RDX にバックアップしたデータを ランサムウェアから守るソリューション

BackupExec の『ランサムウェアレジリエンス』機能を

利用して RDX にバックアップする方法のご案内

はじめに

本書は、Veritas Technologies 社のバックアップソフトウェア「BackupExec」のランサムウェアレジ リエンス機能を利用して、RDX ドライブにバックアップしたデータをランサムウェアから保護する方 法についてご紹介することを目的としています。

BackupExec は、中小規模企業向けのバックアップソフトとして国内外で最もよく知られるバックア ップソフトウェアの一つで、物理環境・仮想環境・クラウドデータのバックアップ向けに 45,000 社以 上の企業で利用されるソフトウェアです。

RDX は、OverlandTandberg 社がライセンスを持つディスクカートリッジデバイスで、テープとディ スクの両方の長所を兼ね備えることで中小規模企業向けのバックアップデバイスのデファクトスタン ダードとなっています。ドライブから取り外し可能な RDX データカートリッジと、PC・サーバに接 続する RDX ドライブから成る製品です。



本書手順で使用した環境

バックアップ対象に Windows Active Directory、Microsoft Exchange Server、Hyper-V などの特 殊なデータが含まれていない場合(GRT 対応バックアップではない場合)

バージョン20.4以降のBackupExecではデフォルトでランサムウェアレジリエンス機能が有効 になっているため、ランサムウェア対策に特別な手順は必要ありません。

以下の手順ではまず一般的な(上記の特殊なデータが含まれていない)システムの全体バックア ップ(イメージバックアップ)を取得し、ランサムウェアから保護されていることを確認する手 順まで記載しています。

その後、ExchangeServer や Hyper-V などがバックアップ対象に含まれる場合についての設定 手順についてもご案内いたします。

ステップ1. BackupExec 上で RDX をバックアップデバイスとして構成する

本例では、E:ドライブとして Windows から認識された RDX のボリューム(4TB カートリッジ)を BackupExec 上でストレージ設定します。



↓

BackupExecを開き、「ストレージ」画面を開き、「ストレージを設定」ボタンを押します。



「ディスクベースのストレージ」を選び次に進みます。

WIN-NLMEHLF4FG7 にストレージを設定	_		×
設定するストレージの種類を指定してください。			
			_
ディスクベースのストレージ ローカルまたはリモートディスクストレージ、ディスクカートリッジデバイス、重複排除ディスクストレージ、ストレーシ クおよびレガシーなディスクへのパックアップフォルダを設定に利用できます。	የምレイ、1	仮想ディス	
クラウドストレージ パックアップデータをクラウドに送信できるストレージデバイス。			
マンドレージ OpenStorage デバイス、NDMP サーバー、Remote Media Agent for Linux を構成できます。			=
テープストレージ テープドライバのインストール、ホットスワップ可能なストレージデバイスの置換または追加、ロボットライブラリバ 成、およびバーコードルールの構成の名タスクを使用できます。	(−ティショ	コンの構	
マンジェンジューン ストレージプール ストレージデバイスブールと Backup Exec サーバープールを設定できます。			
メディアセットとメディアボルト	た西牟子	-st.Mm	*
ストレージの種類の違いについて 次へ(N)>	キャンセ	ル

「ディスクカートリッジデバイス」を選び次へ進みます。

ę	🖞 WIN-N	LMEHLF4FG7 にストレージを設定	_		×		
	設定す	するディスクベースのストレージの種類を指定してください。					
	2	ディスクストレージ ポリューム ホットスロップ対応デバイス USB デバイス または FireWire デバイスを使ったストレージです					
	ディスクカートリッジデバイス RDX デバイスなどのディスクカートリッジメディアを使用するデバイスや、USB サムドライブなどの Windows でリムーバブル記憶域として表示されるデバイスのストレージ。						
	■ 重複排除用ディスクストレージ ☆ バックアップサイズを小さくするために、固有のデータのみが格納されるボリュームを使ったストレージです。						
	以前のディスクへのバックアップフォルダをインポート 以前のパージョンの Backup Exec で作成されたディスク上のフォルダのストレージ。既存のディスクへのバックアップフォルダをイン ポートできます。						
	ディスクス	レージの種類の違いについて < 戻る(B) 次へ(N)>	キャンセ	<i>س</i>		

