H８－WG１５

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

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

1 はじめに

電子公証検討ＷＧは商取引における取引当事者の私的自治を最大限尊重するとの基本的考え方に則り「公的機関あるいは取引当事者以外の第三者機関による電子公証ニーズにとどまらず、広くオープン・ネットワーク上での商取引における安全性・信頼性確保のためのガイドライン作成」という目的を達成するため、電子公証の目的、海外の関連動向、企業間の取引や企業内業務での実ビジネス上での電子公証に対するニーズや電子公証を実現するのに必要な基本的な機能について検討した。

今後、電子公証技術及び電子公証システム、法的課題、電子公証システム運用の在り方について調査・研究を行うとともに今までの検討を深度化する。

これらの成果は電子公証システムガイドラインとして取り纏めるものである。

本報告書では、電子公証システムガイドライン作成に向け検討のベースとなる電子公証のニーズと対応案を中心に中間報告するものである。

尚、幅広いニーズを把握するよう心がけたが、それでも限られたモデルにおける検討であることを留意頂きたい。また、本内容は今後の検討で更新、差替えが行われるものであり、参照用資料として使用する以外にこれらを引用することは適切でない。

本内容に対する質問は oride@ecom.or.jp までお願いする。

2 用語の定義

本報告書では次のように定義する。

1. オープンＥＤＩ
   オープンなネットワークでのＥＤＩであり、インターネットの利用も１つの形態である。
2. クローズドＥＤＩ
   クローズドなネットワークの従来型ＥＤＩであり、一般にＶＡＮを利用して行われている。
3. インターネットＥＤＩ
   インターネットを利用したＥＤＩである。
4. 物財
   動産、形のあるもの、引き渡し（物流）が必要なもの。
5. 情報財
   サービス（委託調査、ソフトウエア等で成果物をデジタル情報としてネットワークで提供できるもの。
6. 標準品
   カタログ商品、継続的な取引のおいて注文番号でお互いに認識できる商品。
7. 開発品
   仕様が供給企業から標準的に提示されるものではなく，購入企業から提示されるもので，一部あるいは全部の開発を伴う特注品、ユーザーソフト、委託研究開発を伴うもの。

8. 生産財
   生産のために使われる財、原料・労働・機械設備など。
9. 消費財
   個人的欲望を満たすために直接消費する財。

3 電子公証概論

3.1 電子公証の必要性

オープンなネットワーク上での電子商取引は何時でも、何処からでも、グローバルな領域の取引の実現、さらにランニングコストの低減、取引機会の拡大等の大きなメリットの可能性を秘めている反面、様々な脅威が存在する。

自然災害とかネットワーク障害、ハード、ソフト障害により取引情報が消滅する場合は別として悪意の第三者、悪意及び善意の取引当事者に起因して、一般に言われる盗聴、詐称、改竄や否認や錯誤等により正常な取引が成立せず、金銭的損害の発生や企業の信用度低下に対する不安があるようでは健全な企業間取引は望めない。

これらの脅威や不安に対してはまず技術的に解決を図ることが大切である。しかし、技術面だけでは解決が困難な脅威や不安に社会システムとしてどのような仕組みで安全と信頼性を確保するのかは重要な課題である。

そのため、取引モデルの具体的な業務フローを材料に課題や電子公証ニーズを調査し、技術面、運用面、制度面の総合的な解決の仕組みを検討する。

3.2 電子公証の目的

電子公証の検討をするにあたり、電子公証の目的を次のように仮に設定する。

「ネットワーク上の商取引等における電子的交流の安全・信頼性を確保すること」

（電子的交流：電子メール、電子マネー、電子決済、電子商取引上の契約、電子保存等）

例えば、電子商取引においては、取引当事者が安心して利用できるように第三者に取引に係わる電子文書の真正性（契約の存在や取引の内容等）を証明すること。（図 3-1 電子公証の目的を参照）

人間の経済的、社会的活動には、常にリスクが伴うが、このリスクには、人的リスク、経済的リスク、自然に対するリスクなどがある。

リスクとは、単に被害の発生確率ではなく、被害規模を考慮したものであり、リスク＝Σ（被害ｉの被害規模×被害ｉの発生確率）と言われる。

電子公証の実現には電子情報のやり取りにおけるリスクを如何に効率的に経済的に最小限に押さえるかが重要な課題といえる。

3.3 電子公証と認証について

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。

これに対して、電子公証は、認証というインフラの上で様々なアプリケーション（電子商取引、電子申請等）をする場合の安全・信頼性確保をすることである。

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。

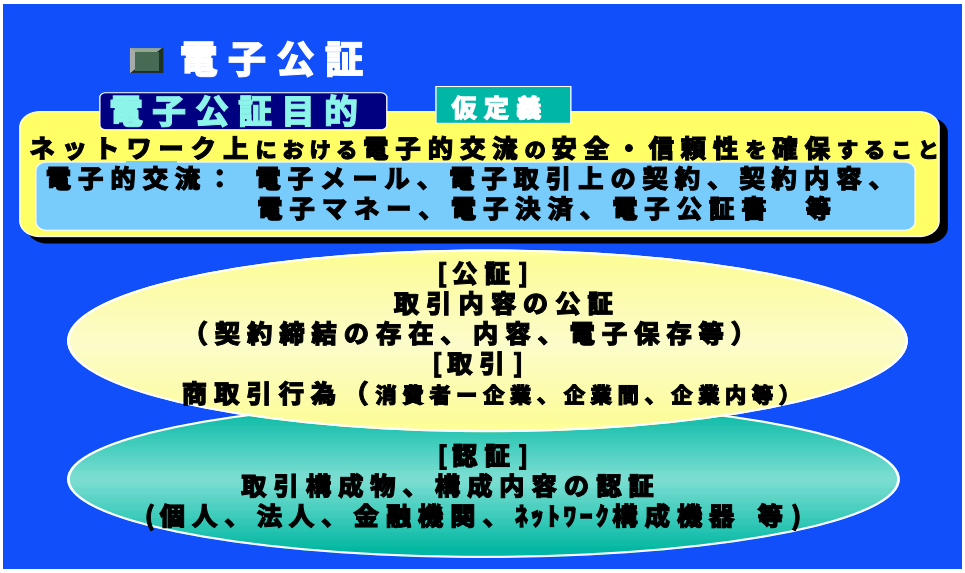


図 3-1電子公証の目的

4 オープンＥＤＩの検討の視点

4.1 企業間取引における視点

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。

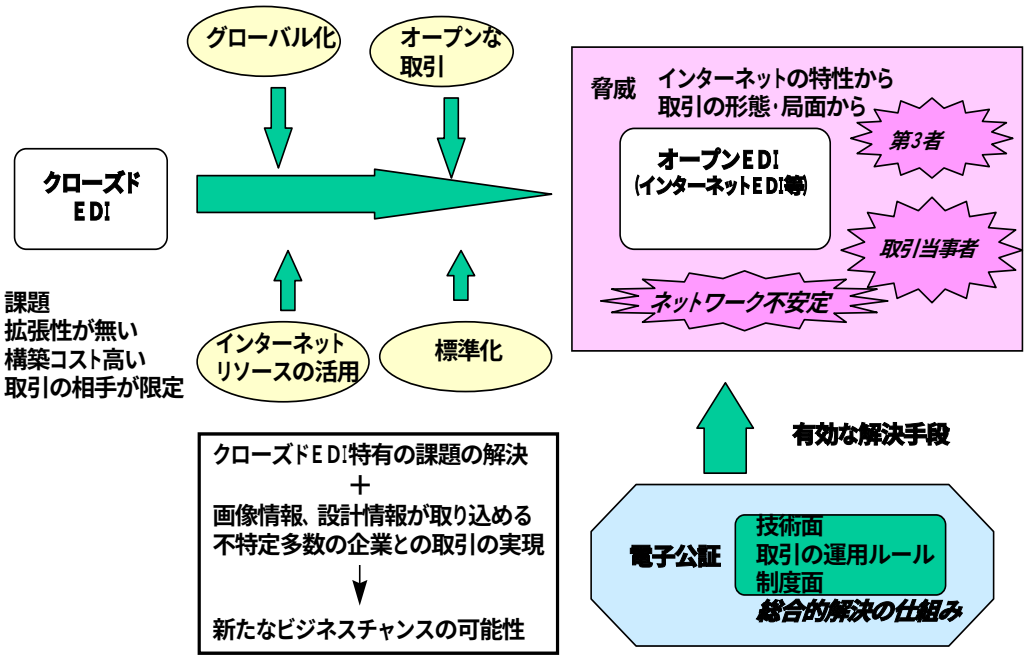


図 4-1オープンＥＤＩ化と電子公証

さらに、オープンＥＤＩ（インターネットＥＤＩ等）は、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、特にオープンなネットワークの特性からの、グローバルな不特定多数企業間を対象にした継続取引や継続取引を前提としない１回限りの取引の実現の可能性を秘め、経営基盤の強化や新たなビジネスチャンスとなり得ることも有り、オープンＥＤＩ実現環境整備は重要である。

以下に米国におけるインターネットＥＤＩの動向を記載する。
これらは、従来型のクローズドＥＤＩにインターネットを利用したものであるが、今後不特定多数企業を対象とした募集段階～基本契約段階における応用や継続取引を前提としない１回限りの取引への取り組みが進展するものと思われる。

参考＜米国のインターネットＥＤＩの動向＞

「インターネットＥＤＩ」は、まだ米国でもサービスが開始されたばかりであり、その成否については未知数であるが、オープン・ネットワーク上でのＥＤＩサービス提供者としての運用実体を見る上で非常に参考になると考える。「インターネットＥＤＩ」にはいくつかの形態があり、ただ単純に、通信回線にインターネットを利用したものから、「 GE Tradeweb 」のようにＥＤＩのサービスエンジンをWWWで開発し、運用サービスを提供しようというものまで様々である。

分類としては、以下が一般的である。

①電子メール型：

電子メールにＥＤＩフォーマットなどのファイルを添付して送る。この際、添付ファイルは暗号化される。代表的な製品としてはプレメノス社の TEMPLAR があり、これを採用した事例として昨年９月にサービス開始した Kleinschmidt（ＶＡＮ）が属すると思われる。

②エクストラネット型：

エクストラネット（Extranet）では、インターネットを、暗号化技術などを活用して、プライベートな通信ネットワークであるかのごとく利用する。代表的な製品としては、サン・マイクロシステムズ社の SunScreen や Tradewave 社の TradeＶＰＩが属すると思われる。

③アクセス経路型：

既存のＶＡＮ会社などが運営するＥＤＩへのユーザーのアクセス経路としてインターネットを利用するものである。代表的な製品としてはＧＥインフォメーシ ョン・システムズ社の TradeWeb が属すると思われ、すでに１９９６年６月から実施されている。

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。

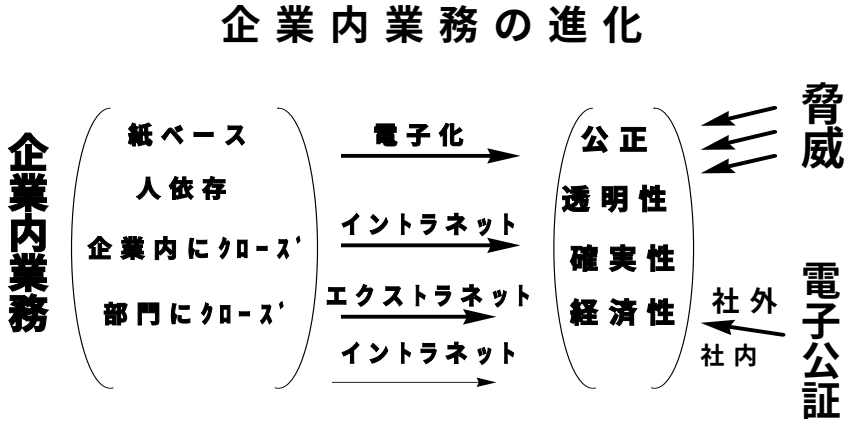


図 4-2企業内業務の進化

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。

5 電子公証のニーズ調査

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、管理情報等）
- 電子申請・届出
- 電子調達（行政）
- 電子保存

