AWS ホワイトペーパー

# AWS クラウド導入フレームワークの概要

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS クラウド導入フレームワークの概要: AWS ホワイトペーパー

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、Amazon のものではない製品またはサービスと関連付けてはならず、また、お客様に混乱を招くような形や Amazon の信用を傷つけたり失わせたりする形で使用することはできません。Amazon が所有しない商標はすべてそれぞれの所有者に所属します。所有者は必ずしも Amazon と提携していたり、関連しているわけではありません。また、Amazon 後援を受けているとはかぎりません。

# Table of Contents

要約 ..... 1
要約 ..... 1
はじめに ..... 2
ビジネスの成果の加速 ..... 3
基本的な機能 ..... 5
クラウドトランスフォーメーションジャーニー ..... 7
ビジネスのパースペクティブ ..... 10
人員のパースペクティブ ..... 13
ガバナンスのパースペクティブ ..... 17
プラットフォームのパースペクティブ ..... 21
セキュリティのパースペクティブ ..... 24
オペレーションのパースペクティブ ..... 28
まとめ ..... 32
付録: AWS CAF の機能の図 ..... 33
寄稿者 ..... 34
その他の資料 ..... 35
改訂履歴 ..... 36
注意 ..... 37

# AWS クラウド導入フレームワークの概要

公開日: 2021 年 11 月 22 日 (改訂履歴)

## 要約

デジタルテクノロジーの急速な拡大により、市場セグメントや業界は大きく変化し続けています。アマゾン ウェブ サービス (AWS) を導入することにより、変化するビジネス状況や進化する顧客のニーズに対応できるよう、組織を変革することができます。世界で最も包括的に広く導入されているクラウドプラットフォームである AWS は、コストの削減、ビジネスリスクの低減、オペレーションの効率の向上、俊敏性の向上、イノベーションの迅速化、新しい収益源の創出、顧客や従業員のエクスペリエンスの改革を支援します。

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、AWS の革新的な利用によるデジタルトランスフォーメーションとビジネスの成果の加速を支援します。AWS CAF を使用して、トランスフォーメーションの機会を識別して優先順位を付け、クラウドへの対応を評価して改善し、トランスフォーメーションのロードマップを反復的に進化させます。

# はじめに

デジタルテクノロジーの急速な拡大により、さまざまな市場セグメントや業界で変化が加速し、競争が激化しています。特定の競争優位性を維持することがますます難しくなっているため、企業はさらに短い期間での改革を迫られています。例えば、S&P 500 の企業の 50% は、今後 10 年間で入れ替わると予測されています。

同様に、民間人の期待や行動の変化は、公共機関にデジタルサービスの提供を改善するようプレッシャーを与えています。世界中の組織がデジタルトランスフォーメーションを進めており、デジタルテクノロジーを活用して組織の変革を推進し、変化する市場に適応し、顧客を満足させ、ビジネスの成果を加速させています。

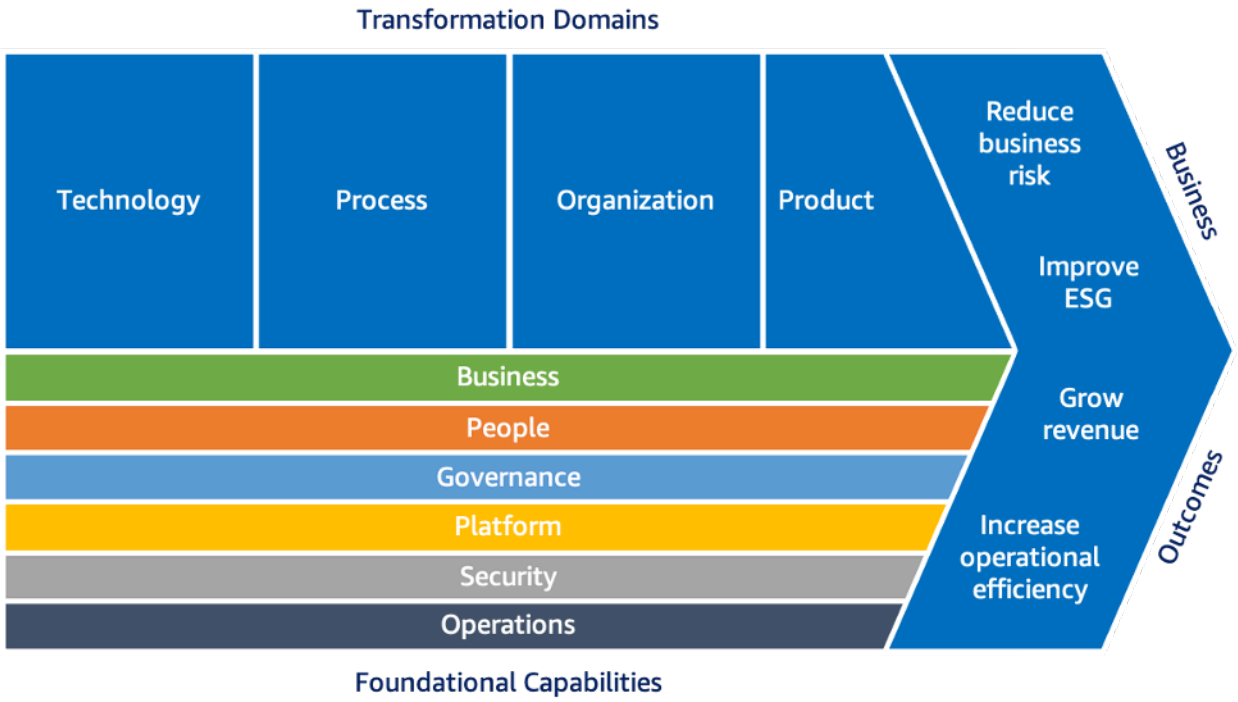
急成長中のスタートアップ企業、大企業、主要な政府機関など、数百万の AWS のお客様が AWS を活用してレガシーのワークロードの移行とモダナイズを行い、データ駆動型となり、ビジネスプロセスをデジタル化および最適化し、オペレーションモデルとビジネスモデルを改革しています。クラウドを活用したデジタルトランスフォーメーション (クラウドトランスフォーメーション) により、コストの削減、ビジネスリスクの低減、オペレーションの効率の向上、俊敏性の向上、イノベーションの迅速化、新しい収益源の創出、顧客や従業員のエクスペリエンスの改善など、ビジネスの成果を向上させることが可能になっています。

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 (クラウドへの対応) は、組織の一連の基本的な機能によって支えられています。AWS CAF はこれらの機能を明らかにし、世界中の何千もの組織が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ために活用してきた規範的ガイダンスを提供します。

AWS と AWS パートナーネットワークは、取り組みの各段階でお客様を支援するツールやサービスを提供します。AWS Professional Services は、クラウドトランスフォーメーションに関連する特定の成果を実現可能な AWS CAF と連携した一連のサービスによって支援を提供するエキスパートのグローバルチームです。

# 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の成果の加速

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は、一連の基本的な機能によって実現されるクラウドを活用した組織の変革 (トランスフォーメーション) により、ビジネスの成果が加速することを示しています。このトランスフォーメーションの分野は、テクノロジーからプロセス、プロセスから組織、組織から製品の順にトランスフォーメーションが可能になるバリューチェーンを表しています。主なビジネスの成果には、ビジネスリスクの低減、ESG (環境、社会、ガバナンス) のパフォーマンスの向上、収益の増加、オペレーションの効率の向上などがあります。




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

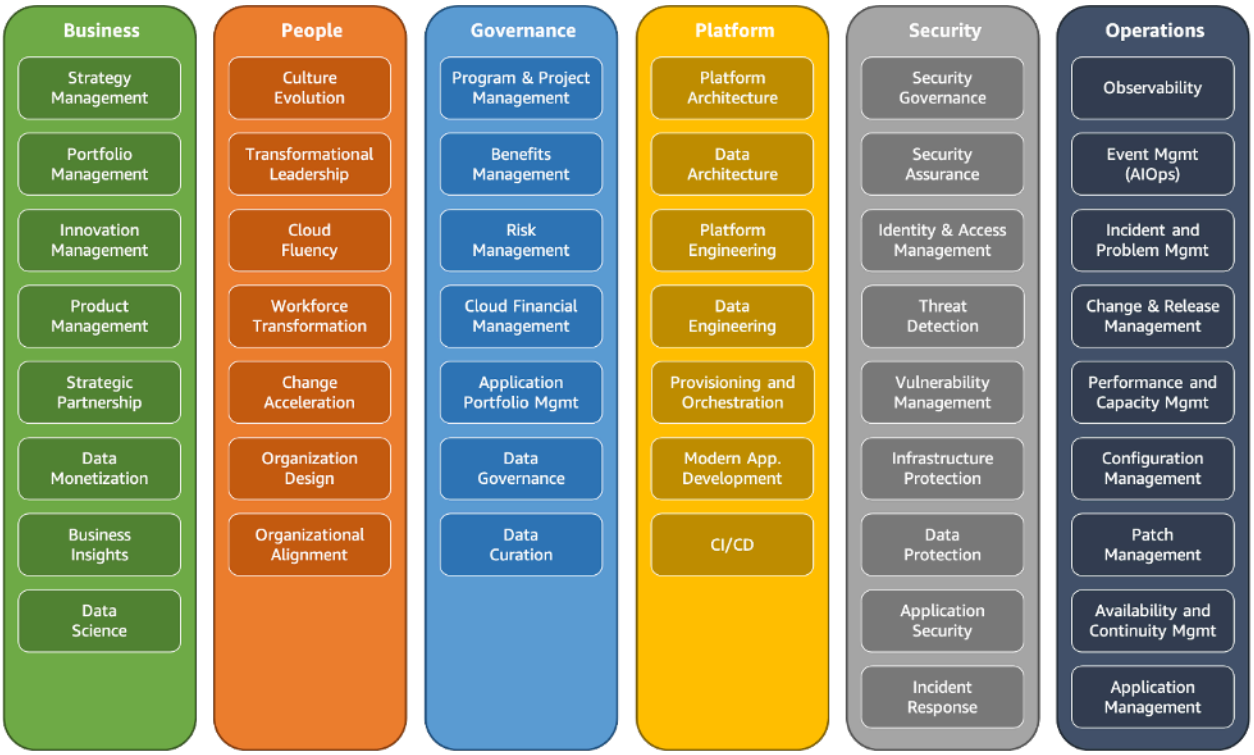
- テクノロジーのトランスフォーメーションでは、クラウドを使用して、レガシーのインフラストラクチャ、アプリケーション、データおよび分析プラットフォームを移行およびモダナイズすることに重点を置いています。Cloud Value Benchmarking によると、オンプレミスから AWS への移行により、ユーザー 1 人あたりのコストが 27% 削減され、管理者あたりの VM 管理数が 58% 増加し、ダウンタイムが 57% 減少し、セキュリティイベントが 34% 減少しています。
- プロセスのトランスフォーメーションでは、ビジネスオペレーションのデジタル化、自動化、最適化に重点を置いています。これには、新しいデータおよび分析プラットフォームを活用して実用的なインサイトを得ることや、機械学習 (ML) を利用して、カスタマーサービスエクスペリエン

