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

(1)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イ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　④UPS ⑤蓄電池　⑥非常用発電機 ⑦コンセント　など
3	通信設備	①MDF/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（パッケージなど）　②室外機（クーリングタワーなど） 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。

ネットワーク認証業務に関するガイドライン

Ⅰ　趣旨

本報告書において検討したとおり、ネットワーク認証（通信ネットワークを通じて提供される認証）は、ネットワーク取引において不可欠のインフラとなることから、適正な方法で提供されることがネットワーク取引の発展のためには極めて重要である。

こうしたことから、ネットワーク認証業務が適正に提供されるための法的枠組みの在り方について早急な検討が求められるが、本ガイドラインは、検討の際の参考となることを期待している。

また、現在、既にネットワーク認証業務を提供しているか、あるいは提供しようとしている民間の事業者のビジネス上の指針となることも期待している。

報告書においても述べたとおり、ネットワーク認証業務に関する法制化を検討するに当たっては、ネットワーク認証業務が萌芽期にあることにも鑑み、必要最小限の法的措置に限定することが重要である。また、法制化の検討に当たっては、国際的整合性の確保や技術革新に対する柔軟な対応が可能な仕組みの確保が重要である。

また、本ガイドラインは、あくまでも民間事業者によるネットワーク認証業務の提供を促進するとの観点から、とりまとめたものであり、拘束力をもつものではなく、本ガイドラインの遵守をもって認証機関の法的責任が免除される性格のものでもない。

また、本ガイドラインは、あくまでも基本的事項を定めたものであり、認証機関が実際に業務運営を行うに当たっては、更に細目的な運営基準を自主的に定めることが望ましい。

なお、本ガイドラインは、主として公開鍵暗号方式によるネットワーク認証業務を念頭に置いたものとなっているが、これは、公開鍵暗号方式が現時点で国際的にみて主流となっていることを踏まえているものであり、公開鍵暗号方式が特に技術的優位性を有していることを意味するものではない。

Ⅱ　認証機関の備えるべき要件

1　技術的安全・信頼性の確保

(1)暗号に関する専門知識

暗号方式を利用したネットワーク認証業務を提供する場合には、認証機関は、暗号に関する専門知識を有する管理者を置くことが望ましい。

また、公開鍵証明証の偽造防止のため、認証機関は安全性の高い暗号鍵を用いて自己の発行する公開鍵証明証にデジタル署名を行うことが必要である。

(2)認証システムへの不正アクセス防止措置

認証システムに対する外部からの不正アクセス等を防止するために、信頼性の高いファイアウォールの構築等の措置を講ずることが必要である。

(3)設備の安全性・信頼性確保

安定的継続的に業務を提供するために、認証システムについて設備の安全性・信頼性を確保するための措置を講ずることが必要である。

【設備の安全性・信頼性確保のための措置の例】

① 設備の多重化等
ネットワーク設備を含む設備の多重化や保管データのバックアップ等の措置を講ずること。

② 災害対策
認証システムを、地震、火災、水害等の自然災害から守るための安全対策を講ずること。

③ 誤操作対策
認証システムの運用者による誤操作等により、蓄積データが簡単に消滅してしまうことのないよう安全対策を講ずること。

また、情報通信システムを構築するに当たっては、「情報通信ネットワークの安全・信頼性基準」（昭和62年郵政大臣告示第73号）に準拠することが望ましい。

(4)関連施設内への部外者の不正侵入防止のための措置

認証システムの設置場所への部外者の立入りが無制限に行われないよう、施錠等による厳重な管理を行うことが必要である。

(5)業務提供の継続性・迅速性の確保

継続的かつ迅速なサービス提供を行い得るような設備上・運営上の体制作りが必要である。
特に、証明証の失効リストの公開については、顧客や証明証を受け取った第三者に対する不測の不利益を防止するためにも、特に迅速性の確保が必要である。

2 財務的基盤

認証機関は業務提供に当たって、一定の法的責任を負う可能性があることから、安定的な財務的基盤を維持することが望ましい。
また財務諸表等の公表を通じて、自己の財務状況の開示を行うことが望ましい。

