「生き残りのためのバックアップ論」

いつまで続く？ランサムウェアの脅威。 電帳法対策も。

依然として猛威をふるうランサムウェア。ひとたび感染しようものなら、ほぼ確実にシステムは使用不能になり、その被害は甚大なものとなる。これまでにも様々な対策が講じられてきているが、完全に防ぎきることは難しい。そこで改めて不可欠な存在となるものが、バックアップである。

感染によりファイルが暗号化されても、バックアップがあれば復旧が可能となる。これが現在、もっとも確実なランサムウェア対策となっているのが実情だ。もちろん、ランサムウェア以外にも、コンピューティングを取り巻く環境には、様々なリスクが存在している。あらゆることに備えていく意味で、バックアップの役割は重要である。

本稿では、ランサムウェア対策における「バックアップの肝」について紹介する。長年、国内企業として、システム/データ保護ソリューションを手掛けている株式会社 アクティファイの佐藤氏に取材し、最新事情も絡めて詳しく解説をいただいた。尚、実際に用いているのは、同社が開発・販売するActiveImage Protectorだ。参考にしていただきたい。

目次

■改めて考える「バックアップとは何か」

■猛威をふるい続けるランサムウェア [1] [2]
[1] 完全な防御はできない
[2] クラウドでも感染! 対策は？

■昨今におけるバックアップの注目ポイント [1] [2] [3]
[1] クラウド上でより使いやすく
[2] LTOの有効活用
[3] 2次、3次の保存先を確保

■電子帳簿保存法による経理データへの対策

■ユーザーもスキルアップ？

改めて考える「バックアップとは何か」

まずはバックアップについて、改めて考えてみたい。誰もが思い浮かべるのは、「何らかの事情で失ってしまったファイルを取り戻したい」という状況だ。この「何らかの事情」として考えられるのは、以下のようなものがあるだろう。

・システム不具合
・ウイルス感染
・デバイスの故障
・人的な操作ミス
・災害

残念ながらハードウェアにも寿命があり、絶対に避けては通れない。いつかは使えなくなる日がくる。もしものハードウェアトラブルの場合でも、データが正しくバックアップされていれば、仮に業務に影響が出たとしても、致命的なダメージは避けられる。また、ヒューマンエラーも否定できない。誰にでも、間違って必要なファイルを消してしまった経験はあるだろう。企業でも個人でも、ハードウェアの進歩に呼応し、データは増大する一方である。更にDX化の推進により、今後もデータは、より一層増え続け、そして重要性も高くなっていく。それに伴うリスクを回避する

のが、バックアップと言えるだろう。
バックアップについて、佐藤氏は次のように語る。

「想定すべきシチュエーションは、多岐に渡ります。“従業員がデータを持ち出した”“操作ミスでデータを失った”“ハードウェア障害が発生した”といったリスクから、如何にデータを守るか。もちろん、ランサムウェアの脅威も依然としてあります。ランサムウェア対策としてEDR（Endpoint Detection and Response）などを導入するのも良いですが、その前にバックアップ運用がしっかりとできているかどうかが重要です。バックアップの保存先を複数持たせて分散化をおこなうことで、ランサムウェア対策/災害対策などに幅広く対処することができます」

株式会社 アクティファイ
取締役営業本部長
佐藤 尚吾氏

「ランサムウェア対策は、バックアップと組み合わせることで効果が高まります。バックアップは、災害対策にも、ヒューマンエラーへの対策にもなります。多様なニーズに対応可能ですので、コストパフォーマンスに優れます。もちろん、ランサムウェアも重大な懸案事項の1つですが、それを抜きにしても、バックアップがより重要になっていくことは間違いありません」

「また、国が掲げる働き方改革に呼応し、少ない工数で効率良く運用でき、現場で働く人たちの負担軽減に寄与する。こういったことも、バックアップに求められる役割と考えています」

猛威をふるい続けるランサムウェア [1] [2]

