オフィスのトータルサポート 株式会社 SK-NET

中小規模企業（SOHO）のセキュリティ対策、アンチウィルスだけで十分だと考えていませんか？

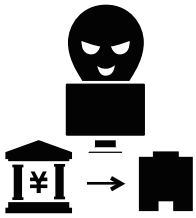
本当に今の対策で万全と言えますか!?

『ウチは小さい企業だから･･･』
『アンチウィルスソフト入れてるから大丈夫』
『怪しいページや、メールは開かないようにしているから･･･』
『うちの事務所は PC の台数が少ない』
このようにおっしゃるユーザー様は、まだまだたくさんいらっしゃいます。
しかし、昨今これだけではセキュリティ対策は不十分であることは、
ニュースや報道の通りです。大事なのは PC の台数ではなく、
インターネットに接続されている社内ネットワーク上に重要なデータがあるかどうかです。

被害が多い代表的なウィルス（一部）

標的型メール

標的型メールによる「気づけない攻撃」が多数発覚しています。
標的型サイバー攻撃をうけた多くの企業において、外部からの指摘により初めて攻撃が発覚しており、
また標的型サイバー攻撃の 8 割が、標的型メールが攻撃の発端であったことも確認されています



ネットバンク詐欺ツール

企業をターゲットにしたネットバンキング不正送金の被害が増えています。
詐欺ツールに感染すると最終的に金銭被害を受けます。
企業が被害を受けた場合、対策を行っていない場合保障外となるため、対策は重要です。

ランサムウェア（身代金要求型ウイルス）

感染した PC をロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、
元に戻すことと引き換えに「身代金」を要求する不正プログラムです。
最近では、共有フォルダまで暗号化され、企業にとって重要な情報が使用不能になるケースも出てきています。
※現金を支払っても元に戻らないケースがほとんどですが、まれに支払をすれば元に戻った事例も確認しています。

攻撃を仕掛ける側もセキュリティ対策をしている会社とウィルスソフトだけの会社があればウィルスソフトだけの会社を選ぶでしょう。
より簡単に攻撃できる方を選ぶのは当たり前です。ニュースに取り上げられるのは大企業が多いですが
実際には取り上げられていない中小企業への攻撃件数は計り知れません。
『気づかないうちに大企業への攻撃の踏み台にされていた』、『巧みに誘導された標的型攻撃だった』
そうなる前に、今一度セキュリティについて見直してみてください。