ISG 制御ポリシーの設定

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 制御ポリシーは、指定された条件とイベントに対応してシステムが実行するアクションを定義します。一貫したポリシー言語を使用して幅広いシステム アクション、条件、およびイベントを組み合わせることによって、柔軟で正確な ISG の設定方法を提供できます。このモジュールでは、ISG 制御ポリシーの設定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 制御ポリシーの機能情報」（P.50）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 制御ポリシー設定の前提条件

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 制御ポリシーの機能情報」（P.50）を参照してください。

認証および認可のアクションを定義する前に、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）方式のリストを設定する必要があります。

ISG 制御ポリシー設定の制約事項

制御ポリシーは、セッションで直接アクティブ化されることはなく、指定されたコンテキストでアクティブ化されます。コンテキストでホストされるすべてのセッションに制御ポリシーが適用されます。

特定のコンテキストに適用できる制御ポリシー マップは 1 つだけです。

制御ポリシーは、ルータの Command-Line Interface（CLI; コマンドライン インターフェイス）だけで定義できます。

すべてのアクションがすべてのイベントに関連付けられるわけではありません。

制御ポリシー マップが定義されると、既存の制御クラス間に新しい制御クラスを挿入できなくなります。

ISG 制御ポリシーに関する情報

制御ポリシー

制御ポリシーは、指定されたイベントと条件に対応してシステムが実行するアクションを定義します。たとえば、特定の加入者を認証し、特定のサービスへのアクセス権を付与するように制御ポリシーを設定できます。

制御ポリシーは 1 つ以上の制御ポリシー ルールで作成されます。制御ポリシー ルールとは、制御クラスと 1 つ以上のアクションの関連付けです。制御クラスは、アクションを実行する前に満たす必要のある条件を定義します。

制御ポリシーの定義には 3 つの手順があります。

1. 1 つ以上の制御クラス マップを作成します。

   制御クラス マップは、アクティブ化するポリシーに対して満たす必要のある条件を指定します。オプションで、クラスの評価を開始するイベントも指定します。制御クラス マップには、複数の条件を含めることができ、それぞれの条件が true または false に評価されます。Match ディレクティブを使用して、クラスが true と評価されるためには、個々の条件のすべてまたは一部が true と評価されるか、またはいずれも true と評価されないかを指定できます。

2. 制御ポリシー マップを作成します。

   制御ポリシー マップには 1 つ以上の制御ポリシー ルールが含まれます。制御ポリシー ルールは、制御クラス マップを 1 つ以上のアクションに関連付けます。アクションに番号が付けられ、順に実行されます。

3. 制御ポリシー マップを適用します。

   制御ポリシー マップは、コンテキストに適用するとアクティブ化されます。制御ポリシー マップは、次のタイプのコンテキストのいずれかに適用できます。次のリストは、コンテキストのタイプを優先順位の高い順に示しています。たとえば、PVC に適用される制御ポリシー マップは、インターフェイスに適用される制御ポリシー マップよりも優先されます。

   - Permanent Virtual Circuit（PVC; 相手先固定接続）
   - Virtual Circuit（VC; 仮想回線）クラス
   - 仮想テンプレート
   - サブインターフェイス
   - インターフェイス
   - グローバル

   一般的に、より限定的なコンテキストに適用される制御ポリシー マップが、より汎用的なコンテキストに適用されるポリシー マップよりも優先されます。

（注） トラフィック ポリシーは、ISG で使用される別のタイプのポリシーです。トラフィック ポリシーはデータ パケットの処理を定義し、サービス ポリシー マップまたはサービス プロファイルで設定されます。トラフィック ポリシーの詳細については、「Configuring ISG Subscriber Services」モジュールを参照してください。

差別化された初期ポリシー制御

加入者の認証失敗は、access-reject（RADIUS サーバが Reject で応答）またはアクセス要求のタイムアウト（RADIUS サーバに到達不能）が原因で発生する可能性があります。

ISG 制御ポリシーと、「radius-timeout」イベントおよび「access-reject」イベントに設定されたアクションを使用すると、システムで認証の失敗の理由を判断できます。さまざまなイベントがスローされます（受信した認証の拒否、利用できない RADIUS サーバのイベントなど）。これによって、制御ポリシーで、認証の失敗の各タイプに対して複数のアクションを指定できます。たとえば、RADIUS サーバがダウンしているか、到達不能な場合、加入者に一時的なアクセス権を付与できます。

