Joho System linkai
情報通
2015.August　8月号
発　行：東京税理士会 情報システム委員会
題　字：神津　信一（四谷）
（税理士会員章の日輪と八重桜をイメージしています。）

税理士事務所のための情報セキュリティ

情報システム委員会委員　菅沼　俊広

マイナンバー対策における税理士の立場

本年10月５日よりいよいよ「通知カード」が配布され、来年１月よりマイナンバーの利用が始まります。

最近、税務会計ベンダーやコンサルティング会社を中心に、かなり多くのマイナンバーについての研修会が開催されていますが、税理士にとって何がどう変わり、どのような対策をとる必要があるかについて明確に説明されている研修会はあまりありません。

税理士がマイナンバー対応策として行わなければならないことは、自らの事務所での対策、顧問先に対する対策の２つがあります。

自らの事務所での対策は、顧問先と同様、個人番号関係事務実施者としての対策と受託者（顧問先から税務会計業務を委託される）としての対策が必要となります。

マイナンバー使用者にはマイナンバーを業務に利用する個人番号利用事務実施者と、税・社会保障・災害に関する手続きにのみマイナンバーを使用する個人番号関係事務実施者の２つがあります。

税理士は、顧問先に対しては税務会計に関する業務を委託されている受託者としての立場となりますが、自らの事務所では、従業員等のマイナンバーを税・社会保障に関する手続きに使用する個人番号関係事務実施者となります。

個人番号関係事務実施者がマイナンバーを税・社会保障に関する手続きに使用する場合に行わなければならないことは、基本方針の作成、マイナンバー取扱規程の作成、４つの安全管理措置（組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置）、顧問契約書（委託契約書）の見直しとなります。

基本方針、取扱規程、顧問契約書の雛形は、既に日本税理士会連合会が発表している税理士向けガイドラインの中で提示されており、また、日本税理士会連合会のウェブサイト（会員専用）で編集可能な様式が提供されていますので、そちらを利用するのが良いと思います。

マイナンバー対策に必要な安全管理措置

問題は、安全管理措置をどこまで行えば良いのか？ということだと考えられます。

ポイントは、マイナンバーをいつ、誰が、どこで扱うかということを明確にすることです。

マイナンバーの使用については厳格な管理が必要となりますが、マイナンバーを使用しない場合は、厳格な管理は不要となります。もちろん、税理士業務上の守秘義務や個人情報の管理については、行わなければなりませんが、一生変わらないマイナンバーの取扱いに求められるほど厳格な管理は必要ないのです。

マイナンバーは、税・社会保障手続き以外では全く使わないことにして、マイナンバーを取扱う担当者、取扱場所、取扱時期を限定すれば（可能であれば所長税理士のみがマイナンバーを取扱う）、所長税理士のみが教育を受け、取扱規程を守り、所長の事務スペースのみを立入禁止にし、所長の鍵のかかる机等の引出しにマイナンバーの入った書類を保管、期限後に廃棄を行えば、職員についての安全管理措置は不要になります。

所長が申告・申請を行う税務会計ソフトについては、ほとんどの税務会計ベンダーが既存のシステムを改修し、マイナンバーと社員IDのデータベースについては、既存の税務会計システム内ではなく、クラウド上に保管する方向で検討されているようなので、これ以外にマイナンバーを電子データで扱わず、所内LANからも所長のコンピュータを切り離しており、作業ログ管理ができれば、職員のコンピュータについては、マイナンバー対応についての新しい仕組みは不要となります。

一方、従来と同様、職員を顧問先毎に担当割を行い、所長は申告最終チェックを行うという業務の流れの場合、全職員がマイナンバーを取扱うことになってしまうので、全職員に研修を行い、全職員のコンピュータにアクセス・作業ログ管理を行うことが必要になり、事務作業スペースについても、外部の方からは隔離されたスペースを確保する工事を行うことが必要となってしまいます。

このように、既存の業務内容を見直し、マイナンバー使用者・使用機器を極力限定することで、マイナンバー対策を低コストで行うことが可能となります。既存業務の見直しを行わず、従来と同様の業務内容とした場合、上述のように場合によっては、マイナンバー対策にかなりのコストが必要となってきますので、注意が必要です。

