『RADIUS Attributes Overview and RADIUS IETF Attributes』

Remote Authentication Dial-In User Service（RADIUS）属性は、RADIUS プログラムに保存されたユーザ プロファイル内の特定の認証、認可、およびアカウンティング（AAA）要素を定義するために使用されます。この章では、サポートされる RADIUS 属性を示します。

RADIUS 属性の概要

IETF 属性と VSA の比較

RADIUS インターネット技術特別調査委員会（IETF）属性は、255 個の標準属性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 属性は標準であり、属性のデータは事前に定義されています。IETF 属性を使用して AAA 情報を交換するクライアントとサーバは、属性の正確な意味や各属性値の一般的な範囲など、属性データについて合意する必要があります。

RADIUS ベンダー固有属性（VSA）は、ベンダー固有 IETF 属性（属性 26）に由来しています。属性 26 を使用して、ベンダーは 255 種の属性を追加作成できます。つまり、ベンダーは、IETF 属性のデータとは異なる属性を作成して、属性 26 の背後でカプセル化することができます。新しく作成された属性は、ユーザが属性 26 を受け入れる場合に受信されます。

VSA の詳細については、「RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値」の章を参照してください。

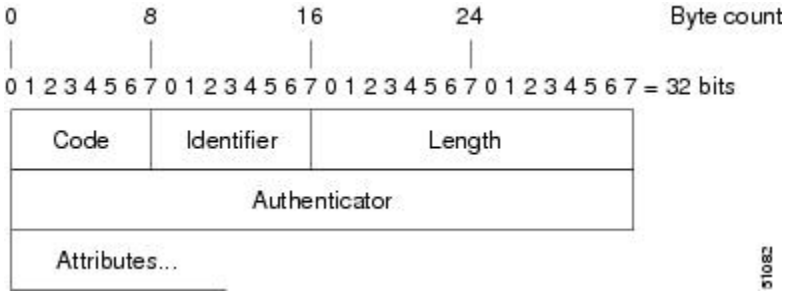
RADIUS パケットのフォーマット

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。

次の図に、RADIUS パケット内のフィールドを示します。

（注） VSA の図については、「RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値」の章の図 1 を参照してください。

図 *1 : RADIUS* パケット図



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。オーセンティケータには次の 2 つのタイプがあります。
  - 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、属性情報を含む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、ユーザにアクセスを許可している特定のネットワーク アクセス サーバ（NAS）へのアクセスを許可するかどうかを RADIUS サーバが判断するための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。RADIUS サーバは、Access-Request パケットを受信した後、応答を返す必要があります。

Access-Accept：RADIUS サーバは、Access-Request パケットを受信した後、Access-Request パケット内のすべての属性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：RADIUS サーバは、Access-Request パケットを受信した後、どの属性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：RADIUS サーバは、Access-Accept パケットの受信後、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応答する場合は、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。各ファイルには、ユーザの認証や認可のレベルが定義されています。ディレクトリ ファイルには、ユーザの NAS が実装できる属性が定義され、クライアント ファイルには、RADIUS サーバに要求を行えるユーザが定義され、ユーザ ファイルには、セキュリティおよび構成データに基づいて RADIUS サーバが認証するユーザ要求が定義されます。

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属性に依存する属性のリストが格納されています。ただし、独自の属性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。このファイルでは属性値が定義されるため、構文解析要求などの属性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 などの属性の ASCII 文字列「名」
- ID：属性の数値「名」。たとえば、User-Name 属性は属性 1 です。

- 値型：属性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による 32 ビット値（上位バイトが先頭）
  - string：0 ～ 253 オクテット

特定の属性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、整数ベースの属性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には、RADIUS サーバへの認証要求とアカウンティング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ます。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完全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
#----------------  ---------------
10.1.2.3:256        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 サーバが認証する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属性が設定されます。

