HP Technology at Work

# ビジネスの“攻め”に活かす 個人情報保護法対策」

» もとのページに戻る


コンプライアンス第一弾の 個人情報保護法」が全面施行されてまもなく一年。法に後押される形とは言え、情報保護への意識が高まり、企業がさまざまな取り組みに着手したことは、大きな進歩だと言えます。しかし実際には多くの企業が、行うべき対策の第一歩を踏み出したにすぎないのが実情。では企業は今後、どんな視座で、どんな対策を進めていけばいいのでしょうか。単なる法対策ではなく『ビジネス発展の一つのフックにする」ためには？…… この法のエキスパートたちが『これからの対策のカギ」を指南します。??≫?**つづきを読む**

≫?**あなたの会社の 個人情報保護法対策必要度」を今すぐチェック！**

**??Profile**

**鈴木正朝**
新潟大学教授 情報法、法情報学）
≫?情報法研究室 鈴木氏ホームページ）

**佐藤慶浩**
日本HP 個人情報保護対策室 室長

**Contents**

≫?【Chapter 1】?全面施行元年の取り組みから導き出されること
≫?【Chapter 2】?情報をどう管理すべきか ？
≫?【Chapter 3】?現状での問題点と解決法
≫?【Chapter 4】?ITが果たす役割とは？

**Top**?/? 1?/? 2?/? 3?/? 4　　次へ »

**個人情報保護についてさらに詳しくは］**

≫ ?個人情報保護に必要不可欠な情報セキュリティ
≫ ?セキュリティ
≫ ?日本HP社内の 個人情報保護ガイドライン」を無償で提供

**【分アンケート】**

≫?お聞かせください！ あなたの感想。
?抽選で3名様に 『HP iPAQ rx1950 Pocket PC』差し上げます！

»? もとのページに戻る
?

HP Technology at Work?>?ビジネスの“攻め”に活かす 個人情報保護法対策」

» もとのページに戻る

# 【Chapter 1】全面施行元年の取り組みから導き出されること

**顧客満足度向上」の観点から具体策を探れば、正しい答えはおのずと出てくる**

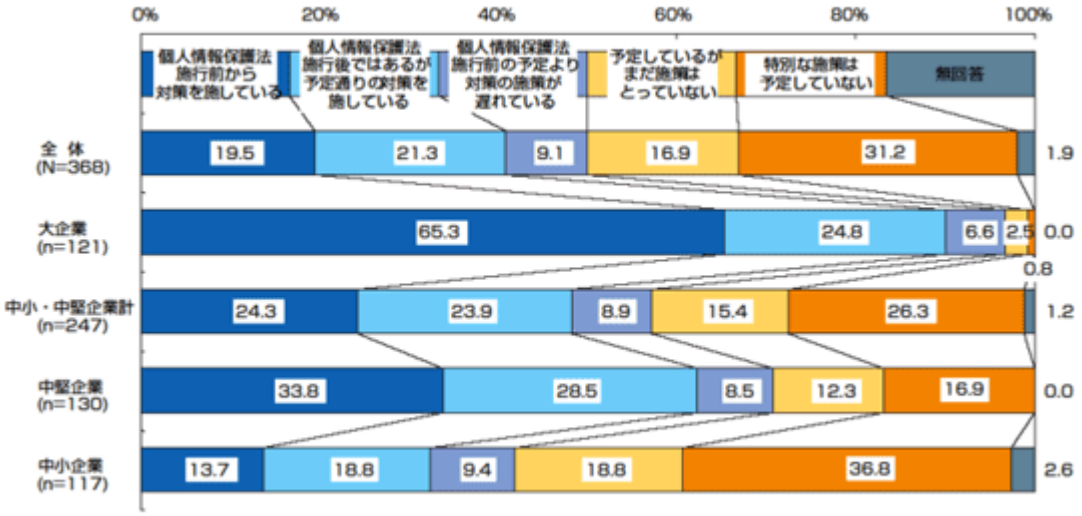
**《Newsletter編集部》個人情報保護法が全面施行されてそろそろ一年を迎えます。企業や関係者の方々からはどんな声が聞こえてきていますか?**

**鈴木**　何をどこまでどの程度やればいいのかわからず途方に暮れるという声はよく聞きますね。企業としてはなるべく自由にビジネスをやりたいわけですから、個人情報保護法に限らず法規制を歓迎する人は少ないのだろうと思います。

しかし、欧米、特にEUから見れば、日本の個人情報の保護に対する法的な取り組みが遅れていたのは確かで、EU域内の企業でも何年も前から現在の日本企業と同様の悩みに直面し、それを克服する努力をしてきたのですから、日本企業だけ「できない」と対策を放棄するわけにもいかないというところだと思います。

**佐藤**　HPでは昨年「個人情報保護法対策の進展調査」を実施したのですが、そこでは中小・中堅企業の深刻な状況が浮かび上がっています。たとえば、大企業でも対策をやったところとやっていないところがあるのですが、「今後対策予定があるか」という問いに対しては、ほぼ100パーセントの企業が「予定がある」と答えています。ところが中小・中堅企業の場合、「対策はしていないし、これからも行なうつもりはない」との答えが1/4近くもあり、かなりの企業が「対策そのものを放棄してしまった」ような節もある。また、個人情報保護法の内容に対する理解度の設問では、半数以上がその内容をほとんど理解していないことが読みとれ、法そのものへの理解も、実際の取り組みも、かなり偏りがあるというのが現時点での実情になっています（下図参照）。

■個人情報保護法対策の進展調査




出典：日本HP「個人情報保護法対策の進展調査」
http://h50146.www5.hp.com/info/newsroom/pr/fy2006/fy06-006.html

**鈴木**　なるほど、確かに個人情報保護法には悪口も多いですよね（笑）。ただ、とにかくはじめの一歩を踏み出し、少なくともこの一年で、個人情報保護に対する意識を高めたという意味では、基本的には評価すべきだとも考えます。全国的に保護水準を底上げし、短期的に見れば政策的に一定の効果をあげたわけですし、この法がなければ、企業の情報セキュリティ対策などへの投資はここまで伸びなかったと思います。

