セキュリティ対策虎の巻（第2回）

攻撃を食い止める多層防御。UTMソリューション

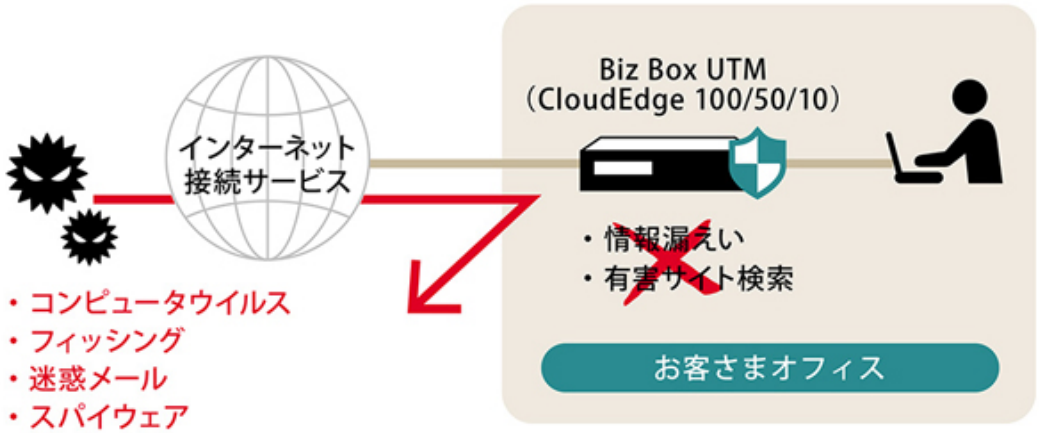
2020.11.04

よくマスコミで報道される企業の情報漏えい事件の多くは、セキュリティ対策をしていなかったわけではない。攻撃者の手口の巧妙化が進むと、これまでは有効とされていた対策が通用しなくなるからだ。ウイルス対策ソフトやファイアウォールだけといった、単一的・局所的なセキュリティ対策ではもはや防ぎ切れなくなっている。

こうした課題を解決する1つの方法が多層防御だ。攻撃の入り口から出口まで、複数のセキュリティ対策を組み合わせて“どこか”で攻撃を食い止めるやり方だ。これを実現するのがUTM（統合脅威管理）である。

UTMは複数のセキュリティ機能を1台に統合し、さまざまな脅威に対応できる。NTT西日本では、中小規模の事業所に適したソリューションとして「セキュリティおまかせプラン プライム」を用意している。このソリューションは、ネットワークの入り口と出口対策に加えて、24時間365日の通信監視や標的型攻撃メール対策訓練を含む、いわば“セキュリティのよろずおまかせ”プランでUTMソリューションも組み込まれている。悪意のあるメールやウイルスといった外部脅威への防御と、メール訓練機能による社員のセキュリティ意識向上および社内の感染拡大を未然に防ぐ内部脅威への防御を備えた「事前対策」。さらに、万が一の異常発生時には電話やメールお知らせをする「事後対策」により、セキュリティ対策を複合的にサポートする。

【UTMの仕組み】



近年は標的型攻撃に見られるように、特定の企業の機密情報や顧客情報を盗み取り、第三者に転売する金銭目的の攻撃は後を絶たない。「うちは標的型攻撃の被害に遭うような情報は持っていない」と考える経営者もいるかもしれない。だが、対策の手薄な企業がその踏み台になり、取引先が狙われる危険性もある。「標的型攻撃とは無関係」とは言っていられない

。攻撃者の手口が巧妙化し、いくつかのステップを踏んで攻撃を仕掛け、目的の機密情報を盗み取る手口が知られている。その手口を理解し、対策を講じることが、不正アクセスや情報漏えいを防ぐ手立てとなる。

入り口から出口まで複数の対策を組み合わせる… 続きを読む