情報社会に問われる企業の社会的責任

情報モラルの確立で築く社会の信頼

財団法人ハイパーネットワーク社会研究所
http://www.hyper.or.jp/

このパンフレットをご利用いただくにあたって

インターネットの普及により、世界中の企業、世界中の人々が、より自由に情報を活用し、コミュニケーションをとることが可能になりました。今、ビジネスも人々の生活もインターネットなしでは考えられない時代になってきたといえます。

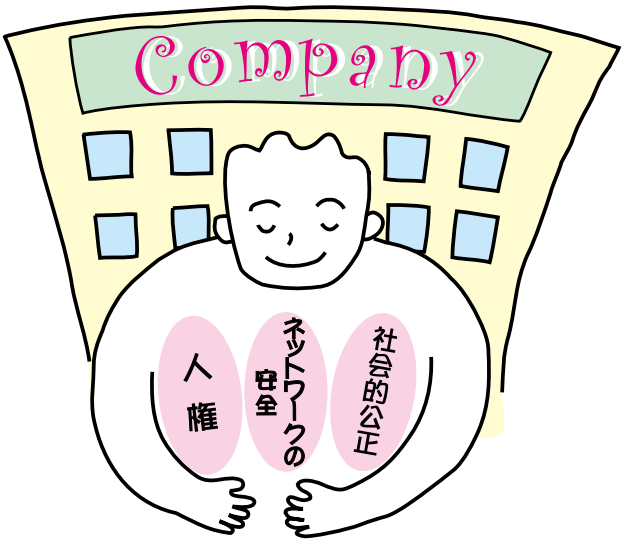
その一方で、個人情報の漏洩、コンピュータウイルスや不正アクセス、ネットワーク上でのプライバシー侵害や名誉毀損など、インターネットの利用にともなう新たな社会問題が発生しています。

こうした中で、企業がIT（情報通信技術）を有効に活用しつつ、健全なネットワーク社会を築くためには、情報を扱う際の、人権の尊重、安全への配慮、社会的公正への配慮といった「情報モラル」の確立が求められています。

今日では企業における「情報モラル」の確立は、企業の社会的な責任のひとつであるといえます。

このパンフレットは、
企業がインターネットなどITを活用して情報を扱う上で配慮すべき問題とは何か、それらの問題に対して、社会的責任を果たすために企業はどのような取り組みをすべきか、についてまとめたものです。

それぞれの企業が、情報社会において信頼と共感を得る企業活動を一層推進するためにご利用いただければ幸いです。



もくじ

インターネットを活用した企業活動と新たな課題

情報社会における企業の社会的責任

情報モラルにかかわる問題と求められる対応

インターネットを活用した企業活動と新たな課題

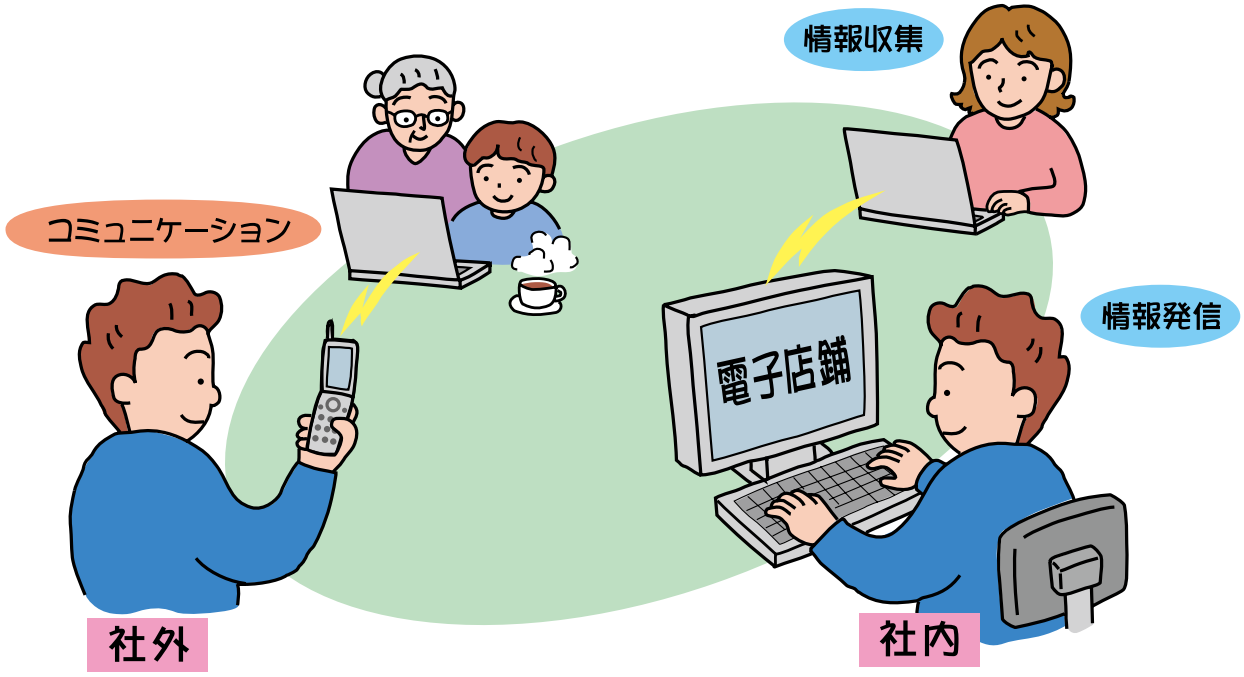
インターネットは企業と社会を結ぶ情報基盤

現在、IT（情報通信技術）は企業活動に欠かせないもののひとつとなっています。とりわけ、インターネットの普及によって、ITを利用する人の範囲も広がり、社員の誰でもがその利用者となりました。その用途も、情報の収集、情報の発信、コミュニケーション、電子店舗の運営まで、幅広くなっています。

これは大企業ばかりでなく、中小企業においても同じです。総務省の調査によると、従業員数が100～299人規模の中堅・中小企業の78.2%がホームページを開設しており、電子商取引（インターネットを利用した調達や販売）を行っている企業も46.3%に達します。（グラフ1参照）。

企業ばかりでなく、生活者の利用も広がっています。2007年末における日本のインターネット利用者数は8811万人、人口普及率は69.0%に達しています（グラフ2参照）。

インターネットは、企業と企業、企業と消費者、企業と投資家など、企業と社会を結ぶ重要な社会生活基盤のひとつであるといえます。



効率性と利便性が利用を広げる

インターネットが急速に普及している背景には、企業活動や人々の生活をより効率的で利便性の高いものにする手段として期待されていることがあります。企業は、インターネットの活用によって、時間や場所の制約なしに、大量の情報を素早く処理し、伝達することが可能となりました。また、インターネットを利用することで、世界中の取引先や消費者と、時間や場所に縛られることなく、いつでもコミュニケーションをとり、商品やサービスの受発注をすることも可能となりました。

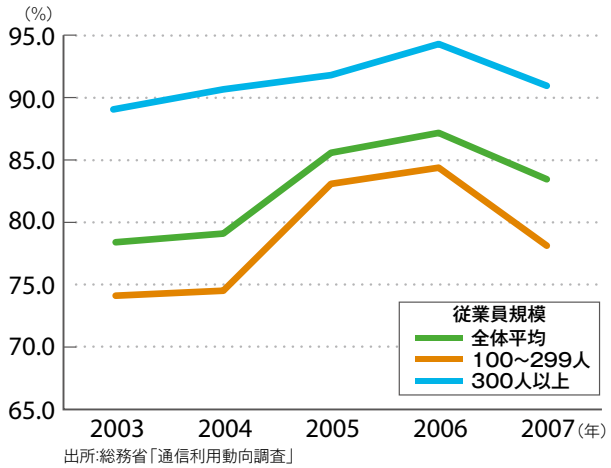
いまやインターネットは社会に不可欠な存在といえます。企業にとっては、インターネットをいかに適切かつ効果的に活用するかどうかが、これからの時代を生き抜く上で欠かせない条件だといえます。

情報社会の課題ー情報漏洩やウイルスが大きな社会問題に

インターネットの普及が進み、それへの社会的な依存度が高まるなかで、情報を利用するときの管理の不備、誤った使い方、悪用などによって生じる社会的な課題が大きくなっていることも事実です。

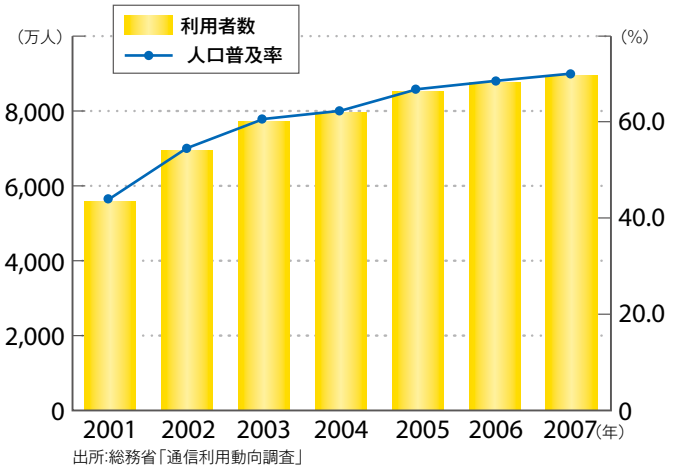
最近では、プライバシー侵害や詐欺被害につながる個人情報の流出や、ネットワーク利用の安全を脅かすコンピュータウイルスの拡散などが、大きな社会問題になっています。2006年には、大手印刷会社の業務委託先社員がダイレクトメール用の個人情報860万件を不正に持ち出し、その一部を詐欺グループに売り渡したことにより、インターネット通販などで不正に利用されるという事件も発生しています。

グラフ1. 中堅･中小企業のホームページ開設率



出所:総務省「通信利用動向調査」

グラフ2. インターネット利用者数及び人口普及率の推移



出所:総務省「通信利用動向調査」

個人情報の漏洩は、プライバシーの侵害を引き起こし、企業の信用を失う

個人情報の流出やコンピュータウイルスのほかにも、不正アクセス、ネットを利用した詐欺・悪徳商法、名誉毀損・誹謗中傷などのITネットワークにからむ事件は後を絶ちません。

