SCE との ISG 統合の設定

Intelligent Services Gateway（ISG）は、エッジ デバイスが柔軟で拡張性の高いサービスを加入者に提供できる、構造化フレームワークを提供する Cisco IOS ソフトウェアの機能セットです。このモジュールでは、ISG および Cisco Service Control Engine（SCE）を、加入者セッションに対する単一のポリシー実施点として機能するように設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュール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、「SCE との ISG 統合の設定の機能情報」（P.357）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。

目次

SCE との ISG 統合の設定に関する前提条件

SCE と ISG を統合するための設定には、次の前提条件が適用されます。

ハードウェア要件

- 次のいずれかの ISG プラットフォーム（Cisco IOS Release 12.2(33)SRC 以降）
  - Cisco 7200 ルータ
  - Cisco 7301 ルータ
  - Cisco 7600 ルータ
- SCE プラットフォーム
- ISG デバイスと SCE との間に次の 2 つの接続
  - ISG デバイスと SCE がポリシー情報を交換するための制御パス
  - 加入者トラフィックを伝送するデータ パス
- ISG プラットフォームと通信できるように設定済みのポリシー サーバ。ISG-SCE 統合によって、ポリシー サーバと SCE の間の通信レイヤは不要になります。

ソフトウェア要件

- Cisco IOS Release 12.2(33)SRC 以降の ISG
- Cisco Software Release 3.1.0 以降の SCE

SCE との ISG 統合の設定に関する制約事項

SCE との ISG の統合には、次の制約事項が適用されます。

- SCE ポリシーを非アクティブ化すると、そのポリシーは SCE 上のセッションから削除され、セッション ポリシーはデフォルトの SCE ポリシーに戻ります。
- 1 つのセッションに一度に適用できる SCE ポリシーは 1 つだけです。追加のポリシーを適用すると、それまで SCE に適用されていたポリシーが上書きされます。

この機能には、RADIUS および RADIUS 拡張機能（RFC 3576 で規定）上で動作し、PUSH および PULL の 2 つのモードを持つ制御バス通信プロトコルが必要です。

- PULL モードでは、ISG デバイスは SCE からクエリーが送信されるまで待機します。
- PUSH モードでは、加入者セッションで外部サービスがアクティブ化されると、ただちに ISG デバイスによって外部機能のダウンロードが開始されます。

SCE と連携して加入者管理を行うために、制御バス プロトコルは次を実行する必要があります。

- セッションのプッシュをサポートし、セッションに関連した変更を SCE に加える。
- ID ベースのクエリーを使用して、セッション、関連 ID 、および SCE ポリシー プロファイルを ISG デバイスからプルできるようにする。

- 次のようなアカウンティング イベントをサポートする。
  - SCE の開始済みアカウンティング イベントを非同期で受け入れる。
  - SCE のアカウンティング データを、該当する ISG セッションに関連付ける。
  - SCE のアカウンティング データを解析し、プロトコル変換を実行する。

ログイン時に Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）ユーザに割り当てられるユーザ単位の IP サブネットは、SCE と通信できません。RADIUS アトリビュート Framed-Route によって、PPP ユーザにはログイン時にユーザ単位のスタティック ルートがダウンロードされます。ISG は、CoA Provision Session（ProvSess; プロビジョニング セッション）アトリビュートでは、PPP セッション用のユーザ単位のサブネット アドレスを SCE に対して送信しません。

SCE との ISG 統合の設定に関する情報

ISG-SCE 統合の概要

SCE との ISG の統合機能は、ISG と SCE をポリシー プレーン レベルで統合し、ISG と SCE が単一の論理エンティティとして機能して加入者に関するプロビジョニングを行えるようにします。ISG デバイスと SCE は通信しながら連携して加入者セッションを管理し、他の外部コンポーネントと連携する必要性が最小限に抑えられます。ISG は加入者管理をレイヤ 4 以下で処理します。SCE は主にレイヤ 4 以上を対象としています。ISG と SCE を連携するように設定すると、次の機能を持つツールを利用できるようになります。

- 加入者マッピング：加入者認識情報を ISG と SCE との間に配布します。共有の加入者セッションは、ISG によって割り当てられた固有のセッション ID を使用して、両方のデバイスから参照されます。IP アドレス、IP サブネット、Network Access Server（NAS; ネットワーク アクセス サーバ）ID、NAS ポートなどの識別キーも、セッションに割り当てられます。セッションに対してイネーブルにする必要がある SCE ポリシーは、ポリシー名によって特定されます。
- 加入者ポリシーの更新：加入者ポリシーをリアル タイムで変更します。

