



## FlexVPN の概要

RFC 4306 に基づく次世代のキー管理プロトコルであるインターネット キー エクスチェンジバージョン 2 (IKEv2) は、IKE プロトコルの機能拡張です。IKEv2 は、相互認証を実行して SA を確立および管理するために使用します。

FlexVPN は、シスコによる IKEv2 標準の実装であり、サイト間アクセス、リモートアクセス、ハブ アンド スポーク トポロジ、および部分メッシュ (スポーク間ダイレクト) を組み合わせたユニファイドパラダイムと CLI を備えています。FlexVPN は、トンネルインターフェイスパラダイムを広範に使用し、かつ暗号マップを使用してレガシー VPN 実装との互換性を維持するシンプルなモジュラ フレームワークを提供します。

本書の構成は、次のとおりです。

- [インターネット キー エクスチェンジバージョン 2 \(IKEv2\) および FlexVPN リモートアクセスの設定 \(1 ページ\)](#)
- [FlexVPN サーバーの設定 \(2 ページ\)](#)
- [FlexVPN クライアントの設定 \(2 ページ\)](#)
- [IKEv2 ロード バランサの設定 \(2 ページ\)](#)
- [IKEv2 フラグメンテーションの設定 \(2 ページ\)](#)
- [IKEv2 再接続の設定 \(2 ページ\)](#)
- [IKEv2 パケット オブ ディスコネクトの設定 \(2 ページ\)](#)
- [IKEv2 認可変更のサポートの設定 \(3 ページ\)](#)
- [集約認証の設定 \(3 ページ\)](#)
- [付録 : FlexVPN の RADIUS 属性 \(3 ページ\)](#)
- [付録 : IKEv2 およびレガシー VPN \(3 ページ\)](#)

# インターネット キー エクスチェンジバージョン 2 (IKEv2) および FlexVPN リモート アクセスの設定

このモジュールでは IKEv2 CLI について説明します。このモジュールは、基本セクションと高度なセクションに分かれています。

基本セクションでは、基本の IKEv2 コマンドを紹介し、IKEv2 スマートデフォルトと FlexVPN リモートアクセスに必要な必須の IKEv2 コマンドについて説明します。このモジュールは、後続の章を理解するための前提条件です。

高度なセクションでは、グローバル IKEv2 コマンドについて説明します。また、デフォルト IKEv2 コマンドをオーバーライドする方法についても説明します。

## FlexVPN サーバーの設定

このモジュールでは、FlexVPN サーバーの機能、FlexVPN サーバーの設定に必要な IKEv2 コマンド、リモートアクセスクライアント、およびサポートされる RADIUS 属性について説明します。

## FlexVPN クライアントの設定

このモジュールでは、FlexVPN クライアント機能と FlexVPN クライアントに必要な IKEv2 コマンドについて説明します。

## IKEv2 ロード バランサの設定

このモジュールでは、IKEv2 ロード バランサ サポート機能と、IKEv2 ロード バランサの設定に必要な IKEv2 コマンドについて説明します。

## IKEv2 フラグメンテーションの設定

RFC 機能に準拠した IKE フラグメンテーションでは、IETF の **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントの提案に従って、インターネット キー エクスチェンジ バージョン 2 (IKEv2) パケットのフラグメンテーションを実装しました。

## IKEv2 再接続の設定

AnyConnect 機能の AutoReconnect 機能の IOS IKEv2 サポートは、Cisco AnyConnect でユーザーが操作しない、IKEv2 ネゴシエーションの再確立に役立ちます。

## IKEv2 パケット オブ ディスコネクトの設定

IKEv2 リモートアクセス認可変更 (CoA) のパケット オブ ディスコネクト機能は、シスコがサポートするデバイスのアクティブな暗号 IKEv2 セッションを停止します。

## IKEv2 認可変更のサポートの設定

FlexVPN - QoS および ACL 用 IKEv2 CoA 機能は、アクティブな IKEv2 暗号セッションでの RADIUS 認可変更 (CoA) をサポートしています。

## 集約認証の設定

FlexVPN RA - Cisco AnyConnect クライアントのサポートを拡張することで、AnyConnect 機能の集約認証サポートは、集約認証方式を実装します。このクライアントでは、独自の AnyConnect EAP 認証方式を使用し、Cisco AnyConnect クライアントと FlexVPN サーバー間にインターネットを介したセキュア トンネルを確立します。

## 付録：FlexVPN の RADIUS 属性

このモジュールでは、FlexVPN サーバーでサポートされる RADIUS 属性について説明します。

## 付録：IKEv2 およびレガシー VPN

このモジュールには、暗号化マップやインターネット キー エクスチェンジバージョン 2 (IKEv2) による DMVPN などのレガシー VPN の設定例が含まれています。



## 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。