組織幹部のための情報セキュリティ対策

企業や組織にとっての情報セキュリティ対策は、いまや重要な経営課題のひとつであり、組織幹部自らが率先して指揮を取らなければなりません。

ここでは、組織幹部のための情報セキュリティ対策として、最初に行うべき情報セキュリティポリシーを中心に説明します。

※特に重要な項目には マークがついています。

情報セキュリティ対策の必要性

重要!

企業や組織のＩＴ化の促進に伴い、「保有する情報資産を有効に活用できること」がＩＴ社会におけるひとつのキーワードになりました。そして、組織内においてデータを共有するだけでなく、インターネットを利用して情報を提供したり収集したりすることが一般的になるにつれて、より高密度な情報がより高速にやり取りされるようになってきています。

しかし、現在の企業や組織は、ＩＴへの依存による利便性の向上と引き換えに、大きな危険性を抱え持つことになってしまいました。いまや、企業や組織にとって、情報セキュリティに対するリスクマネジメントは重要な経営課題のひとつと考えなければなりません。特に、個人情報や顧客情報を取り扱う場合には、これを保護するということが、企業や組織にとっては社会的責務でもあるという点にも注意しなければなりません。

ここで大切なことは、このような情報セキュリティ対策は画一的なものではなく、企業や組織の持つ情報や組織の規模、体制によって、大きく異なるという点にあります。つまり、業務形態、ネットワークやシステムの構成、保有する情報資産などを踏まえた上で、その内容に見合った情報セキュリティの対策を立てなければなりません。

なお、今日、情報セキュリティ対策は、世界的にも重要な経営課題であると認識されており、情報セキュリティ製品・システム評価基準（ISO/IEC15408）や情報セキュリティマネジメントシステムの認証基準（ISO/IEC27001）が、国際標準として規格化されています。情報セキュリティ対策の重要度が高まるにつれて、日本国内においても、これらの国際基準を採用する企業が増えてきています。

ここで企業における情報セキュリティに係る主要なトラブルとその影響を紹介しておきます。

■機密情報の漏洩

社内のネットワークやコンピュータから機密情報が持ち出された場合には、悪意のある者に情報が渡ったり、インターネットで公開されてしまったりする危険性があります。また、社内のコンピュータのウイルス感染により、機密情報が漏洩することもあります。

「企業・組織」の情報セキュリティ対策：組織幹部

■個人情報の流出

保有する個人情報が流出してしまうと、賠償問題、訴訟問題にまで発展することがあります。また、企業イメージや信頼性を大きく損なうため、顧客が離れてしまう可能性があります。

■ホームページの改ざん

企業の顔とも言えるホームページが改ざんされるということは、企業イメージの損失になります。さらに、ホームページにウイルスを埋め込まれてしまった場合には、閲覧者のコンピュータにウイルスを感染させてしまうこともあります。

これらのことは、会社としての情報セキュリティ対策が不足しているということを露呈することにもなり、取引会社からの信頼を失い、取引停止につながるかもしれません。

■システムの停止

社内の基幹システムが停止してしまうと、最悪の場合、業務が完全に停止してしまうことも考えられます。また、インターネットのショッピングサイトが停止してしまうと、販売機会を失うことになり、場合によっては顧客が競合会社のショッピングサイトに移動してしまうかもしれません。

■ウイルスへの感染

現在のウイルス感染は、既に感染したコンピュータだけの問題ではなくなっています。ウイルスの中には、そのコンピュータに登録されているメールアドレスを使って一斉にウイルス自身を複製してばらまいたり、ネットワーク上の他のコンピュータにウイルスを感染させるものがあります。

最近では、コンピュータに保存されている文書を自動的に電子メールで送信するウイルス、インターネットにコンピュータのパスワードを自動的に発信するウイルス、外部からの不正侵入を手助けするウイルスなど、情報セキュリティに大きく関わるウイルスも登場してきています。

企業や組織の幹部には、こういった情報セキュリティに係るリスクを可能な限り軽減するために、強固な情報セキュリティ対策が要求されているということへの認識と理解が必要です。

