便利な情報一覧

本冊子の内容に関連する、便利な情報の一覧を以下に記します。
併せてご活用ください。

消費者庁「個人情報の保護」に関するサイト
www.caa.go.jp/seikatsu/kojin/

経済産業省「個人情報保護（ガイドライン、取組実践事例紹介）」
www.meti.go.jp/policy/it_policy/privacy/

厚生労働省「厚生労働分野における個人情報の適切な取扱いのためのガイドライン等」
www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/

一般財団法人日本情報経済社会推進協会「プライバシーマーク制度」
privacymark.jp

一般財団法人日本情報経済社会推進協会「情報セキュリティマネジメントシステム（ISMS）」
www.isms.jipdec.jp/isms.html

独立行政法人情報処理推進機構(IPA)の中小企業向けセキュリティ情報
www.ipa.go.jp/security/manager/

NPO 日本ネットワークセキュリティ協会
「2009年情報セキュリティインシデントに関する調査報告書」
www.jnsa.org/result/incident/2009.html

■情報モラル普及啓発制作物(監修：中小企業庁　発行：(財)ハイパーネットワーク社会研究所)
www.hyper.or.jp/moral/contents

パンフレット『企業に求められる情報モラル』
～人権に配慮した情報の取り扱い～

パンフレット『情報モラル実践事例集』
～企業に求められる人権に配慮した情報の取り扱い～

ビデオ『情報モラルが会社を救う―IT時代の社会的責任』
www.hyper.or.jp/moralvideo/video1/

ビデオ『実践・情報モラルあなたの会社は大丈夫？』
www.hyper.or.jp/moralvideo/video2/

※このほか、セミナー開催などの普及啓発活動を行っています。

経済産業省中小企業庁
www.chusho.meti.go.jp/

経済産業省中小企業庁委託事業

発行　財団法人ハイパーネットワーク社会研究所

〒870-0037大分県大分市東春日町51-6　大分第2ソフィアプラザビル4F
TEL:097-537-8180　FAX:097-537-8820
www.hyper.or.jp/　電子メール：moral@hyper.or.jp

2007年３月発行
2011年５月改訂

PRINTED WITH SOY INK

リサイクル適性Ⓐ
この印刷物は、印刷用の紙へリサイクルできます。

企業に求められる情報モラル実践ガイド

人権に配慮した個人情報の取り扱い方

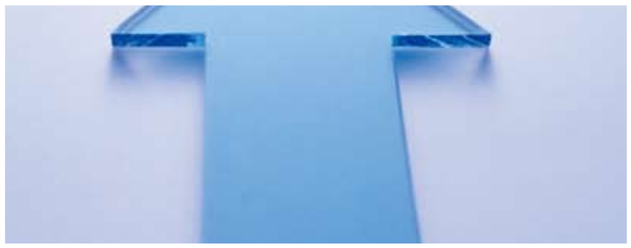
情報技術の普及にともなって、世界中の企業・人々が、より自由に情報を活用し、コミュニケーションすることが可能になりました。一方、個人情報の取り扱いを誤り、大きな事件・事故につながるケースも少なくありません。

この冊子は、人権に配慮した個人情報の取り扱い方のポイントを、日ごろの業務・実際の場面に沿って解説したものです。

企業に求められる情報モラル確立の手引きとして、ぜひご活用下さい。

Contents

個人情報の取り扱いと人権への配慮
個人情報取り扱い方のポイント 業務の場面に沿って
取得▸利用▸委託▸保管▸維持▸廃棄・運搬▸問合せ▸事故



財団法人 ハイパーネットワーク社会研究所

企業に求められる情報モラル

個人情報の取り扱いと人権への配慮

個人情報の不適切な取り扱いがどのような問題を引き起こす恐れがあるのか、企業はどのような姿勢で取り組まねばならないかを考えてみましょう。

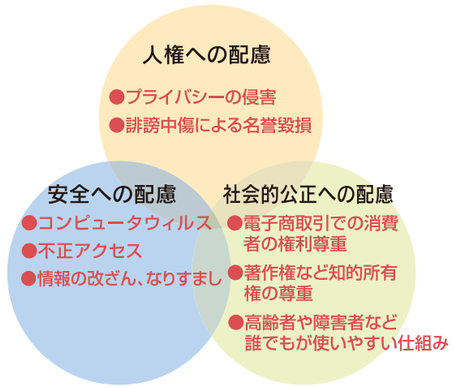
健全な情報社会を築くために必要な情報モラル

情報社会が進むなかで、情報の役割は一段と重要性を増しています。個人情報についても、製品やサービスの利便性を高めるなど、その活用は企業と生活者双方に欠かせないものです。

