第２章　認証機関等の業務に係る脅威

１　認証機関の業務に係る脅威及びその方法

認証機関は、ネットワーク上における「本人確認」の役割を果たすものであるが（第１章２（３）参照）、この認証機関の役割を逆に悪用し、犯罪者が認証機関を設立し、若しくは認証機関と結託し、又は認証機関をだます等して、認証機関が発行する公開鍵証明証に当該公開鍵証明証に記録された公開鍵の使用者として現実の使用者とは異なる他人や架空人物が記録されることとなると、公開鍵証明証に記録された者と現実の使用者が異なる公開鍵がネットワーク上を流通し、当該公開鍵の現実の使用者は公開鍵証明証に記録された使用者になりすますことで、詐欺等のなりすまし犯罪を行うことが可能となる。従って、認証機関は、認証システムを悪用して犯罪を行おうとする者からの攻撃を受けやすいと言える。

認証機関を利用した公開鍵の不正流通の手段としては、次のように、公開鍵の不正登録又はすり替え、失効させるべき公開鍵又は公開鍵証明証の利用及び公開鍵証明証の偽変造を行うことにより、公開鍵証明証に記録された者と現実の使用者を異ならせることができ、詐欺等のなりすまし犯罪を行うことができる。それぞれ、認証機関又は認証機関の従業員等内部者による不正行為による場合と部外者の不正行為による場合とが考えられる。

（１）公開鍵の不正登録又はすり替え

認証機関又は認証機関の従業員等内部者による公開鍵の不正登録又はすり替えの他、部外者が、登録（更新）申請時に、他人名義を使って申請を行う方法のほか、申請・審査を経ず、認証機関に対しクラッキングを行い不正登録する方法などにより、なりすましを行うことができる。

（２）失効させるべき公開鍵又は公開鍵証明証の利用

認証機関及び認証機関の従業員等内部者による失効させるべき公開鍵又は公開鍵証明証を使用する方法の他、部外者が失効させるべき公開鍵又は公開鍵証明証が失効するまでのタイムラグを利用する方法により、なりすましを行うことができる。

（３）公開鍵証明証の偽変造

認証機関及び認証機関の従業員等内部者による公開鍵証明証を偽変造

する方法の他、部外者による認証機関が発行した公開鍵証明証の偽変造又は認証機関の秘密鍵の不正入手による公開鍵証明証の偽変造による方法により、なりすましを行うことができる。

2　鍵回復機関の業務に係る脅威

鍵回復機関（鍵預託型）は多数の利用者の秘密鍵等の保管・管理を行っており、犯罪者等はこれを攻撃することにより、一度に多数の秘密鍵を入手することが可能となり、それを利用することで、多数の人の情報を不正入手したり、多数の人になりすまし、様々な犯罪を行うことが可能となる。

また、鍵回復機関（鍵回復型）が自己の秘密鍵を復号鍵として鍵回復業務を行う場合には、当該秘密鍵を入手することにより、当該鍵回復機関を利用するすべての利用者のセッションキーを復号し、当該利用者の情報を不正に入手することが可能となる。鍵回復機関に係る秘密鍵等の不正入手の手段としては、鍵回復機関又は鍵回復機関の従業員等内部者が不正行為により入手する場合と部外者がクラッキング、鍵回復権限を有する者へのなりすまし等による場合とが考えられる。

さらに、利用者の秘密鍵等を入手するため、犯罪者が鍵回復機関を設立するおそれもある。

第３章　認証機関に関するガイドライン等

１　認証機関の在り方をめぐる国内の検討状況

認証機関の在り方については、各省庁等がそれぞれの立場から検討を行っており、ガイドライン等を発表している。

警察庁の外郭団体である（財）社会安全研究財団は、犯罪に対し脆弱であるネットワーク社会においては、情報の保護及び本人確認を図ることが犯罪防止上、重要であり、これには暗号技術の利用が有効としているが、認証機関の業務が適正に行われない場合、暗号技術の利用がかえって犯罪を助長する結果となりうることから、認証機関及び鍵回復機関の適格性及び業務の適正性を確保する必要があるとの立場から、平成１０年３月、「情報セキュリティビジョン策定委員会報告書」を作成、公表している。

