AWS クラウド導入フレームワーク

クラウドを活用したデジタルトランスフォーメーションの加速

初回発行日: 2015 年 2 月

更新日: 2021 年 11 月 22 日

注記

お客様は本書の情報について、ご自身の評価に基づき判断する責任を負います。本書は、(a) 情報提供のみを目的としており、(b) AWS が現在提供している製品や方法を記載していますが、これらは予告なく変更される場合があり、(c) AWS または AWS の関連会社、サプライヤーもしくはライセンサーのいかなる約束または保証も提供するものではありません。AWS の製品またはサービスの利用については、明示的か黙示的かを問わず、いかなる保証もなく「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で行われるいかなる契約の一部でもなく、そのような契約の内容を変更するものでもありません。

目次

要約

デジタルテクノロジーの普及によって市場セグメントおよび業界の変革が続く中、アマゾン ウェブ サービス (AWS) を導入すれば、変化するビジネスの状態や進化する顧客のニーズに対応するために組織を変革できるようになります。AWS は、世界で最も包括的で広く導入されているクラウドプラットフォームであるため、コストの削減、ビジネスリスクの低減、オペレーション効率の改善、俊敏性の向上、イノベーションのスピードアップ、新しい収益の創出、カスタマーエクスペリエンスと従業員のエクスペリエンスの変革を実現するのに役立ちます。

AWS クラウド導入フレームワーク (AWS CAF) は、AWS の経験とベストプラクティスを活用して、デジタルトランスフォーメーションを実現し、AWS を革新的に利用してビジネス成果を加速できるようにします。AWS CAF を使用することで、トランスフォーメーションの機会を特定して優先順位付けし、クラウド活用の成熟度を評価して改善し、トランスフォーメーションロードマップを反復的に進化させることができます。

はじめに

デジタルテクノロジーの急速な普及により、さまざまな市場セグメントおよび業界で変化が加速し、競争が激化しています。競争上の優位性を維持することがますます困難になってきているため、企業は、今まで以上に短期間で自社を革新する必要があります。例えば、今後 10 年で S&P 500 企業の 50% が別の企業に入れ替わると予想されています。

同様に、市民の期待と行動が変化しているため、デジタルサービスデリバリーを改善するように公共部門の組織にプレッシャーがかかっています。世界中の組織がデジタルトランスフォーメーションを行っています。デジタルテクノロジーを活用して、変化する市況への適応、顧客満足度の向上、ビジネス成果の加速を実現できるように、組織の変化を推進しています。

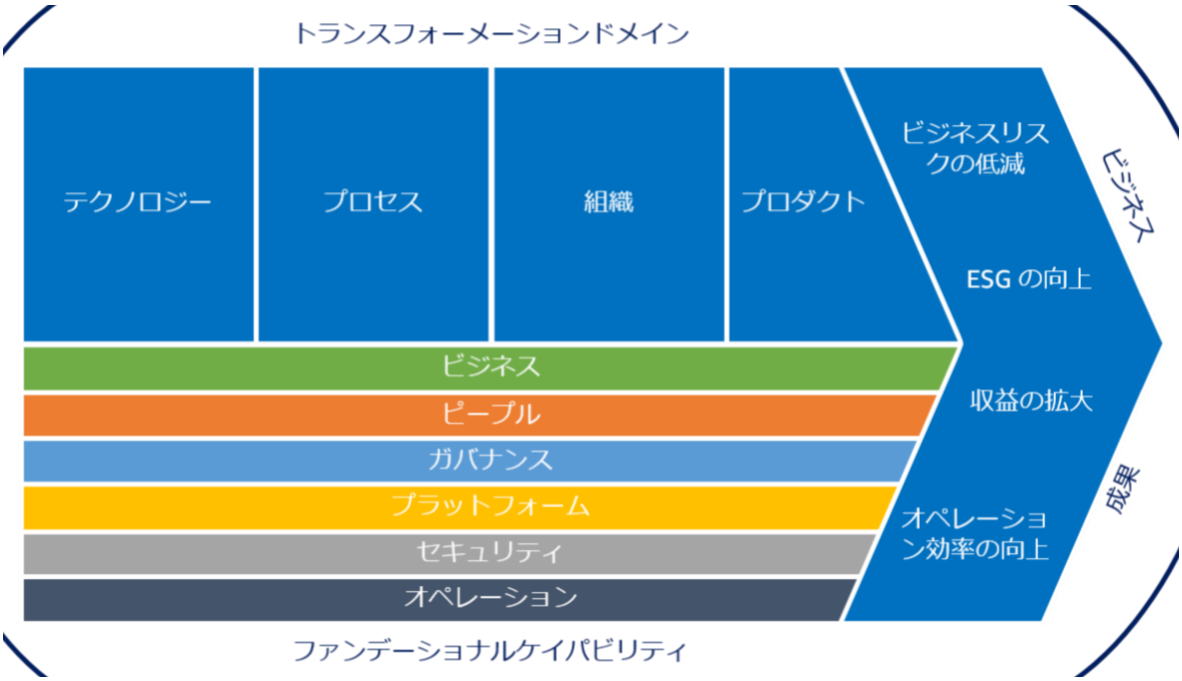
最も急速に成長しているスタートアップ、最大規模のエンタープライズ企業、トップ政府機関など、何百万もの AWS のお客様が AWS を活用して、レガシーワークロードの移行とモダナイズ、データ駆動型への移行、ビジネスプロセスのデジタル化と最適化、運用モデルとビジネスモデルの変革を行っています。クラウドを活用したデジタルトランスフォーメーション (クラウドトランスフォーメーション) により、ビジネス成果の改善 (コストの削減など)、ビジネスリスクの低減、オペレーション効率の改善、俊敏性の向上、イノベーションのスピードアップ、新しい収益の創出、顧客と従業員の体験の改善を実現できます。

クラウドを効果的に活用してデジタルトランスフォーメーションを実現する能力 (クラウド活用の成熟度) は、一連の基盤となるケイパビリティによって支えられます。AWS CAF は、こうしたケイパビリティを特定し、世界中の何千もの組織が使用してクラウドトランスフォーメーションジャーニーを加速するのに成功してきた規範的ガイダンスを提供しています。

AWS および AWS パートナーネットワークでは、ジャーニーの各ステップを進められるようにするツールとサービスを用意しています。AWS Professional Services は、AWS CAF に沿った様々な支援メニューを提供するグローバルなエキスパート集団であり、クラウドトランスフォーメーションを通じて企業がビジネス成果を達成するのをお手伝いします。

クラウドを活用したデジタルトランスフォーメーションによるビジネス成果の加速

次の図のクラウドトランスフォーメーションのバリューチェーンでは、ファンデーショナルケイパビリティによりクラウドを活用した組織的変化 (トランスフォーメーション) が実現した結果、ビジネス成果が加速することが示されています。トランスフォーメーションドメインは、テクノロジーの変革がプロセスの変革を可能にし、プロセスの変革が組織の変革を可能にし、組織の変革がプロダクトの変革を可能にするというバリューチェーンを表しています。主なビジネス成果として、ビジネスリスクの低減、ESG (環境・社会・ガバナンス) の改善、収益の拡大、オペレーション効率の向上が挙げられます



クラウドトランスフォーメーションのバリューチェーン

- **テクノロジートランスフォーメーション**では、レガシーのインフラストラクチャ、アプリケーション、およびデータと分析のプラットフォームを、クラウドを利用して移行とモダナイズすることにフォーカスします。Cloud Value Benchmarking では、オンプレミスから AWS に移行することで、ユーザーあたりのコストが 27% 低下し、管理者あたりの管理対象 VM が 58% 増加し、ダウンタイムが 57% 減少し、セキュリティインシデントが 34% 減少すると示されています。

- **プロセストランスフォーメーション**では、ビジネスオペレーションのデジタル化、自動化、および最適化にフォーカスします。新しいデータと分析プラットフォームを活用して行動につなげられる示唆を得たり、機械学習 (ML) を使用してカスタマーサービスエクスペリエンス、従業員の生産性や意思決定、ビジネスの予測、不正の検出と防止、産業オペレーションを改善したりすることなどがこれに含まれます。これを行うことで、運用コストの削減、従業員のエクスペリエンスとカスタマーエクスペリエンスの向上を実現しながら、オペレーション効率を改善できます。
- **組織トランスフォーメーション**では、運用モデルの刷新にフォーカスします。つまり、顧客の価値を生み出して自社の戦略的な狙いを満たすために、ビジネスのチームとテクノロジーのチームをどう統合するか。アジャイル手法を活用して高速に反復および進化させながら、プロダクトやバリューストリームに基づいてチームを編成すると、対応が早くなり、顧客を中心にして考えられるようになります。
- **プロダクトトランスフォーメーション**では、新しい価値提案 (プロダクト、サービス) および収益モデルを作成することによるビジネスモデルの刷新にフォーカスします。これを行うことで、新しい顧客を獲得したり、新しい市場セグメントに参入したりすることができます。Cloud Value Benchmarking では、AWS を導入することで、新しい機能やアプリケーションの市場投入までの時間が 37% 短縮し、コードのデプロイの頻度が 342% 増加し、新しいコードのデプロイ時間が 38% 短縮すると示されています。

ファンデーショナルケイパビリティ

前のセクションで説明した各トランスフォーメーションドメインは、次の図に示されている一連のファンデーショナルケイパビリティによって実現します。ケイパビリティとは、プロセスを活用することで、リソース (人材、テクノロジー、その他の有形無

形のアセット) をデプロイして特定の成果を実現する組織的能力のことです。AWS CAF のケイパビリティは、クラウド活用の成熟度 (クラウドを効果的に活用してデジタルトランスフォーメーションを実現する能力) の改善に役立つベストプラクティスのガイダンスになります。AWS CAF では、6 つのパースペクティブ (ビジネス、ピープル、ガバナンス、プラットフォーム、セキュリティ、オペレーション) でケイパビリティを分類しています。各パースペクティブは、職能的に関連するステークホルダーがクラウドトランスフォーメーションジャーニーで所有または管理する一連のケイパビリティで構成されています。

