



# RADIUS アトリビュート概要と RADIUS IETF アトリビュート

Remote Authentication Dial-In User Service (RADIUS; リモート認証ダイヤルイン ユーザ サービス) アトリビュートは、RADIUS デーモンに保存されたユーザ プロファイル内の特定の Authentication, Authorization, and Accounting (AAA; 認証、認可、およびアカウントリング) 要素を定義するために使用されます。このモジュールでは、現在サポートされている RADIUS アトリビュートを列挙します。

## 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。このモジュールに記載された機能に関する情報を探したり、各機能がサポートされているリリースのリストを確認したりするには、[P. 20 の「RADIUS アトリビュートの概要と RADIUS IETF アトリビュートの機能情報」](#)を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp> からアクセスできます。Cisco.com のアカウントは必要ありません。

## この章の構成

- 「RADIUS アトリビュートに関する情報」 (P.1)
- 「RADIUS IETF アトリビュート」 (P.5)
- 「その他の参考資料」 (P.18)
- 「RADIUS アトリビュートの概要と RADIUS IETF アトリビュートの機能情報」 (P.20)

## RADIUS アトリビュートに関する情報

この項では、RADIUS アトリビュートがクライアントとサーバ間で AAA 情報をどのように交換するかを理解するうえで重要な情報について説明します。次の項で構成されています。

- [IETF アトリビュートと VSA の比較](#)
- [RADIUS パケットのフォーマット](#)
- [RADIUS ファイル](#)
- [サポートに関するドキュメント](#)

## IETF アトリビュートと VSA の比較

RADIUS Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) アトリビュートは、255 個の標準アトリビュートで構成されるオリジナルのセットで、クライアントとサーバ間での AAA 情報の伝達に使用されます。IETF アトリビュートは標準であるため、アトリビュートデータは事前定義されてその内容も認識されています。このため、IETF アトリビュートを介して AAA 情報を交換するすべてのクライアントとサーバは、アトリビュートの厳密な意味や各アトリビュート値の一般的な限界など、アトリビュートデータに一致させる必要があります。

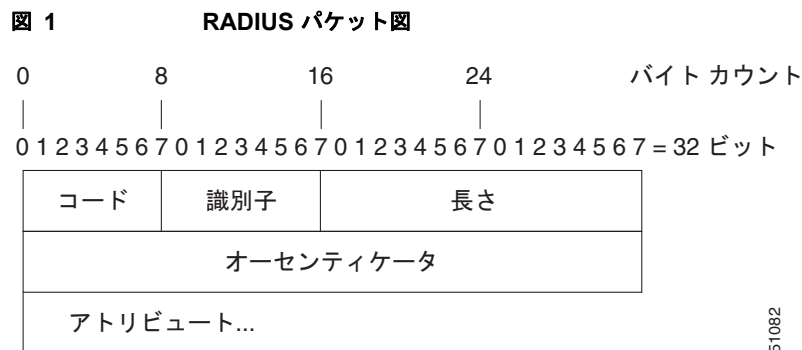
RADIUS Vendor-Specific Attribute (VSA; ベンダー固有アトリビュート) は、1 つの IETF アトリビュート (Vendor-Specific (アトリビュート 26)) から派生したものです。アトリビュート 26 を使用すれば、ベンダーは、追加の 255 個のアトリビュートを自由に作成できます。つまり、ベンダーは、どの IETF アトリビュートのデータとも一致しないアトリビュートを作成して、アトリビュート 26 の背後にカプセル化することができます。そのため、新しく作成されたアトリビュートは、アトリビュート 26 を受け入れているユーザに受け入れられます。

VSA の詳細については、「[関連資料](#)」(P.18) を参照してください。

## RADIUS パケットのフォーマット

RADIUS サーバと RADIUS クライアント間のデータは、RADIUS パケットで交換されます。データフィールドは左から右に転送されます。

図 1 に、RADIUS パケット内のフィールドを示します。



各 RADIUS パケットには、次の情報が含まれています。

- コード: コードフィールドは 1 オクテットです。次の RADIUS パケットのタイプを識別します。
  - Access-Request (1)
  - Access-Accept (2)
  - Access-Reject (3)
  - Accounting-Request (4)

- Accounting-Response (5)
  - 識別子：識別子フィールドは 1 オクテットです。RADIUS サーバの要求と応答の照合を支援し、重複した要求を検出します。
  - 長さ：長さフィールドは 2 オクテットです。パケット全体の長さを示します。
  - オーセンティケータ：オーセンティケータ フィールドは 16 オクテットです。最上位オクテットが最初に転送されます。RADIUS サーバからの応答の認証に使用されます。次の 2 種類のオーセンティケータがあります。
    - Request-Authentication：Access-Request パケットと Accounting-Request パケットで使用できます。
    - Response-Authenticator：Access-Accept、Access-Reject、Access-Challenge、および Accounting-Response パケットで使用できます。

## RADIUS パケット タイプ

次のリストは、アトリビュート情報を含めることが可能なさまざまなタイプの RADIUS パケットをまとめたものです。

**Access-Request**：クライアントから RADIUS サーバに送信されます。このパケットには、RADIUS サーバで、ユーザにアクセスを許可している特定の Network Access Server (NAS; ネットワーク アクセス サーバ) へのアクセスを許可するかどうかを判断可能な情報が含まれています。認証を実行しているユーザは、Access-Request パケットを提出する必要があります。Access-Request パケットを受信した RADIUS サーバは、応答を返す必要があります。

**Access-Accept**：Access-Request パケットを受信した RADIUS サーバは、Access-Request パケット内のすべてのアトリビュート値が受け入れ可能な場合に、Access-Accept パケットを送信する必要があります。Access-Accept パケットには、クライアントからユーザにサービスを提供するために必要な設定情報が含まれています。

**Access-Reject**：Access-Request パケットを受信した RADIUS サーバは、どのアトリビュート値も受け入れ可能でなかった場合に、Access-Reject パケットを送信する必要があります。

**Access-Challenge**：Access-Accept パケットを受信した RADIUS サーバは、応答が必要な Access-Challenge パケットをクライアントに送信できます。クライアントで応答の仕方がわからない場合、または、パケットが無効な場合は、RADIUS サーバがそのパケットを破棄します。クライアントがパケットに回答する場合は、オリジナルの Access-Request パケットと一緒に新しい Access-Request パケットを送信する必要があります。

