

## 公認会計士業務における情報セキュリティの指針に係るQ & A (実務ガイダンス)

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 1 月 13 日  
最終改正 2022年 10 月 13 日  
日本公認会計士協会  
監査・保証基準委員会  
(実務ガイダンス:第2号)

### 目 次

	頁
1. 本実務ガイダンスの目的.....	1
2. 本実務ガイダンスにおける用語の定義.....	1
3. Q&A.....	3
I はじめに.....	3
Q 1 品質管理基準報告書第1号実務指針第1号の2020年10月23日付けの改正のポイントを教えてください。また、本実務ガイダンスの2022年1月13日付け改正の内容を教えてください。.....	3
Q 2 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。.....	3
Q 3 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」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、品質管理基準報告書第1号実務指針第1号との関係を教えてください。.....	3
Q 4 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。.....	4
Q 5 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。.....	5
Q 6 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。.....	5
II 情報セキュリティ管理の重要性.....	5
Q 7 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。.....	5
Q 8 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のでしょうか。.....	6
Q 9 公認会計士業務を遂行するに当たり非常勤者や業務委託先など外部の人材や、クラウドなど	

の外部サービス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。.....	6
Ⅲ 情報漏洩に関するリスクの認識と対応.....	7
Q10 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。...	7
Q11 外部の委託業者との間で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な点について注意すればよいでしょうか。.....	7
Q12 ICT(情報通信技術)の進展に伴う業務環境の変化に対して、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。.....	8
Ⅳ 経営者の役割.....	9
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、特に留意すべき点がありますか。.....	9
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。.....	10
Q15 どのようにしたら情報セキュリティの意識を社員・職員全員が持つようになりますか。..	10
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。.....	10
Q17 「9. クラウドサービス等を含む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。.....	11
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、オンライン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。.....	11
Q19 ファイルサーバや仮想デスクトップ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。.....	13
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何でしょうか。.....	13
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、留意すべき点がありますか。.....	14
Q22 電子データ授受に関する方針を定める上で留意する点を教えてください。.....	15
Ⅴ 情報セキュリティ担当者の役割.....	15
Q23 情報機器や電子ファイルの暗号化で利用するIDやパスワードの管理について、留意すべき事項を教えてください。.....	15
Q24 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。.....	16
Q25 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。....	17
Q26 エンドポイントセキュリティ対策を実施する上での留意点を教えてください。.....	18
Q27 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。.....	19
Q28 情報が漏洩してしまう可能性が高まる状況を識別するためにはどのような方法がありますか。また、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。.....	20

Q29	ファイルサーバや仮想デスクトップとしてクラウドサービスを利用する場合に、業者（委託先）を選ぶ際の留意点を教えてください。 .....	21
Q30	ファイルサーバや仮想デスクトップ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。 .....	23
Q31	ファイルサーバや仮想デスクトップ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。 .....	23
Q32	当事務所ではSNSを利用した情報発信を行っています。その際に留意する点がありますか。 .....	24
Q33	情報資産台帳の作成や情報資産の棚卸が必要になる場合はどのような場合でしょうか。また、どのように作成すればよいでしょうか。 .....	25
Q34	セキュリティ対策の実効性に関するモニタリングを行う場合、特に留意する事項にはどのようなものがありますか。 .....	25
Q35	公認会計士事務所（監査法人）としてリモートワーク（テレワーク）を推進していく上で、担当者として特に留意する事項にはどのようなものがありますか。 .....	26
VI	利用者の役割 .....	28
Q36	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。 ....	28
Q37	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。 ..	28
Q38	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。 ....	30
Q39	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。 ....	31
Q40	万が一、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。 ....	31
付録1	：セキュリティ・ポリシーの例示 .....	33
付録2	：業務の局面におけるリスクとリスク対応例（Q10参照） .....	39
付録3	：外部委託管理規程の例示 .....	44
付録4	：2015年12月14日付け会員向けお知らせ .....	48
付録5	：2009年7月22日付け会員・準会員宛メッセージ .....	53
付録6	：2005年9月27日付け会員・準会員宛メッセージ .....	56

## 1. 本実務ガイダンスの目的

本実務ガイダンスは、品質管理基準報告書第1号実務指針第1号「公認会計士業務における情報セキュリティの指針」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、品質管理基準報告書第1号実務指針第1号の項目と対応するように作成しているため、品質管理基準報告書第1号実務指針第1号と対応させながら読んで理解を深めていただきたい。

2009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5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。

本実務ガイダンスは、一般に公正妥当と認められる監査の基準を構成するものではなく、会員が遵守すべき基準等にも該当しない。また、2022年1月13日時点の最新情報に基づいている。

## 2. 本実務ガイダンスにおける用語の定義

本実務ガイダンスにおいて使用する用語の定義は、以下のとおりであり、品質管理基準報告書第1号実務指針第1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。  
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。
- ・ 経営者  
本実務ガイダンスにおいて、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指す。

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

### 3. Q&A

#### I はじめに

Q 1 品質管理基準報告書第1号実務指針第1号の2020年10月23日付けの改正のポイントを教えてください。また、本実務ガイダンスの2022年1月13日付け改正の内容を教えてください。

A 1 2016年7月25日改正以降、ITの進歩が更に加速していることから、全ての情報技術への対応を中心とした整理を続けることは、対応の網羅性・迅速性の観点からむしろ望ましくないとの考え方に至りました。そこで、汎用的な考え方やITの進歩があっても基本的な考え方が変わらない、業務及びそこで取り扱う情報資産の量・質に応じた継続的なリスクアセスメントを行う整理に変更しています。

実務指針の改定後もIT環境とその利用方法の変化が進み、リモートワークやそれを支える各種クラウドサービスの利用が一般的となり、従来通りの環境認識ではとらえられないセキュリティリスクも増加しています。コミュニケーションスタイルも従来の直接対面・電話・電子メールからオンライン会議やチャットなどリモート前提となってきたためこれらの変化に対応して、Q&Aの内容を見直しました。

Q 2 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。

A 2 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、品質管理基準報告書第1号実務指針第1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。

Q 3 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」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、品質管理基準報告書第1号実務指針第1号との関係を教えてください。

A 3 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」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、品質管理基準報告書第1号実務指針第1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。品質管理基準報告書第1号実務指針第1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、ファイルサーバや仮想デスクトップ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。一方でフォルダを使わないケースもありますが、その場合も個々のファイル単位でアクセス権の管理が必要になります。

「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あり、電子データの漏洩、改竄等や、期待されていたITシステムや制御システム等の機能が果たされないといった不具合が生じないようにすることです。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品質管理基準報告書第1号実務指針第1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。現在の業務においては電子情報のやり取りが多くを占めてきており、サイバー空間固有の特徴を捉えて個別の対策を行う必要があるものの、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。

Q 5 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。

A 5 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。
- ・ 自社のみでの取組のみならず、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検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。

Q 6 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。

A 6 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、品質管理基準報告書第1号実務指針第1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、経済産業省から公表されている「サイバーセキュリティ経営ガイドライン」とその付録や手引き、プラクティス集が経営陣の役割にも触れており、改訂頻度も一定程度行われているため全体像として分かりやすい構成になっています。

リモートワークに関しては、総務省から2021年5月31日に公表されているテレワークセキュリティガイドライン（第5版）、中小企業等担当者向けテレワークセキュリティの手引き（第2版）などが挙げられます。

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」（2017年5月30日施行）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

Q 7 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。

A 7 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。また、ランサムウェアのように、公認会計士事務所（監査法人）のシステム自体へのアクセスができなくなってしまうマルウェアもあり、可用性の観点からも対策が求められます。さらには、公認会計士事務所（監査法人）のシステムのアカウントが乗っ取られ誤った処理が行われて



しまう完全性の観点にも留意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。

近年のサイバーセキュリティ攻撃は巧妙になってきており、これを予防的に防ぎきることは難しくなっていることから、早期の検知を行えるような組織やシステム運用上の仕組みを導入する事や、影響の特定早期化や対応の早期化など被害の最小化につながる取り組みを行っていくことも大事です。

Q 8 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。

A 8 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「業務上取り扱っ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」（2005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」（2015年4月22日付け公表）

Q 9 公認会計士業務を遂行するに当たり非常勤者や業務委託先など外部の人材や、クラウドなどの外部サービス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。

A 9 近年の公認会計士業務は、求められる専門性の高まりや業務の効率性、人材の効率的な活用などの観点から、組織外のリソースを使う事が以前にも増して一般的になってきています。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。

