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

なぜ情報セキュリティポリシーを設定する必要があるのか、その必要性は以下の3点に集約されます。

各種情報セキュリティ対策を可能にするため

情報セキュリティポリシーを策定することで、いくつかの情報セキュリティ対策が可能になります。大きくは、物理的情報セキュリティ対策、人的情報セキュリティ対策 、技術的情報セキュリティ対策の3つです。

物理的情報セキュリティ対策とは、従業員が業務で使用するパソコンの盗難や、サーバールームへの不正な立ち入りなどを防ぐことです。従業員がパソコンを廃棄する際にデータを完全に削除するようルール化することも、物理的情報セキュリティ対策に含まれます。

人的情報セキュリティ対策とは、情報セキュリティに関する教育を従業員に行うことを示します。従業員がサイバー攻撃に関する正しい知識を身に付けていれば、スパムメールを不用意に開封してしまうといったリスクを抑えることができます。

技術的情報セキュリティ対策とは、外部からの不正アクセスやサイバー攻撃を、専用のソフトウエアを用いて防ぐことです。ウイルス対策ソフトなど、サイバー攻撃に対抗できる対策を自社ネットワークに導入することで、未然に防ぐことが可能です。

社内の情報セキュリティリテラシーを高めるため

情報セキュリティポリシーを設定することで、社内の情報セキュリティリテラシー向上が見込めます。

例えば、新しい従業員が入社した際や、新たなサイバー攻撃が流行し始めたタイミングなどに、従業員に対する情報セキュリティ教育を実施することで、社内全体の情報セキュリティに対する意識が向上できます。

緊急時に迅速に対応できるようにするため

サイバー攻撃に遭い情報機器が使えなくなった場合などの緊急事態が発生した場合にも、情報セキュリティポリシーが役に立ちます。

例えば、災害時などで社内の情報セキュリティソフトウエアが正常に作動しなくなった場合、一刻も早く、情報セキュリティを復旧させる必要があります。情報セキュリティポリシーによって、あらかじめ部署や業務ごとに対応の手順をガイドラインで定めておけば、緊急時でもスムーズな現場対応が可能となります。

情報セキュリティポリシー策定のポイント

情報セキュリティポリシーを策定するポイントとして、以下の5つに留意する必要があります。

守るべき資産を明確にする

情報セキュリティポリシーでは、守るべき資産を明確にする必要があります。どれだけ従業員の情報セキュリティリテラシーを高めても、「どの情報資産が重要なのか」を明確にしなければ、何をどう守ればよいのか判断ができません。

例えば、顧客情報の流出を防ぐために「顧客の名前・住所・電話番号を守る」と定めても、「顧客のメールアドレスを守る」と定めていなければ、メールアドレスの流出事故が発生する恐れがあります。どの情報が自社にとって守るべき情報なのか、守るべき情報資産の範囲を洗い出し、情報セキュリティポリシーに明記しておくことが重要です。

対象者・範囲を定める

情報セキュリティポリシーは、自社が雇用する従業員だけが順守すればよいものではありません。派遣社員や取引先など、自社の業務に関わる人全てが守る必要があります。対象者の範囲を確実に定めておくべきです。

対象となる従業員の役職や地位についても、定義すべきでしょう。例えば人事役員は従業員の給与情報を扱えるが一般の従業員は扱えないなど、役職によって情報セキュリティポリシーの適用範囲が異なる場合は、ガイドラインに図表やイラストを用いて明示しましょう。

具体的なガイドラインを設定する

情報セキュリティポリシーは、内容が具体的であることが求められます。例えばパスワードに関するルールを情報セキュリティポリシーに記載する際は「複雑に設定する」という抽象的な表現ではなく「最低10文字以上にする」「アルファベットと数字を1文字以上含める」など具体的に記載することが求められます。

情報セキュリティポリシーに関する体制を整える

情報セキュリティポリシーの策定には、一定の時間がかかります。そのため運営組織や委員会などを立ち上げるなどで、策定のための体制を整える必要があります。その際、経営層と現場責任者のどちらも参画していなくてはいけません。

情報セキュリティポリシーは企業の経営方針に関わるものですが、現場の感覚と乖離したガイドラインを策定すると、ガイドラインを策定しても実効性の乏しいものになってしまいます。現場視点をもつ人材が、経営層と共に策定することが理想的です。

情報セキュリティポリシーを定期的に更新する

情報セキュリティポリシーは、一度策定すれば終わりというものではありません。サイバー攻撃の手法は日々進化しているため、情報セキュリティポリシーも定期的な更新をしていく必要があります。一定期間ごとに運用上の問題点を洗い出し、改善を繰り返すことで、自社に最適なガイドラインが策定できるようになります。

情報セキュリティポリシーのサンプル

情報セキュリティポリシーは企業によって異なりますが、ひな型となるガイドラインのサンプルは存在します。サンプルを自社に適した内容に作り変えていくことで、情報セキュリティポリシー策定を効率化することができます。

JNSA（日本ネットワークセキュリティ協会）のサンプル

JNSAは、情報セキュリティに関する情報共有や啓発をしている特定非営利活動法人です。同法人では、中小企業向けに最新の情報セキュリティポリシーのサンプルを公開しています。

2022年1月時点で公開されているバージョンでは、スマートデバイスやSNSなど、さまざまな技術やサービスに対応するガイドラインが公開されており、国際標準のISO/IEC27001を順守した内容となっています。
https://www.jnsa.org/result/2016/policy/

IPA（情報処理推進機構）のサンプル

IPAは、情報社会システムの安全性・信頼性の確保を目的とした独立行政法人です。同機構では中小企業の情報セキュリティ対策ガイドラインを提供しており、経営者・現場責任者の意見を取り入れた例文を公開しています。

ガイドラインは基本編から実践編まで、フェーズごとに内容が分かれているため、経営者がITに詳しくない場合でも活用しやすくなっています。
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

まとめ

企業がサイバー攻撃やヒューマンエラーによる情報漏えいを防ぐためには、情報セキュリティポリシーを策定する必要があります。あらかじめガイドラインを策定することで、緊急時でも迅速な対応が可能になり、社内情報セキュリティリテラシーの向上が期待できます。