大規模セキュリティー施策（第5回）

セキュリティ専任者ゼロの奥の手、クラウドUTM

2018.11.14

「終わりなき戦い」「完璧な防御など存在しない」といわれるセキュリティ対策。テクノロジーの進歩と同時に脅威も複雑・巧妙化しているのが現実だ。最近、注目を集めているのが「クラウド」と「専門家の力」をフル活用した新しい取り組みだ。

多拠点でのUTMの課題

現在のセキュリティ対策として広く使われているのは、端末常駐型の対策ソフトだ。メールの添付ファイルに仕込まれたマルウエアなどの不正なプログラムを削除したり、危険なWebサイトへの接続を遮断したりする機能を持つ。今ではほとんどのユーザーが、この対策ソフトを導入している状況だ。

ただし、端末常駐型の対策ソフトによる防御には大きな弱点がある。それはすべての端末においてインストールと頻繁な更新が必須という点だ。新種、亜種のマルウエアが日々膨大に発見される現在、そのすべてに対応するのは至難の業だ。さらに、スマホやタブレット活用が業務でも進む状況で、すべての端末にソフトをインストールし、日々更新を徹底するには限界がある。そこで端末だけでなく、ネットワークの出入り口となる部分に機器を導入し、集中的に対策を行う仕組みが登場した。UTM（統合脅威管理）と呼ばれるこの方法は、セキュリティ強化につながるものとして評価され、企業などで導入が進められている。

ところが最近、“UTMの管理が追いつかない”という困った状況が発生しつつある。特に支社、営業所、工場、倉庫など多くの拠点を持つ企業・組織では、各拠点で生じるネットワーク機器の管理負荷が大きくなるケースや、そもそも各拠点にUTMを設置する予算がないケースがある。潤沢な予算を組み、IT担当者を各拠点に配置できればよいが、なかなかそうもいかない。攻撃する側から見れば、管理の甘い拠点は格好のターゲットとなる。

クラウドUTMのメリット

増加の一途をたどるセキュリティ関連の負担を抑えるために、さまざまな取り組みが進められている。その中で、効果的な方法として注目を集めているのが、クラウド型のセキュリティ対策だ。

これまで、UTMにおいても、拠点ごとに機器を設置して個別運用する仕組み（オンプレミス）が主流だった。同時接続するユーザー数や必要な機能に応じて製品を選択する方法だ。しかし、クラウド上での集中管理という選択肢がUTMにも出てきた。

例えば、NTT西日本グループであるNTTスマートコネクトの「SmartConnect Network & Securityクラウド型UTM」は、複数拠点におけるインターネット接続とUTMを統合して、効率的にセキュリティ管理を行う。データセンター内に設置されるフォーティネット社製UTM機器は、オンプレミスと同様に柔軟な設定が可能で、高い信頼性を持つ。すべての拠点を1台のUTMに集約できるのでコスト削減にもつながる。今後UTMを導入したいと考えるユーザーに加え、現在オンプレミスで運用中のユーザーについても有効なソリューションといえる。

併せて、すでにUTM機器を導入しているユーザーには、その運用監視を提供するサービスも登場している。ソフトバンク・テクノロジーの「マネージド・セキュリティ・サービス for UTM」は、各拠点に設置されたUTMを専門アナリストが監視して、運用をサポートする。人手不足で管理に手が回らない企業や、情報システム部を持たない企業にとって頼もしい。

SOCとネットワークも検討のカギ… 続きを読む