UCS ドメイン ポリシーの設定

ドメイン ポリシー

Cisco Intersight のドメイン ポリシーを使用すると、ポート設定、ネットワーク制御設定、VLAN と VSAN の設定など、UCS ファブリック インターコネクトのさまざまなパラメータを設定できます。ドメイン ポリシーは、任意の数のドメイン プロファイルに割り当てることで、構成基準を提供できます。Cisco Intersight のドメイン ポリシーは、アプリケーションに固有の新機能です。ドメイン プロファイルを使用したポリシーベースの構成は Cisco Intersight Essentials の機能であり、Cisco UCS B シリーズ M5 および M6 サーバ、Cisco UCS C シリーズ M5、M6、および M7 サーバ、および UCS ドメイン内の Cisco UCS X シリーズ M6 および M7 サーバでサポートされます。

Cisco Intersight のドメイン ポリシー作成ウィザードには 2 つのページがあります。

- **[全般（General）]**：組織を選択し、ポリシーの名前を入力できます。オプションで、ポリシーの識別に役立つ短い説明とタグ情報を含められます。タグはkey：value形式である必要があります。たとえば、Org:IT または Site:APJ などです。
- **[ポリシーの詳細（Policy Details）]**：ポリシーの詳細ページには、UCS ドメイン ポリシーに適用可能なプロパティがあります。

Cisco Intersight で設定できるドメイン ポリシーは次のとおりです。

- **[ポート ポリシー（Port Policy）]**：ファブリック インターコネクトのポートとポート ロールを設定します。各ファブリック インターコネクトには、ポートの集合が固定ポート モジュール内に存在します。ポートまたはポートチャネルをイネーブルまたはディセーブルにできます。

  ポート ポリシーはスイッチ モデルに関連付けられます。ネットワーク設定の制限は、スイッチ モデルによっても異なります。

  サポートされるポートとポート チャネルの最大数は次のとおりです。

  - イーサネット アップリンク、Fibre Channel over Ethernet（FCoE）アップリンク ポート チャネル、およびアプライアンス ポート チャネル（組み合わせ）：12
  - ポート チャネルあたりのイーサネット アップリンク ポート：16
  - ポート チャネルごとの FCoE アップリンク ポート：16
  - イーサネット アップリンクおよび FCoE アップリンク ポート（複合）：31
  - サーバ ポート：Cisco UCS 6454 では 54 ポート、Cisco UCS 64108 ファブリック インターコネクトでは 108 ポート

- **[イーサネット ネットワーク制御ポリシー（Ethernet Network Control Policy）]**：アプライアンス ポート、アプライアンス ポート チャネル、または vNICS のネットワーク制御構成を行います。
- **イーサネットネットワークグループポリシー（Ethernet Network Group Policy）**：アプライアンス ポート、アプライアンス ポート チャネル、または vNIC の許可 VLAN およびネイティブ VLAN を構成します。
- **[VLAN 設定ポリシー（VLAN Configuration Policy）]**：特定の外部 LAN への接続を生成します。
- **[VSAN 設定ポリシー（VSAN Configuration Policy）]**：ファイバ チャネル ファブリックを 1 つ以上のゾーンに分割します。各ゾーンでは、VSAN で相互通信できるファイバ チャネル イニシエータとファイバ チャネル ターゲットのセットが定義されます。
- **[NTP ポリシー（NTP Policy）]**：NTP サービスを有効にして、Cisco Intersight によって管理される UCS システムが NTP サーバの時刻と同期するように設定します。NTP サービスを有効化するには、NTP サーバとして動作する 1 ～ 4 台のサーバの IP/DNS アドレスを指定する必要があります。NTP サービスを有効にすると、Cisco Intersight によりエンドポイ

ント側で NTP の詳細が設定されます。詳細については、「NTP ポリシーの作成」を参照してください。

- **[ネットワーク接続ポリシー（Network Connectivity Policy）]**：エンドポイントから DNS サーバ上のリソース レコードを追加または更新するために使用される DNS ドメイン設定と、エンドポイント上の IPv4 および IPv6 用の DNS サーバ設定を指定します。

- **[システム QoS ポリシー（System QoS Policy）]**（プレビュー）：個々の vNIC にシステム クラスを割り当てることで、接続されたネットワークの重要性に基づいてネットワーク トラフィックの優先順位付けを行います。Intersight は、DCE（Data Center Ethernet）を使用して、Cisco UCS ドメイン内のすべてのトラフィックを処理します。イーサネットに対するこの業界標準の機能拡張では、イーサネットの帯域幅が 8 つの仮想レーンに分割されています。内部システムと管理トラフィック用に 2 つの仮想レーンが予約されています。それ以外の 6 つの仮想レーンの Quality of Service（QoS）を設定できます。Cisco UCS ドメイン全体にわたり、これら 6 つの仮想レーンで DCE 帯域幅がどのように割り当てられるかは、システム クラスによって決定されます。

  各システム クラスは特定のタイプのトラフィック用に帯域幅の特定のセグメントを予約します。これにより、過度に使用されるシステムでも、ある程度のトラフィック管理が提供されます。たとえば、[ファイバ チャネル優先度（Fibre Channel Priority）] システム クラスを設定して、FCoE トラフィックに割り当てる DCE 帯域幅の割合を決定することができます。構成のセットアップでは、システム クラスの各入力を検証して、重複または無効なエントリを防止します。

  この機能はプレビューであり、実稼働環境で使用するためのものではありません。Cisco では、テスト ネットワークまたはテスト システムでこの機能を使用することを推奨しています。

  次のリストは、設定可能なシステム クラスをまとめたものです。

  - Platinum、Gold、Silver、および Bronze：これらは、サービスプロファイルの QoS ポリシーに含めることができる設定可能なシステム クラスのセットです。各システム クラスはトラフィック レーンを 1 つ管理します。これらのシステム クラスのプロパティはすべて、カスタム 設定やポリシーを割り当てるために使用できます。

  - ベスト エフォート（Best Effort）：基本的なイーサネット トラフィックのために予約されたレーンに対する QoS を設定するシステム クラスです。このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、必要に応じて、データ パケットのドロップを許可するドロップ ポリシーがあります。このシステム クラスをディセーブルにはできません。

  - ファイバ チャネル（Fibre Channel）：これは、Fibre Channel over Ethernet トラフィックのために予約されたレーンでの Quality of Service を設定するシステム クラスです。このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、データ パケットが絶対にドロップされないことを保証するドロップなしポリシーがあります。このシステム クラスをディセーブルにはできません。

- **マルチキャストポリシー（Multicast Policy）**（プレビュー）：インターネット グループ管理プロトコル（IGMP）のスヌーピングおよびIGMPクエリアの設定に使用されます。IGMPスヌーピングは、特定のマルチキャスト伝送に含まれるべき VLAN のホストを動的に決定します。

  1 つ以上の VLAN に関連付けることができるマルチキャスト ポリシーを作成、変更、削除できます。マルチキャスト ポリシーが変更されると、そのマルチキャスト ポリシーに関連付けられたすべてのVLANが再処理され変更が適用されます。デフォルトでは、IGMPスヌーピングが有効になり、IGMP クエリアが無効になります。IGMP クエリアをイネーブルにすると、ローカルおよびピア IGMP スヌーピングクエリアインターフェイスの IPv4 アドレスを設定できます。

- **[Simple Network Management Protocol（SNMP）ポリシー（Simple Network Management Protocol (SNMP) Policy）]**：管理対象デバイスから SNMP トラップを利用して障害およびアラート情報を送信するためのSNMPを設定します。管理対象デバイスに設定されている既存の SNMP ユーザまたは SNMP トラップは削除され、このポリシーで設定するユーザまたはトラップに置き換えられます。

- **[Syslog ポリシー（Syslog Policy）]**：エンドポイントのローカル ロギングとリモート ロギング（最小シビラティ（重大度））を設定できます。このポリシーは、ローカルファイルおよびリモート syslog サーバに syslog メッセージを保存するための設定サポートも提供します。

- **[スイッチ制御ポリシー（Switch Control Policy）]**（プレビュー）：次を含むファブリック インターコネクト（FI）の複数のネットワーク操作を設定および管理できます。

