Ｈ９－ＷＧ１５－１

電子公証システムガイドライン

（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

本報告書は、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。

１９９７年５月に通産省より、「デジタル経済の時代に向けて～世界的な電子商取引の発展のために～」と題する政策の基本的スタンスに関するペーパーが公表され、５原則の１つに「安全と信頼性」がある。

商取引を安心して行う上で、重要なことは安全と信頼性確保であるが、オープンなネットワークとデジタルをキーワードとする電子商取引にはリアルとは別の新たな問題点が想定される。

そこで、企業間取引、企業内業務、消費者―企業間における様々な取引モデルの業務フローを材料に課題やニーズを検討し、『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、特に取引当事者間の信頼性確保の視点から「“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。

その上で、取引当事者自らのシステム構築にも効果的なアプローチを提供する「取引当事者が安全と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」の概念を作成し、タイプ別の適用事例（案）を提示した。

一方信頼性ある第三者機関の活用を踏まえ、電子公証センターの在り方、主要サービスの内容、運用の要件、実現上の課題等を示した。

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。

また、添付資料では北米の電子公証関連サービス事業の事例（証拠力を高め、紛争の防止や解決）をはじめ、電子公証関連技術、電子保存に関する動向等を掲載する。

電子商取引は始った所であり、電子公証に対する実運用面からの課題やニーズを的確に把握し、適宜見直すことが肝要である。

また、ガイドラインというよりも、概説書的な内容になった面が否めないが、社会システムとしての合意形成と電子商取引の促進にに少しでもお役に立てれば幸いである。

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。例えば、ファイアーウオールへの電子公証機能拡張も有効な手段の１つとなる。

(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) 自由心証主義にもと、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「安全」であり「信頼」である。「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、「信頼」とは取引当事者間の「信頼」構築を意味している。ここでは、「安全」と「信頼」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。

リアルの世界の商取引は、取引相手への訪問、電話、ＦＡＸで行うのが一般的である。では、インターネットなどのネットワークによる商取引とリアルの世界の商取引とは、何が異なるのであろうか。このあたりが、電子商取引を一般的に広めていく上でのポイントとなる。

1.1.2 電子商取引のキーワード

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、「ネットワーク」そして「デジタル」を前提としている点である。この前提を考慮すると、安心を得るためには、リアルの世界にはない別の要素も必要となってくる。

ネットワークは、電話や郵便、ＦＡＸに変わる手段であると同時に、物流もかねている場合がある。リアルの世界以上に、相手への到達や時間に対する考え方を厳密に管理する必要がある。例えば、インターネットを使用する場合、現状では発信元から受取人までの経路が保証されていないケースが一般的である。また、相手方がいつ受け取ったかを確認するのは困難である。発信した情報が相手に確実に届いているのか、相手が何時その情報を受け取ったのか、などのチェックのために、リアルの世界とは異なる環境が必要となる。

また、デジタルは、明らかにリアルの世界にはないフォーマットであり、これにより保存・保管に対する考え方をこれまでと変える必要がある。何故ならば、ハードディスクなど、磁気媒体上のデータは完全な複製が容易なこと、保存されている状態（デジタル情報）では人間の目で見ることができないことなど、原本や見読性という考え方がこれまでの紙ベースと非常に異なる性質のものであるからだ。

今後、電子商取引が限定された当事者間で行う商行為ではなく、個人間の取引を含めて広く受け入れられるには、安心を得るために必要な新たな機能が効果的に提供される必要がある。リアルの世界とは異なる、ネットワークやデジタルなど、電子商取引の特異性を十分に考慮した機能の提供である。

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各機能をまとめてみる。ここでは、機能を３つの大きなカテゴリ（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）に分けた。

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、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。例えば、新たに商取引を開始する場合には、取引相手の信用度をチェックするという意味で企業格付を利用するが、次回以降、継続の取引に毎回必要となるわけではない。さらに例を挙げれば、クローズドなＥＤＩとオープンなＥＤＩを比較しても、取引対象があらかじめ特定できるケースとそうでないケースとでは、必要な機能は自ずと異なってくる。

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。トラブルの種類は、リアルの世界とは異なるが、必要な機能としては同様なものとなろう。

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。

次項では、各カテゴリに含まれる機能を簡単に説明する。詳細説明は、添付資料編を参照されたい。

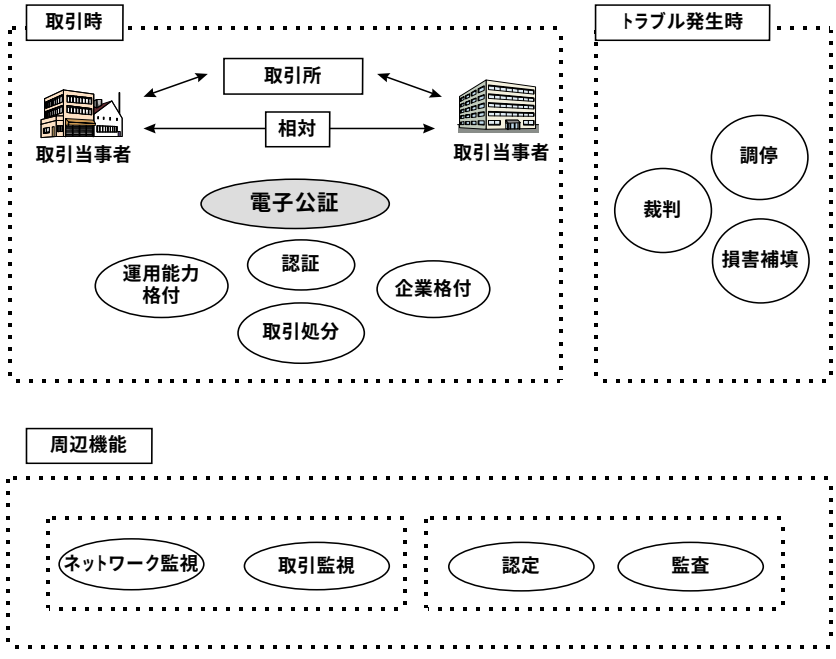


図 1-1安心な電子商取引を行うために使用すると想定される機能分類

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。本ガイドラインでは、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。

1.3 電子商取引と電子公証

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。選択は、取引の当事者が判断を行うことになろう。

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。ネットワークおよびデジタルをキーワードとして考えた場合、「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」ことは非常に重要である。まさしくリアルの世界とは異なる機能を要求されている部分である。

2 電子公証概論

2.1 電子公証の役割

１章の「安心な電子商取引実現に向けて」において安心な電子商取引には安全と信頼性確保が不可欠であると述べた。電子商取引をする場合前述したように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維持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。

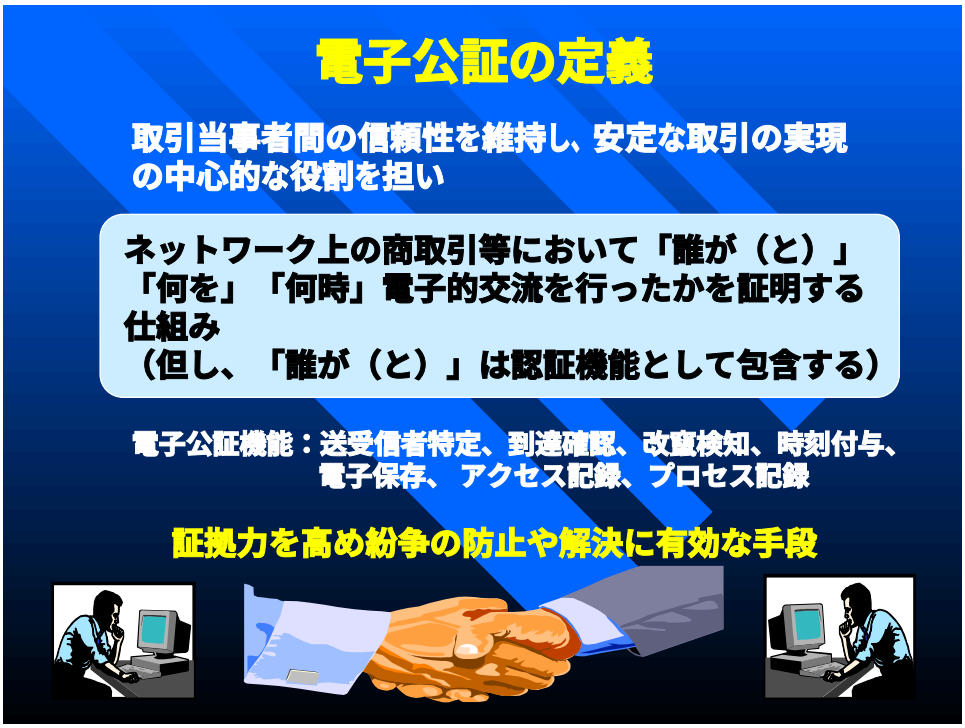


図 2-1電子公証とは

2.3 電子公証と認証

認証局（Certification　Authority）とは

「定義」

公開鍵暗号方式において、申請者の公開鍵に対してその公開鍵が申請者自身のものであることを証明し、それに基づき認証書を発行することの他、認証書の送付、申請者の公開鍵の登録・管理、認証局自身の鍵の生成・管理、認証書の執行登録・管理を行う機関。尚、認証書のフォーマットは、ＩＴＵ Ｘ．５０９で定められており、申請者の公開鍵、申請者のＩＤ、有効期間、認証書の署名（デジタル署名）などが含まれる。

「解説」

認証書の発行に際しては、事前にユーザーの本人情報が登録され、本人であることが証明されることが前提となる。

なお、この本人情報の登録は、認証局が行っても良いし、認証局とは別の機関が行っても良い。

以上のように認証の機能として電子商取引をする場合の取引構成物、構成内容を認証（個人、法人、金融機関、ネットワーク構成機器：サーバー等）することがある。

例えば、お店で買い物をする場合を考えてみると、お互いの顔を見、商品を見ながらこれをください、はいどうぞという形で契約が成立する訳であるが、これが遠隔の取引相手と電子的に交渉が行われるとなると、取引相手が本当に存在し、間違いなくその本人に間違いないか、さらに取引の存在や内容（注文の品名、数量等）の真正性が証明される必要がある。

2.4 オープンなＥＤＩからの視点

電子商取引は企業間、企業内、消費者―企業間の場面において利用がある。オープンなネットワークを利用した取引が、それぞれの場面において、検討され、実験され、商用開始が行われているが、これらオープンなネットワークにおける特定・不特定多数との取引について概観する。

2.4.1 企業間取引の視点

世界で現在１８０、０００社程度の企業がＥＤＩを導入しているが、その多くが大企業を中心とした企業群である。ポテンシャルとしては２００万社が利用するとの推定もある（ACTRA 社の説明によると）中で現状の企業間ＥＤＩがさほど普及しない理由として、

◇固有の通信プロトコル
◇取引先毎のフォーマット設定
◇業務システムとの統合が困難
◇コスト構造の問題

等があげられている。これらの問題を解決する可能性があるものとしてオープン・ネットワーク上でのＥＤＩの１つである「インターネットＥＤＩ」の利用が急速に注目を浴びつつある。

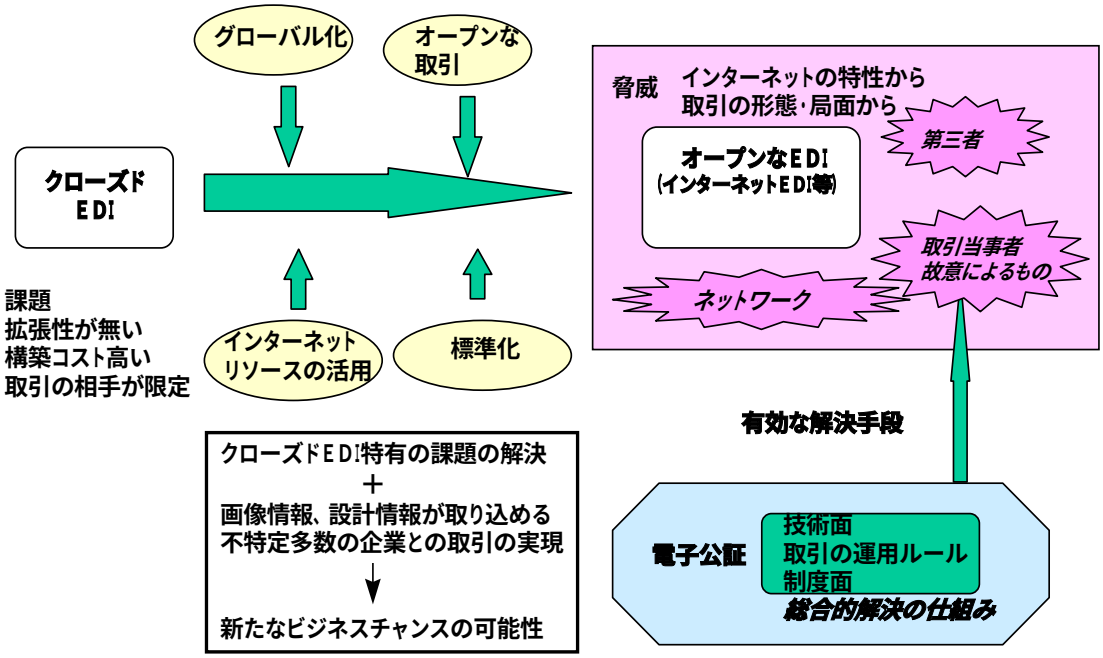


図 2-2オープンなＥＤＩと電子公証

このインターネットＥＤＩは引合から決済のプロセスが中心であるが、取り扱える情報が画像、設計情報とビジュアルに表現可能であること、システムの構築が安価であること、相互運用性があることにより、中小企業への普及が可能である等の特徴を有す。

さらに、オープンなネットワークの特性を利用し、グローバルに不特定多数企業間を対象に（例えばＷｅｂを利用）、広く募集を行い良い製品、高度な技術を獲得する手段としても着目されている。本プロセスは基本契約締結前の初めての取引企業も含めた電子的やり取りであり、色々なリスクを有しているため、１章で説明したような「安心な電子商取引実現に向けた仕組み」の検討と整備が重要となる。しかし、これらの仕組みの検討もこれからであり、実現可能な部分（例えば募集から提案までとか）から進められ、ニーズの顕在化、環境整備の兼ね合いから、電子化の領域が広がるであろう。

米国におけるインターネットＥＤＩの動向は添付資料参照

2.4.2 企業内業務における視点

企業では現在、ネットワークを用いた情報化、電子化が進行している。企業内部の諸プロセスにおける情報交換を電子化し、迅速な処理、意思決定のためのインフラ整備が整い

つつある。これらの電子化においては、インターネット技術が積極的に活用されており、これによりハードウェアコスト、ソフトウェアコスト、インテグレーションコスト、を低減することが可能となっている。このような技術の代表的なものとして、電子メール、ＷＷＷサーバ・クライアントシステム、電子ニュース、ＦＴＰ等がある。これらはインターネットの標準的な通信プロトコルの上に構築されたものであり、企業内の情報交換に留まらず、そのオープン性ゆえに企業外との情報交換にも効果的に利用されようとしている。このようなコミュニケーションの環境は今後とも進化・発展していくと考えられている。

ネットワークの高速化と低価格化、コンピュータのコストパフォーマンスの向上、メディアの融合化を促進する周辺機器・装置の開発、オブジェクト指向技術などを利用した新たなソフトウェア製品の出現等、相乗・複合効果により情報はますます高度に処理されようとしている。通信やネットワークの利用形態も多様化しており、モバイルコンピューティング、テレワーク、コンピュータテレフォーニー、電子会議などが導入されようとしている。このように既存の処理形態の電子化が進行する一方で、新たなコミュニケーション環境を積極的に活用する試みが始まっている。

このような環境では、各構成メンバーがパーソナルコンピュータを利用し、いわば分散処理的に業務を処理する。ビジネス環境がこのような比較的オープンな処理環境に移行しつつあること、またもともとビジネス利用を想定していないインターネットによる通信環境であること、さらに、上に述べたように電子化の割合、蓄積量が多くなる程、問題点や脅威は増大していくものと予想される。従って、従来のホストコンピュータでの集中管理形態であまり意識されなかった問題点や脅威点を再度検討しておく必要がある。

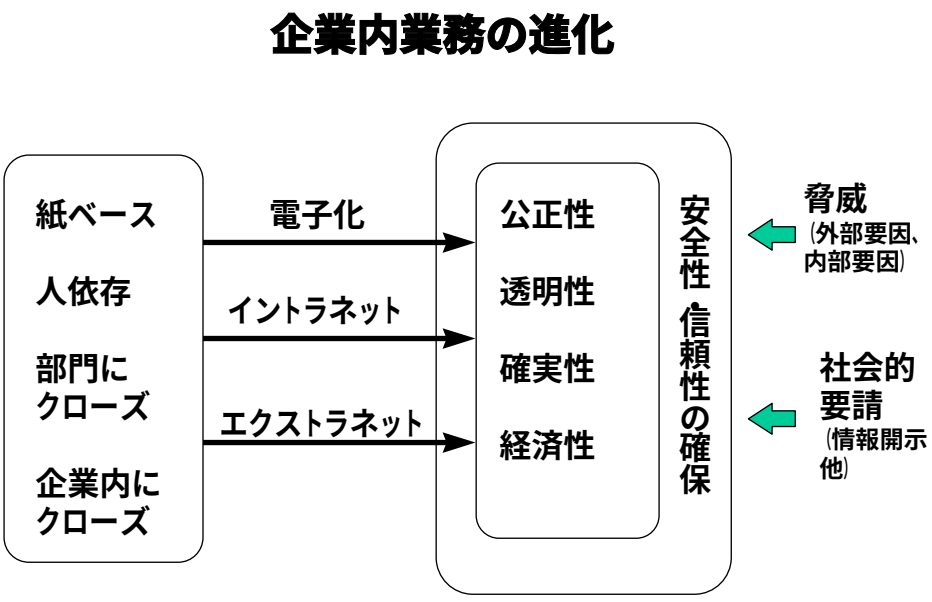


図 2-3企業内業務の進化

また今日、企業は対外的に積極的に情報を開示し、公正性、透明性を標榜する事が期待される。その一つとして、企業活動基盤が電子化される環境においてこの期待に応える仕組を備える必要性が検討されなければならない。

さらに、企業間における電子的情報交換はますます進むと期待され、それと並行して企業内業務も電子化、ネットワーク化が進行し、これらの業務はシームレスに、連続的に、有機的に接続され、遂行されるであろう。

2.4.3 消費者―企業間取引の視点

ＥＣＯＭが１０月２８日に発表した「電子商取引意識調査」によると、消費者からみた利点・長所として、①自宅にいながら購入できる、②２４時間購入できる、③海外等遠隔地の商品を手軽に購入できるなどの回答が目立っている。一方短所・不安として、①自分のデータが他人に洩れる恐れがある、②購入代金を間違って請求される恐れがある、③実際の商品との違いが有りすぎるなどの回答が多かったとの報告がされている。

このように、便利さに対する魅力を感じながらも、不安も持っていることが分かる。

従って、消費者―企業間取引では、企業間取引とは取引環境が異なるため、安全性・信頼性確保のみならず、消費者保護、プライバシー保護の視点からの検討も必要となる。

2.5 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。

一般の（リアルの世界の）商取引においても正常に取引が行われている間は、法律について特に意識することはないが、ひとたびトラブルが発生した場合には否応無しに必要となってくる。ネットワーク上においてもそれは同じである。リアルの商取引と違う点は、リアルにおいてそのようなトラブルが発生することに備えて取りうる措置が、ネットワーク上では同じようには取れない場合がある点である。

具体的には、取引の相手方の確認（取引資格も含めて）、取引内容の文書化（契約書、受発注書、覚書等）がリアルの世界と同様には困難である。

リアルの世界では相手先の確認について、印鑑証明書、商業登記簿謄本、資格証明書等でその正当性を確認できるとともに、それらの書類については「公文書」としての法的裏付けがある。また、既に取引がある場合は相手方の確認にはそう手間はかからない（対面、電話等）。

一方、ネットワーク上の場合、上記書類に代わる本人確認資料として考えられる物は電子署名である。ただ、現状では電子署名の前提となる認証書、認証局等について何ら裏付けはない。この点が、一旦トラブルが発生した場合の証拠能力がリアルの世界の書類と異なる点である。

また、契約書等の書類に関しても、リアルの世界では署名捺印によりその改竄が困難であり、また、その内容および存在について、公証人制度、内容証明郵便等の制度によって証拠力を高める事は可能であるが、ネットワーク上ではこのような制度は存在しない。この点においてもリアルの世界とは異なる。

ネットワーク上での商取引はビジネスチャンスの拡大として注目を浴びているが、その普及に関してはこれらの問題点をクリアにし、当事者に不安を与えない制度を構築する必

要がある。

ただし、このような制度を構築するにあたっては、技術的な対応によるものと取引ルールに関わるものに分けられ、どちらも利用者の立場から見た民間主導での確立が望ましいと考えられる。

電子公証検討WGの考える「電子公証」は必ずしも現行の公証システムと同じシステムではなく、当事者間における解決を基本にしている。ネットワーク（オープンネットワークを含む）における安全な商取引環境の確保（安全性、信頼性の確保）をめざす電子公証を考えるにあたり、現在の商取引の安全性を実現しているシステムおよび法的な裏付けとの整合性を考える必要が有り、ここでは商取引に特に関係の深い現行法の考え方と、電子公証との整合性を検討していきたい。