**Accounting-Request**：クライアントから RADIUS アカウンティング サーバに送信され、アカウンティング情報を提供します。RADIUS サーバが正常に Accounting-Request パケットを記録したら、Accounting-Response パケットを提出する必要があります。

**Accounting-Response**：RADIUS アカウンティング サーバからクライアントに送信され、Accounting-Request が正常に受信および記録されたことが伝えられます。

## RADIUS ファイル

クライアントからサーバに AAA 情報を伝送するためには、RADIUS で使用されるファイルのタイプを理解しておくことが重要です。各ファイルでユーザの認証または認可レベルを定義します。ディレクトリ ファイルでは、ユーザの NAS に実装可能なアトリビュートを定義します。クライアント ファイルでは、RADIUS サーバへの要求が許可されたユーザを定義します。ユーザ ファイルでは、RADIUS サーバでセキュリティ データと設定データに基づいて認証されるユーザ要求を定義します。

- [ディレクトリ ファイル](#)

- クライアント ファイル
- ユーザ ファイル

## ディレクトリ ファイル

ディレクトリ ファイルには、NAS でサポートされているアトリビュートに依存するアトリビュートのリストが格納されています。ただし、独自のアトリビュートのセットをカスタム ソリューション用のディレクトリに追加できます。このファイルではアトリビュート値が定義されるため、構文解析要求などのアトリビュート出力を解釈できます。ディレクトリ ファイルには次の情報が含まれています。

- 名前：User-Name などのアトリビュートの ASCII 文字列「名」
- ID：アトリビュートの数値「名」。たとえば、User-Name アトリビュートはアトリビュート 1 です。
- 値型：アトリビュートは次の値型のいずれかとして指定できます。
  - abinary：0 ～ 254 オクテット
  - date：ビッグ エンディアン順の 32 ビット値。たとえば、1970 年 1 月 1 日 00:00:00 GMT 以降の秒数。
  - ipaddr：ネットワーク バイト順の 4 オクテット
  - integer：ビッグ エンディアン順の 32 ビット値（上位バイトが先）
  - string：0 ～ 253 オクテット

特定のアトリビュートのデータ型が整数の場合は、オプションで、整数を拡張して何らかの文字列と一致させることができます。次のサンプル辞書には、整数ベースのアトリビュートと対応する値が含まれています。

```
# dictionary sample of integer entry
#
ATTRIBUTE      Service-Type      6          integer
VALUE          Service-Type      Login      1
VALUE          Service-Type      Framed     2
VALUE          Service-Type      Callback-Login  3
VALUE          Service-Type      Callback-Framed  4
VALUE          Service-Type      Outbound   5
VALUE          Service-Type      Administrative  6
VALUE          Service-Type      NAS-Prompt  7
VALUE          Service-Type      Authenticate-Only  8
VALUE          Service-Type      Callback-NAS-Prompt  9
VALUE          Service-Type      Call-Check  10
VALUE          Service-Type      Callback-Administrative  11
```

## クライアント ファイル

クライアント ファイルは、RADIUS サーバへの認証要求とアカウント要求の送信を許可された RADIUS クライアントのリストが含まれている点で重要です。認証を受けるには、クライアントからサーバに送信された名前と認証キーがクライアント ファイル内のデータと一致する必要があります。

クライアント ファイルの例を次に示します。この例に示すキーは、**radius-server key SomeSecret** コマンドと同じにする必要があります。

```
#Client Name      Key
#-----
10.1.1.2.3:256    test
```

```
nas01          bananas
nas02          MoNkEys
nas07.foo.com  SomeSecret
```

## ユーザ ファイル

RADIUS ユーザ ファイルには、RADIUS サーバで認証されたユーザごとのエントリが含まれています。ユーザ プロファイルとも呼ばれるエントリごとに、そのユーザがアクセス可能なアトリビュートが設定されます。

ユーザ プロファイルの最初の行は、常に、「ユーザ アクセス」行です。つまり、サーバはユーザにアクセス許可を出す前に、最初の行のアトリビュートをチェックする必要があります。最初の行にはユーザの名前が含まれています。この名前は、最大 252 文字にすることができ、後ろにユーザのパスワードなどの認証情報が続きます。

ユーザ アクセス行に関連付けられたその他の行は、要求元のクライアントまたはサーバに送信されるアトリビュート応答を表します。応答内で送信されるアトリビュートは、ディレクトリ ファイルで定義する必要があります。

ユーザ ファイルを調べるときは、等号 (=) 文字の左側のデータがディレクトリ ファイルで定義されたアトリビュートで、等号文字の右側のデータが設定データであることに注意してください。



(注)

空白行はユーザ プロファイルのどの場所にも挿入できません。

RADIUS ユーザ プロファイル (Merit Daemon フォーマット) の例を次に示します。この例では、ユーザ名が `cisco.com`、パスワードが `cisco` で、ユーザは 5 つのトンネルアトリビュートにアクセスできます。

```
# This user profile includes RADIUS tunneling attributes
cisco.com Password="cisco" Service-Type=Outbound
  Tunnel-Type = :1:L2TP
  Tunnel-Medium-Type = :1:IP
  Tunnel-Server-Endpoint = :1:10.0.0.1
  Tunnel-Password = :1:"welcome"
  Tunnel-Assignment-ID = :1:"nas"
```

## RADIUS IETF アトリビュート



(注)

RADIUS トンネルアトリビュート用の Cisco IOS Release 12.2 では、32 個のタグ付きトンネルセットが L2TP 用にサポートされています。

ここでは、次の各手順について説明します。

- サポートされている [RADIUS IETF アトリビュート](#)
- [RADIUS アトリビュート解説の包括的リスト](#)

## サポートされている RADIUS IETF アトリビュート

表 1 に、シスコがサポートしている IETF RADIUS アトリビュートとそれらが実装されている Cisco IOS リリースを示します。アトリビュートがセキュリティ サーバ固有の形式の場合は、この形式が指定されます。

リスト内のアトリビュートの説明については、表 2 を参照してください。



(注)