[1] 完全な防御はできない

ランサムウェアについては、すでにマスコミなどの報道でご存じの方が大半であろう。この10年ほどで、実に多くの被害が報告されている。感染したコンピューターやLANのすべてのファイルを暗号化して身代金を支払うよう警告を発し、システムを使用不能にする。セキュリティベンダーによるソリューションをはじめ、様々な対策が講じられているが、完全には防ぎきれていないのが実情と言えるだろう。
佐藤氏は次のように語る。

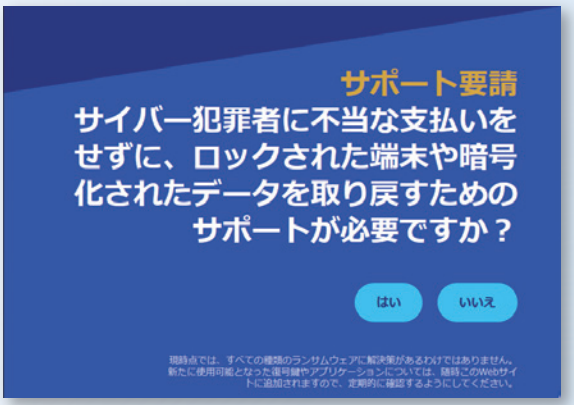
「新しいランサムウェアに対し、ふるまい検知で対応する技術も進歩していますが、100%の防御は不可能です。トロイの木馬型などもあるようで、今後も情報収集は不可欠です」

「完全に防ぐことができない以上、最終手段としてのバックアップ運用は今後更に重要さを増してくると思います」

尚、ランサムウェア対策として、「The No More Ransom Project」といったものがある。
佐藤氏によれば、

「このサイトでは、ランサムウェア感染データの復号ツールを提供しています。代表的なランサムウェアに対応し、現時点で170位の復号ツールがあります。しかし、復元を保証するものではないとあり、実際にどの程度の有効性があるかは不明な部分もあります」

とのことだ。
また、国内でも、例えば「警察庁サイバー警察局」が「ランサムウェア被害防止対策」というものを掲げている。
これについても、佐藤氏は次のように語る。



The No More Ransom Project（https://www.nomoreransom.org/ja/index.html）

「最終的には“被害を如何に軽減するか”の対策です。具体的には、

・バックアップを取りましょう
・アクセス権を制限しましょう
・ログを見ましょう

となっています。しかし、2つ目の項目であるアクセス権の制限ですが、実際にこれをしてしまうと、今までActiveDirectoryでログインすればすべてのサーバーにログインできていたものが、1つ1つのサーバーにログインする必要がでてしまい、非常に利便性が損なわれます。セキュリティレベルを最高に保ちたいのであれば、それこそ“電源を入れないでください”や“すべて紙でやりましょう”となってしまう。セキュリティの問題を議論すると、

こういった極論になってしまいがちです」

「しかしながら、企業の運営にデータは不可欠です。弊社が提供しているシステム/データ保護ソリューションは、BCP（事業継続計画）対策と言えます。クラウドに保存すればDR（ディザスタリカバリー）も兼ねられます。如何にして企業活動を継続していくか、長年に渡りSIerさんと検討を重ねてきました。実際にエンドユーザーの事業を様々なカタチで支えているSIerさんに、今後も更なる情報提供や運用方法の提案をおこなっていきます」

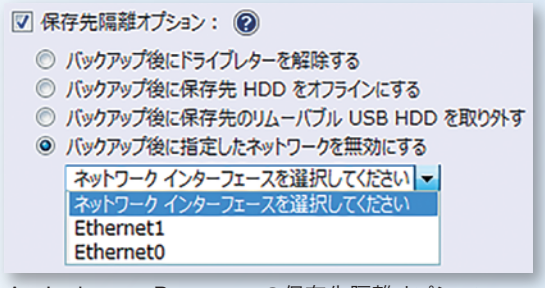
[2]クラウドでも感染！ 対策は？

佐藤氏によれば、SIerにすら、「クラウドのファイルはランサムウェアの感染被害に遭わない」といった過信が存在するとのことだ。確かにローカル/ネットワークドライブは短時間で感染してしまう。また、UNC接続のNASなども多少の遅延はあるものの、最終的には感染してしまう。では、クラウド上のファイルはどうか？　VPN接続の共有フォルダーなどよりは接続に手続きが必要なため、感染の可能性は低いと思われる。更に、オブジェクトストレージのオブジェクトロッカー機能などを使うことで、ファイルの変更自体を許可しない、つまり感染を防止することが可能との見方もできる。
しかし、佐藤氏によると