などが考えられる。

本報告書では、企業―企業間の電子商取引、企業内業務を対象に検討している。

前者の企業―企業間の取引には継続的取引と継続的取引を前提としない取引がある。（図5-1 取引形態の特性参照）

本報告書では継続的な取引をモデルとし、「募集～取引企業を特定するまで」と「取引企業を特定した後の引き合い～決済まで」に分けて検討する。

後者の企業内業務については「商取引情報の社内部門間処理」の局面、ならびに「社内に閉じた意思決定プロセス機密情報データベース」の局面につき議論を進める。

5.1 企業間取引

5.1.1 企業間取引の取引形態

（1）「不特定多数企業間取引」

「募集～取引企業を特定するまで」とは、不特定多数企業に対する取引の募集から、取引相手を特定する（通常基本契約締結）時点までとする。

このケースは従来のクローズドなネットワーク上では対応できなかった取引プロセスであるが、今後のオープン・ネットワーク環境の普及・進展とともに電子的に処理されうるものと考える。

（2）「特定多数企業間取引」

「取引企業を特定した後の引き合い～決済まで」はすでに企業が特定している継続的もしくは都度取引プロセスを扱うこととし、取引関係を構築する局面については「不特定企業間取引」と同様と考えられるため詳細は取り扱わない。

このケースは、現在のクローズドＥＤＩでの処理が基本となるが、オープンＥＤＩにおける新たな視点での検討が必要と考える。特に従来のクローズドＥＤＩは一部の大企業を中心として普及し中小企業へのＥＤＩの導入はこれからであることから、広い視点からの検討が必要となる。

5.1.1.1 取引形態別の特性

継続的取引を前提とする場合、前提としない場合の取引形態を取引プロセス別に取引業務の特性を「図 5-1 取引形態の特性」に表す。

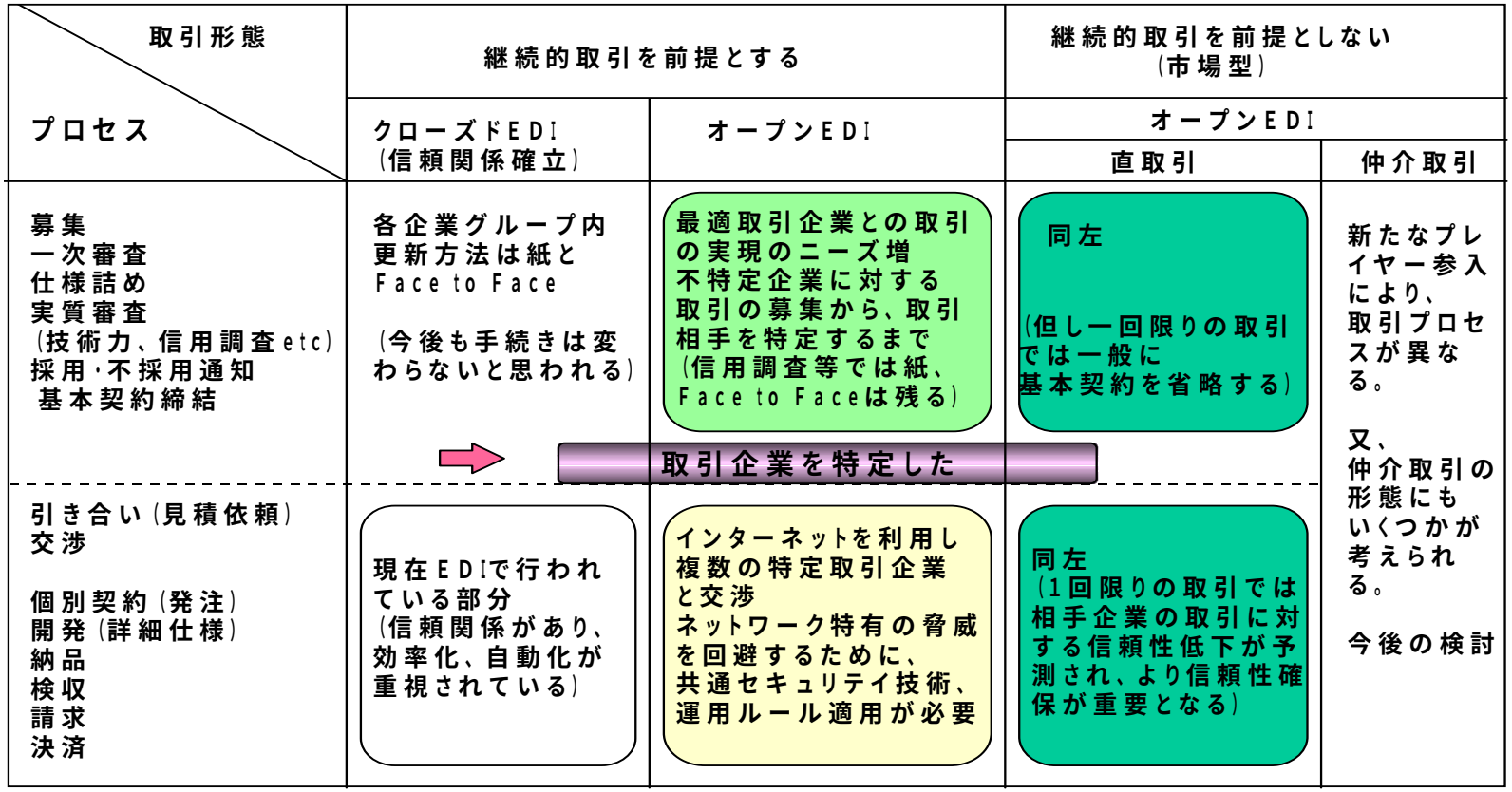

取引形態
プロセス
継続的取引を前提とする
継続的取引を前提としない
（市場型）
クローズドEDI
（信頼関係確立）
オープンEDI
オープンEDI
直取引
仲介取引
募集
一次審査
仕様詰め
実質審査
（技術力、信用調査etc）
採用・不採用通知
基本契約締結
各企業グループ内
更新方法は紙と
Face to Face
（今後も手続きは変わらないと思われる）
最適取引企業との取引の実現のニーズ増
不特定企業に対する
取引の募集から、取引相手を特定するまで
（信用調査等では紙、Face to Faceは残る）
同左
（但し一回限りの取引では一般に
基本契約を省略する）
新たなプレイヤー参入により、
取引プロセスが異なる。
又、
仲介取引の形態にもいくつかが考えられる。
今後の検討
取引企業を特定した
引き合い（見積依頼）
交渉
個別契約（発注）
開発（詳細仕様）
納品
検収
請求
決済
現在EDIで行われている部分
（信頼関係があり、効率化、自動化が重視されている）
インターネットを利用し
複数の特定取引企業と交渉
ネットワーク特有の脅威を回避するために、
共通セキュリテイ技術、
運用ルール適用が必要
同左
（1回限りの取引では相手企業の取引に対する信頼性低下が予測され、より信頼性確保が重要となる）

図 5-1取引形態の特性

説明１：
継続的取引を前提としない市場型取引の取引形態には直取引と仲介取引に分類される。
仲介取引では仲介業者という新たなプレイヤが存在するため、取引プロセス自体が変わる。
また、仲介業者の役割として、お見合い型、お任せ型とか色々と考えられる。

説明２：
継続的取引が主にに行われている代表として生産財がある。その理由としては取引企業を特定するまでの労力（企業の信用調査、技術力、生産能力、品質管理等）は大変であり、一度よい取引関係が確立できればお互いに継続することにより、安定的供給が確保できることにある。また、１回限りの取引だからといって、取引企業を特定するプロセスを省略するとかは基本的にはない。
特に、開発的要素がある場合途中から代替企業への切り替えは影響が大きい。
それは、例えば納入日が確保できずに企業の信用を失うとか、ビジネスのチャンスを逸することは許されないからである。

説明３：
消費財のように万一トラブルがあった場合に代替品や別のメーカーから調達の可能性がある場合は取引企業を特定するまでのプロセスにおける調査は、代替品や代替企業からの供給確保が可能な場合には軽減できる。

説明４：
取引企業を特定するまでのプロセスで継続的取引を前提にする場合と、継続的取引を前提としない場合では、例えば募集時の提示条件（ルール）は異なる。
継続の場合は採用通知後の基本契約の段階で取引条件を取り決める事が出来るが、１回限りの取引の場合は募集時に採用、不採用の基準とか取引条件（支払条件とか）を分かりやすく提示することが必要である。

説明５：
継続的取引を前提にした場合としない場合での第三者からの脅威については基本的には変わらない。しかし当事者間の脅威については継続的取引を前提としない１回限りの取引の脅威が大きいと思われる。
（継続的取引の取引停止が存在しない分悪意が起きやすい）

説明６：
認証について、企業を特定するまでと、特定後に分けて検討する。
企業を特定する（不特定多数企業の中から取引企業を特定する）までのプロセスでは如何に条件にかなった企業を効率的に選定するかが最大の課題である。
そのためには、効率的にふるいにかけることであり、企業の真正性は最初に（例えば提案書を受理した時点や一次審査段階で）確認する行為となる。（応募企業が知名度の高い企業だとしても、詐称されていない保証はない）

企業の真正性を証明する１つの手段として、公開鍵方式の認証局の電子認証書がある。電子署名により応募内容を受理することにより、送信者の特定（秘密鍵の保持者＝公開鍵の申請者）と電子情報の非改竄（完全性）を保証できるため、この場面での安全性・信頼性確保の有効な手段として考えられる。
また、取引企業と基本契約の締結が完了し、さらに当事者間の信頼関係が確立されている場合については当事者間では取引情報の送信者の特定ができればよい。従って、当事者間の否認が無い前提では例えばデジタル署名以外の方式として、ＩＤ，パスワードを暗号化し送信することも考えられる。また、デジタル署名を利用する場合でも第三者からの脅威に対する影響が大きくない取引情報に関しては取り引き情報毎に認証局に認証書を取り寄せる必要が無い場合もある。認証のレベルは色々あり、取引相手との信頼関係、取引情報の重要性等に応じた認証が必要となる。

説明７：
電子公証について、企業を特定するまでと、特定後に分けて検討する。
企業を特定するまでは相手企業と信頼関係が確立されていないことによるニーズは大きい。（例えば、契約までのプロセスの確証）
企業が特定された後の取引メッセージ全てに対しての電子公証は不要である。
企業経営に影響する金銭的損害、競争力低下、社会的信用に係わりある部分に対する要求度は高い。

説明８：
電子公証対象の取引情報に対しては、取り引き情報の真正性を証明するため（送信者を特定できること、送信内容の完全性が保証されていること）にはデジタル署名が有効な手段である。
但し、継続取引関係場合、取引メッセージ毎に認証局に公開鍵の電子証明書を取り寄せることは不経済であり、リアルタイム性を損なうため、当事者間で鍵管理や、鍵更新時等の取り決めをすることにより、１週間に１回とかに減らすことも可能となる。さらに外部からの脅威（詐称、盗聴、改竄）に対する手当てができれば送信企業の確認ができればよいので、ＩＤ，パスワード等の利用も考えられる。

結論：
以上より、継続的取引を前提とする場合、継続的取引を前提としない場合でも企業を特定すること（お互いの取引関係を確立すること）が重要であり、特定されればその企業と如何に効率的に取引を行うかということになる。

5.1.1.2 取引形態別開発品、標準品の取引プロセスの特性

取引形態、取引プロセス、取引対象（生産財／消費財、物財／情報財、開発品／標準品）の特性を踏まえた検討の１例として、物財の開発品／標準品の特性を示す。

表 5-1取引形態別開発品、標準品の特性

取引形態 / プロセス	継続的取引を前提とする			継続的取引を前提としない（市場型）	
		オープンEDI		オープンEDI（直取引）	
	クローズドEDI（信頼関係樹立）	開発品	標準品	開発品	標準品
募集 一次審査 仕様詰め 実質審査 （技術力、信用調査etc） 採用・不採用通知 基本契約締結（継続取引時締結）	各企業グループ内 更新方法は紙と Face to Face （今後も手続きは変わらないと思われる） A	開発品は途中から代替が困難である （機密情報は対策上小出し） A	標準品は複数企業が製品化し代替可能 B	1回限りの開発品の取引は少ない C	代替可能な標準品がメイン D
	→ 取引企業を特定した				
引き合い（見積依頼） 交渉 個別契約（発注） 開発（詳細仕様） 納品 検収 請求 決済	現在EDIで行われている部分 （信頼関係があり、効率化、自動化が重視されている）	仕様、性能、品質等の電子情報が多い （物財は次回から特注品） E	注文（品名、数量、単価等）情報がメイン F	仕様、性能、品質等の電子情報が多い G	注文（品名、数量、単価等）情報がメイン H
利用企業とニーズ	大企業中心	大企業ー中小企業利用多		利用少増分野	中小企業利用多

