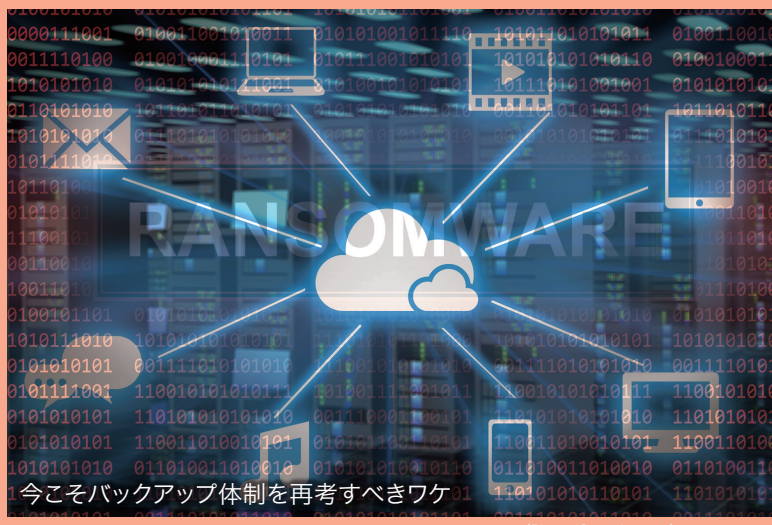
「取ったら終わり」では論外 ランサムウェア大流行時代のバックアップを再考する

デジタルトランスフォーメーション（DX）の機運が高まる中、ビジネスにおけるデータは「企業の資産」と呼ばれるほど重要性が増している。同時にデータを狙うランサムウェアが猛威を振るっており、企業は災害や障害に加え、マルウェアからもデータを保護しながら、万が一のときは円滑に復旧できるバックアップ体制を構築しなければならない。今求められているバックアップの最適解を探る。



今こそバックアップ体制を再考すべきワケ

(Photo/Getty Images)

ランサムウェアで浮き彫りになるバックアップ強化の必要性

DXの取り組みが加速しており、これまで紙の資料や手作業に依存していた業務をデジタル化したり、デジタル技術を活かしてビジネスモデル自体を変革しようと取り組む企業が増えている。それに伴い、企業が保有するデータはその重要性を増しつつ、量も増加の一途をたどっている。

その中で企業に課せられた課題は、「いかにデータを保護するか」である。災害や障害に備えておくこともちろん大切だが、近年では「ランサムウェア」の存在も無視できない。

ランサムウェアが侵入すると、データを暗号化するなどの障害を引き起こし、その解決のために身代金を要求する。そもそもの侵入を防ぐセキュリティ対策の強化はもちろん重要だが、100%防ぐことは難しい。現実的な対策としてはまず「攻撃されるかもしれない」という前提に立った上で、バックアップデータからいかに確実に、かつ迅速に復旧するべきかを考える必要がある。

しかし、最近の巧妙化するランサムウェアは、本番データだけでなくバックアップデータも狙うことで、復旧を阻止しようとする手口も現れている。単に「バックアップを取ったから安心」とは言えなくなった状況下で、企業はどのようなバックアップ体制を構築すれば良いのだろうか。

改めて見直したい、バックアップデータの「二次保存先」

先述のように、いまやバックアップデータすらもランサムウェア攻撃の被害に遭うケースがある。「そのため、バックアップは一次保存だけでは不十分です。企業にはデータを二次保存するためのストレージを確保することが求められています」と語るのは、システム・データ保護ソリューションを展開するアクティファイの取締役　営業本部　本部長 佐藤 尚吾氏だ。

では、バックアップデータの二次保存先をどのように考えるべきだろうか。まず、ランサムウェアによる感染は、守るべきファイルがランサムウェアの侵入した環境の近くに存在するほどリスクが高い。たとえば、ある拠点のPCからランサムウェアが侵入した際、そのPCが接続しているネットワークドライブなどは真っ先に感染が広まってしまうだろう。

そうしたリスクを避けたいという目的や、そもそも自社でITインフラを管理する負荷を低減したいという意図から、最近ではデータの保管先にパブリッククラウドのストレージを選択する企業も増えてきた。しかし、クラウドも万能ではない。特に大容量のデータを保有する企業では、データ転送が課題になることもある。

