公開草案　平成 19 年 10 月 24 日

ＩＴ委員会報告第　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

平成　年　月　日

日本公認会計士協会

―目次―

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（監査法人）が業務を実施するに当たり、クライアント等から種々の情報を電子データとして入手する機会が多くなってきている。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。）を持ち歩き、クライアントと業務に関する情報のやりと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、といったことがごく普通の状況になってきている。これらの結果、特に意識しないうちに、業務に関する情報は電子化されてＰＣ内に蓄積されることになる。

これらの電子データは、本来、紙の情報に比べ十分な管理が必要であるにもかかわらず、目に見える物体として存在しないこともあり、その管理体制が追いつかなくなりがちである。

クライアント等から入手した情報が外部に漏洩したとなれば、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（監査法人）としての存続が危ぶまれることにもなりかねない。公認会計士は、従来からの守秘義務の意味を再認識し、ＩＴの利便性とそこに潜むリスク、特にクライアント等に関する情報の漏洩・流出の危険性を十分に認識し、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、その対策を検討するとともに、ＩＴの有効活用による業務等の効率化と品質の向上を図らなければならない。

２．本委員会報告の目的と対象範囲

このような状況を踏まえ、本委員会報告は、公認会計士が業務（監査業務に限定されない）において留意すべきＩＴに関する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いる。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さまざまである。そのため、この委員会報告では、情報漏洩（紛失を含む）という観点から、ＩＴを利用する場合の情報セキュリティに焦点を絞り、対象とする電子データは、業務に直接関係するものに限定している。

したがって、紙媒体でしか存在しないデータ、あるいは公認会計士事務所（監査法人）の管理部門が管理する電子化されたデータ、例えば、人事データ、経理データ、品質管理に関するデータは対象としていない。

なお、情報漏洩を防ぐセキュリティ対策としては、コンピュータや情報システム自体の技術的な面（システム面）も重要であるが、「人の面」についても十分な対策を講じる必要がある。なぜならば、システム面のセキュリティだけを強化しても、利便性が損なわれるわりには情報漏洩を効果的に防ぐ手段とはなり得ないし、また、多くの情報漏洩は内部者の行為に起因するとも言われているからである。

また、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」において取扱が明示されているため、留意する必要がある。

３．紙媒体の情報のセキュリティ

上記でも触れたが、紙媒体でしか存在しないデータについては、本委員会報告の対象外である。しかし、例えば、監査調書といった業務に関連したもの、電子データを印刷したものについては、電子データと同様に十分な管理体制をとることが必要である。

Ⅱ．ＩＴ時代における秘密漏洩の危険性

１．守秘義務の重要性についての再認識

公認会計士法第 27 条には、秘密を守る義務として、「公認会計士は、正当な理由がなく、その業務上取り扱っ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った後であっても同様とする。」との規定がある。また、「監査基準　第二　一般基準８」にも、「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、または窃用してはならない。」との規定がある。

公認会計士の場合、業務の特殊性から、機密性の高い情報に触れることが多く、従来から公認会計士の守秘義務の重要性は叫ばれてきた。したがって、守秘義務については、「情報管理」といった面から実務的に考えることが重要である。

最近のＩＴの進歩は、我々の業務にもその影響が及んでいる。例えば、ＰＣにより表計算ソフト等で作成した電子データを送受信するとともに、電子データ自体を調書や基礎資料とするケースもある。また、以前はフロッピーディスク（以下「ＦＤ」という。）によりデータの授受を行っていたが、最近の記憶媒体は、ＦＤの数千倍のデータを扱うことが可能になり、かつ、短時間にコピーすることができるようになっている。さらに、インターネットに代表されるネットワーク社会が実現したことにより、電話（音声）や郵便（紙媒体）と比較して、様々な情報を、大量に、多数の人に、一瞬に伝達することが可能になっている。業務にこうしたＩＴの進歩を取り入れた結果、公認会計士は、情報管理という点で従来とは比べものにならない程のリスクを負っている。そのため、情報の内容及び機密性に応じて、ＰＣ、インターネット、電子メールの利用の程度を検討し、場合によっては、これらの利用を控える必要がある。