BackupExec上でのこのデバイスの名前を決めます。この例ではデフォルトのまま進みます。

WIN-NLMEHLF4FG7 にストレージを設定	_		×
ディスクカートリッジデバイスに使用する名前と説明を指定してください。			
名前(M): ディスクカートリッジデバイス 0001			
説明(D):			
< 戻る(<u>B</u>) 次へ(<u>N</u>):	>	キャンセ	IL)

ディスクカートリッジデバイスとして構成するディスクを選択する画面になりますので、RDXのボリューム(本例では E:ドライブ)を選択します。

WIN-NLMEHLF4FG7 にストレージを設定	_		×
ディスクカートリッジデバイスの場所を指定してください。			
ディスクカートリッジデバイス(D): (E :			
< 戻る(<u>B</u>) 次へ()	<u> </u>) >	キャンセ	۱ <i>۱</i>

設定内容を確認して、「完了」ボタンを押します。

WIN-NLMEHLF4FG7 にストレージを設定		_		×
ストレージ設定の概略				
ストレージカテゴリ				~
ディスクベースのストレージ				
ストレージの種類				\approx
ディスクカートリッジデバイス				
ディスクカートリッジデバイスの名前と説明				~
名前: ディスクカー	、リッジデバイス 0001			
説明:				
ディスクカートリッジデバイスの場所				~
ドライブ文字: E:				
· · · · · · · · · · · · · · · · · · ·				
	< 戻る(<u>B</u>) 完	7(E)	キャンセ	1

「ストレージ」画面にディスクカートリッジデバイス 0001 が追加されていることを確認します。

● ●
□ 雪がの □ 一時停止 □ 一時停止 □ 一時停止 □ 二 □ 二 □ 一時停止 □ 二 □ □ □ □ □ □ □ </td
ビュー 状態 設定 ストレージ操作 メディア操作 オンパイス 0001 詳細 オペズのストレージ ディスクカートリッジデバイス 0001 詳細 ディスクカートリッジデバイス 0001 詳細 マロー・ション 名前 ▲ 状態 ストレージの種類 アクティブアラート ストレージの傾向 容量 (新) 季ブイスクカートリッジデバイス 0001 (FLDR000001) オンライン ディスクカー・・・ 220 MB/3
すべてのストレージ ディスクカートリッジデバイス 0001 詳細 名前 ▲ 状態 ストレージの種類 アクティブアラート ストレージの傾向 容量 ※ ディスクカートリッジデバイス 0001 (FLDR000001) オンライン ディスクカー… 220 MB/3.
名前▲ 状態 ストレージの種類 アクティブアラート ストレージの傾向 容量 ● ディスクカートリッジデバイス 0001 (FLDR000001) オンライン ディスクカー… 220 MB/3
ディスクカートリッジデバイス 0001 (FLDR000001) オンライン ディスクカー 220 MB/3.
* 「「「WIN-NLMEHLF4FG7 アラート 🕿 0 🛕 1 🛐 0 🏫 11 ジョブ 🕸 0 🥅 0 🆄 0 👘 0 約 1 🔅

※ランサムウェアレジリエンス機能となる「ディスクストレージのロックダウンステータス」は最初から有効になっています。

· ·			· · · · · · · · · · · · · · · · · · ·
\odot	🍿 WIN-NLMEHLF4FG7 🛛 アラート 😵 0 🛕 1 🏹 0 🐨 11 🛛 ジョブ 🅸 0 👼 1 🏖 0	ē.	VERITAS
		ディフクフトレージのロックダウンフテータフィ方効	
		ノースノストレーンのロシシシシノスノーノス・有効	

