情報セキュリティの必要性

・情報システムの停止による損失

・顧客情報の漏洩（ろうえい）による企業や組織のブランドイメージの失墜

・社内情報の流出であれば企業価値を大きく下げる

企業や組織だけでなく取引先や顧客などへも波及

重要な経営課題のひとつであり社会的責務でもある

情報セキュリティ対策は、世界的にも重要な経営課題であると認識されており、情報セキュリティ製品・システム評価基準や情報セキュリティマネジメントシステムの認証基準が、国際標準として規格化されている

例　5

C 社はネットサービスをすぐに使えコスト削減もできるメリットからレンタルサーバのサービスを利用することにした。それから業務は効率よく順調に進んでいたが、レンタルサーバに接続できないという症状が発生。サービス事業者に連絡すると障害が発生し利用できないとのこと。さらにレンタルサーバ内にあった重要データがすべて消えてしまっており、復旧もできないという連絡が来た。そのレンタルサーバにしか保存しておらず、バックアップも取得していなかった。サービス規約をよく読むとデータのバックアップや復旧は利用者の責任であると記載。すべて丸投げ可能のサービスで、このような責任や業務は発生しないと考えて利用していた。業務もできずデータも消去されただただ途方に暮れるしかなかった。

クラウドは障害やメンテナンスなどで利用できなくなることを想定し、バックアップ取得や停止時の代替手段などを用意しておく。利用規約を熟読し利用者側にはどこまで責任があり、何をしなければならないのかを確認をしておく。

情報セキュリティポリシーの概要/目的/内容

3 つの階層

①基本方針

組織や企業の代表者による宣言

・なぜ情報セキュリティが必要か

・どのような方針で情報セキュリティを考えるか

・顧客情報はどのような方針で取り扱うのか

②対策基準

情報セキュリティ対策の指針を記述

どのような対策を行うかという一般的な規定のみ

③実施手順

対策基準ごとに対策内容の具体的手順を記載

企業の情報資産を脅威から単純に守ることだけでなく、導入や運用を通して社員の情報セキュリティに対する意識の向上や取引先や顧客からの信頼性の向上といった二次的なメリットも得られる

情報セキュリティポリシー教育

「意識」と「警戒」

・意識

いつでもどこかでサイバー攻撃が起きる可能性を認識していること

・警戒

サイバー攻撃を予測し、実際に攻撃を受けた時、素早く行動して反応すること

テクノロジーが検出に失敗した場合

「最後の防衛線は人である」

常に人がミスするような方法をとる

「最大の弱点も人である」

情報セキュリティポリシー教育

意識～従業員を尊重する

1. 信頼の文化を醸成する

・従業員との信頼関係構築が重要

・セキュリティ問題の重要性を認識と、発生時に報告する教育をする際、オープンで親しみやすい雰囲気の中で行えば、会社の利益のために進んで取り組む

・従業員を最も脆弱とみなした場合、信頼を築くのは難しい

・罰せられたり嘲笑されたりする恐れを感じている場合、URL をクリックしたり添付ファイルを開いても報告してくれない可能性

従業員自らの積極的な行動にすることで、
問題発生時に即対処できる、傷口が広がらないようにできる

まとめ

現状

日々進化したサイバー攻撃があり、常に企業は情報資産を奪われるリスクを抱えている

認識

自社は大丈夫、自社の社員は大丈夫、ウイルス対策ソフトを導入しているから問題ないということは大問題

行動内容

・情報セキュリティポリシーの策定
・教育
・評価
・アップデート

個々が現状を認識と警戒を続けるための機能、仕組みを作り上げることが重要