アドレスオブジェクト

アドレスオブジェクト

[アドレスオブジェクト（Address Object）]は、定義方法に応じて、[セキュリティポリシールールセットルール（Security Policy Rule Set Rule）] の [送信元（Source）] または [宛先（Destination）]として、または[リバースプロキシサービスオブジェクト（Reverse Proxy Service Object）] の [ターゲットバックエンドアドレス（Target Backend Address）] として使用するための 1 つ以上の IP、CIDR、または FQDN のセットを表します。アドレスオブジェクトは、従来の構成を使用して静的に設定することも、クラウド構成を使用して動的に設定することもできます。

アドレスオブジェクトは、セキュリティポリシールールまたはルールセットの [送信元（Source）]、[宛先（Destination）]、または [リバースプロキシターゲット（Reverse Proxy Target）] フィールド内の 1 つ以上の IP、CIDR、または FQDN のセットを表します。また、リバース プロキシ サービス オブジェクト内のターゲット バックエンド アドレスとして定義することもできます。このセクションでは、送信元オブジェクトと宛先オブジェクトに焦点を当てます。

バージョン 24.04 以降、特定の IP アドレスまたは IPアドレスの範囲を**除外する**ようにアドレスオブジェクトを設定できるようになりました。

送信元/宛先

これらのオブジェクトは、IPアドレスまたはCIDRに明示的にマッピングする一致基準を定義するために使用されます。オブジェクトはポリシールール内で参照され、ポリシールールが処理されるときにゲートウェイインスタンスに入るトラフィックに対して評価されます。

送信元および宛先アドレスオブジェクトは、ゲートウェイインスタンスに入るアプリケーション トラフィックを照合するために IP アドレスと CIDR が明示的に必要な場合に役立ちます。これらのオブジェクトは、ポリシールール定義の送信元フィールドと宛先フィールド内で参照されます。これらの各フィールドに入力するために使用されるアドレスオブジェクトのタイプは、トラフィックフロー、アプリケーションタイプ、および使用例によって異なります。

送信元または宛先アドレスオブジェクト

送信元または宛先アドレスオブジェクトは、セキュリティ ポリシー ルール セット内のルールの送信元または宛先を指定します。これは、送信元または宛先 IP アドレスに基づいてトラフィックを照合するために、ルールによって使用されます。さまざまなタイプのアドレスオブジェクトは、次のように定義されます。

IP/CIDR/FQDN（静的）アドレスオブジェクト

IP/CIDR/FQDN アドレスオブジェクトは、IP アドレス、CIDR ブロック、または FQDN のセットとして設定されます。IP/CIDR アドレスオブジェクトの例は次のとおりです。

- DNS サーバーの宛先 IP。
- SMTP リレーサーバーの宛先 IP。
- NTP サーバーの宛先 IP。
- アプリケーション ワークロードの送信元 IP またはサブネット。

FQDN アドレスオブジェクトは、DNS 解決に基づいて IP を許可またはブロックするための FQDN の明示的なセットを定義します。FQDN が FQDN アドレスオブジェクト内で定義され、ポリシールール内で参照される場合、ゲートウェイインスタンスは DNS 解決を実行して対応する IP アドレスを取得し、着信トラフィックを照合します。デフォルトでは、キャッシングは有効ではありません。この場合、DNS 解決は 60 秒ごとに実行され、ゲートウェイインスタンスは取得した解決を60秒間使用します。FQDNアドレスオブジェクト内で指定されたFQDNが多数の（それぞれ400を超える）IPアドレスに解決される場合、キャッシングを有効にできます。この場合、キャッシュサイズやキャッシュ TTL と一緒に DNS 解決間隔を指定できます。

FQDNアドレスオブジェクトは、UDPベース（例：NTP）、または要求パケットにホスト情報が存在しないTCPトラフィック（例：SMTP）のいずれかのアプリケーショントラフィックで照合する場合に便利です。いずれの場合も、たとえば内部ワークロードが接続する必要がある、適切なすべての NTP サーバーまたは SMTP サーバーの IP アドレスのリストを手動で定義するのではなく、FQDN アドレスオブジェクトを使用して、この種のアプリケーション トラフィックで照合することをお勧めします。

