ITmedia エンタープライズ SPECIAL

いつもの方法ではデータを守れない!?

ランサムウェア対策のバックアップで必ず押さえるべき3つの要件

国内でも感染被害が急激に拡大しているランサムウェアは、事業継続を脅かす存在だ。実際に診療データを人質にとられた米国の医療機関が身代金の支払いを余儀なくされた事態も起きている。その対策にはバックアップが有効とされるが、実はランサムウェアの特性を考慮しないと失敗しかねないのだ。

ランサムウェア対策でのデータ保護の重要性

世界的に深刻化しているマルウェアの一種「ランサムウェア」の被害が、国内でも急激に拡大している。情報処理推進機構（IPA）の報告でも、2014 年半ばからランサムウェア感染に関する相談が増加し続けており、沈静化の兆しは一向に見えない。攻撃手法の巧妙さが増す状況では、今後の被害拡大が危惧されている。

そこで IT 部門に求められているのが、ランサムウェア被害を回避するための事前対策である。柱となるのは、ウイルス対策ソフトの導入などを通じた感染の「予防」と、万一に備えたバックアップによるデータの「保護」の 2 つだ。これらは情報セキュリティ対策の一環として以前から実施されてきたことだろう。

ただしランサムウェア対策においては、実は後者の重要性がより高いといわれる。前者は感染を防ぐ上ではもちろん重要だが、未知の手法を使う攻撃などへの対応は難しい。万一の感染で被害が発生すれば、PC やファイルが使えず仕事ができなくなってしまい、事業継続に甚大な影響を及ぼす。感染を回避できない可能性を考慮すれば、後者の対策が不可欠なのは明らかだ。

日本ヒューレット・パッカード（HPE）のストレージ事業統括本部マーケティング部で担当マネージャーを務める諏訪英一郎氏は、「ランサムウェアに感染してしまうとデータは暗号化されてしまい一切アクセスができません。「身代金」を支払ってもデータを取り戻せる保証はありません。一度でも感染すれば自社のデータが失われたのと同然といえるでしょう。セキュリティソフトなどによる予防も完全とは言い切れません。被害時に迅速な復旧を通じて事業継続性を確保するためにも、バックアップによるデータの保護が必要です」と話す。

単純なバックアップでは対応不可能!?

そこで HPE は、ランサムウェア対策の要件も満たすという重複排除バックアップソリューション「HPE StoreOnce」を提案している。諏訪氏によれば、ランサムウェア対策では単にバックアップをするだけでは不十分であり、3 つの要件を満たす必要があるという。

要件の 1 つ目は「データの保存先」だ。企業ではさまざまな媒体にシステムやデータをバックアップしているが、近年は低価格化を追い風に NAS や DAS の採用も増えている。だが、それらの利

ランサムウェア対策におけるバックアップで考慮すべき 3 つの要件

バックアップ対象	ユーザーデータ、アプリケーションデータだけではなく、システム復旧に必要なすべてのデータが対象
データ保持期間	数日〜2週間とかでは不十分。潜伏期間に対応するためには、数か月以上のデータを保持する必要がある
バックアップ方法	バックアップデータがネットワークから切り離され完全にオフラインである必要がある

用はランサムウェア対策には向かない。ランサムウェアはネットワークを介して感染を広げることから、ネットワークに接続されているドライブのバックアップデータまで暗号化される可能性が高いからだ。この点を踏まえれば、バックアップ先にはネットワークから完全に隔離できる媒体を選択する必要がある。

2 点目が「バックアップ対象」である。企業には PC や各種アプリケーションなどに数多くのデータが存在し、従来は運用の手間を考慮して業務上重要度の高いものに絞ってバックアップが行われてきた。だが、情報資産を保護する観点では、万一の際に迅速にシステム全体を復旧させなければならず、一部のアプリケーションやユーザーデータだけではなく、システムにまつわるデータを丸ごとバックアップ対象に含める必要がある。

最後の要件は、「バックアップの頻度とデータの保持期間」だ。バックアップは有効性の高い対策ではあるが、やはり万能ではない。リカバリ時の現業への影響を抑えるには、“ 今 ” とバックアップ時とのタイムラグをできる限り短くする必要がある。そのためにはバックアップ頻度を増やすべきだが、一方でランサムウェアの中には、感染から数カ月にわたって潜伏した後に活動を開始するものも存在する。データの安全性を担保するなら、より長期間のデータ保持も必須となってくる。今までのように 1 ～ 2 週間日次、あとは月次というようなバックアップでは不十分であり、バックアップ方式や運用方法を根本から見直すことが求められているのだ。

