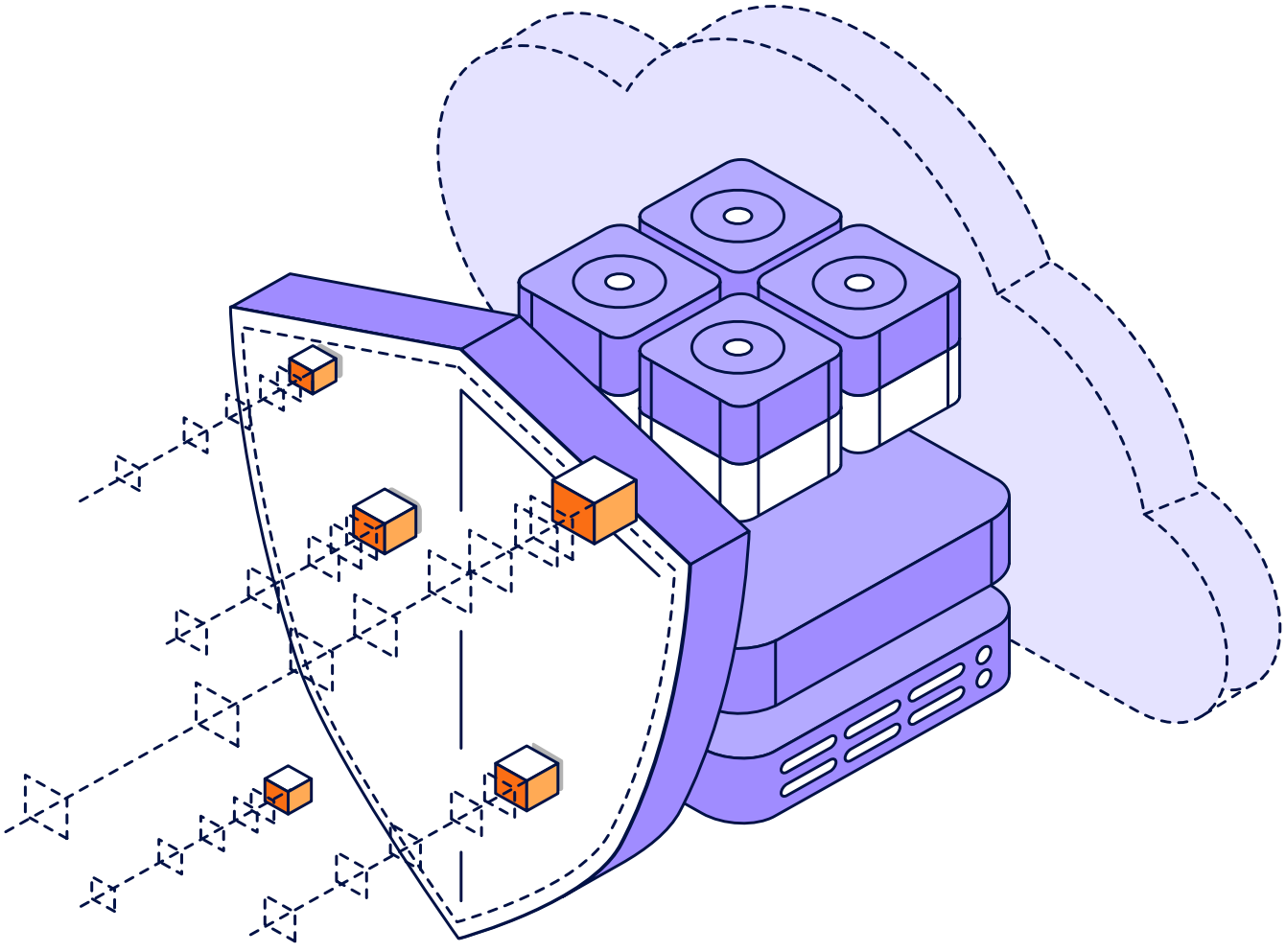
ハイブリッドクラウドのためのサイバー回復性

IT 担当者とセキュリティ担当者 7,000 人以上から得た教訓とは



ここ数年で、オンプレミスのデータセンターから「***理にかなっていればクラウド***」への転換が起こり、その後さらに***クラウドファースト***戦略、***あらゆる場所でハイブリッド***の状態を経由して、現在は最新の IT を実現するための通常モードとして「***戦略的マルチクラウド***」が使用されるようになりました。2024 年に向けた現在、クラウドベースのサービスを活用すべきかどうか、あるいはどのクラウドサービスを活用すべきかは、論点にはなっていません。現在の課題は「いくつクラウドが必要なのか」であり、サイバーセキュリティによるインシデントの予防、データ保護、その他の重大な IT 統制を確保しながら、自社の IT チームでその全てのクラウドをどう管理できるかという点が懸念されています。

