情 報 メ デ ィ ア 36－6
電子化知的財産・社会基盤 7－6
（2000．1．29）

ネットワーク取引における電子認証局のモデルの提案

関西大学大学院 総合情報学研究科　松田浩延
matsuda@osk.enicom.co.jp

概要

ネットワーク取引の発展が要請されている中、セキュリティの確保が重要となってきている。

本稿ではネットワーク取引のセキュリティを支える電子認証局について、取引参加者別による必要性の整理を行う。また、公的電子認証機関と民間電子認証機関の役割分担について考察し、民間電子認証機関のモデルを提案する。

注）ここでは「電子商取引(Electronic Commerce)」のうち、オープンネットワークを使用して契約の申し込みから成立までを行うものを、とくにネットワーク取引として定義する。[1]

A Model of Certification Authority in Electronic Commerce

Hironobu MATSUDA

ABSTRACT

Security is very important mechanism for the development of electronic commerce systems.

The purpose of this paper is to explain the necessity of certification authority, which supports the security of electronic commerce.

I describe in this paper, the role allotment of the public certification authority and the private certification authority.

And thus, propose a model of a private electronic attestation organization.

1. 背景

ネットワーク取引は、従来型取引と比較して供給者、需要者の双方に利便性の向上をもたらすため、今後の発展が期待されている。[2]

- 供給者の利便性：店舗関連コスト等の削減。商品・価格の更新の迅速化。マーケットの拡大。
- 需要者の利便性：地理的・時間的制約の解消。大量の情報検索。

一方、セキュリティへの不安がネットワーク取引での大きな阻害要因となっている。特に取引の相手方の真正性確認は現在のインターネット上では、ほとんどできないといった状態である。

ネットワーク取引の発展には、セキュリティの確保が急務である。

2. 現状の問題と電子認証局の必要性

ネットワーク取引のセキュリティを確保する技術の一つに公開鍵暗号方式[3]がある。公開鍵暗号方式とは共通鍵暗号システムの鍵配送のコストを軽減するものとして登場したもので、関連する２つの鍵(公開鍵と秘密鍵)を用意し、その一方を公開するので公開鍵暗号と呼ばれる。

公開鍵暗号システムはその一組(2 つ)の鍵を使う特性から、通常の暗号としての機能(秘匿機能)の他にデジタル署名としての機能(認証機能)を持つ。デジタル署名とは、公開鍵で復号化可能なメッセージは秘密鍵で暗号化したメッセージであると推定できることを利用して、秘密鍵の所有者を特定し本人確認

を行うものである。

この公開鍵暗号方式のもつ通常の暗号としての用途とデジタル署名としての用途を組み合わせることによりネットワークセキュリティの安全性は確保できるように思われがちである。(表1参照)

表 1：暗号と署名のセキュリティ効果

	秘匿性	完全性	同一性	否認防止
通常の送信	×	×	×	×
暗号(秘匿機能)	○	○	×	×
署名(認証機能)	×	○	○	○
暗号＋署名	○	○	○	○

しかし、このデジタル署名でも本当の意味での認証の確保は困難である。なぜなら、公開鍵は「公開鍵を事前に公開する」という点が弱点となるからである。

デジタル署名は公開鍵に対応する秘密鍵の持ち主の同一性を保証するが、その持ち主が名乗っている本人であることまでは保証できない。

たとえば、Aの知らないところでBがAの公開鍵として偽の鍵を公開された場合、第三者がこの鍵はAのものであると信用する危険があるということが挙げられる。

この問題を解決するのが電子認証局(Certification Authority)である。以下では電子認証局について考察し、電子認証局が社会インフラとして重要な役割を果たすことを示す。

3. 電子認証局

3.1. 公的機関と民間機関の役割分担

電子認証局の運営を公的機関が行うか私的機関が行うかはつねに議論されている。[4 5]

取引の段階から見ると認証の機能は、本人確認(Identification)と権限付与(Authorization)の2段階に区分できる[6]。本人確認とは送られてきた情報が、本人が発信したもの確認することであり、権限付与とは確認した本人に取引の当事者能力があるか確認することである。