情報資産の維持管理

情報資産を維持管理するためには、情報資産を「機密性」、「完全性」、「可用性」に係る脅威から保護することが必要となります。

機密性（Confidentiality）

許可された者だけが情報にアクセスできるようにすること

機密性が維持できていないと　→　**不正アクセス、機密漏洩**

完全性（Integrity）

情報が正確かつ完全であること

完全性が維持できていないと　→　**データの改ざん**

可用性（Availability）

許可された者が必要なときにいつでも情報にアクセスできるようにすること

可用性が維持できていないと　→　**サービス停止**

●機密性は、コンピュータやシステム、データベースなどにアクセスできるユーザーを制限することを意味しています。許可されていないユーザーは、情報やシステムにアクセスすることができないようにしたり、データを閲覧することはできるが書き換えることはできないようにしたりします。このことは、不正アクセスや情報漏洩に対する防御につながります。

●完全性は、許可されていない者によって情報が改ざんされたり、破壊されたりしないことを指します。

●可用性は、正規のユーザーが情報を利用しようとしたときには、いつでも情報にアクセスすることができることを意味しています。つまり、可用性を維持するということは、情報を提供するサービスが常に動作するということを表します。

これらに対する脅威から情報資産を維持管理するということが、情報セキュリティ対策に要求される行為になります。そして、企業や組織の保有する情報資産の特質をよく検討して、機密性、完全性、可用性のバランスを考慮することが大切です。

必要な情報セキュリティ対策

組織や企業で発生する可能性のあるトラブルとそれぞれの情報セキュリティ対策には、主に以下のものがあります。

ウイルス感染

対策
- ウイルス対策ソフトの導入
- OSのアップデート
- Webブラウザのセキュリティ設定
- 電子メールソフトのセキュリティ設定

災害などによる機器障害

対策
- バックアップ
- 無停電電源装置の設置
- 設備の安全管理

不正侵入

対策
- パスワード管理
- ファイアウォールの導入
- 不正侵入検知システムの導入
- OSのアップデート
- ソフトウェアのアップデート

情報漏洩

対策
- ファイアウォールの導入
- 顧客データなどの管理
- 資料の廃棄ルールの徹底
- メディア、機器の廃棄ルールの徹底
- 無線LANのセキュリティ設定
- ユーザー権限の管理
- パスワード管理

この図からもわかるように、組織や企業を脅かす情報セキュリティの危険性にはさまざまなものがあります。これらの情報セキュリティに対する多様なリスクから情報資産を防御するためには、組織内における情報セキュリティ対策の方針と規則を整理して、すべての社員、職員に対するセキュリティ意識の向上を促さなければなりません。このような規定化された情報セキュリティ対策の方針や行動指針を情報セキュリティポリシーと言います。

情報セキュリティポリシーの概要と目的

重要!

情報セキュリティポリシーとは、企業や組織において実施する情報セキュリティ対策の方針や行動指針のことです。情報セキュリティポリシーには、社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、ならびに情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するのが一般的です。

この情報セキュリティポリシーを作成する目的は、企業の情報資産を情報セキュリティの脅威から守ることですが、その導入や運用を通して社員や職員の情報セキュリティに対する意識の向上や、顧客に対する信頼性の向上といった副次的なメリットを得ることもできます。

情報セキュリティポリシーを整備する上で大切なことは、情報セキュリティ担当者だけがネットワークやコンピュータなどに対する情報セキュリティ対策を心がければよいというものではないという点です。情報資産を共有するすべての社員や職員が適切な情報セキュリティ意識を持たなければ、ウイルス、情報漏洩などから防御することは困難です。

情報セキュリティポリシーを導入することで、主に以下のような効果が考えられます。

- 組織内の情報資産が明らかになり、効果的なセキュリティ対策が可能になる。
- 社員や職員の情報セキュリティに対する意識が向上する。
- 取引先や顧客、株主などに対する企業や組織としての信頼性が向上する。