「確かに、オブジェクトストレージで感染したという話を聞くことは少ないです。しかし、ランサムウェアも進歩していますので、S3パケットにアクセスできるようになれば、オブジェクトストレージでの感染も十分有り得ることです」

とのことだ。
まずは、「クラウドは安全」という考えを捨てることから始めたい。さて、ここからは、ActiveImage Protectorを利用したランサムウェア対策について見ていこう。ActiveImage Protectorには、保存先隔離オプションが実装されており、バックアップの保存先をバックアップ後にアクセスできない状態にすることができる。やり方は4通りある。

(1)バックアップ後にドライブレターを解除する
バックアップ先として指定した保存先ディスク内のボリュームに対して、バックアップ後に自動でドライブレターの割り当てを解除する。次回のバックアップ時には、自動的に再度ドライブレターを割り当てる。

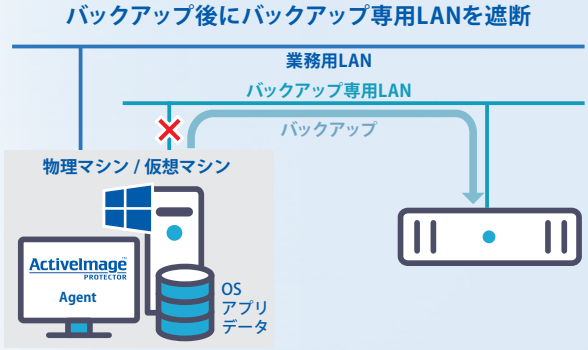


ActiveImage Protectorの保存先隔離オプション

(2)バックアップ後に保存先HDDをオフラインにする
バックアップ先として指定した保存先ディスク自体をバックアップ後に自動でオフライン状態にする。次回のバックアップ時には、自動的に再度オンライン化をおこなう。

(3)バックアップ後に保存先のリムーバブルUSB HDDを取り外す
バックアップ先として接続したリムーバブルUSB HDDをバックアップ後に自動で取り外した状態にする。ただし、USB機器であるため、次回のバックアップ時には、USB HDDを手動で接続して、再度認識させる必要がある。

(4)バックアップ後に指定したネットワークを無効にする
バックアップ対象からネットワーク上の共有フォルダーに接続している特定のネットワークカードを、バックアップ後に自動的に無効化する。次回のバックアップ時には、自動的に有効化をおこなう。この機能を使用する場合、図のようにバックアップ対象マシンのネットワークカードの一方をバックアップ専用のセグメントに接続する。



バックアップ専用のセグメントを設定

バックアップ専用のセグメントに、保存先となるNASなどを接続することにより、バックアップ実行時以外は、社内のネットワークから切断された状態となり、バックアップ保存先であるNASが感染する可能性を下げることができる。
佐藤氏によれば、

「ドライブレターの割り当て解除については、あまり知られていない機能でした。同業のバックアップベンダーにおいても、“ドライブレターを割り当てていない場所にバックアップを保存しておけば安心”という認識があります。しかし、ランサムウェアがUUIDパケットにアクセス可能になれば、ドライブレターの有無に関係なく、ボリュームは感染対象となります。更に、攻撃者が何らかの手段で管理者権限を奪った場合には、これらの対策は意味をなさないことになってしまいます」

と、メリット以外の部分もあるという。
バックアップ先に接続できない状態にするという点がポイントになるだろう。つまり、物理的に遮断されていれば、ランサムウェアと言えど手が出せないのである。
このことからすると、後述するLTOも、かなり効果的な対策になる。LTOのカートリッジは、普段、ドライブから外してロッカー（鍵付き）などに保存されている。この状態であれば、バックアップファイルの感染の可能性は基本的にないだろう。

