



での VMware Cloud のアイデンティティとアクセスの管理 AWS

# AWS 規範ガイド



# AWS 規範ガイド: での VMware Cloud のアイデンティティとアクセスの管理 AWS

Copyright © 2024 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 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は、Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

# Table of Contents

序章 .....	1
対象者 .....	2
ターゲットを絞ったビジネス成果 .....	2
ID 管理の概要 .....	3
ID フェデレーションと SSO .....	4
一般的なベストプラクティス .....	5
VMware ID 管理サービス .....	7
VMware クラウドサービスコンソール .....	7
ID とアクセスの管理 .....	7
AWS レコメンデーション .....	8
VMware vCenter サーバー .....	9
ID とアクセスの管理 .....	9
AWS レコメンデーション .....	10
関連する VMware のサービス .....	12
VMware 上のクラウド AWS .....	12
ID とアクセスの管理 .....	13
AWS レコメンデーション .....	14
VMware NSX .....	14
ID とアクセスの管理 .....	15
AWS レコメンデーション .....	16
VMware ログの Aria オペレーション .....	17
ID とアクセスの管理 .....	17
AWS レコメンデーション .....	18
VMware Aria Operations for Networks .....	18
ID とアクセスの管理 .....	19
AWS レコメンデーション .....	19
VMware Aria オペレーション .....	19
ID とアクセスの管理 .....	20
AWS レコメンデーション .....	20
VMware ライブサイバーリカバリ .....	21
ID とアクセスの管理 .....	21
AWS レコメンデーション .....	22
VMware HCX .....	22
ID とアクセスの管理 .....	23

AWS レコメンデーション .....	23
VMware ライブサイトリカバリ .....	24
ID とアクセスの管理 .....	24
AWS レコメンデーション .....	25
サンプルグループとロール .....	26
次のステップ .....	31
リソース .....	32
関連 AWS リソース .....	32
VMware ドキュメント .....	32
VMware 上のクラウド AWS .....	32
VMware vCenter サーバーと vCenter シングルサインオン .....	32
VMware NSX .....	33
VMware HCX .....	33
VMware アリアと vRealize スイート .....	33
VMware ライブサイトリカバリ .....	33
VMware ライブサイバーリカバリ .....	33
ドキュメント履歴 .....	34
用語集 .....	35
# .....	35
A .....	36
B .....	38
C .....	40
D .....	44
E .....	48
F .....	50
G .....	51
H .....	53
I .....	54
L .....	56
M .....	57
O .....	61
P .....	64
Q .....	67
R .....	67
S .....	70
T .....	74

---

U .....	75
V .....	76
W .....	76
Z .....	77
.....	lxxix

# VMware Cloud on の ID とアクセスの管理 AWS

Richard Milner-Watts、Abdenour Kansab、Chris Porter、Amazon Web Services

Vern Bolinius、VMware

2024 年 9 月 ([ドキュメント履歴](#))

## 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

ID およびアクセス管理は、システムへのアクセスを、許可されたユーザーとアプリケーションのみに制限するという原則です。これには、必要なネットワークリソースのみにアクセスを制限することも含まれます。クラウド環境では、ID 管理とアクセス管理は通常、ユーザー、ユーザーグループ、アプリケーションの識別、認証、承認に使用するポリシーとサービスで構成されています。

VMware Cloud on AWS は VMware、で vSphere ベースのワークロードをサポートします AWS クラウド。このクラウドインフラストラクチャの設定、管理、バックアップ、モニタリング、分析には、多くの VMware サービスとツールを使用できます。ID とアクセスの管理に使用する機能と制御は、サービス間で異なります。このドキュメントでは、以下の VMware サービスの ID とアクセスを管理するためのベストプラクティスと推奨事項を提供します。

- VMware Aria オペレーション
- VMware ログの Aria オペレーション
- VMware Aria Operations for Networks
- VMware 上のクラウド AWS
- VMware クラウドサービスコンソール
- VMware HCX
- VMware NSX
- VMware ライブサイバーリカバリ
- VMware ライブサイトリカバリ
- VMware vCenter サーバー

このガイドでは、の VMware Cloud および関連 VMware サービスにおける ID とアクセス管理の概要 AWS とベストプラクティスについて説明します。各サービスの簡単な説明と、そのサービスの ID アクセスと管理に関する考慮事項についても説明します。また、Cloud VMware on の一部としてサービスを設定するための推奨事項も提供しています AWS。

### Important

このガイドで説明されている VMware サービスの多くは、他のクラウドまたはオンプレミス VMware ソリューションで使用されています。このガイドの推奨事項とベストプラクティスは、の VMware Cloud に固有のものであり、AWS。これらの推奨事項は、他の環境では適用されない場合があります。

## 対象者

このガイドは、クラウド環境またはハイブリッド環境で AWS に VMware Cloud を実装する責任を負うアーキテクトとセキュリティエンジニアを対象としています。

## ターゲットを絞ったビジネス成果

このガイドは以下を行う際に役立ちます。

1. VMware Cloud on および関連 VMware サービスのさまざまな ID AWS およびアクセス管理コントロールを理解する
2. VMware Cloud on を安全に運用するために推奨されるベストプラクティスに精通する AWS
3. 外部 ID プロバイダーによるフェデレーション認証で利用できるオプションを理解する

# ID 管理の概要

## 注意

2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

VMware では、ID、認証、承認の管理に、次の業界標準のコンセプトと ID の階層を使用しています。

- ユーザーとは、何らかの役割で特定の環境にアクセスする個人のことです。ローカルユーザーを作成したり、フェデレーションを使用して外部 ID プロバイダーのユーザーを認証したりできます。詳細については、「[ID フェデレーションと SSO](#)」を参照してください。
- グループは、ユーザーの集合を論理的にグループ化するメカニズムを提供します。これにより、それらのユーザーに一貫性のあるアクセス許可を提供でき、管理オーバーヘッドを軽減できます。ロールは、ユーザーまたはグループにアクセス許可を付与するために使用されます。詳細については、「[Roles and Permissions in the SDDC](#)」(VMware ドキュメント)を参照してください。
- VMware クラウドの組織は、1 つまたは複数の VMware サービスへのアクセスを制御します。ユーザーとグループは、組織内のサービスにアクセスするにはいずれかの組織に属している必要があります。[Identity Governance and Administration](#) の機能を有効にすると、フェデレーテッド ID はセルフサービスで VMware 組織への加入をリクエストできます。詳細については、「[VMware クラウドサービスコンソール](#)」を参照してください。

アクセス許可により特定のオブジェクトにアクセスできるようになります。またアクセス許可は、親オブジェクトから継承することも可能です。1 人のユーザーまたは 1 つのグループに重複する複数のアクセス許可が割り当てられている場合、最も制限の緩いものが適用されます。詳細については、「[Hierarchical Inheritance of Permissions](#)」を参照してください (VMware ドキュメント)。

これらの構造的要素を使用することで、最小特権のポリシーを採用し、ユーザーの要件に基づいてインフラストラクチャ内に論理的なアクセス境界を設定することができます。最小特権とは、ユーザーとアプリケーションに、タスクを実行するための必要最小限のアクセスのみを許可する原則のことです。不正アクセスが発生した場合は、この業界のベストプラクティスに従うことで、損害を与えたり機密データを盗んだりする攻撃者の能力を抑制できます。また、この原則に従うことで、承認済みのユーザーであってもアクセスすべきでないデータにはアクセスさせないようにすることができます。

必要なリソース以外はアクセスできないようにすれば、生産性も向上し、トラブルシューティングのサポートの必要性を減らすことができます。

VMware Cloud on を使用する場合 AWS、ID とアクセスを管理するための 2 つの主要なサービスとツール、[VMware クラウドサービスコンソール](#)と [VMware vCenter サーバー](#)。これらサービスの詳細については、本ガイドの後半では説明します。

## ID フェデレーションと SSO

多くの企業が、外部の ID プロバイダー (IdP) とのフェデレーションを設定したいと考えています。設定すると、ユーザーにシングルサインオン (SSO) のエクスペリエンスを提供できます。VMware Cloud と vCenter Server は、共にエンタープライズフェデレーションをサポートしています。

- VMware Cloud は Security Assertion Markup Language (SAML) 2.0 ベースをサポートし IdPs、Lightweight Directory Access Protocol (LDAP) をサポートしています。詳細については、「[What is enterprise federation and how does it work with VMware Cloud Services](#)」(VMware ドキュメント) を参照してください。
- VMware Cloud on で vCenter Server を操作する場合 AWS、外部 IdP を使用した vCenter Server へのフェデレーションは現在サポートされていません。使用できるのは組み込みの IdP のみです。こちらは LDAP を介した Microsoft Active Directory の使用をサポートしています。詳細については、「[Identity Sources for vCenter Server with vCenter Single Sign-On](#)」(VMware ドキュメント) を参照してください。

本ガイドで取り上げている、その他の関連する VMware サービスの中には、IdP からのダイレクトフェデレーションもサポートしているものがあります。ただし、すべてのサービスでフェデレーションを設定すると、ユーザーの管理ポイントが増え、管理が難しくなります。代わりに、VMware Cloud Services Console のグループとロールを使用すれば、共通の ID ソースを使用したり、他の VMware Cloud サービスのアクセス許可を設定したりできます。また、Hybrid Linked Mode を設定し、オンプレミスの vCenter Server インスタンスと同じ ID を使用することもできます。これにより、フェデレーションと ID の管理ポイントが 2 つのサービスまで減ります。Hybrid Linked Mode の詳細については、「[Configuring Hybrid Linked Mode](#)」(VMware ドキュメント) を参照してください。

# 一般的なベストプラクティス

## 注意

2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは引き続き、Broadcom を通じて利用できます。詳細については、 の AWS 担当者にお問い合わせください。

## Important

このガイドで説明する VMware サービスの多くは、他のクラウドやオンプレミスの VMware ソリューションでも使用されています。このガイドに記載する推奨事項とベストプラクティスは、VMware Cloud on AWS 専用です。これらの推奨事項は、他の環境では適用されない場合があります。

