AWS 決定ガイド

AWS クラウドガバナンスサービスの選択

AWS クラウドガバナンスサービスの選択: AWS 決定ガイド

Table of Contents

AWS クラウドガバナンスサービスの選択

最初のステップを実行する

目的	どの AWS クラウドガバナンスサービスが組織に最適かを判断するのに役立ちます。
最終更新日	2024 年 12 月 23 日
対象サービス	• AWS Artifact • AWS Audit Manager • CloudFormation • AWS CloudTrail • AWS Config • AWS Control Tower • AWS Organizations • AWS Security Hub CSPM • AWS Service Catalog • AWS Systems Manager • AWS Trusted Advisor

AWS クラウドガバナンスの概要

クラウドガバナンスは、ビジネス目標に合わせて AWS クラウド 使用するのに役立つ一連のルール、プロセス、レポートです。

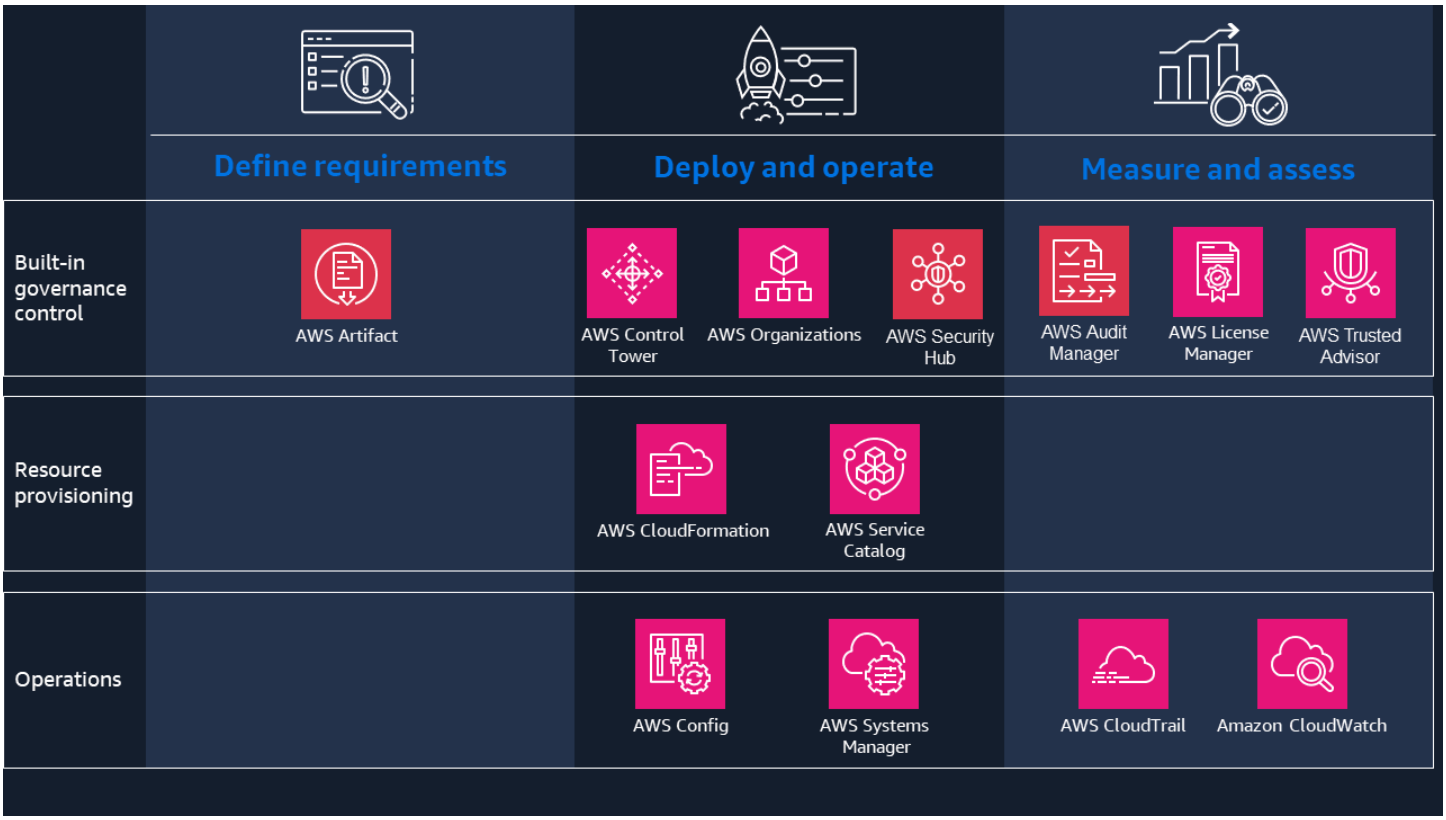
これには、マルチアカウント戦略、継続的モニタリング、コントロールポリシーを有効にすることで、セキュリティが含まれます。チェック、レポート、修復を自動化することで、コンプライアンスについて説明します。企業全体でコントロールを適用することで、オペレーションをカバーします。アイデンティティとアクセス管理を大規模に一元化することで、アイデンティティをカバーします。使用状況レポートとポリシーの適用を容易にすることで、コストをカバーします。また、評価とテストを CI/CD パイプラインに統合して検証できるようにすることで、レジリエンスについても説明します。