**佐藤**　その通りだと思います。ただし私がこの一年を振り返り感じるのは、実際の対策について、個人情報保護法のごく一部でしかない「漏洩防止」の部分にだけ注目が集まってしまっているのではないかということですね。個人情報保護法では本来その部分にはあまり触れていないのですが、結果としてその方向にのみ力を入れている企業が少なくない。また「利用目的の通知」や「本人関与への取り組み」といった規定について積極的に対策を進めた大企業でも、実際には「漏洩防止」の部分しか行なっていないケースが、実は相当あるのではないかと思います。

**鈴木**　現状ではいろいろと改善の余地もありますよね。中小企業を中心にまだまだ理解が進んでいないところは啓発活動を継続していく必要がありますし、過剰反応に対しても意識を変えるような活動が必要でしょう。また現行法のかかえる構造的な問題もあるわけですが、これについても、個人情報保護指針の作成を促す、さらには個別法の検討も行うなど、どんどん改善を繰り返していくべきだと考えます。

**編集部）現行法の構造的な問題とは？**

**鈴木**　個人情報の保護のために企業がなすべきことは、業種ごとに特徴があり、事業規模等によってもその対策レベルが異なることがあります。たとえば、医療機関であれば「医療カルテ」など医療情報が中心となります。情報の取り扱いも医療現場の安全と業務効率の観点からの検討が必要ですし、また、患者さんの権利利益の保護などの視点も重要です。本人への開示一つとっても「病名告知」という難しい問題があるように、一般企業とは異なる医療法制を踏まえた特別の定めが必要です。

このように情報の取り扱い方は本来、業種や業務の特性に応じ、丁寧に個別的に規律していく必要があるのですが、現在の個人情報保護法では、民間企業を包括的にカバーする「包括規制」が採用されています。ところが現場はさまざまですから、包括規制による一律の規制では当然に混乱が生じ、守るべきルールもあまりにも抽象的で「自社の業務で具体的に何をどこまでやればいいかわからない」という問題が起こっているのだと思います。

やはり、「個人情報」と一口に言っても、その概念は非常に広く、たとえば顧客コードや名刺から医療カルテまでとても幅広い範囲のものを含みます。それらを単一のルールで取り扱うのは、もともと非常に難しいということ。また、事業の種類や規模を問わずにひと括りに「個人情報取扱事業者」として規制している点も問題で、個人事業主もメガバンクも同じルールで規制することにはやはり無理があると思います。これらは企業が対策に苦慮している大きな理由でもあるのですが……。

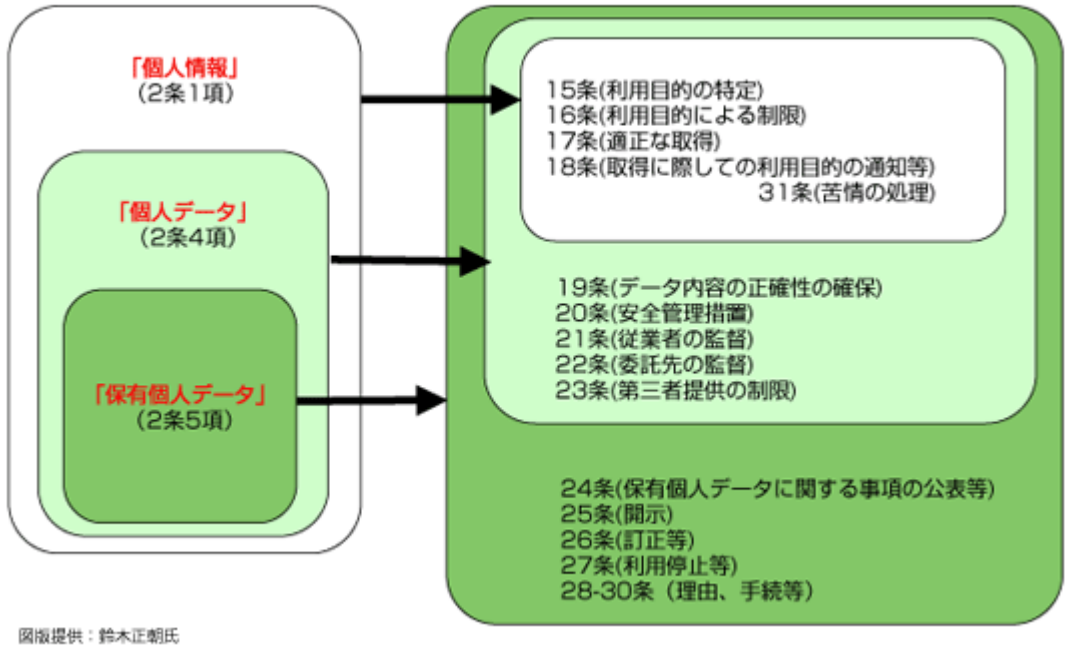
**編集部）「包括法制」でスタートした理由は？**

**鈴木**　本来は「業種などに応じて個別に法律を作った方がよい」ことは、みんなわかっているのです。しかし、個々の規制対象となると、規制を受ける特定業界が抵抗することも多く、解決が難しい新たな論点も出てきますし、法律ができるまでに何年もの時間を要することにもなってしまいます。そうした過去の経験から「包括規制」という政策をとらざるを得ない状況があったわけで、もともと起草担当者も、包括規制が副作用をともなう立法政策であることは、重々承知していたのではないかと思います。

**編集部）そうした課題を解決し、次のステップにいくにはどうしたらいいのでしょうか？**

**鈴木**　まずは、過剰反応などの問題が起こる原因を分析することが必要です。法律が制定されたばかりで十分な周知がなされていないというのが原因なら、過渡的問題ですから、啓発活動でやがて解消されるはずです。しかし、それだけでは解決できない法律自身に根ざす問題が大きな原因なら、それを改善していく必要があります。

