組織幹部のための情報セキュリティ対策－実践編

企業や組織における情報セキュリティ対策は、情報セキュリティポリシーを策定したところから始まると言えます。ここでは、策定した情報セキュリティポリシーを元に、組織幹部が実践すべき情報セキュリティ対策について説明します。

※特に重要な項目には マークがついています。

情報セキュリティポリシーの実施サイクル

重要!

情報セキュリティポリシーは、文書化して策定するだけではあまり効果がありません。以下のような実施サイクルによって、情報セキュリティポリシーを発展させていくことを検討してください。

策定

情報資産の洗い出しを行い、組織や企業の状況に合った情報セキュリティポリシーを策定する。

導入

情報セキュリティポリシーを全社員、全職員に配布する。必要に応じて、集合研修などの教育を行う。

運用

情報セキュリティポリシーに則って行動することで、目的とする情報セキュリティレベルを維持することができる。

評価

導入後の現場の状況や問題点、社会的な状況などを踏まえて、定期的に情報セキュリティポリシー自体を評価する。また、遵守されているかどうかのチェックも必要である。

見直し

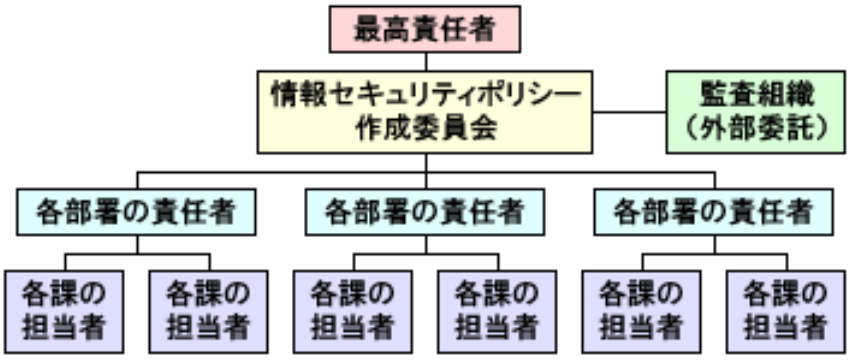
評価の内容を参考にして、情報セキュリティポリシーの見直しを行う。

情報セキュリティポリシーは、企業や組織の状況、新たな脅威、新しい法律の施行など社会的な状況により、定期的に見直さなければなりません。そのためにも、このようなサイクルに基づいて実施することで、情報セキュリティポリシーを常に適切なものにしておくことが大切です。この実施サイクルによって、実情に合った情報セキュリティポリシーを導入することが、すべての社員や職員に遵守させることの第一歩になります。

情報セキュリティポリシー担当の組織化

情報セキュリティポリシーを策定するには、まず責任者を明確にして、情報セキュリティポリシー策定に携わる人材を明確に組織化することが必要になります。企業や組織の規模や代表者の考え方などによって、その組織の作り方には多くのやり方があります。この組織の活動内容が情報セキュリティポリシー策定の成果に大きく影響するため、できる限り、予算や人材などの組織内のリソースが活用できるような方法で、担当者を組織化しなければなりません。

ここでは、主な情報セキュリティポリシー策定の 3 つの組織化案を掲示しておきます。いずれの場合にも、組織幹部も主要メンバーとして参加することが大切です。



組織化の例

■委員会を組織する

各部署から適任者を集めて、情報セキュリティポリシー策定委員会を組織する方法です。情報セキュリティポリシーの策定時に、各部署の意見を反映しやすく、導入時にもすべての部署に伝達しやすくなるという大きなメリットはありますが、通常業務を行いながら参加する場合には、どうしても委員会の業務が後回しになってしまいがちです。そのため、委員会を組織する場合には、情報セキュリティポリシーの策定が完了するまで、一定期間情報セキュリティポリシーの業務に専任させるという方法も検討すべきかもしれません。

