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－

はじめに

企業にとって、いまやIT（情報技術）の活用は、必要不可欠なものとなっています。その一方、プライバシー侵害や名誉毀損、コンピュータウイルスの感染や不正アクセスによる情報漏洩など、インターネットの利用にともなう人権侵害の危険性が増大し、個人や社会の安全を脅かす問題も広がってきました。

社会の一員である企業にとって、お客様や社員をはじめとする人々の人権を守ることは、重要な責務であることはいうまでもありません。企業が、ITを活用しつつ、そうした社会的責任を果たすためには、組織として「情報モラル」を確立することが求められているのです。

経営者の皆さんは、組織として人権を守り、情報モラルを確立することが重要な経営課題だということを、しっかり理解してください。

また、情報を扱う部門の管理者や現場の担当者の皆さんは、人権を守り、情報モラルを尊重することが大事な仕事のひとつだということを十分理解したうえで、日々の業務にたずさわってください。

目　次

この冊子のご利用方法

この冊子は、皆さんがインターネットなどITを利用するときに配慮すべき人権をはじめとした情報モラルにかかわる問題について理解を深め、組織としての情報モラルを構築していただく手引きとしてつくられたものです。

前半の「総論編」では、企業が情報を扱う際に心がけるべき、人権を中心とした情報モラルの説明と、組織の情報モラル構築方法の全体像を示しています。

後半の「個別テーマ編」では「個人情報保護」や「情報セキュリティ」、「消費者保護」など、個別の課題ごとに、現状と実際の取組方法を説明しています。

できれば通読をおすすめしますが、必要なテーマだけ読んでも理解できる構成になっていますので、関心のあるテーマからお読みいただくこともできます。社内研修のテキストなどとしてご活用いただければ幸いです。

企業に求められる情報モラル

企業にとって、組織の情報モラルの構築は、重要な社会的責任のひとつです。
企業に求められる情報モラルとは何でしょう。
なぜ組織の情報モラルが必要なのでしょうか。

求められる情報モラルとは

インターネットをはじめとするIT（情報技術）は、企業活動に欠かせないものとなっており、ITを活用できるかどうかは、企業の発展を大きく左右するといっても過言ではありません。

しかし、社会の一員としての企業にとって、ITの活用で本当に成果をあげるためには、操作方法を習得するだけでは不十分です。ITを利用して扱う情報が、顧客、取引先、株主、従業員など一人ひとりの権利や安全を損なうことのないように配慮する、組織としての情報モラルの構築が欠かせません。

情報モラルとは、企業が情報を取り扱う際に配慮が求められる考え方と行動です。具体的には、「人権を尊重すること」、「安全を脅かさないこと」、「社会的な公正を守ること」の3つの視点に立った実践が求められます。

この後、なぜ情報モラルが必要なのかを、経営面と情報社会の課題への具体的な取組策の2つの観点から、さらに詳しく説明しましょう。

企業に求められる情報モラル

企業の社会的責任

まず、経営の観点から、なぜ企業に情報モラルが求められるのかを考えましょう。

企業は経済活動を通じて利益をあげることで存続していきます。同時に、企業の経済活動は、顧客、取引先、株主、従業員、地域社会などに支えられて成り立っていることも事実です。

したがって、企業には経済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るのです。

企業の社会的責任として、環境・消費者・地域社会などへの配慮が求められているのと同様、情報社会に生きる今日の企業にとっては、情報を取り扱う際に人権や安全、社会的公正に配慮することは、重要かつ当然求められる社会的責任です。

企業が扱う情報は、人々のプライバシーや名誉などの人権、社会の安全や安心と結びついています。企業には、情報を通じて人々の人権や社会の安全を預かっているという大きな責任があるのです。

こうした責任を軽視し、情報漏洩によるプライバシー侵害などを起こした企業は、信用を失墜し、売上を大幅に減らし、対処を間違えば存続の危機に直面しかねません。残念ながら、そうした事例は後を絶ちません。

組織における情報モラルの役割

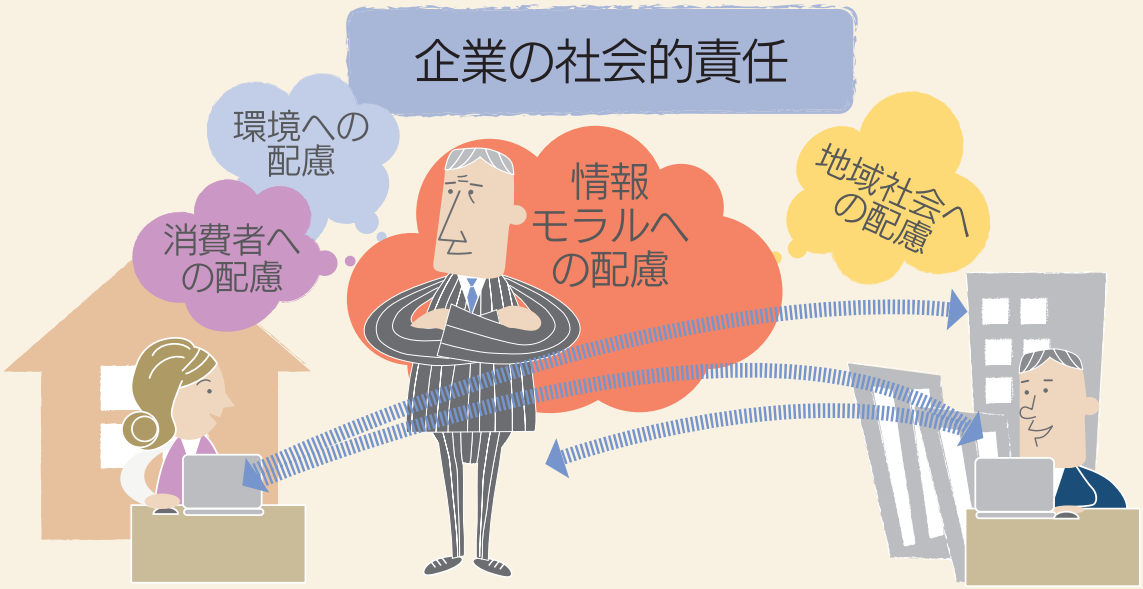
つぎに、情報社会が抱える課題に対する具体的な取組策として、なぜ組織の情報モラル構築が必要か、情報モラルがどのような役割を果たすのかを考えましょう。

例えば、情報社会が抱える重要な課題のひとつである情報セキュリティ対策としては、技術的な対策や、法律や規則の制定など制度的な対策があります。

しかし、技術を導入しても、それだけで問題を防ぐことはできません。システムを適切に運用できるかどうかは、組織のモラルによるところが大きいからです。

同様に、法律や規則を制定しても、実際に守られるかどうかは組織と人のモラルにかかっています。

さらに、技術的な対策や法律・規則は一律に適用されがちです。策定に時間を要し、後手にまわりがちでもあります。すべての問題に、いつでもきめ細かく対応できる保証はありません。問題が発生したときに判断を下すのは常に人間であって、その人間の判断を支える大切な役割を果たすのが、情報モラルなのです。



情報モラルの3つの視点

企業が情報を取り扱う際に必要とされる情報モラルには、人権、安全、社会的公正の3つの視点からの配慮と実践が求められます。

人権への配慮

情報にかかわる人権への配慮とは、表現の自由、個人の名誉や信用、プライバシーなどの人格権を尊重することです。

具体的には、企業が顧客や従業員の個人情報を扱う際には、プライバシー侵害を引き起こさないよう、情報の収集、利用、保管にあたって、本人の意思を尊重し、適切な管理を行う必要があります。

また、企業のホームページや社内ネットワークにおいては、他者のプライバシーを侵したり、名誉や信用を傷つけたり、差別や偏見を助長しない配慮が求められます。

安全への配慮

情報にかかわる安全への配慮とは、情報漏洩、コンピュータウイルス、不正アクセス、情報の改ざん、なりすまし、誤操作、システム障害、データの間違いなどに対する情報セキュリティ対策を徹底することです。

具体的には、セキュリティ意識の啓発やセキュリティシステムの活用など、セキュリティリスクに対する組織的予防策と、事故が起きてしまった場合の被害拡大防止、業務復旧、再発防止、損害補償、信頼回復などの事後対応策の実施が求められます。

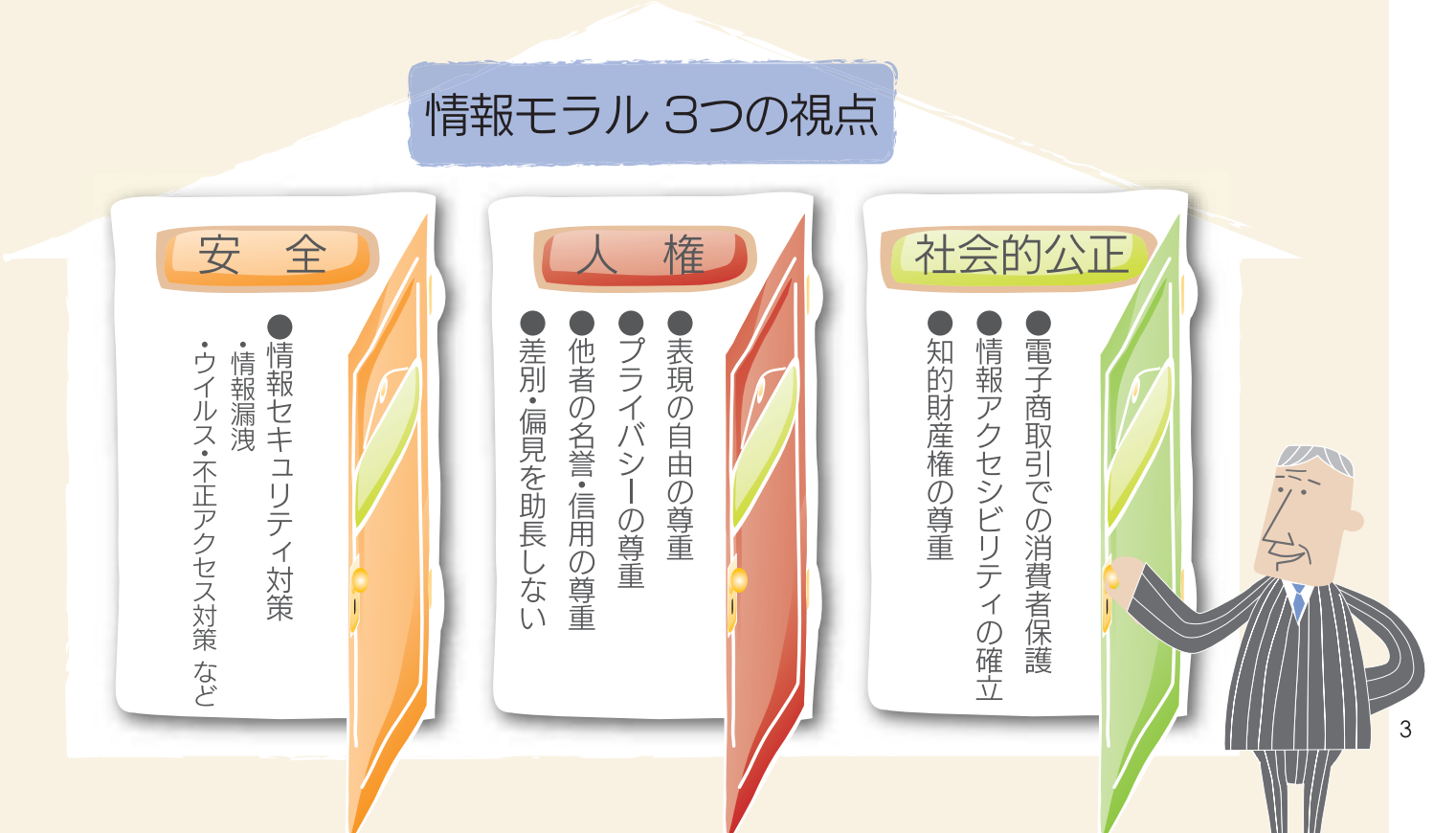
社会的公正への配慮

社会的公正への配慮とは、消費者・取引先との取引や、著作物などの情報の利用において、適法・適正で、他者の権利・利益を尊重した情報の提供や利用に取組むことです。

具体的には、電子商取引では、誇大広告や不正取引をしない、必要な情報を漏れなく開示し、分かりやすく説明するなど、消費者の権利の尊重が求められます。

情報アクセシビリティの確立では、高齢者や障害者を含むすべての人の知る権利を尊重し、必要な情報に、誰もが使いやすい形でアクセスできるようにすることが求められます。

知的財産権保護では、著作権、工業所有権、営業秘密などにかかわる情報を扱う際に、無断での複写や不正な利用をしないよう、他人の権利を尊重した公正な利用が求められます。



