H11－認証・公証WG－1

企業間電子商取引への認証技術の適用

平成１２年３月

電子商取引実証推進協議会

認証・公証WG

はじめに

JIPDEC とアンダーセン・コンサルティング社との共同調査によれば、１９９８年時点では、わが国の BtoC の市場規模は６５０億円であり BtoB の市場規模は 8.6 兆円である。また 2003 年時点での市場規模ははそれぞれ 3.2 兆円、68 兆円と予測されている。BtoC は一方のプレーヤである消費者が個人であって、企業のような集団的意思決定メカニズムが無く、各人の行動様式があるベクトルを形成するまでに時間の掛かる特徴があるのに対して、BtoC は既存の取引形態をより効率的なものに改善する動き（BPR：Business Process Reengineering）と捉えることができ、投資に対する経済的効果によってのみその方向が定まるので、はるかに動きが速く、その方向も予測しやすい。認証の検討は BtoC から始まったが、BtoB の方がはるかに市場規模が大きく、その動きも速いのでガイドライン等の環境面での整備が急がれている。

BtoB の EC は既存の EDI などの流れの延長線上にあり、ビジネスの形態面でマクロに見ればその変化はごくゆるやかである。現行の企業間取引のほとんどは特定の相手との間での継続的取引であり、EC になってもその大半はこのような特定企業の集団に閉じて行われる。この場合には、企業集団が形成される過程において契約を取り交わすことができ、認証に関する各種の約束事を契約の中で取り決めることが出来る。ここではこのようなクローズな環境での取引形態を契約型取引と呼ぶ。

一方、上述のような契約関係を事前に結ぶことが出来ない、いわば毎回新規取引を行う形態は現在あまり例を見ることは出来ないが、オープンネットワーク利用がもたらす新しいビジネス形態として想定することができる。ここではこのようなオープンな環境での取引形態を公募型取引と呼んでいる。

電子的手段による取引契約についてさまざまな観点から議論が行われているが、これらの議論はここでいうオープンな環境を想定することにより抽象論に終始している場合が散見される。BtoB の EC における認証の適用の検討に際しては、これらの議論の抽象性に惑わされることなく、クローズな世界から始めるプラクティカルなアプローチをするべきである。

認証は電子的手段によらない従来の取引においても行われてきた機能であり、独立な主体間の契約とその遂行という取引行為の性質自体から必然的に要求されてきたものと考えられる。この必然性は取引の実現手段とは独立に生じるものと考えられるので、当 WG での検討は従来の取引の各段階における認証の必要性の分析から始める帰納的アプローチを採った。

また当 WG では企業間 EC への認証の適用と並んで公証の適用を検討してきた。H11 年度の報告書では、公証を取引に伴うトラブルを事前に防ぐための機能と捉え、さらにその本質は第三者対抗要件であると考えてきた。ここでいう第三者が全くの第三者であるか、それとも上述のようなクローズな企業集団の一員ではあるが取引当事者ではないと言う意

味での第三者であるかが、当 WG の検討スコープに大きな影響を与えると考えた。全くの第三者の場合には、従来は公証人役場の機能が利用されており、その電子化は別の場で検討されているため、当 WG で新たに検討しないことにした。もっぱら企業集団内の第三者対抗要件を意識する公証機能を検討対象とし、公証人役場の機能と区別するためにこれを「私的公証」と呼んだ。この検討は今年度も継続してきたが、今年度報告書では混乱や誤解を避けるために、あえて「私的公証」と言う言葉を使わず、「トラブルを回避するための要件ないし方策」と言う表現をしている

企業間電子商取引の展開に際する認証の具体的適用局面において、本ガイドラインがその検討の一助になれば幸いである。このガイドラインは初版であり、実際の適用から得られた教訓をフィードバックできれば更に良いものにして行けると考えている。

連絡先

電子商取引実証推進協議会(ECOM)
認証・公証ワーキンググループ
〒135-8073
東京都江東区青海 2-45 タイム 24 ビル 10 階
TEL：(03)5531-0061
FAX：(03)5531-0068
E-mail：info@ecom.or.jp
http://www.ecom.or.jp

目次

第1章　企業認証の適用

1.1　アプリケーションモデル

1.1.1 企業間電子商取引のプロセスと認証の必要性について

(1)　リアル世界におけるビジネスプロセスと認証について

①　プロセスのモデル

リアル世界における企業間商取引の標準的なプロセスモデルは、契約、発注、納入、検収、決済の各ユニットによりとらえることができる。また、契約前におけるプロセスについては、取引の性格・状況により特定の相手との個別契約による場合と、不特定多数と契約をおこなう場合の２つの場合に分かれる。

一連のプロセスモデルを図で表すと次の通りとなる。

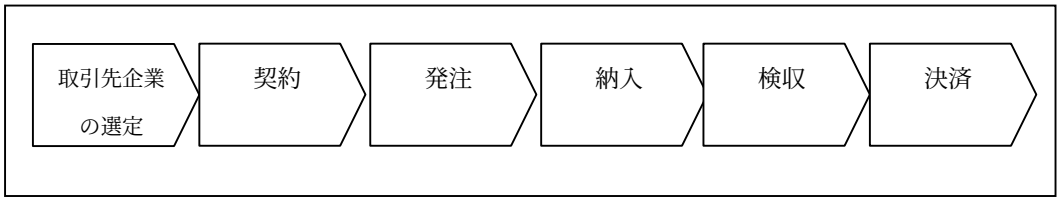


図 1-1　企業間商取引における標準的なビジネスモデル

また、上記モデルを構成する各ユニットの位置づけは次のようになる。

＜１＞　取引先企業の選定

取引先企業が特定の相手なのか不特定多数なのかを判断し、取引先を具体的に選定するユニット

＜２＞　契約

企業間取引を開始させるユニット

＜３＞　発注

上記の契約内容にもとづいた発注行為を実際にはじめるユニット

＜４＞　納入

上記の契約内容にもとづき、購入商品を発注企業に納めるユニット

＜５＞　検収

発注企業が商品納入後、当該商品が上記の契約内容にもとづいていることを確認するユニット

＜6＞　決済

発注企業が受注企業に対して、契約内容にもとづき、決済機関を介して、もしくは当事者間で直接、購入代金を支払うユニット

② 各ユニットにおける認証行為の機能と手段

これら一連の企業間商取引ユニットの遂行上、商取引当事者間双方の不利益やトラブルを避けるために、各々のユニットにおける真正性を確保することが必要である。このために多様な認証機能が存在する。この認証機能が用意されていないと、商取引ビジネスそのものが円滑に運用されなくなる可能性がある。

リアル世界での企業間取引においては、対面取引かつ書面の存在を前提としたビジネスプロセスモデルの中で互いの認証機能が形成されている。

この場合、実際には認証とは呼ばれていないが、対面取引下での状況や行為、また書面を通じて、取引当事者間における相手の特定と確認やビジネスプロセスユニット単位の真正性確保を行っており、実際には意図せずして認証をおこなっているといえる。

次に、ビジネスモデル各ユニット単位にリアル世界における実際の認証方法をみていくことにする。

表 1-1　リアル社会における認証

	認証の機能と対象範囲	認証方法
取引先企業の状態	【企業実在性確認】 当該取引企業が実際に存在していることを確認する	－第三者の証明を利用する方法 ・登記簿謄本／抄本 ・取引金融機関からの実在証明等 －広告媒体やその他機関を利用し、契約当事者の情報を入手する方法 ・一般広告媒体 ・信用機関による企業調査
	【企業所属個人実在性確認】 取引個人がその企業に実際に所属していることを確認する	－物理的（対面的）方法 ・企業所属名刺の授受 ・外見、容姿等による個人属性情報の取得 ・取引先企業を実際に訪問することによる確認 ・取引先企業へ実際に電話をすることによる確認

	認証の機能と対象範囲	認証方法
取引先企業の状態（前ページからの続き）	【企業信頼性確認】 取引企業が取引をするに値する信頼性があるかを確認する	－取引企業の開示資料を利用する方法 ・有価証券報告書 ・－決算書 ・ディスクロージャー資料
契約	【企業本人意思確認】 契約内容が取引企業の企業意思によるものであることを確認する 【契約内容存在確認】 契約内容が取引企業の企業意思によるものであることを確認する	－契約書類を取り交わす方法 ・契約内容項目の記載 ・企業代表者の署名、社印の押印 ・契約当事者の署名、捺印 ・契約締結日時記載 ・契約書の送付／受領確認
発注	【受注事実確認】 発注企業が発注した事実を証明し、受注企業は発注した事実を確認する 【発注完了確認】 受注企業が受注した事実を証明し、発注企業は受注した事実を確認する	－発注書類を取り交わす方法 ・発注確認項目の記載 ・発注当事者の署名、捺印 ・発注日時記載 ・発注書の送付／受領確認
納入	【納入事実確認】 発注企業が納入した事実を証明し、受注企業は納入した事実を確認する 【受領確認】 受注企業が納品した事実を証明し、発注企業は納品した事実を確認する	－納入書類を取り交わす方法 ・納入確認項目の記載 ・契約当事者の署名、捺印 ・納入日時記載 ・納入書の送付／受領確認
検収	【検収事実確認】 受注企業が納入商品について契約内容と相違ない事実を発注企業へ確認する	－検収書類を取り交わす方法 ・検収確認項目の記載 ・契約当事者の署名、捺印 ・検収日時記載 ・検収書の送付／受領確認
決済	発注企業が購入代金を支払済であることを証明し、受注企業が購入代金を受取済であることを確認する	－決済機関の認証機能を利用する方法 ・支払者が購入代金を支払済であることを決済機関が証明する 購入者が購入代金を受領済であることを決済機関が証明する

(2)　バーチャル世界への移行に伴う（の実現に向けた）電子認証の必要性

①　何故認証が必要か？

バーチャル世界での企業間商取引においても、基本的にはリアル世界での企業間商取引とそのプロセスは同じであり、そのプロセス中の認証に関しても同様に必要である。しかしバーチャル世界での企業間商取引においては、対面取引と異なり電子的書面を通じて取引のプロセスが進行するために、認証に関しても以下に挙げられる対応が必要となる。

まず第１になりすましへの対応である。リアル世界における対面または電話の声などによる取引相手の確認と異なり、バーチャル世界では電子的に他者に成りすますことが可能である。そこで、バーチャル世界でインターネットを介して電子的書面により商取引を行っている（行おうとしている）相手が、正当な相手なのか他者がなりすましたのかを確認する必要があり、不正な相手と商取引を行ってしまうことへの防止のためにこの対応は必要である。

第２に電子的書面の改竄や複製への対応である。紙による書面と異なり電子的書面の特徴として、複製しても劣化しないことと、内容の改竄が容易でかつその痕跡が残らないことが挙げられる。これにより、まずは不正に複製された電子的文書が使用される可能性がまず考えられる。次に実際に商取引を行うべき本来の取引内容を示した電子的書面とは異なる内容の電子的書面が商取引の場に不正に使用される可能性がある。従って、バーチャル世界でインターネットを介して手許に届いた電子的書面の正当性及び完全性の確認が必要であり、不正に改竄された電子的書面を扱うことを防止する対応が必要である。またさらには、契約原本または原本とみなされる電子的書面に対する改竄、紛失、漏洩、悪用等を防止する善管義務が契約当事者及びその責任主体に生じることは、リアル社会における契約行為と全く同様であり、その管理の際にも認証は重要な機能となる。

このように、正当な内容の電子的書面で、正当な相手とバーチャル世界での商取引を行っていくために、相手の特定と確認及び電子的文書の正当性と完全性を保証する手段が必要である。この際の電子的書面の内容証明（原本または原本とみなせる）機能が公証の機能であり、当事者（責任主体）確認と、その正当権限者の権限確認が認証の機能である。

②　認証の機能と対象範囲

認証の機能レベルには、アプリケーションの要求によって以下のようなレベルが考えられる。

（ア）　本人性・実在性を確認する

（イ）　（ア）＋権限・資格を確認する。

（ウ）　（イ）＋与信

また、企業認証の認証対象（エンティティ）としては、次ぎの３つが考えられる。

– 代表者
– 権限を委譲された個人
– 企業

これらのエンティティとしてどれを採用するかは、取引の環境・条件・当事者間の合意等によって定まる。これは、リアル世界での商取引においても、同様に行われていることである。このため、全ての取引を企業の代表者が行うわけではなく、権限を委譲された担当者が行うこととなる。

従って、認証のどの機能レベルをどのエンティティに付与し、運用していくかに関する企業内認証局・登録局の取り決めが必要である。

(3) 企業間電子商取引における認証モデルについて

認証モデルについては、大きく以下の２つのモデルを考える。

– クローズドモデル（契約型取引モデル）
– オープンモデル（公募型取引モデル）

（１）で見てきたリアル世界におけるビジネスプロセスをバーチャル世界に適用させた場合、契約から先のプロセスにおいてはどの商取引においても同様のプロセスが適用されるが、契約前におけるプロセスにおいては、次の２つの場合に分かれる。

まず第１に、特定の相手との個別契約により契約以降のプロセスが電子的に実施される場合であり、クローズドモデル（契約型取引モデル）と呼ぶ。この場合、認証の対象となる取引相手は限定されており、商取引を行う企業間相互の取り決めにより認証の方法及び適用の決定がなされる。

第２に、バーチャル世界において取引先の募集から行い、基本契約までを電子的に行う場合であり、オープンモデル（公募型取引モデル）と呼ぶ。この場合、認証の対象となる相手は不特定多数であり、第三者の認証による実在証明や信頼性証明が必要となる。この場合、契約以降のプロセスは当事者間の合意・契約によるプロセスとして、クローズドモデルと同様のプロセスが適用される。

次でそれぞれのモデルの詳細について触れたい。

1.1.2 契約型取引モデル

ここで、企業認証における「契約型取引モデル（クローズドモデル）」を定義する。契約型取引モデルとは、取引を行う企業群があらかじめ定まっていて閉じた世界を形成しているモデルである。このモデルでは、取引企業間、もしくは取引企業集合を代表する機関等があらかじめ構築した認証局が認証管理の主体を行う。つまりあらかじめ想定される閉じた世界及びそこで使用されるアプリケーションにおいてのみ、認証が使用されるようなモデルである。従って、その認証管理の運用ポリシー及び仕組みに関しても、そこで使用されるアプリケーションに特化したものを利用することができる。

このようなモデルに関して、以下でその特徴を考察する。

(1)　プロセス

①　契約時における認証利用方法の取り決め

契約型取引モデルにおいては、一般的に、最初に認証が必要とされるアプリケーションが決定される。そしてそのアプリケーションにより取り扱われるデータに対して要求されるいくつか要件により認証の方法が決められることとなる。ここで考慮すべき要件には以下のものが考えられる。

- セキュリティのレベル
- 認証局（／登録局）の運用形態
- ユーザビリティ
- 費用
- etc.

これらの要件を考慮した上で、認証の技術的方式、さらには認証局の具体的な運用といった認証の仕様が取り決められる。この認証の仕様の取り決めに関して、B-to-Bにおける場合を考えると、代表的なものとして２つのケースが考えられる。

第１は、企業グループ内での取引及び情報交換に認証を使用するものである。例えば、グループ企業間の資材調達といったＳＣＭ (Supply Chain Management)、さらには、下請けに対する業務委託に関するやりとり、といった数々の場面が考えられる。一般に、これらのアプリケーションの仕様は、その企業間の情報通信方法を含めて、企業グループにおける親会社もしくはその意向を受けたグループ内システム開発会社により決定される。このとき、アプリケーションにおけるセキュリティ要件が定義され、その中の一項目として、認証に対する要件が定義される。認証局が必要とされる場合には、定められたポリシーに基づき、親会社もしくはそれを代行するグループ内の会社が、それら認証局などの認証管理の主体となり、例えば、電子認証書、ユーザＩＤ／パスワード等を発行する。

もう１つは、その取引及び情報交換の範囲が、企業グループをまたがる場合である。企業グループ内取引からの拡張として、他企業がその取引に参入してきた場合、もしくは業界において特定の企業グループが寡占的な位置を占める場合には、企業グループ内の認証の仕組みがそのまま利用されると思われる。しかし、貿易 EDI のように、当初から企業グループをまたがって、アプリケーションの仕様が設計される場合には、一般に、業界団体、及びそのために組織されたコンソーシアム等が、その役を担うことになる。そこでは、認証のためのポリシーも定義され、実際の認証局／登録局の運用フェーズにおいては、業界団体／コンソーシアムがそのまま認証管理の主体となることも可能であるが、そのための会社の設立、もしくは認証サービス会社に対する業務委託という形態をとることも考えられる。

②　認証対象の登録

アプリケーションでユーザの認証を行うためには、あらかじめユーザとしての登録

がなされる必要がある。ユーザはアプリケーションにおいて認証されるために、そのユーザ固有の知識／物／身体的特徴等を電子的な情報として提示する。そのためにこれらの情報はあらかじめ、登録申請者の確認とともに、固有の情報として登録されなければならない。

BtoB においては、企業が認証の対象となり、その登録を確実なものとするための申請者確認の方法としては、申請時に公的な物として、商業登記に基づく登記簿謄抄本、登録印鑑の押印及び印鑑証明書の提出などが考えられる。但し、企業グループ内における認証の場合には、認証局を運用する会社／部門により、あらかじめグループ内企業における各アプリケーション業務の担当部門／担当者が知らされていることもあるため、より簡便な方法として、認証局から直接にそれら担当部門／担当者に対して、認証のための情報、例えばユーザＩＤ／パスワード、またはＰＫＩにおける鍵ペアなどを安全に配布するなどの方法も考えられる。

③ 認証の利用

認証のための登録が完了すると、アプリケーションにおいて実際に認証が使用されることとなる。認証に使用される鍵は、当初に定められた認証のポリシーにより、企業、部門、個人、及びアプリケーションなどを単位として作成／管理される。いずれの場合においても、各企業内でそのポリシーをよく理解した上で、鍵の使用及び管理に関する規定をまとめ、各人がそれを遵守する必要がある。

(2) 運用上の留意点／特徴

① 認証システムの継続利用を可能とするために維持管理できるルール、仕組み作り

契約型取引モデル（クローズドモデル）において構築した認証システムを継続的に利用していくためには、いくつかの注意すべき事項が考えられる。上述したように、このモデルは、特定のアプリケーションでの使用を前提にした認証モデルである。そのような場合、特に、認証システムが継続的に信頼おける物であるためには、ユーザの登録管理が重要な課題となる。つまり、企業ユーザは一度登録された後にも、そのアプリケーションを使用する権利／資格を喪失した場合には、直ちに登録が取り消されなければならない。そのためには、以下のような項目に関して、特別な考慮がなされる必要がある。

- 認証の有効期間
- 組織や担当の変更など登録事項の変更に関する認証局に対する報告義務
- 登録企業に関する情報の入手手段の確立
- etc.

