サービス プロバイダーの WiFi オフロードのための、ASR 1000 シリーズ アグリゲーション サービス ルータでの iWAG

初版：2012 年 11 月 28 日

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでの Intelligent Wireless Access Gateway（iWAG）機能の実装では、2 種類の主要なテクノロジーが関係します。それは、Cisco ゲートウェイ GPRS サポート ノード（Cisco GGSN）に接続するためのグローバル パケット ラジオ サービス（GPRS）トンネリング プロトコル（GTP）と、Cisco Packet Data Network Gateway（PGW）に接続するためのプロキシ モバイル IPv6（PMIPv6）を使用した Mobile Access Gateway（MAG）です。これら 2 つテクノロジーの Cisco Intelligent Services Gateway（ISG）との統合と、サービス プロバイダー（SP）WiFi の組み合わせは、iWAG の重要な概念です。

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの iWAG は、GTP を使用して Cisco GGSN を通じた既存の 3G モバイル コアと統合するためのクライアントレス ソリューションを提供します。iWAG は、Cisco ISG フレームワークを利用して、ユーザ トラフィックをモバイル ネットワークに選択的に迂回させたり、インターネットに直接オフロードできます。このマニュアルでは iWAG の GTP とその設定に関する情報を提供します。

IWAG の PMIPv6 および ISG の設定の詳細については、『*Intelligent Wireless Access Gateway Configuration Guide, Cisco IOS XE Release 3S*』を参照してください。

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。機能と注意点に関する最新情報については、ご使用のプラットフォームとソフトウェア リリースに該当するリリース ノートを参照してください。本モジュールに記載されている機能についての情報と、各機能がサポートされているリリースの一覧については、「サービス プロバイダーの WiFi オフロードのための、Cisco ASR 1000 シリーズ ルータでの iWAG の機能情報」（P.28）を参照してください。

プラットフォームのサポートおよび Cisco IOS と Cisco Catalyst のオペレーティング システム ソフトウェア イメージのサポートに関する情報を検索するには、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。

内容

iWAG の導入の概要

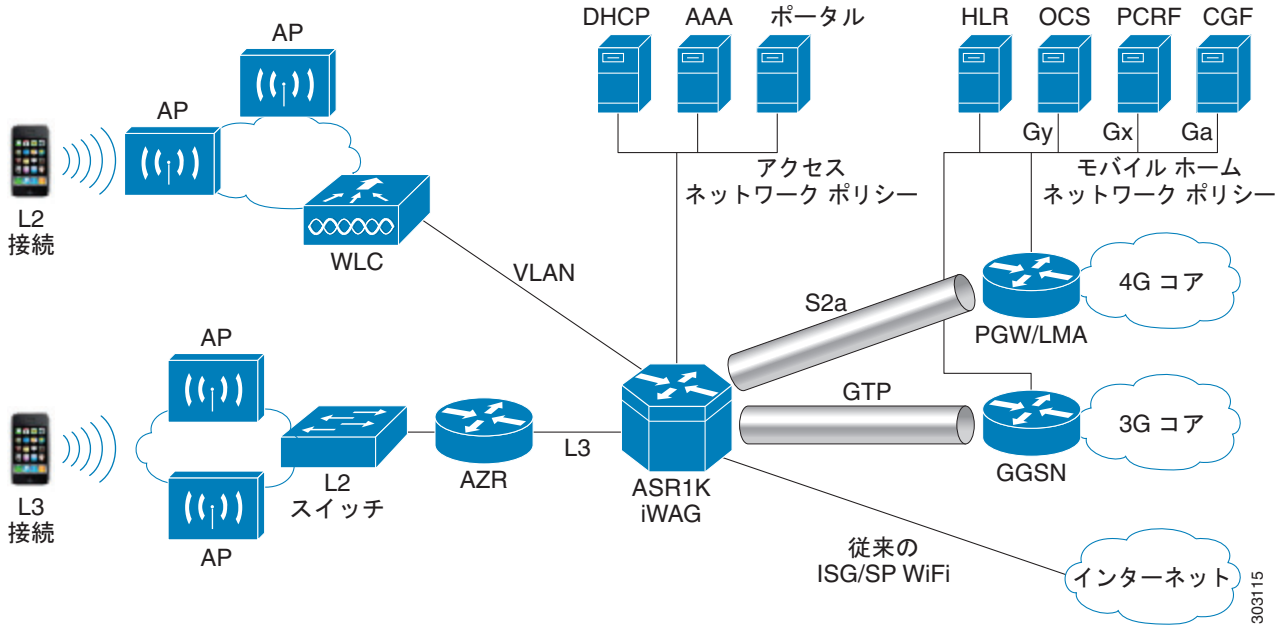
サービス プロバイダーは、WiFi とモビリティ製品を組み合わせて使用し、サービスの使用が非常に集中しているエリアでモビリティ ネットワークをオフロードします。WiFi とモビリティの両方を同時に提供することは望ましい導入と見なされ、iWAG 機能の進化につながります。

