Intelligent Services Gateway コンフィギュレーション ガイド、Cisco IOS Release 15.1S

Intelligent Services Gateway Configuration Guide, Cisco IOS Release 15.1S

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Intelligent Services Gateway（ISG）機能のロードマップ

この機能ロードマップでは、『*Cisco IOS Intelligent Services Gateway コンフィギュレーション ガイド*』に記載されている Cisco IOS の機能と、各機能が記載されている資料を示します。ロードマップは、お使いのリリースで使用できる機能を参照できるように編成されています。お探しの機能名を検索し、「参照先」列に記載された URL をクリックして、その機能の説明を含むマニュアルにアクセスしてください。

機能とリリース サポート

表 1 に、次の Cisco IOS ソフトウェア リリース群の ISG 機能のサポートを示します。

- 「Cisco IOS Release 15.0S」
- 「Cisco IOS Release 12.2SR」
- 「Cisco IOS Release 12.2SB」

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 1 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 1 に、各ソフトウェアの最新リリースの一覧を示します。また、対象のリリースで使用可能な機能をアルファベット順に紹介します。

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能

リリース	機能名	機能の説明	参照先
Cisco IOS Release 15.0S			
15.0(1)S	DHCP サーバ ユーザ認証	この機能は、DHCP クライアントを認証するために使用します。	『Configuring ISG Access for IP Subscriber Sessions』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
15.0(1)S	ISG：アカウンティング：セッション単位、サービス単位、およびフロー単位	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。	『Configuring ISG Accounting』
15.0(1)S	ISG：認証：DHCP オプション 82 ライン ID：AAA 認証サポート	この機能は、回線 ID およびリモート ID に基づいて認可に対するサポートを提供することにより、ISG 自動加入者ログインの機能を拡張します。	『Configuring ISG Policies for Automatic Subscriber Logon』
15.0(1)S	ISG：フロー制御：フロー リダイレクト	サービス プロバイダーが ISG レイヤ 4 リダイレクト機能を使用すると、加入者 TCP または UDP パケットを適切な処理のために指定されたサーバにリダイレクトできるようにすることによって、ユーザ環境が向上します。ISG レイヤ 4 リダイレクトは、個々の加入者セッションまたはフローに適用できます。	『Redirecting Subscriber Traffic Using ISG Layer 4 Redirect』
15.0(1)S	ISG：フロー制御：QoS 制御：IP セッションのための MQC サポート	Cisco ISG IP セッションで Modular QoS CLI（MQC）プロビジョニングを提供します。	『Configuring MQC Support for IP Sessions』
15.0(1)S	ISG：装置：セッションとフローのモニタリング（ローカルおよび外部）	ISG には、インターフェイス統計情報と CPU 統計情報を連続的にモニタするためのメカニズムが用意されています。この機能により、指定された間隔で更新される統計情報を表示する **show interface monitor** コマンドと **show processes cpu monitor** コマンドが導入されます。	『Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging』
15.0(1)S	ISG：ネットワーク インターフェイス：IP ルーテッド、VRF Aware MPLS	ISG は、加入者セッションをネットワークに接続するために複数の種類の転送をサポートしています。このような接続には、インターネット、社内のイントラネット、ISP、またはコンテンツ配信のためのウォールド ガーデンなどがあります。ISG では、ネットワーク アクセスのためにルーテッド インターフェイスおよび MPLS 対応のインターフェイスの両方がサポートされます。	『Configuring ISG Network Forwarding Policies』
15.0(1)S	ISG：ポリシー制御：DHCP ポリシー	この機能によって、ISG は DHCP と動的に相互動作し、DHCP 加入者に割り当てる IP アドレスに影響を及ぼすポリシーを適用できます。	『Configuring ISG Access for IP Subscriber Sessions』
15.0(1)S	ISG：ポリシー制御：ISG-SCE 制御バス	この機能によって、コントロール パネル レベルで ISG デバイスと SCE デバイスを統合し、加入者セッションにポリシーを適用するときに、この 2 つのデバイスが 1 つのデバイスとして動作できます。	『Configuring ISG Integration with SCE』
15.0(1)S	ISG：ポリシー制御：セッション単位の多次元 ID	ISG 制御ポリシーでは、セッションの確立中に加入者 ID 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、ID 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。	『Configuring ISG Control Policies』
15.0(1)S	ISG：ポリシー制御：ポリシー サーバ：CoA	この機能によって、動的認可を容易にする RADIUS Change of Authorization（CoA）拡張を ISG がサポートします。	『Enabling ISG to Interact with External Policy Servers』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
15.0(1)S	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）	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。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。	『Configuring ISG Control Policies』
15.0(1)S	ISG：ポリシー制御：ポリシー：トリガー（時間、ボリューム、期間）	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。	『Configuring ISG Control Policies』
15.0(1)S	ISG：ポリシー制御：サービス プロファイル	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。	『Configuring ISG Subscriber Services』
15.0(1)S	ISG：ポリシー制御：ユーザ プロファイル	ISG ユーザ プロファイルは、指定された加入者の ISG セッションに適用すべき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。	『Configuring ISG Subscriber Services』
15.0(1)S	ISG：セッション：認証	ISG 自動加入者ログインでは、認可要求でユーザ名の代わりに、指定された別の ID を使用できます。AAA サーバが、指定された ID に基づいて加入者を許可できることにより、加入者からパケットを受け取るとすぐに、AAA サーバから加入者のプロファイルをダウンロードできるようになります。	『Configuring ISG Policies for Automatic Subscriber Logon』
15.0(1)S	ISG：セッション：認証：シングル サインオン	シングル サインオンを使用すると、加入者がアクセス プロバイダーまたはサービス プロバイダーの管理ドメイン内の他のデバイスによって提供されるサービスにアクセスできる場合、セッションを複数回認証する必要がなくなります。	『Overview of ISG』
15.0(1)S	ISG：セッション：Auth：PBHK	この機能は、外部ポータルでのセッション識別のためにインバンド シグナリング メカニズムを提供します。加入者からの TCP パケットは、ISG ゲートウェイのローカル IP アドレスと一定範囲のポートにマッピングされます。このマッピングにより、ポータルはセッションが開始された ISG ゲートウェイを識別できるようになります。	『Configuring ISG Port-Bundle Host Key』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
15.0(1)S	ISG：セッション：作成：インターフェイス IP セッション：L2	ISG IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成されます。	『Configuring ISG Access for IP Subscriber Sessions』
15.0(1)S	ISG：セッション：作成：インターフェイス IP セッション：L3	ISG IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成されます。	『Configuring ISG Access for IP Subscriber Sessions』
15.0(1)S	ISG：セッション：作成：IP セッション：サブネットおよび発信元 IP：L2	ISG セッションは、特定のデータ フロー間でサービスとポリシーを関連付けるために使用される主要なコンポーネントです。IP サブネット セッションとは、単一の IP サブネットからの IP トラフィックを含む ISG セッションです。発信元 IP セッションには、単一の発信元 IP アドレスからのトラフィックが含まれます。	『Configuring ISG Access for IP Subscriber Sessions』
15.0(1)S	ISG：セッション：作成：IP セッション：プロトコル イベント（DHCP）	ほとんどの ISG セッションは、すでにアクティブなセッションに関連付けられないデータ フローの検出時に作成されます。ISG は、加入者から最初の DHCP DISCOVER パケットを受信したときに、IP セッションを作成するように設定できます。	『Configuring ISG Access for IP Subscriber Sessions』
15.0(1)S	ISG：セッション：作成：IP セッション：サブネットおよび発信元 IP：L3	ISG セッションは、特定のデータ フロー間でサービスとポリシーを関連付けるために使用される主要なコンポーネントです。IP サブネット セッションとは、単一の IP サブネットからの IP トラフィックを含む ISG セッションです。発信元 IP セッションには、単一の発信元 IP アドレスからのトラフィックが含まれます。	『Configuring ISG Access for IP Subscriber Sessions』
15.0(1)S	ISG：セッション：ライフサイクル：アイドル タイムアウト	ISG アイドル タイムアウトは、接続をを終了するまでに、その接続をアイドルにしておく時間を制御します。	『Configuring ISG Policies for Session Maintenance』
15.0(1)S	ISG：セッション：ライフサイクル：POD	ISG は、外部ポリシー サーバと相互動作するように設定できます。ポリシー サーバは、RADIUS Packet of Disconnect（POD; パケット オブ ディスコネクト）を使用して、ISG セッションのライフサイクルを管理できます。POD メッセージの主な役割は、ISG セッションを終了することです。	『Enabling ISG to Interact with External Policy Servers』
15.0(1)S	ISG：セッション：保護および復元力：キープアライブ：ARP、ICMP	この機能は、モニタする接続のタイプによって、ARP または ICMP を使用してキープアライブ メッセージを設定することにより、IP 加入者セッションのヘルス モニタを実行できます。	『Configuring ISG Policies for Session Maintenance』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
15.0(1)S	ISG：セッション：VRF 転送	ISG セッションは、特定のデータ フローでサービスとポリシーを関連付けるために使用される主要なコンポーネントです。ネットワーク サービスのためにルーティングが必要な場合、ISG セッションは、Virtual Routing and Forwarding（VRF）インスタンスに関連付けられます。ISG VRF 転送は、仮想ルーティング ドメイン間でアクティブ セッションを動的に切り替える手段を提供します。	『Configuring ISG Access for IP Subscriber Sessions』
15.0(1)S	ISG: Subscriber Aware Ethernet	SIP-400 または Ethernet Services Plus（ES+）アクセス側ラインカードを持つ Cisco 7600 シリーズ ルータ上に分散する IP および PPPoE セッションに、ISG 機能を提供します。	『ISG: Subscriber Aware Ethernet』
Cisco IOS Release 12.2SR			
12.2(33)SRE2	ISG：トリプルキー認証サポート	この機能によって、アクセス要求メッセージで SESM から RADIUS サーバにロケーション情報を渡すことにより、トリプルキー認証が可能になります。	『Enabling ISG to Interact with External Policy Servers』
12.2(33)SRE	DHCP サーバ ユーザ認証	この機能は、DHCP クライアントを認証するために使用します。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(33)SRE	ISG：AAA ワイヤレス拡張機能	RADIUS プロキシ拡張は、モバイル ワイヤレス環境に対して追加のサポートを提供します。この機能には、RADIUS アトリビュート 31 の処理に関する変更が含まれています。	『Configuring ISG as a RADIUS Proxy』
12.2(33)SRE	ISG：認証：RADIUS プロキシ WiMax 拡張機能	RADIUS プロキシ拡張は、WiMax ブロードバンド環境に対して追加のサポートを提供します。	『Configuring ISG as a RADIUS Proxy』
12.2(33)SRE	ISG：装置：DHCP リース クエリー サポート	DHCP リース クエリー トランザクションとは、特殊なメッセージ タイプがある DHCP トランザクションです。これにより、クライアントは、IP アドレスの所有者とリース有効期間に関して DHCP サーバに問い合わせることなどができます。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(33)SRE	ISG：ポリシー制御：差別化された初期ポリシー制御	この機能は、RADIUS サーバがダウンしている場合、またはネットワークの問題のために RADIUS サーバにアクセスできない場合に、加入者に対して最小限または一時的なネットワーク アクセスを提供します。	『Configuring ISG Control Policies』
12.2(33)SRE	ISG：セッション：マルチキャスト：共存	この機能は、同じサブインターフェイスでマルチキャスト セッションと IP セッションが共存できるようにして、同じ VLAN 上ですべての加入者とサービス（データとマルチキャスト）をホストする機能を導入します。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(33)SRE	ISG：スタティック セッションの作成	この機能によって、管理者が開始したスタティック IP セッションが可能になります。	『Configuring ISG Access for IP Subscriber Sessions』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SRD	ISG：認証：DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon	この機能によってサービス プロバイダーは、DHCP オプション 60 およびオプション 82 によって TAL をサポートでき、オプション 82 への VPN-ID 拡張によってホールセール型の IP セッションをサポートできます。	『Configuring DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon』
12.2(33)SRC	IP 加入者セッションの CLI アップデート	ISG IP 加入者セッションを設定するために使用するコマンドの一部は、このリリースで変更され、または置き換えられました。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(33)SRC	ISG：アカウンティング：セッション単位、サービス単位、およびフロー単位	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。	『Configuring ISG Accounting』
12.2(33)SRC	ISG：アカウンティング：ポストペイド	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 は、ポストペイド課金用のアカウンティング サーバに、セッションとサービスに対するアカウンティングの開始レコードと終了レコードを送信します。アカウンティング サーバは、レコードを解釈して、課金情報を生成します。	『Configuring ISG Accounting』
12.2(33)SRC	ISG：アカウンティング：料金切り替え	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。課金料率が一定の時間に変更され、料率変更の境界を超えてセッションがアクティブだった場合、ISG は課金サーバにアカウンティング データを提供し、境界であることを示します。料金切り替えは、プリペイド課金からポスト ペイド課金への切り替えなど、アカウンティング方式間で使用することもできます。	『Configuring ISG Accounting』 『Configuring ISG Support for Prepaid Billing』
12.2(33)SRC	ISG：アカウンティング：時間ベースのプリペイド	ISG プリペイド課金サポートによって、ISG は加入者の利用可能なクレジットを調べ、その加入者にサービスへのアクセスを許可するかどうか、およびアクセスの継続可能期間を判別できます。ISG は時間ベースのプリペイド課金をサポートします。	『Configuring ISG Support for Prepaid Billing』
12.2(33)SRC	ISG：アカウンティング：ボリューム ベースのプリペイド	ISG プリペイド課金サポートによって、ISG は加入者の利用可能なクレジットを調べ、その加入者にサービスへのアクセスを許可するかどうか、およびアクセスの継続可能期間を判別できます。ISG はボリューム ベースのプリペイド課金をサポートします。	『Configuring ISG Support for Prepaid Billing』
12.2(33)SRC	ISG：認証：DHCP オプション 82 ライン ID：AAA 認証サポート	この機能は、回線 ID およびリモート ID に基づいて認可に対するサポートを提供することにより、ISG 自動加入者ログインの機能を拡張します。	『Configuring ISG Policies for Automatic Subscriber Logon』
12.2(33)SRC	ISG：フロー制御：フロー リダイレクト	サービス プロバイダーが ISG レイヤ 4 リダイレクト機能を使用すると、加入者 TCP または UDP パケットを適切な処理のために指定されたサーバにリダイレクトできるようにすることによって、ユーザ環境が向上します。ISG レイヤ 4 リダイレクトは、個々の加入者セッションまたはフローに適用できます。	『Redirecting Subscriber Traffic Using ISG Layer 4 Redirect』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SRC	ISG：フロー制御：QoS 制御：動的レート制限	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。	『Configuring ISG Network Forwarding Policies』
12.2(33)SRC	ISG：フロー制御：QoS 制御：IP セッションのための MQC サポート	Cisco ISG IP セッションで Modular QoS CLI（MQC）プロビジョニングを提供します。	『Configuring MQC Support for IP Sessions』
12.2(33)SRC	ISG：装置：拡張条件付きデバッグ	ISG には、デバッグ出力のフィルタリング用に各種の条件を定義する機能が用意されています。条件付きデバッグでは、セッション、フロー、加入者、およびサービスの診断に使用できる非常に具体的な関連情報が生成されます。	『Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging』
12.2(33)SRC	ISG：装置：セッションとフローのモニタ	ISG には、インターフェイス統計情報と CPU 統計情報を連続的にモニタするためのメカニズムが用意されています。この機能により、指定された間隔で更新される統計情報を表示する **show interface monitor** コマンドと **show processes cpu monitor** コマンドが導入されます。	『Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging』
12.2(33)SRC	ISG：ネットワーク インターフェイス：IP ルーテッド、VRF-Aware MPLS	ISG は、加入者セッションをネットワークに接続するために複数の種類の転送をサポートしています。このような接続には、インターネット、社内のイントラネット、ISP、またはコンテンツ配信のためのウォールド ガーデンなどがあります。ISG では、ネットワークアクセスのためにルーテッド インターフェイスおよび MPLS 対応のインターフェイスの両方がサポートされます。	『Configuring ISG Network Forwarding Policies』
12.2(33)SRC	ISG：ネットワーク インターフェイス：トンネリング（L2TP）	ISG は、加入者セッションをネットワークに接続するために複数の種類の転送をサポートしています。このような接続には、インターネット、社内のイントラネット、ISP、またはコンテンツ配信のためのウォールド ガーデンなどがあります。ISG では、ネットワークへのトンネル インターフェイスがサポートされます。	『Configuring ISG Network Forwarding Policies』
12.2(33)SRC	ISG：ポリシー制御：Cisco ポリシー言語	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。ISG ポリシー言語は、Cisco Common Classification Policy Language（C3PL）に準拠しています。	『Configuring ISG Control Policies』
12.2(33)SRC	ISG：ポリシー制御：DHCP ポリシー	この機能によって、ISG は DHCP と動的に相互動作し、DHCP 加入者に割り当てる IP アドレスに影響を及ぼすポリシーを適用できます。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(33)SRC	ISG：ポリシー制御：ISG-SCE 制御バス	この機能によって、コントロール パネル レベルで ISG デバイスと SCE デバイスを統合し、加入者セッションにポリシーを適用するときに、この 2 つのデバイスが 1 つのデバイスとして動作できます。	『Configuring ISG Integration with SCE』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SRC	ISG：ポリシー制御：セッション単位の多次元 ID	ISG 制御ポリシーでは、セッションの確立中に加入者 ID 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、ID 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。	『Configuring ISG Control Policies』
12.2(33)SRC	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）	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。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。	『Configuring ISG Control Policies』
12.2(33)SRC	ISG：ポリシー制御：ポリシー：トリガー	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。	『Configuring ISG Control Policies』
12.2(33)SRC	ISG：ポリシー制御：ポリシー サーバ：CoA	この機能によって、動的認可を容易にする RADIUS Change of Authorization（CoA）拡張を ISG がサポートします。	『Enabling ISG to Interact with External Policy Servers』
12.2(33)SRC	ISG：ポリシー制御：ポリシー サーバ：CoA ASCII コマンド コード サポート	この機能によって、ISG は、Account Logon、Account Logoff、Service Logon、Service Logoff、および Account Status クエリーに対する ASCII コマンド コードを受信し、コマンド コードに基づいて、要求された機能を実行できます。	『*Cisco IOS ISG RADIUS Interface Guide*』
12.2(33)SRC	ISG：ポリシー制御：ポリシー サーバ：SSG-SESM プロトコル	ISG は、SESM ポリシー サーバとの通信にシスコ独自のプロトコルをサポートしています。	『*Cisco SSG-to-ISG DSL Broadband Migration Guide*』
12.2(33)SRC	ISG：ポリシー制御：RADIUS ポリシー拡張	ISG RADIUS プロキシ機能により、ISG は、RADIUS 認証を使用するクライアント デバイスと、AAA サーバの間のプロキシとして機能できるようになります。ISG RADIUS プロキシ機能によって、ISG は RADIUS のパケット フローを「詮索」（観察）できるようになり、認証が成功すると、対応する ISG セッションを透過的に作成できます。	『Configuring ISG as a RADIUS Proxy』
12.2(33)SRC	ISG：ポリシー制御：サービス プロファイル	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。	『Configuring ISG Subscriber Services』
12.2(33)SRC	ISG：ポリシー制御：ユーザ プロファイル	ISG ユーザ プロファイルは、指定された加入者の ISG セッションに適用すべき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。	『Configuring ISG Subscriber Services』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SRC	ISG：セッション：Auth：PBHK	ISG Port-Bundle Host Key 機能は、外部ポータルにおいて、セッションを識別するためのインバンド シグナリング メカニズムとして機能します。加入者からの TCP パケットは、ISG ゲートウェイのローカル IP アドレスと一定範囲のポートにマッピングされます。このマッピングにより、ポータルはセッションが開始された ISG ゲートウェイを識別できるようになります。	『Configuring ISG Port-Bundle Host Key』
12.2(33)SRC	ISG：セッション：認証：シングル サインオン	シングル サインオンを使用すると、加入者がアクセス プロバイダーまたはサービス プロバイダーの管理ドメイン内の他のデバイスによって提供されるサービスにアクセスできる場合、セッションを複数回認証する必要がなくなります。	『Overview of ISG』
12.2(33)SRC	ISG：セッション：認証	ISG 自動加入者ログインでは、認可要求でユーザ名の代わりに、指定された別の ID を使用できます。AAA サーバが、指定された ID に基づいて加入者を許可できることにより、加入者からパケットを受け取るとすぐに、AAA サーバから加入者のプロファイルをダウンロードできるようになります。	『Configuring ISG Policies for Automatic Subscriber Logon』
12.2(33)SRC	ISG：セッション：作成：インターフェイス IP セッション：L2	ISG IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成されます。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(33)SRC	ISG：セッション：作成：インターフェイス IP セッション：L3	ISG IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成されます。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(33)SRC	ISG：セッション：作成：IP セッション：プロトコル イベント（DHCP）	ほとんどの ISG セッションは、すでにアクティブなセッションに関連付けられないデータ フローの検出時に作成されます。ISG は、加入者から最初の DHCP DISCOVER パケットを受信したときに、IP セッションを作成するように設定できます。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(33)SRC	ISG：セッション：作成：IP セッション：サブネットおよび発信元 IP：L2	ISG セッションは、特定のデータ フロー間でサービスとポリシーを関連付けるために使用される主要なコンポーネントです。IP サブネット セッションとは、単一の IP サブネットからの IP トラフィックを含む ISG セッションです。発信元 IP セッションには、単一の発信元 IP アドレスからのトラフィックが含まれます。	『Configuring ISG Access for IP Subscriber Sessions』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SRC	ISG：セッション：作成：IP セッション：サブネットおよび発信元 IP：L3	ISG セッションは、特定のデータ フロー間でサービスとポリシーを関連付けるために使用される主要なコンポーネントです。IP サブネット セッションとは、単一の IP サブネットからの IP トラフィックを含む ISG セッションです。発信元 IP セッションには、単一の発信元 IP アドレスからのトラフィックが含まれます。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(33)SRC	ISG：セッション：作成：P2P セッション（PPPoE、PPPoXoX）	ISG セッションとは、特定のデータ フロー間でサービスとポリシーが関連付けられる主要なコンテキストです。Point-to-Point（P2P; ポイントツーポイント）セッションは、シグナリング プロトコルを通じて確立されます。ISG は、PPP、PPPoE、および PPPoA など各種の P2P カプセル化を処理します。	『Configuring ISG Access for PPP Sessions』
12.2(33)SRC	ISG：セッション：ライフサイクル：アイドル タイムアウト	ISG アイドル タイムアウトは、接続をを終了するまでに、その接続をアイドルにしておく時間を制御します。	『Configuring ISG Policies for Session Maintenance』
12.2(33)SRC	ISG：セッション：ライフサイクル：Packet of Disconnect（POD）	ISG は、外部ポリシー サーバと相互動作するように設定できます。ポリシー サーバは、RADIUS Packet of Disconnect（POD; パケット オブ ディスコネクト）を使用して、ISG セッションのライフサイクルを管理できます。POD メッセージの主な役割は、ISG セッションを終了することです。	『Enabling ISG to Interact with External Policy Servers』
12.2(33)SRC	ISG：セッション：VRF 転送	ISG セッションは、特定のデータ フローでサービスとポリシーを関連付けるために使用される主要なコンポーネントです。ネットワーク サービスのためにルーティングが必要な場合、ISG セッションは、Virtual Routing and Forwarding（VRF）インスタンスに関連付けられます。ISG VRF 転送は、仮想ルーティング ドメイン間でアクティブ セッションを動的に切り替える手段を提供します。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(33)SRC	ISG：セッション保護および復元力：キープアライブ：ARP、ICMP	この機能は、モニタする接続のタイプによって、ARP または ICMP を使用してキープアライブ メッセージを設定することにより、IP 加入者セッションのヘルス モニタを実行できます。	『Configuring ISG Policies for Session Maintenance』
12.2(33)SRC	ISG: Subscriber Aware Ethernet	この機能によって、Cisco 7600 ルータで ISG 機能を利用できるようになります。 次の ISG アカウンティング機能は、Cisco 7600 ルータでサポートされていません。 • サービス単位 • フロー単位 • ポストペイド • 料金切り替え • 時間ベースまたはボリューム ベースのプリペイド	『ISG: Subscriber Aware Ethernet』
12.2(33)SRC	Service Gateway Interface	SGI は、ポリシー、加入者、およびセッションに対する ISG の管理機能にアクセスするための Web サービス インターフェイスを実装するものです。	『Service Gateway Interface』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
Cisco IOS Release 12.2SB			
12.2(31)SB2	ISG：ポリシー制御：ポリシー サーバ：CoA ASCII コマンド コード サポート	この機能によって、ISG は、Account Logon、Account Logoff、Service Logon、Service Logoff、および Account Status クエリーに対する ASCII コマンド コードを受信し、コマンド コードに基づいて、要求された機能を実行できます。	『*Cisco IOS ISG RADIUS Interface Guide*』
12.2(31)SB2	ISG：ポリシー制御：RADIUS ポリシー拡張	ISG RADIUS プロキシ機能により、ISG は、RADIUS 認証を使用するクライアント デバイスと、AAA サーバの間のプロキシとして機能できるようになります。ISG RADIUS プロキシ機能によって、ISG は RADIUS のパケット フローを「詮索」（観察）できるようになり、認証が成功すると、対応する ISG セッションを透過的に作成できます。	『Configuring ISG as a RADIUS Proxy』
12.2(31)SB2	IP 加入者セッションの CLI アップデート	ISG IP 加入者セッションを設定するために使用するコマンドの一部は、このリリースで変更され、または置き換えられました。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(28)SB	ISG：アカウンティング：セッション単位、サービス単位、およびフロー単位	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。	『Configuring ISG Accounting』
12.2(28)SB	ISG：アカウンティング：ポストペイド	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 は、ポストペイド課金用のアカウンティング サーバに、セッションとサービスに対するアカウンティングの開始レコードと終了レコードを送信します。アカウンティング サーバは、レコードを解釈して、課金情報を生成します。	『Configuring ISG Accounting』
12.2(28)SB	ISG：アカウンティング：料金切り替え	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。課金料率が一定の時間に変更され、料率変更の境界を超えてセッションがアクティブだった場合、ISG は課金サーバにアカウンティング データを提供し、境界であることを示します。料金切り替えは、プリペイド課金からポスト ペイド課金への切り替えなど、アカウンティング方式間で使用することもできます。	『Configuring ISG Accounting』 『Configuring ISG Support for Prepaid Billing』
12.2(28)SB	ISG：アカウンティング：時間ベースのプリペイド	ISG プリペイド課金サポートによって、ISG は加入者の利用可能なクレジットを調べ、その加入者にサービスへのアクセスを許可するかどうか、およびアクセスの継続可能期間を判別できます。ISG は時間ベースのプリペイド課金をサポートします。	『Configuring ISG Support for Prepaid Billing』
12.2(28)SB	ISG：アカウンティング：ボリューム ベースのプリペイド	ISG プリペイド課金サポートによって、ISG は加入者の利用可能なクレジットを調べ、その加入者にサービスへのアクセスを許可するかどうか、およびアクセスの継続可能期間を判別できます。ISG はボリューム ベースのプリペイド課金をサポートします。	『Configuring ISG Support for Prepaid Billing』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(28)SB	ISG：認証：DHCP オプション 82 ライン ID：AAA 認証サポート	この機能は、回線 ID およびリモート ID に基づいて認可に対するサポートを提供することにより、ISG 自動加入者ログインの機能を拡張します。	『Configuring ISG Policies for Automatic Subscriber Logon』
12.2(28)SB	ISG：フロー制御：フロー リダイレクト	サービス プロバイダーが ISG レイヤ 4 リダイレクト機能を使用すると、加入者 TCP または UDP パケットを適切な処理のために指定されたサーバにリダイレクトできるようにすることによって、ユーザ環境が向上します。ISG レイヤ 4 リダイレクトは、個々の加入者セッションまたはフローに適用できます。	『Redirecting Subscriber Traffic Using ISG Layer 4 Redirect』
12.2(28)SB	ISG：フロー制御：QoS 制御：動的レート制限	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。	『Configuring ISG Network Forwarding Policies』
12.2(28)SB	ISG：装置：拡張条件付きデバッグ	ISG には、デバッグ出力のフィルタリング用に各種の条件を定義する機能が用意されています。条件付きデバッグでは、セッション、フロー、加入者、およびサービスの診断に使用できる非常に具体的な関連情報が生成されます。	『Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging』
12.2(28)SB	ISG：装置：セッションとフローのモニタ	ISG には、インターフェイス統計情報と CPU 統計情報を連続的にモニタするためのメカニズムが用意されています。この機能により、指定された間隔で更新される統計情報を表示する **show interface monitor** コマンドと **show processes cpu monitor** コマンドが導入されます。	『Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging』
12.2(28)SB	ISG：ネットワーク インターフェイス：IP ルーテッド、VRF-Aware MPLS	ISG は、加入者セッションをネットワークに接続するために複数の種類の転送をサポートしています。このような接続には、インターネット、社内のイントラネット、ISP、またはコンテンツ配信のためのウォールド ガーデンなどがあります。ISG では、ネットワーク アクセスのためにルーテッド インターフェイスおよび MPLS 対応のインターフェイスの両方がサポートされます。	『Configuring ISG Network Forwarding Policies』
12.2(28)SB	ISG：ネットワーク インターフェイス：トンネリング（L2TP）	ISG は、加入者セッションをネットワークに接続するために複数の種類の転送をサポートしています。このような接続には、インターネット、社内のイントラネット、ISP、またはコンテンツ配信のためのウォールド ガーデンなどがあります。ISG では、ネットワークへのトンネル インターフェイスがサポートされます。	『Configuring ISG Network Forwarding Policies』
12.2(28)SB	ISG：ポリシー制御：Cisco ポリシー言語	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。ISG ポリシー言語は、Cisco Common Classification Policy Language（C3PL）に準拠しています。	『Configuring ISG Control Policies』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(28)SB	ISG：ポリシー制御：DHCP ポリシー	この機能によって、ISG は DHCP と動的に相互動作し、DHCP 加入者に割り当てる IP アドレスに影響を及ぼすポリシーを適用できます。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(28)SB	ISG：ポリシー制御：セッション単位の多次元 ID	ISG 制御ポリシーでは、セッションの確立中に加入者 ID 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、ID 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。	『Configuring ISG Control Policies』
12.2(28)SB	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）	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。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。	『Configuring ISG Control Policies』
12.2(28)SB	ISG：ポリシー制御：ポリシー：トリガー	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。	『Configuring ISG Control Policies』
12.2(28)SB	ISG：ポリシー制御：ポリシー サーバ：CoA	この機能によって、動的認可を容易にする RADIUS Change of Authorization（CoA）拡張を ISG がサポートします。	『Enabling ISG to Interact with External Policy Servers』
12.2(28)SB	ISG：ポリシー制御：ポリシー サーバ：SSG-SESM プロトコル	ISG は、SESM ポリシー サーバとの通信にシスコ独自のプロトコルをサポートしています。	『*Cisco SSG-to-ISG DSL Broadband Migration Guide*』
12.2(28)SB	ISG：ポリシー制御：サービス プロファイル	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。	『Configuring ISG Subscriber Services』
12.2(28)SB	ISG：ポリシー制御：ユーザ プロファイル	ISG ユーザ プロファイルは、指定された加入者の ISG セッションに適用すべき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。	『Configuring ISG Subscriber Services』
12.2(28)SB	ISG：セッション：Auth：PBHK	ISG Port-Bundle Host Key 機能は、外部ポータルにおいて、セッションを識別するためのインバンド シグナリング メカニズムとして機能します。加入者からの TCP パケットは、ISG ゲートウェイのローカル IP アドレスと一定範囲のポートにマッピングされます。このマッピングにより、ポータルはセッションが開始された ISG ゲートウェイを識別できるようになります。	『Configuring ISG Port-Bundle Host Key』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(28)SB	ISG：セッション：認証：シングル サインオン	シングル サインオンを使用すると、加入者がアクセス プロバイダーまたはサービス プロバイダーの管理ドメイン内の他のデバイスによって提供されるサービスにアクセスできる場合、セッションを複数回認証する必要がなくなります。	『Overview of ISG』
12.2(28)SB	ISG：セッション：認証	ISG 自動加入者ログインでは、認可要求でユーザ名の代わりに、指定された別の ID を使用できます。AAA サーバが、指定された ID に基づいて加入者を許可できることにより、加入者からパケットを受け取るとすぐに、AAA サーバから加入者のプロファイルをダウンロードできるようになります。	『Configuring ISG Policies for Automatic Subscriber Logon』
12.2(28)SB	ISG：セッション：作成：インターフェイス IP セッション：L2	ISG IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成されます。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(28)SB	ISG：セッション：作成：インターフェイス IP セッション：L3	ISG IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成されます。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(28)SB	ISG：セッション：作成：IP セッション：プロトコル イベント（DHCP）	ほとんどの ISG セッションは、すでにアクティブなセッションに関連付けられないデータ フローの検出時に作成されます。ISG は、加入者から最初の DHCP DISCOVER パケットを受信したときに、IP セッションを作成するように設定できます。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(28)SB	ISG：セッション：作成：IP セッション：サブネットおよび発信元 IP：L2	ISG セッションは、特定のデータ フロー間でサービスとポリシーを関連付けるために使用される主要なコンポーネントです。IP サブネット セッションとは、単一の IP サブネットからの IP トラフィックを含む ISG セッションです。発信元 IP セッションには、単一の発信元 IP アドレスからのトラフィックが含まれます。	『Configuring ISG Access for IP Subscriber Sessions』
12.2(28)SB	ISG：セッション：作成：IP セッション：サブネットおよび発信元 IP：L3	ISG セッションは、特定のデータ フロー間でサービスとポリシーを関連付けるために使用される主要なコンポーネントです。IP サブネット セッションとは、単一の IP サブネットからの IP トラフィックを含む ISG セッションです。発信元 IP セッションには、単一の発信元 IP アドレスからのトラフィックが含まれます。	『Configuring ISG Access for IP Subscriber Sessions』

表 1　Cisco IOS Release 12.2SB、12.2(33)SR、および 15.0S でサポートされる ISG 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(28)SB	ISG：セッション：作成：P2P セッション（PPPoE、PPPoXoX）	ISG セッションとは、特定のデータ フロー間でサービスとポリシーが関連付けられる主要なコンテキストです。Point-to-Point（P2P; ポイントツーポイント）セッションは、シグナリング プロトコルを通じて確立されます。ISG は、PPP、PPPoE、および PPPoA など各種の P2P カプセル化を処理します。	『Configuring ISG Access for PPP Sessions』
12.2(28)SB	ISG：セッション：ライフサイクル：アイドル タイムアウト	ISG アイドル タイムアウトは、接続をを終了するまでに、その接続をアイドルにしておく時間を制御します。	『Configuring ISG Policies for Session Maintenance』
12.2(28)SB	ISG：セッション：ライフサイクル：Packet of Disconnect（POD）	ISG は、外部ポリシー サーバと相互動作するように設定できます。ポリシー サーバは、RADIUS Packet of Disconnect（POD; パケット オブ ディスコネクト）を使用して、ISG セッションのライフサイクルを管理できます。POD メッセージの主な役割は、ISG セッションを終了することです。	『Enabling ISG to Interact with External Policy Servers』
12.2(28)SB	ISG：セッション：VRF 転送	ISG セッションは、特定のデータ フローでサービスとポリシーを関連付けるために使用される主要なコンポーネントです。ネットワーク サービスのためにルーティングが必要な場合、ISG セッションは、Virtual Routing and Forwarding（VRF）インスタンスに関連付けられます。ISG VRF 転送は、仮想ルーティング ドメイン間でアクティブ セッションを動的に切り替える手段を提供します。	『Configuring ISG Access for IP Subscriber Sessions』

ISG の概要

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。このマニュアルでは、ISG の概要、メリット、実装の開始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 の概要の機能情報」（P.27）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 の概要

ISG とは

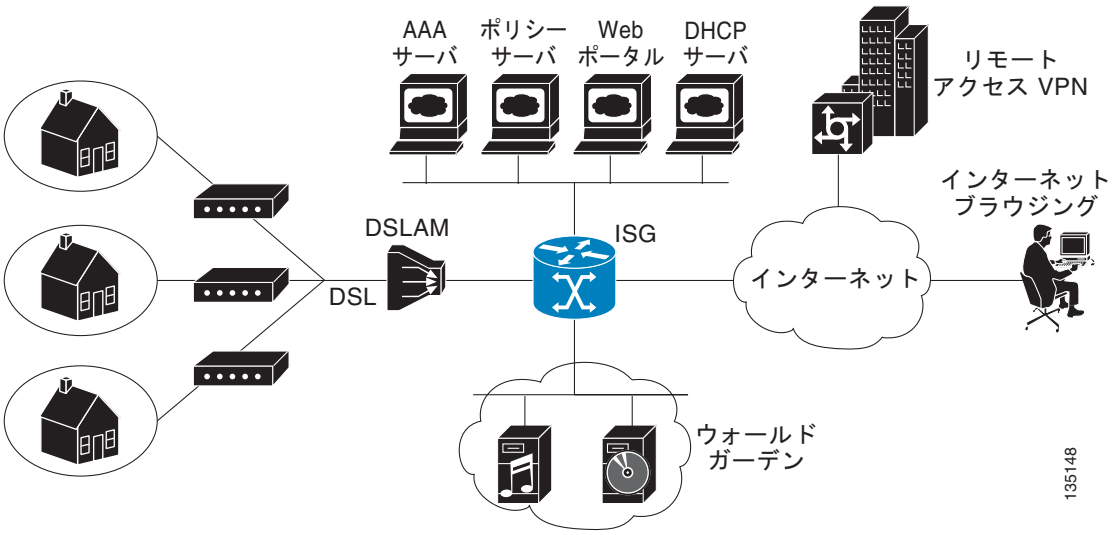
ISG は、エッジ アクセス デバイスによって柔軟で拡張性の高いサービスを加入者に提供できる構造化フレームワークです。ISG は加入者管理の、次の主要部分を処理します。

- 加入者の識別
- サービスとポリシーの決定
- セッション ポリシーの強制
- セッションのライフサイクル管理
- アクセスとサービスの使用状況のアカウンティング
- セッションの状態モニタリング

さらに、ISG では、RADIUS プロトコルへの制御ポリシーおよび Change of Authorization（CoA）拡張機能によって、プロビジョニングおよびサービスのアクティブ化に動的要素が導入されています。

ISG 対応デバイスはネットワークのアクセス エッジおよびサービス エッジで展開でき、Digital Subscriber Line（DSL; デジタル加入者線）、Public Wireless LAN（PWLAN）、およびモバイル ワイヤレスなどの加入者ネットワーク環境に適用できます。さらに、ISG は特定のソリューションでの加入者およびサービスの情報の、柔軟な配布を実現するよう設計されています。図 1 に、サービス プロファイル データを Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）データベースに格納し、オンデマンドで取得およびキャッシュできる一般的な DSL 展開を示します。

図 1　　DSL 展開のトポロジ例



ISG で直接サービスを定義することもできます。どのような場合でも、サービスのアクティブ化は、ローカルで定義された制御ポリシー、ユーザ プロファイルの対応付け、または外部ポリシー サーバまたはポータル アプリケーションからの CoA コマンドの結果としてトリガーされます。

ISG の原理

ISG アーキテクチャの基礎となっているのは、共通セッション レイヤのプロビジョニングです。このレイヤでは、汎用加入者セッションの管理と、エッジ デバイスへのアクセスの提供に使用されるテクノロジーが分離されます。

このセッション管理レイヤでは、加入者の識別情報の抽出とサービスのアクティブ化の決定のために共通の方法が提供されます。次の項では、この方法について説明します。

- 「加入者セッション」（P.19）
- 「加入者アクセス」（P.20）
- 「加入者の識別」（P.20）
- 「加入者サービス」（P.20）
- 「ポリシー」（P.21）
- 「ポリシーのダイナミックな更新」（P.21）

加入者セッション

ISG 加入者セッションは、エッジ デバイスを操作するすべての加入者のために作成された汎用システム コンテキストです。加入者セッションは、ポリシーをできるだけ早く適用するために、最初の操作で作成されます。このようなポリシーによって、加入者の識別情報の取得が容易になります。すべての加入者セッションがローカルの固有 ID に割り当てられ、その後、セッションを参照するために使用できます。

セッション コンテキストはセッション管理レイヤでの共通の処理のための基本ですが、セッション コンテキストに含まれるトラフィックのタイプはさまざまです。セッション タイプは、セッションで処理されるパケットのタイプに応じて、レイヤ 2 またはレイヤ 3 に分類できます。たとえば、PPP セッションはレイヤ 2 セッションで、PPP ネゴシエーションを使用して確立されたリンクを介して転送されたすべてのパケットを含みます。IP セッションには 1 つの IP アドレスで加入者デバイスと交換されるすべての IP パケットが含まれるため、レイヤ 3 です。セッションがレイヤ 2 またはレイヤ 3 のどちらであるかによって、セッションに対してアクティブ化できるポリシーのタイプがある程度決まります。

また、ISG によって、インターフェイスに対して IP セッションを定義する方法に、柔軟性がもたらされます。たとえば、特定のインターフェイスで、1 つのアドレス（IP セッション）、サブネット（IP サブネット セッション）、またはインターフェイス自体（IP インターフェイス セッション）に基づいて IP セッションを分類するために ISG をプロビジョニングでき、インターフェイス上で転送されたすべての IP パケットが、同じセッションに含まれます。

ネットワーク展開では、ISG セッション タイプは個々の加入者エンティティを示すようにプロビジョニングする必要があります。たとえば、個々の IP アドレスを持ついくつかの加入者デバイスが家庭内 LAN に接続された加入者の家庭に、特定の ISG インターフェイスを直接接続できます。LAN に接続された各デバイスを個別の加入者としてモデル化し、複数のポリシーおよびサービスを相互に適用するように計画する場合、IP セッションを想定してインターフェイスをプロビジョニングする必要があります。ただし、家庭が 1 つの加入者アカウントで表され、交換されるすべてのパケットのための共通の処理が必要な場合は、インターフェイスまたはサブネット セッションとしてインターフェイスをプロビジョニングする必要があります。

加入者アクセス

ISG では、特定のアクセス メディアとプロトコルのプロビジョニングおよび処理が、すべてのセッション タイプに適用できる機能から可能な限り分離されます。このモデルには、次の利点があります。

- 加入者サービスの共通セットを、異種加入者ネットワークが集約される ISG 上で使用できます。
- 加入者サービスの共通セットは、アクセス テクノロジーが異なる場合でも、複数の ISG に使用できます。
- 特定の加入者のために、サービス プロビジョニングを変更する必要なしにアクセス方法を変更できます（プロビジョニングまたはローミングによる）。
- 新しいアクセス プロトコルが使用できるようになると、サービス コンテキストを変更する必要なしに既存のエッジ展開に利用できます。新しいアクセス プロトコルが ISG フレームワークに導入されます。

加入者の識別

最初の制御プロトコル パケットを加入者デバイスから受信したときに、加入者セッションが作成されます。制御プロトコルは、セッション タイプに応じて異なります。制御プロトコルがない場合は、加入者からの最初のデータ パケットによってセッションが通知されます。

セッションの開始時に、ある程度の識別情報が利用可能になりますが、通常は加入者の完全な識別には不十分です。制御ポリシーを使用すると、セッションの開始時に利用可能となった識別情報を、加入者からのその後の ID の抽出を促し、セッションの新しいポリシーを決定するために使用できます。次の例では、ISG で加入者の ID を処理する方法を示します。

- 加入者のアクセス プロトコルが PPPoA の場合、コール要求が着信した ATM 仮想接続をセッションの開始時に利用できます。制御ポリシーは、サービス「ISP-A」で定義されたトンネル上の Virtual Path Identifier（VPI; 仮想パス識別子）1 ですべてのセッションを転送するが、VPI 2 を介してネットワークにアクセスしようとするすべての加入者に、ユーザ名を要求するよう定義できます。
- IP セッションでは、DHCP プロトコル イベントによってセッションの開始が通知された場合、TCP リダイレクト ポリシーをアクティブ化できます。このポリシーによって、外部 Web ポータルでのユーザ名と資格情報の収集が容易になります。

加入者サービス

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。サービスがセッションでアクティブ化されると、そのサービスに含まれるすべてのポリシーがそのセッションでアクティブ化されます。同様に、サービスが無効になると、そのサービスに含まれるすべてのポリシーがそのセッションから削除されます。

サービスは、多数の加入者に適用できるポリシーの特定の組み合わせを処理するために役立ちます。このアプリケーションでは、永続的データの重複が削減され、1 つのアクションおよび一度の参照でポリシーのグループをアクティブ化できます。

サービスは Command-Line Interface（CLI; コマンドライン インターフェイス）からエッジ デバイス上で直接定義することも、外部リポジトリで定義することもでき、必要に応じてダウンロードできます。ダウンロードされたサービス定義は、1 つ以上のセッションでアクティブになっている限り、デバイスにキャッシュされています。

サービスは次のいずれかの方法でアクティブ化されます。

- 制御ポリシーの実行の結果として
- CoA service-logon コマンドの受信
- サービスに自動アクティブ化のフラグが付けられたユーザ プロファイルの参照

サービスには主にトラフィック ポリシーが含まれます。特定のサービスに組み込まれるポリシーに関して、いくつかの制約事項があります。たとえば、異なるトラフィック方向（インバウンドとアウトバウンド）に適用されない限り、デフォルト以外の異なるトラフィック クラスを指定する 2 つのトラフィック ポリシーをサービスに含めることはできません。

サービスにネットワーク転送ポリシーが含まれる場合、*プライマリ サービス*と呼ばれます。特定のセッションに対して一度に 1 つのプライマリ サービスのみをアクティブ化できます。プライマリ サービスは相互に排他的です。

ポリシー

ISG では、次の 2 つの基本ポリシー タイプのサポートが導入されています。

- トラフィック ポリシー
- 制御ポリシー

トラフィック ポリシーは、データ パケットの処理を定義し、ポリシーを適用するためのパケットベースの条件を定義するトラフィック クラスと、データ ストリームで特定の処理を実行する機能インスタンスであり、*機能*と呼ばれる 1 つ以上のトラフィック アクションで構成されます。トラフィック ポリシーで設定されるトラフィック アクションは、トラフィック クラスによって定義された条件を満たすデータ パケットのために起動されます。

ネットワーク転送ポリシーは、アクションが、特定の Virtual Routing and Forwarding（VRF）を使用したパケットのルーティングや、レイヤ 2 接続を介したパケット転送などのネットワーク転送アクションである特定のタイプのトラフィック ポリシーです。ネットワーク転送ポリシーは「クラスレス」で、転送アクションを適用するための条件を絞り込むことはできません。

制御ポリシーはシステム イベントの処理を定義し、1 つ以上の制御ポリシー ルールと、含まれるポリシー ルールの評価方法を決める決定方式によって構成されます。制御ポリシー ルールは、制御クラス（柔軟な条件節）、条件が評価されるイベント、1 つ以上の制御アクションで構成されます。制御アクションは「認証」や「サービスのアクティブ化」などの汎用システム機能です。

制御ポリシーはインターフェイスまたは ATM Virtual Circuit（VC; 仮想回線）などのさまざまなターゲット上でアクティブ化でき、通常は加入者 ID の抽出と認証、セッションでのサービスのアクティブ化を制御します。トラフィック ポリシーは、セッションでのみアクティブ化でき、通常はサービスのアクティブ化によって適用されます（そうでない場合もあります）。

制御ポリシーは機能に固有のコンフィギュレーション コマンドのため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。制御ポリシーは、システムの動作を指定するための直感的で拡張可能なフレームワークを表現します。システムに追加機能が追加された際、管理者は新しいコンフィギュレーション コマンドのセットを完全に学習する必要はなく、制御ポリシーに含めることができる新しいイベントやアクションを学習するだけですみます。

ポリシーのダイナミックな更新

従来は、加入者の基本 ID が認証された後、セッションの確立時のみに加入者ポリシーが指定されていました。ISG では、セッション ポリシーをいつでも変更できるダイナミック ポリシー モデルが導入されました。

セッション ポリシーはセッションの開始時に評価され、アクセス プロトコルを介して加入者から収集した追加の ID またはサービス選択情報をいつでも再評価できます。さらに、制御ポリシーのアクティブ化または外部アプリケーションからの CoA コマンドによって、セッションのポリシーを更新できます。外部アプリケーションからの CoA コマンドの場合、外部アプリケーションでは、管理者の操作、バックエンド処理、または加入者の操作（Web ポータルでのサービス選択など）の結果としてポリシーを更新できます。

ISG の利点

ISG には次のような利点があります。

- Cisco 製品全体のセッション管理のための共通システムとアクセス テクノロジー。新しいアクセス プロトコル、転送プロトコル、および機能を、影響を最小限に止め、再利用の可能性を最大限に引き出しながら組み込むことができます。
- 加入者 ID、サービス アプリケーション、加入者のアクセス タイプとセッション タイプに関する問題の切り分け。
- 柔軟なセッション定義。
- 柔軟なセッション検出。
- ID、サービスのアクティブ化、およびポリシー アクティブ化への柔軟で直感的なアプローチ。
- 複数の信頼レベル。セッションの認可は認証の条件となりません。
- 制御ポリシー。制御ポリシーでは分散ポリシーの意思決定を容易にし、エッジ デバイスとポリシー サーバの間のラウンドトリップ遅延を削減し、システム イベント処理を一貫した直感的な方法で記述できます。
- 制御ポリシーとトラフィック ポリシーのための共通のポリシー モデルおよび言語。
- CoA を介したダイナミック ポリシー 更新のプロビジョニング（サービスのアクティブ化または「ポリシー プッシュ」による）。
- 既存の Cisco IOS インフラストラクチャを使用した、セッション機能の提供。
- 既存の Cisco IOS インフラストラクチャを使用した、セッションの状態とライフ サイクルの追跡。
- 加入者の操作の最初のインスタンスでのセッション コンテキストの作成。その結果、加入者トラフィックにすぐにポリシーを適用できるようになります。
- サービス データの柔軟な配布。
- 幅広いアカウンティング オプション。プリペイド アカウンティング、ポストペイド アカウンティング、プリペイド アカウンティングとポストペイド アカウンティングの切り替え、中間アカウンティング、イベントベースのアカウンティング、フローベースのアカウンティングなど。
- 外部アプリケーションへのシングル サインオン サービス。
- サービスベースの Dynamic Host Configuration Protocol（DHCP）プールと DHCP サーバの判別、DHCP によるダイナミックな再アドレス指定、VRF 転送などの「公平なアクセス」展開をサポートする柔軟なインフラストラクチャ。
- RADIUS や CoA などの標準的な外部インターフェイスのサポート。

ISG 実装の計画

ISG は非常に柔軟で、幅広い機能をサポートします。ISG の設定を開始する前に、システムを慎重に計画する必要があります。ここでは、考慮する必要のあるシステムの重要な点について説明します。

信頼モデル

信頼レベルは特定のアプリケーション ドメインのセキュリティのニーズによって決まり、加入者ネットワークによって提供されるセキュリティを継承します。次の状況では、加入者 ID を認証する必要がありません。

- セキュリティが重要ではないと考えられる場合
- エンドツーエンド セキュリティがインバンドで提供される場合
- 加入者ネットワークが本質的に安全である場合

加入者を認証する必要があるかどうかは、アクセス プロトコルの選択に影響します。認証が必要ない場合、制御ポリシーを使用して、加入者 ID に基づいて認可およびその他のセッション ポリシーを判断できます。

認証が必要だと考えられる場合、認証済みの ID は次の期間だけ信頼されます。

- セッションの期間
- 定期的な再認証が指定されるまで
- セッションの期間以上。たとえば、登録のライフタイム

完全なセキュリティの場合、再認証を必要とせずに、認証の前に（エッジへの）セッションを保護するために暗号化メソッドを使用できます。ただし、これによって、管理およびパフォーマンスのオーバーヘッドが発生します。

加入者アクセス モデル

信頼モデルでは、アクセス プロトコルの選択がほぼ決まります。ただし、アクセス モデルは基盤となるメディア（ATM やイーサネットなど）、エンドポイントのタイプ（PC、携帯電話、PDA など）、モビリティの要件、加入者のデバイスでインストールされるソフトウェアに影響するシステムの性能、拡張性の要件などの要因によっても異なります。

シングル サインオンの要件

加入者がアクセス プロバイダーまたはサービス プロバイダーの管理ドメイン内の他のデバイスによって提供されるサービスにアクセスできる場合、追加の認証は必要でしょうか、あるいは加入者 ID は信頼すべきでしょうか。後のデバイスでは追加の加入者識別情報を収集するためにアクセス デバイスを照会し、加入者がアクセス デバイスによってすでに認証済みであるかどうかを確認する必要があります。シングル サインオン機能は、CoA の「セッション照会」機能によって提供されます。

ネットワーク転送

加入者はどのようにして、ネットワーク サービスへのアクセス権を得るべきでしょうか。ネットワーク転送には、次の機能が含まれます。

- レイヤ 2 接続。たとえば、L2TP Network Server（LNS; L2TP ネットワーク サーバ）への Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）トンネル
- すべてのセッション パケットを特定の VRF またはルーティング ドメインに関連付けることによるレイヤ 3 接続

サービスのパッケージ化

加入者ポリシーをサービスにまとめる場合、どうすればよいでしょうか。サービスをパッケージ化するには、次のことを考慮する必要があります。

- 特定のポリシーの組み合わせが複数の加入者に共通しているか。
- 共有されているポリシー の組み合わせが特定の転送ドメインに依存しているか。
- 加入者がサービス ドメイン間を移動する必要があるか。
- デバイスまたはリモート リポジトリでサービスを定義する必要があるか。外部で定義されたサービスは、1 つ以上のセッションでアクティブ化されている限り、ローカルにキャッシュされます。

請求モデル

サービスの使用に応じて加入者に請求するにはどうすればよいでしょうか。次のような請求オプションがあります。

- 使用時間またはボリュームに応じて請求
- 事前に（プリペイド）または定期的に（従来のポストペイド）請求
- セッションに対してプロビジョニングされたポリシーに従って請求
- 使用した時間帯に応じて請求（請求方法の切り替え）

関連情報

ISG を設定するには、次のモジュールを参照してください。

- 『Configuring ISG Control Policies』: ISG 制御ポリシーの設定方法について説明します。特定の条件やイベントに応じてシステムが実行するアクションを定義します。
- 『Configuring ISG Access for PPP Sessions』: ISG レイヤ 2 セッションの処理のためのポリシーの設定方法について説明します。
- 『Configuring ISG Access for IP Subscriber Sessions』: IP 加入者セッションを開始し、加入者 IP アドレス指定を管理し、ダイナミック VPN 選択を設定するように ISG を設定する方法について説明します。
- 『Configuring ISG Port-Bundle Host Key』: ISG Port-Bundle Host Key 機能を設定する方法について説明します。この機能は、加入者からの TCP パケットを ISG ゲートウェイのローカル IP アドレスとポートの範囲にマッピングします。このマッピングにより、外部ポータルで、セッションが開始された ISG ゲートウェイを識別できます。
- 『Configuring ISG as a RADIUS Proxy』: RADIUS 認証を使用するクライアント デバイスと AAA サーバの間のプロキシとして動作するように ISG を設定する方法について説明します。

