# 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<br>CoA 要求<br>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**<br><br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• 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**<br><br>例：<br>`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*...]<br><br>例：<br>`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*...]<br><br>例：<br>`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*...]]<br><br>例：<br>`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*...]<br><br>例：<br>`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。<br>• **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**<br><br>例：<br>`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*<br><br>**例：**<br>`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**<br><br>**例：**<br>`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**<br><br>**例：**<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• 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**<br><br>**例：**<br>`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**<br><br>例：<br>`Router(config)# aaa server radius dynamic-author` | ISG を AAA サーバとして設定します。<br>• 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*]<br><br>例：<br>`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*<br><br>例：<br>`Router(config-locsvr-da-radius)# port 1600` | RADIUS サーバ ポートを指定します。<br>• デフォルト値は 1700 です。 |
| ステップ 6 | **server-key** [**0** \| **7**] *word*<br><br>例：<br>`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**}<br><br>例：<br>`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**}<br><br>例：<br>`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**<br><br>例：<br>`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**<br><br>例：<br>`Router> enable` | 特権 EXEC モードを開始します。<br>• 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**<br><br>例：<br>`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**<br><br>例：<br>`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**<br><br>例：<br>`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**<br><br>例：<br>`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**<br><br>例：<br>`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。<br>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。<br><br>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。<br>・テクニカル サポートを受ける<br>・ソフトウェアをダウンロードする<br>・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<br>・ツールおよびリソースへアクセスする<br>- Product Alert の受信登録<br>- Field Notice の受信登録<br>- Bug Toolkit を使用した既知の問題の検索<br>・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<br>・トレーニング リソースへアクセスする<br>・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<br><br>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<br>12.2(33)SRC<br>12.4(20)T<br>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。<br>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。<br>• 「初期認可と動的認可」（P.200）<br>• 「AAA クライアントとしての ISG の設定」（P.201）<br>• 「AAA サーバとしての ISG の設定」（P.203）<br>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。<br>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<br>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。<br>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。<br>• 「ISG のトリプルキー認証」（P.200）<br>• 「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） |

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。