IKE 用コール アドミッション制御

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 Internet Key Exchange（IKE; インターネット キー エクスチェンジ）プロトコルに対する Call Admission Control（CAC; コール アドミッション制御）のアプリケーションを表します。CAC は、ルータが同時に確立できる IKE および IPsec Security Association（SA; セキュリティ アソシエーション）（つまり、CAC へのコール）の数を制限します。

機能情報の入手

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IKE 用コール アドミッション制御に関する機能情報」（P.8）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

IKE 用コール アドミッション制御に関する前提条件

- ルータに 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

ルータが別のルータに対して、あるいはルータが別のルータから確立できる IKE 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。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。
- **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。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。

CAC は新しい SA だけに（つまり、ピア間に SA がまだ存在しないとき）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 要求だけが拒否されるのは、システム リソースが不足している、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 アソシエーションの制限

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 要求を廃棄します。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 の制限数を設定します。

ネゴシエーション時の IKE 接続数の制限

Cisco IOS Release 12.4(6)T では、ネゴシエーション時の IKE 接続数の制限は有効であり、設定できます。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。

crypto call admission limit ike in-negotiation-sa *number* コマンドを使用すると、設定された数のネゴシエーション時の IKE SA が、許可された IKE SA の最大数とは別個でネゴシエーションを開始します。

crypto call admission limit コマンドの **all in-negotiation-sa** *number* および **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

ここでは、次の各手順について説明します。

- 「IKE SA 制限値の設定」（P.3）（任意）
- 「システム リソース制限値の設定」（P.4）（任意）
- 「IKE 設定用のコール アドミッション制御の確認」（P.5）（任意）

（注） 次のいずれかの設定手順を実行する必要があります。

IKE SA 制限値の設定

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 モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
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：** `Router(config)# crypto call admission limit ike sa 25`	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。
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 モードを終了して、特権 EXEC モードに戻ります。

システム リソース制限値の設定

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 モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
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。 **（注）** 「システム リソースの使用状況」（P.3）を参照してください。
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 モードを終了して、特権 EXEC モードに戻ります。

IKE 設定用のコール アドミッション制御の確認

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。

```
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。

```
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

ここでは、次の設定例について説明します。

- 「例：IKE セキュリティ アソシエーション制限値の設定」（P.6）
- 「例：システム リソース制限値の設定」（P.6）

例：IKE セキュリティ アソシエーション制限値の設定

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
```

例：システム リソース制限値の設定

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

内容	参照先
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*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB 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、および機能セットの 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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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に関する機能情報

表 1 に、この機能のリリース履歴を示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。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。

表 1　IKE 用コール アドミッション制御に関する機能情報

機能名	リリース	機能情報
IKE 用コール アドミッション制御	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 Internet Key Exchange（IKE; インターネット キー エクスチェンジ）プロトコルに対する Call Admission Control（CAC; コール アドミッション制御）のアプリケーションを表します。 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。 • 「IKE 用コール アドミッション制御に関する情報」（P.2） • 「IKE 用コール アドミッション制御の設定方法」（P.3） 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**

表 1　IKE 用コール アドミッション制御に関する機能情報 （続き）

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。 • 「セキュリティ アソシエーションの制限」（P.2） • 「システム リソースの使用状況」（P.3） • 「IKE SA 制限値の設定」（P.3） • 「IKE 設定用のコール アドミッション制御の確認」（P.5） 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**

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2004 ミ 2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2004–2011, シスコシステムズ合同会社 .
All rights reserved.