しかしその一方で、個人情報の漏洩や不適切な利用など、人々の人権や安全を脅かす事件も後を絶ちません。こうしたなかで、有用な情報を生かしながら健全な情報社会を築くためには、情報を取り扱うときに、情報をやり取りする相手の権利や安全を損なわないように配慮をする情報モラルが求められます。

情報社会に求められる情報モラルとしては、「人権を尊重すること、システムや情報の安全を守ること、社会的な公正に配慮すること」があげられます。

情報モラル



情報モラルの構築は企業の社会的責任です

企業は経済活動を通じて収益を上げることが大きな目的です。しかし今日、社会の一員である企業には、経済的利益だけを追求するのではなく、企業活動がもたらす社会的な影響に配慮して、自らの行動を律する社会的責任が求められています。

企業の社会的責任としては、環境問題、人権問題、法令順守などの取り組みが行われていますが、情報を取り扱う上での社会的配慮としての情報モラルの構築も、また企業の重要な社会的責任のひとつなのです。

個人情報の漏洩は人権侵害にもつながります

個人情報はほとんどの企業が扱う情報ですが、その個人情報の漏洩が大きな社会問題となっています。このため、2005年度に個人情報保護法※が施行され、企業にも適正な管理責任が求められるようになりました。個人情報保護法が対象とする個人情報は、氏名、住所、生年月日、ＩＤなど、個人につけられた番号や記号、さらには写真や音声などを含む幅広いものです。

こうした個人情報が漏洩すると、次のような権利侵害や危険の発生する恐れがあります。

- 知られたくない人に個人情報が渡ってしまう
- 他人に知られたくない個人および私生活にかかわる情報が第三者に公開されてしまう
- 架空請求や振り込め詐欺などの犯罪に使われる
- 悪質業者による不快なダイレクトメール送付や電話、メールなどによる執拗な勧誘につながる
- 知らないところで自分の情報が使われているかもしれないという不安が生じる

安全・安心な生活が奪われる深刻な被害も

さらに、病歴や犯罪歴などのデリケートな情報や、クレジット番号などの重要な情報が漏洩すれば、より深刻な人権侵害や経済的被害につながります。ドメスティックバイオレンスやストーカーに苦しむ人には、自分の居場所やメールアドレスが漏れるだけでも安全な生活が奪われることになります。

また、コンピュータ化の進展により、本人の知らない間にあちこちにある個人情報を結びつけて詳細な個人データベースをつくることも可能になっています。しかし、このようなことが勝手に行われては、安心した生活が送れません。

取得・利用・保管・廃棄などの場面にも脅威が潜んでいます

個人情報は漏洩だけが問題ではありません。国民生活センターの個人情報相談窓口には、「不正な手段で個人情報を取得しているのではないか」「本人の同意なく第三者に情報を提供しているのではないか」「利用目的以外に利用しているのではないか」といった様々な苦情や相談が多く寄せられています（図1）。

取得、利用、委託、保管、入力・更新、廃棄・運搬、問い合わせ対応、事故対応など、個人情報を取り扱いずれの場面でも、不適切な取り扱いやミスが発生すれば、それは個人情報の提供者本人の権利や安全を脅かすことになり得るのです。

漏洩事件・事故の原因の多くは企業内にあります

個人情報の取り扱いにかかわる事件や事故はどんな原因で起きているのでしょうか。日本ネットワークセキュリティ協会の調査によれば、情報漏洩の原因で最も多かったのは、「誤操作」で、続いて「管理ミス」、「紛失・置忘れ」、パソコンなどの「盗難」、「不正な持ち出し」の順番でした（図2）。盗難を除けば、原因の多くは企業内にあるのです。