２．秘密漏洩の危険性

公認会計士は、その業務の実施に当たり、「秘密漏洩」に関しては従来から細心の注意を払ってきているが、ＩＴの発達により、それは質、量ともに大きく変化してきている。

例えば、ＩＴの発達によりクライアント等から入手する様々な企業情報が電子化され、監査調書も電子化されている。この様に、お互いに所有する情報が電子化されることにより、そのデータの送受信においても、盗聴、改ざん、なりすまし等の危険性がある。

また、インターネットでは、電子データが、何処をどのように回って相手方に到着するのかが明らかではなく、何処で盗み見られているか分からない。

電話の場合には掛け間違えればすぐに分かるが、電子メールで宛先を間違えた場合には、送ってしまったデータは取り消すことができない。しかも、送信されるデータ内容も多様であり、ネットワークに接続しているＰＣからデータが盗まれても気が付かないことも考えられる。このように、ＩＴには、利便性と裏腹に多くの潜在的な危険性が存在する。

３．電子化に対応する情報セキュリティ

様々な危険性が潜在しているＩＴではあるが、業務の効率化を図るため、公認会計士はこれを積極的に利用している。したがって、こうしたＩＴ環境の変化に呼応して、公認会計士は新たな情報セキュリティを考える必要がある。特に、インターネットを介した外部接続が行われるようになると、スタンドアロンでの情報処理の時とは比べものにならないような新たなセキュリティが必要となる。インターネット利用という視点から、以下セキュリティ対策をみていくこととする。

(1)　インターネット利用に係る情報セキュリティ

ネットワークは組織内での情報交換に利便性を発揮するが、その利便性は外部接続を通じてより高まることになり、インターネット接続により情報交換の利便性は飛躍的に向上した。しかし、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危険性が高く、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てシステムに侵入し、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、定期的ないしは随時に変更するのが常識であるが、変更の都度パスワードを覚えるのが苦手なために、ついＰＣの側にパスワードをメモしたりすると、セキュリティは無きに等しくなる。このための防衛策としては、ＩＣカード方式などパスワードに代わる方法が考えられるが、その前に、セキュリティに対する公認会計士の意識向上が必要である。

電子メールは、日本国内のみならず世界各国との情報交換が 24 時間いつでも行え、その便利さからお互いの時間の有効活用が図られ、頻繁に利用されている。しかし、インターネット上を情報が流れる時は、葉書と同様に、情報の中身を見せながら運んでいるのに等しいものといえ、このためメールの暗号化等の対策の検討が必要である。

また、電子メールによるインターネットを介しての情報交換は、相手方のメールアドレスを間違えることによる情報漏洩が生じる危険性がある。情報の重要度に応じて、電子メールと添付ファイルの暗号化、パスワード処理など十分なセキュリティ対策を行って、万が一情報が盗まれた場合であっても中身を簡単に見ることができないようにする対策の検討が必要である。

ＩＴ時代における情報セキュリティも、我々が扱う会社情報が紙媒体か電子媒体かの違いであるだけで、公認会計士が注意すべき基本的な事項は変わりないものと考えられる。しかし、会社情報の電子化が進めば進むほど便利さが先に立って、セキュリティの対策を講じずに最新のＩＴを利用してしまう行為が情報漏洩につながりかねない。したがって、公認会計士としては、相当の注意をもって電子データを取り扱うことが求められる。

(2)　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。）、ＦＤ、ＣＤ－Ｒ、ＵＳＢメモリなどに保存された電子データは、紙の場合に比してコピーされたことが分かり難いこと、漏洩

した際の情報量に格段の差があること等により、紙以上にセキュリティ対策が必要となる。そのため電子化された重要データが保存された媒体は、施錠可能な保管庫に収納しておく等の検討が必要である。

運搬についても、圧縮技術の進歩により、電子データは、例えＦＤ一枚でも大量の情報が保存可能であり、情報漏洩した場合の影響は計り知れないものがある。このため、物理的媒体の場合には、担当者又は信頼できる業者に安全な輸送（郵送）を依頼する必要がある。