ス、従業員の生産性と意思決定、ビジネス予測、不正行為の検出と防止、産業オペレーションなどを改善することが含まれます。これにより、オペレーションコストを削減し、従業員や顧客のエクスペリエンスを改善するとともに、オペレーションの効率を向上させることができます。

- 組織のトランスフォーメーションでは、ビジネスチームとテクノロジーチームがどのように協力して顧客価値を創出し、戦略的意図を満たすかというオペレーションモデルの再考に重点を置いています。製品や価値のストリームを中心にチームを編成し、アジャイル手法を活用して迅速に反復および進化させることで、対応力を高め、より顧客中心になることができます。
- 製品のトランスフォーメーションでは、新しい価値提案 (製品、サービス) と収益モデルを作成することで、ビジネスモデルを再考することに重点を置いています。これにより、新規顧客の獲得や新しい市場セグメントへの参入に役立てることができます。Cloud Value Benchmarking によると、AWS を採用することで、新機能やアプリケーションの市場投入までの時間が 37% 短縮され、コードのデプロイ頻度が 342% 増加し、新しいコードのデプロイにかかる時間が 38% 短縮されています。

# 基本的な機能

前のセクションで説明したトランスフォーメーションの各分野は、次の図に示す一連の基本的な機能によって実現されます。機能とは、特定の成果を実現するために、リソース (人員、テクノロジー、その他の有形無形のアセット) をデプロイするプロセスを活用する組織の能力です。AWS CAF の機能は、クラウドへの対応 (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を提供します。AWS CAF は、その機能をビジネス、人員、ガバナンス、プラットフォーム、セキュリティ、オペレーションの 6 つのパースペクティブでグループ化しています。各パースペクティブは、機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において担当または管理する一連の機能で構成されています。




AWS CAF のパースペクティブと基本的な機能

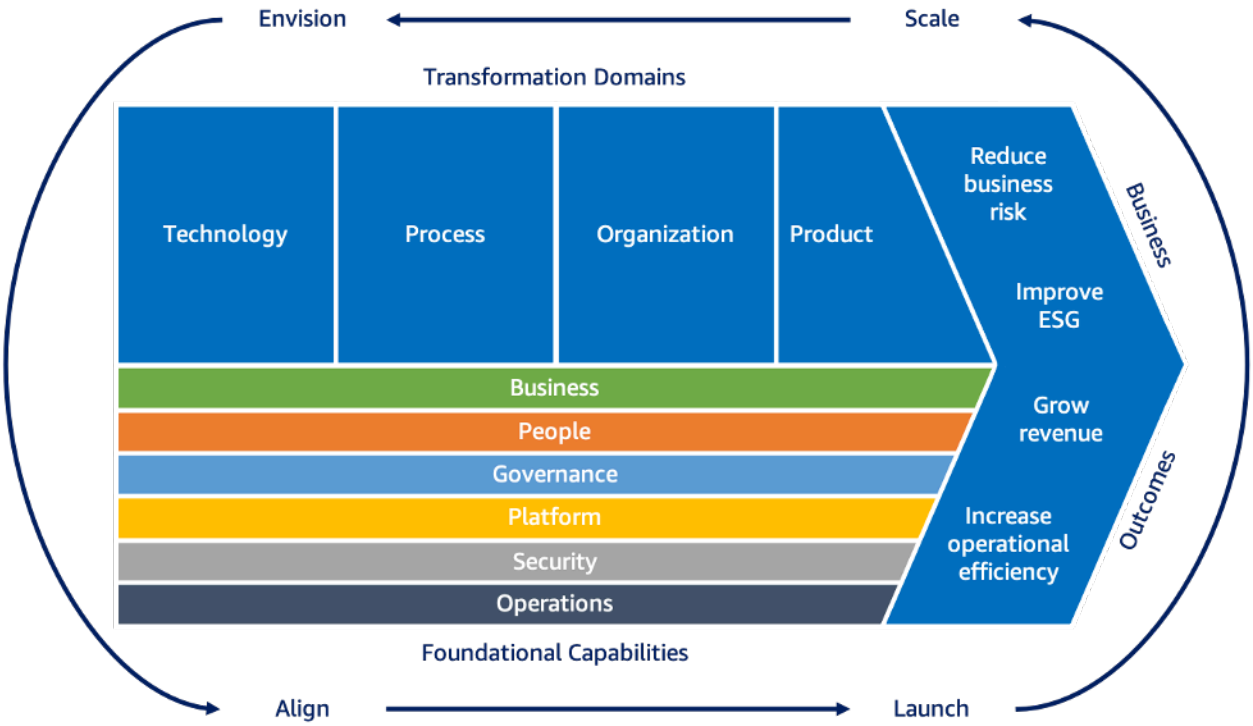
- ビジネスのパースペクティブでは、クラウドへの投資がデジタルトランスフォーメーションの成功とビジネスの成果を確実に加速させるよう支援します。一般的なステークホルダーとしては、最高経営責任者 (CEO)、最高財務責任者 (CFO)、最高執行責任者 (COO)、最高情報責任者 (CIO)、最高技術責任者 (CTO) などが挙げられます。
- 人員のパースペクティブでは、テクノロジーとビジネスの架け橋となり、クラウドジャーニーを加速させ、文化、組織構造、リーダーシップ、ワークフォースに焦点を当てながら、継続的に成長、

学習し、変化が当たり前になるような文化へと組織がより迅速に進化できるようにします。一般的なステークホルダーとしては、CIO、COO、CTO、クラウドディレクター、複数部門にわたるリーダー、エンタープライズ全体のリーダーなどが挙げられます。

- ガバナンスのパースペクティブでは、組織の利益を最大化し、トランスフォーメーションに関連するリスクを最小限に抑えながら、クラウドの取り組みをオーケストレートすることを支援します。一般的なステークホルダーとしては、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) などが挙げられます。
- プラットフォームのパースペクティブでは、エンタープライズグレードのスケーラブル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導入を支援します。一般的なステークホルダーとしては、CTO、テクノロジーリーダー、アーキテクト、エンジニアなどが挙げられます。
- セキュリティのパースペクティブでは、データやクラウドワークロードの機密性、完全性、可用性の実現を支援します。一般的なステークホルダーには、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、セキュリティアーキテクトやエンジニアなどが挙げられます。
- オペレーションのパースペクティブでは、ビジネスのニーズを満たすレベルでクラウドサービスを確実に提供することを支援します。一般的なステークホルダーとしては、インフラストラクチャおよびオペレーションのリーダー、サイト信頼性エンジニア、IT サービスマネージャーなどが挙げられます。

# 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によって異なります。トランスフォーメーションを成功させるには、目標とする状態を定め、クラウドへの対応を把握し、アジャイル手法を採用してギャップを埋める必要があります。トランスフォーメーションを段階的に行うことで、広範な予測を行う必要性を最小限に抑えつつ、価値を迅速に実現することができます。反復的なアプローチを採用することで、経験から知見を得つつ、推進力を維持し、ロードマップを進化させることができます。AWS CAF では、次の図に示す 4 つの反復的かつ段階的なクラウドトランスフォーメーションフェーズを推奨しています。



