監査・保証基準委員会実務指針第５号

公認会計士業務における情報セキュリティに関する実務指針

２００８年１月16日
改正　２０１０年３月19日
改正　２０１２年８月30日
改正　２０１６年７月25日
改正　2020年10月23日
改正　2022年10月13日
最終改正　２０２３年７月28日
日本公認会計士協会

項番号

Ⅰ　本実務指針の範囲及び目的
　１．本実務指針の範囲及び目的 1
　２．背景 6
　３．定義 10
Ⅱ　要求事項 11
Ⅲ　適用指針
　１．情報セキュリティ管理の重要性
　　(1) 情報漏えいのリスク A1
　　(2) 情報の不正又は私的利用のリスク A2
　　(3) ＩＴの進歩に対応する情報セキュリティ A3
　　(4) 紙媒体の情報セキュリティ A4
　　(5) サイバーセキュリティ A5
　２．情報漏えいに関するリスクの識別と対応
　　(1) 業務の理解、関連する内部統制の識別、リスクの識別 A6
　　(2) 識別したリスクへの対応 A7
　　(3) 緊急時を想定したリスク対応 A8
　　(4) 情報の重要度 A9
　　(5) セキュリティ・ポリシー A10
　３．経営者の役割
　　(1) 経営者の役割 A11
　　(2) 情報セキュリティ対策 A14
　　(3) セキュリティ・ポリシーの策定 A16
　　(4) トップダウンによる周知徹底 A17

(5) 遵守状況の把握と対策 A18
(6) 情報セキュリティに関する教育研修の実施 A19
(7) 電子データ授受の方針 A20
(8) 紙媒体に関する文書管理の方針 A21
(9) クラウドサービス等を含む外部委託先等の管理 A22
(10) サイバーセキュリティ対応 A23
(11) 情報漏えい時の対応 A24
４．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 A25
(2) 電子データに対するアクセス権限の設定と管理 A26
(3) パスワードの設定と管理 A27
(4) 電子データのバックアップと管理 A28
(5) 外部ネットワークとの接続管理 A29
(6) マルウェア対策 A30
(7) サポート期間が終了したＯＳやソフトウェアの利用禁止 A31
(8) 情報機器に対するセキュリティ対策 A32
(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 A33
(10) 電子データ授受の際の留意点 A34
(11) 紙媒体の情報セキュリティ上の留意点 A35
(12) クラウドサービス等の利用の際の留意点 A36
(13) SNS の利用ポリシー A37
(14) 情報資産台帳の作成と棚卸 A38
(15) セキュリティ対策の実効性に関するモニタリング A39
５．利用者の役割
(1) 利用者の役割 A40
(2) 電子データの管理 A43
(3) パスワードの管理 A44
(4) 電子データのバックアップ A45
(5) 外部ネットワークへの慎重な接続 A46
(6) マルウェア対策 A47
(7) サポート期間が終了したＯＳやソフトウェアの利用の禁止 A48
(8) 情報機器の管理 A49
(9) 情報機器やバックアップ媒体の廃棄 A50
(10) 電子データ授受の際の留意点 A51
(11) 紙媒体等の管理 A52
(12) クラウドサービス等の利用の際の留意点 A53
(13) SNS 利用の際の留意点 A54
Ⅳ　適用

《Ⅰ　本実務指針の範囲及び目的》

《１．本実務指針の範囲及び目的》

１．本実務指針は、公認会計士業務（公認会計士事務所等が行う業務をいう。）において留意すべき情報セキュリティに係る実務上の指針を提供するものである。

２．情報セキュリティにおいては、情報の機密性、完全性及び可用性の維持が求められるが（秘密性：アクセスを認可された者だけが、情報にアクセスできることを確実にすること、完全性：情報及び処理方法が正確であること、及び完全であることを保護すること、可用性：認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。）、本実務指針では、その中で秘密性（紛失、不正又は私的利用を含む。）に焦点を絞っている。

３．本実務指針の対象とする情報の形態は、電子データだけではなく紙媒体を含み、その範囲は関与先から入手した情報等、主に業務に直接関係する情報である。公認会計士事務所等の職員・経理に関する情報等、業務に直接関連しない情報についても、本実務指針を参考にして情報セキュリティ体制を構築することが想定される。

