## 第 13 回 DM フォーラムより

△▼△▼△▼△▼△▼△▼△▼△▼△

### 個人情報法保護法／<br>多くの事業者がつまずくポイントと、その解決策

㈱シーピーデザインコンサルティング<br>代表取締役社長　鈴木　靖氏

**個人情報保護対策は誰のため？**

タイトルの通り、個人情報保護法にはつまずく点が多い。しかし、つまずく以前に間違った道を歩いている方が中にはいる。従業者に対して、個人情報保護法の勉強会やテストを熱心にしている会社でも、何を目的に、誰のためにやっているのか聞くと、答えが出ないところもある。驚いたことに、社長や会社のためと思っている方も多い。当たり前のことだが、個人情報保護は社長のためではなく顧客のためだ。そのことをはっきり理解していただきたい。

私が実際見た例として、個人情報保護法が施行された 4 月 1 日をもって、これまでのポイントカード制度を廃止し、ポイントカードの顧客情報を全て廃棄した会社があった。これは、狂牛病問題が起こったときの事例とよく似ている。そのときの対策法は、牛肉を提供するのをやめることだった。そうすれば自分の会社の牛丼で狂牛病患者が出ることはない。同じように個人情報も、全て廃棄して明日からはもう使わないという解決でいいのだろうか。誰のための情報廃棄だろうか。これは、何かあると会社が傷つくという考えが根底にある。本来は顧客のことを第一に考えるべきなのに、それが浸透していないために生活者が安心して個人情報を預けられなくなっている。

個人情報保護法に怯えて個人情報を取り扱わないようにするか、当社の個人情報取り扱い方針はこうだと正々堂々と表明していくのかが大きな分かれ道。安心して個人情報を預けられる会社と見てもらえるかどうかが重要だ。そこを踏み外してしまうと、お客様からは正確な情報をもらえず、今後のビジネスが成り立たない。

**法対応の次の段階－プライバシーマーク－**

法対応はやって当たり前だが、その次の段階でとまどいがあるかもしれない。一つは継続性の問題。法対応では、違法か適法かという、ある時点のところだけに目がいってしまう。教育や監査を定期的に行うなどして、活動を継続させる必要がある。また、この法律では、簡単に白か黒かはっきりしないという問題もある。尼崎の脱線事故が起こったとき、家族が病院に担ぎ込まれたのかどうか教えてくれと言ったにも関わらず、病院は個人情報だから開示できないとした。しかし、本当にそれでいいのか答えは出なかった。現時点でどう判断するか、また、状況によってどう変化していくか、法律ではそこまで規定されていない。

そこで、今注目を集めているのがプライバシーマーク。プライバシーマークは、4月の施行以前は取得企業が約千社だったが、現在は二千社を超えている。最初の段階では、情報処理の会社が中心だったが、現在は B2C をしている会社まで広がっている。先に述べたような継続性や向上性を築きあげるために、プライバシーマークの取得はその手段となりえると考える企業が増えたのではないだろうか。

**個人情報取扱い契約とは？**

4 月 1 日以降、顧客と事業者（以下A社）の間には‘個人情報取扱契約’が成り立つと見なされる。‘個人情報取扱契約’には3つの項目があり、1つめは利用の範囲を目的縛りと事業者縛りで制限していること。目的縛りとは、生活者が想定していないような使い方をしてはいけないということ。事業者縛りとは、顧客が個人情報を渡したA社以外に無許可で他の会社に渡してはいけないということ。2つめは正確性と安全性の確保。3つめは透明性を確保し、苦情対応を行うこと。このことを、生活者の目線でもう一度見直す必要がある。

**「個人情報保護法を守れない」という結論**

しかし、見直しを行った結果、特異な対応をとるケースもあった。あるホテルは、「個人情報保護法を守れない」という結論を出した。そこは VIP が泊まるような高級ホテル。VIP が誕生日だと、部屋に花束とメッセージカードが贈られる。個人情報保護法では、個人情報を取得した場合、利用目的を本人に通知、公表しなければならないが、VIP の方には花束を贈るために誕生日の情報を利用させて頂きますとはもちろん伝えない。そんなことをすると、せっかくのサービスが台無しだ。これは個人情報保護法には反しているが、お客様の視点で見ると、苦情は出ないだろう。また、メッセージカードには、支配人の名前でサインしているので、本人は、私が前に挨拶した支配人から花が届いたと喜んでくれることだろう。もちろん、これは特殊な例であり、万が一のリスクも残っている。しかし、今やるべき事は、それを踏まえた上で、生活者の立場に立って見直すことだ。