1.1.3 公募型取引モデル

(1) オープンモデル定義及び特徴

オープンモデルとは、取引参加者が特定のメンバに固定されず、広範囲かつオープン

に取引相手を求める形態であ。具体例としては、オークション、公開調達などが考えられる。当モデルでは、身分確認に用いる認証書は認証モデル内の代表企業が発行したものではなく、一般の認証局が発行したものである。

(2)　オープンモデルで利用される認証システム

利用される認証局は、公募企業によって選択される。この際選択される認証局は以下のような要件を満たしている必要がある。

1. 公募企業により信頼のある認証局であると認められる事
2. 公募企業が提供するサービスに認証ポリシーが適している事
3. 公募企業が提供するサービスに認証行為の内容が適している事

公募企業によって選択される認証局は複数存在しうる。

(3)　オープンモデルへの参加要件

応募企業は、公募企業によって選択された認証局のうち、少なくとも一つの認証書を所有する必要があり、これをもって当認証モデルへの参加要件とする。

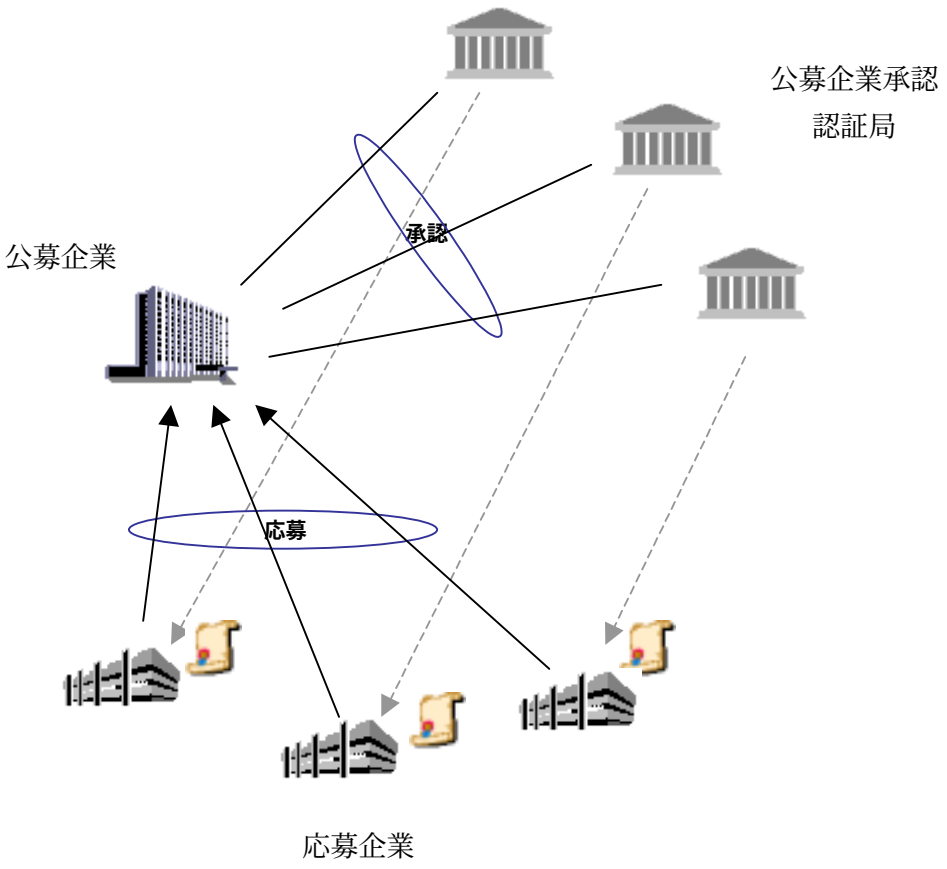


図 1-2　オープンモデル認証局選定～応募企業参加まで

(4)　オープンモデルのビジネスプロセスについて

オープンモデルでのビジネスプロセスは以下のようになる。

① オープンモデル参加企業リストより取引相手を選定する
　公募企業は、参加企業リストから取引相手を選定する
② 外部認証システムを利用し、取引相手の実在性の確認を行う
　上で選定した企業が属する認証局に対して実在性の確認を行う
③ 相手の信用調査などを行う
　公募会社は、契約を締結するにあたり、取引相手の信用調査などを行う。
④ 契約を締結する

取引が継続的なものになる場合、クローズドモデルの認証に移行することが考えられる。

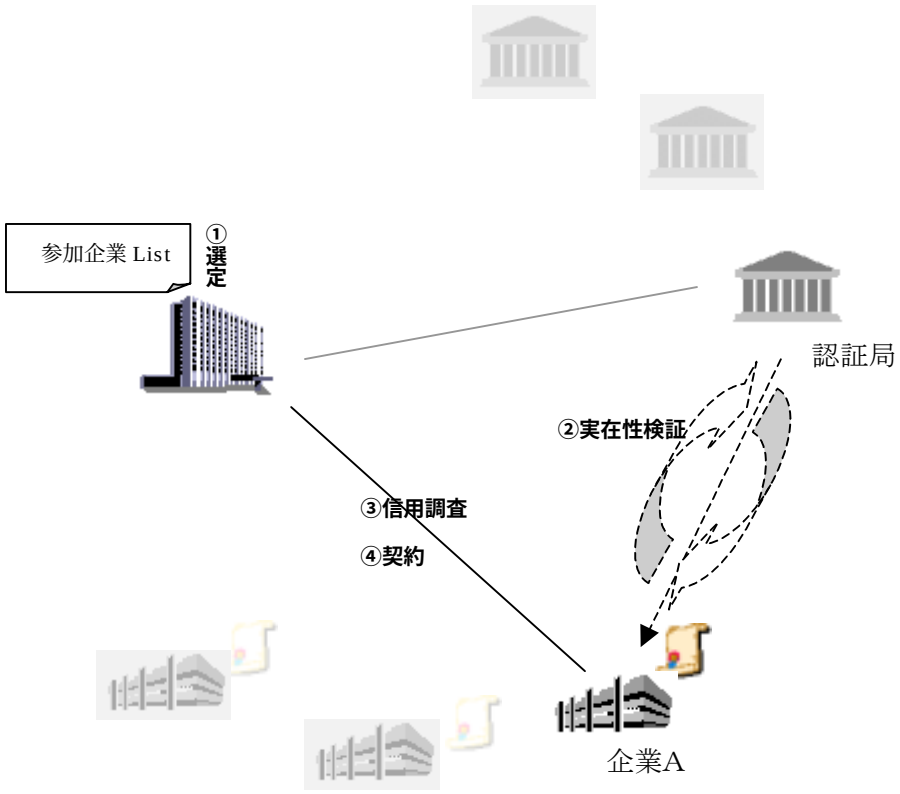


図 1-3　オープンモデル内ビジネスプロセス

1.2　認証の適用技術

1.2.1　二者間認証と三者間認証

認証は事前の登録を前提として、ある人（企業）が事前に登録したその人（企業）であることを確認する行為である。企業間電子商取引における認証の具体例としては、ある企

業コンソーシアム内における電子商取引に先立って、相手企業がそのコンソーシアムのメンバ企業であることの確認を行う場合が挙げられる。この場合、そのコンソーシアムのメンバになることが上述した登録に該当し、確認は具体的な取引トランザクションの都度行われる。

すなわち、認証は、登録管理者（上記の登録を管理する人または組織）、認証者（相手を確認したい人または組織）、認証請求者または認証の対象者（相手に自分が登録してあることを主張する人または組織）の３種類のプレーヤによって構成される。ここで認証者と認証請求者（認証の対象者）とは各個別の取引トランザクションの通信当事者である。

認証の方法は、上記のプレーヤと取引トランザクションの流れとの関係によって、二者間認証と三者間認証とに分けることができる。登録管理者が常に認証者に成り得る取引形態の場合が二者間認証であり、登録管理者が認証者とは別である場合が三者間認証である。二者間認証は取引が常に登録管理者である組織とそれ以外の組織との間でのスター型で行われる場合に可能な方法であり、三者間認証はそれ以外の形態、すなわち登録管理者以外の組織同士の間で取引が行われるネット型に対応できる方法である。

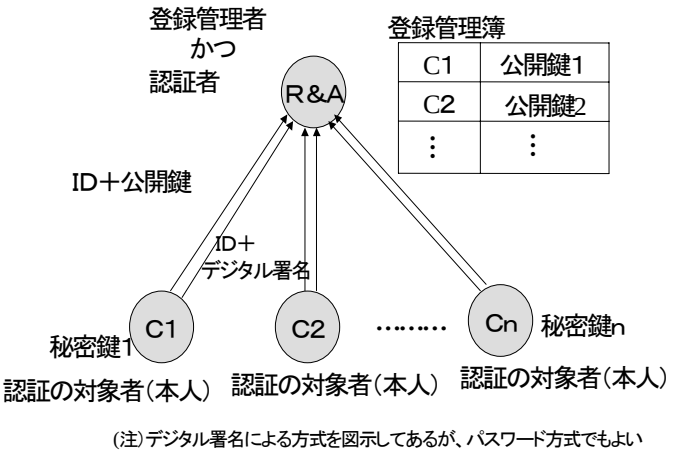


図 1-4　二者間認証

認証の対象者は認証者に対して、自分が事前に登録した本人であることを証明する必要がある。そのためには登録時に自身しか知らない（または自身しか持ち得ない）情報を登録しておき、認証時にこれを示すことによって上記の証明を行う。この情報を認証情報と呼ぶ。認証情報としては、指紋や筆跡などのバイオメトリクス、パスワードやデジタル署名などの秘密情報が使われる。（この他に、社員証やパスポートなどの所有物も広義の認証情報として用いられてきたが、ネットワークを介して提示することができないので、所有物に関してはここではこれ以上触れない。）

二者間認証においては、認証者がすなわち登録管理者であるので、登録された認証情報は認証者の手元にあって、認証者が自由に参照できるので、提示された認証情報と登録してある認証情報との照合に際して特別な処理は不要である。

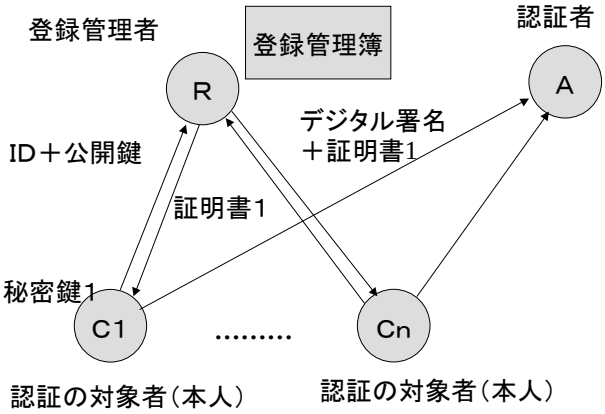


図 1-5 三者間認証

一方、三者間認証においては、認証者が認証情報の照合を行う際に、登録してある認証情報を得るための特別な手段が必要になる。そのためには認証者から登録管理簿にアクセスする特別なパスを設定する考え方もあるが、現在一般的に使われているのは、認証の対象者が認証者に示す証明書（認証書）中にこれを置く方法である。すなわち、証明書（認証書）は登録管理者から認証者に登録済みの認証情報を伝える媒体としての役割も担っている。上述したように、二者間認証では、このような仕組みは不要である。

1.2.2 二者間認証

三者間認証は取引形態に制約が無い一般的な方法であるが、二者間認証の方が認証書にかかわる仕組みが不要なため低コストで実現できる可能性がある。部品調達のような企業グループ内で行われる企業間電子商取引の取引形態は中心企業（部品調達企業）と各部品メーカとの間でのスター型であり、現実には二者間認証で十分なケースもかなり多い。

(1)　サーバ認証／ＩＤパスワード認証

企業間取引を安全に行うためには、その取引の両端において互いに相手が誰であるのかを確実に知ることができる必要がある。例えば、あるトランザクションが、アプリケーション・プログラムが実行されるサーバ上において行われる場合には、ユーザは、まずそのサーバ／アプリケーション・プログラム（以下、認証の主体としては、サーバとアプリケーション・プログラムを区別しない）が確実に自分の望む組織／団体（／個人）

により運用されていることを確認するとともに、反対にサーバ側でユーザ自身が認証されるための何らかの情報を提供しなければならない。このような場合に使用される認証方式の１つが「サーバ認証／ＩＤ パスワード方式」である。

ここでは特に、ユーザはブラウザを使用し、アプリケーション・プログラムは Web サーバ上で実行されるものとし、そのサーバの認証に使用される認証書は X.509 に対応している事とする。

① 方式の特徴

一般にこの方式においては、ユーザは最初のサーバ・アクセス時、またはアプリケーションに対するアクセス時にデジタル認証書によりサーバの確認を行うとともに、暗号化された安全なセッション上で、サーバがユーザの認証を行うためのユーザＩＤとそれに対応するパスワードを提示する。つまりユーザは自身の認証に関して、デジタル認証書を使用する必要がないために、その取得及び運用管理に関わる手間から解放される。しかしながら、一般的にセキュリティの観点からは、ユーザＩＤ／パスワードはユーザの知識のみによる管理になること、さらにはサーバ側にそれらの情報が一元的に管理されることになりがちであることなどにより、漏洩の危険性が大きくなる可能性があることをシステム構築及び運用時には考慮しなければならない。

② 具体例

ユーザ認証のためにユーザＩＤ／パスワードを使用するシステムを構築するにあたってはいくつかの方法が考えられる。ここではそれらの中で代表的と考えられるものをいくつか挙げる。

A. サーバ毎にユーザＩＤ／パスワードを管理

ユーザ認証が必要とされるアプリケーション・プログラムが実行されるサーバ上に、ユーザＩＤ／パスワードをともに保管する方法である。システム構築／運用が容易ではあるが、アプリケーション・プログラム及びコンテンツ管理者とユーザ認証の管理者が同一でない場合には、ユーザＩＤ／パスワードの保管方法、サーバのルート権限の管理、アプリケーション・プログラム及びコンテンツの更新管理等の運用方法を充分に検討する必要がある。

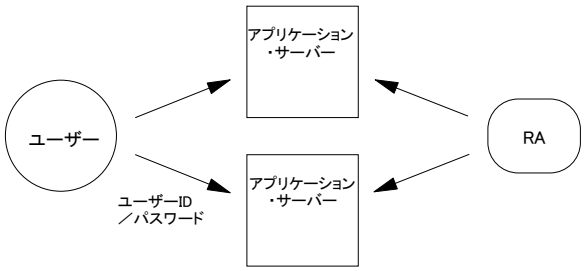


図 1-6　アプリケーションサーバによる管理

B.認証サーバを設置し、ユーザＩＤ／パスワードを一括管理

アプリケーション・プログラムが実行されるサーバとは別に、ユーザＩＤ／パスワードを管理する別のユーザ認証用のサーバを用意する方法である。ユーザＩＤ／パスワードの管理と、アプリケーション・プログラム及びコンテンツの管理をサーバ単位で別々に行うことができる。ただし一般的に、ユーザＩＤ／パスワードはセッション上でしか暗号化されないため、一時的にせよ、アプリケーション・サーバ上で暗号化されない状態でそれらの情報が存在することがあるため、必要に応じて、そのための対策をとる必要がある。

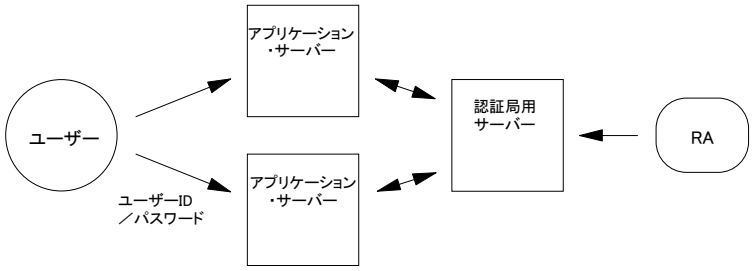


図 1-7 認証サーバによる管理

C.シングル・サイン・オン製品を利用したユーザＩＤ／パスワードの一括管理

ユーザはアプリケーション・サーバに対して直接に自身の認証を要求するのでなく、シングル・サイン・オン（ＳＳＯ）・サーバに対して認証を要求する。アプリケーション・サーバはこの認証情報に基づいて、ユーザの認証を行う方法である。ＳＳＯサーバのタイプには、ＳＳＯサーバ自身がプロキシーとして動作するようなプロキシー・タイプや、またＳＳＯサーバとの間に確立した認証情報を Cookie として利用する Cookie タイプなど、いくつかのタイプが存在する。アプリケーション・サーバの構成、さらには必要とされるセキュリティ要件等を充分に検討した上で、適当な方式を選択する必要がある。