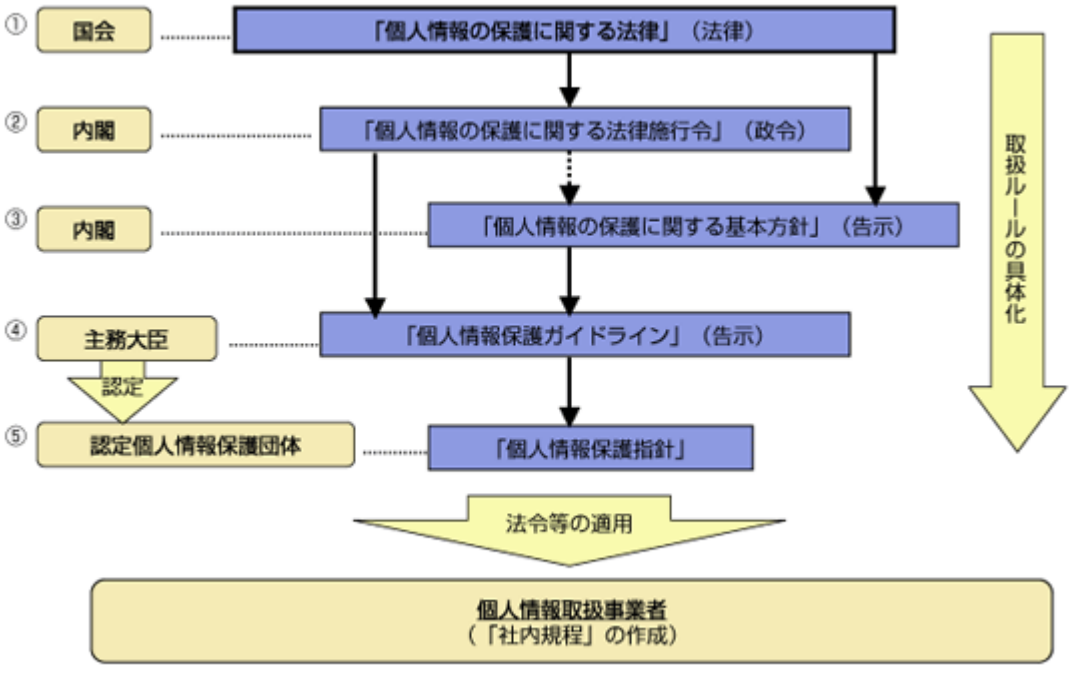
■対象情報と個人情報取扱事業者の義務




図版提供：鈴木正朝氏
岡村久道著「個人情報保護法」133頁の図を一部改変

ただ 包括規制」が問題であることは当然、起草担当者もわきまえているわけですから、その副作用を緩和する仕組みも実は用意されているのです。一つは 個人情報」の取り扱いについて、一度に全ての義務を課すのではなく、保有の状況に応じて、 個人情報」 個人データ」 保有個人データ」の3つに段階に区分して、規制に適応するという方法。つまり、取得した 個人情報」は、名簿化やコンピュータ入力によるデータベース化で 個人データ」となり、自社の権限の及ぶ 個人データ」を6ヶ月以上保有すると 保有個人データ」になる……。そのように、保有の段階に応じた3つの概念を用意することで、絞り込みを行い、段階的に義務が追加されていくという仕組みが採用されており、広範な 個人情報」概念による過剰規制の緩和を行なおうとしています（上図参照）。

■個人情報保護法の適用ルール




図版提供：鈴木正朝氏

もう一つは、 法律」→ 政令」→内閣による 基本方針」 告示）→主務大臣による ガイドライン」 告示）

→認定個人情報保護団体による 個人情報保護指針」と下位のルールにいくにしたがって段階的にルールを詳細化 ･具体化する仕組みも採用しています。最後の 認定個人情報保護団体」は、主に業界団体を認定することを想定したものです。したがって、各業界団体は、自ら監督官庁に認定を願い出て、それぞれの業界の業務に応じた詳細なルールを、官と民とが協議しながら作り込むこともできるのです。ですから、民間の努力次第では、個人情報保護法の運用の枠の中で、 個別法制」的なルールを作りあげることはできるわけですね。法律の中身が抽象的にすぎて対応できないと対策をあきらめるのではなく、この認定個人情報保護団体制度を活用して、自ら 個人情報保護指針」を策定し、ルールの詳細化に努めるべきではないかと思います （上図参照）。?≫? **【Chapter 2】情報をどう管理すべきか ？**

« 戻る　Top?/? 1?/? 2?/? 3?/? 4　次へ »

**個人情報保護についてさらに詳しくは］**

≫ ?個人情報保護に必要不可欠な情報セキュリティ
≫ ?セキュリティ
≫ ?日本HP社内の 個人情報保護ガイドライン」を無償で提供

**【分アンケート】**

≫?お聞かせください！ あなたの感想。
?抽選で3名様に 「HP iPAQ rx1950 Pocket PC」差し上げます！

»? もとのページに戻る

?

# 【Chapter 2】
# 情報をどう管理すべきか？

**ポイントは、「不要な情報は取得しない」情報に必要以上にアクセスさせない」**

**編集部)企業はどのような姿勢で、個人情報保護に臨むべきだと思いますか？**

**佐藤**　本来、個人情報保護は、法律がなかったとしても対策をとってしかるべきテーマなのではないかと思います。意外ですが、アメリカには、日本の包括法制のような個人情報保護法に該当する法律はありません。

ただし、多くの企業で日本の法律以上に厳しい「社内規定」が設けられ、それによって秩序が保たれているという状況があります。ところが日本の場合、「法律にあるのだから、とにかくそれを順守しなければならない」という点にだけ目がいってしまい、「コンプライアンス対策」という側面から個人情報保護法が語られるようになってしまっています。

では、本来どうあるべきか？どんな視点で対策を行うべきか？……そこでカギとなるのが、「顧客満足度向上」という観点から、具体策を導く方策だと思います。つまり「どうすればお客様が喜び、満足していただけるだろうか」「安心していただけるだろうか」「不快感を与えずに済むだろうか」という視点から、「企業としてどのように取り組むか」を考えるべきだということ。そこから法律を捉えれば、おのずと正しい答えが出てくるのではないかという考え方です。

