ＩＴ委員会実務指針第４号

公認会計士業務における情報セキュリティの指針

平成 20 年１月 16 日
改正　平成 22 年３月 19 日
改正　平成 24 年８月 30 日
最終改正　平成 28 年７月 25 日
日本公認会計士協会

－目　　次－

頁

Ⅰ　はじめに

１．背景

情報技術（以下「ＩＴ」という。）の発達に伴い、公認会計士が業務を実施するに当たり、被監査会社、税務、コンサルティング等の顧客（以下「クライアント等」という。）から種々の情報を電子データとして入手する機会が増え、また、公認会計士一人ひとりが、パーソナルコンピュータ（以下「ＰＣ」という。）等の情報機器を持ち歩き、クライアント等と業務に関する情報のやり取りに電子メールを利用する、情報収集のためにインターネットを利用する、といったことは、既に日常になっている。そして、業務に関連する情報は電子データだけとは限らず、紙媒体でも存在し、電子データと同様に、持ち歩くことも多い。

公認会計士は、これらの情報の重要性を認識し、紛失や漏洩への対応を行っているが、紛失や漏洩への対応は終わりがなく、常に、自らの管理体制を見直すことが必要である。また、不正・私的利用という観点だけではなく、マルウェアによる情報詐取など、ＩＴの進歩に合わせた情報セキュリティ及び体制の見直しを行うことも必要と考えられる。

クライアント等から入手した情報が外部に漏洩した、不正の目的又は私的利用のために持ち出されたとなれば、当事者である公認会計士がクライアント等からの信頼を失うばかりでなく、公認会計士としての存続が危ぶまれることにもなりかねず、さらに公認会計士業界全体に多大な影響を及ぼすこととなる。公認会計士は、従来からの守秘義務の意味を再認識し、電子データだけではなく紙媒体の情報も含めた、特にクライアント等に関する情報の漏洩・流出、不正・私的利用のリスクを十分に認識し、公認会計士業務という最も社会的信頼性を保持すべき業務の観点から、その対策を検討しなければならない。

２．本実務指針の目的と対象範囲

このような状況を踏まえ、本実務指針は、公認会計士が監査に限定されない全ての業務において留意すべき情報セキュリティについての指針を提供することを目的としており、公認会計士は、本実務指針に従って情報漏洩を防ぐ体制を構築し、運用することが必要である。

公認会計士の業務は、監査、税務、コンサルティングなど多岐にわたり、その中で取り扱う情報も様々である。そのため、本実務指針では、情報漏洩（紛失、不正・私的利用を含む。）に焦点を絞り、対象とする情報は、電子データだけではなく紙媒体も含まれ、業務に直接関係する情報に限定し、公認会計士事務所（監査法人）自身の管理に関する情報は対象としていない。

なお、監査業務における監査調書については、品質管理基準委員会報告書第１号「監査事務所における品質管理」も適用されるため、留意する必要がある。

３．本実務指針における用語の定義

本実務指針において使用する用語の定義は、以下のとおりである。

・　公認会計士等

公認会計士及び公認会計士事務所（監査法人）の職員等をいう。

・　公認会計士事務所（監査法人）

業務を行うために開設した会計事務所、監査法人をいう。

・　クライアント等

被監査会社、税務、コンサルティング等の顧客をいう。

・　グループ会社

公認会計士等と資本関係がある会社、又は公認会計士事務所（監査法人）の主要な経営者が兼務する他の事務所や組織をいう。

なお、倫理規則に定めるネットワーク・ファームと同義である。

・　職員等

公認会計士事務所（監査法人）の職員（派遣、パート、アルバイト等を含む。）をいう。

Ⅱ　情報セキュリティ管理の重要性

１．守秘義務の重要性についての再認識

監査基準の一般基準８は、「監査人は、業務上知り得た事項を正当な理由なく他に漏らし、又は窃用してはならない。」とし、監査業務に係る情報漏洩の防止を求めている。また、公認会計士法第 27 条には、公認会計士の義務の一つとして、「公認会計士は、正当な理由がなく、その業務上取り扱つたことについて知り得た秘密を他に漏らし、又は盗用してはならない。公認会計士でなくなつた後であつても、同様とする。」との規定がある。さらに、同法第 34 条の 10 の 16、第 49 条の２において、特定社員、公認会計士の使用人その他の従業者に対しても同様の規定が設けられている。公認会計士、特定社員及び公認会計士の使用人その他の従業者等は、守秘義務を負っていることを再認識しなければならない。

なお、グループ会社、非常勤者、外部の専門家に対しても、守秘義務を求めることが必要であり、そのためには守秘義務に関する契約の締結、情報漏洩のリスクの程度に応じた管理を行うことが必要である。

２．情報漏洩のリスク

公認会計士等は、その業務の実施に当たり、様々な情報に接している。これらの情報の取扱いには従来から細心の注意を払ってきているが、ＰＣや電子メール等の誤操作、移動時の紛失、盗難、マルウェアの感染等により、常に情報漏洩のリスク

がある。

３．情報の不正・私的利用のリスク

公認会計士等が業務で入手した情報は、クライアント等にとって非常に重要な機密情報又は社外秘の情報に当たるものであり、その経済的価値の高いものが多い。そのため、情報の持ち出し等による、不正又は私的利用のリスクが常にある。

