Ｈ９－ＷＧ１５－１

電子公証システムガイドライン要約版

（Ver. 1.0）

平成 10 年３月

電子商取引実証推進協議会
電子公証検討ＷＧ
電子公証検討ＳＷＧ

はじめに

「電子公証システムガイドライン」は、電子商取引参加者や企業の電子化推進部門、さらには電子公証サービス事業者を対象に電子商取引を安心して実現するための指針として纏めたものである。

安心して電子商取引を行うための仕組みの一つである電子公証を、取引モデルの業務フローを材料に検討し、電子公証概論、電子公証のニーズ、取引当事者から見た電子公証、サービス事業者から見た電子公証についての考え方をまとめたものである。

産業の情報化、社会の情報化の進展と共に、従来の「公証」に限定されない様々なサービスニーズに応えるため、技術革新に柔軟に対応できる民間主導（市場の判断と自己責任）の取り組みを促進し、電子商取引の市場拡大に寄与することを狙いとしている。

要旨

『電子公証』を、「ネットワーク上の商取引等における電子的交流の安全・信頼性を確保する仕組み」において、その一構成要素として位置づけたうえで

(1) 安心な電子商取引の実現には認証、電子公証以外にもその取引の形態（例えば不特定多数企業との初めての取引き場合）により、利用が想定されるさまざまな機能（取引時：認証、電子公証、運用能力格付、企業格付、取引処分、トラブル発生時：調停、損害補填、周辺機能：取引監視、認定、監査）がある。

(2) 電子公証の役割と定義を、取引当事者間の信頼性を維持し、安定な取引実現の役割を担い、ネットワーク上の商取引等において「誰が（と）」「何を」「何時」電子的交流を行ったかを証明する仕組み（但し、「誰が（と）」は認証機能として包含する）とする。証拠力を高めることにより、紛争の防止や万一紛争が発生した場合の有効な解決手段となる。

(3) 企業間取引は取引形態（継続的取引を前提とするか、前提としないか）、取引プロセス（取引企業を特定するまで、取引企業を特定以降）、取引対象（生産財／消費財、物財／情報財、開発品／標準品等）により、脅威や不安の大きさは異なるため、電子公証のニーズや要求レベルは一律でなく実ビジネスモデル個々の検討が必要である。不安のある取引相手や万一のトラブル対応において、信頼性ある第三者機関（電子公証センター）は取引の信頼性確保に有効な手段となる。

(4) 企業内では業務の電子化、シームレスなセキュア環境整備（例えばエクストラネット導入）や、市場からの公明性・情報開示等の社会的要請に対し、企業内の認証・電子公証システムが重要な役割を果たす。

(5) 消費者―企業間では決済の方法やデジタルコンテンツを扱うケース、消費者保護（プライバシー保護を含む）の観点から付加的な議論が必要と考えられる。信頼性を確保するための電子公証機能の組み込みや、紛議の場合の事実関係を証明したり、デジタルコンテンツの真正性（ホームページ、情報財、著作権等）を証明する手軽な電子公証センターの利用がある。さらに、オープンな取引が故のリスク負担の基本的な考え方の社会的なコンセンサス作りに向けた議論が重要である。

(6) 電子商取引では契約書に代表される電子情報の証拠力の向上が重要である。この実現には電子的な機構や人的なルールによる運用による企業内電子公証システムや民間の電子公証センターがその役割を担うことができる。

(7) 「電子的交流の安全・信頼性を確保する仕組みのモデル化」としての「電子公証モデル」は法制度、社会的慣行、当事者間の相互のルールといった「人的仕組み」と、ＣＰＵによる処理としての「電子的仕組み」から構成され、電子公証機能のどの機能が必要か、どの程度のセキュリティレベルが必要かは取引相手、取引形態、取引対象、取引のプロセス等の個別の状況で決められるものである。

(8) 「電子的交流の安全・信頼性を確保する仕組み」は社会面と技術面の影響を受けながら発展していくものであり、固定化されるものではない。

(9) 電子公証サービスは最終的な財として消費されるのではなく、社会的活動の情報化が電子公証機能をその一部として必然的に取り組む様になることを示すものである。従って、電子公証サービスの実現には情報技術による新たなビジネスモデルの取り組みと、そこに「電子公証」機能が組み込まれていくアプローチが重要となる。

(10) 自由心証主義のもと、電子データの証拠力は決して否定されてはならないが、同時に何でも認められるわけでもない。求められるセキュリティレベルに応じて個別に議論されるべきであり、その証拠や信頼性強化のためのサポート手段として「電子公証」は必要である。

(11) 電子公証センターの運営主体は公的、民間、企業内システム部門が考えられる。公的機関の公証業務は今後とも重要な役割が期待される。既に米国では民間のサービスが開始され、個々のビジネスモデルの中に電子公証機能の組み込みがされている。従来の「公証」に限定されない様々なサービスニーズへの対応が必要であり、「市場の判断」と「自己責任」の原則による産業の情報化、社会の情報化に向けた市場形成が望ましい。

(12) 民間の電子公証サービス事業実現のための環境整備に向け、①電子公証センター運用ガイドライン②利用約款の作成や電子公証センター自体の認定、監査等の基準、仕組み等検討が重要となる。

(13) 安全および信頼性を確保した電子商取引の実現には、新たな商慣行や法制度の確立も必要であるが、全てが整うのを待つばかりでなく、新たなビジネスモデルに対する積極的な技術導入による試行錯誤も必要である。

1 安心な電子商取引実現に向けて

1.1 安心な電子商取引

1.1.1 安心な商取引

商取引を行う上で、最も重要なことは、**「信頼」**であり**「安全」**である。「信頼」とは取引当事者間の「信頼」構築を意味し、「安全」とは取引当事者を取り巻く外部要因からの「安全」確保を意味している。ここでは、「信頼」と「安全」をあわせて、「安心」という言葉で表現する。リアルの世界では、様々な要素が安心な商取引を支えるために機能している。それは技術やサービスとして提供されていたり、制度として運用されていたりしており、取引の当事者は、取引の内容によってそれらを使い分け、自らの責任で安心を確保している。

ネットワーク上で行われる取引ー電子商取引においても、リアルの世界同様、この安心がキーワードであることにかわりはない。電子商取引がリアルの世界の取引と異なるのは、「**オープンなネットワーク**に起因する第三者からの脅威や当事者の認証や否認防止の必要性」そして「**デジタル**に起因する複製や改竄の容易性からの対策」を前提としている点である。従って、リアルの世界とは別のオープンなネットワーク、デジタルに起因する様々な想定される問題に対する技術、制度、商慣行（運用）面の解決が必要となってくる。

1.2 諸機能説明

1.2.1 諸機能分類

安心な電子商取引を行うために使用すると想定される機能は、大きな３つのカテゴリに分けられる。まず、取引を行う時に必要となる機能のカテゴリである。「電子公証」、「認証」、「取引所」、「運用能力格付」、「取引処分」、「企業格付」がここに含まれるが、取引の当事者は、取引の内容によって、これらの機能を使い分けることになる。

次に、トラブルが生じたときに必要な機能のカテゴリがある。「損害補填」、「調停」、「裁判」が含まれる。３つ目は、ネットワークや各機能を支える周辺機能のカテゴリである。「ネットワーク監視」、「取引監視」、「認定」、「監査」が含まれる。

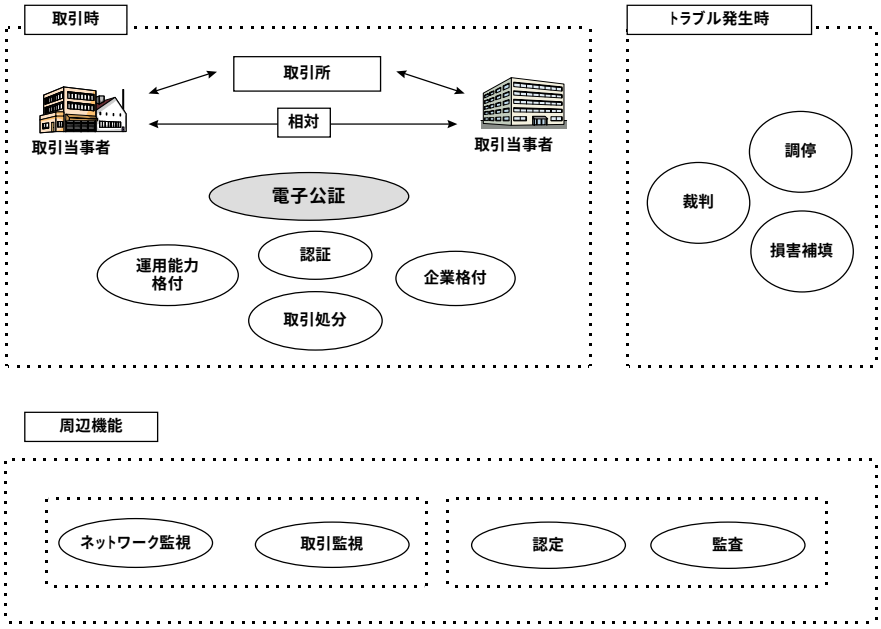


図 1-1 安心な電子商取引を行うために使用すると想定される機能分類

1.2.2 諸機能【取引時】

(1) 電子公証

ネットワーク上の商取引等において誰が（と）、何を、何時、電子的交流を行ったかを証明する仕組み。２章以降電子公証について詳細に記述する。

(2) 認証

電子的交流の対象となる個人、企業、サーバなどの真正性を証明する仕組み。現在では公開鍵基盤での方式が主流である。

今後は、年齢、所属国など、アクセス権限の制御に関連する認証の属性を加えることも考慮されよう。

(3) 取引所

様々な取引を効率的に行うために第三者による仲介・斡旋を行う仕組み。

通常は当事者間のみで取引が行われる。

(4) 運用能力格付

電子的交流を行う相手が信頼するに足る技術力､運用能力を具備するか示す仕組み。

(5) 取引処分

不正な取引などを行った企業等の情報を公開することにより、その企業等を再び取引に参加させない仕組み。

(6) 企業格付

企業の（取引相手としての）信用度を評価し示す仕組み。

1.2.3 諸機能【トラブル発生時】

(1) 損害補填

損害が発生した場合の保険や保証の仕組み。

(2) 調停

取引両当事者の合意に基づき、紛争が発生した場合に中立的な機関が客観的に判断し、解決方法に導く仕組み。

(3) 裁判

リアルの世界の裁判制度を指す。ネットワーク上の裁判という制度は存在しない。

1.2.4 諸機能【周辺機能】

(1) ネットワーク監視

ネットワークが正常に機能していることを監視する仕組み。

(2) 取引監視

ネットワーク上での取引を監視し、不正（偽造電子マネー、不正コピーなど）を検出する仕組み。

(3) 認定

認証局や電子公証センターなど、電子商取引に関わるサービスを提供するために設置された機関が一定の基準を満たしているかを審査し、その結果を公表する仕組み。

(4) 監査

認定を受けた機関が常に基準を満たしていることを定期的にチェックする仕組み。

電子商取引を行う際には、これらがすべて機能している必要があるとは考えていない。取引によっては、すべての機能が必要となるケースもあれば、最小限の機能しか必要としないケースもある。取引の内容により、当事者が判断を行うことになる。