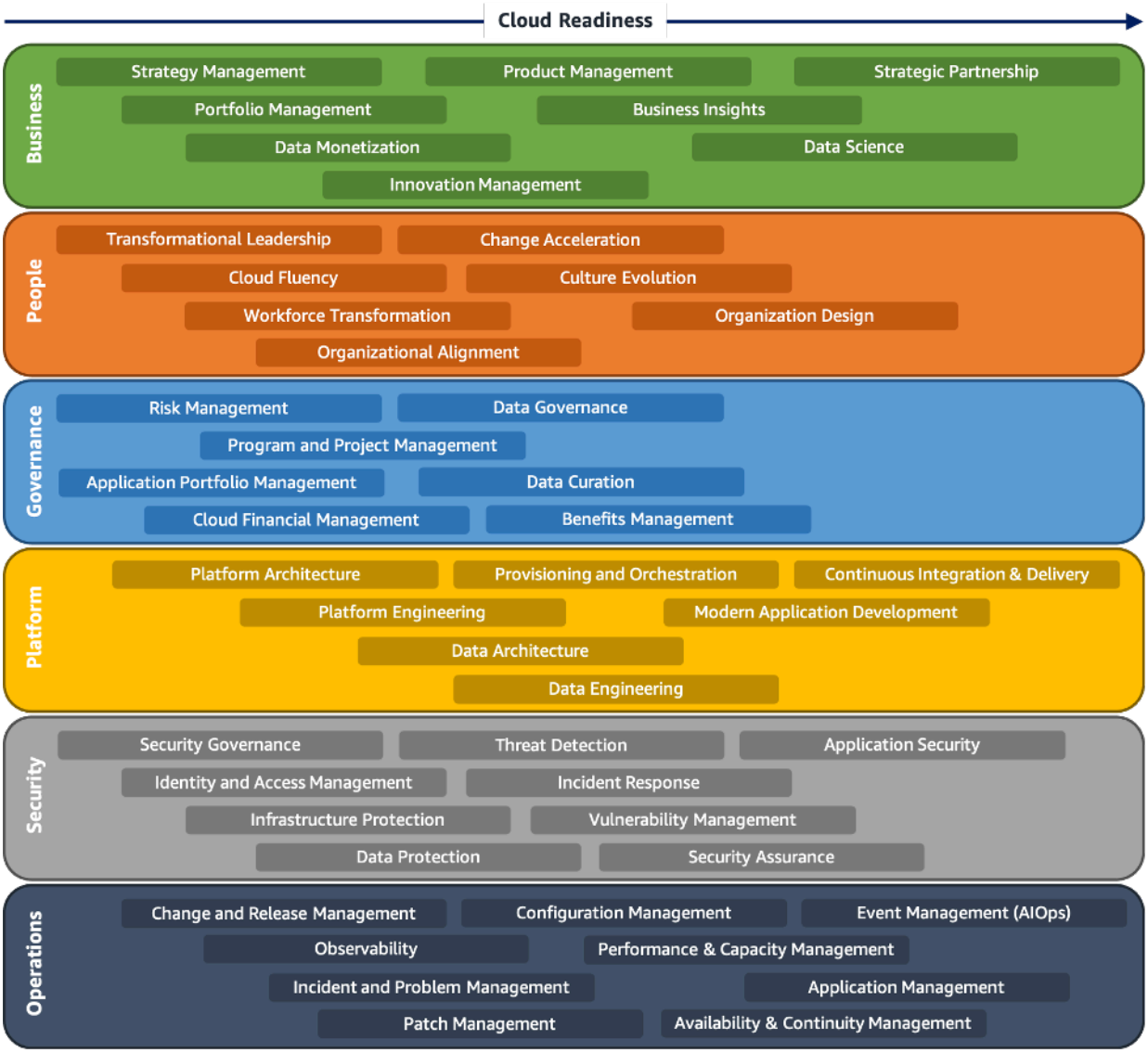

クラウドトランスフォーメーションジャーニー

- 構想フェーズでは、クラウドがビジネスの成果を加速するためにどのように役立つかを示すことに重点を置いています。これは、戦略的なビジネス目標に従って、トランスフォーメーションの 4 つの各分野でトランスフォーメーションの機会を識別し、優先順位を付けることによって行います。トランスフォーメーションの取り組みを主要なステークホルダー (変革に影響を与え、推進できる上級役職者) や測定可能なビジネスの成果と関連付けることで、トランスフォーメーションジャーニーで価値を実現することができます。
- 連携フェーズでは、AWS CAF の 6 つのパースペクティブの機能のギャップを識別し、組織間の依存関係を特定して、ステークホルダーの懸念や課題を明らかにすることに重点を置いています。こ

れにより、クラウドへの対応を改善するための戦略を策定し、ステークホルダーの連携を確実にして、関連する組織の変革管理活動を促進することができます。

- ローンチフェーズでは、本番環境でのパイロットのイニシアチブをとり、段階的にビジネス価値を示すことに重点を置いています。パイロットはインパクトの強いものである必要があり、成功すれば今後の方向性に影響を与えることができます。パイロットから得られた知見は、本番環境に完全にスケールする前にアプローチを調整するために役立ちます。
- スケールフェーズでは、本番環境でのパイロットとビジネス価値を必要な規模に拡大して、クラウドへの投資によるビジネス上の利益を実現および持続させることに重点を置いています。

基本的な機能のすべてに一度に取り組む必要はありません。クラウドトランスフォーメーションジャーニーの中で、基本的な機能を進化させ、クラウドへの対応を進めます。次の図に示す推奨されている順序を、特定のニーズに合わせて調整することを検討します。



## AWS CAF のパースペクティブと基本的な機能の進化

以降のセクションでは、AWS CAF の 6 つのパースペクティブと基本的な機能のそれぞれについて詳しく説明します。

# ビジネスのパースペクティブ: 戦略と成果

ビジネスのパースペクティブでは、クラウドへの投資がデジタルトランスフォーメーションの成功とビジネスの成果を確実に加速させることに重点を置いています。これは、次の図に示す 8 つの機能で構成されています。一般的なステークホルダーとしては、CEO、CFO、COO、CIO、CTO などが挙げられます。

AWS CAF のビジネスのパースペクティブの機能

- 戦略管理 – クラウドを活用して、ビジネスの成果を加速させます。クラウドが長期的なビジネス目標をどのようにサポートおよび実現できるかを検討します。技術的負債をなくし、クラウドを活用してテクノロジーとビジネスオペレーションを最適化する機会を識別します。新しいクラウド対応の価値提案と収益モデルを検討します。新規または改善されたクラウド対応の製品やサービスを新規顧客の獲得や新しい市場セグメントへの参入に役立てる方法を検討します。技術開発やビジネス環境の変化に応じて、戦略目標に優先順位を付け、戦略を長期的に進化させます。
- ポートフォリオ管理 – 戦略的意図、オペレーション効率、提供能力に従って、クラウド製品と取り組みに優先順位を付けます。適切なクラウド製品と取り組みを適切なタイミングで提供することは、戦略をオペレーション可能にし、ビジネスの成果を加速させるために役立ちます。自動検出ツールと、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 (7 つの R) 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だけでなく、低リスク (実証済み) の機会と高リスク (実験的) の機会を考慮して、クラウドポートフォリオのバランスを調整します。移行、モダナイゼーション、イノベーションの取り組みを含め、財務上のメリット (コストの削減や収益の増加) と財務上以外

のメリット (顧客や従業員のエクスペリエンスの向上など) を検討します。リソース、財務、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。価値を実現する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すか、継続的プランニング戦略を採用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、新規または既存のプロセス、製品、エクスペリエンスの開発や改善を行います。クラウドでは、リソースのプロビジョニングやシャットダウンをすぐに行えるため、価値を実現するまでの時間を短縮し、イノベーションにかかるコストとリスクを削減できます。クラウドの導入によるビジネスの俊敏性の向上の可能性を最大限に引き出すために、既存の製品、プロセス、エクスペリエンスの最適化に重点を置いた段階的なイノベーションの取り組みと、新しいビジネスモデルの実現に重点を置いた破壊的なイノベーションの取り組みを組み合わせたイノベーション戦略を策定します。戦略的な優先順位に従ってアイデアを出して選択する仕組みを作り、イノベーションのパイロットの成功を拡大するエンドツーエンドのプロセスを開発します。
- 製品管理 – 内部および外部の顧客に製品としてライフサイクル全体で繰り返し価値を提供するデータおよびクラウド対応製品を管理します。 データおよびクラウド対応の製品を中心にチームを編成することで、俊敏性を高め、より顧客中心になることができます。
  - ビジネス戦略をサポートするバランスのとれた製品ポートフォリオを作成します。
  - 内部および外部の顧客のニーズに応える小規模で力強い横断的なチームを作ります。
  - 製品所有者を識別し、カスタマージャーニーを理解し、製品ロードマップを定義および作成して、製品ライフサイクル全体と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手法を活用して、反復と進化を迅速に行います。
  - 明確に定義されたインターフェイスにより、製品チーム間の依存関係を減らし、より広範なオペレーションモデルに効果的に統合します。
- 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って、ビジネスを創出または拡大します。クラウドホスト型ソフトウェアソリューション、クラウド統合製品、またはクラウド関連のプロフェッショナルサービス、コンサルティングサービス、マネージドサービスを提供している場合は、クラウドプロバイダーと戦略的パートナーシップを結ぶことで、クラウドに関する専門知識を高め、顧客へのソリューションのプロモーションを展開して、カスタマーエンゲージメントを向上させることができます。

  パートナーシップを進めていく中で、販促クレジット、資金支援、共同販売などの機会を活用して、ビジネスの創出または拡大に役立てることができます。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販路を拡大し、技術リソースを活用してクラウドベースの製品やサービスを成熟させます。共同の導入事例を公開して、特定のビジネスの課題の解決に成功したことを強調します。

- データの収益化 – データを活用して、一定のビジネス上の利益を得ます。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。一定のビジネス上の利益を得るために、戦略的意図に沿った包括的で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、顧客や従業員のエクスペリエンス、意思決定を改善する機会や、新しいビジネスモデルを実現する機会を識別します。