４．ＩＴの進歩に対応する情報セキュリティ

クラウドサービス等のＩＴリソースが、ＩＴの進歩により広く普及し、利用されるようになると、新しいリスクが生じ、従来の方法では対応できなくなることがある。したがって、こうしたＩＴの進歩に対応した情報セキュリティ及び体制の見直しを考える必要がある。

また、情報の電子化が進めば進むほど便利さが先に立ち、情報セキュリティの対策を講じずに最新のＩＴを利用してしまいがちであり、このような行為は情報漏洩につながりかねないことを認識しなければならない。

(1) インターネット利用に係る情報セキュリティ

インターネットに接続している状態は、外部から侵入されるリスクが高く、ログオン時のＩＤ、パスワードが盗まれた場合には、正当な権利者になりすましたシステム侵入者が、情報を盗むことが簡単に起こり得る。

パスワードは、他人に推測されないように設定し、定期的又は随時に変更し、パスワードを人目にさらさないなどの対応が必要である。

電子メールの利用に当たっては、誤送信防止やメール本文・添付ファイルの暗号化等の対策が必要である。

(2) クラウドサービス等のＩＴリソース利用に係る情報セキュリティ

自らが保有するにはコスト的にも管理能力の面からも難しいＩＴリソース、例えば、サーバ、グループウェア、事務処理ソフトなどを、使用頻度や使用人数に応じて提供するサービスが増えている。

これらのサービスを利用する際には、情報セキュリティレベルが高い法人向けサービスを利用しなければならない。

また、どんなに情報セキュリティレベルが高いサービスであっても、ログオン時のＩＤ、パスワードが漏洩してしまっては、意味がない。ＩＤ、パスワードの適切な管理を公認会計士事務所（監査法人）側で行わなければならない。

(3) サイバー空間に係る情報セキュリティ

悪意のある第三者が、情報を詐取するために、利用者のＰＣ等にマルウェアを感染させる、偽装したログイン画面を用意してログオン時のＩＤ、パスワードを奪いとる、といった事例が発生している。多くの場合、マルウェアに感染してい

ることやログオン時のＩＤ、パスワードを奪われていることにしばらくの間、気付かない。その結果、情報漏洩が継続し、被害が拡大してしまう。

そのため、ＰＣ等のマルウェア対策ソフトを常に最新の状態に維持するとともに、被害に遭わないための教育研修が重要である。場合によっては、不正な通信が行われていないかをモニタリングすることも考えられる。

(4) インターネット利用以外の情報セキュリティ

ハードディスク（以下「ＨＤ」という。）、ＣＤ－Ｒ、ＵＳＢメモリなどに保存された電子データは、紙媒体の場合に比してコピーが容易であること、漏洩した際の情報量に格段の差があること等により、リスクの性質が異なることになる。そのため、リスクに応じた情報セキュリティ対策を検討する必要がある。

５．紙媒体の情報セキュリティ

監査調書といった業務に関連したものや電子データを印刷した紙媒体の情報は、特別な操作をすることなく内容を見ることができるという特性から、紛失した場合にはそのまま情報漏洩につながる（又は不正利用の）リスクが高い。したがって、電子データばかりでなく紙媒体の情報も、電子データとは別の観点から情報セキュリティの確保に努め、十分な管理体制をとる必要がある。

III　情報漏洩に関するリスクの認識と対応

１．業務の理解、関連する内部統制の識別、リスクの認識

業務に直接関係する情報がどのように管理されているのかについて業務の流れとともにＩＴの利用状況を理解し、関連する内部統制を識別した上で、リスクを認識しなければならない。

なお、サイバー攻撃を受けることによる情報漏洩のリスク、情報を利用できなくなるリスクも併せて検討することが必要である。

また、上記については定期的な見直しが必要である。

２．認識したリスクへの対応

上記で認識したリスクへの対応を検討し、対応すべきリスクについて、当該リスクを発現させない、又は低減させる内部統制を構築し、運用することが必要である。

内部統制の構築に当たっては、予防統制と発見統制の両面の観点から検討を行うことが必要である。

３．環境の変化による一時的なリスク対応の見直し

外部からサイバー攻撃を受けている等、環境が変わった場合は、リスク対応を見直す必要があり、より情報セキュリティを高めた内部統制の運用を一時的に行うこ

とが必要な場合がある。なお、これらの状況が解消された場合は、一時的な内部統制の運用は解除されることになると考えられる。

４．情報の重要度

リスクを認識する際には、情報の重要度を考慮する。

情報について重要度の判定を行うに際しては、通常対象となる情報について、以下の観点から決定する。

・　漏洩による影響
・　消失による影響
・　誤謬による影響

本実務指針では、情報の漏洩（紛失、不正・私的利用を含む。）に焦点を当てているため、原則として上記の重要度に応じた秘密度（取扱いや閲覧をできる度合い）を基本とするのが適当と考えている。

具体的な例としては、以下のものが考えられる。

レベル３（極　秘）：特定の責任者以外の使用を禁止する。
レベル２（秘　密）：業務担当以外の使用を禁止する。
レベル１（社外秘）：社内のみの使用に限定する。
レベル０（公　開）：使用制限なし。

