

第4章 国内における認証機関に関する議論の動向

第1節 警察庁パブリックコメントの募集及びその結果について

1 「認証制度のセキュリティ確保方策についての基本的考え方」の概要

警察庁は、電子認証制度のセキュリティ確保方策の検討に当たり、パブリック・コメントの手法を採り入れ、「認証制度のセキュリティ確保方策についての基本的考え方」を示し、広く国民から意見を募集した。

(1) 実施時期等

ア 実施時期

平成11年11月18日(木)～12月17日(金)

イ 実施方法

警察庁ホームページへの掲載等の方法によって周知を図り、電子メール、FAX、郵便等の方法でコメントを募集した。

(2) 概要

インターネット等において他人になりすます等して行われる犯罪を防止するために、電子認証制度の整備に当たり、認証機関の在り方等について、次のような法制度を整備する必要があるとしている。

ア 公開鍵登録時の確実な本人確認の実施

認証機関に対し、電子証明書を発行する際には、発行を要求する者が名義人本人であることを確実な方法で確認しなければならないこととする法制の整備を図る。その際、本人確認の方法等についても定めることとする。

電子認証は、インターネット等において確実な本人確認の手段を提供するもので、電子証明書を発行するに当たり、認証機関が発行を受けようとする者について確実な本人確認を行うことは当然の前提である。

そのため、認証機関が公開鍵登録時の確実な本人確認を行うような制度を整備する必要があると考える。また、企業等が顧客の本人確認を行った上で電子証明書の発行を認証機関に依頼する場合、その企業にも電子認証の信頼性確保のための一定の措置を求める必要があると考える。

イ 認証機関の秘密鍵の厳格な管理

認証機関に対し、自らが発行する電子証明書の作成に用いる秘密鍵の漏出、破損等を防止するために、当該秘密鍵を厳格に管理することを求める法制の整備を図る。

電子認証制度は、認証機関の秘密鍵によって暗号化されたデジタル署名の真正性に対する信頼に基礎が置かれている。

もしデジタル署名に用いた秘密鍵の管理が厳格に行われなかった場合、秘密鍵を盗取して認証機関のデジタル署名を偽造した上で電子証明書を偽造することにより、他人になりすまして詐欺等の犯罪が行われることが懸念される。また、その結果、電子認証制度に対する信頼が揺らぎ、電子商取引全体の発展を損なうおそれがある。

そのため、認証機関に、電子証明書の作成に用いる秘密鍵の厳格な管理を求める必要があると考える。

ウ 認証機関の適格性及びセキュリティの確保等

認証機関がその業務を適切に遂行し、かつ、一般利用者が安心して電子認証制度を利用できるよう、前記1及び2に加え、認証機関に対し以下の各点を満たすこと

を求める法制の整備を図る。

併せて、これらの各要件を満たす認証機関を認定する制度の整備を図ることにより、信頼性の高い電子認証制度の普及を図る。

- (1) 役員等から暴力団員等を排除するなど人的適格性の確保（注1）
- (2) 顧客情報の厳格な管理
- (3) その他のセキュリティ措置（注2）

インターネット等における、なりすまし等による犯罪を防止するためには、上記1及び2以外にも、認証機関の業務が適切に行われるために必要な事項を満たすよう求める必要があると考える。

また、国民が安心して電子認証を利用できるような仕組みが必要であるが、そのためには、認証機関の設立は自由としつつ、(1)から(3)の条件を満たす認証機関を公的に認定し、それを表示することにより、信頼性の高い電子認証制度が普及する制度の導入が必要であると考えられる。

(注1) 経済活動に係る犯罪や、企業活動そのものに、暴力団や国際的犯罪組織等が関与する状況がうかがわれるが、今後、電子商取引等にもこれらの関与が懸念される。したがって、認証機関の業務の適格性、人的適格性を確保するために、暴力団員を排除する仕組みが必要である。

暴力団員等を排除する例として以下のものがある。

・ 債権管理回収業に関する特別措置法

法務大臣が債権管理回収業を営む許可を行うに当たり、暴力団員による不当な行為の防止等に関する法律第2条第6号に規定する暴力団員等がその事業活動を支配する株式会社（第5条第5号）、暴力団員等をその業務に従事させ又はその業務の補助者として使用するおそれのある株式会社（第5条第6号）、取締役等に暴力団員等がいる株式会社（第5条第7号へ）を排除し、これらの事由の有無について、法務大臣が警察庁長官の意見を聞くものとしている（第6条第1項）

・ 特定非営利活動促進法

特定非営利活動法人の設立の認証に当たって、当該特定非営利法人が暴力団（暴力団員による不当な行為の防止等に関する法律第2条第2号に規定する暴力団。）又は暴力団若しくはその構成員の統制の下にある団体でないことを要件とし（第12条第1項第3号。）、役員欠格事由として、禁錮以上の刑に処せられ、その執行を終わった日又はその執行を受けることがなくなった日から2年を経過しない者（第20条第3号）や暴力団員による不当な行為の防止等に関する法律の規定等に違反したことにより罰金の刑に処せられ、その執行を終わった日又はその執行を受けることがなくなった日から2年を経過しない者（第20条第4号）を定めている。

