ＩＴ委員会研究報告第34号

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」Ｑ＆Ａ

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－

１．本研究報告の目的

本研究報告は、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」（以下「ＩＴ実４号」という。）の内容について、Ｑ＆Ａ方式での具体的な解説を提供し会員に理解を深めていただくことを目的として作成した。

「３．Ｑ＆Ａ」については、ＩＴ実４号の項目と対応するように作成しているため、ＩＴ実４号と対応させながら読んで理解を深めていただきたい。

平成21年７月22日にＩＴ担当常務理事から会員・準会員に向けたメッセージが発せられており、その一部をここに抜粋する。会員・準会員は、このメッセージに改めて留意することが重要である。全文は付録４に掲載した。

> 我々が業務で入手した情報が、クライアントにとっては非常に重要な機密情報にあたることは容易に想像でき、その様な重要な情報を紛失し、外部に漏洩し、不正にあるいは私的に利用し、又は、不正あるいは私的に利用するために持ち出した場合には、そのような事態を引き起こした会員あるいは会員事務所のみが公認会計士法や会則違反に問われ信頼性を喪失するにとどまらず、公認会計士業界全体の信頼性すら損ねることになる。我々の業務の前提は信頼性であり、その信頼性にはクライアント情報の取り扱いに関することも含まれていることは言うまでもない。したがって、我々公認会計士には、そのような事態を引き起こさないための「情報セキュリティ」が重要な課題となる。

２．本研究報告における用語の定義

本研究報告において使用する用語の定義は、以下のとおりであり、ＩＴ実４号と同じである。

- 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。
- 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。

３．Ｑ＆Ａ

Ⅰ　はじめに

Ｑ１　平成28年７月25日改正のポイントを教えてください。

Ａ１　平成24年８月30日改正以降のＩＴの進歩を反映させるとともに、所有している情報資産に対する情報漏洩のリスクを中心とした整理から、業務の流れの中で取り扱う情報資産に対する情報漏洩のリスクを中心とした整理に変更しました。

また、クラウドサービス等のＩＴリソース利用やサイバーセキュリティに係る情報セキュリティをＩＴ実４号に記載し、会員各位の対応を促しています。そして、Ｑ＆Ａの内容を大幅に整理しました。

Ｑ２　管理すべき情報としてはいろいろなものがあると思いますが、なぜ、業務に直接関係するものに限定しているのでしょうか。

Ａ２　情報漏洩（紛失、不正・私的利用を含む。）が特に問題となるのは、監査、税務、コンサルティングなど公認会計士が行う業務に直接関係する情報と考えられるからです。しかし、それ以外の情報を管理しなくてよいということではありませんから、公認会計士事務所（監査法人）においては、ＩＴ実４号に準じて管理体制を検討することが適切です。

なお、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」も適用されることに留意してください。

Ｑ３　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」のA53項に電子的な監査調書の管理に関する記載がありますが、ＩＴ実４号との関係を教えてください。

Ａ３　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」のA53項では、電子的な監査調書の管理手続上の留意点も示されています。

A53. 監査調書に関し、機密性、保管の安全性、情報の完全性、アクセス可能性及び検索可能性を確保するため、監査事務所が整備・運用する管理手続には、以下の事項が含まれることがある。

- 電子的な監査調書のアクセスを正当な権限を有する者に制限するための、監査チームのメンバー間で使用するパスワードの設定
- 監査期間中の適切な段階での電子的な監査調書のバックアップ
- 監査開始時に監査チームのメンバーへ監査調書に含まれる必要な情報を提供し、監査実施中に監査調書を管理し、監査終了時に監査調書をファイルに取りまとめるための手続
- 紙媒体の監査調書に対するアクセス管理、配付及び保管を適切に行うための手続

情報漏洩を防ぐ点については、ＩＴ実４号の取扱いと変わるところはないと考えられます。上記のうち、特に一つ目の「電子的な監査調書のアクセスを正当な権限を有する者に制限するための、監査チームのメンバー間で使用するパスワードの設定」について説明を行います。

電子的な監査調書のアクセスを正当な権限を有する者に制限するためには、まず、セキュリティ・ポリシーに基づき決定された秘密度に応じて、電子的な監査調書にアクセスできる人の範囲を決めます。ＩＴ実４号の具体的な分類の例では、監査調書は「レベル２（秘　密）：業務担当以外の使用を禁止する。」に該当すると考えられ、業務担当者は、監査チームメンバーや審査担当者（レビューパートナー）、その他業務上アクセスする必要のある者になると考えられます。したがって、業務担当者以外の社員・職員等が電子的な監査調書にアクセスできないようにする必要があります。

アクセスの制限方法については、公認会計士事務所（監査法人）のセキュリティ・ポリシー等によることとなりますが、例えば、ファイルサーバを用いてクライアント等の電子データを管理している場合には、クライアント等ごとにフォルダが作成されていると思いますので、そのフォルダごとにアクセス権を設定することになると考えられます。

「パスワードの設定」とありますが、これはパスワードを利用してアクセス管理を行うという意味であって、パスワード以外の他の認証方法を用いることも可能です。また、上述したとおり、パスワードでアクセス管理を行う場合、フォルダごとに管理するのか、個々のファイルにパスワードを設定するかは公認会計士事務所（監査法人）のセキュリティ・ポリシーにより決定することになると考えられます。

なお、重要な電子データにアクセスする場合は、個人別の認証方法を検討しなければならないと考えます。

Ｑ４　サイバーセキュリティと情報セキュリティの違いは何ですか。

Ａ４　サイバーセキュリティは、サイバー空間を対象としたセキュリティの考え方です。サイバー空間は各種デバイス、コンピュータ、ネットワークその他の電子化された世界のため、サイバーセキュリティにおいては電子化された情報資産がその保護対象となります。

一方、情報セキュリティはＩＴ実４号でも記載されているように、その範囲を電子の情報に限定しておらず、紙の資料もその対象に含まれます。サイバー空間固有の特徴はあるものの、サイバーセキュリティにのみ特化した対策を行うのではなく、情報セキュリティの一部として検討することが求められます。

Ｑ５　サイバー空間又はサイバーセキュリティ固有の特徴とは何ですか。

Ａ５　大きく以下の４点が挙げられます。

・　情報の機密性のみならず、可用性（使いたい時に適時に使うことができるか）に

関する点が注目されている。

・　自社のみの取組のみならず、取引先や業務委託先、系列企業などシステム上何らかの形でつながっている企業とも連携した取組が求められる。

・　攻撃の標的にされた場合、攻撃者側は効果を上げるまで多様な手段で執拗に攻撃を仕掛けてくる。

・　平常時の対策のみならず、攻撃を受けるなどの異常な状況を感知した場合に緊急時（有事）の対策も強く求められる。

これらは本来、従来の情報セキュリティを管理していく上でもカバーされるべきもので、サイバーの概念によって生じたものではありません。

Ｑ６　サイバーセキュリティ対策を行う上で、全体像を把握するのに適した資料はありますか。

Ａ６　サイバーセキュリティを含む情報セキュリティ全体の考え方については今までどおり、ＩＴ実４号を活用ください。また、サイバーセキュリティ全体の考え方については、経済産業省から平成27年12月28日に公表された「サイバーセキュリティ経営ガイドライン」が経営陣の役割にも触れており、全体像として分かりやすい構成になっています。

また、金融庁から公表されている「金融分野における個人情報保護に関するガイドライン」及び「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」（平成27年７月２日最終改正）等の各種監督指針も参考になります。

Ⅱ　情報セキュリティ管理の重要性

Ｑ７　公認会計士が業務上留意すべき情報セキュリティの問題は、事務所にどのような影響を与えるのでしょうか。

Ａ７　公認会計士が業務で入手した情報は、経済的価値の高いものが多く、特に電子データのような無形資産は、容易に複製することができるため、単なるＰＣの紛失による情報漏洩防止の対策を講じるばかりでなく、不正・私的利用、マルウェア感染等による情報漏洩防止の対策を検討することが重要です。この対策を怠ると、事務所の運営体制見直しによるコスト負担や信用失墜ということばかりでなく、守秘義務違反による業務停止という事態に至る可能性もあります。

Ｑ８　守秘義務の対象となる秘密に該当する情報の範囲は、どのように考えればよいでしょうか。

Ａ８　公認会計士の守秘義務の対象となる秘密とは、公認会計士法第27条に「業務上取り扱つたことについて知り得た秘密」と規定されていることから、業務上取り扱ったこ

とにより知り得た、一般の第三者が知ることができない情報で、相手方が秘密と認識している情報、公表により利害関係者に影響が及ぶと思われる情報等が該当すると考えられます。

なお、「個人情報の保護に関する法律」、「行政手続における特定の個人を識別するための番号の利用等に関する法律」との関係については、それぞれ以下の通達等をご覧ください。

- リサーチ・センター審理情報〔No.22〕「個人情報保護法下の監査業務の実施に当たって」（平成17年３月11日付け公表）
- 自主規制・業務本部 平成27年審理通達第２号「マイナンバー導入後の監査人の留意事項」（平成27年４月22日付け公表）

Q９　公認会計士業務を遂行するに当たり非常勤者等を利用していますが、「情報セキュリティ管理」の面からどのような点に留意したらよいでしょうか。

Ａ９　情報の漏洩事故は、組織内に原因の所在があるばかりでなく、組織外にある場合も多いことから、非常勤の補助者やグループ会社又は外部の専門家等を利用する場合には、情報漏洩のリスクの程度に応じて対策を講じることが重要です。これは、非常勤者等にどのような作業や業務を委託するのかによって、扱う情報も異なりますので、おのずと対策も異なるからです。例えば、非常勤者に常勤者と同じ作業をさせ、扱う情報も同じだとすれば、常勤者と同レベルの対策をとることになると考えられます。

III　情報漏洩に関するリスクの認識と対応

Q10　警備保障会社、清掃業者など職員以外の人が事務所内に立ち入ることがあり、これらの会社とは守秘義務契約などを締結していますが、リスク要因としてどのように考えるのが適切でしょうか。

A10　警備保障会社、清掃業者といった外部業者と各種契約を結ぶことがあります。これらの契約締結時には、守秘義務などに関する条項も盛り込まれるのが通常ですが、契約を結んだだけでは情報漏洩のリスクを低減することはできないと考えます。

これらの契約を締結することにより、警備保障会社、清掃業者以外の第三者へ情報が漏洩するリスクは低減します。例えば、警備保障の契約をしておけば、不審者の侵入による盗難は防げるでしょうし、清掃業者と適切な廃棄方法についての内容を盛り込んだ契約をしておけば、廃棄物から情報が漏洩するリスクは低減します。しかし、依頼者自身が注意を怠ると、十分なリスクの低減は望めません。例えば、ＰＣが施錠されることなく置かれている、重要な書類やＣＤ－Ｒ、ＵＳＢメモリが机の上に置かれたままである、書類がシュレッダーされることなくゴミ箱に捨てられている、といった状況では、悪意のある人であれば、怪しまれることなく持ち出してしまうことが可能となります。