クラウド内のアカウント、サービス、リソースの使用を設定、管理、モニタリング、制御し、クラウドガバナンスのベストプラクティスを実装するのに役立つさまざまなサービスを提供します。

このガイドは、開発速度を維持し、イノベーションを加速させながら、組織に最適な AWS クラウドガバナンスサービスを決定し、運用レジリエンスを強化し、コストを最適化し、規制や企業標準に準拠するためのコントロールを構築するのに役立つように設計されています。

この動画は、クラウドガバナンスのベストプラクティスを紹介するプレゼンテーションの 6 分間のセグメントです。

AWS クラウドガバナンスを理解する



前の図は、クラウドガバナンスが複数の をどのように活用しているかを示しています。これにより AWS のサービス、ガバナンス要件の定義、システムのデプロイと運用、パフォーマンスの測定と評価を行うことができます。このサービスは、組み込みのガバナンスコントロール、ガバナンスポリシーに沿ったリソースプロビジョニング、環境のモニタリングと管理に役立つ運用ツールを提供します。

AWS クラウドガバナンスサービスを活用すると、クラウドの使用がビジネス目標を確実にサポートできるようになります。具体的には、開発者のスピードと俊敏性の向上、動的な規制環境での運用、合併と買収の合理化、運用レジリエンスの強化が可能になります。

- デベロッパーのスピードと俊敏性の向上 — API を使用して新しい環境を迅速にスピンし、デベロッパーが数週間のプロビジョニングサイクルを待たないようにし、CI/CD パイプラインのプロビジョニングを高速化します。 APIs 構築済みのコントロールとルール、および一般的なリソースを効率的にプロビジョニングするためのinfrastructure-as-codeテンプレートを使用して、ソフトウェア配信プロセスの早い段階で欠陥を見つけて防止します。
- 動的な規制環境で運用 — 常時オンの境界を作成して、 全体のデータへのアクセスを保護および制御し AWS、コンプライアンス要件を体系化し、組織全体のリソース設定の評価を自動化します。
- 合併と買収の合理化 — 安全で適切に設計されたマルチアカウント環境を構築することで、ワークロードをより迅速に移行できます。アカウント作成を一元化し、リソースを割り当て、アカウントをグループ化し、ガバナンスポリシーとコントロールを簡単かつ迅速に適用します。大規模なマルチアカウント管理にプログラムによるアプローチを採用します。
- 運用レジリエンスの強化 — 安全で適切に設計された、回復力のあるマルチアカウント環境を迅速にセットアップします。ワークロードの評価を実行して、回復力に関連する潜在的な弱点を発見します。コスト最適化、パフォーマンス、セキュリティ、耐障害性、サービス制限の 5 つの主要領域に対して自動チェックを実行し、既知のベストプラクティスに従うための推奨事項を受け取ります。
- コストの最適化 — コストと使用状況を時間の経過とともに可視化、理解、管理します。リソース使用率を継続的に分析し、使用率の低いリソースを特定し、アイドル状態のリソースを終了します。

クラウドガバナンスのベストプラクティスは、ワークロードをセットアップして運用するときに効果的に組み込みます AWS。相互運用可能なサービスは、 AWS やサードパーティー製品など、IT 資産に対する一貫した一元化されたガバナンスを実現するのに役立ちます。全体のコントロールの幅と深さは、進化する規制要件を満たし、セキュリティリスクを最小限に抑える AWS のサービス のに役立ちます。

AWS クラウドガバナンス基準を検討する

次のセクションでは、クラウドガバナンス戦略を選択する際に考慮すべき重要な基準をいくつか概説します。特に、組織やビジネス目標に適用される可能性のあるさまざまな種類のクラウド環境、コントロール体制、開発者サポートの機会について説明します。