トップダウンによる周知・徹底

情報セキュリティに対する防御は、保有する情報資産を防御するために重要なことですが、その行為自体は利益を生み出すものではないことから、放っておくとせっかく策定した情報セキュリティポリシーが形骸化してしまうことになってしまいます。情報セキュリティポリシーを「絵に描いた餅」にしないためには、企業や組織の幹部が、トップダウンで情報セキュリティポリシーを全社員に周知徹底することが大切です。

特に、情報セキュリティポリシーを策定する際に企業や組織の幹部は、以下のことに注意しなければなりません。

- 「情報セキュリティは会社の経営課題のひとつに捉えなければならない重要な事柄であること」という認識を深める。
- 情報セキュリティポリシーを策定して運用するためには、多大な時間とコストが掛かること。
- 規定を社員に遵守させるためには、罰則規定も必要となること。

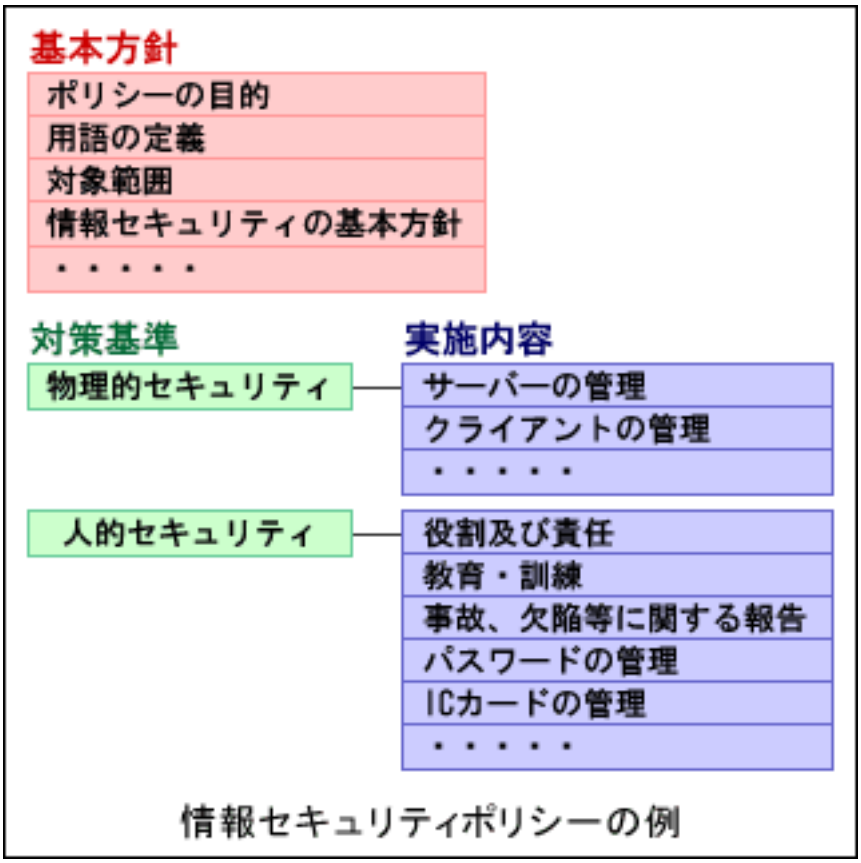
情報セキュリティポリシーの内容

情報セキュリティポリシーでは、「基本方針」、「対策基準」、「実施内容」の 3 つの階層で構成されることが一般的です。

基本方針には、組織や企業の代表者による「なぜ情報セキュリティが必要であるのか」や「どのような方針で情報セキュリティを考えるのか」、「顧客情報はどのような方針で取り扱うのか」といった宣言が含まれます。