情報にかかわる人権課題

企業が扱う情報は人権とどのような結びつきがあるのでしょう。
人権を尊重して情報を取扱うためには、どのような取組が
求められるのでしょうか。

情報は人権とつながっている

企業にとって、情報は、ヒト、モノ、カネと並ぶ重要な経営資源です。同時に、企業の扱う情報は、人々の人権と深いつながりがあります。

企業が預かっている顧客や取引先、株主、従業員などの個人情報を漏洩すれば、個人のプライバシーが脅かされます。

電子商取引サイトで、リスク情報の提供を怠たり、誤った情報や虚偽の情報を提供すれば、消費者の権利が侵され、金銭的な損害にもつながります。

企業が事業活動のために情報の管理と活用を行うことは当然のことですが、企業の情報は、その背後にある人々の人権と深く結びついていることを忘れてはならないのです。

増えつづける人権侵犯事件

インターネットの普及にともない、インターネット上のプライバシー侵害や名誉毀損などの人権侵犯事件が増大しています。

インターネット利用に関連する人権侵犯事件は、2008年には前年比23.2%増と、大幅に増えました。

企業の個人情報の不適切な取扱いが、プライバシー侵害や信用毀損などの深刻な人権被害を招いた例は少なくありません。

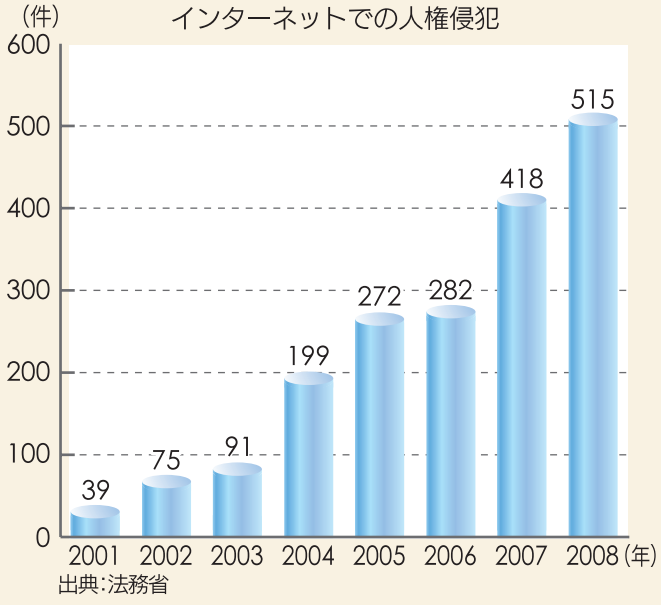
あるエステサロンでは、ウェブサイトの管理ミスで顧客情報が流出し、住所、氏名、電話番号に加えて、身体サイズなどきわめてセンシティブな情報[1]まで漏洩させてしまいました。

被害者は、他人に知られたくない情報を一方的に流出されたことによる多大な精神的苦痛を受けたばかりでなく、ダイレクトメールが送られ、嫌がらせ電話がかかり、望まない訪問販売を受けるなど、二次被害も広範に発生しました。

個人情報の誤りによって信用が毀損され、深刻な経済損失を引き起こした例もあります。

工場を開設したばかりの中小企業の経営者が、信用情報に間違って破産者として登録された事件では、工場稼動に必要な機械・備品のリースや借入金の契約を結べなくなりました。経営者の信用が損なわれたことで、始めたばかりの工場経営が重大な被害を受けたのです。

両方の事件ともに、裁判で、権利侵害が認定され、会社側に被害者への損害賠償が命じられました。



出典:法務省

1「機微な情報」ともいい、一般的には思想・信条、身体・病歴、犯罪歴、出生関連など、高い秘匿性を求められる情報をさします。

経営にも甚大な影響

個人情報の漏洩など人権侵害につながる事件を起せば、自らの企業経営に甚大な影響が及びます。

例えば、460万人分の顧客情報を漏洩したネット接続事業者は、全会員590万人への一律500円の金券の送付を含め、事後対策費が約40億円に達したといわれます。

また、約51万人分の顧客情報を漏洩したテレビ通販事業者は、3ヵ月間営業を自粛し、154億円の減収となりました。

金銭的な損失だけではありません。企業にとってもっとも深刻なのは、社会、顧客、株主、従業員などのステークホルダーから信頼を失うことです。

企業が永年かけて築いてきた信頼は、失うときは一瞬ですが、一度失った信頼を取り戻すのは容易ではありません。

情報の背後にいる人に配慮を

インターネットなどITを活用するなかで、なぜ人権侵害などの問題が起きるのでしょうか。

そのひとつの要因は、情報の背後にある人や社会への配慮が十分ではないことです。

コンピュータのネットワークであるインターネットも、実際に繋がっている先は、人であり、社会です。インターネットでは、人の顔が見えづらいため、そのことをつい忘れがちになり、人権を尊重する意識が薄れてしまうことがあります。

インターネットで、人権侵害を引き起こさないためには、ネットワークの向こうには常に人がいるということを忘れず、人を尊重し、社会とつながっているという意識を持ち続けることが必要です。

新しいメディアの特性を理解

もうひとつの要因は、インターネットなどITによる新しいメディアの社会的な特性の理解が十分でないことです。

インターネットなどのITは、これまでの紙媒体など既存媒体と比べ、大量の情報を簡単に複写し、素早く広域に伝達することが可能です。しかしそれは、大量の個人情報が流出し、ネットワーク上に拡散されやすい、ということでもあります。

また、インターネットは、誰でもが直接世界に向けて情報発信のできる、これまでにないメディアです。しかしその特性をわきまえず、プライバシー侵害や名誉毀損、差別の助長など、人権を侵害する情報を発信すれば、被害者への影響はより大きなものになります。

インターネットなど新しいメディアでの人権侵害を防ぎ、広げないようにするためには、情報がどの範囲にどのように伝わるか、社会にどのような影響を及ぼすか、といった新しいメディアの特性を十分理解して利用することが必要です。

組織の情報モラル構築の基本

組織としての情報モラルを構築するために望まれる
基本的な取組みとはどのようなものでしょう。

情報モラルに関する組織のポリシーを策定

組織の情報モラル構築のために望ましい取組のひとつとして、情報モラルに関する組織のポリシー策定をお勧めします。

具体的には、いまあるプライバシーポリシーや情報セキュリティポリシーに加えて、個別の課題ごとに策定するのでも、企業全体の倫理綱領などに情報モラルに関する内容を盛り込むのでも、それぞれの企業に適したやり方で策定してください。

ポリシーは、「基本方針」、「行動基準」、「運用ルール」の３つの要素で構成するのが望まれます。

「基本方針」は、経営者が自社の基本的な考え方と姿勢を示すものです。「行動基準」は、基本方針を実現するためにとるべき行動や対策の指針を記述します。「運用ルール」は、行動基準を日常業務に落とし込み、実施マニュアルとなるものです。

情報の棚卸しとリスクの把握

次に、自社が扱う情報や、それらの処理の流れを、実務に即して棚卸しすることが必要になります。実際には企業の情報の重要度や処理の仕方はそれぞれの企業によって異なるからです。他社の対策を真似するだけでは、自社で本当に必要なところへの対策がおろそかになり、反面、必要性の薄いところの対策が過剰になるなど、効果的な対策がとれなくなります。

具体的には、自社の扱っている情報を洗い出し、その情報の流れと処理の仕方を書き出します。そして、それに対して、人権、安全、社会的公正の視点から、どのようなリスクと脅威を抱えているかを検討・評価し、リスクと脅威に応じて、リスクの回避策、軽減策などの対策を立てます。

社内の情報モラル啓発

組織の情報モラル確立は、基本方針を策定し、運用ルールを整備しても、それだけではうまくいきません。基本方針やルールを守ろうとする社員一人ひとりが情報モラルを持たなければ、せっかくの情報モラルに関する組織のポリシーは絵に描いた餅になるからです。

日々変化する現場では、技術的対策や運用ルールでは想定されていなかった問題に遭遇することも少なくありません。その場合には、自分だけの判断で大丈夫かどうかも含めて、組織の一員としての社員の対応力が問われます。

そこで、各自の職務の役割と責任に応じた内容で、社員研修や啓発活動を継続的に行い、一人ひとりの情報モラルを組織的に維持向上させていくことが求められます。

適切な技術の選択と運用

情報漏洩やウイルスなどに対する情報セキュリティ対策には、適切なセキュリティ技術の活用も欠かせません。組織の情報モラルの構築は、心構えだけではなく、技術の活用も必要です。

ただし、セキュリティ技術は、強度、使い勝手、費用に応じて様々なシステムがあります。自社の抱えるリスクと脅威に見合った適切なシステムを導入するには、担当者任せにせず、経営者が責任をもってリスク管理の方針を明確にする必要があります。

また、セキュリティ技術はシステムを導入するだけでは十分な効果を発揮しません。むしろ導入後の運用の仕方が大事なことを忘れてはなりません。

最新の事件、事故情報を収集

情報社会は、きわめて変化の速い社会です。ウイルスやネットでの不正行為など、インターネットをめぐるリスクや脅威も、日々新たなものが登場してきます。プライバシー権や著作権などにかかわる社会の意識も急速に変化していきます。

こうした変化に対応するには、新たなリスクをはじめとした最新の動向を的確に把握し、これらの新たなリスクが、自社の扱う情報や情報の扱い方にどのような問題を生じさせる可能性があるのかを検討し、情報を扱う現場に常に注意を喚起することが必要です。

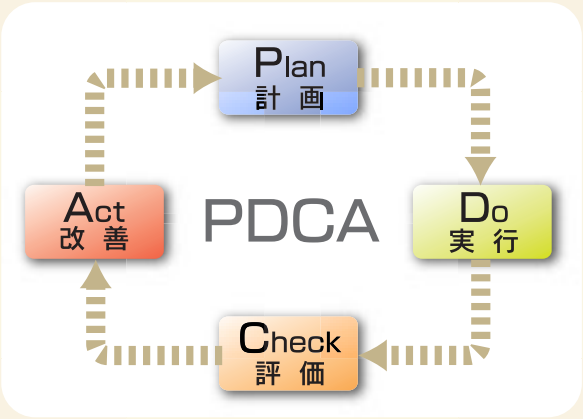
対策の評価・見直しの仕組

組織の情報モラル構築は、一度計画を立て、対策を決めれば、それで終わりとはなりません。対策の見直しが必要なのです。

例えば、計画が不十分で、期待した成果があがらないこともあります。リスク環境の変化により、対策が現実にそぐわなくなることもあります。取組の実態を定期的に点検・評価し、会社経営と同じで、必要に応じて、対策を見直し、追加・修正する仕組が欠かせません。

計画、実行、評価、改善（PDCA）[2]のマネジメント・サイクルが組織の情報モラルを確かなものに育てます。

PDCAサイクル



2 Plan,Do,Check,Actの略

問題発生時の体制づくり

どんなに予防策をとっていても、問題が発生することはあります。いったん問題が発生したときに、被害の拡大を防ぎ、人権と安全を尊重し、説明責任を果たす形で解決に取組むことは、重要な経営責任です。

問題が発生したときには、経営者が現場任せにせず、全社的な権限をもって情報を素早く収集し、企業としての責任をもって問題解決にあたれる組織体制を確立する必要があります。重要な事件や事故については、トップが率先して取組み、問題の解決と事後対応、そして社会への説明責任を果たすことが求められます。

情報モラル構築の効果的な進め方

情報モラル構築の取組を進める上での課題は何でしょう。
組織の情報モラル構築をどうしたら効果的に進められるのでしょうか。

情報モラル構築の課題

多くの企業において、情報モラルの構築や情報セキュリティ対策が必要であるとの認識は高まってきました。

しかし、必要とは分かっていても、「どこからはじめればいいか分からない」、「業績に直結しないので意欲が湧かない」、取組をはじめても、「担当者任せになり、担当者の独り相撲になっている」、「大きな手間やコストをかけづらい」、「どこまでやればいいか分からない」など、様々な悩みを抱えている企業が少なくありません。

