ネットワーク アクセスを制限するための ISG ポリシーの設定

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。ISG は、加入者のセッション帯域幅およびネットワーク アクセス可能性を管理するためのポリシーの使用をサポートします。このモジュールでは、モジュラ Quality of Service（QoS）Command-Line Interface（CLI; コマンドライン インターフェイス）ポリシー、Dynamic Subscriber Bandwidth Selection（DBS）、加入者単位のファイアウォール、ISG ポリシングなどのセッション帯域幅とネットワークアクセスの制限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、「ネットワーク アクセスを制限するための ISG ポリシーの機能情報」（P.336）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。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

ネットワーク アクセスを制限するための ISG ポリシーの前提条件

リリースおよびプラットフォーム サポートの詳細については、「ネットワーク アクセスを制限するための ISG ポリシーの機能情報」（P.336）を参照してください。

ネットワーク アクセスを制限するための ISG ポリシーの制約事項

Cisco IOS Release 12.2(33)SRC 以降のリリースでは、Cisco 7600 ルータが次の制限付きでこの機能をサポートしています。

- トラフィック クラス フィーチャを必要するポリシングは設定できません。

ネットワーク アクセスを制限するための ISG ポリシーに関する情報

ネットワーク アクセスを制限するための ISG ポリシーを設定する前に、次の概念を理解しておく必要があります。

- 「ネットワーク アクセスの制限方法」（P.324）

ネットワーク アクセスの制限方法

ISG は、ネットワーク アクセスを制限するための次の方法をサポートしています。これらの方法は 1 つの ISG セッションに適用し、動的に更新できます。

Modular QoS CLI（MQC）ポリシー

MQC を使用して設定された QoS ポリシーは、加入者のセッションに対してのみサポートされます。MQC ポリシーは ISG サービスに適用できません。

Dynamic Subscriber Bandwidth Selection（DBS）

DBS では、ATM の Virtual Circuit（VC; 仮想回線）レベルで帯域幅を制御できます。加入者ドメインの ATM QoS パラメータは、PPP over Ethernet（PPPoE）または PPP over ATM（PPPoA）セッションが確立されている、ATM Permanent Virtual Circuit（PVC; 相手先固定接続）に対して適用されます。

（注） Cisco IOS Release 12.2(33)SRC では、Cisco 7600 シリーズ ルータで DBS がサポートされていません。

加入者単位のファイアウォール

加入者単位のファイアウォールは Access Control List（ACL; アクセス コントロール リスト）であり、加入者、サービス、およびパススルー トラフィックが特定の IP アドレスおよびポートにアクセスしないようにするために使用します。加入者単位のファイアウォールは、ユーザ プロファイルおよびサービス プロファイルでは設定できません。

ISG ポリシング

ISG ポリシングは、アップストリームおよびダウンストリームのトラフィックのポリシングをサポートします。ISG ポリシングは MQC を使用して設定したポリシングとは異なります。そうした ISG ポリシングは、サービス プロファイル内で設定でき、トラフィック フローのポリシングをサポートします。MQC ポリシーは、サービス プロファイルでは設定できません。また、ISG ポリシングは、ユーザ プロファイルおよびサービス プロファイルで設定して、セッション ポリシングをサポートすることもできます。

（注） Cisco IOS Release 12.2(33)SRC では、Cisco 7600 シリーズで ISG ポリシングがサポートされていません。

ネットワーク アクセスを制限するための ISG ポリシーの設定方法

ここでは、ISG ポリシングおよび加入者単位のファイアウォールを設定する手順について説明します。MQC ポリシー、DBS、およびネットワーク アクセスを制限するためのポリシーの動的な更新に対するサポートを設定する方法については、「その他の参考資料」（P.335）を参照してください。

ここでは、次の作業について説明します。

- 「ISG ポリシングの設定」（P.325）
- 「加入者単位のファイアウォールの設定」（P.330）

ISG ポリシングの設定

ISG ポリシングを設定するには、その前に次の概念について理解しておく必要があります。

- 「ISG ポリシングの概要」（P.325）

ISG ポリシングを設定するには、次の作業を実行します。

- 「ルータのサービス ポリシー マップにおけるポリシングの設定」（P.326）
- 「AAA サーバのサービス プロファイルまたはユーザ プロファイルにおけるポリシングの設定」（P.327）
- 「ISG ポリシングの確認」（P.328）

