サイバーセキュリティ最前線

「一般ユーザー」権限への切り替えで「ゼロトラスト」に着手!!

前号では「ゼロトラスト」という概念とその重要性を紹介したが、中小企業などからは「推奨されている対策が大がかりで何からはじめるべきかわからない」「人材や費用などの面から大がかりな対策をとれない」といった声があがっている。そこで、今号ではより現実的にゼロトラストを推進するための初歩的な取り組みを紹介したい。

「権限」の再確認からスタート

ゼロトラストとは前号でも紹介した通り、「一切を信頼しない」という前提でITセキュリティを構築する考え方であり、内部と外部を区別せず、情報資産やシステムにアクセスするものをすべて検証し、脅威を防ぐことで成立する。

では、どうすれば中小企業でもゼロトラストに着手できるのか。長年にわたりセキュリティシステムの提案を行ってきた㈱ブロード（東京都千代田区）は「侵害の80㌫が特権の誤用、濫用に関係していることから、ゼロトラストの考えのひとつである『最小権限の原則』に着目し、手はじめにパソコンのユーザーに付与される『権限』を再確認してほしい」と強調する。

Windowsの場合、パソコン購入後に電源を入れると、いかなる操作も制約なしに行える「管理者」という権限に設定されるが、それに対して特定の操作に制約が設けられている「一般ユーザー」という権限がある。そもそも、このふたつの権限は利用者ごとにアカウントを設定することで、アクセス可能なファイルを指定したり、好みに応じた表示を設定可能にしたり、不適切な操作でパソコンの動作に不具合が起きることを防いだりするために設けられたものだ。

しかし、最近では第三者によるサイバー攻撃のリスクが大幅に上がっており、あらためてこの区分が重視されるようになってきている。実際、セキュリティが甘い状態で「管理者」権限で日常業務を行うと、マルウェアに侵入されたことを知らないままにそのプログラムを無制限に実行してしまうといったリスクがあり、最悪の場合はIDやパスワードなどの漏えいにもつながる。対して「一般ユーザー」であれば、仮にあらたなプログラムをダウンロードしたり、実行したりしようとしてもOSが許可しないため自動的に処理が停止するようになっている。

また「管理者」権限には、脆弱性を悪用されるリスクもある。脆弱性とはソフトウェア製品などのセキュリティ上の不具合のことで、ブロードによると「マイクロソフト社製品においても、2020年の1年間で1268件が認識されている（前年比48㌫増）」という。だが、この脆弱性を悪用した操作の多くは「管理者」権限を条件としており、「マイクロソフト社製品（19年）のうち脆弱性に関して『重要』と位置づけられたものの77㌫は『一般ユーザー』であればリスクを軽減できる」そうだ。

デメリットの解消方法

こうした事情を考慮すると、すぐにでも「一般ユーザー」に切り替えたいところだが、一方で「一般ユーザー」に切り替えるとシステム変更などの場面で制約が生じるというデメリットもある。が、ブロードによると「一般ユーザー」としてログインしても事前にきめたプログラムについてはインストールや実行が可能になるセキュリティ製品もあるとのことなので、気になる向きは問い合わせてみるといいだろう。また、同じくブロードが取り扱っている「HP Sure Click Enterprise」の利用も効果的だ。このシステムは「マイクロVM（仮想パソコン）で文書ファイルやインターネットのページを開くという仕組みになっており、『管理者』として悪意のあるプログラムを操作したとしても本体にダメージを被ることがない」からだ。

サイバーリスクを軽減するためにも、「一般ユーザー」への切り替えや「HP Sure Click Enterprise」の導入を検討してみてはどうだろうか。