ISG 加入者サービスの設定

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 では *サービス*が、加入者セッションに対して適用できるポリシーの集合として定義されています。このモジュールでは、ISG 加入者サービスの概要、サービスおよびトラフィック クラス（サービス内に定義されたポリシーを限定するために使用するもの）の設定方法、およびサービスのアクティブ化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、「ISG 加入者サービスの機能情報」（P.230）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

ISG 加入者サービス設定の前提条件

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、「ISG 加入者サービスの機能情報」（P.230）を参照してください。

ISG 加入者サービス設定に関する制約事項

各サービスに、デフォルト以外のトラフィック クラスは 1 つしか設定できません。

1 つのセッションで複数のサービスがアクティブになっている場合、最初に一致したクラスについてのみクラス ベース アクションは実行されます。つまり、クラスが 1 つ一致すると、そのクラスに関連付けられているアクションが実行され、他のクラスとの照合は行われません。

ISG デバイスに定義されているサービスは、ポータルにはアドバタイズされないため、外部から選択できません。

Cisco 7600 ルータでは、トラフィック クラスのアトリビュートに基づく加入者サービスの設定はできません。

Cisco 7600 ルータでは、プリペイド課金サービスがサポートされません。

ISG 加入者サービスに関する情報

ISG サービス

ISG サービスは、加入者セッションに適用できるポリシーの集合です。ISG サービスは、加入者のアクセス メディアまたはプロトコルにかかわらず、任意のセッションに適用できます。また、単一のサービスを複数のセッションに適用できます。ISG サービスに、宛先ゾーンまたは特定のアップリンク インターフェイスを関連付けることは必須ではありません。

サービスを定義する方法には、CLI を使用して ISG デバイス上に設定されるサービス ポリシー マップに定義する方法と、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバなどの外部デバイス上に設定されるサービス プロファイルに定義する方法の 2 つがあります。設定は異なりますが、サービス ポリシー マップおよびサービス プロファイルは同じ目的で使用され、どちらにも、加入者セッションに適用できるトラフィック ポリシーの集合とその他の機能が含まれています。トラフィック ポリシーとは、どのセッション トラフィックにどの機能を適用するか定義するものです。また、サービス ポリシー マップまたはサービス プロファイルには、ネットワーク転送ポリシーという、セッション データ パケットをネットワークに転送する方法を指定する、特定のタイプのトラフィック ポリシーが含まれています。

プライマリ サービス

ネットワーク転送ポリシーがサービス プロファイルまたはサービス ポリシー マップに含まれている場合、そのサービスは*プライマリ サービス*と呼ばれます。複数のプライマリ サービスは相互に排他的で、同時にアクティブ化できません。新しいプライマリ サービスをアクティブ化すると、既存のプライマリ サービスおよびサービス グループでの関連付けによって、ISG は既存のプライマリ サービスに依存しているその他のサービスを削除します。

プライマリ サービスが非アクティブ化されると、セッションはネットワーク転送ポリシーがない状態になり、パケットをルーティングまたは転送する手段がなくなります。他のすべてのサービス（または他のすべてのプライマリ サービス）が非アクティブ化された場合に特定のサービスをアクティブ化するようなポリシーを適用すると、このような状態を防止できます。このバックアップ サービスによってネットワーク転送ポリシーがセッションに戻されると、加入者は Web ポータルに到達できるようになります。ポリシーを定義して適用しておかない限り、すべてのサービスが非アクティブ化されても IP セッションは自動的に終了されるわけではないことに注意してください。

トラフィック クラスとトラフィック クラスの優先度

トラフィックをフローに分類するには、フローを分類する Access Control List（ACL; アクセス コントロール リスト）、およびその ACL を適用するトラフィックの方向（インバウンドまたはアウトバウンド）を定義する必要があります。オプションで、トラフィック クラスの優先度を指定することもできます。

トラフィックがトラフィック クラスの仕様に適合することは、トラフィック クラスとの*一致*と呼ばれます。一致した場合、そのトラフィック クラスに対して、トラフィック ポリシーに定義された機能が実行されます。

