Cisco Multicloud Defense：用語

最終更新：2026 年 11 月 5 日

Cisco Multicloud Defense

Cisco Multicloud Defense は、クラウド環境を出入りし、その環境内を移動するトラフィックを検査して保護するための、クラウドネイティブのマルチクラウド ネットワーク セキュリティ ソリューションです。SaaS コントローラとクラウド展開されたゲートウェイを組み合わせて、AWS、Azure、Google Cloud、および OCI にまたがる可視性、ポリシー適用、脅威防止、およびセグメンテーションを提供します。

Cisco Multicloud Defense の用語

アカウントオンボーディング

コントローラがクラウドリソースを検出し、トラフィックの可視性を有効にして、セキュリティインフラストラクチャを展開できるように、クラウドアカウント、サブスクリプション、プロジェクト、フォルダ、またはテナントを Multicloud Defense に接続するプロセス。オンボーディングでは、クラウド固有の前提条件と権限モデルを使用して、AWS、Azure、GCP、および OCI をサポートします。

高度なセキュリティ プロファイル

Multicloud Defense Gateway のデータパスを介して適用される、詳細な検査および適用機能のコレクション。たとえば、IDS/IPS、WAF、ウイルス対策、TLS 復号、DLP、URL フィルタリング、FQDN フィルタリング、アプリケーション層制御などが含まれます。

アプリケーション レイヤ ファイアウォール

IP アドレス、ポート、またはプロトコルのみを使用するのではなく、レイヤ 7 でアプリケーション トラフィックを評価するセキュリティ機能。Multicloud Defense では、アプリケーション レイヤ ファイアウォールはクラウドワークロードの保護に使用され、一般的に WAF やレイヤ 7 の脅威に対する防御などの入力保護に関連付けられます。

アセット検出

オンボーディングされたクラウドアカウントでクラウドリソースとインベントリを検出し、リソースがどのように展開され、相互接続されているかを示す現在のビューを維持する機能。アセット検出は、チームがクラウドの公開状況を把握し、必要な場所にコントロールを配置するのに役立ちます。

自動スケーリング

自動スケーリングは、トラフィック需要に応じてゲートウェイインスタンスを追加または削除できる自動化された機能です。Multicloud Defense Gateway と FTDv ゲートウェイの両方に適用

されます。自動スケーリングはコントローラによって管理され、クラウドワークロードの変更に適応しながら、セキュリティ適用を維持できるように設計されています。

集中型セキュリティモデル

複数のスポークネットワークの適用ハブとして機能する中央サービス VPC、VNet、またはセキュリティ VPC にセキュリティサービスが配置される展開モデル。一元化された設計は、接続されたクラウドネットワーク全体の入力、出力、および水平方向の検査に使用されます。

CIDR

Multicloud Defense では、Classless Inter-Domain Routing（CIDR）は、ネットワーク境界を定義するために使用される基本的な方法です。ワークロードサブネットを識別し、トラフィックをセグメント化し、AWS、Azure、GCP、OCI などの異なる環境にまたがってセキュリティポリシーを構築します。

クラウド アカウント

Multicloud Defense に接続されているクラウドプロバイダーの管理範囲。たとえば、AWS アカウント、Azure サブスクリプション、GCP プロジェクトまたはフォルダ、OCI テナントなどです。

クラウドネイティブのキーストア

お客様が制御するクラウド境界内に秘密キーを保持しながら、TLS インスペクションのユースケースを実現するために使用される、Azure Key Vault などのクラウドプロバイダーのキー管理サービス。

クラウド サービス プロバイダー

AWS、Azure、Google Cloud Platform、Oracle Cloud Infrastructure などのパブリック クラウド プラットフォーム。Multicloud Defense は、クラウドサービスプロバイダー（CSP）のネットワークおよびロギング構造と統合され、ゲートウェイを展開し、アセットを検出し、トラフィックの可視性に必要な情報を収集します。

複合セキュリティモデル

中央集中型と分散型の両方のセキュリティ適用を使用する展開アプローチ。このモデルでは、共有される検査を一元化する一方で、必要に応じてゲートウェイを特定のアプリケーションまたはクラウドネットワークの近くに配置できます。

コンテンツ フィルタリング

コンテンツ、URL、FQDN、カテゴリ、マルウェア判定、またはデータ損失防止ロジックに基づいてトラフィックを制御またはブロックする、検査および適用の仕組み。

コントローラ サービス アカウント

クラウドアカウントでのリソースの検出、インフラストラクチャのオーケストレーション、およびセキュリティワークフローの管理に必要な権限を Multicloud Defense コントローラに付与するために使用される、クラウドアイデンティティまたはサービスアカウント。

データ損失防止

機密データが承認された範囲から離れることを検出または防止するセキュリティ機能。シスコのドキュメントでは、データ損失防止（DLP）は、個人を特定できる情報 （PII）や保護医療情報（PHI）などのデータタイプのコンプライアンスとセキュリティをサポートするものとして説明されています。

データプレーン

Multicloud Defense Gateway で表される、アーキテクチャのトラフィック処理側。データプレーンはトラフィックの検査とポリシー適用を行い、コントローラはコントロールプレーンを提供します。

