教育におけるシングルクラウド、ハイブリッドクラウド、マルチクラウドのための戦略の構築

AWS 規範ガイダンス

AWS 規範ガイダンス: 教育におけるシングルクラウド、ハイブリッドクラウド、マルチクラウドのための戦略の構築

Table of Contents

教育におけるシングルクラウド、ハイブリッドクラウド、マルチクラウドのための戦略の構築

Amazon Web Services (寄稿者)

2023 年 9 月 (ドキュメント履歴)

教育機関は、クラウドコンピューティングが提供する俊敏性、コスト削減、セキュリティ、耐障害性を活用して、リモートラーニング、研究、学生体験、データインサイト、管理などの機能を支援しようとしています。多くの組織が、このデジタルトランスフォーメーションの一環として、ハイブリッドクラウドおよびマルチクラウドのデプロイを評価しています。

このホワイトペーパーでは、クラウドオプションを評価している教育機関の工グゼクティブリーダーや意思決定者向けに、シングルクラウド、ハイブリッドクラウド、マルチクラウドのテクノロジーとガバナンス戦略を作成するための規範的なガイダンスを提供します。このガイダンスは、 AWS が世界中のあらゆる規模の 14,000 を超える教育機関 (初等および中等教育から高等教育まで) と連携してきた経験に基づいています。

概要:

教育機関は、学生、保護者、教員、スタッフ、地域社会に差別化されたサービスや体験を提供するためにデジタルトランスフォーメーションを進める中で、多くの技術的な意思決定に直面しています。多くの組織は、俊敏性、伸縮性、耐障害性、セキュリティ、コスト削減を高めるために、クラウドの導入をすでに決定しています。さまざまなチーム間での既存の関係と投資に基づいて、ほとんどの組織はオンプレミスデータセンター、コロケーション施設、クラウドプロバイダーを組み合わせて使用しています。複数のクラウドオプションが利用可能であることを踏まえ、教育機関はシングルクラウド、ハイブリッドクラウド、マルチクラウドのデプロイモデル (「クラウドデプロイ戦略」セクションで定義) から頻繁に選択する必要があります。

2 つ以上のクラウドサービスプロバイダーのサービスを利用するマルチクラウドは、現在では多くの教育機関で一般的になっています。IT チームが特定のクラウドプロバイダーを好む一方で、他のグループや部門、あるいは個々のユーザーが別のプロバイダーを選択したり、既に利用していたりする場合もあります。適切なクラウドデプロイモデルへと導く明確な戦略を持たない教育機関は、多くの課題に直面します。これらの課題には、不要な複雑性、スタッフへの負担増加、一貫性のないガバナンス、そして複数のプロバイダーに共通する基本機能のみに限定される最小公分母的なアプローチが含まれます。これらの課題はイノベーションを妨げ、デジタルトランスフォーメーションの推進を遅らせます。

一方で、シングルクラウド、ハイブリッドクラウド、マルチクラウドの活用を導くクラウド戦略がある場合は、長期的な成功に向けて運用面で持続可能な形でクラウドの利点を活かしながら、教育ミッションの要件を満たすことができます。この戦略を作成するには、以下をお勧めします。

- プライマリの戦略的クラウドプロバイダーを選択します。
- Cloud Center of Excellence (CCoE) を設立します。
- Software as a Service (SaaS) アプリケーションと基盤クラウドサービスを区別します。
- 各クラウドサービスプロバイダーのセキュリティとガバナンスの要件を確立します。
- 可能な限り、かつ実用的であれば、クラウドネイティブのマネージドソリューションを採用します。
- 既存のオンプレミス投資が継続利用を促す場合は、ハイブリッドアーキテクチャを実装します。
- シングルクラウドのプロバイダーで技術要件またはビジネス要件を満たせないワークロードにのみ、マルチクラウドを適用します。

これらのベストプラクティスについては、このホワイトペーパーの「Recommendations」セクションで詳しく説明します。いずれの推奨事項も重要ですが、教育機関の優先順位はクラウド導入の段階によって異なります。例えば、クラウド導入を始めたばかりの場合は、プライマリの戦略的クラウドプロバイダーの選択、CCoE の設立、クラウドネイティブのマネージドソリューションの採用に注力します。既にシングルクラウドのプロバイダーを使用している場合は、セキュリティとガバナンスの基本要件の確立に注力し、既存のデータセンター投資が継続利用を促す場合は、ハイブリッドアーキテクチャを検討します。組織が既に複数のクラウドプロバイダーを利用している場合は、SaaS アプリケーションを差別化し、マルチクラウドのデプロイを、それを本当に必要とするごく限られたワークロードにのみ適用することに注力します。

目次

クラウドデプロイ戦略

AWS は、クラウドコンピューティングを「インターネットを通じて、従量制料金で IT リソースをオンデマンドで提供すること」と定義しています。物理的なデータセンターやサーバーを購入、所有、保守する代わりに、クラウドプロバイダーから必要に応じてコンピューティング能力、ストレージ、データベースなどのテクノロジーサービスにアクセスできます。クラウドコンピューティングを使用すると、教育機関は、ハードウェアの調達、メンテナンス、キャパシティプランニングなど、差別化されていない重労働を回避できます。クラウドソリューションを導入してデプロイする場合、シングルクラウド、ハイブリッドクラウド、マルチクラウドの複数のモデルから選択できます。

シングルクラウド

このモデルは、単一のクラウドサービスプロバイダーのみを使用します。シングルクラウドのアプリケーションとワークロードは、クラウド上で直接実装される場合もあれば、以前は別の環境でホストされていてクラウドに移行されたものの場合もあります。これらのワークロードでは、クラウドプロバイダーの低レベルなインフラストラクチャサービスを使用することもあれば、より高レベルなマネージドサービスを利用することもあります。いずれにしても、このモデルは単一のクラウドプロバイダーを採用し、そのプロバイダーが提供するクラウドサービスのみを使用します。

ハイブリッドクラウド

ハイブリッドクラウドモデルは、組織が保有するオンプレミスデータセンターと、1 つ以上のクラウドサービスプロバイダーの間でリソースを分散します。通常、このモデルの目的は、オンプレミスに存在する既存の内部システムとのプライベート接続を維持しながら、組織のインフラストラクチャをクラウドに拡張することです。

マルチクラウド

マルチクラウドモデルは、2 つ以上のクラウドサービスプロバイダー間でリソースを分散し、それぞれのサービスを利用します。組織が意図的にマルチクラウドを選択する場合もありますが、多くの場合、これは個々のチーム、部門、またはスタッフが異なるクラウドプロバイダーを好むことによって生じる、意図しない結果です。

推奨事項

シングルクラウド、ハイブリッドクラウド、マルチクラウドの基本を理解したところで、このセクションではモデルを選択するための詳細な推奨事項を示します。

- プライマリの戦略的クラウドプロバイダーを選択する
- CCoE を設立する
- SaaS アプリケーションと基盤クラウドサービスを区別する
- 各クラウドサービスプロバイダーのセキュリティとガバナンスの要件を確立する
- 可能な限り、かつ実用的であれば、クラウドネイティブのマネージドサービスを採用する
- 既存のオンプレミス投資が継続利用を促す場合は、ハイブリッドアーキテクチャを実装する
- シングルクラウドのプロバイダーで技術要件またはビジネス要件を満たせないワークロードにのみ、マルチクラウドを適用する

プライマリの戦略的クラウドプロバイダーを選択する

クラウドの導入は、IT のモダナイズ、コスト効率、イノベーションに不可欠な多くの利点をもたらします。ただし、限定的な SaaS アプリケーションを超えてクラウドテクノロジーを採用すると、教育機関が不要なコストや複雑さを避けるために慎重に計画しなければならない課題が生じる可能性があります。クラウドでのワークロードの実装に伴う技術的およびビジネス上の変更には、ネットワーク、セキュリティ、ガバナンス、運用など、コアインフラストラクチャに対するスタッフのスキル習得支援と調整が必要です。

これらの課題に効果的に対処するための最善のアプローチは、特に組織がクラウドジャーニーの初期段階にある場合、ワークロードの大部分をサポートするプライマリの戦略的クラウドプロバイダーを選択することです。クラウドの利点の実現を簡素化して加速できるように、そのプロバイダーに焦点を当てた導入から始めます。プライマリクラウドプロバイダーの選択は、排他的で不可逆的な決定ではありません。これにより、組織はクラウド導入を反復的に進化させることができます。まずは少数のサービスに焦点を当て、必要に応じて他のクラウドサービスに拡張できます。これにより、遅滞なくクラウドの全体的な利点を実現できます。このアプローチは、プロバイダーの機能を活用し、従業員のスキルとサードパーティーパートナーとの関係を集中的に強化し、ベンダー管理を簡素化するという組織の能力を最大化します。

複数のクラウドプロバイダーを同時に採用しようとしてクラウドジャーニーを開始したものの、その決定と、それによって生じた複雑さを後悔するお客様を見てきました。Gartner はこのインサイトを

記事「6 Steps for Planning a Cloud Strategy」で共有しており、ステップ 2 として、「マルチクラウドアーキテクチャではプライマリプロバイダーを優先する」と述べています。

各クラウドプロバイダーは、さまざまな運用およびサポートモデル、ID およびアクセス管理、ネットワーク、運用、コンプライアンス機能などを導入しています。クラウドプロバイダーの運用モデルは、一度に 1 つに絞って習得する方が効果的です。その後、合理的と判断される場合に、追加のクラウドサービスを反復的かつ段階的に組み込むことができます。プライマリクラウドプロバイダーを採用するかどうかの決定には多くの要因が影響しますが、選択の指針として以下の重要な質問を参考にしてください。

- プロバイダーが提供するサービスの幅と深さはどの程度ですか?

  クラウドプロバイダーごとに提供するサービスは異なります。少なくとも、プライマリプロバイダーに、すべての機能要件に加えて、セキュリティ、ガバナンス、自動化などの横断的かつ運用上のニーズをサポートできる機能があることを確認してください。これらの機能を、イノベーションと運用上の優秀性において実績のある形で提供しているプロバイダーを選択します。アプリケーションだけでなく、データも考慮してください。将来的なデータ統合や転送パターンを考慮し、プロバイダー間で大量のデータを移動する際のコスト、レイテンシー、複雑さを最小限に抑えます。現在のアプリケーションとデータのニーズを満たすだけでなく、時間と共に変化する機関のニーズに対応する新たなユースケースを可能にするような、可能な限り広範かつ多様なサービスを提供できるプロバイダーを選択します。
- プロバイダーは、すべてのセキュリティとコンプライアンスのニーズをサポートできますか?

  教育分野では、セキュリティとコンプライアンスは、あらゆるテクノロジーのデプロイにとって不可欠です。すべてのセキュリティとコンプライアンスのニーズを満たすことができるクラウドプロバイダーを選択します。AWS Artifact などのツールは、セキュリティおよびコンプライアンスレポートへのオンデマンドアクセスのための一元的なリソースを提供することで、プロバイダーを評価するのに役立ちます。クラウドプロバイダー独自のインフラストラクチャやサービスのセキュリティとコンプライアンスだけでなく、それらのサービスを使用して安全で準拠したソリューションを簡単に設計できるかどうかも検討します。構築済みソリューション、クイックスタート、規範的なガイダンスなどを組み合わせて提供し、安全なクラウド導入を加速できるプロバイダーを優先します。
- プロバイダーには堅牢なパートナーネットワークがありますか?

  クラウドトランスフォーメーションは、どの組織も単独では実施しません。導入を加速するには、クラウドプロバイダーとそのパートナーネットワークのサービスと専門知識を活用する必要があります。このネットワークには、クラウドテクノロジー上で動作するソフトウェアを提供したり、統合や支援を行ったりするテクノロジーパートナーに加え、クラウド上での独自アプリケーションの

設計、構築、運用、管理を支援するコンサルティングパートナーが含まれます。既に協力関係のある多くの教育関連のテクノロジープロバイダー、独立系ソフトウェアベンダー (ISV)、コンサルタント、リセラーが、クラウドプロバイダーのパートナーネットワークの一員であることがわかるでしょう。厳選されたコンピテンシーを備えたパートナーによる、最も堅牢なネットワークを持つクラウドプロバイダーを優先します。業界および技術に関する実証済みの専門知識を持つパートナーの存在は重要です。

- プロバイダーはどのようなサポートとスキル習得支援を提供していますか?

  新しいテクノロジーを正常に導入するには、ベストプラクティスの推奨事項、設定ガイダンス、問題解決など、トレーニングや支援を要請するための仕組みが必要です。強力なサポートとトレーニングオプションを提供するクラウドプロバイダーを選択することで、成功への準備が整います。プロバイダーの公式なサポートモデルおよびリソース、さらに、ブログ、フォーラム、動画、ハウツーガイドなど、利用可能なサードパーティーやコミュニティベースのリソースも確認します。プロバイダーのテクニカルサポートプログラムだけでなく、ビジネスと文化のトランスフォーメーションに焦点を当てたプログラムも考慮します。例えば、AWS クラウド導入フレームワーク (AWS CAF) は、テクノロジーだけでなく、ビジネスプロセスや人材を含む視点に焦点を当てることで、組織のデジタルトランスフォーメーションを支援します。広範なトレーニングオプションと、実証済みの信頼性の高いサポートモデルおよびコミュニティを提供するクラウドプロバイダーを優先します。

CCoE を設立する

トランスフォーメーションオフィスまたは Cloud Center of Excellence (CCoE) を通じてクラウドリーダーシップ機能を進化させることを検討してください。CCoE は、組織全体でクラウドテクノロジーを大規模に実装するためのアプローチを開発し、推進します。クラウド導入を成功させるには、関係するチームや部門を代表して意見を述べる担当者を含めるように CCoE を設計します。CCoE は、小規模に開始し、トランスフォーメーションジャーニーを進めながら、ニーズに合わせて段階的に進化させます。 AWS アカウントマネージャーやソリューションアーキテクトなどのプライマリクラウドプロバイダーの担当者は、CCoE の作成を支援するリソースを提供できます。CCoE は、対象分野の専門知識を確立し、組織全体の賛同と信頼を獲得し、ミッション要件を満たすための効果的なガイドラインを策定するための取り組みを加速します。すべての機関で機能する唯一の組織構造はありませんが、以下の質問は独自の CCoE を設計する際に役立ちます。

- CCoE には誰を含めるべきですか?

  初期段階の CCoE には、少数のアーリーアダプターとクラウドチャンピオンしか含まれていない可能性があります。CCoE は小規模のままでもかまいませんが、クラウド導入によって影響を受け

るビジネス機能と技術機能の両方を代表して発言できるチャンピオンを含めるよう進化させる必要があります。ビジネス機能には、変更管理、ステークホルダーの要件、ガバナンス、トレーニング、調達、コミュニケーションが含まれます。これらの機能は通常、機関の管理チームと教育チームのメンバーが担当します。技術機能には、インフラストラクチャ、自動化、運用ツール、セキュリティ、パフォーマンス、可用性が含まれます。これらの機能は通常、機関の IT チームのメンバーが担当します。また、CCoE は、必要に応じてベンダーやパートナーを関与させ、対象分野の専門知識を提供してもらえるようにする必要があります。CCoE は「生きている組織」です。そのメンバーシップ、形態、機能は時間の経過と共に変化し、将来的には、成熟度が高まったタイミングで解散する可能性もあります。

- CCoE はステークホルダーとどのように関係を築くべきですか?

  CCoE は他のチームを支援する立場にあり、クラウド導入の成功に向けた情報提供と、その実現のみを目的としています。CCoE の一部をさまざまな部門、学校、機能に埋め込むことを検討します。これにより、幅広いリソースへのアクセスが可能になり、内部フィードバックが高速化されます。機関内の信頼を確立し、組織内のサイロを解消するために、ステークホルダー間でのパートナーシップとオープンなコミュニケーションを早期に構築することに重点を置きます。CCoE には、ステークホルダーとのコミュニケーション、フィードバックの収集、ユーザーのトレーニングを行うための明確なメカニズムが必要です。CCoE の成功メトリクスには、このようなコラボレーションとコミュニケーションが反映されている必要があります。チームがテクノロジーの構築のみを指標として評価されると、テクノロジーはさらに構築されますが、その活用や成果は軽視されることになります。代わりに、メトリクスでは、CCoE の取り組みによって自立できるようになったチームの数、イニシアチブにおいて CCoE がクリティカルパス上に置かれた回数、開催されたトレーニングイベントの数、CCoE の成果物の採用範囲などを測定する必要があります。適切に構築された信頼できる CCoE は、信頼を基盤としたより大きな組織トランスフォーメーションへの足がかりとなる可能性があります。

- CCoE をどのように設立するべきですか?

  ほとんどの組織は、特定の目的に特化したパイロットプロジェクトからクラウド導入を開始します。これらのプロジェクトの一環として、CCoE を設立します。ジャーニー全体の成功を定義するには、最初の一歩がきわめて重要です。

  - ビジネス上の問題から始めます。テクノロジーのためのテクノロジーは、適切な戦略ではありません。クラウドテクノロジーを試している場合は、どんなに小さく見えても説得力のあるビジネスユースケースを特定します。次に、そのユースケースを起点として、テクノロジーがどのように役立つかを明確に定義した目標を設定します。ソリューションをサイロに実装しないでください。プロジェクトの実装前および実装中には、常にビジネス部門のステークホルダーからフィードバックを受け取ります。成功しているクラウドプロジェクトはすべて、そのテクノロジーを利用する組織との緊密な連携に支えられています。

- 小規模に始めます。やり直しが可能な、低リスクで双方向ドア型のプロジェクトを選びます。つまり、可逆性があり、ミスがあってもすぐに修正できるプロジェクトということです。パイロットプロジェクトは実験が目的です。大規模かつ高リスクなプロジェクトを避けることで、実装と結果をより適切に制御できます。これにより、広範な目標ではなく、特定の定義可能な問題に的を絞ることができます。例えば、自動化が最終目標である場合は、ジョブ全体ではなく特定のタスクの自動化を目指します。
- 結果を定義して測定します。各プロジェクトの進捗状況とパフォーマンスを評価するために、明確なメトリクスを設定します。ステークホルダー間の期待のズレを避けるため、望ましい最終状態をあらかじめ十分に定義しておきます。ビジネスステークホルダーや組織内の他のリーダーと緊密に連携し、期待と測定可能な利益を定義します。また、結果を非技術的な言葉で表現することも重要です。例えば、プロジェクトによって保持率が向上した、解約率が下がった、コストが削減された、納品速度が向上したなど、組織の目標に即した観点で結果を説明します。
- 慣れた領域から始めます。機関がよく知っているドメイン内のプロジェクトを選択します。これにより、意味があり、理解しやすく、実際に効果のある目標をプロジェクトに設定できます。このようなプロジェクトは、信頼を構築し、組織にとってより長期的な成果をもたらします。例えば、データ分析に関する専門知識が既にある場合は、分析プロジェクトから始めて、既存のスキルセットを活用しながらクラウドジャーニーを開始できます。各機関にはさまざまな専門知識があるため、成功するデジタルトランスフォーメーション戦略を立てるには、それぞれの独自のコンポーネントを見つける必要があります。

SaaS アプリケーションと基盤クラウドサービスを区別する

ほとんどの教育機関は、Software as a Service (SaaS) アプリケーションを既に採用しています。SaaS は、サービスプロバイダーが実行および管理する完全なソリューションを機関に提供します。一般的な SaaS アプリケーションには、ワードプロセッシングや E メールなどの生産性向上アプリケーションがありますが、エンタープライズリソースプランニング (ERP)、学生情報システム (SIS)、学習管理システム (LMS) などのミッションクリティカルなワークロードにも SaaS オプションがあります。機関が SaaS サービスを導入すると、IT チームはサービスの維持方法やインフラストラクチャの管理方法について考える必要がなくなり、ユーザーは単にサービスを利用するだけで済みます。この提供モデルにより、IT スタッフの管理負担が軽減されます。多くの機関では、特に、同じアプリケーションをセルフホストするだけの時間、リソース、スキルセットが IT チームにない場合、IT 戦略に「SaaS ファースト」アプローチを採用しています。セルフホストするだけのリソースがあったとしても、SaaS ソリューションを採用し、他のプロジェクトに投資する方が、費用対効果が高い場合もあります。

SaaS アプリケーションを使用する場合、IT チームは基盤となるインフラストラクチャを管理する必要がないため、ベンダーがアプリケーションをホストする場所 (オンプレミスデータセンター、プライマリクラウドプロバイダー、または代替クラウドプロバイダー) はそれほど重要ではありません。プライマリの戦略的クラウドプロバイダーを選択した後でも、別のクラウドプロバイダーや、ベンダーのデータセンターのオンプレミスでホストされている SaaS サービスを利用するという選択肢もあります。逆に、SaaS アプリケーションが 1 つのクラウドプロバイダーでホストされている場合でも、非 SaaS ワークロードに対する強みを考慮して、別のクラウドプロバイダーをプライマリの戦略的プロバイダーとして選ぶこともできます。ホスティング環境の区別は、SaaS アプリケーションよりもセルフホスト型アプリケーションにおいてより重要です。ただし、SaaS が IT 戦略の一環としてクラウドとどのように適合するかを評価する際には、引き続き以下の重要な質問を考慮する必要があります。

- SaaS アプリケーションの可用性とスケーラビリティは高いですか?