それらの疑問の答えを出すために、この調査概要では、2022 年 8 月から 2023 年 3 月までにそれぞれ個別に実施された次の 3 つの調査の結果について、情報をまとめました。

- クラウドプロテクションレポート 2023
  IaaS、PaaS、SaaS 管理者 1,700 人を対象とした、データ保護戦略に関する調査。
- 2023 データプロテクションレポート
  組織のデータ保護戦略を担当する 4,200 人の IT リーダーを対象とした調査。
- 2023 ランサムウェアトレンドレポート
  2022 年にサイバー攻撃を受けた組織に属する CISO/ セキュリティ専門家 / バックアップ専門家 1,200 人を対象とした調査。

これら 3 つの調査は全て、独立した調査機関またはアナリスト会社の無作為のパネルに基づいて実施され、Veeam® はそのデータを受け取り、さまざまな形式で公表しています。レポートでは一貫して、次の 4 つのポイントが明らかにされています。

- クラウドベースのサービスが、データセンターとクラウドホスト型のワークロードを保護する上で鍵になっている。
- クラウドは他の形態と同様か、おそらくそれ以上にランサムウェア攻撃を受けやすくなっている。
- あるクラウドで別のクラウドを保護するのは良いが、クラウドで自ら保護するのは良くない。
- セキュリティ、DR、クラウド、オンプレミスのチーム間の連携が不足しているため、まずはその状況を改善する必要がある。

クラウドベースのサービスはデータセンターとクラウドホスト型のワークロードを保護する上で鍵になっている

82%

イミュータビリティに対応したクラウドベースのストレージを現在利用している組織の割合。

調査では一貫して、クラウドベースのサービスが、クラウドホスト型のワークロードに加えて、従来のオンプレミスのワークロードを保護する上でも不可欠との結果が示されています。*特に注目すべき点は、クラウドベースのストレージにより、**「存続可能な」リポジトリ**（イミュータビリティなど）や、必要時の**ディザスタリカバリ用のインフラストラクチャ**が実現されていることです。*

ほとんどの組織にとって、ランサムウェアからの保護において、次のようなほぼ普遍的といえる状況が見られます。

- データセンターのサーバーを保護するには、データを外部（オフサイトまたはクラウドなど）に出す必要がある。
- ランサムウェアから復旧するには、サイバー脅威による影響を受ける可能性のないバックアップコピーが必要になる。

『2023 ランサムウェアトレンドレポート』の調査結果によると、この 2 つを組み合わせることが 2023 年の「教訓」のようです。**82%** の組織は現在、イミュータビリティに対応したクラウドベースのストレージを利用しています。[1]

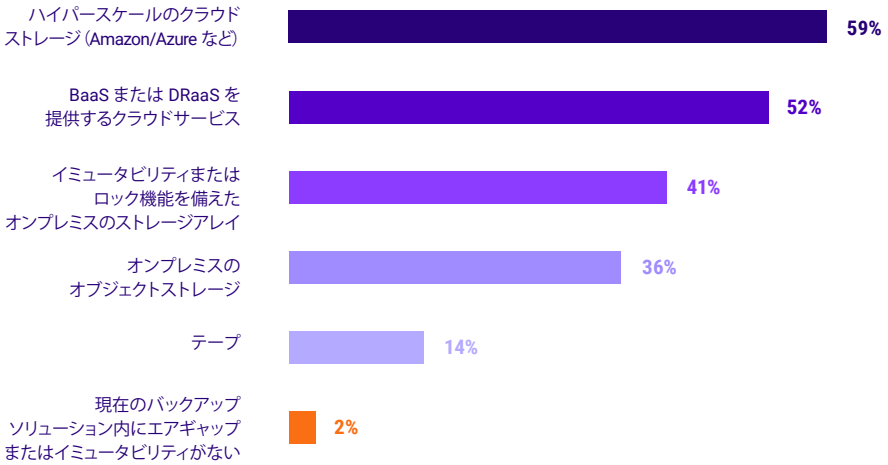


図 1.1

次の媒体を用いた、物理的に隔離されたオフラインのバックアップ、またはイミュータブルバックアップを利用していますか？

存続可能なバックアップコピーを確保できるようになれば、組織はさらに、従来の事業継続性 / ディザスタリカバリ（BC/DR）戦略における他の側面も検討できるようになります。サイバー攻撃が災害の 1 つの（特殊な）形態だと見なされる傾向が高まっており、サイバー回復性とディザスタリカバリが相互に強く関係していると考える人も当然多くなっています。いずれの場合も、次に実用性の観点から**「復元やフェイルオーバーの実行先をどこにするか？」**という課題が生じます。