加入者管理での ISG と SCE の役割

表 31 に、加入者管理での ISG と SCE の固有の役割を示します。

表 31　加入者管理での ISG と SCE の役割

ISG の役割	SCE の役割
加入者の集約（Broadband Remote Access Service：BRAS） 加入者の認可または認証 ポリシー管理 次のポリシーの実施 • Quality of Service（QoS） • Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク） • リダイレクト • セッションの終了 • プリペイド[1] およびポストペイド課金	次のポリシーの実施 • アプリケーション対応サービス • リダイレクトおよびアプリケーション ベースのポリシー管理 • サービス セキュリティ • 動作の分類 • URL キャッシングおよびフィルタリング • 付加価値サービス • ペアレンタル コントロール • 従量課金およびコンテンツ課金（プリペイドおよびポストペイド）

1. Cisco 7600 ルータを ISG デバイスとして設定する場合、プリペイド課金はサポートされません。

ISG は、RADIUS の Change of Authorization（CoA）メッセージの形式で、特定の加入者セッションに関するポリシー（または外部サービス）を SCE にプッシュします。外部サービスのアクティブ化は、ISG 内部のポリシー管理コンポーネント、または外部の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバによってトリガーすることができます。SCE は ISG をポリシー マネージャと見なします。ISG は、外部 AAA サーバから SCE へのサービス アクティブ化要求のプロキシとして機能します。SCE はアカウンティング レコードを ISG に送信します。ISG は、そのアカウンティング レコードを外部 AAA サーバに送信するプロキシとして機能します（設定されている場合）。また、SCE は、プロビジョニングされていないセッションのセッション情報について ISG に問い合わせることもできます。RADIUS の Packet of Disconnect（PoD; パケット オブ ディスコネクト）によってセッションが終了すると、ISG は SCE に通知します。

SCE との ISG 統合の設定方法

SCE との ISG 統合を設定する前に、制御ポリシーとアクセス ポリシー、アカウンティング、セッション メンテナンス、およびネットワーク アクセス規定が ISG に設定されていることを確認してください。これらの設定の詳細については、『Cisco IOS Intelligent Services Gateway Configuration Guide』に説明があります。

また、SCE も正しく設定されている必要があります。SCE の設定方法については、『Cisco Service Control Engine (SCE) Software Configuration Guide, Release 3.1』に説明があります。

SCE との ISG 統合を設定するには、次の作業を実行します。

- 「SCE と ISG との間の通信の設定」（P.347）
- 「ISG での SCE 接続パラメータの設定」（P.348）
- 「ポリシー マネージャでの制御ポリシーの設定」（P.349）
- 「サービスの設定」（P.351）

SCE と ISG との間の通信の設定

SCE と ISG デバイスとの間の通信は、Cisco IOS ソフトウェアの External Policy Delegation（EPD）ハンドラ モジュールによって管理されます。EPD は ISG 上に制御パスを実装して、ISG デバイスと SCE の間のすべてのメッセージングを処理します。ISG と AAA サーバとの間の通信の詳細については、『Cisco IOS Intelligent Services Gateway Configuration Guide』に説明があります。この作業は、ISG デバイスと SCE との間の通信に関する次のようなパラメータを設定するために必須です。

- ISG デバイスおよび SCE からの CoA メッセージの送信先となるポート
- ISG が SCE からのアクセス、アカウンティング、および接続管理要求を受信するポート
- ISG デバイスと SCE との間の共有秘密キー

SCE と ISG デバイスとの間の通信を設定するには、ISG デバイス上で次のコマンドを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa server radius** {**sesm** | **proxy** | **policy-device**}
4. **client** *ipaddress* [**port** *coa destination port*] [**key** *shared secret*]
5. **authentication port** *port number*
6. **accounting port** *port number*
7. **key** *shared secret*
8. **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	**aaa server radius** {**sesm** | **proxy** | **policy-device**} 例： `Router(config)# aaa server radius policy-device`	RADIUS サーバ コンフィギュレーション モードを開始し、RADIUS プロファイルを設定します。

