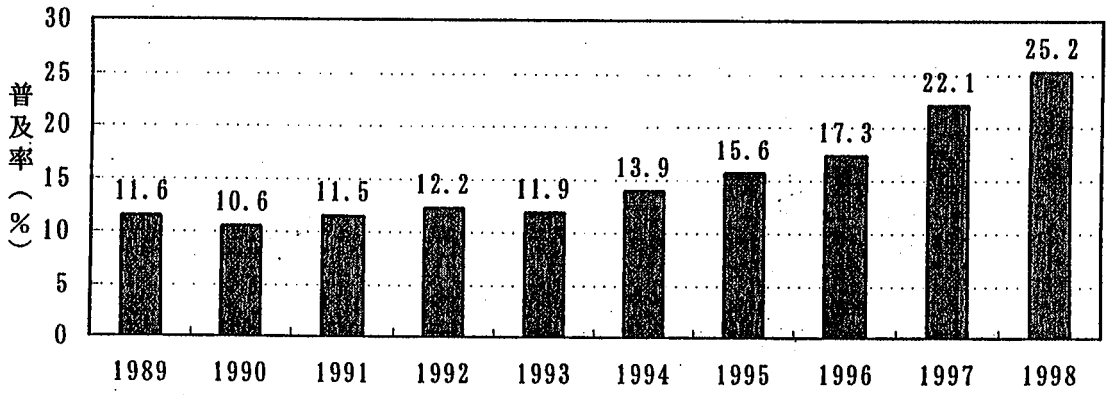
第１章　認証機関の必要性

１　ネットワーク社会の犯罪に対する脆弱性

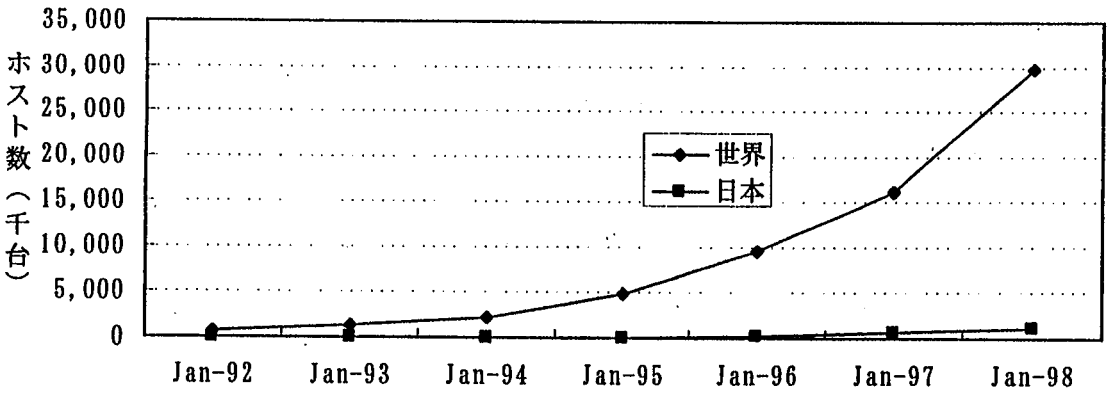
近年における情報化の進展はめざましく、あらゆる業務で、コンピュータ・システムが用いられているだけでなく、パソコンの一般家庭への普及率も年々増加している（図１－１－１参照）。また、コンピュータ相互がネットワークで結ばれることにより、地理的・時間的制約を超えて様々な情報を大量にかつ瞬時に伝達することができるようになり、行政、経済等の様々な分野において業務効率の向上が図られている。インターネットに接続されたホストコンピュータの台数は、平成１０年１月で約１１７万台と２年前の約４．３倍となっており、近年の我が国社会は急速にネットワーク化している状況にあると言える（図１－１－２）。

図１－１－１　パソコンの家庭への普及率の推移



（経済企画庁「消費動向調査」）

図１－１－２　インターネットに接続されているホスト数



（郵政省「平成10年通信白書」）

その一方で、インターネットにおける他人のＩＤやパスワード、あるいは他人のクレジットカード番号、架空名義や他人名義の銀行口座を等を利用したなりすましによる詐欺等のハイテク犯罪及び不正行為が急増し、その被害が問題になっている（図１－１－３、事例参照）。