４．本実務指針においては、公認会計士事務所等が情報セキュリティ体制を構築するに当たっての具体的な指針を提供しているが、公認会計士事務所等は、公認会計士事務所等が支配する事業体についても、本実務指針に準じた情報セキュリティ体制となるよう監督することが求められる。

５．本実務指針は、会員が秘密保持の義務（公認会計士法第27条、倫理規則R114.1項からR114.3項等参照）の遵守のために、秘密情報の紛失、漏えい等を防止する体制の構築に関連している。また、本実務指針は、品質管理基準報告書第１号「監査事務所における品質管理」を適用する監査事務所において、職業倫理の構成要素に関する品質目標の設定、品質リスクの識別及び評価並びに対応（品基報第１号第７項、第８項及び第29項参照）を情報セキュリティに係る領域について行う場合にも関連している。

《２．背景》

６．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、関与先等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。）等を始めとする情報機器を持ち歩き、関与先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。データ分析のために大量のデータのやり取りを行うことや、公認会計士が事務所外部のリソース（サービス）を活用し情報を取り扱う事も一般的になってきている。

７．公認会計士は、これらの情報の重要性を認識し、紛失や漏えいへの対応を行っているが、紛失や漏えい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重要である。また、不正・私的利用という観点だけではなく、サイバー攻撃による情報詐取、破壊等や、RPA（Robotic Process Automation）やＡＩ（Artificial Intelligence）等、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が重要と考えられる。

８．関与先等から入手した情報が外部に漏えいした、又は、不正の目的若しく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関与先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、従来からの秘密保持の意味を再認識し、電子データだけではなく紙媒体の情報も含めた、特に関与先等に関する情報の漏えい・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、その対策を検討することが重要である。

9．「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」（2009 年 7 月 22 日付けＩＴ担当常務理事　会員・準会員宛メッセージ参照）ことを肝に銘じ情報セキュリティの確保に努めることが重要である。

《３．定義》

10．本実務指針における用語の定義は、以下のとおりとする。

(1) 「公認会計士等」－公認会計士事務所等に所属する会員、職員等をいう。ただし、公認会計士事務所等を除く組織所属の会員については含めない。

(2) 「公認会計士事務所等」－会員が業務を行うために開設した事務所及び監査法人をいう。

(3) 「関与先等」－被監査会社、コンサルティング等の顧客をいう。

(4) 「経営者」－本実務指針において、経営者とは、公認会計士事務所等における所長、理事長等の最高経営責任者等を指す。

(5) 「社員・職員等」－公認会計士事務所等の最高経営責任者等を除く社員・職員（派遣、パート、アルバイト等を含む。）をいう。

(6) 「外部委託先」－公認会計士等が何らかの外部のリソース（サービス）を利用している場合における当該リソース（サービス）を提供する企業等をいう。

(7) 「情報機器」－情報にアクセスするための機器のうち、通信機能を有しているものを指すもので、代表的な情報機器としてはＰＣ、スマートフォン、タブレット等がある。

《Ⅱ　要求事項》

11．公認会計士事務所等は、情報セキュリティに係るリスクの識別及び評価を行った上で、情報セキュリティに係る体制を整備及び運用しなければならない。

《Ⅲ　適用指針》

《１．情報セキュリティ管理の重要性》

《(1) 情報漏えいのリスク》

A1．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おり、情報機器の誤操作、移動時の紛失、盗難、マルウェアの感染等により、常に情報漏えいのリスクがあることを認識することが重要である。

《(2) 情報の不正又は私的利用のリスク》

A2. 公認会計士等が業務で入手した情報は、関与先等にとって非常に重要な秘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、公認会計士等は、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ことを認識することが重要である。

《(3) ＩＴの進歩に対応する情報セキュリティ》

A3. 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、公認会計士事務所等は、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ことが重要である。

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えいにつながりかねないことを認識することが重要である。

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等の対応が重要である。

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重要である。

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、事務処理ソフト等を、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することが重要である。

また、情報セキュリティレベルが高いサービスであっても、ユーザー側の設定を適切に行うことが重要である。ＩＤ、パスワードの管理、暗号化機能やバックアップ機能の利用に関する設定、情報公開範囲の設定等は公認会計士事務所等側で適切に行うことが重要である。

