ウェブマスターにもメール配信者にも法の網

知らないでは許されない「個人情報保護法」対策

text：JNSA/個人情報保護ガイドライン作成WG
株式会社大塚商会　S&S本部　佐藤憲一、小林健
協力：日本ネットワークセキュリティ協会（JNSA）
illust：小松恵

いざとなってから勉強しても手遅れ
法律を正しく読み解いてポイントをおさえよう

2001年3月27日に最初の法案が出されていた「個人情報の保護に関する法律」（個人情報保護法、以下「保護法」）が、2003年5月30日に公布された。個人情報取扱事業者の義務や罰則規定は、公布日から2年以内に施行される。現段階では、早ければ来年の後半から全面施行されると予想されているが、対策を考えるにはまず保護法がどんな内容なのかを理解しよう。

JNSA（日本ネットワークセキュリティ協会）の渡部章氏が、表1のとおり個人情報の漏洩事件まとめている。このような事件の多発、コンピュータやネットワークの普及による大量の個人情報の集積と流通などの社会環境の変化に対して、個人を守る必要が高まったことによって制定されたのが保護法である URL 。

「個人情報」とはなにか？

保護法は、「生存している」人の「特定の個人を識別することができる」情報を「個人情報」（第2条1）と言っている（図1）。しかし、「死者に関する情報」は保護法の対象ではない。ただし、生存者に影響のある遺伝子の内容などは保護法の規定する個人情報になる場合がある。また「個人を特定できない情報」も対象外だが、顧客番号によって顧客リストと照合すれば個人が特定できる「販売履歴」といったものは保護法の規定する個人情報になる場合がある。

この個人情報を、5000件以上コンピュータで管理しているものが「個人情報データベース等」（第2条2）で、このデータ

表1：おもな個人情報の漏洩事件

日 付	概　要
2003年 6月26日	大手コンビニエンスストアであるローソンの発行するカード会員約56万人分の氏名、住所などの個人情報が社外に流出
2003年 6月11日	海上保安庁の職員が勤務中に職場のコンピュータを使用し、インターネット上の掲示板に書き込んでいたことが判明。同庁は内部調査を行い、書き込みを行った職員を特定し、口頭で厳重注意を行った
2003年 6月 9日	神戸市に本店のある富士信用組合は、本店の元融資部課長代理が、兵庫県内の法人や個人の手形不渡り情報計3515件を無断でフロッピーディスクにコピーし、大阪市内にある消費者金融業者に渡したとして、窃盗容疑で生田署に告訴
2003年 1月23日	顧客7人の口座番号と貯金残高を探偵事務所の従業員に教え、その見返りとして金銭を得たとして、さいたま市の浦和田島郵便局職員を再逮捕
2002年12月19日	エステティックサロン大手のTBCを経営する「コミー」が管理する5万人余の個人データが流出した問題で、迷惑メールやいたずら電話で被害を受けた10人が同社を相手に総額1,150万円の損害賠償を求める訴えを起こす
2002年12月 4日	三重県四日市市で、市の職員が住民情報オンラインシステムを使用し、住民の個人情報を不正照会した疑いが出ている問題で、四日市市は、「市の独自捜査では限界がある」として不正アクセス禁止法違反の疑いで、職員を特定しないまま四日市南署に告発
2002年10月25日	大分医科大の男性教授が部下の女性技官の電子メールを無断で閲覧していたことが発覚し、この教授を6か月の減給処分に、また、この教授とは別に、職員9人のパソコンに侵入した男性技官を戒告処分にしたと発表

ベースに入っている個人情報が「個人データ」(第2条4)とされている。さらに、仕事をするために「個人情報データベース等」を使っている場合は「個人情報取扱事業者」(第2条3)とされ、保護法のうち「第4章第1節　個人情報取扱事業者の義務」(第15条〜第36条)と、これに違反したら罰を与える「第6章　罰則」(第56条〜第59条)が適用される。

個人情報の不適正な取り扱いとして保護法の規制対象となるものは、(1)個人情報の漏えい(2)個人情報の不正な入手(3)個人情報の不正な利用(4)個人情報の目的外利用(5)第三者への無断提供(6)管理監督義務違反の6つである。この6事項のいずれかに関する苦情が本人から出され、企業や業界団体などによる民間努力で解消できなかった場合に、その企業の業界を所管する省庁などの「主務大臣」が事態の収拾を図ることになる。

