MACsec

この章は、次の内容で構成されています。

MACsec について

MACsec は、IEEE 802.1AE 規格ベースのレイヤ 2 ホップバイホップ暗号化であり、これにより、メディア アクセス非依存プロトコルに対してデータの機密性と完全性を確保できます。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。

802.1 ae MKA と暗号化はリンク、つまり、リンク (ネットワーク アクセス デバイスと、PC か IP 電話機などのエンドポイント デバイス間のリンク) が直面しているホストのすべてのタイプでサポートされますかにリンクが接続されている他のスイッチまたはルータ。

MACsec は、イーサネット パケットの送信元および宛先 MAC アドレスを除くすべてのデータを暗号化します。ユーザは、送信元と宛先の MAC アドレスの後に最大 50 バイトの暗号化をスキップするオプションもあります。

WAN またはメトロ イーサネット上に MACsec サービスを提供するために、サービス プロバイダーは、Ethernet over Multiprotocol Label Switching（EoMPLS）および L2TPv3 などのさまざまなトランスポート レイヤ プロトコルを使用して、E-Line や E-LAN などのレイヤ 2 透過サービスを提供しています。

EAP-over-LAN（EAPOL）プロトコルデータ ユニット（PDU）のパケット本体は、MACsec Key Agreement PDU（MKPDU）と呼ばれます。3 回のハートビート後（各ハートビートは 2 秒）に

参加者から MKPDU を受信しなかった場合、ピアはライブ ピア リストから削除されます。たとえば、クライアントが接続を解除した場合、スイッチ上の参加者はクライアントから最後の MKPDU を受信した後、3 回のハートビートが経過するまで MKA の動作を継続します。

APIC ファブリック MACsec

APIC はまたは責任を負う MACsec キーチェーン ディストリビューションのポッド内のすべてのノードに特定のポートのノードになります。サポートされている MACsec キーチェーンし、apic 内でサポートされている MACsec ポリシー ディストリビューションのとおりです。

- 単一ユーザ提供キーチェーンと 1 ポッドあたりポリシー
- ユーザが提供されるキーチェーンとファブリック インターフェイスごとのユーザが提供されるポリシー
- 自動生成されたキーチェーンおよび 1 ポッドあたりのユーザが提供されるポリシー

ノードは、複数のポリシーは、複数のファブリック リンクの導入を持つことができます。これが発生すると、ファブリック インターフェイスごとキーチェーンおよびポリシーが優先して指定の影響を受けるインターフェイス。自動生成されたキーチェーンと関連付けられている MACsec ポリシーでは、最も優先度から提供されます。

APIC MACsec では、2 つのセキュリティ モードをサポートしています。MACsec **セキュリティで保護する必要があります** 中に、リンクの暗号化されたトラフィックのみを許可する **セキュリティで保護する必要があります** により、両方のクリアし、リンク上のトラフィックを暗号化します。MACsec を展開する前に **セキュリティで保護する必要があります** モードでのキーチェーンは影響を受けるリンクで展開する必要がありますまたはリンクがダウンします。たとえば、ポートをオンにできますで MACsec **セキュリティで保護する必要があります** モードがピアがしているリンクでのキーチェーンを受信する前にします。MACsec を導入することが推奨されて、この問題に対処する **セキュリティで保護する必要があります** モードとリンクの 1 回すべてにセキュリティ モードを変更 **セキュリティで保護する必要があります** 。

（注） MACsec インターフェイスの設定変更は、パケットのドロップになります。

MACsec ポリシー定義のキーチェーンの定義に固有の設定と機能の機能に関連する設定で構成されています。キーチェーン定義と機能の機能の定義は、別のポリシーに配置されます。MACsec 1 ポッドあたりまたはインターフェイスごとの有効化には、キーチェーン ポリシーおよび MACsec 機能のポリシーを組み合わせることが含まれます。

（注） 内部を使用して生成キーチェーンは、ユーザのキーチェーンを指定する必要はありません。

APIC アクセス MACsec

MACsec はリーフ スイッチ L3out インターフェイスと外部のデバイス間のリンクを保護するために使用します。APIC GUI および CLI のユーザを許可するで、MACsec キーとファブリック L3Out インターフェイスの設定を MacSec をプログラムを提供する物理/pc/vpc インターフェイスごと。ピアの外部デバイスが正しい MacSec 情報を使用してプログラムすることを確認するには、ユーザの責任です。