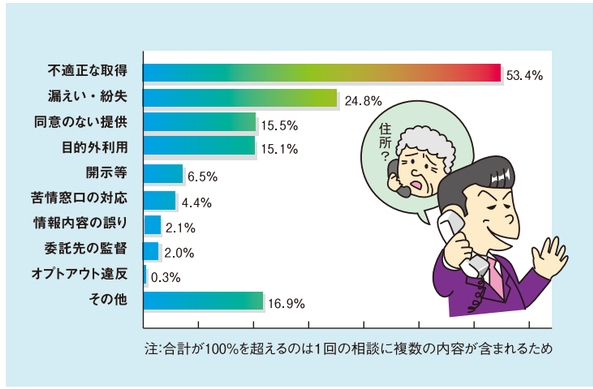
企業が加害者になってしまわないために

個人情報の漏洩は、「企業こそが被害者だ」という気持ちになるかもしれません。しかし、盗難や不正持ち出しなど故意の犯罪でも、企業の管理体制の不備が事件を招くことが多いのは事実です。なによりも、最大の被害者は人権侵害を受ける本人なのです。

個人情報の不適切な取り扱いで事件が起きれば、企業は被害者ではなく、加害者になってしまうという認識が必要です。そうならないためにも、組織として、人権を尊重した個人情報の取り扱いを徹底するとともに、漏洩などによって個人の権利と安全が損なわれないように適切な管理体制を整備することが求められます。

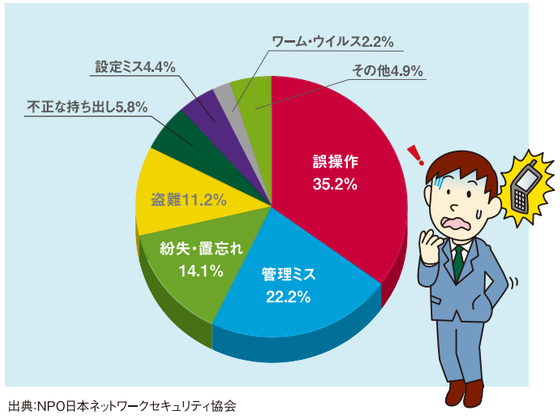
※15ページ参照（個人情報保護法）

図1　個人情報相談窓口の苦情分類別相談件数（2008年度）



出典:国民生活センター

図2　個人情報漏えい原因の件数割合（2008年）



出典:NPO日本ネットワークセキュリティ協会

個人情報取り扱いの対策ポイント

個人情報の取り扱いを８つの場面に分け、日ごろの業務の中でどのような問題に
つながるのか、どのような対策が必要か、そのポイントを示します。

個人情報を取得するとき

企業が個人情報を取得するときに問題となるのは、
主に不正な方法による取得や利用目的を明確に特定しない取得です。

不正な方法による取得

不正な方法での取得とは、個人情報の提供者本人との関係や目的を偽って情報を入手することや、充分な判断力を持たない子供や認知症の高齢者などから、保護者や後見人などの同意・確認を得ずに家族の収入などの個人情報を取得すること、顧客や従業員に監視や個人情報の取得を知らせずにカメラなどの監視装置を使って行動を追跡するなどの場合です。

また、たとえ知らせている場合でも、更衣室のような本来私的な領域にカメラなどによる監視装置を設置するのはプライバシー侵害になります。

利用目的を明確にしない取得

利用目的を明確にしない取得とは、例えばアンケートや会員登録時に「事業活動に用いるため」「提供サービス向上のため」とだけ抽象的に書かれているケースです。これでは、傾向分析だけの利用から、ダイレクトメール送信への利用まで広く考えられ、本人は実際にどう使われるか判断できず、とても安心できません。

個人情報を取得するときは、本人の権利を尊重し、不正な手段をとらないこと、利用目的や利用範囲をできる限りわかりやすく具体的に伝えることが大切です。

対策のポイント

- 本人に対して利用目的をできる限りわかりやすく具体的に示す
- 直接の利用目的に合わない、個人情報を取得しない
- 充分な判断力を有しない子供などからの個人情報の収集は原則的にしない
  どうしても必要な場合は保護者等の確認を得る
- 病歴、信用情報、思想信条、人種、民族などデリケートな情報は、直接業務に必要な場合を除いて取得しない

こんな問題が!