当ガイドラインでは、これらの機能の中から「電子公証」を取り上げて記述する。

2 電子公証概論

2.1 電子公証の役割

安心な電子商取引には安全と信頼性確保が不可欠であり、第三者からの脅威の解決が前提であるが、これが解決できたとしても取引当事者間の信頼性が確保できなければ安心して取引出来ない。

そこで、この取引当事者間の信頼性を確保するための中心的な役割を担う仕組みを電子公証の役割とし定義する。この当事者間の信頼性を確保する仕組みは、その実現レベルにより、第三者からの脅威に対しても有効に機能するものも含まれる。その意味では電子公証は信頼性確保のみならず安全性確保面にも機能する。

取引当事者間の信頼性が低下する要因としては、当事者間の故意によるもの（例えば改竄や否認等）、機密情報や個人情報の漏洩等や故意によらない錯誤や入力ミス等もあるが、前者に対する解決の仕組みであり、後者は約束事（ルール）や教育や啓蒙が重要である。

2.2 電子公証の定義

『電子公証』とは、「ネットワーク上の商取引等における電子的交流の安全・信頼性を確保する仕組み」において、その一構成要素として位置づけられる。

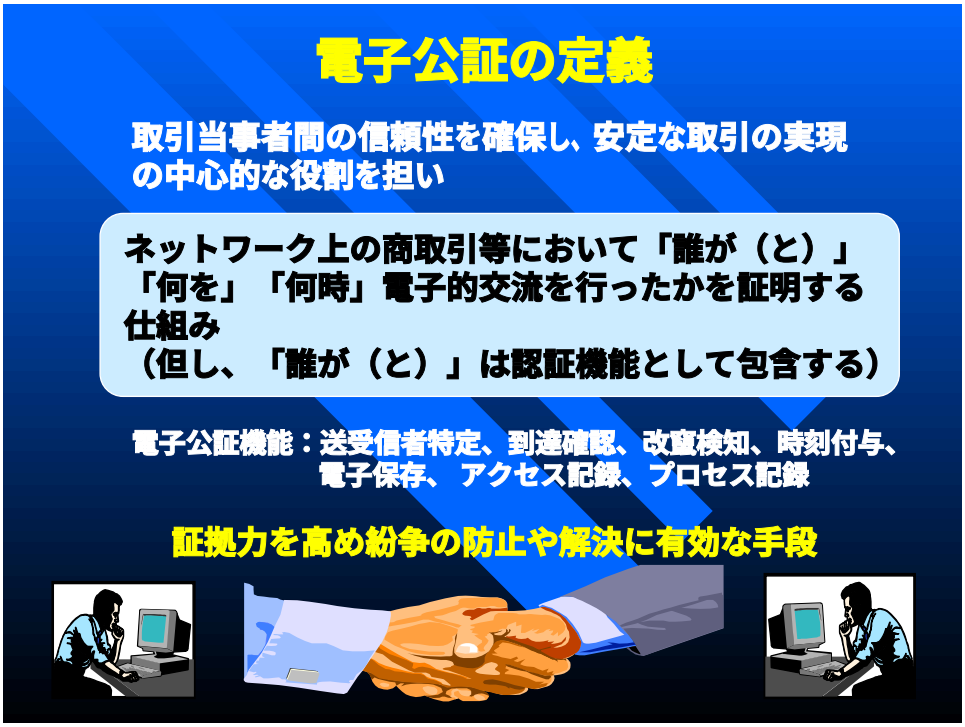


図 2-1電子公証とは

2.3 電子公証機能

2.3.1 送受信者特定機能

(1) 定義：

コンピュータシステム、ネットワークシステム等の利用者を特定する機能。通常、認証機関がその役割をする。

(2) 要件：

- 必要であればあらかじめ送受信者に認証書を発行する。
- 認証書発行の際は送受信者が本人であることを確実に行わなくてはならない。

本人でないと作成できない情報（例：電子署名）・方法（例：零知識証明）を利用し確実に送受信者を特定できなければならない。

2.3.2 到達確認機能

(1) 定義：

送信者から受信者へ情報を送信した事実を証明する機能。

(2) 要件：

・送受信者の認証を行わなくてはならない。

・送信者／受信者の送信／受信の否認を防止できなければならない。

・データを送信する際は、盗聴・改竄がされてないことを保証しなければならない。（例：ＳＳＬ、暗号化、電子署名、ＭＡＣ等）

2.3.3 改竄検知機能

(1) 定義：

文書（電子データ）が改竄されたことを利用者が検知できる機能。

(2) 要件：

改竄検知のためのデータ（例：電子署名、ＭＡＣ、ハッシュ関数）を付加しなくてはならない。

2.3.4 時刻付与機能

(1) 定義：

情報に対して日時データを付与する機能。また、情報に付与された日時データが正しいかを検証する機能。

(2) 要件：

・ 改ざんを防止できなければならない。

・日時データの精度は信頼性の高いものでなければならない。(例：ＧＰＳの利用、ＮＴＰにより信頼性の高い時刻データを提供するサーバと同期をとる)

2.3.5 アクセス記録機能

(1) 定義：

利用者がシステムを利用した事実を記録する機能であり、必要な時点でその事実を立証するために利用される。この前提としては正しいアクセス制御の存在を必要とする。ログ記録は一般的なソフトウェアなどのアクティビティをも含む記録生成機能である。

(2) 要件：

・ログ情報への攻撃・干渉等改竄がないことを保証しなくてはならない。（例：アクセス制御、Write Once、耐タンパー装置 等）

・不正利用、不正アクセス等の攻撃がされてないか検査できなければならない。

・システムが正しく運用されていることを証明できなくてはならない。

・記録する日時データの精度は信頼性の高いものでなければならない。（例：時刻付与機能等）。

2.3.6 プロセス記録機能

(1) 定義：

電子記録が組織や集団の中で更新されたり承認される場合、その更新、承認過程を記録・保持する機能。

電子保存機能やアクセス記録等の基本的な機能の組み合わせにより実現される。特に企業組織では、その活動は構成員による一連の処理の組み合わせにより行われる。

(2) 要件：

・処理過程に問題があった場合の問題分析や解決、あるいは処理が正しく行われたことを証明できなくてはならない。

・記録する日時データの精度は信頼性の高いものでなければならない。（例：時刻付与機能等）。

2.3.7 電子保存機能

(1) 定義：

情報の内容を媒体に記録・保管する機能。

(2) 要件：

・ データの完全性が保証されなければならない。

・必要に応じて読み出し再生ができなければならない。

必要に応じてデータに関する情報（ファイル名、書式・再生のためのソフトウェア等）を記録しなければならない。

・不正な利用、開示ができないよう保管できなければならない（例：暗号化、アクセス制御）。

・ データが保管された日付を証明できなくてはならい（例：時刻付与機能）。

・電子公証事業者の方針によっては、必要に応じて記録情報を削除できなければならない。

・データアクセスの際は、正当な当事者であることを確認できなければならない。（例：認証、アクセス制御）

・電子保存に関する処理のログ情報を記録しなくてはならない。（例：アクセス記録）

2.4 電子公証と法制度

電子公証を検討するにあたって忘れてはならないのがその法的裏付けである。

(1) 電磁的記録の原本性

電磁的記録は従来の原本、謄本、抄本という考え方になじまなず、例えば原本性を保証したシステムに保存された電子情報は原本とみなすとか電子公証センターに保存された電子文書は原本とみなすということも考えられる。

(2) 書類の電子保存

電子保存には

①法律で保存義務が課せられている場合の処理

②証拠として電子保存をする必要がある場合

があり､前者は主管省庁が電子保存原則容認の方向のもとに､要件を検討している。後者については、証拠力が要求され、産業の情報化、社会の情報化の進展により、そのニーズは増えていく。

(3) 電磁的記録と民事訴訟法

日本においては裁判官の自由心証による証拠価値の評価による。つまり、電磁的記録にどれだけの実質的証拠力を認めるかは裁判官の経験則に基づく自由な心証によるものとなる。これは、証拠法則に従って事実を認定しなければならないとする法定証拠主義に対立し、電磁的記録が法定証拠主義をとる諸外国において、どのような扱いをされているかを考慮する必要があり、整合性に注意する必要がある。

(4) 電磁的記録に対する罪

・公的電磁的記録…有形･無形偽造とも処罰

・私的電磁的記録…有形偽造のみ処罰

有形偽造…名義人を偽る

無形偽造…内容虚偽の情報を作成する

(5) 電磁的記録と商法

商法においては経理会計帳簿原本の電磁的記録化の是非が緊急のテーマである。等幅広い領域の検討が必要と思われるが、実ビジネス面に限定すれば（「契約自由の原則」のもと自由心証主義のわが国では）電子情報に対する証拠能力と証拠力がどの様にすれば担保できるかが関心事である。

その中で、ネットワークとデジタルの電子情報の署名・捺印に代替する候補である電子署名にまつわる議論である。

(6) 電子署名の立法化の問題点

電子署名に関して、法務省、通産省（電子商取引環境整備研究会　中間論点整理　平成９年１１月）で議論されているが、電子公証の視点からの問題点を述べる。

現法律は、紙をベースとした業務、商取引を前提に制定されており、法律で書面に印鑑が必要とされている定款、株主総会議事録、取締役会議議事録等を電子化する場合や会計帳簿、貸借対照表のように記名・捺印をし提出義務があるものを電子化する場合と、契約書等のように法律的にその規定が無い書類を電子化する場合が存在する。電子化の場合においても本人の特定と真正性(該当文書に意思の存在)が要求される。

前者では電子署名法等の法的な手当てが必要となるが、後者の契約書は契約自由の原則のもと、書面による署名・捺印の義務はない。しかし、契約書の電子化も現実的に行われるわけであり、後者に対する法的な手当てが必要かどうかを含め、検討が必要である。

自由心証主義のもと、電子データの証拠力は決して否定されてはならないが、同時に何でも認められるわけでもない。求められるセキュリティレベルに応じて個別に議論されるべきであり、その証拠や信頼性強化のためのサポート手段として“電子公証”は必要である。

電子化の対象毎に対応案として（１）電子署名法の立法化（２）新民事訴訟法２２８条４項の改正（３）現法律の解釈論として解決する方法等が考えられる。

しかし、特に（１）については下記の問題点もあり、慎重な検討が必要である。

① 特定技術への法的対応の妥当性（技術的中立性）
② 電子署名＝署名または記名捺印と同効力とするか
③ 電子署名の要件をどうするか
④ 技術的安全性が揺らいだ時、別の有力な認証技術が出た時、法的効力の発生に弾力性を持たせるのか
⑤ 社会コストが高くならないか