  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やローカリゼーション、マイクロセグメンテーション、サブスクライバーの維持、ロイヤルティプログラムやリワードプログラムなどを進めることを検討します。ビジネス上の取引の理解や完了に役立つ取引上の価値、過去の業績の説明や結果の推測に役立つ情報的な価値、活動の自動化、決定の指針、成果の予測に役立つ分析的な価値に注目します。外部での収益化の機会 (マーケットプレイスでのデータの販売など) 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 – リアルタイムインサイトを得て、ビジネス上の課題に答えます。ほぼリアルタイムの詳細なインサイトにより、業績の追跡、意思決定の改善、オペレーションの最適化が可能になり、データ収益化戦略の実施に役立ちます。ビジネスのコンテキストをよく理解した横断的な分析チームを設立します。テクニカルなスキル (統計など) やその他のスキル (視覚化やコミュニケーションなど) を重視します。ビジネス目標と重要業績評価指標 (KPI) に合わせて分析を行います。データカタログを活用して関連するデータ製品を見つけ、視覚化ツールやテクニックを活用してデータの傾向、パターン、関係を発見します。まず「全体像」をつかみ、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、機械学習を活用して、複雑なビジネス上の問題を解決します。予測分析と処方的分析により、オペレーションの有効性、意思決定、顧客や従業員のエクスペリエンスの改善が可能になり、データ収益化戦略の実施に役立ちます。

  ビジネスプロセスのトランスフォーメーションの機会を識別したら、機械学習モデルの構築、トレーニング、テストをサポートするために必要なデータ製品がデータカタログに含まれていることを確認します。継続的インテグレーションと継続的デリバリー (CI/CD) のプラクティスを活用して、機械学習ワークフローのオペレーションの回復性と再現性を高めます。モデルがどのように予測を行うかを理解し、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、そのパフォーマンスをモニタリングします。リスクを減らすために、信頼性の低い予測にはヒューマンレビューを行います。

# 人員のパースペクティブ: 文化と変革

人員のパースペクティブでは、テクノロジーとビジネスの架け橋となり、クラウドジャーニーを加速させ、文化、組織構造、リーダーシップ、ワークフォースに焦点を当てながら、継続的に成長、学習し、変化が当たり前になるような文化へと組織がより迅速に進化できるようにします。このパースペクティブは、次の図に示す 7 つの機能で構成されています。一般的なステークホルダーとしては、CIO、COO、CTO、クラウドディレクター、複数部門にわたるリーダー、エンタープライズ全体のリーダーなどが挙げられます。

AWS CAF の人員のパースペクティブの機能

- 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、自律性、透明性、スケーラビリティのベストプラクティスにより、組織の文化を評価し、段階的に進化させ、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、伝統とコアバリューを活用しつつ、顧客のために継続的な改善とイノベーションに注力するワークフォースを魅了、維持、支援する新しい行動や習慣を取り入れる必要があります。長期的に注力し、顧客に深く関わり、顧客のニーズに合わせて大胆にイノベーションを起こします。目指す文化を形成するために役立つ、すべての役割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。迅速な実験、アジャイル手法、横断的なチームを検討して、責任感と自律性を高め、迅速な意思決定を可能にし、過度の承認や手続きの必要性を最小限に抑えます。
- トランスフォーメーションのリーダーシップ – リーダーシップ能力を強化し、リーダーを結集してトランスフォーメーションを進め、成果重視の横断的な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じくらい人員の変革に重点を置く必要があります。技術とビジネスのリーダーシップがどちらも効果的に発揮されなければ、トランスフォーメーションが失速または行き詰まる可能性があります。テクノロジーとビジネスの両面で、戦略、ビジョン、スコープ、リソースについて重要な決定を下し、コミュニケーションや

協力体制の構築を指示し、結果に対する説明責任をチームに課す経営陣の積極的で明確な支援を得ます。

エグゼクティブレベルとプログラムレベルの両方で、ビジネスリーダーとテクノロジーリーダーが文化変革戦略を共同で策定、主導、実現するようにします。各管理層で、組織のクラウドの価値、優先順位、新しい行動に沿った明確で一貫したコミュニケーションが行われ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や Cloud Center of Excellence (CCoE) によってクラウドのリーダーシップ機能を進化させ、一貫性とスケーラビリティのための体系化されたパターンによるトランスフォーメーションの取り組みを周知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の取り組みを進めていく中で、その時点のニーズを満たすためにこの機能を段階的に進化させます。

- クラウドフルエンシー – 自信を持って効果的にクラウドを活用してビジネスの成果を加速するデジタル能力を高めます。優れたワークフォースに求められるのは、デジタル環境への適応だけではありません。最も大きな課題は、テクノロジー自体ではなく、才能、知識、経験を備えたパフォーマンスの高いワークフォースを雇用、育成、維持し、モチベーションを高める能力です。

  急速な技術革新に対応するため、トレーニング戦略全体でタイミング、ツール、テクノロジーに関するトレーニングに目を向け、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。Skills Guild を導入して、トランスフォーメーションの気運を盛り上げ、推進力を高めます。データリテラシーを推進し、データ分析の人材のスキルと知識を向上させます。仮想トレーニング、クラスルームトレーニング、体験トレーニング、ジャストインタイムトレーニングを組み合わせて、Immersion Day を活用し、正式な認定資格でスキルを証明します。メンタリング、コーチング、シャドーイング、ジョブローテーションの各プログラムを実施します。特定の関心領域を持つ実践コミュニティを開設します。知識を共有したことに対して個人にリワードを与え、知識の引き出し、ピアレビュー、継続的なキュレーションのためのプロセスを正式化します。

- ワークフォースのトランスフォーメーション – 人材を育成し、役割をモダナイズして、重要な能力を自律的に高めることができるデジタルフルエンシー、パフォーマンス、適応力の高いワークフォースを魅了、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には、経営陣のリーダーシップを取り入れ、リーダーシップ、学習、リワード、インクルージョン、パフォーマンス管理、キャリアモビリティ、雇用に対するアプローチをモダナイズするために、従来の HR にとどまらない積極的な人材イネーブルメント計画を行います。

  技術的スキルとそれ以外のスキルのバランスのとれた多様で包括的なワークフォースが必要です。組織全体の役割とスキルのギャップを識別し、組織のクラウドの能力を向上させるワークフォース戦略を策定します。デジタルスキルを持つ人材と学びたい人材を活用し、その事例を作ります。ワークフォースを一時的または長期的に増強するために、パートナーやマネージドサービスプロバイダーの利用を戦略的に検討します。

新しい人材を魅了するには、デジタルビジョンや組織文化を広く発信して強力なエンプロイヤーブランドを確立して、リクルート戦略、ソーシャルネットワークチャネル、外部マーケティングに活用します。

- 変革の促進 – 現在から将来の状態への移行時の人員、文化、役割、組織構造への影響を特定して最小限に抑えるプログラムによる変革促進フレームワークを適用することで、新しい働き方の導入を促進します。クラウドトランスフォーメーションはビジネス部門とテクノロジー部門にわたって幅広い変革を起こします。また、構造化および統合された透明性のあるプログラムによるエンドツーエンドの変革プロセスを適用する組織は、高い確率で価値の実現と新しい働き方の導入に成功します。

  変革促進フレームワークをプロジェクトの開始時からカスタマイズして適用することで、組織の連携を可能にし、1 つの共通のエンタープライズを実現し、プロセスの無駄を減らします。横断的にクラウドのリーダーシップを連携させ、結集します。取り組みの早い段階で、何が成功かを定義します。影響評価によって組織のクラウドへの対応を評価し、将来の構想を立てます。主要なステークホルダー、組織間の依存関係、主なリスク、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、リスク低減戦略で構成される、リスクに対処し、強みを活かす変革促進戦略とロードマップを策定します。

  新しい働き方の受け入れを進め、新しいスキルを習得し、導入を加速させるために、組織を関与させ、新しい能力を実現します。明確に定義されたメトリクスを追跡し、アーリーウィンを祝います。変革の協力体制を確立して、推進力を高めるために役立つ既存の文化の手法を活用します。継続的なフィードバック方法とリワードおよび表彰プログラムに従って変革を行います。

- 組織設計 – 新しいクラウドの働き方に合わせて組織設計を評価し、トランスフォーメーションの取り組みを進めるにつれて進化させます。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進めるにあたって、組織設計がビジネス、人員、オペレーション環境の中核戦略を確実にサポートするようにします。変革の事例を確立し、ビジネスの成功にとって重要な要素であると判断した望ましい行動、役割、文化が組織設計に反映されているかどうかを評価します。

  チーム編成、シフトパターン、指揮命令系統、意思決定手順、コミュニケーションチャネルの観点からも、組織の構造および運営の方法が目標とするビジネスの成果をサポートしているかどうかを判断します。新しいモデルを設計し、変革促進フレームワークを適用して実装します。時間とともに進化するように構築され、ビジョンに沿ったクラウド運用モデルへの移行を促進して実現する集約型のチームの設立を検討します。集約型、非集約型、分散型の構造間のトレードオフを考慮し、クラウドワークロードの戦略的価値をサポートするように組織設計を調整します。内部と外部 (マネージドサービスプロバイダーを使用) のチームの関係を明確にします。