VMware クラウドインフラストラクチャへの ID とアクセスを管理するには、次の AWS 推奨事項を考慮してください。

- 最小特権のポリシーを適用します。ロールベースのアクセスコントロール (RBAC) を使って、ユーザーが自らの役割を果たすために必要となる、最小限のアクセス許可およびアクセス権限を付与します。
- アクセス許可は、できるだけ個々のユーザーではなくグループに付与します。
- ローカルユーザーを設定することは避けます。外部のフェデレーション ID プロバイダーに対してユーザーを認証します。
- すべてのユーザーに多要素認証を設定します。
- パスワードポリシーには、パスワードの強度とローテーションに関する要件を含めます。
- VMware の組織と関連サービスを管理者として完全に制御するための Break Glass の手順を文書化します。「Break Glass」は、ガラスを破って火災警報器を引くという意味から来る名称で、例外的な状況でも、承認済みおよび監査済みの手順を使って、管理者のアクセス権限をすばやく利用できるようにする方法を意味します。
- オンプレミスのデータセンターまたは複数の vCenter Server インスタンスを使用している場合は、Hybrid Linked Mode を使用してクラウドの vCenter Server インスタンスをオンプレミスの

vCenter Single Sign-On ドメインに接続します。これで、vSphere Client の単一のインターフェイスからクラウドとオンプレミス両方のリソースを管理できます。

- vCenter Server、HCX Cloud Manager、NSX Manager などの管理エンドポイントは、できるだけ、パブリックインターネットからではなく内部のネットワークからのみアクセスできるように設定します。
- 管理には、cloudadmin アカウントのようなローカルの認証情報は使用しません。このようなアカウントは、Break Glass 手順の際に使用できるよう確保しておきます。管理用のローカルユーザーアカウントを使って実行されたアクションは特定の個人に帰属することができないため、これらのアカウントは、説明責任を伴わずに変更を施す際などに使用します。
- ルートユーザーや管理ユーザーなどローカルアカウントのパスワードは堅牢な値に変更し、その認証情報は監査を受けるパスワードストアに安全に保管します。こうしたパスワードへのアクセスを許可する承認プロセスを設定します。
- ローカルの認証情報を長期間 (数か月以上など) 保存する場合は、認証情報をローテーションするプロセスを設定します (VMware HCX を使用してネットワークを拡張する場合など)。

これらの推奨事項は、VMware Cloud on のすべての VMware サービス設定に適用されます AWS。各サービスにおけるその他推奨事項については、本ガイドで後ほど解説します。

# VMware ID 管理サービス

## 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

VMware Cloud on を使用する場合 AWS、ID とアクセスを管理するための 2 つの主要なサービスとツール、[VMware クラウドサービスコンソール](#)と [VMware vCenter サーバー](#)。

## VMware クラウドサービスコンソール

[VMware クラウドサービスコンソール](#) (VMware ドキュメント) は、VMwareCloud on を含むVMware クラウドサービスポートフォリオの管理に役立ちます AWS。このサービスでは次のことが行えます。

- ユーザーやグループなどのエンティティの管理
- Live Cyber Recovery や VMware Aria Suite VMware などの他のクラウドサービスへのアクセスを制御する組織を管理する
- リソースやサービスへのロールの割り当て
- 組織にアクセスできるOAuthアプリケーションを表示する
- 組織のエンタープライズフェデレーションの設定
- Aria や VMware Cloud on VMware などのVMwareクラウドサービスの有効化とデプロイ AWS
- 請求とサブスクリプションの管理
- VMware サポートを受ける

## ID とアクセスの管理

VMware Cloud Services Console でユーザー、グループ、ロール、組織を適切に設定することで、最小特権のアクセスポリシーを実装できます。

このサービスの管理者ユーザーはVMwareクラウド環境全体のアクセス許可を変更し、請求情報などの機密情報にアクセスできるため、VMwareクラウドサービスコンソールへのアクセスを保護する

ことが重要です。請求やサポートなど、すべてのコンソール機能にアクセスするには、ユーザーを VMware Customer Connect プロファイル (旧称 MyVMware) にリンクする必要があります。

VMware クラウドサービスコンソールでは、次のタイプのロールを使用して、ユーザーとグループに許可を付与します。

- **組織ロール** – これらのロールは VMware クラウド組織に直接関係し、VMwareクラウドサービスコンソール内のアクセス許可を付与します。基本のロールは次の 2 つです。組織オーナーロールは、組織を管理するためのアクセス許可をすべて持っています。Organization メンバーロールには、VMwareクラウドサービスコンソールへの読み取りアクセス権があります。詳細については、[VMware「クラウドサービスで利用できる組織ロール」](#) (ドキュメント) を参照してください。VMware
- **サービスロール** – 特定のサービスを使用するための、アクセス許可の割り当てを許可するロールです。例えば、DR 管理サービスロールを持つエンティティは、専用サービスコンソールで VMware ライブサイバーリカバリを管理できます。組織内で利用可能なサービスはすべて、1 つ以上のサービスロールが関連付けられています。利用可能なサービスロールの詳細については、対象のサービスの VMware ドキュメントを参照してください。

VMware クラウドサービスコンソールは認証ポリシーをサポートしています。これらは、ログイン時にユーザーが 2 番目の認証トークンを提供する必要があることを規定できます。これは多要素認証 (MFA) とも呼ばれます。

このサービスでの ID とアクセスの管理の詳細については、[「Identity and Access Management」](#) (VMware ドキュメント) を参照してください。

## AWS レコメンデーション

[一般的なベストプラクティス](#)では、上の VMware クラウドの VMwareクラウドサービスコンソールを設定する際に、に加えて以下のことを AWS 推奨しています。

- 組織を作成するときは、VMwareCustomer Connect プロファイルと、vmwarecloudroot@example.com など、個人に属さない関連する会社の E メールアドレスを使用します。このアカウントはサービスあるいはルートアカウントとして取り扱います。また、使用状況を監査し、このメールアカウントへのアクセスは制限する必要があります。会社の ID プロバイダー (IdP) とのアカウントフェデレーションをすぐに設定し、ユーザーがこのアカウントを使用しなくても組織にアクセスできるようにします。このアカウントは、フェデレーション IdP で発生した問題に対処する、Break Glass の手順で使用するために確保しておきます。

- 組織のフェデレーテッド ID を使用して、VMware ライブサイバーリカバリなどの他のクラウドサービスへのアクセスを許可します。複数のサービスで使用しているユーザーやフェデレーションは、個別には管理しません。これにより、ユーザーの入社時あるいは退職時などに、複数のサービスへのアクセス管理が容易になります。
- 組織オーナーのロールは、むやみに割り当てないようにします。このロールを持つエンティティは、組織のあらゆる側面や関連するクラウドサービスへのフルアクセスを自らに付与できます。

## VMware vCenter サーバー

[VMware vCenter Server](#) (VMware ウェブサイト) は、VMware vSphere 環境を管理するための管理プレーンです。vCenter Server では、仮想マシンなどの vSphere リソースにアクセスしたり、や VMware HCX VMware Live Site Recovery などのアドオンにアクセスしたりできるエンティティを管理します。vSphere クライアントアプリケーションを使用して vCenter サーバーを管理します。vCenter Server では、次のことができます。

- 仮想マシン、VMware ESXi ホスト、v VMware SAN ストレージの管理
- vCenter Single Sign-On の設定と管理

オンプレミスのデータセンターがある場合は、Hybrid Linked Mode を使用して、クラウド vCenter サーバーインスタンスをオンプレミスの vCenter Single Sign-On ドメインにリンクできます。vCenter Single Sign-On ドメインに拡張リンクモードを使用して接続されている複数の vCenter サーバーインスタンスが含まれている場合、それらのインスタンスはすべてクラウドにリンクされます SDDC。このモードを使用すると、単一の vSphere クライアントインターフェイスからオンプレミスとクラウドのデータセンターを表示および管理し、オンプレミスのデータセンターとクラウドの間でワークロードを移行できます SDDC。詳細については、[「ハイブリッドリンクモードの設定」](#) (VMware ドキュメント) を参照してください。

## ID とアクセスの管理

VMware Cloud on の [ソフトウェア定義データセンター \(SDDCs\)](#) (VMware ウェブサイト) では AWS、vCenter サーバーを運用する方法はオンプレミスのと似ています SDDC。主な違いは、VMware Cloud on AWS がマネージドサービスであることです。したがって、VMware はホスト、クラスター、仮想マシンの管理など、特定の管理タスクを担当します。詳細については、[「クラウドの違い」](#) および [「グローバルアクセス許可」](#) (VMware ドキュメント) を参照してください。

VMware は のいくつかの管理タスクを実行するため SDDC、クラウド管理者は、オンプレミスデータセンターの管理者よりも必要な権限が少なくなります。で VMware Cloud を作成すると AWS