対策基準には、実際に情報セキュリティ対策の指針を記述します。
多くの場合、対策基準にはどのような対策を行うのかという一般的な規定のみを記述します。

実施内容には、それぞれの対策基準ごとに、実施すべき情報セキュリティ対策の内容を具体的に記載します。



情報セキュリティポリシーの例

情報セキュリティポリシーの策定

情報セキュリティポリシーを策定する場合にもっとも大切なことは、担当者、体制、手順をあらかじめ検討しておくということです。また、情報セキュリティポリシーは、企業や組織の代表者が施行するものであるため、可能な限り、代表者や幹部が策定の作業自体にも関わるような体制を作ることが重要です。

■策定の体制作り

企業や組織の実情や現在の社会状況に見合った情報セキュリティポリシーを策定するためには、適切な人材を確保する必要があります。また、情報セキュリティポリシーの品質を高めるためには、外部のコンサルタントや法律の専門家に参加を依頼することも検討するとよいでしょう。

ただし、外部のコンサルタントに依頼する場合には、できるだけアドバイザの形で協力してもらうことが理想的です。これは、社内の人材によって情報セキュリティポリシーを策定しなければ、その企業や組織に適した内容にすることが困難であるためです。また、情報セキュリティポリシーを策定するという行為そのものが、情報資産の確認と情報セキュリティの意識向上に非常に役立ちます。

■策定の手順

情報セキュリティポリシーの策定手順は、業態、組織規模、目的、予算、期間などによって大きく異なります。ここでは、代表的な策定手順を紹介します。

1. 策定の組織決定（責任者、担当者の選出）
2. 目的、情報資産の対象範囲、期間、役割分担などの決定
3. 策定スケジュールの決定
4. 基本方針の策定
5. 情報資産の洗い出し、リスク分析とその対策
6. 対策基準と実施内容の策定

■策定時の留意事項

効果的な情報セキュリティポリシーを策定するには、以下の点に留意する必要があります。

- 情報資産を明確にする。
- 対象者の範囲を明確にする。
- できる限り具体的に記述する。
- 社内の状況を踏まえて、実現可能な内容にする。
- 運用や維持体制を考えながら策定する。
- 形骸化を避けるために、違反時の罰則を明記する。

個人情報取扱事業者の責務

重要!

個人情報保護法は、個人の権利と利益を保護するために、2005 年 4 月から全面施行された法律で、個人情報を保有する事業者が遵守すべき義務等を定めた法律です。

「個人情報取扱事業者」とは、個人情報保護法第 2 条第 3 項において、「個人情報データベース等を事業の用に供している者」と定義されています。また、「個人情報」とは、生存する個人に関する情報のことで、氏名、生年月日などのデータによって特定の個人を識別できる情報を指しています。なお、保有する個人情報の合計件数が 5,000 件を超えない小規模事業者については、個人情報取扱事業者から除外されています。

個人情報保護法では、個人情報取扱事業者に対し、以下のことを義務付けています。

●個人情報を取り扱うに当たっては利用目的をできる限り特定し、原則として利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない。
●個人情報を取得する場合には、利用目的を通知・公表しなければならない。なお、本人から直接書面で個人情報を取得する場合には、あらかじめ本人に利用目的を明示しなければならない。
●個人データを安全に管理し、従業員や委託先も監督しなければならない。
●あらかじめ本人の同意を得ずに第三者に個人データを提供してはならない。
●事業者の保有する個人データに関し、本人からの求めがあった場合には、その開示を行わなければならない。
●事業者が保有する個人データの内容が事実でないという理由で本人から個人データの訂正や削除を求められた場合、訂正や削除に応じなければならない。
●個人情報の取扱いに関する苦情を、適切かつ迅速に処理しなければならない。

なお、主務大臣は、個人情報取扱事業者に対し、個人情報の取扱に関し報告させることができ、また、個人情報取扱事業者が上記の義務に違反している場合などには、当該事業者に対し、必要な措置をとるべきことを命じることができます。主務大臣の命令に違反した場合や、報告義務に違反した場合には、以下の罰則が科せられます。

●主務大臣の命令に違反した場合　6ヶ月以下の懲役　又は　30 万円以下の罰金
●報告義務に違反した場合　30 万円以下の罰金