この機能は、加入者認証のための IP ベースのセッションのみで使用できます。この機能では、Point-to-Point Protocol over Ethernet（PPPoE）セッションはサポートされません。

制御ポリシーの使用

特定のイベントおよび条件に対応して特定のアクションを実行するように ISG を設定するには、制御ポリシーを使用します。たとえば、次の目的で制御ポリシーを使用できます。

- 加入者セッションが最初に検出されたときに、デフォルトのサービスをアクティブ化する。
- アクセス側に制御プロトコルが存在している場合、加入者 ID の収集に順序を付ける。
- システムでアイドル タイムアウトや、クレジットを使い切った加入者に対応する方法を決定する。
- IP アドレスまたは MAC アドレスに基づく認可をイネーブルにするために、透過的な自動ログインをイネーブルにする。
- セッションを無認証のままで継続できる最大時間を設定する。
- セッションの状態情報を他のデバイスに定期的に送信する

ISG 制御ポリシーの設定方法

制御クラス マップの設定

制御クラス マップには、制御ポリシーを実行するために満たす必要のある条件が含まれます。制御クラス マップには、1 つ以上の条件を含めることができます。制御クラス マップを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type control** [**match-all** | **match-any** | **match-none**] *class-map-name*
4. **available** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
5. **greater-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
6. **greater-than-or-equal** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
7. **less-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
8. **less-than-or-equal** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
9. **match authen-status** {**authenticated** | **unauthenticated**}
10. **match authenticated-domain** {*domain-name* | **regexp** *regular-expression*}
11. **match authenticated-username** {*username* | **regexp** *regular-expression*}
12. **match dnis** {*dnis* | **regexp** *regular-expression*}
13. **match media** {**async** | **atm** | **ether** | **ip** | **isdn** | **mpls** | **serial**}
14. **match mlp-negotiated** {**no** | **yes**}
15. **match nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **circuit-id** *name* | **ipaddr** *ip-address* | **port** *port-number* | **remote-id** *name* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** {**async** | **atm** | **basic-rate** | **enm** | **ether** | **fxo** | **fxs** | **none** | **primary-rate** | **synch** | **vlan** | **vty**} | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
16. **match no-username** {**no** | **yes**}

17. **match protocol** {**atom** | **ip** | **pdsn** | **ppp** | **vpdn**}
18. **match service-name** {*service-name* | **regexp** *regular-expression*}
19. **match source-ip-address** *ip-address subnet-mask*
20. **match timer** {*timer-name* | **regexp** *regular-expression*}
21. **match tunnel-name** {*tunnel-name* | **regexp** *regular-expression*}
22. **match unauthenticated-domain** {*domain-name* | **regexp** *regular-expression*}
23. **match unauthenticated-username** {*username* | **regexp** *regular-expression*}
24. **match vrf** {*vrf-name* | **regexp** *regular-expression}*

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 control** [**match-all** | **match-any** | **match-none**] *class-map-name* 例： `Router(config)# class-map type control match-all class1`	制御ポリシー マップのアクションが実行される条件を定義する制御クラス マップを作成または変更し、制御クラス マップ モードを開始します。
ステップ 4	**available** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**} 例： `Router(config-control-classmap)# available nas-port`	（任意）指定された加入者 ID がローカルで利用可能な場合に true と評価される条件を作成します。
ステップ 5	**greater-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*} 例： `Router(config-control-classmap)# greater-than nas-port type atm vpi 200 vci 100`	（任意）加入者の Network Access Server（NAS; ネットワーク アクセス サーバ）ポート ID が、指定された値よりも大きい場合に true と評価される条件を作成します。

