Joho System linkai
情報通
2016.November 11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。）

中小企業における情報セキュリティ

情報システム委員会委員　菅沼　俊広

今年の年末調整からいよいよマイナンバーの取扱いが本格化し、具体的な対策を検討している先生方も多いことと思います。

顧問先の中小企業にとっても、業務上、インターネットや電子メールを使うことは当然のことになっており、報道されることは少ないですが、情報セキュリティの事故に対する被害も増大しています。警察庁の資料によると、平成27年中のインターネットバンキングに係る不正送金事犯の被害額は約30億7,300万円にのぼっています（「平成27年上半期のインターネットバンキングに係る不正送金事犯の発生状況等について」平成28年３月３日警察庁広報資料より）。

また、税理士が業務上取扱う個人情報については、来年春頃を目途に改正個人情報保護法の全面施行が予定されており、個人情報取扱事業者の範囲や要配慮個人情報の定義の明確化等税理士が所得税の確定申告で扱う個人情報の扱いにも、従来以上の管理が必要になってきています。

こうした中、電子申告の普及やマイナンバー、個人情報保護等情報セキュリティに対する知識は今後ますます重要になってくると考えられます。

中小企業の情報セキュリティ対策は遅れており、情報セキュリティ対策担当者がいる中小企業は19.6％で72％は情報セキュリティに関する窓口がなく、80％は情報セキュリティに関する教育を行っていないのが現状です（「2015年度中小企業における情報セキュリティ対策に関する実態調査報告書」2016年３月IPAより）。情報セキュリティ対策にはコストがかかり、担当者レベルで対策が必要と思っても、経営者の理解が足りず、対策が後手にまわっているという状況もあります。

中小企業に対して日頃から様々な相談に対応し、経営者に影響力のある税理士に情報セキュリティに対する相談対応が今後は求められてくるものと考えられます。

中小企業の情報セキュリティ対策については、「中小企業の情報セキュリティ対策ガイドライン」（IPA　2009年策定）がありましたが、今年９月15日に改訂版が作成され、今月中を目途に公表されることが予定されています。このガイドラインは本編と付録から構成されており、本編は経営者編と管理実践編の２部構成となっており、管理担当者のみでなく、経営者にとって必要な対策を簡潔に説明し、経営者が行うべきことについても明記がされています。

また、付録として最低限の情報セキュリティ対策や情報セキュリティ自社診断シート、セキュリティポリシー作成方法について解説が行われています。経営者にとって情報セキュリティ対策がなぜ必要かについても分かりやすく解説されており、税理士が知っておく知識としては有用なものとなっています。

以下では、このガイドラインから経営者が行うべき点について抜粋し、説明を行います。

情報セキュリティ対策として、経営者が知っておき、また行うべきことは、①情報セキュリティ対策は経営に大きな影響を与えることを自覚すること（情報セキュリティ対策を怠ることで企業が被る不利益）、②自ら動かなければ法的・道義的責任を問われること（経営者が負う責任）、③会社全体として対策をとるために担当者へ指示をすること（経営者は何をすればよいか）です。

１．情報セキュリティ対策を怠ることで企業が被る不利益

⑴資金の喪失

大規模な個人情報の漏えい事故が発生すると、盛んに報道がなされることからも明らかなように、個人情報の適切な保護は人々にとって重要な関心事項となっています。これに伴い、情報漏えい事故が生じた場合の損害賠償額も高額となる例が出ています。また、取引先などの機密情報の漏えいも相手方からの損害賠償請求の対象となります。

⑵顧客の喪失

情報セキュリティ上の事故が発生すると、事故を起こした企業に対する社会的評価は低下します。同じようなサービスを提供している企業が複数あれば、事故を起こしていない企業の製品やサービスを選択しようとする顧客が増えます。事故を起こした企業が再発防止策を定め、事故を起こさずに事業を続けていく中でこうした社会的信用は徐々に回復していきますが、事故の発覚直後には大きなダメージを受けることとなり、事業の存続が困難になる場合もあります。

