認証局運用ガイドライン

(V1.0 版)

平成 10 年 3 月

電子商取引実証推進協議会(ECOM)

認証局検討ワーキンググループ

はじめに

オープンなネットワークを介して行われる電子商取引においては、従来のフェース・ツー・フェースなどによる物理的な取引とは異なり、電子的に相手を確認し、取引の成約を可能にするためのデジタルな認証が重要な役割を果たす。
認証によって、ネットワーク上を流れる取引情報、更には組織内、組織間、個人間などを流れる広範囲な情報に対する盗聴、改竄、詐称などを排除しセキュリティを確保できるだけでなく、商取引に不可欠な信頼や信用を通有させることが可能になる。

本書は、そうしたデジタルな認証の発行等を行う認証局の運営において、拠り所となる指針を提示するものである。本書の構成は、1 章が本ガイドラインの適用対象、範囲と用語の定義、2 章が認証局運営に関わる全般的マネージメント要件、3 章が認証局の各種業務に関する要件、4 章がシステム・設備要件となっている。
本書で対象とするのは、公開鍵に対する認証であり、基本的には以下の機能やサービスの一部あるいは全てを提供する認証局についてである。なお、企業内や業界内等においてクローズされた形で運営される認証局等についても、本ガイドラインが参考になると考える。

- 認証書の発行
- 認証書の失効
- 認証書の開示
- 認証書の保管

本書は、1996 年 12 月に中間的に纏めた「認証局運用ガイドライン（アルファ版）」の不備、不足を補い、更に電子商取引実証実験プロジェクトでの経験を取り入れる事により、実行性を高める意図をもって作成されたものであるが、関連する技術の進展や国際的に標準化が図られつつある各種ガイドラインへの対応等検討が必要な点は多々残されていると考えている。
今後そのような点を取り入れ、改善を重ねる事により、真に信頼される認証局の運用のためのガイドラインとしていきたい。

本書は、平成 9 年から上記「認証局運用ガイドライン（アルファ版）」を作成後、継続して活動してきた下記グループによってまとめられたものです。
関係各位から忌憚のないご意見、ご要望を期待していますので、下記までお寄せ下さい。

電子商取引実証推進協議会(ECOM)
認証局検討ワーキンググループ/運用制度検討サブワーキンググループ(WG08/SWG1)
〒135-8073 東京都江東区青海 2-45 タイム 24 ビル 10 階
TEL：(03)5531-0065　FAX：(03)5531-0068
E-mail：yonekura@ecom.or.jp(米倉)
http://www.ecom.or.jp

目次

1. ガイドラインの利用にあたって

本ガイドラインは、公開鍵暗号システムを利用した公開鍵認証書[1]の生成・開示・更新・廃棄などの認証管理サービスを提供する認証局が、その信頼性及び安全性を確立する上で必要な要件を提示するものである。
本ガイドラインが読者として想定しているのは、認証局の運営者であり、特に、不特定多数の間で行われる電子商取引や電子決済、電子データ交換、電子メールなどで利用可能な認証書を発行する社会的影響度の大きい認証局に焦点を合わせている。

1.1. 適用対象

本ガイドラインの適用対象となる認証局は、以下の認証管理サービスの一部あるいは全てを提供する組織体である(図-1 参照)。

- 認証書の発行あるいは失効を申請する者の真正性の審査(登録局は主としてこのサービスを行う)、
- 認証書の発行・更新・失効、
- 認証書及び失効リストの配布・保管・保存(レポジトリは主としてこのサービスを行う)

本ガイドラインでは、認証局はこれら認証管理サービス全てを提供する者とし、特に断りのない限り、登録局やレポジトリ個々の要件は規定しない。従って、登録局やレポジトリ個々につ

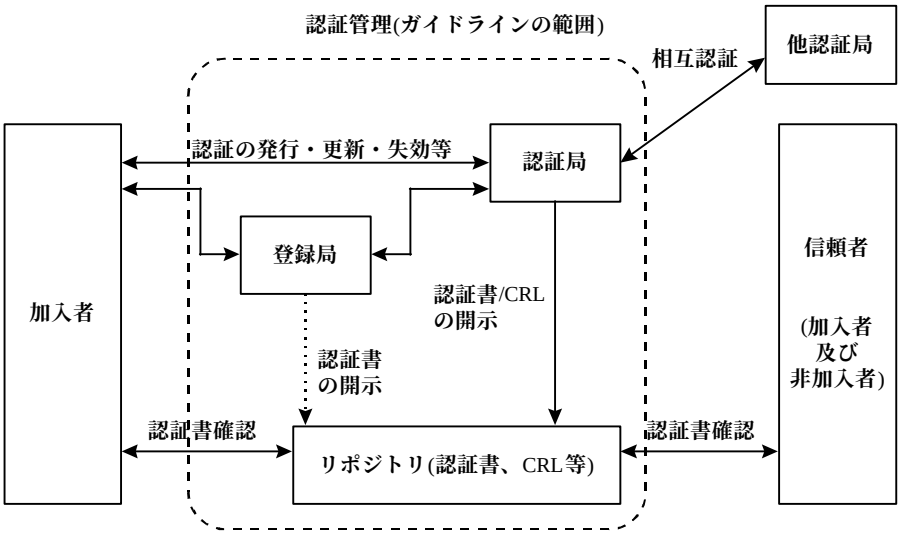


図-1 ガイドラインの対象と範囲

[1] 認証には、本ガイドラインの対象である公開鍵認証以外に、指紋や虹彩等の生体情報や手書きサイン等を利用するものもある。しかし、本ガイドラインはそれらを包括的扱うものではないため、公開鍵認証以外の分野に適用しようとする場合には十分留意されたい。

いては、対応する個所で(例えば認証局を登録局と言うように)適宜読み替えていただきたい。
なお、本ガイドラインでは以下のようなサービスについては対象外である。

- 相互認証[2]
- タイムスタンプ[3]
- 電子公証[3]
- 認証書及び失効リストのプロファイル、等

1.2. 適用範囲

認証書の利用形態は様々であり、それらの用途に応じて、認証書及びそれを管理する認証局の信頼性、安全性などのセキュリティ要件も一般に変わってくる。
そうした中で、本ガイドラインが焦点を合わせているものは、オープンなネットワーク環境下において、不特定多数の間で行われる電子商取引や電子決済、電子データ交換、電子メールなどで利用可能な認証書を発行する社会的影響度の大きい認証局である。
さらに本ガイドラインでは、上記の認証局に比べてセキュリティの確保が容易で影響範囲も限定される認証局(例えば企業内の認証局)、あるいはより高レベルなセキュリティが要求される認証局(例えば認証局に認証書を発行するような上位認証局)についても、参考的に要件を定めている(付録 A 参照)。

1.3. 本書の構成

本ガイドラインは、以下のように構成されている。
(1)マネージメント要件(2 章)
　人、物、金、情報等に関わるマネージメント面での要件を規定。
(2)運用要件(3 章)
　認証局で扱うデータ(認証局の暗号鍵、発行認証書、失効リスト、監査ログ、加入者個人情報等)について、ライフサイクルごとの要件を、機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)等の面から規定。
(3)システム・設備要件(4 章)
　「情報システム安全対策基準」に基づいて、認証局固有のものを付加した要件を規定。

1.4. 用語

1.4.1. 一般的留意事項

本ガイドラインで用いられる表現において、「.... 必要である」「.... しなければならない」という表現は、本ガイドラインで焦点を合わせている認証局にとって最小限不可欠な要件であること意味する。
また、「.... 望ましい」「.... 推奨される」という表現は、信頼性及び安全性をより高いもの

[2] 相互認証については、ECOM の「相互認証ガイドライン」を参照されたい。
[3] タイムスタンプ、電子公証については、ECOM の「電子公証システムガイドライン」を参照されたい。

にする上で望ましい要件であることを意味する。

1.4.2. 用語

1. 公開鍵暗号システム（Public Key Cryptosystem）
   関連した２つの鍵(公開鍵と秘密鍵)を使用する非対称暗号方式(asymmetric cryptographic algorithm)の一つであり、一方の鍵(公開鍵)で暗号化したデータは他方の鍵(秘密鍵)でのみ復号化できるようになっているシステム。２つの鍵は、公開鍵が与えられても、秘密鍵を導き出す事が計算上不可能な特性を持つ。
2. 公開鍵（Public Key）
   公開鍵暗号システムにおける鍵ペアのうちの一つで、通信相手等の他人に知らせて利用してもらうための鍵。
3. 秘密鍵（Private Key）
   公開鍵暗号システムにおける鍵ペアのうちの一つで、他人には知られないように秘密にしておく鍵。
4. 鍵ペア（Key Pair）
   公開鍵暗号システムにおける公開鍵及びそれに対応する秘密鍵。
5. 共通鍵（Secret Key）
   発信者と受信者が同一の暗号鍵を使用してデータの暗号化と復号化を行う対称暗号方式(symmetric cryptographic algorithm)における鍵。
6. 公開鍵基盤（Public Key Infrastructure）
   公開鍵暗号システムを用いて情報システムやコミュニケーションシステムのセキュリティを確保するための一連の技術およびサービス。
7. 認証（Certification）
   個人、法人、装置等を対象として、認証書を生成するプロセス。
8. 本人確認（Identification & Authentication）
   個人、法人､装置等の認証対象者に関する情報が真正であることを審査する行為。
9. 認証書（Certificate）
   認証対象者の識別情報と公開鍵とが対応していることを証明するデジタル文書。認証対象者の識別情報、その公開鍵、鍵の利用目的・範囲、発行認証局名などが含む一連の情報に、認証局のデジタル署名を付加したもの。従って、厳密には公開鍵認証書であるが、本書では曖昧さがない限り単に認証書という。
10. 認証書の発行（Certificate Issuance）
    認証書を生成し、認証書に登録された申請者に対し、その内容を通知する行為。
11. 認証書の失効（Certificate Revocation）
    認証書の有効期間内に、秘密鍵が危瀕した場合、あるいは氏名等の重要な属性情報に変更が生じた場合に認証書を無効にする行為。
12. 認証書の一時失効（Certificate Suspension）
    認証書の有効期間中に一時的に認証書を失効させる行為。
13. 失効リスト（Certificate Revocation List＝CRL）
    失効した認証書のリスト。通常認証局によるデジタル署名が付される。
14. 相互認証（Cross Certification）
    ２つの認証局が相互に認証するプロセス。相互認証により、異なる認証局が発行した認証書の相互流通が可能になり、利用者の認証書利用領域が拡大する。詳細は ECOM「相互認証ガイドライン」を参照されたい。
15. 認証局（Certification Authority＝CA）
    認証書の発行、開示、失効もしくは一時失効等のサービスを行なう信頼された個人または

法人。

16. 登録局（Registration Authority＝RA）
認証書の発行や失効のプロセスにおいて、本人確認などの一部機能を認証局の承認を受けて行う個人または法人。登録局は、認証書や失効リストの生成は行わない。
17. リポジトリ（Repository）
認証書や失効リスト等を保管し、認証書利用者等に対してこれらの開示や配布もしくは検索等のサービスを提供するシステム。
18. 認証書加入者（Certificate Subscriber）
認証局から認証書の発行を受けた者。本書では特に区別が必要な場合を除いて、単に「加入者」という。
19. 認証書信頼者（Relying Party）
取引等において認証書を利用する場合、認証書を受け取って、それを信頼して行動する者。加入者ばかりでなく非加入者も含まれる。本書では特に区別が必要な場合を除いて、単に「信頼者」という。
20. 認証書利用者（Certificate User）
認証書加入者及び認証書信頼者などの認証書を利用する者。本書では特に区別が必要な場合を除いて、単に「利用者」という。
21. ポリシー（Policy）
認証局のサービス・運用等に関する方針や規定、基準。
22. 認証実施規定（Certification Practice Statement＝CPS）
ポリシーに基づいて、認証の実施における手続き、遵守事項などを文書化したもの。利用者等の認証局の外部者に開示されるもの。
23. 事務取扱要領（Operation Manuals）
認証実施規定に基づいて、認証局内部における実務を詳細に規定したもの。
24. 危瀬（Compromise）
秘密鍵や関連機密情報等が、盗難や漏洩、第三者による解読等によってその機密性を失ったか、あるいはその可能性があること。
25. 複数人管理（Dual Control）
秘密情報等へのアクセス、システム運用・操作等における不正行為を防止するために、複数の人間に管理機能を分散させ、全員がそれぞれの管理機能を遂行してはじめて所定の機能が働くようにする作業方式あるいは管理方式。
26. 知識分散（Split Knowledge）
情報を複数の要素に分割し、所定の数の要素が揃わなければ元の情報の一部たりとも再現できないようにすること。
27. デジタル署名（Digital Signature）
署名対象データのハッシュ値(データを数学的な操作によって一定の長さに縮小させたもの。ハッシュ値から元のデータは再現不可能)に対して、秘密鍵で暗号化したもの。デジタル署名の検証は、デジタル署名を公開鍵で復号化した値と元のデータのハッシュ値とを照合することで可能。デジタル署名は、当該秘密鍵の保有者のみが生成できることから文字による署名と同等の効果が推定される。
28. 暗号鍵管理モジュール（Cryptographic Module）
暗号鍵等の生成、保管、利用などにおいて、セキュリティを確保する目的で使用されるソフトウエア、ファームウエア、ハードウエアあるいはそれらを組み合わせた装置。

