覚えておきたい情報セキュリティ&ネットワークのキホン（第1回）

情報セキュリティポリシーとはなぜ必要なのか？どのように作ればよいのか？

2022.03.25

クライアントとの取引内容や機密情報など、企業が円滑にビジネスを進めるためには情報セキュリティポリシーの設定が必要です。情報セキュリティポリシーはなぜ必要で、どのように作ればよいのでしょうか。本記事では、情報セキュリティポリシーの重要性や策定のポイントについて解説します。

情報セキュリティポリシーとは？

情報セキュリティポリシーとは、企業の情報セキュリティに対する行動指針のことです。例えば、外部からサイバー攻撃を受けたときの対応方法や、ヒューマンエラーにより機密情報を漏えいした際の対策について、対外的に示すことが挙げられます。

万が一、機密情報が漏えいした場合、社会的信用の低下など、大きな損失が発生します。機密情報を狙うサイバー攻撃は年々複雑・巧妙化しているため、情報セキュリティポリシーをあらかじめ定めておくことが重要です。

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の内容は企業によって異なりますが、以下の3つを基準に構成されるケースが多いです。

・基本方針
・対策基準
・実施手順

基本方針とは、企業がセキュリティポリシーを策定する上で重要視している根本的な考え方です。

例えば、「なぜ自社には情報セキュリティポリシーが必要なのか」「顧客情報をどのように取り扱うべきなのか」など、セキュリティ対策に関する基本方針・宣言を記述します。この方針に違反した従業員への処分についても、基本方針で定める必要があります。

基本方針を定めることで、具体的に何を対策するのか、どのようにして企業資産を守ればよいのか、が考えやすくなります。

基本方針を実施するための具体的な規則を記述するのが「対策基準」です。一般的には、情報セキュリティ対策に関するルールをまとめることが多いです。

対策基準は企業全体の情報セキュリティポリシーを定めるのではなく、部署や業務ごとの指針についても定めます。対策基準で定められるガイドラインとしては、以下の4つが挙げられます。

・システム開発ガイドライン
・サーバー運用ガイドライン
・社内・社外ガイドライン
・セキュリティ教育ガイドライン

上記ガイドラインを定める際は、具体的な対策方法や基準を設定します。サーバー運用ガイドラインを違反した場合、どのような罰則を定めるのかなど細かくかつ明確に決めておくことが求められます。詳細に設定することで、関係者がガイドラインを準拠しやすくなります。

対策基準で定めた内容を実施するために、手順を明確化することを「実施手順」と呼びます。部署や業務ごとに定めた情報セキュリティポリシーのガイドラインを基準に、実施する方法をマニュアル化することが一般的です。

例えば、情報セキュリティ教育ガイドラインの実施手順を策定する際は、教育の頻度やタイミング、学習形態を定めます。マニュアルを作成するだけではなく、正しく情報セキュリティに関する教育ができているのか、効果測定することも求められます。

実施手順は部署や業務内容によって異なるため、実現性の高い内容を策定することが求められます。

情報セキュリティポリシーの必要性… 続きを読む