VERITAS

# エアギャップと分離によるデータリカバリの強化

データの安全なコピーを維持してサイバー攻撃の影響を無効化

ホワイトペーパー | 2023 年 5 月

## データボルトを作成する理由

サイバーセキュリティは、常にビジネスリーダーの最大の懸念事項です。サイバー脅威はますます巧妙化しており、最大限の損害を与えようと絶えずその手口を磨いています。Gartner 社によると、2025 年までに、すべての取締役会の 40% が専任のサイバーセキュリティ委員会を設け、サイバーセキュリティのポリシー、遂行、リカバリに関する報告と戦略を強化しようとしています[1]。サイバー犯罪の指数関数的な増加により、企業は多大なコストと時間をかけてその低減とリカバリに取り組んでいます。2022 年には 15 秒に 1 件のサイバー攻撃が発生しており[2]、リスクを低減し、不確実性をなくし、環境の制御を維持する戦略の確実な準備は時間との戦いになっています。

回復力およびリカバリ計画に対する確信は、適切なテクノロジとプロセスを備えた信頼性の高いサイバーセキュリティフレームワークの導入から生まれます。上司や経営幹部に自信を持って伝達できるサイバーセキュリティインシデント対応計画はあるのでしょうか。Gartner 社によると[3]、2025 年までに、CEO の 70% がサイバー犯罪からの組織的な回復力を全社的に義務付ける予定です。今こそ、サイバーセキュリティの傾向と、成功するリカバリ計画に不可欠なコンポーネントを理解するときです。ランサムウェア攻撃の動きを止められるように、そしてリカバリのための適切なツールを導入したことを自信を持って取締役会に提示できるようにしてください。

## エアギャップの概要とそれが重要である理由

サイバー攻撃はますます巧妙化しており、ハッカーは、プライマリデータストレージだけでなく、バックアップデータストレージも標的にしています。そこで重要になるのが、ディザスタリカバリ戦略でこのことへの対応を計画しておくことです。ほとんどの場合、ハッカーは、プライマリデータとバックアップデータにアクセスして侵害できるようになるまでシステム内で休眠しています。アクセスできれば、破壊できてしまうのです。

米国標準技術局 (NIST) によると、エアギャップとは、(a) 物理的に接続されておらず、(b) 論理接続が自動化されていない (つまり、データは人による管理のもとで手動によってのみインターフェースを介して転送される) 2 つのシステム間のインターフェースです[4]。従来、エアギャップは、サーモスタットや家電製品などの運用技術を保護するためのゴールドスタンダードでした。現在はほぼあらゆるものが無線または有線ネットワークに接続されているため、リカバリ可能な適切なデータコピーを維持するには厳格なエアギャッププロセスが必要不可欠です。

ネットワークに接続された環境では、無線信号と有線信号がすべて無効化されたシステムさえも経由して、ハッカーはほぼすべてのエントリポイントを悪用できてしまいます。データの安全性を高めるための最も閉ざされたシステムでは、一部の IT 部門は、すべての USB ポートを無効にし、ファラデーケージを使用してすべての無線送信をブロックし、電磁波の漏えいを防ぎます。

自動イメージレプリケーション (AIR) を使用すると、パブリッククラウドを含む同じサイトまたは異なるサイト内のバックアップドメイン間で、バックアップデータをレプリケートできます。バックアップのオフラインエアギャップコピーを有効にして、意図しないソースによるデータアクセスの脅威をさらに軽減することもできます。自社所有のデータセンターとパブリッククラウドでデータが拡大するにつれ、重要なデータの最新の正常なコピーを維持するために、エアギャップ構造を実装するバックアップおよびリカバリソリューションが重要になります。

### クラウドデータとエアギャップ

クラウドファーストが増えています: 企業の 85% が 2025 年までにクラウドファーストになると発表し、94% がマルチクラウド戦略を実装しています[5]。クラウド戦略の加速が急増した結果、異なるツールや意思決定権限が混在している可能性があります。プライマリデータとリポジトリをさまざまなパブリッククラウドオプションで多様化および最適化するのと同様に、稼働を再開できるように最適に構築されたソリューションでデータリカバリアプローチを最適化することが重要です。

ベリタスは、考えられる最適なオプションとして分離型リカバリ環境 (IRE) の機能をお勧めします。IRE で提供されるエアギャップソリューションは、重要なデータの安全なコピーを作成してファイルのクリーンなセットをオンデマンドで管理者に提供し、マルチクラウド環境内でランサムウェア攻撃からの影響を無効化します。

