COHESITY

クラウドバックアップ:

BaaSの詳細な評価ガイドとチェックリスト

データアジリティ、運用効率、サイバーレジリエンスの向上

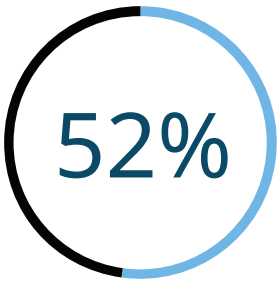
目次

クラウド時代のバックアップ

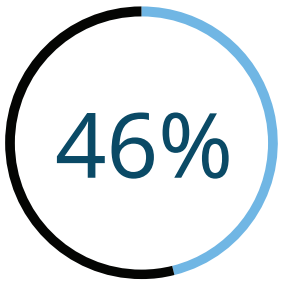
近年、クラウドコンピューティングによるITの近代化は、急速な革新と成長をもたらしています。しかし、重要なITインフラがすべてクラウドの導入と同じペースでレベルアップしたわけではないため、組織が手に負えないような非効率性や脆弱性を生み出しています。

見過ごされがちなクラウドのバックアップインフラのモダナイゼーションへの動きは、SaaSベンダーが提供するものを超え、最新のアプリケーションをクラウド上で実行するのと同じようなアジリティを企業にもたらすことができます。なぜなら、BaaS (サービスとしてのバックアップ) は、クラウド以前に構築されたレガシーのバックアップサイロを統合し、同時にクラウドでの体験、運用、コストを改善し強化する事業継続性の基本だからです。さらに、BaaSを利用することで、企業のサイバーレジリエンスを維持しながら、ビジネスインサイトのためにすべてのデータの潜在能力をより効果的に最大化することができます。

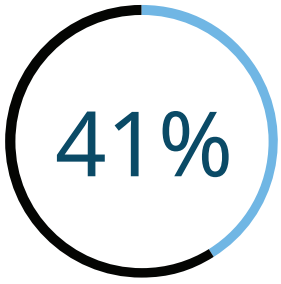
クラウドベースのデータ保護サービスの最も一般的なメリット



セキュリティの向上



バックアップの復旧性と信頼性の向上



IT人件費の削減

引用: Enterprise Strategy Group、「The Evolution of Data Protection Cloud Strategies」、2021年。

クラウドジャーニーに次の一歩を踏み出す

BaaSサービスを評価する際は、データがどのように保護されるか、どのような請求になるかなど、検討すべき機能を把握することが大切です。このガイドでは、重要な評価基準を詳細に説明し、クラウドジャーニーで参照できるチェックリストを提供します。

クラウドバックアップソリューションの比較では、まずサービスが以下の重要なBaaS機能にどう対応しているかを把握することから始まります:

1. データ保護と運用の自由度の向上
2. セキュリティとランサムウェアへの備えの強化
3. サステナビリティを備えた消費とコストの柔軟性の実現

現在の課題の評価

クラウドバックアップサービスを評価する前に、自社のオンプレミスで管理する (つまり、セルフマネージドの) バックアップとリカバリ環境と、バックアップベンダーが管理しクラウドでホスティングするバックアップとリカバリ環境の主な違いを明確にすることが大切です。表1は、セルフマネージドのオンプレミス専用のソリューションに共通するバックアップとリカバリの10の課題を概説したものです。

セルフマネージドのオンプレミス専用のソリューションに共通するバックアップとリカバリの10の課題

1. サイロ化したインフラストラクチャ (個別のサーバー、専用ストレージターゲットなど) は費用が高く、CAPEXが上がる
2. モダンでクラウドネイティブなSaaSアプリケーションの保護に対するサポートが不足しているため、ビジネスにおける競争力が不利な状況に置かれている
3. バックアップのワークフローを設定する際、異なるデータソースに対して複数の断片化されたUIで複雑な管理を行う必要があるため、ITのフラストレーションを増加させる
4. データをオンサイトや異なるパブリッククラウドに移行する場合は、ボルトオン型のクラウドゲートウェイが必要になり、複雑さが増す
5. フォークリフトアップグレードやシステム停止を要するアップグレードのため、計画的なダウンタイムが必要になる
6. リストアが遅いためRTO (目標復旧時間) の未達や最後の時点へのみの復旧となり、RPO (目標復旧時点) に悪影響を及ぼす
7. 圧縮を伴う可変/固定ブロックの重複排除は、コストが上昇につながる
8. ランサムウェア対策機能がないため、ビジネスへのリスクが高まる
9. 断片化のためデータの再利用できず、インサイトが見えなくなっている
10. 最新機能のデプロイが遅く、イノベーションの妨げとなる