2. マネージメント要件

認証局に求められるものは、信頼性と安全性である。それに応えるためには、所謂人、物、金、さらには情報の面での信頼性と安全性を高めるための方策が必要になる。本章では、それらのうちで、認証局全般に関わるマネージメント面の要件について述べる。

2.1. 義務

認証局には、認証の信頼性と安全性を確保するために、自らが果たすべき各種の義務と責任がある。しかし、認証局だけで信頼性と安全性が確保できるものではなく、加入者及び信頼者もまた負うべき義務がある。

2.1.1. 認証局の義務

(1)認証局自身の信頼性と安全性の確保
本ガイドラインで述べられるマネージメント要件、運用要件、システム・設備要件に適うポリシーを明確化し、それを実行するために必要な具体的手順・手続きを定めて、適切な運用を継続する義務がある。
(2)登録局やレポジトリの信頼性と安全性の確保
認証局が外部の登録局やレポジトリ等と連携する場合には、認証局はそれらの外部機関に認証局の定めたポリシーを遵守させ、信頼性と安全性の一貫性を保持する義務がある。
(3)加入者及び信頼者に対する適切な情報提供
認証局は、次に述べるような加入者及び信頼者の義務について周知させる義務がある。また、その履行に必要な各種情報を適切なタイミングで提供する義務もある。

2.1.2. 認証書加入者の義務

(1)正確な情報の提示
加入者は、認証申請などに際して、正確な情報を認証局に提示する義務がある。
(2)認証書発行の確認
加入者は、認証局による認証書発行に際して、認証書の記載情報を確認する義務がある。
(3)秘密鍵の保護
加入者は、公開鍵/秘密鍵ペアの生成において、信頼できるソフトウェアやハードウェア等を利用して安全な方法で生成するとともに、秘密鍵は他人に知られないように管理する義務がある。
(4)迅速な失効手続き
加入者は、秘密鍵が危瀕した場合や認証書記載の情報に変更が生じた場合等、迅速に失効手続きを行う義務がある。

2.1.3. 認証書信頼者の義務

(1)認証書の適格性のチェック
信頼者は、受け取った認証書が目的に適したものであるかどうかを判断する義務がある。例

えば、取引の金額的な限度は、認証の真正性保証レベルや補償レベル等に応じて決める義務がある。

(2)認証書の確認

受け取った認証書の有効期限、利用目的、署名の正当性を確認する義務がある。

(3)失効のチェック

受け取った認証書が失効していないことを確認する義務がある。

(4)認証書以外の情報の利用

取引の重要性に応じて、認証書だけに依存するのではなく他の手段も併用する必要があることを認識しておく義務がある。

2.2. 責務

(1)認証局は、認証局が果たすべき義務及び認証書を取得または利用しようとする者が果たすべき義務を定めておく必要があるとともに、双方の義務を前提とする認証局の責任と保証に関するポリシーを定め、開示する必要がある。

(2)またポリシーを開示するに際し、利用者が認証局の信頼度を評価でき、さらに利用者の履行すべき義務および認証局の履行すべき義務について利用者が容易に理解できるように、CPSを開示するだけでなく、重要な事項については概要をまとめて開示する工夫が必要である。

認証局が責任を問われる場合として例えば以下の事象が考えられ、それぞれの事象に対してポリシーに定められた認証局の規定と義務に鑑み責任と補償の内容を定める必要がある。

(a)マネージメント要件・組織規定違反

- 内部犯罪により、認証局が定めた認証実施規定に違反した行為があり、それによって利用者に損害を与えた。

(b)運用要件・認証局の鍵管理規定違反

- パスワードや秘密鍵の管理体制が不備なことによってパスワードや秘密鍵の情報が漏洩し、利用者に損害を与えた。

(c)運用要件・認証書管理規定違反

- 加入者が認証局に登録を申請した際、登録手続きを誤って不完全な認証書が発行され、利用者に損害を与えた。
- 認証局の認証書管理において、管理システムの運営ミスにより認証書発行および保管データが消失し、加入者の認証書利用が不可能となり、利用者に損害を与えた。

(d)運用要件・失効管理規定違反

- 加入者が通知してきた認証書失効通知を、失効リストに正しく登録せず、利用者が失効リストを参照したうえで有効な認証書と認識して使用したことにより、利用者に損害を与えた。

(e)運用要件・加入者情報管理規定違反

- 登録情報（各加入者のプライバシー情報等）が、内部犯罪により外部に持ち出され、不正に使用されたことによって加入者に損害を与えた。この場合は、マネージメント要件・組織規定違反にも関係するとともに、運用要件・監査規定違反にも関係してくる。

(f)システム・設備要件違反

- 認証関連システムダウンにより、認証サービスが一時的に利用不能となり、利用者が損害を被った。
- 充分な予防措置がとられずハッカー等の不法侵入者により、認証局の秘密鍵または加入者のプライバシー情報等が盗まれ、加入者が損害を被った。

- 何者かが認証局の秘密鍵を偶然または故意に解読し、利用者に損害を与えることがあり得る。このような場合は、認証局の知らない所で起こるため、監査などで発見することは困難である。暗号は技術の革新とともに、何時かは破られる可能性を常に有しており、その影響は決して小さくないとみられる。暗号技術を利用している認証局としては、技術・アルゴリズム等について、その最新動向を把握し、安全性と信頼性を絶えず高める努力が必要である。

2.3. 組織・人事管理と事務取扱要領等の規定

認証局の運用においては、技術面とともに、組織、人事、事務処理等の面からも安全性と信頼性を高めることが重要となる。

2.3.1. 独立性/第三者性

(1)認証局の安全性と信頼性を長期的に確保するためには、特定の企業・機関・組織の短期的/自己戦略的な影響からできるだけ独立しており、また第三者的に公平な立場を保持できることが望まれる。
(2)利用者の利便性を高めるために複数の認証局が相互に接続し合う場合には、異なる認証局相互の利用者の信頼を得るうえでも、できるだけ第三者性を高めることが望ましい。

2.3.2. 専門性

(1)安全性と信頼性の高い運用を持続的に行い、また技術進歩に適切かつ充分に対応していくため、さらにはトラブル等に迅速に対応するためには、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が必要である。
特に、認証サービス自体がまだ揺籃期にある現在、未知や想定外の問題が惹起する可能性が高く、そのような問題に迅速に対応していくためには専門的な知識やスキルを有する要員を確保しておくことが必要である。

2.3.3. 組織体制

認証局の運用に関わる組織の体制としては、以下が必要である。
(1) クリティカルデータに接触可能な部署は他から隔離されていること。
(2) 事故を未然に防ぐために、部署内での内部牽制が行われること。
(3) 部署外からの監査等のチェック機能が働くこと。
(4) 事故発生時に、その発生源が特定できること。

2.3.4. 人事管理

(1) 認証局の信頼確保のために信頼できる人材が運用にあたる必要がある。そのためには採用において適切な人物審査を行う必要がある。
(2) 実際の運営にあたり、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必要がある。

2.3.5. 事務取扱要領等の規定

認証局のポリシーを実務として遂行していくためには、作業項目や手続き、さらにはコンテンジェンシープラン等について、具体的作業が正確に行えるようにマニュアル等を整備し、それらが適正に実施されるようマネージメントすることが必要である。特に以下の観点から、ポリシーに準じた厳密な事務取扱要領等を規定しておく必要がある。

(1) セキュリティの対象となる場所へのアクセス
- 入退館、入退室管理
- 施錠、鍵の管理
- 監視装置等へのアクセス 等

(2) セキュリティの対象となる機器類（端末等）へのアクセス
- 端末使用権限
- カード、キー等の保管 等

(3) セキュリティの対象となる情報へのアクセス
- 情報のセキュリティレベル
- アクセス権限付与
- 媒体類の取扱い（持込み、持出しを含む）
- ドキュメント類の管理 等

2.4. 財務基盤

広範な一般消費者や法人等を対象としてサービスを提供するような認証局は、情報ネットワークにおけるインフラ的な役割を果たすようになってくる。万一こういった認証局が倒産等で存続が立ち行かなくなった場合、発行済みの認証書は有効期限までは効力を有するが、認証書の信頼性の根拠である認証書発行者の鍵管理等が危機にさらされることになる。
また、物理的に安全な設備や、認証・暗号・コンピュータ・法律の専門家や技術者の採用、高度で安全な認証システムの開発・運用や信頼性の確保等を賄うに充分な資金を有していることが重要である。

(1) 認証局は、以下の点から、十分な財務基盤を保持し運営していく必要がある。
- 認証局の責に帰される損害への賠償。
- 認証局の諸機能遂行に係る継続的な投資。

2.5. 情報開示

認証局は認証を受けようとする者、あるいは既にサービスを受けている加入者からの信頼を得るため、その判断基準となる経営情報、技術情報、運用などについて、認証局のセキュリティ維持に影響を及ぼさない範囲で、十分な情報の開示あるいは公開を行う必要がある。
また、異常時に際しても必要情報が利用者等に適切に知らされるよう、開示方式、開示タイミングなどの条件を定めておくことも必要である。例えば、開示方法としてセキュアな Web や、加入者を対象としたセキュア電子メール、郵便などが挙げられよう。

2.5.1. 経営情報

(1) 利用者が認証局の経営に対する健全性を確認できるように、財務状況を含めた経営情報の開示あるいは公開が必要である。例えば、認証局が法人の場合は、主要株主、役員、財務諸表

等の情報を開示あるいは公開する必要がある。

2.5.2. 技術情報

(1) 利用者が認証局の技術に対する安全性や信頼性を判断できるように、開示あるいは公開できる範囲での技術情報の開示あるいは公開が必要である。例えば、暗号アルゴリズム、暗号通信プロトコル等の技術情報を開示あるいは公開する必要がある。

2.5.3. 安全対策実施状況

(1) 認証局の業務運営が安全に実施されているか利用者が確認できるように、業務運営（内部不正防止対策、権限の分散、教育など）に対する定期的な監査実施結果などを開示あるいは公開する必要がある。

2.5.4. 認証実施規定

(1) 利用者が認証局を信頼性・安全性・経済性等の面から評価できるように、認証実施規定(CPS)を開示あるいは公開することが必要である。

2.6. 機密保持

利用者への十分な情報開示あるいは公開を行う一方で、認証局の安全性や信頼性に影響を及ぼすような情報に対しては、情報システムの持つ瞬時性と広域性を念頭に置いた適切な情報管理が重要である。

2.6.1. セキュリティ維持に関わる機密情報の保持

(1) 運用者の特定、運用体制、マシン室のレイアウト、監査情報、設備・システムセキュリティ等の機密にすべき情報については、その影響度を十分考慮した取り扱い方法を定め、それに従った運用が適正に行われているか適時確認することが必要である。

2.6.2. 加入者関連情報保護

(1) 加入者に関わる情報が目的外に利用されたり、不正に漏洩されたりすることがないように、機密範囲とその取り扱い方法を定め、それに従った運用が適正に行われているか適時確認することが必要である。加入者に関わる情報には、加入者が認証書申請時に提供するプライバシー情報だけでなく、認証局がその運用によって知り得た情報(例えば、どのような利用者から認証書の有効確認の問合せがあったかという情報やその頻度)なども含まれる。

2.7. 業務終了

(1)認証局が何らかの理由により、その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、その内容を加入者等直接その影響を受けるものに通知する必要がある。

3. 運用要件

認証局が行う基本的な業務として、認証書の発行･失効に対する審査、認証局の鍵管理、認証書管理、失効管理、加入者秘密情報管理、監査があげられる。
認証局が信頼性を保つためには、これらの業務運用が安全かつ確実に継続されることが必要である。

3.1. 審査

審査は、認証局あるいは登録局が認証書の発行及び失効に先立って、申請者の本人確認及び申請情報の真正性確認を行うためのものである。審査が不十分であれば、本章で述べる他の運用要件及び次章で述べるシステム･設備要件を如何に満たしていようとも、認証書の信頼性は失われてしまう。
仮に、認証局の本人確認が充分でなかった場合には、他人の名前を騙って認証書を入手することが可能となり、その人になりすまして取引ができてしまうことになるからである。従って、申請方式(オンライン・書類送付・出頭）に応じて、どのような本人確認方法を準備するかが重要になってくる。

3.1.1. 認証書の新規発行時の審査

認証書の新規発行申請に対する審査は、一般に本人確認、唯一性確認、審査結果通知、登録などの処理からなる。

3.1.1.1. 本人確認と情報の真正性確認

認証書の信頼性は､対象者の属性情報(名前や所属等)の真正性及び公開鍵が対象者に属していることの確実性に依存する。真正性確認や本人確認の方法はいろいろあるが、基本的には以下のことが必要である。

(1) 申請された情報の真正性確認のために、信頼できる機関・組織・人による証明あるいは確認済みの情報と一致していることを照査する必要がある。より高い真正性確認のために、複数の情報源の情報を利用するのが望ましい。
(2) 申請者の本人確認のために､真正性確認とは異なる手段を用いることが必要である｡例えば､審査結果等の通知に際して、申請者に通知が確実に届くような手段(例えば郵便など)を利用する必要がある。より高い信頼性を確保するためには、本人出頭が望ましい。
(3)オンライン申請以外の場合は、認証書の不正発行を防止するために、審査処理を複数人で分担して行なう必要がある。