つまり、外部業者といかなる契約締結を行っていても、依頼者自身が情報管理意識

を持って対処することが重要です。

Q11　情報漏洩に関するリスクの認識と対応は、具体的にどのように行えばよいでしょうか。

A11　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を業務の流れとＩＴの利用状況に沿って理解し、関連する内部統制を識別した上で、リスクを認識し、リスク対応策を実施します。

例えば、クライアント等と資料のやり取りを電子メールで行う場合、メールの宛先の選択、ファイルの添付、メール本文の記載、送信ボタンのクリックといった流れがありますが、それぞれの場面でどのような内部統制が行われているかを識別します。メールの宛先の選択であれば、オートコンプリートを使用しないルールにしている、ファイルを添付する場合はクライアント等と合意したパスワードを設定する、メール本文に重要情報は記載しないルールにしている、等の内部統制を識別します。その上で、オートコンプリート使用禁止の設定がされていないことにより誤送信するリスク、パスワードを設定しないまま送信するリスク、といったリスクを認識します。これらを受けて、リスク対応策として、メールの設定でオートコンプリートを使用しない設定に変更しポリシーで変更を許可しないようにする、外部アドレスに添付ファイルを送る場合は自動で暗号化し、パスワードを別メールで自動的に送る仕組みを導入するなどのリスク対応策をとります。

業務の局面におけるリスクとリスク対応例の参考資料を付録２に掲載しましたので、参考にしてください。

Q12　IoT（Internet of Things）の動向について、情報セキュリティ管理上どのような点を考慮しておけばよいでしょうか。

A12　これまで外部との通信を行う主体は、コンピュータなどの情報・通信機器が主なものでした。情報処理機能や通信機能の高機能化、低価格化が進むことで、様々なものに通信機能が付加されることにより、自動認識や自動制御、遠隔計測などを行うことが可能になることがモノのインターネット（IoT）です。IoTが進んでいくことで便利になる一方、情報セキュリティの面からは管理対象が増加し、その特性上、情報セキュリティリスクが顕在化しやすくなる状況にあると言えます。

具体的な特性としては、２点あります。１点目は、その管理が意識から漏れやすい点です。総務部門で管理しているネットワークプリンタ、通信機能を有した監視カメラ、入退室の管理機器、人事部所管の出社退社情報（タイムカード関連の機器）など、従前情報システム部門が管理していなかった部署がこれらの機器を管理していることが挙げられます。これらの部門の情報セキュリティ意識が高くない場合、機器のセキュリティ設定を出荷（初期）状態のまま稼働をさせたり、社外から見える設定にしてしまったりと社内の情報セキュリティリスクが高まることになります。

２点目はモニタリングの困難さです。IoT機器も他の情報通信機器同様にセキュリティ対策とそのモニタリングが必要ではあるものの、対策及び監視方法はまだ発展途上の段階にあります。そのような状況ではありますが、これらの対策を怠った場合、自社の情報セキュリティ上問題が生じるのみならず、他社へのDDoS攻撃などの踏み台として使われることにもつながるため留意してください。

Ⅳ　経営者の役割

Q13　情報セキュリティ対策に対する経営者としての役割を果たす上で、特に留意すべき点はありますか。

A13　事務所の経営者として特に留意すべき点は、情報セキュリティ対策の重要性を認識し、率先して実際の行動に反映する意識が重要であるという点です。

また、情報セキュリティは、組織全体として対応する必要性があることから、情報セキュリティを重視する組織風土を醸成することが重要です。

そのためには、情報セキュリティに関する経営者の基本方針として、セキュリティ・ポリシーを策定・表明し、組織内外の環境変化に応じて見直すことが重要です。

その契機としては、例えば、情報セキュリティ担当者や職員等が発見した情報セキュリティ対策に関する問題点を率直に聞き入れ、その改善提案を、積極的に取り入れることなどが挙げられます。また、このような態度を示すことは、職員等が事務所の方針に従い、「やらされている」という感覚を緩和することが期待できると同時に、事務所全体で情報セキュリティに取り組もうとする機運を高める効果が期待できます。

サイバーセキュリティに関連した領域においては、自社のネットワーク上の動きやセキュリティの監視を行うSOC（Security Operation Center）機能や、CSIRT（Computer Security Incident Response Team）機能などを自組織の中でどのように担保するか、組織の基本方針決定と体制構築の監督（及び基本方針の見直し）が重要です。

なお、セキュリティ・ポリシーの例示を付録１に掲載しますので、参考にしてください。

Q14　一時的に情報セキュリティを高めた内部統制の運用を限定的に行うという点で、特に留意すべき点は何でしょうか。

A14　外部からサイバー攻撃等を受けている等、緊急時に備えるためには、経営者が警戒心を発揮し、組織内外に対して適時に情報発信できる管理態勢へ移行する仕組みを検討することが重要です。

そのためには、経営者の権限に基づく適切な人材の配置、権限と責任及び情報伝達経路の明確化、緊急時を想定した訓練等が重要と考えられます。

また、緊急時の管理態勢への移行のタイミングとしましては、セキュリティインシデント(例えば、不審なアクセスやスパムメールなど）を検知した場合などが考えられますが、組織においてセキュリティインシデントを明確に定義しておくことが重要で

す。

Q15　どのようにしたら情報セキュリティの意識を職員全員が持つようになりますか。

A15　職員等に対し、情報の取扱いに関する機密保持の誓約書を採用時や毎年提出してもらうことや、万が一漏洩事故を起こした場合の罰則について就業規則に定めておくことにより、抑止効果を通じて情報セキュリティの重要性を認識してもらうという方法が挙げられます。

　また、定期的かつ実効的な教育研修を通じ、仮に情報漏洩が発生した場合や外部からサイバー攻撃を受けた場合に、組織や活動にどのような影響が生じるのかについて周知及び討論する方法などが挙げられます。

Q16　複数の公認会計士と共同で業務を行っています。このとき、電子データの管理方針は、どのようにしたらよいでしょうか。

A16　事務所に所属していない複数の公認会計士と共同で業務を行う場合、ＰＣが貸与されないことが多いと思われますので、各自のＰＣで作業を行うことから作成された電子データがそれぞれのＰＣの中に保存されることになります。そのため、電子データの一元管理ができないだけでなく、各自のＰＣのセキュリティの程度が分からないことから、漏洩のリスクも高まることになります。

　経営者としては、このような場合の管理方針を定めることが重要です。例えば、業務に使用するＰＣのセキュリティのレベルを統一するように求め、業務終了時には各自のＰＣには電子データを残さず、全て回収する、といったことや、Q18に示すクラウドサービスを利用すること等が考えられます。

Q17　「９．外部委託先等の管理」とありますが、具体的にどのような点に留意して対策を行えばよいでしょうか。

A17　外部委託先等（外部の専門家、外部委託業者、非常勤職員、グループ会社、外部のＩＴリソース等）の管理に当たっては、公認会計士事務所（監査法人）が組織内部において実施している各種安全対策を踏まえ、具体的には、以下のような対策を行うことが一例として考えられます。

・　外部委託業者や外部の専門家又はグループ会社を利用するに当たっては、情報の取扱いに関して契約書の中に機密保持の条項を明確に織り込む、又は機密保持の覚書や守秘義務の誓約書等を別途取り交わす。
・　外部委託業者、外部の専門家又はグループ会社の安全管理状況について、契約締結前や締結後に適宜確認を行い、情報セキュリティの管理状況を把握する。
・　外部のＩＴリソースを利用する場合には、受託会社のセキュリティ管理状況の評価を適切に実施するために、定期的な報告を求めたり、第三者による評価レポート

を入手して検討する。

・　グループ会社における情報セキュリティ研修については、公認会計士事務所（監査法人）と共同で実施し、情報セキュリティに対する意識を同一レベルに合わせる。

・　非常勤職員については、情報を取り扱う頻度に応じてＰＣの貸与又は利用を制限する。また、情報セキュリティに関する教育研修についても漏れなく実施する。

Q18　事務所内にサーバを設置して管理していくことができず、メールやスケジュール管理を始め、インターネットストレージなどのクラウドサービスを利用していますが、その際の留意点を教えてください。

A18　メールやインターネットストレージといったクラウドサービスを利用する場合、業務に直接関係する情報もクラウドサービス上で取り扱うことになるため、クラウドサービス利用に伴うリスクを検討することが重要です。例えば、インターネットストレージは、インターネットを経由して自由に読み書きが可能な、外部に保管されているＨＤのことで、提供されるサービスの内容、セキュリティの程度、使用（保管）できるＨＤの容量など様々ですが、以下の②に記載しているようなリスクに対応可能なクラウドサービス事業者を選ぶことが重要です。

①　インターネットストレージの利点

・　インターネット接続環境さえ整っていれば、時間と場所を選ばずにアクセスできる。

・　適切な業者の提供するサービスを利用することで、ユーザ自身がＨＤ等を所有するよりもセキュリティの高い環境を実現できる（事業継続計画（ＢＣＰ）対策や税理士事務所を併設している場合の情報分離対策など）。

②　導入した場合の考えられるリスク

・　インターネットに接続できる端末があればどこからでもアクセス可能である。

・　ユーザ自身が物理的にＨＤを保有しない（できない）ため、ＨＤの物理的なコントロール権限（サーバへの取付け、取外し、使用後の破壊処理等の権限）がユーザ側にない。

・　ＨＤへの論理的なコントロール権限やアクセス制限について、ＨＤを管理する会社の定めるポリシーや、社会的（法規制等）又は環境的（天災、通信回線の断絶）な影響で制限を受ける可能性がある。

・　サービス提供業者の都合でサービスを利用できない事態が生じる場合（例えば、サーバメンテナンス等によるサービスの停止時等）、業務継続が困難になる可能性がある。

・　クラウドサービスの利用契約によっては、一つのＨＤを複数の契約者が共用している場合があり、他のユーザの管理不備によって障害や情報漏洩が引き起こされる可能性がある。

・　暗号化通信に対応していないサービスを提供している事業者や、クラウドサービス事業者内の経路（例えば、メインサーバとバックアップサーバとの間の通信）で

は暗号化通信を行っていない場合があり、暗号化されない通信については、内容が外部に知られてしまう可能性がある。

クラウドサービスは、上記①の利点を有することから、適切な利用を行えば業務の効率化にとって有用なものとなりますが、②のリスクとして考えられる点を考慮しなければ、セキュリティ面での不安が生じます。セキュリティ面での事故が起こった場合に生じる信用低下、損害賠償等のリスクの大きさを考えると、業務に直接関係する情報をクラウドサービスで扱う際には、効率性やコストよりもセキュリティ面を優先して、利用するサービスを選定すべきと考えます。

これらを踏まえて、クラウドサービスの導入に際してリスクへの対応をどのようにするのかを検討するとともに、導入後においても定期的にリスクの内容や発生可能性等を見直し、対応についても検討し直すことが重要です。