- 相手を騙すなど不正な手段による取得
- 判断力の弱い子供や高齢者などからの取得
- 利用目的を具体的に特定・明示しない取得

取得 利用 委託 保管 維持 廃棄・運搬 問合せ 事故

個人情報を利用するとき

個人情報を利用するときによく問題が起きるのは、
目的外の利用、誤送信・誤操作による情報漏洩、第三者への無断提供などです。

目的外での利用

目的外での利用としてつい犯しがちなのは、取得時には利用目的として告げていないのに、製品やサービスのダイレクトメールを出してしまうケースです。自社にとって必要と思われる利用でも、相手にとっては迷惑なことがあります。相手の意思を尊重することが大切です。また、このようなことは会社の信用失墜にもつながります。

誤送信や誤操作による漏洩

ＦＡＸや電子メール・郵便を送るときに宛先を間違えて他人の情報を送ってしまうケースが少なくありません。個人宛のＦＡＸやメールにはデリケートな情報が含まれていることも多く、とくに注意が必要です。電子メールでは、同時に多数の人に送る同報機能の設定ミスで大量のメールアドレスが漏洩したり、誤って顧客名簿を添付してしまうケースもあります。これらはうっかりミスですが、漏洩による被害の規模は大きくなります。

第三者への無断での提供

ある大学で外国要人の講演会参加者名簿を警備のためとして無断で当局に提供したことがプライバシー侵害として訴えられ、損害賠償の対象となった例があります。適正に取得した個人情報でも、災害や事故などの緊急時を除いて、第三者に無断提供することは許されません。

対策のポイント

- 情報を取得するときに伝えた目的以外に個人情報を使わない
- 個人情報データベースの目的や内容がいつでも分かるように管理する
- 送信時に他の者が確認するなど、組織的なチェック体制をつくる
- 誤送信を防ぐ電子メールの送信管理機能などの備わったシステムの導入など技術的対策を行う
- 第三者提供が必要な場合は利用目的に明示する
- 後から第三者提供が必要になったときは、あらためて本人の同意または確認を得る

こんな問題が!

- 利用目的に明示しないでダイレクトメールに利用
- 電子メールやＦＡＸの誤送信
- 取得した個人情報を第三者に無断で提供

取得 利用 委託 保管 維持 廃棄・運搬 問合せ 事故

個人情報の取り扱い業務を委託するとき

ＩＴ分野では外部事業者への委託が幅広く行われていますが、
委託先事業者による個人情報漏洩事件・事故も少なくありません。

委託の際に起きうる事件・事故

委託の際における事件・事故で多いのは、故意であるかないかにかかわらず、データ入力、システムの開発や運用にともなう情報漏洩です。
例えば、

- 個人情報のデータ処理システムを開発するために委託された顧客情報を、名簿業者や犯罪組織に販売された
- 運搬途上にパソコンが盗まれた
- 自宅に持ち帰ったパソコンがウイルスに感染して個人データが漏洩した

などの事件・事故が多発しています。

委託先に対する管理監督が求められる

委託先事業者の漏洩事件だから委託元は関係ないというわけにはいきません。本人から見れば、個人情報はあくまで委託元の企業に預けたものです。個人情報を預かった企業は、委託先に対しても本人の権利侵害が発生しないよう最善の管理監督を行うことが求められます。