SDDC、cloudadmin ユーザーが自動的に作成され、[CloudAdmin](#) ロールが割り当てられます (VMware ドキュメント)。この権限のあるローカルユーザーアカウントを使用して、vCenter サーバーと vCenter Single Sign-On にアクセスできます。Cloud Services Console で VMware Cloud on AWS Administrator または Administrator (Delete Restricted) VMware サービスロールを持つユーザーは、cloudadmin ユーザーの認証情報を取得できます。CloudAdmin ロールには、上の VMware クラウドの vCenter サーバーで可能な最大アクセス許可があります AWS SDDC。このサービスロールの詳細については、[CloudAdmin 「権限」](#) (VMware ドキュメント) を参照してください。Cloudadmin ユーザーは、の VMware Cloud の vCenter Server で使用できる唯一のローカルユーザーです AWS。他のユーザーにアクセス権限を付与するときは外部の ID ソースを使用します。

vCenter Single Sign-On は、セキュリティトークン交換インフラストラクチャを提供する認証ブローカーです。ユーザーが vCenter Single Sign-On を認証すると、そのユーザーは、API 呼び出しを使用して vCenter サーバーおよびその他のアドオンサービスで認証するために使用できるトークンを受け取ります。cloudadmin ユーザーは、vCenter サーバーの外部 ID ソースを設定できます。詳細については、[vCenter 「Single Sign-On を使用する vCenter サーバーの Identity Sources」](#) (VMware ドキュメント) を参照してください。

vCenter Server では、次の 3 種類のロールを使用して、ユーザーとグループにアクセス許可を付与します。

- システムロール — このロールは編集や削除は行えません。
- サンプルロール — このロールは、頻繁に実行されるタスクの組み合わせとして機能します。これらのロールはコピー、編集、削除が可能です。
- カスタムロール — システムロールとサンプルロールが必要なアクセスコントロールを提供しない場合は、vSphere クライアントでカスタムロールを作成できます。既存のロールを複製して変更することもできれば、新たにロールを作成することもできます。詳細については、[vCenter 「サーバーカスタムロールの作成」](#) (VMware ドキュメント) を参照してください。

SDDC インベントリ内のオブジェクトごとに、ユーザーまたはグループに割り当てることができるロールは 1 つだけです。1 つのオブジェクトで、ユーザーまたはグループが、組み込みのロールの組み合わせを必要とする場合、2 つの選択肢があります。1 つ目の方法は、必要なアクセス許可を持つカスタムロールを作成することです。もう 1 つの方法は、2 つのグループを作成し、それぞれに組み込みのロールを割り当て、両方のグループにユーザーを追加することです。

## AWS レコメンデーション

では [一般的なベストプラクティス](#)、での VMware クラウド用 vCenter サーバーを設定する際に、に加えて以下のことを AWS 推奨しています AWS。

- cloudadmin ユーザーアカウントを使用して、Single Sign-On vCenter で外部 ID ソースを設定します。外部 ID ソースから、管理目的で使用するための適切なユーザーを割り当てて、cloudadmin ユーザーの使用は中止します。vCenter Single Sign-On を設定する際のベストプラクティスについては、[「Information Security and Access for vCenter Server」](#) (VMware ドキュメント) を参照してください。
- Client で vSphere、各 vCenter Server インスタンスの cloudadmin 認証情報を新しい値に更新し、安全に保存します。この変更は、VMware クラウドサービスコンソールには反映されません。例えば、Cloud Services Console で認証情報を表示すると更新前の値が表示されます。

 Note

このアカウントの認証情報が失われた場合、VMware サポートによって認証情報がリセットされます。

- アクセスに cloudadmin アカウント day-to-day を使用しないでください。このアカウントは、Break Glass 手順の一環として使用できるように確保しておきます。
- vCenter サーバーへのネットワークアクセスをプライベートネットワークのみに制限します。

## 関連する VMware のサービス

### 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

この章では、の VMware Cloud に関連する以下の VMware サービスの ID とアクセスを管理するためのベストプラクティスと推奨事項について説明します AWS。

- VMware クラウドサービスコンソールで管理されるサービス：
  - [VMware 上のクラウド AWS](#)
  - [VMware NSX](#)
  - [VMware ログの Aria オペレーション](#)
  - [VMware Aria Operations for Networks](#)
  - [VMware Aria オペレーション](#)
  - [VMware ライブサイバーリカバリ](#)
- VMware vCenter Server で管理されるサービス：
  - [VMware HCX](#)
  - [VMware ライブサイトリカバリ](#)

このガイドでは、各サービスの簡単な説明と、そのサービスの ID アクセスと管理コントロールについて説明し、そのサービスをの VMware クラウドの一部として設定するための AWS 推奨事項を示します AWS。

## VMware 上のクラウド AWS

### 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

[VMware Cloud on AWS](#) (VMware ドキュメント) は、オンプレミスvSphereの ベースの環境を に移行 AWS して拡張するのに役立つVMware、 と VMware によって共同で設計されたサービスです AWS クラウド。

このサービスへのアクセスを許可する組織に属している場合は、 VMware クラウドサービスコンソール AWS から の VMware クラウドにアクセスできます。VMware Cloud on では AWS、次のことができます。

- を作成および削除しますSDDCs。
- SDDC グループを管理します。
- ネットワークとクラスターパラメータを含む SDDCsを管理します。
- VMware vCenter サーバーの cloudadmin ユーザー認証情報にアクセスします。このユーザーの詳細については、本ガイドの「[VMware vCenter サーバー](#)」を参照してください。
- の cloud\_admin ユーザー認証情報にアクセスしますVMwareNSX。このユーザーの詳細については、本ガイドの「[VMware NSX](#)」を参照してください。
- Live Site Recovery や SDDCsなどのアドオンサービスを VMware 内で有効化してデプロイ VMwareしますHCX。
- HCX やVMwareライブサイトリカバリなどのアドオンサービスのコンソールにアクセスします。

## ID とアクセスの管理

VMware Cloud Services Console を使用して、 上の VMware Cloud の ID とアクセスを管理します AWS。VMware Cloud on では AWS、次のサービスロールを使用できます。

- 管理者 – このロールは、 の VMware Cloud へのフルアクセスを持ちます AWS。
- 管理者 (制限付き削除 ) — このロールは、SDDC削除オペレーションを除き AWS、 上の VMware Cloud へのフルアクセスを持ちます。
- NSX クラウド管理者
- NSX クラウド監査人

### Note

NSX Cloud Admin と NSX Cloud Auditor VMware は、 の使用に関連していますNSX。詳細については、「[VMware NSX](#)」を参照してください。

クラウドサービスポータル内の にアクセスするには、2つの管理者ロールのうちの1 SDDC つが必要です。2つの NSX クラウドロールのいずれかを持たないユーザーは、クラウドサービスポータル内のSDDCネットワークとセキュリティタブにアクセスできません。さらに、NSX管理者認証情報にアクセスすることもできません。

## AWS レコメンデーション

に加えて [一般的なベストプラクティス](#)、では、で VMware Cloud を設定するときに次のことを AWS 推奨しています AWS。

- 管理者にアクセス権限を付与するときは Administrator (Delete Restricted) ロールのみを使用する。を削除する必要がある場合は、ブレークグラスアクセス用に管理者ロールを予約します SDDC。
- ネットワークおよびファイアウォール設定へのアクセスを必要としないユーザーには、NSXロールを許可しないでください。詳細については、このガイドの「[VMware NSX](#)」を参照してください。
- cloudadmin のローカルユーザーアカウントのパスワードは、堅牢な値に変更し、その認証情報は、監査を受けるパスワードストアに安全に保管する。このパスワードは、vSphere ウェブクライアントを使用してVMware vCenter サーバーで変更できます。

## VMware NSX

### 注意

2024年4月30日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

[VMware NSX](#) (VMware ドキュメント) は、レイヤー2からレイヤー7までの Open Systems Interconnection (OSI) モデルを再現するネットワーク仮想化レイヤーを提供します。これには、切り替え、ルーティング、ファイアウォールなどの機能があります。には2つのバージョンがありますNSX。元のバージョン (NSX-V) では、vCenter サーバーもデプロイする必要があります。新しいバージョン (NSX-T) は、ハイブリッドアーキテクチャのサポートを可能にする vCenter Server からデカップリングされています。VMware Cloud on は NSX-T AWS を使用します。

NSXは、vSphere および v とともに SAN、上の VMware Cloud のコアコンポーネントです。NSX は、内のすべてのネットワーク機能を提供し、オーバーレイネットワーク SDDC とネットワークアンダーレイを形成する AWS ネイティブコンポーネント間のインタラクションを管理します。NSX は、を呼び出し NSX APIs で リソースを管理する vCenter サーバーや VMware などの他のサービスと緊密に連携 HCX しています。

NSX では、次の操作を行うことができます。

- スwitチングとルーティングの管理。
- ネットワークとパブリックインターネット VMs 間のインライン検査に分散ファイアウォールを使用するなど、ファイアウォールを管理する
- 仮想プライベートネットワークを管理する (VPNs )
- 動的ホスト設定プロトコル (DHCP) とドメインネームシステム (DNS) を設定する

クラウドサービス VMware コンソール NSX から、または専用の NSX Manager ウェブユーザーインターフェイス (UI) から にアクセスできます。NSX Manager ウェブ UI には、VMware クラウドサービスコンソールでは利用できないいくつかの追加機能があります。詳細については、[SDDC 「Network Administration with NSX Manager」](#) ( VMware ドキュメント) を参照してください。

Cloud VMware on NSX で にアクセスするときは、次の点に注意してください AWS。

- VMware Cloud Services Console NSX から にアクセスするには、VMware Cloud on AWS Administrator ロールを割り当てる必要があります。SDDC ネットワークとセキュリティタブ NSX で にアクセスできます。このロールの詳細については、本ガイドの「[VMware 上のクラウド AWS](#)」を参照してください。
- NSX Manager ウェブ UI を開くには、SDDC 設定タブのリンクを選択するか、SDDC 概要ページで Open NSX Manager を選択します。詳細については、「[Open NSX Manager](#)」( VMware ドキュメント) を参照してください。
- SDDC が Payment Card Industry Data Security Standard (PCIDSS) モードの場合、VMware クラウドサービスコンソールのネットワークとセキュリティタブ NSX から にアクセスすることはできません。NSX Manager ウェブ UI を使用する必要があります。

## ID とアクセスの管理

VMware クラウドサービスコンソールを使用して、への ID とアクセスを管理します VMware NSX。NSX の VMware クラウドでは AWS、次のサービスロールを使用できます。

- NSX Cloud Admin – このロールは、の VMware Cloud で VMware NSX 機能を管理できません AWS。
- NSX Cloud Auditor – このロールは NSX サービス設定とイベントを表示できますが、変更を加えることはできません。