- 『Configuring ISG Policies for Automatic Subscriber Logon』：認可要求でユーザ名の代わりに指定された ID を使用し、加入者からパケットを受信するとすぐに、ユーザ プロファイルを AAA サーバからダウンロードできるように ISG を設定する方法について説明します。
- 『Enabling ISG to Interact with External Policy Servers』：外部ポリシー サーバからポリシーを取得するか、またはポリシー サーバでダイナミックなセッション ポリシーの更新を可能にするための ISG の設定方法について説明します。
- 『Configuring ISG Subscriber Services』：ISG 加入者サービスのしくみ、サービスおよびサービスに適用できるトラフィック クラスの設定方法、サービスのアクティブ化方法について説明します。
- 『Configuring ISG Network Forwarding Policies』：アップストリーム ネットワークとのパケットのルーティングや転送を可能にするネットワーク ポリシーの設定方法について説明します。
- 『Configuring ISG Accounting』：ISG アカウンティングの設定方法について説明します。セッション単位およびサービス単位のアカウンティング、ブロードキャストアカウンティング、ポストペイドの請求方法の切り替えなどが含まれます。
- 『Configuring ISG Support for Prepaid Billing』：ISG でのプリペイド アイドル タイムアウトやプリペイド請求方法の切り替えなどを含む、プリペイド課金サポートを設定する方法について説明します。
- 『Configuring ISG Policies for Session Maintenance』：ISG セッションおよびアイドル タイムアウトの設定方法について説明します。
- 『Redirecting Subscriber Traffic Using ISG Layer 4 Redirect』：加入者のレイヤ 4 トラフィックをリダイレクトして、加入者認証、初期および定期的な広告、アプリケーション トラフィックのリダイレクト、および DNS リダイレクトを容易にする方法について説明します。
- 『Configuring ISG Network Forwarding Policies』：モジュラ Quality of Service（QoS）CLI 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。
- 『Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging』：ISG のデバッグのフィルタリングを容易にするための条件付きデバッグの使用方法について説明します。

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*』

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 の概要の機能情報

表 2 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 2 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 2　ISG の概要の機能情報

機能名	リリース	機能設定情報
ISG：セッション：認証：シングル サインオン	12.2(28)SB 12.2(33)SRC 15.0(1)S	シングル サインオンを使用すると、加入者がアクセス プロバイダーまたはサービス プロバイダーの管理ドメイン内の他のデバイスによって提供されるサービスにアクセスできる場合、セッションを複数回認証する必要がなくなります。 この機能に関する詳細については、次の項を参照してください。 • 「ISG 実装の計画」（P.23） 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。

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**

PPP セッションのための ISG アクセスの設定

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。このマニュアルでは、Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）加入者のための ISG アクセスを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、「PPP セッションのための ISG アクセスの機能情報」（P.65）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

PPP セッションのための ISG アクセスに関する前提条件

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、「PPP セッションのための ISG アクセスの機能情報」（P.65）を参照してください。

使用されるアクセス プロトコルは、インターフェイス上にプロビジョニングされている必要があります。

ローカル PPP 認証が必要な場合は、インターフェイスまたは仮想テンプレートで **ppp authentication** コマンドを設定する必要があります。

このマニュアル内の作業と例は、ISG 制御ポリシーの設定方法および使用方法に関する知識があることを前提としています。制御ポリシーの設定方法の詳細については、「Configuring ISG Control Policies」モジュールを参照してください。

PPP セッションのための ISG アクセスに関する制約事項

Cisco 10000 シリーズ ルータ上の PPPoX セッションでは、Modular Quality of Service（QoS）Command Line Interface（MQC）ポリシーと ISG ポリシーを、同時に設定できません。たとえば、MQC ポリシーと ISG ポリシーは、PPPoX セッションの仮想テンプレート インターフェイスに適用できません（静的にも RADIUS からも）。

PPP セッションのための ISG アクセスの設定に関する情報

PPP セッションのためのアクセスを設定する前に、次の概念について理解しておく必要があります。

- 「PPP セッションのための ISG アクセスの概要」（P.54）
- 「PPP セッションのための ISG 加入者 IP アドレス管理」（P.55）
- 「PPP セッションのための ISG アクセスに対するデフォルト ポリシー」（P.55）
- 「PPP セッションのための ISG 制御ポリシーを使用する利点」（P.56）

PPP セッションのための ISG アクセスの概要

レイヤ 2 セッションは、ピア エンティティと ISG デバイスとの間で動作する制御プロトコルによって確立されます。通常、レイヤ 2 セッションは、同じ物理メディア上の他のセッションから隔離するためにカプセル化されます。

システムは、レイヤ 2 セッションにデフォルト処理を提供しますが、プロトコルを転送またはローカルで終端するためのポリシー、またはアクセス プロトコルから収集された ID データに基づいて、ローカルで加入者を認証するためのポリシーの設定が必要な場合があります。ISG 制御ポリシーは、アクセス プロトコルから、ピア エンティティの ID および資格情報を抽出するように設定できます。このメカニズムでは、プロトコルによって明示的に提供される ID、あるいは基盤となるメディアまたはアクセス ポートのネイティブな ID のいずれかの、セッションに関連する ID に基づいてレイヤ 2 セッションのサービスをプロビジョニングできます。

ISG は、次のレイヤ 2 アクセス プロトコルをサポートします。

- PPP
- PPP over Ethernet（PPPoE）
- PPP over ATM（PPPoA）

- Layer 2 Tunnel Protocol（L2TP）
- Layer 2 Forwarding（L2F）プロトコル

PPP セッションのための ISG 加入者 IP アドレス管理

ISG 加入者 IP アドレス管理は、ローカルで終端される IP セッションまたはレイヤ 2（PPP）セッションに適用されます。

加入者は、特定の IP サービス ドメイン内でルーティングを受けるためには、ドメイン固有の IP アドレスをネットワークに知らせる必要があります。加入者が IP サービス ドメイン（アクセス プロバイダーによって管理される任意のプライベート ドメインを含む）間を移動する場合は、ネットワークに知らせる IP アドレスを、新しいドメインを反映して変更する必要があります。ローカルで終端される PPP セッションについては、ISG は、次の IP アドレスの割り当て方法をサポートします。

- ユーザ プロファイル内の IP アドレス
- ユーザ プロファイル内の IP サブネット
- ユーザ プロファイル内の名前付きアドレス プール
- ローカル アドレス プール
- PPP のための IP アドレス管理の標準的方法（PPP セッションのための IP アドレス管理サポートの詳細は『*Cisco IOS Dial Technologies Configuration Guide*, Release 12.2』を参照）

ローカルで終端された PPP セッションが、ある Virtual Routing and Forwarding（VRF）インスタンスから別の VRF に転送される場合、IPCP を使用して、ピア IP アドレスが再ネゴシエーションされます。

PPP セッションの VRF 転送

VRF 転送では、新しいプライマリ サービスの選択に従って、ISG 加入者セッションをある VRF から別の VRF に移動できます。Network Access Point（NAP; ネットワーク アクセス ポイント）からの IP アドレスで PPP セッションが確立されると、加入者は Web ポータルへのアクセス、およびサービス プロバイダーの選択が可能になります。PPP セッションの VRF 転送では、ISG は、IP アドレスを新しいドメインから PPP セッションに再度割り当てる必要があります。PPP セッションでは、IP Control Protocol（IPCP）再ネゴシエーションによって、IP アドレスが再度割り当てられます。

PPP 再ネゴシエーションなしでは、PPP セッションの VRF 転送はサポートされません。

PPP セッションのための ISG アクセスに対するデフォルト ポリシー

ISG は、制御ポリシーが設定されいない場合のレイヤ 2 セッションのデフォルト処理を提供します。**vpdn enable** コマンドが設定されている場合で、ユーザ名にドメイン名が指定されている（たとえば、user@domain）か、または Dialed Number Identification Service（DNIS; 着信番号識別サービス）番号が提供されている場合、システムはこの情報に基づいて認可を行います。Virtual Private Dialup Network（VPDN）トンネル情報が検出されると、セッションは L2TP Network Server（LNS; L2TP ネットワーク サーバ）での処理のために転送されます。リモート LNS で認証が要求されている場合、**ppp authentication** コマンドを PPP インターフェイスまたは仮想テンプレートで設定する必要があります。**vpdn authen-before-forward** コマンドが設定されている場合、PPP セッションを LNS に転送する前に、PPP セッションの認証がローカルで試行されます。

ドメイン名または DNIS のトンネル情報が検出されていない場合、または **vpdn enable** コマンドが設定されていない場合は、Stack Group Bidding Protocol（SGBP）認可が試行されます（SGBP が設定されている場合）。SGBP を使用して認可情報を取得できない場合、PPP セッションはローカルで終端され

ます。ローカル終端は、ピアと ISG デバイスの間で PPP セッションが確立され、IP ペイロードがルーティングされることを意味しています。後者の場合、**ppp authentication** コマンドが PPP インターフェイスまたは仮想テンプレートで設定されている場合のみ、認証が行われます。

セッション開始イベントに ISG 制御ポリシーが定義されている場合、デフォルト処理ではなく、そのポリシーが優先されます。

PPP セッションのための ISG 制御ポリシーを使用する利点

ISG は、アクセス プロトコルを介してピア エンティティからの ID 情報と資格情報の抽出を制御することによって、レイヤ 2 セッションのサービス決定に柔軟なアプローチを提供します。たとえば、コール要求が着信する ATM Permanent Virtual Circuit（PVC; 相手先固定接続）に基づいてサービスが決定される場合、セッションの確立およびサービスの提供の前に、制御プロトコルの実行が完了している必要はありません。この方法では、ローカル リソースを節約し、コール セットアップ時間を改善できます。

制御ポリシーを使用した PPP セッションのための ISG アクセスの設定方法

ISG レイヤ 2 アクセスを設定するには、次の手順を実行します。

1. 加入者 ID が、レイヤ 2 セッション処理にどのように影響するかを決定します。具体的には、プロトコルを転送するのか。ローカルで終端するのか、および加入者をローカルで認証するかどうかを決定します。
2. レイヤ 2 セッション処理を提供するため、制御ポリシーを設定します。制御ポリシーの設定方法の詳細については、「Configuring ISG Control Policies」モジュールを参照してください。レイヤ 2 アクセスの制御ポリシーの例については、「PPP セッションのための ISG アクセスの設定例」（P.61）を参照してください。
3. PPP セッションの ISG VRF 転送をイネーブルにします。
4. 必要に応じて、設定の確認とトラブルシューティングを行います。

ここでは、次の作業について説明します。

- 「PPP セッションのための ISG VRF 転送のイネーブル化」（P.56）
- 「PPP セッションのための ISG アクセスのトラブルシューティング」（P.59）

PPP セッションのための ISG VRF 転送のイネーブル化

VRF 転送では、新しいプライマリ サービスの選択に従って、ISG 加入者セッションをある VRF から別の VRF に移動できます。この手順は、次のセクションから構成されます。

- 「前提条件」（P.57）
- 「サービス ポリシー マップでの VRF の指定」（P.57）
- 「PPP セッションの VRF 転送の確認」

前提条件

この手順は、仮想テンプレートおよび IP アドレスの割り当て方法を設定することによって、PPP セッションのサポートが設定されていることを前提としています。VRF 転送が機能するためには、元の VRF、ループバック インターフェイス、および IP アドレス プールを、ユーザ プロファイルではなく、仮想テンプレートで指定する必要があることに注意してください。仮想テンプレートおよび PPP セッションのサポートの設定方法については、『*Cisco IOS Dial Technologies Configuration Guide*』を参照してください。

サービス ポリシー マップでの VRF の指定

VRF 転送は、新しいプライマリ サービスがセッションに対してアクティブな場合に発生し、セッションが 1 つの VRF から別の VRF に転送されます。サービスは、外部 Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバ上のサービス プロファイル内、または ISG デバイス上のサービス ポリシー マップに設定できます。ISG デバイス上のサービス ポリシー マップに VRF 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. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**
6. **sg-service-group** *service-group-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 service** *policy-map-name* 例： `Router(config)# policy-map type service service1`	ISG サービスの定義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、サービス 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	**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。

	コマンドまたはアクション	目的
ステップ 5	**sg-service-type primary** 例： `Router(config-service-policymap)# sg-service-type primary`	サービスをプライマリ 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。プライマリ サービスは、**sg-service-type primary** コマンドを使用してプライマリ サービスとして定義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。
ステップ 6	**sg-service-group** *service-group-name* 例： `Router(config-service-policymap)# sg-service-group group1`	（任意）ISG サービスをサービス グループに関連付けます。 • 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。

PPP セッションの VRF 転送の確認

PPP セッションの VRF 転送を確認するには、次の作業を実行します。**show** のすべての手順はオプションで、任意の順序で実行できます。

手順の概要

1. **enable**
2. **show subscriber session all**
3. **show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
4. **show ip route** [**vrf** *vrf-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 all** 例： `Router# show subscriber session all`	加入者が選択したサービスに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 3	**show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**} **例：** `Router# show idmgr session key session-handle 48000002`	ISG セッションおよびサービス ID に関する情報を表示します。
ステップ 4	**show ip route** [**vrf** *vrf-name*] **例：** `Router# show ip route`	ルーティング テーブルの現在のステータスを表示します。

PPP セッションのための ISG アクセスのトラブルシューティング

この作業のコマンドを使用すると、レイヤ 2 セッションのモニタとトラブルシューティングを行えます。これらのコマンドはすべてオプションで、特定の順序で入力する必要はありません。

手順の概要

1. **enable**
2. **show subscriber session detailed**
3. **debug condition**
4. **debug subscriber packet** [**event** | **full** | **detail**]
5. **debug subscriber error**
6. **debug subscriber event**
7. **debug subscriber fsm**
8. **debug pppatm** {**event** | **error** | **state**} [**interface atm** *interface-number*[**.***subinterface-number*]] **vc** {[*vpi*/*vci*]*vci* | *virtual-circuit-name*}
9. **debug ppp** {**packet** | **negotiation** | **error** | **authentication** | **subscriber switch**}

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** 例： `Router# show subscriber session detailed`	ISG 加入者セッションに関する情報を表示します。
ステップ 3	**debug condition** *condition* 例： `Router# debug condition username user5@example.com`	指定された条件に基づいて、デバッグ出力をフィルタリングします。 **（注）** 条件付きデバッグの詳細については、「Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging」モジュールを参照してください。
ステップ 4	**debug subscriber packet** [**event** | **full** | **detail**] 例： `Router# debug subscriber packet event`	Subscriber Service Switch（SSS）コールのセットアップ中のパケットに関する診断情報を表示します。
ステップ 5	**debug subscriber error** 例： `Router# debug subscriber error`	SSS コールのセットアップ中に発生する可能性のあるエラーに関する診断情報を表示します。
ステップ 6	**debug subscriber event** 例： `Router# debug subscriber event`	SSS コールのセットアップ イベントに関する診断情報を表示します。
ステップ 7	**debug subscriber fsm** 例： `Router# debug subscriber fsm`	SSS コール セットアップ状態に関する診断情報を表示します。
ステップ 8	**debug pppatm** {**event** | **error** | **state**} [**interface atm** *interface-number*[*.subinterface-number*]] **vc** {[*vpi*/*vci*]*vci* | *virtual-circuit-name*} 例： `Router# debug pppatm error`	インターフェイス上または Virtual Circuit（VC; 仮想回線）上での PPP over ATM（PPPoA）イベント、エラー、および状態に関する診断情報を、グローバルまたは条件付きで表示します。
ステップ 9	**debug ppp** {**packet** | **negotiation** | **error** | **authentication** | **subscriber switch**} 例： `Router# debug ppp packet`	PPP を実装しているインターネットワーク内での、トラフィックおよび対話に関する情報を表示します。

例

次の例では、ユーザ名「cpe6_1@example.com」に基づいて、**debug subscriber packet detail** コマンドの出力がフィルタリングされます。

```
Router# debug condition username cpe6_1@example.com
Condition 1 set

Router# show debug
Condition 1: username cpe6_1@example.com (0 flags triggered)

Router# debug subscriber packet detail
SSS packet detail debugging is on

Router# show debug
SSS:
  SSS packet detail debugging is on
Condition 1: username cpe6_1@example.com (0 flags triggered)

Router#
```

PPP セッションのための ISG アクセスの設定例

ここでは、次の例について説明します。

- 「PPP セッションのための ISG アクセスの設定：例」（P.61）
- 「再ネゴシエーションを使用した PPP セッションの VRF 転送：例」（P.63）

PPP セッションのための ISG アクセスの設定：例

次に、PPP 加入者にサービスを提供する ISG ポリシーの設定例を示します。この例では、次のアクションを実行するための ISG を設定します。

- ATM Virtual Path Identifier/Virtual Channel Identifier（VPI/VCI; 仮想パス ID/仮想チャンネル ID）に基づく PPP 転送

  ISG は、VPI が 200 未満および VCI が 100 未満のすべての加入者に対して、転送サービス「xconnect」をアクティブにします。このポリシー ルールにより、ISG は PPP プロトコル全体を実行することなく、関連付けられた加入者にサービスを提供できます。その他すべての加入者は、ユーザ名で指定されるドメインに基づいてサービスを取得します。ISG は、ユーザ名をプロトコルから取得する必要があります。

- PPP ローカル終端

  ISG は、「ispa」ドメインと一致する加入者に対して、「ispa」サービスをアクティブすることによって、ローカル終端を提供します。システムは、方式リスト「list1」を使用して、加入者の認証を行います。ローカル終端サービスについては、サービス プロファイル、インターフェイス、または仮想テンプレートで他の VRF が指定されない限り、グローバル VRF がデフォルトで適用されます。

- 転送前 PPP 認証

  ISG は、セッションを LNS に転送する前に、「ispb」ドメインと一致する加入者をローカル認証します（サービス ポリシー マップ「ispb」は VPDN グループを指定しているため、セッションは LNS に転送されます）。加入者は、方式リスト「list2」を使用して認証されます。

- ローカル認証なしの PPP 転送

  ISG は、「ispc」ドメインと一致する加入者に対して、ローカル認証なしでセッションを LNS に転送します。

- PPP ドメインの除外

  ISG は、「ispd」ドメインと一致する加入者のセッションに対するサービスを拒否し、接続を解除します。

- PPP ドメインに基づくサービスのアクティベーション

  その他のドメインと一致する加入者に対して、ISG は指定されたドメインと同じ名前を持つサービスをアクティブにします。

制御クラス マップを設定することで、制御ポリシー ルールを実行するために適合すべき条件を定義します。

```
class-map type control match-all PPP_SESSION
  match identifier protocol ppp

class-map type control match-all NAS_PORT_CONDITION
  class type control match identifier name PPP_SESSION
  less-than identifier nas-port type atm vpi 200 vci 100

class-map type control match-all ISPA
  match identifier unauthenticated-domain ispa

class-map type control match-all ISPB
  match identifier unauthenticated-domain ispb

class-map type control match-all ISPC
  match identifier unauthenticated-domain ispc

class-map type control match-all ISPD
  match identifier unauthenticated-domain ispd
```

トップレベル制御ポリシー マップを定義します。

```
policy-map type control L2_ACCESS
```

コールが着信する ATM VPI/VCI に基づいて転送サービスをアクティブにする、制御ポリシー ルールを定義します。

```
 class type control NAS_PORT_CONDITION event session-start
  1 service-policy type service xconnect
```

プロトコルからドメイン名を収集する、制御ポリシー ルールを定義します。ドメイン名は、構造化されたユーザ名から入手できます（たとえば、user@domain）。

```
 class type control PPP_SESSION event session-start
  1 collect identifier unauthenticated-domain
  2 service-policy type control DOMAIN_BASED_ACCESS
```

ネストされた制御ポリシーを定義します。

```
policy-map type control DOMAIN_BASED_ACCESS
```

サービス「ispa」のアクティブ化によってローカル終端を提供する、制御ポリシー ルールを定義します。

```
 class type control ISPA event session-start
  1 authenticate aaa list list1
  2 service-policy type service ispa
```

サービス「ispb」をアクティブ化する前に、ローカルで加入者を認証するシステムを設定する、制御ポリシー ルールを定義します。サービス「ispb」は、セッションを LNS に転送するよう指定します。

```
 class type control ISPB event session-start
  1 authenticate aaa list list2
  2 service-policy type service ispb
```

サービス「ispc」をアクティブにする制御ポリシー ルールを定義して、転送を指定します。

```
 class type control ISPC event session-start
  1 service-policy type service ispc
```

サービス「ispd」と一致する加入者に対して、セッションの接続解除を行う制御ポリシー ルールを定義します。

```
 class type control ISPD event session-start
  service disconnect
```

その他すべてのドメインに対してデフォルトを定義する制御ポリシー ルールを定義します。これにより、指定されたドメインと同じ名前を持つサービスがアクティブになります。

```
 class type control always event session-start
    service-policy type service identifier unauthenticated-domain
```

サービス ポリシー マップを設定します。

```
policy-map type service xconnect
  service vpdn group 1

policy-map type service ispa
  service local
  ip vrf forwarding red

policy-map type service ispb
  service vpdn group 2

policy-map type service ispc
  service vpdn group 3
```

制御ポリシー マップをグローバルに適用します。

```
service-policy type control L2_ACCESS
```

再ネゴシエーションを使用した PPP セッションの VRF 転送：例

次に、PPPoE を使用してセッションを確立するコンフィギュレーション、および VRF を関連付けるために作成される RADIUS サービス プロファイルの例を示します。この例では、PPP セッションは、最初に実行されるときにはデフォルトのルーティング テーブルに属し、IP アドレスがデフォルト IP アドレス プール「DEF-POOL」から割り当てられます。加入者が「ISP-RED」サービスを選択すると、ISG は「ISP-RED」サービス プロファイルをダウンロードし、セッションに適用します。その後、PPP セッションは VRF「RED」に転送されます。クライアント デバイスと ISG デバイスの間で IPCP 再ネゴシエーションが実行され、加入者はプール「POOL-RED」から新しい IP アドレスを割り当てられます。

```
ip vrf RED
 rd 1:1

interface Loopback0
 ip address 10.0.0.1 255.255.255.0

interface Loopback1
 ip address 10.0.1.0 255.255.255.0
 ip vrf forwarding RED
!
interface Ethernet0/0
  pppoe enable

interface Virtual-Template1
 ip unnumbered Loopback0
 service-policy control RULE2
 peer default ip address pool DEF-POOL
 ppp authentication chap

ip local pool DEF-POOL 172.16.5.1 172.16.5.250
ip local pool POOL-RED 172.20.5.1 172.20.5.250
```

ISP RED のサービス プロファイル

```
Cisco-AVpair = ip:vrf-id=RED
Cisco-AVpair = "ip:ip-unnumbered=loopback 1"
Cisco-AVpair = ip:addr-pool=POOL-RED
Cisco-AVpair = subscriber:sg-service-type=primary
Cisco-AVpair = subscriber:sg-service-group=RED-GROUP
Cisco-SSG-Service-Info = IPPPOE-RED
Cisco-SSG-Service-Info = R10.1.1.0;255.255.255.0
Framed-Protocol = PPP
Service-Type = Framed
```

その他の参考資料

ここでは、PPP セッションのための ISG アクセス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*』
AAA 設定作業	『*Cisco IOS Security Configuration Guide*』の「Authentication」の項
AAA コマンド	『*Cisco IOS Security Command Reference*』の「Authentication, Authorization, and Accounting (AAA)」の項
PPP 設定作業	『*Cisco IOS Dial Services Configuration Guide*』の「PPP Configuration」の項
PPP コマンド	『*Cisco IOS Dial Services Command Reference*』

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/public/support/tac/home.shtml

PPP セッションのための ISG アクセスの機能情報

表 4 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 4 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 4　ISG レイヤ 2 アクセスの機能情報

機能名	リリース	機能設定情報
ISG：セッション：作成：P2P セッション（PPPoE、PPPoXoX）	12.2(28)SB 12.2(33)SRC	ISG セッションとは、特定のデータ フロー間でサービスとポリシーが関連付けられる主要なコンテキストです。Point-to-Point（P2P; ポイントツーポイント）セッションは、シグナリング プロトコルを通じて確立されます。ISG は、PPP、PPPoE、および PPPoA など各種の P2P カプセル化を処理します。 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。 • 「PPP セッションのための ISG アクセスの設定に関する情報」（P.54） • 「制御ポリシーを使用した PPP セッションのための ISG アクセスの設定方法」（P.56） 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。

IP 加入者セッションのための ISG アクセスの設定

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 は、ルーテッド レイヤ 2 またはレイヤ 3 アクセス ネットワークから ISG に接続する加入者の IP セッションをサポートします。このモジュールでは、IP 加入者セッションの確立、加入者 IP アドレッシングの管理、およびダイナミック Virtual Private Network（VPN; バーチャル プライベート ネットワーク）選択の設定のために、ISG を設定する方法について説明します。

（注） このマニュアルで説明する各項と設定手順は、Network Address Translation（NAT; ネットワーク アドレス変換）が ISG 以外のレイヤ 3 ゲートウェイで実行されていることを前提としています。

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、「IP 加入者セッションのための ISG アクセスの機能情報」（P.114）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

IP 加入者セッションのための ISG アクセスに関する前提条件

リリースおよびプラットフォームの要件の詳細については、「IP 加入者セッションのための ISG アクセス の機能情報」（P.114）を参照してください。

Dynamic Host Configuration Protocol（DHCP）サーバが、DHCP リース プロトコルをサポートしている必要があります。

IP 加入者セッションのための ISG アクセスに関する制約事項

重複する IP アドレスに関する制約事項

同じ Virtual Routing and Forwarding（VRF; 仮想経路フォワーディング）インスタンス内で重複する IP アドレスは、サポートされていません。

異なる VRF 内の重複する IP 加入者は、スタティック IP 加入者セッションおよびルーテッド IP 加入者セッションに対する同じインターフェイス上ではサポートされていません。異なる VRF 内の重複する IP 加入者は、レイヤ 2 接続された DHCP 加入者セッションに対する同じインターフェイス上でサポートされています。

IP サブネット セッションに関する制約事項

IP サブネット セッションは、**ip subscriber l2-connected** コマンドで設定されたインターフェイス上ではサポートされていません。IP サブネット セッションは、インターフェイス上で **ip subscriber routed** コマンドが設定されている場合のみサポートされます。

ISG DHCP に関する制約事項

レイヤ 3 DHCP リレー エージェントが ISG デバイスと加入者デバイスの間に存在する場合、ISG は DHCP 要求をリレーできません。

DHCP リース クエリーでは、Cisco 7600 および 7200 シリーズ ルータ、および Cisco 10000 シリーズ ルータがサポートされます。

ダイナミック VPN 選択に関する制約事項

ダイナミック VPN 選択は、IP インターフェイス セッション、IP サブネット セッション、およびグローバルではない VRF インターフェイスから入る加入者に対しては、サポートされていません。

ダイナミック VPN 選択は、アクセス インターフェイス上で静的な VPN コンフィギュレーションを持つ加入者に対しては、サポートされていません。

アドレス再割り当ての行われたダイナミック VPN 選択は、DHCP によって開始されたルーテッド IP 加入者セッションに対してはサポートされていません。ルーテッド IP 加入者の IP アドレスは、アクセス ネットワーク内でルーティング可能になっている必要があります。Internet Service Provider（ISP; インターネット サービス プロバイダー）または VRF の所有するプライベート アドレスは、重複していたり、加入者と ISG デバイスとの間のネットワークでルーティングできないことがあるため、このような加入者には IP アドレスを割り当てられません。

IP セッション全般に関する制約事項

Packet of Disconnect（PoD; パケット オブ ディスコネクト）は、IP 加入者セッションではサポートされていません。

IP 加入者セッションは、ambiguous IEEE 802.1QinQ（QinQ）または IEEE 802.1Q（Dot1Q）サブインターフェイスではサポートされていません。

IP 加入者セッションは、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）パケットを受信するインターフェイスではサポートされていません。

Modular Quality of Service（QoS）Command-Line Interface（CLI; コマンドライン インターフェイス）（MQC）に基づくシェーピングとキューイングは、IP 加入者セッションではデフォルト クラスの出力方向でサポートされています。

スタティック IP セッション上での機能の設定はサポートされていません。

Cisco 10000 シリーズ インターネット ルータに関する制約事項

ISG は、Cisco 10000 シリーズ インターネット ルータ上では、RADIUS パケットによって開始された IP 加入者セッションをサポートしていません。

IP インターフェイス セッションは、Cisco 10000 シリーズ インターネット ルータ上の ATM メイン インターフェイスと ATM マルチポイント サブインターフェイス上ではサポートされません。

IP 加入者セッションと PPP over ATM または PPP over Ethernet（PPPoX）セッションは、同じ ATM メイン インターフェイスまたはサブインターフェイス上ではサポートされません。複数の IP 加入者セッションまたは複数の PPPoX セッションのいずれかを、ATM メイン インターフェイスまたはサブインターフェイスで一度に設定できます。

IP 加入者セッションは、次のインターフェイス上ではサポートされません。

- マルチリンク インターフェイス
- トンネル インターフェイス
- 仮想テンプレート インターフェイス
- IPsec トンネル

DHCP が開始した IP セッションでは、DHCP 制御パケット（bootps パケットと bootpc パケット）を許可するためのアクセス リストを明示的に設定する必要があります。DHCP 制御パケットを許可するようにアクセス リストが設定されていない場合、IP セッションに適用される ISG 機能がこれらのパケットをドロップする場合があるため、予期しないまたは誤った ISG 動作が発生する可能性があります。たとえば、DHCP が開始した IP セッションを維持する DHCP 更新パケットが、IP セッションに適用されるセキュリティ アクセス リストによってドロップされる可能性があります。

Cisco 10000 シリーズ ルータでは、同じインターフェイス上で ISG も設定されている場合、Parallel eXpress Forwarding（PXF）パス内で unicast Reverse Path Forwarding（uRPF）がサポートされません。たとえば、次の構成では PXF パス内で uRPF がサポートされます。

```
interface GigabitEthernet7/0/0
 ip address 10.10.10.1 255.255.255.252
 ip verify unicast reverse-path
```

ところが、次の構成では PXF パス内で uRPF がサポートされません。

```
interface GigabitEthernet7/0/0
 ip address 10.10.10.1 255.255.255.252
 ip verify unicast reverse-path
 service-policy type control isg-control
 ip subscriber routed
 initiator unclassified ip-address
```

この構成では、ルータが受信するすべての IP パケットのうち、その発信元 IP アドレスが既存の ISG IP セッションと一致しないものは、Cisco 10000 Route Processor（RP）にパントされ、uRPF 処理が行われます。これにより、Cisco 10000 RP 上での割り込みレベル CPU 使用率が増大する場合があります。IP スプーフィングの問題を防止するため、すべての正当な IP ネットワークを発信元として指定する入力 Access Control List（ACL; アクセス コントロール リスト）の実装を検討してください。Cisco 10000 シリーズ ルータは、ISG 処理を実行する前に PXF 内の入力 ACL を処理します。

ISG インターフェイスに適用されるアクセス リストは、既存の ISG セッションに属する IP トラフィックに対しては、その ISG セッションがクリアされて再導入されるまで有効になりません。したがって、ACL を適用して ISG-enabled インターフェイス上のトラフィックをフィルタリングするには、ACL を適用した後、必ず ISG をクリアしてください。

Cisco 10000 シリーズ ルータでは、アクセス インターフェイス上で VRF インスタンスが変更されたときに、既存のセッションが終了されます。

Cisco 7600 ルータに関する制約事項

Cisco IOS Release 12.2(33)SRC では、Cisco 7600 ルータは、次のアクセス インターフェイス上で IP 加入者セッションをサポートしません。

- Gigabit EtherChannel（ポート チャネル）
- スイッチ仮想インターフェイス
- Generic Routing Encapsulation（GRE）
- PPP
- Layer 2 Tunnel Protocol（L2TP）

Shared Port Adapter Interface Processor（SIP2）Network Processor（NWP）は、アクセス インターフェイス、ネットワーク インターフェイス、およびマルチサービス インターフェイス上で ISG 加入者トラフィック用に設定された IP 機能をサポートしません。

加入者冗長性とロード バランシングは、IP 加入者に対してはサポートされません。

Cisco IOS Release 12.2(33)SRE 以降のリリースでは、Cisco 7600 ルータは、SIP400 および ES+ ラインカード上でのみ、および次のインターフェイス上でのみ IP 加入者セッションをサポートします。

- SIP400 ラインカード上のメイン インターフェイスとアクセスタイプ サブインターフェイス
- Ethernet Services Plus（ES+）ラインカード上のメイン インターフェイスとすべてのタイプのサブインターフェイス
- ES+ ラインカード上のポートチャネル インターフェイス

Cisco 7600 ルータには、ラインカード単位およびルータ シャーシ単位の IP 加入者セッション数に制限があります。アクティブなセッション数が次の制限を超えると、エラー メッセージが表示されます。

- Cisco 7600 シャーシ : 32,000 加入者セッション（Cisco IOS Release 12.2(33)SRE1 以降のリリースでサポート）
- ES+ ラインカード : ポート グループごとに 4000 加入者セッション、ラインカードごとに 16,000 セッション（Cisco IOS Release 12.2(33)SRE 以降のリリースでサポート）
- SIP400 ラインカード : 8000 加入者セッション（Cisco IOS Release 12.2(33)SRD4 以降のリリースでサポート）

IP 加入者セッションのための ISG アクセスに関する情報

IP 加入者セッションのタイプ

ISG は、次の 3 タイプの IP 加入者セッションをサポートします。

IP セッション

IP セッションには、単一の加入者 IP アドレスに関連付けられたすべてのトラフィックが含まれます。IP アドレスがシステムに固有でない場合は、VRF や MAC アドレスなど、他の識別特性によってセッションの ID の一部が形成されます。ISG は、DHCP パケット、未分類の IP アドレスまたは MAC アドレスを持つパケット、または RADIUS パケットの受信時に、IP セッションを作成するように設定できます。詳細については、「IP 加入者セッションの開始」（P.73）を参照してください。

IP セッションは、接続されている加入者デバイス（ISG から 1 ルーティング ホップ）、またはゲートウェイから 2 ホップ以上の加入者デバイスに対してホストされます。

IP インターフェイス セッション

IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成され、インターフェイスがシャットダウンされてもセッションを継続します。デフォルトでは、IP インターフェイス セッションは、完全なネットワーク アクセス権を持つ「unauthenticated」状態で開始します。

IP インターフェイス セッションは、加入者がインターフェイスで表現され（PPP を除く）、複数の IP アドレスを使用して通信する状況で使用される場合があります。たとえば、Routed Bridge Encapsulation（RBE; ルーテッド ブリッジ エンカプセレーション）を使用する加入者は、複数の PC をサポートする家庭用 Customer Premises Equipment（CPE; 顧客宅内機器）への専用の ATM Virtual Circuit（VC; 仮想回線）を持っている場合があります。

IP サブネット セッション

IP サブネット セッションは、単一の IP サブネットに関連付けられているすべてのトラフィックを表します。IP サブネット セッションは、特定の IP サブネットに関連付けられているパケットへの均一なエッジ処理の適用に使用されます。IP サブネット セッションが設定されている場合、ISG は、そのサブネットを単一の加入者として取り扱います。これは、ISG の機能および機能性が、サブネット トラフィックに集約として適用されることを意味しています。

IP サブネット セッションは、ルーテッド IP 加入者トラフィック用にサポートされています。

IP サブネット セッションは IP セッションと同じ方法で作成されますが、加入者が認可または認証されていて、Framed-IP-Netmask アトリビュートがユーザ プロファイルまたはサービス プロファイルに存在する場合に、ISG が発信元 IP に基づくセッションを、Framed-IP-Netmask アトリビュート内にサブネット値を持つサブネット セッションに変換する点が異なります。

（注） 入力インターフェイスが単一のサブネットにマップされる場合、サブネットは、IP インターフェイス セッションで調整される場合があります。ただし、ISG が加入者から 2 ホップ以上離れている場合、および同じインターフェイスを通して複数のサブネットにアクセスする可能性がある場合には、トラフィックを識別し、各サブネットに適切なエッジ機能性を適用するように IP サブネット セッションを定義できます。

マルチキャスト セッションと IP セッションの共存

ISG セッション マルチキャスト共存機能では、Cisco 7600 シリーズ ルータの同じサブインターフェイス上でマルチキャストおよび IP セッションが共存できるようにして、同じ VLAN 上ですべての加入者とサービス（データとマルチキャスト）をホストする機能が導入されます。ISG IP セッションは、非アクセスタイプのサブインターフェイスでサポートされます。既存のセッションがある場合、またはセッションが存在しない場合であっても、このサポートがあると、IP セッション用に設定されたインターフェイスをマルチキャスト トラフィックが、セッションを作成することなくアップストリームとダウンストリームの両方向で通過し易くなります。

IP 加入者の接続

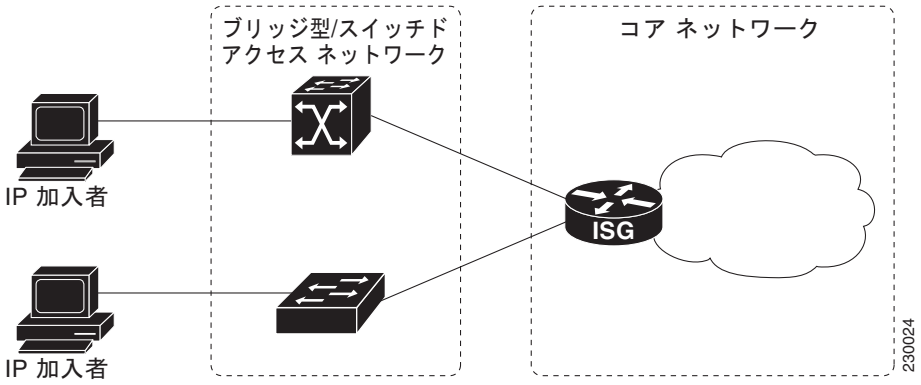
IP 加入者は、レイヤ 2 接続されたアクセス ネットワークまたはルーテッド アクセス ネットワークのいずれかを通して ISG に接続します。ここでは、次のタイプの IP 加入者接続について説明します。

- 「レイヤ 2 接続されたアクセス ネットワーク」（P.72）
- 「ルーテッド アクセス ネットワーク」（P.73）

レイヤ 2 接続されたアクセス ネットワーク

レイヤ 2 接続された加入者は、ISG の物理インターフェイスに直接接続されるか、またはブリッジ型ネットワークやスイッチド ネットワークなどのレイヤ 2 アクセス ネットワークを通して ISG に接続されます。レイヤ 3 フォワーディングは存在しないか、または加入者トラフィックをレイヤ 2 アクセス ネットワーク内で誘導するためには使用されません。加入者の IP アドレスは、レイヤ 2 接続された物理インターフェイスと同じサブネット内に存在する場合も、また存在しない場合もあります。図 2 に、レイヤ 2 接続されたアクセス ネットワークの例を示します。

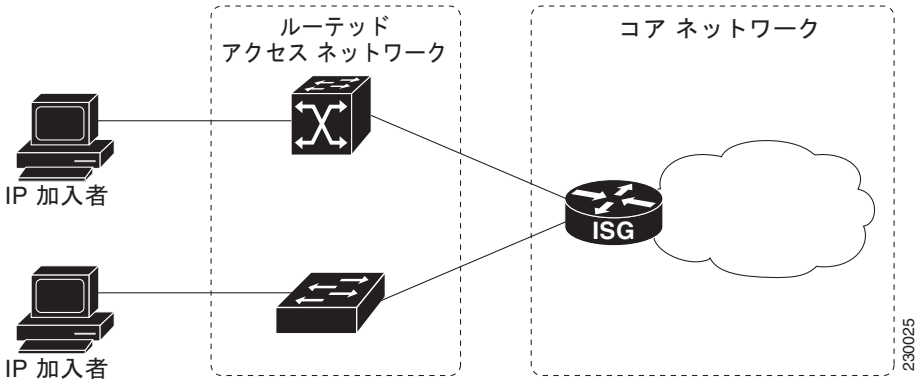
図 2　レイヤ 2 接続されたアクセス ネットワーク



ルーテッド アクセス ネットワーク

ルーテッド加入者トラフィックは、ISG に到達する前に、少なくとも 1 台の中継ルータがあるレイヤ 3 アクセス ネットワークを通してルーティングされます。加入者の IP アドレスは、少なくともレイヤ 3 アクセス ネットワーク内でルーティング可能です。レイヤ 3 アクセス ネットワークには、単一のルーティング ドメインが含まれており、したがって重複する IP アドレスをサポートしません。図 3 に、ルーテッド アクセス ネットワークの例を示します。

図 3　ルーテッド アクセス ネットワーク



IP 加入者セッションの開始

ISG は、インターフェイス上の IP セッションまたは IP サブネット セッションの開始を表す、次のイベントの 1 つ以上を許可するよう設定できます。

- DHCP DISCOVER パケット

  次の条件と一致する場合、DHCP DISCOVER パケットを受信すると、IP セッションの作成がトリガーされます。

  - ISG は、新しい IP アドレスの割り当てに関して DHCP リレーまたはサーバとして機能します。
  - 加入者は、DHCP 用に設定されます。
  - DHCP DISCOVER パケットは、加入者から受信する最初の DHCP 要求です。

- 未分類の発信元 IP アドレス

  ルーテッド IP 加入者に関しては、未分類の発信元 IP アドレスを持つ IP パケットが出現することにより、新しい IP セッションがトリガーされます（その IP アドレスに対して、IP セッションがまだ存在しないことを意味しています）。

- 未分類の発信元 MAC アドレス

  レイヤ 2 接続された IP 加入者に関しては、未分類の発信元 MAC アドレスを持つ IP パケットが出現することにより、新しい IP セッションがトリガーされます（その MAC アドレスに対して、IP セッションがまだ存在しないことを意味しています）。

- RADIUS Access-Request パケット

  ルーテッド アクセスまたはレイヤ 2 接続されたアクセスに関しては、ISG が RADIUS プロキシとして機能しているときに RADIUS Access-Request パケットが出現することにより、新しい IP セッションがトリガーされます。

IP 加入者のアドレッシング

ISG が IP 加入者の IP アドレッシングを処理する方法については、次の項を参照してください。

- 「ISG 加入者 IP アドレスの割り当て方法」（P.74）
- 「パブリック IP アドレスとプライベート IP アドレス」（P.75）
- 「IP アドレスの重複」（P.76）
- 「DHCP を使用した ISG 加入者 IP アドレスの割り当て」（P.76）

ISG 加入者 IP アドレスの割り当て方法

IP 加入者は、IP アドレスを静的に設定するか、または IP アドレスを割り当てる機能を持つ何らかのネットワーク プロトコルで動的に取得します。加入者は、特定の IP サービス ドメイン内でルーティングを受けるためには、ドメイン固有の IP アドレスをネットワークに知らせる必要があります。加入者が IP サービス ドメイン（アクセス プロバイダーによって管理される任意のプライベート ドメインを含む）間を移動する場合は、ネットワークに知らせる IP アドレスを、新しいドメインを反映して変更する必要があります。

ここでは、ISG が各タイプのレイヤ 3 セッション用にサポートする IP アドレスの割り当て方法について説明します。

- 「IP インターフェイス セッション」（P.74）
- 「IP セッション」（P.75）
- 「IP サブネット セッション」（P.75）

IP インターフェイス セッション

IP インターフェイス セッションに関しては、ISG は、加入者 IP アドレスの割り当てに関与（または認識）しません。

IP セッション

IP セッションに関して、ISG は、次の IP アドレスの割り当て方法をサポートします。

- スタティック IP アドレス

  加入者のスタティック IP アドレスがサービス ドメインに対して正しく設定されている場合、ISG は、その加入者の IP アドレスを割り当てる必要がありません。

- DHCP

  IP アドレスの割り当てに DHCP が使用されている場合で、DHCP によって割り当てられた IP アドレスがサービス ドメインに対して正しい場合、ISG は、その加入者の IP アドレスを割り当てる必要がありません。

  DHCP によって割り当てられた IP アドレスがサービス ドメインに対して正しくない場合、または VRF 転送によってドメインが変更された場合、ISG は、DHCP IP アドレスの割り当てに関与するように設定できます。

  ISG が DHCP IP アドレスの割り当てに関与するためには、次の条件を満たす必要があります。

  - 加入者が、レイヤ 2 接続されている。
  - ISG デバイスが、DHCP サーバまたはリレーとして機能することにより、DHCP 要求のパス内に存在する。
  - 加入者が、静的に設定された IP アドレスを持つ。

  これをサポートした展開では、推奨される IP アドレスの割り当て方法が DHCP になります。

IP サブネット セッション

IP サブネット セッションでは、ユーザ プロファイルに IP サブネットが指定されます。

パブリック IP アドレスとプライベート IP アドレス

IP 加入者にどのように IP アドレスが割り当てられても、その IP アドレスは、パブリック IP アドレスか、プライベート IP アドレスのカテゴリに入ります。IP 加入者にプライベート IP アドレスが割り当てられ、加入者がインターネットに到達する必要がある場合、加入者とインターネットの間にある ISG やファイアウォールなどのレイヤ 3 ゲートウェイは、加入者のプライベート IP アドレスに対して NAT を実行する必要があります。

アクセス ネットワークがレイヤ 2 接続されたネットワークの場合、加入者 IP アドレスは、アクセス インターフェイスに対してネイティブでも外部でもかまいません。ネイティブ加入者 IP アドレスは、アクセス インターフェイス上でプロビジョニングされたサブネットに属するアドレスです。外部加入者 IP アドレスは、アクセス インターフェイス上でプロビジョニングされたサブネットに属さないアドレスです。リテール ISP が自分の IP アドレス割り当てから IP アドレスを IP 加入者に割り当てたが、それがホールセール ISP とは異なる場合、またはホーム アクセス ネットワーク内でネイティブなスタティック IP アドレスを持つ IP 加入者が外部アクセス ネットワークに移動した場合、外部加入者 IP アドレスになる可能性があります。外部 IP アドレスを持つ外部 IP 加入者をサポートするには、ISG は、ISG 自身の MAC アドレスを持つ外部 IP アドレスから送信される Address Resolution Protocol（ARP; アドレス解決プロトコル）要求に応答する必要があります。アクセス ネットワークはレイヤ 2 接続されているため、ISG は、すべての加入者との隣接関係を維持します。

アクセス ネットワークがルーテッド ネットワークの場合、加入者 IP アドレスは、アクセス ネットワーク内でルーティング可能になっている必要があります。ルーティングできない場合、加入者トラフィックは ISG に到達できません。この場合、ISG は各加入者と隣接関係を持てませんが、登録者へのネクストホップという隣接関係を持ちます。ネクストホップは、ISG 上のルーティング プロセスによって決定されます。

IP アドレスの重複

アクセス ネットワークが VPN 機能なしで展開されている場合、アクセス ネットワーク内の IP アドレス空間は、すべての IP 加入者に共有されます。IP アドレスが動的に割り当てられる場合、これらのアドレスが重複しないように注意する必要があります。重複する IP アドレスが意図的に IP 加入者に割り当てられた場合、アクセス ネットワークは、レイヤ 2 分離メカニズムを使用して IP アドレス空間を区別する必要があります。たとえば、アクセス ネットワークは、各 IP アドレス空間を別々の VLAN に置くことができます。

アクセス ネットワークがローカル IP 加入者とローミング ユーザの両方に対して処理を行う場合、ローミング加入者のスタティック プライベート IP アドレスが、別の加入者のネイティブ プライベート IP アドレスと重複する可能性があります。たとえば、一般にはダイナミック IP アドレスを割り当てるパブリック ワイヤレス ホット スポットが、一時的なローミング ユーザに、静的に設定された IP アドレスでアクセスを提供する場合があります。この特殊な重複状態をサポートするには、すべての IP 加入者は、重複する MAC アドレスの存在しない、レイヤ 2 接続されたアクセス ネットワークに属している必要があります。この場合、IP 加入者は、MAC アドレスを使用して区別できます。

DHCP を使用した ISG 加入者 IP アドレスの割り当て

ISG が（DHCP サーバまたは DHCP リレーのどちらかとして）DHCP 要求のパス内にある場合、ISG が、加入者 IP アドレスの割り当てに使用される IP アドレス プールと DHCP サーバに影響を与えることがあります。加入者に割り当てられている IP アドレスに影響する ISG をイネーブルするには、DHCP アドレス プール クラスをアドレス ドメインに関連付けます。DHCP アドレス プール クラスも、加入者に関連付けられたサービス ポリシー マップ、サービス プロファイル、またはユーザ プロファイルで設定する必要があります。加入者から DHCP 要求を受信すると、DHCP は、加入者に関連付けられたアドレス プール クラスを使用して、要求に対するサービスに使用する DHCP アドレス プールを決定します。その結果、IP アドレスは、要求単位で、ローカル DHCP サーバによって提供されるか、または選択されたプールに定義されたリモート DHCP サーバにリレーされます。

IP 加入者 ID

ISG は、IP セッションの作成時に IP 加入者を一意に識別する必要があるため、IP 加入者 ID は、IP セッションの開始と密接に関連しています。ただし、IP 加入者を識別する必要性は、セッションの開始フェーズの後で発生します。ここでは、ISG が IP 加入者を一意に識別する方法について説明します。

- 「ルーテッド IP 加入者 ID」（P.76）
- 「セカンダリ ID としての MAC アドレス」（P.77）
- 「DHCP リース クエリーのサポート」（P.77）
- 「レイヤ 2 接続された IP 加入者 ID」（P.78）
- 「インターフェイス IP 加入者 ID」（P.78）

ルーテッド IP 加入者 ID

定義により、加入者 IP アドレスは少なくともアクセス ネットワーク内でルーティング可能になっている必要があるため、アクセス ネットワークがルーテッド ネットワークの場合、加入者 IP アドレスを使用して IP 加入者を一意に識別できます。

加入者 IP アドレスを識別方法として使用する場合、ISG は加入者 IP アドレスが一意であると見なします。また、アクセス ネットワークがレイヤ 3 ロード バランシング、冗長性、または非対称ルーティングで展開されている場合、ISG は、同じ IP 加入者からの IP トラフィックが異なるアクセス インター

フェイスに到着すると見なします。このタイプの展開をサポートするため、ISG は、同じアクセス ネットワークに接続されているすべてのアクセス インターフェイス用として、単一の IP アドレス空間を想定します。

単一の物理アクセス ネットワーク上で、複数の IP アドレス空間をサポートする必要がある場合、アクセス ネットワークは、何らかのレイヤ 2 カプセル化を使用して、各 IP アドレス空間に個別の論理アクセス ネットワークを作成する必要があります。この場合でも、ISG は、論理アクセス ネットワークに接続するすべての論理アクセス インターフェイスに対して、単一の IP アドレス空間を持つことができます。

加入者 IP アドレスがプライベート IP アドレスの場合、アクセス ネットワークは、それらの加入者トラフィックをルーティング可能になっている必要があります。加入者トラフィックがインターネット宛ての場合は、NAT を実行する必要があります。

ルーテッド IP 加入者に関して、加入者 IP アドレスは IP セッションのキーとして機能します。ISG は、IP トラフィックを次のように IP セッションに関連付けます。

- アップストリーム方向では、IP パケットの発信元 IP アドレスが IP セッションの識別に使用されます。発信元 IP アドレスは、加入者 IP アドレスです。
- ダウンストリーム方向では、IP パケットの宛先 IP アドレスが IP セッションの識別に使用されます。宛先 IP アドレスは、加入者 IP アドレスです。

IP 加入者が VPN ユーザの場合、加入者 IP アドレスは ISG 上のグローバル ルーティング テーブルおよび VPN ルーティング テーブルの両方でルーティング可能になっている必要があります。

IP サブネット加入者の場合、加入者 IP アドレスは、/32 の IP ホスト アドレスではなく、IP プレフィクス アドレスとして定義されます。この IP プレフィクスは、エンド ユーザが使用する IP アドレス範囲をカバーしますが、ISG から見ると単一の論理 IP 加入者を表しています。この展開では、すべてのエンド ユーザが、ISG から提供される同じ接続およびサービスを共有します。

異なるネットワーク マスクを持つ IP 加入者の分類を正規化するため、ISG は、ネットワーク マスクとルーテッド IP 加入者の加入者 IP アドレスを組み合せて使用します。

セカンダリ ID としての MAC アドレス

セッションの開始時に、**collect identifier mac-address** コマンドを設定する必要があります。このコマンドは、ISG デバイスに対して、MAC アドレスをセッション ID の一部として格納するよう指示します。ルーテッド IP 加入者セッションに関して、MAC アドレスは、DHCP リース クエリー プロトコルを使用して、DHCP サーバから収集されます。コマンド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。

DHCP リース クエリーのサポート

DHCP リース クエリー メッセージは、DHCP リレー エージェントから DHCP サーバに送信される DHCP メッセージ タイプです。DHCP リース クエリー対応リレー エージェントは、IP エンドポイントの場所を DHCP リース クエリー メッセージに送信します。

DHCP リース クエリー トランザクションは、特別なメッセージ タイプを持つ DHCP トランザクションです。これにより、クライアントは、IP アドレスのオーナーおよびリースの有効期限に関して、DHCP サーバに問い合わせることができます。リース クエリーのための DHCP サーバの設定の詳細については、「DHCP サーバの IP アドレスの設定」（P.102）を参照してください。

レイヤ 2 接続された IP 加入者 ID

レイヤ 2 接続されたアクセス ネットワークは、ネイティブ IP アドレスを持つ IP 加入者に加えて、外部 IP アドレスおよび重複する IP アドレスを持つ IP 加入者に対して IP 接続を提供できます。そのようなアクセス ネットワークでは、加入者 IP アドレスが一意ではない可能性があり、ISG は加入者がどの種類の IP アドレスを持っているかにかかわらず、加入者 MAC アドレスを使用してレイヤ 2 接続された IP 加入者を識別します。

プライベート IP アドレスまたは重複する IP アドレスを持つ、IP 加入者のインターネット宛てのトラフィックは、NAT の対象となります。

レイヤ 2 接続された IP 加入者に関して、加入者 MAC アドレス（VLAN 内で一意）および IP アドレスの両方が IP セッションのキーとして使用されますが、それらのキーは使用される方向が異なります。

- アップストリーム方向では、IP パケットの VLAN ID と発信元 MAC アドレスが IP セッションの識別に使用されます。
- ダウンストリーム方向では、IP パケットの宛先 IP アドレスと VLAN ID の両方が、IP 加入者コンテキストの識別に使用されます。