  多くのベンダーは、自社の SaaS サービスにクラウドを採用することを既に決定しています。これにより、ベンダーは可用性とスケーラビリティの向上というクラウド上の利点を実現できます。さらに、ベンダーは、物理インフラストラクチャを管理および維持する代わりに、クラウドの責任共有モデルを採用できるため、新機能の提供により多くの時間とリソースを費やすことができます。このような利点があるため、クラウドファーストでクラウドホスト型のソリューションを提供するプロバイダーを優先する必要があります。

- SaaS アプリケーションはセキュリティ要件を満たすことができますか?

  SaaS を評価するときは、アプリケーションが保存するデータ、そのデータの使用方法、そのデータを保護するために実装されているセキュリティコントロールについて知っておくことが重要です。独自のセルフホスト環境のようにデータストレージを直接制御できない場合でも、ベンダーがデータを適切に処理するためのメカニズムとコントロールを備えていることを確認する必要があります。SaaS ソリューションに組み込まれているセキュリティ機能と、追加設定が必要な機能を把握しておいてください。クラウドにより、SaaS プロバイダーはより可用性が高くスケーラブルなソリューションを構築できます。また、責任共有モデルにより、より安全なソリューションを構築することもできます。クラウドセキュリティツールとサービスをソリューションの一部として活用しているプロバイダーを優先する必要があります。

- SaaS アプリケーションデータは誰が所有しており、どのようにアクセスできますか?

  SaaS を利用する場合、機関のデータを適切に処理することをプロバイダーに委ねることになります。SaaS アプリケーションのサービス条件とサービスレベル契約を確認して、データの所有権、可用性、耐久性などの寄与要因を理解してください。データをバックアップまたはエクスポートす

るメカニズムを評価します。これは、プロバイダーを変更する場合や、プロバイダーがサービスを停止する場合に特に重要です。

- 環境に関係なく、他のサービスやセルフホストアプリケーションは SaaS アプリケーションと統合できますか?

  SaaS ソリューションを採用する際には、同じホスティング環境を共有するサービスとアプリケーション (つまり、同じクラウドプロバイダーまたは同じベンダーのデータセンターを使用するアプリケーション) は、よりシームレスに統合できると考えがちです。しかし、現在のほとんどの SaaS ソリューションは API とサードパーティーの統合を幅広くサポートしているため、同じ環境にホストされているソリューションに限定する必要はありません。必要な統合が存在する場合、ソリューション同士が同じ基盤環境を共有している必要はありません。例えば、クラウドベースの学生ファイルストレージとして、Google Drive や Microsoft OneDrive などの SaaS ソリューションを使用しているとします。仮想デスクトップとアプリケーションのストリーミングを学生に提供するために、Amazon WorkSpaces アプリケーションが要件に最適であると判断する場合があります。これらのサービスは異なる環境で実行されますが、WorkSpaces アプリケーションには Google Drive および Microsoft OneDrive とのネイティブ統合があるため、学生は既存のストレージを引き続き使用できます。

- SaaS アプリケーションは一元化された ID 管理をサポートしていますか?

  IT チームが異なる ID ストアを管理したり、ユーザーが複数の認証情報セットを覚えたりする必要がないように、SaaS ソリューションが既存の ID 管理またはシングルサインオンソリューションとの統合をサポートしていることを確認してください。分散した ID 管理は生産性を低下させ、特権の過剰付与や脆弱なパスワードなど、不適切なセキュリティプラクティスにつながる可能性があります。希望する SaaS ソリューションがシングルサインオンまたは既存の ID ストアをサポートしていない場合は、そのソリューションを採用するビジネス価値が、ユーザーやスタッフへの負担の増加を上回るかどうかを評価してください。

- SaaS アプリケーションとのネットワーク通信を保護するにはどうすればよいですか?

  場合によっては、SaaS アプリケーションと通信するためにセルフホスト型アプリケーションが必要になることがあります。通常、この通信は、適切な認証および認可メカニズムで保護された API を介して行われます。ただし、2 つのアプリケーションのホスティング環境によっては、その通信を簡素化または保護するために、代替または追加のメカニズムが必要になる場合があります。例えば、アプリケーションをクラウドプロバイダーでセルフホストし、同じクラウドプロバイダーでホストされている SaaS アプリケーションと統合する必要がある場合、ベンダーはいくつかの接続オプションを提供することがあります。クラウド固有のピアリング接続、プライベート API、AWS PrivateLink などのプライベートインターフェイスを使用して、その通信がパブリックインターネットを通過しないようにできます。同様に、オンプレミスアプリケーションが AWS

Direct Connect などのサービスを介してクラウドプロバイダーへの専用ネットワーク接続を持っている場合は、その同じ接続を使用して、同じクラウドプロバイダーでホストされている SaaS アプリケーションと通信できます。

各クラウドサービスプロバイダーのセキュリティとガバナンスの要件を確立する

教育機関には、コンプライアンス、ガバナンス、サイバーセキュリティに関する達成すべきさまざまな目標があります。これらの目標を達成できなかった場合のリスクには、機関の評判の低下、罰金、身代金、機密データの侵害、知的財産の盗難、ミッションクリティカルな機能の低下または完全な喪失などがあります。責任共有モデルにより、クラウドサービスを導入する機関は、インフラストラクチャのセキュリティに関する一部の責任をクラウドサービスプロバイダーに移管することで、管理上の負担を軽減できます。さらに、オンプレミスデプロイでは利用できない、管理が難しい、またはコストがかかることの多い機能を提供する、専用のクラウドネイティブセキュリティサービスの恩恵を受けることができます。例としては、ウェブアプリケーション保護用の AWS WAF、分散型サービス拒否 (DDoS) 対策用の AWS Shield、脅威検出用の Amazon GuardDuty などのサービスがあります。クラウドセキュリティとガバナンスの戦略が成功すれば、IT チームやセキュリティチームは設計による安全なシステム構築に集中でき、機関は進化するミッション要件に迅速に適応でき、教員や研究者には革新的な学習やイノベーションのための安全な環境が提供されます。セキュリティとガバナンスの要件を評価するには、以下の重要な質問を検討してください。

- ワークロードはどのコンプライアンスフレームワークに準拠する必要がありますか?

  教育機関は、サポートするステークホルダーやワークロードが多数存在するため、多くのコンプライアンスフレームワークに準拠する必要があります。これらのコンプライアンスフレームワークには、家族教育の権利とプライバシー法 (FERPA)、医療保険の相互運用性と説明責任に関する法律 (HIPAA)、連邦リスク認可管理プログラム (FedRAMP)、サイバーセキュリティ成熟モデル認定 (CMMC)、国際武器取引規則 (ITAR)、犯罪司法情報サービス (CJIS)、および Payment Card Industry Data Security Standard (PCI DSS) が含まれます。CMMC のように、関連するワークロードが準拠していると認定されるまで、研究助成金が交付されない場合もあります。各フレームワークは一意であり、ワークロードのサブセットにのみ適用される可能性があります。どのワークロードがどの要件に準拠する必要があるかを理解し、各ワークロードの環境でそれらの要件を満たすことができることを確認してください。クラウド環境では、自身の責任範囲とクラウドプロバイダーの責任範囲の違いを理解しておくようにしてください。コンプライアンスを達成して維持するには、必要な知識、リソース、スキルセットを備えておく必要があります。

- 複数のクラウドプロバイダー間でコンプライアンスを徹底しながら、イノベーションを妨げないようにするために、どのようなメカニズムを導入していますか?

  教育機関がクラウドを初めて導入する場合は、プライマリの戦略的クラウドサービスプロバイダーを 1 社選択し、設計上安全なクラウド環境を設計、エンジニアリング、運用する方法を理解することに集中することをお勧めします。理想的には、セルフサービスシステムに自動的に埋め込まれたセキュリティコントロールにより、ユーザーは IT チームによる介入を最小限に抑えつつ、安全なクラウド環境を迅速にデプロイできるようになります。単一のプロバイダーに絞ることで、セキュリティとコンプライアンスの確保に必要なリソースと時間の投資を抑えることができます。多くの成功している機関では、コンプライアンス要件の大半を満たし、堅牢なパートナーネットワークを持ち、構築済みのコンプライアンスソリューションを提供し、安全なセルフサービス自動化を可能にするクラウドサービスプロバイダーを選択しています。複数のクラウドプロバイダーでセキュリティとコンプライアンスを確保する必要がある場合は、各環境のコンプライアンスを管理するためのスキルセットとリソースを構築するために、追加の投資が必要になります。各クラウドプロバイダーが異なる基盤環境、すなわちランディングゾーンを使用している場合、各ランディングゾーンがサポートできるコンプライアンス標準と要件を理解する必要があります。これにより、特定のワークロードをそのプロバイダーでホストできるかどうかが決まる可能性があります。プロバイダーごとにコンプライアンスを個別に管理したり、複数のプロバイダー間で管理を一元化できるカスタム構築されたソリューションやパートナーソリューションを使用したりできます。AWS Marketplace では、コンプライアンス要件を満たすターンキーソリューションも提供しています。

- 複数のクラウドプロバイダーのコストと使用状況を評価して制御するにはどうすればよいですか?

  教育機関がクラウドを初めて導入する場合は、どのクラウドサービスが使用されているか、リソースの所有者が誰か、それらのクラウドリソースの目的は何か、消費を最適化することでどのようなコスト削減が可能か、といった情報を把握するために、コストの可視化と制御のメカニズムを確立することをお勧めします。機関は、クラウドサービスプロバイダーと提携して、ミッションクリティカルなシステムの移行とモダナイズを実施することで、エンタープライズレベル契約の交渉、ボリュームディスカウントの適用、プロバイダーの専門知識の活用が可能となり、大きな投資収益率を実現できます。複数のプロバイダーでコストと使用状況を管理する必要がある場合は、社内のプロセスやツール、またはパートナーソリューションを活用して、各プロバイダーのコストと使用状況を集計して分析する方法を検討してください。多くの組織では、クラウド財務運用 (FinOps) を重要な機能と位置づけ、クラウドコストの管理と最適化のための機能の普及と導入にリソースを投入し始めています。

- 時間の経過と共にユーザーアクセス許可を簡単に管理するためのメカニズムはありますか?

  学術機関がクラウドを導入する際には、主要なステークホルダーのニーズを把握することをお勧めします。機関システムのユーザーには、学生、教員、研究者、IT スタッフ、管理、セキュリ

ティ、一般市民、サードパーティーの共同研究者が含まれます。これらのユーザーの主要なニーズを特定し、クラウドサービスへのアクセスを許可するための適切なメカニズムが整っていることを確認する必要があります。ユーザーの種類によって、必要とされるクラウドサービスへのアクセスの種類も異なります。例えば、学生、教員、一般市民はアプリケーションにアクセスする必要があります。IT スタッフ、管理者、セキュリティはクラウドインフラストラクチャにアクセスする必要があります。研究者やそのサードパーティーの共同研究者は安全な研究環境にアクセスする必要があります。教員は安全な教育環境にアクセスする必要があり、クラウドテクノロジーへの実践的なアクセスを学生に提供したい場合もあります。自動的にこれらの ID を一元管理するためのツールを用意し、ロールや責任の変化に応じてアクセス許可を特定、付与、取り消すために、確立されたプロセスを使用する必要があります。

- 新しいシステムを ID 管理ソリューションと適切に統合するメカニズムはありますか?

  学術機関では、新しいシステムを ID 管理システムと簡単に統合できるようにすることをお勧めします。これにより、ステークホルダーが ID 管理システムと簡単に統合できるシステムを調達して構築できるようになり、さまざまなミッションクリティカルな機能を柔軟にサポートできます。統合プロセスを簡素化することで、ステークホルダーがシングルサインオン、パスキー、多要素認証 (MFA) といったセキュリティのベストプラクティスを実装していない独自のアクセスコントロール手段を使用する可能性が低くなります。ID 管理システムが、ネイティブ統合または業界標準プロトコルを通じて必要なシステムと相互運用できることを確認します。

- インシデントの効果的な検出と対応を可能にするメカニズムはありますか?

  教育機関は、サイバー攻撃やランサムウェアのターゲットになることがよくあります。このようなインシデントを効果的に検出して対応できるように、2 つの視点から成るアプローチをお勧めします。

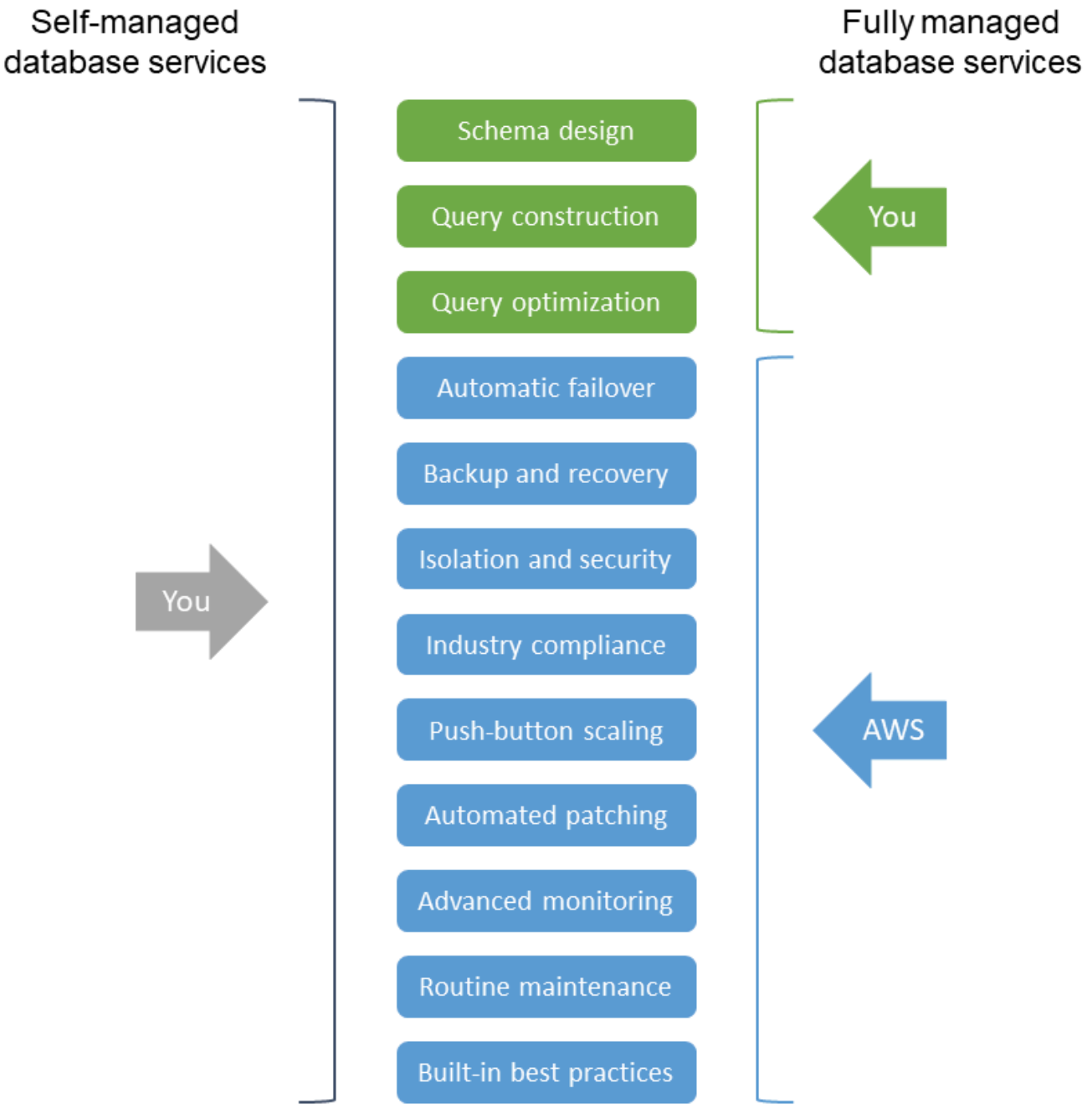
  - クラウド環境に自動的に埋め込まれるセキュリティコントロールという形で、予防策に重点を置きます。
  - サイバーインシデント対応者がセキュリティ違反をタイムリーに検出、封じ込め、軽減するのに役立つ検出機能を実装します。

コンプライアンスと同様に、各環境のイベントを検出、防止、対応するためのリソース、スキルセット、ツールを確保しておく必要があります。単一のプライマリクラウドプロバイダーに集中することで、必要なリソースを抑えることができます。成熟したセキュリティ運用チームを持たない教育機関は、これらの分野において、独立系ソフトウェアベンダー、マネージド型検出および対応プロバイダー、サイバーセキュリティコンサルタントから支援を受ける必要があります。

可能な限り、かつ実用的であれば、クラウドネイティブのマネージドサービスを採用する

クラウドサービスを活用する方法を初めて検討するときは、チームが使い慣れているインフラストラクチャサービスや開発ツールを使用することが最善の方法のように思えるかもしれません。しかし、クラウドネイティブのマネージドサービス、特にサーバーレスオプションを選択することで、コスト、労力、複雑さを大幅に削減できます。

クラウドネイティブのマネージドサービスを利用することで、スタッフの時間と労力を要する、差別化されていない IT タスクの多くが排除されます。これらの時間と労力は、ミッションに重点を置いたアクティビティに費やす方が有効です。さらに、プロバイダーがサービスの機能を改善するにつれて、ソリューションは効率、セキュリティ、レジリエンス、パフォーマンスなどの特性における段階的な改善を自然に継承します。例えば、フルマネージドデータベースサービスは高機能なリレーショナルデータベース管理システムですが、データベースが実行される基盤となるサーバーやオペレーティングシステムをプロビジョニングおよび管理する必要はありません。これにより、自前のデータセンターや、クラウドでプロビジョニングするセルフマネージドの仮想サーバーでリレーショナルデータベースを維持する際に、通常必要となる管理タスクがなくなります。次の図は、この違いを示したものです。



インフラストラクチャ管理を排除することの利点は、クラウドネイティブのマネージドサービスを、同等のセルフマネージドのアプローチと比較すると明らかです。そのため、購入またはカスタム開発したアプリケーションが実行されるコンポーネントをデプロイする必要がある場合は、時間と労力を削減するために、クラウドネイティブのマネージドサービスを使用する必要があります。

チームがクラウドでソリューションの構築、デプロイ、管理を担当する場合は、クラウドプロバイダーの差別化された機能とイノベーションを最大限に活用するために、クラウドネイティブのマネージドサービスを使用します。この戦略により、クラウドサービスを選択、統合、デプロイする際に、これらのプロジェクトに必要な時間と労力を削減しながら、レジリエンスとセキュリティを向上させることができます。クラウド戦略を成功させるには、カスタムソリューションをクラウドに移行したり、クラウドで新しいソリューションを開発したり、ライセンスソフトウェアをクラウドにデプロイしたりするときに、これらのクラウドネイティブの構成要素を採用することを検討してください。クラウドネイティブのマネージドサービスのオプションを評価するときは、以下の重要な質問を考慮してください。

- 教育ミッションの中核となる機能に、スタッフの時間と労力をより集中させる必要がありますか?