■既存部門が担当する

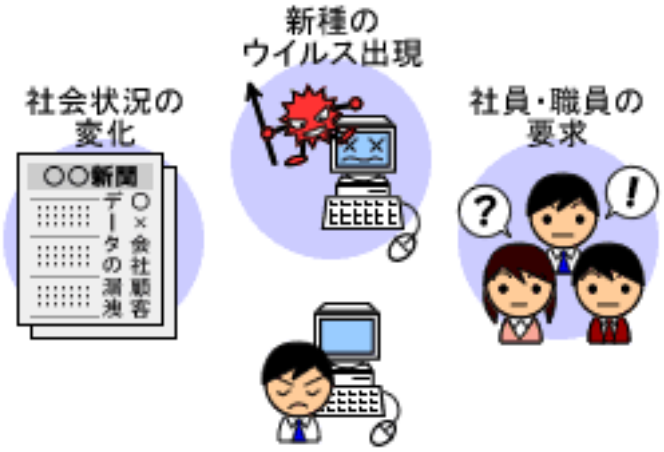
情報システム部などの既存部門の一部のスタッフが担当する方法です。この方法は、いわば組織内における IT の専門家が参加できるというメリットはありますが、既存部門の人材を補充しない限り、本来のシステムやネットワークの管理業務がおろそかになってしまう危険性もあります。

■新規部門を設立する

新たに情報セキュリティ部門といった専門部隊を設立する方法も考えられます。もっとも理想的な組織と言えますが、情報セキュリティ対策に多くのリソースを割り当てることができる大企業に限られるかもしれません。

情報セキュリティポリシーの評価と見直し

情報セキュリティポリシーは、運用を開始した後にも、社員、職員の要求や社会状況の変化、新たな脅威の発生などに応じて、定期的な見直しが必要です。また、見直しを行った結果、必要に応じて情報セキュリティポリシーを改定しなければなりません。この作業を繰り返すことが、情報セキュリティ対策の向上に役立ちます。



■情報収集、評価、監査、リスク分析

●コンピュータの情報セキュリティ対策は、常に変化しているものです。そのため、常に最新の情報セキュリティ関連の情報を収集する体制が必要です。そして、収集した情報を参考にして、現在の情報セキュリティポリシーの内容に不足している項目がないかどうかを評価します。

●定期的に社員、職員へのヒアリングを行い、情報セキュリティポリシーが適切に守られているか、有効に機能しているかなどについての調査を行い、その結果を評価という形で整理します。

●ホームページで個人情報を収集していたり、顧客情報を取り扱っていたりする場合には、できる限り、社外のコンサルタントに監査を依頼するようにすべきです。

●新たな脅威や社会状況の変化に伴い、変動するリスクの分析と対応方法の考察を行います。

■見直しと改訂

評価、監査、調査の結果、社員や職員からの要求に基づいて、情報セキュリティポリシーの見直しと改訂を行います。改定した情報セキュリティポリシーは、再び導入のプロセスを経て、運用サイクルに乗せていきます。

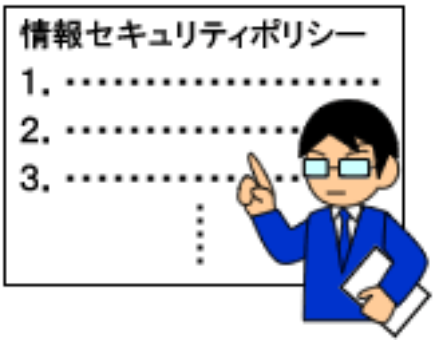
情報セキュリティポリシーの監査

情報セキュリティポリシーに則して、定期的に監査を行うことで、情報セキュリティが適切に守られていることを確認しなければなりません。情報セキュリティポリシーの監査では、主に以下の内容をチェックします。

●情報セキュリティポリシーが社員、職員に正しく遵守されているか？
●情報セキュリティポリシーが現場の状況に適合しているか？
●最新の法律や情報セキュリティの状況を踏まえ、情報セキュリティポリシーに不備、不足はないか？

ここで注意しなければならないことは、「情報セキュリティポリシーは守ってますか？」といった形だけの社員、職員への確認は、無意味なものになることが多いという点にあります。そのため、外部のコンサルタントに依頼して、客観的に判定してもらうことも効果的です。コストの問題などで、定期的に外部に委託することが困難な場合でも、チェック項目の内容をコンサルタントに依頼したり、チェックそのものはできる限り別の人間がチェックを担当するなど、しっかりとした監査手法を採用することが大切です。

