ＜名前＞**

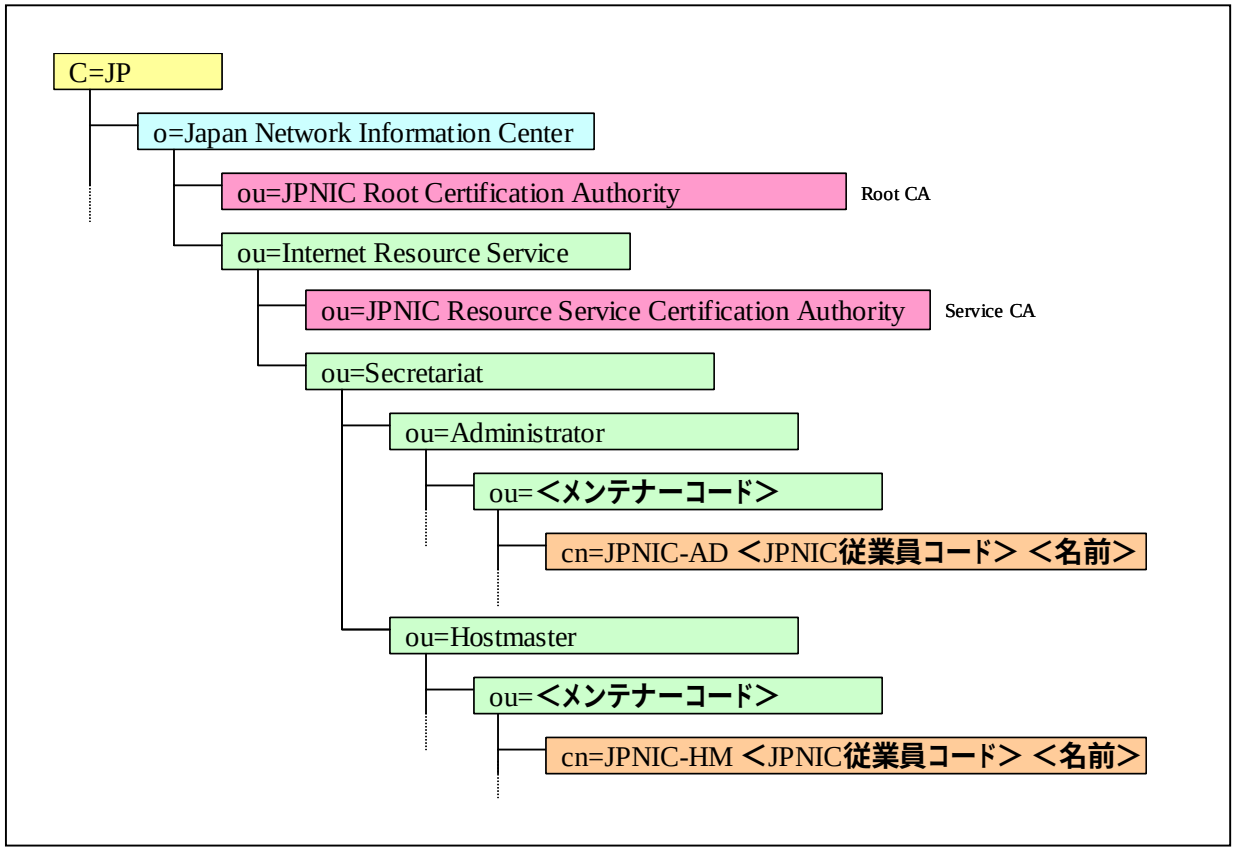
使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名	cn	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	inetOrgPerson
3	名前	sn	○	－	cn と同値
4	ライセンス ID	uid	－	－	
5	電子メールアドレス	mail	○	－	
6	オンラインフラグ	o	○	－	“online”,“offline” 文字列
7	証明書	userSMIMECertificate	－	－	binary、カレントの証明書
8	証明書＜履歴＞	userCertificate	－	○	binary、証明書の履歴

JPNIC CA 情報ツリー

ツリー構成

JPNIC CA 情報ツリーについては、下図のとおりである。



ツリーの頂点として“ o=Japan Network Information Center,c=JP ”を作成し、この配下に様々なエントリを作成する。

“ o=Japan Network Information Center,c=JP ”の直下に、“ ou=JPNIC Root Certification Authority ”、“ ou=Internet Resource Service ”を作成する。

“ ou=JPNIC Root Certification Authority ”は、JPNIC ルート認証局である。

“ ou=Internet Resource Service ”は、IP アドレス認証局に関する情報の格納場所である。この直下に、“ ou=JPNIC Resource Service Certification Authority ”、“ ou=Secretariat ”を作成する。

“ ou=JPNIC Resource Service Certification Authority ”は、IP アドレス認証局である。

“ ou=Secretariat ”は、証明書格納用エントリの格納場所である。

この直下に、“ ou=Administrator ”、“ ou=Hostmaster ”を作成する。

“ ou=Administrator ”は、契約者の格納場所である。この配下に、メンテナーコード別に証明書格納用エントリ“ cn=JPNIC-AD ＜JPNIC 従業員コード＞ ＜名前＞ ”を作成する。

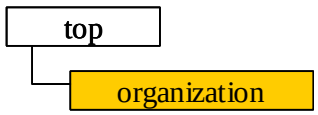
“ ou=Hostmaster ”は、メンテナー申請者の格納場所である。この配下に、メンテナーコード別に、証明書格納用エントリ“ cn=JPNIC-HM ＜JPNIC 従業員コード＞ ＜名前＞ ”を作成する。

オブジェクトクラス
JPNIC CA 情報ツリーで使用するオブジェクトクラスは、以下である。

「使用する属性」は、アプリケーションからの利用に基づいた定義である。そのため、ディレクトリ内における定義とは異なる場合がある。

■ コンテナ用オブジェクトクラス（1）

コンテナを作成するために、organization オブジェクトクラスを使用する。
organization オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成である。



ツリー内における対象オブジェクトは、以下である。

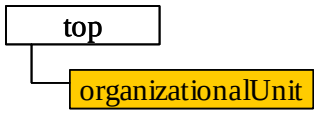
o=Japan Network Information Center

使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名、組織名	o	○	―	RDN 属性
2	オブジェクトクラス	objectClass	○	―	organization

■ コンテナ用オブジェクトクラス（2）

コンテナを作成するために、organizationalUnit オブジェクトクラスを使用する。
organizationalUnit オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成である。



ツリー内における対象オブジェクトは、以下である。

ou=Internet Resource Service
ou=Secretariat
ou=**＜メンテナーコード＞**
ou=Administrator
ou=Hostmaster

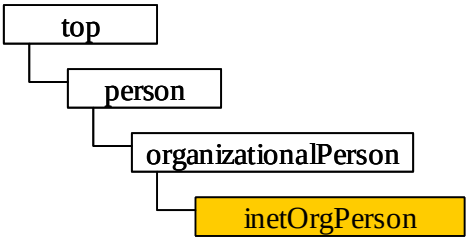
使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名、メンテナーコード	ou	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	organizationalUnit

■ 証明書格納用オブジェクトクラス

証明書を格納するために、inetOrgPerson オブジェクトクラスを使用する。

inetOrgPerson オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成である。



ツリー内における対象オブジェクトは、以下である。

cn=JPNIC-AD ＜JPNIC**従業員コード**＞ ＜**名前**＞

cn=JPNIC-HM ＜JPNIC**従業員コード**＞ ＜**名前**＞

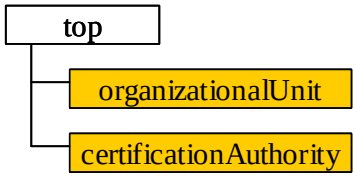
使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名	cn	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	inetOrgPerson
3	名前	sn	○	－	cn と同値
4	ライセンス ID	uid	－	－	
5	電子メールアドレス	mail	○	－	
6	オンラインフラグ	o	○	－	“ online ”,“ offline ”,“ ”(値無し)
7	証明書	userSMIMECertificate	－	－	binary、カレントの証明書
8	証明書＜履歴＞	userCertificate	－	○	binary、証明書の履歴

■ CA 用オブジェクトクラス

CA を作成するために、ornaginzationalUnit オブジェクトクラス、certificationAuthority オブジェクトクラスを使用する。

organizationalUnit オブジェクトクラスは構造型オブジェクトクラス、certificationAuthority オブジェクトクラスは補助型オブジェクトであり、以下の構成である。



ツリー内における対象オブジェクトは、以下である。

ou=JPNIC Root Certification Authority

ou=JPNIC Resource Service Certification Authority

使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名、CA	ou	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	organizationalUnit
3	補助クラス	objectClass	○	－	certificationAuthority
4	CA 証明書	cACertificate	○	－	binary
5	ARL	authorityRevocationList	○	－	binary
6	CRL	certificateRevocationList	○	－	binary

5.2.5. 業務設計

業務設計では、すべての業務関係者の業務フローを作成した。その上で必要な機能の洗い出し、やりとりが発生する情報の洗い出し等を行った。

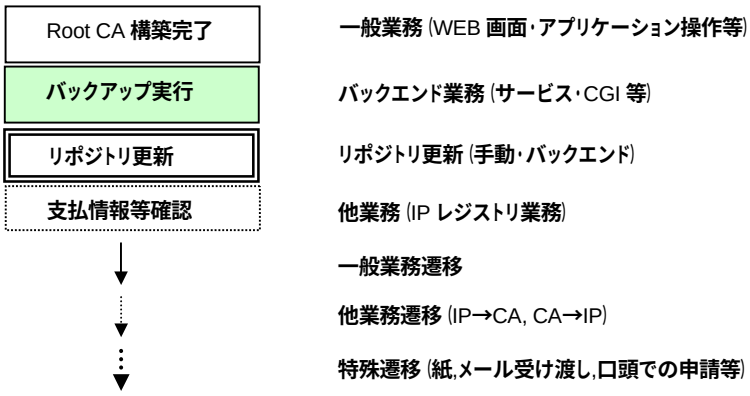
5.2.5.1. 業務フロー一覧

	業務内容	JPNIC CA 運用担当者	JPNIC RootCA 管理者	JPNIC IP アドレス CA 管理者	JPNIC 業務管理者	JPNIC 業務担当者	契約管理者	資源管理者	一般申請者
1	JPNIC ルート認証局構築業務	○	○						
2	JPNIC ルート認証局失効業務	○	○						
3	JPNIC ルート認証局鍵更新業務	○	○						
4	JPNIC ルート認証局 CRL 発行業務	○	○						
5	JPNIC ルート認証局バックアップ業務	○							
6	IP アドレス認証局(認証)構築業務	○	○	○					
7	IP アドレス認証局(認証)失効業務	○	○	○					
8	IP アドレス認証局(認証)鍵更新業務	○	○	○					
9	IP アドレス認証局(認証) CRL 発行業務	○		○					
10	IP アドレス認証局(認証)バックアップ業務	○							
11	JPNIC 業務			○	○				

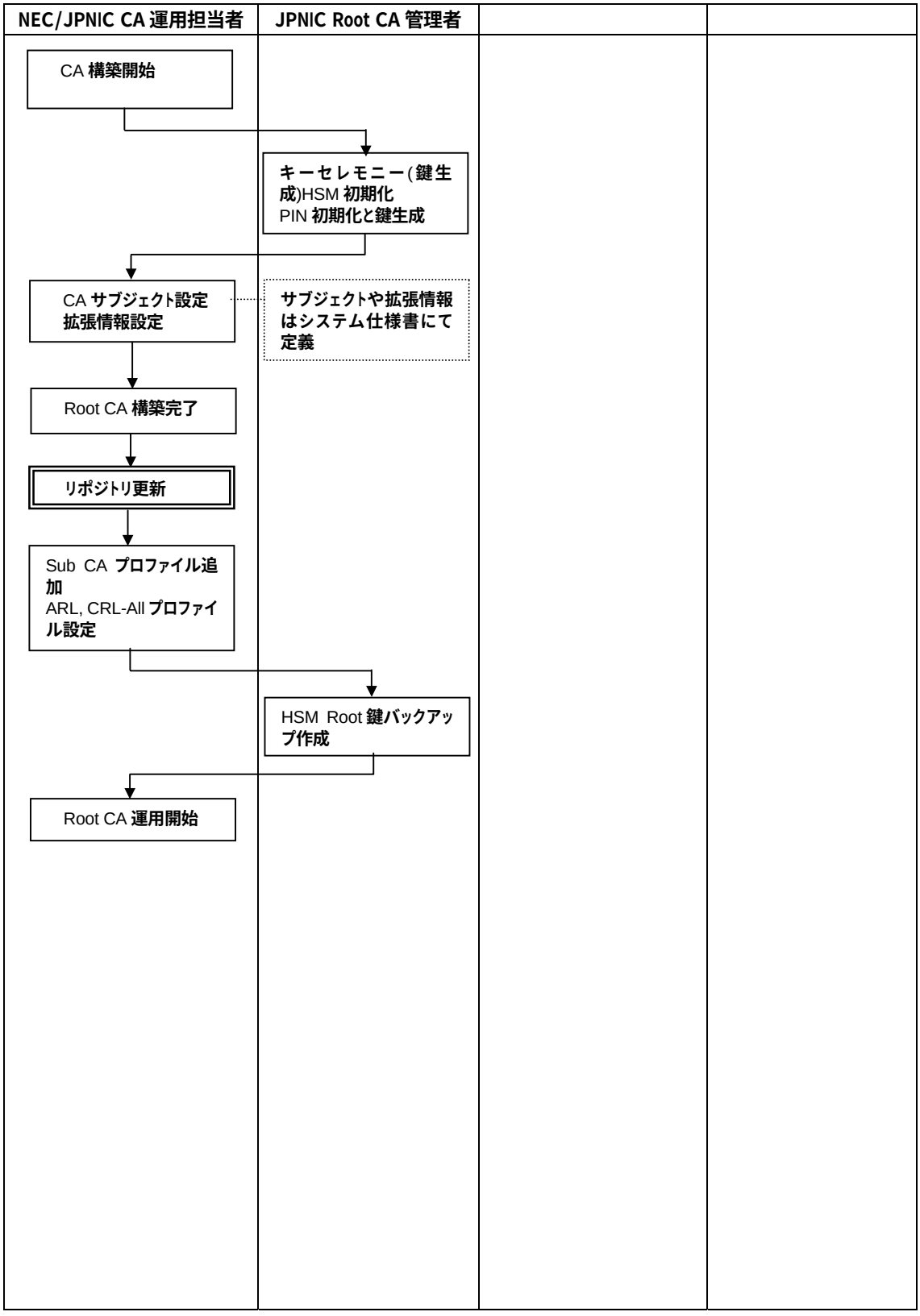
	管理者証明書 発行業務								
12	JPNIC 業務 管理者証明書 失効業務			○	○				
13	JPNIC 業務 管理者証明書 更新業務			○	○				
14	JPNIC 業務 担当者証明書 発行業務			○	○	○			
15	JPNIC 業務 担当者証明書 失効業務			○	○	○			
16	JPNIC 業務 担当者証明書 更新業務			○	○	○			
17	メンテナー契約 管理者証明書 発行業務			○	○	○	○		
18	メンテナー資源 管理者証明書 発行業務			○	○	○		○	
19	メンテナー契約 管理者証明書 失効業務				○	○	○		
20	メンテナー資源 管理者証明書 失効業務				○	○		○	
21	メンテナー契約 管理者証明書 更新業務			○	○	○	○		
22	メンテナー資源 管理者証明書 更新業務			○	○	○		○	
23	メンテナー 申請者証明書 発行業務						○	○	○

24	メンテナー 申請者証明書 失効業務						○	○	○
25	メンテナー 申請者証明書 更新業務						○	○	○
26	指定事業者 サーバ証明書 発行業務			○		○	○		
27	指定事業者 サーバ証明書 失効業務			○		○	○		
28	指定事業者 サーバ証明書 更新業務			○		○	○		