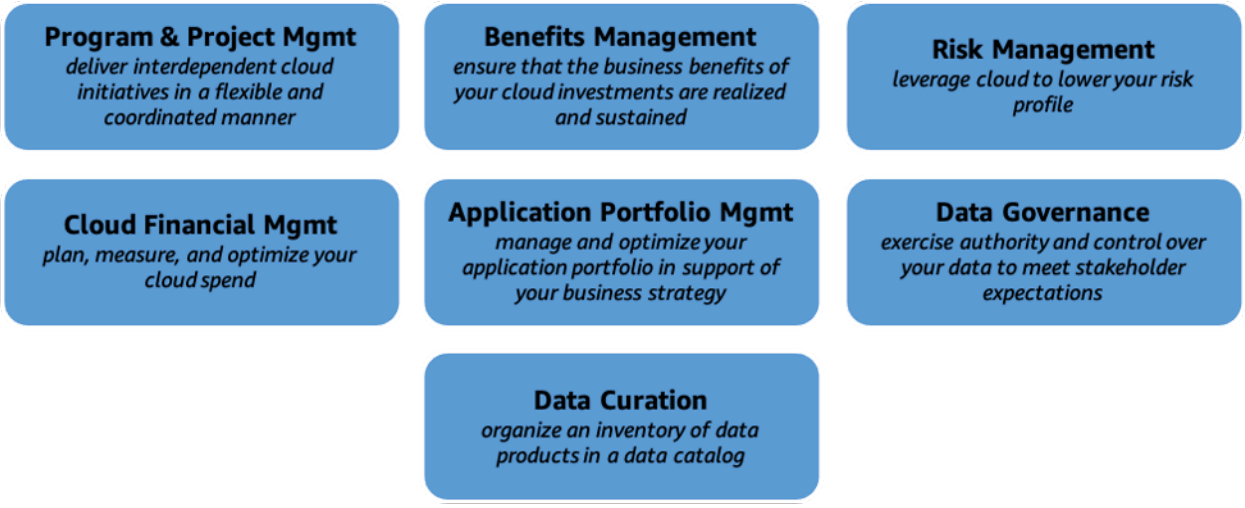
- 組織の連携 – 組織構造、ビジネスオペレーション、プロセス、人材、文化の間に継続的なパートナーシップを確立し、企業が市場に迅速に適応し、新しい機会を活用できるようにします。クラウドの価値実現を推進するために、組織の連携がテクノロジーとビジネス戦略の架け橋となり、テクノロジーの変革がビジネスの成果を生み出すビジネスユニットに受け入れられるようにします。

  オペレーションの回復性、ビジネスの俊敏性、製品/サービスのイノベーションなどのビジネスの成果に優先順位を付けます。人材が自律的に機能し、主要な目標に注力し、より適切な意思決定を行い、生産性を向上できるようにします。リーダーシップの俊敏性、ワークフォースのトランスフォーメーション、人材イネーブルメント、文化、組織構造における人員の能力が最初から統合されるように、変革促進フレームワークを早期に適用することについてリーダーシップのコミットメントを得ます。

  クラウド導入のための測定可能な目標、共通のゴール、方法を設定し、役割レベルでのスキル開発の期待を定めて、持続可能な変革の責任感を醸成します。トップダウンアプローチで共通の価値、プロセス、システム、働き方、スキルを開発し、ビジネスの成果を共同で追求して、部門間のサイロを破壊します。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。継続的な導入とイノベーションを表彰し、リワードを与えます。

# ガバナンスのパースペクティブ: 統制と監視

ガバナンスのパースペクティブでは、組織の利益を最大化し、トランスフォーメーションに関連するリスクを最小限に抑えながら、クラウドの取り組みをオーケストレートすることに重点を置いています。これは、次の図に示す 7 つの機能で構成されています。一般的なステークホルダーとしては、最高トランスフォーメーション責任者、CIO、CTO、CFO、CDO、CRO などが挙げられます。




AWS CAF のガバナンスのパースペクティブの機能

- プログラムおよびプロジェクト管理 – 相互に関係するクラウドの取り組みを柔軟かつ調整された方法で提供します。複雑で横断的なクラウドトランスフォーメーションの取り組み (特により従来型の構造の組織) では、慎重な調整が必要です。これらの相互関係の多くはその時々でのみ明らかになるため、プログラム管理は特に重要です。複数の取り組みを調整して、コスト、スケジュール、労力、利益を最適化または統合することで、相互関係を管理します。

  ビジネスのスポンサーと定期的にロードマップを検証し、問題があれば適時にシニアリーダーシップにエスカレーションして、説明責任と透明性を高めます。アジャイル手法を採用して、広範な予測を行う必要性を最小限に抑えつつ、経験から得られた知見によって適応して、トランスフォーメーションを進めることができるようにします。変更に対応できるようにするために、適切に優先順位付けしたバックログを作成し、エピックやストーリーのかたちで作業を構成します。
- 利益管理 – クラウドへの投資によるビジネス上の利益が確実に実現され、持続するようにします。トランスフォーメーションの成功は、その結果として生じるビジネス上の利益によって決まります。必要な利益を事前に明確に把握しておけば、クラウドへの投資に優先順位を付けて、トランスフォーメーションの進捗を長期的に追跡できます。メトリクスを特定し、必要な利益を数値化して、関係するステークホルダーに伝達します。利益のタイミングと期間を戦略目標に合わせます。

利益の実現のロードマップに利益の提供を組み込みます。実現した利益を定期的に測定し、利益の実現のロードマップに対する進捗を評価して、必要に応じて期待される利益を調整します。

- 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することができます。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するオペレーションリスクと、評判、ビジネスの継続性、変化する市場に迅速に対応する能力に関連するビジネスリスクを特定して数値化します。クラウドがリスクプロファイルの低減にどのように役立つかを理解し、アジャイルのケイデンスの一部としてリスクを繰り返し特定および管理します。クラウドを活用して、インフラストラクチャの運用や障害に関連するリスクを低減することを検討します。インフラストラクチャへの多額の先行投資の必要性を減らし、不要なアセットを購入する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のプロビジョニングとプロビジョニング解除をすぐに行い、調達のスケジュールのリスクを低減します。
- クラウドの財務管理 – クラウドの支出を計画、測定、最適化します。クラウドがもたらすリソースのプロビジョニングの容易さや俊敏性のメリットと、チームのクラウドの支出に対する財務上の説明責任を併せて考えます。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て、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上の役割と責任を明確にし、財務、ビジネス、テクノロジーの各組織の主要なステークホルダーがクラウドのコストについて共通の理解を持つようにします。より動的な予測と予算編成のプロセスに進化させ、コストの差異や異常をより迅速に識別します。

  アカウント構造とタグ付け戦略を、組織と製品のクラウドへのマッピングに合わせます。アカウントとコスト配分タグを構造化し、クラウドリソースを特定のチーム、プロジェクト、ビジネスの取り組みにマッピングして、使用パターンを詳細に把握します。コストカテゴリを定義し、カスタムルールを使用してコストと使用状況の情報を整理して、ショーバックやチャージバックを簡素化します。一括請求 (コンソリデーティッドビリング) を使用すると、クラウドの請求を簡素化して、ボリュームディスカウントを実現できます。俊敏性への影響を最小限に抑えつつ、スケーラブルな方法でクラウドの使用を管理するガードレールを作成します。

  技術的負債を負わないように、ワークロードが適切に設計され、最もコスト効率が良い方法でオペレーションが行われるようにします。需要ベースと時間ベースの動的な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うようにします。アイドル状態または十分に活用されていないクラウドリソースに関する支出を特定して廃止することで、クラウドのコストを削減します。

  オンプレミスとクラウドのソフトウェアライセンスの管理を一元化して、ライセンス関連のコストの超過とコンプライアンス違反を減らし、申告ミスを回避します。クラウドリソースに含まれるライセンスと、所有しているライセンスを区別します。ライセンスの使用にルールベースの管理を活用して、新規および既存のクラウドへのデプロイに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の使用状況を可視化し、ベンダーの監査を迅速化します。コンプライアンス違反に対するリアルタイムの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 – ビジネス戦略をサポートするために、アプリケーションポートフォリオを管理および最適化します。アプリケーションはビジネス能力を支え、それを関連するリソースにリンクさせます。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、モダナイゼーションの機会を識別するために役立ちます。効果的なアプリケーションポートフォリオ管理機能により、アプリケーションの無秩序な増加を最小限に抑え、アプリケーションの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との継続的な整合性を確保します。

  最も重要なアプリケーションから始めて、包括的なビジネス能力の観点から定義し、基盤となるソフトウェア製品や関連するリソースにマッピングします。エンタープライズアーキテクチャ、IT サービス管理 (ITSM)、プロジェクト/ポートフォリオ管理など、関連するエンタープライズシステムのデータを利用することで、各アプリケーションの全体像を把握します。主要なテクノロジーや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、アプリケーションの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要求します。組織がアプリケーションへの投資から得られる価値を最大化するために、アプリケーションポートフォリオの健全性を定期的に評価します。

- データガバナンス – ステークホルダーの期待に応えるために、データに対する権限と管理を行使します。ビジネスプロセスと分析能力は、正確、完全、適時、関連性の高いデータに依存しています。データの所有者、スチュワード、管理者などの重要な役割を定義して割り当てます。ガバナンスにフェデレーション (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。データディクショナリ、分類、ビジネス用語集などの標準を指定します。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。