こうした課題を抱える企業が効果的に組織の情報モラル構築を進めるにはどうしたらよいのか、考えてみましょう。

トップが経営課題として取組む

「業績に直結しないので意欲が湧かない」のは、企業のトップが情報モラルを建前としか考えず、本音では目先の業績に目が奪われているときによくみられます。

たしかに情報モラルは、目先の収益に直結するものではありません。しかし、事業活動は顧客など社会の信頼があってはじめて成り立つものです。信頼を失えば、企業の存続すら危うくします。

社会の信頼を得るための情報モラル構築は、長い目で見た事業継続と成長のために、より上位に置くべき経営課題なのです。

経営課題としての位置づけを明確にできるのはトップだけです。現場は常にトップの姿勢を見ています。組織の情報モラル構築はトップが経営課題として取組めるかどうかにかかっています。

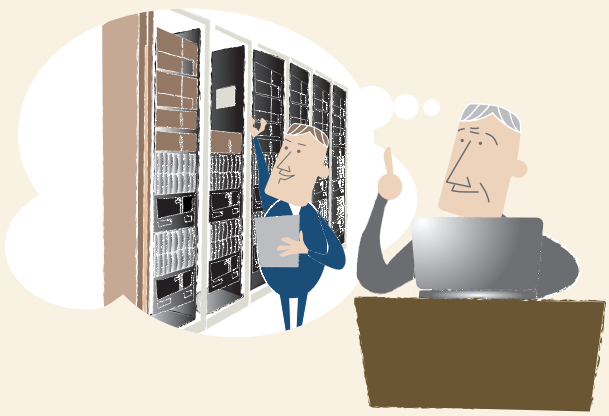
できるところからはじめる

「何からはじめればいいか分からない」、「どこまでやればいいか分からない」、「手間やコストをかけづらい」という悩みをよく聞きます。

なにより、「できることからはじめる」ことが大切です。お金をかけずに始められる方法もたくさんあります。

机の上の整理整頓という、当たり前のことから始めた企業では、整理整頓が情報管理にも仕事のしやすさにも役立つと実感することで、取組の効用が現場に認識されたといいます。

できることからはじめて、それぞれの企業の事業や業務スタイルに合わせた段階的なステップアップを図ることが、無理のない進め方といえます。



日常業務に結びつける

不用意なデータ廃棄により情報漏洩事件を引き起こした企業の社員が、「社内教育は何回も受けたが、まさか自分のこととは思っていなかった」と述懐しています。

情報モラル構築の取組が「担当者の独り相撲に終わっている」、「組織全体に浸透しない」ことの原因としては、社員一人ひとりが情報モラルを自分の仕事にかかわる問題として捉えていないことがあげられます。

一般的な注意事項を知識として教えるだけではなく、それぞれの職場で実際に行っている業務に結びつけて学習し、対策を立てることが必要です。

また、現場の業務実態を無視したルールを作ると、逸脱行為を招きやすくなります。現場の参加を得て、現場が納得するルールづくりの推進が大切です。

組織としての仕組みづくり

「情報モラル構築の取組をはじめたけどうまくいかない」という企業では、担当者任せ、個人のモラル任せ、対策の形だけ整えた形式主義に陥っているケースがよくあります。

組織の情報モラル構築にとって、社員一人ひとりのモラル向上は重要です。責任の明確化も必要です。しかし、個人任せにして、個人の責任ばかりを追及すると、組織としての責任の所在をあいまいにし、再発防止につながりません。

責任の明確化は、責任の押し付けではなく、組織としての問題解決のためのものです。そのためには、問題を隠さない、風通しのよい組織にすることが重要です。

人権や安全にかかわる問題では、個人では判断に迷うこともよくあります。こうした問題に対処するには、社員が気軽に相談や問い合わせのできる仕組みを用意することが必要です。

性悪説より「性弱説」の姿勢で

個人情報の漏洩事件が起きると、「いままでは性善説でやってきたが、これからは性悪説で厳しく取り締まる」と表明する経営者が少なくありません。

しかし、性悪説に基づいて取り締まりの対象にするといわれた従業員は、モチベーションを保てるでしょうか。むしろ、「性弱説」に立ってみることを薦めます。

人は完全ではありません。間違いを犯しがちなものです。ふと心の弱さや、心の隙が生じることもあるでしょう。良心に従おうとしても、組織のこれまでのやり方に流されてしまうこともあります。

従業員を被害者や加害者にしてしまわないために、組織として支える姿勢が、職場がギスギスすることを防ぎ、現場の協力を得ることにもつながります。

この章からは、情報モラルにかかわる7つのテーマを個別にとりあげ、
それぞれの問題の現状と、企業に求められる取組のあり方を紹介します。

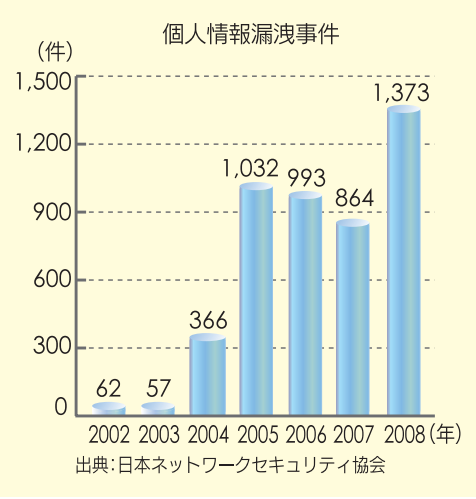
個人情報保護

個人情報の不適切な取り扱いが人権侵害を招きます。
企業に求められる個人情報保護の取組とはどういったものでしょうか。

止まらない個人情報の漏洩

企業による個人情報漏洩事件が後を絶ちません。日本ネットワークセキュリティ協会の調査では、2008年に報道された個人情報漏洩事件は1373件に達しました。毎日4件弱の発生となります。

2009年にも、証券会社の元社員が電話番号、年収区分などの入った顧客情報148万人分を持ち出し、一部を名簿業者に売却した事件が発覚しました。この情報を元にしたとみられる悪質業者からの望まざる勧誘などによる二次被害も発生しています。



出典:日本ネットワークセキュリティ協会

電話番号が知られるだけでも

氏名と電話番号は電話帳にも掲載されています。その程度の個人情報が漏れただけで、なぜプライバシー侵害と大騒ぎするのかという声を聞くことがあります。

その程度なら気にならないという人もたしかにいます。しかし、家族がストーカーによる嫌がらせ電話に苦しめられている家庭もあります。そうした家庭が、電話帳への掲載は希望しないと申し出たにも関わらず、電話会社のミスで掲載されてしまった事件では、裁判でプライバシー侵害と認定され、企業に損害賠償が命じられました。

ストーカーやドメスティックバイオレンスの被害者は、名前と住所や電話番号が流出するだけでも、日々怯えながらの生活を強いられます。企業が預かる個人情報には、そうした事情を抱えた人の場合もあることを忘れてはなりません。

プライバシー観の変化

個人情報にかかわるプライバシー観も変化しています。

従来、プライバシー権とは、主として社会に公表していない私生活や私事を他人に知られない権利とされていました。

しかし、ITの普及により、一度提供された個人情報が、当初の目的にとどまらず、別の用途に転用したり、他のデータと照合して利用することが容易になりました。

本人の同意を得ないで、個人情報を当初の目的以外に使うことはプライバシー権の侵害となります。データの照合や統合による人物像(プロファイル)を一方的につくって利用することも、プライバシー権侵害につながる恐れがあります。

それを防ぐためには、個人情報を使う際には、本人の意思を確認する必要があります。こうした自己情報の管理(コントロール)権も、プライバシー権の重要な一部なのです。

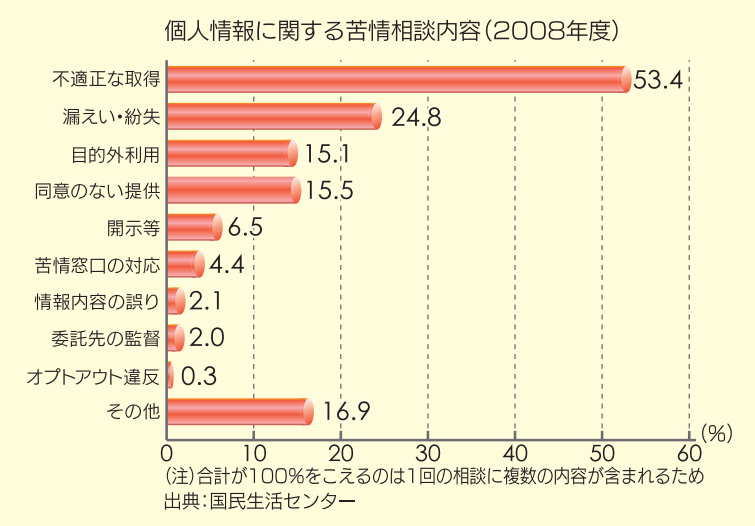
問題は漏洩だけではない

個人情報保護は情報漏洩ばかりに目が向きがちですが、問題はそれだけではありません。

国民生活センターによると、全国の相談窓口に寄せられた苦情・相談の中で最も多かったのは、本人に無断で情報を取得するなどの「不適正な取得」で、53.4%と全体の半数以上を占めました(2008年度)。

2番目は「情報の漏洩・紛失」でしたが、「本人に同意の無い第三者提供」や「目的外の利用」についての苦情も少なくありませんでした。これをみても人々の懸念は情報漏洩だけではないことがわかります。

本人の権利を尊重し、不安を解消するためには、漏洩対策はもちろん、個人情報の取得や利用の方法、苦情等への対応のいずれにも、本人の意思を十分尊重することが求められます。

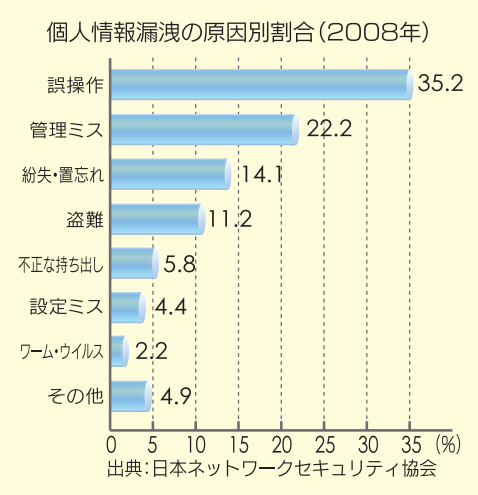


なぜ問われる企業の管理責任

本来、個人情報を盗み、悪用する人物こそが責められるべきなのに、なぜ企業の管理責任がこれほど問われるのでしょうか。

ひとつは、情報漏洩事件の多くが、組織内部の管理上の不備が原因で発生しているからです。日本ネットワークセキュリティ協会の調査では、個人情報漏洩事件の原因の第1位は、電子メールやFAXの送り間違いなどの「誤操作」によるものでした。以下、「管理ミス」など内部管理上の原因が上位を占め、「盗難」は第4位、「不正持ち出し」は第5位でした。

もうひとつは、個人情報は適正な管理を前提として、本人から託された“預かりもの”だからです。人権にかかわる重要な情報を預かっているのです。そこには企業として大きな管理責任が存在するのです。



個人情報にかかわる法律

2005年に「個人情報の保護に関する法律」(略称:「個人情報保護法」)が本格施行されました。

この法律は、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制定されたもので、5000件以上の個人情報を取り扱う事業者には、利用目的の特定や安全管理など、個人情報を適正に管理するための義務を課しています。

なお、個人情報保護法に関して各業種で講ずべき施策については、各業種所管の省庁ごとにガイドラインが公表されていますので、参考にして下さい。

また、民法では、個人情報の不適切な取り扱いにより個人のプライバシー権を侵害すれば、不法行為として損害賠償責任等が問われます。

ただし、民法では、取り扱っている個人情報の件数は関係ありません。個人情報保護法による管理義務が課せられない事業者にも、個人情報の適正な管理が求められるのです。

個人情報保護

個人情報管理の基本

人権に配慮した個人情報管理のためには、取得、利用、委託、保管・維持、社外作業・運搬・廃棄、本人対応といった個人情報を扱う流れに沿い、個人情報保護法の定めに従って、以下の事項を守ることが基本となります。

取得

個人情報を取得するときには
①利用目的をできる限り特定する
②利用目的を本人に通知・公表する
③偽りその他不正な手段で取得をしない
④業務に関係ない情報は取得しない

利用

個人情報の利用にあたっては
①本人の同意なく取得時に伝えた目的以外に使用しない
②本人の同意なく第三者に提供しない
③誤送信・誤操作による漏洩・毀損を防ぐ安全対策をする

