ゼロトラストという考え方

ゼロトラスト（ZERO TRUST）

- ” never trust, always verify” --- 決して信用せず、常に確認
- すべてのトラフィックを調べ、ログを取る
- 内側からの脅威にも備える設計
- コンプライアンス、セキュリティポリシーを遵守する細分化されたデザイン

MICRO-SEGMENTATION

ユーザ、データ、ロケーションに基づいて、
セキュリティの境界を細分化

近年、ネットワークセキュリティの分野で、ゼロトラストというコンセプトがクローズアップされてきました。
これは、従来の perimeter-based のようなファイアウォールで境界を決め、外部からの脅威についてセキュリティツールなどで社内を守るという考え方では、システムが多様化し、とても守り切れないほど複雑化してきた背景があります。
昔からセキュリティに対する考え方について、海外の性悪説に対し、日本は文化的に性善説で対応を考えてしまう傾向がありました。但し、スマートフォンなどのモバイル機器や、IoT デバイス等がたくさん企業にも持ち込まれるようになると、ファイアウォール内は安全だとか、社員の不正を疑うような仕組みは不要だとか、などといった考え方を見直さざるを得ないような時代になってきました。
ゼロトラストというコンセプトは、もはやセキュリティの境界内の行動も、システムも、サービスのオペレーションでさえ信頼せず、承認されたアクセスのみ許可されるように自動的に検証するという考えです。つまりは、社内での業務プロセスのための操作さえ疑い、チェックするという性悪説的な考えです。
確かに、今の技術をもってすれば、多種多様なセキュリティツールを組み込み自動化することは可能なのかもしれません。ただ、それを監視する人、管理する人は中央集権的に権限を集中させるのでしょうか？それとも、三権分立のような仕組みでお互いに監視し合えるところまで仕組みを考えるべきなのでしょうか？疑うところからはじめる仕組みは、管理方法についても、ポリシー作りから運用までとてもたいへんそうです。
例えとして適切でないかもしれませんが、昨今、中国で街中に 2 億台近くの監視カメラが設置され、顔認識の AI などを駆使してあらゆる個人情報を追跡する「社会信用システム」が話題になっています。監視システムは交通規則を無視して道路を横断する歩行者を特定し、その人物の顔と名前を道路脇のディスプレーに映し出すようなことまで行い、プライバシーの問題で脅威を感じるという意見もある一方、そこで暮らす人々は、モラルが保たれ安心だという意見も多い様です。日本でもここまですれば、駐車禁止や、煽り運転などが減少する期待があり、防犯のためにも監視を強化すべきという考えに賛同したくなる人もいるでしょう。
セキュリティに対する考え方も、時代と共に変化します。それゆえ、企業は常にリスク分析を行い、適宜セキュリティポリシーの見直しをすることがますます重要になってきているといえます。