  仮想サーバーであっても、サーバーを管理するには、システムソフトウェアのアップグレードやパッチを適用して最新の状態を維持するための時間と注意が必要です。これらのタスクを処理するマネージドサービスを使用することで、IT スタッフの時間を、組織のミッションにより密接に関係するアクティビティに振り向けることができます。例えば、コンテナをデプロイする必要がある場合は、サーバーの設定や維持が不要な AWS Fargate のようなサーバーレスのマネージドサービスを検討してください。基盤となるインフラストラクチャを調達、プロビジョニング、管理する必要がなくなるため、新機能の提供、パフォーマンスの最適化、ユーザーエクスペリエンスの向上に集中できます。マネージドサービスをセルフマネージドオプションと比較して評価するときは、この利点を考慮してください。
- チームがクラウドネイティブのマネージドサービスを採用するには、どのような労力がかかりますか?

  クラウドネイティブのマネージドサービスを使用してソリューションを設計および実装するには、学習曲線が伴う場合がありますが、こうした労力は、ソリューションのライフタイムを通じてコスト、時間、複雑さを削減することで回収されます。クラウドコンピューティングはオンデマンドで従量制料金のため、クラウドネイティブサービスを使用すると、先行投資を抑えつつ、よりアジャイルな方法で迅速に反復や実験ができます。これにより、イノベーションが促進され、プロジェクトのタイムラインが短縮されます。ただし、これらの利点を効果的に実現するには、最適な使用パターンに関するスタッフトレーニングや、サービス固有の API に対応するコードのリファクタリングなど、サービスを採用して使用するために必要となる可能性がある事項を考慮してください。サービスが業界標準またはオープンソースの API を使用している場合でも、機能差やバージョンの不一致に対応するため、アプリケーションをリファクタリングまたは設定する必要がある場合があります。
- 現在、インフラストラクチャをどのようにデプロイおよび管理していますか? そのレベルのコントロールを維持する必要がありますか?

クラウドでインフラストラクチャをホストおよび管理するには、ベアメタルホスト、仮想マシン、マネージドコンテナサービス、サーバーレスサービスなど、さまざまな方法があります。現在、オンプレミス環境で仮想マシンやコンテナなどの同様のインフラストラクチャを使用している場合でも、特定のワークロードに別のアプローチが適しているかどうかを検討してください。例えば、すべてのアプリケーションを仮想マシンで実行する代わりに、アプリケーションのコンテナ化を検討し、Amazon Elastic Container Service (Amazon ECS) などのマネージドコンテナサービスを活用してください。これにはリファクタリングが必要になる場合がありますが、AWS App2Container などのツールを使用してコンテナ化を簡素化および支援できます。さらに一歩進めて、すべてのコンポーネントにサーバーまたはコンテナをデプロイするのではなく、完全なサーバーレスオプションを検討してください。サーバーレステクノロジーは、自動スケーリング、組み込みの高可用性、従量課金制の請求モデルを備えており、俊敏性の向上とコスト最適化を実現します。同時に、サーバーの管理やキャパシティ計画が不要になります。AWS Lambda などのサーバーレスコンピューティングサービスは、サーバーレスアーキテクチャの中核を成します。Lambda は一般的なプログラミング言語をサポートしており、開発者はインフラストラクチャを管理する代わりにアプリケーションコードに集中できます。ワークロードごとにこれらのオプションを検討し、学習曲線、管理オーバーヘッド、コスト、ライセンスなどの要因を考慮してください。

- ライセンスされたソフトウェアのインフラストラクチャをデプロイおよび管理する必要がありますか?

  独立系ソフトウェアベンダー (ISV) からライセンスされたソフトウェアをデプロイおよび管理する場合、クラウドインフラストラクチャを使用してオンプレミスのデプロイを模倣することが論理的に思える場合があります。例えば、オンプレミスの仮想マシンをクラウドホスト型の仮想マシンに置き換えることを検討する場合があります。これは実行可能なオプションですが、アーキテクチャのコンポーネントのいずれかをクラウドネイティブのマネージドサービスに置き換えることができるかどうかを検討してください。例えば、セルフマネージド型データベースサーバーを、同じデータベースエンジンを実行しながら管理上の負担を軽減するフルマネージド型データベースサービスに置き換えられる場合があります。多くの ISV は、マネージドサービスを利用するクラウドアーキテクチャを既に使用しており、デプロイを簡素化するために構築済みのテンプレートを提供する場合もあります。可能な場合は、クラウドデプロイの規範的なガイダンスとサポートを提供する ISV をお勧めします。ライセンスされたソフトウェアをクラウドにデプロイする前に、クラウド環境のライセンスとオンプレミスのライセンスとの違いを理解するために、必ず ISV に相談してください。

- マネージドサービスを使用すると、ベンダーロックインが発生する可能性があることを懸念していますか?

多くのクラウドネイティブのマネージドサービスは、一般的な業界標準と API をサポートするように構築されています。例えば、AWS Glue や Amazon EMR などの分析サービスは、Apache Spark や Apache Parquet などの業界標準の処理およびストレージフレームワーク上に構築されています。AWS Lambda は、Java、Go、Microsoft PowerShell、Node.js、C#、Python、Ruby のコードをネイティブにサポートしています。Amazon Relational Database Service (Amazon RDS) は、SQL Server、Oracle、PostgreSQL、MySQL など、一般的なデータベースエンジンの複数のバージョンをサポートしています。サービスに独自の API がある場合、クラウドに依存しない一般的なプロトコルを使用して、ネイティブソリューションまたはパートナーソリューションが API とやり取りできる場合があります。例えば、Amazon Simple Storage Service (Amazon S3) には直接統合するためのサービス固有の API がありますが、AWS Storage Gateway を使用する場合、ネットワークファイルシステム (NFS)、サーバーメッセージブロック (SMB)、Internet Small Computer System Interface (iSCSI) などの標準ストレージプロトコルを使用して操作することもできます。運用上のオーバーヘッドを最大限削減しながら、ニーズに最適なクラウドネイティブのマネージドサービスを選択することにそれでも集中する必要がありますが、一般的な業界標準やプロトコルを使用する、または利用できるサービスが望ましい場合もあります。

既存のオンプレミス投資が継続利用を促す場合は、ハイブリッドアーキテクチャを実装する

ほとんどの教育機関は、エンタープライズアプリケーション、データストレージソリューション、エンドユーザーコンピューティング (EUC) 環境、共有コンピューティングリソースをホストするために、さまざまな規模のオンプレミスデータセンターに投資しています。これらのデータセンターのすべてのリソースは、さまざまな更新サイクルの対象となります。この更新サイクルでは、将来の成長を考慮し、ピークスケールに対応するために十分な容量をプロビジョニングする必要があります。これは、年に数回のみ必要になる場合があります。その結果、リソースは多くの場合、次の更新サイクルまでアイドル状態になります。新しいハードウェアの計画、予算編成、調達、デプロイには、数週間、場合によっては数か月以上かかる場合があります。この長いプロセスはイノベーションを妨げ、学習と研究を遅らせる可能性があります。

クラウドコンピューティングは、これらの課題の多くを解決します。クラウドはオンデマンドで従量制料金の IT リソースを提供するため、大規模な事前計画や投資を行わずに、現在の容量と実際の需要をより密接に一致させることができます。ただし、オンプレミスのハードウェアとリソースに既に多額の投資をしている場合は、それらのリソースを効率的に活用し、必要に応じてクラウド技術を用いてハイブリッドモデルで強化することを検討する必要があります。

成功するハイブリッドクラウド戦略は、既存の投資を活用しながら、それらの投資単独では得られない俊敏性、スケーラビリティ、信頼性を実現します。次の考慮事項が、開始の際に役立ちます。

- 新しいワークロードをホストする必要がある場合、まずクラウドについて考えますか?

  パブリッククラウドインフラストラクチャとプライベートクラウドインフラストラクチャをどのように組み合わせて使用するかによって、ハイブリッドクラウド戦略が定義されます。クラウドファーストアプローチは、クラウドがすべてのワークロードに適した選択肢であることを意味するわけではありません。ただし、新しいワークロードを計画する場合、特に、新しいテクノロジーを必要とするワークロードや、オンプレミスで利用可能なストレージとコンピューティング容量を超えるワークロードの場合は、クラウドを最初のオプションとして評価してください。一時的で一貫性のない使用パターンを持つワークロード、迅速な結果を必要とするワークロード、簡単に移植できるワークロード、最新のハードウェアを必要とするワークロードは、クラウドのスケーラビリティと伸縮性を活かすのに最適な候補です。また、利用可能な容量がある場合でも、オンプレミスで利用できないクラウドネイティブのマネージドサービスからワークロードが恩恵を受けるかどうかを検討してください。

- オンプレミス環境の TCO を理解し、新しい投資を行う際に CFO と提携していますか?

  独自のオンプレミスデータセンターを維持する真の総保有コスト (TCO) を理解しておくことをお勧めします。オンプレミスでのインフラストラクチャの所有と運用には、ハードウェア、ソフトウェア、サポートだけでなく、施設、ユーティリティ、保険、スタッフの稼働時間など、多くの隠れたコストが伴います。これらのコストは、スタッフの生産性、運用レジリエンス、ビジネスの俊敏性に悪影響を及ぼす可能性があります。現在のライセンス構造とその更新およびメンテナンス期間も評価します。最高財務責任者 (CFO) と連携することで、新しい投資を計画する際に、隠れているすべてのコストを特定できます。ライセンスによっては、クラウドでの Bring Your Own License (BYOL) オプションが提供されている場合があり、または、クラウドサービスとの適合性に違いがある場合があります。現在のインフラストラクチャの真の TCO を理解することで、組織全体の TCO に最も大きな影響を与えるワークロードのクラウド導入を優先できます。 AWS アカウントチームには、オンプレミス TCO をよりよく理解するためのツールがすぐに用意されています。

- ハイブリッドデプロイをサポートするには、どのようなインフラストラクチャが必要ですか?

  ハイブリッドモデルを正常に採用するには、基盤となるネットワーク、セキュリティ、インフラストラクチャツールが必要です。クラウドプロバイダーとの適切なネットワーク接続を維持できることを確認します。これは、既存のインターネット接続、仮想プライベートネットワーク (VPNs)、などの専用接続 Direct Connect、サードパーティーの接続プロバイダー、Internet2、リージョンの研究および教育ネットワークの組み合わせによる場合があります。オンプレミス環境とクラウド環

境全体で ID とアクセスの管理が統一されていることを確認します。一貫したセキュリティ、コスト、使用ガードレールを適用するためのツールとプロセスを確立します。

- IT スタッフがハイブリッドデプロイを運用する準備はできていますか?

  クラウドサービスには、チームが持っていない特定のスキルセットが必要になる場合があります。効果的なクラウド導入のために IT スタッフのスキルアップに必要なトレーニングとスキル習得支援を制限するには、クラウドプロバイダーがオンプレミスとクラウドの両方にわたる既存のスキルセットを再利用し、それを基盤として構築されたサービスを提供しているかどうかを検討してください。例えば、Kubernetes を使用していて、それに精通している場合は、Amazon Elastic Kubernetes Service (Amazon EKS) または Amazon EKS Anywhere の使用を検討してください。NetApp を使用していて、それに精通している場合は、Amazon FSx for NetApp ONTAP の使用を検討してください。同様に、使用している既存のパートナーソリューションに、クラウド環境のネイティブ統合またはサポートがあるかどうかも検討してください。

- 長期ストレージまたは使用量の少ないコンピューティングをオンプレミスからクラウドにオフロードできますか?

  クラウドストレージには、長期データストレージ用のコスト効率の高いオプションがいくつか用意されています。例えば、Amazon Simple Storage Service (Amazon S3) は、さまざまなユースケース向けに最適化されたさまざまなストレージ層を提供します。機関が特定のデータを長期間保持する必要がある場合は、Amazon Glacier などのコールドストレージソリューションを検討してください。このデータをクラウドストレージにオフロードすると、価値のある高性能なオンプレミスストレージを解放できます。AWS Storage Gateway などのサービスを使用すると、オンプレミスアプリケーションは SMB、NFS、iSCSI などの標準プロトコルを使用してクラウドストレージ層に簡単にアクセスできます。同様に、使用頻度が低い、または使用量が少ないコンピューティングタスクをオフロードすることを検討してください。このようなタスク専用のオンプレミスサーバーがある場合は、代わりにスケーラブルなクラウドコンピューティングサービスを使用できます。この場合、リソースはオンデマンドでプロビジョニングされ、使用した分だけ料金が発生します。こうした低コストの長期ストレージと使用量の少ないコンピューティングのオプションにより、クラウドはバックアップやディザスタリカバリの用途にも最適です。クラウドの安全で耐久性があり、スケーラブルなストレージとコンピューティングを使用すると、必要なストレージとコンピューティングインフラストラクチャを自分で維持することなく、データを保護し、災害発生時にも迅速に復旧できます。

- 実験とイノベーションのための十分な容量がオンプレミスにありますか?

  固定サイズのオンプレミス環境では伸縮性と俊敏性がないため、ユーザーが利用できるサービスとテクノロジーが制限される可能性があります。厳密な更新サイクルがある場合、新しいワークロードは次のサイクルまで実装を待つ必要がある場合があります。この運用モデルは、実験を制限し、

イノベーションを遅らせる可能性があります。新規または新しいワークロードをテストする必要がある場合は、スケーラブルで伸縮自在なクラウドサービスの使用を検討してください。クラウドリソースはオンデマンドでプロビジョニングおよびプロビジョニング解除でき、使用した分に対してのみ料金が発生するため、組織のリスクを最小限に抑えながら、実験とフェイルファストを行うことができます。

- データをオンプレミスに保持することを強制する固有のコンプライアンス要件またはパフォーマンス要件はありますか?

  データレジデンシー要件またはレイテンシー要件が厳しいワークロードでは、データをオンプレミスに保持するか、可能な限りユーザーの近くに保持する必要があります。これらのユースケースでは、既存のオンプレミスリソースの使用を優先できます。ただし、クラウドプロバイダーがオンプレミスでクラウドベースのテクノロジーを使用するエッジサービスまたはメカニズムを提供しているかどうかを検討してください。エッジサービスは、データ処理、分析、ストレージを自身のエンドポイントの近くで行えるようにし、標準的なクラウドプロバイダーのデータセンターの外部にツールをデプロイできるようにします。例えば、AWS は AWS Local Zones や AWS Wavelength などのサービスを提供し、エンドユーザーに近い特定の場所にアプリケーションをデプロイします。また、AWS Outposts、AWS Storage Gateway、Amazon ECS Anywhere、Amazon EKS Anywhere などのサービスを使用して、既存のデータセンターにクラウドサービスと機能を導入することもできます。

シングルクラウドのプロバイダーで技術要件またはビジネス要件を満たせないワークロードにのみ、マルチクラウドを適用する

マルチクラウドとは、複数 (2 つ以上) のクラウドサービスプロバイダーからクラウドサービスを利用することを指します。マルチクラウド戦略を持つことは、複数のクラウドプロバイダーの差別化された機能を活用できるオプションや、単一のクラウドプロバイダーが対応できないデータ主権要件を満たす機能など、特定の利点をもたらす可能性があります。ただし、使用するプロバイダーごとに、そのプロバイダーを効果的に使用するための適切な人材、スキル、トレーニング、ツールセットがあることを確認してください。さらに、特定のワークロードにマルチクラウド戦略を使用する場合は、各クラウドプロバイダーの必要なサービスを統合および相互運用するための追加リソースが必要になります。マルチクラウドは、利点が投資の増加を上回る場合にのみ検討することをお勧めします。マルチクラウド戦略を選択すべきかどうかを判断するには、以下の重要な質問を検討してください。

- さまざまなクラウドプロバイダーが提供するサービスをナビゲートするためのリソースとスキルセットはありますか?

複数のクラウドプロバイダーがさまざまな製品やサービスを提供する場合、スタッフには、各プロバイダーの機能をナビゲートするための基本的なスキルが必要です。1 つのクラウドプロバイダーのサービスのみを使用する場合でも、使用しているサービスや機能によっては、スタッフにスキルアップやトレーニングが必要になることがあります。マルチクラウド戦略を検討している場合は、既存のリソースを評価して、複数のクラウドプロバイダーのサービスを効果的に使用するために必要な追加のスキルセットを決定します。単一のクラウドプロバイダーを使用する場合よりも、スタッフを補強したり、スキルアップとトレーニングに追加の時間と費用を投資したりする必要があるかもしれません。異なるクラウドプロバイダーを使用している個別のチームまたはユーザーが既に存在する場合は、状況に応じて、それらをプライマリクラウドプロバイダーに統合することで得られる組織的な利点を考慮してください。

- 特定のマルチクラウドアーキテクチャでは、どのような追加のオーバーヘッドが発生しますか?

  マルチクラウドの一般的な推進要因は、他のクラウドプロバイダーのサービスと差別化できる機能を持つプロバイダーから特定のマネージドサービスを使用したいというものです。例えば、インフラストラクチャのニーズにはあるクラウドプロバイダーを使用し、ドメインおよびディレクトリサービスには別のプロバイダーのマネージドサービスを使用する場合があります。ただし、その単一のマネージドサービスによって管理上の負担が軽減され、そのアーキテクチャコンポーネントの管理が簡素化された場合でも、コードのリファクタリング、プライベート接続のニーズ、手動による統合作業など、他のワークロードに対して追加のオーバーヘッドが発生する可能性があります。この追加のオーバーヘッドを事前に特定し、そのオーバーヘッドが、チームが差別化されたサービスから得られる利点を相殺したり上回ったりしないようにします。

- クラウドプロバイダー間でモニタリングと管理を一元化するには、どのようにしますか?

  さまざまなクラウドプロバイダーのリソースを使用してアプリケーションと機能のデプロイを開始するときは、そのようなリソースをどのようにタグ付けし、モニタリングし、管理するかを検討してください。各プロバイダーには独自のツールがあり、他の環境に拡張できる場合があります。例えば、Amazon CloudWatch を使用して、主要なメトリクスとログのモニタリング、アラームの作成、単一環境、ハイブリッド環境、マルチクラウド環境にわたるアプリケーションとインフラストラクチャの視覚化を行うことができます。AWS Systems Manager を使用して、リソースの可視性と制御を向上させ、運用上の問題を迅速に診断して修正し、環境間で仮想マシンの更新やパッチ適用などのプロセスを自動化することもできます。プロバイダーのツールでは対応できない要件がある場合は、パートナーソリューションを検討できますが、追加コストや統合作業が発生する可能性があります。

- さまざまなクラウドプロバイダーを使用する場合、自動化を使用して Infrastructure as Code を管理するにはどうすればよいですか?