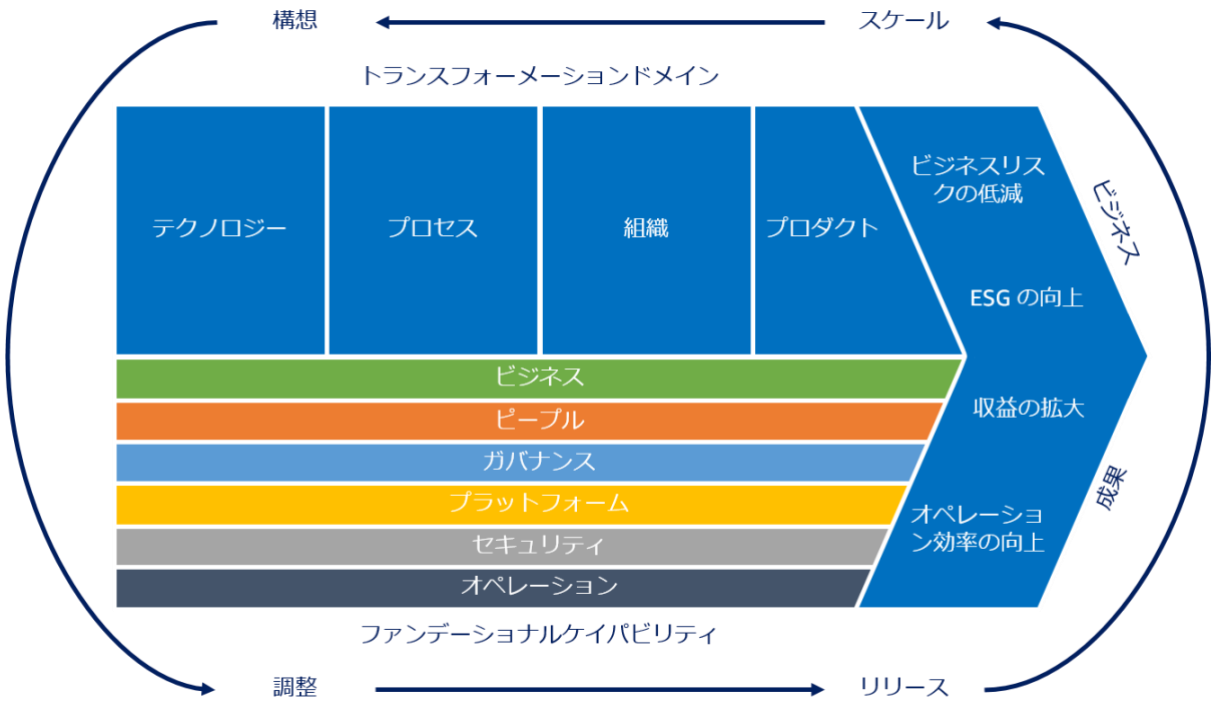
AWS CAF のパースペクティブおよびファンデーショナルケイパビリティ

- **ビジネスパースペクティブ**では、デジタルトランスフォーメーションの目標およびビジネス成果をクラウドへの投資で確実に加速できるようにします。一般的なステークホルダーとして、最高経営責任者 (CEO)、最高財務責任者 (CFO)、最高執行責任者 (COO)、最高情報責任者 (CIO)、最高技術責任者 (CTO) が挙げられます。

- **ピープルパースペクティブ**は、テクノロジーとビジネスの懸け橋の役割を果たします。文化、組織の構造、リーダーシップ、人材にフォーカスし、組織をさらに迅速に進化させ、継続的な成長、学習を行い、変化を受け入れる文化を醸成できるようにクラウドジャーニーを加速します。一般的なステークホルダーとして、CIO、COO、CTO、クラウドディレクター、部門横断の企業全体のリーダーが挙げられます。
- **ガバナンスパースペクティブ**では、組織のメリットを最大化し、トランスフォーメーションに伴うリスクを最小化しながら、クラウドイニシアチブを統合的に推進できるようにします。一般的なステークホルダーとして、最高トランスフォーメーション責任者、CIO、CTO、CFO、最高データ責任者 (CDO)、最高リスク責任者 (CRO) が挙げられます。
- **プラットフォームパースペクティブ**では、拡張性のある大規模なハイブリッドクラウドプラットフォームの構築、既存のワークロードのモダナイズ、新しいクラウドネイティブソリューションの実装を行えるようにします。一般的なステークホルダーとして、CTO、テクノロジーのリーダー、アーキテクト、エンジニアが挙げられます。
- **セキュリティパースペクティブ**では、データとクラウドワークロードの高い機密性、完全性、可用性を実現できるようにします。一般的なステークホルダーとして、最高情報セキュリティ責任者 (CISO)、最高コンプライアンス責任者 (CCO)、内部監査のリーダー、セキュリティのアーキテクトとエンジニアが挙げられます。
- **オペレーションパースペクティブ**では、ビジネスの要求を満たすレベルでクラウドサービスが確実に提供されるようにします。一般的なステークホルダーとして、インフラストラクチャーとオペレーションのリーダー、サイトリライアビリティエンジニア、IT サービスマネージャーが挙げられます。

クラウドトランスフォーメーションジャーニー

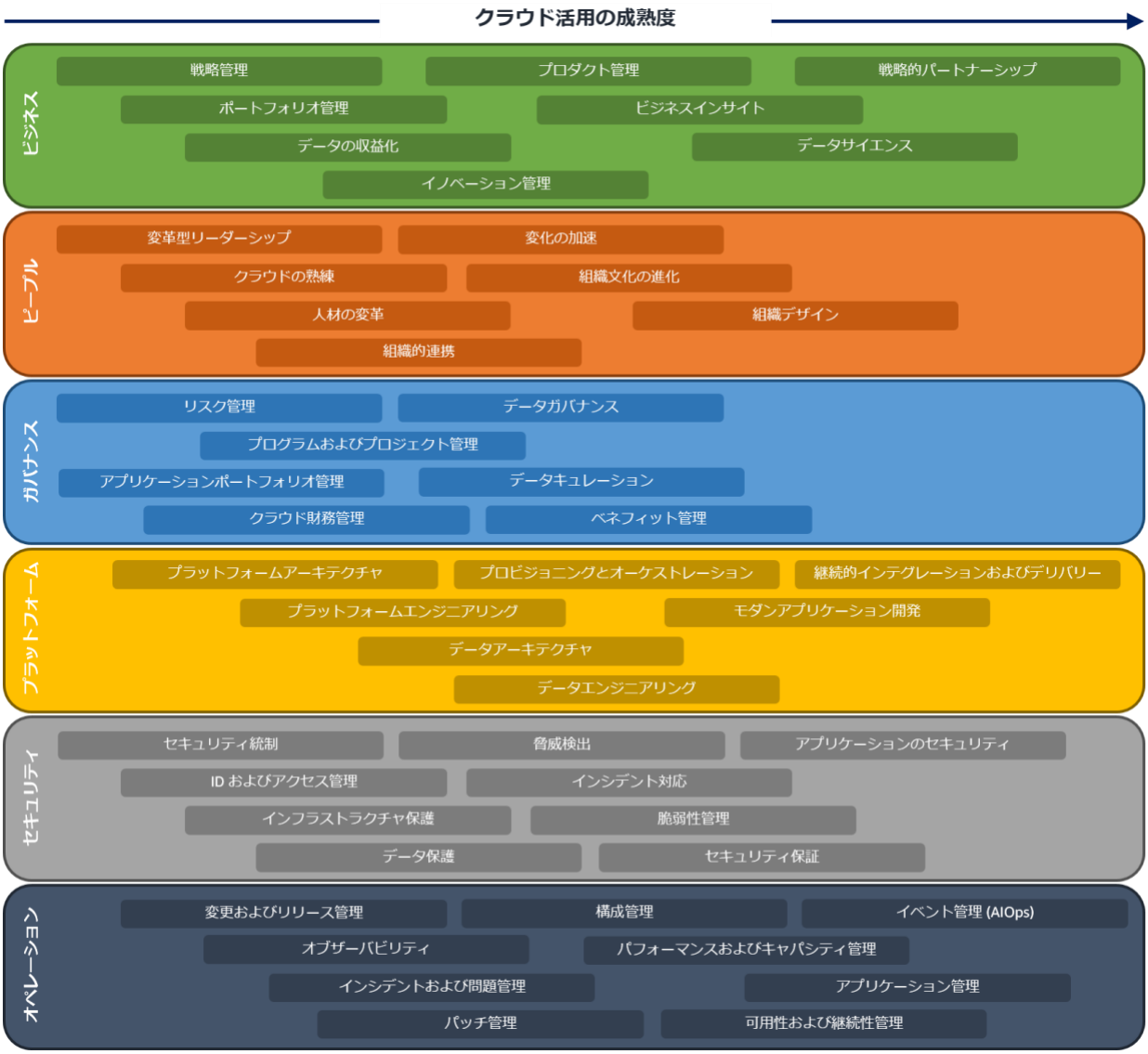
クラウドジャーニーは、組織ごとに独自のものです。トランスフォーメーションを成功させるには、目指すべき理想の状態を想定し、クラウド活用の成熟度を把握し、ギャップを埋めるアジャイル方式を採用する必要があります。増分的にトランスフォーメーションを行うことで、先の見えない予測を行う必要性を最小限に抑えながら、迅速に価値を示すことができます。反復的アプローチを採用することで、推進力を保ち、経験から学びながらロードマップを進化させることができます。AWS CAF では、反復的で増分的なクラウドトランスフォーメーションの 4 つのフェーズが推奨されています (次の図を参照)。



