調査研究論文

電子認証技術に関する動向調査

通信経済研究部研究官（技術開発研究担当）　丸山　誠二

［要約］

本年4月に施行された『電子署名及び認証業務に関する法律』により、電子署名が法的に効力を持つこととなり、電子商取引の急速な拡大が予測されている。

一方、郵政事業を取り巻く環境も急激に変化しており、更なるお客様ニーズに合ったサービスを提供するためには、電子商取引に対応したサービスの提供が必須となる。そこで、電子商取引を支える技術として有効な手段である電子認証について、その技術や電子認証を活用したサービス及びその業務内容などについて動向調査を実施した。

本稿では、インターネット上で安全な電子商取引を実現するための基盤技術の一つとして注目されている公開鍵基盤（PKI）について、使用される暗号技術と構成要素、その運営を担う認証局の運営方式などをまとめている。また、電子認証を専業とするホスティングサービスプロバイダや特定業界向け認証サービス、海外の郵便事業体における認証サービス等の概要を併せて紹介する。

1　はじめに

近年の著しいIT化の進展により、誰もが日常的にインターネット上で情報の発信や受信を行う時代へと変化してきた。特に企業においては、サービスの向上やコスト削減等を実現する手段として、B to BやB to Cの電子商取引を積極的に行っている。これら電子商取引を実現するためには、ネットワーク基盤が必要不可欠である他に、インターネット上にある情報を送り手と受け手以外の第三者から守る暗号化技術が必要となり、更に、通信相手を認証する機能が重要視され、これを実現するためには電子署名等による認証技術が有効と考えられている。

本年4月に施行された『電子署名及び認証業務に関する法律』は、電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進を図ることを目的としており、電子署名が法的な効力を持つことによって、電子商取引が拡大していくことが予測されている。

一方、郵政事業を取り巻く環境も急激に変化しており、更なるお客様ニーズに合ったサービスを提供するためには、電子商取引に対応したサービスの提供が必須となる。そこで、電子商取引を支える電子認証にかかる先端技術や、電子認証を活用したサービス及びその業務内容などについて動向調査を行った。

2　電子認証と公開鍵基盤（PKI）

2. 1　電子認証

電子認証とは、「本人の同一性確認」を電子的に行うことである。「本人の同一性確認」とは、ある者が真に当該本人であるということを確認することである。このため、本人しか知り得ない情報、或いは本人しか持ち得ない物品等により本人を確認することとなる。

⑴　電子認証における認証方式

電子的に行われる認証方式の代表的なものとして、次の3種類を挙げることができる。

①　カード等の所有物による認証方式

ICカードその他を所有していることにより、本人の同一性確認を行う方法。ただし、カードの所有に依存するため、盗難の際に問題となる。そのため、通常は、カードの所有のみで認証を行うことは避け、暗証番号の入力などを併用する。

②　パスワード等の記憶による認証方式

パスワード、暗証番号、その他のユーザしか知り得ない情報により、本人の同一性確認を行う方法。

③　生体特性等による認証方式

本人の生体特性等により、本人の同一性確認を行う方法。認証方式として、次の2つに大別される。

・身体の特徴（指紋、虹彩、声紋、…）
・行動の特徴（筆跡、タイピングの特徴、…）

⑵　電子認証により実現できること

①　機密情報へのアクセス権の管理

電子的な機密情報或いは私的な情報へのアクセス権の管理が可能となる。いわゆるログインと呼ばれる概念や、電子文書へのパスワード付与等により広く使われている。

②　手続きや作業等の責任の明確化

電子認証により特定の作業を行った際の責任を明確にすることが可能となる。従来の押印やサイン等により責任を明確化していたことに代わる可能性を有している。

2. 2　公開鍵基盤（PKI；Public Key Infrastructure）

公開鍵基盤は、インターネット上で安全な電子商取引を実現するためのインフラとして注目されており、公開鍵暗号方式という暗号技術を使用して電子認証を実現する手段の一つである。

⑴　PKIで使用される暗号方式

暗号化とは、ある情報を、解読方法を知らない者には意味を成さない状態にすることである。通常は、送信者から受信者へ通信を行っても、常に覗き見（盗聴）されるリスクが存在するが、暗号化することでリスクを極小にしつつ通信を行うことができる。このとき、オリジナルの情報を平文（ひらぶん）、暗号化された情報を暗号文と呼ぶ。そして、暗号文を再び意味を成す状態、すなわち平文に戻すことを復号といい、暗号化や復号の方法を正確に定めるものを鍵と呼んでいる。

