



アナタの会社、対策は万全ですか？

個人情報保護法は 利用目的の 明示がポイント！

2005年4月、企業の情報セキュリティ戦略に大きなインパクトを与える、「個人情報保護法」が施行された。いよいよ本番を迎えたこの法律に対して、どう立ち向かうべきかを考えていこう。



止まらない 個人情報の漏洩

各種サービス提供のための会員データや営業のための顧客情報が漏洩した、というニュースが珍しくなくなって久しい。不正にデータベースにアクセスされた、あるいは顧客情報が入ったノートPCを盗まれたなど理由はいろいろだが、ひどいケースでは数万人、数十万人の情報が漏洩したというケースもある。

また、事故ではなく、収集した個人情報を故意に名簿業者などに販売するというケースも多い。名簿の種類によっては、買い取り価格が1件あたり数百～数千円に上ることもあり、金銭目当てに自社の顧客情報を不正に販売しているわけだ。

こうして漏洩した個人情報は、地域別や年齢別、あるいは趣味別などといった分類および加工が行なわれ、名簿業者の手によって販売される。名前も知らない会社から突然ダイレクトメールが送られてきたという経験は多くの人が持っていると思う。その裏にはこうした個人情報の流通があった。

個人情報保護法の 3つのポイント

個人情報にまつわるこれらのトラブルに対応するために施行されたのが、「個人情報保護法（正式名称：個人情報の保護に関する法律）」と呼ばれている法律である。

実はこれまで、個人情報の漏洩や流出を明確に罰する法律はほとんど整備

されていなかった。確かに1998年に「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」というものが公布され、さらに1990年に新たな規定が盛り込まれるなどして全面施行されてはいた。

ただ、この法律は行政機関が収集した個人情報の保護が目的であり、民間企業が保有する個人情報に関しては対象外であった。つまりそれまでは、民間企業の従業員がそれを持ち出して名簿業者に販売しても、個人情報の流出という観点では罰せられなかったわけだ（個人情報が保存された記録メディアを「窃盗」したとして起訴されたケースはあるが、個人情報を盗んだとして罰せられたわけではない）。

こうした法律の不備を解消する目的で施行されたのが今回の個人情報保護法であり、民間企業での漏洩や流出にも対応がなされている。

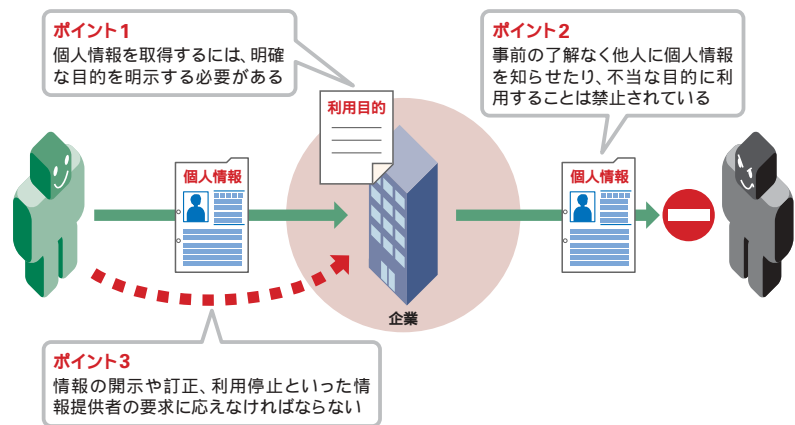
では、この法律では何を定めているのか。これを手っ取り早く理解するポイントは3つ挙げられる。

まず1つは、個人情報を取得するに当たって、利用目的を明示しなければならないというもの。たとえば、その個人情報を利用してダイレクトメールを送信するのか、あるいはマーケティング上の分析に利用するのかといったことを明文化し、提供を受ける際に通知しなければならない。もちろん、通知した目的以外で個人情報を利用することはできない。

