**税理士事務所が保有する情報の管理**

最近の社会現象のひとつとして、オレオレ詐欺や振り込め詐欺のような犯罪の背後には、何らかの個人情報の流出の結果といった要因が考えられる。

金融機関等における顧客情報の流出問題については、私達税理士事務所においても、多くの教訓を与える。

税理士の業務は、企業と個人の重要な機密を取り扱うものであり、もしこの顧客情報が流出したり漏洩されることにより、多大な損害を顧客に与えることに対しては、当然損害賠償責任を負わなければならないし、また、流失そのものが顧客からのクレームの対象となりうる。

　今や、この情報管理を徹底することが、税理士業務の中で重要な部分を占めていると言える。

　税理士事務所においては、今後あらゆる情報の管理規程やチェックリストを整備してゆく必要があると言える。

「個人情報の保護に関する法律」が平成１７年４月１日から全面施行された。特定の個人を識別することができる５,０００名以上の個人情報を取扱う事業者に対して、利用目的を超えた個人情報の利用、個人情報の不正取得や本人の同意を得ない第三者提供など、ずさんな管理をしないよう規制する法律である。

　例え私達税理士事務所がこの法律の対象とならない事業者であっても、充分に情報管理を行ってゆかねばならない。

1．税理士事務所が保有する情報

税理士事務所は、業務を遂行する過程で様々な情報を日常的に取扱い保管する。生存する特定の個人を識別することができる個人情報も当然のように扱っているし、顧客の会計や財務に関する情報を山のように作り出している。

2．顧客から提供される情報

・顧客企業の役員、従業員等の個人情報

年末調整事務を行うために提供を受ける、個人の住所、生年月日、扶養家族等の情報。相続税事務では、戸籍謄本や住民票等。家族構成や例えば障害者であるかなどの重要で幅広い情報が含まれる。

・顧客企業の会計・財務情報

記帳、決算事務を行うために提供を受ける会計・財務の情報。会計帳簿、伝票類、領収証、預金通帳、残高証明書その他明細書等。これらのコピ－。

3．事務所が作成する情報

・顧客の個人情報

事務所で作成する顧客の、出資者や役員の情報を記載した管理表、年度別の営業成績等を記載した業歴表等。作成した給与台帳、源泉徴収簿や源泉徴収票、顧客従業員の管理表等。また、ホルダ－等に整理された顧客の名刺も個人情報である。

・顧客の財務・税務の情報

作成した月次の試算表等財務報告書、決算書、総勘定元帳等。決算整理のため作成した調書。事務所保存用の税務申告書、申請書等。各種メモ。

　その他取扱い上注意を要するものに各種の名簿がある。提供された顧客の同業者名簿、労働組合や社内同好会名簿等。そして、税理士会から提供される会員名簿、税理士会支部の役員名簿や組織図等がある。

　また、それぞれ自己の事務所の従業員に関する事項も大切な情報である。

4．情報の保管

会計事務所は、関与先の多くの情報を保有しており、当然その秘密を守る義務がある。

特に最近では、ＣＤやＦＤ、携帯メモリーといったものにデ－タを取り入れ持ち歩くことも可能である。したがって、これら情報を紛失したり、盗まれたり、破損したりすると関与先へ大きな損害を与えるとともに、税理士事務所の信用の失墜という痛手をこうむることになる。損害賠償を請求されることもありうる。

　各税理士事務所は、デ－タが外に漏れないように安全に管理をする義務があり、万全な体制を組むようにしなければならない。

　例えば、情報の管理方法と責任の所在がはっきりしているか、その情報が事務所のさまざまな場所に保管されていれば、その保管場所ごとに誰が責任を持って管理しているかを確認する必要がある。そのために従業員などに対する適正な監督が必要であり、また、業者に情報管理を委託した場合、その業者に対する監督も必要になる。日頃からの教育の徹底が重要になると考えられる。