## 分離型リカバリ環境

従来のネットワーク分離ソリューションでは、安全な場所間の接続を物理的または論理的に分割しており、すべての通信のやりとりが不可能になります。これは、データ転送を分離型環境に制限し、3 次コピーが必要な場合にリカバリ時間目標 (RTO) とリカバリポイント目標 (RPO) を脅かすものです。ソースからターゲットへレプリケーションデータをプッシュすると一般的に考えられているソースドメインは、レプリケーションジョブを独立して処理し、ターゲットドメインへ送信します。この従来のアプローチでは、接続が停止したりブロックされたりした場合、重要なデータを安全な環境へレプリケートするために利用できる時間が制限されることになります。

一方、プルレプリケーションモデルは、レプリケーション要求をターゲットから開始します。ベリタスの NetBackup の IRE ソリューションは、プルレプリケーションモデルを提供してデータ移動を最適化します。このモデルでは、データ送信要求が IRE のメディアサーバー重複排除プール (MSDP) から発信され、反対方向の接続はデータフローをより適切に制御して、論理的かつ物理的に環境の保護を強化します。IRE へのレプリケーションは、IRE エアギャップスケジュールで定義される特定の時間帯のサポートなど、IRE 内から完全に制御できるようになりました。

侵入検出メカニズムと送信中および保管中のデータの暗号化を含む複数のセキュリティ層により、データ転送中に NetBackup IRE に侵入することはできません。データジャーニー全体にわたって、データは保存場所を問わず安全です。ストレージは侵害されず、悪質なユーザーや権限のないユーザーがデータを読み取ったり変更したりするリスクは一切ありません。ベリタスは、オンプレミスおよびクラウドでのデータ分離オプションを NetBackup Recovery Vault によって提供します。これは、シームレスなクラウドの STaaS (Storage as a Service) であり、エアギャップによってランサムウェア攻撃を防止し、規模に応じて最適化され、予測可能なコストによってデータの移行性を確保します。

ベリタスは、オンプレミスまたはクラウドのすべての NetBackup を IRE フレームワークに変換できるシンプルなワークフローを提供し、3 つの主要な原則に基づくランサムウェア攻撃からの回復力を実現します。

- **保護**: 分離型のリカバリ機能を容易に組み込み、ベリタスのゼロトラストセキュリティ戦略と合致する多要素認証 (MFA) およびロールベースのアクセス制御 (RBAC) をサポートします。
- **検出**: NetBackup IT Analytics は、ランサムウェアをリアルタイムで検出できる異常検出を提供します。統合された NetBackup マルウェアスキャン機能は、異常スコアに基づいて優先順位を設定できるリカバリ前のマルウェアスキャンを提供します。
- **回復**: 分離型環境、クラウド、またはオンプレミスでデータセット全体のリカバリを統合します。RPO および RTO に関する幅広い要件を管理できます。

