経営相談 Q&A

「SECURITY ACTION（セキュリティアクション）」の宣言について

Q 私は中小企業の代表者です。最近、取引先で自社のネットワークがコンピュータウイルスによる被害を受けたという話を聞きました。当社では対策としてウイルス対策ソフトを導入していますが、それ以上の特段の対策は行っていません。情報セキュリティをレベルアップするには、何から手をつければ良いでしょうか。

A 現在のＩＴ社会では、「企業経営」においてＩＴ活用による攻めと同時に、「情報セキュリティ」による守りが要求されます。

その情報セキュリティに関しては、秘密情報が漏洩した場合、被害者への損害賠償などの支払い、取引停止や顧客喪失、ネットの遮断による業務効率のダウン、従業員の士気低下など悪影響が発生するリスクがあります。そのため事前の備えとしてセキュリティのレベルアップが重要となります。

ご質問への答えとして、組織的セキュリティ強化のため、最近活用が増加している独立行政法人情報処理推進機構が推進中の「SECURITY ACTION」（以下、「セキュリティアクション」）宣言への取組みを紹介します。「セキュリティアクション」は自社で実施できる情報セキュリティに係るチェック項目から成り、以下でその内容を説明します。

■「セキュリティアクション」とは

経済産業省所管の独立行政法人情報処理推進機構が安全・安心なＩＴ社会を実現するために取組みを進めているものです。対象は中小企業等で、情報セキュリティ対策への取組みを自社で診断し企業自身がその内容を外部に宣言する制度です。

この制度はあくまで「自己宣言」であり、認定や承認といった第三者がお墨付きを与えるものではありません。

この「セキュリティアクション」は取組みの深度によって２段階の取組目標があり、基準を満たせば外部に宣言します。

２段階は「★一つ星」と「★★二つ星」でそれぞれロゴマークを利用し対外的にアピールします。

「★一つ星」 サンプル SECURITY ACTION ★ セキュリティ対策自己宣言

「★★二つ星」 サンプル SECURITY ACTION ★★ セキュリティ対策自己宣言

■「★一つ星」の取組内容は

「情報セキュリティ５か条」が達成目標となります。取組む内容は次の５項目です。

（１）ＯＳやソフトウェアは常に最新の状態にしよう！

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点が解決されず、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やソフトウェアには、修正プログラムを適用する、もしくは最新版を利用するようにしましょう。

（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。

（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流出したＩＤ・パスワードが悪用された

りすることで、不正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。

（４）共有設定を見直そう！

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を間違ったために、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。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。

（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。

■「★★二つ星」の取組内容は

「★★二つ星」で必要な内容は次の通りです。

（１）「５分でできる！情報セキュリティ自社診断」を活用してチェックを行う

全部で 25 項目あり、基本的対策の５項目のほか、従業員個人として必要な対策 13 項目と組織として必要な対策７項目がチェック項目となっています。「★一つ星」よりはチェック項目が多いですが、特に難度の高い項目はありません。この診断で自社の対策状態を把握しましょう。

（２）企業の基本方針である「情報セキュリティポリシー」を定め、外部に公開する

こちらについては、方針を定めるのは難しいと思われるかも知れませんが、独立行政法人情報処理推進機構（ＩＰＡ）ＨＰにサンプルが掲示されています。サンプルを参考に経営者の責任、社内体制の整備、従業員の取組みなど５項目について方針を立案します。

■取組みのメリット

「セキュリティアクション」に取組むメリットは次の通りです。

（１）取組むべき目安がわかる

取組むべき理由や対策が項目毎に解説してあり、具体的な対策が取りやすい。

（２）外部へのアピールができる

取り組んだことにより「セキュリティアクション」のロゴマークを使うことができるようになります。自社ポスターやパンフレット、名刺などで使用し外部へアピールできます。

（３）社員への意識づけができる

取組むためには自社セキュリティの内容を全社で確認することが必要で、経営陣だけでなく従業員も自社のセキュリティ状態に意識を向けるようになります。こうして、会社全体でセキュリティ意識の向上や行動の変化が現れ、レベルが向上します。

（４）ＩＴ導入補助金等に申請できる

自社の課題解決やニーズに合ったＩＴツール導入のための経費を一部補助するいくつかの補助金では「セキュリティアクション」が申請要件となっているものがあります。補助金を活用して業務効率化や売上アップにつなげることができます。

■取組みの留意点

これらメリットの多い「セキュリティアクション」への取組みですが、あくまで自社による宣言ですので、一定のレベルに達していることを国等が認定したりするものではありません。第三者の誤解を招く表現とならないよう注意が必要です。

■まとめ

今後の更なるステップアップとして、「中小企業の情報セキュリティ対策ガイドライン」を参考に、情報セキュリティ規程の制定や、既に制定している場合は規程の見直しによる新たな脅威等への対応を継続的に実施しましょう。　（刀祢善光）

独立行政法人情報処理推進機構（ＩＰＡ）ＨＰ
https://www.ipa.go.jp/security/security-action/