	コマンドまたはアクション	目的
ステップ 6	**greater-than-or-equal** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*} **例：** `Router(config-control-classmap)# greater-than-or-equal nas-port vlan 10`	（任意）指定された加入者 NAS ポート ID が、指定された値と同じか、それ以上の場合に true と評価される条件を作成します。
ステップ 7	**less-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*} **例：** `Router(config-control-classmap)# less-than nas-port type atm vpi 200 vci 105`	（任意）指定された加入者 NAS ポート ID が、指定された値よりも小さい場合に true と評価される条件を作成します。
ステップ 8	**less-than-or-equal** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*} **例：** `Router(config-control-classmap)# less-than-or-equal nas-port ipaddr 10.10.10.10`	（任意）指定された加入者 NAS ポート ID が、指定された値と等しいか、またはそれよりも小さい場合に true と評価される条件を作成します。
ステップ 9	**match authen-status** {**authenticated** | **unauthenticated**} **例：** `Router(config-control-classmap)# match authen-status authenticated`	（任意）加入者の認証ステータスが、指定された認証ステータスと一致する場合に true と評価される条件を作成します。
ステップ 10	**match authenticated-domain** {*domain-name* | **regexp** *regular-expression*} **例：** `Router(config-control-classmap)# match authenticated-domain cisco.com`	（任意）加入者の認証されたドメインが、指定されたドメインと一致する場合に true と評価される条件を作成します。
ステップ 11	**match authenticated-username** {*username* | **regexp** *regular-expression*} **例：** `Router(config-control-classmap)# match authenticated-username regexp "admin@.*com"`	（任意）加入者の認証されたユーザ名が、指定されたユーザ名と一致する場合に true と評価される条件を作成します。

	コマンドまたはアクション	目的
ステップ 12	**match dnis** {*dnis* | **regexp** *regular-expression*} **例：** `Router(config-control-classmap)# match dnis reg-exp 5551212`	（任意）加入者の着信番号識別サービス番号（DNIS 番号。*called-party number* とも呼ばれる）が、指定された DNIS 番号と一致している場合に true と評価される条件を作成します。
ステップ 13	**match media** {**async** | **atm** | **ether** | **ip** | **isdn** | **mpls** | **serial**} **例：** `Router(config-control-classmap)# match media atm`	（任意）加入者のアクセス メディア タイプが、指定されたメディア タイプと一致している場合に true と評価される条件を作成します。
ステップ 14	**match mlp-negotiated** {**no** | **yes**} **例：** `Router(config-control-classmap)# match mlp-negotiated yes`	（任意）加入者のセッションがマルチリンク PPP を使用して確立されたかどうかに応じて true または false と評価される条件を作成します。 • **yes** キーワードが使用された場合、この条件は、加入者のセッションがマルチリンク PPP ネゴシエーションを使用して確立された場合に true と評価されます。
ステップ 15	**match nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **circuit-id** *name* | **ipaddr** *ip-address* | **port** *port-number* | **remote-id** *name* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** {**async** | **atm** | **basic-rate** | **enm** | **ether** | **fxo** | **fxs** | **none** | **primary-rate** | **synch** | **vlan** | **vty**} | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*} **例：** `Router(config-control-classmap)# match nas-port type ether slot 3`	（任意）加入者の NAS ポート ID が、指定された値と一致する場合に true と評価される条件を作成します。
ステップ 16	**match no-username** {**no** | **yes**} **例：** `Router(config-control-classmap)# match no-username yes`	（任意）加入者のユーザ名が利用可能かどうかに応じて true または false と評価される条件を作成します。 • **yes** キーワードが使用された場合、この条件は、加入者のユーザ名が利用可能ではない場合に true と評価されます。
ステップ 17	**match protocol** {**atom** | **ip** | **pdsn** | **ppp** | **vpdn**} **例：** `Router(config-control-classmap)# match protocol ip`	（任意）加入者のアクセス プロトコル タイプが、指定されたプロトコル タイプと一致している場合に true と評価される条件を作成します。
ステップ 18	**match service-name** {*service-name* | **regexp** *regular-expression*} **例：** `Router(config-control-classmap)# match service-name service1`	（任意）加入者に関連付けられたサービス名が、指定されたサービス名と一致している場合に true と評価される条件を作成します。