インターフェイス IP 加入者 ID

アクセス インターフェイスが IP 加入者の識別に使用されると、各アクセス インターフェイスが単一の IP 加入者に対応します。アクセス インターフェイスが利用可能になり次第、ISG は、インターフェイスをキーとして使用して IP セッションを作成し、このインターフェイスのすべての送受信 IP トラフィックを IP セッションに関連付けます。

IP トラフィックと IP 加入者を正確に関連付けるため、ISG は、IP 加入者を識別する方法としてインターフェイスを使用するように設定する必要があります。その後 ISG は、次のように IP トラフィックを分類します。

- アクセス ネットワーク（アップストリーム方向）から IP トラフィックを受信すると、ISG は入力インターフェイスを使用して IP セッションを識別します。
- コア ネットワーク（ダウンストリーム方向）から IP トラフィックを受信すると、ISG は、出力インターフェイスを使用して IP セッションを識別します。

IP 加入者の VPN 接続とサービス

ここでは、ISG IP 加入者の VPN 接続とサービスについて説明します。

加入者 VPN メンバシップ

IP 加入者は、展開要件に基づいて VPN サービスを持つ場合と持たない場合があります。VPN サービスを持たない場合、IP 加入者は、常に 1 つの VPN ドメインにのみ属している可能性があります。IP 加入者は、次のいずれかの方法で VPN ドメインに関連付けられています。

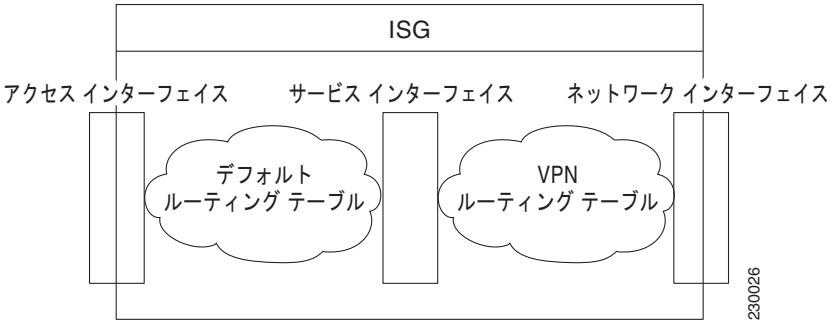
- スタティック VPN 割り当て : VPN IP 加入者はスタティック VPN ドメインに属しています。IP 加入者は、ISG に接続すると、事前に割り当てられた VPN ドメインに配置されます。
- ダイナミック VPN 選択 : VPN IP 加入者は、ダイナミック サービス ログインを通して、異なる VPN ドメインの中からドメインを選択および切り換え可能です。新しい VPN ドメインが選択されると、新しい VPN ドメインの VPN サービスが IP 加入者に適用される前に、現在の VPN ドメインの VPN サービスを削除する必要があります。

  ダイナミック VPN 選択は、セッションの開始時に VRF がダウンロードされ加入者セッションに適用される自動サービス ログインを通して開始するか、または選択されたサービスに対応する VRF に加入者が転送される Web ポータルの加入者サービス選択を通して開始できます。

マルチサービス インターフェイス モデル

スタティック VPN 設定を持たない加入者に関しては、ISG デバイス上でマルチサービス インターフェイスが VRF に IP セッションをマップするように設定する必要があります。マルチサービス インターフェイスは、VPN ルーティング ドメインとデフォルト ルーティング ドメインの間の境界を表します。IP 加入者が接続期間全体を通じて複数のルーティング ドメインに関連付けられる可能性がある場合、マルチサービス インターフェイスは、1 つの VPN ドメインから別の VPN ドメインに切り換える IP 加入者の境界ポイントとして機能します。1 つのマルチサービス インターフェイスが、各ルーティング ドメイン用に設定されている必要があります。図 4 に、マルチサービス インターフェイス モデルを示します。

図 4　　マルチサービス インターフェイス モデル



VPN アドレッシング

加入者セッションがある VPN ドメインから別のドメインに転送されると、そのセッションは実質的に新しいアドレッシング ドメインに属します。このドメインは、加入者の以前のドメインと重複する場合も、重複しない場合もあります。それに従って、パケットがサービス ドメイン内から正しくルーティング バックされるように、加入者のネットワーク側アドレスを変更する必要があります。

Web ポータルとの対話なしでは加入者の ID および加入サービスを判断できない場合は、VRF 転送が必要です。IP パケットがポータル サーバとの間でルーティングされるためには、少なくとも開始時にローカル ルーティング コンテキストが必要です。ポータルベース サービスの選択に従い、加入者は、

通常、選択されたサービス ドメインに関連付けられている VRF に転送される必要があります。また、VRF 転送に従い、加入者は、新しいドメイン内でルーティング可能なアドレスを受け取る必要があります。

ISG が加入者デバイスと隣接し、DHCP リレーまたはサーバとして機能している場合は、DHCP を使用して加入者にドメイン固有のアドレスを割り当てられます。

VRF 転送をサポートするには、DHCP を短い初期リースで設定するよう強く推奨します（既存の加入者アドレスを変更できるのは、現在のリース期限が切れたときだけです）。加入者は、次の DHCP の更新要求を受信するまで、選択したドメインにアクセスできません。短い初期リース期間を使用することにより、VRF の変更と DHCP の更新の間隔が最小になります。長いリース期間を使用する場合、IP アドレス変更は、アウトオブバンド方式を実装して開始する必要があります。

加入者デバイスで、新しいアドレスの割り当てに DHCP を使用できる場合は、転送の実行にサブネットベース VRF 選択を使用できます。サブネットベース VRF 選択（*VRF の自動分類* とも呼ばれる）は、発信元 IP サブネット アドレスに基づいて、入力ポートで VRF を選択する機能です。

サービス プロバイダーおよび組織は、元々重複していないパブリック IP アドレス ブロックを割り当てています。したがって、パブリック IP アドレスが割り当てられる場合、VPN IP 加入者の IP アドレスは重複しません。異なる VPN ドメインの VPN IP 加入者にプライベート IP アドレスが割り当てられると、アクセス ネットワークでアドレスの重複が起こる場合があります。

異なる VPN ドメインの VPN IP 加入者を分割するレイヤ 2 カプセル化が行われない場合、アクセス ネットワークは単一の IP アドレス空間です。したがって、VPN IP 加入者を展開する場合、ISG は、重複する IP アドレスを処理できる必要があります。重複する IP アドレスを持つ VPN IP 加入者による IP 接続は、レイヤ 2 接続されたアクセス ネットワークを介して、ISG に接続された場合のみ可能です。

VPN IP 加入者 ID

ISG は、非 VPN IP 加入者の識別と同じ方法で、VPN IP 加入者を識別します。アップストリーム IP トラフィックは、アクセス ネットワークから VPN に流れる加入者 IP トラフィックとして定義されます（サービス プロバイダー コア ネットワークの最上位に位置）。ダウンストリーム IP トラフィックは、VPN からアクセス ネットワークに送信される加入者 IP トラフィックとして定義されます。

VRF 転送のサービス モデル

プライマリ サービスとは、そのサービス定義にネットワーク転送ポリシー（VRF など）を含むサービスです。1 つのセッションに対して、一度に 1 つのプライマリ サービスだけをアクティブにできます。*セカンダリ* サービスとは、ネットワーク転送ポリシーを含まないすべてのサービスです。

すでにアクティブ化されたプライマリ サービスを持つ加入者が、他のプライマリ サービスを選択しようとすると、ISG は現在のすべてのサービス（現在のプライマリ サービスを含む）を非アクティブ化し、新しいプライマリ サービスをアクティブにすることで、VRF を切り換えます。

すでにアクティブ化されたプライマリ サービスを持つ加入者が、セカンダリ サービスを選択しようとすると、ISG のアクションは、そのセカンダリ サービスがサービス グループの一部かどうかによって異なります。*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。表 5 は、加入者がセカンダリ サービスを選択した場合に、ISG が実行するアクションを示しています。

表 5　セカンダリ サービスの ISG アクティベーション ポリシー

プライマリ サービスの特性	セカンダリ サービスの特性	ISG で行われる動作
サービス グループ アトリビュートのないプライマリ サービス	サービス グループのあるセカンダリ サービス	セカンダリ サービスを起動しない。
	サービス グループのないセカンダリ サービス	セカンダリ サービスを起動する。
サービス グループ アトリビュートのあるプライマリ サービス	異なるサービス グループのあるセカンダリ サービス	セカンダリ サービスを起動しない。
	同じサービス グループのあるセカンダリ サービス	セカンダリ サービスを起動する。
	サービス グループのないセカンダリ サービス	セカンダリ サービスを起動する。

ダイナミック VPN 選択の利点

いわゆる*公平なアクセス ネットワーキング*をサポートする必要がある市場において、ルーティングと転送ドメイン（*ネットワーク サービス*とも呼ばれる）の間で、加入者セッションの切り換えが必要になることがよくあります。公平なアクセス ネットワーキングは、サービス プロバイダーによるリテール加入者ネットワークへの公平なアクセスを、アクセス プロバイダーが可能にしなければならないことを定めた取締規則でしばしば要求されます。ISG ダイナミック VPN 選択は、ネットワーク サービス間での加入者の転送を可能にすることで、公平なアクセス ネットワーキングを促進します。

CoA クライアントに対する VRF-Aware サポート

- ISG は、CoA クライアント（RADIUS サーバ）に対する VRF-aware 機能をサポートしているため、1 台の CoA クライアントが複数の VRF の加入者を処理できます。加入者セッションは、CoA クライアントが設定されているものとは別の VRF 内に存在することも可能です。IP 加入者セッションが別の VRF 内に存在する場合に CoA メッセージを ISG に送信するには、表 6 に示す Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）をセッション ID で使用する必要があります。

表 6　VRF ID VSA の説明

サブアトリビュート ID	アトリビュート タイプ	値	例
250	account-info	S<*subscriber-ip-address*[:vrf-id=*vrf-name*]> • S：加入者 IP のコード • *vrf-name*：Network Access Server（NAS; ネットワーク アクセス サーバ）が加入者 IP アドレスを検索する VRF	Cisco-Account-Info=S10.0.0.3:vrf-id=subscriber_VRF1

次に、VRF の設定例を示します。

RADIUS ユーザ プロファイル

```
simulator radius subscriber 401
 authentication smith pap smith
 vsa cisco 250 S10.0.0.3:vrf-id=subscriber_VRF1
 vsa cisco generic 252 binary 015042484b
```

加入者セッションの検索は、VRF を提供する方式に基づいて行われます。加入者 IP アドレスの検索に使用する VRF を決定する優先順位は、次のとおりです。

1. セッション ID の一部として CoA メッセージ内にある VRF
2. クライアント コンフィギュレーション内にある VRF
3. CoA クライアントが属する VRF

表 7 に、クライアントがサーバに CoA メッセージを送信した場合の、予想される動作を示します。

表 7　　vrf-id アトリビュートを使用した予想される動作

vrf-id がある場所		
CoA メッセージ	CoA クライアント コンフィギュレーション	加入者 IP アドレスが検索される VRF
あり	あり	CoA メッセージ内の VRF
あり	なし	CoA メッセージ内の VRF
なし	あり	クライアント コンフィギュレーション内の VRF
なし	なし	クライアント側インターフェイスのコンフィギュレーション内の VRF
vrf-id=global	なし	サーバ上のグローバル ルーティング テーブル内の VRF

IP セッションの終了

IP セッションは次のいずれかの方法で終了されます。

- DHCP リースの期限切れまたはクライアントからの DHCP 解除

  DHCP を使用して新しいセッションが検出される場合、その分離も DHCP イベントによって通知されることがあります。

- application stop

  セッションを終了するために使用されるアプリケーション コマンドです。**application stop** コマンドは、通常、加入者が Web ポータルからアカウント ログオフを開始する場合に、セッションを終了するために使用されます。アプリケーションの停止は、管理者が加入者の悪質な行動に対応するために起こすアクションなど、管理者のアクションによって引き起こされる可能性もあります。

- アイドル タイムアウトとセッション タイムアウト

  アイドル タイムアウトとセッション タイムアウトは、IP セッションの終了を検出または強制するために使用できます。

- 制御ポリシー

  「サービス切断」アクションを含む制御ポリシーは、セッションを終了するために使用できます。

DHCP-Initiated IP セッションの IP セッション回復

IP セッションが終了した場合（アカウントのログオフまたはセッションのタイムアウトなど）、または IP セッションが失われた場合（ルータのリロードなど）、クライアントは引き続き有効期限内の DHCP リースを保持できます。この場合 ISG はセッションの再起動を実行し、DHCP のリース期限が切れるまでクライアントの IP 接続の停止を防止します。セッションの再起動イベントが発生した場合、ISG が実行するアクションの定義する制御ポリシーを設定できます。ポリシーが定義されていない場合は、デフォルトのポリシーが有効になります。デフォルトのポリシーでは、ISG はセッションの再起動の 60 秒後にセッションを接続解除し、次の設定に相当します。

```
policy-map type control GLOBAL
 class type control always event session-restart
  1 service disconnect delay 60
```

このデフォルト ポリシーは、次の **show subscriber policy rules** コマンドの出力に表示されます。

```
Rule: internal-rule-session-restart
 Class-map: always event session-restart
  Action: 1 service disconnect delay 60
  Executed: 0
```

IP 加入者セッションのデフォルト サービス

IP セッションは、後続の加入者パケットを適切に処理するために、デフォルト サービスを必要とする場合があります。たとえば、メニュー駆動の認証やサービス選択を実行可能なキャプティブ ポータルに対して、TCP パケットを許可または強制する場合などがあります。IP セッションに対してデフォルトのサービス ポリシー マップまたはサービス プロファイルを設定して、トラフィックをリダイレクトしたり、セッション ID のための Port-Bundle ホストキー機能をイネーブルにしたり、透過的な自動ログインをイネーブルにできます。

また、デフォルト サービスにはネットワーク サービスも含まれることがあり、加入者が Web ポータルにアクセスし、認証とサービス選択を行えるようになります。

IP 加入者セッションのための ISG の設定方法

ISG レイヤ 3 アクセスを設定するには、次の作業を実行します。

- 「IP 加入者用の ISG セッションの作成」（P.83）（必須）
- 「DHCP を使用した ISG 加入者 IP アドレスの管理」（P.95）（必須）
- 「ISG ダイナミック VPN 選択の設定」（P.103）（必須）
- 「DHCP サーバの IP アドレスの設定」（P.102）（必須）

IP 加入者用の ISG セッションの作成

ISG は、加入者側インターフェイスの IP トラフィック用の IP セッションを作成します。

（注） Cisco 7600 ルータの場合、ISG IP セッションは、アクセス サブインターフェイス上と非アクセス サブインターフェイス上の両方で設定できます。

次の作業では、インターフェイス上で IP セッションをイネーブルにし、セッションを識別する方法を示します。

- 「ルーテッド ISG 加入者用の IP 加入者セッションの作成」（P.84）（必須）
- 「レイヤ 2 接続された ISG 加入者用の IP 加入者セッションの作成」（P.86）（必須）
- 「ISG IP インターフェイス セッションの作成」（P.87）（必須）
- 「ISG スタティック セッションの作成」（P.88）（必須）
- 「ISG IP サブネット セッションの作成」（P.90）（必須）
- 「DHCP-Initiated IP セッションのための IP セッション回復の設定」（P.91）（必須）
- 「ISG IP 加入者セッションの確認」（P.93）（任意）
- 「ISG IP 加入者セッションのクリア」（P.94）（任意）

ルーテッド ISG 加入者用の IP 加入者セッションの作成

ルーテッド IP 加入者とは、ISG に達する前に、少なくとも 1 台の中継ルータがあるレイヤ 3 アクセス ネットワークを通じてルーティングされる加入者です。ルーテッド IP 加入者用の IP セッションを作成するよう ISG 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. **interface** *type number*

   または

   interface *type number* **access**
4. **ip subscriber routed**
5. **initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified ip-address**}
6. **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。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* または **interface** *type number* **access** **例：** `Router(config)# interface GigabitEthernet 1/0/0` または `Router(config)# interface GigabitEthernet 1/0/0.100 access`	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。 • **access**：サブインターフェイスを指定します。
ステップ 4	**ip subscriber routed** **例：** `Router(config-if)# ip subscriber routed`	インターフェイス上でホストされる IP 加入者のタイプを指定し、ISG IP 加入者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	**initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified ip-address**} **例：** `Router(config-subscriber)# initiator dhcp class-aware`	指定されたパケット タイプの受信時に IP 加入者セッションを作成するよう、ISG を設定します。 • **dhcp**：ISG は、DHCP DISCOVER パケットを受信すると IP セッションを開始します。**class-aware** キーワードで DHCP にクラス名を提供することにより、ISG は、HDCP によって割り当てられる IP アドレスに影響を与えることができます。 • **radius-proxy**：ISG は、RADIUS Access-Request パケットを受信すると IP セッションを開始します。 **（注）** RADIUS プロキシ機能は、Cisco 7600 ルータ上ではサポートされません。 • **unclassified ip-address**：ISG は、未分類の IP 発信元アドレスを持つ最初の IP パケットを受信すると IP セッションを開始します。 • このコマンドを複数回入力すると、IP セッションの開始方法を複数指定できます。 **（注）** クライアント IP アドレスの割り当てで、ISG デバイスが DHCP リレーまたは DHCP サーバのどちらかとして機能する場合は、DHCP DISCOVER パケットの受信時に IP セッションを開始するよう、ISG を設定する必要があります。**initiator unclassified ip** コマンド、または **initiator unclassified mac** コマンドではなく、**initiator dhcp** コマンドを設定する必要があります。
ステップ 6	**end** **例：** `Router(config-subscriber)# end`	（任意）特権 EXEC モードに戻ります。

レイヤ 2 接続された ISG 加入者用の IP 加入者セッションの作成

レイヤ 2 接続された加入者は、ISG の物理インターフェイスに直接接続されるか、またはブリッジ型ネットワークやスイッチド ネットワークなどのレイヤ 2 アクセス ネットワークを通して ISG に接続されます。レイヤ 2 接続された IP 加入者用の IP セッションを作成するよう ISG 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. **interface** *type number*
   または
   interface *type number* **access**
4. **ip subscriber l2-connected**
5. **initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified mac-address**}
6. **arp ignore local**
7. **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	**interface** *type number* または **interface** *type number* **access** 例： `Router(config)# interface GigabitEthernet 1/0/0` または `Router(config)# interface GigabitEthernet 1/0/0.100 access`	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。 • **access**：サブインターフェイスを指定します。
ステップ 4	**ip subscriber l2-connected** 例： `Router(config-if)# ip subscriber l2-connected`	インターフェイス上でホストされる IP 加入者のタイプを指定し、ISG IP 加入者コンフィギュレーション モードを開始します。 **（注）** レイヤ 2 接続された加入者用の IP セッションの設定には、**ip subscriber l2-connected** コマンドの使用を推奨します。加入者 IP アドレスがアクセス ドメインでルーティング可能な場合、**ip subscriber routed** コマンドを使用することもできます。

	コマンドまたはアクション	目的
ステップ 5	**initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified mac-address**} 例： `Router(config-subscriber)# initiator unclassified mac-address`	指定されたパケット タイプの受信時に IP 加入者セッションを作成するよう、ISG を設定します。 • **dhcp**：ISG は、DHCP DISCOVER パケットを受信すると IP セッションを開始します。**dhcp** キーワードを使用する場合は **class-aware** キーワードが必要です。 • **radius-proxy**：ISG は、RADIUS パケットを受信すると IP セッションを開始します。 （注） RADIUS プロキシ機能は、Cisco 7600 ルータ上ではサポートされません。 • **unclassified mac-address**：ISG は、未分類の MAC 発信元アドレスを持つ最初の IP パケットを受信すると IP セッションを開始します。 • このコマンドを複数回入力すると、IP セッションの開始方法を複数指定できます。 （注） クライアント IP アドレスの割り当てで、ISG デバイスが DHCP リレーまたは DHCP サーバのどちらかとして機能する場合は、DHCP DISCOVER パケットの受信時に IP セッションを開始するよう、ISG を設定する必要があります。**initiator unclassified ip** コマンド、または **initiator unclassified mac** コマンドではなく、**initiator dhcp** コマンドを設定する必要があります。
ステップ 6	**arp ignore local** 例： `Router(config-subscriber)# arp ignore local`	（任意）同じインターフェイス上で、ISG が、宛先の着信 Address Resolution Protocol（ARP; アドレス解決プロトコル）要求に応答しないようにします。
ステップ 7	**end** 例： `Router(config-subscriber)# end`	（任意）特権 EXEC モードに戻ります。

ISG IP インターフェイス セッションの作成

ISG IP インターフェイス セッションは、指定されたインターフェイスまたは指定されたサブインターフェイスを通るすべての IP パケットを対象とします。ISG IP インターフェイス セッションを作成するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*[**.***subinterface-number*]
4. **ip subscriber interface**
5. **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	**interface** *type number*[*.subinterface-number*] 例： `Router(config)# interface ethernet 0/0.1`	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	**ip subscriber interface** 例： `Router(config-if)# ip subscriber interface`	インターフェイス上でホストされる IP 加入者のタイプを指定します。
ステップ 5	**end** 例： `Router(config-if)# exit`	（任意）特権 EXEC モードに戻ります。

ISG スタティック セッションの作成

ISG スタティック セッション作成機能では、管理者が開始したスタティック IP セッションが可能になります。ISG スタティック セッションでは、CLI からスタティック IP セッションを設定できます。スタティック IP セッションは、サーバ アドレスのグループを設定することによって作成できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip subscriber list** *list-name*
4. **ip source** *ipaddress* **mac** *macaddress*
   または
   ip source *ipaddress* **mask** *subnetmask*
5. **exit**
6. **interface** *type number* または
   interface *type number* **access**
7. **ip subscriber l2-connected**
   または
   ip subscriber routed
8. **initiator static ip subscriber list** *list-name*
9. **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	**ip subscriber list** *list-name* **例：** `Router(config)# ip subscriber list mylist`	IP 加入者リスト名を指定し、サーバ リスト 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	**ip source** *ipaddress* **mac** *macaddress* または **ip source** *ipaddress* **mask** *subnetmask* **例：** `Router(config-server-list)# ip source 209.165.200.225 mac 0.7.f` または `Router(config-server-list)# ip source 209.165.200.225 mask 255.255.255.224`	スタティック サーバ IP アドレスおよび MAC アドレス（L2-connected の場合）、またはサブネット マスク（ルーテッドの場合）を指定します。
ステップ 5	**exit** **例：** `Router(config-server-list)# 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。
ステップ 6	**interface** *type number* または **interface** *type number* **access** **例：** `Router(config)# interface GigabitEthernet 1/0/0` または `Router(config)# interface GigabitEthernet 1/0/0.100 access`	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。 • **access**：サブインターフェイスを指定します。
ステップ 7	**ip subscriber l2-connected** または **ip subscriber routed** **例：** `Router(config-if)# ip subscriber l2-connected` または `Router(config-if)# ip subscriber routed`	インターフェイス上でホストされる IP 加入者のタイプを指定し、ISG IP 加入者コンフィギュレーション モードを開始します。 **（注）** レイヤ 2 接続された加入者用の IP セッションの設定には、**ip subscriber l2-connected** コマンドの使用を推奨します。ただし、加入者 IP アドレスがアクセス ドメインでルーティング可能な場合、**ip subscriber routed** コマンドを使用することもできます。

	コマンドまたはアクション	目的
ステップ 8	**initiator static ip subscriber list list-name** 例： `Router(config-subscriber)# initiator static ip subscriber list mylist`	パケット タイプとして static を指定して IP 加入者セッションを作成し、セッションをリストに追加します。
ステップ 9	**end** 例： `Router(config-subscriber)# end`	（任意）特権 EXEC モードに戻ります。

ISG IP サブネット セッションの作成

IP サブネット セッションは、単一の IP サブネットに関連付けられているすべてのトラフィックを表します。IP サブネット セッションは、特定の IP サブネットに関連付けられているパケットへの均一なエッジ処理の適用に使用されます。IP サブネット セッションが設定されている場合、ISG は、そのサブネットを単一の加入者として取り扱います。これは、ISG の機能および機能性が、サブネット トラフィックに集約として適用されることを意味しています。IP サブネット セッションを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
   または
   interface *type number* **access**
4. **ip subscriber routed**
5. **initiator unclassified ip-address**
6. **end**
7. Framed-IP-Netmask アトリビュートをサービスまたはユーザ プロファイルに追加します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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* または **interface** *type number* **access** **例：** `Router(config)# interface GigabitEthernet 1/0/0` または `Router(config)# interface GigabitEthernet 1/0/0.100 access`	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。 • **access**：サブインターフェイスを指定します。
ステップ 4	**ip subscriber routed** **例：** `Router(config-if)# ip subscriber routed`	インターフェイス上でホストされる IP 加入者のタイプを指定し、ISG IP 加入者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	**initiator unclassified ip-address** **例：** `Router(config-subscriber)# initiator unclassified ip-address`	未分類の IP 発信元アドレスを持つ IP パケットを受信すると IP 加入者セッションを作成するように、ISG を設定します。
ステップ 6	**end** **例：** `Router(config-subscriber)# end`	（任意）特権 EXEC モードに戻ります。
ステップ 7	Framed-IP-Netmask アトリビュートをサービスまたはユーザ プロファイルに追加します。	加入者の IP サブネット セッションをイネーブルにします。 • 加入者が認可または認証されていて、Framed-IP-Netmask アトリビュートがユーザ プロファイルまたはサービス プロファイルに存在する場合、ISG は発信元 IP に基づくセッションを、Framed-IP-Netmask アトリビュート内のサブネット値を持つサブネット セッションに変換します。

DHCP-Initiated IP セッションのための IP セッション回復の設定

ISG がセッションを終了またはリロードした後、IP セッションの回復時に特定のアクションを実行するように ISG を設定するには、次の作業を実行します。この作業は、DHCP-Initiated IP セッションにのみ適用されます。

セッション回復のためのポリシーが設定されていない場合、ISG は次のデフォルト ポリシーを適用します。

```
policy-map type control GLOBAL
 class type control always event session-restart
  1 service disconnect delay 60
```

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 session-restart**
5. *action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
6. *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**}}
7. *action-number* **set-timer** *name-of-timer minutes*
8. **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`	制御ポリシーの定義に使用される制御ポリシー マップを作成または変更し、制御ポリシー 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** {*control-class-name* | **always**} **event session-restart** 例： `Router(config-control-policymap)# class type control always event session-restart`	セッションの再起動時に評価される制御クラスを指定し、ポリシー マップ クラス制御コンフィギュレーション モードを開始します。 • 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。

	コマンドまたはアクション	目的
ステップ 5	*action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**} **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。
ステップ 6	*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。
ステップ 7	*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 8	**end** **例：** `Router(config-control-policymap-class-control)# end`	（任意）特権 EXEC モードに戻ります。

ISG IP 加入者セッションの確認

IP 加入者セッションの設定と作成を確認するには、次の作業を実行します。コマンド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 subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]
3. **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]
4. **show platform isg session-count** {**all** | *slot*}

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	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*] 例： `Router# show subscriber session detailed`	加入者セッションの ISG ポリシーおよび ISG 機能に関する情報を表示します。
ステップ 3	**show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]] 例： `Router# show ip subscriber ip 10.10.10.10`	ISG IP 加入者セッションに関する情報を表示します。
ステップ 4	**show platform isg session-count** {**all** | *slot*} 例： `Router# show platform isg session-count all`	アクティブな ISG 加入者セッション数をライン カードごとに表示します。
ステップ 5	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

ISG IP 加入者セッションのクリア

IP 加入者セッションをクリアするには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]
3. **clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]] **例：** `Router# show ip subscriber ip 10.10.10.10`	（任意）ISG 加入者 IP セッションに関する情報を表示します。
ステップ 3	**clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]] **例：** `Router# clear ip subscriber ip 10.10.10.10`	ISG IP 加入者セッションをクリアします。
ステップ 4	**exit** **例：** `Router# exit`	特権 EXEC モードを終了します。

トラブルシューティングのヒント

ISG IP 加入者セッションをトラブルシューティングするには、次のコマンドを使用します。

- **debug ip subscriber**
- **debug condition**

DHCP を使用した ISG 加入者 IP アドレスの管理

この作業を実行するには、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。

- 「DHCP を使用した ISG 加入者 IP アドレスの割り当て」（P.76）

DHCP を使用して ISG 加入者 IP アドレスを管理するには、次の作業を実行します。

- 「ダイナミック DHCP クラス アソシエーションのための ISG インターフェイスの設定」（P.96）（必須）
- 「DHCP サーバ ユーザ認証の設定」（P.97）（必須）
- 「サービス ポリシー マップ内の DHCP クラスの設定」（P.100）（必須）
- 「サービス プロファイルまたはユーザ プロファイル内の DHCP クラスの設定」（P.101）（必須）
- 「DHCP サーバの IP アドレスの設定」（P.102）（必須）

前提条件

ISG が DHCP を使用して IP アドレスを割り当てるためには、次の前提条件があります。

- 加入者が、レイヤ 2 接続されている。
- ISG が DHCP 要求のパス内にあり、DHCP サーバまたはリレーとして機能している。
- 該当する IP サブネットが加入者インターフェイス上で設定されている。

この作業は、ネットワーク内で DHCP が設定されていることを前提としています。

ダイナミック DHCP クラス アソシエーションのための ISG インターフェイスの設定

クラス名を持つローカル DHCP コンポーネントを提供することで、インターフェイス上の加入者への IP アドレスの割り当てに、ISG が影響を与えられるようにするには、次の作業を実行します。クラス名とは、**ip dhcp pool** コマンドを使用して設定されたクラスのことで、アドレスのプールまたはリレーの宛先を参照していてもかまいません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*

   または

   interface *type number* **access**
4. **ip address** *ip-address mask* [**secondary**]
5. **ip subscriber** {**l2-connected** | **routed**}
6. **initiator dhcp class-aware**
7. **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。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* または **interface** *type number* **access** 例： `Router(config)# interface GigabitEthernet 1/0/0` または `Router(config)# interface GigabitEthernet 1/0/0.100 access`	設定用の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。 • **access**：サブインターフェイスを指定します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 209.165.200.225 255.255.0.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 5	**ip subscriber** {**l2-connected** | **routed**} 例： `Router(config-if)# ip subscriber l2-connected`	ISG IP 加入者コンフィギュレーション モードをイネーブルにします。
ステップ 6	**initiator dhcp class-aware** 例： `Router(config-subscriber) initiator dhcp class-aware`	DHCP DISCOVER パケットを受信したときに IP セッションを作成するよう、ISG を設定します。 • **class-aware**：DHCP にクラス名を提供することにより、ISG は、HDCP によって割り当てられる IP アドレスに影響を与えることができます。
ステップ 7	**end** 例： `Router(config-subscriber)# end`	（任意）特権 EXEC モードに戻ります。

DHCP サーバ ユーザ認証の設定

サーバ上で DHCP クライアントを認証するには、次の作業を実行します。

前提条件

DHCP サーバ ユーザ認証をイネーブルにするには、ISG フレームワークを使用する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name* **local**
5. **ip dhcp pool** *pool-name*
6. **network** *network-number mask*

7. **exit**
8. **interface** *type number*
9. **ip subscriber l2-connected**
10. **initiator dhcp class-aware**
11. **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	**aaa new-model** 例： `Router(config)# aaa new model`	Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）をイネーブルにします。
ステップ 4	**aaa authentication login** *list-name* **local** 例： `Router(config)# aaa authentication login mylist local`	ログイン時の AAA 認証を設定します。
ステップ 5	**ip dhcp pool** *pool-name* 例： `Router(config)# ip dhcp pool testpool`	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 6	**network** *network-number mask* 例： `Router(dhcp-config)# network 172.16.0.0 255.240.0.0`	Cisco IOS DHCP サーバ上の DHCP アドレス プールのプライマリまたはセカンダリ サブネットに、ネットワーク番号とマスクを設定します。
ステップ 7	**exit** 例： `Router(dhcp-config)# 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。
ステップ 8	**interface** *type number* 例： `Router(config)# interface Ethernet 0/0`	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。

	コマンドまたはアクション	目的
ステップ 9	**ip subscriber l2-connected** 例： `Router(config-if)# ip subscriber l2-connected`	インターフェイス上でレイヤ 2 接続された IP セッションを設定し、IP 加入者コンフィギュレーション モードを開始します。
ステップ 10	**initiator dhcp class-aware** 例： `Router(config-subscriber)# initiator dhcp class-aware`	DHCP によって開始された IP セッション用の、DHCP のクラスを開始します。
ステップ 11	**end** 例： `Router(config-subscriber)# end`	特権 EXEC モードに戻ります。

トラブルシューティングのヒント

debug ip dhcp server events コマンド、**debug ip dhcp server packet** コマンド、および **debug subscriber policy dpm event** コマンドを使用すると、DHCP 認証を確認できます。次に、**debug subscriber policy dpm event** コマンドの出力例を示します。

```
*Apr 20 20:20:03.510: SG-DPM: DHCP Discover notification from client, mac_address =
001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Could not find a dhcp_context for 001a.7014.c03e:
*Apr 20 20:20:03.510: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.510: SG-DPM: Session Initiation notification on Active
*Apr 20 20:20:03.510: SG-DPM: Allocated SHDB Handle (0xB6000252) for Mac address
001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Client is able to perform DHCP Authentication.Setting the
SSS_INFOTYPE_DHCP_AUTH_KEY
*Apr 20 20:20:03.510: SG-DPM: Sending Session start to PM, mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Request for Classname from client, mac_address =
001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.514: SG-DPM: No session found in ID manager
*Apr 20 20:20:03.514: SG-DPM: Processing sg_dpm_get_more_keys from SSS hdl 56000E52
*Apr 20 20:20:03.514: SG-DPM: DPM is providing Auth-User
```

また、**show subscriber session detailed** コマンドおよび **show ip dhcp binding** コマンドを使用すると、加入者情報と DHCP プール情報を表示できます。次に、**show ip dhcp binding** コマンドの出力例を示します。

```
Router# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.0.1            0100.1a70.1530.38       Nov 18 2008 03:43 PM    Automatic
```

サービス ポリシー マップ内の DHCP クラスの設定

サービス ポリシー マップに DHCP クラスを割り当てるには、次の作業を実行します。このサービス ポリシー マップがアクティブな加入者には、DHCP プールまたはクラスに関連付けられたリモート サーバから、IP アドレスが割り当てられます。

前提条件

DHCP プールが設定されている。DHCP プール内で設定されたクラスと、サービス ポリシー マップ内で設定された DHCP クラスが一致している。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-name*
4. **classname** *class-name*
5. **end**
6. **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	**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-name* 例： `Router(config)# policy-map type service service1`	設定用にサービス ポリシー マップを作成するか、既存のサービス ポリシー マップを指定して、サービス 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	**classname** *class-name* 例： `Router(config-service-policymap)# classname class1`	DHCP プールをサービス ポリシー マップに関連付けます。
ステップ 5	**end** 例： `Router(config-service-policymap)# end`	（任意）特権 EXEC モードに戻ります。
ステップ 6	**show policy-map type service** 例： `Router# show policy-map type service`	（任意）すべてのサービス ポリシー マップの内容を表示します。 • このコマンドを使用して、DHCP クラスがサービス ポリシー マップに関連付けられていることを確認します。

次の作業

サービス ポリシー マップに DHCP アドレス プール クラスを設定後は、制御ポリシーを使用してサービスをアクティブにするなど、サービス ポリシー マップをアクティブにする方法を設定することがあります。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 プロファイルまたはユーザ プロファイル内の DHCP クラスの設定

ユーザ プロファイルまたはサービス プロファイルに DHCP クラスの Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）を追加するには、次の作業を実行します。ユーザ プロファイルまたはサービス プロファイルがアクティブな加入者には、DHCP プールまたはクラスに関連付けられたリモート サーバから、IP アドレスが割り当てられます。

前提条件

DHCP アドレス プールが設定されている。DHCP アドレス プール内で設定されたクラスと、サービス プロファイルまたはユーザ プロファイル内で設定された DHCP アドレス プール クラスが一致している。

手順の概要

1. DHCP クラス アトリビュートを、ユーザ プロファイルまたはサービス プロファイルに追加します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	DHCP クラス アトリビュートを、ユーザ プロファイルまたはサービス プロファイルに追加します。 例： `26,9,1 = "subscriber:classname=class-name"`	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。

次の作業

サービス ポリシー マップまたはサービス 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。

DHCP サーバの IP アドレスの設定

ネットワーク上で使用する DHCP サーバの指定、またはネットワーク上で利用可能な複数の DHCP サーバの IP アドレスの設定、およびルーテッド IP セッションの DHCP リース クエリーの指定を行うには、次の作業を実行します。

（注） DHCP リース クエリーが実行される場合、ルーテッド IP セッションに対して DHCP サーバ IP アドレスを設定する必要があります。

前提条件

- DHCP サーバが DHCP リース プロトコルをサポートしている。
- 電話機の IP アドレスが DHCP アドレス割り当てによって割り当てられている。
- トラフィックがレイヤ 3 として分類されている。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}
4. **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	**ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}} 例： `Router(config)# ip dhcp-server query lease retries 3`	ネットワーク上で利用可能な 1 つまたは複数の DHCP サーバの IP アドレスを設定し、ルーテッド IP セッションの DHCP リース クエリーを指定します。
ステップ 4	**end** 例： `Router(config)# end`	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。

ISG ダイナミック VPN 選択の設定

ISG ダイナミック VPN 選択を設定するには、次の手順を実行します。

- 「マルチサービス インターフェイスの設定」（P.103）（必須）
- 「サービス ポリシー マップでの VRF の指定」（P.104）（必須）
- 「IP セッションの VRF 転送の確認」（P.105）（任意）
- 「IP セッションの VRF 転送のトラブルシューティング」（P.107）（任意）

マルチサービス インターフェイスの設定

マルチサービス インターフェイスを設定するには、次の手順を実行します。

制約事項

IP インターフェイス機能（QoS およびアクセス リストなど）は、マルチサービス インターフェイス上でサポートされません。

1 つのマルチサービス インターフェイスは、1 つの VRF だけに属すことができます。たとえば、次のような設定は機能しません。

```
interface multiservice 1
 ip vrf forwarding VRF_A
!
interface multiservice 2
 ip vrf forwarding VRF_A
```

手順の概要

1. **enable**
2. **configure terminal**
3. **interface multiservice** *interface-number*
4. **ip vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask*
6. **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。

	コマンドまたはアクション	目的
ステップ 3	**interface multiservice** *interface-number* 例： `Router(config)# interface multiservice 1`	ダイナミック VPN 選択をイネーブルにするマルチサービス 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	**ip vrf forwarding** *vrf-name* 例： `Router(config-if)# ip vrf forwarding vrf1`	VPN VRF をインターフェイスまたはサブインターフェイスに関連付けます。
ステップ 5	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.16.0.0 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。 • VPN の IP アドレスを指定します。
ステップ 6	**end** 例： `Router(config-if)# end`	（任意）特権 EXEC モードに戻ります。

サービス ポリシー マップでの VRF の指定

VRF 転送は、新しいプライマリ サービスがセッションに対してアクティブな場合に発生し、セッションが 1 つの VRF から別の VRF に転送されます。サービスは、外部 AAA サーバ上のサービス プロファイル内、または ISG デバイス上のサービス ポリシー マップに設定できます。ISG デバイス上のサービス ポリシー マップに VRF 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. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**
6. **sg-service-group** *service-group-name*
7. **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。

	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 サービスの定義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、サービス 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	**ip vrf forwarding** *name-of-vrf* 例： `Router(config-service-policymap)# ip vrf forwarding vrf1`	サービスを VRF に関連付けます。
ステップ 5	**sg-service-type primary** 例： `Router(config-service-policymap)# sg-service-type primary`	サービスをプライマリ 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。プライマリ サービスは、**sg-service-type primary** コマンドを使用してプライマリ サービスとして定義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。
ステップ 6	**sg-service-group** *service-group-name* 例： `Router(config-service-policymap)# sg-service-group group1`	（任意）ISG サービスをサービス グループに関連付けます。 • 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。
ステップ 7	**end** 例： `Router(config-service-policymap)# end`	（任意）特権 EXEC モードに戻ります。

IP セッションの VRF 転送の確認

IP セッションの VRF 転送を確認するには、必要に応じて次の作業手順を実行します。

手順の概要

1. **enable**
2. **show subscriber session uid** *session-identifier* **detail**
3. **show ip subscriber** [**dangling** *seconds* | **detail** | **ip** *ip-address* | **mac** *mac-address* | **vrf** *vrf-name* [**dangling** *seconds* | **detail** | **ip** *ip-address*]]
4. **show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
5. **show ip route** [**vrf** *vrf-name*]
6. **show ip dhcp binding** [**ip-address**]
7. **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	**show subscriber session uid** *session-identifier* **detail** 例： `Router# show subscriber session uid 4 detail`	特定のセッション ID を持つ ISG 加入者セッションに関する情報を表示します。
ステップ 3	**show ip subscriber** [**dangling** *seconds* | **detail** | **ip** *ip-address* | **mac** *mac-address* | **vrf** *vrf-name* [**dangling** *seconds* | **detail** | **ip** *ip-address*]] 例： `Router# show ip subscriber vrf vrf1`	ISG IP 加入者セッションに関する情報を表示します。
ステップ 4	**show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**} 例： `Router# show idmgr session key nativeip-vrf ip-address 209.165.200.225`	ISG セッションおよびサービス ID に関する情報を表示します。
ステップ 5	**show ip route** [**vrf** *vrf-name*] 例： `Router# show ip route`	ルーティング テーブルの現在のステータスを表示します。
ステップ 6	**show ip dhcp binding** [**ip-address**] 例： `Router# show ip dhcp binding`	Cisco IOS DHCP サーバのアドレス バインディングを表示します。
ステップ 7	**exit** 例： `Router# exit`	特権 EXEC モードを終了します。

IP セッションの VRF 転送のトラブルシューティング

この手順のコマンドを使用すると、IP セッションの VRF 転送をトラブルシューティングできます。コマンドはどの順序で入力してもかまいません。

手順の概要

1. **debug subscriber** {**event** | **error** | **packet** | **policy** | **service**}
2. **debug ip subscriber** {**event** | **error** | **packet** | **fsm** | **all**}
3. **debug subscriber policy dpm** {**error** | **event**}
4. **debug ip dhcp server** {**events** | **packets** | **linkage** | **class**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**debug subscriber** {**event** | **error** | **packet** | **policy** | **service**} 例： `Router# debug subscriber service`	加入者ポリシー、ポリシー サーバ イベント、およびサービスの変更に関するデバッグ メッセージを表示します。
ステップ 2	**debug ip subscriber** {**event** | **error** | **packet** | **fsm** | **all**} 例： `Router# debug ip subscriber error`	サービス ゲートウェイ上で作成される IP セッションに関するデバッグ メッセージを表示します。
ステップ 3	**debug subscriber policy dpm** {**error** | **event**} 例： `Router# debug subscriber policy dpm event`	DHCP イベントに関連する、ポリシー実行についての診断情報を表示します。
ステップ 4	**debug ip dhcp server** {**events** | **packets** | **linkage** | **class**} 例： `Router# debug dhcp ip dhcp server events`	Cisco IOS DHCP サーバのデバッグをイネーブルにします。

次の作業

レイヤ 3 セッションを起動するよう ISG を設定後は、Port-Bundle Host Key 機能、未認証の加入者トラフィックのリダイレクト、または自動加入者ログインなど、加入者 ID および認可のためのポリシーを設定することがあります。ここでは、これらのポリシーを設定する手順について説明します。

- *『Configuring ISG Port-Bundle Host Key』*
- *『Redirecting Subscriber Traffic Using ISG Layer 4 Redirect』*
- *『Configuring ISG Policies for Automatic Subscriber Logon』*

IP 加入者セッションのための ISG アクセス の設定例

ここでは、次の例について説明します。

例：ISG IP インターフェイス加入者

次の例は、イーサネット インターフェイス 0/0 で IP インターフェイス セッションを設定する手順を示しています。

```
interface ethernet 0/0
 ip subscriber interface
```

例：ISG ルーテッド IP 加入者

次の例は、ルーテッド アクセス ネットワークを通じて、ギガビット イーサネット インターフェイス 0/1.401 上で ISG に接続する加入者の IP セッションを作成するための、ISG の設定方法を示しています。ISG は、DHCP DISCOVER パケット、有効な着信 IP パケット、および RADIUS Access-Request パケットを受信すると、IP セッションを作成します。

```
interface GigabitEthernet 0/1.401
 ip subscriber routed
  initiator dhcp class-aware
  initiator unclassified ip-address
  initiator radius-proxy
```

例：ISG レイヤ 2 接続された IP 加入者

次の例は、レイヤ 2 接続されたアクセス ネットワークを通じて、ギガビット イーサネット インターフェイス 0/1.401 上で ISG に接続する加入者用の IP セッションを作成するための、ISG の設定方法を示しています。ISG は、有効な発信元 MAC アドレスを持つ任意のフレームを受信すると、IP セッションを作成します。

```
interface Ethernet 0/0.1
 encapsulation dot1Q 100
 ip unnumbered Loopback1
 ip subscriber l2-connected
  initiator unclassified mac-address
  arp ignore local
```

例：ISG スタティック セッションの作成

次の例は、レイヤ 2 接続されたアクセス ネットワークを通じて、ギガビット イーサネット インターフェイス 0/4 で ISG に接続する加入者用のサーバ 209.165.200.225 に対して、ISG スタティック セッションを作成する方法を示しています。ISG は、有効な発信元 IP アドレスを受信するとスタティック セッションを作成します。

```
ip subscriber list mylist
 ip source 209.165.200.225 mac 0.7.f
interface GigabitEthernet 2/0/0
 ip subscriber l2-connected
  initiator static ip subscriber list mylist
```

例：DHCP-Initiated セッションの回復

次の例は、VRF「FIRST」に属する加入者のセッションの再起動時に、「FIRST-SERVICE」と呼ばれるサービスに適用する ISG ポリシーを設定する方法を示しています。

```
class-map type control TEST
 match vrf FIRST

policy-map type control GLOBAL
 class type control TEST event session-restart
  1 service-policy type service name FIRST-SERVICE
```

例：DHCP クラス対応機能を持つ ISG インターフェイス

次の例は、DHCP Class-Aware 機能を持つギガビット イーサネット インターフェイス 1/0/0.400 を設定する方法を示しています。これで、ISG は、DHCP IP アドレス割り当てに影響を与えることができます。「SERVICE_DHCP」サービスがアクティブな場合、DHCP プール「DHCP_POOL2」がアドレスの割り当てに使用されます。その他の場合には、デフォルトのプール「DHCP_POOL1」が使用されます。

```
interface GigabitEthernet1/0/0.400
 encapsulation dot1Q 400
 ip address 10.1.15.1 255.255.255.0 secondary
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_406a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP_POOL1
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.1
   lease 0 0 30
   class default
!
ip dhcp class default
!
ip dhcp pool DHCP_POOL2
   network 10.1.15.0 255.255.255.0
   default-router 10.1.15.1
   lease 0 0 30
   class DHCP_CLASS2
!
```

```
ip dhcp class DHCP_CLASS2
!
policy-map type service SERVICE_DHCP
 classname DHCP_CLASS2
!
```

例：ISG の DHCP アドレス プール クラスおよびリレー動作

ここでは、ISG の DHCP アドレス プール コンフィギュレーションおよびリレー動作の例を示します。

ISG 設定と DHCP サーバの共存

次の設定例で、ISP1 社と ISP2 社は ISP です。ISP1 社は、On-Demand Address Pools（ODAP）を使用して動的に割り当てられたアドレス プールからアドレスを割り当てます。ISP2 社の顧客アドレスは、アドレス プール 10.100.0.0/16 から割り当てられます。どの ISP にも関連付けられていない顧客は、アドレス プール 10.1.0.0/16 から割り当てられたアドレスを持ち、リース時間は 10 分間に設定されます。

```
!Address pool for ISP1 customers

ip dhcp pool isp1-pool
 origin dhcp
 class isp1
!
!Address pool for ISP2 customers
!
ip dhcp pool def-pool
 network 10.100.0.0 255.255.0.0
 class isp2
!
!Address pool for customers without an ISP
!
ip dhcp pool temp
 network 10.1.0.0 255.255.0.0
 lease 0 0 10
 class default
```

ISG 設定と DHCP リレー エージェントの共存

次の設定例には、「poolA」と「poolB」という 2 つの ISP があります。「poolA」ISP とその顧客は、10.1.0.0/16 から 10.3.0.0/16 の範囲のアドレスを持つことができ、10.55.10.1 の DHCP サーバにリレーされます。「poolB」ISP とそのカスタマーは、10.2.0.0/16 から 10.4.0.0/16 の範囲のアドレスを持つことができ、10.10.2.1 の DHCP サーバにリレーされます。

```
!Address ranges:

interface ethernet1
 ip address 10.1.0.0 255.255.0.0
 ip address 10.2.0.0 255.255.0.0 secondary

interface ethernet2
 ip address 10.3.0.0 255.255.0.0
 ip address 10.4.0.0 255.255.0.0

!Address pools for poolA1 and poolA2:
 ip dhcp pool poolA1
 relay source 10.1.0.0 255.255.0.0
 class poolA1
 relay target 10.55.10.1

!Address pool for poolA2:
```

```
ip dhcp pool poolA2
 relay source 10.3.0.0 255.255.0.0
 class poolA2
 relay target 10.55.10.1

!Address pools for poolB1 and poolB2:

ip dhcp pool poolB1
 relay source 10.2.0.0 255.255.0.0
 class poolB1
 relay target 10.10.2.1

ip dhcp pool poolB2
 relay source 10.4.0.0 255.255.0.0
 class poolB2
  relay target 10.10.2.1
```

リレー用のセキュア ARP の設定では、アドレス プール コンフィギュレーション モードで **update arp** コマンドを使用して、セキュア ARP がすでに DHCP サーバ上で使用したものと同じコンフィギュレーション コマンドが使用されます。システムがこのアドレス プールからアドレスを割り当てる場合は、セキュア ARP が追加されます。システムがこのアドレス プールを使用してパケットをリレーする場合も、セキュア ARP が追加されます。

例：ダイナミック VPN 選択

次の例は、加入者が DHCP グローバル プール「DHCP_POOL1」から、IP アドレスを最初に割り当てられる場合の設定を示しています。加入者が Web ポータルにアクセスして「CorporateVPN」サービスを選択後、ISG が VRF 転送を実行し、加入者は DHCP プール「VPN_POOL1」から新しい IP アドレスを割り当てられます。この場合、単一のマルチサービス インターフェイスが必要です。

```
!
ip vrf VPN_406_1001
rd 406:1001
route-target export 406:1001
route-target import 406:1001
!
interface GigabitEthernet 1/0/0.400
 encapsulation dot1Q 400
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_406a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
ip dhcp relay information trust-all
ip dhcp use vrf connected
!
!!!! Default Global DHCP Pool
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP_POOL1
 network 10.1.10.0 255.255.255.0
 default-router 10.1.10.1
 lease 0 0 30
 class default
!
ip dhcp class default
!
!
```

```
!!! DHCP Pool for CorporateVPN
!
ip dhcp excluded-address 10.1.11.1
!
ip dhcp pool VPN_POOL1
 vrf VPN_406_1001
 network 10.1.11.0 255.255.255.0
 default-router 10.1.11.1
 lease 0 0 30

class DHCP_CLASS_VPN_406_1001

!
interface multiservice 1
 ip vrf forwarding VPN_406_1001
 ip address 10.1.11.1 255.255.255.0
 no keepalive
```

その他の参考資料

ここでは、IP 加入者セッションのための ISG アクセス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
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*』
DHCP の設定	『*Cisco IOS IP Addressing Configuration Guide*』の「*DHCP*」
ISG 制御ポリシー	『*Cisco IOS Intelligent Services Gateway Configuration Guide*』の「Configuring ISG Control Policies」モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco 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
なし	—

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

IP 加入者セッションのための ISG アクセス の機能情報

表 8 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 8 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 8　IP 加入者セッションのための ISG アクセスの機能情報

機能名	リリース	機能情報
DHCP サーバ ユーザ認証	12.2(33)SRE 15.0(1)S	DHCP サーバ ユーザ認証機能は、DHCP クライアントを認証するために使用されます。 Cisco IOS Release 12.2(33)SRE 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。 この機能に関する詳細については、次の項を参照してください。 • 「DHCP サーバ ユーザ認証の設定」（P.97）
DHCP-Initiated IP セッションの IP セッション回復	12.2(31)SB 12.2(33)SRC2	ISG によって、デフォルト ポリシーが提供され、DHCP-Initiated IP セッションの回復後のセッション再起動時に、ISG が行うアクションを決定するポリシーを設定できるようになります。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 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。 • 「DHCP-Initiated IP セッションの IP セッション回復」（P.83） • 「DHCP-Initiated IP セッションのための IP セッション回復の設定」（P.91） この機能によって、次のコマンドが導入または変更されました。**class type control**、**match vrf**

表 8　IP 加入者セッションのための ISG アクセスの機能情報 （続き）

機能名	リリース	機能情報
IP 加入者セッションの CLI アップデート	12.2(31)SB2 12.2(33)SRC	ISG IP 加入者セッションを設定するために使用するコマンドの一部が、変更または置き換えられました。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 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、次の項を参照してください。 • 「IP 加入者セッションのための ISG の設定方法」（P.83） この機能によって、次のコマンドが導入または変更されました。**clear ip subscriber**、**debug ip subscriber**、**identifier interface**、**identifier ip src-addr**、**initiator**、**interface multiservice**、**ip subscriber interface**、**ip subscriber**、**show ip subscriber**
ISG：装置：DHCP リース クエリー サポート	12.2(33)SRE 12.2(33)XNE	DHCP リース クエリー トランザクションとは、特殊なメッセージ タイプがある DHCP トランザクションです。これにより、クライアントは、IP アドレスの所有者とリース有効期間に関して DHCP サーバに問い合わせることなどができます。 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。 • 「IP 加入者 ID」（P.76） • 「DHCP サーバの IP アドレスの設定」（P.102）
ISG：セッション：作成：インターフェイス IP セッション：L2	12.2(28)SB 12.2(33)SRC 12.2SRE	ISG IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成されます。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「ISG IP インターフェイス セッションの作成」（P.87）