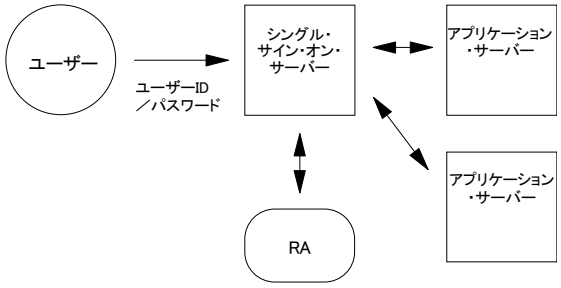


図 1-8 シングルサインオン製品の利用

③ その他、補足事項

「サーバ認証／ＩＤパスワード方式」は、その他の認証方式に比べて、極めて容易にユーザ認証を行うことができる方式であるといえる。しかしながら、上述したよう

に一般的に、ユーザＩＤ／パスワードといったユーザの持つ知識にのみ認証が依存する点、さらには、それらの情報そのものが、サーバ側において一括して管理される点などから、その漏洩を防ぐ手段に対しては充分な配慮が施されなければならない。サーバ側におけるユーザＩＤ／パスワード管理、つまり管理者の役割分担及びシステム上のユーザＩＤ／パスワード保護機能などはもちろんのこと、特に、ユーザ各々におけるパスワード管理がおろそかにならないように注意／指導が徹底される必要がある。ユーザ側からの認証情報を防ぐための手段としては、ユーザＩＤ／パスワードをＩＣカード内に保管／管理するなどの方法も考慮するに値する方法の１つである。

(2)　公開鍵方式

認証情報として公開鍵暗号を利用したデジタル署名を使う方式であるが、二者間認証では証明書（認証書）を使う必要が無く、そのための認証局も不要である。正確に言えば、認証局の機能の内で認証書発行にかかわるＩＡ（Issuing Authority）機能は不要であるが、登録を管理するＲＡ（Registration Authority）機能は必要である。登録は認証の基本的大前提であるので、どのような方式を採るのであれ、登録をつかさどる機能が不要になることはない。

デジタル署名を使う認証は認証者がデジタル署名の検証を行うことによって認証の対象者が登録されている本人であることを確認する。このときに使う公開鍵を得る方法が二者間認証と三者間認証とでは異なる。後述するように三者間認証では認証の対象者がデジタル署名に添付して提示する証明書（認証書）から公開鍵を得るのに対して、二者間認証では直接登録管理簿から公開鍵を得る。登録管理者が管理する登録管理簿に置かれている点ではパスワードと同様であるが、公開鍵は秘密にする必要のない情報であり、みだりに書きかえられないようにさえ管理すれば良く、その意味ではパスワードよりも管理は容易である。

1.2.3　三者間認証

二者間認証では、登録管理者である認証者が職責上知り得た認証情報を用いて別人（別組織）になりすます動機に乏しく認証者に信頼感があるので、パスワードのような同一形式で表現された秘密情報の共有による認証方式を用いることができた。しかし三者間認証では、ある取引における認証者は別の取引における認証の対象者になる場合が容易に想定されるため、パスワードのような同一表現された秘密情報の共有に基づく認証ではセキュリティ上の問題が生じる。すなわち、認証時に知り得た他人（他の組織）のパスワードを用いてのなりすましが可能になってしまう。

そのため三者間認証で用いられる認証情報は、登録された認証情報と提示される認証情報とは、論理的には当然同一であるが、異なる表現をすることにより相互に混用することができない方式を使わなければならない。このような条件を満たす方式としては、現在のところ公開鍵暗号を利用したデジタル署名を用いる方式しかない。この方式では、登録さ

れる認証情報は公開鍵であり、提示される認証情報は秘密鍵を用いてなされたデジタル署名である。両者の照合は単純な照合ではなく、デジタル署名を検証することで行われる。

(1)　認証書（X.509 準拠）を用いる公開鍵方式

① 特徴・特質

X.509 は公開鍵認証書を管理するために定義された国際標準であり、現在 Version3 まで定義されている。

公開鍵暗号方式のフレームワーク及び周辺のデータ構造が規定されており、CA を用いた正しい公開鍵の入手、配布方法の枠組みを定めている。N対N通信の場合に有効な方式であり、オープンモデルにおいては、必須の方式であるが、他の認証方式よりも処理速度が 3 桁ほど遅いという特徴をもつ。

＜認証書の例＞

Version:　　認証書のバージョン（X.509 による）

Serial Number:　　CA より与えられた認証書のシリアルナンバ（ユニークなナンバである）

Signature Algorithm: 認証書のシグネチャアルゴリズム

Issuer:　　認証書の発行機関（X.500 ディレクトリ表現）

Not Before:　　認証書の発行日時

Not After:　　認証書の有効期限

Subject:　　認証書保持者の情報（X.500 ディレクトリ表現）

C=国名,ST=州名,O=組織名,OU=組織単位名,CN=一般名/EMail

Public Key Algorithm: 公開鍵のアルゴリズム（RSA,楕円暗号など）

RSA Public Key:　　公開鍵の内容

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 7 (0x7)
        Signature Algorithm: md5WithRSAEncryption
        Issuer:C=JP,ST=Tokyo-to,L=taito-ku,…
        Validity
            Not Before: Jan 01 10:00:00 1998 GMT
            Not After : Jan 01 10:00:00 1999 GMT
        Subject: C=JP, ST=Tokyo-to, O=aaa.ac.jp,…
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    49:54:43:70:b7:a1:35:0a:e3:53:4d:4c:86:d2:90:
                    00:bd:06:2b:bc:35:55:0b:d7:c4:d6:09:a5:b7:5c:
                    ae:b1:ac:94:54:40:da:7b:71:16:ff:e7:68:5e:00:
                    57:2a:0a:e5:7d:8c:2e:ed:8f:df:c3:ca:37:63:bb:
                    e8:18:39:55:2b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
    Signature Algorithm: md5WithRSAEncryption
        f3:f4:82:60:8e:e0:f8:10:36:9f:d9:a8:c3:b2:83:50:3d:dd:
        2a:9d:b8:75:22:d7:f4:d5:87:4a:7c:c4:3a:7f:b7:72:0f:a3:
        e7:04:71:f0:9a:d5:da:5e:50:c5:13:20:97:8c:ff:69:fa:18:
        5c:b8:29:b7:79:49:03:13:6d:83
```

図 1-9 X509v3 extensions: 認証書 Version.3 の拡張

② 認証の階層

ユーザ識別のための暗号鍵の発行、配信、管理は、厳密なディレクトリ・ベースの方法に依存している。

このため、第三者としての認証局を何度も通すプロセスが必要となる。ＣＡにのみ認証書を発行する上位のＣＡとしては、Internet Society 公認の"Internet PCA Registration Authority"（ＩＰＲＡ)があり、これは、RFC-1422（Certificate-Based

Key Management）でインターネットにおける全ての認証書のトップとなる唯一の発行局と定義されている。また、認証書にはユーザ用認証書やプライベートＣＡ用認証書など、いくつかの種類が提供されており、こうした組織により認証書を発行してもらいその認証書を利用することで、信頼できるＣＡチェインを構築する事が可能となる。尚、こうしたチェインの中に、公的機関による認証との関連の発生が考えられる。

③ 鍵ペア

A. 公開鍵

認証書の中に含まれ、本人の署名を確認するときに使われる。

認証書の中の公開鍵を使い、本人との暗号通信を行うことができる。

B. 秘密鍵

認証書のダイジェストを暗号化しシグネチャを作成する。

公開鍵で暗号化されたデータを復号する。

④ 認証確認方法について

認証書の有効性を調べるには以下のような手順による。

A. 認証書自体のチェック

認証書の期限のチェック及び、認証書の改竄チェックを行う。改竄チェックはＣＡの認証書を用いて行う。認証書のシグネチャにはＣＡの秘密鍵によって署名が行われており、ＣＡの認証書の公開鍵を用いて検証を行う。もし、認証書の Issuer と同様のＣＡ認証書が見つからない場合は検証失敗となる。また、自己発行の認証書の場合、それが上位のＣＡでない限り、信用すべきではない。

B. ＣＡチェインのチェック

信用できるＣＡにたどり着くまでＣＡのチェインを上にたどらなくてはならない。すなわち、信用できるＣＡチェインの存在により、一定のポリシーが確保されていることを認証書の保持者は信用できる事になる。

C. ＣＲＬによる破棄のチェック

ＣＲＬによりその認証書が破棄されたものかどうか確認し、もし破棄された認証書ならば、その認証書のキーペアを盗んだ者によるアクセスである可能性が高いといえる。

⑤ ワークフロー

X.509 による認証書作成までの流れは以下のようになる。

鍵ペア作成

↓

認証書要求作成

↓

認証書要求をＣＡへ送信

↓

ＣＡで署名
↓
認証書作成
↓
ユーザ受信

A. 認証対象者登録

認証書を発行するための情報を認証局に知らせるため、認証書要求が用いられる。認証書要求とは、X.509 に定義されており、本人情報、公開鍵、シグネチャ等により構成される。これらの情報に基づき、認証対象者の登録が行われる。また、要求がＣＡのポリシーに合わない場合、その要求は却下される。

この認証書要求自体も、内部シグネチャを内部公開鍵により検証することで改竄検出が可能である。

B. 鍵ペアの生成

鍵ペアはユーザが生成する。公開鍵と認証書要求を認証局に送信し、認証書を取得した後、秘密鍵と認証書をユーザが管理する。

このように本来鍵の生成・管理はユーザの責任において厳密に行われるべきものだが、本人の不手際により認証書と鍵を損失した場合には新たに認証書を発行し、ＣＲＬも書き換える必要がある。

C. 配布

認証書にはＣＡのデジタル署名が施されており、他者の偽造はできない。

認証書は、ＬＤＡＰなどのデータベースで公開することが可能であり、これにより配布される。

D. 失効

ユーザの秘密鍵が漏洩した場合や秘密鍵の紛失などにより、認証書の有効性がなくなった場合は、ＣＡは直ちにその認証書を無効にしなければならない。このとき、その認証書のシリアルナンバと失効日のリストをファイル化したものが ＣＲＬ(Certificate Revocation Lists)である。ＣＲＬは X.509 に定義され、そのリストとＣＲＬの指紋のＣＡによる署名によって構成されている。

＜CRL の例＞

issuer: CRL を発行した CA

lastUpdate: この CRL の発行日

nextUpdate: この CRL の更新予定日

revoked: 既に破棄された認証書のリスト(シリアルナンバと失効日)

