脱IT初心者「社長の疑問・用語解説」（第58回）

ジ・エンドにさせない「エンドポイント」

2022.10.12

カタカナや略語ばかりでなかなかなじめないIT用語だが、今やITは経営に欠かせない。IT初心者の社長にも、分かりやすく理解できるようにITキーワードを解説する本連載。今回はセキュリティ対策の肝となるエンドポイントだ。

「社長、わが社も社外でパソコンを使う社員が増えてきたので、エンドポイントの対策を強化しませんか」（総務兼IT担当者）

「エンドユーザーであるお客さまを大切にするのはわが社の原点だ。どんどんやりなさい」（社長）

「エンドは同じでも、ユーザーでなく『ポイント』です。例えば、社員が業務で利用するパソコンやスマホ、タブレットなどをIT用語ではエンドポイントと呼びます。そのエンドポイントを守ることがますます重要になっているんです」

「よく分からんが、とにかくエンドをきちんと守ることが大事というわけだな。ワシが理解できるように説明しなさい」

事前と事後の両面で端末を守る

エンドポイントは末端の意味です。IT分野ではネットワークの末端にある端末（パソコンやタブレット、スマホなど）や機器をエンドポイントと呼んでいます。サイバー攻撃が深刻化する中、社員が利用するパソコンやタブレットがウイルスに感染しないための事前対策が必須です。万一、感染してしまった場合の事後対策も欠かせません。事前・事後の両面からエンドポイントのセキュリティ対策を考える必要があります。

Q エンドポイントが注目される理由は何でしょうか

営業活動に加え、テレワークやリモートワークなど社外で端末を利用する機会が増えています。サイバー攻撃に遭うリスクが高まっているため、端末ごとにセキュリティ対策を行うエンドポイントセキュリティが注目されているのです。

Q エンドポイントセキュリティ対策にはどんなものがありますか

代表的な対策にアンチウイルス対策があります。定義ファイルでウイルスかどうかをチェックするアンチウイルス対策製品が数多く提供されています。ただ、定義ファイルにない未知のウイルスはチェックをすり抜けてしまう恐れがあります。そこで、パソコンなどの挙動や振る舞いなどをチェックして未知のウイルスを検知・駆除する次世代アンチウイルス対策と呼ばれる製品・サービスも登場しています。

Q 対策の注意点はありますか

事前対策の他、端末に侵入してしまったウイルスを検知・削除する事後対策ができる製品やサービスも検討しましょう。事後対策では、侵入してしまったウイルスの不審な動きを検知したり、ウイルスを削除したりできる運用面が重要になります。外部のセキュリティ運用サービスの利用も有効です。事前対策や事後対策ができる製品・サービスの選定など、セキュリティに詳しいITサービス事業者に相談するといいでしょう。

ひとごとではないサイバー攻撃

「社長、エンドポイントについて、理解していただけましたか。社員が社外で使う端末のセキュリティ対策を強化しましょう」（総務兼IT担当者）

「セキュリティ対策が必要なのは分かったが、サイバー攻撃はそんなに深刻なのか」（社長）

「競合のA社ではテレワーク中の社員の端末がウイルス感染して、復旧するまで大変だったみたいですよ」

「そうか。事業がジ・エンド（終わり）とならないためにも、端末のセキュリティがポイントというわけだな」