警察庁によると、ハイテク犯罪の検挙数は毎年増加の一途をたどっています（グラフ3参照）。

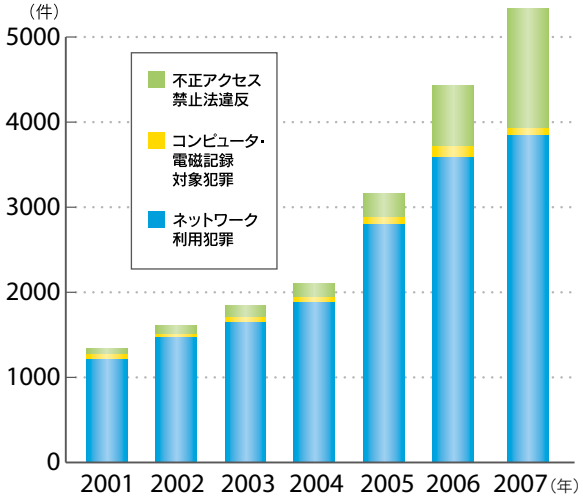
こうした問題では、企業は被害者になるだけなく加害者の立場にもなります。

企業が持つ個人情報を流出させれば、当人のプライバシーを侵害する可能性があります。それに伴い、損害賠償請求を受けることにもなります。さらに、2005年4月に全面施行された個人情報保護法によって、個人データの安全管理のために必要かつ適切な措置を取らなければ、主務大臣からの勧告措置を受けたり、場合によっては罰金などの罰則を受けることにもなります。

また、社員のパソコンがウイルスに感染すれば、取引先の企業や顧客にまでウイルスの感染を拡大させる可能性もあります。2005年度のコンピュータウイルスによる企業の被害総額は、逸失売上やシステム停止にともなう業務効率低下などの復旧コストを加えると、1社当り平均で、中小企業は約430万円、大企業は約1億3000万円に達すると推定されています。※1

※1（独）情報処理推進機構2005年調査より

グラフ3．ハイテク犯罪の検挙状況



出所:警察庁

コラム

個人情報を漏洩した企業の損害賠償責任と損失

●個人情報の漏洩では、自治体における委託事業者からの住民データの漏洩事件で、一人当たり1万円（この他弁護士費用が1人当たり5千円加わる）という損害賠償の命令が管理監督責任を持つ自治体になされた例があります。これは、住民基本台帳レベルの基本情報についての損害賠償額の判例ですが、思想や病歴などにより深刻な精神的被害につながる情報や、クレジット番号など経済的な被害に直接つながる情報が含まれていれば、これよりはるかに賠償額は大きくなります。

●こうした賠償請求以外にも、流出した個人への謝罪、事故対応の経費は少なくありません。460万人分の顧客情報漏洩事件のあった大手インターネット接続事業者では、全会員590万人への謝罪の金券送付など事後対策費用が約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漏洩事件のあった通信販売事業者では、原因究明と対策のための1ヵ月半の営業自粛によって減収額は約150億円に達したといわれます。

企業活動に求められる情報モラルとは

インターネットは企業活動全般に欠かせないものですが、あくまで道具のひとつです。こうした道具を社会に役立つものとするには、操作方法に習熟するだけでは足りません。企業がIT（情報技術）を活用して情報を扱う際には、顧客や取引先、従業員など、やり取りする相手の権利や安全を損なうことのないように配慮する情報モラルの確立が求められます。

インターネットの利用に求められる情報モラルとしては、「人権を尊重すること、ネットワークの安全を脅かさないこと、社会的な公正を守ること」があげられます。

情報モラル

人権への配慮

インターネットの利用にあたっては、
人権に配慮した個人情報の管理や
コミュニケーションが求められます。
具体的には
●プライバシーの侵害
●誹謗中傷による名誉毀損
などの問題を引き起こさないよう
人権に配慮する必要があります。

安全への配慮

インターネットの利用にあたっては、
ネットワークの安全に対する配慮が、
社会的な要請として求められます。
具体的には
●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
などの問題を防ぐよう安全に配慮
する必要があります。

社会的公正への配慮

インターネットでの情報・サービス
提供にあたっては、社会的公正へ
配慮することが望まれます。
具体的には
●電子商取引での消費者の権利尊重
●著作権など知的所有権の尊重
●高齢者や障害者など誰でもが使いやすい
　仕組み
などに配慮する必要があります。

情報社会における企業の社会的責任

企業活動は社会に支えられている

企業は経済活動を通じて収益をあげることが大きな目的であることは確かです。しかし同時に、企業の経済活動は、顧客をはじめ、社員、取引先、投資家、地域など、様々な人々や社会によって支えられていることを忘れてはなりません。企業も社会の一員なのです。そこでは、企業活動によってもたらされる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。

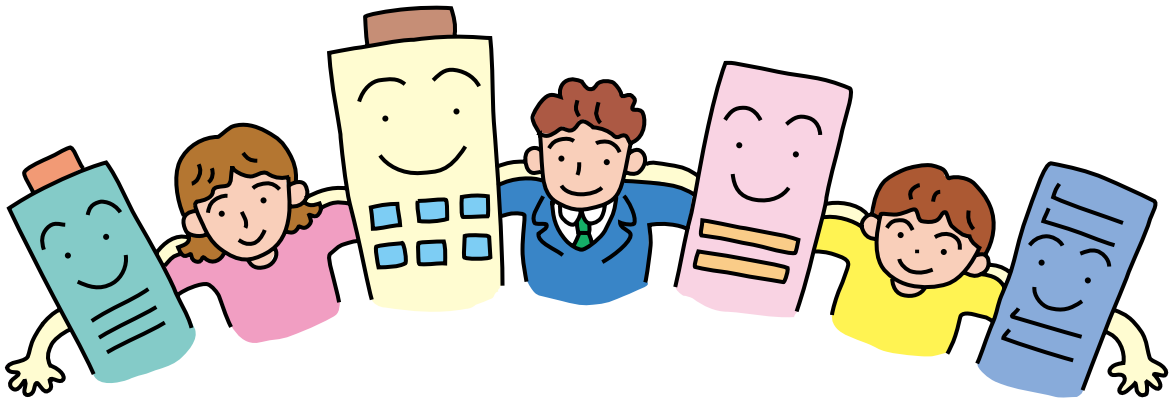
企業の社会的責任というと、環境問題、人権問題、雇用問題、商品の安全性への配慮などがよく言われますが、情報を取り扱う上での配慮も、また、企業の重要な社会的責任のひとつです。

企業は個人情報や取引先の企業情報というものを介して、人々の人権や社会の安全を預かっているのだということを常に意識しておくことが必要です。

企業の社会的責任は重要な経営課題

企業が社会的責任を持った行動をとることは、今日、経営上の重要課題でもあります。管理の不備により、個人情報の漏洩などの不祥事が起きれば、その法的な責任が問われるばかりでなく、こうした事件をきっかけに、永年の努力で築いてきた信頼というブランドを一夜にして失うことにもなります。企業は、収益をあげなければ存続できませんが、社会の信頼を失えば存在する価値そのものを失うことにもなるのです。

その一方で、企業が社会的責任を果たすことは、企業の信用力の向上につながります。情報化社会では、信用力が大きな企業価値ともなります。



社会的にも強まる情報ガバナンスの要請

企業の社会的責任の重要な柱のひとつがコンプライアンス（法令順守）の徹底です。情報や情報システムの利用に関してもコンプライアンス体制の確立が求められています。プライバシー等の人権に配慮した個人情報の適正な管理を求める個人情報保護法、財務報告の正確性を求める金融商品取引法、さらには業務全般の適正性の確保を求める会社法など、個人情報や財務情報など重要な情報を適正に扱うために内部統制の確立を求める法制度が成立しています。

そのため、情報および情報システムの利用にあたり、自社はもとより、顧客、労働者、株主など企業活動に関わる様々な人々の基本的な権利・利益を損なうことのないよう、情報セキュリティ対策とともに、法的に適正な情報の管理を維持するための内部統制と社会的な説明責任を果たす情報ガバナンス体制を築くことが要請されています。

トップが率先して取り組むべき

企業が情報モラルを確立するためには企業トップの役割が重要になります。それは、トップ自らが情報モラルを持たなければならないという当然のことだけではありません。情報モラルを持つことが、業績をあげるのと同様の経営課題そのものだという認識が必要だからです。

情報セキュリティ（安全性）のための対策には、通常の業務とは別の手間やコストがかかることがあります。こうしたとき、トップが情報セキュリティよりも目先の業績の追求ばかりに目を向けていれば、倫理綱領を策定し、社員の情報モラル研修をしたとしても、それは形だけのものになってしまい、現場では、情報モラルに関する優先度が下がってしまうことになります。

経営課題としての位置づけを明確にできるのは経営トップの役割です。現場はトップの姿勢を見ています。情報モラル確立の取り組みが実効性を持つかどうかは、経営トップの姿勢と役割にかかっています。

求められる組織としての情報モラル

情報社会に生きる企業が、情報を扱う際のトラブルを防ぎ、健全な情報社会を維持するためには、情報の利用に際して、人権、社会的安全、社会的公正を尊重する考え方と態度を常に持つ、という情報モラルの確立が求められます（8ページ参照）。

健全な情報社会を維持するために、法律を守ることは大切なことです。しかし、法律は、一律に適用せざるを得ないという制約や、策定に時間がかかるため事後的に作らざるを得ないという事情があるため、法律が全ての問題や事例に対応できているとは言えません。

例えば、電子メールの送信自体は違法ではありません。しかし、必要以上のメールを勝手に送りつづける行為は、受信者の迷惑になるとともに、ネットワークに不必要な混雑を招くものであり、配慮するべき行為といえます。

このように、情報社会においては、法律の精神を尊重することはもちろんですが、それぞれの場面に応じて、自らの情報モラルに基づいた判断と行動が求められます。

コラム

情報モラルの心構え

人権、社会的安全、社会的公正に配慮した情報モラルを確立する上での
基本的な心構えとしては、以下のことが大切です。

① 人と社会を大切にすること

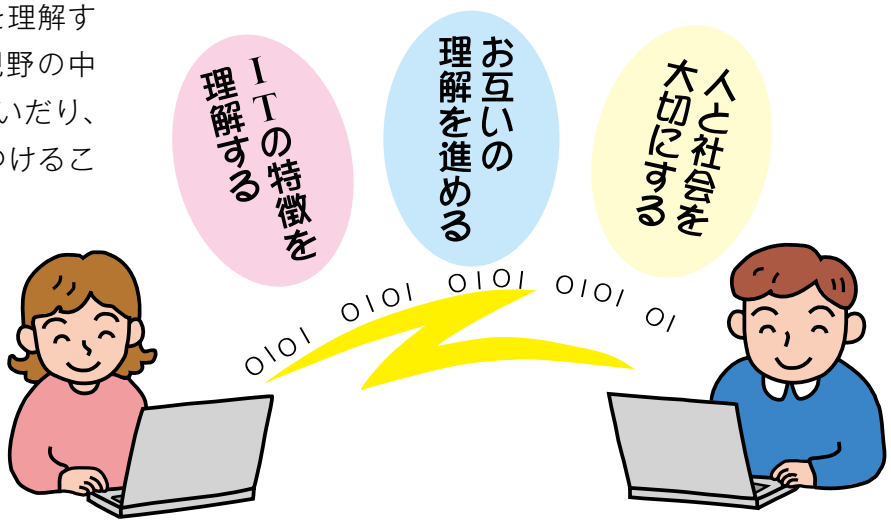
どんなにコンピュータとネットワークが普及しても、その向こうに繋がっているのは人であり、社会です。相手の顔が見えにくいインターネットでは、ついそのことを忘れてしまいがちです。そうしたとき、人権を尊重する意識や社会の安全に対する意識が薄れてしまうことになります。