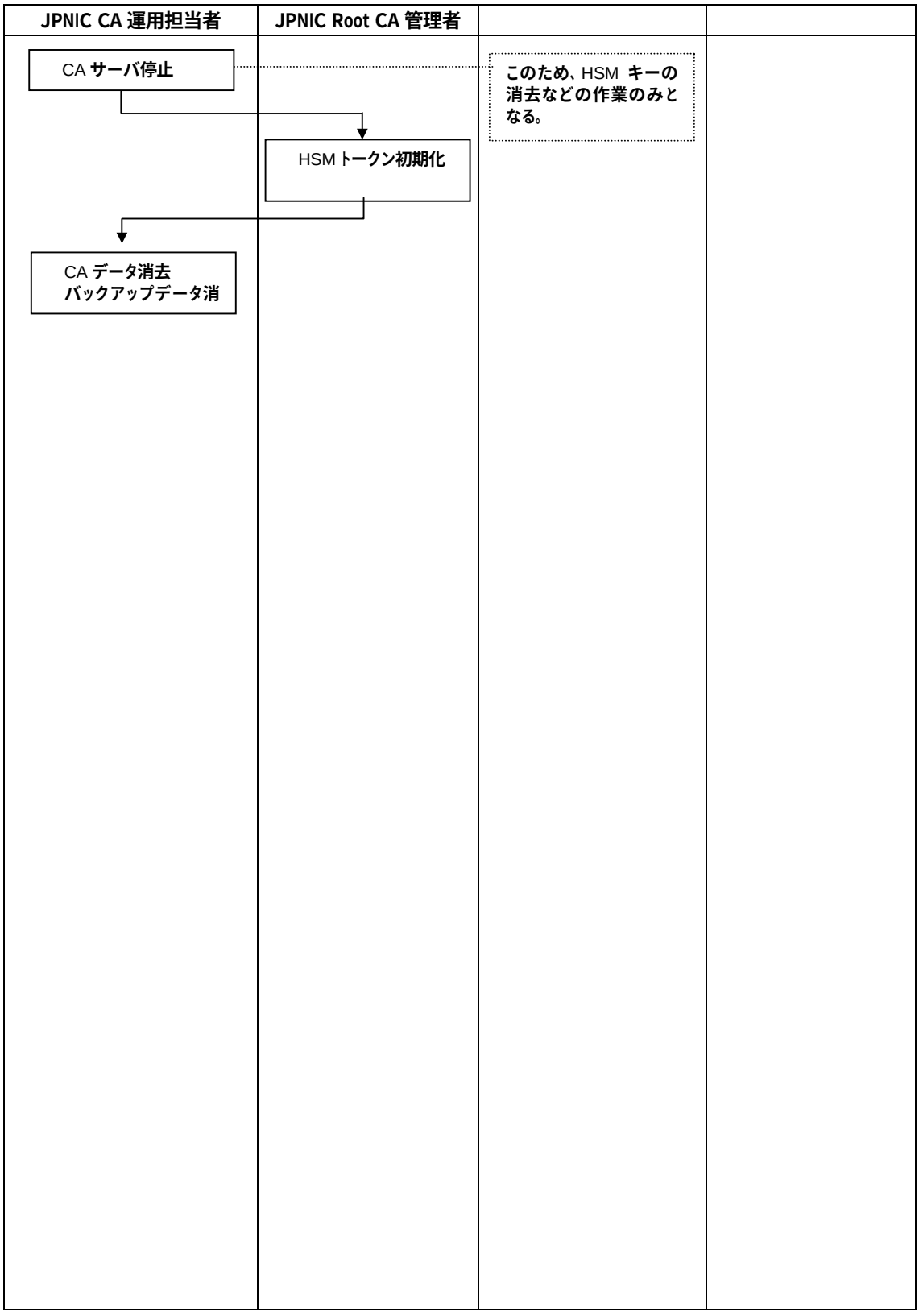
凡例



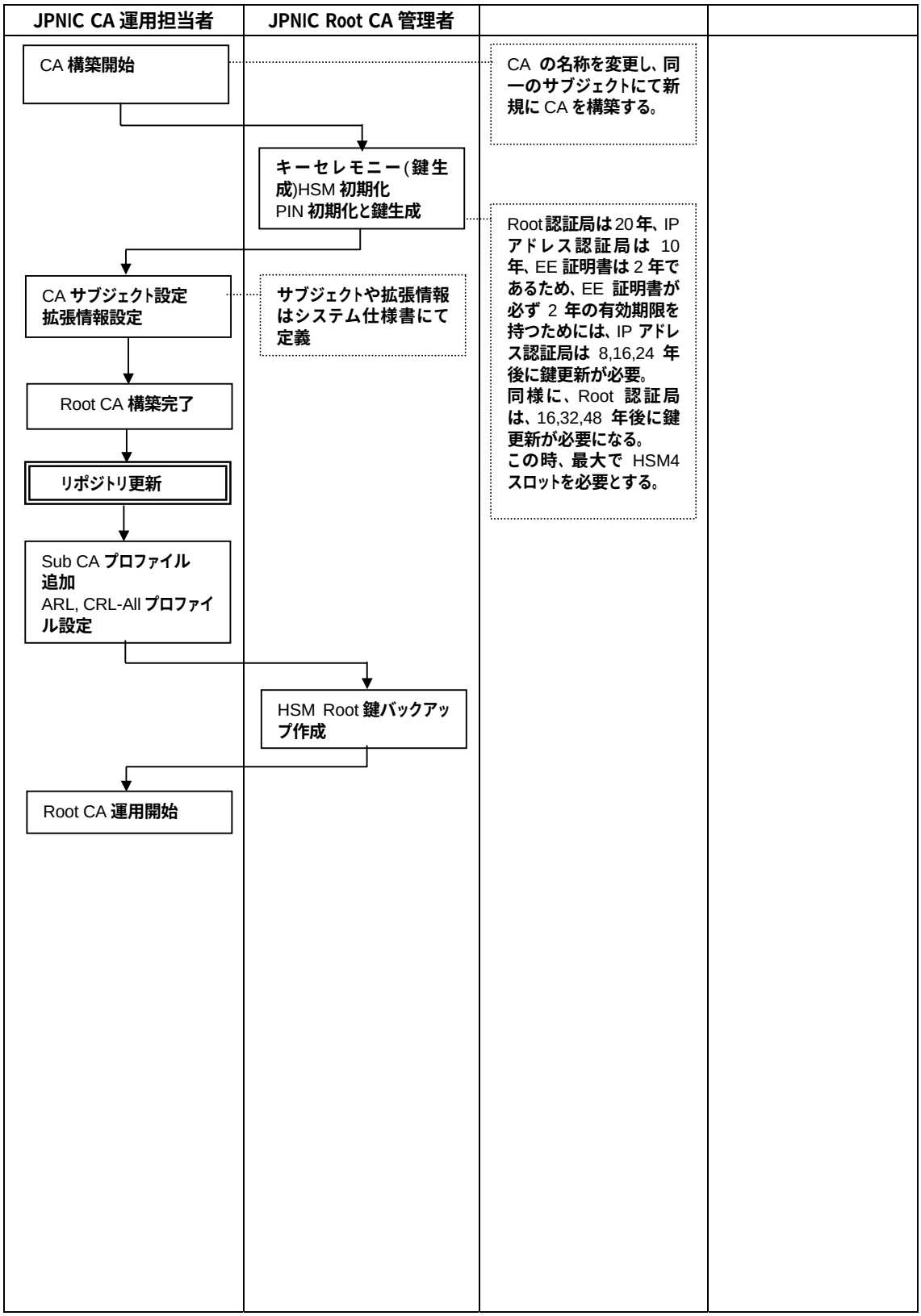
5.2.5.2. JPNICルート認証局構築業務



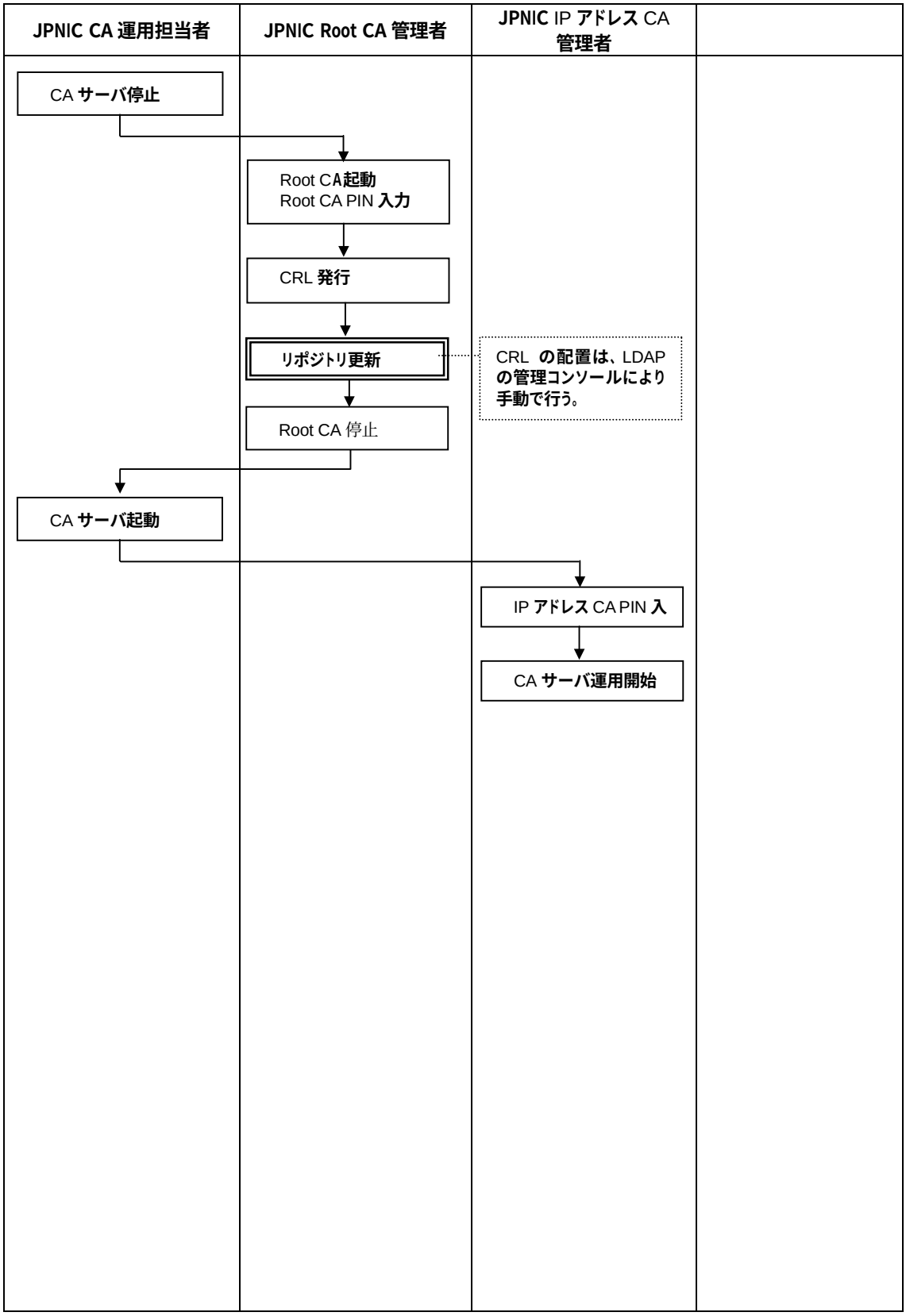
5.2.5.3. JPNICルート認証局失効業務



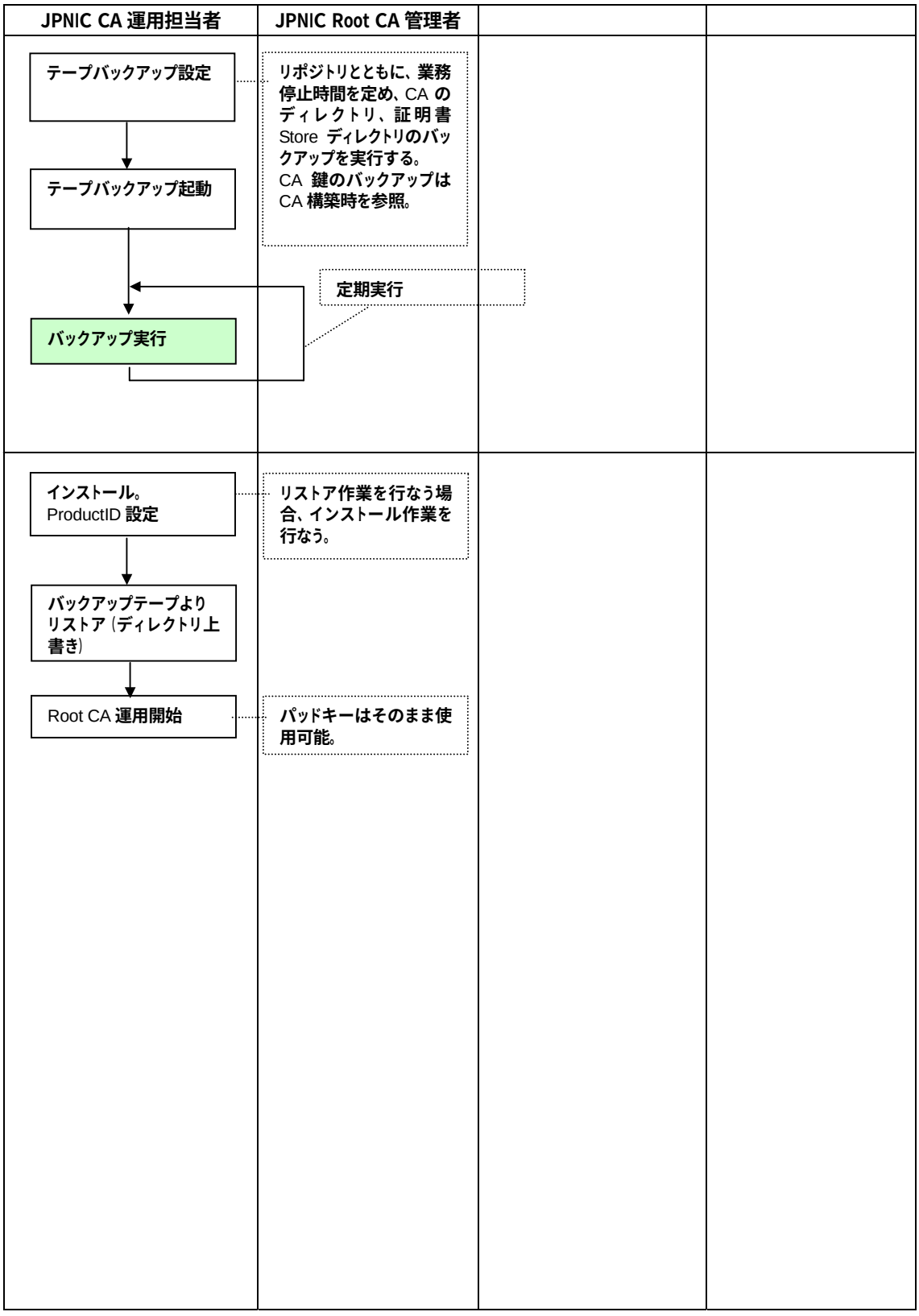
5.2.5.4. JPNICルート認証局鍵更新業務



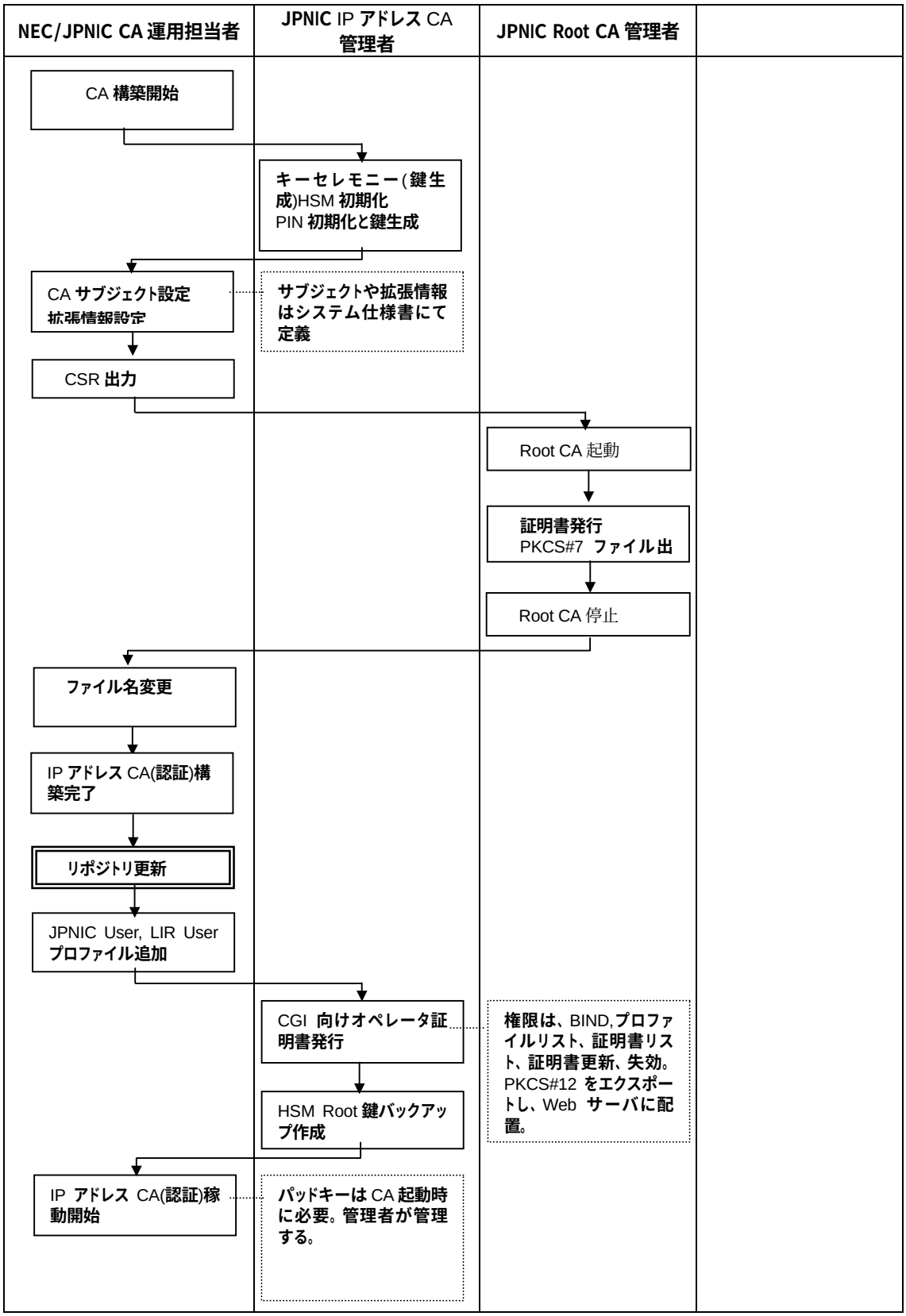
5.2.5.5. JPNICルート認証局CRL発行業務



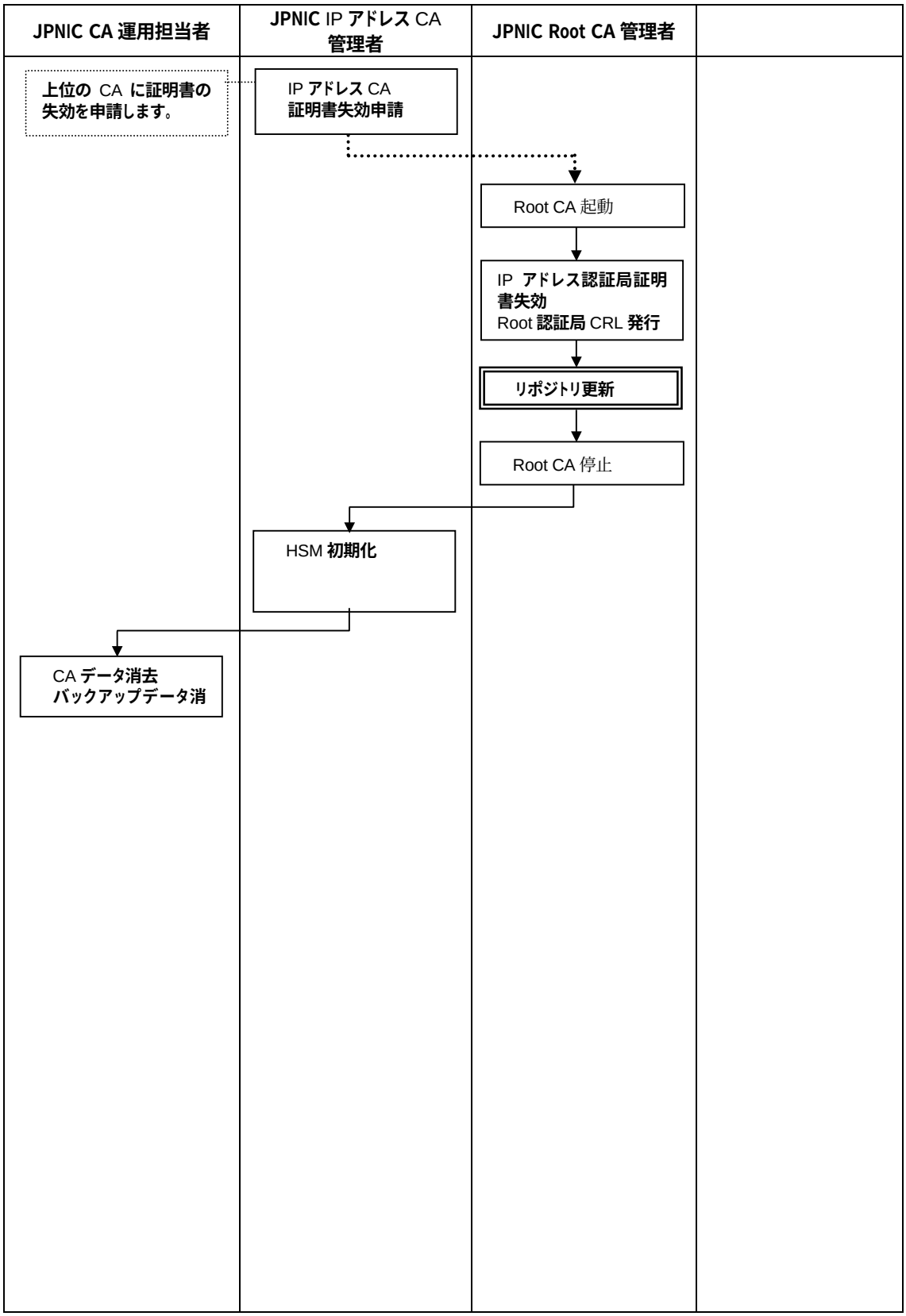
5.2.5.6. JPNICルート認証局バックアップ業務



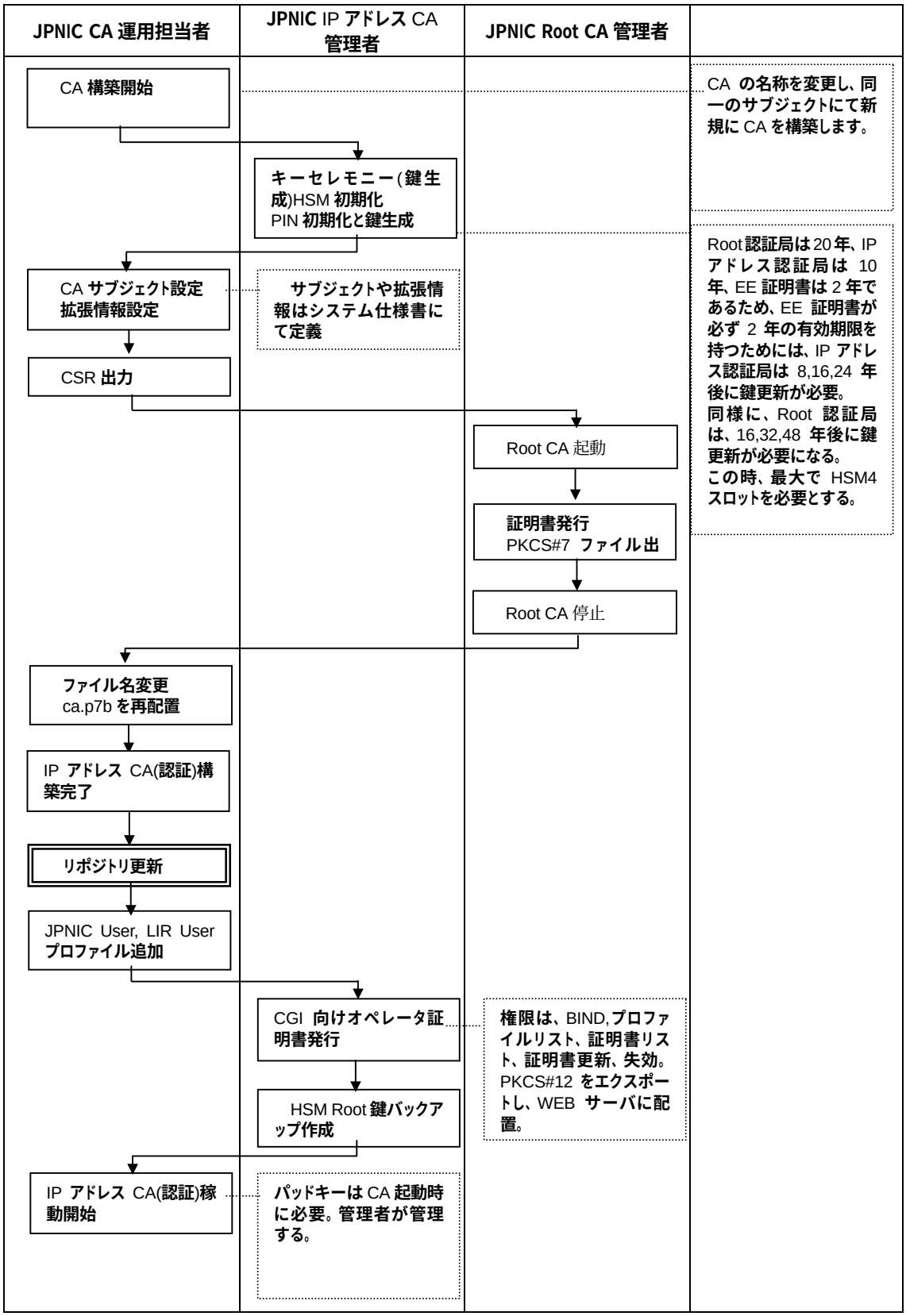
5.2.5.7. IPアドレス認証局(認証)構築業務



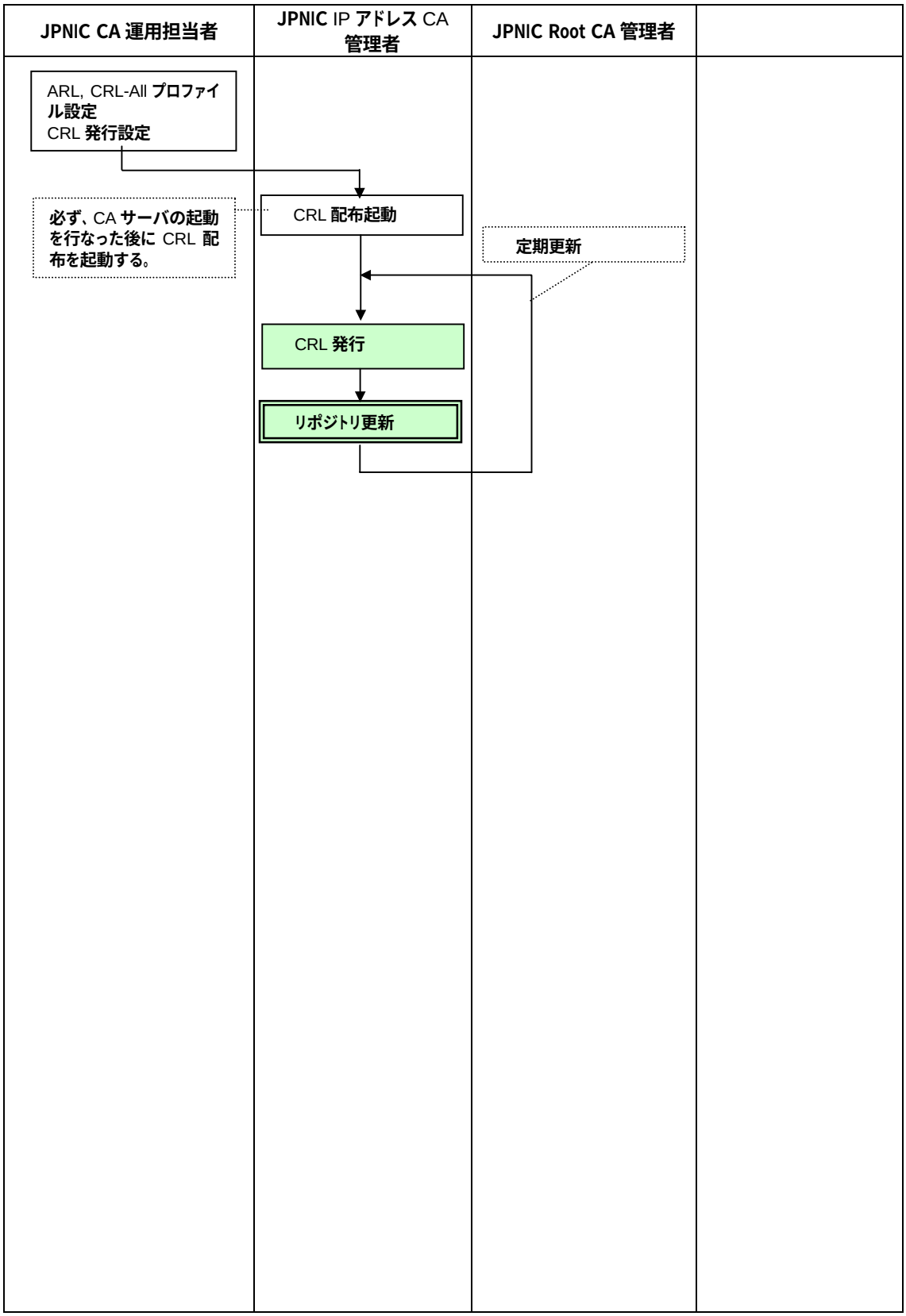
5.2.5.8. IPアドレス認証局(認証)失効業務



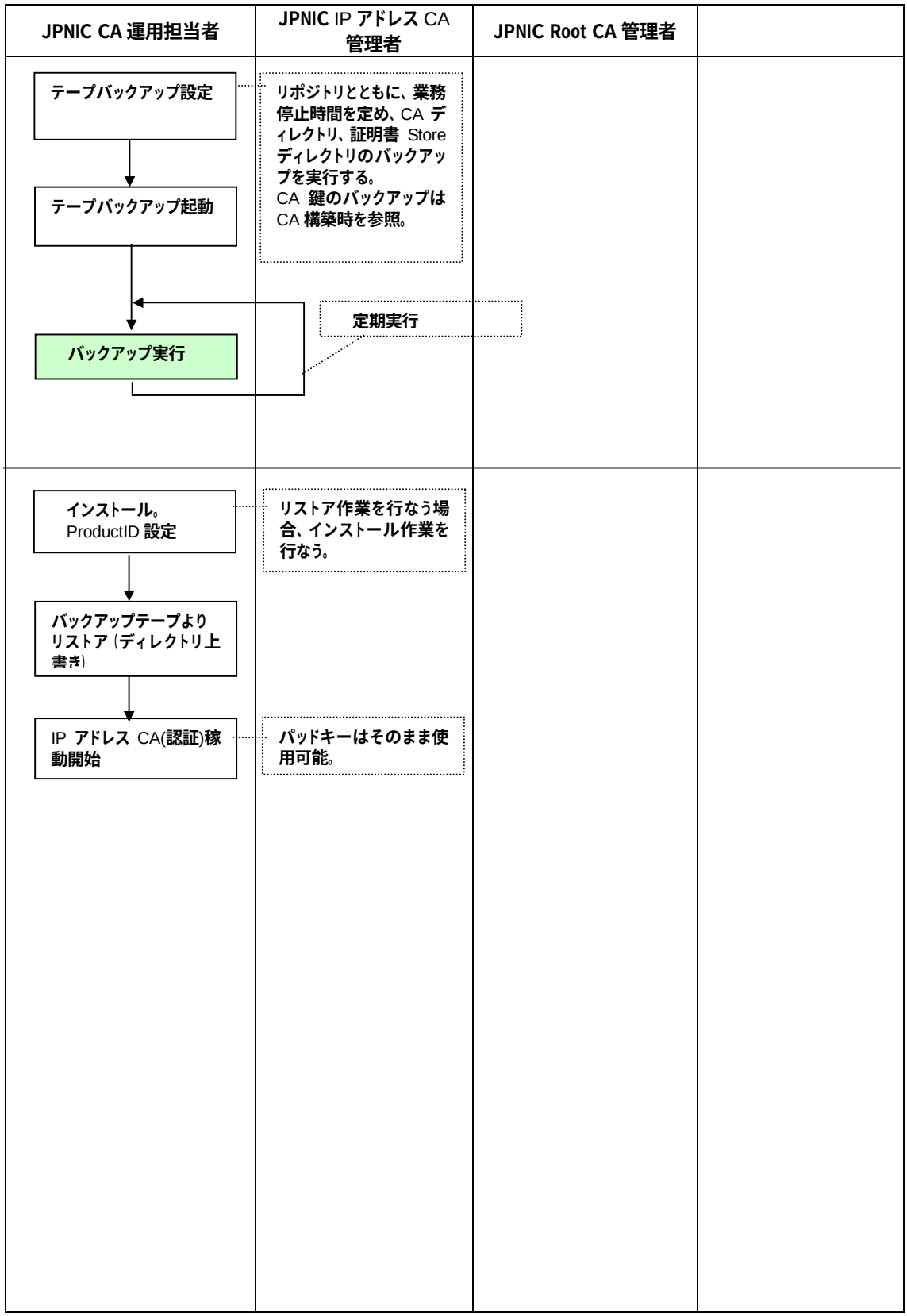
5.2.5.9. IPアドレス認証局(認証)更新業務



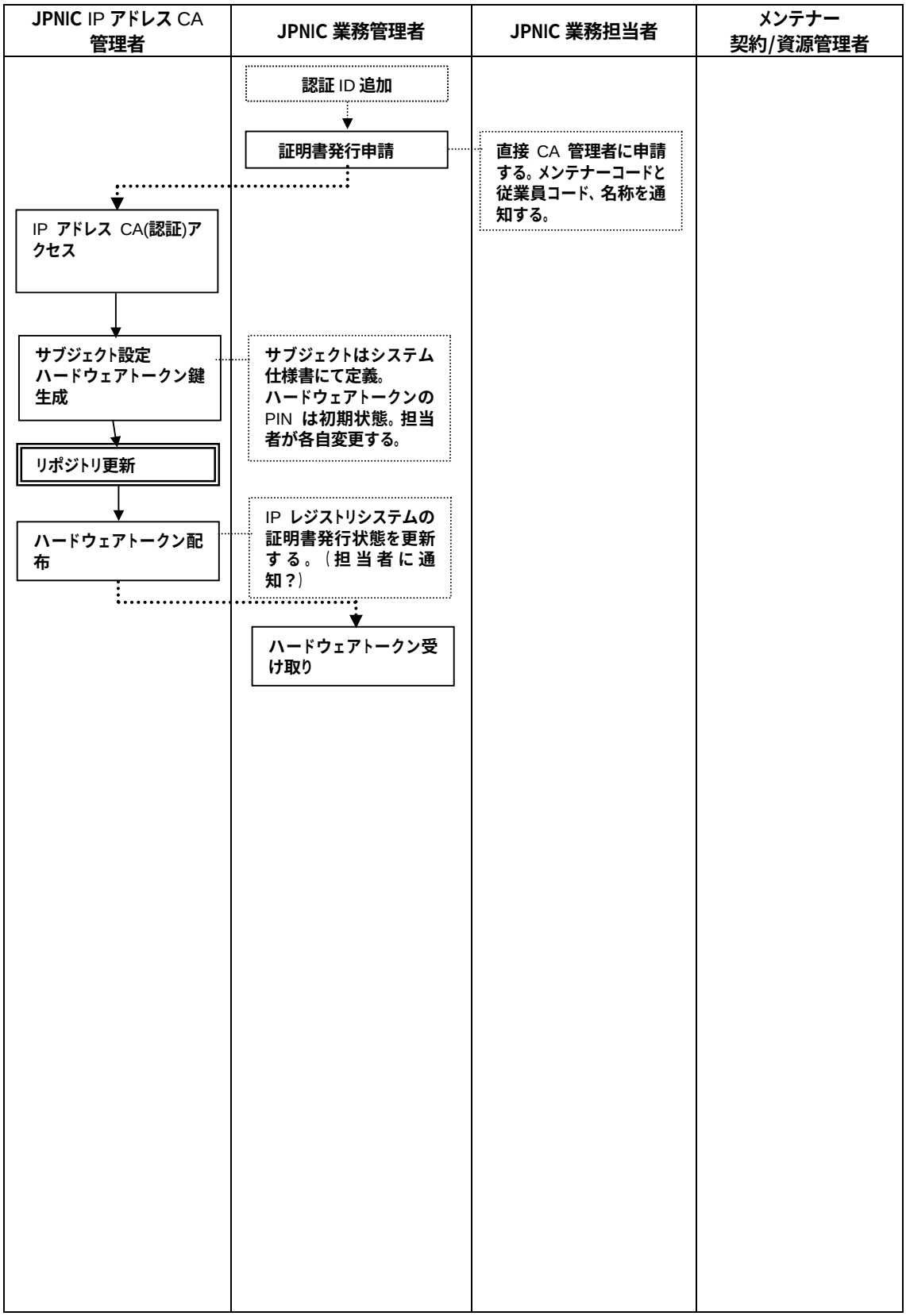
5.2.5.10. IPアドレス認証局(認証)CRL発行業務



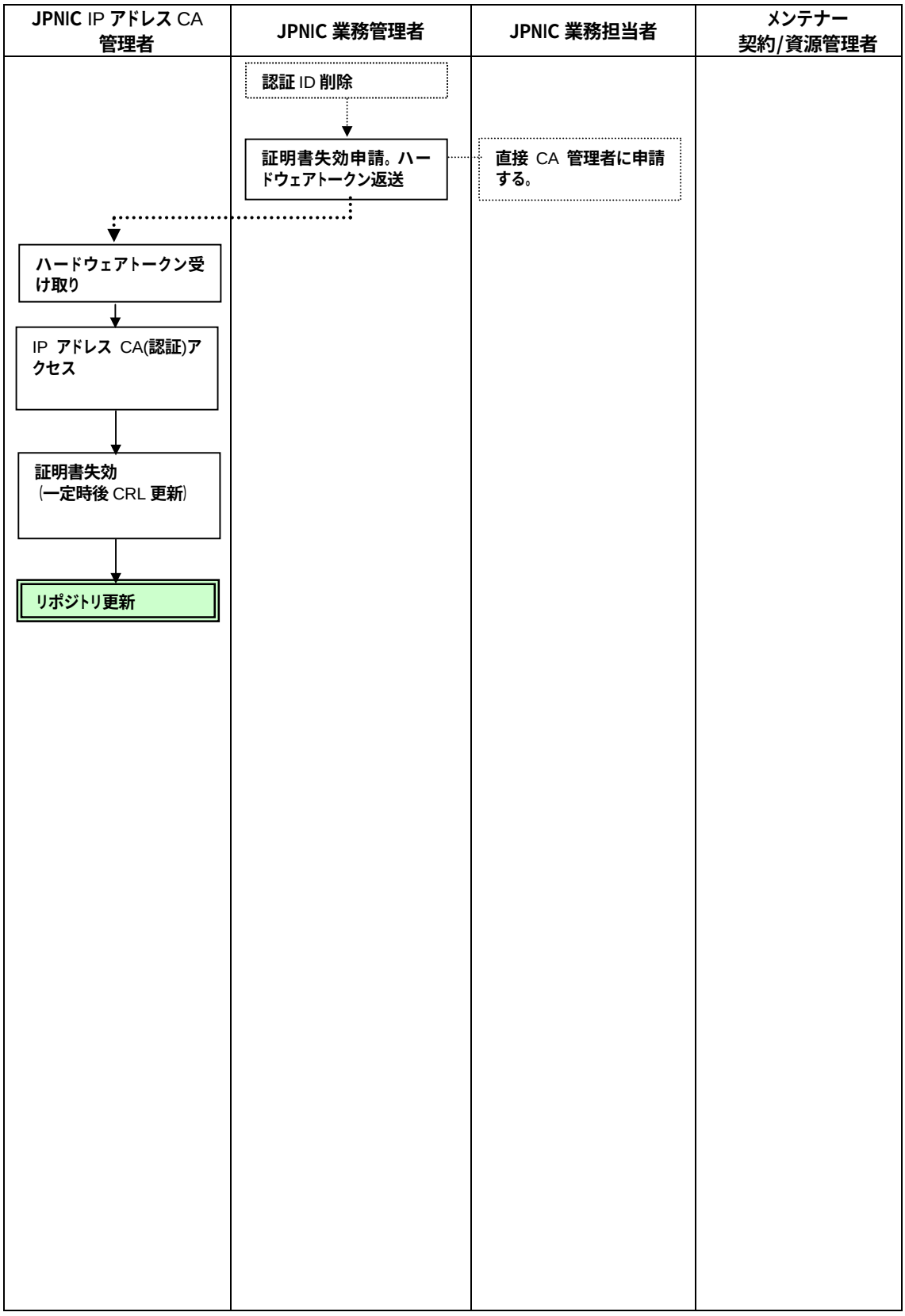
5.2.5.11. IPアドレス認証局(認証)バックアップ業務



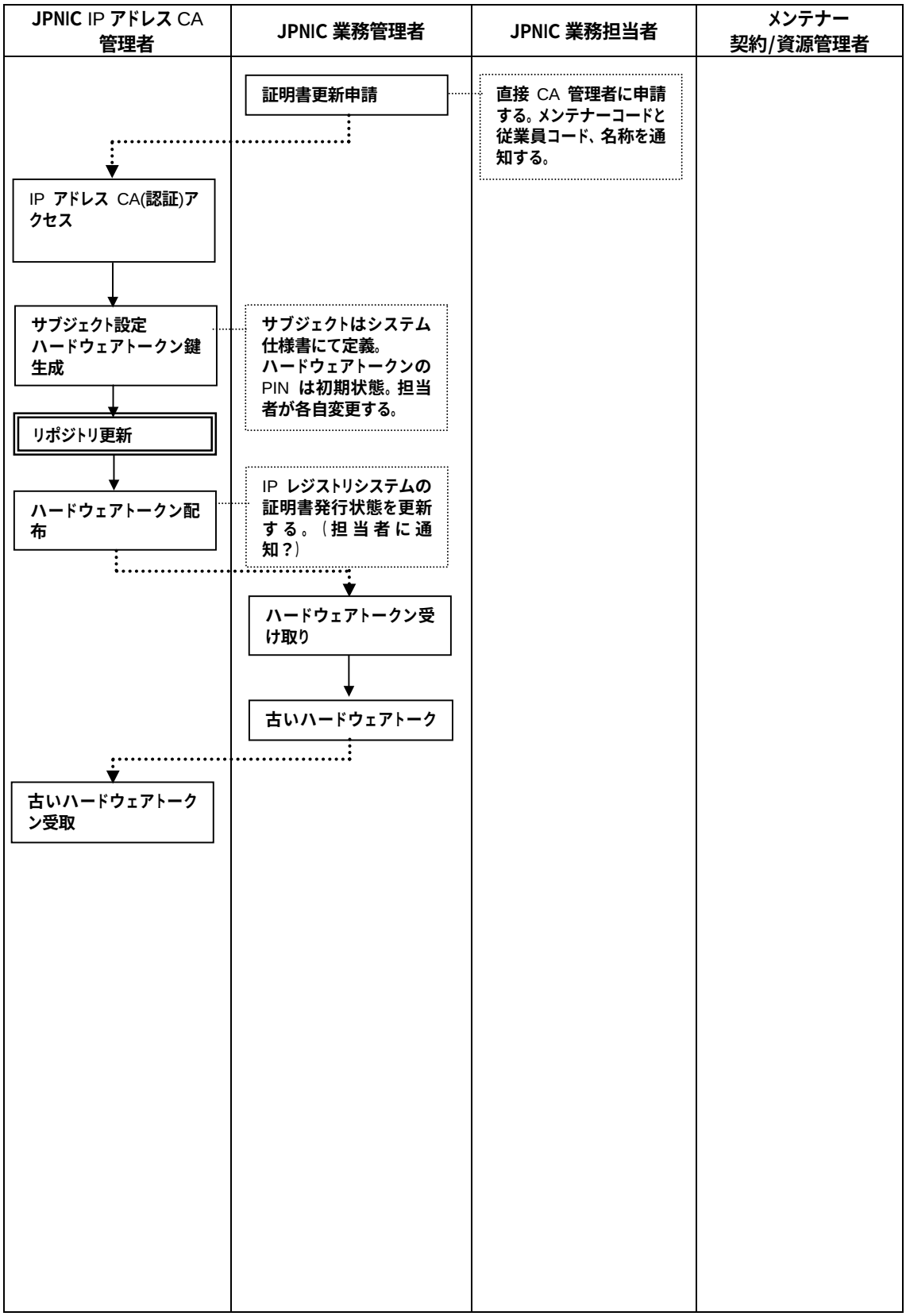
5.2.5.12. JPNIC業務管理者証明書発行業務



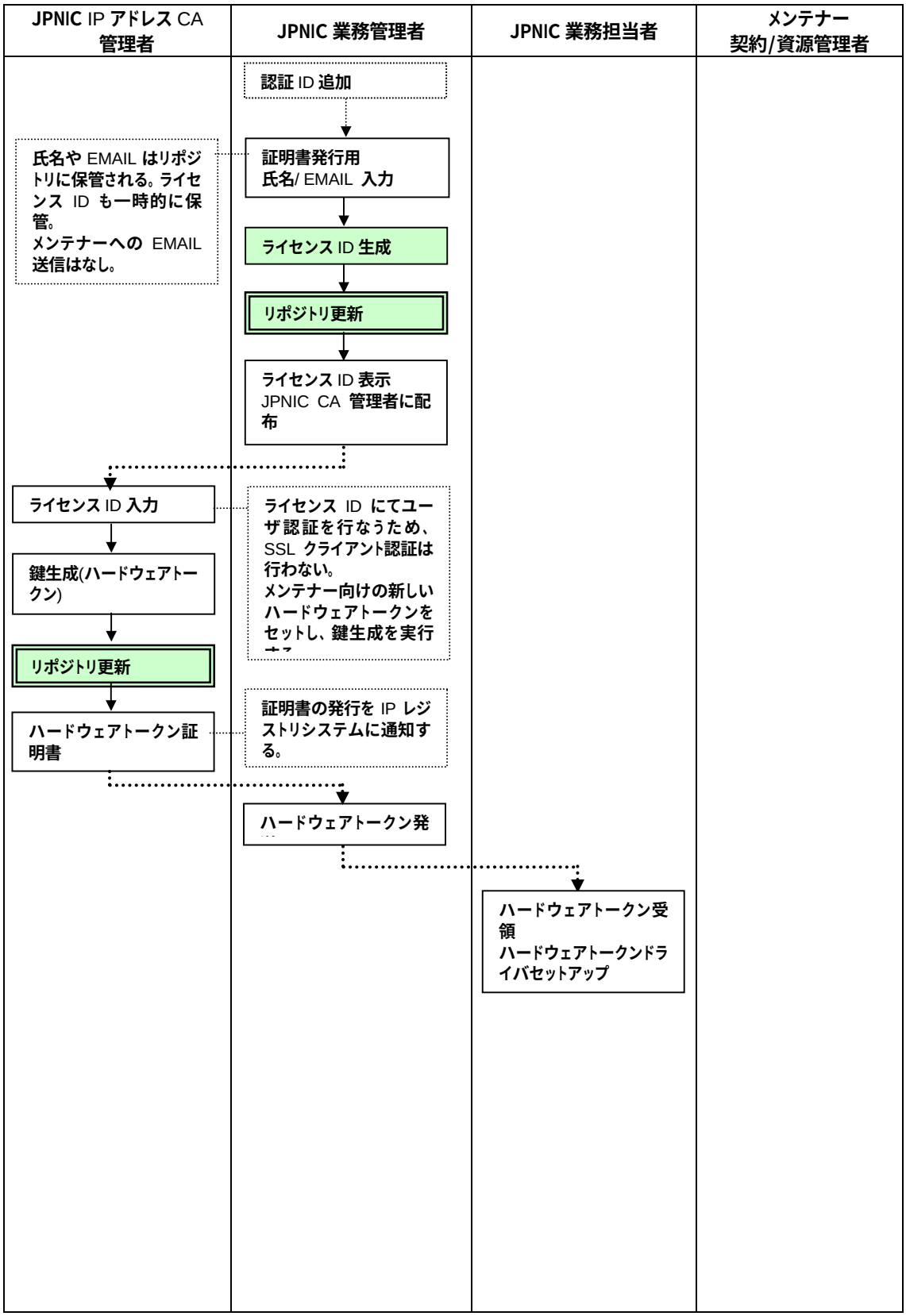
5.2.5.13. JPNIC業務管理者証明書失効業務



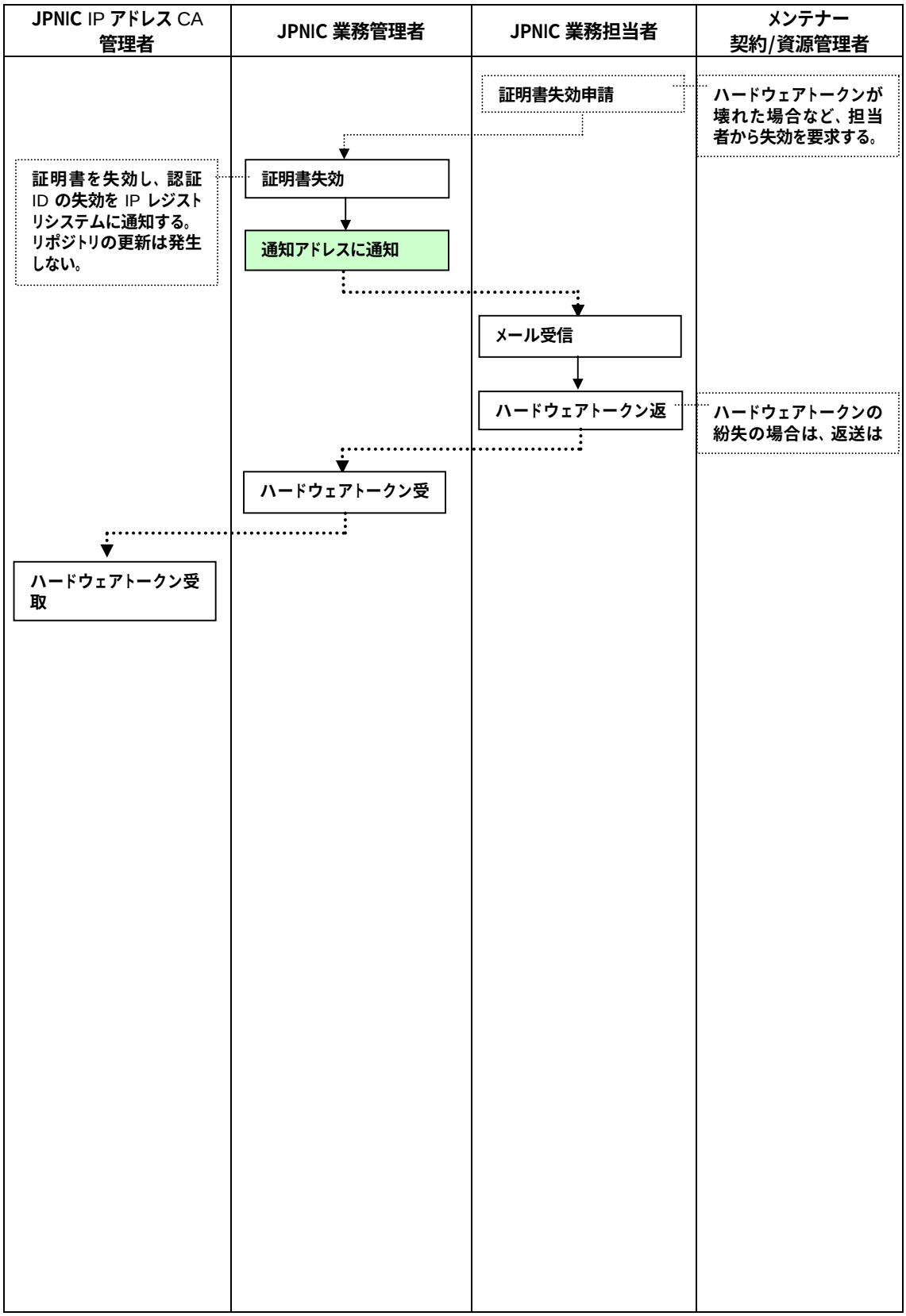
5.2.5.14. JPNIC業務管理者証明書更新業務



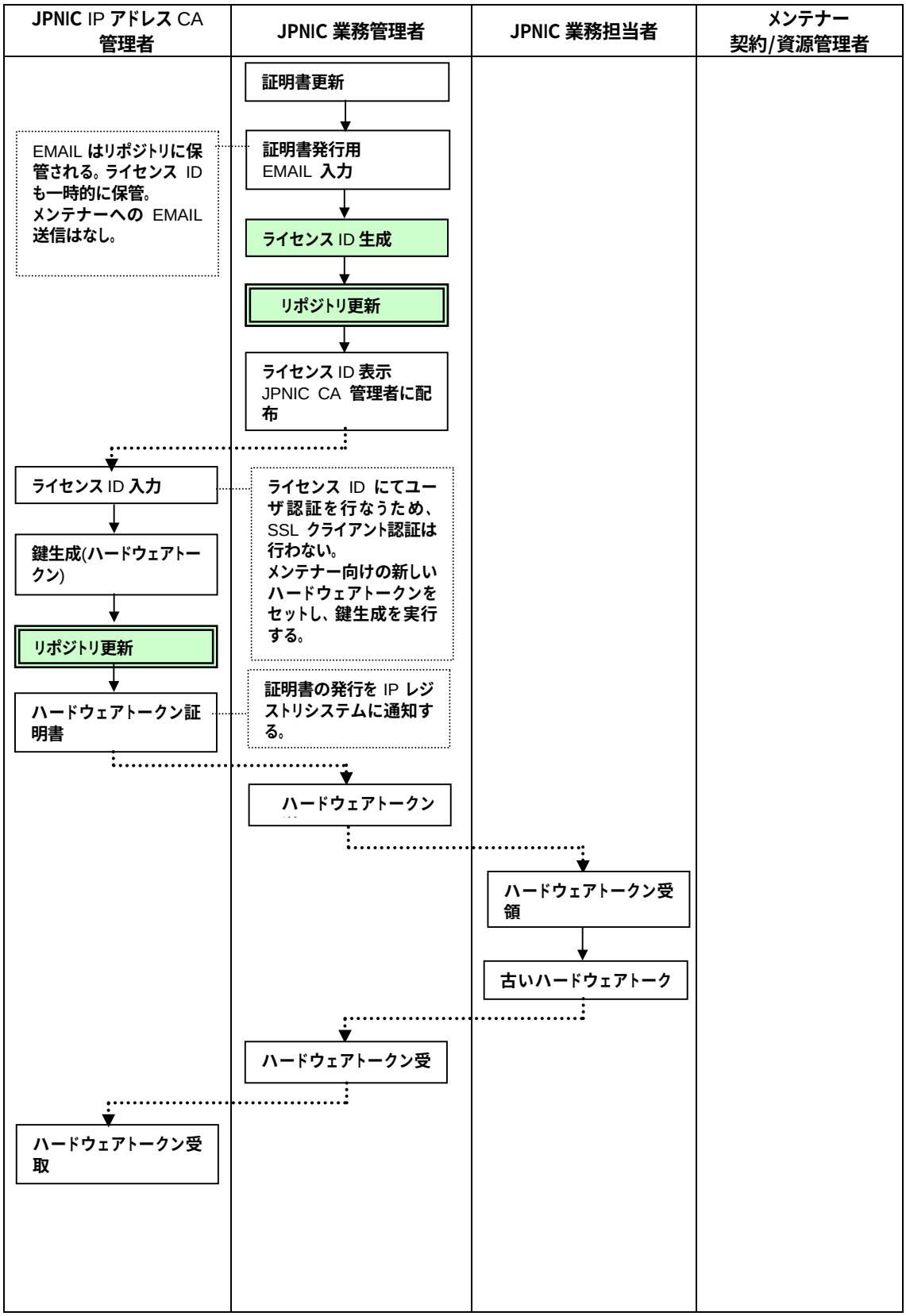
5.2.5.15. JPNIC業務担当者証明書発行業務



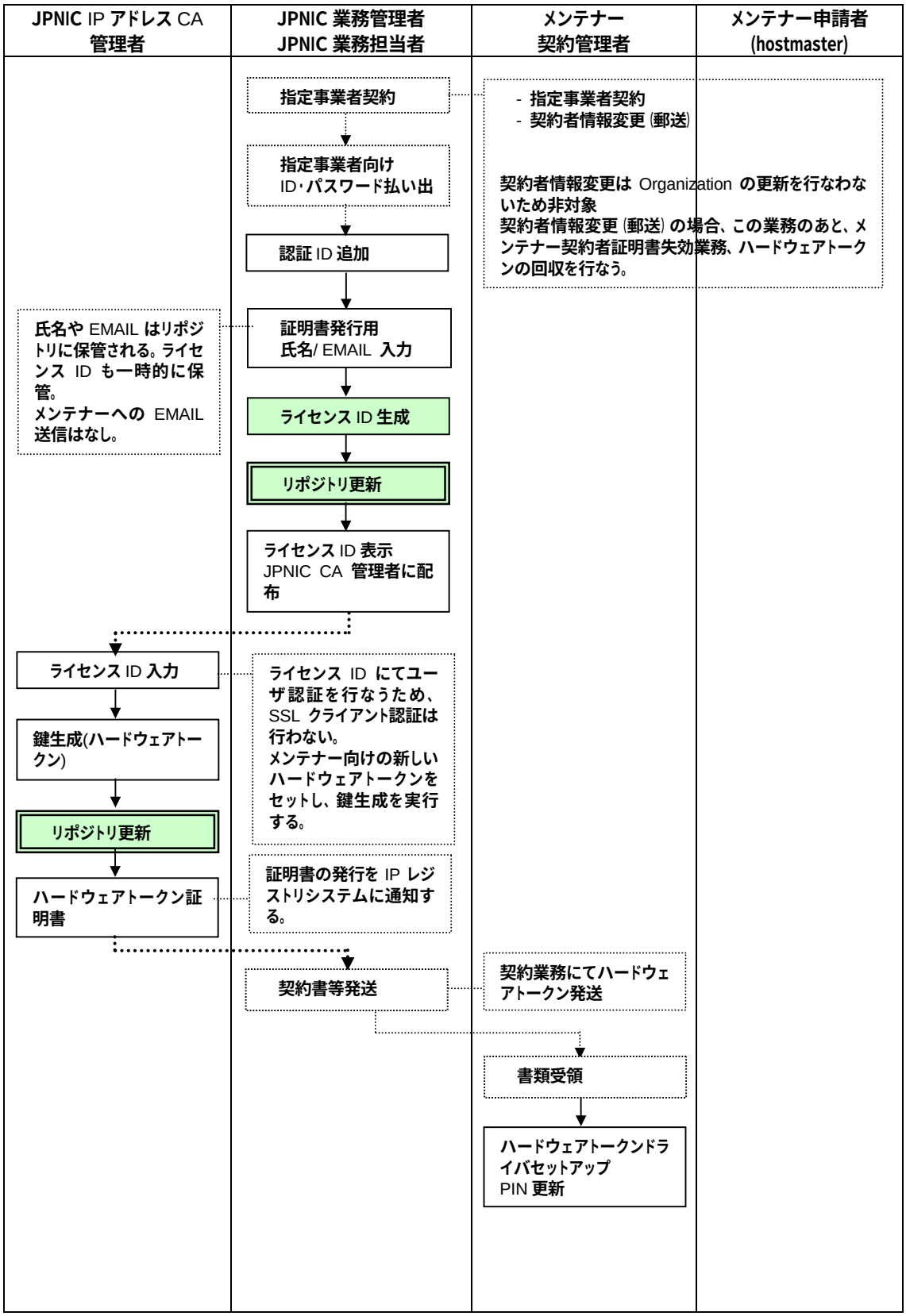
5.2.5.16. JPNIC業務担当者証明書失効業務



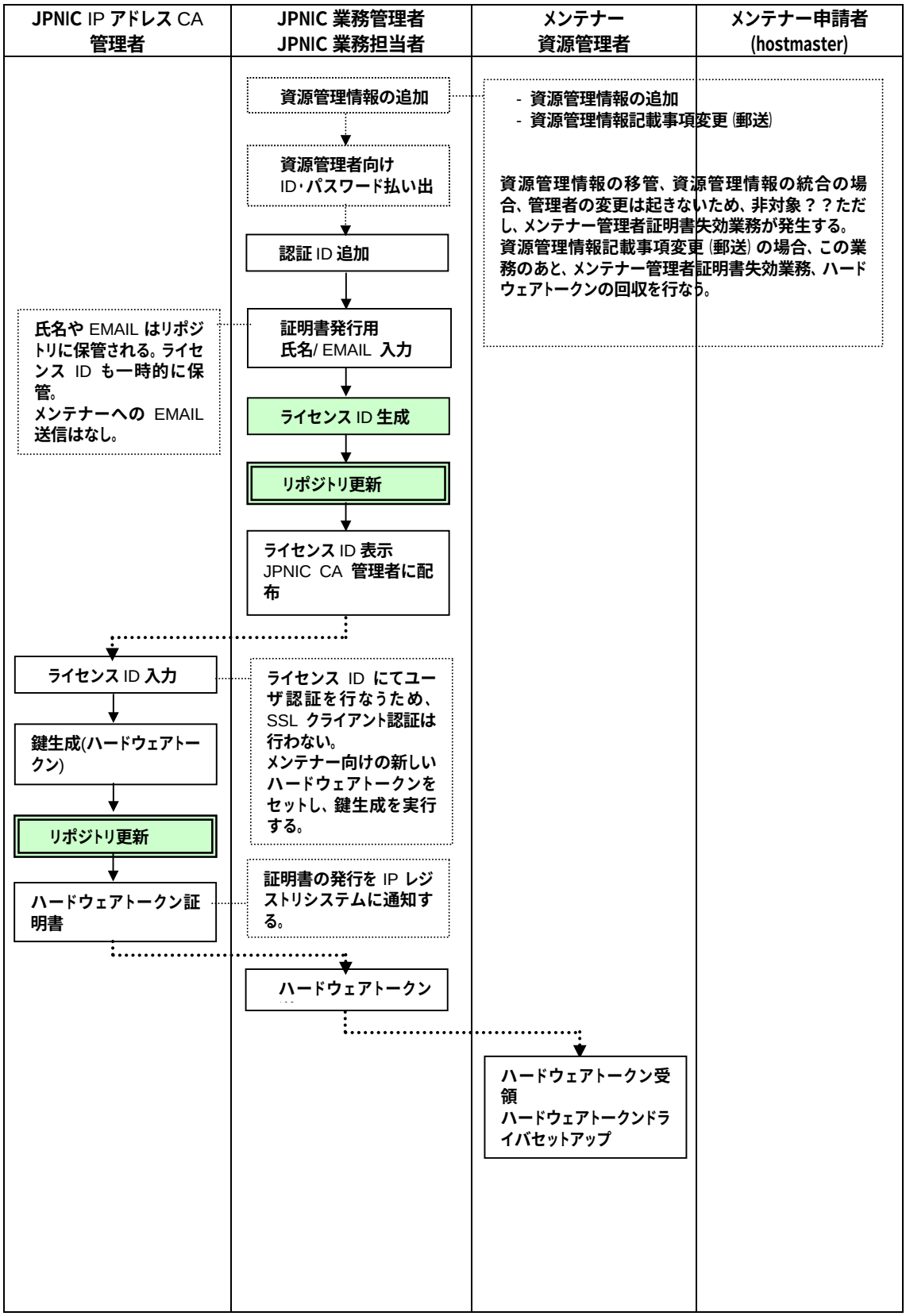
5.2.5.17. JPNIC業務担当者証明書更新業務



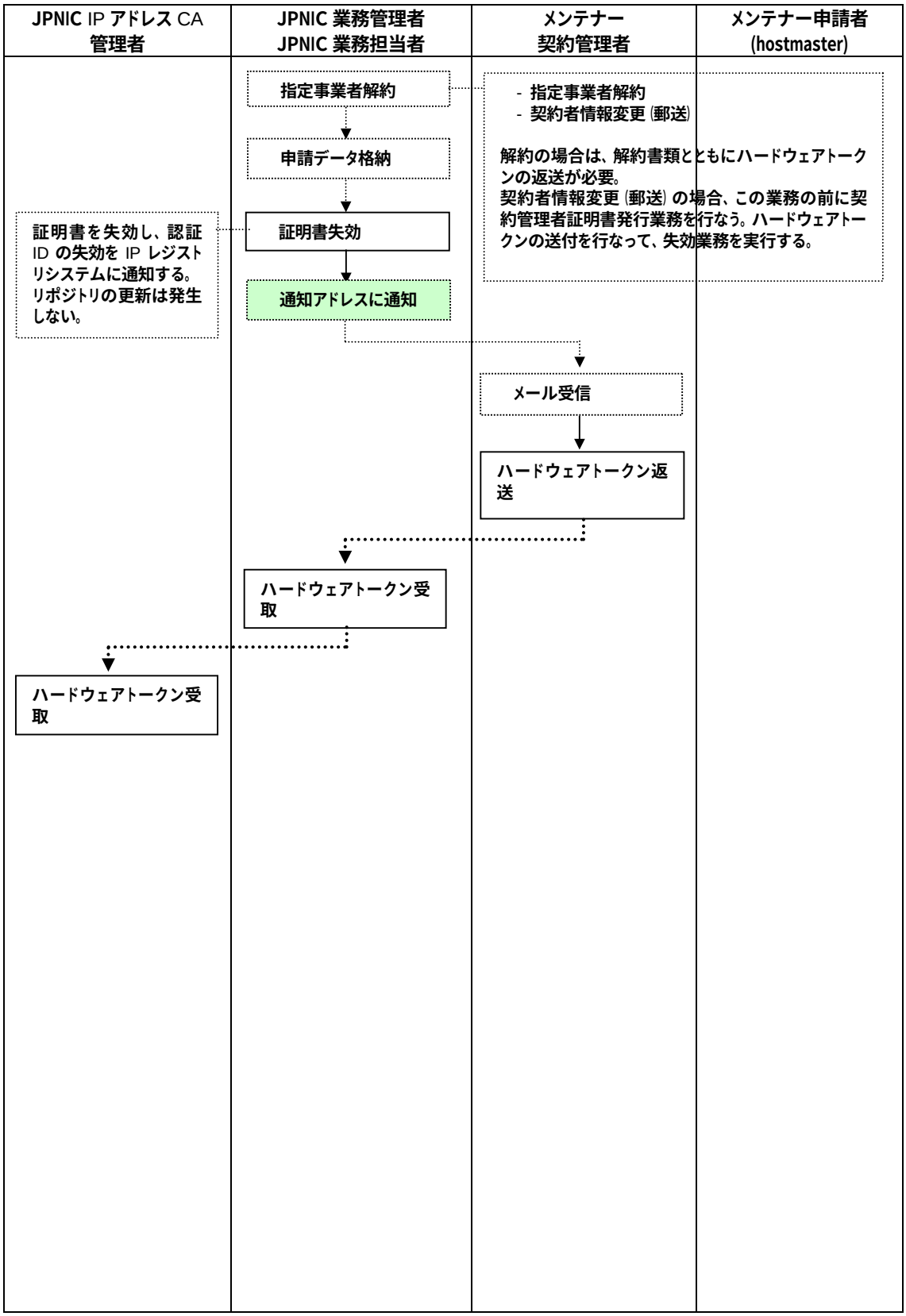
5.2.5.18. メンテナー契約管理者証明書発行業務



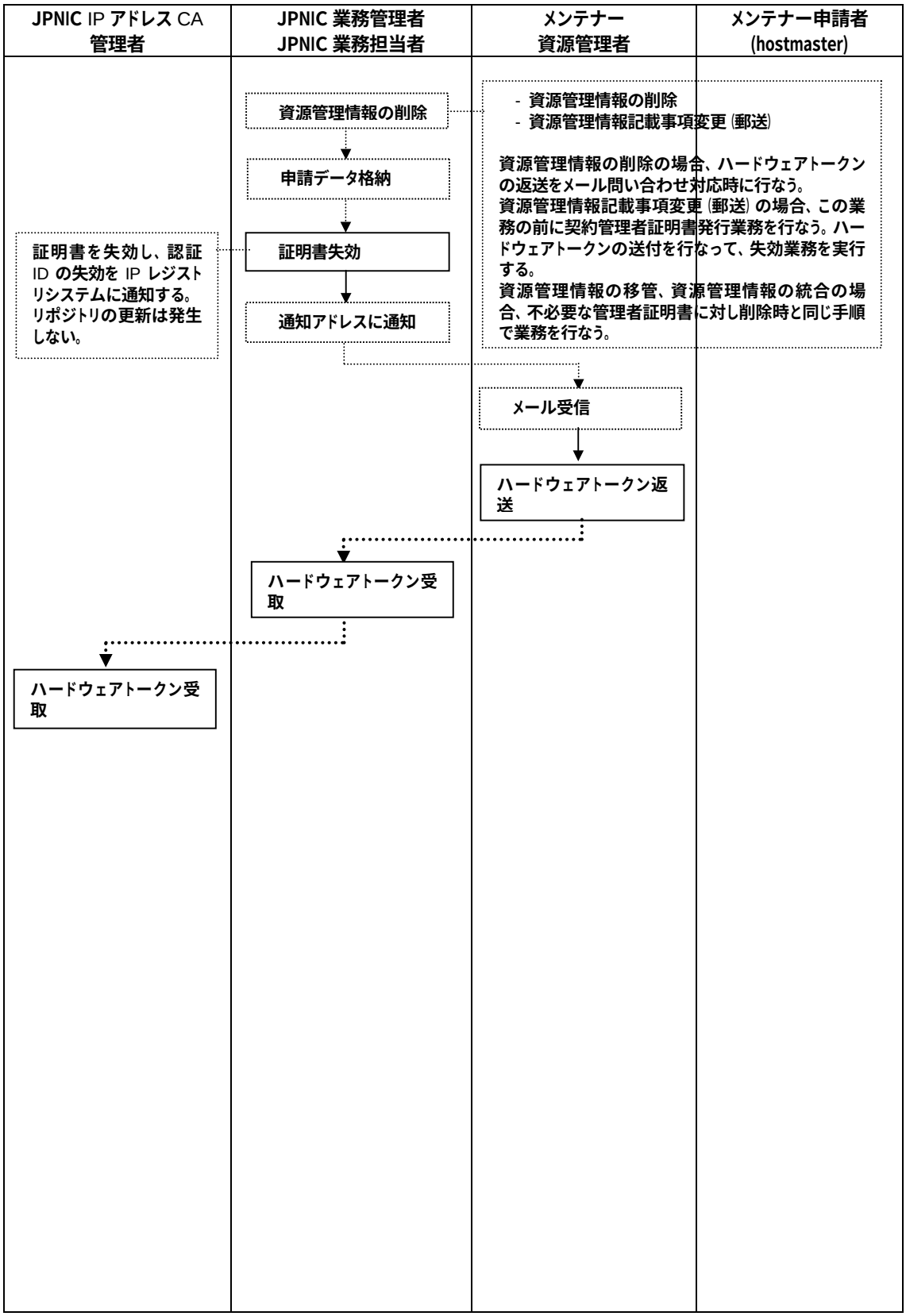
5.2.5.19. メンテナー資源管理者証明書発行業務



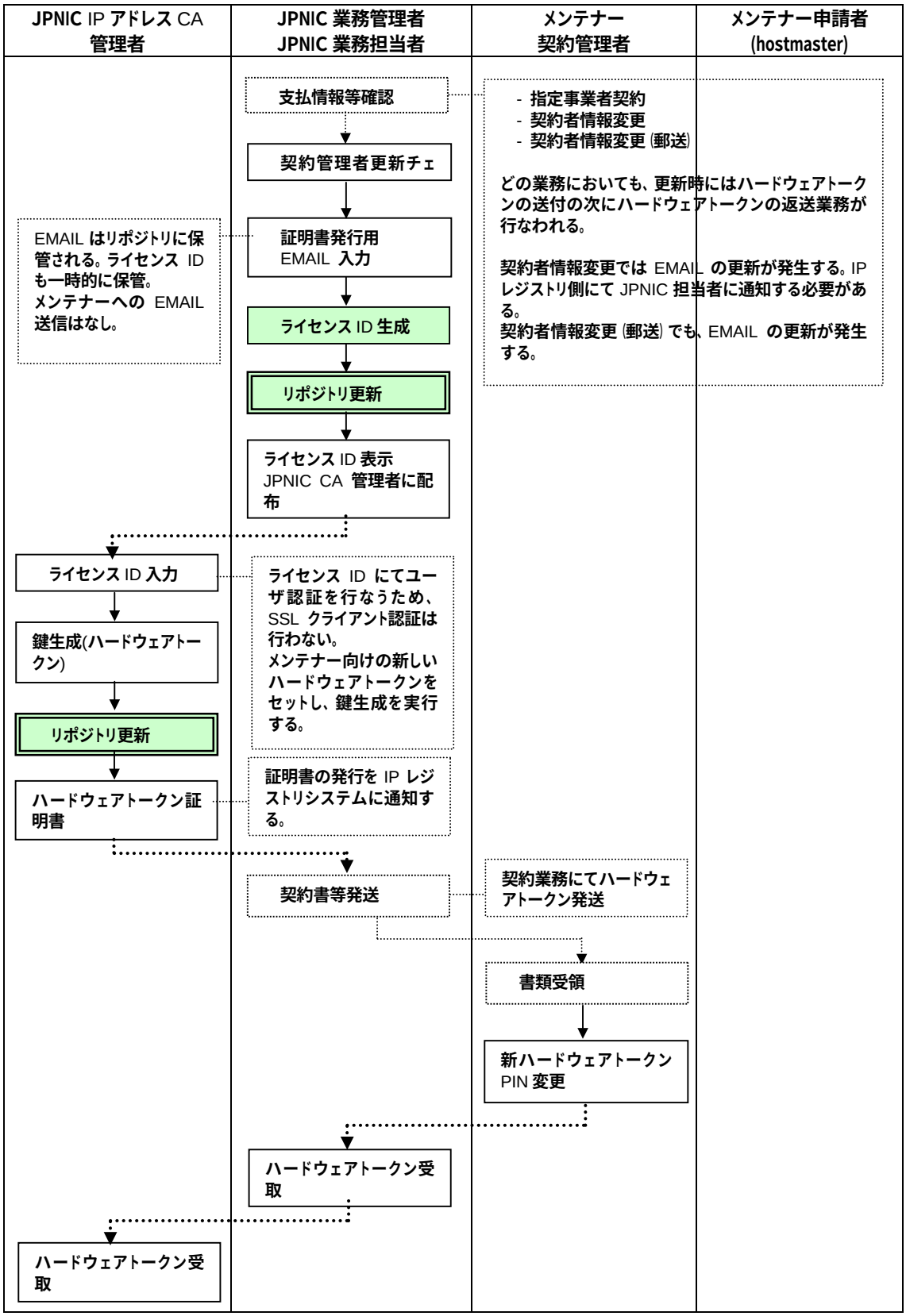
5.2.5.20. メンテナー契約管理者証明書失効業務



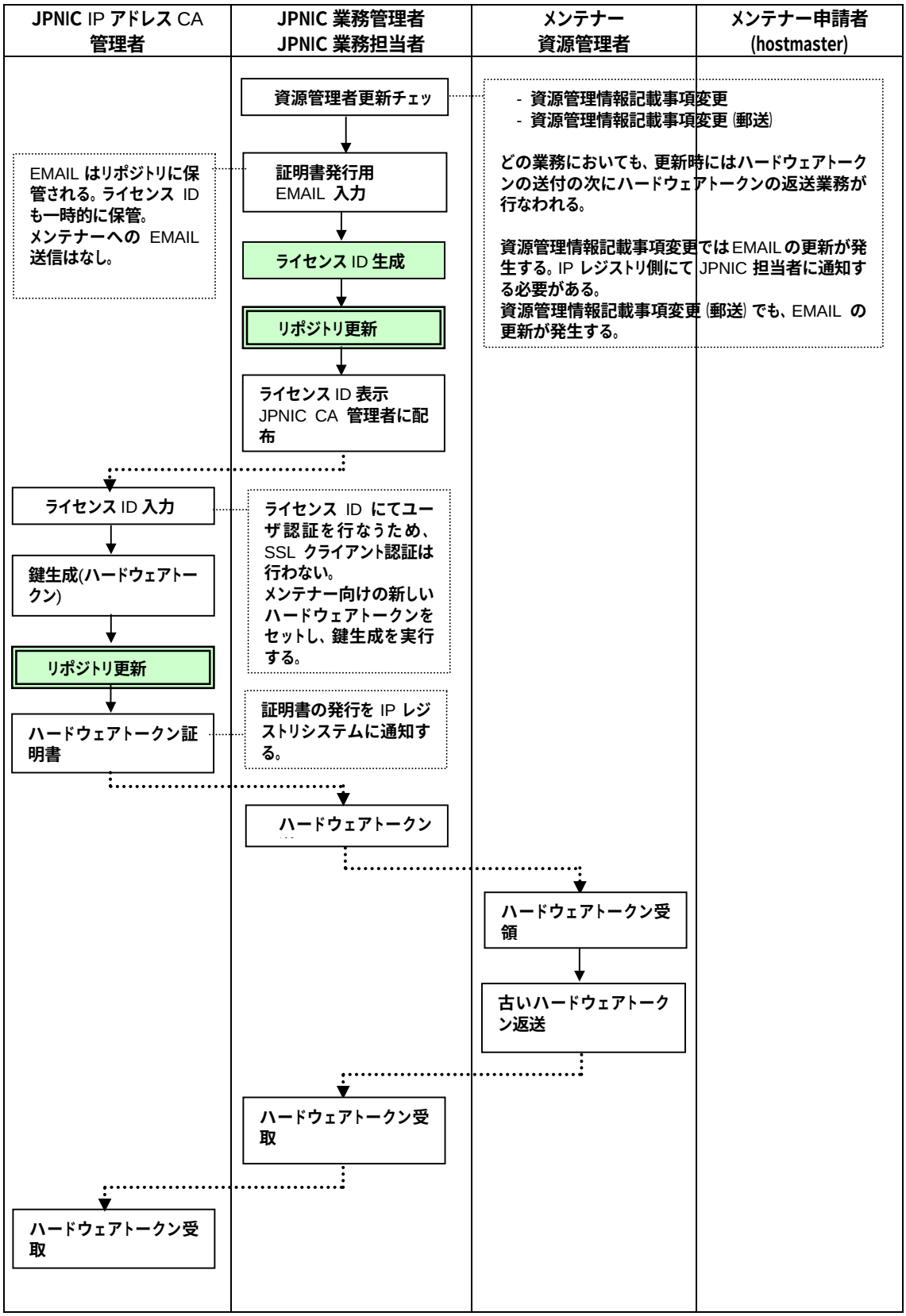
5.2.5.21. メンテナー資源管理者証明書失効業務