Q19　ファイルサーバとしてクラウドサービスを利用している場合、業務に直接関係する情報を保存する際の留意点を教えてください。

A19　クラウドサービスに業務に直接関係する情報を保存する場合、まず保存する情報の範囲と取扱いルールを検討し、明確化することが重要です。

情報の性質や重要度を考慮して、クラウドサービスに情報を保存して問題がないか検討することが重要ですし、例えば、ＩＴ実４号の「Ⅲ 情報漏洩に関するリスクの認識と対応」で例示しているレベル３（極　秘）の情報など、特に重要な情報を外部に預けないように範囲を区切ってクラウドサービスを活用することや、監査調書や監査調書の基となる情報の保存に当たり事務所内にサーバを設置して保存する場合のリスクと比較考量することも検討に値します。保存する情報に個人情報が含まれる場合には、状況により個人情報保護法に基づく適切な委託先に対する監督義務が生じることも考えられます。

情報の重要度については、その情報が失われた場合、又は漏洩した場合における信用の失墜、顧客の喪失等の影響を十分考慮することが重要です。

また、クラウドサービス事業者によっては、データセンターが海外にある場合もあります。あらかじめデータセンターの所在地における法規の適用に係る問題を認識して、現地の法執行機関による情報の差押えなどのリスクを受容するか否かの検討を行うことも重要です。

情報をクラウドサービスに保存する際の取扱いルールを定めるとともに、当該ルールが公認会計士事務所（監査法人）のセキュリティ・ポリシーやその他の規程、ＩＴ実４号で要求される事項を満たすことを確かめます。

公認会計士事務所（監査法人）のセキュリティ・ポリシーやその他の規程で、公認会計士事務所（監査法人）外に情報を置くことを禁止していたり、外部委託に関する制限をしていたりすると、クラウドサービスの利用が難しくなる場合もあります。また、公認会計士事務所（監査法人）とそのクライアントとの契約等によって制約を受ける場合も考えられます。それらの場合には、規程を実態に整合させるよう、規程の

見直しを行うことが重要です。

いずれにせよ、クラウドサービスの利用時に起き得るトラブルに伴って想定されるリスクが、業務の上で許容される範囲内に抑えられることを確認した上で、クラウドサービスを利用することが重要です。

さらに、サービスの停止やクラウドサービス上に保存した情報が失われた場合でも業務の継続が可能なように、また、情報の喪失に伴う影響を大きくしないために、適切な間隔でクラウドサービス外に情報のバックアップ（複製）を定期的に取ること及び情報の保管期限を適切に定めることも重要です。

Q20　サイバーセキュリティ対策を行う上で特に対処しなくてはいけないポイントはなんでしょうか。

A20　経済産業省が平成27年12月28日に公表した「サイバーセキュリティ経営ガイドライン」では、経営陣の関与が強調されています。サイバーセキュリティリスクを経営リスクの一環として捉え、経営者自身がその対策に能動的に取り組むべき（リーダーシップ）と触れられています。ヒト・モノ・カネといったリソースをセキュリティ領域に配分することが経営陣に求められます。会員各位におかれては、「「今般の日本年金機構における個人情報流出事案を踏まえた金融庁からの要請について」（平成 27 年６月 30 日 会長周知文書）に関する会員各位の対応について（お知らせ）」（平成27年12月14日）（付録３参照）を踏まえた対応が重要です。

Q21　サイバーセキュリティ対策を行う人材が不足しています。外部リソースの活用を考えていますが、留意すべき点はありますか。

A21　サイバーセキュリティの全ての対策を自組織の人材にて賄うのは、技術的にもコスト的にも難しい場合があり、外部リソースの活用を検討することは合理的な考え方と言えます。一方で、技術的に理解しづらく、その活動内容についての評価が難しい領域であることから、その活動がブラックボックス化し、外部リソースに全て任せてしまうケースも見受けられますが、サイバーセキュリティは自らが積極的に取り組むべきものという意識を持って、外部リソースを適切に管理することが重要です。

一般的に外部リソースを活用する可能性が高い領域は、以下のような技術的又は非定常的な分野が想定されます。

- セキュリティの外部監査
- 技術的な対策の整備
- 社内研修の実施
- 継続的なモニタリングの実施（SOC機能を含む。）
- 一時的にセキュリティを高めた内部統制の運用実施
- 非常時（緊急時）の技術的対応及び外部説明に関わる事前準備・実践対応（SOC機能を含む。）

Ⅴ　情報セキュリティ担当者の役割

Q22　ＰＣやネットワーク機器の設定について留意すべき事項を教えてください。

A22　まずはＰＣやネットワーク機器に備わっているセキュリティ機能を利用します。またＰＣに限らず、業務にスマートフォンやタブレット端末等を利用する場合にも、同様の管理を実施します。さらに、近年、ＰＣ等の情報機器だけでなく、複合機など様々な機器に通信機能を持たせていることがあります（IoT）。このような場合には、外部から機器内部に記憶されている情報を閲覧等されないように、適切な設定を実施することが重要です。

①　ＰＣの設定

・　特殊な権限を持っているAdministratorを利用できない設定にする。

・　Windowsに標準で用意されているファイアウォール等のセキュリティ機能を有効にする。

・　ＰＣ起動時にパスワードが必要となる設定にする。

・　Windowsログイン時にパスワードが必要となる設定にする。

・　スクリーンセイバーを使用し、復帰時にパスワード入力画面を表示させる設定にする。

・　暗号化ソフトにより、ＨＤの暗号化を行う。

・　マルウェア対策ソフトを導入する。

②　ネットワークの設定

・　有線LANを利用する場合、セキュリティ機能が充実しているルーターを使用する。

・　無線LANを利用する場合、機器に備わっているセキュリティ機能を活用する。

③　サーバの設置

レンタルサーバを利用する際には、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」（以下「ＩＴ実７号」という。）などの第三者による評価レポートを入手することにより、レンタルサーバのサービスを提供しているサーバ会社がセキュリティに対して適切な体制を整えているかをチェックする。

④　パスワードの設定

・　他人に推測されにくく、機械的な処理で割り出しにくいパスワードのルール設定を行う。

・　定期的にパスワードを変更する設定を行う。

・　同じパスワードを数世代、使えない設定にする。

⑤　その他

・　情報・通信機器以外でもネットワークへの接続や電話回線を利用した通信を行う機器が導入される場合、その形態・取り扱う情報などリスクに応じた初期設定を行う。

Q23　ノートＰＣ等からの情報漏洩を避ける、日常的な防止策にはどのようなものがありますか。

A23　以下のような防止策が考えられます。

①　ＰＣの利用

・　ノートＰＣに保管する電子データは最小限とし、不急のものは事務所のファイルサーバに保存する。

・　電子データごとにパスワードを設定する。

・　ＵＳＢメモリは、事務所所有のもののみを利用可とし、業務専用とした上で暗号化ソフトを使用する。

・　セキュリティが不透明な外部ストレージサービスは利用しない。

・　Windowsやワープロ・表計算ソフトの不具合を修正するソフト（パッチ）を適時に適用する。

・　サポート期限の切れたＯＳやソフトウェアを利用しない。

・　マルウェア対策ソフトを常に最新版に更新する。

・　業務に不必要なソフトウェアをインストールしたり、ウェブサイトにアクセスしたりしない。

・　不正・私的利用に対するモニタリングを実施する。

・　必要に応じてＩＤの棚卸しを実施する。

②　ネットワークの利用

・　非常勤者のＰＣや私用のＰＣは、事務所のネットワークに接続しないルールにする。

・　外出先で公衆無線LANは利用しない。

③　サーバの利用

・　ファイルサーバは、鍵のかかる部屋等の中に設置する。

④　パスワードの利用

・　パスワードを付箋に書き留め、ＰＣに貼ったりしない。

・　パスワードをソフトウェア等に記憶させない。

Q24　マルウェア対策を実施する上での留意点を教えてください。

A24　マルウェアから防御するためには、全てのＰＣ・サーバにマルウェア対策ソフトを導入するとともに、常に最新の状態に維持されるようにします。そのため、情報セキュリティ担当者は、全てのＰＣにおいてパターン・ファイルの更新の設定が正しく行われるよう留意してください。

また、公認会計士事務所（監査法人）として一元的にマルウェアの進入口の防御を行うことも重要です。例えば、メールサーバ用のマルウェア対策ソフトをインストールすることで、外部との電子メールの送受信の段階でマルウェアを除去することがで

きます。

さらに、信用できないウェブサイトは閲覧しないようにする、不明な内容の添付ファイルは開かないようにするなどの基本的な防衛策を利用者に対して周知するとともに、業務に必要な安全なソフトウェアのみをＰＣにインストールされるように、インストール権限を情報セキュリティ担当者のみに設定するなどの対策が考えられます。

Q25　サイバー攻撃に対して、どのような準備と対応が考えられますか。

A25　マルウェア対策も有効ですが、これだけでは未知のマルウェアに感染すると被害を食い止めることができません。マルウェア対策ソフトやファイアウォールなど、一つのソフトウェアや機器に依存するのではなく、全体としての対策を心掛け、侵入→感染→拡大という攻撃フェーズに応じた拡大防止策及び緩和を図ることのできる柔軟な対策の実施が考えられます。また、不正な通信の発生を検知するために、通信記録（ログ）を取得・分析することが有効な場合があります。

Q26　情報が漏洩してしまう可能性が高まった場合に備えて、準備しておくことはありますか。

A26　緊急時の対応体制や対応手順が決められていない場合、影響範囲や損害を特定することが遅れ、結果として被害が拡大し、公認会計士事務所（監査法人）の社会的責任の追及や訴訟、信用の失墜につながるおそれがあります。そこで、ＰＣの紛失等、情報漏洩が発生する可能性が高まった際の、経営者への報告手順や初動対応の内容、通常業務への復帰手順などを定めておくことが望まれます。

①　マルウェア感染が発生した場合

感染したＰＣを事務所内のネットワークから切り離した上で、当該ＰＣからのマルウェア駆除を実施するとともに、他のＰＣへの感染状況を確認するなど、被害を最小限にとどめることが重要です。そのため、マルウェア感染が発生した場合には、利用者が直ちに情報セキュリティ担当者に報告する仕組みを周知しておくことが重要です。

②　標的型メールが届いた場合

巧妙な標的型メールを誰かが開いてしまうことは避けられないことと認識した上で、影響範囲や損害を特定し、正常化に着手できる準備や手順を用意しておくことが重要です。感染したＰＣが残存している場合、再度情報漏洩等が発生し、事態が長期化するおそれがあります。感染したＰＣの調査など、事務所内だけでは技術的に対応が困難なものについては、外部の専門家を利用することもあらかじめ想定してください。

Q27　ファイルサーバとしてクラウドサービスを利用する場合に、業者を選ぶ際の留意点を教えてください。

A27　クラウドサービスを利用した場合であっても、情報セキュリティの観点からの責任を全てクラウドサービス事業者に委譲することはできませんが、システム自体の更新や保守から解放されるため、適切なクラウドサービス事業者のサービスを選択しモニタリングすることによって、自らがサーバを運用するよりもセキュリティの向上・維持が容易になる可能性があります。このためには、適切な委託先選定と定期的な委託先評価を行うことが重要です。特にＩＴは日々進化しているため、継続的に評価を行うことによって、リスク評価をアップデートするだけでなく、適当な提供価格であるかどうかも見直すことができます。