以下にオンライン申請、書類送付申請、出頭申請のそれぞれの場合における本人確認及び真正性確認の方法を例示する。

- **オンライン申請**

  申請者が認証局に対してオンライン形態で認証書申請を行う方式である。
  例えば、カード会員等個人の認証に適した申請方法である。認証局所定の申請フォームを画面上に呼び出し、入力フィールド(申請必要項目）に以下のような情報を複数入力させて認証

局に送信する。

・生年月日
・自宅住所
・自宅電話番号
・クレジットカード番号/預金口座番号
・暗証番号(PIN)
・母親旧姓(米国の例)

等々、及びその組合わせが考えられる。本人確認は、これらの情報を信頼できる機関(クレジットカード会社、銀行等)の保有する情報、あるいは自局が保有する情報との突き合わせ、及び審査結果等を簡易書留などで申請者に郵送することによって行なわれる。

- **書類送付申請**

認証局所定の申請書式に必要事項を記載させるとともに、申請者が本人であることを証明する以下のような書類を送付させる。

・印鑑登録証明書(法人・個人)
・戸籍謄本(個人)
・商業登記簿謄本(法人)

等々、およびその組み合わせが考えられる。本人確認は、証明書等の記載事項及び捺印の確認をもって行われる。

- **出頭申請**

申請者本人が出頭しての対面による申請受付のことである。認証局所定の申請書式に必要事項を記載させるとともに、以下のような書類を提示させる。

・運転免許証
・パスポート
・健康保険証

等々、およびその組み合わせが考えられる。本人確認は、証明書等の写真および記載事項の確認をもって行なわれる。

3.1.1.2. 申請の受理と意思確認

(1) 認証申請者からの申請を認証局が受理したことを申請者に対して返答通知するとともに、併せて申請の意思確認を行う必要がある。なお、意思確認は、結果通知による事後的確認であっても構わない。

3.1.1.3. 唯一性確認

(1)被認証者名について、少なくとも当該認証書を発行する認証局配下では重複がなくユニークであることを確認する必要がある。
(2)申請者の公開鍵について、少なくとも当該認証書を発行する認証局配下では重複していないことを確認するのが望ましい。
(3)認証書に記載される公開鍵に対応する正当な秘密鍵を申請者が所持していることを確認するのが望ましい。

例えば、申請情報に秘密鍵でデジタル署名させるか、あるいはチャレンジデータ[4]にデジタル署名させて認証局に送付させる方法等によって行なう。

[4] チャレンジデータは、申請者が予め予想できないようなデータで通常は乱数を使う。

3.1.1.4. 審査情報の登録

(1)申請情報及び審査情報は、後から利用できるように登録しておく必要がある。
(2)申請時に、予め失効などの事故に対する情報など(例えば、失効申請代行者など)を登録させることが望ましい。

3.1.1.5. 審査結果の通知

(1)審査結果は、通知あるいは問合せに対する回答等によって、申請者に通知する必要がある。

3.1.2. 認証書の定期更新時の審査

(1)認証書の定期更新申請に対する審査は、新規発行時の場合と同様、本人確認、唯一性確認、意思確認、審査結果通知、登録などの処理が必要である。
(2)なお、本人確認や意思確認については、新規発行時とは異なる手段を用いて行なうことも可能である。例えば、名前などの重要な情報に変更がない場合には、申請情報に対して更新前の秘密鍵でデジタル署名させることで本人確認や意思確認を行うことも可能である。

3.1.3. 認証書の失効時の審査

認証書の失効及び一時失効の申請に対する審査は、本人確認、審査結果通知、登録などの処理からなるが、新規発行や定期更新の場合とは多少処理が異なる。
失効申請するのが誰か、また失効の理由として何が考えられるかをまとめると表-1 になる。
なお、一時失効の手続き等は基本的に正規の失効と同様である。

表-1 失効申請のパターン

申請者	失効理由(例)	申請者確認の方法(例)
本人	秘密鍵の漏洩等の危瀕	本人の署名
	秘密鍵の消失(パスワード忘れ、ファイル消去等)	新規発行と同様の手続
	重要な認証情報の変更	同上
第三者機関(登録局)	組織異動	第三者機関の署名
	不正利用	同上
認証局	認証局のミス	認証局が確認
	利用者の虚偽申請	同上

3.1.3.1. 申請者確認

失効における申請者確認は、悪意の第三者が他人の認証を失効させることがあり得るので、それを防ぐために必要である。
(1)申請者の本人確認は、秘密鍵の危瀕時などの場合には迅速に行なう必要がある。
例えば、秘密鍵の危瀕時などの場合には、申請情報にデジタル署名を付したもので受け付けるなど(この場合は、秘密鍵を不正に入手した者、あるいは正当な保持者による失効申請は実効性がある)。
(2)秘密鍵の消失、重要情報の変更の場合は、新規発行と同等の本人確認が必要である。
(3)認証書の誤りや不正使用の検知、本人による失効申請が困難な事由の発生、あるいは認証書の不正発行などの場合は、登録局や認証局あるいは事前に登録されている機関などが本人に代わって失効申請できるようになっていることが必要である。

(4)オンライン申請以外の場合は、認証書の不正な失効を防止するために、審査処理を複数人で分担して行なう必要がある。

3.1.3.2. 失効情報の登録

(1)失効リスト生成などのために使用した申請情報及び審査情報は後から利用出来る様に登録する必要がある。

3.1.3.3. 失効審査結果の通知

(1)失効審査結果は、通知あるいは問合せに対する回答等によって、申請者に通知する必要がある。

3.1.4. 失効後の認証書の再発行時の審査

失効事由によっては認証書の再発行を行なわない場合があるが、再発行する場合には以下の審査を行なう必要がある。
(1)公開鍵や重要情報の変更が伴う失効の場合、失効後の認証書の再発行は、認証書の新規発行と同様の処理が必要である。
(2)本人以外の失効申請に基づく失効の場合、失効後の認証書の再発行は、認証書の新規発行と同様の処理が必要である。

3.2. 認証局の鍵管理

認証局は、認証書や失効リストの署名、鍵の暗号化などに使用する秘密鍵／公開鍵ペア、重要な秘密情報を暗号化するための共通鍵、及び鍵生成時の秘密パラメータ等について、それらの全ライフサイクルにわたって安全で信頼性の高い管理が要求される。

3.2.1. 鍵の生成

(1)鍵ペアや共通鍵の生成は、信頼できる暗号鍵生成システムを利用して行なう必要がある。なお、暗号鍵生成システムの機能は、暗号鍵管理モジュールの内部に実装されていることが望ましい。
(2)鍵ペアや共通鍵の生成は、複数人管理のもとで行う必要がある。なお、複数人管理では、メンバーを異なる組織の権限を有する者から構成することが望ましい。

3.2.2. 鍵の保管

(1)暗号鍵生成システムによって生成された鍵は、複数の鍵構成要素に知識分散することによって単独では鍵に関する秘密情報を一切知り得ないように保管するか、あるいは暗号鍵管理モジュール内に保管する必要がある。
(2)鍵を知識分散して保管する場合には、知識分散された鍵の情報は各鍵構成要素について、権限を有する者が個別に保管する必要がある。
(3)一方、鍵を暗号鍵管理モジュール内で保管する場合には、複数人の権限を有する者が揃わなければ暗号鍵管理モジュールの持ち出し等ができないよう複数人管理のもとで保管する必要がある。

3.2.3. 鍵の利用

(1)保管されている秘密鍵や共通鍵をデジタル署名や復号に利用する際には、暗号鍵管理モジュールに入れて使用することが必要である。
鍵が知識分散されて保管されている場合には、利用の前に秘密情報を暗号鍵管理モジュールにロードする必要があるが、そのロード処理は複数人管理のもとで行うことが必要である。
(2)暗号鍵管理モジュールを認証書発行システム等に接続したり、暗号鍵管理モジュール内の鍵を利用可能状態にする操作は、複数人管理のもとで行う必要がある。
(3)暗号鍵管理モジュールが接続されたシステムを停止する場合などにおいて、暗号鍵管理モジュール内の鍵を利用可能状態から利用停止状態に切り替える処理は、複数人管理のもとで操作を行う必要がある。
(4)鍵の利用において、より高いセキュリティを確保するため、暗号鍵管理モジュールを含むシステムを必要の都度スタンドアロンで運用することが望ましい。

3.2.4. 鍵のバックアップ

(1)秘密鍵や共通鍵の偶発的な消失等によって、認証局業務の停止、さらに鍵の更新に伴う対応処理の発生などを避けるために、鍵のバックアップを行う必要がある。バックアップにおけるセキュリティ要件は、保管と同程度以上でなければならない。
(2)バックアップされた鍵は、鍵が保管あるいは利用されている場所から離れた所に保管することが望ましい。

3.2.5. 鍵の保存

(1)有効期間が終了した秘密鍵や共通鍵で、それらが有効期間後も必要になるものは(例えば、鍵暗号化鍵を復号するための秘密鍵など)、保存期間を定めて、複数人管理や知識分散による保存(archiving)を行う必要がある。
(2)認証局の公開鍵は有効期間後も可用性を確保することが必要であり、改竄されないように保存する必要がある。

3.2.6. 鍵の廃棄

(1)有効期間が終了した認証局のデジタル署名用の秘密鍵や、保存期間が終了した鍵などは、その後の不正利用が行われないように廃棄する必要がある。
(2)廃棄は、複数人管理のもとで、秘密情報の一部でも露顕したり残存させたりすることなく行われる必要がある。

3.2.7. 鍵の定期更新

(1) 認証局の鍵は、あらかじめ有効期間を設け、定期的に更新する必要がある。なお、鍵の有効期間の設定は認証局のポリシーによる。

3.2.8. 鍵の危瀕／災害時の復旧

(1)認証局は、認証局の秘密鍵が内部不正によって漏洩したり、第三者によって秘密鍵が解読された場合、さらには災害によって認証局がダメージを受けた場合などの事態に対して、事前に対応策を策定しておく必要がある。
(2)認証局の秘密鍵が危瀕した場合、あるいはその可能性がある場合、認証局は速やかに対応す

る認証書の失効を行う必要がある。
(3)認証局の秘密鍵が危瀕した場合、その秘密鍵で署名した加入者の認証書を失効させ、失効させたことを加入者に通知する必要がある。また、下記の対応を行う必要がある。
- 申請者からの認証要求を見合わせている旨の開示。
- 利用者が認証局の状況確認を行える窓口の設置。

(4)認証局の秘密鍵の危瀕／災害の事態から復旧する際には下記の対応が必要である。
- 安全な環境に復していることの確認。
- 認証局の鍵と認証書の更新。
- 加入者の認証書の再発行手続き。

(5)認証局の秘密鍵が危瀕していないかを確認するため、認証書の利用状況についてサンプリングなどの方法でモニタリングを行うことが望ましい。
(6)認証書の再発行に当っては、認証局側からの自動再発行はせず、加入者からの再発行要求があった場合にのみ行うのが望ましい。

3.2.9. 認証局の公開鍵の管理

(1)認証局は生成した鍵ペアの公開鍵に対して、上位認証局が存在する場合にはその上位認証局から認証書を取得するか、存在しない場合には自らの秘密鍵で署名した認証書を作成する必要がある。
(2)認証局の認証書は広く一般に開示もしくは公開する必要がある。

3.3. 認証書管理

認証局が認証書を作成し申請者に送付する際には、不正な生成や改竄、漏洩等が行われないようにすることが必要であり、また認証書の登録、管理に際しても、不正なアクセスが行われない様に管理する必要がある。

3.3.1. 認証書作成

(1) 認証書作成にあたっては、不正な生成が行なわれないようにする手続きを定める必要がある。特にオフラインで生成する場合には審査処理を分離するとともに、権限を有する者以外はアクセスできないシステムが必要である。

3.3.2. 認証書送付

(1)認証書送付にあたっては、セキュアな手段を講じることが必要である。
(2)認証書を送付する際、受取りの確認ができる手段を選択することが望ましい。

3.3.3. 認証書の登録・保管

(1)認証局は作成した認証書の登録・保管において、不正アクセスを防止するためにアクセス管理を行なう必要がある。
(2)登録・保管された認証書は、災害もしくは消失等に備えてバックアップをとっておくことが望ましい。

3.3.4. 認証書の開示

(1) 認証局は登録・保管された認証書の開示もしくは非開示等についてポリシーで明らかにする必要がある。開示もしくは公開する場合は、以下の様に開示先・開示方法･開示期間などについても明確にする必要がある。

- 開示先：誰に開示するかを、明確に定める必要がある。
- 開示方法：開示の方法としては、開示サービスの時間帯等と併せて、アクセス方法、開示情報フォーマット等も明確にする必要がある。
- 開示期間：認証書の開示期間は加入者への認証書発行後、その認証書の有効期限内は開示する必要がある。

3.3.5. 認証書の保存

(1)発行した認証書の有効期限が切れた後も、改竄、消去、漏洩等の不正なアクセスがなされないような対策を講じて、認証局は一定の期間認証書を保存する必要がある。

3.4. 失効管理

秘密鍵の危瀕や重要な認証情報の変更等で失効した認証書は、失効リストとして生成され保管、管理される必要があると共に、正当な利用者の問合せに適宜応じる必要がある。

3.4.1. 失効リストの生成

(1)失効リストの生成および認証局による署名は、認証書発行の場合と同等のセキュリテイ管理が必要である。

(2)失効リストの発行は１週間毎、１日毎などというように定期的に行う必要がある。当該期間中に失効がない場合でも、ないことを知らせるために失効リストを発行する必要がある。どのような周期で行うかは、利用者に明確に示しておく必要がある。