3 内部管理規程

(1)内部不正防止対策

信頼性のある業務提供を確保するため、内部管理規程を定めて従業員による内部不正防止に努めることが必要である。

(2)権限の分散

内部不正防止のため、適切な権限分散や業務のローテーションを行うことが望ましい。

(3)研修等の実施

内部管理規定の内容について従業員に対して周知徹底させるために、従業員に対する研修等を実施することが望ましい。

(4)業務監査

業務運営体制の信頼性を確保するために、その業務運営の状況について、定期的に外部の専門家による監査を実施することが望ましい。

Ⅲ 認証機関が業務運営上充たすべき事項

1 本人確認

公開鍵登録に際しては、通常、本人しか知り得ない（ないし持ち得ない）情報や身体的特徴等により身元を確認することが必要である。
本人確認の具体的方法については、個々の認証サービスの水準によっても異なりうるが、以下のような方法が考えられる。

【本人確認の例】
・個人の場合：運転免許証、パスポート、写真入りの身分証明証、住民票、印鑑証明等による確認
・法人の場合：登記簿謄本及び代表者の印鑑証明等による確認

また、こうした方法の他にも、認証機関が、既に顧客に関して、十分な対照データをもっている場合には、そうしたデータと照合することによって、本人確認を行うことも考えられる。
なお、認証機関がどのような方法で本人確認を行っているかについては、顧客以外の第三者にも公開する必要がある。
認証機関への登録申請について、代理人が本人に代わって申請を行う場合には、認証機関は、代理人が正当な代理権を有するかどうかについて、十分な確認を行うことが必要である。また、認証機関は、代理申請の際に求められる要件について、あらかじめ明確にしておくことが望ましい。

2 公開鍵証明証の記載事項

公開鍵証明証の記載事項については、認証サービスの内容によって異なり得るが、ITU—TのX.509勧告等の国際標準に準拠することが必要である。
また、認証機関が、公開鍵証明証の発行に際して、賠償責任限度額を設定する場合には、公開鍵証明証にも当該限度額の記載を行うことが必要である。

3 公開鍵証明証の公開

認証機関が発行した公開鍵証明証については、それを受領した第三者等が確認可能なように、原則として、公開することが必要である
公開の具体的な方法としては、公衆通信ネットワークを通じてアクセス可能な状態（例えばインターネットのホームページ）での公開等が考えられる。
ただし、証明証の公開に当たっては、証明証の交付を受けた本人の承認を得ること、または公開によって守秘すべき情報の漏洩に結びつかないことの確認が必要である。

4 証明証の有効期限

公開鍵証明証を発行するに当たっては、顧客の暗号鍵の強度等を勘案して、一定の有効期限を設けることが望ましい。
また、有効期限を定めない場合には、暗号鍵の安全性が時間の経過により低下することについて、顧客に対して注意喚起を行うことが望ましい。

5 証明証の失効

(1)失効事由
認証機関の発行した公開鍵証明証を失効させることが必要な場合の例としては、以下のようなものが考えられるが、いずれの場合にも、失効の要件やその手続き等を明確にする必要がある。

【顧客が個人の場合】
① 顧客本人（又は代理人）の請求があった場合
② 本人が死亡した場合
③ 登録事項が事実と相違する場合や証明証が虚偽の申請に基づき発行されたことが明らかになった場合
④ 司法機関等の判断があった場合

【顧客が法人の場合】
① 代表者による請求があった場合
② 登録事項が事実と相違する場合や証明証が虚偽の申請に基づき発行されたことが明らかになった場合
③ 司法機関等の判断があった場合
④ 法人が解散した場合

【顧客が法人所属の個人の場合】
① 本人の死亡・退職等の場合
② 登録事項が事実と相違する場合や証明証が虚偽の申請に基づき発行されたことが明らかになった場合
③ 司法機関等の判断があった場合
④ 法人が解散した場合

(2)失効事実の公表
認証機関は、公開鍵証明証を失効させた場合には、第三者が容易にアクセスできる手段(例えばインターネットのホームページ)で、その事実を公表することが必要である。
また、その公表に当たっては、失効時点だけでなく、事後的にも参照が可能なように、失効リストの形で公表することが必要である。
ただし、電気通信事業者が、発信者の通信を媒介する際に、併せて受信者に対して証明証を送付するような形態の場合には、失効リストの公表は不要である。

6 時刻証明等

(1)証明証に発行時刻を付記する形態
認証機関が、その発行する公開鍵証明証に発行時刻を付記する場合には、認証機関は、正確な時刻管理が求められるほか、国際取引に用いられる場合を想定して、どの標準時刻を用いたかについて明確にする必要がある。