こうした問題を引き起こさないためには、ネットワークの向こうには人がいるということを忘れず、人と社会を大切にする意識を持ち続けることが求められます。

② お互いの理解を進めること

情報に関わるトラブルでは、名誉毀損問題における表現の自由と名誉権のように、お互いの権利が衝突する場面も少なくありません。こうしたとき、人を大切にするといっても、こちらの思い込みだけでは問題は解決しません。ここで必要なのは、お互いの理解を進める努力です。問題の状況を的確に把握すること、相手を理解するために聞く耳を持つこと、こちらを理解してもらうために的確な説明責任を果たすことが大切です。

お互いの立場や見方を理解する努力を行えば、広い視野の中で、衝突の行き過ぎを防いだり、新たな解決への道を見つけることも可能になります。



③ インターネットの特徴と影響力を理解すること

インターネットはこれまでに使ってきた新聞やテレビなどのメディアとは異なった影響力をもっています。技術の面でも利用の面でも進化が速いものです。利用するにあたっては、情報がどのような伝わり方をするのか、どのような問題が起きる可能性があるのか、といったインターネットの特徴と影響力を理解しておくことが大切です。（9ページ参照）。

コラム

ＩＴ（情報技術）の特徴

その長所と短所を理解することがリスク回避につながる

ネットワーク社会における情報モラルを確立するためには、
その特徴を理解して活用することが大切です。

① 情報の加工、編集、複写が簡単にできる

コンピュータによって、情報を加工、編集、複写することが容易になりました。

しかしそのことは、大切な情報が目に見えないところで書き換えられたり、複写されたりする可能性にもつながっています。

② 情報を素早く広域に伝送できる

技術の進歩により、大量の情報を一瞬にして世界中に送信することも可能になりました。

しかしそのことは、漏洩した個人情報がネットワーク上をどこまでも拡散したり、世界中にウイルスをばら撒いてしまったりという恐れにもつながっています。

③ 時間と場所の制約がなくなる

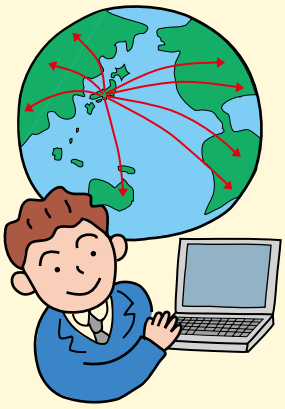
インターネットは時間と場所の制約をなくしました。

しかし、顔をあわせることの無いネットワーク上のやり取りは、なりすましや詐欺といった犯罪のリスクとともに、操作ミスによる間違い、コミュニケーションの行き違いなどの問題を広げる可能性にもつながっています。

④ 誰でも情報発信者になれる

ホームページなどを利用して、誰でもが直接世界中に情報を発信できるようになりました。また、匿名での情報発信も可能だということも特徴です。

しかしその一方で、プライバシーの侵害、名誉毀損、差別の助長など、人権侵害や社会的公正を損なう事件が発生するリスクも高まっています。



⑤ オープンなネットワークである

インターネットは、全ての利用者がつながっているオープンなネットワークです。

しかしオープンなネットワークであることは不正なアクセスを受けたり、途中で情報が覗かれてしまったり、改ざんされてしまうというリスクも同時にもたらしています。

組織の情報モラル確立のために

1 情報モラルに関する基本綱領を策定する

情報にかかわる法律の遵守をはじめ、組織としての情報モラル規範を倫理綱領や社内規定などの形で策定し、それを社内に徹底させる必要があります。

ただし、倫理綱領を策定しただけでは、形だけの取り組みに終わる可能性もあります。倫理綱領をより実効性のあるものにするためには、基本理念の記述だけではなく、それを日常の事業活動と結びつけた行動綱領の形にするなどして、社員一人ひとりの日々の活動につながる取り組みが求められます。

2 運用基準と組織的なチェック体制を設ける

情報モラルに関する基本綱領を実現するためには、ITシステムや情報を扱う上での具体的なマニュアルともなる運用基準をつくる必要があります。

ただし、運用基準を作ったとしても、人間は間違いを犯すことがあります。また、全ての対応がマニュアル通りに処理できるわけでもありません。こうしたとき、情報やシステムの運用管理を個人任せにしてしまわないように、情報の内容や処理の重要度に応じて、事前又は事後の報告や確認など、組織として責任を持つためのチェック体制をつくることが求められます。

3 必要なときに相談できる組織体制をつくる

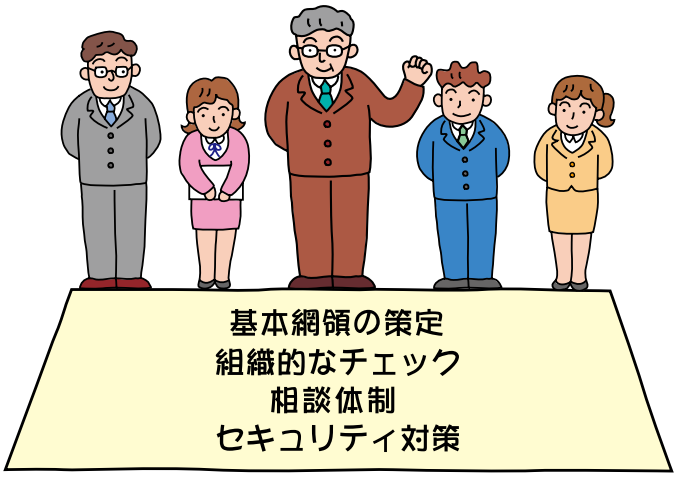
情報を取り扱う際に、それが法律や社会的な倫理に抵触しないか、技術的な危険はないかなど、どのような対応が適切であるかの判断が難しい場合があります。こうしたとき、利用者の相談や問い合わせに対応できる仕組みを準備することが重要です。

どのような組織体制を準備するかは、それぞれの企業の組織事情によって異なりますが、組織規模が小さく専門的な担当者をおけないなど内部での対応が難しい場合は、外部の専門家や専門機関を利用することも一つの方法です。

4 適切なセキュリティ技術を活用する

情報漏洩やウイルスなどの情報セキュリティ問題に対処するためには、セキュリティ技術の活用も欠かせません。

技術対策には、セキュリティの強度、使い勝手、コストなどに応じて様々なシステムや方法があります。扱う情報の重要度やリスクの度合いを検討したうえで、適切なセキュリティ技術を選択することが必要です。また、セキュリティ技術は導入するだけでは十分な効果は得られません。むしろ導入後の運用の仕方がカギを握ります。



5 社員の情報モラル意識を高める

倫理綱領や社内規則をつくり、組織の管理体制を整え、技術的な情報セキュリティ対策を行ったとしても、十分とはいえません。なぜなら、社員一人ひとりに情報モラルがなければ、規則や管理体制、技術対策も、十分に機能しないからです。

たとえば、利用者のパスワードは、情報セキュリティを守るための技術対策ですが、利用者がセキュリティの自覚を持たず、パスワードをメモしてパソコンのディスプレイに貼り付けておけば、せっかくの技術も役に立たなくなります。

また、現場では、規則や技術対策が想定していない問題に遭遇することも少なくありません。そうした場面では、社員一人ひとりの判断力が求められます。その元になる情報モラル意識の醸成が重要です。日常業務に結びつく形で社員研修や啓発活動を行い、社員一人ひとりの情報モラルを向上させていく取り組みが求められます。

6 委託事業者にも明確な確認を

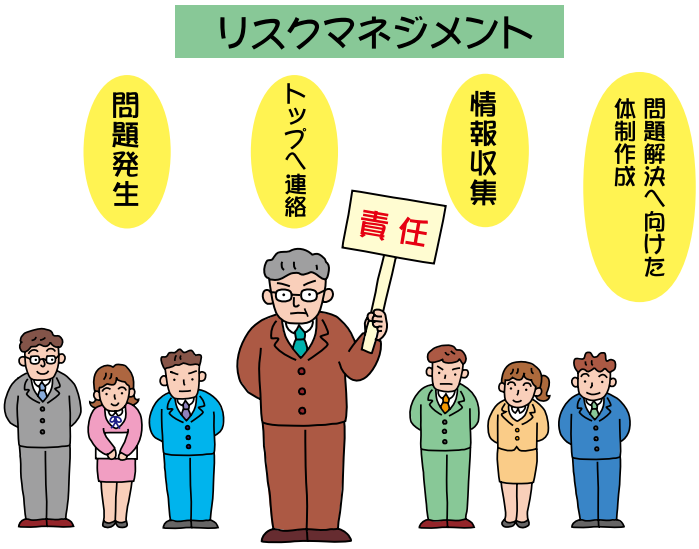
個人情報の入力作業や給与明細の印刷、またホームページの作成・運用などを、外部の事業者に委託するケースは多くみられます。しかし、個人情報の流出事故が委託先で発生している例も少なくありません。

外部の事業者へ業務を委託する際には、法令の遵守や、社内の倫理基準に準じた情報の扱いに関する取り組みが出来ているかどうかの確認を、明確な形で取り交わすことが必要となります。また、実際の運用にあたっても、事業者に対する適切な管理・監督を行うことが求められます。

7 もし、問題が起きてしまったら…

どんなに予防対策をとっても、問題が発生することはあります。問題が発生したときに、問題の拡大を防ぎ、適切に問題の解決を図ることは、企業の社会的責任としても、企業のリスクマネジメント（危機管理）としても重要な課題です。そのためには、問題の発生にあたり、全社的な権限を持って情報を素早く収集し、企業としての責任を持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。

そうした組織は、委員会方式をはじめ、それぞれの組織事情に応じて様々な形態が考えられますが、いずれにしても、顧客情報の漏洩など重要な問題に関しては、トップが率先して取り組み、社会に向けた説明責任を果たしていくことが必要となります。



情報モラルにかかわる問題と求められる対応

個人情報保護

個人情報は個人からの預かりもの

企業は業務のなかで多くの個人情報を利用しています。顧客名簿や取引履歴情報、採用時の応募者情報や社員の人事情報などがあげられます。これらの個人情報は、企業にとっては経営資源のひとつでもあり、なくてはならない有用な情報です。しかしこうした個人情報を、勝手に収集したり、無制限に利用すれば、プライバシーの侵害や犯罪行為や迷惑行為につながる恐れもあります。