主務大臣は、最初に事実関係や双方の主張を聞くための「報告の徴収」を行い、企業に非のある場合は「勧告」する。この段階で事態収拾に急を要する場合は「命令」による強制解決を図る。通常は、勧告に企業が適切な対応を行わない場合に命令を行う。

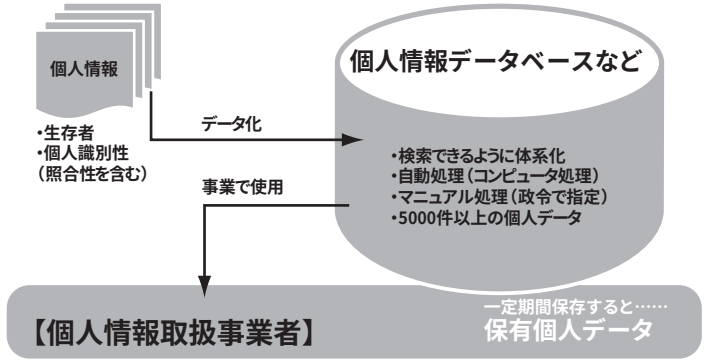
そして命令しても、企業が事態を適切に解決しようとしない場合などは、保護法第56条から第59条に規定している「6か月以下の懲役か30万円以下の罰金」が科せられる。また、企業の従業員が主務大臣の命令に従わなかった場合などは、従業員が罰を受けるとともに、第58条に基づいてその企業も罰金を払わなければならない。

なお、主務大臣に苦情を出さなくとも従前のトラブル解決のように裁判所に持ち込むこともできる。

保護法は、「個人情報取扱事業者」以外の民間の組織や個人には罰則を規定していない。第3条(基本理念)に規定している内容しか適用されない。つまり、個人情報を「個人の人格尊重の理念の下に慎重に取り扱う」ように「図られなければならない」だけで、具体的に何をしなければならないとか、何をしてはだめだとはされていない。従来の刑法などの法律で罪になることを行ったり、訴えられて裁判で負けないかぎりは罰せられない。

以上をまとめると、保護法はコンピュータで処理される個人データ、またはコンピュータで処理することができる個人情報を事業や仕事に使っている企業に対する規制となる。よって、本稿は保護法の影響を受ける個人情報取扱事業者について「企業」と記述し、企業でウェブサイトの構築や管理、またはメールを配信するようなコンピュータを管理するシステム担当者などの個人情報保護のあり方を解説する。

図1：個人情報の定義



まずは利用目的を完璧にする

企業が保護法対策として行わなければならない責任と義務は、個人データの流れに沿って、以下①〜④の4つのフェーズに分けて考えられる。

最初は「①個人情報を入手するときの注意」だ。個人情報を入手するには、ウェブや電子メール、葉書によるアンケート、キャンペーン、問い合わせ、各種登録などによって個人から「直接入手する場合」と、ダイレクトメールの発送やデータ入力、システム管理といった業務委託などで個人データを預かるような「間接入手」をする場合がある。

いずれの場合でも、何らかの目的を持って集めるわけである。保護法でも、集める目的を「利用目的」と表現し、利用目的を「できる限り特定する」(第15条1)ことを企業に要請している。ただし、利用目的としてどのような項目を明らかにしなければならないかについて法律では規定されていない。そこで、いつ、誰が、どのように入手して、何のためにどのように取り扱い、管理し、いつまで保有し、問い合わせ窓口はどこかといった事項を利用目的に明記するといい。

保護法は利用目的と異なって取り扱う場合に、その差異の度合いによって2通りの規定をしている。「目的外利用」は従前からトラブルが多く、法で罰せられないように慎重に対策を打つ必要がある。まず1つ目は「若干の変更」についてだ。たとえば、当初は電子メールだけだった入手方法を、ウェブサイトでの入手方法も開発したので追加するといった「変更前と相当の関連性を有すると合理的に認められる範囲内」(保護法第15条2)の変更の場合に、何らかの制限をする規定は保護法にはない。ただし「関連性を有する」と判断するのは個人であり、企業ではない。利用目的を「少しくらいの変更なら」と安易な判断で変えたり、まして「少しずつ何回かに分けて変えていけばいい」などと姑息なことを考えてはいけない。