一般に暗号方式は、鍵の種類により2つに大別される。

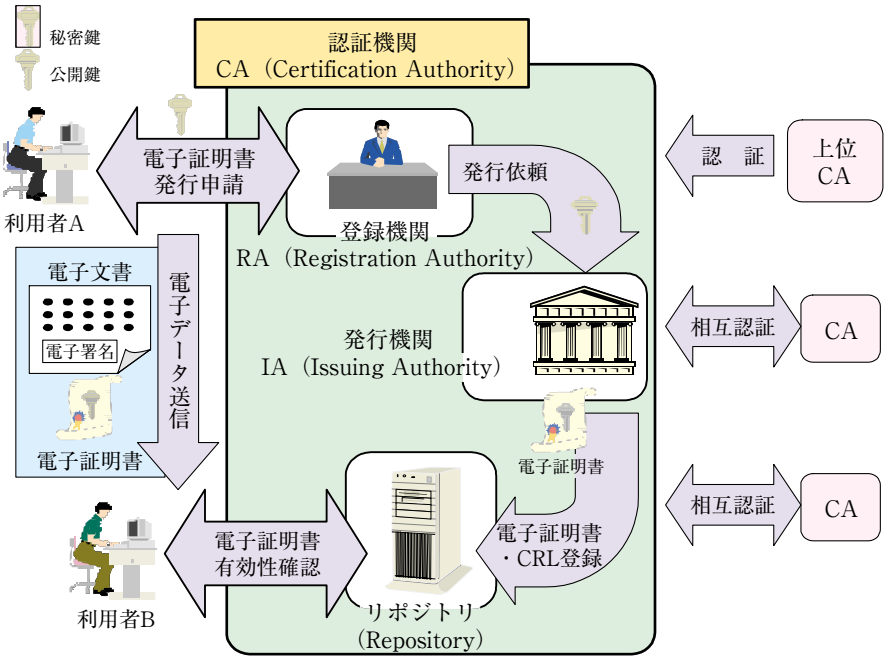
①　共通鍵暗号方式

秘密鍵暗号、或いは対称鍵暗号と呼ばれており、この方式で使われる鍵のことを共通鍵という。共通鍵暗号は、暗号化と復号に同一の鍵を利用する方法である。

【利点】
・公開鍵暗号に比べて処理が早い。

【欠点】
・ネットワークを利用した鍵の送付に安全性が確保できない。

図表１　PKI利用の大まかな流れ



・通信相手毎に複数の鍵を管理する必要がある。

代表的な共通鍵暗号方式としては、DES（Data Encryption Standard）があり、米国政府標準暗号として長年利用されていたが、コンピュータ性能の向上や暗号解読技術の進歩により暗号としての強度が不安視されてきた。そこで1997年に公募が行われ、2000年10月に次世代の米国政府標準暗号AES（Advanced Encryption Standard）としてRijindaelが選ばれ、パブリックコメント期間を経て正式発表となる予定である。

②　公開鍵暗号方式

公開鍵暗号は、非対称鍵暗号とも呼ばれ、異なった鍵のペアを使って暗号化と復号を行う。一方の鍵から他方の鍵を導き出すことは数学的に非常に困難であることが証明されており、これによって実現できる方式である。この２つの鍵のうち、公開する一方の鍵を公開鍵と呼び、秘密にするもう一方の鍵を秘密鍵、或いは私有鍵と呼ぶ。この公開鍵と秘密鍵のどちらを使っても暗号化は可能であるが、復号の際にはペアとなっている他方の鍵を使う必要がある。

【利点】

・ネットワークを利用した鍵の送付に安全性が確保できる。

・一つの秘密鍵を管理するだけで良い。

【欠点】

・共通鍵暗号に比べて処理速度が遅い。

代表的な公開鍵暗号方式には、RSA（Rivest, Shamir, Adleman）、離散対数暗号、楕円曲線暗号などがある。

秘密鍵の格納として、次の方法が挙げられる。

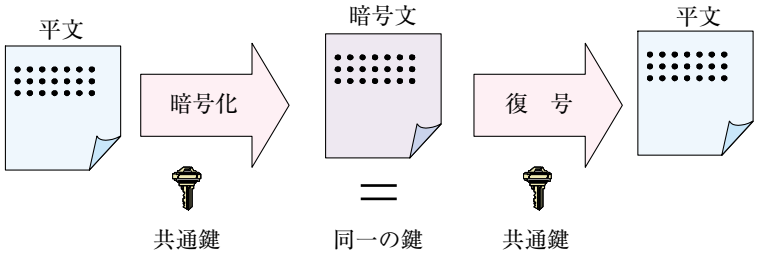
・ハードディスク内：可搬性に乏しくコピーや覗き見される危険性が高い。

・フロッピーディスク内：可搬性はあるが、コピーや覗き見される危険性がある。

・ICカード内：可搬性があり、コピーや覗き見される危険性はない。

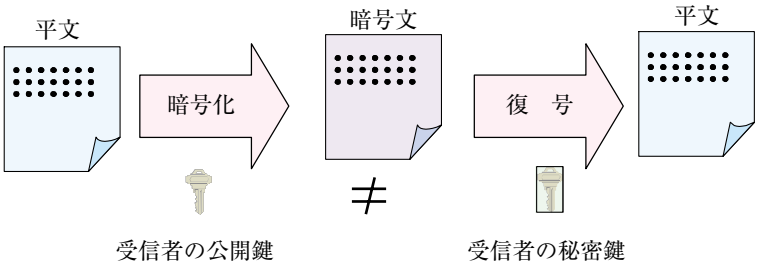
なお、日本国内の次世代暗号方式は、平成15年度の電子政府実現に向け、利用可能な暗号技術のリスト作成を目的に、情報処理振興事業協

図表 2　共通鍵暗号方式での暗号化と複合



（暗号化と復号の鍵が共通）

図表 3　公開鍵暗号方式での暗号化と複合



（暗号化と復号の鍵が異なる）

会（IPA）が、公募によって暗号方式の募集を行い、安全性等の詳細な評価を経て、パブリックコメントを求める状況にある。

⑵　PKIが提供するもの

①　認証（Authentication）

遠隔地の利用者が自分だと主張することを第三者機関である認証局が他の利用者に対して保証すること。

②　完全性（Integrity）

データが改ざんされていないことを保証すること。従来の技術であれば、誰かが意図して行う改ざんに対しては無力であったが、PKIの仕組みであれば、意図して行われた改ざんを検出することが可能となる。

③　秘匿性（Confidentiality）

データのプライバシーを保証すること。意図した特定（或いは意図した複数の）相手にのみ内容を読むことを認め、それ以外の相手に対しては、データが読めない状態にできる。

④　否認防止（non-repudiation）

否認とは、ある人が自分で行った行為を認めないことを指し、例えば、注文しておきながら注文の行為を否定することである。電子署名を施した文書では、利用者の秘密鍵が漏洩していない限り、その電子署名を作成したのは当該利用者であることを証明することが可能となり、否認行為を防ぐことができる。

⑶　PKIの構成要素

①　認証局（CA; Certificate Authority）

公開鍵暗号を利用するユーザが多数いる場合、個々のユーザと各々の公開鍵を結びつける仕組みが必要となる。この仕組みを担う機関として、「ユーザから信頼される第三者機関」（TTP; Trusted Third Party）が必要となり、この第三者機関を、認証機関、もしくは認証局と呼んでいる。