通産省は、電子商取引の促進による経済振興を図る立場から、電子商取引における取引情報等に対する盗聴、改ざん、詐称等を排除し、電子商取引における信頼を確保する必要があるとしている。同省から援助を受けた様々な民間企業が参画している電子商取引実証推進協議会は、実証実験の結果に基づき、平成１０年３月、認証局運用ガイドライン（１．０版）を作成、公表している。

また、郵政省は、電子商取引において不可欠なインフラである電子認証について、認証業務が適正に提供されるための法的枠組みが必要との立場から検討を行い、平成９年５月、「ネットワーク認証業務に関するガイドライン」を作成、公表している。

２　各ガイドライン等の内容

１で掲げた各ガイドライン等の内容は、それぞれ次のとおりである。このうち、犯罪防止の観点から認証機関が具備すべき要件を定めているものは、「情報セキュリティビジョン策定委員会報告書」だけである。

（１）情報セキュリティビジョン策定委員会報告書

ア　従業員等内部者による不正行為の防止方策

（ア）従業員等の適格性の確保

一定の前科を有する者等類型的に公開鍵の不正登録を行うおそれのあ

る者が認証機関又はその役員若しくは従業員ではないことを確保する必要があるとしている。

（イ）内部管理規程の整備

内部管理規程の内容については、具体的に触れられていないが、内部者が不正行為を行いにくい環境を整備するためには、その整備が必要であるとしている。

（ウ）組織体制

内部けん制、監視等により不正行為を防止するため、権限を分散する必要があるとしている。

（エ）財務的基盤の確保

財政状態の悪化により、不正行為を誘発することのないように、継続的に認証業務を行い得る財政的基盤を保有している必要があるとしている。

（オ）情報開示

特に触れられていない。

（カ）監査

具体的な監査方法については触れられていないが、外部監査を含めた監査体制が必要であるとするとともに、監査用記録を保存する必要があるとしている。

（キ）個人情報の保護

業務上、多数の個人を識別する情報を知り得ることから、なりすましによる公開鍵の登録その他のなりすましによる犯罪等を防止するため、業務上知り得た個人を識別する情報の開示を禁止する必要があるとしている。

イ　部外者による不正行為の防止方策

（ア）情報セキュリティ専門家等の確保

クラッキング等に備えて、システムのセキュリティを保全するとともに、クラッキング等があった場合に的確に対応する能力を有する者を配置している必要があるとしている。

（イ）公開鍵及び公開鍵証明証の登録・管理等に係るシステムのセキュリテ

ィ確保

ファイアウォールの設置等公開鍵及び公開鍵証明証の登録・管理等を行うシステムのセキュリティが確保されている必要があるとしている。

（ウ）本人確認に関する事項

他人になりすました公開鍵の登録等を防止するため、対面での運転免許証の提示や、近年実用化の研究が進められているバイオメトリックス技術の活用により確認する等、確実な本人確認が必要であるとしている。

（エ）公開鍵証明証の管理に関する事項

一つの公開鍵及びその対になる秘密鍵が長期にわたり利用された場合には、秘密鍵の不正入手等により、これと対になる公開鍵に係る公開鍵証明証を不正に利用したなりすましによる犯罪等の発生のおそれがあることから、このようなおそれの少ない適切な有効期間を定めることが必要であるとしている。

また、秘密鍵が不正に入手された場合において、当該秘密鍵と対になる公開鍵に係る公開鍵証明証を不正に利用したなりすましによる犯罪等の発生のおそれがあることから、公開鍵証明証を迅速・確実に失効させるとともに、利用者に周知させる必要があるとしている。

（オ）物理的要件

認証機関の設置場所へ部外者の立入りが無制限に行われないよう、立入禁止区域を設定し、立入禁止区域への施錠等物理的な侵入を防止する施設のセキュリティが確保がされている必要があるとしている。

（２）認証局運用ガイドライン（１．０版）

ア　従業員等内部者による不正行為の防止方策

（ア）従業員等の適格性の確保

信頼できる人材を確保するため、採用時に適切な人物審査を行う必要があるとし、採用後も、メンタルヘルス・健康管理・適切な処遇等における継続した人事管理を行う必要があるとしている。