ISG ポリシングの概要

トラフィック ポリシングを使用すると、インターフェイスで送受信されるトラフィックの最大レートを制御できます。多くの場合ポリシングは、ネットワークに出入りするトラフィックを制限するために、ネットワークの終端でインターフェイス上に設定します。このレート パラメータの範囲内に入っているトラフィックが送信されますが、パラメータの範囲外となるトラフィックはドロップされるか、または別の優先順で送信されます。

ISG ポリシングは、アップストリームおよびダウンストリームのトラフィックのポリシングをサポートしており、セッションまたはフローに適用できます。ここでは、Session-Based ポリシング、および Flow-Based ポリシングについて説明します。

Session-Based ポリシング

Session-Based ポリシングは、1 つのセッションに関する加入者トラフィック全体に適用されます。図 6 では、セッション ポリシングが PPPoE クライアントから ISG へ、および ISG から PPPoE クライアントへ移動するすべてのトラフィックに適用されます。

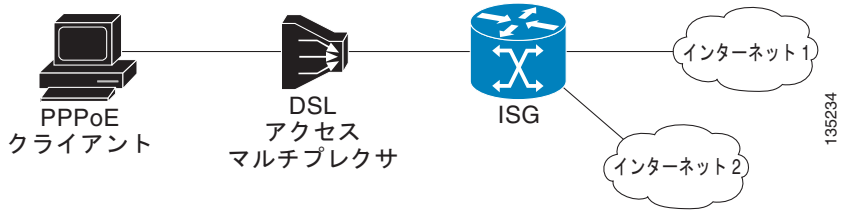
図 6　　Session-Based ポリシング

Session-Based ポリシングのパラメータは、トラフィック クラスを指定しないユーザ プロファイルまたはサービス プロファイルのいずれかで、AAA サーバに設定できます。これは、サービス ポリシー マップのルータにも設定できます。ユーザ プロファイルに設定された Session-Based ポリシングのパラメータは、サービス プロファイルまたはサービス ポリシー マップに設定された Session-Based ポリシングのパラメータよりも優先されます。

Flow-Based ポリシング

Flow-Based ポリシングは、トラフィック クラスによって指定された、宛先ベースのトラフィック フローにのみ適用されます。図 7 では、Flow-Based ポリシングで PPPoE クライアントと Internet 1 または Internet 2 の間のトラフィックを制限できます。

図 7　　Flow-Based ポリシング



Flow-Based ポリシングは、トラフィック クラスを指定しているサービス プロファイルで、AAA サーバに設定できます。これは、サービス ポリシー マップ内のトラフィック クラスでルータに設定することもできます。Flow-Based ポリシングおよび Session-Based ポリシングは、加入者トラフィック上に共存し、同時に動作可能です。

ルータのサービス ポリシー マップにおけるポリシングの設定

CLI を使用してルータ上に ISG ポリシングを設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic** *class-map-name*
5. **police input** *committed-rate normal-burst excess-burst*
6. **police output** *committed-rate normal-burst excess-burst*

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** *policy-map-name* 例： Router(config)# policy-map type service service1	ISG サービスを定義するために使用される、サービス ポリシー マップを作成または変更します。
ステップ 4	[*priority*] **class type traffic** *class-map-name* 例： Router(config-service-policymap)# class type traffic silver	すでに設定されているトラフィック クラスをポリシー マップに関連付けます。
ステップ 5	**police input** *committed-rate normal-burst excess-burst* 例： Router(config-service-policymap-class-traffic)# police input 20000 30000 60000	アップストリーム トラフィックの ISG ポリシングを設定します。 • これらのパラメータは、加入者からネットワークへのトラフィック フローを制限するために使用されます。
ステップ 6	**police output** *committed-rate normal-burst excess-burst* 例： Router(config-service-policymap-class-traffic)# police output 21000 31500 63000	ダウンストリーム トラフィックの ISG ポリシングを設定します。 • これらのパラメータは、ネットワークから加入者へのトラフィック フローを制限するために使用されます。

次の作業

サービス ポリシー マップのアクティブ化の方法を設定できます。たとえば、サービスのアクティブ化に制御ポリシーを使用できます。サービスをアクティブにする方法については、「Configuring ISG Subscriber Services」モジュールを参照してください。