業務において、ＦＤ等を介して会社と情報交換を行う場合や作成したデータの印刷を依頼する場合がある。この場合、そのＦＤ等に保存されている他の会社情報や編集履歴等を消し忘れたりすると、その情報が漏洩してしまうことになる。こうした行動は、公認会計士の信頼性に疑問を投げかける結果ともなりかねない。ＦＤ等を渡した会社が他の会社の情報が含まれることを知った場合、自分の会社の情報も他の会社に提供されてしまっているのではとの疑問から、公認会計士の守秘義務に対する疑念を生じさせてしまうからである。

ＰＣ自体の管理も重要である。我々は、クライアントのデータをＰＣ上で利用することが多いが、業務終了後、そのデータをそのまま放置しておくとＰＣが盗難にあった場合、ここから外部に情報が漏洩することになる。また、業務現場である会社の会議室や公認会計士事務所(監査法人)で食事等のため離席した時に第三者に侵入され、ＰＣや情報を盗まれる危険性もある。したがって、ＰＣ起動時のパスワード、スクリーンセーバーのパスワード、ＨＤ全体の暗号化等によるセキュリティ対策が必要となる。また、ＰＣだけでなくＰＤＡ（携帯型情報端末）や携帯電話等の情報機器も重要な電子データを扱うことが可能なため、ＰＣと同様に取り扱いを検討する必要がある。

Ⅲ．電子データの分類とリスク分析・対応

１．電子データの分類

(1)　電子データの分類の必要性

公認会計士が業務上扱う電子データには、例えば

・監査調書
・クライアントの経理データ、税務申告データ
・マネジメントレター
・クライアント作成の資料
・クライアントとの守秘義務契約により指定された情報
・業務を通じて知ったクライアントのインサイダー情報
・クライアントから得た、会社組織のノウハウ（マニュアル、事例)、人事、経営情報等

などがあり、これら様々な情報が電子データとしてＰＣやサーバのＨＤ、ＵＳＢメモリのようなメモリカード、ＣＤ－Ｒ、ＤＶＤといった各種のメディアに保管されていることと思われる。これらの電子データは情報漏洩が許されないものだけではなく、既に公開されている情報も含まれている。したがって、電子データといっても一律に取り扱うことは適当ではなく、重要度に応じた分類を行い、これに応じて管理をすることが一般的である。

なお、ここで管理の対象とすべき電子データは、業務上必要な電子データに限るべきであり、これらの電子データを扱う情報機器やメディアは、所有権の有無にかかわらず、公認会計士事務所（監査法人）の管理対象となる。また、不要となった電子データは廃棄・削除しなければならない。

(2)　重要度に応じた分類の方法

電子データについて重要度の判定を行うに際しては、通常対象となる電子データについては、以下の観点から重要性を決定する。

① 漏洩による影響

担当者の不正使用、担当者以外の事務所職員または外部からの不正アクセス、文書・媒体の複製または持出し、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、罰則の程度

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

③ 誤謬による影響

過失、改ざん等により、情報に誤謬を生じた場合の影響の度合い

本報告では情報の漏洩（紛失を含む）に焦点を当てているため、分類の方法としては原則として上記の重要性に応じた秘密度（取扱や閲覧をできるものの度合）を基本

とするのが適当と考えている。

具体的な分類の例としては、下記が考えられる。

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。

(3)　分類に応じた管理

情報漏洩を防ぐためには、分類に応じた管理方法や保管期限を明確にしておく必要がある。情報の分類に応じた管理を適切に行わない場合、重要な情報を十分ではないレベルで管理してしまう可能性がある。また、逆に、保管期限を過ぎた情報や重要でない情報を不必要なレベルで管理する可能性もあり、その方針はそれ自体では問題はないかもしれないが、いたずらに煩雑な管理は情報セキュリティ担当者や利用者の負担が増すばかりで、情報の流通を阻害し、結果として管理が実施されないこととなってしまう可能性がある。