  - **[ポート数の最適化（Port Count Optimization）]**：VLAN ポート数の最適化が有効になっている場合は、仮想ポート（VP）グループがファブリック インターコネクト（FI）で設定され、VLAN ポート数の最適化が無効になっている場合は、設定された VP グループが FI から削除されます。

  - **[MAC エージングタイム（MAC Aging Time）]**：MAC アドレステーブルエントリの MAC エージングタイムを設定できます。MAC エージングタイムは、MAC エントリが期限切れになり、MAC アドレステーブルからエントリを廃棄するまでの時間を指定します。

  - **[リンク制御グローバル設定（Link Control Global Settings）]**：メッセージ間隔時間の設定を秒単位で有効にし、err-disabled 状態のポートの回復アクションをリセットできます。

- **[フロー制御ポリシー（Flow Control Policy）]**：ポートおよびポート チャネルのプライオリティフロー制御の設定を有効にします。

- **[リンク制御ポリシー（Link Control Policy）]**：ポートのリンク制御管理状態と設定（通常またはアグレッシブ）モードを有効にします。

- **[リンク集役ポリシー（Link Aggregation Policy）]** リンク集約プロパティを設定できます。リンク集約は、複数のネットワーク接続を並列に組み合わせて、スループットを向上させ、冗長性を実現します。

ポート ポリシーの作成

ポートポリシーは、イーサネットまたはファイバチャネルトラフィックを伝送するユニファイドポート、ポートの役割、速度などのポートパラメータの設定に使用されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure** > **Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[ポート（Port）]** を選択して、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
スイッチ モデル	次の スイッチ モデルのいずれか 1 つを選択します。 • Cisco UCS 64108 ファブリック インターコネクト • Cisco UCS 6454 ファブリック インターコネクト • Cisco UCS 6536 ファブリック インターコネクト （注） スイッチモデルは、さまざまなネットワーク設定機能をポリシーに提供します。ポリシーが作成されると、スイッチモデルは変更できません。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
ユニファイド ポート デフォルトでは、未設定のすべてのポートはイーサネット ポートです。青いスライダーを使用して、ファイバーチャネルポートの範囲を選択します。選択したファイバーチャネル ポートが青色で強調表示されます。	
ファイバ チャネル（FC）	ファイバチャネル用に選択されたポート範囲を表示します。 （注） • Cisco UCS 6454 ファブリック インターコネクトの有効な FC ポート範囲：**[ポート 1 ～ 16（Port 1-16）]** • Cisco UCS 64108 ファブリック インターコネクトの有効な FC ポート範囲：**ポート 1 ～ 16** • Cisco UCS 6536 ファブリック インターコネクトの有効な FC ポート範囲：**ポート 33 ～ 36**
イーサネット	イーサネット用に選択されたポート範囲を表示します。

7. **[ブレイクアウトオプション]**ページで、ファイバーチャネルまたはイーサネットのブレイクアウト ポートを構成します。

（注） ブレイクアウト ポートを構成するには、ファブリック インターコネクト ファームウェアをファームウェア バージョン 4.2(2a) 以降にアップグレードする必要があります。

Cisco UCS 6536 ファブリック インターコネクトでは、FC ブレークアウトのみがサポートされています。

- グラフィック画像内の有効なポートをクリックするか、画像の下にある表でポート番号を選択して、ブレイクアウトするポートを選択します。

  以下は、さまざまな Cisco UCS ファブリック インターコネクトのブレイクアウト ポート範囲です。

  - Cisco UCS 64108 ファブリック インターコネクト、有効なブレイクアウト ポート範囲は 97 ～ 108

- Cisco UCS 6454 ファブリック インターコネクト、有効なブレークアウトポート範囲は 49 ～ 54
- Cisco UCS 6536 ファブリック インターコネクト。有効なブレイクアウト ポートの範囲は 1 ～ 36

- [構成（Configure）] をクリックします。

  ポップアップ ウィンドウが表示されます。ブレークアウト ポートに設定できる管理速度が表示されます。

  イーサネット ブレークアウト ポートは、ブレークアウトなし、4x10G の管理速度、4x25G の管理速度の 3 つのオプションで構成できます。

  FC ブレークアウト ポートは、4x8G、4x16G、および 4x32G の 3 つの異なる**管理速度**で構成できます。

- 目的の速度を選択します

（注） イーサネットブレークアウトを構成し、FI のリブートを必要とせずにブレークアウト速度を切り替えることができます。

FC ブレークアウト速度を変更しても、FI をリブートする必要はありません。

イーサネット ブレイクアウトから FC ブレイクアウトへの切り替え、またはその逆の切り替え、またはイーサネット ポートから FC ブレイクアウト ポートへの切り替え、またはその逆の切り替えには、毎回 FI のリブートが必要です。

- [設定（Set）] をクリックします。
- [次へ（Next）] をクリックします。

8. **[ポート ロール（Port Roles）]** ページで、グラフィック イメージで、またはグラフィック画像の下にある表で選択して、ポート ロール用に構成する必要があるポートを選択します。

選択したポート	選択したポート番号を示します。
名前	ユーザが決定したポート名。
タイプ（Type）	タイプは**イーサネット**または **FC**. です。

[ロール（Role）]	

ポートロールタイプを選択します。

イーサネット ポートのロールは次のとおりです。

- **Unconfigured**：デフォルト
- **サーバ（Server）** トラフィックはすべて、I/O モジュールを経由して、ファブリック インターコネクトのサーバ ポートへ進みます。

  （注）
  - Cisco UCS 6454 ファブリックインターコネクトの場合、許可されるサーバポートの最大数は、54 です。Cisco UCS 64108 ファブリックインターコネクトの場合、許可されるサーバポートの最大数は、108 です。
  - Cisco UCS 6536 ファブリック インターコネクトの場合、サーバー ロールは 10G ブレークアウト ポートではサポートされていません。
  - サーバー ポート構成は、Cisco UCS 6454 ファブリック インターコネクトのポート 49 ～ 54 および Cisco UCS 64108 ファブリック インターコネクトのポート 97 ～ 108 でブレークアウト ポートを構成した後にのみ、直接接続 Cisco UCS C シリーズ サーバーを検出するためにサポートされます。
  - Cisco UCS 6454 ファブリック インターコネクトの場合はポート 49 ～ 54、Cisco UCS 64108 ファブリック インターコネクトの場合はポート 97 ～ 108 にブレークアウト ポートを設定した後、シャーシ、シャーシに接続されたブレード サーバ、または FEX に接続されたラック サーバの検出はサポートされません。

- **イーサネットアップリンク**：イーサネットトラフィックはユニファイドアップリンクポートを通過します。

  （注） 許可されるイーサネットアップリンクポートと FCoE アップリンクポートの最大数は 31 です。

- **アプライアンス**：トラフィックがアップリンクポートを通過することなく、ネットワークファイルシステムがファブリックインターコネクトに直接接続できるようにします。

FC ポートのロールは次のとおりです。

- **FC アップリンク**：FC トラフィックは FC アップリンク ポート

	を通過します。FC ポートのロールを FC アップリンク ポートとして指定するには、ポートの VSAN スコープが、VSAN 設定ポリシーでストレージおよびアップリンクとして、またはアップリンクとして作成されている必要があります。 • **[FC ストレージ（FC Storage）]**—FC ポートはストレージ ポートとして機能します。FC ポートのロールを FC ストレージ ポートとして指定するには、ポートの VSAN スコープが、VSAN 設定ポリシーでストレージおよびアップリンクとして、またはストレージとして作成されている必要があります。さらに、FC がスイッチング モードになっている必要があります。 • **[未構成（Unconfigured）]**—未構成は、ポートのデフォルトのロールです。
管理速度	管理ポートの速度です。次のオプションがあります。 • 1GBPS • 10GBPS • 25GBPS • 40GBPS • 100GBPS （注） • ブレークアウト ポートのどのロールに対しても、管理速度を選択することはできません。 • Cisco UCS 6536 ファブリック インターコネクトの場合、サーバ ポートでは 25G/40G/100G 接続のみがサポートされます。 （注） 25GBPS の管理速度が選択されている場合、**[25GBPS 銅線ケーブル ネゴシエーションを有効にする（Enable 25GBPS Copper Cable Negotiation）]** は、3 メートルを超える銅ケーブルに対して自動的に有効になります。 25GBPS 銅線ケーブル ネゴシエーションを有効にします。 • アプライアンス、イーサネット アップリンク、FCoE アップリンク ポート ロールでのみサポートされます。 • ブレークアウト ポートをサポートしていません。 • ファームウェア バージョン 4.2(1a) 以降をサポートします。 • [自動（Auto）] に設定された FEC 構成のみをサポートします。
[VSAN ID]	VSAN 構成ポリシーで指定されている FC ポートの VSAN ID です。