スイッチ プロファイルの注意事項および制約事項

MACsec は次のスイッチでサポートされます。

- N9K-C93108TC-FX3P
- N9K-C93108TC-FX
- N9K-C93180YC-FX3
- N9K-C93180YC-FX
- N9K-C93216TC-FX2
- N9K-C93240YC-FX2
- N9K-C9332C
- N9K-C93360YC-FX2
- N9K-C9336C-FX2
- N9K-C9348GC-FXP、10G +のみ
- N9K-C9364C
- N9K-C9332D-GX2B（5.2(3) リリース以降）

MACsec は次のライン カードでサポートされます。

- N9K-X9716D-GX（5.2(2) リリース以降）
- N9K-X9736C-FX

次の注意事項および制約事項に従って、スイッチで MACsec を設定します。

- MACsec は10G QSA モジュールではサポートされていません。
- MACsec は Cisco ACI リーフ スイッチの 1G の速度ではサポートされていません。
- MACsec は、L3Out が有効になっているリーフ スイッチ ポートでのみサポートされます。たとえば、Cisco ACI リーフ スイッチとコンピュータ ホスト間の MACsec はサポートされていません。スイッチ間モードのみがサポートされます。
- 銅線ポートを使用する場合、銅線ケーブルは 10G モードでピア デバイス（スタンドアロン N9k）に直接接続する必要があります。

- ピアの 10G 銅線 SFP モジュールはサポートされません。
- Cisco Application Policy Infrastructure Controller（APIC）リリース 4.0 以降では、MACsec はリモート リーフ スイッチでサポートされています。
- FEX ポートは MACsec ではサポートされません。
- **must-secure** モードは、ポッド レベルではサポートされていません。
- 「default」という名前の MACsec ポリシーはサポートされていません。
- 自動キー生成は、ファブリック ポートのポッド レベルでのみサポートされます。
- そのノードのファブリック ポートが **[必須セキュア]** モードの MACsec で実行されている場合、ノードの再起動をクリアしないでください。
- MACsec を実行しているポッドに新しいノードを追加する、またはポッド内のノードのステートレス リブートを行うには、ノードをポッドに参加させるために、**must-secure** モードを **should-secure** に変更する必要があります。
- ファブリック リンクが **should-secure** モードである場合にのみ、アップグレードまたはダウングレードを開始します。アップグレードまたはダウングレードが完了したら、モードを **must-secure** に変更できます。**must-secure** モードでアップグレードまたはダウングレードすると、ノードがファブリックへの接続を失います。失われた接続を回復するには、**should-secure** モードで、Cisco APIC に表示されるノードのファブリック リンクを設定する必要があります。ファブリックが MACsec をサポートしていないバージョンにダウングレードされた場合、ファブリック外のノードがクリーン リブートされる必要があります。
- PC または vPC インターフェイスの場合、MACsec は PC または vPC インターフェイスごとのポリシー グループを使用して展開できます。ポート セレクタは、特定のポートのセットにポリシーを展開するために使用されます。したがって、L3Out インターフェイスに対応する正しいポート セレクタを作成する必要があります。
- 設定をエクスポートする前に、**should-secure** モードで MACsec ポリシーを設定することを推奨します。
- スパイン スイッチ上のすべてのリンクは、ファブリック リンクと見なされます。ただし、スパイン スイッチ リンクを IPN 接続のために使用している場合、そのリンクはアクセス リンクとして扱われます。これらのリンクで MACsec を展開するには、MACsec アクセス ポリシーを使用する必要があります。
- リモート リーフ ファブリック リンクを IPN 接続に使用する場合、そのリンクはアクセス リンクとして扱われます。これらのリンクで MACsec を展開するには、MACsec アクセス ポリシーを使用する必要があります。
- リモート リーフ スイッチのファブリック リンクに **must-secure** モードを不適切に導入すると、ファブリックへの接続が失われる可能性があります。こうした問題を防ぐため、「must-secure モードの展開 （5 ページ）」で説明している手順に従ってください。
- 新しいキーが空のキーチェーンに追加されるか、アクティブなキーがキーチェーンから削除された場合、MACsec セッションの形成または切断に最大で 1 分かかります。