法律の条文の解釈から入ると、「適切な安全管理措置を講ぜよ」という20条の規定のために、たとえば「住所変更の申し出の際の本人確認をどの程度すればよいか」が問題になったりします。しかし、本来は「合法かどうか」という視点より、「お客様に安心していただきつつ利便性を損ねないためには、どの程度の確認作業が必要かどうか」という視点から考えた方がいいわけで、このようなアプローチで対策を行った企業は、おそらく個人情報保護法対策が負担になっておらず、むしろ顧客満足度向上のためのいい機会になっているのではないかと思います。そうではなく、条文を追いかけて対策を行っていると、「苦しい」し、「仕方なくやる」という位置づけのものになってしまうわけですね。

**編集部)具体的な対策を行う上でのポイントを教えてください。**

**佐藤** たとえば情報の漏洩対策を「個人情報に限って行う」ということは、企業では本来はできない話だと思うのですが、現状では情報セキュリティ対策からこの部分だけを「特出し」でやろうとしてとまどっているのが散見されます。しかし本来はやはり「情報セキュリティ対策」全体を見ながら、「自社では何をすべきか」を見直し、不十分な部分の対策をとっていくことが必要なのではないかと思います。

**鈴木** 私も全く同じ考えですね。企業活動の中で「個人情報」はもちろん重要なのですが、重要情報はそれだけではありませんね。そもそも個人情報といった抽象的な捉え方では、それを現場に徹底することには無理があります。例えば、議事録に参加者名が記載されていた場合、それは「個人情報」として別の取り扱い方をするでしょうか。通常は、議事録は議事録としてファイリングされますし、経理で取り扱われる情報も個人名が記載されているからといって、別の取り扱い方になるわけではありません。つまり、企業の業務に即したプロセスの中で情報をハンドリングし、その運用のあり方を、適法であることを前提に、安全にかつ効率的に改善していくことが、対策を行なう上でのポイントになってくると思います。

ただし実際には、ハンドリングしている一つの情報が「個人情報」であると同時に「プライバシーに係る情報」であることも多く、さらに、顧客情報は通常、契約によって取得していることが多いので、契約上の守秘義務の対象であることが大半です。またお客様情報は「営業秘密」として管理していることもありますね。ですから、適法性の確認も、個人情報保護法だけではなく、場合によっては、契約内容に違反していないことや不法行為に該当しないことの確認が必要になりますし、不正競争防止法などの確認が必要になってくるケースもあるのです。

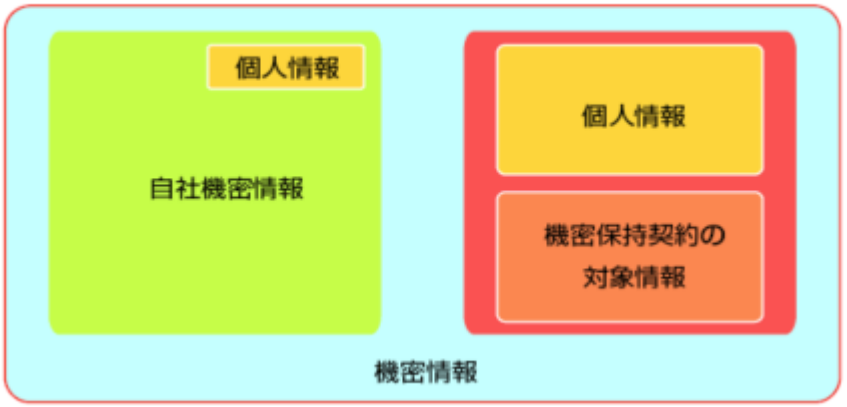
ですから、社内の重要情報を 個人情報」としてのみ取り上げて、 個人情報保護法」だけを見て社内管理をしているとしたら、うまくいかないと思います。個人情報管理も、 情報管理一般」として捉え、関連する法律と契約内容の確認を前提とした社内体制を組み上げていかなければ、内部統制時代だけに、痛い思いをすることにもなりかねません。

**編集部)個人情報を 情報管理一般」と捉えるなら、対策も一般的な情報セキュリティ対策と同じアプローチでいいのですか？**

**佐藤**　企業が守らなければいけない機密情報には 企業自身が自ら作っている機密情報」と個人情報などの 人から預かった機密情報」の2種類があり、それらはそれぞれ、情報として取り扱い方、捉えられ方が異なる性質を持つと考えています。

まず前者の自ら作る機密情報は、ビジネスに応じてどんどん発生するわけですから、 生めよ増やせよ」でたくさん作ることは、企業にとっていいことだと捉えられると思います。それに対して後者の預かり機密情報というのは、自ら作ってはいない性質のものですが、預かり過ぎてしまうと 守るための負担」も増えてしまいます。だからまずは 必要のないものは預からないようにする」ことから始めなければならないのです。 必要のないものをもらってそれで対策をする」ことは、企業にとっては全く不毛なコストになりますから、それが後者の情報の漏洩対策を行ういちばんの出発点になります (下図参照)。