```
issuer= /C=JP/L=Osaka/O=NIT/OU=TEST/CN=local…
lastUpdate=Oct 6 05:00:00 1998 GMT
nextUpdate=Nov 5 05:00:00 1998 GMT
revoked: serialNumber=07 revocationDate=Oct 8 10:00:00 1998 GMT
revoked: serialNumber=05 revocationDate=Nov 1 10:00:00 1998 GMT
```

E. 更新

認証書の期限が切れた際、認証書の更新を実施する。

F. 取引時の認証

取引データを送信する際は、自らの秘密鍵で送信データに署名を行い、相手の認証書の中に含まれる公開鍵を使って暗号化を行う。取引データを受信した際は、相手の認証書の中に含まれる公開鍵を使って署名の検証を行い、自らの秘密鍵を使って復号を行う。

1.2.4 取引権限の認証

BtoC と比べて、BtoB における認証の特徴は取引権限を認証の対象としなければならない点である。すなわち、企業間の取引とは言っても、実際の取引トランザクションのやり取りは自然人である取引担当者が行なうものであって、企業自体やその企業の代表権者が行うわけではない。企業は取引を行う権限を担当者に委譲して実際の取引業務を行わせているのである。

従って、取引トランザクションのやり取りの先立って、相手がその企業における当該取引に関する権限を委譲されていることを確認する必要がある。換言すれば、BtoB における相手認証は相手が単にその企業に属していることの確認だけでなく、その取引に関する権限を持っていることを確認しなければならない。

認証の一環として権限まで確認するにはいくつかの方法がある。日本の企業においては、各人の権限が明示的に規定されているケースは少ないと考えられ、実際の業務は権限の所在を運用的に解釈することで行われていると考えられる。また権限についての考え方も企業毎に異なるので、その運用にもさまざまな形があると予測される。取引権限の認証の実現にあたっては、以下の方法の中から運用の柔軟性およびコスト面で一番適した方法を選ばなければならない。

(1) 権限を認証書中に明記する方法

担当者毎に発行された認証書にその担当者が持っている権限を明記する方法であって、権限認証をストレートに実現した形と言えるが、難点がいくつかある。すなわち、職務権限を明示的に規定する文化が無いところではこの方法は取り得ないし、明示的な規定ができたとしても個別の権限定義はそれぞれの企業文化の影響を強く受けるものであっ

て、企業間での標準化は現実的でないので、この方法の採用はやはり困難である。

(2)　取引担当者を互いに登録しておく方法

企業への所属を示す認証書が各担当者に発行される。相手の認証を行った後で、その人が登録してある取引担当であることを確認する方法である。従来の取引では担当者同士が名刺交換などで互いに相手を認識し合うことがよく行われており、これは単なる儀礼ではなく取引相手をそれぞれの頭に登録して以後の認証に使っているに他ならない。この慣習をそのまま持ち込んだ方法と考えて良く、その点においてスムースなECへの移行が期待できる方法であるが、複数の担当を登録しておく等の担当者の不在等に柔軟に対応できる方式が望まれる。

(3)　特定部門への所属を認証書中に明記する方法

特定部門への所属をもって特定権限が委譲されていると解釈する方法である。例えば、購買課に所属している人には発注権限が委譲されていると見なす考え方である。権限を明記する方法と同じく、部門の機能定義が企業間で統一され得ないところに難点がある。

(4)　ＩＣカード所持をもって権限所有と解釈する方法

取引権限を持つ担当毎に認証用の秘密鍵を与える考え方であるが、認証用の秘密鍵をＩＣカードに格納しておき、そのカードを持っている人がその権限を委譲されていると解釈する方法である。カードには認証書も合わせて格納するのが普通であるが、この運用では認証書の名義をどうするかが問題になる。従来の慣行からの連続性を考えれば、その部門長名義にしておくのが無難と思われるが、この運用に対して法的な裏付けを与えるためには契約型であれば利用規約でしかるべく言及しておくべきであろう。

権限と言う抽象的な存在をカードと言う物理的なものに置き換えて管理する考え方であり、現実の企業における社印等の管理に近い運用が可能なことから、比較的導入しやすい方法と言えよう。そのカードを利用できる複数担当をカード利用時にパスワード等で認証できる機能を持たせて盗用などに対するセキュリティを強化することも可能である。

(5)　アプリケーションサーバの認証による方法

ＥＣにおけるトランザクションのやり取りは各企業の担当部門に置かれたアプリケーションサーバから行われるのが通例である。従って、そのサーバを確認することで、間接的にそのサーバを利用している部門ひいてはその部門の権限の確認を行うことができる。ＩＣカードの場合と同様に、そのサーバの利用者の認証をパスワードなどでサーバ側でローカルに行うことも有効である。この方法の利点としては実現に際して特別な認証機能の開発が必要無く、ＳＳＬの持つサーバ認証の機能をそのまま生かせる点が挙げられる。

1.3　認証システム適用における検討項目

ここでは、「１．１ アプリケーションモデル」において規定された取引モデルを想定し

た企業間電子商取引において、「１．２ 認証の適用技術」で紹介された認証方式のなかで、特に「Ｘ．５０９認証書を用いた公開鍵暗号方式」を利用した認証方式を適用する場合の検討項目を示す。本節では認証システム適用検討における要件定義フェーズと、認証システムを実現してこれを利用するに至るまでの過程を規定する企画フェーズでの、認証システム特有の検討項目に絞って記述する。

なお、ここで言う認証システムとは、業務システムとしての企業間電子商取引において、取引当事者の本人性や資格権限等の確認・登録、認証書発行の申請と受付、認証書の発行・保管管理、認証書の有効性検証、取引における証明行為（デジタル署名、認証書添付）と取引電文の完全性を含むそれらの検証等を行うための機能をもち、認証局、被認証者、認証確認者等のプレイヤーから構成されるシステム全体を示す。

1.3.1 要件定義フェーズにおける検討項目

認証システムの要件定義においては、適用対象である企業間電子商取引の調査･分析を基に、認証システムの対象とする範囲や投資効果等を分析評価して、認証システム適用の基本要件を纏める。

要件定義フェーズにおいては下記の手順で検討を進める。

① 認証システム適用業務の調査・分析

・現行の業務モデルがある場合は、そこで適用されている認証方法の調査・分析を行う。

・「１．１のアプリケーションモデル」を参考に、適用対象プロセスを洗い出し規定する。

② 認証システムの調査･分析

・上記の調査に基づき電子化する企業間電子商取引の業務プロセスにおける認証システムについて、その目的、機能、実現方式（アーキテクチャ）、規模、能力、保守･運用方法、障害の影響、コストなどの要因を調査･分析する。

・合わせて、認証システムの技術動向を調査し、システム化における優位性や有効性についての確認をする。

③ 基本方針の確定

・認証システムの適用対象業務範囲、適用形態、開発対象、外部認証局の活用等、認証システム実現の基本方針を確定する。

・電子化する企業間電子商取引システム全体と認証システムの関連など、企業において認証システムを適用する際の組織のモデル／形態を検討し、企業内での適切な認証システムの適用形態について方針を定める。

④ 認証システム化の対象範囲の選定と投資目標設定

・電子化する企業間電子商取引システムの全体目標を前提に、認証システムとしての費用の概算、得られる効果、考えられるリスクなどを分析する。これらの分析に基

づき、認証システムの規模、開発形態、必要なリソースなどを決定し、企業間電子商取引システム全体の開発計画に反映する。

要件定義を進める手順は上記のように、通常のシステム開発における要件定義手順との大きな相違はない。ここでは、上記の手順において認証システム特有の、以下の検討項目について記述する。

(1)認証システム実現方式の決定
(2)認証対象（取引当事者･権限）の決定
(3)認証局の実現形態

(1)　認証システム実現方式の決定

認証システムにおいて、基本的な認証技術として X.509 認証書を用いる場合であっても、適用する電子商取引の特性に応じて、認証システムの実現方式は変わってくる。「１．１ アプリケーションモデル」で述べた類型化を参照して、より詳細に適用対象の電子商取引を分析して特性を明確にし、認証システムの実現方式を決定する必要がある。その場合の検討の観点を以下に示す。

① 取引の分類

「１．１ アプリケーションモデル」で示した、「契約型取引モデル」、「公募型取引モデル」の分類から見た取引タイプの分類を行い、実現する認証システムの概要を方針決定する。

② 取引メカニズムの分析

取引がどのような方式で電子化されていて、またどのようなネットワーク／媒体を利用するのかまた取引のどのプロセスが自動化され、人間の処理／判断がどこに入るのかと言った観点で整理する。これによって認証システムの必要とされる特性・機能を洗い出す。また、取引の全プロセスを通じて１つの認証方式で対応できる場合と、プロセス毎に認証方式を変えることが必要となる場合も有り、対象となるプロセス毎の整理が必要となる場合もある。

③ 取引を実現する当事者

上記取引メカニズムを利用して実際の電子商取引を実施する当事者を特定する。この当事者は認証対象ともなるので、次の「（２）認証対象の決定」で詳細に記述するが、認証対象の属性や広がり、取引当事者間での認証対象の合意方法などにより、実現する認証システムを検討する必要がある。

④ 取引の重要性の評価

対象となる電子商取引の当該企業における重要性、社会的影響などを、取引の特性・内容から分析する。これには、この取引が認証システムの障害等で実現できなかった場合や不正な取引になった場合、また取引情報が外部に漏洩した場合、などを想定し

たリスク分析に基づく損失コストの評価などにより行う。これによって認証システムに要求される信頼性、安全性等のレベルを方向づけ、また投資コスト算定の前提とする。

⑤ コストパフォーマンス評価による投資の決定

電子商取引の実現による収益（パフォーマンス）に対応して、取引システムへの投資がコストとして算出され比較評価される。認証システムもこの取引システムへの投資の一環として、上記の取引の重要性から見た認証システムの効果によって、そのコストを算出して、認証システムとしての投資の方向性を定める。

⑥ 認証システムの実現技術の適性評価

電子商取引の重要性にも関連して、この取引の社会的な影響を考慮した場合、適切なるレベルの認証技術の適用が、企業の社会的責任として発生する。適用する認証技術の適性評価を、公表されている技術情報や適用事例評価などを基にして行う。

⑦ 認証システムの運営形態

電子商取引システムの運営と合わせて、認証システムの運営形態も決定する必要がある。認証システムを構成する多くの機能要素を円滑に維持運用して行くためには、認証システム全体の運用要件を元に、その運営形態を確定する必要がある。特に、取引当事者の本人性や資格権限等の確認・登録、認証書発行の申請と受付、認証書の発行・保管管理、認証書の有効性検証に関わる機能は、従来の商取引と大きく変わる要素であり、これらの機能を実現するシステムを運用する機関（以下認証局と言う）については、共同運営を含めて自営する場合と、外部の機関に全てまたは一部の運用を委託する場合とがある。上記の認証局に要求される種々の要件を考慮しまた、電子商取引する相手企業との関係をも考慮した上で方針を決定する。

(2)　認証対象（取引当事者･権限）の決定

認証対象（取引当事者･権限）の決定は、適用する認証システムの特性に大きく左右される。しかし、認証対象の捉え型には様々な考え方が有り、多面的に分析して決定する必要がある。

本節では認証対象を決定する際の検討項目を記述する。

① 取引当事者/権限の捉え型

企業間取引においては取引が複雑であり、同一の企業間取引でも、取引の形態や内容により、また取引を構成する個々のプロセスに応じて、取引当事者や取引に必要となる権限が変わるケースが有る。

取引当事者として想定されるのは下記であり、これらが認証対象となる。

- 当該企業の代表者
- 当該取引の実行権限者
- 上記実行権限者より権限を移譲された取引担当者
- 当該取引の担当部署及び責任者

- 当該取引の担当システム（アプリケーションサーバなど）　など

これらの取引当事者は、認証システム側で決定するものではなく、業務アプリケーションとしての電子商取引システム自体の設計過程において決定されるものであるが、認証システムの適用検討の担当者はこの電子商取引システム設計段階において、取引当事者/権限が明確となる様に要請する必要が有る。

規定された取引当事者/権限を認証対象として捉え、その属性や組織内での運用の形態に応じて、適切な認証システムの実現方式を採用することが必要である。また、取引当事者/権限は取引相手の企業との間で事前に合意が必要なケースも有り、またその属性がダイナミックに変動する場合も多く、その様なケースに備えて合意するための取り決めや、通知/伝達方法を事前に定めておく必要がある。

② 運用上の留意事項

上記の検討で取引相手/権限が定まって電子商取引及び認証システムの運用が開始された後も、認証システムを安定的に運営しその信頼性を保持していくためには、認証システムを維持管理して行く仕組み作りが必要である。本節では認証システムを運用していく場合の留意事項について記述する。

A. 登録／リボーク

取引相手の登録／リボーク方法は様々有り、これは取引する各企業内或いは企業間でルールを定める必要がある。このルールは取引の内容を考慮すると共に、下記のような登録／リボークの発生状況を考慮した方式とする必要がある。

- 取引への新規企業の参加や、参加者の脱退のような大量登録／リボークの発生
- 人事異動や組織変更のような、定期的／同時的な大量登録／リボークの発生
- 相手確認や権限審査ルールの変更に伴う一時的な、大量登録／リボークの発生

リボークが発生した場合は、これを速やかに取引システムに反映する事が必要であり、このためのシステム的及び運用面での仕掛け作りが必要である。また、個人（担当）単位、担当グループ単位、組織単位、サーバもしくはクライアント（端末）単位等登録やリボークをどの単位で行うかによって運用の容易性・コストや認証の信頼性が異なってくる。このためリボークリストの定期的な作成とその公開、取引システムでのリボーク検証の仕組みなどを、リボーク発生による取引への影響と、リボーク検証のシステム化及び運用コストとの兼ね合いで評価し、適切な実現方式を選択することが必要である。

B.認証書への反映

認証書を利用した認証システムにおいては、この認証書への記載事項を取引システムの実現方式と合わせて定めておく必要がある。また、認証書は一般に有効期限が定められており、その期限内で認証書への記載事項が変更となる事も有り、その場合未変更の認証書を利用する事で、取引事故が発生し、認証システムの信頼性を損なうことになる。認証書の記載事項が変更となる場合は、速やかに当該認証書の

リボーク処理と再発行により、安全な電子商取引の継続を維持する必要がある。認証書への記載事項変更は事前に分かっていることが多いので、認証システムでは同一の相手に対しての認証書への記載事項変更に伴う認証書の事前再発行等の仕掛けを作る事で、遅滞無い電子商取引の継続を実現する必要がある。

(3)　認証局の実現形態

認証システムの実現方式の検討項目の１つに、認証局の運営形態の決定がある。認証局の運営には下記のような形態がある。

- 認証局を完全に自営化して運営する。
  例：契約型モデルにおいて特定の企業が、参加企業の認証書の発行申請に伴う確認・審査及び認証書発行・管理を行なうことが、契約の前提となっている場合
  例：契約型モデルにおいて、特定の企業が認証書発行・管理を行なう機能を分担し、確認審査機能は参加企業が分担する場合