トラフィック クラスを持つサービスが複数ある場合、デフォルトでは、サービスのインストール順にパケットの照合が行われます。トラフィック クラスには優先度を割り当てることもできます。トラフィック クラスの優先度によって、指定された照合でどのクラスを最初に使用するかが決まります。つまり、複数のトラフィック クラスと一致するパケットは、優先度が高いクラスに分類されます。

いずれの ACL とも一致しないパケットは、デフォルト トラフィックの一部と見なされ、セッションにトラフィック ポリシーが適用されない場合と同じように処理されます。デフォルト クラスはサービスごとに存在します。デフォルト クラスのデフォルト アクションは、トラフィックを渡すアクションです。デフォルト クラスを、トラフィックをドロップするように設定できます。デフォルトのトラフィックは、メイン セッションのアカウンティングと見なされます。

1 つのサービスには、1 つのトラフィック クラスおよび 1 つのデフォルト クラスを含めることができます。

トラフィック クラスには、Cisco IOS の **show** コマンドによって追跡できる固有識別情報が割り当てられます。

トラフィック ポリシー

トラフィック ポリシーは、データ パケットの処理方法を定義します。1 つのトラフィック ポリシーには、1 つのトラフィック クラスと 1 つ以上の機能が含まれます。ISG 制御ポリシーをトリガーするイベントは指定できますが、トラフィック ポリシーのトリガーは暗黙的であり、データ パケットの到着がトリガーとなります。

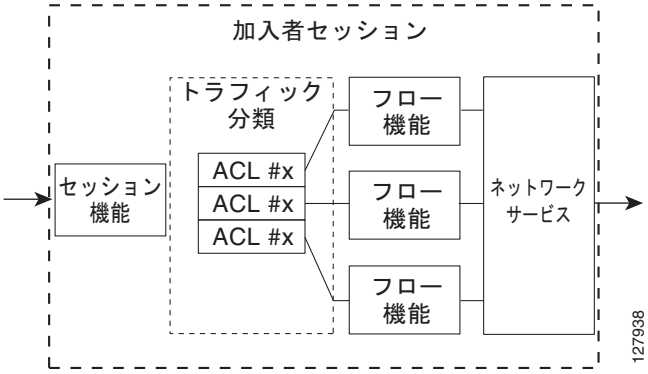
トラフィック ポリシー内に設定された機能は、そのトラフィック クラスで定義されるトラフィックに対してのみ適用されます。さまざまな機能を持つ複数のトラフィック ポリシーを、1 つのセッションに適用することができます。

ISG の機能

ISG 機能とは、セッションのデータ ストリームに対して特定の操作を実行する機能コンポーネントです。機能はトラフィック クラスに関連付けても、関連付けなくても構いません。ただし、機能をトラフィック クラスに関連付けると、そのトラフィック クラスと一致するパケットにしか適用できなくなります。関連付けない場合は、機能をセッションのすべてのパケットに適用できます。

図 5 に、加入者セッションおよびそのセッション内のトラフィック フローに、どのように機能が適用されるかを示します。

図 5　　セッションおよびフローに対する ISG 機能の適用



（注） 同じ機能を指定していて、特定のトラフィック フローではなくセッション全体に適用される 2 つ以上のサービスを、同時に 1 つのセッションに対してアクティブ化してはいけません。1 つのセッションに対してこのようなサービスが 2 つ以上アクティブ化されると、いずれかのサービスの非アクティブ化によって、その機能はセッションから除去されます。

同じ機能を指定していて、特定のフローではなくセッションに適用される複数のサービスを、加入者に提供する必要がある場合は、それらのサービスを相互に排他的になるように設定します。つまり、このようなサービスを加入者が一度に複数アクティブ化できてはいけません。同様に、制御ポリシーでも、このようなサービスを一度に複数アクティブ化できてはいけません。

サービス グループ

サービス グループとは、特定のセッションに対して同時にアクティブにできるサービスをグループ化したものです。一般的なサービス グループには、1 つのプライマリ サービスと 1 つ以上のセカンダリ サービスが含まれます。