#### Note

名前にかかわらず、これらのロールは VMware NSX クラウドサービスとは関係ありません。

次のユーザーは にアクセスできます NSX。

- cloud\_admin ローカルユーザー。組み込みの高特権ローカル NSX ユーザーです。NSX Cloud Admin ロールを持つユーザーは、このユーザーアカウントの認証情報にアクセスできます。同様の名前にもかかわらず、cloud\_admin ユーザーは cloudadmin@vmc.local vCenter Single Sign-On ローカルユーザーとは異なります。
- クラウドサービスコンソールで NSX Cloud Admin サービスロールまたは NSX Cloud Auditor VMware サービスロールのいずれかが割り当てられているユーザー。これらのユーザーは、VMware クラウドサービスコンソールユーザーまたは外部フェデレーティッドユーザーです。
- を通じて ID ソース NSX から へのアクセスが直接許可されているユーザー LDAP。

## AWS レコメンデーション

に加えて [一般的なベストプラクティス](#)、では、で VMware クラウド NSX 用に を設定するときに、次のことを AWS 推奨しています AWS。

- ネットワークとファイアウォールの管理は担当するが、の管理は担当しないユーザーがいる会社の場合は SDDCs、これらのユーザーにいずれかの NSX ロールを付与しますが、管理者ロールは付与しません。これらのユーザーは、NSX Manager ウェブ UI NSX から にアクセスする必要があります。
- cloud\_admin のローカルユーザーアカウントのパスワードは堅牢な値に変更し、その認証情報は、監査を受けるパスワードストアに安全に保管します。このパスワードを変更するには、VMware サポートに連絡する必要があります。
- 内で外部ユーザーに直接アクセス権を付与することは避けてください NSX。代わりに、VMware クラウドサービスコンソールでエンタープライズフェデレーションを設定し、ロールとグループを使用してこのサービスへのアクセスを許可します。

# VMware ログの Aria オペレーション

## 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

[VMware Aria Operations for Logs](#) (VMware ドキュメント)、以前の VMware vRealize Log Insight Cloud は、VMware によって生成されたログデータを視覚化およびクエリするのに役立つログストレージおよび分析ツールです SDDCs。VMware Aria Operations for Logs では、次のことができます。

- Operations のオンプレミスインスタンスとの統合 vRealize
- マシンで生成されたあらゆる種類のログデータの収集と分析。
- アラートを設定する
- 他の VMware サービスのログのモニタリングと分析

この一元化されたログ管理サービスには 2 つのバージョンがあります。VMware vRealize Log Insight は、内でアプライアンスとして実行できるオンプレミスバージョンです SDDC。VMware Aria Operations for Logs は software-as-a-service (SaaS) バージョンです。VMware Cloud on は、デフォルトのログ記録サービスとしてクラウドバージョン AWS を使用します。これは変更できません。オンプレミスのバージョンを使用するときは、ログをクラウドインスタンスからオンプレミスインスタンスに転送する必要があります。

VMware Aria Operations for Logs は、の VMware クラウドに含まれています AWS。組み込まれたバージョンでは、取り込みの容量と保存期間に制限があります。これらの制限は、必要に応じてプレミアムサブスクリプションにアップグレードすることで増やすことができます。詳細については、「[サブスクリプションと請求](#)」(VMware ドキュメント)を参照してください。

## ID とアクセスの管理

VMware クラウドサービスコンソールを使用して、ID と Aria Operations for Logs VMware へのアクセスを管理します。VMware Aria Operations for Logs は、フェデレーテッド ID や、VMware クラウドサービスコンソールで設定したグループなど、同じユーザーを使用します。このサービスのアクセス許可を付与するには、サービスロールを割り当てるか、Aria Operations for Logs VMware 内で

カスタムロールを設定できます。詳細については、[「サービスロール」](#) (VMware ドキュメント) を参照してください。

VMware vRealize ログインサイトには 2 つのデフォルトロールがあります。Administrator ロールにはフルアクセスとコントロールの権限があります。User ロールには読み取り権限があり、ダッシュボードを作成できます。カスタムロールを使用すると、特定のデータセットのみにアクセスを許可できます。これらのデータセットには、ユーザーが使用できるログデータを制限するフィルタが含まれています。詳細については、[「データセットの作成」](#) (ドキュメント) を参照してください。VMware

## AWS レコメンデーション

本ガイドに記載している「[一般的なベストプラクティス](#)」に従ってください。このサービスの ID とアクセスの管理に関して追加の推奨事項はありません。

## VMware Aria Operations for Networks

### 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

VMware 以前の VMware vRealize Network Insight Cloud である Aria Operations for Networks は、vRealize Network Insight の SaaS バージョンです。[VMware vRealize Network Insight](#) (VMware ドキュメント) は、ワークロードのトラフィックフローを理解するのに役立ちます。このサービスを使用すれば、ネットワークの問題を診断したり、ワークロードのセグメント化に役立つファイアウォールルールをモデル化したりできます。VMware Aria Operations for Networks では、次のことができます。

- ハイブリッド環境とマルチクラウド環境の確認。
- トラフィックフローのトラブルシューティングと分析。
- アプリケーションの検出と分析。
- ワークロード間の依存関係のマッピング。

このサービスには 3 つのバージョンがあります。VMware vRealize Network Insight は on-premises-only バージョンです。VMware Aria Operations for Networks は SaaS バージョンです。vRealize

Network Insight Universal は、オンプレミスソリューションまたはフェデレーティッドクラウド SaaS ソリューションとしてデプロイできます。すべてのバージョンは、の VMware Cloud と互換性があります AWS。

## ID とアクセスの管理

VMware Cloud Services Console を使用して、アイデンティティと Aria Operations for Networks VMware へのアクセスを管理します。VMware Aria Operations for Networks は、フェデレーティッド ID や、VMwareクラウドサービスコンソールで設定したグループなど、同じユーザーを使用します。VMware Aria Operations for Networks では、次のサービスロールを使用できます。

- Administrator — このロールにはフルアクセスとコントロールの権限があります。
- Member — このロールのアクセス権限は制限付きです。
- Auditor — このロールのアクセス権限は読み取り専用です。

## AWS レコメンデーション

本ガイドに記載している「[一般的なベストプラクティス](#)」に従ってください。このサービスの ID とアクセスの管理に関して追加の推奨事項はありません。

## VMware Aria オペレーション

### 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

[VMware Aria Operations](#) (VMware ドキュメント)、以前の VMware vRealize Operations Cloud は、VMwareCloud on のオペレーション管理プラットフォームです AWS。このサービスは、人工知能と機械学習 (AI/ML) を活用して、ハイブリッドクラウドのデプロイにおけるアプリケーションとインフラストラクチャの最適化、プランニング、スケールをサポートします。VMware Aria Operations では、次のことができます。

- パフォーマンスと容量の、AI/ML を活用した最適化に関する推奨事項の確認。
- コンプライアンスとリソース設定の管理。

- ユーザーの問題の解決やアラートへの対応など、トラブルシューティングに役立つツールへのアクセス。
- [Management Pack](#) (VMware ドキュメント) を使用して、このサービスのモニタリング、トラブルシューティング、修復機能を拡張する

このオペレーション管理サービスには 2 つのバージョンがあります。VMware vRealize オペレーションは、内でアプライアンスとして実行できるオンプレミスバージョンです SDDC。VMware Aria Operations は、Operations の software-as-a-service (SaaS) vRealize バージョンです。SaaS どちらのバージョンも の VMware Cloud と互換性があります AWS。VMware Cloud on AWS はマネージドサービスであり、一部のリソースへのアクセスが制限されているため、すべての vRealize オペレーション機能がサポートされているわけではありません。詳細については、[「既知の制限事項」](#) (VMware ドキュメント) を参照してください。

## ID とアクセスの管理

VMware クラウドサービスコンソールを使用して、Aria オペレーションへの ID VMware とアクセスを管理します。VMware Aria Operations は、VMware クラウドサービスコンソールで設定したフェデレーティッド ID を含む同じユーザーを使用します。このサービスのアクセス許可を付与するには、サービスロールを割り当てるか、Aria Operations VMware 内でカスタムロールを設定できます。使用可能なサービスロールの詳細については、[「ロールと権限」](#) (ドキュメント) を参照してください。VMware

組み込みロールには、管理者、GeneralUser の 3 つがあり ReadOnly、必要に応じて、特定のアクセス許可要件に合わせてカスタムロールを作成できます。グループを作成すると、複数ユーザーのアクセス許可を管理することに伴う管理オーバーヘッドを最小限に抑えられます。

オペレーションのオンプレミスバージョンはローカルユーザー VMware vRealize をサポートし、クラウドバージョンとオンプレミスバージョンの両方がフェデレーティッドユーザーをサポートします。ただし、ユーザーの外部 ID プロバイダーへのフェデレーションは、vRealize オペレーションのオンプレミスバージョンとクラウドバージョンによって異なります。オンプレミスバージョンでは、を介して外部 IdP からユーザーを直接フェデレーションすることも LDAP、vCenter サーバーでフェデレーションした ID を使用することもできます。クラウドバージョンでは、VMware クラウドサービスコンソールで設定したフェデレーティッドユーザーを含む同じユーザーを使用します。

## AWS レコメンデーション

[一般的なベストプラクティス](#) では、で VMware クラウドの VMware Aria オペレーションを設定する際に、に加えて以下のことを AWS 推奨しています AWS。

- ユーザーを直接フェデレーションすることは避けます。クラウドバージョンでは、VMwareCloud Services Console でユーザーをフェデレートし、ロールとグループを使用してこのサービスへのアクセスを許可します。このサービスのオンプレミスバージョンでは、認証されたソースの ID を使用するか、シングルサインオン (SSO) を有効にします。詳細については、「[認証ソース](#)」および「[シングルサインオンソースの設定](#)」(VMware ドキュメント)を参照してください。