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、最初の行の属性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属性応答を表します。応答内で送信される属性は、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属性で、等号文字の右側のデータが構成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 company.com、パスワードが user1 で、ユーザは 5 つのトンネル属性にアクセスできます。

```
# This user profile includes RADIUS tunneling attributes
company.com  Password="user1" 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 属性

（注） RADIUS トンネル属性では、L2TP に 32 個のタグ付きトンネル セットがサポートされます。

サポートされている RADIUS IETF 属性

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

リスト内の属性の説明については、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属性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* 属性

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
1	User-Name	あり	あり	あり	あり	あり	あり	あり	あり
2	User-Password	あり	あり	あり	あり	あり	あり	あり	あり
3	CHAP-Password	あり	あり	あり	あり	あり	あり	あり	あり
4	NAS-IP Address	あり	あり	あり	あり	あり	あり	あり	あり
5	NAS-Port	あり	あり	あり	あり	あり	あり	あり	あり
6	Service-Type	あり	あり	あり	あり	あり	あり	あり	あり
7	Framed-Protocol	あり	あり	あり	あり	あり	あり	あり	あり
8	Framed-IP-Address	あり	あり	あり	あり	あり	あり	あり	あり
9	Framed-IP-Netmask	あり	あり	あり	あり	あり	あり	あり	あり
10	Framed-Routing	あり	あり	あり	あり	あり	あり	あり	あり
11	Filter-Id	あり	あり	あり	あり	あり	あり	あり	あり
12	Framed-MTU	あり	あり	あり	あり	あり	あり	あり	あり
13	Framed-Compression	あり	あり	あり	あり	あり	あり	あり	あり
14	Login-IP-Host	あり	あり	あり	あり	あり	あり	あり	あり
15	Login-Service	あり	あり	あり	あり	あり	あり	あり	あり
16	Login-TCP-Port	あり	あり	あり	あり	あり	あり	あり	あり
18	Reply-Message	あり	あり	あり	あり	あり	あり	あり	あり
19	Callback-Number	いいえ（No）	いいえ (No)	いいえ（No）	いいえ（No）	いいえ（No）	いいえ (No)	あり	あり
20	Callback-ID	いいえ（No）	いいえ (No)	いいえ（No）	いいえ（No）	いいえ（No）	いいえ (No)	いいえ（No）	いいえ（No）
22	Framed-Route	あり	あり	あり	あり	あり	あり	あり	あり
23	Framed-IPX-Network	いいえ（No）	いいえ (No)	いいえ（No）	いいえ（No）	いいえ（No）	いいえ (No)	いいえ（No）	いいえ（No）

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
24	状態	あり	あり	あり	あり	あり	あり	あり	あり
25	Class	あり	あり	あり	あり	あり	あり	あり	あり
26	Vendor-Specific	あり	あり	あり	あり	あり	あり	あり	あり
27	Session-Timeout	あり	あり	あり	あり	あり	あり	あり	あり
28	Idle-Timeout	あり	あり	あり	あり	あり	あり	あり	あり
29	Termination-Action	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
30	Called-Station-Id	あり	あり	あり	あり	あり	あり	あり	あり
31	Calling-Station-Id	あり	あり	あり	あり	あり	あり	あり	あり
32	NAS-Identifier	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
33	Proxy-State	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
34	Login-LAT-Service	あり	あり	あり	あり	あり	あり	あり	あり
35	Login-LAT-Node	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
36	Login-LAT-Group	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
37	Framed-AppleTalk-Link	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
38	Framed-AppleTalk-Network	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
39	Framed-AppleTalk-Zone	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
40	Acct-Status-Type	あり	あり	あり	あり	あり	あり	あり	あり
41	Acct-Delay-Time	あり	あり	あり	あり	あり	あり	あり	あり
42	Acct-Input-Octets	あり	あり	あり	あり	あり	あり	あり	あり
43	Acct-Output-Octets	あり	あり	あり	あり	あり	あり	あり	あり
44	Acct-Session-Id	あり	あり	あり	あり	あり	あり	あり	あり
45	Acct-Authentic	あり	あり	あり	あり	あり	あり	あり	あり
46	Acct-Session-Time	あり	あり	あり	あり	あり	あり	あり	あり
47	Acct-Input-Packets	あり	あり	あり	あり	あり	あり	あり	あり
48	Acct-Output-Packets	あり	あり	あり	あり	あり	あり	あり	あり
49	Acct-Terminate-Cause	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり	あり	あり	あり
50	Acct-Multi-Session-Id	いいえ（No）	あり	あり	あり	あり	あり	あり	あり
51	Acct-Link-Count	いいえ（No）	あり	あり	あり	あり	あり	あり	あり
52	Acct-Input-Gigawords	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
53	Acct-Output-Gigawords	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
55	Event-Timestamp	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
60	CHAP-Challenge	あり	あり	あり	あり	あり	あり	あり	あり
61	NAS-Port-Type	あり	あり	あり	あり	あり	あり	あり	あり
62	Port-Limit	あり	あり	あり	あり	あり	あり	あり	あり
63	Login-LAT-Port	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
64	Tunnel-Type[1]	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
65	Tunnel-Medium-Type 1	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
66	Tunnel-Client-Endpoint	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
67	Tunnel-Server-Endpoint 1	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
68	Acct-Tunnel-Connection-ID	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
69	Tunnel-Password 1	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
70	ARAP-Password	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
71	ARAP-Features	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
72	ARAP-Zone-Access	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