業務の実行やIT機能は外部に移転することが可能ですが、説明責任は移転することが出来ないことから、外部にどのような作業や業務を委託するのかによって、扱う情報も異なることを前提にリスクに応じた対策を行う事が肝要です。例えば、非常勤者等に常勤者と同じ作業をさせ、扱う情報も同じだとすれば、モニタリングも含めて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 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。

A10 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、現状における関連する内部統制を識別した上で、残存リスクを認識し、必要な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想定リスクに対応する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、ファイルを添付する場合はクライアント等とあらかじめ年度初めなどに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オートコンプリートを使用した結果、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ことにより悪意の第三者による情報の不正取得を許してしまうリスク、といったルールが守られないことに起因する残存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ルールを強制適用する仕組みを導入する、具体的には、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た上でシステムのポリシーで当該設定の変更を許可しない、又は、外部ドメインのメール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ツールを導入する等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。

Q11 外部の委託業者との間で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な点について注意すればよいでしょうか。

A11 警備保障会社、清掃業者、クラウドベンダーといった外部業者との間では、取引の開始にあたり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。

確かにこうした守秘義務を含んだ機密保持契約を締結することにより、契約当事者以外の第三者へ情報が漏洩するリスクの低減が期待できます。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一定程度低減するでしょう。しかしながら、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USBメモリ等の外部記憶媒体が机の上に置かれたままである、書類がシュレッダーで裁断されることなくゴミ箱に捨てられている、清掃業者が休日に清掃を行う場合などに社員・職員の立合いがないといった状況では、公認会計士事務所（監査法人）内に立ち入る外部業者が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。

また、クラウドサービスを利用している場合でも、依頼者側でIDなどのアクセス権を適切に管理していなければ、退職者がもともと付与されていたIDを使って退職後に内部の情報を持ち出すといったリスクが残り続けることになります。

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。

Q12 ICT(情報通信技術)の進展に伴う業務環境の変化に対して、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 従来使用してきたパーソナルコンピュータ(PC)に加えてタブレットやスマートフォンといった情報機器の活用が進み始め、またデータの保管場所に関しても自社用のサーバからクラウドストレージへの移行や、さらにはネットワークの無線化、情報機器間の通信の多様化など、公認会計士事務所(監査法人)を取り巻く業務の環境も絶えず変化してきています。こうした状況の中にあつては、新しく導入される情報機器やサービスの利便性だけに目を向けるのではなく、これらに潜むセキュリティリスクを正しく理解した上で、あらかじめ適切な設定を行ってから利用することが重要です。一例として、近年急速に普及してきているIoT(Internet of Things)について留意すべきポイントを整理すると以下の通りです。

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、従来はインターネットに接続していなかった様々なものに通信機能が付加されることにより、相互に情報交換を行うことを通じて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)と呼ばれるものです。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、人事部所管の出勤退社情報(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する等、自社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等、意図せずに加害行為に加担す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るですか。

A13 公認会計士事務所（監査法人）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・表明する必要があります。特に近年は、IT技術の急速な進化に伴うIT環境の複雑化及びリモートワーク等の働き方の多様化が非常に早いスピードで展開しており、情報セキュリティの検討範囲・対策手段も常に変化する事を認識した上で、セキュリティ対策の妥当性、現場への効果を随時モニタリングし組織内外の環境変化に適宜対応することが重要です。

その契機としては、例えば、情報セキュリティ担当者や社員・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、社員・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。

逆にしてはならないこととしては、例えば、対策やモニタリングを情報セキュリティ担当者任せにしてしまい、取組の実効性が伴っていない状況を放置していることや、経営者が自分自身を取組の対象外としてしまい、継続的な知識の習得や自身の対応を行わないことなどが挙げられます。経営者のこのような姿勢は組織全体の取組全体に対する意欲を減少させ、実態のない形骸化した管理のみが残ることにつながります。

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。

また、業務効率の向上、環境変化に伴う多様なニーズへの対応から、業務を外部に委託する場合があります。個人情報や業務上の機密情報が取り扱われる場合には、業務を委託した企業での情報漏洩の可能性を考慮した対策が必要です。委託先企業における情報セキュリティ対策の実施状況の調査等、外部委託先等の管理が重要です。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。

なお、新型コロナウイルス感染症の拡大により普及したリモートワークでは、今まで実施してきたクライアント先や公認会計士事務所（監査法人）内での業務と比べ、情報の外部への持ち出し、オンラインストレージを使用してのクライアントとの資料のやり取りやリモート会議の実施等により、重要な情報の流出につながるリスクが存在しますし、リモートワークを狙ったサイバー攻撃も発生しています。経営者はリモートワークによるリスクを認識し、セキュリティ対策を実施する必要性を理解した上で、リモートワークに対応するセキュリティ・ポリシーへ見直すことが重要で

す。また、リモートワーク環境下においてセキュリティインシデントが発生した場合は、事務所に比べコミュニケーションが制限され、対応が遅れる可能性があります。インシデント発生の連絡受付や対応に当たって迅速な対応が取れる体制になっているか確認し、必要に応じて体制の見直しを行います。

**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予算と人材の確保、権限と責任及び連絡体制の明確化、緊急時を想定した模擬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。セキュリティインシデントの内容によっては、クライアント等の外部利害関係者への情報開示が必要となりますので、情報開示の要否や開示内容も検討しておくことが望ましいです。

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

A15 社員・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(特に情報漏洩事故の場合における信用の失墜、顧客の喪失等)について周知及び討論する方法などが挙げられます。

特にリモートワークでは、事務所以外で業務を行うためセキュリティ面での統制が及びにくく、加えて業務とプライベートの区切りも曖昧になりセキュリティ意識も薄れがちになります。リモートワークによる情報漏洩リスクを盛り込むなど研修内容をアップデートしたり、リモート研修の実施により、リモート環境下においても対象者全員が受講できるように管理することが重要です。

**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となります。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となります。

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OSや、ウイルス対策ソフトの設定、HD、SSDの暗号化等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、全て回収し一元的に管理する、といったことや、Q18に示すクラウドサービスで用意されている仮想デスクトップ等を利用すること等が考えられます。

Q17 「9. クラウドサービス等を含む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、クラウドサービスを含む外部の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。
- ・ クラウドサービスを含む外部の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、契約時に受託会社のセキュリティ管理状況に関する資料を入手し、必要に応じて質問を行う、契約後は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。当該クラウドサービスが行っているバックアップの体制・バックアップデータの保存先等の情報も把握する。
- ・ 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、オンライン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 メールやオンライン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、オンラインストレージは、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、SSD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、SSD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) オンラインストレージの利点

- ・ 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、SSD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。特にリモートワーク化では自宅等で業務を行う事も想定され、セキュリティ面での統制が及びにくく、加えて業務とプライベートの区切りも曖昧になりセキュリティ意識も薄れがちになる。ウイルス対策等が不十分なPCを利用する事で不測のデータ流出の可能性がある。
- ・ 日々の業務の中で、組織変更に伴う担当者移動、退職者・新期加入者の発生等、アクセス権のタイムリーな変更・調整ができていないと、退職者が引き続き情報に不正にアクセスする等、情報漏洩の原因になる可能性がある。
- ・ ユーザ自身が物理的にHD、SSDを保有しない（できない）ため、HD、SSD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、SSD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、SSD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、SSD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** ファイルサーバや仮想デスクトップ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。例えば、品質管理基準報告書第1号実務指針第1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、品質管理基準報告書第1号実務指針第1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）を定期的にと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ならないポイントは何でしょうか。

A20 経済産業省が2017年11月16日に公表した「サイバーセキュリティ経営ガイドライン Ver2.0」では、経営者の関与が強調され、経営者は、以下の3原則を認識し、対策を進めることが重要と述べ



ています。

- (1) 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
- (2) 自社はもちろんのこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
- (3) 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

例えばファイアウォールの検知状況を分析する等を含め、事務所のセキュリティ状況を細かく分析し、セキュリティリスクのアセスメント状況に応じた対策を講じるとともに、適切なリソースの確保と配分を行うことが重要です。

ネットワークを介したセキュリティに対する脅威のほかにも、2019年12月に発覚した神奈川県庁の行政文書が委託業者の従業員により流出した事例のように、システム関連の作業に関係して情報漏洩が発生するリスクについても対策を検討する必要があります。