「現在では多彩なクラウドソリューションが登場しており、

二次保存先の選択肢は以前よりはるかに広がりました。しかし、大容量データを転送するための通信環境が実用レベルに追い付いていないという現状も見受けられます。多くの中小企業はインターネット回線を1回線しか保有していないため、大容量のバックアップデータをクラウドに転送すると、日常業務のデータの送受信に多大な影響を及ぼしかねません」（佐藤氏）

またクラウドの懸念点として、大容量のデータの転送を高い頻度で行うと、トラフィック課金のパブリッククラウドのサービスでは、想像以上にコストが高くなってしまうケースもある。そのほかにも、大量の機密情報を持つ企業の場合、社内のセキュリティポリシーの制約上、そもそもクラウドを活用できないということもある。

こうした背景もあり、依然としてオンプレミスが有利な選択肢となる部分も多い。オンプレミスにストレージアプライアンスを導入した場合、大量のデータをある程度長期にわたって保存する前提であればパブリッククラウドよりもコストを押さえることが可能だ。また、オンプレミスのバックアップでは、上書き禁止や物理的にネットワークから切り離すことでランサムウェアによる感染リスクを低減するテープストレージにも注目が集まっている。

「ランサムウェアなどの脅威からデータを守るために、どのように保管すれば良いかは企業の業種や規模によって多種多様であり、一概に何が正解であるか決めることはできません。オンプレミスやクラウドを含めたさまざまな選択肢を検討した上で、それぞれの『いいとこ取り』をしながら運用体制を構築するべきです」（佐藤氏）

迅速かつ確実なデータ復旧を支援する「ActiveImage Protector」

まさにこうしたニーズに応えるのが、アクティファイの提供するシステム・データ保護ソリューション「ActiveImage Protector」である。

Windowsの物理／仮想サーバのバックアップを担う同ソリューションは、OS、データを含むボリューム、ディスク単位のバックアップから、ファイルやフォルダ単位のバックアップにも対応。保存先の選択肢も幅広く、ローカル接続のHDDのほかに、NASやUSBストレージ、LTOテープストレージ、Amazon S3（およびその互換オブジェクトストレージ）、SFTPサーバなどを利用することができる。

アクティファイ 取締役 営業本部 本部長　佐藤 尚吾氏

また、バックアップデータを複数の環境に保存する運用を企業が行うにあたり、もう1つ注意するべきことが、データのリカバリである。企業のビジネスがデータやデジタルツールに依存する今日、データをいかに素早く必要な環境に復旧させて業務を再開できるかは重要なポイントである。

同ソリューションは、「全てのバックアップデータを素早く確実に復元させる」というコンセプトのもと、多くの企業が安心して使えるように配慮したさまざまな特長を備えている。その例が以下である。

1.ユーザー企業の要望に応えた扱いやすさ

物理サーバ／仮想サーバを問わず、わかりやすい操作性・使い勝手を実現している。ネットワークの設定を除けば、ウィザードに従って任意のディスクやファイルなどを選択するだけで、バックアップデータの取得やリカバリが容易にできる。

バックアップのスケジュールに関しても、曜日を指定するなど自由に設定可能だ。1つのプロファイルに対して複数のスケジュールを作成できるため、たとえば週単位でバックアップしていたものに対して「毎月1日だけはフルバックアップを行う」という設定を加えることもできる。

「市場に流通しているバックアップ製品の多くは海外メーカー製品である中、国産製品であるActiveImage Protectorは、国内ユーザーの声やニーズを製品に反映させながら機能追加を続けてきました。もちろん、機能が豊富になると操作のわかりやすさが損なわれるリスクがあります。そのため、当製品ではそのバランスに配慮しながら、ユーザーが操作ミスなく確実に使いこなせることを念頭に開発を続けてきました」（佐藤氏）

2.エージェントの有無を問わず仮想マシンをバックアップ

仮想マシンをバックアップする際は、ActiveImage Protectorを仮想マシンに直接インストールして運用する、いわゆるエージェントベースのバックアップ方式のほかに、直接のインストールが不要なエージェントレスバックアップ方式を利用でき、企業はこれらの2種類から用途に応じて選んで利用できる。後者の方式を用いれば、ソフトウェアをインストールできないレガシーOSのサーバ（Windows Server 2003など）でもバックアップを行うことができるため、よりさまざまなシステム構成に対応できる。

一般的には、HCI（Hyper-Converged Infrastructure）で稼働するVMware vSphere上の仮想マシンは、vCenterを経由してバックアップを取得するが、仮想マシンが別なホストに移動した場合、増分バックアップが継続できない。