73	ARAP-Security	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
74	ARAP-Security-Data	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
75	Password-Retry	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
76	Prompt	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
77	Connect-Info	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
78	Configuration-Token	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
79	EAP-Message	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
80	Message-Authenticator	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
81	Tunnel-Private-Group-ID	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
82	Tunnel-Assignment-ID 1	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり
83	Tunnel-Preference	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
84	ARAP-Challenge-Response	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
85	Acct-Interim-Interval	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり	あり

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
86	Acct-Tunnel-Packets-Lost	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
87	NAS-Port-ID	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
88	Framed-Pool	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）
90	Tunnel-Client-Auth-ID [2]	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
91	Tunnel-Server-Auth-ID	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	あり
200	IETF-Token-Immediate	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）	いいえ（No）

[1] この RADIUS 属性は、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 属性は、RFC 2865 および RFC 2868 に基づきます。

RADIUS 属性解説の包括的リスト

次の表に、IETF RADIUS 属性とその説明を示します。属性がセキュリティ 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* 属性

番号	IETF 属性	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	Access-Challenge の後に続くユーザのパスワードとユーザ入力を示します。16 文字を超えるパスワードは、RFC 2865 の仕様により暗号化されます。

番号	IETF 属性	説明
3	CHAP-Password	Access-Challenge に対する応答で PPP Challenge Handshake Authentication Protocol（CHAP）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。
5	NAS-Port	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（**radius-server extended-portnames** 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。 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 **00ttt** です。ここで、**ttt** は回線番号または非同期インターフェイスユニット番号です。 • 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 **10xxx** です。 • プライマリレート ISDN インターフェイス上のチャネルの場合、この値は **2ppcc** です。 • 基本レート ISDN インターフェイス上のチャネルの場合、この値は **3bb0c** です。 • 他のタイプのインターフェイスの場合、値は **6nnss** です。

番号	IETF 属性	説明
6	Service-Type	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。 • 要求内： 既知の PPP または Serial Line Internet Protocol（SLIP）接続の場合にフレーム化。**enable** コマンドの場合は Administrative-user。 • 応答内： Login：接続を確立します。Framed：SLIP または PPP を開始します。Administrative User：EXEC または **enable ok** を開始します。 Exec User：EXEC セッションを開始します。 サービス タイプは、次のような特定の数値で示されます。 • 1：Login • 2：Framed • 3：Callback-Login • 4：Callback-Framed • 5：Outbound • 6：Administrative • 7：NAS-Prompt • 8：Authenticate Only • 9：Callback-NAS-Prompt

番号	IETF 属性	説明
7	Framed-Protocol	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。 フレーム構成は次のように数値で指定されます。 • 1：PPP • 2：SLIP • 3：ARA • 4：Gandalf 独自のシングルリンク/マルチリンク プロトコル • 5：Xylogics 独自の IPX/SLIP
8	Framed-IP-Address	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 **radius-server attribute 8 include-in-access-req** コマンドを使用します。
9	Framed-IP-Netmask	ユーザがネットワーク上でデバイスを使用している場合に、ユーザに対して設定する IP ネットマスクを示します。この属性値によって、指定されたマスクを使用して Framed-IP-Address にスタティック ルートが追加されることになります。

番号	IETF 属性	説明
10	Framed-Routing	ユーザがネットワーク上でデバイスを使用している場合に、ユーザに対するルーティング方式を示します。この属性に対してサポートされている値は、「None」と「Send and Listen」だけです。 ルーティング方式は次のように数値で指定されます。 • 0：なし • 1：ルーティング パケットの送信 • 2：ルーティング パケットのリッスン • 3：ルーティング パケットの送信とリッスン
11	Filter-Id	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。この属性は、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。
12	Framed-MTU	最大伝送ユニット（MTU）が PPP 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。

番号	IETF 属性	説明
13	Framed-Compression	リンクに使用される圧縮プロトコルを示します。この属性により、EXEC認可時に生成される PPP または SLIP オートコマンドに「/compress」が追加されます。これは EXEC 認可以外には実装されていません。 圧縮プロトコルは次のように数値で指定されます。 • 0：なし • 1：VJ-TCP/IP ヘッダー圧縮 • 2：IPX ヘッダー圧縮
14	Login-IP-Host	Login-Service 属性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。
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。 • 0：Telnet • 1：Rlogin • 2：TCP-Clear • 3：PortMaster • 4：LAT
16	Login-TCP-Port	Login-Service 属性も存在する場合に、ユーザを接続すべき TCP ポートを定義します。