検出、展開、防御

Multicloud Defense のワークフロー。検出は、クラウドアカウントに接続し、リソースおよびトラフィックのインベントリを作成します。展開は、VPC、VNet、およびゲートウェイをセットアップします。防御は、保護用のポリシー、ルールセット、およびプロファイルを作成して管理します。

分散セキュリティモデル

セキュリティ適用を中央ハブのみに配置するのではなく、アプリケーション、ワークロード、または個々のクラウドネットワークの近くに配置する展開モデル。このモデルは、チームがアプリケーションローカルの検査、スケーリング、またはセグメンテーションを必要とする場合に役立ちます。

ダイナミック アドレス オブジェクト

クラウドリソースの変更に応じて更新される、クラウドネイティブのリソース属性に基づくポリシーオブジェクト。ダイナミック アドレス オブジェクトによって、常に手動で更新しなくても、ポリシーがクラウドリソースに合わせて調整されます。

水平方向のセキュリティ

ワークロード、サブネット、VPC、VNet、またはクラウドネットワーク間で水平方向に移動するトラフィックの検査および適用の仕組み。ラテラルムーブメントを制限し、アプリケーション間および階層間でセグメンテーションや最小権限アクセスを導入するのに役立ちます。

出力ゲートウェイ

アウトバウンドおよび水平方向のトラフィックを保護するために使用されるゲートウェイ。FQDN フィルタリング、URL フィルタリング、データ損失防止（DLP）、IDS/IPS、ウイルス対策、転送プロキシ、TLS 復号、および関連する制御を提供できます。

出力セキュリティ

クラウドワークロードまたはネットワークからインターネット、SaaS サービス、その他のネットワーク、またはその他のクラウド環境に向けたトラフィックの制御。出力セキュリティは、データ持ち出し、コマンドアンドコントロール トラフィック、マルウェア通信、不正な接続先を防止するのに役立ちます。

エンフォースメントポイント

トラフィックポリシーが適用されるゲートウェイインスタンスまたはゲートウェイクラスター。コントローラがポリシーを定義してオーケストレーションし、ゲートウェイがそのポリシーをインラインで適用します。

フォワードプロキシ

アウトバウンドクライアントトラフィックのプロキシ機能。Multicloud Defense では、フォワードプロキシ機能は一般的に、出力検査、TLS 復号、URL/FQDN フィルタリング、データ損失防止（DLP）、侵入防御に関連しています。

転送モード

完全なパケットまたはコンテンツペイロードを検査せずに、送信元と接続先の通信に基づいてアクセスを制御するゲートウェイ動作モード。通常、水平方向のフローと、IP アドレス、レイヤ 4 情報、タグ、または FQDN に基づく出力フィルタリングに使用されます。

gateway

PaaS コンポーネントとしてお客様のクラウドアカウントに展開された Multicloud Defense データプレーンコンポーネント。ゲートウェイは、トラフィックをインラインで検査し、入力、出力、および水平方向のユースケースにポリシーを適用します。

ゲートウェイインスタンス

Multicloud Defense Gateway 展開の一部を形成するクラウドコンピューティングインスタンス。複数のインスタンスをクラウドロードバランサの背後に配置することで、拡張性と高可用性を提供できます。

ハブアンドスポーク アーキテクチャ

中央サービスネットワークまたはセキュリティハブが複数のスポーク VPC、VNet、または VPC ネットワークに接続するネットワーク設計。Multicloud Defense は、この設計を一元化された検査と適用に使用します。

イングレス ゲートウェイ

アプリケーションまたはワークロード宛てのインバウンドトラフィックを保護するために使用されるゲートウェイ。WAF、レイヤ 7 DoS 保護、IDS/IPS、ウイルス対策、リバースプロキシ、TLS 復号、地理的 IP 制御、および悪意のある IP のフィルタリングを提供できます。

入力セキュリティ

インターネットまたは外部ネットワークからクラウド環境に入るトラフィックの制御。入力セキュリティは、エクスプロイト、ボット、マルウェア、悪意のある IP、DoS の試行、およびその他のインバウンドの脅威から Web および非 Web アプリケーションを保護します。

インライン検査

トラフィックがデータパスのゲートウェイを通過しているときに実行されるトラフィック検査。インライン検査では、トラフィックが宛先に到達する前に、ポリシーによってトラフィックの許可、拒否、復号、スキャンを実行したり、その他の制御を適用したりできます。

inventory

検出されたクラウドリソース、その属性、および関係のモデル。インベントリはコントローラによって定期的に更新されるため、管理者は現在のリソースと、その接続状況を確認できます。

最小権限アクセス

ワークロード、階層、環境、またはクラウドネットワーク間で承認された通信のみを許可するセグメンテーションの原則。Multicloud Defenseは、セグメンテーションを使用して、水平方向のアクセスに最小権限を適用できるようにします。

Multicloud Defense Controller

Cisco Multicloud Defense の SaaS コントロールプレーン。このコントローラは、中央管理、クラウドアカウントのオンボーディング、検出、ゲートウェイライフサイクルの自動化、ポリシーオーケストレーション、ロギング、アラート、計測、およびサードパーティのオペレーションツールとの統合機能を提供します。