- 認証局の一部機能の運営を外部に委託する。
  例：契約型モデルにおいて認証書発行・管理を専門業者に、認証書の発行申請に伴う確認・審査を参加企業に委託する場合
- 認証局の業務自体を外部の認証局に委託する。
  例：公募型モデルにおいて、公募する企業が信頼できる認証局を選定し、応募企業にそれを指定することで、外部認証局の発行した認証書を利用する場合

自営化する場合と外部に委託する場合及び委託範囲で、それぞれ下記のようなメリット、デメリットが有り、これを認証システム全体の要件に照らして比較評価し、方針を確定する。

表 1-2　認証局システムの運営形態の比較

	認証局の自営	発行・管理機能を外部へ委託	外部認証局の利用
利用目的への適合性	利用目的に合わせた運用となる	利用目的に合った委託先の選定により、目的に適合した運用が可能	利用目的に合った認証局を選定するが、基本的には、当該認証局の利用目的を前提とした運用とする必要がある
認証書の形式	Ｘ．５０９の規定内で設定可能	委託先の規定及び委託元からの要求への対応により、決定される	基本的には、当該認証局の規程に合わせる必要がある
認証局の運営責任	自営企業に全責任がある	認証局としての責任は委託元が負う。ただし、委託先と委託元で、機能分担により責任分界がある	認証局に全責任がある
安全性、信頼性	利用目的に必要なレベルで設定される	発行・管理には高い安全性と信頼性が期待できる	一般に高い安全性と信頼性を具備する
初期コスト 運用コスト	特定目的利用となるため、初期／運用コストは高くなり易い。ただし、利用目的に合わせ機能や運用形態を絞り込む事でコストを低減可能である	委託部分については、初期／運用コスト的には優位性が期待できる。ただし、委託元での初期投資や運用コストが有り総合的なコスト評価が必要である	汎用的な共同利用型システムであり、初期／運用コスト的には優位である

本節では外部の認証局を活用する場合、その選定において検討すべき事項を記述する。

① 認証局の中立性／公共性

認証局は当該電子商取引の範囲において、取引当事者が必要と認める中立性／公平性を保持することが必要である。特に公募型モデルで複数の企業が参加する社会的な影響の大きい取引を、外部認証局の発行する認証書を利用して実施する場合には、その中立性／公共性に配慮する事が必要である。これについては、当該認証局の運営母体、既に利用している企業過去の運営実績等から評価する。契約型モデルで認証局を自営する場合は、契約の規定でその中立性が明示されているかなどの観点から評価する。一部の機能を外部に委託する場合、委託業務の内容と委託先での業務規定を参照して評価する。

② 認証局のサービス内容

利用する外部認証局及び業務委託先の提供するサービスする内容（サービス時間帯、登録手続き、リボーク通知のタイミングなど）が、実現しようとする電子商取引から見た認証システムの要件に合致しているかを評価する。また、ヘルプデスクなどの運用支援サービスの有無についても確認する。

③ 認証局の安全性／信頼性

認証局としてのセキュリティ技術や運用面での安全性のみならず、経営的な安定性など、信頼できる認証サービスを安定的かつ継続的に提供できる事を見極める。また障害等で取引に影響が無いようなコンティンジェンシープランが策定されているか等についても確認する。

④ 認証局の情報公開性

認証局はその特性上公開できない情報があるが、利用者として知るべき情報も多々有り、これらについて事前にＣＰＳ（Certificate Practice Statement）などを入手して評価するとともに、運営状況、監査結果などの情報が適切に公開される仕組みとなっている事を確認する。特に公募モデルで外部認証局を利用する場合や外部機関に一部の業務を委託する場合は、その経営状況含めた情報の開示を受けて、安定的な電子商取引の継続を図る必要がある。

⑤ 認証局の資格・要件

現在一部の電子商取引に関する認証サービスでは上位認証局による認定などの一定の資格要件が要求されているが、今後認証サービスには、電子商取引の形態により様々な要件が課せられる事が予想される。必要な資格要件が具備されまた、継続的にその資格要件が維持されているかを資格要件取得の実績及び監査する仕組みについて確認する。

⑥ 認証局利用に係わるコスト

当該認証サービスに要するコストを見積り、他の認証局の利用との比較や自営方式の検討等と合わせて総合的にコスト評価する。

1.3.2 企画フェーズにおける検討項目

本節では、上記の要件定義フェーズでの規定事項を前提として、具体的に認証システムの適用を実現するための方針を確定し、また適用実現に至るのでのプロセスを規定する企画プロセスの検討項目について記述する。

企画フェーズにおいては下記の作業の手順で検討を推進する。

① 認証システムの適用対象内容の確定

認証システムの適用対象となる組織、責任者、担当者、サーバなどについて確定する。

② 認証システムの課題の解決方針確定

認証システム適用における具体的な業務上の問題点を解析し、解決方法を明確にすると共に、情報システム技術を用いて解決すべきシステム課題を明らかにする。

③ 認証システムの概要確定

認証システムが実現する機能、扱うデータ、処理方式、システムの保守･運用方法、システムの運用／管理体制について概要を確定する。

④ 適用情報技術の調査／評価による方針決定

認証システムの実現のための技術動向を詳細に調査する。技術／システムの比較評価などにより、適用する技術やシステム、外部認証機関の選定などについて方針を定める。

⑤ 認証システムモデルの作成

認証システム適用の対象プロセスにおいて、上記に基づいて認証システムの概要を整理し、認証システムをモデル化し適用性を検証する。

⑥ システム処理方式の策定

上記モデルに基づき認証システムを実現する情報処理システムの機能を明らかにし、この機能について情報と処理の流れを確定する。この機能を実現するために必要な、システム処理方式を策定する。認証システムを開発する場合は、この処理方式に従って開発を進める。

⑦ 費用とシステム投資効果の評価

認証システム実現時の定量的、定性的効果予測を行う。また、開発・運用・保守に関する期間・体制・工数の大枠を予測し、システム実現のための費用を見積る。費用と効果を対比させ、システムへの投資効果と投資回収の時期などを明確にする。

⑧ 全体の企業間電子商取引システムとの整合性評価

認証システムに対する企画と全体の企業間商取引システムの企画とで、技術的、業務的運用等の側面で整合しているかを検証する。不整合がある場合は、前のステップに戻って企画を再度策定する。本作業の成果として必要に応じて利用規約等の運用規程を策定する。

企画フェーズを進める手順は上記のように、通常のシステム開発における企画フェーズの手順との大きな相違はない。ここでは、上記の検討において次の認証システム特有の検討項目について記述する。

(1) 鍵管理
(2) 登録プロセス
(3) 発行プロセス（再発行プロセス含む）
(4) リボーク／更新プロセス
(5) 認証書有効性確認プロセス
(6) 利用規約

(1) 鍵管理

電子商取引における暗号鍵の安全な管理は、取引の安定性確保のために必須である。ここでは公開鍵暗号方式での認証システムとの関連における鍵管理について記述する。

① 管理する鍵と鍵管理の考え方

公開鍵方式においてセキュアな鍵管理が要求されるのは秘密鍵であり、その鍵の所有者責任で鍵を安全に管理する事が鍵管理の基本である。ただし、鍵にはライフサイクルが有り所有者以外の人間がそのライフサイクルに関わってくる事も想定され、ライフサイクル全般にわたる鍵管理が必要である。各ライフサイクルの各プロセスにおける鍵管理の検討項目を記述する。

② 鍵生成プロセス

このプロセスは鍵所有者が行う場合もあるが、情報システム部門もしくは総務部門等が一括して行う事も想定される。いずれの場合でも下記の項目については事前に定め、これを遵守する事が必要である。

- 鍵生成を行う人（人数、資格要件など）
- 鍵生成の方法（生成プロセスの可監査性、特定者による複製の防止など）
- 鍵の強度、有効期限の規定
- 生成した鍵の認証システムへの安全な組み込み
- 安全なバックアップの取得手順
- 参加企業の鍵生成を一括して行う場合の管理（コピーを保管するか、配布後消去するか等）

③ 鍵の利用･保管プロセス

ここからは利用者サイド主体の管理となるが、管理方式や使用するシステム、媒体等については事前に確定し、その方式また、そのシステムを利用者に周知徹底させて、利用して安全な利用、保管を実現する。

- 生成した鍵の保管方法（格納方式、バックアップ方法、アクセス方式など）
- 鍵安全性のチェック（危殆化していないかのチェックなど）
- 鍵の回復手順（回復許可の権限、立ち会い者、リカバリプロセスの規定）
- 鍵利用記録の取得、保持、監査規定

④ 鍵廃棄／破壊プロセス

- 鍵廃棄／破壊プロセスの実施責任／部署の確定（上記の一括生成した部門による、一括廃棄などの検討）
- 保管媒体から消滅方法、または媒体の破壊方法
- バックアップ含めた廃棄／破壊
- 作成プロセス記録の滅却
- 破壊プロセスの記録取得、保持、監査

なお、認証局システムを自営する場合や、認証書発行を外部委託する場合は、認証局の秘密鍵を生成、保管・管理、廃棄・破壊する必要があるが、これについては、認証局としての運用規程によって定める。

(2)　登録プロセス

登録プロセスに関しては、１．３．１の要件定義で規定された項目を、認証システム開発へ展開するための下記の事項を検討する。

① 登録プロセスの実現形態

ここでは登録システム設計の前提となる、登録プロセスの実施部署、その手続き、認証システムとの業務処理インタフェース、運用体制などを規定する。手続きにおいて重要な本人確認の方法については、使用する情報や確認手段を明確に定める必要がある。

② 登録プロセスの実行形態

想定される登録処理の形態（大量一括処理、不定期少量処理など）と上記の登録プロセス実現形態の両方を考慮して、最適な登録システムを実現するための項目を整理する。また、システム処理形態（オンライン処理、バッチ処理）の概要を定める。また、利用者の登録処理インタフェースについても、方針を確定する。

③ 登録情報の確定

登録時には本人確認を行った上で、申請された情報内容を確認・審査する必要がある。この対象となる情報は要件定義過程において整理はされているが、企画フェーズではこの情報の項目レベルにおいてを確定させ、事務規定や認証システムの設計・運用に反映する必要がある。

(3)　発行プロセス（再発行プロセス含む）

発行プロセスに関しては、登録プロセスとの連携を前提として、安全な認証システムの運用による確実な認証書発行を実現するための項目を整理する。認証書発行を委託する場合には、委託先との間で交換すべき情報と交換方法等を定める必要がある。また、この場合には組織情報などの機密情報を委託先で扱う事から、情報機密保持等を含む委託先との契約についても考慮する必要がある。

① 発行プロセスの実現形態

ここでは認証システム設計の前提となる、発行プロセスの実施部署、その手続き、利用者へのサービス提供方式、電子商取引システムとのインタフェース、運用体制などを規定する。なお、発行プロセスの実現形態の検討においては、認証システムの運用がどのような形態で行われるかによって規定される。

② 発行プロセスの実行形態

前提となる登録処理の形態に対応した発行処理の実現方式（大量一括処理、不定期少量処理など）と、上記の発行プロセス実現形態の両方を考慮して、最適な認証システムを実現するための項目を整理する。また、システム処理形態（オンライン処理、バッチ処理）の概要を定める。また、利用者への発行、再発行処理インタフェースについても、方針を確定する。

③ 発行情報の確定

発行時には登録時の申請情報に加えて認証システムで付加する情報を合わせて、認証書を作成する。この情報は要件定義過程において整理はされているが、企画フェーズではこの情報の項目レベルで確定させ、X.509 との適合性検証、適用する電子商取引システムとの整合性検証を行う必要がある。

(4) リボーク／更新プロセス

リボーク／更新プロセスに関しては、登録／発行プロセスとの連携を前提として、リボーク／更新の受付と、迅速な認証システムでの対応（リボークリストの作成、ＯＣＳＰ（Online Certificate Status protocol）等による認証書有効性検証、更新に伴う認証書再発行など）を実現する処理・運用方式を確定するための項目を整理する。また認証書発行を委託する場合には、発行同様にリボークについても、委託先との間で交換すべき情報と交換方法等を定める必要がある。また、この場合にはリボーク情報は機密性が高いので、情報機密保持としてリボークの扱いを委託先との契約で反映する様考慮する必要がある。

① リボーク／更新プロセスの実現形態

ここではリボーク／更新情報の発生元と、リボーク登録／更新登録プロセスの実施部署の連携やその手続き、電子商取引システムとのインタフェース、運用体制などを規定する。

② リボーク／更新プロセスの実行形態

前提となる登録／発行処理の形態を考慮して、リボーク／更新プロセスを実現するために、最適なシステム実現方式を整理する。また、リボークリストの作成、認証書有効性検証に関して、認証システムの中で実現する必要があり、リボークリスト発行のタイミング／インターバル、リボークリストの公開方式、証書有効性検証の方式などを確定する。

③ リボーク／更新情報の確定

リボーク／更新時にはリボーク／更新申請情報を基に、認証システムで管理している登録時の情報と情報を参照して、必要な処理を行う必要がある。リボーク／更新情報は要件定義過程において整理はされているが、企画フェーズではこの情報の項目レベルで確定して、認証システムの処理との整合性を検証する必要がある。

(5) 認証書有効性確認プロセス

交換された認証書は受取り側で有効性確認（有効期限内でありかつリボークしていない事の確認）を行う必要がある。認証書の有効性確認を実現するためには、自営の認証システム或いは委託先にレポジトリを設け、ＯＣＳＰなどのプロトコルによりアクセスして、認証書の有効性を検証する方法、自営の認証システム或いは委託先で認証書のリボークリストを発行しこれを定期的に利用者に配布して、利用時に当該認証書の有効性を検証する方法などが有る。これらの運用方式やシステム処理に沿って利用する利用者

側の認証検証ソフトのを選定／開発する必要がある。

(6)　利用規約

オープンなネットワークを利用した企業間電子商取引を行う場合、送受信の確認、トラブル時の対応等を定めた電子商取引の業務規約やデータ交換規約等を取り交わす事が必要となる。

これらの規約を前提として電子商取引において認証を使用する場合、当事者間において認証の利用に関する規約が別途必要になる。

利用規約に盛り込む内容としては、利用手続きに関する規約、認証システムの提供者並びに利用者の義務と責任及びトラブル発生時の対処、認証局の運営形態に応じた業務分担に関する規約などが考えられる。

利用手続きに関する規約は、上記の登録／発行（再発行）／リボーク等の各過程における、利用者との間で発生する運用に関する規定を行う、また、安全で信頼性のある認証システムの運用を実現するために、利用者に対して予め認識してもらう必要のある項目は示しておく。

① 利用者側での準備作業及び準備するリソース

認証システムを利用するために必要な、利用者側での準備作業について示す。利用者側のシステムで必要なシステム環境や、情報の設定、媒体の準備などを示す。

② 登録／発行／利用プロセスの実施手続き

認証システムの提供する登録／発行／利用プロセスを活用するために利用者に実施してもらう事項を示す。登録フォーマットの入手方法、必要な登録情報、登録情報の認証システムへの渡し方、認証書作成状況の参照方法、認証書の取得方法、リボーク登録の方法、リボークリストの入手方法、認証書の有効性確認方法、再発行手続きの方法、ヘルプデスク活用方法など。また運用を考慮したサービス時間、発行までの待ち時間等の情報も提供する。