クラウドトランスフォーメーションジャーニー

- **構想フェーズ**では、どのようにクラウドでビジネス成果を加速できるのかを示すことにフォーカスします。これは、戦略的ビジネス目標に合わせて 4 つのトランスフォーメーションドメインのそれぞれで変革の機会を特定して優先順位付けすることで行います。変革イニシアチブを主要ステークホルダー (影響力を持ち、変化を推進できるシニアリーダー) および測定可能なビジネス成果に関連付けることで、トランスフォーメーションジャーニーを進めながら価値を示すことができます。
- **調整フェーズ**では、6 つの AWS CAF パースペクティブでケイパビリティのギャップを特定すること、組織横断の依存関係を特定すること、およびステークホルダーの懸念と課題を明らかにすることにフォーカスします。これにより、クラウド活用の成熟度を改善するための戦略の策定、ステークホルダーの連携の確保、関連する組織の変更管理アクティビティの促進を行えます。
- **リリースフェーズ**では、本番環境でパイロットイニシアチブを実施すること、および増分的なビジネス価値を示すことにフォーカスします。パイロットは影響力が高くなくてはなりません。そうなっていれば、成功した場合に将来の方向性を決定するのに役立ちます。パイロットから学ぶことで、本稼働にスケーリングする前にアプローチを調整できます。
- **スケールフェーズ**では、本番環境でのパイロットおよびビジネス価値を必要な規模に拡張し、クラウドへの投資に伴うビジネスのメリットが実現して維持されることを確認することにフォーカスします。

すべてのファンデーショナルケイパビリティに同時に取り組まなくても構いません。クラウドトランスフォーメーションジャーニーを進めながら、ファンデーショナルケイパビリティを進化させ、クラウド活用の成熟度を改善していきます。次の図で示した推奨手順を参考に、お客様の特定のニーズに合わせて調整することを検討してください。



AWS CAF のパースペクティブおよびファンデーショナルケイパビリティの進化

以降のセクションでは、6 つの AWS CAF パースペクティブとそれを支えるケイパビリティについて詳細に説明します。

ビジネスパースペクティブ: 戦略と成果

ビジネスパースペクティブでは、デジタルトランスフォーメーションの目標およびビジネス成果をクラウドへの投資で確実に加速することにフォーカスします。次の図に示し

た 8 つのケイパビリティで構成されています。一般的なステークホルダーとして、CEO、CFO、COO、CIO、CTO が挙げられます。

AWS CAF のビジネスパースペクティブのケイパビリティ

- **戦略管理** – クラウドを活用して、ビジネス成果を加速します。クラウドでどのように長期的なビジネス目標を支えて形作ることができるのかを検討します。技術的負債を返済する機会およびクラウドを活用してテクノロジーやビジネスオペレーションを最適化する機会を特定します。クラウドで可能になる新しい価値提案と収益モデルを探求します。クラウドで可能になる (新規の、あるいは改善された) プロダクトとサービスにより、どのように新しい顧客を獲得したり、新しい市場セグメントに参入したりすることができるのかを検討します。時間の経過とともに、ビジネス環境における技術的な進歩や変化に対応して、戦略的目標を優先順位付けし、戦略を進化させます。

- **ポートフォリオ管理** – 戦略的意図、オペレーション効率、提供能力に合わせて、クラウドを活用したプロダクトおよびイニシアチブを優先順位付けします。適切なクラウドプロダクトおよびイニシアチブを適切なタイミングで提供することで、戦略を運用可能にし、ビジネス成果を加速できます。自動化された検出ツールと、 アプリケーションをクラウドへ移行するための 7 つの移行戦略 (7 Rs と呼ぶ) を活用して、既存のアプリケーションポートフォリオを合理化し、データ駆動型のビジネスケースを作成します。
  短期的な成果と長期的な成果、および低リスクの (実証済みの) 機会と高リスクの (実験的な) 機会を考慮して、クラウドポートフォリオのバランスを取ります。移行、モダナイズ、およびイノベーションのイニシアチブを組み込み、財務 (低コスト/収益増加) のメリットおよび財務以外 (例えば、カスタマーエクスペリエンスと従業員のエクスペリエンスの向上) のメリットを考慮します。リソース、財務、およびスケジュールの制約に合わせて、ポートフォリオのビジネス価値を最適化します。価値実現までの時間を短縮するために、計画サイクルの頻度を増やしたり、継続的計画戦略を採用したりすることを検討します。
- **イノベーション管理** – クラウドを活用して、プロセス、プロダクト、およびエクスペリエンスを新規に開発したり、既存のものを改善したりします。リソースを瞬時に起動や停止できるようにすることで、クラウドは、価値実現までの時間を短縮し、イノベーション関連のコストとリスクの低減に役立ちます。クラウドの導入で得られる、向上したビジネスの俊敏性をフル活用するために、既存のプロダクト、プロセス、およびエクスペリエンスの最適化にフォーカスした増分的イノベーションイニシアチブと、新しいビジネスモデルの実現にフォーカスした革新的イノベーションイニシアチブを組み合わせたイノベーション戦略を策定します。戦略の優先順位に合わせてアイデアを募って選択するためのメカニズムを作成し、成功したイノベーションパイロットをスケーリングするためのエンドツーエンドのプロセスを開発します。

- **プロダクト管理** – ライフサイクル全体で、プロダクトとして社内外の顧客に反復可能な価値を提供する、データとクラウドを活用したサービスを管理します。データとクラウドを活用したプロダクトごとにチームを編成することで、俊敏性を向上させ、顧客を中心にして考えられるようになります。
  - ビジネス戦略を支える、バランスの取れたプロダクトポートフォリオを作成します。
  - 社内外の顧客のニーズを支える、権限を持った小規模な永続的な部門横断のチームを作り上げます。
  - プロダクトオーナーを特定し、カスタマージャーニーを把握し、プロダクトロードマップを定義および作成し、エンドツーエンドのプロダクトライフサイクルおよび関連するバリューストリームを管理します。
  - クラウドプラットフォームとアジャイル方式を活用して、高速にイテレーションして進化させます。
  - 明確に定義されたインターフェイスによって、プロダクトチーム間の依存関係を低減し、効果的に統合してより広範な運用モデルを作成します。

- **戦略的パートナーシップ** – クラウドプロバイダーとの戦略的パートナーシップにより、ビジネスを構築または成長させます。クラウド上に構築されたソフトウェアソリューション、クラウド統合プロダクト、あるいはクラウド関連の専門的なコンサルティングサービスまたはマネージドサービスを提供する場合、クラウドプロバイダーとの戦略的パートナーシップは、クラウドの専門知識を培い、顧客にソリューションを販売促進し、成功するカスタマーエンゲージメントを推進するのに役立ちます。パートナーシップジャーニーを進めながら、販促クレジット、資金提供の特典、および共同販売の機会を活用して、ビジネスを構築または成長させることができます。クラウドプロバイダーのマーケットプレイスチャネルを活用して、リーチや技術リソースを拡大し、クラウドベースのプロダクトとサービスを成熟させることができます。共同導入事例を公開し、特定のビジネスの課題を解決することに成功したことを取り上げます。
- **データの収益化** – データを活用して、測定可能なビジネスのメリットを獲得します。クラウドは、大量のデータの収集、保存、分析を容易にします。測定可能なビジネスのメリットを得るために、戦略的意図に合わせて、包括的かつ長期的なデータ収益化戦略を策定します。データと分析を活用してオペレーション、カスタマーエクスペリエンスと従業員のエクスペリエンス、意思決定の改善および新規ビジネスモデルの実現を行う機会を特定します。

例えば、顧客の行動に関するインサイトを活用して、ハイパーパーソナライゼーションとローカライゼーション、マイクロセグメンテーション、サブスクライバーの継続、ロイヤルティプログラム、リワードプログラムなどを推進します。ビジネストランザクションを理解して完了できるようにするトランザクションの価値、過去のパフォーマンスを説明して結論を推論できるようにする情報の価値、およびアクティビティを自動化し、意思決定を導き、成果を予測できるようにする分析の価値にフォーカスします。外部での収益化の機会 (例えば、マーケットプレイスでのデータ販売) を検討する前に、まず組織の内部でデータを収益化します。

- **ビジネスインサイト** – リアルタイムのインサイトを得て、ビジネスの問題に答えを見つけます。リアルタイムの具体的なインサイトにより、ビジネスパフォーマンスの追跡、意思決定の改善、オペレーションの最適化を実現することで、データ収益化戦略を実施するのに役立ちます。ビジネスコンテキストをよく把握している部門横断型の分析チームを結成します。技術 (統計など) および技術以外 (可視化やコミュニケーションなど) のスキルにフォーカスします。分析の取り組みをビジネスの目標と重要業績評価指標 (KPI) に合致させます。データカタログを活用して、関連するデータプロダクトおよび可視化のツールと技術を特定し、データのトレンド、パターン、および関係を検出します。まず、「全体像」に焦点を合わせ、必要に応じて詳細にドリルダウンします。
- **データサイエンス** – 実験、高度な分析、および機械学習を活用して、複雑なビジネスの問題を解決します。予測分析と処方的分析により、オペレーション効率、意思決定、カスタマーエクスペリエンスと従業員のエクスペリエンスを改善できるようにすることで、データ収益化戦略を実施するのに役立ちます。

ビジネスプロセス変革の機会を特定した後に、機械学習モデルの構築、トレーニング、およびテストを支援するために必要なデータプロダクトがデータカタログに確実に含まれるようにします。継続的インテグレーションと継続的デリバリー (CI/CD) 手法を活用して、機械学習ワークフローのオペレーションのレジリエンスと再現性を改善します。モデルがどのように予測を行うのかを把握し、潜在的なバイアスを特定します。適切なモデルを本番環境にデプロイし、パフォーマンスをモニタリングします。リスクを軽減するために、信頼性の低い予測は人間の目で確認します。

ピープルパースペクティブ: 文化と変化

ピープルパースペクティブは、テクノロジーとビジネスの懸け橋の役割を果たします。文化、組織の構造、リーダーシップ、人材にフォーカスし、組織をさらに迅速に進化させ、継続的な成長、学習を行い、変化を受け入れる文化を醸成できるようにクラウドジャーニーを加速します。このパースペクティブは、次の図に示した 7 つのケイパビリティで構成されています。一般的なステークホルダーとして、CIO、COO、CTO、クラウドディレクター、部門横断の企業全体のリーダーが挙げられます。