iWAG 導入には、簡易 IP ユーザ（従来の ISG と WiFi）およびモバイル IP ユーザ（GTP トンネリングおよび PMIPv6）の組み合わせが含まれます。*モビリティ サービス*という用語は、ユーザ トラフィックに適用される GTP サービスまたは PMIPv6 サービスを指すために使用されます。iWAG はモバイル IP ユーザにモビリティ サービスを提供し、その結果、モバイル クライアントがシームレスに 3G または 4G モビリティ ネットワークにアクセスできます。iWAG は簡易 IP ユーザにモビリティ サービスを提供しません。したがって、簡易 IP ユーザは Cisco ISG を介してパブリック ワイヤレス LAN（PWLAN）ネットワークにアクセスできます。クライアントは、可能な場合、WiFi インターネット（パブリック ワイヤレス）にアクセスするデバイスです。ただし、WiFi が使用できない場合、同じクライアントが 3G または 4G モビリティ ネットワークを使用してインターネットに接続します。

iWAG には、シスコの ISG 加入者認識を備えた転送またはスイッチング要素があります。iWAG には、WiFi のホールセール モデルに対する RADIUS ベースの認証およびアカウンティング、およびポリシーベースの加入者ルーティングがあります。

図 1 に、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでの iWAG の導入モデルを示します。

図 1　　Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでの iWAG の導入



iWAG の GTP の制約事項

次の制約事項が iWAG 機能の GTP に適用されます。

- 3G モビリティ ネットワークから WLAN へのローミングは、GTP と Cisco ISG セッションではサポートされていません。
- IPv6 および Quality of Service（QoS）はサポートされません。
- 新しく確立されたコールのみが WLAN 第 3 世代パートナーシップ プロジェクト（3GPP）IP アクセスにオフロードされます。
- WLAN オフロードのための iWAG ソリューションは、現在 3G Universal Mobile Telecommunications System（UMTS）のみで使用でき、4G Long Term Evolution（LTE）では使用できません。

IP アドレスの割り当てに関する情報

GTP トンネル上の GGSN は、サービス プロバイダー ドメインに基づいて、各加入者に一意の IP アドレスを割り当てます。単一の IP アドレス割り当て（非 NAT）の場合、アクセスが WLAN であるため、次のホスト設定パラメータを Microsoft クライアント用にプロビジョニングする必要があります：

- デフォルト ゲートウェイ
- サブネット マスクとプレフィックス長
- ドメイン ネーム システム（DNS）サーバ アドレス

- ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）サーバ アドレス

認証方式に関する情報

認証とは、ネットワークおよびサービスへのアクセスを許可する前にユーザを識別する方法です。iWAG は次の認証方式をサポートしています。

- 802.1x 認証（Extensible Authentication Protocol Method for GSM Subscriber Identity Module（EAP-SIM））および Extensible Authentication Protocol Method for Authentication and Key Agreement(EAP-AKA)
- Web 認証
- Media Access Control-Transparent Auto Logon（MAC-TAL）認証

802.1X 認証

802.1x 認証方式は、信頼できる WiFi ネットワークで使用されます。この方式では、Microsoft クライアントは、使用するための IP アドレスが割り当てられる前に認証されます。

Web 認証

Web 認証方式は、信頼できない WiFi ネットワークで使用されます。この方式では、Microsoft クライアントは、使用するための IP アドレスが割り当てられた後に認証されます。

iWAG は、対応する GGSN にクライアント セッションをトンネリングする前に認証を完了するため、Open Garden ポリシーと L4 リダイレクトを適用するために、Cisco ISG 機能を使用します。

MAC-TAL 認証

MAC-TAL 認証方式は Web 認証方式に関連付けられており、Microsoft クライアントは、あるアクセス ポイントから別のアクセス ポイントへ移動し再接続するときに再認証を試行しますが、クライアントを認証した AAA サーバはクライアントの過去の結果のレコードを保持しています。このため、このような再接続が発生した場合、iWAG は、発信ステーション ID としてクライアントの MAC アドレスを使用した、再認証のための Access Accept メッセージを受け取ります。

GGSN 選択に関する情報

GTP は、Microsoft クライアントの Packet Data Protocol（PDP）コンテキストを作成しなければならない場合、PDP コンテキスト作成要求を送信する GGSN を識別する必要があります。ユーザ プロファイルには通常、アクセス ポイント名（APN）と GGSN アドレスのいずれかまたはその両方が設定されます。これらのどちらもない場合、ボックスごとにデフォルトの GGSN アドレスが iWAG で設定されます。

GGSN 選択アルゴリズムは、GGSN を識別するために、次の手順を実行します。

1. GGSN アドレスがユーザ プロファイルで設定されている場合、アドレスに最も高いプライオリティが設定され、使用のために選択されます。

   GGSN アドレスがなく、APN がユーザ プロファイルに存在する場合は、APN が使用のために選択されます。GTP は、この名前をアドレスまたはアドレスのリスト（DNS サーバがロード バランシングを実行する場合）に解決するために、このボックスに設定されている DNS サーバに DNS クエリーを送信します。返信としてアドレスのリストを受信した場合、GTP はこのリスト全体を記録し、新しい PDP コンテキストの確立時にこのリストからのラウンドロビン割り当てを実行します。