表1: セルフマネージドのオンプレミスのバックアップとリカバリ環境の評価

デジタルビジネスは急速に進展しています。クラウドバックアップは、クラウドとデジタルトランスフォーメーションのジャーニーを維持するだけでなく、加速させることができます。

1 データ保護と運用の自由度を高める

組織がどのような種類の情報をどれくらいの期間保護しなければならないか、というビジネスや規制の要件は変化しています。そのような変化に迅速に対応できる包括的なクラウドバックアップソリューションが必要です。クラウドネイティブ、SaaS (Software as a Service)、オンプレミスのアプリケーションすべてに、保持ポリシーとSLA (サービスレベルアグリーメント) をサポートする一貫した方法がなければ、自社の全データを保護し、すでに過負荷のITスタッフにさらなる負担増を強いないことをどうやって保証できるでしょうか?

クラウドバックアップがビジネスにもたらす価値は、保険よりもはるかに大きいものです。運用の自由度が高く、最も高度なデータソース保護を実現するには、次の5つの重要な運用機能を備えたBaaSを選ぶ必要があります:

幅広いデータソースに対応

バックアップはシンプルであるべきです。しかし、現在ミッションクリティカルな全データのバックアップを管理することが難しいのは、異なるポリシー、SLA、保持期間を持つさまざまなクラウドプラットフォーム、サービス、APIがあるためです。これが複雑さを生んでいます。最適なシンプルさを実現するために必要なのは、複数の環境やクラウド全体で幅広いワークロードセットに対応する単一のBaaSソリューションです。これは、クラウドプロバイダーが提供するビルトインの保護機能以上の単一の統合サービスで、Amazon EC2やRDSだけでなくSaaSアプリケーション (Microsoft 365など) といったクラウドワークロードも統合し保護するサービスです。

最新のBaaSソリューションでは、レガシーなバックアップサイロを排除し、さまざまなデータソースセットに対して包括的で一貫したエンタープライズクラスの保護を実装することができます。これには以下が含まれます:

- クラウドネイティブのアプリ
- SaaSのワークロードとアプリ
- 内製のクラウドアプリ
- 仮想/物理サーバー
- 従来型/コンテナ型アプリケーション
- リレーショナル/分散データベース
- ファイルと非構造化データ

データ保護以外の目的でセカンダリコピーをクラウドへ送るメリット

41% オンプレミスのリソースに比べて優れたセキュリティ

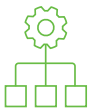
38% オンプレミスのリソースに比べて優れた可用性

37% より弾力性に優れたスケーラビリティ

36% より高いレベルのエンドユーザー同時接続を実現

35% 新規プロジェクトをデプロイする時間や価値を実感するまでの時間の短縮

引用: Enterprise Strategy Group、「From Data Backup to Data Intelligence」2022年



統合管理

クラウドコンピューティング時代より前に設立した組織は、Microsoft 365、Salesforce、Workdayといったクラウドベースのサービスをフル活用しながら、一部ワークロードのバックアップと復旧を自社管理している可能性があります。データがどこにあろうと、またはどのようにデプロイされていようと、組織にはエンタープライズレベルの保護が必要です。しかも、そのプロセスに管理サイロを生み出してはならないのです。適切なBaaSソリューションは、バックアップと復旧管理をひとつのUIに統合します。そのため、既存のSaaSアプリ (Microsoft 365やSFDCなど) に搭載された管理UIを利用したい場合でも、オンプレミスにあるセルフマネージド型のアプリやワークロードすべてを単一コンソールで完全に可視化することができます。導入検討中のBaaSソリューションが、ハイブリッドやマルチクラウド環境全体でバックアップデータを完全に統合し、単一インターフェイスを使用してデータを迅速にグローバル検索したりどこへでも復旧したりできることを確認してください。

シンプルな運用

クラウドプロバイダーは責任共有モデルで運営されています。クラウドプロバイダーが保証するのは、インフラストラクチャの稼働時間です。自社のデータを保護するのはあなたの責任です。例えばMicrosoft 365はMicrosoft Azureのクラウドで実行されますが、Microsoft 365の各生産性向上アプリ、Teams、SharePointには、それぞれ独自の制限された保護ポリシーが存在します。人材獲得競争が激化するにつれ、ほとんどの時間をワークロードやクラウドプロバイダーによる保護の管理といったルーティン作業に費やしているITの専門家は、ビジネスにより大きな影響を与える新たなチャンスを求めるようになります。エンタープライズグレードのBaaSは、数百ものポリシーを定期的に作成、実行することでITスタッフの負荷を軽減し、彼らがイノベーションに注力するための時間を提供します。また、データを可視化し、複数のクラウドサービスやオンプレミスのアプリでデータを保護する方法をシンプルにしながら、データをセキュアに守ります。

