第４章　鍵回復機関に関するガイドライン等

１　鍵回復機関の在り方をめぐる国内の検討状況

鍵回復機関について、今のところ、サービスの提供を行っているものはなく、その在り方について検討を行っているのも、警察庁の外郭団体である（財）社会安全研究財団だけである。

平成１０年３月に作成、公表された「情報セキュリティビジョン策定委員会報告書」では、鍵回復機関には多数の秘密鍵が保管・管理されることから、内部者及び部外者等による秘密鍵等の盗取が発生するおそれがあるため、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している。

２　報告書の内容

情報セキュリティビジョン策定委員会報告書で示された鍵回復機関が満たすべき要件は次のとおりである。

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秘密鍵等の不正入手を行うおそれのある者が鍵回復機関又はその役員若しくは従業員で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、継続的に鍵回復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

なりすましや秘密鍵等の漏洩を防止するために、受託に係る秘密鍵等その他の個人を識別する情報に係る守秘義務を従業員等に対し課す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）秘密鍵等の管理及び回復のシステムのセキュリティの確保

秘密鍵等の管理についてオープンネットワークに接続されないコンピュータを利用する等秘密鍵の管理・回復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）物理的要件

部外者の立入禁止、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。

第５章　認証機関等に対する調査の概要及び結果

１　調査の内容

この章では、国内で既に業務を行っている認証機関及び鍵回復機関のどのくらい存在するかを把握するとともに、「情報セキュリティビジョン策定委員会報告書」において、犯罪防止の観点から認証機関及び鍵回復機関が具備すべきとされている要件について、存在が確認された認証機関及び鍵回復機関が、当該要件を満たしているかどうかを調査する。

２　調査対象会社の概要

（１）認証機関

	日本ﾍﾞﾘｻｲﾝ（株）	日本認証ｻｰﾋﾞｽ（株）	ｻｲﾊﾞｰﾄﾗｽﾄ（株）
設　立	平成８年２月	平成９年９月	平成９年４月
所在地	神奈川県川崎市幸区堀川町580-16	東京都港区芝1-10-11　ｺｽﾓ金杉橋ビル	北海道札幌市北区北７条西1-1-2
資本金	２億７千万円	４億７千万円	１５億円
事業開始	平成８年６月	平成９年１０月	平成９年１０月
特色等	米国の認証機関であるﾍﾞﾘｻｲﾝの子会社	日立、富士通、ＮＥＣが電子商取引事業に関し全面連携。公開鍵証明証の発行を専門的に行う。	米国ＧＴＥ社の参加する合弁会社
出資者等	NTTﾃﾞｰﾀ、新日本製鐵、三菱商事、さくら銀行　等	日立製作所、富士通、ＮＥＣ　等	GTE社、BUG社、野村総研、NTTﾄﾞｺﾓ　等
主な事業内容	・公開鍵証明証の発行（公開鍵の登録及び本人確認は銀行等が実施） ・公開鍵証明証の管理	・公開鍵証明証の発行（公開鍵の登録及び本人確認は銀行等が実施） ・公開鍵証明証の管理	・公開鍵証明証の発行（公開鍵の登録及び本人確認は銀行等が実施） ・公開鍵証明証の管理

（２）鍵回復機関

鍵回復機関の存在は確認できず、これに対する調査を行うことはできなかった。

３　調査の結果

（１）従業員等内部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の確保

Q

従業員を採用する基準はありますか？あれば、その内容をお教え願います。

基準がない場合であっても、従業員の適格性を確保するために、採用時に留意している事項がございましたら、その内容をお教え願います。

A

３社とも、内部者による不正行為を防止するためには、信頼できる従業員を確保することが最も重要と考えていると答えているものの、採用する際の基準を明確に定めているものは無かった。

しかしながら、各社とも、採用前に、複数の人間により、時間をかけ、面接を行う方法により、信頼できる人間であるかの確認を行っている。その中では、コンピュータ・システムに関する知識も問われ、情報セキュリティに関する専門家であるかどうかの判断もなされる。中には、第三者（人材派遣会社）による面接を受けさせ、多様な観点から認証機関の従業員としての適格性を備えているかを試される。

また、採用時に、業務上知りえた秘密を保持する義務を遵守する等を内容とする宣誓書の提出を求めるものが２社あった。また、試用期間を通常より長く設定するものもあった。

イ　内部管理規程の整備

Q

内部者による不正行為を防止する目的で定められた内部管理規程はありますか？あれば、その内容についてお教え願います。

A

各社とも以下のような内容の内部者による不正行為を防止することを目的とした内部管理規程を定めている。

・認証機関内の各部屋への入室を制限し、どの職責がある者がどの部屋に入ることができるかを定めている。

・重要な情報やコンピュータが保管されている部屋には、単独の入室を認めず、複数以上の者の入室を必要としている。

・重要なデータが保管されているコンピュータ等の装置を操作する場合、相互に牽制し、適正性を確保するため、複数以上の者による操作を必要とする。

ウ　組織体制

Q

内部者間の相互牽制を行うため、権限の分散を行っていますか？権限の分散を行っているのであれば、その内容についてお教え願います。

A

各社とも、メンテナンス、オペレーション、営業、管理等の部門ごとに、権限を分けており、上層の経営陣以外には、権限が集中しないようになっている。認証機関内の各部屋及び装置へのアクセス権限についても部門ごとに定められており、例えば、コンピュータのメンテナンスを行う者は単独で入室ができないこととし、入室する権限を有する他部門の者の同伴を必要とするなど、場合によって、異なる部門の者が入室しなければ、装置の操作ができないような仕組みを作っている会社もある。

