ニューノーマル処方箋（第34回）

すべての通信を信用しない「ゼロトラスト」とは何なのか

2024.01.30

＜目次＞

すべての通信を信用しない「ゼロトラスト」とは何なのか？

企業のセキュリティ対策というと、これまでは社内のネットワークを守るためにファイアウォールを設置し、外部の不正アクセスやサイバー攻撃を防ぐ「境界型セキュリティ」が一般的でした。

しかし、テレワークやクラウドサービスが普及した今、社外から社内ネットワークに、もしくは社内から社外のクラウドサービスに接続する機会は日常的に起きています。そのため、従来の境界型セキュリティのままでは、セキュリティ対策が不十分で、悪意のある第三者の侵入を許してしまう恐れがあります。

こうした従来のセキュリティ対策の一歩先を行く考え方として「ゼロトラスト」が存在します。ゼロトラストは、たとえ境界内部の通信であっても無条件に信用せず、全ての通信を確認し、認証・認可を行う手法となります。

ゼロトラストは、どのようにしてセキュリティを維持するのでしょうか？また、従来の境界型セキュリティと比べ、どのような点が異なるのでしょうか？ IPAが公開している資料「ゼロトラスト移行のすゝめ」から、その仕組みを読み解きます。

ゼロトラストではなぜ「IDの統制」が最重要なのか

同資料によると、ゼロトラストは、【1】ID統制（ID管理）、【2】デバイス統制・保護、【3】ネットワークセキュリティ、【4】データ漏えい防止、【5】ログの収集・分析、という5つの要素から構成されるといいます。

【1】の「ID統制」とは、誰が社内のリソースにアクセスしようとしているのかを、その都度識別し、認証・認可を行うことを指します。

退職した従業員のIDを使用不可にすることも、ID統制に含まれます。退職者の従業員のIDが利用できる状態になっている場合、そのアカウントが何者かに悪用され、機密ファイルが外部に流出することもあり得ます。資料ではID統制について「ゼ

ロトラストの概念を実装するにあたり、最も重要と言える」と断言しています。

ID統制を可能にするサービスとしては、「IDaaS（アイダース、ID as a Service）」があります。IDaaSは、複数のアプリやサービスに登録されているIDやパスワードを、クラウド上で一元的に管理するサービスのことです。IDaaSを利用すれば、従業員はアプリやサービスへのサインインを一度に行えるため（いわゆるシングルサインオン[SSO/Single Sign On]）が利用でき、従業員の利便性にも寄与します。

ゼロトラストは、デバイスの管理もできる… 続きを読む