もう1つは「若干とは言い難い変更」についてだ。変更前の利用目的に対して関連性の薄い内容に変更する場合に、保護法第18条3に基づいて、変更後の利用目的を本人に直接電子メールや郵便、電話、FAXなどで通知するか、ウェブサイトなどに公表しなければならない。アンケートに回答して送ったら、いつの間にか利用目的が変わっていて思いもよらない不要

な商品サンプルが送付されては、本人も「何だこの企業は!」と苦情を持ち込み、結果として企業側は有利にならない。

管理と利用、廃棄を徹底する

保護法対策としては、次に「②保管時の注意」がある。入手した後の個人データは、サーバーや記録媒体に保管したり、リストや管理票に印刷して保管したりすることになる。こうした保管時は「安全管理措置」(第20条)を講じて、個人データが漏えいしたり、無くなったり、内容がおかしくなったりしないように管理しなければならない。

また、コンピュータに保管した個人データを取り扱う「従業員の監督」(第21条)、保管代行倉庫業者やサーバーのハウジング会社などの「委託先の監督」(第22条)についても適切に対処する必要がある。きちんと管理するには、業務上の取り扱い方法についてマニュアルを作成して周知徹底を図り、ルールが守られているかチェックを怠らずに必要な改善を行わなければならない。さらに、取り扱っている個人データに対する本人からの開示や削除、訂正、利用停止の要請を受け付ける問い合わせ窓口を設けて、対応しなければならない。

その次は「③利用(預託・提供を含む)時の注意」だ。企業は適正な利益を得ることによって存続できる。そうした事業を行ううえで、個人情報は適切に取り扱うことによって付加価値を付けて有用なものにできるが、扱い方を誤れば企業にとって損失をもたらすこともある。取り扱う際に、企業内での利用や業務委託などで企業外に個人データの処理などを預託するときに「従業者の監督」(第21条)および「委託先の監督」(第22条)を行う必要がある。なお、ここで言う「利用」とは、自社内のみで取り扱うことを指し、「預託」とは業務委託で社外に個人情報をいったんは渡すものの、委託した業務が終了し次第すみやかに個人情報を返却してもらって回収することを指す。また、「提供」とは対価を得るなどして個人情報を第三者に渡して返却を求めないことを言う。

最後は「④廃棄時の注意」だ。個人データが保管されていたコンピュータや記録媒体、プリントアウトした紙、印刷ミスで使用しなくなったダイレクトメールのラベルなどを廃棄する際は、「安全管理措置」(第20条)に規定されているとおり「必要かつ適切な措置を講じなければならない」。また、ハードディスク上に保管されている個人データのファイルだけを削除する場合や、個人情報データベースなどに入っている特定個人のレコードだけを削除する場合についても、「漏えい、滅失又はき損の防止」(第20条)を図らなければならない。

これらの対策を検討する際は、妥当な処置を講じたと一般的にみなされる施策にしなければならない。もし事故が発生した場合に自分たちはちゃんと対策をとっていたと主張しても、世間のレベルに対してあまりに低い内容の施策であれば、何も対策していなかったのと同様にみなされて裁判で敗訴してしまうおそれがある。

具体的な対策を検討する秘訣

施策の内容を検討する際は、ISOやJISなどの公的な規範に基づいた内容にするとよい(図2、表2参照)。①の入手時の利用目的を提示することや、②の本人関与として開示や訂正、削除、利用停止を受ける問合せ窓口については、JIS Q 15001に基づく施策にする。③④の保護法第20条に適合させるうえでの安全性の確保についてはJIS X 5080に基づく施策にする。

また、保護法が「個人情報取扱事業者」として企業全体で個人情報の保護を行うことを要求していることに応ずるうえで、個人情報保護の施策は企業の事業や業務全体で最適化することが望ましい。これは、企業内のリスクマネジメントに個人情報保護を取り込むことによって実現できる。リスクマネジメントはJIS Q 2001に基づく施策にする。

