ランサムウェア対策5ステップの最後の砦

『復旧』の実装でビジネス影響を最小化する

近年、ランサムウェアの被害を受ける企業や組織が増えている。リモートワークの普及によって侵入経路が増えたこと、攻撃手法が多様化・巧妙化していることがセキュリティ対策を困難なものとする原因だ。セキュリティ対策にはさまざまな方法があるが、ビジネス影響の最小化を目的とした際に特に重要となるポイントはバックアップデータの安全確保と復旧を確実に行える環境を整えることである。本稿ではランサムウェアによる被害を始めとしたセキュリティ対策を講じる上で、最適なバックアップと復旧の仕組みを紹介しよう。

最重要な「復旧」から着手するセキュリティ対策

昨今、ランサムウェアによる被害が多発している。攻撃側はランサムウェア・アズ・ア・サービス（Ransomware as a Service；ランサムウェアを提供するサービス）を確立しており、これまでよりも簡単に高度な攻撃を仕掛けられるようになった。

もちろん、防御側もランサムウェア被害の深刻さを理解し、何らかのセキュリティ対策は講じている。例えば、ファイアーウォールや UTM（Unified Threat Management：統合脅威管理）による境界型防御、デバイスへのアンチウィルスソフト導入、データのバックアップなどがある。昨今ではゼロトラスト型のセキュリティ対策も普及しつつあるが、それでもサイバー攻撃の被害に遭うケースも見られる。被害に遭うリスクを可能な限り低減させられるよう速やかな対応が求められる中、企業や組織はどのようにセキュリティ対策を強化すれば良いのか。

結論から言えば、サイバー攻撃の被害に遭う可能性を考慮してバックアップデータの安全確保と復旧を確実に行うことが最も重要だ。米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワークには、「識別」「防御」「検知」「対応」「復旧」のステップがある。本来であれば、自社が各ステップに対応できているか明らかにした上で、優先度が高い領域から対処することが理想的だ。しかし、攻撃手段の高度化・巧妙化、対応の緊急性を考えると、サイバー攻撃の被害に遭っても確実に復旧できる仕組みを整えることが先決だろう。

ランサムウェアの侵害を考慮した バックアップ / 復旧の体制

では、バックアップや復旧の仕組み作りは何から始めるべきか。まず着手すべきは、自組織内におけるバックアップへの意識を変革することだ。セキュリティの専門家でない経営者や従業員は、自社ですでにバックアップを取得できているため安全だと考えている傾向にある。しかし、肝心のバックアップデータがランサムウェアに感染して復旧できなくなる可能性までは考慮できていないことが多い。一部のランサムウェアは、侵入後内部データのみならずバックアップデータまで暗号化するため復旧は困難を極める。この点を見落としているからこそ、多くの企業や組織が被害に遭っている。

今後はハードウェアの故障に備えたバックアップではなく、ランサムウェアの侵害に備えたバックアップシステムを構築しなければならない。

考えられる方法は、バックアップシステムを堅牢なものに構築し直すことだ。バックアップサーバの OS も攻撃リスクの少ない Linux OS や専用 OS を利用することが求められる。攻撃検知機能を持つバックアップシステムの利用も欠かせない。昨今のバックアップ製品にはランサムウェア対策のさまざまな機能が備わっていることが多い。具体的には、権限付与・多要素認証といったアクセス管理、バックアップ元の異常検出、バックアップデータのマルウェア検出などがある。最新のバックアップ製品を用いれば、比較的容易に復旧対策を行えるだろう。

データをバックアップする際、一般的には運用データも含めたコピーデータを 3 つ用意して2種類の異なる媒体に保存し、残った1つのデータをオフサイトなどの全く別の場所に保存する「3-2-1 ルール」が推奨されている。

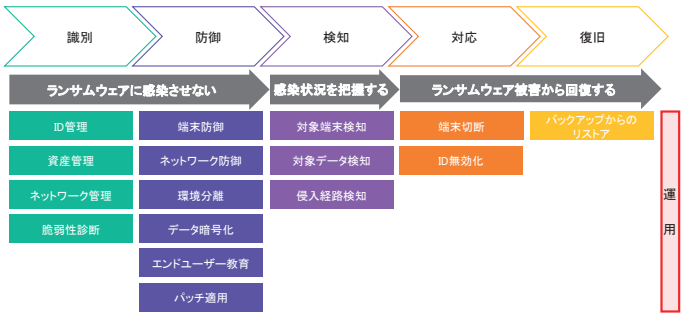
ただし、ランサムウェア対策をより強化するためには「3-2-1-1 ルール」を適用することが重要となる。これは、コピーしたデータを 3 つ用意して 2 つを異なる媒体に保存し、1 つを別の場所へ、残った 1 つのコピーデータを一度書き込

