参考資料

認証局運用ガイドライン（１．０版）
ネットワーク認証業務に関するガイドライン

H9－WG08－1

認証局運用ガイドライン
(1.0版)

平成10年3月

電子商取引実証推進協議会
認証局検討WG

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。

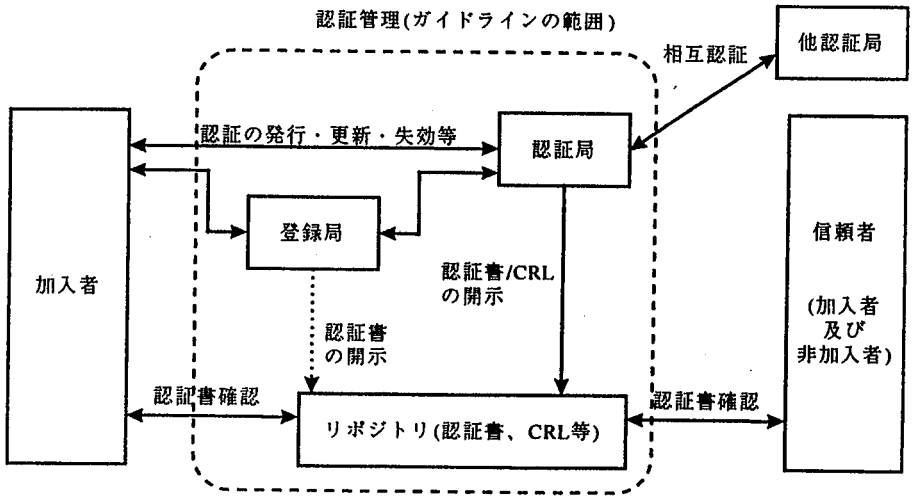

図-1 ガイドラインの対象と範囲

[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。

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。

---

[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。

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. 危瀕（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、秘密鍵が危殆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。