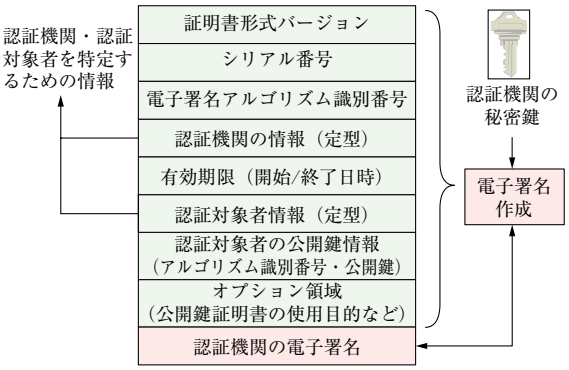
②　電子証明書

認証局によって作成される公開鍵の有効性を保

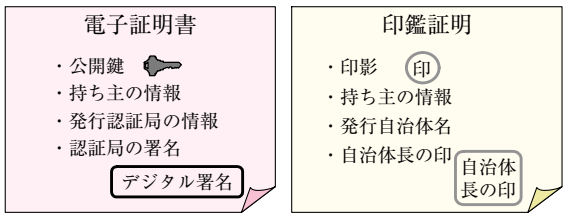
証するデジタル化された証明書である。その内容は、認証対象者の名義と公開鍵情報を含んだデータ構造となっており、これに認証局が電子署名を施すことで鍵ペアと本人との結合を認証する。

図表4にITU（国際電気通信連合電気通信標準化部門）が定めた電子証明書の標準仕様を示す。

図表4　電子証明書の標準仕様（X. 509 ver 3 形式）



図表5　電子証明書と印鑑証明書の比較



また、電子証明書と印鑑証明書の内容比較を図表5に示す。

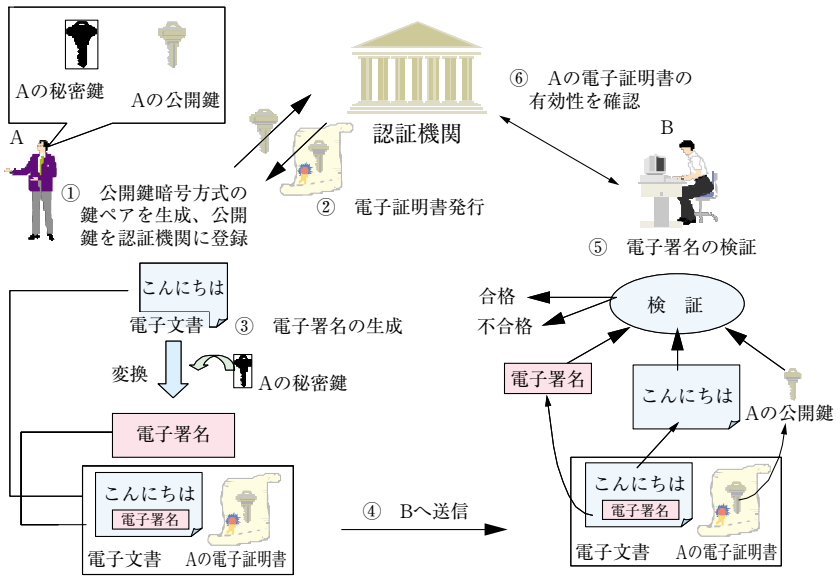
③　電子署名

様々な暗号方式に基づき電子的に作成された固有の識別子（署名）の総称を電子署名と呼び、中でも公開鍵暗号方式に基づく電子的署名をデジタル署名と定義することが一般的となっている。これにより、データ送信者を認証し、データの完全性を保証することができる。なお、電子署名に法的効力を認めるかどうか、どの方式を電子署名と認めるかといった事項は、国によって異なる。米国などは州によっても異なっている。

④　タイムスタンプ

電子商取引などで扱う電子データには、作成日時や有効期限について第三者機関が保証する時刻を利用する必要がある。これは、デジタルタイムスタンプ、或いはタイムスタンプと呼ばれ、特定の日時には既に文書が存在していたことを証明する。正確な時間管理機器を備えた信頼できる第三者機関が電子データに時刻を添付し、その結果に電子署名を付与することで実現できる。

図表6　電子署名利用の流れ



⑤　CP（Certificate Policy）

認証局が証明書を発行するときのポリシー。証明書を特定のコミュニティやアプリケーションに共通のセキュリティ要件に沿って提供するための規則である。

⑥　CPS（Certification Practice Statement）

信頼される第三者機関が、認証を利用するものに対して、信頼性、安全性、経済性などを評価できるように認証機関のセキュリティポリシー、約款及び外部との信頼関係などに関する詳細を規定した文書である。

⑦　リポジトリ

ディレクトリ構造の証明書や失効情報を格納するデータベースである。

2. 3　認証局のセキュリティ

認証局は、PKIの安全性を支える重要な役割を果たしており、認証局そのもののセキュリティレベルが、その認証局によって支えられているPKIのセキュリティレベルに非常に大きな影響力を持つことになる。従って、以下に挙げる事項に留意し、セキュリティレベルを維持することが重要である。

⑴　セキュリティポリシー

セキュリティ保護のための運用面での指針となり判断基準となるものである。従って、認証局に求められるセキュリティレベルに応じたセキュリティポリシーを策定することが重要となる。加えて、認証局のセキュリティレベルを維持するためには、セキュリティポリシーを策定した後も、導入、運用、評価・見直しというサイクルを継続的に続けていく必要がある。更に、情報技術の進歩の早さや、ハッカー等の技術の巧妙化に伴い、この見直しのサイクルは短期間であることが望まれる。

