電子署名普及に向けた調査検討報告書

平成18年 3 月

次世代電子商取引推進協議会

序文

情報ネットワークを介した電子商取引の利用の拡大に伴い、信頼性・安全性確保は極めて重要な課題となっている。電子商取引の普及には電子署名（代理署名を含む）の利用により取引相手の信頼性保証（なりすまし及び改ざんの検知、否認防止）を行うことが必要であり、公開鍵基盤（PKI）による電子署名は、技術的にも利用環境としても利用可能な状況にある。国内では電子政府のサービス展開に伴って政府企業間（B2G）において利用され始め、また企業間（B2B）においても一部の業種で利用され始めているが、その展開のスピードは遅い。さらに、企業消費者間(B2C)や消費者間（C2C）では、多くのトラブルがすでに発生しているにもかかわらず、ほとんど利用されていない。

本調査研究では、旧電子商取引推進協議会で検討された、「署名文書の長期保存」、「属性認証」及び「リバティ、OASIS 等の規格に沿った実現方式の調査検討」等の成果を踏まえ、かつ、電子署名法の改正の検討が行われるのにあわせ、これまで議論されてきた三文判 PKI（利用の制限を設けた電子署名）等の電子署名の運用の多様化に関する検討を行なった。この検討のなかから、電子署名普及のための課題を抽出した。

本報告書が、電子署名の利用を検討している企業、機関の方々にとって一助になることができれば幸いである。

平成 18 年 3 月

次世代電子商取引推進協議会

目　次

まえがき

e-Japan 計画では、すべての国民が情報通信技術を活用し、その恩恵を最大限に享受できる社会の実現に向けて、市場原理に基づき民間が最大限に活力を発揮できる環境を整備し、2001 年 1 月にスタートし、5 年以内に世界最先端の IT 国家となることを目指して、今年度はその 5 年目にあたる。

この間、2001 年 4 月に電子署名法が施行され、公開鍵暗号基盤（PKI）によるデジタル署名が法的な意味合いを持つことになり、現在 2006 年度の改定に向けた検討が行われている。

また、2005 年 4 月 1 日から「e-文書法」という新しい法律が施行された。この e-文書法とは「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（通則法）及び「民間事業者等が行う書面の保存等における情報通信技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」（整備法）という 2 つの法律をまとめた呼称のことである。各書類の保存方法等は、所管の各省庁から省令の形で指示される。

この法律は、民間においてこれまで法律によって紙による保存が義務づけられていた書類を、電子化したデジタルデータによって保存することを認めるものである。

このように、デジタル署名の利用は、政策的にも制度的にも利用を拡大する方向にあり、また、技術的にも利用環境としても利用可能な状況にある。

しかしながら、電子政府のサービス展開に伴って G2B において利用され始め、また B2B においても一部の業種で利用され始めているが、その展開のスピードは遅い。さらに、B2C や C2C では、多くのトラブルがすでに発生しているにもかかわらず、ほとんど利用されていない。

本調査研究では、電子署名法の改正の検討が行われるのにあわせ、これまで議論されてきた三文判 PKI（厳密な運営を求めない電子署名）等のデジタル署名の運用の多様化に関する検討や、各業界の電子商取引で採用すべきデジタル署名のポリシーやデジタル署名を利用すべきケースの分析など、デジタル署名の利用のためのガイドラインの作成とデジタル署名の利用の拡大と定着のための提言をまとめる。

すなわち、電子契約などデジタル署名の利用の定着に焦点を絞り、社会が受け入れるための、社会的ニーズ、導入上の障害、実現のための技術的な成熟度、など多面的な視点からの調査分析、ガイドラインの作成、評価を 3 年計画で進める。

本年度は、初年度に当たりデジタル署名が利用されるべき分野、そのために検討すべき項目の洗い出しを行い本報告書にまとめた。

各章の概要は以下のとおりである。

第 1 章では、公開鍵暗号基盤の構築を進め始めた 2000 年から 2004 年ごろに、識者が描いてい

たデジタル署名の利用分野を紹介するとともに、現状のデジタル署名の利用状況について国内の代表的な利用事例と動向を示して解説する。

第2章では、デジタル署名の普及を妨げていると思われる問題を有識者の意見などが記載されている報告書などからピックアップし、さらにワーキングメンバーからの意見も加えて分類した。次に分類ごとにその意見の本質を理解して、価格あるいは利用環境などPKIのインフラに関わるもの、法的な制約によるもの、あるいはガイドラインや啓発に関するものなどその対策方法を分析し、問題点の抽出を行った。

第3章では、ECOMのADR（裁判外紛争解決）WGがまとめた2003年度、2004年度のECのトラブル事例をセキュリティ確保の観点から分析し、デジタル署名を利用することによってトラブル回避できる利用分野、利用場面を整理した。

第4章では、2章と3章の検討内容を踏まえ、今後デジタル署名を普及すべき分野と普及のために必要な具体的対策を導くため、問題点を絞り込み、重点課題を設定した。

今後、この報告書に基づき、ユーザ企業を中心とした体制を作り、課題の検討を進めていく予定である。

1．電子署名の利用状況

1.1　電子署名とは

電子署名とは、デジタル文書の正当性を保証するために付けられる署名情報のことである。文字や記号、マークなどを電子的に表現して署名行為を行なうこと全般を指す。現実の世界で行なわれる署名を電子的手段で代替したものといえる。特に、公開鍵暗号方式を応用して、文書の作成者を証明し、かつその文書が改ざんされていないことを保証する署名方式のことを「デジタル署名」という。電子署名に法的効力を認めるかどうか、また、どの方式を電子署名として認めるかといった事項は、国によって異なる。アメリカなどでは州によっても異なる場合がある。

「電磁的記録に記録できる情報について行われる措置」であって次の２つの要件に「いずれも該当するもの」。①当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。（本人性の確認）②当該情報について改変が行われていないかどうかを確認することができるものであること。（非改ざん性の確認）［電子署名法］

本 WG では以後、上記の「デジタル署名」のことを電子署名のこととして、以後検討する。

1.2　電子署名の利用形態と期待分野

電子署名が当初期待されていた分野を次に示す。

(1) 電子メール

メールクライアントソフトウェアで電子署名の機能を使用することにより送信文書の完全性（改ざんされていないこと）を保つものである。

①S/MIME を利用した電子メール

S/MIME とは Secure Multipurpose Internet Mail Extensions のことで、MIME の機能を拡張したもの。電子メールの暗号化と電子署名に関する国際規格となっている。

RSA 公開鍵暗号方式を用いてメッセージを暗号化および署名して電子メールを送受信する。RSA Data Security 社によって提案され、IETF によって標準化された。この方式で暗号化メールをやり取りするには、受信者側も S/MIME に対応している必要がある。

(2) オンラインクレジットカード決済

①SET（Secure Electronic Transactions）

インターネット上で、クレジットカード決済を安全に行うための規格。利用するのには購入者側のパソコンと店舗のサーバに専用ソフトウェアを搭載しておく必要がある。購入者がインターネットでクレジットカードで買い物をする際の情報は PKI により暗号化およびデジタル署名が付与され、購入者のパソコン、店舗サーバ、クレジットカード会社間でやりとりされる。購入者が送るクレジットカード情報については、クレジットカード会社の公開鍵で暗号化を行うため、店舗はカード番号等を知ることはできない。［SECAD］

(3) 電子入札・申請

省庁や自治体の入札案件や各種申請を、インターネットを利用して行うものである。民間企業などが所定の機関から発行された電子証明書を用いて、入札データや申請データに署名を施し、電子入札・申請を行うものである。

(4) 電子契約

電子的な文書で契約情報を残すような場合に、従来の紙への署名／押印に代わり電子署名を電子文書ファイルに付けて契約を行うものである。

「書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律」（通称 IT 書面一括法）の施行により、企業間での契約への展開が期待されていた。

(5) インターネットコンテンツへの署名

(a) プログラムコードへの電子署名

ソフトウェア開発者や Web 構築者が提供するプログラムコードに対して行う電子署名で、ActiveX コントロール、Java アプレット、HTML コンテンツなどに付与することができる。この署名により、プログラムコードをダウンロードしたエンドユーザは、開発元やそのプログラムコードが署名された時点から変更されていないことを確認できる。

(b) XML 署名

XML 文書に電子署名を付与するもので、文書作成者の身元を証明し、またその文書が改ざんされていないことを保証するものである。

XML 文書はテキスト形式であり、バイナリデータに比べ改ざんや模倣が容易にできてしまうリスクがある。このため、公開鍵暗号技術を用いた XML 署名により、電子商取引などの安全性を高めている。

(c) PDF 署名

PDF 文書に電子署名を付与し、作成者の証明と改ざん防止を図るものである。PDF 文書作成時に電子署名機能を使うことで、電子署名付 PDF 文書とすることができる。

1.3　電子署名が利用されている分野

(1) 商取引の文書（見積書、契約書、検収完了書）における電子署名活用

リース取引の見積書から契約書、検収完了書までを自動的に作成するもので、契約書の署名についても電子署名を利用することで処理を完全ペーパーレスにした。

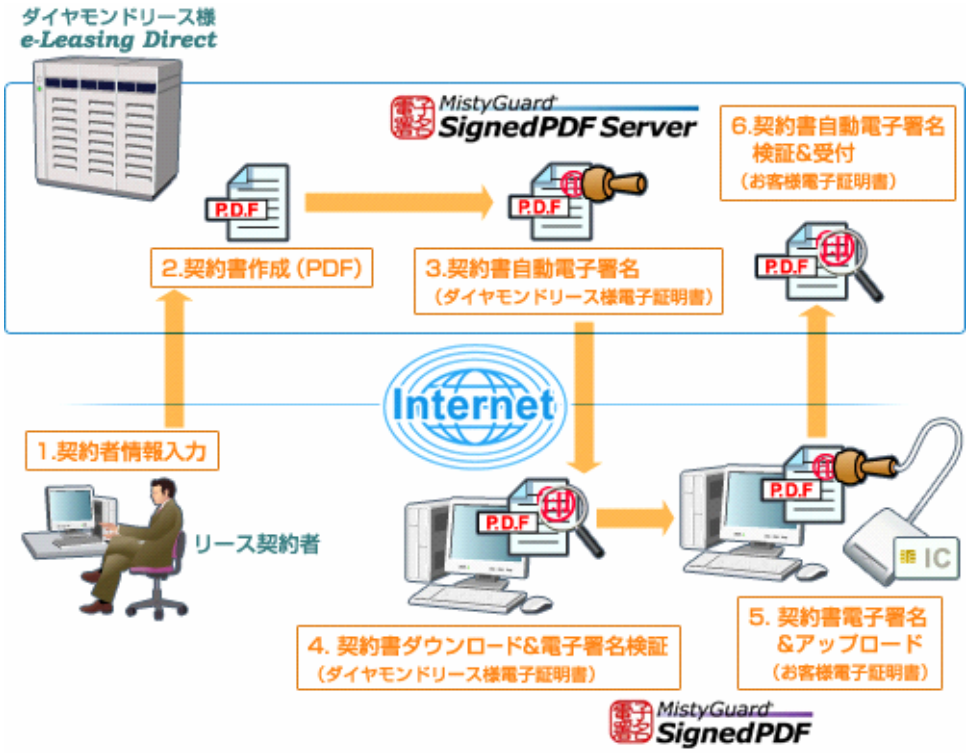

図 1-1 電子リース取引（三菱電機㈱提供）

(2) 給与明細における電子署名活用

インターネットを通して給与明細を確認する際に、給与明細書電子ファイルに電子署名を付与することで改ざんされていない保証をするシステムである。

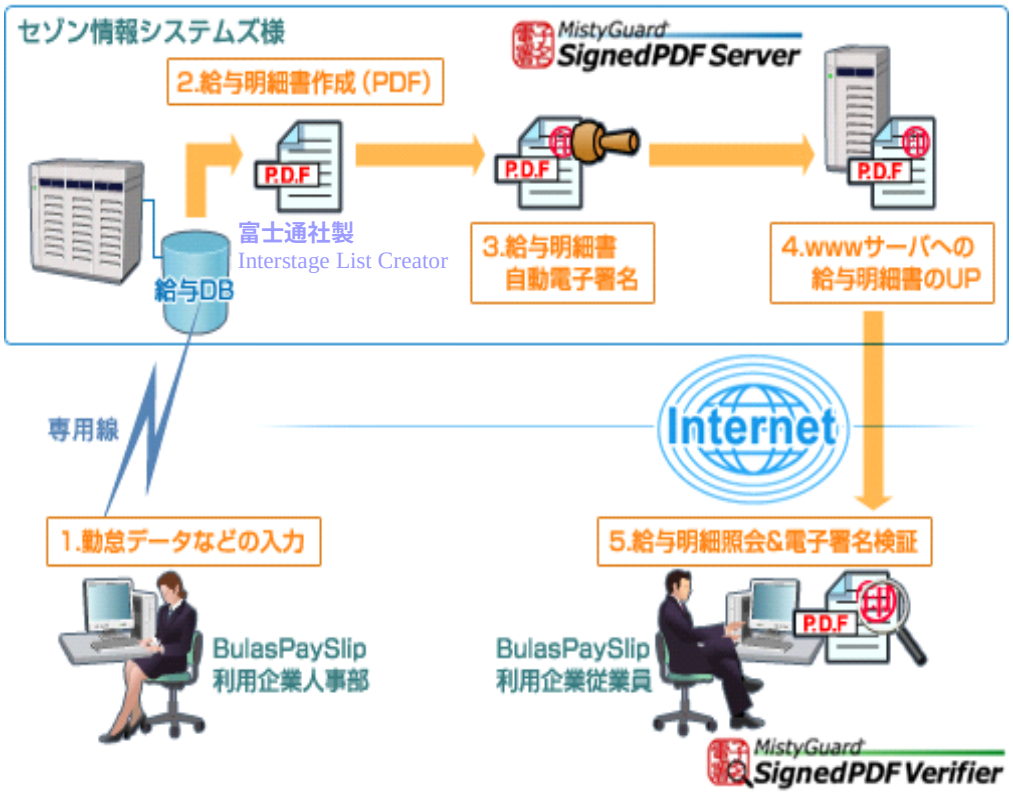

図 1-2 給与明細システム（三菱電機㈱提供）

(3) 契約における電子署名活用

前述の IT 書面一括法の施行後、建設業界では国土交通省が電子的手段により請負契約を締結しようとする際の参考として、建設業法施行規則に規定する「技術的基準」にかかわるガイドラインを素早く定めた。このガイドラインでは特定認証局の電子証明書を利用する事が推奨されており、契約コスト削減というメリットもあって、電子署名活用を後押しする形となった。

実際に、図 1-3 のような電子契約システムが構築、運用されている。

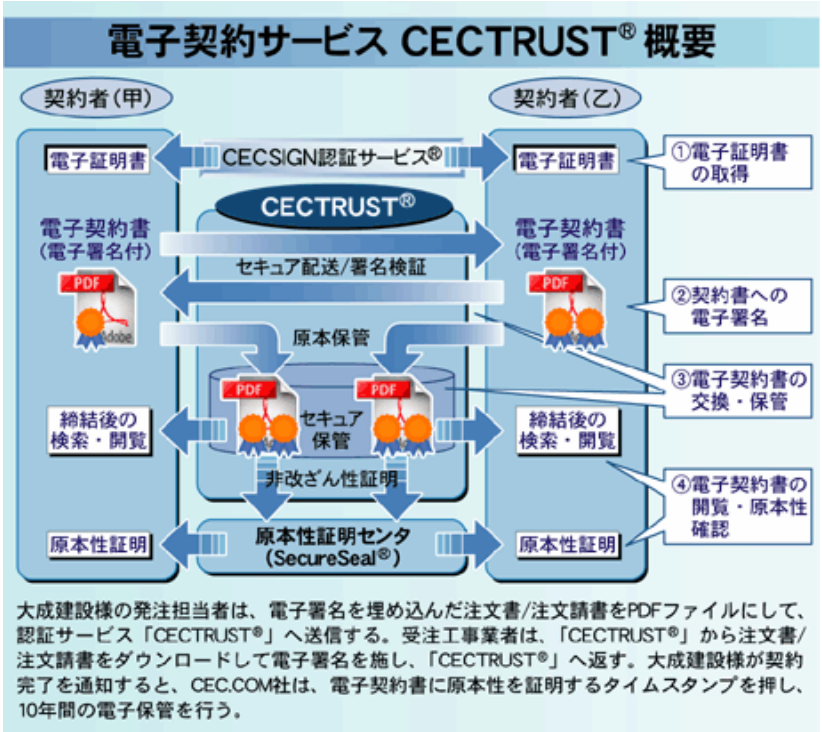

図 1-3 電子契約システム（大成建設㈱：㈱NTT データ提供）

現在では、建設業界だけでなく製造、鉄道、ガス、通信、情報通信などあらゆる業界で電子署名を活用した電子契約が広がりはじめている。

(4) 発注・請求業務における電子署名活用

日用品化粧品業界では、業界メーカー311 社と業界卸売業 463 社との間で、発注データ、請求データなどのデータの交換（EDI）を行っている。従来はダイアルアップにより専用ネットワークへ接続し、運用会社の基幹サーバへアクセスする方式をとっていたが、2005 年 8 月よりインターネットを活用した新しいシステムを構築し、運用をはじめている。この方式では、ユーザ（メーカー、卸売業者）は EDI データを作成後、デジタル署名を付与、メッセージを暗号化して、インターネットを経由して運用会社の基幹サーバへとデータを送信する。なお、証明書は運用会社が設立した認証局が発行するプライベート証明書であり、それ以外（パブリック証明書）などは認めていない。[PLANET]

(5) 医療機関における電子署名活用

(a) 電子カルテおよびアクセス記録に対する署名

複数の医療機関及び患者を含めて情報ネットワークを活用する地域医療連携が各地で取り組まれている。この中で、電子カルテやデータへのアクセスに対して電子署名が利用されるケースがでてきている。

地域医療情報連携プロジェクトの１つである PLANET（亀田総合病院を中心とする南房総地域ネットワーク）では、医師がカルテを作成する際に、IC カードに入った電子証明書から電子署名を付与できる情報システムが構築されている。また、患者がインターネットにより自分の情報にアクセスする際に、同じく IC カードの電子証明書を活用して、認証、アクセス権の判別と同時にアクセス記録に署名付けて保存することにより、記録の真正性を確保している。[KAMEDA]

(b) 患者紹介システム

日本医師会が実証実験を行ったシステムで、加盟医師間で、電子署名を使って、患者を紹介しあうものである。

医師は患者を他の医師に診てもらったほうがいい場合などに、パソコンで署名入り紹介状と簡易カルテを書き込み、別の医師に送付を行う。相手の医師は専用ソフトを使い、紹介状を書いた医師名や所属医療機関を照合・確認する仕組みである。