FEC	ポートの前方誤り訂正設定: • 自動（Auto） • Cl91：25 GBPS および 100 GBPS の管理速度でサポート （注） サーバー ポート ロールに Cl91 が存在しません。 • Cl74：25GBPS の管理速度でサポート
優先度（Priority）	トラフィックをルーティングし、QoS を保証するポートのプライオリティを選択します。
モード（Mode）	ポートモードを選択します。ポートモードは、Trunk または Access です。

[接続されているデバイスの種類とデバイス番号（Connected Device Type and Device Number）]	各ポートまたは一連のポートのデバイス タイプとデバイス番号を選択します。 （注） このオプションは、サーバーの役割にのみ適用されます。 デフォルトでは、このオプションは無効になっています。 イネーブルにするには： • ポートを選択し、**[構成（Configure）]** をクリックします。 • **[手動シャーシ/サーバー番号付（Manual Chassis/Server Numbering）]**けボタンをオンにします。 各ポートの**[接続デバイス タイプ（Connected Device Type）]**と**[デバイス番号（Device Number）]**を指定できるテーブルが表示されます。 （注） **[自動入力番号付け（Auto-Fill Numbering）]**を有効にして、好みに応じて各ポートの**[接続デバイス タイプ（Connected Device Type）]**、**[開始デバイス番号（Starting Device Number）]**、および**[デバイスごとのポート（Ports per Device）]**を編集できます。 • [保存] をクリックして、[ポート ロール] リスト ビューに [接続されたデバイス タイプ] 列と [デバイス番号] 列を表示します。 （注） 選択した**[デバイス番号（Device Number）]**が他のポートの他のサーバー/シャーシにすでに割り当てられている場合、次に使用可能な番号が検出されたサーバーに割り当てられます。このアクションにより、ポート ポリシーの展開が失敗することはありません。 （注） ポート ポリシーの変更は FEX には適用されません。

イーサネット ネットワーク グループ	イーサネット アップリンクまたはアプライアンス ポートに接続するイーサネット ネットワーク グループ ポリシーを選択します。イーサネットネットワークグループポリシーは、許可された VLAN とネイティブ VLAN を指定します。 （注） イーサネット ネットワーク グループ ポリシーは、イーサネット アップリンクおよびアプライアンス ロールを持つポートにのみ適用されます。 （注） 分離 VLAN を構成するためのイーサネット ネットワーク グループを作成するには、グループが完全に分離していることを確認します。VLAN の部分的なオーバーラップは許可されません。
イーサネットネットワーク制御	アプライアンスポートにアタッチするイーサネットネットワーク制御ポリシーを選択します。イーサネットネットワーク制御ポリシーでは、CDP の有効化または無効化、MAC 登録モードの指定、アップリンク障害時のアクション、MAC セキュリティの詳細および LLDP の詳細を指定できます。 （注） イーサネットネットワーク制御ポリシーは、アプライアンスロールを持つポートにのみ適用されます。
[ポート（Port）]	有効なポート範囲を選択します。 • **ポート 1 ～96**：自動、10 GBPS、および 25 GBPS • **ポート 89～96**：自動、1 GBPS、10 GBPS、および 25 GBPS • **ポート 97～108**：自動、40 GBPS、および 100 GBPS
ポートチャネル **[ポートチャネルの作成（Create Port Channel）]** をクリックして、選択したポートのロールを選択します。 グラフィックイメージ内のポートをクリックするか、テーブル内の目的のポートの横にあるボックスをクリックして、設定するポートを選択します。	

[ロール（Role）]	ポートチャネルのロールタイプ。ロールタイプは次のいずれかになります。 • イーサネットアップリンクポートチャネル • FC アップリンクポートチャネル • FCoE アップリンクポートチャネル • アプライアンス ポートチャネル （注） • 許可されているポートの最大数： • イーサネット アップリンク ポート チャネル、FCoE アップリンク ポート チャネル、およびアプライアンス ポート チャネル（組み合わせ）は 12 • FC アップリンク ポート チャネルは 4 • ポートチャネルあたりのイーサネットポートは 16 • ポートチャネルごとのFCoEアップリンクポート：16 • どのポート チャネルに対しても、通常のポートとブレイクアウト ポートを組み合わせることはできません。たとえば、メンバーが 1/96 および 1/97/1 のアップリンク ポート チャネル ID 100 は許可されません。 • Cisco UCS 6536 ファブリック インターコネクトの速度が 100G のポートが N9K-C93180YC-FX3 に接続されている場合、ポート ロールを割り当てるときに**自動ネゴシエーション**を無効にする必要があります。 • FC アップリンク ポート チャネルの場合、ポート速度が異なるポート チャネルは許可されません。たとえば、FC アップリンク ポート チャネル ID 101、メンバー 1/33、ポート速度 8Gbps、および 1/34、ポート速度 16Gbps は許可されません。
PC ID	このスイッチに対してローカルなポートチャネルの固有識別子。

管理速度	アップリンク、アップリンクポートチャネル、および FCoE アップリンクポートチャネルの管理ポートチャネル速度オプションは次のとおりです。 • 1GBPS • 10GBPS • 25GBPS • 40GBPS • 100GBPS FC アップリンクおよび FC アップリンクポートチャネルの管理ポートチャネル速度オプションは次のとおりです。 • 8GBPS • 16GBPS • 32GBPS （注） ブレークアウト ポートの任意のロールには、管理速度を選択できません。
優先度（**Priority**）	トラフィックをルーティングし、QoS を保証するためのポートチャネルのプライオリティを選択します。
モード（**Mode**）	ポートチャネルモードを選択します。ポートチャネルモードは、Trunk または Access です。
イーサネット ネットワーク グループ	イーサネット アップリンクまたはアプライアンス ポート チャネルに接続するイーサネット ネットワーク グループ ポリシーを選択します。イーサネットネットワークグループポリシーは、許可された VLAN とネイティブ VLAN を指定します。 （注） イーサネット ネットワーク グループ ポリシーは、イーサネット アップリンクおよびアプライアンス ロールを持つポート チャネルに適用されます。 （注） 分離 VLAN を構成するためのイーサネット ネットワーク グループを作成するには、グループが完全に分離していることを確認します。VLAN の部分的なオーバーラップは許可されません。

イーサネットネットワーク制御	アプライアンスポートチャネルにアタッチするイーサネットネットワーク制御ポリシーを選択します。イーサネットネットワーク制御ポリシーでは、CDP の有効化または無効化、MAC 登録モードの指定、アップリンク障害時のアクション、MAC セキュリティの詳細および LLDP の詳細を指定できます。 （注） イーサネットネットワーク制御ポリシーは、アプライアンスロールを持つポートチャネルにのみ適用されます。
[ポート チャネル（Port Channel）]	選択有効ポート チャネルの範囲は 1 ～ 256 です。
ピン グループ ピン グループを使用して、サーバー上の vNIC/vHBA から、イーサネット/FC トラフィックをファブリック インターコネクトのアップリンク イーサネット/FC ポートにピン接続します。このピン接続を使用して、サーバからのトラフィックの分散を管理できます。FI がスイッチング モード (イーサネットおよび FC) の場合、静的ピン接続はサポートされません。 サーバーにピン接続を構成するには、LAN/SAN 接続ポリシーに LAN/SAN ピン グループを含める必要があります。 **[ピン グループの作成（Create Pin Group）]** をクリックして、LAN および SAN データトラフィックを流すことができる FI のポート/ポート チャネルを指定します。	
ピングループタイプ	ピンされたポート/ポート チャネルにフローする必要があるデータトラフィックのタイプ。タイプは次のとおりです。 • LAN • SAN
ピングループ名	ピン グループの名前。この名前は、ピン グループが作成されると、LAN/SAN 接続ポリシーの作成ページに表示されます。
インターフェイスタイプ	ファブリック インターコネクトのインターフェイスのタイプ。 • Port • ポート チャネル
Port Selection	使用可能な表から、データ トラフィック フローにピンする必要があるポートとブレークアウト ポートを選択できます。 デフォルトでは有効。