## VMware ライブサイバーリカバリ

### 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

[VMware Live Cyber Recovery](#) (VMware ドキュメント) は、ディザスタリカバリに階層化されたアプローチを提供するサービスとしてのディザスタリカバリ (DRaaS) ソリューションです。特定のワークロードの要件を満たすように、目標復旧時点 (RPO) と目標復旧時間 (RTO) のコストとタイムスケールを調整できます。そうすることで、信頼性の高い保護と、ディザスタリカバリリソースの効率的な活用との間でバランスを取ることができます。VMware ライブサイバーリカバリでは、次のことができます。

- 仮想マシンのバックアップの作成。
- 耐久性の高いクラウドストレージへのバックアップの保管。
- オンデマンドからホットスタンバイまで、復旧する対象に合わせたデプロイ方法の柔軟な選択。
- カスタム RPOs とを設定する RTOs

## ID とアクセスの管理

VMware Cloud Services Console を使用して、VMware Live Cyber Recovery の ID とアクセスを管理します。VMware Live Cyber Recovery は、フェデレーテッド ID や、VMware クラウドサービスコンソールで設定したグループを含む同じユーザーを使用します。このサービスのアクセス許可を付与するには、VMware ライブサイバーリカバリサービスロールを割り当てるか、VMware ライブサイバーリカバリ内にカスタムロールを作成します。利用可能なサービスロールの詳細については、[VMware 「ライブサイバーリカバリのエンドユーザーロール」](#) (VMware ドキュメント) を参照してください。

VMware Live Cyber Recovery には、サービスの運用に使用できるいくつかの組み込みロールが含まれています。

- 管理者 - API トークンへのアクセスを除く、フルコントロール。
- Auditor — ユーザーインターフェースに読み取り専用でアクセスできます (ユーザー管理は除く)。コンプライアンスレポートへのアクセス権限があります。
- DR Admin — ディザスタリカバリ計画を作成、テスト、実行します。
- Backup Admin — 保護対象のサイトと保護グループを管理します。を復元するためのアクセス VMs。
- Plan Tester — ディザスタリカバリ計画を作成し、テスト復旧を実行します。
- SDDC 管理者 - を管理します SDDCs。

## AWS レコメンデーション

本ガイドに記載している「[一般的なベストプラクティス](#)」に従ってください。このサービスの ID とアクセスの管理に関して追加の推奨事項はありません。

## VMware HCX

### 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

[VMware HCX](#) (VMware ドキュメント) は、間のワークロードの移行を可能にするアプリケーション モビリティプラットフォームです SDDCs。VMware HCX は VMware Cloud on に含まれ AWS ており、ワークロードの移行に使用できます。VMware では HCX、次のことができます。

- 間でマルチサイトメッシュを設定する SDDCs
- HCX サイト間でネットワークを拡張する
- 仮想マシンの移行。

## ID とアクセスの管理

VMware vCenter サーバーを使用して、への ID とアクセスを管理しますVMwareHCX。VMware HCX では、vCenter サーバーやへのアクセスなど、リソースと移行を作成および管理するために、他の VMware サービスへのアクセスが必要ですNSX。VMware HCX には 2 つのコンポーネントサービスがあります。

- HCX Cloud Manager – VMwareクラウドサービスコンソールで、VMware HCX に対して を有効にしますSDDC。これにより、選択した 内に HCX Cloud Manager アプライアンスがインストールされますSDDC。詳細については、[vSphere クライアント \(ドキュメント\) の HCX 「インストーラ OVA のデプロイ」](#) を参照してください。VMwareデプロイ後、vCenter Server cloudadmin 認証情報を使用して HCX Cloud Manager サービスにアクセスできます。
- HCX コネクタ — HCX Connector Open Virtualization Archive (OVA) ファイルは、HCXCloud Manager サービスを通じて取得できます。このファイルを使用して、任意の vCenter Server インスタンスに HCX Cloud Manager アプライアンスをインストールします。これにより、そのインスタンスが VMware の移行ソースとして設定されますHCX。各HCXコネクタインスタンスには、独自の管理者認証情報とルート認証情報があります。

両方のコンポーネントサービスをデプロイしたら、vCenter サーバーVMwareHCX経由で にアクセスできます。Administrators vCenter Single Sign-On グループには、HCX管理者ロールが自動的に付与されます。をインストールすると、Single Sign-On vCenter に多くのロールと権限HCXが追加されます。これらを使用して、さまざまなタイプのユーザーに基づいてHCX、VMware のきめ細かなアクセスコントロールを作成します。

## AWS レコメンデーション

に加えて[一般的なベストプラクティス](#)、では、で VMware クラウドVMwareHCX用に を設定するとき、次のことを AWS 推奨しています AWS。

- Gateway Firewall ルールを使用して、HCXCloud Manager サービスへのネットワークアクセスを制限します。
- オンプレミスの HCX Connector 管理者とルートユーザーの認証情報を安全に保存します。自社のポリシーに従ってこれらの認証情報をローテーションすることを検討します。VMware は Cloud HCX Manager に代わってこれらの認証情報を管理します。
- オンプレミスのHCXコネクタインスタンスの場合は、さまざまなタイプのHCXユーザーのニーズに合ったカスタムHCXロールを作成することを検討してください。例えば、を設定して管理する

ユーザーにはより寛容なロールを作成し HCX、移行のみを管理するユーザーにはより寛容なロールを作成します。

- Cloud VMware on VMwareHCX とペアリングする場合は AWS、cloudadmin ユーザーを使用する必要があります。
- HCX Cloud と VMware Cloud on をペアリングする場合 AWS、VMwareCloud on AWS SDDC と Active Directory 間の認証はサポートされていません。詳細については、[「\[VMC on AWS\] AD unsupported for HCX Cloud to Cloud setup」](#) (VMware ナレッジベース記事 90433) を参照してください。

## VMware ライブサイトリカバリ

### 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

[VMware Live Site Recovery](#) (VMware ドキュメント) は、オンプレミス環境向けの VMware Site Recovery Manager サービスに基づく、サービスとしてのオンデマンドのディザスタリカバリ (DRaaS) ソリューションです。VMware Live Site Recovery では、次のことができます。

- レプリケーション、オーケストレーション、自動化の実装を通じて、サイトに障害が発生した場合にワークロードを保護する。
- 保護に役立つ end-to-end ディザスタリカバリソリューションを作成する SDDCs

## ID とアクセスの管理

VMware vCenter サーバーを使用して、VMware Live Site Recovery への ID とアクセスを管理します。VMware Live Site Recovery は、仮想マシンのレプリケーションや電源オフなど、ユーザーに代わってオペレーションを実行します。VMware Live Site Recovery は、ロールと権限を使用して、適切なアクセス許可を持つユーザーのみが、リカバリプランのすべてのステップを実行するなど、リカバリオペレーションを実行できるようにします。

詳細については、[VMware 「ライブサイトリカバリの権限、ロール、アクセス許可」](#) (ドキュメント) を参照してください。VMware

フェデレーテッド ID を使用して vCenter サーバーにアクセスする場合は、Hybrid Linked Mode を使用してこれらのグループにエンティティを追加する必要があります。詳細については、「[ハイブリッドリンクモードの設定](#)」(VMware ドキュメント)を参照してください。

## AWS レコメンデーション

[一般的なベストプラクティス](#)では、での VMware Cloud の VMware ライブサイトリカバリを設定する際に、に加えて以下のことを AWS 推奨しています AWS。

- ソースサイトとターゲットサイトの両方で、ユーザーに同じロールが割り当てられていることを確認します。これにより、保護されたオブジェクトと復旧したオブジェクトに同じアクセス許可が付与されます。
- Hybrid Linked Mode を使用して、vCenter サーバー内のフェデレーテッド ID のロール割り当てを管理します。
- VMware Live Site Recovery は、内でのみプライベート IP アドレスを使用します SDDC。に合わせて [一般的なベストプラクティス](#)、Cloud VMware on AWS がプライベート IP アドレスに vCenter 解決されていることを確認します。

## サンプルグループとロール

### 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

次の表は、で VMware Cloud を使用するための ID とアクセスの管理戦略の例を示しています AWS。ユーザーペルソナ、ペルソナがアクセスする必要がある VMware サービス、組織とグループのメンバーシップ、割り当てられたロール、使用されるアイデンティティのタイプ (ローカルユーザーやフェデレーテッドアイデンティティなど) の概要を説明します。この表を出発点として、このガイドで推奨されているベストプラクティスに従った企業戦略を設計してください。

ユーザーペルソナ	アクセスしたサービス	VMware クラウドサンプルグループ名	VMware クラウドサービスロール	vCenter Single Sign-On サンプルグループ名	vCenter シングルサインオンロール	アイデンティティソース
組織のブレイクグラス	VMware クラウドサービスコンソール	なし	組織の所有者	なし	なし	ローカルユーザー (サービスアカウントの E メールアドレス)
VMware 管理者	VMware クラウドサービスコンソール vCenter サーバー	vmware_admins	組織の所有者	vmware_admins	管理者	フェデレーション ID プロバイダー

ユーザーペ ルソナ	アクセスし たサービス	VMware ク ラウドサン プルグルー プ名	VMware ク ラウドサー ビスロー ル	vCenter Single Sign-On サ ンプルグ ループ名	vCenter シ ングルサイ ンオンロー ル	アイデン ティティソ ース
	HCX  VMware ラ イブサイ トリカバリ  VMware ラ イブサイ バーリカバ リ  vRealize オ ペレーショ ン					
バックアッ プ管理者	vCenter サーバー	なし	なし	vmware_ba ckups	パワーユー ザー	フェデレー ション ID プロバイ ダー

ユーザーペ ルソナ	アクセスし たサービス	VMware ク ラウドサン プルグルー プ名	VMware ク ラウドサー ビスロール	vCenter Single Sign-On サ ンプルグ ループ名	vCenter シ ングルサイ ンオンロー ル	アイデン ティティソ ース
ディザスタ リカバリ管 理者	vCenter サーバー  VMware ク ラウドサー ビスコン ソール  VMware ラ イブサイト リカバリ  VMware ラ イブサイ バーリカバ リ	vmware_dr	組織のメン バー  DR 管理者  DR SDDC 管理者	vmware_dr	SrmAdmini strator  HmsCloudA dmin	フェデレー ション ID プロバイ ダー
VMware 演 算子	VMware ク ラウドサー ビスコン ソール  vCenter サーバー  HCX  vRealize オ ペレーショ ン	vmware_op s	組織のメン バー  vROps 管 理者	vmware_op s	パワーユー ザー	フェデレー ション ID プロバイ ダー