認証のうち本人確認については公的機関の担当とするのが妥当であると考える。信用の基本は公的機関の証明書に負うところが多く、またすべての法人を網羅する点でも公的機関は優れているのでこの部分につては民間の役割とする利点はない。

法務省が商業登記台帳を基に公的電子認証機関の設立を検討している[7]が、これはまさに本人確認を担当するものといえる。

2段目の権限付与については公的機関がこれを行うべきではなく民間機関の役割とすべきであろう。なぜなら、権限付与は与信と密接に関連するものであり、公的機関が民間事業者や個人の与信を設定することは好ましくないと考えられるからである。

この役割分担に基づいて実際に電子認証局を用いてネットワーク取引が行われる過程を示したものが図1である。

1.まず、ネットワーク上で商品を販売する企業(A)は自分用の秘密鍵と与信の発行を民間電子認証局(C)へ申し込む。

2.申し込みを受けたCはAの窓口での審査(将来的にはAの示す公的電子認証機関発行の認証書)をもとにAの存在確認を行う。

3.さらにCはAについての与信調査を行う。
4.その後CはAへの秘密鍵発行と、3で調査したAの与信情報の公開を行う。
5.Aはネットワーク上で自己の公開鍵及び与信情報の存在個所を示す。
6.Aとの取引を望む者(B)は5.の情報からCで公開されている公開鍵と与信情報を入手する。
7.Bは取引情報の秘匿と確実にAだけにメッセージが届くようにAの公開鍵で暗号化した契約の申し込みメッセージをAへ送信する。
8.Aは確かにAが送信したこと及び事後に否認しないことを約束するため、自分の秘密鍵で暗号化した契約の承諾メッセージをBへ送信する。

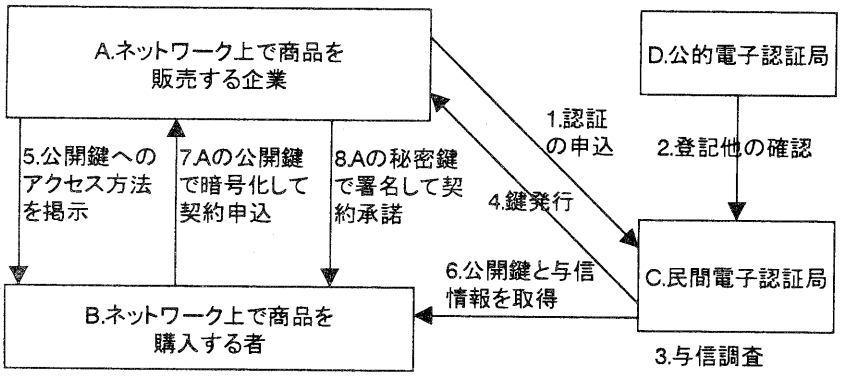

図 1：電子認証局を用いてネットワーク取引が行われる過程

3.2. 電子認証局が必要な取引形態

電子認証局を必要とするネットワーク取引の参加者に注目して、電子認証局とどのような関わりを持つか分類した。(表2参照)

1.企業が企業の認証を行う。
1-1.企業間の取引きが固定的である場合
例)あるメーカが常時取引きのある部品メーカに発注処理を行う。
1-2.新規の取引関係である場合
例)インターネット上で公開入札を行う。
2.企業が個人の認証を行う。
例)銀行がオンライン取引きの相手となる顧客の認証を行う。
3.個人が企業の認証を行う。
例)インターネットのWEBサイトで見つけたオンラインショップから商品を購入する。
4.個人が個人の認証を行う。
例)インターネットのNewsシステムで見つけたフリーマーケットで商品を購入する。

1-1.の場合、常態化した取引相手について与信管理をする必要は薄いと考えられる。
さらにこういった場合VPN(Virtual Private Network)を構築するのが一般的であると思われるので、電子認証局の必要性は少ないと考える。