9. [保存（Save）] をクリックします。

イーサネット ネットワーク グループ ポリシーの作成

イーサネット ネットワーク グループ ポリシーを使用すると、UCS サーバ上の VLAN の設定を管理できます。これらの設定には、許可される VLAN の定義、ネイティブ VLAN の指定、QinQ VLAN の指定が含まれます。

このポリシーは、VIC QinQ トンネリングもサポートします。QinQ（802.1Qin802.1Q）トンネルにより、ネットワーク内の異なる VLAN を分離および分離できます。QinQ VLAN を設定するには、特定のポート、ポート チャネル、または vNIC の VLAN 設定の一部として、目的の VLAN ID を指定できます。これにより、単一の VLAN トランクを介した複数の VLAN の伝送が可能になります。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure** > **Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[イーサネット ネットワーク グループ（Ethernet Network Group）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	**[基本情報（Essential Information）]**
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの設定（Set Tags、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（Property）	**基本情報（Essential Information）**
VLAN 設定	

プロパティ（Property）	基本情報（Essential Information）
ネイティブ VLAN	このプロパティを使用すると、仮想インターフェイスのネイティブ VLAN ID または対応する vEthernet を 1 ～ 4093 の範囲で指定できます。 • ネイティブ VLAN が許可された VLAN にすでに含まれていない場合は、許可されたVLANのリストに自動的に追加されます。 • QinQ トンネリングが有効になっている場合、ネイティブ VLAN と許可 VLAN のプロパティが組み合わされます。
Q-in-Q トンネリングを有効にする	スライドして、VIC QinQ（802.1Qin802.1Q）トンネリングを有効にします。
[許可された VLAN（Allowed VLAN）]	仮想インターフェイスに許可される VLAN を参照します。カンマ区切りの VLAN ID と VLAN ID 範囲のリストを指定することで、許可された VLAN を指定できます。 たとえば、VLAN ID 10、20、30 ～ 40 を入力して VLAN 10、20、30 ～ 40 の範囲を許可できます。 （注） このプロパティは、*[QinQ トンネリングの有効化（Enable QinQ Tunneling）]* スライダが無効になっている場合にのみ表示されます。
QinQ VLAN	このプロパティにより、QinQ トンネリングの構成が有効になり、単一の VLAN 内の複数の VLAN のカプセル化が容易になります。サポートされる VLAN ID の範囲は 2 ～ 4093 で、ネットワークトラフィックを効果的に管理および分離できます。 （注） このプロパティは、*[QinQ トンネリングの有効化（Enable QinQ Tunneling）]* スライダが有効になっている場合にのみ使用できます。

（注） サーバーを隔離ホストまたはコミュニティ ホストにするには、許可VLANとネイティブVLANの両方で隔離 VLAN またはコミュニティ VLAN の ID を指定します。

7. **[作成（Create）]** をクリックします。

イーサネット ネットワーク制御ポリシーの作成

UCS ドメインのネットワーク制御設定を設定するイーサネットネットワーク制御ポリシー。このポリシーは、ポート ポリシーで定義されたアプライアンス ポート、および FI 接続された UCS サーバ上の LAN 接続ポリシーで定義された vNIC にのみ適用されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure** > **Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[イーサネット ネットワーク コントロール（Ethernet Network Control）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[CDP の有効化（Enable DNS）]	インターフェイスの Cisco Discovery Protocol（CDP）を有効にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[MAC 登録モード（MAC Register Mode）]	スイッチに登録する必要があるMACアドレスを決定します。次のように指定します。 • **[ネイティブ VLAN のみ（Only Native VLAN）]**：MACアドレスはネイティブVLAN のみに追加されます。デフォルトではこのオプションが設定され、port+VLAN のカウントが最大になります。 • **[すべてのホスト VLAN（All Host VLANS）]**：MAC アドレスは関連付けられたすべての VLAN に追加されます。トランキングを使用するよう設定されているが、無差別モードで実行されていない VLAN の場合、このオプションを選択します。
[アップリンク障害時の動作（Action on Uplink Fail）]	スイッチがエンドホスト モードのとき、使用可能なアップリンク ポートがないと、インターフェイスがどのように動作するか決定します。 • **[リンク ダウン（Link Down）]**：スイッチ上でアップリンク接続が失われたときにvNICの動作状態をダウンに変更します。vNIC のファブリック フェールオーバーが有効になります。これがデフォルトのオプションです。 • **[警告（Warning）]**：使用可能なアップリンク ポートがない場合であっても、サーバ間の接続を維持します。スイッチ上でアップリンク接続が失われたときのファブリック フェールオーバーは無効になります。

[プロパティ（Property）]	[基本情報（Essential Information）]
[MAC セキュリティ（MAC Security）] **[構築（Forge）]**	パケットがサーバからスイッチに送信される場合に、構築されたMACアドレスが許可されるか、または拒否されるかを決定します。次のように指定します。 • **[許可（Allow）]**：すべてのサーバ パケットは、そのパケットと関連付けられているMACアドレスとは無関係に、スイッチで受け入れられます。これがデフォルトのオプションです。 • **[拒否（Deny）]**：最初のパケットがファブリック インターコネクトに送信された後、それ以降のすべてのパケットは、それと同じMACアドレスを使用する必要があります。そうでなかった場合、スイッチによりメッセージなしで拒否されます。実質的に、このオプションによって、関連する vNIC のポート セキュリティが有効になります。
[LLDP]	インターフェイスが LLDP パケットを送受信できるかどうかを決定します。 • インターフェイス上での LLDP パケットの伝送を有効にするには、**[伝送を有効化（Enable Transmit）]** をクリックします。 • インターフェイス上での LLDP パケットの受信を有効にするには、**[受信を有効化（Enable Receive）]** をクリックします。

7. **[作成（Create）]** をクリックします。

VLAN ポリシーの作成

VLAN ポリシーによって特定の外部 LAN への接続が生成されます。VLAN は、ブロードキャスト トラフィックを含む、その外部 LAN へのトラフィックを切り離します。VLAN ポリシーを使用して、VLAN およびプライベート VLAN を作成できます。

（注） それぞれのVLANがマルチキャストポリシーに関連付けられていることを確かめてください。既存の VLAN を編集し、マルチキャスト ポリシーに関連付けることができます。マルチキャスト ポリシーをプライベート VLAN に関連付けることはできません。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure** > **Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[VLAN]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、**[VLAN の追加（Add VLAN）]** をクリックし、次のポリシーの詳細を設定します。

（注） イーサネット ネットワーク ポリシーごとに許可される VLAN の最大数は 3000 です。

[プロパティ（Property）]	[基本情報（Essential Information）]
VLANの追加	VLAN の追加をクリックして、VLAN とプライベート VLAN を追加します。
[名前/プレフィックス（Name/Prefix）]	単一の VLAN の場合、VLAN 名を指定します。VLAN の範囲の場合、各 VLAN 名に使用されるプレフィックスを指定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[VLAN ID]	VLAN ID 番号または 2 ～ 4093 の番号の範囲を入力します。ハイフンを使用してIDの範囲を入力することができ、複数のIDまたはID範囲をカンマで区切って入力できます。有効なVLAN IDまたはID範囲として、たとえば50、200、2000～2100を指定できます。3915～4042、4043～4047、4094、および4095のVLANは使用できません。該当するIDはシステム使用のために予約されているためです。 VLAN ID に割り当てる名前によって抽象化層が追加されることで、ネームド VLAN を使用するサービス プロファイルに関連付けされたすべてのサーバを一括してアップデートできるようになります。
[アップリンクでの自動許可（Auto Allow on Uplinks）]	このファブリックインターコネクトの全アップリンク ポートおよびポート チャネルでこの VLAN を許可するかどうかを決定するために使用されます。 **有効**：アップリンク ポートおよびポート チャネルでこの VLAN を許可します。 **無効**：非接続VLANの設定を無効にします。
マルチキャストポリシー	**[ポリシーの選択（Select Policy）]** をクリックし、VLAN に関連付ける必要があるマルチキャストポリシーを選択します。 すべての VLAN で使用可能な新しいマルチキャスト ポリシーを作成するには、**[新規作成（Create New）] を**クリックします。 （注） プライベート VLAN のマルチキャスト ポリシーは追加できません。
[VLAN 共有を有効にする（Enable VLAN Sharing）]	プライベート VLAN の作成を**[有効（Enable）]**にします。