　各事務所の情報の管理方法として

1.紙や書類に記録してファイルする。

2.録音、録画テ－プに記録する。

3.フロッピ－ディスク、ＭＯ、ＣＤ－Ｒ、ＤＶＤ等に記録する。

等が考えられる。

　各事務所の情報の保管場所として

1.担当者の机の引き出し。

2.各従業員のロッカ－。

3.事務所の倉庫の中。

4.パソコンサ－バ－のハ－ドディスクの中。

5.所長の自宅。

6.外部業者に委託。

等が考えられる。

　以上、関与先の個人情報をはじめとする業務上知りえた事項の安全管理を体制面、技術面の両方で徹底することが重要である。

5．情報の伝達

　関与先等に情報を伝達する方法は、口頭(電話を含む)・手渡し・郵便・FAX・電子メ－ル等がある。しかし、税理士事務所から伝達する情報は、信書(注)に該当するものが多いので特に注意を要する。

(注)信書とは、特定の受取人に対し、差出人の意思を表示し、又は事実を通知する文書のこと。例えば、申請書・申告書・試算表・請求書類等が該当する。

情報の移送･通信等の対策として、口頭(電話を含む)及び手渡しは、出来れば直接関与先等の担当者及び責任者に行うことが必要である。郵便は、安全確実に関与先等に送付できるものにし、誤送の場合の確認が出来る方法等を講じる必要がある。FAXの送付ミスの対策として、特に重要情報を送る際に、受信相手が電話に出たのを確認してその場で送るという「ウエイティング･ルール」(昔のFAX送信システムのこと)を採用すると効果的である。電子メールの場合、発信する前に送信先の確認を再度することで誤送が防げる。重要情報はメールでやり取りしないルールが必要である。また、ウイルス対策も日頃から注意する必要がある。

6．情報の廃棄

　税理士事務所が保有する情報は、管理保管されていればよいというわけではない。情報の陳腐化、保存年限の経過、顧客との解約等により、いらなくなった情報を廃棄する必要が出てくる。

　日々発生する紙による情報は、不要になった都度シュレッダーで処分するのが手っ取り早い。しかし処分の是非に係る適切な判断は不可欠である。なお、ミスコピーの裏面再利用は、節約意識の高揚には有益であろうが、内容によってはシュレッダーで処分する方が安全な場合があろう。

　解約した顧客に係る情報は、原則として返却することが望ましい。しかし当該顧客に係る事務所内部作成書類の一部は秘密であり、次第にそれらの書類は溜まってゆく。保存年限の経過した重要書類とともにこれら事務所スペースを圧迫する紙による情報はいずれ廃棄しなければならない。廃棄の方法は、業者に依頼して焼却することとなるが、輸送時の漏洩防止や焼却事実の確認が可能な専門の業者に委託（保存段ボールのまま回収し、一切開封せず輸送・溶解処理し、処理証明書の発行をするシステムがある）することが望ましい。

　なお、パソコンの買い換えや廃棄に際しても、必ずハードディスクのデータを完全に消去するよう努めなければならない。

7．従業員の管理

税理士事務所には「個人情報保護法」に関係なく税理士法３８条により、税理士は、正当な理由がなくて、税理士業務に関して知り得た秘密を他に洩らし、又は窃用してはならないとして、秘密保持に義務が課せられている。また、従業員に対しても、法５４条により業務に関して知り得た秘密を他に漏らし、又は窃用してはならないとし、かつ従業員でなくなった後においてもまた同様とする、としている。さらに法４１条の２により税理士は、税理士業務を行うため使用人その他の従業者を使用するときは、税理士業務の適正な遂行に欠けるところのないよう当該使用人その他の従業者を監督しなければならないとして、使用人等に対する監督義務も課せられており、個人情報保護法に類する規定が設けられている。

個人情報保護法２１条によると、個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない、としている。

近年特にＩＴ化の進展に伴い個人情報の保護に関する意識が高まっており税理士も関心を持たざるを得なくなってきている。個人情報が外部に何らかの原因で流出した場合には、事務所は信用失墜を被ることになり、その被害が大きい場合には損害賠償の問題に発展する可能性もある。