動的クラウド構成

クラウドネイティブなアドレスオブジェクトは、Multicloud Defense Controller によって定期的なインベントリ収集（API ベース）またはリアルタイムのイベントトラッキング（GCP パブ/サブ統合）を通じて検出される動的なクラウドリソースです。これらのリソースは、VPC/VNET、インスタンス ID、セキュリティグループ、サブネット ID などの個別のリソースである場合も、ユーザー定義のタグを介して参照されるリソースのセットである場合もあります。Multicloud Defense Controller は、リアルタイムのイベントトラッキングとターゲットを絞った API コールの組み合わせを使用して、クラウドリソースに関連付けられた IP アドレスを動的に入力します。したがって、クラウドネイティブリソースに後で加えられた変更は、このリソースを参照するアドレスオブジェクト内に自動的に反映されます。

（注） クラウドネイティブの構造を使用して送信元または宛先アドレスオブジェクトを定義すると、単一クラウド環境とマルチクラウド環境の両方で真にダイナミッククラウドポリシーを作成できます。クラウド環境内でクラウドリソースが追加、削除、または変更されると、アドレスオブジェクトはこれらの変更を反映するように動的に更新されるため、境内のすべてのアプリケーションと機能でセキュリティ態勢が自動的に更新されます。

VNet および VPC 環境でのユーザー定義タグ

タグは、一連のタグで定義されたクラウドリソースの IP アドレスまたは CIDR をアドレスオブジェクトにマッピングします。GCP のラベルはキーと値のペアであり、これはさまざまな環境（開発、ステージング、生産など）用にリソースを分類するためによく使用されます。送信元または宛先アドレスオブジェクト内では、ユーザー定義のタグを使用して、インスタンス、VPC/VNET、サブネット、セキュリティグループなどのリソースを参照できます。最も一般的な用途として、組織はタグを使用してインスタンスを分類します。

タグベースのポリシールールは、動的クラウドポリシーの非常に強力なコンポーネントです。特定のタグを持つインスタンスのグループに対して、詳細なポリシールールを定義することができます。これらのポリシールールを設定すると、適切なタグを持つ新しいインスタンスが展開されるたびに、それが属するインスタンスのカテゴリに定義されている対象のセキュリティポリシーが自動的に継承されます。これは、Multicloud Defense Controller が新しいインスタンスが展開されたことを検出するだけでなく、そのインスタンスに割り当てられているタグも検出するためです。その後、このインスタンスベースのタグを参照する送信元または宛先アドレスオブジェクトを、新しいインスタンスの IP アドレスで動的に更新します。インスタンスが誤ったタグを使用したりタグなしで展開されている場合、適切なポリシールールと一致しないため、他のリソースとの通信は許可されません。

VNet と VPC では、タグによって、VPC に関連付けられた CIDR がアドレスオブジェクトの CIDR にマッピングされます。VPC または VNET 内に展開されたインスタンスに一致するルールを、コンテキストに応じて作成できます。検出された VPC または VNET の名前を使用して一致基準を定義できるため、特定の VPC または VNET に関連付けられている CIDR を手動で調べる必要がなくなります。VPC または VNET への変更は、介入なしでポリシールールで動的に更新されます。VPC または VNET が削除され、その場所に新しい VPC/VNET が作成されると、 CIDR を再利用してもルールは適用されなくなります。

インスタンス ID

インスタンス ID は、インスタンスに関連付けられた IP アドレスを、アドレスオブジェクト内の IP アドレスのリストにマッピングします。これにより、インスタンスの設定を手動で調べることなく、特定のインスタンスのポリシールールをコンテキストに応じて作成できます。ポリシールールには、インスタンスへの変更またはインスタンスの削除が反映されます。ポリシールールは他のインスタンスには適用できないことに注意してください。これは、インスタンスが削除され、同じ設定の新しいインスタンスに置き換えられた場合でも同じです。