AAA サーバのサービス プロファイルまたはユーザ プロファイルにおけるポリシングの設定

手順の概要

1. AAA サーバのユーザ プロファイルまたはサービス プロファイルにポリシング VSA を追加します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	次のポリシング Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）を AAA サーバのユーザ プロファイルに追加します。 26, 9, 250 "QU;*committed-rate*;*normal-burst*;*excess-burst*; D;*committed-rate*;*normal-burst*;*excess-burst*" または AAA サーバのサービス プロファイルに次のポリシング VSA を追加します。 26,9,251 "QU;*committed-rate*;*normal-burst*;*excess-burst*; D;*committed-rate*;*normal-burst*;*excess-burst*"	アップストリームおよびダウンストリームのトラフィックの ISG ポリシングをイネーブルにします。 • committed rate および normal burst を指定すると、excess burst は自動的に計算されます。 • アップストリームまたはダウンストリームのパラメータを最初に指定できます。

次の作業

サービス プロファイルのアクティブ化の方法を設定できます。たとえば、サービスのアクティブ化に制御ポリシーを使用できます。サービスをアクティブにする方法については、「Configuring ISG Subscriber Services」モジュールを参照してください。

ISG ポリシングの確認

ISG ポリシングの設定を確認するには、この作業を実行します。

手順の概要

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]

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	**show subscriber session** [**detailed**] [**identifier** *identifier*	**uid** *session-id*	**username** *name*] 例： `Router# show subscriber session detailed`	ISG 加入者のセッション情報を表示します。

例

次に、ポリシング パラメータがサービス プロファイルに設定されている場合の **show subscriber session** コマンドの出力例を示します。「Config level」フィールドは、ポリシング パラメータが設定されている場所を示しています。この場合は、サービス プロファイル内に設定されています。

```
Router# show subscriber session detailed

Current Subscriber Information: Total sessions 2

Unique Session ID: 1
.....
Session inbound features:
Feature: Policing
  Upstream Params:
Average rate = 24000, Normal burst = 4500, Excess burst = 9000
Config level = Service

Session outbound features:
Feature: Policing
  Dnstream Params:
Average rate = 16000, Normal burst = 3000, Excess burst = 6000
Config level = Service
.....
```

次に、アップストリーム ポリシング パラメータがユーザ プロファイルに指定されており、ダウンストリーム ポリシング パラメータがサービス プロファイルに指定されている場合の **show subscriber session** コマンドの出力例を示します。

```
Router# show subscriber session all

Current Subscriber Information: Total sessions 2

Unique Session ID: 2
.....
Session inbound features:
Feature: Policing
  Upstream Params:
Average rate = 24000, Normal burst = 4500, Excess burst = 9000
Config level = Per-user  ============> Upstream parameters are specified in
the user profile.

Session outbound features:
Feature: Policing
  Dnstream Params:
Average rate = 16000, Normal burst = 3000, Excess burst = 6000
Config level = Service =============> No downstream parameters in the user
profile, hence the parameters in the service profile are applied.
.....
```

加入者単位のファイアウォールの設定

加入者単位のファイアウォールを設定するには、その前に次の概念を理解しておく必要があります。

- 「加入者単位のファイアウォール」（P.330）
- 「前提条件」（P.330）
- 「制約事項」（P.330）

セッション単位の ACL を設定するには、次の作業を実行します。

- 「AAA サーバのユーザ プロファイルまたはサービス プロファイルにおける加入者単位のファイアウォールの設定」（P.330）
- 「サービス ポリシー マップでの加入者単位のファイアウォールの設定」（P.331）
- 「ISG の加入者単位のファイアウォールの確認」（P.332）

加入者単位のファイアウォール

加入者単位のファイアウォールは Cisco IOS ACL であり、加入者、サービス、およびパススルー トラフィックが特定の IP アドレスおよびポートにアクセスしないようにするために使用します。

ACL は、AAA サーバ上のユーザ プロファイルまたはサービス プロファイル、あるいは ISG のサービス ポリシー マップに設定することができます。ACL は、番号付けまたは名前付けされているアクセス リストで、ISG に設定することができます。また、ACL ステートメントはプロファイルの設定に含めることができます。

サービスに 1 つの ACL を追加すると、そのサービスのすべての加入者は、指定された IP アドレス、サブネット マスク、およびポートの組み合わせに対してサービスからアクセスできなくなります。