- スパインスイッチのラインカードまたはファブリックモジュールをリロードする前に、すべての **must-secure** リンクを **should-secure** モードに変更する必要があります。リロードが完了し、セッションが **should-secure** モードになったら、モードを **must-secure** に変更します。
- 暗号スイート AES 128 または Extended Packet Numbering（XPN）のない AES 256 を選択する場合は、Security Association Key（SAK）の有効期限を明示的に指定する必要があります。SAK の有効期限値をデフォルト（「無効」）のままにすると、インターフェイスがランダムにアウトオブサービスになる可能性があります。
- フレームの順序が変更されるプロバイダーネットワーク上で MACsec の使用をサポートするには、リプレイウィンドウが必要です。ウィンドウ内のフレームは順不同で受信できますが、リプレイ保護されません。デフォルトのウィンドウ サイズは 64 です。Cisco APIC GUI または CLI を使用する場合、リプレイ ウィンドウのサイズは、0 ー 2^{32}- 1 の範囲で設定できます。XPN 暗号スイートの場合、最大リプレイ ウィンドウ サイズは 2^{30}-1 です。これより大きなウィンドウ サイズを設定しても、ウィンドウ サイズは 2^{30}-1 に制限されます。暗号スイートを非 XPN 暗号スイートに変更した場合、制限はなく、設定されたウィンドウ サイズが使用されます。
- 5.2(2) リリース以降で Cisco N9K-X9716D-GX ライン カード ファブリック ポートで MACsec を使用していて、それを 5.2(2) より前のリリースにダウングレードした場合、そのような以前のリリースではこのラインカードで MACsec はサポートされません。ただし、MACsec がサポートされていないことによる障害は発生しません。このシナリオでは、ピア リーフ スイッチが MACsec をサポートしている場合、セッションはセキュアな状態で起動します。ただし、スパイン側では、セッションが保留中として表示されます。
- リンク レベル フロー制御（LLFC）およびプライオリティ フロー制御（PFC）は、MACsec ではサポートされません。

must-secure モードの展開

must-secure モードに設定されているポリシーを誤って展開すると、接続が失われる可能性があります。そのような問題を避けるため次の手順に従う必要があります。

- MACsec **must-secure** モードを有効にする前に、各リンク ペアにキーチェーンがあることを確認する必要があります。確実を期すため、ポリシーを **should-secure** モードで展開し、MACsec セッションが想定されるリンクでアクティブになったら、モードを **must-secure** に変更することをお勧めします。
- **[必須セキュア]** に設定されている MACsec ポリシーでキーチェーンの交換を試行すると、リンクがダウンする原因となる可能性があります。この場合は、次の手順に従います。
  1. 新しいキーチェーンを使用している MACsec ポリシーを **[should-secure]** モードに変更します。
  2. 影響を受けるインターフェイスが **[should-secure]** モードを使用しているか確認します。
  3. 新しいキーチェーンを使用するように MACsec ポリシーを更新します。

4. アクティブな MACsec セッションと関連するインターフェイスが新しいキーチェーンを使用していることを確認します。
5. MACsec ポリシーを **[必須セキュア]** モードに変更します。

- **must-secure** モードで展開された MACsec ポリシーを無効化/削除するには、次の手順を実行します。
  1. MACsec ポリシーを **[should-secure]** に変更します。
  2. 影響を受けるインターフェイスが **[should-secure]** モードを使用しているか確認します。
  3. MACsec ポリシーを無効/削除します。

キーチェーンの定義

- 開始時刻が **[現在]** のキーチェーンに 1 個のキーが存在します。**must-secure** を、即座にアクティブになるキーを持たないキーチェーンで展開した場合、キーの時刻が来て MACsec セッションが開始されるまで、トラフィックはリンク上でブロックされます。**should-secure** モードが使用されている場合、キーが現在になり、MACsec セッションが開始されるまでトラフィックが暗号化されます。
- 終了時刻が **infinite** のキーチェーンに 1 個のキーが存在する必要があります。キーチェーンの期限が切れると、**must-secure** モードに設定されている影響を受けるインターフェイスでトラフィックがブロックされます。設定されたインターフェイス **はセキュア** モード暗号化されていないトラフィック送信します。
- 終了時刻のオーバーラップし、キーの間に移行すると、MACsecセッションを順番に使用されるキーの開始時刻が残っています。