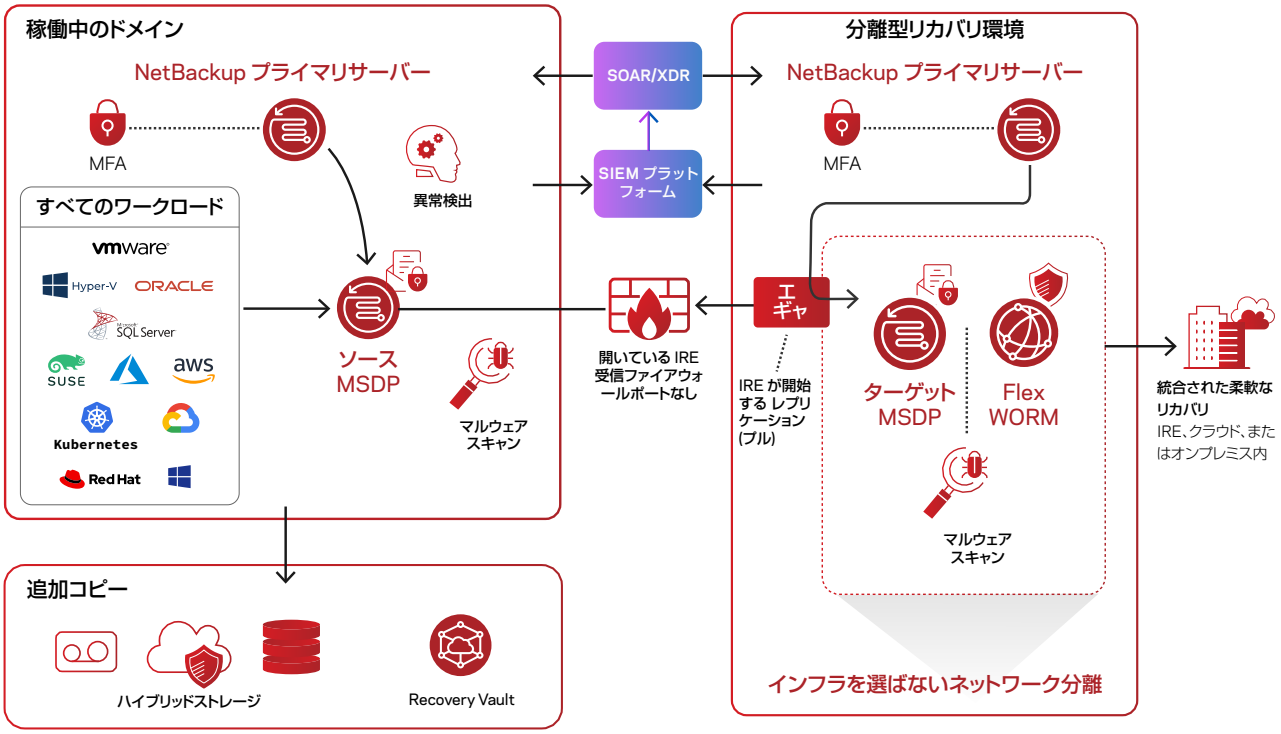


図 1. NetBackup の分離型リカバリ環境

分離型環境は、ランサムウェアとマルウェアに対抗するための回復力をさらに強化します。

### ゼロトラストによる保護の強化

ゼロトラストポリシーは、さらに保護を強化します。ゼロトラストの考え方を全社的に導入すると、壊滅的な攻撃のリスクが低減することが実証されています。

ベリタス IRE は、Flex アプライアンスのコンテナベースのマルチテナント WORM (Write Once Read Many) ストレージに基づき、OS とゼロトラストアーキテクチャを強化しています。ユーザー、ツール、マシンの ID およびアクセス管理 (IAM) を MFA と RBAC で強化することにより、機密性の高いデータとバックアップへのアクセスを制限します。データにアクセスする必要があるユーザーのみを許可する必要があります。パスワードの健全性も最優先事項です。

これらの領域へのアクセスを、すべてがゼロトラストに基づいて構築された強力な IAM 制御、権限制御、強化、安全なハードウェアによって防止できます。影響を最小限に抑える複数のセキュリティ層が用意されているため、侵害が発生した場合でも、攻撃面や影響範囲が少なくなります。システムに侵入したサイバー犯罪者は、多くの場合、環境内を横方向に移動して重要なビジネスデータ、機密情報、バックアップシステムを検索します。

### 異常検出とマルウェアスキャン

包括的な可視化、インテリジェントな異常検出、マルウェアスキャンにより、すべてのデータの場所を確実に把握するとともに、運用の複雑さを軽減し、コスト管理を最適化することができます。ベリタスの AI 搭載の異常検出は、環境全体で通常とは異なるデータとユーザーアクティビティを認識し、疑わしいアクティビティをほぼリアルタイムで警告します。この機能によってデータは常にリカバリ可能な状態となっており、ランサムウェア攻撃を受けた場合は直ちに対処して、マルウェアの含まれるバックアップを分離し、バックアップデータへのマルウェアの影響を限定することができます。スキャンされ、安全であることが検証済みのイメージ全体を復元することも、個々のファイルを復元することもできます。復元対象としてマークされているファイルが感染している場合は、未感染のバックアップから復元できます。これにより、ターゲットマシンを再感染させるリスクを負うことなく、安全かつ効果的にデータをリカバリできます。

