電子商取引のための認証局（CA：Certificate Authority）
－信頼できるビジネス環境構築のために－

中尾 康二
（株）KDD研究所

近年のインターネットの普及に伴い，家庭にいながらにしてショッピングをしたり，オークションに参加するといった便利な環境が現実のものになってきている．電子ショッピング，電子教育，電子医療，電子オークションなど，ネットワークを介して容易に，迅速に，商取引にかかわるサービス，いわゆる「電子商取引」を享受できる時代を迎えようとしている．このようなインターネットの世界では，実際に通信を行っている相手が見えないことにより，通信相手が本人かどうかを確認することがきわめて重要なこととなる[1]．特に，近年のネットワークのオープン化，広域化に伴い，世界各国の情報を簡単に入手でき，世界中のコンピュータシステムへのアクセスが容易になった反面，システムへの不正なアクセス（攻撃）やネットワークを流れる情報の漏洩が発生しやすい環境となり，信頼できるビジネス環境の構築が難しいといった局面を迎えている．たとえば，インターネットを用いたクレジットカードショッピングは便利ではあるが，注文を受け付ける仮想店舗（インターネット上の商店）が本当に実在の正しい商店であるかを確認せずにクレジットカードを利用すると，注文した商品が届かない，不当な金額を請求される，トラブルの問合せもできない（逃げられる）などの問題が生じる可能性があった．これらの不安要素を一掃し，信頼できるビジネス環境を構築するためには，通信相手の本人確認（以降，「認証」と呼ぶ）を十分に行うための手段が重要となる．

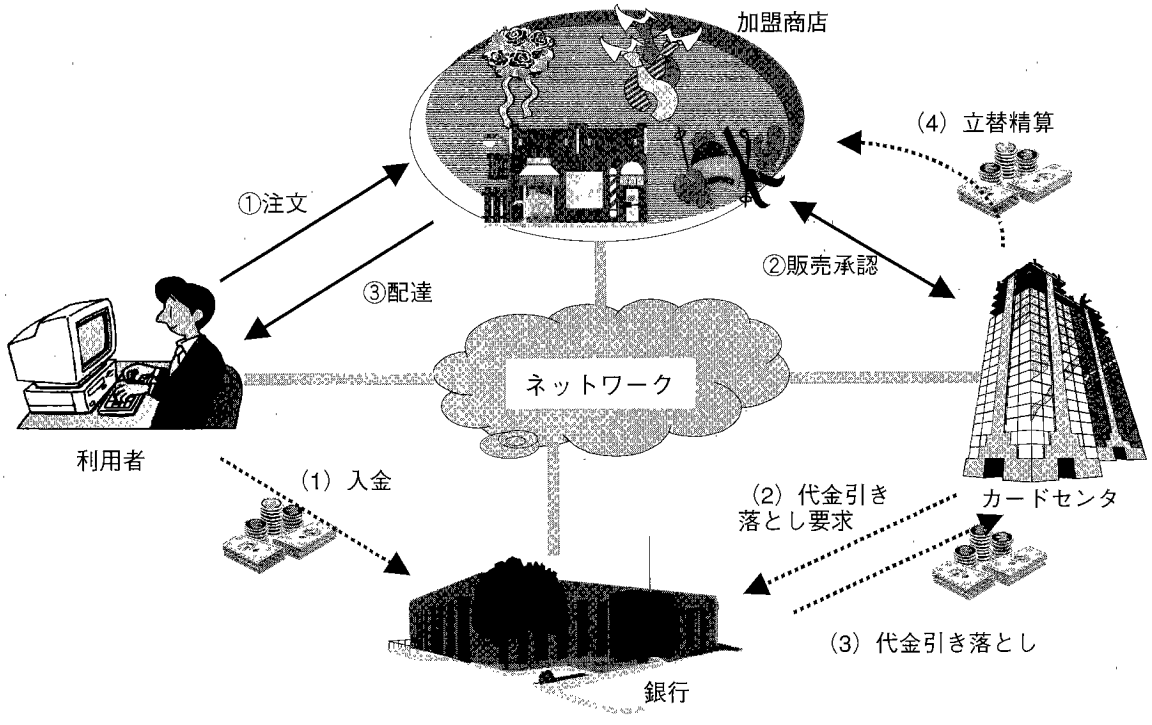

図-1 電子商取引の仕組み（クレジットカード利用の場合）

●電子商取引における認証の重要性

電子商取引では，インターネット上でのクレジットカードを用いたものが最も一般的である[2]．**図-1**で示すように，利用者は，①～③の手順により注文した品物を入手することができる．支払いについては，(1) ～ (4) の手順にて支払い精算がなされる．したがって，カードを用いたオンラインショッピングでは，ネットワークを介してこれらの商取引がなされるため，利用者と加盟店舗との間，加盟店舗とカードセンタの間，カードセンタと銀行の間において，通信相手の確認，すなわち認証を実施することが不可欠となる．