サービス グループ内のセカンダリ サービスは、プライマリ サービスに依存するため、プライマリ サービスがすでにアクティブである場合以外、アクティブ化してはいけません。プライマリ サービスがアクティブ化された後、同じグループを参照している他のサービスもアクティブ化できます。ただし、他のグループに属するサービスは、プライマリである場合に限りアクティブ化できます。別のサービス グループのプライマリ サービスがアクティブ化されると、現行のサービス グループのすべてのサービスは、前のプライマリ サービスに依存するものであるため非アクティブ化されます。

サービスのアクティブ化方式

サービスをアクティブ化する方式には、次の 3 つがあります。

- 自動サービス アクティブ化
- 制御ポリシーによるサービス アクティブ化
- 加入者起動のサービス アクティブ化

自動サービス アクティブ化

自動サービス アトリビュートは、ユーザ プロファイルに設定できるアトリビュートであり、ユーザ プロファイルのダウンロード時（通常は認証後）に、加入者が指定のサービスに自動的にログインできるようにします。ユーザ プロファイルに自動サービス アトリビュートが指定されている機能は、*自動サービス*と呼ばれます。複数のサービスを自動サービスとしてユーザ プロファイルに指定できます。

制御ポリシーによるサービス アクティブ化

ISG 制御ポリシーを設定すると、特定の状況およびイベントに応答してサービスをアクティブ化できます。

加入者起動のサービス アクティブ化

加入者起動のサービス アクティブ化は、加入者がポータルで手動によりサービスを選択したときに実行されます。

加入者からのサービス アクティブ化要求をシステムが受信すると、ISG ポリシー エンジンは、イベント「service-start」と一致するポリシーを検索します。一致するポリシーが見つからない場合、デフォルトではポリシー エンジンは、デフォルトの AAA ネットワークの承認メソッド リストを使用してサービスをダウンロードします。このデフォルトの動作は、次のポリシー設定の場合の動作と同じです。

```
class-map type control match-all SERVICE1_CHECK
   match service-name SERVICE1
policy-map type control SERVICE1_CHECK event service-start
   1 service-policy type service name SERVICE1
```

これと同じデフォルトの動作が、加入者のログオフにも適用され、ISG ポリシー エンジンはイベント「service-stop」と一致するポリシーを検索します。

ポリシーが設定されている場合、サービスをどのように適用するか指定するのはポリシーで行います。

ルータでの ISG サービスの設定方法

ISG サービスを設定する方法は 2 つあります。1 つは、CLI を使用してローカル デバイス上にサービス ポリシー マップを設定する方法です。もう 1 つは、リモート AAA サーバ上にサービス プロファイルを設定する方法です。直接 ISG 上にサービス ポリシーを設定するには、次の作業を実行します。

- 「セッション単位の機能を持つ ISG サービスの設定」（P.216）
- 「トラフィック ポリシーを持つ ISG サービスの設定」（P.218）
- 「ISG サービス ポリシー マップでのデフォルト クラスの設定」（P.221）
- 「ISG 加入者サービスのアクティブ化」（P.222）
- 「ISG サービスの確認」（P.224）

セッション単位の機能を持つ ISG サービスの設定

サービス内に設定された機能のうち、特定のタイプの機能は、特定のトラフィック フローではなく加入者セッション全体に対して適用する必要があります。このようなセッション単位の機能を持つよう設定するサービスに、トラフィック クラスを含めてはいけません。トラフィック クラスを含まないサービス ポリシー マップを ISG に設定するには、次の作業を実行します。

（注） サービス ポリシー マップに設定できるコマンドの中には、他の設定も行わないと正しく動作しないものがあります。実際の ISG 機能の設定方法の詳細については、『*Cisco IOS Intelligent Services Gateway Configuration Guide*』の他のモジュールに説明があります。