昨今におけるバックアップの注目ポイント [1] [2] [3]

[1] クラウド上でより使いやすく

ActiveImage Protectorの機能で、クラウド関連のものを紹介したい。In-Cloud Standby機能だ。これは、バックアップイメージからクラウド上にスナップショットを作成する機能である。必要に応じて、作成したスナップショットから仮想マシンとして起動することができる。また、In-Cloud Standbyでバックアップの保存先が拡張され、クラウド上のVLAN内のファイルサーバー、同一クラウド内外のクラウドストレージを保存先として選択可能となっている。

バックアップに求められる要素として、RTOの短縮が挙げられるが、In-Cloud Standby機能やそれ以外にもHyperBoot、HyperRecovery LIVE!機能などを利用することで、より短時間で復旧が可能となる。

ActiveImage Protectorでは、バックアップの保存先としてクラウドストレージもサポートしている。具体的には以下の通り。

・Amazon S3
・Azure Storage
・S3互換のオブジェクトストレージ（Nifty Cloud、Cloudian）
・Wasabi
・Neutrix Cloud Storage

ここで注目したいのは、Wasabiである。Amazon S3互換で、低価格が魅力なオブジェクトストレージである。これまでAmazon S3では価格面で折り合えなかったユーザーでも、利用可能となり得る。

Wasabiについて、佐藤氏は次のように語る。

「低価格オブジェクトストレージのWasabiにも対応しています。ここまで簡単に書き込みがおこなえる製品は他にないでしょう。元々、S3互換ですが、Wasabi用のインターフェイスを弊社で開発しました。また、Neutrix Cloudのオブジェクトストレージに書き込みができるのは、ActiveImage Protectorのみです。このように、独自で小回りのきく開発をしています。更に言えば、オブジェクトストレージをNASと同様に扱うことができます」

「速度を求めるのであれば、費用はかかりますがAWS Direct Connectを使えば良いでしょう。接続ポート1Gbpsでは、上限の100MB/sの96.5%まで可能なオブジェクトストレージもあるようです。高スペックなNASを保存先にするより高速に利用でき、ActiveImage Protectorを使えば、増分バックアップをはじめオンプレミスのNAS同様にバックアップを運用することができます。ディスク容量の追加など冗長化されていることを考慮するとメリットがあります」

Wasabiへのバックアップ画面

現在アクティファイでは、高スペックな国内データセンター環境による新たなストレージサービスの提供準備と、バックアップ保存先としてオンプレミス環境からのシームレスな移行を実現するソリューションの準備を進めているとのこと。

国内企業であるメリットを最大限に生かした総合サービスに発展することを期待したい。

[2] LTOの有効活用

LTO（Linear Tape Open）は、シーゲート、HP、IBMによって開発されたオープンフォーマットのテープデバイスである。現在も規格の改訂が進行しており、より高速化、大容量化が成されている。最新のLTO-9では、無圧縮で容量18TB、転送速度400MB/sとなっている。ちなみにSATAのHDD/SSDは、500MB/s位である。

かつて、テープは遅い、低容量と言われ、佐藤氏によれば今でも疑問視する人が少なくないとのことだ。しかし、その当時から長期保管が可能で、保存用のメディアとしての信頼性は高い。一方、その構造上、ランダムアクセスができないというデメリットもある。ただし、バックアップメディアとしてみれば、有力な選択肢となり得る。

ActiveImage Protectorでは、LTOテープライブラリ内でのテープの移動や再スキャンなど、テーププールとライブラリ管理の強化がおこなわれている。

佐藤氏によれば、

「協業しているタンベルグのチェンジャー付きのドライブとテープは、比較的リーズナブルな費用で導入できると思います。企業データのバックアップ用に10TB以上の保存先として考えた場合、取り外しデバイスであることによるランサムウェア感染対策としての有効性も踏まえると、コストパフォーマンスは悪くありません」