セキュリティ グループ（Security Group）

セキュリティグループは、セキュリティグループに関連付けられたネットワークインターフェイスの IP アドレスを、アドレスオブジェクト内の IP アドレスのリストにマッピングします。セキュリティグループへのフィールドの追加または削除など、インターフェイス関連の変更は、アドレスオブジェクト内の IP アドレスのリストに動的に反映されます。これにより、組織は既存のセキュリティグループを、ゲートウェイ データパス パイプラインの高度なセキュリティ機能に連携させることができます。

サブネット ID

サブネット ID は、サブネットに関連付けられた CIDR をアドレスオブジェクトの CIDR にマッピングします。これにより、サブネットの設定を手動で調べることなく、特定のサブネット ID に関連付けられたすべてのリソースのポリシールールをコンテキストに応じて作成できます。VPC または VNET は通常、複数のサブネットに分割され、これらのサブネット内に展開されたリソースは異なる目的で使用される場合があります。たとえば、あるサブネット内のインスタンスには、特定の高度なセキュリティプロファイルのセットが必要な場合や、異なるトラフィックフロー要件がある場合があります。サブネットごとに異なるセキュリティルールを作成するプロセスを簡素化するために、Multicloud Defense では、サブネットの名前を一致基準に使用するポリシールールを定義できます。したがって、各サブネットには、一意のセキュリティプロファイルを持つ一意のポリシールールを設定できます。サブネットおよびサブネット内に展開されたインスタンスへの変更は、ポリシールールに動的に反映されます。

Geo IP

Geo IP アドレスオブジェクトは、Geo IP の国名のセットとして設定されます。これらのオブジェクトは、地理的な場所（国）に基づいて IP アドレスから送受信されるトラフィックを許可またはブロックするために使用されます。Multicloud Defense は、更新された Geo IP のリストを維持するために MaxMind GeoIP2 データベースと統合されます。

国名と国コード、または IP アドレスから Geo IP 国コードの完全なリストを確認するには、GeoNames の Web サイトにアクセスしてください。

グループ

グループ アドレス オブジェクトは、送信元または宛先アドレスオブジェクトのセットとして設定されます。グループでは、個々のアドレスオブジェクトを定義してからグループ化することで柔軟性が提供され、グループのメンバーに基づいてトラフィックを照合するために必要なルールの数が簡素化されます。グループは、メンバーが静的、動的、またはこの 2 つの組み合

わせのいずれであるかを問わず、グループのメンバーから一連の IP、CIDR、または FQDN を継承します。

送信元または宛先アドレス オブジェクト パラメータ

タイプ	モード：動的または静的	パラメータ	必須またはオプション	注記
IP/CIDR/FQDN	静的	値	必須	アドレスオブジェクトあたりの FQDN の総数は 200 個に制限され、各 FQDN は最大 400 個の IP に解決できます。Multicloud Defense Gateway は、DNS レコード TTL に関係なく、60 秒ごとに DNS 解決を実行します。
VPC/VNet ID	動的	CSP アカウント	必須	
		地域	必須	
		リソース グループ	オプション	Azure のみ
		VPC/VNet ID	必須	
セキュリティ グループ（Security Group）	動的	CSP アカウント	必須	
		地域	必須	
		VPC/VNet ID	必須	
		リソース グループ	オプション	Azure のみ
		セキュリティ グループ ID	必須	

タイプ	モード：動的または静的	パラメータ	必須またはオプション	注記
アプリケーション セキュリティ グループ	動的	CSP アカウント	必須	Azure のみ
		地域	必須	
		リソース グループ	必須	
		アプリケーション セキュリティ グループ	必須	
インスタンス ID	動的	CSP アカウント	必須	
		地域	必須	
		VPC/VNet ID	必須	
		リソース グループ	オプション	オプション
		インスタンス ID	必須	
サブネット ID	動的	CSP アカウント	必須	
		地域	必須	
		VPC/VNet ID	必須	
		リソース グループ	オプション	Azure のみ
		サブネット ID	必須	