表 8　IP 加入者セッションのための ISG アクセスの機能情報 （続き）

機能名	リリース	機能情報
ISG：セッション：作成：インターフェイス IP セッション：L3	12.2(28)SB 12.2(33)SRC 12.2SRE	ISG IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成されます。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「ISG IP インターフェイス セッションの作成」（P.87）
ISG：セッション：作成：IP セッション：プロトコル イベント（DHCP）	12.2(28)SB 12.2(33)SRC	ほとんどの ISG セッションは、すでにアクティブなセッションに関連付けられないデータ フローの検出時に作成されます。ISG は、加入者から最初の DHCP DISCOVER パケットを受信したときに、IP セッションを作成するように設定できます。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「IP 加入者セッションのための ISG の設定方法」（P.83）
ISG：セッション：作成：IP セッション：サブネットおよび発信元 IP：L2	12.2(28)SB 12.2(33)SRC	ISG セッションは、特定のデータ フロー間でサービスとポリシーを関連付けるために使用される主要なコンポーネントです。IP サブネット セッションとは、単一の IP サブネットからの IP トラフィックを含む ISG セッションです。発信元 IP セッションには、単一の発信元 IP アドレスからのトラフィックが含まれます。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「IP 加入者セッションのための ISG の設定方法」（P.83）

表 8　IP 加入者セッションのための ISG アクセスの機能情報 （続き）

機能名	リリース	機能情報
ISG：セッション：作成：IP セッション：サブネットおよび発信元 IP：L3	12.2(28)SB 12.2(33)SRC	ISG セッションは、特定のデータ フロー間でサービスとポリシーを関連付けるために使用される主要なコンポーネントです。IP サブネット セッションとは、単一の IP サブネットからの IP トラフィックを含む ISG セッションです。発信元 IP セッションには、単一の発信元 IP アドレスからのトラフィックが含まれます。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「IP 加入者セッションのための ISG の設定方法」（P.83）
ISG：セッション：マルチキャスト：共存	12.2(33)SRE	ISG セッション マルチキャスト共存機能では、Cisco 7600 シリーズ ルータの同じサブインターフェイス上でマルチキャストおよび IP セッションが共存できるようにして、同じ VLAN 上ですべての加入者とサービス（データとマルチキャスト）をホストする機能が導入されます。 Cisco IOS Release 12.2(33)SRE 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。 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。 • 「マルチキャスト セッションと IP セッションの共存」（P.72） • 「ルーテッド ISG 加入者用の IP 加入者セッションの作成」（P.84） • 「レイヤ 2 接続された ISG 加入者用の IP 加入者セッションの作成」（P.86） • 「ISG IP サブネット セッションの作成」（P.90） • 「ダイナミック DHCP クラス アソシエーションのための ISG インターフェイスの設定」（P.96）

表 8　IP 加入者セッションのための ISG アクセスの機能情報 （続き）

機能名	リリース	機能情報
ISG：セッション：VRF 転送：	12.2(28)SB 12.2(33)SRC	ISG セッションは、特定のデータ フローでサービスとポリシーを関連付けるために使用される主要なコンポーネントです。ネットワーク サービスのためにルーティングが必要な場合、ISG セッションは、Virtual Routing and Forwarding（VRF）インスタンスに関連付けられます。ISG VRF 転送は、仮想ルーティング ドメイン間でアクティブ セッションを動的に切り替える手段を提供します。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「IP 加入者セッションのための ISG の設定方法」（P.83）
ISG：スタティック セッションの作成	12.2(33)SRE 12.2(33)XNE	ISG スタティック セッション作成機能では、管理者が開始したスタティック IP セッションが可能になります。 Cisco IOS Release 12.2(33)SRE 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。 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、次の項を参照してください。 • 「ISG スタティック セッションの作成」（P.88） この機能によって、次のコマンドが導入または変更されました。**initiator static subscriber list**、**ip source**、**ip subscriber list**、**show ip subscriber static list**
CoA クライアントに対する VRF-Aware サポート	12.2(31)SB12	1 台の CoA クライアントが、異なる VRF の ISG 加入者をサポートできます。

IP セッションのための MQC サポートの設定

IP セッションに対する MQC サポート機能では、Cisco Intelligent Services Gateway（ISG）IP セッションでモジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）プロビジョニングを提供します。ローカルで設定したのか、リモート Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバからダウンロードしたのかに関係なく、セッションでモジュラ QoS CLI（MQC）構文の全セットを使用できます。

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、「IP セッションのための MQC サポートの機能情報」（P.127）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

IP セッションのための MQC サポートに関する制約事項

IP セッションのための MQC サポート機能には次の制約事項が適用されます。

- PPP セッションでの IP セッションの作成はサポートされません。

（注） このマニュアルでは、一般的な用語の PPP を使用して、すべてのプロトコル タイプを表します。プロトコルには、PPP over Ethernet（PPPoE）や PPP over ATM（PPPoA）などがあります。サポートされるプロトコルは、プラットフォームに応じて異なります。たとえば、Cisco 7600 シリーズ ルータでは PPPoA や PPP over Ethernet over ATM（PPPoEoA）がサポートされません。Cisco 7600 シリーズ ルータの詳細については、ご使用の Cisco IOS リリースの『*Cisco 7600 Series Cisco IOS Configuration Guide*』を参照してください。

- ポートチャネル リンクのためのアクセス側のインターフェイスの冗長性は、Cisco 10000 シリーズのシステムではサポートされません。Cisco IOS Release 12.2(33)SRE 以降の Cisco 7600 シリーズのシステムでは、ポートチャネル リンクのための 1 対 1 のアクセス側のインターフェイスの冗長性がサポートされますが、Ethernet Services Plus（ES+）ラインカードでのみサポートされます。ただし、コア側の冗長性は Cisco 10000 シリーズと Cisco 7600 シリーズの両方のシステムでサポートされます。
- アップストリーム トラフィックではマーキングとポリシングの機能のみが動作し、ダウンストリーム トラフィックではキューイング、ポリシング、マーキングのすべての MQC 機能が動作します。
- クラスレベルのキューは、セッション ポリシー マップの子レベルでのみ使用できます。その他のすべてのレベルには単一レベルのポリシーが必要で、デフォルトのキューを使用します。
- Cisco 10000 シリーズ システムでは、ATM Virtual Circuit（VC; 仮想回線）を介した IP セッションでポリシー マップのキューイングがサポートされません。ただし、ATM サブインターフェイスでポイントツーポイント インターフェイスのポリシー マップのキューイングを設定できます。
- Gigabit EtherChannel（GEC）を介した IP セッションはサポートされません。
- ISG ポリサーのサポートは Cisco 10000 シリーズ システムでのトラフィック クラス セッションに制限されます。
- IP セッションの負荷を分散できないため、ロード バランシングはどのシステムでもサポートされません。

Cisco 7600 シリーズ システムでの IP セッションのための MQC サポートの制約事項

Cisco 7600 シリーズ システムでの IP セッション機能のための MQC サポートには、次の制約事項が適用されます。

- トラフィック クラスはサポートされません。
- Cisco IOS Release 12.2(33)SRE 以降の Cisco 7600 シリーズのシステムでは、ポートチャネル リンクのための 1 対 1 のアクセス側インターフェイスの冗長性がサポートされますが、これは ES+ ラインカードでしかサポートされません。
- ATM インターフェイスでのセッションはサポートされません。
- IP セッションは、ambiguous IEEE 802.1Q in 802.1Q（QinQ）サブインターフェイスではサポートされません。

IP セッションのための MQC サポートに関する情報

サポートされるインターフェイス

IP セッションでの MQC がサポートされるインターフェイスには、システム別に次のものがあります。

- Cisco 10000 シリーズ システム
  - 物理イーサネット
  - .1Q、QinQ（unambiguous のみ）
- Cisco 7200 シリーズおよび Cisco 7300 シリーズ システム
  - 物理イーサネット
  - .1Q、QinQ（unambiguous のみ）
  - キューイングなしの MQC over ATM
  - ATM 1483 RBE と ATM ルーテッド Permanent Virtual Circuits（PVC; 相手先固定接続）
  - Generic Routing Encapsulation（GRE）トンネル。ポリシー マップは、セッションとトンネルで同時には使用できません。
- Cisco 7600 シリーズ システム
  - .1Q または QinQ サブインターフェイスのあるギガビット イーサネット
  - Routed Bridge Encapsulation（RBE; ルーテッド ブリッジ エンカプセレーション）
  - Permanent Virtual Connection（PVC; 相手先固定接続）

MQC は次のインターフェイスでサポートされていません。

- Bridge-Group Virtual Tunnel Interface（BVI）
- GEC
- Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）セッション（L2TP ネットワーク サーバ（LNS）上）用に設定されるインターフェイス

次の機能と設定は、IP セッションでの MQC に使用されます。

- トラフィック クラス用の ISG ポリサー

（注） Cisco 7600 シリーズ システムでは、トラフィック クラスがサポートされません。

ISG ポリサー

複数のトラフィック クラスがある IP セッション、およびポリサーとして動作する 1 つまたは複数のトラフィック クラスがある IP セッションで動作するように、設定を作成できます。ISG ポリサーは下位互換性のために維持され、今すぐ MQC に移行しない場合には完全にサポートされます。ただし、ISG ポリサーと MQC の両方がある場合、ISG ポリサーを使用するか、または MQC に完全に移行する必要があります。ISG ポリサーから MQC へ完全に移行しない場合は、設定上の問題が発生します。

ポリシー マップでの優先順位

ポリシー マップはサービス ポリシーを指定するために 1 つ以上のインターフェイスに対応付けることができます。ソースをコンテキストと組み合わせて設定すると、ポリシー マップが適用される QoS が決まります。3 つの設定ソースとその一般的な優先順位は次のとおりです。

1. ユーザ単位（加入者単位）の設定
2. サービス プロファイル
3. インターフェイス コンフィギュレーション

この優先順位は一般的な条件を示しており、サービス プロファイルとユーザ単位の設定は、インターフェイスの設定よりも優先順位が高くなっています。

ただし、ユーザ プッシュ単位の Change of Authorization（CoA）は、重複する機能や共通の機能の現在のユーザ単位の設定を置換します。同様に、新しいサービスにログインしたとき、その設定によって、重複している機能を、以前に設定され、ユーザ単位の設定ソースからまだ適用されていないサービス プロファイルから置換します。

新しいサービスからログオフすると、より優先順位の高い設定ソースが適用されていない場合、既存の設定が再適用されます。

このような優先順位が指定されると、ポリシー マップが次のように決まります。

- セッションにポリシー マップがない場合、着信ポリシー マップが適用されません。
- 既存のポリシー マップが着信ポリシー マップよりも高い優先順位のソースから設定される場合、着信ポリシー マップが適用されません。
- 既存のポリシー マップが着信ポリシー マップよりも低い優先順位のソースから設定される場合、着信ポリシー マップがこれを置換します。

Cisco 10000 シリーズ システムでの継承ルール

親インターフェイスのポリシーおよびキューのための Cisco 10000 シリーズ システムでの継承ルールは次のとおりです。

- ポリシー マップのないセッションが開始された場合、直接の親からポリシーやキューを継承します。直接の親は、たとえば、サブインターフェイスやメイン インターフェイスです。
- 継承されたポリシーのあるセッションで RADIUS サーバからのポリシーを受信した場合、まず、継承されたポリシーが削除され、RADIUS サーバからポリシーが適用されます。
- ポリシーのないセッションが開始された場合、親インターフェイスにもポリシーがありませんが、後で親にポリシーが適用され、次の 2 つの結果となる可能性があります。
  - メイン インターフェイスにポリシーが適用され、そのインターフェイス上のセッションがポリシーを継承します。メイン インターフェイスの下のサブインターフェイスでの独自のポリシーのないセッションもこのポリシーを継承します。

  - ポリシーはサブインターフェイスに適用され、そのサブインターフェイスでのセッションがポリシーを継承します。
- ユーザが親インターフェイスからポリシーを削除すると、次の 2 つの結果となる可能性があります。
  - サブインターフェイスからポリシーが削除され、ポリシーを継承したサブインターフェイスでのセッションから継承が解除されます。メイン インターフェイスにポリシーがある場合は、ポリシーが削除されたサブインターフェイスでのセッションがそのポリシーを継承します。
  - ポリシーがメイン インターフェイスから削除され、メイン インターフェイスから継承が解除され、このポリシーを継承したサブインターフェイスでのセッションからも継承が解除されます。
- ポリシーをまだ持たないセッションが RADIUS サーバからポリシーを受け取った場合は、新しいポリシーをインストールするだけで済みます。ただし、親から継承したポリシーがあるセッションで RADIUS サーバから新しいポリシーを受け取った場合、最初に親ポリシーの継承を解除し、その後で新しいポリシーをインストールする必要があります。
- セッション ポリシーが削除された場合、そのセッションはポリシーがある最も近い親、サブインターフェイス、またはメイン インターフェイスからポリシーを継承します。

IP セッションのための MQC サポートの設定方法

- 「IP セッションへの ISG QoS の設定」（P.124）

ローカル サービス プロファイルの設定の詳細については、『*Cisco IOS Intelligent Services Gateway Configuration Guide*』の「Configuring ISG Control Policies」の章にある「Configuring Per-Session QoS Using the ISG Framework」を参照してください。

ローカル加入者プロファイル MQC のサポート

サービス プロファイルで QoS ポリシー マップを設定するには、次の手順の各ステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *service-name*
4. **service-policy** *policy-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	**policy-map type service** *service-name* 例： `Router# (config)# policy-map type service service1`	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。ポリシー マップとそのサービス設定を指定します。
ステップ 4	**service-policy** *policy-name* 例： `Router# (config-service-policymap)# service-policy service-policy1`	サービス ポリシーを設定します。

IP セッションへの ISG QoS の設定

すでに設定されているトラフィック クラスをポリシー マップに関連付けるには、次の手順の各ステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *service-name*
4. **class type traffic** *class-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 service** *service-name* 例： `Router# (config)# policy-map type service`	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。ポリシー マップとそのサービス設定を指定します。
ステップ 4	**class type traffic** *class-name* 例： `Router# (config-service-policymap)# class type traffic`	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。

IP セッションのための MQC サポートの設定例

QoS ポリシー マップ、サービス プロファイル、およびコマンド ポリシー マップの設定：例

次に、Cisco 7600 シリーズ システムで QoS ポリシー マップ、サービス プロファイル、およびコマンド ポリシー マップを設定する方法の例を示します。コマンド ポリシー マップは、インターフェイス イーサネット 0/0 上で **service-policy** キーワードで設定されます。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map match-any EF-customer
Router(config-cmap)# match access-group name CUSTOMER-EF
Router(config-cmap)# class-map match-any EF-WAN
Router(config-cmap)# match qos-group 6
Router(config-cmap)# policy-map PREMIUM_MARK_IN
Router(config-pmap)# class EF-customer
Router(config-pmap-c)# set cos 6
Router(config-pmap-c)# set dscp ef
Router(config-pmap-c)# set qos-group 6
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# set dscp af11
Router(config-pmap-c)# set qos-group 1
Router(config-pmap-c)# set cos 1
Router(config-pmap-c)# policy-map PREMIUM_UB_OUT
Router(config-pmap)# class EF-WAN
Router(config-pmap-c)# police cir 200000000
Router(config-pmap-c-police)# priority
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# policy-map type service PREMIUM_SERVICE
Router(config-service-policymap)# service-policy input PREMIUM_MARK_IN
Router(config-service-policymap)# service-policy output PREMIUM_UB_OUT
Router(config-service-policymap)# policy-map type control INT
Router(config-control-policymap)# class type control always event account-logon
Router(config-control-policymap-class-control)# 1 service-policy type service name
PREMIUM_SERVICE
Router(config-control-policymap-class-control)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# pppoe enable group global
Router(config-if)# service-policy type control INT
```

その他の参考資料

関連資料

内容	参照先
ISG 制御ポリシーの設定方法	『*Cisco IOS Intelligent Services Gateway Configuration Guide*』の「Configuring ISG Control Policies」の章
MQC を使用した QoS ポリシーの設定方法	『*Cisco IOS Quality of Service Solutions Configuration Guide*』
ISG コマンド	『*Cisco IOS Intelligent Services Gateway Command Reference*』
セッション単位での QoS 機能の適用方法	『*Cisco IOS Quality of Service Configuration Solutions Guide*』の「Per-Session QoS」の章

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

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。またこの機能による既存 MIB のサポートに変更はありません。	なし

RFC

RFC	タイトル
この機能がサポートする新規 RFC または改訂 RFC はありません。また、この機能による既存 RFC の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

IP セッションのための MQC サポートの機能情報

表 9 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 9 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 9　IP セッションのための MQC サポートの機能情報

機能名	リリース	機能情報
IP セッションのための MQC サポート	12.2(33)SRC 15.0(1)S	Cisco ISG IP セッションで MQC プロビジョニングを提供します。 次のコマンドが導入または変更されました。**policy-map** および **service-policy**
ISG：セッション：マルチキャスト：共存	12.2(33)SRE	Cisco IOS Release 12.2(33)SRE では、Cisco 7600 シリーズのルータに ISG セッション マルチキャスト共存機能のサポートが追加されました。

ISG ポートバンドル ホスト キーの設定

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。このモジュールでは、加入者からの TCP パケットを、ISG ゲートウェイのローカル IP アドレスおよび一定範囲のポートにマッピングする、ISG Port-Bundle Host Key 機能の設定方法について説明します。このマッピングにより、外部ポータルで、セッションが開始された ISG ゲートウェイを識別できます。

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 Port-Bundle Host Key の機能情報」（P.139）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

ISG Port-Bundle Host Key 機能の前提条件

リリースおよびプラットフォームの要件の詳細については、「ISG Port-Bundle Host Key の機能情報」（P.139）を参照してください。

外部のポータルは、ポートバンドル ホスト キーをサポートし、同じポートバンドル ホスト キー パラメータが設定されている必要があります。

ISG Port-Bundle Host Key 機能の制約事項

- ISG Port-Bundle Host Key は、ポータル、および接続されているすべての ISG で個別にイネーブルにしておく必要があります。
- **source** コマンドで設定されたすべての ISG 発信元 IP アドレスは、ポータルが存在する管理ネットワーク内でルーティング可能になっている必要があります。
- 各ポータル サーバでは、接続されているすべての ISG のポートバンドル長を同じにする必要があります。
- ISG Port-Bundle Host Key 機能では TCP が使用されます。パケットは、TCP トラフィックを送信していない加入者に対してはマップされません。
- ユーザ プロファイルで Port-Bundle Host Key 機能を指定した場合は、そのユーザ プロファイルが IP パケットの到着前に有効になっていたときだけ機能します。たとえば、PPP セッションや、透過的な自動ログイン機能を備えた Dynamic Host Configuration Protocol（DHCP）で開始される IP セッションなどです。
- Cisco 7600 ルータでは、Port-Bundle Host Key 機能をセッションに適用できますが、フロー レベルでは適用できません。
- Cisco 7600 ルータでは、レイヤ 4 リダイレクトと Port-Bundle Host Key を、最大 150 の並列セッションで同時にイネーブルにできます。

ISG Port-Bundle Host Key に関する情報

ISG Port-Bundle Host Key の概要

ISG Port-Bundle Host Key 機能は、外部ポータルにおいて、セッションを識別するためのインバンド シグナリング メカニズムとして機能します。加入者からの TCP パケットは、ISG ゲートウェイのローカル IP アドレスと一定範囲のポートにマッピングされます。このマッピングにより、ポータルはセッションが開始された ISG ゲートウェイを識別できるようになります。また、このマッピングにより、加入者が重複する IP アドレスを持っている場合でも、セッションを一意に識別できます。ISG Port-Bundle Host Key 機能では、重複する IP アドレスを持つ加入者がいる場合でも、複数の Virtual Routing and Forwarding（VRF）に対して 1 つのポータルを展開できます。

Port-Bundle Host Key のメカニズム

ISG Port-Bundle Host Key 機能を使用して、ISG は、加入者とポータルの間の TCP トラフィックにおいて、Port-Address Translation（PAT; ポート アドレス変換）および Network Address Translation（NAT; ネットワーク アドレス変換）を実行します。加入者の TCP 接続が設定されていると、ISG はポート マッピングを作成します。このマッピングでは、発信元 IP アドレスを設定済みの ISG IP アドレスに変更し、発信元 TCP ポートを ISG から割り当てられたポートに変更します。Web ページにアクセスしている場合は、1 人の加入者が同時に複数の TCP セッションを持つことができるため、ISG はポートのバンドルを各加入者に割り当てます。割り当てられたポートバンドル ホスト キー、またはポート バンドルと ISG 発信元 IP アドレスの組み合わせにより、各加入者は一意に識別されます。ホスト キーは、ポータル サーバと ISG 間で送信される RADIUS パケット内の、Subscriber IP の Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）で伝達されます。表 10 に、Subscriber IP VSA を示します。ポータル サーバが加入者に応答を送信すると、ISG は変換テーブルを使用して、宛先 IP アドレスおよび宛先 TCP ポートを識別します。

表 10　Subscriber IP VSA の説明

アトリビュート（ID）	ベンダー ID	サブアトリビュート ID とタイプ	アトリビュート名	アトリビュート データ
26	9	250 Account-Info	Subscriber IP	S *subscriber-ip-address* [:*port-bundle-number*] • S：加入者 IP の Account-Info コード。 • *subscriber-ip-address* [:*port-bundle-number*]：port-bundle number は、ISG Port-Bundle Host Key 機能が設定されている場合のみ使用されます。

加入者とポータルの間の各 TCP セッションでは、ISG は、ポート バンドルの 1 つのポートをポート マップとして使用します。個々のポート マッピングは、非アクティブ タイマーに基づいて、再使用が可能であるというフラグを設定されますが、いったん割り当てられると明示的には削除されません。ポート バンドルの数は、ISG アドレスごとに制限されていますが、ポート バンドルの使用に対して設定できる ISG IP アドレスの数には制限がありません。

ポートバンドル長

ポートバンドル長は、1 つのバンドル内のポート数を決定するために使用されます。デフォルトでは、ポートバンドル長は 4 ビットです。ポートバンドルの最大長は 10 ビットです。使用できるポートバンドル長の値、およびそれに対応するバンドルごとのポート、およびグループごとのバンドルの値については、表 11 を参照してください。ポート バンドルでポートを使い切ってしまったことを示すエラー メッセージが頻繁に発生する場合は、ポートバンドル長を増やすことがあります。

表 11　ポートバンドル長と、対応するバンドルごとのポート数およびグループごとのバンドル数の値

ポートバンドル長（ビット）	バンドルごとのポート数	グループごと（および ISG 発信元 IP アドレスごと）のバンドル数
0	1	64512
1	2	32256
2	4	16128
3	8	8064
4（デフォルト）	16	4032

表 11　ポートバンドル長と、対応するバンドルごとのポート数およびグループごとのバンドル数の値 （続き）

ポートバンドル長（ビット）	バンドルごとのポート数	グループごと（および ISG 発信元 IP アドレスごと）のバンドル数
5	32	2016
6	64	1008
7	128	504
8	256	252
9	512	126
10	1024	63

（注）　ポータル サーバごとに、接続されているすべての ISG のポートバンドル長を同じにする必要があります。これは、ポータル サーバの BUNDLE_LENGTH 引数で指定されている設定済みの値に対応しています。ある ISG でポートバンドル長を変える場合は、ポータル上の設定において、必ず対応する値を変更してください。

ISG Port-Bundle Host Key の利点

外部ポータル使用のために拡張された加入者の重複 IP アドレスのサポート

ISG の Port-Bundle Host Key 機能を使用すると、加入者の IP アドレスまたは VRF メンバシップに関係なく、外部ポータルのアクセスが可能になります。ポートバンドル ホスト キーを使用しない場合、単一の外部ポータルにアクセスするすべての加入者は、一意の IP アドレスを持つ必要があります。また、ポートバンドル ホスト キーでは、ポータルが存在するドメインから VRF 特有のアドレスが分離されるため、ルーティング上の注意点が単純化されます。

加入者および ISG IP アドレスに対するポータル プロビジョニングが不要

ISG Port-Bundle Host Key 機能を使用しない場合に、ポータルで ISG に RADIUS パケットを送信したり、加入者に HTTP パケットを送信するには、事前に加入者および ISG IP アドレスに対してポータルをプロビジョニングしておく必要があります。ISG Port-Bundle Host Key 機能により、1 つのポータル サーバが複数の ISG に対応できるようにしたり、1 つの ISG が複数のポータル サーバに対応できるようにするためのポータルのプロビジョニングが不要になります。

ISG Port-Bundle Host Key の設定方法

- 「サービス ポリシー マップでの ISG Port-Bundle Host Key 機能のイネーブル化」（P.133）
- 「AAA サーバのユーザ プロファイルまたはサービス プロファイルでの Port-Bundle Host Key 機能のイネーブル化」（P.134）
- 「Port-Bundle Host Key パラメータの設定」（P.134）
- 「ISG Port-Bundle Host Key の設定の確認」（P.136）

サービス ポリシー マップでの ISG Port-Bundle Host Key 機能のイネーブル化

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するには、この作業を実行します。ISG Port-Bundle Host Key 機能は、このサービス ポリシー マップを使用しているすべての加入者に適用されます。

（注） この機能に対して 1 つの専用サービス ポリシーを使用することを推奨します。他の ISG 機能とポリシーを共有しないでください。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-name*
4. **ip portbundle**
5. **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 service** *policy-name* 例： `Router(config)# policy-map type service service1`	ISG サービスの定義に使用する、サービス ポリシー マップを作成または定義します。
ステップ 4	**ip portbundle** 例： `Router(config-service-policymap)# ip portbundle`	サービスに対して、ISG Port-Bundle Host Key 機能をイネーブルにします。
ステップ 5	**end** 例： `Router(config-service-policymap)# end`	（任意）特権 EXEC モードに戻ります。

次の作業

サービス ポリシー マップまたはサービス 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。サービスのアクティブ化方法の詳細については、「Configuring ISG Subscriber Services」モジュールを参照してください。

AAA サーバのユーザ プロファイルまたはサービス プロファイルでの Port-Bundle Host Key 機能のイネーブル化

Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバのユーザ プロファイルまたはサービス プロファイルで ISG Port-Bundle Host Key 機能をイネーブルにするには、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 Port-Bundle Host Key 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 Port-Bundle Host Key アトリビュートを追加します。 26,9,1 = "ip:portbundle=enable"	ユーザ プロファイルまたはサービス プロファイで ISG Port-Bundle Host Key アトリビュートをイネーブルにします。

次の作業

サービス プロファイルで ISG Port-Bundle Host Key 機能をイネーブルにした場合、制御ポリシーを使用してサービスをアクティブにするなど、サービス プロファイルをアクティブにする方法を設定することがあります。サービスのアクティブ化方法の詳細については、「Configuring ISG Subscriber Services」モジュールを参照してください。

Port-Bundle Host Key パラメータの設定

ISG Port-Bundle Host Key パラメータを設定し、ISG が、ダウンストリーム トラフィックに対する IP アドレスおよびポート番号を検出するために変換表を使用するインターフェイスを指定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip portbundle**
4. **match access-list** *access-list-number*
5. **length** *bits*

6. **source** *interface-type interface-number*
7. **exit**
8. **interface** *type number*
9. **ip portbundle outside**

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	**ip portbundle** 例： `Router(config)# ip portbundle`	IP ポートバンドル コンフィギュレーション モードを開始します。
ステップ 4	**match access-list** *access-list-number* 例： `Router(config-portbundle)# match access-list 101`	加入者のトラフィックと比較するためのアクセス リストを指定して、ポート マッピング用のパケットを指定します。
ステップ 5	**length** *bits* 例： `Router(config-portbundle)# length 5`	ISG ポートバンドル長を指定します。この長さは、バンドルあたりのポート数、およびグループあたりのバンドル数を決定します。 • デフォルトのビット数は 4 です。 • 詳細については、「ポートバンドル長」を参照してください。
ステップ 6	**source** *interface-type interface-number* 例： `Router(config-portbundle)# source loopback 0`	メイン IP アドレスが、ISG によって加入者トラフィックの宛先 IP アドレスへマップされるインターフェイスを指定します。 • 発信元インターフェイスとしてループバック インターフェイスを使用することを推奨します。
ステップ 7	**exit** 例： `Router(config-portbundle)# 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。
ステップ 8	**interface** *type number* 例： `Router(config)# interface ethernet 0/0`	設定用のインターフェイスを指定します。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 9	**ip portbundle outside** 例： `Router(config-if)# ip portbundle outside`	設定中のインターフェイスについて、ポータルから加入者へ向かっているトラフィックの場合は、宛先 IP アドレスと TCP ポートを、実際の加入者 IP アドレスと TCP ポートに逆変換するよう ISG を設定します。

ISG Port-Bundle Host Key の設定の確認

ISG Port-Bundle Host Key の設定に関する情報を表示するには、この作業を実行します。

手順の概要

1. **enable**
2. **show ip portbundle status** [**free** | **inuse**]
3. **show ip portbundle ip** *portbundle-ip-address* **bundle** *port-bundle-number*
4. **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 ip portbundle status** [**free** | **inuse**] 例： `Router# show ip portbundle status free`	ISG ポートバンドル グループの情報を表示します。
ステップ 3	**show ip portbundle ip** *portbundle-ip-address* **bundle** *port-bundle-number* 例： `Router# show ip portbundle ip 10.10.10.10 bundle 65`	特定の ISG ポート バンドルの情報を表示します。
ステップ 4	**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。

ISG Port-Bundle Host Key の設定例

ISG Port-Bundle Host Key の設定：例

次に、すべてのセッションに適用するために、ISG Port-Bundle Host Key 機能を設定する方法の例を示します。

```
policy-map type service ISGPBHKService
 ip portbundle
!
policy-map type control PBHKRule
 class type control always event session-start
  1 service-policy type service ISGPBHKService
!
service-policy type control PBHKRule

interface ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip portbundle outside
!
ip portbundle
 match access-list 101
 length 5
 source loopback 0
```

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*』

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 Port-Bundle Host Key の機能情報

表 12 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 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 12 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 12　ISG Port-Bundle Host Key の機能情報

機能名	リリース	機能情報
ISG：セッション：Auth：PBHK	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG Port-Bundle Host Key 機能は、外部ポータルにおいて、セッションを識別するためのインバンド シグナリング メカニズムとして機能します。加入者からの TCP パケットは、ISG ゲートウェイのローカル IP アドレスと一定範囲のポートにマッピングされます。このマッピングにより、ポータルはセッションが開始された ISG ゲートウェイを識別できるようになります。 このモジュールでは、ISG Port-Bundle Host Key 機能の設定方法について説明します。 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。

RADIUS プロキシとしての ISG 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 RADIUS プロキシ機能により、ISG は、RADIUS 認証を使用するクライアント デバイスと、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバの間のプロキシとして機能できるようになります。RADIUS プロキシとしてコンフィギュレーションされている場合、ISG は RADIUS のパケット フローを「詮索」（観察）できるようになり、認証が成功すると、対応する ISG セッションを透過に作成できます。ここでは、ISG を RADIUS プロキシとして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、「ISG RADIUS プロキシの機能情報」（P.157）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

ISG RADIUS プロキシの前提条件

Cisco IOS イメージが、AAA および ISG をサポートしている必要があります。

ISG RADIUS プロキシの制約事項

Wireless Internet Service Provider roaming（WISPr）アトリビュートはサポートされていません。

ISG RADIUS プロキシに関する情報

ISG を RADIUS プロキシとして設定する前に、次の概念について理解しておく必要があります。

- 「ISG RADIUS プロキシの概要」（P.142）
- 「ISG RADIUS プロキシによるアカウンティング パケットの処理」（P.143）
- 「RADIUS クライアントのサブネット定義」（P.143）
- 「モバイル ワイヤレス環境のための ISG RADIUS プロキシのサポート」（P.143）
- 「ISG RADIUS プロキシの利点」（P.144）

ISG RADIUS プロキシの概要

Public Wireless LAN（PWLAN; 公衆無線 LAN）およびワイヤレス メッシュ ネットワークには、数百ものアクセス ポイントを含めることが可能で、各アクセス ポイントは AAA サーバに RADIUS 認証要求を送信する必要があります。ISG RADIUS プロキシ機能を使用すると、アクセス ポイントは、AAA サーバに認証要求を直接送信せずに、ISG に送信できるようになります。ISG はこの要求を AAA サーバへ中継します。AAA サーバは ISG へ応答を送信し、次にこの応答を適切なアクセス ポイントへ中継します。

ISG は RADIUS プロキシとして機能する場合、加入者の認証および認可のときに生じる RADIUS フローからユーザ固有のデータを検出し、認証が成功すると、対応する IP セッションを透過的に作成できます。この機能は、よりネットワーク エッジに近いデバイスによって認証された加入者に対する ISG に関して、自動ログイン機能を提供します。

RADIUS プロキシとして設定されている場合は、RFC 2865、RFC 2866、および RFC 2869 に記載されているように、ISG は、クライアント デバイスによって生成されたすべての RADIUS 要求、および対応する AAA サーバによって生成されたすべての RADIUS 応答をプロキシします。

ISG RADIUS プロキシ機能はクライアント デバイスのタイプには依存せず、Password Authentication Protocol（PAP; パスワード認証プロトコル）と Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）の両方、Access-Challenge パケット、および Extensible Authentication Protocol（EAP）メカニズムを使用した、標準認証（1 回のアクセスと要求/応答の交換）をサポートします。

認証の要求とアカウンティングの要求が別の RADIUS クライアント デバイスから開始された場合、ISG は相関ルールにより、すべての要求を該当するセッションに関連付けます。たとえば、集中型 PWLAN 展開では、認証要求は無線 LAN（WLAN）のアクセス ポイントから開始され、アカウンティング要求は Access Zone Router（AZR）で生成されます。Calling-Station-ID（アトリビュート 31）によって関連付けを十分に信頼できる場合、これらの異なる RADIUS フローをベースとなるセッションに関連付ける処理は自動的に行われます。

認証が成功すると、RADIUS の応答から収集した認可データが、対応する ISG セッションに適用されます。

ISG RADIUS プロキシ動作を使用して作成されたセッションは通常、Accounting-Stop パケットを受け取って終了します。

ISG RADIUS プロキシによるアカウンティング パケットの処理

デフォルトでは、ISG RADIUS プロキシは、受け取ったアカウンティング パケットに対してローカルに応答します。**accounting method-list** コマンドを使用すると、RADIUS プロキシ クライアントのアカウンティング パケットを特定のサーバへフォワードするよう、ISG を設定できます。アカウンティング パケットのフォワーディングは、すべての RADIUS プロキシ クライアントに対してグローバルに設定することも、クライアントごとに設定することもできます。

RADIUS クライアントのサブネット定義

ISG が、すべて同じサブネット上に存在している複数のクライアント デバイスに対するプロキシとして機能している場合は、各デバイスに対する個々の IP アドレスではなく、1 つのサブネット定義を使用してクライアントを設定できます。このように設定することにより、1 つの設定をすべてのクライアント デバイスで共有できるようになります。

モバイル ワイヤレス環境のための ISG RADIUS プロキシのサポート

ISG RADIUS プロキシはモバイル ワイヤレス特有のプロセスを使用して、Gateway General Packet Radio Service（GPRS）Support Node（GGSN）環境に対するサポートを提供します。ここでは、ISG RADIUS プロキシ アトリビュートのサポートと処理について説明します。

- 「アトリビュートの処理と RADIUS 要求との相関」（P.143）
- 「3GPP アトリビュートのサポート」（P.144）

アトリビュートの処理と RADIUS 要求との相関

認証要求とアカウンティング要求が別の RADIUS クライアント デバイスから発生している場合、ISG は相関ルールを使用して、すべての要求を該当するセッションに関連付けます。Calling-Station-ID（アトリビュート 31）によって関連付けを十分に信頼できる場合、これらの異なる RADIUS フローをベースとなるセッションに関連付ける処理は自動的に行われます。

モバイル ワイヤレス環境では、アトリビュートの処理および RADIUS 要求とセッションとの相関は、PWLAN 環境とは異なる実装になっています。たとえば、ある PWLAN 環境ではアトリビュート 31 が MAC アドレスとなり、GGSN 環境ではアトリビュート 31 が Mobile Station Integrated Services Digital Network（MSISDN）となります。これは普通の数字または英数字の文字列です。また、ある GGSN 環境では、アトリビュート 31 以外のアトリビュートを使用して RADIUS 要求の相関を行うこともできます。

ISG RADIUS プロキシは、RADIUS プロキシ クライアントでアトリビュート 31 に対して MAC または MSISDN のどちらの形式を使用するかを指定することによって、モバイル ワイヤレス環境をサポートしています。形式は、**calling-station-id format** コマンドを使用して指定します。また、**session-identifier** コマンドを使用して、RADIUS 要求の相関を実行するために他の（アトリビュート 31 以外の）アトリビュートを使用するよう、ISG RADIUS プロキシを設定できます。

3GPP アトリビュートのサポート

GGSN 環境における ISG RADIUS プロキシは、表 13 に示す Third Generation Partnership Project（3GPP）アトリビュートを認識および解釈する必要があります。これらのアトリビュートは、アカウンティング要求の一部を形成します。

表 13　ISG RADIUS プロキシでサポートされる 3GPP アトリビュート

アトリビュート	説明	ベンダー ID/タイプ
3GPP-IMSI	ユーザ用の International Mobile Subscriber Identity（IMSI）。	10415/1
3GPP-Charging-Id	この Packet Data Protocol（PDP）コンテキスト用のチャージング ID（GGSN アドレスと組み合わせて PDP コンテキスト用の固有 ID を構成）。	10415/2
3GPP-SGSN-Address	コントロール メッセージの処理に、GPRS Tunneling Protocol（GTP）コントロール プレーンで使用される Serving GPRS Support Node（SGSN）アドレス。これを使用して、ユーザが接続される Public Line Mobile Network（PLMN）を識別できます。	10415/6

ISG RADIUS プロキシの利点

ISG RADIUS プロキシの使用には次の利点があります。

- EAP 加入者セッションに対して、ISG の完全な機能セットを適用できる。
- 既存の Network Access Server（NAS; ネットワーク アクセス サーバ）および AAA サーバの最小限の停止時間で、ISG デバイスを導入できる。
- すべてのアクセス ポイントではなく、ISG だけをクライアントとして設定すればよいため、RADIUS サーバのコンフィギュレーションが簡単になる。

RADIUS プロキシとしての ISG の設定方法

ここでは、次の各手順について説明します。

- 「ISG RADIUS プロキシ IP セッションの開始」（P.145）（必須）
- 「ISG RADIUS プロキシ グローバル パラメータの設定」（P.146）（必須）
- 「ISG RADIUS プロキシのクライアント固有パラメータの設定」（P.148）（任意）
- 「RADIUS プロキシ イベントの ISG ポリシーの定義」（P.150）（必須）
- 「ISG RADIUS プロキシ設定の確認」（P.151）（任意）
- 「ISG RADIUS プロキシ セッションのクリア」（P.152）（任意）

ISG RADIUS プロキシ IP セッションの開始

RADIUS クライアントから RADIUS プロキシ メッセージを受け取ったときに IP セッションを開始するよう ISG 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. **interface** *type number*
4. **ip subscriber** {**interface** | **l2-connected** | **routed**}
5. **initiator radius-proxy**
6. **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	**interface** *type number* 例： `Router(config)# interface fastethernet 1/0/0`	設定する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	**ip subscriber** {**interface** | **l2-connected** | **routed**} 例： `Router(config-if)# ip subscriber routed`	インターフェイス上で ISG IP 加入者のサポートをイネーブルにし、インターフェイス上で ISG に接続するために IP 加入者が使用するアクセス方法を指定し、加入者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	**initiator radius-proxy** 例： `Router(config-subscriber)# initiator radius-proxy`	いずれかの RADIUS パケットを受け取ったら IP セッションを開始するよう、ISG を設定します。
ステップ 6	**end** 例： `Router(config-subscriber)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ISG RADIUS プロキシ グローバル パラメータの設定

デフォルトですべての RADIUS プロキシ クライアントに適用される ISG RADIUS プロキシ パラメータを設定するには、この作業を実行します。クライアント固有のパラメータも設定し、このグローバル設定よりも優先することも可能です。クライアント固有の設定を指定するには、「ISG RADIUS プロキシのクライアント固有パラメータの設定」（P.148）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius proxy**
5. **session-identifier** {**attribute** *number* | **vsa vendor** *id* **type** *number*}
6. **calling-station-id format** {**mac-address** | **msisdn**}
7. **accounting method-list** {*method-list-name* | **default**}
8. **accounting port** *port-number*
9. **authentication port** *port-number*
10. **key** [**0** | **7**] *word*
11. **timer** {**ip-address** | **request**} *seconds*
12. **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	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa server radius proxy** 例： `Router(config)# aaa server radius proxy`	ISG RADIUS プロキシ サーバ 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 5	**session-identifier** {**attribute** *number* | **vsa vendor** *id* **type** *number*} **例：** `Router(config-locsvr-proxy-radius)# session-identifier attribute 1`	（任意）あるセッションの RADIUS サーバ要求を相互に関連付け、RADIUS プロキシ モジュール内のセッションを識別します。
ステップ 6	**calling-station-id format** {**mac-address** | **msisdn**} **例：** `Router(config-locsvr-proxy-radius)# calling-station-id format msisdn`	Calling-Station-ID の形式を指定します。
ステップ 7	**accounting method-list** {*method-list-name* | **default**} **例：** `Router(config-locsvr-proxy-radius)# accounting method-list fwdacct`	RADIUS クライアントからのアカウンティング パケットの転送先となるサーバを指定します。 **（注）** デフォルトでは、ISG RADIUS プロキシはアカウンティング パケットをローカルに処理します。
ステップ 8	**accounting port** *port-number* **例：** `Router(config-locsvr-proxy-radius)# accounting port 2222`	ISG が RADIUS クライアントからのアカウンティング パケットを待ち受けるポートを指定します。 • デフォルトのポートは 1646 です。
ステップ 9	**authentication port** *port-number* **例：** `Router(config-locsvr-proxy-radius)# authentication port 1111`	ISG が RADIUS クライアントからの認証パケットを待ち受けるポートを指定します。 • デフォルトのポートは 1645 です。
ステップ 10	**key** [**0** | **7**] *word* **例：** `Router(config-locsvr-proxy-radius)# key radpro`	暗号キーが、ISG と RADIUS クライアント間で共有されるように設定します。 • 0 は、暗号化されていないキーをフォローするよう指定します。 • 7 は、非公開のキーをフォローするよう指定します。
ステップ 11	**timer** {**ip-address** | **request**} *seconds* **例：** `Router(config-locsvr-proxy-radius)# timer ip-address 5`	セッションを終了するまでに、指定されたイベントを ISG が待機する時間を指定します。 • **ip-address**：IP アドレスがセッションに割り当てられるまで、ISG が待機する時間を指定します。 • **request**：クライアント デバイスからアクセス要求を受け取るまで、ISG が待機する時間を指定します。
ステップ 12	**end** **例：** `Router(config-locsvr-proxy-radius)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ISG RADIUS プロキシのクライアント固有パラメータの設定

ISG RADIUS プロキシにクライアント固有のパラメータを設定するには、この作業を実行します。この設定は、指定したクライアントまたはサブネットのみに適用されます。クライアント固有の設定は、グローバルな ISG RADIUS プロキシの設定よりも優先されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius proxy**
5. **client** {**name** | *ip-address*} [*subnet-mask* [**vrf** *vrf-id*]]
6. **session-identifier** {**attribute** *number* | **vsa vendor** *id* **type** *number*}
7. **calling-station-id format** {**mac-address** | **msisdn**}
8. **accounting method-list** {*method-list-name* | **default**}
9. **accounting port** *port-number*
10. **authentication port** *port-number*
11. **key** [**0** | **7**] *word*
12. **timer** {**ip-address** | **request**} *seconds*
13. **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	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa server radius proxy** 例： `Router(config)# aaa server radius proxy`	ISG RADIUS プロキシ サーバ 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	**client** {**name**	*ip-address*} [*subnet-mask* [**vrf** *vrf-id*]] 例： `Router(config-locsvr-proxy-radius)# client 172.16.54.45 vrf myvrftable`	クライアント固有のパラメータを設定できる RADIUS プロキシ クライアントを指定し、RADIUS クライアント 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 6	**session-identifier** {**attribute** *number* | **vsa vendor** *id* **type** *number*} **例：** `Router(config-locsvr-radius-client)# session-identifier vsa vendor 5335 type 123`	（任意）あるセッションの RADIUS 要求を相互に関連付け、RADIUS プロキシ モジュール内のセッションを識別します。
ステップ 7	**calling-station-id format** {**mac-address** | **msisdn**} **例：** `Router(config-locsvr-radius-client)# calling-station-id format msisdn`	Calling-Station-ID の形式を指定します。
ステップ 8	**accounting method-list** {*method-list-name* | **default**} **例：** `Router(config-locsvr-radius-client)# accounting method-list fwdacct`	RADIUS クライアントからのアカウンティング パケットの転送先となるサーバを指定します。
ステップ 9	**accounting port** *port-number* **例：** `Router(config-locsvr-radius-client)# accounting port 2222`	ISG が RADIUS クライアントからのアカウンティング パケットを待ち受けるポートを指定します。 • デフォルトのポートは 1646 です。
ステップ 10	**authentication port** *port-number* **例：** `Router(config-locsvr-radius-client)# authentication port 1111`	ISG が RADIUS クライアントからの認証パケットを待ち受けるポートを指定します。 • デフォルトのポートは 1645 です。
ステップ 11	**key** [**0** | **7**] *word* **例：** `Router(config-locsvr-radius-client)# key radpro`	暗号キーが、ISG と RADIUS クライアント間で共有されるように設定します。 • 0 は、暗号化されていないキーをフォローするよう指定します。 • 7 は、非公開のキーをフォローするよう指定します。
ステップ 12	**timer** {**ip-address** | **request**} *seconds* **例：** `Router(config-locsvr-radius-client)# timer ip-address 5`	セッションを終了するまでに、指定されたイベントを ISG が待機する時間を指定します。 • **ip-address**：IP アドレスがセッションに割り当てられるまで、ISG が待機する時間を指定します。 • **request**：クライアント デバイスからアクセス要求を受け取るまで、ISG が待機する時間を指定します。
ステップ 13	**end** **例：** `Router(config-locsvr-radius-client)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

RADIUS プロキシ イベントの ISG ポリシーの定義

セッションの開始時に適用されるポリシーを設定し、ISG が指定したサーバに対して RADIUS パケットをプロキシできるようにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization radius-proxy** {**default** | *list-name*} *method1* [*method2* [*method3...*]]
5. **policy-map type control** *policy-map-name*
6. **class type control** {*control-class-name* | **always**} **event session-start**
7. *action-number* **proxy** [**aaa list** {**default** | *list-name*}
8. **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	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa authorization radius-proxy** {**default** | *list-name*} *method1* [*method2* [*method3...*]] 例： `Router(config)# aaa authorization radius-proxy RP group radius`	ISG RADIUS プロキシ加入者の AAA 認可方法を設定します。 • 方法は、次のいずれかです。 – **group** *group-name*ÅF**server group** *group-name* コマンドで定義された、認可用の RADIUS サーバのサブセットを使用します。 – **group radius**ÅF**aaa group server radius** コマンドで定義された、認可用のすべての RADIUS サーバのリストを使用します。
ステップ 5	**policy-map type control** *policy-map-name* 例： `Router(config)# policy-map type control proxyrule`	コントロール ポリシー マップを作成または変更します。これにより、ISG コントロール ポリシーを定義し、コントロール 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。

	コマンドまたはアクション	目的
ステップ 6	**class type control** {*control-class-name* | **always**} **event session-start** 例： `Router(config-control-policymap)# class type control always event session-start`	アクションを設定できるコントロール クラスを指定し、コントロール 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	*action-number* **proxy** [**aaa list** {**default** | *list-name*} 例： `Router(config-control-policymap-class-control)# 1 proxy aaa list RP`	指定したサーバに RADIUS パケットを送信します。 • ステップ 4 の **aaa authorization radius-proxy** コマンドで指定したサーバに RADIUS プロキシ パケットをフォワードするよう ISG を設定するには、このコマンドを使用します。
ステップ 8	**end** 例： `Router(config-control-policymap-class-control)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ISG RADIUS プロキシ設定の確認

ISG RADIUS プロキシ設定を確認するには、次の 1 つ以上のコマンドを使用します。コマンドは任意の順序で入力できます。

手順の概要

1. **show radius-proxy client** *ip-address* [**vrf** *vrf-name*]
2. **show radius-proxy session** {**id** *id-number* | **ip** *ip-address*}
3. **show subscriber session** [**identifier** {**authen-status** {**authenticated** | **unauthenticated**} | **authenticated-domain** *domain-name* | **authenticated-username** *username* | **dnis** *dnis* | **media** *type* | **nas-port** *identifier* | **protocol** *type* | **source-ip-address** *ip-address subnet-mask* | **timer** *timer-name* | **tunnel-name** *name* | **unauthenticated-domain** *domain-name* | **unauthenticated-username** *username*} | **uid** *session-identifier* | **username** *username*] [**detailed**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show radius-proxy client** *ip-address* [**vrf** *vrf-id*] 例： `Router# show radius-proxy client 10.10.10.10`	RADIUS プロキシの設定情報、および ISG RADIUS プロキシ クライアントのセッションの概要を表示します。
ステップ 2	**show radius-proxy session** {**id** *id-number* | **ip** *ip-address*} 例： `Router# show radius-proxy session ip 10.10.10.10`	ISG RADIUS プロキシ セッションの情報を表示します。 （注） ID は、**show radius-proxy client** コマンドの出力内にあります。
ステップ 3	**show subscriber session** [**identifier** {**authen-status** {**authenticated** | **unauthenticated**} | **authenticated-domain** *domain-name* | **authenticated-username** *username* | **dnis** *dnis* | **media** *type* | **nas-port** *identifier* | **protocol** *type* | **source-ip-address** *ip-address subnet-mask* | **timer** *timer-name* | **tunnel-name** *name* | **unauthenticated-domain** *domain-name* | **unauthenticated-username** *username*} | **uid** *session-identifier*| **username** *username*] [**detailed**] 例： `Router# show subscriber session detailed`	ISG デバイスの加入者セッションの情報を表示します。

ISG RADIUS プロキシ セッションのクリア

ISG RADIUS プロキシ セッションをクリアするには、この作業を実行します。

手順の概要

1. **enable**
2. **clear radius-proxy client** *ip-address*
3. **clear radius-proxy session** {**id** *id-number* | **ip** *ip-address*}

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	**clear radius-proxy client** *ip-address* **例：** `Router# clear radius-proxy client 10.10.10.10`	指定されたクライアント デバイスに関連付けられているすべての ISG RADIUS プロキシ セッションをクリアします。
ステップ 3	**clear radius-proxy session** {**id** *id-number* | **ip** *ip-address*} **例：** `Router# clear radius-proxy session ip 10.10.10.10`	特定の ISG RADIUS プロキシ セッションをクリアします。 **（注）** ID は、**show radius-proxy client** コマンドの出力内にあります。

ISG RADIUS プロキシの設定例

ここでは、次の例について説明します。

- 「ISG RADIUS プロキシの設定：例」（P.153）
- 「ISG RADIUS プロキシおよびレイヤ 4 のリダイレクト：例」（P.154）

ISG RADIUS プロキシの設定：例

次の例では、ISG が RADIUS プロキシとして機能し、RP と呼ばれるメソッド リストへ RADIUS パケットを送信するよう設定します。RADIUS パケットを受け取ったときに IP セッションを開始するよう、FastEthernet インターフェイス 0/0 が設定されます。

```
!
aaa new-model
!
aaa group server radius EAP
server 10.2.36.253 auth-port 1812 acct-port 1813
!
aaa authorization radius-proxy RP group EAP
aaa accounting network FWDACCT start-stop group EAP
aaa accounting network FLOWACCT start-stop group EAP
!
aaa server radius proxy
session-identifier attribute 1
calling-station-id format msisdn
authentication port 1111
accounting port 2222
key radpro
message-authenticator ignore

! The method list "FWDACCT" was configured by the aaa accounting network FWDACCT
! start-stop group EAP command above.
```

```
accounting method-list FWDACCT
client 10.45.45.2
timer request 5
!
client 10.45.45.3
key aashica#@!$%&/
timer ip-address 120
!
!
! This control policy references the method list called "RP" that was configured using the
aaa authorization radius-proxy command above.
policy-map type control PROXYRULE
class type control always event session-start
1 proxy aaa list RP
!
!
!
bba-group pppoe global
!
!
interface FastEthernet 2/1/0
ip address 10.45.45.1 255.255.255.0
ip subscriber routed
initiator radius-proxy
no ip route-cache cef
no ip route-cache
no cdp enable
!
! The control policy "PROXYRULE" is applied to the interface.
service-policy type control PROXYRULE
!
!
radius-server host 10.2.36.253 auth-port 1812 acct-port 1813 key cisco
radius-server host 10.76.86.83 auth-port 1665 acct-port 1666 key rad123
radius-server vsa send accounting
radius-server vsa send authentication

aaa new-model
!
!
aaa group server radius EAP
server 10.2.36.253 auth-port 1812 acct-port 1813
!
```

ISG RADIUS プロキシおよびレイヤ 4 のリダイレクト：例

次に、ISG RADIUS プロキシおよびレイヤ 4 のリダイレクトの両方に対して設定されている ISG ポリシーの例を示します。

```
aaa authorization network default local
!
redirect server-group REDIRECT
 server ip 10.255.255.28 port 23
 !
class-map type traffic match-any traffic1
match access-group input 101
!
policy-map type service service1
 class type traffic traffic1
  redirect list 101 to group REDIRECT
!
policy-map type control PROXYRULE
```

```
 class type control always event session-start
  1 proxy aaa list RP
  2 service-policy type service name service1
!
access-list 101 permit tcp host 10.45.45.2 any
```

次に、**show subscriber session** コマンドの対応するサンプル出力の例を示します。

```
Router# show subscriber session username 12345675@cisco

Unique Session ID: 66
Identifier: aash
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:40, Last Changed: 00:00:00

Policy information:
  Authentication status: authen
  Active services associated with session:
    name "service1", applied before account logon
  Rules, actions and conditions executed:
    subscriber rule-map PROXYRULE
      condition always event session-start
        1 proxy aaa list RP
        2 service-policy type service name service1

Session inbound features:
Feature: Layer 4 Redirect ------>>> L4 redirect is applied to the session at session start
  Rule table is empty
Traffic classes:
  Traffic class session ID: 67
   ACL Name: 101, Packets = 0, Bytes = 0
Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0