3.4.2. 失効リストの保管

(1)失効リストは、不正アクセスによる改竄、消去、漏洩等が行われない様に保管する必要がある。

(2)失効リストは災害もしくは消失等に備えバックアップを取っておく事が望ましい。

(3)失効した認証書が膨大になる場合の対応として、失効リストを分散配置したり、高度な失効管理が行える機関にその一部ないし全ての機能を行わせることも可能である。

3.4.3. 失効リストの開示

(1)失効した認証書もしくは認証書の最新ステータスは、失効リスト等によって正当な利用者が問合せ出来る様にする必要がある。

3.4.4. 失効リストの保存

(1)失効した認証書の当初の有効期限経過後も、認証局は一定の期間失効リストおよび関連するデータを保存しなければならない。

3.5. 加入者秘密情報管理

加入者が認証申請時等で認証局に提示した情報は、プライバシ侵害もしくは不正利用等の防止のために、情報のアクセス、保管、開示等について十分なセキュリティを考慮する必要がある。

3.5.1. 加入者秘密情報の定義

加入者秘密情報とは、認証書あるいは失効リストに記載される情報以外の加入者に関する情報であり、加入者のプライバシーに係る情報および利用履歴等を含む。例えば認証書の発行・更新・失効のために加入者から提示された氏名、生年月日、パスワードその他の記述又は加入者に付された番号、記号その他の符号（当該情報のみでは識別できないが、他の情報と容易に照合する事ができ、それにより当該個人を識別できるもの）が含まれる。

3.5.2. 加入者秘密情報へのアクセス権限

(1) 加入者秘密情報へのアクセスは、機密保持の為に、権限を有する者だけが行なえる様にする必要がある。

3.5.3. 加入者秘密情報の保管

(1) 加入者秘密情報は、不正に改竄・消去・漏洩等がなされないように安全に保管する仕組み、および必要に応じて取り出せる仕組みを持つことが必要である。
(2) 加入者秘密情報は、災害等により消失することのないように必要に応じてバックアップをとることが望ましい。

3.5.4. 加入者秘密情報の開示

(1) 認証局は、加入者秘密情報を開示してはならない。ただし、以下の場合はその限りではない。
- 加入者本人または本人の代理人から自己の登録情報に関して開示要求があった場合。
  ただし、認証局はあらかじめ本人であることを確認する要領を定める必要があり、その要領に従って本人確認を実施した後、開示するものとする。
- 法令の定めにより、回答が義務づけられているもの。また、法令の範囲内で本人の同意を得た場合。

3.5.5. 加入者秘密情報の保存

(1) 認証書の有効期限が切れた後も、認証局は一定の期間加入者秘密情報を保存する必要がある。
(2) また、加入者秘密情報は、不正なアクセスによる情報の改竄・消去・漏洩等が無いよう適切な手段を講じて保存する必要がある。

3.6. 監査

認証局は、要求される業務の専門性、信頼性等が十分に保たれているかを監査されなければならない。従って、監査情報の取得・管理、監査人の選定、監査頻度等を明確に規定し監査を受けると共に、監査実施結果を速やかに開示する事が求められる。

3.6.1. 監査の目的

認証局は、CPS 等に定められた基準を遵守しているか否かをマネージメント、運用、設備・システムの面から監査することにより、利用者からの信頼性の維持・確保を図るものとする。

3.6.2. 監査情報の定義

監査情報とは、認証局の CPS・技術情報・安全対策実施状況・システムイベントの記録等の監査を行うために必要な情報をいう。例えば、監査情報には以下のような情報が含まれる。

- 認証申請の情報：申請書類、申請受付担当者、本人確認手段など
- 認証局の鍵管理履歴：生成、ロード、バックアップ、保管、リカバリー、廃棄など
- 機密情報のアクセス履歴：機密データの入出力・削除、セキュリティプロファイルの変更、システムダウンと復旧処理、監査情報のアクセス、設備等の入退室など
- 受発信データ：認証局が交信したデータ、発行認証書、失効申請など

3.6.3. 監査情報の保管

(1) 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竄、消去、漏洩等に対して保護し、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。
(2) また、監査情報は適正な間隔でバックアップを取り、隔地保管することが望ましい。

3.6.4. 監査人の選定

(1) 監査人は、コンピュータ･セキュリィティに関する専門的知識を有するもので、監査対象から独立かつ客観的立場の者を選定することが望ましい。

3.6.5. 監査の頻度

(1) 監査の頻度は、最低年１度行う必要がある。しかし、以下の事態が生じた場合はこの限りではない。

- システム資源の異常な負荷増大、処理件数の異常増加、通常とは異なる時間帯や場所からのアクセスがあった場合
- CPS 等に重要な変更があった場合
- 利用者間のトラブルが多発した場合
- その他、監査が必要と判断される場合

3.6.6. 監査結果の開示と対処

(1) 監査実施後は、監査結果を速やかに開示するものとし、監査の結果として欠陥が指摘された場合には、以下の対処を行う必要がある。

- 欠陥が修正されるまでの対処(例えば、運用の停止、利用者に対する十分なアナウンス等)
- 欠陥への対処

3.6.7. 監査後の監査情報及び監査結果の保存

(1) 監査情報及び監査結果の保存は、監査後の保存期間を予め定め、不正なアクセスによる情報の変更・改竄・削除等が無いよう適切かつ合理的な安全対策を講ずる必要がある。

4. システム・設備要件

コンピュータ・システムのシステム・設備要件については、「情報システム安全対策基準」（通産省）、「不正アクセス対策基準」（通産省）が作成されており、安全対策の詳細項目については、それらの基準を参考にされたい。
認証局のシステム・設備要件としては、最低限「情報システム安全対策基準」のＢグループに準拠している必要がある。
本章では、安全対策項目の中でも特に認証局として留意すべき事項について以下に特記する。

4.1. システムの開発管理

認証局の業務システムの開発・保守においては、機密情報の漏洩防止、システムの完全性、可用性の確保のために十分な品質、セキュリティ対策を講じておくことが必要である。

4.1.1. システムの品質管理

(1)開発担当者に求められる開発経験、能力等を明らかにし、適切な人材を開発に当てることで、品質やセキュリティの低下を防ぐことが必要である。
(2)品質記録（レビューの記録、試験成績書等）を残すことにより、開発時のバグの混入を低下させる必要がる。
(3)設計、製造、試験等の開発工程において、セキュリティポリシーに従ったセキュリティ機能が作り込まれているか、確認しておくことが必要である。
(4)不正プログラムの混入防止
アクセス管理機能その他のセキュリティ機能について開発担当者による意識的な不正プログラムの混入を防ぐ為、開発終了後、該当部分についての第３者によるソースプログラムのレビュー等を実施することが望ましい。

4.1.2. 開発環境

4.1.2.1. 開発に使用するソフトウェアの管理

(1)OS、開発ツール等開発に使用するソフトウエアのバージョン/レベルやそれらの品質状況を管理することにより、バグの混入度合いを低下させ、また不正プログラムの混入を防止する必要がある。
(2)認証局の業務システムに使用するソフトウェアを外部から導入する際には、事前に評価を行ないバグや不正プログラムの混入を防止し、運用開始後の障害発生度合いを低下させる必要がある。

4.1.2.2. 開発環境へのアクセス管理

(1)開発を行うコンピュータシステムへのアクセスはID､パスワード等の個人認証機能により不正アクセスまたは不正者による不正ロジックの混入等を防止する必要がある。
(2)ソフトウェア開発環境の置かれている部屋は、入退出管理が行われ、管理責任者あるいは管理責任者が許可した者だけが入退出できる環境下にあることが望ましい。

(3)開発終了後のドキュメントやプログラムは、管理責任者あるいは管理責任者が許可した者だけがアクセスできる環境下で保管されることが望ましい。

4.1.2.3. 実運用システムの環境設定の管理

認証局業務のシステムを実運用に移行する場合のセキュリティ上重要なシステム環境設定は、誤った設定、不正な設定がされないために、権限を持った特定の者が複数人で作業を行い、相互に確認し合うことが必要である。

4.2. システムセキュリティ

システム情報の改竄、消失、漏洩等に対する保護や業務の安定的継続のためにシステムのセキュリティを確保することが必要である。

4.2.1. システム構成

(1)導入ソフトウェア全体のコピーをソフトウェアシステム構成のバックアップとして作成することが必要である。
(2)認証情報等の重要な情報を扱うシステム、構成機器については、認証業務の停止を防止するために２重化しておくことが望ましい。
(3)導入システムに関しては、常にセキュリティ上の欠陥等の情報収集に留意し、必要な措置を遅滞なく行うことが望ましい。

4.2.2. 外部ネットワークへの接続

(1)システムを外部のオープンなネットワークに接続する場合は、ファイア・ウォールの設置や重要なシステムの別ネットワーク化等の対策を講じておくことが必要である。
(2)また、ファイア・ウォールのシステム、機器についても防犯・防災対策を講じておくことが必要である。

4.2.3. システムの運用

(1)システムの操作は、不正なアクセスを防止するために権限を有する者が ID、パスワード等の個人認証機能を利用する事によってはじめて可能になる様な対策を講じる必要がある。
(2)システムの異常状態、不正運用等を早期に発見するために、システムの稼動状況をモニタリングし監視する必要がある。

4.3. 暗号鍵管理モジュール

認証書発行等に用いるデジタル署名用秘密鍵やそれに関わるパラメタ情報等の生成、保管、利用等においては、高度のセキュリティが要求される。そうした高度なセキュリティを確保する手段として、ソフトウェアやハードウェア、ファームウェア等で構成された暗号鍵管理モジュールを使用する必要がある。

4.3.1. 暗号鍵管理モジュールのセキュリティ機能

(1) 暗号鍵管理モジュールの使用にあたっては、使用する運用条件等を考慮にいれて、以下のセキュリティ機能の一部あるいは全てを組み合わせた適切な暗号鍵管理モジュールを選択する必要がある。

- 不正顕示(Tamper evident)
  不正なアクセスによる暗号鍵等内部データの漏洩、改竄及び不正使用の証拠を残す機能。
  例としては、暗号鍵管理モジュールへの不正な物理的アクセスにより施錠が解かれた場合にその証拠が残る機能や、物理的な損傷が残り、サービスへの再使用ができなくなる機能等がある。
- 不正防護(Tamper resistant)
  不正なアクセスによる暗号鍵等内部データの漏洩、改竄及び不正使用から防護する機能。
  例としては、物理的に非常に強固なカバーによる保護、電磁波や X 線による内部情報の漏洩を防止する措置、アクセス権限の確認機能等がある。
- 不正対抗(Tamper responsive)
  不正なアクセスによる暗号鍵等内部データの漏洩、改竄及び不正使用に対し対抗動作を行う機能。
  例としては、不正アクセスを検知した時点で内部データをゼロクリアする機能等がある。

4.3.2. 暗号鍵管理モジュール使用システムの機能

(1) 暗号鍵管理モジュールあるいはそれを使用するシステムの操作(例えば、初期化やデータ入出力のための操作、あるいは内部の暗号鍵を利用可能状態または利用停止状態にするための操作など)には、複数人管理を要求するメカニズムを備えている必要がある。
(2) さらに暗号鍵管理モジュールあるいはそれを使用するシステムは、そこから暗号鍵等の秘密情報を出力する場合に、秘密情報を複数要素に知識分散し、単独の要素だけでは元の情報の 1 ビットをも知り得ないようにするメカニズムを備えている必要がある。

4.4. 設備

認証局が設置される建物の立地場所、構造や敷設される電源設備、通信設備等の設備については、適切な防災及び安全対策を施す必要があるが、特に認証システムを設置する室等認証局特有のセキュリティ要件を満足する必要がある。

4.4.1. 設備の種類

一般的に設備には、建物、電源設備、通信設備、空調設備、内装設備、地震対策設備、防災設備、防犯設備、自動運転設備などがある。
具体的にこの設備を構成する機器・材料、構造を表-2 にまとめる。

表-2 設備機器・材料

#	設備	機器・材料、構造など
1	建物	構造として、柔構造（S 造[*1]）、剛構造（SRC 造[*2]、RC 造[*3]） 立地条件＊4、室のレイアウト＊5
2	電源設備	①受・変電設備　②分電盤 ③トランス　④ UPS ⑤蓄電池　⑥非常用発電機 ⑦コンセント　など
3	通信設備	① MDF/TDF/IDF　②回線（電話含む） ③同軸線　④光ケーブル　など
4	空調設備	①室内機（パッケージ等）　②室外機（クーリングタワー等） ③制御盤　など
5	内装設備	①フリーアクセスフロア　②間仕切り（パーティション）
6	地震対策設備	①床耐震材　②免振床 ③機器固定設備　など
7	防災設備	①スプリンクラー消火設備　②２酸化炭素消火設備　など
8	防犯設備	①入退出管理装置　②侵入者警報装置　など
9	自動運転設備	①自動運転監視盤　②警報盤 ③各種センサ　など