●強い認証方式と第三者のお墨付き

ネットワークにおける不正行為の多くは犯罪者による利用者への「なりすまし」によるものである．取引相手の認証を怠ると，別の相手にお金を支払ったり（仮想店舗のなりすましなど），カードを他人に悪用されたり（他人による利用者へのなりすまし）する可能性があることから，電子商取引を信頼したビジネス環境として構築するためには，強い認証方式，および信頼できる第三者のお墨付きが必要となる．すなわち，強い認証方式により，自分にしか作成できない情報を作り相手に送り，それを相手が確認することで，相手が自分を認証することができる．さらに，「本当に自分が作成したこと」を信頼できる第三者によって保証する（お墨付きをもらう）ことができれば，どのようなトラブルがあろうとも，その認証は正当なものとなり，裁判においても有効な資料とすることができる．これらはセキュリティ技術が重要なことを示している．

強い認証方式とは

BさんがAさんを認証することは，Aさんしか作成できない情報Iを作ること，Bさんがその情報IをAさんが作成したものと検証できること，の2つにより実現される．Aさんしか（情報Iを）作成できないということは，Aさんしか知らない「秘密情報」を持つことと同じである．逆に，Aさんが（情報Iを）作成したことを検証するためには，Aさん以外の人も知り得る情報により，検証されなければならない．本技術を実現するためには，通常，公開鍵暗号方式が用いられる．

公開鍵暗号方式[3]

公開鍵暗号方式は，自分で秘密にしておく鍵（秘密鍵）と公開してもよい鍵（公開鍵）という異なった2種類の鍵のペアにより構成される．その使い方としては，情報を秘匿するために，情報を相手Bの公開鍵で暗号化し，送信者Aが相手Bに送り，情報の受け手（相手B）はBの秘密鍵により転送情報を復号化し，情報を得る（**図-2**）．しかし，送信相手B以外の第三者は，秘密鍵がないため復号できず，情報を得ることができない．B（相手）がA（自分）を認証する場合は，逆に，情報をAの秘密鍵で復号（署名）し，それをBに送り，Bは転送情報を送信者Aの公開鍵を用いて暗号化（検証）する．この場合，秘密鍵のことを署名鍵ともいい，署名処理を実行できるものは，秘密鍵を保有している本人のみである（**図-3**）．公開鍵暗号方式は，情報を秘匿するよりも，強い認証を提供することに適している方式である．ここで，公開鍵は，公開されたディ