高い信頼性とパフォーマンス: 無停止アップグレード

今日の流れの速いデジタルビジネスの世界で、IT運用とLOB (事業部門) チームがバックアップに求めているのは、柔軟性、可用性、拡張性、そして信頼性です。最新のBaaSソリューションは、ランサムウェア攻撃に対抗しながらも、必要なデータを必要なときに利用可能な状態にすることで、SLA達成やビジネス成果の加速を支援します。クラウドバックアップは、ビジネスを中断させることなく、常時オンで更新も保護も行える準備が整っています。

データセンターの設置面積をほぼゼロへ

レガシーのバックアップインフラストラクチャには通常、サイバー攻撃に対してデータをより脆弱にするような製品パッチが含まれています。個々のSaaSベンダーがクラウドバックアップを行うということは、ランサムウェアの侵入経路が多くなるということです。オンプレミスのハードウェアがほとんどもしくはまったくない単一の統合BaaSサービスは、データセンターのフットプリントを減らすことで攻撃対象領域を縮小し、保護を強化します。

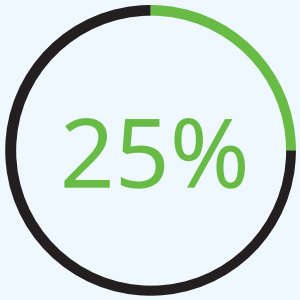
ベンダーへの質問: データ保護と運用の自由度を高める

- バックアップに関連するアップデートやアップグレードのために発生するダウンタイムを組織 (ビジネスおよびアプリケーションのオーナー) がどれくらい許容できるか?
- 次のソリューションでは、組織で利用可能なさまざまなデータソースをすべてバックアップすることについて、どのような期待をしているか?
- SaaS、クラウドネイティブ、オンプレミスのアプリおよびデータのバックアップ管理にスタッフがどれだけの時間を割けるか?
- データの保護と保持に対する規制要件やビジネス要件の変更に迅速に適応するために、どのようなプロセスを導入しているか?
- オンプレミスのインフラストラクチャとサイバーセキュリティのリスクプロファイルの低減のために、どのようなIT環境の変更を検討しているか?

2 セキュリティとランサムウェアへの備えを強化

企業のデータは攻撃され、サイバー犯罪者はますます富を得ています。Cybersecurity Venturesによれば、2031年までにビジネスへのランサムウェアの攻撃が2秒に1回となり、その被害額は年間2,650億ドルになると予想されています。このため、組織はITアジリティの向上に加え、セキュリティ体制を強化してランサムウェアからデータを適切に守る必要があります。

BaaSは企業が身代金の支払いを拒否する上で役に立ちますが、BaaSサービスがすべて同じランサムウェア対策機能を提供しているわけではありません。以下のような、重要なランサムウェア対策機能を備えたBaaSソリューションに投資する必要があります:



25%の組織が、悪意のある削除がSaaSデータ損失の最大の原因であると回答しています。

引用: Enterprise Strategy Group、「The Evolution of Data Protection Cloud Strategies」、2021年

イミュータブルスナップショット

ランサムウェアが暗号化、変更、削除することができないイミュータブルスナップショットで構築したクラウドバックアップなら、データをより強固に保護することができます。適切なBaaSは、構造化/非構造化データ (メールから音声や動画ファイル、画像まですべて) がバックアップされ、万が一ランサムウェア攻撃が発生した際には復旧できるよう準備が整っています。

異常検知とアラート

「2022年データ侵害のコスト」の調査によると、侵害を特定し、封じ込めるまでの平均日数は277日でした。このような長い期間があれば、サイバー犯罪者はデータの暗号化だけでなく、データを窃取してダークウェブで販売することもできてしまいます。そのため、ほぼリアルタイムの強力な自動異常検知は、BaaSサービスの重要な機能です。クラウドバックアップでは通常のシステム運用を継続して追跡し、ランサムウェア攻撃を示す不正行為やユーザーの異常行動を素早く見分けることができます。アラート機能と合わせれば潜在的な危険の通知と是正開始が実現し、どちらもランサムウェア攻撃の影響範囲を最小限に抑えることに繋がります。