Multi-account strategy

その意味： クラウド環境のベストプラクティスの実装は、安全なマルチアカウント戦略の採用にかかっています。アカウントを構成要素として使用し、セキュリティとインフラストラクチャ

OUs の基本 OUs、サンドボックス化とワークロードの追加 OU などの組織単位 (OU) にグループ化します。 OUs

重要な理由： マルチアカウント戦略は、クラウド環境で自然な境界と分離を提供します。これにより、クォータとアカウント制限の管理、アカウントのプロビジョニングとカスタマイズの自動化、管理アカウントへのアクセス制限による最小特権の原則の適用が可能になります。これにより、環境全体のユーザーのアクティビティとリスクを追跡できます。マルチアカウント戦略は、移行プロジェクトや合併や買収などの組織変更のために構築できる基盤として機能します。

AWS Organizations を使用して複数の AWS アカウント を組織に統合し、リソースの割り当て、アカウントのグループ化、ガバナンスポリシーの適用に使用できます。

をオーケストレーションサービスAWS Control Towerとして使用し AWS Organizations、その上に階層化して AWS 資産を構造化し、OUs とマルチアカウント環境に対するガバナンスを拡張します。

Controls management best practices

その意味： コントロール管理のベストプラクティスの実装には、さまざまなアプローチを含めることができます。検出コントロールは、定義されたセキュリティポリシーに違反するリソースをキャッチします。予防的コントロールは、特定のアクションをブロックすることでセキュリティベースラインを保護します。また、プロアクティブコントロールはリソースをプロビジョニングする前にスキャンし、非準拠のコードのデプロイを停止し、開発者に修正するよう指示します。相互運用性 AWS のサービス により、新しい市場に成長するにつれて、 AWS やサードパーティー製品を含む IT 資産全体を一元管理し、制御できます。

重要な理由： コントロール管理のベストプラクティスにより、大規模なコントロールをプログラムで実装し、コンプライアンスを自動的に設定したり、コンプライアンス違反を修正したりできます。これは、組織が医療、ライフサイエンス、金融サービス、公共部門などの規制された業界で事業を行っている場合、特定の規制フレームワークが適用される場合、または特定の企業標準やデータレジデンシーとデジタル主権の要件に準拠している場合に特に重要です。

複数の をオーケストレーション AWS のサービス して、組織のセキュリティとコンプライアンスのニーズを確保し、 を使用しAWS Control Tower、構成設定を定義してそれらからの逸脱を検出し、 を使用しAWS Config、 で規制と業界標準 AWS の使用とコンプライアンスを監査する機会を検討してくださいAWS Audit Manager。

Cloud governance for developers

その意味： デベロッパー向けのクラウドガバナンスのベストプラクティスを実装するには、Infrastructure as Code (IaC) を使用して作業の再現性と一貫性を確保し、セキュリティの脆弱性を検出するプロセスを確立します。

重要な理由： これにより、チームはガバナンスプロセスに自信を持ちながら迅速に行動できます。これにより、開発者はスタック全体にデプロイできる単一の信頼できるソース、レプリケート、再デプロイ、再利用できるインフラストラクチャ、インフラストラクチャとアプリケーションのバージョニングを一緒に制御できる機能、セルフサービスアクションを選択できます。

デベロッパー向けのクラウドガバナンスには、コードのセキュリティ脆弱性の検出も含まれます。これにより、コード品質の向上、重大な問題の特定、一貫したリリースパイプラインの確保、ブループリントを使用したプロジェクトの起動が可能になります。

AWS のサービス 同様の Service Catalog を使用して、事前に承認された infrastructure-as-code テンプレートをビルダーに提供する方法と、誰が、どこで、どのように使用できるかを決定する対応する IAM ポリシーを検討してください。

Scalability and flexibility

とは： クラウドガバナンスの対策がインフラストラクチャとシームレスに成長し、変化する要件に適応するのに役立つ を選択します AWS のサービス 。組織の成長とスピードを考慮してください。

重要な理由： スケーラビリティと柔軟性を考慮すると、クラウドガバナンスの配置が堅牢で応答性が高く、動的なビジネス環境をサポートできるようになります。

迅速なスケーリングを支援するために、 は、 AWS Organizations や などAWS のサービス、他のいくつかの の機能 AWS Control Tower を調整して AWS IAM Identity Center、ランディングゾーンを 1 時間以内に構築します。Control Tower は、ユーザーに代わってリソースを設定および管理します。

AWS Organizations では、複数のアカウントで 40 以上のサービスのリソースを管理できます。これにより、個々のアプリケーションチームはワークロードに固有のクラウドガバナンスのニーズを柔軟に管理し、一元化されたチームも可視化できます。

