サイバーセキュリティ最前線

「ゼロトラスト」という概念にもとづいたハイレベルなセキュリティ環境のつくり方

昨年、内閣府は「政府CIO補佐官等ディスカッションペーパー」として「政府情報システムにおけるゼロトラスト適用に向けた考え方」という文書を発表。その影響もあって、最近、ゼロトラストという概念がにわかに注目されている。そこで、今号ではゼロトラストにもとづくセキュリティ対策について考えてみたい。

一切を信頼しない考え方

ゼロトラストとは文字通り「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だ。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）によると「従来型のセキュリティは、インターネットに対して社内ネットワークの内部には正当なユーザー（従業員）とコンピューター、プログラム、データしか存在しないという前提にもとづいて運用されている。だが、ゼロトラストでは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はすべて検証し、脅威を防ぐことを重視している」という。

それにしても、なぜ近年、ゼロトラストは重視されるようになってきたのか。その点について、ブロードは「高度なサイバー攻撃はネットワークに入りこんだ後に内部からの横展開で重要なデータを狙うことが多いし、働き方改革やDXを推進するなかで社外での使用時も社内と同等以上のセキュリティレベルの確保が必要」と指摘。また「『政府CIO補佐官等ディスカッションペーパー』でもリモートワークが普及した昨今においては『これまでの（社内外を隔てる城壁があるかのような）境界型セキュリティの考え方だけでは、その実現が困難』とされており、コロナ禍にあってゼロトラストがますます重要視されている」としている。

エンドポイントの強化も必須

ゼロトラストの導入には①あらゆるユーザー、ネットワーク、デバイスが正当であることを確認②ネットワークの内部と外部を区分しない③どのようなネットワークからでも安全なアクセスの実現④最小権限の原則とNeed to Knowコンセプト（必要がある最小限の人のみ知らせる）の適用⑤あらゆる通信記録の監視といった指針がある。また、それには企業組織ごとにリスクの度合いや予算、必要な期間などを加味しなければならない。たとえば④については「内部のユーザーが悪いことはしないという前提で、ユーザーアカウントに操作に制限のない管理者権限を付与してしまっているケースが多々あるが、これでは不正な操作が可能なだけでなく、マルウェアの動作にブレーキがかからず大幅なリスク増加になってしまう。また、サーバー管理者用のアカウントとパスワードを複数の担当者が共有して、ほとんど変更しないケースも見受けられるが、これもまた不正アクセス発生要因となる」とブロードは指摘。だからこそ「ゼロトラストにもとづいたセキュリティを導入・運用しなければならない」としている。

このほか、前出の「政府CIO補佐官等ディスカッションペーパー」ではエンドポイントのセキュリティ強化についても言及されているが、その際に役立つのがブロードが日本総代理店を務める米国発のセキュリティ製品「HP SCE（旧Bromium）」だ。これはメールやインターネット経由のデータを一切信頼せず、パソコン本体から隔離された仮想環境でウェブサイトを閲覧したり、文書ファイルを安全に開いたりできるというシステムで、ゼロトラストにもマッチしているし、自宅など社外のネットワーク利用時でも同じレベルのセキュリティが有効になる。「徹底したセキュリティを追求する米軍などにもはやくから採用され、国内でも金融機関などでの採用が広がっている」というから、導入を検討してみてはどうだろうか。