	コマンドまたはアクション	目的
ステップ 19	**match source-ip-address** *ip-address subnet-mask* 例： `Router(config-control-classmap)# match source-ip-address 10.10.10.10 255.255.255.255`	（任意）加入者の送信元 IP アドレスが、指定された IP アドレスと一致している場合に true と評価される条件を作成します。
ステップ 20	**match timer** {*timer-name* | **regexp** *regular-expression*} 例： `Router(config-control-classmap)# match timer TIMERA`	（任意）指定されたポリシー タイマーの終了時に true と評価される条件を作成します。
ステップ 21	**match tunnel-name** {*tunnel-name* | **regexp** *regular-expression*} 例： `Router(config-control-classmap)# match tunnel-name regexp L.*`	（任意）加入者の Virtual Private Dialup Network（VPDN）トンネル名が、指定されたトンネル名と一致している場合に true と評価される条件を作成します。
ステップ 22	**match unauthenticated-domain** {*domain-name* | **regexp** *regular-expression*} 例： `Router(config-control-classmap)# match unauthenticated-domain example.com`	（任意）加入者の無認証のドメイン名が、指定されたドメイン名と一致する場合に true と評価される条件を作成します。
ステップ 23	**match unauthenticated-username** {*username* | **regexp** *regular-expression*} 例： `Router(config-control-classmap)# match unauthenticated-username regexp examplename1`	（任意）加入者の無認証のユーザ名が、指定されたユーザ名と一致する場合に true と評価される条件を作成します。
ステップ 24	**match vrf** {*vrf-name* | **regexp** *regular-expression}* 例： `Router(config-control-classmap)# match vrf regexp examplename2`	（任意）加入者の VPN Routing and Forwarding（VRF）が、指定された VRF と一致する場合に true と評価される条件を作成します。

制御ポリシー マップの設定

制御ポリシー マップには、制御クラスを 1 つ以上のアクションに関連付ける 1 つ以上の制御ポリシー ルールが含まれます。制御ポリシー マップを設定するには、次の作業を実行します。

（注） ポリシー ルールで設定できるアクションは、**class type control** コマンドによって指定されたイベントのタイプに応じて異なります。たとえば、**account-logoff** が指定された場合、ポリシー ルールで設定できるアクションは **service** だけです。ここに示す手順では、ポリシー マップで設定できるすべてのアクションを示します。

デフォルト メソッドのリスト

制御ポリシー アクションのデフォルト メソッドのリストを指定する場合、デフォルトのリストは **show running-config** コマンドの出力には表示されません。たとえば、次のコマンドを設定するとします。

```
Router(config-control-policymap-class-control)# 1 authenticate aaa list default
```

show running-config コマンドの出力に次の情報が表示されます。

```
1 authenticate
```

名前付きのメソッドのリストが **show running-config** コマンドのリストに表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} [**event** {**access-reject** | **account-logoff** | **account-logon** | **acct-notification** | **credit-exhausted** | **dummy-event** | **quota-depleted** | **radius-timeout** | **service-failed** | **service-start** | **service-stop** | **session-default-service** | **session-restart** | **session-service-found** | **session-start** | **timed-policy-expiry**}]
5. *action-number* **authenticate aaa list** *list-name*
6. *action-number* **authorize use method** {**aaa** | **legacy** | **rm** | **sgf** | **ssg** | **xconnect**}[**aaa** *parameter-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id**| **dnis** | **mac-address** | **nas-port** | **remote-id** | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username | vendor-class-id**}
7. *action-number* **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username | vrf**}
8. *action-number* **if upon network-service-found** {**continue** | **stop**}
9. *action-number* **proxy accounting aaa list** {*list-name* | **default**}
10. *action-number* **service** [**disconnect** | **local** | **vpdn**]
11. *action-number* **service-policy type control** *policy-map-name*
12. *action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}}
13. *action-number* **set** *name* **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username | vrf**}
14. *action-number* **set-timer** *name-of-timer minutes*
15. *action-number* **substitute** *name matching-pattern pattern-string*
16. **end**