**自分の業務にまつわる作業を見直す**

生活者の視点で考えるようになったら、次は会社の中を見渡してどこまで想像できるかだ。現在、あなたが担当している業務の中での個人情報の取得、入力、送信、利用などについて、いつ、どこで、誰が、何のために、どのように作業をしているのか説明を求められても、その全ての質問に答えるのはかなり厳しいだろう。

解決の一歩は、まずアクセス制限とアクセスログを取っておくことから。少なくとも一つ一つの項目のアクセスを制限し、その部分にタッチできる人数をとにかく減らす。そして、アクセスした記録をできる限り取っていくことだ。

ある大手のブロードバンドの会社が、450 万人の個人情報漏洩事件を起こした。第一次の対外発表で、漏洩した個人データの対象者 240 名（後に実際は 450 万人とわかった）を特定したと発表した。同時に、漏洩した個人情報データの項目が特定できたとし、漏えいした情報はどの項目かあえて言わずに、クレジットカード番号と銀行口座番号は含まれていないと発表した。漏洩の原因は不明。会社は最初、135 名のシステムエンジニアでなければデータベースにアクセスすることができないと答えたが、これは事実ではなかった。犯人は、元派遣社員のオペレーターだと後に分かった。当然オペレーターはデータにアクセスすることができる。しかし、検索キーを使ってヒットした分の情報しか見られないようになっており、全データを見ることはできないという理由で漏洩ルートの対象からはずした。なぜオペレーターが全件データベースを盗むことができたかというと、全件ヒットするようなキーワードを入れれば全てのデータをみることができたのだ。こんなことができるようなシステムを入れていたことがそもそもの問題で、起こるべくして起こってしまった事件だ。

最初は、アクセスログを見れば誰が犯人なのかすぐわかると思っていたが、1週間分のアクセスログしか残っていなかった。これに総務省からクレームが付いた。これは、事件があって初めてわかったこと。その後、オペレーターが全件ヒットできないようにシステムを改善して、常時アクセス可能な者はシステムエンジニアの3名に絞った。

システムにはある程度のアクセス制限があっても、出力してバインダーに綴じたものをキャビネットに置き、そのキャビネットの鍵が誰でも使えるところにあるということもあるかもしれない。様々なケースでもう一度項目を確認して、できる限りのアクセス制限とアクセスログを追求することが必要だ。

**個人情報の適正管理をするには**

**1. 案件の整理**

一つの会社の個人情報取扱案件数は、約 300～700 件ある。もしみなさんの会社で案件数がそこまで挙がっていないとしたら、おそらく調査が至っていないということだ。一つ一つの案件を整理するには、どういう関係の案件なのか親帳簿を作り、それに基づいて 300～700 件の子帳簿を作るという作業から始まる。子帳簿を作る時に重要なのが、管理者は誰なのか、利用目的は何なのかをはっきりさせること。利用目的の欄を見ると、○○帳簿などと平然と書く人がいるが、「利用目的」と「利用」は全く違う。このことは各種ガイドラインでもうまく説明しきれていない。利用目的は、あくまで本人に何が起こるかということ。たとえばDMが届く、アフターサービス時に本人確認に使う、などのようにできる限り特定しなければならない。

**2. フロアマップの整理**

個人情報取扱案件を整理すると同時にフロアマップを作成していく。個人情報を全く取り扱わないAゾーン、取り扱うBゾーン、専門に取り扱うCゾーンに分ける。もちろん、もっと多くの段階に分けても構わないが、最低限3段階の仕切りが必要だ。時々、うちの会社は狭く、3段階に分けられないのでBゾーンとCゾーンの2段階でいいですかと言う人がいる。しかしそれは大変。なぜかというと、Bゾーンは個人情報取扱場所なので、入館管理、つまり部外者が入ってきたときは記録を残していただきたい。ということは、郵便配達の人などが来る度に入館記録に記入してもらわなければならない。そんなことは実際できない。できないとそこから穴が空いていく。

個人情報を置かないAゾーンは必要だ。AゾーンからBゾーンに入るときには部外者の記録を残し、BゾーンからCゾーンには従業者しか入れず、従業者でも入室記録を取る。このように、目に見えるようなゾーニングをした方が良いだろう。これは、従業者に対して、現在会社が個人情報保護に向けての取り組みをしているとアピールする効果もある。