タイプ	モード：動的または静的	パラメータ	必須またはオプション	注記
ユーザー定義タグ	動的	CSP アカウント	オプション	
		地域	オプション	
		VPC/VNet ID	オプション	
		リソース グループ	オプション	Azure のみ
		リソース/タグ/値	必須	リソースとタグのキーと値のペアのリスト。リソースには、インスタンス、VPC/VNet、サブネット、ロードバランサ、セキュリティグループ、セキュリティグループ（Azure）などがあります。
Geo IP		値	必須	
Group		Address	必須	

リバース プロキシ ターゲット アドレス オブジェクト

リバースプロキシターゲットアドレスオブジェクトは、リバースプロキシサービスオブジェクトのバックエンド ターゲット アドレスとして指定されます。これは、サービスオブジェクトによって、アプリケーションへのバックエンド接続を確立するために使用されます。アプリケーションは、1 つ以上のアプリケーション ロード バランサまたはインスタンスの IP または FQDN形式のアドレスとすることができます。さまざまなタイプのリバースプロキシターゲット アドレス オブジェクトは、次のように定義されます。

静的 IP/FQDN アドレスオブジェクト

IP/FQDN アドレスオブジェクトは、IP アドレスまたは FQDN のセットとして設定されます。複数の IP または FQDN が設定されている場合、ゲートウェイは、バックエンド接続を設定するときに、設定されたフィールドの中で優先順位が設定されていないアドレスを処理します。1 つの FQDN が設定されている場合、ゲートウェイは DNS を使用して FQDN を解決し、バックエンド接続の設定時に使用する IP アドレスを決定します。

ダイナミック アプリケーション アドレス オブジェクト

アプリケーション アドレス オブジェクトは、そのアプリケーションタグによって決定される個々のアプリケーション ロード バランサのクラウドリソースとして設定されます。この設定では、Multicloud Defense リアルタイムインベントリ検出を使用してクラウドアカウントから取得された、クラウドリソースで表される一連の IP または FQDN が動的に入力されます。クラウドリソースへの変更は、アドレスオブジェクトに自動的に反映されます。設定の結果、複数の IP または FQDN が生成された場合、ゲートウェイは、バックエンド接続を設定するときに、優先順位が設定されていないフィールドを処理します。設定の結果、1 つの FQDN が生成された場合、ゲートウェイは DNS を使用して FQDN を解決し、バックエンド接続の設定時に使用する IP アドレスを決定します。

リバース プロキシ ターゲット アドレス オブジェクトのパラメータ

Type	モード：動的または静的	パラメータ	必須またはオプション	注記
IP/FQDN	[静的（Static）]	値	必須	
アプリケーション	動的	CSP アカウント	必須	
		地域	必須	
		VPC/VNet ID	必須	
		リソース グループ	オプション	Azure のみ
		タグ/値	必須	単一タグのキーと値のペア

システムオブジェクト

Multicloud Defense は、ポリシーの作成を簡素化するために、事前定義されたアドレスオブジェクトのリストを提供します。すべてのシステムオブジェクトは編集または削除できません。変更が必要な場合は、システムオブジェクトの複製を作成できます。

名前	説明
いずれか	これは、IPv4 アドレス空間全体を表します。
any-private-rfc- 1918	これは、RFC-1918 で定義されているすべての IPv4 プライベートアドレスを表します。
インターネット	これは、プライベート IPv4 アドレス（RFC1918）を除いた IPv4パブリックアドレス空間全体を表します。

送信元/宛先アドレスオブジェクトの作成

このオブジェクトの詳細については、送信元または宛先アドレス オブジェクト パラメータ（5 ページ）を参照して ください。Multicloud Defense で送信元/宛先アドレスオブジェクトを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）]>[セキュリティポリシー（Security Policies）]>[アドレス（Addresses）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [送信元/宛先（Src/Dest）] を選択します。

ステップ 4 [名前（Name）] にアドレスオブジェクトを識別するための一意の名前を入力します。

ステップ 5 （任意）オブジェクトの説明を入力します。これにより、オブジェクトを他のオブジェクトと区別するのに役立つ文脈を提供できます。

ステップ 6 [オブジェクトタイプ（Object Type）] を選択します。オブジェクトタイプの詳細については、「アドレスオブジェクト （1 ページ）」を参照してください。次のいずれかのタイプを選択します。