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 MY-POLICY`	制御ポリシーを定義するために使用される、制御ポリシー マップを作成または変更します。
ステップ 4	**class type control** {*control-class-name* | **always**} [**event** {**access-reject** | **account-logoff** | **account-logon** | **acct-notification** | **credit-exhausted** | **dummy-event** | **quota-depleted** | **radius-timeout** | **service-failed** | **service-start** | **service-stop** | **session-default-service** | **session-restart** | **session-service-found** | **session-start** | **timed-policy-expiry**}] 例： `Router(config-control-policymap)# class type control always event session-start`	アクションが設定される制御クラスを指定します。 • 制御クラスが **always** のポリシー ルールは、常に制御ポリシー マップ内でプライオリティが最も低いルールとして扱われます。
ステップ 5	*action-number* **authenticate aaa list** *list-name* 例： `Router(config-control-policymap-class-control)# 1 authenticate aaa list LIST1`	（任意）認証要求を開始します。
ステップ 6	*action-number* **authorize use method** {**aaa** | **legacy** | **rm** | **sgf** | **ssg** | **xconnect**}[**aaa** *parameter-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** | **dnis** | **mac-address** | **nas-port** | **remote-id** | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username** | **vendor-class-id**} 例： `Router(config-control-policymap-class-control)# 1 authorize identifier source-ip-address`	（任意）指定された ID に基づいて、認可の要求を開始します。

	コマンドまたはアクション	目的
ステップ 7	*action-number* **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username | vrf**} **例：** `Router(config-control-policymap-class-control)# 1 collect identifier authen-status`	（任意）アクセス プロトコルから指定された加入者 ID を収集します。
ステップ 8	*action-number* **if upon network-service-found** {**continue** | **stop**} **例：** `Router(config-control-policymap-class-control)# 2 if upon network-service-found stop`	（任意）加入者のネットワーク サービスが識別された後で、システムでポリシー ルールの処理を継続する必要があるかどうかを指定します。
ステップ 9	*action-number* **proxy accounting aaa list** {*list-name* | **default**} **例：** `Router(config-control-policymap-class-control)# 1 proxy accounting aaa list default`	（任意）要求をプロキシ化するリストを指定します。
ステップ 10	*action-number* **service** [**disconnect** | **local** | **vpdn**] **例：** `Router(config-control-policymap-class-control)# 3 service disconnect`	（任意）PPP セッションのネットワーク サービス タイプを指定します。
ステップ 11	*action-number* **service-policy type control** *policy-map-name* **例：** `Router(config-control-policymap-class-control)# service-policy type control domain based access`	（任意）指定された制御ポリシー マップを親制御ポリシー マップ内にネストします。
ステップ 12	*action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}} **例：** `Router(config-control-policymap-class-control)# 1 service-policy type service aaa list LISTA name REDIRECT`	（任意）ISG サービスをアクティブ化します。 • サービス名の代わりに ID を指定すると、指定された ID と同じ名前のサービスがアクティブ化されます。

	コマンドまたはアクション	目的
ステップ 13	*action-number* **set** *name* **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username** | **vrf**} 例： `Router(config-control-policymap-class-control)# 1 set APJ identifier authen-status`	（任意）変数名を設定します。
ステップ 14	*action-number* **set-timer** *name-of-timer minutes* 例： `Router(config-control-policymap-class-control)# 1 set-timer TIMERA 5`	（任意）名前付きのポリシー タイマーを開始します。 • タイマーの期限切れによって、イベント timed-policy-expiry が生成されます。
ステップ 15	*action-number* **substitute** *name matching-pattern pattern-string* 例： `Router(config-control-policymap-class-control)# 1 substitute TPK SUBA SUBB`	（任意）変数コンテンツ内の一致パターンを再書き込みパターンによって置換します。
ステップ 16	**end** 例： `Router(config-control-policymap-class-control)# end`	（任意）現在の設定セッションを終了し、特権 EXEC モードに戻ります。

制御ポリシー マップの適用

制御ポリシー マップは、コンテキストに適用してアクティブ化する必要があります。制御ポリシーをコンテキストに適用するには、次の 1 つ以上の作業を実行します。

- 「ルータでの制御ポリシー マップのグローバルな適用」（P.40）
- 「インターフェイスまたはサブインターフェイスへの ISG 制御ポリシー マップの適用」（P.41）
- 「仮想テンプレートへの ISG 制御ポリシー マップの適用」（P.42）
- 「ATM VC クラスへの ISG 制御ポリシー マップの適用」（P.43）
- 「ATM PVC への制御ポリシー マップの適用」（P.43）

ルータでの制御ポリシー マップのグローバルな適用

制御ポリシー をグローバルに適用するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**

3. **service-policy type control** *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	**service-policy type control** *policy-map-name* 例： `Router(config)# service-policy type control policy1`	制御ポリシーを適用します。

