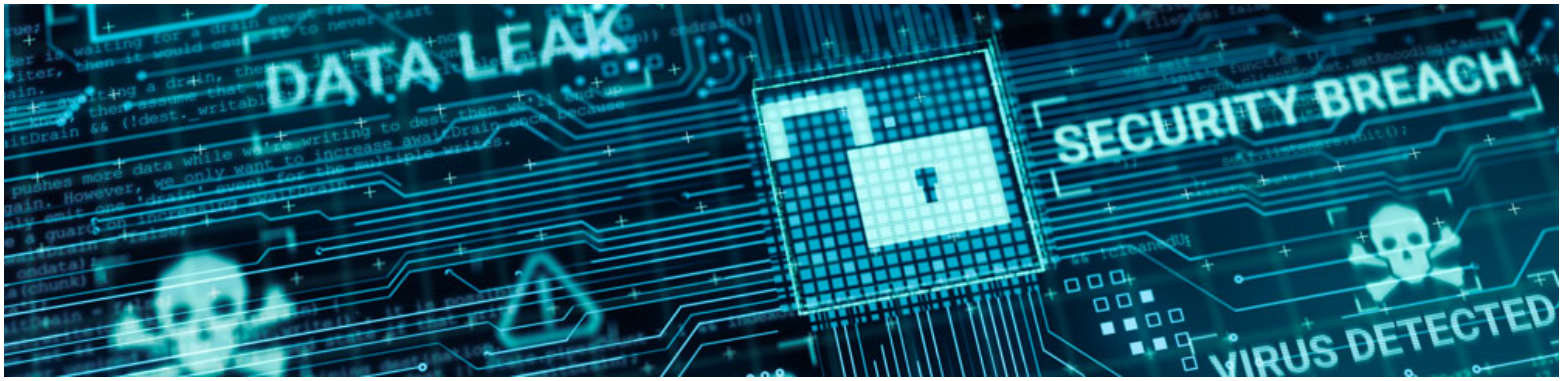
SMEレジリエンス 情報セキュリティ版 Vol.002
Resilience Information
発信日:2024年11月11日 発信部署:中小企業セグメント営業部
リスクコンサルティングユニット
No.031-24-R005

事業活動存続のカギとなる“情報資産のバックアップ”について

昨今のサイバー攻撃の増加やランサムウェアの流行により、企業や団体などにおいて**“バックアップ”**の重要性の認識が格段に上がっています。
今回は、**“情報資産のバックアップ”**についてお話いたします。

●転ばぬ先の杖として

企業で運用管理している情報資産は、取引企業情報、営業秘密情報、在庫データ、注文データ、経理情報、マニュアルや社員情報など多岐にわたります。
それらの情報にアクセスできなくなったり、消失してしまったりすると、企業の事業の継続にも影響を及ぼします。
バックアップを行うことは、情報資産保護の基本となります。
情報資産をバックアップすることにより、データファイルやシステムの復旧が可能になり、事業の継続を可能にします。



利用中の情報資産に以下のような問題がある場合、事業継続困難となることも。

①バックアップがなかった。
②バックアップは存在したが、そのバックアップデータ自体が暗号化されていた。
③暗号化されていない利用可能なバックアップデータがあったが、
適切に復旧作業を行うことができなかった。

②のケースでは、
バックアップデータを作成する過程で、元となるデータファイルが既にランサムウェアに感染した結果、ファイルが暗号化されており、そのファイルをバックアップ側に取り込んでしまうことで、復旧に使うためのバックアップファイル等も暗号化されたファイルになってしまった事例がありました。

ところで、バックアップの運用については、バックアップ対象、頻度と方式、保存期間、データの重要度・用途、保管媒体の種類、保管場所などを考慮して行う必要があります。これらの中でも“頻度と方式”についての検討は重要ポイントです。

バックアップを考えた時、１週間単位で行う、１ヶ月単位で行うなど、頻度（時間的間隔）の決定が必要です。過去に遡って復旧する必要がある場合、フルバックアップ、差分バックアップ、増分バックアップなど、方式を検討しバックアップ取得日（世代）を遡って復旧できるように検討しましょう。“世代管理”についてここでは深く触れませんが、保存されたデータの世代を遡っての復旧作業を意識し、あらかじめ頻度と保存期間なども考慮した上で、効率的で有効なバックアップ方式を決めてバックアップ運用を実行する必要があります。

また、前述③のような事態とならないように、復旧するシステムの優先度をあらかじめ設定し、事前にバックアップからの復旧手順の確認や復旧訓練をしておくことも重要です。

●3−2−1ルールでバックアップ

バックアップトラブルの解決策のひとつになるバックアップの3−2−1ルールは、組織がデータをバックアップする際に、あらゆるデータ消失シナリオに対応するために組織が実践すべきとされている“データバックアップの考え方・ルール”です。

バックアップの3−2−1ルールとは、
①バックアップデータを3つ以上保有する。
②2つの異なる媒体にデータを保管する。
③バックアップデータの１つはオフサイト（遠隔地/クラウドなど）に保存する。

組織に合わせた最適なバックアップ方法を3-2-1ルールの視点から導入検討すると良いでしょう。

図：内閣官房内閣サイバーセキュリティセンター【インターネットの安全・安心ハンドブックVer 5.00＜中小組織向け抜粋版＞】より
https://security-portal.nisc.go.jp/guidance/handbook.html

AIG損害保険株式会社
〒105-8602 東京都港区虎ノ門4-3-20
03-6848-8500
午前９時～午後5時（土・日・祝日・年末年始を除く）
https://www.aig.co.jp/sonpo
お問い合わせ・お申し込みは