特別な (AA) リリースまたは初期開発 (T) リリースで実装されたアトリビュートが次のメインラインイメージに追加されています。

表 1 サポートされている RADIUS IETF アトリビュート

番号	IETF アトリビュート	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
1	User-Name	yes	yes	yes	yes	yes	yes	yes	yes
2	User-Password	yes	yes	yes	yes	yes	yes	yes	yes
3	CHAP-Password	yes	yes	yes	yes	yes	yes	yes	yes
4	NAS-IP Address	yes	yes	yes	yes	yes	yes	yes	yes
5	NAS-Port	yes	yes	yes	yes	yes	yes	yes	yes
6	Service-Type	yes	yes	yes	yes	yes	yes	yes	yes
7	Framed-Protocol	yes	yes	yes	yes	yes	yes	yes	yes
8	Framed-IP-Address	yes	yes	yes	yes	yes	yes	yes	yes
9	Framed-IP-Netmask	yes	yes	yes	yes	yes	yes	yes	yes
10	Framed-Routing	yes	yes	yes	yes	yes	yes	yes	yes
11	Filter-Id	yes	yes	yes	yes	yes	yes	yes	yes
12	Framed-MTU	yes	yes	yes	yes	yes	yes	yes	yes
13	Framed-Compression	yes	yes	yes	yes	yes	yes	yes	yes
14	Login-IP-Host	yes	yes	yes	yes	yes	yes	yes	yes
15	Login-Service	yes	yes	yes	yes	yes	yes	yes	yes
16	Login-TCP-Port	yes	yes	yes	yes	yes	yes	yes	yes
18	Reply-Message	yes	yes	yes	yes	yes	yes	yes	yes
19	Callback-Number	no	no	no	no	no	no	yes	yes
20	Callback-ID	no	no	no	no	no	no	no	no
22	Framed-Route	yes	yes	yes	yes	yes	yes	yes	yes
23	Framed-IPX-Network	no	no	no	no	no	no	no	no
24	State	yes	yes	yes	yes	yes	yes	yes	yes
25	Class	yes	yes	yes	yes	yes	yes	yes	yes
26	Vendor-Specific	yes	yes	yes	yes	yes	yes	yes	yes
27	Session-Timeout	yes	yes	yes	yes	yes	yes	yes	yes
28	Idle-Timeout	yes	yes	yes	yes	yes	yes	yes	yes
29	Termination-Action	no	no	no	no	no	no	no	no
30	Called-Station-Id	yes	yes	yes	yes	yes	yes	yes	yes
31	Calling-Station-Id	yes	yes	yes	yes	yes	yes	yes	yes
32	NAS-Identifier	no	no	no	no	no	no	no	yes
33	Proxy-State	no	no	no	no	no	no	no	no
34	Login-LAT-Service	yes	yes	yes	yes	yes	yes	yes	yes
35	Login-LAT-Node	no	no	no	no	no	no	no	yes

表 1 サポートされている RADIUS IETF アトリビュート (続き)

番号	IETF アトリビュート	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
36	Login-LAT-Group	no	no	no	no	no	no	no	no
37	Framed-AppleTalk-Link	no	no	no	no	no	no	no	no
38	Framed-AppleTalk-Network	no	no	no	no	no	no	no	no
39	Framed-AppleTalk-Zone	no	no	no	no	no	no	no	no
40	Acct-Status-Type	yes	yes	yes	yes	yes	yes	yes	yes
41	Acct-Delay-Time	yes	yes	yes	yes	yes	yes	yes	yes
42	Acct-Input-Octets	yes	yes	yes	yes	yes	yes	yes	yes
43	Acct-Output-Octets	yes	yes	yes	yes	yes	yes	yes	yes
44	Acct-Session-Id	yes	yes	yes	yes	yes	yes	yes	yes
45	Acct-Authentic	yes	yes	yes	yes	yes	yes	yes	yes
46	Acct-Session-Time	yes	yes	yes	yes	yes	yes	yes	yes
47	Acct-Input-Packets	yes	yes	yes	yes	yes	yes	yes	yes
48	Acct-Output-Packets	yes	yes	yes	yes	yes	yes	yes	yes
49	Acct-Terminate-Cause	no	no	no	yes	yes	yes	yes	yes
50	Acct-Multi-Session-Id	no	yes	yes	yes	yes	yes	yes	yes
51	Acct-Link-Count	no	yes	yes	yes	yes	yes	yes	yes
52	Acct-Input-Gigawords	no	no	no	no	no	no	no	no
53	Acct-Output-Gigawords	no	no	no	no	no	no	no	no
55	Event-Timestamp	no	no	no	no	no	no	no	yes
60	CHAP-Challenge	yes	yes	yes	yes	yes	yes	yes	yes
61	NAS-Port-Type	yes	yes	yes	yes	yes	yes	yes	yes
62	Port-Limit	yes	yes	yes	yes	yes	yes	yes	yes
63	Login-LAT-Port	no	no	no	no	no	no	no	no
64	Tunnel-Type <sup>1</sup>	no	no	no	no	no	no	yes	yes
65	Tunnel-Medium-Type <sup>1</sup>	no	no	no	no	no	no	yes	yes
66	Tunnel-Client-Endpoint	no	no	no	no	no	no	yes	yes
67	Tunnel-Server-Endpoint <sup>1</sup>	no	no	no	no	no	no	yes	yes
68	Acct-Tunnel-Connection-ID	no	no	no	no	no	no	yes	yes
69	Tunnel-Password <sup>1</sup>	no	no	no	no	no	no	yes	yes
70	ARAP-Password	no	no	no	no	no	no	no	no
71	ARAP-Features	no	no	no	no	no	no	no	no
72	ARAP-Zone-Access	no	no	no	no	no	no	no	no
73	ARAP-Security	no	no	no	no	no	no	no	no
74	ARAP-Security-Data	no	no	no	no	no	no	no	no
75	Password-Retry	no	no	no	no	no	no	no	no
76	Prompt	no	no	no	no	no	no	yes	yes
77	Connect-Info	no	no	no	no	no	no	no	yes

表 1 サポートされている RADIUS IETF アトリビュート (続き)