ユーザーペ ルソナ	アクセスし たサービス	VMware ク ラウドサン プルグルー プ名	VMware ク ラウドサー ビスロール	vCenter Single Sign-On サ ンプルグ ループ名	vCenter シ ングルサイ ンオンロー ル	アイデン ティティソ ース
ネットワー クチーム	VMware ク ラウドサー ビスコン ソール  vCenter サーバー	vmware_ne tworks	組織のメン バー  NSX クラ ウド管理者	vmware_ne tworks	Readonly	フェデレー ション ID プロバイ ダー
セキュリ ティチーム	VMware ク ラウドサー ビスコン ソール  vCenter サーバー  HCX (一時 的なアクセ ス)  VMware ラ イブサイト リカバリ  VMware ラ イブサイ バーリカバ リ  vRealize オ ペレーショ ン	vmware_se curity	組織のメン バー  vROps ReadOnly	vmware_se curity	Readonly	フェデレー ション ID プロバイ ダー

ユーザーペ ルソナ	アクセスし たサービス	VMware ク ラウドサン プルグルー プ名	VMware ク ラウドサー ビスロール	vCenter Single Sign-On サ ンプルグ ループ名	vCenter シ ングルサイ ンオンロー ル	アイデン ティティソ ース
監査人	VMware ク ラウドサー ビスコン ソール  vCenter サーバー	vmware_au dit	組織のメン バー	vmware_au dit	Readonly	フェデレー ション ID プロバイ ダー

## 次のステップ

### 注意

2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、 の AWS 担当者にお問い合わせください。

このガイドでは、VMware Cloud on および関連する VMware VMware サービスのアイデンティティ AWS とアクセスを管理するために推奨されるベストプラクティスについて説明しました。これらの推奨事項は、クラウドおよびハイブリッドクラウドのインフラストラクチャを保護し、不正アクセスを阻止するように設計されているだけでなく、それらのスケール性と効率性を高めるようにも設計されています。ユーザーをグループに割り当てた後にロールをグループに割り当てると、アクセス許可をより迅速に付与または制限することができ、ユーザーを個別に設定することに伴うオーバーヘッドを最小限に抑えることができます。また、外部の ID プロバイダーとのフェデレーション、および vCenter Single Sign-On を使用することで、シームレスなシングルサインオンエクスペリエンスをユーザーに提供できます。

ご自身の会社に適した ID とアクセスの管理戦略を設計するには、[サンプルグループとロール](#) の表を参照してください。本ガイドで推奨事項を確認した後は、[リソース](#) セクションに記載されているリンクをご確認いただくことをお勧めします。これらのリソースは、VMware Cloud サービスの詳細と、本ガイドで解説しているベストプラクティスの設計方法について学ぶのに役立ちます。

# リソース

## 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

## 関連 AWS リソース

- [VMware Cloud on AWS の概要と運用モデル](#)
- [Cloud on VMware のワークロードのディザスタリカバリオプション AWS](#)
- [VMware Cloud on のストレージオフロードオプションの設定 AWS](#)
- [VMware Cloud VMware SDDC on を使用してに AWS をデプロイする AWS](#)
- [AWS を使用してで VMware クラウドVMwareSDDCに移行する VMware HCX](#)

## VMware ドキュメント

### VMware 上のクラウド AWS

- [VMware Cloud Services を使用したエンタープライズ フェデレーションの設定](#)
- [VMware クラウドサービスの Identity and Access Management](#)

### VMware vCenter サーバーと vCenter シングルサインオン

- [での認可について vSphere](#)
- [vSphere 上の VMware クラウドでの 管理 AWS](#)
- [vSphere vCenter Single Sign-On による認証](#)
- [vCenter Single Sign-On アイデンティティソースの設定](#)
- [Hierarchical Inheritance of Permissions](#)
- [vCenter サーバーの情報セキュリティとアクセス](#)
- [vSphere 共通タスクに必要な権限](#)

## VMware NSX

- [NSX 管理ガイド](#)
- [NSX-T データセンターの情報セキュリティとアクセス](#)

## VMware HCX

- [VMware HCX ドキュメント](#)
- [VMware HCX ユーザーアカウントとロールの要件](#)

## VMware アリアと vRealize スイート

- [VMware vRealize オペレーションドキュメント](#)
- [vRealize Operations Cloud でのロールと権限](#)
- [VMware vRealize ログインサイトのデータセット](#)
- [ログの VMware Aria オペレーションの開始方法](#)
- [VMware クラウドサービスのドキュメント](#)
- [vRealize ネットワークインサイトユーザー管理](#)

## VMware ライブサイトリカバリ

- [VMware ライブサイトリカバリのドキュメント](#)
- [VMware ライブサイト復旧の権限、ロール、アクセス許可](#)

## VMware ライブサイバーリカバリ

- [VMware ライブサイバーリカバリドキュメント](#)
- [VMware ライブサイバーリカバリのエンドユーザーロール](#)

# ドキュメント履歴

## 注意

2024 年 4 月 30 日以降、の VMware Cloud AWS は AWS またはそのチャネルパートナーによって再販されなくなります。このサービスは、引き続き Broadcom を通じて利用できます。詳細については、の AWS 担当者にお問い合わせください。

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。今後の更新について通知を受ける場合は、[RSSフィード](#) をサブスクライブできます。

変更	説明	日付
<a href="#">VMware サービス内容</a>	VMware クラウドディザスタリカバリをVMwareライブサイバーリカバリに置き換え、VMwareサイトリカバリをVMwareライブサイトリカバリに置き換えました。詳細については、 <a href="#">VMware「ライブリカバリリリースノート」</a> を参照してください。	2024 年 9 月 4 日
<a href="#">VMware HCX アクセス</a>	で VMware クラウドVMwareHCXの を設定するための <a href="#">AWS 推奨事項</a> を更新しました AWS。	2023 年 6 月 5 日
<a href="#">初版発行</a>	—	2022 年 11 月 3 日

# AWS 規範的ガイドの用語集

以下は、AWS 規範的ガイドが提供する戦略、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します。
- 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にある程度の最適化を導入します。例: オンプレミスの Oracle データベースをの Oracle 用 Amazon Relational Database Service (Amazon RDS) に移行します AWS クラウド。
- 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 に移行します。
- 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: オンプレミスの Oracle データベースをの EC2 インスタンス上の Oracle に移行します AWS クラウド。
- 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。サーバーを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移行します。例: の移行 Microsoft Hyper-V アプリケーション 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。
- 使用停止 — 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コントロール」](#)を参照してください。

## 抽象化されたサービス

[「マネージドサービス」](#)を参照してください。

## ACID

[原子性、一貫性、分離性、耐久性](#)を参照してください。

## 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](#) よりも柔軟ですが、より多くの作業が必要です。

## 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の方法。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

行のグループに対して動作し、グループの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](#)を参照してください。

## AIOps

[「人工知能オペレーション」](#)を参照してください。

## 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。

### アプリケーションコントロール

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](#)の需要要素であり、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?](#)」を参照してください。

### 人工知能オペレーション (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。AIOps が移行戦略で AWS どのように使用されるかの詳細については、「[オペレーション統合ガイド](#)」を参照してください。

### 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。

### アトミック性、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コントロール (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 ( [ABAC](#) ) [ドキュメント](#)の「[の AWS IAM](#)」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。

## アベイラビリティゾーン

他のアベイラビリティゾーンの障害から 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 内の個別の場所。

## 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 ののに役立つ、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分類します。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 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

個人または組織に混乱や損害を与えることを目的とした [ボット](#)。

## BCP

[事業継続計画](#)を参照してください。

## 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 で動作グラフを使用して、失敗したログオン試行、不審な API 呼び出し、および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 [Data in a behavior graph](#) 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。 [エンディアンネス](#) も参照してください。

## 二項分類

バイナリ結果 (2 つの可能なクラスのうちの一つ) 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

2 つの異なる同一の環境を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他の環境 (グリーン) で実行します。この戦略は、影響を最小限に抑えながら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インタラクション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、有益または有益なボットもあります。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ているものがあります。

## ボットネット

[マルウェア](#) に感染し、[ボット](#) のヘルダーまたはボットオペレーターとして知られる 1 人の当事者による管理下にあるボットのネットワーク。ボットは、ボットとその影響をスケールするための最もよく知られているメカニズムです。

## 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なら、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、[「ブランチについて」](#) (GitHub ドキュメント) を参照してください。

## ブレイクグラスアクセス

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なります。詳細については、Well-Architected [ガイド](#) の「[ブレイクグラス手順の実装](#)」インジケータ AWS を参照してください。

## ブラウフィールド戦略

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、ホワイトペーパー [AWSでのコンテナ化されたマイクロサービスの実行](#) 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。

## 事業継続計画 (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。

## Canary デプロイ

エンドユーザーへのバージョンの低速かつ段階的なリリース。自信が持てたら、新しいバージョンをデプロイし、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

[「データキャプチャの変更」](#) を参照してください。

## データキャプチャの変更 (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、同期を維持するためにターゲットシステムの変更を監査またはレプリケートするなど、さまざまな目的で使用できます。

## 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、システムの回復力をテストします。[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](#) テクノロジー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 に移行するときに通常実行する 4 つのフェーズ AWS クラウド :

- 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
- Foundation – クラウド導入を拡大するための基本的な投資 (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。これらが AWS 移行戦略とどのように関連しているかについては、[「移行準備ガイド」](#) を参照してください。