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」（2015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）」（2015年12月14日）（付録4参照）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ます。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。）

Q22 電子データ授受に関する方針を定める上で留意する点を教えてください。

A22 電子データ授受の過程における責任の範囲をクライアントとの間で明確にすることが必要です。特にクライアントの提供する環境を利用する場合は、クライアントのセキュリティ・ポリシーに従う必要があるため、当該環境を利用することによって生じるリスクはクライアントにあることを明確にすることが重要となります。必要に応じて電子データ受け渡しに関する文書を作成することも有用と考えられます。

授受対象となるデータの範囲や方法を選択するにあたっては、公認会計士事務所（監査法人）のセキュリティ・ポリシーだけではなく、クライアントのセキュリティ・ポリシーも勘案する必要があります。電子データ授受の際の情報漏洩のリスクを想定し、受け渡しデータの範囲は必要最小限とすることが重要です。また、選択した方法で運用するための具体的な手順はクライアントとの合意に基づいて設定することが必要となります。

## V 情報セキュリティ担当者の役割

Q23 情報機器や電子ファイルの暗号化で利用するIDやパスワードの管理について、留意すべき事項を教えてください。

A23 IDやパスワードの管理は、情報セキュリティ対策の基本となる事項です。最近では端末のロック解除等にとどまらず、ファイルの暗号化、クラウドサービスの利用、ネットワークへのアクセス等様々な場面でIDやパスワードの使用が必要となってきていますが、セキュリティ担当者としてID、パスワードの設定、管理に際して留意すべき事項をまとめると、以下のような点が挙げられます。

### (1) セキュリティレベルに合わせたID、パスワードの設定

例えば、公認会計士事務所（監査法人）のファイルサーバや仮想デスクトップに関する管理者権限のIDやパスワードや、公認会計士事務所（監査法人）のネットワークへアクセスするためのセキュリティキーについては、一般的なユーザIDやパスワードと比較してより慎重に管理する必要があります。情報セキュリティ担当者としては、必要に応じてID、パスワードの管理に関するレベルを定めて、それに応じた対策を以下に示す留意事項の中から選択して、対策を行うことが考えられます。

### (2) ID、パスワードの設定に関する留意事項

- ・ 状況に応じて定期的にパスワードを変更する設定を行う。
- ・ パスワードの変更を義務付ける場合、同じパスワードを数世代、使えない設定にする。
- ・ システムの開発、保守を担当する業者に対してシステム管理者権限を貸し出す際は、返却後速やかにパスワードを変更する。
- ・ パスワードをソフトウェア等に記憶させない設定にする。
- ・ 公認会計士事務所（監査法人）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）。
- ・ 外部記憶媒体（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。

(3) ID、パスワードの管理に関する留意事項

パスワードの管理に関する以下のようなポリシーをセキュリティ・ポリシーとして定め、利用者に遵守を促すことが考えられます。

- ・ 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、何のためのパスワードか明示する形で紙に書いて保管をしない。
- ・ 複数人でID・パスワードを共有しない。
- ・ 個人で利用しているSNSサービス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) ID、パスワードの使用に関する留意事項

- ・ PC等端末の起動時にパスワードが必要となる設定にする。
- ・ OSログイン時にパスワードが必要となる設定にする。
- ・ PCを一定期間使用しない場合は自動的にスリープ状態になるようにし、復帰時にはパスワードが必要となる設定にする。
- ・ 電子データの授受に際しては、パスワードによる暗号化を行う。

**Q24** 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。

A24 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等の設定

- ・ 特殊な権限を持っているAdministratorを利用できない設定にする。
- ・ OS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。
- ・ 暗号化ソフトにより、HD、SSDの暗号化を行う。
- ・ エンドポイントセキュリティ対策ソフトを導入する。
- ・ OSについては、セキュリティパッチ等OSの更新が自動的に適用される設定にしておく。また、使用しているソフトウェアについても、必要に応じて自動アップデート等を有効にしておく。
- ・ 顔認証、指紋認証、ワンタイムパスワードなど、端末を紛失した場合であっても、容易に情報を取り出せないよう、端末の個人認証を強化する。

(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。
- ・ 外部ネットワークとの接続部については、ファイアウォールを設置する等、外部からの侵入対策をとる。

同時に、ログ管理についての機能についてもQ20、21のサイバーセキュリティ対策の仕組み

としての有用性（インシデント発生時の証跡、継続的なモニタリング実施）について議論し、ログ保存方法・期間も含めて検討する（Q27、34にも具体的記述あり）

- ・メールの送受信についてもフィルタリングを行い、不審なプログラムの授受がないか監視できるようにする。
- ・閲覧可能なウェブサイト又は閲覧してはならないウェブサイトを見極め、フィルタリングの実施を通じて実効性を確保する。例えば、情報漏洩防止以外の目的においても、業務に関係ない以下のようなサイトへのアクセスを抑制する。
  - ・アダルトサイト
  - ・ギャンブルサイト
  - ・出会い系サイト
  - ・暴力的なサイト
  - ・利用を許可していない、データの授受が可能なサイト
- ・公認会計士事務所（監査法人）外から公認会計士事務所（監査法人）内のネットワークにアクセスできるようにする場合には、セキュリティレベルの高い仮想専用線（VPN）を利用する。

### (3) サーバの設置

- ・サーバの用途やそのサーバ上で取扱うデータの分類などにより、オンプレミス環境で構築運用するか、クラウド環境等などの外部サービスとして利用するかを検討し、設置場所（自社サーバ室、データセンターハウジング、外部ホスティング）についても運用管理面での体制やコスト（利用ユーザ数）、実現可能なセキュリティ対策を含め留意する。

外部サーバを利用する際には、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」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、サービスを提供している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) 機器の廃棄

使用しなくなった情報機器について、記憶領域を有する物については譲渡せず、廃棄する場合にも記憶領域をドリルで物理的に破壊した上で廃棄するなど、廃棄のプロセスでの漏洩防止に留意する。

### (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を導入する場合、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。

<b>Q25</b> 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。
---

A25 以下のような防止策が考えられます。

#### (1) PCの利用

- ・PCに保管する電子データは最小限とし、不急のものは公認会計士事務所（監査法人）のファイルサーバや仮想デスクトップに保存する。

- ・ USBメモリは、公認会計士事務所（監査法人）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。
  - ・ OSやワープロ・表計算ソフトの、不具合を修正する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・私的な目的による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許可なく接続しないルールにする。
  - ・ 外出先で公衆無線LANはむやみに利用しない。
- (3) サーバの利用
- ・ ファイルサーバや仮想デスクトップは、鍵のかかる部屋等の中に設置する。
- (4) 機器の廃棄
- ・ 重要な情報を取り扱うファイルサーバや仮想デスクトップ等の場合は、ディスク障害や保守メンテナンス時に重要なデータが保存されたHD、SSDを返却せずに、自社で保管又は処分が可能な「ディスク返却不要オプション」を用意している機器ベンダーもあるので、自社で情報漏洩のリスクを完全にコントロールできるサービスがあれば積極的に検討する事が望ましい。
- (5) その他
- ・ PC以外のタブレットやスマートフォン等の機器の取扱いに関しても、セキュリティ面に考慮した運用管理が可能なMDM（モバイルデバイス管理）やMAM（モバイルアプリケーション管理）など、紛失盗難対策や情報漏洩対策として検討する事を推奨する。

また、上記のような対策を実施すると同時に、不要な情報を保有しないようなルールを決めるようにすることも重要です。

- ・ 個人情報が含まれるデータについては、個人を特定できるようなデータを除去した上で入手する。
- ・ 入手したデータを社員・職員等の間で共有する場合、必要以上にデータをコピーして保有しないようにする。
- ・ 仕訳データ等、情報量が多いデータについては、実際に作業に必要な部分のみを抽出して使用し、ソースデータには暗号化を施すようにする。

**Q26** エンドポイントセキュリティ対策を実施する上での留意点を教えてください。

A26 マルウェアから防御するためには、全てのPC・サーバにエンドポイントセキュリティ対策ソフトを導入するとともに、常にこれらの対策ソフトやOS、アプリケーションが、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）として一元的にエンドポイントセキュリティの入口の防御を行うことも重要です。例えば、メールサーバ用のエンドポイントセキュリティ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、不明な内容の電子メールの添付ファイルやURL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だけが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限定するなどの対策が考えられます。