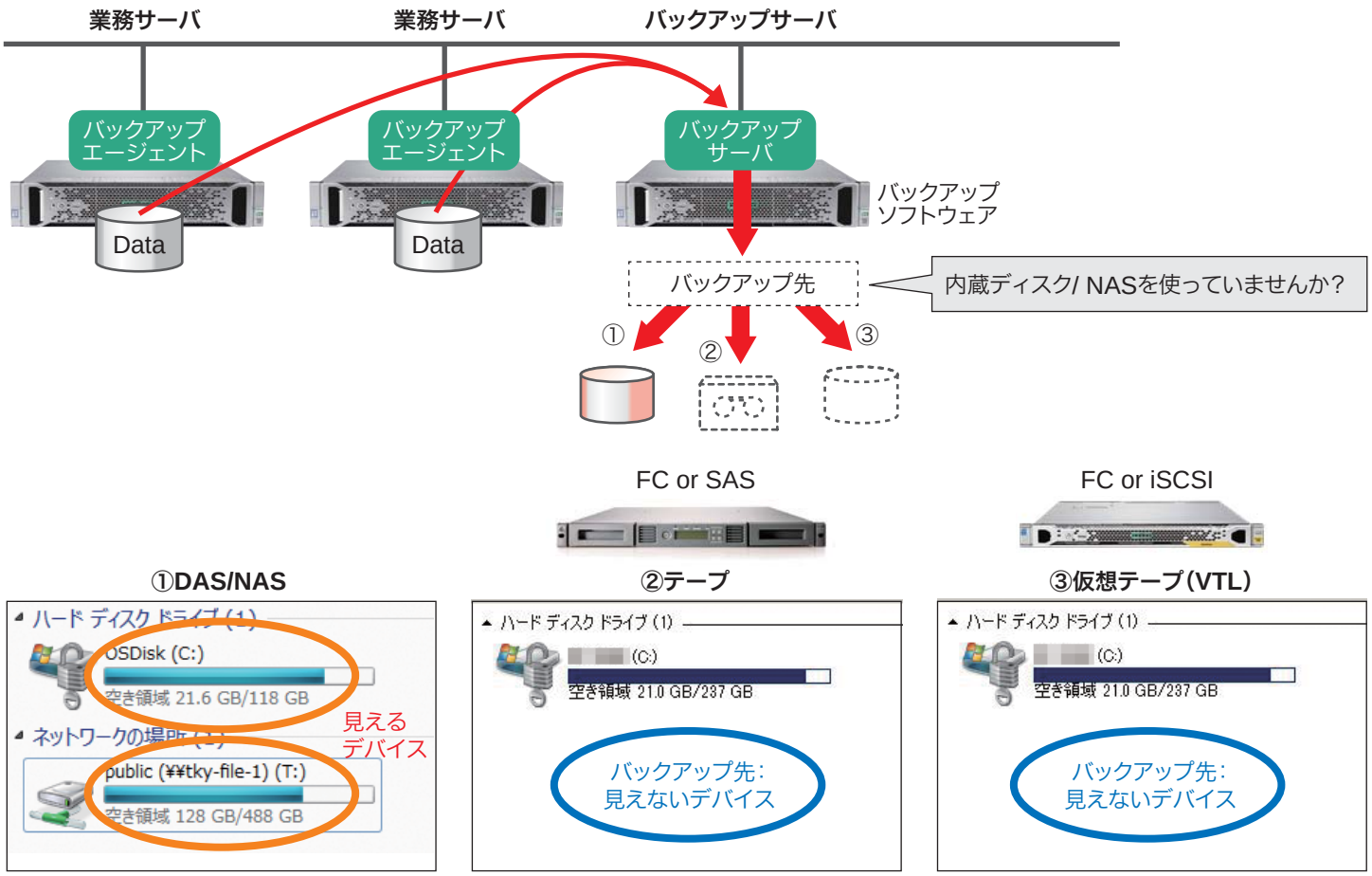
「ランサムウェア対策を目的としたバックアップでは、通常と比較して満たすべき要件が大きく異なることを念頭に置く必要があります。その上で、要件の溝を埋めるための手法と、そのための製品の双方の見極めが企業に求められています」（諏訪氏）