(6) 電子文書の長期保存への取組み

次世代電子商取引協議会（ECOM）では、平成 12 年度より電子文書の長期保存について検討を進めている。

平成 12 年度　電子署名文書の長期保存に関する要件整理
平成 14 年度　タイムスタンプサービスの実態調査および利用ガイドライン、運用ガイドラインの作成
平成 15 年度　電子署名文書の長期保存に関する実用化動向の調査および署名ポリシーの整理
平成 16 年度　電子文書の長期保存と見読性に関するガイドラインの作成

また、平成 17 年度は長期署名フォーマットの相互運用性試験プロジェクトを企画し、「長期署名フォーマットのプロファイル」を策定し、このプロファイルに基づいたテスト仕様を作成し、実験参加 13 社と実験協力 2 社により参加各社の製品（一部プロトタイプを含む）の相互運用性テストを実施している。

1.4　参考資料、URL

［SECAD］情報セキュリティアドミニストレータ基本テキスト第２版（TAC 出版）
［PLANET］株式会社プラネット　http://www.planet-van.co.jp/index.html
［KAMEDA］南房総地域ネットワーク　http://info.planet.kameda.jp/

2．電子署名の普及における問題点

2.1　現状認識と問題分析へのアプローチ

ビジネスユース、カスタマーユースを問わず、情報セキュリティの必要性と注目度は日に日に増している。企業において、情報セキュリティを実現・維持する専門の役割である『情報セキュリティアドミニストレータ』の受験者が毎年増加傾向にあることや、個人情報保護法、e-文書法など、セキュリティに係る法令が近年次々と施行されていることも、その裏づけといえよう。

情報セキュリティは様々な方法・手段により実現・維持されるものであるが、データや文書の真正性を保証するにはPKI技術を利用した『電子署名』に代わる有力な技術はない。しかしながら、その利用はe-Japan戦略を始めとする行政系主導の施策により導入を進められた官公庁中心の電子申請、電子入札、そして電子納税など一部にとどまっている。民間分野においては、SSLの普及によりサーバ認証などでは使われ始めているものの、電子署名の用途では少数の利用例にとどまっている状況である。

実際、一般ユーザにとっては、電子署名というもの自体なじみの薄いものであり、システム提供者・技術者にとっては、知ってはいてもPKI技術は面倒で処理が重いという印象が強いようである。また技術的にも、PKIは万全ではなく使い方によってリスクを含んでいるとの指摘(*1,*2)もある。

これらの問題点が、普及にあたって本当に問題なのか、あるいは何がより根源的な問題なのかを探り、普及を阻害する原因を取り除く対策を考える必要がある。

以下では、ビジネスユース、カスタマーユースそれぞれに登場する『利用者』『サービス提供者』それぞれの視点から、経済面、技術面、及び、心理面などを考慮して問題点をカテゴライズして抽出し、さらに、それぞれの具体的な阻害要因を掘り下げていく。

*1) 情報処理　コラム「電子認証いまむかし」46巻7号（2005.7)、46巻8号（2005.8）
*2) Carl Ellison and Bruce Schneier, "10 Risks of PKI", Computer Security Journal, v16, n1, 2000, pp.1-7（URL: http://www.counterpane.com/pki-risks.html）

2.2　問題点の抽出

電子署名あるいはPKIを導入しない理由として利用者やサービス提供者などが、それぞれの立場でいろいろな問題点を挙げることが多い。一般によく言われる問題点を、需要、適用可能範囲、法令・施策、標準化・相互運用性、安全性・信頼性、導入容易性、操作性・運用性、保守性に分類して表 2-1 に列挙した。備考には、それを問題と感じる人を、利用者（利）／提供者（提）／開発者（開）に分類して記載した。

表 2-1 電子署名普及の問題点と考えられているもの

	分類	問題点	備考
1	需要	①署名者がメリットを感じるサービス／ユースケースが少ない	①利/提
		②メリット（使うと何が良くなるのか）が分からない／逆に匿名性が損なわれる	②利
		③その場で効果を実感しにくい（事後のトラブルで効果を発揮）	③利
		④必要性（困窮感）がない／代替手段がある	④利/提
		⑤法令による電子署名の使用義務はない	⑤利/提
		⑥投資対効果（ROSI）が見えにくい	⑥提
		⑦PKI があまり理解されていない／署名が常識とはなってない	⑦提
		⑧電子認証局がビジネスとして成立しにくい／受益者負担になっていない	⑧提/利
2	適用可能範囲	①汎用性が高いアプリケーションが少ない。	①利/提
		②汎用性が高い ID（識別子）を持つ証明書が無い	②利/提
		③認証ドメインの相互運用を実現するのが容易でない	③提/開
		④使用可能な処理系が Windows 系に偏っている	④利/開
3	法令、施策	①電子署名法は、自然人の署名に限定されている	①提
		②電子署名法に基づく特定認証認定の認証局は高コスト	②提
		③気軽に使える安価な三文判的な証明書がない	③利
		④公的個人認証サービスは利用に制約がある	④提
		⑤e-文書法などの効果はまだ限定的である	⑤提
4	標準化、相互運用性	①暗号アルゴリズムや署名データ形式が複数存在して相互運用性に難がある／アルゴリズム危殆化のリスクもある	①開/利
		②電子文書長期保存の標準的プロファイルがなく長期的相互運用が困難	②開/提
		③PKI の SDK／ツールキットの API が、ベンダー依存	③開
		④利用者の秘密鍵の格納媒体として確立したものがない（IC カード（カードリーダやドライバ）は標準化が不十分）	④利
		⑤PKI 利用の（システム化や導入の）ガイドラインがない（業界単位のセキュリティポリシーを実施徹底するために必要。）	⑤提
5	安全性、信頼性	①証明書（認証局）の信頼性の判断基準がない（格付けがない）	①利
		②証明書の失効管理や検証は面倒で、適切に実施されないケースもある	②提/開
		③利用者の義務事項や注意すべき事項が、認識されていない（難しい）	③利
		④秘密鍵には漏洩・危殆化のリスクがある（AP や端末環境の変造による漏洩のリスクもある）	④利/開

6	導入容易性	①PKI 導入コストが高い（証明書取得、PKI アプリケーション開発、認証局構築などのコスト） ②独自認証局の構築は技術的、コスト的に難しい ③PKI アプリケーション開発は技術面及びコスト面で容易でない（失効管理及び失効確認の負担が少なくない） ④既存の情報システムやソフトパッケージへ組み込むことが困難／署名を付与した電子文書をライフサイクル管理する仕組みがまだない ⑤公開鍵証明書の入手が難しい（どの認証局から取得すべきかが不明） ⑥PKI 利用者になるには技術面（知識）、コスト面（証明書取得、IC カードとカードリーダなど）で障壁が高い	①利/提 ②提 ③開 ④開/提 ⑤利 ⑥利
7	操作性、運用性	①認証局の構築・運用は容易でない ②秘密鍵の管理は面倒／署名の都度、秘密鍵を使用するための PIN（暗証番号）を入力するのは煩わしい ③証明書の有効期限や失効を意識する必要があることが煩わしい／有効期限が切れないうちに更新する必要がある	①提 ②利 ③利/開
8	保守性	①アルゴリズム危殆化による再署名やシステム変更の影響は大きい ②PKI アプリケーションが SDK に依存し、ベンダー独立にはなっていないため保守ベンダも限定される ③暗号アルゴリズムや IC カードなどを変更する場合、改造など手間がかかる／利用者環境も変更が必要になる	①提/開 ②開 ③開/利

2.3 問題点の解説

前節で挙げた問題点の中には、本質的なものや複雑な背景を持つものもあれば、実際にはさほど問題でないものや、誤解・誤認識に基づくものもありうる。各分類において、説明を要するものを中心に、以下に詳述する。

2.3.1 需要

インターネットが普及した現在、安全、安心なネットワーク社会を実現する仕組みの必要性は高まっているはずである。実際、スパムメールやネット取引のトラブルなど問題が発生し始めているが、これまでの IT 基盤は、安全・安心を提供する十分なセキュリティの基盤が実現されていない。それらの問題を解決する一つの手段が電子署名であり、その需要がどのような状況にあるか考察する。

電子署名に対する需要として、利用者やシステム提供者が電子署名を利用／導入するモチベーション（動機）が大きいかどうかが重要である。動機には、積極的なものと、消極的なものがある。積極的な動機とは、それを用いることで大きなメリットやインセンティブがあるため自発的に利用しようとすることである。消極的な動機とは、やらないと問題が生じるため、あるいは義務付けられているためやむを得ず導入するものといえる。

(1) 利用者側の需要

利用者が需要を感じるのは、「大きなメリットがある」あるいは「ないと困る」といった場合と想定される。しかし、電子署名（あるいは PKI）によってメリットが出る「サービスが少ない」、署名がないと「困るシーンがない」のが現状といえる。

前者については、効果的なアプリケーションが少ないことの他、署名のメリットはその場で実感しにくい（事後のトラブル時に効果を発揮する（図 2-1））、電子署名の効果（あるいは存在自体）がそもそも知られていないという事情もあるであろう（理想としては、署名や PKI の仕組みを知らなくても使える状況になるのが望ましいが）。逆に、署名は、自分の責任を明確にするものであり、一般的に匿名性を特徴とするインターネットサービス等においては、心理的に逆効果になりうる場合もあると考えられる。

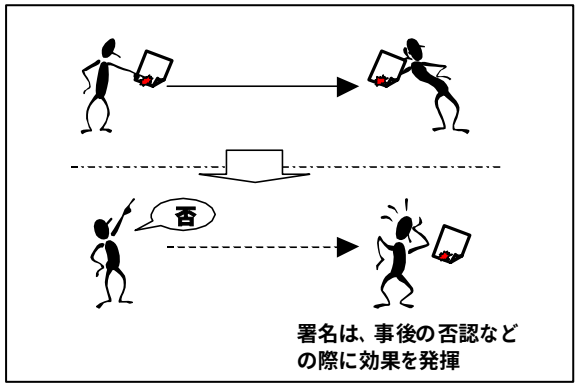

図 2-1 電子署名の効果

後者については、法令等による電子署名の使用義務がないこと、代りの手段で十分と思われていることが理由と考えられる。PKI の代替手段は、「認証（Authentication）」用途としては確かにパスワードや生体認証などが種々存在し、要求レベルに応じて使い分けることは可能であるが、「署名」用途については有力な代替手段はなく、電子署名が現状最も効果的な方法と

言える。しかし、両者に共通の基盤である PKI 証明書のインフラが未整備であること、PKI 自体の理解が不十分で用途の違いが認識されていないことも、普及を阻んでいる原因であろう。

また、ビジネスとして発展するためには受益者負担の構造になっているべきであるが、現状では、証明書取得費用は利用者が負担することが多い。署名等により不正な情報を受け取るリスクを回避できるサービス提供者が本来の受益者であるが、情報送信側（例えば電子申請サービスにおける申請者）である利用者が自己負担で証明書を取得しなければならないとすると、受益者としての実感がなく取得の意欲につながらないと思われる。証明書取得が参加条件であるクローズなシステムの場合は利用者としても取得の必要性を感じるが、オープンで証明書が必須でないシステムにおいては、提供者側が受益者として費用負担するビジネスモデルも必要であろう。例えばETC（Electronic Toll Collection System）のように、経費を補助するなどの施策が有効かもしれない。

(2) 提供者側の需要

次に提供者の視点で考えると、システムや情報を脅威から守るために必要なもの、あるいは利用者増など収益につながるものであれば導入する動機になるといえる。

脅威への対策として有効な技術であるが導入が進んでいないのは、電子署名の効果や技術そのものがあまり知られていないことに加え、将来の被害を未然に防ぐ技術であるがため、投資対効果（ROI:return on investment 投資収益率、ROSI:return on security investment セキュリティの投資収益率）を評価することが難しく、導入に踏み切れないことが考えられる。

利用者増については、まだ潜在ニーズの掘起しが不十分で、有用かつ確立されたユースケースモデルが少ないこともあり、使いたいと思う有用なアプリケーションが少ないのも確かである。従って、署名を付与することがメリットになるサービスの創出や、署名付与が常識という文化の醸成が必要と考えられる。とはいえ、実際に迷惑メール対策や企業内不正防止等、必要性は高まっており、業種では医師や会計士、建築士、マスコミなど社会的責任を負う人の署名は有用性が高いはずである。

サービスの提供には、アプリケーションの開発とともに基盤（インフラ）が必要で、PKI においては電子認証局がそれにあたる。基盤の整備・普及のためには、公共の認証局は別としても、民間の運営であれば認証局自体もビジネスとして成立することが必要である。現状では、PKI のニーズは限られていて認証局ビジネスが成立しにくいため、一般ユーザが利用しやすく、またそれなりに信用度のある認証局（証明書はフリーソフトでも作成できるが、それが信用力を持つかどうかは別である）は多くない。これがまた、PKI を一般ユーザから遠ざける原因にもなっている。

2.3.2 適用可能範囲

電子署名の基盤である PKI が広く使われるためには、PKI 利用者を表す識別子（ID）が広く通用することと、広く普及したアプリケーションにおいて扱えることが重要と考えられる。以下、識別子と PKI アプリケーションの適用範囲に関する問題が普及を妨げている状況について述べる。

(1) 識別子とドメイン

PKI 技術は公開鍵と秘密鍵の対のうち、秘密鍵を保有者が厳重に保管し、公開鍵は広く公開し他人に使われることで、暗号化や認証、電子署名としての利用が可能となる。その際、公開鍵が確かに保有者（正確には対となる秘密鍵の保有者）のものであることが保証されていることが前提である。そのために、認証局が保有者（の識別子）と公開鍵の関係を証明する証明書を発行している（図 2-2)。

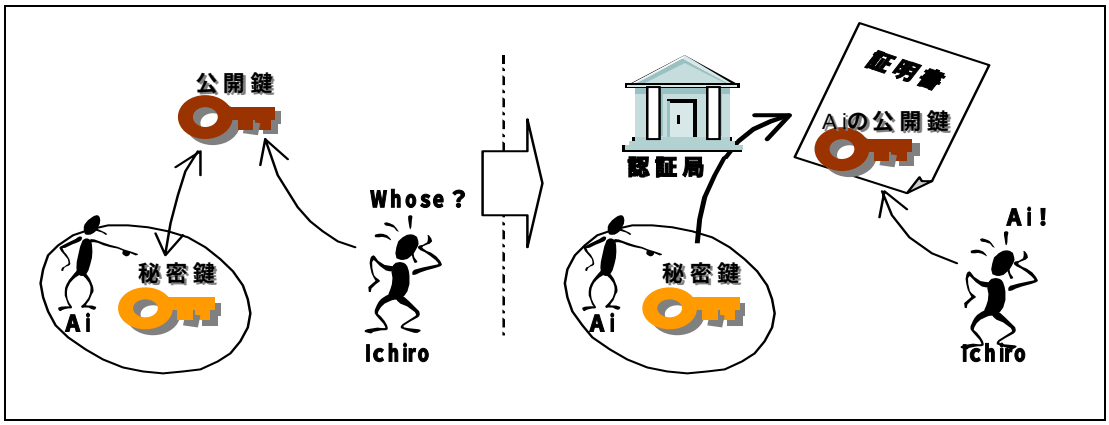

図 2-2 認証局と証明書の役割

ここで、世界中の保有者と鍵の対応を保証する認証局があれば理想であるが、現実にはローカルな認証局が多数存在し、その管理下の保有者（すなわちローカルなドメインの識別子）に対して保証する構造となっている。各認証局配下の利用者間では互いに信頼することが可能であるが、ドメインをまたぐ信頼関係を構築できないと、PKI の適用範囲（利用範囲）は広がらない。

適用範囲を広げるには、できるだけ汎用的な識別子を持つ証明書を発行する方法と、ローカルなドメイン間を連携させる方法がある。汎用的な識別子の証明書を多くの利用者に発行するということは、多くの人を管理し保証することにほかならず、そのような認証局を運営できる組織は多くない。多くの場合は企業内の利用者や、特定のサービスの利用者を管理・識別するのみである。そのため、公共的な認証基盤（インフラ）が期待され、公的個人認証サービスなどの普及が待たれる。一方、ドメインを連携させる方法には、相互認証や階層認証などの信頼モデル（信用モデルともいう）の技術（参考 1）がある。しかし相互に認証するには、保証レベルや運用方法を表すポリシー（CP/CPS）を互いに容認できることが必要であり、簡単に連携できるわけではない。

参考１：信頼モデル（信用モデル） http://www.ipa.go.jp/security/pki/051.html

・単独CAモデル

1つのCAが全てのユーザに証明書を発行する方式。

構成がシンプルであるので証明書の検証が容易であるが、複数の証明書ポリシーを持つ場合、管理が煩雑となる。

・相互認証モデル

2つのCAを互いに接続する方式。

互いに信頼し合う双方向信頼と一方が片方しか信頼しない片方向信頼の選択が可能。複数のドメインを接続する場合は、ブリッジ CA モデル、メッシュモデルの中で利用される。相手のX.509v3証明書拡張の対応のための実装が要求される。

・階層型モデル

階層型モデルにおける複数のCAを階層型（ツリー構造）に構成する方式。

認証パスは、上位の CA に向かって順にたどることで構築できるため、クライアントでの処理が容易。証明書利用者は、ルート CA の証明書を信用点として保持しておくことで、ルート CA を基点とするすべての CA から発行された証明書を検証できる。しかし、階層型モデルにおいては、上位のCAのポリシーが下位のCAに継承されていくため、異なるポリシーの組織同士を接続することが難しくなっている。万一、ルート CA の信用が失われると、配下の全ての下位CAの信用も失われてしまう。

・Webモデル（Webブラウザで利用）

あらかじめクライアントのアプリケーションにルートCAの一覧を埋め込む方式。

便利な反面、事前に登録されているルート CA が本当に信頼できるか否かを、証明書利用者が確認できない問題点がある。

・メッシュモデル

複数のCAを相互認証により接続する方式。

異なる CA ドメインを柔軟に接続することができるが、認証構造が複雑になるため、認証パスの構築にコストがかかってしまう。

・ブリッジCAモデル

複数のCAがブリッジCAを介して接続する方式。

米、カナダ、日本の政府認証基盤でも採用されている信用モデル。

署名のチェーンの検証だけでなく、各種の制約拡張の解釈が重要になり、多くのX.509v3証明書拡張の対応のための実装が要求される。また、実装例が少ないため、高度な相互運用が要求される。

(2) アプリケーションの適用範囲

上記のようなローカルな識別子であっても例えば企業内システムにPKIを適用することは可能である。しかし、ローカルなシステムではPKIでなくても十分な場合が多く、導入の動機にはなりにくかった。例えば、システム内のサーバでアクセス権を一括管理したり、作成文書を

データベースで厳重に管理しておけば十分な場合が多い。PKI の普及のためには汎用的なアプリケーションで利用できること、それもあまり意識せず使えることが重要であろう。実際、通信のレイヤでは SSL のサーバ認証に使われることが多くなっている。さらに、クライアント認証や署名付きメールの普及、新たなアプリケーションの出現が待たれる。

2.3.3 法令・施策

政府は日本の社会の IT 化を推進するため、2001 年から 5 年間の e-Japan 戦略を策定し、IT 化の鍵である PKI 基盤を整備するなど、数々の施策、法令を打ち出してきた。