サイバー攻撃の被害者から得た教訓として、組織の復元戦略には、ランサムウェアなどの危機からの修復時に、データセンターのサーバーをクラウドホスト型インフラストラクチャに復旧できるようにすることが盛り込まれています。[2]

図 1.2

ランサムウェアからサーバーを復旧する際の、データの復元先は？

上記のデータは、ほとんどの組織が、危機の範囲に基づいた、柔軟なハイブリッド戦略をとっていることを示しています。その証拠に、**71%** の組織はクラウドを使用して復元できる一方、**81%** の組織はオンプレミスのインフラストラクチャを使用して復元できており、この 2 つは多くの部分で重なり合っています（柔軟性）。組織がディザスタリカバリ計画で対策している、より広い範囲の危機の発生時に、**54%** の組織は、代替的な場所にフェイルオーバーする計画である一方、**46% は、クラウドホスト型インフラストラクチャをディザスタリカバリサイトとして使用する計画です**。とは言え、クラウドを利用したディザスタリカバリサイトを確立する方法はいくつかあります。[3]

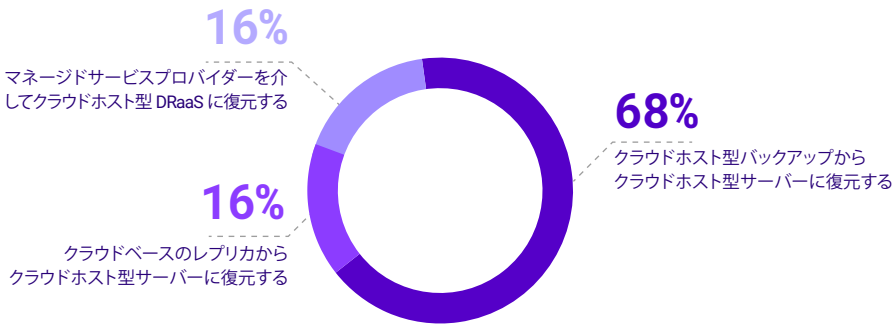


図 1.3

ディザスタリカバリ用のクラウドサービスを使用している場合、事業運営はどのように再開されますか？

ディザスタリカバリ計画で活用するのが Disaster Recovery as a Service（DRaaS）プロバイダーであっても、Amazon Web Services や Microsoft Azure などの自己管理によるクラウドホスト型インフラストラクチャであっても、成功させるためには最終的に次の 2 つの重要な機能が必要になります。

- リストアの実行中にバックアップを変換できる機能。たとえば、元々物理サーバーか仮想サーバーで保護されていた本番サーバーをクラウドホスト内に復元して、稼働させること。
- 復元プロセスのオーケストレーション機能。たとえば、リストアワークフローの実行中にマルウェア検出のために隔離すること。

残念ながら、現在は次のような状況です。

- フェイルオーバーによる復元のためのオーケストレーションされたワークフローのスクリプトを作成できる組織は、わずか **18%**。[4]
- リストアの実行中に、環境への再感染を防止する手段として、隔離されたテスト領域、つまり「サンドボックス」を利用してマルウェアの有無をスキャンしている組織は、わずか **44%**。[5]

これらは、自社のデータ保護ソリューションまたはサービスが復元プロセスを大規模に自動化できるかどうか、また確実に安全に復元できるかどうかを尋ねるもので、シニアリーダーシップにとっては答えづらい質問だと思われます。

クラウドは他の形態と同様か、おそらくそれ以上にランサムウェア攻撃を受けやすい

*クラウドベースのサービスはハイブリッド IT アーキテクチャ内部でシームレスにアクセスできるようになっていると想定されることから、***サイバー攻撃の発生時、クラウドベースのワークロードも他の形態と同程度に影響を受けやすい***ことが、調査で一貫して明らかになっています。実際、データセンターリソースと比べると、クラウドサービスへのアクセスを防止するためにはさまざまなセキュリティ技術を利用する必要があります。それを考慮すると、ユーザーとクラウドプラットフォームの間の接続性を妨害するといった他の攻撃の可能性も生まれます。*