説明Ａ：
開発品は途中から別の企業への切り替えには仕切り直しのため時間がかかり、困難である。
従って、取引企業を特定するには技術面、信用面、生産能力、品質面等十分な調査が必要である。
特に、開発基本仕様のやり取りが頻繁に行われるため、情報の安全、信頼性要求は多い。
また、次回の取引からは本開発品は特注品（該当企業しか製品がない）としての扱いとなるため、より慎重な調査が必要である。
機密保持のために提案内容の交渉、信用調査状況を踏まえ情報の提供が必要となる。
基本契約締結時には機密保持に関する取り決めを交わす必要がある。

説明Ｂ：
標準品においても企業を特定するまでのプロセスはＡと変わらないが、万一トラブルが発生した時には、代替品や代替企業を事前に調査することによりリスク軽減が可能である。

説明Ｃ：
継続的取引を前提としない場合においては開発品を対象とするケースは下記理由で一般に少ないと思われる。
理由①：相手企業に機密開発情報が流れる。
理由②：１回限り取引のための企業特定に多大な労力をかける必要がある。
理由③：短期の代替選定は困難である。
但し、今後ますます製品のライフサイクルの短縮化と高度な技術（技術革新の要求される）の必要性により、開発品における１回限りの取引の潜在ニーズは大きいとも言える。

説明Ｄ：
この領域（Ｄ，Ｈ）は今後中小企業にもビジネスチャンスを提供する。
安くて、良い製品を幅広く調達できる可能性を秘めており、安全と信頼性が確保できる仕組みが整備されると利用ニーズは大きい。

説明Ｅ：
開発品の場合は調達側と受託側の開発仕様、性能、品質に関するやり取りが頻繁に行われる。
この領域では内容自体が複雑なため言った、言わないのトラブルが起きやすい。
また、機密情報の管理が必要な領域である。

説明Ｆ：
注文情報（品名、数量、単価等）が頻繁にやり取りされ、その結果、請求や決済情報が当事者間、銀行に行き交う領域で、効率性が重要視される。
金銭的損害に直結する取り引き情報（例えば、注文情報、請求情報、決済情報）に対しては特に安全性、信頼性が要求される。

説明G：
Ｅと同じ事が言える。
また、１回限りにおいても機密保持契約が重要である。

説明H：
Ｆと同じ事が言える。
更に、お互いに信頼関係が確立されていないため、当事者の故意による改竄や否認に対する脅威・不安が存在する。

まとめ：
（１）開発品の場合は機密保持及び途中からの代替の困難性もあり、ネットワーク上の取引においてもリアルな取引と同様に実務的には一般的に継続的な取引が前提となる。
　しかし、技術革新が早い分野等においては、１回限りの取引に対する潜在ニーズは大きいと思われる。
（２）標準品の場合はリスクを軽減可能であり、継続的取引を前提としない。特にニュービジネスの分野として注目され、中小企業のビジネスチャンス領域にもなり得る。

5.1.1.3 取引形態別開発品、標準品のプロセス毎の脅威

　第三者からのものと、取引当事者からの脅威について、代表的脅威の事例をマッピングしたものが、「表 5-2 取引形態別開発品、標準品における第三者からの脅威」「表 5-3 取引形態別開発品、標準品における当事者からの脅威」である。

表 5-2取引形態別開発品、標準品における第三者からの脅威

取引形態 / プロセス	継続的取引を前提とする			継続的取引を前提としない（市場型）	
		オープンEDI		オープンEDI（直取引）	
	クローズドEDI（信頼関係樹立）	開発品	標準品	開発品	標準品
募集 一次審査 仕様詰め 実質審査 （技術力、信用調査etc） 採用・不採用通知 基本契約締結（継続取引時締結）	各企業グループ内 更新方法は紙と Face to Face （今後も手続きは変わらないと思われる）	なりすまし募集、応募 機密情報を盗む A	なりすまし募集、応募 B	なりすまし募集、応募 機密情報を盗む C	なりすまし募集、応募 D
	⇒	取引企業を特定した			
引き合い（見積依頼） 交渉 個別契約（発注） 開発（詳細仕様） 納品 検収 請求 決済	現在EDIで行われている部分 （信頼関係があり、効率化、自動化が重視されている）	なりすまし発注、請求 機密情報を盗む E	なりすまし発注、請求 発注内容（数量、金額）の改竄 F	なりすまし発注、請求 機密情報を盗む G	なりすまし発注、請求 発注内容（数量、金額）の改竄 H
利用企業、ニーズ	大企業中心	大企業ー中小企業 利用多		利用少 増分野	中小企業 利用多

表 5-3取引形態別開発品、標準品における当事者からの脅威

取引形態 / プロセス	継続的取引を前提とする			継続的取引を前提としない（市場型）	
	クローズドEDI（信頼関係樹立）	オープンEDI		オープンEDI（直取引）	
		開発品	標準品	開発品	標準品
募集 一次審査 仕様詰め 実質審査 （技術力、信用調査etc） 採用・不採用通知 基本契約締結（継続取引時締結）	各企業グループ内 更新方法は紙と Face to Face （今後も手続きは変わらないと思われる）	応募内容の否認 応募内容受信否認 応募内容の改竄 機密情報の悪用 打合内容の否認 不採用通知の受信否認 （信頼関係がない） A	同左 但し、機密情報に対する脅威は少ない B	応募内容の否認 応募内容受信否認 応募内容の改竄 機密情報の悪用 打合内容の否認 不採用通知の受信否認 （信頼関係がない） C	同左 但し、機密情報に対する脅威は少ない D
		取引企業を特定した			
引き合い（見積依頼） 交渉 個別契約（発注） 開発（詳細仕様） 納品 検収 請求 決済	現在EDIで行われている部分 （信頼関係があり、効率化、自動化が重視されている）	無権限者の発注 個別契約の否認 個別契約の内容否認 納品の受領否認 請求書の金額改竄 請求書受信否認 機密情報の悪用 （信頼関係構築 が可能） E	同左 但し、機密情報に対する脅威は少ない F	無権限者の発注 個別契約の否認 個別契約の内容否認 納品の受領否認 請求書の金額改竄 請求書受信否認 機密情報の悪用 取引停止が無い分脅威は大きい G	同左 但し、機密情報に対する脅威は少ない H
利用企業、ニーズ	大企業中心	大企業ー中小企業 利用多		利用少 増分野	中小企業 利用多

(1) **第３者からの脅威の例示**

① 説明Ａ：

募集の段階では機密情報は出せない。従って小出しに開発情報を出していくことになる。

しかし、企業を絞って取引企業を選択する段階では少し具体的な内容も提供し、提案してもらうことになる。ここでは第三者がこれらの開発情報を盗聴し、悪用することが起きる。

② 説明Ｅ：

取引企業との具体的な開発仕様を盗聴し、悪用する。さらには、金額の入った取引情報に対し、なりすましや改竄を行い、振り込ませる。

③ 説明Ｆ，Ｈ

金額の入った取引情報に対しなりすましを行い、振り込ませる。

(2) **当事者からの脅威の例示**

① 説明Ａ、Ｃ：

応募内容の否認、応募内容の受信否認、応募内容の改竄、打合内容の否認、機密情報の悪用が考えられる。

② 説明Ｅ、Ｇ：

無権限者の発注、個別契約の否認、内容否認、納品の受領否認、請求書の金額改竄、請求書受信否認、機密情報の悪用等がある。信頼関係のあるＥでは故意による改竄、否認は起こりにくい。但し、Ｇでは次回以降の取引期待が薄い分脅威は大きい。

また、故意でない電子的処理のために起きるトラブル（例えば入力ミス、操作ミスした場合高速に相手に間違った内容が伝達される）に対する手だてが必要。

③ 説明Ｂ，Ｄ：

Ａ，Ｃと同様なことが言える。但し、機密情報に対する脅威は少ない。

④ 説明Ｆ，Ｈ：

Ｅ，Ｇと同様なことが言える。但し、機密情報に対する脅威は少ない。

Ｈは１回限りの取引で取引停止効果が無い分脅威は大きい。

以上、取引形態別に取引プロセス毎に開発品、標準品それぞれの特性、第三者からの脅威、当事者からの脅威の代表例を示した。

次に、募集～基本契約締結までと、引き合い～決済までの具体的な取引局面別課題と電子公証ニーズについて述べる。

5.1.2 取引企業を特定するまで（募集～基本契約締結）

企業間における取引モデルとして、その取引の対象となる商品を情報材と物財に分類して

検討したが、取引プロセスでの納品段階の物流という違いがあるだけで、他の取引プロセスにおいては同一であった。

今後、特に情報材、物財固有の問題として明記しない場合においては両者を併せて検討するものとする。

また、取引の誘因をホームページによる募集を前提として検討したが、メーリングサービス（現実の取引におけるダイレクトメール）型の募集形態も今後発展することが考えられる。この場合には、メールアドレス業者というような新しい取引関係者が介在することが予測されるが、本来の取引当事者の業務プロセスの一部を代行しているものと捉え、取引の直接当事者の業務プロセスを中心に検討する。

5.1.2.1 業務フロー

業務フローについては購入企業内でのものと，供給企業内でのもの，相互のものとがあるが，ここでは夫々の社内での業務の流れについては詳細な記述は避け，相互の関係に注力するものとする。

①募集

募集者が自社のホームページ上に募集を広告

(募集要領の項目)

・募集者の属性
・募集内容(概略スペック)
・募集条件(購入価格、納期等)
・募集者のデジタル署名
・応募者の属性記入欄
・応募内容(概略商品説明)記入欄
・応募条件(販売価格、納期等)
・応募者デジタル署名欄

②応募（プロポーザル）受付

③一次審査

④交渉（スペック打ち合わせ）

⑤実質審査

⑥採用決定、採用・不採用通知

⑦基本契約締結

［用語の定義］

・購入企業：入札案件としてインターネット上のホームページへ登録する企業
・供給企業：インターネット上のホームページに登録された入札案件を見て、応札する企業
・入札：供給企業が、案件に対して供給する条件を電子メールを使って購入企業に送ること
・落札：購入企業が、入札した企業の中から、供給企業を１社に決定すること