・電子署名法（2001 年施行）
・GPKI/LGPKI の構築（2001 年～2005 年）
・公的個人認証サービス（2004 年サービス開始）
・e-文書法（2005 年施行）
等

しかし、その利用条件の制約などにより、普及に十分な効果があがっていないものもある。以下、それらについて考察する。

(1) 電子署名法について

2001 年 4 月に電子署名法が施行され、この法によって適正に行われた電子署名は、手書き署名や押印がなされた文書と同様に文書が真正に成立したとの推定効が与えられるようになった。また、この法律の施行に伴い民間に証明書を発行する特定認証業務制度が導入された。しかしここで、普及にあたって 2 つの問題が存在すると言われている。1 点目は、署名法は従来の署名に代わるのもとして制度化されたため、自然人による署名行為を想定しているものの、ビジネスシーンでの活用があまり考慮されていないこと、2 点目は、特定認証業務の運用基準が複雑・厳格であり、運用コストがかかることである。

1 点目については、証明書の利用目的が個人的なものであれば問題はない。しかし、現時点での証明書の利用シーンとしては「企業に属している個人」「組織に属している個人」としてビジネスで利用する場面が多いため、制度面と利用面のギャップを引き起こしてしまっている。ビジネスで利用するのに、取得手続きは個人で行わなければならない状況にある。

2 つ目については、認定取得しようとする事業者の負担が大きく、参入の障壁となることと、取得したとしても運用コストが高く、証明書価格に転嫁すると利用者にとっても負担となることである。これは転じて証明書の普及を阻み、認証事業者のビジネスを困難なものにしている。実際、認定を取得するとなると、設備、運用の認定基準を満たさなくてはならないため、証明書を発行する本人身元確認と、証明書と鍵を本人に結びつける作業に関して非常に高いハードルを課している（参考 2）だけでなく、証明書の利用目的が単一的になりがちで汎用性に乏しくなるという弊害も起こる。

参考２：特定認証業務認定取得のステップ

http://www.mitsubishielectric.co.jp/security/info/solution/solution01/pdf/pki200307.pdf

１．認証局運用規程（CPS）の作成

認証局の運用に関する基本規程。これらの規程が基準の要求事項を満たすように作成する。

２．認証局業務の管理策

電子認証局の運営では、電子認証局の署名鍵の生成、保管、廃棄、及び証明書のライフサイクルに厳格な管理を行う必要があるため、鍵管理のセキュリティ対策や手順を定める。

(1) 事務取扱要領

証明書関連業務手順書

認証システム運用管理手順書

(2) セキュリティ規程

文書・媒体等アクセス制御規程

設備室セキュリティ規程

ネットワークセキュリティ規程

(3) 業務管理規程

教育・訓練計画、

災害復旧計画

監査規程

３．認証システム仕様書作成

(1) システム仕様書

(2) 試験要領書

(3) システム操作手順書

このような信頼性の高い証明書も必要と思われるが、よりビジネスにマッチした証明書にも市場があると考えられ、それに対する規定や判定基準がないのも問題である。公的な認証局や特定認証業務の認定認証局以外に、民間運営の認証局や無料の認証局もあるが、それらに対する信用レベルの基準が無く、利用者が目的に応じた選択ができない状況である。よって民間レベルで普及するには、実社会での実印相当ばかりでなく、認印として利用されている三文判的な用途への展開を可能とする規定やガイドライン、格付け制度の制定などが必要であろう。

(2) GPKI、LGPKI と民間 PKI の関わりについて

行政分野では政府認証基盤（GPKI）、地方公共団体組織認証基盤（LGPKI）が電子署名基盤として整備・構築された。GPKI は、国の行政機関に電子申請・届出等を行うとき利用され、ブリッジ認証局が府省認証局、商業登記認証局、民間認証局と相互認証することによって、他の認証局から認証されている者同士のデータ通信を可能としている。また、LGPKI は、住民・企業が地方公共団体に電子申請・届出等を行うとき、あるいは地方公共団体間で文書のやり取りを電子的に行うときに、利用されており、GPKI と LGPKI は、相互認証をおこなっている。このよ

うに、政府、地方公共団体では、PKI を用いた文書のやり取りが推進されているが、民間との間では相互認証（ブリッジ認証局への接続）できる認証局は限られており、民間普及の起爆剤にはまだなっていない。（なお、民間認証局同士のブリッジについては規定がない。）

(3) 公的個人認証サービスの民間利用について

政府では住民記帳台帳カード（以下住基カード）を交付しているが、個人情報保護が重要視されている現在では当初予測よりも低迷を続けている。また住基カードには、本人性を公的に証明する手段（実印の印鑑証明のようなもの）として利用できる公的個人認証サービス（JPKI）の電子証明書を格納することが可能であるが、電子証明書発行数は住基カード発行数の一部に留まっている。

この普及が進んでいない理由としては、住基カードそのものの普及状況の他、有料でること（カード発行費用に加え、IC カードリーダの購入費用や証明書発行費用が必要)、利用できるシーンが少ないことがある。利用シーンについては、省庁や自治体が各種サービスでのサポート範囲を広げつつあるが、市民にとって行政サービスは日常活動の一部に過ぎず、必需品となるには至っていない。普及にとって鍵となる民間利用に対しては、公的個人認証法によりこの証明書の検証者が公的機関と認定認証事業者に限定されているため、一般の民間事業者が証明書の正当性を確認できない、つまり提示されても扱えないことが問題となっている。また、証明書の格納媒体が住基カードに事実上限定されていることも普及の阻害要因の１つと言えるかもしれない。

(4) e-文書法について

2005 年 4 月に e-文書法が施行され、民間の負担を軽減する為、複数省庁に跨って、紙媒体での保存を義務付けている 200 を超える法律のうち、一部の例外を除き一括して電子文書での保存が可能となった。その際必要となるのが、電子署名と、タイムスタンプである。電子署名については、先に述べた電子署名法に基づいた電子署名を必要としている。タイムスタンプについては各省庁によってガイドラインが異なるが、厚生労働省や国税庁などでは、紙を電子文書化する際の要件の一つとして、限定した文書に限り、タイムスタンプの付与を義務づけている。しかし、e-文書法には電子文書を義務付ける強制力がなく、タイムスタンプの法制度的な裏付けもない。

2.3.4 標準化・相互運用性

PKI の利用は、署名する人と検証する人、暗号化する人と復号する人のように二者の相互関係であり、広く利用されるためには、標準化は必須である。基本的な証明書の形式などは X.509 で国際標準として規定されている。しかし実際に相互運用するにあたっては、その運用規約や実装規約、ガイドライン的なものが整備されていないことが、電子証明書の流通性を阻害し、また、利用者の利用環境を不統一で不便なものにすることがある。具体的には、技術面の問題（暗号アルゴリズムや署名形式の種類、署名データフォーマットの不統一、SDK(Software Development Kit)や IC カードドライバのベンダ依存性など)がシステム開発を困難にしたり利用者に不便を強いる

こと、適用分野や業界毎に署名用途や権限属性などを定義するガイドラインが十分整備されていないことが情報の流通性やシステムの相互運用性を阻害することについて述べる。

(1) 暗号アルゴリズムの問題

暗号アルゴリズムに関しては、電子署名の安全性を維持する上で欠かせないものだが、時代とともにその解読法が進化するため脆弱化が進行し、より安全度が高いもの、あるいはより長い鍵長のものへと主流は移り変わる。その結果、主流の移行期には巷で利用されている暗号アルゴリズムが同時期に数種類存在することとなる。署名に必要なダイジェストを生成するハッシュ関数は、従前よく使われていた MD5（128 ビットのメッセージダイジェストを生成）から SHA-1（160 ビットのメッセージダイジェストを生成）に移行してきたが、さらに SHA-1 の安全性も危うくなりつつあり、2010 年を目途に使用を中止する動き（米国 NIST の勧告）もある。よく知られている代表的な暗号アルゴリズムの RSA についても鍵長 1024 ビットから 2048 ビットへの移行が勧告されている。このような状況に対応するには、複数の暗号をサポートし、かつそれらの変更にも柔軟に対応する必要があるため、システム開発者に対する負荷を高めるとともに、利用者にも環境の変更などを強いることになる。

(2) 署名データフォーマットの問題

電子署名の主要な用途の一つとして、文書への署名がある。昨今、e-文書法や、個人情報保護法の施行や証券取引法の改正（日本版 SOX 法）に向けた動きなどの影響によって、企業内の電子文書の管理が重視される中、ペーパーベースの文書を電子化した際の真正性を確保するために重要になってくる。

しかし、電子署名には基本となる PKI 技術からくる有効期限や失効という制約が付きまとう。長期に保存する文書については、有効期限の限界を超え、失効などのリスクに備えるとともに、長期に互換性を保つことが必要である。また保存されるデータが特定のシステムへの依存性が高いフォーマットでは、長期保存が実現できたとはいえない（署名データの種類だけでも、CMS 署名、XML 署名、PDF 署名などがある）。署名の有効性を延長する長期署名の技術として RFC や ETSI で定められた「CAdES」や「XAdES」といった標準フォーマットがあるが、それらのプロファイルについても、あいまいな箇所があることや、選択肢が多すぎる箇所があり、現状、相互運用性を担保して長期に署名文書を保存できるスキームがない。（この問題については ECOM として、相互運用性を高めるため標準的なプロファイルを 2005 年に提案している。）

(3) ベンダ依存の問題

開発者にとっては、PKI 関連の SDK や、鍵の保管に重要な IC カードなどの周辺装置仕様において、標準化が十分ではなく提供ベンダで異なることが問題である。このため、SDK や装置ごとに対応する開発者のスキルが限定され、システム開発の難易度を上げていることから、必要なときに開発者の手配ができないという弊害が起こる可能性も高い。加えて、採用するシステムによってはひとつのベンダ製品に統一することが必要となるため、利用者側の自由度が制限されてしまうことも考えられよう。例えば、利用者が異なるシステムを利用するためには、異

なる IC カードとカードリーダを保有しなければならないケースもありうる。

(4) ガイドライン、権限属性の問題

電子署名が適用される分野や業界毎に、署名用途や権限属性などのガイドラインを早期に定義することも重要である。例えば、医療分野においては、医療の IT 化として、電子カルテの普及促進、遠隔医療システムの基盤整備、レセプトデータなどの有効活用に積極的に取り組むとともに、HPKI（ヘルスケア PKI）に関する証明書ポリシー等のガイドラインを定めている。

基本となるガイドラインが定まっていない場合は、特定分野や業界内においても信頼の根拠となる認証局が異なったり、署名の信頼性のレベルにバラツキが生じてしまうなど、利用者に混乱をきたし、システムの相互運用性を阻害することになる。実際、医療分野以外の業界ではガイドラインが制定されている例がほとんどない為、業界標準化の壁を越えらず、普及が進まない状況にある。

また、PKI は鍵所有者を証明するが、その所有者の権限や属性を明示的に証明するものではなく、システムへのアクセスや文書への署名が何の権限に基づくものかは別途定める必要がある。実際、現実社会では、本人の権限の範囲内で仕事が遂行されている。例えば、ある企業の発注行為は担当者が発注権限をもっているからこそ、他社へ発注することが可能である。しかし、その担当者が本当に発注権限をもっているか否かは企業内では疑う余地が無いが、これがオープンな企業間取引で電子商取引の契約となると、有資格者かどうかの判別は困難である。そこで業界ごとなどのガイドラインを設けて公開鍵証明書の使い方を定めるなどの運用が必要となる。例えば GPKI 府省認証局では証明書を自然人ではなく官職に紐付けることにより、権限を表す運用としている。

権限・属性を定義する技術としては、X.509 の属性証明書があり、公開鍵証明書により本人認証を行った後、そのユーザーの「権限」を属性証明書により確認することができる。しかし権限や属性のグローバルな基準がなく、相互運用性が保証されないため、普及には至っていない。

2.3.5 安全性・信頼性

電子署名の安全性と信頼性（reliability ではなく trust の意）を保つためには、守られなければならない前提事項がいくつかある。認証局側の適切な運用（登録審査、秘密鍵運用、失効管理）はもちろん、アプリケーション側での検証処理、利用者側での秘密鍵の保管と更新などである。これらは利用目的のセキュリティレベルに応じて適切になされる必要があるが、他の技術（パスワードなど）に比べて運用が煩雑と感じられる原因となり、PKI が敬遠される傾向につながっている。また利用者の視点からは、技術の難解さなどにより安全性・信頼性のレベルやリスクが十分理解できず、用途に見合った信頼性レベルの認証局を選択できないなどの問題がある。これら、安全性・信頼性に関して普及を妨げている要因について述べる。

(1) 認証局の運用

公開鍵証明書は本来、鍵と識別子（ID）を結びつけるものであり、生身の個人や資格・権限

を証明するものではないことに注意する必要がある。その ID が確かにその本人のものであるかどうかは、認証局が登録申請時に如何に厳密に確認・審査したかに依存し、またその本人がその資格や権限を有するかどうかは証明書のポリシー（CP）に依存する。例えば電子メールによる申請で発行された証明書は、そのメールアドレスが存在するという以上のことを保証はできず、その信頼性の範囲で利用する必要がある。また運用中の問題としては、認証局の鍵の安全性確保と、利用者の鍵の失効管理がある。認証局の鍵はその認証局の信頼性（その鍵によって署名された公開鍵証明書の信頼性）の源であり、厳格な（運用者自身の不正も防ぐ）管理と、適正な更新が必要である。利用者の鍵については、利用者からの失効申請を受け、速やかにその失効情報を提供して検証可能とすることが認証局の信頼性につながる。

現状、全ての認証局がこのような運用を行っているとは限らず、その信頼性は一様ではない。しかし、その違いが一般利用者に十分理解されているとは言えず、またその差を分かりやすく表現する基準もない。（認証局は証明書ポリシーを CP として提示していることが多いが、それを読みこなしている利用者は少ないであろう。）一般の利用者に分かりやすい認証局の格付けなどがあると便利かもしれない。現時点では唯一、電子署名法により『特定認証業務の認定をうけた電子認証局』であれば、主務省庁（総務省、法務省、経済産業省）の指定する調査機関が、毎年「特定認証業務として定めた運用基準を遵守しているか」を調査しているため応分の信頼度を期待でき、経済産業省などが一般公開（参考 3）しているため客観的な判断は可能である。しかし、それ以外の電子認証局についてはその限りではない。（この他、米国公認会計士協会（AICPA）とカナダ勅許会計士協会（CICA）が定めた「WebTrust for CA」認定・保証制度もあるが、これは主に認証局の業務・サービス・環境を監査して認定するものである。）

参考 3：特定認証業務の認定をうけた電子認証局

経済産業省・商務情報政策局・情報セキュリティ政策室電子証明及び認証業務に関する法律による認定認証業務一覧 http://www.meti.go.jp/policy/netsecurity/digisign_ninteiitiran.htm

(2) アプリケーションの処理

電子署名を利用する際には、署名の検証を適切に行う必要がある。検証処理とは、署名値の確認（署名対象データのダイジェストと署名データを復号したものとの比較）、認証パスの確認（通常、自分のルート CA からの証明書の連鎖）、有効期限の確認、失効有無（有効性）等の確認である。秘密鍵が完全に守られていれば（アルゴリズムが危殆化しない限り）、署名検証、パス検証、有効期限の確認を行えば検証できるが、秘密鍵の漏洩のリスクが存在する以上、失効確認は欠かせない。失効確認失効確認以外は署名データと証明書があればその場でオフラインで処理できるが、失効確認はオンラインで確認するか、何らかの方法で予め失効情報を入手しておいて確認する必要がある。（参考 4）

最も一般的な方法は、失効リスト（CRL）を定期的に入手しておき、証明書検証時に CRL に掲載されていないか確認する方法であるが、CRL 入手時からのタイムラグにより失効を見逃すリスクを許容しなければならない。また CRL をオンラインで入手する場合、失効した証明書が

増加するとCRLのサイズが大きくなり、通信データ量が増大するという問題もある。オンラインで確認する方法としてはOCSPなどがある。これらは検証用のサーバにアクセスして有効性を確認するものであるが、そのサーバにアクセスする機構を作りこむ必要があるとともに、サーバ自体の信頼性をどう確認するかという問題もある。このような特徴やリスクを正しく理解し使い分ける必要があるが、結局システムによっては面倒な失効管理や失効確認を行わず、別の手段（利用者DBなど）で利用者の有効性を確認することも多い。

参考4：電子証明書の主な有効性確認方法

(1) CRL（Certificate Revocation List 証明書失効リスト）

失効したデジタル証明書のリスト。利用中止などの理由で有効期間内に失効させられたデジタル証明書の一覧で、デジタル証明書の受取人は証明書とCRLを照合することにより、証明書が現在も有効であるかどうか確認できる。CRLは認証局（CA）から定期的に最新のものが配布される。CRLの仕様はデジタル証明書の仕様を定めたITU-T X.509で定められている。

CRLのなかでも、電子認証局の公開鍵に対する公開鍵証明書の失効情報を扱うCRLはARL（Authority Revocation List）と呼ばれる。検証者がCRLやARLを入手する際には、LDAP、HTTP等のプロトコルが利用される。

(2) OCSP（Online Certificate Status Protocol）

デジタル証明書の有効性をリアルタイムで確認するプロトコル。OCSPサーバはCA自身や、CRLを集中管理するVAが運営する。OCSPクライアントはサーバに対してデジタル証明書を確認させることによって、自力でのCRL取得や照合の手間を省略できる。OCSPで確認できるのはデジタル証明書が失効しているか否かということだけなので、有効期限が切れていないかどうかの確認などはクライアントが自分で行なう必要がある。OCSPの仕様はRFC 2560で規定されている。

(3) 利用者側の管理

電子署名の信頼性を保つためには、利用者側にも、秘密鍵の安全な保管と適切な更新の義務がある。これは、運転免許証やパスポートなどと同様に、本人であることを証明するものであれば当然のことであるが、パスワードを紙にメモしたり、更新しなかったりすることがあるように、情報リテラシーの格差が存在する状況で、全ての利用者に期待することは難しいかもしれない。しかし、その管理をおろそかにした結果、他人に悪用されることは、本人、または所属する企業等に莫大な損害を及ぼすことにもなりかねないことを認識してもらうよう、啓発していく必要があろう。

また、信頼点（信頼する認証局の自己署名証明書）の管理も重要である。Windows（及びブラウザ）が保持する信頼点群を証明書検証に用いる場合には、利用者が信頼点の管理（追加、削除等）を適切に実施する必要がある。しかし、追加時、警告メッセージが表示されても安易に追加せず、本物かどうかをフィンガープリントで確認しているだろうか。逆に、予め保持されている信頼点群にはWebTrust for CA認定を取得していないものや、実行するアプリケーシ