海外で一部導入されている「電子署名法」等、新しい技術に法律的な「お墨付き」を与えることにより利用者の不安等を取り除くことはできるが、ここで考えなければならないことはそれが新たな「規制」を生み出さないことである。目に見えない「デジタル情報」を扱う関係上、一般の利用者にはその問題点、優劣がわかりにくいということもあるが、基本的には「市場」が判断する仕組みが必要である。「市場の判断」には当然「自己責任」という考え方も含まれており、一部に痛みを伴うことも考えられるが、グローバルなネットワーク上ですべてを管理することは困難であり、「市場の判断」と「自己責任」による発展を原則とし、市場の力に余ったときにのみ何らかの対策を国際的な協調をもって介入する方策が望ましいと考えられる。

3 電子公証のニーズ

電子公証の必要な場面として代表的なものとして

- 電子商取引（企業―企業間、消費者―企業間）
- 企業内業務（調達、見積、企画、請求・精算、管理情報、研究・開発等）
- 電子申請・届出（ワンストップ／ノンストップサービス等）
- 電子調達（行政）
- 電子保存

などが考えられる。

企業間取引、企業内業務、消費者―企業間におけるそれぞれの代表的モデルの取引形態、局面の電子公証のニーズを検討すると電子公証の要求レベルの違いはあるものの基本的に要求される機能は同じであることが分かる。但し、企業内、消費者―企業間はそれぞれ特有の特性やプロセスを有しており、これらに対する検討が重要である。

3.1 企業間取引

(1) 企業間取引は取引形態（継続的取引を前提とするか、前提としないか）、取引プロセス（取引企業を特定するまで、取引企業を特定以降）、取引対象（生産財／消費財、物財／情報財、開発品／標準品等）、取引金額の大小により、脅威や不安の大きさは異なるため、認証・電子公証のレベルは一律でなく個々の検討が必要である。

(2) 不特定多数企業との取引については、そのニーズは殆どないという議論もある。これは不特定多数企業との取引を行うこと自体リスクが大きくて、現在の伝統的な取引や商慣行からは考えられないというものである。しかし、既に新たな商品を短期間に効率的に見つける方法として、ＷＥＢ－ＥＤＩによる試みも行われている。これは希望する商品を高品質、短納期、安価で入手するための手段として従来の特定多数企業間のみを対象にするのではなく不特定多数企業をも対象にするものであり、今の所、募集から基本契約締結のプロセスの一部の電子化にすぎない、しかし、オープンな企業とオープンなルールにより、募集から基本契約締結までも包含したプロセスが全て電子的な処理に置き換わることはできないにしても、安心な電子商取引実現環境の整備との兼ね合いから徐々に電子的な処理にシフトしていくと予測され、電子公証ニーズはオープンになればなるほど増えていく。

(3) 具体的なアプローチは情報技術による新たなビジネスモデルの取り組みと、その個別のビジネスプロセスの中に「電子公証」機能を組み込んでいくことにより、個々のビジネス分野への情報化の進展が図られることである。

（汎用的なサービスとしては、セキュアな電子情報配信サービス、セキュアな電子保存サービス等がある。）

3.2 企業内業務

業務処理の効率化に留まらず、対外的信用向上の視点も必要である。

(1) 企業内電子公証の果す役割には企業間電子商取引の場で想定されるものと違った側面がある。企業内電子公証は単に企業内部に閉じたものではなく、企業内外に対して必要に応じて情報を提供することもある、ということを想定しなければならない。従って、企業内電子公証の運用サービスポリシーは企業が決めるとしても、その信頼性、中立的立場の確保が要求されることになる。

(2) 業務処理過程の電子的捕捉とその記録保持（プロセス記録）は企業・組織活動を正確に捉えることを可能とし、不正処理の排除、正規な意志決定プロセスの確保、品質管理、効率的な企業経営の維持に非常に役立つ。

(3) 電子化は企業内の電子情報自体が証拠としての利用される場面の発現と、電子情報

に対する証拠能力、証拠力の高いことが要求され、電子公証ニーズは増えていく。
(4) 企業内では業務の電子化と取引先の拡大、コストの削減や取引先との企業間ワークフローによる取引の効率化を促進するためのエクストラネット導入によるシームレスなセキュア環境整備の必要性と企業の公明性・情報開示等の社会的要請に対応するため、企業内の認証・電子公証システムが重要な役割を果たす。

3.3 消費者―企業間取引

消費者―企業間では決済の方法やデジタルコンテンツを扱うケース、消費者保護（プライバシー保護を含む）の観点からの議論から、次のことが言える。

(1) 決済の方法にはクレジット、銀行振込、郵便為替、現金書留の前払いや後払いとさまざまな方法があり、安全性確保の責任主体も異なったり、要求されるレベルも異なる。そのため決済方法に応じた安全性確保の仕組みが必要である。
(2) 消費者がデジタルコンテンツを取り扱う場合には幾つかの側面が存在する。ホームページの真正性、情報財の真正性、さらには知らず知らずのうちに違法の海賊版を購入することがないというデジタルコンテンツそのものに対する安心感を確保する仕組みが必要である。
(3) 安全性確保は主体となる事業者が主体となり、安全性が確保された通信ツールの提供を行うと同時に、消費者への安全確保の啓蒙をする必要がある。
(4) 信頼性面（取引当事者関）では、契約の存在、内容について、消費者、事業者両者が、お互いに証明出来るよう心掛ける必要がある。事業者は消費者から信頼確保できる仕組み（電子公証機能もその一部）を構築し、消費者への提供ツールにも、消費者保護の機能（電子公証機能）を含めることが必要である。
(5) 企業間は当事者がほぼ対等なのに対し、消費者-企業間は技術弱者が当事者となるため、技術弱者が不利にならないように相談機関(消費者センターのような)の有効性検討が必要。
(6) 個人情報保護に関しては複数のプレイヤーが係わるため、責任の所在が不明瞭となり易い。そこで統括責任主体の導入についても検討が必要ではないか。
(7) 安全性・信頼性は一方のみで確保できるものではない、まず、事業者サイドとしての考え方を提示し、消費者にも自己責任の概念を取り入れる事が重要である。電子商取引そのものに起因する危険よりも、起因しない危険(パスワード漏洩、カード番号漏洩、類推可能なパスワードの設定など)に対する消費者の意識向上を目指す啓蒙活動が重要である。
(8) リアルの取引においてもリスクはないわけではないが電子商取引を導入することにより消費者に新たなリスクを転嫁しないようにすることが重要である。そのためにはリアルと共通のリスク、電子商取引特有のリスクと分類し、責任とリスク分担の社会的コンセンサスの形成が重要である。

さらには、消費者が必要に応じて簡単に利用できる電子公証センター（紛争が生じた場合、当事者以外で事実関係を証明できる信頼性ある第三者機関）の整備も必要ではなかろうか。

4 取引当事者から見た電子公証

4.1 電子公証モデル

『電子公証』とは、「ネットワーク上の商取引等における電子的交流の安全・信頼性を確保する仕組み」において、その一構成要素として位置づけられ、その中で「“ 誰が（と）”、“ 何を ”、“ 何時 ” 電子的交流を行ったかを証明する仕組み」であるとした。この「仕組み」を最もイメージしやすい事例は、実社会における公証役場を、ネットワーク上の仮想空間に投影し、かつ法的な根拠も有するところの、いわゆる「電子公証センター」であろう。しかし、その場合の「電子公証」は、実社会における公証役場の延長線上でとらえた結果として、当然のことながら “ 公的な第三者機関 ” により運営されることが条件付けられることになる。これに対し、電子公証検討ＷＧでは、契約は「契約自由の原則」のもとに私的自治において取引は行われる必要があるとの基本的な考え方により、もっと幅広い視点から検討を進めることとした。

従って、「証明する」という行為についても “ 公的な第三者機関 ” による行為のみを指すのではなく、例えばデファクトスタンダード化された技術に基づき、あるレベルでの信頼性・安全性が社会的に認知された機構（ＤＥＳによる暗号化、ＲＳＡによるデジタル署名など）を、電子的交流の主体相互に使用することにより、その信頼性・安全性のレベルと担保可能な範囲に応じた証拠力を持たせるような場合も含めることとした。

安全性・信頼性の確保は、当事者の意識そのものであり、商業の慣習として利用され、社会システムとして認知される “ 民間の第三者機関 ” や “ 企業内電子公証システム ” の存在が情報社会においては、重要な役割を担うと考える。

4.1.1 電子公証モデルの必要性とモデルの考え方

このように検討対象の範囲を広めた結果、その対象へのアプローチの視点を予め明確化しておくことが特に必要であり、その方法として「電子的交流の安全・信頼性を確保する仕組み」のモデル化を試みた。そこで作成したモデルは既存の「仕組み」の単なる整理にとどまらず、その適用範囲や、検討課題の所在、今後どのような「仕組み」が求められるのか、といったことに対しても何らかの示唆を与えてくれるはずである。

モデルの作成は、以下の考えに基づいている。

(1) 「仕組み」には、法制度、社会的慣行、当事者相互のルールといった「人的仕組み」と、ＣＰＵによる処理としての「電子的仕組み」（すなわち「電子的機構」）がある。

(2) したがって、「電子的交流の安全・信頼性を確保する仕組み」とは、こうした社会面と技術面からの影響を受けながら発展していく。

(3) その発展プロセスとは、主に「人的仕組み」を、人手を介さず自動的に、かつ確実に実行してくれる手段としての「電子的機構」に置き換えていくプロセスであるといえる。

(4) 置き換えられた「電子的機構」は、その運用のために新たな人的介在を必要とし、その「電子的機構」により確保できる安全・信頼性のレベルは、機構の質だけでなくそうした人的介在の質（すなわち、その運用者がどこまで信頼できるか等）にも依存する。

(5) したがって、そうした人的介在を全く必要としない発展段階が、最終的に理想とする段階である。そのような段階では、電子的交流の主体が全く意識することなく、その電子的交流に関わる情報が、安全な状態で全て記録され、また必要な時にはいつでも取り出せる。

なお、「人的仕組み」を、人手を介さず自動的に、かつ確実に実行してくれる手段としての「電子的機構」に置き換えていくプロセスの例として、暗号化があげられる。すなわち、第二次大戦中、軍事的な電文を暗号解読表に従って、人手で暗号化し（すなわち「人

的仕組み」に対応）、その内容が敵に漏洩するのを防いだわけであり、これに対し、現代では電子メールの内容を、例えばＤＥＳの暗号化ソフト（すなわち「電子的機構」に対応）を使って暗号化している。

また、当事者相互にしか知り得ないような情報で電子メールの交換相手を確認する、といった手段（すなわち「人的仕組み」に対応）に対し、電子認証により相手確認する場合も、同様に「電子的機構」への置き換えがなされたと言える。