	コマンドまたはアクション	目的
ステップ 4	**client** *ipaddress* [**port** *coa destination port*] [**key** *shared secret]* 例： `Router(config-locsvr-radius)# client 10.10.10.1 key cisco port 1431`	クライアント固有の詳細情報を設定します。 • この IP アドレスは CoA メッセージの宛先を示します。ポートを設定しなかった場合は、デフォルトのポート（3799）が使用されます。ISG は CoA メッセージを SCE に送信して、セッションのプロビジョニング、更新、または非アクティブ化、およびポリシーのアクティブ化または非アクティブ化を行います。 • 特定のクライアント用に設定された共有秘密キーは、**key shared-secret** コマンドで設定されたキーよりも優先されます。
ステップ 5	**authentication port** *port-number* 例： `Router(config-locsvr-radius)# authentication port 1433`	EPD ハンドラがセッションを待ち受け、SCE からのクエリー要求を識別するポートを指定します。 • ポートを指定しなかった場合は、デフォルトのポート（1645）が使用されます。
ステップ 6	**accounting port** *port-number* 例： `Router(config-locsvr-radius)# accounting port 1435`	EPD ハンドラが SCE からのアカウンティングおよびピアリング要求とメンテナンス パケットを待ち受けるポートを指定します。 • ポートを指定しなかった場合は、デフォルトのポート（1646）が使用されます。
ステップ 7	**key** *shared-secret* 例： `Router(config-locsvr-radius)# key xxxxxxxxxx`	EPD ハンドラと SCE の間の共有秘密キーを設定します。 • このキーは、クライアント単位の共有秘密キーが設定されていない場合に使用されます。
ステップ 8	**exit** 例： `Router(config-locsvr-rasius)# exit`	RADIUS サーバ コンフィギュレーション モードを終了します。

ISG での SCE 接続パラメータの設定

サーバ接続管理をサーバ単位またはグローバルに設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-peer address** *ip-address* **keepalive** *seconds*
4. **policy-peer keepalive** *seconds*
5. **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	**policy-peer address** *ip-address* **keepalive** *seconds* **例：** `Router(config)# policy-peer address 10.10.10.1 keepalive 6`	指定の IP アドレスで定義される特定のポリシーに対して、キープアライブ値（秒）を設定します。 • 有効値は、5 ～ 3600 です。 • デフォルト値は 0 です。 • デフォルト値が ISG デバイスで有効になっている場合は、外部ポリシー デバイスから提示されるキープアライブ値が使用されます。
ステップ 4	**policy-peer keepalive** *seconds* **例：** `Router(config)# policy-peer keepalive 10`	キープアライブ値（秒）をグローバルに設定します。 • 有効な値の範囲は、5 ～ 3600 です。 • デフォルト値は 0 です。 • サーバ単位のキープアライブ値が設定されていない場合に、このグローバル値が使用されます。 • ISG デバイスと SCE に異なる値が設定されている場合は、低い方の値がキープアライブ インターバルとして使用されます。 • サーバ単位またはグローバルのどちらの値も設定されていない場合は、デフォルト値ゼロが使用されます。
ステップ 5	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

ポリシー マネージャでの制御ポリシーの設定

Cisco IOS コマンドで設定されたルールに従ってサービスをダウンロードするようにポリシー マネージャを設定するには、次の手順に従います。

ISG での制御ポリシーの設定

ISG デバイスで制御ポリシーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **service-policy type service name** *service-name*
6. **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	**policy-map type control** *policy-map-name* 例： `Router(config)# policy-map type control GOLD_POLICY`	指定したポリシー マップを ISG 上に設定し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 4	**class type control** {*class-map-name* | **always**} **event session-start** 例： `Router(config-control-policymap)# class type control always event acct-notification`	class-map-name に定義されている状況と一致する場合に、またはあるイベント タイプが発生する度に、アクションを適用するよう指定します。 • イベント タイプには、account-logoff、account-logon、acct-notification、credit-exhausted、quota-depleted、service-failed、service-start、service-stop、session-default-service、session-restart、session-service-found、session-start、timed-policy-expiry などがあります。
ステップ 5	*action-number* **service-policy type service name** *service-name* 例： `Router(config-control-policymap)# 1 service-policy type service name sce-service`	この制御ポリシーが該当する場合に、実行するアクションのリストを定義します。
ステップ 6	**exit** 例： `Router(config-control-policymap)# exit`	ポリシー マップ コンフィギュレーション モードを終了します。

AAA サーバでの自動サービスの設定

自動サービスによってサービスを ISG にダウンロードするには、次の手順を実行します。

手順の概要

1. Cisco-Avpair="subscriber: auto-logon-service=sce-service"

手順の詳細

ステップ 1 Cisco-Avpair="subscriber: auto-logon-service=sce-service"