業務の外部委託

個人情報の処理業務を外部委託(アウトソーシング)するときは
①委託先の安全管理体制を確認したうえで契約を結ぶ
②委託先の安全管理に対する管理監督を行う

保管・維持

個人情報を保管・維持(メンテナンス)するときには
①情報漏洩・滅失・毀損を防ぐための安全対策を整備する
②個人情報の入力・更新の際は、正確かつ最新の内容を確保する

社外作業・運搬・廃棄

個人情報を社外に持ち出したり、廃棄するときには
①原則的に個人情報は社外に持ち出さないようにする
②持ち出す場合も、私物のパソコンには個人情報を入れない
③万一の流失に備えてデータを暗号化する
④個人情報および記憶媒体の廃棄の仕方にルールを設けて管理する

本人への対応

本人からの情報開示や訂正の請求、苦情などへの対応に際しては
①窓口を設置し、その存在を周知する
②正確に答えられるよう、個人情報の所在情報を全社的に整理・管理する
③過度な負担にならない範囲で、問い合わせ者の本人確認を行う
④本人の求めに応じて開示、訂正、利用停止を行い、応じられない場合は、その理由を説明する
⑤本人の権利・利益を尊重し、誠実かつ迅速に対応する

なお、個人情報保護法では、個人情報とは、生存する個人に関する情報で、その情報に含まれる氏名その他の記述により特定の個人が識別できるものを指します。個人に関する情報には、氏名、生年月日など個人を識別する情報に限らず、財産、職種、肩書、本人の画像・音声などの情報も含まれます。社員番号など記号だけのものでも、他の情報と照合して特定の個人を容易に識別できるものは、個人情報にあたります。

マネジメントシステム

組織としての個人情報保護対策は、場当たり的に実施するのではなく、個人情報保護についてのマネジメントシステムを整備することが望まれます。

マネジメントシステムとは、組織としての目的を達成するために、「方針」、「計画」、「実施手段」、「実施体制」、「実施過程」、「点検および見直し」などを管理し、継続的に改善を進める、実践的な組織経営の枠組みです。

個人情報保護のためのマネジメントシステムは、以下のような手順で整備します。

①プライバシーポリシー（個人情報保護の基本方針）を策定する
②自社で扱っている個人情報の洗い出しとリスクの確認をし、対策を講じる
③個人情報の取扱いに関する具体的な内部規定を策定する
④個人情報保護の実施と運用のための組織をつくる
⑤社員教育を実施する
⑥監査を実施し、必要な改善を行う
⑦全てのプロセスを文書化する
⑧経営トップによる見直しを行う

初めから万全な個人情報保護対策をとれなくても、こうしたプロセスを繰り返すことで、それぞれの組織に合ったより効果的な保護対策の実現が可能となります。

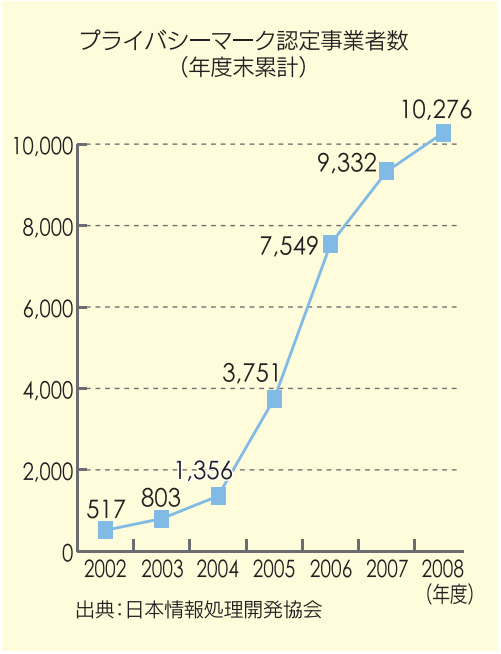
プライバシーマーク

個人情報のマネジメントシステムの適切性を第三者機関が認定する制度として、「プライバシーマーク」があります。

個人情報保護法自体には、具体的にどのような措置をすれば法律の要求を満たすかまでは書かれていません。

個人情報保護のマネジメントシステムのガイドラインとしては、JIS Q15001というJIS規格が制定されています。このJIS規格を参考にすることで、個人情報保護法に対応したマネジメントシステムがつくれます。プライバシーマーク制度は、このJIS規格に準拠した認証制度です。

プライバシーマークを取得するには、社内のマネジメント体制を整備するとともに、認定機関の審査を受ける必要があります。認定期間は2年間で、2年ごとに更新審査があります。プライバシーマークを取得すれば、事業活動を通じてのプライバシーマークの使用が認められ、顧客や取引先など社会に対して、個人情報の適正な取り扱いの体制ができていることを示すことができます。



出典：日本情報処理開発協会

保護法への“過剰反応”

個人情報保護法の誤解や無理解などにより、“過剰反応”ともいえる現象も起きています。

鉄道事故等では、被害者家族からの入院の問い合わせに、病院が第三者提供違反に当たるとの理由で、回答を拒否したという問題が起きています。

これは保護法の誤解によるものです。同法には、人の生命保護にかかわる場合で本人同意を得るのが困難な場合は、本人同意が無くても第三者提供を認める「適用除外」規定が設けられています。

また、製品購入者情報を、漏洩防止として一括削除し、リコール等の連絡が困難になった事例もあります。

古い情報の管理は甘くなりがちになることから、不要なものを廃棄するのは正しい措置とも言えます。しかしその情報が人命にかかわる可能性がある場合には、安易に廃棄せず、適正に管理すべきなのです。あくまで人権のための個人情報保護であることを忘れてはなりません。

表現の自由・プライバシー権・名誉権

インターネット上での名誉毀損など表現をめぐるトラブルが増えています。
企業のインターネット利用では、どのような注意が必要でしょうか。

表現をめぐる人権侵害

表現の自由は、最も尊重しなければならない人権のひとつです。しかし、インターネットでは、他人のプライバシー暴露、セクハラ、名誉毀損、差別や偏見の助長などによる人権侵害が深刻な問題となっています。

ある大手金融機関で、支店長が電子メール等を使って部下の女性職員に交際を強要したセクハラ事件が発生しました。この事件では、本人はもちろん会社側も職場の管理責任を問われて損害賠償の対象となりました。

あるブログでは、根拠のない噂をもとに、「あんた殺人犯　死ねば」、「殺人事件関係者と思われる人物」などと執拗に書き込まれる事件が発生し、書き込みをした会社員など7人が脅迫および名誉毀損の容疑で書類送検されています。

ホームページの表現と人権

表現にかかわる人権侵害の問題は、社員個人による名誉毀損などの事件だけではなく、企業のホームページなどでも起こります。

企業のホームページでは、プライバシー権・肖像権、差別や偏見を助長する表現、著作権などへの十分な配慮が欠かせません。

大手検索サイトが提供する写真を使った街路検索サービスでは、個人の家が特定されたり、家の中が覗かれるとの懸念から、写真の提供にあたってプライバシーへの配慮を求められた例があります。

また、ある化粧品会社が、「偉くなるのは薄毛ではない人のようです」、「子孫も迷惑です」などの表現で育毛剤の広告ページを公開してしまい、薄毛の人を侮辱し偏見を助長するとの消費者の抗議を受け、該当ページを削除し、謝罪に至った例もあります。

顧客交流サイトの管理責任

著作権侵害、プライバシー侵害、名誉毀損などの問題で、企業が管理責任を問われるのは、企業自身や社員の発信する情報だけではありません。

企業が顧客参加型の掲示板などのコミュニティサイトを運営管理している場合も注意が必要です。こうしたサイトで、参加者が他人の著作物を無断で掲載したり、プライバシー侵害や名誉毀損などに結びつく発言をし、権利侵害の事実を知りながら放置すれば、管理者としての責任が問われることがあります。

企業が誹謗中傷を受けることも

企業が誹謗中傷の対象となるケースもあります。ある動物病院が掲示板サイトで、「過剰診療、誤診、詐欺」「ヤブ医者」などといわれのない誹謗中傷を受けた事件では、発言の削除と名誉毀損による損害賠償を求める裁判を起し、勝訴した事例があります。

ネット社会の理解とモラルの向上

インターネットでプライバシー侵害や名誉毀損事件が起きる背景には、ネットの影響力を十分に理解していないことも含めて、情報モラルの欠如があります。

インターネットは公共の場です。それを忘れて、日常の噂話のつもりで書き込んだものが、プライバシー侵害や名誉毀損となることがあります。非対面型で匿名性の高いメディアのため、その特性を悪用したり、悪意はなくても不用意な発言や情報によって、他人を傷つけてしまうことがあります。

こうしたトラブルを防ぐためには、社内の情報研修等において、機器操作などの技術的な学習だけでなく、インターネットの影響力や危険性など社会的な特性を理解し、一人ひとりの情報モラルの向上を図ることが求められます。

表現の自由とのバランス

表現の自由は大切な人権ですが、それが他者の人権を著しく侵害する場合、無制限に認められるものではありません。ネット上での表現活動が個人の名誉やプライバシーなど他者の人権とぶつかる恐れがある場合、両者のバランスをよく考えて、慎重に表現活動やコミュニケーションを行う必要があります。

ただし、トラブルを恐れるあまり、必要な情報の発信や開かれたコミュニケーションを抑えてしまうのは、人権尊重の観点からも本末転倒です。

表現の自由は“優越的”といわれるほど大切な人権です。他者の人権を尊重したうえで、必要な情報の発信や、お互いの理解を深めるための開かれたコミュニケーションを積極的に行う姿勢も忘れてはなりません。

求められる企業の対応策

名誉毀損やプライバシー侵害を防ぐために、企業は適切な対応策を講ずる必要があります。

社員による名誉毀損やセクハラなどの行為については、社内での人権啓発を徹底するとともに、問題が発生したときの人権救済のために、通報相談窓口を設置しておくことが求められます。

顧客向けのコミュニケーション・サイトを運営している場合は、プロバイダ責任制限法の対象となります。この法律の内容をよく理解するとともに、利用規約を設け、利用者に他人の権利利益を侵害しないようマナーを守ることを求めるなど、適切な運営管理を図ることがトラブル防止につながります。

ホームページの情報内容については、制作者の個人任せにせず、組織としてのチェック管理体制を整備することが必要です。

情報セキュリティ

企業の情報システムは社会の安全と結びついています。
企業はセキュリティリスクに対して、どのような対策が
求められるのでしょうか。

セキュリティ対策は社会的責任

インターネットを利用した様々なサービスで、企業の果たす役割はますます大きくなり、それだけネットワークの安全についての企業の責任も大きくなってきました。

ネットワークの安全管理をおろそかにすると、個人情報の漏洩によるプライバシー侵害、ネット上での不正な財産詐取、社会インフラの停止[3]、といった被害につながる恐れがあります。

企業のコンピュータがウイルスに感染し、ネットワークを通じて広がれば、企業は被害者になるだけではなく、加害者にもなります。企業の情報セキュリティ対策は、いまや大きな社会的責任なのです。

3 例えば2008年に航空会社のシステム障害で、多数の便が欠航ないし遅延する事故が起きています。

セキュリティ上の脅威

企業がネットワークを利用する上で認識すべきセキュリティ上の脅威には、コンピュータウイルス、スパイウェア[4]、不正アクセス、情報の盗み見、情報の改ざん、なりすまし、システムダウン、などがあります。

これらの脅威は、次々と新しい手法が登場しています。

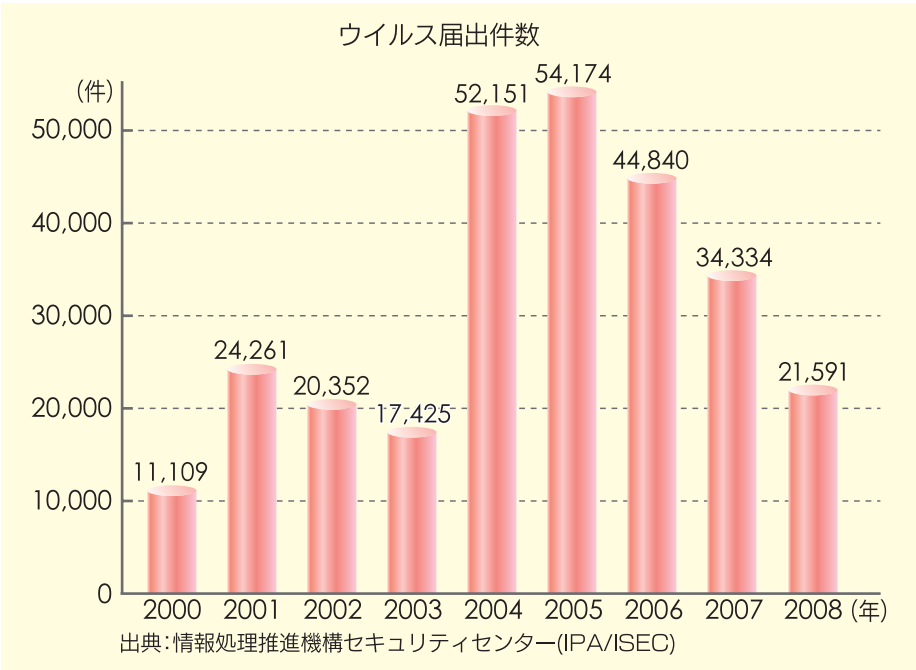
ボットネットによる攻撃

そうした脅威のひとつがボットネットです。ボットはウイルスの一種ですが、感染したコンピュータ自体には目立った被害を与えません。ボットに感染させた多くのコンピュータがネットワークで結ばれ、ロボットのように操作されることからボットネットと呼ばれています。