AWS クラウドガバナンスサービスを選択する

クラウドガバナンスオプションを評価する基準がわかったので、組織のニーズに適した AWS クラウドガバナンスサービスを選択する準備が整いました。次の表は、どのサービスがどの状況に最適化さ

れているかを示しています。これを使用して、組織やユースケースに最適なサービスを決定できます。

ユースケースのタイプ	いつ使用するか?	推奨サービス
要件の定義	AWS セキュリティおよびコンプライアンスドキュメントのオンデマンドダウンロードを提供します。	AWS Artifact
デプロイと運用	Infrastructure as Code を使用してクラウドプロビジョニングを高速化するには。	AWS CloudFormation
	理想的な構成設定を表し、AWS リソースがそこからドリフトしているかどうかを検出するには。	AWS Config
	組織のセキュリティとコンプライアンスのニーズを満たすと同時に、 AWS のサービスユーザーに代わって複数の を設定およびオーケストレーションするには。	AWS Control Tower
	複数の AWS アカウント を組織に統合するには、リソースの割り当て、アカウントのグループ化、ガバナンスポリシーの適用、一元的かつ大規模な管理に使用できます。	AWS Organizations
	サポートされている一連のセキュリティ標準でルールに対して自動チェックと継続的チェックを実行するには。	AWS Security Hub CSPM

ユースケースのタイプ	いつ使用するか?	推奨サービス
	誰が、どこで、どのように使用できるかを決定する、事前に承認された infrastructure-as-code テンプレートと対応する IAM ポリシーをビルダーに提供する。	Service Catalog
	マルチクラウドおよびハイブリッド環境で、 および のリソース AWS のend-to-endの管理を提供します。	AWS Systems Manager
測定と評価	AWS 使用状況を監査し、リスクと規制や業界標準への準拠を評価する。	AWS Audit Manager
	の運用およびリスク監査、ガバナンス、コンプライアンスを有効にするには AWS アカウント。	AWS CloudTrail
	AWS リソースと で実行しているアプリケーションを AWS リアルタイムでモニタリングするには。	Amazon CloudWatch
	AWS とオンプレミス環境全体でベンダーからのソフトウェアライセンスを一元管理します。	AWS License Manager
	ベストプラクティスに照らして使用状況と設定を評価する。	AWS Trusted Advisor

AWS クラウドガバナンスサービスを使用する

これで、各 AWS クラウドガバナンスサービスの動作と、どちらが適切かを明確に理解できたはずです。

を使用して、利用可能な AWS 各クラウドガバナンスサービスの詳細について調べる方法を検討するために、各サービスがどのように機能するかを調べるための経路を用意しました。以下のセクションでは、詳細なドキュメント、実践的なチュートリアル、その他のリソースへのリンクを提供します。

AWS Artifact

- の開始方法 AWS Artifact

  セキュリティおよびコンプライアンスレポートのダウンロード、法的契約の管理、通知の管理を行います。

  ガイドを詳しく見る »
- での契約の管理 AWS Artifact

  を使用して、アカウントまたは組織の契約 AWS マネジメントコンソール を確認、受諾、管理します。

  ガイドを詳しく見る »
- AWS パート 1 の監査の準備 – AWS Audit Manager、 AWS Configおよび AWS Artifact

  AWS のサービス サービスを使用すると、監査で使用される証拠の収集を自動化できます。

  ブログを読む »

AWS Audit Manager

- の開始方法 AWS Audit Manager

  AWS マネジメントコンソール、Audit Manager API、または を使用して Audit Manager を有効にします AWS CLI。

  ガイドを詳しく見る »
- 監査所有者向けチュートリアル: 評価の作成

  Audit Manager サンプルフレームワークを使用して評価を作成します。

チュートリアルの開始方法」

- 受任者向けチュートリアル: コントロールセットの確認

  Audit Manager の監査所有者によって共有されたコントロールセットを確認します。

  チュートリアルの開始方法」

AWS CloudTrail

- イベント履歴の表示

  CloudTrail をサポートするサービス AWS アカウント については、 の AWS API アクティビティを確認してください。

  チュートリアルの開始方法」
- 管理イベントをログに記録する証跡を作成する

  証跡を作成して、すべてのリージョンの管理イベントを記録します。

  チュートリアルの開始方法」

AWS Config

- AWS Config features

  設定履歴やスナップショットからカスタマイズ可能なルールやコンフォーマンスパックまで AWS Config、 のリソース追跡機能について説明します。

  ガイダンスを詳しく見る »
- AWS Config の仕組み

  サービスがリソースを検出して追跡し AWS Config、さまざまなチャネルを介して設定項目を配信する方法について詳しく説明します。

  ガイドを詳しく見る »
- リスクとコンプライアンスワークショップ

  AWS Config と AWS マネージド Config ルールを使用してコントロールを自動化します。

ワークショップの詳細 »