「クラウドはもうすぐ来るのではなく、もう来ている」と言われますが、同時に、IT 部門はクラウドベースのサービス内で新しいワークフローの運用が開始されるのとほぼ同じペースでオンプレミスのプラットフォームを廃止しているわけではないことを認識する必要があります。組織は、IT 配備のために増えつつあるハイブリッド戦略の一環として、クラウドホスト型インフラストラクチャを採用しています。

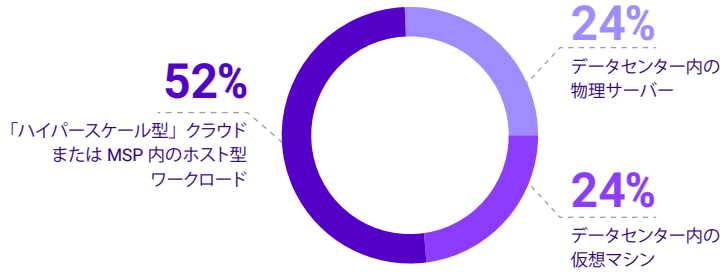


図 2.1

本番サーバーのワークロードに使用する「ハイブリッド型」プラットフォームの配分（2024 年予測）。[6]

注意点として、データセンター中心の IT 設備内でプラットフォームが発展していく状況とは異なり、導入、使用、保護の対象となるのは「1 つのクラウド」アーキテクチャだけではありません。これはどのクラウドベンダーにも言えることです。そうではなく、クラウドアーキテクチャは無数にあり、それぞれ幅広いプロバイダーがいて、その基盤となる管理フレームワークも非常に多様であることを認識する必要があります。

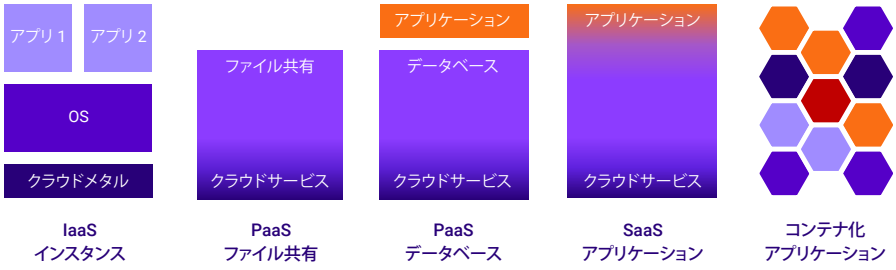


図 2.2

無数のクラウドアーキテクチャ。

クラウドベースのサービスは回復性のあるサービスだとよく捉えられますが、残念ながら、システム停止は依然として発生しています。その原因としては、クラウドサービスプロバイダー内部の問題、管理者によるクラウドサービスをまたいだ構成ミス、ユーザーとクラウドサービスの間の接続性の問題などが挙げられます。一方で、2021 年と 2022 年の両調査レポートにおいて、サイバー攻撃によるシステム停止は前年比で増加しており、2021 年、2022 年の両方で、最も影響の大きいシステム停止の原因であり続けています（2023 年もそのペースが落ちている兆候は見られません）。[7]

- **48%** の組織で、**「パブリッククラウドのリソースが利用不能になった」**ため IT の中断が発生しました。
- **52%** の組織で、**「インフラストラクチャまたはネットワークの停止」**により IT の中断が発生しました。
- **53%** の組織で、**「サイバーセキュリティイベント」**ため IT の中断が発生しました。

ほとんどのサイバー攻撃では、最初の侵入が体系的に機会を探るものであっても（ユーザーがクリックすることを期待してフィッシングメールのスパムを送信するなど）、その同じ攻撃者が、既知の脆弱性のあるシステムや、普及率の高い IT プラットフォームが十分に保護されていない可能性のあるシステムを標的にしています。『2023 ランサムウェアトレンドレポート』の調査結果によると、**サイバー犯罪者による攻撃の 38% で、クラウドホスト型ワークロードが標的となりました。**[8]

サイバー攻撃の被害に遭った 1,200 人に対する調査では、暗号化などの影響を受けたデータ量が、クラウドホスト型データとデータセンターのデータでほぼ同じであったことが確認されました。

