TRC EYE Vol. 88

東京海上日動リスクコンサルティング（株）
情報グループ
主席研究員　　近森　健三

個人情報保護対策とリスクコントロール

第２回　教育と監査

■ルールを形骸化させないための仕組み作り

いくら立派な個人情報保護方針を掲げ、規程類を整備しても、それらが守られていなければ全く意味がない。更に、そのような状態を放置していると、「ルールはルール。実際の仕事はそうはいかない。」という考えを認めてしまうことになり、コンプライアンス意識をますます低下させることになってしまう。個人情報保護はマニュアルや文書だけで機能するものではなく、役員をはじめ従業員・スタッフなどの組織内の人間が現場で実践してはじめて実現できるものである。特に日本の場合はマニュアルや文書ができるとそこで安心してしまい、「仏作って魂入れず」となりがちである。従って、方針や規程類等を策定したら、ルールの形骸化を防ぐための対策や仕組み作りが重要となる。一つは組織内にルールを周知徹底するための「教育」の仕組みであり、もう一つはルールの遵守状況をチェックし、是正・改善するための「監査」の仕組みである。

■教育の実施

営業成績を上げることには熱心だが規程やルールを守るのは苦手という社員は多い。特に、忙しいとか面倒であるという現場の都合が優先されコンプライアンスが後回しになってしまうことは、残念ながらままある話である。個人情報保護に限らず、ルールや規制が守られるかどうかは、組織内でのコンプライアンス遵守の風土と各個人の自覚に大きく左右される。また、ルールそのものを認知していなかったり、ルールを守らなかった場合に何が起きるかということを理解していなかったりすると、これもルール違反を引き起こす原因となる。

コンプライアンス遵守の風土と個人の自覚を醸成するためには、トップマネジメントの強い意思のもと、地道に教育を継続することが必要不可欠である。その際、単にルールの内容や項目の説明に留まるのではなく、なぜ個人情報を守らなければならないのか、世の中では何が起きているのか、個人情報保護の遵守によって企業や組織が何を達成しようとしているのか、という「趣旨」「背景」「目的」について十分に説明し理解させることが重要である。普段仕事をしていると既存のルールでは判断が付きかねる事態に遭遇することがある。このような時に、ルールの趣旨や目的という根本に立ち返って考えることができな

ければ、誤った判断をしたり、判断することを避けたりしてしまう。また、教育は一度だけではなく、繰り返し定期的に実施する必要がある。繰り返し定期的に行うことは、規程やルールの理解度を深めるだけではなく、コンプライアンス重視の風土造りにつながる。個人情報保護の教育を実施するうえでのポイントをまとめると以下のとおりである。

①当事者意識の喚起

各部門における個人情報はすべて当該部門の長など現場の責任者が把握し管理するということを強調し、現場責任者の当事者意識を喚起する。個人情報保護の取りまとめ事務局がやってくれるという意識ではルールの徹底はできない。世間の実際の事故事例に加え、自らの組織内における事故やミスの事例などを教材に加え、身近な問題であることを認識させると効果的である。

②教育方法の工夫

個人情報保護の事務局から部門の管理責任者へ、部門の管理責任者から部門の従業員へと徐々に段階を落としながら実施する方式は、労力や時間を要するため全組織に展開するのに時間を要する場合があるが、質疑応答などが出やすく他の方法と比較して一般に教育効果は高い。これに対し、E ラーニングツール、教育用ビデオなどを活用した一斉教育は、展開は早いが臨場感に欠ける場合がある。これらのメリット・デメリットを踏まえたうえで、いくつかの教育方法を交えつつ実施すると良い。

③教育効果の検証

教育した内容は、実際に従業員に実行されてはじめて意味がある。説明会や教育用ビデオで視聴者がずっと居眠りしていたならば、教育を終了したとはいえない。従って、必ず理解度テストを実施し、全員が及第点を取るように徹底するようにしたい。なお、理解度テストは教育プログラムの良否の判断にも有用であり、平均点が低い場合は教育施策を見直す必要がある。また、従業員のルール遵守の意識を高めるために、理解度テストの合格者に対して「理解したからにはルールを守ります」という趣旨の誓約書にサインさせることもひとつの手段である。