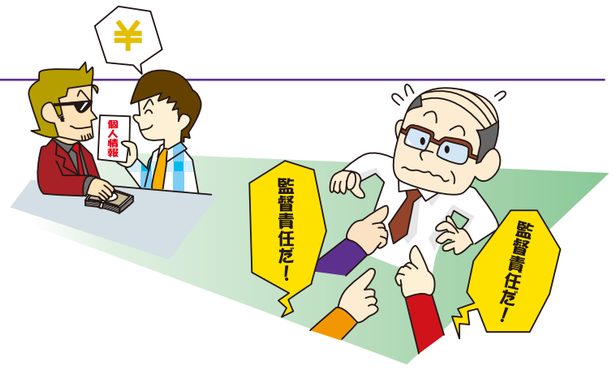
一方、個人情報を扱う業務の委託を受けた企業は、自社の個人情報を扱うときと同様の管理体制が求められます。委託された個人情報の保管、維持、廃棄・運搬、事故対応について本書の注意点を参考にして対策に取り組んでください。

対策のポイント

- 委託先の個人情報保護にかかわる安全管理体制を確認して委託契約を結ぶ
- 契約書等に個人情報の取り扱いを定め、適切に行われているかを定期的に確認する
- 個人情報の社外への持ち出しを禁止する
- システム開発時に個人情報の実データは使わない
- 業務委託の際に渡す情報は、本当に必要なものに限定する
- 委託を受けた企業は、保管、維持、廃棄・運搬、事故対応に対する管理体制を構築する

こんな問題が!

ある公的機関で、システムの開発を委託した民間事業者の再々委託先のアルバイト従業員が住民の個人データ 22 万人分を不正コピーして名簿業者に転売。裁判で当該機関の監督管理責任が問われ、プライバシー侵害などの恐れがあるとして損害賠償が確定した。



個人情報を保管・管理するとき

個人情報が大量に漏洩する事件や事故が発生しやすいのは、
保管・管理の安全対策に問題があるときです。

発生件数の多いパソコンの盗難や紛失

保管・管理の際の事件・事故で、発生件数の多いケースは、個人情報の入ったパソコンや記憶装置の盗難や紛失です。個人情報そのものではなく、パソコンを狙う盗難も少なくありませんが、そのなかに顧客名簿などがあれば個人情報の大規模流失につながります。

また、インターネットに接続されたサーバーに入っている個人情報データベースが、設定のミスで外部からアクセス可能になっていたために、個人情報が漏洩した例もあります。

故意に情報を盗み出すケースも

社員や派遣社員といった内部の人間がアクセス権限を悪用して個人情報を盗み出す事件も発生しています。退職後に、使っていたパスワードが消去されず、不正アクセスされた事件もあります。

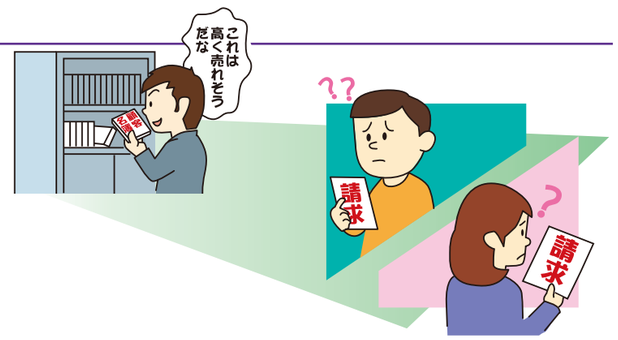
故意による犯罪は、悪意で個人情報を持ち出し、それを元に脅迫したり、架空請求詐欺に使ったり、悪質な業者に売り渡すなど、大きな二次被害につながる可能性が高いのです。故意の犯罪とはいえ、多くの場合、安全管理が不十分な隙をつかれて起きたものです。従業員を守るためにも、出来心で道を踏み外すことが起きないよう、きちんとした安全管理対策をとることが大切です。

対策のポイント

- 社内のどこにどのような個人情報があるかを整理し把握する
- 個人情報の入った媒体や機器は施錠管理する
- 個人情報へのアクセス制限を厳格に実施する
- 利用権限を持つ人でも一度に必要以上のデータにアクセスできないようにする
- 万一の流出に備え、データの暗号化を実施する
- 最新のセキュリティ情報を常にチェックしておく
- アクセスの記録をできる限り取る
- 不必要な個人情報はできるだけ持たない

こんな問題が!