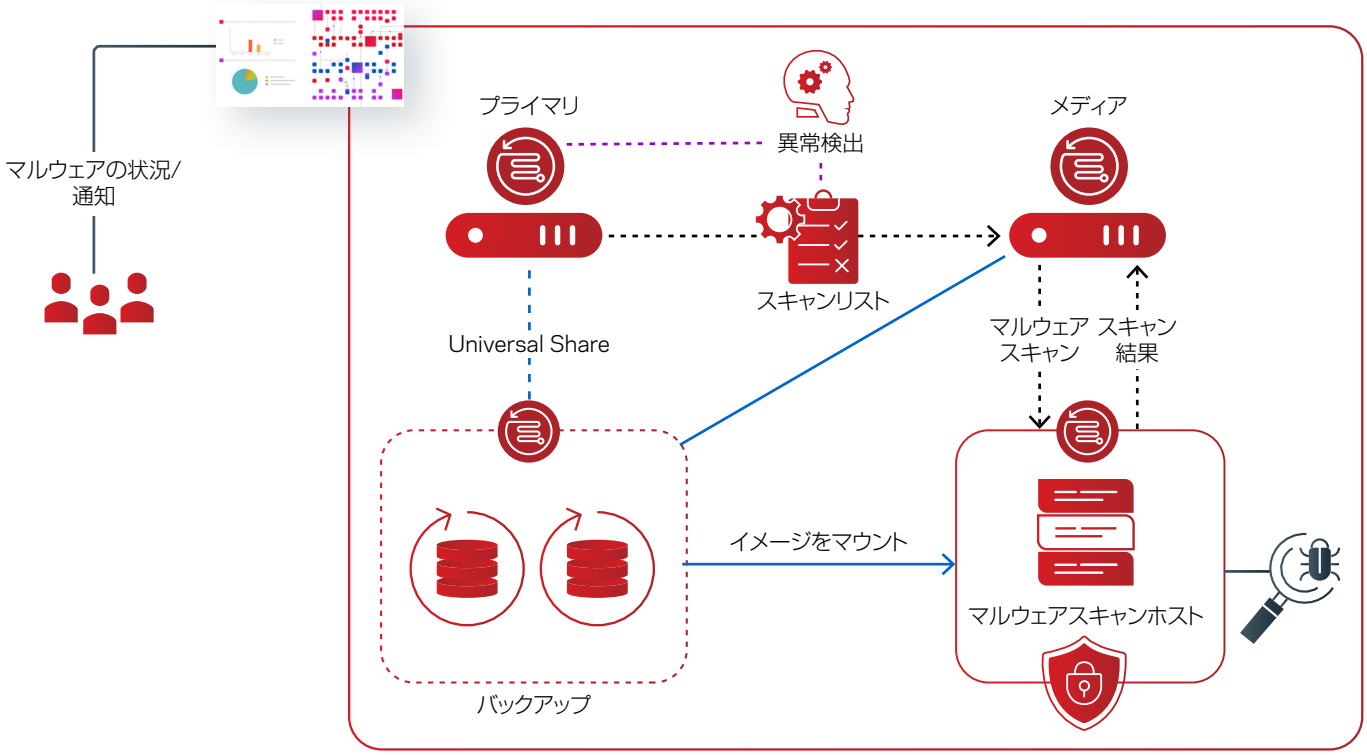


図 2: NetBackup に統合されているマルウェアスキャン

### 改ざんも消去も不可能なストレージを使用したリカバリ

改ざんも消去も不可能なストレージにより、決められた期間 (または常時)、誰も何もデータを変更、暗号化、または削除することはできません。データの改ざんや不正アクセスも防ぎます。IRE 戦略の一環として、NetBackup Recovery Vault は、お客様のニーズに応じてスケールアップまたはスケールダウンできる、改ざんも消去も不可能なクラウドベースのストレージソリューションを提供します。

## IRE による確実なリカバリ

NetBackup の分離型のリカバリ環境なら、リスクを低減し、不確実性をなくし、制御を維持できます。Veritas.com/ja/jp にアクセスする、またはベリタスチームに問い合わせて、ベリタスのソリューションがマルチクラウド環境内でどのようにランサムウェア攻撃からの回復力を確保できるかをご確認ください。

企業のサイバーレジリエンス戦略のギャップを解消しましょう。詳細をご確認ください >


1. www.gartner.com/en/newsroom/press-releases/2021-01-28
2. www.sonicwall.com/resources/white-papers/2023-sonicwall-cyber-threat-report/
3. www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
4. csrc.nist.gov/glossary/term/air_gap
5. www.gartner.com/en/newsroom/press-releases/2021-11-10


### ベリタスについて

Veritas Technologies は、マルチクラウドデータ管理のリーダーです。データの保護、リカバリ能力、コンプライアンスを確保するために、Fortune Global 100 の 95% を含む、先進企業 80,000 社以上が、ベリタスのソリューションを導入しています。ベリタスは、ランサムウェアのようなサイバー攻撃がもたらす脅威に対してお客様が必要とする回復力を提供し、大規模な環境でも信頼できると評価をいただいております。単一の統合されたアプローチを通じ、800 以上のデータソース、100 以上のオペレーティングシステム、1,400 以上のストレージターゲット、60 以上のクラウドをサポートしており、ベリタスの実行能力に匹敵するベンダーは他にありません。Cloud Scale Technology により、ベリタスは運用にかかる煩雑さや業務量を削減しつつ優れた価値を提供する、自律型データ管理の戦略を提供しています。ベリタステクノロジーズ合同会社は、Veritas Technologies の日本法人です。

VERITAS


〒107-0052 東京都港区
赤坂 1-11-44
赤坂インターシティ 4 階
www.veritas.com/ja/jp

各国オフィスとお問い合わせ先については、弊社の Web サイトを参照してください。
veritas.com/ja/jp/company/contact





V1626 05/23