2.5.1 法律･制度整備の検討の必要性

(1) 現行法

電子公証を考える際に、まず、現状における諸制度についての考えをまとめてみたい。

① 公証人制度

公証人制度には大きく分けて 2 種類ある。１つは英米系公証人でもう１つはラテン（大陸）系公証人制度である。英米系公証人は私製証書作成者の認証のみを職とするもので法曹資格を有しない。ラテン系の公証人は署名の認証だけでなく公正証書の作成権限を有し、法曹資格を持つ。日本における公証人法はラテン系である。各国の公証人制度の違いは電子公証人を考えるにあたっての各国の考え方の違いに結びつくことが考えられ、今後各国で電子公証が検討されるにあたってのインターオペラビリティに注意が必要となる。

② 確定日付

確定日付は文書作成日について第三者に完全な証拠力が有る。その日付は公正証書の日付、公証人役場で私署証書に押した日付、登記所で押された日付、その他官庁･公所で押された日付（内容証明郵便など）などである。

③ 内容証明郵便（配達証明付）

手紙の内容、宛先、送付･到達日を証明。差出人は 3 通同じ物を作成し、差出人が 1 通手元控えとする他、郵便局においても 1 通を 5 年間保存することにより、証明するもの。

④ 印鑑と署名

署名とは作成者本人がその氏名を記入するものであり、押印は作成者本人の何らかの意志表示を示すものである。記名は作成者名を本人が記入する以外の方法で表示するものである。記名の場合、押印することにより作成者の意図を補完し、署名と同じ効力を持つことができる。つまり、記名＜署名＝記名＋捺印＜署名＋捺印の順でその効力は高くなる。

⑤ 原本、謄本、抄本の位置づけについて

原本とは一定事項を表示する確定的なものとして作られた文書である。一般に作

成者の署名捺印が有り、数通作成することも可能である。

謄本とは原本の内容を全部写し取ったものであり、原本の内容を証明するものである。

正本とは謄本の一形式であり権限あるものが原本に基づいて作成するものである。外部においては原本と同一の効力を持って通用するものである。

抄本は原本の一部を抜き出したものであり、原本の必要な部分の証明である。原本と同一の証拠能力を認められる。

(2) 電磁的記録の問題点

① 電磁的記録の原本性

従来のに学説における電磁的記録の原本性とは「コンピュータ処理の原則からいえば、作成時点および作成場所における中央演算処理装置（ＣＰＵ）の中のデータがオリジナルであり、その他のデータ（磁気テープ、磁気ディスク等に記録されたもの）はすべてコピーになる」というものであった。現在のようにパソコンを中心としたコンピュータが身近なものとなり、商取引においてもかかすことのできないツールとして当り前に利用されていることを考えると、上記における原本、謄本、正本、抄本という考え方で見ると、電磁的に記録されたデータをこのように分類することはなじまないといえる。実際に、処理中のパソコンのＣＰＵの中にあるデータのみが原本であり、ハードディスクなどに保存処理をしたとたんそれがコピーとなるというような考え方では、保存できるものはコピーだけで、原本というものは存在しなくなってしまうというおかしなことになってしまう。また、ネットワーク社会において遠隔地からデータが送られてくることは今や当り前になっており、データが作成された場所と処理される場所が違うことは十分にありえることである。このような場合においてもデータを入力した端末のＣＰＵにあったものが原本で、遠隔地のコンピュータ（例えば端末とホストコンピュータの関係）に送られたものはコピーであるといった考え方はなじまない。紙による記録から電磁的記録に代わろうとしている現代において以上のように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議論もある。以下に、書類の電子保存に関する考え方を述べる。

(3) 書類の電子保存に関する考え方

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証拠として電子的データを保存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、社内の電子化の進展により、そのニーズは増えていく。（例：ＰＬ文書）

文書を保存する場合、必要となる要件は真正性、見読性、保存性の３つである。

・真正性の確保…内容の故意または過失による虚偽入力、書換、消去及び混同を防止すること。

・見読性の確保…内容に応じて見読可能な状態に容易にできること。

・保存性の確保…保存期間内において復元可能な状態で保存すること。

電磁的記録を証拠書類として考える場合、上記の確保が必要となる。証拠力を向上させるには改竄を防止したり、検知したり、消去できない媒体を利用する等の技術や電子公証センターのような信頼性のある第三者機関の活用が有効な手段となる。

2.5.2 電磁的記録と民事訴訟法

(1) 自由心証主義

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。

（例えば、米国においてはＥＴＦ法によって電磁的記録に一応の推定効力を与えている。）

注：ＥＴＦ法…Electronic Funds Transfer：電子資金移動

(2) 証拠能力と証拠力

証拠能力とは、証拠として事実認定に利用できるかどうかの適格性のことである。電磁的記録の証拠能力を考えるにあたり、電磁的記録についての信頼度が裁判官の心証形成に及ぼす影響は関連技術の信頼度と社会システムの存在によるものといえる。

証拠力とは証拠価値のことであり、証拠としてどの程度役に立つかということである。

証拠力には「形式的証拠力」と「実質的証拠力」がある。

「形式的証拠力」とは作成者の意志に基づいて作成されたかどうかということであり、「実質的証拠力」とは事実認定にどの程度役に立つかということである。電磁的記録においては特に「形式的証拠力」が問題となる。文書であれば、公務員が職務上作成したものには推定規定があり、私文書の場合は署名捺印による推定規定があるが、「電子署名」といわれるものがこれに代わりうるか検討が必要。

(3) 証拠方法と新種証拠

証拠が取り調べられて裁判官の心証が形成されるまでの段階に３つの概念的区分がある。

① 証拠方法…証人、当事者、鑑定、書証、物証
② 証拠能力…証拠調べにより裁判官が知得した内容のこと
③ 証拠原因…裁判官の心証形成の原因となるもの。証拠資料の他口頭弁論の主旨など。

電磁的記録の証拠能力を考える場合、証拠方法が特に重要である。

電磁的記録が証拠方法のどれに該当するのかは説が別れており、明確に規定されていない。新民事訴訟法において新種証拠とされたビデオテープ、録音テープなども書証とすべきかどうか明確に規定されておらず、大きく分けて４つの説がある。

(4) 電磁的記録の証拠説

① 書証説…出力印字による「見読可能性」あり。データも出力印字のためのプログ

ラムと一体として「文書性」を肯定すべき。

② 検証説…磁気テープには「見読可能性」は無く、文書性を否定。
磁気の内容と出力された文書の同一性を鑑定する必要が有る。

③ 新書証説…出力印字し、署名捺印した文書（生成文書）を原本とする。
一定操作により見読可能となる「可能文書」とみなす。

④ 個別機能説…独立文書説（情報媒体から独立した文書）
生成文書情報媒体上のデータ、内容を推認させる「報告証書」にすぎず、証拠価値は相対的に低い。

(5) 民事訴訟法における書証の規定と電磁的記録の考え方

① 文書…成立の真否は筆跡又は印影によって証明できる。
（公文書、私文書は署名または押印にて真正に成立）
・処分証書（契約書等証明しようとする法律行為が記述）
・報告文書（人の見聞、意見等を記した文書）

② 準文書…図面、写真、録音テープ、ビデオテープ他情報をあらわすために作成された物件で文書でないものについて準用。

電磁的記録は新種証拠として準文書に位置づけられる録音テープ、ビデオテープと、個別検討されるその他磁気ディスク等に分けられる。

(6) 電子公証の導入による影響

電子公証の導入により電磁的記録は「新書証説」が定説となり、電子公証から出力印字した文書を原本として提出し書証として証拠調べを行うことが考えられる。この場合、電子公証の社会的信用力が問題となる。

電子公証センターの運営は公的運営と私的運営が考えられるが、公的運営の場合は公文書扱いとなると考えられる。私的運営の場合でも信頼性のある第三者であれば裁判官の心証形成に良い影響を与えることが可能と考えられる。

2.5.3 電磁的記録と刑法

(1) 刑法上の「文書」の概念と電磁的記録

刑法上における文書の概念は「文字又はこれに代わるべき符号を用い永続すべき状態において物体上に記載した意思表示」であり、電磁的記録は「文書」ではない。

(2) 刑法上の電磁的記録

電磁的記録とは「電子的方式、磁気的方式その他人の知覚によっては認識できない方式で作られる記録。電子計算機による情報処理の用に供されるもの。」

・電子的方式…ＩＣカード、ＲＯＭ、ＲＡＭ
・磁気的方式…磁気ディスク、磁気テープ、光ディスク
（永続性という観点から通信中のデータ、ＣＰＵで処理中のデータは含まれない）

(3) 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

(4) 可視性と可読性

有価証券を例にすると可視性は必ずしも必要とされない。

2.5.4 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。

(1) 経理会計帳簿原本の電磁的記録化の必要性

現状…紙に出力することによって、新たに「可視性･可読性」を加え、改竄が困難になる。また、署名捺印により出力者と作成者の同一性を推定できる。

電子公証の活用がこれらの問題を代替保証可能かが問題。

(2) 電磁的記録の経理上の取扱い

現状原本の地位獲得に至らず

① 会計帳簿…電磁的記録を排除するといえないが、関連分野との整合性･関連性の問題有り。（電磁的記録を原本とする余地は少ない）

② 計算書類…署名が必要なため紙である必要がある。電子署名が署名として適確とは現状いえない。

(3) 電磁的記録が認められていない理由と認められるための要件

① 電磁的記録に対して改変が加えられていないことの保証が必要であり、ソフト的、ハード的な対処が必要。

② 閲覧容易性の確保

米国の例…ＥＤＧＡＲ(Electronic Data Gathering, Analysis and Retrieval system) システム（有価証券報告書の通信データ送付・閲覧）

同様のシステムを日本で導入した場合の考え方は学説で分かれる。

・書証説（電磁的記録は原本、出力印字したものは謄本）

・新書証説（生成文書に署名捺印が原本、電磁的記録は単なる可能文書で資料）

・個別機能説（生成文書に署名捺印が原本、電磁的記録の証拠調べは検証による）

③ 望ましい要件…原始証票から最終の帳簿までのトレースが可能であることが望ましい。

2.5.5 電子公証の証明力（証拠力）向上

(1) 必要な要件…電子公証機能と実現のレベル

送受信者特定、到達確認、改竄検知、時刻付与、アクセス記録、プロセス記録、電子保存等の機能を人的仕組みから電子的仕組みに置き換えるプロセス。

2.5.6 原本性保証電子保存システム

(1) 電子保存システムに関する考察としては、下記が必要である。

① 外部からの物理的不正アクセス防止（強固な金庫など）

② 利用者による論理的不正アクセス防止（管理者による認証等）

(2) 電子的に保存する情報についてのセキュリティ

電子保存システムのパッケージ化

（メディアのパッケージ化、ＣＰＵによる管理…ファイル種別毎のアクセス管理、

制御プログラムのＲＯＭ化）

修正した場合、修正前のファイルを保存するため追跡可能。

2.5.7 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。

電子署名法

デジタル署名等により法的効力を生じさせることが必要とも考えられるが、その際には下記の問題点がある。

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

以上、電子公証を検討するにあたっての法的問題を整理してきたが、現行の日本の法体系では、今後一層の技術開発及び社会システムの確立が必要であり、国際的な整合性を取りながら定着させていくことが必要である。

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。

以下、企業間取引、企業内業務、消費者―企業間における様々な取引形態、局面、対象の電子公証の課題、ニーズを整理する。

取引形態別の特性、取引対象毎の特性、取引プロセスの第三者からの脅威、当事者からの脅威等は「電子公証検討調査報告書」を参照。

3.1 企業間取引

3.1.1 電子商取引の取引形態別検討の必要性

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、一律でなく個々の検討が必要である。

「基本的な考え方」

（１）本ガイドラインでは不特定多数企業と特定多数企業は次のように定義しており、認証とは別の意味合いで使用している。

不特定多数企業とは基本契約締結前の企業であり、基本契約締結後は特定多数企業として登録がされた企業である。但し、基本契約締結前でも実質的に基本契約締結を前提としているような場合は特定多数企業とみなされる。

認証はその企業の存在や真正性を確保したり、他の企業との識別等を行う行為であり、取引プロセスや取引情報価値により、認証の狙いや厳密性（認証レベル）は異なる。

（２）不特定多数企業と取引を開始するには募集～基本契約締結等のプロセスが必要。

（３）継続取引が中心に行われている代表では生産財があり（取引企業特定労力は大、安定的供給の確保他）、継続的取引を前提としない取引には消費財が考えられる。（代替品、代替企業からの確保他）

（４）開発品は機密情報の取り扱い、代替の困難性等より、継続的な取引が一般であるが、先端技術の必要性により、１回限りの取引ニーズは大きいと思われる。

3.1.2 認証・電子公証のレベルの違い

継続取引を前提とした生産財（開発品）の場合を例に認証、電子公証のレベルの違いについて記述。

「基本的な考え方」

（１）前述のように認証はその企業の存在や真正性を確保したり、他の企業との識別等を行う行為で電子公証は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とする。

従って、電子公証は認証を包含しており、「何を」、「何時」の要素について重点を置く。

（２）第三者からの脅威・不安（詐称、盗聴、改竄等）には認証、デジタル署名、暗号等の共通インフラが有効となる。攻撃対象メッセージは金銭、機密情報が中心である。

（３）当事者からの脅威・不安（改竄、否認）にには ルール、認証、電子公証、デジタル署名、暗号等が有効となる。

(1) 認証について

取引のどこの局面から認証が必要になるか、その認証の狙いは何か、認証の対象情報は何か、認証レベルや方法、認証に必要な鍵の管理、運用等を当事者からの脅威面より検討すると

＜募集～基本契約締結＞

① 不特定多数企業から提案書を受け付けた段階より、応募企業の認証が始る。ここでの認証はその企業の存在、真正性を確かめることが最大のポイントである。（提案書自体が要求レベル以下では認証行為は不要となる。）

② 基本契約締結までは、基本的には不特定多数企業の１社であり、ここでの認証は該当メッセージの送信者の識別と否認（発信事実、内容等）を防止することがポイントである。

③ なお、基本契約締結前は信頼性を確保するためにメッセージ毎に認証局に電子認証書を問い合わせる等の木目細かい認証が必要であるという議論と基本契約前で法的に束縛されないので認証は緩やかで良いとの議論がある。認証レベルについては（注）を参照。

＜引き合い～決済＞

個別契約前に取引企業（特定多数企業）と電子交換協定、取引のルールの取り決めを行う。

④ 既に取引の実績が豊富で信頼関係（故意による脅威が無い場合）がある場合は該当メッセージの送信者の識別で十分なことが多い。

⑤ 取引実績が少ない場合や信頼関係が十分でない場合は送信者の識別と否認防止がに対応できる認証が必要となる。

（注）認証レベルについて

電子的認証を行う以前に本人確認を行い登録手続きをする。登録段階で決まる認証レベルは登録時の本人確認の手続きで決定する。これは電子的認証の方法とは関係しない。従って認証のレベルは電子的認証を可能とするまでの登録手続きと電子的認証が行われる利用局面について評価される。表 3-1 認証レベル表参照。

表 3-1認証レベル表

認証項目	ID とパスワード	共通鍵	公開鍵	所有物	バイオメトリックス
登録時の認証レベル	方式に依存せず	方式に依存せず	方式に依存せず	方式に依存せず	方式に依存せず
電子認証時の認証レベル	低	中	高	高	高
特徴	簡便、安価。相手毎に登録が必要。	鍵配信の問題がある。	一つの鍵ペアを多数相手に対して利用。毎回登録する必要がない。	ワンタイムパスワード、チャレンジレスポンス、等	指紋、動的署名等

尚、運用面においてなりすまし問題が発覚しその結果登録情報を無効にする必要が生じた場合、どれだけの時間でシステムを更新するか等の規定や、公開鍵の場合は認証局への電子証明書の問い合わせサイクルによってもレベルは異なる。

例示

・全てのメッセージに対して毎回電子証明書を問い合わせる。
・定期的に（例えば１回／週）問い合わせる。
・メッセージ毎に（重要メッセージは毎回、以外は定期的に）問い合わせる。

(2) 電子公証について

実ビジネス上の取引局面毎の課題とニーズを把握することが検討のベース。

＜募集～基本契約締結＞

① 取引企業と基本契約締結するまでは基本的には不特定多数企業の一社であり、信頼関係が無い分相手企業の改竄、否認を意識する領域である。

② 応募内容の改竄、否認（送信、受信、内容等）や不採用通知の受信否認防止等は信頼性を確保するために必要である。基本契約書は法的な拠り所となるものであり、証拠としての電子保存が重要である。

③ 尚、並行して行われる相手企業の信用調査（資産内容、負債状況、業績、財務、風評、経営者資質、品質管理力他の安定性、成長性、信頼性等）の状況によっても電子公証に対する厳密性は変わる。

＜引き合い～決済＞

④ 金銭的損害、競争力（機密情報漏洩）低下は最大関心事であり、注文情報の数量・金額、請求情報、支払情報等に対する信頼性ニーズは極めて高い。

⑤ まずは第三者からの脅威に対する解決の仕組み（技術中心）がベースになり、その上で取引企業との取引関係により、どこまで当事者間で「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」）の取り決めができるかである。クローズドな取引かグローバルな取引か、取引形態、取引の対象、取引

金額の大小、取引数量の大小、信頼関係、拡張性等により、必要とされる電子公証レベルは異なる。

⑥ 当事者の改竄や否認防止は当事者間の**「人的仕組み」、「電子的機構」**により、基本的には解決は可能であるが、機密情報の悪用等は最終的には相手を信用するしかなく、別途機密保護契約等が必要である。

⑦ これらのルールの遵守に不安がある相手や万一の（取引金額が大きくダメージが大）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）は信頼性確保に有効な手段となる。

3.1.3 まとめ

以上、電子商取引の形態、対象、取引局面等で認証、電子公証に求められるレベルが異なり一律ではないことを説明した。今後具体的に実ビジネスのモデル化をする事が必要である。また、このように一律でない場合、業界、業際、グローバル化の視点からどの様な仕組みがよいかの検討が必要である。

前述したように、オープンなＥＤＩは従来のＥＤＩの課題を解決し、インターネットの有する可能性を追求できることに意義がでてくる。従って、新たなビジネスプロセスに認証、電子公証の仕組みをどの様に組み入れていくかが重要である。

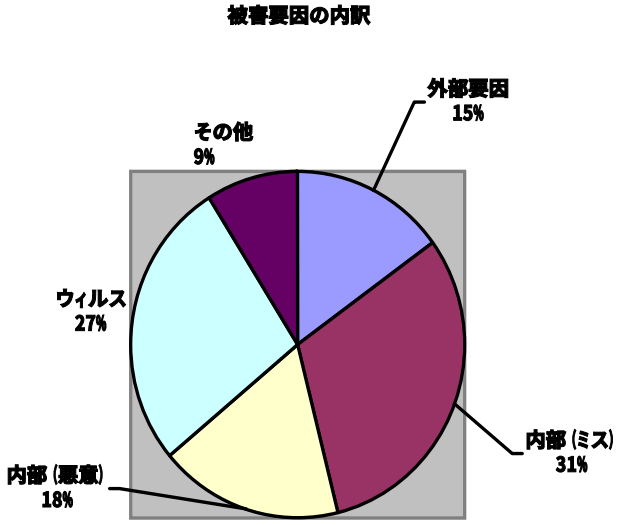
3.2 企業内業務

3.2.1 企業内業務における安全性と信頼性

今日的な企業内電子情報交換の場における安全性、信頼性について検討するために、現在企業内で実行されている電子化された業務の幾つかをそれらの特性や特徴毎に選定し分析の対象とした。業務の特性として、社外関係の有無、金銭の直接的関係の有無、定型業務であるか非定型業務であるか、決裁型であるかアクセス型であるか、等を考慮した。（詳細は電子公証検討調査報告書（電子公証システムガイドライン作成に向けて）平成９年５月を参照。）その結果今日の新たな情報基盤には少なくとも以下のような課題が存在することが分かった。

- システムからの盗聴・漏洩・改竄
- 電子記録媒体からの漏洩・改竄
- 電子承認印の偽造
- 電子情報の送信否認・受信否認
- 電子情報の到達確認、受諾確認
- 電子記録内容の不備
- 行為の確認、承認内容の否認
- 不正規な電子決裁、電子稟議処理
- 電子保管中の文書の紛失、破壊
- 重要文書を誤って第三者に送付
- なりすましによる不正アクセス
- パスワード管理の問題
- 人事考課情報等のプライバシー保護

また図にあるように、ある調査によればコンピュータの不正利用の多くは企業内にあると報告されている。



出展：丸文株式会社 広報誌「MIA」Vol.54 から
Information Week/Ernst and Young/Data General(1996 年 10 月現在)

3.2.2 企業内電子公証の必要性

前節の課題に対して企業組織で問題解決のためにとることができる対策は幾つかある。それらとして、規則と教育、技術的手段、運用、ソフトウェアシステム、認証機能、そして電子公証機能を取り上げ課題との関連性について考察した。その結果、電子公証機能を利用することにより企業内に存在する課題の多くを解決することができ、これにより要求される安全性、信頼性の水準を向上させることができると期待される。

今後企業内で進行すると予想されている情報の電子化に伴い、企業活動は電子情報基盤の上で行われる。これにより今日企業に期待されている社会的要求、即ち公正性、透明性、確実性、経済性等の要求は電子情報基盤に存在する各種の脅威にさらされることになる。かかる観点において、電子公証の存在はその対策の一つとして役割を果すことが期待される。企業はこの時さらに、自ら電子情報基盤に関する安全性のポリシーを設定しさらに公表することによりその要求に十分応えることができよう。また、適切な企業内電子公証の存在により既存の企業活動の場合に比較してより理想的に社会的要求に応えることができるとも期待される。