ステップ2. バックアップジョブを作成する

「バックアップとリストア」画面で「バックアップ」ボタンのメニューを出し、「ディスクカートリッジにバックアップ」を選択します。



左側にバックアップ対象、右側にバックアップ先の設定画面が出るので、まず左側のバックアップ対象の「編集」ボタンを押します。

⑧ パックアップ定義のプロパティ	- D X
名前(<u>N</u>): WIN-NLMEHLF4FG7 バックアップ 00003 説明(<u>D</u>):	
😠 💐 WIN-NLMEHLF4FG7	浸 バックアップ
すべて選択済み	🥱 完全 (🔨
C:	ジョブ名: WIN-NLMEHLF4FG7 バックアップ 00003-完全
dig E:	スケジュール: 1 週 ごと、(金曜日)、23:00
G:	ストレージ: ディスクカートリッジストレージ
	保持期間: 2週間
る。 Microsoft Sol Server イクスタクス	☞ 増分 (◇)
	ジョブ名: WIN-NLMEHLF4FG7 バックアップ 00003-増分
	スケジュール:時間23:00、1日ごと このパックアップは、最初の完全パックアップが完了す ままで定行されません。
	ストレージ: ディスクカートリッジストレージ
	保持期間: 1週間
クレデンシャルのテストと編集(I) [編集(E)]	ステージを追加(S) ▼ 【編集(E)

バックアップしたい項目を選択して「OK」をします。本例ではシステム全体をバックアップするので、 バックアップ先となる E:ドライブや空の DVD ドライブなどを除く全てを選択しています。

⑧ バックアップ選択リスト		— 🗆 X
 グバックアップ選択リスト WIN-NLMEHLF4FG7 バックアップ 00004 ・ ・ ・	WIN-NLMEHLF4FG7 参照 選択の詳細 ビジネスクリティカルとしてタグ付け(1) ビジネスクリティカルとしてタグ付け(1) ・ (2) @ C: ・ (2) @ C:	- □ × Simplified Disaster Recovery: オン ● ▼ ルとしてタグ付け解除(U)
+ - (= =)	 ▶ (2) (20) EFI システム/(-テイション ▶ (2) (20) Microsoft SQL Server 1 ▶ (2) (20) (20) (20) (20) (20) (20) (20)	soft SQL Server インスタンス ム状態
<u>へルプ(H)</u>		OK キャンセル

次に右側のバックアップ先に関する「編集」を押します。

🐵 バックアップ	「定義のプロパティ					×
名前(<u>N</u>): 説明(<u>D</u>):	WIN-NLMEHLF4FG7 パックアップ 00	0003]	
•	WIN-NLMEHLF4FG7		ा र्	クアップ		
すべて選	択済み		😑 完全		(\sim
C:			ジョブ名:	WIN-NLMEHLF4FG7 パックアッ 00003-完全	プ	
SE E			スケジュール:	1 週ごと、(金曜日)、23:00		
🍏 G:			ストレージ:	ディスクカートリッジストレージ		
🧐 EFI	システムハーテイション		保持期間:	2 週間		
MIC NIC	rosoft SQL Server 177977		→ ₩/\			-
1 27	アム状態		19 増分 ジョブ名:	WIN-NLMEHLF4FG7 バックアッ 00003-増分	יש דו	<u>)</u>
			スケジュール:	時間 23:00、1 日 ごと このパックアップは、最初の完全パックアッ るまで実行されません。	ブが完 ア す	
			ストレージ:	ディスクカートリッジストレージ		
			保持期間:	1 週間		
26	デンシャルのテストと編集(I) 編集(E)		ステージを追加(<u>S</u>) ▼ 第	s集(<u>E</u>)	
へルプ(<u>H</u>)				ОК (キャン	<u>ل</u> الله

まずスケジュールを設定します。設定したいスケジュール内容に設定して(ここではまだ「OK」は押 しません)、次の「ストレージ」設定に進みます。本例では1回きりの完全バックアップを作成するの で、増分のウィンドウは削除し、「繰り返しなしのスケジュールで今すぐ実行」を選択しています。

🐵 バックアップオプション	— 🗆 X
スケジュール ストレージ ネットワーク 通知 テスト実行	 ・ ・ ・ Backup Exec は、デフォルトのバックアップジョブ設定を使って新しいバックアップジョブを作成します。必要に応じて設定を変更できます。
快起 Advanced Open File Advanced Disk-based Backup ブリポストコマンド ファイルとフォルダ Microsoft SQL	 ジョブのデゾブレートキ(い): 完全 Cのジョブランブレートのひがりやすい名前を入力にます。名前はデフォルトのジョブ名の作成に使います。 ジョブ名(い): WIN-NLMEHLF4FG7 パックアップ 00003-完全 スケジュール: ● 繰り返し(C): 1 週 ごと、(金曜日)、23:00 ● 繰り返しなしのスケジュールで今ずぐ実行(W): ● スケジュールを設定せずに作成(い) ● 保留にする(い)
へルプ(<u>H)</u>	OK キャンセル