- IP/CIDR/FQDN
- VPC/VNet ID
- セキュリティ グループ（Security Group）
- アプリケーション ID（Azure のみ）
- インスタンス ID
- サブネット ID
- ユーザー定義タグ
- Geo IP
- サービスエンドポイント（クラウドサービス IP）
- グループ

（注）
[グループ（Group）] を選択すると、特定の IP アドレスまたは IP アドレスの範囲を含めたり除外したりできます。

ステップ 7 ステップ 6 で選択したタイプに応じて、次のパラメータを入力します。

- [値（Value）]：有効な IP、CIDR、または FQDN IP アドレスを入力します。
- [CSPアカウント（CSP Account）]：ドロップダウンメニューを使用して、 コントローラにすでに接続されているクラウド サービス プロバイダーのアカウントを選択します。

- [リージョン（Region）]：クラウド サービス プロバイダーの所在地であるリージョンをセレクトします。
- [VPC]：ドロップダウンメニューを使用して、VPC または VNet を選択します。選択したクラウドサービス プロバイダーのアカウントによって、使用可能なオプションが異なる場合があることに注意してください。
- [サブネット（Subnet）]：ドロップダウンメニューを使用して、VPC または VNet に適用するサブネットを選択します。
- （Azure のみ）[リソースグループ（Resource Group）]：ドロップダウンメニューを使用して、選択内容と互換性のあるリソースグループを選択します。
  - [リソースレベル（Resource Level）]：ドロップダウンメニューを使用して値を選択します。
  - [リソースタグ（Resource Tag）]：ドロップダウンメニューを使用して、リソースタグとしてキーワードを選択します。
  - [値（Value）]：リソースグループの有効な値を入力します。これは、IP/CIDR/FQDN オブジェクトで想定される [値（Value）] のエントリとは異なることに注意してください。
- [Geo IP]：ドロップダウンメニューを使用して、選択した地理位置情報に関連付けられている特定の IP を選択します。
- [X-Forwarded-Forの照合が有効（X-Forwarded-For Match Enabled）]：ゲートウェイに XFF HTTP ヘッダーフィールドの照合を許可するには、このチェックボックスをオンにします。
- [アドレス（Address）]：既存のオブジェクトを選択します。この選択により、アドレスのグループが決定されます。
- [アドレスを含める（Include Addresses）]：このオプションは、ステップ 6 でタイプとして [グループ（Group）] を選択した場合にのみ適用されます。含めたい特定の IP アドレス、または IP アドレスの範囲を入力します。`any` を使用して、すべての有効なアドレスを含めることもできます。
- [アドレスを除外（Exclude Addresses）]：このオプションは、ステップ 6 でタイプとして [グループ（Group）] を選択した場合にのみ適用されます。除外する特定の IP アドレスまたは IP アドレスの範囲を入力します。`any` を使用して、すべての有効なアドレスを含めることもできます。アドレス除外は Multicloud Defense Controller から検証されないことに注意してください。

ステップ 8 （任意）[一致する式（Matching Expression）] を含めます。これは、オブジェクトを実行するために一致する必要がある、一連の条件を表します。

ステップ 9 完了したら、[保存（Save）] をクリックします。

リバース プロキシ ターゲット アドレス オブジェクトの作成

このオブジェクトの詳細については、リバース プロキシ ターゲット アドレス オブジェクトのパラメータ （8 ページ）を参照して ください。Multicloud Defense でリバース プロキシ ターゲット アドレス オブジェクトを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）]>[セキュリティポリシー（Security Policies）]>[アドレス（Addresses）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [リバースプロキシターゲット（Reverse Proxy Target）] を選択します。

ステップ 4 [名前（Name）] にアドレスオブジェクトを識別するための一意の名前を入力します。

ステップ 5 （任意）オブジェクトの説明を入力します。これにより、オブジェクトを他のオブジェクトと区別するのに役立つ文脈を提供できます。

ステップ 6 [オブジェクトタイプ（Object Type）] を選択します。オブジェクトタイプの詳細については、「アドレス オブジェクト （1 ページ）」を参照してください。次のいずれかのタイプを選択します。