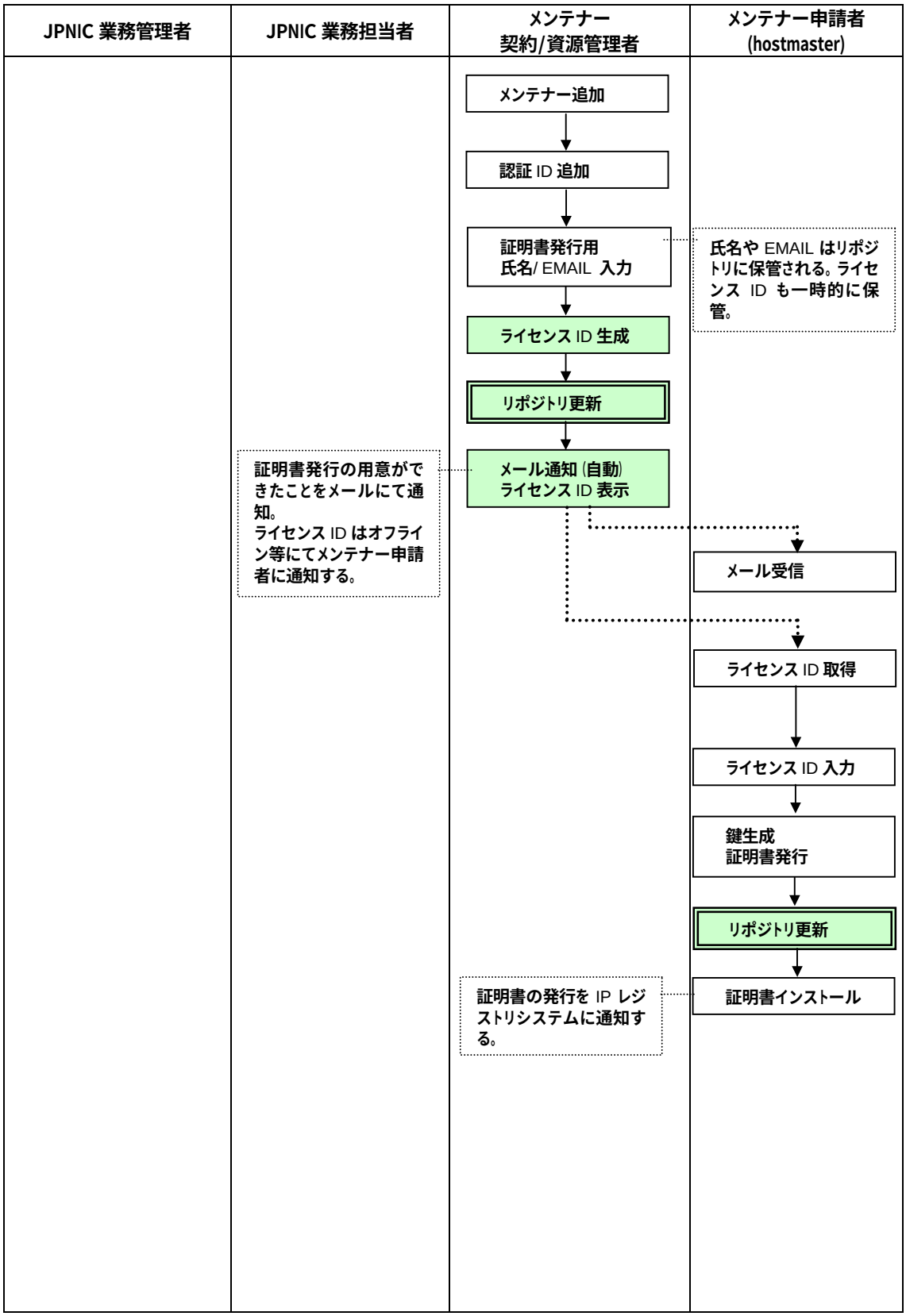
5.2.5.22. メンテナー契約管理者証明書更新業務



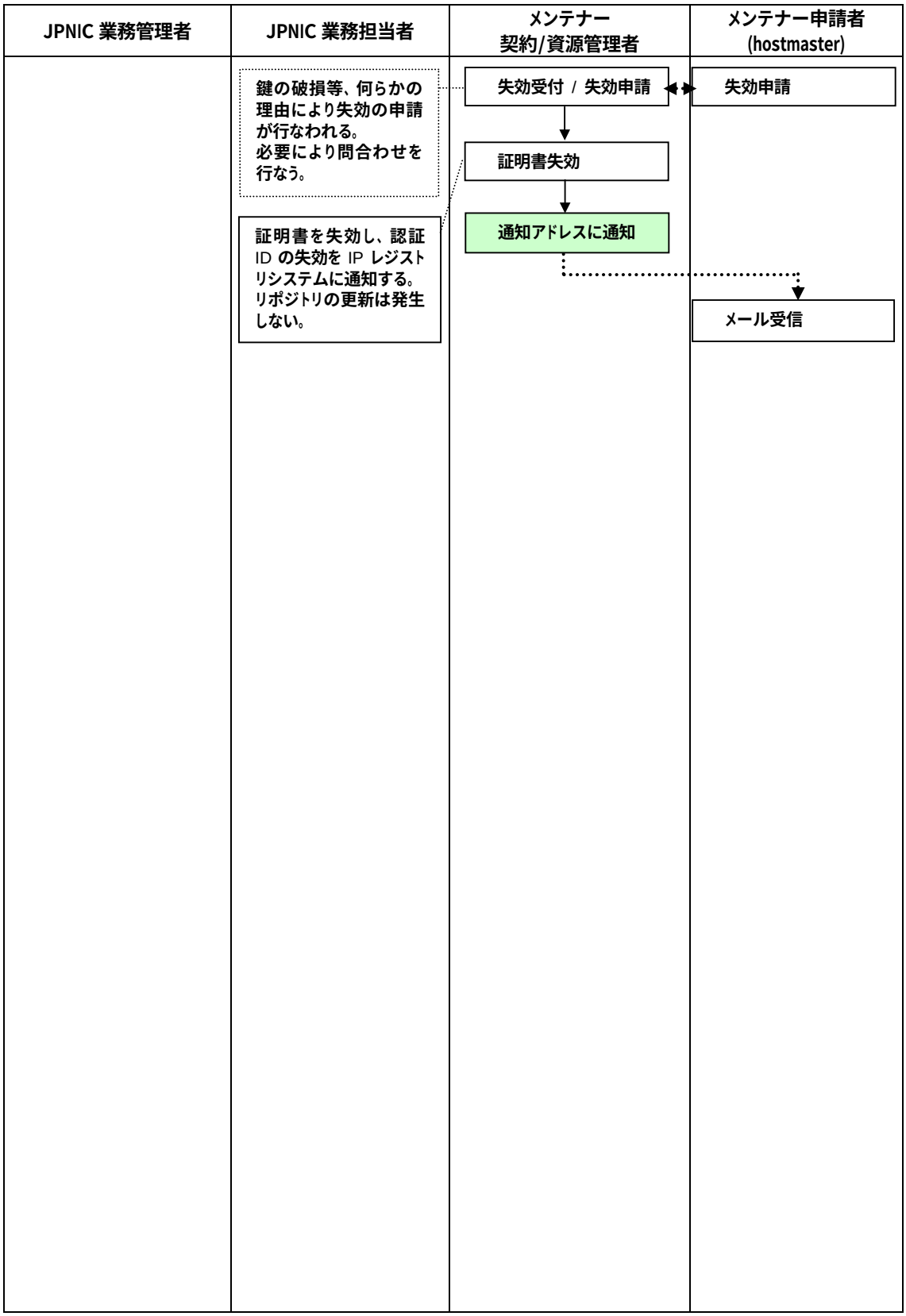
5.2.5.23. メンテナー資源管理者証明書更新業務



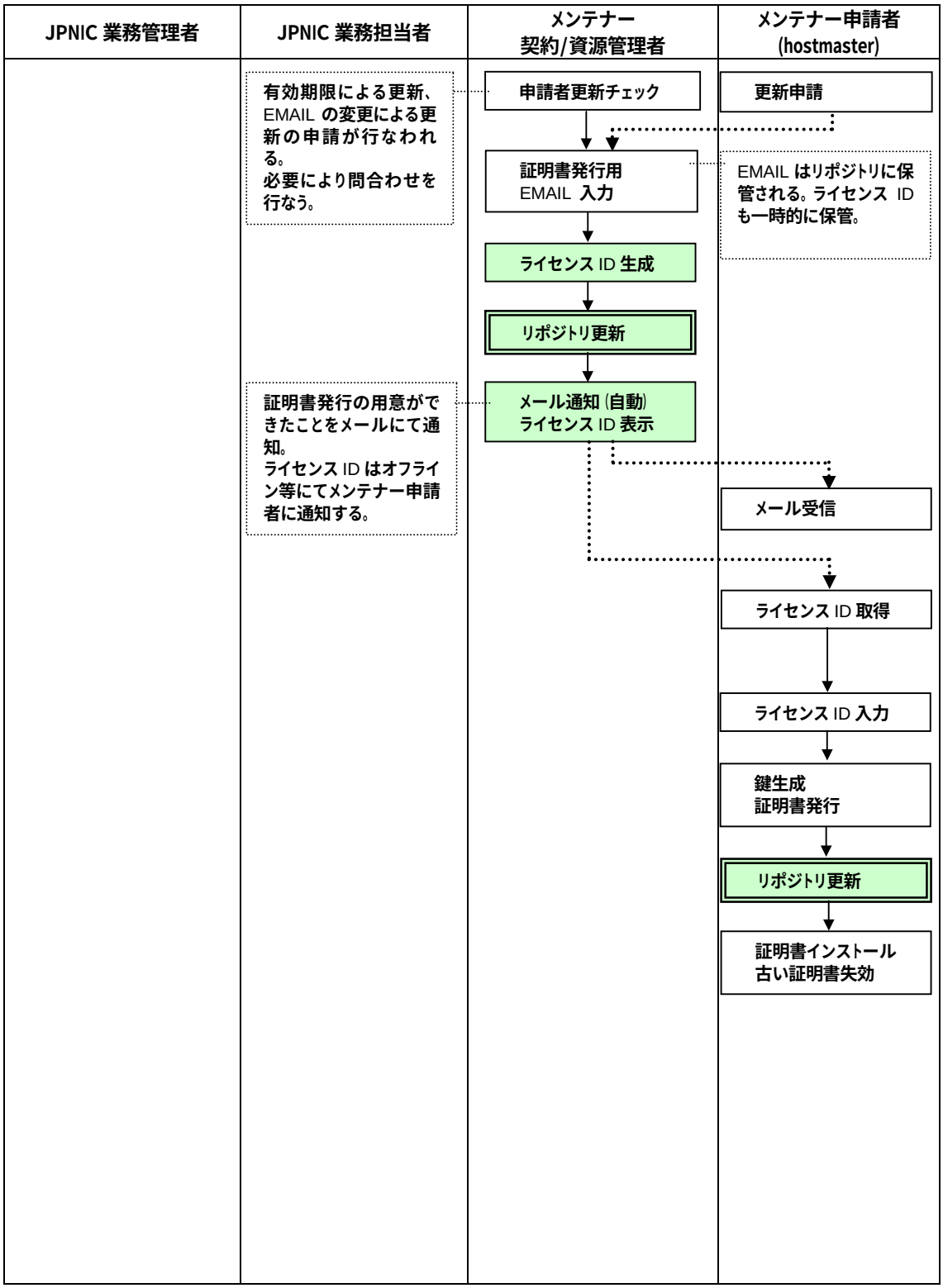
5.2.5.24. メンテナー申請者証明書発行業務



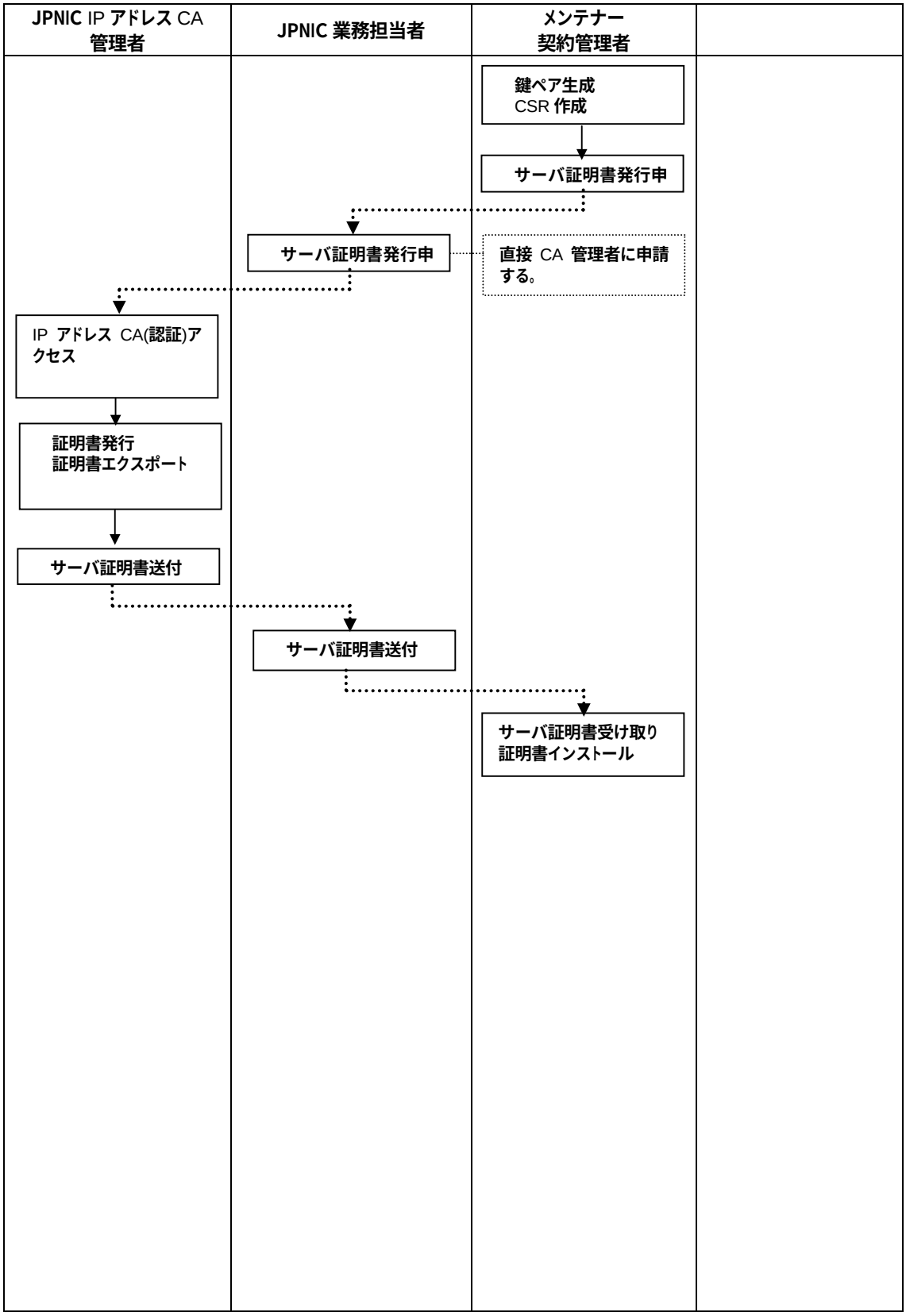
5.2.5.25. メンテナー申請者証明書失効業務



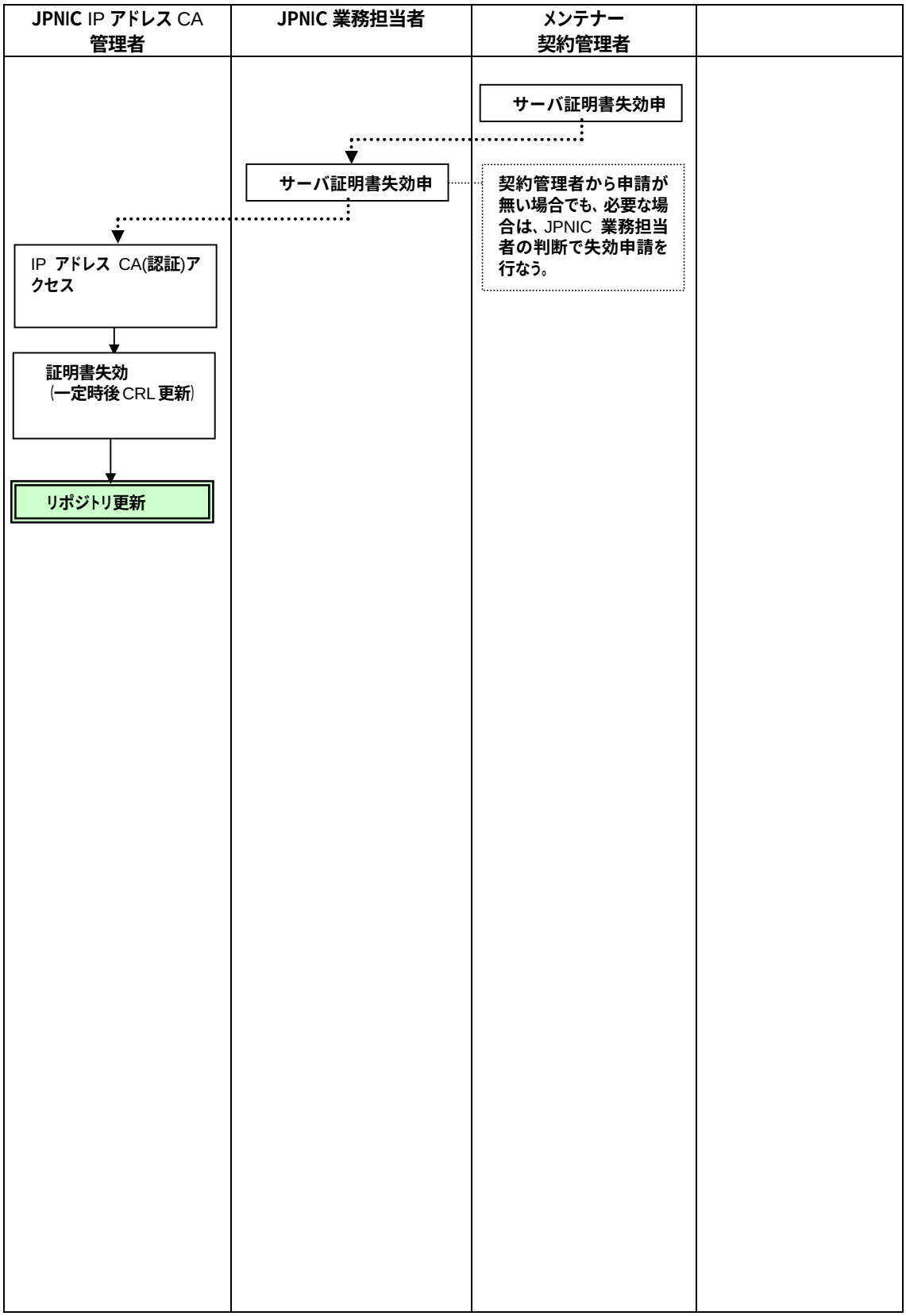
5.2.5.26. メンテナー申請者証明書更新業務



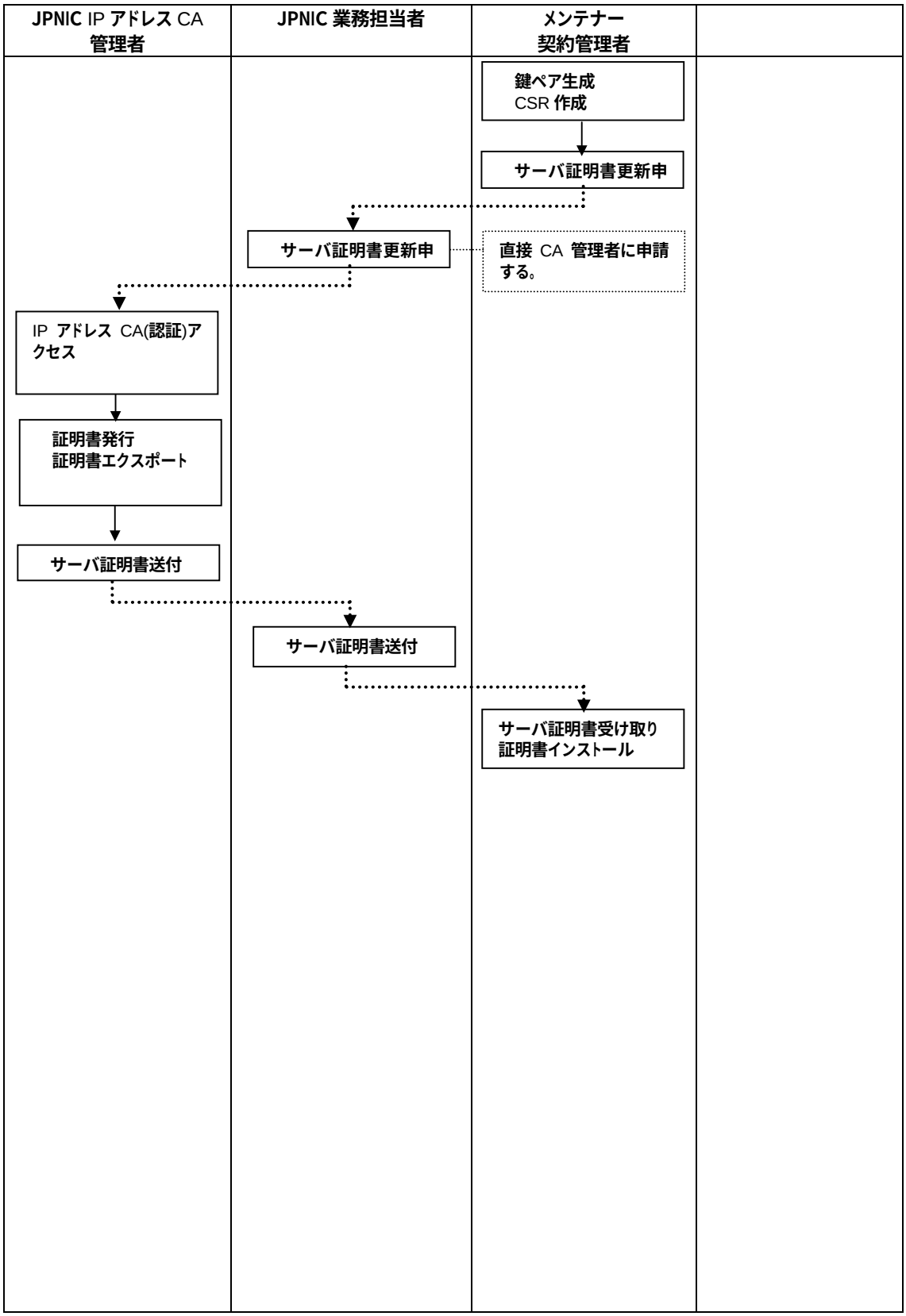
5.2.5.27. 指定事業者サーバ証明書発行業務



5.2.5.28. 指定事業者サーバ証明書失効業務



5.2.5.29. 指定事業者サーバ証明書更新業務



5.2.6. インタフェースの設計

IP アドレス認証局（認証）は、IP レジストリシステム等で使われる認証用途の証明書を発行するだけでなく、IP 指定事業者におけるメンバ管理者が申請業務で使われる証明書（ホストマスタ証明書）の発行申請、失効申請を受け付ける役割を持つ。証明書の発行対象であるユーザの概念は、登録情報における「認証 ID」を軸として定義される。「認証 ID」と IP 指定事業者の関連付けや、申請業務の対象となるアドレス資源との関連付けは「メンテナー」という概念を用いて行われる。

メンテナーは RPSL における mntner に似た概念で、アドレス資源を管理している主体とそのアドレスブロックの情報を併記したデータである。これによって一つの IP 指定事業者が複数のアドレスブロックの割り振りを受ける状況を表現することが出来る。また IP 指定事業者が更にアドレス資源の割り振りを行なった際に、その割り振り構造を表現することができるのである。

本節ではメンテナーに関連付けられた認証 ID の管理画面のイメージについて述べる。認証 ID は証明書の利用者一人一人に割り当てられる識別子である。IP 指定事業者はアドレス資源の申請業務に複数の担当者を設けることが出来るよう、一つのメンテナーに対して複数の認証 ID を定義できるものとした。

5.2.6.1. 外向き申請受付

（1） メンテナー一覧

証明書管理
管理者メンテナー：MNT-zxxxxxx **＜メンテナー一覧＞** **メンテナー** **MNT-zxxxxxx** **MNT-zxxxxxx** **MNT-zxxxxxx**

証明書管理画面ではメンテナーの一覧を表示する。SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。メンテナーコードはリンクとなっており、その 1 つをクリックすると「認証 ID 一覧」に遷移する。

（2） 認証 ID 一覧

証明書管理

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　申請者用

＜認証情報設定＞

認証ID	サブジェクトDN シリアル番号 有効期限	操作
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******	申請中
