改訂：2026 年 8 月 12 日

Azure 上の Cisco ISE の使用に関する既知の制限事項

Microsoft Azure Cloud Services における Cisco ISE の既知の制限事項

Microsoft Azure Cloud Services で Cisco ISE を使用する場合の既知の制限事項は次のとおりです。

- Azure 仮想マシンを使用して Cisco ISE を作成すると、Microsoft Azure はデフォルトで DHCP サーバーを介して VM にプライベート IP アドレスを割り当てます。Microsoft Azure で Cisco ISE 展開を作成する前に、Microsoft Azure によって割り当てられた IP アドレスを使用して、フォワードおよびリバース DNS エントリを更新します。

  Cisco ISE をインストールした後、Microsoft Azure でネットワーク インターフェイス オブジェクトを更新して、VM に静的 IP アドレスを割り当てることができます。手順は次のとおりです。

  1. VM を停止します。
  2. [プライベートIPアドレス設定（Private IP address settings）] > [割り当て（Assignment）] > [静的（Static）] の順に選択します。
  3. VM を再起動します。
  4. Cisco ISE シリアルコンソールで、Gi0 インターフェイスに IP アドレスを割り当てます。
  5. Cisco ISE アプリケーションサーバーを再起動します。

- デュアル NIC は、2 つの NIC（ギガビットイーサネット 0 とギガビットイーサネット 1）のみをサポートします。セカンダリ NIC を設定するには、まず Azure でネットワーク インターフェイス オブジェクトを作成し、Cisco ISE インスタンスの電源をオフにしてから、このオブジェクトを Cisco ISE にアタッチします。

  Azure に Cisco ISE をインストールして起動したら、Cisco ISE CLI を使用して、ネットワーク インターフェイス オブジェクトの IP アドレスをセカンダリ NIC として手動で設定します。

- Microsoft Azure 環境では Cisco ISE をアップグレードできません。新規インストールのみ実行できます。ただし、設定データのバックアップと復元は実行できます。ハイブリッド Cisco ISE 展開のアップグレードについては、ハイブリッド展開のアップグレードのガイドラインを参照してください。

- パブリッククラウドはレイヤ 3 機能のみをサポートします。Microsoft Azure の Cisco ISE ノードは、レイヤ 2 機能をサポートしていません。たとえば、Cisco ISE CLI を介してアクセスされる DHCP SPAN プロファイラプローブおよび CDP プロトコル機能はサポートされていません。

- 設定データを復元してバックアップするには、まずバックアップ操作を完了します。次に、CLI を使用して Cisco ISE を再起動し、Cisco ISE GUI から復元操作を開始します。詳細については、ご使用のリリースの『*Cisco ISE Administrator Guide*』にある「Maintain and Monitor」の章を参照してください。

- パスワードベースの認証を使用した Cisco ISE CLI への SSH アクセスは、Azure ではサポートされていません。Cisco ISE CLI には、キーペアを介してのみアクセスでき、このキーペアは安全に保存する必要があります。

  秘密キー（または PEM）ファイルを使用していてそのファイルを失った場合、Cisco ISE CLI にアクセスできません。

  パスワードベースの認証を使用して Cisco ISE CLI にアクセスする統合はサポートされていません。

- Azure Cloud での Cisco ISE 展開では、Accelerated Networking はサポートされていません。この機能を有効にすると、ノードの登録や登録解除などの操作が失敗する可能性があります。

Azure 上の Cisco ISE 展開における順序が不正なフラグメンテーションの制限事項

Microsoft Azure のデフォルトの仮想ネットワークスタックは、セキュリティ上の理由（特に FragmentSmack 脆弱性に対処するため）で順序が不正な IP フラグメントをドロップし、これらのフラグメントが接続先の仮想マシンに到達できなくなります。この動作は、Cisco ISE 展開に影響を与える可能性があります。その結果、Cisco ISE およびネットワークデバイスは完全な RADIUS パケットを受信しない可能性があり、認証、承認、およびダイナミック アクセス コントロール リスト（DACL）プッシュが失敗します。

この問題は、Azure のデフォルト VPN ゲートウェイ、Azure ExpressRoute、または Azure Virtual WAN を使用する場合に、すべての Cisco ISE バージョンで発生する可能性があります。この問題は、大きな証明書、DACL プッシュ、または複数の属性を持つ RADIUS 認証およびアカウンティング要求を含む EAP-TLS パケットなど、大きな RADIUS パケットでよく見られます。

この問題を軽減するには、サードパーティの VPN ゲートウェイ（Cisco Catalyst 8000V や Cisco ASAv など）を Azure 仮想マシンとして展開します。このゲートウェイはオンプレミス環境からの VPN トンネルを終了し、フラグメンテーション再構成をサポートします。Azure のデフォルト VPN ゲートウェイは、フラグメンテーション再構成をサポートしていません。

Azure にサードパーティの VPN ゲートウェイを展開してオンプレミスとのサイト間 VPN 接続を確立した後、次の手順を実行して、大きな RADIUS パケットを確実に処理し、Azure 環境でのフラグメンテーションの問題による認証エラーを軽減します。

1. サードパーティの VPN ゲートウェイで、ip virtual-reassembly を有効にすると、フラグメント化されたパケットが不正な順序で受信された場合でも、正しくリアセンブルされます。

   Catalyst 8000V の場合は、次のコマンドを使用します。

   ```
   ip virtual-reassembly-out
   ```

   Cisco ASAv の場合は、次のコマンドを使用します。

   ```
   fragment reassembly full outside
   ```

2. サイト間 VPN の NAT トラバーサルでは、UDP 4500 に変換された大きな IPsec パケットがフラグメント化される可能性があるため、サードパーティ VPN ゲートウェイで暗号化される前にフラグメンテーションを有効にします。

   Cisco ASAv の場合は、次のコマンドを使用します。

   ```
   crypto ipsec fragmentation before-encryption
   ```

3. Azure ポータルで、VPN ゲートウェイ VM の内部インターフェイスと外部インターフェイスの両方で IP 転送を有効にします。

4. Azure ルーティングテーブルを更新して、サードパーティ VPN ゲートウェイを介した仮想ネットワーク接続を許可します。これにより、オンプレミスのリソースにアクセスできます。

これらの設定を行った後も認証エラーが断続的に発生する場合は、Microsoft サポートチケットを開いて、サブスクリプション内の Azure VPN ネットワークコンポーネントに対して [順序が不正なフラグメントを許可する（allow out-of-order fragments）] オプションを有効にします。

（注）

ネットワークデバイス（WLC やスイッチなど）と Cisco ISE 出力の両方でパケットのフラグメンテーションを減らすには、ネットワークデバイスの RADIUS 送信元インターフェイスと Cisco ISE の RADIUS インターフェイスで MTU を小さくすることを検討してください。ほとんどの環境では一般的な MTU 値（1,400 バイト）が有効ですが、パス MTU 検出（PMTUD）ツールを使用してサブネット間の最適な MTU を決定することで、最適なパフォーマンスを得ることができます。

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。