GUI を使用したファブリック リンクの MACsec の設定

ステップ 1 メニュー バーで、**Fabric** > **Fabric Policies** > **Policies** > **MACsec** > **Interfaces** をクリックします。**Navigation** ウィンドウで、**Interfaces** を右クリックして **Create MACsec Fabric Interface Policy** を開き、次の手順を実行します:

a) **Name** フィールドに、MACsec ファブリック インターフェイス ポリシーの名前を入力します。
b) **MACsec Parameters** フィールドで、以前に設定した MACsec パラメータ ポリシーを選択するか、新しいものを作成します。
c) **MACsec Keychain Policy** フィールドで、以前に設定した MACsec パラメータ ポリシーを選択するか、新しいものを作成して、**Submit** を作成します。

MACsec Keychain Policy を作成するには、GUI を使用した MACsec キーチェーン ポリシーの設定 （8 ページ）を参照してください。

ステップ 2 **MACsec Fabric Interface Policy** をファブリック リーフまたはスパイン ポート ポリシー グループに適用するには、**Interfaces** > ***Leaf/Spine*** **Interfaces** > **Policy Groups** > ***Spine/Leaf*** **Port Policy Group_*name*** をクリックします。**Work** ウィンドウで、今作成した **MACsec Fabric Interface Policy** を選択します。

ステップ 3 **MACsec Fabric Interface Policy** をポッド ポリシー グループに適用するには、ナビゲーション ウィンドウで **Pods** > **Policy Groups** > **Pod Policy Group_*name*** をクリックします。**Work** ウィンドウで、今作成した **MACsec Fabric Interface Policy** を選択します。

GUI を使用したアクセス リンクの MACsec の設定

ステップ 1 メニューバーで、**[ファブリック]**>**[外部アクセス ポリシー]** をクリックします。**Navigation** ウィンドウで、**Policies** > **Interface** > **MACsec** > **Interfaces** をクリックし、**Interfaces** を右クリックして **Create MACsec Fabric Interface Policy** を開き、次の手順を実行します:

a) **Name** フィールドに、MACsec アクセス インターフェイス ポリシーの名前を入力します。

b) **MACsec Parameters** フィールドで、以前に設定した MACsec パラメータ ポリシーを選択するか、新しいものを作成します。

c) **MACsec Keychain Policy** フィールドで、以前に設定した MACsec パラメータ ポリシーを選択するか、新しいものを作成して、**Submit** を作成します。

MACsec Keychain Policy を作成するには、GUI を使用した MACsec キーチェーン ポリシーの設定 （8 ページ）を参照してください。

ステップ 2 **MACsec Access Interface Policy** をファブリック リーフまたはスパイン ポート ポリシー グループに適用するには、**Interfaces** > ***Leaf/Spine*** **Interfaces** > **Policy Groups** > ***Spine/Leaf*** **Policy Group_*name*** をクリックします。**Work** ウィンドウで、今作成した **MACsec Fabric Interface Policy** を選択します。

APIC GUI を使用した MACsec パラメータの設定

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順にクリックします。**ナビゲーション**] ペインで、[をクリックする **インターフェイス ポリシー** > **ポリシー**] を右クリックし、 **MACsec ポリシー** を開く **MACsec アクセス パラメータ ポリシーの作成** し、次のアクションを実行します。

a) **Name** フィールドに、MACsec アクセス パラメータ ポリシーの名前を入力します。

b) **セキュリティ ポリシー** フィールドで、暗号化されたトラフィックのモードを選択し、をクリックして **Submit** 。

（注） MACsec を展開する前に **セキュア モードをする必要があります** キーチェーンは、影響を受けるインターフェイスに導入する必要があります、またはインターフェイスがダウンします。

ステップ 2 適用する、 **MACsec アクセス パラメータ ポリシー** リーフまたはナビゲーション ペインで、スパイン ポートのポリシー グループをクリックして **インターフェイス ポリシー** > **ポリシー グループ** > **スパイン リーフ/ポリシー Group_ 名** 。**作業**] ペインで、[、 **MACsec アクセス インターフェイス ポリシー** だけを作成します。

