

IT セキュリティ対策は企業の経営課題

IT のセキュリティ対策は、企業の重要課題

特定企業を狙った犯罪も増加
大企業だけでなく、中小企業も対策が必要
利便性を求めれば、リスクも増大



IT 部門だけの責任にせず
経営レベルの取り組みが必要

企業が IT のセキュリティリスクに対して対策をとることは、重要視すべき経営課題です。

インターネットが普及し始めた頃では、姿が見えない個人レベルの愉快犯による不特定多数へのばらまき型のサイバー攻撃が多かったのですが、サイバー犯罪も組織化され、特定の企業を狙った標的型攻撃が多くなってきました。

近年、話題になってきた「サプライチェーン攻撃」は、大企業が直接狙われるだけでなく、協力会社の中小企業などのセキュリティレベルが低いところを経由して、巧妙な攻撃を仕掛けてきます。

インターネットの普及により、ネット販売や、流通管理などの企業活動は、圧倒的に利便性が向上しました。

これは、今までカギをかける必要もないような田舎の家が、公道ができると自動車によって短時間でいろんなところに行けるようになり、不便だった生活が一変して便利になることに似ています。

公道に出れるようになるということは、反対に不特定多数の人が、その家へ訪れ易くもなります。よって、泥棒や、犯罪者から守るために、カギを二重にするなど家の防犯の強化が必要になります。

サイバー犯罪も同じで、ネットをビジネスで利用して便利になることを望めば、確かに業務は効率的になり生産性向上や売上アップも期待できますが、それに伴って企業を守るためのセキュリティ対策が必要です。便利になった分、リスクも増大するという現実があります。

その例として、連日ニュースになっているハッキング等の事件によって不正に流出した個人情報、億単位の数の ID やパスワードがダークウェブで売買されていることが知られています。

インターネットの恐ろしいところは、遠隔地から、物音一つ立てず、顔も見せず、短時間で大規模の犯罪を可能にしてしまうことです。たとえば、仮想通貨取引所を狙った犯罪などは、銃を持って顔を隠して銀行を襲撃するようなりリスクを冒さなくても、ほんの数分で、物理的には持ち運べないような数百億円規模の窃盗事件が現実に発生してしまっています。

ハッキングのための手法や、プログラムが、ダークウェブで販売されていたり、プログラムを複数実行したりコピーすることで、とてつもなく大量のサイバー攻撃が毎日仕掛けられています。

企業は、IT 部門の担当者任せにせず、経営が責任を持って全社レベルのセキュリティ対策が必要です。