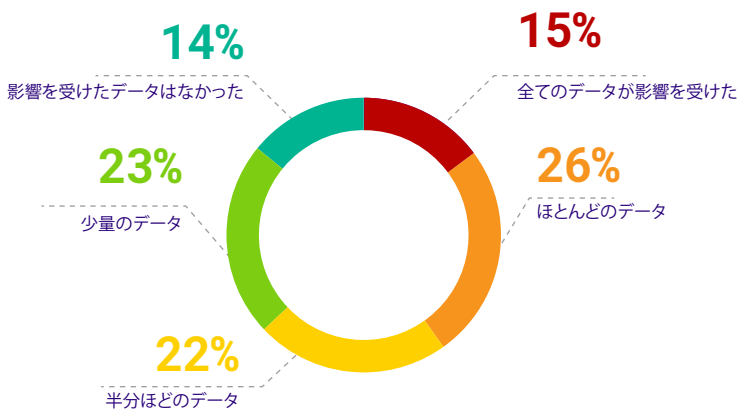


図 2.3

クラウドプラットフォーム上でホストされるデータのうち、直近のランサムウェア攻撃により影響を受けたデータの割合。[9]

重要な点として、データセンターのデータ、ブランチオフィス / リモート環境のデータ、クラウドホスト型のデータで近い感染率となっていることから、次の 2 つの実態があることが推察されます。

- ハイブリッド IT は非常にシームレスな構成であるため、サイバー犯罪者による犯行が標的の環境内で開始された後は、クラウドホスト型データも、物理データセンター内のアプリケーションやファイルと同程度に攻撃に対して脆弱です。
- このようにシームレスであり、同等の脆弱性があることから、クラウドホスト型のファイル、データベース、アプリケーションは、オンプレミスのワークロードと同じ手法で、同じように厳格に保護する必要があります。

2024 年までに、自己管理型の物理データセンターの外部で実行されるワークロードの方が、従来の上げ床式スペースで実行されるワークフローよりも初めて多くなる見込みです。

あるクラウドで別のクラウドを保護するのは良いが、クラウド自ら保護するのは良くない

*クラウドのデータをバックアップした「担当者」と、データを保護する現在の「手段」について2023 年に調査したところ、3 つの調査プロジェクトの全てで、オンプレミスのデータの保護を担当する**「中心的な」バックアップチーム（またはサービスプロバイダー）がクラウドホスト型データの保護も担当する場合が最も多い**ことが確認されました。ただし、この「手段」については混乱が多く見られました。その典型的なケースとして、組織が多機種に対応したエンタープライズ・バックアップ・ソリューションではなく、プラットフォーム「組み込み」のユーティリティを使用するしかないと思い込んでいる場合があります。*

組織がクラウドホスト型ワークロードを保護する「手段」を考察する前に、さまざまな「担当者」を考察することが重要になります。データ保護の担当者の大半は「従来の」IT バックアップチームであり、クラウド管理者との比率でいうと約 2:1 という、おおよそ一貫した調査結果となっています。

2 : 1

「従来の」IT バックアップチームとクラウド管理者によるデータ保護の作業の比率。

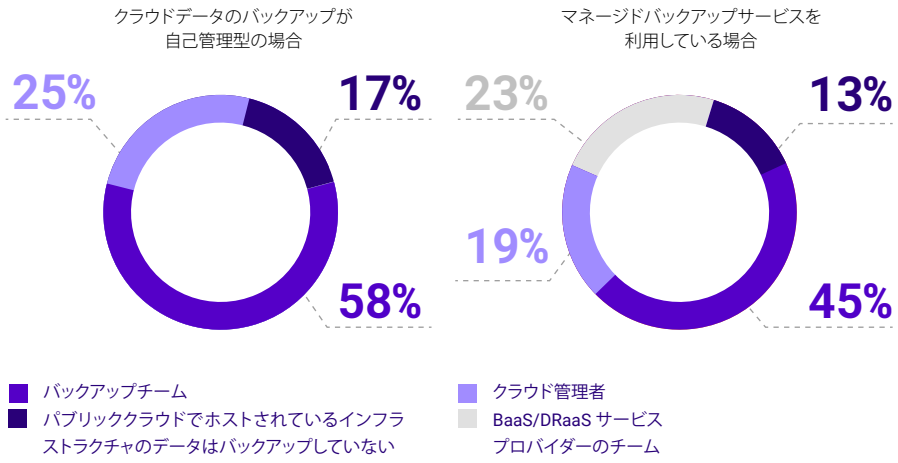


図 3.1

クラウドでホストされているサーバーのバックアップやデータ保護の管理を担当しているのは誰ですか？[10]

