経営相談 Q&A

「中小企業の情報セキュリティ対策ガイドライン」のポイント

Q

中小企業の当社業務は顧客の情報を扱うことが少なく、これまで情報セキュリティについては安易に考えていました。しかし、最近メディア等で情報漏洩やサイバー攻撃に関する話題が大きく取り上げられていることから、何らかの対策を講じる必要性を感じています。ただ、何から手をつけたらよいかわかりません。何か参考となる資料はないでしょうか。

A

独立行政法人情報処理推進機構（IPA）(※)が公表している「中小企業の情報セキュリティ対策ガイドライン」を活用するとよいでしょう。

中小企業における IT の利活用が進む一方で、新たな脅威も発現し、事業に悪影響を及ぼすリスクも高まっています。また、個人情報保護法の改正等に伴い情報セキュリティに対する社会的要請、法的責任が拡大し、情報セキュリティへの取り組みは優先課題となっています。そこで、IPA では「中小企業の情報セキュリティ普及に関する委員会　ガイドライン検討ワーキンググループ」を開催し、有識者の意見を踏まえ、2009 年に「中小企業の情報セキュリティ対策ガイドライン」を策定し、2017 年 5 月 10 日に最新の改訂版を公開しています。

（※）日本における IT 国家戦略を技術面、人材面から支えるため 2004 年に設立された、経済産業省所管の独立行政法人。

本編第 1 部の「経営者編」では、情報セキュリティ対策に関して、経営者が認識し、自らの責任で対応しなければならない事項について説明しています。第 2 部の「管理実践編」では、情報資産や情報システムなどの管理を実践される方（管理者層）を対象として、中小企業において情報セキュリティポリシーを策定し、これをもとに対策を実践していくための手順について説明しています。

さらに、企業や個人などに最低限求められる「情報セキュリティ 5 か条」のほか 25 の診断項目に答えることで自社の対策状況が把握できる「5 分でできる！情報セキュリティ自社診断」、自社のセキュリティポリシーを策定する際にすぐに使えるひな形や情報資産管理台帳のサンプルが付けられた「わが社の情報セキュリティポリシー」が付録として用意されています。

■「情報セキュリティ 5 か条」

企業の規模に関わらず、必ず実行したい重要な対策が 5 か条にまとめられています。

1．OS やソフトウエアは常に最新の状態にしよう！

OS やソフトウエアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いの OS やソフトウエアに修正プログラムを適用する、もしくは最新版を利用しましょう。

＜対策例＞
- Windows Update（Windows OS の場合）/ソフトウエア・アップデート（Mac OS の場合）
- Adobe Flash Player/Adobe Reader/Java 実行環境（JRE）など利用中のソフトウエアを最新版にする

2．ウイルス対策ソフトを導入しよう！

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）は常に最新の状態になるようにしましょう。

＜対策例＞
- ウイルス定義ファイルが自動更新されるよう設定する
- 統合型のセキュリティ対策ソフト（ファイヤーウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト）の導入を検討する

3．パスワードを強化しよう！

パスワードが推測や解析されたり、ウェブサービスから窃取したID・パスワードが流用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。

＜対策例＞
- パスワードは英数字記号含めて10文字以上にする
- 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
- 同じID・パスワードをいろいろなウェブサービスで使い回さない

4．共有設定を見直そう！

データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため無関係な人に情報を覗き見られるトラブルが増えています。クラウドサービスや機器は必要な人にのみ共有されるよう設定しましょう。

＜対策例＞
- クラウドサービスの共有範囲を限定する
- ネットワーク接続の複合機やカメラ、ハードディスク（NAS）などの共有範囲を限定する
- 従業員の異動や退職時に設定の変更（削除）漏れがないように注意する

5．脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付きのメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとしたりする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

＜対策例＞
- IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る
- 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する

■5分でできる！情報セキュリティ自社診断

25項目の設問に答えるだけで自社のセキュリティレベルを把握できる「自社診断シート」と、その解説、情報セキュリティ対策を従業員に会社のルールとして周知する時に活用できる情報セキュリティハンドブックのひな形で構成されています。自己診断シートは、あまり費用をかけることなく実行することで効果がある情報セキュリティ対策が25項目に絞り込まれています。

取り返しのつかないことになる前に、自社のセキュリティ状況を診断シートでチェックしましょう。

■わが社の情報セキュリティポリシー

情報セキュリティは、ひな形をそのまま使ってもうまく機能しません。自社に適した情報セキュリティ対策を行うには、まずは企業が活動を行う際に直面する情報セキュリティ関連のリスクを確認する。そして、組織として実行すべき情報セキュリティ対策を組織の正式な規則として情報セキュリティポリシーを定め、これに基づいて従業員が行動することでリスクを現実的に問題のないレベルまで封じ込める必要があります。

用意されているひな形を活用して自社の情報セキュリティポリシーを策定してみましょう。

本ガイドラインはIPAのホームページ上に無料で公開されていますので、必要に応じてダウンロードして活用してください。　（丸尾尚史）

https://www.ipa.go.jp/security/keihatsu/sme/guideline/