クラウドでリソースを実行すると、リソースの自動プロビジョニングと管理により、さまざまな環境を効率的に管理できます。API やネイティブ自動化ツールは、クラウドプロバイダーによって異なります。可能であれば、さまざまなクラウドプロバイダーのリソースに対応できる共通のオーケストレーションおよびデプロイツールセットを使用することを検討してください。これにより、柔軟性が向上し、複数のクラウドクラウドにまたがる運用が簡素化されます。ただし、各プロバイダーのネイティブ自動化ツールを個別に使用し、適切な使用を確保するための組織プロセスを確立する方が簡単な場合があります。

- 各クラウドプロバイダーが満たす必要があるコンプライアンス要件と規制要件はありますか?

  データの保存と処理方法を決定する規制上の考慮事項がある場合があります。クラウドプロバイダー全体の各クラウド環境に自動的に適用できるポリシー (ネットワークトラフィック、ストレージ、セキュリティなど) の標準化に焦点を当てます。アプリケーションがデータと通信する方法を検討し、同じプロバイダーでホストします。アプリケーションとそのデータがプロバイダー間で断片化されている場合、コンプライアンス要件と規制要件を確実に満たすことは困難です。多くの場合、セキュリティとアクセスコントロールを簡素化しながら、ネットワークレイテンシーを最小限に抑え、データスループットを最大化し、データ送信を制限するには、アプリケーションをできるだけデータの近くに配置することをお勧めします。

- クラウドプロバイダー全体にアプリケーションをデプロイすると、TCO を最小限に抑え、料金割引を最大化できますか?

  マルチクラウドを検討するときは、総保有コスト (TCO) を考慮することが重要です。複数のクラウドプロバイダーでアプリケーションを実行すると、各環境でリソースを維持および管理するための運用コストと管理オーバーヘッドが増加する可能性があります。さらに、使用量を複数のプロバイダーに分散させると、特定のプロバイダーのボリュームディスカウントやエンタープライズ契約を利用するのが難しくなります。マルチクラウドの利点が TCO の増加に見合うかどうかを判断するときは、これらの要因を考慮してください。

ユースケースの例

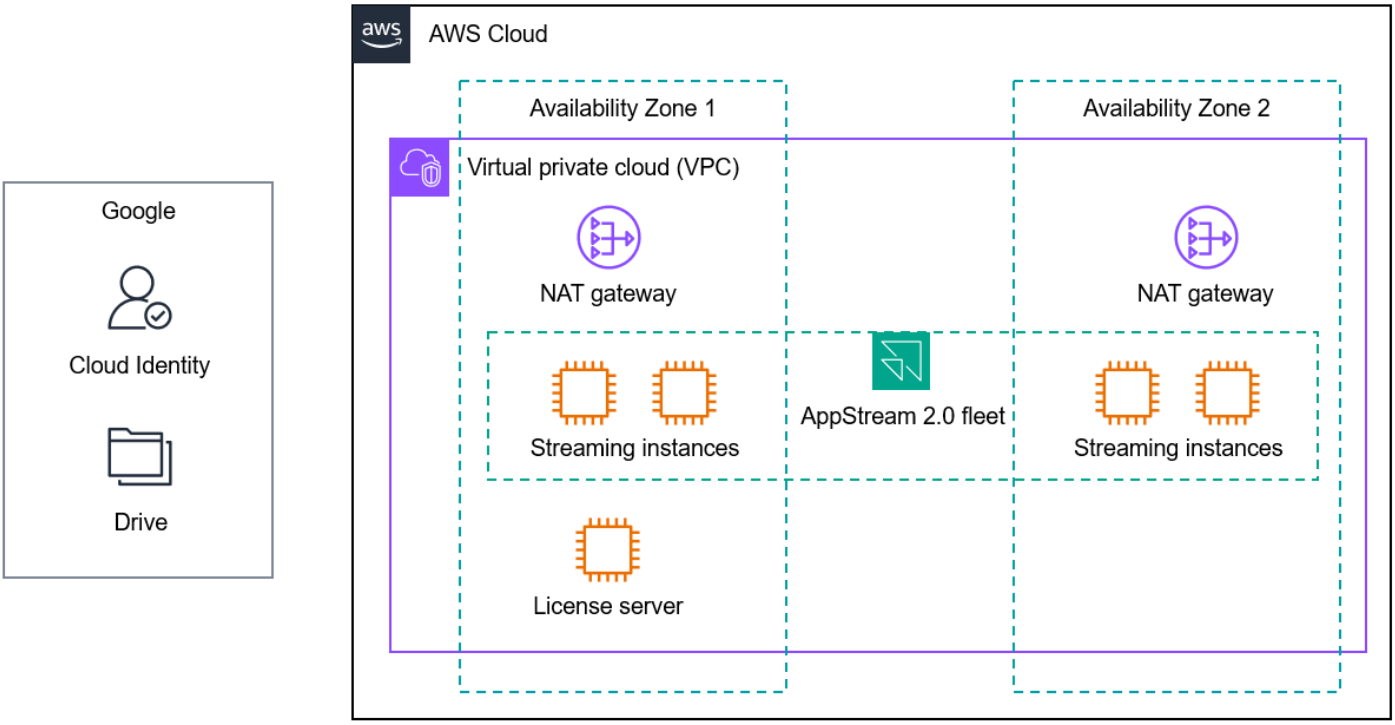
さまざまなシナリオにおけるこれらの原則の適用をよりよく理解するために、いくつかのユースケースの例について説明します。これらのユースケースは、実際の教育機関がクラウドサービスを導入している方法に基づいています。

- 仮想コンピュータラボ
- 学生の成功の予測
- ID フェデレーションとシングルサインオン
- 研究コンピューティングにおけるクラウドでのバースト

仮想コンピュータラボ

ウェブベースの学習ツールが広く利用され、ラップトップ、Chromebook、タブレットなどのユーザーデバイスが豊富にあるにもかかわらず、ほとんどの教育機関では、リソース集約型やレガシーアプリケーション向けに物理的なコンピュータラボを維持しています。こうしたコンピュータラボは、科学、技術、エンジニアリング、数学 (STEM)、キャリアと技術教育 (CTE)、メディアとアート、エンジニアリングなどのカリキュラムで必要とされています。学校は、クラウドベースの仮想デスクトップやアプリケーションストリーミングサービスを活用することで、物理的なコンピュータラボを拡張または置き換え、すべての学生が、いつでも、どこからでも、あらゆるデバイスで必要なアプリケーションにアクセスできるようにできます。これにより、デジタルの公平性が向上し、リモート学習が可能となり、一貫したユーザーエクスペリエンスと安全なリモートアクセスを確保しながら、コストを削減できます。

初等および中等 (K12) 教育では、多くの米国の学校がフルマネージド型のデスクトップおよびアプリケーションストリーミングサービスである Amazon WorkSpaces Applications を使用して仮想コンピュータラボを提供し、Adobe Creative Cloud、Autodesk ソフトウェア、Project Lead the Way (PLTW) などの STEM および CTE カリキュラムへのアクセスを提供します。また、多くの K12 組織では、SaaS アプリケーションである Google Workspace と Google Drive を利用して、学生のシングルサインオンとファイルストレージをすでに管理しています。これらの機関は、SAML 2.0 フェデレーションを通じて Google Workspace と WorkSpaces アプリケーションの間でシングルサインオンを設定できます。また、学生が既存のストレージを使用できるように、WorkSpaces アプリケーションと Google Drive 間のネイティブ統合を設定することもできます。次の図は、このユースケースの WorkSpaces アプリケーションのデプロイを示しています。



このアーキテクチャは、次の推奨事項に従います。

- プライマリの戦略的クラウドプロバイダーを選択します。このアーキテクチャでは、1 つのプライマリクラウドプロバイダーのクラウドサービスを使用します。同じプロバイダーでホストされていない SaaS アプリケーションとの統合が含まれていますが、これらの統合は簡単な設定で実現できます。クラウドに関する専門知識とスキルセットは、プライマリクラウドプロバイダーのサービスをデプロイおよび管理するためにのみ必要です。
- SaaS アプリケーションと基盤クラウドサービスを区別します。Google Workspace と Google Drive は AppStream 2.0 と同じクラウドプロバイダーでホストされていませんが、このデプロイでは必要な統合が行われているため問題ありません。シングルサインオンにより ID 管理を一元化でき、SAML 2.0 を使用して安全に設定できます。学生の永続クラウドストレージを有効にするには、Google Drive と WorkSpaces アプリケーションで簡単な設定変更が必要です。
- 各クラウドサービスプロバイダーのセキュリティとガバナンスの要件を確立します。このアーキテクチャで使用されているサービスと統合は、機関のセキュリティとガバナンスの要件を満たすのに役立ちます。ストリーミングトラフィックは暗号化されます。Google Workspace を使用したフェデレーションにより、ID 管理を一元化できます。Amazon Virtual Private Cloud (Amazon VPC) などのネットワークサービスは、サブネット、ルーティング、ファイアウォールの設定に対応しています。DNS 設定、エージェント、仮想アプライアンス、または Amazon Route 53 Resolver DNS Firewall などのマネージドサービスを使用して、コンテンツをフィルタリングできます。などの

サービスを使用するとAWS Control Tower、WorkSpaces アプリケーションをホストする AWS アカウントが標準の組織ガードレールとコントロールに準拠していることを確認できます。

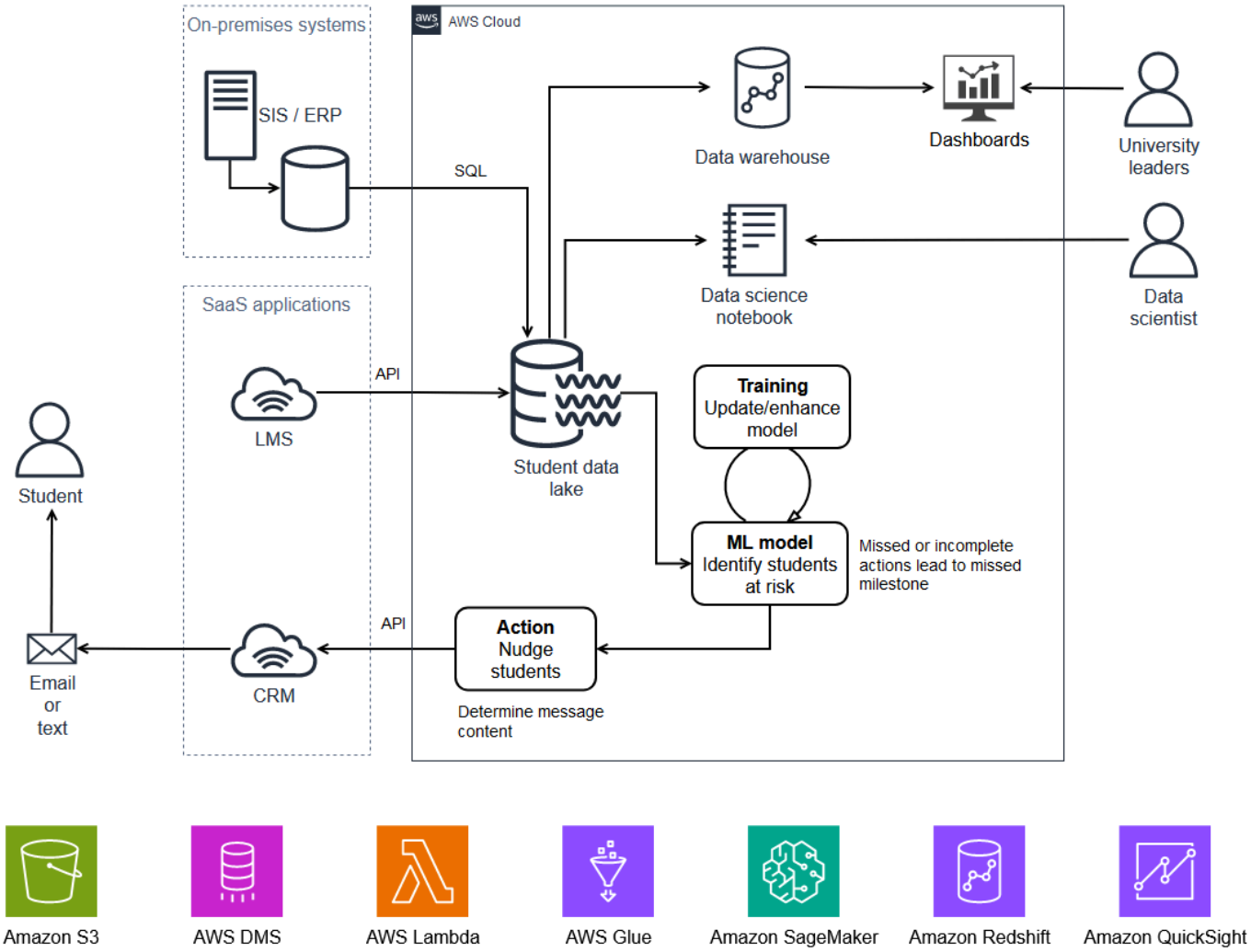
- 可能な限り、かつ実用的であれば、クラウドネイティブのマネージドソリューションを採用します。WorkSpaces アプリケーションは、デスクトップおよびアプリケーションストリーミング用のマネージドサービスです。サーバーのプロビジョニング、スケーリング、保守を気にすることなく、デスクトップとアプリケーションをストリーミングできます。アプリケーションをインストールし、適切な ID、ネットワーク、ストレージソリューションを接続して、それらのアプリケーションを一元管理し、ユーザーにストリーミングします。これにより、自前の仮想デスクトップストリーミングソリューションを管理する際に必要となる未分化の手間のほとんどを省けます。

学生の成功の予測

米国中西部のある大学は、新入生にとっていくつかの重要なアクティビティが、最初の学期での成功と学位取得の両方を予測するうえで高い予測力を持つことを発見しました。この大学は、これらのアクティビティの完了を監視するシステムを導入し、主要な期限が近づいたり過ぎたりした場合には、学生にこれらのステップを完了するように促したいと考えました。

SaaS 学習管理システム (LMS) のデータは、このソリューションの重要な入力でしたが、そのデータは、大学の IT チームが使用するデータウェアハウスツールではアクセスと処理が困難であることが判明しました。さらに、学生へのメッセージは、学校のクラウドベースの顧客関係管理 (CRM) システムを通じて送信する必要がありました。機能的なソリューションを構築し、学生へのプロンプトの有効性を評価するために、大学は CRM を通じてメッセージを送信し、そこからデータを収集する必要がありました。

大学はソリューションを開発し、単一のクラウド環境にデプロイしました。このソリューションは、クラウドネイティブのマネージドサービス、プロビジョニングされたクラウドサーバー、オンプレミスシステムおよびクラウドベースの SaaS アプリケーションとの統合を組み合わせたものです。次の図に示すように、このソリューションは学生情報システム (SIS)、LMS、CRM からデータレイクにデータを取り込みます。この取り込んだデータを使用して、重要なアクティビティを実行できないおそれがある学生を特定し、CRM を通じてその学生にメッセージを送信して、大学のリーダーシップにダッシュボードを提供します。



このアーキテクチャは、次の推奨事項に従います。

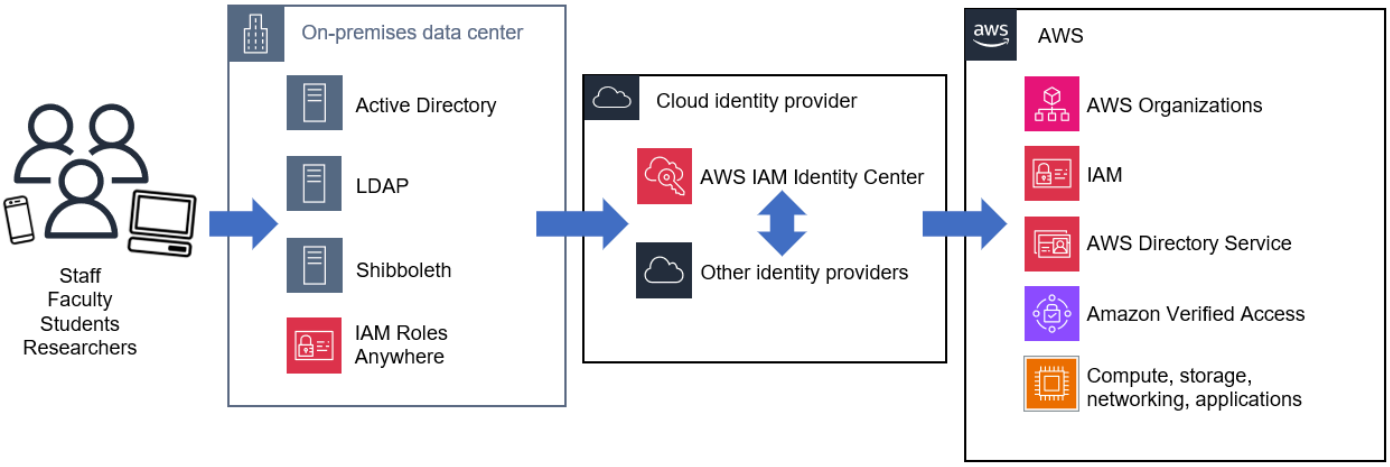
- プライマリの戦略的クラウドプロバイダーを選択します。大学の戦略的クラウドプロバイダーが、デプロイされたソリューション全体をホストしています。これにより、IT スタッフとビジネススタッフは、統合された単一のクラウド機能セットでスキルの開発に集中できます。
- SaaS アプリケーションと基盤クラウドサービスを区別します。大学は、SaaS アプリケーションとコアクラウド分析サービスを区別し、SaaS アプリケーションとの統合を使用してデータを収集し、適切な通信を開始します。
- 各クラウドサービスプロバイダーのセキュリティとガバナンスの要件を確立します。大学は、学生データを適切に処理するために、転送中および保管中の暗号化を含むガードレールとコントロールを適用することで、アーキテクチャのすべてのコンポーネントの安全性を確保します。

- 可能な限り、かつ実用的であれば、クラウドネイティブのマネージドソリューションを採用します。クラウドネイティブのマネージドサービスは、データインジェスト、ストレージ、データベース、抽出、変換、ロード (ETL) 機能に使用されるため、エンドツーエンドのデータ処理ワークフローの開発時間を短縮できます。

ID フェデレーションとシングルサインオン

コアシステム全体で一貫した ID 管理を確保することは、あらゆるテクノロジーを効果的かつ安全に採用するための鍵です。教育機関では、ID 管理を簡素化し、運用上の負担を軽減し、多要素認証や最小特権アクセスなどのベストプラクティスを一元的に適用するために、AWS IAM アイデンティティセンター、Microsoft Entra ID (旧 Azure Active Directory)、Okta、JumpCloud、OneLogin、Ping Identity、CyberArk などのクラウドベースの ID およびシングルサインオンソリューションを導入するケースが増えています。

これらの教育機関の多くでは、オンプレミス環境向けに Active Directory や Shibboleth などの ID 管理とディレクトリサービスを引き続き運用しています。これらのサービスはクラウドベースのソリューションと統合することで、学生、教員、スタッフの一元化された ID 管理とシングルサインオンが可能になります。クラウドソリューションプロバイダーには、クラウド ID プロバイダーを介して、既存のアプリケーション、SaaS ソリューション、クラウドサービスに ID をフェデレーションできる、堅牢で統合が容易な ID 管理プラットフォームが求められます。次の図は、アーキテクチャの例を示しています。



このアーキテクチャは、次の推奨事項に従います。

- プライマリの戦略的クラウドプロバイダーを選択します。このアーキテクチャでは、プライマリクラウドプロバイダー AWS として を使用します。このアーキテクチャは、クラウド ID プロバイ

ダーとオンプレミスの既存の ID 管理およびディレクトリサービスと統合することで、プライマリクラウドプロバイダーのサービスと、他のアプリケーションや SaaS ソリューションの両方へのアクセスの自動プロビジョニングと管理をサポートします。これにより、機関のテクノロジーポートフォリオにより多くのアプリケーションとサービスが追加されていくにつれて、セキュリティとガバナンスの要件を一貫性をもって管理しやすい方法で満たすことができます。