個人情報が従業員により社外に流失した場合には使用者責任により税理士本人にその責任が問われることになる。従業員が行う補助業務に対して、高度な注意義務が要求され、従業員に対する指導・監督義務違反も問われることになる。従業員のみならず、アルバイトや派遣社員による個人情報の漏洩も考えられるので、これらの者に対する指導・監督も必要である。

また、退職した従業員による情報の漏洩ということも充分に考えられるので、

職員採用時に就業期間中の情報管理の注意事項や退職時の関与先情報の漏洩を未然に防ぎ退職による関与先の移動を防ぐためにも身元保証書や個人情報に関する機密保持合意書の作成は必要である。

　このようなことから従業員等を監督するに当たって次のような情報の管理が考えられる。

採 用 時・・・身元保証書や個人情報機密保持の合意書

教　　育・・・定期的に個人情報に関する教育研修を実施する。

内部規程・・・個人情報取扱に関する内部規程を作成し、あるいは内部規程の　　　　　　　中に個人情報取扱項目を設けて周知徹底する。

定期監査・・・個人データが適切に取り扱われているか定期的に監査する。

**〔税理士事務所における情報管理チェックリスト〕**

税理士事務所が保有する情報について、まず、情報管理の意識の徹底を再確認し、税理士事務所全体で情報の管理、チェックリストに基づき管理体制を点検。×が付くチェック項目は、改善策を検討。

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | 項　　　　　　　　目 | ﾁｪｯｸ  ○× |
| 事務所での啓蒙 | （基　　　本） | | |
| 1 | 情報漏洩等が発生した場合、関与先等への対策をとっているか |  |
| 2 | 従業員等に対して、情報管理の監督・指導を徹底しているか |  |
| （確　　　認） | | |
| 3 | 重要情報、帳簿・証憑書類の保管・管理を行っているか |  |
| 4 | SSD、USBメモリ、DVD・CD等の電磁的記録媒体の保管・管理を適切に行っているか |  |
| 5 | ノートパソコン等の持ち出し時の管理は大丈夫か |  |
| 6 | 情報処理の外部委託業者に対する監督を行っているか |  |
| 7 | 書類・文章の裏書きの取扱い及び廃棄の管理を行っているか |  |
| 8 | 各種名簿等の保管・管理及び廃棄は大丈夫か |  |
| 9 | オフコン・パソコンサーバーの電磁的記録媒体の管理は大丈夫か |  |
| 10 | 所長等、自宅での情報管理の徹底を行っているか |  |
| （テレワークを実施している場合） | | |
| 11 | 「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（チェックリスト）」等を利用し、適切なセキュリティ環境を構築しているかを確認しているか |  |
| コンピューター関連 | 12 | 誤操作・FAX、メールの誤送信はないか |  |
| 13 | システム設定、接続設定の誤りはないか |  |
| 14 | 内外部からの不正アクセスを排除しているか |  |
| 15 | ハッキング・ウィルス対策がとれているか |  |
| 16 | 業務上支障があるファイルはバックアップし保管しているか |  |
| 17 | 起動時はパスワード、ログインパスワードを設定しているか |  |
| 18 | ソフトの持ち出し時、メール送付の際、パスワードを設定しているか |  |
| 19 | パスワードは他人に知られない様にしているか |  |
| 20 | SSD、USBメモリ、DVD・CD等の電磁的記録媒体の持ち出し時にはパスワード設定等、セキュリティ対策をとっているか |  |
| （テレワークを実施している場合） | | |
| 21 | サーバ又はクラウド等の利用によりデータを一元管理しているか |  |
| その他 | 22 | 保存文章等は施錠出来る書庫、ロッカー、キャビネット等に保存しているか |  |
| 23 | 保存期間を設定し、経過した文章・書類等については速やかにシュレッダー等で廃棄しているか |  |
| 24 | 携帯電話のメモリやメールの取り扱い及び管理を行っているか |  |
| 25 | 危機管理体制の再検討 |  |

※　このチェックリストは全てではありません。事務所に適合した項目を追加して下さい