ストレージの設定で、バックアップ先のストレージが「ディスクカートリッジストレージ」になって いることを確認します。バックアップの完了後にカートリッジを取り出すオプションにチェックをつ けることもできます。

バックアップ先を確認したら「OK」を押します。

🐵 バックアップオプション			_		×
スケジュール					
ストレージ	🔁 このバックア:	ップ定義のすべてのバックアップジョブのオプション:			
ネットワーク	優先度(R): 通堂	•			
通知					
テスト実行					
検証	完全 完全				_
Advanced Open File	ストレージ(S):	😹 ディスクカートリッジストレージ (1 デバイスがこのプールに存在)			•
Advanced Disk-based Backup					_
プリ/ポストコマンド	保持する期間(K):	2 💭 週間 🔻			
ファイルとフォルダ		🥅 ジョブの完了後にメディアを取り出す(F)			
Microsoft SQL	圧縮(P):	tal 🔹			
	暗号化の種類(C):	[al ▼			
			* /* = +	771.1477.	
	11年限のないが、ません。	ノビスがらナーダを休護するために明考れての使用をお勧めします。NDMIP バックアップにソフトウエア明考れ	を決用9	95519.02	2
へルプ(H)		ОК		キャンセ	211/

バックアップ対象、バックアップ先・スケジュールとも設定が終わったので、OKを押します。 今回は「スケジュールせず今すぐ実行」を選択したので、OKを押したらすぐにバックアップが開始 されます。

🐵 バックアップ定義のプロ	パティ			— C	x נ
名前(<u>N</u>): WIN-NLM 説明(<u>D</u>):	NEHLF4FG7 バックアップ 0	0003			
😠 📑 WIN-N	NLMEHLF4FG7		الا	クアップ	
すべて選択済み		 Image: A start of the start of	🤭 完全		\bigcirc
C:			ジョブ名:	WIN-NLMEHLF4FG7 パックアップ 00003-完全	
SE E			スケジュール:	1 週 ごと、(金曜日)、23:00	
🍲 G:			ストレージ:	ディスクカートリッジストレージ	
6 EFI システムパー	-テイション		保持期間:	2 週間	
Microsoft SQL	L Server インスタンス				
[●] システム状態			₩ 9 宿分		۲
			ジョブ名:	WIN-NLMEHLF4FG7 バックアップ 00003-増分	
			スケジュール:	時間 23:00、1 日 ごと このパックアップは、最初の完全パックアップが売 るまで実行されません。	77
			ストレージ:	ディスクカートリッジストレージ	
			保持期間:	1 週間	
クレデンシャルの	テストと編集(I) 編集((<u>E</u>)		ステージを追加(S) ▼ 編集(<u>E</u>)
ヘルプ(<u>H</u>)				ок (*	ヤンセル

ジョブモニター画面を開き、バックアップが実行中になっていれば無事に開始されています。

Ø Veritas Backup Exec™										- 🗆	×
الا کے ال	ド ックアッ	2日 プとリストア	い ジョブモニター	ביים גרע	-ジ	加 レポート	インス	また タントクラウドリカノ	עז		
■標準 → リートとフィルタ	<u>ツリー表示</u> リスト表示 ノ	し (ックアップカレン	ğ- IJZŀ7	 三編集 ※削除 Øキャンセ 	相優労 (を) 今す して () 失敗	に度・ で実行 てしたリソースの	(み再試行	❶ 保留 ▼ ☞ テスト実行 ■ ジョブのアクティビテ	ジョブ履歴を表示	 ジョブ履歴 	
Ľ1-		バックアップ	リストア				ジョブ				
				ジョ	ブ - 1 項目						
名前 ▲	サーバー	ストレ	ージ	ジョブ	の種類	状能	ジョ	ブの状態		バイト数	開始問
🕨 🎘 WIN-NLMEHLF4FG7 パッ	WIN-NLM	ИЕН 🦉 🗄	ディスクカートリッジス	スト バック	アップ	実行中	۲)動作中:リソースのを	食出中	0 //1ト	2023
4				ジョブ	爾麻 - 1 頂	B					÷
夕益	++_114_	751-31	ಚಾಗಗಳ	ほね ぷっけ) 准体应		明松時刻	約了時刻 —	(双)风味明	ポイト教
1日前 日ディスクストレージを設定 00	9-11-	ディフクカー	510 510	(主大児 ション :))品が古 Ø2) 5	011/15k	進沙中	100%	開始時刻 2023/05/10 1	2023/05/10 1	00:00:05	0.1
											.,
<		111									ŀ
🔅 🍴 WIN-NLMEHLF4FG	7 アラート 🤅	30 🛕 1 🛛	2 0 🕤 11	ジョブ 🏖 0	🧝 1 🏖	0 🔅	<i>6</i>			VE	RITAS