- SaaS アプリケーションと基盤クラウドサービスを区別します。このアーキテクチャは、複数のタイプのクラウドベースの SaaS およびオンプレミスの ID システムを統合して、 AWS クラウドサービスやその他のアプリケーションへのアクセスを提供します。多くのクラウドベースの ID プロバイダーとシングルサインオンソリューションも SaaS アプリケーションであり、ネイティブ統合や SAML などの標準プロトコルを使用して、環境間で連携できます。
- 各クラウドサービスプロバイダーのセキュリティとガバナンスの要件を確立します。このアーキテクチャは、米国国立標準技術研究所 (NIST) サイバーセキュリティフレームワーク (CSF)、NIST 800-171、NIST 800-53 など、多数のセキュリティフレームワークが発行するアイデンティティおよびアクセス管理に関するガイダンスに準拠しています。AWS Organizations、AWS Identity and Access Management (IAM)、およびその他の AWS のセキュリティ、アイデンティティ、コンプライアンスサービスとの統合により、グループのアクセス許可に基づいて安全できめ細かなアクセスコントロールを提供できます。
- 可能な限り、かつ実用的であれば、クラウドネイティブのマネージドサービスを採用します。このアーキテクチャでは、ID 管理とシングルサインオンにクラウドベースのマネージドサービスを使用します。これにより、インフラストラクチャ管理に費やす時間と労力が削減され、これらの重要なシステムのメンテナンスが容易になります。
- 既存のオンプレミス投資が継続利用を促す場合は、ハイブリッドアーキテクチャを実装します。このアーキテクチャは、Active Directory、Lightweight Directory Access Control (LDAP)、および Shibboleth ワークロードをホストするためのインフラストラクチャに対する既存のオンプレミス投資を統合し、コア ID サービスを最終的にクラウドベースのインフラストラクチャへ移行するための道筋を提供します。さらに、オンプレミスワークロードで AWS リソースへの証明書ベースのアクセスが必要な場合は、AWS Identity and Access Management Roles Anywhere を使用できます。

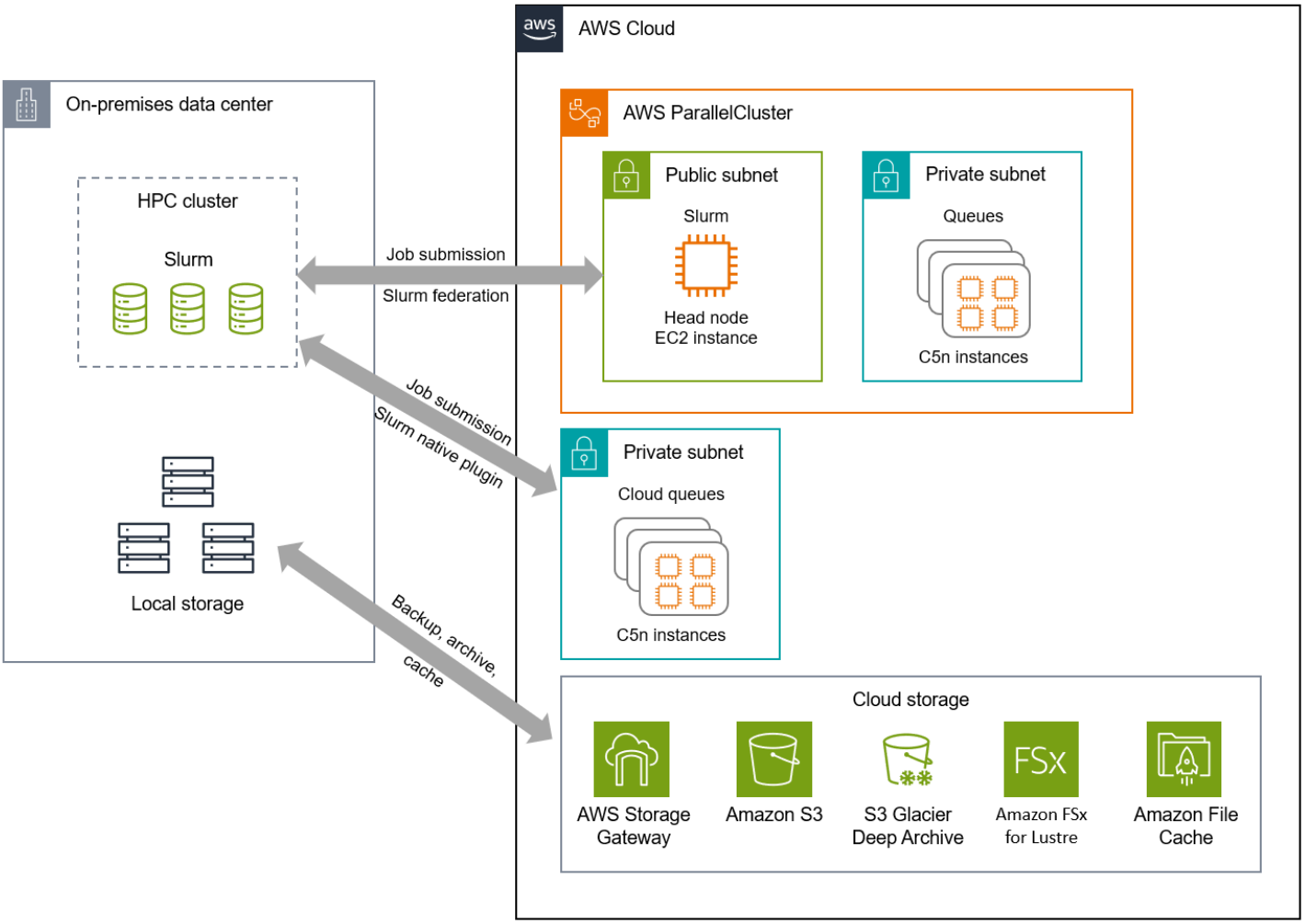
研究コンピューティングにおけるクラウドでのバースト

米国の R1 (博士課程大学 – 研究活動が非常に活発) に分類される研究機関の研究コンピューティンググループは、長年にわたり、Slurm スケジューラを使用してオンプレミスのハイパフォーマンスコンピューティング (HPC) クラスターを運用していました。数週間の定期メンテナンスを除き、クラスターは 80～95% の使用率で稼働しており、ほとんどのキューが満杯でした。

機関での研究活動の増加により、容量と処理能力の課題が生じていました。特定のキューでは、数人の著名な研究者が常に長時間実行されるシミュレーションを実行していたため、他のユーザーの待機時間が長くなっていました。新たに採用された教員は、気象予測用の新しい人工知能と機械学習 (AI/ML) モデルを構築するために多数の気象シミュレーションを実行する必要がありましたが、利用可能な容量よりも多くの容量を必要としていました。研究コンピューティンググループには、機械学習モデルのトレーニングに使用する最新のグラフィックス処理ユニット (GPU) に対するリクエストも増加していました。新しい GPU の資金は確保されていても、チームは、データセンター内のラックスペースを拡張するための承認を得るまでに、数か月待たなければなりませんでした。

多くの研究者が古いデータを削除したがらなかったため、ローカルストレージの容量も課題となっていました。オンプレミスの貴重な高性能ストレージを解放するには、よりスケーラブルで長期的なストレージオプションが必要でした。

クラウドは、オンプレミスの容量が不足している場合に研究コンピューティングをクラウドにバーストできる、ハイブリッドなコンピューティングおよびストレージソリューションによって、これらの課題に対処します。次のアーキテクチャ図は、AWS ParallelCluster や AWS Storage Gateway などのツールを使用して、いくつかのコンピューティングとストレージのバーストアプローチを示しています。



このアーキテクチャは、次の推奨事項に従います。

- プライマリの戦略的クラウドプロバイダーを選択します。このアーキテクチャでは、最小公分母アプローチによる制約を回避するために、1 つのプライマリクラウドプロバイダーを使用します。これにより、プライマリクラウドプロバイダーが提供するイノベーションやネイティブなコンピューティングおよびストレージサービスを活用できます。研究コンピューティングチームは、異なるクラウド環境での対応方法ではなく、プライマリクラウドプロバイダーが提供する環境におけるワークロードの最適化に集中できます。
- 各クラウドサービスプロバイダーのセキュリティとガバナンスの要件を確立します。このアーキテクチャで使用される各サービスとツールは、プライベート接続、転送中および保管中のデータ暗号化、アクティビティのログ記録など、研究コンピューティングチームのセキュリティおよびガバナンス要件を満たすように設定できます。
- 可能な限り、かつ実用的であれば、クラウドネイティブのマネージドサービスを採用します。このアーキテクチャでは、マネージド型のストレージおよびコンピューティングサービスに加えて、

クラスター管理を簡素化するツールを使用できます。これにより、研究コンピューティングチームは、クラスターや基盤となるインフラストラクチャを自分たちで管理する必要がなくなり、こうした管理の複雑さや時間的負担から解放されます。

- 既存のオンプレミス投資が継続利用を促す場合は、ハイブリッドアーキテクチャを実装します。このアーキテクチャにより、機関はオンプレミスのリソースを引き続き使用しながら、クラウドを活用して容量を増やし、必要に応じてコンピューティング能力を増強できます。クラウドを利用することで、コンピューティングタイプを適切なサイズにして価格パフォーマンスを最大化し、追加のオンプレミスハードウェアに多額の先行投資を行うことなく、最新のテクノロジーを活用してイノベーションを促進できます。

次の手順

クラウドワークロードに適したデプロイモデルを選択するには、慎重に検討する必要があります。このホワイトペーパーで概説されている推奨事項を使用して意思決定を行い、不要な複雑性、スタッフへの負担増加、一貫性のないガバナンス、最小公分母的なアプローチなどの一般的な落とし穴を回避します。これらのベストプラクティスに従うことで、クラウド導入を加速し、組織の目標をより効果的に達成し、さらには上回ることができます。

長期的な成功を確実にするために、プライマリの戦略的クラウドプロバイダーを選択し、組織の成熟度を高める Cloud Center of Excellence (CCoE) を設立することを忘れないでください。SaaS アプリケーションと基盤となるクラウドサービスを区別し、それぞれの主要なセキュリティとガバナンスの要件を特定します。可能な限り、クラウドネイティブのマネージドサービスを導入し、既存のデータセンター投資が継続利用を促す場合は、ハイブリッドアーキテクチャを実装します。最後に、マルチクラウドは本当に必要なワークロードにのみ適用します。

AWS は、シングルクラウド、ハイブリッドクラウド、マルチクラウド環境の管理に役立つ適切な位置にあります。、AWS Systems Manager、Amazon CloudWatch などの AWS 管理およびオブザーバビリティソリューションを使用してAWS Config、環境に関係なく、インフラストラクチャとアプリケーションの管理とモニタリングを簡素化および一元化できます。Amazon Athena、AWS Glue、AWS DataSync などのデータおよび分析サービスを使用すると、保存場所を問わず、すべてのデータからインサイトを得ることができます。AWS Outposts、、 などのハイブリッドソリューションAWS Snow Familyを使用するとAWS Wavelength、必要な場所に AWS インフラストラクチャとサービスを導入できます。Amazon EKS Distro などのツールは AWS、セルフマネージド Kubernetes クラスターを 、オンプレミス、またはその他のクラウド上に構築するのに役立ちます。

クラウド戦略を定義するときは、次のステップを検討してください。

1. AWS クラウド導入フレームワーク (AWS CAF) を確認して、トランスフォーメーションの機会を特定して優先順位を付け、クラウドの準備状況を評価して改善し、トランスフォーメーションロードマップを繰り返し進化させます。
2. クラウド実装を概念実証として開始するシステムを特定します。これにより、前提を検証するためのクラウド基盤またはフレームワークを定義し、将来のクラウド実装も可能になります。
3. AWS アカウントチームと協力して、クラウド実装の目標について話し合います。 AWS アカウントチームは、明確化の提供、アプローチの提案、依存関係の特定、チームと協力して最初の概念から実装までのジャーニーの計画に役立てることができます。

寄稿者

このガイドの寄稿者は次のとおりです。

- AWS、Education、Solutions Architecture、Senior Manager、Kevin Arand
- AWS、K-12 Education、Senior Solutions Architect、Kevin McCandless
- AWS、Education、Principal Solutions Architect、Craig Jordan
- AWS、SLG & K-12 Education、Principal Solutions Architect、Jesse Roberts
- AWS、Education、Principal Solutions Architect、Jianjun Xu
- AWS、Education、Senior Solutions Architect、Josh Badal
- AWS、Education、Senior Solutions Architect、Raj Chary

詳細情報

詳細については、次を参照してください。

- AWS アーキテクチャセンター
- Public Sector Cloud Transformation
- AWS クラウド導入フレームワーク (AWS CAF)
- ハイブリッドおよびマルチクラウド向けの AWS ソリューション

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
初版発行	—	2023 年 9 月 15 日

AWS 規範ガイダンスの用語集

以下は、 AWS 規範ガイダンスが提供する戦略、ガイド、パターンで一般的に使用される用語です。エントリを提案するには、用語集の最後のフィードバックの提供リンクを使用します。

数字

7 Rs

アプリケーションをクラウドに移行するための 7 つの一般的な移行戦略。これらの戦略は、ガートナーが 2011 年に特定した 5 Rs に基づいて構築され、以下で構成されています。

- リファクタリング/アーキテクチャの再設計 — クラウドネイティブ特徴を最大限に活用して、俊敏性、パフォーマンス、スケーラビリティを向上させ、アプリケーションを移動させ、アーキテクチャを変更します。これには、通常、オペレーティングシステムとデータベースの移植が含まれます。例: オンプレミスの Oracle データベースを Amazon Aurora PostgreSQL 互換エディションに移行する。
- リプラットフォーム (リフトアンドリシェイプ) — アプリケーションをクラウドに移行し、クラウド機能を活用するための最適化レベルを導入します。例: お客様のオンプレミスの Oracle データベースを AWS クラウドの Oracle 用の Amazon Relational Database Service (Amazon RDS) に移行する。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: 顧客関係管理 (CRM) システムを Salesforce.com に移行する。
- リホスト (リフトアンドシフト) — クラウド機能を活用するための変更を加えずに、アプリケーションをクラウドに移行します。例: お客様のオンプレミスの Oracle データベースを AWS クラウドの EC2 インスタンス上の Oracle に移行する。
- 再配置 (ハイパーバイザーレベルのリフトアンドシフト) – 新しいハードウェアを購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。オンプレミスプラットフォームから同じプラットフォームのクラウドサービスにサーバーを移行します。例： Microsoft Hyper-Vアプリケーションを に移行します AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したいアプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。
- 廃止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

ABAC

「属性ベースのアクセス制御」をご覧ください。

抽象化されたサービス

「マネージドユーザー」をご覧ください。

ACID

「原子性、一貫性、分離性、耐久性 (ACID)」をご覧ください。

アクティブ/アクティブ移行

(双方向レプリケーションツールまたは二重書き込み操作を使用して) ソースデータベースとターゲットデータベースを同期させ、移行中に両方のデータベースが接続アプリケーションからのトランザクションを処理するデータベース移行方法。この方法では、1 回限りのカットオーバーの必要がなく、管理された小規模なバッチで移行できます。アクティブ/パッシブ移行よりも柔軟な方法ですが、さらに多くの作業が必要となります。

アクティブ/パッシブ移行

ソースデータベースとターゲットデータベースを同期させながら、データがターゲットデータベースにレプリケートされている間、接続しているアプリケーションからのトランザクションをソースデータベースのみで処理するデータベース移行方法。移行中、ターゲットデータベースはトランザクションを受け付けません。

集計関数

複数行に処理を行い、グループ全体を対象に単一の戻り値を計算する SQL 関数。集計関数の例としては、SUM や MAX などがあります。

AI

「人工知能」をご覧ください。

AIOps

「AI オペレーション」をご覧ください。

匿名化

データセット内の個人情報を完全に削除するプロセス。匿名化は個人のプライバシー保護に役立ちます。匿名化されたデータは、もはや個人データとは見なされません。

アンチパターン

繰り返し起こる問題に対して頻繁に用いられる解決策で、その解決策が逆効果であったり、効果がなかったり、代替案よりも効果が低かったりするもの。

アプリケーション制御

マルウェアからシステムを保護するために、承認されたアプリケーションのみを使用できるようにするセキュリティアプローチ。

アプリケーションポートフォリオ

アプリケーションの構築と維持にかかるコスト、およびそのビジネス価値を含む、組織が使用する各アプリケーションに関する詳細情報の集まり。この情報は、ポートフォリオの検出と分析プロセス の重要な要素であり、移行、モダナイズ、最適化するアプリケーションを特定し、優先順位を付けるのに役立ちます。

人工知能 (AI)

コンピューティングテクノロジーを使用し、学習、問題の解決、パターンの認識など、通常は人間に関連づけられる認知機能の実行に特化したコンピュータサイエンスの分野。詳細については、「人工知能 (AI) とは何ですか?」をご覧ください。

AI オペレーション (AIOps)

機械学習技術を使用して運用上の問題を解決し、運用上のインシデントと人の介入を減らし、サービス品質を向上させるプロセス。 AWS 移行戦略での AIOps の使用方法については、オペレーション統合ガイド を参照してください。

非対称暗号化

暗号化用のパブリックキーと復号用のプライベートキーから成る 1 組のキーを使用した、暗号化のアルゴリズム。パブリックキーは復号には使用されないため共有しても問題ありませんが、プライベートキーの利用は厳しく制限する必要があります。

原子性、一貫性、分離性、耐久性 (ACID)

エラー、停電、その他の問題が発生した場合でも、データベースのデータ有効性と運用上の信頼性を保証する一連のソフトウェアプロパティ。

属性ベースのアクセス制御 (ABAC)

部署、役職、チーム名など、ユーザーの属性に基づいてアクセス許可をきめ細かく設定する方法。詳細については、 AWS Identity and Access Management (IAM) ドキュメントの「 の ABAC AWS」を参照してください。

信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリーバージョンを保存する場所。匿名化、編集、仮名化など、データを処理または変更する目的で、信頼できるデータソースから他の場所にデータをコピーすることができます。

アベイラビリティーゾーン (AZ)

他のアベイラビリティーゾーンの障害から AWS リージョン 隔離され、同じリージョン内の他のアベイラビリティーゾーンへの低コストで低レイテンシーのネットワーク接続を提供する 内の別の場所。

AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドへの移行を成功させるための効率的で効果的な計画を立て AWS るための、 のガイドラインとベストプラクティスのフレームワークです。 AWS CAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用という 6 つの重点分野にガイダンスをまとめています。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、 AWS CAF は、クラウド導入を成功させるための組織の準備に役立つ人材開発、トレーニング、コミュニケーションに関するガイダンスを提供します。詳細については、AWS CAF ウェブサイトと AWS CAF のホワイトペーパー を参照してください。

AWS ワークロード認定フレームワーク (AWS WQF)

データベース移行ワークロードを評価し、移行戦略を推奨し、作業見積もりを提供するツール。AWS WQF は AWS Schema Conversion Tool (AWS SCT) に含まれています。データベーススキーマとコードオブジェクト、アプリケーションコード、依存関係、およびパフォーマンス特性を分析し、評価レポートを提供します。

B

不正なボット

個人や組織に混乱や損害を与えることを目的としたボット。

BCP

「ビジネス継続性計画 (BCP)」をご覧ください。

動作グラフ

リソースの動作とインタラクションを経時的に示した、一元的なインタラクティブビュー。Amazon Detective の動作グラフを使用すると、失敗したログオンの試行、不審な API 呼び出し、その他同様のアクションを調べることができます。詳細については、Detective ドキュメントの「動作グラフのデータ」を参照してください。