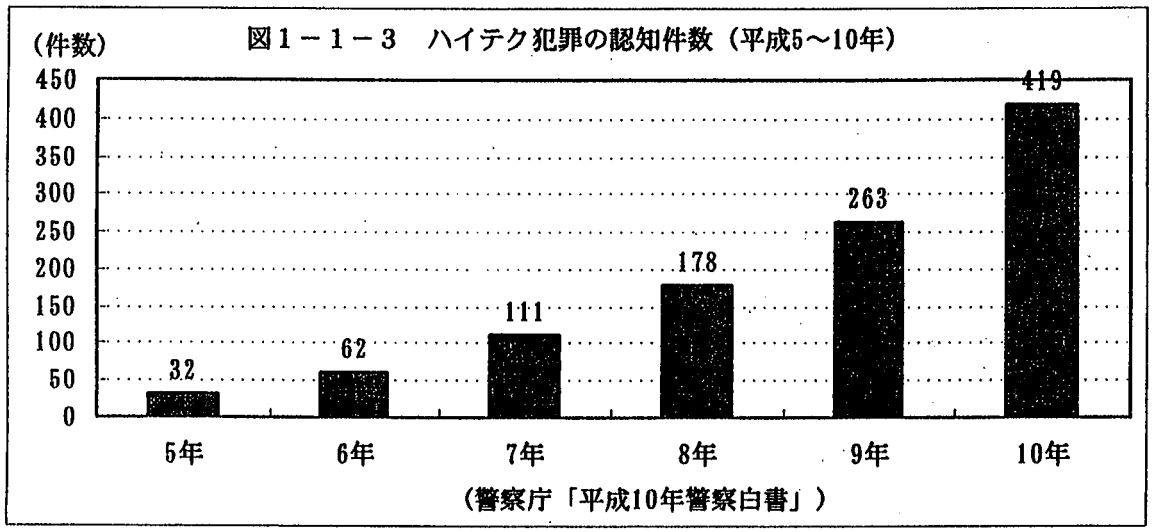


図１－１－３　ハイテク犯罪の認知件数（平成5～10年）
（警察庁「平成10年警察白書」）

事例１　わいせつ図画販売等事件

平成９年３月に逮捕された会社員は、パソコン通信を通じて購入した他人のＩＤ、パスワード及び銀行口座を利用して、電子掲示板にわいせつビデオテープの販売広告を掲載して購入者を募り、わいせつビデオを販売していたもの。

事例２　パソコン機器販売詐欺事件

平成９年３月に逮捕された自営業者は、クラッキングにより入手した他人のＩＤ、パスワード及び架空名義で開設した銀行口座を使用し、電子掲示板上にパソコン機器の販売広告を掲載、購入を申し込んだ者に対し架空名義の銀行口座に入金を指示し、これを騙取したもの（被害額約２４０万円）。

ネットワーク社会の特徴として、匿名性（ＩＤ、パスワード等の電子情報のみによって行為者を特定せざるを得ず、その特定が困難な性質）、無痕跡性（行為の物理的痕跡が残らない上、唯一残る電子的データの痕跡も改ざん、消去が容易である性質）、時間的・場所的無限定性（２４時間社会であるとともに、ネットワーク上の至る所で行為ができる性質）、超高速性（行為がボタン一つで一瞬にして完結する性質）等が挙げられ、これらの特徴は、ネットワークに係る犯罪等を行おうとする者にとって、自らの身分を明かさず、犯罪等の証跡を残さずに、国際的な規模で、しかも一瞬にして犯罪等を行うことが可能な環境が整うことを意味しており、実際、事例にもあるようなネットワークを利用したなりすまし犯罪が発生している。

このようななりすまし犯罪をはじめとするハイテク犯罪の急増は、内外において、深刻な問題となっており、このような認識の下、平成１０年５月に開催されたバーミンガムサミットにおいて、各国首脳は、ハイテク犯罪に対処するための法制や法執行機関の体制の整備、法執行機関と産業界の対話の促進等に取り組むことに合意した。国内においても、第１４２回国会施政方針演説及び第１４３回国会所信表明演説において、内閣総理大臣がハイテク犯罪対策を重要政策課題と位置付けている。

ハイテク犯罪や各種の不正行為は、このようなネットワーク社会の特徴に起因して多発しており、これらの特徴を鑑みると、事後の犯罪に対する取締りはもとより、事前の犯罪発生抑止対策を講じることが重要である。特に、ネットワークにおけるなりすましを防止する「本人確認」を確実に行うほか、情報の漏洩、盗聴、改ざん等を防止する「情報の保護」を図ることが重要である。ネットワーク上の「情報の保護」及び「本人確認」を確保するために、認証機能及び秘匿機能を有する暗号技術を利用することが極めて有用であり、現に電子商取引等においても利用され始めているところである。