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	[失効][更新]
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	失効済み

認証 ID 一覧画面ではメンテナーが保持する認証 ID の一覧を表示する。操作対象のメンテナーの情報と SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。認証 ID1 つにつき、それぞれ失効と更新のボタンが用意され、証明書に関する操作を行なえるようになっている。証明書失効の場合「証明書失効」に遷移し、証明書更新の場合は「証明書更新」に遷移する。

(3)　証明書申請

証明書申請の個人情報入力画面を表示する。CN に含まれる名称と申請が行なわれたことを通知する E-MAIL アドレスの入力フォーム（テキストフィールド）が存在する。証明書の申請を実行する場合は、「証明書を申請する」ボタンをクリックする。「証明書申請完了」へ遷移する。

（4） 証明書申請完了

証明書申請完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　申請者用
認証ID:　　***********

証明書申請完了**

**証明書の申請を受け付けました。
名称：*********
EMAIL：****@xxxｘｘ.ne.jp

以下のライセンスIDをメンテナーに通知してください。
ライセンスID：******-******-******

[戻る]**

証明書の申請の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、対象メンテナーに申請通知のメールを送信する。ライセンス ID がシンセ移管料画面に表示されるので、この画面を印刷するなどして、ユーザにライセンス ID を通知する。

(5)　証明書失効

証明書失効

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　申請者用
認証ID:　　**********

シリアル番号：　******
サブジェクトDN：C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　　9999/99/99 99:99:99
終了日時：　　9999/99/99 99:99:99**

**(注意！) 失効処理を行うと、メンテナーがログインできなくなります。
よくご確認のうえ、失効処理を行ってください。**

証明書を失効する

[戻る]

証明書失効の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。証明書の失効を実行する場合は、「証明書を失効する」ボタンをクリックする。「証明書失効完了」に遷移する。

（6） 証明書失効完了

証明書失効完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　申請者用
認証ID:　　***********

証明書失効完了**

証明書の失効が完了しました。

シリアル番号：　****
サブジェクトDN：C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　9999/99/99 99:99:99