SCE から ISG デバイスにサービス名をダウンロードします。

サービスの設定

サービスを設定するには、次の手順を実行します。この機能の設定は、Cisco IOS の Command Line Interface（CLI; コマンドライン インターフェイス）コマンドを使用して ISG デバイス上で実行することも、AAA サーバ上で実行することもできます。

ISG でのサービスの設定

アカウンティング機能を含むサービスを設定する手順、および SCE デバイス上の外部ポリシーをアクティブ化するには、次の手順に従います。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *service-map-name*
4. **class-map type traffic** *class-map-name*
5. **accounting aaa list** *listname*
6. **sg-service-type external-policy**
7. **policy-name** *name*
8. **service-monitor enable**
9. **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	**policy-map type service** *service-map-name* 例： `Router(config-traffic-classmap)# policy-map type service SVC`	サービスを作成し、トラフィック クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**class-map type traffic** *class-map-name* 例： `Router(config-control-policymap-class-control)# class-map type traffic bar`	トラフィック クラスを定義し、制御ポリシー マップ クラス コンフィギュレーション モードを開始します。 **（注）** Cisco 7600 ルータにはトラフィック クラスを設定できません。
ステップ 5	**accounting aaa list** *listname* 例： `Router(config-service-policymap)# accounting aaa list list1`	ISG にアカウンティングを設定し、サービス ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 6	**sg-service-type external-policy** 例： `Router(config-control-policymap)# sg-service-type external-policy`	サービスを外部ポリシーとして定義し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 7	**policy-name** *name* 例： `Router(config-control-policymap)# policy-name gold`	対応する SCE 上の外部ポリシー名を定義します。
ステップ 8	**service-monitor enable** 例： `Router(config-control-policymap)# service-monitor enable`	外部ポリシー デバイスに対するサービス モニタリングをイネーブルにします。
ステップ 9	**exit** 例： `Router(config-pol-map)# exit`	ポリシー マップ コンフィギュレーション モードを終了します。

AAA サービスでのサービスの設定

外部 AAA サーバでサービスを設定するには、次の手順を実行します。

手順の概要

1. Cisco:Avpair="subscriber:sg-service-type=external-policy"
2. Cisco:Avpair="subscriber:policy-name=gold"
3. Cisco:Avpair="subscriber:service-monitor=1"
4. Cisco:Avpair="accounting-list=list1"

手順の詳細

ステップ 1 Cisco:Avpair="subscriber:sg-service-type=external-policy"

サービスを外部ポリシーとして定義します。

ステップ 2 Cisco:Avpair="subscriber:policy-name=gold"

対応する ISG 上の外部ポリシー名を定義します。

ステップ 3 Cisco:Avpair="subscriber:service-monitor=1"

外部ポリシー デバイスに対するサービス モニタリングをイネーブルにします。

ステップ 4 Cisco:Avpair="accounting-list=list1"

ISG にアカウンティングを設定します。

トラブルシューティングのヒント

次のコマンドを使用すると、SCE との ISG 統合に関するトラブルシューティングを行えます。

- **show subscriber policy peer {address** *ip-address* **| handle** *connection-handle* **|** *id* **| all}**

例

ここでは、**show subscriber policy peer** コマンドの出力例を示します。

show subscriber policy peer all

次に、このコマンドに **all** キーワードを使用した場合の出力例を示します。

```
Router# show subscriber policy peer all

Peer IP: 10.0.0.10
Conn ID: 11
Mode   : PULL
State  : ACTIVE
Version: 1.0
Conn up time: 00:00:14
Conf keepalive: 0
Negotiated keepalive: 1000
Time since last keepalive: 00:00:14
Remove owner on pull: TRUE
```

show subscriber policy peer all detail

次に、**show subscriber policy peer** コマンドに **detail** キーワードを追加した場合の出力例を示します。

```
Router# show subscriber policy peer all detail

Peer IP: 10.0.0.10
Conn ID: 11
Mode   : PULL
State  : ACTIVE
Version: 1.0
Conn up time: 00:04:00
Conf keepalive: 0
Negotiated keepalive: 1000
Time since last keepalive: 00:04:00
Remove owner on pull: TRUE
Associated session details:
12.134.4.5session_guid_str
12.34.4.5session_guid_str
```

SCE との ISG 統合の設定例

ISG 制御パスの設定：例

次の例は、ISG 制御パスを、SCE 管理 IP アドレスおよび共有認証キーを指定して設定する方法を示しています。

```
aaa server radius policy-device
 client 10.10.10.10
 key cisco
 message-authenticator ignore
!
policy-peer address 10.10.10.10 keepalive 60
!
interface FastEthernet5/1
 ip address 10.10.10.1 255.255.255.0
```

