RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値

インターネット技術特別調査委員会（IETF）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバの間でベンダー固有属性（属性 26）を使用してベンダー固有の情報を伝達する方法が規定されています。属性26はベンダー固有属性をカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張属性をサポートできます。

RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値に関する情報

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、特定の認可タイプを表すシスコの「protocol」属性です。使用可能なプロトコルには、IP、IPX、VPDN、VOIP、SHELL、RSVP、SIP、AIRNET、OUTBOUND があります。「attribute」および「value」は、シスコの TACACS+ 仕様で定義されている適切な属性値（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。

たとえば、次の AV ペアは IP 許可の際（PPP の IPCP アドレス割り当ての際）、シスコの「multiple named ip address pools」機能を起動します。

```
cisco-avpair= ”ip:addr-pool=first“
```

「*」を挿入すると、AV ペア「ip:addr-pool=first」は任意指定になります。AV ペアはオプションにできることに注意してください。

```
cisco-avpair= ”ip:addr-pool*first“
```

次に、ネットワーク アクセス サーバからユーザがログインしたときに、すぐに EXEC コマンドを実行する方法の例を示します。

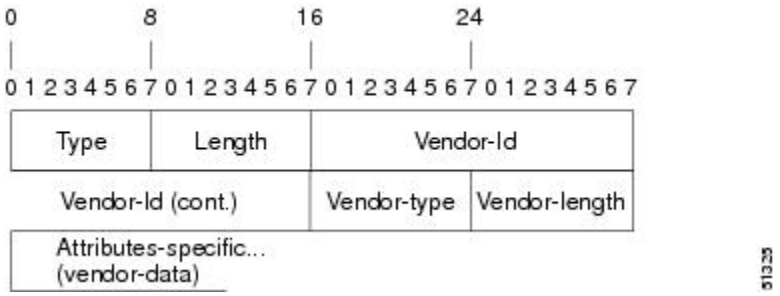
```
cisco-avpair= ”shell:priv-lvl=15“
```

属性 26 には、次の 3 つの要素が含まれています。

- タイプ
- 長さ
- ストリング（またはデータ）
  - Vendor-Id
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

次の図は、属性 26 の「背後で」カプセル化される VSA のパケット形式を示します。

図 *1* : 属性 *26* の背後でカプセル化される *VSA*



（注） VSA の形式はベンダーが指定します。Attribute-Specific フィールド（Vendor-Data とも呼ばれる）は、ベンダーによるその属性の定義によって異なります。

次の表に、「ベンダー固有 RADIUS IETF 属性テーブル」（次の 2 番目の表）で表示される重要なフィールドを示します。これは、サポート対象のベンダー固有 RADIUS 属性（IETF 属性 26）を表示します。

表 *1*：ベンダー固有属性表のフィールドの説明

フィールド	説明
番号	次の表に示されるすべての属性は、IETF 属性 26 の拡張です。
ベンダー固有のコマンドコード	特定のベンダーの識別に使用する定義されたコード。コード 9 は Cisco VSA、311 は Microsoft VSA、529 は Ascend VSA を定義します。
サブタイプ番号	属性 ID 番号。この番号は、属性 26 の背後でカプセル化される「2 番めのレイヤ」の ID 番号であること以外、IETF 属性の ID 番号に似ています。
属性	属性の ASCII ストリング名。
説明	属性の説明。