上記は、主に既知のセキュリティ脅威に対する対策ですが、これらの対策を上回るだけでは防げない新たな攻撃が行われるリスクが常に存在するという点が、ネットワークセキュリティを考える場合の課題として挙げられます。

一般的に、エンドポイントセキュリティ対策ソフト等による対処は、実際に発生した新たな攻撃方法等の情報を検知、収集し、これに対する対処方法をパターン・ファイルとして定期的に配信することで最新の新たな攻撃方法にも対処する仕組みをとっていますが、この「新たな攻撃方法の検知」と「これに対する対処法の配信」の時間差を利用して、対処方法が配信される対策ができる前に集中的に攻撃が行われることがあります。

このような「対策方法がない攻撃」に対処するためには、仮にこれらのパターン・ファイルで定義されていない場合でも、プログラムの挙動が不審であると判断される場合には隔離等を行う「ふるまい検知・ふるまい分析」の機能を導入することも考えられます。

ふるまい検知は、攻撃の可能性があるプログラムの挙動を監視して対策を行うため、実際はマルウェア等ではないプログラムについても検知してしまいうこともあります。また、マルウェア等だけでなく不審な挙動を起こしたプログラムについては全て監視対象とするため、PC等の負荷を高めてしまうといった欠点もありますが、特にセキュリティ対策がより重要と考えられる機器やネットワークを構築する場合には、セキュリティ対策の一つとして有効です。ほかにも、PCの中に仮想化された別のPC環境を作成し、不審なプログラムについてはその中で動作させてみた上で不正なプログラムかどうかを判定する「サンドボックス」といった技術もあり、これら未知の脅威でもある程度の対応が可能なこれらの技術を必要に応じて導入することも考えられます。

**Q27** 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。

**A27** エンドポイントセキュリティ対策ソフトも有効ですが、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。エンドポイントセキュリティ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望ましいと考えられます。サイバー攻撃を受ける可能性が誰にでもあるとの前提の下、社員・職員等に対してサイバー攻撃の予行演習を行い、実際の攻撃がどのようなものかを理解してもらうことは、事前対策になります。

また、外部ネットワークとの接続部分にファイアウォールを設置することにより、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、不正なアクセスと思われる通信が発生した場合に、レポートメールを受信できるようにするといった対策をとることができます。

サイバー攻撃等のインシデントが発生した事を想定し、外部業者等セキュリティに関して相談出来る窓口等について事前に確認したり、セキュリティベンダー等に日頃の対策について意見を求めるなどの対応が有効と考えられます。

Q28 情報が漏洩してしまう可能性が高まる状況を識別するためにはどのような方法がありますか。また、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。

A28 情報漏洩のリスクは常に高いわけではありません。例えば、業務上使用するPCのOSや、ソフトウェアに関して重大なセキュリティ上の欠陥が発見された際に、その欠陥に対してパッチが適用されるまでの間に集中的に攻撃することが考えられ、そのような状況下では外部環境として情報漏洩リスクが高まっていると考えられます。

また、公認会計士事務所（監査法人）のサーバやネットワークに対するアクセスログにおいて、外部からのアクセスが短期間に急増している場合は、公認会計士事務所（監査法人）の情報機器に関するIPアドレス等が何らかの理由で流出し、外部からの攻撃の標的になりやすい状況になっていることが考えられます。

このような、情報漏洩のリスクが高まっている状況を把握するためにも、例えばOS等の販売元から配信されるセキュリティ情報をメールで自動的に入手できるようにしておく、セキュリティのパッチは速やかに適用する、公認会計士事務所（監査法人）のネットワークへの外部とのアクセス状況を継続的にチェックするといった対策をとることが重要です。

また、実際に情報が漏洩してしまう可能性がある場合、緊急時の対応体制や対応手順が決められていないと、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や感染が疑われる場合には、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であると認識した上で、早期に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、情報漏洩等が再度発生し、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、公認会計士事務所（監査法人）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。

(3) 利用者から情報を漏洩した可能性がある旨の連絡を受けた場合

物理的に端末等を紛失した場合、まずは可能であれば遠隔操作で端末のデータを消去する、当該ユーザIDでの端末の起動ができないようにするといった対処を行うとともに、当該端末で扱っていた情報の範囲を可能な限り特定することが重要です。もし端末を利用して公認会計士事務所（監査法人）のサーバ等に遠隔アクセスできるようになっている場合は、直ちに当該端末からのアクセスを遮断するための対策を講じ、それ以上の被害の拡大を抑える必要があります。

また、ネットワークを介した漏洩の蓋然性が高い場合、ネットワークアクセスを直ちに遮断する、当該ユーザIDを無効にする、といった対処を行った上で、当該ユーザIDでアクセスできるデータの範囲を特定する必要があります。

連絡を受けた直後、可能な限り速やかに上記の対策をとると同時に、漏洩の可能性があるデータ内容に基づき、監督官庁への報告及び当該データの提供元や警察を含む利害関係者への連絡を検討することがあります。

情報漏洩の原因や漏洩源の特定、漏洩したデータの範囲の把握特定に際しては、情報セキュリティ担当者のみ能力では限界がある場合も想定されます。そのような場合には、速やかに外部の専門家に依頼して、原因や漏洩源、流出データの範囲を特定し、それ以上の情報の漏洩が生じないような対策をとることが、その後の被害拡大を抑制するための有効な手段になります。

**Q29** ファイルサーバや仮想デスクトップとしてクラウドサービスを利用する場合に、業者（委託先）を選ぶ際の留意点を教えてください。

**A29** 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移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、リスク評価を更新するだけでなく、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
- ・ ウイルス等のエンドポイントセキュリティ対策の状況



- ・ 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（I SMS、I T SMS、BCMS、Pマーク、ASP・SaaS認定サービス、保証実3702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1年ごと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ため、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、それぞれの公認会計士事務所（監査法人）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System and Organization Controls (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、SOC2 (保証実3702やSSAE18に準拠した保証報告書)は、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、保証業務実務指針3702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。

**Q30** ファイルサーバや仮想デスクトップ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。

**A30** 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に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 (事業者側が一方向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) を定期的に取りることが可能か。)

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」のボタンを押すだけの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。

**Q31** ファイルサーバや仮想デスクトップ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。

**A31** ファイルサーバや仮想デスクトップ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、公認会計士事務所 (監査法人) 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。必要なアクセス管理が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。
- ・ 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。
- ・ 外部公開設定等可能なサービスなどの場合、初期設定（利用開始時）にて、全てのユーザに公開となっている可能性もある為、管理者として設定出来る項目を網羅的に事前チェック（設定判断含む）することを必ず行う。

**Q32** 当事務所ではSNSを利用した情報発信を行っています。その際に留意する点はありますか。

A32 SNSによる情報発信は、適時性、情報伝播のスピード、情報更新の容易さ等から有用な場合もありますが、誤った情報や、社会通念上問題があると判断される情報についても、素早く拡散され收拾がつかなくなるリスクがあります。一度誤った情報が流されると、風評被害等による影響が長引く可能性も考えられます。

また、普段からSNSを使って頻繁に情報を公開している場合、何らかの理由で情報の更新が滞り、情報の開示が長期間ストップした場合、そのこと自体が情報を発信する側の管理体制の不備や、自身にとって不都合な情報の開示をためらっていると受け取られ、風評被害につながるおそれもあります。そのほか、アカウント乗っ取りによる誤情報の発信等のリスクも考えられます。

そのため、SNSを使った情報発信を行う際は、以下のような点に留意することが重要です。

- ・ 情報を発信する前に、当該情報が正確かどうかをチェックする体制を作る。
- ・ 公式アカウントを取得できるサービスの場合、サービス提供者から公式アカウントの認定を受けたいうでアカウントを開設する。
- ・ アカウント情報（ID、パスワード）等の管理を行い、万が一乗っ取り被害にあった場合の対応策を検討しておく。
- ・ 複数のSNSサービスを利用する場合、それぞれで発信する情報に齟齬が出ないように留意する。

このほか、公認会計士事務所（監査法人）が公式に運用するアカウント以外にも、公認会計士事務所（監査法人）に所属する社員・職員等が、個人のアカウントを利用して情報を公開することで、結果として公認会計士事務所（監査法人）に対して風評被害が発生するといった事態も考えられます。個人アカウントでの情報公開を公認会計士事務所（監査法人）として完全にコントロールすることは容易ではありませんが、公認会計士事務所（監査法人）のポリシーにおいてSNSの利用に関するルールを定めておく、定期的に情報セキュリティ担当者が社員・職員等のアカウントをモニターし、問題のあるような情報発信をしていないかを確認する、といった対策が考えられます。