ActiveImage Protectorではエージェントの有無に関係なく、仮想マシンが別なホストに移動しても、増分バックアップを継続できる。vCenterへの登録も不要。保存先のディスクを選択するだけで良いため、別途バックアップサーバを構築する必要もない。

3.保存先の柔軟性とスピード

ActiveImage Protectorは、先述のようにAmazon S3互換のオブジェクトストレージへ直接バックアップできる。パブリッククラウドへの保存の場合、そのスピードが気になるところだが、「一般的な転送速度で15GBのデータをクラウドにバックアップすると、およそ20～30分かかりますが、ActiveImage　Protectorなら5分程度で完了します」と佐藤氏は自信をのぞかせる。

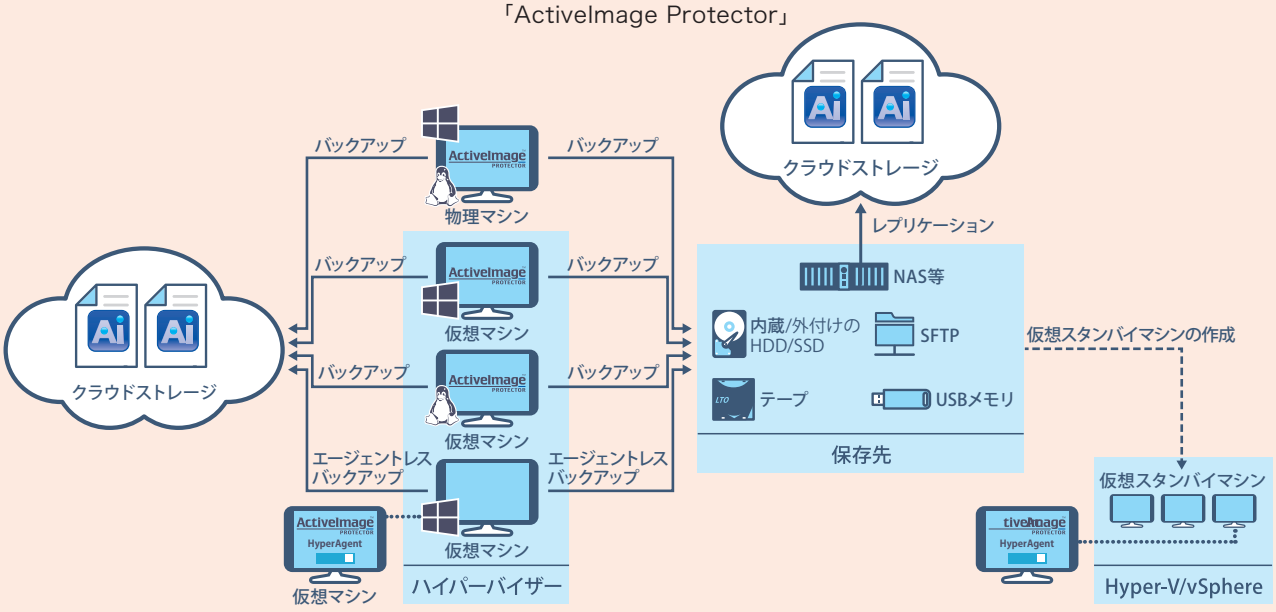
バックアップの保存先についてもう1つ特筆すべきは、同製品の最新版で追加されたLTOテープストレージ対応である。LTOテープストレージは大容量データの長期保存に適しているほかに、メディアに保存したデータを上書き禁止にしたり、社内ネットワークから物理的に容易に切り離したりできるため、ランサムウェアによる攻撃を見越した強固なデータ保護対策を実現できる。

ActiveImage Protectorはコストパフォーマンスにも優れており、特に仮想環境用のエディションである「Virtual」においては、1ホスト1ライセンスで同一ホスト上の仮想マシンを数量に制限なくバックアップできるため、多数の仮想マシンを運用している場合、大幅なコスト削減が見込める。また、ランサムウェア対策を含むBCP対策、DR対策として、遠隔地へのバックアップのニーズも高まっているが、その際にバックアップデータを転送するためのレプリケーションソフトも無償で提供している。