認証システムの提供者並びに利用者の義務、責任及びトラブル発生時の対処に関する規約は、第２章を参照して作成するが、代表的な項目としては下記が考えられる。

① 利用者の義務

秘密鍵の管理責任、受取った認証書の有効性確認に関する責任、リボークを認識した場合の通知に関する責任など、認証システム或いは外部認証局の規定した義務規定。

② トラブル時の対応

リスク要因及び発生時の責任分界、通知／連絡の経路、当面の処置などの規定

認証局の運営形態に応じた規約としては、下記のような項目が挙げられる。

① 業務分担と責任分界

認証書の発行申請から有効期限満了やリボークによる認証書の破棄に至るまでの、認証書のライフサイクルを通じた、認証書に関わる業務の分担に基づく、業務分担者間での運用、責任分界に関する規約の策定

② ＣＰＳの策定

認証書の発行・管理に関する機能を外部に委託する場合は、委託元がＣＰＳを策定する事が必要になる場合がある。一方、中核企業が認証書の発行・管理に関する機能を担当し、参加企業に認証書の発行申請に伴う本人確認や権限審査を委託する場合、中核企業のＣＰＳに従う場合がある。このように業務の分担形態に応じて、ＣＰＳの策定の要否と作成責任を決め、認証局全体としての利用規約を定める必要がある。

第2章 想定されるトラブルの回避手法

2.1 トラブル回避の考え方

2.1.1 本章のスコープ

オープンネットワーク上での電子商取引拡大をのためには、各種アンケート結果にもみられるように、安全性に対する要求は高い。

特に、企業間電子商取引にとって、悪意の第三者による妨害、悪意・善意の取引当事者等に起因する各種トラブルからの回避が、企業間電子商取引を、拡大する大きな要因になると考えられる。

本章では、このような企業間取引のトラブルを検討するにあったて以下の企業間取引モデルと発生トラブルの当事者について、以下の整理を行った。

(1) 企業間取引モデル

企業間取引モデルについては、前期 企業間電子商取引における認証・公証適用の考え方で記述した以下の２モデルに分類した。

① 契約型モデル

商取引などの企業間交流を目的とするクローズドなグループを構成する企業群において、紛争発生時の事実確認手段として何らかの契約関係を利用することを、当該グループへの参加条件とする場合のモデル。発生トラブル解決の実現方法として、取引当事者がその機能を具備する場合と、第三者の提供する機能を利用する場合とが考えられる。発生トラブル解決機能を提供する機関は当該グループ内で予め約款等により、その利用と効力を明らかにしておく必要がある。

② 公募型モデル

取引所あるいは公募の主催企業と、不特定の応募企業との、事前の契約関係を前提としない取引形態モデル。、取引当事者または第三者からの事実確認要求に対応するために、公証機能を用いる場合のモデル。発生トラブル解決の実現方法として、取引主催企業がその機能を具備する場合と、第三者の提供する機能を利用する場合とが考えられる。発生トラブル解決機能を提供する機関は、応募企業に対し、事前に、その利用と効力を明らかにしておく必要がある。

(2) 発生トラブルの当事者

発生トラブルの当事者は、以下にモデル化できる。

① 契約当事者間のトラブル（図２－１におけるＡの関係）

企業間電子商取引の当事者間のトラブルであり、関係者は電子商取引当事者となる。

② 電子商取引当事者とその電子商取引に直接関係のない第三者間のトラブル

電子商取引当事者とその電子商取引に直接関係のない第三者間のトラブルであり、

関係者は電子商取引当事者と第三者となる。

ここで、第三者については、以下の形態が考えられる。

- 取引グループにおける取引グループ内第三者（図２－１におけるＢの関係）
  例えば、公募型における他応募者又は企業グループにおけるグループ内企業等
- 無契約第三者（図２－１におけるＣの関係）
  当該電子商取引に直接又は間接的にも何ら関係の無い、第三者

以上の整理を図２－１に示す。

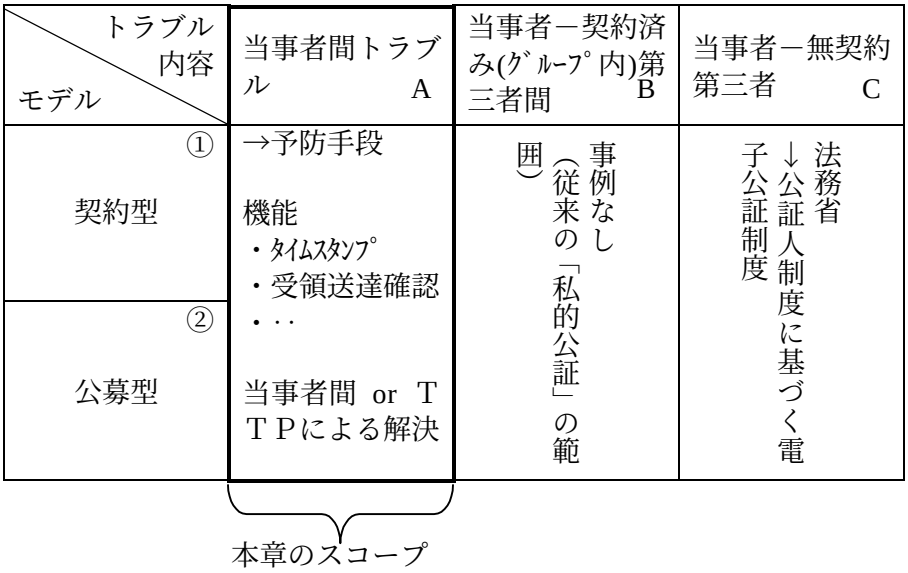


図 2-1　スコープ

本章で取り扱うトラブル回避策は以下の観点から、上記企業間取引モデルの２モデルにおける契約当事者間のトラブルとする。（図２－１におけるＡのモデル）

- 図２－１におけるＣのモデルに示した、第三者の関連したトラブルは、契約関係が無く、法制度面の対応が必要と考えられる。
- 図２－１におけるＢのモデルに示した、第三者の関連したトラブルは、一般的に直接取引者間（例えば、発注者と受注者）以外では契約関係が無く、法制度面の対応が必要と考えられる。

2.1.2　電子商取引におけるトラブルの分類

本節では、電子商取引におけるトラブル内容を理解するため、電子商取引で起きうるトラブルを、トラブルの性格や原因によって分類する。

まず、一般的な商取引に関わるトラブルを時系列、トラブルの性格によって分類し、電子商取引という手段が関係する部分を明確化する。

その上で、電子商取引という手段を利用すること特有のトラブルを、トラブルの性格、

原因によって分類する。

(1)　商取引に関わるトラブルの分類

電子商取引に限らず、二者間での商取引において起き得るトラブルは、以下のように分類することができる。

① 時系列による分類

商取引のプロセスは、契約、契約内容の履行、決済の各段階に分けることができる。各々のプロセスにかかわるトラブルの発生は、それぞれのプロセスの実施時の他に、そのプロセスの以前、以後が有り得るが、ここでは、トラブルが発生する時期ではなく、原因が存在する時期で分類する。

② トラブルの性格による分類

それぞれのプロセスに関わって発生するトラブルは、その性格により、大まかに以下の様に分類できる。

- プロセス実施が不可能となる、あるいは当事者の一方が実施を拒否するトラブル（実施不可）
- プロセスの実施方法が当事者間で合意されないトラブル（実施方法不合意）
- プロセスの実施が完了しない、あるいは実施内容が合致しないトラブル（実施不完全）
- プロセスで実施される内容に不備や矛盾、虚偽等が含まれるトラブル（内容不全）
- プロセスやその内容に関わり、当事者間のみで保持しなければならない情報が第三者に漏れる（機密漏洩）

以上の分類と、それぞれにあてはまる代表的な例を、表２－１に示す。

表 2-1 商取引におけるトラブルの分類とトラブル例

商取引プロセス / トラブルの性格	契約	契約内容の履行	決済
実施不可	・無資格 ・認可を受けていない	・契約不履行 ・一方の倒産	・不払い ・取引銀行の倒産
実施方法不合意	・発信主義か受信主義かで合意できない ・文書の書式・様式が合意できない	・納品方法で合意できない	・振り込み日の不合意 ・使用する決済手段を一方が認めない
実施不完全	・注文書が届かない ・決済権限者が関わったことが証明されない ・内容が改竄される ・契約をしていないと主張する	・納品物送付途中での破損 ・送った納品物が届かない ・納品日の改竄 ・受信した納品物の改竄 ・検収結果が届かない	・口座番号間違え ・振り込みがなされていないと主張する
内容不全	・契約内容に不備や矛盾がある ・実施内容に不法行為が含まれる ・実施者の資格に虚偽があった	・結果に不満足 ・実施内容に虚偽がある	・送金額間違え ・残高不足で引き落としできない
機密漏洩	・契約内容が第三者に漏れる	・実施内容が第三者に漏れる	

(2)　電子商取引特有のトラブル

表２－１に挙げたトラブルのうち、プロセスを電子データの交換によって実施する場合を、電子商取引と考えることができる。

トラブルのうち、「実施不可」及び「内容不全」に関わるトラブルは、プロセスが電子的に実施されるか否かによってトラブルの内容が変わるものではない。電子商取引のトラブルとして検討対象となるのは、「実施方法不合意」「実施不完全」及び「機密漏洩」である。本章では、これらのうち、機密情報については漏洩しない為の方策をとること、暗号化等の機密保持手段を含めて、電子的商取引の手段・方法については当事者間で合意がなされていることを前提に、実際に電子商取引を実施する際に起き得るトラブルの分析を行う。

なお、電子商取引の手段・方法としては、以下のような項目等について当事者間で合意がなされるべきである。

A.　意思、納品物等の電子データを作成・確認する為に使用するソフトウェア
B.　電子データ送信のプロトコル、データ変換形式
C.　通信経路
D.　送信データを暗号化する場合は、暗号アルゴリズムや使用方法
E.　送信される注文書、納品物等の発効タイミング（送信時、受信時、確認時、電子データ内記載等）

(3)　電子商取引の手順

二者間で電子的に商取引プロセスを実施する場合、契約書、提案への同意、納品物等の内容（以下、送信される内容を「文書」という）を持つ電子データが、一方から他方に送られることが積み重ねられる。このうちの１回を取り出した場合の手順を、以下に示す。

① 当事者Ａが、自らの意思、納品物等を当事者Ｂに伝達する。
　[1-1]　当事者Ａが、自らの使用する機器を用いて、自らの文書を電子データとして作成し、Ｂへの送信を指示する。
　[1-2]　Ａの使用機器が、電子データをＢに向けて送信するため、通信経路に対して経路や宛て先などの情報を付加して送信する。
　[1-3]　通信経路を通じて電子データが伝達され、Ｂの使用する機器に到着する。
② 当事者Ｂは、伝達された電子データより、当事者Ａの文書を確認する。
　[2-1]　当事者Ｂの使用する機器が、到着した電子データからＡの文書を表示する。
　[2-2]　当事者Ｂが、表示されたＡの文書内容を確認する。

以上について、図２－２に示す。

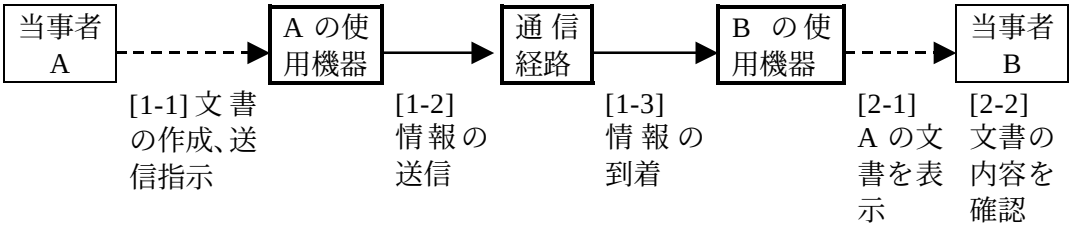


図 2-2　電子商取引における商取引プロセスの実施例

(4)　電子商取引でのトラブルの発生

前項に示した商取引プロセスにおいて起き得るトラブルを、以下に列挙する。

(a)　プロセス実施が不適当。

　プロセスが、何らかの資格が必要な場合や、明確に法人の決済権限者の了解が必要な場合などに、無資格者、無権限者によって文書が作成される。

(b)　当事者Aの文書が当事者Bに伝達されない。

　担当者間の情報の不達、伝達内容の誤り、当事者Bによる誤認識等

(c)　当事者Bが、当事者Aが送信していない情報を当事者Aからの文書と認識する。

　他者からの文書をAからの文書と誤認識すること等。

(d)　当事者Aが作成した文書と、当事者Bが確認した文書とが異なる。

　Aが保存している「作成した文書」とBが保存している「確認した文書」の内容が一致しない等。

(e)　双方の当事者のいずれかによる、プロセスの一部または全体の否認。

　プロセスそのものの否認、Bによる同意の否認のほか、実施日、担当者、実施内容等プロセスの一部に対する否認が考えられる。

(5)　電子商取引トラブルの内容と原因

(a)～(f)に示すトラブルが、図２－２に示す電子商取引の手順中に発生する場合、その具体的な内容と原因は、以下の表に示すものが想定される。

なお、トラブルを検討する上で、下記前提条件を設定する。

- 当事者Aの意思は、Aの使用機器（以下、機器Aという。同様に、Bの使用機器を機器Bという）から送信される情報に正しく表現される。記載ミスはない。
- 機器A、機器Bとも、同一の情報に対応して当事者との間で入出力される意思内容は同一である。
- 当事者Bは、機器Bに出力された情報から意思を正しく解釈する。解釈ミスはない。

表 2-2　(a)　プロセス実施が不適当

トラブルの内容	原因
当事者 A が無資格	当事者 A が当事者 B の資格を未確認
当事者 A が無権限	当事者 A が当事者 B の権限を未確認
当事者 A が本人でない	当事者 A が当事者 B が本人であることを未確認
当事者 B が無資格	当事者 B が当事者 A の資格を未確認
当事者 B が無権限	当事者 B が当事者 A の権限を未確認
当事者 B が本人でない	当事者 B が当事者 A が本人であることを未確認

表 2-3　(b)　当事者 A の文書が当事者 B に伝達されない

トラブルの内容	原因
情報の消滅	機器 A における消滅 通信経路上における消滅 機器 B における消滅
当事者 B 以外への伝達	A からの誤指示 通信経路の誤配 機器 B への成りすまし 当事者 B への成りすまし

表 2-4　(c)　当事者 B が、当事者 A が送信していない情報を当事者 A からの文書と認識する

トラブルの内容	原因
他者から受信した情報を当事者 A からと認識	当事者 A へのなりすまし 機器 A へのなりすまし

表 2-5　(d)　当事者 A が作成した文書と、当事者 B が確認した文書とが異なる

トラブルの内容	原因
A の送信情報と B の受信情報の不一致	機器 A での不完全な記録 機器 A での送信までに改竄 機器 A からの不完全な送信 通信経路にて改竄 機器 B への不完全な到着（通信経路の不完全な伝達） 機器 B の不完全な受信 機器 B での不完全な記録 機器 B の受信以降改竄

表 2-6　(e)　プロセス実施後、双方の当事者のいずれかによる
プロセスの一部または全体の否認

トラブルの内容	原因
当事者 A の存在否定	当事者 A の存在確認の無保証
当事者 A の資格否定	当事者 A の資格確認の無保証
当事者 A の本人否定	当事者 A の本人確認の無保証
当事者 B の存在否定	当事者 B の存在確認の無保証
当事者 B の資格否定	当事者 B の資格確認の無保証
当事者 B の本人否定	当事者 B の本人確認の無保証
当事者 A の送信否定 当事者 B の受信否定	機器 A からの送信が無保証 通信経路の受信が無保証 通信経路からの送信が無保証 機器 B の受信が無保証
当事者 A の送信内容否定 当事者 B の受信内容否定	機器 A からの送信内容の無保証 通信経路の受信内容の無保証 通信経路からの送信内容の無保証 機器 B の受信内容の無保証
当事者 A の送信日時否定 当事者 B の受信日時否定	機器 A からの送信日時の無保証 通信経路の受信日時の無保証 通信経路からの送信日時の無保証 機器 B の受信日時の無保証

表中、無保証とは、プロセスにおいて実施された内容が改竄されることなく保存されていることを証明できないことを意味する。すなわち、実施されたことの記録が、消滅（事故）、消去（故意）、変化（事故）、改竄（故意）のいずれもされていないことを証明できなければ、無保証となる。

(6)　従来の手続きでの対応

従来の、電子商取引を利用しない当事者間の手続きでは、全項(a)～(f)に示すトラブルを回避する為に、さまざまな方法が採用されている。下記に、契約時に行われている方法の例を示す。

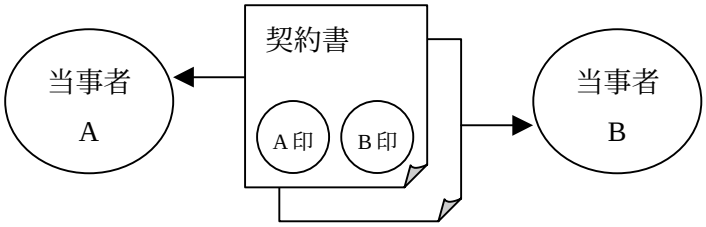
①　契約文書の交換

大抵の場合、契約行為等の確認は、当事者の間で、同内容の契約書を取り交わすことや、注文書に対して注文請書を返信することなど、相互に、紙等の見読可能な媒体に記録された文書を取り交わすことで相互に確認される。

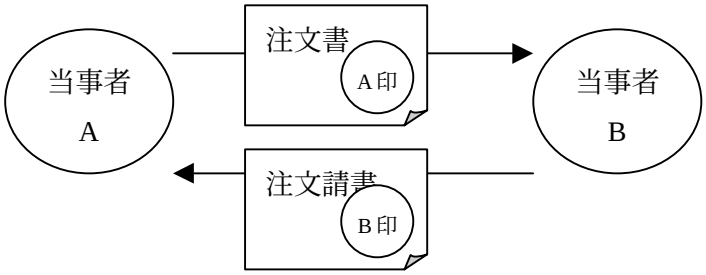
また、契約書や注文書、注文請書（以下「文書」という）には、当事者の捺印がなされ、確かに当該当事者が意思表示していることを示す。

文書を取り交わした結果、当事者Ｂは当事者Ａの意思を示す文書を、当事者Ａは当事者Ｂが同意したことを示す文書を、相互に保持する。

上記を、図２－３に示す。



同一内容の契約書に双方の同意を示す印を捺印し、双方で保持



双方が、相手の意思を示す印が捺印された文書を保持

図 2-3 文書の交換

② トラブル回避への効果

以上の方法が、商取引におけるトラブルを回避する為に持つ効果を、(a)～(f)の分類に従って解説する。

(a) プロセス実施が不適当

必要に応じて、文書には担当者、資格者を示す記述がなされる。また、必要であれば、文書取り交わしの際に、免許の提示、免許番号の記述等による資格証明がなされる。