なお、情報はクライアント等の状況や時間の経過などに応じて、その重要度が変化することがある。したがって、定期的に見直す手続が必要である。

５．セキュリティ・ポリシー

情報セキュリティを維持するためには、セキュリティ・ポリシー（情報セキュリティ対策の基本方針）を定めなければならない。セキュリティ・ポリシーでは、前述したリスク認識の結果や情報の重要度に応じて、具体的なアクセス制御などの管理方法を定めることが必要となる。しかし、ただ単にセキュリティの基本方針や細則、ガイドラインやマニュアルといったものを策定しても、実際の運用とかけ離れた「理想的」なものでは意味がなく、現実的なセキュリティ・ポリシーを策定し、運用することが必要である。

セキュリティ・ポリシーの設定は経営者の役割であるが、運用は組織全体で行う必要がある。

情報漏洩、システム停止、データ誤謬のそれぞれのリスクについて検討し、セキュリティ・ポリシーを記述するのが一般的であるが、ここでは公認会計士等の守秘義務の観点から情報漏洩防止を中心に記述する。

なお、状況に応じて見直すことが必要である。

(1) セキュリティ対策

認識しているリスクの程度や情報の重要度に応じて対策を規定し、規定化の程度を検討する必要がある。また、下記の観点から、当該情報（電子メール、電子データ、紙媒体、日常会話など）の使用に当たって留意すべき事項を網羅する必要がある。

・　当該情報を使用、保管する「場所」の管理（建物の仕様、入退出記録、警備など）
・　当該情報を使用する「人」の管理（権限の設定、認証の方法、教育など）
・　当該情報を伝達、保管する「手段、媒体」の管理（ファイルサーバ、暗号化、媒体の保管、通信など）
・　外部ネットワークとの接続の管理（ファイアウォールなど）
・　当該情報の利用状況の管理（情報の利用・持ち出しに関する記録など）

(2) セキュリティ管理体制

セキュリティ管理の実施に当たっては、経営者が最高責任者となる。セキュリティ・ポリシーには管理体制を明確に定める必要があり、例えば、教育、点検、監査についても組織の規模に応じて規定することを検討する。

(3) セキュリティ・ポリシーの構成

セキュリティ・ポリシーは、本人だけでなく職員等の全員が遵守すべき規程となる。規程の構成としては、次の例が挙げられる。

・　セキュリティ・ポリシー（情報セキュリティ対策の基本方針）
・　情報セキュリティ対策基準（重要度に応じたセキュリティ対策の基準を規定化）
・　実施手順書（基準を具体化した実際の運用手順、情報機器やソフトウェアの使用方法についてマニュアル化）

Ⅳ　経営者の役割

１．経営者の役割

経営者とは、公認会計士事務所（監査法人）における所長、理事長等の最高経営責任者等をいう。経営者は、情報漏洩のリスクの適時・適切な把握、必要となる対策の実施を行うことが求められることから、業務上使用する情報を保護するという情報セキュリティマネジメントを経営上の重要課題として捉え、かつ社会的責務でもあることに留意しなければならない。

その責務を果たすためには、まず、経営者が情報セキュリティを重視する意識を持ち、技術的な面（システム面）における対策も重要であるが、実際の態度や行動に反映させることが効果的かつ効率的である場合があることに留意しなければならない。

なお、識別している情報漏洩のリスクの程度、業務上使用する情報の量や重要性

によっては、CISO（情報セキュリティ最高責任者等）やCSIRT（Computer Security Incident Response Team）の設置を検討することが重要である。

情報セキュリティ対策については、情報セキュリティ担当者や利用者が不備を発見し、改善提案を行った場合は、経営者はこれを積極的に取り入れるなど、経営者、情報セキュリティ担当者、利用者が一体となってセキュリティを高めようとする環境を作ることも必要である。

また、情報漏洩は過失のみならず、故意により発生する場合もあることから、経営者は情報セキュリティ対策の立案に当たり、職員等による不正や私的利用を防止・発見する仕組みの導入についても検討する必要がある。

2．情報セキュリティ対策

業務上使用する情報を様々なリスクから守るための情報セキュリティ対策は多岐にわたるが、一般的には以下のような観点からの対策が考えられる。

- 組織的安全対策

  例えば、情報セキュリティ責任者・担当者の任命、情報セキュリティ方針及び関連規程の整備

- 人的安全対策

  例えば、職員等に対する教育研修の実施、情報セキュリティに関する誓約書の入手、情報セキュリティ違反時の罰則に関する規定の制定

- 物理的安全対策

  例えば、業務上使用する情報の保管場所に対する入退出管理の実施、情報機器に対する災害対策装置・備品の設置

- 技術的安全対策

  例えば、情報システムにおけるアクセス制御の実施、マルウェア対策ソフトの導入

- 利用状況監視対策

  例えば、情報持ち出しの監視や防止策の実施、ＰＣの点検、アクセスログの監視・分析の実施

上記に掲げた情報セキュリティ対策は一例であり、画一的なものではない。これらの対策は、事務所や組織の規模・体制などによって異なることから、それぞれの実態に応じた対策を講じることが必要である。その際、クライアント等から公認会計士事務所（監査法人）としての情報管理体制が自社と同等であるかを問われている場合は、クライアント等が考えている情報の重要度に応じ、管理体制を構築することも検討する必要がある。