＊１：S 造（鉄骨構造：Steel Structure）
＊２：SRC 造（鉄骨・鉄筋コンクリート構造：Steel-framed Reinforced Concrete Structure）
＊３：RC 造（鉄筋コンクリート構造：Reinforced Concrete Construction）
＊４：立地条件として、火災、水害、地震あるいは電磁界、落雷、空気汚染などの被害の恐れのある場所を避けることなど。
＊５：室のレイアウトととして、室は窓や出入り口をできるだけ少なくし、操作室(オペレーション室）とサーバ設置室とは分離・独立させることなど。

4.4.2. 認証局特有の要件

(1)認証システム設置室の隔離
認証書や個人の審査情報などを扱う認証書発行システムを設置する室（認証システム設置室）は、最低限間仕切りなどで隔離し、その他の業務システムとは別の室に設置する必要がある。

(2)認証システム設置室への入退出
認証システムを設置する室への入退出は ID カードなどにより限られた要員のみに限定する必要がある。ハードウェア保守などの随時業務でこの認証システム設置室への入退出が必要な場合は、許可された要員の帯同を伴うことなどのルール作りが必要である。
さらに、入退出ログについては、ID カード等と連携したものが望ましく、ログの内容を定期的に検査し、改竄されないよう対策を講じる必要がある。

(3)認証システム設置室への不正侵入監視
認証システム設置室が無人となる場合、センサなどにより不正侵入を検知し、システム管理者などへ通知する対策を講じることが望ましい。

付録

A. 認証局のレベリング

一般的に認証局の発行する認証書は利用用途に応じて要求される信頼性が異なり、又それと対応して認証書の発行、更新、失効等の管理を行なう認証局に要求されるマネージメント要件、運用要件、システム・設備要件も異なってくる。
本ガイドラインの作成においては、認証局に要求される信頼性を３つのレベルで想定し、中レベルにおいて必要とされる要件を本文にて規定している。ここでは、低レベルと高レベルの信頼性要件を含めた規定を試みた。

A.1. 各レベルの想定モデル

①低レベル保証：企業内従業員認証、E-メール認証等認証の保証範囲が局所的もしくは決済を伴わないレベル
②中レベル保証：電子商取引における一般顧客認証等高額ではないが決済に対する保証を与えるレベル
③高レベル保証：企業間電子商取引における企業もしくは責任者認証等高額取引の契約に使用されるレベル

A.2. 各レベルの要件

項目		低レベル保証	中レベル保証	高レベル保証
マネージメント要件	責務	責任と補償の内容を定め利用者に周知する事	同左	同左
	組織・人事管理と事務取扱要領等の規定	①クリティカルデータに接触可能な部署は他から隔離されている事 ②事故を未然に防ぐために、部署内での内部牽制が行われる事 ③部署外からの監査等のチェック機能が働く事 ④事故発生時に、その発生源が特定できる事	同左	同左
	財務基盤	―	以下の財務基盤を保持し運営する事 ①認証局の責に帰される損害への賠償 ②認証局の諸機能遂行に係る継続的な投資	同左

項目			低レベル保証	中レベル保証	高レベル保証
	情報開示		－	以下の情報を開示する事 ①経営情報 ②技術情報 ③安全対策実施状況 ④認証実施規定(CPS)	同左
	機密保持		①セキュリティ維持に関わる機密情報を保持する事 ②加入者関連情報を保護する事	同左	同左
	業務終了		業務終了を加入者等に通知する事	同左	同左
審査	認証書新規発行時の審査	本人確認と情報の真正性確認	申請された情報は信頼出来る機関､組織もしくは人による証明もしくは確認済みの情報と一致している事を照査する事	左記に加え、 ①例えば審査結果の通知を申請時の手段とは別の方法で行なう等、より本人確認の信頼性を高める事 ②オンライン申請以外の場合には、審査処理を複数人で分担する事	左記に加え､本人出頭による確認を行なう事
		申請の受理と意思確認	－	認証申請を受理した事を申請者に回答すると共に、申請の意思確認を行なう事	同左
		唯一性確認	被認証者名が当該認証局配下で重複がなくユニークである事を確認する事	同左	左記に加え、 ①申請者の公開鍵が当該認証局配下で重複していない事を確認する事 ②認証書に記載される公開鍵に対応する正当な秘密鍵を申請者が所持している事を確認する事
		審査情報の登録	申請情報及び審査情報を登録する事	同左	左記に加え､申請時に失効等の事故への対処に関する情報を登録する事
		審査結果の通知	－	通知あるいは問合せに対する回答等によって申請者に通知する事	同左
	認証書定期更新時の審査		新規発行時の審査と同等に行なう事、但し本人確認､意思確認は新規発行時とは異なる手段を用いて行なう事も可能	同左	同左

項目			低レベル保証	中レベル保証	高レベル保証
	認証書失効時の審査	申請者確認	秘密鍵の危瀬時には本人確認を迅速に行なう事	左記に加えて、 ①秘密鍵の消失、重要情報の変更の場合は新規発行時と同等の本人確認を行なう事 ②認証書の誤りや不正使用の検知、本人による申請が困難な事由の発生、あるいは認証書の不正発行等の場合は、登録局や認証局あるいは事前に登録されている機関等が本人に代わって申請出来る様にしておく事 ③オンライン申請以外の場合には、審査処理を複数人で分担する事	同左
		失効情報の登録	失効リスト生成のための申請情報､審査情報を登録する事	同左	同左
		失効審査結果の通知	―	通知あるいは問合せに対する回答等によって申請者に通知する事	同左
	失効後の認証書再発行時の審査		①公開鍵や重要情報の変更による失効後の認証書再発行に対しては、新規発行時と同等の処理を行なう事 ②本人以外の失効申請に基づき失効した後の認証書再発行に対しては、新規発行と同等の処理を行なう事	同左	同左
認証局の鍵管理	生成		鍵ペアや共通鍵の生成は信頼できる暗号鍵生成システムを使用して行なう事	鍵ペアや共通鍵の生成は信頼できる暗号鍵生成システムを使用して複数人管理の基で行なう事	①暗号鍵生成システムの機能は暗号鍵管理モジュールの内部に実装されている事 ②鍵生成の際の複数人管理ではメンバーを異なる組織の権限を有する者から構成する事

項目		低レベル保証	中レベル保証	高レベル保証
	保管	暗号鍵生成システムによって生成された鍵は暗号化し保管する事	①複数の鍵構成要素に知識分散する事によって単独では鍵に関する秘密情報を一切知り得ない様に保管するか 又は 暗号鍵管理モジュールに保管する事 ②複数の鍵構成要素に知識分散する場合には、各構成要素は権限を有する者が個別に保管する事 ③暗号鍵管理モジュール内で保管する場合には、複数人の権限を有する者が揃わなければ暗号鍵管理モジュールが持ち出せないなど複数人管理の基で保管する事	①鍵の保管は暗号鍵管理モジュール内から取り出さずに行なう事 ②暗号鍵管理モジュールの管理は、異なる組織のメンバーによる複数人管理の基で行なう事
	利用	―	①利用する際には暗号鍵管理モジュール内で使用する事 ②暗号鍵管理モジュールを利用もしくは停止する場合等の操作は複数人管理の基で行なう事	①左記の複数人管理のメンバーは異なる組織から構成されている事 ②暗号鍵管理モジュールを含むシステムはスタンドアロンで運用する事
	バックアップ	―	①秘密鍵や共通鍵はバックアップを行なう事 ②バックアップに際しては保管と同程度以上のセキュリティを確保する事	左記に加え、鍵の利用場所と離れた所にバックアップする事
	保存	①有効期間が終了した秘密鍵や共通鍵の内、有効期間後も必要なものは、保存期間を定め保存する事 ②認証局の公開鍵は有効期間後も可用性を確保するために改竄されない様に保存する事	左記に加え、有効期間が終了した秘密鍵や共通鍵の内、有効期間後も必要なものは、保存に際し複数人管理や知識分散の基で行なう事	同左
	廃棄	有効期間が終了した認証局のデジタル署名用の秘密鍵や保存期間が終了した鍵等は廃棄する事	左記に加え、廃棄に際しては複数人管理の基で秘密情報の一部でも露見したり残存させたりしない事	同左
	定期更新	予め有効期限を設け、定期的に更新する事	同左	同左

項目		低レベル保証	中レベル保証	高レベル保証
認証局の鍵管理	鍵の危瀬/災害時の復旧	①秘密鍵の危瀬もしくは災害によるダメージ等の事態に備え、対応策を事前に作成しておく事 ②秘密鍵が危瀬したもしくはその可能性がある場合、認証局は速やかに対応する認証書の失効を行なう事	左記に加え、 ①秘密鍵が危瀬した場合、その秘密鍵で署名した加入者の認証書を失効させ、それを加入者に通知し以下の対応を行なう ・申請者からの認証要求を見合わせている旨の開示 ・利用者が認証局の状況確認を行なえる窓口の設置 ②認証局の秘密鍵の危瀬もしくは災害の事態から復旧する際には下記の対応を行なう事 ・安全な環境に復している事の確認 ・認証局の鍵と認証書の更新 ・加入者の認証書の再発行手続き	左記に加え ①認証局の秘密鍵が危瀬していないかを確認するため認証書の利用状況についてサンプリングなどの方法でモニタリングを行なう事 ②加入者への認証書の再発行に際しては、自動発行ではなく加入者からの要求で行なう事
	公開鍵	①認証局は生成した鍵ペアの公開鍵に対して上位認証局が存在する場合はそこから認証書を取得するか、または上位認証局が存在しない場合は自らの秘密鍵で署名した認証書を作成する事 ②認証局の認証書は広く一般に開示もしくは公開する事	同左	同左
認証書管理	作成	―	オフラインで生成する場合には審査処理を分離すると共に権限を有する者以外はアクセス出来ないシステムである事	同左
	送付	―	認証書の送付にはセキュアな手段を講じる事	左記に加え、受け取りの確認が出来る手段を選択する事
	登録・保管	―	認証書の登録・保管において不正アクセスを防止するためにアクセス管理を行なう事	左記に加え、災害もしくは消失に備えバックアップを取って置く事

項目		低レベル保証	中レベル保証	高レベル保証
	開示	―	①登録・保管された認証書の開示もしくは非開示等についてポリシーで明らかにする事 ②開示もしくは公開する場合には、下記について明確にする事 ・開示先：誰に開示するかを明確にする事 ・開示方法：開示サービス時間帯と併せアクセス方法、開示情報フォーマット等も明確にする事 ・開示期間：加入者への認証書発行後その有効期限内は開示する事	同左
	保存	―	発行した認証書の有効期限が切れた後も改竄、消去、漏洩等に対する保護を講じて一定期間保存する事	同左
失効管理	失効リストの生成	失効リストの生成及び署名は､認証書発行と同等なセキュリテイ管理を行なう事	失効リストの発行は失効の発生の有無に関わらず定期的に行なう事、又発行サイクルについては利用者に明確にする事	同左
	失効リストの保管	―	失効リストは不正アクセスによる改竄、消去、漏洩等に対する保護を行なう事	左記に加え､災害もしくは消失に備えバックアップを取って置く事
	失効リストの開示	―	失効した認証書もしくは認証書の最新ステータスは失効リスト等によって正当な利用者が問合せ出来る様にする事	同左
	失効リストの保存	―	失効した認証書の当初の有効期限経過後も一定の期間失効リスト及び関連データを保存する事	同左
加入者秘密情報管理	加入者秘密情報へのアクセス権限	加入者秘密情報へのアクセスは権限を有する者だけが行なえる様にする事	同左	同左
	加入者秘密情報の保管	―	不正な改竄、消去、漏洩等に対する保護を行なう事	左記に加えて､利用者秘密情報は災害等により消失する事がない様に必要に応じてバックアップを取る事

項目		低レベル保証	中レベル保証	高レベル保証
	加入者秘密情報の開示	－	下記を除き加入者秘密情報を開示してはならない ・加入者本人又は代理人から自己の登録情報について要求があった場合、但し本人もしくは代理人である事を確認する規定を事前に定めそれに基づいて本人確認を行なった後に開示する事 ・法令の定めにより回答が事務付けられているもの、又法令の範囲内で本人の同意を得た場合	同左
	加入者秘密情報の保存	－	①認証書の有効期限が切れた後も一定期間保存する事 ②不正なアクセスによる改竄、消去、漏洩等に対する保護を行なう事	同左
監査	監査情報の保管	－	監査情報はアクセス権限を明確にし、改竄、削除等に対する保護を行なう事	左記に加え、重要な情報はバックアップを取る事
	監査人の選定	－	コンピュータセキュリテイに関する専門知識を有する者で監査対象から独立かつ客観的立場にある者を選定する事	監査人は複数人を選定する事
	監査の頻度	－	監査は、下記事態発生の場合を除き、年最低１度行なう事 ・システム資源の異常な負荷増大、処理件数の異常増加、通常とは異なる時間帯や場所からアクセスが発生した場合 ・CPS 等に重要な変更が生じた場合 ・利用者間のトラブルが多発した場合 ・その他監査が必要と判断される場合	監査は左記事態発生の場合を除き、年最低２度行なう事