個人向けのサービスを利用しないのは当然ですが、委託先選定に当たっては、情報セキュリティ対策、サービスの稼働状況、利用者サポート体制、契約終了時のデータの取扱い、事業者の事業継続性についても考慮することが重要です。具体的な留意点としては以下の事項が考えられます。

（情報セキュリティ対策）

以下の項目について、ネットワークを含むシステムとデータ管理に関するセキュリティ対策の説明を受け、検討します。

- ＯＳやアプリケーションに対するセキュリティパッチやアップデートの状況
- サーバやネットワークの多重化・冗長化の状況
- データの管理体制とバックアップの状況
- 暗号化の状況
- ウィルス等のマルウェア対策の状況
- 不正アクセス対策の状況
- 障害や攻撃に対する対策の状況
- データセンターの災害対応と防犯・入退室管理などの監視体制の状況
- データセンターの運用に関する要員の信頼性とアクセス管理・管理者特権や操作ログの管理状況
- 再委託先の有無、その管理体制の状況
- サービス提供に関する定期的な報告（月次報告等）の状況
- 第三者による認証や評価報告書の取得の有無（ＩＳＭＳ、ＩＴＳＭＳ、ＢＣＭＳ、Ｐマーク、ＡＳＰ・ＳａａＳ認定サービス、ＩＴ実７号等）

（サービスの稼働状況）

サービスの利用可能時間が業務上の条件に合致しているかどうか確かめます。システムが障害に強いかどうか、障害が発生した場合やメンテナンスによる停止時間が許容できるかどうかについて過去の実績等の説明を受け、検討します。

（利用者サポート体制）

サービスの使い方が分からないときにどのような支援が提供されるか確かめます。ヘルプデスクがある場合にサービス提供日と時間帯は適当か、サービス提供事業者が遠隔地であった場合に電話やメールで十分なコミュニケーションができるかについて検討を行います。

（契約終了時のデータの取扱い）

サービス利用を終了する場合、データを自らのシステムや他の事業者に移行することになるため、必要なタイミングでデータが返却されるか、その転送スピードは十分か、データ形式は他のシステムでも受入れ可能な形式かどうか、返却後はクラウドサービス事業者のシステムから確実に消去されるのかについて検討を行います。

（事業者の事業継続性）

事業者が何らかの理由によってサービス提供を停止する、又は事業継続が困難になった場合にはサービスが利用できなくなるばかりではなく、データが消失する可能性もあります。したがって、事業基盤がしっかりした事業者かどうか検討を行います。また、万一に備えて自らデータのバックアップを保有するかどうかについても検討を行います。

委託先からの月次報告は情報セキュリティ担当者が受領し、運営状況について問題が発生していないかどうかを確かめます。その上で、例えば、１年経過後に定期的な委託先評価を行う場合は、理想的には品質評価基準等を策定して臨むべきものと考えられますが、委託先選定時に検討した事項を再度簡便に確かめるだけでも効果があります。

この際、評価期間に発生した問題点を内容と程度に応じて分類し、取りまとめておけば、より具体的な評価ができると考えられますので、情報セキュリティ担当者に情報が集まるような仕組みを作っておくと便利です。例えば、ヘルプデスクに問い合わせる場合には、情報セキュリティ担当者が一元的に行う（パスワードを忘れた等の各人の問題は除く。）、メールであれば必ず情報セキュリティ担当者をＣＣ：に入れる運用にするなど、それぞれの事務所の体制や規模に合わせて工夫することが考えられます。

また、委託先を評価するに当たってはService Organization Control (SOC) レポートを入手することも有効です。SOCレポートのうちＩＴ実７号やSOC2は、委託先のセキュリティ、可用性、処理のインテグリティ、機密保持又はプライバシーに関する独立第三者による保証報告書です。これまで述べてきたような種々の評価を実際に委託先に対して行うことは困難なこともあり得ます。そのような場合、ＩＴ実７号やSOC2を入手し、その内容を事務所のセキュリティ・ポリシーに照らして十分な水準にあるかどうかを確認することで評価するという方法も検討することが考えられます。

Q28　ファイルサーバとしてクラウドサービスを利用する場合、クラウドサービス事業者と契約を結ぶ際の留意点を教えてください。

A28　クラウドサービスは、メンテナンスや障害のために、予告して、又は突然停止することがあります。その対策方針等は、ＳＬＡ（サービス・レベル・アグリーメント、又はサービスレベル契約書）・約款等において確認しておくことが重要です。

具体的には、以下のような項目が挙げられます。

・　サービスの稼働率、障害発生頻度、障害時の復旧時間などのサービスレベルは示されているか。
・　混雑時にアクセスが極端に遅くなる等の障害が生じないよう対策を講じてあるか。
・　委託元による委託先への監査権の有無
・　データセンターサイトの公開、非公開（サイトは国内か海外か）
・　バックアップ管理の状況
・　契約の解除に関する規定（事業者側が一方的に解除できる条件でないか、ユーザ側が解除する場合のペナルティ等はないか、等）
・　サービス停止時・終了時にデータが必要なタイミングで返却されるか（又は適切な間隔でクラウドサービス外に情報のバックアップ（複製）を定期的に取ることが可能か）。

利用するサービスによっては、契約に当たって、ユーザが「同意」のボタンを押すケースも考えられますが、安易に同意せずに利用規約等の内容を確認した上で押すように留意してください。

なお、契約の更新や見直しについて、１年ごとなどの定期的な頻度でサービスレベルや制約事項、コスト等につき検討を行うといった対応も考えられます。

Q29　ファイルサーバとしてクラウドサービスを利用する際のユーザ管理の留意点を教えてください。

A29　ファイルサーバとしてクラウドサービスを利用する際にも、ユーザを適切に管理することが重要です。誰でも自由にサービスを利用できるようにするのではなく、事務所で想定するアクセス権限に応じ、利用できる人とその権限を定めて管理を行うことが重要です。クラウドサービスの中には、ユーザ管理やアクセス制限が困難なものもあります。アクセス制限が管理できるクラウドサービスを利用することが重要と考えます。

具体的な留意点としては、以下の事項が考えられます。

・　利用できる権限者のみを登録する。
・　利用者について、アクセスできる情報の権限管理を行う。
・　複数人でＩＤ・パスワードを共有しない。
・　事務所のパスワードポリシーに則したパスワードを設定する（複雑性・定期的な変更等）。

・　電子証明書の導入によってアクセスできる端末を制限する。
・　管理者アカウントを用意し、定期的にモニタリングを行う（ルールどおりの運用が行われているか、ＩＤが不当に追加されていないか等）。
・　退職した利用者のＩＤなど、不要となったＩＤは削除する。

Ⅵ　利用者の役割

Q30　事務所のセキュリティ・ポリシーに従って業務を行っていれば、大丈夫でしょうか。

A30　近年、マルウェア対策ソフトでも十分に検知できないマルウェアを、標的型メールを使って送付する等、非常に手の込んだ攻撃を行う事例が散見されます。これらの攻撃は、セキュリティ・ポリシーに基づくシステム的な防御策を行っても、防ぎきれるものではありません。したがって、所属する会社・組織の対策のみに依存するだけではなく、情報機器を取り扱う全ての者がセキュリティに対する意識を高く持ち、セキュリティに関する情報や知識を積み重ねて、自ら防御することが最も重要です。

なお、セキュリティ対策全般に関する情報源として、一般に向けて公表されているウェブサイト等では、以下のようなものがあります。

・　総務省：「国民のための情報セキュリティサイト」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
・　IPA 独立行政法人 情報処理推進機構：「情報セキュリティ」のページ
http://www.ipa.go.jp/security/

これらのサイトでは、セキュリティ対策の例や、実際に発生したセキュリティ事故の事例等も確認することができます。

上記は主に情報セキュリティ全般に関する情報を提供していますが、個別のソフトウェアに関するセキュリティ情報については、ＯＳやソフトの販売元（ベンダー）のサイトや、当該ソフト（ＳＮＳや無料コミュニケーションアプリ等も含む。）の開発元のサイト、又はマルウェア対策ソフトの販売元のサイト等で確認することができます。

また、日本公認会計士協会のウェブサイトでも、セキュリティ対策に関する基礎情報が確認できるサイトを用意しています。
https://www.hp.jicpa.or.jp/n_member/security/

Q31　セキュリティ対策の基本として知っておくべきものにはどのようなものがありますか。

A31　セキュリティ対策の基本的なものとしては以下のようなものが考えられます。

①　情報機器（ＰＣ、スマートフォン等）の利用に際して留意すべき事項
・　端末（ＰＣ等）に大量のデータを保管したまま持ち歩かない。
・　公衆無線ＬＡＮ等のパブリックなネットワークに接続してデータの送受信を行

わない。

・　不特定多数の者が利用できる端末を使って、重要なデータ等のやり取りを行わない。

・　個人で所有している端末を、勝手に業務用途に持ち込まない。

・　情報を記録する媒体（ＵＳＢメモリ等）にはセキュリティ対策（パスワード設定等）が施されたものを使う。

・　各種情報（端末、媒体、サーバ等）にアクセスする際のパスワードを、紙に書いて保管をしない。

・　端末を持ち歩く際は、端末の電源を切る等ロックをかけた上で、常に自分の目の届くところで保持する。

・　重要な情報をメールでやり取りする際は、暗号化した上で送信する。

・　業務用端末には不必要なソフトをインストールしない。

②　書類の取扱いに際して留意すべき事項

・　プリンタで印刷した書類をそのままにしない。

・　席を離れる際には、重要な書類が散逸しないように片付ける。

・　持ち歩く際は、カバン等に入れて、常に自分の目の届くところで保持する。また、不必要な書類は持ち歩かない。

・　書類を補完する際は、事務所で定めたルールに基づき、ロックのかかる書棚等に保存する。

・　機密書類を処分する際にはシュレッダーにかけるか、専門の業者に依頼して裁断する等、情報が他者に読み取られないように留意する。

なお、上記の対策はごく基本的なものです。技術の進歩により、必要となる対策は日々変わってきます。また、現時点では有効な対策が、数か月後には効果がなくなることも考えられます。最も大切なのは、情報を扱う人が、その時点におけるセキュリティリスクに対して意識を高く持ち、自ら積極的な対策をとることにあります。

Q32　やむを得ず、大量のデータをやり取りする場合に留意する点を教えてください。

A32　ＣＡＡＴを適用する場合等、やむを得ず大量のデータの授受をするに当たっては、依頼、取得、利用、保管、返却・廃棄の各局面において以下の点に留意してください。

①　依頼

ＣＡＡＴを適用する趣旨、作業内容、作業中の電子データの管理、作業後の電子データの返却・廃棄方法等について、クライアント等と十分に打合せを行い、合意をしておくことが重要です。

また、電子データについては、適用する目的が達成できる必要最小限にすることがポイントです。分析などに使用しない項目、特に氏名等の個人情報や未公表事実に該当するデータは可能な限り入手を控えることが、情報漏洩のリスクの対策上、重要です。