■個人情報と機密情報の関係

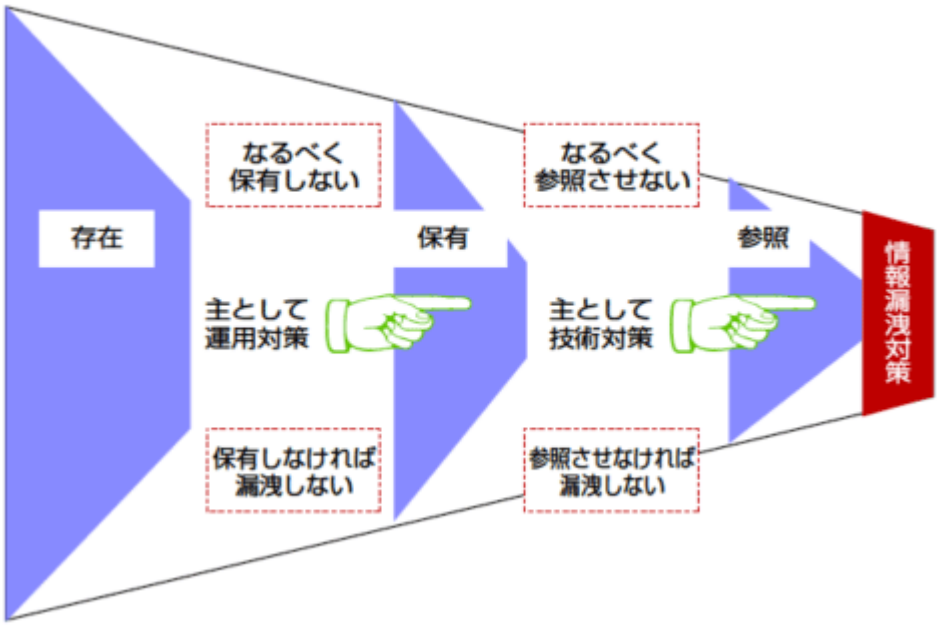



**編集部)情報を預かりすぎないためには、具体的にどんなルールを定めればいいのですか？**

**佐藤**　たとえば ダイレクトメールを送らない」のであれば住所を聞く必要はないわけですが、こうした情報の取捨選択のルールを企業はあらかじめ決めていかなければなりません。そして、そこで ダイレクトメールを送らないのであれば住所を聞かなくてもいい」というルールではなく、もっと明確に、聞くことを禁止する、つまり ダイレクトメールを送らないのであれば住所を聞くことを禁止する」というルールを設定するのです。

社員は、 会社のためによかれ」と思い情報をたくさん持ってくるわけですから、その人たちに対しては、 許可条件」ではなく 禁止条件」を決めてあげる、というのがポイントになります。これがないと、仕事に前向きな社員を抱えていればいるほど、いらない情報が集まってきてしまうことになります。こうした 取得しない」という発想は、これまでの情報セキュリティにはなかった考え方ですが、個人情報保護対策を行う上では非常に重要なカギになってくる部分でもあると思います。

■情報漏洩防止の基本原理




**編集部)取得した個人情報は、どう取り扱えばいいのですか？**

**佐藤**　もらってきた情報に必要以上にアクセスをさせない」というのが一番のポイントです。情報はどんな局面でどのように使われるかわかりませんから、誰がどのような権限で使うことができるのかというのは、明確には決められないし、そこを決めるとビジネスの自由度がなくなり、ビジネスチャンスを失うことにもつながってしまいます。しかし、個人情報の場合は極めて明確で、連絡先情報に該当するような住所とか電話番号などを、企業が使う目的はだいたい限られるわけです。たとえば住所を使うのであれば郵便に使う、電話番号は電話をかけるために使う……という具合に、非常にシンプルです。

ですから、そこでは　電話番号は電話をかける業務の人だけがアクセスできるようにすればいい」という非常にシンプルな情報セキュリティ・ルールを作成すればいいのです。通常、情報セキュリティのルールはこれほどシンプルには作れないものですが、個人情報は項目ごとの用途を絞り込めるのですから、アクセスできる人もそれにあわせて絞っていけばいいわけです。

もちろんそのためのITとして、情報セキュリティの基盤が必要なことは変わりませんが、絞り込めば、漏洩対策をしなければならない範囲もぐっと狭まります。そうしないと、社員全員のPCが顧客情報にアクセスできる会社では、全てのPCのリスクを減らすという話になってしまう。まずは入り口で絞り込み、さらに情報の出口でも絞り込み、そこに集中して対策を行っていく。対策の対象を少なくすれば、そこにより高度な対策を施すことができ、より効果的な手段を選ぶことができるというメリットもあります（上図参照）。≫ **【Chapter 3】現状での問題点と解決法**

« 戻る　Top / 1 / 2 / 3 / 4　次へ »

**個人情報保護についてさらに詳しくは］**

- ≫ 個人情報保護に必要不可欠な情報セキュリティ
- ≫ セキュリティ
- ≫ 日本HP社内の「個人情報保護ガイドライン」を無償で提供

**［1分アンケート］**

≫?お聞かせください！ あなたの感想。
?抽選で3名様に「HP iPAQ rx1950 Pocket PC」差し上げます！

»? もとのページに戻る
?

# 【Chapter 3】
# 現状での問題点と解決法

**発注側は受注側に 何をすべきか」 何をしてはいけないか」を明確に示すべき**

**編集部）利用目的を明示 公表する」不必要な情報は入手しない」、そして情報セキュリティの一定のルールのもと、 情報にアクセスできる権限を絞る」など、いくつかのポイントについて教えていただきましたが、その管理はなかなか大変かもしれません。**

**鈴木**　特に 利用目的の管理」はやっかいですね。個人情報保護法では、直接、書面で情報を取得する時は、利用目的を明示し（18条2項）、それ以外は通知または公表する（18条1項）というように定められています。

ですから、まずはこの顧客との接点を管理することが重要です。もし、情報の取得にあたり、現場に利用目的の起案権限を渡してしまうと、それぞれの現場で、さまざまな利用目的が起案されてしまいますね。その数は、申込用紙やアンケート用紙を作成するとか、Webページ上の申込画面の設計などの度に、どんどん増えていきます。