AWS CAF のピープルパースペクティブのケイパビリティ

- **組織文化の進化** – デジタルトランスフォーメーションの目標と、俊敏性、自主性、明確性、スケーラビリティのベストプラクティスを利用して、組織文化を評価し、増分的に進化させ、体系化します。デジタルトランスフォーメーションを成功させるには、顧客のために継続的に改善および革新することに注力した人材を獲得、維持し、権限を与えるといった新しい行動と考え方を取り込みながら、長く受け継がれてきたものとコアバリューを活用する必要があります。長期的な視点を持ちつつ、顧客を重視し、大胆に革新して顧客のニーズを満たします。望ましい文化を形作れるようにする、すべての職務の行動と目標を認識するための組織全体のアプローチを策定します。オーナーシップと自主性を推進し、迅速な意思決定を可能にし、過度な承認やお役所仕事の必要性を最小限に抑えるために、迅速な実験、アジャイル手法、および部門横断的なチームを検討します。
- **変革型リーダーシップ** – リーダーシップ能力を強化し、リーダーを動員することで、革新的な変化を推進し、成果にフォーカスした部門横断型の意思決定を可能にします。クラウドトランスフォーメーションを成功させるには、リーダーは、テクノロジーと同様に、人材の変化にもできる限り注意を払わなければなりません。技術とビジネスのリーダーシップの効果的な融合がなければ、トランスフォーメーションが遅くなったり、停滞したりしてしまう可能性があるからです。技術とビジネスの両方の部門から目に見える積極的な、経営陣によるスポンサーシップを獲得します。両部門は、戦略、ビジョン、スコープ、およびリソースに関する重要な意思決定を行い、コミュニケーション、連携の構築、チームに結果責任を負うように行動します。

経営陣とプログラムの両方のレベルで、ビジネスとテクノロジーのリーダーが、カルチャーチェンジ戦略を共同で開発、統率、実現するようにします。経営陣レイヤーのそれぞれが、明確で一貫したコミュニケーションを行って、クラウドの価値、優先順位、新しい行動について組織を連携させていることを確認します。トランスフォーメーションオフィス/Cloud Center of Excellence (CCoE) を介してクラウドリーダーシップの機能を進化させ、一貫性とスケーラビリティの体系化されたパターンを利用してトランスフォーメーションの取り組みを奨励および推進することを検討します。トランスフォーメーションジャーニーを進めながら、その時々のニーズに合わせて、この機能を増分的に進化させます。

- **クラウドの熟練** – デジタル力を身につけ、自信を持って効果的にクラウドを活用してビジネス成果を加速します。優れた人材の要件は、デジタル環境への適応だけではありません。最大の課題はテクノロジー自体ではなく、パフォーマンスの高い、才能と知識を備えた熟練の人材を雇用、育成、維持、刺激する能力です。

  テクノロジーのイノベーションが急速なペースで進んでいるため、タイミング、ツール、およびテクノロジーのトレーニングに関連した全体的なトレーニング戦略を策定し、その後、既存のクラウドスキルを評価して、目標を絞ったトレーニング戦略を策定します。スキルギルドを実施して、ワクワク感を演出し、トランスフォーメーションジャーニーの推進力を培えるようにします。データリテラシーを奨励して、データ分析に関する人材スキルと知識を高めます。バーチャル、クラスルーム、体験型、ジャストインタイムのトレーニングを組み合わせ、Immersion Day を活用し、正式な AWS 認定試験でスキルを検証します。メンタリング、コーチング、シャドウイング、ジョブローテーションのプログラムを実施します。特定の関心分野を持つ研修コミュニティをセットアップします。ナレッジ共有した社員に報酬を与え、ナレッジの可視化、評価検証、継続的な維持管理のプロセスを標準化します。

- **人材の変革** – 人材を活用し、役割をモダナイズすることで、主要な能力を自主的に推進できる、デジタルを使いこなす、パフォーマンスの高い適応型人材を獲得、育成、維持します。クラウドトランスフォーメーションを成功させるために、従来型の人材管理を超えて人材育成計画を積極的に推進して経営幹部のリーダーシップを組み入れ、リーダーシップ、学習、報酬、インクルージョン、パフォーマンス管理、キャリアの流動性、採用をモダナイズします。
  技術のスキルと技術以外のスキルを適切に組み合わせた、多様性に富んだインクルーシブな人材が必要です。組織全体で役割とスキルのギャップを特定し、組織のクラウド能力を改善する人材戦略を策定します。デジタルスキルを備えた人材および学習意欲の高い人材を活用し、模範とします。パートナーおよびマネージドサービスプロバイダーを使用して労働力を一時的または永続的に補強することを戦略的に検討します。
  新しい人材を獲得するために、デジタル化を推進する方針と組織文化を公に宣伝して強力な雇用企業ブランドを築き上げ、採用戦略、ソーシャルネットワークチャネル、および外部マーケティングでそれを利用します。
- **変化の加速** – 現在の状態から将来の状態に移行する際に人材、文化、職務、組織構造に対する影響を特定して最小限に抑える計画的な変革フレームワークを適用して、新しい働き方の導入を加速します。クラウドトランスフォーメーションは、ビジネスとテクノロジーの両部門で広範囲に及ぶ変化を生み出します。組織は、構造化され、統合された透明性の高い変更プロセスを、仕組みとして隅々まで適用すれば、成功率が高くなり、価値実現および新しい働き方の導入が促進されます。

プロジェクトの最初から変革フレームワークをカスタマイズして適用することで、組織の連携を実現し、1 つの共有されたエンタープライズの実体を創出し、プロセスから無駄を削減します。部門横断的なクラウドリーダーシップを連携させて動員します。ジャーニーの初期の成功がどのようなものかを定義します。影響評価によって組織のクラウド活用の成熟度を評価することで、将来を構想します。主要ステークホルダー、組織横断的な依存関係、主要リスク、トランスフォーメーションの障壁を特定します。リスクに対処して強みを活用する変革戦略とロードマップを策定します。これは、リーダーシップアクションプラン、人材エンゲージメント、コミュニケーション、トレーニング、およびリスク軽減戦略で構成されます。

組織のエンゲージメントを高め、新しい能力で強化することで、新しい働き方の受け入れを促進し、新しいスキルを学習し、導入を加速します。明確に定義されたメトリクスを追跡し、早期段階での成功を祝います。変更を連携させ、推進力を高められるようにする既存の文化的原動力を活用します。変更が継続的フィードバックメカニズム、報酬プログラム、認定プログラムに準拠しているようにします。

- **組織デザイン** – クラウドの新しい働き方に合致しているか、組織デザインを評価し、トランスフォーメーションジャーニーを進めながら進化させます。クラウドを活用してデジタルトランスフォーメーションを行う際に、組織デザインがビジネス、人材、運用環境のコア戦略を確実に支えるようにします。変更の正当性を確証し、組織デザインが、ビジネスの成功の重要な要素であると判断した望ましい行動、職務、文化を反映しているかを評価します。

チーム結成、シフトパターン、指示命令系統、意思決定手順、コミュニケーションチャネルの観点から、現在の組織の構造化と運営の方法で望ましいビジネス成果を引き続き支えられるかを判断します。変革フレームワークを適用して、新しいモデルを設計して実装します。ビジョンに合わせてカスタマイズできるクラウド運用モデルへの移行を最初に促進して実現する、時間の経過とともに進化するように構築された中央集権チームを結成することを検討します。集中型、非集中型、分散型の構造間のトレードオフを検討し、クラウドワークロードの戦略的価値を支えられるように組織デザインを調整します。内部と外部のチームの関係を明確化します (マネージドサービスプロバイダーの使用)。

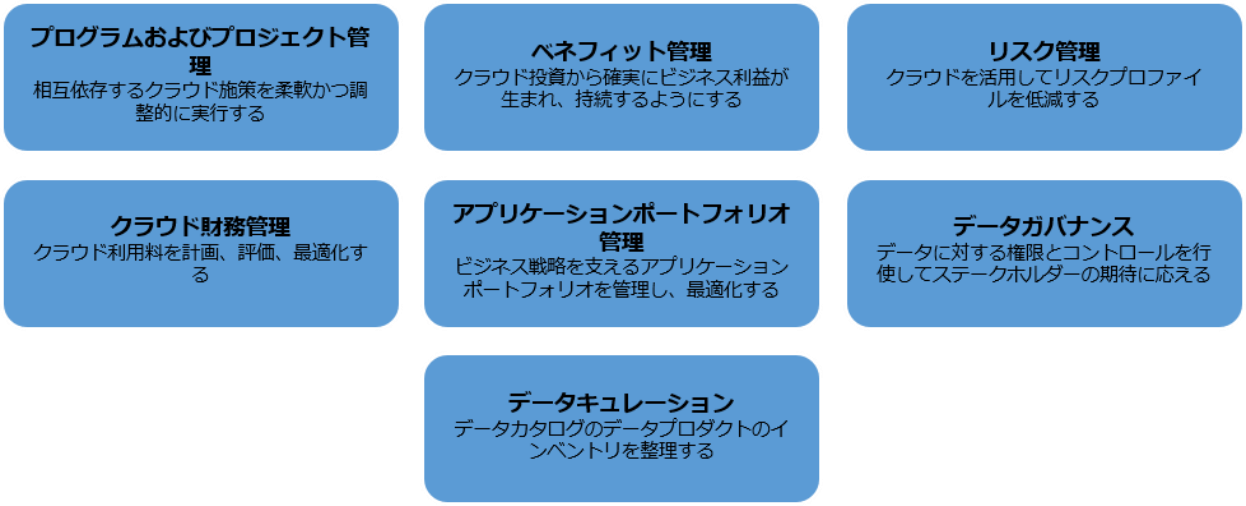
- **組織的連携** – 組織構造、ビジネスオペレーション、プロセス、人材、文化の間の継続的連携を確立して、市況へのエンタープライズの迅速な適応および新しい機会を捉える能力を実現します。クラウド価値の実現を補強するために、組織的連携は、テクノロジーとビジネスの戦略間の懸け橋となり、テクノロジーの変化が、ビジネス成果を生み出すビジネスユニットに受け入れられるようにします。