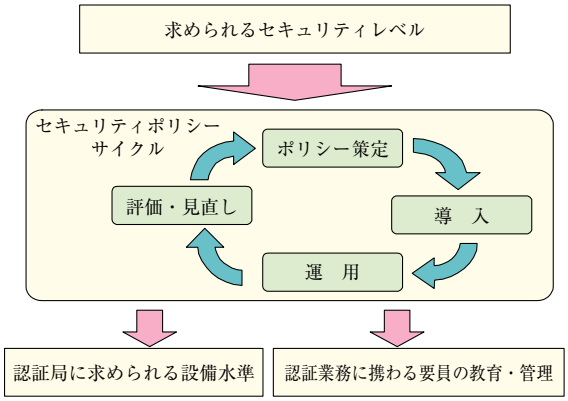
⑵　建物等に求められる物理的なセキュリティ

サーバ等に物理的危害を与えられることの無いように入退室管理について考慮する必要がある。また、天災等の不測事態や停電等が発生した場合、サービス提供をどのようにするか等の検討を加えておく必要もある。

⑶　認証業務に携わる要員の教育・管理等の人的セキュリティ

セキュリティポリシーをどれだけ厳格に定めたとしても、実際に情報を扱いセキュリティ保護を行うのは人である。そのため、認証業務に携わる要員の責任や役割、教育・管理等の人的セキュリティについての規定を定めなければならない。

図表７　セキュリティポリシーのサイクル



2. 4　認証局の運営方式

認証局（CA）の機能は、登録と発行の２つの機能に大別され、この機能をどのように運営するかによって認証局の運営方式が異なってくる。それぞれの機能に対応した機関を登録機関（RA; Registration Authority）と発行機関（IA; Issuing Authority）と呼び、通常、次の３つの形態が考えられる。

⑴　プライベート認証局[1)]方式

認証局の機能を全てインソースで行う方式であ

る。すなわち、電子証明書の発行申請受付や、発行処理等をすべて自前で行う方式である。

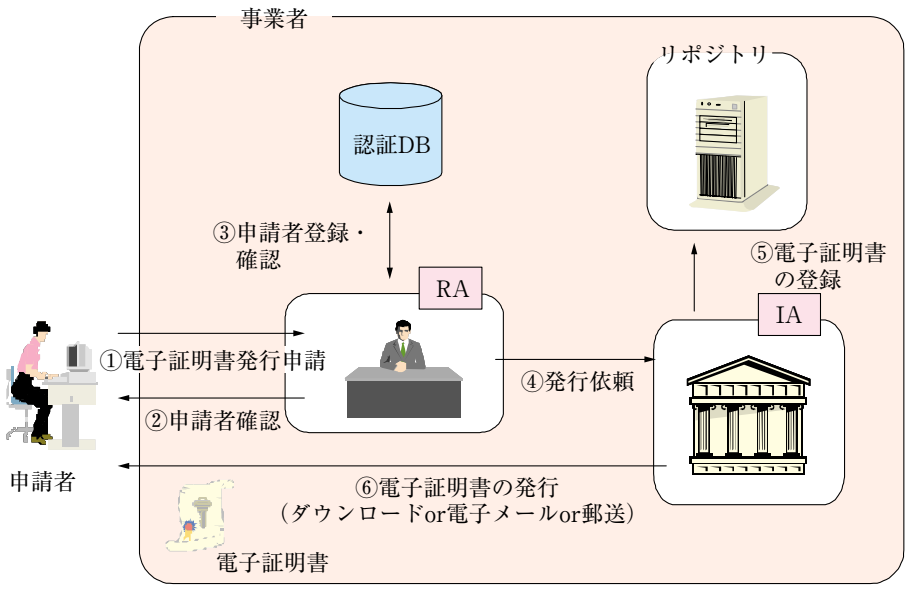
【利点】

・電子証明書発行業務の管理を自前で行うことが出来る。
・登録時の検査を自前で行うことが出来る。
・電子証明書発行に伴うコストを抑えられる。

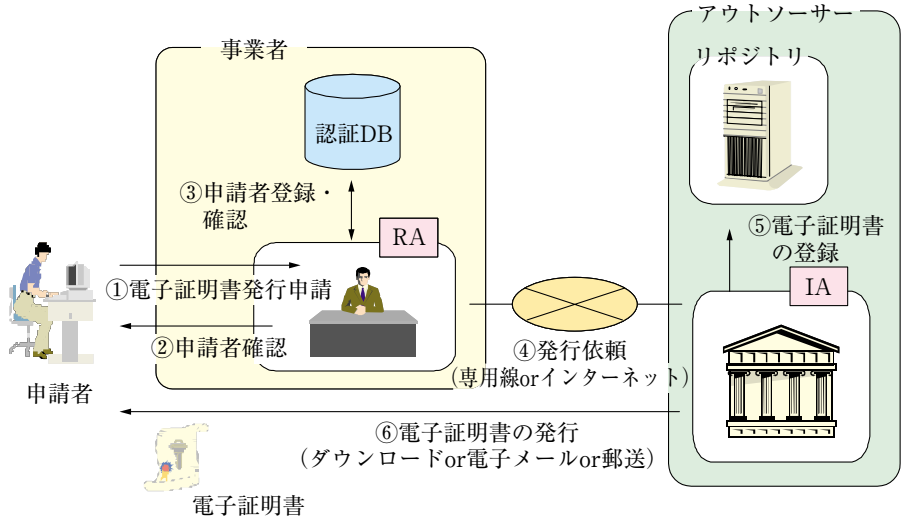
【欠点】

・全て自前で用意するために、初期コストが高くなる。
・運営に携わる要員を自前で用意する必要がある。
・運営に携わる要員の教育が必要である。

図表 8　プライベード認証局運営方式



図表 9　IAの外部委託運営方式



1）企業内もしくは関連グループ内に限定して行われるケースがプライベートなCAと指されることが多いが、本稿では、一般の利用者を対象に電子認証を事業として行うために自前でRA・IAを持つ運営を指す。