4.1.2 電子公証モデルの内容

「人的仕組み」が「電子的機構」に置き換えられて発展していくプロセスを５段階に分け、各々の段階に応じたタイプⅠ～Ⅴのモデルを作成した。これらの各モデルは、どのように発展していくかという視点から作成したものではあるが、それはどちらかというと、考えられるモデルをタイプ分けする上で一貫した視点を与えることが目的である。したがって、これらのモデルは、現在の発展段階がどこであるかを分析することが目的なのではなく、あるシステムを構築しようとする時に、必要とされる安全・信頼性のレベルやコストパフォーマンスに応じて、適用すべきモデルのタイプを選択し、安全・信頼性設計に対して効果的な視点を与えることを主な目的にしている。

(1) タイプⅠモデル

このモデルでは、電子的交流を行う主体Ａと主体Ｂとの間に、安全・信頼性を確保する仕組みとして、電子的機構が全く存在せず、主体相互間で予め決めたルール、または慣行といった人的ルールにより、ある程度の安全・信頼性を確保している。

【　例　】

・何のセキュリティ機構も組み込まれていない電子メールシステムを使用しているが、予め「電子メールを受け取った場合には、受け取った旨の電子メールを必ず返信すること」、あるいは「当事者しか知り得ない情報を必ず付加して電子メールを送ること」といったルールを決めて運用することにより、送達確認や相手確認を行う。

(2) タイプⅡモデル

このモデルでは、人的ルールの一部を電子的機構に置き換え、それを当事者各々の内部に持つことで、安全・信頼性を確保している。この場合、当事者各々が持つ電子的機構は同一ではなく、また、電子的機構を運用するためのルールというものが新たに発生する。しかし、タイプⅠモデルと比較して、ルール全体の負荷はより小さなものとなっており、かつ電子的機構化されたルールはより確実に実行されている。

【　例　】

・暗号化の鍵を安全に保管しておく記憶媒体として、主体ＡはＩＣカードを、主体ＢはＰＣカードを使用する場合。

(3) タイプⅢモデル

タイプⅡモデルにおいては主体Ａ、主体Ｂが異なる電子的機構を内部に持っていたのに対し、こうした電子的機構がデファクトスタンダード化されるなど、一般的に認知されることによって同一の電子的機構を当事者の各々が内部に共有する。またこれに伴って、ルールの負担は更に軽減されることになる。

【　例　】

・標準セキュリティプロトコルとしてＳＳＬによる電子メールを使用する場合。

(4) タイプⅣモデル

公的か否かにかかわらず、一般に認知された第三者機関が提供する電子的機構を当事者各々が利用する。この場合、第三者機関を介在させることで、電子的交流全体の安全・信頼性を高めている。

【　例　】

・電子認証局や、電子的交流に関わる各種証明書（送信・受信日時、内容等）発行局を設ける場合。

(5) タイプＶモデル

法制度を除く人的ルール、及び機構の運用ルールの全てが電子的機構に置き換えられた、理想的段階のモデル。人的介在を全く必要とせず、したがって電子的交流の主体が全く意識することなく、その電子的交流に関わる情報が安全な状態で全て記録され、また必要な時にはいつでも取り出せる。

なお、このような状態はまだ実現するに至っていない。図 4-1 電子公証モデルの説明参照。

電子公証モデル

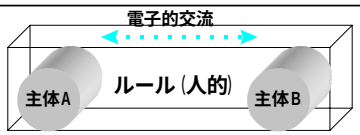
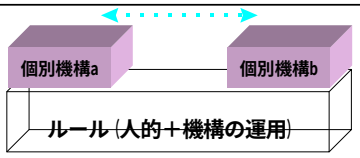
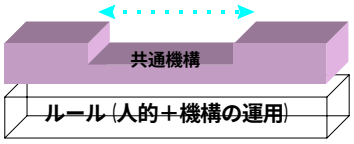
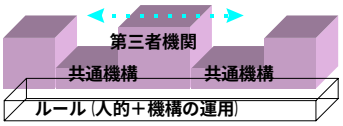
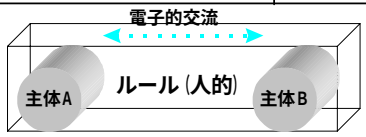
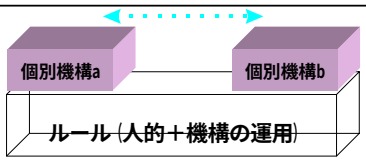
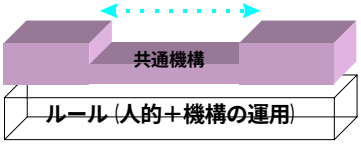
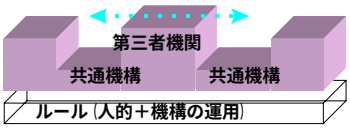
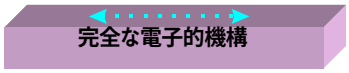
タイプ	モデル	説明
Ⅰ		当事者間において、特に安心･安全の一部を保証する電子的機構をもたない。例えば、何のセキュリティ機構も組み込まれていない電子メールシステムを利用して商取引に関する情報をやり取りしている。
Ⅱ		当事者間に固有の電子的機構を内部に持ち、当事者間のみに通用する仕組みにより安心･安全の一部を保証する。 例えば、当事者間のみの事前取り決めによって、内容／フォーマットなどを規定し暗号化などし商取引情報をやりとりしている状況（従来のEDIに近い状況）
Ⅲ		一般的に認知された電子的機構を当事者のそれぞれが内部 に共有する。例えば、標準セキュリティプロトコルが組み込ま れた電子メール、インターネットEDIアプリケーション等を利用して商取引情報をやり取りしている状況。
Ⅳ		公的／私的を問わず一般に認知された第三者機関の提供･認知する電子的機構を当事者がそれぞれ共有する。 商取引情報の一部または全部はは第三者機関を介してやり取りされる。
Ⅴ		運用ルールがすべて電子的に処理可能な完全な電子的機構例示は困難

図 4-1電子公証モデルの説明

4.1.3 電子公証モデル適用の考え方

安全・信頼性を確保には電子的交流送受信者特定、到達確認、改竄検知、時刻付与、アクセスの記録、プロセス記録、電子保存に関わる仕組みが必要であり、これらの仕組みの各々について「人的仕組み」から「電子的機構」への置き換えが存在し、したがって前述のタイプⅠ～Ⅴのモデルは、システム全体に関してだけではなくこれらの各々の仕組み毎に適用できる。したがってあるシステムを開発する場合、これらの「仕組み」毎に、求められる安全・信頼性のレベルに応じてどのモデルを選択するか、ということを検討すべきであり、こうした視点で検討することは、そのシステムの設計に対し一つの効果的なアプローチを提供してくれるはずである。なお、実際のモデル選択にあたっては、求められる安全・信頼性のレベルだけではなく、その時点で利用できる製品や技術のレベル、そしてコストパフォーマンスからの観点等も必要となる。

電子公証モデルにおける電子的機構と適用技術例

タイプ	モデル	保護対象	「誰が誰と」		「何時」	「何を」	
		機　能	主体の確認	到達確認	時刻確認	保　管	秘　匿
I			－	－	－	－	－
			当事者しか知り得ない情報で相手を確認する	受取った旨の電子メールを必ず返信する	送受信する電子メール中にその日時を記入する	保存対象、期間等、基本的ルールのみ決める	予め取決めた簡易なアルゴリズムで暗号化
II			公開または共通鍵暗号方式による相互認証	－	各々のシステムの時計を使用	追記型記憶媒体（CD－R等）を使用	相手に応じて暗号方式を選択使用
			主体が各々、相手の鍵を個別管理	受取った旨の電子メールを必ず返信する	用途に応じた精度で定期的に時刻合わせする	各々使用する記憶媒体を事前に相互通知	主体が各々、相手の鍵を個別管理
III			PGP方式等による相互認証	X.400等による送達確認	NTP(Network Time Protocol)等で同期をとる	原本性を保証可能な電子保存機構を共有	DES等の標準的な暗号方式を使用
			公開鍵の正当性は各々自己管理	相手が内容も見たものとみなす	同期の精度を予め決めておく	上記電子保存機構の運用ルール	主体が各々、相手の鍵を個別管理
IV			認証局による相互認証	電子公証センターによる配達証明	電子公証センターによるタイムスタンプ	電子公証センターによる内容証明	－
			認証局利用規程	電子公証センター利用規程	電子公証センター利用規程	電子公証センター利用規程	－
V			（ まだ実現されていない ）				

（注）点線より上段は「機構」、下段は「ルール」について記載。

図 4-2電子公証モデルにおける電子的機構と適用技術例

電子公証モデルと適用領域

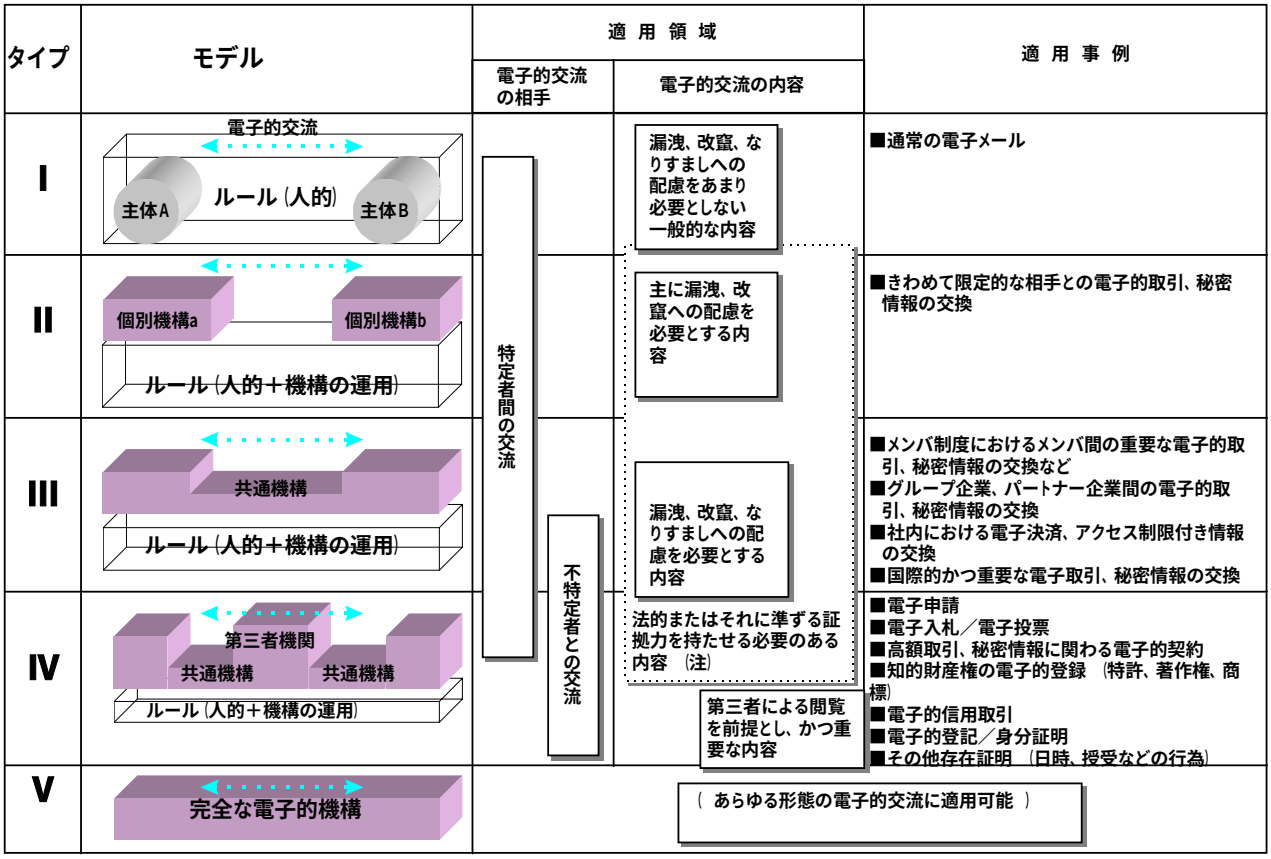


図 4-3電子公証モデルと適用領域

図 4-3 に適用事例を例示したが、電子入札で調達側が公的機関の場合と民間機関の場合必ずしもモデルタイプがIVに限定されるものではなく、IIIの場合もある。特に民間企業の場合は信用する企業の応札という調達企業側の論理が働く。しかし、今後のグローバルな取引にはより高い公正性や透明性が必要となろう。