- IP/CIDR/FQDN
- アプリケーション

ステップ 7 ステップ 6 で選択したタイプに応じて、次のパラメータを入力します。

- [値（Value）]：有効な IP、CIDR、または FQDN IP アドレスを入力します。
- [CSPアカウント（CSP Account）]：ドロップダウンメニューを使用して、 コントローラにすでに接続されているクラウド サービス プロバイダーのアカウントを選択します。
- [リージョン（Region）]：クラウド サービス プロバイダーの所在地であるリージョンをセレクトします。
- [VPC]：ドロップダウンメニューを使用して、VPC またはVNetを選択します。選択したクラウドサービス プロバイダーのアカウントによって、使用可能なオプションが異なる場合があることに注意してください。
- [サブネット（Subnet）]：ドロップダウンメニューを使用して、VPC または VNet に適用するサブネットを選択します。
- （Azure のみ）[リソースグループ（Resource Group）]：ドロップダウンメニューを使用して、選択内容と互換性のあるリソースグループを選択します。

ステップ 8 ドロップダウンメニューを使用して、このオブジェクトの既存の[アプリケーションタグ（Application Tag）] とその [値（Value）] の両方を選択します。

ステップ 9 完了したら、[保存（Save）] をクリックします。

アドレスオブジェクトの編集

変更できないパラメータを変更する必要がある場合は、アドレスオブジェクトをアドレスオブジェクトの複製してから、必要に応じてパラメータを変更する必要があります。

アドレスオブジェクトを編集するには、次の手順を実行します。すべてのパラメータを編集できるわけではないことに注意してください。

手順

ステップ 1 **[管理（Manage）]**>**[セキュリティポリシー（Security Policies）]**>**[アドレス（Addresses）]**に移動します。
ステップ 2 編集するアドレスオブジェクトの横にあるボックスをオンにします。
ステップ 3 [編集（Edit）] をクリックします。
ステップ 4 必要に応じてパラメータを変更します。
ステップ 5 完了したら、[保存（Save）] をクリックします。

アドレスオブジェクトの複製

元のアドレスオブジェクトの代わりにクローンを使用する場合は、元のすべての関連付けをクローンに置き換える必要があります。関連付けは、1 つ以上のセキュリティ ポリシー ルール セットのルールまたはリバース プロキシ サービス オブジェクトのセットで行われます。関連付けは、[詳細の表示（View Details）]を表示することで確認できます。

既存のアドレスオブジェクトを複製するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）]**>**[セキュリティポリシー（Security Policies）]**>**[アドレス（Addresses）]**に移動します。
ステップ 2 複製するアドレスオブジェクトの横にあるチェックボックスをオンにします。
ステップ 3 [複製（Clone）] をクリックします。
ステップ 4 必要に応じてパラメータを指定および変更します。
ステップ 5 完了したら、[保存（Save）] をクリックします。

アドレスオブジェクトの削除

アドレスオブジェクトがポリシールールセットまたはリバース プロキシ サービス オブジェクトでアクティブに使用されている場合、1 つ以上の関連付けが設定されるため、アドレスオブジェクトを削除できなくなります。アドレスオブジェクトを削除するには、最初にすべての関連付けを削除する必要があります。その後、アドレスオブジェクトを削除できます。関連付けは、[詳細の表示（View Details）]を表示することで確認できます。

手順

ステップ 1 **[管理（Manage）]**>**[セキュリティポリシー（Security Policies）]**>**[アドレス（Addresses）]**に移動します。
ステップ 2 削除するアドレスオブジェクトの横にあるボックスをオンにします。
ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 [保存（Save）] をクリックして削除を確認します。

[詳細の表示（View Details）]

アドレスオブジェクトの [詳細（Details）] を表示するには、**[管理（Manage）]**>**[セキュリティポリシー（Security Policies）]**>**[アドレス（Addresses）]**ページでオブジェクトの [名前（Name）] をクリックします。[詳細（Details）] には、そのタイプと設定に基づいて入力された IP、CDIR、および FQDN が表示されます。また、ポリシールールセットおよびオブジェクトサービスとの関連付けも表示されます。

[詳細の表示（**View Details**）]

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。