水野施設長の介護マネジメント塾

6 月号

情報セキュリティ対策の基本

はじめに

皆さん、こんにちは。

前回、情報セキュリティに対する脅威とリスクについてお話ししましたが、今回はもう少し詳しくお話ししたいと思います。

情報セキュリティマネジメントにおいては、情報セキュリティのリスクを機密性のリスク、完全性のリスク、可用性のリスクと、大きく 3 つに分類しています。この 3 種類すべてのリスクから組織を保護するために、情報セキュリティマネジメントが有効といえるということです。

今回は、この情報セキュリティの 3 要素について、情報セキュリティの基本についてお話ししたいと思います。

総合的な対策が求められる情報セキュリティ

ITが進歩し続けている現代においては、情報セキュリティの重要性を十分に理解し、それに必要と思われるさまざまな対策を実施していても、被害に遭わないという保障はありません。

平成１５年に行われた総務省の通信利用動向調査によると、全体の 94%の企業がセキュリティに関する対応を行っていると答えていますが、一方で、72%がウイルスの発見や被害などによるなんらかの被害を受けたと回答されています。

また、企業が情報通信ネットワークを利用する上での問題点、課題としては、「セキュリティ対策の確立が困難」が 66%と最も多く、次ぎに、「ウイルス感染に不安」が 62%、「従業員のセキュリティ意識が低い」が 43%というように続いており、セキュリティ関連の問題が上位を占めていることがわかります。

情報セキュリティ対策は、ただ単に機器やシステムを導入しても十分な効果を期待することはできません。それは、組織にある情報システムをほぼ網羅した対策をとったつもりでも、たった一箇所のセキュリティ・ホールがあれば、そこから被害が拡大してしまうからです。

ですから、組織内にある基幹のシステムはもちろん、Web サイトのセキュリティ対策、業務委託先のパソコンのデータなどに至るまで、総合的な対策が求められます。そして、そのための不可欠な要件とされているのが、「機密性」、「完全性」、「可用性」の 3 つというわけです。

実効性のあるセキュリティポリシー

「機密性」、「完全性」、「可用性」という３要素をおわかりいただけたでしょうか。機密性は、ネットワーク上で扱う情報が外部に漏れることなく、許可されたユーザーのみが確実に情報にアクセスできること。完全性とは、情報が改ざんなどされず、正確、完全である状態を維持すること。そして可用性は、いつでもシステムの情報に確実にアクセスできることです。

これが、情報セキュリティ対策の根底となる考え方で、ここから、様々な脅威に対して、どのような対策を行っていくべきかを自施設の環境に合わせて考えていくことになります。

例えば、機密性を保つためには職員をはじめとするユーザー認証やアクセス制限、データ暗号化などの対策や、完全性を維持するためには不正侵入を防御するファイアウォールやウイルス/ワームなどの対策、可用性にはシステム管理やバックアップなどの仕組みが必要になります。

そして実際に、情報セキュリティに取り組むにあたっては、組織ごとのセキュリティポリシーが重要となります。セキュリティポリシーとは、個人情報の保護や機密漏洩の防止をはじめ、組織がコンピュータセキュリティに対する基本方針をまとめたものです。

セキュリティポリシーの策定は、一部の担当者のみで決められるものではありません。経営層や各部門の責任者、組織によっては、外部の監査機関なども含めたさまざまな立場で、組織が保護すべき情報資産をすべて洗い出すとともに、その中で、組織が抱えるリスクの分析などを行えば、自ずと情報セキュリティの問題点も見えてくるはずですし、だからこそ、組織全体で、必要な、また効果、実効性のあるセキュリティ対策が行えるからです。

セキュリティレベルをきちんと保つために

基本的なセキュリティポリシーが作成されれば、次ぎに、実際に行う手順（ルール）を決めていきます。例えば、誰がどの情報を利用できるのかといったアクセス権限の設定をはじめ、どんな方法で情報を保護するのか、被害を受けた時にどう対応するのかという手順を決め、継続的な情報収集に基づき、具体的なセキュリティ対策を講じていくわけですが、情報セキュリティ対策は、これで終わりではありません。

ここからがさらに大切なこととして、セキュリティポリシーとその手順・ルールを定期的に見直すことです。セキュリティポリシーやルールを決めていても、冒頭にお話ししたとおり、ITが進歩し続けている現代において永久的に効果があり続けることはありません。そのため、情報資産に新たな脅威が発生してないか、システム環境に変化はないかを確認するなど、現在の状況にセキュリティポリシーや手順・ルールが合っているのか、効果的に運用されているのかなどを見極めることが必要となってきます。

つまり、セキュリティレベルをきちんと保つためには、セキュリティ対策基準の策定、導入、運用、評価・見直しのサイクルを「繰り返し」実施することがポイントとなるのです。

※参考文献

総務省　通信利用動向調査（平成 15 年）