②　取得

電子データをクライアント等から入手する際に以下の点に留意することが重要です。

・　電子データは適用する目的が達成できる必要最小限にすること。
・　電子データが保存されたＵＳＢメモリ、ＤＶＤ等のメディアは、紛失リスクを低減させるため、必要以上の持ち歩きを控えること。
・　電子データをメディアに保存する場合は、暗号化等の情報漏洩対策を施すこと。
・　電子データをメールで取得することは可能な限り控え、やむを得ない場合は、メールの誤送信に気をつけるのはもちろん、暗号化等の情報漏洩対策を施すこと。

なお、クライアント等と電子データの授受に際して、受領書のようなものを作成して取り交わすことも有用です。

③　利用

分析などの作業を行う場合は、元データからコピーを作成して作業を行うことがあると考えられますが、不要なコピーを作成しないようにすることが重要です。コピーが複数作成されると、それだけ管理する対象が増えることになり、情報漏洩のリスクが高まることになります。

また、業務実施者の作業については、上司による適切な指導監督が重要です。

なお、情報漏洩のリスクを下げる方法として、例えば、電子データの提供元であるクライアント先の安全な場所にＣＡＡＴ用ＰＣやＨＤを設置し、その場所で作業を行うことも考えられます。

④　保管

作業終了後、元データ、作業途中に作成された中間ファイル、作業結果などの電子ファイルは、監査調書等として保管しておくべきものとそうでないものとに分類し、保管不要としたものについては下記⑤に従って返却・廃棄することが重要です。

保管期間は、他の電子データと同様、セキュリティ・ポリシーで定めている期間になると考えます。

なお、通常、元データそのものを監査調書として保管しておく必要性は低いと考えますが、十分な検討を行ってください。

⑤　返却・廃棄

クライアント等とあらかじめ合意した方法で、返却・廃棄を行うことが重要です。なお、返却に当たっては、受領書のようなものを作成して取り交わすことも有用です。

なお、ＣＡＡＴの適用に当たり、対象となる情報システムによっては、電子データを簡単に取得できない場合があり、その対応としてＩＴの専門家が作業を行うことも考えられます。その場合は、上記①から⑤についてはＩＴの専門家の利用も考慮に入れることが考えられます。

また、クラウドサービスを利用して電子データを授受する方法も考えられますが、Q27を参考に、情報漏洩対策等が十分であるかどうかに留意することが重要です。

Q33　業務中以外で、セキュリティ対策として何か留意すべきことはありますか。

A33　最近では、ＳＮＳ等で自分の動向を容易に公開できるようになりました。ただ、業務での出張中に、出張先の風景等を写真に撮りＳＮＳにアップロードすることで、写真の位置情報から往査先の情報が推測できる等、思わぬところで情報漏洩が生じるおそれがあります。

また、業務中にクライアント等で起こった出来事をＳＮＳにアップロードした場合、仮に具体的なクライアントの情報を記載していなかったとしても、ＳＮＳのＩＤ等を元に個人を特定された上、その関連情報等を元にクライアント等を特定され、情報漏洩を行ったことと同じような結果になることも考えられます。

ＳＮＳを利用する際は、その特性を理解するとともに、複数の情報源から個人の情報を特定されるおそれがあるといったインターネットの特性に十分留意して利用してください。

Q34　万が一、機密情報を漏洩してしまった場合には、どのようにすればよいですか。

A34　情報を漏洩してしまったことが分かった時点で、事務所のセキュリティ・ポリシー等に従い、可及的速やかに所属する事務所の責任者又はシステム管理担当者に申し出て、必要な対策をとることが重要です。対策が早ければ情報の漏洩を最小限度に抑えることができ、かつ、原因の特定もしやすくなります。

最も問題なのが、情報を漏洩したかもしれないことに気付いたにもかかわらず、これを事務所等に報告せず放置することです。放置することで情報漏洩の範囲が広がり、また、ログ情報等がなくなることで、原因の究明も困難になってしまいます。

近年では技術の発達に伴いセキュリティに関する攻撃の手法も多様化し、情報漏洩につながる可能性のある事故やミスを完全に防ぐことは難しくなっています。事故やミスが発生した際には、その原因となるセキュリティホールを埋めることが最優先となりますので、まずは情報セキュリティ担当者へ報告してください。

付録１：セキュリティ・ポリシーの例示

以下のセキュリティ・ポリシーの例は、職員数10人程度の公認会計士事務所（監査法人）が最低限検討すべき事項を前提として作成しています。

なお、事務所の状況に応じて取捨選択し、修正の上、参考として利用してください。

Ⅰ　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）の例

１．基本方針

この基本方針は、公認会計士〇〇事務所の業務を実施するに当たり、全ての事務所職員が情報セキュリティの重要性を認識した上で遵守すべき方針である。対象となる全ての情報は、その重要性に応じ「情報セキュリティ対策基準」に基づき、取り扱われなければならない。

２．目的

この基本方針は、当事務所が社会的信頼性の高い業務を提供するに当たり、取り扱う情報の漏洩や消失といった事態を未然に防ぐべく、必要となるセキュリティ対策を実施するためのポリシーを明確にすることを目的とする。

３．対象範囲

この基本方針の対象とする情報の範囲は以下の事項とし、電子データのみならず紙媒体の情報も含むものとする。

- 業務実施により知り得たクライアント等の情報
- 実施した業務に関する情報（契約金額、作業時間等）
- 事務所がノウハウとして独自に保有する情報（マニュアル、事例など）
- その他の情報（事務所職員の人事情報、経営情報など）

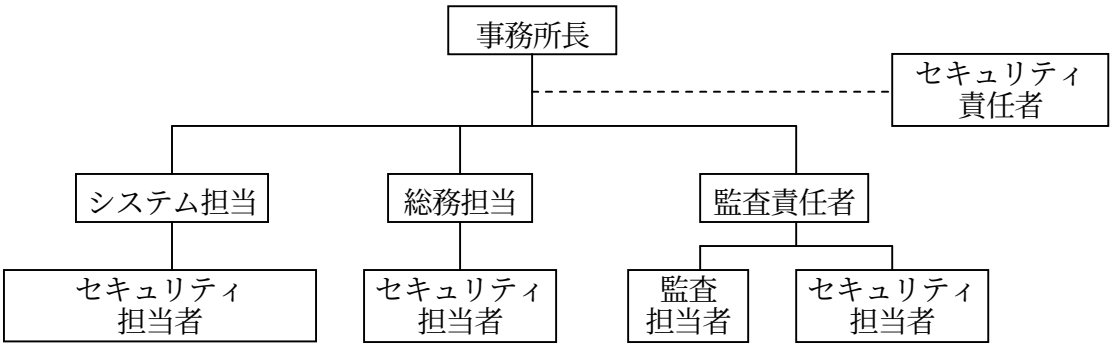
４．対象者と適用範囲

この基本方針の対象者には、事務所職員のみではなく、警備・清掃業務等の委託先、派遣職員等を含む。また、基本方針は、対象範囲の情報を取り扱う全ての場所、回線、機器に適用する。

５．管理体制

情報管理の責任は、事務所長が担うものとする。その実行、管理に当たっては、セキュリティ責任者を定め、各部門でセキュリティ担当者を任命して以下の体制により実施する。

（体制の例）



（※）セキュリティ責任者は、情報セキュリティの全般管理を実施する役割として設置することが望ましいが、必ずしも設置が求められるものではなく、組織の規模に応じ、各部門のセキュリティ担当者を中心にセキュリティ体制を構築することも一つの方法として考えられる。

6．情報の分類

対象となる情報については、以下の観点から重要性に応じた分類を行う。

(1) 漏洩による影響

担当者の不正使用及び担当者以外の事務所職員及び外部からの不正アクセス、文書・媒体の複製及び持ち出し、盗難に関して、当該情報が漏洩した場合の信用の失墜、損害賠償、罰則を考慮して重要性を決定する。

(2) 消失による影響

事故、不正操作、火災、天災等により当該情報が消失した場合、情報を適時に利用できない場合の影響を考慮して重要性を決定する。

(3) 誤謬による影響

過失、改竄等により、情報に誤謬を生じた場合の影響を考慮して重要性を決定する。

7．情報の保管期限

情報の種類、重要度に応じて保管期限を定める。なお、保管期限を過ぎた情報については、必要な承認手続を経て、廃棄・削除するものとする。

8．実施状況の点検及び監査

この基本方針及び情報セキュリティ対策基準の遵守状況について、定期的にセキュリティ実施状況の点検を行うとともに、内部監査を実施する。

9．評価及び見直しの実施

実施状況の点検及び監査の結果並びにその他ＩＴの進歩等、組織を取り巻く状況の変化を踏まえ、基本方針、対策基準及び実施手順書の見直しを定期的に行う。

Ⅱ　情報セキュリティ対策基準の例

１．物理的対策基準

(1) 事務所

- 事務所への入退出を適切に管理すること。
- 窓、非常口など通常の出入口以外の通路を適切に管理すること。
- 地震、火災、侵入などの影響を考慮した立地、建造物であること。

(2) セキュリティ区画

- 重要度の高い情報を保有する区画又はアクセス可能な端末を設置する区画について、ドアが施錠され、壁又は堅牢なパーテーションで区切られ、入退室を適切に管理すること。
- 同区画において、温度、粉塵、湿度、振動等の環境要因を適切に管理し、消火設備、検知器が必要な保守点検を受けていること。
- 同区画に対して、深夜休日単独作業を管理すること。

２．システム対策基準

(1) ネットワーク

- ネットワーク接続の仕様、機器を統一して管理すること。
- 各ネットワーク機器の状況、トラフィック、システム停止に関して、適切な統制管理を行うこと。
- レベル２以上の電子データを保有する機器について、ファイアウォール、暗号化通信等の適切なセキュリティ仕様を適用し、適切に運用されていることを適時に管理すること。

(2) ハードウェア

- セキュリティレベルに応じて信頼性のある機器を選定すること。

(3) ＯＳ、ソフトウェア（グループウェア、データベース等）

- セキュリティに配慮したソフトウェアの設定を行うこと。
- 適時にパッチなどの更新プログラムを適用すること。

(4) 業務システム

- 適切な品質管理を行い、利用する電子データのレベルに応じたセキュリティ対策をとること。

(5) マルウェア

- 適切なマルウェア対策ソフトを使用し、パターン・ファイルを適時に更新する等、最新の状態を維持すること。

(6) バックアップ

- 電子データの重要度分類に基づき、適切な頻度で電子データ等のバックアップを行うこと。

３．アクセス管理基準

(1) アクセス管理

・　重要な電子データにアクセスする場合は、個人別にＩＤとパスワードを用いること。
・　電子データごとに利用可能な権限（変更可能権限を含む。）を設定すること。
・　当該権限は、定期的及び職務権限変更時に見直すこと。

(2) ＩＤ管理

・　管理台帳（紙か電子的かを問わない。）を整備し、常に最新の状態に保つこと。
・　定期的に棚卸しを行い、退職者などの不要なＩＤが残されたままになっていないか確認すること。

(3) パスワード管理

・　推測されにくいパスワード（例えば、英数字混在の８桁以上）を使用すること。
・　有効期限を決めるなど、必要に応じて変更すること。
・　上記仕様は、システムで強制設定すること。