③ 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「HDD」という。）、CD-R、USB メモリ等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、漏えい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ことが重要である。

《(4) 紙媒体の情報セキュリティ》

A4. 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えいにつながる（又は不正利用の）リスクが高い。したがって、公認会計士事務所等は、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ことが重要である。

《(5) サイバーセキュリティ》

A5. サイバー攻撃は日進月歩で高度化されており、これまでの対策だけでは情報セキュリティを維持することが難しいケースも増加している。今後、公認会計士事務所等がＩＴを活用した監査やコンサルティングを行っていく場合に当該領域の対応を強化していくのはもちろんのこと、そうでない場合でも既存業務が日々高まるサイバーセキュリティリスクにさらされていることを強く認識することが重要である。

このような状況の下、公認会計士事務所等においては、経営上の最優先のリスクの一つとして、経営者の強いリーダーシップの下、組織的にその対策を進めていくことが重要である。この際に、業務の委託先や連携先についても連動した対策が必要であることにも留意する。

《２．情報漏えいに関するリスクの識別と対応》

《(1) 業務の理解、関連する内部統制の識別、リスクの識別》

A6. 公認会計士事務所等は、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、リスクを識別することが重要である。通常、識別したリスクは分析し、発現の頻度や影響の重要度を勘案して評価することとなる。特に、サイバー攻撃を受けることによる情報漏えいのリスク、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重要である。

また、上記の一連の手続については定期的な見直しが重要である。

《(2) 識別したリスクへの対応》

A7. 公認会計士事務所等は、上記で評価したリスクに対して、移転、回避、受容、低減といったリスクへの対応を選択することとなる。その結果、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、運用することが重要である。

なお、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重要である。

《(3) 緊急時を想定したリスク対応》

A8. 公認会計士事務所等は、外部からサイバー攻撃を受けている等、平時と環境が変わった場合を想定し、より情報セキュリティを高めた内部統制の運用を踏まえたリスク対応を事前に検討することが重要である。緊急時に設定される管理責任者の内外に対するコミュニケーションについても、平時では情報収集を基本とする安定運用が重視されるが、緊急時では限られた情報の中で意思決定を迫られる等、必要となる対応は状況に応じて変化することが想定される。平時より緊急時に必要な情報についても事前にすり合わせしておくことは、緊急時に困難な状況下においても

意思決定を行うのに有用と考えられる。

緊急時における対応を有効ならしめるためには、平時に実践演習を定期的に行う等、緊急時の対応を平時の対応に組み込むことも有効である。

《(4) 情報の重要度》

A9. 公認会計士事務所等がリスクを識別する際には、情報の重要度を考慮することが重要である。

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ことが考えられる。

- 漏えいによる影響
- 消失による影響
- 誤謬による影響

本実務指針では、情報の漏えい（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られる。

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、情報は関与先等の状況や時間の経過等に応じて、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重要である。

《(5) セキュリティ・ポリシー》

A10. 公認会計士事務所等が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）を定めることが重要である。セキュリティ・ポリシーでは、前述したリスクの識別の結果や情報の重要度に応じて、具体的なアクセス制御等の管理方法を定めることになると考えられる。しかし、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」なものでは形骸化する可能性が高く、現実的なセキュリティ・ポリシーを策定し、運用することが重要である。

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ことが重要である。また、状況に応じて、内容を見直すことも重要である。

情報漏えい、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、情報を適切に管理し、情報漏えいを防止する観点から重要と考えられる項目は、以下のとおりである。

① セキュリティ対策

識別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ことが重要である。また、下記の観点から、電子メール、電子データ、紙媒体、日常会話等の情報の使用に当たって留意すべき事項を網羅することが重要である。

・　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、警備等）
・　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（SNS（Social Networking Service）利用を含む。）等）
・　当該情報を伝達、保管する「手段及び媒体」の管理（ファイルサーバ、暗号化、媒体の保管、通信等）
・　外部ネットワークとの接続の管理（ファイアウォール、外部サービス等）
・　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等）

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ことが重要であり、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ことが考えられる。

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）

《３．経営者の役割》

《(1) 経営者の役割》

A11. 経営者は、情報漏えいのリスクの適時・適切な把握及び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する。