  運用のレジリエンシー、ビジネスの俊敏性、プロダクト/サービスのイノベーションなどのビジネス成果を優先順位付けします。人材が自主的に作業し、重要な目標にフォーカスし、より優れた意思決定を行い、生産性を改善できるようにします。変革フレームワークの早期適用にリーダーシップが深く関与するようにし、リーダーシップの俊敏性、人材トランスフォーメーション、人材イネーブルメント、文化、および組織構造における人材ケイパビリティが最初から組み込まれているようにします。

クラウド導入の測定可能な目標、共同の目標、メカニズムを設定し、持続可能な変更オーナーシップを生み出すための職務レベルでのスキル開発への期待を創出します。トップダウンアプローチを採用して、価値、プロセス、システム、作業スタイル、スキルを共有することで、協調的にビジネス成果を推進し、部門間の垣根を取り払います。イノベーションの取り組みをカスタマーエクスペリエンスに結び付けます。継続的に導入および革新している人材を認識して報酬を与えます。

ガバナンスパースペクティブ: 制御と監督

ガバナンスパースペクティブでは、組織のメリットを最大化し、トランスフォーメーションに伴うリスクを最小化しながら、クラウドイニシアチブを統合的に推進することにフォーカスします。次の図に示した 7 つのケイパビリティで構成されています。一般的なステークホルダーとして、最高トランスフォーメーション責任者、CIO、CTO、CFO、CDO、CRO が挙げられます。



AWS CAF のガバナンスパースペクティブのケイパビリティ

- **プログラムおよびプロジェクト管理** – 相互依存関係にあるクラウドイニシアチブを協調しながら柔軟に実施します。複雑な部門横断的なクラウドトランスフォーメーションイニシアチブでは、注意深い調整が必要です (特に従来型の構造の組織で顕著)。こうした相互依存関係の多くは実施するまで明らかにならないため、プログラム管理が特に重要です。コスト、スケジュール、取り組み、およびメリットの最適化または統合のための複数のイニシアチブを連携させることで、相互依存関係を管理します。
  ビジネスのスポンサーとともにロードマップを定期的に検証し、問題がある場合はシニアリーダーに適時にエスカレーションし、説明責任と透明性を促進します。アジャイル方式を採用して、先の見えない予測の必要性を最小限に抑え、トランスフォーメーションジャーニーを進めながら経験から学んで適応できるようにします。変化に対応できるように、適切に優先順位付けされたバックログを作成し、エピックとストーリーの形で作業を構造化します。
- **ベネフィットの管理** – クラウド投資に伴うビジネスベネフィットが確実に実現し、維持されるようにします。トランスフォーメーションの成功は、結果として得られるビジネスベネフィットによって決まります。期待するベネフィットを前もって明確に特定しておくことで、クラウドへの投資を優先順位付けし、経時的にトランスフォーメーションの進捗を追跡できます。メトリクスを特定し、期待するベネフィットを定量化し、関連するステークホルダーに伝えます。ベネフィットのタイミングおよび存続期間が戦略的目標に合致するようにします。ロードマップにベネフィットの実現を組み込みます。実現するベネフィットを定期的に測定し、ベネフィット実現ロードマップに照らして進捗を評価し、必要に応じて期待されるベネフィットを調整します。

- **リスク管理** – クラウドを活用して、リスクプロファイルを低減します。インフラストラクチャの可用性、信頼性、パフォーマンス、セキュリティに関連した運用リスクと、評判、ビジネス継続性、変化する市況に迅速に対応する能力に関連したビジネスリスクを特定して定量化します。クラウドでリスクプロファイルを低減し、アジャイルケイデンスの一環として引き続きリスクを反復的に特定して管理する方法を理解します。クラウドを活用して、インフラストラクチャのオペレーションおよび障害に関連したリスクを低減することを検討します。多額のインフラ初期投資の必要性を減らし、使われない資産への投資リスクを低減します。ユーザーのニーズに応じて、クラウドを活用してリソースを瞬時に起動と停止することで、調達スケジュールのリスクを軽減します。
- **クラウド財務管理** – クラウド利用料を計画、測定、および最適化します。クラウドによって得られるリソースプロビジョニングの容易性と俊敏性のメリットをチームのクラウド利用料の財務的説明責任と組み合わせます。これにより、チームはクラウドワークロードを継続的に最適化し、最適な料金モデルを使用できるようになります。クラウドに関連する財務担当の役割と責任を明確化し、財務、ビジネス、およびテクノロジーの組織における主要ステークホルダーがクラウドコストに関する共通の理解を形成するようにします。より動的な予測と予算編成プロセスに進化させ、コスト差異と異常をより迅速に特定します。

組織とプロダクトがどのようにクラウドにマップされるのかに合わせて、アカウント構造とタグ付け戦略を調整します。アカウントとコスト配分タグを構造化して、クラウドリソースが特定のチーム、プロジェクト、およびビジネスイニシアチブに紐づけされるようにし、利用パターンをきめ細かく把握できるようにします。ショーバックやチャージバックを簡素化するカスタムルールを使用して、Cost Categories を定義し、コストと使用量情報を整理します。一括請求を使用して、クラウドの請求を簡素化し、ボリューム割引を実現できるようにします。ガードレールを構築して、俊敏性への影響を最小限に抑えながらスケーラブルな方法でクラウド使用量を制御します。

技術的負債が生じないようにするために、ワークロードが Well-Architected で、最もコスト効率の高い方法で運用されるようにします。需要ベースおよび時間ベースの動的プロビジョニングを活用して、必要なリソースに対してのみ支払います。 アイドル状態または使用率の低いクラウドリソースに関連した支出を特定して排除することで、クラウドコストを削減します。

オンプレミスおよびクラウドのソフトウェアライセンスの管理を一元化することで、ライセンス関連のコスト超過の削減、コンプライアンス違反の削減、および報告ミスの回避を実現します。クラウドリソースに含まれているライセンスと所有しているライセンスを区別します。ライセンスの利用でルールベースのコントロールを活用して、新規および既存のクラウドデプロイに対するハード制限やソフト制限を設定します。ダッシュボードを使用して、ライセンス使用量を可視化し、ベンダー監査を加速します。コンプライアンス違反に対するリアルタイムアラートを実装します。

- **アプリケーションポートフォリオ管理** – ビジネス戦略を支えるために、アプリケーションポートフォリオを管理して最適化します。 アプリケーションはビジネス機能の基盤であり、その機能を関連リソースに紐付けます。正確で完全なアプリケーションインベントリは、合理化、移行、モダナイズの機会を特定するのに役立ちます。効果的なアプリケーションポートフォリオ管理機能があれば、アプリケーションの無秩序な増加を最小限に抑え、アプリケーションライフサイクル計画を促進し、クラウドトランスフォーメーション戦略に継続的に整合することができます。

  最も重要なアプリケーションから始め、包括的なビジネス機能の観点からアプリケーションを定義し、基盤となるソフトウェアプロダクトと関連リソースにアプリケーションを紐づけします。エンタープライズアーキテクチャ、IT サービス管理 (ITSM、IT service management)、プロジェクトおよびポートフォリオ管理などの関連エンタープライズシステムからデータを取得して、各アプリケーションの全体像を構築します。主要なテクノロジーとビジネスのステークホルダー (アプリケーション所有者を含む) を特定し、アプリケーションメタデータを定期的にエンリッチ化および検証するように依頼します。組織がアプリケーションへの投資から得る価値を最大化するために、定期的にアプリケーションポートフォリオの正常性を評価します。
- **データガバナンス** – データに対する権限とコントロールを行使してステークホルダーの期待に応えます。ビジネスプロセスおよび分析能力は、時宜にかなった関連性の高い正確かつ完全なデータに依存しています。データ所有者、スチュワード、カストディアンなどの主要な職務を定義して割り当てます。ガバナンスのフェデレーティッド (データメッシュ) アプローチを採用することを検討します。データ辞書、分類、ビジネス用語集などの標準を規定します。参照する必要があるデータセットを特定し、参照データエンティティ間の関係をモデル化します。

データライフサイクルポリシーを策定し、継続的コンプライアンスモニタリングを実装します。戦略および運用のデータのニーズに合わせて、データ品質の取り組みを優先順位付けします。データ品質標準を策定し、主要な品質属性、ビジネスルール、メトリクス、および目標を特定します。データバリューチェーンの各ステップでデータ品質をモニタリングします。データ品質の問題の根本原因を特定し、原因となっている該当プロセスを改善します。重要なデータプロダクト用のデータ品質ダッシュボードを実装します。

- **データキュレーション** – メタデータの収集、整理、アクセス、エンリッチ化を行い、メタデータを使用してデータカタログ内のデータプロダクトのインベントリを整理します。データカタログは、データ利用者が関連するデータプロダクトを素早く見つけたり、出所や品質などのコンテキストを理解したりできるようにすることで、データの収益化およびセルフサービス分析を促進するのに役立ちます。

  データカタログの調整役を務めるリードキュレーターを特定します。データ収益化戦略に合わせて、構造化データや非構造化データも含め、主要データプロダクトをカタログ化します。系統など、関連するテクノロジーとビジネスのメタデータを特定して収集します。標準のオントロジー、ビジネス用語集、オートメーション (機械学習を含む) を活用して、データのタグ付け、インデックス付け、自動分類を行います。必要に応じて手動のタグ付けによって補い、個人を特定できる情報 (PII) を適切に処理します。ソーシャルキュレーションを利用して、クラウドソーシングによりデータのエンリッチ化を検討します。つまり、データ利用者がデータプロダクトの評価、レビュー、アノテーション付けを行えるようにすることを検討します。