表 *2*：ベンダー固有 *RADIUS IETF* 属性

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
MS-CHAP 属性				
26	311	1	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでしか使用されません。この属性は、PPP CHAP ID と同じです（RFC 2548）。
26	311	11	MSCHAP-Challenge	ネットワーク アクセス サーバが MS-CHAP ユーザに送信するチャレンジが含まれます。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。（RFC 2548）。
VPDN 属性				
26	9	1	l2tp-busy-disconnect	LNS の vpdn-group で、事前にコピーするよう設定された仮想テンプレートを使用している場合、この属性は、接続先の事前にコピーされたインターフェイスが検索されない、新しい L2TP セッションのディスポジションを制御します。属性が true（デフォルト）の場合、セッションが LNS により切断されます。そうでない場合は、新しいインターフェイスが仮想テンプレートからコピーされます。
26	9	1	l2tp-cm-local-window-size	L2TP 制御メッセージの最大受信ウィンドウ サイズを指定します。この値は、トンネルの確立中にピアにアドバタイズされます。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	l2tp-drop-out-of-order	正しくない順序で受信したデータ パケットをドロップして、シーケンス番号を順守します。これは受信した場合の処理方法であって、データ パケット上でシーケンス番号が送信されるわけではありません。
26	9	1	l2tp-hello-interval	hello キープアライブ インターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。
26	9	1	l2tp-hidden-avp	イネーブルにすると、L2TP 制御メッセージで、大文字小文字を区別する AVP にスクランブルがかけられるか、または非表示になります。
26	9	1	l2tp-nosession-timeout	タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。
26	9	1	tunnel-tos-reflect	LNS でトンネルに入るパケットに対して、IP ToS フィールドを各ペイロード パケットの IP ヘッダーからトンネル パケットの IP ヘッダーにコピーします。
26	9	1	l2tp-tunnel-authen	この属性を設定すると、L2TP トンネル認証が実行されます。
26	9	1	l2tp-tunnel-password	L2TP トンネル認証および AVP 隠蔽に使用される共有秘密。
26	9	1	l2tp-udp-checksum	これは認可属性で、L2TP がデータ パケットに対して UDP チェックサムを実行する必要があるかどうかを定義します。有効な値は「yes」と「no」です。デフォルトは「no」です。
H323 属性				
26	9	23	Remote-Gateway-ID（h323-remote-address）	リモート ゲートウェイの IP アドレスを示します。
26	9	24	Connection-ID（h323-conf-id）	会議 ID を識別します。
26	9	25	Setup-Time（h323-setup-time）	以前、グリニッジ標準時（GMT）およびズール タイムと呼ばれていた協定世界時（UTC）でのこの接続のセットアップ時間を示します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	26	Call-Origin（h323-call-origin）	ゲートウェイに対するコールの発行元を示します。有効値は、originating および terminating です（回答）。
26	9	27	Call-Type（h323-call-type）	コールのレグ タイプを示します。使用可能な値は **telephony** と **VoIP** です。
26	9	28	Connect-Time（h323-connect-time）	このコール レッグの UTC での接続時間を示します。
26	9	29	Disconnect-Time（h323-disconnect-time）	このコール レッグが UTC で接続解除された時間を示します。
26	9	30	Disconnect-Cause（h323-disconnect-cause）	Q.931 仕様によって、接続がオフラインにされた理由を示します。
26	9	31	Voice-Quality（h323-voice-quality）	コールの音声品質に影響する Impairment Factor（ICPIF）を指定します。
26	9	33	Gateway-ID（h323-gw-id）	下位のゲートウェイの名前を示します。
大規模のダイヤルアウト属性				
26	9	1	callback-dialstring	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。
26	9	1	data-service	説明はありません。
26	9	1	dial-number	ダイヤルする番号を定義します。
26	9	1	force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。
26	9	1	map-class	ユーザ プロファイルに、ダイヤルアウトするネットワーク アクセス サーバ上で同じ名前のマップ クラスで設定される情報の参照を許可します。
26	9	1	send-auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
その他の属性				
26	9	2	Cisco-NAS-Port	NAS-Port アカウンティングに追加的なベンダー固有属性（VSA）を指定します。属性値ペア（AVPair）ストリングの形式で追加的な NAS-Port 情報を指定するには、radius-server vsa send 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。 （注） この VSA は、通常アカウンティングで使用されますが認証（Access-Request）パケットで使用される場合もあります。
26	9	1	min-links	MLP に対するリンクの最小数を設定します。
26	9	1	proxyacl#<n>	ダウンロード可能なユーザ プロファイル（ダイナミック ACL）を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。
26	9	1	spi	登録中にホーム エージェントがモバイル ノードの認証で必要とする認証情報を伝送します。この情報は、**ip mobile secure host <addr>** コンフィギュレーション コマンドと同じ構文です。基本的に、この文字列に続く残りのコンフィギュレーション コマンドはそのまま含まれます。これにはセキュリティ パラメータ インデックス（SPI）、キー、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。
26	9	1	client-mac-address	PPPoE クライアントの MAC アドレスが含まれます。 （注） この属性は、PPP over Ethernet（PPPoE）または PPP over ATM（PPPoA）にのみ適用できます。

NAS を設定して VSA を認識し使用する方法については、「RADIUS の設定」機能モジュールの「ベンダー固有 RADIUS 属性を使用するためのルータの設定」セクションを参照してください。

RADIUS Disconnect-Cause 属性値

Disconnect-cause 属性値は、接続がオフラインにされた理由を指定します。属性値は、アカウンティング要求パケットで送信されます。セッションの認証が失敗しても、これらの値は、セッションの終了時に送信されます。セッションが認証されないと、属性が開始レコードを生成せずに終了レコードを発生させる可能性があります。

次の表に、Disconnect-Cause（195）属性の原因コード、値、および説明を示します。

（注） Disconnect-Cause は、RADIUS AVPairs で使用されるごとに 1000 ずつ増分されます。たとえば、disc-cause 4 は 1004 になります。

表 *3 : Disconnect-Cause* 属性値

原因コード	値	説明
2	Unknown	理由は不明。
4	CLID-Authentication-Failure	calling-party 数の認証の失敗。
10	No-Carrier	キャリアが検出されない。 （注） 最初のモデム接続中に接続解除があると、コード 10、11、および 12 が送信される場合があります。
11	Lost-Carrier	キャリアの喪失。
12	No-Detected-Result-Codes	モデム結果コード検出の失敗。
20	User-Ends-Session	ユーザがセッションを終了した。 （注） コード 20、22、23、24、25、26、27、および 28 は、EXEC セッションに適用されます。
21	Idle-Timeout	ユーザ入力待機中のタイムアウト。 コード 21、100、101、102、および 120 は、すべてのセッション タイプに適用されます。
22	Exit-Telnet-Session	既存の Telnet セッションによる接続解除。
23	No-Remote-IP-Addr	SLIP/PPP への切り替え不能。リモート エンドに IP アドレスがない。
24	Exit-Raw-TCP	既存の raw TCP による接続解除。
25	Password-Fail	間違ったパスワード。