経営者は、このような情報セキュリティ対策の立案に向けて、組織内におけるセ

キュリティ・ポリシーを策定・整備し、全員へ周知徹底を図り、併せて情報セキュリティ意識を適切なものとするよう措置を講じなければならない。

3．セキュリティ・ポリシーの策定

セキュリティ・ポリシーは、業務上使用する情報や情報システムに対して、どのように取り組み、組織がどのように行動すべきかという全社的なセキュリティの方針について、経営者が明文化したセキュリティに対する「経営方針」ということができる。したがって、「何をどのくらい重視するのか」は、各組織によって異なることとなる。

セキュリティ・ポリシーは、就業規則、各種管理規程と並ぶ「情報」の管理規程であり、これを遵守する以下の４～９に記載するような適切な統制活動が必要である。

4．トップダウンによる周知徹底

経営者は、セキュリティ・ポリシーを決定するだけでなく、自らこの方針を組織内に知らしめ、全ての職員等に対し浸透させる主導的立場にある。セキュリティ・ポリシーを単に策定しただけでは情報セキュリティの実効性がないことに留意しなければならない。

策定したセキュリティ・ポリシーが有効に機能するためには、情報セキュリティ対策を職員等に任せきりにするのではなく、対策の実現に向けて経営者が率先して指揮を取らなければならないし、絶えず情報セキュリティの重要性を訴え続けることが必要である。

5．遵守状況の把握と対策

セキュリティ・ポリシーに基づいてとるべき情報セキュリティ対策が実施され、組織内の情報セキュリティ運用体制が適切に遵守されているかについて、経営者は、適時にモニタリングするとともに、改善すべき点を早期に発見し、是正する役割を担っている。そのためには、例えば、各担当者による自己点検や内部監査を定期的に実施し、問題点や状況の変化を経営者にフィードバックさせる等の方法がある。経営者は、情報セキュリティ担当者や利用者からの意見を考慮しつつ現状を把握した上で、セキュリティ・ポリシーそのものや対策の見直しの必要性を検討し、改善に努めなければならない。

6．情報セキュリティに関する教育研修の実施

セキュリティ･ポリシーを正しく理解し、策定した情報セキュリティ対策に従って組織内部で業務上使用する情報を適切に取り扱うためには、職員等に対する教育

研修が不可欠である。

情報セキュリティは、外部環境・内部環境の動向、ＩＴの進歩などにより絶えず変化するものであることから、教育研修に関しても職員等の採用時、セキュリティ・ポリシーの見直し時など、その他状況の変化に応じて定期的に実施していくことが必要である。すなわち、経営者は教育研修の実施時期・実施方法、研修テーマについて適切に検討の上、効果的な教育研修によって情報セキュリティに対する組織全体の意識を高める役割を担っている。

7．電子メール等による電子データ授受の方針

インターネットや電子メール、また、ＵＳＢメモリといったリムーバブル・メディアの利用によって、大量の電子データが瞬時にして一度にやり取りされている。しかし、一方でネットワーク上での電子データ送信時の不正取得・改竄、ファイル交換ソフトを介した電子データの漏洩又はメールアドレスの宛先違いによる誤送信やＵＳＢメモリの紛失などによる電子データの流出、といったリスクは高い。

経営者は、こうした事態に適切に対処し、漏洩等のリスクを低減させるための方針を電子メール等の利用度合いに応じて定めなければならない。一度の不正アクセスや操作ミスが大規模な情報漏洩につながり、結果的に多大な社会的影響を及ぼす可能性があることに十分留意する必要がある。

8．紙媒体に関する文書管理の方針

監査調書やクライアント等から入手した資料、電子データを印刷した文書等の紙媒体についても、電子データ同様十分な管理体制をとることが必要である。経営者は、こうした紙媒体の紛失や盗難による情報漏洩を防ぐため、利用・保管・移動・廃棄といったそれぞれの局面に応じた文書管理の方針を策定し、組織内において周知徹底を図らなければならない。

9．外部委託先等の管理

情報漏洩は内部の利用者からだけでなく、外部委託先等を通じて発生することが少なからずある。また、内部関係者であっても、雇用形態の違いやグループ会社のような異なる組織の関与などによって生じる情報セキュリティへの意識差異が、情報漏洩のリスクを高める可能性もあることから、経営者は、以下のような状況も視野に入れた上で、対応方法を検討する必要がある。

- 外部専門家の利用
- 外部委託業者の利用
- 非常勤職員による情報の取扱い
- 公認会計士事務所（監査法人）のグループ会社との情報のやり取り

外部のＩＴリソースを利用している場合は、「10．クラウドサービス等の利用の際のリスクの認識と対応」を参照のこと。

10．クラウドサービス等の利用の際のリスクの認識と対応

サーバや業務ソフトなどのＩＴリソースを自ら保有・運用することが管理能力的・コスト的に難しい場合、外部のＩＴリソースを利用することがある。このサービスは、広く一般に提供されているものなど、様々な形態が存在するため、情報漏洩に対する備えも異なっていることが考えられる。

これらのサービスを利用する際には、「Ⅲ　情報漏洩に関するリスクの認識と対応」に従って、リスク認識、リスク対応を行うことになるが、特に以下の点について、十分に検討することが必要である。