URL http://law.e-gov.go.jp/htmldata/H15/H15HO057.html

図2:個人情報保護と規範

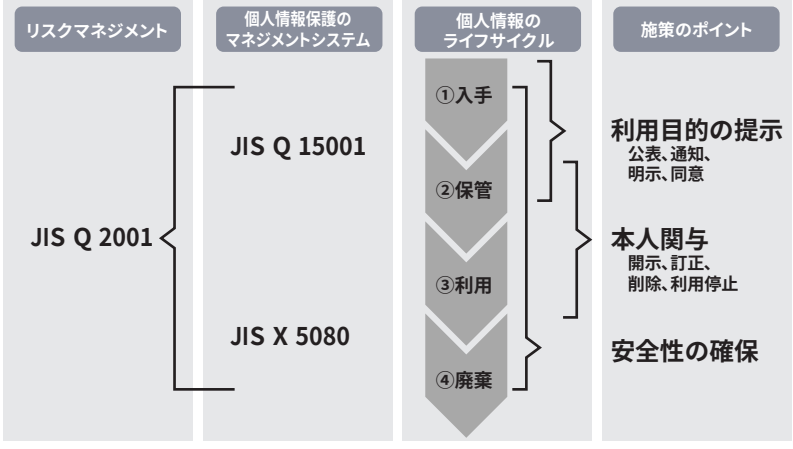


表2:施策を検討する際に参照すべき公的な規範

企業の保護法対策フェーズ	公的規範の項目	内 容
①個人情報入手時の注意 ②保管時の注意	JIS Q 15001:1999 「個人情報保護に関するコンプライアンス・プログラムの要求事項」	個人情報保護に関する第三者認証である「プライバシーマーク制度」の認証基準でもある。
③利用時の注意 ④廃棄時の注意	JIS X 5080:2002 「情報技術ー情報セキュリティマネジメントの実践のための規範」	ISO/IEC 17799:2000(BS7799-1:1999)を翻訳などしたもので、ISMS(情報セキュリティマネジメントシステム)に関する第三者認証である「ISMS適合性評価制度」の認証基準の元にもなっている。
個人情報保護の施策を企業全体に最適化させる	JIS Q 2001:2001 「リスクマネジメント構築のための指針」	あらゆる組織のどのようなリスクにも適用できるリスクマネジメントシステム構築の一般的な原則および要素をまとめた規格。

「うちの会社は何とかなるだろう」の甘さが命取りに

いまから着手するための「保護法」への具体策

これまでは「保護法に基づき企業が実施すべき事柄」を整理した。しかし、保護法にかぎらず、法律は表現があいまいでかつ抽象的であり、企業内においてシステムを構築して運用するわれわれには難解である。そこで、企業として具体的にはどのようなことをどのように対処すればいいのか、何から実施すればいいのかを8項目挙げてみた。こうした対応を行う際に「主体は顧客だ」という認識がもっとも重要である。顧客から見て、個人情報がきちんと管理されているかを認識できることが肝心なのだ。

適切で迅速な対応が評価を生む

1 複数の問い合わせ窓口は絶対にやめる

まず、最初に企業がしなくてはならないことは、「身に覚えのないダイレクトメール」などについて、顧客が自分の個人情報に関して企業に問い合わせてくる窓口を明確にすることだ。保護法では、顧客の苦情処理を適切かつ迅速に行うことが規定されている。

苦情は電話かメールが中心である。電話は営業やコールセンター、総務などどの部署にかかってくるかわからない。メールは、ウェブマスターが対応することが多い。つまり、1人の顧客にいくつもの窓口があるわけだ。そこで、相談窓口を一本化しなければならない。この場合に大切なのは、相談窓口の責任者は経営陣（常任役員）であることが望ましい。決裁権をもつ人にすぐ判断を求めなければならない問い合わせが多いので、いわゆる“たらい回し”にせずにスムーズに対応するためだ。それには、各部署で生じた苦情を、相談窓口へ速やかにかつ正確に伝える仕組みも必要である。