2つめは入手した個人情報の内容を他人に知らせたり、不当な目的に利用することは禁止されているという点。あらかじめ本人の同意を得ていない限り、第三者に開示、提供することはできない。また個人情報を保有する企業は、従業員や外部の業者などを監督する義務もあり、たとえばダイレクトメールの発送を委託した業者から漏洩した場合でも、発送リストを提供した企業がその責任を負うことになる。

3つめは、情報の開示や訂正、利用停止といった、情報提供者の要求に応えなければならないという点である。

図1 個人情報保護法の3つのポイント



たとえば個人情報を提供したときに、利用目的としてダイレクトメールの送付という項目がなかったとしよう。それにも関わらずダイレクトメールが送られてきたときに、情報を提供した個人は利用停止を求めることができるようになったわけだ。

また、個人情報保護法では「講じなければならない対策」としてリスト1の内容を挙げている。ここまで紹介した3つのポイントに配慮しつつ、このリストに挙げられている対策を施せば万全の体制で対応できる。

個人情報は3つに分類できる

さて、ここまで書いてきた「個人情報」は、法律上大きく3つに区別されている。まず1つは取得したそのままの情報である「個人情報」である。その個人情報が検索しやすい形でデータベースなどに登録されると「個人データ」となる。そして、6カ月以上消去せずに保存される個人データのことを特に「保有個人データ」と呼んで区別している。

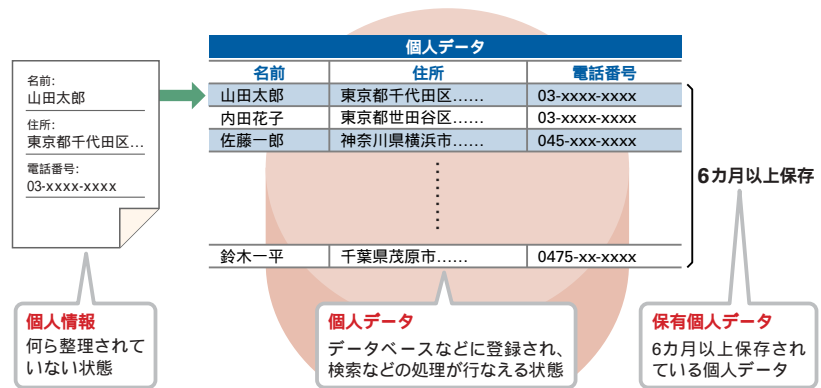
名刺に例えると、特に整理されていないバラバラの名刺はただの個人情報で、名刺上のデータを使って住所録を作成すると個人データになる。そして、これを6カ月以上消去せずにいると保有個人データということになる(図1)。

ここでポイントになるのは、保持している個人情報が5000件を超え、さらにそれが保有個人データに該当するか否かだ。これに該当すると「個人情報取扱事業者」となり、個人情報保

リスト1 個人情報保護法第20条に明記された「講じなければならない」18項目

組織的安全管理措置	
組織体制の整備	個人データの安全管理措置の評価、見直し、改善
規定等の整備・運用	事故または違反への対処
個人データ取扱台帳の整備	
人的安全管理措置	
雇用および契約時における非開示契約の締結	
従業員に対する教育、訓練の実施	
物理的安全管理措置	
入退室管理の実施	機器・装置等の物理的保護
盗難等に対する対策	
技術的安全管理措置	
個人データへのアクセスにおける識別と認証	個人データを取り扱う情報システムに対する不正ソフトウェア対策
個人データへのアクセス制御	個人データの移送・通信時の対策
個人データへのアクセス権限の管理	個人データを取り扱う情報システムの動作確認時の対策
個人データのアクセス記録	個人データを取り扱う情報システムの監視

図2 個人情報と個人データ、保有個人データの違い



護法を守る義務が生じる。逆に言えば、5000件以上の保有個人データがない、あるいは5000件以上の個人データを集めていても6カ月以内に消去していれば、個人情報保護法は適用されないということになる。ただ、法律的には適用されなくても、後述する情報漏洩によるリスクがなくなるわけではない。それを考えると、できる限り遵守する