業務フローを図 5-2 募集～基本契約までの業務フローに示す。

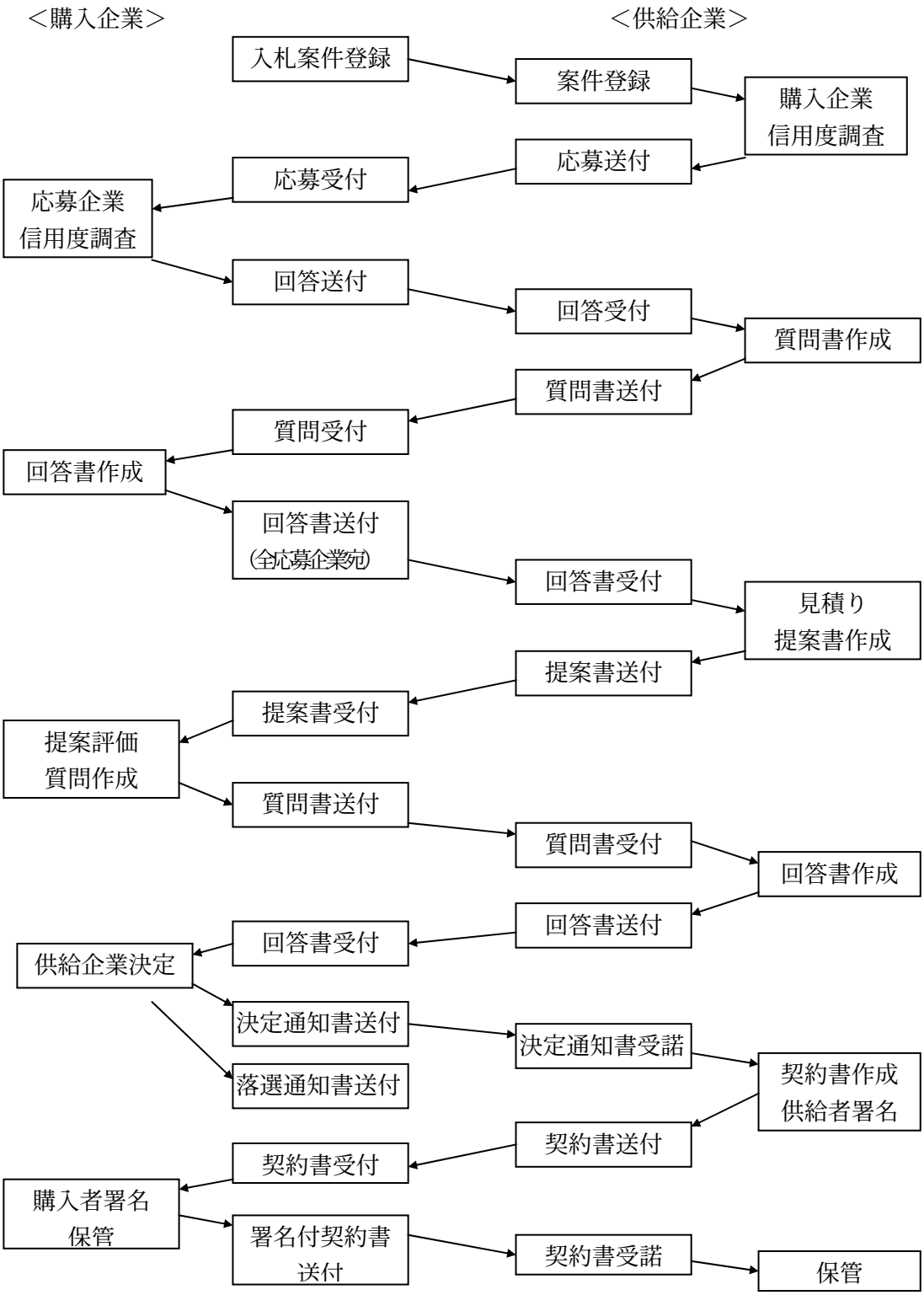


図 5-2募集～基本契約までの業務フロー

5.1.2.2 取引企業を特定するまでの（不特定による）特徴

(1) **課題の特徴**

不特定の取引先との情報の交換を前提とするため、相手方との信頼関係がないものとして取引を行うことになる。そのため、発生する１つ１つの課題は特定企業間取引より質的にも量的にも大きいものになると考える。

例えば、募集段階においても相手方の認証の前に、自社を相手方に認証させることが必要になる。自社のロゴマークや商標に代わる企業のデジタル署名のようなものが必要と思われるが、ホームページにデジタル署名を誰でもがその場で確認できる方法で表示することは、複製の危険に晒されることも容易に想像でき現実的でない。

相手方が特定できない（しない）のであるから、相手方の悪意や故意に関係ない視点での課題として捉える必要がある。

(2) **公証ニーズ（機能）の特徴**

課題を解決する方法としては、技術・ルール・運用が考えられるが、取引先が特定できていないのであるから、相手方の技術水準は自社の要求を満たしているとは限らない。また、運用も相手方との合意なく行えるものではない。

そこで、電子商取引に参加するための社会的なインフラとしてのルールが重要になる。例えば、取引の募集を行う場合に、今後の情報の交換にはこの位の設備（機械）と技術（運用する人を含む）レベルを客観的に表示できる基準のようなもの（企業格付と技術格付を合わせた）が社会的に認知されていれば、募集する企業だけでなく応募する企業にとってもメリットがあると考えられる。

5.1.2.3 取引局面別課題と公証ニーズ

ここでは、各取引ごとに発生すると思われる課題と、その課題を解決するのに必要な公証ニーズ（機能）を「表 5-4　取引局面課題と電子公証ニーズ（１）」「表 5-5 取引局面別課題と電子公証ニーズ（２）」に整理した。

表 5-4取引局面別課題と電子公証ニーズ（1）

募集～基本契約取引局面	課題	電子公証ニーズ	特記事項
1．募集段階	不特定多数企業に要求を知らしめる 自社であることを応募企業に納得させる 自社の意図するところを正しく伝える 応募条件等の改竄防止 応募先を表示しジャンクメールがこない	・(認証局) ・電子情報未改竄証明機能 ・(メールのフィルター、転送機能)	「募集企業のホームページであること、および募集企業の存在を応募者が確認できる機能が必要」
2．プロポーザル受入時	募集先に間違いなく届くこと	・電子情報到達証明機能	
3．一次審査時	応募者の実在性を確かめる 応募内容の情報の真正性を確認する 応募者の応募内容の否認を防止する	・(電子的商業登記簿) ・電子情報未改竄証明機能 ・電子情報割印登録機能 ・電子日付証明機能	応募要領に品質、納期、価格等を網羅し、否認を防止
4．スペック打ち合せ	情報の機密を保持する 打ち合せの過程を保管	・(暗号技術・認証技術) ・電子情報割印機能 ・電子情報日付証明機能 ・電子情報未改竄証明機能	一次審査後の契約相手候補とのやり取り情報は第3者に盗聴出来ないようにする。 また、機密保持契約が必要言った、言わないが起きやすい場面が多いため、記録が必要

表 5-5取引局面別課題と電子公証ニーズ（2）

募集～基本契約取引局面	課題	電子公証ニーズ	特記事項
5．実質審査	商品（提案内容）そのものにたいする ・性能 ・品質 応募者に対する審査 ・信用調査 ・技術力調査 ・生産力調査	・（暗号技術・認証技術） ・公平かつ中立な各審査項目についての格付け機関 ・電子情報日付証明機能 ・電子情報未改竄防止機能	この部分はリアルな世界で行われ、ノウハウに依存している。特に、応募者に対する審査の電子化が非常に難しい。 安全度の目安を提供する格付け機関の整備 （但し、損害負担は自社） 保険制度の整備 8。（10）信用格付機関参照
6．採用・不採用通知	応募者に間違いなく通知が届くこと 採用・不採用の結果の改竄を防止する	・（暗号技術・認証技術） ・電子情報日付証明機能 ・電子情報未改竄証明機能 ・電子情報到達証明機能	不採用通知を発信すればそこで取引は終了するため到達機能は必要となる。
7．基本契約締結	契約書の保管は完璧にしなければならない 契約の日付を証明できなければならない 契約書の真正性が証明できなくてはならない	・電子情報保管機能 ・電子情報割印機能 ・電子情報日付証明機能 ・電子情報未改竄証明機能	何時、誰と、何を契約したかを保管し、真正性が証明される必要がある。

5.1.3 取引企業が特定された以降（引き合い～決済）

企業間取引モデルとして、「物財」、「情報財」を検討したが、その違いは相手方の企業を特定した以降の引き合いから決済までのフローに現れる。この違いを取引の段階で整理したものを「表 5-6 物財と情報財の違い」に示す。

表 5-6物財と情報財の違い

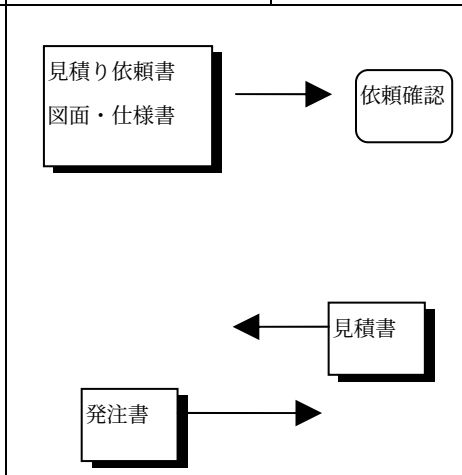
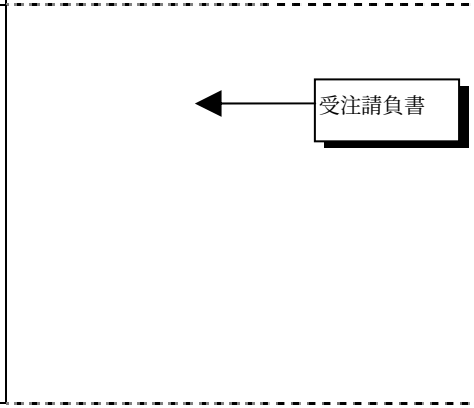
	取引プロセス	開発（仕様を含む）	商品の移動	検品（中間物を含む）
物財	ネットワーク	ネットワーク	物流	物流（一部ﾈｯﾄﾜｰｸで可）
情報財	ネットワーク	ネットワーク	ネットワーク	ネットワーク

すなわち、「物財」モデルでは商品の移動（納品や検品等）が物流で行われるのに対して、「情報財」モデルではこれらの物の移動がネットワークを通して行われる。この違いがモデルの特性に顕著に現れる。

ここでは、物財の業務フローの例について示し、情報財の業務フローについては情報財の開発業務を資料２に添付する。

5.1.3.1 物財の業務フロー

「図 5-3 物財の取引プロセスと電子公証の利用局面」を示す。この業務フローは、企業間で取引の基本契約が締結されていることを前提としている。この前提で引き合い（見積り）から決済までの業務フローと電子公証のニーズを示している。このフローは、開発品（設計変更含む）を対象にしている。

プロセス	フロー	電子公証	担保すべき	脅威	想定されるトラブル	対応方法		
	発注企業	受注企業	利用ニーズ	情報			当事者間	第三者介在
見積り			○ ＊信用 ＊企業秘密	見積り依頼者 見積り者 見積り内容 見積り日	なりすまし	カラ発注・受注	発注・受注確認後の授受 取引における共有鍵の設定 ＩＣカード	認証局利用による同一性の確認
						無権限者による発注・受注	取引担当者の設置 社内認証書（担当ＩＤ）の利用ＩＣカード	
					盗聴	製品仕様の盗聴	取引における共有鍵の設定（暗号化）	
						見積書の盗聴	取引における共有鍵の設定（暗号化）	
					改竄	製品仕様の改竄	取引における共有鍵の設定（暗号化） デジタル署名	デジタル署名の利用（認証局利用）
						見積書の改竄	取引における共有鍵の設定（暗号化） デジタル署名	デジタル署名の利用（認証局利用）
発注･受注			△ ＊信用 ＊企業秘密	発注者 受注者 発注内容	なりすまし	カラ発注・受注	発注・受注確認後の授受 取引における共有鍵の設定 ＩＣカード	認証局利用による同一性の確認
						無権限者による発注・受注	取引担当者の設置 社内認証書の利用 ＩＣカード	
					未着	発注･受注の否認	発注・受注確認書の授受 開封確認の返送（ソフトによる自動化）	第三者経由での送信（配達証明）
					改竄	発注･受注内容の改竄	取引における共有鍵の設定（暗号化） デジタル署名	
					盗聴	発注･受注書の盗聴	取引における共有鍵の設定（暗号化）	

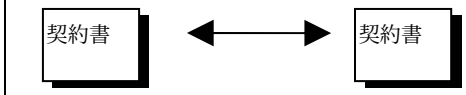
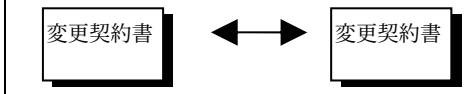
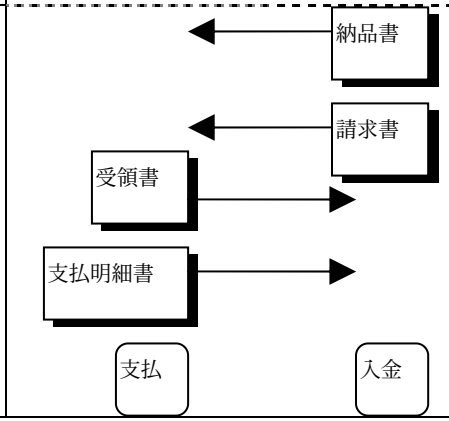
契約		△ ＊信用 ＊企業秘密	契約者 契約内容	なりすまし	なりすましての契約	取引における共有鍵の設定（暗号化）ＩＣカード	認証局利用による同一性の確認
				盗聴	契約内容の盗聴	取引における共有鍵の設定（暗号化）	
				否認	契約内容の否認	デジタル署名	第三者での契約書保管
				改竄	契約内容の改竄	デジタル署名	第三者での契約書保管
契約内容の変更･取消		○ ＊信用	変更内容 変更依頼者	なりすまし	悪意の第三者による変更・取消	変更・取引確認書の授受 取引における共有鍵の設定 ＩＣカード	認証局利用による同一性の確認
					無権限者による変更・取消	取引担当者の設置 社内認証書の利用 ＩＣカード	
				未着	変更･取消の否認	変更・取引確認書の授受 開封確認の返送（ソフトによる自動化）	第三者経由での送信（配達証明）
				改竄	変更･取引内容の改竄	取引における共有鍵の設定（暗号化）デジタル署名	
				盗聴	変更･取引依頼書の盗聴	取引における共有鍵の設定（暗号化）	
請求･支払		○ ＊収入 ＊信用	請求者 請求先 請求金額 請求日	なりすまし	無権限者からの請求	請求確認書の授受 取引における共有鍵の設定 ＩＣカード	認証局利用による同一性の確認
				未着	請求内容の否認	請求内容確認書の授受 開封確認の返送（ソフトによる自動化）	第三者経由での送信（配達証明）
				改竄	請求･支払内容の改竄	取引における共有鍵の設定（暗号化） デジタル署名	
				盗聴	請求･支払内容の盗聴	取引における共有鍵の設定（暗号化）	