終了日時：　9999/99/99 99:99:99**

[戻る]

証明書の失効の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。失効を行なった証明書のシリアル番号、サブジェクト DN、開始日時、終了日時を表示する。CGI は証明書が失効されたことを IP レジストリシステムに通知する。

(7)　証明書更新

証明書更新

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　申請者用
認証ID:　　***********

シリアル番号：　******
サブジェクトDN：　C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　　9999/99/99 99:99:99
終了日時：　　9999/99/99 99:99:99**

EMAIL：

**(注意1) 更新処理を行うと、現在の証明書は自動的に失効されます。
よくご確認のうえ、更新処理を行ってください。**

**(注意2) メンテナーのEMAILを更新する場合、EMAILを入力してください。
空欄の場合は、現在のアドレスを流用します。**

証明書を更新する

[戻る]

証明書更新の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。EMAIL アドレスの変更を行なう場合、EMAIL テキストフィールドに入力する。証明書の更新を実行する場合は、「証明書を更新する」ボタンをクリックする。「証明書更新受付け完了」に遷移する。

（8） 証明書更新受付け完了

証明書更新受け付け完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　申請者用
認証ID:　　***********

証明書更新受け付け完了**

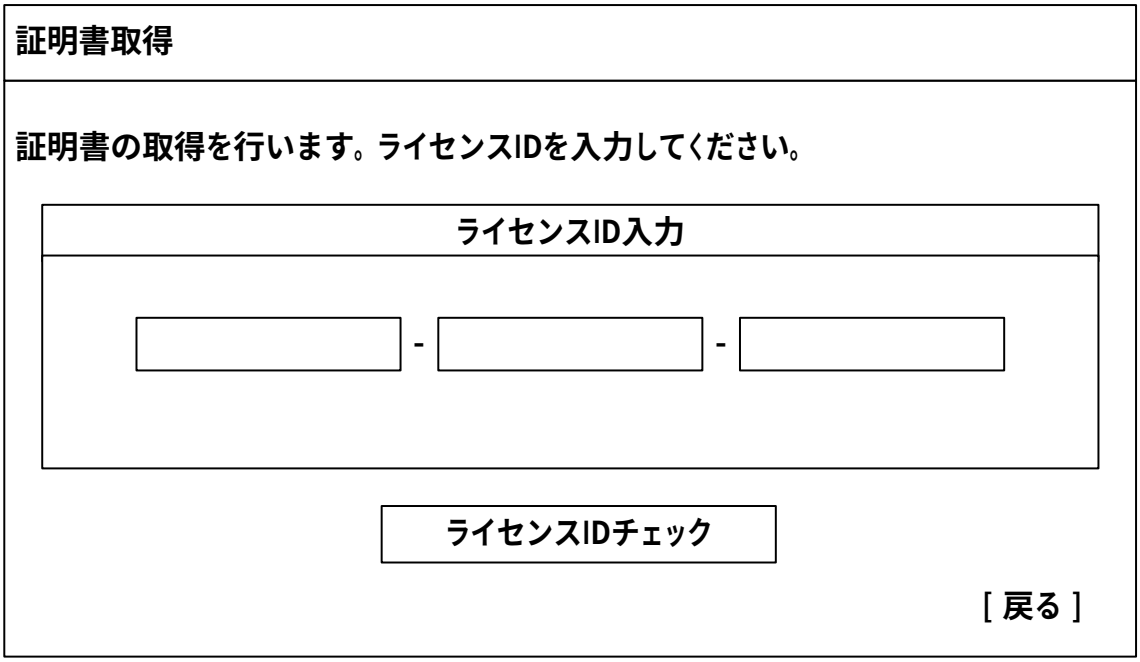
**証明書更新の申請を受け付けました。
名称：*********
EMAIL：****@xxxｘｘ.ne.jp

以下のライセンスIDをメンテナーに通知してください。
ライセンスID：******-******-******

[戻る]**

証明書更新の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、対象メンテナーに申請通知のメールを送信する。ライセンス ID が申請完了画面に表示されるので、この画面を印刷するなどして、ユーザにライセンス ID を通知する。

(9)　証明書取得



証明書の取得を行なう。ライセンス ID を 3 つに別れているテキストフィールドに入力する。「ライセンス ID チェック」ボタンを押すことで、認証を行ない「証明書取得（鍵生成）」に遷移する。

（10） 証明書取得（鍵作成）

証明書取得

証明書の鍵ペアを生成し、証明書を取得します。

メンテナー: MNT-zxxxxxx
権限種別: 申請者用
認証ID: *********

メンテナー情報確認

以下の情報で証明書を発行します。

名称: *******
EMAIL: ****@xxxｘｘ.ne.jp**

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書を取得する