Configuration sources associated with this session:
Service: service1, Active Time = 00:00:40
Interface: FastEthernet0/1, Active Time = 00:00:40
```

その他の参考資料

ここでは、ISG RADIUS プロキシ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*』
ISG の設計と展開	• 『*Cisco ISG Design and Deployment Guide: ATM Aggregation*』 • 『*Cisco ISG Design and Deployment Guide: Gigabit Ethernet Aggregation*』
RADIUS アトリビュート	『*RADIUS Attributes Overview and RADIUS IETF Attributes*』
ベンダー固有アトリビュート	『*Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco 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
RFC 2865	*『Remote Authentication Dial In User Service（RADIUS）』*
RFC 2866	*『RADIUS Accounting』*
RFC 2869	*『RADIUS Extensions』*

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 RADIUS プロキシの機能情報

表 14 には、この機能のリリース履歴の一覧が表示されています。

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 14 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 14　ISG RADIUS プロキシの機能情報

機能名	リリース	機能情報
ISG：AAA ワイヤレス拡張機能	12.2(33)SRE	この機能は ISG RADIUS プロキシを機能拡張し、モバイル ワイヤレス環境に対する追加サポートを提供します。この機能には、RADIUS アトリビュート 31 の処理に関する変更が含まれています。 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 RADIUS プロキシに関する情報」（P.142） • 「RADIUS プロキシとしての ISG の設定方法」（P.144） この機能によって、次のコマンドが導入されました。**session-identifier**、**calling-station-id format**
ISG：認証：RADIUS プロキシ WiMax 拡張機能	12.2(33)SRE 12.2(33)XNE	この機能は ISG RADIUS プロキシを機能拡張し、WiMax ブロードキャスト環境に対する追加サポートを提供します。 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。 • 「ISG RADIUS プロキシに関する情報」（P.142） • 「RADIUS プロキシとしての ISG の設定方法」（P.144） 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。

表 14　ISG RADIUS プロキシの機能情報 （続き）

機能名	リリース	機能情報
ISG：ポリシー制御：ISG 用 RADIUS プロキシ拡張機能	12.2(31)SB2 12.2(33)SRC 12.2(33)SRE	この機能は、ISG が、RADIUS 認証を使用するクライアント デバイスと AAA サーバ間でプロキシとして機能するようにします。この機能では、モバイル加入者に対する認証要求を特定の RADIUS サーバへ送信する必要がある PWLAN およびワイヤレス メッシュ ネットワークにおいて、ISG を展開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。 • 「ISG RADIUS プロキシに関する情報」（P.142） • 「RADIUS プロキシとしての ISG の設定方法」（P.144） この機能によって、次のコマンドが導入または変更されました。**aaa authorization radius-proxy**、**aaa server radius proxy**、**accounting method-list**、**accounting port**、**authentication port**、**clear radius-proxy client**、**clear radius-proxy session**、**client**（ISG RADIUS プロキシ）、**debug radius-proxy**、**initiator radius-proxy**、**key**（ISG RADIUS プロキシ）、**message-authenticator ignore**、**proxy**（ISG RADIUS プロキシ）、**show radius-proxy client**、**show radius-proxy session**、**timer**（ISG RADIUS プロキシ） 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。

RADIUS ベースのポリシング

RADIUS ベースのポリシング機能では、Intelligent Services Gateway（ISG）として動作しているルータで、特定のセッションおよびサービスのポリシング レートを自動的に変更できるようになります。

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、「RADIUS ベースのポリシングの機能情報」（P.174）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

RADIUS ベースのポリシングの前提条件

ポリシー マップ内のクラスを参照する前に、ISG のすべてのトラフィック クラスを設定する必要があります。

ISG が ANCP ベースの動的サービス ポリシーを作成および適用する前に、ISG 上で QoS ポリシー マップを設定および適用する必要があります。

RADIUS ベースのポリシングの制約事項

サービス単位のポリシングを、階層ポリシーの親レベルで class-default クラスに設定することはできません。サービス単位のポリシングは、子レベルまたは孫レベルの class-default クラスで設定できます。

一時ポリシーは、running-configuration ファイルに現れません。オリジナルのポリシー設定のみが現れます。

パラメータ化された Quality of Service（QoS）は、IP セッションに対してはサポートされていません。

パラメータ化されたアクセス コントロール リスト（pACL）名は、最大 80 文字に制限されています。pACL 名は、RADIUS Change of Authentication（CoA）または Access-Accept メッセージの ACL エントリと、ISG に設定されている ACL 名を連結することで形成されます。pACL 名が 80 文字を超えると、パラメータ化の操作は失敗し、エラー メッセージが表示されます。CoA メッセージの場合は、ISG が RADIUS サーバに negative Ack（Nack）応答も送信します。

RADIUS ベースのポリシングに関する情報

RADIUS ベースのポリシング機能を設定するには、次の点を理解しておく必要があります。

- 「RADIUS アトリビュート」（P.160）
- 「VSA 1 としてパラメータ化された QoS ポリシー」（P.163）
- 「QoS ACL のパラメータ化」（P.163）

RADIUS アトリビュート

RADIUS は、Access-Accept および CoA メッセージに特別なアトリビュートを埋め込むことによって、ISG デバイスと通信します。RADIUS ベースのポリシングは、このアトリビュート交換を使用してサービスをアクティブまたは非アクティブにして、セッションに適用されているアクティブな QoS ポリシーを変更します。

ここでは、RADIUS ベースのポリシングで使用されている RADIUS のアトリビュートについて説明します。

- 「RADIUS アトリビュート 250 および 252」（P.161）
- 「Cisco VSA 1」（P.161）

RADIUS アトリビュート 250 および 252

RADIUS は Access-Accept メッセージでアトリビュート 250 を使用し、CoA メッセージでアトリビュート 252 を使用して、パラメータ化されたサービスをアクティブおよび非アクティブにします。ISG サービスは ISG デバイス上にローカルに設定されており、RADIUS はサービス名のみを送信します。

アトリビュート 250 および 252 には、サービスのアクティベーションについて次の構文があります。

- Access-Accept メッセージ

```
250 "Aservice(parameter1=value,parameter2=value,...)"
```

- CoA メッセージ

```
252 0b "service(parameter1=value,parameter2=value,...)"
```

RADIUS は、サービスを非アクティブにするときに、CoA メッセージのアトリビュート 252 のみを使用します。RADIUS はアトリビュート 252 で、サービスのアクティベーションで使用したものと同じ情報を使用します。ただし、サービスの非アクティベーションでは、サービスのアクティベーションで使用した 0b パラメータの代わりに、構文で 0c を使用します。

```
252 0xC "service(parameter1=value,parameter2=value,...)"
```

VSA 252 には、サービスの非アクティベーションについて上記の構文があります。

Cisco VSA 1

RADIUS は Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）1 コマンドを使用して、セッション上のアクティブな QoS ポリシーを変更します。この VSA の形式は次のとおりです。

```
av-pair = "policy-type=command 9 parameter1 ,...,parametern"
```

セッション上でアクティブになっている QoS ポリシーに対して、クラスおよび QoS アクションを追加したり削除したりするには、次の Cisco VSA 1 形式を使用します。

```
qos-policy-in=add-class(target,(class-list),qos-actions-list)
qos-policy-out=add-class(target,(class-list),qos-actions-list)
qos-policy-in=remove-class(target,(class-list))
qos-policy-out=remove-class(target,(class-list))
```

RADIUS メッセージに指定されているポリシング パラメータを使用して ISG を作成できるようにするには、セッションで QoS ポリシーをアクティブにしておく必要があります。指定されたディレクションで QoS ポリシーがアクティブになっていない場合、ISG はポリシーを作成しません。

Cisco VSA に指定されている変更を実装するときに、ISG は、ISG デバイスに設定されているオリジナルの QoS ポリシーは変更しません。代わりに対象のセッションでアクティブな QoS ポリシーをコピーし、そのポリシー コピーに必要な変更を加えます。このポリシーは、*一時ポリシー*と呼ばれます。ISG デバイス上に最初に設定されている QoS ポリシーは変更されません。

ここでは、アクティブなポリシーのポリシング パラメータを自動的に変更するための、Cisco VSA 1 コマンドについて説明します。

- 「Add-Class プリミティブ」（P.162）
- 「Remove-Class プリミティブ」（P.163）

Add-Class プリミティブ

QoS アクションをトラフィック クラスに追加または変更するには、add-class プリミティブを使用します。このアトリビュートの形式は次のとおりです。

```
qos-policy-in=add-class(target,(class-list),qos-actions-list)
qos-policy-out=add-class(target,(class-list),qos-actions-list)
```

- *target* フィールド：変更する QoS ポリシーを表します。このフィールドで有効な値は sub のみです。これは加入者セッションに割り当てられているアクティブな QoS ポリシーを意味します。このアトリビュートを含んでいる Access-Accept メッセージまたは CoA メッセージは、加入者セッションを対象にしている必要があります。
- *class-list* フィールド：丸括弧で囲まれたクラス名のリストで、指定された QoS アクションが適用されるトラフィック クラスを識別します。指定するクラス名は、ユーザが設定したクラス マップか、またはシステムで生成された class-default クラスのいずれかにする必要があります。クラス名を指定した順序は、QoS ポリシー内のクラスの階層レベルを表しています。

たとえば、次のクラス リストは「voip」という名前のクラスを表します。これはネストされたポリシーに追加されます。VoIP クラスは、親の class-default クラスに適用されている、ネストされた子ポリシーに設定されます。

```
(class-default, voip)
```

- ISG の設定

```
policy-map child
    class voip
        police 8000

policy-map parent
    class class-default
        service-policy child
```

次のクラス リストは voip-2 クラスを指定しています。これは、ネストされたポリシーに設定され、そのポリシーは、ネストされた他の子ポリシーの voip-aggregate クラスに適用されます。次に、voip-aggregate クラスを含んでいるポリシーは、ターゲット セッションに割り当てられている QoS ポリシーの class-default クラスの下でネストされています。

```
(class-default, voip-aggregate, voip-2)
```

- MSQ の設定

```
policy-map child2
    class voip-2
        police 8000

policy-map child1
    class voip-aggregate
        police 20000
        service-policy child2

policy-map parent
    class class-default
        shape 512000
        service-policy child1
```

qos-actions-list フィールドは、ポリシングなどの QoS アクションを表します。その後に丸括弧で囲まれたアクション パラメータが続き、カンマで区切られます。たとえば、次の設定例は、ポリシング アクションを表し、パラメータ *bps*、*burst-normal*、*burst-max*、*conform-action*、*exceed-action*、および *violate-action* を定義しています。アクション パラメータは丸括弧で囲みます。

```
(voip-aggregate police(200000,9216,0,transmit,drop,drop))
```

（注） この例では、最後に閉じ括弧が二重になっています。これは、VSA の構文で、target、class-list、および qos-actions-list を丸括弧で囲んで指定するためです。

Remove-Class プリミティブ

セッションにおけるアクティブな QoS ポリシーで定義されているトラフィック クラスと QoS アクションを削除するには、remove-class プリミティブを使用します。このアトリビュートの形式は次のとおりです。

```
qos-policy-in=remove-class(target,(class-list))
qos-policy-out=remove-class(target,(class-list))
```

- *target* フィールド：変更する QoS ポリシーを表します。このフィールドで有効な値は sub のみです。これは加入者セッションに割り当てられているアクティブな QoS ポリシーを意味します。このアトリビュートを含んでいる Access-Accept メッセージまたは CoA メッセージは、加入者セッションを対象にしている必要があります。
- *class-list* フィールド：丸括弧で囲まれたクラス名のリストで、削除する 1 つまたは複数のクラスを識別します。指定するクラス名は、ユーザが設定したクラス マップか、またはシステムで生成された class-default クラスのいずれかにする必要があります。クラス名を指定した順序は、QoS ポリシー内のクラスの階層レベルを表しています。

たとえば、次の VSA1 アトリビュートは、親の class-default クラスに適用されているネストされた子ポリシーから、Class1 クラス、および関連するすべての QoS ポリシーを削除します。

```
qos-policy-out=remove-class(sub,(class-default,Class1))
```

ある QoS ポリシーから 1 つのトラフィック クラスを削除すると、そのクラスのすべてのアトリビュートも削除されます。同じアトリビュートを持つクラスをもう一度追加するには、add-class RADIUS アトリビュートを再発行し、必要なパラメータと値を提示する必要があります。

VSA 1 としてパラメータ化された QoS ポリシー

CoA メッセージ内の複数の複合文字列はサポートされません。次の例に示すように、VSA 1 の動作が訂正されないからです。

```
vsa cisco 250 S152.1.1.2
vsa cisco generic 252 binary 0b suffix "q-p-out=IPOne1-isg-acct1(1)((c-d,tv)1(10000))"
vsa cisco generic 252 binary 0b suffix "q-p-out=IPOne1-isg-acct(1)((c-d,voip)1(10000))"
```

この例では次の動作になります。

- ターゲット上ですべてのサービスがイネーブルになる。
- 2 番めのコマンド構文でパラメータ化されている QoS ポリシーは、ISG サービスでエコーされない。
- 最初のコマンド構文でパラメータ化されている QoS ポリシーはエコーされる。

QoS ACL のパラメータ化

パラメータ化された QoS アクセス コントロール リストの機能は、1 つの Access-Accept メッセージまたは CoA メッセージにおける ISG および QoS の複数のパラメータ化されたサービスをサポートします。この機能により、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）デバイスでパラメータを動的に変更できます。

RADIUS ベースのポリシングの設定方法

RADIUS サーバは、RADIUS 上の加入者のユーザ プロファイルに設定されている Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）、および ISG から受け取った Advanced Node Control Protocol（ANCP）通知レートに基づいて、新しいポリシング レートを決定します。RADIUS は新しいレートを、Access-Accept メッセージまたは CoA メッセージの ISG へ送信します。

Access-Accept または CoA メッセージを受け取った後、ISG はセッションに適用されたオリジナルのポリシー マップをコピーし、コピーされた一時ポリシーのポリシング レートを、RADIUS に示されたとおりに変更します。ISG は、オリジナルのポリシーのシェーピング レートは変更しません。一時ポリシーを変更した後で、ISG は一時ポリシーを加入者サービスへ適用します。

ここでは、次の作業について説明します。

- 「RADIUS を使用したサービス単位のポリシングの設定」（P.164）
- 「RADIUS ベースのポリシングの確認」（P.168）

RADIUS を使用したサービス単位のポリシングの設定

サービス単位のポリシングを設定するには、次の設定作業を実行します。

- 「ポリシングを使用した階層的 QoS 子ポリシーの設定」（P.164）
- 「ポリシングを使用した階層的 QoS 親ポリシーの設定」（P.166）
- 「RADIUS サーバでのサービス単位のポリシングの設定」（P.167）

ポリシングを使用した階層的 QoS 子ポリシーの設定

ポリシングを使用して階層的 QoS 子ポリシーを設定するには、次の手順を使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-name*
5. **shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** offset} **aal5** *subscriber-encap*]
6. **police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
7. **exit**

手順の詳細

	コマンド	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。

	コマンド	目的
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** *policy-map-name* 例： `Router(config)# policy-map child`	ポリシー マップを作成または変更し、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。 • *policy-map-name* はポリシー マップの名前です。
ステップ 4	**class** *class-name* 例： `Router(config-pmap)# class voip`	指定するトラフィック クラスに対して QoS パラメータを設定し、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。 • *class-name* は、**class-map** コマンドを使用して以前に設定したトラフィック クラスの名前です。
ステップ 5	**shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*] 例： `Router(config-pmap-c)# shape average 10000`	表示されたビット レートにトラフィックをシェーピングします。 • **average** は、それぞれの間隔で送信されたビットの最大数です。PRE3 でのみ使用できます。 • *mean-rate* は、1 秒あたりの Committed Information Rate（CIR; 認定情報レート）ビット（bps）です。
ステップ 6	**police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*] 例： `Router(config-pmap-c)# police 10000`	トラフィック ポリシングを設定します。 • *bps* は平均レート（bps）です。有効値は 8000 ～ 200000000 です。 • （任意）*burst-normal* はノーマル バースト サイズ（バイト）です。有効値は 1000 ～ 51200000 です。デフォルトのノーマル バースト サイズは 1500 バイトです。 • （任意）*burst-max* は超過バースト サイズ（バイト）です。有効値は 1000 ～ 51200000 です。 • **conform-action** *action* は、レート制限に適合するパケットで実行するアクションです。 • **exceed-action** *action* は、レート制限を超えるパケットで実行するアクションです。 • （任意）**violate-action** *action* は、ノーマルおよび超過バースト サイズに違反するパケットで実行するアクションです。
ステップ 7	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。 **（注）** 作成する各子ポリシー マップに対してステップ 1 ～ 5 を繰り返します。または、各ポリシー マップに定義するそれぞれのトラフィック クラスに対してステップ 2 ～ 5 を繰り返します。トラフィック クラスに対して、**shape** コマンドまたは **police** コマンドのいずれかを指定しますが、同じクラスに両方のコマンドを指定しないでください。各トラフィック クラスに対して、**priority**, **set precedence** や **random-detect** コマンドなど、他のコマンドを指定することもできます。トラフィック クラスに対して指定できるコマンドの詳細については、『*Cisco 10000 Series Router Quality of Service Configuration Guide*』を参照してください。

Police コマンドのアクション

次のキーワードを使用して、**police** コマンドでアクションを指定できます。

- **drop**：パケットをドロップします。
- **set-cos-transmit** *value*：パケットの Class of Service（COS）値を設定し、送信します。
- **set-discard-class-transmit** *value*：パケットの廃棄クラス アトリビュートを設定します。
- **set-dscp-transmit** *value*：IP Differentiated Services Code Point（DSCP）の値を設定します。
- **set-frde-transmit** *value*：Frame Relay フレームに、0 から 1 のフレーム リレー Discard Eligibility（DE）を設定します。
- **set-mpls-experimental-imposition-transmit** *value*：付けられたラベル ヘッダーに、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Experimental（EXP）ビット（0 ～ 7）を設定します。
- **set-mpls-experimental-topmost-transmit** *value*：入力または出力インターフェイスで、最上位の MPLS ラベル ヘッダーに MPLS EXP フィールドの値を設定します。
- **set-prec-transmit** *value*：IP precedence の値を設定します。
- **set-qos-transmit** *value*：QoS グループ値を設定します。
- **transmit**：パケットを送信します。パケットは変更されません。

ポリシングを使用した階層的 QoS 親ポリシーの設定

ポリシングを使用して階層的 QoS 親ポリシーを設定するには、次の手順を使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class class-default**
5. **shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*]
6. **service-policy** *policy-map-name*
7. **exit**

手順の詳細

	コマンド	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	目的
ステップ 3	**policy-map** *policy-map-name* 例： `Router(config-pmap)# policy-map parent`	ポリシー マップを作成または変更します。 • *policy-map-name* はポリシー マップの名前です。
ステップ 4	**class class-default** 例： `Router(config-pmap)# class class-default`	class-default traffic クラスを変更し、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 5	**shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*] 例： `Router(config-pmap-c)# shape average 10000`	表示されたビット レートにトラフィックをシェーピングします。 • **average** は、それぞれの間隔で送信されたビットの最大数です。PRE3 でのみ使用できます。 • *mean-rate* は 1 秒あたりの CIR ビットです。
ステップ 6	**service-policy** *policy-map-name* 例： `Router(config-pmap-c)# service-policy child`	親の class-default クラスに子ポリシー マップを適用します。 • *policy-map-name* は子ポリシー マップの名前です。
ステップ 7	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。

RADIUS サーバでのサービス単位のポリシングの設定

RADIUS を使用して加入者サービスに対してポリシングを設定するには、RADIUS のサービス プロファイルで次の Cisco VSA を設定します。

```
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-list), shape(rate))"
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-list), police(rate))"
```

ISG は、これらの VSA が含まれている RADIUS の Access-Accept メッセージまたは CoA メッセージを受け取ると、セッションにおいてアクティブな状態のオリジナルのポリシー マップをコピーし、class-list フィールドに指定されているトラフィック クラスのポリシング レートを変更します。ISG は一時ポリシーのみ変更し、一時ポリシーを加入者サービスに適用します。オリジナルのポリシー マップは変更しません。

（注） サービス単位のポリシングは、親の class-default クラスには適用されません。

詳細については、「RADIUS アトリビュート」（P.160）を参照してください。

RADIUS ベースのポリシングの確認

ISG での RADIUS ベースのポリシングの設定を確認するには、特権 EXEC モードで次のいずれかのコマンドを使用します。

コマンド	目的
Router# **show policy-map interface**	すべてのインターフェイスに割り当てられたすべてのポリシー マップに設定されている、すべてのクラスの設定を表示します。
Router# **show policy-map interface** *interface* [**input** | **output**]	指定されたインターフェイスに割り当てられたすべてのインバウンドまたはアウトバウンド ポリシー マップに設定されている、すべてのクラスの設定を表示します。 *interface* はインターフェイスまたはサブインターフェイスの名前です。 **input** は、割り当てられているインバウンド ポリシーの統計を表します。 **output** は、割り当てられているアウトバウンド ポリシーの統計を表します。**input** または **output** を指定しなかった場合、ルータは指定されたインターフェイスに割り当てられたすべてのインバウンドおよびアウトバウンド ポリシーに設定されている、すべてのクラスの情報を表示します。
Router# **show policy-map** *policy-map-name*	指定するポリシー マップに含まれているすべてのトラフィック クラスの設定を表示します。 *policy-map-name* は表示する設定情報のポリシー マップの名前です。 *policy-map-name* 引数の値を指定しなかった場合、このコマンドはルータに設定されたすべてのポリシー マップの設定を表示します。
Router# **show policy-map** *policy-map-name* **class** *class-name*	指定するクラスの設定を表示します。指定するポリシー マップには、このクラスが含まれています。 *policy-map-name* は、表示するクラスの設定が含まれているポリシー マップの名前です。 *class-name* は、対象とする設定を持つクラスの名前です。*class-name* 引数の値を指定しなかった場合、このコマンドはポリシー マップに設定されたすべてのクラスの設定を表示します。
Router# **show policy-map session** [**output** | **output** | *uid*]	セッションごとに、設定されているインバウンドまたはアウトバウンド ポリシー マップを表示します。加入者セッションに適用されている動的なポリシー マップも表示します。いずれの引数も指定しなかった場合、このコマンドはすべてのセッションおよび設定されたポリシー マップを表示しますが、この表示によりパフォーマンスに影響を与えることがあります。 **input** はインバウンド ポリシー マップを表します。 **output** はアウトバウンド ポリシー マップを表します。 *uid* はセッション ID を表します。
Router# **show running-config**	running-configuration ファイルを表示します。このファイルには、ルータの現行の設定、およびデフォルトの QoS ポリシーが含まれています。
Router# **show running-config interface** *interface*	指定したインターフェイスの中で、running-config ファイルに現在設定されているインターフェイスの設定、およびそのインターフェイスに割り当てられているサービス ポリシーを表示します。

RADIUS ベースのポリシングの設定例

ここでは、次の設定例について説明します。

QoS ACL のパラメータ化の追加：例

次の例は、CoA または Access-Accept メッセージを通じて、発信元 IP アドレスおよび宛先 IP アドレスのセット パラメータ、set-src-dst-ip-in-acl をパラメータ化する方法を示しています。パラメータ化された QoS サービスは、パラメータ化された QoS サービスの RADIUS フォームに追加されます。

```
VSA252 0b q-p-out=IPOne(1)((c-d,voip)13(201.10.1.0/28,202.3.20/29))
! The above command activates the service in a CoA message.

vsa cisco generic 1 string
"qos-policy-out=add-class(sub,(class-default,voip),set-src-dst-ip-in-acl(10.10.1.0/28,10.3
.20/29))"
! The above command activates the service in a Access-Accept message.
```

ルータは次のように設定されます。

```
ip access-list extended IPOne-acl
 remark Voice-GW
 permit ip host 10.0.1.40 any
!
class-map match-any voip
  match access-group name IPOne-acl
!
class-map type traffic match-any IPOne
 match access-group output name IPOne-acl
 match access-group input name IPOne-acl
 !
!
policy-map type service IPOne
 10 class type traffic IPOne
  accounting aaa list default
 !
!
policy-map output_parent
  class class-default
    police 32000 32000 32000 conform-action transmit exceed-action drop violate-action
drop
  service-policy output_child
  !
!
policy-map output_child
  class voip
    police 32000 32000 32000 conform-action transmit exceed-action drop violate-action
drop
    !
  !
!
! RADIUS relays the string for service activation. After the VSA is received, a new ACL is
created.
ip access-list extended IPOne-acl-10.10.1.0/28,10.3.20/29
 remark Voice-GW
```

```
 permit ip host 10.0.1.40 any
 permit ip 10.10.1.0 0.0.0.15 any
 permit ip any 10.10.1.0 0.0.0.15
 permit ip 10.3.2.0 0.0.0.7 any
 permit ip any 10.3.2.0 0.0.0.7
!
! A new class map is created.
class-map match-any voip-10.10.1.0/28,10.3.20/29
  match access-group name IPOne-acl-10.10.1.0/28,10.3.20/29
!
! The old class is replaced with the new class in the output QoS policy of the subscriber,
along with any other attributes.
```

ISG サービス アカウンティングによる QoS ACL のパラメータ化の追加

次の例は、ISG アカウンティング サービスを設定することにより、QoS アカウンティングを追加する方法を示しています。

```
policy-map type service IPOne
 10 class type traffic IPOne
  accounting aaa list default
 !
 class type traffic default in-out
 !
!
! After the VSA is received, a new traffic class map is created on the service.
class-map type traffic match-any IPOne-10.10.1.0/28,10.3.2.0/29
 match access-group output name IPOne-acl-10.10.1.0/28$10.3.2.0/29
 match access-group input name IPOne-acl-10.10.1.0/28$10.3.2.0/29
!
! A new ISG service is created.
policy-map type service IPOne(tc_in=IPOne-acl-10.10.1.0/28$10.3.2.0/29)
 10 class type traffic IPOne-10.10.1.0/28,10.3.2.0/29
  accounting aaa list default
 !
 class type traffic default in-out
!
```

Access-Accept メッセージを使用したポリシング レートの設定：例

ここでは、access-accept メッセージを使用してトラフィック クラスのポリシング レートを設定する方法の例を示します。

ISG オリジナル ポリシー

この設定例では、RADIUS Access-Accept メッセージを使用して、階層的なポリシーの子レベルで、トラフィック クラスのポリシング レートを変更します。

```
class-map match-any Premium
    match access-group name Premium_Dest
!
policy-map Child
    class Premium
    shape average 5000
!
policy-map Parent
    class class-default
        shape average 10000
        service-policy Child
!
ip access-list extended Premium_Dest
permit ip any 192.168.6.0 0.0.0.255
```

```
permit ip any 192.168.5.7 0.0.0.64
```

RADIUS の設定

次の Cisco VSA は、RADIUS のユーザ プロファイルに設定されています。この VSA は、Child ポリシーの Premium クラスのポリシング レートを変更します。Child ポリシーは、Parent ポリシーの class-default クラスに適用されます。

```
radius subscriber 6
    framed protocol ppp
    service framed
    vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default, Premium),
    police(200000))"
```

RADIUS の Access-Accept メッセージ

ISG は、次の RADIUS Access-Accept メッセージを受け取ります。ユーザ プロファイルに設定されている上記の Cisco VSA は、Access-Accept メッセージ内にあることに注意してください。

```
1d21h: RADIUS: Received from id 1645/3 192.168.1.6:1812, Access-Accept, len 100
1d21h: RADIUS: authenticator 4A 2C F7 05 4B 88 38 64 - DE 60 69 5A 4B EE 43 E1
1d21h: RADIUS: Framed-Protocol [7] 6 PPP [1]
1d21h: RADIUS: Service-Type [6] 6 Framed [2]
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default, Premium),
police(200000))"
1d21h: RADIUS(0000000D): Received from id 1645/3
1d21h: SSS PM [uid:4][65ADE2E8]: SERVICE: Adding Service attachment to event
1d21h: RADIUS/ENCODE(0000000D):Orig. component type = PPoE
1d21h: RADIUS(0000000D): Config NAS IP: 0.0.0.0
1d21h: RADIUS(0000000D): sending
```

ISG の一時ポリシー

ISG はセッションに現在適用されているサービス ポリシーをコピーし、適切な変更を行う New_Parent という名前の一時ポリシーを作成します。Access-Accept メッセージに含まれている Cisco VSA に基づいて、ISG は Premium トラフィック クラスにポリシング レートを追加します。Premium クラスは一時的な New_Child ポリシーに設定され、New_Parent の class-default クラスに適用されます。

```
policy-map New_Child[New cloned child policy]
    class Premium
        police 200000[New policing rate]
        shape average 5000
!
policy-map New_Parent[New cloned parent policy]
    class class-default
        shape average 10000
        service-policy New_Child[New cloned child policy attached to the new
            cloned parent policy]
```

CoA メッセージを使用したポリシング レートの設定：例

ここでは、CoA メッセージを使用してサービスのポリシング レートを設定する方法の例を示します。

ISG オリジナル ポリシー

この設定例は、RADIUS CoA メッセージを使用して、サービスのポリシング レートを変更します。この変更は、次の ISG 設定に基づいています。

```
policy-map Child
    class Premium
        police 12000
```

```
!
policy-map Parent
    class class-default
        shape average 10000
        service-policy Child
```

RADIUS の設定

次の Cisco VSA は、RADIUS のユーザ プロファイルに設定されています。この VSA は Child ポリシーの Premium クラスを変更します。これは、Parent ポリシーの class-default クラスに適用されます。

```
radius subscriber 1048
    vsa cisco 250 S192.168.1.10
    vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default, Premium),
    police(200000))"
```

RADIUS CoA メッセージ

ISG は、次の RADIUS CoA メッセージを受け取ります。ユーザ プロファイルに設定されている上記の Cisco VSA は、CoA メッセージ内にあることに注意してください。

```
1d21h: RADIUS: COA received from id 0 192.168.1.6:1700, CoA Request, len 106
1d21h: COA: 192.168.1.6 request queued
1d21h: RADIUS: authenticator FF A2 6B 63 06 F0 E6 A3 - 0D 04 6C DC 01 0A BE F1
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.10"
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default, Premium),
police(200000))"
1d21h: ++++++ CoA Attribute List ++++++
1d21h: 63C829B0 0 00000009 ssg-account-info(427) 10 S192.168.1.10
1d21h: 63C82A18 0 00000009 qos-policy-out(378) 45 add-class(sub,(class-default, Premium),
police(200000))
1d21h:

ISG#
1d21h: RADIUS(00000000): sending
1d21h: RADIUS(00000000): Send CoA Ack Response to 192.168.1.6:1700 id 0, len 65
1d21h: RADIUS: authenticator 62 B4 B0 1A 90 10 01 01 - F6 C8 CD 17 79 15 C7 A7
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.10"
1d21h: RADIUS: Vendor, Cisco [26] 27
1d21h: RADIUS: ssg-account-info [250] 21 "$IVirtual-Access2.2"
```

ISG の一時ポリシー

ISG はセッションに現在適用されている Parent という名前のサービス ポリシーをコピーし、適切な変更を行う New_Parent という名前の一時コピーを作成します。Access-Accept メッセージに含まれている Cisco VSA に基づいて、ISG は Premium トラフィック クラスのポリシング レートを 5000 ～ 200,000 bps の範囲で変更します。Premium クラスは New_Child ポリシーに設定され、New_Parent の class-default クラスに適用されます。

```
policy-map New_Child[New cloned child policy]
    class Premium
        police 200000[New policing rate]
!
policy-map New_Parent[New cloned parent policy]
    class class-default
        shape average 10000
        service-policy New_Child[New cloned child policy attached to the new
            cloned parent policy]
```

その他の参考資料

ここでは、RADIUS ベースのポリシング機能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
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*』

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

RADIUS ベースのポリシングの機能情報

表 15 に、このモジュールの機能を示します。

このテクノロジーの機能でここに記載されていない情報については、『Cisco 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 15 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 15　RADIUS ベースのポリシングの機能情報

機能名	リリース	機能情報
ISG：ポリシー制御：ポリシー サーバ：RADIUS ベースのポリシング	12.2(33)XNE	RADIUS ベースのポリシング機能は、RADIUS サーバを使用して加入者のポリシー情報を提供できるように、ISG 機能を拡張したものです。 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。 • 「RADIUS ベースのポリシングに関する情報」（P.160） • 「RADIUS ベースのポリシングの設定方法」（P.164）
RADIUS ベースのポリシング アトリビュートの変更	12.2(33)XNE	RADIUS ベースのポリシング アトリビュートの変更機能では、Access-Accept および CoA メッセージに特別なアトリビュートを埋め込むことによって、RADIUS サーバが ISG と通信できます。RADIUS ベースのシェーピングおよびポリシングは、このアトリビュート交換を使用してサービスをアクティブまたは非アクティブにして、セッションに適用されているアクティブな QoS ポリシーを変更します。 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。 • 「RADIUS ベースのポリシングに関する情報」（P.160） • 「RADIUS ベースのポリシングの設定方法」（P.164）
QoS ACL のパラメータ化	12.2(33)XNE	QoS ACL のパラメータ化機能により、QoS ACL が拡張されます。この機能により、AAA デバイスでパラメータを動的に変更できます。 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。 • 「RADIUS ベースのポリシングに関する情報」（P.160） • 「RADIUS ベースのポリシングの設定方法」（P.164）

自動加入者ログインのための 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。このモジュールでは、認可要求でユーザ名の代わりに指定された ID を使用し、加入者からパケットを受信するとすぐに、ユーザ プロファイルを Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバからダウンロードできるように ISG を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、「ISG 自動加入者ログインの機能情報」（P.187）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 自動加入者ログインの前提条件

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 自動加入者ログインの機能情報」（P.187）を参照してください。

ご使用の AAA の実装によっては、ユーザ プロファイルのパスワード フィールドで、送信元 IP アドレス、MAC アドレス、リモート ID、回線 ID のいずれかの ID を設定する必要があります。また、パスワード フィールドへのグローバル アドレスの設定が必要になることもあります。

IP セッションの許可で回線 ID およびリモート ID を使用するには、DSLAM が DHCP Option 82 情報に回線 ID およびリモート ID を挿入する必要があります。

PPPoE セッションの許可でリモート ID を使用するには、PPPoE クライアントが PPPoE Tag ID または回線 ID にリモート ID 情報を提供する必要があります。

ISG 自動加入者ログインの制約事項

認可要求のユーザ名フィールドには、253 文字の制限があります。

トラフィック クラスに基づいた自動加入者ログインは、Cisco 7600 ルータでは設定できません。

ISG 自動加入者ログインに関する情報

- 「ISG 自動加入者ログインの概要」（P.178）
- 「ISG 自動加入者ログインでサポートされる ID」（P.179）
- 「回線 ID およびリモート ID に基づいた認可」（P.179）
- 「ISG 自動加入者ログインが設定されている場合のアカウンティング動作」（P.179）

ISG 自動加入者ログインの概要

サービス プロバイダーは通常、IP セッションの開始時にポリシーを実装します。このポリシーは、すべての加入者パケットを認証用のログイン ポータルへリダイレクトします。認証が正常に終了すると、加入者ごとの認可データが AAA サーバから返されます。いくつかの展開（通常は、加入者ネットワークがスプーフィングおよび Denial of Service（DoS; サービス拒絶）攻撃から十分に保護されているような展開）では、サービス プロバイダーは、認証を省略し、加入者の身元を信頼しようとします。ISG 自動加入者ログインにより、サービス プロバイダーは加入者がログインしなくても、サービスへの特定の加入者アクセスを許可できます。

ISG 自動加入者ログインでは、認可要求でユーザ名の代わりに、指定された ID を使用できます。AAA サーバが、指定された ID に基づいて加入者を許可できることにより、加入者からパケットを受け取るとすぐに、AAA サーバから加入者のプロファイルをダウンロードできるようになります。

自動加入者ログインをトリガーするイベントは、session-start です。IP セッションでは、DHCP DISCOVER 要求を受け取ったとき、または認証されていない送信元 IP アドレスが検出されたときに session-start が発生します。PPPoE セッションでは、PPPoE Active Discovery Initiation（PADI）パケットを送信してクライアントがセッションを開始しようとしたときに、session-start が発生します。

ISG 自動加入者ログインでサポートされる ID

IP セッションでは、認可要求でユーザ名の代わりに、IP アドレス、MAC アドレス、回線 ID、リモート ID、または回線 ID とリモート ID の組み合わせの ID を使用するよう、ISG デバイスを設定できます。

PPPoE セッションでは、認可要求でユーザ名の代わりにリモート ID を使用するよう ISG デバイスを設定できます。

回線 ID およびリモート ID に基づいた認可

回線 ID およびリモート ID のフィールドは、DHCP リレー エミュレート情報のオプション（Option 82 とも呼ばれる）の一部で、PPPoE Tag VSA です。これらのフィールドは、DSLAM によって DHCP および PPPoE メッセージに挿入されます。認可要求で回線 ID、リモート ID、または回線 ID とリモート ID の組み合わせをユーザ名として使用するよう、ISG デバイスを設定できます。

デフォルトでは、ISG デバイスは回線 ID とリモート ID を使用します。これはレイヤ 2 のエッジ アクセス デバイスによって認可用に提供されます。**ip dhcp relay information option** コマンドが設定されている場合、ISG デバイスは、DHCP メッセージ内で受け取る回線 ID およびリモート ID を使用します。

ISG 自動加入者ログインが設定されている場合のアカウンティング動作

MAC アドレスに基づく認可のアカウンティング動作

認可要求でユーザ名として MAC アドレスが送信されると、MAC アドレスは、アカウンティング レコードの発信ステーション ID としても送信されます。

リモート ID および回線 ID に基づく認可のアカウンティング動作

DHCP Option 82 認可を使用している IP セッションでは、アカウンティング メッセージとともに、回線 ID とリモート ID Cisco VSA が AAA サーバに送信されます。認可用のユーザ名として回線 ID とリモート ID の組み合わせを設定できますが、そのアトリビュートはアカウンティング レコードでは個別に送信されます。アカウンティング レコード内で、NAS Port ID として回線 ID とリモート ID をまとめて送信するよう設定することも可能です。

PPPoE セッションでは、アカウンティング レコードで Remote ID VSA が送信され、NAS Port ID としてリモート ID も送信されます。

radius-server attribute 31 remote-id コマンドが設定されている場合、リモート ID はアカウンティング レコード内で発信ステーション ID として送信されます。

自動加入者ログインのための ISG ポリシーの設定方法

制御ポリシー クラス マップにおける自動ログインのトラフィック識別

ISG 自動加入者ログインが適用される対象についてトラフィックを指定する、制御ポリシー クラス マップを設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type control match-all** *class-map-name*
4. **match source-ip-address** *ip-address subnet-mask*

   または

   match nas-port circuit-id *name*

   または

   match nas-port remote-id *name*
5. **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	**class-map type control match-all** *class-map-name* 例： `Router(config)# class-map type control match-all TAL-subscribers`	制御クラス マップを作成します。これは、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します。

	コマンドまたはアクション	目的
ステップ 4	**match source-ip-address** *ip-address subnet-mask* または **match nas-port circuit-id** *name* または **match nas-port remote-id** *name* **例：** `Router(config-control-classmap)# match source-ip-address 10.1.1.0 255.255.255.0` または **例：** `Router(config-control-classmap)# match nas-port circuit-id circuit1` または **例：** `Router(config-control-classmap)# match nas-port remote-id remote1`	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。 または 加入者の回線 ID が、指定された値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。 または 加入者のリモート ID が、指定された値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 5	**end** **例：** `Router(config-control-classmap)# end`	（任意）特権 EXEC モードに戻ります。

自動加入者ログインのための ISG 制御ポリシーの設定

加入者の認可を開始し、指定された ID を、認可要求のユーザ名フィールドに挿入する ISG 制御ポリシーを設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*]
6. **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 TAL`	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** {*class-map-name* | **always**} **event session-start** 例： `Router(config-control-policymap)# class type control TAL-subscribers event session-start`	関連付けられているアクション セットを実行するために満たす必要のある条件を定義する、制御クラスを指定します。 • 「制御ポリシー クラス マップにおける自動ログインのトラフィック識別」の作業で設定した制御クラスマップを指定します。
ステップ 5	*action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*] 例： `Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier source-ip-address`	指定された ID を認可要求のユーザ名フィールドに挿入します。
ステップ 6	**end** 例： `Router(config-control-policymap-class-control)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

次の作業

service-policy type control コマンドを使用して、制御ポリシーをコンテキストに適用する必要があります。制御ポリシーの適用の詳細については、「Configuring ISG Control Policies」モジュールを参照してください。

ポリシーを設定して、自身の IP アドレスまたは MAC アドレスの認可が失敗した自動ログインの加入者に対して、どのような処置をするかを確認したい場合があります。たとえば、加入者を、認証用のポリシー サーバにリダイレクトする、といった場合です。

Calling-Station-ID として送信するリモート ID のイネーブル化

アカウンティング レコードおよびアクセス要求の Calling-Station-ID（アトリビュート 31）フィールドで、ISG デバイスがリモート ID を送信できるようにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute 31 remote-id**

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	**radius-server attribute 31 remote-id** 例： `Router#(config) radius-server attribute 31 remote-id`	アカウンティング レコードおよびアクセス要求の Calling Station ID（アトリビュート 31）フィールドで、ISG デバイスがリモート ID を送信できるようにします。

ISG 自動加入者ログインの確認

自動加入者ログインが成功したかどうかを確認するには、この作業を実行します。

手順の概要

1. **enable**
2. **show subscriber session**

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。

ステップ 2 **show subscriber session**

ISG 加入者セッションの情報を表示するには、**show subscriber session** コマンドを使用します。出力で、セッションが「authen」のステートで開始されたことが示された場合、自動加入者の認可は成功しています。自動加入者の認可が成功しなかった場合、セッションは開始されますが、ステートは「unauthen」になっています。

次の出力例は、自動加入者の認可が成功したセッションの情報を示しています。

```
Router# show subscriber session all

Current Subscriber Information: Total sessions 1
------------------------------------------------
Unique Session ID: 3
Identifier: aabb.cc01.3000
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:24, Last Changed: 00:00:21

Policy information:
  Authentication status: authen
  Rules, actions and conditions executed:
    subscriber rule-map DEFAULT
      condition always event session-start
        1 authorize identifier mac-address

Session inbound features:
 Feature: IP Idle Timeout
  Timeout value is 600
  Idle time is 00:00:21
Configuration sources associated with this session:
Interface: Ethernet0/0, Active Time = 00:00:24
```

ISG 自動加入者ログインの設定例

IP アドレスに基づいた自動加入者ログイン：例

次の例では、クライアントが 1.1.1.0 サブネットからのものである場合、ISG は認可要求を、加入者の送信元 IP アドレスをユーザ名として「TAL_LIST」に送信します。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。

ISG の設定

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

aaa authorization network 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 10.1.1.0 255.255.255.0
```

```
!
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 service-policy type service aaa list LOCAL name redirectprofile
  3 set-timer TIMERB 5 minutes
!
 class type control CONDF event timed-policy-expiry
  1 service disconnect
```

ユーザ プロファイルの設定

```
1.1.1.1 Password = "cisco"
 Service-Type = Outbound,
 Cisco:Account-Info = "AAuto-Internet;proxy-user;cisco"
```

サーバ プロファイルの設定

```
Auto-Internet Password = "cisco"
 Cisco:Service-Info = "IAuto-Internet",
 Cisco-Avpair = "traffic-class=input access-group 100"

proxy-user Password = "cisco"
 Idle-Timeout = 5
```

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*』

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 自動加入者ログインの機能情報

表 16 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 16 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 16　ISG 自動加入者ログインの機能情報

機能名	リリース	機能設定情報
ISG：セッション：認証（MAC、IP）	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG 自動加入者ログインでは、認可要求でユーザ名の代わりに、IP アドレスまたは MAC アドレスを使用することができます。この機能により、加入者からパケットを受け取るとすぐに、AAA サーバから加入者のプロファイルをダウンロードできます。 このモジュールでは、この機能について説明します。 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：認証：DHCP オプション 82 ライン ID：AAA 認証サポート	12.2(28)SB 12.2(33)SRC 15.0(1)S	この機能は、回線 ID およびリモート ID に基づいて認可に対するサポートを提供することにより、ISG 自動加入者ログインの機能を拡張します。 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。 • 「ISG 自動加入者ログインでサポートされる ID」（P.179） • 「回線 ID およびリモート ID に基づいた認可」（P.179） • 「ISG 自動加入者ログインが設定されている場合のアカウンティング動作」（P.179） • 「自動加入者ログインのための ISG ポリシーの設定方法」（P.180） 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。

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon 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。DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon 機能を使用すると、サービス プロバイダーは Dynamic Host Configuration Protocol（DHCP）オプション 60 およびオプション 82 によって Transparent Automatic Logon（TAL）をサポートでき、オプション 82 への Virtual Private Network（VPN; バーチャル プライベート ネットワーク）ID 拡張によってホールセール型の IP セッションをサポートできるため、家庭向けのトリプルプレイ サービスをプロビジョニングできるようになります。

この機能はプラットフォームに依存せず、Cisco 7600 ルータ、Cisco 7200 ルータ、および Cisco 7301 ルータでサポートされます。

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、「DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の機能情報」（P.197）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

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の前提条件

認可に使用されるベンダー クラス ID（オプション 60）には、カスタマーのアプライアンス（PC、電話機、またはセットトップ ボックス）によってベンダー クラス ID を DHCP オプション 60 の情報に挿入する必要があります。

ホールセール型 IP セッションのプロビジョニングでは、VPN-ID を回線 ID およびリモート ID と一緒に DHCP オプション 82 の情報に挿入する必要があります。

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の制約事項

RADIUS プロキシ ユーザは、この機能でサポートされません。

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon に関する情報

ISA Automatic Subscriber Logon

TAL を使用すると、指定された ID を認可要求でユーザ名の代わりに使用できます。Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバによる指定された IP に基づく加入者の認可をイネーブルにすると、加入者からのパケットが受信されるとすぐに、AAA サーバから加入者のプロファイルをダウンロードできます。

セッションの開始は、TAL をトリガーするイベントです。DHCP で開始された IP セッションの場合、DHCP DISCOVER 要求の受信時にセッションが開始されます。

オプション 60 およびオプション 82 に基づく認可

回線 ID およびリモート ID フィールド（オプション 82）は、DHCP リレー エージェント情報オプションの一部です。Digital Subscriber Line Access Multiplexer（DSLAM; デジタル加入者線アクセス マルチプレクサ）は、オプション 82 のフィールドを DHCP メッセージに挿入し、カスタマーのアプライアンスはオプション 60 のフィールドを挿入します。

認可要求でユーザ名として回線 ID、リモート ID、またはベンダー クラス ID、あるいはこれらの組み合わせを使用するように ISG ポリシーを設定できます。また、NAS-Port-ID を認可の ID として使用するように ISG ポリシーを設定することもできます。NAS-Port-ID を ID として使用する場合、回線 ID、リモート ID、およびベンダー クラス ID の組み合わせを含めるように設定できます。

デフォルトでは、ISG でレイヤ 2 エッジ アクセス デバイスによって認可のために指定される回線 ID とリモート ID を使用します。**ip dhcp relay information option** コマンドの設定によって、ISG が受信したオプション 82 の情報を使用して独自に情報を生成するか、または（**encapsulate** キーワードが指定されている場合に）以前のオプション 82 を独自のオプション 82 と一緒にカプセル化するかが指定されます。詳細については、『*Cisco IOS IP Addressing Services Configuration Guide*』の「Configuring the Cisco IOS DHCP Relay Agent」を参照してください。

オプション 60 およびオプション 82 を含めるように NAS-Port-ID が設定されていない場合、NAS-Port-ID が DHCP リレー エージェント情報パケットを受信した ISG インターフェイス（たとえば、Ethernet1/0）で入力されます。

DHCP オプション 82 および VPN-ID サブオプション

IP セッションのホールセール サービスをサポートするには、認可要求で VPN-ID を回線 ID およびリモート ID と一緒に指定する必要があります。Transparent Automatic Logon 機能用の VPN-ID サポート付き DHCP オプション 60 およびオプション 82 では、家庭内のデバイスを差別化できるように、2 セットのオプション 82 の情報を 1 つのメッセージに含めることができます。

- オプション 82 の情報の 1 番めのセットには、家庭内のデバイスに関連付ける家庭の情報とオプション 60 が含まれます。
- オプション 82 の情報の 2 番めのセットには、VPN-ID が設定されている場合、家庭の VPN 情報が含まれます。

DHCP サーバは、VPN-ID、リモート ID、回線 ID、およびアドレスを割り当てるためのオプション 60 の情報とともに、リレーによって転送されたオプション 82 の情報を処理します。

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の設定方法

認可のためのユーザ名または NAS-Port-ID を使用して、TAL 用の ISG ポリシーを設定できます。

- 「オプション 60 およびオプション 82 を使用した ISG 制御ポリシーの設定」（P.192）
- 「NAS-Port-ID を使用した ISG 制御ポリシーの設定」（P.193）
- 「オプション 60 およびオプション 82 を含む NAS-Port-ID の設定」（P.194）

オプション 60 およびオプション 82 を使用した ISG 制御ポリシーの設定

認可要求のユーザ名フィールドに指定された ID を挿入する ISG 制御ポリシーを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*]
6. **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 TAL`	制御ポリシー マップ コンフィギュレーション モードを開始して、制御ポリシーを定義します。
ステップ 4	**class type control** {*class-map-name* | **always**} **event session-start** 例： `Router(config-control-policymap)# class type control TAL-subscribers event session-start`	制御ポリシー マップ クラス コンフィギュレーション モードを開始して、関連付けられた実行するアクションのセットと一致させる必要のある条件を定義します。 • 「Identifying Traffic for Automatic Logon in a Control Policy Class Map」の項で設定された制御クラス マップを指定します。
ステップ 5	*action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*] 例： `Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier source-ip-address vendor-class-id plus circuit-id plus remote-id`	指定された ID を認可要求のユーザ名フィールドに挿入します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-control-policymap-class-control)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

NAS-Port-ID を使用した ISG 制御ポリシーの設定

認可要求の NAS-Port-ID で使用する ISG 制御ポリシーを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier nas-port**
6. **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 TAL`	制御ポリシー マップ コンフィギュレーション モードを開始して、制御ポリシーを定義します。
ステップ 4	**class type control** {*class-map-name*	**always**} **event session-start** 例： `Router(config-control-policymap)# class type control TAL-subscribers event session-start`	制御ポリシー マップ クラス コンフィギュレーション モードを開始して、関連付けられた実行するアクションのセットと一致させる必要のある条件を定義します。 • 「Identifying Traffic for Automatic Logon in a Control Policy Class Map」の項で設定された制御クラス マップを指定します。

	コマンドまたはアクション	目的
ステップ 5	*action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier nas-port** 例： `Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier nas-port`	NAS ポート ID を認可要求のユーザ名フィールドに挿入します。
ステップ 6	**end** 例： `Router(config-control-policymap-class-control)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

オプション 60 およびオプション 82 を含む NAS-Port-ID の設定

オプション 60 およびオプション 82 を含めた NAS-Port-ID 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. **radius-server attribute nas-port-id include** {*identifier1* [**plus** *identifier2*] [**plus** *identifier3*]} [**separator** *separator*]

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	**radius-server attribute nas-port-id include** {*identifier1* [**plus** *identifier2*] [**plus** *identifier3*]} [**separator** *separator*] 例： `Router(config)# radius-server attribute nas-port-id include circuit-id plus vendor-class-id`	NAS-Port-ID のオプション 60 およびオプション 82 に DHCP リレー エージェントを含めます。

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の設定例

例：NAS-Port-ID のオプション 60 およびオプション 82

次の例では、**radius-server attribute nas-port-id include** コマンドを使用して、回線 ID、リモート ID、およびベンダー クラス ID を使用したオプション 60 およびオプション 82 の認可を設定します。

```
interface Ethernet0/0
 service-policy type control RULEA
!
interface Ethernet1/0
 service-policy type control RULEB
!
class-map type control match-all CONDA
 match source-ip-address 10.1.1.0 255.255.255.0
!
class-map type control match-all CONDB
 match vendor-class-id vendor1
!
policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier vendor-class-id
!
policy-map type control RULEB
 class type control CONDB event session-start
  1 authorize aaa list TAL_LIST password cisco identifier nas-port
!
radius-server attribute nas-port-id include circuit-id plus remote-id plus vendor-class-id
separator #
```

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*』
自動加入者ログインのための ISG ポリシーの設定	『*Cisco IOS Intelligent Services Gateway Configuration Guide*』の「Configuring ISG Policies for Automatic Subscriber Logon」の項
DHCP リレー エージェントの設定	『*Configuring the Cisco IOS DHCP Relay Agent*』の「Configuring the Cisco IOS DHCP Relay Agent」の項

規格

規格	タイトル
なし	–

MIB

MIB	MIB リンク
•	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
なし	–

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

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の機能情報

表 17 に、この機能のリリース履歴を示します。

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 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 17 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 17　DHCP オプション 60 およびオプション 82 のサポートおよび VPN-ID のサポートの機能情報

機能名	リリース	機能情報
ISG：認証：DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon	12.2(33)SRD	サービス プロバイダーは、DHCP オプション 60 およびオプション 82 によって TAL をサポートでき、オプション 82 への VPN-ID 拡張によってホールセール型の IP セッションをサポートできます。 この機能はプラットフォームに依存せず、Cisco 7600 ルータ、Cisco 7200 ルータ、および Cisco 7301 ルータでサポートされます。 次のコマンドが導入または変更されました。 **radius-server attribute nas-port-id include**

ISG と外部ポリシー サーバとの相互動作のイネーブル化

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。このマニュアルでは、ISG がセッション ポリシーを取得したり、外部ポリシー サーバからのセッション ポリシーの動的アップデートを受け入れられるように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、「ISG と外部ポリシー サーバとの相互動作の機能情報」（P.209）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 と外部ポリシー サーバとの相互動作に関する制約事項

ISG と外部ポリシー サーバは、同じ Virtual Routing and Forwarding（VRF）インスタンスで使用できる必要があります。

ISG と外部ポリシー サーバとの相互動作に関する情報

初期認可と動的認可

ISG は、加入者別およびサービス別の情報が格納された*ポリシー サーバ*と呼ばれる外部デバイスと連携動作します。ISG は、ISG と外部ポリシー サーバとの間で対話の 2 つのモデル（初期認可と動的認可）をサポートしています。

初期認可モデルでは、ISG は、セッションの特定の時点で、外部ポリシー サーバからポリシーを取得する必要があります。このモデルでは、一般的に、外部ポリシー サーバは RADIUS を使用した Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバです。ISG は、RADIUS クライアントになります。AAA サーバの代わりに、一部のシステムは、Lightweight Directory Access Protocol（LDAP）など、他のデータベース プロトコルに変換される RADIUS プロキシ コンポーネントを使用します。

動的認可モデルでは、外部ポリシー サーバは、ISG に対して動的にポリシーを送信できます。これらの処理は、（サービスの選択を通じて）加入者がインバンド方式で開始することも、管理者の操作を通じて開始することもできます。または、アプリケーションは、何らかのアルゴリズムに基づいてポリシーを変更できます（たとえば、1 日の特定の時間に、セッションの Quality of Service（QoS）を変更します）。このモデルは、Change of Authorization（CoA）RADIUS 拡張によって容易になります。CoA は、RADIUS にピアツーピア機能を導入し、ISG と外部ポリシー サーバがそれぞれ RADIUS クライアントおよびサーバとして動作できます。