ビジネスマナー教育をなめるな

2 社員の態度次第では苦情が100倍に増える

ある金融機関のテレビコマーシャルは、コールセンターでのオペレーターの対応を放映して企業好感度を上げている。ビジネスマナーは、企業としてのしつけである。しつけは定期的に教育し、守れない社員には上司がその都度注意することが肝心である。しかしながら、この教育は新入社員に対する教育の1回だけしか行っていない企業がほとんどではないだろうか。顧客との電話応対時の挨拶や敬語の使い方はもちろんのこと、メールでのビジネス文書の書き方は、定期的に教育すべきである。特に「お客様相談室」は当然のことで、顧客と接する部署やその社員は1年に1回は定期的に実施すべきでだ。ビジネスマナー教育は、顧客の苦情を100倍に増やしたり、その逆に100分の1に減らしたりすることを心得ることである。

データは一元管理が理想的

3 各部門バラバラの取り扱いでは話にならない

顧客の個人情報を企業が入手するのは、営業部門やマーケティング部門、そして公開ウェブサイトの管理部門が中心となる。各部門によりその活動目的が違うため、個人情報の入手や管理、利用方法がバラバラだ。しかし顧客から見れば、

その企業だけしか見えていない。本来、個人データを一本化するためには、CRMの構築が最適だろうが、時間と費用がかかる。このため、企業の個人情報の取り扱いに関する標準化を図り、各部門に推進してもらうことが肝心である。右の囲みは「製品登録はがき」の例だが、保護法が施行されればこうした個人情報の取り扱いに関する文言の記載は必須となる。例中の1～4の本文は標準化部分であるので、これをひな形にして考えてほしい。これを元にすればフェアやセミナー、ウェブアンケート、案内文などにも利用できる。

「お客様登録はがき」にご記入いただく個人情報の取り扱いについて

本商品に同梱されている「お客様登録はがき」(以下「登録はがき」といいます)に記入いただくお客様の個人情報は、以下のとおりお取り扱いいたします。

1. お客様の個人情報は、弊社内で弊社商品の購買層等を分析する目的、または弊社の商品情報をお客様に提供する(以下「ユーザーサービス」といいます)目的、およびアンケート等を送付する目的のみに使用し、他の目的には一切使用いたしません。
2. 登録はがきを弊社に返送するか否かは、お客様の任意で決定して下さい。但し、登録はがきが返送されなかった場合および必要事項を記入いただかなかった場合は、ユーザーサービスのご提供が困難である事をご了承ください。
3. 弊社は、ユーザーサービスを行うため、個人情報の取り扱いに関する契約を締結した上で、ダイレクトメール代行業者またはFAXサービス代行業者にお客様の個人情報を預託する場合があります。
4. お客様は弊社に対して、いつでも弊社が有しているお客様の個人情報をお客様に開示するよう求めることができます。
5. 前項の事項の開示の結果、当該個人情報に誤りがある場合は、お客様は弊社に対して当該個人情報の訂正または削除を要求することができます。
6. 前2項の開示、訂正または削除を要求される場合は、次項の個人情報に関する相談窓口まで文書かお電話または電子メールでご連絡ください。

弊社の個人情報に関する相談窓口
○○株式会社
xxxx部(個人情報ご相談窓口)
TEL：03－xxxx－xxxx
FAX：03－xxxx－xxxx
電子メール：xxx@impress.co.jp

コンテンツの更新ばかりに集中していない？

4 アクセス管理の徹底が最悪の事態を避ける

ウェブでの個人情報漏洩事件は数か月間もデータが閲覧可能になっていることが多い。こうしたことに関してウェブサイトのシステム管理者は、何をどうしておけばいいかまでは十分な注意を払う余裕もなく、ウェブサイトの開設とコンテンツの作成に気が集中してしまうのだろう。

OSのセキュリティーアップデートをはじめ、ウイルスチェックツールのパターンファイルの更新とリアルタイムチェックの実行や、サーバーのアクセス権限設定の見直し、ウェブコンテンツの改ざん検知ツールの利用、改ざんされた場合に備えて安全なマスターコンテンツをレプリケートするなどの基本的なことを怠ってはいけない。

さらに、公開ウェブサーバーからDMZ上のデータベースサーバーにODBCで接続する際のアカウントやデータベース管理アカウントのパスワードを定期的に変更し、「guest」などのデフォルト設定アカウントを変更、削除したり、データベースサーバーへのアクセスを社内外問わず制限したり、社内ネットワークから不必要にODBC接続していないかチェックしたりすることも、必ず実施しなければならない。