マイナンバー対策に必要な情報セキュリティ

現在の税理士業務にはコンピュータやインターネットが必須のものとなっており、それに伴って情報セキュリティの知識が重要なものとなってきています。

マイナンバーの導入により、本人確認が厳格化され、紙で申告書を提出する場合には、申告者本人のマイナンバー、本人確認書類、税務代理権限証書、税務代理権限があることを証明する書類（税理士証票等）が必要となり、手続きがかなり煩雑なものとなります。

一方で、電子申告の場合は、従来通りの手続きで良く、業務効率の面から考えても、電子化を推進せざるを得なくなってきています。

紙と電子の大きな違いは、複製の容易さと大量データの処理と考えることができます。

紙の場合は、電子と異なり複製が困難で、紛失したかどうかについても容易に見つけることができず、また、大量に複製することも困難です。

電子化の推進で必要となってくるのが、情報セキュリティの知識です。

情報セキュリティにおける「セキュリティを高める」とは、リスクを減らすことを意味します。また、ここでのリスクとは、資産、脅威、脆弱性からできており、リスクを減らすためには、資産、脅威、脆弱性のいずれかを減らすことが必要になります。

通常、資産と脅威を減らすことは困難なので、脆弱性を減らすことが、リスクを減らし、セキュリティを高めることになります。

脆弱性とは、弱いところ、コンピュータ用語では、一般にコンピュータやソフトウェア、ネットワークなどが抱える保安上の弱点を意味し、脆弱性が残された状態でコンピュータを使用していると、不正アクセスに利用されたり、ウィルスに感染する危険性が高まってしまうことを意味します。

脆弱性をマイナンバーの安全管理措置との関係で説明すると、主に物理的安全管理措置、技術的安全管理措置をどのように行うかということになります。

事務所内への立ち入りについて何も制限を行わない、ノートパソコンやUSBの管理に制限を設けない場合は脆弱性が高い状態（物理的安全管理措置をほとんど行っていない状態）となり、インターネットの接続に不正アクセス対策やウィルス対策を行っていない、ネットワークのアクセス権管理を行っていない場合は脆弱性が高い状態（技術的安全管理措置をほとんど行っていない状態）になっており、マイナンバー対策を行っていない状態と考えられてしまいます。

具体的にどう対策を行うかについては、上述のマイナンバー対策に必要な安全管理措置に記載した通りですが、このような対策をとることによって情報セキュリティにおける脆弱性を減らし、リスクを減らすことになるのです。

コンピュータやソフトウェア、ネットワークなどが抱える保安上の弱点は、日々発見されており、その弱点をついた攻撃が行われています。年金機構の情報漏えいを初めとするコンピュータからの情報漏えいの原因は、脆弱性についての対策が行われていなかったことに起因しています。

現在、マイナンバーは税・社会保障・災害以外には利用ができませんが、今後のマイナンバーの利用拡大につれて、ますます情報セキュリティに対する知識が重要なものとなってきます。また、情報セキュリティの対策を十分行っていれば、顧客に対して安全管理措置を十分行っていることを説明することも可能となり、マイナンバー対策をしっかり行っている税理士事務所として顧客の信頼性を高めることにもつながっていくと考えられます。

なお、９月１日には東京税理士会データ通信協同組合でも、IPA（独立行政法人情報処理推進機構）が実施している情報セキュリティの研修会が行われます。この研修の受講により情報セキュリティの基本知識を顧客に指導する知識を習得することができます。

電子申告に関する今後の会員サポート施策について

「情報通」７月号でもお伝えしたとおり、平成21年より各支部に委員を配置し電子申告の普及・推進活動を行ってきた電子申告推進委員制度については、電子証明書（ICカード）取得率及び電子申告利用率向上に関して一定の成果が見られたため、その役割を終えたものとして、第59回定期総会をもって終了となりました。

これに伴い、今後、電子申告を始めて間もない会員の方や、これから電子申告を開始する会員の方など、電子申告を利用する上で質問や相談を希望の場合には、各支部の情報システム関連部署に対応してもらうこととなりましたので、所属支部の情報システム関連部署までお問い合わせいただきますようお願い致します。

また、本会に設置されております「会員相談室」では、随時相談の相談項目に、情報システム関連項目が新たに加えられましたので、随時相談の性質上少々お時間をいただきますが、そちらも併せてご利用下さい。

各支部情報システム関連部署の皆様には、今後も本会の電子申告推進施策にご協力賜りますようお願い申し上げます。