その責務を果たすために、また、公認会計士事務所等に属する全ての者が、情報セキュリティ上安心して業務に従事できる環境を整備するとともに、情報セキュリティ対策を導入することに伴う業務効率の低下による抵抗感を緩和するために、経営者はリーダーシップを発揮して情報セキュリティ対策を進めることが重要である。さらに、経営者は、公認会計士事務所等の内部はもちろんのこと、情報セキュリティへの取組に対する社会一般からの信頼を向上させるために、そのコミュニケーションの方法等を検討することが重要である。

A12. 経営者は、情報漏えいのリスクの適時・適切な把握のために、まず、対象となる情報資産の洗い出し、情報資産管理台帳の作成と適時な更新を行い、次に、把握した情報資産について、情報が漏えいした場合のリスクを評価し、適切な対策を検討することに留意する。

その対策を実施するためには、必要な予算と人材の確保に努めることが重要である。予算については、情報漏えい等の事故の発生防止のための対策だけでなく、継続的な情報セキュリティ研修等の教育の実施、情報漏えいや情報資産が利用できなくなる事故の発生を想定した緊急時の連絡体制の整備や模擬訓練の検討、事故発生による被害の拡大防止や、復旧対応も含めて考えるこ

とが有用である。識別している情報漏えいのリスクの程度、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）の設置についても検討することが考えられる。

A13. 情報漏えいは過失のみならず、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ことが重要であり、さらに、組織外部からのサイバー攻撃に対しても十分に留意する。

《(2) 情報セキュリティ対策》

A14. 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、一般的に考えられる対策を例示すると以下のとおりである。

- 組織的安全対策
  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
  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
  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
  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
  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・体制等によって異なることから、経営者はそれぞれの実態に応じた対策を講じることが重要である。その際、関与先等から公認会計士事務所等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、関与先等が考えている情報の重要度に応じた管理体制の構築を検討することが適切である。

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ることが重要である。

A15. 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経営者、情報セキュリティ担当者以外の社員・職員等（以下「利用者」という。）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等、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重要である。

《(3) セキュリティ・ポリシーの策定》

A16. 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、各種管理規程等と並ぶ「情報」の管理規程であり、これを遵守するためには以下の(4)から(11)に記載するような適切な統制活動が重要である。

《(4) トップダウンによる周知徹底》

A17. 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、全ての社員・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する。

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社員・職員等に一任するのではなく、対策の実現に向けて経営者が率先して指揮を取ることが適切であり、絶えず情報セキュリティの重要性を訴え続けることが重要である。

《(5) 遵守状況の把握と対策》

A18. 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、改善に努めることが重要である。

《(6) 情報セキュリティに関する教育研修の実施》

A19. 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、社員・職員等に対する教育研修が重要である。

情報セキュリティは、外部環境・内部環境の動向、ＩＴの進歩等により絶えず変化するものであることから、経営者は、教育研修に関しても社員・職員等の採用時、セキュリティ･ポリシーの見直し時等、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適切である。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。

SNS の利用は、自身の行動内容や写真を投稿したことをきっかけとして、関与先等の未公開情報が漏えいしてしまうことも考えられるため、経営者は、当該領域についても SNS に関する利用ガイドラインの策定、教育研修の実施、ネット上のモニタリング等、利用の程度とリスクに応じた対策を検討することが重要である。

《(7) 電子データ授受の方針》

A20. 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・改ざん、ファイル交換ソフトを介した電子データの漏えい又はメールアドレスの宛先違いによる誤送信やUSBメモリの紛失等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、漏えい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ることが重要である。一度の不正アクセスや操作ミスが大規模な情報漏えいにつながり、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。

《(8) 紙媒体に関する文書管理の方針》

A21. 監査調書や関与先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に留意する。経営者は、こうした紙媒体の紛失や盗難による情報漏えいを防ぐため、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ることが重要である。

《(9) クラウドサービス等を含む外部委託先等の管理》

A22. 情報漏えい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、社員・職員等の雇用形態の違いやネットワーク・ファームのような異なる組織の関与等によって生じる情報セキュリティへの意識差異が、情報漏えい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ことが重要である。

- 外部専門家の利用
- 外部委託先の利用
- 非常勤職員による情報の取扱い
- 公認会計士事務所等のネットワーク・ファームとの情報のやり取り

また、サーバや業務ソフト等の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、クラウドサービスとして広く一般に提供されているもの等、様々な形態が存在するため、情報漏えいに対する備えも異なっていることが考えられる。