④定期的な実施

個人情報保護の教育は、新人教育、部門別教育、管理責任者教育、役員教育など様々な階層や部門別にきめ細かなカリキュラムを作って計画的に実施する。中途採用や人事異動などで新たに部門に配属された要員の教育も怠ってはならない。また、事業の発展や機構改編、情報システムの更新などによっても対策が変化し得るため、毎年定期的にかつ反復して実施する必要がある。

■監査の実施

個人情報保護対応の取り組みについてはリスクマネジメントの考え方が有効であることは前回に述べた通りである。マネジメントシステムでは、P（Plan）→D（Do）→C（Check）→A（Act）のサイクルの運用による継続的改善が鍵となる。PDCA サイクルを運用する上で日本企業に共通した弱点がC（Check）

にあたる点検・評価である。方針を立ち上げて実行はするが、その有効性について客観的に点検・評価をするフェーズが今ひとつ弱い。そのためＡ（Act）につながらない。点検・評価業務は決して華々しいものではないし、組織内で批判的な立場に立つのは難しい面もある。しかし、昨今はこの組織内でのチェック機能である「内部統制」がより重視されるようになっており、個人情報保護においても重要な位置付けにある。

点検・評価については、まず各部門内において、個人情報の管理状況や取扱状況が予め定めた実施計画やルール通りできているのかどうかを自主的に点検・評価することが基本となる。自主点検はなるべく気軽に取り組むことができるよう、チェック項目は基本的なもの（例えば個人情報台帳の作成状況や、個人情報を含んだ文書・データ・媒体などの保管状況、廃棄状況、ID・パスワード管理等）に絞込みつつ、逆に１～２ヶ月に１回など頻度を上げる方が効果的である。

そして、最も重要なものが組織内の第三者による客観的な点検・評価、すなわち内部監査である。内部監査においては、自主点検ではカバーしていない部分を含め各部門におけるルールの遵守状況をチェックするだけでなく、組織内の個人情報対応を推進する事務局の活動状況や推進方法もチェックする必要がある。現場でのルールの遵守状況が芳しくない場合、その原因として教育ツールが理解しにくい、或いはルールそのものが実務に即していない、推進計画に無理があるなどの問題があるかも知れない。このような問題について、当事者である推進側が自らを客観的に評価することは難しいからである。内部監査を実施する監査員には、監査分野についての知識、監査のスキル、助言・提案能力、そして客観的な視点が求められる。そのため、内部監査は専任の内部監査員により行われることが望ましいが、これが難しい場合には、被監査部門と利害関係の無い他部門の社員などを監査員に任命し、必要な教育を実施した上で監査チームを構成しても良い。いずれの場合においても、被監査部門からの独立を担保するため、監査員の任命は経営者自らが実施する必要がある。一般的な監査の進め方は次の通りである。

①内部監査の年度計画の策定（経営者の承認）
②内部規程を基にした監査チェックリストの作成
③内部監査の個別計画の策定（被監査部門との監査日程調整）
④監査の実施、客観的な事実の収集(文書提出、インタビュー、実査等)
⑥指摘事項のまとめ、証拠の確認
⑦監査報告書の作成(被監査部門との事実確認実施後)
⑧監査報告書の経営者への報告

そして、経営者は、内部監査の結果を踏まえ、個人情報保護管理体制を見直し、改善のための施策を講じる。その際、個人情報保護の最高責任はあくまでも経営者にあることを認識したうえで、組織の方向性を明確に打ち出すことが求められる。

次回（第三回）は、外部委託先の管理について述べてみたい。

出典：特定非営利活動法人ネットワークリスクマネジメント協会発行
NRAメールマガジン『啓・警・契』第１０６号
URL：http://www.nra-npo.jp/

（第 88 号　2006 年 1 月発行）