（イ）内部管理規程の整備

認証機関の業務を適正に行うためには、具体的作業が正確に行えるよう、作業項目や手続き等についてマニュアルを整備し、それが適正に実

施されるよう管理することが必要であるとしている。特に、セキュリティの対象となる場所へのアクセス、セキュリティの対象となる機器類へのアクセス、セキュリティの対象となる情報へのアクセス等について、ポリシーに準じた厳密な事務取扱要領（内部管理規程）を規定しておく必要があるとしている。

（ウ）組織体制

事故を未然に防ぐための部署内での相互牽制が行え、部署外からの監査等チェック機能が働くようにし、かつ事故発生時の発生源が特定できるような体制にする必要があるとしている。

（エ）財務的基盤の確保

認証機関の責に帰される損害への賠償及び認証機関の諸機能遂行に係る継続的な投資を行うことができるよう十分な財政基盤を保持する必要があるとしている。

（オ）情報開示

認証機関の信頼性、安全性を確認できるように、財務状況を含めた経営情報、暗号アルゴリズム、暗号通信プロトコル等の技術情報、内部不正防止対策、権限の分散、教育など業務運営に関する監査結果等を開示する必要があるとしている。

（カ）監査

認証機関に要求される業務の専門性、信頼性等が十分に保たれているかどうかを調べるために、利用者との契約事項、内部管理規程等各種基準を遵守しているかどうかを、運営、設備、システムの面から監査を行うことにより、利用者の信頼性の維持・確保を図る必要があるとしている。

監査にあたっては、コンピュータ・セキュリティに関する専門的知識を有する監査対象から独立かつ客観的立場の者により、申請書類、申請受付担当者、本人確認手段などの認証申請に係る情報、暗号鍵の生成、ロード、バックアップ、保管、リカバリー、廃棄などの暗号鍵管理に係る履歴、機密データの入出力・削除、セキュリティプロファイルの変更、設備等への入退室管理などの機密情報のアクセス履歴、認証機関が交信

したデータ、発行認証機関、失効申請などの受発信データ等の情報を対象に、最低年１度行う。監査の結果、欠陥が指摘された場合、欠陥の対処措置を講ずるとともに、監査結果等の保存については、保存期間を予め定め、不正アクセスによる情報の変更、改ざん及び削除等がないよう適切かつ合理的な安全対策を講ずる必要があるとしている。

（キ）個人情報の保護

公開鍵証明証の申請時に入手した認証機関の利用者に関する個人情報は、プライバシー侵害もしくは不正利用等の防止のために、これらの情報にアクセスできる者を限定したり、不正に改ざん・消去・漏洩等がなされないように安全に保管する仕組みを持つようにする必要があるとしている。

イ　部外者による不正行為の防止方策

（ア）情報セキュリティ専門家等の確保

安全性と信頼性の高い業務を持続的に行い、技術進歩に適切かつ十分に対応し、また、トラブル等が発生した場合に迅速に対応するためには、情報セキュリティ技術やシステム監査等の専門家を配置しておく必要があるとしている。

（イ）公開鍵及び公開鍵証明証の登録・管理等に係るシステムのセキュリティ確保

外部のオープンなネットワークに接続する場合は、ファイア・ウォールの設置等の対策を講じるとともに、ファイアウォール等の機器についての防犯・防災対策を講じる必要があるとしている。

（ウ）本人確認に関する事項

本人確認を行う際、信頼できる機関・組織・人による証明あるいは確認済みの情報と一致していることを照査する必要があるとし、より高い信頼性を確保するためには、本人出頭による方法が望ましいとしながらも、オンライン申請、書類送付申請、出頭申請のそれぞれの場合の本人確認の方法を例示している。

○　オンライン申請

認証機関に対しオンライン形態で公開鍵証明証の申請を行う場合、

生年月日、住所、電話番号、クレジットカード番号、暗証番号等の情報を複数入力させて、これらの情報が信頼できる機関（クレジットカード会社、銀行等）の保有する情報、又は自らが保有する情報と突き合わせる方法が考えられるとしている。

○　書類送付申請

認証機関が定める申請書式に必要事項を記載させ、印鑑登録証明書、戸籍謄本、商業登記簿謄本等と併せて送付させ、申請書式の記載事項と各証明書等の記載事項及び捺印とを突き合わせる方法が考えられるとしている。