特に、最近はホームページで収集した個人情報が漏洩したり、組織内のデータベースの顧客情報が流出したりといったケースが非常に増えてきています。やはり、個人情報や顧客情報を保管している場合には、常に情報漏洩の危険性があるということを念頭において、できる限り監査を外部のコンサルタントなどに依頼することを検討しましょう。



事故やトラブル発生時の対応

情報セキュリティに関わる事故やトラブルが発生した場合には、情報セキュリティポリシーに記載されている対応方法に則して、適切かつ迅速な処理を行うことこそが、損失を最小限に抑える最大の対策です。

事故やトラブルが発生した場合には、以下の手順で対応します。なお、ここでは、ネットワークへの不正侵入を例として取り上げることにします。

（1）事故の検知

定期的なログチェックや障害検知ツールの利用によって、不審な状況の発生を検知する。

（2）事故の初動処理

関連する部署や担当者へ連絡を行い、あらかじめ設定した優先順位によって手続きを行う。情報が漏洩しているなどの危険があれば、この段階でホームページを閉鎖する、データをインターネットから接続されていないコンピュータに退避するなどの処置が必要である。なお、ユーザーに被害が及ぶ可能性がある場合には、速やかにユーザーに連絡を行う。

（3）事故の分析

被害内容や事故の規模を整理して、事故が発生した原因を分析し、対応策を決定する。

（4）復旧作業

システムを復旧して、正常に動作していることを確認する。復旧が完了したら、関係者やユーザーへの連絡を行う。

（5）再発防止策の実施

原因を究明して、同様の事故が再発しないように対策を講じる。事故に対する処理や対策で必要な項目については、情報セキュリティポリシーに反映する。

組織幹部として、これらの一連の処理の中でもっとも重要なことは、常に状況を判断できるような情報伝達ルールを確立しておくことです。過去に発生した情報漏洩事件などでは、組織幹部への情報伝達が遅れたり、正確な情報が伝わらなかったりしたために、もっとも大切な初動処理にミスが発生して、その結果、事故の被害をさらに拡大させてしまっているケースが数多く見受けられます。

これらの情報セキュリティに関する事故の事例を参考にして、適切な対応が可能な情報伝達や対応方法の規則を情報セキュリティポリシーに組み込んでおくことで、情報セキュリティ対策をさらに万全なものにすることができます。

情報セキュリティ教育の実施

重要!

策定した情報セキュリティポリシーに関しては、組織幹部も含め全社員、職員に情報セキュリティ教育を実施して、遵守することを徹底しなければなりません。

単に、分厚い書類を渡したり、形だけの方針や指針を伝えるだけでは、社員、職員に情報セキュリティポリシーに則って行動してもらうことは困難です。

そのため、同意書にサインしてもらう、違反時の規定を設けるなどの方法で、情報セキュリティポリシーの運用を意識させる仕組みが必要です。また、情報セキュリティ診断システムなどを利用して、導入した成果や情報セキュリティポリシーの浸透具合をチェックするというのも効果的です。

いずれにしても、すべての社員や職員が遵守するからこそ、情報セキュリティポリシーに意味があり、たったひとりの人間によるずさんな管理が情報セキュリティに対するリスクを招いてしまうという意識が大切です。そして、そのような情報セキュリティに対する意識を正しく啓発することが、企業や組織における大切な情報セキュリティ対策のひとつなのです。

不正アクセス防止対策促進に関する優遇措置

法人または個人事業者における不正アクセス対策に対して、以下のような税制支援を行っています。

■情報基盤強化税制

対象：

国税（所得税、法人税）

適用期間：

平成18年4月1日から平成20年3月31日までの取得等（2年間）

対象とする設備：

ISO/IEC15408に基づき評価･認証を受けた

1）サーバー用オペレーティングシステム又はこれがインストールされたサーバー

2）データベース管理ソフトウェア又はその機能を利用するアプリケーション

3）ファイアウォール（ 1）又は 2）と同時に設置する場合に限る）

■ネットワークセキュリティ維持税制

対象：

地方税（固定資産税）

適用期間：

平成18年4月1日から平成20年3月31日まで（2年間）

対象とする設備：

ネットワークセキュリティ維持装置（対象の情報システムについて、情報通信ネットワークにおけるセキュリティ脅威から情報システムを防護するために必要な電気通信設備）であって、取得価格250万円以上のもの。