驚くことに、8 人に 1 人 (13%) は、組織がクラウドホスト型インフラストラクチャのバックアップをしていないと思うと回答しました。その質問後、ハイブリッド戦略を採用している多くの組織に対する次の質問は、クラウドバックアップを同じクラウド内、異なるリージョン、異なるクラウド、またはオンプレミスのいずれに配置可能であるかについての認識を問うものでした。これはクラウドホスト型ワークロード向けのバックアップソリューションを選択する際に重要な検討項目となります。

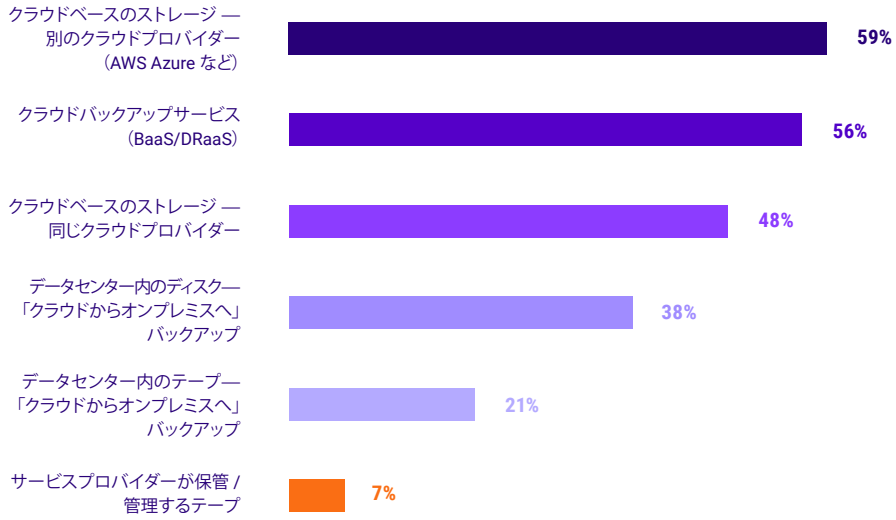


図 3.2

1 年以上保持しているクラウドバックアップデータについて、それらのバックアップはどこに保管していますか？[11]

- IT リーダーの **37%** は、「ワークフローをクラウドから別のクラウドに移動できること」を「最新」または「革新的」なデータ保護ソリューションの特徴であると考えています。[10]
- **88%** の組織に、ワークロードをクラウドからオンプレミスに戻した経験、または別のクラウドに移動した経験があります。[11]

言うまでもなく、クラウドホスト型ワークロード向けのバックアップソリューションを選択する際に、単純に、多くのクラウド企業が特定のワークロード向けに提供している「組み込み」のユーティリティまたはエクスポート機能を使用するという手段もあります。多くの場合、クラウドワークロードを包括的に保護するサードパーティのツールが利用可能であることを知っていれば、その手段は選択されていません。[12]

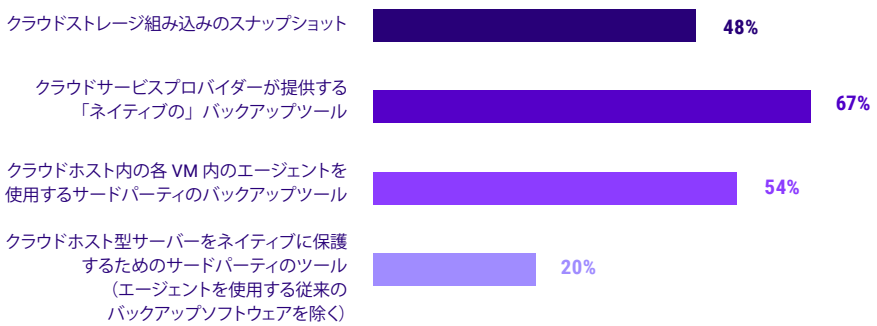


図 3.3

クラウドでホストされているデータの保護の手段として知っているものはどれですか？（現在実際に使用しているかどうかは問いません）

*スナップショットについて検討する場合は、*オンプレミスのファイルサーバーのスナップショットに完全に頼れるかどうか、自問してみてください。スナップショットは、最新に近い復元ポイントまで復元するためのパワフルな復元ツールであり、瞬時に復元できる場合もあります。次のような理由から、**スナップショットはバックアップに代わる手段にはなり得ません。**

- 同じサイロで攻撃に晒されるため（スタンドアロン NAS が IaaS ストレージスタックに関連付けられ、共通のログイン情報などが使用されます）。
- 長期的に保持するにはコストが高いため。そのため、ほとんどの組織でスナップショットの保持期間は数日となっている一方、バックアップの保持期間は週単位、月単位、年単位となっています。