個人情報がインターネット上に流出するようなことがあれば、どこまでも拡散する恐れがあり、回収することも困難です。

また、外部には流出していないとしても、企業に集められた個人情報が、どのような管理のされ方や使われ方をしているかが分からない場合には、利用者の不安が大きくなります。

企業としては、個人情報は、個人から管理を託された預りものという意識を持って、慎重な管理と適切な利用を徹底することが求められます。

表：主な個人情報漏洩・紛失事件

年　次	業　種	経　路	原　因	漏洩件数および事件概要
1999年	自治体	業務委託業者	不正コピー	健康診断システム開発の再々委託先のアルバイト社員が仕事のため持ち出した約22万人分の住民基本台帳データを電子媒体へ不正にコピーして名簿業者に転売。
2002年	美容業者	ウェブサイト	不注意な設定	ウェブサーバーのアクセス制限のかけ忘れにより資料やプレゼントに応募してきた顧客の氏名・住所・電話番号などの個人情報約5万件がウェブサイトから流出。迷惑メールなどの二次被害も発生。
2003年	自治体	内部職員	不注意な廃棄	用地買収などに絡む地権者名や補償金額等の個人情報を含む文書約100件が記録されたパソコンを廃棄。廃棄したパソコンの取得者がデータが消去されていないことを発見。
2004年	通信会社	派遣社員	不正アクセス	業務委託先の元派遣社員が勤務時に知ったパスワードを他人に教え、不正アクセスにより顧客情報約450万件が引きだされ、それを元に同社恐喝事件が発生。
2005年	金融機関	内部関係者	紛失	預金・貸出残高等を含む個人・法人約130万件の顧客情報の入ったCD-ROMを紛失。金融庁より個人情報保護法に基づき国内初の是正勧告が出された。
2006年	警察	ネットワーク	ウイルス感染	私物のパソコンに入れたファイル交換ソフト「ウィニー」がウイルスに感染。自宅に持ち帰って作業に使った事件関係者の個人情報約4400件を含む捜査関連資料がインターネットに流出。
2007年	印刷会社	内部関係者	不正持ち出し	ダイレクトメール用に預かった業務委託先企業の顧客情報約860万件を内部関係者が持ち出して転売。これらの情報が詐欺などで不正使用された。

名刺も個人情報のひとつ

個人情報とは、氏名、住所、電話番号、生年月日、顔の画像や声などのように、その情報だけで特定の個人が識別できるものです。

また、他の情報と組み合わせて照合することで特定の個人を識別できるものも個人情報に該当します。たとえば、商品の取引履歴情報も会員名簿などと組み合わせることができれば個人情報に該当します。

個人情報は従来の「一般には公開していない情報や、知られたくない情報」という意味でのプライバシー情報だけとは限りません。例えば、取引先の担当者から受け取る名刺情報なども個人情報に該当します。

なぜ個人情報の漏洩が起きるのか

個人情報保護における最大の問題は情報の漏洩です。個人情報の漏洩は、なぜ起きるのでしょうか。

情報漏洩の原因は、外部からの犯罪によるものと、内部関係者による犯罪や管理上のミスによるものがあります。

外部からの犯罪としては、ネットワークの隙を狙った不正なアクセスによって個人情報が盗み出されるケースや、電子商取引などで入力中の個人情報が電話の盗聴と同じ様に盗み見されるなどのケースがあります。

意外に多い外部からの漏洩

個人情報漏洩事件の多くの事例は、外部からの犯罪よりは、内部の関係者による犯罪や、ずさんな管理によるもの、うっかりミスによるものだといえます。具体的には次のような事例があります。

「雇用者が退職後、使えないはずのパスワードが使えるようになっていたため、顧客情報を引き出されてしまった。」

「顧客情報を自宅で分析しようと持ち出したUSBメモリ等の記憶媒体を紛失してしまった。」

「社員の誰でもがアクセス可能なコンピュータに重要な顧客情報が置かれていた。」

「個人情報が入ったままのパソコンを廃棄してしまった。」などです。

基本的な安全管理の不足、情報セキュリティに関する配慮の欠如が原因になっている例が少なくありません。

発見が遅れやすい情報の流出

コンピュータ上の個人情報の場合、物の窃盗事件と違って、情報が盗まれても、情報そのものがなくなるわけではありません。このため、流出したことに気づかず、発見が遅れてしまうことがあります。流出した個人情報が他の犯罪に使われたことで流出の事実が明らかになるケースも少なくありません。

その意味で、個人情報の漏洩問題に対処するには、防衛と監視という両面から、技術的な対策を図ると同時に、社員の安全対策意識の向上や組織的な管理体制を整備することが重要な課題となってきます。

個人情報保護法の順守

企業からの大量な個人情報の漏洩が頻発するなかで、2003年5月に「個人情報の保護に関する法律」（以下、「個人情報保護法」）が公布施行され、2005年4月から全面施行となっています。

この法律は、事業者における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。そのため、法と政令では、業務の目的で5,000件以上の個人情報を取り扱う事業者に対して、取り扱い上の義務を課しています（「個人情報保護法における個人情報の取り扱い上の義務」参照）。

個人情報保護というと、個人情報の漏洩問題にばかり目が向きがちです。たしかに、漏洩問題は重要度の高い問題です。しかし「個人情報の取り扱い上の業務」項目を見てもわかるように、それは個人情報保護の一部に過ぎません。個人情報の保護は、漏洩を防止するだけではなく、個人情報の収集、利用、維持管理の全てにおいて、当該個人を尊重した適正な運用管理が求められることを忘れてはなりません。

扱う個人情報の件数が少なく法的な管理義務が適用されない事業者も、個人情報を適正に運用管理しなければならないことに変わりはありません。

▼個人情報の保護に関する法律
http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html【内閣府】

個人情報保護法における個人情報の取り扱い上の義務（項目概要）

①あらかじめ個人情報の利用目的をできる限り特定しておく。
②個人情報を利用目的の達成に必要な範囲でのみ利用する。
③偽りその他不正な手段によって個人情報を取得してはならない。
④個人情報の取得にあたって、利用目的を、本人に通知・公表する。
⑤個人データを正確かつ最新の内容で保つように努める。
⑥個人データの安全管理のための必要かつ適切な措置を講じる。
⑦従業員、委託先に対しても、安全管理のために必要かつ適切な監督を行う。
⑧あらかじめ本人の同意を得ない限り、個人データを第三者に提供してはならない。
⑨保有する個人データの利用目的等、一定の項目について本人の知り得る状態にしておく。
⑩保有する個人データを本人の求めに応じて開示、訂正、利用停止を行う。求めに応じられない場合は、その理由の説明に努める。
⑪個人情報の取り扱いに関する苦情の適切かつ迅速な処理に努める。

個人情報保護法のガイドラインを参考に

個人情報保護法は基本的な方向を示すものですが、具体的に求められる取り組みは、それぞれの業種や扱う業務によって異なります。このため、それぞれの事業分野に関わる所轄の省庁から具体的なガイドラインが出されています。経済産業省からは「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」が2008年2月に改正されています。こうしたガイドラインを参考に、法律が求める個人情報保護の取り組みを企業として進めることが必要です。

▼個人情報保護法に関する各省庁のガイドライン
http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html【内閣府】

個人情報保護　その対応･対策

●組織としての対策

個人情報保護について組織として取り組むには、①個人情報保護の意識を徹底すること、②個人情報保護法を遵守すること、が求められます。また、これらを組織の制度的な取り組みとして行うために、③組織体制を整備すること、が求められます。

●とるべき具体的措置

個人情報保護法には、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が書いてあるわけではありません。

具体的にとるべき措置は、各省庁が示すガイドラインなどを参考に、それぞれの企業が扱う、個人情報の内容、利用の仕方、技術環境、社会的な規範などの条件を考慮し、社会に受け入れられる個人情報保護の仕組みを企業自身で構築する必要があります。

●外部委託事業者の管理･監督

個人情報の処理を外部の事業者に委託している企業は、社内体制の整備だけでなく、委託先事業者の監督も必要です。個人情報保護法では、委託先事業者で個人情報漏洩などが発生した場合に、委託元の企業にも監督責任が問われることにもなります。個人から大切な個人情報を預かっている以上、そこまでの責任があるということです。

個人情報保護についての基本姿勢

①必要のない情報は収集したり保管したりしない
②情報を収集するときは本人に必ず利用目的を正確に伝える
③個人情報は個人からの預かりものだという意識を徹底する

個人情報保護のためのマネジメントシステム

組織としての個人情報保護の取り組みは、**「マネジメントシステム」**として整備をすることが望まれます。

マネジメントシステムとは、組織が目標を達成するための管理体制の仕組みです。計画を立て、計画を実行し、計画どおりに実行されているかを評価し、その評価に基づいて不備な点を改善していくという、PDCAサイクル※1を繰り返すことで実現します。

具体的には、以下のような手順で進めます。

①プライバシーポリシーの策定

どのような方針で個人情報を扱うかをまとめた「個人情報保護基本方針（プライバシーポリシー）」を経営者が決定し、これを社員に周知させる。またホームページなどで、顧客など一般の人が分かるように公表する。

②具体的な内部規程の策定

プライバシーポリシーを実現するため、個人情報に関する法令及びその他の規範に照らし、どのような取り扱い上の措置が必要かを明確にして、具体的な内部規程を策定する。

③個人情報の洗い出しとリスク確認

自社で保有する個人情報を洗い出し、それぞれの取り扱いに関するリスクを確認し、リスクに応じたセキュリティ対策を講じる。

④運用組織の形成

経営者が管理責任者を選任し、個人情報保護の実施と運用に係る業務を行なう組織をつくる。

⑤社員教育の実施

社員の理解を進めるため、社内規程で教育研修を規定し、これを継続的に実施する。

⑥監査の実施

監査責任者を選任し、個人情報保護の取り組みの運用状況を定期的に監査するとともに、その監査に基づき、継続的に取り組みの改善に努める。

⑦プロセスの文書化

説明責任を果たせるようにすべてのプロセスで文書化を行い検証･追跡を可能にする。

※1　ＰＤＣＡ＝Plan Do Check Actの略

個人情報保護についての第三者評価

個人情報保護のマネジメント･システムとしては、JIS Q15001 という JIS 規格が制定されています。この JIS 規格を参考に自社のマネジメントシステムを構築することができます。また、マネジメントシステムを構築したとき、その適切性を第三者機関が認定するプライバシーマークという制度があります。これを利用すれば自社の取り組みの適切性を客観的に評価することができます。