SCE との ISG 統合：例

次の例は、2 つの SCE を、同じ認証ポートおよびアカウンティング ポートを使用して設定する方法を示しています。ISG は、一方の SCE に関する CoA メッセージの処理にポート 1700 を使用し、もう一方の SCE に関してはデフォルト ポート 3799 を使用します。ISG との各 SCE のピアリングは、異なるキープアライブ間隔で維持されます。

ユーザ セッションが開始されると、POLICY-LOCAL が適用されます。AAA サーバのユーザ プロファイルに自動ログインの指定がある場合、セッションは SCE-SERVICE-LOCAL サービスの使用を開始します。このサービスは、SCE サービス モニタ機能をイネーブルにします。ユーザ プロファイルに SCE-SERVICE-LOCAL サービスに対する自動ログインの指定がない場合、SCE は、*policy-name* の引数および **service-monitor** コマンドに、SCE のデフォルト値設定を使用します。

```
aaa accounting network service_acct start-stop group radius
```

```
aaa accounting network session_acct start-stop group radius

aaa server radius policy-device
 authentication port 1343
 accounting port 1345
 message-authenticator ignore
 client 10.10.10.1 port 1341 key cisco

class-map type traffic match-any bar
 match access-group input 102

access-list 102 permit ip any any

policy-map type service sce_service
 class type traffic bar
  accounting aaa list service_acct
 sg-service-type external-policy
 policy-name gold
 service-monitor enable

policy-map type control sce_policy
 class type control always event session-start
   1 service-policy type service sce_service
 class type control always event acct-notification
  1 proxy aaa list session_acct
```

SCE 制御バスの設定：例

PUSH モードに設定された SCE 制御バス セットアップ

次の例は、PUSH モードの SCE 制御バスの設定方法を示しています。

```
scmp
scmp name ISG radius 10.10.10.2 secret cisco auth 1433 acct 1435
scmp subscriber send-session-start
interface LineCard 0
 subscriber anonymous-group name all IP-range
  192.168.12.0:0xffffff00 scmp name ISG
```

PULL モードに設定された SCE 制御バス セットアップ

次の例は、PULL モードの SCE 制御バスの設定方法を示しています。

```
scmp
scmp name ISG radius 10.10.10.2 secret cisco auth 1433 acct 1435
interface LineCard 0
 subscriber anaonymous-group name all IP-range
  192.168.12.0:0xffffff00 scmp name ISG
```

その他の参考資料

関連資料

内容	参照先
ISG コマンド	『Intelligent Services Gateway Command Reference』
AAA 設定作業	『*Cisco IOS Security Configuration Guide*』の「Authentication, Authorization, and Accounting (AAA)」の項
AAA コマンド	『*Cisco IOS Security Configuration Guide*』の「Authentication, Authorization, and Accounting (AAA)」の項
SCE コンフィギュレーション	『*Cisco Service Control Engine (SCE) Software Configuration Guide*, Release 3.1』

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/en/US/support/index.html

SCE との ISG 統合の設定の機能情報

表 32 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

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するには、Cisco Feature Navigator を使用します。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 32 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。特に明記していないかぎり、その機能は、一連のソフトウェア リリースの以降のリリースでもサポートされます。

表 32　SCE との ISG 統合の機能情報

機能名	リリース	機能情報
ISG：ポリシー制御：ISG-SCE 制御バス	12.2(33)SRC 12.2(33)SB 15.0(1)S	ISG アカウンティングは、アカウントまたはサービスの使用に対して課金する手段を提供します。ISG アカウンティングは RADIUS プロトコルを使用して、ISG と外部の RADIUS ベース AAA または仲介サーバが簡単に連携できるようにします。 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。 • 「SCE との ISG 統合の設定に関する情報」（P.345） • 「SCE との ISG 統合の設定方法」（P.346） Cisco IOS Release 12.2(33)SRC では、サポートに Cisco 7600 ルータのサポートが追加されました。 **（注）** トラフィック クラス機能は Cisco 7600 ルータに設定できません。 Cisco IOS Release 12.2(33)SB では、サポートに Cisco 10000 ルータが追加されました。 次のコマンドが、新たに導入または変更されました。**aaa server radius policy-device**、**class type control**、**clear subscriber policy peer**、**clear subscriber policy peer session**、**policy-name**、**policy peer**、**proxy（ISG RADIUS プロキシ）**、**service-monitor**、**sg-service-type external policy**、**show subscriber policy peer**