また、上層の経営陣の専横を防ぐため、各部門から米国本社に

それぞれの部門に関する業績等を直接報告する仕組みを構築し、米国本社による牽制を行っている会社もある。

エ　財務的基盤の確保

Q 資本金の額はいくらですか？ 財務諸表等を公開していますか？

A

4億7千万円～15億円。

1社を除き、公開会社でないことを理由に、財務諸表は公開していない。

オ　監査

Q 業務監査は実施していますか？また、その頻度はどれくらいですか？ 監査人は内部者ですか外部者ですか？ 監査人はどのような資格や知識を有する者が行っているのですか？ 監査の記録は保存していますか？保存している記録はどのようなものであり、どのくらいの期間保管していますか？

A

各社とも業務監査を行っており、3社のうち1社が年2回、その他が年1回、定期的な自己監査を行っている。自己監査の方法については、内部規程、ＣＰＳに基づき作業が行われているかどうかを確認するという内容のものである。

また、各社とも顧客であるクレジットカード会社が認証機関に要求している基準を満たしているかどうかという観点から、当該クレジットカードの者による監査を受けている。

これ以外に、2社が、外資系監査法人によるシステム監査を受

けることとしている。

監査人の資格・要件については、各社とも、特に定めていないと回答しているが、ある社は、監査の経験が長い者をその任に当てていると答えている。

各社とも、監査記録は、７年～１０年間、改ざんされないよう厳重に金庫等に保管することとしている。保存する記録は、各社とも全ての監査結果を保存すると回答しており、ある社は、監査記録のうち最も重要なものは、暗号鍵の破壊に関する記録であると答えている。

カ　個人情報の保護

Q

公開鍵証明証の申請時に入手する個人情報の保護に関して、内部管理規程を整備していますか？整備しているのであれば、その内容をお教え願います。

個人情報を保護するためには、どのような方策を行っていますか。

A

各社とも、公開鍵証明証を発行する際の本人確認を行っていないので、個人情報を保管することはないとのことである。

従って、保護すべき対象がないので、個人情報保護のための措置は講じてない。

（２）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の確保

Q

認証機関に対する不正アクセス等のトラブルに対応できるように、情報セキュリティに関する専門家は配置していますか？

情報セキュリティ専門家が有する知識の具体的内容は？

A

各社とも、セキュリティ対策には力を入れており、当然のこととして、情報セキュリティに関する専門家を配置している。ある社は、社員全体の１／４が情報セキュリティに関する専門家であると答えている。

各社とも、情報セキュリティに関する専門家が有すべき知識の基準は定めていないが、採用時に行う面接において、情報セキュリティに関する質問を行う等して、その専門家の確保に努めていると回答している。

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

Q

ファイアウォールの設置等のセキュリティ確保の実施を行っていますか？行っているのであれば、その内容についてお教え下さい。

A

各社とも、セキュリティ対策の詳細な部分については、部外秘であることを理由に、回答していないが、ファイアウォールの設置はもちろん、その他のセキュリティ対策についても十分な措置を講じているとのことである。

ある社は、重要なデータを暗号化し、その暗号鍵を分割して、複数の人間が持ち合うという措置を講じていると回答した。

ウ　本人確認に関する事項

Q

公開鍵証明証の申請を受理する際に行う本人確認の方法についてお教え下さい。

本人確認をクレジットカード会社等に行わせている場合は、その方法についてお教え下さい。

A

各社とも、クレジットカード会社、銀行等の顧客の依頼に応じ、クレジットカード会社の会員、銀行の顧客に対し、公開鍵証明証を発行する業務を行うのみで、本人確認は行っていない。

クレジットカード会社における本人確認方法は、カード発行の際に行う審査と同じであり、申請者に氏名、住所、電話番号、銀行口座番号等を記載させるものである。

エ　公開鍵証明証の管理に関する事項

Q

公開鍵証明証には、有効期限が設定されていますか？設定されているのであれば、その年数をお教え下さい。

失効した公開鍵証明証については、周知するなどの措置がとられていますか。

A

各社とも、公開鍵証明証の有効期限については、顧客との契約に応じ、１～３年の間としている。

失効した公開鍵証明証の周知については、１社が失効情報をホームページに掲載している以外は、周知を行っていない。

オ　物理的要件

Q

建物は、自然災害に耐えうる構造になっていますか？また、部外者の侵入を防止するような構造になっていますか？そうであれば、その内容についてお教え下さい。

利用者の個人情報等保護すべき情報が保管されている部屋の構造は強固になっていて、そこへの立入りが制限されていますか？

A

各社とも、大きな地震（阪神大震災程度）に耐えられる建物内に認証業務を行う部屋が置かれている。中には、停電に対応できるよう自家発電装置を設置しているところもある。

部外者の侵入防止対策としては、各社とも、各部屋にビデオカメラを設置し、モニタリングを行っており、部屋の構造についても、複数の部屋を通過しなければ、重要なデータ等が保管されているコンピュータが置かれている部屋にたどり着けないよう工夫が施されている。各部屋に入る際には、カード等による認証を行うなどのアクセスコントロールを行っており、中には、入退室の記録（ログ）を保存しているものもある。

また、各社とも、内部管理規程に基づき、重要な保護すべき情報が保管されている部屋への入室できる者を少数に限定しており、また、入室には複数の人間を必要とすることとしている（デュアルコントロール）。