事情が変わったではすまない

5 監査なき情報漏洩の防止は無理

企業の経営戦略や社会情勢の変化はもとより、社内組織や人事の変更でも、社内サーバーやネットワーク環境が日々変わっていく。これらへの対応を即座に行わなければならないシステム管理者は、変更された顧客の個人情報データの社内フローに関して、細かくチェックする時間がなかなか取れないのが現状だろう。そして、結局はシステム上の問題というより、運用上の人的ミスによる個人情報データの漏えいが発生してしまう。最近ではモバイルPCの台頭により、どこからでも簡単に社内ネットワークやサーバーにアクセスできるようになっていることも、管理を複雑にしている原因だ。

そこで、顧客の個人情報の入手方法や個人情報データベースの管理体制、個人情報データベースを活用する部署の体制をはじめとし、それらのシステム全体に関する監査を行うことが大切になる。この作業は、まずは外部監査会社に依頼し、その監査基準や方法を把握したうえで、その後は自社内で実施できるようにすればいいだろう。

疑ってかかるぐらいが良い？

6 業務委託先との契約書を至急見直せ

企業の個人情報に関する事件では、業務委託先による個人情報の流出がもっとも多い。また、そのほとんどが個人情報データベースをコピーされているため、数十万人単位の被害者数となってる。

これでは、企業が社内のネットワークセキュリティーを確保して社員教育を徹底したとしても、その被害額は莫大なものとなってしまう。至急、委託先との契約書を見直してほしい。単なる「委託契約」や「秘密保持契約」だけでは保護法への対処はできない。業務を発注する企業側に、「監査権」または「監督権」を追加することはもちろんのこと、損害賠償についても再度協議することが望ましい。損害賠償額については、通常は契約金を限度としていることが多いが、実際に事件などが起きた場合の損害はそんな金額では追いつかないためだ。

また、顧客の個人情報を大量に取り扱っている、もしくは個人情報が企業経営の根幹である場合は、万が一のために、ネットワークに関する損害保険に加入することも検討の余地がある。

「これぐらい大丈夫だろう」が危険

7 ゴミの山を宝の山にしない秘訣

ここ最近は、クライアントPCの低価格化による買い換えや、ハードディスクの大容量化に伴う各種のバックアップ装置などの利用が多くなってきた。

サーバー機を処分するときは、システム管理者がディスク内のデータをソフトウェア的にもハードウェア的にも完全に消去するなど、万全の対策を施すことが肝心だ。もしディスク障害などでハードディスクやバックアップテープなどに消去ツールが使えない場合は、記録部分を取り出して傷つけたり破壊したりしてから廃棄しなければいけない。そして、クライアントPCの廃棄処分にも細心の注意を払わなければならない。かならず、自社内でデータ消去ツールを適用してから廃棄するか、信頼のおけるシステムインテグレーターや廃棄業者に守秘契約を締結のうえで依頼する。

どうせやるならもっと完璧に！

8 プライバシーマーク制度で上を目指せ

保護法に適合し得る唯一の個人情報保護に関する第三者認証として「プライバシーマーク制度」URL がある。

個人情報の取り扱いに関して多少の差異はあるが、保護法よりも厳しいレベルの個人情報保護を求めている（表）。それだけ、認証を取得した企業は社会的信頼を得ることができるとも言えるだろう。

また、認証を取得した後も2年ごとに更新の審査を受けなければならない。そのため、個人情報の保護について継続的に確実な施策を実施するマネージメントサイクルの適切な区切りにもなるだろう。これから保護法が施行されるまでの約2年の間に、このプライバシーマーク制度の認証を取得することを目的に、社内整備をすることが保護法への対処として一番の早道でもある。

また、ここまで保護法対策のために保護法がもっとも着目しているコンピュータ上の管理について、システムの種類と管理上の役割を踏まえて、誰が何をどのようにすればいいかについて解説してきた。しかし、その内容はまだ一端である。おのおのの企業の事情に合わせた対策を講じるのは非常に手間や時間、費用を要することだろう。

保護法が効力をもつ施行時期は、来年後半からと見られている。その時点になって「対策していない」では企業活動が行えなくなる事態にも発展する。次ページに対策のポイントと関連資料をまとめたので、至急これを参考に着手して、総合的に対策を進めてほしい。