*ワークロードを中心とした、または組み込みの「ネイティブ」のユーティリティを検討する場合は、*オンプレミスのプラットフォームが以下の手段で保護されているかを確認してください。

- **Oracle** データベースの保護に ZDLRA（または RMAN）を使用している。
- **Windows Server** のバックアップに NTBackup ユーティリティ(またはシステムツール)を使用している。
- **VMware** ホストのバックアップに VDPA のみを使用している。
- **Microsoft 365** のバックアップに ASB のみを使用している。

次に、IT チームがバックアップ用に管理したいツールの数と、（それらのツールはそれぞれ異なるリポジトリと形式でデータを書き込むことから）ストレージの予算額を確認してください。スナップショット取得ツールやその他のシングルプラットフォーム向けのユーティリティ（「組み込み」ツールなど）には、さらに問題があります。それらの大部分は、つい最近のエラー(データの上書きやインポート不良など）から短時間でロールバックできるように、保持期間が制限された設計となっているためです。数週間も潜伏する可能性のあるランサムウェアから復旧することを考えると、そのような限定されたアプローチでは不十分である（あるいは桁違いのコストがかかる）と思われます。こういった所感は、次の 2 つのデータポイントでも数値として現れています。

- IT リーダーの **35%** は、**「オンプレミスや IaaS/SaaS のポリシーの保護が標準化されていること」**を「最新」または「革新的」なデータ保護ソリューションの特徴であると考えています。[13]
- **42%** の組織は、**「クラウドホスト型ワークロードを保護できること」**がエンタープライズデータ保護ソリューションに必要不可欠な特徴であると考えています。[14] この所感が、2023 年の調査で最も多く、また最も重要な回答となりました。

35%

「オンプレミスや IaaS/SaaS のポリシーの保護が標準化されていること」を「最新」または「革新的」なデータ保護ソリューションの特徴であると考える IT リーダーの割合。

セキュリティ、DR、クラウド、オンプレミスのチーム間の連携が不足しているため、まずはその状況の改善を

*この 3 つの調査プロジェクトではデータ保護を担当する IT リーダー、CISO または類似したエグゼクティブ、セキュリティ専門家、IaaS/PaaS/SaaS 管理者、バックアップ運用担当者など、幅広いペルソナが対象となりました。その全ての調査で、1 つのチームだけで中心的機能を担当することはなく、常に影響力や責任の範囲が重なり合っていることが確認されました。それなのに、**戦略的要件とテクノロジーの実装 / 使用のいずれでも、回答者が他のチームとしっかり連携しているとはほぼ感じていないことがデータで明らかになりました。***

これらの調査の大半で、使用しているテクノロジーやそのテクノロジーの選択に至った理由 / 戦略に重点を置いていますが、調査データ上は、これらの調査の対象となったペルソナ間での連携が不足していることが一貫して明確に示されています。[15]

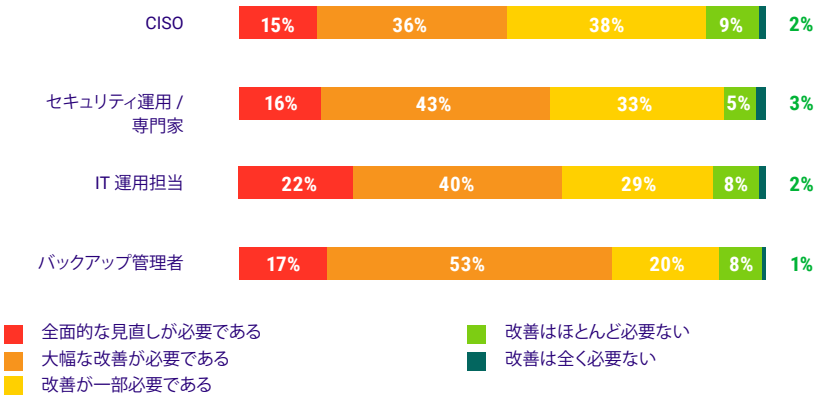


図 4.1

貴社の IT バックアップチームとサイバーセキュリティチームが完全に連携するためには、どれほどの改善が必要だと考えていますか？

注目すべきポイントとして、『2023 ランサムウェアトレンドレポート』で調査対象となった 4 つのペルソナのうち、イベントからの修復に「近い」立場にいるほど（たとえばバックアップ管理者の方が CISO よりも近い）、チーム間の協力や連携に満足していません。