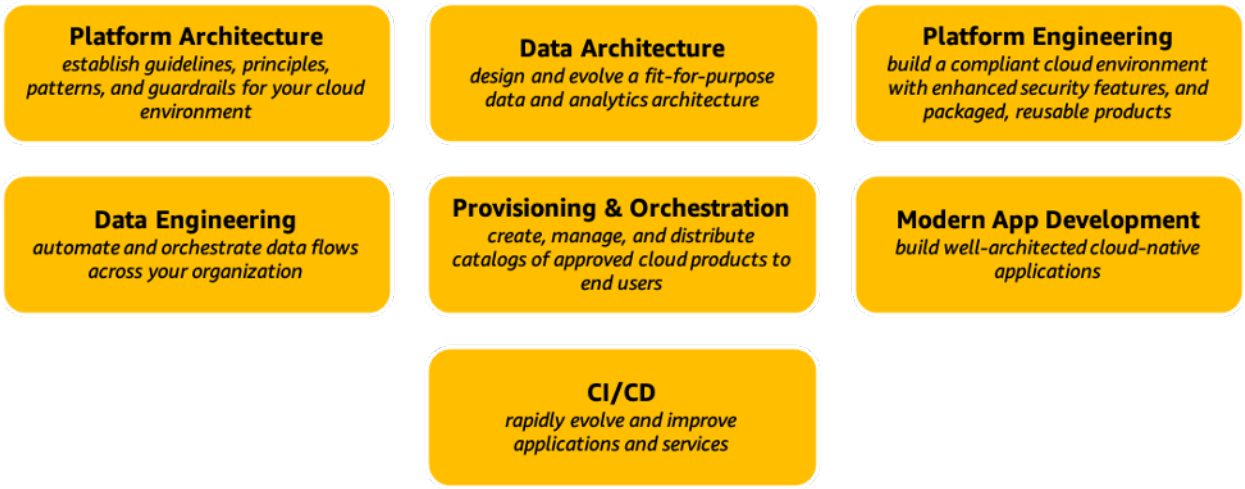
  データライフサイクルポリシーを策定し、継続的なコンプライアンスの監視を実施します。戦略およびオペレーション上のデータのニーズに合わせて、データ品質への取り組みに優先順位を付けます。データ品質標準を確立します。主要な品質特性、ビジネスルール、メトリクス、目標を特定します。データバリューチェーンのすべての段階でデータ品質を監視します。データ品質の問題の根本原因を特定し、ソースで関連するプロセスを改善します。重要なデータ製品にデータ品質ダッシュボードを実装します。

- データキュレーション – メタデータを収集、整理、アクセス、エンリッチ化し、データカタログにデータ製品のインベントリを整理するために使用します。データカタログは、データコンシューマーが該当するデータ製品をすばやく見つけて出所や品質などのコンテキストを理解できるようにすることで、データの収益化やセルフサービスの分析を促進します。

データカタログのモデレーションを担当するリードキュレーターを指定します。データ収益化戦略に従って、構造化データや非構造化データなどの主要なデータ製品をカタログ化します。リネージなど、関連する技術および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、インデックス作成、自動分類を行います。必要に応じて手動でタグ付けして、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使用したクラウドソーシングによるデータエンリッチメントを検討します。具体的には、データコンシューマーがデータ製品の評価、レビュー、注釈付けを行えるようにすることを検討します。

# プラットフォームのパースペクティブ: インフラストラクチャとアプリケーション

プラットフォームのパースペクティブでは、エンタープライズグレードのスケーラブルなハイブリッドクラウド環境によって、クラウドワークロードのデリバリーを加速させることに重点を置いています。これは、次の図に示す 7 つの機能で構成されています。一般的なステークホルダーとしては、CTO、テクノロジーリーダー、アーキテクト、エンジニアなどが挙げられます。




AWS CAF のプラットフォームのパースペクティブの機能

- 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 によるクラウド環境は、実装の迅速化、リスクの軽減、クラウドの導入の促進に役立ちます。クラウドの導入を進める社内標準について、組織のコンセンサスを形成します。認証、セキュリティ、ネットワーク、ログ記録とモニタリングを容易にする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ます。レイテンシー、データ処理、データレジデンシーの要件に従って、オンプレミスで保持する必要があるワークロードを検討します。クラウドでのバースト、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 – 目的に合ったデータおよび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および分析アーキテクチャは、複雑さ、コスト、技術的負債を低減するとともに、急速に増えるデータから実用的なインサイトを得るために役立ちます。多層化されたモジュラーアーキテクチャを採用することで、適切なツールを適切なジョブに使用し、新しい要件やユースケースに合わせてアーキテクチャを反復的かつ段階的に進化させることができます。

要件に基づいて、アーキテクチャの各層の主要なテクノロジー (取り込み、ストレージ、カタログ、処理、使用など) を選択します。継続的な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サポートに重点を置き、データレイクと専用データストアの間のデータの移動を容易にするためにレイクハウスアーキテクチャの採用を検討します。

- プラットフォームエンジニアリング – セキュリティ機能が強化され、パッケージ化された再利用可能なクラウド製品を使用して、コンプライアンスに準拠したマルチアカウントクラウド環境を構築します。効果的なクラウド環境により、新しいアカウントを簡単にプロビジョニングして、そのアカウントが組織のポリシーに確実に適合するようにできます。キュレートされた一連のクラウド製品により、ベストプラクティスを体系化し、ガバナンスを支援するとともに、クラウドデプロイの速度と一貫性を高めることができます。ベストプラクティスのブループリント、検出ガードレール、予防ガードレールをデプロイします。クラウド環境を既存のエコシステムと統合して、必要なハイブリッドクラウドのユースケースを実現します。

  アカウントのプロビジョニングのワークフローを自動化し、複数のアカウントを活用して、セキュリティとガバナンスの実現をサポートします。オンプレミス環境とクラウド環境の間の接続や、異なるクラウドのアカウント間の接続をセットアップします。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、既存の ID プロバイダー (IdP) とクラウド環境の間にフェデレーションを実装します。ログの一元化、クロスアカウントのセキュリティ監査の確立、インバウンドとアウトバウンドのドメインネームシステム (DNS) リゾルバーの作成、ダッシュボードでのアカウントとガードレールの可視化を行います。

  社内標準と構成管理に従って、クラウドサービスの使用を評価および認証します。社内標準をセルフサービスのデプロイ可能な製品や使用可能サービスとしてパッケージ化し、継続的に改善します。Infrastructure as Code (IaC) を活用して、宣言型の方式で構成を定義します。

- 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およびオーケストレートします。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は、生産性の向上と市場投入までの時間の短縮に役立ちます。データエンジニアリングチームは、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、データ管理を横断的に行います。メタデータを活用することにより、raw データを使用して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のガードレールとセキュリティ管理のほか、モニタリング、ログ、アラートを実装して、パイプラインの障害に備えます。よくあるデータ統合パターンを識別し、パイプラインの開発の複雑さを抽象化する再利用可能なブループリントを作成します。ブループリントをビジネスアナリストやデータサイエンティストと共有し、セルフサービスによる運用を可能にします。

- プロビジョニングとオーケストレーション – 承認済みのクラウド製品のカタログを作成および管理して、エンドユーザーに配布します。組織が拡大するにつれ、インフラストラクチャのプロビジョニングの一貫性をスケーラブルで繰り返し可能に保つことは難しくなってきます。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により、一貫したガバナンスを実現してコンプライアンスの要件を満たすとともに、ユーザーは承認済みのクラウド製品のみを迅速にデプロイできるようになります。承認済みのクラウド製品を公開、配布、参照、使用するための一元管理されたセルフサービスポータルを設計および実装します。API やパーソナライズされたポータルを介して、クラウド製品にアクセスできるようにします。お使いの IT サービス管理 (ITSM) ツールと統合し、構成管理データベース (CMDB) の更新を自動化します。
- モダンアプリケーション開発 – Well-Architected によるクラウドネイティブの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のプラクティスは、イノベーションのスピードと俊敏性を実現するために役立ちます。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、リソースの使用率を最適化して、ゼロからピークの需要まで自動的にスケールできます。イベント駆動型アーキテクチャを活用した独立したマイクロサービスとしてアプリケーションを構築することにより、アプリケーションをデカップリングすることを検討します。すべてのレイヤーとアプリケーション開発ライフサイクルの各段階でセキュリティを実装します。

  スケールアウトとスケールインのプロセスを自動化します。または、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して、コストを削減し、効率性を高め、既存の投資を最大限に活用します。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行すること) やリファクタリング (レガシーアプリケーションをクラウドネイティブのアーキテクチャに書き換えること) を検討します。アーキテクチャでサービスクォータと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に悪影響を及ぼさないようにします。
- 継続的インテグレーションと継続的デリバリー – 従来のソフトウェア開発プロセスや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速くアプリケーションやサービスを進化させ、改善します。継続的インテグレーション、テスト、デプロイなどの DevOps のプラクティスを導入することで、俊敏性を高め、イノベーションを加速し、変化する市場により適応し、ビジネスの成果をより効率的に上げることができます。継続的インテグレーションと継続的デリバリー (CI/CD) の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最小限の実行可能なパイプラインから始めて、より多くのコンポーネントとステージを含む継続的デリバリーのパイプラインに移ります。ユニットテストをできるだけ早く作成して、コードを中央リポジトリにプッシュする前に実行するようにデベロッパーに促します。継続的デリバリーのパイプラインにステージングと本番稼働のステップを含めて、本番環境へのデプロイの手動の承認を検討します。インプレース、ローリング、イミュータブル、ブルー/グリーンなど、複数のデプロイ戦略を検討します。

# セキュリティのパースペクティブ: コンプライアンスと保証

セキュリティのパースペクティブでは、データやクラウドワークロードの機密性、完全性、可用性の実現を支援します。これは、次の図に示す 9 つの機能で構成されています。一般的なステークホルダーとしては、CISO、CCO、内部監査リーダー、セキュリティアーキテクト、セキュリティエンジニアなどが挙げられます。

AWS CAF のセキュリティのパースペクティブの機能

- セキュリティガバナンス – セキュリティ上の役割、責任、説明責任、ポリシー、プロセス、手順を策定、維持、効果的に伝達します。説明責任を明確にすることは、セキュリティプログラムの有効性にとって重要です。業界や組織に適用されるアセット、セキュリティリスク、コンプライアンスの要件を理解することは、セキュリティの取り組みの優先順位付けに役立ちます。今後の方向性とアドバイスを提供することで、チームの動きが速くなり、トランスフォーメーションを加速できます。