- AWS Config Rule Development Kit ライブラリ: 大規模なルールの構築と運用

  Rule Development Kit (RDK) を使用してカスタム AWS Config ルールを構築し、RDKLib でデプロイします。

  ブログを読む »

AWS Control Tower

- の開始方法 AWS Control Tower

  コンソールまたは APIs を使用して AWS Control Tower ランディングゾーンを設定する方法について説明します。

  ガイドを詳しく見る »

- AWS Control Tower コントロール管理ワークショップ

  AWS ベストプラクティスと一般的なコンプライアンスフレームワークに合わせて、マルチアカウント環境でガバナンスを設定する方法について説明します。

  ワークショップの詳細 »

- Amazon Bedrock と を使用したアカウント管理のモダナイズ AWS Control Tower

  セキュリティツールアカウントをプロビジョニングし、生成 AI を活用して AWS アカウントセットアップと管理プロセスを迅速化します。

  ブログを読む »

- を使用して適切に設計された AWS GovCloud (US) 環境を構築する AWS Control Tower

  組織単位 (OUs) と を使用して AWS ワークロードを管理するなど、 AWS GovCloud (US) リージョンでガバナンスを設定します AWS アカウント。

  ブログを読む »

AWS Organizations

- の開始方法 AWS Organizations

用語と概念の確認 AWS Organizations、一括請求の使用、組織ポリシーの適用など、 の使用を開始する方法について説明します。

ガイドを詳しく見る »

- 組織の作成と設定

  組織を作成し、2 つの AWS メンバーアカウントで設定します。

  チュートリアルの開始方法」

- 複数のアカウントを使用した AWS 環境の整理

  複数の を使用することで AWS アカウント 、ビジネスアプリケーションとデータを分離して管理し、Well-Architected フレームワークの AWS 柱全体で最適化する方法について説明します。

  ホワイトペーパーを読む »

- と連携するサービス AWS Organizations

  で使用できる AWS のサービス サービス AWS Organizations 、および組織全体レベルで各サービスを使用する利点を理解します。

  ガイドを詳しく見る »

- AWS Organizationsでの組織単位のベストプラクティス

  OU 構造と特定の実装例について、組織を構築する際の AWS ベストプラクティスの推奨アーキテクチャについて詳しく説明します。

  ブログを読む »

- AWS Organizations SCPs の設計上の考慮事項による運用上の優秀性の実現

  SCPs が組織内で作成された複数のアカウントでプロビジョニングされた AWS のサービス および リソースへのアクセスを制御する方法について説明します。

  ブログを読む »

AWS Security Hub CSPM

- 有効化 AWS Security Hub CSPM

スタンドアロンアカウントで AWS Security Hub CSPM AWS Organizations または で を有効にします。

ガイドを詳しく見る »

- クロスリージョン集約

  AWS Security Hub CSPM 結果を複数の集約リージョンから単一の集約リージョン AWS リージョン に集約します。

  ガイドを詳しく見る »

- AWS Security Hub CSPM ワークショップ

  AWS Security Hub CSPM と を使用して AWS 環境のセキュリティ体制を管理および改善する方法について説明します。

  ワークショップの詳細 »

- Security Hub の 3 つの繰り返しの使用パターンとデプロイ方法

  最も一般的な 3 つの AWS Security Hub CSPM 使用パターンと、検出結果を特定して管理するための戦略を改善する方法について説明します。

  ブログを読む »

AWS クラウドガバナンスリソースの詳細

アーキテクチャ図

セキュリティ、アイデンティティ、ガバナンス戦略の開発に役立つリファレンスアーキテクチャ図をご覧ください。

アーキテクチャ図を調べる

ホワイトペーパー

ホワイトペーパーでは、組織に最適なセキュリティ、アイデンティティ、ガバナンスサービスの選択、実装、使用に関するインサイトとベストプラクティスについて詳しく説明します。

ホワイトペーパーの詳細

ソリューション

これらのソリューションを使用して、セキュリティ、アイデンティティ、ガバナンス戦略をさらに開発および改善します。

ソリューションを詳しく見る

ドキュメント履歴

次の表に、この決定ガイドの重要な変更点を示します。このガイドの更新に関する通知については、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	ガイドが最初に公開されました。	2024 年 10 月 4 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。