⑵ 発行機関（IA）の外部委託運営方式

認証局の機能のうちRAを事業者の内部に置き、IAをアウトソースして運営する方式である。

【利点】

・登録時の検査を自前で行うことが出来る。
・発行機関の構築という初期投資を抑えることが可能となる。
・電子証明書の発行業務という定型的な作業をアウトソースすることでコストを抑えることが出来る。

【欠点】

・発行機関をアウトソースするため、運用費用が相対的に高くなる。
・登録業務に携わる要員を自前で用意する必要がある。
・電子証明書の発行には、発行枚数に比例したコストが通常発生する。

⑶ 完全な外部委託運営方式

認証局の機能であるRA・IAを事業者の内部には置かず、全てアウトソースして運営する方式である。図表８の「事業者」部分が「アウトソーサー」に置き換えられて運営されることになる。

【利点】

・認証局業務全般をアウトソースすることで初期投資を抑えることが出来る。

【欠点】

・全てをアウトソースするため、運用費用が相対的に高くなる。
・電子証明書の発行には、発行枚数に比例したコストが通常発生する。

2. 5　認証局運営上の課題

認証局を構築・運営する上で、現時点では、いくつかの課題や問題点がある。

⑴ PKI全般に関する課題

① 公開鍵・秘密鍵・証明書に関するオペレーションが多様・複雑

PKIに関連するアプリケーションの操作方法や電子証明書の取得方法が標準化されていない。このため、ある程度の技術を持ったユーザでなければ、操作が煩雑であったり利用が難しいという問題が存在している。

⑵ 認証局に関する課題

① 認証局の秘密鍵の安全確保

認証局の秘密鍵が漏洩した場合、その認証局が発行している電子証明書全てが信頼性を失ってしまう。認証局は、秘密鍵を厳重に管理する必要がある。

② 障害・災害時における秘密鍵やリポジトリのバックアップなど

認証局において障害が発生した場合、秘密鍵の情報やリポジトリのバックアップが失われる可能性がある。そして、秘密鍵の情報が失われた場合には、その認証局が発行している電子証明書を新たな秘密鍵を使って再発行しなければならない。また、リポジトリのデータが失われた場合には、電子証明書の有効性確認が行えなくなり運用に支障をきたす。これらの対応策（システムの二重化等のバックアップ体制、セキュリティ体制）の検討が必要である。

⑶ 電子証明書に関する課題

① 証明書有効期間の制約

暗号には技術的な寿命があるため、公開鍵暗号方式の鍵にもライフサイクルが存在し時間と共に陳腐化する。このライフサイクルが証明書の有効期間に対する制約条件となる。

② 電子証明書の拡張領域利用による互換性

電子証明書の拡張領域を利用する場合、アプリ

ケーション側でその利用を判別しなければならないが、アプリケーションに正しい取扱が実装されていなければ、その互換性に問題が発生することがある。

③　電子証明書に記載される情報内容

電子証明書に記載される個人情報の種類や記入領域、言語等が統一化されていないため、複数の認証局間で個人を認証する際に問題が生じる可能性がある。

⑷　電子署名に関する課題

①　XMLの標準化

インターネット上でやり取りする文書の構造を記述する言語XML（Extensible Markup Language）は、電子商取引の注文書や送り状のような電子版の標準ドキュメント作成の主流となりつつある。現在、電子署名付きのXMLが標準化の過程にある。

⑸　暗号に関する課題

①　暗号の技術的な寿命

コンピュータの性能向上や暗号解読技術の進歩により暗号の強度が弱くなる。また、理論上は万全の暗号技術であっても、その実装や鍵の管理に問題があればセキュリティ面からも強度が弱くなる。そのため、暗号には解読されるリスクが存在していることを認識しておく必要がある。

⑹　要員管理に関する問題

①　運用スキルとオペレーション権限の分散

認証局、特に発行機関内での運用スキルを多くの人が知ることは、セキュリティ上問題である。また、オペレーション権限は一人に集中せず、複数の人に分散させることが重要である。そのため、オペレーション権限を分散させつつ、少ない補充要員で業務をカバーすることが必要である。

②　要員のセキュリティ意識

認証局の運用に従事する要員のセキュリティ意識が重要である。技術的に高いセキュリティを確保しても、要員のセキュリティ意識が低ければ、全体のセキュリティレベルが低下してしまう。

⑺　オペレーションに関する問題

①　ログの管理手法

電子証明書を多数発行し、多くの有効性確認を受ける認証局では、有効性確認の件数やそれら記録を残すことを想定し、不測の事態があった際にログを検証することを含めて、ログ管理手法等に検討が必要である。

②　電子証明書の廃棄

電子証明書の有効期限内でありながら盗難・漏洩等があった場合、不正利用を防ぐため、その電子証明書の廃棄が必要となる。これは、認証局が電子証明書の失効情報を利用者に対して提供することで不正利用を防止できるが、現状では、失効情報の提供手段が標準化されていない。加えて、失効情報そのものが、プライバシーに密接に結びついているため、慎重に取り扱う必要もある。

失効情報の提供手段としては、大きく分けて2つある。

・CRL（Certificate Revocation List）

電子証明書の失効リストがリポジトリ等を介して提供され、ユーザが有効性を確認する方式であり、多く使われている。問題点として、一定の間隔をおいて失効リストを更新するため、失効手続きから失効情報が公開されるまでにタイムラグが発生し、この間に不正利用される可能性がある。また、運用規模に比例してCRLが大きくなる傾向にあり、ユーザがCRLを取得するには大きなファイルをダウンロードしなければならない。

・OCSP（Online Certificate Status Protocol）

オンラインでリアルタイムに電子証明書の失効

状態を確認する方式で、OCSPレスポンダ・サーバに対し、利用者が電子証明書の有効性確認を行う仕組みである。技術的にはCRLより優れているが、アプリケーション対応が進んでいないこと、OCSPレスポンダのスケーラビリティ確保など技術的な課題も残っている。