⑶業務の喪失

情報セキュリティ上の事故が発生すると、被害の拡大を防止の観点から、自社で運用しているサーバーの停止や、インターネットへの接続の遮断などの措置を行います。この結果、ふだんインターネットを通じて発注している取引先からみると、営業を停止しているのと同じ状態になるため、措置を講じている間は事業機会の喪失となります。さらに、自社の業務で電子メールやグループウェアが使えなくなったり、グラウト上のサービスに接続できなくなったりすることで、社内の業務効率が大幅に低下してしまいます。

⑷従業員への影響

情報セキュリティ対策の不備を悪用した内部不正が容易に行えるような職場環境は、従業員のモラル低下を招く要因となります。また、事故を起こしたにもかかわらず、従業員のみを罰して経営者が責任を取らないような対応をとることで、従業員が働く意欲を失う恐れがあります。情報漏えいなどの事故による企業としてのイメージダウンを嫌って転職する従業員も現れます。

また、従業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされるなどの不利益を受けることも考えられます。

２．経営者が負う責任

情報セキュリティ対策に関する経営者の責任について、次に示す２種類の観点から説明します。

⑴経営者などに問われる法的責任

企業が個人情報などの管理義務がある情報を適切に管理していなかった場合、経営者や役員、担当者は業務上過失として処罰などの対象となります。個人情報やマイナンバーに関する違反の場合は刑事罰が科されるほか、個人情報保護委員会による立入検査の対象にもなります。

さらに、民法上の不法行為とみなされた場合は、経営者が個人として責任を負うべき損害賠償請求の対象となります。

⑵関係者や社会に対する責任

適切に管理することを前提に預かった情報を漏えいさせてしまった場合に問われるのは、前述の法的責任や、その情報の当事者に対する責任だけではありません。情報漏えい事故の発生は、営業停止、売上高の減少、企業イメージの低下などで、自社に損害をもたらすだけでなく、取引先に対する信頼関係の喪失、業界やサービス全体のイメージダウンなどをも生じさせることにもなります。ゆえに、情報セキュリティ対策は、顧客・取引先・従業員・株主などに対する経営者としての責任を果たすための手段としても重要といえます。

３．経営者は何をすればよいか

これまで示してきた内容をもとに、企業における情報セキュリティの確保の観点から、経営者に求められる役割（経営者は何をすればよいか）を説明します。

企業における情報セキュリティの確保に向けて、経営者は、以下に示す「３原則」について認識した上で、「重要７項目の取組」の実施を管理者層に指示する必要があります。

なお、この内容は、経済産業省及びIPAが2015年12月に「サイバーセキュリティ経営ガイドライン」として策定した内容を、中小企業向けに編集したものです。

⑴経営者が認識する必要がある「３原則」

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です。

① 情報セキュリティ対策は経営者のリーダーシップのもとで進める
② 委託先における情報セキュリティ対策まで考慮する
③ 情報セキュリティに関する関係者とのコミュニケーションは、どんなときにも怠らない

⑵企業として実施する「重要７項目の取組」

経営者は、以下の「重要７項目の取組」について、自ら実践するか、実際に情報資産や情報システムなどの管理を実践する管理者層に対して指示することで、着実に実施することが必要です。

① 情報セキュリティに関するリスクを認識し、組織全体での対応方針を定める
② 情報セキュリティ対策を行うための資源（予算、人材など）を確保する
③ 情報セキュリティのリスクを把握し、どこまで情報セキュリティ対策を行うのかを定めたで担当者に実行させる
④ 情報セキュリティ対策に関する定期的な見直しを行う
⑤ 業務委託する場合や外部ITシステムやサービスを利用する場合は、自社で必要と考える情報セキュリティ対策が担保されようにする
⑥ 情報セキュリティに関する最新動向を収集する
⑦ 緊急時の社内外の連絡先や被害発生時に行うべき内容について準備しておく

経営者の認識が高まり対策を講じるためには、情報セキュリティマネジメントを担う人材の育成も必要になります。

今年の春から国家試験「情報処理技術者試験」の新たな試験区分として「情報セキュリティマネジメント試験」が創設されています。

上述のように中小企業ではなかなか情報セキュリティに精通した人材を確保することが困難であるため、できれば税理士がこのような資格を取得し、顧問先の中小企業を指導・支援していければ望ましいと思われます。