## CMDB

[「設定管理データベース」](#) 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、次のようなものがあります。GitHub または Bitbucket Cloud。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動画などのビジュアル形式から情報を分析および抽出する [AI](#) の分野。例えば、 はオンプレミスのカメラネットワークに CV を追加するデバイス AWS Panorama を提供し、Amazon SageMaker は CV の画像処理アルゴリズムを提供します。

## 設定ドリフト

ワークロードの場合、設定は想定状態から変化します。これにより、ワークロードが非準拠になる可能性があり、通常は段階的かつ意図的ではありません。

## 設定管理データベース (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、移行のポートフォリオ検出および分析段階で CMDB のデータを使用します。

## 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 とリージョン、または組織全体に 1 つのエンティティとしてデプロイできます。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 is commonly described as a pipeline. CI/CD は、プロセスの自動化、生産性の向上、コード品質の向上、より迅速な提供に役立ちます。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

一元的な管理とガバナンスにより、分散型の分散データ所有権を提供す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。信頼できる ID のみが、期待されるネットワークから信頼できるリソースにアクセスしていることを確実にします。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。

## データの事前処理

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。データの事前処理とは、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通常、大量の履歴データが含まれており、クエリや分析によく使用されます。

## 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る。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。

## ディープラーニング

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。

## defense-in-depth

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

ティの手法。この戦略を採用するときは AWS、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て、リソースの安全性を確保します。例えば、a defense-in-depth 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で利用できるサービス](#)を参照してください。

## デプロイメント

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、Implementing security controls on AWSの[Detective controls](#)を参照してください。

## 開発値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、もともとリーンな製造プラクティス向け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ます。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](#)では、ファクトテーブル内の量的データに関するデータ属性を含む小さなテーブル。ディメンションテーブル属性は通常、テキストフィールドまたはテキストのように動作する

離散数値です。これらの属性は、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よく使用されます。

## 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)

[災害](#)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に使用する戦略とプロセス。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 (ポストン: 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については、「[コンテナと Amazon Word API Gateway を使用してレガシー Microsoft ASP.NET \(ASMX\) ウェブサービスを段階的にモダナイズする](#)」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逸脱の追跡。例えば、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 ガバナンス要件のコンプライアンスに影響を与える可能性のある[ランディングゾーンの変更を検出](#)したりできます。

## DVSM

「[開発値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、応答時間を短縮できます。

### 電子データ交換 (EDI )

組織間の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プロセス。

### 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

Virtual Private Cloud (VPC) 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の作成](#)」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利用できる、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、サマリー統計を計算し、データの視覚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

[星スキーマ](#)の中央テーブル。事業運営に関する量的データを保存します。通常、ファクトテーブルには、メジャーを含む列とディメンションテーブルへの外部キーを含む列の2種類の列が含まれます。

### フェイルファスト

頻繁で段階的なテストを使用して開発ライフサイクルを短縮する哲学。これはアジャイルアプローチの重要な部分です。

### 障害分離の境界

では AWS クラウド、アベイラビリティゾーン、コントロールプレーン AWS リージョン、データプレーンなどの境界で、障害の影響を制限し、ワークロードの耐障害性の向上に役立ちます。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 Explanations (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として表されます。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

同様のタスクを実行するように求める前に、タスクと必要な出力を示す少数の例を [LLM](#) に提供します。この手法は、プロンプトに埋め込まれた例 (ショット) からモデルが学習するコンテキスト内学習のアプリケーションです。少数ショットプロンプトは、特定のフォーマット、推論、またはドメイン知識を必要とする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コントロール」](#) を参照してください。

### きめ細かなアクセスコントロール (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

段階的なアプローチを使用するのではなく、[変更データキャプチャ](#)による継続的なデータレプリケーションを使用して、可能な限り短い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)

一般化データとラベルなしデータの大規模なデータセットでトレーニングされている大規模な深層学習ニューラルネットワーク。FMsは、言語の理解、テキストと画像の生成、自然言語での会話など、さまざまな一般的なタスクを実行できます。詳細については、[「基礎モデルとは」](#) を参照してください。

## G

### 生成 AI

大量のデータに対してトレーニングされ、シンプルなテキストプロンプトを使用してイメージ、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る [AI](#) モデルのサブセット。詳細については、[「生成 AI とは」](#) 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)

Amazon CloudFront では、特定の国のユーザーがコンテンツディストリビューションにアクセスできないようにするオプションです。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分散の制限」](#)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 ワークフローはレガシーと見なされ、[トランクベースのワークフロー](#)はモダンで推奨されるアプローチです。

### ゴールデンイメージ

システムまたはソフトウェアの新しいインスタンスをデプロイするためのテンプレートとして使用されるシステムまたはソフトウェアのスナップショット。例えば、製造では、ゴールデンイメージを使用して複数のデバイスにソフトウェアをプロビジョニングし、デバイスの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 (OUs) 全体のリソース、ポリシー、コンプライアンスの管理に役立つ大まかなルール。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、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。](#)

### ハイアベイラビリティ (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に使用されるデータセットから保留されている、ラベル付きの履歴データの一部。ホールドアウトデータを使用してモデル予測をホールドアウトデータと比較することで、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

ソースデータベースを、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) に移行します。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。緊急性のため、通常、ホットフィックスは一般的な DevOps リリースワークフローの外部で行われます。

## 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 CPU およびメモリ使用量が 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

[「産業モノのインターネット」](#) 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

既存のインフラストラクチャを更新、パッチ適用、または変更するのではなく、本番環境のワークロードに新しいインフラストラクチャをデプロイするモデル。イミュータブルなインフラストラクチャは、本質的に [ミュータブルなインフラストラクチャ](#) よりも一貫性、信頼性、予測性が高くなります。詳細については、AWS 「Well-Architected フレームワーク」の「[イミュータブルインフラストラクチャを使用したデプロイ](#)」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 (インGRESS) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション外からの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 セキュリティリファレンスアーキテクチャ](#) 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VPCsを使用してネットワークアカウントを設定することをお勧めします。

## 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](#) によって導入された用語は、接続、リアルタイムデータ、自動化、分析、AI/ML の進歩によるビジネスプロセスのモダナイゼーションを指します。

## 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。

## 産業モノのインターネット (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、[「産業モノのインターネット \(IIoT\) 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。

## 検査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 セキュリティリファレンスアーキテクチャ](#)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VPCsを使用してネットワークアカウントを設定することをお勧めします。

## 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、「[AWS による機械学習モデルの解釈可能性](#)」を参照してください。

## IoT

「[モノのインターネット](#)」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

## ラベルベースのアクセスコントロール (LBAC )

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ている必須アクセスコントロール (MAC) の実装。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)

大量のデータに基づいて事前トレーニングされた深層学習 AI モデル。LLM は、質問への回答、ドキュメントの要約、テキストの他の言語への翻訳、文の完了など、複数のタスクを実行できます。詳細については、[LLMs とは](#) 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

[「ラベルベースのアクセスコントロール」](#) 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 [「最小特権の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

[「7R」](#) 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。[エンディアンネス](#) も参照してください。

## 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またはプライバシーを侵害するように設計されているソフトウェア。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、不正アクセスにつながる可能性があります。マルウェアの例としては、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 のサービスが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、ユーザーが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する。Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB は、マネージドサービスの例です。これら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、制御するためのソフトウェアシステム。これにより、生産現場の生産物が完成した製品に変換されます。

## MAP

[「移行促進プログラム」](#)を参照してください。

## メカニズム

ツールを作成し、ツールの採用を推進し、調整のために結果を検査する完全なプロセス。メカニズムは、動作中にそれ自体を強化して改善するサイクルです。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。

## メッセージキューイングテレメトリトランスポート (MQTT)

リソースに制約のある IoT デバイス用の、[パブリッシュ/サブスクライブ](#)パターンに基づく軽量な machine-to-machine (M2M) 通信プロトコル。

## マイクロサービス

明確に定義された APIs を介して通信し、通常は小規模で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。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、軽量な APIs 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)

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。組織がクラウドへの移行のための強固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ちます。MAP には、従来の移行を体系的に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ための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と所有者、移行エンジニア、デベロッパー、スプリントに取り組む 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には、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 アプリケーション移行サービスを使用して Amazon EC2 への移行をリホストします。

## 移行ポートフォリオ評価 (MPA )

に移行するためのビジネスケースを検証するための情報を提供するオンラインツール AWS クラウド。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) と移行計画 (アプリケーションデータ分析とデータ収集、アプリケーショングループ化、移行の優先順位付け、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](#)の最初のフェーズです。

## 移行戦略

ワークロードを に移行するために使用するアプローチ AWS クラウド。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、「」の「[アプリケーションをモダナイズするための戦略 AWS クラウド](#)」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、[「」の「アプリケーションのモダナイゼーション準備状況の評価 AWS クラウド」](#)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

[「移行ポートフォリオ評価」](#)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。

### ミュータブルインフラストラクチャ

本番ワークロードの既存のインフラストラクチャを更新および変更するモデル。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](#)をベストプラクティスとして使用することを推奨しています。

## O

### OAC

[「オリジンアクセスコントロール」](#)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

[「組織の変更管理」](#) 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

[「オペレーションの統合」](#) を参照してください。

## OLA

[「運用レベルの契約」](#) 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。

## オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

産業用オートメーション用の A machine-to-machine (M2M) 通信プロトコル。OPC-UA は、データの暗号化、認証、認可スキームを備えた相互運用性標準を提供します。

## 運用レベルの契約 (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 IT グループが相互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 )

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問のチェックリストと関連するベストプラクティス。詳細については、AWS Well-Architected フレームワークの [「運用準備状況レビュー \(ORR \)」](#) を参照してください。

## 運用テクノロジー (OT)

物理環境と連携して産業運用、機器、インフラストラクチャを制御するハードウェアおよびソフトウェアシステム。製造では、OT と情報技術 (IT) システムの統合が、[Industry 4.0](#) トランスフォーメーションの主要な焦点です。

## 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 内のすべてのイベントをログ AWS CloudTrail に記録すること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、変化の採用を加速し、移行に伴う問題に対処し、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や戦略に備え、移行するのに役立ちます。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から、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。

