Technology Transfer
テクノファNEWS

企業における〝個人情報保護法〟への対応

（有）アドバンス・ティ　代表　富永卓椰氏

テクノファは創立以来１０年、ＩＳＯ監査実践研究会総会を毎年一回開催して来た。１１年目を迎えて『テクノファ年次フォーラム』と衣替えをし、引き続き最新情報を提供して行くことになった。

本号は１１月２５日のフォーラムにおいて行われた講演の中から、情報セキュリティのエキスパート、富永卓椰氏による『企業における個人情報保護法対応』（要旨）をご紹介する。

個人情報とは　個人情報保護に関する法律(以下、個人情報保護法)の定義は、生存する個人に関する情報である。当該情報に含まれる氏名、生年月日、その他の記述等により特定の個人を識別することができるもの総て、また、他の情報と容易に照合することができるものも含まれる。

諸氏はJIS Q 15001(1999)やプライバシーマーク制度をご存知であろう。15001は個人情報の保護に関するコンプライアンス・プログラムの要求事項をまとめたJIS規格である。その定義においても、「生存する」という言葉はないものの基本的には個人が識別されれば個人情報である。参考までに法律はJIS Q 15001をもとに検討された。

今回の法律のスキームとして、個人情報保護法で言い表わせない部分については関係省庁がガイドラインを作ることになっており各省庁が対応した。話の中では経済産業省(以下、経産省)のガイドライン(10/13改訂版)を引用していく。

経産省ガイドラインに個人情報が例示されている。個人情報の対象は幅が広い。本人の氏名は容易に想像がつく。更に生年月日、連絡先、会社の

（有)アドバンス・ティ 代表　富永卓椰氏

職位・所属等と本人の氏名の組み合わせ、これも個人情報である。

防犯カメラの映像が上げられている。よく会社入門口や構内で撮影されている。録画されたものが一定期間保存される。これも個人情報である。本人の顔が映っており、本人が特定できるということである。会社で録画する時は要注意である。

特定個人が識別できるメールアドレス情報も対象だが、管理が難しいところである。@マークのあとは会社の識別になっているのが普通だが、@マークの前はどうだろう。社員番号や記号などが付けられていることもあるが、大抵はその人の名前が付いているだろう。多い姓になればフルネームになる。

会社にはメールサーバーがある。そこに貯まったのが個人のPCに配信される。皆さんにもいろいろな人からメールが来るだろう。そのメールを個人情報として管理せよといっているのだ。便利のために作ったメールアドレスのリストも、個人情報として対象になる。この辺は結構影響力が大きいだろう。

雇用管理情報、言うなれば社員情報である。今回の法律は顧客情報とか社員の情報、派遣社員などという区分をしていない。だから顧客情報も社員情報も同じように管理しなければならない。

あとでも出てくるが、開示請求を考えてみよう。顧客の開示請求には通常「苦情相談窓口」や「お客様対応窓口」が作られていると思う。然らば社員の開示請求はどこで受けるか。決まっていないというのが結構多く、多分人事とかがやるだろう。この法律には、対外・対内という壁がないのである。

官報、電話帳、職員録等で公にされている情報も個人情報である。例えば電話帳は「電話をかける」という明確な利用目的なら良いが、他の目的に使うと許されなくなる。職員録とか社員帳、社員名簿、よく問題になる住民基本台帳なども利用目的以外に使うことができなくなる。

また、個人情報に該当しない事例として3つ上げられている。個人ではない法人の情報、特定個人が判別できないメールアドレス情報、そして統計情報である。サマリーされた統計には個人の名前はない。携帯電話のメールアドレスは簡単に掛かって来ないよう複雑なアドレスを頭につける。特定個人が判別しにくいので個人情報には該当しないのである。

ひと口に個人情報と言っても結構いろいろな処まで絡んでくることはお分かり頂けただろうか。

個人情報漏洩事件の実態　個人情報が漏洩した事件が幾つも起きている。説明は省くが、強調したいことは損害賠償の金額が凄く高くなっていることである。この法律が適用されるともっと高くなるだろうと思う。もう一点、情報漏洩事件は社外というよりは社内の人間が絡んでいると思って頂きたいことである。外部の人間の出入りに厳しく対応しているところは多いが、社内の人間や委託や派遣の人に対しての管理は出来ているだろうか。はっきり言って不十分だろう。誘因になるかと思う。

ひとたび事件が起こると莫大な出費になる。直接的な被害として個人情報の回収や回復にかかる費用、そして損害賠償に何億円も掛かったりする。間接的な被害も大きい。イメージダウン、信用力の低下、売上の減少がついて回る。