厳格なアクセス制御

「2022年データ侵害のコスト」の調査によると、2022年の初期攻撃ベクトルで最も多かったのは、侵害された認証情報でした。そのため、組織にはユーザーのIDとアクセス権をより効果的に管理する責任が課せられています。優れたBaaSサービスは、細かい単位でのロールベースのアクセス制御 (RBAC) をサポートし、不正当事者がデータを脅かすことを防止します。また、多要素認証 (MFA、「持っている」ことと「知っている」ことの2段階認証) で認証し、フィッシングスキームやその他のパスワードハッキングを軽減できるサービスを探す必要があります。

データ隔離

クラウド時代より前の企業のデータ復旧手段として最も一般的だったのは、オフサイトの施設にあるテープに保存されたデータを物理的にオンサイトに戻すというものでした。しかし、このプロセスでは、もはや企業の求める復旧SLAを満たすことができません。

最新のBaaSは、バックアップデータをオフサイトのクラウドに移動して保護することで、本番環境からデータを隔離します。例えば最新のBaaSでは、データを別のテナントに移動することでAWSにあるサービスの隔離を実現することができます。そのため、ランサムウェア攻撃後に迅速に復旧する必要がある場合でも、本番環境を再感染させることなく復旧することが可能です。

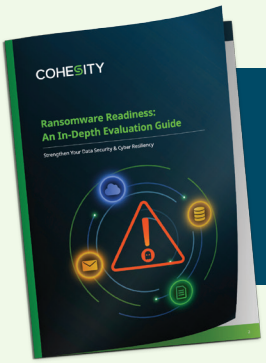
大規模な高速データ復旧

ランサムウェアが蔓延し、マルウェア開発の速度が遅くなる兆しも見られないことを考えると、組織はサイバー攻撃からの迅速な復旧に備える必要があります。これには、自信を持って大規模にデータを復旧するプロセスやテクノロジーが含まれます。

数百台の仮想マシン、大規模なデータベースや大量の非構造化データ、Microsoft 365の生産性データなど、あらゆる種類のデータを迅速に復旧でき、なおかつどの時点や場所へでも大規模かつ即座に復旧できるクラウドバックアップサービスが必要です。

ベンダーへの質問: セキュリティとランサムウェアへの備えを強化

- さまざまなすべてのアプリやワークロードをランサムウェアからどのように守るか?
- 現在、ビジネスデータへの不正アクセスをどのように防止しているか?
- 大規模なランサムウェアからデータを復旧するために、どのような計画があるか?



ランサムウェアへの備え: 徹底評価ガイド

意思決定プロセスに役立ちます。

3 消費とコストの柔軟性、そして持続可能性も実現

データ駆動型はビジネスにおけるニューノーマルです。そのため、企業は自社が収集、保護しているデータを使って新たなインサイトを発見し、製品やサービスの市場投入までの時間を短縮しようとますます努力しています。しかし、ビジネスに力を与えるデータは指数関数的な速度で増加しており、その維持にはより多くのコストがかかります。サービスプロバイダーモデルへの移行は、ビジネスの収益にとっても、ITや調達チームにとってもメリットがあります。BaaSのサブスクリプションは、複数のバックアップハードウェアやクラウドベンダーと契約するという調達における時間を短縮することができます。また、BaaSサブスクリプションでは更新もシンプルになります。予測可能な価格設定のため、予算の不透明性もなくすことができます。

財務管理と透明性を改善するBaaSを検討するのであれば、予測可能性と選択肢の両方を提供するプロバイダーを選ぶ必要があります。

容易な導入

BaaSを検討する企業にとって、柔軟性は最も重要な要素です。選択したBaaSサービスが管理しやすい契約期間 (1年など) を提供し、必要な容量に対してのみ支払いが行えることを確認してください。また、コストの予測可能性を最大化するため、請求が理解しやすい (透明性があり細かい単位で計測される) かどうかも考慮する必要があります。選択肢が1つしかないセルフマネージドサービスとは違い、最新のBaaSソリューションには、フロントエンド、バックエンド、ユーザーベースのライセンスなど、複数のライセンスオプションで柔軟性を最大化しています。BaaSサービスは、サインアップ、アカウントの設定、データソースの接続、ワークロードの自動検出といった導入が簡単であるべきです。これにより、ミッションクリティカルなデータやアプリケーションの保護を数分で開始できるはずです。

ライセンスのポータビリティ

組織のリーダーはITに投資することでビジネスの成果を達成します。テクノロジーによってそのデプロイの方法や場所を変更することを強いられるべきではありません。オンサイトとクラウド両方で実行しているワークロードとアプリに対応するバックアップが必要な場合、コンサンプションモデル間でライセンスを移動できるBaaSプロバイダーを探す必要があります。