  お客様のクラウドにおけるセキュリティ上の責任を理解します。関連するステークホルダー、アセット、情報交換のインベントリ、分類、優先順位付けを行います。業種や組織に適用される法令、規則、規制、標準/枠組みを確認します。組織のリスクアセスメントを年に 1 回実施します。リスクアセスメントは、特定したリスクや脆弱性が組織に影響を及ぼす可能性と重大度を判断するために役立ちます。特定したセキュリティ上の役割と責任に十分なリソースを割り当てます。コンプライアンスの要件と組織のリスク許容度に従って、セキュリティ上のポリシー、プロセス、手順、統制を策定し、新しいリスクや要件に基づいて継続的に更新します。
- セキュリティ保証 – セキュリティプログラムとプライバシープログラムの有効性を継続的に監視、評価、管理、改善します。組織やサービスを提供する顧客は、実施した統制によって規制要件

が満たされ、ビジネス目標とリスク許容度に従っ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ようになるという信頼と自信を必要としています。

統制を包括的な統制の枠組みに文書化し、その目的を満たす実施可能なセキュリティとプライバシーの統制を確立します。クラウドベンダーの監査報告書やコンプライアンス認証または証明を確認することで、クラウドベンダーが実施している統制、それらの統制がどのように検証されたか、その統制が自社の拡大した IT 環境で効果的に運用されているかを理解することができます。

環境を継続的に監視および評価し、統制の運用の有効性を検証して、規制や業界標準へのコンプライアンスを証明します。セキュリティ上のポリシー、プロセス、手順、統制、記録を確認し、必要に応じて主要な人員にヒアリングを行います。

- アイデンティティおよび許可管理 – アイデンティティと許可を大規模に管理します。アイデンティティを AWS で作成するかアイデンティティソースに接続し、ユーザーに必要な許可を付与して、AWS リソースや統合されたアプリケーションのサインイン、アクセス、プロビジョニング、オーケストレーションを行えるようにすることができます。効果的なアイデンティティおよびアクセス管理は、適切なユーザーやマシンが適切な条件で適切なリソースにアクセスできるようにするために役立ちます。

  AWS Well-Architected フレームワークでは、アイデンティティを管理するための関連する概念、設計原則、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、一元管理されたアイデンティティプロバイダーの利用、大規模できめ細かなアクセスコントロールと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が含まれます。ユーザーやマシンのアイデンティティで AWS やワークロードへのアクセスをコントロールするには、特定の条件で特定のリソースの特定のサービスのアクションに許可を設定します。最小権限の原則を使用して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数が拡大し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。ポリシーをスケールできるように属性に基づいて許可を付与します (ABAC)。ポリシーが必要な保護を提供していることを継続的に検証します。

- 脅威の検出 – 潜在的なセキュリティ上の設定ミス、脅威、予期しない動作を把握および識別します。セキュリティ脅威について理解を深めることで、保護管理の優先順位付けが可能になります。効果的な脅威の検出により、脅威により迅速に対応し、セキュリティイベントから知見を得ることができます。戦術的、行動的、戦略的なインテリジェンスの目的と全体的な手法について合意します。関連する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オペレーション化を行います。

  監視を環境全体に展開して重要な情報を収集し、特定の場所で特定の種類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さまざまなイベントソースの監視データを関連付けて、強固なセキュリティ体制を実現し、可視性を高めます。不正ユーザーの行動パターンを理解するために、デセプション技術 (ハニーポットなど) を活用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、是正、緩和します。脆弱性は、既存のシステムへの変更や新しいシステムの追加によっても発生する可能性があります。脆弱性を定期的にスキャンして、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使用して、システムを既知の脆弱性と関連付けます。脆弱性のリスクに基づいて、是正措置に優先順位を付けます。是正措置を適用して、関連するステークホルダーに報告します。レッドチームと侵入テストを活用して、システムアーキテクチャの脆弱性を特定し、必要に応じてクラウドプロバイダーに事前承諾を求めます。
- インフラストラクチャの保護 – 意図しない不正アクセスや潜在的な脆弱性から、ワークロードのシステムやサービスを保護できます。意図しない不正アクセスや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、クラウドにおけるセキュリティ体制を強化できます。多層防御を活用して、データやシステムを保護するための一連の防御メカニズムを多層化します。

  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を必要としないワークロードを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、ネットワークファイアウォールを使用して、トラフィックを制御します。システムやデータの価値に応じて、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に Virtual Private Cloud (VPC) エンドポイントを活用します。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などを使用して、各層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て、オンプレミスやエッジ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 – データの可視性と管理を維持します。また、組織内でのデータのアクセス方法と使用方法も維持します。意図しない不正アクセスや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重要な目的の 1 つです。適切な保護と保持の管理を判断しやすくするために、重要度と機密性 (個人を特定できる情報など) に基づいてデータを分類します。データ保護管理とライフサイクル管理ポリシーを定義します。保管中および転送中のすべてのデータを暗号化し、機密データを別の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。
- アプリケーションのセキュリティ – ソフトウェア開発プロセスでセキュリティの脆弱性を発見して解決します。アプリケーションのコーディング段階でセキュリティ上の欠陥を見つけて修正するため、時間、労力、コストを節約でき、本番環境での稼働時にはセキュリティ体制に自信を持つことができます。コードと依存関係の脆弱性をスキャンしてパッチを適用して、新しい脅威から保護します。開発と運用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

的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識別します。

- 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、潜在的な被害を減らします。セキュリティインシデントに対する迅速、効果的、一貫性のある対応は、潜在的な被害を減らすために役立ちます。クラウドテクノロジーとその利用方法について、セキュリティオペレーションやインシデント対応のチームを教育します。ランブックを作成して、インシデント対応方法のライブラリを作成します。主要なステークホルダーを関与させて、選択が与える影響を組織に広く周知します。

  セキュリティイベントをシミュレートし、机上演習や訓練を通じてインシデント対応を練習します。シミュレーションの結果を復習することで、対応体制の規模を改善し、価値を実現するまでの時間を短縮して、リスクをさらに軽減します。インシデント後分析を行って、標準化された方法を活用して根本原因を特定および解決することにより、セキュリティインシデントから知見を得ます。

# オペレーションのパースペクティブ: 正常性と可用性

オペレーションのパースペクティブでは、ビジネスの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確実に提供することに重点を置いています。オペレーションを自動化および最適化することにより、ワークロードの信頼性を高めつつ、効果的にスケールできます。このパースペクティブは、次の図に示す 9 つの機能で構成されています。一般的なステークホルダーとしては、インフラストラクチャおよびオペレーションのリーダー、サイト信頼性エンジニア、IT サービスマネージャーなどが挙げられます。

AWS CAF のオペレーションのパースペクティブの機能

- 可観測性 – 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実用的なインサイトを得ます。クラウドのスピードと規模でオペレーションを行う場合、問題は発生時 (理想的にはカスタマーエクスペリエンスを損なう前) に発見できる必要があります。ワークロードの内部の状態と正常性を把握するために必要なテレメトリ (ログ、メトリクス、トレース) を作成します。アプリケーションの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らアラートを生成します。

  合成モニタリングを使用して 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) を作成して、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、リクエストがアプリケーションで処理される過程を追跡し、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、ネットワークに関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設定して、パフォーマンスへの影響の原因を把握します。データを 1 つのダッシュボードに集約し、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を一元的に把握できるようにします。

- 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て、適切な対応を決定します。ノイズの除去、優先度の高いイベントの重視、差し迫ったリソースの枯渇の予測、アラートとインシデントの自動生成、考えられる原因と是正措置の特定が可能になることで、インシデントの発見と対応にかかる時間を短縮できます。イベントストアパターンを定義し、機械学習 (AIOps) を活用して、イベントの関連付け、異常の検出、因果関係の特定を自動化します。インシデント管理システムやプロセスなど、クラウドサービスやサードパーティー製ツールと統合できます。イベントへの対応を自動化し、手動のプロセスによって発生するエラーを減らすことで、迅速かつ一貫した対応を実現します。
- インシデントおよび問題管理 – サービスのオペレーションを迅速に復旧し、ビジネスへの悪影響を最小限に抑えます。クラウドの導入により、サービスの問題やアプリケーションの状態の問題への対応プロセスを高度に自動化して、サービスのアップタイムを向上させることができます。より分散したオペレーションモデルに移行することにより、関連するチーム、ツール、プロセスの間のインタラクションが合理化され、重大なインシデントや複雑なインシデントの解決を迅速化できます。ランブックで、エスカレーションのトリガーやエスカレーションの手順などのエスカレーションの経路を定義します。

  インシデント対応の訓練を実施し、得られた知見をランブックに取り入れます。インシデントのパターンを識別して、問題を特定し、是正措置を決定します。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、ワークフローを結び付けます。責任を問わないインシデント後分析を活用して、インシデントに寄与する要因を特定し、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 – 本番環境へのリスクを最小限に抑えつつ、ワークロードを導入および変更します。従来のリリース管理は、デプロイに時間がかかり、ロールバックが難しい複雑なプロセスでした。クラウドの導入により、CI/CD 技術を活用して、リリースとロールバックを迅速に管理できます。クラウドの俊敏性に合った自動承認ワークフローによ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。小規模で可逆的な変更を頻繁に行うことで、変更の範囲を縮小します。ライフサイクルのすべての段階で変更をテストし、結果を検証して、デプロイの失敗によるリスクと影響を最小限に抑えます。結果が達成されない場合に以前の正常な既知の状態に自動的にロールバックすることで、復旧時間を最小限に抑えるとともに、手動プロセスによるエラーを減らします。
- パフォーマンスおよびキャパシティ管理 – ワークロードのパフォーマンスをモニタリングし、キャパシティが今後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実質的に無制限ですが、サービスクォータ、キャパシティの予約、リソースの制約により、ワークロードの実際のキャパシティは制限されます。このようなキャパシティの制約を理解して、効果的に管理する必要があります。主要なステークホルダーを特定し、目的、範囲、目標、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、目標に対するパフォーマンスを定期的に確認およ