以上のように、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。

ところで、現在企業内で利用されているシステムの多くは既存のパッケージソフトウェアや業務特性を考慮した特定用途のソフトウェアシステムであり、これらのシステムには一般的に安全性・信頼性のコントロールが組込まれている。従って、電子公証機能に相当する機能が既に部分的にも考慮されている。現状では、このような理由と業務規則の存在により、運用の安全性・信頼性が確保されているとし、多くの場合、新たな公証機能を企業内システムに導入する緊急性は意識されていない。

今後、情報の電子化が高度化するに従い、意思決定の諸プロセスやより機密度の高い情報も電子化の対象となることが予想されている。また紙媒体を想定している各種規制の規制緩和の期待もある。このような状況の変化に伴い、安全性、信頼性に要求される水準も変化していく。企業が要求する安全性、信頼性の水準はまちまちであるものの、企業は置かれた環境とそこで要求される安全性、信頼性の水準を把握し、それに応じて企業内電子公証を位置づける必要がある。

3.2.3 これからの企業内電子公証の利用局面

企業内の諸業務は次第に電子化されていくことが期待されているが、以下では今後の電子化において公証機能との関連により業務の安全性、信頼性が向上すると考えられる利用局面の例をあげた。

3.2.3.1 業務処理過程の電子的捕捉とその記録保持

企業・組織では組織構造のコントロール、例えば水平的な検査・照合プロセスや垂直的な承認プロセス、により業務を処理する。これを電子的情報の視点でみると処理過程はデータの状態変化、遷移と捉えることができる。従って、このようなデータの変遷を電子的に正しく記録・保持すること、即ちプロセス記録を保持することにより、企業・組織活動を正確に捉えることができるのであり、これにより、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、効率的な企業経営を維持していくことができる。この例として、稟議や各種承認プロセスにおける承認事実の記録、原データ、確定データの保管、あるいは組織間に渡る依頼事項に対する変更指示、変更要求、変更受諾等の事実記録等があげられる。

3.2.3.2 より高い証拠力を求める局面

以下ではより高い証拠力を必要とする情報や局面を想定した。場合により企業外の電子公証サービスを利用することも考えられる。

① 先発明主義の特許、発明の証拠としてのタイムスタンプ。
② 契約内容遵守の事実を記録しそのタイムスタンプを得る。
③ 勤怠管理。
④ アイデア、企画等の知的生産物の保護、評価。
⑤ 各種契約書、権利書、覚え書き等の記録保存。
⑥ ＰＬ法関連文書

3.2.4 企業内業務と企業間取引きを包含した電子公証

企業が関係する電子商取引は大きく企業間情報交換と企業内情報交換の場で考えることができる。企業間情報交換では注文情報、検収情報、請求情報、支払情報等を企業間の取り決めにしたがって、お互いの企業の窓口部門が電子情報のやり取りをする。企業内情報交換では、これらの情報を生成する社内関連部門間（例えば、システム開発部門、生産管理部門、資材部門等）での情報交換が行われる。企業内ではその組織規模が大きくなるにつれ部門毎の独立性が強くなってくる。そして大きな事業部門や事業所間の情報交換では企業間取引きの型に類似してくる。また今日では関連企業間での情報交換も積極的にネットワークを介して行われており、構成されるネットワークはエクストラネット（注）と呼ばれている。社員からの社外から社内システムに直接アクセスするニーズに応えるため、社内にＣＡ局を立ち上げ、証明書を発行し、本人認証による不正アクセス防止と暗号システムによる機密情報の交換の実験も行われつつあり、企業内からの認証・電子公証の取り組みが今後の展開に拍車をかけるであろう。このように企業における情報交換の場はマクロには階層構造を形成している。今日、企業にはさらなる業務の効率化、短縮化の目標を達成すべく、全ての階層に渡ってシームレスな電子的業務処理を行うことが期待されている。

企業における電子的情報交換の安全性、信頼性の要求は企業間の関係、関連企業間の関係、事業部門間の関係、部門間の関係、あるいは最小組織単位においてのいずれにも要求されている。その要求水準は個別企業、階層レベル毎に違っているが、企業内といえども電子公証自身に要求される信頼性の水準は高くなければならない。企業内の電子公証を考えるにあたり一元的に電子公証を実現する方法もあれば、組織構造に依存した階層的電子公証の実現方法も考えられる。今後は企業内電子公証の必要性に鑑みて企業毎に企業を取り巻く環境の中で総合的な視点から安全性、信頼性を検討し対策がなされる必要がある。

（注）エクストラネット導入の背景

①公開見積り・競争入札による部財調達によるコストの削減

②取引先の拡大

③取引先との企業間ワークフローによる取引の効率化

④図面データの交換による協調作業の迅速化／効率化

3.3 消費者―企業間取引

前述の企業間取引においては、現状では一般に特定多数の継続取引を前提とし（継続的取引を前提としない市場型の取引も試行されつつある）、取引金額も大きく、さらに組織的な情報技術の整備、活用が可能である。

一方、消費者―企業間取引においては、大半が不特定多数の１回限りの少額の取引であり、情報技術の活用も個人に依存し、情報技術の弱者であると同時に、プライバシーの保護についても、相手に委ねざるを得ない面を有す。

従って、消費者―企業間取引においては、これらの消費者を取り巻く環境を考慮した取引における安全性・信頼性の確保が重要である。

尚、本検討に関しては、ＥＣＯＭにて発表されている、ガイドラインや約款を参考にし

た。

3.3.1 想定されるトラブル

トラブルには電子商取引に特有のものとリアルの通信販売と共通のものと存在する。

これらの分析から言えることは、企業間取引、企業内業務、消費者―企業間取引と基本的に求められるセキュリティは同じであり、電子公証に要求される機能も変わらない。

しかし、消費者―企業間では電子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。

以下、消費者の視点から見た安全性、信頼性確保、個人情報保護に対する要求は何か、代表的な決済モデルとして、クレジット決済代行型タイプ、クレジット決済非代行型タイプ、クレジット未使用型タイプについて、消費者の視点からの安全性・信頼性について検討が必要と思われるポイント及びデジタルコンテンツの取り扱い、リスク負担の基本的な考え方について述べる。

想定されるトラブルは添付資料を参照。

3.3.2 消費者の視点から見た安全性、信頼性確保、個人情報保護に対する要求

3.3.2.1 「安全性確保に関して」（第三者からの脅威面から）

消費者の視点からは安全性（通信上の）に関して、

① どのプレイヤーの指示に従えばよいのか
② 安全性はどのように確保されるのか
③ 第三者からの脅威で被害が生じた場合はその損害を誰が被るのか
④ 消費者としてする事があれば何か

3.3.2.2 「信頼性確保に関して」（取引当事者間の信頼性確保面から）

「誰が（と）」、「何を」、「何時」電子的にやり取りしたかを証明する仕組みとして、取引データの記録・保存が必要である。

消費者の視点からは

① どのプレイヤーにその役割を期待すべきか
② 記録・保存する対象データと期間は
③ 信頼性の高い記録・保存であるか（外部、内部犯罪）
④ 必要時には請求して見せてもらえるか
⑤ 自己防衛として消費者は何をする必要があるのか

「参考」

一般に電子情報は簡単に改竄されやすいと言われるが、日常業務で作成されたものは証拠能力（証拠として裁判所に提出可）を有し、セキュアな保存を施すことにより、証拠力が高まると言われる。例えば技術的には全ての情報にタイムスタンプを付与するとか、改竄を検知可能にするとか（ＭＡＣ）、改竄ができない様にするとか（アクセス制御）、消去ができないようにする（ＷＯＲＭ）とかである。また人的面では複数特権、物理的な堅

牢な建物等が証拠力を高めることになる。また当事者が保存する方法以外に信頼性ある第三者に委託することも有効な手段となる。

3.3.3 タイプ別モールと安全性・信頼性確保、消費者保護の在り方（例示）

3.3.3.1 モールタイプ１（クレジット決済代行型タイプ）

(1) 関連図

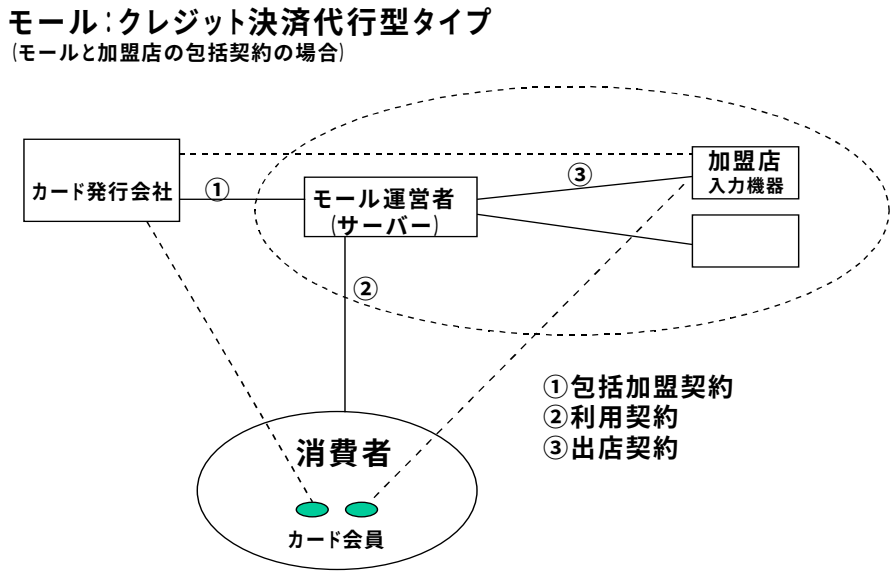


図 3-1クレジット決済代行型タイプ関連図

(2) 仕組み概要

消費者は決済にクレジットを利用、モール運営者はカード発行会社と包括契約、モール運営者は加盟店と包括契約を締結する。従って本ケースでは消費者と加盟店間の利用規約は不要。

(3) 安全性・信頼性確保、個人情報保護に対する意見

① 安全性確保

本ケースの場合は決済の責任（カード発行会社は請求書と本人の食違いのトラブルの窓口であり、一番責任ある主体）を負うカード会社が安全性について、責任ある対応が不可欠であり、消費者とモール間の手順・安全措置の提示はカード会社が、行うのが合理的

② 信頼性確保

注文情報に関してはモール運営者が取引データの記録・保存をし、消費者との信頼性を確保する。

請求書を発行するカード会社も決済金額に関する問い合わせに的確に対応するための必要な取引データと金額を記録保存する。

モール運営者とカード会社の取引データの記録・保存の責任主体（消費者の視点

から）はどちらが合理的かは検討を要す。同一性確保が必要

③ 個人情報

カード会員情報、モール会員情報は其々の責任で管理し、取引情報はカード会社、モール運営者、加盟店間で業務遂行上必要情報のみとする。

個人情報が分散すると管理が不明瞭になり、トラブルの主体が不明確となり易いため、統括責任主体の在り方についても検討を要す。

3.3.3.2 モールタイプ２（クレジット決済の非代行型タイプ）

(1) 関連図

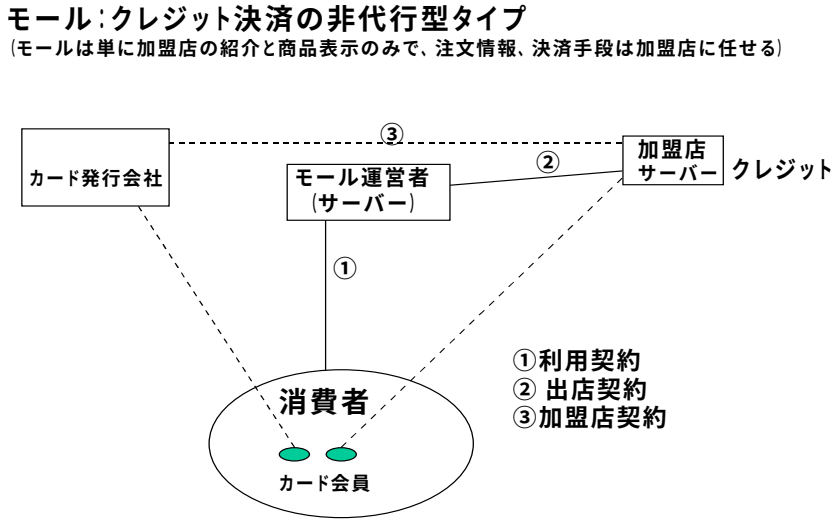


図 3-2クレジット決済の非代行型タイプ関連図

(2) 仕組み概要

消費者は決済にクレジットを利用、モール運営者は加盟店の紹介と商品表示のみで、決済は加盟店に任せるタイプである。従って本ケースでは消費者と加盟店間の売買契約における契約内容が重要となる。

(3) 安全性・信頼性確保、個人情報保護

① 安全性確保

本ケースの場合は決済の責任（カード発行会社は請求書と本人の食違いのトラブルの窓口であり、一番責任ある主体）を負うカード会社が安全性について、責任ある対応が不可欠であり、注文情報や決済は消費者と加盟店間とし、手順・安全措置の提示はカード会社が、行うのが合理的

② 信頼性確保

注文情報に関しては加盟店が取引データの記録・保存をし、消費者との信頼性を確保する。

請求書を発行するカード会社も決済金額に関する問い合わせに的確に対応する

ための必要な取引データと金額を記録保存する。

加盟店とカード会社の取引データの記録・保存の責任主体（消費者の視点から）はどちらが合理的かは検討を要す。同一性確保が必要。

③ 個人情報

カード会員情報、モール会員情報は其々の責任で管理し、取引情報はカード会社、、加盟店間で業務遂行上必要情報のみとする。

消費者からは加盟店に注文情報を出したのであるから、個人情報の責任主体は個々の加盟店であることが合理的

しかし、問題点は消費者は各加盟店と契約することになるため、個人情報の管理の統括責任主体が存在しない。

3.3.3.3 モールタイプ３（クレジット未使用タイプ）

(1) 関連図

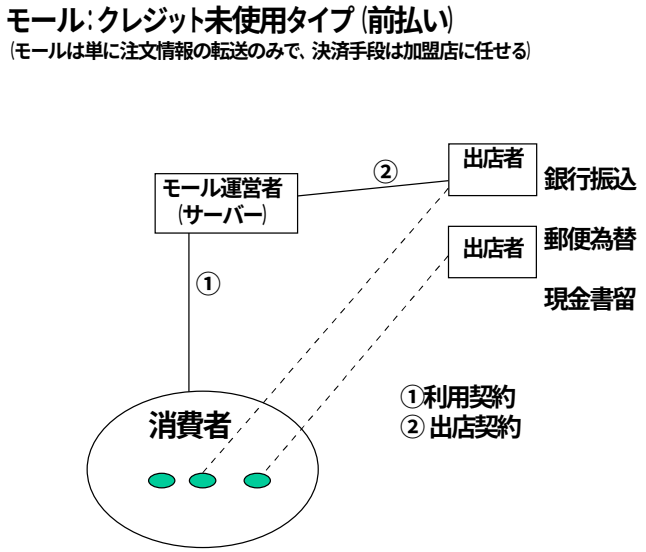


図 3-3クレジット未使用タイプ（前払い）関連図

(2) 仕組み概要

決済は後払いで、モール運営者は出店者の商品表示と注文情報の転送のみで、決済は出店者に任せるタイプである。

(3) 安全性・信頼性確保、個人情報保護

① 安全性確保

本ケースの場合は前払いのため、出店者は決済リスクが無いため、消費者とモール運営者間のネットワーク上の安全性のハードルは低くても良いかもしれない。

（例えば注文情報を出店者が消費者に確認する等の手続を入れるとか）。本件は検討を要す。注文情報の消費者とモール間の、手順・安全措置の提示はどちらが行

うべきかは、（消費者からは注文情報を受信窓口のモールの方が分かり易いがトラブル時の責任主体との関連を含めて）検討を要す。

② 信頼性確保

モールは注文情報を単に転送するだけであるため、取引データの記録・保存は出店者が行い、消費者との信頼性を確保する。

前払い方式ではお金を支払ったが商品が来ないトラブルが起きやすい。

トラブルの本質を見極める必要があるが、まず、責任主体（受付窓口）を明らかにすると同時に過去のトラブルや想定されるトラブルに適切な対策をする。

＜トラブルの例示＞

・注文を受けていないと否認する：本ケースでは出店者から注文情報の受託確認を返送する等である程度解決可能（デジタル署名等で否認不可：ハードルが高くなる）

・配送したと主張する：多分これが多いいと思われるが、配送会社が商品を届けた場合の受取印や署名で確認

・それ以外

③ 個人情報保護

モール会員情報はモールの責任で管理し、取引情報は出店者の責任で管理する。

3.3.4 デジタルコンテンツの取り扱い

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。

１つはホームページの真正性をどの様に確認するかである。もう１つは購入したデジタルコンテンツの真正性をどの様に確認すればよいかである。さらには知らず知らずのうちに違法の海賊版（著作権侵害）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である。

(1) ホームページの真正性

現在世界膨大な数のモールが立ち上がっているが、それが本物かどうかを見極めることは一般の消費者には不可能である。従って、他のモールと類似の名称で出した場合経験者は別として一般の消費者には分からない。また、詐欺まがいに安く商品の値付けをし、払い込ませた後、雲隠れする事はリアルの世界よりも簡単にできる。このようなトラブルに対しては、信頼性ある第三者機関（例えば電子公証センター）がまる適マークを付与する（透かし等）仕組みや不正なホームページや企業を公表し、被害を最小限に押さえる等の仕組が必要である。

(2) 情報財（デジタルコンテンツ）の真正性

情報財をネットワークを通してダウンロードする場合、そのデジタルコンテンツが本物である事を消費者は一般に確認できない。通常動作確認か画像の場合それに近い内容が出れば問題無しとしている。しかし、必要時にはそれが本物であることを確認する方法を整備する事が必要である。さもなければ消費者は一方的に買わされてしまう。この解決手段としても色々考えられる。１つはダウンロードしたデジタルコンテンツを電子公証センターの保証された本物と突き合わせる方法。１つは信頼性ある第

三者のまる適マークの入ったデジタルコンテンツを確認する方法である。

(3) 著作権等

デジタル技術を用いればデータは簡単に複製し加工することができるが、電子商取引ではこの特徴が両刃の剣となる。インターネット上の商取引ではしばしばコンピュータプログラムやゲームソフト、電子アートや電子音楽など電子化されたさまざまな知的財産を売り買いすることになる。このような電子商取引を加速するためには、売り手には彼等の知的財産が盗まれないという、買い手には本物の製品を入手しているという安心感が必要で、そのためにも特許権、著作権、商標権などの保護が重要となる。

著作権保護については、複製を防止する「電子透かし」などの技術も有効である。しかし例えばオリジナル作品をデジタル化しデータベース化した場合など誰にどこまでの権利を認めるかとか著作権侵害の有無をどういうしくみで管理するのか、といった制度上の議論が世界知的所有権機関（ＷＩＰＯ）において国際的なバランスを考慮しながら続けられていることからその結論を待つ必要がある。

電子公証の観点からは、デジタルコンテンツの作成者もしくはその著作権管理団体などが信頼性ある第三者機関へその内容を登録する、もしくはその機関の発行するユニークな識別情報を活用することによっての解決も可能であろう。

3.3.5 リスク負担の基本的考え方

消費者・企業間で電子決済技術を用いた取り引きを行う際には、様々なリスクが伴うものと想定される。ここでは、クレジットカードを利用する際のリスクを、クレジットカード会社、店舗、システム運用者、顧客の４者でどのように分担するか、その基本的考え方に関する議論を整理する。

(1) 基本的な前提

消費者・企業間取り引きに、電子商取引の手法を導入する際には、まず以下のような基本的な前提を置く必要がある。

① 電子商取引を導入することにより、自己責任をベースに新たなリスクが消費者に転嫁されることが無い

② 事業において主要な役割を果たす主体が積極的にリスクを負担する

(2) 想定されるリスク

まず、消費者・企業間の電子決済において考慮しなければいけないリスクを以下の３種類のリスクに分類して議論を進める。

① 電子商取引を利用するか否かに関係なく存在する（リアルの通信販売と共通）リスク

例：与信リスク

② 電子商取引を利用することにより新たに発生する（電子商取引に特有）リスクのうち予め想定が可能なもの

例：システムの誤作動等によるリスク

③ 電子商取引を利用することにより新たに発生する（電子商取引に特有）リスクの

うち予め想定が不可能なもの

例：暗合・認証機能が破られる

(3) リスク分担の考え方

リスク分担については、①のリスクに関しては既存のクレジット約款に準じてクレジットカード会社、店舗、顧客が分担する。基本的なリスクは従来とほぼ同じであるが、従来は保険でカバーしていた部分については暫定的にクレジットカード会社がリスクを負担し、実績が蓄積され保険が利用可能になり次第保険を適用する等の検討が必要である。②のリスクに関しては、システムの誤動作等、発生原因を特定できるものとし、発生原因の担当主体がリスクを負担する。ただし、原因が特定できないときは顧客を除く３者協議の上で負担を決めるものとする。③のリスクに関しては、暗合・認証機能が破られるという想定のもとに事業を行うことはできないことから、顧客を除く３者協議の上で負担もしくは対策を決めるものとする。