インターフェイスまたはサブインターフェイスへの ISG 制御ポリシー マップの適用

ISG 制御ポリシーをインターフェイスまたはサブインターフェイスに適用するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number [.subinterface number]*
4. **service-policy type control** *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。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number*[*.subinterface-number*] 例： Router(config)# interface gigabitethernet 0/1.1	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**service-policy type control** *policy-map-name* 例： Router(config-if)# service-policy type control policy1	制御ポリシーを適用します。

仮想テンプレートへの ISG 制御ポリシー マップの適用

ISG 制御ポリシー マップを仮想テンプレートに適用するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **service-policy type control** *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	**interface virtual-template** *number* 例： Router(config)# interface virtual-template0	仮想テンプレート インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**service-policy type control** *policy-map-name* 例： Router(config-if)# service-policy type control policy1	制御ポリシーを適用します。

ATM VC クラスへの ISG 制御ポリシー マップの適用

VC クラスはあらかじめ設定された VC パラメータのセットで、特定の VC または ATM インターフェイス用に設定および適用されます。ISG 制御ポリシー マップを ATM VC クラスに適用するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **service-policy type control** *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	**vc-class atm** *vc-class-name* 例： `Router(config)# vc-class atm class1`	ATM VC クラスを作成し、ATM VC クラス コンフィギュレーション モードを開始します。 • VC クラスは ATM インターフェイス、サブインターフェイス、または VC に適用できます。
ステップ 4	**service-policy type control** *policy-map-name* 例： `Router(config-vc-class)# service-policy type control policy1`	制御ポリシーを適用します。

ATM PVC への制御ポリシー マップの適用

ISG 制御ポリシーを ATM PVC に適用するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface atm** *interface-number*[**.***subinterface-number* {**mpls** | **multipoint** | **point-to-point**}]
4. **pvc** *vpi*/*vci*
5. **service-policy type control** *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	**interface atm** *interface-number*[*.subinterface-number* {**mpls** | **multipoint** | **point-to-point**}] 例： `Router(config)# interface atm 5/0.1 multipoint`	ATM インターフェイスまたはサブインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**pvc** *vpi*/*vci* 例： `Router(config-if)# pvc 2/101`	ATM PVC を作成し、ATM 仮想回線コンフィギュレーション モードを開始します。
ステップ 5	**service-policy type control** *policy-map-name* 例： `Router(config-if-atm-vc)# service-policy type control policy1`	制御ポリシーを適用します。

ISG 制御ポリシーのモニタリングとメンテナンス

任意で次の作業を実行すると、ISG 制御ポリシーの動作のモニタとメンテナンスを実行できます。手順はどの順序で実行してもかまいません。

手順の概要

1. **enable**
2. **show class-map type control**
3. **show policy-map type control**
4. **clear class-map control**
5. **clear policy-map control**

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 control** 例： `Router# show class-map type control`	ISG 制御クラス マップに関する情報を表示します。 • 特定のクラスが評価された回数と、その結果についての統計情報が表示されます。
ステップ 3	**show policy-map type control** 例： `Router# show policy-map type control`	ISG 制御ポリシー マップに関する情報を表示します。 • ポリシー マップ内の各ポリシー ルールが実行された回数についての統計情報が表示されます。
ステップ 4	**clear class-map control** 例： `Router# clear class-map control`	制御クラス マップ カウンタをクリアします。
ステップ 5	**clear policy-map control** 例： `Router# clear policy-map control`	制御ポリシー マップ カウンタをクリアします。

ISG 制御ポリシーの設定例

レイヤ 2 アクセスおよびサービス プロビジョニングの制御ポリシー：例

次に、以下の結果を生成する制御ポリシーを設定する方法の例を示します。

- VPDN 転送は、「example1.com」からダイヤルインした全員に適用されます。
- ローカルで終端されたレイヤ 3 ネットワーク リソースが、「example2.com」からダイヤルインした全員に提供されます。
- その他すべてのユーザは除外されます。

```
! Configure the control class maps.
class-map type control match-all MY-FORWARDED-USERS
 match unauthenticated-domain "example1.com"
!
class-map type control match-all MY-LOCAL-USERS
 match unauthenticated-domain "example2.com"
```

```
!
! Configure the control policy map.
policy-map type control MY-POLICY
 class type control MY-FORWARDED-USERS event session-start
  1 service-policy type service identifier nas-port
  2 service local
!
 class type control MY-LOCAL-USERS event session-start
  1 service local
!
 class type control always event session-start
  2 service disconnect
!
! Apply the control policy to dialer interface 1.
interface Dialer1
 service-policy type control MY-POLICY
```