４．職員等行動基準

(1) 電子メールの利用制限

・　業務に関係のない電子メールの私的利用は原則として禁止すること。
・　当事務所が定めるメールソフト又はメールシステム以外を使用しないこと。
・　電子メールの本文には機密情報等の重要な事項を記載しないこと。

(2) インターネットの利用制限

・　業務に関係のないウェブサイトの閲覧及びインターネットの私的利用は、原則として禁止すること。
・　当事務所が取り扱う情報をインターネット上に発信・公開しないこと。

(3) ソフトウェアのインストール制限

・　業務に関係のないソフトウェアのインストールは、原則として禁止すること。
・　業務上必要と考えられるソフトウェアのインストールに当たっては、セキュリティ責任者の許可を得た上で実施すること。

(4) 重要な情報の個人保管の禁止

・　業務上重要な電子データに関しては、原則として個人のＰＣや記憶媒体に保存せず、当事務所で定めた所定のサーバに保存すること。
・　業務上重要な紙媒体に関しては、原則として個人が管理するデスク等には保管せず、当事務所で定めた所定のキャビネットに保管し、施錠すること。
・　ＰＣが盗難又は紛失にあった場合、利用者は、直ちにセキュリティ責任者に報告すること。

(5) 書類の管理（コピー、プリンタにより出力した文書など）

・　業務上重要な情報をコピーした場合又はプリンタにより出力した場合は、速やかに回収し、長時間放置しないこと。

(6) 機密事項に関する会話に関する注意

・　執務室外で業務に関連する会話をしないこと。

(7) ＰＣの管理

・　ＰＣは、盗難又は毀損の防止に向けて、各利用者が責任を持って管理すること。

Ⅲ　情報の分類の例示

公認会計士○○事務所の情報を、次の４種に分類する。

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。

レベル３　（極　秘）	
利用可能者	当該業務の責任者及び責任者の許可した主任担当者 事務所内で任命された品質管理者等
保管場所	物理的媒体の場合、常時施錠された金庫等に保管する。 電磁記録は暗号化し、紙媒体の場合、複写を困難とする対策を講じる。 インターネット経由の電子メール送信は禁止する。
運搬・通信	高度の暗号化を行い、安全に運搬・通信を行う。 なお、伝送の場合は、専用回線又はこれと同等の回線を使用する。
認証	保管データの使用に当たっては、指紋等による生体認証、ＩＣカード、パスワード等の認証方法を複数組み合わせる。

レベル２（秘　密）	
利用可能者	当該業務責任者の許可した担当者
保管場所	物理的媒体の場合、施錠可能な保管庫等に保管する。 電磁記録は暗号化し、ファイルサーバに共有データとして保存する場合、当該サーバは十分な安全対策を施す。 電子メールでの送信については、十分な暗号化対策を講じる。
運搬・通信	物理的媒体の場合は、担当者又は信頼できる業者が安全に輸送する。 電子データについては、適切な暗号化を行う。
認証	利用に当たっては、鍵、ＩＣカード、パスワード等の認証を必要とする。

レベル１（社外秘）	
利用可能者	事務所職員 外部委託の場合、秘密保持契約を要する。
保管場所	配付資料は回収する。 十分な職員教育を行う。

Ⅳ　電子メールに関するセキュリティ・ポリシーの例示

・　電子メールの利用は、業務目的に限定する。
・　機密情報は、電子メールでやり取りしてはならない。
・　機密情報を電子メールでやり取りする場合は、クライアント等と合意の上で行い、暗号化などの措置を施さなければならない。
・　個人のメールアドレスに転送してはならない。
・　電子メールを送信する際には、宛先をよく確認し、誤った宛先に送信しないようにしなければならない。
・　ファイルを添付する場合には、パスワードを設定しなければならない。なお、そのパスワードは別手段により相手に通知しなければならない。

なお、一般的な事柄ですが、以下の点についても留意した方がよいと考えます。
・　文章表現、サイズ等に関し、一般的な電子メール使用上のマナーに反してはならない。

付録２：業務の局面におけるリスクとリスク対応例（Q11参照）

Ⅰ 想定事例によるリスク分析

類型	No.	作業場面（状況）	想定されるリスク例	参照番号
収集	1	資料を受け取るためにメールでクライアントとやり取りする	・相手先を間違える、ＣＣ：に関係ない人が含まれているなどにより、メールを誤って送付してしまう。 ・第三者に通信を盗聴されてしまう、データを改竄されてしまう、又は第三者が本人になりすまして不正な利用をしてしまう。 ・マルウェアに感染してしまう。	① ⑥ ⑧
	2	現場にて資料をＵＳＢメモリ等（リムーバブルメディア）で受け取る	・ＵＳＢメモリ等を紛失する、又は盗難されてしまう。 ・他クライアントのデータが保存されたままクライアントに渡してしまう。 ・マルウェアに感染してしまう、又はマルウェアに感染したＵＳＢメモリ等をクライアントに渡してしまう。	③ ④ ⑧
利用	3	上司にメールで調書のレビュー依頼をする	・相手先を間違える、又はＣＣ：に関係ない人が含まれているなどにより、メールを誤って送付してしまう。	①
	4	他人とのユーザＩＤの貸し借り（代理入力等）	・第三者が本人になりすまして不正な操作をしてしまう。	⑥
	5	人事異動、事務所退職等	・アクセス権を変更していなかったため、異動者、退職者が元部署のデータを取得することができてしまう。 ・メールアドレスを無効にしていなかったため、異動者、退職者にメールが届いてしまう。 ・ＩＤを無効にしていなかったため、退職者や退職者になりすました第三者が外部から侵入し、不正な操作をしてしまう。	⑥ ①、⑥ ⑥
	6	ソフトウェアの利用	・アプリケーションやＯＳ（オペレーティングシステム）へのセキュリティパッチの適用やバージョンアップを行わなかったため、（セキュリティホールを利用して）第三者が外部から侵入し、不正な操作をしてしまう。	⑥、⑧
	7	インターネットの利用	・マルウェアに感染してしまう。 ・標的型メール攻撃の攻撃対象となってしまう。	⑧ ⑦

類型	No.	作業場面（状況）	想定されるリスク例	参照番号
保管	8	ＰＣ内にデータを保管	・ＰＣを紛失する、又は盗難されてしまう。 ・ファイルを誤って消去してしまう。 ・マルウェアに感染してしまう。 ・離席時に第三者が不正に利用してしまう。 ・ＰＣが故障して、データを読み取ることができなくなってしまう。	③ ② ⑧ ⑥ ⑨
	9	ＵＳＢメモリ等（リムーバブルメディア）にデータを保管	・ＵＳＢメモリ等を紛失する、又は盗難されてしまう。 ・ファイルを誤って消去してしまう。 ・マルウェアに感染してしまう。 ・ＵＳＢメモリ等が故障して、データを読み取ることができなくなってしまう。	③ ② ⑧ ⑨
	10	事務所のファイルサーバ上の共有フォルダにデータを保管	・システム障害によりサービスが停止する、又はデータを読み取ることができなくなってしまう。 ・第三者がデータを閲覧してしまう、又はデータを改竄してしまう。	⑩ ⑥
	11	クラウドサービス事業者が提供するストレージサービスにデータを保管	・システム障害によりサービスが停止する、又はデータを読み取ることができなくなってしまう。 ・事業者の倒産によりサービスが停止してしまう。 ・アクセス権の設定間違いで、一般に公開されてしまう。	⑩ ⑪ ⑥
廃棄	12	過去の古いデータが保管されている	・不要なデータを保存することによって、全体としてのシステム関連費用が増大してしまう。 ・データフォーマットが陳腐化してしまい、古いデータを読み取ることができなくなってしまう。	⑤ ⑨、⑪
	13	システム更新に伴い、古い情報機器を廃棄する	・ファイルを誤って消去してしまう。 ・情報機器内にデータが保存されたまま廃棄してしまう。	② ④

Ⅱ リスク対応例

想定されるリスク例			リスク対応例
種別	No.	リスク例	対応例
利用者のミス	①	メール誤送信	・ファイルの暗号化、強制暗号化ツールの導入 ・メールの暗号化 ・オートコンプリートの使用禁止
	②	データの破損、誤消去	・定期的なバックアップの実施 ・操作マニュアルの作成、利用
	③	情報機器の紛失、盗難	・ファイルの暗号化、強制暗号化ツールの導入 ・定期的なバックアップの実施 ・物理的な施錠管理（保管場所、セキュリティワイヤー等）、持ち出しルールの設定
	④	データの消去漏れ	・使用後のファイル削除ルールの設定 ・ファイルの暗号化、強制暗号化ツールの導入 ・削除ツールの利用、専門の外部業者の利用
	⑤	不要データによる管理コストの増大	・電子データの保管期限の設定 ・電子データの定期的な棚卸し
第三者の悪意	⑥	情報の不正取得、改竄、なりすまし	・ＩＤ（メールアドレスを含む。）・アクセス権の付与・削除手続の設定 ・ＩＤ（メールアドレスを含む。）・アクセス権の定期的な棚卸し ・起動時パスワード、スクリーンセイバーのパスワード等の設定 ・ファイルの暗号化、強制暗号化ツールの導入 ・パスワードルールの設定（桁数、定期的変更等）
	⑦	標的型メール攻撃	・セキュリティ教育研修の徹底
	⑧	マルウェアの感染	・マルウェア対策ソフトの導入 ・適時、適切なバージョンアップ（セキュリティパッチの適用を含む。） ・業務用情報機器の私用禁止
システム障害	⑨	情報機器の故障、破損によるデータの滅失	・適時、適切なシステム更新（投資） ・定期的なバックアップの実施
	⑩	サービスの停止	・定期的なバックアップの実施

想定されるリスク例			リスク対応例
種別	No.	リスク例	対応例
事業者の事情	⑪	サービスの停止	・事業者の選定基準の設定 ・定期的なバックアップの実施

付録３：平成27年12月14日付け会員向けお知らせ[1]

会員各位

平成 27 年 12 月 14 日

「今般の日本年金機構における個人情報流出事案を踏まえた金融庁からの要請について」（平成 27 年６月 30 日 会長周知文書）に関する会員各位の対応について（お知らせ）

常務理事　中　村　元　彦

平成 27 年６月 30 日に森会長名のお知らせ「今般の日本年金機構における個人情報流出事案を踏まえた金融庁からの要請について」が発出されており、会員に対して、情報セキュリティ管理態勢及びサイバーセキュリティ管理態勢を点検しつつ、通信記録（ログ）の取得・分析等を通じた情報漏洩の検知を含め、個人情報を含む重要情報の適正な管理を行うよう、要請されています。

これは、６月１日に日本年金機構から公表された個人情報流出事案を受けた金融庁からの要請によるものであり、今般、会員各位の対応に当たっての参考情報として、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」（以下「ＩＴ実４号」という。）を中心に本要請に関連する項目について整理いたしましたので、改めてお知らせいたします。

コンピュータウィルス等による情報詐取の事案は増える一方であり、我々公認会計士は、その扱っている情報の重要性を再認識し、情報セキュリティ管理態勢・サイバーセキュリティ管理態勢に関する内部統制を見直し、一層向上させていくことが求められています。