## オリジンアクセスコントロール (OAC )

In CloudFront は、Amazon Simple Storage Service (Amazon S3) コンテンツを保護するためのアクセスを制限するための拡張オプションです。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、および 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 )

In CloudFront は、Amazon S3 コンテンツを保護するためのアクセスを制限するためのオプションです。OAI を使用すると、CloudFront は Amazon S3 が認証できるプリンシパルを作成します。認証されたプリンシパルは、特定の CloudFront ディストリビューションを介してのみ S3 バケット内のコンテンツにアクセスできます。Word も参照してください。[OAC](#) より詳細で強化されたアクセスコントロールを提供します。

## ORR

[「運用準備状況レビュー」](#) を参照してください。

## OT

[「運用技術」](#)を参照してください。

### アウトバウンド (出力) 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 セキュリティリファレンスアーキテクチャ](#)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、インスプレクションVPCsを使用してネットワークアカウントを設定することをお勧めします。

## P

### アクセス許可の境界

ユーザーまたはロールが持つことができるアクセス許可の上限を設定するための Word プリンシパルにアタッチされる IAM 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、名前、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

[「プログラム可能な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

アクセス許可の定義 ([アイデンティティベースのポリシー](#)を参照)、アクセス条件の指定 ([リソースベースのポリシー](#)を参照)、または の組織内のすべてのアカウントに対する最大アクセス許可の定義 AWS Organizations ([サービスコントロールポリシー](#)を参照) が可能なオブジェクト。

## 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。詳細については、[マイクロサービスでのデータ永続性の有効化](#)を参照してください。

## 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、「[移行準備状況ガイド](#)」を参照してください。

## 述語

true または を返すクエリ条件。通常は false WHERE 句にあります。

## 述語のプッシュダウン

転送前にクエリ内のデータをフィルタリングするデータベースクエリ最適化手法。これにより、リレーショナルデータベースから取得して処理する必要があるデータの量が減少し、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、Implementing security controls on AWSの[Preventative controls](#)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「[ロールの用語と概念](#)」の「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じてプライバシーを考慮に入れたシステムエンジニアリングアプローチ。

## プライベートホストゾーン

Amazon Route 53 が 1 つ以上の DNS 内のドメインとそのサブドメインの VPCs クエリに応答する方法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

非準拠のリソースのデプロイを防止するように設計された[セキュリティコントロール](#)。これらのコントロールは、プロビジョニング前にリソースをスキャンします。リソースがコントロールに準拠していない場合、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 )

設計、開発、発売、成長と成熟、辞退と削除まで、ライフサイクル全体にわたる製品のデータとプロセスの管理。

## 本番環境

[「環境」](#)を参照してください。

## プログラム可能なロジックコントローラー (PLC )

製造では、マシンをモニタリングし、製造プロセスを自動化する、信頼性が高く適応性の高いコンピュータです。

## プロンプトの連鎖

1 つの [LLM](#) プロンプトの出力を次のプロンプトの入力として使用して、より良いレスポンスを生成します。この手法は、複雑なタスクをサブタスクに分割したり、事前対応を繰り返し調整または拡張したりするために使用されます。これにより、モデルのレスポンスの精度と関連性が向上し、より詳細でパーソナライズされた結果が得られます。

## 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。

## publish/subscribe (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。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](#) では、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できるチャンネルにイベントメッセージを発行できます。システムは、公開サービスを変更せずに新しいマイクロサービスを追加できます。

## Q

### クエリプラン

SQL リレーショナルデータベースシステム内のデータにアクセスするために使用する、手順などの一連のステップ。

### 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

[「責任者」、「説明責任者」、「相談先」、「通知先」\(RACI\)](#) を参照してください。

### RAG

[「取得拡張生成」](#) 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

[「責任者」、「説明責任者」、「相談先」、「通知先」\(RACI\)](#) を参照してください。

### RCAC

[「行と列のアクセスコントロール」](#) を参照してください。

### リードレプリカ

読み取り専用で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。

## 再設計

[「7R」](#) 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

[「7R」](#) 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、[AWS リージョン「アカウントで使用できるを指定する」](#) を参照してください。

### 回帰

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

[「7R」](#) 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

[「7R」](#) を参照してください。

### プラットフォーム変更

[「7R」](#) を参照してください。

### 再購入

[「7R」](#) を参照してください。

## 回復性

中断に耐えたり、中断から回復したりするアプリケーションの機能。で障害耐性を計画するときは、[高可用性](#)と[ディザスタリカバリ](#)が一般的な考慮事項です AWS クラウド。詳細については、[AWS クラウド「レジリエンス」](#)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。

## 責任、説明責任、相談、情報提供 (RACI) 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。サポートを含めると、マトリックスは RASCI マトリックスと呼ばれ、除外すると RACI マトリックスと呼ばれます。

## レスポンスコントロール

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、Implementing security controls on AWSの[Responsive controls](#)を参照してください。

## 保持

[「7R」](#)を参照してください。

## 廃止

[「7R」](#)を参照してください。

## 取得拡張生成 (RAG )

レスポンスを生成する前に、[LLM](#) が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を参照する[生成 AI](#) テクノロジー。例えば、RAG モデルは組織のナレッジベースやカスタムデータのセマンティック検索を実行する場合があります。詳細については、[RAG とは](#)」を参照してください。

## ローテーション

攻撃者が認証情報にアクセスすることをより困難にするために、[シークレット](#)を定期的に更新するプロセス。

## 行と列のアクセスコントロール (RCAC )

アクセスルールが定義されている基本的で柔軟な SQL 式の使用。RCACは、行のアクセス許可と列のマスクで構成されます。

### 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 (IdPs) が使用す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 AWS API で作成しなくても、AWS Management Console にログインしたり、IAM オペレーションを呼び出したりできます。SAML 2.0 ベースのフェデレーションの詳細については、Word 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

[「監視コントロールとデータ収集」](#)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 AWS Secrets Managerパスワードやユーザー認証情報などの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。シークレット値は、バイナリ、単一の文字列、または複数の文字列にすることができます。詳細については、[Secrets Manager ドキュメントの「Secrets Manager シークレットの内容」](#)を参照してください。

## 設計によるセキュリティ

開発プロセス全体を通じてセキュリティを考慮したシステムエンジニアリングアプローチ。

### 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、[予防的](#)、[検出的](#)、[応答的](#)、[プロアクティブ](#)の4つの主なタイプがあります。

### 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。

### セキュリティ情報とイベント管理 (SIEM) システム

セキュリティ情報管理 (SIM) システムとセキュリティイベント管理 (SEM) 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、その他のソースからデータを収集、監視、分析して、脅威やセキュリティ違反を検出し、アラートを生成します。

### 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に自動的に対応または修正するように設計された、事前定義され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の実装に役立つ[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。自動応答アクションの例としては、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、認証情報のローテーションなどがあります。

### 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。SCPsは、管理者がユーザーまたはロールに委任できるアクションのガードレールを定義するか、制限を設定します。SCPs を許可リストまたは拒否リストとして使用して、許可または禁止されるサービスまたはアクションを指定できます。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

のエンドポイントの 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、スループットなど、サービスのパフォーマンス側面の測定。

## サービスレベルの目標 (SLO )

サービス[レベルのインジケータ](#)によって測定される、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、ユーザー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

[セキュリティ情報とイベント管理システム](#)を参照してください。

## 単一障害点 (SPOF )

システムを中断させる可能性のあるアプリケーションの 1 つの重要なコンポーネントの障害。

## 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。

## split-and-seed 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

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、[「」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 AWS クラウド」](#)を参照してください。

## SPOF

[単一障害点](#)を参照してください。

## star スキーマ

トランザクションデータまたは測定データを保存するために 1 つの大きなファクトテーブルを使用し、データ属性を保存するために 1 つ以上の小さなディメンションテーブルを使用するデータベースの組織構造。この構造は、[データウェアハウス](#)またはビジネスインテリジェンスの目的で使用するため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、宿主にと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](#)。このパターンを適用する方法の例については、[「コンテナと Amazon API Gateway を使用してレガシー Microsoft Word.NET \(ASMX\) ウェブサービスを段階的にモダナイズする」](#)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 Availability Zone に存在する必要があります。

## 監視コントロールとデータ収集 (SCADA)

製造では、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生産オペレーション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

ユーザーインタラクションをシミュレートして潜在的な問題を検出したり、パフォーマンスをモニタリングしたりする方法でシステムをテストします。[Amazon CloudWatch Synthetics](#) を使用して、これらのテストを作成できます。

## システムプロンプト

動作を指示するために、コンテキスト、指示、またはガイドラインを [LLM](#) に提供するための手法。システムプロンプトは、コンテキストを設定し、ユーザーとのやり取りのルールを確立するのに役立ちます。

## 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が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

VPCs ネットワーク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トランジットハブ。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の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「[AWS Organizations を他の AWS のサービスで使用する 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つのピザを食べることができる small 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。詳細については、[深層学習システムにおける不確実性の定量化](#) ガイドを参照してください。

## 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 VPCs 間の接続。詳細については、Amazon [VPC ドキュメントの「Word ピアリングとは」](#)を参照してください。VPC

### 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

現在のレコードに関連する行のグループに対して計算を実行する SQL 関数。ウィンドウ関数は、移動平均の計算や、現在の行の相対位置に基づく行の値へのアクセスなどの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

[「書き込み 1 回」、「読み取り多数」を参照してください。](#)

## WQF

[AWS 「Word Workload Qualification Framework」](#) を参照してください。

## Write Once, Read Many (WORM )

データを 1 回書き込み、データの削除や変更を防ぐストレージモデル。承認されたユーザーは、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](#) を利用する攻撃、通常はマルウェア。

### 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

タスクを実行するための指示を [LLM](#) に提供しますが、タスクのガイドに役立つ例 (ショット) はありません。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

CPU とメモリの平均使用量が 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。

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。