図 5-3物財の取引プロセスと電子公証の利用局面

5.1.3.2 取引局面別課題と電子公証ニーズ

各プロセスにおける取引局面での課題は、当事者間の外部および内部からの脅威、すなわち、脅威によって想定されるトラブルである。これらの課題に対応する解決策として電子公証の手段が考えられる。「図 5-3 の業務フローについての課題と電子公証のニーズ」を各フローに対応させて同じ図の右欄に示してある。

図には項目のみをまとめて対比してあるが、それぞれについて次のような課題が含まれている。

(1) **脅威の検討**

脅威については、当事者からの故意によるもの（改竄、否認）と故意でないもの（錯誤）と第三者からの脅威（詐称、改竄、盗聴）、ネットワーク障害に起因する脅威（未到着、伝送遅延等）がある。従来のクローズな世界では、クローズドなネットワークの利用による第三者からの脅威が少ないこと、特定企業間の継続的取引で当事者の故意による脅威は殆どないこと、専用線、公衆回線によりネットワークの信頼性も確保し易い環境にあった。しかしオープンネットワーク上ではそれぞれの想定される脅威は多く、輻輳する。例えば受信確認ルールを決めて運用した場合、相手から受信確認が戻らない場合第三者の改竄かネットワーク障害か相手が否認しているのか送信側からは確認が出来ない。この事により、取引を行う相互間で不安・不信感が生じかねず、円滑な取引を阻害する要因となる。すなわち、善意の取引きが信用を失うケースになることがある。

従って、オープンなネットワークでの取引上の問題点を整理し、リカバリー策を決めることにより、信頼性の確保を図ることが極めて重要である。

しかも、取引モデルのフェーズ毎にその度合いも違い、その度合いに応じた対応が必要となってくる。

(2) **電子公証ニーズ（対応策）**

対応方法については、技術的な対応と運用面での対応とあり、また、当事者間で対応するものと第三者の介在を必要とするものがある。

技術的な対応としては主に暗号技術によるもので、送信電文の暗号化と認証局を利用したデジタル署名による盗聴・改竄の防止があり、運用による対応については送受信の確認のやりとり、中立の第三者を経由した電文の送信、中立の第三者への保管依頼による否認、改竄の防止がある。ただし、電文の未着については確認電文の未着等も考えられ（第三者を経由した場合でも同様）、未着原因の責任の所在もオープンネットワークの場合はっきりしないため、それのみで完全に対応しきれるものではなく、フェーズによっては最終的に運用面で電話等による確認が必要なことも有りうる。

取引情報別にどこまでの確認（再送信回数、代替確認方法等）をするかを取り決めることも必要である。

また、契約、変更、取消等重要な局面においては、取引の内容、当事者間での信頼関係に応じて、タイムスタンプ、第三者への保管依頼の利用も必要な場合がある。

5.1.3.3 運用ルール

取引局面での課題に対する電子公証のニーズを前項で示したが、継続取引を前提とする場合は当事者間の運用ルールでどのように解決していくかは重要であり、ポイント（基本的事項の例）を以下に示す。

(1) **デジタル署名に関するルール**

・認証局による方法

電子署名に使用する公開鍵は第三者機関としての認証局が保証する。

・当事者管理による方法

予め何らかの安全な方法で、当事者間相互に公開鍵を通知し合っておく。

公開鍵の使用方法についても当事者間でルールをきめておく。たとえば、相手方の鍵の確認を毎回する必要はなく、鍵の有効期限内ならＯＫとするとか、一定期間毎に行うなど、あるいは何かトラブルがあったときに認証局に確認するなど。

(2) **暗号化に関するルール**

暗号化に使用する暗号方式は双方で合意された方式であること。

共通鍵暗号方式を使用する場合、安全な鍵の授受方法を予め決めておく。

(3) **メッセージプロトコル**

文書の受取りが完了したと見なす時点をどの時点とするかを予め相互に決めておく。（開封確認通知、メール返信等）。

文書送信先から受信確認メッセージが返されない場合、また受信したメッセージが判読不能の場合の対処方法（リトライ、不成立判断等）を予め決めておく。（二重発注防止等）

(4) **書換え不能な記憶媒体に関するルール**

使用する記憶媒体（ＣＤ－ＲＯＭ等）の種類、管理者、アクセス権限、保存期間、文書の差替え等、文書管理ルールを予め決めておく。

(5) **ＩＣカードに関するルール**

１枚のＩＣカードにＩＤ、資格（管理者のランクなど）、権限（アクセスや承認など）を入力して使用する場合の入力管理やデータ更新の運用ルールを決めておく。

(6) **タイムスタンプ・改竄防止処理方法・保管期間等**

5.1.3.4 まとめ

取引企業を特定後の引き合い～決済のプロセスにおける脅威の内容、原因がある程度明らかになってきた。

これらの総合的解決をするために、オープンＥＤＩのベースとなる標準ルールの策定が重要と考える。

暗号技術、鍵管理、機密保持、デジタル署名、否認防止、追跡機能、故意でないトラブル対応等を網羅する必要がある。

5.2 企業内業務

企業内業務における電子公証ニーズを調査するにあたり、幾つかの業務モデルを検討する必要があり、そのモデル選択に際して、その検討対象がひろくカバーされるために、以下の特性を考慮した。

［社外関係の有無］

企業外との情報交換では、相手企業の情報を扱うことになる。今後、企業間での電子商取引が進むとを想定して、特にこのようなプロセスの内、企業内プロセス部分を検討しておく必要がある。企業内でも、部門を越えた処理等は電子化による効率化が期待される反面、部門間の管理上の違いなどを考えると企業間で考えられる問題点と同じような問題点が存在する可能性がある。一方、企業内部に閉じている場合は個人的な情報をもとにした処理である場合が多く、これに特徴的な問題点を検討する必要がある。

［金銭の直接的関係］

社内においても脅威のひとつとして考えられる。

［定型／非定型］

定型的な業務は、システム化が比較的容易であるだろう。これに対して、業務単位毎に処理内容が異なる非定型の場合には、従来、人の判断（企画とか根回し）では処理され電子的な処理が遅れている領域であり、電子化に伴う問題があることが考えられる。

［決裁型／アクセス型］

企業内の多くの業務では職務階層の中で、情報の内容が承認され、決裁の後、実行されるという意志決定プロセスのサイクルを繰り返している。一方で、情報はシステムに蓄積され、それをアクセスするという局面がある。通常、蓄積データは機密である事が多く、情報処理を電子化する場合、アクセス制御が必要であり、無権限者による変更、更新管理が重要である。

調達・入札と見積・契約は企業の外と関係するプロセスであり、お互いに相補関係にあるものとしてが考えられる。決裁処理の典型としては企画・稟議を、直接お金が関係するものとして請求・精算を、そしてデータベースや情報システムなどへのアクセス例として顧客情報システムを、企業内に閉じたプロセス例として人事考課プロセス、そして特許申請を検討した。一般に企業内プロセスは幾つかのプロセスがお互いに相互作用を持っていたり、同じような処理を含むことが多いので、結果として重複する部分も存在する。「表 5-7 企業内業務の特性」にはここで選定された業務の関連する特性を示しているが、個別企業や会社では業務規定や習慣に違いがあり、この表で示した特性が必ずしも当てはまらないかも知れないが、それで一般性が失われることはない。

他の幾つかの業務プロセスの例は添付資料３にある。

表 5-7企業内業務の特性

	社外との関係の有無		金銭の直接的関係		定型/非定型		決裁型/アクセス型	
	あり	なし	あり	なし	定型	非定型	決裁型	アクセス型
調達･入札	◎		○	○	○	○	○	○
見積･契約	◎		○	○	○	○	○	○
企画･稟議	○	◎	○	◎	○	◎	◎	
請求･精算	○	◎	◎	○	◎		◎	
顧客情報	◎		○	◎	◎			◎
人事考課		◎		◎	◎	○	○	◎
特許申請	○	○		◎	◎		◎	○

◎：特徴が著しい　○：部分的に特徴がある

注）決裁型　：承認プロセスによる情報処理を特徴とする
　　アクセス型：情報システムや蓄積機密情報へのアクセスを特徴とする

5.2.1 企業内業務モデル（特許出願申請）

特許出願申請では、発明の後、社内で出願に関する承認・決裁プロセスを経た後、社外の特許事務所と協力しながら、申請プロセスを処理する。この時の情報は機密である。この一連の業務が企業内業務全てを代表するものではないが、企業内の多くの業務処理に含まれるステップを含んでいるので、ここでは代表例として説明する。