○　出頭申請

申請者を出頭させ、認証機関が定める申請書式に必要事項を記載させ、運転免許証、パスポート、健康保健証等を提示させ、申請書式の記載事項とそれらの写真及び記載事項とを突き合わせる方法が考えられるとしている。

（エ）公開鍵証明証の管理に関する事項

公開鍵証明証については、定期的に更新する必要があるとし、新規発行時の場合と同様、本人確認の手続が必要としている。

また、秘密鍵の紛失等により失効した公開鍵証明証については、失効リストに掲載、保管し、正当な利用者の問い合わせに適宜応じる必要があるとしている。

（オ）物理的要件

認証機関が設置される建物の立地場所、構造や敷設される電源設備、通信設備等の設備について、適切な防災及び安全対策を施す必要があるとしている。立地条件としては、火災、水害、地震あるいは電磁界、落雷、空気汚染などの被害の恐れのある場所を避ける必要があるとしている。

認証機関内部の公開鍵証明証や個人の審査情報などを取り扱うコンピュータ・システムを設置している室は、最低限間仕切りなどで隔離し、その他の業務を行うコンピュータ・システムとは別の室に設置する必要があるとしている。また、当該室には、ＩＤカード等を利用することに

より、限られた要員のみに限定する必要がある。また、当該室への入退出に際し、ログ等の記録を残すとともに、当該室が無人となっても、センサなどにより不正侵入を検知し、システム管理者等へ通知するような対策を講ずる必要があるとしている。

（３）ネットワーク認証業務に関するガイドライン

ア　従業員等内部者による不正行為の防止方策

（ア）従業員等の適格性の確保

特に触れられていない。

（イ）内部管理規程の整備

従業員による内部不正を防止するためにも内部管理規程を整備する必要があるとしている。

（ウ）組織体制

内部不正を防止するため、適切な権限分散や業務ローテーションを行うことが必要であるとしている。

（エ）財務的基盤の確保

認証機関は業務の提供に当たって、一定の法的責任を負う可能性があることから、安定的な財務的基盤を維持することが望ましいとしている。

また、財務諸表等の公表を通じて、自己の財務状況の開示を行うことが望ましいとしている。

（オ）情報開示

認証業務は、まだ萌芽期にあり、利用者にとっては、その業務内容や法的責任等についても、不明確な点も多いことから、業務内容、安全対策、法的責任、財務的基盤等について、広く利用者に対して開示をしていくことが望ましいとしている。

また、利用者以外に対してもどのような方法で本人確認を行っているについて広報する必要があるとしている。

（カ）監査

業務運営体制の信頼性を確保するため、その業務運営の状況について、定期的に外部の専門家による監査を実施することが望ましいとしている。

（キ）個人情報の保護

公開鍵証明証の申請時に入手する利用者に関する個人情報は、業務提供のために必要最小限の情報に限定すべきとしている。

また、個人情報が、その入手目的以外に流用されたり、第三者に開示されたりすることがないよう、個人情報の保護に関する内部管理規程を定める必要があるとしている。個人情報の保護に関する内部管理規程は、個人情報を扱う立場にある従業員に対して適切な研修を実施するなどして、周知徹底を図ることが望まれるとしている。

イ　部外者による不正行為の防止方策

（ア）情報セキュリティ専門家等の確保

情報セキュリティ対策を講ずる必要はあるとしながらも、情報セキュリティ専門家の登用については特に触れられていない。

（イ）公開鍵及び公開鍵証明証の登録・管理等に係るシステムのセキュリティ確保

認証機関に対する外部からの不正アクセス等を防止するために、信頼性の高いファイアウォールの構築等の措置を講ずることが必要であるとしている。

（ウ）本人確認に関する事項

本人確認に際しては、通常、本人しか知り得ない（ないし持ち得ない）情報や身体的特徴等により身元を確認することが必要であるとしている。その例として、個人の場合、運転免許証、パスポート、写真入りの身分証明証、住民票、印鑑証明等による確認、法人の場合、登記簿謄本及び代表者の印鑑証明等による確認を挙げている。

（エ）公開鍵証明証の管理に関する事項

公開鍵証明証は、暗号鍵の強度等を勘案して、一定の有効期限を設けることが望ましいとしている。

（オ）物理的要件

地震、火災、水害等の自然災害から守るため、設備の安全性を確保するための措置を講ずる必要があるとしている。