（注）法的またはそれに準ずる証拠力を持たせるにはタイプIV以外においても、当事者の取り決めや、人的・電子的に証拠力を高める仕組と管理がされておれば、タイプⅠ～IIIにおいても証拠力は十分ある。但し、証拠力の高い、低いという違いがあり、一般には当事者間で紛争となった場合、当事者間の証拠よりも、信頼性ある第三者機関によるものが相対的に証拠力は高いといえる。

さらには、モデルのタイプ毎に、以下の情報を整理しておけばシステムの安全・信頼性設計に大いに役立つものと思われる。

- 利用できる製品や技術の種類、及びその標準化状況
- その機構に対応した運用ルールの事例
- 関連する法律
- 関連するガイドライン

4.2 電子公証システム

企業の電子的情報交換を広くとらえると、図 4-4 企業内と企業間の情報交換の場に示したように企業内の情報交換の場と、企業間の情報交換の場に分けて考えることができる。企業内システムは、従来より企業目的達成のために合目的な手段として導入されている。そのようなシステムは特定企業用途に開発されたものであれ、あるいは汎用的なパッケージソフトウェアによるものであれ、何らかの安全性・信頼性のコントーロールが考慮されて、加えて運用上も組織コントロールのもとに行われている。業務の電子化と取引先の拡大、コストの削減や取引先との企業間ワークフローによる取引の効率化を促進するためのエクストラネット導入によるシームレスなセキュア環境整備の必要性と企業の公明性・情報開示等の社会的要請に対応するため、企業内の安全性・信頼性確保これまで以上に重要となる。これに対して企業間情報交換においては相対的にその歴史も浅く、また実績に乏しい。さらにその発展はオープンネットワーク上で起こると期待されている。従ってその実体としても発展過程としてもモデル I、II、III、IV などと、目的や要求されるレベルに応じて様々であると考えられる。企業間情報交換も企業内情報交換も同じモデルで説明できるが、企業内システムは既に多岐に渡り導入・運用が進んでいるためそのシステム要件を考察するにあたっては一様なアプローチをとるのが困難である。次に企業間と企業内の二つのシステムに考えられる特徴的な実現環境において可能な電子公証システムの要件とシステム概念図を例示する。

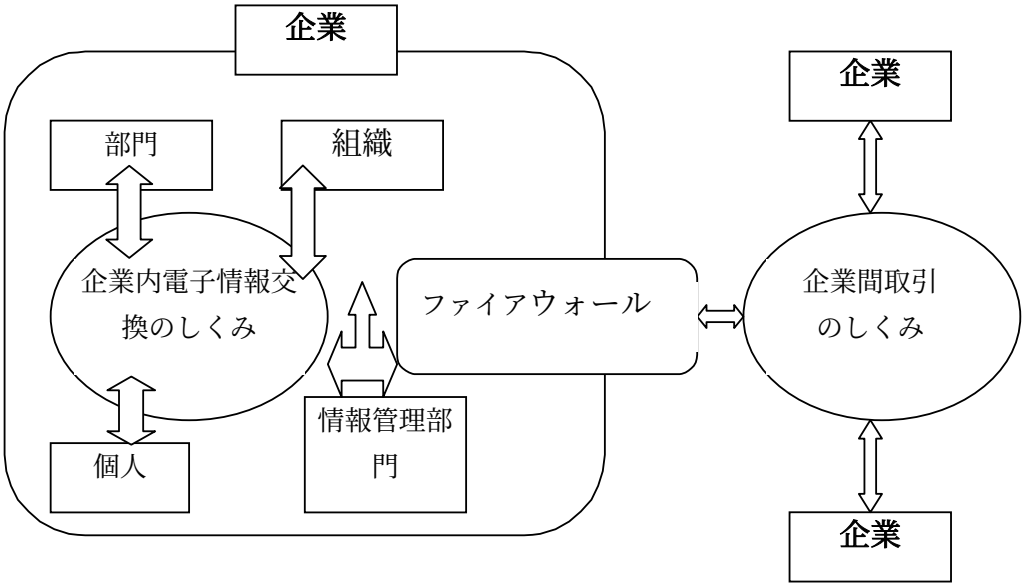


図 4-4企業内と企業間の情報交換の場

4.2.1 企業間の電子公証システム

4.2.1.1 システム要件

ここでは、第三者機関の電子公証センターを介在させることで電子的交流の安全性・信頼性を高めている電子公証モデルのタイプⅣの要求される機能別システム要件、人的ルールを示す。

表 4-1 タイプⅣのシステム要件

機能名	システム要件	人的ルール(運用ルール要件)
送受信者特定機能	認証局の発行する公開鍵証明書を用いて取引相手を確認する。またデジタル署名を付与することも可能とする。認証書が正当なものかどうかの確認を行う。	認証局の利用規定に従う。また互換性のある認証局どうしを使うことを当事者間で取り決める。
到達確認機能	電子公証センターに送受信の仲立ちをしてもらう。	電子公証センターの利用規定に従う。どの公証センターを使うか事前に当事者間で取り決める。
改竄検知機能	電子公証センターの非改竄証明を利用する。	電子公証センターの利用規定に従う。どの公証センターを使うか事前に当事者間で取り決める。
時刻付与機能	電子公証センターの時刻証明を利用する。	電子公証センターの利用規定に従う。どの公証センターを使うか事前に当事者間で取り決める。
電子保存機能	電子公証センターの電子保存サービスを利用する。	電子公証センターの利用規定に従う。どの公証センターを使うか事前に当事者間で取り決める。また、ファイル書式などは当事者間で決定する。
アクセス記録機能	当事者が電子公証センターにアクセス記録を確実にとってもらい、公開するデータを預ける。	当事者は相手がアクセスできる範囲を取り決める。

4.2.1.2 システム概念図（例示）

こららの要件を踏まえて、当事者と電子公証センターの機能をシステム概念図として、示す。

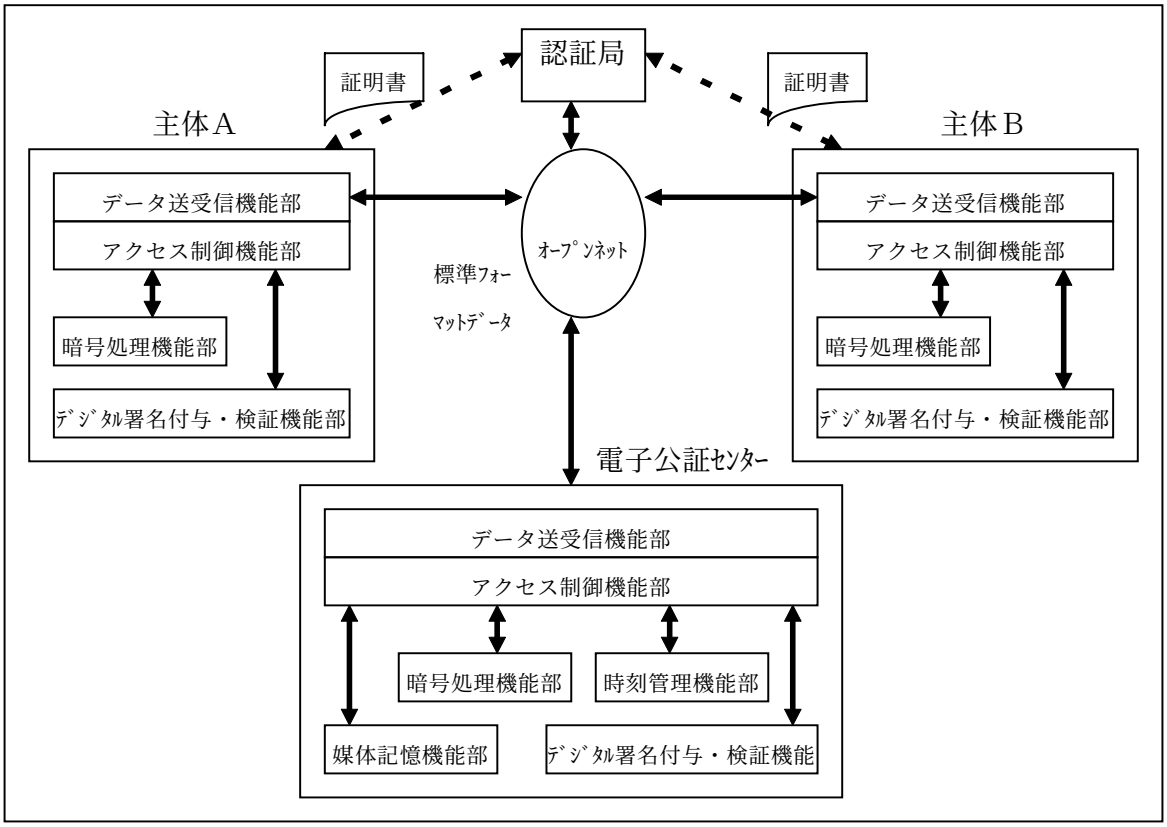


図 4-5 タイプⅣシステム概念図

4.2.2 企業内電子公証システム

4.2.2.1 システム要件

グループウェア、ワークフローツールを使った企業内情報交換のもとで、モデルタイプⅣを想定したシステム要件は以下のようになる。（モデルタイプⅠ、II、III については本文に説明されている。）