「ActiveImage Protectorでは、起動環境から起動したその時点から、LTOを認識できるようにしています。テープメディアチェンジャーであっても、読み込めばリカバリーポイントの一覧が表示されます。そこからOSごと戻すことができます。以前より随分


LTOドライブとカートリッジ

便利になっています」

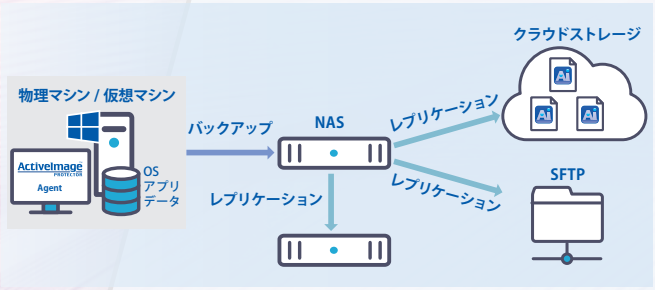
「しかし、ハードウェア機器である以上、故障などの可能性もあるため、複数のテープで管理、または、2次保存先として月次バックアップ用などと、役割を明確にして運用することをお勧めします」

とのことだ。

[3] 2次、3次の保存先を確保

ActiveImage Protectorでは、バックアップの保存先として様々なデバイスに対応している。
具体的には以下の通り。

・ローカルディスク（内蔵/外付け）：ATA/SATA/eSATA/SCSI/SAS/FireWire（IEEE 1394）接続のHDD/SSD、記憶域に作成された仮想ハードディスク
・ネットワークドライブ：NAS（SMB/CIFSファイル共有プロトコル互換のWindows OSの共有フォルダーおよびSamba）/iSCSI/SAN接続のネットワークドライブ
・クラウドストレージ：Amazon S3、Azure Storage、S3互換のオブジェクトストレージ（Nifty Cloud、Cloudian）、Wasabi
・USB接続のHDD/SSD/RDX/メモリ
・LTO（磁気テープ）
・SFTPサーバー



一般的には、ローカルディスクやネットワークドライブが候補となるであろう。
ランサムウェアへの対策を考慮する上で佐藤氏は、

「特にデータのバックアップは分散化が肝となります。1か所の保存先ではリスクが高いです」

と指摘する。
バックアップでよく言われてきた台詞に「バックアップデータは別の場所に保存する」というのがある。火災や天災に見舞われた場合、サーバーと同じ場所に保存していては、同時にバックアップデータも失うことになる。複数拠点で展開する企業であれば、本社以外にも遠隔地の支社にバックアップデータを保存しておくことが望まれる。この時、テープや外付けUSB HDDなどであれば、搬送もやりやすいだろう。
佐藤氏は

「ActiveImage Protectorは、様々な保存先に幅広く対応しています。例えば、LTOがあれば、取り外しデバイスとして利用できます。また、Wasabiでは大きなファイルも保存できますし、データ転送料もかかりません。AWSと比較しても半額です。中でも有効なのは、安価な外付けUSB HDDです。常時接続のNASよりも遥かに安全で、どのような規模の会社でも運用しやすいと言えます」

「いずれにしても、最低でも2重、できれば3重のバックアップがあれば安心かと思います」

と説明する。
つまり「バックアップの2次、3次保存先を確保せよ」ということになる。しかし、小規模企業などでは、別の拠点もなく遠隔地への保存が難しいことも考えられる。そのような場合、佐藤氏によれば、銀行の貸金庫を利用する事例もあるとのことだ。HDDやSSDなどを使えば可能だろう。
最後に、ランサムウェアの新たな脅威について紹介したい。
佐藤氏によると、

「最近、もっとも危険と感じているのは、トロイの木馬型で、ある程度時間が経過してから活動するようなランサムウェアです。この場合、バックアップも全滅してしまう可能性があります」