[プロパティ（Property）]	[基本情報（Essential Information）]
[共有タイプ（Sharing Type）]	共有タイプは次のとおりです。 • **[プライマリ（Primary）]** : プライベート VLAN のプライマリ VLAN。セカンダリ VLAN はプライマリ VLAN にマッピングされます。 （注） 隔離 VLAN またはコミュニティ VLAN を作成する前に、プライマリ VLAN を作成する必要があります。 • **[隔離（Primary）]** : セカンダリ VLAN の 2 つの共有タイプの 1 つ。特定のプライマリ VLAN の下でマップできる隔離 VLAN は 1 つだけです。 • **[コミュニティ（Community）]**: セカンダリ VLAN の共有タイプの 1 つ。プライマリ VLAN には複数のコミュニティ VLAN をマップできます。
プライマリ VLAN ID	コミュニティまたは隔離 VLAN がマッピングされるプライマリ VLAN。 （注） セカンダリ VLAN がプライマリ VLAN にマッピングされている場合、プライマリ VLAN を変更または削除することはできません。

（注） ドメイン プロファイルの VLAN 構成が変更された場合、サーバー プロファイルの対応する変更は、サーバー プロファイルが再展開された後にのみ有効になります。

7. **[追加（Add）]** をクリックします。

VSAN ポリシーの作成

VSAN ポリシーを使用すると、同じ SAN ファブリックに物理的に接続されているデバイスを分離する Virtual SAN（VSAN）を作成できます。VSAN により、ファイバチャネルファブリッ

クのセキュリティと安定性が向上し、共通の物理インフラストラクチャ上に複数の論理 SAN を作成できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure** > **Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[VSAN]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次の手順を実行します。
   - **[トランキングモード（Trunking Mode）]** をクリックして、ファイバチャネルアップリンクトランキングを有効または無効にします。

     ファブリック インターコネクト上の名前付き VSAN でトランキングを有効ににした場合、そのファブリック インターコネクトのすべてのファイバ チャネル アップリンク ポートで、Cisco UCS ドメインのすべての名前付き VSAN が許可されます。ファブリック インターコネクトがファイバ チャネル エンドホスト モード用に設定されている場合、ファイバ チャネル アップリンクのトランキングを有効にすると、ID が 3840～4079 の範囲にあるすべての VSAN が動作不能になります。

   - **[VSAN の追加（Add VSAN）]** をクリックし、次のポリシーの詳細を設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[名前（Name）]	ユーザが VSAN コンフィギュレーションに付けた名前。

[プロパティ（Property）]	[基本情報（Essential Information）]
VSAN の範囲	VSAN の範囲です。VSAN がストレージおよびアップリンク VSAN、ストレージ VSAN、またはアップリンク VSAN のいずれであるかを示します。 VSAN の範囲は次のとおりです。 • ストレージとアップリンク • ストレージ • アップリンク （注） VSAN の FC ゾーン ポリシーを作成する場合、VSAN スコープはストレージである必要があります。
[VSAN ID]	スイッチ上の VSAN の一意の識別子。VSAN ID は 1 ～ 4093 の範囲で指定できます
[FCoE VLAN ID]	ファイバチャネル接続に使用される VLAN に割り当てられた固有識別情報。 VSAN 設定に関連付けられている FCOE VLAN の ID は、2 ～ 4093 である必要があります。3915ー4042、4043～4047、4094、4095のVLAN IDは、システム使用のために予約されています。 デフォルトでは、VLAN 4048 はスイッチの VSAN-1 にマッピングされます。VSAN ポリシーで FCoE に VLAN 4048 を使用しようとすると、エラーが発生します。この場合、VSAN ポリシーで別の FCOE VLAN ID を使用するように VSAN-1 を明示的に設定する必要があります。

7. **[作成（Create）]** をクリックします。

NTP ポリシの作成

NTP ポリシーは、Cisco Intersight によって管理される UCS システムが NTP サーバの時刻と同期するように設定するために、NTP サービスを有効にします。NTP サービスを有効化するに

は、NTP サーバとして動作する 1 ～ 4 台のサーバの IP/DNS アドレスを指定する必要があります。NTP サービスを有効にすると、Cisco Intersight によりエンドポイント側で NTP の詳細が設定されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure** > **Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[NTP]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[Enable NTP]	NTP ポリシー設定をイネーブルにします。
NTP サーバ （NTP Servers）	NTP サーバの IP アドレスまたはホスト名のコレクション。
[タイム ゾーン（Time Zone）]	エンドポイントのタイムゾーンを選択できるタイムゾーンのコレクション。 このプロパティは、スイッチおよび Cisco IMC（スタンドアロン）サーバに適用されます。

NTP の設定にホスト名を使用する場合は、ネットワーク接続ポリシーで DNS サーバ情報を設定する必要があります。

7. **[作成（Create）]** をクリックします。

ネットワーク接続ポリシーの作成

ネットワーク接続ポリシーを使用すると、IPv4 アドレスと IPv6 アドレスを設定して割り当てることができます。

[ダイナミック DNS（Dynamic DNS）]

ダイナミック DNS（DDNS）は、 DNS サーバのリソース レコードを追加または更新するために使用されます。DDNS オプションを有効にすると、DDNS サービスは現在のホスト名、ドメイン名、および管理 IP アドレスを記録し、DNS サーバのリソース レコードを更新します。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure** > **Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[ネットワーク 接続（Network Connectivity）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のプロパティを設定します。

   [共通プロパティ（Common Properties）]

[プロパティ（Property）]	[基本情報（Essential Information）]
[ダイナミック DNS の有効化]（Enable Dynamic DNS）	ダイナミック DNS を有効化します。 このプロパティは、ファブリック インターコネクトには適用されません。
[ダイナミック DNS 更新ドメイン（Dynamic DNS Update Domain）]	ダイナミック DNS ドメインを指定します。このドメインは、メイン ドメインまたはサブ ドメインのどちらにもできます。 このプロパティは、ファブリックインターコネクトには適用されません。

IPv4 のプロパティ

[プロパティ（Property）]	[基本情報（Essential Information）]
DHCP から IPv4 DNS サーバアドレスを取得	IPv4 アドレスが Dynamic Host Configuration Protocol（DHCP）から取得されるか、または特定の DNS サーバのセットから取得されるか。 • [有効（Enabled）]：Intersight は DHCP を使用します • [無効（Disabled）]：Intersight は IPv4 DNS サーバの設定済みセットを使用します。 このプロパティは、ファブリック インターコネクトには適用されません。
[優先 IPv4 DNS サーバ（Preferred IPv4 DNS Server）]	プライマリ DNS サーバの IP アドレス。このプロパティは、**[IPv4 DNS サーバアドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。
[代替 IPv4 DNS サーバ（Alternate IPv4 DNS Server）]	セカンダリ DNS サーバの IP アドレス。このプロパティは、**[IPv4 DNS サーバ アドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。

[プロパティ（Property）]	[基本情報（Essential Information）]
[IPv6 の有効化（Enable IPv6）]	IPv6 を有効にするかどうかを指定します。IPv6 プロパティは、このプロパティが有効になっている場合にのみ設定できます。

[IPv6 のプロパティ（IPv6 Properties）]