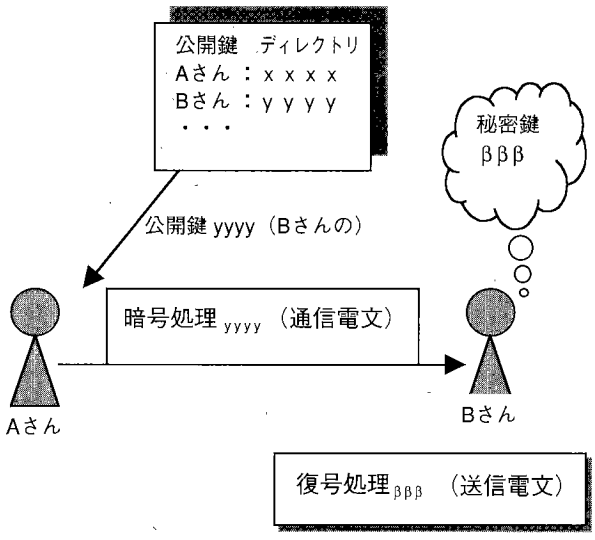

図-2　公開鍵暗号方式を用いた情報秘匿

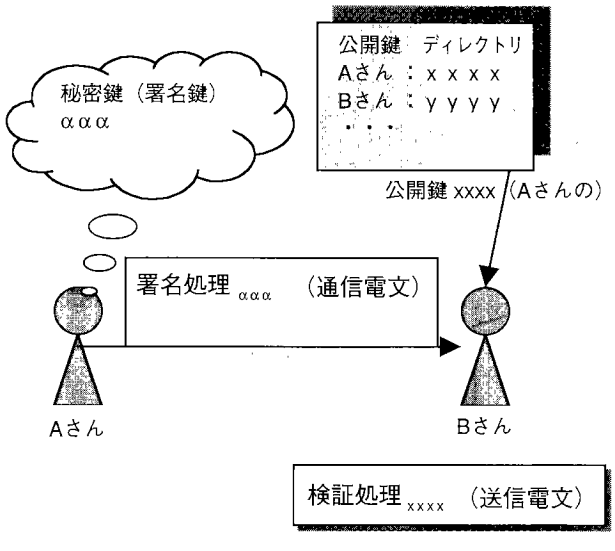

図-3　公開鍵暗号方式を用いた認証

レクトリに格納されることになるが，提供された公開鍵が本当に正しい本人のものなのかを保証する必要性がある．

公開鍵の第三者によるお墨付き：認証局

通信相手から直接手渡された公開鍵は本人のものと信用できなくもないが，オープンなネットワークを介して目に見えない相手から送られた公開鍵，公開ディレクトリに掲載されている公開鍵については，本人のものである保証はない．このために，公開鍵を信頼できる第三者によって保証してもらう(お墨付きをもらう)必要がある．そこで信頼できる第三者機関となる「認証局」が必要となる．認証局によって厳密に利用者の審査を行い，本人の公開鍵であることの証（公開鍵証明書と呼ぶ）を発行する．

●認証局（CA）の役割

認証局はCA（Certificate Authority）と呼ばれ，公開鍵の証となる「公開鍵証明書」を発行する信頼できる第三者機関である．**図-4**で示すように，利用者（Bさん）の公開鍵を保証するために，Bさんへ公開鍵証明書を発行する．Aさんは，認証局CAによって保証された公開鍵を持ったBさんは信用できるが，証明書のないCさんについてはビジネスパートナーとして信用できないことになる．また，認証局は発行した証明書が何らかの理由（たとえば，不正利用の発覚）で有効性がなくなり，証明書を失効しなくてはいけなくなったときに，証明書失効リスト（CRL: Certificate Revocation List）にその失効対象の証明書を追加し，適宜利用者に公開することも重要な仕事である．すなわち，認証局では，公開鍵証明書の発行管理，証明書失効リストの発行管理が主な役割となる．

公開鍵証明書の内容[4)]

公開鍵証明書に記載される内容は**図-5**で示すように，管理番号（バージョン番号，シリアル番号），署名方式，証明書発行者名，証明書の有効期間，公開鍵の所有者名，所有者の公開鍵情報，およびこれらの情報を認証局で署名した証明書の署名情報により構成される．これは公開鍵を印鑑とした場合，役場である第三者機関が印鑑証明を発行することと同じである．本証明書は，ITU-T勧告X.509（ディレクトリ：認証フレームワーク）により国際的に標準化されており，プロトコルを規定する抽象構文記法（ASN.1）により記述される．証明書を受け取った利用者は信頼する認証局の公開鍵によってこの証明書の正しさを確認する．一般的に，認証局の公開鍵は利用者が個別に保存している．

公開鍵証明書の正当性の確認方法

相手の公開鍵証明書の正当性を確認するためには，(1) 相手の公開鍵を発行した認証局の公開鍵を用いて公開鍵証明書の正当性を確認すること，(2) 発行された証明書が有効期間内にあること，(3) 証明書が証明書失効リストに載っていないこと，を調べて証明書の有効性・正当性を確認する．なお，相手の公開鍵証明書は，通信相手から直接送られてくる場合もあるが，認証局が提供する公開ディレクトリから入手することも可能である．しかしいかなる入手手段にしろ，上記3点の確認・検査をクリアできれば，相手の公開鍵は保証されていることに

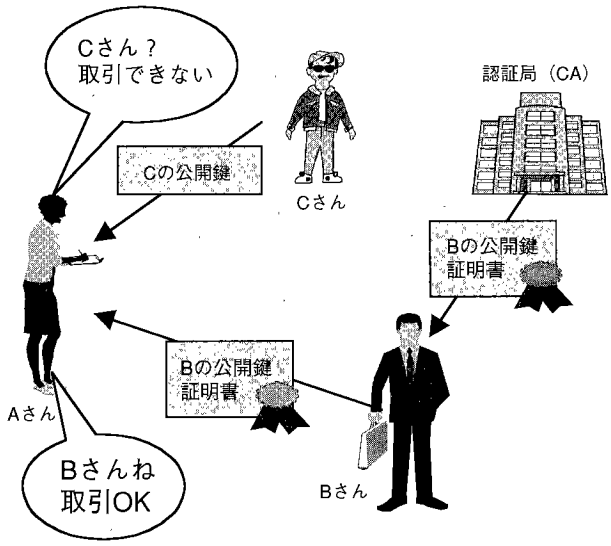

図-4　認証局の役割

管理番号（バージョン番号）
管理番号（シリアル番号）
署名方式
証明書発行者名
証明書の有効期間
公開鍵の所有者名
所有者の公開鍵情報
証明書の署名情報

図-5　公開鍵証明書に記載される内容

なる．

●認証局の構成イメージ

実際，認証局は，登録局，発行局，証明書・失効証明書ディレクトリの3要素により成り立っている．「登録局」は利用者からの申請処理の受け付け，利用者への証明書の発行を行い，「発行局」は実際の証明書の作成（公開鍵による計算処理），失効処理（署名を付与）を分担する．また，「証明書・失効証明書ディレクトリ」は有効証明書，失効証明書を格納するデータベースで，登録局からの有効証明書，失効証明書の登録や利用者からの失効リストの検索を受け付ける（**図-6**）．