[戻る]

証明書取得の確認画面を表示する。指定のライセンス ID から証明書を発行するメンテナーの情報を検索し、操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。「証明書を取得する」ボタンを押して秘密鍵を生成し、CGI 側にて CA サーバにアクセス、証明書の発行を行なう。この後、「証明書インストール」に遷移する。

（11） 証明書インストール

証明書インストール

証明書を発行しました。お使いのPCに証明書をインストールします。

メンテナー: MNT-zxxxxxx
権限種別: 申請者用
認証ID: *********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書をインストール

証明書のインストール画面を表字する。操作を行なっているメンテナーコード、認証 ID を表示する。この画面が表示される時点で、CA から証明書が発行されローカル PC にダウンロードされており、「証明書をインストール」ボタンを押すことで、証明書のインストールが行なえる。インストール後に「証明書インストール完了」に遷移する。

（12） 証明書インストール完了

証明書インストール完了

証明書のインストールが完了しました。

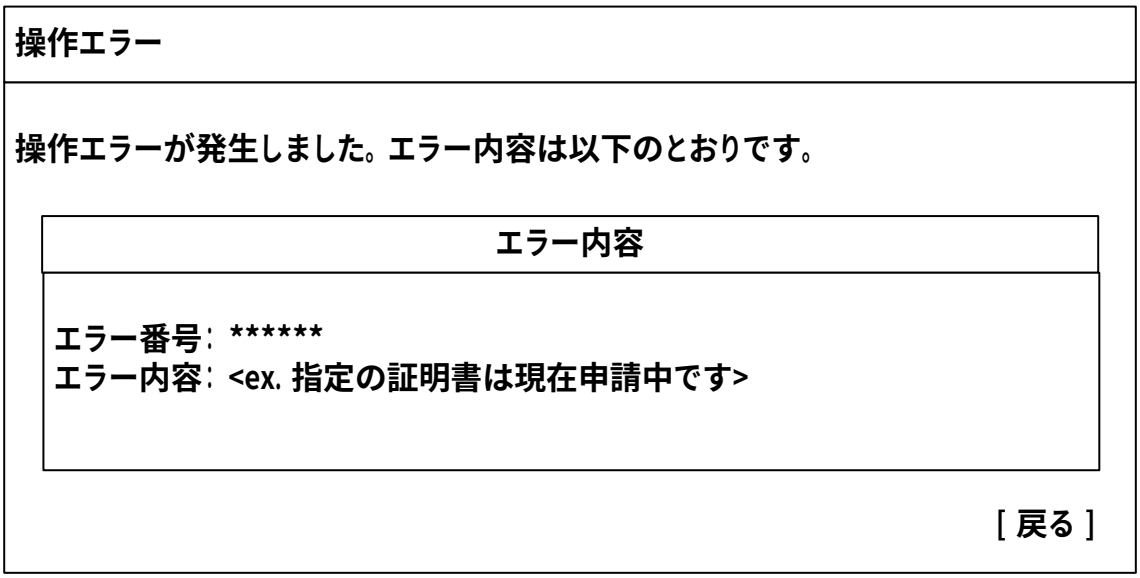
メンテナー: MNT-zxxxxxx
権限種別: 申請者用
認証ID: *********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

[戻る]

証明書インストールの完了を表示する。操作を行なっているメンテナーコード、認証 ID を表示する。また、発行した証明書のサブジェクトの表示も行なう。

（13） エラー表示



エラー一般の表示を行なう画面。エラー番号やそのエラーの内容を表示する。

5.2.6.2. 内向き申請受付（業務管理者向け）

（1） メンテナー一覧

証明書管理

管理者メンテナー：MNT-zxxxxxx

メンテナー	権限種別	名前
MNT-zxxxxxx	JPNIC業務担当者用	**********
MNT-zxxxxxx	JPNIC業務担当者用	**********
MNT-zxxxxxx	JPNIC業務担当者用	**********

証明書管理画面ではメンテナーの一覧を表示する。SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。メンテナーコードはリンクとなっており、その 1 つをクリックすると「従業員コード一覧」に遷移する。

(2)　従業員コード一覧

証明書管理

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　JPNIC業務担当者用

＜認証情報設定＞

従業員コード	サブジェクトDN シリアル番号 有効期限	操作
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******	申請中
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	[失効][更新]
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	失効済み

