「Call Admission Control for IKE」

IKE 用コール アドミッション制御機能は、Cisco IOS ソフトウェアでのインターネット キー エクスチェンジ（IKE）プロトコルに対し、コールアドミッション制御（CAC）を適用したものです。CAC は、IKE と IPsec セキュリティ アソシエーション（SA）（つまり CAC へのコール）をルータが同時に確立できる数を制限します。

IKE 用コール アドミッション制御に関する前提条件

- このデバイスで IKE を設定します。

IKE 用コール アドミッション制御に関する情報

IKE セッション

デバイスが別のデバイスとの間で確立できるインターネット キー エクスチェンジ（IKE）セキュリティ アソシエーション（SA）の数を制限する方法には、次の 2 つがあります。

- **crypto call admission limit** コマンドを入力して、IKE SA の絶対制限値を設定します。設定された制限値に達すると、デバイスは新しい IKE SA 要求をドロップします。
- **call admission limit** コマンドを入力して、システムリソース制限値を設定します。チャージ単位で設定されたレベルのシステム リソースが使用されている場合、デバイスは新しい IKE SA 要求をドロップします。

コール アドミッション制御（CAC）は新しい SA のみ（つまり、ピア間に SA がまだ存在しないとき）に適用されます。既存の SA を保存するためにあらゆる処置が行われます。新しい SA 要求が拒否されるのは、システム リソースが不足しているか、あるいは設定された IKE SA 制限値に達したことが原因です。

セキュリティ アソシエーション制限

SA（セキュリティ アソシエーション）は、2 つ以上のエンティティがセキュリティ サービスを使用して特定のデータ フローのために安全に通信する方法を記述したものです。IKE は接続のパラメータを識別するために、必ず SA を使用します。IKE では、独自に SA をネゴシエーションして確立できます。IKE SA は、IKE だけで使用され、双方向です。IKE SA は、IPsec を制限できません。

IKE は、ユーザが設定した SA 制限値に基づいて SA 要求をドロップします。IKE SA 制限値を設定するには、**crypto call admission limit** コマンドを入力します。ピア ルータから新しい SA 要求があると、IKE はアクティブな IKE SA の数とネゴシエーション中の SA の数が、設定された SA 制限値を満たしているか、超えているかを判別します。この数が制限値より大きい、または等しい場合、新しい SA 要求は拒否され、syslog が生成されます。このログには、SA 要求の送信元および宛先 IP アドレスが含まれます。

crypto call admission limit コマンドの **ipsec sa** *number* および **ike sa** *number* キーワードと引数のペアには、確立された IPsec SA と IKE SA の数の制限値を設定します。

ネゴシエーション時の IKE 接続数の制限

Cisco リリースに基づいて、デバイスで設定できる内部 IKE ネゴシエーション接続の数を制限できます。このタイプの IKE 接続は、認証および実際の確立前のアグレッシブ モード IKE SA またはメイン モード IKE SA を表します。IKEv2 の最大内部ネゴシエーション CAC のデフォルト値は 40 です。

crypto call admission limit ike in-negotiation-sa *number* コマンドを使用すると、IKE が新しい SA 要求の拒否を開始する前にデバイスが確立できるインターネット キー エクスチェンジ（IKE）と IPsec セキュリティ アソシエーション（SA）の最大数を指定できます。

crypto call admission limit コマンドの **all in-negotiation-sa** *number* と **ike in-negotiation-sa** *number* のキーワードと引数のペアは、ネゴシエーション時のすべての SA とネゴシエーション時の IKE SA を制限します。

システム リソースの使用状況

ルータの CPU サイクルまたはメモリ バッファが不足した場合に、IKE がそのことを認識できるように、CAC はグローバル情報リソース モニタをポーリングします。システム リソースの使用量レベルを表す制限値を 1 ～ 100000 までの範囲で設定できます。設定レベルのリソースが使用されると、IKE は SA 要求を廃棄します（新たに受け入れません）。システムリソース使用量の制限を設定するには、**call admission limit** コマンドを入力します。

新しい着信 SA 要求ごとに、ルータにかかる現在の負荷が数値に変換され、システムリソースの使用量レベルが表示されます。また、この数値と、**call admission limit** コマンドによって設定されたリソース制限値が比較されます。現在の負荷が、設定されたリソース制限値を超えると、IKE は新しい SA 要求を廃棄します。ルータの負荷には、アクティブな SA、CPU の使用量、および考慮される SA 要求が含まれます。

call admission load コマンドを実行すると、現在のシステムリソース使用量の倍率を表す 0 ～ 1000 の乗数値と 1 ～ 32 秒の負荷メトリックのポーリングレートが設定されます。システム リソースの使用量レベルの数値は、（倍率 * 現在のシステム リソースの使用量）/ 100 という式で計算されます。Cisco Technical Assistance Center（TAC）技術者からの指示がないかぎり、**call admission load** コマンドを使用することは推奨しません。

IKE 用コール アドミッション制御の設定方法

IKE セキュリティ アソシエーション制限の設定

IKE SA の絶対制限値を設定するには、次の作業を実行します。制限値に達すると、ルータは新しい IKE SA 要求を廃棄します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto call admission limit** {**all in-negotiation-sa** *number* | **ipsec sa** *number* | **ike** {**in-negotiation-sa** *number* | **sa** *number*}}
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto call admission limit** {**all in-negotiation-sa** *number*	**ipsec sa** *number*	**ike** {**in-negotiation-sa** *number*	**sa** *number*}} 例：	ネゴシエーション時の IKE SA の最大数、合計 SA 数、または IKE が新しい SA 要求を拒否し始める前に確立できる IKE SA またはIPsec SA の最大数を指定します。IKEv1 の推奨 CAC 値は 40 です。