両方の GGSN アドレスも APN もない場合、デフォルトの GGSN アドレスが使用されます。

2. GGSN アドレスが選択されると、選択した GGSN に到達可能でない可能性があります。GGSN へのアクセスのために許可された試行数だけ失敗すると、GGSN は停止していると見なされます。このようなシナリオでは、高い優先順位または低い優先順位を持つ別の GGSN とのさらなる再試行は実行されません。Microsoft クライアントの PDP コンテキストが単に確立に失敗します。この GGSN アドレスが DNS 解決の結果である場合、この APN の GGSN アドレス リストのエントリは、APN を使用するする処理が再度実行されないように削除されます。

iWAG の認証、許可、カウンティング方法

ここでは、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの iWAG の認証、認可、アカウンティング（AAA）を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *group-name*
5. **server-private** *ip-address* **[auth-port** *port-number* **| acct-port** *port-number***] [non-standard] [timeout** *seconds***] [retransmit** *retries***] [key** *string***]**
6. **aaa authentication login {default |** *list-name***} {[passwd-expiry]** *method1* **[***method2***...]}**
7. **aaa authorization network** *authorization-name* **group** *server-group name*
8. **aaa authorization subscriber-service {default {cache | group | local} |** *list-name***}** *method1* **[***method2***...]**
9. **aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default |** *list-name***} [vrf** *vrf-name***] {start-stop | stop-only | none} [broadcast] group** *group-name*
10. **action-type {none | start-stop | stop-only}**
11. **group {tacacs+ server-group}**
12. **aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default |** *list-name***} [vrf** *vrf-name***] {start-stop | stop-only | none} [broadcast] group** *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	**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 group server radius** *group-name* **例：** Router(config)# **aaa group server radius** AAA_SERVER_CAR	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。
ステップ 5	**server-private ip-address [auth-port** *port-number* **| acct-port** *port-number***] [non-standard] [timeout** *seconds***] [retransmit** *retries***] [key** *string***]** **例：** Router(config-sg-radius)# **server-private** 5.3.1.76 **auth-port** 2145 **acct-port** 2146 **key** cisco	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。
ステップ 6	**aaa authentication login {default | list-name} {[passwd-expiry] method1 [method2...]}** **例：** Router(config-sg-radius)# **aaa authentication login default** none	ログイン時の AAA 認証を設定します。
ステップ 7	**aaa authorization network** *authorization-name* **group** *server-group name* **例：** Router(config)# **aaa authorization network** ISG_PROXY_LIST **group** AAA_SERVER_CAR	シリアル ライン インターネット プロトコル（SLIP）、ポイントツーポイント プロトコル（PPP）、PPP ネットワーク コントロール プログラム（NCP）、AppleTalk Remote Access（ARA）など、すべてのネットワーク関連サービス要求について許可を実行します。
ステップ 8	**aaa authorization subscriber-service {default {cache | group | local} |** *list-name***} method1 [method2...]** **例：** Router(config)# **aaa authorization subscriber-service default local group** AAA_SERVER_CAR	Cisco ISG が加入者サービスを提供するための 1 つ以上の AAA 認可方法を指定します。

	コマンドまたはアクション	目的
ステップ 9	**aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default | *list-name*} [vrf *vrf-name*] {start-stop | stop-only | none} [broadcast] group** *group-name* **例：** `Router(config)# aaa accounting network PROXY_TO_CAR`	RADIUS または TACACS+ を使用する場合の課金およびセキュリティのために、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 10	**action-type {none | start-stop | stop-only}** **例：** `Router(cfg-acct-mlist)# action-type start-stop`	アカウンティング レコードに対して実行されるアクションのタイプをイネーブルにします。
ステップ 11	**group {tacacs+ server-group}** **例：** `Router(cfg-preauth)# group AAA_SERVER_CAR`	事前認証に使用する AAA TACACS+ サーバ グループを指定します。
ステップ 12	**aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default | *list-name*} [vrf *vrf-name*] {start-stop | stop-only | none} [broadcast] group** *group-name* **例：** `Router(config)# aaa accounting network ISG_PROXY_LIST start-stop group AAA_SERVER_CAR`	課金および RADIUS や TACACS+ を使用する際のセキュリティのために、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。

iWAG が DHCP プロキシとして動作している場合の DHCP の設定方法

ここでは iWAG がダイナミック ホスト コンフィギュレーション プロトコル（DHCP）プロキシとして動作するときに、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの iWAG のダイナミック ホスト コンフィギュレーション プロトコル（DHCP）を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp excluded-address [vrf** *vrf-name***]** *ip-address* **[***last-ip-address***]**
4. **ip dhcp pool** *pool-name*
5. **network** *network-number* **[***mask* **[secondary]** | */prefix-length* **[secondary]**
6. **default-router** *ip-address*
7. **domain-name** *domain*
8. **lease {***days* **[***hours* **[***minutes***]] | infinite}**