ョンによっては必ずしも適切でないものが含まれていることを理解しているだろうか。このような処理を適切に行うことは、十分な知識と理解が必要で、容易なことではない。

2.3.6 導入容易性

電子署名を利用するには、公開鍵証明書を提供する「電子認証局」の構築、PKI をハンドリングできるアプリケーションと利用者の環境の準備が必要である。それぞれにおいて、PKI の導入上のハードルがあり、導入が容易でないと考えられている。以下、サービス提供側の準備と、利用者環境の準備の問題について述べる。

(1) サービス提供側の準備について

サービスで電子署名を利用するためには、利用者に証明書と PKI 対応のアプリケーションを提供する必要がある。証明書を発行する電子認証局は、理論上は誰もが構築し、運用することが可能であるが、「信頼できる」電子認証局を物理的に構築し、運用するためには前項に述べたとおり、様々な負担が伴うものである。電子認証局の構築・運用には、PKI に関する知識はもちろんのこと、高度なシステム構築ノウハウと、それを維持するための運用ノウハウが不可欠である。当然、システム構築には相応の費用がかかり、安全性を維持するための設備投資も必要となる。運用規程（CPS）の作成、各種障害対応用のサポートデスクの設置などは意外に負担が大きいものである。このようなことから、サービス提供者が独自で電子認証局を構築・運用するにはリスク、コストともに大きく、敬遠されがちである。

認証局を自分で運用するのではなく、ASP として利用する、あるいは証明書だけ購入する方法もあるが、やはりコストの問題（多くの場合、証明書１枚、年間いくらという価格体系である）と、証明書（を発行する認証局）の信頼性については、導入者の経営判断が必要である。

また、アプリケーションについても、前述したような規約や標準を意識し、危殆化や失効に配慮した開発を行う必要があり、開発者の負担は大きいと感じられる。また既存のサービスに外付けできるものではなく、組み込む必要があるため改造も容易ではない。

(2) 利用者環境の準備について

一方、利用者が電子署名あるいは PKI を使うためには、証明書と鍵の入手、PKI を扱えるソフトの導入、そして鍵を安全に保管できるデバイス等の用意が必要である。

先ず、証明書の入手について敷居が高いと考えられている。個人的な趣味や遊びで利用するレベルのものなら無料の提供サイトなどもあるが、ビジネスシーンで通用するような電子証明書の入手は、それほど簡単ではない。さらに、B2B や B2C を実現するためには、サービスごとに専用の電子証明書を取得せざるを得ない状況にあることも、導入意欲を低下させている。しかも、その利用範囲がクローズな世界、すなわち仲間うちだけに終始していれば、PKI の効果を感じる場面も少なく、継続して利用する意欲が薄れていくこともあるだろう。

PKI を扱えるソフトについては、実は「自分が作成した電子ファイルに電子署名を施し、電子メールに添付して第三者に送信すること」は比較的容易に実現できる環境にある。それは、多くの人が普段利用している標準的なメールソフトが、既に電子証明書をハンドリングできる

機能を備えているからである。しかし、相手側が対応しなければ意味がない。また、個々のサービスについては専用のソフトが必要であり、それを個別にインストールする面倒さに利用者は実際以上に距離感を覚えているのではないだろうか。

また、PKI を利用するためには通常、秘密鍵を『耐タンパ性』に優れたデバイスに格納する。簡単にいえば、秘密鍵を他人が容易にアクセスしたり取り出したりすることができないデバイスのことで、IC カードがその代表として挙げられる。しかし、『耐タンパ性』に優れたデバイスを利用することは、安全性を高めることに有効だが、デバイスによっては特殊な読み取り装置が必要で、相応の費用がかかってしまう。加えて、普段の利用環境にないデバイスを新たに設置し、インストールしたりすることは利用者にとって物理的にも心理的にも負担を強いることにもなり、導入の阻害要因になりうる。

2.3.7 操作性・運用性

電子署名を安全に使うためには、前述のように守らなければならない運用があり、それらは逆に操作性の低下や運用コストの上昇につながる。以下、利用者の操作性、提供者の運用性に関する問題点について述べる。

(1) 利用者の操作性

一般の利用者にとっては PKI や電子署名の概念・仕組み・用語は難解であり、十分理解している人は少ないであろう。また、その仕組みを知らなくても使いこなせる製品が普及していないことも、パスワードなどに比べて利用時の心理障壁となっていると考えられる。特に、秘密鍵の安全な管理が PKI の根幹であり、耐タンパデバイスや PIN（暗証番号：Personal Identification Number）で保護したうえ、有効期間があるため定期的に更新しなければならず、ユーザの負担はどうしても大きくなる。実際には安全な管理の必要性はパスワードも同じであるが、より厳格さを求められるため負担感が高まるとも考えられる。

(2) 提供者側の運用性

基盤を提供する側（認証局など）の運用も、面倒であり、運用コストが高くなると考えられている。具体的には、登録時の審査から、システムの秘密鍵の管理や有効期限による更新、上位 CA との認証パス構築、検証情報（失効情報）の提供などである。認証の例に置き換えて考えてみると、パスワードの場合、適当な初期パスワードを与えれば、後はユーザが適宜更新するだけで、運用者はほとんど手間がかからないシステムが多いことに比べて、PKI の運用は重いと感じられている。（実際にはパスワードの場合も、より安全な運用を求めれば、それなりの運用、例えば郵送での通知や定期的な更新などが必要ではあるが。）これらのことが負担感となり、電子署名や PKI の利用を妨げる一因となっていると考えられる。

2.3.8 保守性

PKI 技術を使い続けるためには、保守の問題も重要である。保守にはシステムのハードウェア、ソフトウェアの他、利用技術、方式そのものもある。PKI の特徴である暗号アルゴリズムそのも

のの変更に伴う保守性について述べる。

前述の通り、PKI は数学的な解読の困難さに基づく方式であるため、計算能力の向上など技術の進歩により安全性が低下する（危殆化という）リスクを本質的に伴っている。そのため、様々な、より強固なアルゴリズムが考案されているが、そのことはシステム的には、プログラムの変更やシステムの入替え、ユーザに配布された鍵や証明書の交換という運用が避けられないことを示している。さらには、署名済みの文書等についても、その有効性を保持するためには再署名（長期署名）等の処理が必要となる。システムやユーザが保管している文書についてはまだしも、流通している文書等については対処が困難である。

システムについて言うと、プログラム変更は暗号技術に密接に結びついた SDK を駆使しなければならず、SDK や暗号アルゴリズムが変わるとアプリケーション開発および維持管理へのインパクトはさらに大きくなる。

またユーザ側にとっても、耐タンパデバイスの交換となると手間に加えて費用負担が発生する可能性もある。（これも、パスワードであれば、記憶をリフレッシュするだけで良く、負担感が小さい。）これらのことも、PKI 技術が敬遠される一因と言える。

2.4 問題点の相関

前節で述べた各問題点には因果関係のあるものも少なくない。「電子署名（PKI）が普及していない」すなわち「証明書が普及していない」という現状を中心に置いて、その原因となる問題点を辿るように、主な問題点の相関を図 2-3 に示した。提供者はサービス提供者、経営者、CA 運用者に細分した。

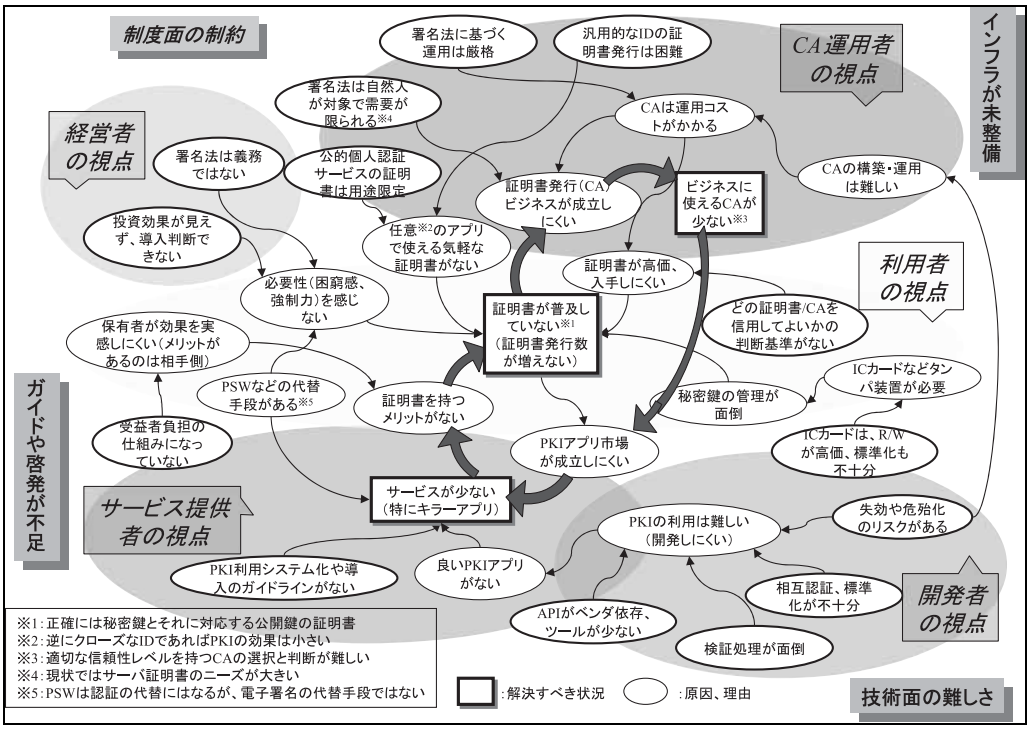

図 2-3 電子署名及びその基盤となる PKI 普及上の主な問題点の相関

この相関の起点（矢印の出発点）となるものがより根本の原因と考えられる。おおまかに言うと、インフラの整備、制約の多さ、技術的困難さ、ガイドや認知・啓発の問題に分けられる。また、証明書が普及していない（需要が少ない）→CA が増えない→PKI 利用サービス（アプリ）が生まれない→証明書が増えないという相関関係はループしており、この負の連鎖を断つためには、1 つの問題だけ解決するのではなく、複数の問題を同時に解決する施策が必要であろう。

3．電子署名利用モデルに関するケーススタディ

本章では電子署名普及に関する課題設定の前に、具体的な問題が発生しているネット通販やネットオークションにおいて電子署名の利用が問題解決に役立つかどうかの観点でケーススタディを実施する。

3.1　ネット通販、ネットオークションにおける問題意識

近年、インターネットとパソコンの普及によりネット通販やネットオークションの利用が急激に広がっているが、それに伴いトラブルも急激に増加してきている。(図 3-1 参照)

今後、多くの国民が安心して安全にこれらのネット取引を利用できるようにするためには、ECOM の取り組みのように問題発生時のトラブル相談窓口[注1)] を継続的に開設すると供に、いかにして問題の発生を未然に防ぐか、発生した場合に迅速に解決する手段を提供できるかが大きな課題である。

注 1）ECOM「インターネット関連 ADR 実証実験報告書」参照

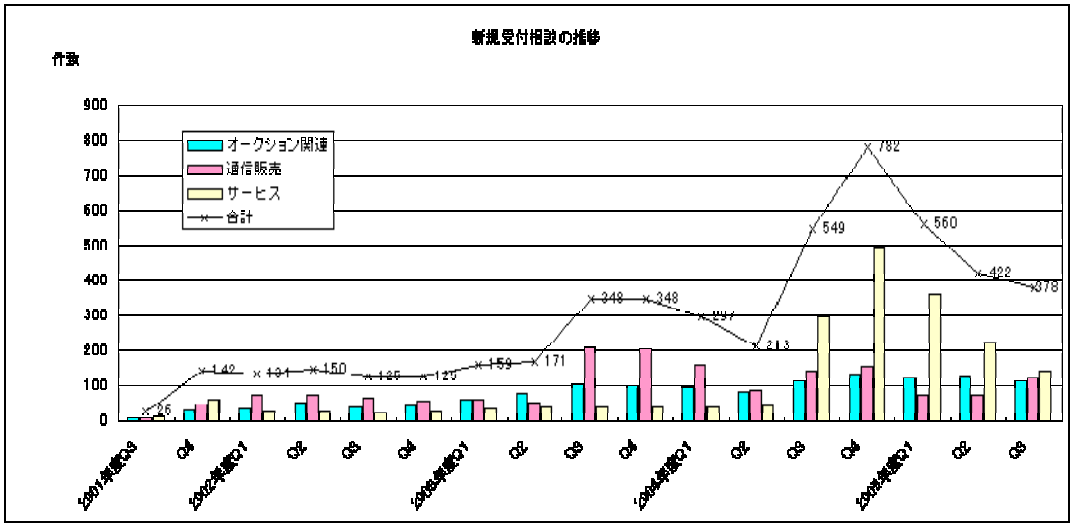

図 3-1 ネット通販・ネットオークション等におけるトラブルの増加

3.2　トラブルの類型

これらのネット通販やネットオークションにおけるトラブルは、トラブルの種類に着目して、いくつかの類型に分類することが出来る。以下に類型を示す。

また、「インターネット関連 ADR 実証実験報告書」の具体的事例を分析し、どのトラブル類型に対応するのかを別紙 1 に掲載している。

1) 商品未受領

① 代金振り込み後に連絡が付かなくなる

② 連絡は付いているが言を左右にして返金されない（詐欺的）

③ 経営破綻等

2) 商品に不満
   ① 説明と実物が違う、
   ② 瑕疵がある等
   ③ 偽ブランド物
   ④ 輸送上の破損
   ⑤ サービス内容
3) 代金関連
   ① 代金が支払われない
   ② キャンセル手数料
   ③ 金額関連、送料負担、税金表示等
   ④ 重複請求
4) その他
   ① オークションの評価欄での誹謗中傷
   ② オークション手続きの問題
   ③ 名誉毀損
   ④ 個人情報流出

これらのトラブル類型においては、事前に取引相手の実在性や信用度を確認出来ることも重要であるが、トラブルが発生した後に取引相手と連絡ができるかどうかで、解決の可能性が大きく変わってくる。最終的なトラブル解決手段である訴訟を視野におくと、相手に訴状を送達できるかどうかが、大きな分かれ目になる。すなわち、相手の住所等の連絡先を確実に知ることが出来る手段が担保されているかどうかが、ポイントとなる。

3.3 ネット取引における相手確認の類型

インターネットの世界は、取引相手を直接対面で視認することが出来ないため、間接的な方法により相手の存在や信用を確認することが必要となる。

ここでは、ネット取引において利用可能な相手方確認手段の類型とその強度について比較評価する。評価の観点としては、次の 2 点を上げることが出来る。

① 相手の実在性を確認できる
   相手が実在の人物・組織であり、相手とコンタクトする手段が確保されているか
② 相手の同一性を確認できるか
   繰り返し取引や取引内のやりとりで、既知の人物・組織（自分が信頼している者）と同一の相手と対応しているのかを担保出来るのか

また、インターネット越しに、確実に相手を確認できる手法である電子署名の利用方法としては、次の 2 通りが考えられる。

(1) 直接利用型
   売買契約成立時点に契約書に署名を打ったり、売買のトランザクションに署名を打つことに

より直接電子署名を利用する方法である。具体的には、Web から注文する時点で注文書や請け書に署名を打たせたり、s/MIME を利用した署名付き電子メールの利用が考えられる。この方法では、電子署名を利用する際に署名者の公開鍵証明書を直接確認できる反面、公開鍵証明書そのものをを相手に送付する必要があるため、公開鍵証明書に個人情報を含む場合には個人情報漏洩のリスクが発生する。

(2) 間接利用型

直接的に取引トランザクションの中で署名を使うのではなく、モール事業者やオークションサイトが、業者や個人が取引に参加する前に、予め参加規約や申込書に電子署名を打たせて本人確認し、トラブル発生時に裁判所の命令などにより本人の情報を開示すると言った使い方である。この使い方であれば個人情報漏洩のリスクは大幅に低減される。

以下にそれぞれの相手確認手段において、上記の観点から確実な確認が可能であるか評価する。

1) 電子メールアドレス、URL

簡単な申請で取得できるため、確認の信用度は低い。ある程度同一性は確認できるが、実在性の確認は困難である。DNS の乗っ取りや電子メールのすり替え等が発生すると、同一性の確認も出来なくなる。

2) 電話番号（固定電話：携帯電話では無いという意味）

一方的に通じなくなったり、インターネット電話の普及により実在性の確認が不十分である。同一性はある程度確認できる。しかし、C2C 取引では一般的に開示されない。

3) 住所（郵送等の手段により確認済みのもの）

ある程度の実在性、同一性の確認が可能であるが、一方的に掲示されているだけでは信用できない。また、ネット通販においては、特定商取引法上、開示が義務付けられているが、C2C 取引では開示されないことも多い。

4) 銀行口座・クレジットカード番号

同一性は確認出来るが、実在性確認の信用度はそれほど高くない。

5) トラストマーク等のオンラインショップ向けマーク

マーク制度が何を保証しているかによっても異なるので、利用においては当該のマーク制度の保証内容を確認する必要がある。当該のマーク制度が同一性、実在性ともに保証している場合で、かつ運営主体等が信頼できる物であれば、同一性、実在性供に十分信用できる。しかしマークの複製を掲示している場合があるので、マーク自体が本物であることも十分検証する必要がある。

6) モール事業者

大手のモール事業者（楽天やビッターズ等）では、ある程度、出展店舗の実在性確認を行っており、消費者はトラストマークよりもモール事業者の信用力（ブランド力）を当てにして購入を決定する傾向がある。この場合の実在性確認の根拠はモール事業者による出展店舗確認の内容によって変わってくる。モール事業者と出展者の間で対面を含む継続的なやり取りがなされる場合には、十分信頼が置ける確認となるが、インターネットのみでの確認する場合には確実な本人確認が困難であり、項番 10 や項番 11 の電子証明書を利用して確認の手法が有効と思われる。

また、モールの出店マークを不正に掲示して信用を得ようとする店舗も出てきていることから、マークの信頼性を担保する仕掛けや、電子証明書を用いた確認の仕掛けを採用することにより、より確実に信頼性を保証することが出来る。

7) オークションサイト

オークションにおいては、現状、出品者の本人確認や実在性確認は十分ではなく、組織的なものも含め、詐欺が多発している状況である。現在の対応はオークションサイト独自の「補償」スキームによって一部金銭的に救済する手段が提供されている。より根本的なトラブル回避（詐欺防止）手段として、オークションサイトの本人確認方法に関して、項番 10 や項番 11 の電子証明書を利用した確認の手法に誘導または義務付けることが有効と思われる。

8) 一般の電子証明書

電子署名が打たれていることにより、同一の署名であれば相手の同一性については確認できるが、実在性については証明書を発行する認証局の本人確認方法により大きく異なってくるため、一般の電子署名の場合には、署名がなされているからといって一概に信用できるとはいえない。また、個人で作成した認証局から証明書を発行することも容易となってきているため、公的ではないこれらの認証局から発行した証明書は十分な本人確認手段とはならない可能性がある。

9) 商業登記の電子証明書

同一性、実在性供に十分保証されるが、詐欺的な企業の場合には、詐欺を働いた直後に計画倒産する等の手口もある。また、取得コストが高く、登記された法人のみの利用に限られる。