会員各位におかれては、趣旨を理解の上、適切に対応いただきますようお願いいたします。

１．日本年金機構の個人情報流出事案の概要と根本原因、再発防止策の提言内容

今回の要請に対応するためには、日本年金機構における個人情報流出事案の原因が何かを理解し、自らの状況に置き換えて考えてみることが有用と思われます。また、特定された再発防止策も、参考になる事項があると思われます。

該当事案が発生した原因分析と対応策の検討結果は、日本年金機構、厚生労働省、内閣サイバーセキュリティセンターから、それぞれ公表されています。

このお知らせでは、厚生労働省から公表されている「日本年金機構における不正アクセスによる情報流出事案検証委員会検証報告書」（以下「報告書」という。）から概要を紹介します。

[1]本文中に記載の条文等は発信当時のものである。

【日本年金機構における不正アクセスによる情報流出事案の概要】

事案の概要（報告書 P.16）	標的型メールを送付する手口によって機構 LAN システムが三段階にわたる標的型攻撃を受けた結果、共有フォルダに保管されていた大量の個人情報等が外部に流出してしまった。
第１段階の攻撃	２つの公開メールアドレス宛てに同一のアドレスから不審メール２通が送信され、受信した職員の一人がこれを開封し、メール本文に記載されていた URL のリンクをクリックしたことで、その端末に不正プログラムがダウンロードされ、外部との不正な通信が発生した。この通信は４時間にわたり続いたものの、発見され、不正プログラムは駆除された。 内閣サイバーセキュリティセンターから日本年金機構へ不審な通信に関する通報がなされていたが、日本年金機構内で情報が伝達され、最終的にシステム担当者がこの通報を受け取るまでに２時間半を要した。また、全職員に対しての注意喚起が行われたものの、一般的な事項にとどまり、この攻撃の事実を引用した説明などはなされていなかった。
第２段階の攻撃	第１段階の攻撃から 10 日後、第１段階の時と同じ送信元アドレスから日本年金機構の職員個人のメールアドレス宛てに 101 通のメールが送られてきた。日本年金機構はこのメールについて受信拒否設定を行ったが、翌日には、別のメールアドレスから 19 通のメールが送られてきた。ここでも受信拒否設定を行ったが、同日の午後には、さらに別のメールアドレスから１通のメールが送られてきた。 この一連の攻撃により、３台の端末がウィルスに感染したが、第１段階の攻撃の時に取った対策により、外部との不審な通信は行われなかった。 日本年金機構は、全職員に対してこの攻撃の事実を引用した注意喚起を行ったが、メールを受信した職員に対する開封確認を行っておらず、３台の端末が感染したことも２週間気付かなかった。
第３段階の攻撃	第２段階の攻撃から２日後、新たな送信元アドレスから公開メールアドレス宛てに５通のメールが送られてきた。このメールを受信した日本年金機構の職員のうち１人がメールを開封し、添付ファイルを開いてしまったため、ウィルスに感染し、そこから 26 台の端末に感染が拡大してしまった。そして、感染から３日間、外部との不審な通信が行われ、共有フォルダに保存されていた大量の個人情報等が外部へ送信された。 日本年金機構は、職員から不審なメールを受信したという報告を受けたものの、添付ファイルを開封していた事実は５日間経過するまで

	把握できなかった。また、外部との不審な通信も１週間把握することができなかった。
根本原因 （報告書 P.27）	①　日本年金機構、厚生労働省ともに、標的型攻撃の危険性に対する意識が不足しており、事前の人的体制と技術的な対応が不十分であったこと。 ②　インシデント発生後においては、現場と幹部の間、関連する組織間に（例えば、日本年金機構と厚生労働省、同一組織間の各部署、日本年金機構と運用委託会社など）、情報や危機感の共有がなく、組織が一体として危機に当たる体制になっておらず、その結果、組織内の専門知識を持つ者の動員ができず、担当者が幹部の明確な指揮を受けることもできないままに場当たり的な対応に終始し、迅速かつ的確な対処ができなかったこと。
再発防止策の提言 （報告書 P.33）	①　一部の者だけではなく組織が一体となった体制の整備、運用が必要である。 ②　日本年金機構等の役職員全員が標的型攻撃に対する危機意識を持つことが必要であり、今回の情報流出事件のもたらした結果の重大性と標的型攻撃の危険性を一部の職員だけではなく、日本年金機構全ての役職員が自分たちのこととして今後も認識し続けなければならない。 ③　標的型攻撃に際しては、組織が全体となってこれに対応する必要があり、それぞれの役職員が、これは自分の仕事ではないとか、自分の担当範囲でも従来通りのパターンを繰り返して漫然と対応するような姿勢ではなく、平素から困難に際し協力し合って逃げずに対処する組織作りを心がけるべきである。

２．会員各位における対応

上記の根本原因分析と再発防止策の提言内容を踏まえると、少なくとも、職員の意識、情報の管理態勢、インシデント発生時の対応方法については、それらが有効に機能しているのかも含めて再確認を行っておくことが重要と考えられます。

また、今回の標的型攻撃の状況や上記以外の個人情報漏洩事案を見ると、情報詐取を完全に防ぐことは難しく、それゆえ、いかに早く発見し、被害を最少にとどめるか、といった視点から考えることも有用と考えられます。

会員の事務所等の状況に応じた対応が必要となりますが、以下に具体的な対応に当たっての考え方をまとめましたので、ご留意ください。

(1) 職員向け研修の実施状況・内容の確認・見直し

ＩＴ実４号Ⅳ６「情報セキュリティに関する研修の実施」では「情報セキュリティ・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各種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」とされています。

教育研修が不十分だと、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ます。

留意事項としては、例えば以下の事項が考えられます（ＩＴ実４号Ⅳ６参照）。

- 外部環境・内部環境の変化に合わせて教育研修の内容が見直されているか。
- 定期的に教育研修が行われているか。

(2) 内部管理態勢の確認・見直し

公認会計士が業務上取り扱う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と考えられます（ＩＴ実４号Ⅳ、Ⅴ、Ⅵ参照）。

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ます。

留意事項としては、例えば以下の事項が考えられます（ＩＴ実４号Ⅲ２～３、Ⅳ５参照）。

- 経営者、情報セキュリティ担当者、利用者は、自身の役割を正しく理解し、実行しているか。
- 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。
- 外部環境・内部環境の変化に合わせて内部管理態勢の見直しを行っているか。

なお、公認会計士・監査審査会から公表されている「監査事務所　検査結果事例集」（平成 27 年７月）では、次の問題点が挙げられています。

- 規程等の運用が行われていることを実態に踏み込んで確認しているか（形式的な確認にとどまっていないか）。

(3) 事案発生時の対応方法の確認・見直し

ＩＴ実４号Ⅳ10「情報漏洩時の対応」では、「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」とされております。

万が一の場合を想定した対応方法が周知、理解されていない場合は、情報漏洩が発生しても気付かず、被害を拡大させるリスクがあります。

留意事項としては、例えば以下の事項が考えられます（ＩＴ実４号Ⅲ３、Ⅳ10 参照）。

- 事案発生時の対応を職員が理解しているか。
- 状況に合わせて対応方法の見直しを行っているか。

(4) 情報の整理、所在の把握

公認会計士が業務上取り扱う情報には、監査先の情報やそれらを記載した監査調書など、様々なものがあります。これらの情報はセキュリティ・ポリシーに従い、重要度に応じて分類され、管理することが有用と考えられます（ＩＴ実４号Ⅲ参照）。

管理すべき情報が特定されていない、セキュリティ・ポリシーが実態に即していない、セキュリティ・ポリシーや細則に従った運用がなされていない、といった場合には、情報漏洩のリスクが非常に高まっていると考えられ、情報漏洩となった場合の影響は甚大になることが想定されます。

留意事項としては、例えば以下の事項が考えられます（ＩＴ実４号Ⅲ１(1)～(3)参照)。

- 情報が重要度に応じて分類されているか。
- 重要度に応じた管理方法が徹底されているか。
- 保管期限を超えた情報が廃棄されているか。

３．参考になるウェブサイト

① 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」
http://www.hp.jicpa.or.jp/specialized_field/main/34_13.html

② 日本年金機構の情報流出事案に関する報告書

・日本年金機構
「不正アクセスによる情報流出事案に関する調査結果報告書」
http://www.nenkin.go.jp/files/kuUK4cuR6MEN2.pdf

・厚生労働省
「日本年金機構における不正アクセスによる情報流出事案検証委員会検証報告書」
http://www.nenkin.go.jp/files/XtYrbhaJKiEk4.pdf

・内閣サイバーセキュリティセンター
「日本年金機構の個人情報流出事案に関する原因究明調査結果」
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

③ 独立行政法人　情報処理推進機構（IPA）

・情報セキュリティ安心相談窓口
http://www.ipa.go.jp/security/anshin/index.html

・情報セキュリティ対策
https://www.ipa.go.jp/security/measures/index.html

④ 特定非営利活動法人　日本ネットワークセキュリティ協会

・情報セキュリティ対策
http://www.jnsa.org/ikusei/

以　上

付録４：平成21年７月22日付け会員・準会員宛メッセージ[2]

公認会計士業務上の電子化された情報の管理について

平成21年７月22日
日本公認会計士協会
ＩＴ担当常務理事　中山　清美

平成17年４月に個人情報保護法が施行されて以来、公認会計士業界に限らず多くの業界で大量の情報が保存されたノートパソコンやUSBメモリの紛失、Winny等のファイル交換ソフトによる情報の漏洩などが報道されている。

今日の公認会計士業務においては、ノートパソコン、USBメモリ等の電子機器に、クライアントから入手した個人情報を含む種々の情報や、監査調書等の業務のために取りまとめた情報（いわゆるクライアント情報）を保存し持ち歩く機会が格段に増してきている。また、業務の都合上やむを得ず、それらの情報を自宅に持ち帰り、自宅のパソコンで作業する場合もある。

我々が業務で入手した情報が、クライアントにとっては非常に重要な機密情報にあたることは容易に想像でき、その様な重要な情報を紛失し、外部に漏洩し、不正にあるいは私的に利用し、又は、不正あるいは私的に利用するために持ち出した場合には、そのような事態を引き起こした会員あるいは会員事務所のみが公認会計士法や会則違反に問われ信頼性を喪失するにとどまらず、公認会計士業界全体の信頼性すら損ねることになる。我々の業務の前提は信頼性であり、その信頼性にはクライアント情報の取り扱いに関することも含まれていることは言うまでもない。したがって、我々公認会計士には、そのような事態を引き起こさないための「情報セキュリティ」が重要な課題となる。

１．情報セキュリティ意識を共有すること

会員及び会員事務所は、個人情報保護法への対応を含むクライアント情報に対する管理体制について厳正に見直すとともに、会員事務所及びその関係会社において業務に従事する全ての者の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ずる必要がある。一人による情報の紛失や漏洩、不正・私的利用又はそれを目的とした持ち出しが、公認会計士業界全体に対する信頼性の喪失に直結することを改めて認識し、情報管理体制の厳正な見直しを行うべきである。