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 excluded-address [vrf** *vrf-name***]** *ip-address* **例：** Router(config)# **ip dhcp excluded-address** 192.168.10.1	DHCP サーバが DHCP クライアントに割り当てない IP アドレスを指定します。
ステップ 4	**ip dhcp pool** *pool-name* **例：** Router(config)# **ip dhcp pool** test	DHCP サーバに対し DHCP アドレス プールを設定し、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 5	**network** *network-number* **[***mask* **[secondary] |** */prefix-length* **[secondary]** **例：** Router(dhcp-config)# **network** 192.168.0.0 255.255.0.0	Cisco IOS DHCP サーバ上の DHCP アドレス プールのプライマリ サブネットまたは DHCP アドレス プールのセカンダリ 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 6	default-router *ip-address* [*last-ip-address*] **例：** Router(dhcp-config)# **default-router** 192.168.10.1	DHCP クライアントでデフォルト ルータ リストを指定します。
ステップ 7	**domain-name** *domain* **例：** Router(dhcp-config)# **domain-name** starent.com	DHCP クライアントのドメイン名を指定します。
ステップ 8	**lease {***days* **[***hours* **[***minutes***]] | infinite}** **例：** Router(dhcp-config)# **lease 1 2 2**	Cisco IOS DHCP サーバから DHCP クライアントに割り当てられる IP アドレスのリース期間を設定します。

iWAG 用 Cisco ISG クラス マップおよびポリシー マップの設定方法

ここでは iWAG 用 Cisco ISG クラス マップおよびポリシー マップを設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type traffic match-any** *class-map-name*
4. **match access-group output {access-group | name** *access-group-name***}**
5. **match access-group input {access-group | name** *access-group-name***}**
6. **policy-map type service** *policy-map-name*
7. **[***priority***] class type traffic {***class-map-name* **| default {in-out | input | output}}**
8. **accounting aaa list** *aaa-method-list*
9. **[***priority***] class type traffic {***class-map-name* **| default {in-out | input | output}}**
10. **drop**
11. **policy-map type control** *policy-map-name*
12. **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}]**
13. **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}}**
14. **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***]**

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	**class-map type traffic match-any** *class-map-name* **例：** Router(config)# **class-map type traffic match-any** TC_OPENGARDEN	パケットを指定された Cisco 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 output {access-group | name** *access-group-name***}** **例：** Router(config-traffic-classmap)# **match access-group output name** ACL_OUT_OPENGARDEN	指定したアクセス コントロール リスト（ACL）に基づいて、Cisco ISG トラフィック クラス マップの一致基準を設定します。
ステップ 5	**match access-group input {access-group | name** *access-group-name***}** **例：** Router(config-traffic-classmap)# **match access-group input name** ACL_IN_OPENGARDEN	指定した ACL に基づいて、Cisco ISG トラフィック クラス マップの一致基準を設定します。
ステップ 6	**policy-map type service** *policy-map-name* **例：** Router(config)# **policy-map type service** OPENGARDEN_SERVICE	Cisco ISG 加入者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 7	**[***priority***] class type traffic {***class-map-name* **| default {in-out | input | output}}** **例：** Router(config-service-policymap)# 20 **class type traffic** TC_OPENGARDEN	パケットを指定された Cisco 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 8	**accounting aaa list** *aaa-method-list* **例：** Router(config-service-policymap)# **accounting aaa list** PROXY_TO_CAR	Cisco ISG アカウンティングをイネーブルにし、アカウンティング アップデートを転送する AAA メソッド リストを指定します。
ステップ 9	**[***priority***] class type traffic {***class-map-name* **| default {in-out | input | output}}** **例：** Router(config-service-policymap)# **class type traffic default in-out**	パケットを指定された Cisco 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 10	**drop** **例：** Router(config-service-policymap)# **drop**	Cisco ISG を、デフォルト トラフィック クラスに属するパケットを廃棄するように設定します。
ステップ 11	**policy-map type control** *policy-map-name* **例：** Router(config)# **policy-map type control** BB_PROFILE	Cisco ISG コントロール ポリシーを定義する制御ポリシー 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 12	**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 Cisco ISG 制御ポリシーで設定できる制御クラスを指定します。
ステップ 13	*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)**#** 10 **service-policy type service name** OPENGARDEN_SERVICE	Cisco ISG サービスをアクティブにします。
ステップ 14	*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)**#** 20 **authorize aaa list** ISG_PROXY_LIST **password** cisco **identifier** mac-address	Cisco ISG 制御ポリシーの指定された ID に基づいて許可の要求を開始します。

iWAG の加入者の発信側の設定方法

ここでは、iWAG の加入者の発信側を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface GigabitEthernet** *slot/subslot/port*
4. **description** *string*
5. **ip address** *ip-address mask* **[secondary [vrf** *vrf-name***]]**
6. **negotiation auto**
7. **service-policy type control** *policy-map-name*
8. **ip subscriber {l2-connected | routed}**
9. **initiator {dhcp [class-aware] | radius-proxy | static ip subscriber list** *listname* **| unclassified ip | unclassified mac}**
10. **initiator {dhcp [class-aware] | radius-proxy | static ip subscriber list** *listname* **| unclassified ip | unclassified mac}**