(1) リスク認識

外部のＩＴリソースのサービス内容、情報セキュリティに対する考え方、事故発生時の補償、稼働状況などを理解し、利用するとした場合のリスクを認識することが必要である。

法人向けサービスを利用しなければならず、利便性やコストにばかりとらわれることのないように留意が必要である。

(2) リスク対応

多くの場合、公認会計士事務所（監査法人）側で、上記で認識したリスクを発現させない、又は低減させる内部統制を構築することは難しい。そのため、定期的な報告を求めたり、ＩＴ委員会実務指針第７号「受託業務のセキュリティ、可用性、処理のインテグリティ、機密保持及びプライバシーに係る内部統制の保証報告書」などの第三者による評価レポートを入手する等、内部統制の状況を確かめることが必要である。

11．サイバーセキュリティ対応

マルウェア等による情報詐取の事案は増えており、かつ、手口も巧妙さを増している。

この場合でも、「Ⅲ　情報漏洩に関するリスクの認識と対応」に従って、リスク認識、リスク対応を行うことに変わりはないが、特に以下の点について、十分に検討することが必要である。

(1) 職員等向け教育研修の実施状況・内容の確認・見直し

教育研修が不十分であると、情報セキュリティに対する意識が希薄になり、情報漏洩のリスク及びインシデント発生の可能性が非常に高くなると考えられる。そのため、外部環境・内部環境の変化に合わせた教育研修の定期的な実施が必要である。

(2) 内部管理態勢の確認・見直し

公認会計士等が業務に直接関係する情報を適切に管理するためには、経営者、情報セキュリティ担当者及び利用者が、果たすべき役割を正しく認識し、実行することが重要であり、自身の役割の認識が不十分、ないしは、実行できていない場合には、情報漏洩のリスクが非常に高まっていると考えられる。

特にセキュリティ・ポリシーや規程等が正しく、意図されたとおりに運用されているかを、実態に踏み込んで確認することが必要である。

(3) 事案発生時の対応方法の確認・見直し

マルウェア等による情報詐取の事案等が発生した場合の対応方法が職員等に周知され、理解されていることが必要である。周知不足、理解不足の場合、被害を拡大させてしまうことにつながる。

(4) 情報の整理・所在の把握

管理すべき情報が特定され、セキュリティ・ポリシー等に従った管理が行われている必要がある。

これらが実施されていない場合、情報漏洩のリスクが非常に高まっていると考えられ、情報漏洩となった場合、被害状況の把握や情報漏洩の拡大阻止等が行えず、影響は甚大になることが想定される。

(5) 通信記録（ログ）の取得・分析等

マルウェア等に感染したかどうかは、すぐに判明しないこともある。そのため、不正な外部通信が行われていないか、通信記録（ログ）を取得・分析することが有効な場合がある。

なお、マルウェア等に感染した場合は、情報漏洩が発生していないかどうか、通信記録（ログ）を取得・分析することを検討する必要がある。

12. 情報漏洩時の対応

情報漏洩の可能性が生じた場合、当該情報の内容、範囲、原因を把握し、漏洩の拡大を防ぐとともに、当該情報の利害関係者の被害を最小限とする対策が必要となる。そのため、情報漏洩が起きた際の連絡方法（報告先、報告方法を含む。）、体制、対応策などを「緊急時対策」として整理し、連絡方法（報告先、報告方法を含む。）については全職員等に周知徹底しておかなければならない。なお、漏洩した場合に備えて、情報の内容、範囲を迅速かつ正確に把握する方法をあらかじめ検討しておくことも有用である。特に、外部委託業者を利用している場合やグループ会社での情報漏洩の発生時など、自らが直接把握できない場合は注意が必要である。

情報漏洩のリスクを考える場合、その損害額は、直接の損害賠償金額だけでなく、信用の失墜、調査、通知、広報、問合せ窓口等に係る人件費、経費を含めて検討し

ておくことが望まれる。

Ⅴ　情報セキュリティ担当者の役割

１．情報セキュリティ担当者の役割

情報セキュリティ担当者は、経営者の策定したセキュリティ・ポリシーに従って、下記の事項について方針を定め、定めた方針に応じて必要な情報機器の設定を実施することが求められる。さらに、紙媒体の情報の取扱いに関する方針についても定めなければならない。ただし、紙媒体の情報セキュリティ担当者は、電子データの情報セキュリティ担当者と同一の者であることを要しない。

また、情報セキュリティ担当者は、利用者に対して下記の方針の説明を行い、遵守を求める役割を担う。

２．電子データに対するアクセス権限の設定と管理

情報セキュリティ担当者は、経営者が実施したリスク認識の結果に基づき、電子データに対するアクセス権限の設定方針を定めなければならない。また、情報セキュリティ担当者は、その方針に基づいて情報機器の設定を行い、電子データごとにアクセス権限の設定を行わなければならない。

なお、情報機器の設定やアクセス権限の設定は、定期的な棚卸し、人事異動、担当会社の変更等に伴い、見直し・変更を行わなければならない。また、退職者については、そのアクセス権限の削除を速やかに実施しなければならない。

アクセス権限の設定が適切であったとしても、そのアクセスを許可された者（公認会計士事務所（監査法人）の内部者・外部者の区分を問わない。）の不正・私的利用による情報漏洩は起こり得る。したがって、情報セキュリティ担当者は、そのリスクを低減するために、電子データへのアクセスログやＰＣの利用ログ等を分析するなどのモニタリングの導入による抑止力の必要性について、検討しなければならない。