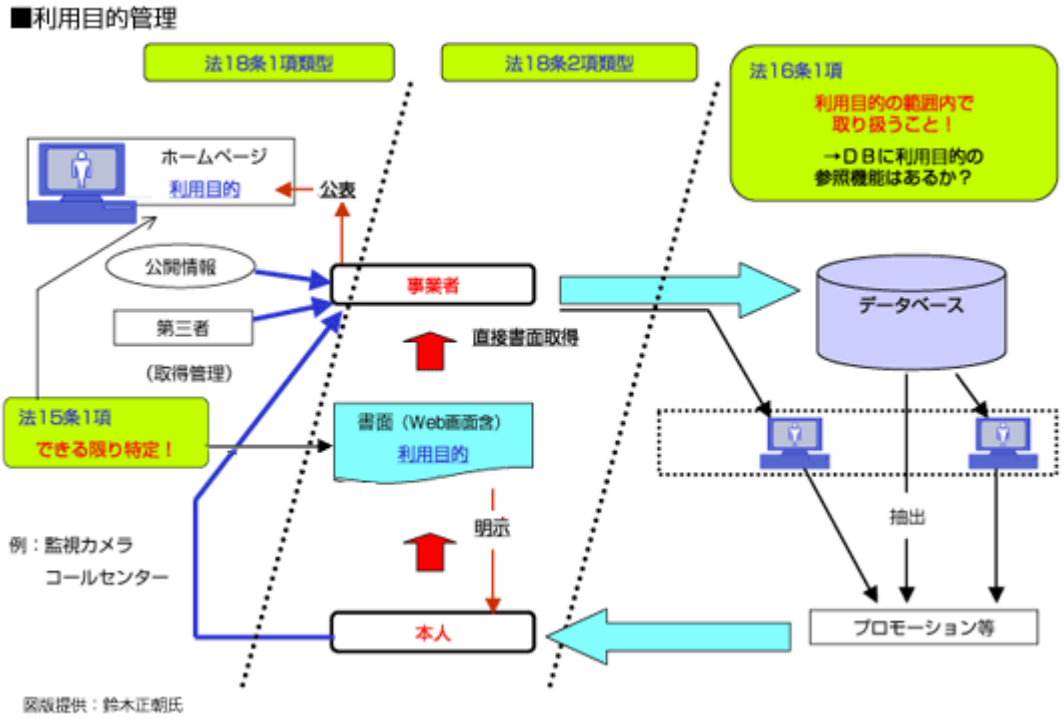
利用目的」の数が増えていくと、数ヶ月、数年と時間が経過するほど、社内全体で管理していくことが困難になっていきます。ところが、個人情報保護法は、個人情報をその利用目的の範囲内で使うことを義務づけていますので（16条1項）、効率的な管理のためには、業務内容を分類して定型化された利用目的を作成し、特定の部門がそれを管理していかなくてはいけません。

さらに、取得した個人情報が、商品・サービスの提供や請求書発行、クレジット決済といった業務に関連している場合、通常は、社内の基幹的な顧客データベースに格納されていくものですが、こうした顧客データベース上の個人情報は多くの場合、商品の発送やサービスの提供だけではなく、プロモーションでのダイレクトメール送付などにも使われます。しかし、実際はプロモーションで利用しようと思っても、個々の顧客ごとに、 利用目的を参照すること」はほとんどできません。ところが、1万人にダイレクトメールを送ろうと思っても、その中に ダイレクトメールには用いない」と利用目的を明示した情報が混入しているかもしれないわけですから、最低限、データベースに利用目的参照機能がなければ、利用できないということになるわけです。ただ、大方の企業は、利用目的を格納するためにデータベースの仕様変更はしていないでしょうから、これだと構造的に16条違反となってしまいます。

また、今後、多くの企業が経営環境の変化により、業務内容が大きく変容する事態に直面すると思われますが、その場合も利用目的のしばりが、企業活動を継続する上でのネックになる可能性があります。というのも、利用目的変更のためには 同意」を対象となる顧客全員から取り付ける必要があるのですが、その手続きにかかるコストは膨大なものになります。また、こうした手続のつど、旧利用目的のままの顧客グループと新利用目的への移行を同意した顧客グループが出てきますから、変更同意をしないお客さまを切り捨てるならともかく 全て抱えてビジネスをするとなると、それに応じた顧客管理をする必要がでてきます。こうした分岐が重なっていくと、顧客グループは利用目的の種類だけ分割されていくことになります。また、顧客がリピーターの場合、一人で多数の利用目的を見ている可能性が高いので、その場合どうするかといった運用ルールも決めて、あらかじめ約款などに反映しておくことも考えておかねばならないでしょう。

このように、利用目的による法的しばり（15条1項）の運用を強めれば、企業の経済活動が停滞してしまうことにもなりかねません。今はまだ、この問題が顕在化していませんが、数年のうちに国内のほとんどの企業が、こうした事態に対処しなければならないという現実に直面することになるのではないでしょうか。

**佐藤**　やはり漏洩ばかりに対処してきたので、アンバランスになってしまった部分がありますよね。今、鈴木先生が言われたデータベース内の個々の個人情報ごとの 利用目的管理」は、漏洩対策をするだけなら、データベースの中身が守られていればいいということになり不要です。しかし利用目的管理をしないままどんどんと情報を入れていくと、どの個人にどんな利用目的を通知したかがわからなくなり、今度は事実上、データベース中の個人情報の利用ができなくなり、不明なデータをすべて廃棄しなければならない事態になるかもしれません（下図参照）。




**編集部）ビジネスの観点では、委託先や協力会社との間での個人情報保護法の扱いをどうするか、という問題も顕在化しています。**

**鈴木**　現実のビジネスの現場では、垂直的分業と水平的分業が交錯し、一社では完結できないさまざまな問題が横たわっています。

垂直的分業での問題は、仕事の受発注で生じる下請関係での安全管理措置の費用負担をどうするかということです。下請事業者も一般に個人情報取扱事業者ですから、個人情報保護法の遵守は当然の義務です。したがって、建前上は委託元から法律に即した安全管理措置を遵守せよと言われても、決して不当な要求ではないわけです。

しかし、実際には新たな費用負担を強いるケースも多く、結果として、下請だけに安全管理措置の負担が課せられてしまいがちです。また、委託元が、委託先に対して何をどのように安全管理していくべきか、その仕様を示していないという「安全管理措置の丸投げ」といった問題もあります。これでは、委託元は半ばマネジメントを放棄して、委託先に安全管理対策の責務を全部投げてしまっているのと同じことになってしまいます。

**佐藤**　本来は、委託元が委託先に、セキュリティの要件について、SLA（Service Level Agreement）を提示し、具体的に「こうしてください」「これはしないでください」と明確な指示をすべきなのです。委託先がそれを守らない結果、漏洩が起これば、委託先の責任にもなると思いますが、そのような明確な指示がない中での漏洩は、やはり委託元の責任ということになると思います。