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 GigabitEthernet** *slot/subslot/port* **例：** `Router(config)# interface GigabitEthernet 1/3/3`	ギガビット イーサネットのインターフェイス 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	**description string** **例：** `Router(config-if)# description access interface connected to subscriber`	インターフェイスの設定に説明を加えます。
ステップ 5	**ip address** *ip-address mask* **[secondary [vrf** *vrf-name*]] **例：** `Router(config-if)# ip address 192.171.10.1 255.255.0.0`	インターフェイスのプライマリ 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 6	**negotiation auto** **例：** `Router(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスでの自動ネゴシエーションをイネーブルにします。
ステップ 7	**service-policy type control** *policy-map-name* **例：** `Router(config-if)# service-policy type control BB_Profile`	制御ポリシーをコンテキストに適用します。
ステップ 8	**ip subscriber {l2-connected | routed}** **例：** `Router(config-if)# ip subscriber l2-connected`	インターフェイス上で Cisco ISG IP 加入者のサポートをイネーブルにし、IP 加入者がインターフェイス上で Cisco ISG を接続するために使用するアクセス方式を指定します。

	コマンドまたはアクション	目的
ステップ 9	**initiator {dhcp [class-aware] | radius-proxy | static ip subscriber list** *listname* **| unclassified ip | unclassified mac-address}** **例：** `Router(config-subscriber)# initiator unclassified mac-address`	指定されたタイプのパケットの受信時に IP 加入者セッションを作成するように Cisco ISG をイネーブルにします。
ステップ 10	**initiator {dhcp [class-aware] | radius-proxy | static ip subscriber list** *listname* **| unclassified ip | unclassified mac-address}** **例：** `Router(config-subscriber)# initiator dhcp`	指定されたタイプのパケットの受信時に IP 加入者セッションを作成するように Cisco ISG をイネーブルにします。

iWAG のトンネルの発信側の設定方法

ここでは、iWAG のトンネルの発信側を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface GigabitEthernet** *slot/subslot/port*
4. **description string**
5. **ip address** *ip-address mask* **[secondary [vrf** *vrf-name***]]**
6. **negotiation auto**

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 GigabitEthernet** *slot/subslot/port* **例：** `Router(config)# interface GigabitEthernet 1/3/5`	ギガビット イーサネット インターフェイスのインターフェイス 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 4	**description** *string* **例：** `Router(config-if)# description interface connected to GGSN`	インターフェイスの設定に説明を加えます。
ステップ 5	**ip address** *ip-address mask* **[secondary [vrf** *vrf-name*]] **例：** `Router(config-if)# ip address 192.170.10.1 255.255.0.0`	インターフェイスのプライマリ 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 6	**negotiation auto** **例：** `Router(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスでの自動ネゴシエーションをイネーブルにします。

モバイル クライアント サービスの抽象化とアクセス リストをイネーブルにする方法

ここでは、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータのモバイル クライアント サービス抽象化とアクセス リストをイネーブルにする方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mcsa**
4. **enable sessionmgr**
5. **ip access-list {{standard | extended}** {*access-list-name* | *access-list-number*} | **helper egress check}**
6. **permit ip any any**
7. **permit udp any any**
8. **ip access-list {{standard | extended}** {*access-list-name* | *access-list-number*} | **helper egress check}**
9. **permit ip any any**
10. **permit udp any any**

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	**mcsa** **例：** `Router(config)# mcsa`	Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上でモバイル クライアント サービスの抽象化をイネーブルにします。
ステップ 4	**enable sessionmgr** **例：** `Router(config-mcsa)# enable sessionmgr`	Cisco ISG からの通知を受信するように、モバイル クライアント サービスの抽象化をイネーブルにします。
ステップ 5	**ip access-list {{standard | extended} {***access-list-name* **|** *access-list-number***} | helper egress check}** **例：** `Router(config)# ip access-list extended ACL_IN_OPENGARDEN`	IP アクセス リストを名前または番号で定義するか、IP ヘルパー アドレスの宛先を持つパケットのフィルタリングをイネーブルにします。
ステップ 6	**permit ip any any** **例：** `Router(config-ext-nacl)# permit ip any any`	パケットが名前付き IP アクセス リストを通過できる条件を設定します。
ステップ 7	**permit udp any any** **例：** `Router(config-ext-nacl)# permit udp any any`	パケットが名前付き UDP アクセス リストを通過できる条件を設定します。
ステップ 8	**ip access-list {{standard | extended} {***access-list-name* **|** *access-list-number***} | helper egress check}** **例：** `Router(config)# ip access-list extended ACL_OUT_OPENGARDEN`	IP アクセス リストを名前または番号で定義するか、IP ヘルパーアドレスの宛先を持つパケットのフィルタリングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 9	**permit ip any any** **例：** `Router(config-ext-nacl)# permit ip any any`	パケットが名前付き IP アクセス リストを通過できる条件を設定します。
ステップ 10	**permit udp any any** **例：** `Router(config-ext-nacl)# permit udp any any`	パケットが名前付き UDP アクセス リストを通過できる条件を設定します。