▼個人情報保護マネジメントに関するJIS規格
http://www.webstore.jsa.or.jp/webstore/JIS/FlowControl.jsp【(財)日本規格協会】
http://www.jisc.go.jp/app/JPS/JPSO0020.html【日本工業標準調査会】(検索ページでQ15001と入力すると閲覧のみ可能)
▼プライバシーマークに関する情報
http://privacymark.jp/【(財)日本情報処理開発協会プライバシーマーク事務局】

個人情報保護のための技術対策も忘れずに

技術的な対策は、個人情報の流出などを防ぐ安全管理対策が中心になります。名刺などはカギのかかる場所にしまうなどの対策がありますが、コンピュータやインターネットで扱う目に見えない情報の管理は、専門的なシステム技術による対策も必要となります。

個人情報保護のための技術対策は、外部を対象にした対策と、内部を対象にした対策に分けられます。

【外部からの情報盗難を防ぐ】

外部を対象にした対策としては、不正アクセスによるコンピュータ内の情報の盗難と、電子商取引の際の情報の盗み見を防止するなどの必要があります。

不正アクセスを防ぐには、ファイアウォールの設置が必要です。ファイアウォールとはネットワークの入り口で許可された通信方法以外の通過を防ぐ仕組みです。

ネットワーク上での盗み見対策は、暗号化による対策が必要です。電子商取引のホームページで顧客が注文情報や個人情報を入力する際に、そのデータを暗号化して送信することで、途中で盗み見をされたとしても、簡単には解読されなくなります。

【内部の利用管理を徹底する】

内部に対する管理としては、アクセス制御と利用履歴の管理が基本的な対策としてあります。

アクセス制御とは、個人情報を誰がどこまで扱えるかを決めて管理することです。そのためには、個人情報にファイルを扱う権限を必要のある少数の人に限定し、ID、パスワードによって管理を行います。

さらに、高度なアクセス制御機能を持ったシステムの導入や、最近では、指紋や瞳の虹彩で個人を判別する生体認証などのシステムを導入する方法も進められています。

利用履歴の管理は、個人情報など重要なデータについて、誰が･いつ･どのように利用したかの履歴を取ることで、不正利用を抑止することにつながります。

情報セキュリティ

インターネット利用の安心と安全を守ることは企業の社会的責任

インターネットなどを利用する際の安全に関わる脅威としては、コンピュータウイルス、不正アクセス、情報の盗み見、情報の改ざん、なりすまし、などがあります。ネットワークが停止するようなことがあれば、利用者の不安を高めるとともに、ビジネス活動や社会生活に大きな影響を与えることになります。

今日では、インターネットなどを利用したサービスにおける企業の役割はますます大きくなっています。それだけに、企業にとっては、その利便性を享受するだけではなく、利用にともなうセキュリティ（安全性）の確保は、社会的責任のひとつであるといえます。

情報セキュリティ　その対応・対策

セキュリティマネジメントシステム

【セキュリティ対策の心構え】

OECDでは、2002年に「情報システム及びネットワークのセキュリティのためのガイドライン」を改定し、セキュリティの9原則を掲げています。その中では、セキュリティ方針を決め、リスクを特定し、幅広い観点からセキュリティ対策を講じ、それを適切に運用し、再評価した結果をフィードバックするという情報セキュリティマネジメントシステムによる取り組みが求められています。

【第三者認証制度を活用】

情報セキュリティマネジメントシステム（ISMS＝Information Security Management System）とは、企業などの組織が情報を適切に管理し、機密を守るための包括的な枠組みのことです。セキュリティ対策だけでなく、情報を扱う際の基本的な方針（セキュリティポリシー）や、それに基づいた計画、実施、計画の見直しまで含めた、総括的なリスクマネジメント体系のことを指します。その適合性を客観的に評価するのが第三者認証制度の一つであるISMS適合性評価制度です。情報セキュリティマネジメントシステムの構築にあたっては、こうした制度を利用するのも有効です。企業が自らのセキュリティ対策に取り組むためのガイドラインとしても重要な視点といえます。また、情報セキュリティ監査制度を利用することも有効な方法です。

▼ISMSに関する情報
http://www.isms.jipdec.jp/isms.html【（財）日本情報処理開発協会情報マネジメントシステム推進センター】

▼情報セキュリティ監査制度に関する情報
http://www.meti.go.jp/policy/netsecurity/audit.htm【経済産業省】

[OECDのセキュリティ9原則]

①**認識原則**：参加者は、セキュリティの必要性ならびに自分達にできるセキュリティ対策について認識すべきである。
②**責任原則**：参加者は、情報システム及びネットワークのセキュリティに責任を負うべきである。
③**対応原則**：参加者は、セキュリティへの事件・事故へ対応するために、時宜を得た協力的な方法で行動をすべきである。
④**倫理原則**：参加者は、他者の正当な利益を尊重すべきである。
⑤**民主主義原則**：情報システム及びネットワークのセキュリティは、民主主義社会の価値に適合すべきである。
⑥**リスク評価原則**：参加者は、リスク評価を行うべきである。
⑦**セキュリティの設計及び実装原則**：参加者は、情報システム及びネットワークの基本的な要素としてセキュリティを組み込むべきである。
⑧**セキュリティマネジメント原則**：参加者は、セキュリティマネジメントへの統合的アプローチを採用すべきである。
⑨**再評価原則**：参加者は、情報システム及びネットワークのセキュリティの監査点検及び再評価を行い、セキュリティの方針、実践、手段及び手続に適切な修正をすべきである。

コンピュータウイルス

コンピュータウイルス（以下、ウイルスとする）はコンピュータの正常な働きを妨害するプログラムのことです。インターネットの普及以前からウイルスはありましたが、ネットワークの普及によって、その影響力が急速に高まっています。

【わずか数日で世界に被害を拡大】

2003年初頭に発生した「SQLスラマー」というウイルスは、韓国で大規模なネットワークの接続障害を引き起こしたのをはじめ、各国のオンライン銀行の運用にも障害が発生するなど、わずか数日で世界中に大規模な被害をもたらしました。

最近では、「ウィニー」などのファイル交換ソフトに感染するウイルスの被害も広がっています。こうしたウイルスによって、自宅に持ち帰った会社の重要書類や個人情報のファイルがファイル交換ソフトを通じて知らぬ間にネットワークに公開されてしまうという事件が頻発しています。

また、ウイルスのように感染したコンピュータ自体に直接被害をもたらすよりも、遠隔操作によって他のコンピュータへの不正アクセスや迷惑メールの大量発信の踏み台として感染したコンピュータを利用するボットと呼ばれる悪質なソフトウェアも登場しています。

【閲覧するだけでも感染】

ウイルス感染の原因は、これまで、電子メールにウイルスが添付されてくるケースが大半でした。しかし、最近では、電子メールや閲覧ソフトなどのセキュリティ上の欠陥をついたウイルスが登場し、ネットワークに接続するだけ、または閲覧するだけで、ウイルスに感染してしまうケースもあります。

【自らが加害者に】

コンピュータウイルスは自社が被害を受けるだけではありません。ウイルスに感染していることを知らずにウイルスに感染した電子メールを送ってしまえば、自らが感染源にもなりかねません。

コンピュータウイルス　その対応・対策

●ウイルス対策ソフトの導入

コンピュータウイルス対策として、ウイルス・チェック用のソフトウェアの導入は欠かせません。このソフトは、ファイルの中身を検査して、ウイルスがないかどうかをチェックしてくれるものです。

チェック用のソフトの導入後は、新しいウイルスに対処できるよう、ウイルス・チェック用のデータを常に新しいものに更新することを忘れてはなりません。

●ソフトウェアの欠陥をふさいでおく

電子メールやホームページ閲覧ソフト（InternetExplorer等）、オペレーティングソフト（Windows等の基本ソフト）等ソフトウェア自体のセキュリティ上の欠陥をついて侵入するものはウイルス対策ソフトだけでは防げないことがあります。メーカーの提供する欠陥対処情報に従ってソフトウェアの欠陥をふさぎ常に最新の状態にしておくことが必要です。このほか、不審な電子メールの添付ファイルは安易に開かない、知らないホームページを閲覧するときは、閲覧ソフトのセキュリティ強度を高めて利用する、ファイル交換ソフトを入れたパソコンで重要な情報は扱わないなど、万一のウイルスの脅威に留意した利用を社内に周知徹底することが求められます。

▼ウイルス、不正アクセス、ボット等についての情報
http://www.ipa.go.jp/security/【（独）情報処理推進機構（IPA）セキュリティセンター】

不正アクセス

【不正アクセスは情報漏洩の原因に】

不正アクセスとは、コンピュータへの正規のアクセス権（利用権限）を持たない人が、パスワードを盗んだり、ソフトウェアの不具合などを悪用してアクセス権を取得し、不正にコンピュータを利用、あるいは利用を試みる行為です。

不正アクセスは、目的で分ければ、システムの妨害を狙ったものと、コンピュータ内の情報を盗み出したり、情報を操作することを狙ったものがあります。

システムの妨害を受ければ、システムが使いにくくなったり、場合によってはシステム停止につながります。情報の盗用が目的の場合は、個人情報や機密情報の漏洩・悪用につながります。情報操作が目的の場合は、詐欺などにつながる恐れがあります。

【外からも内からもある不正利用】

不正アクセスの手段は様々です。ソフトウェアのセキュリティ上の欠陥をついて侵入するケース、大量のアクセスを集中させてシステムが混乱している隙に侵入するケース、アクセス用のパスワードを盗んで侵入するケースなどがあります。これらは、外部からのネットワークへの不正アクセスです。しかし、内部関係者による不正な情報持ち出しは、外部からのものよりもはるかに多くなっているのが現実です。

また、悪意を持った情報の持ち出しではなく、家で残業するために持ち出したデータを自宅のパソコンにコピーして使っていたところ、それが不正アクセスによって盗まれてしまったというケースもあります。

▼不正アクセス行為の禁止等に関する法律
http://www.meti.go.jp/policy/netsecurity/fusei_access_law.htm【経済産業省】

不正アクセス　その対応・対策

●外部不正利用対策にはファイアウォール

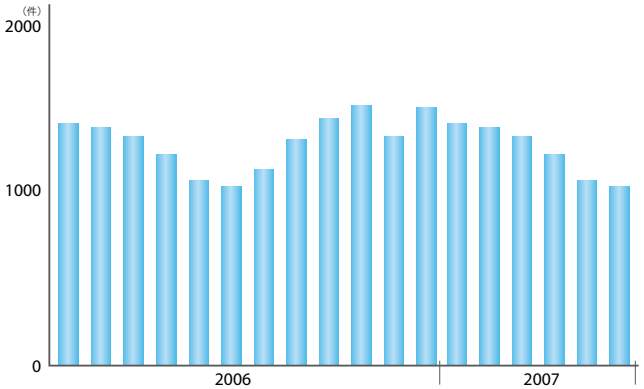
外部からの侵入を防ぐための技術対策としてはファイアウォールの設置が欠かせません。ファイアウォールは、自社のネットワークを守るために、ネットワークの入り口に関門を設けて、許可された通信だけを通す仕組みです。