18	Reply-Message	RADIUS サーバを使用してユーザに表示される可能性のあるテキストを示します。この属性はユーザ 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。

番号	IETF 属性	説明
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。デバイス 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。この属性は 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	状態	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。この属性は CHAP チャレンジにしか適用できません。
25	Class	（アカウンティング）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ティング 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

番号	IETF 属性	説明

26	Vendor-Specific	ベンダーに一般使用に適さない独自の拡張属性の使用を許可します。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダータイプ 1（名前は「cisco-avpair」）です。値は、次の形式のストリングです。
		
		`protocol : attribute sep value`
		
		「protocol」は、特定の認可タイプに使用するシスコの「protocol」属性の値です。「attribute」および「value」は、シスコの TACACS+ 仕様で定義されている適切な AV ペアです。「sep」は、必須の属性の場合は「=」、任意指定の属性の場合は「*」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。
		
		`cisco-avpair= ”ip:addr-pool=first“`
		`cisco-avpair= ”shell:priv-lvl=15“`
		
		1つめの例は、IP認可の際（PPP の IPCP アドレスの割り当て中）にシスコの「Multiple Named ip address Pools」機能を有効化します。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。
		
		表 1 に、サポートされているベンダー固有 RADIUS 属性（IETF 属性 26）を示します。

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。この属性値は、ユーザ単位の絶対タイムアウトになります。

番号	IETF 属性	説明
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。この属性値は、ユーザ単位のセッションタイムアウトになります。
29	Termination-Action	終了は次のように数値で指定されます。 • 0：デフォルト • 1：RADIUS 要求
30	Called-Station-Id	（アカウンティング）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（着信番号識別サービス（DNIS）または同様の技術を使用）。この属性は、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	（アカウンティング）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技術を使用）。この属性の値は、TACACS+ の「remote-addr」の値と同じです。この属性は、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。**radius-server attribute 32 include-in-access-req** 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 属性 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、完全修飾ドメイン名（FQDN）が属性内で送信されます。

番号	IETF 属性	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属性。この属性は、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	ユーザをローカル エリア トランスポート（LAT）で接続すべきシステムを示します。この属性は、EXEC モードでのみ使用できます。
35	Login-LAT-Node	ユーザが LAT で自動的に接続されるノードを示します。
36	Login-LAT-Group	ユーザに使用が認可されている LAT グループ コードを識別します。
37	Framed-AppleTalk-Link	AppleTalk デバイスであるシリアル 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	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	（アカウンティング）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	（アカウンティング）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	（アカウンティング）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。

番号	IETF 属性	説明
43	Acct-Output-Octets	（アカウンティング）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	（アカウンティング）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ティング識別子。Acct-Session ID の番号は、デバイスの電源を入れ直したり、ソフトウェアをリロードしたりするたびに、1 から再開します。この属性を 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 **radius-server attribute 44 include-in-access-req** コマンドを使用します。
45	Acct-Authentic	（アカウンティング）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。この属性は、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、この属性が省略されます。
46	Acct-Session-Time	（アカウンティング）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	（アカウンティング）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	（アカウンティング）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。

番号	IETF 属性	説明
49	Acct-Terminate-Cause	（アカウンティング）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。 **1.** ユーザ要求 **2.** 搬送が失われた **3.** サービスの消失 **4.** アイドル タイムアウト **5.** セッション タイムアウト **6.** 管理リセット **7.** 管理リブート **8.** ポート エラー **9.** NAS エラー **10.** NAS 要求 **11.** NAS リブート **12.** ポートの不要化 **13.** ポートの横取り **14.** ポートの保留 **15.** 使用できないサービス **16.** コールバック **17.** ユーザー エラー **18.** ホスト要求 （注） 属性49に関して、シスコは1 ～ 6、8、9、12、および15 ～ 18 の値をサポートしています。

番号	IETF 属性	説明
50	Acct-Multi-Session-Id	（アカウンティング）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ティング識別子。 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。
51	Acct-Link-Count	（アカウンティング）アカウンティング 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ティング要求内にこの属性を追加できます。
52	Acct-Input-Gigawords	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。
53	Acct-Output-Gigawords	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。

番号	IETF 属性	説明