とのことだ。
トロイの木馬型でなくても、社内LANに侵入され、情報漏洩が陰で進行していることもある。攻撃者はいよいよ奪うものがなくなり、最後の稼ぎとしてランサムウェアを仕込むこともある。状況にもよるが、半年から1年程度潜伏されることになる。こうなると、以前に取ったバックアップ、例えば3か月前のバックアップであっても、すでに感染状態になっている。
佐藤氏は続ける。

「もし、バックアップが感染していた場合、そこからから復元をしても2次災害を引き起こしかねません」（再度のランサムウェアへの感染）

「ActiveImage Protectorに用意されている専用ツールのHyperBootを使い、まずはバックアップイメージから直に仮想マシンとして起動（復元をせずに起動）させ、不審なユーザーが作成されていないか、ランサムウェアに感染していないかなどを十分確認した上で、社内のネットワークに接続するなどの手順を踏む必要があるでしょう」

また、バックアップは長期に渡っての管理も必要になってくるという。この点についても、佐藤氏は実情を訴える。

「“古いバックアップデータでは意味がない”と言う方もいます。しかし、実際にランサムウェアの被害にあった方からは、“例え半年前、1年前の状態でも良いので復元して欲しい”という声も聞えてきます。やはり、こういったことへの対応も必要になってくる

と思われます」

具体的には、年次、月次といったバックアップファイルの管理が必要になってくるだろう。

電子帳簿保存法による経理データへの対応

既にご存じの方も多いと思うが、電子帳簿保存法により、最低でも7年間の経理データの保存が必要になる。法律上は7年だが、実際に企業活動を継続していく上では、永続的に保存することになるだろう。
更に、佐藤氏は、

「帳簿や領収書、請求書などが電子データになると、こういったものにもランサムウェア対策が必要になります。データ保存計画として考えた場合、7年または10年という期間がまずネックになります。一般的なハードウェアのメーカー保守期限の多くは5年程度に設定されています。それを超えた保守が必要な場合には、オブジェクトストレージやテープになります」

「データの電子化が進むほど、ランサムウェアに限らずサイバー攻撃自体をどう回避するかがポイントになります。特に日本社会では、"インターネットに接続したコンピューターはいつ被害に遭ってもおかしくない"という認識そのものが欠けています。誰しもが常に脅威と背中合わせであるということを十分に理解する必要があります」

と説明する。

ユーザーもスキルアップ？

アクティファイのサポート体制についても話を聞くことができた。

「最近のソフトウェアベンダーのユーザーサポートは、効率化の名のもと、Webのみ、つまり、チャットや問い合わせフォームのみといった対応が多いです。これはベンダー側にとっては効率的であっても、ユーザー側からすれば非効率的な話です。弊社では"電話"それも、外部に委託することなく、エンジニアを含む社員が直接の通話でサポート対応をします。また、Webでの対応については、ユーザーの使いやすさを優先し、フォームではなく直接メールで受け付けています」

「弊社にとってもサポートの効率化は課題です。そこで弊社が取り組むのは"ユーザーのスキルアップ"です。電話やメールのやり取りでは伝えるのが難しい、技術的な説明や画面表示の内容については、Webサイトにアップした資料を基に、"何ページのどこがわからない"というようにお伝えいただくことで、効率良くサポートできます」

「仮に、サポートからの返事に2週間もかかることがあっては、現場のストレスは溜まる一方です。問題解決が短時間で済むことはユーザーにとっても大きなメリットです」

と佐藤氏は語る。
同社の製品はSIerがエンドユーザーに納入する。SIerからの信頼を得るには、地道な積み重ねがものをいう。
佐藤氏は以下のように続ける。

「サポートチームでは、エンジニア1人ひとりにサーバーを1台ずつ割り当てています。大容量データに対応すべくディスクも拡張し、64TBのボリュームを用意したりしています。そのような環境で様々な検証をおこなっています」

「今後もサービスレベルは決して落としません。ユーザーの環境に見合った環境がないと相応のサポートはできません。サポートチームも継続的なレベルアップが重要と考えます」

今後も同社の取り組みに期待をするところである。機会をみてまた紹介していきたい。

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