ボットネットは、狙いを定めたコンピュータに不正アクセス攻撃を仕掛けて情報を盗んだり、迷惑メールを大量に配信するために使われます。犯罪ビジネスの温床にもなっていると言われています。

一度に100万台以上のコンピュータを操るボットネットもあると言われています。そのなかには、セキュリティに欠陥のある家庭のパソコンから企業のコンピュータまで多くが組み込まれています。自社のコンピュータに直接の被害がなくても、ボットネットに組み込まれてしまうことで、犯罪に加担することになってしまいます。

4 ウイルスの一種。コンピュータに侵入してファイルの情報、画面の情報、キー入力の情報等を盗み出す機能を持ちます。



出典：情報処理推進機構セキュリティセンター(IPA/ISEC)

脆弱性を狙った攻撃

ウイルスの感染手法も多様化しています。これまでは電子メールの添付ファイルにウイルスを潜ませる方法が一般的でした。

その後、ソフトウェアの脆弱性(安全上の欠陥)をついて、利用者が特別な操作をしなくても感染させるタイプのものが登場しました。

そのひとつがUSBメモリーを利用したウイルスです。USBメモリーをパソコンに挿入したときに自動起動するソフトウェアの脆弱性をついて感染を広げます。企業ではデータのやりとりにUSBメモリーがよく使われることもあり、ここ数年、ウイルス感染の大きな原因となっています。

もうひとつは、改ざんされたウェブサイトの閲覧による感染です。これはウェブサイトを改ざんして外部からウイルスを埋め込み、そこにアクセスした利用者のコンピュータに感染するものです。

社員がそうしたサイトにアクセスして被害に遭うだけではありません。自社のウェブサイトが改ざんされれば、自社のホームページを訪れたお客様に被害を及ぼすことになります。

犯罪目的の攻撃が増加

以前のウイルスや不正アクセスは、技術力を誇示する愉快犯型のものが中心でした。しかし、最近は、犯罪目的の攻撃が増えていることにも注意が必要です。

愉快犯は、感染を広げて注目されること自体が目的でした。そのため、ウイルスの存在を多くの人が知ることになり、対策も幅広く進められました。

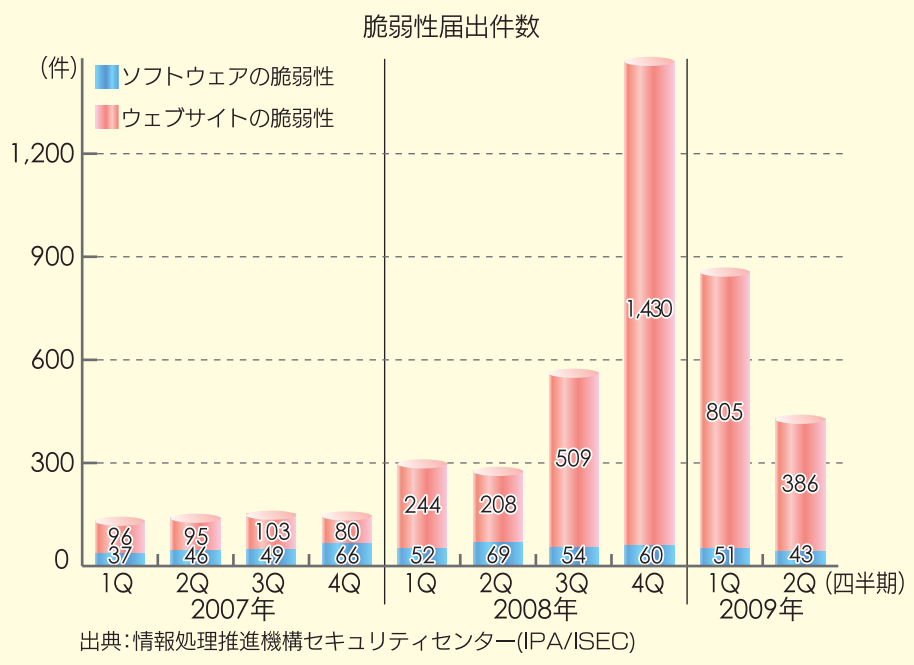
一方、犯罪を目的としたものには、標的を絞った攻撃もあり、こうしたケースでは、社会的な注意が喚起されにくく、対策が後手に回りがちです。また、犯罪を目的とした攻撃は、金銭的な利益を目的に、組織化されたものもあると言われ、個人情報や機密情報の盗難、システムダウンなどの深刻な被害につながっています。

利用者の心理をつく脅威

利用者の心理の隙をついて、個人情報を騙し取ったり、ウイルスの感染を図るものもあります。

そのひとつがフィッシング詐欺です。これは金融機関等からのメールを装って、金融機関とそっくりに作られた偽サイトにアクセスさせ、利用者が入力した口座番号や暗証番号等を盗み、預金などを不正に引き出してしまうものです。

顧客になりすましてウイルスを感染させるものもあります。顧客対応窓口などに、苦情を装ったメールを出し、担当者が添付ファイルを開かざるを得ないようにし、スパイウェアに感染させ、企業情報を盗み出す、という事件も発生しています。



出典:情報処理推進機構セキュリティセンター(IPA/ISEC)

情報セキュリティ

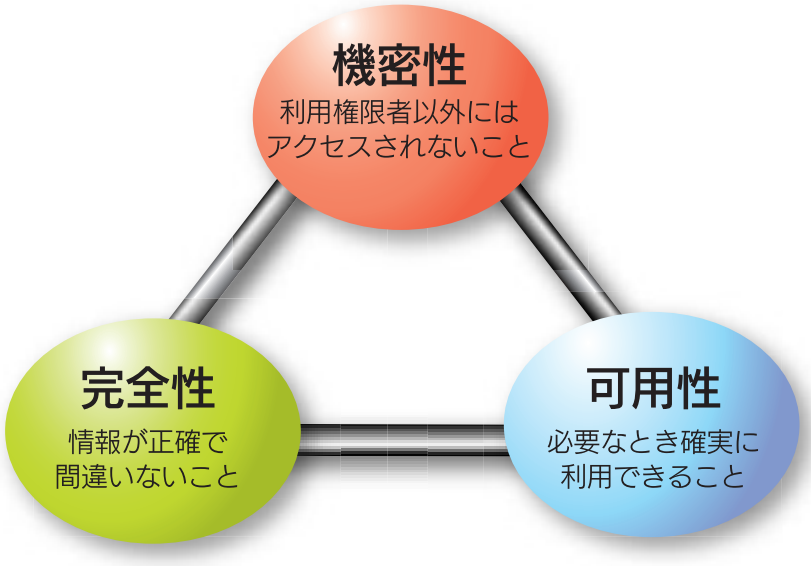
情報セキュリティの3要素

情報セキュリティで守らなければならないのは、「機密性」、「完全性」、「可用性」の3要素です。

機密性とは、正規の利用権限を持つ人にしか利用させないことです。ID、パスワードなどの認証システムによるアクセス制御、情報の暗号化などによる無権限者の閲覧防止などの対策が求められます。

完全性とは、情報の改ざん、入力・更新時の入力ミスを防ぎ、情報を正確に保つことです。不正アクセスの防止、入力・更新時のチェック体制の強化、電子署名による情報改ざん防止などの対策が求められます。

可用性とは、システム障害などで必要なときに情報が利用できなくならないようにすることです。設備の災害対策、システムや情報の二重化、データのバックアップなどの対策が求められます。



セキュリティ対策の枠組み

組織の情報セキュリティ対策は、技術的対策、物理的対策、制度・人的対策の3つを組み合わせて実施します。

技術的対策

アクセス制御のための認証システム、ウイルス対策ソフト、ファイアウォール、不正アクセス監視システム、システム二重化などが、情報システムへのセキュリティ技術の導入・運用による対策です。

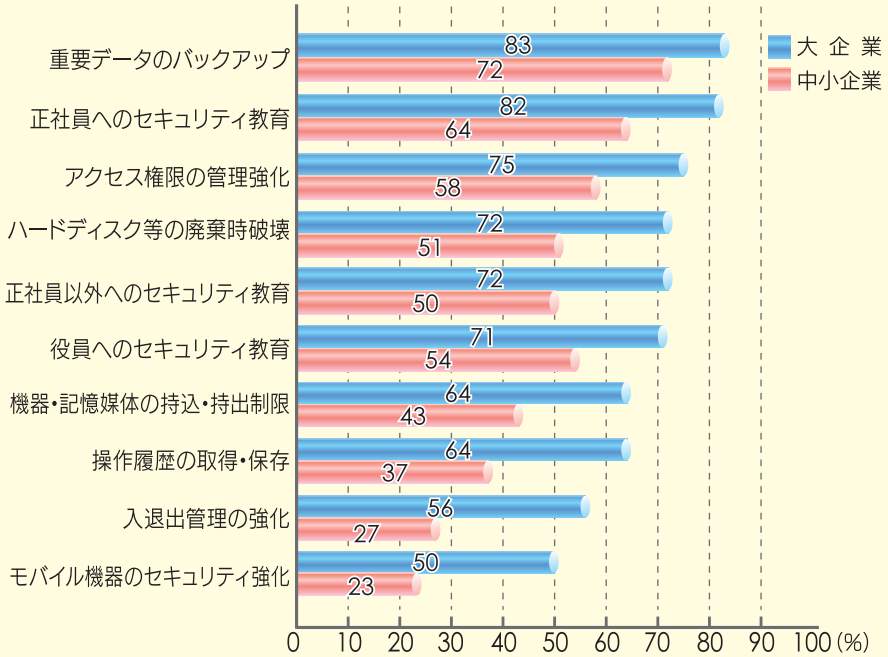
物理的対策

重要情報を扱う場所の入退館管理やゾーン分離、データ盗難防止の施錠、防災設備の設置、監視・記録カメラの設置などが、物理的な安全措置による対策です。

制度・人的対策

安全管理組織の整備、安全規定の整備、安全管理措置の評価・見直し・改善、従業員に対する啓発・研修・訓練などの教育活動、事故や違反への対処などが、制度・人的な対策です。

企業の組織・運用面でのセキュリティ対策実施率（2008年）



注：大企業は従業員数300人以上、中小企業は同300人未満

出典：情報処理推進機構セキュリティセンター(IPA/ISEC)

脅威への対策

以下に、主な情報セキュリティ上の脅威への対策を紹介します。

コンピュータウイルス対策

ウイルス対策用ソフトの導入は欠かせませんが、使用にあたっては、ウイルスをチェックするデータファイルを常に最新のものに更新する必要があります。使用しているソフトウェアの脆弱性を、メーカーの最新情報に従って修復しておくことも必要です。

技術的な対策だけでなく、憶えのないメールの添付ファイルを安易に開かない、知らないウェブサイトでは閲覧ソフトのセキュリティ強度を高める、仕事用のパソコンではファイル交換ソフトを使わないなど、利用上の注意を社内に徹底することも大切です。

不正アクセス対策

外部からの不正アクセス対策としては、ファイアウォール、認証システム、不正侵入検知システム、操作履歴(ログ)管理システムなどの技術対策が有効です。

技術対策と同時に、パスワード管理を厳格に行う、重要な情報の複写・持ち出しを禁止するといった、内部の人的対策も重要です。情報の重要度や機密度に応じてアクセス権限を明確にし、認証システムに反映させ、二重チェック体制を導入するなど、組織的な管理体制の整備も欠かせません。