他の幾つかの業務プロセスの例は添付資料３にある。

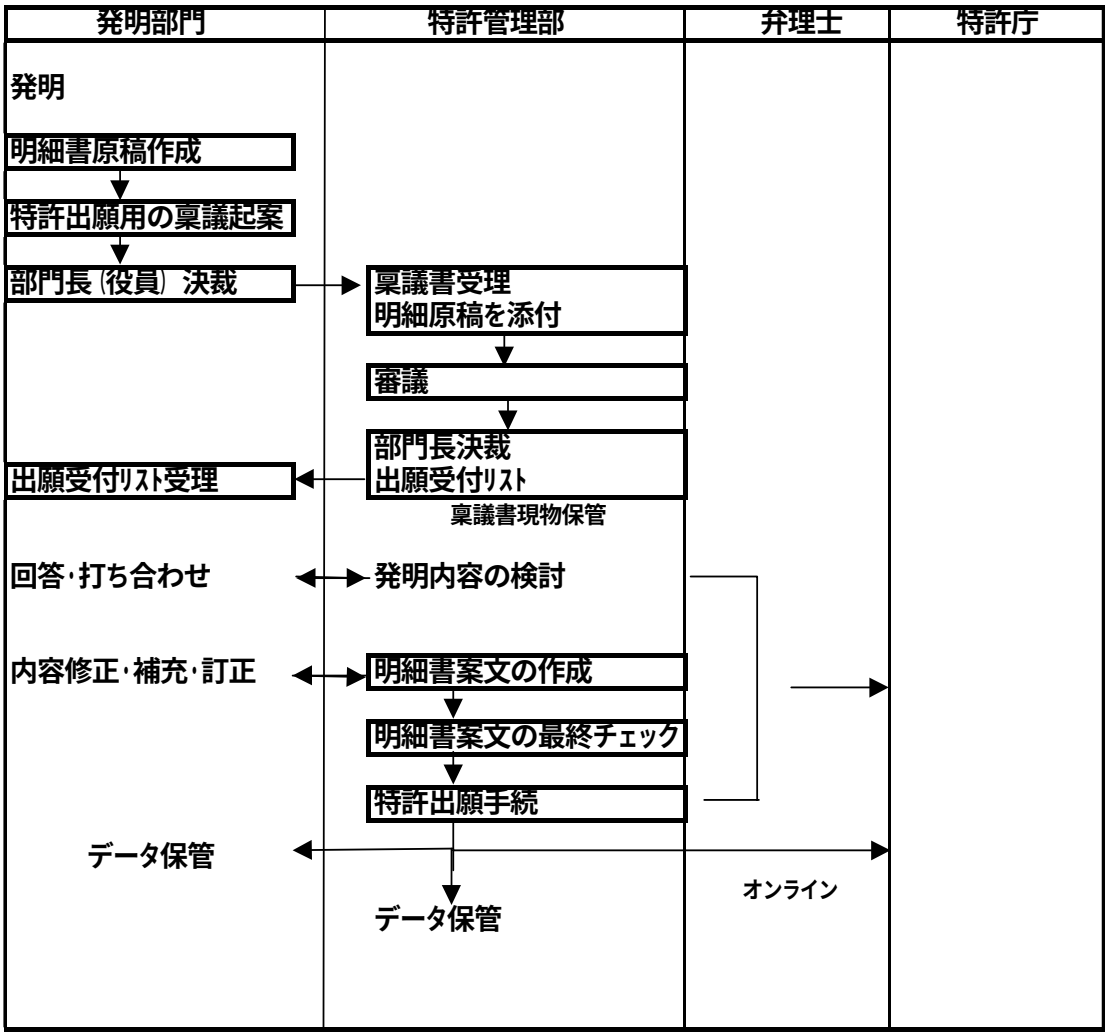


図 5-4特許出願申請に関する業務フロー

処理の概略は「図 5-4 特許出願申請に関する業務フロー」に示されており、処理は以下の段階を含んでいる。

(局面 1)発明

特許申請をしようとする場合、発明者が発明した時点でその発明内容とその時刻を後日客観的に証明することができるように、何らかの手段を講じていることが望ましい。

(局面 2)起案

発明者は発明内容を説明した特許明細書の案を作成すると共に特許出願用の稟議書を起案する。

(局面 3)部門長の決裁

所属部門の役員クラスの部門長が決裁する。

(局面 4)特許管理部門での審議

特許管理部門で、その内容の審議をして、特許管理部門の部門長が決裁する。

(局面 5)明細書の作成

発明者、特許管理部門、そして弁理士のあいだで出願用特許明細書を作成する。

(局面 6)出願

弁理士を通じて、特許庁に特許出願をするとともに、出願書類を、発明者の部門と、特許管理部門において管理する。

局面１～６における課題として以下の項目がある。

(課題)処理時間

従来は社内処理で時間がかかるので、公証役場に持ち込むこともあった。

(課題)情報の漏洩

内容の漏洩。発明部門、特許管理部門、弁理士などから情報が漏洩する心配がある。

(課題)発明時刻の証明(米国出願)

電子化が進んだ場合、従来紙に署名して時刻の証明をしていたが、電子情報ではどうするか。米国特許を申請するとき、発明があった日時時刻が問題となる場合があり、これを客観的に証明するためにタイムスタンプ機能が必要とされる。

(課題)アクセスコントロール

機密情報の漏洩を防ぐため関係以外へのアクセスは制限される必要がある。

処理時間の問題は電子化により解決されることが大いに期待される項目であるが、それ以外の項目は電子化にあたり十分に考慮され解決されている必要がある。

5.2.2 課題

前節特許出願申請の例に加えて、検討された他の業務プロセスにおいて得られた課題をまとめてみると、以下のようになる。

(課題のまとめ)

- システムからの盗聴・漏洩・改竄
- 印刷物、記録媒体からの漏洩・改竄
- 承認印の偽造、承認印・押印の偽造
- 送信否認・受信否認の防止
- 到達確認、受諾確認の必要性
- 情報の記録内容の不備
- 行為の確認、承認内容の否認防止

- 正規で現実的な電子決裁、電子稟議処理
- 保管中の文書の紛失、破壊
- 契約文書を誤って第三者に送付(自分からの発信時)
- 不正アクセス(なりすまし)、パスワード認証
- プライバシーの保護（人事考課）
- 記録経過の保持
- 発明時刻の証明

5.2.3 課題の主要解決法

情報システムが安全に正しく効率よく利用されるために、以下の点を考慮する。

(1)運用規則を定め、管理者および一般ユーザの電子情報に対する認識を一定水準に保つ。特に、企業内電子情報に対する管理義務、機密保持義務を定め、あるいは、例えば不正競争防止法や民法などの関連においても周知徹底させる。パスワードや所有物による認証をする場合、その管理義務や、事故責任を定めておく。印刷物、記録媒体の管理義務、を周知徹底する。不正アクセスや情報の漏洩、改竄の意味するところを説明し、倫理、道徳観を植え付けることにより、総合的に情報の電子化、高度化に対する企業文化を育成する。

(2)前記運用規則がユーザにとって困難なく適用されるように、物理的にもソフトウェア的にもシステム環境、運用環境を準備・設定する。さらに、システム利用者に対して具体的に何を、どうすればよいのかという教育をする。システムの安全性を高めるために、新たな技術的対応策を講じたり、新たな機能を導入したり或いは利用可能な企業外のしくみの利用を検討する。

そのような新たな技術としては、暗号技術や、ＩＣカードあるいはバイオメトリック素技術などを用いた新しい認証技術、或いは新たなビジネス環境に要求されている電子公証的機能等が考えられる。また、現在利用可能な仕組みとしては認証局やタイムスタンプサービス等がある。

(3)実運用にあたり、検査・監査を定期的に行ない、不正利用や好ましくない運用を是正するとともに、取り巻く環境の変化にも対応する。

企業内では、これらの問題を解決するための方策の選択肢は相対的に多い。それは、業務規則などにより一定の秩序水準が保たれていると考えられるためである。仮に利用するソフトウェアシステムに制限があったとしても、それを運用することも可能であろう。企業では、必要性や経済性等の諸点について検討し、対応策が選択されることになる。

5.2.4 電子公証のニーズ

企業内での電子公証の意味合いは、「企業の構成メンバーがネットワーク上で電子的交流の安全・信頼性を確保すること」である。諸プロセスの検討で解ったように、一般的脅威が存在するため、企業内にも電子公証のニーズがあると考えられる。企業内で必要とされる機能の多くは、既存の業務処理用ソフトウェアシステムに搭載されている。このような専用システムやパッケージソフトウェアには、電子公証的機能に相当する機能が既に部分的に考慮

されている。現状では、業務規則の存在と、利用しているソフトウェアシステムの機能により、一般的に運用の安全性が確保されているとし、多くの場合、新たな公証的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。しかしながら、取り巻くビジネス環境の変化により安全性・信頼性を確保する対策も変化せざるを得ない状況と予想される。

「表 5-8 課題と解決策」は抽出された課題と、その課題が関係するであろう対応策を、教育・規則、技術、運用、既存のソフトウェアシステム(グループウェア、ワークフロー等)、認証局の利用、電子公証的機能との関連において挙げてみた。「○」による関連の強弱は一様ではないが、それを測る尺度を現時点で設定することは難しい。企業内では、組織の中で処理されるという特殊性があり、これを考慮した公証的機能があれば、電子的交流の安全・信頼性を向上させることが期待される。ここでの検討の結果、企業内で特に必要とされる電子公証的機能は想定され得るものの、詳細な機能分析検討は行なわれていない。その一つの理由として、暗号システムを企業に導入する場合の是非と考えられる問題点が明らかになっていないことにある。不特定多数企業間での電子的情報交換では、前提として認証局の利用が考えられているが、企業内ではどこまでのセキュリティが必要でその解決策として公開鍵の導入が必要か、ＩＤ，パスワード方式でも可能かを十分検討する必要がある。

表 5-8課題と解決策

課題＼対応策	規則と教育	技術	運用	ソフトウェアシステム	認証局機能	電子公証的機能
盗聴	○	○	○	○	―	―
漏洩	○	○	○	―	○	―
改竄	○	○	○	○	○	○
送信否認・受信否認	○	○	○	○	○	○
到達確認・受諾確認	○	○	○	○	―	○
行為の確認、承認内容の否認	○	○	―	―	○	○
不正アクセス・なりすまし	○	○	○	○	○	―
詐称	○	○	―	―	―	○
記録経過の保持	○	○	―	○	―	○
記録内容の不備	○	○	○	○	○	○
自分が間違って第三者に送付		○	○	―	○	―
プライバシーの保護	○	○	○	○	○	―
保管中文書の紛失、破壊	○	○	○	○	―	○
承認印の偽造	○	○	○	―	○	○
印刷物、記録媒体からの漏洩・改竄	○	○	○	―	―	―
正規で現実的な電子決裁・稟議処理	○	○	○	○	―	○
発明時刻の証明	○	○	―	―	―	○

「○」印は何らかの関連があることを、「―」は関係しないこと

5.2.5 今後の検討課題

現在、企業内一般業務処理において、公開鍵インフラを導入している事例が殆ど見られず、

企業内で導入する場合の一般的諸問題についての理解が浸透していない。企業外での一般的な認証局の運用に関する問題は既に議論されてきているが、それらは企業や特定組織内での運用を想定したものではない。

今後情報システムのオープン化が進行するであろうことを考えると、従来の管理、運用方法では不十分であるだろう。ここで新たな導入技術の一つのきっかけとなるのは、暗号技術である。暗号技術はこれまで、特殊な場面でしか利用されていない。特に一般企業では利用可能なソフトウェアシステムが殆どなかったため、その利用は皆無に近かった。今日、電子商取引の時代を迎え、また、一方でコンピュータの演算能力も著しく向上していることもあり、暗号を用いたソフトウェアの利用は容易になってきた。さらに、 SSL、クレジットカードの電子決済プロトコル SET、暗号化電子メールなどは規格化や標準化が進み商用利用としてのソフトウェアシステムの開発が進行している。それらはまた、すでにインターネットで一般に利用されつつある。そして、一部の企業では、業務処理の手段として、暗号技術を含んだソフトウェアシステムの利用を開始している。公開鍵技術の導入は、さらに企業間との情報交換に際してもシームレスな環境を設定することができると考えられている。このような環境の変化に対して、新たな技術を導入する度合、時期は企業によってまちまちであるものの、次第にその導入が進むものと予想される。企業に必要とされる電子公証の具体的な機能は、セキュリティとの関連で検討される必要がある。

企業間取引においては、電子化された情報を利用して取り引きをする場合の法制度上の諸問題が提示されている。しかしながら、企業内の電子化された情報について、企業論理の観点から、あるべき企業情報システムとしては十分検討整理する必要がある。法制度上の多くは、紙による情報をもとに制定されており、電子化された情報に関して、運用上、技術上どのような対策が必要であるのかを整理する必要がある。例えば、書類であれば一般管理者が機密情報であることを容易に明示することができたが、電子化された機密情報は少なくとも同じ要領で機密扱いにすることはできないであろう。

情報の電子化の究極は企業内外の情報交換全般にわたって合理的に行なうことであり、これにより、効率的で迅速な処理が可能となる。今回の検討では、主として企業内プロセスだけに着目してその問題点を検討したが、今後は企業間取引を含んだ総合的、連続的なプロセスの中での合理性を検討する必要がある。企業内外が連続的な電子的情報交換を行なうためには、データの書式や交換規約を標準化して、相互運用性を確保する必要がある。

以上今後の課題をまとめると

① 企業内でのセキュリティ（公開鍵インフラやＩＤ，パスワード等導入）に関する諸問題の検討。

② 企業内電子情報システムの安全性、信頼性、機密性の確保の要件と関連法制度。

③ 企業間取引など対外的要求事項との関連。

④ オープンネットワークに接続する安全で信頼のおけるシステム運用を、客観的に評価する基準。

⑤ 相互運用性、標準化の動きからみた企業内システムに考慮される課題。

等が考えられる。

6 電子公証の要求度（レベル）

6.1 企業間取引の脅威と企業ダメージ

企業は存続し、社会に貢献することが必要である。

電子取引の脅威は自然災害を除けば、第３者の脅威、取引当事者の脅威、ネットワークの障害に起因する脅威が存在する。これらの脅威により、企業がダメージを受けるものとして代表的なものは、金銭的損害、競争力低下、社会的信用の失墜等の質的な面、量的な面がある。

これらを表にしたものが「表 6-1 取引の脅威と企業ダメージ」である。

３．２節で前述したように企業におけるダメージを考える場合には、その大きさだけでなく発生確率を考慮したリスクとしてとらえる必要がある。リスク=∑（被害の大きさ×被害の発生確率）このリスクを効率的に経済的に最小限に押さえる仕組みの一つとして電子公証が考えられる。