**Q33** 情報資産台帳の作成や情報資産の棚卸が必要になる場合はどのような場合でしょうか。また、どのように作成すればよいでしょうか。

A33 台帳の作成が必要となる情報の量や、保管場所の規模等については公認会計士事務所（監査法人）の状況により異なりますので一概には言えませんが、例えば、情報の管理場所が複数に分散している場合（ファイルサーバや仮想デスクトップが複数ある、書面資料の格納場所が公認会計士事務所（監査法人）外に複数ある等）の場合は、何らかの形で保管場所・部門ごとに管理している情報を棚卸できるようにしておく体制を作っておくことが望ましいものと思われます。特に、不要な情報を長期間保持しておくことは、情報漏洩時のリスクを増大させる可能性がありますので、長期間保管されている不要な情報がないかどうかにつき、定期的に確認できる体制になっているか、という観点で、台帳の整備を始めることも考えられます。

まずは、情報を管理する機器の単位ごとに、その中にどのような情報が保管されているのかを把握し、例えば公認会計士事務所（監査法人）内で作成した、公認会計士事務所（監査法人）内のみで利用するデータ（例：事務所の会計、給与データ）、公認会計士事務所（監査法人）外から入手した重要ではないデータ（例：公表済みの決算書）、公認会計士事務所（監査法人）外から入手した重要なデータ（例：未公表の決算書、クライアントの会計データ、個人情報に記載されている資料）といった分類を行うことから始めて、公認会計士事務所（監査法人）の状況に応じて管理内容を詳細化していく、といった対応が考えられます。

**Q34** セキュリティ対策の実効性に関するモニタリングを行う場合、特に留意する事項にはどのようなものがありますか。

A34 具体的にモニタリングを行う項目としては、以下のようなものが考えられます。

- OSやMicrosoft Officeなど、業務に利用するソフトウェアについて、各端末で利用されているバージョンを把握するとともに、バージョンごとの使用期限を一覧で管理し、サポート切れを起こしていないか定期的にチェックする。
- ファイルサーバや仮想デスクトップへのアクセスや、公認会計士事務所（監査法人）外から公認会計士事務所（監査法人）内のネットワークアクセスについて、アクセスログを取得できるようにしておき、不審なアクセスがないか定期的にログをチェックする。
- 電子データのバックアップを取得するようにしている場合、設定したサイクルごとにバックアップファイルが作成されているか確認する。また、可能であればバックアップデータを基に復元ができるかどうかのテストを実施する。

どの程度までモニタリングを行うかについては、公認会計士事務所（監査法人）で利用している情報機器の種類や量、取り扱う情報の量にもよるため、セキュリティ・ポリシーでその範囲を定めておくことも考えられます。

Q35 公認会計士事務所（監査法人）としてリモートワーク（テレワーク）を推進していく上で、担当者として特に留意する事項にはどのようなものがありますか。

A35 具体的な留意事項としては、以下のようなものが考えられます。

- ・ 暗号化されていない回線の利用やポップアップによる意図しない情報の共有、音漏れなど、リモート会議に係るリスクを勘案してリスク評価を見直し、セキュリティ・ポリシーでカバーされているかどうか経営者と連携して確認し、必要に応じて改定手続を行う。
- ・ リモートワークの実施を許可するIT環境、物理的環境について定義を行う。
- ・ リモートワークに利用する端末、アプリケーションの利用、データを格納する環境及びその関係を整理し、必要に応じて追加のセキュリティ対策を講じる。
- ・ 導入拡大に当たって新規のIT環境を構築利用する場合、多くの社員・職員等に一斉展開する場合には、同時大量接続など可用性の観点も含めた事前検証を実施する。
- ・ 社員・職員等に対する事前の研修や試験などを、開始時、また、一定期間ごとに実施して、セキュリティを始めとする業務上の留意点の認識を共有する。
- ・ Q24にも記載されているように、自宅を含め、外部から公認会計士事務所（監査法人）への接続に当たってはVPNを利用する（Q24参照）。
- ・ 紙媒体については可能な限りこれを利用しない。
- ・ リモートワーク環境における印刷の制限・禁止を行う。

（リモート会議の実施に対する主なリスク）

分類	タイトル/概要	リスクの説明
利用方針	会議や会議ルールの規程・ルールが存在しない	新しい会議形式への対応、新しいリモート会議ツールの採用可否などを定めることができるルールが組織に無い場合、利用者がセキュリティを考慮せずリモート会議ツールを導入したり、会議時のセキュリティが保たれなかったりするおそれがある。
リモート会議関連のリスクの洗い出し	リスクが洗い出されていない、又は長年にわたり見直されていない	リモート会議関連のリスクは比較的新しく、また、新しいリスク自体も頻繁に認識されている。独立行政法人情報処理推進機構（IPA）などの信頼できる組織から具体的なリモート会議関連のリスクを抽出し、評価し、対応するPDCAサイクルを、そのリスク特性も踏まえて適切な頻度で実施しないとリスク認識が陳腐化するおそれがある。
リモート会議ツール関連リスク	契約に係るリスク （主催者の場合）	リモート会議ツールは様々な事業者によってサービスが提供されており、簡易に利用できるものも多い反面、秘密保持や想定外のデータ利用に関して義務が強く課されていないプロバイダー・ベンダーを利用してしまっておそれがある。
	利用可能なリモート会議ツールを限定していない （主催者・参加者とも）	利用可能なリモート会議ツールをあらかじめ指定・限定しない場合、セキュリティ評価が行われていなかったり、組織のルールに適合してなかったりするリモート会議ツールをユーザが勝手に利用してしまうリスクがある。特にクライアントから利用したことのないリモート会議ツールを指定された場合、明確な回答が出来ないためやむを得ず使ってしまうケースに留意する。

	<p>リモート会議ツールの脆弱性の対応が事業者によってなされない (主催者・参加者とも)</p>	<p>脆弱性が生じているにもかかわらず、一定の期間内に対応しない(出来ない)リモート会議ツールも存在する。このようなリモート会議ツールを利用し続けてしまうと、情報漏洩リスクが高まる。</p>
	<p>リモート会議ツールが利用可能であり続けることをモニタリングしない (主催者の場合)</p>	<p>一旦利用を開始したリモート会議ツールに対して、サービスレベルの変更やセキュリティの状況を適時、又は定期的に確認していないと、リモート会議ツール利用開始時と異なるセキュリティ水準であるにもかかわらず、それを意識しないままリモート会議が行われてしまうため、情報漏洩リスクが高まる。</p>
	<p>契約停止・利用中止に係るリスク (主催者・参加者とも)</p>	<p>公認会計士事務所(監査法人)内のルールに対応できないサービスに対して契約停止を行うプロセスがない、又は契約・利用停止を利用者に適時に伝えないことで、セキュリティ水準等に達していないサービスを受け続けてしまうリスクが存在する。</p>
リモート会議実施に関わるリスク	<p>想定外の参加者の存在</p>	<p>主催者が誤って本来参加しないはずの組織・人に会議URLを送ってしまったたり、主催者・参加者が不用意に会議URLを共有したりすることで無関係な人物が会議に参加してしまうリスクが生じる。</p>
	<p>会議参加環境の整備</p>	<p>主催者は参加者の会議参加環境が確認しづらく、例えば、家庭からリモート会議に参加する場合、会議画面が見えたり、音漏れによって同居者に会議内容が漏れたり、スマートスピーカーを通じて情報が漏洩するリスクが生じる。</p>
	<p>公共のネットワークを利用した環境からの参加</p>	<p>暗号化されていない公共Wi-Fi(ホテルのLAN環境など)を利用した参加などを制約しないと情報漏洩リスクが高まる。</p>
	<p>会議参加者による会議の無断録画・撮影</p>	<p>会議参加者がスマートフォンやタブレットを使い主催者に無断で会議を録画したり、スナップショット機能を用いて撮影するリスクが存在する。</p>
	<p>会議主催者による録画内容の無断共有及び拡散</p>	<p>会議を録画する場合、録画データを会議主催者が参加者に無断で会議参加者以外と共有してしまうリスクが存在する。また、会議主催者が録画データを誤って漏洩・拡散してしまうリスクも存在する。</p>
	<p>会議外の情報の共有リスク</p>	<p>会議時に他の参加者に情報を共有する際に、本来共有すべきでない情報を共有してしまうリスクが存在する。例えば、デスクトップやフォルダの表示により、どのような情報を保持しているかが見えてしまう、誤った資料を投影してしまう、共有中にチャットなど画面上のポップアップが表示されてしまう、などが考えられる。</p>