プラットフォームパースペクティブ: インフラストラクチャとアプリケーション

プラットフォームパースペクティブでは、拡張性のある大規模なハイブリッドクラウドプラットフォーム環境でクラウドワークロードの配信を加速することにフォーカスします。次の図に示した 7 つのケイパビリティで構成されています。一般的なステークホルダーとして、CTO、テクノロジーのリーダー、アーキテクト、エンジニアが挙げられます。

AWS CAF のプラットフォームパースペクティブのケイパビリティ

- **プラットフォームアーキテクチャ** – クラウド環境のガイドライン、原則、パターン、ガードレールを確立して維持します。Well-Architected に基づいて設計されたクラウド環境は、実装の加速、リスクの低減、クラウド導入の推進に役立ちます。クラウド導入を推進する全社標準について組織内で合意を形成します。ベストプラクティスのブループリントとガードレールを定義して、認証、セキュリティ、ネットワーク、およびログ記録とモニタリングを促進します。レイテンシー、データ処理、データ保管先の制約のためにオンプレミスに留める必要があるワークロードを検討します。クラウドでの爆発的なトラフィックの処理、クラウドへのバックアップと災害対策、分散データ処理、エッジコンピューティングなどのハイブリッドクラウドのユースケースを評価します。
- **データアーキテクチャ** – 目的に沿ったデータと分析アーキテクチャを設計して進化させます。適切に設計されたデータと分析のアーキテクチャにより、指数関数的に増大するデータボリュームから行動につなげられるインサイトを引き出しながら、複雑性、コスト、技術的負債を削減できます。適切なジョブで適切なツールを使用できるようにする階層型のモジュラーアーキテクチャを採用するとともに、新たに生じた要件やユースケースに合うようにアーキテクチャを増分的に進化させます。

  要件に基づいて、取り込み、ストレージ、カタログ、処理、利用などのアーキテクチャレイヤーごとに主要テクノロジーを選択します。継続的管理を簡素化するために、サーバーレステクノロジーの採用を検討します。リアルタイムのデータ処理の扱いにフォーカスし、レイクハウスアーキテクチャを採用してデータレイクと目的別データストア間のデータ移動を促進することを検討します。

- **プラットフォームエンジニアリング** – 高度なセキュリティ機能と再利用可能なパッケージ化されたクラウドプロダクトでコンプライアンスに沿ったマルチアカウントのクラウド環境を構築します。効果的なクラウド環境があれば、チームは、新しいアカウントを簡単に作成し、作られたアカウントが組織のポリシーに確実に準拠するようにすることができます。一連の整理されたクラウドプロダクトを利用することで、ベストプラクティスを体系化できます。これにより、クラウドの構築のスピードと一貫性を向上させながら、ガバナンスを確保できます。ベストプラクティスのブループリント、発見的および予防的なガードレールを実装します。クラウド環境を既存のエコシステムに統合して、理想的なハイブリッドクラウドのユースケースを実現します。

  アカウント作成ワークフローを自動化し、複数のアカウントを活用することで、セキュリティとガバナンスの要求にこたえます。オンプレミス環境とクラウド環境間および異なるクラウドアカウント間の接続をセットアップします。既存の ID プロバイダー (IdP) とクラウド環境間のフェデレーションを実装し、ユーザーが既存のログイン認証情報を使用して認証できるようにします。ログ記録を一元化し、アカウント横断のセキュリティ監査を確立し、インバンドおよびアウトバウンドのドメインネームシステム (DNS) リゾルバーを作成し、アカウントとガードレールをダッシュボードで可視化します。

  企業の標準および構成管理に合わせて利用するためにクラウドサービスを評価および認定します。セルフサービスでデプロイ可能なプロダクトと利用可能なサービスとして企業標準をパッケージして継続的に改善します。Infrastructure as Code (IaC) を活用して、宣言的な方法で設定を定義します。

- **データエンジニアリング** – 組織全体のデータフローを自動化し、オーケストレーションします。自動化されたデータおよび分析のプラットフォームとパイプラインにより、生産性を向上させ、市場投入までの時間を短縮できます。インフラストラクチャとオペレーション、ソフトウェアエンジニアリング、およびデータ管理で構成された部門横断的なデータエンジニアリングチームを結成します。メタデータを活用して、未加工データを取り込んで最適化されたデータを生成するパイプラインを自動化します。関連するアーキテクチャーガードレール、セキュリティコントロール、モニタリング、ログ記録、アラートを実装して、パイプラインの障害に備えます。一般的なデータ統合パターンを特定し、パイプライン開発の複雑性を取り払った再利用可能なブループリントを構築します。ビジネスアナリストおよびデータサイエンティストにブループリントを共有し、セルフサービスの方法で運用できるようにします。
- **プロビジョニングとオーケストレーション** – エンドユーザーに向けて承認済みのクラウドプロダクトのカタログを作成、管理、配信します。スケーラブルかつ反復可能な方法で一貫したインフラストラクチャの構築を維持する作業は、組織が成長するに従い複雑化します。合理化されたプロビジョニングとオーケストレーションを利用することで、ユーザーが承認済みのクラウドプロダクトのみを迅速にデプロイできるようにしながら、一貫したガバナンスを実現し、コンプライアンス要件を満たすことができます。承認済みのクラウドプロダクトの公開、配信、参照、利用のための一元管理されたセルフサービスポータルを設計して実装します。API やパーソナライズされたポータルを介してクラウドプロダクトにアクセスできるようにします。IT サービス管理 (ITSM、IT service management) のツールに統合し、構成管理データベース (CMDB、configuration management database) に対する更新を自動化します。

- **モダンアプリケーション開発** – Well-Architected フレームワークに基づくクラウドネイティブアプリケーションを構築します。モダンアプリケーション開発手法により、イノベーションに必要なスピードと俊敏性を実現できます。コンテナとサーバーレステクノロジーを使用することで、リソース使用量を最適化し、ゼロからピークの需要まで自動的にスケーリングできます。イベント駆動型のアーキテクチャを活用して、独立したマイクロサービスとして構築することで、アプリケーションを分離することを検討します。すべてのレイヤー、およびアプリケーション開発ライフサイクルの各ステージにセキュリティを実装します。スケールアウトおよびスケールインのプロセスを自動化するか、サーバーレステクノロジーを使用します。既存のアプリケーションをモダナイズすることで、コストを削減し、効率性を向上させ、既存の投資を最大限活用します。リプラットフォーム (独自のコンテナ、データベース、またはメッセージブローカーをマネージドクラウドサービスに移動すること) およびリファクタリング (クラウドネイティブアーキテクチャに合わせてレガシーアプリケーションを再作成すること) を検討します。アーキテクチャでサービスクォータ および物理リソースを考慮して、ワークロードのパフォーマンスや信頼性が悪影響を受けることがないようにします。
- **継続的インテグレーションと継続的デリバリー** – 従来型のソフトウェア開発およびインフラストラクチャ管理プロセスを使用している組織よりも高速にアプリケーションおよびサービスを進化させ、改善します。継続的なインテグレーション、テスト、デプロイとともに DevOps の手法を採用すると、俊敏性が高まり、イノベーションの迅速化、変化する市場への適応の改善、ビジネスの結果を推進する効率の向上を実現できます。継続的インテグレーションと継続的デリバリー (CI/CD) パイプラインを実装します。

継続的インテグレーションの実用最小限のパイプラインから始め、コンポーネントやステージを追加した継続的デリバリーパイプラインに移行します。できるだけ早期に単体テストを作成し、コードを中央リポジトリにプッシュする前に単体テストを実行するように開発者に促します。継続的デリバリーパイプラインにはステージングステップと本番稼働ステップを含め、本番稼働デプロイでは手動による承認を検討します。インプレース、ローリング、イミュータブル、Blue/Green の各デプロイメントなど、複数のデプロイ戦略を検討します。

セキュリティパースペクティブ: コンプライアンスと保証

セキュリティパースペクティブでは、データとクラウドワークロードに対する高い機密性、完全性、可用性を実現できるようにします。次の図に示した 9 つのケイパビリティで構成されています。一般的なステークホルダーとして、CISO、CCO、内部監査のリーダー、セキュリティアーキテクト、セキュリティエンジニアが挙げられます。

AWS CAF のセキュリティパースペクティブのケイパビリティ

- **セキュリティ統制** – セキュリティの役割、責務、説明責任、ポリシー、プロセス、手順を策定、維持し、効果的に伝達します。セキュリティプログラムの効果が発揮されるようにするには、明確な説明責任系統を確保することが重要です。アセット、セキュリティリスク、および業界/組織に適用されるコンプライアンスの要件を理解することで、セキュリティの取り組みを優先順位付けすることができます。継続的な指示と助言を提供することで、チームが迅速に移行できるようにして、変革を加速できます。
  クラウド「内」のセキュリティに対する責任を理解します。関連するステークホルダー、アセット、および情報連携のインベントリ作成、分類、優先順位付けを行います。業界/組織に適用される法律、規則、規制、標準/フレームワークを特定します。組織に対する年次リスク評価を実施します。リスク評価は、特定されたリスクや脆弱性が組織に影響する可能性および影響の大きさを判別するのに役立ちます。特定されたセキュリティの役割と責任に十分なリソースを割り当てます。コンプライアンス要件および組織のリスク許容度に合わせて、セキュリティのポリシー、プロセス、手順、およびコントロールを策定し、変化するリスクおよび要件に応じて、継続的に更新します。
- **セキュリティ保証** – セキュリティとプライバシーに関するプログラムの有効性を継続的にモニタリング、評価、管理、改善します。自社の組織、および顧客は、規制要件を満たすようコントロールされていること、ビジネス目標とリスク許容度に合わせてセキュリティとプライバシーのリスクを効果的かつ効率的に管理できることについて、信頼と確信を求めています。
  コントロールを文書化して包括的なコントロールフレームワークを作成し、該当する目標を満たす、実証可能なセキュリティとプライバシーのコントロールを確立します。クラウドベンダーが提供する監査レポート、コンプライアンスの認定や証明をレビューし、クラウドベンダーが実装している制御の仕組みが、どのように検証され、効果的に運用されているのかを理解します。