今も後遺症を引きずっているある通信会社は、事件直後契約が半分近くに減ったと聞いた。現在は少し回復したようだが、企業のイメージダウンは結構大きかったようだ。その他にも信用ダウンによる株価の低下、与信枠の減少、M&Aは言い過ぎかもしれないが、そこにもつながっていくかもしれない。

何故会社の人間が漏洩事件に関わるのか。社内の人間は情報へのアクセスが容易に出来る。システムの設定とか仕組みなどに精通している。正式なユーザーID、パスワードを持っているので、その情報まで行くのは当り前の世界である。その気になればいつでも引出すことはできる。

彼らは不正アクセスを成功させるヒントを沢山持っている。会社には中枢にサーバーがある。サーバーの管理者名も知っている。例えばユーザーIDが社員番号であったり、パスワードがその人の名前かもしれない。そんなヒントから知るところになったりする。それも中に入っていく誘因になるだろう。

漏洩問題は発見が難しい。外部の者には入退出まで厳重にチェックする。ネットワーク系で進入するものもファイアウォールで厳しいチェックが掛かる。しかし中の人間にはどうだろう。例えばメールのやり取りを検閲するところは殆どないだろうから、情報のやり取りは自由である。その気になれば重要な情報をサーバーから取り込むことができる

「テクノファNEWS第57号」訂正とお詫び

8頁(左13行)のご紹介記事に誤りがありました。
深くお詫びを申し上げますとともに訂正致します。
(誤)　リコー株式会社　金本副社長
(正)　リコー株式会社　紙本副社長

ということである。

最後に利用者、利用形態が多様化していること。会社には社員のほかいろいろな雇用関係を持つ人が大勢いる。そしてネットワークで物理的に LAN がつながっている。モバイル PC などは幾らでもアクセスできる。つまり情報は幾らでも洩れてしまうということになる。

これはマネジメントの問題だと思うが、情報管理が不徹底だということである。会社や家も含めて情報が資産として体系的に、何処にどれだけあるか把握されていないことが多い。把握されていないから倉庫にあった個人情報がなくなっても分からない。

あとはマネジメントの問題としてルールがないこと。ないから守れない。またルールはあってもきちんと運用されるまでに落とされていないこともある。マネジメントシステムとしては不適合である。ルールがないのは重大な不適合と言うべきだろう。

これが法律となると訴訟が起こる。例えば社員が漏らしたとしよう。会社にはルールがなかった。それは会社の管理がへぼかったからで、会社の過失が大きくなってくる。「不適合」への対応として、会社はいろいろなルールを文書化しておかなければならない。そして社員に伝えておかなければならない。ここがもの凄く重要になってくる。

法律は、各所に「手順をつくれ」と書いてある。手順がないと致命傷になる。漏洩事件の背景などから話をして来たが、これから法律の概要をお話したい。

個人情報の保護に関する法律　この法律は、全 6 章よりなる。時間がないので第 4 章、「個人情報取扱事業者の義務等」を中心に説明させて頂く。その前に用語の定義をしておきたい。

第 2 条、「**個人情報**」の定義。生存する、特定の個人を識別する、容易に照合する…ということがキーワードだと冒頭に申し上げた。

この法律には JIS Q 15001 にはなかった「生存する」が加えられた。本人の権利利益の侵害を未然に防止することが法律の目的なので、開示、訂正、利用停止等の請求は本人でなければ出来ないということである。ただ通常は死亡すると遺族のところへ墓地の売り込み等に訪れることがある。そうすると死者の情報が遺族の個人情報に転化するので、遺族に対する個人情報侵害ということにもなる。しかしこの法律は本人の没後は対象にならないことを明示している。

「特定の個人を識別する」、個人が識別できれば総てが対象になると考えてほしい。名前があるものは基本的に対象だと思って頂きたい。そういうものは会社の中にはいろいろあると思う。顧客の情報、名刺のファイルも個人情報として考える。これから年賀状の時期になる。コンピュータで出すことが多いが、ファイルされた年賀状のリストなども特定の個人を識別するものとして、法律の対象になってくる。

「容易に照合する」、特別な費用、手間をかけることなく照合できるものは個人情報である。

またコンピュータの話になるが、通常は社員番号とか契約者番号につけていろいろな情報を一つのファイルにして作っておく。一方、社員番号と社員の名前、或いは契約者番号と契約者の名前というファイルが別にあって、実際に処理する時はヒットさせて出力することが多い。社員番号と社員の名前が入っているものはもともと個人情報として管理しなければならない。一方の社員番号だけのファイルも、「容易に照合する」ことができるからこれも管理の対象にしないといけない。これだけ上げただけでも相当、情報としては広がったと思って頂きたい。