ある信販会社で、内部犯行によって、貸付残高を含む個人情報が約 100 万件漏洩。この流失情報を利用したとみられる架空請求、振り込め詐欺などの事件が各地で 400 件近く発生した。



個人情報を維持管理するとき

個人情報が正しく維持管理されなければ、企業にとっての価値が損なわれるだけでなく、個人の権利利益を損なうことにもなります。

誤った個人情報を登録してしまうと…

個人の信用情報を間違って登録すると、その信用情報に基づいて行われるリース契約やクレジット契約などが結べなくなるなど、個人情報の提供者本人の生活に大きな影響を及ぼす恐れがあります。実際、間違って破産者あるいは延滞者として登録されたために各種の契約ができなくなり、信用毀損を受けたとして損害賠償の対象となった事例があります。また、電話帳への掲載を断ったにもかかわらず手続きミスで掲載してしまい、裁判でプライバシー侵害と判断された事例もあります。

古い個人情報の取り扱いにも注意

使い終わった古い個人情報は企業にとって価値が下がるため管理がおろそかになりがちです。このため情報漏洩の危険も高くなります。個人情報を保管する場合は、必要に応じて保存期間を定め、必要のなくなったものは安全確実に廃棄するルールを確立することが求められます。

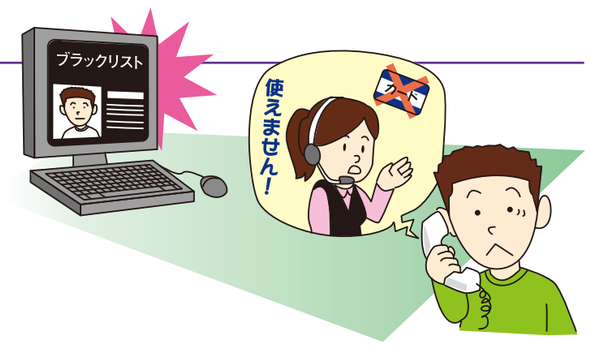
ただし、なんでも廃棄すればいいわけではありません。命にかかわるような製品の欠陥にともなう製品リコールのために購入者情報が必要になる場合もあります。保存期間や廃棄のルールを定める場合は、こうした点への配慮も含めて検討することが大切です。

対策のポイント

- 入力の誤りを防ぐために情報の維持更新を個人に任せず組織的なチェックが可能な仕組みをつくる
- 取得した個人情報が社会的にどのような役割と影響を持つかを見極め、それに応じた保存期間や廃棄についてのルールを整備する
- 当該個人からの訂正の受付と訂正作業を確実に行う仕組みをつくる

こんな問題が!

信用情報会社が名前の読みが同じ他人の破産情報を間違って登録し、会社経営者が自社のリース契約やローン契約を拒否されたケースが訴訟になり、個人の経済的信用および名誉が毀損されたとして、500万円の損害賠償が命じられた。



個人情報の廃棄・運搬・社外作業のとき

保管・管理とともに、個人情報の漏洩や紛失が発生しやすいのが、廃棄・運搬・社外作業のときです。

パソコンの廃棄や持ち運びの場面で

紙や電子記憶媒体、パソコンや記憶装置などを廃棄物として捨てる際、個人情報が含まれていて、流出するケースが多くみられます。個人情報がその中にあることを忘れていたり、ゴミとして扱って、大切な個人情報が入っていることへの配慮を欠いてしまう、などが原因です。

廃棄にあたっては、紙ならシュレッダーか焼却、ハードディスクなら専用ソフトによるデータの消去か物理的な破壊など、媒体に応じた処理のルールを定めることが必要です。

個人情報を運んでいるときには、パソコンや記憶媒体の置き忘れや盗難が情報漏洩につながるケースが多発しています。忘れ物や盗難は個人情報に限らず起きますが、個人情報の場合は人権侵害につながる恐れがあります。「パソコンを網棚に乗せない」「記憶媒体の運搬方法を定める」などのルールにより慎重な管理が求められることを忘れてはなりません。