●認証局を用いた認証サービスの現状

認証局は信頼できる第三者機関として，公的な機関（政府機関など）が運営する場合もあるが，信頼サービスを売りとした民間機関，民間企業が運営する場合もある．また，会社組織などの閉じたネットワークにおいては，人事部等の運営する社内組織が認証局の役割を担う場合が多い．

商用化が進む認証局

認証局は，すでに商用化されているものが多々あり，米国のベリサイン社を筆頭に，複数の会社によってその運用がなされている．日本においても，富士通，日立，NECを中心とする日本認証サービスが開始されており，また，セコム，帝国データ，野村證券において同様の認証サービスが商用化されている．さらに，ITS（高度道路交通システム）で構築中の高速道路の自動支払いシステム（ETC）においても，建設省の外郭団体（ORSE）による認証局の運用が決定されている．

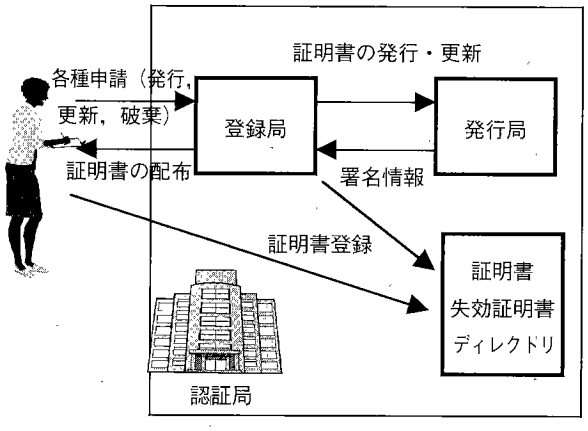

図-6　認証局の構成イメージ

企業内専用の認証局

セキュリティ問題はインターネットのようなオープンな通信環境ばかりではない．セキュリティ侵害の80%以上は組織内で起こっているとの報告もある．そこで最近では，組織内においても公開鍵証明書を使って，高信頼な認証を行う要求が増えてきた．企業内でセキュリティを確保するには外部の認証局を使うのでなく，組織内に信頼できる認証局を立てることが必要となる．

企業システムには組織内の社員や関連企業，企業の顧客などの情報といった「財産」が収められるという関係上，外部組織による認証局に任せることなく，自身のセキュリティ・ポリシー（安全基準方針）において認証サービスを管理，運用しようとすることは，信頼できる企業システム環境の構築に最もかなった考え方である．

●認証局の今後の課題

より使いやすい電子商取引の環境が整備されることにより，日本中の一億の人間が電子商取引の利用者になることも遠い将来ではない．発行される公開鍵証明書の数もそれに伴い膨大となり，運用管理上の問題が生じるのも時間の問題である．具体的な今後の課題としては，膨大な数の証明書の発行処理，登録処理を効率的に実行することが挙げられる．また，公開鍵証明書の失効リストについては，誰もが閲覧できる場所に一元管理する必要があるため，閲覧方法，グローバルな管理方法が課題である．さらに，現状では認証局への登録手順，失効処理依頼手順，公開鍵証明書の検索手順などが標準化（統一化）されていないため，自分の所属する認証局以外へのアクセスにおいて支障が出てくることも考慮し，認証局へのアクセス手順の標準化も重要な課題である．

これらの課題は，電子商取引のみならず，電子ショッピング，電子メールなどのさまざまなアプリケーションにおいて，解決すべき共通な課題と認識されており，認証局の技術検討は，安全性プロトコルなどの検討まで含めた広い意味での公開鍵をベースとした技術基盤（公開鍵暗号共通基盤PKI（Public Key Infrastructure）と呼ぶ）の検討の一部であると考えられている．以上の課題を解決し，認証局が広域的に普及し，いつでも，どこでも，だれとでも，高い信頼度に基づき，世界規模の電子商取引ができる時代が来ることを強く期待したい．

参考文献
1) http://www.ecom.or.jp
2) Secure Electronic Transaction (SET) Specification (1996).
3) 岡本, 山本: 現代暗号 シリーズ／情報科学の数学, 産業図書 (1997).
4) ITU-T Recommendation X.509 "Directory: Authentication Framework".

（平成12年2月2日受付）