「**個人情報データベース等**」。個人情報を含む集合物である。①電子計算機を用いて検索できるもの。コンピュータにファイルとして入っているものと思って頂きたい。②容易に検索することができるもの。要はカルテとか、問合せの葉書の束とか容易に検索することができるのであれば「個人情報データベース等」に入る。まとまりがあるものは個人情報データベース等と思って欲しい。

個人情報データベース等に該当する例
- 電子メールソフトに保管されるメールアドレス帳
- ユーザーID とログ情報が保管された電子ファイル
- 名刺情報を業務用パソコンに格納、他の社員が検索できるもの
- 限定された（五十音順に整理した…）人材登録カード、例えば社員の履歴書とか社員ファイル。
- 氏名、住所、企業別に分類整理されている市販の人名録

該当しない例
- 他の社員が分からない分類がされている名刺
- 乱雑に保管されているアンケートの原票。

ガイドラインは、上記の通りである。

それらの個人情報データベース等を「**事業の用**」に供している人が「**個人情報取扱事業者**」である。

「**事業の用**」とは、社会通念上事業と認められるもので、営利、非営利は問わない。例を上げてみよう。ある人がホームページを立ち上げている。特に料金も取っていない。誰かがアクセスして意見などを書いてくる。すると履歴が残る。ホームページを立ち上げている人は「個人情報取扱事業者」になる。事業者とは言っても普通の会社だけではなく、いろいろなことで「個人情報取扱事業者」になると思って頂きたい。但し、国の機関、地方公共団体は除外。権利利害を害するおそれが少ない者も除くという制限が付く。過去 6 ヶ月の 1 日でも 5,000 名を超える「**特定の個人の数**」を持たなかった者はこのおそれが少ない者ということである。1 日でも 5,000 名を上回ったら「個人情報取扱事業者」である。

ガイドラインの事例にある電子メールソフトに保管されるメールアドレス帳、例えば 50 名の社員が居てそれぞれが 100 名位づつデータを持っていれば 5,000 名、社員 50 名も含めれば 5,050 名となる。つまり「個人情報取扱事業者」である。

他の例を挙げよう。委託先とか発注先、又は製品の納入先などで、○○会社、××会社と書いて、担当者：誰々さんと書いてある。担当誰々さんと書かれていれば個人情報である。そういうリストがある会社は多いだろう。よく製造会社の人は我々の会社にはそんな個人情報はないと言われる。しかし社員情報、名刺の情報、更に取引先の個人情報と思われるものを足して本当に 5,000 名にならないだろうか。ならなければ「個人情報取扱事業者」ではない。普通ならば、5,000 名を超えてしまうのが一般的なのである。

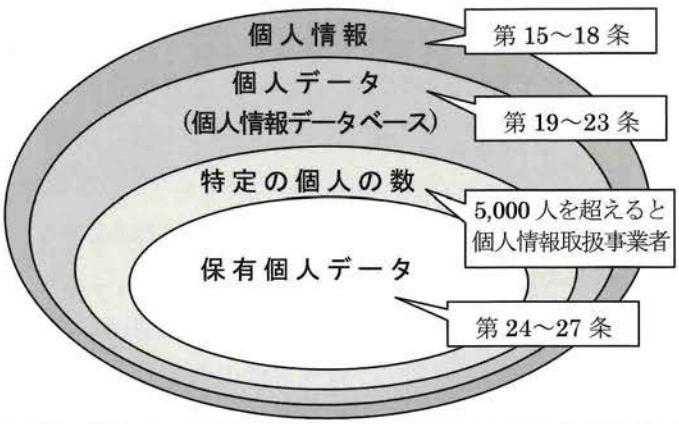
ただ、特定の個人の数に算入しないものがある(経産省ガイドライン)。そのまま使う電話帳、市販の電話帳 CD-ROM は数に入れない。カーナビゲーションシステム内臓情報、市販の地図情報…等々も省いて良い。電話帳を持った、カーナビ付自動車を買った、途端に個人情報取扱事業者、それはないだろうということである。

この中で注意を要するのは「倉庫に預かった荷物内や、データセンターで個人情報として認識しないで預かる情報の中の個人情報」である。これは認識できない…として、特定の個人の数に入れなくてもよいとされている。「荷物として預かっただけ」は理解できる。しかしデータセンターやアウトソーシングで預かる所では、よくバックアップしたりプリントアウトして個人情報が分かってしまうことがある。それは除いてよいというが、少し気掛かりだ。