財団法人日本情報処理開発協会（JIPDEC）プライバシーマーク事務局
URL http://privacymark.jp/

個人情報保護法とプライバシーマーク

カテゴリー	法令・規範	個人情報保護法（第15条〜第36条、第56条〜第59条、附則第1条〜第5条）	プライバシーマーク制度（JIS Q 15001:1999）
全般	レベル	「常識の範囲」のレベルを明確化した企業が遵守すべき最低限のルール	「望ましい取り扱い」のレベルを明確化した
	強制力	法律であり、適合することが当然	事業の要に応じて判断して申請する
	目標	悪くないようにする	大丈夫な状態にする
	管理レベル	Plan-Do（マネジメント）	Plan-Do-Check-Action（マネジメントシステム）
	対象領域	原則として社外の個人情報が対象	社外のみならず就業者の個人情報を含む
対象	個人の状態	原則として生存者のみ	生死問わず
	情報形態	原則としてデータのみ	形態問わず
	情報件数	大量	件数問わず
	保有期間	長期	期間問わず
	利用理由	事業の要	理由問わず
	取り扱いレベル	量と期間に応じて取り扱いが変わる	リスクに応じた取り扱いをする
個人の権利の尊重	本人関与	オプトアウトを中心に要求	オプトインとオプトアウトの両方を要請
	事前同意	原則として同意は必要ない	同意が必要
	利用目的の開示	利用目的の通知、公表	利用目的の明示
	利用目的の内容	利用目的に特に規制なし	適切な利用目的が必要で、その範囲は物理・論理・取扱者、情報の機密度、権限など
	対情報主体	不安な相手にはならない	安心を与え、信頼を得る
賞罰	賞	適合して当然なのでインセンティブは無い	社会的信頼を得るというインセンティブあり
	罪決定の手順	報告の徴収→勧告→命令	報告書提出→実態調査→改善勧告・要請
	罪の決定	命令に適切に対処しない	申請に虚偽があった、または実態を改善・解消しない
	罰の内容	6か月以下の懲役または30万円以下の罰金。社名は公表しない	認定の取消し 社名の公表

