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

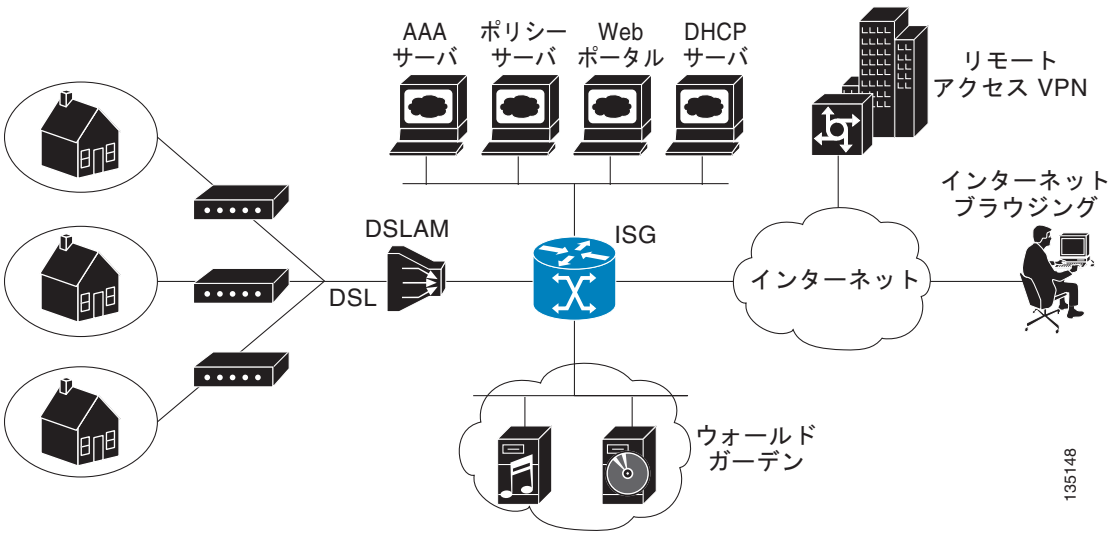
ISG は、エッジ アクセス デバイスによって柔軟で拡張性の高いサービスを加入者に提供できる構造化フレームワークです。ISG は加入者管理の、次の主要部分を処理します。

- 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

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。