ISG のトリプルキー認証

トリプルキー認証は、ISG が Cisco Service Management Engine（SME）ポータルにユーザをリダイレクトした後に、ユーザ名、パスワード、およびロケーションに基づいて、ユーザを認証する方法です。SME サーバは、認証を受ける加入者の発信元 IP アドレスに基づいて、ロケーション情報を提供します。トリプルキー認証サポート機能が導入される前には、ユーザは、ユーザ名とパスワードだけに基づいて認証されていました（2 キー認証）。また、トリプルキー認証機能によって、Service Selection Gateway（SSG）から ISG プラットフォームへの移行も容易になります。これは、SSG がトリプルキー認証を使用しているためです。

SSG に対して、Cisco Subscriber Edge Services Manager（SESM）サーバは、加入者のロケーションを含む文字列とともに SSG に送信するユーザ ログイン要求に、RADIUS アトリビュート 31（calling-station ID）を追加します。次に、SSG は、RADIUS サーバに送信するアクセス要求メッセージにこの値を含めます。RADIUS サーバでは、ユーザ名、パスワード、およびロケーションの文字列に基づいて、ログインが認証されます。

ISG トリプルキー認証では、SME が CoA アカウント ログイン要求のアトリビュート 31 で ISG に送信するロケーション文字列は、ISG が加入者を認証するために RADIUS サーバに送信するアクセス要求パケットで繰り返し使用されます。ISG は、RADIUS サーバへのアクセス要求メッセージに含まれる Cisco Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）でロケーション文字列を送信します。

アトリビュート 31 と Cisco VSA SME の両方で、SME からのアカウント ログイン要求にロケーション情報が含まれる場合は、Cisco VSA ロケーション文字列の値が優先されます。ロケーション情報は、アトリビュート 31 または Cisco VSA 250 のいずれかとして SME から受信されます。ロケーション情報は、セッション認証要求、ISG からのセッション アカウンティング要求、およびプリペイド認可要求に含まれます。

表 18 に、トリプルキー認証に使用される Cisco Vendor-Specific non-AVPair アトリビュートを示します。

表 18　Cisco Vendor-Specific Non-AVPair アトリビュート

サブアトリビュート ID	アトリビュート タイプ	値	機能	例	使用場所
250	account-info	L<*location-string*>	トリプルキー認証の 3 番めのキー	LWiFiHotSpot001	アクセス要求 CoA 要求 アカウンティング

ISG と外部ポリシー サーバとの相互動作を可能にする方法

AAA クライアントとしての ISG の設定

AAA メソッド リストを設定し、ISG が AAA サーバからポリシーを取得できるようにするには、次のタスクを実行します。このタスクは、初期認可モデルと動的認可モデルの両方で実行する必要があります。

前提条件

AAA メソッドで参照されるサーバとサーバ グループを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
4. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands level** | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
6. **aaa authorization subscriber-service** {**default** {**cache** | **group** | **local**} | *list-name*} *method1* [*method2...*]
7. **aaa service-profile key username-with-nasport**
8. **aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands level**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*
9. **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	**aaa authentication login** {**default** | *list-name*} *method1* [*method2*...] 例： `Router(config)# aaa authentication login PPP1 group radius`	ログイン時に使用する 1 つ以上の AAA 認証方法を指定します。
ステップ 4	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...] 例： `Router(config)# aaa authentication ppp default group radius`	PPP を実行しているシリアル インターフェイスで使用する、1 つ以上の AAA 認証方法を指定します。
ステップ 5	**aaa authorization** {**network** | **exec** | **commands level** | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2*...]] 例： `Router(config)# aaa authorization network NET1 radius`	ネットワークへの加入者のアクセスを制限するために使用する、1 つ以上の AAA 認可方法を指定します。
ステップ 6	**aaa authorization subscriber-service** {**default** {**cache** | **group** | **local**} | *list-name*} *method1* [*method2*...] 例： `Router(config)# aaa authorization subscriber-service default local group radius`	サービスの提供で使用する、ISG 用の 1 つ以上の AAA 認可方法を指定します。 • **cache**、**group**、または **local** キーワードと組み合わせて使用する **default** キーワードによって、認可方法に対して、それぞれデフォルト キャッシュ グループ、サーバ グループ、またはローカル データベースが選択されます。
ステップ 7	**aaa service-profile key username-with-nasport** 例： `Router(config)# aaa service-profile key username-with-nasport`	AAA セッションのサービス プロファイル パラメータを設定します。

	コマンドまたはアクション	目的
ステップ 8	**aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands level**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name* **例：** `Router(config)# aaa accounting network default start-stop group radius`	課金またはセキュリティ目的のために、要求されたサービスの AAA アカウンティングをイネーブルにします。
ステップ 9	**end** **例：** `Router(config)# end`	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。

AAA サーバとしての ISG の設定

動的認可によって、ポリシー サーバは ISG に対してポリシーを動的に送信できます。AAA サーバとして ISG を設定し、動的認可をイネーブルにするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa server radius dynamic-author**
4. **client** {**name** | *ip-address*} [**key** [**0** | **7**] *word*] [**vrf** *vrf-id*]
5. **port** *port-number*
6. **server-key** [**0** | **7**] *word*
7. **auth-type** {**all** | **any** | **session-key**}
8. **ignore** {**server-key** | **session-key**}
9. **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。

	コマンドまたはアクション	目的
ステップ 3	**aaa server radius dynamic-author** 例： `Router(config)# aaa server radius dynamic-author`	ISG を AAA サーバとして設定します。 • 動的認可ローカル サーバ コンフィギュレーション モードを開始します ÅB
ステップ 4	**client** {**name** | *ip-address*} [**key** [**0** | **7**] *word*] [**vrf** *vrf-id*] 例： `Router(config-locsvr-da-radius)# client 10.76.86.90 key cisco`	ISG が通信するクライアントを指定します。
ステップ 5	**port** *port-number* 例： `Router(config-locsvr-da-radius)# port 1600`	RADIUS サーバ ポートを指定します。 • デフォルト値は 1700 です。
ステップ 6	**server-key** [**0** | **7**] *word* 例： `Router(config-locsvr-da-radius)# server-key cisco`	RADIUS クライアントと共有する暗号キーを指定します。
ステップ 7	**auth-type** {**all** | **any** | **session-key**} 例： `Router(config-locsvr-da-radius)# auth-type all`	セッション認可に使用するアトリビュートを指定します。
ステップ 8	**ignore** {**server-key** | **session-key**} 例： `Router(config-locsvr-da-radius)# ignore session-key`	共有暗号キーまたはアトリビュート 151 を無視するように ISG を設定します。
ステップ 9	**end** 例： `Router(config-locsvr-da-radius)# end`	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。

トリプルキー認証用のロケーション VSA のイネーブル化

ISG が認証要求とアカウンティング要求にロケーション VSA を含められるようにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server vsa send accounting**
5. **radius-server vsa send authentication**

6. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。 • 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 new-model** 例： `Router(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**radius-server vsa send accounting** 例： `Router(config)# radius-server vsa send accounting`	ISG が RADIUS アトリビュート 26 によって定義されるアカウンティング VSA を認識し、使用できるようにします。
ステップ 5	**radius-server vsa send authentication** 例： `Router(config)# radius-server vsa send authentication`	ISG が RADIUS アトリビュート 26 によって定義される認証 VSA を認識し、使用できるようにします。
ステップ 6	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

例

次に、アカウンティングと認証のために VSA を使用するように、ISG を設定する方法の例を示します。

```
aaa new-model
!
!
radius-server vsa send accounting
radius-server vsa send authentication
```

ISG と外部ポリシー サーバとの相互動作の設定例

例：ISG と外部ポリシー サーバとの相互動作

次の例では、外部ポリシー サーバと相互動作するよう ISG を設定します。

```
!
aaa group server radius CAR_SERVER
 server 10.100.2.36 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
!
aaa server radius dynamic-author
 client 10.76.86.90 key cisco
 client 172.19.192.25 vrf VRF1 key cisco
 client 172.19.192.25 vrf VRF2 key cisco
 client 172.19.192.25 key cisco
 message-authenticator ignore
```

例：トリプルキー認証

次に、ロケーション アトリビュートなどのセッション情報を含む認証レコードの例を示します。この出力は、**debug radius accounting** コマンドまたは **gw-accounting syslog** コマンドを使用して表示できます。

```
*Feb  5 01:20:50.413: RADIUS/ENCODE: Best Local IP-Address 10.0.1.1 for Radius-Server
10.0.1.2
*Feb  5 01:20:50.425: RADIUS(0000000F): Send Access-Request to 10.0.1.2:1645 id 1645/5,
len 107
*Feb  5 01:20:50.425: RADIUS:  authenticator 4D 86 12 BC BD E9 B4 9B - CB FC B8 7E 4C 8F
B6 CA
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  19
*Feb  5 01:20:50.425: RADIUS:   ssg-account-info   [250] 13  "LWiFiHotSpot001"
*Feb  5 01:20:50.425: RADIUS:  Calling-Station-Id  [31]  16  "AAAA.BBBB.CCCC"
*Feb  5 01:20:50.425: RADIUS:  User-Name           [1]   7   "george"
*Feb  5 01:20:50.425: RADIUS:  User-Password       [2]   18  *
*Feb  5 01:20:50.425: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
*Feb  5 01:20:50.425: RADIUS:  NAS-Port            [5]   6   0
*Feb  5 01:20:50.425: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Feb  5 01:20:50.425: RADIUS:  NAS-IP-Address      [4]   6   10.0.1.1
*Feb  5 01:20:50.425: RADIUS(0000000F): Started 5 sec timeout
*Feb  5 01:20:50.425: RADIUS: Received from id 1645/5 10.0.1.2:1645, Access-Accept, len 68
*Feb  5 01:20:50.425: RADIUS:  authenticator 49 A1 2C 7F C5 E7 9D 1A - 97 B3 E3 72 F3 EA 56 56
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  17
*Feb  5 01:20:50.425: RADIUS:   ssg-account-info   [250] 11  "S10.0.0.2"
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  31
*Feb  5 01:20:50.425: RADIUS:   Cisco AVpair       [1]   25  "accounting-list=default"
*Feb  5 01:20:50.433: RADIUS(0000000F): Received from id 1645/5
*Feb  5 01:20:50.437: RADIUS/ENCODE(0000000F):Orig. component type = Iedge IP SIP
*Feb  5 01:20:50.437: RADIUS(0000000F): Config NAS IP: 0.0.0.0
*Feb  5 01:20:50.437: RADIUS(0000000F): sending
```

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*』
AAA 設定作業	『*Cisco IOS Security Configuration Guide*』のパート 1「Authentication, Authorization, and Accounting (AAA)」
AAA コマンド	『*Cisco IOS Security 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 と外部ポリシー サーバとの相互動作の機能情報

表 19 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 19 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 19　ISG と外部ポリシー サーバとの相互動作の機能情報

機能名	リリース	機能情報
ISG：ポリシー制御：ポリシー サーバ：CoA	12.2(28)SB 12.2(33)SRC 12.4(20)T 15.0(1)S	この機能によって、動的認可を容易にする RADIUS Change of Authorization（CoA）拡張を ISG がサポートします。 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。 • 「初期認可と動的認可」（P.200） • 「AAA クライアントとしての ISG の設定」（P.201） • 「AAA サーバとしての ISG の設定」（P.203） 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。 Cisco IOS Release 12.4(20)T で、この機能が T シリーズに統合されました。
ISG：セッション：ライフサイクル：Packet of Disconnect（POD）	12.2(28)SB 15.0(1)S	この機能によって、外部ポリシー サーバは、RADIUS Packet of Disconnect（POD; パケット オブ ディスコネクト）を受信したときに、ISG セッションを終了できるようになります。
ISG：トリプルキー認証サポート	12.2(33)SRE2	この機能によって、アクセス要求メッセージで SESM から RADIUS サーバにロケーション情報を渡すことにより、トリプルキー認証が可能になります。 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 のトリプルキー認証」（P.200） • 「トリプルキー認証用のロケーション VSA のイネーブル化」（P.204）

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。

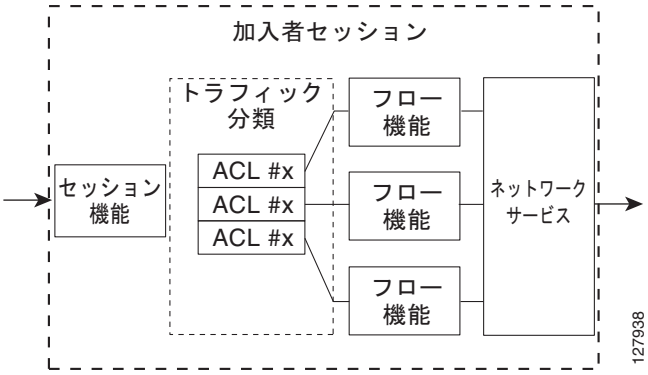
トラフィック ポリシー内に設定された機能は、そのトラフィック クラスで定義されるトラフィックに対してのみ適用されます。さまざまな機能を持つ複数のトラフィック ポリシーを、1 つのセッションに適用することができます。

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="Aservice-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）

ISG: Subscriber Aware Ethernet

ISG: Subscriber Aware Ethernet 機能は、SIP-400 または Ethernet Services Plus（ES+）アクセス側ラインカードを持つ Cisco 7600 シリーズ ルータ上に分散する IP および PPPoE セッションに、Intelligent Services Gateway（ISG）機能を提供します。

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: Subscriber Aware Ethernet の機能情報」（P.238）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: Subscriber Aware Ethernet の前提条件

次について理解している必要があります。

- High Availability（HA; ハイ アベイラビリティ）
- In-service Software Upgrade（ISSU）
- セッション メンテナンス制御
- Port-Bundle Host Key（PBHK）
- Layer 4 Redirect（L4RD）
- アカウンティング
- Access Control List（ACL; アクセス コントロール リスト）
- Quality of Service（QoS）

このような機能と ISG の連携の詳細については、『*Cisco IOS ISG Configuration Library*』を参照してください。

ハードウェア

次のハードウェアが Cisco 7600 シリーズ ルータに取り付けられている必要があります。

- Cisco ギガビット イーサネット V2 Shared Port Adapter（SPA; 共有ポート アダプタ）を装着した Cisco SIP-400 ラインカード
- Cisco Ethernet Services Plus（ES+）ラインカード
- メモリ 4 GB（推奨）の Cisco RSP720 ルート スイッチ プロセッサ（必須）

RADIUS およびポリシー サーバは必須ではありません。ただし、Cisco 7600 シリーズ ルータに ISG を実装する一般的な方式では、別筐体の RADIUS Authorization, Authentication, and Accounting（AAA; 認証、認可、アカウンティング）サーバ、つまり AAA 情報が格納された物理的に独立したサーバが必要です。

ソフトウェア

SIP-400 または Ethernet Services Plus（ES+）アクセス側ラインカードを装着した各 Cisco 7600 シリーズ ルータ用の、ISG の加入者認識イーサネット機能が入ったイメージの入手方法については、シスコの代理店へお問い合わせください。

ISG: Subscriber Aware Ethernet の制約事項

次の ISG 機能は Cisco 7600 シリーズ ルータで利用できません。

- IP 加入者機能は、次のアクセス インターフェイスではサポートされません。
  - 仮想テンプレート
  - Gigabit EtherChannel（GEC）（ポート チャネル）

（注） Cisco IOS Release 12.2(33)SRE 以降、ポート チャネルは Cisco 7600 シリーズ ルータの Ethernet Services Plus（ES+）ラインカードでのみサポートされます。また、ポート チャネルは IP インターフェイス セッションをサポートしません。

  - Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）
  - Generic Routing Encapsulation（GRE）

  - Layer 2 Tunnel Protocol（L2TP）
  - L2TP Access Concentrator（LAC）
  - L2TP Network Server（LNS）

（注） アクセス インターフェイスの詳細については、『*Cisco 7600 Series Cisco IOS Software Configuration Guide*』の「IP Subscriber Awareness over Ethernet」の章を参照してください。

- 加入者の冗長化は 1:1 のアクセス スタンバイ モデルでのみ利用できます。
- ロード バランシングは IP および PPPoE 加入者に対してサポートされません。
- Multiservice Interface（MSI）に関するインターフェイス統計情報
- トラフィック クラスはサポートされません。トラフィック クラスは Cisco 7600 シリーズ ルータには設定できません。このため、他のルータではフロー レベルで適用可能な機能（アカウンティング、アイドル タイムアウト、セッション タイムアウト、ポリサー、および L4RD）を、Cisco 7600 シリーズ ルータではセッション レベルで適用する必要があります。
- L4RD および PBHK の機能は、Route Processor（RP; ルート プロセッサ）レベルで実装されます。
- プリペイド機能。
- Dynamic Subscriber Bandwidth Selection（DBS）。
- ISG HA 機能には、次の制約事項があります。
  - スイッチオーバー時にアイドル タイマーおよびセッション タイマーが開始されます。
  - PBHK および L4RD 変換はチェックポイントの対象になりません。そのためスイッチオーバー時には、すべての変換情報が更新されます。この更新によって、既存の TCP および HTTP セッションは切断されます。
- PPPoE セッションのみに対する ambiguous VLAN のサポート。
- IP および PPPoE セッションのアクセス サブインターフェイスでの合法的傍受。
- セッションのグループ化。

Cisco 7600 シリーズ ルータの統計情報ポーリングに関して、次の点に注意してください。

- 統計情報はラインカードからルータへ 10 秒ごとに送信されます。このため、ポーリングのたびに統計情報に 10 秒間の遅れが発生します。
- アイドル タイムアウト値およびキープアライブ間隔の下限は 30 秒です。

Segment Switching Manager（SSM）インフラストラクチャは、Cisco Online Insertion and Removal（OIR; 活性挿抜）に準拠するため、SPA が取り外された場合であっても、設定が削除されていなければセッションを切断しません。この場合にセッションを確実に切断するためには、ラインカードまたは SPA を OIR で取り外す際に、セッションのキープアライブ機能を設定するか、または **clear ip subscriber slot** *slotnum* **no-hardware** コマンドを使用して、手動でセッションを消去する必要があります。

次の表に、ラインカード、インターフェイス、および設定に関するさまざまなイベントの後に、そのルータでセッションが再プロビジョニングされるか（つまり、OIR 挿入後にラインカード上で再プログラムされるか）、それとも終了されるかを示します。

表 21　　イベント統計情報

イベント	再プロビジョニング	切断
ラインカードまたは SPA の OIR 挿入	あり	なし
ラインカードまたは SPA の OIR 取り外し	なし	なし

表 21　　イベント統計情報 （続き）

イベント	再プロビジョニング	切断
ラインカードのリロード	あり	なし
インターフェイスの管理停止	なし	なし
インターフェイスの停止	なし	なし
加入者インターフェイスの設定削除	なし	あり

（注）　SPA の OIR 挿入および取り外しの影響は、Ethernet Services Plus（ES+）ラインカードには適用されません。この再プロビジョニングおよび切断に関する内容が該当するのは、PPPoE および IP セッション（L2 接続および転送）だけです。IP インターフェイス セッションには該当しません。

ルータの OIR サポートの詳細については、『*Cisco Online Insertion and Removal (OIR) Support in Routers*』を参照してください。

ISG: Subscriber Aware Ethernet に関する情報

サポートされるアクセス セッション タイプ

- インターフェイス
- スタティック IP および DHCP IP
- PPPoE

サポートされるアクセス インターフェイス

- Ethernet
- QinQ VLAN
- .1Q および QinQ アクセス インターフェイス（**access** キーワードが指定されたもの）

（注）　access キーワードは Cisco 7600 シリーズ ルータに固有のキーワードです。

- Gigabit EtherChannel（GEC）（ポート チャネル）

このポート チャネルは 1:1 の冗長構成です。また、ポート チャネル バンドル内のメンバー リンクを動的に処理できるように、Link Aggregation Control Protocol（LACP）がイネーブルになっています。ポート チャネルには 2 つのメンバーがあり、一方のメンバーがアクティブで、もう一方のメンバーがスタンバイ状態になります。メンバーのポートには、異なるラインカードのポートを使用できますが、Ethernet Services Plus（ES+）ラインカードにする必要があります。

アクセス インターフェイスの詳細については、『*Cisco 7600 Series Cisco IOS Software Configuration Guide*』の「IP Subscriber Awareness over Ethernet」の章を参照してください。

サポートされる IP セッション

- IP セッションとの DHCP の統合
- スタティック IP サブネット セッション
- 送信元 IP アドレスおよび MAC アドレス セッション（IP セッション）

サポートされる PPP セッション

- PPPoE
- PPPoEoVLAN
- PPPoEoQinQ

（注） Cisco IOS Release 12.2(33)SRC では、PPP および IP セッションをサポートするのは、Cisco 7600 シリーズ ルータのイーサネット インターフェイスのみです。

サポートされるサービス

- アイドル タイムアウト
- セッション タイムアウト
- IP セッションに関する Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）および Address Resolution Protocol（ARP; アドレス解決プロトコル）のキープアライブ
- 条件付きデバッグ（ラインカードではなくルータでサポートされます）
- 動的 Virtual Private Network（VPN）選択
- 限定的 PBHK および L4RD
- ポリシー制御：ポリシー サーバ：Change of Authorization（CoA）ASCII コマンド コード サポート
- QoS
- セッション アカウンティング
- セキュリティ：ユーザ単位の ACL

セッションおよび呼び出しのサポート

- ISG の加入者認識イーサネット機能は、ISG 機能について最大 32,000 のセッションをサポートします。
- Dynamic Host Control Protocol（DHCP; 動的ホスト制御プロトコル）では、1 秒あたり最大 50 の呼び出しがサポートされます。

ISG: Subscriber Aware Ethernet の設定方法

Cisco 7600 シリーズ ルータに ISG: Subscriber Aware Ethernet を設定する方法の詳細については、『*Cisco 7600 Series Cisco IOS Software Configuration Guide*』の「IP Subscriber Awareness over Ethernet」の章を参照してください。

ISG: Subscriber Aware Ethernet の設定例

ISG: Subscriber Aware Ethernet の設定の詳細および具体的な作業については、『*Cisco 7600 Series Cisco IOS Software Configuration Guide*』の「Configuration Examples」を参照してください。

その他の参考資料

関連資料

内容	参照先
ISG 機能の設定	• 『*IP Subscriber Awareness over Ethernet*』 • 『*Cross-Platform Release Notes for Cisco IOS Release 12.2SB*』
ISG コマンド	『*Cisco IOS ISG Command Reference*』
ルータの OIR サポート	『*Cisco Online Insertion and Removal (OIR) Support in Routers*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

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。またこの機能による既存 MIB のサポートに変更はありません。	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
この機能がサポートする新規 RFC または改訂 RFC はありません。また、この機能による既存 RFC の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: Subscriber Aware Ethernet の機能情報

表 22 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 22 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 22　ISG: Subscriber Aware Ethernet の機能情報

機能名	リリース	機能情報
ISG: Subscriber Aware Ethernet	12.2(33)SRC 15.0(1)S	ISG: Subscriber Aware Ethernet 機能は、SIP-400 アクセス側ラインカードを持つ Cisco 7600 シリーズ ルータ上に分散する IP および PPPoE セッションに、Intelligent Services Gateway（ISG）機能を提供します。 12.2(33)SRC では、この機能が Cisco 7600 シリーズ ルータで追加されました。 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: Subscriber Aware Ethernet に関する情報」（P.234） • 「ISG: Subscriber Aware Ethernet の設定方法」（P.236） 次のコマンドが、新たに導入または変更されました。**clear ip subscriber**、**show ccm clients**、**show ccm queues**、**show ccm sessions**、**show ip subscriber**
ISG：セッション：マルチキャスト：共存	12.2(33)SRE	Cisco IOS Release 12.2(33)SRE では、Cisco 7600 シリーズのルータに ISG セッション マルチキャスト共存機能のサポートが追加されました。
Cisco 7600 ES+ シリーズ ラインカードでの IP セッション サポート	12.2(33)SRE	Cisco IOS Release 12.2（33）SRE では、ES+ シリーズ ラインカードに対する IP および PPPoE セッション サポートが、Cisco 7600 シリーズ ルータに追加されました。
ポート チャネルでの PPPoE および IPoE セッション サポート（1:1 冗長構成）	12.2(33)SRE	Cisco IOS Release 12.2(33)SRE では、ポート チャネルの PPPoE および IPoE セッション サポートが、Cisco 7600 シリーズ ルータに追加されました。

ISG ネットワーク転送ポリシーの設定

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 ネットワーク転送ポリシーは、アップストリーム ネットワークとのパケットのルーティングまたは転送を可能にする転送ポリシーのタイプです。このモジュールでは、ネットワーク転送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 ネットワーク ポリシーの機能情報」（P.246）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 ネットワーク転送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 ネットワーク ポリシーの機能情報」（P.246）を参照してください。

ISG ネットワーク転送ポリシー設定の制約事項

サービスには 1 つのネットワーク転送ポリシーのみを含めることができます。

各加入者セッションで、一度にネットワーク転送ポリシーの 1 つのインスタンスのみを有効にできます。

ISG ネットワーク ポリシーに関する情報

- 「ネットワーク ポリシー」（P.240）
- 「ネットワーク ポリシーのソースの設定」（P.240）

ネットワーク ポリシー

加入者パケットがネットワークに到達するには、何らかの形式の転送を加入者セッションに指定する必要があります。アップストリーム ネットワークとのパケットのルーティングまたは転送を可能にするトラフィック ポリシーは、*ネットワーク転送ポリシー*とも呼ばれます。

ネットワーク転送ポリシー タイプがルーティングの場合、転送の決定はレイヤ 3 で実行され、Virtual Routing and Forwarding（VRF）識別子を指定して、ルーティングの決定を行うために使用する必要のあるルーティング テーブルを示す必要があります（各 VRF は 1 つのルータ内の独立したルーティング コンテキストを示す）。ネットワーク ポリシー タイプが転送の場合、転送の決定はレイヤ 2 で実行されます。これは、すべての加入者パケットがシステム内の 1 つの仮想エンドポイントに転送されるか、またはその逆方向に転送されることを意味します。この仮想エンドポイントはレイヤ 2 トンネルを表し、トンネル識別子は使用すべきトンネルを決定します。ネットワーク転送ポリシーが指定されていない場合、グローバル ルーティング テーブルがトラフィックのルーティングに使用されます。

ネットワーク転送ポリシーが含まれる ISG 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。

ネットワーク ポリシーのソースの設定

ネットワーク ポリシーは、外部 Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバのユーザ プロファイルおよびサービス プロファイル、または ISG 対応デバイス上のサービス ポリシー マップで設定できます。ユーザ プロファイルで設定されたネットワーク転送ポリシーは、サービスで指定されたネットワーク転送ポリシーよりも優先されます。

ネットワーク転送ポリシーがユーザ プロファイルまたはサービス プロファイルで指定されていない場合、ISG セッションは別のソースからネットワーク サービスを継承します。ISG は次のソースからネットワーク サービスを継承できます。

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

これらの設定ソースは、優先順位の高い順に示してあります。たとえば、仮想テンプレートに設定されたネットワーク転送ポリシーは、インターフェイス上で設定されたネットワーク転送ポリシーよりも優先されます。

各加入者セッションで、一度にネットワーク転送ポリシーの 1 つのインスタンスのみを有効にできます。

ISG ネットワーク ポリシーの設定方法

- 「サービス ポリシー マップ内の PPP セッション用ネットワーク ポリシーの設定」（P.241）
- 「サービス ポリシー マップ内の IP セッション用ネットワーク ポリシーの設定」（P.243）

サービス ポリシー マップ内の PPP セッション用ネットワーク ポリシーの設定

ネットワーク ポリシーは、外部 AAA サーバのユーザ プロファイルおよびサービス プロファイル、または ISG デバイス上のサービス ポリシー マップで設定できます。ISG デバイス上のサービス ポリシー マップ内の PPP セッションにネットワーク転送ポリシーを設定するには、次の作業を実行します。

（注） ネットワーク転送ポリシーがユーザ プロファイル、サービス プロファイル、またはサービス ポリシー マップで指定されていない場合、加入者セッションは別のソースからネットワーク転送ポリシーを継承します。詳細については、「ネットワーク ポリシーのソースの設定」（P.240）を参照してください。

前提条件

この作業は、Virtual Private Dialup Network（VPDN）グループが設定されていることを前提としています。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **service vpdn group** *vpdn-group-name*

   または

   service local

   または

service relay pppoe vpdn group *vpdn-group-name*

5. **ip vrf forwarding** *name-of-vrf*

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	**service vpdn group** *vpdn-group-name* または **service local** または **service relay pppoe vpdn group** *vpdn-group-name* 例： `Router(config-service-policymap)# service vpdn group vpdn1` 例： `Router(config-service-policymap)# service local` 例： `Router(config-service-policymap)# service relay pppoe vpdn group vpdn1`	Virtual Private Dialup Network（VPDN）サービスを提供します。 または ローカル終端サービスを提供します。 または PPPoE over VPDN L2TP トンネルをリレーして、VPDN サービスを提供します。 • **service local** コマンドを設定してサービスをローカルに終端する場合、**ip vrf forwarding** コマンドを設定してセッションを終端するルーティング ドメインも指定できます。
ステップ 5	**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。 • 次のステップは、ステップ 4 で **service local** コマンドを設定した場合にだけ実行します。**service local** コマンドを設定した場合、**ip vrf forwarding** コマンドを使用して、セッションを終端するルーティング ドメインを指定できます。ルーティング ドメインを指定しなかった場合、グローバル VRF が使用されます。

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。

サービス ポリシー マップ内の IP セッション用ネットワーク ポリシーの設定

ネットワーク ポリシーは、外部 AAA サーバのユーザ プロファイルおよびサービス プロファイル、または ISG デバイス上のサービス ポリシー マップで設定できます。デバイス上のサービス ポリシー マップ内の IP セッションにネットワーク転送ポリシーを設定するには、次の作業を実行します。

（注） ネットワーク転送ポリシーがユーザ プロファイル、サービス プロファイル、またはサービス ポリシー マップで指定されていない場合、加入者セッションは別のソースからネットワーク転送ポリシーを継承します。詳細については、「ネットワーク ポリシーのソースの設定」（P.240）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**

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。

	コマンドまたはアクション	目的
ステップ 4	**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。
ステップ 5	**sg-service-type primary** 例： `Router(config-service-policymap)# sg-service-type primary`	サービスをプライマリ 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。プライマリ サービスは、**sg-service-type primary** コマンドを使用してプライマリ サービスとして定義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。

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。

ISG ネットワーク ポリシーの設定例

PPP セッション用ネットワーク転送ポリシー：例

次に、PPP セッションのためにネットワーク転送ポリシーで設定されたサービス ポリシー マップの例を示します。

```
policy-map type service my_service
 service vpdn group vpdn1
```

IP セッション用ネットワーク転送ポリシー：例

次に、IP セッションのためにネットワーク転送ポリシーで設定されたサービス ポリシー マップの例を示します。

```
policy-map type service my_service
 ip vrf forwarding vrf1
```

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*』
VPDN 設定作業	『*Cisco IOS VPDN Technologies Configuration Guide*』
PPP および VPDN コマンド	『*Cisco IOS VPDN Technologies Command Reference*』

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 ネットワーク ポリシーの機能情報

表 23 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 23 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 23　ISG ネットワーク転送ポリシーの機能情報

機能名	リリース	機能設定情報
ISG：ネットワーク インターフェイス：IP ルーテッド、VRF-Aware MPLS	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG では、セッションをネットワークに接続するために複数の転送タイプがサポートされます。このような接続には、インターネット、社内のイントラネット、ISP、またはコンテンツ配信のためのウォールド ガーデンなどがあります。ISG では、ネットワーク アクセスのためにルーテッド インターフェイスおよび MPLS 対応のインターフェイスの両方がサポートされます。 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 ネットワーク ポリシーに関する情報」（P.240） • 「ISG ネットワーク ポリシーの設定方法」（P.241） 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：ネットワーク インターフェイス：トンネリング（L2TP）	12.2(28)SB 12.2(33)SRC	ISG では、セッションをネットワークに接続するために複数のインターフェイス タイプが柔軟にサポートされます。このような接続には、インターネット、社内のイントラネット、ISP、またはコンテンツ配信のためのウォールド ガーデンなどがあります。ISG では、ネットワークへのトンネル インターフェイスがサポートされます。 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 ネットワーク ポリシーに関する情報」（P.240） • 「ISG ネットワーク ポリシーの設定方法」（P.241） 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 アカウンティングの設定

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 アカウンティングを設定する方法について説明します。これにはセッション単位アカウンティングまたはフロー単位アカウンティング、ブロードキャスト アカウンティング、およびポストペイド料金切り替えが含まれます。

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 アカウンティングの機能情報」（P.266）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 アカウンティングの前提条件

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 アカウンティングの機能情報」（P.266）を参照してください。

ISG アカウンティングの制約事項

ポストペイド課金および料金の切り替えは、Cisco 10000-PRE2 ではサポートされていません。

ISG アカウンティングは、RADIUS プロトコルだけをサポートしています。

定期的アカウンティングと組み合わせて、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）ブロードキャスト アカウンティングを使用した場合、アカウンティング グループごとに異なるアカウンティング期間を設定できません。

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 ISG アカウンティングをサポートしています。

- Cisco 7600 ルータはトラフィック クラスをサポートしていないため、トラフィック クラスに基づくフロー単位アカウンティングをサポートしていません。
- ISG のポストペイド料金切り替えとサービス単位のアカウンティングは、Cisco 7600 ルータではサポートされていません。

ISG アカウンティングに関する情報

- 「ISG アカウンティングの概要」（P.248）
- 「ISG アカウンティング レコード」（P.249）
- 「中間 ISG アカウンティング アップデート」（P.250）
- 「ブロードキャスト ISG アカウンティング」（P.250）
- 「ISG ポストペイド料金切り替え」（P.250）

ISG アカウンティングの概要

ISG は、セッション単位、およびフロー単位のアカウンティングの両方をサポートしています。セッション単位のアカウンティングは、1 つのセッションについてのすべてのフロー トラフィックの合計です。セッション単位のアカウンティングは、ユーザ プロファイル、サービス プロファイル、またはサービス ポリシー マップでイネーブルにできます。

トラフィック クラスによって定義されるセッション トラフィックのサブセットを考慮したフロー単位のアカウンティングは、サービス プロファイルまたはサービス ポリシー マップでイネーブルにできます。フロー単位アカウンティングを設定する場合は、セッション単位アカウンティングとフロー単位アカウンティングを RADIUS サーバで相関付けられるよう、Parent-Session-ID Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）がアカウンティング レコードに含まれます。

ユーザ プロファイルでアカウンティングを設定した場合、サービス名アトリビュートはアカウンティング レコードに含まれません。

aaa accounting network default コマンドを設定し、AAA メソッド リストを指定した場合に、セッション アカウンティングがイネーブルになります（デフォルトのメソッド リストではなく、名前付きメソッド リストを使用することを推奨します）。フロー単位アカウンティングは、デフォルトでディセーブルになっており、サービス プロファイルまたはサービス ポリシー マップで AAA メソッド リストを指定した場合にだけ実行されます。ISG アカウンティングでは、指定した AAA メソッド リストに、Accounting-Start レコード、中間レコード、および Accounting-Stop レコードが送信されます。

ANCP ポートでの ISG アカウンティング メッセージ

Access Node Control Protocol（ANCP）ポートでセッションに対して ISG により送信されるアカウンティング メッセージには、nas-tx-speed、nas-tx-speed-bps、nas-rx-speed、および nas-rx-speed-bps の各 AAA アトリビュートが含まれます。ISG は、ISG に対して、またはインターフェイス上で設定する Quality of Service（QoS）から送信される Digital Subscriber Line Access Multiplexer（DSLAM; デジタル加入者線アクセス マルチプレクサ）ANCP 通知から、これらのアトリビュート値を取得します。

ANCP ポートが UP 状態である場合、アトリビュート値は ISG に送信される DSLAM ANCP 通知から取得されます。ANCP ポート状態が DOWN 状態に変化した場合、ANC アカウンティング メッセージには、DSLAM 通知で送信された AAA アトリビュートが引き続き含まれます。

ANCP ポート状態が UP 状態に設定されたことがない場合、ISG は、インターフェイス上の QoS ポリシーから nas-tx-speed、nas-tx-speed-bps、nas-rx-speed、および nas-rx-speed-bps の AAA アトリビュートを取得できます。

QoS ポリシーから AAA アトリビュートを取得するには、ANCP ネイバーの設定前に、ポリシーを設定する必要があります。設定されていない場合、ISG では、セッションが確立されたときの AAA アトリビュートに対する以前の値（存在する場合）が使用されます。

QoS ポリシー値が変更された場合、ISG は ANCP ネイバーが削除され、再設定されるまで、以前の値を使用し続けます。

ISG アカウンティング レコード

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。ISG は、account logon、account logoff、service logon、および service logoff の各イベントが発生したときに、AAA アカウンティング メソッド リストに対して、関連アトリビュートとともにアカウンティング レコードを送信します。アカウンティング サーバは、レコードを解釈して、ポストペイド セッションに対する課金情報を生成するように設定できます。

アカウントのログインとログオフ

加入者が ISG にログインし、または ISG からログオフしたときに、ISG では、指定した AAA メソッド リストに対して RADIUS Accounting-Request レコードが送信されます。Accounting-Request レコードに含まれる Acct-Status-Type アトリビュートは、レコードが加入者セッションのスタート（開始）またはセッションのストップ（終了）をマークしているかどうかを示します。

system、**default**、**start-stop**、および **group** キーワードを指定して **aaa accounting** コマンドをイネーブルにした場合、アカウンティング レコードが AAA サーバに送信されます。加入者がログインしたときに、ISG は、AAA サーバに Accounting-Start レコードを送信します。加入者がログオフしたときに、ISG は、Accounting-Stop レコードを送信します。

サービスのログインとログオフ

ISG は、加入者に対してサービスがアクティブになったときに、AAA サーバに RADIUS Accounting-Start レコードを送信し、サービスが非アクティブになったときに Accounting-Stop レコードを送信します。レコードには、親セッションのアカウンティング セッション ID とは異なるセッション ID が含まれています。

Accounting-Request レコードに含まれる Acct-Status-Type アトリビュートは、レコードがサービスの開始または終了をマークしているかどうかを示します。サービスの名前は、サービスのログインとログオフに対するアカウンティング レコードに含まれています。

アカウンティング レコードは、アカウントおよびサービスのログインとログオフ以外のイベントに対して送信できます。詳細については、『*Cisco IOS Security Configuration Guide,* Release 12.2』の「Configuring Accounting」の章を参照してください。

中間 ISG アカウンティング アップデート

ISG は、中間（断続的）RADIUS アカウンティング アップデートをサポートしています。これは、「ウォッチドッグ」RADIUS アカウンティングと同様に動作します。アカウンティング アップデートは、ISG によって Accounting-Start レコードと Accounting-Stop レコードが送信される間の時間に送信されます。

ISG は、新しい情報（新しい IP アドレスなど）に対するアカウンティング アップデートと、設定可能な間隔でアカウンティング レコードが送信される定期的アカウンティングの 2 種類の中間アカウンティングをサポートしています。

新しい情報の中間アカウンティングは、グローバルにイネーブルまたはディセーブルにできます。定期的アカウンティングは、グローバル、ユーザ プロファイル内、サービス内など、特定のコンテキストに対してイネーブルにできます。

ブロードキャスト ISG アカウンティング

ISG は、AAA ブロードキャスト アカウンティングをサポートしています。これは、複数の RADIUS サーバにユーザ アカウンティング レコードを送信する機能です。AAA ブロードキャスト アカウンティングは、RADIUS サーバ用に地理的冗長性をサービス プロバイダーに提供し、ホールセール モデルのパートナーにアカウンティング レコードを提供します。AAA ブロードキャスト アカウンティングの設定については、『*Cisco IOS Security Configuration Guide*』の「Authentication, Authorization, and Accounting」パートにある「Configuring Accounting」の章を参照してください。

ISG ポストペイド料金切り替え

ISG ポストペイド料金切り替えでは、接続の有効期間中に料金を変更できます。この機能は、1 日の特定の時間に料金が変更される時間ベースまたはボリューム ベースのポストペイド セッションに適用されます。

一般的に、サービス プロバイダーは、ポストペイド料金切り替えを使用して、加入者の接続中に、加入者に異なる料金を提供します。たとえば、オフピーク時間中は加入者を低料金に変更します。

ポストペイド接続に対する料金の切り替えを処理するために、アカウント パケットは、さまざまな料金切り替えの間隔中に、使用情報をログに記録します。サービス プロファイルには、料金の変更が発生する時間の詳細を示す週間料金切り替えプランが含まれます。ISG は、すべての料金切り替えポイントで使用状況をモニタし、中間アカウンティング レコードにこの情報を記録します。課金サーバは、すべての中間アカウンティング アップデートをモニタし、各料率で送信されるトラフィックに関する情報を取得します。

（注） 料金の切り替えは、時間ベースの課金サービスでは必要ありません。課金サーバは、サービスのログイン タイムスタンプとログオフ タイムスタンプを確認しているため、その時間中に適用されるさまざまな料金を計算できます。

ISG アカウンティングの設定方法

- 「ISG のセッション単位アカウンティングのイネーブル化」（P.251）（必須）
- 「ISG のフロー単位アカウンティングのイネーブル化」（P.254）（必須）
- 「ISG ポストペイド料金切り替えの設定」（P.256）（必須）
- 「ISG アカウンティングとポストペイド料金切り替えの確認」（P.257）（任意）

ISG のセッション単位アカウンティングのイネーブル化

セッション単位アカウンティングは、次の場所で設定できます。

- AAA サーバのユーザ プロファイル
- AAA サーバのサービス プロファイル
- ISG デバイスのサービス ポリシー マップ

この手順は、次のセクションから構成されます。

- 「AAA サーバのユーザ プロファイルでのセッション単位アカウンティングのイネーブル化」（P.251）
- 「AAA サーバのサービス プロファイルでのセッション単位アカウンティングのイネーブル化」（P.252）
- 「ルータのサービス ポリシー マップでのセッション単位アカウンティングのイネーブル化」（P.252）

前提条件

ISG は、ユーザ プロファイル、サービス プロファイル、またはサービス ポリシー マップで指定した AAA メソッド リストにアカウンティング レコードを送信します。このセッションのタスクは、**aaa accounting** コマンドを使用して AAA メソッド リストが設定されていることを前提としています。詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

AAA サーバは、ISG アカウンティングをサポートするように設定する必要があります。

AAA サーバのユーザ プロファイルでのセッション単位アカウンティングのイネーブル化

この手順のアトリビュートを使用して、AAA サーバのユーザ プロファイルでセッション単位アカウンティングをイネーブルにします。サービス プロファイルではなくユーザ プロファイルでアカウンティングを設定した場合、Service Name アトリビュートがアカウンティングに表示されません。

手順の概要

1. Cisco-Avpair="accounting-list=*accounting-mlist-name*"
2. IETF RADIUS attribute Acct-Interim-Interval（アトリビュート 85）

手順の詳細

ステップ 1 Cisco-Avpair="accounting-list=*accounting-mlist-name*"

ユーザ プロファイルに Accounting アトリビュートを追加します。このアトリビュートは、アカウンティングをイネーブルにし、アカウンティング アップデートを送信する AAA メソッド リストを指定します。

ステップ 2 IETF RADIUS attribute Acct-Interim-Interval（アトリビュート 85）

（任意）ユーザ プロファイルに Acct-Interim-Interval（アトリビュート 85）を追加します。このアトリビュートでは、中間アップデートの間隔を秒数で指定します。

AAA サーバのサービス プロファイルでのセッション単位アカウンティングのイネーブル化

この手順のアトリビュートを使用して、AAA サーバのサービス プロファイルでセッション単位アカウンティングをイネーブルにします。セッション単位アカウンティングでは、サービス プロファイルにトラフィック クラス アトリビュートを含めてはいけません。

手順の概要

1. Cisco-Avpair="accounting-list=*accounting-mlist-name*"
2. IETF RADIUS attribute Acct-Interim-Interval（アトリビュート 85）

手順の詳細

ステップ 1 Cisco-Avpair="accounting-list=*accounting-mlist-name*"

サービス プロファイルに Accounting アトリビュートを追加します。このアトリビュートは、アカウンティングをイネーブルにし、アカウンティング アップデートを送信する AAA メソッド リストを指定します。

ステップ 2 IETF RADIUS attribute Acct-Interim-Interval（アトリビュート 85）

（任意）サービス プロファイルに Acct-Interim-Interval（アトリビュート 85）を追加します。このアトリビュートでは、中間アップデートの間隔を秒数で指定します。

ルータのサービス ポリシー マップでのセッション単位アカウンティングのイネーブル化

ルータのサービス ポリシー マップでセッション単位アカウンティングを設定するには、空のトラフィック クラス マップ（アクセス リストを指定しないトラフィック クラス マップ）を設定し、サービス ポリシー マップの空のトラフィック クラス内でアカウンティングをイネーブルにする必要があります。サービス ポリシー マップでセッション単位アカウンティングをイネーブルにするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type traffic match-any** *class-map-name*
4. **exit**
5. **policy-map type service** *policy-map-name*
6. [*priority*] **class type traffic** *class-map-name*
7. **accounting aaa list** *AAA-method-list*

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 empty-class`	指定した ISG トラフィック クラスとのパケットの照合に使用されるトラフィック クラス マップを作成または変更し、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。 • セッション単位アカウンティングでは、空のトラフィック クラス マップを作成します。これは、トラフィックの照合用のアクセス リストを指定しないトラフィック クラス マップです。
ステップ 4	**exit** 例： `Router(config-traffic-classmap)# exit`	トラフィック クラスマップ コンフィギュレーション モードを終了します。
ステップ 5	**policy-map type service** *policy-map-name* 例： `Router(config)# policy-map type service service1`	ISG サービスの定義に使用されるサービス ポリシー マップを作成または定義し、サービス 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 6	[*priority*] **class type traffic** *class-map-name* 例： `Router(config-service-policymap)# class type traffic empty-class`	ポリシーを作成または変更する名前付きトラフィック クラスを指定し、サービス ポリシー トラフィック クラス コンフィギュレーション モードを開始します。 • このステップでは、ステップ 3 で作成した空のトラフィック クラス マップを参照します。
ステップ 7	**accounting aaa list** *AAA-method-list* 例： `Router(config-service-policymap-class-traffic)# accounting aaa list list1`	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。

次の作業

サービス ポリシー マップまたはサービス 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。

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、ISG アカウンティングをトラブルシューティングできます。

- **debug aaa accounting**
- **debug radius** [**brief**]

- **debug subscriber feature name accounting** {**event** | **error** | **detail**}

ISG のフロー単位アカウンティングのイネーブル化

ISG フロー単位アカウンティングは、次の場所で設定できます。

- AAA サーバのサービス プロファイル
- ISG デバイスのサービス ポリシー マップ

この手順は、次のセクションから構成されます。

- 「AAA サーバのサービス プロファイルでのフロー単位アカウンティングのイネーブル化」（P.254）
- 「ルータのサービス ポリシー マップでのフロー単位アカウンティングのイネーブル化」（P.255）

前提条件

ISG は、ユーザ プロファイル、サービス プロファイル、またはサービス ポリシー マップで指定した AAA メソッド リストにアカウンティング レコードを送信します。このセッションのタスクは、**aaa accounting** コマンドを使用して AAA メソッド リストが設定されていることを前提としています。詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

AAA サーバは、ISG アカウンティングをサポートするように設定する必要があります。

AAA サーバのサービス プロファイルでのフロー単位アカウンティングのイネーブル化

AAA サーバのサービス プロファイルでフロー単位アカウンティングを設定するには、次のタスクを実行します。

前提条件

このタスクは、トラフィックを指定するための IP アクセス リストが定義されていることを前提としています。

手順の概要

1. Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"
2. Cisco-Avpair="accounting-list=*accounting-mlist-name*"
3. IETF RADIUS attribute Acct-Interim-Interval（アトリビュート 85）

手順の詳細

ステップ 1 Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"

ISG トラフィック クラス アトリビュートをサービス プロファイルに追加します。このアトリビュートは、サービスの適用先となる入力トラフィックと出力トラフィックを指定します。入力と出力の両方のトラフィック分類子をサービス プロファイルに追加できます。

ステップ 2 Cisco-Avpair="accounting-list=*accounting-mlist-name*"

AAA サーバのサービス プロファイルに Accounting アトリビュートを追加します。このアトリビュートは、アカウンティングをイネーブルにし、アカウンティング アップデートを送信する AAA メソッド リストを指定します。AAA メソッド リストが設定されている必要があります。

（注） トラフィック クラスを含まないサービス プロファイルでこのアトリビュートを設定した場合、アカウンティングはフローではなく、セッションで実行されます。

ステップ 3 IETF RADIUS attribute Acct-Interim-Interval（アトリビュート 85）

（任意）AAA サーバのサービス プロファイルに、IETF RADIUS attribute Acct-Interim-Interval（アトリビュート 85）を追加します。このアトリビュートでは、中間アップデートの間隔を秒数で指定します。

ルータのサービス ポリシー マップでのフロー単位アカウンティングのイネーブル化

特定のフローに対するローカル サービス ポリシー マップでフロー単位アカウンティングをイネーブルにするには、次のタスクを実行します。

前提条件

このタスクは、トラフィック クラス マップが定義され、IP アクセス リストに関連付けられていることを前提としています。トラフィック クラスの設定の詳細については、「Configuring ISG Subscriber Services」モジュールを参照してください。

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*

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 サービスの定義に使用されるサービス ポリシー マップを作成または定義し、サービス 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。

	コマンドまたはアクション	目的
ステップ 4	[*priority*] **class type traffic** *class-map-name* 例： `Router(config-service-policymap)# class type traffic firstclass`	以前に設定したトラフィック クラスをポリシー マップに関連付け、サービス ポリシー トラフィック 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 5	**accounting aaa list** *AAA-method-list* 例： `Router(config-control-policymap-class-traffic)# accounting aaa list list1`	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。 • AAA メソッド リストが設定されている必要があります。

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、ISG アカウンティングをトラブルシューティングできます。

- **debug aaa accounting**
- **debug radius** [**brief**]
- **debug subscriber feature name accounting** {**event** | **error** | **detail**}

次の作業

サービス ポリシー マップまたはサービス 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 ポストペイド料金切り替えの設定

ISG ポストペイド料金切り替えは、AAA サーバのサービス プロファイルで設定できます。

サービス プロファイルにトラフィック クラスを含めた場合、ポストペイド料金切り替えは指定したフローに適用されます。トラフィック クラスを設定しなかった場合、ポストペイド料金切り替えはセッションに適用されます。セッション単位またはフロー単位のポストペイド料金切り替えを設定するには、次のタスクを実行します。

前提条件

ポストペイド料金切り替えが機能するためには、ISG のセッション単位またはフロー単位のアカウンティングを設定する必要があります。

手順の概要

1. Cisco-AVpair = "PPW*hh*:*mm*:*ss*:*d*"
2. Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"

手順の詳細

ステップ 1 Cisco-AVpair = "PPW*hh*:*mm*:*ss*:*d*"

Post Paid VSA をサービス プロファイルに追加します。このアトリビュートは、ポストペイド料金切り替えに対して週間料金切り替えポイントを指定します。次に、構文について説明します。

hh:*mm*:*ss*:*d*：週間料金切り替え時間。

- hh = 時間 <0 ～ 23>
- mm = 分 <0 ～ 59>
- ss = 秒 <0 ～ 59>
- d = 曜日を表すビットマップ形式。各曜日は、次のように 1 ビットで表現されます。

  00000001 = 月曜日

  00000010 = 火曜日

  00000100 = 水曜日

  00001000 = 木曜日

  00010000 = 金曜日

  00100000 = 土曜日

  01000000 = 日曜日

ステップ 2 Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"

ISG トラフィック クラス アトリビュートをサービス プロファイルに追加します。このアトリビュートは、サービスの適用先となる入力トラフィックと出力トラフィックを指定します。入力と出力の両方のトラフィック分類子をサービス プロファイルに追加できます。

次の作業

サービス ポリシー マップまたはサービス 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 アカウンティングとポストペイド料金切り替えの確認

- **show subscriber session** コマンドを使用して、ISG アカウンティングとポストペイド料金切り替えのコンフィギュレーションを確認します。
- **show aaa sessions** コマンドを使用して、AAA 加入者セッションに関する情報を表示します。
- **show aaa user** コマンドを使用して、AAA 加入者に関する情報を表示します。

例

ここでは、確認のために使用するコマンドの出力例を示します。

ISG アカウンティングがフローに適用される場合の show subscriber session の出力

次の例では、トラフィック クラスを指定したサービス プロファイルで ISG アカウンティングが設定されるため、アカウンティングは親セッションではなく、フローで実行されます。この例で、157 はトラフィック クラスに固有の ID です。

```
Router# show subscriber session detailed uid 157
```

```
Subscriber session handle: E5000092, state: connected, service: Ltm Internal
Unique Session ID: 157
Identifier:
SIP subscriber access type(s): Traffic-Class
Root SIP Handle: 2B000011, PID: 76
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 3 minutes, 45 seconds, Last Changed: 3 minutes, 45 seconds
AAA unique ID: 0
Switch handle: F300015F

Session inbound features:
Feature: Service accounting
 Service: video1
 Method List: remote-local
 Outbound direction:
        Packets = 84, Bytes = 33600


Feature: Policing
 Upstream Params:
Average rate = 8000, Normal burst = 1500, Excess burst = 3000
Config level = Service

Session outbound features:
Feature: Service accounting
 Service: video1
 Method List: remote-local
 Outbound direction:
        Packets = 84, Bytes = 33600

Feature: Policing
 Dnstream Params:
Average rate = 64000, Normal burst = 12000, Excess burst = 24000
Config level = Service

Configuration sources associated with this session:
Service: video1, Active Time = 3 minutes, 46 seconds
```

ISG アカウンティングがセッションに適用される場合の show subscriber session の出力

次の例は、フローではなくセッションに対する **show subscriber session** コマンドのサンプル出力を示しています。

```
Router# show subscriber session detailed uid 730

Subscriber session handle: 3800009A, state: connected, service: Local Term
Unique Session ID: 730
Identifier: igq2acct
SIP subscriber access type(s): IP-Interface/Account-Logon-CH
Root SIP Handle: A600000E, PID: 75
Child SIP Handle: F9000018, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 3 minutes, 57 seconds, Last Changed: 2 minutes, 59 seconds
AAA unique ID: 81
Switch handle: 890003A0
Interface: ATM6/0.1

Policy information:
  Authentication status: authen
  Config downloaded for session policy:
  From Access-Type: Account-Logon-CH, Client: SM, Event: Got More Keys
    Profile name: apply-config-only, 2 references
      ssg-account-info     "SAfoo"
  Rules, actions and conditions executed:
```

```
    subscriber rule-map rule1
      condition always event any-event
        action 1 authenticate

Session inbound features:
Feature: Session accounting
 Method List: foo
 Outbound direction:
        Packets = 10, Bytes = 1000

Session outbound features:
Feature: Session accounting
 Method List: foo
 Outbound direction:
        Packets = 10, Bytes = 1000

Configuration sources associated with this session:
Interface: ATM6/0.1, Active Time = 3 minutes, 58 seconds
```