	コマンドまたはアクション	目的
	`Router(config)# crypto call admission limit ike sa 25`	
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 セキュリティ アソシエーション制限の設定

IKEv2 SA の絶対制限値を設定するには、次の作業を実行します。制限値に達すると、ルータは新しい IKE SA 要求を廃棄します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 limit** {**max-in-negotiation-sa limit** *number* | **max-sa limit** *number*}
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 limit** {**max-in-negotiation-sa limit** *number*	**max-sa limit** *number*} 例： `Router(config)# crypto ikev2 limit max-in-negotation-sa 5000`	コールアドミッション制御を次のようにイネーブルにします。 • max-in-negotation-sa limit：ノード上での IKEv2 SA のネゴシエーションの受け入れの合計数を制限します。 • max-sa limit：ノード上での IKEv2 SA の合計数を制限します。
ステップ 4	**exit** 例：	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Router(config)# exit`	

システム リソース制限の設定

システム リソースの制限値を設定するには、次の作業を実行します。負荷単位で設定されたレベルのシステム リソースが使用されている場合、ルータは新しい IKE SA 要求を廃棄します。

手順の概要

1. **enable**
2. **configure terminal**
3. **call admission limit** *charge*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**call admission limit** *charge* 例： `Router(config)# call admission limit 1000`	システム リソースを使用する場合、システム リソースのレベルを設定して、IKE による新しい SA 要求の受け入れを停止します。 • *charge*：有効な値は 1 ～ 100000 です。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKE の CAC の設定確認

IKE 設定の CAC を確認するには、次の手順を実行します。

手順の概要

1. **show call admission statistics**
2. **show crypto call admission statistics**

手順の詳細

ステップ 1 **show call admission statistics**

このコマンドを使用して、グローバル CAC コンフィギュレーション パラメータおよび CAC の動作をモニタします。

例：

```
Router# show call admission statistics
Total Call admission charges: 82, limit 1000
Total calls rejected 1430, accepted 0
Load metric: charge 82, unscaled 82%
```

ステップ 2 **show crypto call admission statistics**

このコマンドを使用して、暗号 CAC 統計情報をモニタします。

例：

```
Router# show crypto call admission statistics
----------------------------------------------------------------------
               Crypto Call Admission Control Statistics
----------------------------------------------------------------------
System Resource Limit:      111 Max IKE SAs:     0 Max in nego:  1000
Total IKE SA Count:           0 active:          0 negotiating:     0
Incoming IKE Requests:        0 accepted:        0 rejected:        0
Outgoing IKE Requests:        0 accepted:        0 rejected:        0
Rejected IKE Requests:        0 rsrc low:        0 Active SA limit: 0
                                                   In-neg SA limit: 0
IKE packets dropped at dispatch:        0
Max IPSEC SAs:   111
Total IPSEC SA Count:           0 active:          0 negotiating:     0
Incoming IPSEC Requests:        0 accepted:        0 rejected:        0
Outgoing IPSEC Requests:        0 accepted:        0 rejected:        0
Phase1.5 SAs under negotiation:         0
```

IKE 用コール アドミッション制御の設定例

IKE セキュリティ アソシエーション制限値の設定例

次の例では、IKE が新しい SA 要求を拒否し始めるまでの SA の最大値を 25 に指定する方法を示します。

```
Router(config)# crypto call admission limit ike sa 25
```

システム リソース制限値の設定例

次の例では、負荷単位で設定されたシステム リソースのレベルが 9000 に達したときに、IKE が SA 要求を廃棄するように指定する方法を示します。

```
Router(config)# call admission limit 9000
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IKE の設定	「Configuring Internet Key Exchange for IPsec VPNs」
IKE コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2409	『*The Internet Key Exchange*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IKE 用コール アドミッション制御の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : IKE* 用コール アドミッション制御の機能情報

機能名	リリース	機能情報
「Call Admission Control for IKE」	12.3(8)T 12.2(18)SXD1 12.4(6)T 12.2(33)SRA 12.2(33)SXH	IKE 用コール アドミッション制御機能は、Cisco IOS ソフトウェアでのインターネット キー エクスチェンジ（IKE）プロトコルに対し、コール アドミッション制御（CAC）を適用したものです。 この機能は、Cisco IOS Release 12.3(8)T で導入されました。 この機能は Cisco IOS Release 12.2(18)SXD1 に統合され、Cisco 6500 および Cisco 7600 ルータに実装されました。 Cisco IOS Release 12.4(6)T では、ネゴシエーション時の IKE 接続数の制限を設定する機能が追加されました。 この機能に関する詳細については、次の各項を参照してください。 次のコマンドが導入または変更されました。**call admission limit**、 **clear crypto call admission statistics**、 **crypto call admission limit**、 **show call admission statistics**、 **show crypto call admission statistics**。

機能名	リリース	機能情報
IKEv1 の強化	15.1(3)T	IKEv1 の強化機能とは、IKE 機能のコール アドミッション制御（CAC）に対して行われた拡張機能を表します。 この機能は、Cisco IOS Release 15.1(3)T で導入されました。 この機能に関する詳細については、次の各項を参照してください。 次のコマンドが導入または変更されました。**crypto call admission limit**、 **show crypto call admission statistics**。

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。