従業員コード（認証 ID）一覧画面ではメンテナーが保持する従業員コードの一覧を表示する。操作対象のメンテナーの情報と SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。従業員コード 1 つにつき、それぞれ失効と更新のボタンが用意され、証明書に関する操作を行なえるようになっている。証明書失効の場合「証明書失効」に遷移し、証明書更新の場合は「証明書更新」に遷移する。

(3)　証明書申請

証明書申請の個人情報入力画面を表示する。CN に含まれる名称、申請が行なわれたことを通知する E-MAIL アドレスの入力フォーム（テキストフィールド）が存在する。証明書の申請を実行する場合は、「証明書を申請する」ボタンをクリックする。「証明書申請完了」へ遷移する。

（4） 証明書申請完了

証明書申請完了

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　JPNIC業務担当者用
従業員コード：　********

証明書申請完了

証明書の申請を受け付けました。

名称：*******
EMAIL：****@xxxｘｘ.ne.jp**

**以下のライセンスIDをCA管理者に通知してください。
ライセンスID：******-******-******

[戻る]**

証明書の申請の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコードを表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、CA 管理者に申請通知のメールを送信する。ライセンス ID が申請完了画面に表示されるので、この画面を印刷するなどして、CA 管理者にライセンス ID を通知する。

(5)　証明書失効

証明書失効

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　JPNIC業務担当者用
従業員コード：　************

シリアル番号：　******
サブジェクトDN：C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=********
開始日時：　9999/99/99 99:99:99
終了日時：　9999/99/99 99:99:99

(注意！) 失効処理を行うと、業務担当者がログインできなくなります。
よくご確認のうえ、失効処理を行ってください。

証明書を失効する

[戻る]

証明書失効の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。証明書の失効を実行する場合は、「証明書を失効する」ボタンをクリックする。「証明書失効完了」に遷移する。

(6)　証明書失効完了

証明書失効完了

管理者メンテナー：MNT-zxxxxxx

メンテナー：　　MNT-zxxxxxx
権限種別：　　JPNIC業務担当者用
従業員コード：　********

証明書失効完了

証明書の失効が完了しました。

シリアル番号：　****
サブジェクトDN：C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　　9999/99/99 99:99:99
終了日時：　　9999/99/99 99:99:99**