制約事項

セッション単位の機能とトラフィック ポリシーを持つよう設定されたサービスは、正しく動作しません。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **authenticate aaa list** *name-of-list*
5. **classname** *dhcp-pool-name*
6. **ip portbundle**
7. **ip unnumbered** *interface-type interface-number*
8. **ip vrf forwarding** *name-of-vrf*
9. **service deny**
10. **service relay pppoe vpdn group** *VPDN-group-name*
11. **service vpdn group** *VPDN-group-name*
12. **sg-service-group** *service-group-name*
13. **sg-service-type** {**primary** | **secondary**}

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。

	コマンドまたはアクション	目的
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	**authenticate aaa list** *name-of-list* 例： `Router(config-service-policymap)# authenticate aaa list mlist`	このサービスはアクティブ化の条件として認証を必要とするため、認証要求を開始することを指定します。
ステップ 5	**classname** *dhcp-pool-name* 例： `Router(config-service-policymap)# classname green`	Dynamic Host Configuration Protocol（DHCP）アドレス プールをサービスまたは特定の加入者に関連付けます。
ステップ 6	**ip portbundle** 例： `Router(config-service-policymap)# ip portbundle`	このサービス ポリシー マップで ISG Port-Bundle Host Key 機能をイネーブルにします。
ステップ 7	**ip unnumbered** *interface-type interface-number* 例： `Router(config-service-policymap)# ip unnumbered ethernet 0`	インターフェイスに IP アドレスを明示的に割り当てなくても、インターフェイスで IP 処理をイネーブルにします。
ステップ 8	**ip vrf forwarding** *name-of-vrf* 例： `Router(config-service-policymap)# ip vrf forwarding blue`	サービスを VRF に関連付けます。 • このコマンドの設定により、このサービスはプライマリ サービスとなります。
ステップ 9	**service deny** 例： `Router(config-service-policymap)# service deny`	加入者セッションに対するネットワーク サービスを拒否します。
ステップ 10	**service relay pppoe vpdn group** *VPDN-group-name* 例： `Router(config-service-policymap)# service relay pppoe vpdn group group1`	加入者セッションに対して、Layer 2 Tunnel Protocol（L2TP）トンネルによる PPPoE Active Discovery（PAD）メッセージのリレーをイネーブルにします。
ステップ 11	**service vpdn group** *VPDN-group-name* 例： `Router(config-service-policymap)# service vpdn group vpdn1`	ISG 加入者セッションに Virtual Private Dialup Network（VPDN）サービスを提供します。 • このコマンドの設定により、このサービスはプライマリ サービスとなります。

	コマンドまたはアクション	目的
ステップ 12	**sg-service-group** *service-group-name* 例： `Router(config-service-policymap)# sg-service-group group1`	サービスを指定したサービス グループに関連付けます。
ステップ 13	**sg-service-type** {**primary** | **secondary**} 例： `Router(config-service-policymap)# sg-service-type primary`	サービスをプライマリまたはセカンダリ サービスとして定義します。 • プライマリ サービスは、ネットワーク転送ポリシーが含まれるサービスです。サービスをプライマリ サービスとして定義するには、**sg-service-type primary** コマンドを使用する必要があります。プライマリ サービスではないサービスは、デフォルトではセカンダリ サービスとして定義されます。

トラフィック ポリシーを持つ ISG サービスの設定

ISG トラフィック ポリシーには、1 つのトラフィック クラスと 1 つ以上の ISG 機能が含まれます。トラフィック クラスによって、機能を適用するトラフィックを定義します。トラフィック ポリシーを持つ ISG サービスをルータに設定するには、次の作業を実行します。

- 「ISG トラフィック クラス マップの定義」（P.218）
- 「トラフィック ポリシーを持つ ISG サービス ポリシー マップの設定」（P.219）

ISG トラフィック クラス マップの定義

トラフィック クラス マップを設定するには、次の作業を実行します。通常、トラフィック クラス マップには、フローを分類する Access Control List（ACL; アクセス コントロール リスト）と、その ACL を適用するトラフィックの方向（インバウンドまたはアウトバウンド）を指定します。

（注） 空のトラフィック クラス マップを設定することもでき、アクセス リストの指定がないトラフィック クラス マップを設定して、トラフィック ポリシーを含むサービスを、すべてのセッション トラフィックに適用するように設定できます。