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。「エンディアン性」もご覧ください。

二項分類

バイナリ結果 (2 つの可能なクラスのうちの 1 つ) を予測するプロセス。例えば、お客様の機械学習モデルで「この E メールはスパムですか、それともスパムではありませんか」などの問題を予測する必要があるかもしれません。または「この製品は書籍ですか、車ですか」などの問題を予測する必要があるかもしれません。

ブルームフィルター

要素がセットのメンバーであるかどうかをテストするために使用される、確率的でメモリ効率の高いデータ構造。

ブルー/グリーンデプロイ

それぞれが独立しているが、同一の環境を 2 つ作成するデプロイ戦略。現在のアプリケーションバージョンを 1 つの環境 (ブルー) で実行し、新しいアプリケーションバージョンを別の環境 (グリーン) で実行します。この戦略は、最小限の影響で迅速にロールバックするのに役立ちます。

ボット

インターネット経由で自動タスクを実行し、人間のアクティビティややり取りをシミュレートするソフトウェアアプリケーション。インターネット上の情報のインデックスを作成するウェブクローラーなど、一部のボットは有用または有益です。悪質なボットと呼ばれる他のボットの中には、個人や組織を混乱させたり、損害を与えたりすることを意図したものもあります。

ボットネット

マルウェアに感染しており、ボットハーダーまたはボットオペレーターと呼ばれる単一の当事者によって制御されているボットのネットワーク。ボットネットは、ボットとその影響力を拡大する仕組みとして、非常によく知られています。

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといいます。既存のブランチから新しいブランチを作成し、その新しいブランチで機能を開発した

り、バグを修正したりできます。機能を構築するために作成するブランチは、通常、機能ブランチと呼ばれます。機能をリリースする準備ができたら、機能ブランチをメインブランチに統合します。詳細については、「ブランチの概要」(GitHub ドキュメント) を参照してください。

ブレークグラスアクセス

例外的な状況では、承認されたプロセスを通じて、ユーザーが AWS アカウント 通常アクセス許可を持たない にすばやくアクセスできるようにします。詳細については、 AWS Well-Architected ガイダンスの「ブレークグラス手順の実装」インジケータを参照してください。

ブラウンフィールド戦略

環境の既存インフラストラクチャ。システムアーキテクチャにブラウンフィールド戦略を導入する場合、現在のシステムとインフラストラクチャの制約に基づいてアーキテクチャを設計します。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

価値を生み出すためにビジネスが行うこと (営業、カスタマーサービス、マーケティングなど)。マイクロサービスのアーキテクチャと開発の決定は、ビジネス能力によって推進できます。詳細については、AWSでのコンテナ化されたマイクロサービスの実行ホワイトペーパーの「ビジネス機能を中心に組織化」セクションを参照してください。

ビジネス継続性計画 (BCP)

大規模移行など、中断を伴うイベントが運用に与える潜在的な影響に対処し、ビジネスを迅速に再開できるようにする計画。

C

CAF

「AWS クラウド導入フレームワーク」を参照してください

カナリアデプロイ

エンドユーザーへのバージョンリリースを、時間をかけて段階的に行うこと。確信が持てたら新規バージョンをデプロイして、現在のバージョン全体を置き換えます。

CCoE

「Cloud Center of Excellence」を参照してください。

CDC

「変更データキャプチャ」を参照してください。

変更データキャプチャ (CDC)

データソース (データベーステーブルなど) の変更を追跡し、その変更に関するメタデータを記録するプロセス。CDC は、ターゲットシステムでの変更を監査またはレプリケートして同期を維持するなど、さまざまな目的に使用できます。

カオスエンジニアリング

障害や破壊的なイベントを意図的に導入して、システムの耐障害性をテストすること。AWS Fault Injection Service (AWS FIS) を使用して、 AWS ワークロードにストレスを与え、その応答を評価する実験を実行できます。

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

予測を生成するのに役立つ分類プロセス。分類問題の機械学習モデルは、離散値を予測します。離散値は、常に互いに区別されます。例えば、モデルがイメージ内に車があるかどうかを評価する必要がある場合があります。

クライアント側の暗号化

ターゲットがデータ AWS のサービス を受信する前に、ローカルでデータを暗号化します。

Cloud Center of Excellence (CCoE)

クラウドのベストプラクティスの作成、リソースの移動、移行のタイムラインの確立、大規模変革を通じて組織をリードするなど、組織全体のクラウド導入の取り組みを推進する学際的なチーム。詳細については、 AWS クラウド エンタープライズ戦略ブログの CCoE 投稿を参照してください。

クラウドコンピューティング

リモートデータストレージと IoT デバイス管理に通常使用されるクラウドテクノロジー。クラウドコンピューティングは、一般的に、エッジコンピューティングに接続されています。

クラウド運用モデル

IT 組織において、1 つ以上のクラウド環境を構築、成熟、最適化するために使用される運用モデル。詳細については、「クラウド運用モデルの構築」を参照してください。

導入のクラウドステージ

組織が、 AWS クラウドへの移行時に通常実行する 4 つの段階。

- プロジェクト — 概念実証と学習を目的として、クラウド関連のプロジェクトをいくつか実行する
- 基礎固め — お客様のクラウドの導入を拡大するための基礎的な投資 (ランディングゾーンの作成、CCoE の定義、運用モデルの確立など)
- 移行 — 個々のアプリケーションの移行
- 再発明 — 製品とサービスの最適化、クラウドでのイノベーション

これらのステージは、 AWS クラウド エンタープライズ戦略ブログのブログ記事「クラウドファーストへのジャーニー」と「導入のステージ」で Stephen Orban によって定義されました。移行戦略との関連性については、 AWS 「移行準備ガイド」を参照してください。

CMDB

「構成管理データベース (CMDB)」を参照してください。

コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、GitHub や Bitbucket Cloud があります。コードの各バージョンはブランチと呼ばれます。マイクロサービスの構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

コールドキャッシュ

空である、または、かなり空きがある、もしくは、古いデータや無関係なデータが含まれているバッファキャッシュ。データベースインスタンスはメインメモリまたはディスクから読み取る必要があり、バッファキャッシュから読み取るよりも時間がかかるため、パフォーマンスに影響します。

コールドデータ

めったにアクセスされず、通常は過去のデータです。この種類のデータをクエリする場合、通常は低速なクエリでも問題ありません。このデータを低パフォーマンスで安価なストレージ階層またはクラスに移動すると、コストを削減することができます。

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオといった、ビジュアル形式の情報を分析および抽出する AI の分野。例えば、Amazon SageMaker AI では、CV 用の画像処理アルゴリズムを利用できます。

設定ドリフト

ワークロードにおいて、設定が想定した状態から変化すること。これによって、ワークロードが非準拠になる可能性がありますが、この状態は、徐々に生じ、意図的なものではありません。

構成管理データベース (CMDB)

データベースとその IT 環境 (ハードウェアとソフトウェアの両方のコンポーネントとその設定を含む) に関する情報を保存、管理するリポジトリ。通常、CMDB のデータは、移行のポートフォリオの検出と分析の段階で使用します。

コンフォーマンスパック

コンプライアンスチェックとセキュリティチェックをカスタマイズするためにアセンブルできる AWS Config ルールと修復アクションのコレクション。YAML テンプレートを使用して、コンフォーマンスパックを AWS アカウント および リージョンの単一のエンティティとしてデプロイすることも、組織全体にデプロイすることもできます。詳細については、 AWS Config ドキュメントの「コンフォーマンスパック」を参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD は一般的にパイプラインと呼ばれます。プロセスの自動化、生産性の向上、コード品質の向上、配信の加速化を可能にします。詳細については、「継続的デリバリーの利点」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「継続的デリバリーと継続的なデプロイ」を参照してください。

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

ネットワーク内のデータを重要度と機密性に基づいて識別、分類するプロセス。データに適した保護および保持のコントロールを判断する際に役立つため、あらゆるサイバーセキュリティのリスク管理戦略において重要な要素です。データ分類は、 AWS Well-Architected フレームワークのセキュリティの柱のコンポーネントです。詳細については、「データ分類」を参照してください。

データドリフト

実稼働データと ML モデルのトレーニングに使用されたデータとの間に有意な差異が生じたり、入力データが時間の経過と共に有意に変化したりすることです。データドリフトは、ML モデル予測の全体的な品質、精度、公平性を低下させる可能性があります。

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

非一元的で分散型のデータ所有権を持つとともに、一元的な管理およびガバナンスを行えるアーキテクチャフレームワーク。

データ最小化

厳密に必要なデータのみを収集し、処理するという原則。でデータ最小化を実践 AWS クラウドすることで、プライバシーリスク、コスト、分析のカーボンフットプリントを削減できます。

データ境界

AWS 環境内の一連の予防ガードレール。信頼された ID のみが、期待されるネットワークから信頼されたリソースにアクセスできるようにします。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

raw データをお客様の機械学習モデルで簡単に解析できる形式に変換すること。データの前処理とは、特定の列または行を削除して、欠落している、矛盾している、または重複する値に対処することを意味します。

データ出所

データの生成、送信、保存の方法など、データのライフサイクル全体を通じてデータの出所と履歴を追跡するプロセス。

データ件名

データを収集、処理している個人。

データウェアハウス

分析などのビジネスインテリジェンスをサポートするデータ管理システム。データウェアハウスには、一般的に、大量の履歴データが含まれており、多くの場合、それらはクエリや分析に使用されます。

データベース定義言語 (DDL)

データベース内のテーブルやオブジェクトの構造を作成または変更するためのステートメントまたはコマンド。

データベース操作言語 (DML)

データベース内の情報を変更 (挿入、更新、削除) するためのステートメントまたはコマンド。

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

予測のために複数の深層学習モデルを組み合わせます。ディープアンサンブルを使用して、より正確な予測を取得したり、予測の不確実性を推定したりできます。

深層学習

人工ニューラルネットワークの複数層を使用して、入力データと対象のターゲット変数の間のマッピングを識別する機械学習サブフィールド。

多層防御

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリティの手法。この戦略を に採用するときは AWS、リソースの保護に役立つように、 AWS Organizations 構造の異なるレイヤーに複数のコントロールを追加します。たとえば、多層防御アプローチでは、多要素認証、ネットワークセグメンテーション、暗号化を組み合わせることができます。

委任管理者

では AWS Organizations、互換性のあるサービスが AWS メンバーアカウントを登録して組織のアカウントを管理し、そのサービスのアクセス許可を管理できます。このアカウントを、そのサービスの委任管理者と呼びます。詳細、および互換性のあるサービスの一覧は、 AWS

Organizations ドキュメントの「AWS Organizationsで使用できるサービス」を参照してください。

トラブルシューティング

アプリケーション、新機能、コードの修正をターゲットの環境で利用できるようにするプロセス。デプロイでは、コードベースに変更を施した後、アプリケーションの環境でそのコードベースを構築して実行します。

開発環境

「環境」を参照してください。

検出管理

イベントが発生したときに、検出、ログ記録、警告を行うように設計されたセキュリティコントロール。これらのコントロールは副次的な防衛手段であり、実行中の予防的コントロールをすり抜けたセキュリティイベントをユーザーに警告します。詳細については、「 AWSでのセキュリティコントロールの実装」の「検出的コントロール」を参照してください。

開発バリューストリームマッピング (DVSM)

ソフトウェア開発ライフサイクルのスピードと品質に悪影響を及ぼす制約を特定し、優先順位を付けるために使用されるプロセス。DVSM は、もともとリーンマニュファクチャリング・プラクティスのために設計されたバリューストリームマッピング・プロセスを拡張したものです。ソフトウェア開発プロセスを通じて価値を創造し、動かすために必要なステップとチームに焦点を当てています。

デジタルツイン

建物、工場、産業機器、生産ラインなど、現実世界のシステムを仮想的に表現したものです。デジタルツインは、予知保全、リモートモニタリング、生産最適化をサポートします。

ディメンションテーブル

スタースキーマにおいて、ファクトテーブルの定量データに関するデータ属性が含まれる小さいテーブル。ディメンションテーブルの属性は、通常、テキストフィールド、またはテキストのように扱える個別の数値で示されます。これらの属性は、一般的に、クエリの制約、フィルタリング、結果セットのラベル付けに使用されます。

ディザスタ

ワークロードまたはシステムが、導入されている主要な場所でのビジネス目標の達成を妨げるイベント。これらのイベントは、自然災害、技術的障害、または意図しない設定ミスやマルウェア攻撃などの人間の行動の結果である場合があります。

ディザスタリカバリ (DR)

ディザスタによるダウンタイムとデータ損失を最小限に抑えるための戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 でのワークロードのディザスタリカバリ AWS: クラウドでのリカバリ」を参照してください。

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

各コンポーネントが提供している変化を続けるドメイン、またはコアビジネス目標にコンポーネントを接続して、複雑なソフトウェアシステムを開発するアプローチ。この概念は、エリック・ エヴァンスの著書、Domain-Driven Design: Tackling Complexity in the Heart of Software (ドメイン駆動設計:ソフトウェアの中心における複雑さへの取り組み) で紹介されています (ボストン: Addison-Wesley Professional、2003)。strangler fig パターンでドメイン駆動型設計を使用する方法の詳細については、「コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズ」を参照してください。

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

ベースライン設定からの偏差を追跡します。たとえば、 AWS CloudFormation を使用してシステムリソースのドリフトを検出したり、 を使用して AWS Control Tower 、ガバナンス要件への準拠に影響するランディングゾーンの変更を検出したりできます。

DVSM

「開発バリューストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

EDI

「電子データ交換」を参照してください。

エッジコンピューティング

IoT ネットワークのエッジにあるスマートデバイスの計算能力を高めるテクノロジー。クラウドコンピューティングと比較すると、エッジコンピューティングは通信レイテンシーを短縮し、応答時間を改善できます。

電子データ交換 (EDI)

組織間で行う、ビジネスドキュメントの自動交換。詳細については、「電子データ交換とは」を参照してください。

暗号化

人間が読み取り可能なプレーンテキストデータを暗号文に変換するコンピューティング処理。

暗号化キー

暗号化アルゴリズムが生成した、ランダム化されたビットからなる暗号文字列。キーの長さは決まっておらず、各キーは予測できないように、一意になるように設計されています。

エンディアン

コンピュータメモリにバイトが格納される順序。ビッグエンディアンシステムでは、最上位バイトが最初に格納されます。リトルエンディアンシステムでは、最下位バイトが最初に格納されます。

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

仮想プライベートクラウド (VPC) 内でホストして、他のユーザーと共有できるサービス。を使用してエンドポイントサービスを作成し AWS PrivateLink 、他の AWS アカウント または AWS Identity and Access Management (IAM) プリンシパルにアクセス許可を付与できます。これらのアカウントまたはプリンシパルは、インターフェイス VPC エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon VPC) ドキュメントの「エンドポイントサービスを作成する」を参照してください。

エンタープライズリソースプランニング (ERP)

エンタープライズの主要なビジネスプロセス (会計、MES、プロジェクト管理など) を自動化および管理するシステム。

エンベロープ暗号化

暗号化キーを、別の暗号化キーを使用して暗号化するプロセス。詳細については、 AWS Key Management Service (AWS KMS) ドキュメントの「エンベロープ暗号化」を参照してください。

環境

実行中のアプリケーションのインスタンス。クラウドコンピューティングにおける一般的な環境の種類は以下のとおりです。

- 開発環境 — アプリケーションのメンテナンスを担当するコアチームのみが使用できる、実行中のアプリケーションのインスタンス。開発環境は、上位の環境に昇格させる変更をテストするときに使用します。このタイプの環境は、テスト環境と呼ばれることもあります。
- 下位環境 — 初期ビルドやテストに使用される環境など、アプリケーションのすべての開発環境。
- 本番環境 — エンドユーザーがアクセスできる、実行中のアプリケーションのインスタンス。CI/CD パイプラインでは、本番環境が最後のデプロイ環境になります。
- 上位環境 — コア開発チーム以外のユーザーがアクセスできるすべての環境。これには、本番環境、本番前環境、ユーザー承認テスト環境などが含まれます。

エピック

アジャイル方法論で、お客様の作業の整理と優先順位付けに役立つ機能カテゴリ。エピックでは、要件と実装タスクの概要についてハイレベルな説明を提供します。例えば、 AWS CAF セキュリティエピックには、ID とアクセスの管理、検出コントロール、インフラストラクチャセキュリティ、データ保護、インシデント対応が含まれます。 AWS 移行戦略のエピックの詳細については、プログラム実装ガイドを参照してください。

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

データセットを分析してその主な特性を理解するプロセス。お客様は、データを収集または集計してから、パターンの検出、異常の検出、および前提条件のチェックのための初期調査を実行します。EDA は、統計の概要を計算し、データの可視化を作成することによって実行されます。

F

ファクトテーブル

スタースキーマの中央にあるテーブル。ビジネスオペレーションに関する定量的データが保存されます。一般的に、ファクトテーブルは、2 種類の列で構成されます。1 つは測定値が含まれる列、もう 1 つはディメンションテーブルへの外部キーが含まれる列です。

フェイルファスト

開発ライフサイクルを短縮するために、頻繁かつ段階的にテストを行う哲学であり、アジャイルアプローチでは、この考え方がきわめて重要です。

障害分離境界

では AWS クラウド、障害の影響を制限し、ワークロードの耐障害性を高めるのに役立つアベイラビリティーゾーン AWS リージョン、コントロールプレーン、データプレーンなどの境界。詳細については、「AWS 障害分離境界」を参照してください。

機能ブランチ

「ブランチ」を参照してください。

特徴量

お客様が予測に使用する入力データ。例えば、製造コンテキストでは、特徴量は製造ラインから定期的にキャプチャされるイメージの可能性もあります。

特徴量重要度

モデルの予測に対する特徴量の重要性。これは通常、Shapley Additive Deskonations (SHAP) や積分勾配など、さまざまな手法で計算できる数値スコアで表されます。詳細については、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

機能変換

追加のソースによるデータのエンリッチ化、値のスケーリング、単一のデータフィールドからの複数の情報セットの抽出など、機械学習プロセスのデータを最適化すること。これにより、機械学習モデルはデータの恩恵を受けることができます。例えば、「2021-05-27 00:15:37」の日付を「2021 年」、「5 月」、「木」、「15」に分解すると、学習アルゴリズムがさまざまなデータコンポーネントに関連する微妙に異なるパターンを学習するのに役立ちます。

数ショットプロンプト

LLM に、タスクと望ましい出力を示す例を少数提示した後に、類似のタスクを実行させること。この手法は、プロンプトに記述された例 (ショット) からモデルが学習する「インコンテキスト学

習」の一種です。数ショットプロンプトは、特定のフォーマット、推論、専門知識が必要なタスクに効果的です。「ゼロショットプロンプト」も参照してください。

FGAC

「きめ細かなアクセス制御」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

変更データのキャプチャによる継続的なデータ複製を利用して、段階的なアプローチではなく、可能な限り短時間でデータを移行するデータベース移行方法。目的はダウンタイムを最小限に抑えることです。

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

大規模な深層学習ニューラルネットワークであり、一般化およびラベル付けされていないデータからなる大規模データセットでトレーニングされています。FM により、言語理解、テキストおよび画像生成、自然言語での会話といった、一般的な各種タスクを実行できます。詳細については、「基盤モデルとは何ですか?」を参照してください。

G

生成 AI

AI モデルのサブセット。大量のデータでトレーニングされており、シンプルなテキストプロンプトを使用して、画像、動画、テキスト、オーディオなどの新しいコンテンツやアーティファクトを作成できます。詳細については、「生成 AI とは何ですか?」を参照してください。

ジオブロッキング

「地理的制限」を参照してください。

地理的制限 (ジオブロッキング)

特定の国のユーザーがコンテンツ配信にアクセスできないようにするための、Amazon CloudFront のオプション。アクセスを許可する国と禁止する国は、許可リストまたは禁止リスト