３．パスワードの設定と管理

情報セキュリティ担当者は、パスワードの文字数や使用する文字の種類等のパスワード設定方針と、パスワードの取扱いや有効期限等のパスワード管理方針を定めなければならない。また、情報セキュリティ担当者は、その方針に基づいて情報機器の設定を行うとともに、利用者に対してパスワードの設定方法及び管理方法の遵守を求めなければならない。

４．電子データのバックアップと管理

情報セキュリティ担当者は、情報機器の破損等により電子データが滅失し、業務の継続に大きな障害が発生しないよう、経営者が実施した電子データの重要度分類の結果に基づき、電子データのバックアップ方針を定めなければならない。情報セキュリティ担当者は、その方針に基づいてバックアップを実施するとともに、バックアップを実施した媒体を元の電子データと同様に適切に管理しなければならない。

５．外部ネットワークとの接続管理

情報セキュリティ担当者は、インターネット等の外部ネットワークと事務所のネットワークを接続する場合には、経営者の策定したセキュリティ・ポリシーに従って、外部からの不正アクセスや事務所からの情報漏洩を防ぐために、適切に設定されたファイアウォール等の設置を検討しなければならない。

６．マルウェア対策

情報セキュリティ担当者は、経営者の策定したセキュリティ・ポリシーに従って、業務用ＰＣやサーバ等のコンピュータにマルウェア対策ソフトを導入するとともに、導入後も最新の状態を維持しなければならない。また、経営者の策定したセキュリティ・ポリシーに定めた方法・タイミングに従って、通信記録（ログ）の取得・分析、外部からの侵入を検知するシステムの導入・運用といった対応を行う。

情報セキュリティ担当者は、マルウェア感染が発生した場合には、利用者が直ちに当該ＰＣを事務所のネットワークから切り離すとともに、情報セキュリティ担当者に報告する体制にしなければならない。

ソフトウェアには、不具合が含まれている場合や、悪意のあるソフトウェアが存在し、それらのインストールによりセキュリティ上の欠陥を誘発する可能性があるため、情報セキュリティ担当者は、業務利用目的のＰＣに業務に必要のないソフトウェアをインストールさせないように方針を定め、その方針に従った情報機器の設定を行うとともに利用者へ周知しなければならない。

情報セキュリティ担当者は、ＯＳやソフトウェアにセキュリティ上の欠陥が発見された場合、メーカーによりその対策プログラムが提供されているかどうかの情報に留意することが必要である。これらの対策プログラムが提供されている場合には、対策プログラムを導入することにより既存のソフトウェアに影響がないか検討を行ったのち、利用者に対して対策プログラムの配付とインストールを指示することが必要である。

７．サポート期間が切れたＯＳやソフトウェアの利用禁止

サポート期間が切れたＯＳやソフトウェアは、セキュリティ上の欠陥が発見されても対策プログラムが提供されないことから、利用を停止し、新しいバージョンのものに速やかに移行することが必要である。

８．情報機器に対するセキュリティ対策

情報セキュリティ担当者は、情報機器の紛失や盗難、通信内容の傍受による情報漏洩を防ぐため、暗号化や推測が困難なパスワードを設定するなど、無線ＬＡＮ等のネットワーク機器やＰＣ、ＵＳＢメモリ等の使用に関する方針を定め、機器に備わっているセキュリティの機能を使用するなど、一定レベルのセキュリティを施さなければならない。

９．情報機器やバックアップ媒体の廃棄に当たっての留意点

情報セキュリティ担当者は、廃棄する情報機器に搭載されているＨＤなどの記憶媒体やＣＤ－Ｒなどのバックアップ媒体からの情報漏洩を防ぐため、物理的に破壊する、廃棄は情報セキュリティ担当者が一括して行うなど、情報機器やバックアップ媒体の廃棄に係る適切な方針を定め、利用者に周知しなければならない。

10．電子データ授受の際の留意点

情報セキュリティ担当者は、電子データ授受の際の情報漏洩を防ぐため、授受される電子データに対し、暗号化や推測が困難なパスワードを設定するなどの電子メールやＵＳＢメモリ等による電子データ授受に関する方針を定めなければならない。また、情報セキュリティ担当者は、その方針に基づき情報機器の設定を行うとともに、利用者に対して遵守を求めなければならない。

11．紙媒体の情報セキュリティ上の留意点

情報セキュリティ担当者は、紙媒体の情報漏洩を防ぐため、以下の紙媒体の性質に留意して、利用者による紙媒体の利用、移動、保管及び廃棄に関する方針を定め、利用者に対して遵守を求めなければならない。なお、その際には、電子データに対する情報セキュリティ対策と同様に、不正・私的利用による情報漏洩のリスクも十分に留意する必要がある。

