2025年　第5号

中小企業の皆様へのお役立ち情報 OMジャーナル

For the next solutions
オンワード マネジメント

平素より格別のご厚情を賜り、深く感謝申し上げます。今月のテーマは「サイバーリスク」です。大企業を襲ったサイバー攻撃。他人事では無く自らのリスクとして対策を考えましょう。

アサヒビールや ASKUL を襲ったサイバー攻撃

9 月にアサヒビールへのサイバー攻撃が発生し、システム障害により深刻な被害が生じました。原因はランサムウェア（身代金要求型ウイルス）によるもので、最近になって個人情報が流出した可能性も発表され、被害はさらに拡大する様相を見せています。

さらに 10 月には大手通販会社のアスクルでも、同様にランサムウェアによるシステム障害が発生し、法人向けサイト「ASKUL」や個人向け「LOHACO」などの受注・出荷業務が一時停止する事態となりました。いずれのケースも、情報漏えいや業務停止といった実害に直結し、企業の信頼や事業継続に大きな影響を与えています。

大企業ならセキュリティ体制が整い、従業員への教育も徹底されているから大丈夫、と思いがちですが、実際にはサイバー攻撃を完全に防ぐことは極めて困難です。攻撃者は技術の隙を突くだけでなく、人的ミスや取引先経由の侵入など、複数の経路から巧妙に攻撃を仕掛けてきます。実際、サイバー攻撃の約 50%は中小企業を標的にしているとも言われています。私たちはサイバー攻撃を「他人事」とせず、自社でもいつ発生してもおかしくないリスクとして想定し、対策を継続的に実践していくことが重要です。

サイバー攻撃による被害

サイバー攻撃による被害は主に以下の様に分類されます。
①情報漏洩による損害（例：外部からの不正アクセスにより個人情報が流出し損害賠償請求を受ける）
②ネットワーク中断による損害（例：自社製品生産ラインが停止し逸失利益が発生）
③自社システムの損害（例：データ復旧費用、※フォレンジック調査費用　等）
※サイバー攻撃の影響範囲を確定する調査でパソコン 1 台あたり 200 万円以上かかるケースも

サイバー攻撃に備える（サイバー保険への加入）

サイバー攻撃被害を防ぐためには、まず社内体制整備が大切ですが、保険に加入していない場合は是非サイバー保険に加入しておくことをお勧めします。サイバー保険では個人情報漏洩に起因する賠償責任を補償するだけでなく営業継続費用、原因調査費用、データ復元費用なども含め幅広くサイバー攻撃被害に備えることが可能です。被害発生時の緊急サポートサービスが付帯されており、社内教育用の無料ツールも利用できます。ご検討の際は是非、当社へお声掛け下さい。複数保険会社から最適なプランをご提案できます。

HP・インスタ・Xでも情報発信中！フォローもお願いします