輸送経済
THE YUSO-KEIZAI

第3475号　1949年4月23日（第三種郵便物認可）

6/28
2022年
（令和４年）
（毎週火曜日発行）

発行所　輸送経済新聞社 ©
本　社　☎03（3206）0711㈹
編集企画部　☎03（3206）0713㈹
営業部　☎03（3206）0717㈹
中部支社　☎052（385）8001㈹
関西支社　☎06（6449）5021㈹
URL:http://www.yuso.co.jp
E-mail:yk@yuso.co.jp
発行者　佐藤　周

サイバー攻撃の標的に
復元する仕組み構築が鍵

物流電子データ

企業では業務の効率化のために従来、紙で管理していた業務に関わる情報を電子化する取り組みが進んでいる。一方、電子データが増える中でサイバー攻撃（＝3面コラム「ことば　教えて！」を参照）を受けるリスクも高まっており、物流企業も例外ではない。セキュリティー対策の専門家は「バックアップデータで元の状態に短時間で戻す仕組みを構築することが重要」と話す。（遠藤　俊）

物流ではDX（デジタルトランスフォーメーション）の一環で、紙の保管書類を電子データに置き換える動きが進む。関東の食品物流企業の担当者は「社内サーバーで一括で管理できる」と話す。九州の中堅物流企業のシステム担当者は「配送依頼、貨物、輸送といった業務全般の情報を電子化し、全体の効率化につなげている」とする。大手倉庫会社の担当者は「リモートワークが広がる中で、データ共有がしやすく利便性を感じている」。

一方、別の九州の中堅企業トップは「膨大なデータをどう安全に保管するか検討しなくてはならない」と話す。多くの場合、データ活用にはインターネット接続が不可欠で、常にサイバー攻撃を受けるリスクがある。

例えば関東の３PL企業は昨年、拠点内のサーバーに不正アクセスを受け業務が一時停止した。別の大手は運用するパソコンに不正アクセスされメールが閲覧された。今後、企業の保有データは増加が見込まれ、セキュリティー対策の充実が欠かせない。

攻撃者は弱点から侵入する

セキュリティー対策に詳しいデロイトトーマツグループの佐藤功陛パートナーは「まずは社内のシステムにアクセスできる機器の把握が必要」と話す。悪意ある攻撃者は社内システムに入ることができる端末のソフトウエアの弱点を突いて侵入し、データの窃取や改ざん、暗号化を狙う。ソフトウエアを更新し弱点を修正することで侵入を防げるが、「更新作業には業務を止める必要があり、手付かずになっているケースも少なくない」（佐藤パートナー）。

さらに、対策を実施しても万全ではない。「新しい弱点が発見され攻撃される可能性がなくなることはない」（同）。そこで鍵となるのが、被害を受けてもデータを即座に復旧できる体制の構築。例えばIT企業が提供する、バックアップから瞬時に復元する製品を導入することは有効な手段。外付けハードディスクなどの記録媒体に保存する方法もある。「日頃から復元の作業手順を訓練することも効果が期待できる」（同）。

万一、情報漏えいした場合には、回収不可能だ。信用回復のためにも迅速な業務復旧と再発防止策が求められる。

データは今後、ますます企業の成長を支える要因になる。守り抜くにはセキュリティー対策を見直し、コストと時間をかけて拡充することが大切になりそうだ。

近年のサイバー攻撃の主な手口の流れ

①社内のシステムに侵入できそうな弱点を持つ機器を探す

↓

②発見した弱点を持つ機器から社内システムに侵入

↓

③データの窃取・改ざん・暗号化を行う