個人情報取扱事業者には義務と罰則がある。

個人情報取扱事業者の義務 ◆利用目的 ◆適正な取得 ◆内容の正確性確保 ◆安全管理措置 ◆従業者の監督 ◆委託先の監督 ◆第三者提供の制限 ◆保有個人データの公表、開示、訂正、利用停止 ◆苦情の処理…これらの手順を作れという。個人情報を漏洩すれば当然罰せられる。しかし 3 月 31 日までに手順を決めなければそれも「違反」、罰則が掛かるのである。そう認識して欲しい。

「個人情報」等の位置づけ



図は「個人情報等の位置づけ」としてまとめてみたものである。まず用語の定義を補足する。

「**個人データ**」、個人情報データベース等を構成する個人情報をいう。「**保有個人データ**」、個人情報取扱事業者が開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権利を有する個人データ(6 ヶ月以内に消去するものは除く)をいう。

個人情報は冒頭説明したように広い全体である。この法律は個人情報全体に掛かってくる。個人情報取扱事業者の義務の 15 条から 18 条が個人情報に関係するところである。データベースに掛かるものが 19 条から 23 条。その中から電話帳などを引いたものが特定個人の数で、5,000 人を超えると個人情報取扱事業者になる。

その中で自分の会社で開示する権利があるもの、訂正する権利があるもの、それが保有個人データで24条から27条。必要なところだけをピックアップして簡単に説明しよう。

15条（利用目的の特定）、取扱事業者は個人情報を取り扱うに当って、利用目的をできる限り特定せよという。ここが曲者、できる限りとはどれ位か。経産省のガイドラインは「○○事業における商品の発送、アフターサービス、新商品・サービスに関する情報のお知らせ」のために使いたいので個人情報を下さい…と言えという。極端な事例だが、「記入された氏名・住所・電話番号は、名簿として販売することがある」、本人がOKと言えば名簿として出すわけである。

できる限り特定していない事例、「事業活動に用いるため」、「サービス向上のため」、「営業に使うため」。普通の会社はここまでOKを取っていなかったと思う。「営業で使うために個人情報を貰いますよ」、と言わなくてはダメだということである。利用目的はできる限り細かく特定する。今日も皆さんの情報が出されていると思うが、できる限り特定されているだろうか。

16条、あらかじめ本人の同意を得ずに特定された利用目的を超えて個人情報は使えない。同意とは、個人に伝えてevidence（証拠）を貰うものが同意である。経産省ガイドラインの事例には「同意する旨を本人から口頭又は書面で確認」とある。録音があればともかく、口頭は証拠が残らないので係争すると弱い。何かあった時には対抗できる書面がよい。

JIS Q 15001は同意を取れというところが多い。この法律では概ね通知と公表でよしとされている。但し「同意が必要」なところは二つ残った。一つが「利用目的を超えて使う時」、それだけ厳しく見られるということである。補足すると、経産省のガイドラインには「～すべきこと」、「～することがのぞましい」の二つの書き方がある。「～すべきこと」は、今回の場合ガイドラインとはいえ法律が適応されるものだと思わなければならない。「～すべきこと」を守らなければ、報告を受けた主務大臣が調査を命じ法を適用することがある。

17条、個人情報取扱事業者は、偽り、その他不正の手段により個人情報を取得してはならない。ここで注意するのは子供から取る時だ。子供は対面すれば分かるが、例えばホームページなどからとる時には分からない。注釈を加えて「親の同意を得ること」を明示しておかないと不正な取得になる。

18条は、利用目的は本人に通知し、又は公表すること。予め公表している場合はいい。ガイドラインによれば、通知又は公表が必要な事例はインターネット、官報、問合せ、クレーム等から取得する時。第三者提供により取得する時。利用目的を明示しなければならないのは、申込書、契約書、アンケート、懸賞の応募。

19条、持っている個人情報を正確かつ最新の内容に保つように努めること。法律を作る過程でもめたところだ。某先生は「パソコンボタンを3回も押せば個人情報は全部出てくる。従業員に一週に一度確かめさたらどうか」と言われた。それだけでも会社にひと仕事増えるくらい大変である。結局無理ということで避けた経緯がある。「正確かつ最新の内容」は、住所が変わったと言われた時に直せばいいことになった。

20条、個人データの安全管理をせよ。簡単に書いてあるが、要はセキュリティを保てということである。経産省ガイドラインでは、組織的安全管理措置（5項目）、人的安全管理措置（2項目）等を設けるよう18項目が上げられている。ISMSを知る人は分かるだろうが、要求事項を守れと言っているのだ。