項目		低レベル保証	中レベル保証	高レベル保証
	監査結果の開示と対処	―	①監査実施後は結果を速やかに開示あるいは公開する事 ②監査結果に欠陥がある場合は下記の対処をする事 ・欠陥が修正される迄運用の停止、利入者への通知等の対処 ・欠陥への速やかな対処	同左
	監査後の監査情報及び監査結果の保存	―	監査実施後の監査情報及び監査結果の保存は、期間を定め改竄、削除、変更等に対する保護を講じる事	同左
システム開発管理	品質管理	―	①開発担当者に求められる経験、能力等を明らかにし適切な人材を開発に当てる事 ②品質記録を残すことにより開発時のバグ混入を低下させる事 ③設計、製造、試験等の開発工程においてセキュリテイポリシーに従ったセキュリテイ機能が作り込まれているか確認する事	左記に加え、開発担当者による意識的な不正プログラムの混入をレビュー等によって防止する事
	開発に使用するソフトウエアの管理	―	① OS, 開発ツール等開発に使用するソフトウエアはバージョン/レベルやそれらの品質状況を管理する事によりバグの混入度の低下及び不正プログラムの混入を防止する事 ②認証局の業務システムに使用するソフトウエアを外部から導入する際には事前に評価を行ないバグや不正プログラムの混入を防止する事	同左

項目		低レベル保証	中レベル保証	高レベル保証
	開発環境へのアクセス管理	―	開発を行なうコンピュータシステムへのアクセスはID、パスワード等の個人認証機能により不正アクセス及び不正者による不正ロジックの混入等を防止する事	左記に加え、 ①ソフトウエア開発環境が置かれている部屋は入退室管理が行われ、管理責任者あるいは管理責任者が許可した者だけが入退室可能な事 ②開発終了後のドキュメントやプログラムは管理責任者あるいは管理責任者が許可した者だけがアクセス出来る環境下で保管される事
	実運用システムの環境設定の管理	―	認証局業務システムを実運用に移行する場合のシステム環境設定は、誤った設定、不正な設定が行なわれないために権限を持った特定の者が複数人で作業を行ない相互に確認しあう事	同左
システムセキュリテイ	システム構成	―	導入ソフトウエア全体のコピーをソフトウエア構成のバックアップとして作成する事	左記に加え、 ①認証情報等の重要情報を扱うシステム、構成機器については業務の停止を防止するために２重化する事 ②導入システムに関しては常にセキュリテイ上の欠陥等の情報を収集し必要な措置を講じる事
	外部ネットワークへの接続	―	①システムを外部のオープンなネットワークに接続する場合はファイアウオールの設置や重要なシステムの別ネットワーク化等の対策を講じる事 ②ファイアウオールのシステム、機器についても防犯、防災対策を講じる事	同左

項目		低レベル保証	中レベル保証	高レベル保証
	システムの運用	－	①システムの操作は権限を有する者だけが行なえ且つ ID、パスワード等の個人認証機能を利用する事により不正な操作を防止する事 ②システムの稼動状況をモニタリングし異常状態、不正運用等を監視する事	同左
暗号鍵管理モジュール	暗号鍵管理モジュールのセキュリティ機能	－	運用条件等を考慮して適切な機能を有する暗号鍵管理モジュールを選択する事	同左
	暗号鍵管理モジュール使用システムの機能	－	①暗号鍵管理モジュールあるいはそれを使用するシステムの操作には複数人管理を要求するメカニズムを備えている事 ②暗号鍵管理モジュールあるいはそれを使用するシステムはそこから暗号鍵等の秘密情報を出力する場合、秘密情報を複数要素に知識分散し単独の要素だけでは元の１ビットをも知り得ない様にするメカニズメを備えている事	同左
建物・設備	建物立地場所	コンピュータ室は火災、電磁界の被害を受ける恐れの少ない場所に設ける事	コンピュータ室は、火災、電磁界、漏水、水害等の水による被害を受ける恐れの少ない場所に設ける事	建物、コンピュータ室は、火災、電磁界、水害、落雷、空気汚染による被害を受ける恐れの少ない場所に設ける事
	建物の構造	建物は、耐火構造、耐震構造とする事	同左	同左
	建物入退出管理	①窓、扉には防犯措置を講ずる事 ②入退出記録をとり、管理する事	左記に加え、入退出に関する管理規定を整備し、管理責任者を決める事	入退出者に関する資格審査を行い、識別証により入退出を管理する事
	認証システム設置室	－	他業務システムとは分離する事	操作室、サーバ室等を分離する事
	認証システム設置室への入退出管理	①物理錠による施錠･解錠を行う事 ②入退出に関する管理規定を整備し、管理責任者を決める事	① ID カード等による施錠・解錠を行う事 ②同左	①生体認証装置による施錠・解錠を行う事 ②同左 ③センサ等により不正侵入を検知し、システム管理者に通知出来る事

	項目	低レベル保証	中レベル保証	高レベル保証
	認証システム設置室の入退出ログ管理	入退出記録をとり、管理する事	①入退出ログは改竄されないよう対策を講じる事 ②ログの内容は定期的に検査する事	①同左 ②左記に加え、定期的に入退出の監査を行なう事
	設備保守方法	保守方法の明文化と設備毎の作業員を特定を行う事	設備保守要員には当該セキュリティ権限を有する要員の帯同を行う事	同左
	電源設備	避雷措置、防火、耐火措置等の防災措置及び防犯措置を講ずる事	①電圧、周波数等の安定した電力を供給できる措置を講じておく事 ②電源系統の２系統化、蓄電池の併用等による停電対策を講じる事	災害時等の継続的停電の対策として、自家発電設備を設置する事
	空調設備	防火、耐火、漏水対策等の防災措置及び防犯措置を講ずる事	適切な室内空調を安定して提供できる事	同左

B. 公開鍵基盤の概要

公開鍵基盤(PKI：Public Key Infrastructure)は、電子商取引をはじめとして、情報処理システムのセキュリティやコミュニケーションシステムの信頼性を確保する上で必要となる様々なサービスのインフラストラクチャーとなるものである。
本書でいう認証書は、少なくとも利用者の名前と公開鍵(ビット列)を情報として含むデジタル文書で、認証局のデジタル署名を付したものを言う。従って認証をより正確に表現するならば公開鍵認証ということになる。
以下では PKI を構成するサービスについて概観する。

B.1. 暗号サービス

PKI で利用される基本的な機能・技術として以下のものがある。
(1)鍵ペアの生成・保管：公開鍵/秘密鍵のペアを生成するとともに、秘密鍵はパスワード等で保護されたファイルや IC カード等のハードウェア/ソフトウェアのモジュールに保存して他人に知られないように保管する機能。なお、鍵の用途として主に以下のものが挙げられる。
・デジタル署名
・通信データ秘匿用共通鍵の暗号化
・否認防止など。
(2)デジタル署名の生成：メッセージダイジェストを生成し、デジタル署名する機能。
(3)デジタル署名の検証：メッセージとそれに対するデジタル署名が署名者のものであるかどうかを検証する機能。
(4)通信データ秘匿用共通鍵の生成･配布：通信文を暗号化するための共通鍵を生成し、それを相手に配布するための機能。

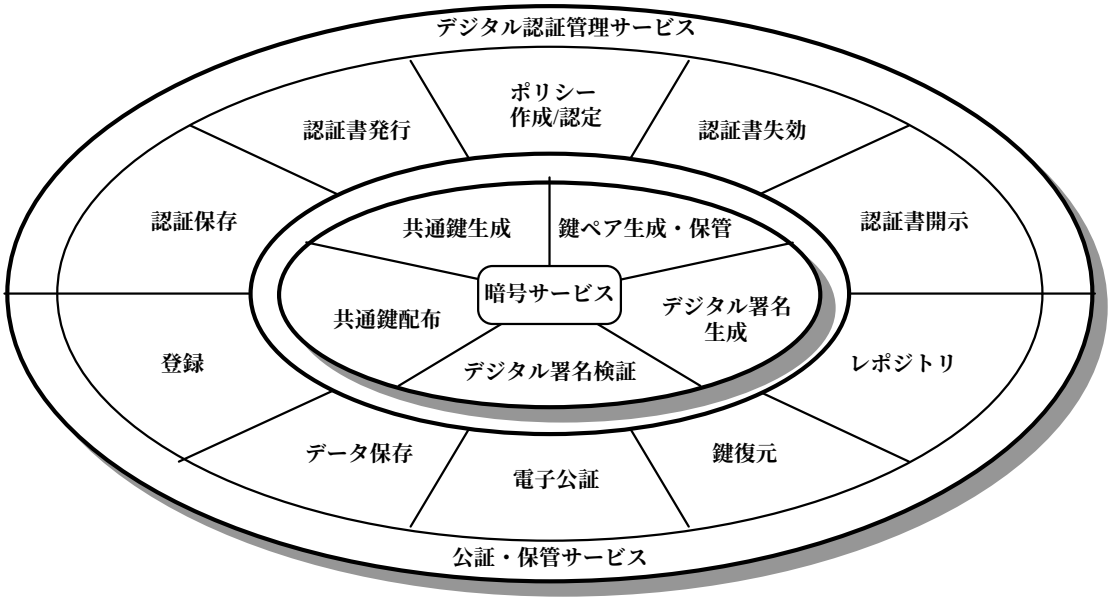


図 B-1公開鍵基盤の構成

B.2. 認証書管理サービス

PKI の中で核となる認証書の管理に関する以下のサービスであり、主として認証局によって提供されるものである。

(1)認証書の発行(Certificate Issuance)：
個人や法人等の加入者に対して認証書を発行する。発行する認証書には、階層構造の下位に位置する下位認証局(subordinate CA)、相互認証における相手の認証局等に対するものも含まれる。

(2)認証書の失効(Certificate Revocation)：
被認証者は、認証書に含まれる公開鍵と対になった秘密鍵をなくしたり、盗まれたり、あるいは解読されたりした場合、またはその可能性がある場合には、その認証書を無効にする必要がある。認証局は被認証者の確認を取った上で、認証書失効リスト(Certificate Revocation List: 失効リスト)等によって、失効情報を利用者等の関係者に知らせる。
失効の一種に一時失効(Certificate Suspension)がある。これは、ある期間だけ失効させるものであり、一時失効の期間が過ぎれば、通常自動的に失効は解除される。一時失効は、漏洩等の可能性がある場合や、不在の場合等に利用される。

(3)認証書の開示(Certificate Publish)：
発行済みの認証書を他の人が入手できるようにするため、レポジトリ(X.500 仕様のものやそれ以外のレポジトリなど)に登録する 。レポジトリは認証局が管理する場合もあるし、認証局以外の第三者が管理する場合もある。
なお、そのようなレポジトリとしては種々のアクセス制限の機能が用意され、プライバシーを守りたい場合には不特定多数に公開しないようになっているものもある。

(4)認証書の保存(Certificate Archiving)：
発行済みの認証書や失効リスト等を長期にわたって保管する。これは、デジタル署名した文書自体が認証書の有効期限を超えて存在するため、それに対応させて有効期限が過ぎた認証書を、長期間保管しておく必要があるからである。

(5)ポリシーの作成/認定(Policy Creation/Approval)：
認証業務の実施に際して必要となる各種のポリシー(Policy)を定める。ポリシーには、認証局の運用に関わる要員、設備、各種手続き等を明確化した運用ポリシー、及び利用者や他の認証局等に対して認証を発行する際の審査基準等を定めた発行ポリシー等がある。

B.3. 関連サービス

前記の認証書管理サービスに加えて、以下のような各種の関連サービスも PKI の構成要素として考えられる。これらのサービスは、認証局が付加サービスとして提供することもあるし、別の機関が提供することもある。

(1)登録((Registration)：
個人情報等を登録・管理し、認証書の発行や失効に必要な本人確認を認証局に代わって行うサービス。実際の認証書発行等は認証局が行う。

(2)データ保管(Data Archiving)：
デジタル文書等のデータを長期間にわたって保管･管理するサービス。書き換え不可能な媒体等に保管することで改竄等を防ぐとともに、媒体の陳腐化によるアクセス不能等が起こらないように適宜バックアップや保管媒体の更新等が行われる。

(3)電子公証(Notary)：
デジタル文書の公証を行うサービス。

(4)鍵復元(Key Recovery)[5]：
鍵を無くしたり、あるいは鍵をアクセスするためのパスワードを忘れたりした場合に備えて、あらかじめ鍵の複製を預かっておき、利用者等の要請に応じて鍵の復元を行うサービス。鍵は公開鍵方式の秘密鍵の場合もあるし、共通鍵方式の鍵の場合もある。
(5)レポジトリ(Repository)：
個人等の属性情報を総合的に管理・提供するサービス。属性情報には、認証書ばかりでなく、電話番号、E メールアドレス等の情報が含まれる。
(6)その他：
鍵の保管を IC カード等のハードウェアトークンで行うような場合、鍵の生成、IC カードへの書き込みを行うサービス等のいろいろなサービスが想定される。

B.4. 認証アーキテクチャー

B.4.1. 構造と加入者

PKI における認証は、一般的に、階層構造を基本にしており、以下のような加入者から構成される。
(1)ポリシー承認局(PAA：Policy Approval Authority)
- PAA は階層構造の配下にある PCA のポリシーについて基準を定め、配下の PCA のポリシーの承認を行い、それらに認証書を発行する。PAA は PCA に対してのみ認証書の発行を行う。
- PAA は自分の公開鍵に対して自分の秘密鍵でデジタル署名した認証書(ルート認証書)を発行する。有効期限は、一般に PCA や CA のものより長い。
- ルート認証書及び PCA 等に対する認証書の発行は、原則的にオフラインで行われる。