このように、プロセス自体の成立は、事前に確認される他、必要に応じて文書内に記録される。

(b) 当事者Aの意思が当事者Bに伝達されない

当事者Aと当事者Bが対面して契約内容を確認する、あるいは、文書の送付と到着を相互の連絡で確認する。また、当事者Aの意思が当事者Bに伝達されたことは、Bの捺印がなされた文書がAに保持されることで確認される。

郵便を利用して文書を送信する場合、配達確認を利用することで確認可能である。

(c) 当事者Bが、当事者Aが伝達していない情報を意思と認識する

当事者Bの捺印がなされた文書を当事者Aが受け取ることで、当事者Aは、当事者Bが認識した意思が、自らが発した意思であることを確認できる。

(d)　当事者Ａの意思と、当事者Ｂが同意した内容とが異なる

当事者Ｂの捺印がなされた文書を当事者Ａが受け取ることで、当事者Ａは、自らが発した意思と当事者Ｂが認識した意思とが一致していることを確認できる。

(e)　プロセス実施後、双方の当事者のいずれかによる、プロセスの一部または全体の否認

相互に意思を示す文書を保持することで、プロセス全体の否認は回避できる。また、交換する文書の内容に、Ａからの発信日、Ｂの受信日、Ｂの受諾日、担当者、内容、納期等、否認を回避したい事項を記述しておくことで、個別の項目についての否認を回避できる。

郵便を利用して文書を交換する場合、Ｂによる受信の否認を回避する為には、配達証明が、文書の内容の否認を回避する為には、内容証明が、また、発信時刻の無保証によるプロセス否認を回避するためには、郵便の引受時刻証明が、それぞれ利用可能である。

(f)　機密情報の漏洩

文書受け渡しに関わり、第三者の手を渡らせない為に、対面による確認行為を行うことも可能である。

(7)　電子商取引におけるトラブルの分類

以上に基づき、当事者Ａと当事者Ｂの間での電子商取引のトラブルについて、表２－７に分類・整理する。また、従来の商取引における、遠隔地間での文書交換の例である、郵便による対応を、参考として付記する。

表 2-7 電子商取引におけるトラブルの分類

分類	当事者 A	機器 A	通信経路	機器 B	当事者 B	郵便による対応（参考）
(a)　プロセス実施が不適当	資格未確認 権限未確認				資格未確認 権限未確認	
	本人未確認				本人未確認	配達証明
(b)　当事者 A の意思が当事者 B に伝達されない	宛先誤指示		誤配	成りすまし	成りすまし	配達証明
		情報消滅	情報消滅	情報消滅		配達証明
(c)　当事者 B が、当事者 A が伝達していない情報を意思と認識する	成りすまし	成りすまし				配達証明
(d)　当事者 A の意思と、当事者 B が同意した内容とが異なる		不完全記録 改竄 不完全送信	不完全受信 改竄 不完全送信	不完全受信 不完全記録 改竄		内容証明
(e)　双方の当事者のいずれかによる、プロセスの一部または全体の否認	存在無保証 資格無保証 本人無保証	送信内容無保証	受信内容無保証 送信内容無保証	受信内容無保証	存在無保証 資格無保証 本人無保証	内容証明
		送信無保証 送信日時無保証	受信無保証 受信日時無保証 送信無保証 送信日時無保証	受信無保証 受信日時無保証		引受時刻証明 配達証明

表中、無保証とは、プロセスにおいて実施された内容が改竄されることなく保存されていることを証明できないことを意味する。すなわち、実施されたことの記録が、消滅（事故）、消去（故意）、変化（事故）、改竄（故意）のいずれもされていないことを証明できなければ、無保証となる。

2.2　トラブル回避のための要件

前節では検討対象とする企業間取引モデルを定義した上で、取引の成立に関するトラブルの原因について分析を行った。

本節では前記のトラブルを防止するために、取引の実行段階でどの様な証明内容を得ておかねばならないかについて記述している。そしてここに挙げる証明項目で前記のトラブルが回避できることを確認している。

検討対象としている取引モデルは、取引に先立ち取引関係者の間に基本契約が成立していることを想定している。トラブル回避のためには、基本契約であらかじめ何を持って本節の証明とするかについて取引関係者の間で合意しておくことが必要である。

各証明項目は説明をわかりやすくするため機能をできるだけ単純化しているが、実際の仕組みではこれらの証明項目は複合的に実現されるのが合理的である。実現手段については次節で記述されるが、本節の証明項目と必ずしも１対１になっていないことに注意されたい。

2.2.1　本人証明

(1)　定義

ネットワーク上の人物について、ある時点において、その人物が現実世界に存在する特定の人物であることと、かつその人物の会社名、所属部署名や役職などの所属に関する属性情報を証明するものである。なお、後者の属性情報は、時間の経過とともに変化するため、この属性情報の変更の通知を証明要求時にのみ行うか、もしくは適宜、変更がなされた時点で関係者に通知するか否かなどの通知方法についての問題は運用面で生ずる。

本証明を実施する機関としては、本人が所属する会社、組織、及びそれ以外の第三者機関の場合、もしくは、１つないしは複数の個人の場合が想定される。

本証明の要求は、契約当事者でかつ相手方の本人証明を要求する人物、及び契約当事者でかつ相手側に本人認証を行う必要がある人物、および契約当事者以外の第三者が要求する場合が想定される。

(2)　必要性

例えば、ネットワークを介した取引において、成り済ましを防止するために必要となる。偽の取引相手との通信によって生じる損害としては、機密情報の漏洩や虚偽の取り引きによる経済的損失が考えられる。

2.2.2　本人資格証明

(1)　定義

ネットワーク上の人物について、ある時点において、その人物が有する権限に関する属性情報を証明するものである。但し、権限に関する情報が、２．２．１の本人証明に

よる所属に関する属性情報で、十分である場合は、その属性情報とその属性が有する権限（例えば、本人が所属する組織の責任内規など）を以って、本証明は実現可能である。なお、２．２．１の所属情報と同じく、この権限に関する情報についても、時間の経過とともに変化するため、この属性情報の変更の通知を証明要求時にのみ行うか、もしくは適宜、変更がなされた時点で関係者に通知するか否かなどの通知方法についての問題は運用面で生ずる。

本証明を実施する機関としては、本人が所属する会社、組織、及びそれ以外の第三者機関の場合、もしくは、１つないしは複数の個人想定される。

本証明の要求は、契約当事者でかつ相手方の本人証明を要求する人物、及び契約当事者でかつ相手側に本人認証を行う必要がある人物、および契約当事者以外の第三者が要求する場合が想定される。

(2)　必要性

例えば、ネットワーク上での資材の発注において、発注を要求した当事者が、その発注契約について、相応の権限を有しているかどうかを確認するために必要となる、但し、会社間の基本契約により、大多数の場合は、発注を受ける側は、発注を要求した当事者が、発注側の会社に所属する人物であることが確認するのみで、権限が無い当事者からの発注による損害は、発注側の会社の責任となる場合が多いが、かようなトラブルを未然に防止する上で本証明は必要と思われる。

2.2.3　発行証明

(1)　定義

ネットワークを介したＡとＢの取引に於いて、ＡがＢあてに発行した文書mが存在する場合、文書mがＡによって発行されたことをＡが証明するもの。この証明の存在により、Ａは文書mをＢ宛に発行したことを否定できない。

証明される内容は下記である。

- 文書mは、Ａによって作成されたものであること。
- 文書mは、Ｂ宛に発行されたものであること。

但し、ここでＡとは、公開鍵Ａに対応する秘密鍵の持ち主であることを意味しているに過ぎず、実社会で特定の存在である人間や組織を意味しているわけではない。公開鍵Ａに対応する秘密鍵の持ち主が、実社会でどの様な存在であるかについては、別の証明（本人証明、資格証明）に依存する。

(2)　必要性

文書mの発行者Ａが、一連の取引に関連する文書mの送信の事実を否定し、mが関係する取引についてＡが無効の主張を行うケースが想定される。この場合Ｂは、取引の有効性を立証するために、Ａが発行を否定している文書mがＡによって発行されたことを

証明する必要が出てくる。

上記の例のように、本証明を必要とするのは、通常文書mの受領者であるBである。

(3) 補足説明

「発行証明」という用語であるが、ISO/IEC 13888 Non-repudiation ではほぼ同様な内容について、「non-repudiation of origin」と表現している。

2.2.4 受領証明

(1) 定義

ネットワークを介したAとBとの取引に於いて、AがB宛に発行した文書mが存在する場合、文書mがBによって受け取られたことをBが証明するもの。この証明の存在により、BはAからの文書mを受領したことを否定できない。

証明される内容は下記である。

- 文書mはBによって受け取られたこと。
- 文書mはAによって作成されたものであること。

但し、ここでBとは、公開鍵Bに対応する秘密鍵の持ち主であることを意味しているに過ぎず、実社会で特定の存在である人間や組織を意味しているわけではない。公開鍵Bに対応する秘密鍵の持ち主が、実社会でどの様な存在であるかについては、別の証明（本人証明、資格証明）に依存する。

この証明はBによる受け取り確認により可能となるものだが、証明としてはBがmの発行者が、単に公開鍵Aに対応する秘密鍵の持ち主であることを確認するだけである。従ってこの証明をAが利用する際、Aは別の手段（本人証明、資格証明）で秘密鍵Aの持ち主と同一であることを証明する必要がある。

(2) 必要性

一連の取引に関連してAがBあてに発行した文書mが何らかのトラブルでBに届いていなかったり、あるいはBが悪意を持って当該取引を無効にするため、文書mの受け取りを否認するケースが想定される。このような場合、Bが文書mを受け取ったという確証をAが所有することでトラブルが回避される。

上記の例のように、本証明を必要とするのは、通常、文書mの発行者であるAである。

(3) 補足説明

「受領証明」という用語であるが、ISO/IEC 13888 Non-repudiation ではほぼ同様な機能について、「non-repudiation of delivery」と表現している。

2.2.5 取引データ完全性の証明

(1) 定義

Aによって発行された取引に関係する文書mが存在するとき、mが発行時点から改竄

等の修正を受けることなく、完全性を維持していることの証明。

証明される内容は

- 文書mが発行時点から改竄等の変更を受けていないこと。
- 文書mはAによって発行されたものであること。

この証明は文書の発行者であるAが必要とする場合もあるし、A以外の主体が必要とする場合もある。

(2) 必要性

取引合意内容の証明が必要なことは、デジタルな世界では既存の社会での商取引にも増して重要性を帯びてくる。

例えば、関係者（取引当事者または、第三者）がその内容を改竄した場合に、商行為の基盤となっている「取引内容の完全性」が証明されなくなるわけで、そうなってしまっては商行為も何も行えない環境しか残らないのである。

同時に、契約不履行、詐欺、損害賠償請求といった法的手段を伴う行為に対応できる認証書（法的証拠能力）が必要になる所以である。

(3) 解説及び説明の補足

発行文書が一連の取引の中でどの様な意味合いをもって発行されたのかは、取引プロセスに関する事前の取り決め、文書の内容、文書の発行日時、等で決定される。本証明は純粋に文書の完全性を証明するものである。

定義の説明中のAとは、公開鍵Aに対応する秘密鍵の持ち主であることを意味しているに過ぎず、実社会で特定の存在である人間や組織を意味しているわけではない。公開鍵Aに対応する秘密鍵Aの持ち主が、実社会でどの様なそんざいであるかについては、別の証明（本人証明、資格証明）に依存する。

2.2.6 時刻証明

(1) 定義

取引者間に共通の時刻における、事象（イベント）の発生もしくはデータの存在を証明する。事象にはその属性として時刻が付随する。電子的な情報処理においては電子的処理の状態遷移に対して時刻印を付す意味があるが、実社会においては、ある時刻に何かが起こったという事象発生に時刻を関連するだけでなく、ある時刻にその状態であったこと、あるいはその時刻にデータが存在したことを証明するために時刻印と関連させる必要性がある。

(2) 必要性

時刻証明を誰が行うかは場合による。あるデータや事象の所有者が過去のある時刻に事象やデータが存在することを証明する場合と、その反対に、問題の相手が過去のある時刻でデータを入手していたり、ある事象と関わっていることを立証する場合がある。

例えば、電子メールは送信者から受信者までの間を幾つかのコンピュータでリレーされる。経路上のコンピュータがいつ処理するかを送信者は知ることができない。送信期限が決められていて、着信時刻の遅れが想定される場合には送信時刻の証明を行うニーズがある。着信から一定期間にアクションが要求されている場合、送信者側は、受信者の受信時刻を証明するニーズがある。催促状を送るような場合、送信者は受信時刻を証明する意味がある。

表 2-8　証明一覧

	証明項目		制限事項	証明者例（注1）
本人証明	被証明者が所属する会社名	（被証明者の所属、役職、等の属性）	証明日時and/or有効期限	認証機関
資格証明	被証明者の資格内容		証明日時and/or有効期限	認証機関
発行証明(by A)	発行文書の発行者	発行文書の宛先（受領予定者）		発行者
受領証明(by B)	発行文書の受領者	発行文書の発行者		受領者
取引データ完全性証明	発行文書の発行者	発行文書の非改竄性		文書自体
発行時刻証明	発行文書の発行時刻			第三者機関
受領時刻証明	発行文書の受領時刻			第三者機関

（注1）証明者は2．3で記述される実現方法に依存する。

表 2-9　トラブル回避のための証明

トラブル	原因									
	発行者A	利用証明	機器A	利用証明	通信経路	利用証明	機器B	利用証明	受領者B	利用証明
プロセス実施が不適当	B資格未確認	B本人資格証明							A資格未確認	A本人資格証明
	B権限未確認								A権限未確認	
	B本人未確認	B本人証明							A本人未確認	A本人証明
当事者Aの意志が当事者Bに伝達されない	宛先誤指示	B受領証明			誤配	B受領証明	成りすまし	B受領証明＋B本人証明	成りすまし	B受領証明＋B本人証明
			情報消滅	B受領証明	情報消滅	B受領証明	情報消滅	B受領証明		
当事者Bが当事者Aが伝達していない情報を意志として誤認する	成りすまし	A発行証明＋A本人証明	成りすまし	A発行証明＋A本人証明						
当事者Aの意志と当事者Bが同意した内容が異なる	(事後)改竄	データ完全性証明	不完全記録	データ完全性証明	不完全受信	データ完全性証明	不完全受信	データ完全性証明	改竄	データ完全性証明
			改竄		改竄		不完全記録			
			不完全送信		不完全送信		改竄			
双方の当事者のいずれかによるプロセスの一部または全部の否認	A存在無保証	A本人証明＋発行時刻証明	送信内容無保証	取引データ完全性証明	受信内容無保証	取引データ完全性証明	受信内容無保証	取引データ完全性証明		
	A資格無保証	A本人資格証明＋発行時刻証明	送信無保証	受領証明	送信内容無保証	取引データ完全性証明	受信無保証	受領証明		
	A本人無保証	A本人証明＋発行時刻証明	送信日時無保証	発行時刻証明	受信無保証	受領証明	受信日時無保証	受領時刻証明		
					受信日時無保証					
					送信無保証	受領証明				
					送信日時無保証					

2.3　実現方法

前節では企業間取引におけるトラブル回避に必要な証明項目について説明した。本節では前節で説明したトラブル回避証明を実現する仕組みについて説明する。

2.3.1　システムパターン