iWAG の GTP の設定方法

ここでは、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの iWAG の GTP を設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **gtp**
4. **n3-request** *request-number*
5. **interval t3-response** *response-number*
6. **interval echo-request** *request-number*
7. **interface local GigabitEthernet** *slot/subslot/port*
8. **apn** *apn-name*
9. **ip address ggsn** *ip-address*
10. **default-gw** *address* **prefix-len** *value*
11. **dns-server** *ip-address*
12. **dhcp-server** *ip-address*
13. **dhcp-lease** *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	**gtp** **例：** `Router(config)# gtp`	Cisco ASR 1000 シリーズ アグリゲーション サービス ルータで iWAG の GTP を設定します。
ステップ 4	**n3-request** *request-number* **例：** `Router(config-gtp)# n3-request 3`	iWAG のサービング GPRS サポート ノード（SGSN）が要求に応答する待ち時間を秒単位で指定します。デフォルト値は、1 です
ステップ 5	**interval t3-response** *response-number* **例：** `Router(config-gtp)# interval t3-response 10`	障害が送信される前に、制御メッセージを再試行する回数を指定します。デフォルト値は 5 です。
ステップ 6	**interval echo-request** *request-number* **例：** `Router(config-gtp)# interval echo-request 60`	iWAG の SGSN がエコー要求メッセージを送信する前に待機する時間（秒）を指定します。範囲は 60 ～ 65535 です。デフォルト値は 60 です。値 0 はエコー要求機能をディセーブルにします。
ステップ 7	**interface local GigabitEthernet** *slot/subslot/port* **例：** `Router(config-gtp)# interface local GigabitEthernet 0/0/3`	転送インターフェイスを GGSN と通信するように設定します。
ステップ 8	**apn** *apn-name* **例：** `Router(config-gtp)# apn starent.com`	汎用パケット無線サービス（GPRS）ロード バランシングの APN とマッチングする ASCII 正規表現ストリングを設定します。
ステップ 9	**ip address ggsn** *ip-address* **例：** `Router(config-gtp-apn)# ip address ggsn 192.170.10.2`	GGSN の IP アドレスを設定します。
ステップ 10	**default-gw** *address* **prefix-len** *value* **例：** `Router(config-gtp-apn)# default-gw 192.171.10.1 prefix-len 16`	加入者のデフォルト ゲートウェイ アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 11	**dns-server** *ip-address* **例：** `Router(config-gtp-apn)# dns-server 192.165.1.1`	DHCP クライアントで使用可能なドメイン ネーム システム（DNS）IP サーバを指定します。
ステップ 12	**dhcp-server** *ip-address* **例：** `Router(config-gtp-apn)# dhcp-server 192.168.10.1`	特定のパブリック データ ネットワーク（PDN）アクセス ポイントを入力したモバイル ステーション ユーザに対して IP アドレスを割り当てるためのプライマリおよびバックアップ DHCP サーバを指定します。
ステップ 13	**dhcp-lease** *seconds* **例：** `Router(config-gtp-apn)# dhcp-lease 3000`	Cisco IOS DHCP サーバから DHCP クライアントに割り当てられる IP アドレスのリース期間を設定します。

iWAG の設定例

ここでは、次の設定例について説明します。

- 「例：TAL 認証方式を使用した iWAG の設定」（P.21）
- 「例：EAP-SIM 認証方式を使用した iWAG の設定」（P.23）
- 「例：Web ログオン認証方式を使用した iWAG の設定」（P.25）