２．情報セキュリティ体制を構築し、運用すること

業務で使用している電子機器等への具体的な対応に先立ち、まず会員事務所における情報セキュリティのための組織・規定などを整備する必要がある。また、この整備を通じ、情報セキュリティに対する社員・職員などの構成員個々人の意識レベルを高めていくことが最も重要なポイントとなる。

会員事務所が管理すべき情報は、クライアント情報のみならず、会員事務所で作成し

[2]本文中に記載の条文等は発信当時のものである。

た業務マニュアルや書式類も重要な情報であり、いずれも管理すべき重要な財産である。

重要な財産が、紛失や漏洩、不正・私的利用又はそれを目的とした持ち出しなどのリスクに晒されないよう、会員事務所には、その構成員の情報セキュリティに関する意識レベルを高め、適切な管理体制を構築することが求められる。これらの事態を防ぐためのいくつかの具体的施策があるが、前述のとおり最も重要なポイントは会員事務所構成員個々人のセキュリティ意識の向上にあり、そのためにはまず会員事務所責任者が率先して情報セキュリティを意識した行動をとり、絶えず構成員にその重要性を訴え続けることが必要となる。

会員事務所における情報セキュリティについては、「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」（ＩＴ委員会報告第４号　平成20年１月16日）、「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Ｑ＆Ａ」（ＩＴ委員会研究報告第34号　平成20年１月16日）に詳細な記述があるので是非参照されたい。

３．紛失リスクを小さくすること

情報の紛失リスクは、次のような式で考えられる。

「ノートパソコン等に保存されている情報の質と量」

×「ノートパソコン等の機器の紛失リスク」

ノートパソコンやUSBメモリ等は持ち運びに便利であるが、同時に、常に紛失のリスクに晒されていることになる。

したがって、まずノートパソコン等に保存するクライアント情報の質的重要性を極力低いものとし、同時にその量を極力少なくすることを考えるべきである。例えば「その日の外出先で必要となるクライアント情報に限定してノートパソコン等に保存する」というような対応が考えられる。

次に、クライアント情報が保存されているノートパソコン等を持ち運ぶ機会をできるだけ少なくするということが重要となる。業務上やむを得ず携帯せざるを得ない時には、手許から離さず常に注意を払うという意識を持つことが重要となる。不注意による紛失のみならず盗難という事態も想定し、その備えへの取り組みも必要な時代であると認識する必要がある。

４．紛失しても漏洩となるリスクを引き下げること

盗難等による紛失という事態が発生した時、情報が外部に漏洩することになれば極めて深刻な事態となる。情報の外部への漏洩リスクを引き下げるため、例えば、ノートパソコンにはパスワードによるセキュリティを施し、ノートパソコン内のハードディスクやUSBメモリ等の外部記憶装置は暗号化する必要がある。また、これらの技術的措置を複合的に施すことによって、漏洩に至るリスクをゼロに近づけることが可能であり、その経済的負担はさほどではない。

業務で使用するパソコン等の電子機器に一定レベルのセキュリティを施すことは、必須事項である。

なお、会員事務所において業務上使用するパソコン等は会員自身以外が操作する機会はないと考えられるが、自宅のパソコン等は家族などの共有者がいることから、そのセキュリティ対策を確認しておく必要がある。例えば、会員自身の知らないところで家族等共有者のインストールしたソフトウェアがウィルスに感染し、利用している本人も知らないうちにパソコン内の情報が外部へ漏洩するといった事態も考えられる。

５．個人情報保護法に関するガイドラインの適用

公認会計士は、個人情報・データの取扱いや紛失や漏洩に関し、個人情報保護法・同施行令等関係法令のほか、金融庁が定めている「金融分野における個人情報保護に関するガイドライン」（以下、金融庁ガイドラインという。）の適用を受け、その遵守に努めることとなる。また、当該ガイドラインの安全管理措置等についての実務指針として、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」がある。

なお、個人情報保護法でいう個人情報取扱事業者に該当するか否かは、会員事務所として取扱う個人情報数の合計数によることとなっているので、確認しておくべきである。

６．万一紛失が発生した場合

会員あるいは会員事務所が個人情報・データを保存したノートパソコン、USBメモリ等を紛失した場合には、直ちに金融庁に報告しなければならない。紛失の全容が把握されていない段階であっても、紛失したという事実を直ちに報告すべきものと解される（金融庁ガイドライン第22条第１項）。

また金融庁への報告と同時に、紛失した個人情報の対象者に対して速やかに通知しなければならない。この通知は、会員事務所が講ずべき措置であり、クライアントから入手した個人情報であれば、まずクライアントに連絡し、クライアントを通じて当該対象者に通知することも考えられる（金融庁ガイドライン第22条第３項）。

以上の報告及び通知とともに、二次被害防止等の観点から事実関係・再発防止策等について早急に公表することも求められている（金融庁ガイドライン第22条第２項）。

個人情報以外のクライアント情報を紛失した場合には、当該クライアントに速やかに事実関係を連絡するとともに、その後の対応方法等について当該クライアントと協議する必要がある。

７．おわりに

以上、個人情報保護法への対応を含め、会員事務所としての情報セキュリティについて概括的に示した。社会が公認会計士に寄せる期待、信頼を裏切らないためにも、上述したような対応が求められるものであり、したがって情報セキュリティは職業倫理に係る重要な課題であると認識すべきである。

以　上

付録５：平成17年９月27日付け会員・準会員宛メッセージ[3]

会員・準会員　各位

平成17年９月27日
日本公認会計士協会
ＩＴ担当常務理事　高木　勇三

一人の情報の紛失は、業界に対する信頼性の喪失に直結しています

本年４月に個人情報保護法（注１）が施行されて以来、会員事務所でのノートＰＣ（パソコン）の紛失が報道されていますが、私どもの業務においてはいまやノートＰＣ、ＵＳＢメモリ等の電子機器などに、クライアントから入手した個人情報も含めた種々の情報や監査調書等の業務のために取りまとめた情報といったいわゆるクライアント情報を電子ファイル化して持ち歩くことが常態となっています。つまりこれら情報の紛失の可能性は以前と比べて格段に高まっているわけです。

一方私どもの業務の前提は信頼性であり、その信頼性の内にはクライアント情報に対する取扱に関することも含まれていることは言うまでもありません。このため一会員個人あるいは一会員事務所におけるクライアント情報の紛失は、当該個人や当該会員事務所に対する信頼性の喪失にまず繋がるわけですが、そればかりでなくこのようなクライアント情報の紛失は業界全体の信頼性の喪失にも繋がります。つまり私どもの業務の前提の崩壊にも繋がるということです。

その意味で個人情報保護法への対応を的確かつ適切に行うことはもとより、少なくともクライアント情報に対する管理体制について厳正に見直すとともに、会員事務所及びその関係会社において業務に従事する全ての者の情報管理意識を適切なものとするよう措置を講ずることが必要です。

一人の情報の紛失が業界に対する信頼性の喪失に直結することを改めて認識され、情報管理体制の厳正な見直しを行うべきことを改めて強く要請いたします。

まずは紛失リスクを小さくすること

情報の紛失リスクは、次のような式で考えられます。

「ノートＰＣ等に保存されている情報の質と量」×「ノートＰＣ等の機器の紛失リスク」

ノートＰＣやＵＳＢメモリ等はモビリティ性があるからこそ便利なわけですが、モビリティ性があるということは常に紛失のリスクにさらされていることも意味します。したがって、まずノートＰＣ等に保存するクライアント情報の質的重要性を極力低いものとし同時に、その量を極力少なくすることを考えるべきです。例えば「その日に外出先で必要となるクライアント情報に限定してノートＰＣ等に保存する」というような対応です。

次にクライアント情報が保存されているノートＰＣ等を携帯する機会をできるだけ少なくするということが重要です。もちろん携帯時には常に注意を払うべきといった意識を持つことも重要です。盗難という事態も想定しその可能性を低めるための取り組みも必要

[3]本文中に記載の条文等は発信当時のものである。

です。

紛失しても漏洩となるリスクを少しでも引き下げること

盗難等による紛失という事態が生じてしまった時、それが外部への漏洩につながると極めて深刻な事態となりますが、その漏洩リスクをゼロに近づけることはテクノロジとして可能です。例えばノートＰＣにはパスワードによるセキュリティを施すことが基本的に可能です。ノートＰＣ内のハードディスクを暗号化することも可能ですし、ＵＳＢメモリ等の外部記憶装置についても暗号化可能です。

このようなテクノロジを複合的に施すことにより漏洩に至るリスクを極めて小さなものとすることが可能であり、その経済的負担もそれほどではありませんので、ＰＣ等の機器への一定レベルのセキュリティ対応は是非とも求められます。

そもそも情報セキュリティ体制を構築しておくこと

以上のような具体的な対応とともに、会員事務所における情報セキュリティのための組織・規定を整備し、情報セキュリティに対する社員・職員等の意識レベルを高めることも同じく重要です。これらについてはＩＴ委員会研究報告第26号（平成16年６月)、「公認会計士が業務上留意すべき情報セキュリティ」において説明されていますが、改めてお読みください。

個人情報保護法に関するガイドラインの適用

個人情報・データの取扱や紛失・漏洩に関しては、私どもは金融庁が定めている個人情報保護法ガイドライン(注２)の適用を受けるあるいはその遵守に努めることとなります。個人情報保護法と併せて当該ガイドライン、そして当該ガイドラインの安全管理措置等についての実務指針（注３）について改めてお目通しください。

なお個人情報保護法でいう個人情報取扱事業者には、会員事務所として取扱う個人情報数は合計でカウントされますので、かなりの数の会員事務所が該当することとなると思われます。改めて、ご確認ください。

万一紛失が発生した場合

１．個人情報を入れたノートパソコン、ＵＳＢメモリなどを紛失した場合は、直ちに金融庁に報告することとされています。紛失した全容が把握されていない段階であっても、紛失したという事実については直ちに報告すべきものと考えられます。(金融庁ガイドライン22条１項)

２．金融庁への報告と同時に紛失した個人情報の対象者に対して速やかに通知することとされています。通知は会員事務所が講ずべきとされている措置ですが、クライアントから入手した個人情報であればまずクライアントに連絡し、クライアントから当該対象者に通知していただくことも考えられます。(金融庁ガイドライン22条３項)

３．以上の報告及び通知とともに二次被害防止等の観点から事実関係・再発防止策等について早急に公表することも求められています。(金融庁ガイドライン22条２項)

以上、個人情報保護法への対応を含め、会員事務所としての対応について概括的にお示ししましたが、公認会計士は「情報に関するプロ」と社会から位置づけられています。そのプロに寄せる社会からの期待を裏切らないために、以上に述べたような対応をとることが是非とも求められるものであり、したがって職業倫理に係る話であるとの認識も必要であることを付言します。

以　上

（注１）　個人情報保護法：「個人情報の保護に関する法律」
（注２）　金融庁が定めている個人情報保護法ガイドライン：「金融分野における個人情報保護に関するガイドライン」
（注３）　ガイドラインの安全管理措置等についての実務指針：「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」

以　上