番号	IETF アトリビュート	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
78	Configuration-Token	no	no	no	no	no	no	no	no
79	EAP-Message	no	no	no	no	no	no	no	no
80	Message-Authenticator	no	no	no	no	no	no	no	no
81	Tunnel-Private-Group-ID	no	no	no	no	no	no	no	no
82	Tunnel-Assignment-ID <sup>1</sup>	no	no	no	no	no	no	yes	yes
83	Tunnel-Preference	no	no	no	no	no	no	no	yes
84	ARAP-Challenge-Response	no	no	no	no	no	no	no	no
85	Acct-Interim-Interval	no	no	no	no	no	no	yes	yes
86	Acct-Tunnel-Packets-Lost	no	no	no	no	no	no	no	no
87	NAS-Port-ID	no	no	no	no	no	no	no	no
88	Framed-Pool	no	no	no	no	no	no	no	no
90	Tunnel-Client-Auth-ID <sup>2</sup>	no	no	no	no	no	no	no	yes
91	Tunnel-Server-Auth-ID	no	no	no	no	no	no	no	yes
200	IETF-Token-Immediate	no	no	no	no	no	no	no	no

1. この RADIUS アトリビュートは、2 つのドラフト IETF 文書、RFC 2868「*RADIUS Attributes for Tunnel Protocol Support*」と RFC 2867「*RADIUS Accounting Modifications for Tunnel Protocol Support*」に基づきます。
2. この RADIUS アトリビュートは RFC 2865 と RFC 2868 に基づきます。

## RADIUS アトリビュート解説の包括的リスト

表 2 に、IETF RADIUS アトリビュートとその説明を示します。アトリビュートがセキュリティ サーバ固有の形式の場合は、この形式が指定されます。

表 2 RADIUS IETF アトリビュート

番号	IETF アトリビュート	説明
1	User-Name	RADIUS サーバで認証されるユーザの名前を示します。
2	User-Password	ユーザのパスワードまたは Access-Challenge に続くユーザの入力を示します。16 文字未満のパスワードは、RFC 2865 仕様で暗号化されます。
3	CHAP-Password	Access-Challenge に対する応答で PPP Challenge-Handshake Authentication Protocol (CHAP; チャレンジ ハンドシェイク認証プロトコル) ユーザが入力した応答値を示します。
4	NAS-IP Address	認証を要求しているネットワーク アクセス サーバの IP アドレスを示します。デフォルト値は 0.0.0.0/0 です。



表 2 RADIUS IETF アトリビュート (続き)

番号	IETF アトリビュート	説明
5	NAS-Port	<p>ユーザを認証しているネットワーク アクセス サーバの物理ポート番号を示します。NAS-Port 値 (32 ビット) は、1 つまたは 2 つの 16 ビット値 (<b>radius-server extended-portnames</b> コマンドの設定に依存) で構成されます。各 16 ビットの数値は、次のように、解釈用の 5 桁の 10 進整数として表示されるはずですが、</p> <p>非同期端末回線、非同期ネットワーク インターフェイス、および仮想非同期インターフェイスの場合、この値は <b>00ttt</b> です。ここで、<b>ttt</b> は回線番号または非同期インターフェイス装置番号です。</p> <p>通常の同期ネットワーク インターフェイスの場合、この値は <b>10xxx</b> です。</p> <p>プライマリ レート ISDN インターフェイス上のチャンネルの場合、この値は <b>2ppcc</b> です。</p> <p>基本レート ISDN インターフェイス上のチャンネルの場合、この値は <b>3bb0c</b> です。</p> <p>その他のタイプのインターフェイスの場合、この値は <b>6nnss</b> です。</p>
6	Service-Type	<p>要求されたサービスのタイプまたは指定されたサービスのタイプを示します。</p> <ul style="list-style-type: none"> <li>• 要求内 : <ul style="list-style-type: none"> <li>既知の PPP または SLIP 接続の場合は Framed。</li> <li><b>enable</b> コマンドの場合は Administrative-user。</li> </ul> </li> <li>• 応答内 : <ul style="list-style-type: none"> <li>Login : 接続を確立します。</li> <li>Framed : SLIP または PPP を開始します。</li> <li>Administrative User : EXEC または <b>enable ok</b> を開始します。</li> </ul> </li> </ul> <p>Exec User : EXEC セッションを開始します。</p> <p>サービス タイプは、次のような特定の数値で示されます。</p> <ul style="list-style-type: none"> <li>• 1 : Login</li> <li>• 2 : Framed</li> <li>• 3 : Callback-Login</li> <li>• 4 : Callback-Framed</li> <li>• 5 : Outbound</li> <li>• 6 : Administrative</li> <li>• 7 : NAS-Prompt</li> <li>• 8 : Authenticate Only</li> <li>• 9 : Callback-NAS-Prompt</li> </ul>

表 2 RADIUS IETF アトリビュート (続き)

番号	IETF アトリビュート	説明
7	Framed-Protocol	<p>フレーム化アクセスに使用されるフレーム構成を示します。他のフレーム構成は許可されません。</p> <p>フレーム構成は次のように数値で指定されます。</p> <ul style="list-style-type: none"> <li>• 1 : PPP</li> <li>• 2 : SLIP</li> <li>• 3 : ARA</li> <li>• 4 : Gandalf 独自のシングルリンク/マルチリンク プロトコル</li> <li>• 5 : Xylogics 独自の IPX/SLIP</li> </ul>
8	Framed-IP-Address	<p>access-request 内でユーザの IP アドレスを RADIUS サーバに送信することによって、ユーザに対して設定する IP アドレスを示します。このコマンドを有効にするには、グローバル コンフィギュレーション モードで <b>radius-server attribute 8 include-in-access-req</b> コマンドを使用します。</p>
9	Framed-IP-Netmask	<p>ユーザがルータまたはネットワークの場合に、ユーザに対して設定する IP ネットマスクを示します。このアトリビュート値によって、指定されたマスクを使用して Framed-IP-Address に静的ルートが追加されることとなります。</p>
10	Framed-Routing	<p>ユーザがルータまたはネットワークの場合に、ユーザに対するルーティング方式を示します。このアトリビュートに対しては、「なし」と「送信とリッスン」の値だけがサポートされています。</p> <p>ルーティング方式は次のように数値で指定されます。</p> <ul style="list-style-type: none"> <li>• 0 : なし</li> <li>• 1 : ルーティング パケットの送信</li> <li>• 2 : ルーティング パケットのリッスン</li> <li>• 3 : ルーティング パケットの送信とリッスン</li> </ul>
11	Filter-Id	<p>ユーザのフィルタ リストの名前を示し、%d、%d.in、または %d.out としてフォーマットされます。このアトリビュートは、最近のサービス タイプ コマンドに関連付けられます。ログインと EXEC の場合は、0 ~ 199 の回線アクセス リスト値として %d または %d.out を使用します。フレーム化サービスの場合は、インターフェイス出力アクセス リストとして %d または %d.out を使用し、入力アクセス リストとして %d.in を使用します。この番号は、参照しているプロトコルに対する自己符号化です。</p>
12	Framed-MTU	<p>Maximum Transmission Unit (MTU; 最大伝送ユニット) が PPP またはその他の手段でネゴシエートされない場合に、ユーザに対して設定可能な MTU を示します。</p>
13	Framed-Compression	<p>リンクに使用される圧縮プロトコルを示します。このアトリビュートによって、EXEC 認可中に生成された PPP または SLIP autocommand に「compress」が追加されることとなります。非 EXEC 認可には実装されていません。</p> <p>圧縮プロトコルは次のように数値で指定されます。</p> <ul style="list-style-type: none"> <li>• 0 : なし</li> <li>• 1 : VJ-TCP/IP ヘッダー圧縮</li> <li>• 2 : IPX ヘッダー圧縮</li> </ul>
14	Login-IP-Host	<p>Login-Service アトリビュートが含まれている場合に、ユーザが接続するホストを示します (この動作はログイン直後に開始されます)。</p>

表 2 RADIUS IETF アトリビュート (続き)

番号	IETF アトリビュート	説明
15	Login-Service	ユーザをログイン ホストに接続するために使用すべきサービスを示します。 サービスは次のように数値で指定されます。 <ul style="list-style-type: none"> <li>• 0 : Telnet</li> <li>• 1 : Rlogin</li> <li>• 2 : TCP-Clear</li> <li>• 3 : PortMaster</li> <li>• 4 : LAT</li> </ul>
16	Login-TCP-Port	Login-Service アトリビュートも存在する場合に、ユーザを接続すべき TCP ポートを定義します。
18	Reply-Message	RADIUS サーバ経由でユーザに表示される可能性のあるテキストを示します。このアトリビュートはユーザ ファイルに含めることができますが、プロファイル当たりの Reply-Message エントリ数を 16 以下にする必要があります。
19	Callback-Number	コールバックに使用するダイヤリング文字列を定義します。
20	Callback-ID	呼び出される場所の名前、つまり、ネットワーク アクセス サーバによって解釈される場所の名前 (1 つ以上のオクテットからなる) を定義します。
22	Framed-Route	このネットワーク アクセス サーバ上のユーザに対して設定するルーティング情報を指定します。RADIUS RFC 形式 (net/bits [router [metric]]) と従来のドット区切りのマスク (net mask [router [metric]]) がサポートされています。ルータ フィールドを省略するか、0 にした場合は、ピア IP アドレスが使用されます。現在、メトリックは無視されます。このアトリビュートは access-request パケットです。
23	Framed-IPX-Network	ユーザに対して設定される IPX ネットワーク番号を定義します。
24	State	ネットワーク アクセス サーバと RADIUS サーバ間で状態情報の保持を可能にします。このアトリビュートは CHAP チャレンジにしか適用できません。
25	Class	(アカウントリング) RADIUS サーバで入力された場合に、このユーザに関するすべてのアカウントリング パケットにネットワーク アクセス サーバで追加される任意の値。

表 2 RADIUS IETF アトリビュート (続き)

番号	IETF アトリビュート	説明
26	Vendor-Specific	<p>ベンダーに一般使用に適さない独自の拡張アトリビュートの使用を許可します。シスコの RADIUS 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートされているオプションは「cisco-avpair」という名前の vendor-type 1 です。この値は次の形式の文字列です。</p> <pre>protocol : attribute sep value</pre> <p>「Protocol」は、特定の認可タイプを表すシスコの「protocol」アトリビュートです。「Attribute」と「value」は、シスコの TACACS+ 仕様で規定されている AV ペアで、「sep」は、必須アトリビュートの場合は「=」で、オプションアトリビュートの場合は「*」です。これにより、TACACS+ 認可で使用できるすべての機能を RADIUS にも使用できるようになります。次に例を示します。</p> <pre>cisco-avpair= "ip:addr-pool=first" cisco-avpair= "shell:priv-lvl=15"</pre> <p>最初の例は、IP 認可中 (PPP の IPCP アドレス割り当て中) に、シスコの「複数の名前付き IP アドレス プール」機能をアクティブにします。2 つめの例は、ネットワーク アクセス サーバからのユーザ ログイン直後に EXEC コマンドにアクセスできるようにします。</p> <p>表 1 に、サポートされているベンダー固有の RADIUS アトリビュート (IETF アトリビュート 26) を示します。「TACACS+ Attribute-Value Pairs」モジュールに、IETF アトリビュート 26 と一緒に使用可能なサポートされている TACACS+ Attribute-Value (AV) ペアの全リストが記載されています (RFC 2865)。</p>
27	Session-Timeout	セッションを終了する前に、ユーザにサービスを提供する最大秒数を設定します。このアトリビュート値は、ユーザ単位「絶対タイムアウト」になります。
28	Idle-Timeout	セッションが終了する前にユーザに許可されるアイドル接続の最大秒数を設定します。このアトリビュート値は、ユーザ単位「セッションタイムアウト」になります。
29	Termination-Action	<p>終了は次のように数値で指定されます。</p> <ul style="list-style-type: none"> <li>• 0 : デフォルト</li> <li>• 1 : RADIUS 要求</li> </ul>
30	Called-Station-Id	(アカウントिंग) ネットワーク アクセス サーバから、ユーザが Access-Request パケットの一部として、呼び出した電話番号を送信できるようにします (Dialed Number Identification Service (DNIS; 着信番号識別サービス) または同様のテクノロジー)。このアトリビュートは、ISDN と、PRI と一緒に使用された場合の Cisco AS5200 上のモデム コールに対してのみサポートされます。
31	Calling-Station-Id	(アカウントिंग) ネットワーク アクセス サーバから、コールが Access-Request パケットの一部として発信された電話番号を送信できるようにします (自動番号識別または同様のテクノロジー)。このアトリビュートの値は、TACACS+ の「remote-addr」の値と同じです。このアトリビュートは、ISDN と、PRI と一緒に使用された場合の Cisco AS5200 上のモデム コールに対してのみサポートされます。
32	NAS-Identifier	Access-Request を送信したネットワーク アクセス サーバを識別する文字列。 <b>radius-server attribute 32 include-in-access-req</b> グローバル コンフィギュレーション コマンドを使用して、Access-Request または Accounting-Request 内で RADIUS アトリビュート 32 を送信します。フォーマットが指定されなかった場合は、デフォルトで、FQDN がアトリビュート内で送信されます。

表 2 RADIUS IETF アトリビュート (続き)

番号	IETF アトリビュート	説明
33	Proxy-State	Access-Request の転送時にプロキシサーバから別のサーバに送信可能なアトリビュート。このアトリビュートは、Access-Accept、Access-Reject、または Access-Challenge 内でそのまま返され、ネットワーク アクセス サーバに応答が送信される前にプロキシサーバで削除される必要があります。
34	Login-LAT-Service	ユーザを LAT で接続すべきシステムを示します。このアトリビュートは、EXEC モードでのみ使用できます。
35	Login-LAT-Node	ユーザを自動的に LAT で接続すべきノードを示します。
36	Login-LAT-Group	このユーザの認可に使用される LAT グループ コードを識別します。
37	Framed-AppleTalk-Link	AppleTalk ルータであるユーザへのシリアルリンクに使用すべき別の AppleTalk のネットワーク番号を示します。
38	Framed-AppleTalk-Network	ユーザに AppleTalk ノードを割り当てるためにネットワーク アクセス サーバで使用される AppleTalk ネットワーク番号を示します。
39	Framed-AppleTalk-Zone	このユーザに使用すべき AppleTalk デフォルトゾーンを示します。
40	Acct-Status-Type	(アカウントリング) この Accounting-Request がユーザ サービスの始まり (開始) または終わり (終了) をマークするかどうかを示します。
41	Acct-Delay-Time	(アカウントリング) クライアントが特定のレコードの送信を試みる秒数を示します。
42	Acct-Input-Octets	(アカウントリング) このサービスの提供中にポートから受信されたオクテット数を示します。
43	Acct-Output-Octets	(アカウントリング) このサービスの配信中にポートに送信されたオクテット数を示します。
44	Acct-Session-Id	(アカウントリング) ログ ファイル内の開始レコードと終了レコードのマッチングを容易にする一意のアカウントリング識別子。Acct-Session ID 番号は、ルータの電源が再投入されるか、ソフトウェアがリロードされるたびに、1 にリセットされます。このアトリビュートを access-request パケット内で送信するには、グローバル コンフィギュレーション モードで <b>radius-server attribute 44 include-in-access-req</b> コマンドを使用します。
45	Acct-Authentic	(アカウントリング) ユーザがどのように認証されたか、RADIUS、ネットワーク アクセス サーバ自体、およびその他のリモート認証プロトコルのどれで認証されたかを示します。このアトリビュートは、RADIUS で認証されたユーザの場合は「radius」に、TACACS+ と Kerberos の場合は「remote」に、local、enable、line、および if-needed 方式の場合は「local」に設定されます。その他のすべての方式の場合は、このアトリビュートが省略されます。
46	Acct-Session-Time	(アカウントリング) ユーザがサービスを受信していた時間 (秒数) を示します。
47	Acct-Input-Packets	(アカウントリング) このサービスのフレーム化ユーザへの提供中にポートから受信されたパケット数を示します。
48	Acct-Output-Packets	(アカウントリング) このサービスのフレーム化ユーザへの配信中にポートに送信されたパケット数を示します。

表 2 RADIUS IETF アトリビュート (続き)

番号	IETF アトリビュート	説明
49	Acct-Terminate-Cause	<p>(アカウントティング) 接続が終了した理由の詳細を報告します。終了の理由は次のように数値で指定されます。</p> <ol style="list-style-type: none"> <li>1. ユーザ要求</li> <li>2. 搬送波の消失</li> <li>3. サービスの消失</li> <li>4. アイドル タイムアウト</li> <li>5. セッション タイムアウト</li> <li>6. 管理リセット</li> <li>7. 管理リブート</li> <li>8. ポート エラー</li> <li>9. NAS エラー</li> <li>10. NAS 要求</li> <li>11. NAS リポート</li> <li>12. ポートの不要化</li> <li>13. ポートの横取り</li> <li>14. ポートの保留</li> <li>15. 使用できないサービス</li> <li>16. コールバック</li> <li>17. ユーザ エラー</li> <li>18. ホスト要求</li> </ol> <p>(注) アトリビュート 49 に関して、Cisco IOS は 1 ~ 6、9、12、および 15 ~ 18 の値をサポートしています。</p>
50	Acct-Multi-Session-Id	<p>(アカウントティング) ログ ファイル内の複数の関連セッションをリンクするために使用される一意のアカウントティング識別子。</p> <p>マルチリンク セッション内でリンクされたセッションごとに、一意の Acct-Session-Id 値が割り当てられますが、Acct-Multi-Session-Id は共有されます。</p>
51	Acct-Link-Count	<p>(アカウントティング) アカウントティング レコードが生成された時点で特定のマルチリンク セッション内で認識されていたリンク数を示します。ネットワーク アクセス サーバは、複数のリンクが含まれる任意のアカウントティング要求内にこのアトリビュートを追加できます。</p>
52	Acct-Input-Gigawords	<p>サービスの提供中に Acct-Input-Octets カウンタが一周 (2 の 32 乗) した回数を示します。</p>
53	Acct-Output-Gigawords	<p>サービスの配信中に Acct-Output-Octets カウンタが一周 (2 の 32 乗) した回数を示します。</p>

表 2 RADIUS IETF アトリビュート (続き)