例：TAL 認証方式を使用した iWAG の設定

次に、TAL 認証方式を使用して iWAG を設定する例を示します。

```
aaa new-model
!
!
aaa group server radius AAA_SERVER_CAR
server-private 5.3.1.76 auth-port 2145 acct-port 2146 key cisco
!
aaa authentication login default none
aaa authorization network ISG_PROXY_LIST group AAA_SERVER_CAR
aaa authorization subscriber-service default local group AAA_SERVER_CAR
aaa accounting network PROXY_TO_CAR
action-type start-stop
group AAA_SERVER_CAR
!
aaa accounting network ISG_PROXY_LIST start-stop group AAA_SERVER_CAR
!
!
!
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.10.2
ip dhcp excluded-address 192.168.10.3
!
ip dhcp pool TEST
network 192.168.0.0 255.255.0.0
default-router 192.168.10.1
    domain-name starent.com
lease 1 2 2
```

```
!
class-map type traffic match-any TC_OPENGARDEN
match access-group output name ACL_OUT_OPENGARDEN
match access-group input name ACL_IN_OPENGARDEN
!
policy-map type service OPENGARDEN_SERVICE
20 class type traffic TC_OPENGARDEN
    accounting aaa list PROXY_TO_CAR
!
class type traffic default in-out
    drop
!
!
policy-map type control BB_PROFILE
class type control always event session-start
    10 service-policy type service name OPENGARDEN_SERVICE
    20 authorize aaa list ISG_PROXY_LIST password cisco identifier mac-address
 !
!
interface GigabitEthernet1/3/3
descriptions interface connected to LS-IP APP Node
ip address 192.171.10.1 255.255.0.0
negotiation auto
service-policy type control BB_PROFILE
ip subscriber l2-connected
    initiator unclassified mac-address
    initiator dhcp
!
interface GigabitEthernet1/3/5
descriptions connected to LS-GGSN
ip address 192.170.10.1 255.255.0.0
negotiation auto
!
mcsa
enable sessionmgr
!
!
ip access-list extended ACL_IN_OPENGARDEN
permit ip any any
permit udp any any
ip access-list extended ACL_OUT_OPENGARDEN
permit ip any any
permit udp any any
!
!
gtp
n3-request 3
interval t3-response 10
interval echo-request 60
interface local GigabitEthernet0/0/3
apn 1
    apn-name starent.com
    ip address ggsn 192.170.10.2
    default-gw 192.168.10.1 prefix-len 16
    dns-server 192.165.1.1
    dhcp-server 192.168.10.1
    dhcp-lease 30000
!
End
```

例：EAP-SIM 認証方式を使用した iWAG の設定

次に、RADIUS プロキシ発信側を使用し、Extensible Authentication Protocol Method for GSM Subscriber Identity Module（EAP-SIM）認証方式を使用して iWAG を設定する例を示します。

```
aaa new-model
!
!
aaa group server radius AAA_SERVER_CAR
server-private 192.171.10.2 auth-port 1812 acct-port 1813 key cisco
!
aaa authentication login default none
aaa authorization subscriber-service default local group AAA_SERVER_CAR
aaa authorization radius-proxy ISG_PROXY_LIST group AAA_SERVER_CAR
aaa accounting delay-start
aaa accounting network default start-stop group AAA_SERVER_CAR
aaa accounting network PROXY_TO_CAR
action-type start-stop
group AAA_SERVER_CAR
!
aaa accounting network ISG_ACCOUNTING_LIST start-stop group AAA_SERVER_CAR
!
!
aaa server radius proxy
key cisco
calling-station-id format mac-address
authentication port 1812
re-authentication do-not-apply
accounting method-list PROXY_TO_CAR
accounting port 1813
timer ip-address 43200
timer request 43200
timer reconnect 43200
client 192.168.10.3 255.255.255.255
  !
!
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.10.2
ip dhcp excluded-address 192.168.10.3
!
ip dhcp pool TEST
network 192.168.0.0 255.255.0.0
default-router 192.168.10.1
    domain-name starent.com
lease 1 2 2
!
!
class-map type traffic match-any TC_OPENGARDEN
match access-group output name ACL_OUT_OPENGARDEN
match access-group input name ACL_IN_OPENGARDEN
!
policy-map type service OPENGARDEN_SERVICE
20 class type traffic TC_OPENGARDEN
    accounting aaa list ISG_ACCOUNTING_LIST
!
!
policy-map type control BB_PROFILE
class type control always event session-start
    1 proxy aaa list ISG_PROXY_LIST
    20 service-policy type service name OPENGARDEN_SERVICE
!
!
interface GigabitEthernet1/3/3
```

```
description connected to subscriber
    ip address 192.171.10.1 255.255.0.0
negotiation auto
service-policy type control BB_PROFILE
ip subscriber l2-connected
    initiator dhcp
    initiator radius-proxy
!
interface GigabitEthernet1/3/4
description interface connected to AAA server
ip address 192.171.10.1 255.255.0.0
negotiation auto
!
interface GigabitEthernet1/3/5
description connected to GGSN
ip address 192.170.10.1 255.255.0.0
negotiation auto
!
!
mcsa
enable sessionmgr
!
ip access-list extended ACL_IN_OPENGARDEN
permit ip any any
permit udp any any
ip access-list extended ACL_OUT_OPENGARDEN
permit ip any any
permit udp any any
!
radius-server attribute 44 include-in-access-req default-vrf
radius-server attribute 44 extend-with-addr
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req
radius-server attribute 32 include-in-accounting-req
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
radius-server attribute 31 send nas-port-detail
radius-server source-ports extended
radius-server throttle accounting 50
radius-server unique-ident 49
radius-server vsa send accounting
radius-server vsa send authentication
!
!
gtp
n3-request 3
interval t3-response 10
interval echo-request 60
information-element rat-type wlan
interface local GigabitEthernet0/0/3
apn 1
    apn-name starent.com
    ip address ggsn 192.170.10.2
    default-gw 192.168.10.1 prefix-len 16
    dns-server 192.165.1.1
    dhcp-server 192.168.10.1
!
End
```