を使って指定します。詳細については、CloudFront ドキュメントの「コンテンツの地理的ディストリビューションの制限」を参照してください。

Gitflow ワークフロー

下位環境と上位環境が、ソースコードリポジトリでそれぞれ異なるブランチを使用する方法。Gitflow ワークフローは古いと見なされている方法であり、トランクベースのワークフローは推奨されている新しい方法です。

ゴールデンイメージ

システムまたはソフトウェアのスナップショットであり、システムまたはソフトウェアの新規インスタンスをデプロイするテンプレートとして使用されます。製造の例で言えば、ゴールデンイメージを使用すると、複数のデバイスにソフトウェアをプロビジョニングして、デバイス製造オペレーションの速度、スケーラビリティ、生産性を向上させることができます。

グリーンフィールド戦略

新しい環境に既存のインフラストラクチャが存在しないこと。システムアーキテクチャにグリーンフィールド戦略を導入する場合、既存のインフラストラクチャ (別名ブラウンフィールド) との互換性の制約を受けることなく、あらゆる新しいテクノロジーを選択できます。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

ガードレール

組織単位 (OU) 全般のリソース、ポリシー、コンプライアンスを管理するのに役立つ概略的なルール。予防ガードレールは、コンプライアンス基準に一致するようにポリシーを実施します。これらは、サービスコントロールポリシーと IAM アクセス許可の境界を使用して実装されます。検出ガードレールは、ポリシー違反やコンプライアンス上の問題を検出し、修復のためのアラートを発信します。これらは AWS Config、、Amazon GuardDuty AWS Security Hub CSPM、、 AWS Trusted Advisor Amazon Inspector、およびカスタム AWS Lambda チェックを使用して実装されます。

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

別のデータベースエンジンを使用するターゲットデータベースへお客様の出典データベースの移行 (例えば、Oracle から Amazon Aurora)。異種間移行は通常、アーキテクチャの再設計作業の一部であり、スキーマの変換は複雑なタスクになる可能性があります。AWS は、スキーマの変換に役立つ AWS SCTを提供します。

高可用性 (HA)

課題や災害が発生した場合に、介入なしにワークロードを継続的に運用できること。HA システムは、自動的にフェイルオーバーし、一貫して高品質のパフォーマンスを提供し、パフォーマンスへの影響を最小限に抑えながらさまざまな負荷や障害を処理するように設計されています。

ヒストリアンのモダナイゼーション

製造業のニーズによりよく応えるために、オペレーションテクノロジー (OT) システムをモダナイズし、アップグレードするためのアプローチ。ヒストリアンは、工場内のさまざまなソースからデータを収集して保存するために使用されるデータベースの一種です。

ホールドアウトデータ

機械学習モデルのトレーニング用データセットから保留される、ラベル付き履歴データの一部。ホールドアウトデータを使用すると、モデル予測をホールドアウトデータと比較して、モデルのパフォーマンスを評価できます。

同種データベースの移行

お客様の出典データベースを、同じデータベースエンジンを共有するターゲットデータベース (Microsoft SQL Server から Amazon RDS for SQL Server など) に移行する。同種間移行は、通常、リホストまたはリプラットフォーム化の作業の一部です。ネイティブデータベースユーティリティを使用して、スキーマを移行できます。

ホットデータ

リアルタイムデータや最近の翻訳データなど、頻繁にアクセスされるデータ。通常、このデータには高速なクエリ応答を提供する高性能なストレージ階層またはクラスが必要です。

ホットフィックス

本番環境の重大な問題を修正するために緊急で配布されるプログラム。緊急性が高いため、通常の DevOps のリリースワークフローからは外れた形で実施されます。

ハイパーケア期間

カットオーバー直後、移行したアプリケーションを移行チームがクラウドで管理、監視して問題に対処する期間。通常、この期間は 1～4 日です。ハイパーケア期間が終了すると、アプリケーションに対する責任は一般的に移行チームからクラウドオペレーションチームに移ります。

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

AWS クラウド 環境内のアクセス許可を定義する 1 つ以上の IAM プリンシパルにアタッチされたポリシー。

アイドル状態のアプリケーション

90 日間の平均的な CPU およびメモリ使用率が 5～20% のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するか、オンプレミスに保持するのが一般的です。

IIoT

「インダストリアル IoT」を参照してください。

イミュータブルインフラストラクチャ

既存インフラストラクチャの更新、パッチ適用、変更などを行わずに、本番環境ワークロードに使用する新規インフラストラクチャをデプロイするモデル。本質的に、イミュータブルインフラストラクチャは、ミュータブルインフラストラクチャよりも一貫性、信頼性、予測性に優れています。詳細については、 AWS Well-Architected フレームワークにある「イミュータブルインフラストラクチャを使用してデプロイする」のベストプラクティスを参照してください。

インバウンド (受信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーションの外部からネットワーク接続を受け入れ、検査し、ルーティングする VPC。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

増分移行

アプリケーションを 1 回ですべてカットオーバーするのではなく、小さい要素に分けて移行するカットオーバー戦略。例えば、最初は少数のマイクロサービスまたはユーザーのみを新しいシステムに移行する場合があります。すべてが正常に機能することを確認できたら、残りのマイクロサービスやユーザーを段階的に移行し、レガシーシステムを廃止できるようにします。この戦略により、大規模な移行に伴うリスクが軽減されます。

インダストリー 4.0

2016 年に Klaus Schwab 氏が提唱した用語で、接続、リアルタイムデータ、オートメーション、分析、AI/ML の進歩による、ビジネスプロセスのモダナイズを意味します。

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

アプリケーションのインフラストラクチャを一連の設定ファイルを使用してプロビジョニングし、管理するプロセス。IaC は、新しい環境を再現可能で信頼性が高く、一貫性のあるものにするため、インフラストラクチャを一元的に管理し、リソースを標準化し、スケールを迅速に行えるように設計されています。

インダストリアル IoT (IIoT)

製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業部門におけるインターネットに接続されたセンサーやデバイスの使用。詳細については、「インダストリアル IoT (IIoT) デジタルトランスフォーメーション戦略の構築」を参照してください。

インスペクション VPC

AWS マルチアカウントアーキテクチャでは、VPC (同一または異なる 内 AWS リージョン)、インターネット、オンプレミスネットワーク間のネットワークトラフィックの検査を管理する一元化された VPCs。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

IoT

インターネットまたはローカル通信ネットワークを介して他のデバイスやシステムと通信する、センサーまたはプロセッサが組み込まれた接続済み物理オブジェクトのネットワーク。詳細については、「IoT とは」を参照してください。

解釈可能性

機械学習モデルの特性で、モデルの予測がその入力にどのように依存するかを人間が理解できる度合いを表します。詳細については、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

IoT

「IoT」を参照してください。

IT 情報ライブラリ (ITIL)

IT サービスを提供し、これらのサービスをビジネス要件に合わせるための一連のベストプラクティス。ITIL は ITSM の基盤を提供します。

IT サービス管理 (ITSM)

組織の IT サービスの設計、実装、管理、およびサポートに関連する活動。クラウドオペレーションと ITSM ツールの統合については、オペレーション統合ガイドを参照してください。

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

強制アクセス制御 (MAC) の実装で、ユーザーとデータ自体にそれぞれセキュリティラベル値が明示的に割り当てられます。ユーザーセキュリティラベルとデータセキュリティラベルが交差する部分によって、ユーザーに表示される行と列が決まります。

ランディングゾーン

ランディングゾーンは、スケーラブルで安全な、適切に設計されたマルチアカウント AWS 環境です。これは、組織がセキュリティおよびインフラストラクチャ環境に自信を持ってワークロードとアプリケーションを迅速に起動してデプロイできる出発点です。ランディングゾーンの詳細については、「安全でスケーラブルなマルチアカウント AWS 環境のセットアップ」を参照してください。

大規模言語モデル (LLM)

大量のデータで事前トレーニングされた深層学習 AI モデル。LLM では、質問への回答、ドキュメントの要約、他言語へのテキスト翻訳、文を完成させるなど、さまざまなタスクを実行できます。詳細については、「大規模言語モデル (LLM) とは何ですか?」を参照してください。

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースアクセス制御」を参照してください。

最小特権

タスクの実行には必要最低限の権限を付与するという、セキュリティのベストプラクティス。詳細については、IAM ドキュメントの「最小特権アクセス許可を適用する」を参照してください。

リフトアンドシフト

「7 Rs」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。「エンディアン性」もご覧ください。

LLM

「大規模言語モデル」を参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

パターン認識と学習にアルゴリズムと手法を使用する人工知能の一種。ML は、モノのインターネット (IoT) データなどの記録されたデータを分析して学習し、パターンに基づく統計モデルを生成します。詳細については、「機械学習」を参照してください。

メインブランチ

「ブランチ」を参照してください。

マルウェア

コンピュータのセキュリティやプライバシーを侵害するように設計されたソフトウェア。マルウェアは、コンピュータシステムの中断、機密情報の漏洩、不正アクセスを招く可能性があります。マルウェアの例には、ウイルス、ワーム、ランサムウェア、トロイの木馬、スパイウェア、キーロガーなどがあります。

マネージドサービス

AWS のサービス はインフラストラクチャレイヤー、オペレーティングシステム、プラットフォーム AWS を運用し、エンドポイントにアクセスしてデータを保存および取得します。マネージドサービスの例として、Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB が挙げられます。このサービスは、抽象化されたサービスとも呼ばれます。

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するソフトウェアシステムであり、工場では、これによって、原材料から製品を完成させます。

MAP

「Migration Acceleration Program」を参照してください。

メカニズム

ツールを作成してその導入を推進し、導入結果を調べて調整を行うための包括的なプロセス。メカニズムとは、運用中にそれ自体を強化し改善するサイクルを意味します。詳細については、AWS 「 Well-Architected フレームワーク」の「メカニズムの構築」を参照してください。

メンバーアカウント

組織の一部である管理アカウント AWS アカウント 以外のすべて AWS Organizations。 アカウントが 組織のメンバーになることができるのは、一度に 1 つのみです。

MES

「製造実行システム」を参照してください。

Message Queuing Telemetry Transport (MQTT)

発行/サブスクライブのパターンに基づく、軽量のマシンツーマシン (M2M) 通信プロトコルであり、リソースに限りのある IoT デバイスに使用されます。

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス

機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロイ、再利用可能なコード、回復力などがあります。詳細については、AWS「サーバーレスサービスを使用したマイクロサービスの統合」を参照してください。

マイクロサービスアーキテクチャ

各アプリケーションプロセスをマイクロサービスとして実行する独立したコンポーネントを使用してアプリケーションを構築するアプローチ。これらのマイクロサービスは、軽量 API を使用して、明確に定義されたインターフェイスを介して通信します。このアーキテクチャの各マイクロサービスは、アプリケーションの特定の機能に対する需要を満たすように更新、デプロイ、およびスケーリングできます。詳細については、「 でのマイクロサービスの実装 AWS」を参照してください。

Migration Acceleration Program (MAP)

組織がクラウドに移行するための強力な運用基盤を構築し、移行の初期コストを相殺するのに役立つコンサルティングサポート、トレーニング、サービスを提供する AWS プログラム。MAP には、組織的な方法でレガシー移行を実行するための移行方法論と、一般的な移行シナリオを自動化および高速化する一連のツールが含まれています。

大規模な移行

アプリケーションポートフォリオの大部分を次々にクラウドに移行し、各ウェーブでより多くのアプリケーションを高速に移動させるプロセス。この段階では、以前の段階から学んだベストプラクティスと教訓を使用して、移行ファクトリー チーム、ツール、プロセスのうち、オートメーションとアジャイルデリバリーによってワークロードの移行を合理化します。これは、AWS 移行戦略 の第 3 段階です。

移行ファクトリー

自動化された俊敏性のあるアプローチにより、ワークロードの移行を合理化する部門横断的なチーム。移行ファクトリーチームには、通常、運用、ビジネスアナリストおよび所有者、移行エンジニア、デベロッパー、およびスプリントで作業する DevOps プロフェッショナルが含まれます。エンタープライズアプリケーションポートフォリオの 20～50% は、ファクトリーのアプローチによって最適化できる反復パターンで構成されています。詳細については、このコンテンツセットの移行ファクトリーに関する解説とCloud Migration Factory ガイドを参照してください。

移行メタデータ

移行を完了するために必要なアプリケーションおよびサーバーに関する情報。移行パターンごとに、異なる一連の移行メタデータが必要です。移行メタデータの例としては、ターゲットサブネット、セキュリティグループ、 AWS アカウントなどがあります。

移行パターン

移行戦略、移行先、および使用する移行アプリケーションまたはサービスを詳述する、反復可能な移行タスク。例: AWS Application Migration Service を使用して Amazon EC2 への移行をリホストします。

Migration Portfolio Assessment (MPA)

オンラインツール。これによって、 AWS クラウドに移行するビジネスケースの検証に必要な情報を得られます。MPA は、詳細なポートフォリオ評価 (サーバーの適切なサイジング、価格設定、TCO 比較、移行コスト分析) および移行プラン (アプリケーションデータの分析とデータ収集、アプリケーションのグループ化、移行の優先順位付け、およびウェーブプランニング) を提供します。MPA ツール (ログインが必要) は、すべての AWS コンサルタントと APN パートナーコンサルタントが無料で利用できます。

移行準備状況評価 (MRA)

AWS CAF を使用して、組織のクラウド準備状況に関するインサイトを取得し、長所と短所を特定し、特定されたギャップを埋めるためのアクションプランを構築するプロセス。詳細については、移行準備状況ガイドを参照してください。MRA は、AWS 移行戦略の第一段階です。

移行戦略

ワークロードを AWS クラウドに移行するために使用するアプローチ。詳細については、この用語集の 7 Rs エントリと、「組織を動員して大規模な移行を加速する」を参照してください。

ML

「機械学習」を参照してください。

モダナイゼーション

古い (レガシーまたはモノリシック) アプリケーションとそのインフラストラクチャをクラウド内の俊敏で弾力性のある高可用性システムに変換して、コストを削減し、効率を高め、イノベーションを活用します。詳細については、「AWS クラウドでのアプリケーションのモダナイズ戦略」を参照してください。

モダナイゼーション準備状況評価

組織のアプリケーションのモダナイゼーションの準備状況を判断し、利点、リスク、依存関係を特定し、組織がこれらのアプリケーションの将来の状態をどの程度適切にサポートできるかを決定するのに役立つ評価。評価の結果として、ターゲットアーキテクチャのブループリント、モダナイゼーションプロセスの開発段階とマイルストーンを詳述したロードマップ、特定されたギャップに対処するためのアクションプランが得られます。詳細については、「AWS クラウドでのアプリケーションのモダナイゼーションの準備状況を評価する」を参照してください。

モノリシックアプリケーション (モノリス)

緊密に結合されたプロセスを持つ単一のサービスとして実行されるアプリケーション。モノリシックアプリケーションにはいくつかの欠点があります。1 つのアプリケーション機能エクスペリエンスの需要が急増する場合は、アーキテクチャ全体をスケーリングする必要があります。モノリシックアプリケーションの特徴を追加または改善することは、コードベースが大きくなると複雑になります。これらの問題に対処するには、マイクロサービスアーキテクチャを使用できます。詳細については、「モノリスをマイクロサービスに分解する」を参照してください。

MPA

「Migration Portfolio Assessment」を参照してください。

MQTT

「Message Queuing Telemetry Transport」を参照してください。

多クラス分類

複数のクラスの予測を生成するプロセス (2 つ以上の結果の 1 つを予測します)。例えば、機械学習モデルが、「この製品は書籍、自動車、電話のいずれですか?」 または、「このお客様にとって最も関心のある商品のカテゴリはどれですか?」と聞くかもしれません。

ミュータブルなインフラストラクチャ

本番ワークロードに使用する既存のインフラストラクチャを更新および変更するためのモデル。Well-Architected AWS フレームワークでは、一貫性、信頼性、予測可能性を向上させるために、イミュータブルインフラストラクチャの使用をベストプラクティスとして推奨しています。

O

OAC

「オリジンアクセス制御」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

移行プロセス中にソースワークロードを停止させる移行方法。この方法はダウンタイムが長くなるため、通常は重要ではない小規模なワークロードに使用されます。

OI

「オペレーション統合」を参照してください。

Ola

「オペレーショナルレベルアグリーメント」を参照してください。

オンライン移行

ソースワークロードをオフラインにせずにターゲットシステムにコピーする移行方法。ワークロードに接続されているアプリケーションは、移行中も動作し続けることができます。この方法はダウンタイムがゼロから最小限で済むため、通常は重要な本番稼働環境のワークロードに使用されます。

OPC-UA

「Open Process Communications - Unified Architecture」を参照してください。

Open Process Communications - Unified Architecture (OPC-UA)

産業オートメーション用のマシンツーマシン (M2M) 通信プロトコル。OPC-UA により、相互運用の際に、データ暗号化、認証、認可の各スキームを標準化できます。

オペレーショナルレベルアグリーメント (OLA)

サービスレベルアグリーメント (SLA) をサポートするために、どの機能的 IT グループが互いに提供することを約束するかを明確にする契約。

運用準備状況レビュー (ORR)

質問と関連するベストプラクティスのチェックリスト。インシデントや起こり得る障害を理解、評価、防止したり、その範囲を縮小したりする際に役立ちます。詳細については、 AWS Well-Architected フレームワークの「Operational Readiness Reviews (ORR)」を参照してください。

運用テクノロジー (OT)

産業オペレーション、機器、インフラストラクチャを制御するために物理環境と連携させるハードウェアおよびソフトウェアシステム。製造分野では、Industry 4.0 への変革を進める上で、OT と情報技術 (IT) システムの統合に焦点が当てられています。

オペレーション統合 (OI)

クラウドでオペレーションをモダナイズするプロセスには、準備計画、オートメーション、統合が含まれます。詳細については、オペレーション統合ガイドを参照してください。

組織の証跡

組織 AWS アカウント 内のすべての のすべてのイベント AWS CloudTrail を ログに記録する によって作成された証跡 AWS Organizations。証跡は、組織に含まれている各 AWS アカウント に作成され、各アカウントのアクティビティを追跡します。詳細については、CloudTrail ドキュメントの「組織の証跡の作成」を参照してください。

組織変更管理 (OCM)

人材、文化、リーダーシップの観点から、主要な破壊的なビジネス変革を管理するためのフレームワーク。OCM は、変化の導入を加速し、移行問題に対処し、文化や組織の変化を推進することで、組織が新しいシステムと戦略の準備と移行するのを支援します。 AWS 移行戦略では、クラウド導入プロジェクトに必要な変化のスピードにより、このフレームワークは人材アクセラレーションと呼ばれます。詳細については、OCM ガイドを参照してください。

オリジンアクセス制御 (OAC)

Amazon Simple Storage Service (Amazon S3) コンテンツを保護するための、CloudFront のアクセス制限の強化オプション。OAC は AWS リージョン、すべての S3 バケット、 AWS KMS (SSE-KMS) によるサーバー側の暗号化、S3 バケットへの動的 PUT および DELETEリクエストをサポートします。

オリジンアクセスアイデンティティ (OAI)

CloudFront の、Amazon S3 コンテンツを保護するためのアクセス制限オプション。OAI を使用すると、CloudFront が、Amazon S3 に認証可能なプリンシパルを作成します。認証されたプリンシパルは、S3 バケット内のコンテンツに、特定の CloudFront ディストリビューションを介してのみアクセスできます。OAC も併せて参照してください。OAC では、より詳細な、強化されたアクセス制御が可能です。

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用テクノロジー」を参照してください。

アウトバウンド (送信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション内から開始されたネットワーク接続を処理する VPC。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

P

アクセス許可の境界

ユーザーまたはロールが使用できるアクセス許可の上限を設定する、IAM プリンシパルにアタッチされる IAM 管理ポリシー。詳細については、IAM ドキュメントのアクセス許可の境界を参照してください。