前提条件

この作業は、トラフィックの分類に使用する Access Control List（ACL; アクセス コントロール リスト）は設定済みであることが前提になっています。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type traffic match-any** *class-map-name*
4. **match access-group input** {*access-list-number* | **name** *access-list-name*}
5. **match access-group output** {*access-list-number* | **name** *access-list-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	**class-map type traffic match-any** *class-map-name* 例： `Router(config)# class-map type traffic match-any class1`	パケットを指定された ISG トラフィック クラスと照合するために使用する、トラフィック クラス マップを作成または変更します。
ステップ 4	**match access-group input** {*access-list-number* | **name** *access-list-name*} 例： `Router(config-traffic-classmap)# match access-group input 101`	（任意）指定した ACL をベースに、入力クラス マップに対して一致基準を設定します。 • 特定のトラフィック フローではなくすべてのセッション トラフィックに適用するトラフィック ポリシーを定義する場合は、この手順をスキップしてください。
ステップ 5	**match access-group output** {*access-list-number* | **name** *access-list-name*} 例： `Router(config-traffic-classmap)# match access-group output 102`	（任意）指定した ACL をベースに、出力クラス マップに対して一致基準を設定します。 • 特定のトラフィック フローではなくすべてのセッション トラフィックに適用するトラフィック ポリシーを定義する場合は、この手順をスキップしてください。
ステップ 6	**exit** 例： `Router(config-traffic-classmap)# exit`	グローバル コンフィギュレーション モードに戻ります。

トラフィック ポリシーを持つ ISG サービス ポリシー マップの設定

ISG サービスを設定するには、ISG 上にサービス ポリシー マップを作成するか、または外部 AAA サーバ上にサービス プロファイルを作成します。ISG 上のサービス ポリシー マップにトラフィック ポリシーを設定するには、次の作業を実行します。

（注） サービス ポリシー マップに設定できるコマンドの中には、他の設定も行わないと正しく動作しないものがあります。実際の ISG 機能の設定方法の詳細については、『*Cisco IOS Intelligent Services Gateway Configuration Guide*』の他のモジュールに説明があります。

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. **accounting aaa list** *AAA-method-list*
6. **police** {**input** | **output**} *committed-rate normal-burst excess-burst*
7. **prepaid config** *name-of-configuratio*n
8. **redirect** [**list** *access-list-number*] **to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*]
9. **timeout absolute** *duration-in-seconds*
10. **timeout idle** *duration-in-seconds*
11. **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** *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 classb`	作成または変更するポリシーの、名前付きトラフィック クラスを指定します。 • *priority* 引数は、指定した照合で最初に使用するクラスを決定します。複数のトラフィック クラスと一致するパケットは、優先度が高いクラスに分類されます。
ステップ 5	**accounting aaa list** *AAA-method-list* 例： `Router(config-service-policymap-class-traffic)# accounting aaa list mlist1`	アカウンティングをイネーブルにし、アカウンティング アップデートの送信先となる AAA メソッド リストを指定します。
ステップ 6	**police** {**input**	**output**} *committed-rate normal-burst excess-burst* 例： `Router(config-service-policymap-class-traffic)# police input 20000 30000 60000`	ISG ポリシングを、アップストリームまたはダウンストリームのトラフィックに対してイネーブルにします。 • アップストリームとダウンストリームのポリシングを設定するには、このコマンドを 2 回実行します。