3　電子認証事業関連の動向

3. 1　認証局ホスティングサービスプロバイダ

日本国内における主な認証局ホスティングサービス（証明書の発行業務請負）プロバイダが提供する運営方式やPKI製品の特徴等は以下の通りである。

⑴　A社

①　提供可能な運営方式

IAの外部委託方式を提供している。RAは認証事業者である顧客サイドに置き、IAをA社のセンター内で運用してホスティングサービスを行う。顧客である認証事業者とA社との間はインターネットで通信する。

なお、A社が提供するCPSに基づいた運用とすることで、迅速に認証業務が開始できる。

②　特徴等

・顧客である認証事業者は、認証局システム全体の構築、運用（セキュリティ管理、バックアップ、障害復旧など）を気にすることなく、簡単にブラウザ操作で証明書申請の審査、承認、却下、保留の判断と指示をすることで認証局の運用が可能となる。A社は、セキュリティ施設やCPSによって鍵を管理し、証明書を発行するなど認証局のバックエンドを運用する。
・個々の申請者（エンドユーザ）は、簡単なブラウザ操作によって証明書を申請し、使用することができる。

⑵　B社

①　提供可能な運営方式

プライベート認証局方式、IAの外部委託方式、完全な外部委託方式の各方式を提供することが可能である。認証事業者のニーズに合わせたコンサルティングを行い、最も適当な方式が選択できるよう柔軟な対応が得られるが、立ち上げに時間がかかる。

②　特徴等

・認証事業者のニーズに合わせた対応を行うため、フレキシビリティ、管理のしやすさを実現するPKIシステムのコンポーネントが用意されている。
・認証局の運営をアウトソースする場合には、専用パッケージを用意し、認証事業者である顧客企業のブランドを前面に押し出すことが可能である。
・運用を開始後でも、鍵の移行を行うことで、運営形態を変更すること（アウトソースからインソースへ。またはその逆）が可能である。

⑶　C社

①　提供可能な運営方式

プライベート認証局方式、IAの外部委託方式、完全な外部委託方式の各方式を提供することが可能である。認証事業者のニーズに合わせたコンサルティングを行い、最も適当な方式が選択できるよう柔軟な対応が得られるが、立ち上げに時間がかかる。

なお、アウトソースには、顧客のシステムを資産として預かる場所を提供する方式と、システムをリース提供する方式の2種類がある。

②　特徴等

・ユーザ数の増加や時間帯に依存することなく、ユーザ登録・認証処理の自動化やパスワード紛失時の復旧処理を自動的に処理することが可能

である。

・所持していた鍵の紛失やパスワード忘れに対処するため、鍵のリカバーと否認防止の両方を実現する2つの鍵ペアを使用している。
・すべてのアプリケーション（電子メール、Web、デスクトップ）に対し、1回のログインで環境が提供されるユーザ・インターフェースを採用している。
・別々に立ち上げた認証局の統合化や、サービス・グレード毎の個別認証システムを上位層で接続するなど、環境要件の変化に過去のシステムを活かしながら対応することが可能である。

3. 2　認証局サプライヤ

主な認証局サプライヤが提供する技術やソリューションの特徴等を次に挙げる。なお、国内ベンダーには、認証局ホスティングサービスプロバイダ等から技術を導入するなどの関係も多い。

⑴　D社

B社からRA運用機能を導入し、E社からシングル・サインオン技術を導入することによって、PKI製品群を揃えている。

⑵　E社

PKI環境を構築するため、証明書の発行・管理、アクセス・コントロールの集中管理、ファイル暗号化やシングル・サインオンなどのセキュリティ、アプリケーション・サーバとユーザ間の認証などのコンポーネント製品を揃えている。

⑶　F社

企業内において公開鍵を利用する認証システムを実現するPKIのサービスを提供しており、ICカードによる証明書・秘密鍵の格納や、鍵の一括生成、ディレクトリサーバ利用による社内管理情報の共有化などを可能としている。

⑷　G社

ユーザニーズに応じた認証局形態を提供するため、情報管理、アプリケーション、ネットワーク、ウィルス対策、セキュリティ運用、基盤の6つに分類された製品が揃えられている。

⑸　H社

特定顧客を対象としたインターネット電子商取引やイントラネットでの利用を目的とした1万を越える大規模ユーザにも対応できる電子認証局システムを提供している。

⑹　I社

独自技術によりPKIシステムを開発しており、認証サーバによる鍵リカバリーや独自の暗号アルゴリズムなどによって、ネットワーク上での個人認証システムやデータ通信システムを提供している。

⑺　J社（米国）

J社の製品は、Sun　SolarisとWindows　NTプラットフォームの上で稼動するものであり、USPSで導入されている。

日本では、企業がイントラネット／エクストラネット用として利用できる製品を提供しており、リモートアクセスクライアントとアクセス先サイトの双方向認証及びデータ暗号化をサポートしている。

3. 3　企業・特定業界向け認証サービスプロバイダ

特徴のある認証サービスが行われている業種での概要は以下の通りである。

⑴　企業審査用認証サービス／K社

K社は、企業信用調査を実施している企業であり、全国の企業情報をデータベースに、B to B電子商取引において、電子認証や取引相手の与信情報を提供する第三者機関としてサービスを展開している。

K社は、A社、B社から技術協力を得て、サーバ証明書の発行サービスを行っており、電子証明書の発行及びライフサイクル管理等のバックエンド・サービスを、A社にアウトソースしている。また、ルートCA[2)]として各企業にCAの提供サービスを行っている。

