セキュリティ対策虎の巻（第3回）

拠点間のやり取りをVPNですればセキュアになる

2016.08.24

企業資産のデジタル化などネットワークの重要性が増す中、サイバー攻撃による情報漏えいなどさまざまなリスクも拡大傾向にある。

それでは企業にどんなネットワーク環境が必要だろうか。快適に通信できる“高速性”、拠点の追加・変更にも柔軟に対応できる“拡張性”、容易な運用性に加え、不正アクセスやデータの改ざん・盗聴、攻撃者の踏み台を防ぐ“安全性”が重要になる。「ビジネスリスクを回避する意味でも、ネットワーク環境のセキュリティー強化に対応できない企業は、取引を見直さざるを得ない」と指摘する声もある。社内・社外を含めたセキュアなネットワーク環境の利用が求められているのだ。

情報漏えいや誤送信のリスクを低減するネットワーク環境

ネットワーク環境のセキュリティーリスクを低減するには、社外と社内で分けて検討し複数の対策（多層防御）を講じる必要がある。例えば、世界中につながるインターネットは誰でも手軽に利用できるため、さまざまな攻撃を受けるリスクがある。そこで社外向けの対策として、インターネットと社内ネットワークの出入り口（ゲートウエイ）に、UTMやファイアウォールなどのセキュリティー対策を施し、外部からの攻撃を防御することが重要だ。

次に社内向けの対策である。企業の拠点間を結ぶ社内ネットワークとして、導入が進んでいるのが「VPN」（バーチャル・プライベート・ネットワーク）だ。文字通り、“仮想的”に専用のネットワークを構築する。

その特徴は、拠点間のネットワーク上に仮想的なトンネルを作り、そのトンネル内で許可したデータのみを通信するという制御が可能なところだ。拠点間のデータのやり取りで機密情報が外部に漏れたり、外部に誤送信したりするリスクを低減できる。

インターネットVPNとIP-VPNのどちらを選ぶ？… 続きを読む