	コマンドまたはアクション	目的
ステップ 7	**prepaid config** *name-of-configuration* 例： `Router(config-service-policymap-class-traffic)# prepaid config conf-prepaid`	プリペイド課金に関する ISG のサポートをイネーブルにし、プリペイド課金パラメータを定義するための設定を適用します。
ステップ 8	**redirect** [**list** *access-list-number*] **to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*] 例： `Router(config-service-policymap-class-traffic)# redirect to ip 10.10.10.10`	指定されたサーバまたはサーバ グループに、トラフィックをリダイレクトします。
ステップ 9	**timeout absolute** *duration-in-seconds* 例： `Router(config-control-policymap-class-traffic)# timeout absolute 30`	セッションのライフタイムを 30 ～ 4294967 秒の範囲で指定します。
ステップ 10	**timeout idle** *duration-in-seconds* 例： `Router(config-control-policymap-class-traffic)# timeout idle 3000`	接続を終了するまでに、その接続をアイドルにしておく時間を指定します。範囲は、プラットフォームとリリースによって異なります。詳細は、疑問符（?）を入力してオンライン ヘルプ機能を使用してください。
ステップ 11	**end** 例： `Router(config-service-policymap-class-traffic)#end`	（任意）特権 EXEC モードに戻ります。

ISG サービス ポリシー マップでのデフォルト クラスの設定

いずれのトラフィック クラスとも一致しないパケットは、デフォルト トラフィックの一部と見なされ、セッションにトラフィック ポリシーが適用されない場合と同じように処理されます。デフォルトでは、サービスごとにデフォルト クラスが存在します。デフォルト クラスのデフォルト アクションは、トラフィックを渡すアクションです。デフォルト クラスを設定するには、次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. **class type traffic default** {**in-out** | **input** | **output**}
5. **drop**

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	**class type traffic default** {**in-out** | **input** | **output**} **例：** `Router(config-service-policymap)# class type traffic default in-out`	デフォルトのトラフィック クラスをサービス ポリシー マップに関連付けます。 • トラフィックが設定済みのクラス マップのどの一致基準とも一致しない場合、このデフォルトのクラスが、そのトラフィックを誘導するクラスとなります。
ステップ 5	**drop** **例：** `Router(config-service-policymap-class-traffic)# drop`	このクラスと一致するパケットを廃棄するように、デフォルトのトラフィック クラスを設定します。

ISG 加入者サービスのアクティブ化

ISG 加入者サービスをアクティブ化するには、加入者のユーザ プロファイルに自動アクティブ化サービスとしてサービスを指定する方法、サービスをアクティブ化する制御ポリシーを設定する方法、および加入者起動サービス ログインを使用する方法という、3 つの方法があります。加入者のサービスへのログインをイネーブルにするために、特別な設定は必要ありません。

サービスに自動アクティブ化を設定する場合、およびサービスをアクティブ化する制御ポリシーを設定する場合は、次の作業を実行します。

- 「ユーザ プロファイルでの自動サービス アクティブ化の設定」（P.222）
- 「サービスをアクティブ化する ISG 制御ポリシーの設定」（P.223）

ユーザ プロファイルでの自動サービス アクティブ化の設定

加入者のユーザ プロファイルで、サービスに対して自動サービス アクティブ化を設定するには、次の作業を実行します。

手順の概要

1. ユーザ プロファイルに自動サービス 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	`Add the Auto Service attribute to the user profile.` `26,9,251="A`*`service-name`*`[;`*`username`*`;`*`password`*`]"`	このユーザ プロファイルがダウンロードされると、加入者は指定のサービスに自動的にログインします。

サービスをアクティブ化する ISG 制御ポリシーの設定

サービスをアクティブ化する制御ポリシーを設定するには、次の作業を実行します。

前提条件

制御ポリシー マップに名前付き制御クラス マップを指定する場合は、制御クラス マップを設定する必要があります。制御ポリシーの設定の詳細については、「Configuring ISG Control Policies」モジュールを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {**always** | *map-class-name*} [**event account-logon** | **credit-exhausted** | **quota-depleted** | **service-start** | **service-stop** | **session-default-service** | **session-service-found** | **session-start** | **timed-policy-expiry**]
5. *action-number* **service-policy type service** {**name** | **unapply**} *policy-map-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	**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 policy1`	ISG 制御ポリシーを指定するポリシー マップを作成または変更します。