⑵　金融業界向け認証サービス／アイデントラス

世界中の金融機関を通じたインフラの提供を目的とし、1999年３月に欧米の有力金融機関８行によりアイデントラスが設立された。

基本的な認証サービスの流れは、「４コーナーモデル」と呼ばれるビジネスモデルで行われ、すべてのトランザクションはインターネット経由でリアルタイムに行われる。

3. 4　海外郵便事業体の認証サービス

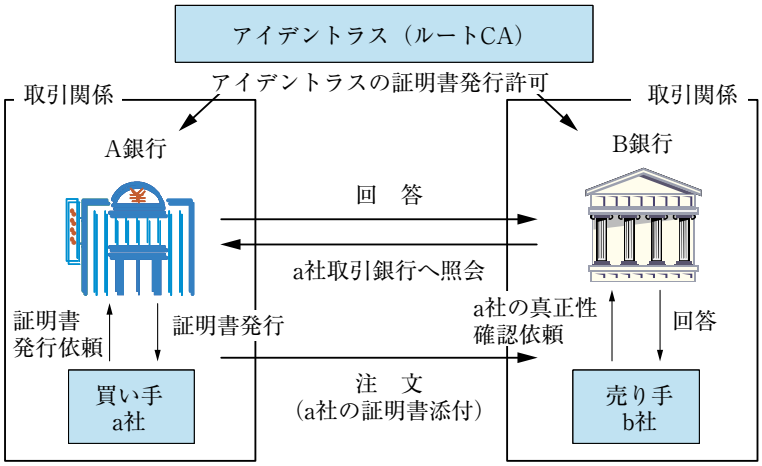
海外の郵便事業体における電子認証等に関するサービスは以下の通りである。

⑴　米国／USPS

米国では、2000年６月に電子署名法案が可決され、FPKI（Federal Public Key Infrastructure）の構築が進められている。この法案では、コンピュータやインターネットに関する知識の乏しい消費者への配慮から、消費者に対し電子署名を使うか、書類上の署名を選ぶかの選択肢が与えられており、更に法的に重要度の高い取引（保険の解約、商品のリコール、抵当流れ処分、遺言など）では、電子署名ではなく書面上の署名が義務付けられている。

米国郵便事業体のUSPSでも、従来の郵便サービスに加え、安全にインターネット上で利用できるポスタルサービスに乗り出している。その中で、現在PKIによる認証が行われているのは電子切手だけであるが、今後、電子データ配送サービスにPKIを利用する可能性もある。主なインターネットサービスは次の通りである。

図表10　アイデントラスの「４コーナーモデル」



2）階層構造型の認証構造において、上位に位置する認証局を指す。下位認証局の公開鍵の発行、執行を管理する。

① 電子切手（PC Postage）

自分のPCとプリンタを郵便料金計器として使用し、郵便料金をオンラインで支払うことを可能にするサービス。USPSと提携している会社のWebサイトからユーザは電子切手を購入し、自分のプリンタで二次元バーコードの電子切手を印刷する。24時間365日電子切手購入が可能なこと、通常の郵便切手料金よりも安いことなどから、業務効率の向上やコストの削減を狙う中小企業を中心に利用されている。

・電子認証の方法

USPSはルートCAとして機能しており、提携各社の認証局では、ユーザが使用するPCに接続する専用機器（PSD; Postal Security Device）に対して鍵ペアを発行する。電子切手には、PSDの秘密鍵を使って電子署名が施され、PSDの公開鍵を使って検証する。公開鍵は、USPSもしくは提携会社のリポジトリから得られる。

② 電子データ配送サービス（PosteCS™）

インターネットを利用した電子データの配送を行うサービス。機密性の高いデータ交換をインターネット上で行うことができる。USPS, Canada Post及びLa Posteが共同で開発したサービス。

・電子認証の方法

認証は、SSL（Secure Sockets Layer）を用いた暗号化、サーバ認証、パスワードによって行われる。文書の有効期限設定が可能であり、Electronic Postmark™と組み合わせれば、データの正確性、信頼性の証明、配送時間の確認が可能となる。

PKIを利用したend-to-endの暗号化、デジタル署名、ユーザの電子認証を行う計画が進められている。

③ Electronic Postmark™

電子消印サービス。ユーザが証明したい文書の存在時刻証明や、文書が改ざん・盗聴されていないことの安全性を保証する。また、誰がいつ文書を見たかを証明する。

⑵ オーストラリア／Australia POST

オーストラリアでは、1998年から電子認証のフレームワークを開発する国家プロジェクトGatekeeperを開始し、PKAF（Public Key Authentication Framework）を策定した。

Australia POSTは、インターネット上でも信頼できる商取引空間を提供するため、Key POST部門を立ち上げた。現在、全国約800の郵便局において、対面による本人確認を行うRAの役割を担っており、証明書の発行をGatekeeperの要件を満たす外部企業に完全委託して行っている。

Australia POSTが提供しているインターネットサービスは、次の通りである。この中で、PKIによる認証を行っているのは、POST eDeliver™である。

① POST eDeliver™

オンラインビジネスを行う企業に商品の保管設備及び配送を提供するサービス。郵便局の最寄り倉庫から顧客へ商品発送を行う。また、インターネット上で、小包の配送依頼、及び依頼した小包の配送状況の確認ができる。