2　暗号技術の概要

（１）暗号技術の基本原理

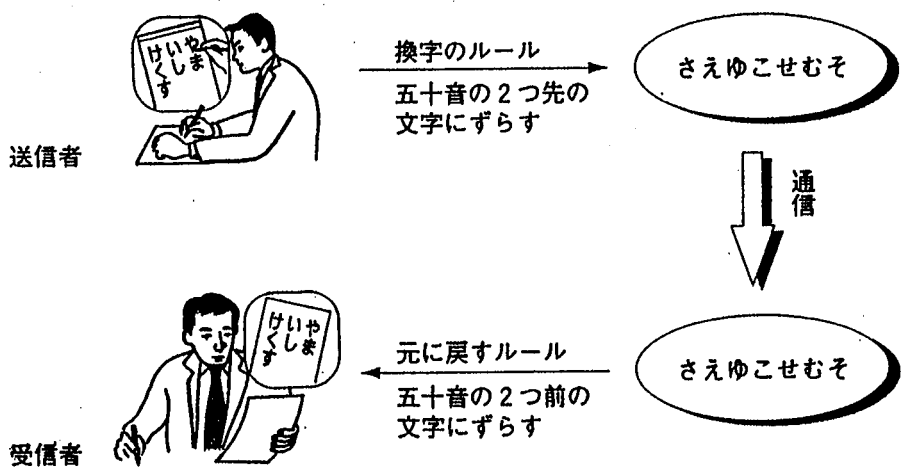
暗号技術とは、メッセージを一定のルールに従って変換することにより、当該ルールを知らない第三者がメッセージの内容を探知することを防ぐための技術であり、メッセージを秘密裡に伝達する秘匿機能及び通信の相手方が当該ルールを知っている正当な通信当事者であることを確認する認証機能を有している。

暗号技術は、メッセージを暗号化すること及び復号することをその基本とする。

暗号化とは、メッセージの文字列を暗号化鍵によって別の文字列に変換することをいい、変換前の文字列を「平文（ひらぶん）」、変換後の文字列を暗号文という。これに対し、復号とは暗号文を復号鍵により平文に戻すことをいい、さらに、解読とは、通信当事者以外の第三者が暗号文を平文に戻すことをいう。そして、暗号化鍵と復号鍵を総称して暗号鍵という。

単純な暗号化の方法の一つとして、次の例に示すようなシーザー暗号方式が挙げられる。

図１－２－１　暗号文通信



これは、「けいやくします」という平文を「五十音列の二個先に文字をずらす」というルールに従って暗号化して得られる「さえゆこせむそ」という暗号文についての例である。

暗号鍵は、暗号アルゴリズム（encryption algorithm）に適用されるパラメータ（parameter）を示すデータであるがあ、この例においては、暗号アルゴリズムとは「五十音列のＸ個先（前）の文字にずらす」と言う操作を指し、パラメータＸは「２」ということになる。そして、「五十音列の二個先の文字にずらす」という操作が暗号化鍵による暗号化に、「五十音列の二個前の文字にずらす」という操作が復号鍵による復号にそれぞれ該当することになる。

これが暗号技術の基本原理であるが、現実の暗号技術は、これとは比較にならないほど複雑化、高度化したものとなっている。

（２）暗号技術の分類

暗号技術には様々なものがあり、その分類方法にも様々なものがるが、暗号鍵の公開性により分類したものが、共通鍵暗号方式及び公開鍵暗号方式の分類である。

ア　共通鍵暗号方式

共通鍵暗号方式とは、暗号化鍵と復号鍵が同じであるため、通信当事者が同じ暗号鍵を所持することとする方式をいい、同じ暗号鍵を保有している者が通信当事者に限られることを前提として、送信者が暗号化した暗号文を復号できる者は受信者のみに限定されることにより暗号鍵を保有しない第三者に対して情報の秘匿を図ることができるとともに、受信者が復号した暗号文を暗号化できる者は送信者のみに限定されることにより送信者の本人確認（認証）を行うことができる。

共通鍵暗号方式の長所は、公開鍵暗号方式に比べ暗号化処理を高速で行うことができることであり、また短所は、通信当事者が暗号鍵を共有する過程において、暗号鍵の漏洩、盗聴等により第三者に暗号鍵を入手され、秘匿及び認証を行い得なくなるリスクを伴うこと等である。