2.の場合には、認証する個人の情報は既に何らかのネットワークを介さない形式で取得済みであることが多い。

(銀行や証券会社などは、脱税やマネーロンダリング防止のために個人を特定できる証明書の提示を求めることが普通である。)

そこで、これらの情報を基に企業側が独自に私的な電子認証局を運営することが可能である。

顧客の預金残高や口座番号を外部に流出させないという要請等から考えても、外部の公共的な電子認証局に委託するより私的なものを運営する方が望ましいと考えられる。

4.の場合、フリーマーケット等でやり取りされる商品はその金額が低く電子認証局などを運営しても費用対効果の点で問題があると思われる。

しかし実際には、売る側からは購入者に支払能力があるか確認したいであろうし、買う側からは振込後商品が送られてこないのではないかといった不安があるであろう。

現実的には商品の受渡という物理的な作業がある限り、代金引換郵便などのサービスを利用することでこれらの問題は解消可能である。

最後に1-2.や3.のような場合であるが、ここに本来の意味での電子認証局の必要性があるのではないかと考えられる。

初めて取り引きを行う企業について、その企業の支払能力や社会的信用度は重要である。

ネットワークではない取引においてはその外観や雰囲気などから信用度を掴もうとするがネットワーク上では非常に困難である。そこで、電子認証局が予め与信調査を行い、その結果をネットワーク上で企業を特定できる公開鍵情報とともに公表することが重要となる。

このことから、民間電子認証局は、継続的な取引関係の無い企業対企業のネットワーク取引や、企業対個人のネットワーク取引を円滑に行うために必要な社会基盤であると考えられる。

表 2：ネットワーク取引の参加者の違いによる電子認証局の必要性

	認証要求者	認証対象者	必要とされる認証機構
1-1	企業	企業 (継続的取引関係にある場合)	認証局ではなく仮想専用線の機能を使用
1-2	企業	企業	公共的な電子認証局
2	企業	個人	私的な認証局
3	個人	企業	公共的な電子認証局
4	個人	個人	認証局は不要

3.3. 民間電子認証局に対する法規制

既存の通信ネットワークの安全性が電気通信事業者に依存しており、故に電気通信事業法によってその規模により免許・登録・届出等の制度を適用しているのに比べて、同じ社会インフラであるセキュリティを担当する電子認証局の運営が自由に行えるというのはバランスを欠くといえる。よって公的機関による何らかの規制は必要であると考える。

民間電子認証局に対する規制の形態としては免許・登録・届出・認定・指定等が挙げられるが、郵政省では認定制度を採用する動向にある。[8]

認定基準を公開して最終的にどの電子認証局を使用するかはユーザの判断に委ねるこの方式の採用は

理解できる。ただし認定を受けない電子認証局の存在を認めることになるので、出来ればもう少し規制色の強い登録制度の方が良いのではないかと思われる。

認定方式とは別に、認証局自体の信用を法規制することによって確保するという方法が提案されているがこれには反対である。なぜなら、国や公的機関に保証してもらうより信用に値するシステムを公開することの方がより高い信用を得られると考えられるからである。あくまでも公的機関の電子認証における役割は本人確認だけにとどめ、それ以外の機能・業務は民間の分野とするのが望ましいと考える。

これらの安全性を確保するための規制とは別に、公開鍵に対応する秘密鍵の寄託機関として電子認証局を位置づけることが検討されているようであるがこれにも反対である。特に犯罪捜査の際に秘密鍵を取得することが検討されているようであるが、これは通信の秘密を侵すものであり到底許容し得ない。実際の犯罪者は電子認証機関による暗号システムなどは使用しないであろう。

4. 民間電子認証局のモデルの提案

認証局運用ガイドライン[9]では、認証局の業務として下記のものを挙げている。

1. 審査：申請者の本人確認及び申請情報の真正性確認を行う。
2. 鍵管理：鍵の生成・保管・破棄・定期更新を行う。
3. 認証書管理：認証書の作成・送付・保管・開示を行う。
4. 失効管理：鍵失効リストの生成・保管・開示を行う。
5. 加入者秘密情報管理：加入者秘密情報の保管・アクセス制限を行う。
6. 監査：定期的な監査の実施と監査情報の保管を行う。