・　技術的なセキュリティを施すよりも、施錠によるアクセス制限や情報持ち出し・回収等の利用状況を監視することによって対応することが効果的かつ効率的である。

・　秘密度が極めて高い情報であっても、通常は暗号化していないため、紙媒体に接することによって当該情報を入手することが可能である。そのため、脆弱な物

理的・人的セキュリティ下においては、電子データ以上の情報漏洩のリスクにさらされている。

12．クラウドサービス等の利用の際の留意点

クラウドサービス等を利用する際には、特に上記２、３、４に従うことが必要である。

Ⅵ　利用者の役割

１．利用者の役割

利用者は経営者の策定したセキュリティ・ポリシーや情報セキュリティ担当者の策定した方針に従うことが必要である。

業務ではＰＣの利用が不可欠になっており、業務中は常に電子データを取り扱っている。業務に関連する情報は、電子データだけでなく紙媒体でも存在する。したがって、利用者は、媒体を問わず、情報を紛失すると情報漏洩の可能性が生じ、関係各所へ重大な影響を与えることを十分認識し、まず、情報の紛失や盗難が生じないよう防止策を施さなければならない。特にＰＣ等を利用する上でのセキュリティ上のリスクを十分認識し、ＰＣ等の管理運用を行うことが必要である。

また、情報セキュリティの維持・向上のために、自ら積極的に行動することが求められる。

２．電子データの管理

(1) 電子データの管理

電子データについては、その紛失や漏洩が発生しないように、決められた運用方針に基づき慎重に取り扱わなければならない。特に電子データを保存した状態でＰＣ等の情報機器を運搬する際には、情報機器の紛失等による電子データの漏洩被害を可能な限り低減させるために、不必要な電子データを情報機器に保存してはならない。また、定期的にＰＣ等の情報機器内の電子データの有無を点検することにより、当座必要でない電子データを事務所等安全な場所に移し、常にＰＣ等情報機器内に保存されている電子データへの意識を高める必要がある。

(2) 個人用ＰＣと業務用ＰＣの区別

業務に関係ない個人利用目的のソフトウェア等をインストールすることにより、セキュリティ上の不具合が生じ、電子データが漏洩する可能性がある。そのため、個人用ＰＣと業務用ＰＣは明確に区別しなければならない。業務に直接関係する電子データを扱うＰＣは、その所有権が個人にあるかどうかにかかわらず、業務用ＰＣとして管理する必要がある。

(3) 電子データの定期的なバックアップ

電子データの滅失等により業務の継続に大きな障害が発生しないよう、ＰＣに保存している電子データについては定期的にバックアップをとることが適当である。

(4) 電子データ保存時の留意事項

電子データは紙媒体の情報と異なり、データ量を意識せず利用する場合が多い。クライアント等から入手した全ての電子データを監査調書等として残すのではなく、入手した電子データを検討して、必要最小限の情報のみを残し、不要な情報は削除する必要がある。

３．パスワードの管理

ＰＣ等情報機器を紛失する場合として、移動途中にカバンごと紛失したり、業務中の離席時に盗難にあうことが想定される。その際、パスワードそのものをメモした手帳が同時に紛失や盗難にあうと、情報が容易に漏洩する可能性がある。不正なパスワードの詐取を防ぐために、パスワードそのものを手帳等にメモしてはならない。

また、経営者の定めた方針に従って、パスワードを設定しなければならない。

４．情報機器の管理

(1) 情報機器の保管

情報機器の紛失・盗難・破損・汚損等の防止に留意し、情報機器を安全に保管することが必要である。

(2) 情報機器の運用

情報機器の紛失や盗難による電子データの漏洩を防ぐため、移動時に情報機器を携帯する場合や、情報機器自体を運搬する場合には、手元から離さない等、正当な注意を払い、情報機器を慎重に管理することが必要である。特にノートＰＣや、ＵＳＢメモリ、外付ＨＤ等のリムーバブル・メディアの情報機器については、可搬性を高めるため、小型軽量に作られていることが多く、紛失や盗難のリスクがより高いため、その保管・携帯方法に十分留意しなければならない。

５．情報機器利用上の留意点

(1) ネットワークへの慎重な接続

一般的に、ネットワーク設備についてはブラックボックス化しており、セキュリティ上のリスクがある。情報機器がネットワーク経由でマルウェアに感染する、情報機器内の電子データがネットワーク上に漏洩・流出するといった可能性があるため、経営者の定めた方針に従うこととし、不用意にネットワークに接続しないよう十分に留意することが必要である。特に無線ＬＡＮについては、有線ＬＡ

N以上にネットワーク形態の自由度が高まっているため、セキュリティ上のリスクが高いことを認識する必要がある。

(2) 電子データの暗号化の実施

特にノートＰＣや、ＵＳＢメモリ、外付ＨＤ等のリムーバブル・メディアの情報機器については、可搬性を高めるため、小型軽量に作られていることが多く、紛失や盗難のリスクが高い。当該情報機器の紛失に伴う電子データの漏洩を防止するため、経営者の定めた方針に従い、ＨＤそのものや、ＨＤ・ＵＳＢメモリ上のデータに対し、暗号化や推測が困難なパスワードを設定しなければならない。

６．電子データ授受の際の留意点

(1) 業務上必要な範囲での電子データの入手

電子データには、その物理的なサイズに比し大量の情報が含まれていることが多く、当該電子データを紛失した場合には、大規模な情報漏洩が発生する可能性がある。また、入手が容易なことから、業務上の必要量以上に電子データを受け取り、結果として未検討資料となる可能性やセキュリティ・ポリシー等で入手しないこととされている情報が含まれる可能性があるため、業務上必要な範囲で当該データの入手を行わなければならない。