この項目をすべておさえれば対策は完璧！

ポイント	概　要	参考URL
①個人情報のリストアップ	自社にどのような個人情報があるか、以下のような項目をリストアップする。 ・個人情報の内容と取り扱う業務の概要 ・取扱者（社内外、部門部署、役職）とその管理責任者。社外の場合は預託、提供の内容と守秘契約の有無 ・個人情報の形態（紙、記録媒体、データなど）。紙の場合はデータにする可能性の有無。 ・データの保管場所（全社管理サーバー、部署管理サーバー、端末、記録媒体、個人の机上、引き出し、キャビネット、倉庫など） ・保有期間と廃棄方法	・情報処理振興事業協会セキュリティセンター（IPA ISEC）の「情報セキュリティインシデントに関わる調査」 URL http://www.ipa.go.jp/security/fy13/report/incident_survey/incident_survey.html
②企業の方針とルールを明示	企業として個人情報保護に関して「プライバシーステートメント」と呼ばれる宣言や「プライバシーポリシー」と呼ばれる個人情報保護施策の方針を企業内外に明示する。また、それに従って管理や承認ルート、役割を含む組織の体制、規程類を整備し、これを業務手順書などに落とし込む。	・日本ネットワークセキュリティ協会（JNSA）の「情報セキュリティポリシーサンプル」（0.92a版） URL http://www.jnsa.org/policy/guidance/index.html ・内閣安全保障　危機管理室情報セキュリティ対策推進室の「情報セキュリティポリシーに関するガイドライン」 URL http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html
③ネットワークセキュリティーの確保	ネットワークのセキュリティーは当然行うことだが、以下のポイントを特におさえておきたい。 ・システム設計を記録し、セキュアかどうかを確認 ・論理アクセス権限を設計し、アカウントやデータディレクトリーを管理 ・ファイアーウォールやルーターの設定を確認 ・無線LANやモバイルのセキュリティーを確保 ・可用性（稼働継続性）の確保 ・データ流通経路のセキュリティーを確保	・IPA ISECの「情報セキュリティ対策実践情報　システム管理者向けのページ」 URL http://www.ipa.go.jp/security/awareness/administrator/administrator.html
④物理セキュリティーの確保	個人データを取り扱う執務室に、関係ない人が勝手にアクセスしたり出入りしたりしないように管理する。また、そのコンピュータや個人データを業務で使う必要のない人の利用なども制限する必要がある。在宅勤務や休日に自宅へコンピュータを持ち帰る際の管理も必要になる。	・通商産業省告示第518号「情報システム安全対策基準」 URL http://www.gip.jipdec.or.jp/policy/std-doc/security-std.html ・経済産業省の「情報セキュリティ管理基準」 URL http://www.meti.go.jp/policy/netsecurity/audit.htm
⑤そのほかの安全性の確保	個人データの暗号化や個人データの真正性を確保する認証機能や電子署名の適用など、通信経路や端末、サーバーのハードディスクなどの個人データを漏えい、紛失、破損などから守る施策が必要だ。またアプリケーションの設計については、設計仕様書を作成して管理することによって、ソースコードの改ざんや不正プログラムの埋め込み、バックドアの排除を図る。	・JNSAの「コンテンツセキュリティ・ガイド」 URL http://www.jnsa.org/houkoku2002/JNSA_CONTENTS_SECURITY ・情報システムコントロール協会（ISACA）が出版しているCOBIT URL http://www.isaca.org/cobit.htm ・情報セキュリティポリシー策定ガイド（ISPME） URL http://www.kk-osk.co.jp/spolicy/books/books.asp
⑥取り扱う人の管理	策定した規程類を周知させる教育や訓練を行うことは最低限必要だ。責任と権限、義務の範囲を明示して知らせ、平時の行動や事故時の対応を理解させなければならない。また、重過失や故意、恣意による事故関与については処罰することを、事故などが発生するよりも前に周知させる。さらに同じ担当者が長期間同じ業務を行う場合には他者との癒着などによる不正行為が発生しやすくなるため、これをジョブローテーションや相互牽制で抑止し、予防する。	・ISACAのCISM関連情報 URL http://www.isaca.org/bk_cism.htm ・情報サービス産業協会（JISA）の「個人情報保護ハンドブック」 URL http://www.jisa.or.jp/activity/report/p-booklet2002.html
⑦業務委託の管理	以下の点を明確にした契約書の締結が最低限必要。 ・業務委託の範囲 ・守秘対象の明確化 ・守秘対象の利用制限 ・守秘管理責任者と作業担当者の明確化 ・再委託の制限 ・再委託時の責任の所在 ・複製の制限と複製物の管理 ・視察と改善指示の権限 ・業務委託終了時の処置 ・守秘期間 ・違約時の処置、解決方法	・JISAの「ソフトウェア開発委託モデル契約」 URL http://www.jisa.or.jp/activity/guideline/dev_contract2002.html
⑧データ廃棄の安全性を確保	ハードディスクについては、データ消去ツールを適用してから廃棄する。ディスク障害などで消去できない場合は、ハードディスクの円盤部分を取り出して物的に破壊してから廃棄する。また、フロッピーディスクや磁気ディスクは記録面に傷をつけたり、切断や破壊してから廃棄する。ちなみに再利用する際はあらかじめ初期化して個人データを消去する。書類などの紙類は、シュレッダーで処理したり溶解処理したりする。	・電子情報技術産業協会（JEITA）「パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去について」 URL http://it.jeita.or.jp/perinfo/release/020807.html
⑨監査の徹底	対策を講じたとしても、リスクをゼロにはできない。対策が継続的に適切なものとなるように、擬似アタックを含むリスク分析や情報セキュリティー監査、システム監査を行う必要がある。	・日本情報処理開発協会（JIPDEC）の「リスクマネジメントシステム」 URL http://www.jipdec.jp/security/JRMS.htm ・経済産業省の「情報セキュリティ管理基準」および「情報セキュリティ監査制度」 URL http://www.meti.go.jp/policy/netsecurity/audit.htm ・JNSAの「情報セキュリティ監査制度を利用した、情報セキュリティ管理策定」 URL http://www.jnsa.org/nsf2003spring/pdf/a4.pdf ・経済産業省の「システム監査基準」 URL http://www.jipdec.jp/security/guideline/system-audit.html

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp