使用例のシナリオ

この章では、さまざまな条件で一般的なシステム動作と RADIUS 対話を監視するために使用可能な使用例のシナリオの例を示します。最初の使用例では、すべての RADIUS メッセージのデバッグが表示されます。他の使用例では、すべてのメッセージ フローがリストされていますが、対象の RADIUS デバッグだけが表示されます。

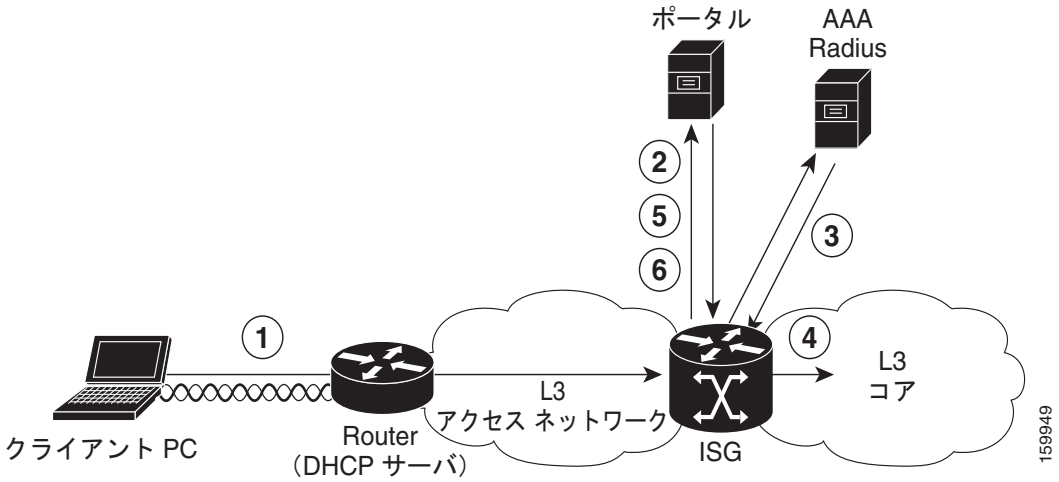
この章では、次の事項について説明します。

使用例 1：ポータル ログイン

この使用例は PWLAN アプリケーションで使用されている典型的なパブリック アクセス コントロールです。このシナリオでは、IP 加入者は IP アドレスを取得し、L3 アクセス ネットワーク上で ISG にルーティングされます。ISG は認証のためにポータルに加入者をリダイレクトし、RADIUS に保存された加入者プロファイルに従ってサービスをアクティブ化します。図 1 に示すアーキテクチャを想定しています。この例では、各番号付き項目は、図 1 の番号に対応しています。

1. ユーザ セッションが新しい IP 送信元アドレスの検出時に作成されます。一部のデフォルト サービスが適用されます。
2. ISG は、ユーザをポータルにリダイレクトします。ユーザは自分のユーザ名とパスワードを入力し、ユーザ クレデンシャルは、ISG に送信されます。
3. ユーザは AAA サーバで認証され、どの機能およびサービスを新しく作成されたセッションに適用するかを指定するユーザ プロファイルが RADIUS から取得されます。
4. ユーザはネットワークにアクセスできます。
5. しばらくすると、ユーザはポータルに戻り、より多くの帯域幅を取得するようにサービスを変更します。新しいポリシング パラメータが CoA によってポータルからプッシュされます。
6. しばらくすると、ユーザはポータルから切断され、セッションが終了します。

図 1　　ポータル ログイン ルーティング図



ISG の設定

ISG アクセス インターフェイスは「ルーテッド」として設定され、次の例に示すように、新しい IP アドレスに基づいて新しいセッションを識別するように設定されます。

```
interface GigabitEthernet0/0.10
  encapsulation dot1Q 10
  ip address 10.1.1.1 255.255.255.0
  service-policy type control RULE_IP_SESSION1
  ip subscriber routed
     initiator unclassified ip-address
```

この使用例の ISG 制御ポリシーを次の例に示します。

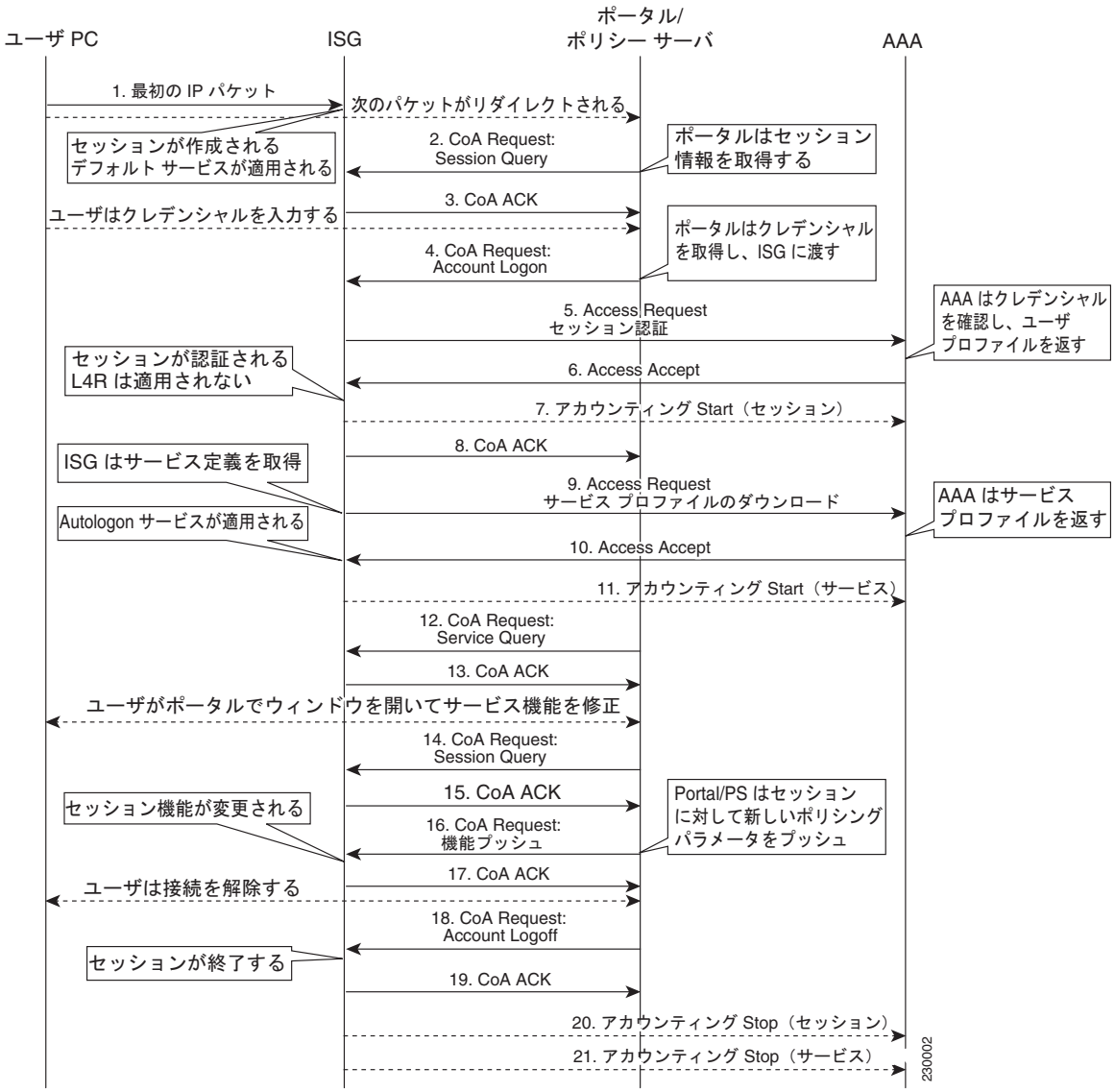
```
policy-map type control RULE_IP_SESSION1
 class type control IP_UNAUTH_COND event timed-policy-expiry
  1 service disconnect
 !
 class type control always event session-start
  10 service-policy type service name PBHK_SERVICE
  20 service-policy type service name L4REDIRECT_SERVICE
  30 service-policy type service name OPENGARDEN_SERVICE
  40 set-timer IP_UNAUTH_TIMER 10
 !

 class type control always event account-logon
  10 authenticate aaa list WEB_LOGON
  20 service-policy type service unapply name L4REDIRECT_SERVICE
 !
!
```

使用例 1：コール フロー

図 2 に、使用例 1 のシーケンス図を示します。各番号付き項目の詳細については、使用例 1：詳細を参照してください。

図 2　　使用例のシーケンス図



使用例 1：詳細

次の各番号付き項目は、図 2 の番号に対応しています。

1. ISG インターフェイスを、新しいセッションとして個々の IP アドレスを識別するように設定します。

```
ip subscriber routed
identifier unclassified ip-address
```

新しいセッションの開始時に、デフォルト サービス（この場合、PBHK、L4-redirect、および Open_Garden）を適用するよう ISG を設定します。これらのサービスは、（この使用例で想定されているように）ISG にローカルに定義することも、外部 AAA サーバに定義することもできます。

```
class type control always event session-start
10  service-policy type service name PBHK_SERVICE
20  service-policy type service name L4REDIRECT_SERVICE
30  service-policy type service name OPEN_GARDEN_SERVICE
```

2. CoA Session Query によるポータル要求セッション情報。これはセッション ID として PBHK ID を使用します。

```
RADIUS: COA  received from id 4 192.168.1.100:32777, CoA Request, len 54
COA: 192.168.1.100 request queued
RADIUS:  authenticator 8C 21 98 CF BF 15 D8 61 - EA A9 2C C5 2D C6 AF BF
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"           PBHK identifier

RADIUS:  Vendor, Cisco       [26]  11
RADIUS:   ssg-command-code   [252] 5
RADIUS:   04 20 26               [Account-Ping  &]
```

3. ISG は、CoA ACK で応答します。対象の情報には、クライアントの IP アドレス、またはセッションの状態（この場合は「unautenticated」）が含まれます。

```
RADIUS(00000027): Send CoA Ack Response to 192.168.1.100:32777 id 4, len 118
RADIUS:  authenticator 04 18 EA 0B A4 77 37 32 - 56 60 F7 31 CD 26 86 01
RADIUS:  Vendor, Cisco       [26]  10
RADIUS:   ssg-command-code   [252] 4
RADIUS:   04 30                 [Account-Ping 0]    "0" means session is not
authenticated
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"        PBHK identifier
RADIUS:  Vendor, Cisco       [26]  22
RADIUS:   Cisco AVpair       [1]   16  "sg-version=1.0"
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  31  "nas-port:10.10.10.11:0/0/1/70"
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2             Client's IP address
```

4. PS は、ユーザのユーザ名およびパスワードを含む CoA Account Logon を発行します。ISG は、このイベントのセッションを認証するように設定されています。認証が成功した場合にだけリダイレクト サービスを削除する 2 番目のアクションが実行されることに注意してください。

```
class type control always event account-logon
   10 authenticate aaa list IP_AUTHEN_LIST
   20 service-policy type service unapply name L4REDIRECT_SERVICE

RADIUS: COA  received from id 5 192.168.1.100:32777, CoA Request, len 84
COA: 192.168.1.100 request queued
RADIUS:  authenticator BF 62 14 C1 6F DE 76 61 - 84 D8 D5 01 14 F8 52 80
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Vendor, Cisco       [26]  15
```

```
RADIUS:   ssg-command-code   [252] 9
RADIUS:   01 49 50 5F 55 43 31            [Account-Log-On IP_UC1]
```

5. ISG が Accept Request を発行して AAA でセッションを認証します。要求には、クライアントのユーザ名とパスワードが含まれます。

```
Send Access-Request to 192.168.1.100:1812 id 1645/16, len 115
RADIUS:  authenticator F4 2C 9B 48 FF 83 A7 5A - 0F 5C 83 FE 5C E8 DE C0
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Login                     [1]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Acct-Session-Id     [44]  10  "00000032"
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Event-Timestamp     [55]  6   1159320597
```

6. クレデンシャルの確認に成功すると、AAA はアクティブ化するサービスがリストされたユーザ プロファイルを含む Access Accept で応答します。認証に成功したため、L4-redirect サービスは適用されません（セッションの制御ポリシーのアクション 20）。

```
RADIUS: Received from id 1645/16 192.168.1.100:1812, Access-Accept, len 193
RADIUS:  authenticator CA E9 E3 20 57 05 06 01 - AD FF F7 86 07 43 33 73
RADIUS:  Reply-Message       [18]  16
RADIUS:   57 65 6C 63 6F 6D 65 20 54 6F 20 49 53 47    [ Welcome To ISG]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-account-info   [250] 23  "AINTERNET_SERVICE_UC1"
RADIUS:  Vendor, Cisco       [26]  25
RADIUS:   ssg-account-info   [250] 19  "NCOA_BOD_1Meg_UC1"
RADIUS:  Idle-Timeout        [28]  6   300
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Vendor, Cisco       [26]  40
RADIUS:   ssg-account-info   [250] 34  "QU;512000;256000;D;512000;256000"
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "subscriber:accounting-list=BH_ACCNT_LIST1"
```

7. ISG はアカウンティング サーバにアカウンティング メッセージを送信して、セッションの開始を通知します。

```
RADIUS(00000027): Send Accounting-Request to 192.168.1.100:1813 id 1646/203, len
180
RADIUS:  authenticator 23 80 8E 14 C7 0F 00 BD - 05 3E 5D 73 D9 84 D3 6A
RADIUS:  Acct-Session-Id     [44]  10  "00000032"
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Vendor, Cisco       [26]  32
RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Unsupported         [151] 10
RADIUS:   42 44 42 39 32 42 45 43         [ BDB92BEC]
RADIUS:  Event-Timestamp     [55]  6   1159320597
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Acct-Delay-Time     [41]  6   0
```

8. ISG は、CoA ACK で PS に応答してアカウント ログオンの成功を通知し、加入者情報および加入者サービス情報を含めます。

```
RADIUS(00000027): Send CoA Ack Response to 192.168.1.100:32777 id 5, len 220
RADIUS:  authenticator C2 9C AB 02 5F 97 DA 2F - E3 B1 F6 E0 4D 7B 9A 77
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-command-code   [252] 9
RADIUS:   01 49 50 5F 55 43 31            [Account-Log-On IP_UC1]
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Reply-Message       [18]  16
RADIUS:   57 65 6C 63 6F 6D 65 20 54 6F 20 49 53 47    [ Welcome To ISG]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-account-info   [250] 23  "AINTERNET_SERVICE_UC1"
RADIUS:  Vendor, Cisco       [26]  25
RADIUS:   ssg-account-info   [250] 19  "NCOA_BOD_1Meg_UC1"
RADIUS:  Idle-Timeout        [28]  6   300
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Vendor, Cisco       [26]  40
RADIUS:   ssg-account-info   [250] 34  "QU;512000;256000;D;512000;256000"
RADIUS:  Vendor, Cisco       [26]  38
RADIUS:   Cisco AVpair       [1]   32  "accounting-list=BH_ACCNT_LIST1"
```

9. セッションに対してアクティブ化するサービスがまだ ISG にキャッシュされていないと仮定して、ISG は AAA に Access Request を送信してサービス定義をダウンロードします。

```
RADIUS(00000027): Send Access-Request to 192.168.1.100:1812 id 1645/17, len 117
RADIUS:  authenticator 6F 50 DA 86 D4 77 5A B1 - 2E 7E 18 AD 68 2B 6F B8
RADIUS:  User-Name           [1]   22  "INTERNET_SERVICE_UC1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Outbound                  [5]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Acct-Session-Id     [44]  10  "00000032"
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Event-Timestamp     [55]  6   1159320597
```

10. サーバはサービス定義（サービス プロファイル）で応答し、ISG はセッションにサービスを適用します。

```
RADIUS: Received from id 1645/17 192.168.1.100:1812, Access-Accept, len 312
RADIUS:  authenticator 28 44 E2 8C DC 5B 8B 3B - 8B 5F 0F 2F 7C D4 4C 71
RADIUS:  Vendor, Cisco       [26]  40
RADIUS:   Cisco AVpair       [1]   34  "ip:traffic-class=in default drop"
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "subscriber:accounting-list=BH_ACCNT_LIST1"
RADIUS:  Vendor, Cisco       [26]  80
RADIUS:   Cisco AVpair       [1]   74  "ip:traffic-class=input access-group name
ACL_IN_INTERNET_UC1 priority 30"
RADIUS:  Vendor, Cisco       [26]  82
RADIUS:   Cisco AVpair       [1]   76  "ip:traffic-class=output access-group name
ACL_OUT_INTERNET_UC1 priority 30"
RADIUS:  Vendor, Cisco       [26]  41
RADIUS:   Cisco AVpair       [1]   35  "ip:traffic-class=out default drop"
```

11. ISG は、BASIC_INTERNET_SERVICE_UC1 のアカウンティング メッセージを送信してサービス開始を通知します。サービスの accounting-ID が parent-session-id 属性によってセッションに関連付けられます。

```
RADIUS(00000027): Send Accounting-Request to 192.168.1.100:1813 id 1646/204, len
205
RADIUS:  authenticator D3 EE 5E 20 AB D1 9A 2A - A8 7B C4 12 BA 78 29 39
```

```
RADIUS:  Acct-Session-Id     [44]  10  "00000033"
RADIUS:  Framed-Protocol     [7]   6   PPP                        [1]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "NINTERNET_SERVICE_UC1"
RADIUS:  Vendor, Cisco       [26]  34
RADIUS:   Cisco AVpair       [1]   28  "parent-session-id=00000032"
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Acct-Status-Type    [40]  6   Start                      [1]
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  NAS-Port-Type       [61]  6   Virtual                    [5]
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Framed                     [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Unsupported         [151] 10
RADIUS:   42 44 42 39 32 42 45 43          [ BDB92BEC]
RADIUS:  Event-Timestamp     [55]  6   1159320597
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Acct-Delay-Time     [41]  6   0
```

12. Portal/PS は自動ログオン サービスが「CoA Session Query for Service Status」を使用して正常にアクティブ化されたかどうかを確認するために ISG に照会します。

```
RADIUS: COA  received from id 8 192.168.1.100:32777, CoA Request, len 72
COA: 192.168.1.100 request queued
RADIUS:  authenticator B6 C5 2C D4 AB CB 3E CD - 9D 91 E9 7D 45 B8 AF 88
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-command-code   [252] 23
RADIUS:   04 49 4E 54 45 52 4E 45 54 5F 53 45 52 56 49 43 45  [INTERNET_SERVICE]
RADIUS:   5F 55 43 31              [Account-Ping _UC1]
```

13. ISG はセッションのサービス情報を Portal/PS に返します。

```
RADIUS(00000027): Send CoA Ack Response to 192.168.1.100:32777 id 8, len 151
RADIUS:  authenticator 67 44 50 B7 D6 89 4A 0A - 23 C9 4E 3A E1 5F A6 4C
RADIUS:  Vendor, Cisco       [26]  39
RADIUS:   ssg-account-info   [250] 33  "N1INTERNET_SERVICE_UC1;6;IP_UC1"
RADIUS:  Vendor, Cisco       [26]  10
RADIUS:   ssg-command-code   [252] 4
RADIUS:   04 31                 [Account-Ping 1]
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  22
RADIUS:   Cisco AVpair       [1]   16  "sg-version=1.0"
RADIUS:  NAS-Port-Id         [87]  31  "nas-port:10.10.10.11:0/0/1/70"
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
```

14. ユーザがポータルで新しいウィンドウを開くと、Portal/PS がセッション情報を必要とする可能性があり、情報の取得に CoA Account Query を使用します。

```
RADIUS: COA  received from id 10 192.168.1.100:32777, CoA Request, len 54
COA: 192.168.1.100 request queued
RADIUS:  authenticator F6 CD 8A 1A 2E 99 B2 B6 - 98 1A 81 70 C2 F5 15 42
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  11
RADIUS:   ssg-command-code   [252] 5
RADIUS:   04 20 26               [Account-Ping  &]
```

15. ISG は、セッションおよびサービス情報で応答します。

```
RADIUS(00000027): Send CoA Ack Response to 192.168.1.100:32777 id 10, len 444
RADIUS:  authenticator E7 64 D2 F5 96 E0 76 2D - D1 AD ED 79 F7 2E 99 C9
RADIUS:  Vendor, Cisco       [26]  60
RADIUS:   ssg-account-info   [250] 54
"N1OPENGARDEN_SERVICE;277;IP_UC1;139;179;24236;213422"
RADIUS:  Vendor, Cisco       [26]  48
RADIUS:   ssg-account-info   [250] 42  "N1INTERNET_SERVICE_UC1;96;IP_UC1;0;0;0;0"
RADIUS:  Vendor, Cisco       [26]  54
RADIUS:   ssg-account-info   [250] 48
"N1PBHK_SERVICE;277;IP_UC1;139;179;24236;213422"
RADIUS:  Vendor, Cisco       [26]  10
RADIUS:   ssg-command-code   [252] 4
RADIUS:   04 31                 [Account-Ping 1]
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Reply-Message       [18]  16
RADIUS:   57 65 6C 63 6F 6D 65 20 54 6F 20 49 53 47    [ Welcome To ISG]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-account-info   [250] 23  "AINTERNET_SERVICE_UC1"
RADIUS:  Vendor, Cisco       [26]  25
RADIUS:   ssg-account-info   [250] 19  "NCOA_BOD_1Meg_UC1"
RADIUS:  Idle-Timeout        [28]  6   300
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Vendor, Cisco       [26]  40
RADIUS:   ssg-account-info   [250] 34  "QU;512000;256000;D;512000;256000"
RADIUS:  Vendor, Cisco       [26]  38
RADIUS:   Cisco AVpair       [1]   32  "accounting-list=BH_ACCNT_LIST1"
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  22
RADIUS:   Cisco AVpair       [1]   16  "sg-version=1.0"
RADIUS:  NAS-Port-Id         [87]  31  "nas-port:10.10.10.11:0/0/1/70"
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
```

16. ユーザがポータルからサービス機能を変更します。PS は CoA 機能プッシュを使用して機能を変更します。この場合、ポリシング レートは 1024K になり、アイドル タイムアウトは 2000 秒に変更されます。

```
RADIUS: COA  received from id 16 192.168.1.100:32777, CoA Request, len 77
COA: 192.168.1.100 request queued
RADIUS:  authenticator C4 14 F5 2F FF BE 68 4D - 60 8E AA 49 7D AA 2C 4F
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  28
RADIUS:   ssg-service-info   [251] 22  "QU;1024000;D;1024000"
RADIUS:  Idle-Timeout        [28]  6   2000
```

17. ISG は、機能が変更されたことを確認します。

```
RADIUS(00000000): Send CoA Ack Response to 192.168.1.100:32777 id 16, len 26
RADIUS:  authenticator 53 5E 5D 13 AF 1A 1C 53 - 75 CD FF 3B C9 01 D5 4C
RADIUS:  Dynamic-Author-Error[101] 6   Success
```

18. ユーザはポータルとの接続を解除します（ログオフします）。Portal/PS は CoA Request: Account Logoff を送信してセッションを終了します。

```
RADIUS: COA  received from id 18 192.168.1.100:32777, CoA Request, len 58
COA: 192.168.1.100 request queued
RADIUS:  authenticator 5B 9E A9 CA EA 1A C2 AC - 1B 4A 89 40 E2 ED E9 F2
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-command-code   [252] 9
RADIUS:   02 49 50 5F 55 43 31            [Account-Log-Off IP_UC1]
```

19. ISG は、CoA ACK で応答します。

```
RADIUS(00000027): Send CoA Ack Response to 192.168.1.100:32777 id 18, len 52
RADIUS:  authenticator D2 D8 A2 19 19 FD E6 C3 - BA 9D 70 5D 58 F6 0A 85
RADIUS:  Vendor, Cisco       [26]  9
RADIUS:   ssg-command-code   [252] 3
RADIUS:   02
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
```

20. ISG はセッションがアカウンティング Stop を使用して終了したことを通知します。

```
RADIUS(00000027): Send Accounting-Request to 192.168.1.100:1813 id 1646/205, len
251
RADIUS:  authenticator 90 CB DD 33 73 11 0A 24 - A3 22 F1 08 83 E5 40 9A
RADIUS:  Acct-Session-Id     [44]  10  "00000032"
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
RADIUS:  Vendor, Cisco       [26]  32
RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
RADIUS:  Acct-Session-Time   [46]  6   197
RADIUS:  Acct-Input-Octets   [42]  6   88902
RADIUS:  Acct-Output-Octets  [43]  6   752244
RADIUS:  Acct-Input-Packets  [47]  6   476
RADIUS:  Acct-Output-Packets [48]  6   621
RADIUS:  Acct-Terminate-Cause[49]  6   user-request              [1]
RADIUS:  Vendor, Cisco       [26]  35
RADIUS:   Cisco AVpair       [1]   29  "disc-cause-ext=TS User Exit"
RADIUS:  Acct-Status-Type    [40]  6   Stop                      [2]
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Unsupported         [151] 10
RADIUS:   42 44 42 39 32 42 45 43         [ BDB92BEC]
RADIUS:  Event-Timestamp     [55]  6   1159320794
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Acct-Delay-Time     [41]  6   0
```

21. ISG はサービスがアカウンティング Stop を使用して終了したことを通知します。

```
RADIUS(00000027): Send Accounting-Request to 192.168.1.100:1813 id 1646/206, len
247
RADIUS:  authenticator 6E 86 93 CD 6A 60 D8 43 - 57 2F B6 9B 84 98 87 AA
RADIUS:  Acct-Session-Id     [44]  10  "00000033"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "NINTERNET_SERVICE_UC1"
RADIUS:  Vendor, Cisco       [26]  34
RADIUS:   Cisco AVpair       [1]   28  "parent-session-id=00000032"
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Acct-Input-Packets  [47]  6   46
RADIUS:  Acct-Output-Packets [48]  6   59
RADIUS:  Acct-Input-Octets   [42]  6   9764
RADIUS:  Acct-Output-Octets  [43]  6   12622
RADIUS:  Acct-Session-Time   [46]  6   197
RADIUS:  Acct-Terminate-Cause[49]  6   user-request              [1]
RADIUS:  Vendor, Cisco       [26]  35
RADIUS:   Cisco AVpair       [1]   29  "disc-cause-ext=TS User Exit"
RADIUS:  Acct-Status-Type    [40]  6   Stop                      [2]
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
```

```
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Unsupported         [151] 10
RADIUS:   42 44 42 39 32 42 45 43          [ BDB92BEC]
RADIUS:  Event-Timestamp     [55]  6   1159320794
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Acct-Delay-Time     [41]  6   0
```

使用例 2：Transparent Auto-Logon

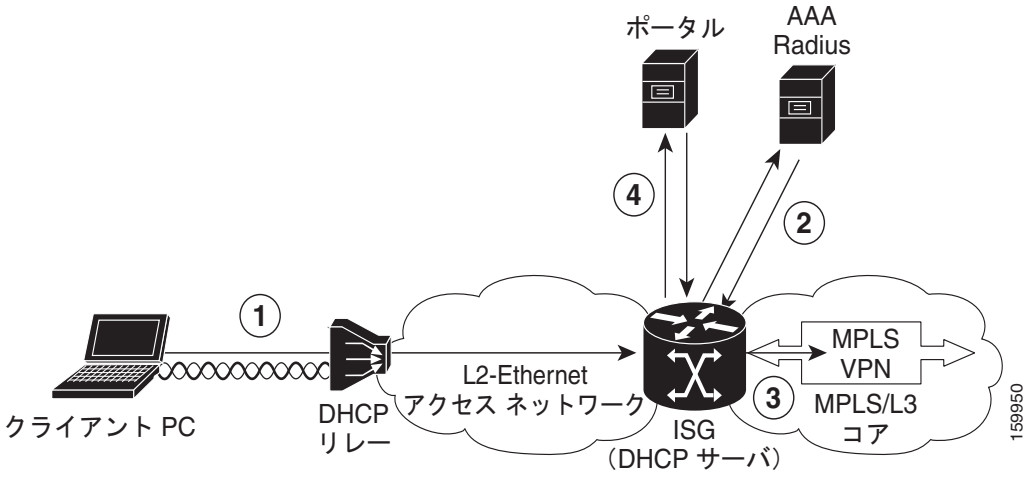
Transparent Auto-Logon（TAL）機能は「サービスへの常時アクセス」の提供を可能にします。つまり、セッションはネットワーク ID に基づいて認可され、アクセスのために加入者認証は必要ありません。

この使用例は、多くの IP セッションが BRAS の単一の VLAN 上で集約される典型的なブロードバンド レジデンシャル アクセスです。PPP と同様のサービスを実現するには、サービス プロバイダーは、DHCP Option-82 フィールドに DSLAM によって入力されるロケーション情報に基づいてエンド ユーザを識別します。

図 3 に、この使用例で使用されるアーキテクチャを示します。この例では、次の各番号付き項目は、図 3 の番号に対応しています。

1. ユーザ セッションが新しい DHCP 対話の検出時に作成されます（ISG は DHCP サーバまたはリレー）。ダウンストリーム スイッチまたは DSLAM によって加入者の物理的なロケーションが DHCP Option 82 に入力されることを前提とします。
2. ユーザは自分の MAC アドレス + DHCP Option 82 情報に基づいて AAA サーバで許可されます。AAA サーバはユーザを許可し、セッションに適用される機能およびサービスがリストされたユーザ プロファイルを返します。サービスの 1 つは、vrf-id と DHCP クラスを含むプライマリ サービスで、VRF 経由でルーティング可能な IP アドレスが割り当てられるようにします。
3. ユーザは、MPLS VPN 経由で自分のサービスにアクセスできます。
4. しばらくすると、ユーザはポータルにアクセスし、帯域幅が増加する「turbo-button」タイプのサービスに加入します。さらにしばらくすると、ユーザはポータルにアクセスし、「turbo-button」タイプのサービスを非アクティブ化して通常のサービスに戻ります。

図 3　　Transparent Auto-Logon ルーティング図



ISG の設定

ここでは、次の内容について説明します。

- 「インターフェイス コンフィギュレーション」（P.2-39）
- 「制御ポリシー設定」（P.2-39）
- 「ポリシー制御クラスマップ」（P.2-39）

- 「DHCP プール」（P.2-40）

インターフェイス コンフィギュレーション

インターフェイス コンフィギュレーションの例を次に示します。

```
!!! Interface Configuration

interface GigabitEthernet0/1.22
 encapsulation dot1Q 22
 ip address 10.3.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_IP_SESSION2a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
```

制御ポリシー設定

制御ポリシー設定の例を次に示します。

```
!!! Control Policy Configuration

policy-map type control RULE_IP_SESSION2a
 class type control IP_UNAUTH_COND event timed-policy-expiry
  10 service disconnect
 !
 class type control BOD1M_CLASS event service-start
  10 service-policy type service unapply name DEFAULT_BW_512K_UC2
  20 service-policy type service identifier service-name
 !
 class type control BOD1M_CLASS event service-stop
  10 service-policy type service unapply identifier service-name
  20 service-policy type service name DEFAULT_BW_512K_UC2
 !
 class type control always event session-start
  10 service-policy type service name PBHK_SERVICE
  20 service-policy type service name OPENGARDEN_SERVICE2
  30 authorize aaa list AUTHOR_LIST1 password cisco123 identifier remote-id plus
circuit-id plus mac-address
  40 service-policy type service name L4REDIRECT_SERVICE2
  50 set-timer IP_UNAUTH_TIMER 5
 !
 class type control always event account-logon
  10 authenticate aaa list AUTHEN_LIST1
  20 service-policy type service unapply name L4REDIRECT_SERVICE2
 !
!
```

ポリシー制御クラスマップ

```
An example of the Policy Control Class-Map configuration is shown below:
!!! Policy Control class-map

class-map type control match-all BOD1M_CLASS
 match service-name BOD1M_SERVICE_UC2
!
class-map type control match-all IP_UNAUTH_COND
 match timer IP_UNAUTH_TIMER
 match authen-status unauthenticated
```

```
!
```

DHCP プール

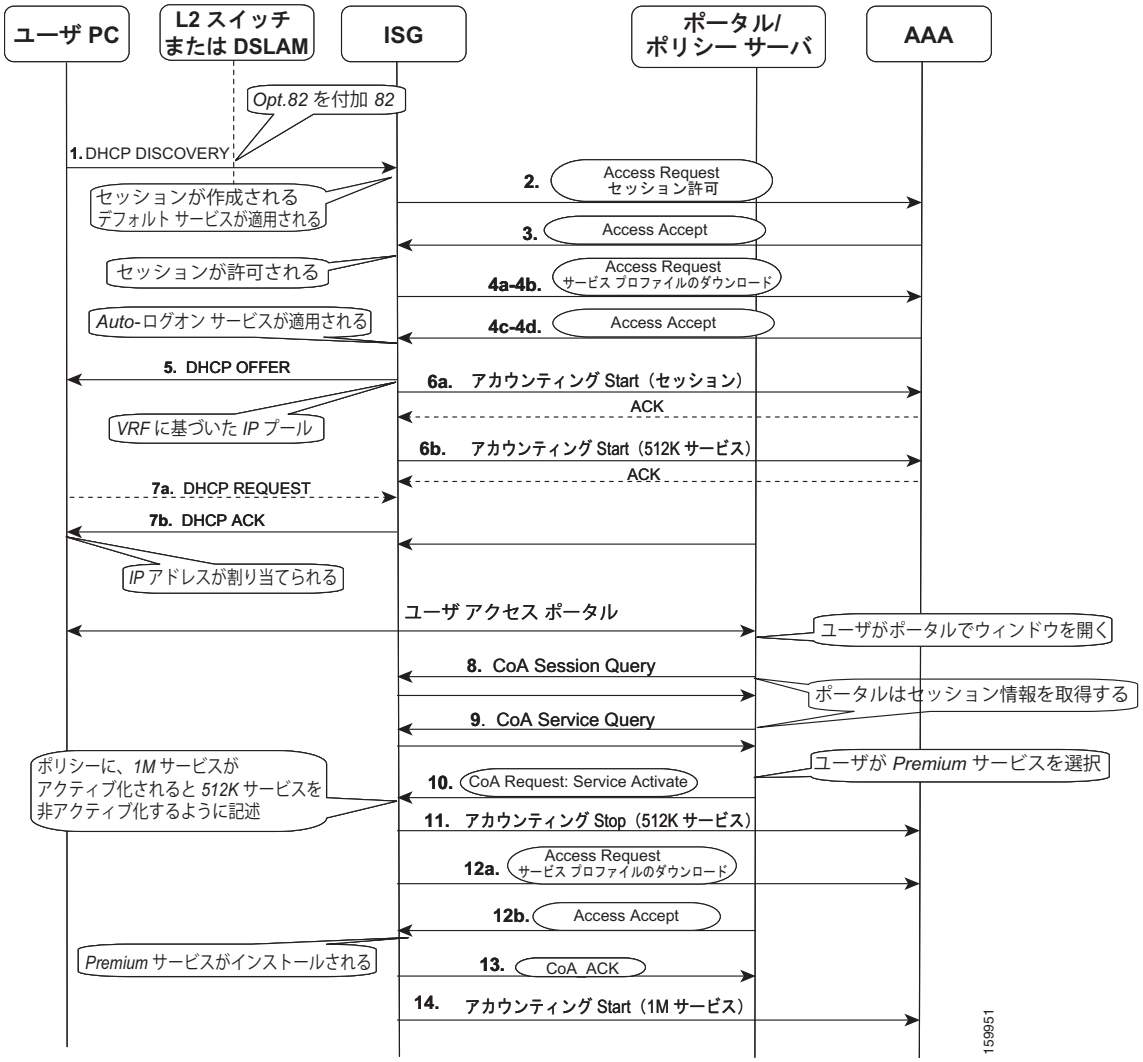
DHCP プール設定の例を次に示します。

```
!!! DHCP POOLS..
ip dhcp excluded-address 10.3.10.1
ip dhcp excluded-address 10.3.11.1
!
ip dhcp pool VPN_UC2_POOL1
   vrf VPN_ISP1
   network 10.3.11.0 255.255.255.0
   default-router 10.3.11.1
   domain-name isgtest.com
   class CLASS1
!
ip dhcp pool DHCP_POOL1
   network 10.3.10.0 255.255.255.0
   default-router 10.3.10.1
   lease 0 0 30
   class default
!
ip dhcp class CLASS1
Ip dhcp class default
!
```

使用例 2：コール フロー

図 4 に、使用例 2 のシーケンス図を示します。各番号付き項目の詳細については、使用例 2：詳細を参照してください。

図 4　　使用例 2 のシーケンス図



使用例 2：詳細

各番号付き項目は、図 4 の番号に対応しています。

1. DHCP DISCOVERY メッセージは加入者によって開始されます。中間デバイス（DSLAM またはスイッチ）が DHCP Option 82 情報を入力して、加入者の物理的なロケーションを特定することを前提とします。ISG インターフェイスを、DHCP 制御トラフィックに対して新しいセッションを開始するように設定します。

   新しいセッションで、デフォルト サービス（この場合 PBHK）を適用し、MAC アドレスおよび DHCP Option 82 情報に基づいてセッションを許可するように ISG を設定します。

2. ISG は Accept Request を発行して、AAA でセッションを許可します。Accept Request には、ユーザ名として MAC アドレスおよび Option 82 情報が含まれており、ポリシーで定義したパスワードが使用されます。この例では、「cisco」が使用されます。

```
Send Access-Request to 192.168.1.100:1812 id 1645/149, len 244
RADIUS:  authenticator A8 6C 11 8C C3 60 7F 67 - 21 C1 07 89 ED 12 2B E9
RADIUS:  User-Name           [1]   47  "0|6|000d.edc0.3f80:0|4|22|1|15:0050.5607.0103"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  Vendor, Cisco       [26]  34
RADIUS:   Cisco AVpair       [1]   28  "circuit-id-tag=0|4|22|1|15"
RADIUS:  Vendor, Cisco       [26]  40
RADIUS:   Cisco AVpair       [1]   34  "remote-id-tag=0|6|000d.edc0.3f80"
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  32  "0|6|000d.edc0.3f80:0|4|22|1|15"
RADIUS:  Service-Type        [6]   6   Outbound                  [5]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Acct-Session-Id     [44]  10  "00000381"
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Event-Timestamp     [55]  6   1159560540
```

3. アイデンティティの確認に成功すると、AAA はユーザ プロファイルおよびアクティブ化するサービスを含む Access Accept で応答します。この例では、「DEFAULT_BW_512K_UC2」および「VPN1_UC2」が使用されます。

```
Received from id 1645/149 192.168.1.100:1812, Access-Accept, len 173
RADIUS:  authenticator AF 6C 9C AB 5A D4 F2 E3 - A4 25 BD 89 96 8F 17 93
RADIUS:  Vendor, Cisco       [26]  28
RADIUS:   ssg-account-info   [250] 22  "ADEFAULT_BW_512K_UC2"
RADIUS:  Vendor, Cisco       [26]  17
RADIUS:   ssg-account-info   [250] 11  "AVPN1_UC2"
RADIUS:  Reply-Message       [18]  16
RADIUS:   57 65 6C 63 6F 6D 65 20 54 6F 20 49 53 47    [ Welcome To ISG]
RADIUS:  Vendor, Cisco       [26]  26
RADIUS:   ssg-account-info   [250] 20  "NBOD1M_SERVICE_UC2"
RADIUS:  Session-Timeout     [27]  6   180000
RADIUS:  User-Name           [1]   47   "
0|6|000d.edc0.3f80:0|4|22|1|15:0050.5607.0103 "
RADIUS:  Idle-Timeout        [28]  6   600
RADIUS:  Vendor, Cisco       [26]  46
RADIUS:   Cisco AVpair       [1]   40  "subscriber:accounting-list=ACCNT_LIST1"
```

4. **4a-4b**. サービスが ISG にキャッシュされていないため、ISG はこれらを AAA から取得する必要があります。

   4c-4d. 両方のサービスの定義が取得され、サービスが適用されます。次の例は、AAA サーバに表示されるサービス定義です。

```
Service Name = "VPN1_UC2"
 CiscoAVPair: ip:vrf-id=VPN_ISP1
```

```
 CiscoAVPair: subscriber:classname=CLASS1
 CiscoAVPair: subscriber:sg-service-type=primary

Service Name = "DEFAULT_BW_512K_UC2"
 CiscoAVPair: ip:traffic-class=output access-group name ACL_OUT_DEFAULT_BW priority 50
 SERVICE INFO: QU;512000;256000;D;512000;256000
 CiscoAVPair: subscriber:accounting-list=ACCNT_LIST1
 CiscoAVPair: ip:traffic-class=input access-group name ACL_IN_DEFAULT_BW priority 50
```

5. ISG はカスタマーによって割り当てられた VRF 内でルーティング可能である DHCP クラスに基づいて IP アドレスを提供します。
6. **6a-6b**. アカウンティング要求がユーザ セッションの開始を通知するために送信され、別のアカウンティング要求がサービス開始を通知するために送信されます。
7. **7a-7b**. ユーザ要求、提供されたアドレス、およびアドレスは、ISG によって配布されます。
8. **8a-9b**. しばらくすると、ユーザがポータルにサイン インすることを前提とします。Portal/PS は 1 つ以上の CoA Request:Account Query を発行して、加入者情報とサービス ステータスを取得します。ISG は加入者情報および加入者サービス情報を含む CoA ACK で Portal/PS に応答します。
9. **9a-9b**. これらの手順では、前の手順と同様にサービス クエリーを処理します。
10. ユーザが新しいサービス「BOD1M_SERVICE_UC2」を選択したと仮定して、Portal/PS は新しいサービス名を含む CoA Request:Service Activate メッセージを発行します。

```
RADIUS: COA  received from id 131 192.168.1.100:32777, CoA Request, len 70
Sep 29 20:14:08.456: COA: 192.168.1.100 request queued
Sep 29 20:14:08.456: RADIUS:  authenticator 12 01 8B 5A 1E 69 13 18 - 05 C2 AC 26 EE
00 E2 3B
Sep 29 20:14:08.456: RADIUS:  Vendor, Cisco       [26]  24
Sep 29 20:14:08.456: RADIUS:   ssg-account-info   [250] 18  "S10.10.10.11:110"
Sep 29 20:14:08.456: RADIUS:  Vendor, Cisco       [26]  26
Sep 29 20:14:08.456: RADIUS:   ssg-command-code   [252] 20
RADIUS:   0B 42 4F 44 31 4D 5F 53 45 52 56 49 43 45 5F 55 43  [BOD1M_SERVICE_UC]
RADIUS:   32                [Service-Log-On 2]
```

11. 制御ポリシーは、1M サービスがアクティブ化されると、512K サービスを切断するように指定します。512K サービスを切断すると、ISG は 512K サービスのサービス停止を通知するアカウンティング要求を送信します。
12. **12a-12b**. 1M サービスの定義が ISG にまだキャッシュされていないという前提があるため、ISG は AAA から 1M サービスの定義を取得する必要があります。AAA におけるサービス定義の例を次に示します。

```
Service Name = "BOD1M_SERVICE_UC2"
CiscoAVPair: ip:traffic-class=in default drop
CiscoAVPair: ip:traffic-class=output access-group name ACL_OUT_BOD1M priority 30
SERVICE INFO: QU;1024000;512000;D;1024000;512000
CiscoAVPair: ip:traffic-class=input access-group name ACL_IN_BOD1M priority 30
CiscoAVPair: subscriber:accounting-list=ACCNT_LIST1
CiscoAVPair: ip:traffic-class=out default drop
```

13. ISG は、1M サービスがインストールされたことを確認します。
14. ISG は、1M サービスが開始されたことを通知するアカウンティング要求を送信します。

使用例 3：サービス認証

この使用例では、ユーザがこのサービスにアクセスする前に、アプリケーション サーバでサービス認証が必要です。サービス プロファイルが ISG によって取得されると、指定されたサーバで追加認証が必要であると（ポリシー ディレクティブ VSA 内で）確認されます。その場合、ユーザ プロファイル内で取得されたユーザ名とパスワードがサービスへのログオンに使用されます。図 5 に、サービス認証のシーケンス図を示します。

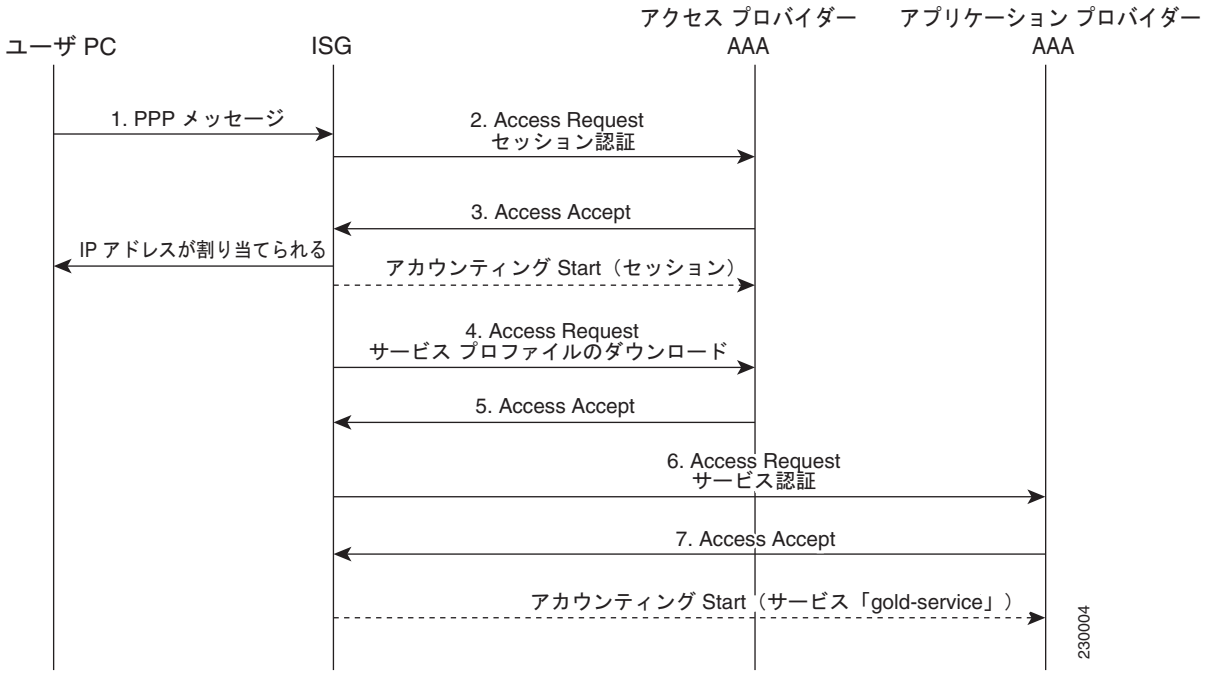
この例では、次のようになります。

- PPP ユーザ セッションが PPP 制御トラフィックの検出時に作成されます。
- ユーザは、AAA サーバで許可されます。
- ユーザ プロファイルには、認証を必要とする autologon サービスが含まれています。
- ISG はアクセスを許可する前にサービスを認証します。

使用例 3：詳細なコール フロー

図 5 に、使用例 2 のシーケンス図を示します。各番号付き項目の詳細については、使用例 3：詳細を参照してください。

図 5　　サービス認証のシーケンス図



使用例 3：詳細

各番号付き項目は、図 5 の番号に対応しています。

1. PPP 制御メッセージは加入者によって開始されます。PPP セッションの場合、PPP セッションが自動的に作成されるため、ISG インターフェイスを設定する必要はありません。この使用例では、セッションが認証を必要とすることを前提としています。この認証はコマンドを使用してイネーブルにします。

   ```
   ppp authentication chap PPP_LIST
   ```

2. ISG が Accept Request を発行して、ユーザのユーザ名とパスワードが含まれるアクセス プロバイダー AAA でセッションを認証します。
3. アイデンティティの確認に成功すると、AAA はユーザ プロファイルおよびアクティブ化するサービス（この場合、「goldservice」）を含む Access Accept で応答します。ユーザ プロファイルの Service Name VSA には、次のような追加のユーザ名とパスワードが含まれています。

   ```
   "Agoldservice;myusername;mypassword"
   ```

4. サービス「goldservice」が ISG にまだキャッシュされていないと仮定して、ISG は Access Request を AAA に送信してサービス定義をダウンロードします。
5. サーバは、サービス定義で応答します。サービス定義内に、特定のアプリケーション サーバでさらに認証が必要であることを示すポリシー ディレクティブ VSA があります。

   ```
   “policy-directive=authenticate aaa list auth-list”
   ```

6. ISG は、サービス認証のために指定サーバに対する Access-Request を開始します
7. クレデンシャルの確認に成功すると、アプリケーション サーバは Access-Accept で応答し、ユーザは自分のサービスにアクセスできます。