[プロパティ（Property）]	[基本情報（Essential Information）]
DHCP から IPv6 DNS サーバアドレスを取得	IPv6 アドレスが Dynamic Host Configuration Protocol（DHCP）から取得されるか、または特定の DNS サーバのセットから取得されるか。 • [有効（Enabled）]：Intersight は DHCP を使用します • [無効（Disabled）]：Intersight は IPv6 DNS サーバの設定済みセットを使用します。 このプロパティは、ファブリック インターコネクトには適用されません。
[優先 IPv6 DNS サーバ（Preferred IPv4 DNS Server）]	プライマリ DNS サーバの IP アドレス。このプロパティは、**[IPv6 DNS サーバアドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。
[代替 IPv6 DNS サーバ（Alternate IPv4 DNS Server）]	セカンダリ DNS サーバの IP アドレス。このプロパティは、**[IPv6 DNS サーバアドレスを DHCP から取得（Get IPv4 DNS Server Addresses from DHCP）]** が無効になっている場合にのみ表示されます。

7. **[作成（Create）]** をクリックします。

SNMP ポリシーの作成

SNMP ポリシーでは、管理対象デバイスから SNMP トラップを利用して障害およびアラート情報を送信するための SNMP 設定を設定します。このポリシーは、SNMPv1、SNMPv2（v2c を含む）、SNMPv3 などの SNMP バージョンをサポートします。管理対象デバイスに設定されている既存の SNMP ユーザまたは SNMP トラップは削除され、このポリシーで設定するユーザまたはトラップに置き換えられます。

SNMP ポリシーを使用すると、SNMP を有効または無効にしたり、アクセスおよびコミュニティ ストリングを指定したり、データの取得に使用する SNMP ユーザの詳細を指定したりできます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。

3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[SNTP]** を選択して、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[SNMP の有効化（Enable DNS）]	エンドポイントでの SNMP ポリシーの状態を表示します。エンドポイントから指定ホストに SNMP トラップを送信するには、このオプションを有効にします。
[アクセス コミュニティ ストリング（Access Community String）]	SNMPv1、SNMPv2 コミュニティストリング、またはSNMPv3ユーザ名を入力します。フィールドには 18 文字まで入力できます。
[トラップ コミュニティ ストリング（Trap Community String）]	他のデバイスに SNMP トラップを送信する際に使用する SNMP コミュニティ グループの名前を入力します。 （注） このフィールドは、SNMPv2c トラップホストまたは宛先にのみ適用されます。
[システム連絡先（System Contact）]	SNMP の実装担当者の連絡先。電子メールアドレスまたは名前と電話番号など、最大 64 文字の文字列を入力します。
[システムの場所（System Location）]	SNMP エージェント（サーバ）が動作するホストの場所。
[SNMP ユーザ（SNMP Users）]	

[プロパティ（Property）]	[基本情報（Essential Information）]
[名前（Name）]	SNMPv3ユーザ名を入力します。このフィールドは 1〜31 文字で指定する必要があります。
[セキュリティ レベル（Security Level）]	エージェントとマネージャーの間での通信で使用するセキュリティ メカニズムを選択します。 • AuthPriv • AuthNoPriv
[認証タイプ（Auth Type）]	ユーザの許可プロトコルとして **[SHA]** を選択します。 （注） MD5 認証プロトコルはサポートされていません。
[認証パスワード（Auth Password）]	ユーザの認証パスワードを入力します。
[認証パスワードの確認（Auth Password Confirmation）]	ユーザの認証パスワードを確認のため入力します。
[プライバシータイプ（Privacy Type）]	ユーザのプライバシープロトコルとして **[AES]** を選択します。 （注） **[DES]** プライバシータイプは、セキュリティ標準を満たすために廃止されました。
[プライバシー パスワード（Privacy Password）]	ユーザのプライバシー パスワードを入力します。
[プライバシーパスワードの確認（Privacy Password Confirmation）]	ユーザのプライバシー パスワードを確認のため入力します。
[SNMP トラップの宛先（SNMP Trap Destinations）]	
[有効化（Enable）]	SNMP ポリシーを使用するには、このオプションを有効にします。
[SNMP バージョン（SNMP Version）]	トラップの SNMP バージョンとして **[V2]** または **[V3]** を選択します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[ユーザ（User）]	トラップの SNMP ユーザを選択します。最大 15 のトラップ ユーザを定義できます。 （注） このフィールドは SNMPv3 にのみ適用されます。
[トラップ タイプ（Trap Type）]	宛先にトラップが送信されたとき、どのタイプであれば通知を受信するかを選択します: • [トラップ（Trap）] • [情報（Inform）]
[宛先アドレス（Destination Address）]	SNMP トラップ情報の送信先アドレスを指定します。最大 10 のトラップ宛先を定義できます。
[ポート（Port）]	入力のサーバーがトラップの宛先と通信するために使用するポート番号を入力します。値の範囲は 1 ～ 65535 です。デフォルトは 162 です。

7. **[作成（Create）]** をクリックします。

システム QoS ポリシーの作成

システム Quality of Service (QoS) ポリシーは、発信トラフィックにシステム クラスを割り当てます。このシステムクラスにより、そのトラフィックの QoS が決定されます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[システム QoS（System QoS）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
Platinum **Gold** **Silver** **Bronze**	このオプションを使用すると、ファブリックインターコネクトに関連付けられた QoS クラスを設定し、そのクラスをQoSポリシーに割り当てることができます。 （注） デフォルトでは、**Best Effort** または **Fibre Channel** システム クラスがイネーブルになっています。
CoS	0 ～ 6 の整数を入力して、サービス クラス（CoS）を設定します。0 は最低プライオリティを表し、6 は最高プライオリティを表します。QoS ポリシーを削除する際や、割り当てられたシステム クラスが無効な際に、システム クラスをトラフィックのデフォルト システム クラスにする必要がある場合を除き、この値を 0 に設定することは避けるよう推奨します。
重み付け	1 ～ 10 の整数。整数を入力すると、**[重み付け（Weight）]** フィールドの説明に従って、このプライオリティ レベルに割り当てられるネットワーク帯域幅の割合が決定されます。
パケット ドロップを許可する	送信中にこのシステムクラスのパケットドロップを許可するように選択できます。 このフィールドは、**[Best Effort] ク**ラスの場合はつねににオンで、パケットのドロップが許可されます。**[Fibre Channel]** の場合はつねにオフで、パケットのドロップは許可されません。

[プロパティ（Property）]	[基本情報（Essential Information）]
[MTU]	チャネルの最大伝送単位（MTU）です。1500 ～ 9216 の範囲の整数を入力します。この値は最大パケット サイズに対応します。

7. **[作成（Create）]** をクリックします。

Syslog ポリシーの作成

Syslog ポリシーでは、エンドポイントからのロギング レベルとして、記録する最小シビラティ（重大度）を定義します。ポリシーはまた、sisylog メッセージを保存するターゲットの場所と、リモート ロギング サーバのホスト名または IP アドレス、ポート情報、および通信プロトコルを定義します。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[Syslog]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
ローカルロギング（Local Logging）	

[プロパティ（Property）]	[基本情報（Essential Information）]
[報告する最小シビラティ（重大度）（Minimum Severity to Report）]	リモート ログで報告する最低のシビラティ（重大度）レベルを選択します。シビラティ（重大度）は次のとおりです。 • 0 緊急 • 1 アラート • 2 重大 • 3 エラー • 4 警告 • 5 通知 • 6 情報 • 7 デバッグ
[リモートロギング：Syslog サーバ 1 および Syslog サーバ 2（Remote Logging - Syslog Server 1 and Syslog Server 2）]	
[有効化（Enable）]	Syslog ポリシーを有効または無効にするには、このオプションを選択します。
[ホスト名/IP アドレス（Hostname/IP Address）]	Cisco IMC ログを保存する Syslog サーバのホスト名または IP アドレスを入力します。リモート システムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。 （注） リモートロギングアドレスとして IPv4 と IPv6 の両方がある場合は、コマンドライン インターフェイス（CLI）を使用して、ファブリック インターコネクトでの IPv4 と IPv6 を設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[報告する最小シビラティ（重大度）（Minimum Severity to Report）]	リモート ログで報告する最低のシビラティ（重大度）レベルを選択します。シビラティ（重大度）は次のとおりです。 • 0 緊急 • 1 アラート • 2 重大 • 3 エラー • 4 警告 • 5 通知 • 6 情報 • 7 デバッグ