また、rfc2527[10]では、電子認証局の業務を RA(Registration Authority)と狭義の CA(Certification Authority)に分けている。

これらを総合すると、電子認証局とは複数の業務の集合であり、各業務はそれぞれ分離可能であることが判る。

代表的な業務の分類例を図２に示す。

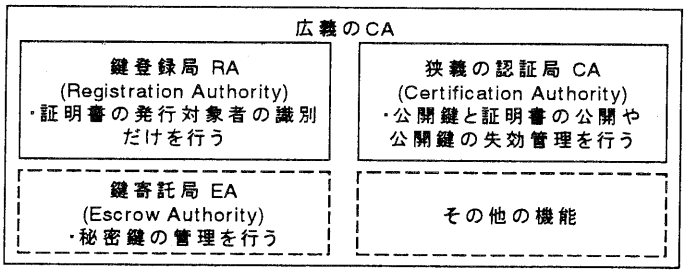

図 2：電子認証局の業務の分類

上記の例をもとに、民間電子認証局の業務分類を提案してみる。(図３参照)

電子認証局の業務の流れとして、まず被認証者からの申込時にその申込者が実際に存在する者であるか、また本人であるかどうかを確認するところから始まる。この本人確認を行う作業を審査業務とする。次に被認証者の与信調査を行う。その後公開鍵と秘密鍵の組を作成し、秘密鍵は被認証者に送付する。公開鍵については与信情報とともに認証書を作成し電子認証局のディレクトリで公開する。これらの業務とは別に与信情報に基づき認証者が取り引きした結果発生した損害を補償する業務や、認証書を公開する費用を請求する課金業務などがある。

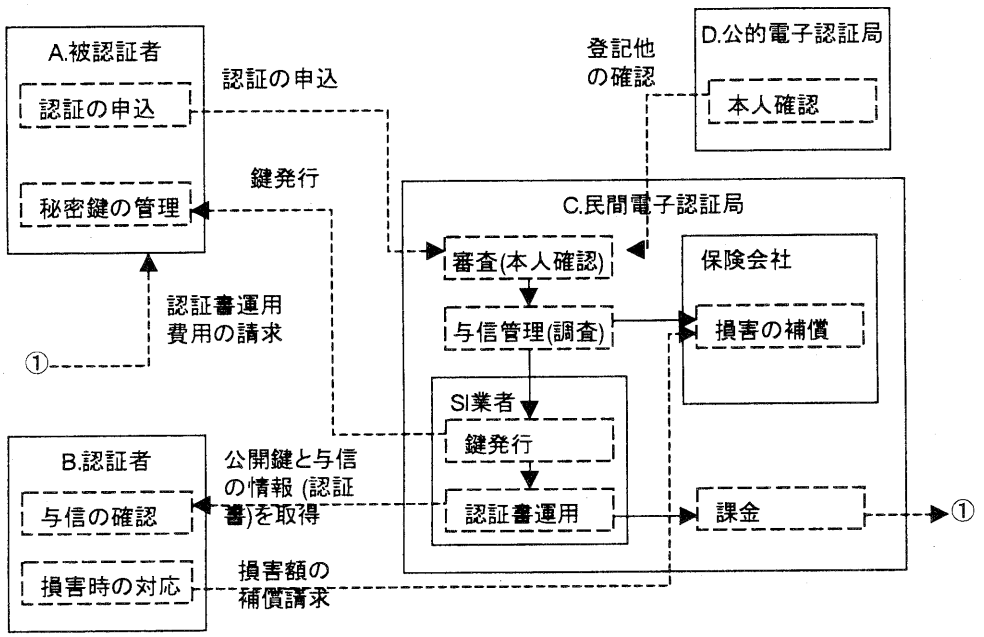

図 3：民間電子認証機関のモデル

以下では民間電子認証局の業務機能の詳細について検討してみる。

4.1. 審査業務 (認証登録業務)