社外での作業時に

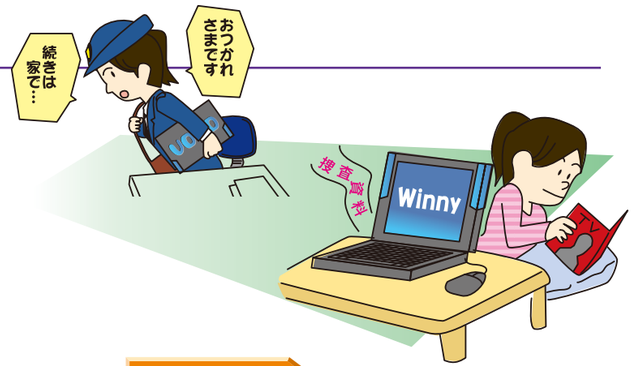
自宅に持ち帰ったパソコンがウィニーなどのファイル交換ソフトを利用したことでウイルスに感染し、そこからパソコンに入っていた個人情報や企業の機密情報がネット上に公開されてしまう事件が頻発しています。ひとたびネット上に公開された情報は瞬時に広がり、回収は不可能です。個人情報は原則的に自宅に持ち帰らないこと、個人情報を扱うパソコンにはファイル交換ソフトを絶対にインストールさせないなどの管理が必要です。

対策のポイント

- 個人情報の所在を管理し媒体廃棄の際にもチェックを行う
- 原則的に個人情報を社外に持ち出さないようにする
- 私物のパソコンで重要な情報を扱わないようにする
- 万一の流失に備えて個人情報ファイルは暗号化する
- 個々人が勝手にソフトをインストールしない
- 個人情報を含む記憶媒体の廃棄は媒体に応じたルールを整備する

こんな問題が!

警察官が私物のパソコンで未成年者の道路交通法違反事件の詳細な資料を作成し、パソコンを家に持ち帰って使用中、ファイル交換ソフトを通じてウイルスに感染し、報道においては匿名とされる未成年者の氏名を含む詳細な捜査資料がネット上の不特定多数に閲覧可能な形で流失した。



問い合わせに対応するとき

個人情報にかかわる本人の権利を尊重するためには、
本人への情報開示などの説明責任を果たせるようにしておくことが必要です。

説明責任としての情報開示

個人情報にかかわる本人の権利を尊重するためには、企業が保有している個人情報について、個人情報の提供者本人への情報開示を含めた説明責任を果たせるようにしておくことが必要です。「個人情報は間違いなく登録し、漏洩や紛失がないようしっかり管理しています」とどんなにいっても、企業が自分に関するどのような情報を保有し、どのような目的で使われ、間違った内容で登録されていないか、などの事柄が実際に確認できなければ、安心して預けておくことはできません。

問い合わせ窓口の設置と適切な対応

個人情報保護法では、本人又は代理人の求めに応じて、①利用目的の通知、②保有本人データの開示、③間違ったデータの訂正、④取得、利用目的、第三者提供について違反があった場合の利用停止、などの義務があるとしています。これを実現するためには、問い合わせ対応の窓口を設置し、それを周知しておくとともに、開示手続きの手間や費用が本人に過度な負担とならないような配慮も求められます。

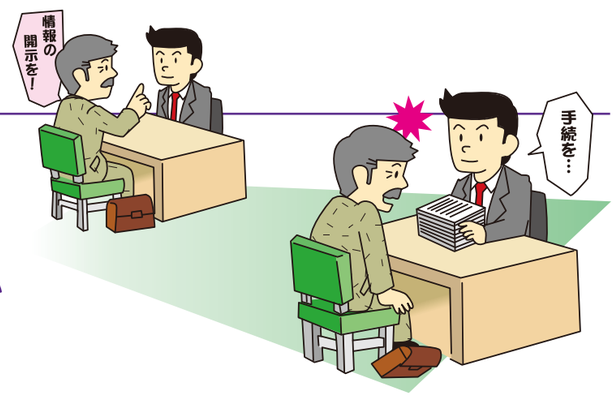
一方、開示の手続きを通じて、他人の情報を不正に入手するなど、新たな人権侵害が発生する恐れもあります。状況や情報の内容に応じて、適切な本人確認の対応も必要です。