次に、**show aaa sessions** コマンドの出力例を示します。

```
Router# show aaa sessions

Total sessions since last reload: 141
Session Id: 167
   Unique Id: 151
   User Name: *not available*
   IP Address: 192.168.0.1
   Idle Time: 0
   CT Call Handle: 0
```

次に、**show aaa user** コマンドの出力例を示します。

特定のユーザに対する出力

```
Unique id 151 is currently in use.
Accounting:
  log=0x20C201
  Events recorded :
    CALL START
    NET UP
    IPCP_PASS
    INTERIM START
    VPDN NET UP
  update method(s) :
    PERIODIC
  update interval = 60
Outstanding Stop Records : 0
  Dynamic attribute list:

1A1CABE8 0 00000001 connect-progress(68) 4 Call Up
    1A1CABF8 0 00000001 pre-session-time(294) 4 0(0)
    1A1CAC08 0 00000001 nas-tx-speed(421) 4 423630024(194014C8)
    1A1CAC18 0 00000001 nas-rx-speed(71) 4 139317740(84DD1EC)
    1A1CAC28 0 00000001 elapsed_time(364) 4 46122(B42A)
    1A1CAC50 0 00000001 bytes_in(135) 4 11434660(AE7AA4)
    1A1CAC60 0 00000001 bytes_out(274) 4 0(0)
    1A1CAC70 0 00000001 pre-bytes-in(290) 4 0(0)
    1A1CAC80 0 00000001 pre-bytes-out(291) 4 0(0)
    1A1CAC90 0 00000001 paks_in(136) 4 92215(16837)
    1A1CADF0 0 00000001 paks_out(275) 4 0(0)
    1A1CAE00 0 00000001 pre-paks-in(292) 4 0(0)
    1A1CAE10 0 00000001 pre-paks-out(293) 4 0(0)
  No data for type EXEC
```

```
  No data for type CONN
  NET: Username=(n/a)
    Session Id=000000A7 Unique Id=00000097
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=189F046C : Name = CAR_mlist
    Attribute list:
      1A1CADF0 0 00000001 session-id(361) 4 167(A7)
1A1CAE00 0 00000001 protocol(297) 4 ip
      1A1CAE10 0 00000001 addr(8) 4 192.168.0.1
      1A1CAE20 0 00000001 Framed-Protocol(101) 4 PPP
      1A1CAE30 0 00000009 clid-mac-addr(37) 6 00 00 04 00 00 2A
--------
  No data for type CMD
  No data for type SYSTEM
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type 8
  No data for type CALL
  No data for type VPDN-TUNNEL
  No data for type VPDN-TUNNEL-LINK
  No data for type 12
  No data for type IPSEC-TUNNEL
  No data for type RESOURCE
  No data for type 15
Debg: No data available
Radi: No data available
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
Start Bytes In = 0             Start Bytes Out = 0
    Start Paks  In = 0             Start Paks  Out = 0
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 0             Pre Bytes Out = 0
    Pre Paks  In = 0             Pre Paks  Out = 0
  Cumulative Byte/Packet Counts :
    Bytes In = 11434660      Bytes Out = 0
    Paks  In = 92215         Paks  Out = 0
  StartTime = 12:02:40 IST Oct 16 2007
  AuthenTime = 12:02:40 IST Oct 16 2007
  Component = IEDGE_ACCOUNTING
Authen: service=NONE type=NONE method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000097
  Session Id = 000000A7
  Attribute List:
    1A1CADF0 0 00000001 port-type(198) 4 PPPoE over VLAN
    1A1CAE00 0 00000009 interface(194) 7 4/0/0/2
PerU: No data available
```

すべてのユーザに対する出力

```
Router# show aaa user all

--------------------------------------------------
Unique id 151 is currently in use.
Accounting:
  log=0x20C201
  Events recorded :
```

```
    CALL START
    NET UP
    IPCP_PASS
    INTERIM START
    VPDN NET UP
  update method(s) :
    PERIODIC
  update interval = 60
Outstanding Stop Records : 0
  Dynamic attribute list:
    1A1CABE8 0 00000001 connect-progress(68) 4 Call Up
    1A1CABF8 0 00000001 pre-session-time(294) 4 0(0)
    1A1CAC08 0 00000001 nas-tx-speed(421) 4 423630024(194014C8)
    1A1CAC18 0 00000001 nas-rx-speed(71) 4 139317740(84DD1EC)
    1A1CAC28 0 00000001 elapsed_time(364) 4 46122(B42A)
    1A1CAC50 0 00000001 bytes_in(135) 4 11434660(AE7AA4)
    1A1CAC60 0 00000001 bytes_out(274) 4 0(0)
    1A1CAC70 0 00000001 pre-bytes-in(290) 4 0(0)
    1A1CAC80 0 00000001 pre-bytes-out(291) 4 0(0)
    1A1CAC90 0 00000001 paks_in(136) 4 92215(16837)
    1A1CADF0 0 00000001 paks_out(275) 4 0(0)
    1A1CAE00 0 00000001 pre-paks-in(292) 4 0(0)
    1A1CAE10 0 00000001 pre-paks-out(293) 4 0(0)
  No data for type EXEC
  No data for type CONN
  NET: Username=(n/a)
    Session Id=000000A7 Unique Id=00000097
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=189F046C : Name = CAR_mlist
    Attribute list:
      1A1CADF0 0 00000001 session-id(361) 4 167(A7)
1A1CAE00 0 00000001 protocol(297) 4 ip
      1A1CAE10 0 00000001 addr(8) 4 192.168.0.1
      1A1CAE20 0 00000001 Framed-Protocol(101) 4 PPP
      1A1CAE30 0 00000009 clid-mac-addr(37) 6 00 00 04 00 00 2A
--------
  No data for type CMD
  No data for type SYSTEM
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type 8
  No data for type CALL
  No data for type VPDN-TUNNEL
  No data for type VPDN-TUNNEL-LINK
  No data for type 12
  No data for type IPSEC-TUNNEL
  No data for type RESOURCE
  No data for type 15
Debg: No data available
Radi: No data available
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
Start Bytes In = 0             Start Bytes Out = 0
    Start Paks  In = 0             Start Paks  Out = 0
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 0             Pre Bytes Out = 0
    Pre Paks  In = 0             Pre Paks  Out = 0
  Cumulative Byte/Packet Counts :
    Bytes In = 11434660      Bytes Out = 0
    Paks  In = 92215         Paks  Out = 0
```

```
  StartTime = 12:02:40 IST Oct 16 2007
  AuthenTime = 12:02:40 IST Oct 16 2007
  Component = IEDGE_ACCOUNTING
Authen: service=NONE type=NONE method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000097
  Session Id = 000000A7
  Attribute List:
    1A1CADF0 0 00000001 port-type(198) 4 PPPoE over VLAN
    1A1CAE00 0 00000009 interface(194) 7 4/0/0/2
PerU: No data available
```

ISG アカウンティングの設定例

フロー単位アカウンティング：例

ローカル サービス ポリシー マップに設定されたフロー単位アカウンティング

次に、「video1」というサービスに対して、サービス ポリシー マップで設定するフロー単位アカウンティングの例を示します。

```
class-map type traffic match-any video1
 match access-group output 101
 match access-group input 100

policy-map type service video1
 class type traffic video1
  accounting aaa list mlist1
```

AAA サーバのサービス プロファイルに設定されたフロー単位アカウンティング

次に、「video1」というサービスに対して、リモート サービス プロファイルで設定するフロー単位アカウンティングの例を示します。

```
video1        Password = "cisco"
   Cisco-AVpair = "traffic-class=input access-group 101 priority 20",
   Cisco-AVpair = "traffic-class=output access-group 112 priority 20",
   Cisco-Avpair = "accounting-list=remote-local",
   Service-Info = "QU;8000",
   Service-Info = "QD;64000"
```

ISG ポストペイド料金切り替え：例

次に、各曜日の深夜におけるポストペイド料金切り替えのコンフィギュレーションの例を示します。

```
Cisco-AVpair = "PPW00:00:00:127"
```

次に、月曜から金曜までの午後 8:00 時におけるポストペイド料金切り替えのコンフィギュレーションの例を示します。

```
Cisco-AVpair = "PPW20:00:00:31"
```

次に、月曜から金曜までの午前 6:00 時におけるポストペイド料金切り替えのコンフィギュレーションの例を示します。

```
Cisco-AVpair = "PPW06:00:00:31"
```

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*』
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 Command Reference*』の「Authentication, Authorization, and Accounting (AAA)」の項
ISG 加入者サービスの設定	『*Cisco IOS Intelligent Services Gateway Configuration Guide*』の「Configuring ISG Subscriber Services」の項

規格

規格	タイトル
なし	—

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。またこの機能による既存 MIB のサポートに変更はありません。	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
なし	—

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 アカウンティングの機能情報

表 24 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 24 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 24　ISG アカウンティングの機能情報

機能名	リリース	機能設定情報
ISG：アカウンティング：セッション単位、サービス単位、およびフロー単位	12.2(28)SB 12.2(33)SRC 12.2(33)XNE 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。 • 「ISG アカウンティングに関する情報」（P.248） • 「ISG アカウンティングの設定方法」（P.250） 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。 **（注）** トラフィック クラスに基づくフロー単位アカウンティングとサービス単位アカウンティングは、Cisco 7600 ルータではサポートされていません。
ISG：アカウンティング：ポストペイド	12.2(28)SB 12.2(33)SRC 12.2(33)XNE	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 は、ポストペイド課金用のアカウンティング サーバに、セッションとサービスに対するアカウンティングの開始レコードと終了レコードを送信します。アカウンティング サーバは、レコードを解釈して、課金情報を生成します。 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。 • 「ISG アカウンティングに関する情報」（P.248） • 「ISG アカウンティングの設定方法」（P.250） 12.2(28)SB では、この機能が導入されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。

表 24　ISG アカウンティングの機能情報 （続き）

機能名	リリース	機能設定情報
ISG：アカウンティング：料金切り替え	12.2(28)SB 12.2(33)SRC 12.2(33)XNE	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。課金料率が一定の時間に変更され、料率変更の境界を超えてセッションがアクティブだった場合、ISG は課金サーバにアカウンティング データを提供し、境界であることを示します。料金切り替えは、プリペイド課金からポストペイド課金への切り替えなど、アカウンティング方法間でも使用できます。 • 「ISG ポストペイド料金切り替え」（P.250） • 「ルータのサービス ポリシー マップでのフロー単位アカウンティングのイネーブル化」（P.255） 12.2(28)SB では、この機能が導入されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 **（注）** トラフィック クラスに基づくフロー単位アカウンティングは、Cisco 7600 ルータでは設定できません。

プリペイド課金のための ISG サポートの設定

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 プリペイド課金サポートによって、ISG は加入者の利用可能なクレジットを調べ、その加入者にサービスへのアクセスを許可するかどうか、およびアクセスの継続可能期間を判別できます。ISG プリペイド課金は、*クォータ*と呼ばれるクレジットの断片がプリペイド課金サーバによって割り当てられる、繰り返し再認可モデルに基づいて作用します。このモデルでは、それぞれが異なる課金レートを持った複数の同時プリペイド サービスに加入者が接続できます。ISG は時間ベースとボリューム ベースの課金をサポートします。

このモジュールは、プリペイド課金のための ISG サポートの設定方法に関する情報を提供します。

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、「プリペイド課金のための ISG サポートの機能情報」（P.288）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

ISG プリペイド課金サポートの前提条件

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、「プリペイド課金のための ISG サポートの機能情報」（P.288）を参照してください。

このマニュアルに示す作業は、加入者セッションが作成されていること、およびサービスのアクティブ化方法が用意されていることを前提としています。

ISG プリペイド課金サポートに関する制約事項

- ISG プリペイド課金サポートは、ISG トラフィック クラスによって定義されているトラフィック フローにのみ適用可能です。
- クォータは、時間の場合は秒単位で、ボリュームの場合はバイト単位で測定されます。測定単位を変更する方法はありません。
- ボリューム クォータは、アップストリームとダウンストリームのトラフィックの組み合わせに対するものです。

ISG プリペイド課金サポートに関する情報

ISG プリペイド課金のためのサポートを設定する前に、次の概念を理解しておく必要があります。

- 「プリペイド課金のための ISG サポートの概要」（P.270）
- 「加入者への許可分を超える ISG によるボリューム クォータ割り当てを防止するためのヒント」（P.271）
- 「ISG プリペイドしきい値」（P.271）
- 「ISG プリペイド アイドル タイムアウト」（P.271）
- 「ISG プリペイド料金切り替え」（P.272）
- 「ISG プリペイド課金の利点」（P.272）

プリペイド課金のための ISG サポートの概要

ISG プリペイド課金サポートによって、ISG は加入者の利用可能なクレジットを調べ、その加入者のサービスをアクティブ化するかどうか、およびそのセッションの継続可能期間を判別できます。加入者のクレジットは、プリペイド課金サーバによって、使用期間（秒数）または許容データ量（バイト数）のいずれかを表す一連のクォータとして管理されます。*クォータ*は、利用可能なクレジットの割り当て、つまり断片です。すべてのクレジットを一度に提供するのではなく、クォータを断片的に割り当てることによって、ISG は複数の同時プリペイド セッションに対してクレジットの使用をサポートできます。

ISG は RADIUS プロトコルを使用して、ISG と外部の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバ間およびプリペイド課金サーバ間の相互動作を容易にします。1 台のデバイスが AAA サーバおよび課金サーバとして動作可能です。

セッション用に最初のクォータを取得するため、ISG は認可要求を AAA サーバに送ります。AAA サーバはプリペイド課金サーバに接続し、そこからクォータ値が ISG に転送されます。次に、ISG はクォータの使用状況を追跡するためにセッションをモニタします。クォータが不足するか、指定された限度に達すると、ISG は再認可を実行します。再認可中に、プリペイド課金サーバは使用可能なクレ

ジットがあれば ISG に追加クォータを提供する場合があります。これ以上のクォータが提供されなければ、ISG はユーザをサービスからログオフさせるか、あるいは他の指定された何らかのアクションを実行します。

サービスが非アクティブ化されると、Accounting-Stop メッセージによって累積使用状況がプリペイド課金サーバに提供されます。

加入者への許可分を超える ISG によるボリューム クォータ割り当てを防止するためのヒント

Cisco IOS プリペイド ボリューム モニタ ポーリング タイマは、ISG がプリペイド再認可を開始するタイミングを決定します。ポーリング タイマ値は（15 秒 < ポーリング モニタ時間 < 300 秒）です。この値は、QV 値、実際のレート、および設定済みボリュームしきい値に基づいて動的に計算されます。プリペイド ボリューム モニタ ポーリング タイマは、直接設定可能ではありません。

最初の認可中（使用レートが未知のとき）の課金漏れを避けるため、QV 値は最低でも（15 X アクセスレート）にしてください。使用レートが既知の場合は、QV 値は少なくとも（15 X 使用レート）にしてください。

入力アクセスレートが QV 値よりもはるかに高い場合は、式（アクセスレート X 15 > QV < アクセスレート X 300）を使用して正しい QV 値を計算することを推奨します。例えば、ADSL2 または VDSL ユーザのアクセスレートは最大 20 Mbps が可能です。これは 1 秒間に約 2.5 MB のデータに相当します。QV 値の計算には、式（2.5 MB X 15 秒 > QV < 2.5 MB X 300 秒）を使用します。この計算結果の QV 値は 37.5 ～ 750 MB の間になります。境界値は避けるようにし、この例では値として QV = 100 MB などとしてください。

ISG プリペイドしきい値

デフォルトでは、加入者がクォータを使い切ったときに、ISG は再認可要求を課金サーバに送信します。ISG プリペイドしきい値は、クォータを使い切る前に、再認可要求の送信を ISG に許可します。プリペイドしきい値が設定されている場合、ISG は残りクォータの量がそのしきい値と等しくなったときに、再認可要求を課金サーバに送信します。プリペイドしきい値は、時間とボリュームの両方に関して設定可能です。

例えば、プリペイドしきい値の設定が 10 秒で、プリペイド課金サーバが ISG にクォータ 30 秒を送信した場合、ISG は、加入者がクォータのうち 20 秒を使い切って残りクォータが 10 秒になったときに、再認可要求をプリペイド課金サーバに送信します。

ISG プリペイド アイドル タイムアウト

ISG プリペイド アイドル タイムアウトを使用すると、指定された期間中トラフィックが受信されなかった場合に、プリペイド サービス セッションを中断できます。ISG は中断中もセッションを維持し続けますが、それまでにプリペイド セッション用として受信したすべてのクォータを解放します。セッションのその後のトラフィックによって ISG は再認可要求を送信し、セッション用の新しいクォータをダウンロードします。

ISG プリペイド料金切り替え

プリペイド料金切り替えによって、セッションのライフタイム中に料金の変更が可能になります。一般的に、サービス プロバイダーは、プリペイド料金切り替えを使用して、アクティブ接続中に異なる料金をエンド ユーザに提供します。例えば、オフピーク時間中はユーザを低料金に変更します。

（注） ISG は、料金切り替えポイントで発生する課金レート変更の計算には関与しません。課金レート変更の計算は、プリペイド課金サーバによって実行されます。

ISG は、切り替えポイント前の時間と後の時間に対応する 2 つのクォータを使用することによって、プリペイド料金切り替えをサポートします。ISG に対する認可応答において、プリペイド課金サーバは料金切り替えポイントと、料金切り替えの前後の期間に対するクォータを指定します。

ISG は料金切り替えが発生するまでプレ料金切り替えクォータを使用します。料金切り替えの前にプレ料金切り替えクォータを使い切った（またはしきい値に到達した）場合は、通常どおりに再認可が行われます。料金切り替えが行われると、ISG はプリペイド セッション モニタリングのためにポスト料金切り替えクォータを使い始めます。再認可は、これらのクォータのいずれかを使い切った場合にのみ行われ、料金が変更された場合には行われません。

プリペイド料金切り替えのアカウンティングのために行われるこのデュアルクォータ方式では、再認可要求が加入者の使用状況に従って調整されるため、料金切り替えのときに再認可要求が課金サーバに殺到しないようになっています。

ISG プリペイド課金の利点

同時プリペイド サービス アクセス

プリペイド課金のための ISG サポート機能は、同じクォータ プールをプリペイド課金サーバで維持しながら、同時プリペイド サービス アクセスをサポートできます。ISG サービスは、同時アクセスと順次アクセスのどちらにも設定可能です。同時アクセスでは、他のサービスに同時に接続しながら、ユーザは別のサービスへのログインを許可されます。

リアルタイム課金

プリペイド課金のための ISG サポート機能では、サービスや課金方式の種類に関係なく、最大の柔軟性を備えた状態でのリアルタイム課金が可能です。ユーザへの課金方式は定額式、使用時間ベース、ボリューム ベースが可能です。

クォータを使い切った場合のリダイレクト

ユーザのクォータが不足した場合、ISG は、サービスから切断されずにユーザがクォータを補給できるポータルへ、そのユーザをリダイレクトできます。

残存クォータの返還

ISG は、ユーザがログインしているがその使用がアクティブでないサービスから、残存クォータを課金サーバに返還できます。課金サーバに返還されたクォータは、ユーザがアクティブに使用中の他のサービスに適用できます。

しきい値

ISG を使用すると、しきい値を設定して、加入者がサービスの割り当てクォータを使い切る前に、プリペイド セッションの再認可が行われるようにできます。

再認可中のトラフィック ステータス

サービスの再認可中に接続済みトラフィックをドロップするよう ISG を設定すると、課金漏れを防止できます。ユーザはサービスに接続したままの状態となり、サービスに再びログインする必要はありませんが、再認可プロセス中はトラフィックが転送されません。このため、ISG が再認可要求を課金サーバに送信する間に、クォータが不足したサービスをユーザが使い続けることが防止されます。

ボリューム ベースと時間ベースの同時プリペイド課金

ISG はプリペイド サービスに対して、時間とボリュームの両方によるレーティングを同時にサポートします。プリペイド課金サーバは、時間とボリュームの両方でクォータを割り当てる場合があり、これらのパラメータ両方に基づいてセッションをモニタします。ISG は、これらのクォータ タイプのいずれかが使い切られると再認可を実行します。

プリペイド課金のための ISG サポートの設定方法

ここでは、次の作業について説明します。

- 「ISG プリペイド課金のための RADIUS アトリビュート サポートの設定」（P.273）（必須）
- 「ISG プリペイド課金設定の作成」（P.274）（任意）
- 「ISG プリペイド課金のイネーブル化」（P.276）（必須）
- 「クレジット切れ時の加入者トラフィックのリダイレクト」（P.278）（任意）
- 「クォータ不足時の加入者トラフィックの転送」（P.281）（任意）
- 「ISG プリペイド課金セッションのモニタ」（P.282）（任意）
- 「ISG プリペイド課金サポートのトラブルシューティング」（P.283）（任意）

ISG プリペイド課金のための RADIUS アトリビュート サポートの設定

ISG が RADIUS アトリビュート 44 を Access-Request パケットに、およびアトリビュート 55 を Accounting-Request パケットにそれぞれ含めるようにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*]
4. **radius-server attribute 55 include-in-acct-req**

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	**radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*] 例： `Router(config)# radius-server attribute 44 include-in-access-req`	ユーザ認証の前に RADIUS アトリビュート 44（アカウンティング セッション ID）を Access-Request パケットで送信します。
ステップ 4	**radius-server attribute 55 include-in-acct-req** 例： `Router(config)# radius-server attribute 55 include-in-acct-req`	RADIUS アトリビュート 55（イベントタイムスタンプ）を Accounting-Request パケットで送信します。

ISG プリペイド課金設定の作成

ISG プリペイド課金パラメータ設定を作成または変更するには、次の作業を実行します。この設定は、ISG プリペイド サポートがイネーブルにされているサービス プロファイルまたはサービス ポリシーマップで参照できます。

デフォルトのプリペイド設定

次のパラメータにデフォルトのプリペイド設定があることに注意してください。

```
subscriber feature prepaid default
 threshold time 0 seconds
 threshold volume 0 bytes
 method-list authorization default
 method-list accounting default
 password cisco
```

デフォルトのプリペイド設定は、いずれかのパラメータを変更しない限り、**show running-config** コマンドの出力に表示されません。

名前付きプリペイド設定のパラメータはデフォルト設定から継承されるため、名前付きプリペイド設定を作成して、1 つのパラメータのみをデフォルト設定とは異なるようにしたい場合、設定が必要なのはそのパラメータのみです。

前提条件

この作業は、AAA 方式リスト、サーバ グループ、およびサーバが設定済みであることを前提としています。詳細については、『*Cisco IOS Security Configuration Guide*』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **subscriber feature prepaid** {*name-of-config* | **default**}
4. **interim-interval** *number-of-minutes*
5. **method-list** {**accounting** | **authorization**} *name-of-method-list*
6. **password** *password*
7. **threshold** {**time** *seconds* | **volume** {*kilobytes* **Kbytes** | *megabytes* **Mbytes** | *bytes* **bytes**}}

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	**subscriber feature prepaid** {*name-of-config*	**default**} 例： `Router(config)# subscriber feature prepaid conf-prepaid`	新しい ISG プリペイド設定を作成するか、またはその変更を行うために既存の設定を指定します。
ステップ 4	**interim-interval** *number-of-minutes* 例： `Router(config-prepaid)# interim-interval 5`	中間プリペイド アカウンティングをイネーブルにして、ISG が中間プリペイド アカウンティング レコードを送信する間隔を指定します。
ステップ 5	**method-list** {**accounting**	**authorization**} *name-of-method-list* 例： `Router(config-prepaid)# method-list accounting list1`	ISG プリペイド アカウンティングまたは認可に使用する AAA 方式リストを指定します。
ステップ 6	**password** *password* 例： `Router(config-prepaid)# password test`	ISG プリペイド認可要求および再認可要求に使用するパスワードを設定します。
ステップ 7	**threshold** {**time** *seconds*	**volume** {*kilobytes* **Kbytes**	*megabytes* **Mbytes**	*bytes* **bytes**}} 例： `Router(config-prepaid)# threshold time 20`	ISG が再認可要求をプリペイド課金サーバに送信するしきい値を設定します。課金サーバによって提供されるクォータから設定済みしきい値を差し引くと、ISG が再認可要求を送信する値になります。 • このコマンドは、時間とボリュームの両方にしきい値を設定するために 2 回入力できます。

ISG プリペイド課金のイネーブル化

サービス ポリシー マップまたはリモート サービス プロファイルでプリペイド課金をイネーブルにするには、次の作業の 1 つを実行します。

- 「サービス ポリシー マップでの ISG プリペイド課金のイネーブル化」（P.276）
- 「AAA サーバ上のサービス プロファイルでの ISG プリペイド課金のイネーブル化」（P.277）

サービス ポリシー マップでの ISG プリペイド課金のイネーブル化

ISG プリペイド課金サポートをサービス ポリシー マップでイネーブルにするには、次の作業を実行します。

前提条件

ISG プリペイド課金は、サービス ポリシー マップ内のトラフィック クラスでイネーブルにされます。この作業は、トラフィック クラス マップと関連付けられた IP アクセス リストを定義してあることを前提としています。

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. **prepaid config** *name-of-configuration*

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 mp3`	ISG サービスの定義に使用する、サービス ポリシー マップを作成または定義します。
ステップ 4	[*priority*] **class type traffic** *class-map-name* 例： `Router(config-service-policymap)# class type traffic class-acl-101`	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	**prepaid config** *name-of-configuration* 例： `Router(config-control-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。 **（注）** このコマンドを実行したからといって、プリペイド課金がフローに確実に適用されるわけではありません。このコマンドによって、最初のプリペイド認可要求が発生します。プリペイド課金がフローに適用されるかどうかは、課金サーバによって決定されます。

次の作業

サービス ポリシー マップまたはサービス 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。

AAA サーバ上のサービス プロファイルでの ISG プリペイド課金のイネーブル化

プリペイド課金のための ISG サポートを、リモート AAA サーバ上に設定されているサービス プロファイルでイネーブルにするには、次の作業を実行します。

手順の概要

1. ISG トラフィック クラス アトリビュートをサービス プロファイルに追加します。
2. ISG プリペイド課金 VSA をサービス プロファイルに追加します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ISG トラフィック クラス アトリビュートをサービス プロファイルに追加します。 `Cisco-AVpair = "ip:traffic-class=in access-group [<acl_number> | name <acl_name>] [priority <n>]"` または `Cisco-AVpair = "ip:traffic-class=out access-group [<acl_number> | name <acl_name>] [priority <n>]"`	サービスの適用先となる入力トラフィックと出力トラフィックを指定します。 • 入力と出力の両方のトラフィック分類子をサービス プロファイルに追加できます。
ステップ 1	ISG プリペイド課金 VSA をサービス プロファイルに追加します。 `26,9,1 = "prepaid-config=`*`{<name-of-config>`*`| default"`	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。

次の作業

サービス ポリシー マップまたはサービス 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。

クレジット切れ時の加入者トラフィックのリダイレクト

サービス プロバイダーは、プリペイド サービスの加入者クレジットが不足したときに、加入者がアカウントを再チャージできるようにしておくことがあります。このセクションの作業を実行すると、加入者のクレジットが不足した場合に、加入者のレイヤ 4 トラフィックを、指定されたサーバにリダイレクトできます。

クレジット切れの場合の ISG レイヤ 4 リダイレクトを設定する前に、次の概念を理解しておく必要があります。

- 「クレジット切れイベント」（P.278）

クレジット切れの場合に加入者のレイヤ 4 トラフィックをリダイレクトするには、次の作業を実行します。

- 「サービス ポリシー マップでの L4 リダイレクトの設定」（P.279）
- 「クレジット切れ時におけるサービス ポリシー マップの加入者トラフィックへの適用」（P.280）

クレジット切れイベント

ISG クレジット切れイベントは、クォータ値が 0（時間またはボリューム）でアイドル タイムアウトが 0 よりも大きい Access-Accept パケットで、プリペイド サーバが応答した場合に発生します。この場合、プリペイド サーバは加入者のクレジットが不十分であると判断しましたが、アイドル タイムアウトによって、加入者がアカウントの再チャージを行える猶予期間が提供されます。一般的に、サービス プロバイダーは加入者のトラフィックを、加入者がアカウントの再チャージを行える Web ポータルにリダイレクトします。アイドル タイムアウト間隔の終わりに、ISG は再認可要求を送信します。

デフォルトの ISG 動作は、クレジット切れイベントが発生した場合に加入者パケットをドロップすることです。

（注） レイヤ 4 リダイレクションは、加入者のクレジットが不足した場合にサービス プロバイダーが行う可能性のある 1 つのアクションです。レイヤ 4 リダイレクションの代わりに、またはそれに加えて、他のアクションを設定できます。

サービス ポリシー マップでの L4 リダイレクトの設定

サービス ポリシー マップで ISG レイヤ 4 リダイレクトを設定するには、次の作業を実行します。ISG レイヤ 4 リダイレクト機能は、AAA サーバ上のサービス プロファイルでも設定できます。

前提条件

ISG レイヤ 4 リダイレクト機能は、サービス ポリシー マップ内のトラフィック クラスで設定されます。この作業は、トラフィック クラス マップを定義していることを前提としています。

トラフィックは、サーバまたはサーバ グループにリダイレクトできます。トラフィックをサーバ グループにリダイレクトする場合、この作業はサーバ グループが設定済みであることを前提としています。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic** *class-name*
5. **redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*]

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 redirect-service`	ISG サービスの定義に使用する、サービス ポリシー マップを作成または定義します。

	コマンドまたはアクション	目的
ステップ 4	[*priority*] **class type traffic** *class-name* 例： `Router(config-service-policymap)# class type traffic class-all`	(任意) 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	**redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*] 例： `Router(config-service-policymap-class-traffic)# redirect to group redirect-sg`	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。

クレジット切れ時におけるサービス ポリシー マップの加入者トラフィックへの適用

クレジット切れの場合にサービスを加入者トラフィックに適用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

名前付き制御クラス マップを指定する場合、この作業はクラス マップが設定済みであることを前提としています。

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 credit-exhausted**
5. *action-number* **service-policy type service name** *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 policyA`	制御ポリシーを定義するポリシー 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** {*control-class-name* | **always**} **event credit-exhausted** 例： `Router(config-control-policymap)# class type control always event credit-exhausted`	アクションが設定される制御クラスとイベントを指定します。
ステップ 5	*action-number* **service-policy type service name** *policy-map-name* 例： `Router(config-control-policymap-class-control)# 1 service-policy type service name redirect-profile`	指定されたサービス ポリシー マップを適用します。 • ISG レイヤ 4 リダイレクト機能が設定済みの、サービス ポリシー マップまたはサービス プロファイルを適用します。

次の作業

制御ポリシーは、**service-policy type control** コマンドを使用してコンテキストに適用する必要があります。

クォータ不足時の加入者トラフィックの転送

デフォルトでは、ISG は、加入者のクォータが不足した場合に加入者パケットをドロップします。この作業を実行すると、クォータ不足イベントが発生した場合にデフォルトを上書きして、加入者トラフィックを転送できます。

この作業を実行するには、その前に次の「Quota-Depleted イベント」で説明する概念を理解しておく必要があります。

Quota-Depleted イベント

Quota-Depleted イベントは、加入者がクォータを使い切ったときに、ISG がまだ課金サーバから再認可応答を受信していない場合に発生します。このイベントは、次の 2 つの状況で発生する可能性があります。

- プリペイドしきい値が未設定で、加入者がクォータを使い切った場合。
- プリペイドしきい値が設定されているが、しきい値に達したときに ISG が送信した再認可要求に対してプリペイド サーバが応答する前に、クォータを使い切った場合。

Quota-Depleted イベントは、加入者にもうクレジットがないことを必ずしも示すわけではありません。ISG は、再認可応答が課金サーバから戻されるまで加入者にクレジットがあるかどうかを正確には認識しません。したがって、一部のサービス プロバイダーは、再認可応答が戻されるまで、クォータ不足時に加入者パケットを転送することがあります。

デフォルトの ISG 動作は、Quota-Depleted イベントが発生した場合に加入者パケットをドロップすることです。

前提条件

名前付き制御クラス マップを指定する場合、この作業はクラス マップが設定済みであることを前提としています。

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 quota-depleted**
5. *action-number* **set-param drop-traffic false**

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 policyB`	制御ポリシーを指定するため、グローバルに、インターフェイスに対して、あるいは ATM VC に対して適用可能なポリシー 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 quota-depleted** 例： `Router(config-control-policymap)# class type control always event quota-depleted`	アクションが設定される制御クラスとイベントを指定します。
ステップ 5	*action-number* **set-param drop-traffic false** 例： `Router(config-control-policymap-class-control)# 1 set-param drop-traffic false`	クォータが不足したときにトラフィックの通過を許可し続けるように ISG を設定します。

次の作業

制御ポリシーは、**service-policy type control** コマンドを使用してコンテキストに適用する必要があります。

ISG プリペイド課金セッションのモニタ

ISG プリペイド セッションをモニタするには、次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。

ISG プリペイド課金サポートのトラブルシューティング

プリペイド課金サポートをトラブルシューティングするには、次の手順を実行します。

手順の概要

1. **show subscriber session**
2. サービス認証に成功したことを確認します。
3. AAA 方式リストが有効で設定済みであることを確認します。
4. **test aaa**
5. **debug subscriber policy prepaid**

手順の詳細

ステップ 1 **show subscriber session** コマンドを使用して、プリペイド課金サポートが設定されたサービスがアクティブ化されていることを確認します。

ステップ 2 サービス認証がサービスに必要な場合は、認証に成功したことを確認します。

ステップ 3 プリペイド課金設定で参照される AAA 方式リストが有効で、**aaa accounting network** コマンドで設定済みであることを確認します。

ステップ 4 **test aaa** コマンドを使用して、ISG から AAA サーバに到達可能なことを確認します。

ステップ 5 **debug subscriber policy prepaid** コマンドを使用して、プリペイド動作に関するデバッグ メッセージを表示します。

ISG プリペイド課金サポートの設定例

ここでは、次の例について説明します。

- 「ISG プリペイド課金サポート：例」（P.284）
- 「クレジット切れおよびクォータ不足のプリペイド課金イベントを処理するための ISG ポリシー：例」（P.285）

ISG プリペイド課金サポート：例

次の例は、次のパラメータで設定された ISG プリペイド課金サポートを示しています。

- 時間しきい値は 20 秒。
- ボリュームしきい値は 1000 バイト。
- クォータ不足イベントが発生した場合、ISG は課金サーバが別のクォータを送信するまで加入者パケットをドロップする。
- クレジット切れイベントが発生した場合、加入者パケットは「redirect-sg」というサーバ グループにリダイレクトされる。
- プリペイド サービスは「mp3」で、サービス ポリシー マップのルータ上で直接設定される。
- このサービスが加入者の認証に使用する AAA 方式リストは「cp-mlist」。サービス アカウンティングの送信先となる方式リストと同じです。
- プリペイド認可、再認可、およびアカウンティングのメッセージは、「ap-mlist」という AAA 方式リストに送信される。

```
!
aaa authorization network default local
aaa authorization network ap-mlist group sg2

aaa authentication network cp-mlist group sg1

aaa accounting network cp-mlist group sg1
aaa accounting network ap-mlist group sg2

service-policy type control RULEA
!
class-map type traffic CLASS-ALL
!
class-map type traffic CLASS-ACL-101
    match access-group input 101
!
policy-map type control RULEA
 class type control always event credit-exhausted
  1 service-policy type service name 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 1000 bytes
 method-list accounting ap-mlist
 method-list authorization default
 password cisco
```

クレジット切れおよびクォータ不足のプリペイド課金イベントを処理するための ISG ポリシー：例

次の例では、Quota-Depleted イベントの後で加入者パケットを転送し、クレジット切れイベントの後で加入者パケットをリダイレクトすることによってデフォルトの ISG プリペイド動作を上書きするため、「RULEA」という単一の制御ポリシーが定義されています。

```
!class-map type traffic CLASS-ALL
!
policy-map type control RULEA
 class type control always event quota-depleted
  1 set-param drop-traffic false
 class type control always event credit-exhausted
  1 service-policy type service name l4redirect
!
policy-map type service l4redirect
 class type traffic CLASS-ALL
  redirect to group SESM
!
subscriber feature prepaid conf-prepaid
 threshold time 100
 threshold volume 1000 bytes
 method-list author prepaidlist
 method-list accounting default
 password cisco
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/cr/isg_r/index.htmber
feature prepaid default
 threshold time 0
 threshold volume 0
 method-list author default
 method-list accounting default
 password cisco
```

その他の参考資料

ここでは、プリペイド課金のための ISG サポート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
AAA 設定作業	『*Cisco IOS Security Configuration Guide*』の「Authentication, Authorization, and Accounting (AAA)」の項
AAA コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS Security Command Reference*』
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
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

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。またこの機能による既存 MIB のサポートに変更はありません。	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
なし	—

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

プリペイド課金のための ISG サポートの機能情報

表 25 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。

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。特定のコマンドのサポートの導入時期に関する詳細については、コマンド リファレンス マニュアルを参照してください。

Cisco IOS ソフトウェア イメージは、Cisco IOS ソフトウェア リリース、機能セット、プラットフォームそれぞれに固有です。プラットフォーム サポートと Cisco IOS 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。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスするには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明の場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

（注） 表 25 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 25　プリペイド課金のための ISG サポートの機能情報

機能名	リリース	機能設定情報
ISG：アカウンティング：料金切り替え	12.2(28)SB	プリペイド料金切り替えによって、セッションのライフタイム中に料金の変更が可能になります。ISG は、料金切り替えポイント前の時間と後の時間に対応する 2 つのクォータを使用することによって、プリペイド料金切り替えをサポートします。料金切り替えは、プリペイド課金からポスト ペイド課金への切り替えなど、アカウンティング方式間で使用することもできます。 • 「ISG プリペイド料金切り替え」（P.272） • 「プリペイド課金のための ISG サポートの設定方法」（P.273）

表 25　プリペイド課金のための ISG サポートの機能情報 （続き）

機能名	リリース	機能設定情報
ISG：アカウンティング：時間ベースのプリペイド	12.2(28)SB	ISG プリペイド課金サポートによって、ISG は加入者の利用可能なクレジットを調べ、その加入者にサービスへのアクセスを許可するかどうか、およびアクセスの継続可能期間を判別できます。ISG は時間ベースのプリペイド課金をサポートします。 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。 • 「ISG プリペイド課金サポートに関する情報」（P.270） • 「プリペイド課金のための ISG サポートの設定方法」（P.273）
ISG：アカウンティング：ボリューム ベースのプリペイド	12.2(28)SB	ISG プリペイド課金サポートによって、ISG は加入者の利用可能なクレジットを調べ、その加入者にサービスへのアクセスを許可するかどうか、およびアクセスの継続可能期間を判別できます。ISG はボリューム ベースのプリペイド課金をサポートします。 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。 • 「ISG プリペイド課金サポートに関する情報」（P.270） • 「プリペイド課金のための ISG サポートの設定方法」（P.273）

セッション メンテナンスのための 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。このモジュールでは、サービス ポリシー マップを介してセッション タイマーおよび接続タイマーを設定する方法について説明します。また、Internet Engineering Task Force（IETF）RADIUS アトリビュートの Session-Timeout（アトリビュート 27）および Idle-Timeout（アトリビュート 28）を Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバのサービス プロファイルで使用して、同じセッション メンテナンス コントロールを設定できます。

アイドル状態のアップストリーム方向でセッション データ トラフィックをモニタするために、IP 加入者セッションのキープアライブ サポートが設定されています。レイヤ 2 接続の加入者に対して、Address Resolution Protocol（ARP; アドレス解決プロトコル）が使用されます。ルーテッド ホスト（レイヤ 3 接続の）加入者では、プロトコルのデフォルトは Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）になります。ICMP は、アクセス インターフェイスが ARP をサポートしていない設定においても使用されます。

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、「セッション メンテナンスのための ISG ポリシーの設定に関する機能情報」（P.307）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

セッション メンテナンスのポリシーを設定するための前提条件

トラフィック クラスが必要になるのは、トラフィック クラスの定義を備えているサーバにアイドル タイマーまたはセッション タイマーインストールされている場合のみです。トラフィック クラスを持たないセッションまたはサービスにタイマーがインストールされている場合は、トラフィック クラスは必要ありません。トラフィック クラスの設定方法については、「Configuring ISG Subscriber Services」モジュールを参照してください。

セッション メンテナンスのポリシーを設定するための制約事項

IP セッション（PPP セッションではない）に適用されるアイドル タイムアウトでは現在、方向を指定する方法がありません。デフォルトでは、アイドル タイマーが適用される方向は常にアウトバウンドになります。

ISG は、セッション単位、およびフロー単位のアカウンティングの両方をサポートしています。セッション単位のアカウンティングは、1 つのセッションについてのすべてのフロー トラフィックの合計です。セッション単位のアカウンティングは、ユーザ プロファイル、サービス プロファイル、またはサービス ポリシー マップでイネーブルにできます。

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 ISG アカウンティングをサポートしています。

- Cisco 7600 ルータはトラフィック クラス機能をサポートしていないため、トラフィック クラスに基づいたセッション コントロールはサポートしていません。

セッション メンテナンスのポリシー設定に関する情報

セッション メンテナンス タイマー

ISG には、セッションおよびその接続に関して制御を維持するための 2 つのコマンドがあります（それぞれのコマンドは単独で設定できます）。**timeout absolute** コマンドは、セッションを終了するまでに、そのセッションを接続しておく時間を制御します。**timeout idle** コマンドは、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制御します。これらの 2 つのコマンドは PPP セッションと IP セッションの両方を検出し、サービス内、セッション単位、またはフロー内で適用できます。すべての加入者トラフィックはタイマーをリセットします。ただし、PPP コントロール パケットなどの非ネットワーク トラフィックはタイマーをリセットしません。

セッション タイマーおよび接続タイマーの範囲は、タイマーが指定されているサービスのタイプによって決まります。トラフィック クラスが定義されていないサービス プロファイルにタイマーが指定されている場合、このタイマー アクションは、セッションまたは接続を終了します。サービス プロファイル内にトラフィック クラス指定子がある場合、タイマー アクションはサービスを無効にします。

セッション メンテナンス タイマーの利点

PPP アイドル タイムアウトの機能は、ISG アイドル タイムアウト機能と置き換えられました。アイドル タイマーは汎用的な機能で、この機能を設定して、PPP セッションと IP セッションの両方でアイドル トラフィックを検出できます。

対象のサービスからトラフィックが生じないために、セッションからサービスを削除する場合、インストールされている期間がどのくらい経過してから削除するかを制御するには、セッションにインストールされているサービス プロファイル内にアイドル タイマーを設定します。サービスに、関連付けられているトラフィック クラス パラメータがある場合は、このタイマーの設定時間が経過したとき、またはセッション自身が終了したときにトラフィック クラスが終了します。

同じことはセッション タイマーにも当てはまります。ただし、セッション タイマーは、セッションから生じるトラフィックに関係なく、セッションまたはサービスを有効にしておく期間を決定します。

セッションのモニタリング

アップストリーム方向における IP 加入者セッションのデータ トラフィックでは、加入者に設定されているキープアライブ機能を使用して、アイドル状態をモニタできます。設定されている期間についてセッションがアイドルになると、キープアライブ要求が加入者へ送信されます。このアクションでは、接続がまだアクティブであることが確認されます。キープアライブ要求および応答に対して使用するプロトコルは、IP 加入者のセッション タイプに基づいて設定できます。直接接続されているホスト（レイヤ #2 接続）の場合は、ARP が使用されます。ルーテッド ホスト（レイヤ 3 接続の）加入者の場合は、ICMP が使用されます。アクセス インターフェイスで ARP をサポートしていない場合は、キープアライブ プロトコルのデフォルトは ICMP になります。

キープアライブ メッセージの ARP

セッションが確立されており、ARP を使用するためにキープアライブ機能が設定されている場合、キープアライブ機能は、後で ARP の応答を確認するための正しいオリジナル エントリとして ARP エントリを保存します。

（注） アクセス インターフェイスでサポート ARP をサポートしていない場合、キープアライブに対するプロトコルのデフォルトは ICMP になります。

ARP が設定されている場合、ARP のユニキャスト要求が加入者へ送信されます。時間の間隔を設定すると、ARP の応答（受信した場合）が検証されます。応答が正しく、加入者が最初に確立されたときに保存したオリジナルのエントリと一致した場合、キープアライブ機能は、設定された時間の間隔だけ、データ プレーンのモニタリングを継続します。応答が正しくない場合、キープアライブ機能は、正しい応答を受け取るまで、または設定されている最大試行回数を超えるまで ARP 要求を再送します。

キープアライブ メッセージの ICMP

ICMP が設定されている場合、設定されている最大試行回数を超えるまで、加入者に「hello」要求が送信され、応答がチェックされます。

IP サブネットのセッションでは、ICMP の「hello」要求に使用されるピア（宛先）IP アドレスは、サブネット内のすべての IP アドレスになります。これは、対象のサブネット内で可能性のあるすべてのホストに対して「hello」要求が（同時ではなく）順に送信されることを意味しています。サブネット内のいずれのホストからも応答がない場合、そのセッションは切断されます。

もうひとつのオプションは、キープアライブ要求に対して ICMP ダイレクト ブロードキャストを設定することです。加入者ホストが IP サブネット ブロードキャスト アドレスを認識すると、ISG は ICMP の「hello」要求をサブネット ブロードキャスト アドレスへ送信できます。この設定が作動するためには、加入者が ISG と同じサブネット上に存在している必要はありません。次の条件が満たされていれば、ダイレクト ブロードキャストのキープアライブ要求は複数ホップ離れていても動作できます。

- サブネットで識別される加入者のグループは、ISG のサブネット加入者セッションでプロビジョニングされたものと同じサブネットを、ローカルにプロビジョニングされている必要があります。それ以外の場合、加入者ホストはサブネット ブロードキャスト アドレスを認識しません。
- ホストに直接接続されているルータは、ダイレクト ブロードキャスト フォワーディングが可能で、IP サブネット ブロードキャストがレイヤ 2 のブロードキャストに変換される必要があります。

これらの 2 つの条件を満たしている場合、ユーザは ICMP キープアライブの設定を最適化し、ICMP パケットの数を最少にできます。

（注） ダイレクト ブロードキャストをイネーブルにすると DoS 攻撃のリスクが高くなるため、サブネット ダイレクト ブロードキャストはデフォルトでオンになっていません。

セッション メンテナンス タイマーのポリシーの設定方法

セッション メンテナンス タイマーを設定するには、アイドル タイマーの設定と、セッション タイマーの設定という、2 つの個別の作業が必要です。これらの 2 つの作業のいずれか、または両方を実行して、セッション メンテナンス コントロールを設定できます。次の作業は、サービス ポリシー マップおよび RADIUS AAA サーバ プロファイルでこれらのタイマーを設定する方法を示しています。

- 「サービス ポリシー マップでのセッション タイマーの設定」（P.295）（必須）
- 「AAA サーバでのセッション タイマーの設定」（P.296）（必須）
- 「サービス ポリシー マップでの接続タイマーの設定」（P.296）（必須）
- 「AAA サーバでの接続タイマーの設定」（P.297）（必須）
- 「セッション タイマーおよび接続タイマー設定の確認」（P.298）（任意）
- 「セッション タイマーおよび接続タイマー設定のトラブルシューティング」（P.298）（任意）

サービス ポリシー マップでのセッション タイマーの設定

サービス ポリシー マップでセッション タイマーを設定するには、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. **timeout absolute** *duration-in-seconds*
6. **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 service** *policy-map-name* 例： `Router(config)# policy-map type service policy1`	ポリシー マップ コンフィギュレーション モードを開始して、サービス ポリシーの設定を開始できるようにします。
ステップ 4	[*priority*] **class type traffic** *class-map-name* 例： `Router(config-control-policymap)# class type traffic class1`	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	**timeout absolute** *duration-in-seconds* 例： `Router(config-control-policymap-class-control)# 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 6	**end** 例： `Router(conf-subscriber-profile)# end`	特権 EXEC モードに戻ります。

次の作業

サービス ポリシー マップまたはサービス 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。

AAA サーバでのセッション タイマーの設定

AAA サーバ プロファイルでセッション タイマーを設定するには、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 RADIUS Session-Timeout 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	**Session-Timeout=***duration-in-seconds*	ユーザ プロファイルまたはサービス プロファイルに、30 ～ 4294967 秒の範囲で IETF RADIUS セッション タイマー（アトリビュート 27）を設定します。

サービス ポリシー マップでの接続タイマーの設定

サービス ポリシー マップで接続タイマーを設定するには、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. **timeout idle** *duration-in-seconds*
6. **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。

	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 policy1`	ポリシー マップ コンフィギュレーション モードを開始して、サービス ポリシーの設定を開始できるようにします。
ステップ 4	[*priority*] **class type traffic** *class-map-name* 例： `Router(config-service-policymap)# class type traffic class1`	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	**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 6	**end** 例： `Router(config-control-policymap-class-traffic)# end`	特権 EXEC モードに戻ります。

次の作業

サービス ポリシー マップまたはサービス 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。

AAA サーバでの接続タイマーの設定

AAA サーバ プロファイルで接続タイマーを設定するには、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 RADIUS Idle-Timeout 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	**Idle-Timeout=***duration-in-seconds*	ユーザ プロファイルまたはサービス プロファイルに、1 ～ 4294967 秒の範囲で IETF RADIUS（アトリビュート 28）を設定します。

セッション タイマーおよび接続タイマー設定の確認

タイマーが正しくインストールされたことを確認するには、この作業を実行します。

手順の概要

1. **enable**
2. **show subscriber session all**
3. **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	**show subscriber session all** 例： `Router# show subscriber session all`	現在の加入者の情報、およびイネーブルになっているタイマーのレポートが表示されます。
ステップ 3	**end** 例： `Router# end`	特権 EXEC モードに戻ります。

セッション タイマーおよび接続タイマー設定のトラブルシューティング

ここでは、セッション メンテナンス タイマーのトラブルシューティングに使用可能な **debug** コマンドを示し、タイマーをイネーブルにするための作業について説明します。

- 「前提条件」（P.298）
- 「制約事項」（P.299）
- 「セッション メンテナンス タイマーで使用可能なデバッグ コマンド」（P.299）
- 「セッション メンテナンス タイマーのデバッグ コマンドのイネーブル化」（P.299）

前提条件

この作業を実行する前に、『*Cisco IOS Debug Command Reference*』の概要の章に説明のある Cisco IOS **debug** コマンドの使用法をよく理解しておいてください。「Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging」モジュールも参照してください。

制約事項

注意 デバッグ出力には、CPU プロセスで高いプライオリティが割り当てられるので、システムが使用不能になる可能性があります。したがって、Cisco IOS **debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合だけにしてください。また、**debug** コマンドを使用するのは、ネットワーク トラフィックとユーザが少ない時間帯、あるいはアクティブ セッションが 1 つのデバッグ シャーシが最適です。そのような時間帯を選んでデバッグを実行すると、**debug** コマンドの処理のオーバーヘッドによってシステム利用が影響を受ける可能性が少なくなります。

セッション メンテナンス タイマーで使用可能なデバッグ コマンド

表 26 に、セッション メンテナンス タイマーの問題を診断するための **debug** コマンドを示します。

表 26　セッション メンテナンス タイマーのトラブルシューティング用デバッグ コマンド

コマンド	目的
debug subscriber feature error	一般的な Feature Manager エラーを表示します。
debug subscriber feature event	一般的な Feature Manager イベントを表示します。
debug subscriber feature name idle-timer error	アイドル タイマーのエラーを表示します。
debug subscriber feature name idle-timer event	アイドル タイマーのイベントを表示します。
debug subscriber feature name session-timer error	セッション タイマーのエラーを表示します。
debug subscriber feature name session-timer event	セッション タイマーのイベントを表示します。

セッション メンテナンス タイマーのデバッグ コマンドのイネーブル化

セッション メンテナンス タイマーの **debug** コマンドをイネーブルにするには、この作業を実行します。

手順の概要

1. **enable**
2. **debug** *command*
3. **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 モードなど、高位の権限レベル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	**debug** *command* 例： `Router# debug subscriber feature name session-timer error`	表 26 に示した 1 つ以上の **debug** コマンドを入力します。 • 終了後は、対応する **no debug** コマンドを入力します。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Router# end`	（任意）特権 EXEC モードに戻ります。

ルータ上でのセッション キープアライブの設定

この作業では、ARP または ICMP のいずれかを使用してルータ上でキープアライブ機能を設定する方法について説明します。

このセッション キープアライブ機能は加入者の健全性および存在についてチェックするため、この機能はフロー単位ではなくそのセッション全体だけに適用されます。

制約事項

- サービス プロファイルに ISG トラフィック クラスの設定が含まれている場合、キープアライブ機能は無効になります。
- PPP over Ethernet（PPPoE）や PPP over ATM（PPPoA）などの非 IP セッションにこの機能が適用されると、この機能のアプリケーションは失敗し、次のようになります。
  - 機能が session-start イベントで適用されると、機能のアプリケーションおよびセッションの両方が失敗します。
  - session-start イベント後にこの機能をセッションにプッシュした場合は、そのプッシュが失敗します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **keepalive** [**idle** *idle-seconds*] [**attempts** *max-retries*] [**interval** *retry-seconds*] [**protocol** {**ARP** | **ICMP** [**broadcast**]}]
5. **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。

	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 policymap1`	サービス 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	**keepalive** [**idle** *idle-seconds*] [**attempts** *max-retries*] [**interval** *retry-seconds*] [**protocol** {**ARP** | **ICMP** [**broadcast**]}] 例： `Router(config-service-policymap)# keepalive idle 7 attempts 3 interval 1 protocol arp`	キープアライブ メッセージをイネーブルにして、最大のアイドル時間、要求数、要求間の間隔、およびキープアライブ メッセージのプロトコルを設定します。 • **idle**、**attempts**、および **interval** キーワードの範囲およびデフォルト値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。 • **protocol**：レイヤ 2 の接続ではデフォルトは ARP、経路選択済み接続ではデフォルトは ICMP です。 • **broadcast**：このオプションはデフォルトではディセーブルになっています。 **（注）** このコマンドが非 IP セッションに適用されると、コマンドは失敗します。コマンドが session-start イベントで非 IP セッションに適用されると、セッションも失敗します。
ステップ 5	**end** 例： `Router# end`	特権 EXEC モードに戻ります。

例

次に、ARP を使用してルータ上でキープアライブ機能を設定する例を示します。

```
policy-map type service accting_service
 class type traffic ALL
 !
  keepalive interval 3 protocol ARP
!
```

RADIUS サーバでのセッション キープアライブの設定

この作業では、RADIUS サーバ上でセッション キープアライブ パラメータを設定する方法について説明します。

手順の概要

1. Service-Name password = "cisco"
2. Cisco-Avpair = "subscriber:keepalive = [idle *period1*] [attempts *Max-retries*] [interval *period2*] [protocol *ICMP* [broadcast] | *ARP*}"