尚、取引当事者の脅威には、故意のものと、故意とは言えないトラブル（電子的処理速度により被害の範囲が大きくなることが想定される）が存在するが、後者のトラブル内容の及び対応策の検討も極めて重要である。

表 6-1取引の脅威と企業ダメージ

トラブルで失う物	取引局面	第三者からのの脅威	当事者からの脅威		ネットワーク障害
			継続取引前提とする	継続取引前提としない	
金銭的損害	発注（個別契約） 納品 請求	なりすまし発注 情報財納品盗聴 なりすまし請求	無権限者による発注 発注／受注の否認 納品内容、納入日改竄 請求金額、請求日改竄	同左 （事前の取り決めの限界と教育に難）	取引情報が相手企業に到達しない
競争力 （機密情報漏洩）	（取引企業特定前） 仕様詰め （取引企業特定後） 開発詳細仕様 納品	開発情報盗聴 開発情報盗聴 開発情報財納品盗聴	開発情報を第3者に流す （継続取引を前提とした場合でも信頼関係樹立までは不安有り）	開発情報を3者に流す 不安大	
社会的信用 取引信頼関係	 納品		監査不適合 企業内の管理 取引相手企業の不祥事による影響 納期遅延 品質不良	監査不適合 企業内の管理 取引相手企業の不祥事による影響 納期遅延 品質不良	

(1) **説明１：金銭的損害**

第三者の脅威はなりすまし発注や請求、納品時の情報財の盗聴と悪用があり、これらは企業の損害となる。

また、当事者間の脅威は無権限者による発注、発注や受注の否認、納品内容・納入日の改竄、請求金額・請求日の改竄がある。但し、継続的な取引関係が確立された企業間ではこれらの脅威は下記理由で一般に起き難い。

① 故意の不正行為は、取引停止となり企業の経営を危うくする。

② 事前に取引上の取り決めを十分行っており、想定されるトラブルを回避出来る仕組みが作れる。

但し、継続的な取引を前提とした場合でも最初の取引とか継続取引を前提としない取引の場合は信頼関係が不十分なことと、事前の取り決め事項が不慣れなことに起因して、起きやすい。

従って、この脅威にどのように対応するかは重要である。

ネットワーク障害に起因して、取引情報が相手企業に到達ないことが有り得て（これは現在のクローズドＥＤＩでも起こり得る）発注側と受注側での取引の有無などによる損害が発生する。

(2) **説明２：競争力低下**

第三者が開発情報を盗聴し、悪用することが考えられる。

これは、調達企業では新商品情報が漏洩することになり、絶対避けなければならない。

また、当事者間の内部の人間が第３者に機密情報を流すことが考えられる。但し、これは現在の取引でも起きることであるが、電子情報の場合はその特性から簡単に盗み、ネットワークを通して証拠が残らないようにすることが容易である。そのための対策も重要である。

金銭的損害も損害の規模によっては、会社の経営を危うくし、新商品開発への原資の削減を余儀なくされ、競争力低下の間接的原因となる。

(3) **説明３：社会的信用失墜**

企業内部、外部（会計監査等）の監査不適合により、信用を失う。

(4) **説明４：取引信頼関係を壊すもの**

部品の納期遅延により、客先への納入が遅れ多大の迷惑をかける。この場合客先の信用は低下し、次受注に支障が出る。

納期遅延、品質確保が重要であり、そのため、企業を特定するプロセスでの信用調査、生産能力、品質管理面の調査がポイントとなる。

6.2 脅威対象別対応

取引企業を特定後のプロセスを中心に脅威対象別対応策を「表 6-2 脅威対象別対応策」にまとめる。

特記事項：継続的取引を前提としない場合

ある購入企業の無権限者がインターネットで不特定多数の企業を対象に部品調達をした場合、供給企業は確認をしないで製造し、購入企業に請求することになる。企業の管理責任は問われるのはもちろんであるが、1回限りの取引では供給企業は購入企業のしかるべき責任部門に確認する等何かしらのルールが必要と思われる。

表 6-2脅威対象別対応策

脅威対象 / 対応策	第三者からの脅威	当事者からの脅威		ネットワーク障害（伝送遅れ含む）
		継続取引前提とする	継続取引前提としない	
技術	○ デジタル署名 暗号化	○ デジタル署名 暗号化 タイムスタンプ ICカード	○ デジタル署名 暗号化 タイムスタンプ ICカード	△ 通信機器、実線の品質、回線容量
当事者間ルール	○ デジタル署名 暗号化を利用	○ 電子交換協定（アクセス制御、内部電子公証） 機密保護契約	△ 同左 （募集段階の社会的ルールが重要）	○ リトライ、不成立判断をルール
罰則	○ 刑事責任	△ （当事者間のルールで損害時負担）	△ （当事者間のルールで損害時負担）	○ 賠償責任（ネットワーク事業者）
保険	○ ニーズは高い	×	△	○ 罰則との整合
第三者機関TTPの電子公証	△ トラブル時当事者、第3者の原因究明	△：最初の取引 △：継続取引後（金額大）	○：金額大 △：金額小	×

凡例　○：対応が可能、必要　×：対応が困難 、不必要　△：中間に位置する

7 電子公証要求機能

第三者からの脅威（詐称、盗聴、改竄）と当事者からの脅威（故意によるもの：改竄・否認、故意によらないもの：錯誤）に対応することが必要であり、基本要件として

①誰が：本人を特定	認証 （注１）	デジタル署名、ＩＤ・パスワード
②何を：完全性	非改竄	デジタル署名、暗号化
③何時：存在したか	日・時付与	タイムスタンプ（注２）
④否認：送達・受信		デジタル署名と受信返信（ルール化 注３）
⑤否認：存在・内容		電子保存（保存性、見読性、完全性）

注１：認証局の認証書（申請法人の公開鍵、申請法人のＩＤ、有効期間、認証局の署名他）

注２：電子申請受付日（消印有効）の証明、発明時刻の証明他

注３：ルール化が基本であるが困難な場合（例：不採用通知）の対応として、第三者機関の活用他

が考えられ、これを要求機能としてまとめると次の通りである。

(1) **電子情報登録機能**
- ・電子公証機能を利用する企業登録する機能で認証局の認証書が必要

(2) **電子情報割印登録機能**
- ・契約書における当事者全員の署名付き電子情報の登録機能
- ・署名の認証は別途必要

(3) **電子情報日付証明機能**
- ・相手方と共通の日付の下に電子情報をやり取りしたことの証明機能（タイムスタンプ）

(4) **電子情報未改竄証明機能**
- ・送信したメッセージと受信したメッセージの同一性保証

(5) **電子情報到達（配達）証明機能**
- ・受信否認防止（応募、契約書、注文書、請書、請求書、採用・不採用通知等の到達証明）

(6) **電子情報発信証明機能**
- ・発進元の認証及び発信否認防止

(7) **電子情報保管機能**
- ・応募、契約書、注文書、請書、請求書、採用・不採用通知等に存在する電子情報および人事情報等社内における各種情報の蓄積機能

(8) **その他**
- ・暗号管理機能、鍵管理機能、追跡及びエラー処理機能他

尚、上記は企業間取引モデルから抽出された電子公証機能であるが、企業内業務の場合は「表 5-8 課題と解決策」にあるように承認行為の確認、機密情報に対するアクセス管理機能他が必要と思われる。

8 環境整備面の課題

(1) 電子保存データの証拠能力

日本において中央省庁が民間企業に対し法令により保存を義務づけている文書は９０９件にのぼる。それらのうち８４件の文書については既に電子媒体による保存が容認されており、さらに１５６件の文書についても電子媒体保存が容認される見込みである。現在電子媒体保存について検討中の文書も１６２件ある。実際政府はこれら法定保存文書や申請・申告については電子化を「原則容認」する方針を決定しており、早晩多くの法定保存文書は電子化されるものと考えられが、行政がこれらを容認する要件としては、一般に、記載事項の法定要件への合致、記録の正確性、安全性の確保、保存性の確保、可視性の確保、管理責任者の設置、秘密保持の確保、共通利用性の確保、主管官庁への事前届け出、一般に妥当と認められる基準での作成、などがあげられる。

また高度情報社会推進本部制度見直し部会では、電子媒体による保存記録が証拠として認められる要件として「データの真正性、見読性、保存性」が必要としている。ここで「真正性」とは「データの故意又は過失による虚偽入力、書き替え、消去及び混同を防止すること」、「見読性」とは「データの内容を必要に応じて見読可能な状態に容易にできること」、「保存性」とは「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」とあり、「真正性」についての議論を中心に進める必要があると考える。

(2) 契約の成立要件

企業間取引における契約の成立要件については、民法における「契約自由の原則」と民事訴訟での「自由心証主義」をとる日本では一般的に書面性が問題となることはなく、個別の案件ごとの対応となる。

「法廷証拠主義」をとる欧米などにおいては１６７７年に制定された詐欺防止法(Statute of Frauds)以来、契約に際して署名付書面が要求されている。アメリカにおいてもＵＣＣ(Uniform Commercial Code)で＄５００以上の商品売買や不動産売買などにおいて署名付書面が要求されている。さらに１９７５年制定のＦＲＥ(Federal Rules of Evidence)においてはさらにこれら書面の認証の必要性が規定されている。ＦＲＥにおける認証の要件としては、いくつかの段階があり、関係者同士による認定、専門家による比較による認定、認証可能な特徴・類似性による認定に加え、信ずるに足る認証プロセスや認証システムの利用も含まれており、電子的な認証について排除されているわけではない。実際電子商取引を推進するにあたってこの署名付書面の問題が浮かびあがっており、すでにユタ州、カルフォルニア州などのいくつかの州では電子署名付データを証拠能力のあるものとして認めつつある。現在電子時代の記録、認証、帰属、情報交換のあり方につき新たにＦＲＥ規定内容の修正を検討中でり、基本的には「署名」「書面」の概念を拡大解釈する方向で進んでいる。

(3) 契約の成立時期

民法では、契約は申込みの意思表示と承諾の意思表示の合致によって成立する。特に民法第５２６条（隔地者間の契約の成立時期）には「①隔地者間の契約は承諾の通知を発っしたる時に成立す」とあり、電子商取引は隔地者間の取引であるとの前提で、その成立時期は原則的に承諾が発信されたときである。

この「発信主義」の原則はもともと書類の送付しか意思伝達手段がなく、契約の承諾行為の到達に相当の日数が必要な時代に、例えば海外の取引相手に船で承諾の手紙を発信する場合などにおいて、契約内容の履行に早くとりかかることができるなどの意味を持っていた。

しかし、現在のネットワーク技術ではメッセージの到達は極めて短時間になされることと、不到達についても容易に知りうること、また不到達が判明した際にあらためて通知することも短時間に可能なことなどから、この「発信主義」については再考の必要があると考える。当電子公証検討ＷＧでは「即時性の高いネットワーク商取引においては契約成立時期を到達主義とする方向で進めるべきで、その際取引両者が発信・到達を確認する技術の必要性が高まる」という観点で議論を進めることとする。

但し、現状のクローズドな企業間ＥＤＩ取引では、申込だけで成立という扱いになっている場合が少なくない。これは継続的な取引関係にある当事者間では問題無いし、商法にも承諾が不要との規定がある（但し、「商人が平常取引を為す者より其の営業の部類に属する契約の申し込みを受けた」ときである）ことから、これらを否定するものではない。

電子商取引における契約成立時期を取引の形態で整理すると以下のようになる。

特定企業間	クローズドなＥＤＩ	申込の時点
特定企業間	オープンなＥＤＩ	到達主義
不特定企業間	オープンなＥＤＩ	到達主義
消費者－企業間	オープンなＥＤＩ	到達主義

(4) データメッセージの撤回・変更

電子データは一旦送信すると極めて短時間のうちに相手方に到着することから、実質上撤回とそれに伴う修正はデータ上だけでは難しい。撤回・修正データを認めるかどうか、どのようなデータについてどのような要件で認めるのかは取引の種類により異なり、基本的には当事者間の合意で処理すべき問題である。

(5) 無権限者による取引

発信人の認証については特定企業間のクローズドなＥＤＩではほとんど問題とならないが、オープンなＥＤＩでは問題となるし、不特定多数企業間取引・消費者取引となると相当深刻な問題である。企業間取引については現在の電子個人認証技術を利用してアクセス・コントロールは可能であるとの前提で、さらに企業内におけるアクセス権限の付与と「なりすまし」を排除する管理などのしくみについて検討を進める。