インターフェイスおよびアクセス メディアに基づいてアクセスを制御するための制御ポリシー：例

次に、特定のインターフェイスおよびアクセス タイプからルータを開始するユーザのみにアクセスを許可する制御ポリシーを設定する方法の例を示します。この場合、PPPoE ユーザのみが許可されます。その他すべてのユーザは除外されます。

最初の条件クラス マップ「MATCHING-USERS」は、マップ内のすべての行が true と評価される場合に true と評価されます。ただし、「MATCHING-USERS」内にあるのは、ネストされたクラス マップ（2 番めの条件）の「NOT-ATM」です。このネストされたクラス マップは、サブ条件を表します。この条件も true と評価される必要があります。クラス マップ「NOT-ATM」は「match-none」を指定することに注意してください。すべての条件行が false と評価される場合にのみ、「NOT-ATM」が true と評価されます。

3 番めの条件は、この加入者に関連付けられた NAS ポートとの一致を指定します。特に、イーサネット インターフェイスおよびスロット 3 に到達した加入者のみが true と評価されます。

```
! Configure the control class maps.
class-map type control match-all MATCHING-USERS
 class type control NOT-ATM
 match media ether
 match nas-port type ether slot 3
!
class-map type control match-none NOT-ATM
 match media atm
!
```

クラス マップ「MATCHING-USERS」内の条件が true と評価された場合、実行する最初のアクションはユーザの認証です。認証に成功した場合、「service1」という名前のサービスがダウンロードされ、適用されます。最後に、レイヤ 3 サービスが提供されます。

「MATCHING-USERS」が true と評価されなかった場合、「always」クラスが適用され、その結果「MATCHING-USERS」と一致しないユーザが除外されます。

```
! Configure the control policy map.
policy-map type control my-pppoe-rule
 class type control MATCHING-USERS event session-start
  1 authenticate aaa list XYZ
  2 service-policy type service service1
  3 service local
!
 class type control always
```

```
  1 service disconnect
!
! Apply the control policy to an interface.
interface ethernet3/0
 service-policy type control my-pppoe-rule
```

最後に、このポリシーはインターフェイスに関連付けられます。

ISG プリペイド課金サポートのための制御ポリシー：例

次に、credit-exhausted イベントの発生時に、加入者パケットをサーバ グループ「redirect-sg」にリダイレクトするように制御ポリシーを設定する例を示します。

```
service-policy type control RULEA
!
policy-map type control RULEA
 class type control always event credit-exhausted
  1 service-policy type service redirectprofile
!
policy-map type service redirectprofile
 class type traffic CLASS-ALL
  redirect to group redirect-sg

policy-map type service mp3
 class type traffic CLASS-ACL-101
  authentication method-list cp-mlist
  accounting method-list cp-mlist
  prepaid conf-prepaid

subscriber feature prepaid conf-prepaid
 threshold time 20
 threshold volume 0
 method-list accounting ap-mlist
 method-list authorization default
 password cisco
```

自動加入者ログインのための制御ポリシー：例

次の例では、クライアントがサブネットからログインする場合、自動加入者ログインが適用され、ユーザ名としての加入者の送信元 IP アドレスとともに認可要求が、リスト TAL LIST に送信されます。認可要求に成功した場合、返されユーザ プロファイルで指定された自動アクティブ化サービスがセッションに対してアクティブ化され、制御ポリシー内のルールの実行が停止します。認可に成功しなかった場合、ルールの実行が続行し、加入者がポリシー サーバにリダイレクトされ、ログインします。加入者が 5 分以内にログインしなかった場合、セッションが切断されます。

```
interface Ethernet0/0
 service-policy type control RULEA

aaa authentication login TAL LIST group radius
aaa authentication login LOCAL local
access-list 100 permit ip any any

class-map type traffic match-any all-traffic
 match access-group input 100
 match access-group output 100

policy-map type service redirectprofile
 class type traffic all-traffic
```

```
  redirect to ip 10.0.0.148 port 8080

class-map type control match-all CONDA
 match source-ip-address 209.165.201.1 255.255.255.0
!
class-map type control match-all CONDF
 match timer TIMERB
 match authen-status unauthenticated

policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier source-ip-address
  2 apply aaa list LOCAL service redirectprofile
  3 set-timer TIMERB 5 minutes
 class type control CONDF event timed-policy-expiry
  1 service disconnect
```