(注2) 例えば、セキュリティに係る適正な人的管理、施設・設備等についてセキュリティ基準を策定することが考えられる。

セキュリティ基準の例としては、例えば以下のような事項を規定することが考えられる。

1 内部者による不正行為への対策

- (1) 役員、従業員等の適格性の確保
- (2) 不正行為防止のための内部管理体制の整備

- ア 内部管理規定の整備
 - イ 権限の分散
 - ウ 教育・研修の実施
 - エ 外部監査を含めた事後監査体制の整備
 - オ 監査用記録の保存 等
- 2 部外者による不正行為への対策
- (1) 情報セキュリティ専門家の確保
 - (2) ファイアーウォールの設置等認証システムのセキュリティの確保
 - (3) 施設内への不正侵入防止等施設のセキュリティの確保
 - (4) 業務遂行上遵守すべき事項等
 - ア 公開鍵登録（更新）時の確実な本人確認の実施
 - イ 電子証明書の適切な有効期限の設定
 - ウ 偽変造の困難な技術の利用その他公開鍵証明書の真正性の確保
 - エ 電子証明書を失効させる必要が生じた場合の迅速、確実な失効及び周知の確保
 - オ 業務上知り得た個人情報に係る守秘義務 等

エ 認証機関のセキュリティ確保の支援

認証機関のセキュリティ確保を支援するための制度の整備も検討する。

- ・第三者による適切なセキュリティ監査を受けられる制度
- ・セキュリティ措置を強化するための行政による支援（注）

電子認証制度の安全性と信頼性を確保するために、認証機関のセキュリティが確保されるよう行政においても適切な支援をとる必要があると考える。

（注）同様の例として、不正アクセス行為の禁止等に関する法律第6条第1項において、不正アクセス行為が行われた場合の都道府県公安委員会による再発防止のための援助措置が規定されている。

オ 電子認証制度悪用行為の可罰化

電子認証制度を悪用する以下の行為等を禁止し、この違反に対して罰則を科す規定が必要である。

- ・他人名義で公開鍵を認証機関に登録する行為
- ・権限なく認証機関の秘密鍵を使用して他人名義の電子証明書を作成する行為
- ・他人名義の秘密鍵・電子証明書をを用いる他人名義のデジタル署名を作成する行為

認証機関の在り方を規定するだけでは、電子認証制度を悪用する行為を防止できない。前記のような電子認証制度を悪用する行為に対して刑罰を科す規定が必要であると考える。

2 その結果について

(1) 受信件数

54件

(2) コメントの概要

ア 認証機関に対する認定制の導入及びその要件について（44件）

認定制の導入については、大筋賛成を得られた。厳格な本人確認、秘密鍵の管理等の要件については、「厳格な顧客情報の保護も盛り込むべき」、「国民が安心して電子商取引を行えるようにするためには必要」などの賛成意見と、「電子商取引の発展を阻害する」、「法律が技術の進歩に対応できない」等を理由に反対する意見があった。

イ 認証機関のセキュリティ確保を支援するための制度整備について（20件）
行政による支援については賛成が大きく反対を上回った。監査制度については、「セキュリティを確保する上で望ましい」とする意見等がある一方、「セキュリティ確保方策は企業の自主性に委ねるべき」等を理由に反対する意見があった。

ウ 電子認証制度を悪用する行為等の禁止及び可罰化（32件）

総意としては、「電子署名・認証制度に対する社会的信頼を確保するために悪用行為を取り締まるべき」とするものの、「現行刑法で対応可能であるので新たな罰則規定の創設には反対する」という意見が全体の約半数あった。

（3）パブリックコメント募集後の方針

認証機関に対する認定基準が比較的ゆるやかなものとなれば、インターネット取引等において他人になりすまして行われる犯罪等が頻発するおそれが高いので、犯罪防止の観点から踏まえた電子認証制度（公開鍵登録時の十分な本人確認の実施、認証機関の人的・物的適格性及びセキュリティの確保等）の構築を法務省、通産省及び郵政省に求めて行くこととした。その結果、平成12年通常国会で成立した「電子署名及び認証業務に関する法律」では警察庁の意見が反映された内容となっている（第3節参照）。また、それ以外に、電子商取引による被害を早期発見し、被害の拡大防止を図るため、インターネット利用者・業界への情報提供等連携を強めていくこととしている。

第2節 3省パブリックコメントの募集及びその結果について

1 法務省、通産省及び郵政省「電子署名・認証に関する法制度の整備について」

法務省、通産省及び郵政省は、それぞれ、「電子取引法制に関する研究会（制度関係小委員会）」（平成8年7月～10年3月）、「電子商取引の環境整備に関する勉強会」（平成11年2月～7月）、「暗号通信の在り方に関する研究会」（平成11年1月～6月）における検討結果を踏まえ、電子署名・認証に関する法制度を整備するに当たり、基本的な論点を整理した「電子署名・認証に関する法制度の整備について」を公表し、広く国民から意見を募った。

（1）実施時期等

ア 実施時期

平成11年11月19日（金）～12月17日（金）

イ 実施方法

郵政省、通産省、法務省の各ホームページへの掲載等の方法によって周知を図り、電子メール、FAX、郵便等の方法でコメントを募集した。

（2）概要

ア 目的

- ① 最近、インターネットが急速に普及しているが、インターネットは国境を問わず、何時でも、どこでも、誰とでも容易に通信が可能であるため、電子商取引をはじめ、金融、教育、医療・福祉、行政等、様々な分野における重要な活動が急速にインターネット上で行われるようになりつつある。
- ② 反面、インターネットは、従来用いられてきた専用線等と異なり、必ずしも通信当事者が一対一の通信経路が確保されないオープンなネットワークであるため、