イ　公開鍵暗号方式

公開鍵暗号方式とは、タイプの異なる二つの鍵が一組の暗号鍵として用いられることを前提として、そのいずれか一方を公開する方式をいい、秘密鍵で暗号化した場合にはその対となる公開鍵によってのみ復号が可能であり、公開鍵で暗号化した場合にはその対となる秘密鍵によっての

み復号が可能である。

公開鍵暗号方式では、送信者が受信者に対してメッセージを暗号化して送る場合において、送信者が受信者の公開鍵を利用してメッセージの暗号化を行うときは当該暗号文を復号することができる主体は受信者に限られることにより情報の秘匿を図ることができ、また、送信者が送信者の秘密鍵を利用してメッセージ等の暗号化（デジタル署名）を行い当該デジタル署名を受信者が送信者の公開鍵を用いて復号することができるときは当該デジタル署名を作成することができるのは送信者のみであることにより、送信者の本人確認を行うことができる。

公開鍵暗号方式の長所は、相手方への配信が必要となる公開鍵は、公開されており、通信当事者以外の者が入手することを前提としていることから、共通鍵暗号方式と異なり配信に際してリスクが存在しないこと等であり、短所は、共通鍵暗号方式と比べ暗号化処理が低速であることである。

（３）認証機関等の概要

ア　認証機関（Certification　Authority：ＣＡ）の概要

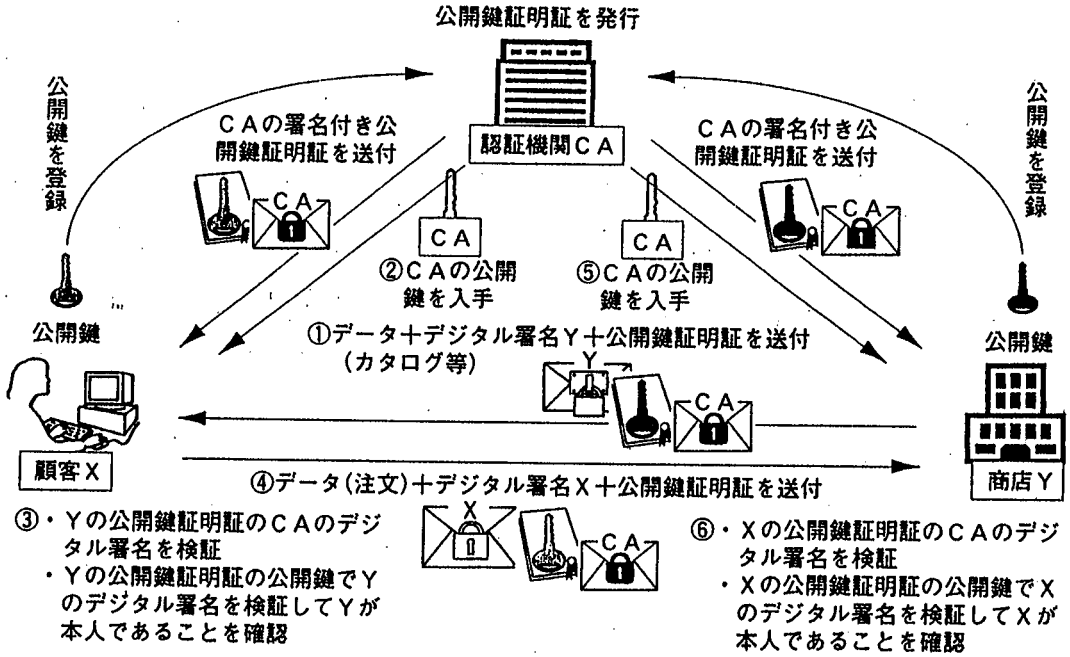
公開鍵暗号方式を利用して、情報の送受信を行う場合、公開鍵と秘密鍵とが合致するかどうかを調べることにより、情報の送受信の相手方の真実性を確認する方法であるので、暗号鍵とその名義人が一致しているという前提が確立している必要があり、公開鍵と公開鍵の名義人とが一致することを保証する「認証機関」が必要となる。現実に、我が国において、認証機関は次々と設立され、現実にサービスが提供されている。