ジョブが「成功」となっていればバックアップ完了です。

Ø Veritas Backup Exec™									- 🗆	×
الان الان الان الان الان الان الان ا	₹ バックアップ。	とリストア ジョフ	型 た_9-	』 ストレージ	」 レポート	インス	タントクラウドリカバ	۲IJ		
□標準 ソートとフィルタ	<mark>ッリー表示</mark> リスト表示 パッ	マー クアップカレンダー	ער איז	編集 *16 削除 多く キャンセル マ 🕝 ダ	優先度 ▼ ∲すぐ実行 ミ敗したリソースのる	(。 み再試行 🔓	 ●保留・ ・ ・<	ジョブ履歴を表示	 ジョブ履歴 ・ 	
ยั่ว-		バックアップ	リストア			ジョブ				
				ジョブ - 0 項	目					
名前 ▲	サーバー	ストレージ		ジョブの種類	状態	ジョ	ブの状態		バイト数	開始時
			<گ ا	ブが左右し	±#6.					
			/ 1		α eπ₀					
				ジョブ履歴 - 2	項目					
名前	サーバー	ストレージ	ジョブの種類	ジョブの状態	進捗率		開始時刻	終了時刻 💌	経過時間	バイト数
ஜ WIN-NLMEHLF4FG7 /(WIN-NLMEH	ディスクカートリッ	バックアップ	2 成功		100%	2023/05/24 11	2023/05/24 11	00:41:49	137
ディスクストレージを設定 00		ディスクカートリッ	ストレージ操作	🐏 成功		100%	2023/05/19 1	2023/05/19 1	00:00:05	0 /(
4										4

バックアップが取得されると、RDX ドライブ内には「VERITAS」フォルダが作成されています。 WindowsAD 等の特殊なバックアップが含まれていなければバックアップデータは全てこの 「VERITAS」フォルダ内に取得され、BackupExec のランサムウェアレジリエンス機能によりこの VERITAS フォルダは保護されているため、VERITAS フォルダ内のファイルを手動で削除しようとし たり暗号化しようとしたりしても拒否されます。

🕳 🗹 📙 🖛	管理	RDX (E:)			- 🗆	×
ファイル ホーム 共有	す 表示 ドライブ ツール					~ ?
\leftrightarrow \rightarrow \land \uparrow \blacksquare $>$	PC > RDX (E:) >		٥, v			Ą
	名前	更新日時		種類	サイズ	
⇒ ジイラン アンビス ■ デフクトップ	BEControl	2023/05/19 16:54		ファイル フォルダー		
	VERITAS	2023/05/19 16:54		ファイル フォルダー		
איאבא 🛱 🗎	e					

試しに削除しようとしても (左)、右図のようにアクセス拒否され失敗します

📕 📝 🛄 🖛 B2E						- 🗆	×	📭 ファイル アクセスの拒否
→ × ↑	共有 → PC	表示 > RDX (E:) > VERITAS > B2D	~ 3	5	B2Dの検索		• • م	この操作を実行するアクセス許可が必要
 ★ 91+97 79 セス ■ デスクトップ ◆ ダウンロード ※ ドキュメント ※ ビクチャ ■ PC ■ RDX (E) ★ カトロ ク 	オ オ 祖数フ (名司 252000001.bkf 252000002.bkf 252000002.bkf 25200003.bkf ごたらの1億の項目を完全に削除しますか? 2620109481.bkf	更新日時 2023/05/19 17:16 2023/05/19 17:22 2023/05/19 17:29		室頬 3KF ファイル 3KF ファイル 3KF ファイル マイル マイル マイル アイル アイル 3KF ファイル 3KF ファイル	977X 7,695,464 KB 52,428,760 52,428,764 9,479,552 KB 52,428,760 52,428,764 20,481,968 20,481,968 20,492 KB	^	このファイルを変更するには、Administra す。 B2D000002.bkf 種類: BKF ファイル サズ: 49.9 GB 更新日時: 2023/05/19 1
	く 項目を選	□ B2D108482.bkf < 副択 49.9 GB	2023/05/24 11:34		BKF ファイル	192.996 KB	~ ~	◇ 詳細情報