このような場合には、少なくとも、法人向けサービスを利用し、自己の公認会計士事務所等と同程度以上の情報セキュリティ対策が実施されているかどうかを確かめることが重要である。また、外部委託先等の選定及び契約に当たっての基準やプロセス、サービス利用開始後の継続的な状況のモニタリング等、リスクに応じたマネジメントプロセスを構築することも重要である。

《(10) サイバーセキュリティ対応》

A23. サイバー攻撃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。攻撃者は秘密情報詐取等の目的を成功させるまで、ターゲットに対して執拗に、ソーシャルエンジニ

アリングやフィッシングメール等を駆使するという特性がある。

このようなことから、組織への入口で完全に阻止することは困難であり、内部への侵入を前提とした対策を講じることが重要である。

この場合でも、経営者は、「２．情報漏えいに関するリスクの識別と対応」に従って、リスクの識別、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重要である。

① 社員・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、情報漏えい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重要である。

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、又は、実行できていない場合には、情報漏えいのリスクが非常に高まっていると考えられる。

経営者は、管理すべき情報が特定され、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重要である。これらが実施されていない場合、情報漏えいのリスクが非常に高まっていると考えられ、情報漏えいとなった場合、被害状況の把握や情報漏えい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。

侵入や攻撃を検知し駆除するための入口対策、侵入や攻撃を受けたとしても情報を外部に流出させない出口対策及びこれらと連携した情報機器ごとのセキュリティを確保するための内部対策が重要である。業務上使用する情報の量や重要性、識別している情報漏えいのリスクの程度によって必要なセキュリティレベルを確保することが重要であり、利用者啓発・対応施策の効果予測の為にもサイバー攻撃対応演習等を実施することは有用であると考えられる。

③ 事案発生時の対応方法の確認・見直し

サイバー攻撃による情報詐取の事案等が発生した場合の対応方法が社員・職員等に周知され、理解されていることが重要である。また、事案等の発生を想定した訓練を定期的に実施し、周知や理解の状況を確かめることが望ましい。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 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り、通信記録（ログ）を取得・分析することが有効な場合がある。経営者は、情報漏えいが発生していないかどうか、例えば一定期間ごとに通信記録（ログ）を取得・分析する体制を構築する等、リスクに応じたモニタリングの仕組みについて検討することが重要である。また、通信記録（ログ）を取得する場合には、通信記録（ログ）を安全に保管するために適切な改ざん・削除防止策を講じることが有用である。

《(11) 情報漏えい時の対応》

A24. 情報漏えい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、漏えい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重要となる。そのため、経営者は、情報漏えいが起きた際の連絡方法（報告先、報告方法を含む。）、体制、対応策等を「緊急時対策」として整理し、連絡方法（報告先、報告方法等を含む。）については全社員・職員等に周知徹底しておくことが重要である。なお、漏えいした場合に備えて、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ネットワーク・ファームでの情報漏えいの発生時等、自らが直接把握できない場合の把握方法の検討は重要である。

情報漏えい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。

《４．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》

A25. 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役割を担っている。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ることが重要である。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》

A26. 情報セキュリティ担当者は、経営者が実施したリスクの識別の結果に基づき、電子データに対するアクセス権限の設定方針を定めることが重要である。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うことになる。

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・変更を行うことが重要である。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することが重要である。

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（公認会計士事務所等の内部者・外部者の区分を問わない。）の不正・私的利用による情報漏えいは起こり得る。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等のモニタリングの導入による抑止力の必要性について、検討する。

《(3) パスワードの設定と管理》

A27. 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、パスワードの使い回しを含めた取扱いや有効期限等のパスワード管理方針を定めることが重要である。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ることとなる。

《(4) 電子データのバックアップと管理》

A28. 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ることが重要である。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することとなる。

《(5) 外部ネットワークとの接続管理》

A29. 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公認会計士事務所等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公認会計士事務所等からの情報漏えいを防ぐために、適切に設定されたファイアウォール等の設置を検討する。

《(6) マルウェア対策》

A30. 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することが重要である。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、閲覧可能なウェブサイトを検討・制限するとともに、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ことが考えられる。