番号	IETF アトリビュート	説明
55	Event-Timestamp	<p>NAS 上でイベントが発生した時刻を記録します。アトリビュート 55 内で送信されるタイムスタンプは、1970 年 1 月 1 日 00:00 UTC 以降の秒数です。アカウントングパケット内で RADIUS アトリビュート 55 を送信するには、<b>radius-server attribute 55 include-in-acct-req</b> コマンドを使用します。</p> <p>(注) アカウントングパケット内で Event-Timestamp アトリビュートを送信するには、ルータのクロックを設定する必要があります (ルータのクロックの設定方法については、『<a href="#">Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4T</a>』を参照してください)。</p> <p>ルータがリロードされるたびにルータのクロックを設定するのを避けるには、<b>clock calendar-valid</b> コマンドを有効にします。このコマンドの詳細については、『<a href="#">Cisco IOS Configuration Fundamentals Command Reference</a>』を参照してください。</p>
60	CHAP-Challenge	ネットワーク アクセス サーバから PPP CHAP ユーザに送信されたチャレンジ ハンドシェイク認証プロトコル チャレンジが保存されます。
61	NAS-Port-Type	<p>ユーザを認証するためにネットワーク アクセス サーバで使用されている物理ポートのタイプを示します。物理ポートは、次のように数値で示されます。</p> <ul style="list-style-type: none"> <li>• 0 : 非同期</li> <li>• 1 : 同期</li> <li>• 2 : ISDN 同期</li> <li>• 3 : ISDN 非同期 (V.120)</li> <li>• 4 : ISDN 非同期 (V.110)</li> <li>• 5 : 仮想</li> </ul>
62	Port-Limit	NAS からユーザに提供される最大ポート数を設定します。
63	Login-LAT-Port	ユーザを LAT で接続すべきポートを定義します。
64	Tunnel-Type <sup>1</sup>	使用されているトンネリングプロトコルを示します。Cisco IOS ソフトウェアは、このアトリビュートに対して L2TP と L2F の 2 つの値をサポートしています。このアトリビュートが設定されていない場合は、L2F がデフォルトとして使用されます。
65	Tunnel-Medium-Type <sup>1</sup>	トンネルの作成に使用される転送メディアタイプを示します。このアトリビュートには、このリリースで使用可能な値 (IP) が 1 つしかありません。このアトリビュートに値を設定しなかった場合は、デフォルトとして IP が使用されます。

表 2 RADIUS IETF アトリビュート (続き)

番号	IETF アトリビュート	説明
66	Tunnel-Client-Endpoint	<p>トンネルの開始側端のアドレスが含まれています。Access-Request と Access-Accept の両方のパケットに含めて、新しいトンネルを開始するアドレスを示すこともできます。Tunnel-Client-Endpoint アトリビュートが Access-Request パケットに含まれている場合は、RADIUS サーバがヒントとしてこの値を取得する必要があります。ただし、サーバがこのヒントに従う義務はありません。このアトリビュートは、Accounting-Request パケットに含める必要があります。このパケットには、トンネルが開始されたアドレスを示す場合に Start と Stop のどちらかの値を伴う Acct-Status-Type アトリビュートが含まれています。このアトリビュートは、Tunnel-Server-Endpoint アトリビュートや Acct-Tunnel-Connection-ID アトリビュートと一緒に使用して、アカウントリングと監査の目的でトンネルを特定する、グローバルで一意の手段を提供できます。</p> <p>次のように、このアトリビュートの 127.0.0.X の値を受け入れるためにネットワーク アクセス サーバの機能が拡張されています。</p> <p>127.0.0.0 は、loopback0 IP アドレスを使用することを示します。  127.0.0.1 は、loopback1 IP アドレスを使用することを示します。  ...  127.0.0.X は、loopbackX IP アドレスを使用することを示します。</p> <p>実際のトンネル クライアント エンドポイント IP アドレスとして使用されることを示す。この機能拡張によって、複数のネットワーク アクセス サーバ全体のスケーラビリティが向上します。</p>
67	Tunnel-Server-Endpoint <sup>1</sup>	<p>トンネルのサーバ端のアドレスを示します。このアトリビュートのフォーマットは、Tunnel-Medium-Type の値によって異なります。このリリースはトンネル メディア タイプとして IP しかサポートしていないため、このアトリビュートに使用できるのは LNS の IP アドレスまたはホスト名だけです。</p>
68	Acct-Tunnel-Connection-ID	<p>トンネル セッションに割り当てられた識別子を示します。このアトリビュートは、Start、Stop、または上記のいずれかを値として持つ Acct-Status-Type アトリビュートと一緒に Accounting-Request パケットに含める必要があります。このアトリビュートは、Tunnel-Client-Endpoint アトリビュートや Tunnel-Server-Endpoint アトリビュートと一緒に使用して、監査の目的でトンネル セッションを一意に特定する手段を提供できます。</p>
69	Tunnel-Password <sup>1</sup>	<p>リモート サーバの認証に使用されるパスワードを定義します。このアトリビュートは、Tunnel-Type の値 (AAA_ATTR_l2tp_tunnel_pw (L2TP)、AAA_ATTR_nas_password (L2F)、および AAA_ATTR_gw_password (L2F)) に基づいて、さまざまな AAA アトリビュートに変換されます。</p> <p>デフォルトで、受信されたすべてのパスワードが暗号化されます。そのため、NAS が暗号化されていないパスワードを復号化しようとする、認可エラーが発生する可能性があります。アトリビュート 69 で暗号化されていないパスワードの受信を可能にするには、<b>radius-server attribute 69 clear</b> グローバル コンフィギュレーション コマンドを使用します。</p>
70	ARAP-Password	ARAP の Framed-Protocol を含む Access-Request パケットを示します。
71	ARAP-Features	NAS から ARAP 「feature flags」 パケット内のユーザに送信すべきパスワード情報が含まれています。
72	ARAP-Zone-Access	ユーザの ARAP ゾーン リストの使用法を示します。
73	ARAP-Security	Access-Challenge パケット内で使用すべき ARAP セキュリティ モジュールを示します。



表 2 RADIUS IETF アトリビュート (続き)