んだデータを消去・変更できない「WORM（Write Once Read Many）」形式で保存する方法だ。1つのコピーデータをクラウドストレージに保管する方法も有効だが、保存するデータ量が増えてしまうため、データ量を削減するための工夫が求められる。

また、サイバー攻撃によってビジネスを停止させられる時間を短くするために、迅速に復旧できる仕組みを整えることもポイントとなる。そのほかにもセキュリティ管理者や IT 担当者への負荷が大きくなりすぎないよう、運用が容易なバックアップ製品の利用を検討すると良いだろう。

マルウェア検出、AI による異常検知で攻撃に対応 HPE が最適なシナリオを提案

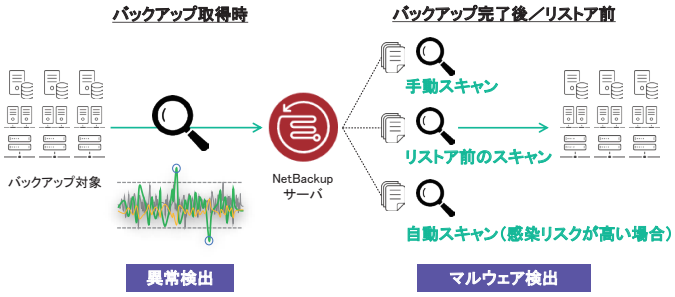
こうした条件を満たすバックアップソリューションが「Veritas NetBackup（以下、NetBackup）」だ。NetBackup は、日本ヒューレット・パッカード（以下、HPE）のコンサルティング /SI サービス「HPE ランサムウェア対策ソリューション」に含まれる。HPE ランサムウェア対策ソリューションは「識別」「防御」「検知」「対応」「復旧」といった 5 つの要素を網羅



HPE が提供するランサムウェア対策ソリューションがサポートする 5 つの要素

しており、バックアップデータの安全確保と確実な復旧を実現する多層防御のシナリオを HPE が提案する。

NetBackup 単体で見ると、ランサムウェア対策に求められる「保護」「検出」「回復」といった機能を 1 つのプラットフォームで実現できるという魅力がある。「検出」においては、バックアップ取得後の AI 技術を活用した異常検出や、リストア前のマルウェアスキャンの機能を提供する。マルウェアに感染していない安全なデータを安全な環境で保存し、迅速に復旧さ



異常検出とマルウェア検出の流れ

せることができる。データ保護に特化した 30 年以上の信頼と実績により、多くのユーザーから高評価されている。

さらに、バックアップ・復旧に関連する機能やサービスを幅広く提供していることもポイントだ。800 以上のデータソースをバックアップできるほか、100 以上の OS のバージョンにも対応している。

バックアップ先も多様な種類から選ぶことができる。最新の仮想環境はもちろん、ディスクやテープなど 1400 以上のストレージと 60 以上のクラウドサービスに対応しており、ハイブリッド / マルチクラウド環境を一元管理可能。運用に関しても NetBackup が提供する「重複排除機能」でデータ量を削減すれば、より多くの世代のデータをバックアップできる。

このように、NetBackup を活用するだけでもランサムウェア対策を強化できる。さらにバックアップシステムの堅牢性を高めたい、最適な多層防御のシナリオを提案してほしい場合は、先述した HPE のランサムウェア対策ソリューションを併用すると良いだろう。巧妙化するランサムウェアの攻撃から自社の情報資産を守る手段の 1 つとして検討していただきたい。

日本ヒューレット・パッカード合同会社

〒136-0072 東京都江東区大島2-2-1
お問い合わせ　TEL：090-5998-1512　E-mail：pnj_ext_info@hpe.com
https://www.hpe.com/jp

すべての製品名、サービス名、会社名、ロゴは、各社の商標、または登録商標です。
製品の仕様・性能は予告なく変更する場合がありますので、ご了承ください。

Hewlett Packard Enterprise