また、許可された通信を装って不正侵入を試みるものがあるため、これらをチェックする不正侵入検知システムというものもあります。ただし、不正侵入検知システムを適切に運用するためには、それを監視する管理者が必要です。不正アクセスが発生したときに、その足跡を追及できるよう、通信データの記録を残しておくことも必要です。

●内部対策にはアクセス権限の管理を

内部の不正利用対策に関しては、情報セキュリティに関する意識の啓発とともに、組織的な管理と技術を組み合わせた対策が求められます。不正アクセスや不正利用を防ぐうえでの意識啓発の基本は、パスワードの管理を厳格に行うこと、大切な情報は原則的に複写したり持ち出したりしないことです。組織としての管理を進めるには、まず、社内の情報の重要度や機密度を評価したうえで、それぞれの情報に誰がアクセスでき、どのような利用を認めるかを明確に規定します。その規定に基づき、情報の種類ごとに社員のアクセス制御を行うことが必要です。アクセス制御のための各種のシステムが提供されていますので、それを合わせて使うとより有効になります。

グラフ4. 不正アクセス観測件数



出所:情報処理推進機構(IPA)セキュリティセンター

情報の盗み見、改ざん、なりすまし

コンピュータネットワークにおいては、情報の盗み見、情報の改ざん、なりすましなどの脅威にも注意が必要です。

【情報の盗み見で情報が漏洩】

情報の盗み見は、電話の盗聴と同じようなものです。オンラインショッピングの際に、クレジットカード番号や住所などの個人情報を送信する必要があります。このとき、何のセキュリティ対策もしていなければ、ネットワーク上をデータが転送される最中に盗み見をされる危険性が高まります。

また、最近では、データの転送中に盗み見をするのではなく、密かに相手のパソコンにソフトウェア（スパイウェア）を送り込み、相手が知らないうちにパスワードや口座番号といった個人情報などを収集するという手口も登場しています。

【情報が改ざんされては取引が行えない】

コンピュータが扱うデジタルデータは修正が容易な上に修正の痕跡が残らないという特徴を持っています。情報の改ざんは、こうした特徴を悪用した行為です。情報の改ざんを防がなければ、ビジネス上の取引において電子的な文書は信用されなくなってしまいます。

【なりすましによる詐欺事件が発生】

なりすましは、お互いに顔を合わさずにコミュニケーションや取引ができるというネットワークの特徴が悪用される行為です。詐欺の一種ですが、実在の店舗であるかのように装って代金を騙しとる事件も発生しています。金融機関や会員制サービスを装った偽サイトを作り、会員のIDや暗証番号を盗みとるフィッシング詐欺も増えています。なりすましを防がなければ、利用者は安心してネットワークを使えなくなります。

情報の盗み見、改ざん、なりすまし　その対応・対策

暗号技術と運用面での対応が求められる

情報の盗み見、改ざん、なりすましへの対策は、暗号技術の利用と、運用面での対応が求められます。

●暗号化で盗み見を防ぐ

情報の盗み見対策としては、やりとりするデータを暗号化することが基本です。電子商取引で、個人情報などをやりとりするときは、必ず導入すべき技術です。暗号化は利用者側のソフトウェアも対応している必要があります。もし、暗号化に非対応のソフトからの利用も受け付けるのでしたら、盗み見をされる危険がある旨の注意を促すことも運用面では必要でしょう。

●スパイウェアへの対策

また、スパイウェアについては、検知ソフトなどを利用して対策することが必要です。無償で配布されている対策ソフトもあります。ICカードや指紋による生体認証などの技術を使って安全を高める例もあります。

また、特別な技術を使わない方法では、契約者毎に固有の番号表を郵送し、取引のたびに、指定した位置の番号を入力してもらうなど、運用の工夫で対策している例もあります。

●電子署名で改ざんやなりすましを防ぐ

情報の改ざんやなりすましを防ぐには、電子署名という技術を利用するのが有効です。紙の文書の印鑑やサインに該当します。これも暗号技術を応用したものです。これによって、電子文書の発信元や発信者が実在の人物であることが確認され、ファイルの中身が改ざんされていないかどうかも確認できます。

▼電子署名及び認証業務に関する法律
http://www.meti.go.jp/policy/netsecurity/digitalsign.htm【経済産業省】

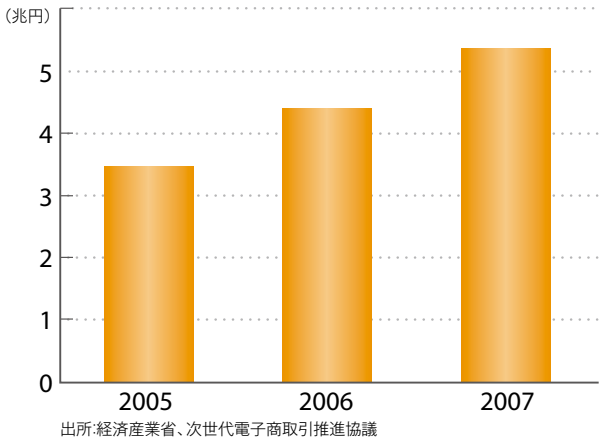
電子商取引における消費者保護

オンラインショッピングへの消費者の不安

消費者向けの電子商取引（オンライン・ショッピング）が広がっています。2007年の電子商取引額は、前年と比べて21.7%増加し、5兆3440億円に達しました。最近では携帯電話から利用できる電子店舗も増えており、今後ますます広がっていくと期待されています。

電子商取引の利用が広がる理由は、時間や場所を制約されないことが、企業にとっても、消費者にとっても利便性が高いからだといえます。しかし、そうした利便性の一方で、消費者が利用しながらも不安を抱えていることも事実です。経済産業省の調査によると、消費者は安全な電子商取引サイト選択の条件として「安全かつ信頼できる代金支払方法が提供されていること」「操作手順がわかりやすいこと」「セキュリティ対策が行われていること」を上位に挙げています。

グラフ5.　5兆円を越えた消費者向け電子商取引



出所:経済産業省、次世代電子商取引推進協議

消費者が安心してショッピングできる取り組みを

企業と消費者では、商品やサービスに関しての情報や、取引に関する習熟度において、大きな格差があります。しかも、コンピュータ画面の上で行われるオンラインショッピングにおいては、実物を見て確かめられないことによる消費者の不安も少なくありません。

こうした消費者の不安を取り除き、安心してショッピングができるようにすることが、消費者向けの電子商取引には欠かせません。そのためには、企業が、消費者の権利利益を尊重した適切な消費者保護の取り組みをすることが求められます。これは、企業の社会的な責任であると同時に、電子商取引の発展にもつながることになります。

インターネットでの買い物の特徴を理解する必要

【消費者の安心に的確な情報提供が欠かせない】

電子商取引における消費者保護を考えるには、消費者向けの電子商取引の特徴と課題を理解することが必要です。

まず、購入の判断をする際、消費者にとって、電子店舗のホームページに掲載された情報だけが買い物の判断材料になります。不適切な商品情報などにより、購入判断に必要な情報が的確に提供されていなければ、消費者は安心して商品購入の判断をすることができなくなります。

【画面上の操作は入力間違いを気づきづらい】

電子商取引の場合、注文の手続は、画面上の操作によって行われます。その際、注文個数を打ち間違えても、気がつかずに注文を送信してしまう事故が少なくありません。インターネットでは一旦送信してしまうと、「ちょっと待って」というわけにはいきません。このため、消費者に想定外の商品が届いてしまうことになります。また、取り消しや返品をするために企業の側も消費者の側も無駄な手間がかかってしまいます。

購入時に個人情報が漏洩することも

消費者は、購入した商品を届けてもらったり、代金を支払うために、住所や氏名、決済方法によってはクレジットカード番号などの個人情報を送信する必要があります。このとき、送信する個人情報が漏洩したり、それが不適切に管理されると、プライバシー侵害などの問題を引き起こす恐れがあります。

また、マーケティングを目的に、消費者に対する電子メールを用いた広告メールもよく使われるようになってきました。企業にとっては、郵便のダイレクト・メールより、手間もコストもかからないことがメリットです。しかしその一方で、必要のない広告メールが多くなってくると、消費者のメール・ボックスが不要な広告メールで埋まってしまったり、メールの受信や検索に時間がかかるという問題が起きてしまいます。

電子商取引に合わせた法令の改定

電子商取引における消費者保護については、まず関連の法律を守ることが最低限のモラルです。もちろん、電子商取引についても、これまでの法令（消費者基本法や消費者契約法、景品表示法など）を守るべきことに変わりはありません。

一方、電子商取引特有の課題に配慮した法律や施行令の改定も行われています。そうした法令を正しく理解して遵守することが求められます。消費者に対する電子商取引は、特定商取引法の「通信販売」として扱われます。また、消費者との契約に関する規定として電子消費者契約法も制定されています。

【消費者に必要な情報の表示義務などを規定】

特定商取引法では、①消費者の購入判断に必要な価格や取引条件などの情報の表示義務、②誇大広告などの消費者に誤認を与える表示の禁止、③受け取りの拒否を通知した消費者への広告メール再送信の禁止、などを規定しています。

▼消費者基本法、消費者契約法
http://www.consumer.go.jp/kankeihourei/index.html【内閣府】

▼不当景品類及び不当表示防止法（景品表示法）
http://www.jftc.go.jp/keihyo/【公正取引委員会】

▼特定商取引に関する法律
http://www.meti.go.jp/policy/economy/consumer/consumer/tokutei/index.html【経済産業省】

広告メールや操作ミスに対する消費者保護の規定

広告メールについては、電子商取引の事業者以外も対象にした、「特定電子メールの送信の適正化等に関する法律」（迷惑メール防止法）も制定されています。内容的には、特定商取引法の施行規則とほぼ同じです。

【注文内容の再確認を義務づけ】

一方、電子消費者契約法では、消費者保護に関して、操作ミスによる契約上のトラブルから消費者を保護するための規定が設けられています。従来の民法では、注文数の間違いなどは消費者の自己責任ということになっていましたが、オンラインでの注文契約については、操作ミスが発生しやすいことから制定されたものです。これによって、電子契約では、消費者が申し込みを行う前に、消費者が申し込み内容を再確認できるような画面構成に事業者がしていなければ、操作ミスによる消費者の申し込みの意思表示は無効になります。