なお、情報はクライアント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、一度分類した管理を固定するのではなく、定期的に見直す手続きが必要である。

２．リスク分析と対応方法

(1)　扱っている電子データの重要度に応じたリスクの認識

後述するように、情報セキュリティを維持するためには、情報セキュリティ対策の方針（セキュリティ・ポリシー）を定めなければならない。前述した電子データの分類に応じて、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のである。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い。したがって現実的なセキュリティ・ポリシーを策定するためには、まずリスク分析を行う必要がある。リスク分析は、電子データの列挙とその電子データが漏洩したときの影響を分析することによって行うこととなる。

一般的な方法として、第一に、電子データを重要度が高い順番で列挙する。使用制限のない公開情報は列挙しないでもよいと考えられる。第二に、その電子データの所有者（あるいは管理者）を特定する。もし、所有者または管理者が特定されていないのであれば、そもそも管理レベルが十分でないデータが存在している可能性を示すかもしれない。当面、そのデータの管理者は作成者とみなして作業を進めるのが現実的である。第三に列挙した電子データが漏洩した場合に与える影響（脅威の大きさ×発生の可能性の大きさ）を測定する。影響の大きな電子データから考慮すべき対象とすべきである。第四に現在の管理状況を考慮すれば、最終的に、電子データ・対応するリスク・現状の管理状況の一覧が作成できる。

このようなリスク分析の結果、例えば「スタッフが持ち歩くノートＰＣに入っているクライアントの非公開情報についてリスクが大きく、現状ではその管理はそれぞれのスタッフに任されている」といった結果を得ることができる。なお、公認会計士事務所（監査法人）の場合、電子データの列挙に際し、最初から詳細かつ網羅的に行おうとするのではなく、思いつくままに重要な電子データを挙げていけばよいし、「監査調書」「クライアントの経理データ」「クライアント作成の資料」のように大きな括りで挙げてもよいと考えられる。

(2)　当該リスクへの対応方法

リスク分析の結果に基づいて現実的に実行可能なセキュリティ・ポリシー（基本方針）や細則を作成し、リスクを低減することとなる。しかし、全てのリスクをセキュリティ・ポリシーなどのルールでカバーする必要はなく、また、カバーしきれないことも十分考えられる。この場合、リスクの原因となる業務そのものを行わないことや、別の手順で実施することを検討してもよい。例えばメモリカードのように容易に扱えてしまう媒体が紛失の可能性を増加させているのであれば、その利用を禁止するといったことが考えられる。リスクへの対応方法には複数の方法があり、リスクの回避や移転（保険を掛けるなど）についても検討することが望ましい。リスク分析を十分に行うことによって、電子データの重要度に応じた、現実に即した必要十分なセキュリティ・ポリシーを設定し、運用することが可能になる。

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。情報セキュリティ担当者は、サーバ等のハードウェアのセキュリティ設定を実施したり、利用者への指導を担当する。利用者は自らのＰＣに安全なパスワードを設定したり、情報セキュリティ担当者の指示に従ってソフトウェアのアップデートを行う必要がある。以後の章では経営者、情報セキュリティ担当者、利用者の役割について詳しく述べる。

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、電子データ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とらえ、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。

２．必要な情報セキュリティ対策

電子データ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、従業員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

・物理的安全対策

例えば、電子データの保管場所に対する入退管理の実施、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、ウィルス対策ソフトの導入

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。

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、組織内における情報セキュリティ対策の方針（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らなければならない。

３．セキュリティ・ポリシーの策定

セキュリティ・ポリシーとは、電子データ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、経営のトップが明文化した、セキュリティに対する「経営方針」である。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。

一般にセキュリティ・ポリシーの策定に当たっては、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するが、ここでは公認会計士の守秘義務の観点から情報漏洩防止を中心に記述する。