表 4-2 タイプⅣのシステム要件

機能名	システム要件	人的ルール（運用ルール要件）
送受信者特定機能	利用者管理機能および企業内認証システム。法律等で規制されるものについては認証局の発行する公開鍵証明書を利用する。	「主管部門あるいは当事者部門において、各アプリケーションの運用規程を制定する」 認証局の利用規定に従う。
到達確認機能	ツールによるでステータスを確認できる機能。分散システム間通信では、標準的なプロトコルで確認できる機能が必要。電子公証センターに送受信の仲立ちをしてもらうことにより、より信憑性を高める。	「同上」 電子公証センターの利用規定に従う。
改竄検知機能	ツールによる公開鍵方式などによる暗号化機能。法律等で規制されるものについては電子公証センターの非改竄証明を利用。	「同上」 電子公証センターの利用規定に従う。
時刻付与機能	ツールによるヘッダ作成機能。法律等で規制されるものについては電子公証センターの時刻証明を利用する。	「同上」 電子公証センターの利用規定に従う。
電子保存機能	ツールによる文書データベース機能、あるいは分散システム間通信においてはトランザクションログ機能。法律等で規制されるものについては電子公証センターの電子保存サービスを利用する。	「同上」 電子公証センターの利用規定に従う。
アクセス制御機能	ID、パスワードによる本人確認機能に加えて、バイオメトリックス等を用いた強化された認証機能。	「同上」
アクセス記録機能	トランザクションログ機能。	「同上」

4.2.2.2 システム概念図（例示）

このような要件に配慮して企業内におけるアクセス管理・電子認証・電子公証システムの構成を想定すると下図のように表すことができる。ネットワーク情報システムの脅威の多くは企業内にあるとの報告があり、ここではバイオメトリックスや一時パスワード発生器を使った強化された利用者認証機能に加えて、アクセス制御を一元管理することを想定している。また、公開鍵暗号による認証機能（認証センター）を使い利用者の他にサーバホストを認証する。公証機能のうち、時刻付与機能、電子保存機能、アクセス記録機能等は独立した専用機能（公証センター）として想定した。これらの機能は必要性に応じて暗号ベースの認証機能とともに外部の公証機能により代用される。

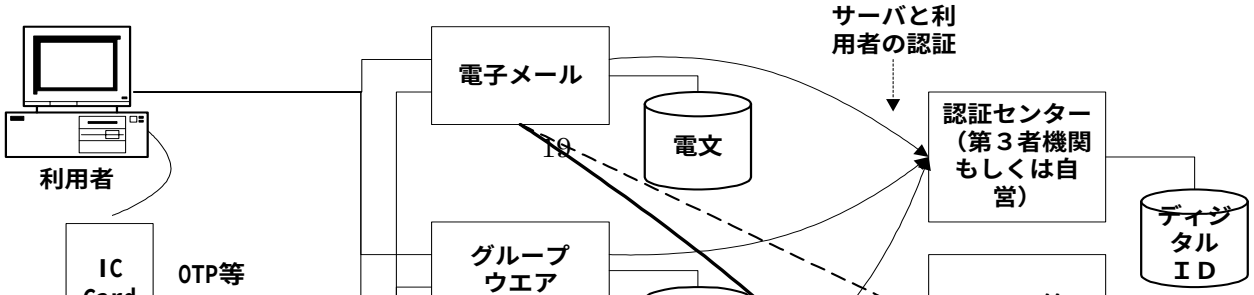


図 4-6企業内電子公証システム図（例示）

5 サービス事業者から見た電子公証

5.1 電子公証センターの主要サービスの内容

(1) 証拠の提出

取引上の紛争が発生し顧客の要請により取引記録等の提出を求められる場面として、

① 紛争相手に証拠があることを提示することによって紛争を抑止

② 調停、裁定の場に当該データを証拠として提出

などが考えられる。提出の方法も提出後の改竄ができないことなどが客観的にわかる方法を採用し、証拠としての有効性を確保する手段を選ぶ等の配慮が必要になる。

(2) 証拠力の有効性の証明

証拠力に疑問が出された場合、調停者、裁定者、紛争相手に対して証拠の信頼性が高く証拠力に疑問がないことを納得させる最大限の努力をする。具体的には、

① 使用技術の信頼性が高いことの証明

② 管理運用が正しく行われ、内部の不正ができにくいことの証明

③ 裁定、調停の場へ、出頭しての証拠の有効性の証言

④ 公証センターの技術、管理運用の認定機関があれば、その認定書の提示

⑤ もし調停者、裁定者の信用の高い公証センターと連携していれば、その連携公証センターの証拠有効性の保証書の提示

(3) 顧客に対するコンサルテーション

① 取引の内容及び段階と個々の公証機能サービスの適合関係

② 公証機能の利用の利点と限界

③ 公証機能と法律の関連（商法、税法）

④ 紛争時の法律相談及び裁定、調停機関の紹介

(4) 基本サービス

時刻証明／内容存在証明／配達確認証明／一般電子保存／保存義務電子保存

5.1.2 時刻証明サービス

当事者以外の第三者によって、文書等に日付時刻を付与するタイムスタンプサービスであり、以下の利用目的が想定される。後に当事者の一方あるいは双方または資格のある第三者からの依頼に基づいてその時刻を証明する。

① 電子文書が確かにその時点で存在した事を証明
　・例：特許のアイデア

② 電子文書が決められた日時までに提出された事を証明
　・例：電子取引所の公開入札、クーリングオフ、電子申請・届出

③ 契約書等の契約日の証明

またタイムスタンプを暗号キーと組合わせることにより、より信頼性の高い暗号化が図れる事から、時刻証明サービスは単独のサービスのみならず配達確認証明サービスや電子保存サービスに付随するサービス機能として位置づけられるものと考えられる。

5.1.3 内容存在証明サービス

誰が、いつ、誰に対して、どのような内容の情報を出したかを証明するサービスである。特に複数の当事者間の利害に関わる文書を改竄から保護するために重要なサービスである。機能要素としては、認証機能（誰が／誰に対して）／時刻証明機能（いつ）／　電子保存機能または暗号化機能（どのような内容を）の組合わせとなる。

本サービスは，以下のような分野で利用される。

① 電子商取引
　例：契約書、注文書、請求書、採用・不採用通知等の内容について、後日の紛争の解決のための証拠として利用

② 電子申請・電子届出等

例１：申請が決められた日時までに正しく提出された事の証明

例２：特許のアイデアを日付とともに記録し後日の証明に備える（先発明主義）

データ自身の内容についての関与は、公証センターの提供するサービスレベルにより異なると考えられる。公証センターが既存の公証人役場における提供サービスと　同等のサービスを提供すると仮定した時には内容の法的適合性まで証明する。通常は　単に存在のみを証明する場合が想定される。サービスレベルと存在証明の機能レベル　については、公証システムを運営する母体との関係から議論されることが必要になる。

5.1.4 配達確認証明サービス

送信者の送信データが間違いなく受信者に配達されたことを証明するサービスである。両当事者の間に第三者機関を置き、送信データをその機関を通じて行うことにより、後日送達の証明を客観的に行うことができる。また確認応答が来ない場合の受信者への文書の再送を代行する事ができる。また送信者からは、送達状態を配達確認センターへ照会する事により、常時確認することができる。

本サービスは、以下のような分野で利用される。

① 電子商取引　　・例：注文書，請求書

② 民事的紛糾　　・例：従来の配達証明郵便の代替

5.1.5 一般電子保存サービス／保存義務電子保存サービス

後日の証拠のため電子的データを保存するサービスである。特に法律面で保存義務が課せられている書類を対象とする場合を保存義務電子保存と呼び、法律とは関係なく一般の利用者が重要書類を保管したい場合を一般電子保存サービスと呼ぶ。

保存義務電子保存について国内では、たとえば商業帳簿およびその営業に関する重要書類（保存期間１０年）、仕訳帳・総勘定元帳（同７年）などの文書がある。

基本的に両者の機能は同様であり、求められる要件としては、以下が考えられる。

① 真正性

データを故意あるいは過失により虚偽入力・書換・消去・混同される事が無いこと。

② 見読性

データの内容を必要に応じて見読可能とする事が容易にできること。

ただし誰でも見せて良いわけではなく、きめ細かいアクセス権制御を必要とする。

③ 保存性

保存期間内において復元可能な状態でデータを保存すること。

保存する書類により要件は異なるが、場合によっては地震・火災等の天災に対する備えも必要になってくる。保存の形式については当事者以外（公証システム自身も含めて）閲覧できない形式の場合と、公証システムの運用者が閲覧の資格を判定し、解読できる形式の場合の２形式が考えられる。

5.2 特徴的な公証サービスの例

基本的な公証サービスを特定領域に適用する、あるいは付加的な機能を組み合わせることによって、どのようなタイプの電子公証センターが実現するかを具体的に例示する。

5.2.1 契約書締結型

電子商取引等において、当事者間のデジタル文書による契約書などの取り次ぎ、保管を行うサービスである。公証センターを経由する事により、確実な送達保証と「言った／言わない」のトラブルの防止を図ることができる。また保管サービスにより，後日トラブルが発生した際に、契約内容等の第三者による証明を得ることができる。

さらに、契約に至るまでの履歴を管理するサービスまで行えば、当該契約成立の経緯も公証しておく事ができる。後日契約内容を更新する場合は、公証番号をキーとして指定することにより新版を作成する事ができる。

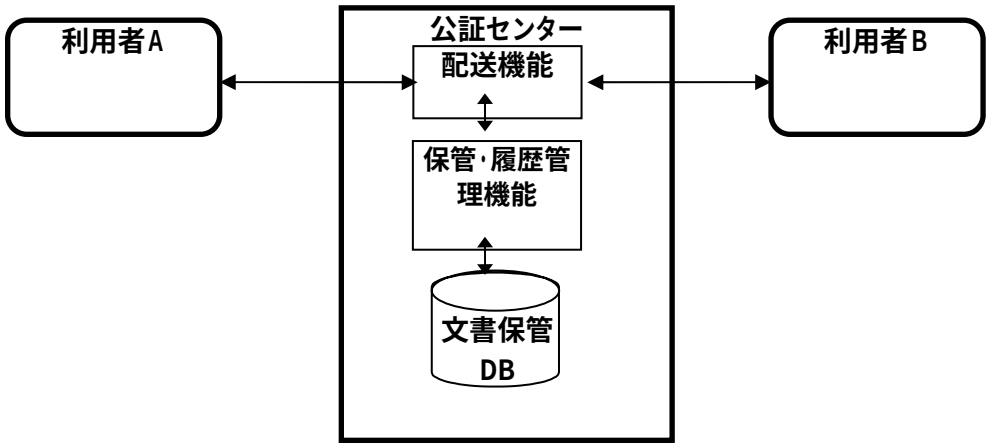


図 5-1配達確認証明サービス

5.2.2 公証番号重視型

特に「公証番号」に重要な意味を持たせ、デジタル文書を直接送付・配布する代わりに公証番号の送付で済ませるなどのサービスである。取引情報などでは電子公証システムに登録したことを「公証番号の通知」をもって行い、当該通知がなされた場合はその取引情報が第三者に保全されている事を保証するような使い方が考えられる。