情報の盗み見への対策は、暗号化が基本です。ホームページで顧客や取引先と情報をやりとりする場合は、通信データを暗号化する必要があります。

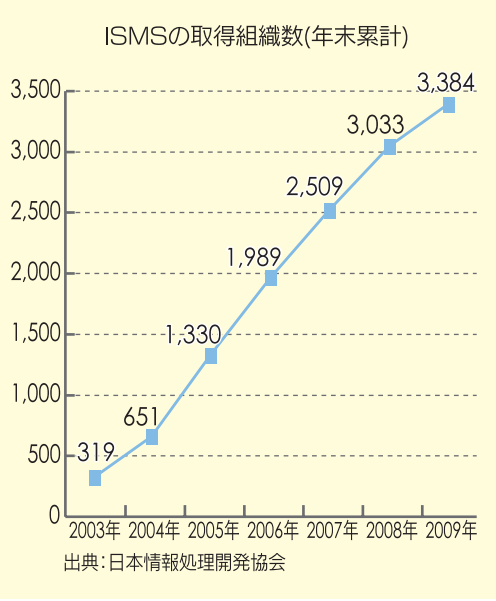
情報の改ざんやなりすまし対策には、電子署名という暗号技術を利用します。紙の書類の印鑑やサインに該当し、電子文書の発信元が実在の人物・組織であること、データが改ざんされていないことが確認できます。

ガイドラインと第三者認証制度

セキュリティ対策の取組み方には、標準的なガイドラインがあり、それを参考に取組を進めることができます。

自社の現状を簡易にチェックするには、IPA(情報処理推進機構)の「5分でできる中小企業のための情報セキュリティ自社診断パンフレット」が効果的です。

また、自社の情報セキュリティマネジメントシステムの適切性を客観的に評価する第三者認証制度としては、国際標準規格のISO27001に準拠したISMS適合性評価制度があります。第三者認証の取得は、取引先から契約上求められることもあり、一定の費用と時間はかかりますが、それだけ効果的な方法と考えられます。



事後対策の準備も忘れずに

情報セキュリティ対策には、予防対策とともに、万一、事故が起きた場合に、人権への配慮など情報モラルにのっとった的確な対応ができるよう、組織としての事後対策も必要です。

事後対策として求められるのは、迅速な現状把握、被害の拡大防止、被害者の権利を尊重した対応(謝罪、説明、補償など)、説明責任を果たす広報、業務の復旧作業、原因の究明と修復、再発防止策の検討・策定と公表などです。

事後対策は、事故が起きてからではなく、リスクマネジメントや事業継続計画のような形で、事前に準備しておくことが望まれます。事後対応にあたっては、現場だけに任せず、経営者が率先して取組むことが重要です。

電子商取引における消費者保護

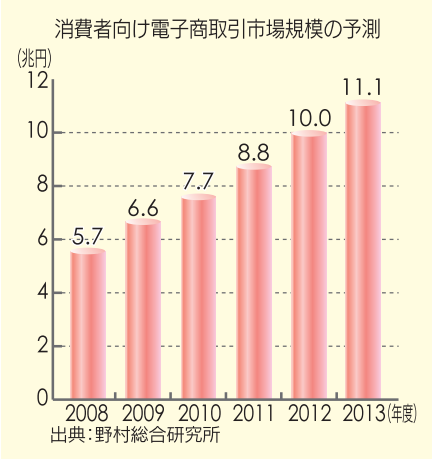
電子商取引をめぐるトラブルが絶えません。消費者の権利を尊重したショッピングサイトをつくるために求められるものは何でしょう。

拡大する電子商取引

消費者向けの電子商取引（オンライン・ショッピング）は年々拡大しています。電子商取引は、消費者にとっても、企業にとっても、インターネットの重要な用途のひとつとして、生活に欠かせないものとなりました。

インターネットで商品やサービスの購入などの電子商取引をした消費者はインターネット利用者の52%に達しています（総務省「通信利用動向調査」2008年）。

消費者向け電子商取引の市場規模は2008年度の5.7兆円から、5年後の2013年度には約2倍の11.1兆円に達すると予測されています（野村総研調べ）。



電子商取引のトラブル

拡大がつづく電子商取引ですが、消費者の権利侵害につながるトラブルも発生しており、消費者が不安を抱えている現状もあります。

消費者の権利侵害につながる問題としては、以下が指摘されています。

①迷惑なダイレクトメールの増加
②誇大広告やまぎらわしい表現による商品説明
③問い合わせ先や所在地などの表示の欠落
④購入判断に必要な商品情報や取引条件などの欠落による行き違い
⑤確認画面がないなど不適切な画面構成・操作手順による誤発注
⑥セキュリティ管理の不備によるプライバシー情報の漏洩

消費者の権利を守る法律

電子商取引における消費者の権利を守るために、次のような法律があり、事業者にはこれらの法律の遵守が求められています。

消費者を対象とした電子商取引は、特定商取引法の「通信販売」として扱われ、義務規定違反は業務停止等の行政処分の対象になります。

同法では、消費者の購入判断に必要な情報の表示義務や、広告に関する規制ルールを定めており、2008年の大幅改正で、規制の対象を指定商品から全商品へ拡大、返品やキャンセルを認めない場合の表示の義務化、事前承諾のない広告メールの禁止など、消費者保護の強化が図られました。

電子消費者契約法は、電子商取引における消費者の操作ミスの救済、契約の成立時点などを定めています。

同法では、消費者が注文の申込を行う前に申込内容を確認できる画面構成に事業者がしていなければ、消費者の操作ミスによって成立した契約を無効とすることができます。

また、割賦販売法では、クレジットカードを扱う事業者に対し、情報保護のための措置を義務付け、カード情報の不正取得・不正提供をした者を刑事罰の対象としています。

特定商取引法における
電子商取引の表示義務項目

1. 社名（個人事業者の屋号又は氏名）
2. 住所（本社、事務所）
3. 連絡先（電話番号）
4. 商品等の価格
5. 送料等の付帯費用
6. 代金の支払い時期及び方法
7. 商品等の引渡し時期
8. 返品やキャンセルに関する事項
9. 代表者又は業務責任者の氏名

注意すべき法令違反事例

企業には、経営の基本姿勢として、消費者の権利尊重と公正な取引の徹底を図ることが求められます。とくに法令遵守は欠かせない要件です。しかし現実には、特定商取引法の規定が守られていないケースも少なくありません。

以下が違反事例としてよく指摘される例です。

購入者に対する表示義務については、返品特約の有無、送料、代表責任者の氏名、商品引渡し期日などが抜けている例が目立ちます。

広告宣伝については、商品やサービスの効能や効果の表示に、裏づけとなる実証データの存在が疑わしいものが少なくありません。また、事前承諾を得ていない広告メールは迷惑メールとして社会問題ともなっています。

注文申込手続については、入力中にリターンキーを押すと自動的に送信されてしまうなど、確認画面のない画面構成のものがトラブルの元となっています。

対策のチェックポイント

消費者の権利尊重と公正な取引を実現する対策のチェックポイントは以下の通りです。

①消費者に必要な情報の開示を行っているか
②理解しにくい表示や表現になっていないか
③消費者に誤解を与える広告表現になっていないか
④広告メールは受信者の事前承諾を得ているか
⑤画面の操作手順が誤操作を招かないようになっているか
⑥顧客情報の漏洩などに対するセキュリティ対策はできているか
⑦消費者の苦情・相談窓口の設置と迅速な対応はできているか

より詳しいガイドラインとして、経済産業省の「電子商取引等に関する準則」、日本通信販売協会の「通信販売業における電子商取引ガイドライン」などが公表されています。

消費者の立場に立ったサービスを

法令遵守は最低限のモラルであり、法律やガイドラインに書かれていることだけで十分とはいえません。例えば、新しい商品やサービスは、法規制などが追いつかないことがあります。しかし、消費者の保護と権利尊重という観点からは、商品やサービスのリスク情報は、たとえ法規制がなくとも、積極的に開示する姿勢が重要です。

電子商取引は、対面販売と比べて、実物に触れられないのが弱点です。その反面、ウェブサイトなどでは大量かつ詳細な情報提供、多彩な表現が可能です。こうした特長を活かせば、物理的に制約のある店頭販売よりも、消費者の求める情報をすばやく効果的に知らせることが可能です。

消費者の立場に立ったサービスを実現すれば、消費者の権利を向上させるとともに、企業への信頼も高まります。

情報アクセシビリティ

情報アクセシビリティは人権のひとつです。
企業に求められる情報アクセシビリティとは何でしょう。
どのような取組が必要なのでしょうか。

新たな情報格差が生まれる

情報機器やホームページを利用するときに、分かりづらい操作、小さすぎる文字、画像や色の違いだけで情報が提供されると、コンピュータに不慣れな人、高齢者、障害者などは、必要な情報へのアクセスが困難となります。

インターネットは、移動や動作に制約のある高齢者や障害者の仕事や生活の可能性を広げる反面、多様な人々への配慮、すなわちアクセシビリティを欠くものであれば、新たな情報格差を生み出す原因ともなってしまいます。

企業にとっては、情報システムや情報サービスの使い勝手が悪ければ、オンラインショップでの顧客離れや、職場の作業能率の低下にもつながります。

情報アクセシビリティは人権

新たな情報格差を生み出さないために、情報アクセシビリティへの十分な配慮が求められます。

情報アクセシビリティとは、生活や仕事をする上で必要な情報を、誰もが公平かつ容易に利用できるようにすることです。

情報社会では、情報アクセシビリティは大切な人権なのです。

国連の「障害のある人の権利条約」[5]では、施設の段差解消などの物理的なアクセシビリティと並んで、情報アクセシビリティは障害者の自立的な生活を実現するための権利だと明記されています。

また、消費者の知る権利としても情報アクセシビリティは重要です。

2004年に改定された「消費者基本法」では、事業者の責務として、「消費者に対し必要な情報が提供されることが消費者の権利であることを尊重し」、「消費者に対し必要な情報を明確かつ平易に提供すること」という、情報アクセシビリティを重視した取組を求めています。

5 日本は2007年に署名し、現在、批准のための法律見直し等の作業を進めています。

ウェブページのアクセシビリティガイドライン

経済産業省では、情報アクセシビリティに配慮したウェブページのデザインを含めた情報機器および情報サービスに関するJIS規格として「高齢者・障害者等配慮設計指針」を策定しています。

JIS規格では、

①企画・制作にあたっては、高齢者・障害者が可能な限り操作又は利用できるよう配慮すること

②できるだけ多くの種類の情報通信機器、画面解像度、閲覧ソフトで利用できるよう配慮すること

③企画から運営にいたるプロセスで常に情報アクセシビリティを確保し、さらに向上するよう配慮すること、などを求めています。

情報アクセシビリティの基本

情報アクセシビリティを実現するための基本的な取組を以下に紹介します。

ユニバーサルデザインの推進

ユニバーサルデザインとは、製品やサービスを提供するときに、年齢、性別、能力、文化的背景等の違いにかかわらず、誰にでも使えるように、はじめから考慮して制作し、改善を繰り返すプロセスです。

特定の利用者専用の製品やサービスを別に用意することではありません。特別扱いではなく、公平に対応することが重要なのです。結果として、別々のものをつくるより、社会的な総コストを抑えることにもなります。

利用者の必要に応じた情報の提供・開示

ユニバーサルデザインの製品やサービスを用意しても、必要な情報が提供されなければアクセシビリティは実現されません。提供側に都合のよい情報ではなく、利用者のニーズに合った情報を的確に提供・開示することが重要です。

誰でもが分かり易い情報

提供・開示される情報は、一般の消費者などその分野の専門家ではない人も利用します。誰もが理解できるよう、平易で分かり易い表現にすることが大切です。

効果的な取組の進め方

情報アクセシビリティ向上の取組を効果的に進めるには、まず、経営者が情報アクセシビリティの重要性を認識し、経営として情報アクセシビリティ向上の必要を明確にすることが重要です。