**編集部）両者が想定しないような事故が起きた場合は？**

**佐藤**　その場合はやはり両者の問題であり、今後、起こらないようにお互いの努力の中で解決していこうということになるでしょうし、結局起こってしまったら、一つ一つ解決していく以外にはないと思います。ただ、世の中で起こるほとんどのことは、実際のところ予見可能なことが多いのです。

たとえば「電車の網棚にパソコンを忘れる」……「人間はうっかりモノを忘れてしまう」ことがあるのですから、それは十分予見可能なことですし、それが想定できれば、起こった時も情報漏洩につながらないよう「外に持ち出すPCはすべて暗号化をする」という方法で、被害を低減することができるわけです。こうした

対策要件を指示する役割を、発注と受注の委託関係で誰が担うべきかといえば、それは本来「委託元」が行うべきであり、もしその企業が予見可能なことに対する指示を怠っていれば、その企業は監督責任を果たしていない、ということになるのです。

**鈴木**　消費者に対しては、消費者から最初に直接個人情報を取得した企業がその責任をとらざるを得ないでしょう。その際、法的責任がいくつか出てくるのですが、まずはお客さまとの契約違反が問われることになりますね。次にそこで生じた損害を委託先に求償できるかどうかが問題になります。

一方、個人情報保護法違反の問題は、主務大臣との関係で論じられますが、委託元自身の安全管理措置義務（20条）、それから委託先の監督責任（22条）が問われます。また同時に委託先自身の安全管理措置義務（20条）も問題になり、事案によっては両方処分ということも可能です。

なお、「委託元はどの程度、委託先を監督していればいいのか」ということがよく問題になりますが、一般論としては、企業の看板・ブランドを信頼した消費者の期待を裏切らないためには、消費者から委託元に期待された安全管理のレベルが、委託先においても維持されるよう、少なくとも委託元と同水準とすべしという考え方はあると思いますね。消費者にとっては、どこに委託しているか知るよしもなく、また、人的リソースが社内か、社外かというのは基本的に関係がないことですから。

したがって委託元はそのために、いろいろ手だてを講じなくてはなりません。委託先の情報セキュリティ投資に応分の費用負担をしてあげること、それから、インハウスで行っている労務管理の手法、たとえば成果主義的な考え方を、委託先にも応用していくなど契約内容に工夫をこらすこと。これは、「バリューベース型アウトソーシング契約」というのですが、委託先の業務の達成レベルに応じて、その報酬額を増減するという管理手法です。そのためには、サービスレベルの事前設定が不可欠で、そこに安全管理の視点からも最低限遵守してもらいたいサービスレベルを明確に示しておく必要があるのですが、その条項がまさにSLAということになってくると思います。

**佐藤**　そうですね。個人情報をお客様が企業に預ける場合、それはその企業のブランドを見て預けているのであって、その企業の委託先が安全であるからという理由ではないのですから、やはり委託元も、委託先も、それぞれの立場でしっかりと役割を果たさないといけないということだと思います。委託元は適切な指示をしない、委託先も明確な指示を受けてもいないのに契約書で安全管理措置義務に同意する……というような状況では、結果的に事故が起こりやすいし、起こった時も損害賠償の責任を「下に下に」押しつけるようなことが起こってしまう。一番上流にいる委託元の責任意識こそが、実は安全管理のカギを握っているということを、委託元はきちんと認識すべきだと思います。

**鈴木**　情報セキュリティ対策というのは、結局「人の問題」にいきつきますので、人事労務管理上の問題も視野に入れて取り組む必要があるでしょう。それから、さきほど垂直的分業と水平的分業について申し上げましたが、こうした分業体制は今日、情報ネットワークに支えられているわけです。特に水平的分業体制によって提供されている商品・サービスは、事業者間の情報システムの連携で支えられているのが一般的です。

しかし、この情報システム間を行き交うデータの全てを企業が正確に把握しているかというとそうではなく、現場の技術者もシステムの安定稼働とデータの正確なやりとりに注力し、それが個人情報保護法の対象情報に該当するかどうかの知識を持ち合わせていないのが実情です。また、文科系主体の管理部門においては、情報システムなどは、いわばブラックボックスですから、問題の所在すら認識していない可能性があるなど、安全管理の前提すら整備されていない場合も多いのではと思います。たとえば、データの提供が第三者提供なのか委託なのかという法的整理ができていない、契約関係のない会社とデータ交換が行われている……など、実際にはこのような問題が、誰も気が付いていない潜在的なところで少なからず発生しているのではないでしょうか。≫**【Chapter 4】ITが果たす役割とは？**

« 戻る　Top 1 2 3 4　次へ »

**個人情報保護についてさらに詳しくは］**

» ?個人情報保護に必要不可欠な情報セキュリティ

» ?セキュリティ

» ?日本HP社内の「個人情報保護ガイドライン」を無償で提供

**【分アンケート】**

»?お聞かせください！あなたの感想。
?抽選で3名様に「HP iPAQ rx1950 Pocket PC」差し上げます！

»? もとのページに戻る
?