その他の参考資料

関連資料

内容	参照先
ISG コマンド	『*Cisco IOS Intelligent Services Gateway Command Reference*』
トラフィック ポリシー	『Configuring ISG Subscriber Services』

規格

規格	タイトル
この機能によって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
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS 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 制御ポリシーの機能情報

表 3 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 3 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 3　ISG 制御ポリシーの機能情報

機能名	リリース	機能設定情報
ISG：ポリシー制御：ポリシー：ドメインベース（自動ドメイン、プロキシ）	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG 制御ポリシーは、特定の契約を履行するために使用されるプライマリ サービスおよびルールを管理します。このようなポリシーには、ポリシー条件を満たしたときにセッション内のフローに適用されるダイナミック トリガーおよび条件付きロジックへのプログラム可能なインターフェイス、セッションのその他の特性が含まれます。ポリシーはドメイン名に関連付けられたサービスをアクティブ化するための要求としてドメインを解釈するように設定でき、ユーザは接続を試行しているドメイン名と一致するサービスを自動的に受けることができます。 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 制御ポリシーに関する情報」（P.30） • 「ISG 制御ポリシーの設定方法」（P.32） 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。
ISG：ポリシー制御：ポリシー：トリガー	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG 制御ポリシーは、時間ベース、ボリュームベース、期間ベースのポリシー トリガーと組み合わせて設定できます。時間ベースのトリガーでは、内部クロックを使用して、特定の時刻にポリシーを適用できます。ボリュームベースのトリガーはパケット数に基づきます。パケット数が指定された値に達したときに、指定されたポリシーが適用されます。期間ベースのトリガーは内部タイマーに基づきます。タイマーが期限切れになると、指定されたポリシーが適用されます。 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。 • 「ISG 制御ポリシーに関する情報」（P.30） • 「ISG 制御ポリシーの設定方法」（P.32） 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。

表 3　ISG 制御ポリシーの機能情報 （続き）

機能名	リリース	機能設定情報
ISG：ポリシー制御：セッション単位の多次元 ID	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG 制御ポリシーでは、セッションの確立中に加入者の識別情報を収集するための柔軟な方法が提供されます。また、制御ポリシーでは、識別情報のより多くの要素がシステムで利用可能になると、セッション ポリシーを繰り返し適用できます。 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 制御ポリシーに関する情報」（P.30） • 「ISG 制御ポリシーの設定方法」（P.32） 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。
ISG：ポリシー制御：Cisco ポリシー言語	12.2(28)SB 12.2(33)SRC	ISG 制御ポリシーは機能に固有のコンフィギュレーション コマンド用の構造化された代替手段であり、設定可能な機能をイベント、条件、アクションとして表現できます。制御ポリシーでは、システムの動作を指定するための整合性のとれた CLI コマンドのセットとともに、直感的で拡張可能なフレームワークが提供されます。 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。 • 「ISG 制御ポリシーに関する情報」（P.30） • 「ISG 制御ポリシーの設定方法」（P.32） 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。
ISG：ポリシー制御：差別化された初期ポリシー制御	12.2(33)SRE 12.2(33)XNE	この機能では、RADIUS 認証の拒否と、RADIUS サーバの利用不能とを区別する機能が提供されます。これによって、RADIUS サーバがダウンしているか、またはネットワークの問題のためにアクセスできない場合、あるいは加入者に対する認証の拒否が受信された場合、加入者に対して最小のアクセス権または一時的なネットワーク アクセス権が付与されます。 Cisco IOS Release 12.2(33)XNE では、Cisco 10000 シリーズ ルータのサポートが追加されました。 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。 • 「ISG 制御ポリシーに関する情報」（P.30） • 「ISG 制御ポリシーの設定方法」（P.32） 次のコマンドが導入または変更されました。 **class type control**

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。