## VI 利用者の役割

**Q36** 事務所のセキュリティ・ポリシーに従って業務を行ってれば、大丈夫でしょうか。

A36 セキュリティ・ポリシーに記載がないなど、ルール上明文化されていない事項で、技術的に可能なサービスについては、暗黙的に許可されていると解釈せず、利用の是非について情報セキュリティ担当者に確認することが必要です。

また、近年、エンドポイントセキュリティ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」  
[https://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/security/](https://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  
<https://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、又はエンドポイントセキュリティ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、リモートワークの普及に伴い、総務省から、リモートワークの導入に当たってのセキュリティ対策についての考え方や対策例を示した「テレワークセキュリティガイドライン」を策定・公表しています。リモートワーク勤務者が意識すべき事項や実施すべき対策を確認することができます。

- ・ 総務省：「テレワークセキュリティガイドライン」  
[https://www.soumu.go.jp/main\\_sosiki/cybersecurity/telework/](https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/)  
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://jicpa.or.jp/n\\_member/support/security/](https://jicpa.or.jp/n_member/support/security/)

**Q37** 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。

A37 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) 情報機器の利用に際して留意すべき事項

- ・ 情報機器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等の外部ネットワークに接続してデータの送受信を行わない。
- ・ リモートワーク拠点のLAN環境については、公認会計士事務所（監査法人）のセキュリティ・ポリシーに従った設定を行う。
- ・ 自宅でリモートワークを実施する場合、自身が所有する無線LANルーター等の機器についてもファームウェアを最新版に更新する。
- ・ 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スマートフォン等の端末を、勝手に業務に使用しない。
- ・ リモートワークを実施する際には、公認会計士事務所（監査法人）の許可を得ている端末で実施する。
- ・ リモートワーク端末のうち、特にスマートフォンやタブレットに関して、不正な改造を実施しない。
- ・ 外部記憶媒体（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、何のためのパスワードか明示する形で紙に書いて保管をしない。
- ・ 情報機器を持ち歩く際は、情報機器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。また、飲酒を伴う宴席の場には情報機器は持っていない。
- ・ 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。
- ・ 不審なメールの添付ファイルやリンク先を安易に開かない。
- ・ 業務用の情報機器には不必要なソフトをインストールしない。
- ・ 使用しなくなった情報機器は譲渡せず、廃棄する場合にもドリルで物理的に破壊するなど、安易に破棄しないように留意する。
- ・ リモートワークの拠点において、社員・職員以外の第三者（家族等）が居ることを認識し、可能な限り専用の環境を構築する。

## (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。
- ・ 紙媒体の持ち出し、第三者が居るリモートワーク環境での印刷を行わない。
- ・ 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ず、飲酒を伴う宴席の場には重要な書類は持っていない。
- ・ 書類を保管する際は、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。



Q38 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。

A38 C A A T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

C A A T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。
- ・ クラウドサービスを利用して電子データを授受する場合には、Q29を参考に、情報漏洩対策等が十分であるかどうか留意する。
- ・ クラウドサービスの利用について、定められた利用ルール範囲で利用する。
- ・ リモートワークで取り扱う情報は、定められた取り扱い方法（利用者・保管場所・利用可能なシステム環境の要件等）に従って取り扱う。

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C A A T用P CやHD、SSD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。

**Q39** 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。

A39 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。

また、個人で利用しているSNSサービス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、使い回しを避けることが重要です。

**Q40** 万が一、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。

A40 情報を漏洩してしまったことが分かった時点で、公認会計士事務所（監査法人）のセキュリティ・ポリシー等に従い、可及的速やかに所属する公認会計士事務所（監査法人）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。

情報を漏洩したことに気が付かないことや、情報を漏洩したことに気付いたにもかかわらず公認会計士事務所（監査法人）等に報告せず放置することは、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。

情報の漏洩が発生した可能性がある、又は実際に発生した際には、被害拡大の防止が最優先となりますので、漏洩の懸念が少しでもある場合には、情報セキュリティ担当者へ速やかに報告してください。

リモートワーク実施時については、公認会計士事務所（監査法人）と比較して周囲の社員・職員に相談しにくい状況にあるため、セキュリティ上の懸念が起きていないか公認会計士事務所（監査

法人) 内の作業以上に留意し、気になる点については公認会計士事務所(監査法人)のルールにのっとり早めの連絡を行うことが必要です。

以 上

- 本実務ガイダンス(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)

## 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）

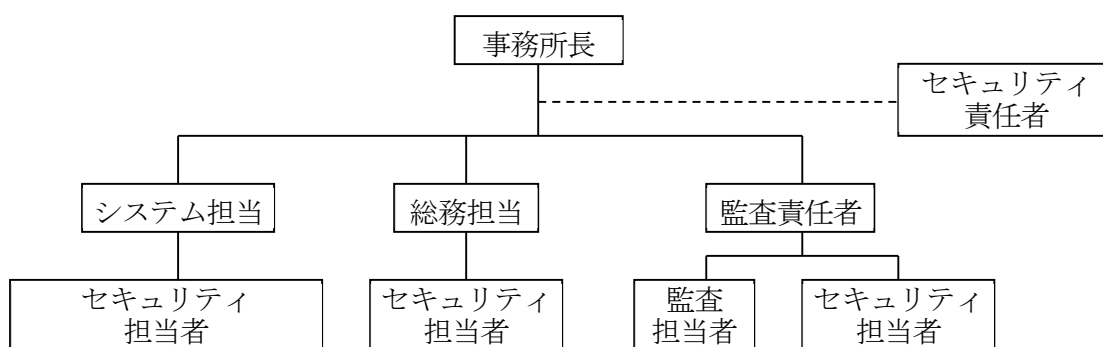
#### 4. 対象者と適用範囲

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) エンドポイントセキュリティ

- ・ 適切なエンドポイントセキュリティ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、英数字記号混在の8桁以上）を使用すること。
- ・ 必要に応じて変更すること。
- ・ 他のIDと同じパスワードを使用しないこと。

### 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。

#### (8) SNSの利用

- ・ 個人アカウントによるSNS利用に当たって情報が漏洩するおそれのある発信をしないこと。

### Ⅲ 情報の分類の例示

公認会計士〇〇事務所の情報を、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）：社内でのみに使用に限定する。

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、ファイルサーバや仮想デスクトップ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（Q10参照）

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	<ul style="list-style-type: none"> <li>・ 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。</li> <li>・ 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。</li> <li>・ マルウェアに感染してしまう。</li> </ul>	① ⑥ ⑧
	2	現場にて資料をUSBメモリ等（外部記憶媒体）で授受する	<ul style="list-style-type: none"> <li>・ USBメモリ等を紛失する、又は盗難されてしまう。</li> <li>・ 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。</li> <li>・ 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。</li> </ul>	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	<ul style="list-style-type: none"> <li>・ 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。</li> </ul>	①
	4	他人とのユーザIDの貸し借り（代理入力等）	<ul style="list-style-type: none"> <li>・ 第三者が本人になりすまして不正な操作をしてしまう。</li> </ul>	⑥
	5	人事異動、事務所退職等	<ul style="list-style-type: none"> <li>・ 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。</li> <li>・ 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。</li> <li>・ 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。</li> </ul>	⑥ ①、⑥ ⑥
	6	ソフトウェアの利用	<ul style="list-style-type: none"> <li>・ 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。</li> <li>・ 有害なフリーソフトのインストールによって、マルウェアに感染してしまう。</li> </ul>	⑥、⑧ ⑧