番号	IETF アトリビュート	説明
74	ARAP-Security-Data	実際のセキュリティ モジュールのチャレンジまたは応答が含まれています。 Access-Challenge パケットと Access-Request パケットの両方に使用できます。
75	Password-Retry	ユーザが切斷されるまでに認証を試みることができる回数を示します。
76	Prompt	ユーザの応答をエコーすべきか否かを NAS に指示します (0=エコーなし、1=エコーあり)。
77	Connect-Info	モデム コールに関する追加情報を提供します。このアトリビュートは start と stop の アカウントレコード内で生成されます。
78	Configuration-Token	使用すべきユーザ プロファイルのタイプを示します。このアトリビュートは、プロキシ に基づく大規模な分散認証ネットワークで使用する必要があります。 Access-Accept 内で RADIUS プロキシサーバから RADIUS プロキシクライアントに 送信されます。NAS には送信しないでください。
79	EAP-Message	Extended Access Protocol (EAP) プロトコルを理解していなくても、NAS で EAP 経由のダイヤルイン ユーザを認証できるように EAP パケットをカプセル化します。
80	Message-Authenticator	CHAP、ARAP、または EAP 認証方式を使用して Access-Requests のスプーフィング を阻止します。
81	Tunnel-Private-Group-ID	特定のトンネル化されたセッションのグループ ID を示します。
82	Tunnel-Assignment-ID <sup>1</sup>	セッションが割り当てられた特定のトンネル イニシエータを示します。
83	Tunnel-Preference	各トンネルに割り当てられた相対プリファレンスを示します。このアトリビュート は、RADIUS サーバからトンネル イニシエータに複数のトンネリングアトリビュート のセットが返される場合に含める必要があります。
84	ARAP-Challenge-Response	ダイヤルイン クライアントのチャレンジに対する応答が含まれています。
85	Acct-Interim-Interval	この特定のセッションの一時更新間隔を秒数で示します。この値は、Access-Accept メッセージにのみ含めることができます。
86	Acct-Tunnel-Packets-Lost	特定のリンク上で失われたパケット数を示します。このアトリビュートは、 Tunnel-Link-Stop の値を持つ Acct-Status-Type アトリビュートと一緒に Accounting-Request パケットに含める必要があります。
87	NAS-Port-ID	ユーザを認証している NAS のポートを識別するテキスト文字列が含まれています。
88	Framed-Pool	ユーザにアドレスを割り当てるために使用すべき、割り当て済みのアドレス プールの 名前が含まれています。NAS が複数のアドレス プールをサポートしていない場合は、 このアトリビュートを無視する必要があります。
90	Tunnel-Client-Auth-ID	トンネル セットアップをトンネル ターミネータで認証するときに、トンネル イニシ エータ (NAS とも呼ばれる) で使用される名前を示します。L2F プロトコルと L2TP プロトコルをサポートします。
91	Tunnel-Server-Auth-ID	トンネル セットアップをトンネル イニシエータで認証するときに、トンネル ターミ ネータ (ホーム ゲートウェイとも呼ばれる) で使用される名前を示します。L2F プロ トコルと L2TP プロトコルをサポートします。
200	IETF-Token-Immediate	ファイル エントリがハンドヘルドセキュリティ カード サーバを示しているログイン ユーザから受け取ったパスワードを RADIUS でどのように処理するかを決定します。 このアトリビュートの値は次のように数値で指定されます。 <ul style="list-style-type: none"> <li>0: いいえ、パスワードが無視されることを意味します。</li> <li>1: はい、パスワードが認証に使用されることを意味します。</li> </ul>

1. この RADIUS アトリビュートは、2つのドラフト IETF 文書、RFC 2868「*RADIUS Attributes for Tunnel Protocol Support*」と RFC 2867「*RADIUS Accounting Modifications for Tunnel Protocol Support*」に基づきます。

## その他の参考資料

次の項で、RADIUS IETF アトリビュートに関する参考資料を紹介します。

## 関連資料

内容	参照先
RADIUS	「 <a href="#">Configuring RADIUS</a> 」モジュール
認証	「 <a href="#">Configuring Authentication</a> 」モジュール
認可	「 <a href="#">Configuring Authorization</a> 」モジュール
アカウントिंग	「 <a href="#">Configuring Accounting</a> 」モジュール
RADIUS ベンダー固有アトリビュート	「 <a href="#">RADIUS Vendor-Proprietary Attributes</a> 」モジュール

## 規格

規格	タイトル
なし	—

## MIB

MIB	MIB リンク
なし	<p>選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFC

RFC	タイトル
<a href="#">RFC 2865</a>	「 <i>Remote Authentication Dial In User Service (RADIUS)</i> 」
<a href="#">RFC 2866</a>	「 <i>RADIUS Accounting</i> 」
<a href="#">RFC 2867</a>	「 <i>RADIUS Accounting Modifications for Tunnel Protocol Support</i> 」
<a href="#">RFC 2868</a>	「 <i>RADIUS Attributes for Tunnel Protocol Support</i> 」
<a href="#">RFC 2869</a>	「 <i>RADIUS Extensions</i> 」

## シスコのテクニカル サポート

説明	リンク
<p>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。</p> <p>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。</p> <ul style="list-style-type: none"><li>・テクニカル サポートを受ける</li><li>・ソフトウェアをダウンロードする</li><li>・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</li><li>・ツールおよびリソースへアクセスする<ul style="list-style-type: none"><li>- Product Alert の受信登録</li><li>- Field Notice の受信登録</li><li>- Bug Toolkit を使用した既知の問題の検索</li></ul></li><li>・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</li><li>・トレーニング リソースへアクセスする</li><li>・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</li></ul> <p>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。</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# RADIUS アトリビュートの概要と RADIUS IETF アトリビュートの機能情報

表 3 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、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できます。Cisco Feature Navigator を使用すると、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サポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp> からアクセスできます。Cisco.com のアカウントは必要ありません。



(注) 表 3 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 3 RADIUS アトリビュートの概要と RADIUS IETF アトリビュートの機能情報

機能名	リリース	機能情報
RADIUS IETF アトリビュート	Cisco IOS Release 11.1	この機能は、Cisco IOS Release 11.1 で導入されました。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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。

© 2001–2009 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2001–2011, シスコシステムズ合同会社.  
All rights reserved.