継続的に環境をモニタリングおよび評価することで、コントロールの運用上の有効性を確認し、規制および業界の標準に対する準拠を示します。セキュリティのポリシー、プロセス、手順、コントロール、およびレコードを確認し、必要に応じて主要な人物にインタビューします。

- **ID とアクセス管理** – ID とアクセス許可を大規模に管理します。AWS 上で ID を作成するか自社の ID ソースに接続して、ユーザーに必要な権限を付与します。それにより、ユーザーは AWS リソースや統合されたアプリケーションに対してサインイン、アクセス、構築、あるいはオーケストレーションすることができます。効果的な ID とアクセス管理を提供すると、適切な権限を持つ人とマシンが適切な条件の下で適切なリソースにアクセスできることを検証できます。

  AWS Well Architected フレームワークでは、関連する概念、設計原則、ID を管理するためのアーキテクチャのベストプラクティスについて説明しています。これには、一元化された ID プロバイダーを利用すること、大規模なきめ細かいアクセスおよび一時的な認証情報のためのユーザーグループと属性の活用、多要素認証 (MFA) などの強力なサインインメカニズムの使用などがあります。 AWS およびワークロードに対する人とマシンの ID によるアクセスをコントロールするために、特定の条件の下で特定のリソースに対する特定のサービスアクションのアクセス許可を設定します。最小権限の原則を使用し、アクセス許可の境界を設定し、サービスコントロールポリシーを使用して、環境やユーザー基盤が大きくなっても適切なエンティティが適切なリソースにアクセスできるようにします。また、属性ベースのアクセスコントロール (ABAC) を付与することで、ポリシーをスケーリングできるようにします。さらに、必要な保護がポリシーで得られていることを継続的に検証します。

- **脅威検出** – セキュリティの設定ミス、脅威、予期しない挙動を理解し、特定します。セキュリティの脅威の理解を深めることで、保護対策を優先順位付けできます。効果的な脅威検出により、より迅速に脅威に対応し、セキュリティインシデントから学ぶことができます。戦術、運用、戦略的インテリジェンスの目標および全体的な手法について合意します。関連性の高いデータソースのマイニング、データの処理と分析、インサイトの周知と実用化を行います。
  環境内で広範囲にモニタリングをデプロイし、必要不可欠な情報を収集し、任意の箇所に特定のタイプのトランザクションを追跡します。ネットワークトラフィック、オペレーティングシステム、アプリケーション、データベース、エンドポイントデバイスなどの複数のイベントソースからのモニタリングデータを相関付け、堅牢なセキュリティ体制を整え、可視性を向上させます。おとり環境 (例えば、ハニーポット) を活用して、不正なユーザー行動パターンを理解することを検討します。
- **脆弱性管理** – セキュリティの脆弱性を継続的に特定、分類、修正、軽減します。既存のシステムの変更や新規システムの追加でも脆弱性が生じることがあります。定期的に脆弱性をスキャンして、新しい脅威から保護します。脆弱性スキャナーとエンドポイントエージェントを利用して、システムを既知の脆弱性に関連付けます。脆弱性リスクに基づいて、修復アクションを優先順位付けします。修復アクションを適用し、関連するステークホルダーに報告します。レッドチームや侵入テストを活用して、システムアーキテクチャ内の脆弱性を特定します。必要に応じて、クラウドプロバイダーから事前の許可を得ます。

- **インフラストラクチャ保護** – ワークロード内のシステムとサービスが、意図しないアクセス、不正アクセス、潜在的な脆弱性から保護されていることを検証します。意図しないアクセス、不正アクセス、潜在的な脆弱性からインフラストラクチャを保護することで、クラウドでのセキュリティ体制を向上することができます。多層防御を活用して、データとシステムを保護するための一連の防御メカニズムを階層化します。

  ネットワークレイヤーを作成し、インターネットアクセスが不要なワークロードはプライベートサブネットに配置します。セキュリティグループ、ネットワークアクセスコントロールリスト、およびネットワークファイアウォールを使用して、トラフィックをコントロールします。システムとデータの価値に応じて、システムとデータにゼロトラストを適用します。クラウドリソースへのプライベート接続では、バーチャルプライベートクラウド (VPC) のエンドポイントを活用します。例えば、ウェブアプリケーションファイアウォールやネットワークファイアウォールを使用して、各レイヤーでトラフィックを検査およびフィルタリングします。強化されたオペレーティングシステムイメージを使用し、オンプレミスからエッジロケーションまですべてのハイブリッドクラウドインフラストラクチャを物理的に保護します。
- **データ保護** – データの可視性と制御、および組織におけるデータのアクセス方法や使用方法を維持管理します。意図しないアクセス、不正アクセス、潜在的な脆弱性からデータを保護することは、セキュリティプログラムの主要な目的の 1 つです。適切な保護および保持の管理方法を決定できるように、重要度と機密性に基づいてデータを分類します (例えば、個人を特定できる情報)。データ保護コントロールおよびライフサイクル管理ポリシーを定義します。保管中のデータおよび伝送中のデータをすべて暗号化し、機密データを別アカウントに保存します。機械学習を活用して、機密データを自動的に検出、分類、保護します。

- **アプリケーションセキュリティ** – ソフトウェア開発プロセスの中でセキュリティに関する脆弱性を検出して対処します。アプリケーションのコーディングフェーズでセキュリティの欠陥を検出して修復すると、時間、労力、コストを削減でき、本番稼働に移行する際にセキュリティ体制に自信を持てます。コードおよび依存関係内の脆弱性をスキャンしてパッチを適用し、新しい脅威から保護できるようにします。開発およびオペレーションのプロセスとツール全体でセキュリティ関連のタスクを自動化することで、人手による介入の必要性を最小限に抑えます。静的コード分析ツールを使用して、一般的なセキュリティの問題を特定します。
- **インシデント対応** – セキュリティインシデントに効果的に対応することで潜在的な損害を低減します。セキュリティインシデントに迅速かつ効果的に、一貫して対応することで、潜在的な損害を低減できます。クラウドテクノロジーとその使い方について、セキュリティオペレーションとインシデント対応のチームに教育します。ランブックを策定し、インシデント対応メカニズムのライブラリを作成します。主要ステークホルダーを巻き込んで、選択したセキュリティ対策がより広範な組織におよぼす影響を深く理解します。

  セキュリティインシデントをシミュレートし、机上演習やゲームデーによってインシデント対応の訓練を行います。シミュレーションの結果に基づいて反復することで、対応体制の規模を改善し、価値実現までの時間を短縮し、さらにリスクを低減させます。事後分析を実施して、標準化されたメカニズムを活用して根本原因を特定して解決することで、セキュリティインシデントから学びます。

オペレーションパースペクティブ: 正常性と可用性

オペレーションパースペクティブでは、ビジネスステークホルダーと合意したレベルでクラウドサービスを提供できるようにすることにフォーカスします。オペレーションを自動化および最適化すると、ワークロードの信頼性を向上させながら、効果的にスケーリングできるようになります。このパースペクティブは、次の図に示した 9 つのケイパビリティで構成されています。一般的なステークホルダーとして、インフラストラクチャーとオペレーションのリーダー、サイトリライアビリティエンジニア、IT サービスマネージャーが挙げられます。

AWS CAF のオペレーションパースペクティブのケイパビリティ

- **オブザーバビリティ** – インフラストラクチャとアプリケーションのデータから行動につなげられるインサイトを得ます。クラウドのスピードと規模で運用している場合、発生した問題を (理想的にはカスタマーエクスペリエンスが損なわれる前に) 検出できる必要があります。ワークロードの内部状態および正常性を理解するために必要なテレメトリ (ログ、メトリクス、トレース) を策定します。アプリケーションエンドポイントをモニタリングし、エンドユーザーへの影響を評価して、測定値がしきい値を超えた場合にアラートを生成します。シンセティック監視を使用して Canary (スケジュールに従って実行される設定可能なスクリプト) を作成し、エンドポイントと API をモニタリングします。トレースを実装して、アプリケーション全体を通過するリクエストを追跡し、ボトルネックやパフォーマンスの問題を特定します。メトリクスとログを使用して、リソース、サーバー、データベース、およびネットワークに対するインサイトを得ます。時系列データのリアルタイム分析をセットアップし、パフォーマンスへの影響の原因を理解します。単一のダッシュボードでデータを一元化することで、ワークロードとそのパフォーマンスに関する重要な情報の統合ビューが得られます。
- **イベント管理 (AIOps)** – イベントを検出し、その潜在的な影響を評価し、適切なコントロールアクションを決定します。ノイズのフィルタリング、優先されるイベントへのフォーカス、差し迫ったリソース枯渇の予測、アラートとインシデントの自動生成、可能性の高い原因と修復アクションの特定を行うことで、インシデントの検出と対応時間を改善できます。イベントストアパターンを確立し、機械学習 (AIOps) を活用することで、イベントの相関付け、異常検出、原因判別を自動化します。インシデント管理システムとプロセスなど、クラウドサービスおよびサードパーティーツールと統合します。イベントへの対応を自動化することで、手動プロセスに伴うエラーを削減し、速やかに一貫した対応を行えるようにします。