原因コード	値	説明
26	Raw-TCP-Disabled	Raw TCP がディセーブルにされた。
27	Control-C-Detected	Control-C が検出された。
28	EXEC-Process-Destroyed	EXEC プロセスが破棄された。
40	Timeout-PPP-LCP	PPP LCP ネゴシエーションがタイムアウトした。 （注） コード 40、41、42、43、44、45、および 46 は、PPP セッションに適用されます。
41	Failed-PPP-LCP-Negotiation	PPP LCP ネゴシエーションが失敗した。
42	Failed-PPP-PAP-Auth-Fail	PPP PAP 認証が失敗した。
43	Failed-PPP-CHAP-Auth	PPP CHAP 認証が失敗した。
44	Failed-PPP-Remote-Auth	PPP リモート認証が失敗した。
45	PPP-Remote-Terminate	PPP がリモート エンドから Terminate Request を受信した。
46	PPP-Closed-Event	上位層がセッションの終了を要求した。
63	PPP-Echo-Replies	TCP 接続が終了した。
100	Session-Timeout	セッションがタイムアウトした。
101	Session-Failed-Security	セキュリティ上の理由から、セッションが失敗した。
102	Session-End-Callback	コールバックにより、セッションが終了した。
120	Invalid-Protocol	検出されたプロトコルがディセーブルにされていたため、コールが拒否された。
600	VPN-User-Disconnect	クライアントによってコールが接続解除された（PPP 経由）。 LNS がクライアントから PPP terminate request を受信するとコードが送信されます。
601	VPN-Carrier-Loss	キャリアの喪失。これは回線が物理的に普通になった結果である場合があります。 クライアントがダイヤラを使用してダイヤルアウトできない場合、コードが送信されます。
602	VPN-No-Resources	コールの処理に使用できるリソースがない。 クライアントがメモリを割り当てることができない場合、コードが送信されます（メモリの不足）。

原因コード	値	説明
603	VPN-Bad-Control-Packet	L2TP または L2F 制御パケットが間違っている。 このコードは、必須の属性値ペア（AVP）が欠落しているなど、ピアから受信した制御パケットが無効な場合に送信されます。L2TP を使用すると、コードは 6 回の再送信後に送信されます。L2F を使用すると、再送信の回数はユーザ設定が可能です。 （注） トンネルにアクティブなセッションがある場合は、VPN-Tunnel-Shut が送信されます。
604	VPN-Admin-Disconnect	管理上の接続解除。これは、VPN ソフトシャットダウンの結果である場合があります。これは、クライアントが最大セッション制限に達するか、最大ホップカウントを超過した場合に発生します。 トンネルが、**clear vpdn tunnel** コマンドの発行によってダウンした場合に、コードが送信されます。
605	VPN-Tunnel-Shut	トンネルのティアダウン、またはトンネルのセットアップが失敗した。 トンネルにアクティブなセッションがあり、トンネルがダウンした場合にコードが送信されます。 （注） このコードはトンネルの認証が失敗した場合は、送信されません。
606	VPN-Local-Disconnect	LNS PPP モジュールによって、コールが接続解除された。 LNS がクライアントに PPP terminate request を送信するとコードが送信されます。これは通常の PPP 接続解除が LNS によって開始されたことを示します。
607	VPN-Session-Limit	VPN ソフト シャットダウンがイネーブルになった。 前述したソフト シャットダウンの制約事項のいずれかによってコールが拒否されると、コードが送信されます。
611	VPDN-Tunnel-In-Resync	VPDN トンネルは HA 再同期中です。

その他の参考資料

ここでは、RADIUS ベンダー固有属性（VSA）および RADIUS Disconnect-Cause 属性値に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
セキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
セキュリティ サーバ プロトコル	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「セキュリティ サーバ プロトコル」の項
RADIUS Configuration	「RADIUS の設定」機能モジュール。

標準

標準	タイトル
インターネット技術特別調査委員会（IETF）インターネット ドラフト：Network Access Servers Requirements	「Network Access Servers Requirements: Extended RADIUS Practices」

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『Remote Authentication Dial In User Service (RADIUS)』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値の機能情報

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 *4 : RADIUS* ベンダー固有属性（*VSA*）および *RADIUS Disconnect-Cause* 属性値の機能情報

機能名	リリース	機能情報
VPDN Disconnect Cause のアカウンティング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。

機能名	リリース	機能情報
ベンダー固有の RADIUS 属性	Cisco IOS XE Release 2.1	このマニュアルは、ネットワーク アクセス サーバと RADIUS サーバの間でベンダー固有属性（属性 26）を使用してベンダー固有の情報を伝達する方法を規定するインターネット技術特別調査委員会（IETF）ドラフト標準を扱います。属性 26 はベンダー固有属性をカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張属性をサポートできます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

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。