例：Web ログオン認証方式を使用した iWAG の設定

次に、Web ログオン認証方式を使用して iWAG を設定する例を示します。

```
aaa new-model
!
!
aaa group server radius AAA_SERVER_CAR
server-private 5.3.1.76 auth-port 2145 acct-port 2146 key cisco
!
aaa authentication login default none
aaa authentication login ISG_PROXY_LIST group AAA_SERVER_CAR
aaa authorization network ISG_PROXY_LIST group AAA_SERVER_CAR
aaa authorization subscriber-service default local group AAA_SERVER_CAR
aaa accounting network PROXY_TO_CAR
action-type start-stop
group AAA_SERVER_CAR
!
aaa accounting network ISG_PROXY_LIST start-stop group AAA_SERVER_CAR
!
aaa server radius dynamic-author
client 5.3.1.76 server-key cisco
auth-type any
ignore server-key
!
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.10.2
ip dhcp excluded-address 192.168.10.3
!
ip dhcp pool TEST
network 192.168.0.0 255.255.0.0
default-router 192.168.10.1
    domain-name starent.com
lease 1 2 2
!
!
redirect server-group REDIRECT-SERVER-GROUP1
server ip 5.3.1.76 port 10080
!
!
ip tftp source-interface GigabitEthernet0
class-map type traffic match-any TC_L4R_class
match access-group input name TC_L4R
!
class-map type traffic match-any TC_OPENGARDEN
match access-group output name ACL_OUT_OPENGARDEN
match access-group input name ACL_IN_OPENGARDEN
!
policy-map type service OPENGARDEN_SERVICE
20 class type traffic TC_OPENGARDEN
    accounting aaa list PROXY_TO_CAR
!
class type traffic default in-out
    drop
!
!
policy-map type service L4Redirect_service
10 class type traffic TC_L4R_class
    redirect to group REDIRECT-SERVER-GROUP1
!
!
policy-map type control BB_PROFILE
class type control always event session-start
```

```
    10 service-policy type service name L4Redirect_service
    20 service-policy type service name OPENGARDEN_SERVICE
!
class type control always event account-logon
    10 authenticate aaa list ISG_PROXY_LIST
    20 service-policy type service unapply name L4Redirect_service
!
!
interface GigabitEthernet1/3/3
description interface connected to subscriber
ip address 192.171.10.1 255.255.0.0
negotiation auto
service-policy type control BB_PROFILE
ip subscriber l2-connected
    initiator unclassified mac-address
    initiator dhcp
!
!
interface GigabitEthernet1/3/5
descriptions interface connected to GGSN
ip address 192.170.10.1 255.255.0.0
negotiation auto
!
!
mcsa
enable sessionmgr
!
!
ip access-list extended ACL_IN_OPENGARDEN
permit ip any any
permit udp any any
ip access-list extended ACL_OUT_OPENGARDEN
permit ip any any
permit udp any any
ip access-list extended TC_L4R
permit udp any any
permit tcp any any
!
!
radius-server attribute 44 include-in-access-req default-vrf
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req
radius-server attribute 32 include-in-accounting-req
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
no radius-server attribute nas-port
radius-server source-ports extended
radius-server unique-ident 73
!
gtp
n3-request 3
interval t3-response 10
interval echo-request 60
information-element rat-type wlan
interface local GigabitEthernet 0/0/3
apn 1
    apn-name starent.com
    ip address ggsn 192.170.10.2
    default-gw 192.168.10.1 prefix-len 16
    dns-server 192.165.1.1
    dhcp-server 192.168.10.1
    dhcp-lease 30000
!
End
```

その他の関連資料

ここでは、iWAG 機能に関する参考資料について説明します。

関連資料

関連項目	参照先
Cisco IOS コマンド	*『Cisco IOS Master Commands List, All Releases』*
『Intelligent Services Gateway Configuration Guide, Cisco IOS XE Release 3S』	*http://www.cisco.com/en/US/docs/ios-xml/ios/isg/configuration/xe-3s/isg-xe-3s-book.html*
Cisco IOS 設定の基礎	*『Cisco IOS Configuration Fundamentals Command Reference』*

標準

標準	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。	—

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに対する MIB を特定してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC[1]	タイトル
RFC 5213	『Proxy Mobile IPv6』

1. サポートされている RFC をすべて紹介しているわけではありません。

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

サービス プロバイダーの WiFi オフロードのための、Cisco ASR 1000 シリーズ ルータでの iWAG の機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。この表には、Cisco IOS Release 3.8.0S 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。

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、対応するコマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する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 および Cisco Catalyst オペレーティング システムのソフトウェア イメージでサポートしている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。

表 1　Cisco ASR 1000 シリーズ アグリゲーション サービス ルータで iWAG の機能情報

機能名	リリース	機能情報
サービス プロバイダーの WiFi オフロードのための、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでの iWAG	3.8.0S	iWAG の導入には、Cisco GGSN に接続するための GTP と、Cisco PGW に接続するための PMIPv6 を使用した MAG の、2 種類の主要なテクノロジーが関係します。これら 2 つテクノロジーの Cisco ISG との統合と、サービス プロバイダー WiFi の組み合わせは、iWAG 機能の重要な概念です。 Cisco IOS XE Release 3.8.0S では、この機能が Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/