覚えておきたい情報セキュリティ&ネットワークのキホン（第4回）

「ゼロトラストセキュリティ」とは何か？

2022.03.25

テレワークや業務でのクラウド利用が広がったことで、従来型の情報セキュリティ対策では安全の維持が難しくなりつつあります。そこで注目されているのが「ゼロトラストモデル」の情報セキュリティフレームワークです。

ゼロトラストセキュリティのフレームワークとは何なのでしょうか？
そして、ゼロトラストセキュリティは今までの情報セキュリティ対策と何が違うのでしょうか？
本記事では、ゼロトラストセキュリティの概要とフレームワークについて整理します。

ゼロトラストモデルとは？基本的な解説

ゼロトラストモデルとは、「すべてのアクセス行為が危険である」と定義した情報セキュリティモデルです。

ゼロトラストは2010年にForrester Research社が提唱していましたが、当時は従来の境界防御型の情報セキュリティ対策が一般的だったため、採用する企業はそこまで多くありませんでした。しかし、テレワークが普及し、社外からでもオフィスと同等のデータにアクセスすることが当たり前となりつつある今、ゼロトラストの重要性が注目されています。

境界防御モデルとは

従来型の情報セキュリティ対策である「境界防御モデル」は、信用する領域と信用しない領域に境界を明確に定めて情報を守る方法です。社内を「信用できる領域」、社外を「使用できない領域」と定めたうえで、社内と社外のネットワークの境界線上に情報セキュリティ対策をすることによって安全な環境をつくり上げます。例えば、ファイアウォールなどの情報セキュリティ機器を設置し、外部からの不正な通信を遮断する考え方です。

こうした境界防御モデルは、守りたいデータやシステムが社内のネットワークにあることを前提としています。しかし、テレワークによって社外ネットワークから社内データにアクセスする機会が増えたことで、社内と社外の境界が曖昧になり、境界防御モデルによる情報セキュリティレベルの低下が懸念されるようになりました。

ゼロトラストモデルの特徴

ゼロトラストモデルは、境界防御のようにネットワークの内外を区別せずに、アクセスするものをすべて疑い、検証することによって脅威を防ぐものです。例えば、ネットワークの内外を問わずデータを暗号化したり、端末すべてのアクセスログを監視したりします。ゼロトラストを採用すれば、もし外部から自社システム内に不正に侵入されたとしても、素早く検知し対処できるようになります。その結果、情報漏えいリスクを最小限に抑えることにつながります。

ゼロトラストフレームワークの主な要素

では、ゼロトラストを自社に導入するにはどうすればよいのでしょうか。IPA（情報処理推進機構）は、以下4つを検討すること

が重要と述べています。

認証・認可
ユーザーが企業内のデータにアクセスする際は、必要最低限の権限のみ付与するようにする。

クラウド利用
境界防御モデルだけではなく、クラウド利用を想定した情報セキュリティ対策を行う。

端末セキュリティ
テレワーク用パソコンやスマートフォンなど、社外で利用する端末がサイバー攻撃の踏み台とならないように情報セキュリティ対策を行う。

ログ管理
サイバー攻撃の経路分析や影響範囲の調査に、アクセスログの収集・分析ができるようにする。

ゼロトラストフレームワークを支えるソリューション… 続きを読む