10) 電子署名法による認定認証局の証明書

同一性、実在性については十分確認できる。しかしながら、証明書取得後の変化（住所変更等）には対応が難しい。また、証明書取得コストが高く、個人での利用は限定的である。

11) 公的個人認証の証明書

インターネットにおいて、個人に関する同一性、実在性の確認について、現時点では最も信頼できる手段と成り得る。住所変更等の証明書取得後の変化にも対応している。しかしながら、現時点では民間における自由な利用が許されていないという課題がある。

これらの類型についての比較を表 3-1 に示す。

表 3-1 信用確認方法による信用度合い評価の違い

#	信用確認方法	実在性の確認	同一性の確認	信用度合い評価			備考（脅威等）
				業者	個人出品者	**個人購入者**	
1	電子メールアドレス、URL	危	△	危	危	危	
2	電話番号（固定電話）	危	△	危	危	危	
3	住所（郵送確認済み）	△	△	△	△	△	偽の店舗
4	銀行口座、クレジット番号	△	○	△	△	△	
5	トラストマーク	○	○	○	―	―	
6	モール事業者の信頼	○	○	○	○	―	モールのブランド
7	オークションサイトの信頼	△	○	△	△	△	業者のスキーム
8	一般の電子証明書	△	○	△	△	△	
9	商業登記電子証明書	○	○	○	―	―	詐欺、偽登録
10	認定認証局証明書	◎	◎	◎	―	―	個人には高価
11	**公的個人認証証明書**	**◎**	**◎**	**ー**	**◎**	**◎**	住所変更対応

評価凡例：　◎：充分安全であるとの推定が成り立つ
○：ある程度安全であるとの推定が成り立つ
△：それのみで安全であるとは言えない
危：それのみで信用するのは危険である
ー：該当しない

3.4　考えられる対応策

ネット通販やネットオークションにおいては、販売者と購入者の間で順番に何回かのやりとりがなされ取引が完了する。このやりとりを取引のフェーズとして分類し、それぞれでどのような確認をすることよりトラブルを防ぐことが出来るか対応策を検討する。

1) 取引のフェーズ

取引は大きく次の 3 つのフェーズに分けることが出来る。

① 購入前フェーズ：商品やサービスを購入する前に事前の調査や問い合わせを行い購入意志を固めるまでのフェーズ。
② 購入中フェーズ：注文から代金支払い、商品の発送・受領といった取引の実体フェーズ
③ 購入後フェーズ：取引が一旦完結した後に、届いた商品に不満があったりして、アフターサービスを必要とするフェーズ。

ネット通販を例に、代表的なネット取引の流れと取引のフェーズとの関係をを図 3-2 に示す。

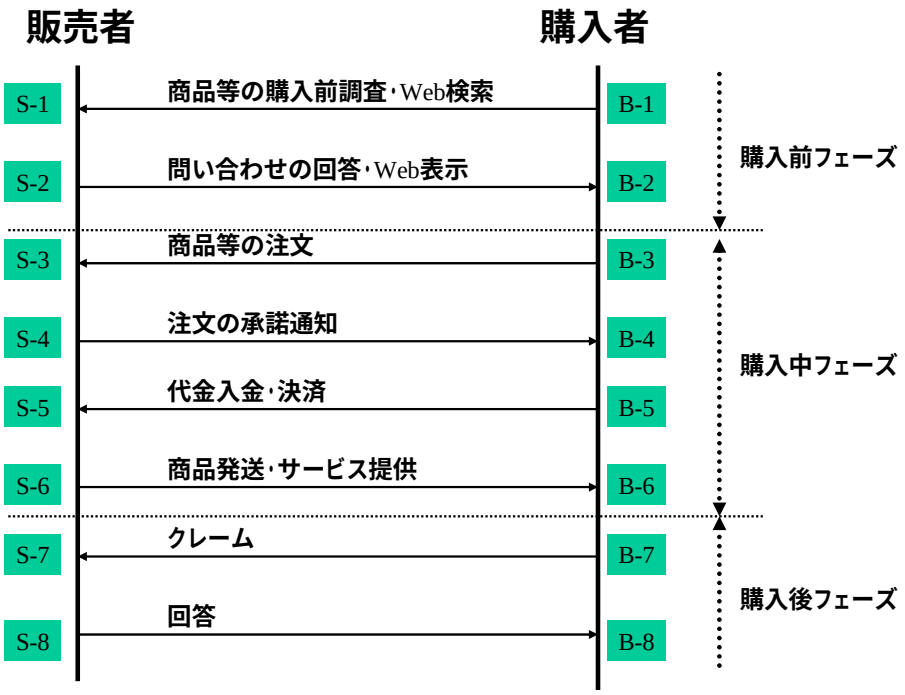

図 3-2 取引フェーズの定義

2) 問題解決の考え方

3.3 節において相手確認の方法により信用度合いの差があることを示したが、次にこれらの確認をどの時点で実施することが有効であるか検討する。

①購入前フェーズ

相手を評価しているフェーズであり、この時点で問題は発生しないが、購入フェーズに入る前に、様々な情報により取引相手を十分確認しておくことが重要である。

②購入中フェーズ

実際に商品の発送や代金の授受が発生するため、その前までに必要な確認を済ませておくことが重要である。

③購入後フェーズ

取引自体は一旦完了しているが、リアルの世界の相対取引では起こりにくいような、商品が偽物であったり、注文と異なった商品が送られてくる等のトラブルが発生し、クレームへと発展することになる。

3) トラブル発生のポイント

図 3-2 に示した取引フェーズの中で、トラブルが発生する可能性が高いポイントをいくつかに絞ることが出来る。内容的には、そのポイントで権利・義務関係が変化する点である。

①B－4：注文の承諾通知受領

注文の承諾通知が購入者に届いているので契約が成立し、購入者の支払い義務と販売者の販売義務が発生するため、キャンセルや代金不払い等のトラブルが発生する。

②S－5：代金支払い／決済後

代金を支払ってしまっているので、商品が到着しないトラブルが発生する。

③B－6：購入後

契約の履行は完了して居るが、品物の瑕疵等の不備による契約解除の問題、オークションサイトの評価欄での誹謗中傷や名誉毀損、個人情報流出といった様々なトラブルが発生する。

具体的な事例におけるトラブルの発生については､別紙１にまとめているので､参照願いたい。

4) 信用確認方法に関する考察

①B2C 取引（ネット通販等）の場合

B2C の取引を想定した場合には、業者の信用が大きなポイントとなるため、購入者となる個人から販売者となるショップに対する信用確認方法に着目して評価する。初回の取引においてはトラストマーク、モール事業者の信用、商業登記や認定認証局の電子証明書等が有効な手段となる。また、繰り返し取引が発生する場合には、同一性の確認が有効に働き郵送確認済みの住所や銀行口座等も役立つ。

②B2C 取引（個人のネットショップ等）の場合

個人で運営しているネットショップでは、現在運用されているトラストマークや商業登記や認定認証局の電子署名書を利用することはコスト負担が大きいため利用が難しい。そこで、モール事業者が信用を仲介したり、ADR（裁判外紛争解決）を個人の出展業者でも利用しやすい低コストな制度として実現してゆく事により問題の解決が図られるであろう。この際、個人事業主に関しては公的個人認証の証明書により本人確認する方法が、コスト面や確認の精度から見ても非常に有効と考えられる。

③C2C 取引の場合（ネットオークション等）

C2C 取引では相手が個人となるため、販売者、購入者両方に関して個人の特定が重要になってくる。初回の取引においては、認定認証局の電子証明書や公的個人認証証明書が有効であるが、コスト的に認定認証局の証明書を個人で取得する機会は少ないため、公的個人認証が最も有力な手段となるであろう。

しかしながら、現状、公的個人認証の用途はプライバシー保護や民業圧迫への配慮から、行政機関等に向けた電子申請等に用途が限られており、現時点の計画では用途拡張のための法律改正がなされても、司法書士等の士業組合が代理申請において利用したり、電子申請に必要な添付書類（診断書等）作成する業者が利用したりする程度である。今後安価な本人確認の手段として、オークションサイト側が公的個人認証の証明書の提示を義務づけるなど、民間においても公的個人認証を活用する道を開いて行くべきと考える。

ネット取引において本人確認を確実に行うことで、自分の身元が知られることによる犯罪抑止効果や、万一のトラブルが発生した場合に本人の追跡を可能とすることにより、迅速なトラ

ブル解決につなげることが出来ると考える。このような情報開示は、プライバシーに配慮すべきとの議論もあるが、個人情報についてはトラブル発生時にのみ開示するようプロバイダーやオークション業者が責任を持って管理する等の方法も十分採りうるものである。

4．電子署名の普及へ向けた課題

4.1　電子署名を取り巻く背景

4.1.1　普及への展望

ブロードバンド等のネットワークの普及や技術の発展に対して、電子署名の普及が進んでいないという声が強い。しかし、電子署名の普及の課題は、技術的な問題以外の部分にあるといってよい。「紙と印鑑」の文化から「電子文書と電子署名」の文化へ移行するために、まずはこれまでの慣習の壁を越える必要がある。また、企業内だけであっても「紙と印鑑」から「電子文書と電子署名」への移行は、業務の本質的な変革が要求される。

電子署名がなされた電子文書は、これまで IT の普及が困難だった業務を劇的に改善する可能性も秘めているが、電子署名を利用した更に効率的な電子社会へと移行させるために、これまでの人々が「最適」と思ってきた実務の意識を変える必要もあるかもしれない。

法制度との結びつきの深い電子署名は、法制度的な課題も多々ある。電子署名法、IT 書面一括法、e-文書法など IT 関連の法制度の整備は進んでいるが、民事法領域の IT 化対応には課題が多く、例えばこれまで商取引を支えてきた手形法は、紙の手形を前提としている。

結局のところ、現在の社会は「紙と押印」を前提にした社会であり、様々な法制度も紙文書を前提に最適化されており、電子文書を前提にした社会への移行には大きな変革を伴うことになる。

2001 年に施行された電子署名法により、電子署名が付された電子文書の真正性に法的な裏づけが出来た訳だが、IT 化を妨げる社会的制約が、電子署名の普及も遅らせた面がある。

このように「電子文書と電子署名」の普及には、様々な「紙と押印」を前提にした社会の制約を取り除き、変革、改革を推し進める必要があった。しかし、こうした変革、改革を進める気運が生まれつつある。2006 年 1 月 19 日に発表された「IT 新改革戦略」では、「構造改革を進め IT 化を妨げる社会的制約を取り除く」としている。「IT 新改革戦略」において「構造改革と IT 化は社会の改革の両輪をなす」とされているが、「電子文書と電子署名」は、正に構造改革により普及のきっかけを見出す可能性が高い。

IT 化による効率化も重要だが、法制度の観点からは、効率と同時に不正に強く、透明性の高い社会を目指すべきであるが、そのためには電子署名の普及は重要な意味を持つ。これは、電子文書の電子署名を付すことについて適度な強制力を働かせる必要があると考えられる。構造改革により、効率化やコスト削減のための電子文書化が推進され、効率化と同時に不正に強く、透明性の高い社会の構築のために電子文書に電子署名を付すという方向性が見えてくる。結局のところ、電子署名が可能というだけでは普及に繋がらなかった。電子署名を使えば、便利な社会が到来するというよりは、コスト削減、利便性への要求が IT 化、電子化への流れを推進し、その電子化の中で適切なセキュリティを保つために電子署名が使われていくと考えるべきであろう。

4.1.2　2001 年施行の電子署名

電子署名の普及の展望を述べる前に、現行の電子署名法について説明する。電子署名法（正式

名称「電子署名及び認証業務に関する法律」）は 2001 年 4 月に施行された。電子署名法に主な内容は、「電磁的記録の真正な成立の推定」と「認証業務に関する任意的認定制度の導入」である。対象は、自然人の電子署名が対象であり、逆に、また、電子証明書に法人、サーバ、エージェントなどの署名などは対象外となっている。より可能な、電子認証（Authentication）や暗号化も範疇ではないと考えられる。

電子署名法の「電磁的記録の真正な成立の推定」と「認証業務に関する任意的認定制度の導入」により、電子署名が利用できる環境が整備された。一方、「自然人」による否認防止の署名という制約や、非常に厳しい認定基準が電子署名の普及を阻害している可能性もある。電子署名は、法制度との結びつきが強いが、電子署名が重要になるのは、重要文書の保存が義務付けられる文書などであるが、電子署名が適合する業務は、これまでの紙前提として法制度に阻まれている面もある。

2001 年 4 月施行の電子署名法は、施行 5 年を向か改正される可能性もあるが、普及という観点で検討されることが望まれる。

4.1.3 2005 年 4 月施行の e 文書法

e 文書法（民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律）は 2005 年 4 月に施行された。この e 文書法は、電子署名に大きな影響を与えつつある。電子署名は、重要な電子文書に大きな意味を持つわけであるが、重要文書の電子化がなされなければ、電子署名自体もあまり意味をなさないという問題がある。そして、電子文書化には、既存の法制度による制約があるが、こうした典型的な例に、紙文書による保存義務を定めた多数の法令等の存在があった。

e 文書法は、法令で保存が義務付けられている文書の電子保存を大幅に認めている。これまでは、IT 基盤を利活用しようにも、その対象となる文書が紙文書では利活用のやりようがなかった訳である。また、これまで、電子署名は、単純にコストと見なされていた面があるが、紙から電子文書へ移行することによりコスト削減が可能ということも理解されつつある。2001 年の電子署名法の施行当時は、ネットワークを介しての利用、それが便利になるという側面が強調されていた。しかし e 文書法により、電子署名は、ネットワークを使ったサービスというよりは、（保存が必要な）紙から電子データの移行にとって重要という認識が生まれつつある。

e 文書法の波及効果は大きなものがある。電子文書の保存には電子署名が重要であることを再認識させられ、紙文書依存の業界が e-文書法で刺激されているが、こうした中、電子文書の管理、保存に対して、様々なソリューションやサービスの提供が開始されつつある。そして、その中で電子署名が有効に利用される兆しが見える。電子署名は、法制度との関係が深く、署名文書は、長期の保存が必要な場合が多い。e 文書法は、文書の保存に署名が有効な技術であることを示した。そして、文書の長期保存について、電子署名だけでなく、タイムスタンプ（時刻証明）の重要性が認識されつつあることも大きい。

電子署名が付けられた電子文書が、更に、標準化が進めば、特定のシステムの依存性を大いに減らすことができる。こうしたことは、特に長期にわたる電子文書の保存には、非常に重要にな

る。情報システムのライフサイクルは短く、文書の保存期間は長くなる傾向がある。こうしたことも含め、電子署名、タイムスタンプを使った安定した長期署名フォーマットの出現が求められているが、これに対応した重要な動きにECOMの「ECOM長期署名フォーマット」がある。

4.1.4　タイムスタンプサービスの整備

2005年に施行された通称e文書法に関連した動向としてタイムスタンプサービスの普及がある。電子署名を行う文書は、基本的に保存されるべき文書であり、その時刻証明などは、重要な意味を持つ。タイムスタンプサービスの主な方式のうちのひとつは、時刻が何らかの形で保証されたサーバが行う電子署名によって実現される。つまりタイムスタンプ自体も電子署名により実現された技術と言える。

電子署名法においては、自然人によるいわゆる自署名がその範疇であり、こうしたサーバ（タイムスタンプサーバ）による署名は、電子署名法の対象外となっている。そうしたこともあり、タイムスタンプによる時刻証明の法的有効性は、一部の省令（財務省令など）で認められたに過ぎないが、とはいえ「タイムビジネス信頼・安心認定制度」が発足するなど、電子文書のセキュリティを確保するために大きな前進があった。

「タイムビジネス信頼・安心認定制度」が適切に運用されれば、タイムスタンプによる時刻証明は、非常に信頼のおけるものになる。従来は、こうした時刻証明は、信頼のおける人手による作業として行われてきた。具体的には、公証人による確定日付の付与といった形で行われてきた。タイムスタンプによる時刻証明は、こうした公証人による確定日付の付与にくらべ、非常に低コストで、かつ自動的に行うことが可能で、社会全体としての大きなコスト削減を可能にするだろう。そうしたこと含め、タイムスタンプによる時刻証明が広く法的根拠を持つことが検討されるべきであろう。

4.1.5　ECOM長期署名フォーマットの重要性

e-文書法は、文書に関連した業界に様々な刺激を与えたが、e 文書法に触発され大きな成果を生みつつあるものに「ECOM長期署名フォーマット」がある。電子文書を長期に保存、管理するためには、「電子文書」のデータとしての独立性の問題がある。5年、7年、10年、30年と法令などで保存が義務付けられている文書を、完全性を保つためにシステムに依存した形で保存することは望ましくない。なぜならシステム自体の寿命があるからである。

電子文書の長期保存や広く文書のセキュリティを実現するためには、暗号技術、タイムスタンプ等の（暗号）技術等によりシステムから独立した電子文書のデータとしての独立性が実現可能といったことは、理論的また技術的には知られていた。しかし、保存されるデータがばらばらのフォーマットでは、長期保存が実現できたと言えない。特定のシステムの依存性を極小化するため標準化されたフォーマットで電子署名技術等の暗号技術を用いて保存されるべきである。長期に保存されるデータだからこそ特定のシステムからの依存性を脱し標準化されたフォーマットで電子署名技術を用いて保存されるべきである。つまり電子文書の長期保存実現には、こうした標準化、そして広く利用されるための相互運用、展開の努力が欠かせない。ECOMの長期署名フォーマットのプロファイルは、正に、こうしたことを実現する上で非常に重要な役割を果たしつつあ

ると言える。電子署名の普及には、ECOM 長期署名フォーマットのプロファイルのような標準化への努力が欠かせないということが認識されるべきであろう。

4.1.6　重要文書の紙文書から電子文書への流れ

様々なコンテンツがデジタルコンテンツ化される中、経済活動に重要な意味を持つ、契約文書などの電子化がそれほど進んでいないことが、電子署名の普及を遅らせている原因になっている。その一方、IT 技術の進歩が原因で紙文書のセキュリティが保てなくなりつつあり、そのために電子署名を利用した電子化が進んでいる分野がある。

(1) IC 旅券（パスポート）
(2) 運転免許書の IC カード化

IC 旅券なども IC カード化やバイオメトリクス情報が格納されていることが強調されている面があるが、それ以上に旅券文書への電子署名が非常に大きな意味を持つ。その他、紙文書の偽造で、問題になっているものとしては、以下のようなものがある。

(1) 通帳の押印の偽造
(2) 構造計算書の偽造

紙ではないが、偽造キャッシュカード問題における磁気ストライプカードのスキミングのように、IT 技術の進歩は、様々な偽造を「早い」「安い」「簡単」にしてしまっている。つまり、紙から電子署名などを施したセキュアな電子文書への移行なくしては、これまでの文書のセキュリティも保てなくなることに注意すべきである。

旧来からの紙文書だけでなく、IT 技術の進歩は、そもそも紙文書では保存不可能な様々なデジタルデータを生んでいる。例えば、医療では大量の画像データが使われている。またゲノム情報のようなものは、保存のため紙文書にするといったことがほとんど不可能な情報量を持つ。これらの保存には、やはり改ざん防止が施されるべきある。

このように、紙文書のセキュリティの低下、紙文書として保存不可能な様々な電子データの出現に対して、保存される電子文書、ないし電子データは、電子署名は適切に利用され保存されるべきである。

企業においては、様々な業務の IT 化はコスト削減、効率化のため行なわれており、結果、企業においての重要文書においても電子文書への依存性を深めている。そうした中、今後施行が予定されている日本版 SOX 法では、財務報告などに関して内部統制が求められている。その他にも、また、それぞれの業界毎の業務について内部統制や法令遵守が求められる傾向にある。企業が IT 技術への依存性を深めていく中、構造計算書の偽造問題に見られるように紙文書を前提とした統制自体が、今後、ますます現実的ではなくなる。e 文書法の影響もあり、文書管理システムに電子署名やタイムスタンプが組み込まれた製品が数多く開発されつつあるが、こうした製品の普及とともに企業においても電子署名が普及していくことになるだろう。

4.1.7　医療 IT の促進と電子署名

今後、電子署名の普及が期待される分野に医療がある。これは、医療改革に関連した IT 技術の促進と無縁ではない。医療の IT 化による効率の向上と、更に、連携による医療の質の確保が要求されているが、このとき同時に不正に強く、透明性の高い医療を提供する必要がある。

e-Japan 重点計画－2004 では、「IT を活用した医療情報の連携活用」、「IT を活用した医療に関する情報の提供」、「電子カルテの普及促進」、「遠隔医療の普及促進」などの目標が掲げられている。これらの実現には電子文書の保存が大きな要件になっている。

こうした動きを受け、医療分野での PKI の標準化も進められている。2005 年 4 月には、「保健医療福祉分野 PKI 認証局　証明書ポリシ」が公表されているが、この証明書ポリシでは、医師などが署名を行うために必要不可欠な署名用証明書の証明書プロファイルなどが規定されている。

保健医療福祉分野 PKI 認証局が発行した証明書が、医師という職業人に普及する意義は大きいものがある。否認防止の署名は、権限、職責など何らかの責任を持った人間が施すことに大きな意味がある。権限、責任のない人にとっては、否認防止の署名を行う意味合いは少ない。例えば、医師が記述するカルテの場合、カルテへの署名は、医師という資格を持った人間が、その責任において文書に署名を施すことが重要であり、法令遵守などを示すためには、この署名文書が適切な期間保存される必要がある。ところが、こうした権限、責任が必要な分野ほど、法制度的な制約がある場合が多く、電子化が進まない場合が多かった。しかし、これらは改革により、これらの制約が解決されようとしている。

2006 年月に発表された政府の IT 新改革戦略では、「医療の構造改革を IT により推し進め効率的な医療を国民に提供すること」とされており具体的には以下のような目標が掲げられている。

> IT による医療の構造改革
> －レセプト完全オンライン化、生涯を通じた自らの健康管理－

こうした「改革」は、電子署名の本質的な普及を促す原動力になるだろう。また、IT 新改革戦略では、医療分野の PKI についても言及している。

> ６．厳格な本人確認を行いつつ診療情報等の安全な交換や参照を実現するため、HPKI（Healthcare Public Key Infrastructure：保健医療福祉分野の公開鍵基盤）、安全で安心なネットワーク基盤等を 2008 年度までに整備する。

医療に限らず、電子署名が使われるべき分野は、トップダウンな政策的な判断が必要な分野が多い。効率、コスト削減のための改革と IT 化、同時に IT 化の中で適切なセキュリティを保つために電子署名の意味が IT 政策担当者などに十分理解されることが重要であろう。

4.1.8　電子申請の普及

電子政府では、電子申請、電子入札、電子申告などにおいて、電子署名が利用されている。し

かし、強制力の働く電子入札以外は、利用率が極端に低いのが現状である。

電子申請、電子申告が普及していない理由は、様々な理由が考えられているが、少なくとも電子申請などを可能にすることが目標になっていたが、これらが利用されることに関しては目標となっていなかった。「IT 新改革戦略」では、利用率が目標として上げられており、そのための施策の検討が促されている。

１．利便性・サービス向上が実感できる電子行政（電子政府・電子自治体）を実現し、国・地方公共団体に対する申請・届出等手続におけるオンライン利用率を 2010 年度までに 50%以上とする。 １．オンライン利用促進対象手続について、各手続の利用目標を含む利用促進行動計画を 2005 年度に策定・公表し、2010 年度までにオンライン利用率 50%以上を達成する。 ２．オンライン利用の促進を図るため、所得税、法人税の電子申告に係る制度・運用の改善策や電子的な税、手数料等の納付普及の方策について検討を行う。 ３．利用者視点に立って、添付書類の電子化、省略・廃止、手続自体の廃止、インセンティブの付与、処理期間の短縮、本人確認方法の簡素化（電子署名を省略できる場合を整理）等、手続の見直し・改善や紙文書による業務処理からの脱却とこれによる職員の意識改革を図る。

この目標どおりの利用率が向上すれば、電子署名自体の普及に拍車がかかると考えられる。

電子申請、電子申告の利用率向上のために簡易なものに関しては「電子署名の簡略化」なども一部提案されている。電子署名が適切に使われることが重要であり、こうしたことが、電子署名に対するリテラシーを向上させ、実質的な普及を促すことになるだろう。

4.1.9　その他の法制度と IT 施策

電子署名は、法制度との結びつきが非常につよい。今後、大きな産業に発展し、また、法制度自体も大きく変化すると考えられる分野に、デジタルコンテンツに関連する分野がある。ブロードバンドが普及し、このブロードバンドの利活用には、デジタルコンテンツの著作権問題などの解決が重要になる。DRM（デジタル著作権管理）だけでなく、デジタルコンテンツの真正性を保証するフレームワークなどでは、電子署名の活用が欠かせない。

紙から電子への流れに関連して制定が予定されている法律として電子債権法（仮称）がある。電子債権において電子署名が使われるかは、現時点では不明であるが、電子債権に関連して普及が促進される可能性がある電子契約などでは、電子署名が適切に利用されるべきである。

4.1.10 電子署名法の改訂の検討

2001 年 4 月 1 日に施行された電子署名法は、来年で施行 5 年になる。この電子署名法は、条文の中で、「政府は、この法律の施行後五年を経過した場合において、この法律の施行の状況について検討を加え、その結果に基づいて必要な措置を講ずるものとする（附則　第三条）」とされている。こうしたこともあり、電子署名法の改正に向けた動きもある。

ドッグイヤーとも言われる急速に発展する IT 技術の世界において、5 年は非常に長い。IT 技術、IT 施策で大きく環境が変化しているが、電子署名法をはじめとする現行の IT 技術の関連した法制度は、こうした環境の変化に追随できていない側面がある。

また、5 年前、電子署名法などが当初目指していた IT 社会との齟齬はたくさんあると考えられる。こうしたことからも、IT 社会が健全に発展するために、大きな役割を果たすと考えられる電子署名の普及は大きな意味を持ち、普及という観点から電子署名法が見直されるべきである。ユビキタスネットワーク社会においては、認証を要するデバイスが人口よりもはるかに多く、またサーバによる署名が、人間が行うよりもはるかに多く想定される。このような将来社会に対する法制度は、はこれまでの法制度の延長上にある「電子署名法」などの枠組みだけではカバーできず、新たな枠組みも検討される必要があると考えられる。

4.2 課題設定の考え方

前節で述べたように、電子署名の普及はこれまでの技術的側面での発展段階から、その次に満たされるべき普及要件である、社会的側面での発展へと移行しつつある。

このような背景を踏まえつつ、2 章で抽出された電子署名普及の問題（2 章［図 2-3］参照）を下記の基準により主要問題へと絞込み、次節の重点課題へと導いた。

絞込みの基準

①根源的な問題点を抽出（問題点連関図の終端を中心に抽出）

②普及対象である民間の活動（ECOM など業界団体活動）で、自ら解決推進できる問題点を選択する

③展開を加速するため、早期に手を打てる問題点を選択する

表 4-1 電子署名普及の問題抽出（下線が全基準を満たす主要問題）

	①を満たした問題	②適	③適
1	**導入コストが大きいが、投資効果が見えず導入判断できない**	○	○
2	電子署名法は義務ではない	―	―
3	**電子署名法に基づく運用は厳格**	○	○
4	公的個人認証サービスの証明書は用途限定	―	―
5	電子署名法は自然人が対象で需要が限られる	―	―
6	受益者負担の仕組みになっていない	―	―
7	**PKI 利用の（システム化や導入の）ガイドラインがない**	○	○
8	API がベンダ依存	○	―
9	検証処理が面倒	―	―
10	相互認証等の標準化が不十分	○	―
11	失効や危殆化のリスクがある	―	―
12	IC カードは、R/W が高価で標準化も不十分	―	―
13	どの証明書/CA を信用してよいかの判断基準がない	○	―
14	汎用的な ID が無い	―	―

4.3 重点課題

前節にて抽出された電子署名普及の主要問題を改めて示す。

主要問題

①導入コストが大きいが、投資効果が見えず導入判断できない

②電子署名法に基づく運用は厳格

③PKI 利用の（システム化や導入の）ガイドラインがない

これらを解決するために、次の重点課題を提言する。

表 4-2 電子署名普及のための重点課題

	課題	課題解決のための検討事項例
1	電子署名の投資効果の視覚化	・社会的注目の高い分野への適用例と効果の試算 「構造計算書偽造」事件、企業統治の機運の高まりなどを背景にして文書の改ざん防止／真正性検証の重要性が認知されている分野について、利用モデルを挙げ、投資効果の試算例を示す。 特に、昨今国会で話題となったメール偽造疑惑など、電子押収物の証拠性も電子署名が直接的に解決する可能性があり、状況証拠を多数集めるコストより大幅な人的・金銭的・時間的コスト削減を見込めることなどを示す。 ・指標の検討 定量的に導入効果を推し量ることができる指標づくりを進める。 ・指標の分類、ランク付け 利用モデルと投資効果の試算から数値化・定量化された指標の分類・ランク付けを行う。 ・社会的コンセンサスの形成 社会で指標を広く共有できるように、作成した指標をたたき台に議論や認知を世間に広めてゆく。 ・国内外の PKI 認証などの標準化、規格化動向の加味、連携
2	三文判電子署名利用モデルの提案	・三文判に適した利用モデルとそのコミュニティ、ベストプラクティスなどの抽出 ・三文判の定義（保証レベルなど） ・三文判のリスクの抽出 ・三文判相当電子署名の適用基準 ・法的背景の解説（どの程度の信頼感が見込めそうかなど） ・国内外の PKI 認証などの標準化、規格化動向の加味、連携 ・ユーザも含めた議論の展開
3	電子署名（実印相当）導入ガイドラインの作成	・三文判との棲み分けの定義（普通電子署名＝実印？） ・通常電子署名に適した利用モデルとそのコミュニティ、ベストプラクティスなどの抽出 ・電子署名の適用基準の明確化 ・法的背景の解説（どの程度の信頼感が見込めそうかなど） ・国内外の PKI 認証などの標準化、規格化動向の加味、連携 ・ユーザも含めた議論の展開

重点課題各項の解説

１．電子署名の投資効果の視覚化

電子署名を利用するためには、認証基盤の整備または選定、運用基準の整備、対応ソフトウェアの整備など、大掛かりな投資（コスト）が必要になることが多い。

この投資は、電子化／電子保存化／インターネット化といった電子署名を利用しなければ従前は困難であったことを実現するような積極的な効果を狙うものか、既存のシステムやサービスの未来の事故・争議などのリスクを抑制する効果を狙うものかに分類できよう。

前者の場合、電子署名の適用によって初めて実現されたサービスがあったとして、電子署名がどのぐらいその実現に貢献したかを定量的に把握するには、数多あるその他のサービスの構成要素との関係を鑑みながら慎重に分析する必要があろう。

また後者はリスクの性質・規模・生起確率によって効果が左右されるため、投資対効果を確定しにくい性質もあると考えられる。

以上のように、考慮すべき要素の多さなどから電子署名の投資対効果についての指標化・視覚化のコンセンサス形成は進んでいない。指標化・視覚化が広く認知・信頼されるまでには、多くの議論と啓発のための時間が必要と思われる。

しかしながら、投資効果を視覚化できていないことが電子署名普及上の根源的で主要な問題点の一つであるため、ECOM 等の業界交流の場を活用して検討を進めて行きたい。

進め方の一例としては、PKI に基づく電子署名が効果的な利用モデル群を設定した上で、電子化／電子保存化／インターネット化のような積極的な効果を指標化するか、リスク抑制効果を指標化する。

前者では、電子署名が重要要素となるような利用モデルを想定し、そのモデルが実現することで得られる全体的効果を推計する。次に電子署名がそのモデルにおいてどれほど不可欠であったかをパラメータとして加味しながら、投資対効果を導出する。

リスク抑制効果の視覚化においては、まず電子署名未適用の利用モデル群に対して、想定リスクや被害を抽出し、社会的信用低下による損失や、金的損失の度合いといった評価項目を設定し、生起確率なども考慮してリスク分類とその強度のランク付けを行う。続いて、同様な分類・ランク付けを電子署名適用後の利用モデルで行い、適用前後を比較することで効果を指標化する。

こうして、コスト及び投資効果を定量化／数値化することによって、投資対効果（ROI 特に ROSI）を視覚化して行く。

視覚化に成功したならば、それが指標として社会的信頼を得られるよう、より広範なコミュニティでの議論や啓発活動へと拡大・発展させていく必要があろう。

2．三文判電子署名利用モデルの提案

既存の PKI を利用した電子署名は、日本の電子政府・自治体の申請手続きなどで扱われる電子文書などが代表するように、厳格で高度なセキュリティを与えることができる。厳格な認証局としては、電子署名法が定めている特定認証業務がある。

しかし、例えば高額でない取引の受発注書のやりとりや、ネットオークションでの取引の意志確認の履歴としての捺印など、それほど厳格でなくても良いが簡易で安価な署名ができればその方が適切というシーンもあるのではないだろうか。

現在のところ、既存の認証局によるいわば実印的電子署名の利用モデルと異なり、このような簡易で安価な PKI に基づく電子署名を活用したいという三文判電子署名利用モデルというものが確立されていない。

ニーズはあるが具体的にどうすれば三文判電子署名を利用できるのか、適用シーン・運用方法・注意点・法的背景・各種基準・導入手順・ベストプラクティスなどを掘り起こし、利用モデルを提案する。

この提案は電子署名の利用モデルの裾野を広げるための位置付けで、次の課題で示す「電子署名（実印相当）導入ガイドライン」と双子の構成を成す。

尚、こちらが「ガイドライン」ではなくその前段階である「利用モデルの提案」となっているのは、「三文判」に関する議論がガイドライン化へと落ち着くには、まだ多くの時間を要するであろうと判断したためである。

3．電子署名（実印相当）導入ガイドラインの作成

重点課題 2. の「三文判電子署名利用モデルの提案」に対し、こちらは実印相当の PKI に基づく電子署名に対するガイドラインを提案する。

このガイドラインでは、厳格な電子署名の本来の威力が十分に発揮できる利用モデル群とベストプラクティスを示すことで、電子署名の本質的な利用可能性をより啓発し、また厳格であるが故に容易でない導入を支援するためのものである。

付　　録

ネット通販、ネットオークションにおけるトラブル事例　　【別紙 1】

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
1	通信販売	ネット上で PC 用品を扱っているショップにて商品を注文し、入金した。入金の確認メールが来たので商品の到着を待っていたが、何の連絡も無しに納期が過ぎた。問い合わせをしたが、商品を発送する気は無いとし、その後 1 ヶ月以上も経った現在も商品の発送は無く、何の連絡も無い。ショップの主張では、注文した商品は「WLS」であったが、それはサイト上の表記ミスで、正しくは「WL」であったとのこと。そこで①注文のキャンセル、または②「WL」(現在未発売) を発送、若しくは③差額 (約 3 万円) を支払って「WLS」を引き渡す、のどれかにして欲しいとの事だった。ショップは契約成立を認めているが、「価格誤表示の時はキャンセルできるとサイトに謳っているのだからキャンセルできる」と一方的に言ってきた。しかしこれは価格誤表記ではなく商品の記載ミスであり、販売店が言ってきた商品はまだ未発売である。その点でも販売店は未発売商品を販売しようとしたことになるので、おかしなことだと思う。その後販売店からは完全に放置されている。こちらも冷静な判断が出来ていない可能性があるので、第三者からの助言が欲しい。	20,727	購入時	1)①	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する
2	通信販売	1 年以上前、指輪を注文し、指定口座に代金 31,000 円を振込んだが、未だに商品が届かない。その間、何回かメールで問い合わせをして、しばらく返答が来ていたが、半年前のメールを最後に連絡がなくなった。1 年以上経っているので、契約をキャンセルし、代金を返金してほしい。また、かなり時間が経っているが、当方が催促していれば、時効にかかることはないか。	31,000	購入時	1)①	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する
3	通信販売	妻が講習会に使用するためのノートパソコンを、講習会に間に合うよう、納期と価格について照会を行った後に注文、代金の振込みを行った。しかし納期を過ぎても届かず、問い合わせても販売店とは一切連絡が取れなくなってしまった。結局講習会には間に合わなかった。自分としては、まずは商品引渡しを希望しているが、出来ないようであれば返金して欲しい。	119,550	購入時	1)①	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する
4	通信販売	商品注文後、代金を振り込んだが、それ以降全く連絡がなく、質問のメールを送ったが、受信されずに戻ってきてしまった。本日、サイトを見ると無くなっていた。電話をしても誰も出ない。警察に連絡した方が良いだろうか	10,294	購入時	1)①	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する
5	通信販売	2 週間前、相手方の HP を見て、徳用コーヒーセット 50 回分を注文した。すぐに自動返信の注文確認メールが来たので、翌日、送料込みの代金 26,000 円を送金した。しかし、その後、商品が届かない。何度か電話をしたが誰も出ず、メールで問い合わせても返事がない。今後、1 週間以内に商品が届かない場合は契約を解除するので、送金済みの 26,000 円を全額返金してほしい。	26,000	購入時	1)①	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する
6	通信販売	約 1 ヵ月前、販売店のネットショップにてパソコンを注文、代金を振り込んだ。その後販売店より 2 回メールが来たが、途中経過の報告もなく、未だに商品が送られてこない。現状も全く連絡のない状態である。代金を先に振り込んでいるので、商品を一日も早く引き渡すか、でなければ返金をして欲しいが、既に注文した機種の上位機種が販売されて、型が古くなってしまっているので、販売店には早急に結論を出して欲しい。	157,290	購入時	1)①	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
7	通信販売	2ヶ月前に『納期4週間』という事で220,000円（税込231,000円）でノートパソコンを注文した。「メーカーに直接注文なので代金先払いのみで、代金を支払った順に商品を発送する」と言われ代金を振り込んだが、4週間経っても商品が届かない。遅れるという連絡も無かったのでメールで問い合わせたが連絡がなく、電話をしても誰も出ない。FAXを送ろうとしてもFAX番号は現在使われていないというアナウンスが流れている。サイト上のフォームを使ってメールを送ったら、「販売終了の為、商品の入荷が遅れていて入荷しない可能性もあるので、差額なしで次期モデルに替えます。またはキャンセル・返金処理をします」という回答があったので、すぐキャンセル・返金希望の旨を伝えたが、現在になっても返事がない。本当に返金してもらえるか不安で仕方無いので、何か返金してもらえる手段は無いだろうか。	231,000	購入時	1)①	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する
8	通信販売	代金振込み後、商品到着予定日になっても商品が到着しない為、電話をしたが繋がらなかった。ホームページには「移転の為休業」のお知らせが出て、その後連絡が無くなってしまった。暫らくしてホームページは「営業停止のお知らせ」に変更になり、「管財人を通して返金する」となっていたが、商品到着予定日から7ヶ月以上たった今も全く連絡が無い状態。3 ヶ月前に警察にも届けたが警察からも連絡がない。	469,581	購入時	1)②	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する
9	通信販売	データベース用のソフトウエアをメーカー（アメリカ）のサイト上からダウンロードして 1 ヶ月間試験的に使用し、気に入れば購入するというシステムがあった。購入を決め、国内で販売権を持つ販売店から、このデータベースソフトを購入した。届いた商品はソフトウエアが収録されているディスクと英語のマニュアルで、その後日本語版のディスクと日本語マニュアルが送られてきた。購入後にライセンスとパスワードの申請をすると、購入したソフトウエアを実際に使用出来るというものだったが、販売店から、「近々バージョンアップがあるので申請するのを待った方が良い」と言われ、数ヶ月後に改めて申請を行った。しかしその後、発行はおろか連絡もなく、こちらからメールや電話等で連絡しても返信は無く、電話も繋がらない。現在ソフトウエアは試用期間が過ぎて使うことが出来ない状態である。現在でもこの会社は営業を続けており、活動はしているようだが、代金の支払日は一昨年のことで、個人で購入したために証明するものを保管していない。振り込みを行った銀行で調べてもらえば分かるかもしないが、返金は可能だろうか。	290,000	購入後	1)②	代金入金後ライセンスが発行されず、支払い済みの証拠が銀行振込の記録かない。	代金振込み前に業者と購入したソフトウェアの使用条件等を電子署名された契約書などにより行っておく。

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
10	通信販売	コレクションしている人形を販売店のサイトより注文し、販売店より在庫がある旨連絡があった。そのわずか数時間後に届いた販売店発行のメールマガジンに、「1 万円以上注文した方には 2,000 円までの希望の商品をサービスする」との記載があった。そこで販売店に、今回自分も 1 万円以上注文したので該当させて欲しいと伝えたら、販売店が承諾してくれた。そこでサービスの人形の希望を「A と B のどちらか」と伝えたら、「A は来月発売なので B を注文商品と同時に送る」ということになった。代金を振り込み、商品が届いたが、一緒に入っていたのは B ではなく A だった。こちらは B を送ってもらうと思っていたので A を既に別の販売店で購入していた。販売店に「A を B と交換して欲しい」と伝えたところ、「B は既に完売していたので、A でも喜ぶと思い A を発送した。交換には応じられない」との返答だった。その後販売店から、「交換には応じるが、その際の送料は全額こちらが負担するように」と言われている。こちらが悪くないので納得できないが送料折半であれば応じようと思う。しかし販売店はあくまでこちらが全額負担との主張を変えない。こんな販売店の対応は許せない。	13,130	購入後	2)①	商品受領後、商品の説明と違うことが判明	購入時に販売する商品の内容や条件に電子署名を行い、販売者を本人確認する
11	通信販売	大放電 20C タイプとのことだったので注文したが、13C の放電をしたところ電池が破損してしまった。(20C とは流せる電流の大きさを表す数字で、具体的には 30 アンペアになる。ところが、実際に使用したところ 13C すなわち 20 アンペアで電池が破損した。）本来大放電出来ない電池なのに、それを偽って販売したことになるので、その旨販売店に伝えたところ、販売店より「破損していない未使用品のみ返品に応じる」との申し出があった。表示の制限値以内での正常使用で破損したものであるため、破損品も含め全品を返品したいと思っている。全額返金してもらうことは可能だろうか。	28,800	購入後	2)①	商品受領後、商品の説明と違うことが判明	購入時に販売する商品の内容や条件に電子署名を行い、販売者を本人確認する
12	通信販売	ネット通販で、イミテーションのブランドバッグを販売している業者からかばんを購入した。しかし、商品がこちらに届くと、イミテーションともいえないような、無名のかばんであった。その日の内に郵便局に連絡し、事情を説明し、返送するつもりだったが、代金引換だったので、支払った代金は現在、郵便局にて保留の状態になっている。郵便局側の返答は「販売事業者と消費者との直接交渉をして頂くしかありません」との事。こちら側からは、再度、ホームページに載っている携帯番号に連絡したが、現在は使用されていませんとのことで、連絡がつかない。クーリング・オフをしたいのだが、送り先の住所に返送すればいいのか、あるいはその他に対策があるのか、教えてもらいたい。	11,500	購入時	2)①	商品受領後、商品の説明と違うことが判明	購入時に販売する商品の内容や条件に電子署名を行い、販売者を本人確認する
13	通信販売	オランダ在住の日本人が経営するアンティークのネットショップでカップと受け皿のセットを注文した。「状態も大変よくワレ・カケ・キズのない商品。色の剥がれが少々」と商品説明が記載されていた。送料込みの代金 15,000 円を指定の銀行口座に振込んだ。数日後に届いた商品を確認したところ、カップと受け皿の色剥げが激しく、説明にはなかったキズがかなり付いていた。店にメールで事情を説明し、振り込み手数料を含む全額返金を申し出たが受け付けられないとの返事が来た。何通もメールを送り返金を要求した。相手方は、最終的に返品については同意したが、返金は「商品到着後」と主張し、振込み手数料も負担しないと言っている。	15,000	購入後	2)①	オークション時の商品説明と実際届いた商品とが異なっている。	代金振込み前に相手側の確認を電子署名された契約書などにより行っておく。

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
14	通信販売	幼虫 21,000 円、証明書 3 部 3,000 円、送料 1,000 円をメールにて申し込んだ。すぐに返信があり代金を振り込み、幼虫は 2～3 日で到着。証明書は 1 週間程度掛かると連絡があったが、その後証明書は届かず、メール・電話で連絡をとるが、留守電対応で連絡がとれない。相手は北海道で、こちら山口の為、対応に困っている。PC がウイルスにやられやり取りメールも破損してしまった。入金した証拠は残っている。あっせんして欲しい。警察にも被害届を出そうと思っている。	25,000	購入後	2)②	購入後商品が不足（幼虫の証明書が来ない）	代金振込み前に相手側の確認を電子署名された契約書などにより行っておく。
15	通信販売	相手方サイトの商品説明では「フィルターリングに補修跡があるが、フィルター装着に問題はない。光学部は大変クリアー。外観良品」とされており、50 年以上前のもので希少価値が高く、あまり市場に出回らない製品だったので、高価だったがローンを組んで購入した。ところが、届いた商品には、サイト上の画像や説明からは想像出来ないキズがあり、外観良品ではなかった。具体的には、レンズ上部のネジ部がブツブツザラザラしていて、フィルターを着ける際、ガタつきがあってしっかり止まらず、脱落するのではないかと不安になる。さらに、商品本体の中央部分に、横に走ったスジ状のものがあった。そこで、相手方に「返品希望」とメールで連絡した。相手方は「50 年を経過したクラシック中古品の性質上、ある程度の使用感、キズは避けられない。当店の保証は、撮影不能等本来の機能に関するものである。外観については、できるだけ忠実な描写に努めているが、通信販売では限界がある。当該商品は、レンズガラス部は大変クリアーで、ヘリコイド、絞りの状態も良好。レンズの命は外観ではない。したがって、サイトに記載してあるとおり、撮影不能等初期不良の場合を除いて、いかなる場合でも交換、返品には応じられない」という返答であった。そうであれば、当方としては返品・返金ではなく、フィルターリングをきれいに補修してほしい。補修が出来ないなら、それに見合った値引きをしてほしい。	60,000	購入後	2)②	購入後商品の傷発見	代金振込み前に相手側の確認を電子署名された契約書などにより行っておく。
16	通信販売	販売店のサイトより、車のパーツを数点注文した。しかし届いた商品のうちリアバンパーに小豆大の傷があり、メーカーに問い合わせたら、「商品を確認するためには販売店を通じてメーカーに商品を返送する必要がある」とのことだったので販売店に伝えた。販売店は「商品を確認するので送り返して欲しい」と言ったので返送した。しかしその後メーカーに聞いても届いていないとのことで、販売店に問い合わせたが話が進まなかった。そこで、ある掲示板に今回の経緯と、この販売店の URL を書き込んだところ、販売店より「法的措置を採る」との連絡があった。しかしそれほど悪い内容を書き込んだわけではなく、その後のメーカーとの話し合いで、「相談者からメーカーに直接送ってくれれば商品を確認して対処する」との回答が来ているので、商品を早く自分のところに返還してくれるか、メーカーに送って欲しい。	67,000	購入後	2)②	購入後商品の傷発見	代金振込み前に相手側の確認を電子署名された契約書などにより行っておく。

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
17	通信販売	通販で猿を購入。雌を指定したにも関わらず雄がきた。店長が間違いを認め、割引価格でもう 1 匹雌を追加購入したが、届いた猿は外見上雄に見えた。到着した日と約 2 ヶ月後に電話、メールで 2 度確認したが、間違いなく雌だと言われた。8 月に健康診断を兼ねて獣医に連れて行くと、2 頭共間違いなく雄だといわれた。店に電話し交換を要求すると、獣医の雄雌の鑑定書を送れば対処すると言われる。送付したところ「商品は希少動物であり、雌雄の判別が難しく獣医の判断も確実性に欠ける。雌雄を指定した場合当店でわかる範囲で判断している。交換に関して確実性を求めるなら、直接来店し自分の目で選択して欲しい。獣医の鑑定料は負担できない」と言われた。事業者は遠方なので来店することは不可能。雌だと断定して販売したのは事業者なのに、今さらこの様な事を言われても困る。この猿は雌の方が人気で、雄ばかりが売れ残る種であり、故意も感じる。獣医師によると生き物である以上、雌雄の判断は確実に出来るとのこと。何とか交換、もしくは返金して欲しい。金額にもよるが裁判になっても構わない。	106,050	購入後	2)②	購入後商品が違う事を発見（性別誤り）	代金振込み前に相手側の確認を電子署名された契約書などにより行っておく。
18	通信販売	1 ヶ月ほど前、画像編集ソフトをクレジット払いで購入した。商品到着後すぐにインストールを行ったところ、インストールの途中で読み出し不正が発生し、インストールが正常に終了しなかったので、CDROM の内容をハードディスクにコピーできるか確認した。すると、途中で CRC エラーが発生し、CDROM から読み出しができなかった。他の CD ドライブを使用しても同様であった。商品の DISK 面を確認したところ、うっすら擦り傷がついていたが、当方は傷つけていない。そこで、相手方 HP のサポートページに、その旨書き込んだところ、相手方に、当方の PC に不具合があると回答されたので、再度こちらの状況を説明したが返事がない。電話もつながらない。そこで先日、今回のいきさつを社長室宛てに封書で郵送したが、これにも返事がない。当方としては、①届いた当初から商品に傷があったので、返品・返金または交換に応じてもらいたい。②メールや郵便で数回質問をしているが、回答がない点について説明してほしい。	6,804	購入後	2)④	破損した商品のクレームに対応しない	代金振込み前に相手側の確認を電子署名された契約書などにより行っておく。
19	通信販売	2 ヶ月前、株式会社名にて、Fax でたまねぎ 10kg 入り 11 箱の注文があり発送したが、代金振込期限になっても振込がないため、電話及び Fax で数回にわたり振り込みを依頼したが、担当者が入院した等の理由を言われ振り込まれない。最近は電話がつながらないので内容証明郵便を送ったが、届けられていないようである。どうすれば支払ってもらえるか。	23,100	購入時	3)①	商品を送ったが入金されない	注文書に電子署名を行うことで、法的効力を担保出来るし、本人確認が出来る

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
20	通信販売	3 週間程前、「商品 1 点、ショッピングクレジットでの支払い希望」という内容の注文を受けた。2 日後に当社から、受注確認メールとして、①注文内容の確認と、②期日までにショッピングクレジットの申込み手続を取ること、③この受注確認メール送信後の注文キャンセルは受けていないこと等を記載したメールを、注文者に送信した。ところが、期日までにショッピングクレジットの申込みがなかったので、当社規定により、支払方法を「銀行振込み」に変更し、改めて設定した期日までに振込むよう、メールで注文者に伝えた。その際、当社の HP にも記載していることだが、①商品の発送は入金確認後になること、②支払期限までに振込みがない場合は、当社の規定により、支払い期日の翌日から完済の日まで年 15%（1 年を 365 日とする日割計算）の割合による遅延損害金を支払って頂くことになることを、重ねて伝えた。その後、配達証明付郵便でも請求書を送付したが、相手方不在のため戻ってきたので、普通郵便で再度請求書を送ったが、未だに支払いがない。商品代金と遅延損害金を支払ってほしい。	133,500	購入時	3)①	注文を受けたが入金がない	商品を発行していないようだが、注文書に電子署名を行うことで、法的効力を担保出来るし、本人確認が出来る
21	通信販売	ネット上にて通販を行っているが、商品到着後 1 週間以内に代金振込という約束で商品を届けたが、配達後 4 ヶ月以上経過した今も、代金が振り込まれない。今までにメール、配達記録付き郵便で合計 10 回以上の督促をし、電話で何度も督促をしているが、その都度、「忙しいから振込に行けない。」との返事があるだけである。忙しいなら、とクレジットカード決済を勧めても、そのときは了承するのだが、手続きは未だにしていない。代金を支払って欲しい。	3,517	購入時	3)①	商品を送ったが入金されない。	注文書に電子署名を行うことで、法的効力を担保出来るし、本人確認が出来る
22	通信販売	CD と DVD を 1 枚ずつ購入したところ、送料を 2,000 円も請求された。商品のサイズから考えても 1,050 円程度のはずなので理由を質問したところ、「特価商品なので 1 台につき 1 件分の送料を頂いている。送料ポイント制だが、今回のような送料になる場合もある」という返答が来た。しかし特価商品ではなかったし、「1 台につき 1 件分」「ポイント制」の意味が分からない。商品ページや購入手続ページにも、そうした説明はない。特定商取引法に違反しているのではないか。	6,888	購入後	3)③	送料トラブル（Web 上の説明と違う）	（Web への掲載内容に誤解がある場合には、電子署名での対応は困難。内容を改ざんされないように説明内容を電子公証の仕掛けで保管することは有効）

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
23	通信販売	相手方 HP に、「同一発売日の商品の送料は 1 回分」「1 配送先につき、合計 1 万円以上注文の場合、送料は 0 円」と記載されていたので、発売予定日が同一の商品 5 点（税込総額 14,175 円）を注文した。注文確認メールも送料 0 円となっていた。後日、相手方から「注文商品のうち 2 点を代金引換郵便にて発送した。」というメールが来たので、届いた商品と引換えに指定された額を支払ったが、後になって、その金額には送料 1,050 円が追加されていたことに気がついた。そこで、相手方と交渉を始め、当方は、①同一発売日で、かつ高額購入なので送料は無料のはず。②確認メールでも送料 0 円とされている。③勝手に分納され、送料を追加された、と主張した。これに対し、相手方は、①発売日は度々変更され、実際の発売日は分からない。②実際の発売日が異なる場合は、商品入荷次第発送している、などと主張し、交渉は決裂した。当初の契約金額を超えない前提で残り 3 点の送付を希望するが、発売延期になった商品が 1 点あるようなので、これを相手方都合によるキャンセルとして、残る 2 点のみでもよい。但し、その際支払う金額は、当初の契約金額から、支払済金額とキャンセル分を差し引いた残額（運送費・代引料を含む）とすべき。なお、他の消費者にも注意喚起したいと思い、この問題に関する HP を作成してアップし、削除不可の掲示板にも書き込みをした。	14,175	購入後	3)③	送料トラブル（Web 上の説明と違う）	（Web への掲載内容に誤解がある場合には、電子署名での対応は困難。内容を改ざんされないように説明内容を電子公証の仕掛けで保管することは有効）
24	通信販売	商品を 2 つ注文したが、販売店の通販規約には、複数の商品を注文の際には、納期表示の遅いものにあわせて他商品の出荷手配をするので、原則として納期の早いものからの出荷はしないとの記載があるにもかかわらず、納期の早いものから先に出荷をされてしまった。そうなると、代引きの場合、1 つしか届いていなくても 2 つ分の代金を請求されてしまう。そこで販売店に問い合わせたところ、この規約にある記載内容を一切認めようとしなかった。1 つが納品された時点で 2 つ分の代金を代引きにて請求されたので受取拒否したら、「キャンセルの際はキャンセル料・再配達料（納期の遅い方に再度合わせて）等がかかる」旨のメールが届いた。納得出来ない。	25,389	購入後	3)③	送料トラブル（Web 上の説明と違う）	（Web への掲載内容に誤解がある場合には、電子署名での対応は困難。内容を改ざんされないように説明内容を電子公証の仕掛けで保管することは有効）