[戻る]

証明書の失効の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、従業員コードを表示する。失効を行なった証明書のシリアル番号、サブジェクト DN、開始日時、終了日時を表示する。CGI は証明書が失効されたことを IP レジストリシステムに通知する。

(7)　証明書更新

証明書更新

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　JPNIC業務担当者用
従業員コード：　***********

シリアル番号：　******
サブジェクトDN：　C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=********
開始日時：　9999/99/99 99:99:99
終了日時：　9999/99/99 99:99:99

EMAIL：

(注意1) 更新処理を行うと、現在の証明書は自動的に失効されます。
よくご確認のうえ、更新処理を行ってください。

(注意2) 業務担当者のEMAILを更新する場合、EMAILを入力してください。
空欄の場合は、現在のアドレスを流用します。

証明書を更新する

[戻る]

証明書更新の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、従業員コードを表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。EMAIL アドレスの変更を行なう場合、EMAIL テキストフィールドに入力する。証明書の更新を実行する場合は、「証明書を更新する」ボタンをクリックする。「証明書更新受付け完了」に遷移する。

(8)　証明書更新受付け完了

証明書更新受け付け完了

管理者メンテナー：MNT-zxxxxxx

メンテナー：　　MNT-zxxxxxx
権限種別：　　JPNIC業務担当者用
従業員コード：　********

証明書更新受け付け完了

証明書更新の申請を受け付けました。

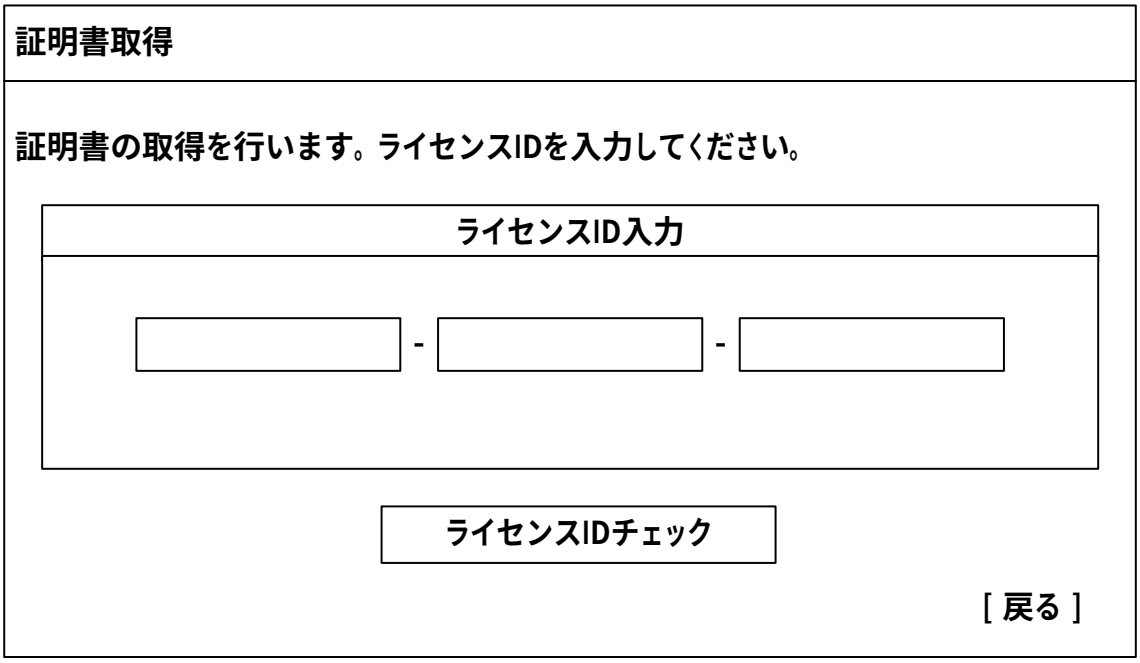
名称：　*******
EMAIL：　****@xxxｘｘ.ne.jp**

**以下のライセンスIDをCA管理者に通知してください。
ライセンスID：******-******-******

[戻る]**

証明書更新の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、従業員コードを表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、CA 管理者に申請通知のメールを送信する。ライセンス ID が申請完了画面に表示されるので、この画面を印刷するなどして、CA 管理者にライセンス ID を通知する。

(9)　証明書取得（ライセンス ID 入力）



証明書の取得を行なう。ライセンス ID を 3 つに別れているテキストフィールドに入力する。「ライセンス ID チェック」ボタンを押すことで、認証を行ない「証明書取得（鍵生成）」に遷移する。

（10） 証明書取得（鍵作成）

証明書取得

証明書の鍵ペアを生成し、証明書を取得します。HWキーを挿入してください。

メンテナー:　　MNT-zxxxxxx
権限種別:　　JPNIC業務担当者用
従業員コード:　********

メンテナー情報確認

以下の情報で証明書を発行します。

名称: *******
EMAIL: ****@xxxｘｘ.ne.jp**

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書を取得する

[戻る]

証明書取得の確認画面を表示する。指定のライセンス ID から証明書を発行するメンテナーの情報を検索し、操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、従業員コードを表示する。また、申請内容の名称と EMAIL を表示する。「証明書を取得する」ボタンを押して秘密鍵を生成し、CGI 側にて CA サーバにアクセス、証明書の発行を行なう。この後、「証明書インストール」に遷移する。

（11） 証明書インストール

証明書インストール

証明書を発行しました。HWキーに証明書をインストールします。

メンテナー:　　MNT-zxxxxxx
権限種別:　　JPNIC業務担当者用
従業員コード:　********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書をインストール

証明書のインストール画面を表字する。操作を行なっているメンテナーコード、従業員コードを表示する。この画面が表示される時点で、CA から証明書が発行されローカル PC にダウンロードされており、「証明書をインストール」ボタンを押すことで、証明書のインストールが行なえる。インストール後に「証明書インストール完了」に遷移する。

（12） 証明書インストール完了

証明書インストール完了

証明書のインストールが完了しました。

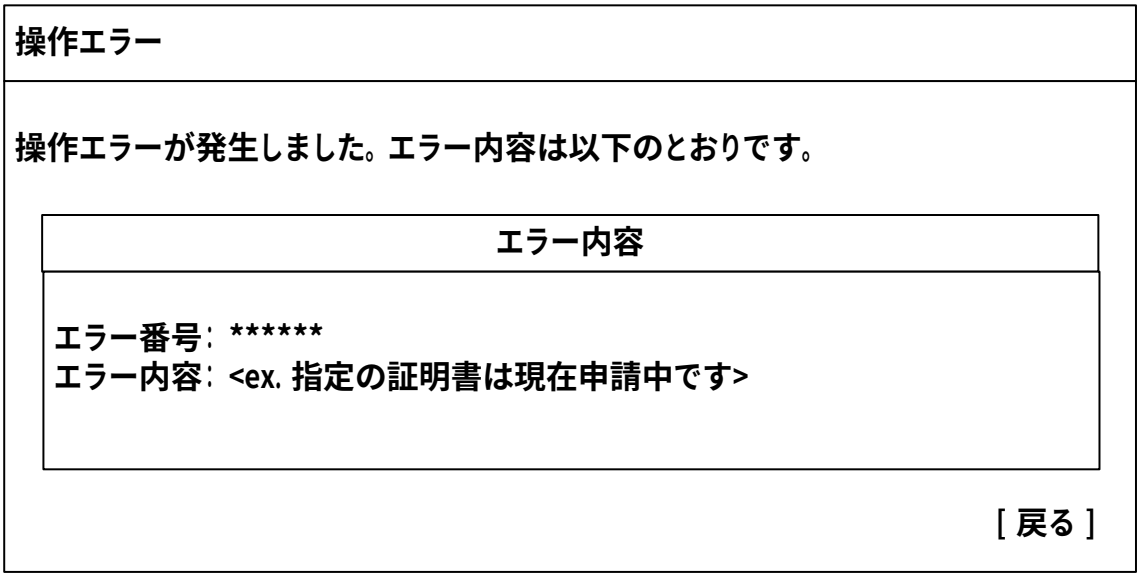
メンテナー:　　MNT-zxxxxxx
権限種別:　　JPNIC業務担当者用
従業員コード:　********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

[戻る]

証明書インストールの完了を表示する。操作を行なっているメンテナーコード、従業員コードを表示する。また、発行した証明書のサブジェクトの表示も行なう。

（13） エラー表示



エラー一般の表示を行なう画面。エラー番号やそのエラーの内容を表示する。

5.2.6.3. 内向き申請受付（業務担当者向け）

（1） メンテナー検索

証明書管理

管理者メンテナー：MNT-zxxxxxx

検索区分：
- ○ **契約管理者番号（完全一致）**
- ○ **資源管理者番号（完全一致）**
- ○ **資源管理者略称（完全一致）**
- ○ **組織名（部分一致）**
- ○ **メンテナーコード（完全一致）**

検索文字列：

検索を実行

証明書管理画面ではメンテナーの検索画面を表示する。SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。検索文字列を入力し、検索を開始すると「メンテナー一覧」へ遷移する。

(2)　メンテナー一覧

証明書管理

管理者メンテナー：MNT-zxxxxx

メンテナー	権限種別	名前	組織名
MNT-zxxxxx	契約管理者用	**********	**********
MNT-zxxxxx	資源管理者用	**********	**********
MNT-zxxxxx	契約管理者用	**********	**********

検索結果のメンテナー一覧を表示する。メンテナーコードはリンクとなっており、その 1 つをクリックすると「認証 ID 一覧」に遷移する。

(3)　認証 ID 一覧

証明書管理

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用

＜認証情報設定＞

認証ID	サブジェクトDN シリアル番号 有効期限	操作
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******	申請中
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	[失効][更新]
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	失効済み

認証 ID 一覧画面ではメンテナーが保持する認証 ID の一覧を表示する。操作対象のメンテナーの情報と SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。認証 ID1 つにつき、それぞれ失効と更新のボタンが用意され、証明書に関する操作を行なえるようになっている。証明書失効の場合「証明書失効」に遷移し、証明書更新の場合は「証明書更新」に遷移する。

（4） 証明書申請

証明書申請の個人情報入力画面を表示する。CN に含まれる名称と申請が行なわれたことを通知する E-MAIL アドレスの入力フォーム（テキストフィールド）が存在する。証明書の申請を実行する場合は、「証明書を申請する」ボタンをクリックする。「証明書申請完了」へ遷移する。

(5)　証明書申請完了

証明書申請完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用
認証ID:　　***********

証明書申請完了**

**証明書の申請を受け付けました。
名称：*********
EMAIL：****@xxxｘｘ.ne.jp**

**以下のライセンスIDをCA管理者に通知してください。
ライセンスID：******-******-******

[戻る]**

証明書の申請の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、CA 管理者に申請通知のメールを送信する。ライセンス ID が申請完了画面に表示されるので、この画面を印刷するなどして、CA 管理者にライセンス ID を通知する。

（6） 証明書失効

証明書失効

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用
認証ID:　　**********

シリアル番号：　******
サブジェクトDN：C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　　9999/99/99 99:99:99
終了日時：　　9999/99/99 99:99:99**

**(注意！) 失効処理を行うと、メンテナーがログインできなくなります。
よくご確認のうえ、失効処理を行ってください。**

証明書を失効する

[戻る]

証明書失効の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。証明書の失効を実行する場合は、「証明書を失効する」ボタンをクリックする。「証明書失効完了」に遷移する。

(7)　証明書失効完了

証明書失効完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用
認証ID:　　***********

証明書失効完了**

証明書の失効が完了しました。

シリアル番号：　****
サブジェクトDN：C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN******
開始日時：　9999/99/99 99:99:99
終了日時：　9999/99/99 99:99:99**

[戻る]

証明書の失効の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。失効を行なった証明書のシリアル番号、サブジェクト DN、開始日時、終了日時を表示する。CGI は証明書が失効されたことを IP レジストリシステムに通知する。

(8)　証明書更新

証明書更新

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用
認証ID:　　***********

シリアル番号：　******
サブジェクトDN：　C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　9999/99/99 99:99:99
終了日時：　9999/99/99 99:99:99**

EMAIL：

**(注意1) 更新処理を行うと、現在の証明書は自動的に失効されます。
よくご確認のうえ、更新処理を行ってください。**

**(注意2) メンテナーのEMAILを更新する場合、EMAILを入力してください。
空欄の場合は、現在のアドレスを流用します。**

証明書を更新する

[戻る]

証明書更新の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。EMAIL アドレスの変更を行なう場合、EMAIL テキストフィールドに入力する。証明書の更新を実行する場合は、「証明書を更新する」ボタンをクリックする。「証明書更新受付け完了」に遷移する。

(9)　証明書更新受付け完了

証明書更新受け付け完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用
認証ID:　　***********

証明書更新受け付け完了**

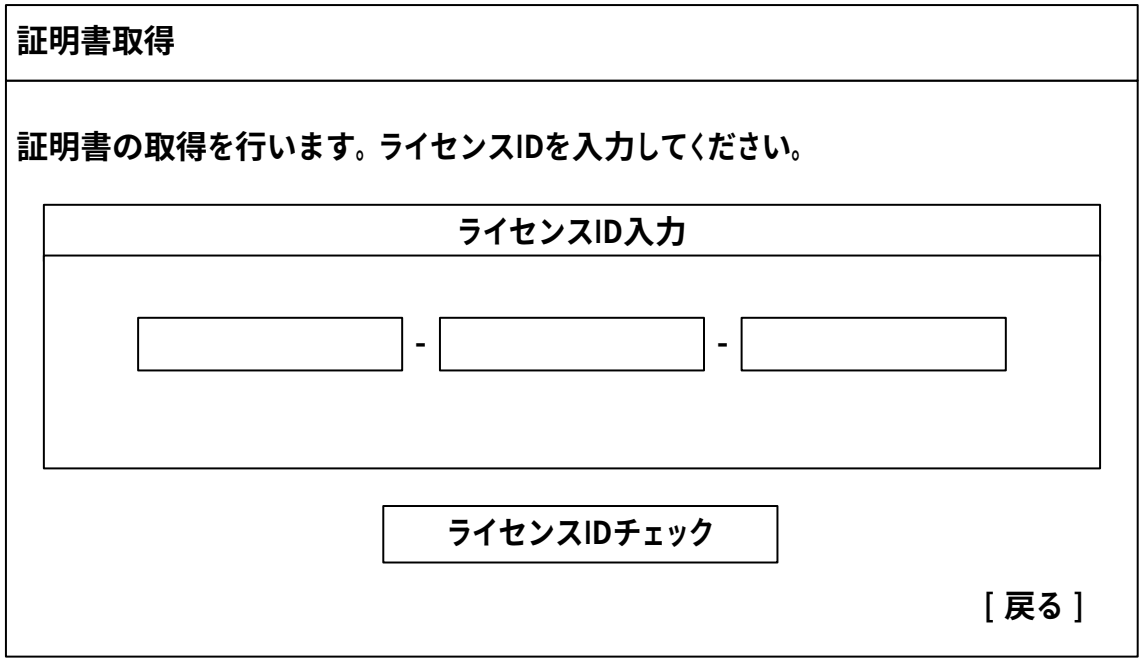
**証明書更新の申請を受け付けました。
名称：*********
EMAIL：****@xxxｘｘ.ne.jp

以下のライセンスIDをCA管理者に通知してください。
ライセンスID：******-******-******

[戻る]**

証明書更新の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、CA 管理者に申請通知のメールを送信する。ライセンス ID が申請完了画面に表示されるので、この画面を印刷するなどして、CA 管理者にライセンス ID を通知する。

（10） 証明書取得（ライセンス ID 入力）



証明書の取得を行なう。ライセンス ID を 3 つに別れているテキストフィールドに入力する。「ライセンス ID チェック」ボタンを押すことで、認証を行ない「証明書取得（鍵生成）」に遷移する。

（11） 証明書取得（鍵作成）

証明書取得

証明書の鍵ペアを生成し、証明書を取得します。HWキーを挿入してください。

メンテナー:　MNT-zxxxxxx
権限種別:　契約管理者用
認証ID:　　********

メンテナー情報確認

以下の情報で証明書を発行します。

名称:　*******
EMAIL:　****@xxxｘｘ.ne.jp**

サブジェクトDN:　C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書を取得する

[戻る]

証明書取得の確認画面を表示する。指定のライセンス ID から証明書を発行するメンテナーの情報を検索し、操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。「証明書を取得する」ボタンを証明書インストール」に遷移する。

（12） 証明書インストール

証明書インストール

証明書を発行しました。HWキーに証明書をインストールします。

メンテナー:　MNT-zxxxxxx
権限種別:　契約管理者用
認証ID:　　********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書をインストール

証明書のインストール画面を表字する。操作を行なっているメンテナーコード、認証 ID を表示する。この画面が表示される時点で、CA から証明書が発行されローカル PC にダウンロードされており、「証明書をインストール」ボタンを押すことで、証明書のインストールが行なえる。インストール後に「証明書インストール完了」に遷移する。

（13） 証明書インストール完了

証明書インストール完了

証明書のインストールが完了しました。

メンテナー:　MNT-zxxxxxx
権限種別:　契約管理者用
認証ID:　　********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

[戻る]

証明書インストールの完了を表示する。操作を行なっているメンテナーコード、認証 ID を表示する。また、発行した証明書のサブジェクトの表示も行なう。

（14） エラー表示

操作エラー

操作エラーが発生しました。エラー内容は以下のとおりです。

エラー内容

エラー番号：****
エラー内容：<ex. 指定の証明書は現在申請中です>**

[戻る]

（15） エラー一般の表示を行なう画面。エラー番号やそのエラーの内容を表示する。

5.3. まとめ

IP アドレス認証局（認証）の構築はいくつかの検討と設計を重ねた上で行われた。はじめに認証情報と証明書の関連性を調査し検討を行った。これは指定事業者に利用されている IP レジストリシステムと連動した形で IP アドレス認証局（認証）が証明書を発行するという協働型の構築である為である。認証情報と証明書の関連性の検討の次に、証明書関連業務（認証業務）を想定した業務フローを作成した。業務フローがあると認証業務に必要な、すなわちシステムが提供すべき機能が明らかになり、業務担当者の間でやり取りされる情報が明らかになる。更に認証業務に必要な機能を満たすシステム構成を検討し、仕様を決め、開発を行った。この作業と平行して認証業務規程（CPS）の更新を行った。

このように認証局の構築にはいくつかの検討が必要となるが、それらの多くは想定している認証の要件を明確にする作業であったと言える。つまり予め想定する認証の内容が明らかであったり、明らかにする為に必要な検討が少なかったりすると、比較的短期間で構築が可能であると考えられる。なお、本調査研究の一環として、前年度には認証の適用先の検討、モデルの設計、証明書アプリケーションの検討、証明書パスの検討等を既に行っていた。これらが今年度の構築の検討資料として役立った。

なお、PKI を認証に利用する場合には、証明書のフィールドの検討、証明書の失効とアカウントの無効化に関する検討、CPS への準拠性の検討および対策などの作業が必要になったことを記しておく。PKI は様々な状況を想定した仕組みを持っているが、認証システムの即時性や利便性の向上の為には更にいくつかの工夫が必要になった。