目的のシステムを実現する上で骨格をなす概念は、インターネットを介してやり取りする文書（トランザクション）の発行者を特定し同時に通信経路における改竄を防止するための「電子署名」[1]と、顔が見えない取引相手が誰であるかを証明する「電子認証」[2]である。

現時点で電子署名と電子認証の両方について現実的に適用可能な技術は「公開鍵暗号方式」であるので、本検討ではＰＫＩをベースとしてトラブル回避証明を実現する仕組みを検討した。

企業間の商取引に於けるトラブル回避証明を実現する仕組みは、以下の観点から３つのパターンに分類できる。

- 証明の実現に関して、取引当事者以外に第三者が関与しているか否か。
- 取引を仲介する第三者が存在するか否か。

但し、公開鍵暗号方式における認証局の存在はベースとするＰＫＩの仕組みであるので、上記の第三者とはしていない。

（1）　当事者相対型

取引のトランザクションは相手との間でのみ交わされる。従って、トラブル回避証明を行うための証拠は取引の当事者が作成し保持する。

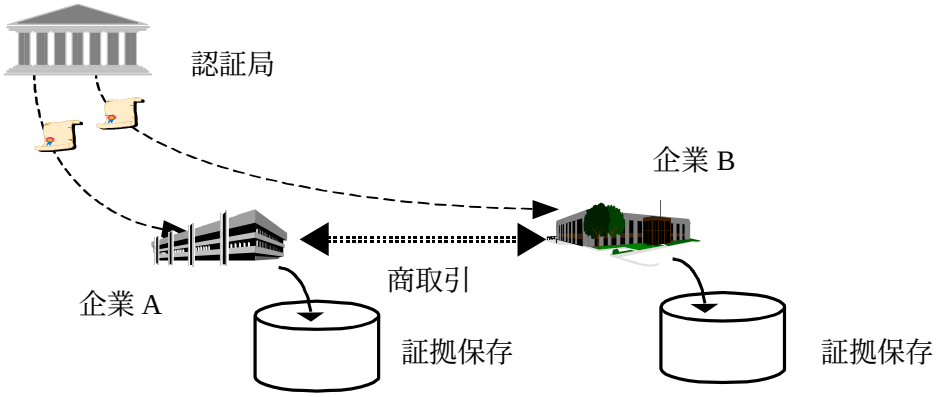


図 2-4　当事者相対型

認証局は必ずしも共通のひとつである必要はない。（以下同様）

（2）　第三者による証拠作成型

---

[1] ある(電子)文書を、ある人が作成、承諾、承認等したことを文書と関連付けて保存しておき、後日それが確認できる機能。

[2] 企業間電子商取引で利用される認証については１章参照。

取引のトランザクションに関するトラブル回避証明を行うための証拠を、第三者が作成する。証拠を第三者機関が保持する場合と、発行を受けた取引当事者が保持する場合の２種類のサブパターンがある。

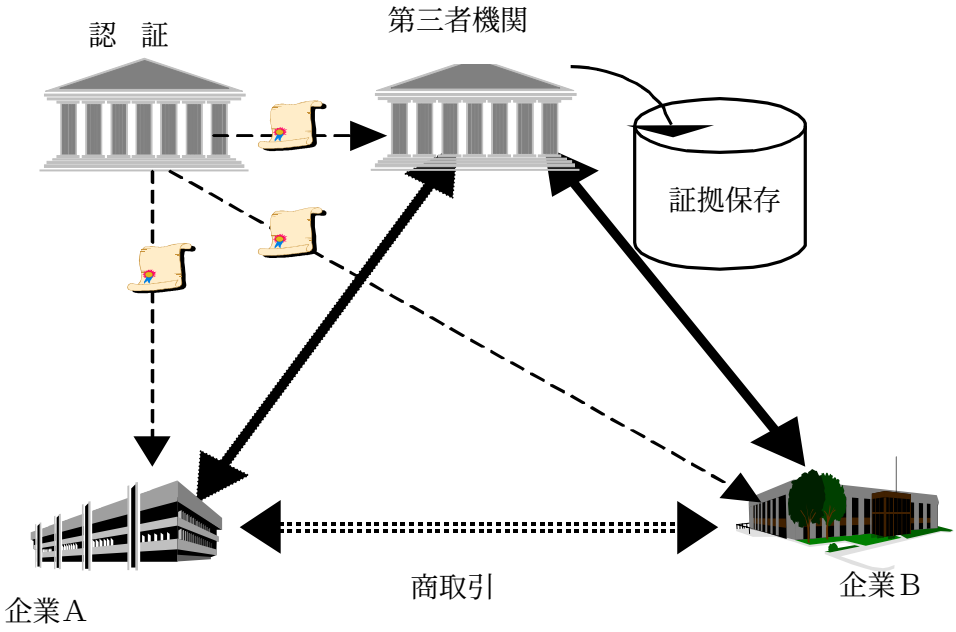


図 2-5　第三者による証拠作成型（第三者保全）

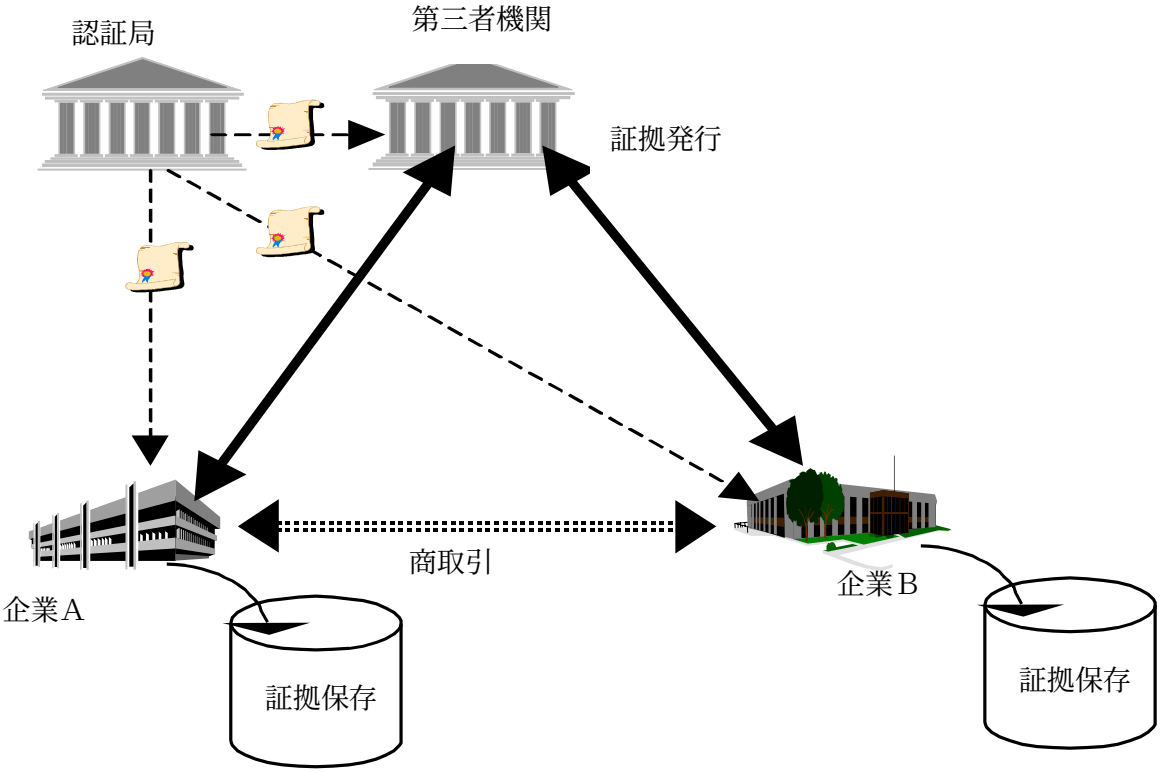


図 2-6　第三者による証拠作成型（当事者保全）

(3)　第三者介在型

取引のトランザクション自体を第三者を介して行う。取引のトランザクションに関するトラブル回避証明を行うための証拠は第三者が作成し保持する。

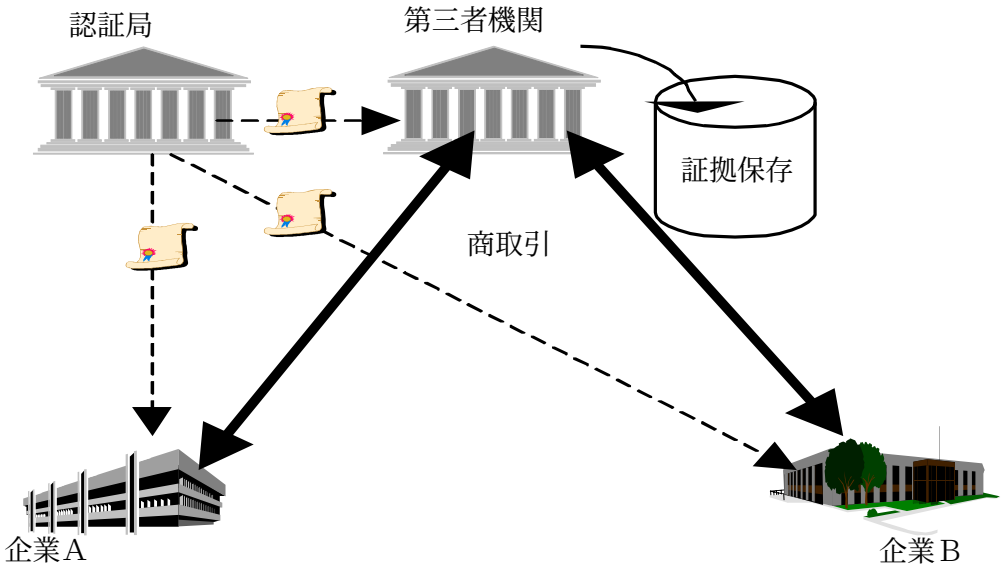


図 2-7　第三者介在型

2.3.2 システムパターンと証明項目

システムパターンにより証明可能な項目に相違がある。下表で○は証明する仕組みの構築が可能であることを示している。

表 2-10　システムパターンと証明項目

システムパターン	証拠保存	本人証明	本人資格証明	発行証明	受領証明	完全性証明	時刻証明
当事者相対型	取引当事者	○	○	○	○	○	
第三者による証拠作成型	取引当事者	○	○	○	○	○	○
	第三者機関	○	○	○	○	○	○
第三者介在型	第三者機関	○	○	○	○	○	○

2.3.3 当事者相対型

(1) 本人証明

署名者の企業所属個人実在性をX.509認証書で認証局が証明する。

署名者の企業所属個人実在性確認する署名の受取手はあらかじめ上記認証局を認知していることが前提である。（基本契約）

本人証明は発行証明および受領証明とリンクして使用されるので、実現方法については図２－８、図２－９を参照されたい。

(2) 本人資格証明

署名者の取引権限を証明する必要がある場合に、この認証書で署名者の取引に関する資格をX.509認証書で認証局が証明する。

各人毎の権限を認証書で証明するよりも、企業内の部門（その業務機能を遂行する担当者の集団）の権限と捉える方がシステムの運用上で便利な場合もある。実現方法としては、１．２．４で挙げたICカードを用いる方法がある。

本人資格証明は発行証明および受領証明とリンクして使用されるので、実現方法については図２－８、図２－９を参照されたい。

(3) 発行証明

取引のトランザクションの文書とその文書の宛先を、発行者が署名することで証明する。実現方法については図２－８を参照されたい。

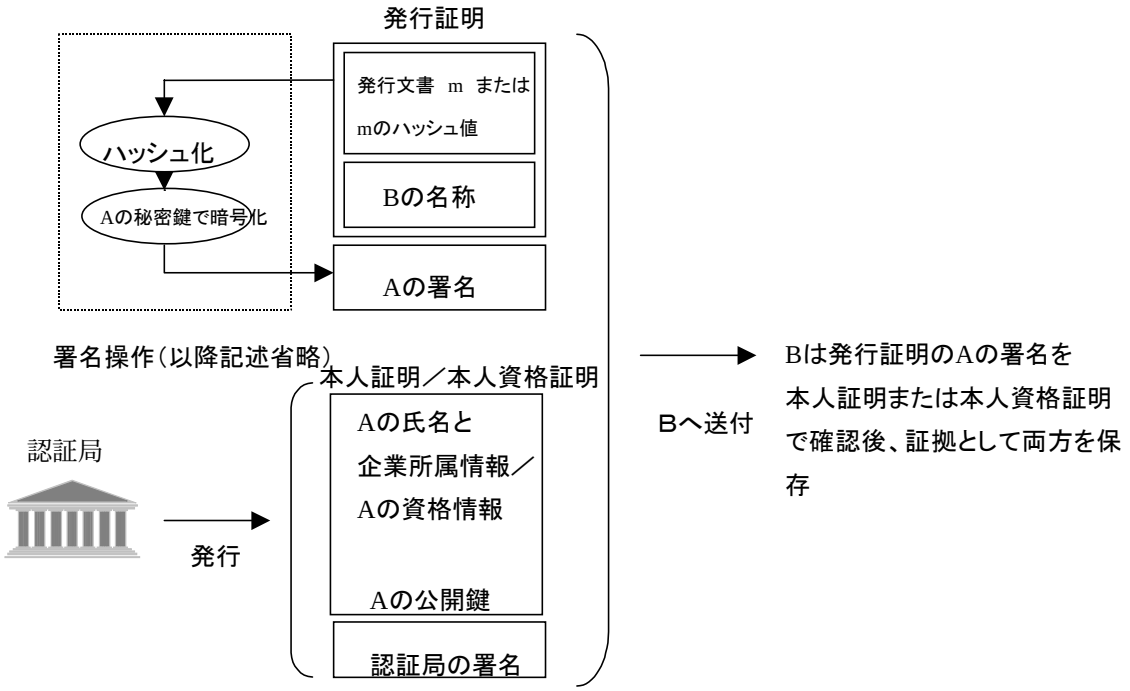


図 2-8　発行証明、完全性証明と本人証明／本人資格証明

(4)　受領証明

発行証明の証拠である｛発行文書＋宛先＋発行者署名｝に対して受領者がデジタル署名することで証明する。実現方法については図２－９を参照されたい。

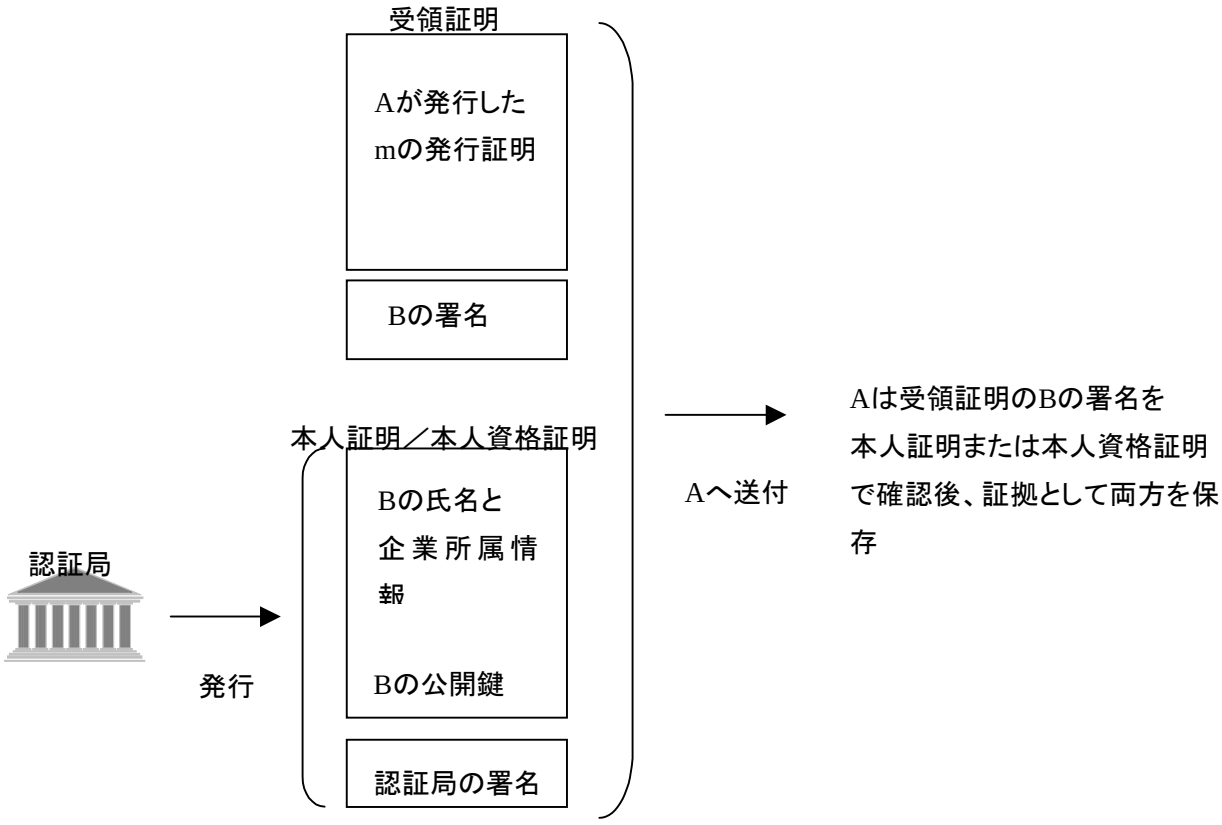


図 2-9　受領証明、本人証明／本人資格証明

(5)　完全性証明

発行文書に発行者が署名をすることで発行者以外のエンティティによる改竄は不可能になる。更に発行者による改竄を防止するためには、発行者による発行文書への署名が含まれている発行証明を受領者が証拠として保存すればよい。すなわち、発行者証明により完全性証明を兼ねることができる。

(6)　時刻証明

取引の双方にとって共通な時刻を管理する仕組みを、取引当事者だけで構築することは困難である。

しかしながらインターネットによらない従来の取引に於いても、事象の発生時刻については取引の双方が了解の上で証拠とすれば良いことが多く、そのレベルを当事者相対型で実現するには、発行証明、受領証明において署名する文書に署名時刻を記入して署

名を行えばよい。

＜参考＞ISO/IEC13888-3 における発行証明、受領証明

１）Non-repudiation of origin token(NRO token)

発行証明に対応する。ISO/IEC13888-3 での定義は以下となっている。

・メッセージ m の発行元 A によって作成。（または機関 C）

・A から受領先 B に送付。

・検証後 B が保存。

NRO token の構造

NRO token = text1 ‖ z1 ‖ Sa(z1)

但し　z1 = Pol ‖ f1 ‖ A ‖ B ‖ C ‖ Tg ‖ T1 ‖ Q ‖ Imp(m)

Pol: non-repudiation policy の識別子

f1: Non-repudiation of origin であることを示すフラグ

A: 文書 m の発行者の識別子

B: 文書 m の受領先の識別子（オプション）

C: 関係機関の識別子（オプション）

Token が C によって発行される場合は必須。このときは A の署名 Sa(z1)は C の署名 Sc(z1)に置き換える。

Tg: token 発行者時間による発行時刻

T1: 文書発行者時間による文書 m の送信時刻（オプション）

Q: 付加情報（オプション）

文書 m の識別子、署名あるいはハッシュ方式、認証書や有効性に関する情報　等

Imp(m): 文書 m もしくは m のハッシュ値を含む m の imprint

２）Non-repudiation of delivery token(NRD token)

受領証明に対応する。ISO/IEC13888-3 での定義は以下となっている。

・受領者 B によって作成。（あるいは機関 C）

・B からメッセージ m の発行者 A を含むエンティティに送付。

・検証後これらのエンティティが保存。

NRD token の構造

NRD token = text2 ‖ z2 ‖ Sb(z2)

但し　z2 = Pol ‖ f2 ‖ A ‖ B ‖ C ‖ Tg ‖ T2 ‖ Q ‖ Imp(m)

Pol: non-repudiation policy の識別子

F2: Non-repudiation of delivery であることを示すフラグ

A: B が文書 m の発行者であると主張する識別子（オプション）

B: 文書 m の受領者の識別子

C: 関係機関の識別子（オプション）

Token が C によって発行される場合は必須。このときは A の署名 Sb(z2)は C の署名 Sc(z2)に置き換える。

Tg: token 発行者時間による発行時刻

T2: 文書受領者時間による文書 m の受領時刻（オプション）

Q: 付加情報（オプション）

文書 m の識別子、署名あるいはハッシュ方式、認証書や有効性に関する情報　等

Imp(m): 文書 m もしくは m のハッシュ値を含む m の imprint

2.3.4 第三者による証拠作成型

(1)　本人証明

署名者の企業および第三者所属個人実在性を X.509 認証書で認証局が証明する。

署名者の企業および第三者所属個人実在性確認する署名の受取手はあらかじめ上記認証局を認知していることが前提である。（基本契約）

本人証明は発行証明および受領証明とリンクして使用されるので、実現方法については図２－１０を参照されたい。

(2)　本人資格証明

署名者の取引権限を証明する必要がある場合に、この認証書で署名者の取引に関する資格を X.509 認証書で認証局が証明する。

各人毎の権限を認証書で証明するよりも、企業内の部門（その業務機能を遂行する担当者の集団）の権限と捉える方がシステムの運用上で便利な場合もある。実現方法としては、１．２．４で挙げた IC カードを用いる方法がある。

本人資格証明は発行証明および受領証明とリンクして使用されるので、実現方法については図２－１０を参照されたい。

(3)　発行証明

取引トランザクションの発生を証明可能な情報（文書そのものでもよいがどのような情報にするかは当事者間で事前に認知必要：基本契約）とその情報の取引当事者を、第三者が署名することで証明する。この時、上記証拠情報に取引当事者も署名を行うことが望ましい。又、署名された証拠情報を第三者が保管する場合と、第三者は証拠情報の発行のみを行い、保管は取引当事者が行う場合の２サブパターンがある。実現方法については図２－１０を参照されたい。

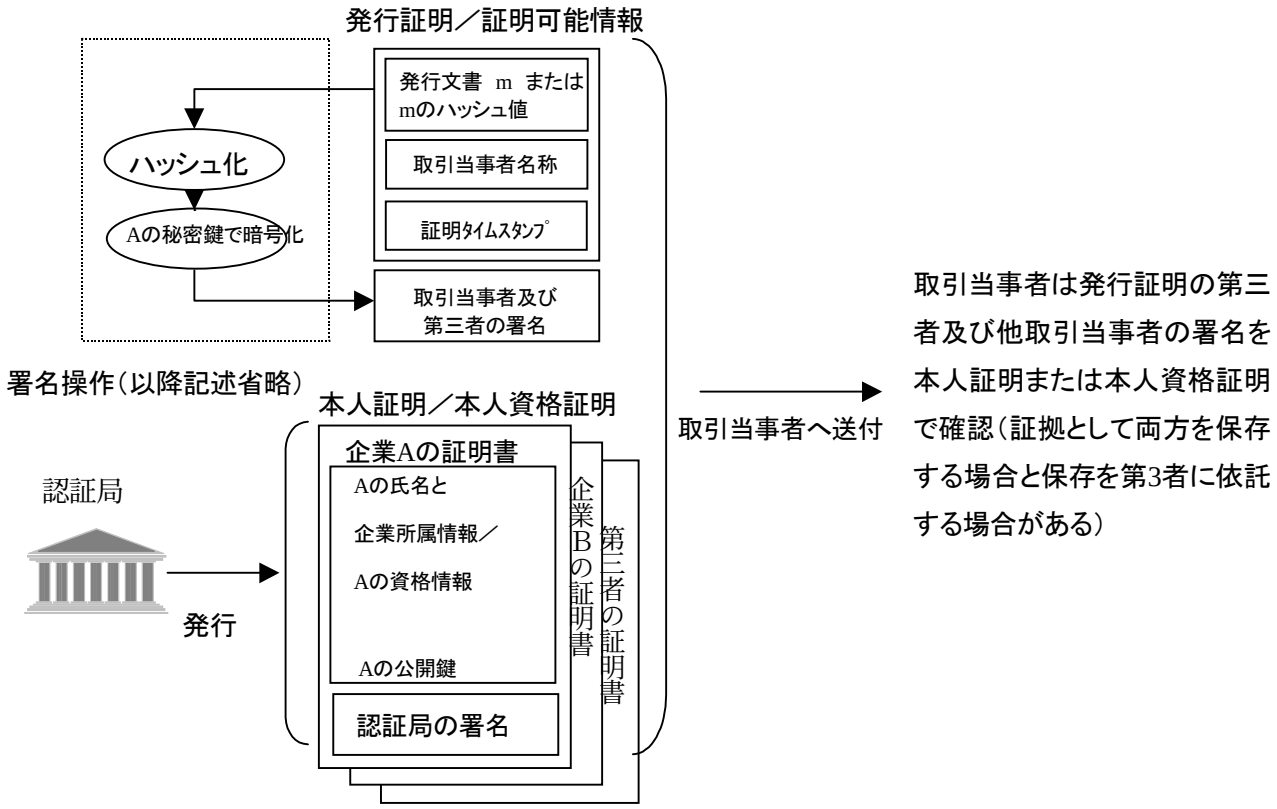


図 2-10　発行証明、完全性証明と本人証明／本人資格証明

(4)　受領証明

発行証明の証拠である｛取引トランザクションの発生を証明可能な情報＋取引当事者＋証明タイムスタンプ｝に対して第三者がデジタル署名することで証明する。この時前項で述べたとおり取引当事者も署名することが望ましい。実現方法については図２－１０を参照されたい。

(5)　完全性証明

証拠情報である｛取引トランザクションの発生を証明可能な情報＋取引当事者＋証明タイムスタンプ｝に対して第三者がデジタル署名することで証明する。この時前項で述べた証拠情報に第三者が署名をすることで第三者以外のエンティティによる改竄は不可能になる。更に第三者による改竄を防止するためには、取引当事者による証拠情報への署名が含まれていることが望ましい。

(6)　時刻証明

取引の双方にとって共通な時刻を管理する仕組みを、取引当事者だけで構築することは困難であることから、証明情報に第三者が証明タイムスタンプとることにより証明する。

この時、第三者がとる証明タイムスタンプの付け方について事前に当事者間で認知が必要となる。（基本契約）

2.3.5 第三者介在型

第三者介在型と前項（第三者による証拠作成型）との相違はビジネスモデルとして取引トランザクション自体の送受に第三者を使用しするか、取引当事者間で送受するかであり、第三者介在型での証明項目の証明方式は前項（第三者による証拠作成型）と同様である。

(1)　本人証明

署名者の企業および第三者所属個人実在性をX.509認証書で認証局が証明する。

署名者の企業および第三者所属個人実在性確認する署名の受取手はあらかじめ上記認証局を認知していることが前提である。（基本契約）

本人証明は発行証明および受領証明とリンクして使用されるので、実現方法については図２－１０を参照されたい。

(2)　本人資格証明

署名者の取引権限を証明する必要がある場合に、この認証書で署名者の取引に関する資格をX.509認証書で認証局が証明する。

各人毎の権限を認証書で証明するよりも、企業内の部門（その業務機能を遂行する担当者の集団）の権限と捉える方がシステムの運用上で便利な場合もある。実現方法としては、１．２．４で挙げたICカードを用いる方法がある。

本人資格証明は発行証明および受領証明とリンクして使用されるので、実現方法については図２－１０を参照されたい。

(3)　発行証明

取引トランザクションの発生を証明可能な情報（文書そのものでもよいがどのような情報にするかは当事者間で事前に認知必要：基本契約）とその情報の取引当事者を、第三者が署名することで証明する。この時、上記証拠情報に取引当事者も署名を行うことが望ましい。又、署名された証拠情報を第三者が保管する場合と、第三者は証拠情報の発行のみを行い、保管は取引当事者が行う場合の２サブパターンがある。実現方法については図２－１０を参照されたい。

(4)　受領証明

発行証明の証拠である｛取引トランザクションの発生を証明可能な情報＋取引当事者＋証明タイムスタンプ｝に対して第三者がデジタル署名することで証明する。この時、前項で述べたとおり取引当事者も署名することが望ましい。実現方法については図２－１０を参照されたい。

(5)　完全性証明

証拠情報である｛取引トランザクションの発生を証明可能な情報＋取引当事者＋証

明タイムスタンプ} に対して第三者がデジタル署名することで証明する。この時前項で述べた証拠情報に第三者が署名をすることで第三者以外のエンティティによる改竄は不可能になる。更に第三者による改竄を防止するためには、取引当事者による証拠情報への署名が含まれていることが望ましい。

(6)　時刻証明

取引の双方にとって共通な時刻を管理する仕組みを、取引当事者だけで構築することは困難であることから、証明情報に第三者が証明タイムスタンプとることにより証明する。

この時、第三者がとる証明タイムスタンプの付け方について事前に当事者間で認知が必要となる。（基本契約）

検討メンバー

ＥＣＯＭ

米倉　昭利　　電子商取引実証推進協議会 主席研究員
菅　　知之　　電子商取引実証推進協議会 主席研究員
加藤　寛之　　電子商取引実証推進協議会 主席研究員

顧問

大山　永昭　　東京工業大学　像情報工学研究施設　教授
須藤　修　　東京大学　社会情報研究所　助教授
岩下　直行　　日本銀行　金融研究所研究第二課　調査役

メンバー

坂本　弘章　　株式会社ＮＴＴデータ　技術開発本部マルチメディア技術センタ
　　セキュリティ担当　課長
田吹　隆明　　株式会社キャディックス　社長付き　シニアリーダー
深谷　清之　　財団法人金融情報システムセンター　総務部　参事役
保倉　豊　　グローバル・フレンドシップ株式会社　代表取締役社長
北田　容一　　株式会社三和銀行　決済業務部　部長代理
宮下　善和　　神鋼電機株式会社　商品開発部
藤本　武　　綜合警備保障株式会社　技術部情報通信課
星野　理　　株式会社帝国データバンク　企画部企画課
高橋　和博　　東電ソフトウェア株式会社　ＣＡＬＳ／ＥＣ技術部　主任
中道　一人　　日本アイ・ビー・エム株式会社　e-ビジネス事業
　　e-Commerce ソリューション事業部 EC ソリューション営業推進
　　主任ソリューション・セールス・スペシャリスト
板倉　和治　　日本電気株式会社　マルチメディアサービス事業企画部
　　エキスパート
光永　聖　　株式会社日立製作所　金融システム事業部
　　金融ソリューションシステム本部決済ソリューションセンタ
　　センタ長
出口　太郎　　株式会社富士総合研究所　社会基盤研究部　研究員
鍛冶　俊彦　　富士通株式会社　インターネットソリューション推進室
　　担当課長
清水　秀樹　　プライスウォーターハウスクーパース・コンサルタント株式会社

	ナレッジ・マネジメント部　マネジャー
河瀬　恭一	松下電器産業株式会社　公共システム営業本部システム推進部
	システム二課　主任技師
大谷　彰宏	三菱電機株式会社　流通・サービス・通信システム部
	ＥＣ事業推進グループ　専任
須田　章	安田火災海上保険株式会社　事務企画部企画グループ　副長

以上、企業名順

平成１２年3月発行予定
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