(4) 今後の考え方

以上の考え方は、実績の蓄積、保険の整備、監査の仕組みの構築がなされるまでの暫定的なものであり、今後これらの問題が解決されていく過程で再度整理する必要がある。

3.3.6 まとめ

電子商取引に参加する消費者はヴァーチャルショッピングモールでの購入者である。通常はWWWのホームページにアクセスすることにより商取引に参加する。ここでの消費者の選択は購入するかしないかであり、条件や契約についての交渉はほとんど行われない。

このような取引においては契約に不慣れな消費者を保護するためには割賦販売法や訪問販売法のような法律による保護が必要である。この中では、消費者が被る損害の最大値（たとえば 38,000 円）を明確にすることも検討されるべきである。

また、購入の申込もクリックすることにより行われることが考えられるので、誤操作を招くような複雑な操作を避けるような画面構成を販売者に要求することも必要である。さらに、クーリングオフのような手続も必要であろう。

また、取引に参加する消費者に対して事業者は取引を安全に行える技術（ツール）を提供する必要があると同時に、消費者も提供されたツールを正しく理解して確実に利用することも取引の安全のために欠かせない要件である。

整理すると、

(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（紛議が生じた場合、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

前章までの電子公証の役割と定義、ニーズをうけて、電子商取引を行う取引当事者が安全と信頼性を確保するための電子公証に要求される機能、実現するための関連技術、電子公証モデル、企業間取引と企業内業務のモデル別システム要件とシステム図を例示する。

4.1 電子公証機能

4.1.1 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。

(3) 備考：

本機能は、通常、認証機関で装備される。

4.1.2 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）

(3) 備考：

インターネットの持つ不安定性（ネットワーク障害の可能性が専用線より高い）と電話のように当事者が直接話をする場合と違い受信者が受信を否認することが考えられる。それを補う機能として本機能は有効である。

4.1.3 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。

(3) 備考：

文書（電子データ）には暗号等により、改竄防止対策を施すことが出来る。しかし、

本機能を利用することにより、不正アクセス等、攻撃にさらされているかが判断可能となる。そのため、本機能の結果はシステムのセキュリティが保たれているか、運用の見直し・セキュリティ対策を行うための情報となる。

4.1.4 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)

(3) 備考：

この機能の利用目的として、時刻付与を信頼性の高い電子保存をする場合の手段として利用する場合と、時間付与自体が意味を持つ場合がある。前者では、例えば受信する電子情報すべてに機械的に受信タイムスタンプを付与することにより、受信後のデータの改竄を困難にする方法である。また、後者では、期限付き公開入札等で受信日とか特許のアイデア等が何時存在したかを第三者に証明する場合である。

4.1.5 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）。

4.1.6 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）。

(3) 備考：

企業間取引きでは二者間での情報交換、情報処理に集約して考えることができるため、この機能は実質的には電子保存機能により実現される。したがってこの機能は企業・組織に特徴的な公証機能である。

4.1.7 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）

(3) 備考：

電子保存機能が「電子データが原本であるための要件（セキュリティ強度、運用方法等、定義されるのであれば）」を満たすことにより、原本を保証できなくてはならない。

4.2 関連技術

4.1 で述べた要求機能を実現するために、関連する主な既存技術について列挙する。

基本的には暗号技術を用いて、送信者／受信者本人でなければ開示／作成できないデータを付加することにより盗聴・改ざんを防止する。また、時刻データも付加することによりデータが存在した時刻の証明可能となる。

データ保存や暗号処理に関してはソフトだけでなくハードに関してもデータの漏洩等を防止するための仕組みが存在する。

これら暗号技術は、電子メール等のアプリケーションに組み込まれ利用されている。

なお、以下に紹介する技術は、セキュリティ技術とその応用技術の一部である。今後電子公証のためのより適した技術が開発されることも十分考えられ、これから説明する技術のいくつかは電子公証システムを構築するのに不適当な技術となる可能性もあり（既に不適当な場合も有り得る）、本章で紹介する技術がすべてではない。詳細は添付資料を参照。

表 4-1電子公証機能と関連技術対応表

機能	関連技術			
	暗号技術	セキュアプロトコル	ハードウェア	応用
送受信者特定機能	共通鍵暗号方式、公開鍵暗号方式、ハッシュ関数、電子署名、MAC	SSL、SET		零知識証明、ワンタイムパスワード
到達確認機能		MDN、SSL		PEM、PGP
改ざん検知機能		SET		S/MIME、PEM、PGP、電子透かし
時刻付与機能		NTP		
アクセス記録		NTP	Write Once、耐タンパー装置	アクセス制御
プロセス記録機能		NTP	Write Once、耐タンパー装置	アクセス制御
電子保存機能		SSL	Write Once、耐タンパー装置	アクセス制御 情報の分割

4.2.1 暗号技術

暗号技術は、ネットワーク・セキュリティを実現するための核となる技術のひとつであり、盗聴・なりすまし・否認といったネットワーク上の脅威から商取引を守る。

暗号化の方式は、暗号化と復号化で同じ鍵を使用する共通鍵暗号方式と、暗号化と復号化で異なる一組の鍵を使用する公開鍵暗号方式がある。

(1) 共通鍵方式

暗号化と復号化で同じ鍵を使用する。メッセージの送り手は受け手ごとに異なる鍵を秘密に保持する。鍵は送受信者間で秘密に保持されるため、第三者によるなりすましと送信事実の否認が防止できる。受け手の鍵で復号できれば同じ鍵をもつ相手が特定でき、かつ、送り手は送った事実を否認できない。しかし、送受信者間で同じ鍵を使用するため、送受信者間において、一方がもう一方になりすますこと、およびは送った事実の否認（送信者は、送ったにも関わらず受信者が送信者になりすまして送ったと主張する）は可能である。電子商取引でなりすましや送信事実の否認を防止するために共通鍵暗号方式を使用する場合には、送受信者間に信頼関係があることが前提条件となる。

(2) 公開鍵方式

暗号化と復号化で異なる鍵を使用する。異なる二つの鍵は、ひとつを公開（公開鍵）し、もうひとつを秘密（秘密鍵）にする。送り手は受け手の公開鍵で暗号化し、受け手は自分の秘密鍵で復号化する方法であり、秘密鍵を管理している受け手以外は読めない。鍵管理は各人が一組の鍵を持つだけで複数の人と通信でき、秘密に管理しなけ

ればならないのは自分の秘密鍵ひとつだけであるという有利な特徴がある。

また、秘密鍵で暗号化して公開鍵で復号化することもできる。送り手は自分の秘密鍵で暗号化し、受け手は送り手の公開鍵で復号化できると、秘密鍵を知っているのは送り手だけであるから誰も送り手になりすますことができず、送られてきたものは確かには送り手からのものであることが証明でき、かつ送り手は送った事実を否認できない。

(3) ハッシュ関数

ハッシュ関数は、任意長のデータを固定長に圧縮する関数で次の２つの性質を持つ。

①同じ圧縮結果が得られる２つの元のデータを見つけることが困難である（衝突をおこしにくい）。

②ある特定の圧縮結果を抽出できるような元データを見つけることが困難である（圧縮結果から元データを見つけられない）。

代表的なハッシュ関数には、ＭＤ５, ＳＨＡがある。

データが変わればデータのハッシュ値が変わるため、データとデータのハッシュ値を保持することにより、後にデータに改変があったかどうかが検知できる。

しかし、ハッシュ関数はだれにでも使用できるため、まったく別のデータを用意してあらたにハッシュ値を求め、あたかも最初からそのデータであったかのように工作することは可能である。これに対抗するために、次に述べるＭＡＣやアクセス制御といった技術が重要となる。

(4) デジタル署名（Digital Signature）

デジタル署名は、暗号ベースの電子署名（Electronic　Signature）を言い、公開鍵暗号方式が採用され、下記の特徴を有す。

・第三者には偽造できない

・作成した本人が否認できない

・誰でも有効性を確認することができるというような性質をもったデータである。

デジタル署名を利用することにより、なりすまし・否認・改ざんを防止する機能を実現する。尚、電子署名は手書き署名を含む広義の表現である。

(5) ＭＡＣ(Message Authentication Code)

ＭＡＣとはデータから生成したハッシュ値を暗号化したものである。正しい鍵を知るもののみがＭＡＣを生成することが可能になるため、偽造を防ぐことが可能である。暗号化は、共通鍵暗号方式、公開鍵暗号方式のいずれで利用可能であるが、各暗号化方式の長所・短所はそのままＭＡＣに引き継がれる。

4.2.2 セキュアプロトコル

(1) ＭＤＮ（Message Disposition Notification）

メッセージを受信後、ＭＤＮに受信者のデジタル署名をつけて返送するＭＩＭＥベースの受信否認拒否機能が提案され、ＩＥＴＦで draft 段階である。送信者は、受信者から返送されるデジタル署名付きレシートにより

・送信したメッセージが配送され、受信者が受け取りを認めた。

・送信したメッセージにデジタル署名をつけていた場合、受信者が送信者を認証し

た。

・送信したメッセージにデジタル署名をつけていた場合、受信者は受信したメッセージの完全性を検証した。

ことがわかる。

ＥＤＩを電子メールベースで行う場合、マルチメディアデータを扱えること、暗号化の有無とデジタル署名の有無の組み合わせが自由なことからＳ／ＭＩＭＥやＰＧＧ／ＭＩＭＥ等を利用して暗号化・認証・送信否認機能を確保し、さらにMDNを採用して受信否認機能を備えることが望ましい。実際に多くのＥＤＩベンダがこれらの機能をサポートし、相互運用性とセキュリティを確保しようとしている。

(2) ＳＳＬ（Secure Socket Layer）

Netscape Communications 社が開発。トランスポート層レベルでのデータ通信をセキュアに行うことを目的とした認証、機密性、完全性を保証するハンドシェイク型の暗号化プロトコル。WWWの通信をセキュアにするプロトコルとして標準的に採用されている。アプリケーションとＴＣＰの間のソケットレベルでアプリケーションとは独立に機能するため、ＨＴＴＰに限らずＦＴＰ, telnet などのＴＣＰ／ＩＰ上のアプリケーション・プロトコルに適用できる。ＳＳＬｖ３では、クライアントとサーバはそれぞれ公開鍵証明書を用いて相互認証を実現している。

(3) ＮＴＰ（Network Time Protocol）

ネットワークに接続されたコンピュータの時刻を同期させることを目的として開発されたプロトコルである。

計算機の日時データを、精度に信頼性のある計算機の日時データに同期させるためのプロトコルである。

また、日時データの信頼性を向上するものとして、ＧＰＳの利用、原子時計等の利用がある。

電子商取引において、「いつ」を公証するためには、計算機が保持してい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。

(4) ＳＥＴ（Secure Electronic Transaction）

インターネット上で安全なクレジットカード決済を行うためのプロトコル仕様である。暗号化技術を使ったメッセージの形式、本人認証の方法、およびこれらのセキュリティ機能を使ったカード会員、加盟店、決済ゲートウェイ間のトランザクションフローを定義している。取引事実否認防止機能はもたず、各インプリメンテーションにおけるルールとポリシーに委ねられている。

4.2.3 ハードウェア

(1) Write Once

文字どおり一度しか書き込みができない仕組みとなっているデバイスである。一度しか書き込みができないため、改ざん防止に効果が期待できる。

(2) 耐タンパー装置

耐タンパー装置は、情報の不正な読み出しや書き換えを防止する装置である（タンパーとは不正にいじることを意味する）。

鍵のようにソフトウェア的にもハードウェア的にも他人が読み出せては困る情報を格納する。たとえば、暗号化、複合の鍵だけではなく暗号アルゴリズムも装置内に保持することにより、鍵を知られずにすむ。装置を解析しようとして筐体や部品を外そうとすると、データが消去される仕組みになっているものもある。

4.2.4 応用

4.2.4.1 アクセス制御

“何時、誰が何をしたか”を証明するにあたり、コンピュータシステムの利用者が誰であるかが正しく判断され（認証機能）、その後、情報等へのアクセスをその人物の権限や属性に依存して適切に制御する必要がある。このアクセス制御機能が不十分であると”誰が何をした”の記録が適切に保存・管理されるとしてもその内容に対する信頼性は確保されない。アクセス制御は、その機能が正しく動作すること、運用上適切な設定が適時行われていること、そしてモニター機能として信頼できる記録が蓄積されること等を必要とする。オープンネットワーク上では多くのシステム構成要素が関係しておりアクセス制御も各要素毎に検討しなければならない。人為的原因による各種の脅威の多くは適切なアクセス制御により排除することができる。今日企業内ではパーソナルコンピュータ、ＬＡＮ、ＷＡＮの導入により従来に比較してますます不正アクセスの脅威が増大している。さらに企業間情報交換の場、情報の受発信の場は企業内にあり、企業内システムとは既にシームレスな環境にある。企業内におけるアクセス制御は企業内システムだけでなく企業間情報交換における安全性・信頼性確保の基本要件でもある。

4.2.4.2 電子メール

電子メールは当事者間で情報を交換する際にもっとも多く利用されるツールである。うまく利用すれば一般業務の効率化も可能であり、電子商取引においても今後多くの局面で利用される。しかし、標準電子メールでは、プレーンテキストでデータを送信すること、さらにその転送プロトコルの特性のため、商取引はもちろんのこと常日頃から電子メールに対して盗聴、なりすまし、改ざん等の脅威が存在している。それら脅威に対抗するために、送受信者間でのエンド・ツー・エンドのセキュリティを確保するためにいろいろな技術、規格が開発されている。それらは公開鍵暗号やデジタル署名技術を利用しており、代表的なものとして下記がある。（詳細は添付資料にある）

(1) Ｓ／ＭＩＭＥ（PKCS Security Service for MIME）

ＲＳＡデータセキュリティ社が提案しているセキュアメールの規格。デジタル署名、データの暗号化、デジタル署名とデータの暗号化の３パターンが可能。公開鍵の正当性を保証する証明書は利用してもしなくても良い。証明書を利用するとき、認証機関等証明書の入手方法については規定していない。公開鍵の正当性の問題から、証明書を利用する方式を利用することが望ましいが、広く相互運用性を確保しようとするとき、認証機関等のしくみの問題がある。

(2) ＰＥＭ（Privacy Enhanced Mail）

RFC1421―1424 で定義されている。デジタル署名でなりすましと改ざんを防止し、データの暗号化で盗聴を防止するセキュアメールの規格である。デジタル署名は必須

であるが、データの暗号化はオプショナルである。

(3) ＰＧＰ（Pretty Good Privacy）

米国の Philip Zimmerman 氏によって開発された暗号化、デジタル署名、鍵の管理などの機能をもつアプリケーション。フリー・ソフトウェアとして流通している。ＭＩＭＥに対応したＰＧＰ／ＭＩＭＥがＩＥＴＦで標準化作業中である。データの暗号化アルゴリズムにはＩＤＥＡ，ＣＡＳＴ等を使用する。公開鍵の正当性の保証は、ユーザ各個人の判断に委ねられる。誰かが誰かの公開鍵を信頼する場合、その公開鍵に自分の鍵で承認を与えるという「ユーザ個人の信頼の輪に基づく鍵管理方式」である。電子商取引では、取引当事者間で公開鍵の正当性を保証するルールの検討が必要である。

4.2.4.3 零知識証明

相手認証に用いられる方法である。原理は、本人認証を行う際、本人でなければ知ることのない秘密情報に対して、本人でなければ回答できない数個の質問をし、相手からの回答から本人を確認する。

零知識証明法がパスワードなどの相手認証と異なる点は、質問とその回答を当事者以外のものが盗聴していたとしても、秘密情報を知ることができない仕組みとなっていることである。

4.2.4.4 情報の分割

一人で管理するには危険であると判断されるような重要な情報に対して、当事者で情報を分割共有するための技術である。元の情報に復元する際は、分割した情報を収集しなくてはならい。なお、当事者の一人が不慮の事故のように分割された情報の消滅のために元の情報に復元できなくなる自体を回避するために、分割したデータのうち、一部だけで元に復元できる方式もある。情報の分割は、暗号鍵管理（Key Recovery）に応用されることが多い。

4.2.4.5 ワンタイムパスワード

パスワード認証では同じ認証データがネットワーク上を何度も移動し、このため盗聴・攻撃の脅威がある。この問題を解決するために毎回異なるパスワードを使用してパスワード認証を行う方法である。パスワード生成には固有のアルゴリズムや同期手法を用いるが、多くの場合、ユーザに固有のパスワード発生器を利用する。ネットワークシステムへのアクセス、リモートシステムへのアクセスに利用される。

4.2.4.6 電子透かし

静止画、動画、音声等のマルチメディアのコンテンツの中に密かに著作権情報を埋め込み（透かし情報）、データの流通や利用権の有無などを検査するためのしくみである。”data hiding”や、”digital watermarking”、または”steganography”と呼ばれることもある。デジタル化された情報の流通が盛んに行われるようになってきた今日、電子透かしは、不正コピーの検出が可能であるため、著作権保護のための有効な技術として期待されている。

電子透かしの特徴として以下が挙げられる。

・透かし情報は、編集、圧縮、変換処理等を施されても消去されない
・透かし情報は、利用者に検知されにくく、改竄や削除が困難
・透かし情報を埋め込んでも品質は劣化しない

電子透かしの実現方式として、人間の視覚や聴覚の感度が鈍い周波数帯のデータにノイズとして埋め込む手法が多く提案されている。

4.3 電子公証モデル

既に述べた通り『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。

4.3.1 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。

・「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。

・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。

・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。

・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。

・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。

4.3.2 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

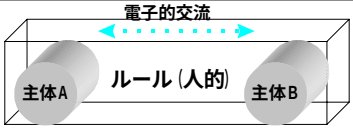
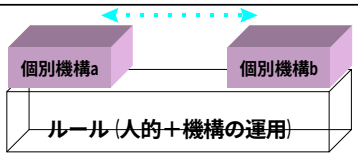
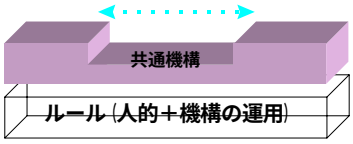
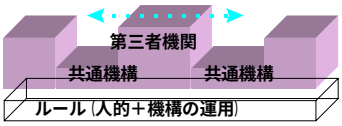
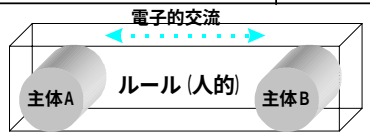
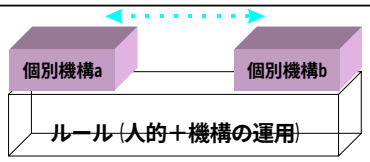
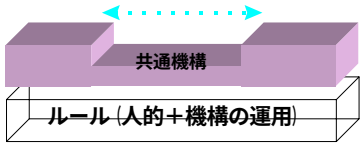
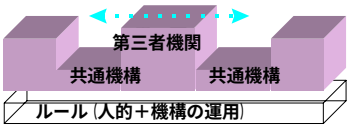
タイプ	モデル	説明
I		当事者間において、特に安心･安全の一部を保証する電子的機構をもたない。例えば、何のセキュリティ機構も組み込まれていない電子メールシステムを利用して商取引に関する情報をやり取りしている。
II		当事者間に固有の電子的機構を内部に持ち、当事者間のみに通用する仕組みにより安心･安全の一部を保証する。 例えば、当事者間のみの事前取り決めによって、内容／フォーマットなどを規定し暗号化などし商取引情報をやりとりしている状況（従来のEDIに近い状況）
III		一般的に認知された電子的機構を当事者のそれぞれが内部 に共有する。例えば、標準セキュリティプロトコルが組み込ま れた電子メール、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

4.3.3 電子公証モデル適用の考え方

「4.1.1　電子公証機能」で述べたように、安全・信頼性を確保して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

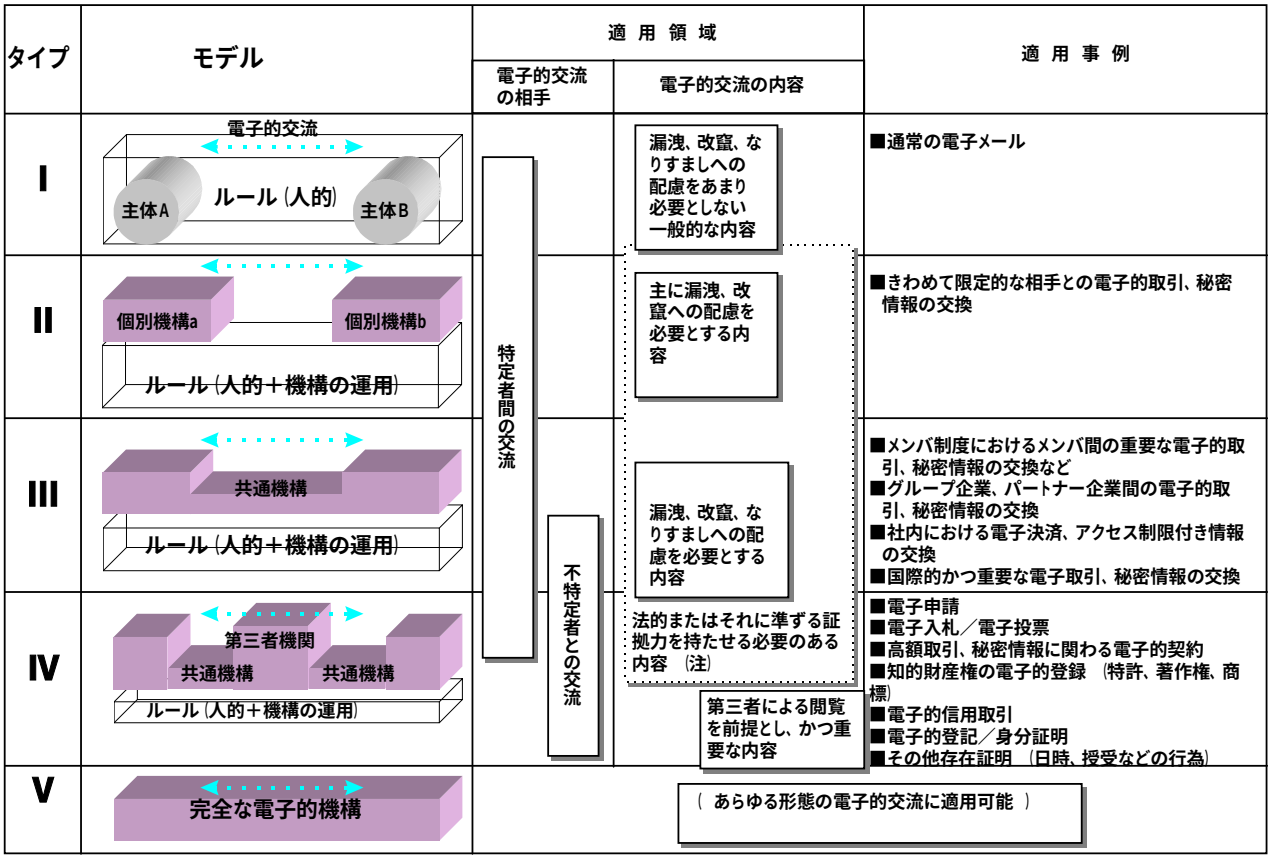


図 4-3電子公証モデルと適用領域

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

4.4 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既に考慮されていなければならず、加えて運用上も組織コントロールのもとに行われていなければならない。即ち、企業内で導入・運用されているシステムにはそれなりの安全性・信頼性があると考えられ、そのシステムの多くは前節のモデル Ⅳ に相当する。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企業内外を接続するファイアーウォールと電子公証システムの関係について考察する。

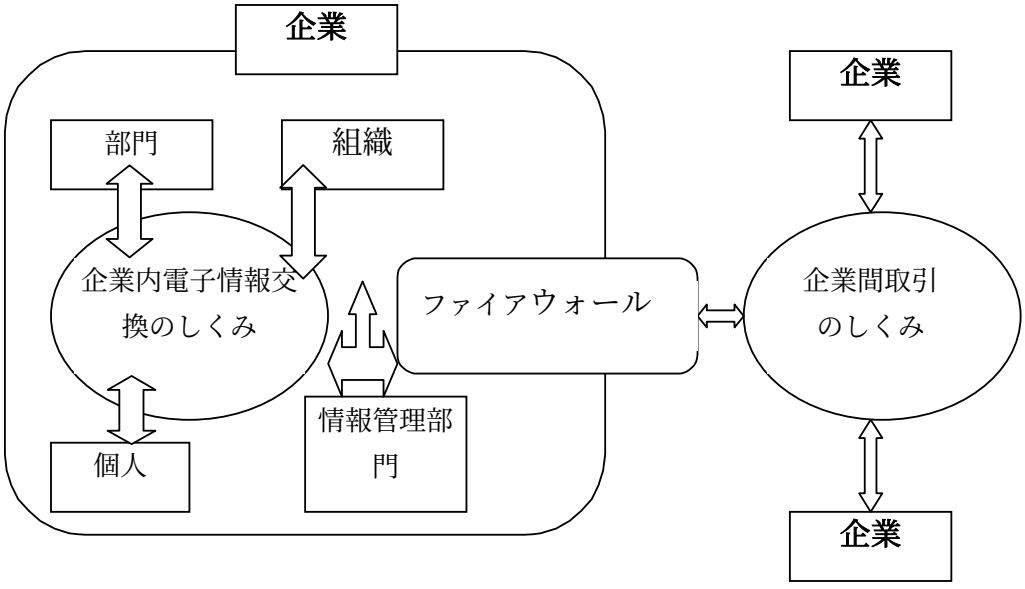


図 4-4企業内と企業間の情報交換の場

4.4.1　企業間の電子公証システム

企業間の電子公証システムも、企業内の電子公証システムも要求される機能は同様のものも考えられる。この節では、主に企業間だから必要もしくは強化が必要だと思われることについて触れ、それぞれのモデルにおいて、要求される機能を実現するためのシステム要件(人的な運用ルール要件も含む)とシステム概念図を例示する。

4.4.1.1　企業間の電子公証のシステム要件

取引金額、取引相手との関係、取引内容を秘匿することの必要性等によって電子公証モデルにおけるシステム要件・運用ルール要件のレベルは異なり、構築にかかるコストも変わる。一般に要件のレベルが高ければ高いほど、かかるコストも高くなると考えられる。

従って一般には、その取引にどの程度安全性・信頼性を必要とするかという要素と、いくらまでコストをかけられるかという要素の天秤で、使用する電子公証モデルが決定すると考えられる。ただ、一取引ごとにレベルの違う複数の電子公証システムを使い分けるということは現実的には考えにくく、自企業でもっとも頻繁に行われる種類の取引の、安全性・信頼性の要求度に合わせて電子公証モデルを選ぶということになると考えられる。

例えば、事務消耗品の発注～決済という取引と、自社の先端技術を用いた開発品の受注～決済という取引を電子商取引で行うとして考えてみると、事務消耗品の発注～決済と、自社の先端技術を用いた開発品の受注～決済の２取引間では、要求される安全性・信頼性の度合いが異なるということは明らかであり、このことは電子公証モデル間でシステム要件や運用ルール要件が異なるということについての説明となる。また、仮にこの企業がモーレツな企業で、自社の先端技術を用いた開発品の受注～決済取引が毎日何件も行われるのに対し､事務消耗品の発注～決済取引は半期に一度まとめて行う程度の頻度だった場合、当然電子化すべき取引は自社の先端技術を用いた開発品の受注～決済取引ということになろう。第三者機関を介在させず自前で電子公証システムを構築した場合、自社の先端技術を用いた開発品の受注～決済取引が電子化された後では、事務消耗品の発注～決済取引はそれ自身では必要もない高度の安全性・信頼性をもって自社の先端技術を用いた開発品の受注～決済取引と同じシステムを使って電子商取引されるか、現状通り電話やＦＡＸで行われることになろう。

以下この節では、４．３の各電子商取引モデルで、４．１で挙げた電子公証機能をどんな手段で実現するか(すなわちシステム要件・運用ルール要件)を説明する。

①　モデルタイプⅠ

このタイプは電子メールのやり取りを除いてシステム的なものはなく、残りすべてを人的ルールでカバーするものである。

表 4-2タイプⅠ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	―	当事者間で相手を確認できるように取り決める。(電子メール本文中で名乗る、合言葉、ID コード、当事者しか知り得ない情報を共有するなど)
到達確認機能	―	当事者間で受信確認の方法を取り決める。(受信した旨の返信電子メール、発信者が受信者へリアルな手段（TEL、FAX、口頭など）や電子的手段(時間をおいて受信確認電子メールを送信するなど)で確認するなど)
改竄検知機能	―	当事者間で内容確認の方法を取り決める。(受信した内容を返信電子メール、発信者が受信者へリアルな手段（TEL、FAX、口頭など）や電子的手段(時間をおいて内容確認電子メールを送信するなど)で確認するなど)
時刻付与機能	―	当事者間で時刻付与の方法を取り決める。(受発信する電子メール本文中に入力するなど)
電子保存機能	―	当事者間で電子保存の方法を取り決める。(保存する対象、保存期間、ファイル書式などの取り決め)
アクセス記録機能	―	当事者間でアクセスできる範囲、記録の方法を取り決める。(電子メール以外のデータには触れない、もし触れてしまったら、時刻、時間、ファイル名を相手に知らせるなど)

② モデルタイプII

モデルタイプⅠで人的ルールでカバーした範囲を、若干システムに置き換えた段階。この段階では、当事者はそれぞれ異なったシステムを用いているため、相互間の凸凹を埋めるための人的ルールが必要である。

表 4-3タイプⅡ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	公開鍵または共通鍵暗号方式を使い、電子メール本文が正常に開ければ本人からの情報とみなす。	それぞれ当事者が相手の鍵を個別に保存する。鍵が相手本人のものであるかどうかは、それぞれ当事者が自己の責任において確認する。(電話、FAX、面談によるリアルでの確認など)
到達確認機能	当事者間だけの固有の方法で返信メールの送信時刻を電子メール本文に付与する。(従来の EDI がこれに近い。)	当事者間で受信確認の方法を取り決める。(受信した旨の返信電子メール、発信者が受信者へリアルな手段（TEL、FAX、口頭など）で確認するなど)
改竄検知機能	公開鍵または共通鍵暗号方式を使い、電子メール本文が正常に開ければ改竄のない情報とみなす。	仮に正常に電子メールが表示されたとしても、確認する必要のある項目などを取り決める必要がある。(金額や時間などが電子メールの内容に含まれているときは、別途確認するなど)
時刻付与機能	当事者個々のシステムの時計を使う。	当事者間で時刻付与の精度維持方法を取り決める。(定期的に一回標準時刻に自システムの時計を合わせるなど)
電子保存機能	記憶媒体に当事者それぞれが保存する。	当事者がお互いに保存媒体、ファイル書式などを事前に通知する。
アクセス記録機能	当事者が自システムの非公開部分については独自にセキュリティを施す。	当事者間でアクセスできる範囲を取り決める。

③ モデルタイプIII

モデルタイプⅡでは、当事者がそれぞれ異なるシステムを使っていたのに対し、このモデルタイプⅢの段階は当事者は同じシステムを使っている。あるプロトコルやアプリケーションが広まり、事実上の標準(デファクトスタンダード)となったような段階がこれにあたる。

尚、この段階で認証局を利用するかしないかは任意だが、ここでのモデルは共通的機構の例として認証局の利用を前提としている。認証局を利用しない場合は、使用する場合よりスケーラビリティは低くなる。またその場合、公開鍵が相手本人のものであるかどうかは、それぞれ当事者が自己の責任において確認(電話、ＦＡＸ、

面談によるリアルでの確認など)し、相手の公開鍵を個別に保存する。

表 4-4タイプⅢ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	お互いに到達確認のできる機能を持ったソフトウェアや標準的なプロトコルを採用する。	当事者間で通信のどの段階で到達したとみなすかの取り決めを行う。
改竄検知機能	標準的で同じアルゴリズム(RSAなど)の公開鍵暗号方式を使ったデジタル署名を電子メール本文に添付し、受信者はそれを検証する。	暗号技術の強度に対しての共通認識が必要である。
時刻付与機能	標準時刻と自システムの時計の同期をとる。またはNTP(ネットワークタイムプロトコル)を採用する。	当事者間で時刻付与の精度維持方法を取り決める。(定期的に標準時間に自システムの時計を合わせるなど)
電子保存機能	物理的には、書き換え不可能な記憶媒体に当事者が個々に取引プロセスを保管し、論理的には暗号化やデジタル署名を用いて、データの真正性・見読性・保存性を確保する。	当事者間で左記の電子保存の方法、ファイル書式、再生のためのソフトウェアなどを取り決める。(必ずしも当事者双方で保管しあう必要はない。)
アクセス記録機能	電子メールによるやり取りの他、当事者間で共有するファイルがある場合(Web 上にデータを書き加える場合など)は、アクセス記録機能のアクセス制御・アクセス記録・プロセス記録のうち、ここではアクセス制御を重視し、非公開データについての保護を行う。	当事者は相手がアクセスできる範囲を取り決める。

④ モデルタイプⅣ

当事者以外の第三者機関が取引に介在しているのがこのタイプである。第三者機関は、必ずしも直接取引に介在するとは限らず、認証局のように間接的に取引に介在するものもある。また、この第三者機関は公的機関か否かは問わない。

表 4-5タイプⅣ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。

⑤ モデルタイプV

完全に人的ルールを介在せず、すべて電子的に処理する理想の段階で、現在はまだ未知の段階である。従って、ここではⅠ～Ⅳのモデルのようなマトリックスは作成困難である。但し、ここで登場する電子的機構に対しての法的な位置付け(絶対的な証拠能力の保証)、保存ファイルの書式の決定は、人的ルールとして必要である。

4.4.1.2 システム概念図（例示）

ここでは、4.4.1.1 で検討したシステム要件をそれぞれの電子公証モデルにあてはめ、図示し、あわせて、運用ルールの要件も列挙する。

① モデルタイプⅠ

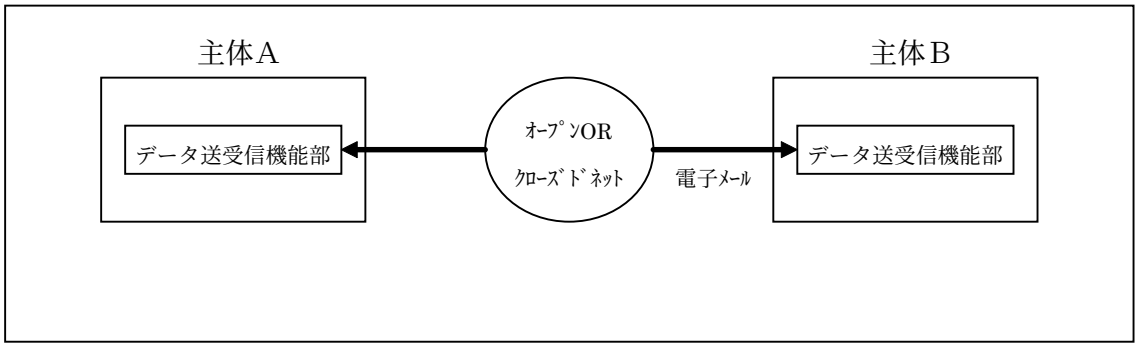


図 4-5タイプⅠシステム概念図

<運用ルール要件(このシステムを使用する際の注意)>
以下の処理方法を当事者間でルール化する。
・通信相手の確認
・電子メール到達の確認
・電子メールの内容の確認
・時刻の付与
・電子保存(対象、範囲、ファイル書式)
・アクセスの許可・不許可の範囲

② モデルタイプⅡ

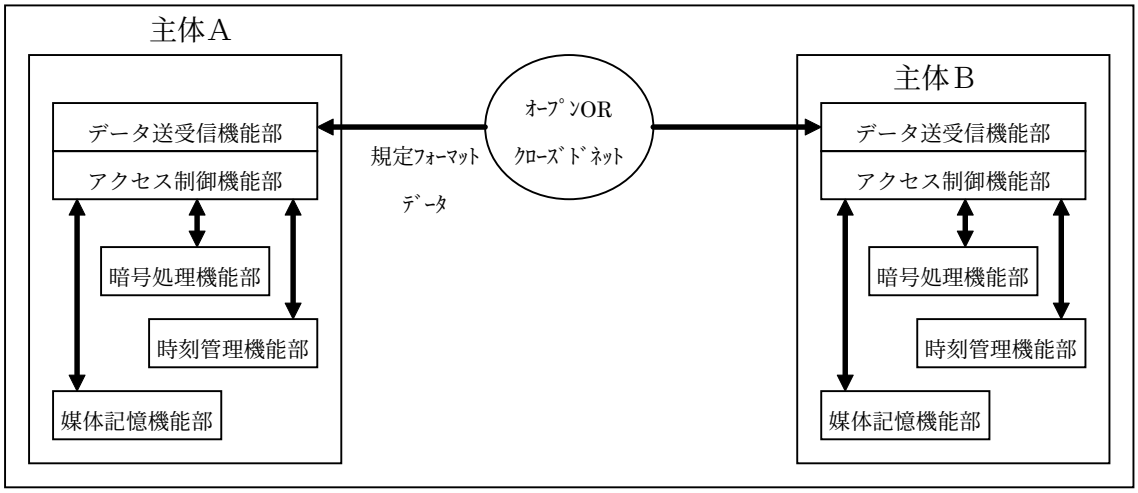


図 4-6タイプⅡシステム概念図

<運用ルール要件(このシステムを使用する際の注意)>
以下の処理方法を当事者間でルール化する。
・相手の鍵を保存する際の本人確認
・電子メールの到達確認

・電子メールの内容の中で確認する必要のある項目の決定と具体的確認
・自システムの時計の精度維持
・使用する保存媒体の事前連絡、ファイル書式などの決定
・相互にアクセスを許可する範囲の決定

③ モデルタイプIII

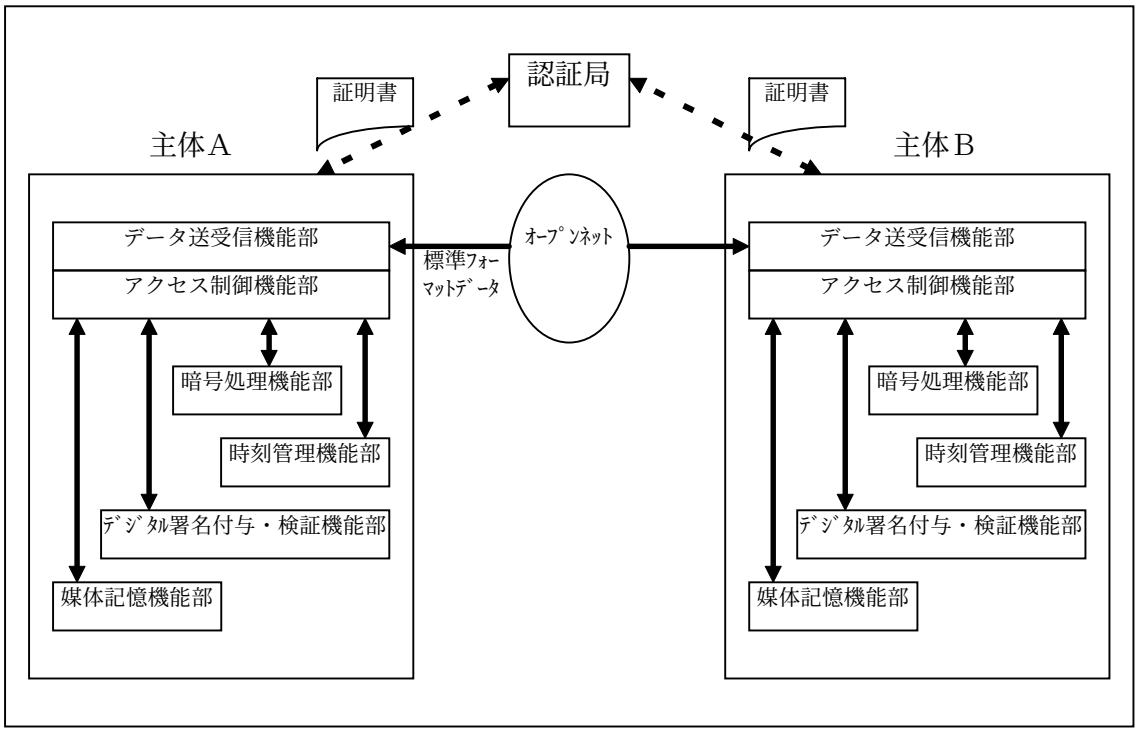


図 4-7タイプⅢシステム概念図

<運用ルール要件(このシステムを使用する際の注意)>
以下の処理方法を当事者間でルール化する。
・利用する認証局の決定
・到達したとみなす通信段階の決定
・暗号技術の強度に対する共通の認識
・自システム時計の精度維持
・電子保存する対象の決定と具体的ファイル書式・方法
・相互にアクセスを許可する範囲の決定

④ モデルタイプIV

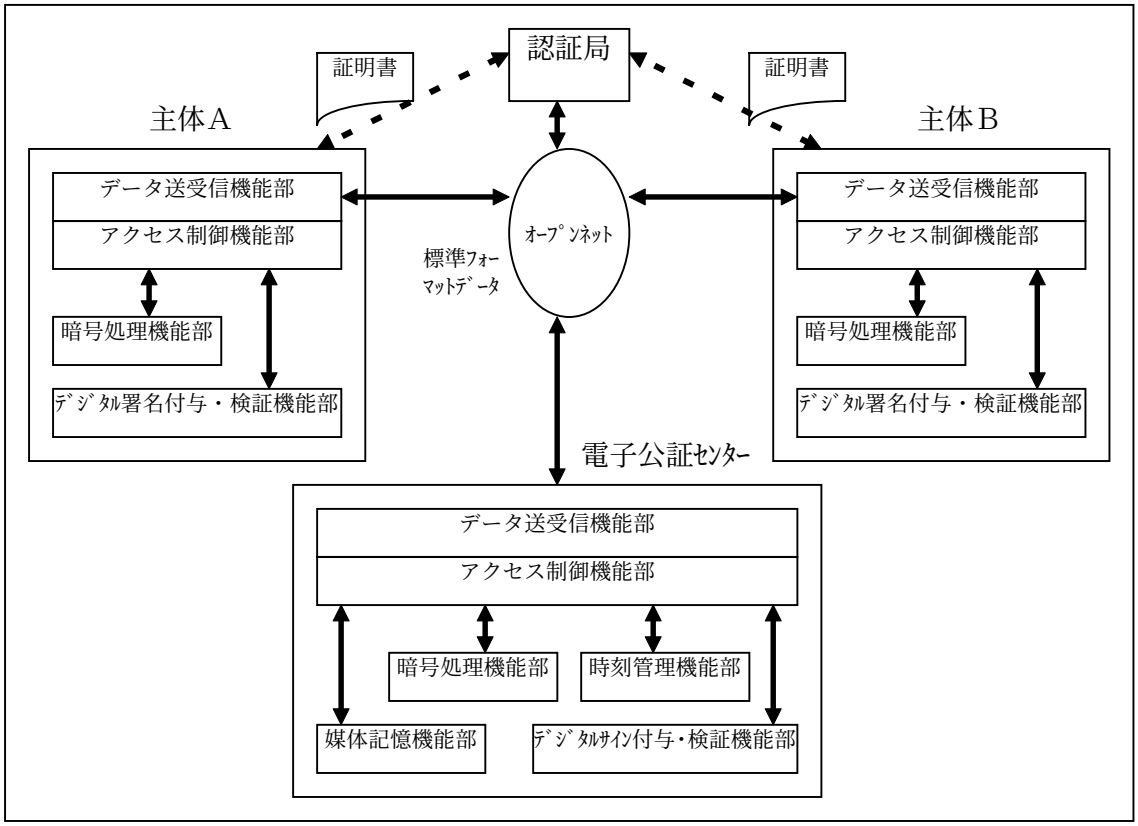


図 4-8タイプIVシステム概念図

<運用ルール要件(このシステムを使用する際の注意)>
当事者は、下記の定められたルールを遵守する。
・認証局の利用規定
・電子公証センターの利用規定
また、当事者間で以下の処理方法をルール化する。
・アクセスを許可する範囲
・保存ファイルの書式、再生のためのソフトウェアの決定

⑤ モデルタイプV

先にも述べた通り、この段階は人的介在を必要とせず、しかも取引当事者が利用する際意識することもなく、電子的交流のすべてが安全に行われかつ保管され、必要に応じ取り出せるという理想的な段階である。現在はまだ到達していないレベルで、ここでのシステム構成図はあらわすことができない。

運用ルール要件としては、この段階に登場する電子的機構の法的な位置付け(絶対的な証拠能力の保証)と、保存ファイルの書式などの取り決めが必要となろう。

4.4.2 企業内電子公証システム

4.4.2.1 企業内における電子公証のシステム要件

企業は企業外とのシームレスな環境のもとで、企業内においても標準的なプロトコルとデータ形式を用いた情報交換を行う必要がある。この要請もあり、多くの場合、市販のグループウエアやワークフローツール等を導入することになるだろう。以下ではごく一般的な状況として既存ツールを用いた各種企業内情報交換を想定し、そこでの要件について述べることとする。

(1) モデルタイプ別に必要とされるシステム要件・運用要件

４．３節で検討した電子公証モデルにより４．１であげた電子公証機能をどのように実現するかを説明する。ただし、企業間の場合は取引きの内容や相手の事情によりモデルタイプⅠからⅣが混在すると考えられるが、企業内システムにおいては企業単独で検討ができることから、最初からモデルタイプⅣのレベルを目指すことが多いと想定される。

① モデルタイプⅠ

適用するツールは企業内電子メールシステムの利用を想定。また、分散システム間通信は適用されていない。

表 4-6タイプⅠ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	メール利用者管理機能が必要	「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」 社内メールシステムを信頼する。
到達確認機能	―	「同上」 業務毎に受信確認方法を取り決める（受信確認メールを返送するなど）
改竄検知機能	―	「同上」 社内メールシステムを信頼する。
時刻付与機能	メーラにヘッダ作成機能が必要	「同上」 業務毎に受信確認方法を取り決める（メールシステムによって付与される時刻など）
電子保存機能	メーラにメールログ機能が必要	「同上」 業務毎に電子保存方法を取り決める（メールログを双方が保管など）
アクセス制御機能	User ID,Password により本人以外の利用を禁止する機能が必要	「同上」 社内メールシステムを信頼する。
アクセス記録機能	メールシステム利用ログ機能が必要	「同上」 社内メールシステムを信頼する。

② **モデルタイプII**

適用するツールは企業内グループウエア、ワークフローツール（個別の製品）の利用を想定。また、分散システム間通信には個別の通信プロトコルを持ったソフトウエアを利用。利用する各ツールは以下ツールと総称する。

表 4-7タイプⅡ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	利用者管理機能が必要	「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」 各ツールについては信頼する
到達確認機能	ツールにステータスを確認できる機能が必要 分散システム間通信では、相手が確実に受信したことを確認できるプロトコルツールにステータスを確認できる機能が必要	同上
改竄検知機能	ツールに公開鍵方式などによる暗号化機能が必要	同上
時刻付与機能	ツールにヘッダ作成機能が必要	同上
電子保存機能	ツールに文書データベース機能が必要	同上
アクセス制御機能	User ID,Password により本人以外の利用を禁止する機能が必要	同上
アクセス記録機能	トランザクションログ機能が必要	同上

③ **モデルタイプIII**

適用するツールは企業内グループウエア、ワークフローツール（個別の製品でありツールと総称する）の利用を想定。また、分散システム間通信には標準の通信プロトコルに対応したソフトウエア（ＥＣ，ＥＤＩ）を利用。

表 4-8タイプⅢ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が必要	「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」各ツールについては信頼する
到達確認機能	ツールにステータスを確認できる機能が必要 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	同上
改竄検知機能	ツールに公開鍵方式などによる暗号化機能が必要	同上
時刻付与機能	ツールにヘッダ作成機能が必要	同上
電子保存機能	ツールに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が必要	同上
アクセス制御機能	User ID,Password により本人以外の利用を禁止する機能が必要	同上
アクセス記録機能	トランザクションログ機能が必要	同上

④ モデルタイプⅣ

適用するツールは企業内グループウエア、ワークフローツール（個別の製品でありツールと総称する）の利用を想定。また、分散システム間通信には標準の通信プロトコルに対応したソフトウエア（ＥＣ，ＥＤＩ）を利用。さらに、法律等で規制される文書類については第三者機関のサービスを利用する。

表 4-9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	モデルタイプⅢに加えて 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	モデルタイプⅢに加えて 法律等で規制されるものについては電子公証センターに送受信の仲立ちをしてもらう	「同上」 電子公証センターの利用規定に従う
改竄検知機能	モデルタイプⅢに加えて 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	「同上」 電子公証センターの利用規定に従う

	改竄証明を利用	
時刻付与機能	モデルタイプⅢに加えて 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	モデルタイプⅢに加えて 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	モデルタイプⅢに加えて バイオメトリクスな認証機能が必要	「同上」
アクセス記録機能	トランザクションログ機能が必要	「同上」

補足）グループウエア、ワークフローツールに対する要件

多くの場合企業内における部門間情報交換は、基本的にはグループウエアやワークフローツールを導入整備する事で対応できると考えられる。これらの製品には以下のような機能が必要とされる。

A. 必要とされる基本的なシステム要件・運用要件

a) 申請・決裁プロセスをロギングする機能

・プロセスとデータを検証可能にする

b) ロギング情報の改竄を防止する機能

・コンピュータ記憶装置への不正アクセス・改竄を防止する

c) 決裁者・決裁ルートの改竄を防止する機能

・なりすましやシステムの環境を改竄することを防止

B. より信頼性を上げるために必要とされるシステム要件・運用要件

a) 本人確認機能

従来のユーザＩＤ＋パスワード方式では高い信頼性、利便性を確保することが難しいという問題がある。これに対しては、バイオメトリクスを用いた手書きサインや指紋による照合システム、ＩＣｶｰﾄﾞやワンタイムパスワード生成器による認証システムとの連携により信頼性を向上することができる。

b) 暗号鍵証明書による個人およびサーバ認証機能

社外の第三者機関を利用するケースと社内でサーバを構築・運用することが想定されるが、経済性、要求される認証レベルを考慮した検討となる。

c) ロギングから目的のプロセスとデータを適確に引き出せる公証機能の仕組み

・問題の発生した取り引きについて、大量データから効率的に抜きだす仕組みが必須である。

・そのためには、多数の業務について各々取り引き名称・コードおよび記録する情報の標準化を中心とした運用の確立が必要となる（外部とはＥＤＩの標準化の制定）。

d) システム管理者からの脅威にも対抗できる機能

現在販売されて利用されているソフトウエア製品は、一般利用者からの不正アクセスには対抗する機能を持っているが、システム管理者などによる内部犯罪に対する対策が不十分である。このため、利用者のパスワード保護、決済ルート等の保護、そしてデータベースの暗号化等の機能が重要である。

4.4.2.2 システム概念図（例示）

以上のことから、社内業務と言えども業務効率化を図ろうと考えた場合、外部企業とのインタフェースが多数発生し、企業間取り引きの仕組みと同じレベルの運用環境が企業内にも必要であることがわかる。

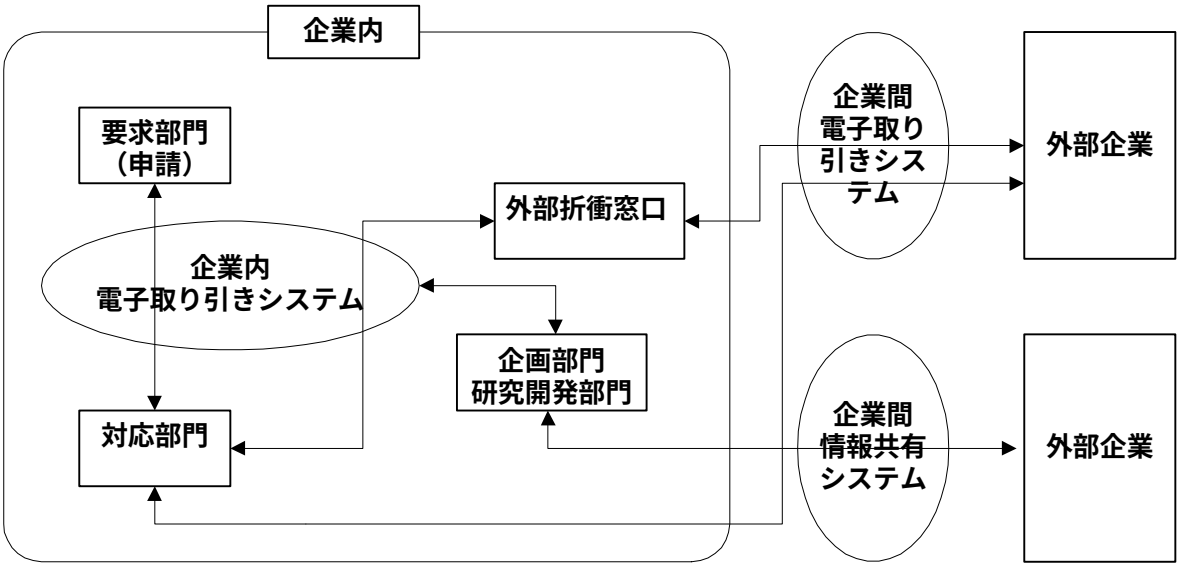


図 4-9企業内と企業間のインターフェイス

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。

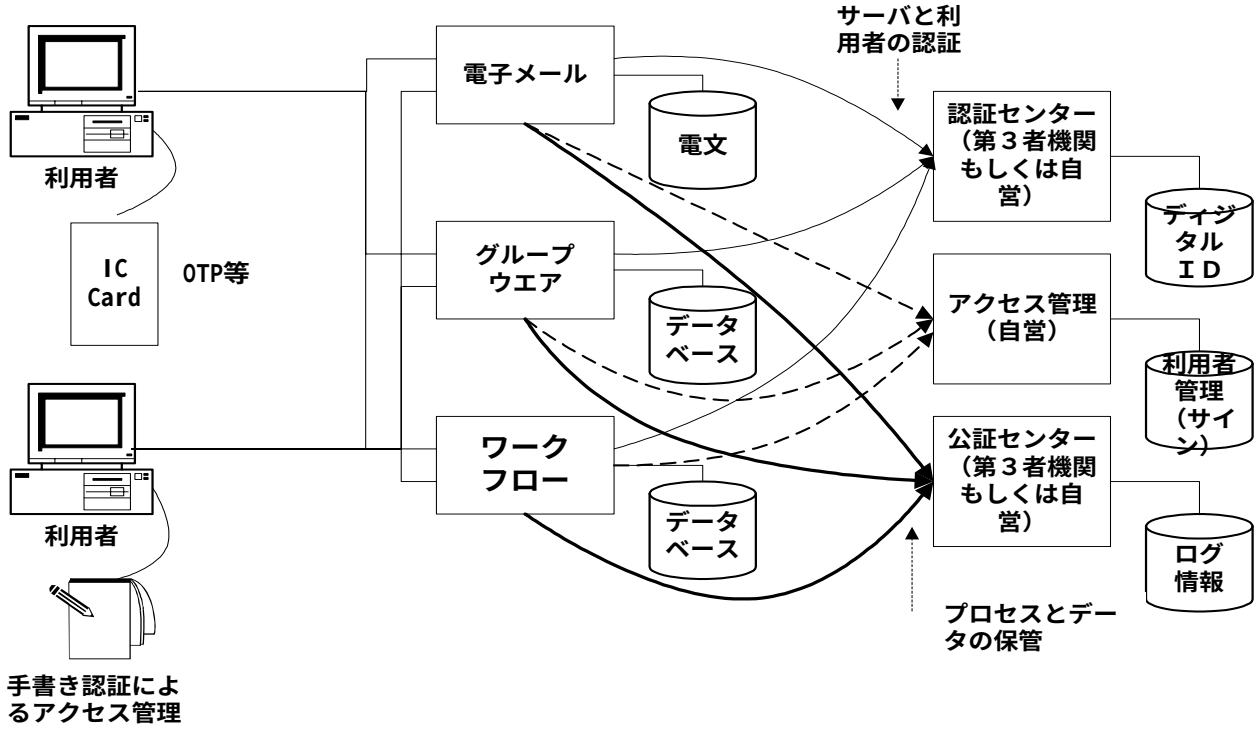


図 4-10企業内電子公証システム図（例示）

4.4.3 電子公証システムとしてのファイアーウォール

企業間情報交換がオープンネットワークを介して行われる時、企業内外の二つの場にはそれらを仲介するファイアーウォールと呼ばれる電子的な情報制御のしくみが配置されている。ファイアーウォールによってはその機能としてアプリケーションレベルで情報の流れを制御・モニターし、その記録をとることができるものがある。例えば電子メールの場合、ファイアーウォール上で電子メールのリレープログラムにより電子メールが転送されると、送受信の宛先、時刻、メッセージＩＤ、相手ホスト等の記録を残すことができる。“いつ誰が何を”を公証するにあたり、“誰が”をソフトウェアシステムやコンピュータホストなどのシステム構成実体に拡張するならば、情報の出入り口であるファイアーウォールの諸機能は特に企業間取引きにおいて重要な電子公証の機能をも提供していることになる。本来ファイアーウォールは企業内ネットワークを保護する目的で配置されている。しかしながら企業内システムと企業間ネットワークの間にあって、中立的な役割を果し、さらにその安全性、信頼性が十分であるならば電子公証システムとして位置づけることもできる。

今日、ファイアーウォール導入に当たり電子公証システムとしての位置づけの認識はない。ファイアーウォールが有する機能の中で電子公証の諸機能と重なるものは、

・アクセス制御とアクセス記録

・関連機能としての利用者認証機能

であるが、取引当事者がこれらの機能を意識して情報交換を行なうことは少ない。ファイアーウォールは前節の公証モデルではタイプ IV に相当している。今後、ファイアーウォ

ールの記録の信頼性を向上させ公証機能としての認識を高めることにより安全性・信頼性確保の一つの手段として利用することができる。

5 サービス事業者から見た電子公証

5.1 電子公証センターへのユーザの期待

5.1.1 電子公証センターがユーザに利用されるためには

(1) ユーザのニーズに適合したサービス機能を合理的コストで、提供をすること。

即ちユーザが取引相手に対して持っている不安度、個々の取引の重要度、取引段階での内容の重要度、インフラに対する信頼性の不安度等により、コストとの兼ね合いで、適合した公証機能を選択し利用する。

(2) 数ある電子公証センター（以下公証センターという）のなかからユーザに選択されるために紛争時に裁定、調停すると思われる第三者に信頼されること、コストパフォーマンスがよい、利用する際の１回毎の事務手続きが簡便であること等が重要になる。

(3) ユーザに対するコンサルタント業務

適合したサービス機能を選択しているとは限らない可能性がある。

そのようなユーザの相談に答え、教育し、合理的で必要な機能を選択できるようにすることは公証センターの役割の一つである。

又、紛争が起きたとき、紛争になれていない顧客の相談にのること。

このようなサービスも、ユーザの公証センターの選択の際の要因になる。

(4) 利用されるための要件

１、機能が豊富で、ユーザの希望する機能が選択できること。

２、料金が低廉で、ユーザが利用し易い事、又機能により料金が選択できること。

３、センターの経営が公平で、信頼性が高いことがユーザにわかりやすいこと。

４、信頼性が高い技術を使用し、運営管理がしっかりしていること。

５、電子公証の利用の際の事務手続きが簡単で、煩雑でないこと。

（利用にともなうユーザの事務量がそれ程増えず、煩雑にならないこと）

６、ユーザが個々の電子商取引の危険性に合致した機能を選択できるような、判りやすい説明がされていること。

７、商取引の安全への保険として、機能の説明と利用料金の判りやすい提示がされること。

5.1.2 提供サービスの概要

(1) 保険的機能（主要サービス）

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。

(2) 証拠の提出

取引相手との間で紛争が発生し、顧客の要請により取引記録の提出を求められる場面として、以下のような例が考えられる。

１、紛争相手に証拠があることを提示し、紛争を抑止する。

２、調停、裁定の場に証拠として提出する。

提出の方法も、提出後の改竄ができない等が、相手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。

(3) 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。具体的内容としては、

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（もしそのような機関があれば）による認定書の提示
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

(4) 顧客に対するコンサルテーション

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
公証機能の利用の利点と限界
公証機能と法律の関連（商法、税法）
紛争時の法律相談及び裁定、調停機関の紹介

尚（2）、（3）、（4）のサービスは主に紛争発生の時のみのサービスのため特別料金を請求することになると思われる。
即ち有効性証明のため、裁定、調停の場に出頭することも考えられるため、少なくとも実費の請求をせざる得ないと思われる。
利用の際のサービス約款のなかに、顧客の要請があったときは、上記（2）、（3）、（4）のサービスを行うことが、記載されることになると思われる。

5.2 電子公証センターの主要サービスの内容

5.2.1 電子公証機能とサービス

電子公証を実現する上で必要となる機能群は、必ずしもそれをそのまま単独で利用したサービスには結びつかない。単機能のみのサービスで利用者のニーズに対応できる場合はあるが、多くの場合いくつかの電子公証機能およびその他付随的な機能を組み合わせることにより利用者の求める､もしくは利用しやすいサービスが提供できるものと考えられる。

以下サービスについての説明において、その名称が機能と同一もしくは類似する場合でも、実際にはいくつかの機能が組み合わされて各サービスが実現されている。

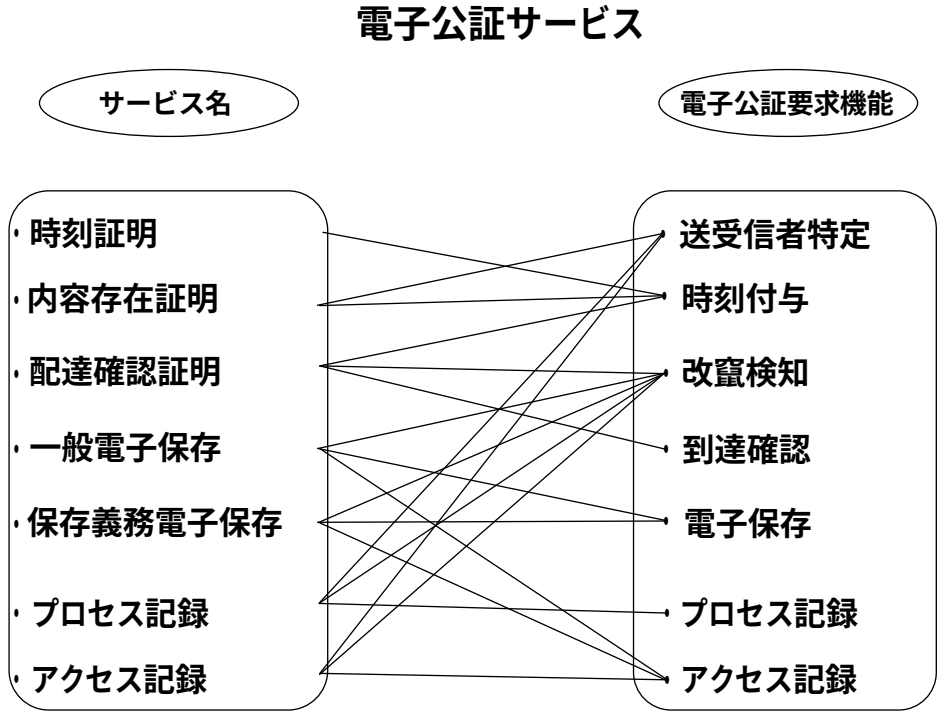


図 5-1電子公証機能とサービス関連図

5.2.2 提供サービスの分類と内容

ここでは，公証センターとして想定される主要なサービスについて，具体的に例示する。

5.2.2.1 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。

(a)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

(b)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

(c)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、電子保存等の用途にも適用が考えられる。

上記の例からわかる通り、時刻証明サービスは単独のサービスとして提供するのではなく、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。（図 5-2 時刻証明の位置づけ）

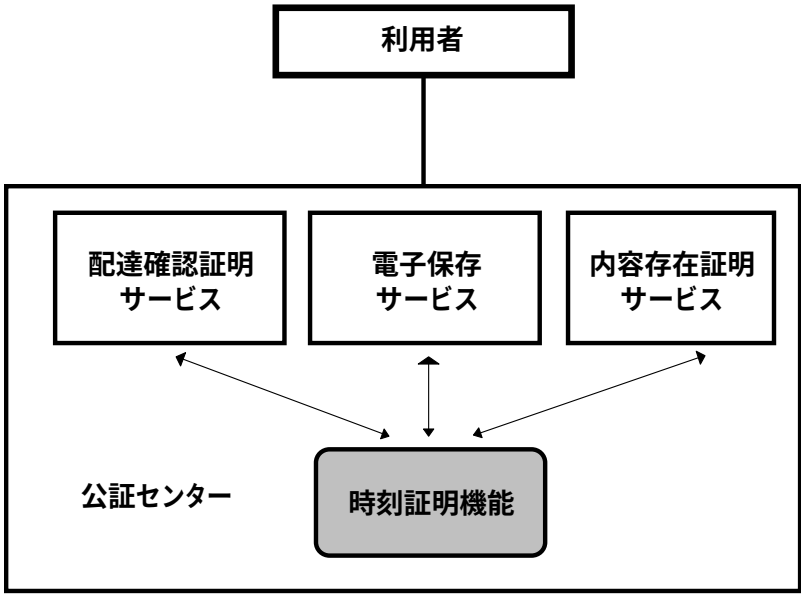


図 5-2時刻証明の位置づけ

なお、タイムスタンプを付与する時点が実際に公証センターへ文書等が到着した時点となるため、ネットワーク上の遅延をどう扱うかが法制度面を含めた運用面の課題事項である。

5.2.2.2 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第三者へ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。

機能要素としては以下の組合わせとなる。

・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）

最後の項目について、どのような内容であったかを証明するためには，公証センターに内容を保管しておけば安全である。しかし簡略な方法として公証センターの秘密鍵で暗号化した文書を当事者へ配布しておき、後日これを解読する公開鍵を証明するこ

とによって代替する事も可能である。当然後者の方法の方が公証センターの設備が少なくてすむ。実際には要求されるセキュリティレベルによって使い分けることになろう。

本サービスは，以下のような分野で利用される。

(a)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

(b)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（先発明主義の場合）

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場合と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。

5.2.2.3 配達確認証明サービス

送信者のデジタル情報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。商取引等において「言った／言わない」の紛争解決のための証拠となる。

電子メールが相手先に確実に到着したことを確認するには、当事者間でルールを設け、受信確認の返信を送付する方法が考えられる。しかしこの場合、返信が失われる事もあるため、まだ相手が読んでいないのか、返信が消失したのか区別がつかない。

また、確かに相手に伝えた事を、後日第三者に証明することが難しい。両当事者の間に第三者機関を置き、送信文書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。（図 5-3 配達確認証明サービス）

本サービスは、以下のような分野で利用される。

(a)電子商取引

例：注文書，請求書

(b)民事的紛糾

例：従来の配達証明郵便の代替

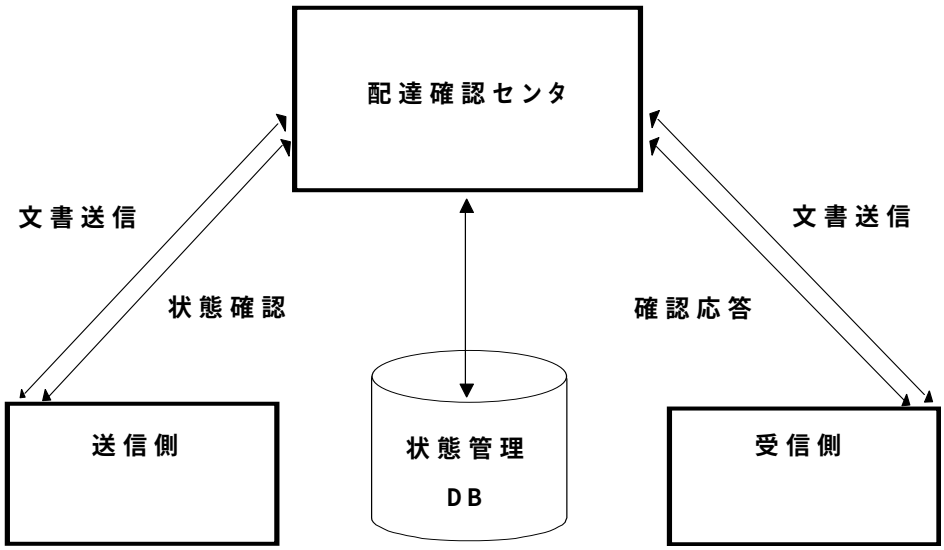


図 5-3配達確認証明サービス

5.2.2.4 一般電子保存サービス

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に応えるサービスを一般電子保存サービスと呼ぶ。基本的に両者の機能は同様であり、詳しくは次項で述べる。

5.2.2.5 保存義務電子保存サービス

法律で保存義務が課せられている各種書類等を電子保存しておくサービスである。

国内では、たとえば表 5-1 主な法定保存文書に示すような文書がある。

当サービスに求められる要件としては、以下が考えられる。

(a)真正性

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

(b)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というわけでもなく、きめ細かいアクセス権制御を必要とする。

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。

表 5-1主な法定保存文書

法定保存文書	保存期間	根拠となる法律・規則
商業帳簿およびその営業に関する重要書類	１０年	商法第３６条
⑴仕訳帳，総勘定元帳，資産・負債・資本に影響を及ぼす一切の取引に関して作成されたその他の帳簿 ⑵棚卸表，貸借対照表，損益計算表，決済関係書類 ⑶現金預金取引等関係書類 ⑷その他の書類(注文書,契約書,送り状等)	７年	法人税法第１４８，１２６～１４６，１５０条 所得税法施行規則第６３，５９～６２，６７条
課税仕入れ等の税額の控除に係わる帳簿または請求書等	７年	消費税法第３０条, 消費税施行規則第５０条
診療録	５年	医師法第２４条，歯科医師法第２３条
株式会社の取締役会議事録および監査役会議事録	１０年	商法第２６０条，株式会社の監査等に関する商法特例法第１８条
雇用保険関係書類	２年 (被保険関係４年)	雇用保険法第１４３条
乗務記録（バス等）	１年	旅客自動車運送事業等運輸規則第２５条
定期自主検査の記録	３年	労働安全衛生法第１０３条，労働安全衛生規則第１３５，１４１条

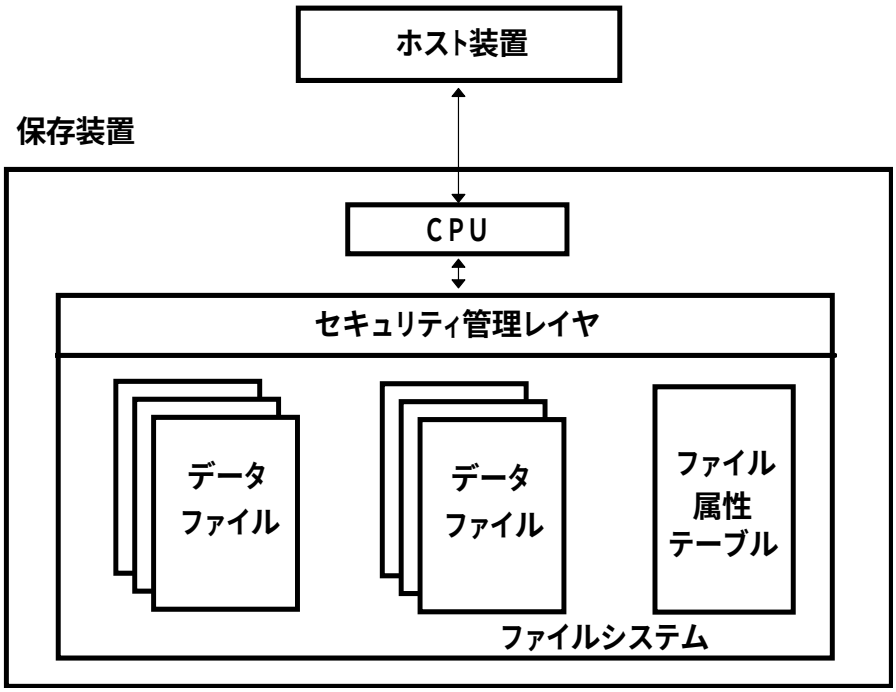


図 5-4電子保存サービスにおけるファイル構成例

5.3 電子公証センターの利用面から見た分類

電子公証センターとして、実現時点での提供サービスや形態から考えていくつかの想定ができる。想定されるものを分類し以下に示す。さらに利用が想定される実ビジネスの特徴的ないくつかの例を以下に示す。

5.3.1 利用方法の分類

ユーザが公証センターを利用する方法として、大事な取引の記録を全て契約公証センターに保管し、全面的に契約公証センターに依頼する方法から、取引内容に合致した特別な機能のみを顧客が公証センターからその都度選択して利用する方法まで幅広くある。

以下、考えられる主な利用方法を列記する。

(1) 会員契約型

特定の会員に対し利用契約を行った上でサービスを提供する場合を想定している。企業内、企業グループ内, 同一目的による個人の集合体などが利用対象と考えられる。

現在でもいくつかの企業グループではネットワークによる相互取り引きなどを行っているが、オープンネットワーク上での新たなビジネス（電子競りなど）が定着した場合にはあらかじめ参加資格を審査し，参加者を限定する場合も考えられるので、この分類はもっとも現実性があるものと考えられる。会員契約の場合、顧客に特典を与えることが多い。即ち、会員割引、ある一定量の無料コンサルタント等である。大事な取引のみで利用するが、コンサルテーションを重視して、会員契約を結ぶ場合もある。

(2) 随時利用型

顧客が公証に精通し、個々の取引に最適に適合した機能を選択し、その機能分野で

権威があり、コストの安い公証センターを選ぶ場合等に利用する。

不特定多数の利用者が参加する場合が想定される分類であるが、単にタイムスタンプ利用型や、事実公証型のサービスを利用する場合と、データ内容公証型のサービスを利用する場合には関与する公証システムのサービス提供時の利用料金などの設定について考慮が必要となる。

(3) 特別機能利用型

例えばタイムスタンプのように、信頼の高い第三者の提供サービスを利用した方が証拠力が高いと思われる機能のみを利用する。資料の保管等の技術的に改竄ができにくい機能は証拠力が採用技術に依存するが、タイムスタンプの証拠力が公証センターの運用管理に依存する場合は、信頼の高い公証センターの機能を利用する。

尚、公証の証拠力が採用技術に全面的に依存する場合は、企業内の自社サーバに公証機能をもたせ、保管することも可能になる。

(4) 特別サービス利用型

例えば、一つの取引でもその途中の工程で、その工程毎に適合した公証機能を利用するが、その後の経過及び取引終了後に公証の必要がなくなることも多い。

それ故、公証センターが一取引毎に取引番号を付与し、取引終了後、取引番号で公証内容を整理し、顧客に提示するようなサービスがある。

又、期限付きの公証機能の場合、顧客への期限切れのお知らせサービス、顧客がある公証を中止してよいかどうか迷ったときのヘルプサービス等も考えられる。

これらはいずれも会員契約の特別サービスになると思われる。

5.3.2 特徴的な公証サービスの例

ここでは、利用面から、どのようなタイプの電子公証センターが実現するかを可能性を含め、類型化してみる。

(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の取り次ぎ、保管を行うサービスである。

取り次ぎを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。

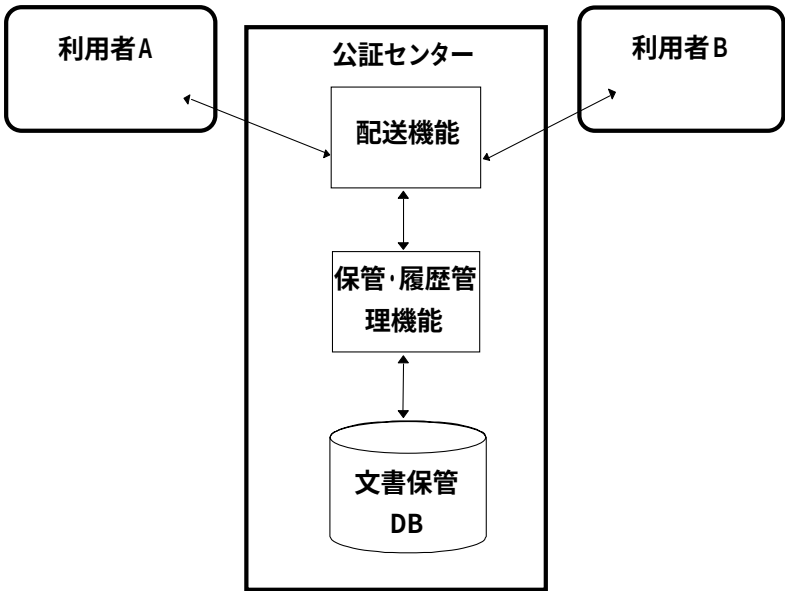


図 5-5配達確認証明サービス

(2) **公証番号重視型**

すべての公証システムにおいて、公証番号は重要なキーであるが、特に「公証番号」に重要な意味を持たせたり、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場合等が考えられる。

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。

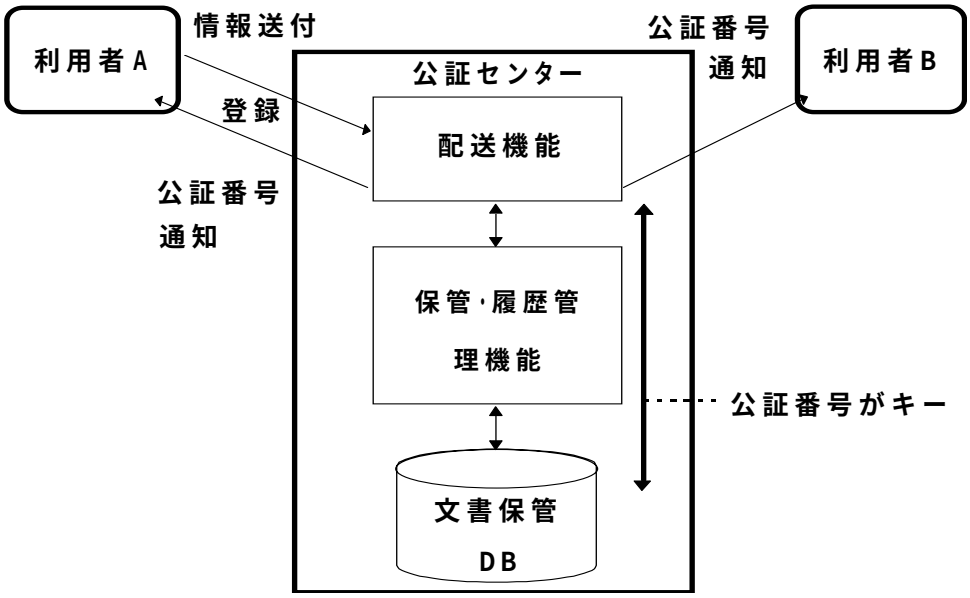


図 5-6公証番号による取引情報通知

(3) **デジタル情報保存型**

電子商取引が盛んになると、特徴的な商品としてネットワーク上で商品そのものを流通することが考えられる。デジタル商品、ソフトウェアなどがこれに該当する。

この場合、当該商品を購入した利用者が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を購入してしまってはいないかなどの危険性がある。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ことになる。

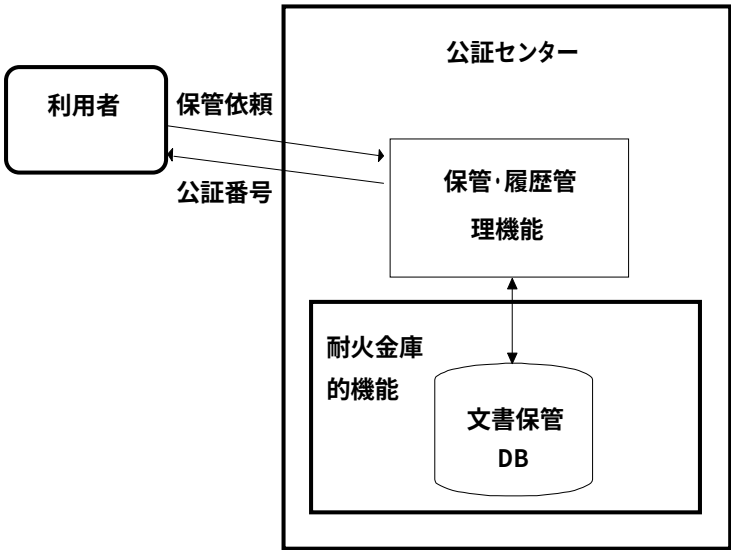


図 5-7デジタル情報保存サービス

(4) **タイムスタンプ利用型**

入札、期限管理、先着順受付等、到着時間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。

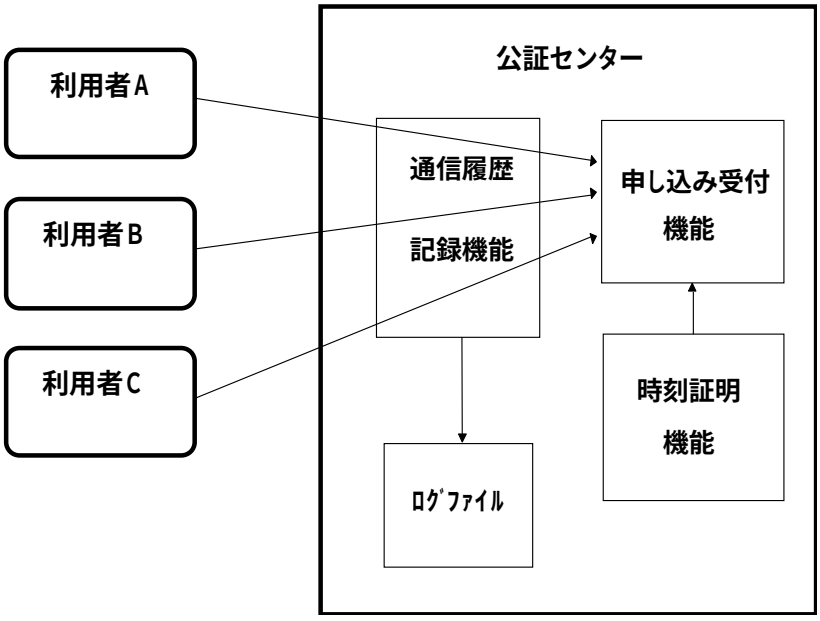


図 5-8タイムスタンプ利用型における通信ログの位置づけ

(5) **広告情報保証型**

インターネット上のホームページで商店（サイバーモール／ウェブショップ）等を開設することにより商取引を行うような分野では、比較的容易にホームページを作成できる事もあり、悪徳業者の横行が懸念される。

サイバーモール利用者からすれば、ホームページ開設者が信頼おける業者である事を保証し、消費者保護センターの役割を代替する第三者機関が欲しい。

そこで、公証センターが発行する公証番号により、ホームページ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「格付け機関」の存在が必要になるのかもしれない。ここでは広告の内容についてあらかじめ審査し登録しておく機関を想定し、現在の映画の映倫制度に類似する役割が期待される。

現在電子マネーやＳＥＴ(Secure Electronic Transaction)を使用したクレジットカードを利用して、インターネット上で売買の決済をする手段が開発されつつあり、今後は広告情報を保証する公証サービスが重要な役割を果たすと考えられる。

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。

5.4 電子公証センターの運営主体について

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。

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。

5.4.1 運営主体の分類

(1) **公的機関・・・**一般的に顧客からみて、証拠力の有効性は最も高く、安全対策はかなり高いが、利用コストは高めで、紛争時の相談、コンサルタントサービスは少ないと思うであろう。

それ故、紛争時に裁判等で争う可能性が高い思われる取引とか、重要な取引記録で長く保管する必要があり、特に紛争時の調停、裁定の場がどこになるか判らない海外取引等での利用が考えられる。

(2) **私的機関・・・**顧客の獲得を図るため、利用コストが安く、利便性、コンサルタントは充実させるであろう。顧客を固定し、収入の安定を図るため、会員特典をつけて、会員契約を増やす施策をとるところも予測される。

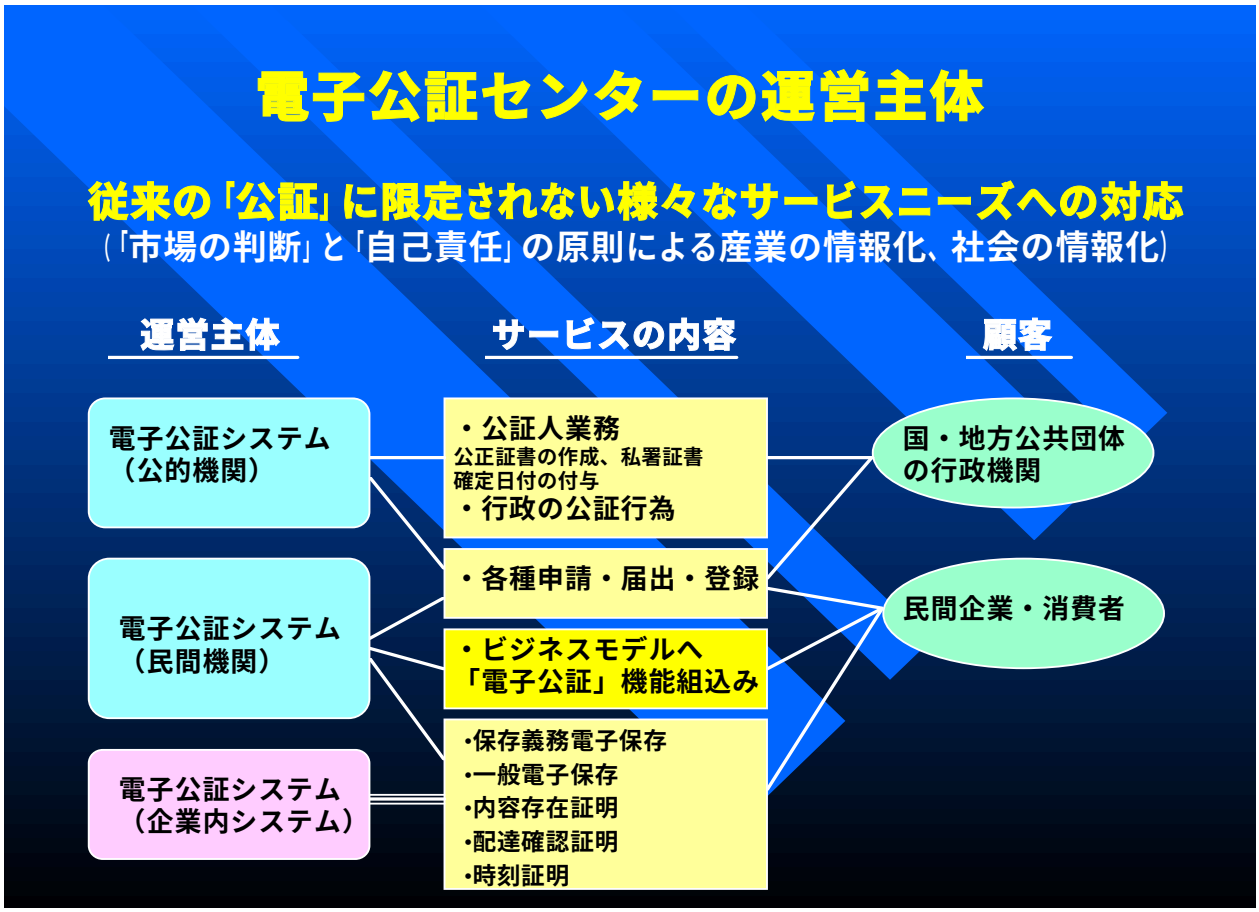


図 5-9電子公証システムの運営主体（例）

5.4.2 私的機関（事業会社）の内容

(1) 事業者

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、ネットワークプロバイダー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。

(2) 事業形態

公証技術の発達により、証拠の有効性が採用技術で保証されると種々の以下のような形態のサービス事業が起きる可能性がある。

1、全機能サービス・・・どんな顧客の要望にも対処する。

2、電子金庫サービス・・主に安全保管のみをサービス。

3、特別機能サービス・・公正な運用管理が必要な機能として、例えばタイムスタンプ機能を、他の公証センターへ、又はユーザの自社シ

ステムへ提供する等のサービス。他に利用コストの安い存在証明サービスのみの提供もある。

4、開発ソフトの販売・リース・・公証技術が発達し、第三者の機関でなくても、採用技術で証拠の有効性が保証されていれば、公証技術のみをユーザに販売する事業があると思われる。サーバは顧客の自社サーバを利用する。バージョンアップ契約の証明のサポート付きサービスも考えられる。

5、コンサルタント業務重視・・・顧客の立場に立った合理的な公証機能の選択、紛争時の相談サービスを充実することで顧客を集める。

5.4.3 電子公証センターの認定、格付け機関

公証センターの証拠力の有効性と安全対策を保証する事業である。公証センター事業者の集まりである協会等が、優良な公証センターの育成を図るための認定機関としてサービスを行う可能性がある。

5.5 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。

例えば、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

安全性に寄与する要件としてはその管理面と技術面の両面があるが、技術要件については次項にまとめる。

安全管理面について電子公証センターとして、天災、外部からのハッカー及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。

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，どのレベルまでの安全性を確保するかは、価格との関係で、運用者とユーザの選択範囲であり，対処すべき安全性の範囲も同様と考えら

れる。したがって、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。

＜既存安全基準の例＞

1.	情報システム安全対策基準	通産省	平成 7 年 8 月
2.	コンピュータウィルス対策基準	通産省	平成 7 年 7 月
3.	コンピュータ不正アクセス対策基準	通産省	平成 8 年 8 月
4.	情報通信ネットワーク安全・信頼基準	郵政省	昭和 62 年 2 月
5.	預金自動支払機(CD)等の防犯基準	警察庁	平成 3 年 6 月
6.	コンピュータシステム・情報通信システムを設置する建築物に係わる安全対策基準	建設省	昭和 61 年 5 月
7.	金融機関等コンピュータシステムの安全対策基準	FISC	平成 3 年 2 月
8.	金融機関等が VAN システムを利用する場合の安全対策基準	FISC	昭和 62 年 3 月

各脅威に対する対策を考察する。

1、天災等

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

バックアップ機器を設置する。

3、外部からの不正

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。

それ故、あるレベル以上の安全対策を持つ必要があると思われる。

此の点が、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

内部の人の不正に対し、管理面からデータの破壊、改竄がにくい仕組みを構築しておくこと。

出来るだけ、 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。

(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 **情報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
（競争入札時に適用する場合など）

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。また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。

特に、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 へなど)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。

5.6 電子公証センターの相互運用面

(1) 公証センターの最低条件

公証センターの相互運用性については公的機関によるサービスの提供と民間機関によるサービスの提供の場合により求められる要件が異なるものと考えられる。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。一方、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一様にガイドラインを制定すべきか議論のあるところと考えられる。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。

(2) 公証センターの信頼性

公証センターが公的機関による運営か、民間による企業運営かに関わらず、第三者に対して、以下の要件などが満足されていなければならないと考えられる。

・公証内容が事実であると認められること

・公証センターが信頼するに相当すると認められること

・提供される事実が第三者の信頼する方法で提供されること

ここでは、第３点目について求められる要件を「相互運用性」として示す。

公証センターの設立を想定すると、複数の公証センターが設立されるものの各々の間には利用技術に何ら互換性がなく、提供される事実を第三者が信頼することと公証センター自身を信頼することがほぼ同等である場合が一例として考えられる。この場合は、公証センターが特定の利用者や事項に偏っていないことを利用技術によって示すことが必ずしもできないため、運営方法や設立者の信用力などによってこれを示さなければならない。

したがって、これらを公にして常にこれを監視する体制も同時に公にすることが必要と考えられる。他方、設立された公証センターが何らかの方法で技術的互換性を保っている場合が考えられる。この場合には、利用技術自身の持つ信頼性や安全性が公証センターの提供する事実の信頼性と等価と認められることを利用して公証センター自身の信頼性とすることを想定しているものと考えられる。

(3) 公証センターの相互運用性

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。また相互利用サービスが実現すると、進展する電子商取引や電子保存文書の利用拡大も見込まれる。万一係争などが発生した場合において公証センターが提供する事実に対する社会全般からの信頼性や利用に対する許容範囲も拡大するものと期待できる。

相互運用性を確保するには、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と、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が考えられる。前者の場合には、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、後者の場合には少なくとも共通の他の公証センターは認める対象の複数の公証センターと同一の技術を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、前者はフラットな関係と捉え、後者は階層的な関係と捉えることができる。

(4) 運用性の確保と事実の提供

相互運用性を確保することは、利用技術や人的運用などにより実現できると考えられるが、各々の公証センターが自身で保持するデータや事実を交換し提供する場合、その保持する情報に対する内容機密保持やプライバシーの観点から何らかのルールが必要と考えられる。

たとえば企業間で取り交わされる契約書などを公証センターが両者の合意のもとに保管している場合には、両当事者からの閲覧要求については、公証センターがこの閲覧要求を提示したものが当事者であると信用するに足る事実があれば認められると考えられる。しかし第三者が要求した場合には、当事者の双方の合意が必要と考え

られ、無制限にこれを提供することは認められないものと考えられる。しかし、さらには、当事者の間で何らかの係争が発生し、裁判所などが第三者になる場合には、保管を依頼した所期の目的に照らして、妥当か否かを判定する必要があるとも考えられる。利用者の観点から考えた場合には、公証センターに対して秘密の保持や事実の開示に対しては慎重であることを期待し、一方公証センターの公共性や信頼性を確保する観点からはある程度の開示に対する自主的判断が必要となる場合も想定される。この要件に対しては、公証センターの利用契約などにより充分に明確化されていることが望ましいものと考えられる。

(5) 利用技術に対する要件

公証センターが利用する技術に対しては、共通化も含めある程度の標準化が望まれる。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と考えられる。具体的には、データの安全性や参加者の本人確認に対して認証機関の発行する証明書を利用することも有効な方法であると考えられる。これは、認証機関の利用を前提としているとも解釈できるが、公証センター自身が証明書を発行しこれに代えることも考えられ、実質的には ISO/IEC9594-8|ITU-T X.509 で規定される証明書を利用することと捉えると、一つの共通技術を利用しているに過ぎない。技術を利用するが運用などについてはサービスの内容や参加者の要求によりいくつかの選択肢が存在するものと考えられる。

5.7 認証機関との連携

(1) 認証書の利用目的

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。公証局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自身の正しさを証明することを実現している。同時に、公証センターの利用者の本人認証などにも利用し、非対面取引きでの安全性確保を実現する。

(2) 公証センターと認証機関の関係

公証センターが利用者の本人確認や利用者に対する自身の正当性を証明するために証明書を利用しており、この認証書発行を行う機関が認証機関である。公証センターとの関係から分類し各々の場合の認証機関に求められる要件について以下にまとめる。

・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。

・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

認証機関と公証センターが同一の運営母体で運営される場合には、認証書の利用目的から考えると考慮する点があると考えられる。利用時においては公証対象データに

対する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。または、公証センターが自分自身の認証を行うため、公証センターの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場合が想定される。しかし利用者の観点からは、運営母体が同一の場合には信頼性についての確認が容易でない事が想定されるため、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が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、ある場合には、利用についてある程度の制約があるものと想定される。認証書の発行についての技術が多様になった場合には、公証センターも本人確認を行うために対応した技術を用意している事が求められる。したがって、公証センターは利用者を想定して可能な限りの技術を用意するが、すべてを網羅する事は容易でないものと考えられる。したがって、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明示する必要がある。一方、利用者の観点から考えると公証センターの選定などの容易さを考慮し、認証書の発行に関する技術の標準化などが望まれるものとなる。認証機関相互の運用性についての検討が行われており、これを活用し公証センターにおける相互運用性の実現を行う事も考えられる。

5.8 電子公証センターの責任の範囲

5.8.1 責任範囲の分類

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。以下どのようなケースが考えられるかをまとめる。（表 5-2 主な責任範囲の分類）

表 5-2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

5.8.2 電子公証センターの基本的責任

責任範囲は契約約款、利用約款で提示されると思われるが、私的機関としての電子公証センターの基本的責任について考察する。

(1) 前提

1、ある時刻に、ある取引文章が、存在したことを証明すること。

2、内容には関知しないこと。

3、紛争時に、顧客の要請にもとづき、証拠として提出すること。

4、証拠としての有効性を証明する努力をすること。

5、裁判、調停の場で証拠の有効性を保証する物ではないこと。

(2) 電子公証の責任範囲

個々の公証センターの特徴として、責任範囲がバラツク可能性が高いが、利用コストとの兼ね合いで、コストが安くなれば責任範囲は当然狭くなり、顧客はその中からコストとの兼ね合いで選択することになる。

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証拠が、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り、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。

将来的には、リスクの程度が読めるようになれば保険会社がビジネスとして行うことになるであろう。

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。

5.8.3 電子公証センターの機能分類毎の責任

公証センターの採用公証技術、運用管理、安全管理等の個別の機能に対する責任について考察してみる。

(1) 採用公証技術

暗号がハッカーに解読される、データがハッカーに破壊される等、採用している公証技術がハッカーに破られる場合の責任。

顧客は公証センターの技術を信用して利用しているため、これが信用できなくなれば公証センターの利用者がいなくなるのでビジネス上でも対策を取る必要がある。特に公証技術のソフトを販売している事業者は、即死活問題となる。

責任範囲として、ハッカー対策のとれたバージョンアップソフトへの交換、顧客への事故情報の開示と、対策方法の指示等を行う事が考えられる。此の問題は、内容により１事業者の問題になる場合と、公証技術全体への不信につながる場合がある。全体の問題になる場合は、業界としての対応が求められる。

(2) 運用管理面

例えば公証センターの職員がデータの改竄に関わるような事件とか、職員の操作ミスでデータが消滅してしまったため、顧客に損害が生じた場合の責任の問題。公証センターに道義的には責任はあるが、現実には損害補償に耐えるだけの資本、又はビジネス規模でなく、実質的に補償ができない可能性が高いと思われる。当然このような不祥事を起こしたセンターは淘汰される。

運用管理を強化しようすればそれに対応してコストもあがることになるが、公証技術が発達すれば、運用管理面をそれほど強化しなくても、不祥事がおきにくい体制に進む可能性も高いと思われる。

(3) 安全管理面

この問題も、同時に複数の顧客に損害が生じたとき、公証センターは損害補償に耐えられないであろう。

それ故、顧客は公証センターの安全対策を確認し、顧客のリスクで公証センターを選別することになるであろう。公証センターは自社の安全対策を顧客に積極的に開示し、事前に危険度を顧客に知らせることが望ましい。

5.9 電子公証センター実現上の課題

公証センターが社会インフラとして、利用者に安心と信頼を与えることが適い、その利用市場が拡大するためには、以下のような課題があるものと考えられる。

- 設立条件の検討
- 提供機能と運営母体の資格条件の検討
- 公共性の検討（公的機関サービスの範囲と民間機関の業務可能範囲）
- 国際間取引に対する有効性の検証と利用条件の検討

など。

5.9.1 電子公証センター事業者の必要性

(1) 役割

電子公証センターの役割は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であり、問題や紛争が生じた場合に、証拠力を高めるための手段として利用される。

これによりユーザが安心して電子商取引を行う一助となり、電子商取引の発展を促進する。

(2) ユーザの期待

直接顔が見えない電子商取引を行うものは、

１、相手が本当にそのものか

２、相手が信用できるか

３、相手が 一度決めた取引の条件、又は存在を途中で、都合により改竄、又は否定しないか

などの不安を持つ。そのために、

１の不安に対して認証局

２に対して信用調査機関

３の不安に対して公証センター

が存在する。

5.9.2 事業として成立する要件（商取引の公証事業）

(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。

当然規模が小さいと公証事業も成立しにくい。

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。

一件あたりの金額が小さい取引では、公証機能の利用コストを負担できない。紛争発生時に調停、裁定の場で公証の証拠を使って決着をつける可能性の高い相手との取引が多い系列会社間、子会社間、会員会社間での取引で、紛争が発生しても当事者間の話し合いで決着が付き、調停、裁定の場まで持ち込まむ可能性が低い場合、又取引停止、除名が恐くて、調停、裁定にまで持ち込む可能性が極端に低い場合は公証機能利用は少なくなる。

注文等の内容の違約による、取引リスクが大きい、又は決済方式が相手の与信を信用した方式である。

決済方式が、代引き、現金引き落とし等の商品との即時交換タイプでは、取引リスクが少なく公証機能の利用は少なくなる。

(2) 第三者が公証サービスを提供するメリットがある。

公証技術が発達し、技術により公証の証拠の有効性が保証され、第三者の運営する公証センターの存在が技術的に必ずしも必要性がない場合における、第三者の公証事業会社の存在意義としては、

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。

などが考えられる。

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

(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

7 まとめ

当WGではいわゆる「電子公証」を検討するに当たって、いくつかの基本的な視点を設定して議論してきた。

ひとつは、「電子公証」について必ずしも現行の公的な位置づけとしての公証人／公証役場などのシステム化を前提として議論するのではなく、むしろ出来うる限り当事者間における紛争解決を基本にして、ネットワーク（オープンネットワークを含む）におけるより安心な商取引環境の確保（安全性、信頼性の確保）する上でどのような電子公証システムが考えうるかにつき議論してきた。従って現在の商取引において安全性を実現しているしくみや法的な裏付けなどについて考察はしているものの、現在の商取引においてすらも実現できていない安全性、信頼性につき必要以上にいたずらに追及しているものではないことである。紛争処理に当たっては、基本的な事項は予め取引当事者間の契約なり運用規約なりに定めるべきで、その内容をもとに判断すべきであると考えられる。

もうひとつの視点は、「電子公証」を実際のビジネスプロセスの中における実ニーズとして捉えることである。現実のビジネスの流れに沿って、安心な電子商取引を実現するためには、法制度を担保にした厳密な「公証」に限定することなく、様々な機能の組み合わせによるサービスが望まれているからである。ここではいくつかのモデルを設定して議論を進めているが、実際の商取引においては実に多様な形態がありうることから、それら多様な取引ニーズに応じた多様なサービスが提供されるべきである。従ってそこに事業性を見いだす民間ベースの多種多様なサービス形態が可能となるはずであり、特に必要があれば公証人／公証役場の電子化も促進されるべきであると考える。

さらに「電子公証」のしくみを技術の側面からのみ捉えるのではなく、現行のしくみを技術に置き換えられる部分を明らかにするとともに、同時にそれを補完するルールや環境などについても同時に検討を試みた。ネットワーク上での商取引はビジネスチャンスの拡大として注目を浴びているが、その普及に関しては当事者に不安を与えない制度を構築する必要がある。このような制度を構築するにあたっては、技術的な対応によるものと取引ルールに関わるものに分けられる。電子公証の目的の一つがオープンなネットワーク上での取引相手の特定、取引内容の特定にあるとすれば、それを可能にする技術開発と社会的な認知が必要となる。

技術開発については民間企業によりすすめられており、現状においても十分活用が可能と考えられるが、社会的認知を得ているというにはまだ不十分であろう。参入を制限しない自由闊達な企業活力を取り込むことにより、技術は日々進化し、問題点を克服して行くが、社会的認知を得ることについては時間が必要となる。社会的認知を一気に高める方法として法律的な裏付けを与えることも考えられる。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。また、発展途上の市場に対してはその方向性をを探るにあたっての指針を示すよき指導者としての役割を期待したい。最終的な裁判での判断については自由心証主義を取る日本の法律を考えた場合､現行の法律の適用要件を緩やかにすることで対応は可能とも考えられる。

商取引を行う当事者にとって、その目的や効果は何ら変わっていないが、そのプロセスが電子的社会と現実社会とで異なっている。具体的には、電子商取引が

・特定が難しく改竄性の高いデータを当事者間を介在する不安定なネットワークを通すことが、商取引の基本プロセスであること。

・そのために、現実社会の商取引に近づけるよう技術的対策を講じた新たなプロセスが付加されること

であろう。端的には、前者が電子商取引特有の脅威の原因であり、後者が電子公証を含む安全な電子商取引を含む安全な電子商取引を実現するための条件である。現実社会の法制度しか存在しない中で、電子商取引を推進していくためには電子商取引の当事者が取引事例を積上げている過程であることを認識して、自己の責任で電子公証等の技術的解決プロセスを実際に導入していくことを必要とする。技術的に提供されたツールの法制度的有効性の実証とツールのベースとなる技術に対応した法制度の改定は同時並行的に進んでいくものと思われる。

安全および信頼性を確保した電子商取引の実現には、新しい商慣行や法制度の確立も必要であることに間違いはないものの、すべてが整うのを待つばかりではなく、商取引当事者の積極的な技術導入による試行錯誤も必要なのではないかと考える。事実この添付資料に紹介するように、北米などではすでに実験の域を越え、特定の市場向けに新しい技術を用いた新しいビジネスが次々と構築されている。これらすべての技術やしくみは必ずしも完全で公的にも認知されているものばかりではないが、確実にそこに取引当事者の現実のニーズと現在適用可能な最善の技術をもってビジネスがなりたっていることもまた事実である。もちろんこの背景には日本と欧米などとの歴史的、文化的な違い、公的機関や規制などに関する考え方の違いがあると考えられるものの、この変化の著しいグローバルなオープン・ネットワーク時代において大胆な試みもまた時には必要となるものと思われる。

「参考文献」

1）石黒 憲彦：電子取引　日本再生の条件
2）岸田 雅雄：企業取引法入門
3）倉田 卓次：遺言・公証
4）通商産業省：電子商取引環境整備研究会　　中間論点整理
　Ｈ９年１１月
5）内田　貴　：電子商取引と法　　ＮＢＬ
6）電子取引法制に関する研究会中間報告書（案）
　Ｈ９年3月２１日
7）帳簿書類の保存等の在り方について（案）
　Ｈ９年3月２６日
８）戒能　一成：通商産業省の電子申請・書類電子保存等の推進状況と今後の展開について
９）大山　永昭：電子保存と行政の電子化について
１０）国際大学グローバル・コミュニケーション・センター：電子公証システムの社会における役割と各国の動向に関する調査
１１）認証局運用ガイドライン（V1.0 版）　　平成１０年１月
　　ＥＣＯＭ　認証局検討ワーキンググループ