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を公認会計士事務所等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を整備することが重要である。

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することが重要である。

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適切である。

《(7) サポート期間が終了したＯＳやソフトウェアの利用禁止》

A31. サポート期間が終了した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、情報セキュリティ担当者は、その利用を停止し、新しいバージョンのもの又はサポート提供期間内にある別製品に速やかに移行することが重要である。

《(8) 情報機器に対するセキュリティ対策》

A32. 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えいを防ぐため、暗号化や推測が困難なパスワードを設定する等、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等、一定レベルのセキュリティを施すことが重要である。

《(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》

A33. 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HDD等の記憶媒体やCD-R等のバックアップ媒体からの情報漏えいを防ぐため、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等、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、利用者に周知することが重要である。

《(10) 電子データ授受の際の留意点》

A34. 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えいを防ぐため、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等の電子メールやUSBメモリ等による電子データ授受に関する方針を定めることが重要である。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ることが重要である。

《(11) 紙媒体の情報セキュリティ上の留意点》

A35. 情報セキュリティ担当者は、紙媒体の情報漏えいを防ぐため、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ることが重要である。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えいのリスクも十分に留意する。

- 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えい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》

A36. クラウドサービス等を利用する際には、情報セキュリティ担当者は、特にA26項からA28項に記載した事項に留意する。

《(13) SNS の利用ポリシー》

A37. 個人でSNSを利用する場合、意図せず情報漏えい等につながる可能性がある。これを防止するため、情報セキュリティ担当者は、社員・職員等のSNSの利用状況に応じ、SNS使用に関するポリシー等を定める。

《(14) 情報資産台帳の作成と棚卸》

A38. 公認会計士事務所等で所有する情報が多岐にわたる場合、情報セキュリティ担当者は、どのような情報を所有しているかを把握するために情報資産台帳を作成することが有用な場合がある。

情報資産台帳に基づき所有する情報を定期的に棚卸することで、情報の漏えいや意図しない削除を早期に検出でき、不必要な情報については定期的に削除することで将来の情報漏えいリスクを低減させることができる。

《(15) セキュリティ対策の実効性に関するモニタリング》

A39. 情報セキュリティ担当者は、情報セキュリティに係る内部統制に関連して、リスクの高い項目を中心とした定期的なモニタリングを行うことも検討する。例えば、各個人のＰＣの中で情報区分に基づいた管理が行われているか、サポート期間が終了したＯＳの使用がないか期限切れの一定期間以前に棚卸を実施する、必要なパッチが当たっているかどうかを確認する、電子データのバックアップログを確認する等、公認会計士事務所等でルール化された統制が正しく運用されているか確かめるといったことが考えられる。

また、外部委託先を利用する場合には、定期的な報告を求めたり、保証業務実務指針 3702「情報セキュリティ等に関する受託業務の Trust に係る内部統制の保証報告書に関する実務指針」等に基づいて発行された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重要である。

《５．利用者の役割》

《(1) 利用者の役割》

A40. 通常、利用者は、経営者の策定したセキュリティ・ポリシーを遵守し、公認会計士事務所等の定める管理策を実行することが求められる。

媒体を問わず、情報機器を紛失すると情報漏えいの可能性が生じ、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管理策を理解し、実行することが重要である。

利用者は業務遂行のため情報機器の利用が不可欠であり、業務中は紙媒体の書類のほかに、常に電子データを取り扱っている。したがって、利用者は情報機器を利用する上での情報セキュリティのリスクを十分認識し、自ら積極的に考え、行動することが求められる。このためには、利用者は、指定された情報セキュリティに関する研修を受講するのみならず、報道等から最新の脅威にも注意を向け続けることに留意する。

A41．通常、利用者は、不審なメールを受信した場合等インシデント又はその疑いを識別した場合やセキュリティ上の課題を認識した場合、情報セキュリティ担当者へ通知することが求められている。

A42．A43項からA54項に記載した事項は、公認会計士事務所等において求められる、一般的な管理策の例示である。

なお、リスクについて詳細に記載されている「４．情報セキュリティ担当者の役割」の項も併せて参考にすることが望ましい。

《(2) 電子データの管理》

A43．通常、経営者の定める方針に従い、次のような管理策を実行することが利用者に求められる。

① 電子データの管理

電子データについては、その紛失や漏えい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う。特に電子データを保存した状態で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えい被害を可能な限り低減させるために、情報機器に保存する電子データをできるだけ限定することに留意する。また、情報機器内に保存している電子データを定期的に点検することにより、当座必要でない電子データを公認会計士事務所等のサーバ等の安全な場所に移し、常に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。