手順の詳細

ステップ 1 Service-Name password = "cisco"

ステップ 2 Cisco-Avpair = "subscriber:keepalive = [idle *period1*] [attempts *Max-retries*] [interval *period2*] [protocol *ICMP* [broadcast] | *ARP*}"

可能なアイドル期間、接続の最大試行回数、試行間の間隔、および使用する通信プロトコルを設定します。

値の範囲とデフォルトは次のとおりです。

- アイドル期間：範囲は 5 ～ 10 秒で、デフォルトは 10 秒です。
- 試行回数：範囲は 3 ～ 10 で、デフォルトは 5 です。
- 間隔：デフォルトは 1 ～ 10 秒です。
- プロトコル：レイヤ 2 接続ではデフォルトは ARP、経路指定されている接続ではデフォルトは ICMP です。
- ブロードキャスト オプション：デフォルトでは、このオプションはディセーブルになっています。

（注） サービス プロファイルに ISG トラフィック クラスの設定が含まれている場合、キープアライブ機能は無効になります。

セッション メンテナンス タイマーの設定例

例：サービス ポリシー マップでのセッション タイマーの設定

次に、サービス ポリシー マップのセッション時間を 4800 秒（80 分）に制限する例を示します。

```
class-map type traffic match-any traffic-class
 match access-group input 101
 match access-group output 102
policy-map type service video-service
 class traffic-class
  police input 20000 30000 60000
  police output 21000 31500 63000
  timeout absolute 4800
 class type traffic default
 drop
```

例：サービス ポリシー マップでの接続アイドル タイマーの設定

次に、サービス ポリシー マップでのアイドル接続時間を 30 秒に制限する例を示します。

```
class-map type traffic match-any traffic-class
 match access-group input 101
 match access-group output 102
policy-map type service video-service
 class type traffic traffic-class
  police input 20000 30000 60000
  police output 21000 31500 63000
  timeout idle 30
 class type traffic default
 drop
```

例：セッション タイマーの show コマンドの出力

次の例は、**show subscriber session all** 特権 EXEC コマンドで表示されたセッション タイマーの設定を示しています。

```
Current Subscriber Information: Total sessions 1
------------------------------------------------
Unique Session ID: 3
Identifier: user01
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:02:50, Last Changed: 00:02:53
AAA unique ID: 4
Interface: Virtual-Access2.1

Policy information:
  Context 02DE7380: Handle 1B000009
  Authentication status: authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    username             "user01"
    Framed-Protocol      1 [PPP]
    username             "user01"
  Prepaid context: not present


Non-datapath features:
 Feature: Session Timeout
  Timeout value is 180000 seconds
```

```
  Time remaining is 2d01h
Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:02:52
```

例：接続アイドル タイマーの show コマンドの出力

次の例は、**show subscriber session all** 特権 EXEC コマンドで表示されたアイドル タイマーの設定を示しています。

```
Current Subscriber Information: Total sessions 1
------------------------------------------------
Unique Session ID: 4
Identifier: user01
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:01:44, Last Changed: 00:01:46
AAA unique ID: 5
Interface: Virtual-Access2.1

Policy information:
  Context 02DE7380: Handle AD00000C
  Authentication status: authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    username             "user01"
    Framed-Protocol      1 [PPP]
    username             "user01"
  Prepaid context: not present


Session outbound features:
 Feature: PPP Idle Timeout
  Timeout value is 2000
  Idle time is 00:01:44
Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:01:47
```

例：セッション タイマーのデバッグ出力

次の例は、セッション タイマーのデバッグ コマンド（**debug subscriber feature error**、**debug subscriber feature event**、**debug subscriber feature name session-timer error**、および **debug subscriber feature name session-timer event**）がイネーブルになっている場合の出力を示しています。

```
*Jan 12 18:38:51.947: SSF[Vi2.1/Abs Timeout]: Vaccess interface config
update; not per-user, ignore
*Jan 12 18:38:53.195: SSF[Vt1/uid:3]: Install interface configured
features
*Jan 12 18:38:53.195: SSF[Vt1/uid:3]: Associate segment element handle
0x95000002 for session 1191182344, 1 entries
*Jan 12 18:38:53.195: SSF[Vt1/uid:3/Abs Timeout]: Group feature install
*Jan 12 18:38:53.195: SSF[uid:3/Abs Timeout]: Adding feature to none segment(s)
```

例：接続アイドル タイマーのデバッグ出力

次の例は、アイドル タイマーのデバッグ コマンド（**debug subscriber feature error**、**debug subscriber feature event**、**debug subscriber feature name idle-timer error**、および **debug subscriber feature name idle-timer event**）がイネーブルになっている場合の出力を示しています。

```
*Jan 12 18:43:15.167: SSF[Vt1/uid:4]: Install interface configured
features
*Jan 12 18:43:15.167: SSF[Vt1/uid:4]: Associate segment element handle
0xF4000003 for session 67108875, 1 entries
*Jan 12 18:43:15.167: SSF[Vt1/uid:4/Idle Timeout]: Group feature install
*Jan 12 18:43:15.167: SSF[uid:4/Idle Timeout]: Adding feature to outbound
segment(s)
*Jan 12 18:43:15.167: Idle Timeout[uid:4]: Idle timer start, duration 2000
seconds, direction: outbound
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] created
02DFFDD8
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] added
02DFFDD8 [outbound]
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097]
installed: ok
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097]
installed: ok
*Jan 12 18:43:19.147: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] bound
```

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*』
ppp timeout idle および **timeout absolute** PPP タイマー コマンド	『*Cisco IOS Dial Technologies 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

セッション メンテナンスのための ISG ポリシーの設定に関する機能情報

表 27 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 27 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 27　ISG セッション メンテナンスの機能情報

機能名	リリース	機能設定情報
ISG：セッション：ライフサイクル：アイドル タイムアウト	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG アイドル タイムアウトは、接続をを終了するまでに、その接続をアイドルにしておく時間を制御します。 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。 • 「セッション メンテナンス タイマー」（P.293） • 「セッション メンテナンス タイマーのポリシーの設定方法」（P.294） 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。

表 27　ISG セッション メンテナンスの機能情報 （続き）

機能名	リリース	機能設定情報
ISG：セッション保護および復元力：キープアライブ：ARP、ICMP	12.2(33)SB 12.2(33)SRC 15.0(1)S	アイドル状態のアップストリーム方向でセッション データ トラフィックをモニタするために、IP 加入者セッションのキープアライブ サポートが設定されています。レイヤ 2 接続の加入者に対して、Address Resolution Protocol（ARP; アドレス解決プロトコル）が使用されます。ルーテッド ホスト（レイヤ 3 接続の）加入者では、プロトコルのデフォルトは Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）になります。ICMP は、アクセス インターフェイスが ARP をサポートしていない設定においても使用されます。 Cisco IOS Release 12.2(33)SRC では、この機能は Cisco 7200 および Cisco 7600 ルータに実装されていました。 Cisco IOS Release 12.2(33)SB では、この機能は Cisco 10000 ルータに実装されていました。 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。 • 「ルータ上でのセッション キープアライブの設定」（P.300） • 「RADIUS サーバでのセッション キープアライブの設定」（P.302） 次のコマンドが導入されました：**keepalive**（ISG）

ISG レイヤ 4 リダイレクトを使用した加入者トラフィックのリダイレクト

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 レイヤ 4 リダイレクト機能を使用して、加入者トラフィックをリダイレクトするように ISG を設定する方法を説明します。サービス プロバイダーが ISG レイヤ 4 リダイレクト機能を使用すると、加入者 TCP または User Datagram Protocol（UDP; ユーザ データグラム プロトコル）パケットを適切な処理のために指定されたサーバにリダイレクトできるようにすることによって、ユーザ環境が向上します。ISG レイヤ 4 リダイレクトは、加入者の認証、初期と定期的なアドバタイジングによる魅了、アプリケーション トラフィックのリダイレクトおよび Domain Name System（DNS; ドメイン ネーム システム）リダイレクトを行うために使用できます。

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 加入者トラフィック リダイレクトの機能情報」（P.322）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

- 「その他の参考資料」（P.320）
- 「ISG 加入者トラフィック リダイレクトの機能情報」（P.322）

ISG 加入者トラフィック リダイレクトの前提条件

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 加入者トラフィック リダイレクトの機能情報」（P.322）を参照してください。

ISG 加入者トラフィック リダイレクトの制約事項

ISG レイヤ 4 リダイレクト機能は、TCP トラフィックまたは UDP トラフィックのみに適用されます。

Cisco IOS Release 12.2(33)SRC 以降では、Cisco 7600 ルータではトラフィック クラス機能がサポートされないため、レイヤ 4 リダイレクト機能は Access Control List（ACL; アクセス コントロール リスト）を使用して使用して設定する必要があるという制限付きで、この機能を Cisco 7600 ルータで使用できます。

ISG 加入者トラフィック リダイレクトに関する情報

レイヤ 4 リダイレクト機能を設定するには、次の概念を理解しておく必要があります。

- 「ISG レイヤ 4 リダイレクトの概要」（P.310）
- 「レイヤ 4 リダイレクト アプリケーション」（P.311）

ISG レイヤ 4 リダイレクトの概要

ISG レイヤ 4 リダイレクト機能では、指定されたパケットを、指定された方法でパケットを処理するサーバにリダイレクトします。たとえば、無許可のユーザによってアップストリームで送信されたパケットを、ユーザをログイン ページにリダイレクトするサーバに転送できます。同様に、ユーザがログインしていないサービスにアクセスを試行した場合、サービスのログイン画面を表示するサーバにパケットをリダイレクトできます。

レイヤ 4 リダイレクト機能では、加入者セッションまたはフローに適用できる 3 種類のリダイレクトがサポートされます。

- 初期リダイレクト：指定されたトラフィックが、機能が適用されてから一定の期間のみリダイレクトされます。
- 定期的リダイレクト：指定されたトラフィックが定期的にリダイレクトされます。トラフィックが、指定された期間だけリダイレクトされます。その後、リダイレクトは別の指定された期間だけ停止されます。このサイクルが繰り返されます。定期的なリダイレクト中は、リダイレクトの期間が終了するまで、すべての新しい TCP 接続がリダイレクトされます。リダイレクト期間の終了後は、新しい TCP 接続がリダイレクトされなくなります。ただし、このリダイレクト期間中に開始された既存のすべての TCP 接続は、リダイレクトが継続され、切断されません。

- 永続的リダイレクト：指定されたトラフィックが指定されたサーバに常にリダイレクトされます。

リダイレクト サーバは、リダイレクトされたパケットに応答するようにプログラミングされた、任意のサーバにすることができます。ISG が Web ポータルで使用される場合は、認証されていない加入者がブラウザ セッションを開始したときに、自動的にログイン ページに送信されるようにできます。Web ポータル アプリケーションは、サービスのログイン ページ、アドバタイジング ページ、メッセージ ページにリダイレクトすることもできます。

リダイレクトされたパケットは、個々のリダイレクト サーバまたは 1 台以上のサーバで構成されるリダイレクト サーバ グループに送信されます。ISG は、リダイレクトされたパケットを受信するために、グループから 1 台のサーバをローテーション方式で順に選択します。

トラフィックがリダイレクトされると、ISG はアップストリーム パケットの宛先 IP アドレスと TCP ポートを、宛先サーバを反映させるように変更します。ダウンストリーム パケットの場合、ISG は宛先 IP アドレスとポートを元のパケットのソースに変更します。

redirection コマンドを含むポリシー マップによってトラフィックが選択される場合、別のサービス選択のために、パケットがポリシー マップの分類方式にフィードバックされます。変更された IP ヘッダーは、別の分類条件の基準とすることができます。たとえば、2 つのクラス マップが存在していて、それぞれに独自の **redirection** コマンドがある場合、パケットをリダイレクトできますが、最初のクラス マップによって選択され、別のクラス マップによってリダイレクトされます。この状況を回避するには、2 回連続するリダイレクトを同じパケットに適用できないように、トラフィック クラス マップを設定します。

レイヤ 4 リダイレクト アプリケーション

レイヤ 4 リダイレクト機能では、次のアプリケーションがサポートされます。

- 無許可のユーザおよび無許可のサービスのための TCP リダイレクト

  加入者からの HTTP トラフィックは、Web ダッシュボードにリダイレクトできます。Web ダッシュボードには、認証および認可を実行できるように加入者がログインできます。

- アドバタイジングによる魅了のための初期リダイレクトと定期的なリダイレクト

  セッションの開始時の短い期間、またはセッション全体で定期的に加入者トラフィックをスポンサーの Web ページにリダイレクトできます。

- アプリケーション トラフィックのリダイレクト

  加入者からのアプリケーション トラフィックは、付加価値サービスを提供するためにリダイレクトできます。たとえば、加入者の Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）トラフィックを、電子メールの転送エージェントとして機能しているローカル電子メール サーバにリダイレクトできます。

- DNS リダイレクト

  DNS クエリーはローカル DNS サーバにリダイレクトできます。Public Wireless LAN（PWLAN; パブリック ワイヤレス LAN）ホット スポットのような展開では、加入者がスタティック DNS サーバ アドレスを持っています。このアドレスでは、特定の場所に到達することはできません。DNS クエリーのローカル DNS サーバへのリダイレクトによって、アプリケーションが設定の必要なしに正常に動作できます。

ISG レイヤ 4 リダイレクトの設定方法

レイヤ 4 リダイレクトをセッションに適用するには、3 つの方法があります。その 1 つは、物理的なメイン インターフェイスまたは論理サブインターフェイスで直接リダイレクトを設定することです。2 番めの方法は、サービス プロファイルまたはサービス マップをレイヤ 4 リダイレクト アトリビュートとともに設定し、そのサービスをセッションに適用することです。3 番めの方法は、レイヤ 4 リダイレクト アトリビュートをユーザ プロファイルで設定することです。

次の作業では、レイヤ 4 リダイレクトの設定方法を示します。最初の作業は任意です。その後の 3 つの作業は 1 つ以上が必須です。最後の作業は任意です。

特定のアプリケーションのためのレイヤ 4 リダイレクト設定の例（無許可のユーザのリダイレクトなど）については、「ISG レイヤ 4 リダイレクトの設定例」（P.317）を参照してください。

- 「リダイレクト サーバ グループの定義」（P.312）
- 「サービス ポリシー マップでのレイヤ 4 リダイレクトの設定」（P.313）
- 「AAA サーバ上のサービス プロファイルまたはユーザ プロファイルでのレイヤ 4 リダイレクトの設定」（P.315）
- 「ISG トラフィック リダイレクトの確認」（P.315）

リダイレクト サーバ グループの定義

トラフィックのリダイレクト先となる 1 台以上のサーバのグループを定義するには、次の作業を実行します。トラフィックがローテーション方式で順にサーバに転送されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **redirect server-group** *group-name*
4. **server ip** *ip-address* **port** *port-number*

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	**redirect server-group** *group-name* 例： `Router(config)# redirect server-group ADVT-SERVER`	リダイレクト サーバ グループ コンフィギュレーション モードを開始して、名前が付けられたリダイレクト サーバ グループ内にサーバのグループを定義します。
ステップ 4	**server ip** *ip-address* **port** *port-number* 例： `Router(config-sg-l4redirect-group)# server ip 10.0.0.1 port 8080`	リダイレクト サーバ グループにサーバを追加します。 • このコマンドを 2 回以上入力して、複数のサーバをサーバ グループに追加することができます。

サービス ポリシー マップでのレイヤ 4 リダイレクトの設定

サービス ポリシー マップでレイヤ 4 リダイレクトを設定するには、次の作業を実行します。

前提条件

ISG レイヤ 4 リダイレクト機能は、サービス ポリシー マップ内のトラフィック クラスで設定されます。この作業は、トラフィック クラス マップを定義していることを前提としています。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。

制約事項

ISG ポリシングおよびアカウンティング機能は、同じサービス ポリシーでのリダイレクトと組み合せてイネーブルにすることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **redirect session-limit** *maximum-number*
4. **policy-map type service** *policy-map-name*
5. **class type traffic** *class-name*
6. **redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*]

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	**redirect session-limit** *maximum-number* 例： `Router(config)# redirect session-limit 5`	（任意）各加入者セッションで許容されるレイヤ 4 リダイレクトの最大数を設定します。
ステップ 4	**policy-map type service** *policy-map-name* 例： `Router(config)# policy-map type service service1`	サービス ポリシー マップ コンフィギュレーション モードを開始して、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 5	**class type traffic** *class-name* 例： `Router(config-service-policymap)# class type traffic class1`	（任意）トラフィック クラス マップ コンフィギュレーション モードを開始して、このサービスを適用するトラフィックを識別するトラフィック クラス マップを指定します。
ステップ 6	**redirect 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。

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。サービスのアクティブ化方法の詳細については、「Configuring ISG Subscriber Services」モジュールを参照してください。

AAA サーバ上のサービス プロファイルまたはユーザ プロファイルでのレイヤ 4 リダイレクトの設定

Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバ上のユーザ プロファイルまたはサービス プロファイルで Cisco Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）としてレイヤ 4 リダイレクト機能を設定できます。このアトリビュートは、セッションのための複数のタイプのリダイレクトを定義するために 2 回以上表示でき、ユーザ プロファイルとサービス プロファイルの両方を同時に使用できます。

手順の概要

1. レイヤ 4 リダイレクト VSA を AAA サービス上のユーザ プロファイルまたはサービス プロファイルに追加します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	レイヤ 4 リダイレクト VSA を AAA サービス上のユーザ プロファイルまたは加入者プロファイルに追加します。 Cisco-AVPair = "ip:l4redirect=redirect to {group *server-group-name* | ip *ip-address* [port *port-number*]} [duration *seconds*] [frequency *seconds*]"	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。

次の作業

サービス プロファイルで ISG レイヤ 4 リダイレクトを設定する場合、サービス プロファイルのアクティブ化方法を設定できます。たとえば、サービスをアクティブ化するために制御ポリシーを使用できます。サービスのアクティブ化方法の詳細については、「Configuring ISG Subscriber Services」モジュールを参照してください。

ISG トラフィック リダイレクトの確認

ISG レイヤ 4 トラフィック リダイレクトの設定と動作を確認するには、次の作業を実行します。コマンド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 redirect translations** [**ip** *ip-address*]
3. **show redirect group** [*group-name*]
4. **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 redirect translations** [**ip** *ip-address*] 例： `Router# show redirect translations ip 10.0.0.0`	セッションの ISG レイヤ 4 リダイレクト変換を表示します。
ステップ 3	**show redirect group** [*group-name*] 例： `Router# show redirect group redirect1`	ISG リダイレクト サーバ グループの情報を表示します。
ステップ 4	**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、アクティブなリダイレクト変換数を示す **show redirect translations** コマンドの出力例を示します。

```
Router# show redirect translations

Load for five secs: 1%/0%; one minute: 2%; five minutes: 2%
Time source is hardware calendar, *11:48:06.383 PST Wed Oct 21 2009
Maximum allowed number of L4 Redirect translations per session: 5

Destination IP/port    Server IP/port    Prot  In Flags  Out Flags  Timestamp
10.0.1.2        23     10.0.2.2   23     TCP                      Oct 21 2009 11:48:01
10.0.1.2        23     10.0.2.2   23     TCP                      Oct 21 2009 11:48:01
10.0.1.2        23     10.0.2.2   23     TCP                      Oct 21 2009 11:48:01

Total Number of Translations: 3

Highest number of L4 Redirect: 3 by session with source IP 10.0.0.2
```

次に、**show subscriber session** コマンドの出力例を示します。この出力は、レイヤ 4 リダイレクトがサービス プロファイルから適用されることを示しています。

```
Router# show subscriber session uid 135

Subscriber session handle: 7C000114, state: connected, service: Local Term
Unique Session ID: 135
Identifier: blind-rdt
SIP subscriber access type(s): IP-Interface
Root SIP Handle: CF000020, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 40 minutes, 30 seconds, Last Changed: 40 minutes, 30 seconds
AAA unique ID: 135
```

```
Switch handle: F000086
Interface: ATM2/0.53

Policy information:
  Authentication status: unauthen
  Config downloaded for session policy:
  From Access-Type: IP-Interface, Client: SM, Event: Service Selection Request, Service
    Profile name: blind-rdt, 2 references
      username             "blind-rdt"
      l4redirect           "redirect to group sesm-grp"
  Rules, actions and conditions executed:
    subscriber rule-map blind-rdt
      condition always event session-start
        action 1 service-policy type service name blind-rdt

Session inbound features:
 Feature: Layer 4 Redirect
  Rule  Cfg  Definition
  #1    SVC  Redirect to group sesm-grp  !! applied redirect
Configuration sources associated with this session:
Service: blind-rdt, Active Time = 40 minutes, 32 seconds
Interface: ATM2/0.53, Active Time = 40 minutes, 32 seconds
```

次に、レイヤ 4 リダイレクトがインターフェイス上で適用されるセッションへの **show subscriber session** コマンドの出力例を示します。

```
Router# show subscriber session uid 133

Subscriber session handle: D7000110, state: connected, service: Local Term
Unique Session ID: 133
Identifier:
SIP subscriber access type(s): IP-Interface
Root SIP Handle: 1E, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 42 minutes, 54 seconds, Last Changed: 42 minutes, 54 seconds
AAA unique ID: 133
Switch handle: 17000084
Interface: FastEthernet0/0.505

Policy information:
  Authentication status: unauthen

Session inbound features:
 Feature: Layer 4 Redirect
  Rule  Cfg  Definition
  #1    INT  Redirect to group sesm-grp
Configuration sources associated with this session:
Interface: FastEthernet0/0.505, Active Time = 42 minutes, 54 seconds
```

ISG レイヤ 4 リダイレクトの設定例

ここでは、次の例について説明します。

- 「無認証の加入者トラフィックのリダイレクト：例」（P.318）
- 「無許可の加入者トラフィックのリダイレクト：例」（P.318）
- 「初期 ISG リダイレクト：例」（P.319）
- 「定期的な ISG リダイレクト：例」（P.319）
- 「DNS トラフィックのリダイレクト：例」（P.319）

- 「PPP セッションのリダイレクト：例」（P.320）

無認証の加入者トラフィックのリダイレクト：例

次の例では、サービス ポリシー マップ「BLIND-RDT」でレイヤ 4 リダイレクトを設定します。このポリシーはすべてのセッションの開始時に適用され、加入者 TCP トラフィックが「PORTAL」という名前のサーバ グループにリダイレクトされます。アカウントのログイン時に加入者が認証され、リダイレクトは適用されません。

```
Service-policy type control DEFAULT-IP-POLICY

policy-map type control DEFAULT-IP-POLICY
 class type control always event session-start
  1 service-policy type service BLIND-RDT
!
 class type control always event account-logon
  1 authenticate aaa list AUTH-LIST
  2 service-policy type service unapply BLIND-RDT

policy-map type service BLIND-RDT
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
redirect server-group PORTAL
 server ip 10.2.36.253 port 80
```

無許可の加入者トラフィックのリダイレクト：例

次の例では、無許可の加入者に対するリダイレクトの設定例を示します。加入者が「svc」という名前のサービスにログインしていない場合、「svc」と一致するトラフィックがサーバ グループ「PORTAL」にリダイレクトされます。加入者がこのサービスにログインすると、トラフィックはリダイレクトされなくなります。加入者がサービスからログオフすると、再びリダイレクトが適用されます。

```
service-policy type control THE_RULE
!
class-map type traffic match-any CLASS-ALL
!
class-map type traffic match-any CLASS-100_110
 match access-group input 100
 match access-group output 110
!
policy-map type service blind-rdt
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
policy-map type service svc-rdt
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
policy-map type service svc
 class type traffic CLASS-100_110
 class type traffic default in-out
  drop
!

policy-map type control THE_RULE
 class type control alwyas event account-logon
  1 authenticate
  2 service-policy type service name svc-rdt
```

```
 class type control cond-svc-logon event service-start
  1 service-policy type service unapply name svc-rdt
  2 service-policy type service identifier service-name
 class type control cond-svc-logon event service-stop
  1 service-policy type service unapply name svc
  2 service-policy type service name svc-rdt
 !
class-map type control match-all cond-svc-logon
 match identifier service-name svc
!
redirect server-group PORTAL
 server ip 10.2.36.253 port 80
```

初期 ISG リダイレクト：例

次の例では、セッションの最初の 60 秒間にすべての加入者のレイヤ 4 トラフィックが「ADVT」という名前のサーバ グループにリダイレクトされるように ISG を設定する方法を示します。最初の 60 秒間の経過後、ISG はセッション終了までトラフィックのリダイレクトを停止します。

```
service-policy type control initial-rdt
policy-map type control intial-rdt
 class type control always event session-start
  1 service-policy type service name initial-rdt-profile
 !
policy-map type service initial-rdt-profile
 class type traffic CLASS-ALL
  redirect to group ADVT duration 60
```

定期的な ISG リダイレクト：例

次の例では、3600 秒おきに 60 秒間すべての加入者トラフィックをリダイレクトする方法を示します。

```
service-policy control periodic-rdt session-start
!
policy-map type control periodic-rdt
 class type control always event session-start
  1 service-policy service periodic-rdt-profile
 !
policy-map type service periodic-rdt-profile
 redirect to group ADVT duration 60 frequency 3600
```

DNS トラフィックのリダイレクト：例

次の例では、すべての加入者 DNS パケットをサーバ グループ「DNS-server」にリダイレクトする方法を示します。

```
service-policy type control DNS-rdt

policy-map type control DNS-rdt
 class type control event session-start
  1 service-policy type service name DNS-rdt-profile
  !
policy-map type service DNS-rdt-profile
 class type traffic CLASS-ALL
  redirect to group DNS-server
```

PPP セッションのリダイレクト：例

次の例では、PPP セッションのレイヤ 4 リダイレクトを設定する方法を示します。

```
class-map type traffic match-any CLASS-L4R
!
policy-map type service svc-rdt
 class type traffic CLASS-L4R
  redirect to group PORTAL
!
policy-map type control THE_RULE
 class type control alwyas event session-start
  1 authenticate
  2 service-policy type service name svc-rdt
!
redirect server-group PORTAL
server ip 10.2.36.253 port 80
!
```

（注） 仮想テンプレートで認証を設定する必要はありません。設定された場合、認証アクションは制御ポリシーに含まれているはずで、リダイレクトされるユーザに対してさえも認証が成功するはずです。

その他の参考資料

ここでは、ISG レイヤ 4 リダイレクト機能に関連する参考資料を示します。

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*』
ISG 加入者サービスの設定	『*Cisco IOS Intelligent Services Gateway Configuration Guide*』の「Configuring ISG Subscriber Services」の項

規格

規格	タイトル
なし	—

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。またこの機能による既存 MIB のサポートに変更はありません。	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
なし	—

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 加入者トラフィック リダイレクトの機能情報

表 28 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。特定のコマンドのサポートの導入時期に関する詳細については、コマンド リファレンス マニュアルを参照してください。

Cisco IOS ソフトウェア イメージは、Cisco IOS ソフトウェア リリース、機能セット、プラットフォームそれぞれに固有です。プラットフォーム サポートと Cisco IOS 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。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスするには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明の場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

（注） 表 28 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 28　ISG 加入者トラフィック リダイレクトの機能情報

機能名	リリース	機能情報
ISG：フロー制御：フロー リダイレクト	12.2(28)SB 12.2(33)SRC 12.2(33)XNE	サービス プロバイダーが ISG レイヤ 4 リダイレクト機能を使用すると、加入者 TCP または UDP パケットを適切な処理のために指定されたサーバにリダイレクトできるようにすることによって、ユーザ環境が向上します。ISG レイヤ 4 リダイレクトは、個々の加入者セッションまたはフローに適用できます。 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 加入者トラフィック リダイレクトに関する情報」（P.310） • 「ISG レイヤ 4 リダイレクトの設定方法」（P.312） 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。 この機能は、Cisco IOS Release 12.2(33)XNE に統合されました。

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。

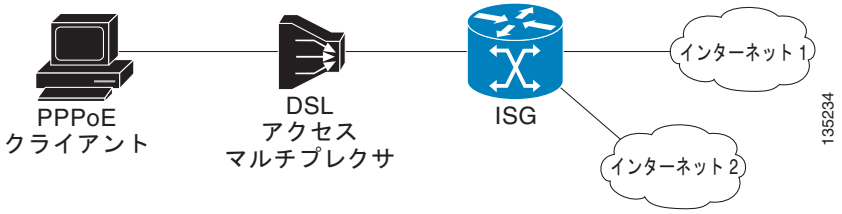
図 6　　Session-Based ポリシング

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。

SAMI ブレードの ISG サポート

SAMI ブレードの ISG サポート機能は、加入者管理機能および Cisco Intelligent Services Gateway（ISG）の機能を Cisco Service Application Module for IP（SAMI）の処理能力と組み合わせたものです。Cisco SAMI ブレードには 6 個の PowerPC（PPC）プロセッサが搭載され、Cisco 7600 シリーズ ルータのスロットを 1 つだけ占有します。つまり、単一のルータ上で最高 600,000 の加入者に対して数多くの ISG 機能をサポートできます。

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、「SAMI ブレードの ISG サポートの機能情報」（P.341）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

SAMI ブレードの ISG サポートの前提条件

- Cisco SAMI ブレードが設置および設定されていること。詳細については、『*Cisco Service and Application Module for IP User Guide*』を参照してください。

- PPC プロセッサが Cisco SAMI ブレード上でどのように設定されているかを理解していること。詳細については、『*Cisco Service and Application Module for IP User Guide*』の「Overview of the Cisco SAMI」の章を参照してください。
- SAMI ブレード上の 6 個すべての PPC が同じ Cisco IOS イメージを実行していること。

SAMI ブレードの ISG サポートの制約事項

次のタイプの ISG セッションは、Cisco SAMI ブレード上でサポートされていません。

- PPP セッション。トラフィックはネイティブ IPoE トラフィックとして Cisco SAMI ブレードに到達する必要があります。
- IP インターフェイス セッション。

(注) IP インターフェイス セッションはサポートされていますが、ISG のサポートにはサブインターフェイス セッションの方が適しています。
IP ルーテッド セッションとレイヤ 2 接続セッションがサポートされています。

次の ISG 機能は、Cisco SAMI ブレードでサポートされていません。

- VRF 選択
- VRF セッション転送

SAMI ブレードの ISG サポートに関する情報

Cisco SAMI ブレードは、加入者との間のトラフィックを受信するための外部物理インターフェイスを持っていません。Cisco 7600 シリーズ ルータ シャーシのスイッチ ファブリックに接続され、内部ギガビット イーサネット ポートが、SAMI ブレードとスーパーバイザ モジュールとの間のインターフェイスを提供します。

6 個の SAMI の PPC を、SAMI ブレード上でそれぞれ個別に設定する必要があります。SAMI ブレードの ISG サポート機能を設定するには、IP 加入者セッションのために ISG アクセスを設定する方法を理解しておく必要があります。詳細については、『*Cisco IOS Intelligent Services Gateway Configuration Guide*』の「Configuring ISG Access for IP Subscriber Sessions」の章を参照してください。

(注) VRF 選択と VRF セッション転送は、この機能ではサポートされていません。

また、次の概念も理解しておく必要があります。

- 「SAMI サブインターフェイス」（P.338）

SAMI サブインターフェイス

サブインターフェイスを各 PPC の GigabitEthernet0/0 単一論理ポート上で作成して設定できるように、Virtual LAN（VLAN）を設定し、スーパーバイザ エンジンから Cisco SAMI ブレードに対して割り当てる必要があります。その後、それらのサブインターフェイス上で ISG をイネーブルにすると、IP ベースの加入者管理機能を実行できます。

詳細については、『*Cisco Service and Application Module for IP User Guide*』の「Maintaining and Monitoring the Cisco SAMI」および「Configuring VLAN Support」を参照してください。

その他の参考資料

ここでは、SAMI ブレードの ISG サポート機能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
Cisco SAMI のインストール、削除、および初期設定	『*Cisco Service and Application Module for IP User Guide*』
IP 加入者セッションのための ISG アクセスの設定	『*Cisco IOS Intelligent Services Gateway Configuration Guide*』の「Configuring ISG Access for IP Subscriber Sessions」の章

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco 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
なし	–

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

SAMI ブレードの ISG サポートの機能情報

表 30 に、この機能のリリース履歴を示します。

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 を使用すると、Cisco IOS、Catalyst OS、Cisco IOS XE 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 30 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 30　SAMI ブレードの ISG サポートの機能情報

機能名	リリース	機能情報
SAMI ブレードの ISG サポート	12.2(33)SRD	加入者管理機能および ISG の機能を、Cisco SAMI ブレードの処理能力と組み合わせます。

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**

Service Gateway Interface

Service Gateway Interface（SGI）機能は、ポリシー、加入者、およびセッションに対する Intelligent Services Gateway（ISG）の管理機能にアクセスするための Web サービス インターフェイスを実装するものです。これによって、アプリケーション開発者は、有料およびオープン ソースの一般的に入手可能なプロトコル、コード化方式、およびツールキットを使用して、加入者管理アプリケーションを作成することができます。

ISG は、ネットワーク デバイス上でセッションおよびサービスをポリシー ベースで制御するためのコンポーネントから成るフレームワークです。この SGI 機能は、ポリシーおよび関連要素のデータ モデルと、それらのポリシーのプロビジョニング、更新、削除、およびアクティブ化制御を行う操作インターフェイスで構成されています。

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、「Service Gateway Interface の機能情報」（P.366）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

Service Gateway Interface の制約事項

リリース 12.2(33)SRC では、SGI 機能で HTTP 転送ポリシーがサポートされません。

リリース 12.2(33)SRC では、クライアントが SGI 機能にアクセスするようになっていません。

Service Gateway Interface に関する情報

Service Gateway Interface 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。

- 「ISG」（P.360）
- 「BEEP」（P.360）
- 「SGI の利点」（P.360）

ISG

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。詳細については、「*Overview of ISG*」を参照してください。

BEEP

Block Extensible Exchange Protocol（BEEP）は、スケーラブル、効率的、シンプル、拡張可能、かつ堅牢なプロトコル規格です。BEEP は、アプリケーション プロトコルを設計するためのフレームワークです。

SGI の利点

SGI は、Web サービス用のサードパーティ製のアプリケーション、ツールキット、および開発プラットフォームを使用して、Cisco IOS ソフトウェアを制御できるようにするプロトコルです。

SGI 機能は ISG プロビジョニングを多言語で表すことができる共通モデルであり、簡単に使用できます。

Service Gateway Interface をイネーブルにする方法

ここでは、次の作業について説明します。

- 「BEEP リスナー接続の設定」（P.360）（必須）
- 「SGI のトラブルシューティング」（P.361）（任意）

BEEP リスナー接続の設定

SGI をイネーブルにするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **sgi beep listener** [*port*] [**acl** *access-list*] [**sasl** *sasl-profile*] [**encrypt** *trustpoint*]
4. **command** [**keyword** *argument*]
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	**sgi beep listener** [*port*][**acl** *access-list*][**sasl** *sasl-profile*][**encrypt** *trustpoint*] 例： `Router(config)# sgi beep listener 2089`	SGI 機能をイネーブルにします。
ステップ 4	**end** 例： `Router(config)# end`	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。

SGI のトラブルシューティング

SGI をトラブルシューティングするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **show sgi** [**session** | **statistics**]
3. **debug sgi** [**error** | **info** | **xml** | **gsi** | **isg-api** | **all**]
4. **test sgi xml** *filename*

手順の詳細

ステップ 1 **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 sgi [session | statistics]**

現在の SGI セッションに関する情報を表示します。このコマンドは、開始済みおよび現在実行中の SGI セッションに関する、実行状態などの情報を表示します。また、開始済みおよび現在実行中の SGI セッションに関する統計情報も表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show sgi session

sgi sessions: open 1(max 10, started 15
session id:1;started at 9:08:05; state OPEN

Router# show sgi statistics

sgi statistics
total messages received 45
current active messages 5; maximum active messages 7
total isg service requests 4
current active services 2; maximum active services 2

sgi process statistics
process sgi handler 1
pid 95, cpu percent (last minute) 1, cpu runtime 10(msec), memory accocated 4200 (bytes)
```

ステップ 3 **debug sgi [error | info | xml | gsi | isg-api | all]**

SGI セッションのデバッグをイネーブルにします。次に、すべてのデバッグをイネーブルにした場合のコマンドの出力例を示します。

```
Router# debug sgi all

Router# show debug
SGI:
SGI All debugging is on
SGI Errors debugging is on
SGI XML debugging is on
SGI Informational debugging is on
SGI Generic Service Interface debugging is on
SGI ISG_API Events debugging is on
SGI ISG_API Errors debugging is on
Router#


Router#
*Jul 1 20:55:11.364: SGI: Session created, session Id 7
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: frame_available: type=M
number=1 answer=-1 more=* size=1400

*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
...
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: frame_available: type=M
number=1 answer=-1 more=. size=111

*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: gitypes:policyGroup>

</objects>
</sgiops:insertPolicyObjectsRequest>
```

```
...
*Jul 1 20:55:11.372: SGI: GSI message received, msgid 1, session 7
*Jul 1 20:55:11.376: SGI: XML parsed successfully, request insertPolicyObjectsRequest,
msgid 1
*Jul 1 20:55:11.376: SGI: authentication request sent to AAA
*Jul 1 20:55:11.376: SGI: req = [0x67454088] authentication succeeded
*Jul 1 20:55:11.376: SGI: Processing insertPolicyObjectsRequest
*Jul 1 20:55:11.376: SGI: insertPolicyObjectsRequest processing policyGroup:VPDN1, type 1,
result: 0
*Jul 1 20:55:11.376: SGI: Processing insertPolicyObjectsResponse
*Jul 1 20:55:11.376: SGI: GSI message sent, msgid 1, session 7
*Jul 1 20:55:12.088: sgi beep listen app beep[0x66245188]: close confirmation: status=+ no
error origin=L scope=C
*Jul 1 20:55:12.088: SGI: Session terminating, session Id 7
Router#
```

ステップ 4 **test sgi xml** *filename*

SGI XML 要求のフォーマットを検証します。XML ファイルは、使用する前にルータにコピーする必要があります。

Service Gateway Interface の設定例

ここでは、次の設定例について説明します。

- 「BEEP リスナー接続の設定：例」（P.363）

BEEP リスナー接続の設定：例

次に、BEEP リスナー接続を設定する例を示します。ポート番号は 2089 に設定します。

```
enable
configure terminal
sgi beep listener 2089
```

その他の参考資料

ここでは、Service Gateway Interface 機能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 の概要	『*Cisco IOS Intelligent Services Gateway Configuration Guide*』
ISG コマンド	『*Cisco IOS Intelligent Services Gateway Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
• なし	選択したプラットフォーム、Cisco 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
なし	—

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

コマンド リファレンス

次のコマンドは、このモジュールで説明した機能で導入または修正されたものです。これらのコマンドの詳細については、『*Cisco IOS Intelligent Services Gateway Command Reference*』（http://www.cisco.com/en/US/docs/ios/isg/command/reference/isg_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html にある『*Cisco IOS Master Command List, All Releases*』を参照してください。

- **debug sgi**
- **sgi beep listener**
- **show sgi**
- **test sgi xml**

Service Gateway Interface の機能情報

表 33 に、この機能のリリース履歴を示します。

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 33 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 33　Service Gateway Interface の機能情報

機能名	リリース	機能情報
Service Gateway Interface	12.2(33)SRC	SGI は、ポリシー、加入者、およびセッションに対する ISG の管理機能にアクセスするための Web サービス インターフェイスを実装するものです。 次のコマンドが、新たに導入または変更されました。 **debug sgi**、**sgi beep listener**、**show sgi**、**test sgi xml**

セッション モニタリングと分散型条件付きデバッグによる ISG のトラブルシューティング

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。このマニュアルでは、ISG セッション モニタリングと分散型条件付きデバッグについて説明します。条件付きデバッグは、ISG のためにデバッグ フィルタリングを容易にし、分散型条件付きデバッグとして利用可能です。

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、「分散型条件付きデバッグの機能情報」（P.378）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 セッション モニタリングと分散型条件付きデバッグの前提条件

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、「分散型条件付きデバッグの機能情報」（P.378）を参照してください。

このモジュールの情報を利用する前に、Cisco IOS の **debug** コマンドの使用法と条件付きデバッグについて理解しておくことを推奨します。これらの内容については、「その他の参考資料」（P.377）を参照してください。

分散型条件付きデバッグに関する制約事項

アクティブ セッションに設定されている条件は、そのセッションが終了して再確立した場合にのみ有効になります。

注意 デバッグ出力には、CPU プロセスで高いプライオリティが割り当てられるので、システムが使用不能になる可能性があります。したがって、Cisco IOS **debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合だけにしてください。また、**debug** コマンドを使用するのは、ネットワーク トラフィックとユーザが少ない時間帯、あるいはアクティブ セッションが 1 つのデバッグ シャーシが最適です。そのような時間帯を選んでデバッグを実行すると、**debug** コマンドの処理のオーバーヘッドによってシステム利用が影響を受ける可能性が少なくなります。

ISG セッション モニタリングと分散型条件付きデバッグに関する情報

- 「ISG セッションとフローのモニタ」（P.368）
- 「ISG 分散型条件付きデバッグ」（P.368）

ISG セッションとフローのモニタ

ISG により、管理者が ISG セッションおよびフローを連続的にモニタできるメカニズムが導入されます。インターフェイス統計情報を表示する **show interface monitor** コマンドと、CPU の使用状況に関する情報を表示する **show process cpu monitor** コマンドは、どちらも指定された間隔でその表示を更新します。これらのコマンドは、表示情報をフリーズまたはクリアする機能も備えています。

ISG 分散型条件付きデバッグ

- 「ISG プラットフォームの拡張条件付きデバッグの利点」（P.369）
- 「分散型条件付きデバッグでサポートされる Cisco IOS ソフトウェア コンポーネント」（P.369）

ISG プラットフォームの拡張条件付きデバッグの利点

数千ものユーザ セッションが ISG プラットフォーム上で稼動しているため、利用可能な各種コンポーネントの **debug** コマンドをイネーブルにした状態で、単一のセッションまたはユーザのメッセージをトレースすることによって、1 つのセッションの 1 つの問題をトラブルシューティングすることは実用的でありません。それよりも、セッションが通過する各種 Cisco IOS コンポーネント全体で、単一のセッションまたはコールのデバッグ メッセージをフィルタリングする方が実用的です。その結果、Cisco IOS ソフトウェアで以前提供されていた条件付きデバッグが拡張され、ISG 用のデバッグ フィルタリングが容易になり、分散型条件付きフィルタリングとして利用可能になりました。

分散型条件付きデバッグでサポートされる Cisco IOS ソフトウェア コンポーネント

次のコンポーネントが ISG 分散型条件付きデバッグ用にサポートされています。

- Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）および RADIUS
- ATM コンポーネント
- Feature Manager
- Policy Manager
- PPP
- PPP over Ethernet（PPPoE）
- Session Manager
- Virtual Private Dialup Network（VPDN）

分散型条件付きデバッグ用にサポートされる実際のコマンドについては、表 34 および表 35 を参照してください。

ISG セッション モニタリングと分散型条件付きデバッグをイネーブルにする方法

ISG セッションとフローのモニタ

インターフェイスおよび CPU 統計情報をモニタするには、次の作業を実行します。**show** コマンドは必須ではなく、任意の順序で入力できます。

手順の概要

1. **enable**
2. **show interface** *type number* **monitor** [**interval** *seconds*]
3. **show processes cpu monitor** [**interval** *seconds*]

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 interface** *type number* **monitor** [**interval** *seconds*] 例： Router# show interface ethernet 3/0 monitor interval 10	インターフェイス統計情報を表示し、指定された間隔で更新します。
ステップ 3	**show processes cpu monitor** [**interval** *seconds*] 例： Router# show processes cpu monitor	詳細な CPU 使用率統計情報を表示し、指定された間隔で更新します。

分散型条件付きデバッグの設定

分散型条件付きデバッグを設定するには、条件付きデバッグをイネーブルにし、1 つ以上のサポートされる **debug** コマンドを発行するという、2 つの主要な作業が必要です。ここでは、これらの必須作業について説明します。

ISG デバッグ条件コマンド

表 34 に、EXEC プロンプトで発行可能な、分散型条件付きデバッグをイネーブルにする **debug condition** コマンドを示します。複数の条件を設定できます。

表 34　サポートされる条件付きデバッグ コマンド

コマンド	目的
debug condition domain *domain-name*	指定されたドメイン名でメッセージをフィルタリングします。
debug condition interface atm *ATM-interface* **vc** {*vci*/*vpi* | *vci*}	指定された仮想回線でメッセージをフィルタリングします。
debug condition interface {**atm** *ATM-interface* **vc** {*vci*/*vpi* | *vci*} | **Ethernet** | **Fast Ethernet** | **Gigabit Ethernet**} **vlan-id** *ID*	指定された VLAN ID でメッセージをフィルタリングします。

表 34　サポートされる条件付きデバッグ コマンド （続き）

コマンド	目的
debug condition mac-address *hexadecimal-MAC-address*	指定された MAC アドレスでメッセージをフィルタリングします。
debug condition portbundle ip *IP-address* **bundle** *bundle-number*	指定された Port-Bundle Host Key（PBHK）でメッセージをフィルタリングします。
debug condition session-id *session-ID*	指定されたセッション ID でメッセージをフィルタリングします。 （注）　セッション ID は、**show subscriber session** コマンドの入力によって取得できます。
debug condition username *email-address*	指定されたインターネット ユーザ名でメッセージをフィルタリングします。

ISG 条件付きデバッグでサポートされるデバッグ コマンド

表 35 に、ISG 条件付きデバッグ用としてサポートされる Cisco IOS デバッグ コマンドを示します。各コマンドはコンポーネント別に示してあります。表 34 に示した **debug condition** コマンドの 1 つをイネーブルにした後で、これらのコマンドの 1 つ以上を発行できます。

表 35　ISG 分散型条件付きデバッグでサポートされるデバッグ コマンド

AAA デバッグ コマンド
debug aaa accounting
debug aaa authentication
debug aaa authorization
debug aaa id
ATM デバッグ コマンド
debug atm arp
debug atm error
debug atm event
debug atm oam
debug atm packet
debug atm state
PPP デバッグ コマンド
debug ppp authentication
debug ppp bap error
debug ppp bap events
debug ppp bap negotiation
debug ppp cbcp
debug ppp error
debug ppp mppe detailed
debug ppp mppe events
debug ppp mppe pack

表 35　ISG 分散型条件付きデバッグでサポートされるデバッグ コマンド （続き）

debug ppp multi data
debug ppp multi events
debug ppp multi frag
debug ppp negotiation
debug ppp pack
debug ppp subscriber
PPPoE デバッグ コマンド
debug pppoe data
debug pppoe error
debug pppoe event
debug pppoe packet
Session Manager デバッグ コマンド
debug subscriber aaa authorization event
debug subscriber aaa authorization fsm
debug subscriber error
debug subscriber event
Feature Manager デバッグ コマンド
debug subscriber feature access-list error
debug subscriber feature access-list event
debug subscriber feature compression detail
debug subscriber feature compression error
debug subscriber feature compression event
debug subscriber feature detail
debug subscriber feature error
debug subscriber feature event
debug subscriber feature interface-config error
debug subscriber feature interface-config event
debug subscriber feature modem-on-hold detail
debug subscriber feature modem-on-hold error
debug subscriber feature modem-on-hold event
debug subscriber feature portbundle error
debug subscriber feature portbundle event
debug subscriber feature portbundle packet
debug subscriber feature qos-policy error
debug subscriber feature qos-policy event
debug subscriber feature static-routes error
debug subscriber feature static-routes event
debug subscriber feature traffic-classification detail
debug subscriber feature traffic-classification error

表 35　ISG 分散型条件付きデバッグでサポートされるデバッグ コマンド （続き）

debug subscriber feature traffic-classification event
Policy Manager デバッグ コマンド
debug subscriber fsm
debug subscriber policy condition
debug subscriber policy detail
debug subscriber policy error
debug subscriber policy event
debug subscriber policy fsm
debug subscriber policy rule
debug subscriber session error
debug subscriber session event
VPDN デバッグ コマンド
debug vpdn call event
debug vpdn call fsm
debug vpdn error
debug vpdn event
debug vpdn event disconnect

制約事項

debug condition session-id コマンドがセッションをフィルタリングするのは、そのセッションが確立した後だけです。セッション ID は、Cisco IOS ソフトウェアによって内部的に生成され、セッション確立時に各セッションに割り当てられる一意の動的な番号です。

VPDN では、トンネルに関連付けられた **debug** コマンドとメッセージは、セッションに関連付けられていないためフィルタリングできませんが、トンネル確立中に表示されます。デバッグ メッセージは、1 つの条件によってフィルタリングがイネーブルにされた場合でも表示されます。

複数の条件が設定されている場合は、いずれかの条件を満たす、すべてのセッションに対応するデバッグ メッセージが表示されます。ドメイン名など、いくつかの条件によって、特にそのドメインに属するすべてのセッションについてデバッグ メッセージがトリガーされます。

分散型条件付きデバッグのイネーブル化

ISG に対して分散型条件付きデバッグをイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **debug condition** *command*
3. **debug** *command*

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	**debug condition** *command* 例： `Router# debug condition username user@cisco.com`	表 34 に示した 1 つ以上の **debug condition** コマンドを入力して、分散型条件付きデバッグをイネーブルにします。
ステップ 3	**debug** *command* 例： `Router# debug subscriber aaa authorization fsm`	サポートされる表 35 の 1 つ以上の **debug** コマンドを入力します。

デバッグ条件の表示

設定されているデバッグ条件を表示するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show debug condition**

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 debug condition** 例： `Router# show debug condition`	デバッグ用に設定されている条件を表示します。

トラブルシューティングのヒント

デバッグのフィルタリング用に設定した条件に従って、Cisco IOS ソフトウェアがメッセージを表示します。

条件を設定すると、次のように番号が割り当てられます。

```
Condition 1 set
```

条件がすでに設定されている場合は、次のメッセージが表示されます。

```
% Condition already set
```

debug condition コマンドの **no** 形式を使用して最後の条件をディセーブルにしようとすると、次のメッセージとプロンプトが表示されます。

```
This condition is the last interface condition set.
Removing all conditions may cause a flood of debugging messages
to result, unless specific debugging flags are first removed.

Proceed with removal? [yes/no]: yes
Condition 1 has been removed
```

ヒント 設定されているすべてのデバッグ条件をディセーブルにする前に、各コマンドの **no** 形式を使用してすべての **debug** コマンドをディセーブルにしてください。

ISG 分散型条件付きデバッグの設定例

インターフェイス統計情報のモニタ：例

次の例は、**show interface monitor** コマンドのサンプル出力を示しています。表示は 10 秒ごとに更新されます。

```
Router> show interface ethernet 0/0 monitor interval 10

Router Name:  Scale3-Router8       Update Secs: 10
Interface Name:   Ethernet 0/0          Interface Status: UP, line is up

Line Statistics:          Total:        Rate(/s)    Delta
Input Bytes:              123456        123         7890
Input Packets:              3456         56          560
Broadcast:                  1333          6           60
OutputBytes:               75717        123         1230
Output Packets:              733         44          440

Error Statistics:         Total:        Delta:
Input Errors:              0               0
CRC  Errors:               0               0
Frame Errors:              0               0
Ignored:                   0               0
Output Errors:             0               0
Collisions:                0               0

No. Interface Resets:  2
End = e       Clear = c      Freeze = f
Enter Command:
```

CPU 統計情報のモニタ：例

次の例は、**show processes cpu monitor** コマンドのサンプル出力を示しています。

```
Router> show processes cpu monitor

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)   Invoked      uSecs    5Sec   1Min     5Min    TTY Process
   3      772          712       1084    0.08%  0.04%    0.02%    0    Exec
  67      276         4151         66    0.08%  0.03%    0.01%    0 L2TP mgmt daemon
 116      604         2263        266    0.16%  0.05%    0.01%    0 IDMGR CORE

End = e    Freeze = f
Enter Command:
```

ISG 分散型条件付きデバッグのイネーブル化：例

次の例は、ユーザ名「user@cisco.com」を持つ PPPoE セッションの PPP、PPPoE、および Session Manager のデバッグをフィルタリングする方法を示しています。定義済みユーザのデバッグ メッセージのみがコンソールに表示されます。他のユーザに関連付けられている他のデバッグ メッセージは表示されません。

```
Router# debug condition username user@cisco.com
Condition 1 set

Router# debug ppp negotiation
Router# debug pppoe event
Router# debug subscriber session event
```

デバッグ条件の表示：例

次の例は、設定されているデバッグ条件を表示する方法を示しています。

```
Router# show debug condition

Condition 1: domain cisco.com (0 flags triggered)
Condition 2: username user@cisco.com (0 flags triggered)
Condition 3: ip 172.19.200.10 (0 flags triggered)
```

デバッグ出力のフィルタリング：例

次の例では、**debug subscriber packet detail** コマンドの出力がユーザ名「cpe6_1@isp.com」に基づいてフィルタリングされます。

```
Router# debug condition username cpe6_1@isp.com

Condition 1 set

Router# show debug

Condition 1: username cpe6_1@isp.com (0 flags triggered)

Router# debug subscriber packet detail

SSS packet detail debugging is on
```

```
Router# show debug

SSS:
  SSS packet detail debugging is on

Condition 1: username cpe6_1@isp.com (0 flags triggered)

Router#
```

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*』
Cisco IOS の **debug** コマンド	『*Cisco IOS Debug Command Reference*』
条件付きデバッグ	『*Cisco IOS Debug Command Reference*』の「Conditionally Triggered Debugging」の章

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

分散型条件付きデバッグの機能情報

表 36 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 36 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 36　ISG セッション モニタリングと分散型条件付きデバッグの機能情報

機能名	リリース	機能設定情報
ISG：装置：セッションとフローのモニタ	12.2(28)SB 12.2(33)SRC 15.0(1)S	ISG には、インターフェイス統計情報と CPU 統計情報を連続的にモニタするためのメカニズムが用意されています。この機能により、指定された間隔で更新される統計情報を表示する **show interface monitor** コマンドと **show processes cpu monitor** コマンドが導入されます。 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 セッションとフローのモニタ」（P.368） • 「ISG セッションとフローのモニタ」（P.369） この機能は、Cisco IOS Release 12.2(28)SB で導入されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。
ISG：装置：拡張条件付きデバッグ	12.2(28)SB 12.2(33)SRC	ISG には、デバッグ出力のフィルタリング用に各種の条件を定義する機能が用意されています。条件付きデバッグでは、セッション、フロー、加入者、およびサービスの診断に使用できる非常に具体的な関連情報が生成されます。 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 分散型条件付きデバッグ」（P.368） • 「分散型条件付きデバッグの設定」（P.370） この機能は、Cisco IOS Release 12.2(28)SB で導入されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。