55	Event-Timestamp	NAS 上でイベントが発生した時刻を記録します。属性 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。アカウンティングパケット内で RADIUS 属性 55 を送信するには、**radius-server attribute 55 include-in-acct-req** コマンドを使用します。 （注） アカウンティング パケット内で Event-Timestamp 属性を送信するには、ネットワーク デバイスのクロックを設定する必要があります（ネットワーク デバイスのクロックの設定方法については、ネットワーク管理の設定ガイドの「基本システム管理」の章の「基本システム管理の実行」を参照してください）。ネットワークデバイスがリロードされるたびにネットワークデバイスのクロックを設定するのを避けるには、**clock calendar-valid** 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、ネットワーク管理の設定ガイドの「基本システム管理」の章の「時刻およびカレンダーサービスの設定」を参照してください）。
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 ハンドシェーク認証プロトコル チャレンジが保存されます。

番号	IETF 属性	説明
61	NAS-Port-Type	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。 • 0：非同期 • 1：同期 • 2：ISDN 同期 • 3：ISDN 非同期（V.120） • 4：ISDN 非同期（V.110） • 5：仮想
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[3]	使用されているトンネリング プロトコルを示します。シスコのソフトウェアでは、この属性の値として L2TP がサポートされます。
65	Tunnel-Medium-Type1	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。この属性には、このリリースで使用可能な値（IP）が 1 つしかありません。この属性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。

番号	IETF 属性	説明
66	Tunnel-Client-Endpoint	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 属性が Access-Request パケットに含まれている場合、RADIUS サーバはその値を指示として取得する必要があります。この属性は、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 属性が含まれています。この属性は、Tunnel-Server-Endpoint 属性や Acct-Tunnel-Connection-ID 属性と一緒に使用して、アカウンティ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。 次のように、この属性の 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。 127.0.0.0 は loopback0 の IP アドレスを使用する必要があることを示し、127.0.0.1 は loopback1 の IP アドレスを使用する必要があることを示します。127.0.0.X は、実際のトンネル クライアント エンドポイントの IP アドレスに loopbackX の IP アドレスを使用する必要があることを示します。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。

番号	IETF 属性	説明
67	Tunnel-Server-Endpoint1	トンネルのサーバ端のアドレスを示します。この属性のフォーマットは、Tunnel-Medium-Type の値によって異なります。リリースによっては、トンネル メディア タイプとして IP のみがサポートされ、IP アドレスまたは LNS のホスト名がこの属性に使用できる場合があります。
68	Acct-Tunnel-Connection-ID	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。この属性は、Start、Stop、または上記のいずれかを値として持つ Acct-Status-Type 属性と一緒に Accounting-Request パケットに含める必要があります。この属性は、Tunnel-Client-Endpoint 属性や Tunnel-Server-Endpoint 属性と一緒に使用して、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。
69	Tunnel-Password1	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。この属性は、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 属性に変換されます。 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と、認可エラーが発生する可能性があります。属性 69 を有効にして、暗号化されていないパスワードを受信できるようにするには、グローバル コンフィギュレーション モードで **radius-server attribute 69 clear** コマンドを使用します。
70	ARAP-Password	AppleTalk Remote Access Control（ARAP）の Framed-Protocol を含む Access-Request パケットを識別します。

番号	IETF 属性	説明
71	ARAP-Features	ARAP feature flags パケットで NAS からユーザに送信する必要のある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 リストの使用方法を示します。
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。
74	ARAP-Security-Data	Access-Challenge および Access-Request パケットに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。
75	Password-Retry	ユーザが切断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。この属性は start と stop のアカウンティング レコード内で生成されます。
78	Configuration-Token	使用するユーザ プロファイルのタイプを示します。この属性は、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 を使用してダイヤルイン 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。

番号	IETF 属性	説明
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-ID1	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。この属性は、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属性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。この属性は、Tunnel-Link-Stop の値を持つ Acct-Status-Type 属性と一緒に 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、この属性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。

番号	IETF 属性	説明
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。 この属性の値は次のように数値で指定されます。 • 0：No - パスワードは無視されます。 • 1：Yes - パスワードが認証に使用されます。

[3] この RADIUS 属性は、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

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Commands List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

RFC

RFC	タイトル
RFC 2865	『Remote Authentication Dial In User Service (RADIUS)』
RFC 2866	『RADIUS Accounting』
RFC 2867	『RADIUS Accounting Modifications for Tunnel Protocol Support』
RFC 2868	『RADIUS Attributes for Tunnel Protocol Support』
RFC 2869	『RADIUS Extensions』

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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

RADIUS 属性の概要と RADIUS IETF 属性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3 : RADIUS* 属性の概要と *RADIUS IETF* 属性の機能情報

機能名	リリース	機能情報
RADIUS IETF 属性	Cisco IOS Release 11.1	この機能は、Cisco IOS Release 11.1 で導入されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。