第４章　これから保護活動に取り組まれる方への提言

本章と第５章、第６章では、アンケート回答の分析結果と訪問時のヒヤリングや観察結果から得られた考察（第２章、第３章参照）を元に、個人情報保護法や不正競争防止法による法律リスクをどのように管理するのかについて提言を行う。

今回の調査を通じて、わずかな十数社の訪問調査であっても、それぞれの企業、法人が保有する情報の量、経営環境、将来的に考え得るビジネスモデルなどが異なれば、その解決方法も自然と異なるであろうことが改めて確認できた。そこで私達は、

①これから保護活動に取り組まれる方への提言（本章）

②既に保護活動に取り組まれている方への提言（第５章）

③中小企業診断士の役割についての提言（第６章）

に分けて、それぞれの立場の方に提言を行う。それらの提言は全く同じところから出発している。読者の立場に合わせて選択して頂きたい。

今回の調査研究に理解を示し、アンケートにご回答いただいた方々は、概ね個人情報や営業秘密の保護に関心を持ち、多くはこれから取り組みを開始あるいは強化しようと考えておられると思われる。これから個人情報保護・営業秘密保護活動に取り組まれる方に、ご自身の取り組みを計画、評価するための指針として、以下の７つのポイントを提言する。

1.計画・目的の重視

個人情報や営業秘密の保護に取り組むことは、社会的なニーズに合わせて業務や管理のあり方を見直して、変更を加えることである。単に、新たな資源を投入して手順を増やすことではなく、新たな見方から活動を再構築することである。なぜならば、個人情報や営業秘密の保護を上手にやりおおせたからと言って、確かに顧客の信用は増すことだろうが、単純に売上が増えるわけではないからである。やるべきことが増えれば、一方で効率化を行わなければならない。新しいコンピュータシステムを導入するならば、業績向上に生かすようにしなければならない。そう考えれば、この取り組みは経営改革の一種である。

改革には目的がある。社会的ニーズへの対応はビジネスチャンスと考えることができる。個人情報も営業秘密も資産と考えることができる。顧客のニーズを実現するために活用して初めて価値が出る。新規事業を考えるなら、事業領域とミッション、顧客、事業戦略を明確にし、現状を良く分析して、経営計画を練り上げる。全く新しいことを始めるのでなければ、そこまで行かなくても、少なくとも自社の顧客が何を望んでいるのかを良く見極め、仕組みをどのように変えていけばよいのかを考える必要がある。基本的な仕組みは変えないということならば、どうすれば効率的に情報の保護ができるのかを考える必要がある。リスク対応だけなら損害賠償保険に入るという考え方もあるが、どの程度のリスクがあるかを見積もらなければならない。いずれにせよ、

どのレベルまで何を変えたいのかをはっきりさせなければならない。効率的に実施するには目標が必要になる。

そこで、次のようなステップで計画、実行をされるようお奨めする。できることから手をつけようと言う考え方で、こうしたステップを複数回実行するのが望ましい。

(1)現状分析

最初に現状分析を行い、長期的な経営計画と照らし合わせることによって、どのような目的やニーズで個人情報、営業秘密の保護に取り組むかを明確にする。プライバシーマークの取得からクレーム予防までいろいろなレベルが考えられる。

(2)目標設定

検討を行う範囲を明確にし、それぞれに達成すべき目標（回避すべきリスク）を明確にする。できれば実行にあたってのマイルストーン（いつまでにどこに到達するか）を設定する。

(3)実行計画

投入すべき資源や実施方法、手順の改善、現状維持などを領域ごとに明確にして実行計画を作成する。実行計画には、必要に応じて組織化、教育を盛り込んでおく。この計画には、あらかじめ、どの時点で実施状況を検証するかについても明確にする方がよい。資源の投入や手順の変更などを予定している場合には、目標や費用対効果の測定手段も検討しておくとよい。

(4)進行管理

実施にあたっては、それが単なる手順の変更であっても、適切なモチベーションや支援を必要とする。また、計画に沿って実行できているか、新たな計画が必要とされるかなどを、計画した時点または定期的にチェックする。問題があれば小さなうちに処置できるよう、コミュニケーションや処置方法についても進展に応じて計画しておく方がよい。