ランサムウェア対策の要件を満たす現実解

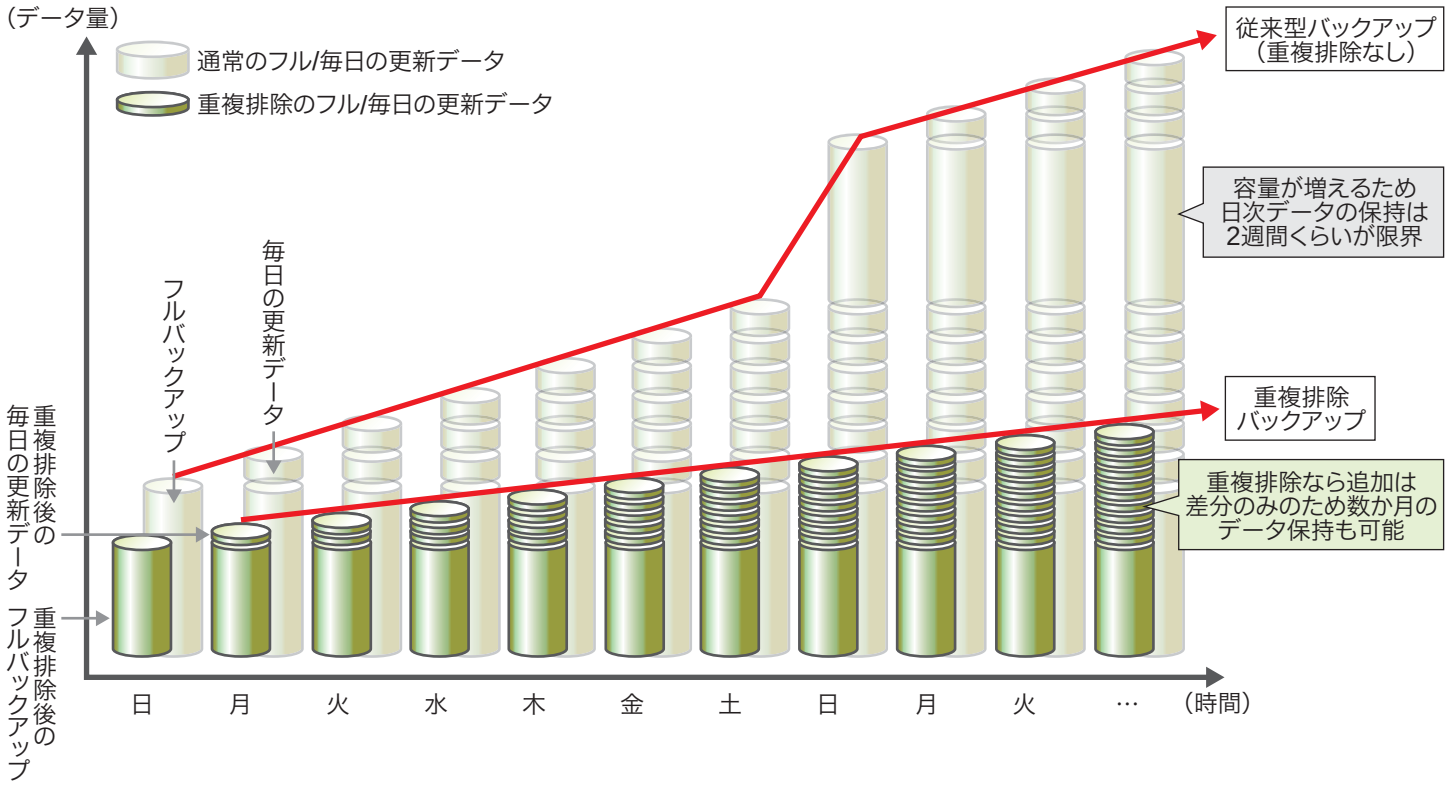
HPE StoreOnce は、こうしたランサムウェア対策のバックアップで考慮すべき要件の全てに対応できるという。特に注目されるのが、最初の要件である「（ネットワークから隔離された）データの保存先」をカバーする仮想テープライブラリ（VTL）機能である。

ランサムウェアのターゲットは個人から企業に移りつつある。そのためサーバや NAS が脅威にさらされているが、これらはネットワーク接続されストレージが OS からデータの保存場所として認識できてしまうことに大きな問題がある。ランサムウェアは、感染拡大にこの仕組みを悪用しているわけだ。これに対して VTL は、その仕組み上、バックアップツールやドライバを介さないと OS から保存場所として認識されない。つまり、物理的にはネットワークに接続されていても、論理的には隔離された環境を整備できることか

バックアップはランサムウェア側から “ 見えない ” 方法が必須



HPE StoreOnce の重複排除によるデータ量の推移イメージ



ら、ランサムウェアの感染が及ばない。

VTL 機能を備えたバックアップ用ストレージは他にもあるが、それらの中にはファイバチャネル（FC）での接続を前提としたものもあり、別途 SAN の整備の手間とコストが必要になる。HPE StoreOnce には FC に加えて iSCSI のインタフェースも用意されており、後者を選択すればバックアップサーバに接続された既存の NAS や DAS を置き換えるだけ済む。