Multicloud Defense Gateway

Cisco Multicloud Defense のインライン適用コンポーネント。お客様のクラウドアカウントに展開され、コントローラからポリシーを受信し、トラフィックを検査して、WAF、IDS/IPS、データ損失防止（DLP）、URL フィルタリング、TLS 復号、ウイルス対策などの保護を適用します。

Multicloud Defense Terraform Provider

Multicloud Defense リソースを展開して管理するための Infrastructure as Code インターフェイス。このインターフェイスにより、DevOps および DevSecOps チームは、Terraform ワークフローを介してセキュリティ インフラストラクチャとポリシーをインスタンス化できます。

ノースバウンドトラフィック

インターネットまたは外部ネットワークからクラウドでホストされているアプリケーションおよびワークロードに向かうインバウンドのトラフィックフロー。Multicloud Defense のドキュメントでは、ノースバウンドトラフィックは一般的に入力保護およびリバース プロキシ インスペクションに関連付けられています。

ノースサウストラフィック

クラウドワークロードからインターネットまたは外部サービスに向かうアウトバウンドのトラフィックフロー。Multicloud Defense のドキュメントでは、この方向を出力保護および転送プロキシまたは転送操作に関連付けています。

OCI

Oracle Cloud Infrastructure（OCI）は、クラウド コンピューティング プラットフォームです。Cisco Multicloud Defense とネイティブに統合されているため、分散環境全体で統一された一貫性のある防御を提供します。

ポリシー

どのトラフィックが許可、拒否、復号、検査、またはログ記録されるかを表すセキュリティ ルールとプロファイルのセット。Multicloud Defenseでは、ポリシーは一元的に作成され、クラウド環境全体のエンフォースメントポイントに適用されます。

プロキシモード

アプリケーションのコンテンツをより詳細に検査するために接続を終端して再確立するゲートウェイ動作モード。プロキシモードは、リバースおよびフォワードプロキシのユースケース、TLS復号、WAF、データ損失防止（DLP）、およびその他のコンテンツ検査機能をサポートします。

リバースプロキシ

インバウンドアプリケーショントラフィックのプロキシ機能。Multicloud Defenseでは、リバースプロキシ機能が入力ゲートウェイで使用され、アプリケーションに到達する前にトラフィックを検査して保護できます。

ルールセット

ポリシーの一部としてトラフィックまたはリソースに適用できるルールのグループ化されたセット。ルールセットを使用すると、管理者はプロファイルと保護されたフローの適用ロジックを整理できます。

セキュリティ プロファイル

侵入防御、Webアプリケーションファイアウォールの動作、URLフィルタリング、TLS復号、データ損失防止（DLP）などの特定の検査または保護動作を定義する再利用可能な設定。

サービス VPC/サービス VNet/セキュリティ VPC

Multicloud Defenseゲートウェイおよびサポートサービスの集中型ハブとして使用されるクラウドネットワーク。スポークネットワークに接続し、インスペクションポイントを介してトラフィックをステアリングします。

スポーク VPC/スポーク VNet

集中型サービスネットワークに接続されたアプリケーションまたはワークロードのネットワーク。スポークネットワークからのトラフィックは、検査のためにMulticloud Defenseゲートウェイにルーティングできます。

タグベースのポリシー

クラウドリソースタグとワークロードアイデンティティを使用してルールを動的に適用するポリシーメソッド。タグベースのポリシーは、クラウド環境の変更時に新しく展開されたリソースが適切なセキュリティ制御を継承するのに役立ちます。

トラフィックの可視性

フローログやDNSクエリログなどのトラフィックおよびDNSデータを使用して、クラウド環境全体の通信パターン、接続先、リスクカテゴリ、および露出状況を把握します。

TLS 復号

検査のために暗号化されたトラフィックを復号し、トラフィック転送時に再暗号化する機能。Multicloud Defenseは、サポートされている設計でキーの管理にクラウドネイティブのキーストアを使用しつつ、プロキシおよびゲートウェイのユースケースでTLS復号をサポートします。

VPC フローログ/DNS クエリログ

ネットワークフローと DNS アクティビティの可視性のために使用されるクラウド ロギング データソース。これらのログは、Multicloud Defense がリソースを検出し、トラフィックについて把握し、セキュリティインサイトを生成するのに役立ちます。

Web アプリケーション ファイアウォール

Web アプリケーションをアプリケーションレイヤ攻撃から保護するために使用されるレイヤ 7 のインスペクション機能。Multicloud Defense には、入力セキュリティ機能の一部として Web アプリケーション ファイアウォール（WAF）が組み込まれています。

ワークロード アイデンティティ

ワークロードを記述する属性（タグ、クラウドメタデータ、デプロイメントタイプ、環境、アプリケーション階層など）。Multicloud Defense は、ワークロード アイデンティティと検出を使用して、クラウドリソース全体にわたるダイナミックポリシーを構築します。

© Cisco Systems, Inc. All rights reserved.

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。