# 【Chapter 4】 ITが果たす役割とは？

**サービスの基本仕様に法令順守の機能を盛り込み、お客様を適切な方向へ導く**

**編集部)今後企業は、個人情報保護法をどう捉え、ビジネスにどう活かしていくべきなのでしょうか ？**

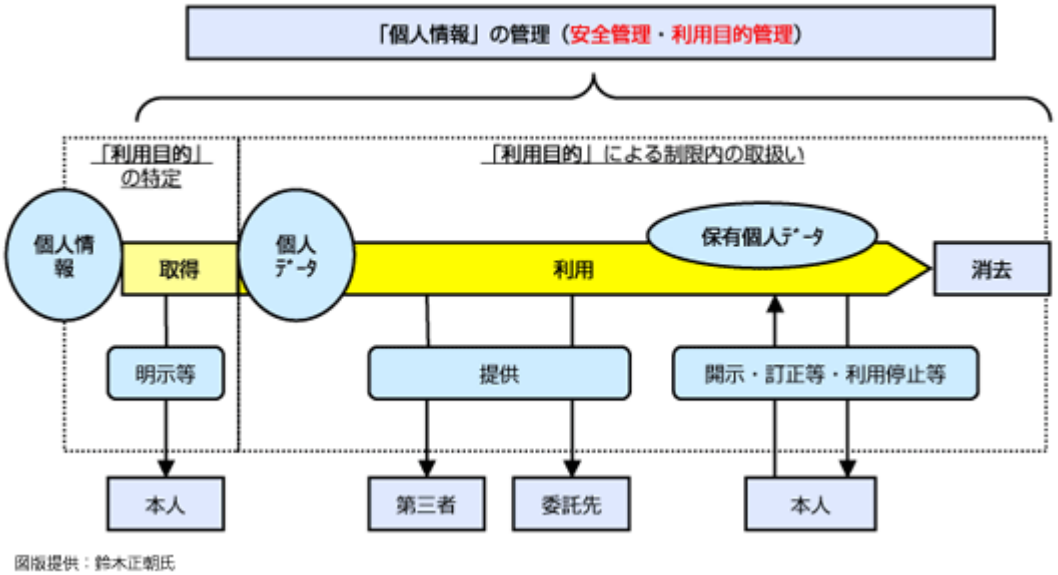
**佐藤**　個人情報保護法を「コンプライアンス」の視点から見ると、対策がつらくなってくるお話をしましたが、実際この法は、それほど無茶なことを強いているわけではなく、企業として守らなければならない 当たり前」のことが書いてあるにすぎないんですね。ですから 企業としてどうすべきか」という視点から出発すれば、法対策は「コスト」ではなく、むしろ「ビジネス最適化」のための施策となるもので、それは企業の情報戦略を見直すいいきっかけになるのではないでしょうか。

たとえば、利用目的を特定する作業は面倒だと思うかもしれませんが、それをせずにセールスプロモーション活動をするということは、取得する個人情報をどう活かせばビジネスチャンスに結びつくかをよく考えずに、プロモーションのコストを使おうとしているということです。利用目的を特定するための文言を考えなければならないことによって、あらかじめ ビジネスプランを明確にすることができるわけです。これはビジネスにとって大きなプラスになるのではないかと思います。

**鈴木**　企業では、従来から 情報」を、人、モノ、金に次ぐ第4の 資産」であると捉え、経営資源の一つとしてその重要性に着目してきたわけですが、さまざまな制約も出てきた今日では、「宝の山」のようでもある一方で、「手間やコストばかりがかかるビジネスの阻害要素」でもあるという見方も出てきています。もちろん個人情報保護法という規制が増えたのは事実なのですが、自社の情報管理体制の改善を進めていけば、ビジネスで今後大きなアドバンテージを得る、格好のきっかけにもなるのではないかと思いますね。

この点は、よく環境規制と環境ビジネスとの関係が引き合いに出されるところです。いずれにせよ規制は規制で逃れようがないのですから、どうせなら前向きに取り組む方が、活路を見出しやすいでしょうし、実際、ビジネスの新しいネタがたくさん出てきているような状況もあります（下図参照）。

■個人情報保護法の全体構造




図版提供：鈴木正朝氏

**編集部)個人情報保護に関して、ITを提供する側のベンダやIT部門の役割は何だと思いますか？**

**佐藤**　これからはITを提供する側も、提供するサービスの基本仕様の中に法令順守の機能を盛り込むことが当たり前になってくるでしょうし、例えば、財務会計ソフトのように、適切に使えば、法律に則ったアウトプットを自然に導いてくれるようなサービスが、個人情報保護についても期待されるのではないかと思います。社会や法規制が要求しているものをシステムで実現できるのであれば、ベンダはそれを取り込んで供給する責任があると思いますし、情報を扱う専門家として、お客様が違法行為に流れないように、適切にアドバイスをするべき立場に今後はなっていくのではないでしょうか。

**編集部)個人情報保護について、HPにどんなことを望まれますか？**

**鈴木**　現代はビジネスがボーダーレスになり、企業の組織そのものも国際化し、日々、情報も国境を超えてやりとりされている状況だと思います。そんな中、主権国家の枠内の法制度ということでやむを得ないことなのですが、個人情報に関しては、米国のプライバシー保護法制、EU各国の個人データ保護法制、そして日本の個人情報保護法制と、それぞれの国に独自の法体系があります。そうすると、必ずいろいろな問題に直面することになると思うんですね。

問題解決のためには、まず「何が問題か」という論点を提示することが必要なのですが、それを明確に示すことができるのが、まさにHPではないかと思います。国際企業として、全社的に共通のプライバシーポリシーを掲げ、本社と各国の法人間で社内データベースを共有し、個人情報も日々行き交う状況にありますし、日米欧の国々にワールドワイドなネットワークを持ち、それぞれのエリアに、情報管理と法制度に関するプロフェッショナルもいらっしゃいます。

米国におけるプライバシー保護の取り組みは有名ですし、そのアドバンテージを活かせば、どのような問題があるかその所在を明確に示すとともに、その解決のためにはどのような方法があるか、いろいろと提言することができるのではないでしょうか。そうした具体的なたたき台が示されれば情報ネットワーク法はもっと実りのあるものになるでしょうし、国際的にビジネスをしている他の企業においても非常に参考になり、助かることと思います。ぜひともHPにはこの分野でもリードしていただきたいと大いに期待しています。

≫?**ご感想をお聞かせください**

« 戻る

Top?/?1?/?2?/?3?/?**4**

**個人情報保護についてさらに詳しくは］**

≫ ?個人情報保護に必要不可欠な情報セキュリティ
≫ ?セキュリティ
≫ ?日本HP社内の「個人情報保護ガイドライン」を無償で提供

**1分アンケート］**

≫?お聞かせください！あなたの感想。
?抽選で3名様に「HP iPAQ rx1950 Pocket PC」差し上げます！

»? もとのページに戻る
?