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
25	通信販売	薬を扱うサイトにてカード決済をしたところ、思っていたよりも金額が 5,000 円弱多かったので詳細を見てみると、ID 発行代（有効期間内は簡単に購入できるシステムらしい）が含まれていた。しかし注文後の確認画面には含まれていなかった。購入先に電話で問い合わせをしたところ「注文する際に、クリックしてはずさないとこの代金が請求される」また「注文後の確認画面ではクリックしてはずした前提で表示される」「取り消しはできない」「それらは画面で表示されている」とのことだった。また半年前に一度注文した時にはかからなかったのでおかしいと思ったが「システムが変わった」との回答だった。確かにきちんと全てを読まなかったことがこちらの落ち度であることは認めるが、こういうシステムは商品以外で余分に儲けようとしているように思える。しかしおおごとにはしたくないのと、相手とかかわりたくないとも思っている。	4,725	購入時	3)③	余計な請求（認識していない追加の請求が来た）	購入時に電子署名で販売者を本人確認し、クレーム先を明確にする
26	通信販売	商品の注文時、HP に「送料一律 980 円」と表示されていた。注文確認メールには「商品代金 7,300 円、消費税 365 円、送料別途、総額 7,665 円」送料を通知する次のメールでは「商品代金 7,300 円、送料 980 円、消費税 414 円、合計金額 8,694 円」となっていたが、送料の分も消費税が加算されていることに気がつかず、最初のメールの総額 7,665 円に送料 980 円を足した 8,645 円を郵便振替で振込んでしまった。すると後日、49 円足りないとの請求メールが来た。しかし、49 円のために郵便局の振込手数料 130 円をかけるのがくやしかったので、「送料の表示と消費税のかけ方がおかしい」と抗議し、キャンセルを申し入れたところ、キャンセルには応じるが、返金の際、振込手数料を差し引くと言われた。当方は、送料の説明不足についての謝罪と、振込金額全額の返金を希望する。	7,300	購入時	3)③	税金の取り扱いがはっきりしない	（Web への掲載内容に誤解がある場合には、電子署名での対応は困難）
27	通信販売	2 ヶ月前、販売店のサイト上より上記商品を 68,100 円（税抜き）で注文したところ、「商品入荷次第発送します。」ということだったので、待っていた。その後納入予定が 2 ヶ月先に延期されたが、その期日直前に商品の納入が困難であるとの理由で、販売店側から一方的に注文をキャンセルされた。販売店に対し抗議したところ、「商品の納入状況によっては、キャンセルすることもある。なお、現在は商品は納品され在庫があるので、再度注文すれば配送することができる。しかし、価格は現在の売価（94,300 円）で販売することになる」とメールが届いた。しかし商品の納入状況によってはキャンセルになる、というのは、一方的な不当条項と思われるし、納品予定であったのにそれ以前にキャンセルされているので納得できない。商品が入荷されているので、こちらは 68,100 円で商品を購入したい。要求は可能だろうか。	68,100	購入時	3)③	販売者が価格を変更	購入時に販売する商品の内容や条件に電子署名を行い、販売者を本人確認する
28	通信販売	1 度の注文に対して、3 度にわたりクレジットカード会社に対して支払請求がされていたことが判明した。販売元はシステムトラブルを理由としているが、ネット上での信用取引において、著しく信頼性を欠くものである。今後このような事を起こさないために、当業者のトラブル対応方針についてのディスクロージャーと迅速な障害対応、改善処置・是正処置を促すことを希望する。ネット取引の信頼性確保のために、このようなトラブルを公表し監視していく必要があると考える。	3,192	購入後	3)④	重複課金	（重複課金に対して電子署名での対応は困難。一回引き落としたら、2 回以上は引き落とせない仕掛けが必要）

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
29	掲示板を介した取引	カードゲームのサイトの金銭トレード掲示板で、カードを安く売ってくれるという人がいたのでメールした。何回かメールでやり取りをした後、先に自分が指定の銀行に振込み、相手方が確認後、配達記録で送ってもらうという事になった。代金着払いを希望していたが、相手方が以前いやな思いをしたとのことで配達記録になった。そこで代金 10,200 円を指定の口座に振込んだが、振込み後メールや電話をしても一切返事が無い。銀行に元払いの手続きを取ったが未だに連絡がないので恐らく断られたと思う。104 にて確認したが、登録されていなかった。また、このカードゲームサイトの掲示板をみたら、同じ口座と名前で被害にあっているという書き込みがあった。どうしたらよいだろうか。	10,200	購入時	1)①	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に電子署名で本人確認する
30	サービス	ネット上で見つけた外車専用のパーツ店より、稀少な自動車部品（トランスミッションとデフレンシャルギア）のオーバーホールを依頼して、トランスミッション分 15 万円、デフ分 13 万円を入金したのだが、デフは修理不能と言われた。あと 15 万かかると言われたのでキャンセルすると伝えたところ、こちらから業者のところに行けば、返金とともにミッションも引き渡すと言われた。そこで納得いかない旨メールをすると、返金するということだったので口座番号を知らせたが入金が無い。修理不能と言われた部品（デフ）と修理代金 13 万を返して欲しい。	280,000	購入後	2)⑤	修理不能な部品（希少品）とその修理代金の返却。	修理の依頼の場合、あらかじめ修理不能となった場合の取り扱いについて記載された契約書を電子署名付きの電子データでもらい、確認しておく。
31	サービス	以前、大リーグで活躍中の日本人選手のサインボールをオークションで購入したので、そのボールを鑑定したいと思い、インターネットで相手方のサイトを見つけた。入会前に、鑑定方法や鑑定してもらいたい品物について確認したところ、相手方のサイトに入会すると、アメリカの権威ある鑑定会社に鑑定依頼する書類を無料で作成してくれるという特典があると説明されたので、3 ヶ月前に、会員登録と入会手続をした。そして、会費 3,500 円を振込み、サインボールなど 3 点の鑑定依頼書類作成を依頼したが、その後、何度催促しても書類が届かない。メールを出しても返事がない。鑑定依頼書類を作成できないのなら、入会を取消し、年会費を返還してほしい。	3,500	購入時	2)⑤	会費を入金したが鑑定のサービスが受けられない	代金振込み前に業者側の確認を電子署名された契約書などにより行っておく。
32	サービス	以前、相手方から購入したブランド物の腕時計を、相手方に買い取ってもらおうと当方から連絡し、150 万円で買い取ってもらうことになった。品物を相手方に送り、1 週間前が買取り代金の振込み期日だったが、振込まれなかった。相手方からは「営業困難な状態になったので、2～3 日遅れで一部支払いし、残金は支払いできる時点でお知らせします」とメールが届いたが、電話で連絡も取れず、メールを出しても返事が来ない。本日 10 万円だけ振込みがあったが、残金 140 万円を早く支払ってほしい。	1,500,000	購入時	3)①	商品を送ったが代金が届かず。商品送付前の相手方の財務状況（支払可能か否か）の確認がなされていない。	支払側が事業者でかつ高額取引の場合、契約前に財務状況を電子署名付きの電子データでもらい、チェックする。

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
33	サービス	1ヵ月半ほど前、姓名判断による人生相談のHPを見て、アドバイスをもらいたいと思い、相手方に電話をかけた。鑑定結果は3～4日で出ること、家族全員関係があるとのことだったので、家族4人分の鑑定を依頼した。4人分20,000円（1人5,000円）を指定口座に振込み、鑑定結果を待っていたが連絡がない。2週間後、相手方に電話したところ、「まだ出来ていない、やめるなら返金する」と言われたので、キャンセルし、当方の返金用口座番号を伝えた。後日、通帳を確認したろ、15,000円しか入金されておらず、5,000円不足していたので、相手方に連絡したら、「解約手数諸費用を差し引いて送った」と言われた。しかし、解約手数料などについては、事前に説明はなかったし、HPにも記載はない。5,000円を返金してほしい。少額訴訟も考えている。	20,000	購入時	3)③	代金入金済みなのに、サービスが提供されない。サービス側の申し出で解約したのに、解約手数料を取られた。	解約を決定する前に返金額を電子署名付きの電子データでもらい、確認する。
34	オークション外取引	オークション出品画面に「在庫確認をしてください」と表示があった為、質問欄から在庫の確認をした。その後、相手方より受注仕入れ専門の会社であることの説明などと共に、商品代金と、「申し込み意思の有無については本書到達後3日以内に返送ください」と書かれたメールが届いた。そこには、「商品入荷の見込みがつかない場合には預かり金を返金する、振込みから50日経過しても商品が入手できない場合には、預かり金と2%の違約金を加えて返済する」と書かれており、「商品発送の優先順位は、振込み確認順」とあった。その日に申し込みをし、送金した。その後、相手方より「入荷がない」と何度かメールが届き、50日過ぎても入荷の気配がない為、キャンセルを申し出た。相手方から、「キャンセルを受け付けたので預かり金を振り込んだ」とのメールが届いたが、返金はなかった。その後催促をしても、「手違いにより振込み手続き終了したら連絡する」といった返答のみで返金がない。商品代金と約束の違約金2%を加算した金額の振込み日を明確にし、至急返金して欲しい。	154,800	購入時	1)①	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する
35	オークション外取引	次点落札となりオークションシステムでは拒否したが、出品者からメールで取引が持ちかけられ応じた。国際送金し、出品者は受領後、メールで品物の発送を連絡してきたが、商品は届かず、その後の連絡も途絶えてしまった。返金を希望する。もし、出品者からの返金が叶わない場合、オークションサイトによる補償を希望するが、海外との取引ということから、補償外になるらしい。その点に疑問がある。サイト運営者は、海外取引であってもユーザーから手数料を取っている。また、出品者に、サイトから私のIDと同時にメールアドレスが連絡されているはずだが、出品者の情報は教えてもらえない。サイト運営者に補償をさせることができないか。	459,049	購入時	1)①	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
36	オークション運営サービス	先日、オークションに入札したところ当方は次点となったが、1週間後、オークションサイトから「落札者候補となった」という連絡が来た。そして、購入するなら「Y」、断る場合は「N」をクリックするようにとのことだったが、「N」を選ぶと、当方に「どちらでもない」との評価が付されるようである。質問は、①この落札者候補の連絡を受け、「Y」で購入意思を表示した時点で、契約が成立すると考えるがどうか。②このサイトの評価は5段階で、「どちらでもない」は3番目だが、実質的にマイナス評価といえると思う。しかも、評価は一生涯 Web 画面から消えず、芳しくない評価は出品者からの「入札者制限」に抵触し、以後の入札に支障を来たす。「N」を選んだ場合にマイナス評価がつくのはおかしい。救済措置があってしかるべきだと思うがどうか。なお、今回の問題について、経済産業省、総務省などに相談したところ、現在、国内のネットオークションに関する「機関」は電子商取引推進協議会のみであると聞いたので、消費者サイドの「苦情・要望」について、客観的意見や業界としてのガイドライン等を教示してもらいたい。オークションサイトにも質問のメールを送り、しかるべき回答をもらってから意思表示を行うと伝えてあり、まだ「Y」「N」の選択はしていない。		購入前	4)①	オークション評価が下がる不安	（オークションサイトの評価システムの機能そのものであり、電子署名での対応は困難）
37	オークションサイト運営サービス	オークションに新品未開封のゲームを出品して、入札価格も高額になり、あと 2 日で終了というときに、いきなり出品を削除された。再出品したが、前回ほど価格が上がるとは思えず、憤慨している。オークションサイトに、削除された理由について質問しても定型文の回答しかもらえない。他に同じゲームを出品している人は削除されていないのに、なぜ私の出品だけが削除されたのか、理由が知りたい。		購入前	4)②	オークションで出品物削除	（オークションサイトの運営に関わる事象であり、電子署名での対応は困難）
38	オークション	友人の ID を利用し商品を落札後、出品者の指定口座に振り込んだが、出品者より連絡がなく商品も届いていない。メールで催促したが返事がなく、連絡先として明記されていた携帯電話に電話をしても通じない。また、番号案内で照会しても名義人での登録はないとのこと、これから先、どのようにするのが一番良いのか教えて欲しい。	148,000	購入時	1)①	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する
39	オークション	オークションで商品を落札し、代金を支払った。その後相手方から「トラブル（自宅の火事）が発生したので、来年 1 月末までに全額返金する」と E メールで連絡があった。しかし、折り返し相手方に E メールや電話で連絡をとっても回答がない。その後、相手方から、返済予定として分割で返金する旨連絡が届いた。自分の希望は、返金よりもまず落札品を今年中に送付してもらうことである。もしできない場合は全額返金を求め、法的手段に訴えたいと思うが、具体的にはどうしたらよいのか。	56,000	購入時	1)②	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
40	オークション	約半年前、知人に依頼され、オークションにてノートパソコンを落札した。代金を振り込み、約 1 週間で届くというので到着を待っていたが、一向に届かなかった。催促のメールを送ると発送が遅れているとのことだった。しかし、翌月になっても届かなかったので、その後も何度か催促のメールを入れたが「しばらく待て」という内容しか返ってこなかった。電話をかけても、最初は繋がっていたがだんだん繋がらなくなっていった。やっと来たメールの回答に、「商品発送が難しいため返金したいので、返金先を教えて欲しい」とあったので、口座名を明記し、何時返金するのかを販売店に尋ねた。返答には期日が記載されていたが、一向に返金されていない。その後弁護士がついたようだったが、その弁護士も辞任し、新しい弁護士を探しているとのこと。未だに返金されず、連絡をとっても「返す」と繰り返すばかりで一向に返す気配がない。少額裁判は販売店が離れているので無理と思う。こういった場合どうしたらよいだろうか。	116,400	購入時	1)②	代金を送ったが商品が届かず販売者と連絡と取れない	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する
41	オークション	1 ヶ月ほど前、オークションで商品を落札し、代金を銀行振込みで支払ったところ、「入金確認後 2 週間以内に配送する」との連絡があったが、商品が送られて来ない。相手方の電話にかけても出ず、メールを送信しても返事がない。そこで、同様の被害に遭った人が作った掲示板から、相手方の住所を入手し、内容証明郵便を送付した。その後、相手方から「トラブルに巻き込まれ、返金の目処が立たないので返金処理はしばらく待って欲しい」と連絡があったが、信用できないため、迅速な返金処理を求めたところ、「事実上の倒産に追い込まれ、返金のあてがない」というメールが送られてきた。その後はメールを出しても返事がなかったが、3 日前、「会社が倒産に追い込まれた。迷惑を掛けてしまい申し訳ない」との内容の手紙が届いた。差出人の住所はなかった。相手方の電話も解約され、全く連絡が取れない。警察には被害届を提出済みである。質問は、①相手方自身は所在不明だが、その母親とは連絡がつく。母親に返金を求めるのは違法か。②少額訴訟を行おうと思うが、手続費用を合算して請求してもよいか。③同様の被害に遭っている人が多数いるが、被害者が協力して 1 つの少額訴訟として手続きを行うことはできるか。	37,425	購入時	1)③	代金を送ったが商品が届かず販売者が倒産して返金に応じられない（詐欺的行為）	購入時に業者の住所を確認できる電子署名を注文請書に付与する等の方法で確認する
42	オークション	2 ヶ月前、アメリカのオークションサイトでブランド物のバッグを落札し、商品代金 1,000 ドルと送料 50 ドルを外国送金為替で支払った。1 ヵ月後、商品が届いたが、オークションの商品説明とは異なるものだった。具体的には、①大きさは 30 センチのはずが、50 センチ程もあった。②ファスナーが壊れており、ダストカバー、キー、ロック、ケアブックなど付属品は一切なかった。③本来デコボコしているはずの表面がツルツルで、持ち手部分は明らかにビニールであった。④布も前後で違うビニールで、内側の布が写真と全く異なっていた。そして、⑤一番大事な製造番号が一切なかったので、偽物だと思い、相手方に、商品の返品と、商品代金と送料、為替手数料、関税の返金を求めたが、全く返事がない。また、オークションの相手方の評価欄を見ると、他にもたくさん詐欺的な出品をしているようで、このような出品者をこのままにしておきたくない。	1050 ドル	購入後	2)②	オークション時の商品説明と実際届いた商品とが異なっている。（商品に傷など）	代金振込み前に相手側の確認を電子署名された契約書などにより行っておく。

	取引形態	相談内容	金額	フェーズ	トラブル類型	トラブル内容	考えられる電子署名による対策
43	オークション	2ヶ月前、オークションでブランド物のキャリーケースを落札した。オークションの説明では、「完全新品未使用で、本体に多少目立たない傷がある程度」とされていたが、実際に届いた商品は、汚れがひどく金具部分は腐食し、一部部品が取れており、とても新品とは思えないものだった。オークション時の説明と異なっているので、返品・返金をメールで要請したが、返答がない。	12,500	購入後	2)②	オークション時の商品説明と実際届いた商品とが異なっている。	代金振込み前に相手側の確認を電子署名された契約書などにより行っておく。
44	オークション	デジタルカメラを出品した。落札されたので、商品を送付したら、落札者よりメールで、「電池を入れても電源が入らない」とのクレームがあった。こちらでは外部電源で撮影し、メモリーをフォーマットした状態で出品していたが、「不具合があれば返品には応じる」と伝えた。その時、「出品手数料・落札手数料はそのままこちらが負担するので、返送料金はご負担ください」と言ったところ、落札者より、「もともと使えない商品を出品していたそっちが悪いのに、なぜ返送料をこちらが負担しなければならないのか、また手数料等はそっちが負担して当たり前」と言われた。返送料を自分が持てば評価は悪くしないとのことだった。落札者より携帯のメールに連絡をくれるよう言われていたので、そのメールアドレスに、「全てこちらが負担します」と伝えたが、文字制限に引っかかったらしく空白メールだと非難され、その後引っかからないよう再度伝えた。その後は、返金が先か、返品が先かでもめている。どうしたらよいだろうか。	1,200	購入後	2)② 3)③	オークション時の商品説明と実際届いた商品とが異なっている（と言われた)。	代金振込み前に相手側の確認を電子署名された契約書などにより行っておく。
45	オークション	入札前に、オークションの質問欄から送料の質問をしたが返答がなかったので、記載の番号に電話をかけた。返答内容には、出品者が負担すべき落札システム使用料を落札者に負担させる等、納得できない点もあったが、商品を気に入ったので入札し、落札した。代金を振込んだ翌日、いつ頃商品が届くのか問い合わせの電話をしたところ、相手方に「何度も電話をかけるのは非常識。メールで聞いてほしい」「キャンセルで結構です」と言われたので、当方もキャンセルを了解した。その後、返金されたが、金額が 17,580 円であった。当方は、商品代金 18,000 円、落札システム手数料 540 円、振込手数料 420 円の合計 18,960 円を負担したので、差額の 1,380 円を返金してほしい。	18,540	購入時	3)②	商品が届く前のキャンセル。	落札前に落札後の条件を電子署名つきの電子データでもらっておく。

メンバーリスト

事務局

前田　陽二	次世代電子商取引推進協議会	主席研究員

顧問

大山　永昭	東京工業大学
菅　　知之	関西大学
平田　健治	大阪大学　大学院

リーダ

佐伯　正夫	三菱電機株式会社
千葉　昌幸	株式会社三菱総合研究所
松本　　泰	セコム株式会社

編集メンバ（上記リーダ以外）

氏名	所属
高塚　　肇	NTT コミュニケーションズ株式会社
出本　　浩	株式会社エヌ・ティ・ティ・データ
榎本　　尚	花王インフォネットワーク株式会社
長島　健一	大日本印刷株式会社
伊藤　正剛	株式会社帝国データバンク
祝　　壮吉	東京電力株式会社
政本　廣志	日本電信電話株式会社
牧　　徳達	みずほ情報総研株式会社
坂上　　勉	三菱電機株式会社
沢田　登志子	電子商取引推進協議会（ECOM）

メンバ（上記以外）

氏名	所属
江幡　　太	株式会社インターネットイニシアティブ
林　　良一	NTT コミュニケーションズ株式会社
中林　武文	NTT コミュニケーションズ株式会社
森岡　竜司	株式会社小松製作所
浜田　　誓	電気事業連合会
小郷　育弘	東芝ソリューション株式会社
後藤　真一	社団法人日本鉄鋼連盟
寺田　　透	富士通株式会社
日向　一人	富士電機ホールディングス株式会社
競　　康諮	株式会社 UFJ 銀行

電子署名普及に向けた調査検討報告書

平成 18 年 3 月発行

発　行　　次世代電子商取引推進協議会

販　売　　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園三丁目 5 番 8 号
機械振興会館　3 階
TEL：03(3436)7500

この資料は再生紙を使用しています。