ユーザ プロファイルに ACL アトリビュートを追加すると、そのアトリビュートは加入者のすべてのトラフィックにグローバルに適用されます。

前提条件

この作業では、アクセス コントロール リストの設定方法について理解していることが前提になっています。

制約事項

IP ACL のみサポートされています。IPX および IPv6 ACL はサポートされていません。

AAA サーバのユーザ プロファイルまたはサービス プロファイルにおける加入者単位のファイアウォールの設定

AAA サーバのユーザ プロファイルまたはサービス プロファイルに加入者単位のファイアウォールを設定するには、この作業を実行します。

手順の概要

1. ユーザ プロファイルまたはサービス プロファイルに Upstream Access Control List Cisco AV-Pair アトリビュートを追加します。
2. ユーザ プロファイルまたはサービス プロファイルに Downstream Access Control List Cisco AV-Pair アトリビュートを追加します。

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	ユーザ プロファイルまたはサービス プロファイルに Upstream Access Control List Cisco AV-Pair アトリビュートを追加します。
	`Cisco-AVpair="ip:inacl=ACL-number"`
	または
	`Cisco-AVpair="ip:inacl=ACL-name"`
	または
	`Cisco-AVpair="ip:inacl[#number]=ACL-statement"`
		Cisco IOS ACL が、加入者からのトラフィックに適用されるように指定します。
		• *ACL-number* および *ACL-name* 引数は、ルータ上に設定されている ACL を表します。
		• *ACL-statement* 引数は、AAA サーバ上のアトリビュート設定に含まれている ACL 定義です。
		• 1 つのプロファイル内で、Upstream Access Control List アトリビュートの複数のインスタンスが発生することがあります。ACL ステートメントごとに 1 つのアトリビュートを使用してください。
		• 同じ ACL に対して複数のアトリビュートを使用できます。

ステップ 2	ユーザ プロファイルまたはサービス プロファイルに Downstream Access Control List Cisco AV-Pair アトリビュートを追加します。
	`Cisco-AVpair="ip:outacl=ACL-number"`
	または
	`Cisco-AVpair="ip:outacl=ACL-name"`
	または
	`Cisco-AVpair="ip:outacl[#number]=ACL-statement"`
		Cisco IOS ACL が、加入者へのトラフィックに適用されるように指定します。
		• *ACL-number* および *ACL-name* 引数は、ルータ上に設定されている ACL を表します。
		• *ACL-statement* 引数は、AAA サーバ上のアトリビュート設定に含まれている ACL 定義です。
		• 1 つのプロファイル内で、Downstream Access Control List アトリビュートの複数のインスタンスが発生することがあります。ACL ステートメントごとに 1 つのアトリビュートを使用してください。
		• 同じ ACL に対して複数のアトリビュートを使用できます。

次の作業

サービス プロファイルのアクティブ化の方法を設定できます。たとえば、サービスのアクティブ化に制御ポリシーを使用できます。サービスをアクティブにする方法については、「Configuring ISG Subscriber Services」モジュールを参照してください。

サービス ポリシー マップでの加入者単位のファイアウォールの設定

ISG のサービス ポリシー マップに加入者単位のファイアウォールを設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}

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** *policy-map-name* **例：** `Router(config)# policy-map type service service1`	ISG サービスを定義するために使用される、サービス ポリシー マップを作成または変更します。
ステップ 4	**ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**} **例：** `Router(config-service-policymap)# ip access-group 100 in`	パケット アクセスを制御するにはアクセス コントロール リストを適用します。 • 1 つのサービス ポリシー マップで、このコマンドの複数のインスタンスを使用できます。

次の作業

サービス プロファイルのアクティブ化の方法を設定できます。たとえば、サービスのアクティブ化に制御ポリシーを使用できます。サービスをアクティブにする方法については、「Configuring ISG Subscriber Services」モジュールを参照してください。

ISG の加入者単位のファイアウォールの確認

ISG の加入者単位のファイアウォールを確認するには、この作業を実行します。

手順の概要

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]
3. **show ip access-lists**

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	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*] **例：** `Router# show subscriber session detailed`	ISG 加入者のセッション情報を表示します。
ステップ 3	**show ip access-list** [*access-list-number* | *access-list-name*] **例：** `Router# show ip access-list`	現在のすべての IP アクセス リストの内容を表示します。