４．セキュリティ・ポリシーの内容

(1)　情報の分類

公認会計士事務所（監査法人）の業務において守秘義務の対象となる情報の種類を把握するために、取扱う情報の量や内容に応じて情報の重要度の分類を行うことが必要である。

業務上での重要な情報としては、例えば以下の情報がある。

・監査調書
・クライアントの経理データ、税務申告データ
・マネジメントレター
・税務申告書
・クライアント作成の資料
・クライアントとの守秘義務契約により指定された情報
・業務を通じて知ったクライアントのインサイダー情報
・クライアントから得た、会社組織のノウハウ（マニュアル、事例)、人事、経営情報等

上記の情報は、同一の内容であっても、クライアントの状況や時点によって情報の重要度は異なり、クライアントのセキュリティ・ポリシーによっても取扱いが異なる。上記の情報に関係していること自体が守秘義務の対象となるケースもある。

(2)　セキュリティ対策

経営者は、上記の情報の重要度に応じて対策を規定し、規程化の程度を検討する必要がある。また下記の観点から、当該情報の使用（電子メール、電子媒体、紙、日常会話など）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）
・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）

(3)　セキュリティ管理体制

セキュリティ管理実施にあたり、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。

(4)　セキュリティ・ポリシーの構成

セキュリティ・ポリシーは、本人だけでなく公認会計士事務所（監査法人）職員（派遣、パート、アルバイトを含む）等（以下、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（基本方針）
・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）

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５～８に記載するような適切な統制活動が必要である。

５．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、すべ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。

６．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を検討し、改善に努めなければならない。

７．情報セキュリティに関する研修の実施

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したがって組織内部で電子データを適切に取扱うためには、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の発達などにより絶えず変化するものであることから、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望ましい。すなわち経営者は研修の実施時期・実施方法、研修テーマについて適切に検討のうえ、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。

８．メール等によるデータ交換の方針

インターネットや電子メールの急速な普及、またＵＳＢメモリのような手軽なリムーバブル・メディアの登場によって、大量のデータが瞬時にして一度にやりとりができるようになり、業務の効率アップに大きく寄与している。しかし一方でネットワーク上でのデータ送信時の盗聴・改ざんやファイル交換ソフトを介したデータの漏洩、あるい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データの流出、といった危険性も高まっている。

経営者はこうした事態に適切に対処し、漏洩等のリスクを軽減させるための方針を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。

９．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、体制、対応策などを「緊急時対策」として整理し、連絡方法については全職員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。

また、漏洩した情報に個人情報が含まれている場合、「金融分野における個人情報保護に関するガイドライン」「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」に従った手続が必要になるため、個人情報取扱事業者たる公認会計士事務所（監査法人）は、金融庁への届出を行い、二次被害の防止、類似事案の発生回避の観点から、当該事実関係及び再発防止策の公表、漏洩事案等の対象となった本人への通知を行うことが必要である。

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、問合窓口等に係わる人件費、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。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、経営者が実施した電子データの重要度分類の結果に基づき、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、定期的及び職務権限変更時に見直さなければならない。

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．ウィルス対策

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、事務所所有のＰＣやサーバ等のコンピュータにウィルス対策ソフトを導入するとともに、

導入後も最新のパターン・ファイルに更新しなければならない。また、情報セキュリティ担当者は、ウィルス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取り外すとともに、情報セキュリティ担当者に報告するような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。特にファイル共有型のソフトウェアについては、データ漏洩の危険性が極めて高いため、その取扱には十分留意することが求められる。

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、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テストを行ったのち、利用者に対して対策プログラムの配布とインストールを指示することが必要である。

サポート期間が終了したＯＳ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、サポート期間が終了したＯＳを搭載しているＰＣやサーバをネットワークに接続する場合には、十分留意することが求められる。

７．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ノートＰＣ、ＵＳＢメモリ等の使用に関する方針を定めなければならない。最低限、機器に備わっているセキュリティの機能を使用することが適当である。

８．電子データや情報機器の廃棄にあたっての留意点

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。

９．データ交換の際の留意点

情報セキュリティ担当者は、データ交換の際の情報漏洩を防ぐため、交換される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メモリ等によるデータ交換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。