現場に浸透させるためには、理念と心構えを啓発することに加えて、社員一人ひとりが、身の回りの業務や情報をアクセシビリティの視点で見直すことが大切です。

また、消費者、障害者、高齢者など多様なニーズを持つ実際の利用者に、企画・設計や評価の段階から参加してもらい、協力して取組むことも必要です。

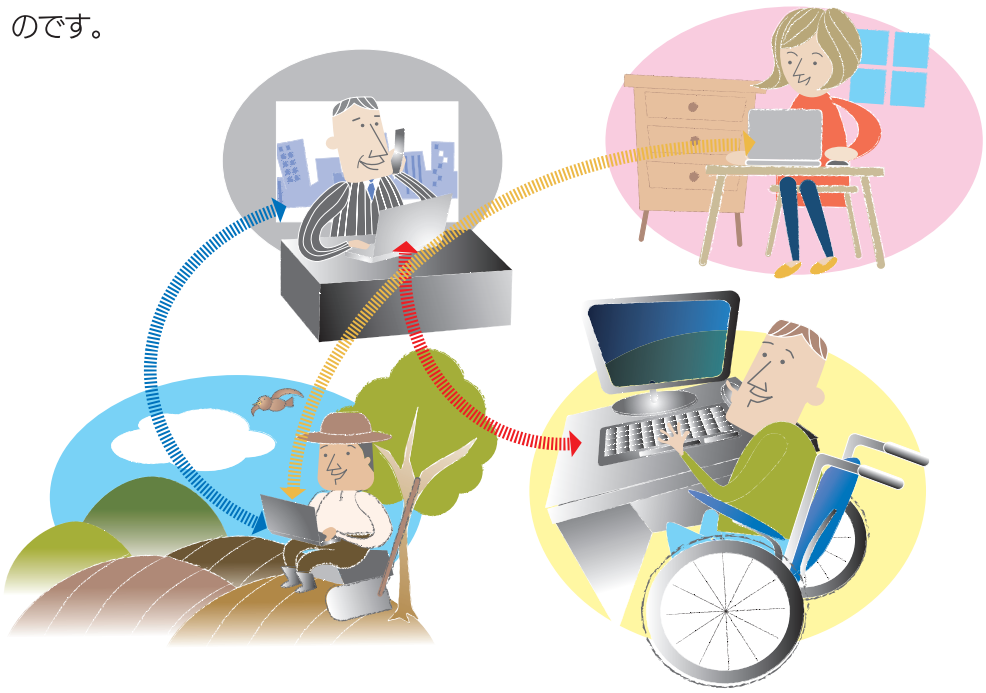
経営に役立つアクセシビリティ

情報アクセシビリティの向上は、人権の向上に寄与するのはもちろん、経営にも役立ちます。

食品偽装事件などの多発により、製品・サービスに対する消費者の不信感が募り、正確な情報提供へのニーズが高まりました。また、高齢化の進展で、今後の大切な顧客として、高齢者層への対応の充実は欠かせない課題です。こうしたなか、企業が消費者の知る権利に応え、ウェブサイトの使い勝手を改善し、情報アクセシビリティ向上に努めることは、企業への信頼と評価につながります。

企業内でも、情報アクセシビリティの向上は、社内の情報の流通を良くし、誰もが働きやすい職場につながります。また、障害者雇用促進法が求める障害者の法定雇用率[6]を遵守する上でも、情報アクセシビリティの向上は欠かせない経営課題なのです。

6 56人以上の民間企業には雇用者数の1.8%以上の障害者の雇用が法定雇用率として義務付けられています。



著作権など知的財産権

インターネットでの著作権侵害が問題となっています。
企業に求められる著作物などの知的財産の公正な利用と
保護の取組とは何でしょう。

インターネットでの著作権侵害

インターネットでは、情報の複写、編集、加工、送信が簡単にできます。こうしたネットワークの特徴を悪用して、著作物を無断で複写使用したり配布する著作権侵害行為が後を絶ちません。

企業も他人事ではありません。2009年には、健康食品販売サイトの運営者が、顧客サービスとして他社のサイトの健康情報を無断で使用したために、著作権法違反で逮捕される事件が起きました。

経費節約のためとして、ソフトウェアを必要な本数購入せず、無断で複写して利用したことが発覚し、著作権法違反に問われる企業も少なくありません。

社員がインターネットを利用して、音楽や映像作品などの著作物を無断で配布したり交換している例もあります。

知的財産にかかわる法律

著作権

著作権法は、文化的な創造物である著作物[7]の公正な利用と、著作者の権利を保護し、文化の発展に寄与することを目的に制定されたものです。

著作者の権利が保護されなければ、著作者は安心して創作活動ができなくなりますし、経済的な損失を蒙ることにもなります。

著作権法は、著作者に無断で、著作物を公表、複製、改変、頒布、貸与することなどを禁止しています。著作権は市販の著作物だけが対象ではありません。個人がウェブに趣味で掲載した創作物も対象になります。

また、著作権法では、他人の著作物を利用する際のルールを定めており、ルールに則った利用は可能です。例えば、私的利用での複製、あるいは適切な範囲での引用などです。

また、著作権には財産権と人格権の2つの側面があります。財産権は、譲渡を受けることも可能ですが、公表権、氏名表示権、内容の同一性保持権などの著作者人格権は譲渡の対象にはなりません。

その他の知的財産権

企業には、著作権以外にも、配慮すべき知的財産権として、特許権、意匠権、実用新案権、などの工業所有権があり、それぞれが法律によって保護されています。

営業秘密については、不正な取得を行えば、不正競争防止法違反となり、刑罰を含む法的な責任が問われます。

また、不正アクセスや保存管理の甘さなどにより、営業秘密にかかわる情報が漏洩する事件も起きています。自社の営業秘密など知的財産情報に関しては、情報セキュリティの側面からの取組も必要になります。

7 具体的には、創造的な表現を持った文章、音楽、絵画、図面、写真、映画、ソフトウェアなどが著作物に該当します。

公正な利用のための取組

企業が著作権侵害行為を防ぎ、著作物の公正な利用を実現するためには、社員一人ひとりの意識の向上と、組織としての管理体制の整備を図る必要があります。

まず、会社として、「著作権を尊重し、著作物の無断使用や無断コピーをしてはならない」ことを明確にし、それを社員全員に徹底します。その上で、ソフトウェアなど企業の情報資産に関する管理責任者と管理規定を設け、その規定に基づいて、違法なコピーや利用が発生しないよう運用していくことが求められます。

ただし、著作物の複製による利用がすべて禁止されているわけではありません。著作者の許諾を得れば、引用の範囲を超えた利用も可能です。社内研修等を通じて、公正な利用のルールをきちんと学習・実践することが必要です。

知的財産管理の方法

著作権、工業所有権、営業秘密などの知的財産は、企業にとって重要な経営資源でもあります。それだけに、自社の知的財産を適切に保護管理すると同時に、他社や他人の知的財産権を尊重することは、企業にとって当然の責務だといえます。

保護管理の方法としては、例えば営業秘密の場合、他の一般情報と明確に区分して、「マル秘」など機密情報であることを明示し、利用権限に基づいたアクセス制御を行うなど、適切な管理体制を整備します。他社の情報を不正な方法で入手しないという倫理規定を明確にすることも必要です。

知的財産は、保護するだけではなく、経営資源として活用することも大切です。戦略的に活用していくためには、社内の知的財産資源を洗い出し、いつでも活用可能なように管理体制を整えておくことが大切です。

著作物管理もうひとつの視点

著作物を扱う企業や著作物の制作者にとって、著作権侵害行為から著作物をいかに守るかは死活問題です。保護のための厳格な管理を求めるのは当然といえます。

しかし、著作物は私的利用における複製が認められているように、利用者の権利があることも忘れてはならないでしょう。著作権の保護対策は、利用者の権利利益にも配慮して、バランスのとれた取組が望まれます。

また、新しい時代の要請に耳を傾けることも大切です。ソフトウェアの分野では、オープンソースという、既存の著作権の枠組みに縛られず、内容の改変も可能なように元のプログラムを公開し、協働で開発を進める取組も行われています。こうした取組のほうが創作活動に有効な場合もあります。著作物の管理も幅広い視野が求められる時代なのです。

労働者の人権と情報

情報管理やITの利用による、労働者のプライバシー侵害や健康被害に対して、企業はどのような取組を進めればいいでしょうか。

不当な個人情報の収集

顧客の個人情報の取扱いは慎重に行なっても、従業員に対しては、雇用者と被雇用者の力関係から、本来取得すべきではない個人情報を一方的に取得するなど、人権侵害を起す例があります。

ある企業で、定期健康診断の際、本人に無断でHIV抗体検査を実施し、感染が判明した期間雇用者に退職を勧奨し、応じないと不景気によるリストラを理由に解雇するという事件が起きました。

この事件の裁判では、業務上の必要性がないHIV検査による従業員の個人情報の取得はプライバシー侵害であるとして、損害賠償の支払を、HIV感染を実質的な理由とする解雇は解雇権の濫用であるとして、解雇の無効と契約期間の賃金の支払を命じています。

セキュリティ対策での権利侵害

情報セキュリティ対策でも、労働者の権利を侵害しない配慮が必要です。

企業はセキュリティ対策として、監視カメラやコンピュータの利用履歴(ログ)の監視をすることがあります。監視自体はセキュリティ対策として有効であり、違法ではありません。

しかし、本来、プライバシーが保持されるべき更衣室への監視カメラの設置など、監視が行き過ぎたり、特定の社員に対する監視など本来の目的以外での監視を行えば、労働者のプライバシー権の侵害となります。

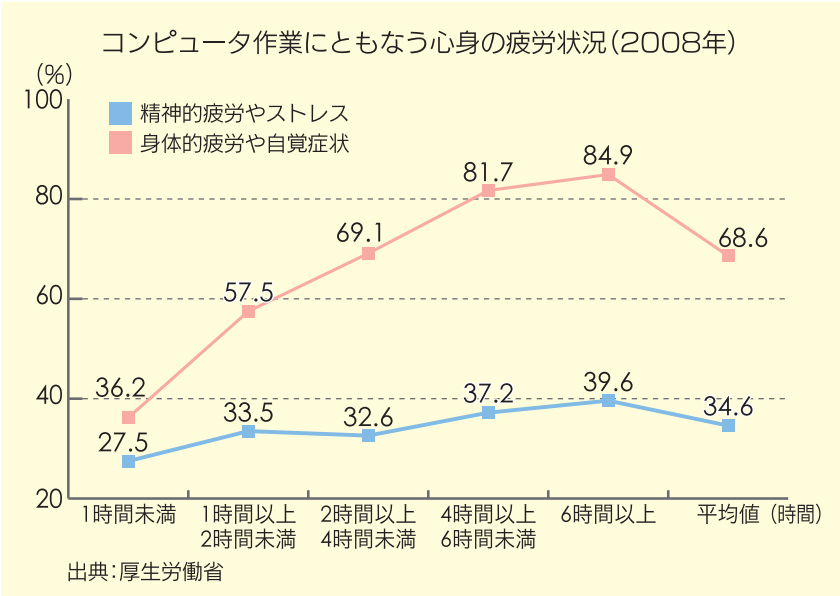
また、労働者の安全管理上の過失に対して、罰則規定を設けること自体は違法ではありませんが、損害賠償を労働者に一方的に負わせる罰則規定を予め設けることは、労働者の権利を侵害するものとして労働基準法違反となります。

IT利用にともなう健康被害

従来は、技術者やキーパンチャーなどの専門家が管理された環境でコンピュータを使用することが多く、そうしたキー入力作業者は、一定間隔毎に休憩を取るなど、作業管理が実施されていました。

しかし、あらゆる職場でコンピュータが使用されるようになり、使用環境は多様化し、労働衛生管理も行き届かなくなっています。仕事でコンピュータを利用している人の35%が精神的疲労やストレスを、69%が身体的疲労を感じているといいます(厚生労働省「技術革新と労働に関する実態調査」2008年)。

ITの利用にともなう労働者の健康被害は見過ごせない問題となっているのです。



出典:厚生労働省

労働者の個人情報保護の指針

労働者の個人情報保護の指針として、厚生労働省は、雇用者に関する「労働者の個人情報保護に関する行動指針」と、求職者に関する「個人情報の取り扱いに関する指針（公正採用に関する告示）」を公表しています。企業には、これらの指針に沿った規定の整備と運用が求められます。

個人情報保護法には含まれていない事項で、これらの指針が求める主な内容は以下のものです。

特定の個人情報の収集制限

法律の定めや特別な職業上の必要がない限り、人種、民族、社会的身分、本籍、出生地その他の社会的差別の原因のおそれのある事項、および、思想、信条及び信仰にかかわる情報の収集を禁止しています。

また、法律や特段の労使合意の規定がある場合を除き、医療上の個人情報の収集や労働者の労働組合活動にかかわる情報の収集も禁止しています。

検査による個人情報の収集制限

労働者に対する、「うそ発見器及び類似機器を使った検査」、「HIV検査」、「遺伝子検査」についてはいかなる場合も原則的に禁止です。「アルコール及び薬物検査」は、職業上の特別な必要があり、かつ本人の同意を得た場合を除いて禁止です。「性格検査」は目的内容を説明したうえで本人の同意を得ることが必要とされています。