GUI を使用した MACsec キーチェーン ポリシーの設定

ステップ 1 メニュー バーで **Fabric** > **Fabric Policies** > **Policies** > **MACsec** > **KeyChains** をクリックします。**Navigation** ウィンドウで、**KeyChains** を右クリックして **Create MACsec Keychain Policy** を開き、次の手順を実行します:

a) **Name** フィールドに、MACsec ファブリック インターフェイス ポリシーの名前を入力します。
b) **MACsec キー ポリシー** テーブルを展開して、キー ポリシーを作成します。

ステップ 2 **MACsec Policy** ダイアログボックスで次の操作を実行します。

a) **Name** フィールドに、MACsec キー ポリシーの名前を入力します。
b) **Key Name** フィールドにキーの名前を入力します (64 文字までの 16 進数)。

（注） キーチェーンあたり最大 64 のキーがサポートされています。

c) **Pre-shared Key** フィールドに、事前共有キーの情報を入力します。

（注）
- 128 ビットの暗号スイートでは、32 文字の PSK だけが許可されます。
- 256 ビットの暗号スイートでは、64 文字の PSK だけが許可されます。

d) **Start Time** フィールドで、キーが有効になる日付を選択します。
e) **End Time** フィールドで、キーの有効期限が切れる日付を選択します。**Ok** と **Submit** をクリックします。

（注） キーチェーンで複数のキーを定義する場合には、古いキーから新しいキーへのスムーズな移行を確実にするために、キーの有効期間をオーバーラップさせて定義する必要があります。古いキーの endTime と新しいキーの startTime をオーバー ラップさせてください。

アクセス ポリシーでキーチェーン ポリシーを設定するには、メニュー バーで **Fabric** > **External Access Policies** をクリックします。**Navigation** ウィンドウで **Policies** > **Interface** > **MACsec** > **MACsec KeyChain Policies** をクリックし、**Create MACsec Keychain Policy** を右クリックして開き、上記の手順を実行します。

NX-OS スタイルの CLI を使用したMACsecの設定

ステップ 1 アクセス インターフェイスの MACsec セキュリティ ポリシーの設定

例：

```
apic1# configure
apic1(config)#   template macsec access security-policy accmacsecpol1
apic1(config-macsec-param)#     cipher-suite gcm-aes-128
apic1(config-macsec-param)#     conf-offset offset-30
apic1(config-macsec-param)#     description 'description for mac sec parameters'
apic1(config-macsec-param)#     key-server-priority 1
apic1(config-macsec-param)#     sak-expiry-time 110
apic1(config-macsec-param)#     security-mode must-secure
aapic1(config-macsec-param)#     window-size 1
apic1(config-macsec-param)#     exit
apic1(config)#
```

ステップ 2 アクセス インターフェイスの MACsec キー チェーンを設定します。

PSK は、2 通りの方法で設定できます:

（注）
- 下のキー 12ab に示すように、**psk-string** コマンドを使用してインラインで設定します。PSK は、ログに記録され、公開されるため、安全ではありません。
- キー ab12 で示すように、新しいコマンド **Enter PSK string** を **psk-string** コマンドの後で使用し、個別に入力して設定します。ローカルにエコーされるだけで、ログには記録されないため、PSK は安全です。

例：

```
apic1# configure
apic1(config)#   template macsec access keychain acckeychainpol1
apic1(config-macsec-keychain)#     description 'macsec key chain kc1'
apic1(config-macsec-keychain)#     key 12ab
apic1(config-macsec-keychain-key)#      life-time start 2017-09-19T12:03:15 end 2017-12-19T12:03:15
apic1(config-macsec-keychain-key)#       psk-string 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)#       exit
apic1(config-macsec-keychain)#     key ab12
apic1(config-macsec-keychain-key)#       life-time start now end infinite
apic1(config-macsec-keychain-key)#       life-time start now end infinite
apic1(config-macsec-keychain-key)# psk-string
Enter PSK string: 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)# exit
apic1(config-macsec-keychain)# exit
apic1(config)#
```

ステップ 3 アクセス インターフェイスの MACsec インターフェイス ポリシーを設定します:

例：

```
apic1# configure
apic1(config)#   template macsec access interface-policy accmacsecifpol1
apic1(config-macsec-if-policy)#     inherit macsec security-policy accmacsecpol1 keychain
acckeychainpol1
apic1(config-macsec-if-policy)#     exit
apic1(config)#
```