び報告します。新しいテクノロジーを定期的に評価して、パフォーマンスを改善し、必要に応じて目標とメトリクスの変更を提案します。ワークロードの使用状況をモニタリングし、今後の比較のためにベースラインを作成して、必要に応じてキャパシティを拡大するためのしきい値を指定します。需要を長期にわたって分析し、キャパシティが季節的な傾向や変動するオペレーションの条件を満たすようにします。

- 構成管理 – すべてのクラウドワークロード、その関係、構成の変更の長期にわたる正確かつ完全な記録を保持します。効果的に管理しないと、クラウドリソースのプロビジョニングの動的かつ仮想の性質により、構成ドリフトにつながる可能性があります。ビジネス属性をクラウドの使用状況にオーバーレイ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従ってリソースを整理します。必須のタグを指定して、ポリシーでコンプライアンスを強制します。Infrastructure as Code (IaC) と構成管理ツールを活用して、リソースのプロビジョニングとライフサイクル管理を行います。構成のベースラインを定義し、バージョン管理を使用して管理します。
- パッチ管理 – ソフトウェアの更新をシステマティックに配布して適用します。ソフトウェアの更新は、新たなセキュリティの脆弱性に対処し、バグを修正し、新しい機能を導入します。パッチ管理のシステマティックなアプローチにより、本番環境へのリスクを最小限に抑えつつ、最新の更新のメリットを得ることができます。指定したメンテナンス期間に重要な更新を適用し、クリティカルなセキュリティ更新はできるだけ早く適用します。次回の更新の詳細をユーザーに事前に通知することで、他の対策が可能な場合はパッチを延期できるようにします。本番環境にロールアウトする前に、マシンイメージを更新してパッチをテストします。パッチの適用中も引き続き可用性を確保するために、アベイラビリティーゾーン (AZ) や環境ごとに個別のメンテナンス期間を検討します。パッチの適用のコンプライアンスを定期的に確認し、違反しているチームに必要な更新を適用するように警告します。
- 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、既存の技術投資、復旧目標、使用可能なリソースを慎重に検討する必要があります。災害やセキュリティイベントの後にできるだけ早く復旧することで、システムの可用性とビジネスの継続性を維持できます。定めたスケジュールに従って、データとドキュメントをバックアップします。

  事業継続計画の一部として、災害対策計画を策定します。ワークロードごとにさまざまな災害シナリオの脅威、リスク、影響、コストを特定し、それに応じて目標復旧時間 (RTO) と目標復旧時点 (RPO) を指定します。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、選択した災害対策戦略を実施します。カオスエンジニアリングを活用して、管理された実験によって回復性とパフォーマンスを向上させることを検討します。計画を定期的に見直してテストし、得られた知見に基づいてアプローチを調整します。

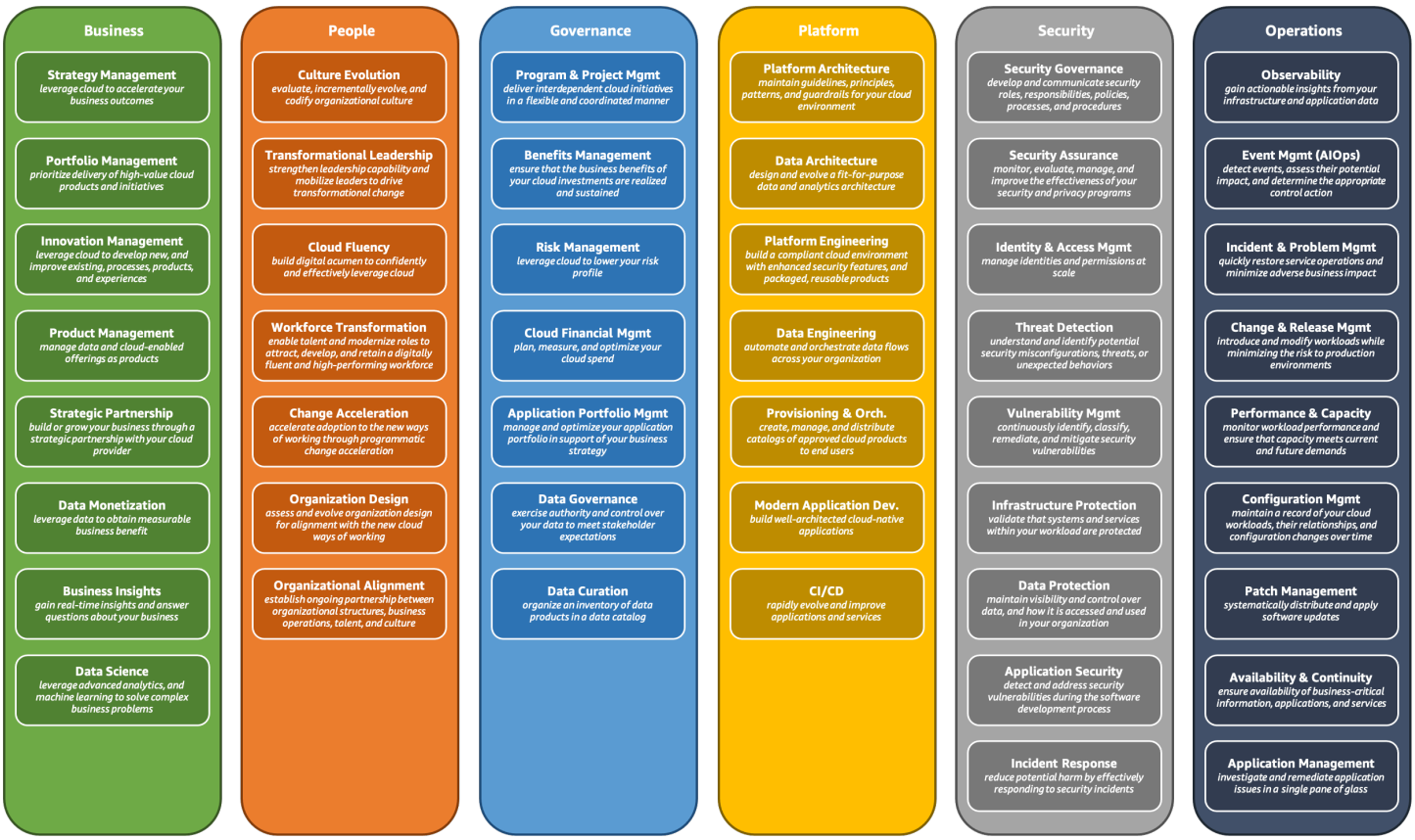
- アプリケーション管理 – アプリケーションの問題を一元的に調査および是正します。アプリケーションのデータを単一の管理コンソールに集約することで、異なる管理ツール間でコンテキストを切り替える必要がなくなり、オペレーションの監視が容易になるため、アプリケーションの問題の是正が迅速化されます。

  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、アプリケーションのコンポーネントやリソースの検出を自動化して、アプリケーションのデータを単一の管理コンソールに統合します。ソフトウェアのコンポーネントやインフラストラクチャのリソースを含めて、開発、ステージング、本番などのさまざまな環境を正確に把握します。オペレーションの問題をより迅速かつ一貫した方法で是正するために、ランブックの自動化を検討します。

# まとめ

技術革新が加速し続ける中、継続的なデジタルトランスフォーメーションの必要性はますます高まっています。AWS CAF は、AWS の経験とベストプラクティスを活用し、AWS の革新的な利用によるビジネスの成果の加速を支援します。AWS CAF を使用して、トランスフォーメーションの機会を識別して優先順位を付け、クラウドへの対応を評価して改善し、トランスフォーメーションのロードマップを反復的に進化させます。

# 付録: AWS CAF の機能の図




AWS CAF の基本的な機能

# 寄稿者

- AWSの多くの内容領域専門家の協力を得て、AWS CAF のワールドワイドリードである Saša Baškarada が作成しています。

# その他の資料

詳細については、以下の資料を参照してください。

- AWS アーキテクチャセンター
- AWS 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 の開始方法
- アマゾン ウェブ サービスの概要

# 改訂履歴

このホワイトペーパーの更新に関する通知を受け取るには、RSS フィードをサブスクライブしてください。

| update-history-change | update-history-description | update-history-date |
| --- | --- | --- |
| 第 3 版 | 機能を更新および拡大。トランスフォーメーションの分野とジャーニーのフェーズを追加。 | 2021 年 11 月 22 日 |
| 第 2 版 | パースペクティブと機能の構造を変更。 | 2017 年 2 月 1 日 |
| 初版 | ホワイトペーパーの初版公開。 | 2015 年 2 月 1 日 |

# 注意

お客様は、この文書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と慣行について説明しており、これらは予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤーまたはライセンサーからの契約上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または暗示を問わず、一切の保証、表明、条件なしに「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 とお客様の間で締結されるいかなる契約の一部でもなく、その内容を修正するものでもありません。

© 2021 Amazon Web Services, Inc. or its affiliates.All rights reserved.