図１－２－２　認証機関の設立状況

	日本ベリサイン	サイバートラスト	日本認証サービス
設立	1996年2月	1997年4月	1997年9月
開始	1996年6月	1997年10月	1997年10月
特色等	米国ベリサイン社の子会社	米国ＧＴＥ社の参加する合弁会社	日立、富士通、ＮＥＣが電子商取引事業に関し全面提供。
主な実施業務	公開鍵の登録 公開鍵証明証の発行 公開鍵証明証の管理	公開鍵の登録 公開鍵証明証の発行 公開鍵証明証の管理	公開鍵証明証の発行 公開鍵証明証の管理 公開鍵の登録及び本人確認は銀行等が実施
出資者等	ＮＴＴデータ 新日本製鐵 三菱商事 さくら銀行　等	ＧＴＥ社 ＢＵＧ社 野村総研 ＮＴＴドコモ　　等	日立製作所 富士通 ＮＥＣ　等

下図は、ネットワーク上における公開鍵暗号方式を利用した認証システムの一例である。

図１－２－３　認証システムの例



顧客Ｘと取引を行おうとする商店Ｙは、認証機関ＣＡに対して自らの公開鍵を提出し、その公開鍵に係るＣＡのデジタル署名付き公開鍵証明証の交付を受ける。公開鍵証明証の交付を受けた商店Ｙは、当該公開鍵証明証及び商店Ｙのデジタル署名を顧客Ｘに対するデータ（カタログ等）に添付して送信する。これを受け取った顧客Ｘは、商店Ｙの公開鍵証明証に付された認証機関ＣＡのデジタル署名を、認証機関ＣＡの真正な公開鍵を入手し検証を行うことによって商店Ｙに係る公開鍵証明証及びそれに記録されているＹの公開鍵の真正性を確認し、さらにその公開鍵を利用して商店Ｙのデジタル署名の検証を行うことによって商店Ｙが本当に商店Ｙであること及びデータ（カタログ等）を商店Ｙが作成したものであることを確認することができる。

同様に、認証機関ＣＡに対し自らの公開鍵を提出し、その公開鍵に係るＣＡのデジタル署名付き公開鍵証明証の交付を受けた顧客Ｘは、当該

公開鍵証明証及び顧客Ｘのデジタル署名を商店Ｙに対するデータ（注文）に添付して送信する。これを受け取った商店Ｙは、顧客Ｘの公開鍵証明証に付された認証機関ＣＡのデジタル署名を、認証機関ＣＡの真正な公開鍵を入手し検証を行うことによって顧客Ｘに係る公開鍵証明証及びそれに記録されているＸの公開鍵の真正性を確認し、さらにその公開鍵で顧客Ｘのデジタル署名の検証を行うことによって顧客Ｘが本当に顧客Ｘであること及び確かにそのデータ（注文）を顧客Ｘが作成したものであることを確認することができる。

以上のようにして、商店Ｙと顧客Ｘは、互いに相手方が本人であること及び送信されたデータ（カタログ等又は注文）が確かにその相手方が作成したものであることを確認し、安心して取引を行うことができる。