ステップ 4 MACsec インターフェイス ポリシーをリーフ (またはスパイン) 上のアクセス ンターフェイスに関連付けます:

例：

```
apic1# configure
apic1(config)#   template macsec access interface-policy accmacsecifpol1
apic1(config-macsec-if-policy)#     inherit macsec security-policy accmacsecpol1 keychain
acckeychainpol1
apic1(config-macsec-if-policy)#     exit
apic1(config)
```

ステップ 5 ファブリック インターフェイス用に MACsec セキュリティ ポリシーを設定します:

例：

```
apic1# configure
apic1(config)#   template macsec fabric security-policy fabmacsecpol1
apic1(config-macsec-param)#     cipher-suite gcm-aes-xpn-128
apic1(config-macsec-param)#     description 'description for mac sec parameters'
apic1(config-macsec-param)#     window-size 1
apic1(config-macsec-param)#     sak-expiry-time 100
apic1(config-macsec-param)#     security-mode must-secure
apic1(config-macsec-param)#     exit
apic1(config)#
```

ステップ 6 ファブリック インターフェイス用に MACsec キー チェーンを設定します:

PSK は、2 通りの方法で設定できます:

（注）
- 下のキー 12ab に示すように、**psk-string** コマンドを使用してインラインで設定します。PSK は、ログに記録され、公開されるため、安全ではありません。
- キー ab12 で示すように、新しいコマンド **Enter PSK string** を **psk-string** コマンドの後で使用し、個別に入力して設定します。ローカルにエコーされるだけで、ログには記録されないため、PSK は安全です。

例：

```
apic1# configure
apic1(config)#   template macsec fabric security-policy fabmacsecpol1
apic1(config-macsec-param)#     cipher-suite gcm-aes-xpn-128
apic1(config-macsec-param)#     description 'description for mac sec parameters'
apic1(config-macsec-param)#     window-size 1
apic1(config-macsec-param)#     sak-expiry-time 100
apic1(config-macsec-param)#     security-mode must-secure
apic1(config-macsec-param)#     exit
apic1(config)#   template macsec fabric keychain fabkeychainpol1
apic1(config-macsec-keychain)#     description 'macsec key chain kc1'
apic1(config-macsec-keychain)#     key 12ab
apic1(config-macsec-keychain-key)#       psk-string 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)#      life-time start 2016-09-19T12:03:15 end 2017-09-19T12:03:15
apic1(config-macsec-keychain-key)#       exit
apic1(config-macsec-keychain)#     key cd78
apic1(config-macsec-keychain-key)# psk-string
Enter PSK string: 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)# life-time start now end infinite
apic1(config-macsec-keychain-key)# exit
apic1(config-macsec-keychain)# exit
apic1(config)#
```

ステップ 7 MACsec インターフェイス ポリシーをリーフ (またはスパイン) 上のファブリック インターフェイスに関連付けます:

例：

```
apic1# configure
apic1(config)#   leaf 101
apic1(config-leaf)#     fabric-interface ethernet 1/52-53
apic1(config-leaf-if)#       inherit macsec interface-policy fabmacsecifpol2
apic1(config-leaf-if)#       exit
apic1(config-leaf)#
```

REST API を使用した MACsec の設定

MACsec ファブリック ポリシーをファブリックのすべてのポッドに適用します。

例：

```
<fabricInst>
 <macsecFabPolCont>
        <macsecFabParamPol name="fabricParam1"  secPolicy="should-secure"
replayWindow="120" >
        </macsecFabParamPol>
        <macsecKeyChainPol name="fabricKC1">
            <macsecKeyPol name="Key1"
preSharedKey="0102030405060708090A0B0C0D0E0F10010203040506070809 0A0B0C0D0E0F10"
keyName="A1A2A3A0" startTime="now" endTime="infinite"/>
        </macsecKeyChainPol>
    </macsecFabPolCont>

    <macsecFabIfPol name="fabricPodPol1" useAutoKeys="0">
        <macsecRsToParamPol tDn="uni/fabric/macsecpcontfab/fabparamp-fabricParam1"/>
        <macsecRsToKeyChainPol tDn="uni/fabric/macsecpcontfab/keychainp-fabricKC1"/>
    </macsecFabIfPol>

    <fabricFuncP>
  <fabricPodPGrp name = "PodPG1">
   <fabricRsMacsecPol tnMacsecFabIfPolName="fabricPodPol1"/>
     </fabricPodPGrp>
 </fabricFuncP>

    <fabricPodP name="PodP1">
  <fabricPodS name="pod1" type="ALL">
   <fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-PodPG1"/>
     </fabricPodS>
 </fabricPodP>

</fabricInst>
```