② Pay it @ POST™

オンライン取引の請求書をプリントアウトし、郵便局へ持参して支払いが行えるサービス。

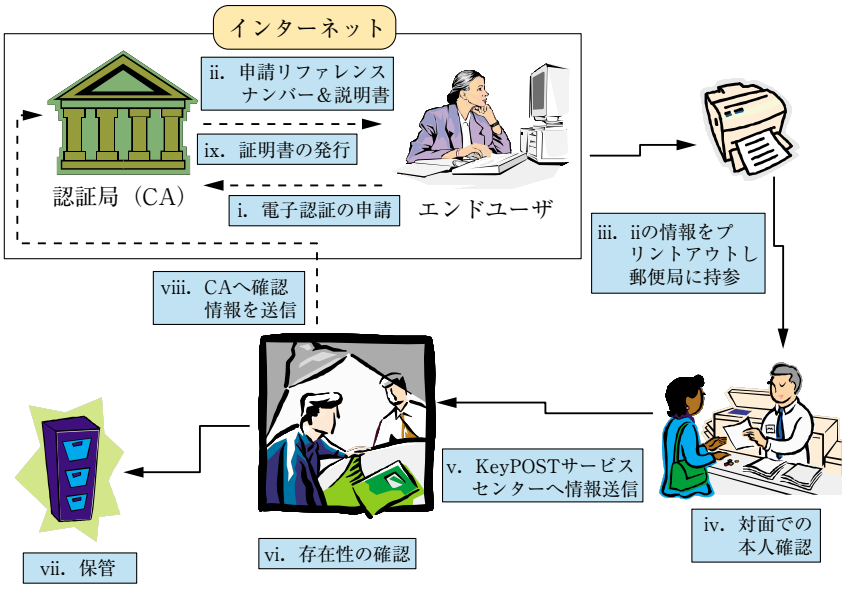
③ POSTbillpay

オンライン上での公共料金などの代金支払や明細票の照会を可能にするサービス。

⑶ ドイツ／Deutsche Post

1995年の株式会社移行後、e-ビジネス部門のDeutsche Post AGが、法人、個人の顧客に対して、インターネットをベースとした新しいサービスを開発しており、社内の主要な4部門（郵便、

図表11　Key POSTによる電子証明書の発行手順



速達便、物流、金融）において、多くのデジタルサービスを展開している。主なサービスは次の通りである。この中でPKIを利用するサービスは、SigntrustとVirtual eTrustである。

①　Signtrust

電子商取引を安全に行うためのデジタル署名と暗号化を提供するサービス。全てのインターネットユーザは、ドイツの電子署名法の基準を満たしているDeutsche Post AGのトラストセンターを通じてデジタル署名を申し込むことができる。これにより、ICカードと暗証番号、カードリーダがあれば、誰でもデジタル署名を保持することが可能になる。

・ICカードの利用

1997年に制定された電子署名法では、ICカードに秘密鍵を格納することが定められている。鍵ペアはDeutsche Postのトラストセンター内で生成され、ディレクトリサービスから公開鍵が検索でき、ICカードに格納された秘密鍵とともに利用することで実現されている。

・アプリケーション

基本的なアプリケーションにeTRUST Mailがある。これはOutlookやLotus Notesと連動し、暗号メールや署名付きメールを送信、受信メールの署名を検証することが可能となる。

②　Virtual eTrust

企業、銀行や公的機関に対して、従業員をメンバーとして登録するための仮想的なトラストセンターを提供するサービス。顧客は、あたかも自前のトラストセンターを持っているかのように、Deutsche Post AGの持つトラストセンターを利用することが出来る。提供されるサービスのレベルは次のとおりである。

レベル１：従業員に対して証明書を発行
レベル２：認証局(IA)のための証明書を発行
レベル３：認証局（IA＋RA）のための証明書を発行

③　eVITA

ショッピングポータルサイトで、1999年５月からサービスを開始。毎月約300万のページビューがあり、ドイツのインターネット市場でその地位を確立している。

④　ePost Portal

ドイツ在住であれば誰でもePostのポータルサ

イトでメールアドレスを取得でき、このメールアドレスは、生涯無料で使用できる。

⑤　eCS

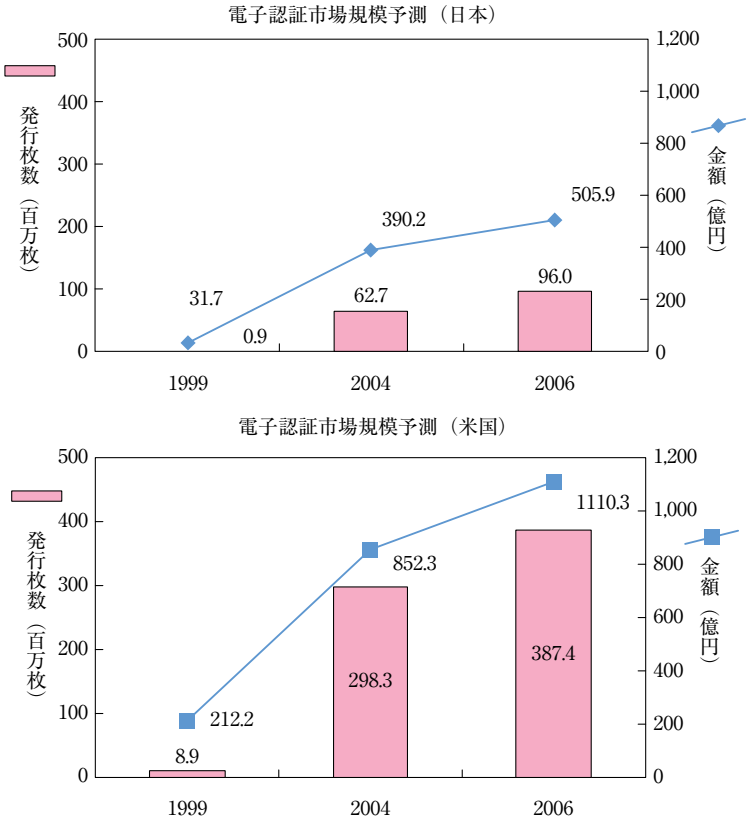
インターネットショップの開設から注文、代金支払い、在庫管理、配送、返品に至るまでのサービスを提供する総合サービスパック。

4　おわりに

インターネットの普及と電子署名法等の整備により、安全な電子商取引や電子政府の実現には電子認証が必要不可欠なものとなる。今後、郵政事業においても、インターネット利用を意識したサービスの充実が期待されてくることから、インターネット上で提供されるサービスを支える電子認証について検討しておくことは重要であり、本調査は、今後の検討を行うための基礎資料となることを期待している。

最後に、電子認証の市場規模を図表12に示す。これは、通商産業省（現経済産業省）と日本ブーズ・アレン・アンド・ハミルトン株式会社（BAH）が平成12年２月15日に発表した「電子認証ビジネスの将来像」の予測値であり、電子認証の使われ方を、B to B、B to C、組織内、公共サービス等でそれぞれモデル化して電子認証市場規模の予測が行われている。

図表12　電子認証市場の規模予測



注）通商産業省・BAH「電子認証ビジネスの将来像」より作成