▼迷惑メール防止法関連
http://www.soumu.go.jp/joho_tsusin/d_syohi/m_mail.html#seifu【総務省】

電子商取引における消費者保護　その対応・対策

まずは法令遵守の取り組みを

特定商取引法に書かれている内容は、通信販売をやる上では当たり前のことだと思われるかもしれません。しかし、経済産業省で法律が遵守されているかどうかをモニタリング調査したところ、違反の恐れのある事例が少なくありませんでした。

●表示すべき情報の欠如と誇大広告

たとえば、消費者に対して表示すべき情報のなかでも、返品特約の有無、送料、代表責任者氏名、商品の引渡し時期などの項目が抜けている例が多くあります。また、商品の効能や効果について、裏づけとなる実証データ等の存在が疑わしいものもあります。こうした情報に基づいて商取引を行えば消費者の権利利益を損なう恐れがあります。

●注文申し込み手順の欠落

注文申し込みの段階においても、入力中にリターンキーを押すことで注文が自動的に送信されてしまったり、申込みの最終段階で内容の確認や訂正ができない画面構成になっていたりすると、消費者に混乱を与え、トラブルのもとになります。

●経済産業省などのガイドラインを活用

法律自体には、基本的な考え方が示されているだけですが、経済産業省からは「電子商取引及び情報財取引等に関する準則」が、日本通信販売協会からは「通信販売業における電子商取引のガイドライン」が出されています。これらを参考に、自社の取り組みを定期的にチェックすることが必要です。

▼電子消費者契約法
http://www.meti.go.jp/topic/data/e11011aj.html【経済産業省】

▼電子商取引及び情報財取引等に関する準則
http://www.meti.go.jp/policy/it_policy/ec/index.html#01【経済産業省】

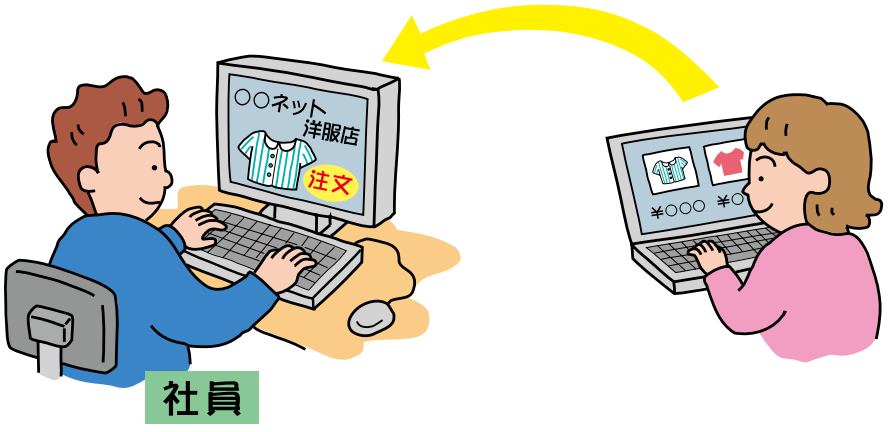
▼通信販売業における電子商取引のガイドライン
http://www.jadma.org/01kyokai/05h2-guideline.html【(社)日本通信販売協会】

消費者の立場に立った情報とサービスの提供を

法令遵守は最小限のモラルです。法令やガイドラインに書かれていることだけをやればいいというわけではありません。商品によっては、まだ法的な規制ができていなかったとしても、消費者の保護と権利尊重という観点から、利用にともなうリスク情報などを、より積極的に開示する姿勢が大切です。

電子商取引は、店頭販売と比べて、実物に触れられないという弱点はあります。しかし、豊かな表現が可能なインターネットの機能を生かせば、限られたスペースの店頭よりも、消費者の求める情報をより効果的に提供できる手段でもあるといえます。

そうした電子店舗ならではの機能を生かし、商品及び取り引きに関する情報の提供や、契約手続などにおいて、消費者の立場に立った画面のつくり方やサービスをすれば、トラブルを防ぐだけにとどまらず、消費者の信頼を高めることにもつながります。



プライバシー侵害、誹謗中傷、名誉毀損

コミュニケーションをめぐる人権侵害

インターネットは自由なコミュニケーションの場、表現活動の場としても、重要な役割を果たしています。電子メール、ホームページ、掲示板、メールマガジン、ブログ、SNS（ソーシャルネットワーキングサービス）※1などが代表例です。企業が顧客を対象にした会員制のホームページで意見交換の場を提供している例もあります。社内においても、電子メール、掲示板、グループウェアなどは、コミュニケーションと情報共有の手段として、なくてはならないものとなっています。

しかし一方では、記載内容や発言をめぐって、プライバシーの侵害や名誉毀損・信用毀損などの人権侵害が問題になる事件も発生しています。なかには、掲載の削除や損害賠償を求める裁判が起こされたケースもあります。

これらのトラブルは、個人間で発生するだけではありません。自社のホームページなどに人権への配慮を欠いた記載があれば、プライバシー侵害や名誉毀損などにつながる恐れがあります。

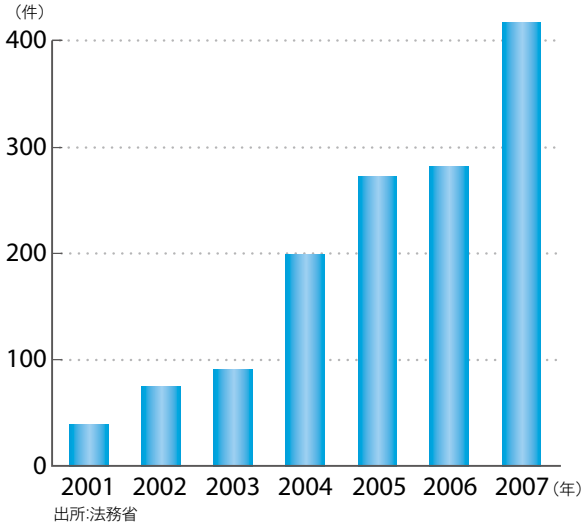
※1　知り合い同士や共通の関心事などを持つ人々のコミュニケーションや交流活動を支援するネットワーク上のサービスのこと。参加の形態は単純な登録制のものから参加者の紹介を必要とするものまで多様である。全国規模で1千万人を越える参加者を集めたサービスもある。最近は、企業内においても社員の情報交流・情報共有の場として利用が広がっている。

企業が誹謗中傷の対象になるケースも少なくない

企業が誹謗中傷の対象になったり、根拠の無いデマを流されたりなど被害に遭うケースも少なくありません。インターネットで銀行破綻の噂が流されたことによって、大量の預金引き出しに見舞われてしまった地方金融機関の例もあります。

企業の管理責任が問われるケースもあります。たとえば、自社で運営している顧客会員向け掲示板サービスの中で、プライバシー侵害や名誉毀損などの行為が行われた場合や、企業が管理している社内ネットワークの中で、セクシャル・ハラスメントなどの人権侵害につながる行為が行われた場合に、会社が人権侵害の事実を知っていながらそれを放置していれば、管理上の責任を問われることもあります。

グラフ6.インターネットにおける人権侵犯事件数の推移



出所:法務省

プライバシー侵害、誹謗中傷、名誉毀損　その対応・対策

噂話のつもりがプライバシー侵害になることも

インターネット上で、プライバシーの侵害や名誉毀損の問題が起きる原因のひとつは、匿名性が悪用される場合です。掲示板サービスなどでは、ニックネームなど匿名で発言できるところが多く、名誉毀損などの事件が発生しても、被害を受けた人が相手を特定できないという問題があります。

また、インターネットという新しいメディアが、どれほどの影響力をもつかを理解しないまま利用することも原因のひとつです。日常の噂話くらいのつもりで記載したものが、プライバシー侵害や名誉毀損など、他人に大きな迷惑をかけてしまうことがあります。

ネットワークの影響力を正しく理解しトラブルを防ぐ

企業の社員が、プライバシー侵害や名誉毀損などの人権侵害を引き起こさないためには、社内の教育と学習を徹底することが必要です。とくに、インターネットでの人権問題に関しては、人権問題の理解を深めるとともに、人権を尊重するうえでの情報の役割の大切さや、インターネットの影響力に対する正しい理解を進めることも必要です。

インターネットで発信された情報が、どのような範囲に、どのような形で伝わっていく可能性があるのかを理解していないと、たとえ本人に悪気はなくても、不用意な情報の掲載や発信によって、思わぬトラブルを引き起こしかねません。

しかし、トラブルを恐れるあまり、情報の発信や、発信すべき情報を押さえるということでは問題の解決にはなりません。表現の自由は最も大切な人権のひとつです。企業は人権を尊重したうえで、お互いの理解を高めるための、開かれたコミュニケーション文化を育てることも大切です。

誹謗中傷には冷静かつ毅然とした対応を

ネットワークのなかで、企業が誹謗中傷などにあった場合の対策も必要です。いわれの無い誹謗中傷を見て見ぬふりをする必要はありませんが、かといって誹謗中傷をしている相手とネットワーク上でやりあうのは賢明ではありません。こうした問題に対しては、組織としての冷静かつ毅然とした対応が求められます。

●内容を分析し、影響を考える

問題が起きた場合、まず、その情報内容の分析と理解を進め、情報がどのような影響をもたらすかといった状況判断を冷静に行います。そのうえで、とるべき対策や措置を検討します。放置すれば、社会への影響が大きいと判断した場合は、記者会見やホームページで社会に向けて事実説明をすることも必要でしょう。

●掲示板もプロバイダー責任制限法の対象

顧客向けの会員サービスで公開掲示板などの運営をしている場合は、プロバイダ責任制限法の対象になります。プロバイダ責任制限法は、掲示板などのなかでプライバシー侵害や名誉毀損などの行為があった場合の、通信事業者や掲示板運営者の賠償責任の範囲と、当該情報の発信者に関する情報開示を請求する権利を規定したものです。

こうした法令の遵守はもちろん、掲示板の運営についてあらかじめ利用規則などを設け、その中で、利用者に対して他者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、適切な運営管理を心がけることがトラブルを防ぐ上で大切です。

▼プロバイダー責任制限法関連情報
http://www.isplaw.jp/【プロバイダ責任制限法対応事業者協議会】

著作権保護

知的財産の尊重が情報社会の発展に欠かせない

インターネットには、世界中から豊富な情報が集まっています。そして、これらの情報は、簡単に複写、編集、加工ができます。

しかし、こうしたネットワークの特徴を利用して、著作権のある楽曲や映画、ソフトウェアなどを、著作者に無断で配布してしまうというような、著作権を侵害する行為も増えています。

また、著作権は市販の著作物だけが対象ではありません。個人が制作したイラストのようなものでも、それが気に入ったからといって、制作者に無断でホームページに使ってしまえば、著作権の侵害にあたります。

こうした著作物や、商標、特許は、知的財産と呼ばれるものです。情報社会においては、こうした知的財産が、企業の活動にも、社会の発展にも、大変に重要な役割を果たしています。