監視（モニタリング）の制限

法律の定めがあるなどの場合を除き、カメラや操作履歴による監視の実施は、実施理由、実施時間帯、収集する情報内容を事前に明示し、労働者の権利を侵害しないよう配慮が求められています。

労働衛生管理の指針

IT機器作業における労働衛生管理については、厚生労働省が「VDT[8]作業における労働衛生管理のためのガイドライン」を公表し、以下の取組を求めています。

①作業環境の管理：作業者の疲労を軽減し作業者が支障なく作業を行えるよう、照明、採光、騒音などを管理します。

②作業管理：作業者の心身の負担が少なく作業ができるよう、作業時間の管理、適切な情報機器・関連什器の選定及び利用時の位置などの調整管理を行います。

③機器および作業環境の維持改善管理：情報機器及び作業環境について、点検と清掃を行い、必要に応じた改善を実施します。

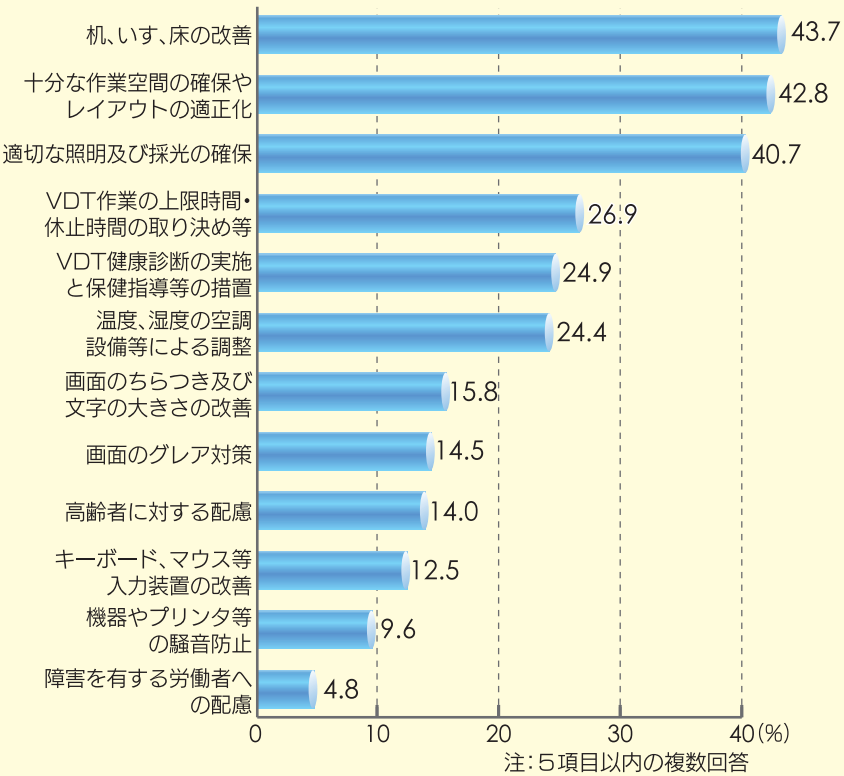
④健康管理：作業者の健康診断や健康相談を実施します。

⑤労働衛生教育：作業者及び作業者の管理者に対して、労働衛生教育を実施します。

企業には、このガイドラインにそった管理体制の整備が求められます。

8 Video（またはVisual）Display Terminal（コンピュータの操作端末）の略。

健康管理のために今後取り組みたい課題（2008年）



注：5項目以内の複数回答

出典：厚生労働省

用語解説

企業の社会的責任 p2
企業が、経済活動だけでなく、環境問題や人権等の社会の幅広い分野に対して、事業活動を通じて与える影響に責任を持つことで、企業の持続的な発展を目指すこと。

企業の情報モラル p1
企業が情報を取り扱う際に配慮が求められる考え方および行動のこと。具体的には人権、安全、社会的公正を損なわないように配慮して情報を扱うことが求められる。

コンピュータウイルス p3
ファイルやプログラムに寄生して気づかれずにコンピュータへ侵入（感染）して、システム妨害、情報破壊、情報改ざんなどの被害をもたらす不正プログラムのこと。

自己情報の管理（コントロール）権 p10
本人が自己にかかわる情報の扱い方をコントロールする権利のこと。個人情報保護法における事業者の管理義務規定は、この権利の考え方を反映したものとなっている。

性弱説 p9
人を、本来的に性善または性悪と決め付けず、誰もが過ちを犯しうる弱さを持った存在であることを前提に、問題に対処しようという考え方。

ソフトウェアの脆弱性 p17
ソフトウェアが、ウイルス感染や不正アクセスなど、安全上の脅威を受ける可能性を防いでいないシステム上の弱点のこと。

知的財産権 p24
知的創作物（発明・著作物等）や営業上の表示（商標・商号等）、その他事業に有用な情報（営業秘密等）などの無形財産にかかわる創作者の権利。

特定商取引法 p20
訪問販売や通信販売など、特定の業態に関して、取引を公正にし、消費者の利益を保護するためのルールなどを定めた法律。電子商取引は、同法の通信販売のルールの適用対象となっている。

ドメスティックバイオレンス p10
夫や恋人など、親密な関係の人から受ける暴力。身体的な暴力のほか、言葉による暴力、罵りや無視などの精神的暴力、手紙等のチェックの強要なども対象となる。

プライバシーマーク p13
個人情報保護マネジメントシステムのJIS規格に適合した管理体制を整備している事業者を認定する第三者認証制度のこと。認定されるとマークの使用が認められる。

プライバシー権 p7
基本的人権のひとつとされ、従来は、みだりに私生活が覗かれたり、公開されないための権利であったが、近年では、自己情報の管理（コントロール）権に拡張されている。

プロバイダ責任制限法 p15
インターネット上で名誉毀損等の権利侵害があったときに、プロバイダや運営管理者が負う損害賠償責任の範囲や、発信者情報の開示請求の権利などを定めた法律。

マネジメントサイクル p8
計画（Plan）、実行（Do）、評価（Check）、改善（Act）のPDCAサイクルを繰り返すことで、目的達成に向けて仕事を効果的に進めるための経営管理手法。

名誉毀損 p4
他人の品性、徳行、名声、信用などの人格的価値についての社会的評価を不法に低下させる行為。名誉権の侵害。民法では不法行為、刑法では名誉毀損罪の対象となる。

リスクと脅威 p6
不正アクセス、ウイルス、災害、故障などを脅威といい、これらの脅威が、情報システムや組織の抱える脆弱性により、実際の被害につながる可能性をリスクという。

リスクマネジメント p19
企業を取り巻くリスクを組織的に管理する経営手法。リスクを洗い出し、分析し、それぞれのリスクに応じて、経営の観点から、回避策、低減策などを準備する。

ISMS p19
Information Security Management System（情報セキュリティマネジメントシステム）の略称。ISO27001の第三者認証制度として国際標準化されている。

ISO p19
International Organization for Standardization（国際標準化機構）の略称。同機構が策定する国際標準規格の名称としても使われている。

参考サイト

最新のデータは以下を参照ください
www.hyper.or.jp/moral/

個人情報保護

- 個人情報の保護に関する法律
  www.caa.go.jp/seikatsu/kojin/houritsu/
- 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/
- プライバシーマーク制度
  privacymark.jp
- 個人情報保護マネジメントのJIS規格
  www.jisc.go.jp/app/JPS/JPSO0020.html

表現の自由・プライバシー権・名誉権

- プロバイダ責任制限法
  law.e-gov.go.jp/htmldata/H13/H13HO137.html
- 法務省人権擁護局インターネット人権相談窓口
  www.moj.go.jp/JINKEN/jinken113.html
- インターネットホットライン連絡協議会
  www.iajapan.org/hotline/

情報セキュリティ

- 経済産業省の情報セキュリティに関する法律・ガイドライン
  www.meti.go.jp/policy/netsecurity/law_guidelines.htm
- 情報処理推進機構（IPA）セキュリティセンター
  www.ipa.go.jp/security/
- IPAの中小企業向け情報セキュリティ対策
  www.ipa.go.jp/security/manager/know/sme-guide/index.html
- ISMS適合性評価制度
  www.isms.jipdec.jp/isms.html
- ネットあんしんセンター（ハイパーネットワーク社会研究所）
  www.hyper.or.jp/anshin/

電子商取引と消費者保護

- 特定商品取引法
  www.no-trouble.jp/#1200000
- 電子消費者契約法
  www.meti.go.jp/topic/data/e11011aj.html
- 経済産業省電子商取引等に関する準則
  www.meti.go.jp/press/20080829004/20080829004.html
- 割賦販売法
  law.e-gov.go.jp/htmldata/S36/S36HO159.html
- 日本通信販売協会通信販売業における電子商取引ガイドライン
  www.jadma.org/guideline/02.html
- 国民生活センター「消費・生活に関するトラブルや対策方法の紹介－インターネット通販」
  www.kokusen.go.jp/soudan_topics/data/internet2.html
- 次世代電子商取引推進協議会
  www.ecom.or.jp
- ECネットワーク（ADRのあっせんなどの相談窓口）
  ecnetwork.jp

情報アクセシビリティ

- 障害のある人の権利条約
  www.mofa.go.jp/mofaj/gaiko/treaty/shomei_32.html
- 高齢者・障害者等配慮設計指針のJIS規格
  www.jisc.go.jp/app/JPS/JPSO0020.html
- 障害者雇用施策
  www.mhlw.go.jp/bunya/koyou/shougaisha.html
- 消費者基本法
  www.consumer.go.jp/kankeihourei/kihon/

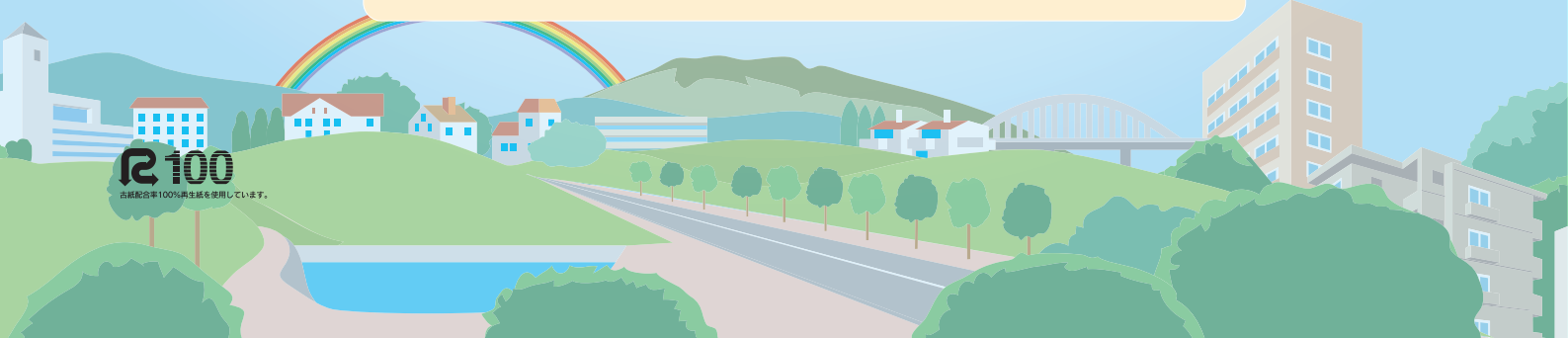
著作権など知的財産権

- 著作権
  www.bunka.go.jp/chosakuken/index_2.html
- 工業所有権関連法
  www.jpo.go.jp/index/houritsu_jouyaku.html
- 不正競争防止法
  www.meti.go.jp/policy/economy/chizai/chiteki/unfair-competition.html

労働者の人権と情報

- 労働者の個人情報保護に関する行動指針
  www2.mhlw.go.jp/kisya/daijin/20001220_01_d/20001220_01_d.html
- 公正採用に関する告示
  www2.mhlw.go.jp/topics/topics/saiyo/dl/saiyo1a.pdf
- 平成20年技術革新と労働に関する実態調査
  www.mhlw.go.jp/toukei/list/48-20.html
- VDT作業における労働衛生管理のためのガイドライン
  www.jil.go.jp/kisya/kijun/20020405_02_ki/20020405_02_ki.html

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
TEL：097-537-8180　FAX：097-537-8820
www.hyper.or.jp　moral@hyper.or.jp
2010年2月　発行



R100
古紙配合率100%再生紙を使用しています。