リーフ 101 の eth1/4 上で MACsec アクセス ポリシーを適用します。

例：

```
<infraInfra>
 <macsecPolCont>
       <macsecParamPol name="accessParam1"  secPolicy="should-secure" replayWindow="120"
 >
        </macsecParamPol>
        <macsecKeyChainPol name="accessKC1">
```

```
            <macsecKeyPol name="Key1"
preSharedKey="0102030405060708090A0B0C0D0E0F10010203040506070809 0A0B0C0D0E0F10"
keyName="A1A2A3A0" startTime="now" endTime="infinite"/>
        </macsecKeyChainPol>
    </macsecPolCont>

    <macsecIfPol name="accessPol1">
        <macsecRsToParamPol tDn="uni/infra/macsecpcont/paramp-accessParam1"/>
        <macsecRsToKeyChainPol tDn="uni/infra/macsecpcont/keychainp-accessKC1"/>
    </macsecIfPol>

    <infraFuncP>
  <infraAccPortGrp name = "LeTestPGrp">
   <infraRsMacsecIfPol tnMacsecIfPolName="accessPol1"/>
     </infraAccPortGrp>
 </infraFuncP>

 <infraHPathS name="leaf">
  <infraRsHPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/4]" />
  <infraRsPathToAccBaseGrp tDn="uni/infra/funcprof/accportgrp-LeTestPGrp" />
 </infraHPathS>

</infraInfra>
```

リーフ 101 の Eth1/49 およびスパイン 102 の eth 5/1 上で MACsec ファブリック ポリシーを適用します。

```
<fabricInst>
 <macsecFabPolCont>
        <macsecFabParamPol name="fabricParam1"  secPolicy="should-secure"
replayWindow="120" >
        </macsecFabParamPol>
        <macsecKeyChainPol name="fabricKC1">
            <macsecKeyPol name="Key1"
preSharedKey="0102030405060708090A0B0C0D0E0F10010203040506070809 0A0B0C0D0E0F10"
keyName="A1A2A3A0" startTime="now" endTime="infinite"/>
        </macsecKeyChainPol>
    </macsecFabPolCont>

    <macsecFabIfPol name="fabricPol1" useAutoKeys="0">
        <macsecRsToParamPol tDn="uni/fabric/macsecpcontfab/fabparamp-fabricParam1"/>
        <macsecRsToKeyChainPol tDn="uni/fabric/macsecpcontfab/keychainp-fabricKC1"/>
    </macsecFabIfPol>

    <fabricFuncP>
  <fabricLePortPGrp name = "LeTestPGrp">
   <fabricRsMacsecFabIfPol tnMacsecFabIfPolName="fabricPol1"/>
     </fabricLePortPGrp>

  <fabricSpPortPGrp name = "SpTestPGrp">
   <fabricRsMacsecFabIfPol tnMacsecFabIfPolName="fabricPol1"/>
     </fabricSpPortPGrp>
 </fabricFuncP>

 <fabricLFPathS name="leaf">
  <fabricRsLFPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/49]" />
  <fabricRsPathToLePortPGrp tDn="uni/fabric/funcprof/leportgrp-LeTestPGrp" />
 </fabricLFPathS>

 <fabricSpPortP name="spine_profile">
  <fabricSFPortS name="spineIf" type="range">
   <fabricPortBlk name="spBlk" fromCard="5" fromPort="1" toCard="5" toPort="1" />
   <fabricRsSpPortPGrp tDn="uni/fabric/funcprof/spportgrp-SpTestPGrp" />
  </fabricSFPortS>
```

```
 </fabricSpPortP>

 <fabricSpineP name="SpNode" >
  <fabricRsSpPortP tDn="uni/fabric/spportp-spine_profile" />
  <fabricSpineS name="spsw" type="range">
   <fabricNodeBlk name="node102" to_="102" from_="102" />
  </fabricSpineS>
 </fabricSpineP>
</fabricInst>
```

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。