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、電子データが漏えいする可能性があるため、個人用ＰＣと業務用ＰＣは明確に区別する。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。

《(3) パスワードの管理》

A44．通常、経営者の定める方針に従い、次のような管理策を実行することが利用者に求められる。

① パスワードのメモ

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、離席時に盗難に遭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も紛失や盗難に遭うと、情報が容易に漏えいする可能性がある。パスワードを手帳にメモする場合には、パスワードの一部を伏せる、パスワードに不要な文字を追加する、何のためのパスワードか明示しない等の配慮をする。

② パスワードの強度

パスワードは、長さ（文字数）、大文字小文字、数字、記号の組合せ等、経営者の定めた方針に従った強度のパスワードを設定する。

③ パスワードの使い回しの禁止

個人で利用しているウェブサイト等からパスワードが流出した場合に備え、業務で使用するパスワードは、個人で利用するものと異なるものとし、使い回しを避ける。

《(4) 電子データのバックアップ》

A45. 電子データの滅失等により業務の継続に大きな困難が発生しないよう、利用者は、情報機器に保存している電子データについて、経営者の定める方針に従い、定期的にバックアップをとることが適切である。

《(5) 外部ネットワークへの慎重な接続》

A46. 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えい・流出するといった可能性がある。また、有線、無線を問わず、無料サービス等は、運用者が信用できない場合もあり、マルウェアの感染のほか、覗き見、データの窃盗等のリスクがあるため、利用者は不用意にネットワークに接続しないように留意する。

《(6) マルウェア対策》

A47. 通常、経営者の定める方針に従い、次のような管理策を実行することが利用者に求められる。

① マルウェア対策ソフトの利用

業務用ＰＣは、マルウェア対策ソフトをインストールし、マルウェア検知用のパターン・ファイルを常に最新版にし、定期的にスキャンを実行する等して、感染リスクを下げる。

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発信される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警告が表示された場合等、マルウェアに感染した可能性がある場合には、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、情報セキュリティ担当者の指示に従い、適切な対応を行う。

③ ソフトウェアのセキュリティ・ホール（脆弱性）対応

新たな脆弱性を悪用した情報漏えい等を防ぐため、情報セキュリティ担当者から配付される、ＯＳやソフトウェアの脆弱性修正プログラムを、利用者は適時に適用・更新する。

④ あらかじめ決めら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又は指定されているもの以外のソフトウェアを使用する場合は、インストール許可申請等、所定の手続に従うものとし、許可なく使用しない。

《(7) サポート期間が終了したＯＳやソフトウェアの利用の禁止》

A48. ＯＳやソフトウェアにはサポート期間があり、この期間が終了すると、セキュリティ上の欠陥（脆弱性）が新たに発見されても、これを補修するセキュリティ対策プログラムが提供されない。このため、利用者は、期間終了までにサポートを受けられるバージョンに移行することが重要である。特に、業務用ＰＣとして、個人所有のＰＣを使用している場合、留意する。

《(8) 情報機器の管理》

A49. 通常、経営者の定める方針に従い、次のような管理策を実行することが利用者に求められる。

① 業務で使用する情報機器

公認会計士事務所等の許可なく、外部記憶媒体や情報機器を持ち込み、又は購入し業務で使用しない。電子メール等の保存される電子データについても配慮するため、個人所有のスマートフォンについても経営者の定める方針に従って使用する。

② 情報機器等の取扱い

情報機器の紛失・盗難・破損・汚損等の防止に留意し、情報機器を安全に管理する。また、移動時に情報機器を携行する場合や、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、情報機器を慎重に取り扱う。

特にノートＰＣや、USB メモリ等の外部記憶媒体については、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・携行方法に留意する。