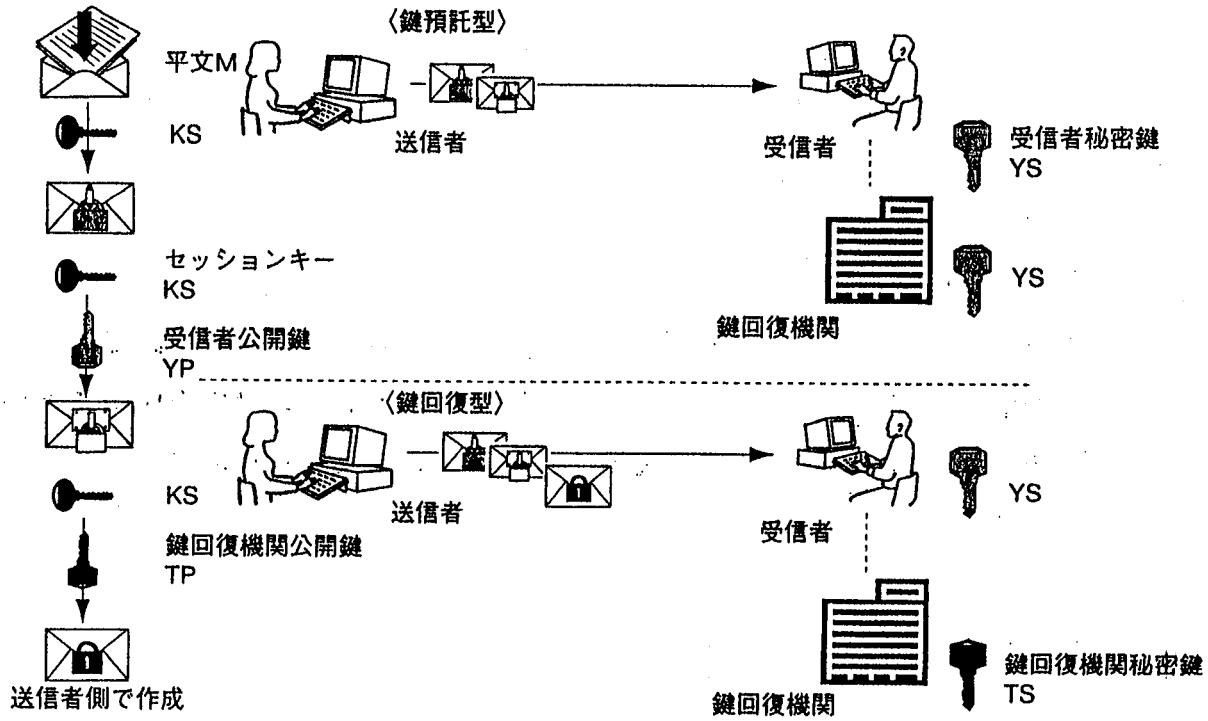
イ　鍵回復機関（ＫＲＡ）の概要

暗号技術の利用者がその暗号鍵を紛失したり、破壊してしまった場合等には、暗号化された情報を復号することができなくなる。

このような場合に備え、暗号文を解読するための暗号鍵等又は暗号文を解読した平文を第三者から入手できるようにする技術ないし仕組みをキーリカバリーシステムと言い、当該システムを利用して暗号鍵等の回復のサービスを提供するのが鍵回復機関である。

キーリカバリーシステムは、利用者の秘密鍵のコピーを鍵回復機関に預託しておく「鍵預託型（Key　Escrow）」と、利用者が情報の暗号化を用いたセッションキーを鍵回復機関の公開鍵等で暗号化したものを暗号文に添付し、利用者が秘密鍵を紛失した場合等には、鍵回復機関が自己の秘密鍵等でセッションキーを回復する「鍵回復型（Key　Encapsulation）」に大別することができる。

図１－２－４　キーリカバリーの仕組みの図



3　暗号技術普及の必要性

なりすましや情報の改ざん等によるハイテク犯罪等ネットワークに係る不正事案が急激に増加し始めている最近の我が国の状況（図１－１－３参照）は、匿名性、無痕跡性、時間的・場所的無限定性のほか、ネットワーク上を流通する情報がネットワークにつながる様々なコンピュータシステムを経由するため、情報の漏えいや改ざんのおそれがある性質等ネットワーク社会の有する犯罪等に対する脆弱性に起因するものである。

したがって、これらの犯罪等を防止するためには、通信当事者が他人になりすました者ではなく本人であること及び通信の内容が通信の途上で盗聴、改ざん等されていないことが確認されること、すなわち「本人確認」と「情報の保護」を図ることが必要である。そして、これらの課題の解決のためには、認証機能（「本人確認」の機能）及び秘匿機能（「情報の保護」の機能）を有する暗号技術（第１章２（１）参照）の利用が有効とされており、様々な暗号技術の開発が進められるとともに、現に利用され始めている。特に公開鍵暗号方式は、秘匿目的に用いられる公開鍵の配信に際して公開鍵を盗取されるリスクが存在しないことから、不特定多数の者が参加するネットワーク社会における「本人確認」機能を有するものとして注目されているが、この公開鍵暗号方式の暗号技術が人々の信頼の下に円滑・効果的に利用されるためには、通信当事者が互いに相手方の真正な公開鍵を確実に入手することが前提となり、公開鍵の真正性を証明しつつ公開鍵の管理・配信等の業務を行う、いわゆる認証機関（Certification Authority）（第１章２（３）参照）の存在が必要となる。

以上のとおり、匿名性、無痕跡性等をその特徴とし、犯罪等に対する脆弱性を有するネットワーク社会において、認証機能及び秘匿機能を有する暗号技術の利用により犯罪等の脅威への対応を図ることが、有力な犯罪防止対策と考えられ、優良な暗号技術を積極的に利用する必要がある。