企業は大量のソフトウェアを利用します。もし職場などで違法コピーが行われれば、ソフトウェアを開発する企業の侵害は甚大になります。それだけに、著作権法を守ることは、企業にとって当然の責任だといえます。

公正な利用と著作者の権利を守る著作権法

【著作権法とは】

文化的な創造物である著作物の公正な利用と、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が著作権法です。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、コンピュータのプログラムなどが著作物に該当します。インターネット上にある著作物も、当然、その対象になります。

著作権法では、著作者の権利を保護するために、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。ただし、利用を無制限に禁止しているわけではありません。個人の私的利用における複製や適切な範囲での引用などについては、著作権の制限も設けられています。

【財産権と著作者人格権の２つの側面】

著作権には、財産権としての著作権と、人格権としての著作者人格権との２つの側面があります。財産権の部分は、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得ません。ですから、もし契約によって財産権の譲渡を受けた場合も、著作者人格権への配慮は必要になります。

著作権以外の知的財産権としては、特許権、意匠権、実用新案権、商標権などの工業所有権があり、それぞれ法律によって保護されています。また、営業秘密についても、不正な競争を目的に不正な方法で取得を行えば、不正競争防止法違反として損害賠償など法的な責任を問われます。

著作権保護　その対応･対策

著作物の公正な利用を進める取り組み

●組織としての取り組みと社員の意識向上

企業が著作権の侵害を防ぐためには、組織としての取り組みと、社員一人ひとりの意識の向上を図る必要があります。

まず、会社として「違法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。さらに、ソフトウェアなどの情報資産に関する管理責任者と管理規程を設け、その規程に基づいて違法な利用が発生しないように運用していくことが望まれます。

●許諾を得ることで利用が可能に

著作物はすべてコピーによる利用が禁止されるわけではありません。適正な範囲での引用は認められています。著作者の許諾を得られれば、引用の範囲を越えた利用も可能です。その意味で、ホームページなどで著作物を利用したい場合には、著作者の許諾を得る、著作物の出所を明らかにする、内容を勝手に改変しないなど、公正な利用に関するルールを守るという姿勢を徹底することが大切になります。

▼著作権に関する情報
http://www.bunka.go.jp/chosakuken/【文化庁】

利用者の権利と新しい時代の著作物管理

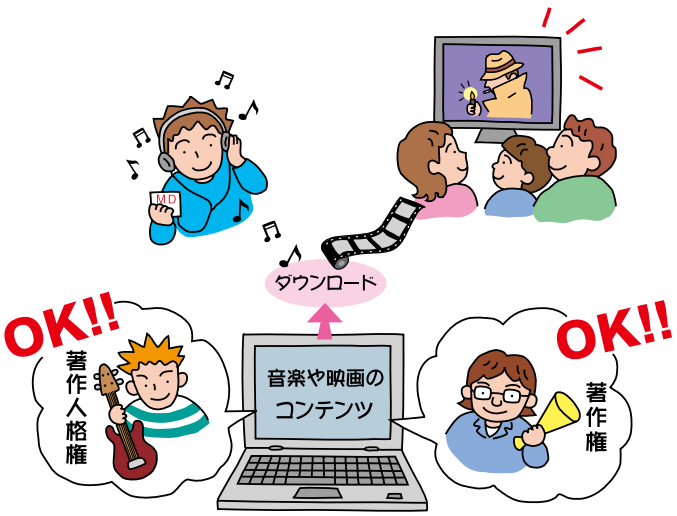
●利用者の権利も大切に

著作者や著作物の流通をビジネスとする企業にとって、著作物を著作権侵害行為からいかに保護するかは死活問題です。それだけに、保護管理のための適切な対策をとる必要があるのは当然です。

しかし、その一方で、著作物には私的利用における複製が認められているように、利用者の権利もあることを忘れてはならないでしょう。著作権の保護対策にあたっては、利用者の利益を極端に損なわないよう、バランスのとれた取り組みが望まれます。

●新しい時代の著作物管理

ソフトウェア開発の分野を中心に、既存の著作権の枠組みで著作物を縛るのではなく、内容の改変なども行えるよう元のプログラムを公開し、共同で利用･開発を進めていくオープン･ソースという取り組みも盛んに行われています。著作物の種類によっては、こうした取り組みのほうが創作活動の発展に有効な場合もあります。著作権保護に対する考え方も時代とともに変化しています。これからは、自社の著作物管理を考える上でも幅広い視野が求められる時代ともいえます。



情報アクセシビリティ

様々な人が企業のホームページを利用している

情報化の進展にともない、人々の生活のなかで情報の果たす役割が、ますます大きくなっています。企業のホームページも、製品やサービスの情報を調べたり、顧客サポートへの問い合わせを行ったりと、様々な用途で使われるようになっています。

こうした利用の広がりとともに、ホームページの利用者は、これまでのようなコンピュータに熟練した人ばかりではなくなってきました。いまでは、子どもや高齢者、何らかの障害を持つ人など、幅広い利用者がホームページを利用しています。また、使用している端末機器や通信速度など、利用環境も様々になっています。

求められる情報アクセシビリティ

【使いづらさが高齢者や障害者の新たな障壁に】

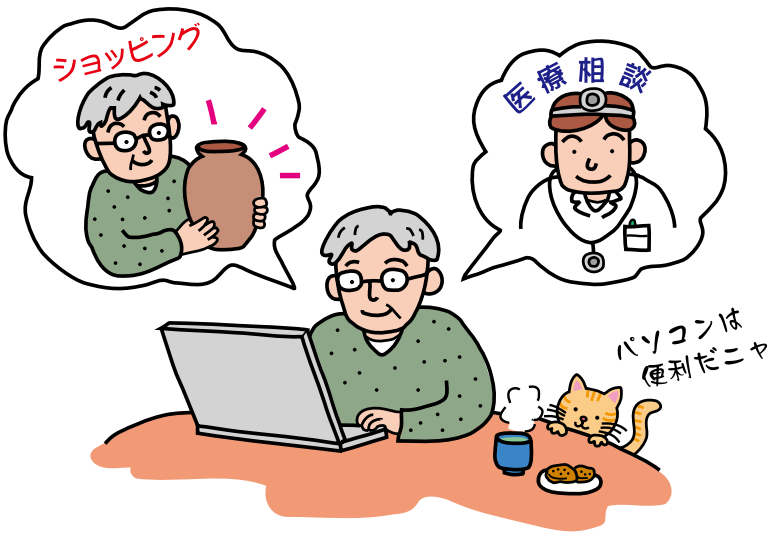
パソコンに不慣れな利用者や、高齢者、障害者が利用することを考えると、多くのホームページは、決して使いやすいものにはなっていないと指摘されています。操作が複雑であったり、小さな文字で説明が書かれていたり、色の違いだけで情報を伝えるようになっていたりすると、コンピュータに不慣れな人や、高齢者、色覚障害のある人などにとっては、内容を把握することが難しく、大変使いづらいものになってしまいます。

オンラインショッピングは、外出が難しい高齢者や障害者にとって、便利な手段になるといわれます。しかし、それが高齢者や障害者に使いづらいものであっては、新たな障壁を生み出してしまうことにもなります。

【情報アクセシビリティとは】

そこで必要になってくるのが、情報アクセシビリティへの配慮です。情報アクセシビリティとは、情報へのアクセスの容易さという意味です。誰でもが公平に、必要な情報へ迷うことなくアクセスできる環境をつくる必要があるということです。

企業がすべての人を尊重して事業を行っていくためには、IT（情報技術）を利用した情報やサービスの提供にあたっても、情報のアクセシビリティに配慮し、誰でもが使いやすい情報やサービスの提供と運営を心がけていくことが望まれます。



情報アクセシビリティ　その対応・対策

広がるユニバーサルデザインの考え方

アクセシビリティに配慮した取り組みとしては、ユニバーサルデザインという考え方が広がっています。

●誰にでも使いやすいものをはじめから設計する

ユニバーサルデザインというのは、誰にでも使いやすいものを、はじめから設計して作ろうという考え方です。高齢者や障害者用のものをわざわざ別に用意しようというのとは違います。それは、特別扱いをしないで、公平に対応するということでもあります。別々のものをつくるより、はじめから誰にでも使えるものをつくったほうが社会的なコストの無駄を小さくすることにつながります。オンラインショッピングのホームページなどのアクセシビリティを考えるうえでも参考になります。

●ユニバーサルデザイン７原則

ユニバーサルデザインの７原則というのは以下のようなものです。対顧客サービスだけでなく、社員が利用するシステムについても、こうした観点から見直してみることが必要です。

1. 誰にでも公平に利用できること
2. 使う上での自由度が高いこと
3. 使い方が簡単ですぐわかること
4. 必要な情報がすぐに理解できること
5. うっかりミスや危険につながりにくいこと
6. 無理な姿勢をとることなく、少ない力でも楽に使用できること
7. 使いやすい広さと大きさを確保すること

人に優しいホームページを

●ウェブアクセシビリティのガイドライン

ホームページ上の情報内容を企画・提供するときに、高齢者や障害者などへの情報アクセシビリティを確保するためのガイドラインも策定されています。

そのひとつが、経済産業省が JIS 規格として策定した「高齢者・障害者等配慮設計指針※1」です。この規格では、①企画・制作にあたって、可能な限り高齢者・障害者が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を、基本方針として求めています。また、ホームページの標準化についても「ウェブコンテンツアクセシビリティ指針※2」が出されていますので、こちらも参考になります。

●必要な説明を分かりやすく提供する

情報アクセシビリティに求められるものは、機能的な使いやすさだけではありません。商品について調べようとしたときに、取り扱い上の注意などの情報が載っていない、説明が難解すぎて分からない、といったことが無いよう、必要な説明を分かりやすく提供することが重要です。

情報アクセシビリティを高めるためには、ユニバーサルデザインの考え方や公表されているガイドラインなどを参考に、企業としてのガイドラインを決めるとともに、情報アクセシビリティの大切さを、サービスを提供する企画・制作にかかわるすべての担当者に周知徹底していくことが求められます。

※1「高齢者・障害者等配慮設計指針ー情報通信における機器、ソフトウェア及びサービスー第三部：ウェブコンテンツ」

※2 国際コンソーシアムW3C「ウェブ・コンテンツ・アクセシビリティ指針」http://www.w3.org/TR/WCAG20/

▼情報アクセシビリティのJIS規格
http://www.jsa.or.jp/【日本規格協会】
http://www.jisc.go.jp/app/JPS/JPSO0020.html【日本工業標準調査会】（検索ページでX8341-3と入力すると閲覧のみ可能）

監　修　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
http://www.hyper.or.jp/　　moral@hyper.or.jp
2004年10月　発行
2008年11月　改訂