セカンダリデータのコピーを、データ保護以外の目的 (開発/テスト、分析など) でパブリッククラウドインフラストラクチャサービスへ送っている

文献: Enterprise Strategy Group、「データバックアップからデータインテリジェンスへ」、2022年。

データ主権要件への対応

最近のESGの調査で、組織におけるコンプライアンスやデータ主権、データの場所に関する問題の懸念が高まっていることがわかりました。クラウドを全面的に導入するのであれば、BaaSサービスを利用することでデータ主権要件を満たすことができます。優れたBaaSソリューションは、データセンターのプライベートクラウド内や優れたパブリッククラウドで動作し、国や現地の規制に従って世界中で地域ごとにデータをセグメント化することができます。

透明性があり、成長に合わせて支払う隠れたコストのない価格設定

経済が不安定なときは、イノベーションのための資金確保が重要な場合があります。BaaSでは、組織はCAPEXからより予測可能なOPEXモデルへと移行することができます。同時に、適切なBaaSソリューションを選ぶと、プロビジョニングや、データのイングレス/エグレス料金など隠れたクラウドコストを排除することができます。バックアップデータを保護し、クラウドに集約するためのセキュアで効率的な方法を提供し、データを活用してインサイトを発見し、リスクを低減することができるサービスを探す必要があります。

持続可能性のメリット

ブランドは今、顧客や従業員をどれだけ大事にしているかということだけでなく、地球の保護にどれだけ取り組んでいるかということに対しても評価されるようになってきています。クラウドバックアップは、データセンターの物理的なハードウェアフットプリントを減らし、企業のESG (環境、社会、ガバナンス) 活動の主要目標であるエネルギー消費量を削減します。ESG目標に合致するBaaSサービスを探すことが大切です。

ベンダーへの質問: 持続可能性を備えた消費とコストの柔軟性の実現

- 過去数年間でバックアップへの投資はどのように変わったか?
- 経済が不安定な時期に、どのような方法でITを最適化し、イノベーションを推進してきた/しているか?
- 組織のESG目標にはどのようなものがあるか?

チェックリスト: BaaSサービス

BaaSを活用することで、クラウド主導のITモダナイゼーションへの次のステップを踏み出すことができます。BaaSは、すべてのデータソースに対する保護目標の前進させ、運用の自由度を高め、ランサムウェアに対して環境を強化し、コストを最適化する理想的な手段です。BaaSサービスを評価する際、こちらのチェックリストで主要な機能を確認することで、組織に最適なソリューションを見つけることができます。

機能		ベンダー1	ベンダー2	ベンダー3
データ保護と運用の自由度を高める	幅広いデータソースに対応	☐	☐	☐
	統合管理	☐	☐	☐
	シンプルな運用	☐	☐	☐
	高い信頼性とパフォーマンス: 無停止アップグレード	☐	☐	☐
	データセンターの設置面積をほぼゼロへ	☐	☐	☐
セキュリティとランサムウェアへの備えを強化	イミュータブルスナップショット	☐	☐	☐
	異常検知とアラート	☐	☐	☐
	厳格なアクセス制御	☐	☐	☐
	データ隔離	☐	☐	☐
	大規模な高速データ復旧	☐	☐	☐
消費とコストの柔軟性、そして持続可能性も実現	容易な導入	☐	☐	☐
	ライセンスのポータビリティ	☐	☐	☐
	データ主権要件への対応	☐	☐	☐
	透明性があり、成長に合わせて支払い可能な隠れたコストのない価格設定	☐	☐	☐
	持続可能性のメリット	☐	☐	☐

「CohesityのBaaSサービスにより、事前に多くの余分なストレージインフラを購入することなく、貴重なユーザーデータを保護することができました。そして、ハードウェアを調達する必要がなかったため、1時間かからずにサービスを起動し実行することができました」

Jake Parham氏
セントジョンズ郡保安官事務所、ITマネージャー

BaaSの活用

BaaSの採用により、ITモダナイゼーションをさらに速く、さらに前進させることができます。よりシンプルで効率的、かつセキュアなエンタープライズグレードの保護を企業が現在使用しているさまざまなデータソースに適用することで、アジリティを高めることができます。ビジネス要件とコンプライアンス要件を満たし、ITデータの管理に関わる時間や手間を削減し、ESG目標を達成する。適切なBaaSサービスなら、これらすべてが実現可能です。

CohesityのBaaSについての
詳細はこちら

COHESITY