7. **[作成（Create）]** をクリックします。

スイッチ制御ポリシーの作成

スイッチ制御ポリシーは、VLAN 数の最適化、、MAC アドレスのエージング時間の設定、およびリンク制御のグローバル設定をサポートします。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[スイッチ制御（Switch Control）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグ（Tag、オプション）]	key-value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. [ポリシーの詳細（Policy Details）] ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
スイッチング モード	
イーサネット	イーサネット切り替えモードを指定します。切り替えモードは、エンド ホストまたはスイッチのいずれかです。 エンドホスト モードでは、ファブリック インターコネクトは、複数のリンクを持つエンド ホストとしてアップストリーム デバイスに表示されます。このモードでは、スイッチはスパニング ツリー プロトコルを実行せず、一連のトラフィック転送ルールに従ってループを回避します。 スイッチ モードでは、スイッチはループを回避するためにスパニング ツリー プロトコルを実行し、ブロードキャストおよびマルチキャスト パケットは従来の方法で処理されます。

[プロパティ（Property）]	[基本情報（Essential Information）]
FC	FC 切り替えモードを指定します。切り替えモードは、エンド ホストまたはスイッチのいずれかです。 エンドホストモードを使用すると、ファブリック インターコネクトは、vHBA を介して接続されているすべてのサーバー（ホスト）に代わって、接続されているファイバチャネル ネットワークに対するエンドホストとして動作することができます。これは、vHBA をファイバ チャネル アップリンク ポートにピン接続することにより実現されます（動的なピン接続または固定のピン接続のいずれか）。これにより、ファイバチャネルポートはファブリックの残りの部分に対してサーバー ポート（N ポート）となります。エンドホスト モードの場合、ファブリック インターコネクトは、アップリンク ポートがトラフィックを相互に転送するのを拒否することでループを回避します。 スイッチ モードは従来のファイバ チャネル スイッチング モードです。スイッチ モードを使用して、ファブリック インターコネクトをストレージ デバイスに直接接続することができます。ファイバ チャネル スイッチ モードの有効化は、SAN が存在しない（たとえば、ストレージに直接接続された 1 つの Cisco UCS システム）POD モデル、または SAN が存在する（アップストリーム MDS を使用）ポッド モデルで役に立ちます。
VLAN ポート数	
VLAN ポート数最適化の有効化	VLN ポート数の最適化を有効にします。このオプションは、デフォルトで無効です。 （注） IMM の Cisco UCS 6400 シリーズおよび 6500 シリーズ FI で VLAN ポート数の最適化が有効になっている PV 数は 108000 です。
システム予約済み VLAN	

[プロパティ（Property）]	[基本情報（Essential Information）]
予約済み VLAN 開始 ID	

[プロパティ（Property）]	[基本情報（Essential Information）]
	予約済みVLAN範囲の開始IDを指定するには、このオプションを選択します。デフォルトでは、開始 ID は 3915 です。開始 ID + 127 の VLAN ID は、VLAN または VSAN ポリシーの構成に使用できません。たとえば、VLAN 開始 ID が 3912 に変更される場合、予約済み VLAN 範囲は 3912-4039 です。予約済みVLAN範囲は、ユーザー定義のVLANまたはVSANポリシーには使用できません。 （注） 始める前に： • 新しい予約済み VLAN 範囲内の既存の VLAN をすべて削除します。 • VLAN または VSAN ポリシーで使用されている予約済み VLAN ブロックに、VLAN または FCoE VLAN がないことを確認します。つまり、ファブリックインターコネクト A と B の両方の VLAN および VSAN ポリシーが、予約済みの VLAN 範囲と競合しないようにします。 • 予約済み VLAN 開始 ID が変更された場合、新しい範囲に含まれていない古い範囲の VLAN は、新しいスイッチ制御ポリシーが展開された後に VLAN および VSAN ポリシーに使用できます。 • デフォルトの予約済み VLAN 範囲は 3916 ～ 4095 です。このシステム予約済みVLAN範囲は変更できますが、VLAN 1002 ～ 1005 は内部使用のためにブロックされており、システム予約済み範囲の一部として使用できないことに注意して

[プロパティ（Property）]	[基本情報（Essential Information）]
	ください。 （注） • 変更を有効にするために、ファブリックインターコネクトが再起動します。複数の変更が加えられた場合でも、再起動は 1 回だけ発生します。 • デバイスの要求解除では、以前に構成された予約済み VLAN は削除されません。その後の要求では、ユーザーが新しい範囲を使用する場合は、スイッチコントロールポリシーを介して予約済み VLAN を構成する必要があります。
予約済み VLAN 終了 ID	予約済み VLAN 範囲の終了 ID。システムは、指定された VLAN 開始 ID から 128 の予約済み VLAN をブロックします。デフォルトでは、終了 ID は 4042 です。この ID は、VLAN ポリシーの構成には使用できません。
MAC アドレステーブルのエージングタイム	
Default	このオプションでは、エンド-ホストモードのデフォルトの MAC アドレスエージング時間を 14,500 秒 に設定します。
Custom	ユーザがスイッチの MAC アドレスエージングタイムを設定できるようにするには、このオプションを選択します。 スイッチモデル UCS-FI-6454 以降のバージョンの場合、有効な時間範囲は 120〜918000 秒です。ユーザが時間範囲を定義すると、スイッチは定義された時間を 5 の倍数にリセットします。

[プロパティ（Property）]	[基本情報（Essential Information）]
なし	MACアドレスエージングプロセスを無効にするには、このオプションを選択します。このオプションは、MACエントリが期限切れにならず、MACアドレステーブルから破棄されないようにします。
エージングタイム (秒)	MACアドレスのエージングタイムを秒単位で定義します。このフィールドは、**[カスタム（Custom）]** オプションを選択した場合にのみ有効になります。
単一方向リンク検出（UDLD）グローバル設定	
メッセージの間隔	アドバタイズメント モードで、双方向に設定されているポートで、UDLDプローブ メッセージ間隔（秒）を定義します。 （注） 有効なメッセージ間隔の時間の範囲は 7ー90 秒です。
リカバリアクション	errdisable のポートを回復するには、**[Reset]** を選択します。 （注） デフォルトでは **[なし（None）]** オプションが選択されています。
ファブリック ポート チャネル vHBA	

[プロパティ（**Property**）]	[基本情報（**Essential Information**）]
ファブリック ポート チャネルの **vHBA** リセットの有効化	

[プロパティ（Property）]	[基本情報（Essential Information）]
	仮想ホスト バス アダプタ（vHBA）は、仮想マシンを論理的にファブリック インターコネクト上の仮想インターフェイスに接続し、仮想マシンがそのインターフェイスによってトラフィックを送受信できるようにします。これは現在、ファイバ チャネル モード (エンドホスト モード/スイッチ モード) を使用して実現されています。 ファブリック インターコネクトと I/O モジュール（IOM）間のメンバー リンクの追加または削除を伴うポート チャネル操作です。このような操作を行うと、I/O の一時停止が長くなったり、仮想マシンからそのターゲットへの接続が切断されたりする可能性があり、vHBA リセットのサポートが必要になります。 **ファブリック ポートチャネル vHBA リセット**が有効に設定されている場合、Cisco UCS IOM ポート チャネル メンバーシップが変更されると、ファブリック インターコネクトは、その Cisco UCS IOM を介して構成された各 vHBA に登録済み状態変更通知（Registered State Change Notification、RSCN）パケットを送信します。RSCN は、仮想インターフェイス カード (VIC) または VIC ドライバがファブリック ポートチャネル vHBA をリセットし、接続を復元できるようにします。 デフォルトでは、ファブリック ポートチャネルの vHBA リセットは無効に設定されています。 無効（デフォルト）の場合、vHBA のリセットは、ファブリック ポート チャネルのすべてのメンバーがダウンしている場合にのみ実行されます。 （注） • この機能は、Cisco Intersight インフラストラクチャ ファームウェア バージョン 4.1(3e) 以降でサポートされています。 • ESX NFNIC ドライバ バー

[プロパティ（Property）]	[基本情報（Essential Information）]
	ジョン 5.0.0.37 以降または 4.0.0.87 以降は、この RSCN を処理します。 • Linux FNIC ドライバ バージョン 2.0.0.85 以降は、この RSCN を処理します。

7. **[作成（Create）]** をクリックします。

.