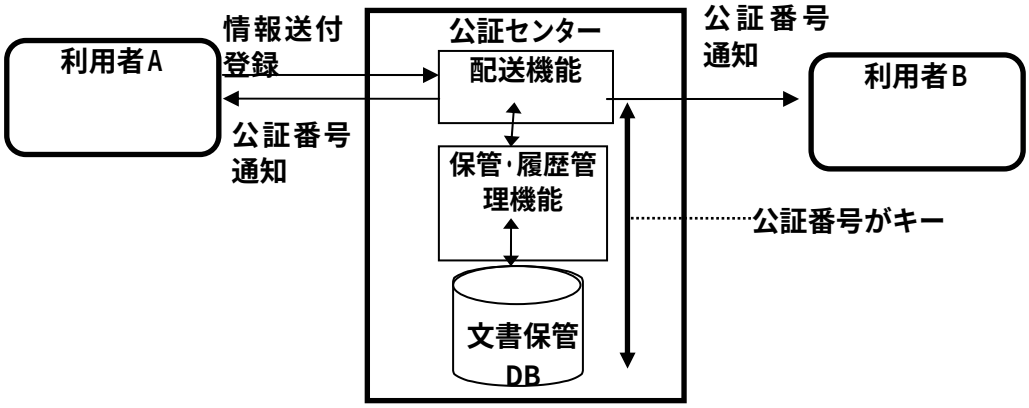


図 5-2公証番号による取引情報通知

5.2.3 デジタル情報保存型

デジタル商品，ソフトウェアなど商品そのものがネットワーク上で流通される場合、当該商品を購入した利用者は商品が正しく送信されてきたか、偽の商店から偽のソフトウェアなどを購入してはいないかなどの危惧がある。これに対し、すでに正規の商品がしかるべき第三者に保管され、簡単に照合できるしくみを提供することが必要となる。

これを想定してデジタル情報を登録し保管する機能を提供するタイプのサービスであり、登録した時点のその情報の存在とその内容を明確に証明する。

また安全に保管するための貸金庫的な機能も期待される。いわばデジタル情報の電子保管サービスである。この場合公証番号は索引するためのキーとして使われる。

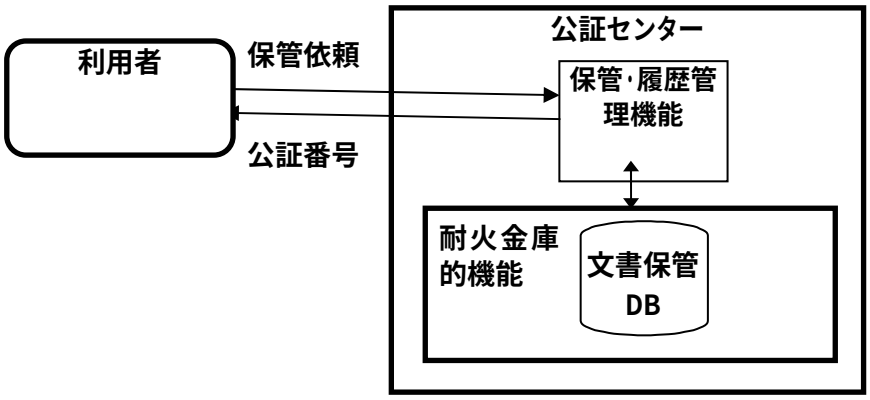


図 5-3デジタル情報保存サービス

5.2.4 タイムスタンプ利用型

入札、期限管理、先着順受付等、到着時刻が重要な意味を持ち、その後の契約の成立等を左右する場合に利用するサービスである。ネットワーク上の遅延やネットワークの障害の扱いが問題となる可能性がある。公証センターとしては、タイムスタンプの付与サービスに付随して、ネットワークの出入り口における情報のやり取りに関し、様々なレベルで履歴（ログ）を取得し，後日の紛争時に事実を証明する必要がある。

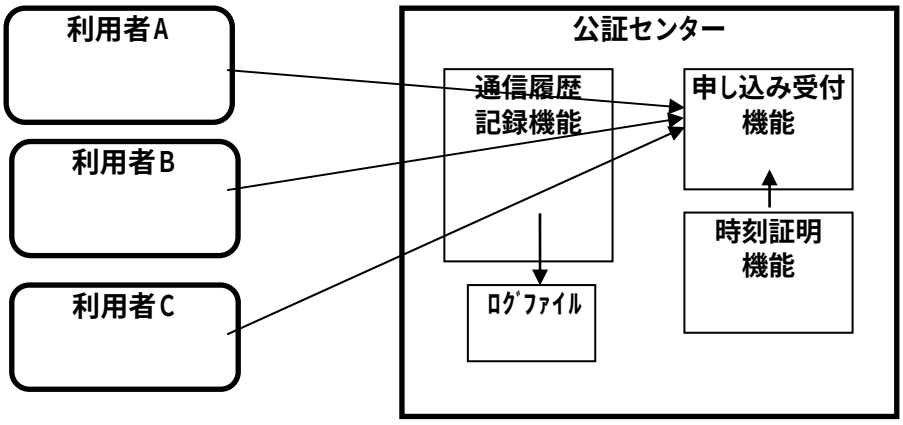


図 5-4タイムスタンプ利用型における通信ログの位置付け

5.2.5 広告情報保証型

公証センターが発行する公証番号により、ホームページなどの作成元の身元を保証するサービスが考えられる。これによってたとえば一流企業の名を騙った偽りの広告などは防ぐことができる。さらに広告の内容そのものを公証センターへ登録するサービスならば、利用者は広告の記述内容を法的に担保することができる。

ただし身元や広告の内容を保証する事ができても、当該業者が信頼できるかどうかは，また別の問題である。これについては公証とは別に企業情報や広告の内容についてあらかじめ審査し登録しておく「格付け機関」の存在が必要になろう。

広告情報に限らず、ホームページから参照される情報そのものに極めて厳密性を要求される場合、たとえば取引条件の提示や学術論文などについても、どの時点のどの内容の情報が本来参照されるべきものであるかを保証する必要がある場合も同様の公証サービスが期待される。

5.3 電子公証センターの運営主体について

電子公証センターの運営主体として、大きく分けると公的機関と私的機関が考えられる。

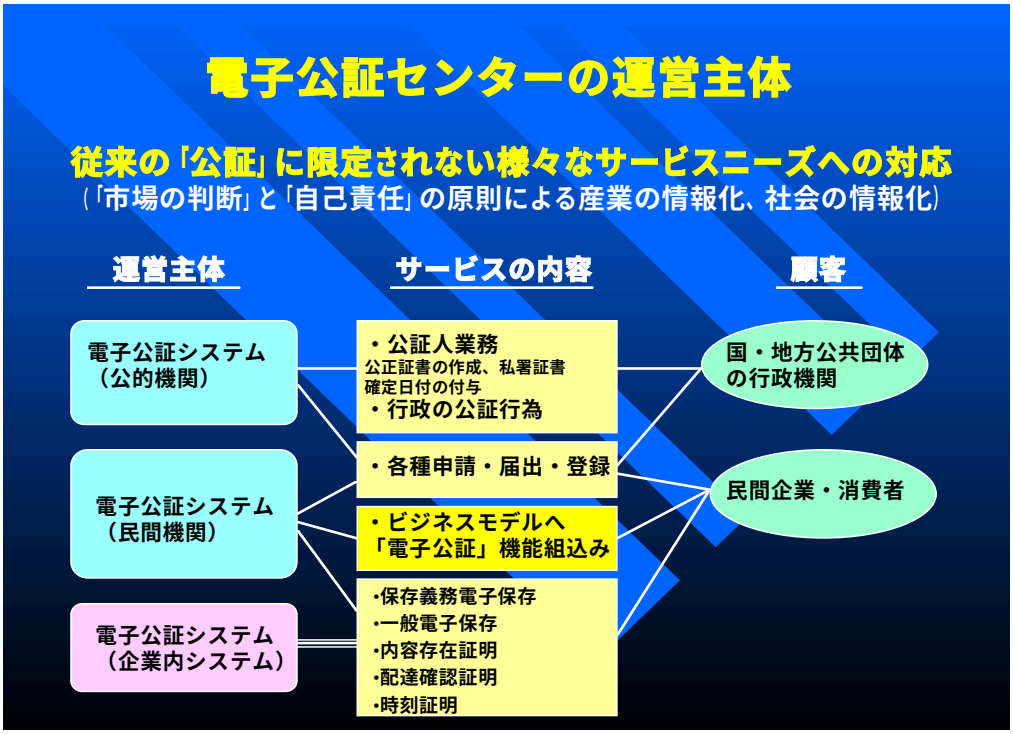


図 5-5電子公証システムの運営主体（例）

公的機関の公証業務は今後とも重要な役割が期待される。一方私的機関（事業会社）が電子公証センターを運用する場合、ビジネスとして成立すると思う誰が行ってもよいが、現時点で事業者たりうる主体を列記する。

① 認証サービス事業者が公証サービスを加える。
② 電子署名サービス事業者が公証サービスを加える。
③ 優れた公証技術開発者がそれを武器に参入する。
④ 電子商取引モール運営者がモールの付帯サービスとして行う。
⑤ （仮）電子商取引推進協会が電子取引業界の発展のため行う。
⑥ 電子商取引保険会社が行う。

既に米国では民間のサービスが開始され、個々のビジネスモデルの中に電子公証機能の組み込みがされている。従来の「公証」に限定されない様々なサービスニーズへの対応が必要であり、「市場の判断」と「自己責任」の原則による産業の情報化、社会の情報化に向け市場形成が望ましい。顧客が公証センターに期待するサービス内容としては、証拠の有効性、コスト、利便性などがある。その中でユーザにより、又は個々の取引の特性により、あるサービスは重視し、あるサービスはそれほど重視しない、といった違いにもとづき顧客が一番適合していると思われる公証センター又はサービス方式を選ぶことになる。

5.4 電子公証センターの要件

公証センターで考慮すべき要件は次の項目が考えられる。

(1) 信頼性要件

信頼性の最大要因は安全性の追求にあるが、運用上の信頼性についても公開、明示することが求められる。たとえば、どのようなセキュリティレベルの技術や情報機器を利用しているか、運用プロセスにおいてどのようにセキュリティを高めているか、運用にたずさわる要員の信頼性をどのように確保しているか、などにつきそれぞれ標準規定を明文化し、顧客などに対して情報公開する必要がある。

仮に業界の自主団体として公証センターの認定､格付け機関などが設立された場合、積極的に高い評価を得るべく情報を公開し監査を受け入れることも必要となる。また実績や財務状況といった経営上の評価も極めて重要となる。

(2) 安全性要件（安全管理面）

安全管理面について電子公証センターとして、天災、外部および内部からの不正等の脅威に対しユーザが安心して利用できるように、すでに策定されているいくつかの安全基準に準拠していることがまず必要である。又その内容を積極的に公表しユーザに安心感を与えることと、利用約款等で安全基準を明示する事も必要であろう。