(2) 電子メールを利用して電子データの送信を行う場合

電子メールを利用して送信する際には、宛先を誤ることによる情報漏洩を防ぐため、送信前に宛先が正当な受信者であることを確認する。また、電子メールの詐取等による情報漏洩を防ぐため、経営者の定めた方針やクライアント等と合意した方針に従い、送信される電子データに対し、暗号化や推測が困難なパスワードを設定することが必要である。

(3) リムーバブル・メディアを利用して電子データの授受を行う場合

当該電子データをＵＳＢメモリ等のリムーバブル・メディアにて授受する場合には、電子データを保存したままＵＳＢメモリ等を紛失する可能性があるため、経営者の定めた方針やクライアント等と合意した方針に従い、授受される電子データに対し暗号化や推測が困難なパスワードを設定することが必要である。また、同時に、速やかに電子データの授受を行い、ＵＳＢメモリ等から当該データを削除しなければならない。

７．マルウェア対策

(1) マルウェア対策ソフトの利用

業務用ＰＣは、経営者の定めた方針に従い、マルウェア検知用のパターン・ファイルを常に最新版にするなど、最新の状態を維持しなければならない。また、定期的にマルウェアへの感染チェックを行わなければならない。

(2) マルウェアに対する対応

情報セキュリティ担当者等からのマルウェア関連情報に留意し、不審な電子メールを受信した場合や、利用しているＰＣが原因不明で動作が安定しない場合、マルウェア対策ソフトによる通知など、マルウェアに感染した可能性が高い場合には、経営者の定めた方針に従って、直ちにネットワークから当該ＰＣを切り離し、その上で情報セキュリティ担当者に報告し、適切な対策を行わなければならない。

(3) ソフトウェアのセキュリティホール対策

経営者の定めた方針や情報セキュリティ担当者の指示に従い、ＯＳやソフトウェアのセキュリティ対策プログラムを適時にインストールしなければならない。

(4) 用意されたソフトウェア以外のソフトウェアを使用する場合

業務で必要なソフトウェアとしてあらかじめ用意されているもの以外のソフトウェアを使用する場合は、経営者の定めた方針に従う必要がある。

８．紙媒体等の管理

(1) 電子データ以外のセキュリティ対策

紙媒体の情報については、セキュリティ対策を施した電子データと異なり、紙媒体の紛失がそのまま情報漏洩につながることに十分留意し、経営者が定めたセキュリティ・ポリシーに従って慎重に取り扱う必要がある。

(2) 紙媒体等の管理

業務上入手した紙媒体の情報等を収納したカバン等の紛失や盗難、作業現場での紙媒体の放置等により、情報等が漏洩する可能性があるため、十分配慮して、その保管・管理を行うことが必要である。特に公表前の決算書ドラフト等の紙媒体の情報や、クライアント等の入館証等については紛失時の影響が大きいため、極めて慎重に対応することが必要である。

紙媒体の情報等を廃棄する場合には、経営者の定めた方針に従って、情報の重要度に応じた適切な廃棄を行うことが必要である。

(3) 印刷済み電子データの管理

関係者以外の者がアクセスできるプリンタに電子データを印刷した場合には、印刷した紙を放置することによる情報漏洩を防止するため、速やかに印刷した紙の回収を行うことが必要である。

(4) ＦＡＸ資料の管理

ＦＡＸ送信には、宛先誤りによる漏洩を防ぐために、送信前に、宛先に適切な受信者が指定されていることを確認することが必要である。また、受信したＦＡＸについても関係者以外の者がアクセスしないよう、送信者と連携を図り、受信ＦＡＸを速やかに回収することが必要である。

９．クラウドサービス等の利用の際の留意点

クラウドサービス等を利用する際には、公認会計士事務所（監査法人）で導入したサービス以外は利用してはならず、利用に当たっては特に上記２、３に従うことが必要である。

10. ＳＮＳ利用の際の留意点

個人でＳＮＳ（Social Networking Service）を利用するに際し、セキュリティ・ポリシー等に定めがある場合は、それらに従うことが必要である。特に業務に関する事項の書き込み・情報の掲載を行ってはならない。

Ⅶ　発効及び適用

１．本報告は、平成 20 年１月 16 日に発効し、平成 20 年４月１日から適用する。ただし同日前に本報告を適用することを妨げない。本報告の適用をもって、ＩＴ委員会研究報告第 26 号「公認会計士が業務上留意すべき情報セキュリティ」（平成 16 年６月 15 日）及びＩＴ委員会研究報告第 33 号「ＩＴ委員会研究報告第 26 号『公認会計士が業務上留意すべき情報セキュリティ』Ｑ＆Ａについて」（平成 18 年１月 17 日）は廃止する。

２．「ＩＴ委員会報告第４号「業務上取り扱う電子データの漏洩を防ぐセキュリティの指針」の改正について」（平成 22 年３月 19 日）は、平成 22 年７月１日以後開始する事業年度から適用する。

３．「ＩＴ委員会報告第４号「公認会計士業務における情報セキュリティの指針」の改正について」（平成 24 年８月 30 日）は、平成 24 年７月１日以後開始する事業年度から適用する。

４．「ＩＴ委員会実務指針第４号「公認会計士業務における情報セキュリティの指針」の改正について」（平成 28 年７月 25 日）は、平成 28 年７月１日以後開始する事業年度から適用する。

以　上