同じような連携不足は、Microsoft 365 の保護のための根拠やツールについて検討する際の SaaS 管理者とバックアップ管理者の間や、クラウドホスト型サーバー、ファイル共有、データベースの保護のための戦略やツールを検討する際の IaaS/PaaS 管理者とバックアップ管理者の間でも確認されました。

検討すべき課題

8 ヶ月以上の期間に及び、7,000 人を超える回答者を対象に実施された調査の結果より、サイバー回復性戦略で検討すべき主な課題として、次のようなものが挙げられます。

- バックアップがイミュータビリティとオフサイトの両方の特徴を備えているか?バックアップは実績あるプロバイダーに管理されているか、それとも自社で管理されているか?
- ディザスタリカバリサイトとしてクラウドインフラストラクチャを使用しても大丈夫か?だめな場合、その理由は?
- IaaS、PaaS、SaaS のワークロードを含めて、クラウドホスト型データの全てをバックアップしているか? その場合、クラウドごとに異なるツールを使用しているか?それとも、全てのクラウド（およびオンプレミスのワークロード）に同じ手段を導入しているか?
- オンプレミス、IaaS、PaaS、SaaS のバックアップに関連するチーム間でどれほど連携が取れているか?
- サイバー対策とデータバックアップのチーム間でどれほど連携が取れているか?
- 前回クラウドベースのデータの復元をテストしたのはいつ頃か?
- 前回大規模なデータセンターの復旧をテストしたのはいつ頃か?
- 前回サイバー対策および BC/DR に関する戦略集を評価し更新したのはいつ頃か?

調査やその考察についてご不明な点がある場合は、StrategicResearch@veeam.com までお問い合わせください。

本書で引用した調査レポート全文は、以下のリンクをクリックしてご覧ください。

- クラウドプロテクションレポート 2023
  IaaS、PaaS、SaaS 管理者 1,700 人を対象とした、データ保護戦略に関する調査。
- 2023 データプロテクションレポート
  組織のデータ保護戦略を担当する 4,200 人の IT リーダーを対象とした調査。
- 2023 ランサムウェアトレンドレポート
  2022 年にサイバー攻撃を受けた組織に属する CISO/ セキュリティ専門家 / バックアップ専門家 1,200 人を対象とした調査。

Veeamの視点

Veeam のバックアップおよびデータ管理プラットフォーム

オンプレミス、端末上、クラウド内を問わず、あらゆるデータが保護され、常に利用可能であると確信できることは、今や過去に例を見ないほど不可欠になっています。Veeam はひとつのプラットフォームで、クラウド、仮想、物理、SaaS、Kubernetes の各環境に対応します。業界で最もシンプルかつ柔軟性と信頼性に優れたパワフルなプラットフォームで、皆様のアプリやデータをランサムウェアや障害、有害な攻撃者から保護しながら、常にアベイラビリティを維持します。

Veeam を利用すれば、データが常に保護されて常に利用可能な状態を保てます。デジタル変革を加速させ、サイバー犯罪からビジネスを保護し、ビジネスの回復性を促進するための確信をお届けします。コストと複雑さの軽減、そしてビジネス目標の達成のために、No.1 のバックアップと復元を誇る Veeam を是非ご活用ください。

詳細については、https://www.veeam.com/jp をご覧ください。

Veeam のハイブリッドクラウド専門家に話を聞く場合は、コンサルティングをご依頼ください（http://vee.am/hybridcloudinquiry）。

本調査データや見解に関するご質問は
StrategicResearch@veeam.com まで

1 『2023 ランサムウェアトレンドレポート』、Q29
2 『2023 ランサムウェアトレンドレポート』、Q25
3 『2023 データプロテクションレポート』、Q45
4 『2023 データプロテクションレポート』、Q46
5 『2023 ランサムウェアトレンドレポート』、Q21
6 『2023 データプロテクションレポート』、Q2
7 『2023 データプロテクションレポート』、Q13 と Q14
8 『2023 ランサムウェアトレンドレポート』、Q9
9 『2023 ランサムウェアトレンドレポート』、Q6
10 『2023 データプロテクションレポート』、Q17
11 『クラウドプロテクションレポート 2023』、Q4
12 『2023 データプロテクションレポート』、Q35
13 『2023 データプロテクションレポート』、Q17
14 『クラウドプロテクションレポート 2023』、Q4
15 『2023 ランサムウェアトレンドレポート』、Q1