公開鍵と実際の存在の紐付けを行うことにより同一性を確保する電子認証局の中枢機能である。

まず、認証の対象からの申し込みを受けてその対象が実際に存在するか確認する必要がある。次に申込者が本当に存在する対象と一致するか確認する必要がある。この確認(審査)が最も重要でありかつ困難なものであると予想される。

実際には対象者に窓口へ出向いてもらうか、郵便で確認を行うなどのネットワーク外での認証が必要であると考える。

ただし、公的電子認証機関の整備が行われ、すべての法人に公開鍵暗号システムによる鍵が付与される状況が整った場合には、この確認には公的電子認証機関の本人確認の情報が利用できるであろう。

4.2. 与信管理業務(加入者情報管理業務)

この業務は、本来の電子認証局の業務ではないが、民間の電子認証局の成否はこの機能の運用次第であると考える。

電子認証局の運営主体は与信管理が行える民間調査会社・債券格付け機関等が中心となるべきであると考えられる。

実際の機能としては、現在与信調査会社や格付け会社などで行われているものと同様のものになるであろう。

4.3. 鍵発行業務(鍵管理業務)

公開鍵と秘密鍵の組は、アルゴリズムが確定すると電子認証局だけでなくユーザが作成することも可能である。しかし、鍵発行は認証機関で行うべきであろう。なぜなら、ユーザから提供された公開鍵だけを管理する場合、その公開鍵に対応する秘密鍵を正しくユーザが作成していることを証明できないためである。

但しこの場合、秘密鍵の保管は行わず、秘密鍵をユーザに渡した時点でその秘密鍵のコピーは破棄するべきである。なぜなら、電子認証局が 秘密鍵を保管する場合、検閲に関する問題が発生する可能性が高いからである。

秘密鍵を紛失してしまった場合は、秘密鍵の再発行をせずに、旧鍵を失効させ新しい鍵を作成するべきである。再発行によって初発行時に確保した信用に傷がつき、認証局の認証書全体の信頼を損ないかねないからである。

鍵の生成は、公開鍵システムの技術進歩や国際標準の新規制定・変更など技術的要素に起因する変動要素が多い。

よって、この機能を運営する主体はコンピュータシステムに詳しい SI 事業者等が担当するのが望ましいと考えられる。

4.4. 認証書運用業務(認証書管理発行業務)

登録された公開鍵に被認証者の固有情報や与信情報などを付与した認証書を作成し、電子認証局自身の公開鍵で署名を行い公開するという、電子認証医局の基幹業務であり、現行の電子認証業者(日本ベリサイン、サイバートラストジャパン・エントラストジャパン他)が主として行っている業務である。

今後はリポジトリの管理業務や、X.509 認証書[11]の生成業務、公開鍵の鍵長の増大への対応、公開鍵システムの技術的な変更(RSA から楕円曲線暗号システムなど)が主業務になるであろう。

当機能も鍵発行機能と同様に SI 業者などコンピュータ技術に特化した事業者が担当するべきであると考える。

4.5. 発生した損害の補償業務

ネットワーク取引における損害発生のうち、電子認証局に関わるものは次の 3 つが考えられる。

1.電子認証局が騙されて偽の認証書を設定した場合。

2.認証書の与信に基づいて取り引きしていたところ認証対象者が債務不履行に陥った場合。

3.電子認証局から秘密鍵が漏れた場合。

1 の偽の認証書については電子認証局がその損害を賠償すべきであると考える。なぜなら、電子認証局は与信調査に基づいて賠償の上限額を認証書に記載することが可能であり、電子認証局が騙されたということは与信調査に不備があったと考えられるからである。