(5)達成状況などの評価

計画通りの効果が上がったか、改善の必要がないかを評価する。できていると思っていてできていないことは、全くできていない状態よりも始末に困るものである。

2.法規・ガイドラインなどの理解

適用される法規やガイドラインについては、背景となる考え方についても知識を得ておくことが望まれる。個人情報保護であれば、上手に活用するために守らなければならないことを定めているのであり、アンタッチャブルにするということではない。また、何故そのような配慮が必要かを知らないと、見落として思わぬところからデータが漏れてしまう可能性もある。不正競争の防止とは、いわば他人のふんどしで相撲を取らないということだから、自己、他人を問わずオリジナリティを大切にするということでもある。顧客に他社の試作品を見せたりしたら、両方の信頼を失うことになる。

また、個々のケースの判断についても基本がわかっていれば応用も利く。例えば、取引先から

営業秘密などの守秘契約を要求された場合、日常の実施事項だけに目をやっていたのでは、特急仕事で別ルートを使うなどという少々特殊な事態で簡単にボロが出てしまう可能性がある。

3. 落とし穴の検討

世の中には完全なものはあまりない。見落としも起こるであろう。例えば、コンピュータのデータを保護しても、出力されたリストや伝票を保護していなければ不完全と言われても仕方がないであろう。情報はいろいろな形を取ることがある。新規ビジネスの開発に夢中になるあまり、自社のものだからといって、過去に収集した個人情報の含まれるデータベースを制限なく利用することを考えてしまうかも知れない。ひとつの観点からだけ見ていては見落とすこともある。

気がつかなかったのだから仕方がないというのは外では通用しない。見落としを完全になくすことはできないと開き直るのは論外である。少なくとも、過去の失敗（仲間うちの話題や報道されたことがうちにもないのかと考えることを含む）を検証したり、採用した方法を別の角度から検討するなど、何らかの努力を惜しむべきではない。特に新しい業務システムや業務手順を採用した場合には、はじめから最後まで危険なところはないか観察するぐらいのことは、やって損はしない。不安があったら、監視手順も併用するとよいだろう。

4. コンプライアンス重視が基本

個々の企業で個人情報の数や営業秘密の有無などの状況は異なるが重要な法律リスクであることには変わりはない。

個人情報保護法では個人情報取扱事業者が定められている。しかし、今は規模が小さくて関係ないと思われても、事業規模が大きくなれば個人情報保護については必ず直面する。また、時間とともに顧客の意識が変わっていくことも考えなくてはならない。住民基本台帳ネットワークに関する訴訟で自治体が負けるケースが続いた。一般社会ではすでに個人情報保護が基本的人権であると認識している。どのような個人情報保護策をとっているかに答えられなければ、顧客はどう感じるであろうか？お得意様に「うちは個人情報取扱事業者じゃないからね。気にしていないよ。」と申し上げることができるであろうか？むしろ、大切なお得意様であれば、今までも口が滑って不利益になることがないよう注意していたのではなかったろうか。

不正競争防止法について、今回は営業秘密を中心に調査したが、元々は商標や表示の制限について制定された法律であり、コピー商品の輸入や販売などについても規定されている。ＷＴＯでは知的財産権の保護を推進している。今後とも強化されていくことが予想されている。

コンプライアンス（遵守）とは法令や公のガイドラインなどのルールを守るということである。金融商品取引法が成立した。その内容から日本版ＳＯＸ法（米国企業改革法のこと）と呼ばれることも多い。その一部に米国ＳＯＸ法と同じく内部統制や情報開示についての経営者の責任に関する条項が盛り込まれているからである。また、会社法（非公開会社が中心になった）にも内部統制の実施が明確にされた。こうした流れを受けて企業会計審議会では内部統制ガイドラインを

設けた。大本である米国の状況と比較すると、ＩＴについて追加、監査コストについては配慮されているが大筋は同じである。

参考のため、このガイドラインから内部統制の目的と要素を以下に示す。

(1)内部統制の４つの目的

①業務の有効性及び効率性

②財務報告の信頼性

③事業活動に関わる法令などの遵守

④資産の保全

(2)内部統制の６つの要素

①統制環境

②リスクの評価と対応

③統制活動

④情報と伝達

⑤モニタリング

⑥ＩＴへの対応

以上、好むと好まざるとに係わらず、コンプライアンス重視が経営に課せられている。

再び世間のことに目を転じても、ライブドアや村上ファンドは反面教師かも知れないが、フェアな競争、コンプライアンス重視の大切さを良く教えてくれた。横浜簡裁で三菱ふそうは行政上の命令がなかったという手続き上の理由で無罪になった。欠陥隠しは認められたのに報道陣を前に幹部が喜んでいたが、そういう勘違いをしていたのではもう顧客は戻らないであろう。顧客から支持を受けるには、従業員が誇りを持って働いてくれるには、サプライチェーンの中で一目置かれる存在になるためには、つまり大競争時代を生き延びようと思うなら、やはり、コンプライアンス重視が欠かせないものとなると考えられる。

