サイバーセキュリティ最前線

バックアップデータだけでなく最適な「レジリエンス」の確立が重要!!

アスクルやアサヒグループホールディングスで生じたランサムウェアの大規模被害事例の全容が判明するにつれ、情報システム関係者の間で「バックアップデータからシステムを早期に復旧できるのか」という点が懸念されている。そこで、今号ではそのあたりの最新事情と対策について紹介したい。

バックアップだけでは難しい

アスクルはランサムウェア（身代金要求型ウイルス）の被害に遭ってから復旧にいたるまで約3カ月もの時間を要した。なぜそこまで時間がかかったのか。その理由のひとつとして、バックアップデータもランサムウェアの影響で暗号化されており、その復旧に膨大な時間がかかったといわれている。アサヒグループホールディングスは現時点でバックアップデータの被害について言及していないが、情報システム関係者の間では「安全性やシステムの整合性の確認のため、復旧に期間を要しているのではないか」と推察されている。

では、一般的な傾向はどうなっているのか。ランサムウェア被害企業へのアンケート調査（警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」）の結果を見ると、バックアップデータを取得しているのが51件、取得していないのが2件であるのに対し、復元可は7件、復元不可は41件となっている。復元できなかった理由としては、アスクルのようにバックアップデータ自体が暗号化されていた場合のほか、復旧を前提とした設計や事前確認が十分でなかったケースもある。

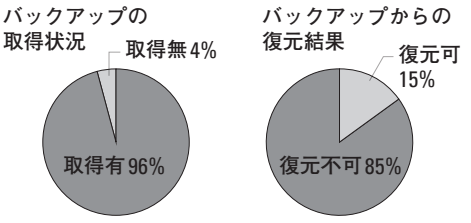
攻撃対象がサーバーに

もちろん、ランサムウェア対策として、バックアップデータの取得は不可欠。とくにこれまではそれぞれが使っているPCが狙われる事例が多かった。その場合はオフィス系ソフトの文書ファイルなどが被害に遭うことが多く、これらのバックアップを取って別の場所に保管することが賢明だ。しかし2023年頃からランサムウェアの被害はサーバーに移行しており、バックアップだけではスムーズに復旧することができなくなってきている。この点について、セキュリティ会社の㈱ブロード（東京都千代田区）は「業務上使用しているデータだけでなく、関連システムやネットワークや通信状況との整合性も含めて検証しなければならず、戻せないこともある」と指摘する。つまり、たんにバックアップデータを取得するだけでなく、システム設計の段階から復旧時の手順確認やテストを入念に行っておく必要があるというのだ。

そのため、ブロードはランサムウェアなどの被害に遭わないようにする「対策」に加え、システム障害時にも事業を継続させる「レジリエンス」（システム被害の影響を最小化し、復旧をスムーズに行う能力）が重要だと提唱する。そして、システム障害時にも業務継続を実現するNeverfail社の「コンテニュイティエンジン（CE）」などが有用なソリューションになると。具体的には「すでに稼働中のシステムであっても、シンプルな手順で組み込むことができるし、有事の場合も数分単位で自動切り替えが完了し、業務を継続することができるようになる」そうだ。

これからは「レジリエンス」も視野に入れたセキュリティ環境の確立が重要になりそうだ。

図表 ランサムウェア被害企業へのアンケート調査
（バックアップデータの取得の有無と復元の可否について）の結果



出典:「令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について」（警察庁サイバー警察局）を参考に編集部が作成