- **インシデントおよび問題管理** – サービスオペレーションを迅速に回復し、ビジネスへの悪影響を最小限に抑えます。クラウドを導入すると、サービスの問題およびアプリケーションの正常性の問題への対応のプロセスを高度に自動化できるため、サービスのアップタイムが向上します。さらに分散した運用モデルに移行すると、関連するチーム、ツール、プロセス間の相互作用を合理化することで、重要なインシデントや複雑なインシデントの解決を促進できます。ランブックにエスカレーションパスを定義し、エスカレーションをトリガーする条件およびエスカレーションの手順を記載します。
  インシデント対応のゲームデーの訓練を行い、得られた教訓をランブックに取り込みます。インシデントパターンを特定して、問題と是正措置を判別します。チャットボットやコラボレーションツールを活用して、オペレーションチーム、ツール、ワークフローを連携させます。事後分析を活用して、インシデントの要因を特定し、対応するアクションプランを策定します。
- **変更およびリリース管理** – 本番稼働環境に対するリスクを最小限に抑えながら、ワークロードを導入して変更します。従来型のリリース管理は、デプロイが遅く、ロールバックしにくい複雑なプロセスです。クラウドの導入により、CI/CD 手法を活用して、リリースとロールバックを迅速に管理できるようになります。クラウドの俊敏性に合った自動化された承認ワークフローを実現する変更プロセスを確立します。デプロイ管理システムを使用して、変更を追跡および実装します。切り戻し可能な小規模な変更を高頻度に行うことで、ひとつの変更の範囲を小さくします。すべてのライフサイクルステージで変更をテストして結果を検証することで、デプロイ失敗のリスクと影響を最小限に抑えます。変更がうまくいかなかった場合、変更前の健全な状態へのロールバックを自動化することで、復旧時間を最小限に抑え、手動プロセスに伴うエラーを削減します。

- **性能とキャパシティ管理** – ワークロードパフォーマンスをモニタリングし、キャパシティが現在と将来の需要を確実に満たすようにします。クラウドのキャパシティはほぼ無制限ですが、サービスクォータ、キャパシティ予約、およびリソース制約のため、ワークロードの実際のキャパシティは制限されます。そのような制約を理解して、効果的に管理する必要があります。主要ステークホルダーを特定し、目的、スコープ、目標、およびメトリクスについて合意します。パフォーマンスデータを収集して処理し、定期的に目標に照らしてパフォーマンスを確認して報告します。定期的に新しいテクノロジーを評価して、パフォーマンスを向上させ、必要に応じて目標やメトリクスを変更することを提案します。ワークロードの使用量をモニタリングし、将来比較するためにベースラインを策定し、必要な場合にキャパシティを拡張するしきい値を特定します。経時的に需要を分析し、キャパシティが季節的トレンドや変動する運用状態に対応できるようにします。
- **構成管理** – すべてのクラウドワークロード、その関係、経時的な設定の変更の正確かつ完全な履歴を記録します。クラウドリソースの生成は動的かつ仮想的な性質のため、設定のドリフトが生じることがあります。ビジネス属性とクラウドリソースを紐づけするタグ付けスキーマを定義して適用し、タグを活用して、技術、ビジネス、セキュリティの側面に沿ってリソースを整理します。必須のタグを指定し、ポリシーを利用してコンプライアンスを適用します。リソースのプロビジョニングやライフサイクル管理で Infrastructure as Code (IaC) や構成管理ツールを活用します。設定のベースラインを確立し、バージョン管理を利用してベースラインを保守します。

- **パッチ管理** – ソフトウェアの更新を体系的に配信し、適用します。ソフトウェアの更新では、新たなセキュリティ脆弱性に対処し、バグを修正し、新機能を導入します。体系的なパッチ管理のアプローチにより、本番稼働環境へのリスクを最小限に抑えながら、最新の更新によるメリットを享受できます。**重要な更新**は指定したメンテナンスウィンドウで、**緊急のセキュリティアップデート**はできる限り早急に適用します。次回のアップデート内容を前もってユーザーに通知し、代替の回避策がある場合は、パッチ適用を延期することも認めます。本番環境に展開する前に、マシンイメージを更新してパッチをテストします。パッチ適用中も稼働を継続できるよう、アベイラビリティーゾーン (AZ) および環境ごとに異なるメンテナンスウィンドウを設定することを検討します。定期的にパッチ適用の準拠を確認し、準拠していないチームには必要な更新を適用するようにアラートを出します。
- **可用性および継続性管理** – ビジネスクリティカルな情報、アプリケーション、サービスの可用性を確保します。クラウド対応のバックアップソリューションを構築するには、既存のテクノロジーへの投資、復旧目標、使用可能なリソースを注意深く考慮する必要があります。災害やセキュリティインシデントの発生後に適時に復旧することで、システムの可用性とビジネスの継続性を維持するのに役立ちます。定義したスケジュールに従って、データおよびドキュメントをバックアップします。

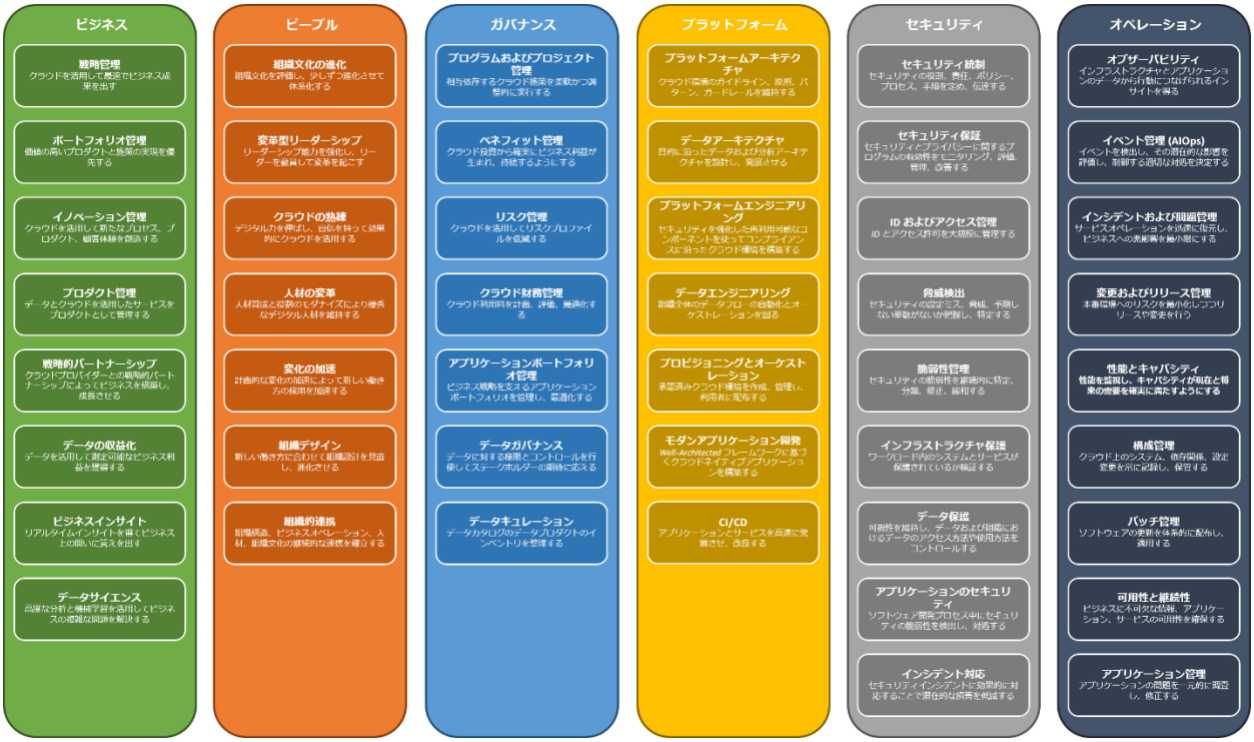
  ビジネス継続性計画のサブセットとして災害復旧計画を策定します。ワークロードごとに各種災害シナリオの脅威、リスク、影響、コストを特定し、それぞれ目標復旧時間 (RTO) と目標復旧時点 (RPO) を定義します。マルチ AZ またはマルチリージョンアーキテクチャを活用して、定義した災害復旧戦略を実装します。カオスエンジニアリングを活用して、制御された実験によってレジリエンシーとパフォーマンスを向上させることを検討します。定期的に計画を確認してテストし、得られた教訓に基づいてアプローチを調整します。

- **アプリケーション管理** – アプリケーションの問題を一元的に調査し、修正します。アプリケーションデータを単一のマネジメントコンソールに集約することで、複数の管理ツール間でコンテキストを切り替える必要が削減されるため、運用の監視が簡素化し、アプリケーションの問題の修復が促進されます。アプリケーションポートフォリオ管理や CMDB などの他の運用管理システムと統合し、アプリケーションコンポーネントやリソースの検出を自動化し、アプリケーションデータを単一のマネジメントコンソールに集約します。ソフトウェアコンポーネントとインフラストラクチャリソースを組み込み、開発、ステージング、本番稼働などの各種環境を定めます。運用の問題をさらに迅速に一貫して修復するために、ランブックの自動化を検討します。

まとめ

テクノロジーのイノベーションが今後も加速していく中、継続的デジタルトランスフォーメーションの必要性がかつてないほど高まっています。AWS CAF は、AWS の経験とベストプラクティスを活用して、AWS を革新的に利用してビジネス成果を加速できるようにします。AWS CAF を使用することで、トランスフォーメーションの機会を特定して優先順位付けし、クラウド活用の成熟度を評価して改善し、トランスフォーメーションロードマップを反復的に進化させることができます。

付録: AWS CAF のケイパビリティポスター



作成者

- AWS CAF、ワールドワイドリード、Saša Baškarada 博士著(多数の AWS のサブジェクトマターエキスパートから助言を受けました)

参考資料

詳細については、以下をご参照ください。

- AWS アーキテクチャセンター
- AWS の導入事例
- AWS 全般のリファレンス
- AWS の用語集

- AWS ナレッジセンター
- AWS 規範的ガイダンス
- AWS クイックスタート
- AWS セキュリティドキュメント
- AWS ソリューションライブラリ
- AWS トレーニングと認定
- AWS Well-Architected
- AWS ホワイトペーパーとガイド
- AWS の使用開始方法
- Amazon Web Services の概要

ドキュメントの改訂

日付	説明
2021 年 11 月 22 日	バージョン 3.0 – ケイパビリティを更新および拡張。トランスフォーメーションドメインおよびジャーニーフェーズを追加。
2017 年 2 月	バージョン 2.0 – パースペクティブおよびケイパビリティの構造を変更。
2015 年 2 月	バージョン 1.0 – 初版。