経営相談 Q&A

中小企業における情報セキュリティ向上のポイント

Q 当社は大手企業の下請けをメインとする従業員 50 名の製造業です。昨今、情報セキュリティの向上に関して取引先からの対応圧力が高まっています。とはいえ、当社としても対応できるリソースに限りがあることから、どのように優先順位をつけて取り組むべきか、教えていただけますか。

A 近年、サイバー攻撃は高度化し、企業のバリューチェーンにおいてセキュリティの脆弱な下請け企業から情報を盗み出すなど、手口はより巧妙になっています。

そこで、中小企業が情報セキュリティを向上させる上で取り組むべきステップをわかりやすくまとめた「中小企業の情報セキュリティ対策ガイドライン」（以下、「ガイドライン」）を下敷きとして、中小企業の経営者と実務担当者、それぞれが取り組むべきポイントについてご紹介します。

■「ガイドライン」の目的・概要

「ガイドライン」は、中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したもので、（独）情報処理推進機構（IPA）が現在第 3 版を発行しています。

本編 2 部と付録から構成され、経営者から担当者まで幅広く使える知識が掲載されています。

■経営者が認識し取り組むべきこと

（1）対策を怠ることで企業が被る不利益

まず、経営者は情報セキュリティ対策を怠ることによって、①金銭の損失、②顧客の喪失、③業務の停滞、④従業員への影響などのリスクが生じることを認識する必要があります。

また、適切な措置を怠った場合には、経営者自身が法的責任を問われるケースや、関係者や社会に対して責任を負わねばならないケースも発生することがあります。

（2）「3 つの原則」と「重要 7 項目の取組」

経営者はこうしたリスクを踏まえたうえで、自らリーダーシップを発揮して情報セキュリティ対策を進める、委託先の対策まで考慮する、関係者と常にコミュニケーションを取る、の 3 原則を認識し、対策をとる必要があります（図表 1 ）。

図表 1 ：経営者が認識すべき「 3 原則」

原則①	情報セキュリティ対策は経営者のリーダーシップで進める
原則②	委託先の情報セキュリティ対策まで考慮する
原則③	関係者とは常に、情報セキュリティに関するコミュニケーションを取る

資料出所：（独）情報処理推進機構セキュリティセンター「中小企業の情報セキュリティ対策ガイドライン第 3 版」

さらに、経営者は以下の「重要 7 項目」について、自ら実践するか、あるいは実際に情報セキュリティ対策を実践する責任者や担当者に対して指示し、確実に実行することが必要です（図表 2 ）。

図表 2 ：経営者が取り組むべき「重要 7 項目」

取組①	情報セキュリティに関する組織全体の対応方針を定める
取組②	情報セキュリティ対策のための予算や人材などを確保する
取組③	必要と考えられる対策を検討させて実行を指示する
取組④	情報セキュリティ対策に関する適宜の見直しを指示する
取組⑤	緊急時の対応や復旧のための体制を整備する
取組⑥	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
取組⑦	情報セキュリティに関する最新動向を収集する

資料出所：（独）情報処理推進機構セキュリティセンター「中小企業の情報セキュリティ対策ガイドライン第 3 版」

■実務担当者が実践すべきこと

実務担当者としては、前述の重要７項目に加えて、できることから取組み、徐々にステップアップする必要があります。特に重要性が高い「情報セキュリティ５か条」についてお伝えします。

（１）情報セキュリティ５か条

①OS やソフトウェアは常に最新の状態に

- OS やソフトウェアを古いまま放置していると、セキュリティ上の問題を悪用したウイルスに感染してしまう危険性がある。
- 使用する OS やソフトウェアには、修正プログラムを適用するとともに、最新版を利用する。

②ウイルス対策ソフトを導入

- ID や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る。
- 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）を常に最新の状態になるようにする。

③パスワードを強化

- パスワードが推測や解析されたり、ウェブサービスから流出した ID やパスワードが悪用されることで、不正にログインされる被害が増加。
- パスワードは「長く」、「複雑に」、「使い回さない」ことで強化する。

④共有設定を見直す

- データ保管などのウェブサービスやネットワーク接続した複合機の設定の誤りから、無関係な人に情報を覗き見られるトラブルが増加。
- 無関係な人がウェブサービスや機器を使えるような設定になっていないことを確認する。

⑤脅威や攻撃の手口を知る

- 取引先や関係者と偽ってウイルス付きのメールを送付したり、正規のウェブサイトに似せた偽サイトを立ち上げて ID やパスワードを盗もうとする巧妙な手口が増加。
- 脅威や攻撃の手口を知り、対策をとる。

（２）自社のセキュリティ上の課題を知る

また、自社セキュリティ上の課題について知るために、「５分でできる！情報セキュリティ自社診断」を活用することをお勧めします（図表３）。

そのうえで、問題があった項目について、解説編を参考に対策を決定し、「情報セキュリティハンドブック（ひな形）」を編集して社内ルールを作成し、周知することが重要と思われます。

図表３：５分でできる！ 情報セキュリティ自社診断

資料出所：（独）情報処理推進機構セキュリティセンター「中小企業の情報セキュリティ対策ガイドライン第３版」

さらに今後、本格的に対策を進めるにあたって、①管理体制の構築、②IT 利活用方針と情報セキュリティの予算化、③情報セキュリティ規程の作成、④委託時の対策、⑤点検と改善　に取り組んでいく必要があるでしょう。

情報セキュリティは、中小企業が独自に取り組むにはなかなか難しいところもあると思われます。本ガイドライン、チェックツール、ひな形などを参考に、ぜひ自社の情報セキュリティポリシーを策定され、効果的に運用されることをお勧めします。

（太田宜志）