Ⅵ. 利用者の役割

１．利用者の役割

ＰＣ等の利用者は、ＰＣ等を紛失するとデータ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、まず盗難紛失が生じないよう防止策を施さなければならない。また、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。

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、重要度（Ⅲ．電子データの分類とリスク分析・対応の１．(2) を参照）を勘案し、その紛失や漏洩が発生しない様に、決められた運用方針に基づき慎重に取り扱う。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。

(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。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。

３．パスワード管理

(1)　パスワードをメモしない

パスワードをメモした手帳等を紛失する事により、パスワードが漏洩する可能性がある。不正なパスワードの搾取を防ぐために、パスワードそのものを手帳等にメモすることは厳に控える必要がある。

(2)　パスワードの定期的な変更

同一のパスワードを使い続けることにより、パスワードが漏洩する危険性が高まるので、経営者の定めた方針に従って、定期的にパスワードを変更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・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、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等の携帯型記憶媒体等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事が多く、紛失する危険性がより高いため、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ウィルスに感染したり、情報機器内のデータがネットワーク上に漏洩・流出する可能性があるため、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注意することが必要である。特に無線ＬＡＮについては、有線ＬＡＮ以上にネットワーク形態の自由度が高まっているため、セキュリティ管理を十分に行うことが必要である。

(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等の携帯型記憶媒体等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事が多く紛失する危険性が高い。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や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．電子データ交換の際の留意点

(1) 業務上必要な範囲での電子データの交換

電子データには、その物理的なサイズに比し大量の電子データが含まれていることが多く、当該データが紛失した場合には、大規模な漏洩が発生する可能性がある。また、交換が容易な事から、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があるため、業務上必要な範囲で当該データの交換を行う。

(2) メールを利用して電子データ交換を行う場合

メールを利用して交換する際には、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。またメールの搾取等による情報漏洩を防ぐため、経営者の定めた方針に従い、交換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)　携帯型記憶媒体を利用して電子データの交換を行う場合

当該データをＵＳＢメモリ等の携帯型記憶媒体にて交換する場合には、電子データを保管したまま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に従い、交換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交換を行い、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．ウィルス対策

(1)　ウィルス対策ソフトの利用

使用するＰＣは、経営者の定めた方針に従い、ウィルス検知用のパターン・ファイルを常に最新版に更新しなければならない。また、定期的にウィルスチェックを行わなければならない。

(2)　ウィルスに対する対応

事務所内の情報システム部門等からのウィルス関連情報に留意し、不審な電子メールを受信した場合や、利用しているＰＣが原因不明で挙動が安定しない場合など、ウィルス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を取り外し、その上で、情報セキュリティ担当者に報告し、適切な対策を行う。

(3)　ウィルスに感染した場合

ウィルス対策ソフトによる通知等で、利用しているＰＣが、万一ウィルスに感染した場合には、直ちに当該ＰＣを事務所ネットワークから取り外し、経営者の定めた方針に従って、情報セキュリティ担当者に報告し、必要な対策を行う。

(4)　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より、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。

(5)　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．紙媒体等の情報セキュリティ

(1)　ＰＣ以外のセキュリティ対策

業務上入手した紙媒体の情報等を収納したかばん等の紛失・盗難により、当該情報

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、クライアントの入館証等については紛失時の影響が大きいため、きわめて慎重に対応することが必要である。また、セキュリティ対策を施した電子データと異なり、紙媒体の情報については、紛失がそのまま漏洩につながる事に十分留意する。

(2) 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プリントアウトした場合には、プリントアウトした紙を放置する事による情報漏洩を防止するため、遅滞なくプリントアウトした紙の回収を行うことが必要である。

(3) 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様、送信者と連携を図り、受信ＦＡＸの遅滞ない回収を行うことが必要である。

Ⅶ. 適用時期

本報告は、平成 20 年４月１日以後開始する事業年度に係る業務から適用する。ただし同日前に開始する事業年度に係る業務から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）および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。ただし、本報告を適用する事業年度前の事業年度に係る業務においては、同報告を利用する。

以　上