当然のことながら、賠償額については認証書記載の上限を超えることはないものとすべきである。

2 の被認証者の債務不履行時における損害について、1 と同様に電子認証局がその損害を補償することを提案する。なぜなら、この債務不履行時の損害賠償こそがネットワーク取引を発展させる強い動機となり、ユーザが電子認証局の存在を必要とし、被認証者が費用を払ってまでも認証を受けようとする要因となるからである。ただし、補償額についてはこれが賠償とは異なり保険的性格のものであるため、保険料を徴収するなどの仕組みの検討が必要であると考えられる。

3 の秘密の管理については電子認証局に高度の管理責任が発生すると考えられ、無過失責任とまではいかないであろうが、高度の注意義務が発生すると考えられる。

そのため、システムのハッキングを受けた場合や、内部者による認証書(個人情報を含む)の漏洩があ

った場合には、ユーザがその漏洩の事実を示すことにより、無過失の証明責任を認証局側に負担させることが妥当であると考える。

4.6. 課金業務

民間電子認証局は、民間が行うものであるので当然何らかの収入の方法を検討しておく必要がある。

ここで、格付け機関や調査機関のモデルを基にその収入の方法を検討してみる。

民間電子認証機関の収入確保の方法として以下の2方式が考えられる。

1.公開鍵や認証書を必要とするユーザに鍵・認証書の参照毎に料金を徴収する方法。

2.信用調査の対象となる側から料金を徴収する方法。

方式1は、一度参照された鍵をコピーされると課金ができなくなることや、料金を回収する方法に難点があるなど問題が多い。

そこで公開鍵を使用することについては無料とし、課金については方式2を採用することを提案する。

この方式は公開鍵情報の利用者に課金しないので、利用者の電子認証局利用に対する抵抗を軽減でき、ネットワーク取引の推進という点から見ても推奨されると考える。

5. まとめ

現状のユーザニーズと暗号技術を考慮した場合、与信管理機能を持つ電子認証局が必要になってくることが予想されるので、その業務の詳細について検討を行った。

まず、公的機関の認証業務を本人確認に絞り込むことで、民間電子認証機関の発展する分野を確保できる。

次に民間電子認証機関が与信管理を主とすることで、消費者にとってはネットワーク取引が安心なものになり、供給者にとっては需要が拡大することでマーケットが拡大することになる。

これらの検討の過程において、新規の企業・企業間(BtoB)の電子商取引や企業・消費者間(BtoC)の電子商取引の発展には、電子認証局制度の確立が必須であることを示した。

今後の課題としては、与信情報の認証書への記述形式の標準化(X.509 との整合性)や国際取引における与信の取り扱いなどが挙げられる。

信用調査会社や債券格付け機関などがネットワーク取引の支え役として積極的に電子認証業務に参画することを期待する。

【参考文献】

[1] 信森毅博「認証と電子署名に関する法的問題」日本銀行金融研究所ディスカッションペーパーシリーズ No.98-J-6(1998/02)

[2] (財)金融情報システムセンター『電子決済研究会(第2部)報告書』(財)金融情報システムセンター(1997/02)

[3] 今井秀樹『暗号のおはなし－情報セキュリティの新しい鍵－』日本規格協会(1993/03)

[4] 岩村充「電子商取引と認証」『法とコンピュータ』No.17 法とコンピュータ学会 (1999/07)7 頁

[5] 高橋和之他『インターネットと法』有斐閣(1999/10)

[6] (財)金融情報システムセンター『金融業務における認証研究会報告書』(財)金融情報システムセンター(1998/04)

[7] 電子取引法制に関する研究会「電子取引法制に関する研究会(制度関係小委員会)報告書」法務省(1998/04)

[8] 暗号通信の在り方に関する研究会「暗号通信の在り方に関する研究会報告書」郵政省(1999/06)

[9] 電子商取引実証推進協議会 認証局検討ワーキンググループ『認証局運用ガイドライン(V1.0 版)』電子商取引実証推進協議会(ECOM) (1998/03)

[10] S. Chokhani/ W. Ford "Certificate Policy and Certification Practices Framework" IETF Request for Comments: 2527 (1999/3)

[11] ITU-T "The Directory: Authentication framework" ITU-T Recommendation X.509 (1997/08)