もちろんお金があればICカードを使って入退管理したり、指紋認証していただければ良いが、お金がない会社はどうするか。私たちがやった事例に、AとBの境目にビニールテープを貼っただけというケースがあった。ビニールテープを貼っただけでは人が入ってくるのではと思われるかもしれないが、入らないようにしたのは従業者の目。従業者が監視して、AからBに入ろうとした部外者はそこで止める。従業者の目がなくなる昼間や夜、営業時間外は鍵をかけるなど、できることはいくらでもある。

**3. 個人情報に触れる可能性のある取引先をどう扱うか**

次に、個人情報を扱う事業者の位置づけを整理しなければならない。個人情報保護法では、原則としては本人の同意なく、個人情報を取得した会社から他の会社に個人データを渡せないので、自社以外は「本人同意のある第三者」か「共同利用の先」か「業務委託先」の3つに振り分けなければならない。会社にある

多機能のコピー機には個人データが残っている。清掃業者がビル掃除でオフィスに入ってきたときに、机の上に置いてある個人データを見る可能性がある。機械のメンテナンス会社、ビルのメンテナンス会社、警備会社などは業務委託先に入れるしかない。業務委託先の選定をして、契約を交わさなければならない。

例えば、プロバイダにサーバを預けていて、そこに不正アクセスがあったとしよう。プロバイダには自分達以上の知識があるとして頼んでいたのだから、委託先管理について私たちは責任があるとしても、世間も同情する。しかし、受け渡しの過程で無くしてしまったケースは、みなさんが十分に管理することができたこと。まずそこをきちんと整理する。そして、委託先においてアクセス制限とアクセスログについてルールを作り、随時報告してもらう。作業者と使う場所を限定し、どのような方法でアクセス制限するのか取り決め、アクセスログは全部残してもらう。もしそれに反すれば、契約打ち切りなども視野に入れる。今まで交わしていた契約を見直し、アクセス制限とアクセスログについて再確認すべきだ。

**4. 利用目的の明示**

次は利用目的の明示について。弁護士には、できるだけ目的を幅広に書いた方が、目的外利用と言われないで済むと言われるかもしれないが、そうすると最終的には会社の信用を失ってしまう。私は逆に「お客様からいただいた個人情報は、商品の発送のためにのみ利用させていただきます」と「にのみ」という言葉を使うことをおすすめする。そうすると、DM発送などはできなくなる。困るのならば、最初からDMを送るということを書く。もし後になって使いたくなった場合には、本人の許可を取る。そこをあいまいにしていると、現場はあれにもこれにも使えるということでどんどん管理が甘くなってしまう。もちろん、縛りをきつくし過ぎると、現場が悲鳴を上げる。しかし、利用目的の明示は、現場を縛っているのではなく、生活者が安心して個人情報を渡せるようにするため。その点を周知徹底してもらう。

**開示などの対応手順**

電力会社は、電気料金の支払いが終わっているかどうかの開示請求が一日に何十件もくる。そこでまず本人確認をすると、ご本人ではないことが多い。電力の加入者はご主人だが問い合わせは奥様という場合がある。その時、杓子定規に「加入者本人でなければ個人情報の開示はできません。ご主人からの委任状と、あなたが奥様だという証明に住民票取ってきてください」と対応すれば、たちまち日々の業務に支障が出る。まず、開示請求が軽微か軽微でないかということを分けなければならない。軽微なら、本人ではなくても情報開示する。そのリスクと実際の現場の仕事を天秤に掛けて、何万分の一のリスクのために毎日繁雑な作業はできないという判断をしている。

**まとめ**

個人情報の漏洩を起こしやすい企業の共通項がある。まず、インターネットがなかなかつながらない。これは、従業者がネットで遊んでいることを意味する。もちろんそういうことをやる従業者がいけないが、もっと悪いのはその上司。管理職が部下の面倒を見ていない。部下がどういう画面を見ているか、部下の背中に回ったことがない。管理職と部下の席が離れていたり、パーティションで仕切られていて中で何をしているか分からず、ひどい会社だと従業者と部外者の見分けさえついていないこともある。

いくらルールを作っても、従業者が他人事だと意味がない。組織として推進し、私たちには説明責任があるということを大原則としなければならない。個人情報を誠実に取り扱っていれば、お客様の信頼も得られるということを、従業者に伝えていく必要がある。自分達が張本人なのだから、自己防衛のためにも、作業者がやるべきルール、管理者がやるべきルール、利用目的、正確性・安全性の確保、要求対応について個人情報を取得する前、利用中、利用後に分けて、どう対応するのか答えを出す。そうすれば、守るべきルールが運用レベルで見えてくる。それを現場レベルに落とす作業に取りかかって欲しいと思う。