セキュリティ対策虎の巻（第7回）

世代管理のデータバックアップでランサムウエア対策

2017.05.24

パソコンやサーバーに保存したファイルを暗号化して使えなくし、データ復元のための身代金を要求するランサムウエア（身代金要求型ウイルス）の被害が広がっている。ランサムウエアに感染するとその従業員のパソコンだけでなく、ネットワークにつながれた、オフィス内にある他のパソコンやサーバーも感染する恐れがある。

新種・亜種のランサムウエアが続々と発生

ランサムウエアが厄介なのは、端末の感染源を駆除しても暗号化されたファイルの復元が難しいことだ。データを復元するツールも情報セキュリティ会社などから提供されているが、あらゆる種類のランサムウエアに有効とは限らない。また、攻撃者に身代金（ビットコインなどの電子マネー）を支払っても、ファイルを復元できる保証はないのが実情だ。

さらに、ランサムウエアは多種多様に変化し続けている。最近では、徐々にファイルを削除していき、身代金をつり上げていく亜種（改造タイプ）のランサムウエアも発見された。ランサムウエアに限らず、新種・亜種のコンピューターウイルスは日々増殖し続けている。場当たり的な対応では、もはやデータを守れない。

そこで、有効な対策のひとつがデータバックアップだ。万一、データが暗号化されたり、破壊されたりしても、感染前のデータをバックアップしていればスムーズな復元が可能だ。ランサムウエア対策だけでなく、機器トラブルや停電によるデータ消失、誤操作によるデータ改変、管理ミスによるデータ消失などのリスクにも対応し、業務継続に必要なデータを保護できる。

意外と厄介なデータバックアップの最適解… 続きを読む