対策のポイント

- 問い合わせ窓口を設置して存在を周知する
- 開示要求に応えられるよう個人情報を全社的に整理して管理する
- 過度な負担にならない範囲で本人確認を行う
- 個人情報保護法の理念を正しく理解し、情報へのアクセスを過度に抑制しない
- 適正に取得した個人情報についても、本人の求めがある場合には、ダイレクトメールの送付などの利用停止に自主的に応ずるようにする
- 本人の権利、利益を尊重し、誠実な対応を心がける

こんな問題が！

- どこに問い合わせをすればいいか分からない
- 開示、訂正、停止等の手続きが必要以上に煩雑、または費用がかかる
- 個人情報保護法の範囲でしか対応してくれず、困っている問題に対して誠意ある対応が得られない



取得 利用 委託 保管 維持 廃棄・運搬 **問合せ** 事故

事件・事故に対応するとき

どんなに対策をしても個人情報が漏洩してしまうことがあります。
万一の事件・事故に備えたリスクマネジメント（危機管理体制の構築）も欠かせません。

事件発生時には、被害者に配慮した対応を

どんなに対策をしても個人情報が漏洩してしまうことはあります。不正アクセスなどの犯罪による個人情報流失の場合、企業は自らも被害者といえます。このため、つい被害者意識ばかりが前に出てしまうことがあります。

しかし、個人情報漏洩の最大の被害者は本人です。漏洩した情報がデリケートな内容であれば深刻なプライバシー侵害につながります。他の情報と一緒に電話番号が漏れれば振り込め詐欺に使われる恐れがあります。

事件が発生したときは、個人情報の回収を行い被害の拡大防止に努めるなど、被害者に配慮した対応が求められます。また、再発防止のための調査と対応策の構築が必要になります。

企業の誠実な対応が求められる

被害者である本人の人権を尊重するということは、単にお詫びをしたり、金券を配ればいいということではありません。ＮＲＩセキュアテクノロジーズ社の調査によると、個人情報が漏れたときに個人が企業に求める誠実な対応としては、「わかった時点で隠さずに通知すること」（78％）、「漏洩後に発生する可能性のある事態への対応策を示すこと」（60％）の順で回答があり、お詫びとして「金券を配る」は36％と下位です。事件により被害者が受ける影響を考慮した上での説明責任を果たすことが求められているといえます。

対策のポイント

- 漏洩、毀損などが発生した場合はその内容を本人が分かるように速やかに伝える
- 二次被害や類似事件を防止するため、可能な限り事実関係、原因、対策を公表する
- 担当者がその場しのぎの広報対応や発表をしないで、組織的な対応ルールをつくり徹底する
- 個人情報の回収など被害の拡大防止に努める
- 再発防止のための調査を行い、対応策を構築する

個人情報保護法とは

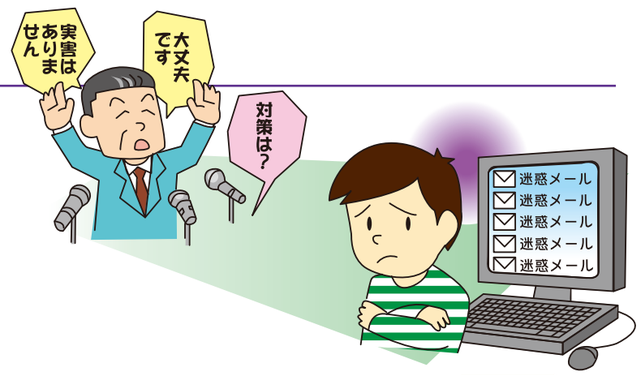
個人情報保護法は、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的に策定されたものです。

事業者が個人情報を取り扱う上で守るべき義務を規定しており、違反した場合の罰則も定められています。

2005年４月から全面施行となっています。

こんな問題が！

ある公的機関で、意見募集のお礼のメールを他の応募者のメールアドレスと名前が分かる形で誤送信。担当者が「実害の報告はない」とマスコミに語ったが、実際には迷惑メールが届くようになった。



取得 利用 委託 保管 維持 廃棄・運搬 問合せ **事故**