（注）

- [ポリシーの詳細（Policy Details）] ページで、既存のすべてのスイッチ制御ポリシーのリンク制御グローバル設定フィールドの値が空白として表示されます。これらのポリシーは、ポリシーの編集/更新時に正しい値を表示します。
- ファブリック インターコネクトの切り替えモードを変更すると、ファブリック インターコネクトはリブートします。

フロー制御ポリシーの作成

ポートごとにプライオリティフロー制御を構成して、システムQoSポリシーおよびイーサネットQoSポリシーによって定義されたCoSのno-drop動作を有効にします。自動およびオンの優先順位では、受信および送信リンク レベルのフロー制御はオフになります。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[フロー制御（Flow Control）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。

プロパティ（**Property**）	基本情報（**Essential Information**）
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（**Property**）	基本情報（**Essential Information**）
プライオリティフロー制御モード	
Auto	Auto はプライオリティフローを送受信します。このフィールドは、デフォルトでイネーブルにされています。
オン（**On**）	ローカルポートでプライオリティ制御フローをイネーブルにします。 （注） **送信方向**と**受信方向**を同時に有効にすることはできません。

プロパティ（**Property**）	基本情報（**Essential Information**）
[オフ（Off）]	ローカル ポートでプライオリティ制御フローを有効にします。 （注） **[送信方向（Send）]** と **[受信方向（Receive）]** を同時に有効にすることができます。
	送信 有効にすると、リンク レベル フロー制御は送信方向に構成されます。
	[受信（Receive）] 有効にすると、リンク レベル フロー制御は受信方向に構成されます。

（注） 優先順位フロー制御が**自動**、**オン**モードの場合、フロー制御を有効にすることはできず、オプションはリストされません。フロー制御を有効にするには、優先フロー制御を**オフ**モードに設定する必要があります。

（注） フロー制御は、フロー制御対応デバイスに接続されているインターフェイスでのみ有効にする必要があります。次のインターフェイス タイプがサポートされています。

- イーサネット アップリンク ポートおよびポート チャネル

7. **[作成（Create）]** をクリックします。

リンク集約ポリシーの作成

このポリシーは、リンク集約プロパティの設定に使用できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure** > **Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[リンク アグリゲーション（Link Aggregation）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[個別に一時停止）Suspend Individual）]	
[いいえ（False）]	**[いいえ（False）]** を選択して、ピアポートからの PDU の受信を続行します。
[はい（True）]	ピアポートから PDU を受信していないポートを一時停止するには、**[はい（True）]** を選択します。
[ACP レート（LACP Rate）]	
[標準（Normal）]	ポートは 30 秒ごとに 1 PDU を受信します。このタイムアウトは 90 秒です。
[高速（Fast）]	ポートはピア ポートから 1 秒ごとに 1 PDU を受信します。このタイムアウトは 3 秒です。

（注） リンク集約は、リンク集約対応デバイスに接続されているインターフェイスでのみ有効にする必要があります。次のインターフェイス タイプがサポートされています。

- イーサネット アップリンク ポート チャネル
- FCoE アップリンク ポート チャネル

7. **[作成（Create）]** をクリックします。

リンク集約ポリシーの作成

このポリシーは、ポートのリンク制御管理状態と構成（通常またはアグレッシブ）モードの構成を有効にします。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure > Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[リンク制御（Link Control）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明（Description、オプション）]	簡単な説明を入力します。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

プロパティ（Property）	基本情報（Essential Information）
[リンク制御の管理状態（Link Control Administrative State）] 管理者が設定および管理を行うポートのリンク制御状態。	
[リンク制御モード（Link Control Mode）]	

プロパティ（Property）	基本情報（Essential Information）
[標準（Normal）]	光ファイバ接続上のインターフェイスの誤った接続による単方向リンクを検出します。
[アグレッシブ（Aggressive）]	光ファイバ リンク上のインターフェイスの誤った接続による単方向リンクに加え、光ファイバ リンクおよびツイストペア リンク上の一方向トラフィックによる単方向リンクも検出します。 • **[UDLD 管理状態（Administrative State）]** が無効の場合、ポリシーを **[アグレッシブ（Aggressive）]** モードに設定できません。 • **[UDLD モード（UDLD Mode）]**（（[通常（normal）] または [アグレッシブ（aggressive）]）を構成する場合、必ず単方向リンクの両側に同じモードを構成してください。

（注） リンク制御ポリシーは、リンク制御対応デバイスに接続されているインターフェイスでのみ有効にする必要があります。次のインターフェイス タイプがサポートされています。

- イーサネット アップリンク ポート
- FCoE アップリンク ポート
- イーサネット アップリンク ポート チャネル
- FCoE アップリンク ポート チャネル

7. **[作成（Create）]** をクリックします。

マルチキャスト ポリシーの作成

マルチキャストポリシーは、Internet Group Management Protocol（IGMP）のスヌーピングおよび IGMP クエリアの設定に使用されます。

（注） それぞれのVLANがマルチキャスト ポリシーに関連付けられていることを確かめてください。既存の VLAN を編集し、マルチキャスト ポリシーに関連付けることができます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ（Service Selector）]** ドロップダウン リストから、**[インフラストラクチャ サービス（Infrastructure Service）]** を選択します。
3. **[ポリシーの構成（Configure** > **Policies）]** に移動し、**[ポリシーの作成（Create Policy）]** をクリックします。
4. **[マルチキャスト（Multicast）]** を選択し、**[スタート（Start）]** をクリックします。
5. **[全般（General）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[組織（Organization）]	組織を選択します。
[名前（Name）]	ポリシーの名前を入力します。
[説明（Description、オプション）]	簡単な説明を入力します。
[タグの追加（Add Tag、オプション）]	key:value形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。

6. **[ポリシーの詳細（Policy Details）]** ページで、次のパラメータを設定します。

[プロパティ（Property）]	[基本情報（Essential Information）]
[スヌーピングの状態（Snooping State）]	IGMP スヌーピングが、どのインターフェイスがホスト、またはマルチキャスト トラフィックの受信で重要な他のデバイスに接続されているかを検出するため、VLAN 内の IGMP プロトコル メッセージを調べるかどうかを決定します。次のいずれかになります。 • **[有効（Enabled）]** : IGMP スヌーピングは、このポリシーに関連付けられた VLAN に使用されます。 • **[無効（Disabled）]** : IGMP スヌーピングは、関連付けられた VLAN に使用されません。

[プロパティ（Property）]	[基本情報（Essential Information）]
[クエリアの状態（Querier State）]	IGMP スヌーピング クエリアが、IP マルチキャスト トラフィックを受信する必要のあるホストからの IGMP レポート メッセージをトリガーするために、IGMP クエリーを定期的に送信するかどうかを決定します。次のいずれかになります。 • **[有効（Enabled）]**：IGMP クエリーは定期的に送信されます。 • **[無効（Disabled）]**：IGMP クエリーは送信されません。これがデフォルトのオプションです。
クエリアの IP アドレス	IGMP スヌーピング クエリア インターフェイスの IPv4 アドレス。 このフィールドは、**[クエリアの状態（Querier State）]** が有効な場合にのみ表示されます。
[クエリアの IP アドレスのピア（Querier IP Address Peer）]	（オプション）ピア IGMP スヌーピング クエリア インターフェイスの IPv4 アドレス。このピア IP アドレスは FI-B に割り当てられます。 このフィールドは、**[クエリアの状態（Querier State）]** が有効な場合にのみ表示されます。

7. **[作成（Create）]** をクリックします。

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。