例

次に、**show subscriber session detailed** コマンドの出力例を示します。加入者単位のファイアウォールの情報は、「Session inbound features」および「Session outbound features」フィールドに示されています。

```
Router# show subscriber session detailed

Current Subscriber Information: Total sessions 1
------------------------------------------------

Session inbound features:

 Feature: Access lists
  Active IP access list:
  104

Session outbound features:

 Feature: Access lists
  Active IP access list:
  subscriber_feature#102341017649
```

show ip access-lists コマンドを使用すると、アクセス リストのステートメントを表示できます。次に、**show ip access-lists** コマンドの出力例を示します。

```
Router# show ip access-lists

Extended IP access list 104 (Compiled)
    10 permit ip host 10.0.1.6 any (500 matches)

Extended IP access list subscriber_feature#102341017649 (per-user)
    10 deny icmp host 10.0.25.25 host 10.0.3.3
    20 permit ip any any
```

ネットワーク アクセスを制限するための ISG ポリシーの設定例

ここでは、次の例について説明します。

ISG ポリシング：例

CLI を使用してサービス ポリシー マップに設定された Flow-Based ポリシング

次に、サービス ポリシー マップでの ISG Flow-Based ポリシングの設定例を示します。

```
class-map type traffic match-any C3
 match access-group in 103
 match access-group out 203

policy-map type service P3
 class type traffic C3
  police input 20000 30000 60000
  police output 21000 31500 63000
```

AAA サーバのユーザ プロファイルに設定された Session-Based ポリシング

次に、ユーザ プロファイルに設定されたポリシングの例を示します。

```
Cisco:Account-Info = "QU;23465;8000;12000;D;64000"
```

AAA サーバのサービス プロファイルに設定された Session-Based ポリシング

次に、サービス プロファイルに設定されたポリシングの例を示します。

```
Cisco:Service-Info = "QU;16000;D;31000"
```

加入者単位のファイアウォール：例

次に、AAA サーバのユーザ プロファイルまたはサービス プロファイルに設定された、加入者単位のファイアウォールの例を示します。この場合、ルータ上に ACL 104 および 105 が設定されています。「In」および「out」は、ACL アプリケーションのインバウンドおよびアウトバウンドの方向を表しています。

```
Cisco-AVpair="ip:inacl=104",
Cisco-AVpair="ip:outacl=105"
```

次に、AAA サーバのユーザ プロファイルまたはサービス プロファイルに設定された、加入者単位のファイアウォールの例を示します。この場合、ルータに名前付き ACL が設定されています。

```
Cisco-AVpair="ip:inacl=named-inacl-123",
Cisco-AVpair="ip:outacl=named-outacl-123"
```

次の加入者単位のファイアウォールの設定例には、ユーザ プロファイルまたはサービス プロファイルの設定における個別の ACL ステートメントが含まれています。

```
Cisco-AVpair="ip:inacl#1=deny icmp host 10.0.25.25 host 10.0.3.3",
Cisco-AVpair="ip:inacl#2=permit ip any any",
Cisco-AVpair="ip:outacl#1=permit ip any any"
```

その他の参考資料

ここでは、ネットワーク アクセスを制限するための ISG ポリシーに関する関連資料について説明します。

関連資料

内容	参照先
ISG コマンド	『*Cisco IOS Intelligent Services Gateway Command Reference*』
MQC を使用した QoS ポリシーの設定方法	『*Cisco IOS Quality of Service Configuration Guide*』の「Applying QoS Features Using the MQC」の項
DBS の設定方法	Cisco IOS Release 12.2(13)T の新機能マニュアルの「Dynamic Subscriber Bandwidth Selection」

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

ネットワーク アクセスを制限するための ISG ポリシーの機能情報

表 29 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。この表には、Cisco IOS Release 12.2(28)SB 以降のリリースで導入または変更された機能だけを示します。

ここに記載されていないこのテクノロジーの機能情報については、「Intelligent Services Gateway Features Roadmap」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 により、どの Cisco IOS および Catalyst OS ソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。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 29 には、一連の Cisco IOS 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 Cisco IOS 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 Cisco IOS 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 29　ネットワーク アクセスを制限するためのポリシーの機能情報

機能名	リリース	機能設定情報
ISG：フロー制御：QoS 制御：動的レート制限	12.2(28)SB 12.2(33)SRC	ISG は、レート制限のポリシーを動的に適用することにより、セッションまたはフローで許可される帯域幅を変更できます。 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。 • 「ネットワーク アクセスの制限方法」（P.324） • 「ISG ポリシングの設定」（P.325） Cisco IOS Release 12.2(33)SRC では、サポートには Cisco 7600 ルータのサポートが追加されました。