(2)ポリシー認証局(PCA：Policy Certification Authority)
- PCA は階層構造の配下の CA のポリシーを定め、CA がポリシーを遵守した運営を行っているかどうかをチェックする。
- PCA は直下の CA に対して認証書を発行するが、基本的には直接加入者に認証書を発行しない。CA に対する認証書の発行は、原則的にオフラインで行う。
- PCA があることで、複数の CA に認証書発行を分散することができ、万が一 CA の鍵が被害を受けた場合の影響を軽減できる。
- PCA の認証書の有効期限を CA の認証書に比べて長くすることで、CA の認証書の更新を円滑に行うことが可能になる。

(3)認証局(CA：Certification Authority)
- CA は PCA の定めたポリシーに準拠して、下位 CA、加入者及び RA に対して認証書を発行する。
- CA は PCA のポリシーに準拠して自所個別のポリシーを定める場合と、自所個別のポリシーは定めず PCA の定めたポリシーと同じにする場合がある。後者の場合は、一般的な意味での CA と区別するために発行局(IA：Issuance Authority)と言うこともある。

(4)登録局(RA：Registration Authority)
- RA は、離れた場所にいる加入者などのために、CA への登録手続きを代行する。但し、認証書の発行は行わない。
- 登録に際しては、CA のポリシーに準拠した手続きに従い本人確認などを行う。
- RA は、LRA(Local RA)とか ORA(Organizational RA)とも呼ばれる。

[5] ISO/IEC における TTP(Trusted Third Party)のガイドライン等、国際的議論を踏まえた検討を別途行う必要がある。

(5)加入者(End Entity)

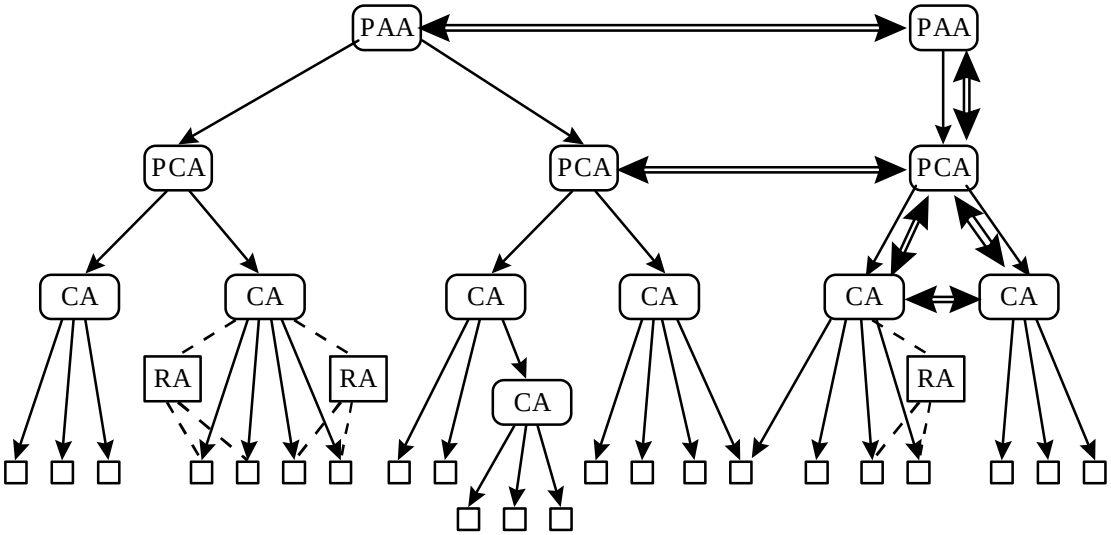
- 加入者は、認証局から認証書の発行を受けた個人、法人、サーバなどを指す。

B.4.2. 認証局のマネージメントドメイン

広義な意味での一般的な認証局は、電子メール用認証書や決済用認証書などの複数レベルの認証書を発行するものと考えられる。この場合、認証局は電子メール用認証書のポリシーを定める PCA や決済用認証書のポリシーを定める PCA 等の機能も有することになる。さらに、それらの PCA を束ねる PAA の機能を有することも考えられる。
従って、認証局がカバーする範囲(認証局のマネージメントドメインと呼ぶ)に対して、そのドメイン内におけるポリシーの統一性や整合性を保つことが求められる。また、他ドメインの認証局との間における相互認証に際しては、CA、加入者等に対する命名規約やポリシー等の整合性を確保する必要があり、そのために予め、他ドメインのものともすりあわせ可能なように配慮しておくことも必要になる。

B.4.3. 相互認証

相互認証は、認証局同士がお互いに認証書を発行し合うものであり、上記のような階層構造においては、PAA 同士あるいは PCA 同士の間、さらには CA 同士あるいは CA と PCA といった様々な組合せが考えられる。しかし、いずれの場合でも相互認証し合うもの同士の間では、ポリシーの整合性が必要になる。



PAA：Policy Approval Authority(ポリシー承認局)
PCA：Policy Certification Authority(ポリシー認証局)
CA ：Certification Authority(認証局)
RA ：Registration Authority(登録局)
□ ：End Entity(加入者)
⟷：相互認証

図 B-2認証のアーキテクチャー

B.5. 認証書

B.5.1. 認証書フォーマット[6]

認証書(Certificate)は、下表に示す項目からなる情報に対してデジタル署名したものである[7]。なお、バージョン１で定められた項目は必須[8]であるが、それ以外のバージョンで定められた項目はオプションである。

Version	項目	説明
V-1	version	バージョン(0 は V-1、2 は V-３を示す)
	serialNumber	認証番号
	signature.algorithmIdentifier algorithm parameters	署名方式
	issuer	認証発行局名(Distinguished Name 形式[9]) ● 国名(country) ● 地域(locality) ● 組織(organization) ● 所属(organizationalUnit) ● 名前(commonName)
	validity notBefore notAfter	有効期限 ● 開始日時 ● 終了日時
	subject	被認証者名(Distinguished Name 形式)
	subjectPublicKeyInfo algorithm subjectPublicKey	被認証者の公開鍵情報 ● 鍵のアルゴリズム ● 鍵(ビット列)
V-2	issuerUniqueID	認証発行局の固有 ID
	subjectUniqueID	被認証者の固有 ID

[6] 出所：ITU Rec. X.509 | ISO/IEC 9594-8　Final draft(1996.6.30)。
[7] これらの項目全体に対するデジタル署名が authrityKeyIdentifier で定義された鍵で行われる。
[8] 被認証者名(Subject)は、従来はグローバルにユニークであることが必要な必須項目であったが、V-3 からオプションになった。
[9] Distinguished Name 形式は、国名、地域、名前等の組合せて、一つのユニークな識別名を作るものであり、識別名の重複は認められない。

Version	項目	説明
V-3	authorityKeyIdentifier keyIdentifier authorityCertIssuer authorityCertSerialNumber	当該認証の署名確認に用いるべき鍵(認証)の識別子 ●鍵識別子(8 進数) ●認証発行局名(GN 形式[10]) ●認証番号
	subjectKeyIdentifier	被認証者が複数の鍵を持つ場合の識別子(鍵の更新時などに利用)
	keyUsage (0) digitalSignature (1) nonRepudiation (2) keyEncipherment (3) dataEncipherment (4) keyAgreement (5) keyCertSign (6) cRLSign	公開鍵の利用目的(ビット列) (0) デジタル署名用 (1) 否認防止用 (2) 鍵の暗号用 (3) 電文の暗号用 (4) 共通鍵の配布用 (5) 認証の署名確認用 (6) 失効リストの署名確認用
	privateKeyUsagePeriod	当該認証の公開鍵に対応する秘密鍵の有効期限。通常公開鍵の有効期限より短い。署名用の鍵だけが対象。
	certifficatePolicies policyIdentifier policyQualifiers	認証発行局のポリシー(以下の複数組合せ) ● ポリシーID(ISO/IEC9834-1 に準拠) ● 認証基準
	policyMappings issuerDomainPolicy subjectDomainPolicy	CA 認証の場合のみ。発行認証局のポリシーと被認証 CA のポリシーのどれとどれが同一かを規定。
	supportedAlgorithms algorithmIdentifier intendedUsage intendedCertificatePolicies	ディレクトリ(X.500)のアトリビュートを定義。コミュニケーションの相手がディレクトリ情報を利用する場合に、事前にそのアトリビュートを知らせるため。
	subjectAltName otherName rfc822Name dNSName x400Address directoryName ediPartyName uniformResourceIdentifier iPAddress registeredID	被認証者の別名(GN 形式)。任意のものを選択。 ● 任意の名前 ● e-mail アドレス ● ドメイン名 ● O/R アドレス(X.400 originator/recipient address) ● ディレクトリ名 ● EDI 用の名前 ● WWW 用の URL ● IP アドレス ● 登録済みオブジェクトの ID(ISO/IEC9834)
	issuerAltName	認証発行局の別名(上記と同様)
	subjectDirectoryAttributes	被認証者の任意の属性。例えば、郵送先、電話番号、顔写真(イメージデータ)等の情報。

[10] GN(General Name)形式は、subjectAltNames の項で利用されているように、一つの加入者に対して複数の識別情報を与えるもの。Distinguished Name 形式と異なりユニーク性は要求されない。

Version	項目	説明
V-3	basicConstraints cA pathLenConstraint	当該公開鍵が、認証局の署名用か加入者(認証を発行できない)のものかの区別。 ● 認証局か加入者の区別 ● 下位に来る認証局のパスの長さの制限(0 の場合は、加入者の認証のみ)
	nameConstraints permittedSubtrees base minimum maximum excludedSubtree	被認証者が認証局である場合(CA 認証)にのみ使用。 上記の basicConstraint で括ったパスの範囲内にある下位 CA について、詳細に認証通用の範囲を名前で規定。 ● 通用可能な下位 CA 及びその配下の階層範囲 －下位 CA の名前(GN 形式) －通用可能な階層範囲の上限 －　〃　下限 ● 通用除外の下位 CA(指定方法は上記と同じ)
	policyConstraints policySet requireExplicitPolicy inhibitPolicyMapping	上記に加えて、ポリシーに対する制約。 ● 必要なポリシーID ● パス長(パス長が指定値を超えた認証にはポリシーの明示が必要。ポリシーマッピングでも可) ● ポリシーマッピング不可のパス長
	cRLDistributionPoints distributionPoint reasons unused keyCompromise cACompromise affiliationChanged superseded cessationOfOperation certificateHold cRLIssuer	失効リストの配布場所。 ● 配布局名(GN 形式 s)。省略時は失効リスト Issuer ● 上記配布局が対象とする失効理由(ビットの on/off) (0)未使用 (1)加入者の鍵が危瀬を受けた (2)CA の鍵が危瀬を受けた (3)認証の情報(被認証者の名前等)が変更(危瀬なし) (4)当該認証が置換えられた(危瀬なし) (5)利用中止 (6)利用の一時中止 ● 失効リストの発行局名。省略時は発行 CA

B.5.2. 失効リストフォーマット

Version	項目	説明
V-1	signature.algorithmIdentifier	署名方式
	issuer	失効リスト発行局名(Distinguished Name 形式)
	thisUpdate	当該失効リストの発行日時
	nextUpdate	次回の発行予定日時
V-2	version	バージョン番号(ない場合は V-1、1 なら V-2 を示す)
	authorityKeyIdentifier keyIdentifier authorityCertIssuer authorityCertSerialNumber	当該失効リストの署名確認に用いるべき認証の識別子 ●鍵識別子(8 進数) ●鍵の認証発行局名(GN 形式) ●認証番号
	cRLNumber	失効リストの発行通し番号
	issuingDistributionPoint distributionPoint onlyContainsUserCerts onlyContainsCACerts onlySomeResons indirectCRL	当該失効リストの配布局と性質 ● 配布局名(GN 形式) ● 加入者の失効専用(の場合に「真」) ● CA 認証の失効専用(の場合に「真」) ● 幾つかの失効理由による(理由フラグをセット) ● 失効理由等の情報は、失効リスト発行局でなく認証発行局に迂回。後記の certificateIssuer の項を参照。
	deltaCRLIndicator	当該失効リストがデルタ失効リストかどうかの識別。ベース失効リストの失効リスト Number を指定することで、それに対する変化分だけを取扱う(両者の発行日時はベース失効リストの方が早い)。[11]
V-1	certificateSerialNumber	認証番号
	revocationDate	失効申請受理日時
V-2	reasonCode unspecified keyCompromise cACompromise affiliationChanged superseded cessationOfOperation certificateHold removeFromCRL	失効理由(以下のコードを指定) (0)理由不明 (1)加入者の鍵が危瀬を受けた (2)CA の鍵が危瀬を受けた (3)認証の情報(被認証者の名前等)が変更(危瀬なし) (4)当該認証が置換えられた(危瀬なし) (5)利用中止 (6)利用の一時中止 (8)一時中止状態の解除(デルタ失効リストの場合に利用。ベース失効リストで上記(6)の状態のものを削除する)
	holdInstructionCode	一時利用中止に対する対処方法(オブジェクト ID を指定)
	invalidityDate	秘密鍵が危瀬にあったと考えられる日時。認証局が失効リストを発行した日時(thisDate)より一般に早い。申請ベースなので、これだけでは否認防止(nonrepudiation)に不十分。
	certificateIssuer	認証発行局名(GN 形式)。indirect 失効リストの場合には失効情報が失効リスト発行局で管理されていないため、指定された CA に迂回する。省略された場合は、直前の加入者と同じ CA(最初に省略された場合は、失効リスト発行者)。