「サポートも製品の一部」という考えのもと、問題を迅速に解決

昨今ではシステム環境はより複雑化している。その中で仮想マシンのバックアップをさまざまなプラットフォームで行うことで、何らかのトラブルが発生することも少なくないだろう。そうしたトラブルに対してもActiveImage Protectorであれば迅速に解決できる。何よりの強みは

構成が複雑になりがちな環境でも、迅速かつ確実なシステム・データ復旧を実現する「ActiveImage Protector」



ソリューションに付随する強力なサポート体制だ。

「アクティファイではサポートも製品の一部と考えているため、永続ライセンスの購入価格*には初年度のサポートも含めています。弊社では相談に対して迅速に対応する電話サポート体制を整えており、問題が発生してから解決までのリードタイムの短さも強みです」（佐藤氏）

＊例：仮想環境用のエディション「Virtual」の場合、19万8000円（税別）

電話サポートだけでは解決できない不具合が発生したときも、過去には現地に直接出向いて詳細な事象を確認した上で、自社環境で不具合を再現し、修正パッチを開発したこともある。まさにこうしたきめ細かな対応こそが、同社が国内の多くのユーザー企業やシステムインテグレーター（SIer）から信頼を得てきた理由であるだろう。

ランサムウェアに感染するも、素早く復旧した事例

ActiveImage Protectorには豊富な導入実績がある。中でも、ランサムウェアの感染から迅速に復旧できたある企業の事例は象徴的だ。

東京に本社を構えるこの企業は、1人の管理者が物理サーバ10台と、同サーバ上で動作している仮想マシン40台をメンテナンスしている。ActiveImage Protectorを使い、物理サーバ（仮想マシンを含む全体）のフルバックを月1回、増分バックアップを毎日取っていた。

同社はある日ランサムウェア攻撃に遭い、ファイルが暗号化されてアクセスできなくなっていることに気がついた。ネットワークを介してランサムウェアに侵入されていたため、複数のサーバが感染している可能性があった。担当者は被害拡大を防止するため、全てのサーバを停止。共有フォルダやメールシステムだけでなく、基幹システムにも影響があったことから、業務の継続が困難になった。担当者はActiveImage Protectorを使い、サーバを感染前の状態に復元しようとしたものの、東京本社内のバックアップデータ自体もほとんどがランサムウェアによって暗号化されて使えなくなっていた。

そこで同社では、ActiveImage Protectorのオフサイトレプリケーション機能によって大阪に転送してあった感染前のバックアップデータを使い、復旧作業を実行。その結果として、感染判明翌日の業務開始までにはサーバはほぼ全て復旧し、社員が業務を遂行できる状況になった。

このほかにも、ある企業ではWindows Update実行後にブルースクリーンが発生し、OSがクラッシュしたものの、ActiveImage Protectorを使ってわずか5分でシステムの復旧に成功。またある工場では、トラブル発生時に専門知識を持たない現場のスタッフがActiveImage Protectorを使って、自力でリカバリした例がある。これらはまさに同ソリューションの使い勝手の良さを象徴した事例だ。

どんな環境でも短時間かつ容易にデータリカバリを目指すアクティファイ

バックアップからのデータリカバリは、サイバー攻撃やハードウェアトラブルといった障害で、急きょ対応せざるを得ないことがほとんどだ。とはいえ前任者からリカバリ方法を引き継ぎされていないことも珍しくなく、また保守契約を結ぶSIerがすぐに対応してくれるとも限らない。急な事態に備えて、エンドユーザーが自己解決できる操作性は極めて重要だといえる。

まさに、こうしたニーズに応えるのがActiveImage Protectorだ。

「創業以来、『どんな環境でも完全にシステムおよびデータを復旧できるソリューションを提供する』ことを掲げて開発を行ってきました。短時間かつ容易にデータを復旧させてビジネスの生産性を上げることが、バックアップ・リカバリの果たすべき役割だと考えています」（佐藤氏）

また同社では、ネットワークセキュリティやストレージ製品を取り扱う企業とも協業しているため、顧客が希望するシステム構成に応じて、セキュリティ対策やITインフラなども含めた提案も可能だ。データが資産となる昨今において、強固なデータ保護対策を実現したい企業は、ぜひアクティファイに相談してみてはいかがだろうか。

お問い合わせ先

Actiphy

株式会社 アクティファイ　〒101-0035 東京都千代田区神田紺屋町8番 NCO神田紺屋町
TEL：03-5256-0877　FAX：03-5256-0878　https://www.actiphy.com　sales@actiphy.com