(2)通信メッセージに時刻を付記して伝送を行う形態
認証機関が、通信を媒介した(ないしは通信が相手方に到達した)時刻について、証明を行う場合にも、認証機関には、正確な時刻管理が求められるほか、どの標準時刻を用いたかについて明確にする必要がある。
また、この場合には、認証機関は、通信の媒介を行うこととなるため、通信の秘密の確保が求められる。

7 内容証明・送達証明

認証機関が、通信内容や通信の送達の有無について証明を行う場合には、認証機関は、通信内容を正確に記録し、事後的な証明が可能な状態にしておくことが必要である。
また、認証機関は、記録した通信内容について、証明を申請した顧客に確認を求めることが望ましい。
なお、この場合には、認証機関は、通信の秘密を確保することが求められる。

8 秘密鍵の生成・管理等

(1)秘密鍵の生成・管理等に伴う認証機関の義務
認証機関は、顧客のために秘密鍵を生成する場合には、容易に解読ないし偽造が行われないよう、サービスに求められる信頼性に応じ、十分に強度のある暗号鍵の生成が必要である。
また、認証機関は、顧客に対して暗号鍵の配送を行う際に、暗号化等の手段を用いて安全確保を図るほか、秘密鍵の保管に当たっては、不正アクセス等に対する十分な防止措置(鍵の分散管理も含めたリスク管理)を講ずることが必要である。
更に、認証機関が顧客の秘密鍵の生成等を行う場合には、内部の不正行為を防止するための業務監査の実施が必要である。

(2)秘密鍵へのアクセス
認証機関が顧客から預かっている秘密鍵を、本人に返却する場合の本人確認について、あらかじめ十分に信頼性のある手続を定め、その手続に従い行うことが必要である。
また、本人以外の者が秘密鍵へのアクセスを求める場合として、以下のような場合が想定されるが、具体的にどのような条件でアクセスが認められるのかについては、契約において明確に規定されることが望ましい。

【本人以外のアクセスの例】
① 本人が死亡した場合の相続人による回復要求
② 暗号鍵を管理していた従業員が退職した場合の、当該法人による回復要求
③ 法律上の手続きを経た司法当局による回復要求

9 業務の中断・停止

業務を中断ないし停止する場合には、十分な時間的余裕をもって顧客に周知を図ることが必要である。また、恒久的に業務を廃止する場合には、他の認証機関に業務あるいはその保有データの引き継ぎを行うことが望ましい。

Ⅳ 顧客関連情報保護

1 顧客関連情報収集の制限

顧客の暗号鍵登録を行う際に、顧客のプライバシーに関わる情報を入手する場合には、業務提供のために必要最小限の情報に限定すべきである。

2 顧客関連情報の保護

認証機関が保有するプライバシーに関する情報については、それが入手目的以外の用途に流用されたり、第三者に開示されたりすることがないよう、顧客関連情報の保護に関する内部管理規定が必要である。
また、内部管理規定の策定だけではなく、プライバシー関連情報にアクセスしうる立場にある従業員に対して適切な研修を実施するなどして、周知徹底を図ることが望まれる。

3 第三者への開示

顧客関連情報の第三者への開示については、原則として、本人(又はその正当な代理人)の同意あるいは法律上の手続きに基づく司法当局の要求等があった場合に限定されるべきである。

Ⅴ 認証機関の開示義務及び利用者責任

ネットワーク認証業務は、まだ萌芽期にあり、その業務内容や法的責任等についても、不明確な点も多いことから、認証機関は、業務内容、安全対策、法的責任、財務的基盤等について、広く利用者に対して開示をしていくことが望ましい。
他方、ネットワーク認証業務の信頼性は、サービスを利用する顧客による厳格な秘密鍵管理が前提となり、また、利用目的に応じたサービスの選択が行われることが望ましいことから、認証機関は、こうした側面に関して、顧客に対して啓発を行うことが望ましい。

Ⅵ 相互認証

認証機関は、自己の顧客のために、他の認証機関の認証要件の信頼性について認証を行うための相互認証のための基準を設けることが望ましい。

認証機関等調査検討委員会

平成１１年６月１日発行

財団法人　社会安全研究財団

〒１０１－００４７　東京都千代田区内神田１－７－８　大手町佐野ビル
Tel　０３－３２１９－５１７７