	コマンドまたはアクション	目的
ステップ 4	**class type control** {**always** | *map-class-name*} [**event account-logon** | **credit-exhausted** | **quota-depleted** | **service-start** | **service-stop** | **session-default-service** | **session-service-found** | **session-start** | **timed-policy-expiry**] **例：** `Router(config-control-policymap)# class type control always event session-start`	クラスを指定し、オプションでアクションを設定するイベントも指定します。
ステップ 5	*action-number* **service-policy type service** {**name** | **unapply**} *policy-map-name* **例：** `Router(config-control-policymap-class-control)# 1 service-policy type service service1`	指定されたサービス ポリシー マップを適用します。 • サービス ポリシー マップを削除するには、**unapply** キーワードを使用します。

ISG サービスの確認

ISG サービスの設定を確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show class-map type traffic**
3. **show policy-map type service**

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 class-map type traffic** **例：** `Router# show class-map type traffic`	すべてのトラフィック クラス マップおよびそれらの一致基準を表示します。
ステップ 3	**show policy-map type service** **例：** `Router# show policy-map type service`	すべてのサービス ポリシー マップの内容を表示します。

ISG サービスの設定例

ここでは、次の例について説明します。

例：フロー単位のアカウンティング用のサービス

次の例では、サービス「SERVICE1」にフロー単位のアカウンティングを設定します。アクセス リスト「SERVICE1_ACL_IN」および「SERVICE1_ACL_OUT」を使用して、トラフィック クラスを定義します。これらの例は同等で、ISG 上に直接設定されるサービス ポリシー マップに設定する方式と、AAA サーバ上に設定されるサービス プロファイルに設定する方式という、2 つのサービス設定方法を示しています。

ISG の設定

```
class-map type traffic match-any SERVICE1_TC
 match access-group input name SERVICE1_ACL_IN
 match access-group output name SERVICE1_ACL_OUT
!
policy-map type service SERVICE1
 10 class type traffic SERVICE1_TC
  accounting aaa list CAR_ACCNT_LIST
 class type traffic default in-out
  drop
```

AAA サーバ設定

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name SERVICE1_ACL_IN priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name SERVICE1_ACL_OUT priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = ISERVICE1
```

例：絶対タイムアウトおよびアイドル タイムアウト用のサービス

次の例では、サービス「SERVICE1」にフロー単位のアカウンティング、絶対タイムアウト、およびアイドル タイムアウトを設定します。アクセス リスト「SERVICE1_ACL_IN」および「SERVICE1_ACL_OUT」を使用して、トラフィック クラスを定義します。これらの例は同等で、ISG 上に直接設定されるサービス ポリシー マップに設定する方式と、AAA サーバ上に設定されるサービス プロファイルに設定する方式という、2 つのサービス設定方法を示しています。

ISG の設定

```
class-map type traffic match-any SERVICE1_TC
 match access-group input name SERVICE1_ACL_IN
 match access-group output name SERVICE1_ACL_OUT
!
policy-map type service SERVICE1
 10 class type traffic SERVICE1_TC
  timeout idle 600
  timeout absolute 1800
  accounting aaa list CAR_ACCNT_LIST
 class type traffic default in-out
  drop
```

AAA サーバ設定

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name SERVICE1_ACL_IN priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name SERVICE1_ACL_OUT priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = ISERVICE1
  session-timeout = 1800
  idle-timeout = 600
```

例：ISG ポリシング用のサービス

次の例では、サービス「BOD1M」にフロー単位のアカウンティングおよび ISG ポリシングを設定します。アクセス リスト「BOD1M_IN_ACL_IN」および「BOD1M_ACL_OUT」を使用して、トラフィック クラスを定義します。これらの例は同等で、ISG 上に直接設定されるサービス ポリシー マップに設定する方式と、AAA サーバ上に設定されるサービス プロファイルに設定する方式という、2 つのサービス設定方法を示しています。

ISG の設定

```
class-map type traffic match-any BOD1M_TC
 match access-group input name BOD1M_IN_ACL_IN
 match access-group output name BOD1M_ACL_OUT
!
policy-map type service BOD1M
 10 class type traffic BOD1M_TC
  accounting aaa list CAR_ACCNT_LIST
  police input 512000 256000 5000
  police output 1024000 512000 5000
 class type traffic default in-out
  drop
```