類型	No.	作業場面 (状況)	想定されるリスク例	参照番号
	7	インターネットの利用	<ul style="list-style-type: none"> <li>・ マルウェアに感染してしまう。</li> <li>・ 標的型メール攻撃の攻撃対象となってしまう。</li> <li>・ 脆弱な公共のインターネット(フリーの公衆無線 LAN を含む。)の利用により通信データが盗聴されてしまう。</li> <li>・ 自宅のインターネット環境を使用する場合、ルーターのファームウェアが最新となっておらず、外部からの攻撃対象となってしまう。</li> </ul>	⑧ ⑦ ⑧ ⑩
	8	資料の印刷	<ul style="list-style-type: none"> <li>・ 社内の複合機で印刷した際、取り忘れによって社内の第三者に情報が閲覧され、または持ち出されてしまう。</li> <li>・ 自宅プリンタやコンビニエンスストアなどのプリントサービスの利用によって、故意または過失による情報の流出が発生してしまう。</li> </ul>	④ ④
	9	オンライン会議の実施	<ul style="list-style-type: none"> <li>・ 画面共有時に、誤って共有すべきではない情報が投影されてしまう。</li> <li>・ 第三者の不正アクセスによって、会話の盗み聞きや画面資料の盗み見がされてしまう。</li> </ul>	⑨ ⑥
	10	シェアオフィスやカフェ、自宅での業務の実施	<ul style="list-style-type: none"> <li>・ PCやスマートフォンの画面を第三者にのぞき見されてしまう。</li> <li>・ 情報機器を紛失もしくは盗難に遭ってしまう。</li> </ul>	⑨ ③
保管	11	PC内にデータを保管	<ul style="list-style-type: none"> <li>・ PCを紛失する、又は盗難されてしまう。</li> <li>・ ファイルを誤って消去してしまう。</li> <li>・ PCがマルウェアに感染してしまう。</li> <li>・ 離席時に第三者がPCを不正に利用してしまう。</li> <li>・ 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。</li> </ul>	③ ② ⑧ ⑥ ⑩
	12	USBメモリ等(外部記憶媒体)にデータを保管	<ul style="list-style-type: none"> <li>・ USBメモリ等を紛失する、又は盗難されてしまう。</li> <li>・ ファイルを誤って消去してしまう。</li> <li>・ USBメモリ等がマルウェアに感染してしまう。</li> <li>・ 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。</li> </ul>	③ ② ⑧ ⑩
	13	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	<ul style="list-style-type: none"> <li>・ 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。</li> <li>・ 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。</li> <li>・ ファイルを誤って消去してしまう。</li> </ul>	⑪ ⑥ ②

類型	No.	作業場面（状況）	想定されるリスク例	参照番号
	14	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	<ul style="list-style-type: none"> <li>・ 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。</li> <li>・ 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。</li> <li>・ ファイルを誤って消去してしまう。</li> <li>・ アクセス権の設定間違いで、一般に公開されてしまう。</li> <li>・ 事業者の倒産によりサービスが停止してしまう。</li> </ul>	<p>⑪</p> <p>⑥、⑫</p> <p>②</p> <p>⑥</p> <p>⑫</p>
廃棄	15	過去の古いデータが保管されている	<ul style="list-style-type: none"> <li>・ 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。</li> <li>・ 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。</li> </ul>	<p>⑤</p> <p>⑩、⑫</p>
	16	システム更新に伴い、古い情報機器を廃棄する	<ul style="list-style-type: none"> <li>・ ファイルを誤って消去してしまう。</li> <li>・ 情報機器内にデータが保存されたまま廃棄してしまう。</li> </ul>	<p>②</p> <p>④</p>
	17	情報機器や機密情報を含んだ紙媒体の資料を、外部の業者を通じて廃棄する	<ul style="list-style-type: none"> <li>・ 廃棄を委託した外部の業者の不適切な管理により、廃棄したはずの情報が漏洩してしまう。</li> </ul>	<p>⑬</p>

## 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	<ul style="list-style-type: none"> <li>・メールの宛先違い（スペルミス、類似アドレスの誤入力）がないかどうかの確認</li> <li>・「Bcc」と「To」「Cc」の使い分けが適切かどうかの確認</li> <li>・オートコンプリートの使用禁止</li> <li>・メールの暗号化</li> <li>・ファイルをメールに添付する代わりにファイル転送サービス経由で受け渡す、またはクラウドストレージ経由で共有する</li> </ul>
	②	データの破損、誤消去	<ul style="list-style-type: none"> <li>・定期的なバックアップの実施</li> <li>・操作マニュアルの作成、利用</li> </ul>
	③	情報機器の紛失、盗難	<ul style="list-style-type: none"> <li>・ファイルの暗号化、強制暗号化ツールの導入</li> <li>・定期的なバックアップの実施</li> <li>・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</li> <li>・遠隔消去（リモートワイプ）ツールの導入</li> </ul>
	④	データの消去および紙面書類の廃棄漏れ	<ul style="list-style-type: none"> <li>・使用後のファイル削除ルールの設定</li> <li>・ファイルの暗号化、強制暗号化ツールの導入</li> <li>・削除ツールの利用、専門の外部業者の利用</li> <li>・紙面書類の保管および廃棄ルールの設定</li> <li>・シュレッダー、廃棄専用 Box の使用による確実な廃棄の実施</li> </ul>
	⑤	不要データによる管理コストの増大	<ul style="list-style-type: none"> <li>・電子データの保管期限の設定</li> <li>・電子データの定期的な棚卸し</li> </ul>
第三者の悪意	⑥	情報の不正取得、改竄、なりすまし	<ul style="list-style-type: none"> <li>・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</li> <li>・ID（メールアドレスを含む）・アクセス権の定期的な棚卸し</li> <li>・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</li> <li>・ファイルの暗号化、強制暗号化ツールの導入</li> <li>・パスワードルールの設定（桁数、定期的変更等）</li> <li>・オンライン会議用 URL およびパスワードの適正な管理</li> </ul>
	⑦	標的型メール攻撃	<ul style="list-style-type: none"> <li>・セキュリティ教育研修の徹底</li> <li>・専門の外部訓練業者の利用</li> </ul>

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
	⑧	マルウェアの感染	<ul style="list-style-type: none"> <li>・ エンドポイントセキュリティ対策ソフトの導入（暗号化ファイルへの対応に留意する。）</li> <li>・ 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。）</li> <li>・ 業務用情報機器の私用禁止</li> <li>・ ウイルス感染の兆候（システムの頻繁なハングアップ、不審なポップアップ画面やアイコンの出現、意図しないメール送信等）の早期認識、発見</li> </ul>
	⑨	PC・スマートフォン画面ののぞき見、不注意な画面共有	<ul style="list-style-type: none"> <li>・ のぞき見防止フィルターの装着</li> <li>・ オンライン会議時におけるデスクトップ画面共有の回避、ポップアップ機能の停止</li> </ul>
システム障害	⑩	情報機器の故障、破損によるデータの滅失	<ul style="list-style-type: none"> <li>・ 適時、適切なシステム更新（投資）</li> <li>・ 定期的なバックアップの実施</li> </ul>
	⑪	サービスの停止	<ul style="list-style-type: none"> <li>・ 定期的なバックアップの実施</li> <li>・ 代替的手段の併用</li> </ul>
委託先管理	⑫	サービスの停止	<ul style="list-style-type: none"> <li>・ 事業者の評価・選定基準の設定</li> <li>・ 定期的なバックアップの実施</li> <li>・ 事業者との契約更新時における SLA や約款の確認</li> <li>・ サービス内容の定期的モニタリング</li> </ul>
	⑬	情報機器、紙面書類の廃棄時の情報漏洩	<ul style="list-style-type: none"> <li>・ 事業者の評価・選定基準の設定</li> <li>・ 廃棄証明書の入手</li> </ul>

## 付録3：外部委託管理規程の例示

### I 総則

#### (目的)

第1条 この規程は、XXXX監査法人（以下「法人」という。）が行う外部委託に関し、公認会計士法及び諸法令に沿った適切な契約の締結と外部委託に関する管理態勢を定めるものであり、クライアント情報の保護及び法人の経営の健全性確保に資することを目的とする。

#### (定義)

第2条 この規程における用語の定義及び略称は、次の各号の定めるところによる。

- (1) 外部委託 法人が事業を営むために必要な業務の一部又は全部を、契約形態にかかわらず、法人以外の他者（グループ会社を含む。）に委託すること（他者が提供するサービスを利用する場合を含む。）をいう。
- (2) 外部委託統括責任者 法人の外部委託を管理する責任者として外部委託管理に関する事務を統括するものをいう。
- (3) 外部委託所管部 外部委託契約を計画実施する各部門をいう。
- (4) 外部委託管理責任者 外部委託所管部において契約の締結に責任を有する者をいう。
- (5) 業務委託契約書 外部委託する業務の性格により分別した請負型及び準委任型の業務委託契約書、又は産業廃棄物処理契約書をいう。
- (6) 委託先 外部委託先事業者をいう。
- (7) 再委託先等 法人の業務を委託された委託先が利用する二次以降の外部委託先事業者をいう。
- (8) モニタリング 契約上取り決めた履行義務の遵守状況、財務経営基盤及び業務遂行体制・進捗状況等に関する審査を実施することをいう。