5. 人の管理

数ある情報漏洩事件のうち、人から漏れたケースが圧倒的に多い。データに限らず、窃盗事件の進入経路などが元従業員から漏れた例もある。つまり、情報漏洩はコンピュータシステムの欠陥以上に、人を含んだセキュリティ体制のほつれによるところが大きい。また、経営資源（人、モノ、金）のうち最も重要でありながら、最も有効活用が難しいと言われるものも人である。

今日では、採用時に入社の条件として情報保護について誓約をさせ、入社後の教育などで徹底する方法が一般的となっている。また、情報セキュリティに取り組む企業では継続的な教育が常識となっている。安全教育と同じく、繰り返さないと効果がないと言われている。組織風土の中にルールの重視があることはもちろんだが、情報リスクについての共通認識も重要である。

退職者から情報漏洩が起こる場合、単に退職者のルールに対する認識や倫理観が不足している

ということだけでなく、退職者に敵対意識を持たれることも考えられる。後者は前者に比較して往々にして系統的、意図的であり、ダメージも大きくなることが想像に難くない。当然、ルールだけでなく情報リスクの認識についても教育により徹底することが必要だが、企業と従業員の関係が良好に維持されることも重要である。そのためには、企業の理念が広く理解され、従業員が高いモラール（意欲）を持って仕事ができるような環境整備が必要である。例えば、役割に応じた責任を自覚してもらうためには、能力に見合った責任・権限を与えることも必要であろう。従業員相互の協力を引き出すためには、情報の公開（共有化）も必要であろう。企業を大切に考えてもらうためには、処遇や能力開発で企業が従業員を大切にすることも必要であろう。つまり、退職者への対応には、企業と従業員の関係を改善することと共通することがある。

昔、商家では勤め上げた番頭さんに「のれん分け」を行った。今日でも人が育つと分社化を行うと言う企業がある。こうした従業員のライフサイクルを通じたキャリアプランなども、必要に応じて検討するべきかもしれない。従業員が辞めるときになって、ようやくあたふたと処置を講じるようでは、情報漏洩のリスク管理が上手だと言えないであろう。

6. 取引先の管理

中小企業では、好むと好まざるとに関わらず、ビジネスに他社とのネットワークが欠かせない。すべての関連業務を社内に取り込むことができるほど、経営資源に余裕がないからだ。それゆえに仕入先、販売先、業務委託先などとも、情報リスクについて協力し合える方が好ましい。単に契約書に盛り込むだけでなく（それはもちろん重要だが）、相互主義の立場で、共通する法律リスクを上手に管理する方法を明確にする必要がある。顧客の個人情報や営業秘密を共有することなく効率的な業務運営ができないからである。

この点（個人情報などの活用、契約など）は次節でも述べるが、普段からパートナーとして助け合うことが重要である。よいパートナーとは互いの目的を実現するため、頼りにすべき存在である。なぐさめ合うだけの関係ではない。時には切磋琢磨も大切である。

7. 第三者によるチェック

計画が進むほどに、活動が計画されたとおりに実行されているかどうか、法規やガイドラインとの適合性はどうか、実施手順に落ちはないか、コンプライアンス、人、取引先との取りきめが適切かなどを検証する必要がある。例えば、会社法では監査が必要である。これが会計監査だけでなく本来は業務監査を含む概念であることは先に述べた。ＩＳＯマネジメントシステムを導入している組織では内部監査がある。これらはいずれも内部で実施するものであるが、その効果を高めるために、企業の外から人を呼んでやってもらっても構わない。

特に、活動初期段階では、実施手順の構築、実施体制の整備、従業員や取引先の管理方法など、第三者による客観的な評価が好ましいと考えられる。なぜならば、これは法律リスクの管理だからである。事が起これば言い訳は効かない。世間の尺度で評価されてしまう。大企業の脱税事件

の報道では「税務署と意見が違う」という声が出るが、時として言い訳にしか聞こえないことがある。思いこみよりも客観的な事実が重要である。

第2章で述べたようにすでに取り組みを開始している企業で自社の取り組みをチェックしたいというニーズがあるが、これはきわめて健康的な反応と思われる。なぜならば通常物事は遅くなるほど対処が難しい。だからリスク管理は予防につきる。予防医学と同じく、問題が起こる前のかすかな予兆を客観的に検出する「検診」が必要なのである。