AAA サーバ設定

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name BOD1M_IN_ACL priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name BOD1M _OUT_ACL priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = IBOD1M
 Cisco-SSG-Service-Info = QU;512000;256000;5000;D;1024000;512000;5000
```

例：加入者単位のファイアウォール用のサービス

次の例では、サービス「SERVICE2」に加入者単位のファイアウォールを設定します。このサービスはトラフィック クラスを含まないため、セッション全体に適用されます。これらの例は同等で、ISG 上に直接設定されるサービス ポリシー マップに設定する方式と、AAA サーバ上に設定されるサービス プロファイルに設定する方式という、2 つのサービス設定方法を示しています。

ISG の設定

```
policy-map type service SERVICE2
 ip access-group INTERNET_IN_ACL in
 ip access-group INTERNET_OUT_ACL out
```

AAA サーバ設定

```
Attributes/
 Cisco-AVPair = ip:inacl=INTERNET_IN_ACL
 Cisco-AVPair = ip:outacl=INTERNET_OUT_ACL
```

例：レイヤ 4 加入者トラフィックのリダイレクト用のサービス

次の例は、「UNAUTHORIZED_REDIRECT_SVC」という名前のサービスの設定を示しています。セッションの開始時にサービスを適用するように、制御ポリシー「UNAUTHEN_REDIRECT」を設定します。

```
class-map type traffic match-any UNAUTHORIZED_TRAFFIC
 match access-group input 100

policy-map type service UNAUTHORIZED_REDIRECT_SVC
 class type traffic UNAUTHORIZED_TRAFFIC
  redirect to ip 10.0.0.148 port 8080

policy-map type control UNAUTHEN_REDIRECT
 class type control always event session-start
  1 service-policy type service name UNAUTHORIZED_REDIRECT_SVC
```

例：認可後のレイヤ 4 リダイレクト サービスの非アクティブ化

次の例では、レイヤ 4 リダイレクトを設定したサービスを、トラフィックの承認後、つまり該当サービスのアクティブ化後に非アクティブ化します。

```
class-map traffic UNAUTHORIZED_TRAFFIC
match access-group input 100

policy-map type service UNAUTHORIZED_REDIRECT_SVC
 class traffic UNAUTHORIZED_TRAFFIC
  redirect to ip 10.0.0.148 port 8080

class-map control match-all CHECK_ISP1
 match service ISP1

policy-map control UNAUTHEN_REDIRECT
 class control always event session-start
  1 service-policy type service name UNAUTHORIZED_REDIRECT_SVC
 class control CHECK_ISP1 event service-start
  1 service-policy type service unapply UNAUTHORIZED_REDIRECT_SVC
  1 service-policy type service name ISP1
```

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*』
ISG コマンド	『*Cisco IOS Intelligent Services Gateway Command Reference*』

規格

規格	タイトル
サポートされる新しい規格や変更された規格はありません。	—

MIB

MIB	MIB リンク
サポートされる新しい MIB や変更された MIB はありません。	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
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	—

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

ISG 加入者サービスの機能情報

表 20 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 20 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 20　ISG 加入者サービスの機能情報

機能名	リリース	機能設定情報
ISG：ポリシー制御：サービス プロファイル	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG ではサービスが、加入者セッションに対して適用できるポリシーの集合として定義されています。サービスは、ルータまたは外部 AAA サーバ上に設定できます。 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。 • 「ISG 加入者サービスに関する情報」（P.212） • 「ルータでの ISG サービスの設定方法」（P.215） Cisco IOS Release 12.2(33)SRC では、この機能が Cisco 7600 ルータに実装されました。
ISG：ポリシー制御：ユーザ プロファイル	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG ユーザ プロファイルは、指定された加入者の ISG セッションに適用できるサービスおよび機能を指定します。ユーザ プロファイルは外部 AAA サーバ上に定義されます。 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。 • 「ユーザ プロファイルでの自動サービス アクティブ化の設定」（P.222）