① 地震等の天災に対しては、地震対策の施された建物に設置する。
遠隔地にバックアップセンターを置く等が考えられる。

② 機器の故障によるデータの破壊に対してはバックアップ機器を設置する。

③ 外部からの不正に対しては、あるレベル以上の安全対策を持つ必要がある。紛争時に証拠となるデータを保存しているので、相手は意図的に外部から侵入し、データの破壊をする可能性が高い。この点が、自社に公証機能を持つか、専門の公証センターを利用するかの判断ポイントになる可能性がある。

④ 内部からの不正に対し、管理面からデータの破壊、改竄をしにくい仕組みを構築しておくことが必要である。技術的に破壊または改竄できない手段を採用し、管理に依存しないで対策がとる方が、安全信頼面及びコスト面でも有利であろう。

さらにオープンネットワーク上で取引が行われることを考えると、世界規模での商取引も視野に入れ、２４時間、３６５日運用を目指す必要がある。

しかし、公証センターのビジネス自体を考えると，対処すべき安全性の範囲とレベルは価格との関係で、運用者とユーザの選択範囲である。従って、すでにある安全基準に準拠するレベルで特段必須要件を定める必要は現時点では認められない。

(3) 技術要件

公証センターが具備すべき主要技術要件を提供サービス別に列挙する。

① 全般に必要な技術
・暗号技術／認証技術／電子署名技術／鍵管理技術／不正アクセス検出技術

② 電子保管サービスに必要な技術
・耐災害電子保存技術／耐不正アクセス電子保存技術／高速検索技術　／満期日管理技術

③ 配達確認証明サービスに必要な技術
・標準的配達確認方式

④ 時刻証明サービスに必要な技術
・正確な時計の実現技術／時刻の改竄防止技術／タイムスタンプ・アルゴリズム／ラッシュアワー時にも公平性を保証する電子データ操作技術

これら技術は、利用者の利便性やサービス提供コスト低減のためには国際的な観点で標準化されることが望ましい。たとえば認証機関が現在採用している技術などはある程度公開されており、安全性の評価が得られているものを利用することが一つの方法である。ただし最終的にどの技術を具備すべきかについてはサービス事業者の取捨選択に委ねるべきである。

(4) 利便性要件

利用者の利用要件により公証センターが提供するサービスレベルが幾つかに分類さ

れるのと同様に、操作方法や利用資格などについてもレベルに応じて選択可能であることが望ましい。また複数の同種サービスを利用する場合には、それぞれの採用技術については標準化されていることが望ましい。利用者が不特定多数に及ぶことを前提とする場合には、容易に利用でき、場合によっては利用補助機能（HELP など）の提供について工夫されることが望ましい。

(5) 価格要件

提供されるサービスにより価格設定が行われることが基本と考えられるが、（３）同様、不特定多数が容易に利用できるような価格設定がなされることが望まれる。特に書留郵便に相当するタイムスタンプ利用型などのサービスにおいては可能な限り低価格とすることが必要である。

(6) 相互運用性要件

公証機関が提供するサービスの場合には、たとえば印鑑証明に相当するデータ内容公証型サービスの提供にあっては、少なくとも日本国内どこの公証センターを利用したとしてもいい同質のサービスであり、かつ相互に内容の互換性が保証されていなければならない。

民間機関によるサービスの場合には、運営母体の選択範囲であるとも考えられるため一様にガイドラインを制定すべきか議論のあるところである。しかし、少なくとも利用者において混乱が生じないことが最低の条件と考えられる。

利用技術の互換性が期待できる場合には、各々の公証センター間で保持するデータあるいは事実を電子的に相互利用するサービスなどが同時に期待できる。

相互運用性を確保するには、

① 設立された公証センター同士が認め合って実現される場合、互いに同一の技術を利用して公証サービスが提供されている場合が想定され、公証センター間の関係についてはそれぞれの公証センターがフラットな関係と捉えられる。

② 複数の公証センターが共通の他の公証センターによって認められることによって実現される場合、少なくとも共通の公証センターとその認める複数の公証センターとの間では同一の技術が利用できることが想定される。公証センター間の関係については共通な公証センターとそれに認知される公証センター群との階層的な関係と捉えることができる。

5.5 認証機関との連携

認証機関の役割は、オープンネットワーク上での本人確認と交換データの改竄、盗聴の防止、否認拒否などのための認証書を発行することにある。公証センターは基本的にこの認証書を利用し、交換データの安全性や証明の発行時における公証センター自身の正しさを証明すると同時に、公証センターの利用者の本人認証などにも利用する。

公証センターとの関係から認証機関に求められる要件について以下にまとめる。

(1) 認証機関と公証センターが別の運営母体により設立される場合

認証機関と公証センターが別の運営母体で運営されているのが一般的と考えられる。この場合には、認証書自身の信頼性は独立した認証機関により提示されるので、公証センターはその利用者に対しては認証書を保持することを前提に各種サービスを提供することとなる。

(2) 認証機関と公証センターが同一運営母体により設立される場合

認証書は公証対象データに対する公証センターの署名として利用することが想定されるため、認証書の発行体と公証センターは連携していなければ参加者の特定時に不都合が生じるものと予想される。しかし公証センターが自分自身の認証を行うと、利用者が公証センターを信頼するに値するかを確認することは困難になるものと考えられる。

具体的には、利用者に対し公証センターを詐称することや、虚偽の事実を保持した

り、本来保管すべき事実を隠蔽したりする事も可能となると考えられる。これに対しては、運営母体の信頼性や運用内容による信頼性を持って代えることも想定されるが、一般的には上位の認証機関に認証されて認証書発行を行う事が必要と考えられる。認証機関の階層構造については認証局ガイドラインなどの他の検討内容を適用することが望ましい。

(3) 複数の認証機関により発行された認証書を利用する場合

公証センターの利用者の保持する認証書が各々別の認証機関により発行されたものであったり、認証書の発行についての技術が多様になった場合には、公証センターも多様な利用者を想定して本人確認を行うために対応した可能な限りの技術を用意する事が求められる。しかし、すべての技術を網羅する事は容易でないものと考えられるため、公証センターでは利用者に対し提供できる技術内容を制限してそのサービスを提供する事が考えられ、その場合にはこれを利用者に明示する必要がある。

5.6 電子公証センターの責任の範囲

電子公証に係わる問題が発生した場合でも、その内容によっては電子公証センター以外にもいくつかの機関がその問題に関与している可能性がある。そのためその問題に対する責任も必ずしもすべて電子公証センターに帰着するものではない。

表 5-1 主な責任範囲の分類

問題	利用者	通信業者	認証機関	格付機関	公証センター
内容不正	○				△内容証明
データ未達		○			○システムダウン
データ誤達		△			○運用ミス
改竄／漏洩		△	○		○セキュリティ技術
データ破壊／消失					○運用ミス セキュリティ技術
利用資格不備	○		○	○	
証拠力不備	△				○運用ミス セキュリティ技術

○：積極的に責任がある　△：なんらかの責任がありうる

電子公証センターの基本的責任については、個々の公証センターの事業特性によって責任範囲がバラツク可能性が高いが、コストが安くなれば責任範囲は当然狭くなり、顧客はその中から利用コストとの兼ね合いで選択することになる。責任範囲は契約約款、利用約款で提示されると思われる

(1) 証拠の有効性の保証

紛争時の公証証拠の有効性を保証しているかの問題又は、調停・裁判で証拠の有効が認められなかったときの補償問題等は議論となる点であろう。一般的には公証センターは証拠の有効性は保証できないと思われるが、もし有効性が公証センターの採用している公証技術、管理運用により認められなかったときは、何らかの補償が問題になると思われる。フォーマット上の問題で証拠としての有効性が認められなかった場合はコンサルタント契約等の問題になる可能性がある。

(2) 安全対策に対する義務と免責事項

公証センターに保管されている情報が、万が一外部ハッカーにより破壊された場合の補償はどうなるか、公証センターはハッカー対策をどの程度まで行う義務があるか、天災等の不可抗力で保管データが破壊されたときの免責の範囲はどこまでか、同じくどの程度の安全対策を行う義務があるか、等も議論になる点である。

安全対策は公証センターの設備投資額に直結する問題となるので、高い安全対策を求めれば、当然利用コストは高くなる。

(3) 損害に対する補償

証拠の有効性の証明の失敗及び公証データの消滅等によるビジネス上の損害発生に対する補償は、公証センターではリスクの程度が読み切れず当面負担できないと思われる。将来リスクの程度が読めるようになれば保険会社が事業化する可能性が高い。

(4) 事業継続が困難になった場合

事業継続が困難になった場合でも、同様のサービス提供者に移管できることが望ましい。利用者との間でその可否につき利用約款などを通してあらかじめ確認する必要がある。

5.7 電子公証センター実現上の課題など

電子商取引の場において電子公証事業が成立する要件としては下記が考えられる。

(1) 公証機能を利用するユーザが事業として成立する規模で存在する事。

① 電子商取引によるビジネス規模がある程度まで大きくなる。
② 一件あたりの取引金額が大きく、利用コストを負担できる。

(2) 第三者が公証サービスを提供するメリットがある。

① 安全対策にコストがかかり、自社システムのほうが固定費が高い。
② 使用頻度が少なく、自社システムのほうがコストが割高になる。
③ 紛争時の相談、コンサルタント内容が充実している。

(3) 公証センターが社会インフラとして認知される。

電子商取引がまだ規模の小さい段階では、採算性からみても公証センター単独事業での私的事業体を維持するのは難しいと思われるが、北米などではある有望市場に限定した配達確認サービスや電子保存サービスに特化した企業が出て来ていることなどからも、電子商取引の拡大する将来的には事業性に富むものと考えられる。

当面実現の可能性が比較的高いと思われる事業形態として、

① 認証サービス等との共同事業
② 電子金庫サービス
③ 電子公証技術ソフトの販売
④ 高額電子商取引業者の自社内システム

などが考えられる。尚採算をあまり考えなくてよい公的機関は別途存在すると考える。

6 今後の検討課題

電子公証の視点から今後の検討が必要と思われる課題について整理すると

(1) オープンなＥＤＩ実現環境の検討

安心な電子商取引の実現には認証、電子公証以外にもその取引の形態（例えば不特定多数企業との初めての取引き場合）により、利用が想定されるさまざまな機能（取引時：認証、電子公証、運用能力格付、企業格付、取引処分、トラブル発生時：調停、損害補填、周辺機能：取引監視、認定、監査）に応じた検討が必要である。

(2) 電子公証サービス事業実現のための環境整備

・海外の事業動向と我が国の事業の在り方
・電子公証センター運用ガイドライン
・利用約款
・相互運用性（公的機関、海外の機関等）

(3) ビジネスモデルへの電子公証機能の組み込みと検証

情報技術を活用した新たなビジネスモデルの取り組みと、そこに「電子公証」機能が組み込まれていくアプローチが重要となる。

(4) 事業者からみた法制度の適用化検討

証拠としての電子保存の証明力（証拠力）向上の要件整理
電子情報と紙混在時の取り扱い時のデータの同一性確保

(5) 企業内外の業務のシームレスなセキュアな環境整備

・企業内の認証・電子公証システムの在り方