③ 電子データの暗号化の実施

情報機器の紛失に伴う電子データの漏えいを防止するため、情報機器や、外部記憶媒体内に保存されているデータに対し、暗号化や推測が困難なパスワードを設定する。

④ 覗き見への配慮

情報機器により、交通機関内や店舗等の場で電子メール等を見る場合、紙面資料と同様に、画面を覗き見られることによる情報漏えいに留意する。

《(9) 情報機器やバックアップ媒体の廃棄》

A50. 電子データは、情報機器内で削除したとしても、容易に復元することが可能である。このため、利用者は、業務やバックアップで使用した外部記憶媒体や情報機器を廃棄する場合、情報セキュリティ担当者に依頼する、又は物理的に破壊する等、経営者の定める方針に従って実施することが重要である。

《(10) 電子データ授受の際の留意点》

A51. 通常、経営者の定める方針に従い、次のような管理策を実行することが利用者に求められる。また、授受等に当たっては、関与先等のセキュリティ・ポリシーも勘案することが必要になる場合があることに留意する。

① 必要な範囲に限定した電子データの入手

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、大規模な情報漏えい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、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も高まる。したがって、業務上必要な範囲で当該データの入手を行うとともに、更に取捨選択し、監査調書として必要な電子データのみが保存されるようにする。

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電子データを送信する際には、宛先を誤ることによる情報漏えいを防ぐため、宛先が正当な受信者であることを送信前に確認する。また、電子メールの詐取等による情報漏えいを防ぐため、メールの本文には、秘密に係る内容を記載しないことが重要である。さらに、メールに添付するファイルに対しては、関与先等と合意した方針に従い、暗号化や推測が困難なパスワードを設定する。

③　外部記憶媒体を利用して電子データの授受を行う場合

USB メモリ等の外部記憶媒体で電子データを授受する場合には、紛失する可能性が高いため、保存す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。また、速やかに電子データの授受を行うとともに、外部記憶媒体から当該データを削除する。

《(11) 紙媒体等の管理》

A52. 通常、経営者の定める方針に従い、次のような管理策を実行することが利用者に求められる。

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、入手者は誰でも容易に閲覧することが可能なことから、紙媒体の紛失がそのまま情報漏えいにつながることに留意し、慎重に取り扱う。

②　紙媒体等の管理

紙媒体の情報等を収納した鞄の紛失や盗難、作業現場での紙媒体の放置等により、情報漏えいする可能性があることに配慮して、その保管・管理を行う。特に公表前の決算書ドラフトや関与先等の入館証等については紛失時の影響が大きいため、慎重に対応することに留意する。

また、紙媒体の情報等を廃棄する場合には、情報の重要度に応じた適切な方法で廃棄を行う。

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、印刷物の放置による情報漏えいを防止するため、速やかに印刷物の回収を行う。

④　FAX 資料の管理

FAX 送信には、宛先誤りによる漏えいを防ぐために、宛先に適切な受信者が指定されていることを、送信前に確認する。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。

《(12) クラウドサービス等の利用の際の留意点》

A53. クラウドサービス等を利用する際は、データの保存を伴うことが多いため、通常、利用者は、公認会計士事務所等で許可したサービス以外は利用しない。また、利用に当たっては特にA43項及びA44項に記載した事項に留意することが重要である。

また、ウェブ上の翻訳サービス等の使用に当たっては、その翻訳元データがサービス提供者によって収集されることに留意する。

《(13) SNS 利用の際の留意点》

A54. 利用者が個人でSNSを利用する際には、業務に関する事項の書込みや情報の掲載を行わない。

《Ⅳ　適用》

・　本報告は、2008 年１月 16 日に発効し、2008 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」（2004 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」（2006 年１月 17 日）は廃止する。

・　「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」（2010 年３月 19 日）は、2010 年７月１日以後開始する事業年度から適用する。

・　「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」（2012 年８月 30 日）は、2012 年７月１日以後開始する事業年度から適用する。

・　「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」（2016 年７月 25 日）は、2016 年７月１日以後開始する事業年度から適用する。

・　「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」（2020 年 10 月 23 日）は、2021 年４月１日から適用する。

・　本実務指針（2023 年７月 28 日）は、2023 年８月１日から適用する。

以　　上

・　本実務指針（2022 年 10 月 13 日改正）は、次の公表物の公表に伴う修正を反映している。
－　監査基準報告書（序）「監査基準報告書及び関連する公表物の体系及び用語」（2022 年７月 21 日改正）