#### (管理の対象とする業務の範囲)

第3条 この規程で管理の対象とする外部委託の範囲は、契約形態にかかわらず、クライアントに対して直接的間接的に影響を及ぼす業務、法人の経営に関わる業務又は内部管理上の必要性を有すると認められる業務のいずれかに該当するものとする。ただし、これらに該当しない一時的なサービスの利用、印刷物等の調製、会計監査を含む第三者による評価、訴訟等の委任、施設工事、運用指図、金銭の信託及び有価証券信託を除く。

#### (法令等の遵守)

第4条 業務を外部委託するに当たっては、公認会計士法等の各種法令に反することのないよう留意し、適切に委託先を指導する。

### II 外部委託の基本原則

#### (外部委託の適否判断)

第5条 外部委託は、次の各号に掲げるいずれかに該当する場合であって、公認会計士法等の各種法令の認める範囲内において実施できるものとする。

- (1) 当該業務を実施するための経営資源（要員・施設・機器等）が不足する場合、かつ法人で不足する当該経営資源を用意して実施することが困難と外部委託統括責任者が止むを得ないと判断した場合
- (2) 当該業務を委託することによって、業務の高度化、高付加価値化が期待できる場合
- (3) 当該業務を委託することによって、リスク管理の高度化が期待できる場合
- (4) 法令上の緊急な要請又は災害等により社内対応が極めて困難な業務である場合
- (5) 当該業務を法人で実施するより、委託する方が経費の節減が確実に期待できる場合
- (6) その他当該業務の内容を勘案し、社外に委託することが望ましいと外部委託管理統括責任者が判断した場合

第6条 前条の実施の決定に係る判断は、職務権限規程に定められた者が行うこととする。

第7条 外部委託所管部は、外部委託契約の締結後においても、委託の必要性を継続的に検証し、外部環境等の変化により当初の適否判断に変更が生じた場合には、委託内容の見直し等必要な措置を取り、外部委託管理統括責任者に報告する。

第8条 外部委託所管部長は、委託業務に関して契約どおりサービス提供が受けられない場合、経営の健全性確保の観点から、委託内容の変更、代替先の検討を含む必要な措置を講じるものとする。

#### (外部委託の適否判断)

第9条 外部委託所管部長は、委託先を選定する際、外部委託を行うことにより、当該委託業務を少なくとも法人が行う場合と同等のサービスの提供又はそれ以上のサービスの提供が行える委託先とすることとし、「外部委託先選定基準」に掲げる事項を満たすことを確認し選定しなければならないものとする。ただし、当該事項のうちの一部に不備・不足等があり、当該不備・不足が委託業務の実施に重大な影響を及ぼさないものと判断されるときは、委託先として選定することができるものとする。

2 外部委託先がグループ会社の場合、前項による手続を省略することができるものとする。

#### (外部委託契約の締結に当たっての留意事項)

第10条 外部委託契約の締結に当たっては、契約相手先、契約期間等必要事項及び次の各号に掲げる事項（委託業務の内容に該当しないものは除く。）を明記した書面の取交又は交付により行う。

##### (1) 守秘義務

秘密情報等の外部漏洩を防止するため、委託先が業務を受託することによって知り得た秘密情報等については、契約期間満了後も第三者に漏洩しないこと、秘密情報等を盗用・改竄しないこと及び受託業務の遂行以外の目的に利用しないことを定める。

##### (2) 報告義務及び監督権限の留保

委託業務管理の観点から、委託した業務が契約どおりに履行できているか、守秘義務が遵守されているか等について、委託業務の性質に従って、定期的又は法人の求めに応じて報告を行うこと、並びに当該委託業務の実施状況に関して法人若しくは法人から委託を受けた外部の専門機関及び監督当局による監査を実施できる旨を定める。

##### (3) 内部統制要件の遵守



委託先が法人の内部統制要件を遵守すること及び再委託先等がある場合にはその内部統制遵守を統制する義務を有する旨を定める。

(4) 損害賠償義務

委託業務の遂行に当たり、法人に損害が発生した場合の損害賠償義務について定める。

(5) 再委託に関する事項

再委託を行う場合は、法人の事前の承認を必要とする旨を定める。

(6) 情報漏洩等の事故・不祥事案や不測の事態等が発生した際の委託先の対応

委託先で情報漏洩等の事故・不祥事案や不測の事態等が発生した際には、委託先が法人に対して直ちに報告を行うとともに事態収拾に向けた責任ある対応を行う旨を定める。

(7) 知的財産権の帰属

法人が委託業務の実施により取得した成果物に係る特許権、実用新案権等の知的財産権は、原則として法人に帰属する旨を定める。

(8) 公益通報に関する事項

委託業務の実施に当たり、法人又は委託先において法令等に違反する事項等が発覚した場合の公益通報者保護法による法人が定める窓口について、周知する旨を定める。

(9) 反社会的勢力の排除に関する事項

委託先及び委託先の役員等が反社会的勢力に該当しないことを確約させる旨を定める。

### Ⅲ 外部委託管理態勢

#### (委託先管理の態勢)

第11条 外部委託管理統括責任者は、法人のリスク管理責任者とし、法人の外部委託を管理する責任者として外部委託管理に関する事務を統括する。

第12条 外部委託管理者は、法人のリスク管理責任者とし、法人の外部委託を管理する責任者として外部委託管理に関する事務を統括する。

#### (外部委託管理計画の策定・承認)

第13条 外部委託管理者は、外部委託契約を締結した場合には、速やかに外部委託管理責任者に届出を行う。

第14条 外部委託管理統括責任者は、外部委託管理者が外部委託契約を締結した場合には、速やかに別に定める様式により外部委託契約の一覧表を更新する。

第15条 外部委託管理者は、第14条により作成した外部委託契約の一覧表に掲げる外部委託契約のうち、この規程に基づいてモニタリングを必要とする外部委託契約（第3条但し書きにより除かれるものを除く。以下同じ。）に関する外部委託管理計画を策定し、外部委託管理責任者に報告する。

第16条 外部委託管理責任者は、前条により報告を受けた外部委託管理計画に必要事項が記載されていることを確認し、同計画による委託先モニタリングを承認する。

第17条 外部委託管理者は、前項の承認を受けた後、同計画に基づく委託先モニタリングを実施し、結果を外部委託管理責任者に報告する。

第18条 外部委託管理者等は、前項により不備事項が確認された場合、委託先にヒアリングし指導を行う。また必要に応じて委託先を通じて再委託先等を指導する。

第19条 外部委託管理責任者は、外部委託管理者が委託先モニタリングを実施し報告された場合には、速やかに委託先モニタリング計画にのっとったものか確認する。

#### (再委託の承認・把握・管理)

第20条 外部委託管理者は、委託先から別に定める再委託承認申請書が提出され、委託業務の一部を再委託することについて承認を求められた場合は、再委託の承認の可否を判断し、その結果を委託先に書面にて通知する。

#### (規程の改廃)

第21条 この規程の改廃は、リスク管理委員会における協議を経て決定する。

#### 附 則

この規程は、×年×月×日から実施する。

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。

コンピュータウイ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の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。

---

<sup>1</sup>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】

<p>事案の概要 (報告書 P. 16)</p>	<p>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。</p>
<p>第1段階 の攻撃</p>	<p>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。</p> <p>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。</p>
<p>第2段階 の攻撃</p>	<p>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。</p> <p>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。</p> <p>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。</p>
<p>第3段階 の攻撃</p>	<p>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。</p> <p>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</p>

	できなかった。
根本原因 (報告書 P. 27)	<p>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。</p> <p>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の対応に終始し、迅速かつ的確な対応ができなかったこと。</p>
再発防止策の 提言 (報告書 P. 33)	<p>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。</p> <p>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。</p> <p>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。</p>

## 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（I T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（I T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（I T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

I T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。

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（I T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（I T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（I T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 I T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](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](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

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

I T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

<sup>2</sup>本文中に記載の条文等は発信当時のものである。



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

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

<sup>3</sup>本文中に記載の条文等は発信当時のものである。

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ーとして可能です。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ー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のが可能であり、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