また、世代ごとの媒体保管が求められる重要なシステムのバックアップは、今でもテープが保存媒体として広く利用されている。ネットワークから物理的に隔離されるテープもランサムウェア対策に活用できそうだが、第 2、第 3 の要件を考慮すれば、現実的でないことは容易に理解できるはずだ。テープでこれら要件を満たすとすれば、一度の作業に要する時間が確実に長くなるし、頻繁な作業が発生してしまう。管理すべきテープの本数も飛躍的に増える。

「小規模企業のランサムウェア対策ならテープも有効でしょう。しかし一般的な企業なら、保護すべきシステムやデータが多数あり、作業の負担が増してしまいます。場合によっては業務に大きな支障を来たしかねません。ランサムウェア感染時のような緊急事態は速やかにリカバリできなければなりませんので、この点でも VTL を利用した方がよいと考えます」（諏訪氏）

テープとディスクの良いとこ取り

HPE StoreOnce の VTL 機能はテープのように扱えるが、実態はあくまでディスクストレージであり、実際のテープにまつわる煩雑性などの制約を受けることがない。例えば、バックアップとリストアの双方で並列処理をすることができ、作業時間を大幅に短縮できる。また、データセンターで世代管理されているバックアップデータからネットワーク経由で迅速にリカバリすることも可能になっている。

さらに、ランサムウェア対策を含めて効率性の高いストレージバックアップに貢献するのが、HPE StoreOnce ならではの重複排除機能だ。

重複排除機能では、データを「チャンク」と呼ばれる小さな単位に分割し、差分データだけをバックアップデータに保存することでデータ容量を大きく圧縮する。HPE ではこの処理を一工夫し、通常では固定されることの多いチャンクのデータ単位を可変させ、かつ平均 4KB という細かい粒度で処理している。これによって、極めて高いデータの圧縮率を実現しているという。

バックアップデータは容量が肥大化してしまうことが多いだけに、重複排除機能の活用はストレージコストの抑制に直結してくる。この点を評価して HPE StoreOnce を導入している企業や組織は非常に多く、あるユーザー環境では圧縮率が 40 分の 1 という極めて効率性に優れた実績を出しているとのことだ。

また、バックアップデータの容量が削減されれば、データセンターなど遠隔地へのレプリケーションもしやすくなる。以前ならデータ容量が大きくなればなるほどネットワーク帯域を拡張しなければならなかったが、HPE StoreOnce では数 Mbps ～の帯域で拠点間のレプリケーションも可能だという。「ネットワークのコストも抑え

HPE StoreOnce のラインアップ

HPE StoreOnce System：次世代連携型重複排除バックアップ

バックアップ総容量（重複排除率20：1時）	20TB～1PB	～110TB	～282TB	～573TB	～3.36PB	～17PB	～34PB
使用可能容量	1～50TB	5.5TB	7.5～15.5TB	15.5～31.5TB	36～216TB	36～864TB	72～1728TB
最大転送速度	1～6TB/時	6.4TB/時	12.7TB/時	12.7TB/時	26.7TB/時	37.7TB/時	184TB/時

ながらバックアップの信頼性を格段に高められます」（諏訪氏）。

HPE では企業の多様なバックアップ要件に対応する製品を豊富に取りそろえている。また HPE StoreOnce のソフトウェア機能を利用できる無償ダウンロード版（URL：www.hpe.com/jp/freebackup）を提供している。バックアップ容量は 1 テラバイトまでだが、諏訪氏は、「『導入前に検証したい』『小さなシステムだけでもまずはバックアップしたい』といった目的でも利用できますので、ぜひ試してみてください」と話す。

ランサムウェアは、金銭目的のサイバー犯罪者にとっては非常に効率的で成功率も高い手法とされ、その脅威がますます深刻化するのは間違いないだろう。バックアップによるシステムやデータの保護は、もはや必須のランサムウェア対策といえる。HPE StoreOnce のような脅威への対応も考慮したバックアップ製品を検討していくべきだ。

日本ヒューレット・パッカード株式会社
東京都江東区大島 2-2-1
https://www.hpe.com/jp/ja/home.html

この冊子は ITmedia エンタープライズ（http://www.itmedia.co.jp/enterprise/）に 2016 年 7 月に掲載された記事をもとに作成したものです。
http://www.itmedia.co.jp/enterprise/articles/1607/11/news003.html