🖙 ファイル アクセスの拒否	-		Х
この操作を実行するアクセス許可が必要です。			
このファイルを変更するには、Administrators からアクセス許可 す。	可を得る必	い要があり	ŧ
B2D000002.bkf 種類: BKF ファイル サイズ: 44.9 GB 更新日時: 2023/05/19 17:22			
再試行(<u>R</u>)	3	キャンセル	
<>> 詳細情報			

バックアップ対象に Windows Active Directory、Microsoft Exchange Server、Hyper-V などの特殊なデータが含まれている場合(GRT 対応バックアップの場合)

BackupExec ではデフォルトでランサムウェアレジリエンス機能が有効になっているものの、 GRT 対応バックアップでは VERITAS フォルダの外にバックアップ関連データが作成され、ラン サムウェアからの保護対象から外れるデータが生じます。GRT バックアップは、AD や Exchange のメールデータ、仮想マシン内の個別データ等を個別にリストアすることを可能にする技術で、 データ復元時の利便性を高めるもので、デフォルトで有効になっていますが、全てのデータを VERITAS フォルダ配下で保護したい場合は GRT 機能を無効にする必要があります。以下ではそ の手順を紹介しています。

バックアップ設定までの手順は上記手順と同じです。

 \downarrow

バックアップ対象の選択の画面で、以下例ではシステムデータと、GRT バックアップ対象とすること ができる Hyper-V データをバックアップ対象として選択しています。

▲ WIN-NLMEHLF4FG7 バックアップ 00007 一冊 WIN-NLMEHLF4FG7	WIN-NLMEHLF4FG7 参照 選択の詳細	Simplif	ied Disaster Re	covery: オフ 🍛
	ビジネスクリティカルとしてタグ付け(I) ビジネスクリティカ	」ルとしてタグ付け解除(U)		
	 ✓ (○) ● ○ ○ ○ ○	サイズ Component マシン	91J	修正日時

右側のバックアップオプションの編集画面では、先ほどの画面と異なり、「インスタント GRT」というメニューと「仮想マシン」というメニューが新しく表示されています。(バックアップ対象に Hyper-V が含まれたため)

本例では先ほど同様まずスケジュールで完全バックアップのみの「今すぐ実行」を選択しています。

バックアップオプション	- D X
スケジュール	
ストレージ	パックアップジョブの追加(B) ▼
ネットワーク	
通知	Backup Exec は、デフォルトのバックアップジョブ設定を使って新しいバックアップジョブを作成します。必要に応じて設定を変更できます。
テスト実行	
検証	🤗 ジョブのテンプレート名(J): 完全
インスタント GRT	このジョブテンプレートのわかりやすい名前を入力します。名前はデフォルトのジョブ名の作成に使います。
Advanced Open File	ジョブ名(J): WIN-NLMEHLF4FG7 パックアップ 00005-完全
Advanced Disk-based Backup	スケジュール: ○ 繰り返し(C): 1 週ごと、(金曜日)、23:00 🔹
プリ/ポストコマンド	 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
ファイルとフォルダ	 スケジュールを設定せずに作成(I)
仮想マシン	
	休留に9 0(0)
(H)	OKキャンセル

次に「インスタント GRT」のメニューでは、どれが選択されていても関係ありません。(次のページ で GRT を無効にするため)



一番下の「仮想マシン」のオプション画面で、「BackupExec Granular Recovery Technology(GRT) を使用して・・・」のチェックを外します。これで GRT が無効になります。

GRT 対象データが Hyper-V ではなく WindowsAD や Exchange 等の場合は、「仮想マシン」のメニューではなくそれぞれ対応したメニューから GRT の使用をオフにすることで同様に無効にできます。



OK でバックアップの設定は完了です。

以上