個人を特定できる情報 (PII)

直接閲覧した場合、または他の関連データと組み合わせた場合に、個人の身元を合理的に推測するために使用できる情報。PII の例には、氏名、住所、連絡先情報などがあります。

PII

「個人を特定できる情報」を参照してください。

プレイブック

クラウドでのコアオペレーション機能の提供など、移行に関連する作業を取り込む、事前定義された一連のステップ。プレイブックは、スクリプト、自動ランブック、またはお客様のモダナイズされた環境を運用するために必要なプロセスや手順の要約などの形式をとることができます。

PLC

「プログラマブルロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

次の操作を可能にするオブジェクト: アクセス許可を定義する (ID ベースのポリシーを参照)。アクセス条件を指定する (リソースベースのポリシーを参照)。 AWS Organizations の組織における全アカウントにアクセス許可の上限を定義する (サービスコントロールポリシーを参照)。

多言語の永続性

データアクセスパターンやその他の要件に基づいて、マイクロサービスのデータストレージテクノロジーを個別に選択します。マイクロサービスが同じデータストレージテクノロジーを使用している場合、実装上の問題が発生したり、パフォーマンスが低下する可能性があります。マイクロサービスは、要件に最も適合したデータストアを使用すると、より簡単に実装でき、パフォーマンスとスケーラビリティが向上します。

ポートフォリオ評価

移行を計画するために、アプリケーションポートフォリオの検出、分析、優先順位付けを行うプロセス。詳細については、「移行の準備状況の評価」を参照してください。

述語

`true` または `false` を返すためのクエリ条件。一般的に、`WHERE` 句に記述されます。

述語プッシュダウン

データベースクエリを最適化する手法。これによって、転送前にクエリ内のデータをフィルタリングします。この手法を取ると、リレーショナルデータベースから取得し処理する必要のあるデータの量が減少するため、クエリのパフォーマンスが向上します。

予防的コントロール

イベントの発生を防ぐように設計されたセキュリティコントロール。このコントロールは、ネットワークへの不正アクセスや好ましくない変更を防ぐ最前線の防御です。詳細については、「AWSでのセキュリティコントロールの実装」の「予防的コントロール」を参照してください。

プリンシパル

アクションを実行し AWS 、リソースにアクセスできる のエンティティ。このエンティティは通常、、IAM AWS アカウントロール、または ユーザーのルートユーザーです。詳細については、IAM ドキュメントの「ロールに関する用語と概念」にあるプリンシパルを参照してください。

プライバシーバイデザイン

開発プロセス全体を通してプライバシーが考慮されているシステムエンジニアリングのアプローチ。

プライベートホストゾーン

1 つ以上の VPC 内のドメインとそのサブドメインへの DNS クエリに対し、Amazon Route 53 がどのように応答するかに関する情報を保持するコンテナ。詳細については、Route 53 ドキュメントの「プライベートホストゾーンの使用」を参照してください。

プロアクティブコントロール

非準拠リソースのデプロイ防止を目的としたセキュリティコントロール。このコントロールにより、プロビジョニング前にリソースをスキャンします。コントロールに準拠していないリソースは、プロビジョニングされません。詳細については、 AWS Control Tower ドキュメントの「コントロールリファレンスガイド」および「 セキュリティコントロールの実装」の「プロアクティブコントロール」を参照してください。 AWS

製品ライフサイクル管理 (PLM)

製品の設計、開発、発売から、成長、成熟、衰退、廃棄に至る、製品のライフサイクル全体を通してデータとプロセスを管理すること。

本番環境

「環境」を参照してください。

プログラマブルロジックコントローラー (PLC)

製造分野で使用される、信頼性と適応性に優れたコンピュータであり、これによって、マシンをモニタリングするとともに、製造プロセスを自動化します。

プロンプトチェイニング

1 つの LLM プロンプトによる出力を次のプロンプトの入力に使用して、より良いレスポンスを生成します。この手法を使用すると、複雑なタスクをサブタスクに分割したり、事前レスポンスを繰り返し改良または拡張したりできます。これによって、モデルのレスポンスの精度と関連性が向上し、粒度の高いパーソナライズされた結果を得られます。

仮名化

データセット内の個人識別子をプレースホルダー値に置き換えるプロセス。仮名化は個人のプライバシー保護に役立ちます。仮名化されたデータは、依然として個人データとみなされます。

発行/サブスクライブ (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。これにより、スケーラビリティと応答性を向上させます。例えば、マイクロサービスベースの MES の場合、マイクロサービスは、他のマイクロサービスがサブスクライブ可能なチャネルにイベントメッセージを発行できます。このシステムでは、発行サービスの変更なしに、新規マイクロサービスを追加できます。

Q

クエリプラン

手順などの一連のステップであり、SQL リレーショナルデータベースシステムのデータにアクセスするために使用されます。

クエリプランのリグレッション

データベースサービスのオプティマイザーが、データベース環境に特定の変更が加えられる前に選択されたプランよりも最適性の低いプランを選択すること。これは、統計、制限事項、環境設定、クエリパラメータのバインディングの変更、およびデータベースエンジンの更新などが原因である可能性があります。

R

RACI マトリックス

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RAG

「検索拡張生成」を参照してください。

ランサムウェア

決済が完了するまでコンピュータシステムまたはデータへのアクセスをブロックするように設計された、悪意のあるソフトウェア。

RASCI マトリックス

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RCAC

「行と列のアクセス制御」を参照してください。

リードレプリカ

読み取り専用に使用されるデータベースのコピー。クエリをリードレプリカにルーティングして、プライマリデータベースへの負荷を軽減できます。

リアーキテクト

「7 Rs」を参照してください。

目標復旧時点 (RPO)

最後のデータリカバリポイントからの最大許容時間です。これにより、最後の回復時点からサービスが中断されるまでの間に許容できるデータ損失の程度が決まります。

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 Rs」を参照してください。

リージョン

地理的エリア内の AWS リソースのコレクション。各 AWS リージョン は、耐障害性、安定性、耐障害性を提供するために、他の から分離され、独立しています。詳細については、「アカウントが使用できる AWS リージョン を指定する」を参照してください。

リグレッション

数値を予測する機械学習手法。例えば、「この家はどれくらいの値段で売れるでしょうか?」という問題を解決するために、機械学習モデルは、線形回帰モデルを使用して、この家に関する既知の事実 (平方フィートなど) に基づいて家の販売価格を予測できます。

リホスト

「7 Rs」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 Rs」を参照してください。

リプラットフォーム

「7 Rs」を参照してください。

再購入

「7 Rs」を参照してください。

回復性

中断に抵抗または中断から回復するアプリケーションの機能。 AWS クラウドでの回復力を計画する際には、一般的に、高可用性とディザスタリカバリが考慮されます。詳細については、「AWS クラウド の耐障害性」を参照してください。

リソースベースのポリシー

Amazon S3 バケット、エンドポイント、暗号化キーなどのリソースにアタッチされたポリシー。このタイプのポリシーは、アクセスが許可されているプリンシパル、サポートされているアクション、その他の満たすべき条件を指定します。

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

移行活動とクラウド運用に関わるすべての関係者の役割と責任を定義したマトリックス。マトリックスの名前は、マトリックスで定義されている責任の種類、すなわち責任 (R) 、説明責任 (A) 、協議 (C) 、情報提供 (I) に由来します。サポート (S) タイプはオプションです。サポートが含まれる場合は RASCI マトリックスと呼ばれ、含まれない場合は RACI マトリックスと呼ばれます。

レスポンシブコントロール

有害事象やセキュリティベースラインからの逸脱について、修復を促すように設計されたセキュリティコントロール。詳細については、「 AWSでのセキュリティコントロールの実装」の「レスポンシブコントロール」を参照してください。

保持

「7 Rs」を参照してください。

廃止

「7 Rs」を参照してください。

検索拡張生成 (RAG)

生成 AI の技術。これにより、LLM では、レスポンスの生成前に、トレーニングデータソースの外部にある信頼できるデータソースが参照されます。例えば、RAG モデルによって、組織のナレッジベースまたはカスタムデータのセマンティック検索を実行できる場合があります。細については、「RAG (検索拡張生成) とは何ですか?」を参照してください。

ローテーション

定期的にシークレット情報を更新して、攻撃者が認証情報にアクセスするのをより困難にするプロセス。

行と列のアクセス制御 (RCAC)

アクセスルールが定義された、基本的で柔軟な SQL 表現の使用。RCAC は行権限と列マスクで構成されています。

RPO

「目標復旧時点」を参照してください。

RTO

「目標復旧時間」を参照してください。

ランブック

特定のタスクを実行するために必要な手動または自動化された一連の手順。これらは通常、エラー率の高い反復操作や手順を合理化するために構築されています。

S

SAML 2.0

多くの ID プロバイダー (IdP) が使用しているオープンスタンダード。この機能を使用すると、フェデレーティッドシングルサインオン (SSO) が有効になるため、ユーザーは組織内のすべてのユーザーを IAM で作成しなくても、 AWS マネジメントコンソール にログインしたり AWS 、API オペレーションを呼び出すことができます。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントの「SAML 2.0 ベースのフェデレーションについて」を参照してください。

SCADA

「監視制御とデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

暗号化された形式で保存するパスワードやユーザー認証情報などの AWS Secrets Manager機密情報または制限付き情報。シークレット値とそのメタデータで構成されます。シークレット値には、バイナリ、1 つの文字列、複数の文字列を指定できます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの概要」を参照してください。

セキュリティバイデザイン

開発プロセス全体を通してセキュリティが考慮されているシステムエンジニアリングのアプローチ。

セキュリティコントロール

脅威アクターによるセキュリティ脆弱性の悪用を防止、検出、軽減するための、技術上または管理上のガードレール。セキュリティコントロールには、主に 4 つの種類があります。4 つとは、予防、検出、レスポンシブ、プロアクティブです。

セキュリティ強化

アタックサーフェスを狭めて攻撃への耐性を高めるプロセス。このプロセスには、不要になったリソースの削除、最小特権を付与するセキュリティのベストプラクティスの実装、設定ファイル内の不要な機能の無効化、といったアクションが含まれています。

Security Information and Event Management (SIEM) システム

セキュリティ情報管理 (SIM) とセキュリティイベント管理 (SEM) のシステムを組み合わせたツールとサービス。SIEM システムは、サーバー、ネットワーク、デバイス、その他ソースからデータを収集、モニタリング、分析して、脅威やセキュリティ違反を検出し、アラートを発信します。

セキュリティレスポンスの自動化

セキュリティイベントへの自動レスポンスまたは自動修復を目的として、事前定義およびプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスを実装するのに役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動レスポンスアクションの例には、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報の更新などがあります。

サーバー側の暗号化

送信先にあるデータの、それ AWS のサービス を受け取る による暗号化。

サービスコントロールポリシー (SCP)

AWS Organizationsの組織内の、すべてのアカウントのアクセス許可を一元的に管理するポリシー。SCP は、管理者がユーザーまたはロールに委任するアクションに、ガードレールを定義したり、アクションの制限を設定したりします。SCP は、許可リストまたは拒否リストとして、許可または禁止するサービスやアクションを指定する際に使用できます。詳細については、 AWS Organizations ドキュメントの「サービスコントロールポリシー」を参照してください。

サービスエンドポイント

のエントリポイントの URL AWS のサービス。ターゲットサービスにプログラムで接続するには、エンドポイントを使用します。詳細については、「AWS 全般のリファレンス」の「AWS のサービス エンドポイント」を参照してください。

サービスレベルアグリーメント (SLA)

サービスのアップタイムやパフォーマンスなど、IT チームがお客様に提供すると約束したものを明示した合意書。

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットといった、サービスパフォーマンス面の指標。

サービスレベル目標 (SLO)

サービスレベルインジケータによって測定され、サービスの状態を表すターゲットメトリクス。

責任共有モデル

クラウドのセキュリティとコンプライアンス AWS について と共有する責任を説明するモデル。AWS はクラウドのセキュリティを担当しますが、お客様はクラウドのセキュリティを担当します。詳細については、「責任共有モデル」を参照してください。

SIEM

「Security Information and Event Management システム」を参照してください。

単一障害点 (SPOF)

特定のアプリケーションを構成する単一の重要なコンポーネントで発生し、システム稼働に支障をきたす可能性のある障害。

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

スプリットアンドシードモデル

モダナイゼーションプロジェクトのスケーリングと加速のためのパターン。新機能と製品リリースが定義されると、コアチームは解放されて新しい製品チームを作成します。これにより、お客様の組織の能力とサービスの拡張、デベロッパーの生産性の向上、迅速なイノベーションのサポートに役立ちます。詳細については、「AWS クラウドでのアプリケーションをモダナイズするための段階的アプローチ」を参照してください。

SPOF

「単一障害点」を参照してください。

スタースキーマ

データベースの編成構造を意味し、1 つの大きいファクトテーブルにトランザクションデータまたは測定データが保存され、1 つ以上の小さいディメンションテーブルにデータ属性が保存されます。この構造は、データウェアハウスやビジネスインテリジェンスを用途とするように設計されています。

strangler fig パターン

レガシーシステムが廃止されるまで、システム機能を段階的に書き換えて置き換えることにより、モノリシックシステムをモダナイズするアプローチ。このパターンは、宿主の樹木から根を成長させ、最終的にその宿主を包み込み、宿主に取って代わるイチジクのつるを例えています。そのパターンは、モノリシックシステムを書き換えるときのリスクを管理する方法として Martin Fowler により提唱されました。このパターンの適用方法の例については、「コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズ」を参照してください。

サブネット

VPC 内の IP アドレスの範囲。サブネットは、1 つのアベイラビリティーゾーンに存在する必要があります。

監視制御とデータ取得 (SCADA)

製造分野において、ハードウェアとソフトウェアを使用して物理アセットと本番運用をモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

ユーザーとのやり取りをシミュレートして、起こり得る問題を検出したり、パフォーマンスをモニタリングしたりすることで、システムをテストします。Amazon CloudWatch Synthetics を使用すると、こうしたテストを作成できます。

システムプロンプト

コンテキスト、指示、ガイドラインなどを提示して、LLM に動作を指示する手法。システムプロンプトは、コンテキストを設定して、ユーザーとやり取りするルールを確立するのに有用です。

T

タグ

AWS リソースを整理するためのメタデータとして機能するキーと値のペア。タグは、 リソースの管理、識別、整理、検索、フィルタリングに役立ちます。詳細については、「AWS リソースのタグ付け」を参照してください。

ターゲット変数

監督された機械学習でお客様が予測しようとしている値。これは、結果変数のことも指します。例えば、製造設定では、ターゲット変数が製品の欠陥である可能性があります。

タスクリスト

ランブックの進行状況を追跡するために使用されるツール。タスクリストには、ランブックの概要と完了する必要のある一般的なタスクのリストが含まれています。各一般的なタスクには、推定所要時間、所有者、進捗状況が含まれています。

テスト環境

「環境」を参照してください。

トレーニング

お客様の機械学習モデルに学習するデータを提供すること。トレーニングデータには正しい答えが含まれている必要があります。学習アルゴリズムは入力データ属性をターゲット (お客様が予測したい答え) にマッピングするトレーニングデータのパターンを検出します。これらのパターンをキャプチャする機械学習モデルを出力します。そして、お客様が機械学習モデルを使用して、ターゲットがわからない新しいデータでターゲットを予測できます。

トランジットゲートウェイ

VPC とオンプレミスネットワークを相互接続するために使用できる、ネットワークの中継ハブ。詳細については、 AWS Transit Gateway ドキュメントの「トランジットゲートウェイとは」を参照してください。

トランクベースのワークフロー

デベロッパーが機能ブランチで機能をローカルにビルドしてテストし、その変更をメインブランチにマージするアプローチ。メインブランチはその後、開発環境、本番前環境、本番環境に合わせて順次構築されます。

信頼されたアクセス

ユーザーに代わって AWS Organizations およびそのアカウントで組織内でタスクを実行するために指定したサービスにアクセス許可を付与します。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、 ドキュメントの「 を他の AWS のサービス AWS Organizations で使用する AWS Organizations 」を参照してください。

チューニング

機械学習モデルの精度を向上させるために、お客様のトレーニングプロセスの側面を変更する。例えば、お客様が機械学習モデルをトレーニングするには、ラベル付けセットを生成し、ラベルを追加します。これらのステップを、異なる設定で複数回繰り返して、モデルを最適化します。

ツーピザチーム

2 枚のピザを分け合えることができるくらい小さな DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

予測機械学習モデルの信頼性を損なう可能性がある、不正確、不完全、または未知の情報を指す概念。不確実性には、次の 2 つのタイプがあります。認識論的不確実性は、限られた、不完全なデータによって引き起こされ、弁論的不確実性 は、データに固有のノイズとランダム性によって引き起こされます。

未分化なタスク

ヘビーリフティングとも呼ばれ、アプリケーションの作成と運用には必要だが、エンドユーザーに直接的な価値をもたらさなかったり、競争上の優位性をもたらしたりしない作業です。未分化なタスクの例としては、調達、メンテナンス、キャパシティプランニングなどがあります。

上位環境

「環境」を参照してください。

V

バキューミング

ストレージを再利用してパフォーマンスを向上させるために、増分更新後にクリーンアップを行うデータベースのメンテナンス操作。

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

プライベート IP アドレスを使用してトラフィックをルーティングできる、2 つの VPC 間の接続。詳細については、Amazon VPC ドキュメントの「VPC ピア機能とは」を参照してください。

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

頻繁にアクセスされる最新の関連データを含むバッファキャッシュ。データベースインスタンスはバッファキャッシュから、メインメモリまたはディスクからよりも短い時間で読み取りを行うことができます。

ウォームデータ

アクセス頻度の低いデータ。この種類のデータをクエリする場合、通常は適度に遅いクエリでも問題ありません。

ウィンドウ関数

現在のレコードに何らかの形で関連している行のグループに計算を実行する SQL 関数。ウィンドウ関数は、移動平均を計算したり、現在の行の相対位置に基づいて他の行の値にアクセスするといったタスクの処理に役立ちます。

ワークロード

ビジネス価値をもたらすリソースとコード (顧客向けアプリケーションやバックエンドプロセスなど) の総称。

ワークストリーム

特定のタスクセットを担当する移行プロジェクト内の機能グループ。各ワークストリームは独立していますが、プロジェクト内の他のワークストリームをサポートしています。たとえば、ポートフォリオワークストリームは、アプリケーションの優先順位付け、ウェーブ計画、および移行メタデータの収集を担当します。ポートフォリオワークストリームは、これらの設備を移行ワークストリームで実現し、サーバーとアプリケーションを移行します。

WORM

「Write-Once-Read-Many」を参照してください。

WQF

「AWS ワークロード資格フレームワーク」を参照してください

Write-Once-Read-Many (WORM)

データを 1 回のみ書き込むことで、データの削除や変更を防ぐストレージモデル。承認済みユーザーは、必要な回数だけデータを読み取ることができますが、変更することはできません。このデータストレージインフラストラクチャは、イミュータブルと見なされます。

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性を悪用した攻撃 (一般的にマルウェアによる)。

ゼロデイ脆弱性

実稼働システムにおける未解決の欠陥または脆弱性。脅威アクターは、このような脆弱性を利用してシステムを攻撃する可能性があります。開発者は、よく攻撃の結果で脆弱性に気付きます。

ゼロショットプロンプト

LLM にタスク実行の手順は提示するが、実行のガイドとして役立つ例 (ショット) は提示しない方法。LLM は、事前トレーニング済みの知識を使用してタスクを処理する必要があります。ゼロショットプロンプトの有効性は、タスクの複雑さとプロンプトの品質によって異なります。「数ショットプロンプト」も参照してください。

ゾンビアプリケーション

平均 CPU およびメモリ使用率が 5% 未満のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するのが一般的です。