[11] 本来失効リストは失効認証書全てを蓄積したもの(ベース失効リストと呼ぶ)であるが、失効数の増大によるパフォーマンスの悪化防止と失効リストの配布元分散のために、デルタ失効リストが考案された。デルタ失効リストはベース失効リストに基づくものであり、ベース失効リストは不可欠である。

B.5.3. 認証書の用途と種類

認証はいろいろな用途に利用することができるが、その用途は大きく次の二つに分けられる。

(1)本人確認(Identification/Authentication)

個人や法人、あるいはサーバー等の名前や所在等についての真正性を確認し、申請された公開鍵の保有者であることを証明するものであり、後述する権限認証のベースとなるものでもある。何によって確認するかによって認証レベルの厳格性に差が生じるが、3〜4 段階程度にレベル分けされることが多い。

(2)権限認証(Authorization)

特定のアプリケーションに応じた権限があること証明するもの。認証の要件がアプリケーションごとに定められるものであり、前記の本人確認と異なり多様な種類が存在し得る。例えば、クレジットカード決済では、カードホルダー、加盟店、ペイメントゲートウェイ等の認証書の形式は同じであるが、それらの処理はアプリケーションに依存している。

権限認証はアプリケーションと密接に結びついており、例えばクレジットカード、銀行等のサービス提供のための一手段として利用されるのが普通である。一方、本人確認は、アプリケーションに依存せず、汎用的な利用が可能である。こうしたことから、通常、それぞれのサービスを提供する認証局は、性格が異なり、それに伴うポリシーも異なる。例えば、損害補償について言えば、権限認証では、あくまでもアプリケーションの範囲内で決まるのに対して、本人認証では認証書が何に使われるかによって補償額が大きく変動することが想定される。

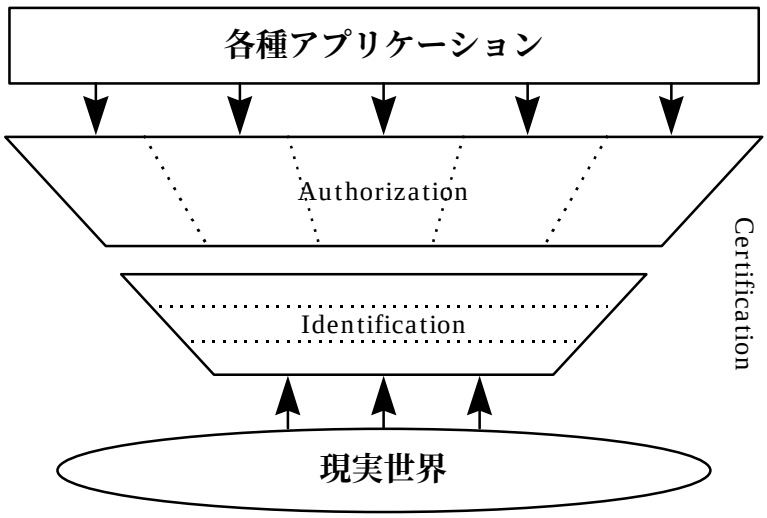


図 B-3認証の種類

C. 参考文献

(1) 電子商取引に関する検討課題について(電子商取引環境整備研究会中間報告), 通商産業省, 1996.4
"http://www.ecom.or.jp/miti/press960423.html"
(2) 電子商取引環境整備研究会-中間論点整理, 通商産業省, 1997.11
"http://www.ecom.or.jp/miti/971127/mokuji.htm"
(3) ネットワークを通じた認証業務の在り方に関する調査研究会-報告書-, 郵政省, 1997.10
"http://www.mpt.go.jp/policyreports/japanese/group/internet/index-net-n.html"
(4) 岩下直行, 宇根正志, キーリカバリー構想を巡る最近の情勢について, IMES Discussion Paper No. 97-J-8, 日本銀行金融研究所, 1997.5
"http://www.imes.boj.or.jp/jdps/97-J-08.pdf"
(5) 楠田浩二, 櫻井幸一, 公開鍵暗号方式の安全性評価に関する現状と課題, IMES Discussion Paper No. 97-J-11, 日本銀行金融研究所, 1997.7
"http://www.imes.boj.or.jp/jdps/97-J-11.pdf"
(6) 情報システム安全対策基準解説書、(社)情報サービス産業協会、1996.10
(7) コンピュータウイルス対策基準[通商産業省告示第 429 号], 通商産業省, 1995.7.7
"http://www.ipa.go.jp/SECURITY/antivirus/kijun429.txt"
(8) コンピュータ不正アクセス対策基準[通商産業省告示第 362 号], 通商産業省, 1996.8
"http://www.ipa.go.jp/SECURITY/ciadr/crack-gl.txt"
(9) コンピュータ不正アクセス対策基準解説書, (財)日本情報処理開発協会, 1996.11
(10) コンピュータセキュリティ基本要件 機能編【第１版】, (社)日本電子工業振興協会, 1994.6
(11) 暗号認証技術を利用した鍵管理システムの調査研究, 認証実用化実験協議会(ICAT), 1996.3.14
[ICAT ホームページ: "http://www.icat.or.jp/"]
(12) 暗号政策と電子現金（電子決済、電子現金とその利用環境整備に関する調査研究会報告書）、郵政省電気通信局、1996.4
(13) 電子決済におけるセキュリテイに関する調査研究中間報告、金融情報システム No. 172, 1996.6
(14) Bruce Schneier, E-MAIL SECURITY, 邦訳：力武 健次監訳「E-Mail セキュリティ」, オーム社, 1995.5.25
(15) ISO/IEC 9594-8 : 1995 | ITU-T Recommendation X.509(1993E), Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 1993.11
[案内："http://www.itu.ch/itudoc/itu-t/rec/x/x500up/x509_27505.html"]
(16) ISO/IEC DIS 11770-1:1996(E) Information technology - Security techniques - Key management - Part 1: Framework, 1996
(17) ISO/IEC CD 11770-3:1996(E) Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques, 1996
(18) ISO DIS 13491-1 Banking - Secure cryptographic devices (retail) - Part 1: Concepts, requirements and evaluation methods, TC68/SC6, 1996.5
(19) ISO/IEC WD 14516-1, Guidelines for the use and management of Trusted Third Party services - Part 1: General Overview, JT1/SC27, 1995.11
(20) ISO/IEC JT1/SC27 WD 14516-2, Guidelines for the use and management of Trusted Third Party services - Part 2: Technical aspects, 1996.6

(21) ISO WD 15782, Banking - Certificate Management Part1: Public Key Certificates, TC68/SC2/WG8, 1997.11
(22) Common Criteria for Information Technology Security Evaluation Part 2: Security function requirements [Version 2.0 Draft], 1997.12.19
"http://csrc.ncsl.nist.gov/cc/ccv1x/p2-xd.pdf"
(23) R. Housley, W. Ford, W. Polk, D. Solo, Internet Public Key Infrastructure X.509 Certificate and CRL Profile, IETF PKIX Working Group, 1997.10.14
"ftp://ftp.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part1-06.txt"
(24) S.Farrell, C. Adams, Internet Public Key Infrastructure Certificate Management Protocols, IETF PKIX Working Group, 1997.11.19
"ftp://ftp.ietf.org/internet-drafts/draft-ietf-pkix-ipki3cmp-06.txt"
(25) S. Chokhani, W. Ford, Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF PKIX Working Group, 1997.9.30
"ftp://ftp.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-02.txt"
(26) Federal Public Key Infrastructure Technical Specifications Part A: Requirements, NIST, 1996.1.31
"http://csrc.ncsl.nist.gov/pki/require5.ps"
(27) Federal Public Key Infrastructure Technical Specifications Part B: Technical Security Policy, NIST, 1996.1.24
"http://csrc.ncsl.nist.gov/pki/tspolicy.ps"
(28) Burr, Federal Public Key Infrastructure Technical Specifications Part C: Concept of Operations, NIST, 1996.2.12
"http://csrc.ncsl.nist.gov/pki/conops.ps"
(29) Federal Public Key Infrastructure Technical Specifications Part D: Interoperability Profile, NIST, 1995.9.27
"http://csrc.ncsl.nist.gov/pki/cross.ps"
(30) The 1994 Mitre PKI Study Final Report, NIST
"http://csrc.ncsl.nist.gov/pki/mitre.ps"
(31) Warwick Ford, A Public Key Infrastructure for Unclassified but Sensitive Applications, NIST, 1995.9.1
"http://csrc.ncsl.nist.gov/pki/fordrept.ps"
(32) Security Requirements for Cryptographic Modules[FIPS PUB 140-1], NIST, 1994.1.11
"http://csrc.nist.gov/fips/fips1401.htm"
(33) Licensing of Trusted Third Parties for the Provision of Encryption Services [Public Consultation Paper], UK Department of Trade and Industry (DTI), 1997.3
"http://dtiinfo1.dti.gov.uk/pubs/"
(34) Digital Signature Guidelines, American Bar Association, 1996.8.1
"http://www.abanet.org/ftp/pub/scitech/ds-ms.doc"
(35) ICE-TEL, Architecture and General Specifications of the Public Key Infrastructure, 1996.9
"http://www.darmstadt.gmd.de/ice-tel/deliverables/download/D1-Architecture.rtf"
(36) VeriSign Certification Practice Statement, VeriSign, Inc., 1996.8.7
"http://www.verisign.com/repository/CPS/"
[日本語版: "http://www.verisign.co.jp/repository/CPS1.1/"]
(37) Utah Digital Signature Act(1996)
"http://www.commerce.state.ut.us/web/commerce/digsig/dsmain.htm"

(38) Bradford Biddle, Misplaced Priorities: The Utah Digital Signature Act and Liabilty Allocation in a Public Key Infrastructure(Draft: October 18,1996)
"http://www.softwareIndustry.org/issues/docs-org/digsig.pdf"
(39) Christopher Kuner 英訳, German Draft Digital Signature Law (SigG), 1996
"http://ourworld.compuserve.com/homepages/ckuner/digsig.htm"
(40) Michael Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce (Draft), 1995.4.22
"http://www.law.miami.edu/~froomkin/articles/trusted.htm"
(41)Internet Law & Policy Forum,Survey of Electronic and Digital Signature Legislative Initiatives in the United States
"http://www.ilpf.org/digsig/digrep.pdf"
(42)Internet Law & Policy Forum, The Role Of Certification Authorities In Consumer Transactions
"http://www.ilpf.org/work/ca/draft.htm"

D.　検討メンバー一覧

ECOM

米倉 昭利	主査	電子商取引実証推進協議会 主席研究員
長　博連	副主査	電子商取引実証推進協議会 主席研究員
角間 和博	副主査	電子商取引実証推進協議会 主席研究員

リーダー・サブリーダー

船越 亘	リーダー	株式会社富士通総研 研究開発部 主席研究員
木暮 素史	サブリーダー	株式会社ディーシーカード マルチメディア企画室 室長
佐藤 裕之	サブリーダー	さくら銀行 ネットワーク業務部 調査役
柴田 勉	サブリーダー	財団法人金融情報システムセンター 安全対策部情報課 課長

メンバー

井上 清司	沖電気工業株式会社 E コマース開発部 開発第一チーム サブチームリーダ
岩下 直行	日本銀行 金融研究所 調査役
内田 勝也	安田火災海上保険株式会社 市場調査部 システム調査役
宇野 順嗣	ユーシーカード株式会社 ＥＣ事業部 調査役
大谷 彰宏	三菱電機株式会社 情報システム製作所 Ｃ／Ｓネットワークシステム部 主事
大橋 哲也	株式会社ジェーシービー 情報ネットワーク事業部 マルチメディア開発課 課長
加藤 丈博	株式会社ミリオンカード・サービス 企画部マルチメディア推進室
河崎 克也	社団法人日本クレジット産業協会 企画調査部 主任
北野 健二	セコム株式会社 通信技術推進室 主任
後藤 邦雄	三井海上火災保険株式会社 火災新種業務部 課長
佐藤 順一	日本信販株式会社 企画本部マルチメディア推進室 チーフマネージャー
島崎 貴志	株式会社野村総合研究所 サイバーコマース事業部 コンサルタント
白鳥 幸和	株式会社ディシーカード マルチメディア企画室 課長
福村 和悦	日本電気株式会社 ネットワーキング技術研究所 部長
藤尾 真嗣	アメリカン・エキスプレス・インターナショナル 業務企画部 副部長
藤野 欣哉	株式会社住友クレジットサービス マルチメディア推進部 副主任
二村 朝康	エヌティティデータ通信株式会社 技術開発本部マルチメディア技術センター
光永 聖	株式会社日立製作所 金融システム本部 新金融システム推進室 室長
森山 将治	株式会社日立製作所 金融システム本部 新金融システム推進室 技師
安國 弘晃	株式会社アドバンス 情報通信事業本部 ＩＴ研究所 次長
吉田 正敏	株式会社シー・アイ・シー 電子取引研究プロジェクトチーム サブマネージャー