ように努力すべきだろう。

個人情報1件あたり1万円!? 情報漏洩のリスク

個人情報保護法には、当然のことながら罰則規定も盛り込まれている。では、この法律を違反するとどのような処分、あるいは罰則が待っているのだろうか。

取得目的の明示や目的内での利用、あるいは情報漏洩といった事態を引き起こすと、事業を所管する主務大臣が「報告の徴収」「助言」「勧告」「命令」「緊急命令」などといった措置を講じるができる。その上で命令に違反すると6カ月以下の懲役、もしくは30万円以下の罰金に課せられる。また報告の徴収を放置する、あるいは虚偽の報告を行なうといったことで30万円以下の罰金に課せられるので注意したい。またこの罰則には両罰規定が盛り込まれている。これは、たとえば従業員が無断で個人情報を持ち出して転売した場合に、従業員だけでなく、雇用者である企業も罰せられるというもの。つまり企業に対する従業員の監督責任が、罰則規定の面からも問われていることになる。

ここまで読んで、命令違反をしてもただか30万円の罰金かと思うかもしれない。確かに金額の面からは大きなダメージにはならないだろう。ただ、企業イメージの観点から考えれば、刑事罰を受けたことによるダメージは無視できない。違反を犯して罰を受けた企業というイメージが広まれば、当然のことながら情報を提供する個人に大きな不安が生じるのは間違いない。また、取引先や株主からの信用が失墜するのも避けられないだろう。

また漏洩した各個人が、慰謝料を求める民事訴訟を起こすというリスクも計算に入れる必要がある。たとえば、住民基本台帳のデータが漏洩した「宇治市住民基本台帳データ大量漏洩事件」では、京都地裁が原告1人あたり1

主務大臣……個人情報取扱事業者が行なう事業などを所管する大臣を主務大臣と呼ぶ。

画面1・2 データベース監視に威力を発揮する「IPLocks」



万5000円（5000円は弁護士費用）の慰謝料を支払うように命じている。もし、1万人の情報が漏洩すれば、1億5000万円であり、被告人の数や企業規模によってはあまりに大きな損害となる。それだけ個人情報は「高価」なものと認識し、運用する必要があるといえる。

データベースを監視して 情報漏洩を防止

さて、こうした個人情報の漏洩によるリスクを避けるために、さまざまなメーカーから多様なセキュリティソリューションが登場している。ただ結論から言ってしまうと、漏洩リスクを完全にゼロにすることはできない。いくらセキュリティを固めても、技術的に完全に抜け穴をふさぐことは難しいからだ。しかし個人情報にアクセスできる人間のモラルだけに頼り、何ら対策を施さないのも問題である。

そこでぜひ実施したいのは、蓄積された個人情報を容易に管理できる環境を構築することだ。具体的にはクライアントPC上に顧客情報を保存することは禁止し、すべてサーバ上のデータベースで一括して保管する。その上で必要なデータについては、ネットワー

ク経由で随時参照する、といった形である。これなら漏洩に対して注意すべきポイントを1カ所に絞ることが可能となり、データベースだけを監視しておけばよいことになる。

なお、データベースの監視というと、データベースソフトから出力されるログのチェックということになる。ただ、特にデータベースへのアクセスが頻繁に発生している環境などでは、すべてのログをチェックするのは現実的ではない。こうしたジレンマを解消するための代表的なソリューションとしてアイピーロックス ジャパンの「IPLocks」が挙げられる。これは情報流出などの継続的な監視を可能にしているほか、監査や分析のための機能も提供している。

個人情報保護法への対応で、もっとも重要になるのは社内体制の整備だろう。いくら総務部や情報システム部門などがあくせくと対応しても、個々の従業員の意識が低くてはせっかくの対策も水の泡になるためだ。すでに施行されたが、改めて社内体制をチェックし、ガイドラインに不備がないか、個人情報保護法の重要性が各従業員に伝わっているかを確認すべきだろう。