(6) 受信確認

受信確認とは、データの名宛人がデータを受領したことを発信人に対して確認するデータである。受信確認自体は、通常は意思表示と理解されていないから（受信確認が自動化されている場合もある）当然に承諾を兼ねうるわけではない。そうだとすれば、意思表示と評価できる承諾メッセージを改めて送らなければならない。いずれにせよ実際には受信を完全に確認する技術は取引当事者間のみではありえず、承諾メッセージまで含んだデータ交換についての取引当事者間の合意か、あるいは第三者の関与による解決が必要となる。

尚、現在インターネットＥＤＩのセキュリティ技術標準化の動きが急で、特にＩＥＴＦ(Internet Engineering Task Force)のＥＤＩ Interoperability Working Group（ＥＤＩＩＮＴ）において、暗号方式、鍵管理、非改竄保証、認証、否認防止、署名付き受信確認、履歴管理、エラー処理などオープンネットワーク上でのセキュリティ技術の標準化活動が進んでおりそのドラフトが作成されている。現在さらにCommerceNet 内のタスクフォースにてこのＥＤＩＩＮＴのドラフトにつき相互運用性についても検証中である。中でも署名付き受信確認の標準化については、本年３月末を目標に検証が進められている。

「参考」 CommerceNet 相互運用性検証タスクフォース参加企業

- Actra Business Systems (GEIS/Netscape)
- AT&T
- Atlas Products International
- CyberPath
- DanNet
- DEC
- EDS
- Harbinger
- Premenos
- Sterling Commerce
- U.S. Dept. of Defense

検討スケジュール

◇電子メール標準	ｓｍｔｐ／ＭＩＭＥ	１９９６年１２月完了
◇セキュリティ標準	Ｓ／ＭＩＭＥ	１９９７年2月まで
◇到達通知標準		１９９７年3月まで

(7) 否認

現状のクローズドなＥＤＩにおいて、特定多数企業間の継続的な取引を前提とした取引では否認は起きにくい。否認によるトラブルが発生した時点で継続的な取引関係が損なわれるからである。これらがオープンなＥＤＩに移行しても同様の理由から否認は起きにくいと考える。

一方、不特定多数企業間、消費者－企業間の取引のように継続的な取引を前提としない場合は否認は起きやすくなると考えられるが、不特定多数企業間についてのみ言えば、一般的に取引行為に入る前の情報交換時の否認であれば実質的な損失はほとんどないと考えられるし、取引行為に入る際には取引相手を選定（単にその存在のみならず、その開発能力・支払い能力なども）することがほとんどであることから通常は考えづらい。

しかし、あえて否認が起きうる特異な場面を想定して検討をした結果、いくつかの局面においては否認を技術や仕組みなどの対策を施せば防止は可能である。

(8) 損害に対する責任分担

不可抗力の事故も含めたネットワーク上の事故から生じる損害については、取引当事者、モール運営者、ネットワーク・サービス提供者、通信回線キャリアなどが関与するため複雑な責任分担となりうるが、基本的には個々のケースを想定した当事者間の合意、またはサービス事業者との契約で処理すべき問題である。

しかしいずれの主体にとっても際限のない責任分担を負う可能性があると、電子商取引の推進そのものをそぐ結果となりうることから、現状の通常取引においても機能している金融機関間やグループ企業間での互助機構や保険会社による損害保険機構を電子商取引についても展開されることが望ましい。

(9) データ交換協定

現在のクローズドなＥＤＩにおいて、取引の事前に当事者間においてデータ交換協定書が取り交わされることが基本となっている。これはオープンなＥＤＩに移行しても必要と考えられ、むしろ積極的に前述の諸課題に対する極めて有効な対策でもあると考える。

一般的にデータ交換協定書には、データ交換手段、データ交換通信業者、通信プロトコル、データフォーマット、データ記録保持方式などについて規定する必要がある。これらの内容については標準化やモデル化が進みつつあり、アメリカ法律家協会（ＡＢＡ）や国連欧州経済委員会（ＥＣＥ）、欧州連合（ＥＵ）などのモデルがあり、日本においても日本情報処理開発協会（ＪＩＰＤＥＣ）が試案を作成している。また日本電子機械工業会（ＥＩＡＪ）や石油化学工業協会（ＪＰＣＡ）などの業界団体においてもその業界ごとの商習慣を加味した標準契約書、モデル契約書が公表されている。

(10) 信用格付機関

電子商取引においては、取引当事者が対面することがないとするならば、所謂認証局とは別に取引の安全度を評価する格付機関のようなものが必要となろう。取引当事者が本当に安心するためには、代金払い込み後に商品未着等の事故が発生した場合に、損害を補填するような制度（保証・保険的機能）があればよいが、現実問題としてはこのようなビジネスの成立は困難である。ならば、「折衷案」として、全面的に損害は補填できなくても、格付けをして取引の安全度の目安を提供するという機関を設けてはどうだろうか。企業の信用格付けと同じように、その企業の電子商取引を行う企

業内システム安定度、運用の精度、過去の電子商取引の実績等により取引の安全度をランク付けする。但し、この機関の評価は、企業や債券の信用格付と同様に、取引に関する意志決定の判断材料の一つとすべきであり、万一損害が発生した場合の損害負担とは別問題である。

(11) 既存メディア（ＦＡＸ，ｔｅｌ等）と融合

本報告書の検討に際しては、企業の取引プロセスをオープンなネットワークへと移行した場合を想定して分析しているが、実際には効率性経済性を鑑みつつ部分的な局面から順次移行されるものと思われる。

その際、ある取引業務についてネットワーク処理を取り込みながらも、並行して紙や電話、ファックスなどの既存メディアが利用されるケースが多いものと考える。これはネットワーク上での取引交流の確実性を一層強化するための補完ツールとして意義があるが、同時に、例えば発注がネットワークで行われ変更・取り消しが電話でなされる、ネットワークで送信した内容と紙面上の内容が異なる、などの混乱を誘発する要因ともなりうる。

またタイムスタンプ機能についても、例えば契約日付と実際の契約書の授受のタイミングが異なるケースなどでは、タイムスタンプよりも契約書の内容の一部としての契約日付が優先されるであろうが、悪意をもてばタイムスタンプの有無に係わらず過去日付の内容を作成しうることも考えられないわけではない。これらは基本的には取引当事者間の取り決めの問題ではあるが、社会的にもいずれのメディアを優先するかについてのコンセンサスやガイドラインが必要となろう。

9 まとめ（今後の活動方針）

ここまでの議論を通じて、企業における実際の取引プロセスの中にはオープンなネットワーク上での取引へ移行するに際しての数多くの課題が存在し、そこに確実に電子公証ニーズが存在することを明らかにしてきた。しかもそれは企業間取引上の重要文書の交換だけにとどまらず、企業内における機密情報などについても対象となりうることも判明してきた。

しかしこれらネットワーク化への課題や電子公証ニーズへの対応については、単に技術的な対応だけにとどまらず、様々な運用上のルールや制度・環境面での整備も含めた総合的な対応が必要となることも事実である。またこれら電子商取引への環境が整ったとしても、利用者としての企業にとってはその必要性と経済性とのトレードオフで順次浸透が図られるものと考える。

従って今後の当ＷＧの進めるべき検討は、さらに企業活動領域を拡大しての課題分析と電子公証ニーズの抽出を進めながらも、同時に電子商取引などの電子交流を導入・展開・活用しようとする企業の視点から、具体的にどのような電子公証の仕組みの利用形態が考えうるのか、その際にどのようなことを準備する必要があるのか、それらの構成する実現可能な技術としてどのようなものがあるのか、などであると考える。

そこには取引当事者間だけのモデルから第三者機関が介在するモデルまでいくつかの視点

が必要となろうし、また企業内か企業外かは別としてこれらの電子公証機能をサービスとして提供する事業者の運用上の要件なども同時に明らかにしていく必要があろう。

検討を通して得られた課題を列挙すると

(1) **取引のルール化検討**

①募集～基本契約締結では対象が不特定多数がゆえの社会的ルールが必要。
やり取りを通して信頼関係の形成を実現するための公正、透明性や確実性が重要。
例：審査基準、採用・不採用通知義務、支払条件提示、機密保持等

②引合～決済では特定多数企業間の取引をいかに効率的に安全に行うかであり、木目細かい個別の契約が必要。
例：相互運用性のあるインターネットＥＤＩプロトコル
（暗号技術、鍵管理、非改竄保証、発信元の認証及び否認防止、署名受信または受信否認、追跡機能、２重発注防止、故意によらない錯誤等）や取引対象に応じた（機密情報、情報財の納品）取り決め

(2) **認証の取引局面別狙いとレベル**

認証は取引のどこの局面からが必要になるか、認証の対象取引情報は何か、認証の狙い・レベル・方法が取引対象毎どのように異なるのかを消費財の取引、不動産の取引等を通して明らかにする。

(3) **電子公証ニーズとレベル**

電子公証のニーズを物財・情報財の開発品をモデルに公募～決済までのプロセスで検討したが、ニーズ幅広いの把握とニーズのレベルをより具体化するための新たなモデルでの調査が必要。

(4) **電子公証技術及び電子公証システム**

(5) **電子公証実現に必要な法的課題**

(6) **電子公証システムの運用の在り方**

中小企業の利用を視野に入れた経済性、利便性、効率性、証拠性等確保

(7) **企業内業務と企業間取引のボーダーレス化に伴う連続性確保の検討。**

公開鍵インフラやＩＤ，パスワード導入の諸問題、安全性、信頼性、機密性確保、社会的信用（監査）

「おもな参考資料」

１．電子取引 日本再生の条件　　Ｈ８年３月　石黒　憲彦
２．企業取引法入門　　Ｈ８年３月　岸田　雅雄
３．ネットワーク社会のセキュリティ　　Ｈ７年８月　藤原　宏高
４．遺言・公証　　倉田　卓次
５．電子商取引に関する検討課題について
（電子商取引環境整備研究会中間報告）　　Ｈ８年４月　通商産業省
６．電子決済、電子現金とその利用環境整備の関する調査研究会
（暗号政策と電子現金）　　Ｈ８年４月　郵政省電気通信局
７．電子情報技術（ＩＴ）を活用した産業のダイナミズム回復のためのプログラム
Ｈ７．１０通産省　機械情報産業局
８．Ｓｕｒｅｔｙ社のＤｉｇｉｔａｌ　ＮｏｔａｒｙTM サービス
９．電子決済研究会報告　　Ｈ８年３月　(財）金融情報ｼｽﾃﾑｾﾝﾀｰ
１０．エレクトロニックコマース革命
（インターネット時代の電子決済システム）Ｈ８年４月　山川　裕　日経ＢＰ社
１１．流通業における電子化取引標準化　調査研究報告書
Ｈ８年３月（財）流通ｼｽﾃﾑ開発ｾﾝﾀｰ
１２．米国の暗号輸出規制（クリッパー模索）キーエスクロー
１３．暗号（ポストモダンの情報セキュリティ）　Ｈ８年４月　辻井　重男
１４．商品先物取引　　Ｈ８年８月　角川　総一
１５．米国における電子金融・電子商取引に関する動向調査
10/20-30 一橋大学　経済研究所教授　　浅子和美(前 FISC 電子決済研究会座長)
電子決済・電子認証・電子マネー
１６．アジアの電子業界におけるＥＤＩの動向　　社　日本電子機会工業会
ＥＤＩセンター　榊原　康行
１７．これからの社会的規制　　社会的規制研究会
１８．電子取引調査研究会報告書　　Ｈ４年３月　　産業情報化推進ｾﾝﾀｰ
１９．電子商取引と法（１）～（４）　　ＮＢＬ　東京大学教授　　内田　貴
２０．ＥＤＩ契約の実務上の留意点（上、中、下）ＮＢＬ 弁護士　　室町　　正美
２１．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
２２．帳簿書類の保存等の在り方について（案）　Ｈ９年３月２６日
帳簿書類の保存等の在り方に関する研究会

平成９年５月発行
発行：電子商取引実証推進協議会
東京都江東区青海２－４５
タイム２４ビル１０階
Tel　03-5531-0061
E-mail　info@ecom.or.jp