法律の中でマネジメントシステムを守れという。守らなければ20条違反、主務大臣から指摘が来て、それでも守れなければ誰かが捕まる。行き過ぎと思うが、現在はそうなっている。

21条、従業者に対して必要かつ適切な監督を行うこと。MSで言う教育、内部監査のことである。経産省ガイドラインによれば、適切な監督とは従業者が社内規程に従っているか定期的に確認することである。定期的確認とは「内部監査」である。ＭＳをやれとしているわけで大変である。

22条、委託先に必要かつ適切な監督を行う。これも大変だと思う。委託先についてはいろいろ議論されもめた。情報サービス産業は特に何重もの入れ子状態で、最終的には個人がデータを入れていると

いう業界である。ここでいう委託先は一次委託だけでなく、最終委託先までを範疇とするのである。例え何次であろうと最終委託先まで必要かつ適切な監督を行えという。

監督とは何か。契約書だけではダメ。ガイドラインは契約内容が遵守されていることを確認せよ、立入検査をせよという。最終委託先まで立入検査をしなければ違法である。認識されたい。

23 条、第三者に提供してはならない。ここにも問題がある。ガイドラインによればグループ会社間も第三者、法人単位なのである。従来グループ間で情報を共有して使っていたのは第三者提供になる。第三者提供する時は本人の同意(これが二つめの同意)を得ること。同意を取らなければグループ会社にも渡せない。

大きな会社などは健康保険組合、共済会など別の団体にすることが多い。例えば会社が社員の情報を取る一次はよいとして、健康保険組合に渡す時には「第三者提供」になる。社員に健保組合に出すという同意を取っておかないと 23 条違反になるということである。

24 条～27 条、ここが保有個人データである。要は開示、訂正、利用停止をしてくれということ。そのための手順を設けよということである。保有個人データの詳細説明は省く。

30 条、通知、開示を求められた時は手数料を徴収できる。無料にすると業務妨害される惧れがある。行政機関では普通 300 円位だが、有識者レベルでは民間はもう少し高くてもいいかなと言っている。料金は各社で決めてもらう。

50 条、適用除外。マスコミ関係、著述業、大学研究機関、宗教団体、政治団体等は除外する。

この法律が一度廃案になった理由がここにある。マスコミ関係の適用除外要求で、それを容れたということである。

56 条、この命令に違反したものは、6 ヶ月以下の懲役又は 30 万円以下の罰金である。主務大臣から注意、勧告、命令と段階を踏み、それでも守らなければ刑事罰である。

刑事罰の後には民事訴訟が必ず付いて回る。ここで負けると民事でも負けるのが通説である。法律に罰則がつくということは、対応するマネジメントシステムに罰則がつくわけである。これは結構インパクトが強いと思う。

今後の進め方についてだが、いちばん初めにやらなければいけないことは、個人情報の定義を会社の中で決めること。その定義に従って個人情報を洗い出すこと。抜けがあるとそれが洩れても分からない。ここが一番重要である。ここだけをまずやってみると後はルールで何とかなるのではないかと思う。

個人情報管理の進め方(富永先生)

1．個人情報の定義を決定
2．定義に従い個人情報の洗い出し
　●業務、場所等を区分して洗い出し
3．リスクの段階を決定
　●顧客、社員、委託先等で分ける
4．洗い出した個人情報をリスクの段階で区分
5．個人情報管理 各種規程類作成
　●リスク毎の管理ルールを決める
6．社員、委託先へ教育する
7．ルールに従い実行する
8．社内、委託先の実施状況を監査する

レジュメに個人情報の管理の要点等、こういうことをやっていかなくてはいけないという参考も含めて付けている。読んで頂ければと思う。

個人情報管理の要点

◆個人情報の特定　企業として管理する個人情報の具体的な定義を決める(機密度の高い情報、メールアドレスの取扱い、年賀状リスト、人事情報等)
◆個人情報の管理　管理の最小単位をどうするか、単発と継続、階層(リスク)別とするか
◆委託先の監督　委託先との契約・覚書、再委託先以降、最終委託先までの監督問題、派遣元との契約
◆従業者の監督　従業者の範囲(定時・嘱託・派遣・アルバイト)、従業者との契約(誓約・同意)、教育・訓練等
◆個人情報保護管理者　管理者の選定、教育、M/R
◆内部監査と教育　監査員の独立性、監査計画
◆緊急時の体制　緊急時の想定、召集
◆顧客対応　開示・訂正・削除、受付窓口、非通常者

以上で話を終らせて頂く。ご清聴に感謝する。